

1 UNITED STATES DISTRICT COURT  
2 FOR THE DISTRICT OF ALASKA

3 UNITED STATES OF AMERICA, )  
4 Plaintiff, )  
5 vs. ) CASE NO. 3:17-cr-00095-SLG  
6 MATTHEW WILLIAM SCHWIER, )  
7 Defendant. )  
----- )

8  
9  
10 PARTIAL TRANSCRIPT OF HEARING ON MOTIONS FOR  
11 RECONSIDERATION (1:36 p.m. - 1:47 p.m.)  
12 **BEFORE THE HONORABLE SHARON L. GLEASON, DISTRICT JUDGE**  
13 November 26, 2019; 1:09 p.m.  
14 Anchorage, Alaska

14 **FOR THE GOVERNMENT:**

15 Office of the United States Attorney  
16 BY: JONAS M. WALKER and CHARISSE M. ARCE  
17 222 West 7th Avenue, #9  
18 Anchorage, Alaska 99513  
19 (907) 271-5071

18 **FOR THE DEFENDANT:**

19 Law Offices of Robert Herz, P.C.  
20 BY: ROBERT M. HERZ  
21 431 West 7th Avenue, Suite 107  
22 Anchorage, Alaska 99501  
23 (907) 277-7171

---

24 **SONJA L. REEVES, RMR-CRR**

25 Federal Official Court Reporter  
222 West 7th Avenue, #4  
Anchorage, Alaska 99513

Transcript Produced from the Stenographic Record

1 (Call to Order of the Court at 1:09 p.m.)

2 (Proceedings took place that are not included  
3 in this Partial Transcript, after which, proceedings  
4 continued as follows:)

5 THE COURT: I understand that perspective. All  
6 right. Thank you.

7 Mr. Herz, go ahead, please.

8 MR. HERZ: Thank you, Your Honor. And I can  
9 put Mr. Fischbach on if necessary, but I think I can  
10 summarize our position. If the Court needs  
11 clarification from Mr. Fischbach, we can offer it.

12 A couple of things. I think the Government's  
13 issue regarding the Wireshark they have indicated is  
14 moot, and I think our point, or the point Mr. Fischbach  
15 was making about, quote-unquote, being able to take  
16 Torrential Downpour while Wireshark is running wasn't a  
17 threat, it was an illustration that the Government's  
18 proposed prophylactic using Wireshark just to determine  
19 if a copy was made is really ineffective.

20 So their goal in using Wireshark would not be  
21 met by using Wireshark. Essentially, unless Wireshark  
22 was being run each and every day of the 21 days and only  
23 if each day, after each day's testing the Wireshark  
24 packets were examined, that would be the only way the  
25 Government would know if a copy got made.

1           If after 21 days of testing it was never  
2 examined, I mean the Wireshark packets were not  
3 examined, then only two possibilities can occur. The  
4 Government seeks to review the packet captures before  
5 trial, in which case they have now discovered attorney  
6 work product, protected information and have discovered  
7 attorney-client information in advance of trial, which  
8 they are not entitled to do. Or the alternative is they  
9 wait until after the trial is complete and then they  
10 want Court permission to examine the packets to see if  
11 copying was made, at which point it's really after the  
12 fact.

13           At that point, if there was copying done, we  
14 didn't do anything to prevent public dissemination of  
15 the software, it's really now being used as evidence to  
16 see if some illegal conduct occurred. So as a  
17 prophylactic measure, it really doesn't serve the  
18 function that the Government states it would serve.

19           THE COURT: Mr. Herz, let me interrupt on that,  
20 because I thought I addressed this in the order as well,  
21 and that is that if there isn't Wireshark or another  
22 type of capture device used, I don't see that  
23 Mr. Fischbach would be able to testify because of the  
24 Daubert issues. I thought I was fairly explicit on  
25 that, maybe in a footnote, but to establish reliability

1 -- and Mr. Fischbach has acknowledged this repeatedly.

2           What I would truly hope to -- so if there is  
3 going to be testimony, then I do intend to order full  
4 discovery of the expert prior to trial, even if the  
5 existing rule doesn't expressly contemplate that, it  
6 will on December 1st I believe. There is going to be a  
7 rule change to 16 that would make that clearer. So  
8 that's my intent is if it's going to be used at trial,  
9 it is fully discoverable, just as I would expect and I  
10 understand the Government has made there.

11           So I wanted you to have that heads-up that  
12 based on the evidence I have heard from both of the  
13 experts, it is extremely improbable that a reliability  
14 standard under Daubert could be established by  
15 Mr. Fischbach without a capture of the work product. So  
16 heads up on that.

17           MR. HERZ: Okay. I appreciate that, Your  
18 Honor. And I guess we can take that up -- that issue up  
19 when it arises, but just as a prefatory response, there  
20 is no other area of science where the reliability of the  
21 science is dependent on audio and video recording or  
22 capturing of the actual testing.

23           Normally the reliability standard is addressed  
24 simply by the expert testifying about the procedures,  
25 the scientific procedures that were utilized in

1 conducting the tests. And that's true when an expert in  
2 DNA testifies about what procedures they used in the  
3 laboratory to produce their DNA results. That's typical  
4 for hair and fibers.

5 Nobody's audio and video recording anything.  
6 They are simply testifying to standard laboratory  
7 procedures. And that's been the case historically even  
8 in computer forensics. So I think there are a number of  
9 valid and different ways to establish the reliability of  
10 testing in computer forensics, not just using a packet  
11 capture program.

12 THE COURT: Well, I'm relying on the testimony  
13 of both experts that's been presented. Mr. Fischbach I  
14 believe -- well, in any event, heads up on that. I was  
15 quite persuaded by the benefits of Wireshark and I tried  
16 to flag that issue in the order, footnote three, page  
17 two of Docket 254.

18 All right. Go ahead, Mr. Herz.

19 MR. HERZ: And we did notice that.  
20 Mr. Fischbach and I did speak -- talk to each other  
21 about it, so we're well aware of the Court's leanings in  
22 that direction.

23 Regarding computer specifications, the Court's  
24 procedure that it outlined actually from the defense  
25 perspective makes a lot of sense in that it would be

1 very helpful to know software specifications and  
2 installation instructions, and then we can tailor a  
3 defense request regarding specifications.

4           At this point, what the Government sounds like  
5 they are doing is they are putting together a computer  
6 based on what their knowledge of the software is and  
7 basically saying that should be adequate. So it sounds  
8 as though they know what the software specifications  
9 are. The problem is they haven't yet shared that with  
10 the defense, and we would like an opportunity to be able  
11 to give specifications to the Government based on how  
12 the software operates, including both versions, not just  
13 version 1.23.

14           And if we don't have that information by  
15 tomorrow, our obligation under the Court's order at 254  
16 is that we have to give specifications, and in the  
17 absence of knowing specifics about the software, we are  
18 very likely going to specify pretty much something very  
19 similar to what the Court saw in the e-mail chain and in  
20 Mr. Fischbach's latest declaration, because we're unable  
21 to specify anything else.

22           And as Mr. Fischbach did point out, some of the  
23 specifications are not simply tailored to the software  
24 specifications, but also to the needs of the software  
25 and hardware Mr. Fischbach needs to run in order to

1 complete his tests.

2           So the specifications we're using take into  
3 account two things: One, the software specifications,  
4 and, two, the hardware and software Mr. Fischbach needs  
5 to use in his testing.

6           So we're concerned if the Government has an  
7 idea about what computer specifications it thinks it  
8 would like to provide to us, we would like to know that  
9 now so we can respond to that tomorrow by our deadline,  
10 or perhaps the Court might want to consider a different  
11 schedule for trading information regarding software  
12 specifications and computer specifications.

13           But as it stands right now, we're probably  
14 going to specify precisely what we have been talking  
15 about in the absence of any additional information  
16 coming from the Government.

17           And so I think the Government has pretty much  
18 said that Wireshark is moot, so respectfully I would  
19 suggest that that means the motion should be denied. On  
20 the other hand, our motion for partial reconsideration  
21 simply addresses the fact that the tests that were  
22 proposed and that the Court has found to be material  
23 cannot be completed with a single network connection and  
24 a single port.

25           And I think Mr. Fischbach made that very clear

1 in his first declaration that was filed, and so the  
2 proposed order we gave the Court eliminates those issues  
3 and allows the testing that's been proposed to move  
4 forward.

5 And then specifically regarding multiple  
6 copies, perhaps we need to clarify that. The issue  
7 involving copies is once Torrential Downpour is  
8 downloaded onto the Government-provided computer, it  
9 would stay there and any additional copies would stay  
10 there, but it's standard computer forensic practice to  
11 have a, quote-unquote, "original copy" on the computer  
12 on which it's installed, and then to make a second copy  
13 or a third copy that you can work on so that you can  
14 always have a reference point to make sure that if there  
15 are any changes they can be documented, because you  
16 don't really want to create by accident any changes.

17 You need to be able to make sure that what  
18 you're working with is in its original condition, so you  
19 need an original copy and then you need a working copy  
20 essentially. And I think Mr. Fischbach can explain that  
21 in more detail if the Court would like, but he's not  
22 talking about making multiple copies outside of the  
23 Government-provided computer domain. All of it stays on  
24 the Government computer, none of it goes anywhere else.  
25 It's just simply creating working copies, which is



1 standard forensic practice.

2 (Requested excerpt concluded, proceedings  
3 continued.)

4

5

CERTIFICATE

6

7

8

9

10

I, Sonja L. Reeves, Federal Official Court Reporter  
in and for the United States District Court of the  
District of Alaska, do hereby certify that the foregoing  
transcript is a true and accurate transcript from the  
original stenographic record in the above-entitled  
matter and that the transcript page format is in  
conformance with the regulations of the Judicial  
Conference of the United States.

11

Dated this 10th day of December, 2019.

12

13

14

15

16

17

18

19

20

21

22

23

24

25

/s/ Sonja L. Reeves  
SONJA L. REEVES, RMR-CRR  
FEDERAL OFFICIAL COURT REPORTER

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
431 W.7<sup>th</sup> Avenue, Suite 107  
Anchorage, Alaska 99501  
907-277-7171 Phone  
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

United States of America, )  
 )  
 Plaintiff, ) Case No. 3:17-cr-0095 SLG  
 )  
 vs. )  
 )  
 Matthew Schwier, )  
 )  
 Defendant. )  
 \_\_\_\_\_ )

**C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE:  
TORRENTIAL DOWNPOUR SOFTWARE**

A period of excludable delay under 18 U.S.C. §3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. A total of 36 days remain before trial must commence pursuant to the Speedy Trial Act.

Comes now, Defendant, Matthew Schwier, by and through counsel, Robert M. Herz, of the Law Offices of Robert Herz, P.C. and hereby moves this court, pursuant to the fifth and sixth amendment of the United States Constitution, and as well Federal Rule of Criminal Procedure 16, and *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny, for an order compelling the government to provide discovery and produce evidence of a copy of the Torrential Downpour software used by the government in its undercover investigation in this case between October 20 and November 24, 2016, those dates being approximate.

## BACKGROUND FACTS

### A. The Indictment.

On April 26, 2019 the government filed a third superseding indictment in this case. Mr. Schwier was arraigned on the new indictment on May 1, 2019. Count 1 of the third superseding indictment reads as follows:

On or about October 20, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, did ***knowingly possess, and knowingly access*** with intent to view, any computer disk, and any other material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8)(a), that has been mailed, and shipped and transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and that was produced using materials that have been mailed, and shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Any image of child pornography involved in the offense involved a prepubescent minor and a minor who had not attained 12 years of age. All of which is in violation of 18 U.S.C. § 2252A(a)(5)(B), (b)(2).

Emphasis supplied.

Count 2 of the third superseding indictment reads as follows:

On or about November 22, 2016, to November 24, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, did **knowingly distribute** any child pornography, as defined in 18 U.S.C. § 2256(8)(a), that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. All of which is in violation of 18 U.S.C. § 2252A(a)(2)(A), (b)(1).

Emphasis supplied. Of note, in this iteration of the distribution count, the government simply claims that Mr. Schwier did “knowingly distribute *any* child pornography....”

The government does not specify an image or provide a file designation nor describe the number of images distributed. However, the government will concede only one act of “distribution” allegedly transpired in this case when the FBI allegedly downloaded and

received one file alleged to contain child porn. A comparison of this iteration of the charge to how it was written in the Second Superseding Indictment is illustrative. Count 2 in the Second Superseding indictment reads as follows:

On or about November 22, 2016, to November 24, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, *did knowingly distribute*, by any means and facility of interstate and foreign commerce, a visual depiction of a minor engaging in sexually explicit conduct, *to wit: "1180842565051.jpg,"* the production of which involved the use of minors engaging in sexually explicit conduct. The production of the visual depiction involved a prepubescent minor and minor under 12 years of age engaging in sexually explicit conduct and the visual depiction was of such conduct. All of which is in violation of 18 U.S.C. § 2252(a)(2), (b)(1).

Emphasis supplied.

As the court can see, in the Second Superseding Indictment the government specifies a single and sole image as allegedly distributed, and indeed, that is the only file the FBI claims that it ever downloaded and received, based on all the discovery provided by the government to date.

## **B. The Investigation**

### **1. The October surreptitious searches.**

According to SA Allison's affidavit in support of the search warrant application, 3:17-mj-00198 DMS, dated April 28, 2017, on or about October 20, 2016 he conducted a surreptitious search of an IP address, later identified as being associated with Mr. Schwier. The agent attempted to download data from the identified IP address, using an FBI modified program of the bitTorrent protocol. This FBI modified program is only available to law enforcement and is known as "Torrential Downpour." This FBI program has never been scientifically validated or verified to be reliable by any

independent third party and shown to work in the manner claimed by the FBI. The FBI program attempted to download data, identified by a specific hash value, believed to contain child pornography. According to the agent, the hash value represents 3439 pieces of data representing a total of 66 files. Allegedly the target IP address “acknowledged” that it had 1387 pieces of data *none of which were downloaded or received by the FBI*. In addition, the modified FBI program allegedly reported that the IP address “possessed” 45 of the files. According to the SA Allison 6 of these files contain child porn based on a review of archived FBI files. *None of those files were downloaded or received by the FBI*.

Later that same day, the FBI program made a second attempt to download data from the same target IP address. The attempt to download data again used an unidentified hash value believed to contain child porn. This hash value, according to the agent, contains 6595 pieces of data and represents 249 files. Of these, the FBI program allegedly identified the IP address as having 6474 pieces of the data and 204 complete files. Based on a review conducted by SA Allison of FBI archived files, allegedly 74 of these files contain child porn. However, as before during the first attempt, *none of the 6474 pieces of data were downloaded or received by the FBI, and none of the files were downloaded or received by the FBI*. See, paragraphs 22-23 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS.

**2. The November surreptitious searches. The FBI again experienced problems downloading files just as it had during the October 2016 surreptitious searches.**

According to SA Allison’s affidavit in support of the search warrant application, 3:17-mj-00198 DMS, dated April 28, 2017, on or about November 20, 2016 between 7:23 p.m. and 7:27 a.m. the next day, he conducted a surreptitious search of an IP address, later identified as being associated with Mr. Schwier. The agent attempted to

download data from the identified IP address, using an FBI modified program of the bitTorrent protocol. The FBI program attempted to download data, identified by specific hash values, believed to contain child pornography. According to the agent, the hash values represent 1545 pieces of data representing a total of 306 files. Allegedly the target IP address “acknowledged” that it had all 1545 pieces of data *none of which were downloaded or received by the FBI*. In addition, the modified FBI program allegedly reported that the IP address “possessed” all 306 of the files. According to SA Allison 28 of these files contain child porn based on his review of archived FBI files. *None of those files were downloaded or received by the FBI.*

On that same day, the FBI program made a second attempt to download data from the same target IP address between 7:43 p.m. and 8:26 p.m.. The attempt to download data again used an identified hash value believed to contain child porn. This hash value, according to the agent, contains 543 pieces of data and represented one (1) file. The FBI program allegedly identified the IP address as having all 543 pieces of the data and the one (1) complete file. Based on SA Allison’s review of FBI archived files, allegedly the one file contained child porn. However, as before, during the first attempt, *none of the 543 pieces of data were downloaded or received by the FBI, and none of the single file was downloaded or received by the FBI.* See, paragraphs 24-25 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS.

On November 22, 2016 a third search of the identified IP address was initiated. This third attempt to download data began on November 22 at 8:48 p.m. and ended on November 24, 2016 at 9:02 p.m. The attempt to download data again used an identified hash value believed to contain child porn. This hash value, according to the agent, contains 4861 pieces of data and represents 5616 files. Of these, the FBI program allegedly identified the IP address as having 4619 pieces of the data and 5309 complete

files. This time two files were completely downloaded and received by the FBI. No other pieces of data and no other files alleged to be “possessed” were downloaded or received by the FBI. Based on SA Allison’s review of the two files received, only one file was determined by the agent to contain child porn. The file designation for that file is 1180842565051.jpg. See, paragraphs 26 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS. It is this one file that forms the basis of count 2 in the Third Superseding Indictment.

### **C. The Forensic Search Of Mr. Schwier’s Hard Drives.**

#### **1. The subsequent FBI search found nothing related to any putative data or files from October 20, 2016 on any of Mr. Schwier’s computers or hard drives.**

The search warrant application was granted by the court on April 28, 2017 and a search of Mr. Schwier’s residence commenced on May 1, 2017. A number of electronic media were seized, including several computers containing internal hard drives, and some external hard drives as well. Subsequent to these items being seized they were forensically analyzed by Agent Allison. Agent Allison reported the results of this forensic evaluation in two “FBI 302s” dated respectively July 7 and July 12, 2017. None of the data or files, and no fragments of any of these files, allegedly identified as being “acknowledged” or “possessed” on October 20, 2016 were found on any media seized from Mr. Schwier. Moreover, AUSA Walker indicated during a hearing before this court on March 25, 2019, that for purposes of count 1 in the Second Superseding Indictment (which alleges the same conduct as in Third Superseding Indictment) that the government could not specify or identify the particular “matter’ or hard drive seized from Mr. Schwier on which any contraband alleged to be possessed on or about October 20 was alleged to be found for purposes of count 1 of the indictment.

**2. The subsequent FBI search of hard drives and computers seized from Mr. Schwier’s residence found nothing related to any putative data or files from November 20, 2016 through November 24, 2016 on any of Mr. Schwier’s computers or hard drives, including the one file allegedly “distributed.”**

None of the data or files, and no fragments of any of these files, allegedly identified as being “acknowledged” or “possessed” on or about November 20 to November 24, 2016 were found on any media seized from Mr. Schwier. There was no trace of the file allegedly downloaded and comprising the file designation 1180842565051.jpg that is the basis for count 2. Defense requests to have access to and to inspect and examine the original file on the original media upon which it was saved by the government when it was downloaded and that comprises 1180842565051.jpg have been denied by the government. The defense requires access to the original file to attempt to determine its actual origins and to authenticate it.

**D. The BitTorrent Network and Torrential Downpour.**

The indictment in this cases alleges that Mr. Schwier downloaded and shared child pornography files using the BitTorrent file-sharing network. BitTorrent is an online peer-to-peer network that allows users to download files containing large amounts of data, such as movies, videos, and music. Instead of relying on a single server to provide an entire file directly to another computer, which can cause slow download speeds, BitTorrent users can download portions of the file from numerous other BitTorrent users simultaneously, resulting in faster download speeds.

To download and share files over the BitTorrent network, a user must install a BitTorrent software “client” on his computer and download a “torrent” from a torrent-search website. A torrent is a text-file containing instructions on how to find, download, and assemble the pieces of the image or video files the user wishes to view. The client software reads the instructions in the torrent, finds the pieces of the target file from



other BitTorrent users who have the same torrent, and downloads and assembles the pieces, producing a complete file. The client software also makes the file accessible to the other BitTorrent users in a shared folder on the user's computer.

Torrential Downpour is law enforcement's modified version of the BitTorrent protocol. Torrential Downpour acts as a BitTorrent user and searches the internet for internet protocol ("IP") addresses offering torrents containing known child pornography files. When such an IP address is found, the program connects to that address and attempts to download the child pornography. The program generates detailed logs of the activity and communications between the program and the IP address. Unlike traditional BitTorrent programs, the government claims that Torrential Downpour downloads files only from a single IP address – rather than downloading pieces of files from multiple addresses – and does not share those files with other BitTorrent users.

#### **E. The Investigations into Defendant's BitTorrent Activity.**

As previously noted in October 2016, Agent Allison used Torrential Downpour to identify an IP address which allegedly was making known child pornography files available on the BitTorrent network. Agent Allison allegedly used Torrential Downpour to connect with this IP address to attempt to download child pornography files on several occasions between October 20, 2016 and November 24, 2016. Presumably had he successfully downloaded any files he would have reviewed the Torrential Downpour activity logs to confirm that the program downloaded complete files solely from this IP address, and would have reviewed the files to confirm that they were child pornography.

Through further investigation, Agent Allison learned the subscriber information for the IP address. He obtained a search warrant for the subscriber's residence, and FBI agents searched the residence on May 1, 2017. They found several items of computer

equipment including several hard drives; all of the equipment was then seized. Mr. Schwier has never made any admission that he had used any computer to knowingly find, download, view or distribute any child pornography. As noted before forensic examinations of the seized media failed to find any of the files allegedly possessed on October 20, or on November 20, or on November 22-24. The forensic examination performed by the FBI did reveal child pornography images on four of the hard drives seized; many of the images though were duplicative of each other. Almost all of the images were thumbnails in a thumbnail cache which could not viewed, manipulated, or distributed by anyone unless using a forensic toolkit available to law enforcement. Notably the file that Torrential Downpour allegedly had downloaded from the IP address was not found on any hard drive or any other seized device.

The government has charged Mr. Schwier with one count of distributing child pornography and three counts of possessing such material. The distribution count is based on the file that Torrential Downpour allegedly downloaded on or about November 22, 2016. The possession counts are based on the child pornography found on the hard drives after the search.

### **ARGUMENT**

Mr. Schwier contends that the Torrential Downpour software is flawed and should be tested and verified by a third party. He also contends that he needs access to the program in order to prepare effective cross examination of Agent Allison and the potential presentation by his own computer expert. Mr. Schwier seeks disclosure of an installable copy of the software pursuant to Federal Rule of Criminal Procedure 16, *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). He also seeks disclosure of Torrential Downpour's user and training manuals. He does not seek the program's source code.

Under Rule 16(a)(1)(E), the government must disclose any “books, papers, documents, data, . . . or portions of any of these items, if the item is within the government’s possession, custody, or control and: (i) the item is material to preparing the defense[.]” To obtain disclosure under subsection (i), “[a] defendant must make a ‘threshold showing of materiality[.]’” *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). “Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present *facts* which would tend to show that the [g]overnment is in possession of information helpful to the defense.” *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (emphasis added); *see also Budziak*, 697 F.3d at 1111-12.

#### **A. Brady v. Maryland**

*Brady v. Maryland*, 373 U.S. 83 (1963), requires the government to disclose to a defendant any and all evidence favorable to him if the evidence is material to guilt or to punishment. The good or bad faith of the prosecution in withholding the evidence is irrelevant: it must be disclosed, even if doubtful, and failure to recognize the evidence does not save the prosecutor from a violation. *Id.* At 87; *Strickler v. Greene*, 527 U.S. 263 (1999); *Youngblood v. West Virginia*, 547 U.S. 867 (2007). Under *Brady* and its progeny the “prosecution,” which includes the prosecuting attorney as well as the investigating agencies, must disclose favorable information that is, or is known to be, in its possession. *Strickler* at 263; *Kyles v. Whitley*, 514 U.S. 419 (1995); *Jackson v. Brown*, 513 F.3d 1057 (9<sup>th</sup> Cir. 2008).

The duty of disclosure extends to evidence relating to the credibility of witnesses. *Strickler* at 263, *Giglio v. United States*, 405 U.S. 150, 154 (1972). The existence or nonexistence of a defense request for the evidence is immaterial to the

prosecution's duty to produce it. *Strickler* at 263; *United States v. Agurs*, 427 U.S. 97, 107 (1976). Even evidence the prosecutor regards as inherently improbable must be disclosed. *In re Chol Soo Lee*, 103 Cal.App.3d 615, 618-619 (1980). "Impeachment evidence ... as well as exculpatory evidence, falls within the Brady rule." *United States v. Bagley*, 473 U.S. 667, 676 (1985). "When the 'reliability of a given witness may well be determinative of guilt or innocence' nondisclosure of evidence affecting credibility falls within this general rule." *Giglio v. United States*, 405 U.S. 150, 15355 (1972). Thus, the prosecution violates due process by "fail[ing] to disclose evidence that the defense might" use "to impeach the Government's witnesses by showing bias or interest." *Bagley*, 473 U.S. at 676. The information need not be admissible so long as it "is likely to lead to favorable evidence that would be admissible." *United States v. Sudikoff*, 36 F.Supp.2d 1196, 1200 (C.D. Cal 1999).

"The prosecution's duty to reveal favorable, material information extends to information that is not in the possession of the individual prosecutor trying the case." *Amado v. Gonzalez*, 758 F.3d 1119, 1134 (9<sup>th</sup> Cir. 2014). In particular, it extends to police officer witnesses. *See e.g., United States v. Price*, 566 F.3d 900, 903 (9<sup>th</sup> Cir. 2009) (reversing and remanding where federal prosecutors failed to learn of exculpatory evidence in the state police's control). The prosecution's duty also extends to situations where there is a dispute between the parties about the significance of the information. The prosecution should not "confuse[] the weight" to be given *Brady* evidence "with its favorable tendency." *Kyles*, 514 U.S. at 451. In order to qualify, the evidence need only have "some weight" that is "favorable" to the defense. *Id.* "[T]he Supreme Court has pronounced that if a prosecutor has doubt about certain evidence' exculpatory value, the prosecutor should err on the side of disclosure." *Schledwitz v. United States*, 169 F.3d 1003, 1014 n.4 (6<sup>th</sup> Cir. 1999)(citing *Kyles*); *United States v. Agurs*, 427 U.S. 97, 108

(1976); *see also United States v. Van Brandy*, 726 F.2d 548, 552 (9<sup>th</sup> Cir. 1984) (“[t]he government, where doubt exists as to the usefulness of evidence, should resolve such doubts in favor of full disclosure”).

### **B. United State’s Attorney Manual**

In addition, the United States Attorney’s Manual rigorously encourages prosecutors “to seek all exculpatory and impeachment information from all members of the prosecution team. Members of the prosecution team include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant. U.S. Dept. of Justice, Justice Manual, § 9-5.001, “Policy Regarding Disclosure of Exculpatory and Impeachment Information.” This policy guides federal prosecutors to probe carefully and to “disclose information that is inconsistent with any element of any crime charged against the defendant or that establishes a recognized affirmative defense, regardless of whether the prosecutor believes such information will make the difference between conviction and acquittal of the defendant for a charged crime.” *Id.* at 9.5001.C. The manual provides for broad interpretation of “impeachment information”: “A prosecutor must disclose information that either casts a substantial doubt upon the accuracy of any evidence—including but not limited to witness testimony—the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information must be disclosed regardless of whether it is likely to make a difference between conviction and acquittal of the defendant for a charged crime” *Id.*

### **C. Discoverability of Investigative Software.**

The Ninth Circuit has addressed the discoverability of government software programs used to investigate child pornography offenses.

Mr. Schwier relies primarily on *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), and cases that have adopted its reasoning. *Budziak* involved the FBI's use of an enhanced version of the LimeWire file-sharing program called "EP2P." *Id.* at 1107. Using that program, the FBI downloaded several child pornography files from an IP address registered to Budziak. *Id.* A forensic examination of his computer revealed multiple child pornography files, including several images the EP2P program had downloaded. *Id.* Budziak was charged with multiple counts of distributing and possessing child pornography. *Id.* The district court denied Budziak's motions to compel disclosure of the government's EP2P program, and he was convicted on each count. *Id.* at 1107-08.

On appeal, the Ninth Circuit held that the district court abused its discretion in denying Budziak's motions to compel. It noted that he did more than assert a generalized need to review the EP2P program before trial; he identified particular defenses to the distribution charges that discovery on the EP2P program could help him develop. *Id.* at 1112. Specifically, he "presented evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his 'incomplete' folder, making it 'more likely' that he did not knowingly distribute any complete child pornography files to [the FBI]." *Id.* at 1112. He also presented "evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings." *Id.* Given this evidence, the Ninth Circuit concluded that "access to the EP2P software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him." *Id.*

Other cases have followed *Budziak*. For example, the district court in *United States v. Crowe*, No. 11 CR 1690 MV, 2013 WL 12335320, at \*7 (D.N.M. Apr. 3, 2013), [Case 3:17-cr-00095-SLG Document 199 Filed 09/12/19 Page 13 of 22](#)

2013), required the government to allow the defense expert to examine and use a copy of the government's confidential Shareaza software at a secure government facility. The court did so because the defendant in *Crowe*, like the defendant in *Budziak*, presented specific evidence to suggest that access to the software was material to preparing the defense. *See id.* Specifically, the defense expert testified that "some of the files alleged to have been found by law enforcement in the shared space of Defendant's computer, were not found there during her analysis." *Id.* See also, *U.S. v. Gonzales*, 2:17-cr-01311-DGC (D.AZ)(Order of court at Doc. 51, filed Feb.19, 2019, ordering disclosure of Torrential Downpour software); *U.S. v. Hartman*, 8:15-cr-00063-JLS (Cen.D. Cal)(Order of court at Doc. 87, filed Nov.24, 2015, ordering disclosure of government proprietary software Peer Spectre and ShareazaLE).

In *United States v. Pirosko*, 787 F.3d 358 (6th Cir. 2015), the court of appeals affirmed a district court decision denying discovery of the "law enforcement tools" used to locate and download child pornography from the defendant's computer. The Sixth Circuit distinguished *Budziak*, noting that *Budziak* had presented the evidence just described *supra*. 787 F.3d at 365-67. The defendant in *Pirosko*, by contrast, "failed to produce any such evidence, simply alleging that he might have found such evidence had he been given access to the government's programs." *Id.* at 365. As a result, discovery was not warranted. *Id.*<sup>1</sup>

---

<sup>1</sup> *See also United States v. Jean*, 891 F.3d 712, 715 (8th Cir. 2018) (affirming denial of motion to compel government software because the defendant was convicted of receiving and possessing child pornography and "the likelihood of any help to [his] defense was 'vanishingly small'"); *United States v. Chiaradio*, 684 F.3d 265, 277 (1st Cir. 2012) (expressing no view on whether the EP2P source code was discoverable under Rule 16 where the defendant "neither contradicted nor cast the slightest doubt upon" the government's evidence that the FBI had downloaded child pornography from his computer); *United States v. Blouin*, 2017 WL 2573993, at \*3 (W.D. Wash. June 14, 2017) (denying motion to compel

Case 3:17-cr-00095-SLG Document 199 Filed 09/12/19 Page 14 of 22

*Budziak* is, of course, binding precedent for this Court. The distinction between it and the *Pirosko* line of cases, just noted, is consistent with traditional Rule 16 principles. As already noted, “[n]either a general description of the information sought nor conclusory allegations of materiality suffice [under Rule 16(a)(1)(E)(i)]; a defendant must present *facts* which would tend to show that the [g]overnment is in possession of information helpful to the defense.” *Mandel*, 914 F.2d at 1219 (emphasis added). In *Budziak* and *Crowe*, the defendants presented evidence to support their contention that discovery of the government software was material to preparing their defense to distribution of child pornography. In the other line of cases, they did not.

**D. Mr. Schwier Has Shown Materiality.**

Counts one and three allege violations of 18 U.S.C. § 2252A(a)(5)(B) and count two alleges a violation of 18 U.S.C. § 2252A(a)(2)(A). The latter section provides criminal punishment for any person who “knowingly receives or distributes, any child pornography . . . . using any means or facility of interstate or foreign commerce . . . including by computer, . . .” Evidence is sufficient to support a conviction for distribution under § 2252A(a)(2) “when it shows that the defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it.” *Budziak*, 697 F.3d at 1109.

---

where the defendant did not dispute that the government’s software downloads files from a single source); *United States v. Maurek*, No. CR-15-129-D, 2015 WL 12915605 at \*3 (W.D. Okla. Aug. 31, 2015) (denying motion to compel where the defendant failed to present specific facts which would tend to show how disclosure of Torrential Downpour would be material to his defense);



Mr. Schwier disputes and certainly casts doubt on whether the government downloaded any child pornography from any device possessed by him, and he disputes that Torrential Downpour consistently works as intended and is free from “bugs” so that it always and reliably downloads from a single source. Mr. Schwier maintains that Torrential Downpour is material to his defense because the distribution charge, Count 2, is based on a child pornography file that Torrential Downpour purportedly downloaded from his computer hard drive but that was not found on any hard drive or other device associated with Mr. Schwier when it was seized by the FBI. Torrential Downpour is also material to his defense because Count 1 specifically alleges he knowingly possessed child pornography on October 20 based on the surreptitious search conducted using Torrential Downpour. The government claims that the Torrential Downpour software allegedly identified and confirmed that child porn files were on a device using a specific IP address later found to be associated with Mr. Schwier. Yet none of those files or even fragments of those files were ever found on any device seized from Mr. Schwier’s residence.

Mr. Schwier has presented an affidavit from his expert, Jeffrey M. Fischbach, confirming that the files are not on any device. Fischbach explains in his Declaration that it is critical to Mr. Schwier’s defense to understand how Torrential Downpour functions in order to determine the program’s reliability and accuracy in identifying the file that Mr. Schwier is charged with knowingly distributing or possessing. *Id.* at ¶ 29. He further states that based on his many years of research and testing of peer-to-peer file sharing software, including BitTorrent, he has discovered that all of these programs “contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable.” *Id.* ¶ 22. Fischbach has opined that all software programs have flaws, and Torrential Downpour is no exception. He bases this opinion on his work in other cases involving Torrential

Downpour and the fact that the files the program allegedly downloaded in this case were not found on Schwier's devices. *Id.* at ¶ 21. Fischbach also provided a plausible explanation for how Torrential Downpour may have erroneously identified Schwier's computer as offering child pornography files over the BitTorrent network. Fischbach explained that, because a torrent is simply a text-file containing the hash values – or “fingerprints” – of the target image and video files, a BitTorrent user who downloads a torrent has fingerprints of the target files, even if he has not yet downloaded them. *Id.* at ¶ 15. Fischbach stated that the actual downloading of the target files occurs only when the client software instructs the torrent to search for those files on the BitTorrent network and download them to a designated folder on the user's computer. *Id.* at ¶ 14. He further stated that a forensic examination of the device used to download the torrent can determine whether the torrent has been used to download the file, and his examination of Schwier's devices revealed no evidence suggesting that he downloaded any files listed that might pertain to counts one through three. *Id.* at ¶ 18. Fischbach opined that Torrential Downpour may have obtained the files from other BitTorrent users, particularly in light of the fact that this is how peer-to-peer file sharing programs are designed to work. *Id.* at ¶ 17.

This evidence brings this case squarely within the holding of *Budziak*. Mr. Schwier has done more than simply request access to the software and argue that it is material to his defense. He has presented evidence that calls into question the government's version of events. Given his evidence, this Court must find that “the functions of the [program] constitute[] a ‘very important issue’ for [Schwier's] defense.” *Budziak*, 697 F.3d at 1112 (quoting *United States v. Cedano-Arellano*, 332 F.3d 568, 571 (9th Cir. 2003)); see *Crowe*, 2013 WL 12335320, at \*7.

Where a defendant has demonstrated materiality, the Court “should not merely defer to government assertions that discovery would be fruitless.” *Budziak*, 697 F.3d at

1112-13. Mr. Schwier “should not have to rely solely on the government’s word that further discovery is unnecessary.” *Id.* at 1113. Because Mr. Schwier has shown that the Torrential Downpour is material to his defense, he should be given access to the program to investigate its reliability and help him prepare for cross-examination of Agent Allison.<sup>2</sup>

Mr. Schwier also contends that Torrential Downpour is material because the program “searches beyond the public domain, essentially hacking computers as it searches for suspect hash values, and over-rides the computer’s settings that otherwise would make files unavailable to be shared.

Mr. Schwier is charged with distributing child pornography based on the government’s claim that the FBI, after apparently at some point identifying his computer as a download candidate for child pornography, infiltrated his computer on October 20, 2016 and attempted to download files. According to the Torrential Downpour software there were allegedly numerous suspect files on the computer. Yet, none of these attempts were successful. The FBI infiltrated his computer again in late November, again according to the software there were numerous suspect files on the computer. Again the FBI attempted to download files, and again all these attempts were unsuccessful, except for two suspect files that were successfully downloaded, and only one that was “verified” to be a prohibited image. Later when the computer hard drive was forensically searched, none of the identified suspected files that

---

<sup>2</sup> Even if the government were to present a log file purportedly showing that Agent Allison used Torrential Downpour to download from Schwier’s device the child pornography file listed in count 2 of the Second Superseding Indictment, and that presumably forms the basis for count 2 in the Third Superseding Indictment, this log file cannot independently confirm that Agent Allison downloaded a complete child pornography file solely from Schwier’s device. Since the log files were created by Torrential Downpour, if the program is flawed in the ways Schwier suggests, these log files would be flawed as well.

Torrential Downpour identified as being on the computer were found on the hard drive. Moreover, the one image that was “successfully” downloaded and “verified” to be a prohibited image also was not found on any hard drive possessed by Mr. Schwier.

The FBI could not find any of the files described by Torrential Downpour as being present and as described in the search warrant affidavit on any of the devices seized from Mr. Schwier. Apart from the allegation of “distribution” in the warrant affidavit, there is no evidence that Mr. Schwier ever physically distributed child pornography to another person. Mr. Schwier may defend the distribution allegation on the basis that he did not knowingly allow others to access files on his computer, and that Torrential Downpour overrode his computer’s settings which were set so as to not share files on the BitTorrent software client. This defense requires access to the Torrential Downpour program. In identical circumstances, the Ninth Circuit ruled that defendant is entitled to discovery of special law enforcement software used to investigate him. *United States v. Budziak*, 697 F.3d 1105 (9<sup>th</sup> Cir. 2012). The court found disclosure of the government software was material to the defense to show that law enforcement may have downloaded only fragments of files from his “incomplete folder; to show that “agents could have used the EP2P software to override his sharing settings”; and because “access to the EP2P software was crucial to Budziak’s ability to assess the program and the testimony of the FBI agents who used it to build the case against him.” *Id* at 1112. The Court held that “the functions of the EP2P software constituted a ‘very important issue’ for Budziak’s defense. Given that the distribution charge against Budziak was premised on the FBI’s use of the EP2P program to download files from him, it is logical to conclude that the functions of the program were relevant to his defense.” *Id*.

Here, the sole evidence of distribution arises from Agent Allison's use of the Torrential Downpour program. This program has been described in testimony by one of its creators as follows:

Torrential Downpour is a law enforcement surveillance software that is used exclusively by law enforcement. It is used to track, investigate, and eventually arrest those sharing child pornography through various P2P sharing networks.... Torrential Downpour is "somewhat unique" in that (1) it is designed to target and download files from a single IP address, as opposed to multiple sources, and restrict downloads to come from only that particular address (this is called a "single source download"); (2) Torrential Downpour creates a detailed log of events for evidentiary purposes; and (3) Torrential Downpour does not share files.

*United States v. Maurek*, 131 F. Supp. 3d 1258, 1261 (W.D. Ok. 2015). The indictment puts the use of this software squarely at issue by claiming that Mr. Schwier distributed child pornography when law enforcement downloaded child pornography from his computer or that he possessed child pornography when the software claimed it was he had it when in fact he did not. The government claims that Mr. Schwier's computer was the sole candidate for each download but acknowledges that BitTorrent software typically assembles a file from multiple sources.

In addition Mr. Schwier seeks disclosure of the "pooled information" that enabled the government to focus on the IP address later determined to be associated with Mr. Schwier.

Mr. Schwier also seeks copies of any license, training materials, user manuals, and instructions associated with the program, needed to effectively cross-examine the investigative officer and/or the government's expert as to their ability to use the program correctly and to testify about it. These materials may also aid in showing that the program was used in a manner that violated Mr. Schwier's rights.

The timing of the police investigation spanning October 2016 to April 2017 also strongly suggests there may have been times that police tried to download files and were unable to do so because sharing was precluded, either by features in the law enforcement software or for other reasons. Such evidence would tend to show that Mr. Schwier did not allow others to download from his computer. Such evidence is discoverable under *Brady* and should be disclosed.

Mr. Schwier also requests chain-of-custody documentation for any files the FBI claim to have downloaded, including but not limited all *meta*-data for any alleged downloaded file. Such documentation is a routine part of the impoundment process for digital evidence and should be provided.

### **CONCLUSION**

Given the problems the FBI had successfully downloading and receiving any files, it is material to the defense of these charges to determine the actual origins of the file with the file designation 1180842565051.jpg. This file was not found on any digital media seized from Mr. Schwier's residence. At this time no known creation or access dates are known to exist for this file, and serious questions exist as to whether this file was ever on any media or device associated with Mr. Schwier. Given the manner in which BitTorrent normally works it is entirely possible this file did not come any device possessed by Mr. Schwier but rather was downloaded from another source. It is imperative that Mr. Schwier have access to the Torrential Downpour software to investigate this and to have access to the actual file as well for inspection and examination. Mr. Schwier has a constitutionally protected right to investigate the Government's claim that this file was downloaded from his computer. Production of the software and the file is essential to the defendant, and to properly preparing a defense and for proper cross-examination of the government's witnesses. Without such access

Mr. Schwier is denied the right to confront the evidence of which he is accused of possessing and distributing.

Respectfully, Mr. Schwier requests an order from the court compelling discovery and the production of the Torrential Downpour software.

DATED at Anchorage, Alaska, this 12th day of September 2019.

THE LAW OFFICES OF ROBERT HERZ, PC  
s/ Robert M. Herz  
431 W. 7<sup>th</sup> Avenue, Suite 107  
Anchorage, Alaska 99501  
Phone 907-277-7171 / Fax 907-277-0281  
[rmherz@gci.net](mailto:rmherz@gci.net)  
AK Bar No. 8706023

**CERTIFICATE OF SERVICE**

I hereby certify that on September 12, 2019, a copy of the foregoing C- Motion to Compel Discovery and Production of Evidence was served electronically on Assistant United States Attorney's Office s/ Robert Herz

## Robert Herz

---

**From:** Robert Herz [rmherz@gci.net]  
**Sent:** Friday, December 06, 2019 5:04 PM  
**To:** 'Walker, Jonas (USAAK) 5'  
**Cc:** 'Jeff M. Fischbach, ABFE'  
**Subject:** RE: Hardware and software Specifications

Mr. Walker,

I would agree that Mr. Fischbach is in the best position to know what his needs are in order to conduct defense testing of the TD software. As such, Mr. Fischbach has concluded his inspection of the system requirements of the laptop supplied by the FBI, and it will not be sufficient to meet defense testing needs. It is a 2014 vintage A1398 MacBook Pro, with minimal speed and memory, and outdated hardware and port specifications. Similar to the machine currently in use at the RCFL, it is unlikely that this laptop also will not support running the Virtual Machines supplied by Mr. Erdely. This machine was the least powerful configuration of MacBook Pro produced in 2014. But, is far slower than the minimum requirements of today's Macs. Notably, at this juncture the Government is seeking an order that Mr. Fischbach only use an Ethernet port. This machine does not have an Ethernet port.

The following are the *minimum requirements* needed in a government supplied machine necessary to conduct defense testing of the TD software. Defense specifications are in black, corresponding specifications of the computer supplied by the government are in red:

2.6GHz 6-core 9th-generation Intel Core i7 processor (4-core 4th generation processor discontinued in 2015 nearly five years ago)

64GB 2666MHz DDR4 memory (16GB 1600 MHz DDR3 -- incapable of additional RAM)

AMD Radeon Pro 5500M with 8GB of GDDR6 memory (2GB discontinued graphics processor)

512GB SSD storage (Unknown)

Thunderbolt / USB-C (No USB-C)

WiFi & RJ45 Ethernet (No Ethernet)

The Mac laptop also must have Bootcamp & **valid** Windows 10 installed.

Please let me know when a machine with these minimum requirements will be supplied and available for Mr. Fischbach's use.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)



---

**From:** Walker, Jonas (USAAC) 5 [mailto:Jonas.Walker@usdoj.gov]  
**Sent:** Friday, December 06, 2019 3:31 PM  
**To:** Robert Herz  
**Cc:** 'Jeff M. Fischbach, ABFE'; Arce, Charisse (USAAC) 1; Russo, Frank (USAAC); Allison, Daryl (AN) (FBI)  
**Subject:** RE: Hardware and software Specifications

Mr. Herz:

Thank you for contacting me regarding your concerns.

Per my email of 12/4 below, the government believes that the computer provided is sufficient to run TD as it would be used in an investigation.

The government does not know what tests Mr. Fischbach intends to run, as the defense has withheld that information from the government. Without knowing what tests Mr. Fischbach intends to run, and the technical requirements of those tests, the government is not in a position to opine regarding what technical specifications are necessary to meet Mr. Fischbach's needs.

Because Mr. Fischbach has access to the technical specifications of the computer, as described below, Mr. Fischbach is the person best situated to answer your question regarding whether the computer is sufficient to run Mr. Fischbach's tests.

Thank you,

-AUSA Jonas M. Walker  
907.271.3983

---

**From:** Robert Herz <rmherz@gci.net>  
**Sent:** Friday, December 6, 2019 2:56 PM  
**To:** Walker, Jonas (USAAC) 5 <JWalker5@usa.doj.gov>  
**Cc:** 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>  
**Subject:** RE: Hardware and software Specifications

Mr. Walker,

I agree the court stayed the requirement that the government does not need to provide the TD computer. But the court did not stay the entire order at Doc. 254. As such, the requirement that the government provide all software documentation related to TD is still binding on the government.

Moreover, I believe this was in recognition that the defense needs the TD software specifications in order to provide a tailored request for computer specifications for the computer that the defense needs to run its tests. Nevertheless, the government prior to knowing what the defense specifications would be, "selected" a computer that the *government believes* the defense should use. This was not the process the court envisioned by its order at Doc.254 and seems a bit "cart before the horse." Given that Doc.254 was not stayed in its entirety, I disagree that the government has complied with the court's orders, or that the court's orders have been exceeded. That Mr. Fischbach is attempting to ascertain the system requirements of the computer the government provided, prior to defense input, only means we are evaluating what has been sent to see if it will meet defense needs. Our preliminary review suggests that it will not be

adequate. When Mr. Fischbach completes his work at the RCFL later today, I will provide the government notice of what specifications are, in fact, needed, and whether the computer sent prematurely will meet defense needs. However, the lack of TD software specifications has significantly hampered the defense in this evaluation.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAC) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Thursday, December 05, 2019 5:44 AM  
**To:** Robert Herz  
**Cc:** 'Jeff M. Fischbach, ABFE'; Monroe, Joseph; Allison, Daryl (AN) (FBI); Steeves, Holly J. (AN) (FBI); Arce, Charisse (USAAC) 1  
**Subject:** RE: Hardware and software Specifications

Mr. Herz:

Good morning. I replied in a separate email chain regarding the defense request for Mr. Monroe to show Mr. Fischbach the computer settings. As indicated, I don't object to that request, and I appreciate Mr. Fischbach's suggestion that he see the settings in person to get the data he needs. That seems like an efficient way to get the data directly to Mr. Fischbach.

At Dkt. 262, the court vacated the order at Dkt. 254 in that the government does not have to provide the TD computer to Mr. Fischbach at this time.

Also in Dkt. 262, the court ordered the defense to provide specifications by 12/6. To assist the defense in this process, I provided the specifications of the selected computer in a prior email chain yesterday; see below, immediately prior to your email.

Accordingly, the government has complied with the Court's orders, and, in fact, has exceeded them, in that Mr. Monroe will be showing the computer details to Mr. Fischbach, which is what Mr. Fischbach requested.

The Court will, no doubt, appreciate the parties' cooperation regarding these technical details.

Thank you,

-AUSA Jonas M. Walker  
907.271.3983

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Wednesday, December 4, 2019 2:49 PM  
**To:** Walker, Jonas (USAAK) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>  
**Cc:** 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>  
**Subject:** RE: Hardware and software Specifications

Mr. Walker,

Unfortunately, this is insufficient information to allow the defense to make a determination whether this machine will be adequate for defense testing purposes. Will you allow Joe Monroe to boot up the computer on Friday in Mr. Fischbach's presence so that more specific information can be obtained about what has been sent?

In addition, does the government intend to provide more and complete information regarding TD software specifications before this Friday, and as required by the court's order at Doc.254?

Thank you for your attention to these requests.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAK) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Wednesday, December 04, 2019 12:41 PM  
**To:** Robert Herz  
**Cc:** 'Jeff M. Fischbach, ABFE'; Allison, Daryl (AN) (FBI)  
**Subject:** RE: Hardware and software Specifications

Mr. Herz:

I am advised that a computer with the following characteristics has been identified, which the government expects to be sufficient:

**Apple MacPro laptop with Windows 10 Pro loaded on Bootcamp partition Laptop has 16GB of RAM, 64-bit Operating System x64 based processor with a 250GB Hard Drive**

Thank you;

-AUSA Jonas M. Walker  
907.271.3983

---

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Tuesday, December 3, 2019 11:41 AM  
**To:** Walker, Jonas (USAAK) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>

Cc: 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>

Subject: Hardware and software Specifications

Mr. Walker,

At Doc. 262 the court ordered the defense to provide the government with the computer specifications the defense deems necessary to allow defense testing of the TD Software on a computer the government will provide for defense testing. Based on information provided to the government in email correspondence, pleadings, and declarations, the defense has made it clear that hardware specifications are predicated in part on the software the computer will run, meaning that it is important to know the specifications of the TD software. Ultimately, defense computer hardware specifications will be based on TD specifications as well as the various software Mr. Fischbach will install and that are needed for defense testing. The court ordered the government at Doc. 254 to provide the defense “with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements.” To date, the government has provided only a user manual for TD version 1.23, and it was redacted. This does not comply with the court order, and prevents the defense from more meaningfully providing computer specifications to the government by this Friday. The defense has provided the government with specifications recently in Mr. Fischbach’s declaration at Doc. 261 para.8. The defense believes that the court intends for the parties to refine these specifications which is why the court changed the defense deadline to December 6. If the parties are to refine the specifications as the court intends, then the government must provide TD software specifications as directed in the court’s order at 254, which in turn will allow the defense to make a more refined and tailored request concerning computer specifications. If the government is not willing to fully disclose software specifications to both TD versions in a timely manner and *before* Friday, which is necessary to allow for defense review and evaluation, then the defense will be unable to refine the specifications previously provided to the government, and those previously provided specifications will stand as to what the defense will be requesting.

Robert M. Herz

Law Offices of Robert Herz, P.C.

The Seventh and E Building

431 West Seventh Avenue, Suite 107

Anchorage, Alaska 99501

Tel. 907-277-7171

Email: [rmherz@gci.net](mailto:rmherz@gci.net)

Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW SCHWIER,

Defendant.

Case No. 3:17-cr-95-SLG-DMS

**ORDER GRANTING MOTION TO DISMISS COUNTS 1 AND 2 AND  
REGULATE PRODUCED DISCOVERY**

The Court, having considered the government's Motion to Dismiss Counts 1 and 2 and Regulate Produced Discovery, the defendant's response at Docket 312, and pursuant to Federal Rules of Criminal Procedure 48 and 16(d), ORDERS that:

1. Count 1 and Count 2 of the Fourth Superseding Indictment at Docket 279 are dismissed without prejudice<sup>1</sup>;
2. By **February 7, 2020**, the defense shall file a certification that Mr. Herz and Mr. Fischbach:
  - a. have deleted, and will not access in the future, the Torrential

---

<sup>1</sup> See *United States v. Hayden*, 860 F.2d 1483, 1487 (9th Cir. 1988) ("If the district court finds that the prosecutor is acting in good faith in making its Rule 48(a) motion [to dismiss without prejudice], it should grant the motion; conversely, Rule 48(a) empowers the district court to exercise its discretion in denying the motion when it specifically determines that the government is acting in bad faith."). The Court finds the government is acting in good faith in seeking the dismissal of the two TD counts. "[W]hen the government requests a Rule 48(a) dismissal in good faith, the district court is duty bound to honor the request." *Id.* at 1488.

Downpour manual produced in discovery, and sealed Dockets 299 and 300; and

- b. will not access in the future the virtual machines the government produced to the defense at the Orange County Regional Computer Forensic Laboratory (OCRCFL), pursuant to the Order at Docket 231, and referred to by the defense at docket 297.

DATED this 31<sup>st</sup> day of January, 2020 at Anchorage, Alaska.

/s/ Sharon L. Gleason  
UNITED STATES DISTRICT JUDGE

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
431 W. 7<sup>th</sup> Avenue, Suite 107  
Anchorage, Alaska 99501  
907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

A period of excludable delay under 18 U.S.C. 3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. As of the date of this filing 36 days remain before trial must commence pursuant to the Speedy Trial Act

**MOTION FOR PARTIAL RECONSIDERATION OF THE COURT’S ORDER AT  
DOC.254 RE: ADDITIONAL TERMS FOR PROTECTIVE ORDER**

Comes now, Matthew Schwier, by and through counsel, Robert M. Herz of the Law Offices of Robert Herz, P.C. pursuant to L.Civ.R. 7.3(h)(1)(A), and the fifth and six amendments of the United States Constitution, hereby moves this court for partial reconsideration of its Order at Doc.254 due to a “manifest error of fact.”

On November 8, 2019 the court ordered the government at Doc. 243 to provide the defense with a copy of the government’s secret proprietary software “Torrential Downpour” used by the government in its surreptitious investigation of Mr. Schwier in this case, so that it could be subjected to independent third party testing, to test among other things the reliability and accuracy of the software. The court gave the government 7 days to comply with the order. The court also invited the government to propose additional terms to the protective order previously entered at Doc.231 if “warranted.” On the day the government was ordered to release the software, the government at Doc.244 filed a motion seeking to add terms to the protective order previously issued at Doc.231. Following additional briefing by the parties, the court issued the Order at Doc.

254 which added additional terms to the protective order at Doc. 231, and from which the defense now seeks partial reconsideration.

The most significant manifest error of fact in the court's order is paragraph 9 which limits the defense to the use of one port and network connection. Factually this error, as explained by Mr. Fischbach in his Declaration in Support of this motion filed herewith, will make it impossible for him to conduct any of the proposed defense tests which this court has deemed material to defense preparation for trial. See, Fischbach Declaration in Support of Defense Motion for Partial Reconsideration of Court's Order at Doc. 254 [hereinafter "Fischbach Declaration"]. See, e.g. paragraph 2 and 5e.

As Mr. Fischbach notes: this restriction prevents him from installing industry accepted software and hardware as well as prevents him from removing his test results from the government provided computer for further examination and analysis on his own equipment, and/or in his own forensic work environment. He would be unable to connect a screen, keyboard, or mouse, let alone the hardware and software that he needs for his tests. The hardware and software required and vetted by industry standard forensic practice would insure more than any prophylactic proposed by the government that no data accidentally alter results or escape the system. Specifically, he writes:

I simply *must* have the ability to connect my own equipment, install my own industry-tested and accepted software and hardware, and to have the ability to remove my results for further examination and analysis. Otherwise, I *cannot* complete the testing that has been found material in this matter. *In short, I need access to multiple computer ports and network connections to run my tests.*

*See*, Fischbach Declaration at paragraph 5(e) emphasis supplied. This factual error in the court's order must be corrected in order for defense testing to be accomplished.

The manifest error of fact in Paragraphs 6 and 7 of the court's order is that these additional terms compromise attorney-client privilege and attorney work product by intruding



upon the confidential and independent defense testing process. These restrictions do not actually provide security to prevent the loss of TD software “into the wild,” but they do prevent the defense from conducting its tests properly and from implementing time-tested forensic-standard procedures (software and hardware) for securing sensitive data. See, Fischbach Declaration at 5(a)-(c). Moreover, requiring the government to be the sole possessor of the password protecting the TD test equipment, both inserts the government into the defense chain of custody and also makes it impossible for Mr. Fischbach to be held accountable for securing either the TD software or his own results as the government now has access to defense work product. Indeed, the only person who should have sole access to defense work product is Mr. Fischbach, and as such he should have sole and exclusive possession of any passwords. Mr. Fischbach sets out the problems presented by these restrictions in detail in his declaration but a few highlights appear below.

While having the government start the computer each time and enter a password seems innocuous, it is not. First it is not consistent with RCFL standard operating procedures (SOP), contrary to the government’s assertion. RCFL’s have a “hands off” policy regarding defense testing and equipment. Fischbach Declaration at paragraph 5(a) and 5(b) sub (c). If the government is in control and custody of the equipment containing defense work product, the government would be able to see the examination progress each time they log Mr. Fischbach back into the system. As Mr. Fischbach writes: “A technically knowledgeable Agent can learn a lot simply from the hardware configuration and setup and the software I am using to perform the tests I need to conduct.” *Id.* at 5(a). Moreover, time-tested industry-practiced methodology requires the initiation of certain hardware and applications on each work-station prior to testing and examination, which would necessarily make the observing agent privy to attorney client privilege. If this individual is technically-trained, then he/she can serve as a conduit of privileged defense information to Mr. Walker. *Id.* at 5(b) sub (b).

Mr. Walker has shown a proclivity for relying on information provided by observing Agents,

e.g. Mr. Monroe's recent email describing defense testing personnel in this case on September 25, or procuring a FBI-302 from the Agent observing the defense testing in the *Gonzales* case. The restrictions in paragraphs 6 and 7 of the court's order do not actually make it less likely that the TD software is inadvertently disseminated but they do seriously compromise the security of privileged defense information and data.

Lastly, in paragraph 8 of the court's order at Doc.254 the court limits the defense Internet connection to a single wired Ethernet connection. The factual error here is the assumption that TD software is less secure using a standard WiFi connection, and somehow more secure without the ability of Mr. Fischbach to install industry vetted forensic hardware and software. Were this true then Det. Erdely would have used a wired Ethernet connection himself when conducting his "validation;" but he did not. He used a standard WiFi connection. There is no valid basis to restricting the defense to a wired Ethernet connection which is substantially more expensive and is not available in many places.

#### Conclusion

The court has found the TD software is material to the defense and that the defense is entitled to conduct independent defense testing. This testing cannot be completed and is impossible without access to multiple ports and network cards. Allowing government Agents to access the computer at start up, perform log in and enter passwords not only affects testing reliability and validity but compromises sensitive and privileged defense data. Lastly, requiring a wired Ethernet connection offers no appreciable security but adds expense to the defense and may not even be available. Attached hereto is a defense proposed Order modifying those paragraphs in the court's order at Doc.254 that addresses these issues so that defense testing is actually possible and can be completed in a safe and secure manner for both the government and the defense.

DATED at Anchorage, Alaska, this 25th day of November 2019.

THE LAW OFFICES OF ROBERT HERZ, PC

s/ Robert M. Herz  
431 W. 7<sup>th</sup> Avenue, Suite 107  
Anchorage, Alaska 99501  
Phone 907-277-7171  
Fax 907-277-0281  
[rmherz@gci.net](mailto:rmherz@gci.net)  
AK Bar No. 8706023

**CERTIFICATE OF SERVICE**

I hereby certify that on Nov 25, 2019, a copy of the foregoing Def M for Partial Reconsideration was served electronically on Assistant United States Attorney's Office s/ Robert Herz

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, ) No. 3:17-cr-00095-SLG  
)  
Plaintiff, )  
)  
vs. )  
)  
MATTHEW WILLIAM SCHWIER, )  
)  
Defendant. )  
\_\_\_\_\_ )

**[PROPOSED] ORDER GRANTING MOTION FOR  
ADDITIONAL TERMS FOR ROTECTIVE ORDER**

Having duly considered the United States' Motion for Additional Terms for Protective Order and Notice of Compliance with Supplemental Order (the "Motion"), the Court

~~grants the Motion and ORDERS that:~~ denies the government's motion at Doc.244 but supplements its orders at Doc.231 and 243 as follows:

- ~~1. The government will provide a computer at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The computer will have one version of Torrential Downpour installed, i.e. version 1.23, one of the versions used in this investigation. The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.~~

//

The government shall produce at the RCFL both versions of the TorrentialDownpour software, the government's "validation" results, and Det. Erdley's Report no later than November 20, 2019.

The government will provide a copy of both Torrential Downpour versions used in this case, i.e. v. 1.15 and v. 1.23 to the defense on either CD/ DVD media or USB solid state or mechanical drive at the Orange County Regional Computer Forensics Laboratory.

- software are
2. The only persons who will have access to the computer are Jeffrey Fischbach and Robert Herz (collectively “the defense”). The defense will have access to the computer for 21 consecutive days of testing. software thirty (30) calendar
3. ~~The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.~~
4. The defense may bring digital media, computers, and phones into the room with the computer. software
5. The defense will not remove the computer from the OCRCFL. The defense will not copy Torrential Downpour. software
6. ~~The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape.~~
7. The defense will not download or distribute child pornography using the computer. Any downloading of child pornography would constitute a violation of the federal criminal code.
8. ~~All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain~~

~~the Wireshark data pending further order of the Court.~~

9. ~~At the conclusion of testing, the FBI will “zip” all the Wireshark files, meaning it will use software to compress them. The FBI will “hash” the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.~~

~~The government may provide the computer by November 20, 2019. The government’s compliance with this Order satisfies the government’s obligations under United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).~~

~~Moreover, the Court reaffirms its prior protective Order (Dkt. 231), as follows:~~

~~Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense’s observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person~~

~~without prior order of the Court.~~

~~Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this case, provided the materials are filed under seal and/or submitted to the Court for in camera inspection.~~

~~Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.~~

DATED this \_\_\_\_\_ day of November, 2019, at Anchorage, Alaska.

---

UNITED STATES DISTRICT COURT JUDGE

Robert M. Herz  
 Law Offices of Robert Herz, P.C.  
 431 W. 7<sup>th</sup> Avenue, Suite 107  
 Anchorage, Alaska 99501  
 907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT  
 FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

A period of excludable delay under 18 U.S.C. 3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. As of the date of this filing 36 days remain before trial must commence pursuant to the Speedy Trial Act

**RESPONSE IN OPPOSITION TO GOVERNMENT CONSOLIDATED FILING  
 AT DOC. 288**

Comes now, Matthew Schwier, by and through counsel, Robert M. Herz of the Law Offices of Robert Herz, P.C. hereby files this response in opposition to the government’s multiple pleadings consolidated as filed by the government at Doc. 288. The government has filed 1) a status report; 2) a notice regarding proposed testing environment; 3) a response to the defense motion for reconsideration at Doc. 256; and 4) an responses in opposition (styled as “responses to objections” ) to the use of the SCIF located at the Los Angeles federal court and to defense computer specifications. All these pleadings were contained in one document.<sup>1</sup> The court invited the defense at Doc. 289 to file a response to the government’s filing. Mr. Schwier will respond *seriatim*.

**1) Government’s Status Report.** The government filed a fourth superseding indictment on December 18, 2019, over two years and four months since the government first indicted Mr. Schwier. This iteration of the indictment, as alleged in count 4, for the first time alleges conduct

<sup>1</sup> This consolidated filing seemingly violates local court rules. See, Local Crim Rule 1.1(b); Local Civ. Rule 7.1(e) and 5.1(f)(2) which require separate pleadings be filed for separate issues.



of *receiving* images pertaining to the date of *November, 2015*. No previous iteration of any indictment in this case alleges conduct from the year 2015. The government offers no explanation for this delay. The government gave notice to the defense on December 27, 2019 that four images that the government intends to rely upon were available to review at the RCFL. After receiving that notice, that same day the defense requested the government provide the filename, pathname, MAC data, and hash values for each image prior to Mr. Fischbach before making the trip to the RCFL. The images themselves are of little value in the context of conducting a forensic computer examination. Today, the government responded to the request but did not provide filenames, pathnames, MAC data and hash values as requested. See Email Chain attached.

## **2) Government Notice of Proposed Testing Environment.**

The government has seemingly repudiated the testing protocol as provided for in the Court's orders at 231, 243 and 254 the terms of which the government previously has approved. The government has twice proposed additional terms to the protective order. See, Doc. 244-1 and 253-5., which have largely been adopted by the court. The only objection raised by the government to the court's protocol, as indicated in its Motion for Reconsideration at Doc.255, was that the court did not mandate any packet capture software. Id. at Doc.255, page 2. The only remaining issues to be resolved were the ones raised by Mr. Schwier at Doc. 256 in his Motion for Reconsideration.

Contrary to the government's claim, the court did not order the government to submit a revised protective order protocol.<sup>2</sup> The court only invited the government to respond to the objections raised by the defense its Motion for Reconsideration at Doc. 256. Purportedly, the government needed to consult with FBI technical experts before it could offer a response to the technical issues raised by the defense. Instead, the government has filed a whole new

---

<sup>2</sup> The government alleges that "At the hearing on November 26, 2019, the Court ordered the government to submit a revised protective protocol." Govt. Doc 288 at 2. Mr. Schwier does not believe the hearing record supports this claim and certainly nothing in the court's order at Doc.262 does.

protocol proposal that is regressive nature, and makes defense testing impossible,<sup>3</sup> as detailed by Mr. Fischbach in the attached Declaration. This new testing protocol creates serious obstacles to defense testing including but not limited to the lack of internet access, dictating a testing environment, government monitoring of defense testing in real time, and prohibiting use of defense equipment and software, among others. Comparing the Government's prior proposal at Doc. 253-4 to its new proposed protocol at 288 and 288-1 should be instructive.

a) Internet Access

Det. Erdeley has made clear that Internet access is required to run and test Torrential Downpour ("TD") software. This was acknowledged by the government: "The defense may bring... an internet hotspot (i.e. one that is compatible to connect to the TD Computer via the network card) into the OCRCFL room with the TD Computer. Doc. 253-4, para. 6. Whereas now:

"Internet access will be **provided by the government for the limited purpose of installing uTorrent** software or other software that requires activation/installation via the Internet on one or more of the test computers. All of the Internet installations/activations/connections will be conducted prior to the installation of TD. **Once the installation of defense's software is complete, the Internet access will be terminated** for the remainder of the testing period."

Doc. 288-1 at para. 5. Emphasis supplied. Previously the government required the defense to bring its own private wireless Internet hotspot, for testing purposes. The Defense is now required to use a **government monitored** Internet connection, but only to install the software that Mr. Erdely used. Following that, the defense has **no Internet for testing purposes**, as required by TD, and in compliance with previously stated defense test specifications determined to be material by the court. Instead of privileged defense methodology and testing, the government will now have monitored access to test results before counsel does.

---

<sup>3</sup> The defense infers that once the Office of General Counsel for the FBI and the FBI technical experts saw the extant terms of the protective order and testing protocol, they strenuously objected and hence proposed entirely new and more regressive terms that they wish to impose upon and govern what should otherwise be independent defense testing in this case.

b) Use Of Defense Testing Equipment

The government previously agreed that: “the defense may bring digital media, computers, cell phones” into RCFL exam room for defense testing purposes. Doc. 253-4 at Para. 6. However, now the government has completely retreated from this position and states:

**No other electronic devices** or storage devices may be brought into the testing room to include but not limited to **computers, phones, laptops, hard drives, or tablets.**

Doc. 288-1 at para. 3. If the court were to adopt this provision, it would mean that the defense has no means of using any hardware necessary to complete its testing, nor any industry standard hardware necessary to insure that no software or data is unintentionally copied, nor the ability for the defense expert to even communicate with counsel during tests.

c) Use Of Defense Testing Software

Previously, the government agreed that: “prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer, all while in the physical presence of the FBI agent or Task Force Officer. The FBI agent or Task Force Officer may observe Mr. Fischbach install the software. Doc 253-4. at para. 5b.

**All software** installed on testing computers cannot be encrypted or password protected and **will be copied/hashed/preserved/ sealed.** The copies will be preserved and only accessed by the government upon Court authorization. (Doc. 288-1 at para 1).

Before defense may install any software on the testing computers the government will conduct virus scans on the software in the presence of the defense expert. (Doc. 288-1 at para. 2) \*\*\*

This installation of defense’s software will be done in a user account designated for Defense. Government will provide access to the Defense user account for this installation process.

Doc. 288-1 at para 11. Prior defense concerns were that an agent could discern privileged methodology by observing defense software installation. The current government proposal requires the defense to provide licensed and/or proprietary software to the government. The

defense has no authority to grant licenses to the government. The government has not addressed concerns about the government *observing* the defense software installation and instead now is requiring the defense to provide the information to the government. Virus scans only serve to provide *more* information about defense methodology. They do not serve to protect government computers, as the government should have *no access* to this equipment in the first place. Under the government proposal, defense software cannot access TD, yet the government is demanding access to examine defense software, which -- under the government proposal -- cannot even directly access TD software. The defense testing methodology cannot work without direct access to TD, using defense software.

d) Wireshark Monitoring

Previously the government sought an Order from the court requiring the defense to use a packet capture technology. The defense objected, and the court did not require that it be used.<sup>4</sup> The government in Doc. 253-4 proposed: “All communications with the TD Computer will be preserved via Wireshark. This preservation includes all communications with TD during testing, and at all times the computer is powered up. The defense shall maintain the Wireshark data pending further order of the Court. Doc. 253-4 at para. 13. Now the government proposes an even more onerous and invasive use of Wireshark:

**One laptop will be dedicated to capturing Wireshark files** for the entire testing period. At the conclusion of the testing, **defense expert may witness the government storing these files** on a CD, hashing them, and sealing them for preservation. The government will not access these files unless the Court authorizes government access. Doc. 288-1 at para 6.

Laptop 4 – **Defense will not be provided any access to this computer.** Wireshark files will be stored here during the testing period.

---

<sup>4</sup> The government sought reconsideration of this issue in Doc. 255 but agreed at the hearing on November 26, 2019 that it was moot based on the information contained in the filing by the defense at Doc. 256 and Mr. Fischbach’s contemporaneous declaration. The defense acknowledges that the court has warned the defense in writing and orally that failure by the defense to use any packet capture software could potentially render some of Mr. Fischbach’s testimony inadmissible under *Daubert*.

Doc. 288-1 at para. 9.

Prior defense concerns were that the government was requiring the defense to create and preserve discovery for the government. Now the government is requiring *real-time* access to that discovery which will be held and preserved *by* the government. The government has proposed that a switch/router will be operating in their test environment system, and that the defense will not have access to it, which means only the government will have access. Anyone from the government would be able to and can plug a computer into that router and monitor in real time what the defense is doing. And in fact that is exactly what laptop 4, the proposed Wireshark computer, will be doing. The defense will not have access to Laptop 4 either. Anyone from the government would be able to and can observe the screen/monitor of Laptop 4 in real time to see what the defense is doing. Moreover, as described by Mr. Fischbach the Wireshark log files and defense results can be manipulated by the government before the defense would be able to see their own results. The defense, in this case, will not even have access to their own discovery, as noted in 288-1 at para 9.

e) Testing Results

Previously the government agreed that the “The defense may bring digital media...” into the exam room at the RCFL. 253-4 at para. 6. Now the government has completely repudiated this:

Defense testing may generate files that are stored on the host computer of Laptop 1, and/or Laptops 2 and 3. Upon conclusion of testing, all files will be copied/ hashed/preserved/sealed and only accessed by the government upon Court authorization. Doc. 288-1 at para. 4.

If requested by the defense expert, at the conclusion of testing **the government will make a copy of the files generated by the defense** software which were stored on Laptop 1, 2, and/or 3. This copy will be on a CD, which will be hashed and **will remain at the OCRCFL** to be available for the defense expert to come and conduct further analysis. If requested by defense, then this CD can be sealed and marked by the defense expert. The CD will not leave the OCRFL.

Doc 288-1 at para 11, 14. A prior concern was that while defense media could be brought into the exam room at the RCFL, the government sought to block the ports which prevented the defense from being able to remove defense results to Mr. Fischbach's office for further analysis. This new proposal still blocks the ports, but now also requires results to be provided to the government. The results themselves would not contain contraband and would not contain a copy of TD, and so attempting to restrict Mr. Fischbach from being able to analyze results using his own equipment and software at his office does nothing to protect TD from being released to the general public and only serves to make defense testing unnecessarily inconvenient and expensive. Under these requirements, the defense will have no ability to further analyze its own test results, while the government must be trusted not to access privileged defense work product. Furthermore, the defense cannot even bring in the hardware necessary to conduct the primary testing that the court has already determined to be material, let alone use hardware necessary to analyze its own results in a non-government environment.

f) Real-Time monitoring of Privileged Defense Work Product

Previously, nothing in any government proposal allowed the government to monitor any part of defense testing, including test design, methodology, use of software or hardware, or communications. Now the government proposes that it be allowed to have the capability to engage in real-time monitoring of defense testing, as previously noted and referenced in Doc. 288-1 paragraphs 6 and 9.

**3) Reply to Government Response in Opposition to Defense Motion for Reconsideration**

In its Motion for Reconsideration at Doc. 256 the defense noted that paragraph 9 of the court's order at Doc. 254 limited the defense to the use of one port. The defense noted that:

this restriction prevents [Mr. Fischbach] from installing industry accepted software and hardware as well as prevents him from removing his test results from the government provided computer for further examination and analysis on his own equipment, and/or in his own forensic work environment. He would be unable to

connect a screen, keyboard, or mouse, let alone the hardware and software that he needs for his tests. Doc.. 256 at 2.

The government's only response is that under the government designed testing environment Mr. Fischbach would be able to use a screen, a mouse and a keyboard, and therefore the objection has no merit or is moot. Doc. 288 at 3. The government fails to respond to the main point of the objection raised by the defense: limited port access prevents Mr. Fischbach from installing his own testing software and hardware and from being able to remove results for further examination and analysis in his own forensic work environment.

Next, the government attempts to respond to the defense objections to paragraphs 6 and 7 of the court's order at Doc. 254. The defense argued that the terms of Paragraphs 6 and 7 of the court's order compromise attorney-client privilege and attorney work product by intruding upon the confidential and independent defense testing process. The government's response is nonsensical. The government asserts that the defense has no work-product privilege associated with TD. The defense has never asserted that it did. What is clear, though, is that the work of agents for the attorney in preparation of litigation is protected by the work product doctrine. *United States v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011). The defense has asserted that the design of the defense testing environment, how equipment is configured, what software and hardware is used, which tests are run, what data is examined would all reveal information that is privileged at this point. The privilege would only be waived *if* Mr. Fischbach were to testify about this subject at trial. The government fails to meaningfully respond to this issue.

The defense has never argued that the mere presence of the computer with government installed contraband and government installed software located at the OCRCFL is in any way privileged. The defense has not argued that Mr. Fischbach's communications with Mr. Monroe are privileged, only that in Mr. Fischbach's experience the government's intrusion into these communications seems to violate long standing nationwide RCFL policies to

maintain the sanctity of independent defense testing of contraband that must occur in a government facility. None of the emails written by Mr. Fischbach to the government or Mr. Monroe divulged anything pertaining to the design of the defense testing environment, how equipment is configured, what software and hardware is used, which tests are run, and what data is examined. None of the emails filed by the defense in this case waived any of this privileged information.

Mr. Fischbach does, indeed utilize industry standard hardware, software, and procedures. As well, over the course of 25 years, Mr. Fischbach has developed and engineered some of his own, many of which have been taught to and utilized by others in the field. There are, however, numerous industry standard forensic practices, software, hardware, and procedures from which a forensic analyst may choose to conduct an examination, based on their appropriateness to the allegations and evidence in question. By way of example, any professional sport has rules and acceptable conduct. The mere fact that opposing teams are required to play from the same rulebook, and will likely choose from a limited number of viable playing strategies, does not negate the fact that *any* strategy would be thwarted if the opposing team were allowed to observe team meetings prior to taking the field.

**4) Use of a more secure testing environment: the SCIF or FBI-Wilshire.**

The government objects to moving the location of the defense testing in this case to a more secure location. The government has repeatedly asserted that its overriding concern is for the prevention of the release of TD into “the wild,” since any release would compromise on-going and future investigations. The exam room at the OCRCFL is open to various defense experts and attorneys working on different cases. A piece of Mr. Fischbach’s own equipment disappeared from this room. Mr. Monroe acknowledged that the RCFL was not as secure as the SCIF or the FBI offices at Wilshire. The defense proposed each of these two alternative locations as more secure environments for testing the government’s sensitive



software. Under the circumstances, it would seem the government would want to utilize a more secure location for testing of the TD software in order to protect it.

The government observes that this case does not involve classified information. This is true. And while the government suggests for this reason alone the request to use the SCIF is unusual, the government does not claim, as it cannot, that this prevents use of the SCIF in this case. “Unusualness” or “appropriateness” should not be the government’s overriding concern considering the government’s self-imposed “level of security” that it has imparted to its software. Thus far, the elements which the government maintains must be kept secret it, the government has already exposed to the defense. Given that both parties, as well as the OCRCFL’s own Joseph Monroe, agree that RCFL facilities are not equipped to monitor against theft of hardware and software, out of an abundance of caution, the defense has simply attempted to provide secure alternatives, based on Mr. Fischbach’s established experience with more secure government facilities.

While Mr. Fischbach acknowledged on record that he has not had the need to renew his National Security Status, if necessary in order to analyze the TD software in a secure environment, he would be willing to undergo an expedited review, as he did in the U.S. v. *Chi Mak* case cited by the government. Furthermore, he notes that in his experience, the SCIF in Los Angeles simply consists of isolated single rooms, containing no access to sensitive information, *other than that which the analyst is currently examining*. Thus, while this may be a “inconsistent use” -case, the treatment of software as “government sensitive” is also an “inconsistent use”-case when compared with all other standard investigative software which have been openly tested and utilized by the forensic community.

Lastly, the defense notes that the government has not raised any objection to moving the testing location to the FBI-Wilshire office. This would be a more secure location than the RCFL and could be used for both testing of the TD software as well as for continuing evidence review.

**5) Government provided computer specifications are insufficient.<sup>5</sup>**

The government erroneously asserts that the defense specifications for a government supplied computer have been “evolving.” The government continues to refer to an email dated November 19, 2019 as somehow constituting a hardware specifications request from the defense. The government continues to conflate the facts, as pointed out in the email thread at Doc. 281-2.<sup>6</sup> As the defense pointed to the government out then: “Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, *Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions.*” That cannot reasonably be construed as a hardware specification request.

What has made the “project more difficult” has been the government’s unwillingness to provide the software specifications, installation instructions, and user manuals as ordered by the court so that the defense could make a tailored defense specifications request. Given the government failure to be forthcoming about TD software specifications, the government should not be heard to complain now that the specifications ultimately provided by the defense are not to their liking.<sup>7</sup>

---

<sup>5</sup> Again, the government asserts that the court ordered the government to respond to defense objections to a government provided computer. The record does not support this assertion. The defense had not made objections to any government supplied computer prior to the November 26 hearing. The court at Doc. 254 ordered the government first to provide to the defense TD software specifications and then the defense was required to provide its computer hardware specifications needed to run its defense tests. Only if the defense did not provide these specifications in a timely manner did the court permit the government to supply equipment that the government thought was “reasonable” under the circumstances.

<sup>6</sup> See, Email Chain at 281-2, specifically dated December 19, 2019 addressed to AUSA Walker.

<sup>7</sup> It is not accurate to describe the defense proposed computer as “state of the art or “top of the line” indeed the proposed specifications are for a mid-range quality computer, albeit “new in box” as the defense has no way of knowing what kind of used computers are in government inventory at any given time.

The government assumes defense testing is attempting to simulate actual investigative activity<sup>8</sup>, in part to justify its own test design (which they call the “testing environment”) and to justify the computers it has chosen. However, the government admits it knows nothing about the tests the defense will run, or the software the defense plans to use, so it is presumptuous to assume that spreading out functions over three computers is a test design that the defense will utilize or that the specifications of the computers the government has chosen will be sufficient for defense tests that are entirely different from and whose purposes are different from anything the government has heretofore done. It may be true that TD can operate on less powerful computers, but this is not relevant as this fails to account for the defense hardware and other software that the defense will use for defense testing that requires more computing power than that needed for simply running TD software.

The proposed specifications of the computers the government wants to supply are inadequate because, Mr. Fischbach is not simply *operating* TD, he is testing it. Thus, the operating specifications the defense has requested from the government,<sup>9</sup> are simply a baseline in order to properly specify hardware and virtual machine variables. While the government continuously specifies environments only suited to approximate Mr. Erdely’s validation procedures (minus the required Internet accesses). The defense, however, has outlined specific tests of the TD software which require other hardware and software to complete, demonstrate, and reproduce the defense tests. In addition to that, *both* the government and the defense have

---

<sup>8</sup> The government writes: “During the actual investigation of Mr. Schwier the Torrential Downpour software was on a different computer than Mr. Schwier’s computer, and, therefore, keeping those functions on separate computers more closely simulates the actual investigative activity.” Doc. 288 at 11.

<sup>9</sup> Despite the government’s claims to the contrary, the defense is unable to locate in the TD materials provided by the government anything that would be considered “software specifications.” On page 7 of the User Manual there is a paragraph titled “System Requirements.” Its only content consists of two lines: “*Torrential Downpour runs on Windows Vista or later, and requires Microsoft.NET 4.0 or later. You also need sufficient disk space to hold the files that you download.*” The government’s claim that it provided software specifications seems disingenuous at best.

specified the need to use multiple “Virtual Machines (VMs).” Mr. Fischbach has already tested the use of just a single Virtual Machine on equipment with specifications equivalent to those proposed, and on the machines provided by the government, and it was entirely non-functional. Thus, the government’s proposed hardware simply cannot be used, even for the government’s own Validation.

DATED at Anchorage, Alaska, this 6th day of January 2020.

THE LAW OFFICES OF ROBERT HERZ, PC

s/ Robert M. Herz  
431 W. 7<sup>th</sup> Avenue, Suite 107  
Anchorage, Alaska 99501  
Phone 907-277-7171  
Fax 907-277-0281  
[rmherz@gci.net](mailto:rmherz@gci.net)  
AK Bar No. 8706023

**CERTIFICATE OF SERVICE**

I hereby certify that on Jan 20, 2020, a copy of the foregoing Notice of Compliance with Order at 262 was served electronically on Assistant United States Attorney’s Office s/ Robert Herz

## Robert Herz

---

**From:** Walker, Jonas (USAAK) 5 [Jonas.Walker@usdoj.gov]  
**Sent:** Wednesday, November 20, 2019 1:45 PM  
**To:** Robert Herz  
**Subject:** RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Is the defense requesting testing using the computer already at the OCRCFL?

-AUSA Jonas M. Walker  
907.271.3983

---

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Wednesday, November 20, 2019 1:33 PM  
**To:** Walker, Jonas (USAAK) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>  
**Cc:** 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>  
**Subject:** RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

We are trying to get this done, and proceed to trial, while placating your fear of "the wild." If you speak with your own experts, I'm sure they can explain to you how virtual machines work, and I'm even more certain that they can tell you exactly what specifications are necessary to install and run TD. Alternatively, you could provide those to Mr. Fischbach, as I have already requested. If you are informing me that you already have personal knowledge that there is no way for Mr. Fischbach to use the computer at the RCFL to install and operate TD, then please provide a computer either with the specifications that are required by the software, or with the hardware/software specifications you requested from me, that I have already provided to you.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAK) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Wednesday, November 20, 2019 11:16 AM  
**To:** Robert Herz  
**Subject:** RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Per your email below, is the defense requesting testing using the computer already at the OCR CFL?

The computer already at the OCR CFL doesn't have internet access. Also, the TD Computer would likely be wiped prior to TD installation.

Thank you,

-AUSA Jonas M. Walker  
907.271.3983

---

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Tuesday, November 19, 2019 11:49 AM  
**To:** Walker, Jonas (USA AK) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>  
**Cc:** 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>  
**Subject:** RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

Because Mr. Fischbach was able to observe the vintage of the Mac used for "validation", he believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation -- thus assuring the government that no copy will be placed on his own equipment. Because his testing protocols do not require any interaction with contraband, he will use his own equipment to interact with TD installed on the computer at the RCFL. Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions. If, however, Mr. Erdely can supply such information, or is able to render an opinion regarding the equipment provided to the RCFL by the AUSA, it would certainly save the loss of valuable time if Mr. Fischbach could be made aware of any limitations prior to beginning his tests.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USA AK) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Tuesday, November 19, 2019 9:04 AM  
**To:** Robert Herz  
**Subject:** US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Good morning.

In Dkt. 249 at 10, Mr. Fischbach wrote: "Towards that end I am amenable to the government providing to me a computer configured to my specifications. In order to assure scientific results, I have to personally conduct the installation of any software to be tested."

Please promptly advise what "specifications" Mr. Fischbach is requesting.

Thank you,

-Jonas M. Walker  
Assistant United States Attorney  
District of Alaska  
907.271.3983

## Robert Herz

---

**From:** Robert Herz [rmherz@gci.net]  
**Sent:** Tuesday, November 19, 2019 2:45 PM  
**To:** 'Walker, Jonas (USAAK) 5'  
**Cc:** 'Jeff M. Fischbach, ABFE'  
**Subject:** RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

Mr. Fischbach says that because he still has not been provided with any TD documentation and other materials that would be typically provided to a user of TD, he would only be able to specify the most robust desktop equipment available to a forensic professional at this time. If you would like to provide TD documentation materials he may be able to give you a more concise specification, and thus save time and money.

However, at this time, given the ambiguity of the software requirements, he can only specify a currently robust (but by no means server-level) workstation. Again, it would be more productive for all concerned, if we simply had a copy of the software specifications. The specifications below are only minimum estimates for TD -- not for his complete testing. For practical, and defense privileged purposes, he will use his own equipment as a testing component, but will not install or copy TD to any of his own devices.

2.6GHz 6-core 9th-generation Intel Core i7 processor  
64GB 2666MHz DDR4 memory  
AMD Radeon Pro 5500M with 8GB of GDDR6 memory  
512GB storage  
Thunderbolt / USB-C  
WiFi & RJ45 Ethernet  
Mac must have Bootcamp & valid Windows 10 installed.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAK) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Tuesday, November 19, 2019 12:14 PM  
**To:** Robert Herz  
**Subject:** RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:



I appreciate the prompt response.

Other than agreeing to use the existing computer, what "specifications" does Mr. Fischbach require, per Dkt. 249 at par. 34?

Thank you,

-AUSA Jonas M. Walker  
907.271.3983

---

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Tuesday, November 19, 2019 11:49 AM  
**To:** Walker, Jonas (USAAK) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>  
**Cc:** 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>  
**Subject:** RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

Because Mr. Fischbach was able to observe the vintage of the Mac used for "validation", he believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation -- thus assuring the government that no copy will be placed on his own equipment. Because his testing protocols do not require any interaction with contraband, he will use his own equipment to interact with TD installed on the computer at the RCFL. Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions. If, however, Mr. Erdely can supply such information, or is able to render an opinion regarding the equipment provided to the RCFL by the AUSA, it would certainly save the loss of valuable time if Mr. Fischbach could be made aware of any limitations prior to beginning his tests.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAK) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Tuesday, November 19, 2019 9:04 AM  
**To:** Robert Herz  
**Subject:** US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Good morning.

In Dkt. 249 at 10, Mr. Fischbach wrote: "Towards that end I am amenable to the government providing to me a computer configured to my specifications. In order to assure scientific results, I have to personally conduct the installation of any software to be tested."

Please promptly advise what "specifications" Mr. Fischbach is requesting.

Thank you,

-Jonas M. Walker  
Assistant United States Attorney  
District of Alaska  
907.271.3983

## Robert Herz

---

**From:** Robert Herz [rmherz@gci.net]  
**Sent:** Thursday, December 19, 2019 7:25 PM  
**To:** 'Walker, Jonas (USAAK) 5'  
**Subject:** RE: Hardware and software Specifications

Mr. Walker,

The defense will respond *seriatim* to your several factually inaccurate statements in your Dec.7 email.

*You wrote: On 11/19/2019, your email (attached) indicated that Mr. Fischbach "believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation."*

First, the defense in the Nov.19 email was trying to work cooperatively, and point out that a *possible* option *might* be to use the existing machine on site; hence the use of the conditional phrase that [the existing machine] "may" be able to accommodate TD installation. You ignore the conditional nature of this statement. Moreover, your quote above is taken out of context and ignores the rest of the email which states: "Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, **Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions.**"

*You wrote: Then, on 12/6/2019, your email (attached) indicated that the original computer was inadequate, and requested the government "allow Mr. Fischbach to use the machine that was recently sent to the RCFL."*

This part of your email is even more troublesome, as the Dec.6 email has nothing to do with the defense wanting to use the newly provided machine to test TD. The defense request was in reference to not being able to run on the existing machine the VMWare software that Det. Erdely used to run his "validation." The defense was requesting the ability to use the newly provided machine to see if we could run the VMWare software on the new machine so the defense could begin finally to evaluate the data generated by the government "validation." Mr. Fischbach had traveled several hours to the RCFL to begin a review of the government validation. The defense was trying use precious time and resources already committed to being at the RCFL for the day, and the government had already previously instructed Joe Monroe that the defense could not have access to the new machine at all; because the government had apparently just realized that day it had released the TD software into the wild by including it along with the validation that had been sent to the RCFL. This was the second time the government had released sensitive information concerning the TD software without so much as a protective order in place, and again had to depend on the honesty of Mr. Fischbach to maintain security over your software that the government does not seem able to keep secure.

*You wrote: Now, however, in your email, below, you are requesting a third computer and identifying additional requirements.*

The defense has not requested a "third" computer with "additional requirements." As you well know, the defense did not request the first government supplied machine, a "vintage" out of date Mac that was sent from Anchorage-FBI to the RCFL. That was a machine supplied by the government without any input from the defense. The defense also did not

request the newly provided machine either. That again was supplied by the government *by fiat* even before any specifications had been provided by the defense, in seeming defiance of the court's order at Doc. 254 and Doc 262.

The defense has repeatedly requested the government comply with the court's order that the government supply documentation, software specifications, and installation instructions. The court order at Doc. 262 only relieved the government of supplying a computer by Dec4. Yet, the government sent a computer to the RCFL anyway, and pre-loaded it with software the government used to run its validation. The defense recognizes that it is the government's goal to limit defense testing to only running the government validation. The defense has made clear that it does not intend to run the government "validation" again, as it has no scientific validity.

Other than being relieved of the duty to supply a computer by Dec.4, no other portion of the court's order at Doc. 254 was stayed or vacated. The government is not in compliance with the court's order, as the defense has never received any TD software specifications or installation instructions. The defense, again in an attempt to accommodate the government, save time, and work cooperatively, nevertheless took time to at least analyze the new machine's system specifications by having the RCFL's Joseph Monroe "boot" it up, again after seeking permission from you. The defense did this to see if the new machine sent by the government without any input from the defense could potentially be used to run the defense tests. It was not adequate.

I don't mind a "hard fight," but you seem quite comfortable playing fast and loose with the facts, as exemplified in the above email from you dated Dec7. It's not the first time this has happened in this case. I find it disturbing. In that regard, your "out of office" email response that I received on Dec. 4 says you "may have limited opportunity to read or respond to your email during December 2 - 13, 2019." On Nov.26 at the hearing you did not indicate to the court you would be out of the office from Dec.2 to Dec. 13, presumably on leave, and that's why you could not meet the court's earlier set deadline to respond to the defense motion for reconsideration. Instead you indicated that FBI technical experts needed all that time until December 13 to advise you and respond to the technical issues raised by Mr. Fischbach. Perhaps it's just coincidence that the technical experts needed the same amount of time to respond that coincided with your time out of the office. It would appear that is why you then requested an additional 7 days after your returned to the office to file a response. The coincidence is striking, and I wonder whether the FBI technical experts that were telephonic for that hearing, if they were called to testify, if they would testify that they were the ones who needed more time, as opposed to you. If the real reason for the delay was your vacation, that would represent a serious lack of candor with the court.

*Your wrote: In the event that a government-owned computer with Mr. Fischbach's requirements is not available, is the defense offering to provide such a computer, which would remain at the OCRCFL, and which the government and Mr. Fischbach would confirm is "wiped" after the case is complete? If such an arrangement is consistent with the to-be-ordered protective protocols, then that may be best way for the defense to use exactly the computer it wants.*

As you learned from your invasive contact with Joseph Monroe regarding the Defense examinations at the RCFL, as well as Mr. Monroe's testimony, the RCFL isn't secure. The Defense has already had equipment stolen or gone missing from the RCFL. While the court has not obligated us to do so, the Defense is not inclined to leave a defense machine worth thousands of dollars there if it cannot be secure and the RCFL will not take responsibility for securing it. Mr. Monroe himself has testified that the RCFL does not have the level of security necessary, and it will not be held accountable for

securing Defense property. It seems questionable if it is even capable of securing the VMWare images, containing TD software that has already been copied to the Defense-privileged Government-owned Mac Tower, currently in the RCFL's civilian workspace, where other civilians sit within inches of the machine, and even utilize some of the same hardware. Even Mr. Monroe himself admitted that the RCFL civilian exam room does not have the level of security of other locations, such as the LA SCIF. Indeed, the court asked the government to address use of the LA SCIF as a location for additional and further defense examinations in this case.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]  
**Sent:** Saturday, December 07, 2019 4:48 PM  
**To:** Robert Herz  
**Cc:** 'Jeff M. Fischbach, ABFE'; Arce, Charisse (USAAK) 1  
**Subject:** RE: Hardware and software Specifications

Mr. Herz:

Good evening.

On 11/19/2019, your email (attached) indicated that Mr. Fischbach "believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation."

Then, on 12/6/2019, your email (attached) indicated that the original computer was inadequate, and requested the government "allow Mr. Fischbach to use the machine that was recently sent to the RCFL."

Now, however, in your email, below, you are requesting a third computer and identifying additional requirements.

The court has allowed the government to file additional briefing by December 20, 2019, regarding protective protocols. That filing may, also, respond to the latest defense request.

In the event that a government-owned computer with Mr. Fischbach's requirements is not available, is the defense offering to provide such a computer, which would remain at the OCRCFL, and which the government and Mr. Fischbach would confirm is "wiped" after the case is complete? If such an arrangement is consistent with the to-be-ordered protective protocols, then that may be best way for the defense to use exactly the computer it wants.

Thank you, and have a nice weekend,

-AUSA Jonas M. Walker  
907.271.3983

**From:** Robert Herz <rmherz@gci.net>  
**Sent:** Friday, December 6, 2019 5:04 PM  
**To:** Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>  
**Cc:** 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>  
**Subject:** RE: Hardware and software Specifications

Mr. Walker,

I would agree that Mr. Fischbach is in the best position to know what his needs are in order to conduct defense testing of the TD software. As such, Mr. Fischbach has concluded his inspection of the system requirements of the laptop supplied by the FBI, and it will not be sufficient to meet defense testing needs. It is a 2014 vintage A1398 MacBook Pro, with minimal speed and memory, and outdated hardware and port specifications. Similar to the machine currently in use at the RCFL, it is unlikely that this laptop also will not support running the Virtual Machines supplied by Mr. Erdely. This machine was the least powerful configuration of MacBook Pro produced in 2014. But, is far slower than the minimum requirements of today's Macs. Notably, at this juncture the Government is seeking an order that Mr. Fischbach only use an Ethernet port. This machine does not have an Ethernet port.

The following are the *minimum requirements* needed in a government supplied machine necessary to conduct defense testing of the TD software. Defense specifications are in black, corresponding specifications of the computer supplied by the government are in red:

2.6GHz 6-core 9th-generation Intel Core i7 processor (4-core 4th generation processor discontinued in 2015 nearly five years ago)

64GB 2666MHz DDR4 memory (16GB 1600 MHz DDR3 -- incapable of additional RAM)

AMD Radeon Pro 5500M with 8GB of GDDR6 memory (2GB discontinued graphics processor)

512GB SSD storage (Unknown)

Thunderbolt / USB-C (No USB-C)

WiFi & RJ45 Ethernet (No Ethernet)

The Mac laptop also must have Bootcamp & **valid** Windows 10 installed.

Please let me know when a machine with these minimum requirements will be supplied and available for Mr. Fischbach's use.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)

---

**From:** Walker, Jonas (USAAC) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Friday, December 06, 2019 3:31 PM  
**To:** Robert Herz  
**Cc:** 'Jeff M. Fischbach, ABFE'; Arce, Charisse (USAAC) 1; Russo, Frank (USAAC); Allison, Daryl (AN) (FBI)  
**Subject:** RE: Hardware and software Specifications

Mr. Herz:

Thank you for contacting me regarding your concerns.

Per my email of 12/4 below, the government believes that the computer provided is sufficient to run TD as it would be used in an investigation.

The government does not know what tests Mr. Fischbach intends to run, as the defense has withheld that information from the government. Without knowing what tests Mr. Fischbach intends to run, and the technical requirements of those tests, the government is not in a position to opine regarding what technical specifications are necessary to meet Mr. Fischbach's needs.

Because Mr. Fischbach has access to the technical specifications of the computer, as described below, Mr. Fischbach is the person best situated to answer your question regarding whether the computer is sufficient to run Mr. Fischbach's tests.

Thank you,

-AUSA Jonas M. Walker  
907.271.3983

---

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Friday, December 6, 2019 2:56 PM  
**To:** Walker, Jonas (USAAC) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>  
**Cc:** 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>  
**Subject:** RE: Hardware and software Specifications

Mr. Walker,

I agree the court stayed the requirement that the government does not need to provide the TD computer. But the court did not stay the entire order at Doc. 254. As such, the requirement that the government provide all software documentation related to TD is still binding on the government.

Moreover, I believe this was in recognition that the defense needs the TD software specifications in order to provide a tailored request for computer specifications for the computer that the defense needs to run its tests. Nevertheless, the government prior to knowing what the defense specifications would be, "selected" a computer that the *government believes* the defense should use. This was not the process the court envisioned by its order at Doc.254 and seems a bit "cart before the horse." Given that Doc.254 was not stayed in its entirety, I disagree that the government has complied

with the court's orders, or that the court's orders have been exceeded. That Mr. Fischbach is attempting to ascertain the system requirements of the computer the government provided, prior to defense input, only means we are evaluating what has been sent to see if it will meet defense needs. Our preliminary review suggests that it will not be adequate. When Mr. Fischbach completes his work at the RCFL later today, I will provide the government notice of what specifications are, in fact, needed, and whether the computer sent prematurely will meet defense needs. However, the lack of TD software specifications has significantly hampered the defense in this evaluation.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAC) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Thursday, December 05, 2019 5:44 AM  
**To:** Robert Herz  
**Cc:** 'Jeff M. Fischbach, ABFE'; Monroe, Joseph; Allison, Daryl (AN) (FBI); Steeves, Holly J. (AN) (FBI); Arce, Charisse (USAAC) 1  
**Subject:** RE: Hardware and software Specifications

Mr. Herz:

Good morning. I replied in a separate email chain regarding the defense request for Mr. Monroe to show Mr. Fischbach the computer settings. As indicated, I don't object to that request, and I appreciate Mr. Fischbach's suggestion that he see the settings in person to get the data he needs. That seems like an efficient way to get the data directly to Mr. Fischbach.

At Dkt. 262, the court vacated the order at Dkt. 254 in that the government does not have to provide the TD computer to Mr. Fischbach at this time.

Also in Dkt. 262, the court ordered the defense to provide specifications by 12/6. To assist the defense in this process, I provided the specifications of the selected computer in a prior email chain yesterday; see below, immediately prior to your email.

Accordingly, the government has complied with the Court's orders, and, in fact, has exceeded them, in that Mr. Monroe will be showing the computer details to Mr. Fischbach, which is what Mr. Fischbach requested.

The Court will, no doubt, appreciate the parties' cooperation regarding these technical details.

Thank you,

-AUSA Jonas M. Walker  
907.271.3983



---

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Wednesday, December 4, 2019 2:49 PM  
**To:** Walker, Jonas (USAAC) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>  
**Cc:** 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>  
**Subject:** RE: Hardware and software Specifications

Mr. Walker,

Unfortunately, this is insufficient information to allow the defense to make a determination whether this machine will be adequate for defense testing purposes. Will you allow Joe Monroe to boot up the computer on Friday in Mr. Fischbach's presence so that more specific information can be obtained about what has been sent?

In addition, does the government intend to provide more and complete information regarding TD software specifications before this Friday, and as required by the court's order at Doc.254?

Thank you for your attention to these requests.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

---

**From:** Walker, Jonas (USAAC) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
**Sent:** Wednesday, December 04, 2019 12:41 PM  
**To:** Robert Herz  
**Cc:** 'Jeff M. Fischbach, ABFE'; Allison, Daryl (AN) (FBI)  
**Subject:** RE: Hardware and software Specifications

Mr. Herz:

I am advised that a computer with the following characteristics has been identified, which the government expects to be sufficient:

**Apple MacPro laptop with Windows 10 Pro loaded on Bootcamp partition Laptop has 16GB of RAM, 64-bit Operating System x64 based processor with a 250GB Hard Drive**

Thank you;

-AUSA Jonas M. Walker  
907.271.3983

---

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Tuesday, December 3, 2019 11:41 AM

**To:** Walker, Jonas (USAAC) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>

**Cc:** 'Jeff M. Fischbach, ABFE' <[jeff@secondwave.com](mailto:jeff@secondwave.com)>

**Subject:** Hardware and software Specifications

Mr. Walker,

At Doc. 262 the court ordered the defense to provide the government with the computer specifications the defense deems necessary to allow defense testing of the TD Software on a computer the government will provide for defense testing. Based on information provided to the government in email correspondence, pleadings, and declarations, the defense has made it clear that hardware specifications are predicated in part on the software the computer will run, meaning that it is important to know the specifications of the TD software. Ultimately, defense computer hardware specifications will be based on TD specifications as well as the various software Mr. Fischbach will install and that are needed for defense testing. The court ordered the government at Doc. 254 to provide the defense “with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements.” To date, the government has provided only a user manual for TD version 1.23, and it was redacted. This does not comply with the court order, and prevents the defense from more meaningfully providing computer specifications to the government by this Friday. The defense has provided the government with specifications recently in Mr. Fischbach’s declaration at Doc. 261 para.8. The defense believes that the court intends for the parties to refine these specifications which is why the court changed the defense deadline to December 6. If the parties are to refine the specifications as the court intends, then the government must provide TD software specifications as directed in the court’s order at 254, which in turn will allow the defense to make a more refined and tailored request concerning computer specifications. If the government is not willing to fully disclose software specifications to both TD versions in a timely manner and *before* Friday, which is necessary to allow for defense review and evaluation, then the defense will be unable to refine the specifications previously provided to the government, and those previously provided specifications will stand as to what the defense will be requesting.

Robert M. Herz

Law Offices of Robert Herz, P.C.

The Seventh and E Building

431 West Seventh Avenue, Suite 107

Anchorage, Alaska 99501

Tel. 907-277-7171

Email: [rmherz@gci.net](mailto:rmherz@gci.net)

Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

## Robert Herz

---

**From:** Walker, Jonas (USAAK) 5 [Jonas.Walker@usdoj.gov]  
**Sent:** Friday, December 06, 2019 3:25 PM  
**To:** Robert Herz  
**Cc:** Monroe, Joseph; Russo, Frank (USAAK); Allison, Daryl (AN) (FBI)  
**Subject:** RE: Schwier: Confirming that virtual machine will not be copied

Mr. Herz:

I appreciate the quick response. My understanding is that Mr. Fischbach is requesting access to the Apple MacPro laptop.

Before I respond, I will request that Mr. Monroe confirm that TD software is not currently loaded onto the Apple MacPro Laptop.

Mr. Monroe: Can you please review the Apple MacPro Laptop and confirm that TD is not currently loaded onto it?

Thank you,

-AUSA Jonas M. Walker  
907.271.3983

-----Original Message-----

**From:** Robert Herz <[rmherz@gci.net](mailto:rmherz@gci.net)>  
**Sent:** Friday, December 6, 2019 2:31 PM  
**To:** Walker, Jonas (USAAK) 5 <[JWalker5@usa.doj.gov](mailto:JWalker5@usa.doj.gov)>  
**Subject:** FW: Schwier: Confirming that virtual machine will not be copied

More accurately, I should say, that the machine from Anchorage DOJ will not open the VMs using the VMware software that Mr. Erdely used to create the VMs, i.e. the machine will not run the VMware software.

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

-----Original Message-----

**From:** Robert Herz [<mailto:rmherz@gci.net>]  
**Sent:** Friday, December 06, 2019 2:11 PM  
**To:** 'Walker, Jonas (USAAK) 5'  
**Cc:** 'Jeff M. Fischbach, ABFE'  
**Subject:** RE: Schwier: Confirming that virtual machine will not be copied

Confirmed.

In full disclosure, prior to knowing that TD may be on the VMs Mr. Fischbach in the presence of Mr. Monroe had copied the flash drive contents onto the computer previously sent to the RCFL from DOJ-Anchorage/FBI-Anchorage.

However, in speaking with Mr. Fischbach, the computer sent from Anchorage that Mr. Fischbach has been using does not have system requirements sufficient to open the flash drive containing the packet capture data or the VMs. Will you allow Mr. Fischbach to use the machine that was recently sent to the RCFL?

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
The Seventh and E Building  
431 West Seventh Avenue, Suite 107  
Anchorage, Alaska 99501  
Tel. 907-277-7171  
Email: [rmherz@gci.net](mailto:rmherz@gci.net)  
Website: [www.robertherzlaw.com](http://www.robertherzlaw.com)

-----Original Message-----

From: Walker, Jonas (USAAC) 5 [<mailto:Jonas.Walker@usdoj.gov>]  
Sent: Friday, December 06, 2019 1:37 PM  
To: Robert Herz  
Cc: Robert Erdely; Allison, Daryl (AN) (FBI); Arce, Charisse (USAAC) 1; [jeff@secondwave.com](mailto:jeff@secondwave.com);  
Joseph Monroe; Russo, Frank (USAAC); Cook, Brian J. (WF) (FBI)  
Subject: Schwier: Confirming that virtual machine will not be copied

All:

Per email traffic, Mr. Fischbach is accessing a flash drive containing packet capture data and virtual machines (VM) from the validation testing that occurred with Det. Erdely in Anchorage. The VMs may contain TD software.

It is the government's understanding that Mr. Fischbach will not be copying the VMs onto his own media (computer, flash drive, etc) or in any way removing the VMs from the OCRCFL.

Mr. Herz, please reply in writing to confirm this correct.

Thank you,

-Jonas Walker  
AUSA, District of Alaska

Sent from my iPhone

## **AFFIDAVIT OF ROBERT ERDELY**

1. This affidavit is regarding the motion titled “C-4 Motion to Compel Discovery and Production of Evidence” in *United States v. Matthew Schwier*, 3:17-cr-0095-SLG.
2. My credentials were previously set forth in my Affidavit filed at Dkt 214-1 and 214-2. Additionally, definitions and descriptions of the BitTorrent P2P Network and the ICAC Law Enforcement System were previously set forth in my Affidavit filed at Dkt. 214-1. I incorporate my credentials, definitions and background information as if fully set forth herein.
3. This affidavit is a supplementation of my previously prepared affidavit filed at Dkt. 214-1. In this affidavit I will address the declaration filed by Mr. Fischbach at Dkt. 203-1.

### **Analysis of Defense Expert’s affidavit**

4. I discussed this investigation with AUSA Jonas Walker who provided the defense experts declaration in this case. The following are my responses related to details found in Jeffrey M. Fischbach’s declaration.
5. In paragraph 3, Mr. Fischbach states: “The authenticity of the file allegedly downloaded by the FBI on or about November 22, 2016 remains in question. There has been no evidence produced, thus far, that the file used to substantiate the search of Mr. Schwier’s property was ever on any media or device associated with Mr. Schwier. Based on my review of the discovery provided by the government this file was not found on any digital media seized from Mr. Schwier’s residence. At this time, there is no known modified, accessed or creation (MAC) dates or times for this file. Similarly, there has been no metadata, typically used for the purposes of authenticating a file, its origin, dominions, and chain of custody. Most concerning to me, is that I have been unable to elicit from the government any of this forensically-crucial material, specific to the file the FBI claims to have downloaded remotely from Mr. Schwier -- the file which justified a search warrant, and subsequent arrest.”

RESPONSE: During the investigation, through the use of Torrential Downpour (TD), the downloaded material is saved to a directory named “download”. The associated log files are contained in the “logs” directory. The logs associated with this investigation detail the date and time when the investigation begins along with other details. Regarding Mr. Fischbach’s request, the dates and times when the file was downloaded is found in the “details.txt” file which is contained within the logs directory. It is my

understanding that this information has already been provided in discovery. This log will provide information as to the date and time the file began the downloading process, the dates and times which each piece of data was received during this investigation and the date and time the download had completed the downloading process. The MD5 and SHA1 hash value of the entire file is located at the bottom of this log file. It also provides information regarding the SHA1 hash verification of every piece downloaded from the suspect computer, where the data downloaded is compared to the values contained within the .torrent file (the instructions). Through the downloading of the file, and this checking of each and every hash value of the pieces received, only a computer possessing the file could have distributed the data to the investigative computer.

6. In paragraph 4, Mr. Fischbach states (in part): “The data provided in response to my request is a Bit Torrent log file, which does not provide any information sufficient to extrapolate chain of custody or determine authenticity.”

RESPONSE: Mr. Fischbach’s claim that the log file does not provide any information to determine the downloaded files authenticity is incorrect. As stated above it contains not only the hash value of the file but each and every piece hash and the verification of those pieces using the SHA1 hashing algorithm.

7. In paragraph 6, Mr. Fischbach states (in part): “A copy of the file stored on some other media provides little to no authentication information about how or when the file was “captured.” The original media itself contains that information.”

RESPONSE: Mr. Fischbach’s claim above is incorrect. Given the fact that accompanying the file downloaded is the detailed log, the SHA1 hashing of the pieces along with the verification of those pieces should provide any expert the means necessary to verify that this is the file associated with the .torrent being investigated. Using the same hashing method used by the BitTorrent file sharing network, the expert can independently verify that this is the file relating to the download conducted. I will make available all of the files associated with the .torrent being investigated and a SHA1 hashing report of those files, confirming that these are in fact all the files described by the .torrent to aid him in his analysis. As the lead instructor of this investigative software and a user of the software (TD), giving a defense expert access to the investigative computer would provide him with access to the investigative software itself and potentially expose him to details of active investigations.

8. In paragraph 9, Mr. Fischbach states (in part): “It is imperative for me to inspect and examine all metadata, as well as determine the file’s true and accurate file

name, file size, and file path, the means by which it was captured and preserved, determine a valid hash value”.

RESPONSE: Mr. Fischbach has received the details.txt (the detailed logging of the investigation) which includes details regarding the file, including not only the files SHA1 hash value of any completed download, but also the hash value of every piece of data downloaded. Examining the .torrent file being investigated include the following:

- file names
- file paths
- file sizes
- piece size
- SHA1 piece hashes

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge and belief.



Detective Robert W Erdely  
Date: 9-19-2019

# Curriculum Vitae

*Robert William Erdely*  
*Pennsylvania State Police (retired)*  
*244 McHenry Road*  
*Indiana, Pa. 15701*

## **Certifications**

---

- 2009 Access Data Certified Forensic Examiner
- 2009 Certified at the Federal Law Enforcement Training Center, Seized Computer Evidence Recovery Specialist
- 2007 Certified Forensic Computer Examiner, International Association of Investigative Specialists
- 2004 Certified Cisco Internetwork Professional
- 2004 Certified Information Systems Security (INFOSEC) Professional.
- 2004 Certified Cisco Security Professional.
- 2004 Certified by ISC2 as a Certified Information Systems Security Professional (CISSP®)
- 2003 CompTIA A+ Certified Professional.
- 2003 Certified a Microsoft Database Administrator
- 2003 Certified as a Microsoft Systems Engineer for Windows 2003
- 2003 Certified as a Microsoft Systems Engineer: Security
- 2003 CompTIA i-Net+ Certified Professional.
- 2003 CompTIA Network+ Certified Professional.
- 2003 Certified Cisco Design Professional.
- 2002 EnCase Certified Examiner
- 2001 Cisco Certified Network Professional.
- 2001 Certified as a Microsoft Systems Engineer for Windows 2000
- 1999 Certified as an Electronic Evidence Collection Specialist, International Association of Computer Investigative Specialists

## **Professional Activities**

---

- 2010-2016 Member of Interpol's Technical Working Group which is currently working with Law Enforcement and Universities to develop tools to investigate the exploitation of children on the internet.
- 2010-Present Instructor for both the International Centre for Missing and Exploited Children and Fox Valley Technical College
- 2009-Present Developed a system to investigate the sharing of child pornography on the internet.. This information is used by law enforcement in over 60 countries to locate, investigate and prosecute these child predators. This system has resulted in the initiation of more than 15,000 investigations and rescuing countless child victims.
- 2007-Present Instructor for the Internet Crimes Against Children (ICAC). Instruct online Investigations, including Peer-to-Peer file sharing networks.

## **Experience**

---

- 2012-Present Detective with the Indiana County District Attorney's Office, Indiana County Pennsylvania. Assigned to investigate child exploitation investigations. I am currently assigned to the FBI Innocent Images Task Force, Pittsburgh, Pennsylvania.



- 2008-2012 Supervisor for the Pennsylvania State Police (PSP) Computer Crime Unit, Harrisburg, PA. Supervised both the investigative and digital forensic sections of the PSP.
- 2003-2008 Supervisor of the Southwest Computer Crime Task Force comprised of State and Local Law Enforcement.
- 1998-2003 Assigned to Bureau of Criminal Investigations, Computer Crime Unit. Responsible for all aspects of proactive and reactive investigations, including evidence duplication, documentation and examination, regarding criminal activities utilizing technology to facilitate the illegal activities.
- 1997-2007 Senior Computer Network Administrator for an Internet Service Provider, providing service to over 3000 users
- 1999-2004 Instructor for the Pennsylvania Chiefs of Police Association for Federal, State and Municipal Police Officers along with representatives of the Attorney General and the District Attorneys regarding computer forensic examination processes and procedures and the online investigation of computer crime.
- January 2003 Speaker at the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network's (MAGLOCLLEN) Internet Investigation training Conference.
- October 2001 Speaker at the Pennsylvania District Attorneys Institute's Computer Crimes Training course.
- 1994-1998 Assigned to PSP Vice Unit, Troop A
- 1992-1994 Assigned to Patrol Unit, PSP, Indiana, PA.

## **Education and Training**

---

- 1989 Community College of the Air Force
- 1990 Edinboro University of Pennsylvania
- 1992 Graduated from the Pennsylvania State Police Academy
- 1994 Drug Investigators Course
- 1995 Narcotics in the mail, Interdiction and Clandestine Labs seminar, U.S. Department of Justice
- 1995 Investigation of Computer Crime, National White Collar Crime Center
- 1996 Vice Investigations Seminar
- 1996 Eastern States vice Investigator training Conference
- 1997 High risk Warrant Service Training
- 1997 Gambling Device Examination Training
- 1997 Top Gun, Undercover Drug Law Enforcement Training
- 1997 Certified to Utilize Electronic Surveillance (Wiretap)
- 1999 Investigation of Computer Crime, International Association of Chiefs of Police
- 1999 Investigation of Computer Crime, SEARCH, the National Consortium for Justice Information and Statistics
- 1999 Unix investigators course at FBI Academy
- 2001 Guidance Forensic Software Intermediate Course
- 2001 Guidance Forensic Software Advanced Course
- 2002 16 hour Windows 2000 Security seminar by Computer Security Institute at FBI Pittsburgh
- 2002 Fundamentals of Incident Handling course at the CERT Coordination Center (Incident Handling for Computer Emergency Response Teams).
- 2002 High Technology Crime Investigation Conference
- 2002 Advanced Data Recovery and Analysis, National White Collar Crime Center
- 2004 Advanced Solaris Administration Course by FBI
- 2004 FBI Symposium on Online Child Pornography/Child Exploitation
- 2005 National White Collar Crime Center's Advanced Data Recovery and Analysis course
- 2005 Attended NTI Forensic Examination training

2006 Department of Defense Cyber Crime Conference

2006 Sun Educational Service course “Securing Solaris & Network Intrusion Detection”

## **Publications**

---

Forensic Investigation of Peer-to-Peer File Sharing Networks.

DFRWS Annual Digital Forensics Research Conference, August 2010

## **Certified Expert**

---

- Certified as a computer expert including online investigations by the United States District Court, Western District of Pennsylvania, in United States vs. Abraham (2006)
- Certified as a computer forensic expert by the United States District Court, Eastern District of Pennsylvania, in United States vs. Schade (2008).
- Certified as a computer expert including online investigations in Middle District of Pennsylvania, United States vs. Doyle. (2011)
- Certified as a computer forensic examiner and in internet investigations in the Eastern District of Pennsylvania, United States vs. Fitzgerald Horton (2013)
- Certified as an expert in the case State of New Jersey v. Julio Gomez-Marte (2015)
- Certified as a computer forensic examiner and in internet investigations US District Court Maryland, US vs. Carl Javan Ross (2016)
- Certified as a computer forensic examiner and in internet investigations State of New Mexico vs. Jeffrey Morrill (2016)
- Testified as an expert in the BitTorrent file sharing network. US v Larry O’Neal US District Court Bangor Maine (2019)
- Testified as a file sharing expert in US v Matthew Lee Lane Eastern District of Washington State

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
431 W.7th Avenue, Suite 107  
Anchorage, Alaska 99501  
907-277-7171 Phone  
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

United States of America, )  
 )  
 Plaintiff, )  
 ) Case No. 3:17-cr-0095 SLG-DMS  
 )  
 vs. )  
 )  
 Matthew Schwier, )  
 )  
 Defendant. )  
 )  
 )  
 \_\_\_\_\_ )

**DECLARATION OF JEFFREY M. FISCHBACH**

I, Jeffrey M. Fischbach, declare as follows:

1. This declaration is written in response to the government’s Dkt. 288, “Notice Regarding Proposed Testing Environment”, and 288-1, “Test Environment Regarding Torrential Downpour”.
2. In both writing my November 25, 2019 Declaration, and at the hearing on November 26, 2019, I attempted to articulate compromise, in order to assuage the government’s concerns for its proprietary software; while remaining focused on the tests deemed necessary in order to competently prepare counsel for trial. At the same time, I have attempted to observe and

DECLARATION OF JEFFREY M. FISCHBACH

reb1

maintain sound scientific and forensic practices -- both necessary to survive a Daubert-Frye challenge, as well as to assure the integrity of my results and to ensure the security of my work product and of the software in question.

3. It appears that the government has almost wholly superseded its Dkt 253-4 with new, much more harsh restrictions proposed in Dkt 288 and 288-1. Nearly every item proposed in Dkt. 288 and 288-1 serves to add additional impediments to Torrential Downpour (TD) testing of any kind, adds several new means for the government to monitor and surveil defense testing, *in real-time*, exposing work product and privilege in the testing process. Yet, while this new proposal adds numerous barriers to performing the tests that the court found material, it does nothing to prevent TD from “escaping” into the “wild”.

4. While the defense has objected to being forced to create discovery of its own testing procedures; in Dkt 288 and 288-1, the government has now gone much further than its proposal in Dkt 253-4. As an expert for decades, I understand that my results will be subject to scrutiny - if used at trial. Hence, I understand I will have to document my work, as well as the forensic measures I have taken to protect assets, such that it could be independently reproduced. The means of doing so, however, has never been dictated to me by the government or by the court.

5. Confirmation bias has long plagued forensics. But, in this particular circumstance, the capability to narrow recorded results by using Wireshark’s built-in filters was actually demonstrated by Mr. Erdely during his “validation” sessions. Thus, with the government documenting my work, not only do they see my test results before I can even report them to counsel, but I have no ability to audit my own discovery for accuracy. I testified on November 26, 2019 that Dkt 253-4’s proposal that I must maintain a Wireshark log of all my work could be easily manipulated. As a result, it seems, the government has now proposed in Dkt 288-1 that *it* must be able to record and maintain easily-manipulated Wireshark logs of all of my testing, as well as control the router which carries all of my testing traffic. Which, in addition to *very* realistically altering my results before I read them, or for the government to collect conflicting results, it also gives the government the opportunity to filter, intercept and modify every piece test input data from one machine, before it even reaches the other, or to return

modified results. Submitting to this proposal has the making of a forensic science scandal rivaling any of the recent FBI lab scandals. Again, I refuse to be a party to bad scientific practices and dangerous precedent.

6. Dkt 288 and 288-1 does, however, carefully dictate the way that the defense can conduct its tests by not only providing an environment designed around Mr. Erdely's TD "validation", but then completely denying the defense use of the Internet for its testing. Something which Mr. Erdely himself stated, during his validation, was a *requirement* for using TD in any way.

7. Despite the government's failure to secure its own software and secrets, I have gone to great lengths, both to voluntarily alert the government and the court about information which they accidentally provided to me, as well as to attempt to use equipment owned by the government, at facilities run by the government, and to utilize very expensive specialized hardware and software at my disposal to further reduce the risk of accidental dissemination. To wit, I suggested the use of the LA SCIF, when it was demonstrated to me that the OCRCFL does not physically guarantee the security of equipment and data left in its shared defense exam room.

8. In Dkt 288, p7 the government refers to my suggestion to use the Roybal SCIF as "unusual" -- not untenable. All parties seem to agree that RCFL facilities are not equipped to monitor against theft of hardware and software, as has already occurred in this case. Out of an abundance of caution, based on decades of experience with government examination facilities, I have provided objectively more secure alternatives to the OCRCFL. In my experience, the SCIF in Los Angeles are simply isolated single rooms, containing no access to sensitive information, *other than that which the analyst is currently examining*. Thus, while this may be a "inconsistent" use-case, the treatment of software as "government sensitive" is also inconsistent with all standard investigative software, which have been openly tested and utilized by the forensic community. I have had access to the SCIF in Los Angeles, where I had permitted use of my own laptop and cellular devices, with only the admonishment of a "lifelong obligation to protect from disclosure the classified information" to which I had access.

9. The government refers to "*general*" principles of SCIF operation. Thus, one can assume

that these principles apply generally, but not exclusively. And, that while my suggestion for a more secure location to conduct my TD tests is “unusual”, it apparently does not go against any particular rules or policies. It should be further noted that, in my *proven* classified experience, while information relative to a particular case is stored in a particular locked and secured SCIF room, the SCIF itself does not provide information to any classified or other case information, beyond the immediate case being examined.

10. I see no reason provided in Dkt 288 to explain why the LA SCIF cannot be used, nor why it is any less secure than the OCRCFL. While the government is correct that the LA SCIF at Roybal is several hours closer to me, which will allow me to complete my work significantly faster, security is the primary reason I suggested this facility, as well as the LA FBI building at Wilshire. I suggested both of these locations before the government decided to impose use of OCRCFL. I have used all three locations in Federal trials many times, and have been long aware that the RCFL does not provide security comparable to the other two sites. Thus, when requesting the ability to continue examining the case in Los Angeles in order to expedite trial readiness, I suggested either the LA Wilshire FBI defense examination facilities or the Roybal SCIF -- for the purposes of hardware, software and data security as well as location.

11. Dkt 288 and 288-1 provide conflicting information, by arguing *both* that I can't use the SCIF because I need to use the Internet and some of my own hardware to conduct my tests, *and* that I can no longer use the Internet *or* my own hardware at the RCFL. While Dkt 288-1, paragraph 3 proposes, “No other electronic devices or storage devices may be brought into the testing room to include but not limited to computers, phones, laptops, hard drives, or tablets”, Dkt 288 (Page 8) states, “...the evidence review includes use of the internet and the presence of Mr. Fischbach's computers. Therefore, the SCIF is not an appropriate place for evidence review in this case.” It appears here that the government acknowledges the need for the defense to utilize its own equipment and Internet service to complete its testing, for the purposes of denying use of the SCIF, yet denies defense use of its own equipment and Internet service for the purposes of using the less-secure defense examination room at the OCRCFL.

12. Similarly, while Dkt 253-4 (Para 6) specifies exactly what kind of Internet device I may

bring to conduct my tests, Dkt 288-1 (Para 5) completely denies *any* use of the Internet at all for testing. And, while Mr. Erdely has gone on-record that TD *requires* use of the Internet for the “validation” he performed in my presence on November 4, 2019, or use of any Torrent activity, the government has, in Dkt 288-1, once again proposed an environment that appears nearly identical to Mr. Erdely’s “validation” methodology. Dkt 288-1 doesn’t even allow me to conduct Mr. Erdely’s own “validation” procedures, let alone the tests the court has already ruled material.

13. Preventing data from being disseminated is one of the key roles of the established forensic hardware I use in my testing and examination. In this new proposal, while the government suggests that its interests are in protecting the software that *they* have already accidentally released to me *without* any of their proposals in place -- I have now been completely restricted from using any equipment to secure any subsequent copies.

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on December ???, 2019.



---

Jeffrey M. Fischbach

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
431 W. 7<sup>th</sup> Avenue, Suite 107  
Anchorage, Alaska 99501  
907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

United States of America, )  
)  
Plaintiff, )  
)  
vs. ) Case No. 3:17-cr-00095 SLG  
)  
Matthew Schwier, )  
)  
Defendant. )

**DECLARATION OF JEFFREY M. FISCHBACH**

I, Jeffrey M. Fischbach, declare as follows:

1. I am a computer forensics expert and founder of SecondWave, Inc. a firm specializing in digital forensics. My offices are located in Los Angeles, California. I am competent to testify and the matters contained herein are based on my own personal knowledge.
2. I am a board-recognized computer forensic examiner specializing in information, communication, stored data and electronic location technologies;
3. I have worked as an expert in this field for more than twenty-five years and have consulted on, and testified in municipal, Federal and military courts, both domestic and abroad, in dozens of cases involving digitally-recorded evidence, and offer my services to both Government and Defense;
4. I have been granted security clearance, and use of a Sensitive Compartmented Information Facility (SCIF) by the DOJ for the purposes listed above;
5. I routinely lecture and provide training in my area of expertise to civilian attorneys, law enforcement, and judges throughout North America, and my opinions have been cited, on record, by the United States Supreme Court;

6. I have conducted hundreds of forensics examinations on thousands of pieces of  
Case 3:17-cr-00095-SLG Document 200-1 Filed 09/12/19 Page 1 of 11



evidence, including hard drives, cell phones, removable storage media, network data centers, and other electronic devices. My Curriculum Vitae is attached hereto.

7. I have provided expert forensic consultation in hundreds of criminal cases throughout the United States, the EU, Japan, Guam, and Rio de Janeiro, since the year 1997, and have testified dozens of times in State, Federal and Military Courts. I have qualified and testified as an Expert in numerous State and Federal Courts in the fields of forensic Data, Cellular Phones, Cellular Tower Coverage, RF Propagation Mapping, GPS Accuracy, Computers, Audio, Video, Data Analysis, and still Image Analysis. I have testified in numerous federal courts as an expert in Computer Forensics and Cellular Phone and Cellular Records analysis. I have worked as a defense expert on dozens of state and federal cases nationwide that were subject to Protective Orders and/or Non-Disclosure Agreements (NDA). I have never violated, nor have I been accused of violating any Protective Order or NDA. To the contrary, my services have been utilized by courts for the purposes of assisting in investigations of alleged misconduct by government agencies. I consult with law enforcement agencies whenever requested.

8. I have been retained as a computer forensics expert by Robert M. Herz, counsel for Mr. Matthew Schwier, for the purpose of assisting with matters related to the searching, collecting, analyzing and producing of electronic evidence in this matter. I have reviewed discovery materials produced to the Mr. Schwier by the Department of Justice including, but not limited to seized and cloned hard drive, SD cardZ, and disc media, as follows:

- a. Government Exhibits 1a, 1b & 1c, a pink folder with printed material enclosed;
- b. Government Exhibit 2a, a pink folder with printed material enclosed; Item 2a appears to be a print-copy of 1B37, but contains no authenticating hash value or chain of custody documentation;
- c. Government Exhibits 3a-3c, a pink folder with printed material enclosed;
- d. Government Exhibits 4a & 4b, a pink folder with printed material enclosed;
- e. Government Exhibits 5a-5e, a pink folder with printed material enclosed;
- f. Government Exhibits 6a-6c, a pink folder with printed material enclosed;

- g. 18-295-02A (CD-R), entitled “hashes”;
- h. 18-295-02A 1b33 A Mac Tower, with attached hard drive, containing forensic image files;
- i. 18-295-02A 1b34 (CD-R), entitled “One CD with hash values containing CP found on comp...”;
- j. 18-295-02A Item 1b36, entitled “One CD containing Bit-Torrent session logs from 11/22/2016”. Contains 2 duplicate folders found in 1B37: SD /2016-11-22\_20-48-30\_31/Download & /2016-11-22\_20-48-30\_31/Log;
- k. 18-295-02A Item 1b37 (SD Card”, entitled “One SD card containing FTK reports, file with hash values, BitTorrent session logs”. Contains SD CARD Distribution/1180842565051.jpg. NO chain of custody provided, but torrent logs were (SD CARD BT Session/2016-11-22\_20-48-30\_31/Logs & SD CARD BT Session/2016-11-22\_20-48-30\_31/Download). Contains ZERO (0) byte files, duplicate provided on CD in Anchorage. 1B37 SD CARD also contains CP hashes [EMPTY FOLDER] & FTKReports, as previously provided;
- l. 18-295-02A Item 5c (CD-R), entitled “Schwier CP hashes”;
- m. 18-295-02A Item 5c (CD-R), entitled “Schwier BT Session”;
- n. 18-295-02A Item 5c (Portable Hard Drive), entitled “Passport”;
- o. 18-295-02A Item 5c (SD Card), entitled “FTK reports, has values, bit torrent”;
- p. 18-295-02A Item 5c (DVD-R), entitled “Obscene Material, return to FBI”;

9. It should be noted that almost every item listed above contained duplicate items, in part, or in whole, within other evidence provided. Although provided individual item identification, the actual volume of unique, non-duplicate evidence in this matter appears to be just a fraction of what appears in the itemized discovery.

10. According to discovery, this case originated on October 20, 2016 when the IP address 216.137.195.191, as identified by FBI SA Daryl Allison, was allegedly sharing files, which he identified as possible child pornography.

11. In order to understand the complexities of the undercover investigation that allegedly identified Mr. Schwier in this matter, it is imperative to understand the difference between the “BitTorrent network”, a “torrent”, an “info hash”, a common web page, and an actual image or video that depicts child pornography.

12. The “BitTorrent network” is essentially a protocol, or set of rules that allows users

to download and/or upload parts of files between many different users for the purposes of reassembling the constituent parts into complete files. The process is analogous to an automobile manufacturer receiving parts of a vehicle from various sources. Minus any single part, the automobile may not be capable of being driven. This means that someone downloading files on the BitTorrent network may get small pieces of a file from many different computers in order to reassemble the complete file on their own computer. This also means that, as a single un-drivable portion of an automobile frame may contain an identifiable registered Vehicle Identification Number (VIN), a user with an empty file container or a small fragment of a file may still be identified on the BitTorrent network as a download candidate for the whole file, even if they don't possess the whole file.

13. The object behind this protocol is similar to automotive assembly line methods. It is to facilitate a fast delivery and assembly of a file, by "shipping" multiple parts simultaneously from numerous sources. As such, a file that might have taken hours to download from a single source, might only take minutes via a torrent network.

14. A "torrent" itself is simply a text file, proprietary to the BitTorrent network that contains instructions for torrent software, such as uTorrent or BitLord, which describes how to download a file or sets of files on the BitTorrent network. Torrent files do not contain content data, such as images or videos, but rather an index containing information about the files associated with that torrent including but not limited to, names of the files instructed to download, the torrent author, the date the author of the torrent created the file, the number of files the torrent is set to download, and the URLs tracking the torrent activity.

15. An "info hash" is a mathematical algorithm or hash value that uniquely identifies the "torrent" on the BitTorrent network. Although it has been described as synonymous with a fingerprint, the info hash only identifies the torrent itself, not the actual files the torrent would download if parsed.

16. If, for example, Person A downloads a torrent to his computer, the info hash and file names of every file associated with that torrent would be automatically saved (cached) to his computer. If that torrent is never parsed, the associated files are never

actually downloaded to the computer and Person A does not possess those files.

However, that torrent may still be read by torrent software and falsely advertised on the BitTorrent network as a download candidate for all of the associated files, even if none of the files exist. Similarly, forensic software would be able to identify the *names* of those files, even though the files themselves had not been received. If Person B tries to download the same torrent on the BitTorrent network, Person A will be listed as a download candidate. However, the files downloaded to Person B's computer will not come from Person A, rather, the bits and pieces will come from other users on the BitTorrent network who actually have the files.

17. During my independent computer forensics examination of items seized from Mr. Schwier, I was not able to locate the torrent, the info hash or the files of child pornography identified during the undercover investigation. In addition, the torrent, the info hash and the files of child pornography were not found by the government's forensic examiner either. According to discovery, it appears that the information that a torrent containing files of child pornography was available at IP address 216.137.195.191 was actually obtained by automated law enforcement sensitive software that monitors peer-to-peer file sharing networks. That software was identified in discovery as Torrential Downpour.<sup>1</sup> "Torrential Downpour" is part of a larger Peer-to-Peer (P2P)

---

<sup>1</sup> See Government discovery Bates Stamped pages:

1. Bates 176-232 – 10/20/16 Details Log: "Torrential Downpour" appears at p. 1 (Bates 176) – "2016-10-20 01:33:56 - Torrential Downpour version 1.23"

2. Bates 233-238 – 10/20/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 233) – "<!-- Torrential Downpour download status -->"

3. Bates 240-267 – 10/20/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 240) – "2016-10-20 01:33:56 - Torrential Downpour version 1.23"

4. Bates 270-531 – 10/20/16 Details Log: "Torrential Downpour" appears at p. 1 (Bates 270) – "2016-10-20 02:14:05 - Torrential Downpour version 1.23"

5. Bates 532-536 – 10/20/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 532) – "<!-- Torrential Downpour download status -->"

6. Bates 540-635 – 10/20/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 540) – "2016-10-20 02:14:05 - Torrential Downpour version 1.23"

7. Bates 637-1901 – 10/20/16 Details Log: "Torrential Downpour" appears at p. 1 (Bates 637) – "2016-10-20 03:46:41 - Torrential Downpour version 1.15" and "2016-10-20 03:46:42 - Torrential Downpour version 1.15"

8. Bates 1902-1915 - 10/20/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 1902) – "<!-- Torrential Downpour download status -->"

9. Bates 1920-1948 – 10/20/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 1920) – "2016-10-20 03:46:41 - Torrential Downpour version 1.15" and "2016-10-20 03:46:42 - Torrential

Downpour version 1.15"

communications investigation toolset collection known as “RoundUp Suite”. See, Liberatore, Levine, Wallach, Wolak & Kerle, 2015. As part of the RoundUp Suite, “Torrential Downpour” was apparently developed to enable single-source peer-to-peer file sharing between law enforcement and target computers potentially sharing contraband files or media. RoundUp Torrential Downpour is a specially modified version of a BitTorrent client. RoundUp Suite is available to law enforcement *only*, and is provided at no cost to eligible law enforcement entities. Liberatore, et al, 2015. As such, scientific peer review has not been conducted, as has been done in other investigative software, like AccessData’s Forensic Toolkit (FTK), and Guidance Software’s EnCase, that can be obtained and tested by individuals in the scientific (e.g., non-law-enforcement) community.

18. The foundational toolsets for what are now known as RoundUp Suite were the product of law enforcement agencies partnering with Oak Ridge National Laboratory in 2009, in an effort to automate investigative processes involving Peer-to-Peer networks. See, Borges et al 2011.

19. I have examined work product, and reviewed available online information about Torrential Downpour, and have read cases where the program was used and described. This information states that the program generates log files for use as evidence in

---

10. Bates 1950-7923 – 11/20/16 Details Log: “Torrential Downpour” appears at p. 1 (Bates 1950) – “2016-11-20 19:23:13 - Torrential Downpour version 1.15” and “2016-11-20 19:23:14 - Torrential Downpour version 1.15”

11. Bates 7924-7937 – 11/20/16 Download Status Log: “Torrential Downpour” appears at p. 1 (Bates 7924) – “<!-- Torrential Downpour download status -->”

12. Bates 7954-7992 – 11/20/16 Summary Log: “Torrential Downpour” appears at p. 1 (Bates 7954) – “2016-11-20 19:23:13 - Torrential Downpour version 1.15” and “2016-11-20 19:23:14 - Torrential Downpour version 1.15”

13. Bates 7994 – Data Written Log: “Torrential Downpour” appears – “<!-- Torrential Downpour data written information -->”

14. Bates 7996-8203 – 11/22/16 Download Status Log: “Torrential Downpour” appears at p. 1 (Bates 7996) – “<!-- Torrential Downpour status -->”

15. Bates 8207-8938 – 11/22/16 Summary Log: “Torrential Downpour” appears at p. 1 (Bates 8207) – “2016-11-22 20:48:30 - Torrential Downpour version 1.15” and “2016-11-22 20:48:3014 - Torrential Downpour version 1.15”

criminal trials. A key purpose of the Torrential Downpour software is to log and document efforts to download contraband from a target computer. According to the discovery provided, as well as repeated unanswered requests for authenticating documentation, the Government has produced in this case no uniquely-identifying device data beyond basic IP addresses associated with the defendant's wireless household network. In my opinion, and in the opinion of respected forensic investigators, comprehensive forensic investigations must include device-identifying data that exceeds basic IP address assignments from an Internet Service Provider (ISP), to include system level Globally Unique Identifier (GUID) logs.

20. In my examination of the government's case I have discovered that the investigator's claim to have accessed numerous files which could not be downloaded. According to the BitTorrent protocol, the only reason a file could not be downloaded is because either no content exists on the queried system, or because that file was not being shared by the user. In the instant case, the investigator identifies numerous files which he says he was unable to download. It is my opinion, given what I know of the BitTorrent protocols, that either the investigator is mistaken, the software was operating in error, or the software has been modified in such a way as to exploit vulnerabilities in the protocols, and force the client to exceed the limitations of the BitTorrent protocol, thus "hacking" the source for evidence of files not intended to be shared.

21. It is well-known, and confirmed, that prior versions of popular BitTorrent client software, including uTorrent, contained serious remote exploits that have since been acknowledged and patched in current versions. (See, BitTorrent Bootstrap 'lazy\_bdecode.cpp' Remote Code Execution Vulnerability, Symantec Corporation [US]: Security Focus.<https://www.securityfocus.com/bid/70812/discuss>). These vulnerabilities allow the client computer to be manipulated remotely, without the user's knowledge.

22. Given Torrential Downpour's alleged ability to "see" files that appear not to be available for download, it seems very likely that the application leveraged a BitTorrent Remote Code Execution vulnerability to allow law enforcement investigators to control the file sharing settings on the suspect devices remotely. Descriptors listed in various

vulnerabilities indicate that use of the exploit could in fact be used to execute code that, by extension, could then modify user settings in an application's sharing permissions. Whether or not a particular vulnerability was exploited, it has been reported in a number of cases that Torrential Downpour may be exploiting vulnerabilities in the Torrent client allowing law enforcement access to files not meant to be publicly shared. A defense examination of the Torrential Downpour software can confirm or deny the use of any BitTorrent vulnerability exploits. Defense experts, in my opinion, should be allowed to examine, under controlled and protected conditions, any and all logs, including system level GUID logs, associated with the investigation of the defendant's internet communications activities as well as the program itself and its user materials.

23. Having examined numerous P2P cases, and from personally observing the testimony of law enforcement personnel on similar cases, serious concerns have been raised regarding "quarantined" or proprietary law enforcement software that has not been subject to peer review, including Torrential Downpour, questioning the software's accuracy and reliability and whether the software is going beyond the scope of "publicly available" information. To my knowledge, as of the writing of this Declaration, this software has never been formally tested and/or validated by anyone and is unavailable for testing by any third-parties.

24. In my experience, it is critical to the defense of Mr. Schwier's case to understand how this software functions in order to determine its reliability and accuracy in identifying files reported as "publicly available" from Mr. Schwier's computer. In addition, forensic review of the Torrential Downpour software may enable the defense to show that the program had capabilities beyond those claimed or acknowledged by law enforcement. This evidence may help the defense demonstrate how law enforcement was able, using the software, to access files on defendant's devices that were apparently inaccessible for download by either specialized law enforcement tools, or by members of the general public. In a measurable way, such capabilities could be had by exploiting [subsequently patched] BitTorrent client software vulnerabilities, and changing or overriding user settings to allow police to access files defendant had intended to keep

private, by searching for files in places defendant had intended to block from access to other Bit Torrent users, or by downloading only fragments of files, rather than complete files.

25. Furthermore, Mr. Herz has requested my assistance in preparing cross-examination of a government witness who will testify about his use of Torrential Downpour as *the* culminating basis of his investigation of Mr. Schwier. Without access to this software, I can neither confirm the technical accuracy of the witnesses' testimony, nor can I competently prepare defense counsel to cross-examine the witness.

26. Thus, the implication in this case is that the software may be identifying files of suspect child pornography as being on Schwier's computer that in fact are not there or are not "publicly available" and were not intended to be shared. Since the Torrential Downpour software has never been independently tested and validated it is critical to Mr. Schwier's defense to understand how this software functions in order to determine its reliability and accuracy in identifying files allegedly belonging to Mr. Schwier. This is especially so when none of the files, the torrent or the info hash were found on any of his computers. Again, to my knowledge, no publicly available study has been undertaken to ascertain the reliability of the data produced and reported by the Torrential Downpour software.

27. In my quarter-century of forensic experience, much of which comes from examining, following, and teaching acceptable scientific and law enforcement practices, it is not acceptable science to rely on a tool (software) that has not been tested and subjected to peer-review. Even less-so when a tool is barred from peer review. This is why most forensic examiners use tools like EnCase and FTK, because they are industry standard tools that are available for testing and validation by anyone and, as such, have been accepted by the Courts as viable tools. However, even those tools have been proven to produce inaccurate and unreliable data at times which has only been discovered through the ability to test and validate them, leading to critical patches in the software.

28. The biggest challenge with developing an accurate tool is the diversity of hardware data being collected and analyzed. This is why even tools like EnCase and FTK



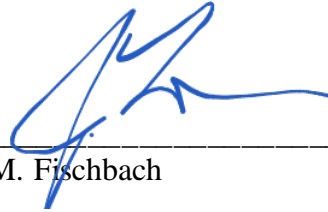
sometimes produce inaccurate and unreliable results. No two computer systems are identical. Computers are installed with different operating systems and there are hundreds of different versions of the same operating system, some are updated regularly and some are not updated at all. Those operating systems have thousands of different settings that can make each system unique in how it functions and records data. Within those operating systems a user can install millions of different software applications from large commercially produced software to small home-made software applications. Software applications may have bugs; data can be corrupted or incomplete; computers can be infected with viruses, Trojans and other malware. All of these variables have an effect on how that data is collected, analyzed and documented by a tool. While a tool may provide accurate information on an updated Windows system without any malware, the same tool may yield false results on a system that has not been updated and is infested with viruses.

29. When talking specifically about peer-to-peer (P2P) software, there are hundreds of versions of file sharing software applications that users can download from the Internet. Some are free and some are paid. Some are updated regularly with new versions, some are not. Some of those applications are open source, meaning the user can actually modify the source code of the application allowing it to function differently than the exact same piece of software installed on another computer. I have personally been researching, testing and analyzing P2P file sharing software available to the public for over ten years including, but not limited to, LimeWire, FrostWire, Bearshare, Ares, BitTorrent, eMule, Phex and Shareaza. What I have discovered in all of these programs is that they can contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable. In that regard, any tool used to collect, analyze and document data associated with these applications may also be inaccurate and unreliable.

30. For all of the reasons stated above, and under general scientific principles, it is my opinion that the software relied upon during the undercover investigation needs to be tested and validated by a qualified third-party to determine its functionality, accuracy and reliability.

31. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, and I hereby reserve the right to amend any statement should additional information be made available to me at a later date.

DATED at Los Angeles, California, this 12th day of September 2019.



---

Jeffrey M. Fischbach

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
431 W.7th Avenue, Suite 107  
Anchorage, Alaska 99501  
907-277-7171 Phone  
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

United States of America, )  
)  
Plaintiff, ) Case No. 3:17-cr-0095 SLG-DMS  
)  
vs. )  
)  
Matthew Schwier, )  
)  
Defendant. )  
)  
\_\_\_\_\_ )

**DECLARATION OF JEFFREY M. FISCHBACH  
IN SUPPORT OF DEFENSE MOTION FOR RECONSIDERATION**

I, Jeffrey M. Fischbach, declare as follows:

1. In its “ORDER RE MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER (Dkt. 254)” the court has demonstrated clear efforts to strike a balance between the need for the defense to complete tests which the court has found to be material, with the government’s concerns regarding *potential* distribution of its proprietary software. However some government language adopted by the court, makes it impossible for me to conduct the tests which the court has found are material to the defense. Mr. Walker himself, has admitted that the arbitrary limits he has asked the court to adopt, *do not* actually serve to prevent the government’s software from “escaping into the wild”. Specifically, the government’s arbitrary constraints on how I physically can and cannot access the government’s own equipment prevents me from conducting the defense tests that I must complete for trial. I do believe, however, that this may be a simple misunderstanding of the software and equipment necessary

DECLARATION OF JEFFREY M. FISCHBACH

reb1

to complete testing and subsequent analysis.

2. Without unfettered access to computer ports, in order to install my own tested, industry-accepted software and hardware, as well as to remove my test results from the government provided computer for further examination and analysis at my laboratory, I simply can't complete the tests that the court has found material to this matter. With current restrictions in place, I can't even connect a screen, keyboard, or mouse, let alone the hardware and software that I need for my tests, and that are required by industry standard forensic practice in order to insure that no data accidentally alter my results or escape the system. As Agent Allison should well know, some of the most effective industry-tested forensic standard software *requires* a USB dongle (key) to remain plugged into the computer's USB port, in order to use the software. Indeed, this USB key was necessary and *required* for Allison to use the software he relied upon in his own work to forensically examine the evidence seized from Mr. Schwier's property. The very same software that produced results inconsistent with TD. Thus, had Agent Allison been subject to Mr. Walker's restrictions of only connecting to one network card port, even he could not have completed his own exam which alerted the defense of these inconsistent findings.

3. If Mr. Walker isn't aware that his arbitrary restrictions limit my work to only reproducing Mr. Erdely's "validation" procedures, then he simply hasn't done his homework or consulted with his own experts. This not only restricts me only to performing Mr. Erdely's "validation" procedures, but it doesn't even allow me to competently utilize the tools available to me to personally assure that no unintended data enters or exits the machine, as Mr. Walker himself claims to fear. I see no scientific or investigative value to utilizing precious resources repeating Mr. Erdely's "validation" here in California. On the contrary, I refuse to be associated with the propagation of "junk science", as dictated by an apparently biased actor, who clearly doesn't understand scientific method or computer security.

4. To a significant degree, the court relied on the government's [PROPOSED] ORDER GRANTING MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER filed on

November 18, 2019, which was little more than a superficial makeover of their prior proposal which only served to allow me to perform *their* proposed “validation”, and not my tests. It appears to me that the court was able to recognize that tests conducted under the government’s own prescribed “validation” procedures would effectively neutralize decades-old practices of independent review. The court’s current order seems to address *most* of those arbitrary government constraints.

5. In order to clearly articulate for the record why I am unable to effectively prepare counsel for trial with certain remaining restrictions, I will address my remaining concerns within Dkt. 254 line-by-line in the following paragraphs. Paragraph numbers in **bold** reference and correspond to the numbered paragraphs in the court’s order at Doc.254.

- a. **(Paragraph 6)** *Government personnel will have access to the TD Computer only for the purposes of starting the TD Computer, entering the password for the defense, and keeping the TD computer secure consistently with OCRFCL standard operating procedures. Government personnel will not observe the defense testing.*

Rather than relying on AUSA Walker’s self-serving interpretation of OCRCFL standard operating procedures, I would urge the court to compel Mr. Walker to produce text from the actual SOP upon which he claims to be relying. Based on his insertion of government personnel into a defense examination, I don’t believe he has even consulted the RCFL. I have personally utilized several RCFL facilities around the country. Contrary to Mr. Walker’s representation, it has been my experience that RCFL personnel have been instructed specifically *not* to interact with equipment used by the defense, specifically because doing so risks physically observing privileged work product, and can lead to accusations of government “snooping”.

In this particular case, Mr. Walker has *already* asked the OCRCFL’s Joseph

DECLARATION OF JEFFREY M. FISCHBACH

reb3

Monroe to provide details about my examination. Should Mr. Monroe, (or other RCFL staff) be in control and custody of the equipment containing my work product, they would be able to see my examination progress each time they have to log me back into the system (which happens every time I so much as leave to use a restroom), as well as hold exclusive possession of the password to access it while I am away, he (they) would most certainly be suspect, should my tests or the computer fail, or should the government appear to gain advanced knowledge of my testing results. While this may not have previously been as great a concern when Mr. Reardon was assigned to the case, it has been of particular concern given Mr. Walker's already proven proclivity to use RCFL staff, with no apparent justification, to provide information about my examination, communication, and consultation. While I do understand that the AUSA does have the power to use the RCFL in this way, I seriously doubt that it is the court's intention for him to continue do so.

**Any** government access to my tests and/or testing environment (hardware/software), including set-up, risks attorney-client privilege and work product, my ability to authenticate my own work, inserts the government into the defense chain-of-custody, and could invalidate my test results. A technically knowledgeable Agent can learn a lot simply from the hardware configuration and setup and the software I am using to perform the tests I need to conduct. The government has not justified how being granted sole password access to my tests, and physically opening the screen every time I need to use the computer, *in any way* serves to secure its software or equipment, (or serves to protect children,) when the equipment itself will already be in the *physical* custody of the government to begin with. Despite his knowledge of the stolen hard drive I reported to Mr. Monroe, Mr. Walker does not so much as specify any need or requirement for well-established forensic software/hardware measures that could be used to *actually* protect the equipment and data (including TD software) against being physically stolen or accessed from the RCFL.

DECLARATION OF JEFFREY M. FISCHBACH

reb4

With the physical restrictions pertaining to access to the government computer, noted below in Paragraph 9 of the court's order, which were imposed at the government's request, I can't even install and utilize these standard measures, let alone the software/equipment I need to perform my tests. All of which leads me to believe that either Mr. Walker is simply naive and has not done his homework, or that his real motivation is to thwart my examination of TD software and/or use it to prove that I have in some way violated a court order, so that he can either eliminate or damage my testimony in the defendant's case.

Moreover, in *no way* is any of this "consistent with OCRCFL standard operating procedures". This is blatant misrepresentation to the court. Mr. Walker himself provided me the password to the computer currently housed at the OCRCFL. Mr. Monroe, to my knowledge has had *no* access to this password or even touched the keyboard of that machine. This does, however, further justify the need for me to have complete, unfettered control over my equipment, including exclusive password control, not shared with the government, while conducting tests at the OCRCFL

*b. (Paragraph 7) Installation of Torrential Downpour software onto the TD Computer will occur as follows:*

*i. a. An FBI agent or Task Force Officer will keep exclusive possession of a USB drive or other removable media containing the Torrential Downpour software. The defense will not possess the Torrential Downpour software, other than on the TD Computer.*

I have consistently agreed that the RCFL should maintain custody of the TD installation disk provided to it. As Mr. Monroe himself has conceded, my own equipment which I was required to leave at the OCRCFL, was stolen from the OCRCFL's Defense Exam room, while I was not present, and while in the custody and control of the government. It would certainly be prudent to make sure that this software is kept secure. However, the tests that were ruled material *do* require testing and analysis of TD which *necessarily* requires that I

DECLARATION OF JEFFREY M. FISCHBACH

reb5

make multiple copies subjected to industry-tested software and hardware analysis. Therefore, while this can all occur within the confines of the OCRCFL, it simply cannot be completed, *in any way*, on a machine restricted in the way the government has outlined. Again, the government's proposed order simply allows for me to conduct Mr. Erdley's "validation" in California, without Det. Erdely's physical presence.

- ii. **b.** *Prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer, all while in the physical presence of the FBI agent or Task Force Officer. The FBI agent or Task Force Officer may observe Mr. Fischbach install the software.*

Mr. Walker has already reached-out to OCRCFL personnel to gain intelligence on my previous examinations and work. Since the passing of the Adam Walsh Act RCFL "Walsh Rooms" (Defense Exam rooms) have been treated as a "firewalled" environment where defense examiners can conduct their work without exposing privilege or work product. The government now seeks to breach this "firewall", which only serves to undermine operational practices that took years to establish. If the government's restrictions are upheld, it could undermine the trust and use of these facilities by defense examiners across the country.

Mr. Erdely's protocols included starting screen capture & monitoring software, as well as Wireshark, *before* the installation and initiation of his software. My time-tested industry-practiced methodology also requires the initiation of certain hardware and applications on each work-station prior to testing and examination, which would necessarily make the observing agent privy to attorney client privilege. At the same time, unless that agent or individual *is* well trained in computer forensics, it is unlikely that he/she would serve *any* value to the government in terms of securing its software. On the other hand, if this individual *is* technically-trained, then he/she serves an even greater value as an "information spy" for Mr. Walker, than in any way to actually secure software.

DECLARATION OF JEFFREY M. FISCHBACH

reb6



*c. After the installation, the FBI agent or Task Force Officer will remove the USB drive or other removable hardware from the TD Computer.*

The government should continue its now long-standing practice of having a *hands-off* policy when it comes to defense forensic examinations. As I have continued to offer, I would encourage the safe custody of the original software in government hands, and I would be willing to personally put it *in* the government's hands the moment I have completed my use of the installation files. More significant in this paragraph, however, is the government's continued use of the term "TD Computer". This further emphasizes that the government intends for me to operate *exactly* as Mr. Erdely's "validation" protocols specify -- not according to my own testing protocols, that this court has already ruled are material to the preparation of the defense in this case. This notion of a "TD Computer" is simply because Mr. Erdely's protocols specify one computer as "TD", and the other as "Suspect". As outlined previously in my redacted declaration, that is not my proposed operating procedure. And that *will not* allow me to complete the tests that have been found to be material in this case.

*d. (Paragraph 8) The defense may bring digital media, computers, cell phones, and an internet hotspot (i.e. one that is compatible to connect to the TD Computer via the network card) into the OCRCFL room with the TD Computer.*

Again, the government sees fit to dictate the defense examination environment, in order to restrict defense testing to its own "validation" protocols. In this case, however, the government is dictating an Internet connection method (Ethernet) that is currently unavailable on most Cellular 4G hotspots, and one that was not even an option on the WiFi hotspot that Mr. Erdely used for his own "validation". If a WiFi connection is unsuitable, or vulnerable, then it begs the question: why did Mr. Erdely use WiFi himself? I suspect that this government proposed requirement was made simply because it is well known that

there are very few “hotspots” for sale that have a wired Ethernet connection, and that those would be very costly for the defendant. For example, a simple search will show that the only Ethernet-equipped hotspot available from Verizon costs more than 4X as much as a comparable WiFi hotspot from Verizon. (\$649.99, compared to \$149.99.)

*e. (Paragraph 9) The TD Computer will contain one network card. The defense will not make any connections to the TD Computer other than through the network card. The TD Computer may access the internet through the network card.*

As stated above, the government seeks to narrow the defense testing and examination to its own “validation” procedures. In order to complete the tests that have been deemed material, I simply *must* have the ability to connect my own equipment, install my own industry-tested and accepted software and hardware, and to have the ability to remove my results for further examination and analysis. Otherwise, I *cannot* complete the testing that has been found material in this matter. In short, I need access to multiple computer ports and network connections to run my tests.

*f. (Paragraph 13) The defense will not tamper with or open the TD Computer.*

I understand and concur with the apparent *spirit* of this paragraph, I would for all of the reasons stated above, ask that the court impose the same admonition on the government. To that end, I had previously considered “tamperability” in my prior equipment specifications *estimate* that was provided to the government last week. Although a desktop machine is considered to be easier and less expensive to repair and upgrade, and has always remained my preferred platform for that reason, I would likely seek to use a laptop for my tests, because while retaining similar capabilities, they are significantly more difficult to alter, and much easier to identify any tampering that has occurred. For several reasons (which I can provide, if necessary, in a redacted document), including this, I tend to rely on Apple laptops, when an examination requires leaving equipment in government custody. At little-to-no added cost compared to similarly-

DECLARATION OF JEFFREY M. FISCHBACH

reb8

equipped desktop machines, I believe these safeguards serve to protect and authenticate chain-of-custody, work-product privilege, as well as *both parties* from any associated accusations.

6. I have been working with sensitive files for a quarter-century. Many of the procedures used by the FBI today were first used and instructed by *me*. So long as I have complete and unfettered access to properly determine and configure the equipment I use for these tests, I will take all the aggressive file containment protocols that I *always* use when examining sensitive material. This however, will necessarily require me to configure all equipment myself, and have access to add and remove all necessary software as my time-tested and industry-accepted protocols dictate, which means I will need access to more than one port on the government provided computer and more than one network connection. If I am allowed to do this I can safely *guarantee* the TD software will not be accidentally copied or distributed while under my control. Should I be required to use the computer as dictated by the government, without the ability to install or connect any previously tested and industry accepted software (much of which is specifically designed to protect data from any unintended use) and hardware to *any* port or connector on the computer, as needed, then not only can I not complete my tests, I would not be able to assure the court that all standard precautions had been taken. Given the necessary access I need on the testing equipment provided by the government, I will take all necessary software and hardware precautions to restrict copy or dissemination of TD, and to secure my forensic work environment, as has been my standard practice for 25 years.

7. The foregoing statements true and correct to the best of my knowledge, and I hereby reserve the right to amend them should additional information be made available to me at a later date.

///

///

DECLARATION OF JEFFREY M. FISCHBACH

reb9

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on November 25, 2019.



---

Jeffrey M. Fischbach

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
431 W.7th Avenue, Suite 107  
Anchorage, Alaska 99501  
907-277-7171 Phone  
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

United States of America, )  
 )  
 )  
 Plaintiff, ) Case No. 3:17-cr-0095 SLG-DMS  
 )  
 vs. )  
 )  
 Matthew Schwier, )  
 )  
 Defendant. )  
 )  
 )  
 \_\_\_\_\_ )

**SUPPLEMENTAL DECLARATION OF JEFFREY M. FISCHBACH  
SUPPLEMENTING DOC. 296**

I, Jeffrey M. Fischbach, declare as follows:

1. This declaration is written to supplement my declaration at Dkt. 296-1 responding to the government’s Dkt 288, “Notice Regarding Proposed Testing Environment”, and 288-1, “Test Environment Regarding Torrential Downpour”.
2. It should be noted that the government’s entire concern over TD, as well as TD’s secret feature being released into the “wild” has been rendered entirely without merit and perhaps disingenuous by its own repeated missteps. As noted previously, the government already

DECLARATION OF JEFFREY M. FISCHBACH

reb1

accidentally exposed its secret feature to me during its demonstration on October 17 and 18, 2019. Without prompting or obligation, *I* alerted *both* the government and the court that this occurred, and volunteered to bound by a verbal nondisclosure agreement, sworn before the court. Had I not volunteered this information, the government would have had no idea that this secret, which the government has described as being critical to its ability to work undercover, without detection, had been exposed to me. I have been trusted since then to observe the oath I *volunteered* to the court. The government has now, once again, accidentally provided me something it claims I cannot be trusted to keep safe. Before settling on a protective order, the government has unintentionally provided me with two working copies of TD, to which I have had unmonitored access for more than two weeks.

3. On December 6, 2019 I traveled to the Orange County RCFL for the purposes of initiating several searches in preparation for trial, and to examine the thumb drive sent by the government containing copies of the Virtual Machines (VM) preserving Mr. Erdely's TD validation, performed in my and Atty. Herz's presence, in Anchorage on November 4, 2019. Shortly after arriving at the OCRCFL, my liaison, Joseph Monroe provided to me the aforementioned thumb drive for use on the government-supplied Mac that I have been using to conduct my Anchorage and Orange County examinations. Upon receiving the thumb drive I informed Mr. Monroe that I would like to copy its contents to the aforementioned government computer, so that I can return the thumb drive to his custody, as not to leave it exposed in a shared civilian exam room. As well, VM's typically do not run well, if at all, on external media. Mr. Monroe agreed, so long as it stayed on that computer, as stipulated.

4. Some time later that afternoon, Mr. Monroe re-entered the defense examination room, and informed me that he had received communication from AUSA Jonas Walker, asking him to remind me that I was not to remove anything from that thumb drive from the OCRCFL. I agreed, and reminded him that I had copied its contents to the government's computer, which he acknowledged. AUSA Walker also memorialized this notice in an email on that date at 2:37PM.

5. A short time later, Mr. Monroe again entered the defense examination room and asked if I

had already begun working with the data from the thumb drive. I let him know that I had, but that I also had been having some trouble with errors attributed to an older model computer. Mr. Monroe then informed me that Mr. Walker believed that there may be copies of TD on the thumb drive he supplied, and reminded me that I was not to copy it. I again reminded him that I had already copied the contents of the thumb drive to the government's computer, to remain in RCFL control and custody. He acknowledged that.

6. I left the OCRCFL two different times that day, since having been provided copies of TD. Each time, I left without any search of my property, as is expected when exiting an RCFL facility. (Upon my final exit for the day, Mr. Monroe simply waved from behind glass, and asked if I had anything still running on the computer.) As usual, I had in my possession a laptop, a tablet, a smartphone, and several pieces of removable media which I typically carry in my computer bag. Any one of which could have been used to remove TD from the OCRCFL. Even if I did not already have those storage devices with me, there is a BestBuy directly across the street from the OCRCFL, where I could purchase one. I left the OCRCFL for a lunch break, lasting at least an hour. Plenty of time to purchase removable media.

7. *If* I had nefarious intentions, TD would have *already* been “in the wild” for the past two weeks. I am unsure when Mr. Walker realized that he accidentally sent me two copies of TD, but I presume it was sometime between at least November 19, and December 6, 2019 -- and not likely coincidental with my arrival at the OCRCFL. However, upon realizing that TD was already in my possession, Mr. Walker simply admonished me, via Mr. Monroe, that I was not to remove it from the RCFL, and then trusted me not to. At the October 17-18 and November 26th hearings in Anchorage, it was conveyed to the court that putting TD in my possession is considered to be “in the wild”. However, even after realizing that TD had already been released to “the wild”, Mr. Walker allowed me unmonitored access to it. At any time, had Mr. Monroe told me that I would not be able to continue my examination due to the accidental release of TD, I would have complied. Instead, I was allowed by the USA to continue my work until standard OCRCFL closing hours, and leave the facility twice -- all the while trusting that I would not remove a copy of TD, or possibly trusting that I was aware of potential consequences

of doing so. Which I am.

8. Simply put, *if* I cannot be trusted with Torrential Downpour, or its secret feature, then both have *already* been irrevocably compromised and released to the wild. And, *nothing* in the government's latest, or even prior proposals will ever get it back. Having earned the respect, not only of defense attorneys, prosecutors, judges, and the media, as well as my entire income for the last quarter century, it is counter intuitive that someone in my position would simply compromise my status for the purposes of aiding criminal behavior. If anything, at least as much as the AUSA and any member of law enforcement, I earn my living *because* individuals are arrested, not because they are empowered to get away with crime. I have every reason, and even several additional legal reasons to keep this software from being compromised. While Mr. Erdely can accidentally reveal a secret TD feature, and Mr. Walker can accidentally release two copies of the software, I would likely be held in contempt of court, at the least, and possibly risk much more. For this reason alone, the government's clear, and demonstrated attempts to thoroughly monitor and collect evidence on me and my examination for the purposes of exposing the breach of a Protective Order, give me pause to consider whether assisting in the defense of one individual may not be worth risking my own career and freedom. I would suspect, given the impositions the government has proposed, very few if any individuals in my position would accept the case.

9. Despite the government's failure to secure its own software and secrets, I have gone to great lengths, both to voluntarily alert the government and the court about information which they accidentally provided to me, as well as to attempt to use equipment owned by the government, at facilities run by the government, and to utilize very expensive specialized hardware and software at my disposal to further reduce the risk of accidental dissemination. To wit, I suggested the use of the LA SCIF, when it was demonstrated to me that the OCRCFL does not physically guarantee the security of equipment and data left in its shared defense exam room.

/ / /

/ / /

DECLARATION OF JEFFREY M. FISCHBACH

reb4



I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on January 6, 2020.



---

Jeffrey M. Fischbach

1 **Storrs Law Firm, PLLC**  
2 Zachary Storrs  
3 Arizona State Bar No. 025780  
4 1641 E. Osborn Rd. Ste 8  
5 Phoenix, AZ 85016-7146  
6 Telephone (480) 231-0126  
7 Facsimile (602) 955-4701  
8 [Zstorrs@hotmail.com](mailto:Zstorrs@hotmail.com)

9 *Attorney for Defendant*

10  
11 **IN THE UNITED STATES DISTRICT COURT**  
12 **DISTRICT OF ARIZONA**

13 United States of America,

14 Plaintiff,

15 vs.

16 Anthony Espinosa Gonzales,

17 Defendant.

18 Case No. CR-17-01311-PHX-DGC

19 **DEFENDANT’S MOTION TO  
20 COMPEL ADDITIONAL DISCOVERY  
21 AND NOTICE OF FILING OF  
22 TORRENTIAL DOWNPOUR  
23 VERSION 1.33 TESTING AND  
24 ANALYSIS**

25 *(Evidentiary Hearing Requested)*

26 Comes now Defendant, Anthony Espinosa Gonzales, by and through undersigned  
27 counsel, pursuant to **Brady v. Maryland**, Rule 16 of the Federal Rules of Criminal  
28 Procedure, and the Due Process Clause of the 5<sup>th</sup> Amendment to the United States  
Constitution and requests that this Court enter an additional order to compel the  
Government to disclose additional discovery, including all previously requested  
discovery relating to the law enforcement Computer program “Torrential Downpour”  
utilized by investigators in this matter. This motion incorporates by reference pleadings,

1 allegations, and argument previously presented in this matter. This motion is further  
2 supported by the following Memorandum of Points and Authorities.

## 3 4 **MEMORANDUM OF POINTS AND AUTHORITIES**

### 5 6 **Introduction**

7  
8 Mr. Gonzales requests that this Court order additional testing of the software  
9 relevant to this matter, to include programs Torrential Downpour, Torrential Downpour  
10 Receptor, and ICAC COPS. Specifically, Mr. Gonzales moves that this Court issue its  
11 Order directing that (1) further testing of the software be granted to the defense; (2)  
12 ICAC COPS be included in that testing; (3) additional source computers be included in  
13 that testing; and (4) industry standard testing be conducted on this suite of software by a  
14 qualified software testing company.  
15

16  
17 In support, Mr. Gonzales offers as **Exhibit A** to this pleading, the Torrential  
18 Downpour Version 1.33 Testing and Analysis report generated by Loehrs Forensics. The  
19 report results from an initial round of data retrieval and examination conducted in  
20 October of 2019 and is based upon the Court's Order entered on August 27, 2019 (**Doc.**  
21 **86**).  
22

### 23 24 **Facts**

25  
26 The truth and accuracy of the Government's claim that its software conducts a  
27 single source download, to include ICAC COPS, is absolutely material to the defense.  
28 The Government has acknowledged that the entirety of the evidence on the eight

1 distribution charges is comprised of the logs of its own software stating that the child  
2 pornography was downloaded from Mr. Gonzalez's computer. On January 31, 2019, the  
3 following exchange took place between this Court and AUSA Helart:

4  
5 The Court: The distribution charged in each of these counts [Counts  
6 One through Eight] is the sharing of the video from  
7 defendant's computer to the Government's computer. That  
8 is the act of distribution that's charged; correct?

9 Ms. Helart: That is correct.

10 The Court: It's not distribution with anybody else, it's that distribution.

11 Ms. Helart: Correct. Yes.

12 **RT 1/31/19**, p. 141, l. 23 to p. 142, l. 4.

13 Later in the hearing, there was discussion about the limitation of the Government's  
14 evidence:

15 The Court: Yeah. But, again, the only evidence you have that that video  
16 that you will be showing the jury came from the defendant's  
17 computer is what Torrential Downpour and its logs tell you.

18 Ms. Helart: It is true.

19  
20 **RT 1/31/19**, p. 143, lls. 18-22.

21  
22 On, June 28, 2018, the defense filed a Motion to Compel Discovery; Preclude  
23 Certain Evidence. Following the Government's Response, an Evidentiary Hearing was  
24 held on August 16, 2019. The defense proposed conducting nine tests of the software. In  
25 the Court's Order, filed on August 27, 2019, tests one and two were deemed unnecessary  
26 because the Government conceded that the Torrential Downpour software program will  
27 identify non-parsed and partially-parsed torrents of investigative interest. [Doc. 86]. The  
28

1 Court granted Mr. Gonzales' request to conduct proposed tests three and four, however  
2 without the inclusion of ICAC COPS. The Court denied the request for tests four and  
3 five. Tests seven, eight, and nine were ordered without objection from the Government.  
4 The Court also granted a request to present a supplemental brief. The defense asserts that  
5 the tests conducted pursuant to the Court's order entered on August 27, 2019, provide  
6 direct evidence and support that the issues raised are material to the preparation of a  
7 defense, provide evidence that there is a 4<sup>th</sup> Amendment issue that must be addressed, and  
8 demonstrate that further testing is necessary to protect Mr. Gonzales' constitutional  
9 rights. A description of some of the tests conducted demonstrates some of the reasons  
10 that further testing is required.

11  
12  
13  
14 The defense respectfully underscores that the results of live testing and forensic  
15 analysis of the Torrential Downpour software has revealed two important realities. First,  
16 contrary to the Government's repeated claims, Torrential Downpour may identify data  
17 that exists outside of shared space to include deleted data. Second, the Government  
18 cannot rely on log files alone because Torrential Downpour may falsely report that a user  
19 possesses data that has been deleted.

#### 20 21 22 **Test VII: Single Source Download**

23 Pursuant to Section VI of the report, "the seventh test determines the accuracy of  
24 Torrential Downpour limiting downloads to a sole IP address against the BitTorrent  
25 protocol." The Single Source Download test was designed to determine Torrential  
26 Downpour's accuracy in limiting downloads to a sole IP address against the BitTorrent  
27 protocol. This is significant because it assures law enforcement that the entirety of the  
28

1 illegal files came from one suspect, as opposed to incomplete pieces from multiple  
2 suspects, as the BitTorrent protocol is designed and instructed to operate by default. The  
3 specific goal of the test is to determine whether Torrential Downpour will obtain files  
4 from other sources during the course of an investigation. However, during the testing the  
5 Government manually instructed Torrential Downpour to connect to a single IP address.  
6 The software did not run natively in an automated state, nor was it used to investigate  
7 suspects concurrently. In other words, the test did not allow the software to fail. This  
8 would be analogous to testing the safety features of a car without conducting a controlled  
9 car crash. Therefore, this test is incomplete and inconclusive.

10  
11  
12 The single source download test of Torrential Downpour was conducted to  
13 determine if the program limits “downloads to a sole IP address against the BitTorrent  
14 protocol.” (**Exhibit A**, p. 4). More directly, “the question is whether Torrential  
15 Downpour will obtain files from other sources when it is unable to conduct a single  
16 source download.” (**Id.**). The test is ultimately meaningless in regard to the actual  
17 functionality of the program as it is used by law enforcement.

## 20 **Argument**

21  
22 The Court found Torrential Downpour material to the defense under Rule  
23 16(a)(1)(E(i)). (Court’s Order, Doc. 86). Nothing could be more material to Mr.  
24 Gonzales’ defense. Again, the logs compose the entirety of the evidence for the  
25 distribution charges. Testing demonstrates that those logs are flawed. As noted in the  
26 Court’s Order: “Evidence is ‘material’ under Rule 16 if it is helpful to the development  
27  
28

1 of a possible defense” **United States v. Budziak**, 697 F.3d 1105, 111 (9<sup>th</sup> Cir. 2012).  
2 Due process requires additional testing. It is fundamentally unfair to ask a defendant to  
3 defend against allegations that are entirely based upon flawed logs without allowing that  
4 defendant to ascertain the extent to which those logs are flawed and how those flaws may  
5 have affected the only evidence presented against him. To prevent a defendant from  
6 doing so is to effectively prevent him from confronting his accuser.  
7

8  
9 The Defendant here wishes to address three primary issues related to these  
10 findings. First, the Government conceded that Torrential Downpour will identify  
11 suspects in child pornography investigations who have no illegal content per the Non-  
12 Parsed Torrent and Partially Parsed Torrents tests. Because of this, and because the  
13 associated torrents and files identified by Torrential Downpour during the FBI  
14 investigation were not located on Mr. Gonzales’ computer, the defense has evidence that  
15 Mr. Gonzales could have been improperly identified by Torrential Downpour when he  
16 did not possess any illegal content.  
17  
18

19 Second, the testing revealed Torrential Downpour will identify suspects as  
20 possessing child pornography for data that has been deleted and unshared. This result,  
21 combined with the fact that the associated torrents and files identified by Torrential  
22 Downpour during the FBI investigation were not located on Mr. Gonzales’ computer,  
23 demonstrates that Mr. Gonzales could have been inappropriately identified by Torrential  
24 Downpour when he did not publicly share any illegal content. It is anticipated that the  
25 Government will argue the difference in Mr. Gonzales’ case is that Torrential Downpour  
26  
27  
28

1 reported downloading data whereas the testing only identified the suspect and could not  
2 download any content. This raises the third issue.

3 Third, the testing was largely inconclusive due to the limitations imposed on  
4 testing the single source download feature of Torrential Downpour. There are essentially  
5 two steps in an investigation using Torrential Downpour: the identification of a suspect  
6 possessing suspected child pornography and downloading data from the suspect as  
7 distribution of child pornography. In this case, Torrential Downpour first identified Mr.  
8 Gonzales as a suspect possessing child pornography. The testing revealed Torrential  
9 Downpour can and will falsely identify suspects as possessing suspected child  
10 pornography that is deleted and unshared. Next, Torrential Downpour allegedly  
11 downloaded illegal material from Mr. Gonzales' IP address. The testing did not allow  
12 Torrential Downpour to connect to multiple suspects and, therefore, the testing could not  
13 determine the possibility that data could have been downloaded from a source other than  
14 Mr. Gonzales during the investigation in this case. There are two logical explanations:  
15 the data was present in shared space when downloaded or it came from somewhere else.  
16 If the data was not on the computer, it must have been downloaded from ICAC COPS or  
17 from other users being monitored. Therefore, the Torrential Downpour logs relied upon  
18 by the Government as evidence that Mr. Gonzales possessed and distributed suspected  
19 child pornography are, in fact, unreliable.  
20  
21  
22  
23  
24

25 Because none of the suspect files that were charged in Counts 1-8 were found on  
26 Mr. Gonzales' computer, there is no forensic evidence to corroborate claims presented by  
27 the Government. If the software performed as described by the Government, the files  
28



1 must certainly have been downloaded to the shared file, distributed during the undercover  
2 investigation, and deleted at some time between the undercover investigation and the date  
3 of seizure. However, if the software does not work as the Government has described, one  
4 of several possible scenarios must have occurred. The testing described in the report that  
5 constitutes **Exhibit A** addresses these scenarios.  
6

7         An imperfect, but, nevertheless, instructive analogy is to consider a scenario in  
8 which a defendant is charged driving under the influence of alcohol where the blood  
9 alcohol analysis constitutes the only evidence against the defendant. A forensic analysis  
10 of Mr. Gonzales' computer revealed none of the materials that constitute the distribution  
11 charges. This is analogous to a driver who presents no poor driving, no smell of alcohol,  
12 no slurred speech, and no other indications of alcohol ingestion. In addition, the results  
13 of the forensic analysis of the computer is also analogous to a driver who has taken and  
14 passed all field sobriety tests and who has given no indication of being inebriated. If the  
15 sole evidence against this defendant is the result of the blood analysis, nothing can be any  
16 more material to the defense than the reliability of that analysis. If that defendant  
17 develops evidence that the blood analysis is flawed in a way that might directly affect the  
18 analysis of her blood, but is not permitted to seek out and present that evidence, then that  
19 defendant can present no meaningful defense at all.  
20  
21  
22  
23

24         Here, there is demonstrable evidence that the Torrential Downpour logs are  
25 unreliable when describing exactly the type of information which forms the basis of the  
26 charges against Mr. Gonzales. One difference between the scenarios is that there would  
27 be no probable cause for a traffic stop or for further testing in the DUI example, whereas,  
28

1 here, the Government is able to conduct the download without probable cause because  
2 the data that they seek is presumed to be in shared space. Another distinction involves  
3 the novelty and complexity of the subject matter. In a DUI case, jurors typically have  
4 knowledge of alcohol use and real world experience that would be likely to make them  
5 understand the issues and question the lack of evidence of alcohol consumption in  
6 comparison to the alcohol analysis. Conversely, jurors likely would not have relevant  
7 knowledge or experience in a trial involving complex issues surrounding a network with  
8 which they are unlikely to have any experience and a government software program with  
9 which they will necessarily have none.  
10  
11

### 12 **Amendment of Prior Arguments**

13  
14 In order to provide proper context, Mr. Gonzales seeks to review and underscore  
15 certain positions previously advanced by both the defense and by the Government. The  
16 defense asserted in its first motion that it had reason to believe that the Government  
17 software used here accesses data beyond the public domain. (**Doc. 25**, p. 6). The Court  
18 has previously established that the log files the Government intends to use in this case are  
19 generated in their entirety by Torrential Downpour. Furthermore, the Government has  
20 repeatedly avowed that the evidence that Torrential Downpour captures is solely within  
21 the public domain.  
22  
23

24  
25 In its Response the Government alleged as follows: "It is important to note that  
26 Torrential Downpour obtains *only* what is being offered *to the public* on the BitTorrent  
27  
28

1 network." (*Emphasis added*). (**Doc. 29**, p. 9, l. 4). Further, at the evidentiary hearing  
2 held January 31, 2019, the following exchange was held regarding the log files:

3 The Court: But they are 100 percent a product of  
4 Torrential Downpour.

5 Ms. Helart: They're generated by Torrential Downpour.

6 The Court: They purport to show what Torrential Downpour  
7 was doing.

8 Ms. Helart: It's what Torrential Downpour captured  
9 *in the public space*.

10 **RT 1/31/2019**, p. 145, ls. 11-18. (*Emphasis added*).

11  
12 The Government's witness at the August 16, 2019 hearing, testified similarly: "Detective  
13 Erdely testified that Torrential Downpour never obtains any unshared information from  
14 any computer running BitTorrent compatible software; rather, the Torrential Downpour  
15 law enforcement software searches the .torrent download candidates the same that any  
16 public user of the BitTorrent network searches and 'only searches for information that a  
17 user has already made public by the very use of the [uTorrent] software.'" (**RT 8/16/19** at  
18 p. 42). Detective Erdely further explained that due to the BitTorrent software's matching  
19 of SHA-1 hash values of downloaded pieces "*it would be absolutely impossible to*  
20 *randomly download files from a suspect's computer which are from unshared folders.*"  
21 (Government's Response, **Doc. 29**, p. 9, l. 25 to p. 10, l. 8, (*Emphasis added*)).

22  
23  
24  
25 The defense asserts that the Government universally claims that this software  
26 cannot possibly access unshared folders. In fact, at the evidentiary hearing held on  
27 August 16, 2019, this Court inquired of the defense if it had any evidence that Torrential  
28

1 Downpour accessed data in the defendant's computer that is beyond the shared space or  
2 public domain. The defense responded that it did not have evidence at that time. The  
3 testing conducted by Loehrs Forensics changes this entirely. The data collection and  
4 analysis conducted thus far provides clear evidence that this claim by the Government is  
5 false.  
6

7 This is a hugely important point for several reasons. The first reason is that Mr.  
8 Gonzales and defendants in other cases have previously asserted that the Government  
9 software does not function as the Government claims. (*See Doc. 25*, Motion to Compel  
10 Discovery; Preclude Certain Evidence). One example of Government claims regarding  
11 access to unshared folders is evidenced by an ROI generated by an agent in attendance at  
12 the data collection conducted in this case in October of 2019, but not disclosed to the  
13 defense in this case. An ROI was made a part of the record in a case in the United States  
14 District Court of Alaska: *United States v. Matthew William Schweir*. **Exhibit B** (Case  
15 3:17-cr-00095-SLG, Document 221-1, 10/16/19). The ROI was used by the Government  
16 in Alaska and elsewhere to assert, not that the software executed the tasks instructed  
17 within the parameters of the testing protocol, which is all it could claim since analysis  
18 had not yet even begun, but that it functioned as the Government has claimed it functions.  
19 These are two very different things. The ROI makes it clear that a distinction can be  
20 drawn. This distinction has, however, in some cases, been lost. In this case, the  
21 Government has chosen to not only not disclose to the defense this ROI, but has not  
22 attempted to make this assertion. The Government cannot successfully make this claim  
23 here, as the defense was present at testing.  
24  
25  
26  
27  
28

1 The Government has zealously fought against disclosing information about its  
2 software. However, the Government may not misrepresent the function of the software  
3 under scrutiny in order to prevent the Court from granting the defense access to that  
4 which it should be entitled based upon Mr. Gonzales' constitutional rights. While the  
5 Government may claim to be making these allegations based upon what the software  
6 owner asserts, the Government is now on notice that, if that is the case, the owner's  
7 assertions may not be trusted.  
8

9  
10 Based upon the testing and validation of the Torrential Downpour software to  
11 date, it is apparent that the software will identify files on a suspect's computer that have  
12 been deleted or moved into non-shared locations. Further, the log files created by  
13 Torrential Downpour will falsely indicate that the user still has the files in spite of those  
14 files being deleted or unshared. This is material to Mr. Gonzales' case because the files  
15 were not found on his computer and the Government relied only on the Torrential  
16 Downpour logs that, based upon testing, may have been false.  
17

18  
19 Although Torrential Downpour was unable to download any deleted and  
20 unshared files from the suspect computer during testing, two critical elements were  
21 omitted from the test, (i) Torrential Downpour's ability to obtain the files from other  
22 sources pursuant to the BitTorrent protocol, and (ii) Torrential Downpour's ability to  
23 obtain the files from the ICAC COPS database. It is imperative that these two elements  
24 are included in the testing and validation of the Torrential Downpour software to  
25 determine whether Torrential Downpour falsely identified Mr. Gonzales as having  
26 those files not found on his computer and whether Torrential Downpour obtained those  
27  
28

1 files from some other source, such as other users, ICAC COPS, or both. These issues  
2 remain relevant even in the scenario in which a detective manually directs the software.  
3

### 4 **Additional Evidence Regarding Single Source Download**

5 The theory of the Government's case and the sole evidence supporting the  
6 distribution charges. Because of these facts, the Government must prove that, indeed,  
7 their computer did not receive the charged items from any other source than defendant's  
8 computer. The BitTorrent network normally functions by use of multi-source downloads  
9 and the Government claims that its software modifies this, guaranteeing that its software  
10 only downloads from a single source. Its proof is nothing more than the logs of its own  
11 software. In order to adequately defend against these claims, it is absolutely material and  
12 essential to the defense to thoroughly test this software utilizing the entire suite of  
13 software to include ICAC COPS.  
14  
15  
16

17 Now that initial data gathering has been conducted, the defense can demonstrate  
18 that at least two additional tests must be conducted to determine whether the  
19 Government's assertion of a single source download is, in fact, accurate.  
20

21 First, because the structure of the data collection utilized only one suspect  
22 computer, determination of single-source downloading cannot be confirmed. In other  
23 words, one additional factor must be included in additional testing: the use of other  
24 computers that possess and share parts of the file to confirm that Torrential Downpour  
25 *cannot* obtain files from other computers. This fact is absolutely material to the defense  
26 of this case.  
27  
28

1 Second, ICAC COPS is likewise material to further testing. Statements made by  
2 Government experts in court support the claim that it is a suite of software rather than  
3 independent working parts.  
4

### 5 **Disclosure of ICAC COPS is Required Pursuant to Rule 16**

6 The Government has repeatedly claimed that ICAC COPS and Torrential  
7 Downpour operate independently for purposes of Torrential Downpour's connection to  
8 the suspect computer and it is, therefore, unnecessary to explore and immaterial to the  
9 defense. For instance, this exchange between the Court and Mr. Erdley:  
10

11 The Court: When the Torrential Downpour program takes those three  
12 pieces of information and goes out to a computer and  
13 communicates and attempts to download child  
14 pornography, is COPS doing anything in that process.

15 Mr. Erdley: No. Nothing.

16 **RT 8/16/19** at p. 42.

17 The data analysis conducted demonstrates that this is not accurate. The data  
18 analysis performed to date verifies that ICAC COPS is an integral and essential  
19 component of the software and must be included in testing in order to satisfy industry  
20 standards regarding function and accuracy. From the Loehrs Report:  
21

22 ... [U]pon learning that references to the ICAC COPS database is contained within  
23 actual system files of the software, it is reasonable to assume that it must also be  
24 contained within the source code. If this is true, it would be fundamental to the  
25 testing process to analyze the source code to determine the importance of the  
26 ICAC COPS database as it relates to the overall functionality of the Torrential  
27 Downpour software. For example, if Torrential Downpour is unable to obtain a  
28 file from the suspect, ICAC COPS could potentially intervene to obtain the file  
from its own database or send instructions to the Torrential Downpour software to  
obtain the file from other IP addresses.

**Exhibit A, p. 7**

1 This specifically addresses the issue of why Agent Daniels may direct Torrential  
2 Downpour to one IP address, but it could nevertheless seek the data elsewhere. As an  
3 example, ICAC COPS could instruct Torrential Downpour to access other computers to  
4 obtain the illegal parts of the torrent. If Torrential Downpour locates only the hash value  
5 of an illegal file, but not the file itself, ICAC COPS could obtain those illegal files from  
6 its own database. These possibilities must be considered in light of the fact that none of  
7 the files charged in Counts 1 through 8 were found on Mr. Gonzales' computer.  
8

9 Gerhard Goodyear, who worked with Mr. Erdley on development of this software,  
10 has testified that the parts of this suite cannot be properly tested separately. (*See* 8/16/19  
11 RT at p. 44 and **Doc. 81-2**.) Agent Daniels, the Government expert in this case, also  
12 testified in *United States v. Douglas Allen Jones*, (Case 2:18-cr-08040-SMB) on  
13 November 26, 2019 as follows:  
14

15 Q. So Torrential Downpour, in order to launch the investigation  
16 you're talking about, it has to interact with this ICAC COPS  
17 database to learn about these leads?

18 A. Only briefly. It's -- it's not doing the search function itself, but it's  
19 just gathering information from the database.

20 Q. Without the information from the database, you can't really  
21 conduct your investigation. Fair to say?

22 A. Um, for Torrential Downpour, yes.

23 District Court of Arizona. Case 2:18-cr-08040-SMB.

## 24 **Torrential Downpour Receptor**

25 Finally, because Torrential Downpour Receptor has only recently been revealed  
26 by the Government's experts as working in conjunction with ICAC COPS and Torrential  
27 Downpour. It has not been tested for accuracy. The defense is unaware whether  
28



1 Torrential Downpour Receptor works in the same or similar way as Torrential  
2 Downpour. Mr. Gonzales submits that Torrential Downpour Receptor logs are, likewise,  
3 material to the defense, as it is part of the suite of software used in this case.  
4

5 Wherefore, Mr. Gonzales moves that this court issue its Order directing that (1)  
6 further testing of the software be granted to the defense; (2) ICAC COPS be included in  
7 that testing; (3) additional source computers be included in that testing; and (4) industry  
8 standard testing be conducted on this suite of software by a software testing facility  
9 chosen by the defense.  
10

### 11 **Conclusion**

12  
13 For the reasons stated in this motion, Mr. Gonzales requests that this Court order  
14 the additional software testing requested.  
15

16  
17  
18 RESPECTFULLY SUBMITTED this 1<sup>st</sup> day of May, 2020.  
19

20 /s Zachary Storrs  
21 Attorney for Defendant  
22  
23  
24  
25  
26  
27  
28

**CERTIFICATE OF SERVICE**

I hereby certify that on May 1, 2020, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF system for filing and transmittal of a Notice of Electronic Filing to the following CM/ECF registrants:

Hon. David G. Campbell  
United States Senior District Judge  
401 West Washington Street  
Phoenix, AZ 85003  
[Campbell\\_Chambers@azd.uscourts.gov](mailto:Campbell_Chambers@azd.uscourts.gov)

Gayle L. Helart  
Assistant United States Attorney  
Two Renaissance Square  
40 N. Central Avenue, Suite 1200  
Phoenix, Arizona 85004-4408  
[Gayle.Helart@usdoj.gov](mailto:Gayle.Helart@usdoj.gov)

Brett A. Day  
Assistant United States Attorney  
Two Renaissance Square  
40 N. Central Avenue, Suite 1200  
Phoenix, Arizona 85004-4408  
[Brett.Day@usdoj.gov](mailto:Brett.Day@usdoj.gov)

By:/s Zachary Storrs

1 **WO**

2

3

4

5

6

**IN THE UNITED STATES DISTRICT COURT**

7

**FOR THE DISTRICT OF ARIZONA**

8

9 United States of America,

No. CR-17-01311-001-PHX-DGC

10

Plaintiff,

11

v.

12

Anthony Espinoza Gonzales,

13

Defendant.

14

15 United States of America,

No. CR-18-00539-001-PHX-DGC

16

Plaintiff,

17

v.

**ORDER**

18

Aaron Anthony Ordonez,

19

Defendant.

20

21

22

Defendants Anthony Espinosa Gonzales and Aaron Ordonez are charged in two separate cases with distributing and possessing child pornography in violation of 18 U.S.C. § 2252(a). Each has filed a motion to compel disclosure of the Torrential Downpour software program used by the FBI in the investigation that led to his indictment. Doc. 25, Case No. CR-17-01311; Doc. 32, Case No. CR-18-00539. Both motions are fully briefed, and the Court held a joint evidentiary hearing on January 31, 2019. Computer forensics expert Tami Loehrs testified on behalf of Defendant Gonzalez,

23

24

25

26

27

28

1 and FBI Agent Jimmie Daniels testified for the government. The Court will grant  
2 Defendant Gonzalez's motion in part and deny it in part, and will deny Defendant  
3 Ordonez's motion.

4 **I. Background.**

5 **A. The BitTorrent Network and Torrential Downpour.**

6 The indictments in these cases allege that Defendants downloaded and shared  
7 child pornography files using the BitTorrent file-sharing network. BitTorrent is an online  
8 peer-to-peer network that allows users to download files containing large amounts of  
9 data, such as movies, videos, and music. Instead of relying on a single server to provide  
10 an entire file directly to another computer, which can cause slow download speeds,  
11 BitTorrent users can download portions of the file from numerous other BitTorrent users  
12 simultaneously, resulting in faster download speeds.

13 To download and share files over the BitTorrent network, a user must install a  
14 BitTorrent software "client" on his computer and download a "torrent" from a torrent-  
15 search website. A torrent is a text-file containing instructions on how to find, download,  
16 and assemble the pieces of the image or video files the user wishes to view. The client  
17 software reads the instructions in the torrent, finds the pieces of the target file from other  
18 BitTorrent users who have the same torrent, and downloads and assembles the pieces,  
19 producing a complete file. The client software also makes the file accessible to the other  
20 BitTorrent users in a shared folder on the user's computer.

21 Torrential Downpour is law enforcement's modified version of the BitTorrent  
22 protocol. Torrential Downpour acts as a BitTorrent user and searches the internet for  
23 internet protocol ("IP") addresses offering torrents containing known child pornography  
24 files. When such an IP address is found, the program connects to that address and  
25 attempts to download the child pornography. The program generates detailed logs of the  
26 activity and communications between the program and the IP address. Unlike traditional  
27 BitTorrent programs, the government claims that Torrential Downpour downloads files  
28 only from a single IP address – rather than downloading pieces of files from multiple

1 addresses – and does not share those files with other BitTorrent users.

2 **B. The Investigations into Defendants’ BitTorrent Activity.**

3 **1. Defendant Gonzales.**

4 In December 2016, Agent Daniels used Torrential Downpour to identify IP  
5 address 24.255.44.200, which allegedly was making known child pornography files  
6 available on the BitTorrent network. Agent Daniels testified that he used Torrential  
7 Downpour to connect with this IP address and download child pornography video files on  
8 eight occasions between December 13, 2016 and January 9, 2017. He reviewed the  
9 Torrential Downpour activity logs to confirm that the program downloaded complete  
10 files solely from this IP address, and reviewed the video files to confirm that they were  
11 child pornography.

12 Through further investigation, Agent Daniels learned the subscriber information  
13 for the IP address. He obtained a search warrant for the subscriber’s residence, and FBI  
14 agents searched the residence on February 8, 2017. They found a Microsoft tablet and  
15 other computer equipment. Gonzales, who lived there with his parents and siblings,  
16 stated during an interview that he had used a tablet to find and view child pornography.  
17 Forensic examinations performed by the FBI and Loehrs revealed child pornography files  
18 on the tablet, but the video files that Torrential Downpour allegedly had downloaded  
19 from the IP address were not found on the tablet or any other seized device.

20 On October 4, 2017, the government charged Gonzales with eight counts of  
21 distributing child pornography and one count of possessing such material. Doc. 6.  
22 The eight distribution counts are based on the video files that Torrential Downpour  
23 allegedly downloaded between December 13, 2016 and January 9, 2017. *Id.* at 1-5. The  
24 possession count is based on the child pornography found on the tablet after the search.  
25 *Id.* at 5-7.

26 **2. Defendant Ordonez.**

27 Agent Daniels conducted a similar investigation into Defendant Ordonez’s  
28 BitTorrent activity. On five occasions between December 2, 2017 and February 5, 2018,

1 Agent Daniels used Torrential Downpour to connect with and download child  
2 pornography files from IP address 24.251.70.98. The FBI obtained a search warrant for  
3 the residence associated with that IP address, and seized Ordonez’s computer during a  
4 search on April 4, 2018. The FBI performed a forensic examination of the computer and  
5 found thousands of child pornography files in the recycle bin, including the files  
6 Torrential Downpour had downloaded. On April 17, 2018, the government charged  
7 Ordonez with five counts of distributing child pornography and one count of possessing  
8 such material. Doc. 10.

## 9 **II. Discussion.**

10 Defendants contend that Torrential Downpour may be flawed and should be tested  
11 and verified by a third party. They also contend that they need access to the program in  
12 order to prepare effective cross examination of Agent Daniels and the presentations by  
13 their own computer experts. Defendants seek disclosure of an installable copy of the  
14 software pursuant to Federal Rule of Criminal Procedure 16, *Brady v. Maryland*, 373  
15 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). Gonzales also seeks  
16 disclosure of Torrential Downpour’s user and training manuals. Neither Defendant seeks  
17 the program’s source code.

18 The government contends that Defendants have failed to show how Torrential  
19 Downpour is material to their defense. The government further contends that even if  
20 materiality has been shown, Torrential Downpour is protected from disclosure by the  
21 qualified law enforcement privilege recognized in *Roviaro v. United States*, 353 U.S. 53  
22 (1957).

### 23 **A. Rule 16(A)(1)(E)(i) – Items Material to Preparing a Defense.**

24 Under Rule 16(a)(1)(E), the government must disclose any “books, papers,  
25 documents, data, . . . or portions of any of these items, if the item is within the  
26 government’s possession, custody, or control and: (i) the item is material to preparing the  
27 defense[.]” To obtain disclosure under subsection (i), “[a] defendant must make a  
28 ‘threshold showing of materiality[.]’” *United States v. Budziak*, 697 F.3d 1105, 1111 (9th

1 Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). “Neither  
2 a general description of the information sought nor conclusory allegations of materiality  
3 suffice; a defendant must present *facts* which would tend to show that the [g]overnment is  
4 in possession of information helpful to the defense.” *United States v. Mandel*, 914 F.2d  
5 1215, 1219 (9th Cir. 1990) (emphasis added); *see also Budziak*, 697 F.3d at 1111-12.

### 6 **1. Discoverability of Investigative Software.**

7 Many cases have addressed the discoverability of government software programs  
8 used to investigate child pornography offenses. The parties each cite lines of cases to  
9 support their positions.

10 Defendants rely primarily on *United States v. Budziak*, 697 F.3d 1105 (9th Cir.  
11 2012), and cases that have adopted its reasoning. *Budziak* involved the FBI’s use of an  
12 enhanced version of the LimeWire file-sharing program called “EP2P.” *Id.* at 1107.  
13 Using that program, the FBI downloaded several child pornography files from an IP  
14 address registered to Budziak. *Id.* A forensic examination of his computer revealed  
15 multiple child pornography files, including several images the EP2P program had  
16 downloaded. *Id.* Budziak was charged with multiple counts of distributing and  
17 possessing child pornography. *Id.* The district court denied Budziak’s motions to  
18 compel disclosure of the government’s EP2P program, and he was convicted on each  
19 count. *Id.* at 1107-08.

20 On appeal, the Ninth Circuit held that the district court abused its discretion in  
21 denying Budziak’s motions to compel. It noted that he did more than assert a generalized  
22 need to review the EP2P program before trial; he identified particular defenses to the  
23 distribution charges that discovery on the EP2P program could help him develop. *Id.*  
24 at 1112. Specifically, he “presented evidence suggesting that the FBI may have only  
25 downloaded fragments of child pornography files from his ‘incomplete’ folder, making it  
26 ‘more likely’ that he did not knowingly distribute any complete child pornography files  
27 to [the FBI].” *Id.* at 1112. He also presented “evidence suggesting that the FBI agents  
28 could have used the EP2P software to override his sharing settings.” *Id.* Given this

1 evidence, the Ninth Circuit concluded that “access to the EP2P software was crucial to  
2 Budziak’s ability to assess the program and the testimony of the FBI agents who used it  
3 to build the case against him.” *Id.*

4 Other cases have followed *Budziak*. For example, the district court in *United*  
5 *States v. Crowe*, No. 11 CR 1690 MV, 2013 WL 12335320, at \*7 (D.N.M. Apr. 3, 2013),  
6 required the government to allow the defense expert to examine and use a copy of the  
7 government’s confidential Shareaza software at a secure government facility. The court  
8 did so because the defendant in *Crowe*, like the defendant in *Budziak*, presented specific  
9 evidence to suggest that access to the software was material to preparing the defense.  
10 *See id.* Specifically, the defense expert testified that “some of the files alleged to have  
11 been found by law enforcement in the shared space of Defendant’s computer, were not  
12 found there during her analysis.” *Id.*

13 Another line of cases has refused to permit defendants in child pornography cases  
14 to gain access to confidential government investigative software. In *United States v.*  
15 *Pirosko*, 787 F.3d 358 (6th Cir. 2015), a case cited by the government in response to  
16 these motions, the court of appeals affirmed a district court decision denying discovery of  
17 the “law enforcement tools” used to locate and download child pornography from the  
18 defendant’s computer. The Sixth Circuit distinguished *Budziak*, noting that the defendant  
19 in that case had presented the evidence described above. 787 F.3d at 365-67. The  
20 defendant in *Pirosko*, by contrast, “failed to produce any such evidence, simply alleging  
21 that he might have found such evidence had he been given access to the government’s  
22 programs.” *Id.* at 365. As a result, discovery was not warranted. *Id.*

23 Other cases have likewise found that the defendant in child pornography cases has  
24 failed to make a showing to support their claim that disclosure of government  
25 investigative software would be material to preparing the defense. *See United States v.*  
26 *Jean*, 891 F.3d 712, 715 (8th Cir. 2018) (affirming denial of motion to compel  
27 government software because the defendant was convicted of receiving and possessing  
28 child pornography and “the likelihood of any help to [his] defense was ‘vanishingly



1 small”); *United States v. Chiaradio*, 684 F.3d 265, 277 (1st Cir. 2012) (expressing no  
2 view on whether the EP2P source code was discoverable under Rule 16 where the  
3 defendant “neither contradicted nor cast the slightest doubt upon” the government’s  
4 evidence that the FBI had downloaded child pornography from his computer); *United*  
5 *States v. Hoeffener*, No. 4:16-CR-00374, 2017 WL 3676141, at \*13 (E.D. Mo. Aug. 25,  
6 2017) (denying motion to compel where “nothing in the . . . receipt-of-child-pornography  
7 charge reveal[ed] that the charge [was] based, to any extent, on materials downloaded  
8 from [the defendant’s] computer while [the FBI] used Torrential Downpour”); *United*  
9 *States v. Blouin*, 2017 WL 2573993, at \*3 (W.D. Wash. June 14, 2017) (denying motion  
10 to compel where the defendant did not dispute that the government’s software downloads  
11 files from a single source); *United States v. Maurek*, No. CR-15-129-D, 2015 WL  
12 12915605 at \*3 (W.D. Okla. Aug. 31, 2015) (denying motion to compel where the  
13 defendant failed to present specific facts which would tend to show how disclosure of  
14 Torrential Downpour would be material to his defense); *United States v. Feldman*, No.  
15 13-CR-155, 2015 WL 248006, at \*6 (E.D. Wis. Jan. 19, 2015) (finding a lack of  
16 materiality where the defendant was charged with receiving and possessing child  
17 pornography based on a search of his computer and not the use of the government’s  
18 software).

19 *Budziak* is, of course, binding precedent for this Court. But the Court finds the  
20 distinction between it and the cases just discussed to be consistent with traditional  
21 Rule 16 principles. As already noted, “[n]either a general description of the information  
22 sought nor conclusory allegations of materiality suffice [under Rule 16(a)(1)(E)(i)]; a  
23 defendant must present *facts* which would tend to show that the [g]overnment is in  
24 possession of information helpful to the defense.” *Mandel*, 914 F.2d at 1219 (emphasis  
25 added). In *Budziak* and *Crowe*, the defendants presented evidence to support their  
26 contention that discovery of the government software was material to preparing their  
27 defense to distribution of child pornography. In the other line of cases, they did not. The  
28 Court will keep this distinction in mind as it considers the arguments of Defendants

1 Gonzalez and Ordonez.

2 **2. Gonzales Has Shown Materiality.**

3 Counts one through eight allege violations of 18 U.S.C. § 2252(a)(2). Doc. 1.  
4 That section provides criminal punishment for any person who “knowingly receives, or  
5 distributes, any visual depiction using any means or facility of interstate or foreign  
6 commerce . . . including by computer, . . . if (A) the producing of such visual depiction  
7 involves the use of a minor engaging in sexually explicit conduct; and (B) such visual  
8 depiction is of such conduct[.]” Evidence is sufficient to support a conviction for  
9 distribution under § 2252(a)(2) “when it shows that the defendant maintained child  
10 pornography in a shared folder, knew that doing so would allow others to download it,  
11 and another person actually downloaded it.” *Budziak*, 697 F.3d at 1109.

12 Defendant Gonzales argues that Torrential Downpour is material to his defense  
13 because the distribution charges are based on child pornography files that Torrential  
14 Downpour purportedly downloaded from his tablet but that were not found on the tablet  
15 when it was seized by the FBI. Doc. 25 at 8-9. He has presented an affidavit from his  
16 expert, Tami Loehrs, confirming that the files are not on the tablet. Doc. 25-5. Loehrs  
17 explains in her affidavit that it is critical to Gonzales’s defense to understand how  
18 Torrential Downpour functions in order to determine the program’s reliability and  
19 accuracy in identifying files that Gonzales is charged with knowingly distributing. *Id.*  
20 at ¶ 17. She further states that based on her many years of research and testing of peer-  
21 to-peer file sharing software, including BitTorrent, she has discovered that all of these  
22 programs “contain bugs, they do not always function as intended and the data reported by  
23 these applications is not always accurate or reliable.” *Id.* ¶ 22.

24 Loehrs offered similar opinions at the evidentiary hearing. She opined that all  
25 software programs have flaws, and Torrential Downpour is no exception. *See* Doc. 50,  
26 Hr’g Tr. at 16:15-23, 18:17-19, 31:6-10 (Jan. 31, 2019). She bases this opinion on her  
27 work in other cases involving Torrential Downpour and the fact that the files the program  
28 allegedly downloaded in this case were not found on Gonzales’s tablet. *Id.* at 16:1-23.

1           Loehrs also provided a plausible explanation for how Torrential Downpour may  
2 have erroneously identified Gonzales’s tablet as offering child pornography files over the  
3 BitTorrent network. Loehrs explained that, because a torrent is simply a text-file  
4 containing the hash values – or “fingerprints” – of the target image and video files, a  
5 BitTorrent user who downloads a torrent has fingerprints of the target files, even if he has  
6 not yet downloaded them. *Id.* at 22:14-23:8. Loehrs stated that the actual downloading  
7 of the target files occurs only when the client software instructs the torrent to search for  
8 those files on the BitTorrent network and download them to a designated folder on the  
9 user’s computer. *Id.* at 23:9-25:3. She further stated that a forensic examination of the  
10 device used to download the torrent can determine whether the torrent has been used to  
11 download the file, and her examination of Gonzales’s tablet revealed no evidence  
12 suggesting that he downloaded the files listed in counts one through eight. *Id.* at 25:4-22,  
13 28:7-9. She opined that Torrential Downpour may have obtained the files from other  
14 BitTorrent users, particularly in light of the fact that this is how peer-to-peer file sharing  
15 programs are designed to work. *Id.* at 31:3-32:12.<sup>1</sup>

16           The Court finds that this evidence brings this case squarely within the holding of  
17 *Budziak*. Defendant Gonzalez has done more than simply request access to the software  
18 and argue that it is material to his defense. He has presented evidence that calls into  
19 question the government’s version of events. Given his evidence, the Court finds that  
20 “the functions of the [program] constitute[] a ‘very important issue’ for [Gonzales’s]  
21 defense.” *Budziak*, 697 F.3d at 1112 (quoting *United States v. Cedano-Arellano*, 332  
22 F.3d 568, 571 (9th Cir. 2003)); *see Crowe*, 2013 WL 12335320, at \*7.<sup>2</sup>

23           The government concedes that the child pornography files charged in counts one  
24

---

25           <sup>1</sup> The government contends that Loehrs’s affidavit is unreliable, citing several  
26 cases rejecting or limiting the scope of her testimony. Doc. 29 at 5, 20-22. The Court  
27 found Loehrs credible at the evidentiary hearing and has no basis at this point for  
excluding her opinions under Federal Rule of Evidence 702.

28           <sup>2</sup> Gonzales asserts that the government’s need to present evidence of Torrential  
Downpour in its case-in-chief also entitles him to discovery under Rule 16(a)(1)(E)(ii),  
but he fails to develop this argument or cite relevant case law.

1 through eight were not found on Gonzales’s tablet. Doc. 29 at 3. The government notes,  
2 however, that torrent names associated with these files were located in a “µTorrent”  
3 client software folder on the tablet, that some of these torrent names were in a  
4 “jump list,” which suggests that Gonzalez had clicked on them, and that other child  
5 pornography files were found on the tablet. *Id.* at 13. Materiality is defeated, the  
6 government contends, because these facts corroborate its claim that Gonzales once  
7 possessed the files charged in counts one through eight and was able to distribute them to  
8 the FBI. *Id.* at 17.

9 But where a defendant has demonstrated materiality, the Court “should not merely  
10 defer to government assertions that discovery would be fruitless.” *Budziak*, 697 F.3d  
11 at 1112-13. While the Court has no reason to doubt the government’s good faith in this  
12 case, Gonzales “should not have to rely solely on the government’s word that further  
13 discovery is unnecessary.” *Id.* at 1113. Because Gonzales has shown that the Torrential  
14 Downpour is material to his defense, he should be given access to the program to  
15 investigate its reliability and help him prepare for cross-examination of Agent Daniels.<sup>3</sup>

16 Gonzales also contends that Torrential Downpour is material to a Fourth  
17 Amendment challenge because the program “searches beyond the public domain,  
18 essentially hacks computers searching for suspect hash values, and therefore conducts a  
19 warrantless search[.]” Doc. 25 at 6. But Gonzales identifies no evidence suggesting that  
20 Torrential Downpour accessed non-public space on his tablet. Gonzales has failed to  
21 show that Torrential Downpour is material to a Fourth Amendment challenge. *See*  
22 *Hoeffener*, 2017 WL 3676141, at \*15 (finding a lack of materiality where the defendant  
23 pointed to no “aspects of his expert’s declaration that support his request for information  
24 based on a search warrant challenge”).

---

25  
26 <sup>3</sup> The government presents a log file purportedly showing that Agent Daniels used  
27 Torrential Downpour to download from Gonzales’s tablet the child pornography file  
28 listed in count four. Doc. 29-2; *see* Doc. 6 at 3. The government asserts that this log file  
and the ones associated with the other distribution counts independently confirm that  
Agent Daniels downloaded complete child pornography files solely from Gonzales’s  
tablet. Doc. 29 at 26. But the log files were created by Torrential Downpour. If it is  
flawed in the ways Gonzales suggests, they likely would be flawed as well.

### 3. Ordonez Has Failed to Show Materiality.

1  
2 Defendant Ordonez asserts that it is critical to understand how Torrential  
3 Downpour functions “to determine its reliability and accuracy in identifying files  
4 reported[ly] involving [his] IP address and whether law enforcement went beyond  
5 accessing information that was publicly available.” Doc. 32 at 3. But Ordonez has  
6 identified no “specific defense to the charges against him that the Torrential Downpour  
7 program could help him develop.” *Maurek*, 2015 WL 12915605 at \*3. Nor has he  
8 presented any evidence in support of this materiality argument. Conclusory allegations  
9 of materiality are not sufficient to compel disclosure under Rule 16(a)(1)(E)(i). *See*  
10 *Budziak*, 697 F.3d at 1111-12 (citing *Mandel*, 914 F.2d at 1219); *Santiago*, 46 F.3d  
11 at 894-95 (the defendant’s “assertions, although not implausible, do not satisfy the  
12 requirement of specific facts, beyond allegations, relating to materiality”).

13 Defendant Ordonez does argue in his motion that his expert needs access to  
14 Torrential Downpour to determine its reliability. Doc. 32 at 2. He clarified in his reply  
15 brief that an associate with Loehrs’s firm, Michele Bush, is his defense expert. Doc. 45  
16 at 4. Bush apparently was retained by Ordonez’s former counsel and prepared a report of  
17 her examination of Ordonez’s computer in July 2018, but the report has not been  
18 disclosed to the government and has not been provided to the Court. *See* Doc. 43 at 2  
19 & n.1. Nor did Defendant Ordonez present an affidavit from Bush to support his motion,  
20 or call Bush to testify at the evidentiary hearing. Loehrs testified at the hearing that her  
21 firm is no longer working on Defendant Ordonez’s case and she has no familiarity with  
22 the FBI’s investigation in that case. Doc. 50 at 58:3-7. Ordonez’s counsel stated that he  
23 intends to engage another expert going forward (*id.* at 169:5-6), and he cross-examined  
24 Agent Daniels at the hearing, but he has presented no case-specific expert evidence to  
25 support the motion to compel.

26 Because Defendant Ordonez has failed to make a threshold showing of materiality  
27 under Rule 16(a)(1)(E)(1), his case falls within the line of cases that distinguish *Budziak*  
28 and deny discovery of government investigative software. *See Pirosko*, 787 F.3d at 366

1 (the defendant’s mere allegation that there were unanswered questions about the  
2 government’s software was not sufficient to show materiality); *Maurek*, 2015 WL  
3 12915605, at \*3 (denying motion to compel disclosure of Torrential Downpour where the  
4 defendant offered nothing more than conclusory allegations of materiality); *United States*  
5 *v. Alva*, No. 2:14-cr-00023-RCJ-NJK, 2018 WL 327613, at \*2 (D. Nev. Jan. 8, 2018)  
6 (distinguishing *Budziak* where the defendant presented no evidence that he did not store  
7 child pornography in shared folders and made no showing that his “theory behind  
8 requesting the RoundUp source code amount[ed] to anything more than an abstract  
9 possibility”); *United States v. Harney*, No. CR-16-38-DLB-CJS, 2018 WL 1145957,  
10 at \*6 (E.D. Ky. Mar. 1, 2018) (finding that the defendant’s arguments in support of his  
11 need for the software were closer to *Pirosko* than *Budziak* because he “merely alleged he  
12 might find evidence in support of his defense if his expert [was] provided the opportunity  
13 to analyze the requested information in its entirety”).

14 **B. *Brady and Giglio.***

15 Defendants also seek disclosure of Torrential Downpour under *Brady v. Maryland*,  
16 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). “The *Brady*  
17 standard for materiality is higher than Rule 16’s, and its scope narrower.” *United States*  
18 *v. Pac. Gas & Elec. Co.*, No. 14-cr-00175-TEH, 2016 WL 3185008, at \*2 (N.D. Cal.  
19 June 8, 2016). Under *Brady*’s constitutional mandate, the government “is obligated by  
20 the requirements of due process to disclose material exculpatory evidence on its own  
21 motion, without request.” *Carriger v. Stewart*, 132 F.3d 463, 479 (9th Cir. 1997). Under  
22 *Giglio*, the government’s obligation to disclose exculpatory evidence was expanded to  
23 include information that could be used to impeach government witnesses. *See Giglio*,  
24 405 U.S. at 154.

25 But it is the government, not the defendant or the trial court, that decides  
26 prospectively what information, if any, is exculpatory and must be disclosed under *Brady*  
27 and *Giglio*. *See United States v. Lucas*, 841 F.3d 796, 807 (9th Cir. 2016). “The  
28 *Brady/Giglio* doctrine does not require the government to disclose neutral . . . evidence.”

1 *United States v. Correia*, No. 2:17-CR-00001-JAD-CWH, 2018 WL 3416517, at \*2 (D.  
2 Nev. July 9, 2018) (citing *United States v. Stinson*, 647 F.3d 1196, 1208 (9th Cir. 2011)).  
3 Defendants have made no showing that Torrential Downpour will prove to be  
4 exculpatory or could be used to impeach a government witness. The Court will deny  
5 Defendants' motions to the extent they seek disclosure of Torrential Downpour under  
6 *Brady* and *Giglio*.

7 This ruling is not inconsistent with Gonzales's showing of materiality under  
8 Rule 16 because "[i]nformation that is not exculpatory or impeaching may still be  
9 relevant to developing a possible defense." *United States v. Muniz-Jaquez*, 718 F.3d  
10 1180, 1183 (9th Cir. 2013). Indeed, "[e]ven inculpatory evidence may be relevant  
11 [because a] defendant who knows that the government has evidence that renders his  
12 planned defense useless can alter his trial strategy [or] seek a plea agreement instead of  
13 going to trial." *Id.*; see also *United States v. Toilolo*, No. CR-11-00506-LEK, 2014 WL  
14 1091715, at \*3 (D. Haw. Mar. 17, 2014) ("Rule 16 is broader than *Brady*, 'requiring  
15 disclosure of all documents material to preparing the defense.'" (quoting *Muniz-Jaquez*,  
16 718 F.3d at 1183)).

### 17 **C. The Qualified Law Enforcement Privilege Under *Roviaro*.**

18 Even when a defendant is entitled to disclosure under Rule 16(a)(1)(E)(i), the  
19 evidence may be withheld under a law enforcement privilege. In *Roviaro*, the Supreme  
20 Court held that the government had a privilege to withhold from disclosure the identities  
21 of certain confidential informants. 353 U.S. at 59. Subsequent cases have expanded the  
22 privilege to other investigative techniques, including software programs like Torrential  
23 Downpour. See *Pirosko*, 787 F.3d at 366 (applying the privilege to the government's  
24 Shareaza program); *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986)  
25 (surveillance equipment); *United States v. Harley*, 682 F.2d 1018, 1020-21 (D.C. Cir.  
26 1982) (surveillance locations).

27 The Supreme Court has declined to establish fixed rules for deciding whether the  
28 government may withhold material information under a law enforcement privilege,

1 holding instead that trial courts must engage in balancing on a case-by-case basis:

2 We believe that no fixed rule with respect to disclosure is justifiable. The  
3 problem is one that calls for balancing the public interest and protecting the  
4 flow of information against the individual's right to prepare his defense.  
5 Whether a proper balance renders non-disclosure erroneous must depend on  
6 the particular circumstances of each case, taking into consideration the  
7 crime charged, the possible defenses, the possible significance of the  
8 informer's testimony, and other relevant factors.

9 *Roviaro*, 353 U.S. at 62. The trial court's balancing must afford due regard to the  
10 government's interest in maintaining the secrecy of its investigative technique, but must  
11 also fully protect the defendant's interest in a fair trial. When the two interests come  
12 squarely into conflict, the defendant's right to a fair trial should prevail because the  
13 government can always choose to protect its investigative technique by dropping the  
14 prosecution and due process dictates that a citizen should never be convicted in an unfair  
15 trial. *See United States v. Turi*, 143 F. Supp. 3d 916, 921 (D. Ariz. 2015).

16 Having considered the particular circumstances of this case and the factors to be  
17 balanced under *Roviaro*, the Court finds that disclosure of an installable copy of  
18 Torrential Downpour for testing by a third-party is not warranted. Child pornography is a  
19 scourge, victimizing the most innocent for the basest of reasons. The government has a  
20 legitimate interest in preserving its ability to investigate and prosecute distribution of this  
21 material – distribution that creates the market and fuels the demand for creation of more  
22 child pornography. Agent Daniels testified that the government's investigative efforts  
23 would be severely hampered if a copy of Torrential Downpour got into the wrong hands.  
24 Countermeasures could be developed that would thwart law enforcement's monitoring of  
25 the BitTorrent network for suspected child pornography. Doc. 50 at 126:10-20. For this  
26 reason, the government closely guards Torrential Downpour and limits the persons  
27 granted access to it. He testified that the program must remain in law enforcement  
28 custody at all times to avoid the risk of disclosure to unauthorized third-parties. *Id.*  
at 126:23-128:15.



1 The Court concludes that this substantial government interest outweighs  
2 Defendant Gonzales's need for an independent copy of Torrential Downpour. *See*  
3 *Harney*, 2018 WL 1145957, at \*11 (finding that the risk of inadvertent leaking by third  
4 parties who would have access to the government's software outweighed the defendant's  
5 need for such material). But given the substantial defense interest established by  
6 Defendant Gonzalez, the Court concludes that his expert should be granted access to  
7 Torrential Downpour for purposes of assisting in preparing the defense. The Court will  
8 balance these interests by adopting the Rule 16 disclosure method authorized in *Crowe*:

9 [T]he defense expert [will be permitted] to examine the software at issue at  
10 a designated law enforcement facility, at a mutually convenient date and  
11 time, for as much time as is reasonably necessary for the expert to complete  
12 her examination. No copies of the software shall be made. The software  
13 shall not leave the custody of the law enforcement agency that controls it.  
14 Any proprietary information regarding the software that is disclosed to the  
15 defense expert shall not be reproduced, repeated or disseminated in any  
16 manner. Violation of [this] order shall subject the defense expert and/or  
17 defense counsel to potential sanctions by this Court.

18 2013 WL 12335320, at \*8.<sup>4</sup>

19 The Court at this point will not require discovery of the Torrential Downpour  
20 manuals. Defendant Gonzalez has not provided evidence or explained how the manuals  
21 will aid in preparation of his defense. Defendant Gonzalez may raise this issue with the  
22 Court if examination of the software by Loehrs suggests that the manuals would be  
23 helpful to the defense, at which point the Court will hear from both parties before making  
24 a decision.

25 **IT IS ORDERED:**

- 26 1. Defendant Gonzales's motion to compel discovery (Doc. 25, Case No. CR-  
27 17-01311) is **granted in part** and **denied in part** as set forth in this order.
- 28 2. Defendant Ordonez's motion to compel discovery (Doc. 32, Case No. CR-

---

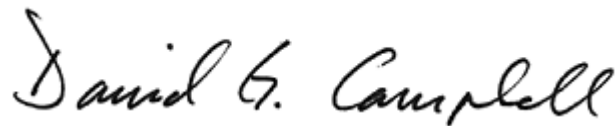
<sup>4</sup> Agent Daniels made clear that such access would pose no security risk. Doc. 50  
at 156:25-157:1-3.

1 18-00539) is **denied**.

2 Excludable delay pursuant to U.S.C. § 18:3161(h)(1)(D) is found to run from  
3 6/28/2018 in Case No. CR17-01311 PHX DGC and 12/7/2018 in Case No. CR18-00539  
4 PHX DGC.

5 Dated this 19th day of February, 2019.

6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



---

David G. Campbell  
Senior United States District Judge

1 **WO**

2

3

4

5

6

**IN THE UNITED STATES DISTRICT COURT**

7

**FOR THE DISTRICT OF ARIZONA**

8

9

United States of America,

No. CR17-01311-001-PHX-DGC

10

Plaintiff,

**ORDER**

11

v.

12

Anthony Espinoza Gonzales,

13

Defendant.

14

15

16

Defendant Anthony Espinoza Gonzales is charged with distributing and possessing child pornography in violation of 18 U.S.C. § 2252(a). Doc. 1. Following an evidentiary hearing on January 31, 2019, the Court granted in part Defendant’s motion to compel disclosure of the Torrential Downpour software the FBI used in the investigation that led to his indictment. Doc. 51. Defendant moves to compel compliance with that order. Doc. 54. The motion is fully briefed (Docs. 55-56, 63-65, 81), and the Court held an evidentiary hearing on August 16, 2019 (Doc. 82). For reasons stated below, the motion is granted in part and denied in part.

17

18

19

20

21

22

23

24

**I. Background.**

25

The indictment alleges that Defendant distributed child pornography files on eight occasions in December 2016 and January 2017. Doc. 1 at 1-5. The government claims that Defendant downloaded and publicly shared the files using BitTorrent, an online peer-to-peer network that allows users to download files containing large amounts of data,

26

27

28

1 such as movies, videos, and music. To download and share files over the BitTorrent  
2 network, a user must install a BitTorrent software “client” on his computer and download  
3 a “torrent” from a torrent-search website. A torrent is a text-file containing instructions on  
4 how to find, download, and assemble the pieces of image or video files the user wishes to  
5 view. Once the torrent is downloaded to the BitTorrent client software, the software reads  
6 the instructions in the torrent, finds the pieces of the target files on the internet from other  
7 BitTorrent users who have the same torrent, and downloads and assembles the pieces,  
8 producing complete files. The client software also makes the pieces of the files accessible  
9 over the internet to other BitTorrent users by placing them in a shared folder on the user’s  
10 computer.

11 The Torrential Downpour software is law enforcement’s modified version of the  
12 BitTorrent protocol. The software is used to identify, on the BitTorrent network, internet  
13 protocol (“IP”) addresses that have torrents associated with known child pornography files.  
14 When such an IP address is found, the software can be used to connect to that address and  
15 attempt to download child pornography.

## 16 **II. The Court’s Prior Order.**

17 Defendant’s computer forensics expert, Tami Loehrs, testified at the initial hearing  
18 in support of Defendant’s motion to compel. Docs. 41, 50. FBI Agent Jimmie Daniels  
19 testified for the government. *Id.* Based in part on Loehrs’s testimony, the Court found  
20 that Torrential Downpour is material to the defense under Rule 16(a)(1)(E)(i) because the  
21 distribution charges are based on child pornography files that Torrential Downpour  
22 purportedly downloaded over the internet from Defendant’s computer, but that were not  
23 found on Defendant’s computer when the FBI seized it pursuant to a search warrant.  
24 Doc. 51 at 8-10. The Court denied Defendant’s request for a copy of Torrential Downpour  
25 under *Roviaro v. United States*, 353 U.S. 53 (1957), given Agent Daniels’s testimony that  
26 the government’s investigative efforts would be severely hampered if a copy got into the  
27 wrong hands. *Id.* at 14-15. But given the substantial defense interest established by  
28 Defendant, the Court concluded that Loehrs should be granted access to Torrential

1 Downpour to assist Defendant in preparing the defense. *Id.* at 15. The Court adopted the  
2 Rule 16 disclosure method authorized in *United States v. Crowe*, No. 11 CR 1690 MV,  
3 2013 WL 12335320, at \*8 (D.N.M. Apr. 3, 2013):

4 [T]he defense expert [will be permitted] to examine the software at issue at  
5 a designated law enforcement facility, at a mutually convenient date and  
6 time, for as much time as is reasonably necessary for the expert to complete  
7 her examination. No copies of the software shall be made. The software  
8 shall not leave the custody of the law enforcement agency that controls it.  
9 Any proprietary information regarding the software that is disclosed to the  
defense expert shall not be reproduced, repeated or disseminated in any  
manner. Violation of [this] order shall subject the defense expert and/or  
defense counsel to potential sanctions by this Court.

10 Doc. 51 at 15.

11 Although the Court concluded that Loehrs should be permitted to examine  
12 Torrential Downpour given that the charged files were not found on Defendant's computer  
13 when it was seized, the Court rejected Defendant's argument that the software is material  
14 to a Fourth Amendment challenge because Defendant identified no evidence suggesting  
15 that the program accessed non-shared space on his computer. *Id.* at 10.

### 16 **III. Defendant's Motion to Compel.**

17 The parties corresponded regarding their proposed testing protocols for Torrential  
18 Downpour. Docs. 54-2, 54-3, 55-5. Based on the government's April 9, 2019 letter and  
19 the motion briefing, some issues have been resolved. A main point of contention is whether  
20 Loehrs may access during testing the Internet Crimes Against Children Task Force's Child  
21 Online Protection System ("COPS").

22 To determine the accuracy and reliability of Torrential Downpour, Loehrs proposes  
23 to perform nine tests: (1) non-parsed torrents, (2) partially-parsed torrents, (3) deleted  
24 torrent data, (4) unshared torrent data, (5) non-investigative torrents, (6) files of interest,  
25 (7) single source download, (8) detailed logging, and (9) restricted sharing. Doc. 56-1  
26 at 21-24. Tests one through six would each conclude with a search of COPS for any  
27 investigative hits on the suspect IP address and determine whether Torrential Downpour  
28

1 attempts to connect with that address to download data. *Id.* at 21-23. The government  
2 agrees to tests seven, eight, and nine, which do not involve COPS. Docs. 54-5 at 4, 55 at 2.

3 Tests one and two – non-parsed torrents and partially-parsed torrents – are relevant  
4 to whether Defendant downloaded complete files containing actual child pornography.  
5 The government does not address the potential materiality of these tests in its response to  
6 Defendant’s motion. *See* Doc. 55.

7 The government objects to tests three and four because they would assess whether  
8 Torrential Downpour accesses non-shared space on the suspect computer, an issue the  
9 Court dealt with in its prior order when it rejected Defendant’s argument that the software  
10 is material to a Fourth Amendment challenge. *Id.* at 3; *see* Doc. 51 at 10.

11 Loehrs wants to conduct tests five and six – non-investigative torrents and files of  
12 interest – to determine whether Torrential Downpour identified Defendant based solely on  
13 torrent files of investigative interest. Doc. 56-1 at 4, ¶¶ 11-12. But Defendant does not  
14 explain in his motion how this is material to the preparation of a defense.

15 To facilitate tests five and six, Loehrs requests that the COPS database be cloned  
16 and moved to a unique testing location on the server. Doc. 56-1 at 21. The new database  
17 would then be loaded with predefined lawful torrents known to be on the suspect computer,  
18 and Torrential Downpour would be directed to pull information from this “test database”  
19 and identify lawful files. *Id.* Loehrs claims that a test database should be used to avoid  
20 further dissemination of child pornography. *Id.*

21 The government objects to tests one through six, asserting that COPS must be  
22 protected from disclosure. Doc. 55 at 3-4. The government explains that public exposure  
23 of COPS could compromise child exploitation investigations worldwide because  
24 disclosure of the torrents being investigated by law enforcement would enable child  
25 pornographers to evade law enforcement detection and destroy evidence to thwart further  
26 investigation. *Id.* The government further explains that cloning and moving the COPS  
27 database, or building a separate database from which to do testing, would require a massive  
28 expenditure of resources. *Id.* at 4.

1 After reviewing memoranda filed by the parties, the Court directed them to provide  
2 supplemental briefing, with supporting affidavit testimony as necessary, to refine the issues  
3 and assist the Court in deciding Defendant’s motion. Doc. 59. The parties filed the briefing  
4 in late June 2019 (Docs. 63-65), and Defendant filed an additional brief shortly before the  
5 August 16 hearing (Doc. 81). Loehrs testified at the hearing in support of Defendant’s  
6 motion. Detective Robert Erdely, who helped create Torrential Downpour and is the  
7 current administrator of COPS, testified for the government. Doc. 82. Defendant filed a  
8 post-hearing brief on August 19. Doc. 85.

9 **IV. Discussion.**

10 **A. Torrential Downpour and Its Interaction with COPS.**

11 In its prior order, the Court described Torrential Downpour as follows:

12 Torrential Downpour is law enforcement’s modified version of the  
13 BitTorrent protocol. Torrential Downpour acts as a BitTorrent user and  
14 searches the internet for internet protocol (“IP”) addresses offering torrents  
15 containing known child pornography files. When such an IP address is  
16 found, the program connects to that address and attempts to download the  
17 child pornography. The program generates detailed logs of the activity and  
18 communications between the program and the IP address. Unlike traditional  
19 BitTorrent programs, the government claims that Torrential Downpour  
20 downloads files only from a single IP address – rather than downloading  
21 pieces of files from multiple addresses – and does not share those files with  
22 other BitTorrent users.

20 Doc. 51 at 2-3.

21 The government now explains that Torrential Downpour is really a suite of software  
22 whose components include (1) “Torrential Downpour Receptor,” which the government  
23 claims is not involved in this case, and (2) the “Torrential Downpour program,” which was  
24 used by Agent Daniels in this case. Doc. 64 at 2-4; *see also* Doc. 29 at 8-9 & n.7. Both  
25 components interact with COPS, but in different ways.

26 Torrential Downpour Receptor roams the internet and queries publicly available  
27 BitTorrent indices searching for IP addresses that have made public requests for specified  
28 torrent files that are of interest to law enforcement officers investigating child exploitative

1 file sharing activities. Doc. 64 at 2. Once Torrential Downpour Receptor detects an IP  
2 address associated with a torrent file of interest, it reports information about the IP address  
3 and the computer's networking port to COPS. *Id.* at 3. This information serves as a lead  
4 for officers to investigate using the Torrential Downpour program. *Id.*

5 The Torrential Downpour program has no search function. *Id.* Instead, officers use  
6 the program to initiate an investigation in one of two ways: (1) the program can interact  
7 with COPS in an automated fashion to obtain an investigative lead consistent with  
8 parameters an officer has set in the program – such as geographic area or a specific torrent  
9 – and the investigative lead is then loaded into the Torrential Downpour program (this is  
10 how Agent Daniels used Torrential Downpour in this case); or (2) officers can manually  
11 input an investigative lead – an IP address, networking port, and torrent – into the program.  
12 *Id.* Each option initiates Torrential Downpour's effort to connect to the suspect IP address  
13 and request a download of the files associated with the torrent. *Id.*

14 The government describes COPS as a repository containing information from  
15 various investigations conducted on several file sharing networks, including BitTorrent.  
16 *Id.* at 2. COPS is comprised of several servers that contain either “records in” – data  
17 received from Torrential Downpour Receptor – or “records out” – data that can be loaded  
18 into the Torrential Downpour program through a web portal used by investigating officers.  
19 *Id.* at 5. The data in COPS includes IP addresses and the “info hash” (unique identifier) of  
20 torrents being investigated by law enforcement officers around the world. *Id.* COPS also  
21 contains data relating to the identities and IP addresses of investigating officers. *Id.* COPS  
22 is updated by the minute with new information received from Torrential Downpour  
23 Receptor. *Id.* at 3.

24 **B. The Government's Use of Torrential Downpour in this Case.**

25 Agent Daniels set parameters in his Torrential Downpour program (v.1.33) to  
26 automatically request leads from COPS for his investigation. *Id.* at 3-4. Based on these  
27 settings, Torrential Downpour automatically downloaded information about Defendant's  
28 IP address, networking port, and the alleged torrents publicly shared by Defendant's IP



1 address. *Id.* at 4. Torrential Downpour then connected with Defendant's IP address and,  
2 the government alleges, downloaded the child pornography files that Defendant's  
3 computer was offering publicly from its shared folder. The downloaded child pornography  
4 is the basis for the charges in counts one through eight of the indictment. *Id.*; *see* Doc. 1  
5 at 1-5.<sup>1</sup>

6 The government does not dispute that Torrential Downpour Receptor was used to  
7 initially identify Defendant's IP address and networking port as points of interest, or that  
8 it reported this information to COPS for further investigation. But the government objects  
9 to any testing of Torrential Downpour Receptor because Agent Daniels did not use the  
10 software in his investigation and the search results received by Torrential Downpour  
11 Receptor were not used as probable cause for the search warrant. Instead, the actual  
12 downloads of child pornography from Defendant's IP address through the Torrential  
13 Downpour program formed the basis for the search warrant request. The government also  
14 asserts that the search of the internet by Torrential Downpour Receptor will not be used by  
15 the government at trial. Doc. 64 at 4, 7-9, 11, 18.

16 **C. Loehrs's Proposed Testing Protocol (Tests One Through Six).**

17 **1. Tests One and Two.**

18 Loehrs describes test one as follows:

19 [T]his first test simulates a scenario in which the Suspect Computer contains  
20 torrents, including legal torrents and torrents of investigative interest.  
21 However, none of the torrents have been parsed or seeded, meaning no  
22 associated files have been downloaded, so the Suspect Computer is void of  
the content of those torrents.

23 Doc. 56-1 at 21.

24 Loehrs explains that this test will determine whether Torrential Downpour identified  
25 Defendant based solely on a torrent that was never parsed, meaning the associated files  
26 were never downloaded to Defendant's computer. *Id.* at 3, ¶ 7. Loehrs claims that the

27 \_\_\_\_\_  
28 <sup>1</sup> Count nine charges Defendant with possessing other child pornography files found  
on his computer when it was seized pursuant to a search warrant. Doc. 1 at 5-6.

1 presence of a torrent alone, which is merely a text file that does not contain contraband,  
2 should not be identified by Torrential Downpour. *Id.*; *see also* Doc. 50 at 22-25.

3 Test two is similar to test one, but involves partially-parsed torrents. This is  
4 Loehrs's phrase for torrents where only some of the associated files were downloaded to  
5 Defendant's computer. Doc. 56-1 at 3, 21.

6 In response to questions from the Court at the August 16 hearing, the government  
7 acknowledged that Torrential Downpour Receptor, like all BitTorrent client software, will  
8 search the internet for torrents of interest and identify an IP address as a potential download  
9 candidate based on a non-parsed or partially-parsed torrent that has been loaded into the  
10 user's client software. Court's LiveNote Hr'g Tr. at 2:19-4:4, 20:20-22:18, 25:5-26:17  
11 (hereinafter "Tr."). Torrential Downpour Receptor will then report the IP address to COPS  
12 for further investigation by law enforcement officers. *Id.* at 3:18-20. Loehrs confirmed  
13 that the purpose of tests one and two is to determine whether Torrential Downpour  
14 identifies a suspect IP address based solely on the address having a non-parsed or partially-  
15 parsed torrent. *Id.* at 6:13-16, 25:18-26:13; *see* Doc. 56-1 at 3, ¶¶ 7-8. Given the  
16 government's concession that this is how the software operates, tests one and two are not  
17 necessary. *See id.*

18 Defendant agreed at the hearing that test one is no longer necessary (Tr. at 6:8-16,  
19 25:15-23), but argued that test two is still needed to determine whether Torrential  
20 Downpour Receptor identifies IP addresses based on a partially-parsed torrent containing  
21 no child pornography files or inadvertently downloaded files (*id.* at 7:5-8, 11:1-12:2).  
22 Defendant argued that he should not have to take the government's word as to how  
23 Torrential Downpour works. *Id.* at 13:1-7.

24 But to obtain discovery under Rule 16(a)(1)(E), Defendant "must make a 'threshold  
25 showing of materiality[.]'" *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012)  
26 (quoting *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). "Evidence is  
27 'material' under Rule 16 if it is helpful to the development of a possible defense." *Id.*  
28 "Neither a general description of the information sought nor conclusory allegations of

1 materiality suffice; a defendant must present facts which would tend to show that the  
2 Government is in possession of information helpful to the defense.” *Id.* at 1112 (quoting  
3 *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

4 Defendant expressed concern that Torrential Downpour Receptor may be  
5 identifying suspects based on lawful torrent files, citing testimony of one of Detective  
6 Erdely’s colleagues. Tr. at 8:4-8, 9:23-10:8; *see* Doc. 81-1 at 8, ¶ 23. Based on her  
7 experience in other cases, Loehrs believes that COPS contains lawful torrent files,  
8 including cartoons, erotica, adult pornography, and images of children that are not sexual  
9 in nature. Doc. 63-1 at 5, ¶ 14.

10 But Defendant failed to explain why it would be helpful to his defense to show that  
11 Torrential Downpour Receptor identified his IP address, and put the address into COPS,  
12 based on lawful torrent files or inadvertently downloaded files. Defendant agreed that  
13 scanning the internet for publicly visible suspicious conduct does not constitute a Fourth  
14 Amendment search. Tr. at 11:19-22; *see also United States v. Ganoë*, 538 F.3d 1117, 1127  
15 (9th Cir. 2008) (defendant’s expectation of privacy in his computer did not “survive [his]  
16 decision to install and use file-sharing software, thereby opening his computer to anyone  
17 else with the same freely available program”); *United States v. Maurek*, 131 F. Supp. 3d  
18 1258, 1262 (W.D. Okla. 2015) (numerous federal courts “have uniformly held there is no  
19 reasonable expectation of privacy in files made available to the public through peer-to-peer  
20 file-sharing networks”) (citations omitted). The fact that Torrential Downpour Receptor  
21 may have identified Defendant’s IP address and put that address into COPS for further  
22 investigation on the basis of non-parsed or partially-parsed torrents related to child  
23 pornography, or Defendant’s inadvertent receipt of a child pornography torrent, or even  
24 Defendant’s possession of torrents that contain lawful adult pornography, is immaterial to  
25 the defense because scanning the internet for publicly available information, even lawful  
26 information, is not a Fourth Amendment violation.

27 Further, the charges in this case are not based on anything Defendant made available  
28 on the internet that was detected by Torrential Downpour Receptor. The charges are based

1 on what allegedly happened when the Torrential Downpour program followed up on the  
2 lead in COPS, contacted Defendant’s IP address, and requested copies of child  
3 pornography his computer was offering to share publicly through the BitTorrent program.  
4 The government alleges that Defendant’s computer shared the child pornography charged  
5 in the indictment on eight different occasions.

6 As noted, the government acknowledges that Torrential Downpour Receptor  
7 identifies a suspect IP address based on the address having a partially-parsed torrent. This  
8 is the fact test two seeks to establish. *See* Doc. 56-1 at 3, ¶ 8. Because this fact has been  
9 conceded by the government, and Defendant has not shown that test two is material to the  
10 defense for some other reason, the Court concludes that test two is not necessary.

## 11 **2. Tests Three and Four.**

12 Tests three and four involve scenarios in which the suspect computer contains  
13 deleted torrent files and torrents where the associated files have been moved to non-shared  
14 space on the computer. Doc. 56-1 at 21-22. The government asserts that the Torrential  
15 Downpour program does not access such non-shared space. Loehrs wants to test that  
16 assertion. *Id.* at 4.

17 The government objects to these tests based on the Court’s rejection of Defendant’s  
18 Fourth Amendment argument. Doc. 55 at 3. In his initial motion to compel, Defendant  
19 argued that Torrential Downpour is material to a potential Fourth Amendment violation  
20 because the program “searches beyond the public domain, essentially hacks computers  
21 searching for suspect hash values, and therefore conducts a warrantless search[.]” Doc. 25  
22 at 6. The Court rejected this argument because Defendant identified no evidence that  
23 Torrential Downpour accessed non-shared space on his computer. Doc. 51 at 10.

24 The defense now proposes a different reason tests three and four are material – a  
25 scenario where Defendant started downloading files associated with a charged torrent,  
26 viewed some of these files and realized one of them contained contraband, and immediately  
27 deleted those files and stopped the download process. Doc. 63-1 at 2, ¶ 5. Loehrs asserts  
28 that it is important to “know if Torrential Downpour identified [the charged] files before

1 or after [Defendant] may have deleted them.” *Id.* Loehrs states that the essential issue  
2 tests three and four will resolve “is whether Torrential Downpour is identifying files *after*  
3 a user has taken an affirmative action to delete them.” *Id.* at 2-3, ¶ 6 (emphasis in original).

4 Detective Erdely testified that the Torrential Downpour program downloads only  
5 those files being shared by the user’s BitTorrent software, and it is unlikely that µTorrent  
6 – the software Defendant used – would share files from non-shared space. Tr. at 31:8-24.  
7 Loehrs countered that BitTorrent software has been found to have exploits allowing it to  
8 access non-shared space, and she believes Torrential Downpour is susceptible to the same  
9 exploits. *Id.* at 37:12-21. Loehrs also stated that Torrential Downpour’s instructions could  
10 have been modified to allow the program to access non-shared space. *Id.* at 33:7-20.

11 The distribution charges are based in large part on log files and Agent Daniels’s  
12 testimony that the Torrential Downpour program downloaded child pornography files from  
13 shared space on Defendant’s computer. Doc. 63 at 2. Defendant argues that he should not  
14 have to accept the government’s word that the files were in shared space when identified  
15 by Torrential Downpour, particularly given that the files were not found on the computer  
16 when the FBI seized it. *Id.* The Court agrees. *See Budziak*, 697 F.3d at 1113.

17 “[E]vidence is sufficient to support a conviction for distribution under 18 U.S.C.  
18 § 2252(a)(2) when it shows that the defendant maintained child pornography in a shared  
19 folder, knew that doing so would allow others to download it, and another person actually  
20 downloaded it.” *Id.* at 1109. Thus, whether the Torrential Downpour program downloaded  
21 the charged files from shared space or non-shared space on Defendant’s computer is  
22 material to the distribution charges. Defendant has made a sufficient Rule 16 factual  
23 showing to conduct tests three and four because the charged files were not found on his  
24 computer when it was seized by the government. Defendant will be permitted to conduct  
25 tests three and four (as modified below) to determine whether the Torrential Downpour  
26 program can access deleted or unshared torrent data. *See id.* at 1113.

27 ///

28 ///

### 3. Tests Five and Six.

1  
2 Test five is a scenario in which the suspect computer contains non-investigative  
3 torrents and associated data. Doc. 56-1 at 22. Test six involves the use of files of  
4 investigative interest. *Id.* at 22-23. Loehrs explains that these tests will determine whether  
5 Torrential Downpour Receptor identifies torrents that contain lawful files. *Id.* at 4,  
6 ¶¶ 11-12; Doc. 63-1 at 4, ¶ 10. But as explained above, whether Defendant's IP address  
7 was identified by Torrential Downpour Receptor based on lawful files is not material to  
8 the defense. Even if that happened, the charges in this case are based on what Defendant's  
9 computer did when it was later contacted by Torrential Downpour.

10 Defendant claims that Torrential Downpour downloaded more than 30 files from  
11 his computer, only three of which were described by Agent Daniels as child pornography.  
12 Doc. 54 at 5; Tr. at 53:17-21. But Defendant is not charged with distributing lawful files.  
13 Each file charged in counts one through eight is alleged to contain images or videos of  
14 child pornography. *See* Doc. 1 at 1-5. And the Court can see no way in which Torrential  
15 Downpour's download of lawful files from Defendant's computer constitutes a defense to  
16 these charges. Distributing three videos containing child pornography along with 27 videos  
17 of lawful content still constitutes distribution of three videos of child pornography.

18 Moreover, the government acknowledged that Torrential Downpour investigates  
19 torrents relating to various child exploitation activities, and, in the process of downloading  
20 torrents known to contain child pornography, will sometimes download lawful files.  
21 Tr. 55:10-57:25. This acknowledgment renders tests five and six unnecessary. *See id.*  
22 at 51:7-52:4.

23 Defendant argued that the issue is whether the files were in fact downloaded from  
24 his computer as the government claims, and, if so, whether they were found in shared space.  
25 Tr. at 51:20-52:13, 54:9-13. But these issues will be addressed by tests three and four  
26 (deleted and unshared files) and test seven (single source download). *See id.* at 54:9-55:9,  
27 60:4-61:7; Doc. 56-1 at 21-23.

28

1 Defense counsel further argued that she should be permitted to test Torrential  
2 Downpour thoroughly for any and all flaws, and posed a series of “what-if” scenarios as to  
3 how Torrential Downpour may work improperly. Tr. at 63:19-66:14. But to conduct  
4 discovery under Rule 16, Defendant must make a threshold factual showing of materiality.  
5 See *Budziak*, 697 F.3d at 1111. Fishing expeditions are not allowed. See *United States v.*  
6 *Chon*, 210 F.3d 990, 994 (9th Cir. 2000) (affirming denial of discovery request where the  
7 government had met its obligations under Rule 16 and “the requested discovery was a ‘far  
8 reaching fishing expedition”); *United States v. Spagnuolo*, 549 F.2d 705, 712-13 (9th Cir.  
9 1977) (affirming denial of motion to compel under Rule 16 where the defendant merely  
10 assumed FBI files would show that his investigation was tainted by unlawful wiretaps and  
11 noting that he had “embarked on the type of fishing expedition condemned by [the] court  
12 in *Ogden v. United States*, 303 F.2d 724 (9th Cir. 1962”); *United States v. Wolfenbarger*,  
13 No. 16-CR-00519-LHK-1, 2019 WL 3037590, at \*8 (N.D. Cal. July 11, 2019) (denying  
14 discovery request in child pornography case and explaining that “Rule 16 does not  
15 authorize ‘a shotgun fishing expedition for evidence’”) (citation omitted). Defendant has  
16 made no threshold showing of materiality with respect to tests five and six.

17 **D. Is Access to COPS Necessary to Conduct Tests Three and Four?**

18 In her proposed testing protocol, Loehrs describes COPS and her request for access  
19 to the system as follows:

20 [COPS] is a web-based component of Torrential Downpour and its operation  
21 including retrieving information about torrents of investigative interest and  
22 reporting historical data back to law enforcement for further investigation.  
23 Access to the [COPS] database will simulate law enforcement’s undercover  
24 BitTorrent investigation by facilitating the same search capabilities relied upon  
25 in [this case].

26 A unique login will be created by the government allowing access to the live  
27 [COPS] system in order to track and locate all information being reported by  
28 Torrential Downpour from the Suspect Computer, described below.

Doc. 54-4 at 8.

1 According to the government, Loehrs mistakenly believes that the COPS database  
2 includes a search function. Doc. 64 at 4. The government notes that Loehrs describes  
3 COPS as a component of Torrential Downpour and its operation, including “*retrieving*  
4 *information* about torrents of investigative interest and reporting historical data back to law  
5 enforcement for further investigation.” *Id.* (quoting Doc. 56-1 at 17; emphasis by the  
6 government). Loehrs also states in her supplemental affidavit that the “COPS database is  
7 how the investigation into [Defendant] began.” Doc. 63-1 at 3, ¶ 8. What Loehrs seems  
8 to be referring to, at least in part, is Torrential Downpour Receptor. *See* Doc. 70-1 at 12  
9 (Detective Erdely’s affidavit stating that it appears some of the tests proposed by Loehrs  
10 would use Torrential Downpour Receptor).

11 The government argues that access to COPS is not necessary or material for the  
12 limited examination of Torrential Downpour the Court has authorized. Doc. 64 at 4. The  
13 government states that the testing Loehrs seeks to run can be conducted by manually  
14 inputting IP addresses, port numbers, and lawful torrents into the Torrential Downpour  
15 program. *Id.* The government notes that law enforcement officers performed these  
16 functions manually prior to the automation of COPS, and can still do so today. *Id.* at 9.

17 At the hearing, Detective Erdely testified that when communicating with the  
18 Torrential Downpour program, COPS provides three pieces of information – an IP address,  
19 port number, and torrent – and Torrential Downpour then operates independently from  
20 COPS to investigate the IP address. Tr. 73:6-25, 78:17-20. He clarified that COPS also  
21 provides a preference for the order in which files are to be downloaded by Torrential  
22 Downpour (files of interest are to be downloaded first). *Id.* at 74:1-77:8. He explained  
23 that standard BitTorrent client software has a similar feature that allows the user to  
24 manually select the files to be downloaded. *Id.* at 74:10-12.<sup>2</sup>

---

25  
26 <sup>2</sup> Defendant asserted that Detective Erdely “changed his story” about how COPS  
27 interacts with Torrential Downpour and this is a basis for providing Loehr’s access to  
28 COPS. *Id.* at 78:8-11. Specifically, Defendant questioned why Torrential Downpour  
downloads lawful files at all if the program can target files known to contain child  
pornography. *Id.* at 12-16. Detective Erdely explained that the universe of child  
pornography is not known to law enforcement, and that files associated with torrents of  
interest are downloaded to determine whether they contain child pornography. *Id.* at



1           Loehrs asserts that COPS must be accessed “in its native state” for testing purposes,  
2 but does not explain why manually inputting IP addresses, port numbers, and torrents into  
3 the Torrential Downpour program, rather than having COPS do so automatically, will not  
4 allow for adequate testing of Torrential Downpour – the program Defendant has sought to  
5 investigate from the beginning and that allegedly downloaded the child pornography from  
6 Defendant’s shared folder. Doc. 63-1 at 3, ¶ 8.

7           The government also provides credible evidence that cloning and moving the  
8 relevant portions of COPS, or creating a simulated database, is not feasible. Doc. 64 at 5-8.  
9 To clone and move the database would require considerable reprogramming because the  
10 COPS source code is not organized in a compartmented form, thus making it difficult to  
11 retrieve the portion dedicated solely to the BitTorrent network. *Id.* at 5. The government  
12 notes that the COPS database design includes various features, such as tables, database  
13 instances, and specific programming for retrieving data, that would be complicated to  
14 replicate. *Id.* at 5-6. The government estimates that cloning and moving the BitTorrent  
15 portion of COPS, and removing law enforcement sensitive data, would require more than  
16 300 hours of work and cost between \$75,000 and \$100,000. *Id.* at 6. The government  
17 explains that creating a simulated version of COPS – a database that has taken nearly eight  
18 years to develop – would also be complicated and could involve dozens of hours of  
19 reprogramming. *Id.* at 6-7. The government notes that populating a simulated database  
20 manually is unnecessary because a database is simply a repository of information,  
21 something that can be accomplished by populating a local log file on Loehrs’s computer.  
22 *Id.* at 7-9.<sup>3</sup>

23           For several reasons, the Court will not grant Defendant access to the COPS database.

24           First, Defendant has not shown that access to COPS is necessary to perform tests  
25 three and four. The question in those test is how Torrential Downpour interacts with a  
26 

---

79:1-22. The Court found Detective Erdely credible in describing how COPS and  
27 Torrential Downpour interact.

28           <sup>3</sup> In his hearing memorandum, Defendant proposes giving Loehrs a limited log-on  
to COPS, similar to allowing someone limited access to online bank accounts. Doc. 81  
at 5. The government made clear that COPS contains no such feature. Tr. 71:2-6.

1 suspect computer – whether it accesses deleted files or non-shared space. The Court is  
2 satisfied that the question can be answered by manually loading the IP address, port  
3 number, and torrent information into the Torrential Downpour program and then observing  
4 how the program interacts with the suspect computer. Access to COPS is not required to  
5 conduct this test.<sup>4</sup>

6 Second, Defendant has not shown that access to COPS is material to preparation of  
7 his defense as required by Rule 16. As discussed above, further investigation of how the  
8 government searches the internet for publicly-offered child pornography will not aid the  
9 defense because such public searches do not violate the Fourth Amendment and the  
10 government does not intend to present evidence regarding Torrential Downpour Receptor  
11 at trial. Similarly, further investigation of the COPS database where Torrential Downpour  
12 Receptor deposits its investigative leads is not material. The government has presented  
13 credible evidence that COPS is simply a data base, not a search engine that conducted  
14 investigative activities in this case, and Defendant provides no facts to suggest otherwise.

15 Third, the Court concludes that COPS is protected from disclosure by the *Roviaro*  
16 privilege. The government has a legitimate interest in preserving its ability to investigate  
17 and prosecute the distribution of child pornography. COPS contains highly sensitive  
18 information about thousands of ongoing investigations into child pornography worldwide.  
19 Doc. 64 at 12; Tr. at 71:7-11. The information includes info hash data for the torrents of  
20 interest, and the IP addresses of both suspects and investigating officers. *Id.* The Court  
21 concludes that the substantial government interest in protecting the secrecy of COPS  
22 outweighs Defendant's need to access the database.

23 Fourth, although Rule 16 permits defendants in criminal cases to obtain discovery  
24 of certain categories of information in the government's possession or control, Rule 16  
25 does not require the government to create information for a defendant. *See United States*

---

26  
27  
28 <sup>4</sup> The defense suggested at the hearing that COPS may provide instructions to the  
Torrential Downpour program that prompt it to look at deleted files or non-shared space  
on the suspect computer, but this suggestion appears to be pure speculation. The defense  
provides no facts to support this suggestion, and facts, rather than speculation, are required  
to obtain discovery under Rule 16. *See Budziak*, 697 F.3d 1112.

1 v. *Hamzeh*, No. 16-CR-21, 2019 WL 1331639, at \*4 (E.D. Wis. Mar. 25, 2019)  
2 (“[A]lthough Rule 16(a)(1)(E) requires the government to disclose evidence, it does not  
3 require the government to create evidence.”); *United States v. Mahon*, No. CR-09-0712-  
4 PHX-DGC, 2011 WL 5006737 at \*3 (D. Ariz. Oct. 20, 2011) (citing cases). The Court  
5 can find no basis for requiring the government to incur the substantial time and expense  
6 required to clone or recreate the COPS database for Defendant’s investigation.

7 **V. Conclusion.**

8 Tests one and two are not necessary because the government acknowledges that  
9 Torrential Downpour Receptor identifies IP addresses based on non-parsed and partially-  
10 parsed torrents. Tests three and four are material to the defense, but Loehrs is not permitted  
11 access to COPS in performing the tests. Tests five and six are not permitted because they  
12 are immaterial and unnecessary. The government has agreed to tests seven, eight, and nine.

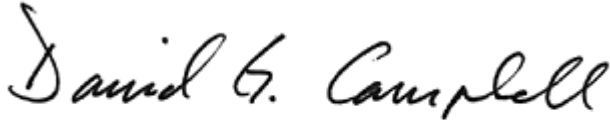
13 **IT IS ORDERED:**

14 1. Defendant’s motion to compel compliance with the Court’s  
15 February 19, 2019 order (Doc. 54) is **granted in part and denied in part** as set forth in  
16 this order.

17 2. Defendant’s motion to submit his supplemental brief (Doc. 85) is **granted**.<sup>5</sup>

18 3. Excludable delay pursuant to U.S.C. § 18:3161(h)(1)(D) is found to run from  
19 4/15/2019.

20 Dated this 27th day of August, 2019.

21 

22 \_\_\_\_\_  
23 David G. Campbell  
24 Senior United States District Judge

25  
26 \_\_\_\_\_  
27 <sup>5</sup> Defendant asserts in his brief that the “handshake” communication between  
28 Torrential Downpour and a suspect’s computer can turn into an ongoing investigation that  
lasts an extended period of time (Doc. 85 at 2-7), but does not explain why this renders  
“all nine tests” material to the defense (*id.* at 7).

BRYAN SCHRODER  
United States Attorney

JONAS M. WALKER  
CHARISSE ARCE  
Assistant U.S. Attorneys  
Federal Building & U.S. Courthouse  
222 West Seventh Avenue, #9, Room 253  
Anchorage, Alaska 99513-7567  
Phone: (907) 271-5071  
Fax: (907) 271-1500  
Email: jonas.walker@usdoj.gov  
charisse.arce@usdoj.gov  
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,            ) No. 3:17-cr-00095-SLG  
  ) )  
  Plaintiff,            ) )  
  ) )  
  vs.                    ) )  
  ) )  
MATTHEW WILLIAM SCHWIER,            ) )  
  ) )  
  Defendant.            ) )  
\_\_\_\_\_ )

**MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER AND  
NOTICE OF COMPLIANCE WITH SUPPLEMENTAL ORDER (Dkt. 243)**

The United States, through undersigned Assistant U.S. Attorney, responds to the Supplemental Order Regarding C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour (the “Order,” Dkt. 243). As explained below, the government has been working diligently to meet the Order’s one-week deadline, and the computer can be available on November 20, 2019.

**A) The government elects to provide limited access to a computer running  
Torrential Downpour, rather than dismiss Counts 1 and 2.**

The Order permits the government to choose between only two options: first, allowing the defense to perform four tests on Torrential Downpour, the nature of which are withheld from the government; or, second, dismissing Counts 1 and 2.<sup>1</sup> The Order is silent regarding technical aspects of how the government must provide the computer.

In the event the Court orders the additional terms of the protective order, below, the government is electing to provide access consistent with the Order, rather than dismissing Counts 1 and 2. The government is selecting this option because the Order does not compel internet access for the computer; nor does it permit the defense to add or remove software or hardware from the computer; nor does it allow the computer to leave the Orange County Regional Computer Forensics Lab (OCRCFL).<sup>2</sup> Most importantly, and consistently with the Court's prior protective order at Dkt. 231, the Order does not result in the software itself being released into "the wild." Finally, the Order leaves in place the broad protective language in Dkt. 231.<sup>3</sup> Thus, the order strikes a "proper balance" between production and

---

<sup>1</sup> "The government may opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense. In that event, the government may still proceed on Count 3." Order, Dkt. 243, at 7.

<sup>2</sup> The OCRCFL is located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. *See* Order Re: Compliance With Discovery Procedure, Dkt. 158 at footnote 4 regarding referring to the OCRCFL as the "Anaheim RCFL."

<sup>3</sup> The Court ordered:

Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other

protection Roviaro v. United States, 353 U.S. 53 (1957).

Accordingly, the government is preparing a computer for defense access at the OCRCFL. The government will take reasonable measures to ensure that the computer will not access the internet, for several reasons. First, the Court did not order internet access. *See* Order, Dkt. 243. Second, because Torrential Downpour is designed to, and does reliably, download child pornography, connecting it to the internet would create a risk that it would fulfill its intended function, thereby facilitating the distribution of child pornography, in violation of 18 U.S.C. § 2252A, and other applicable laws, which the Order does not permit. Third, the Court did not order the defense to have access to ICAC COPS, which could be accessible via the internet. Likewise, the government will take reasonable measures to ensure that Torrential Downpour cannot be digitally or physically removed from the computer.

**B) Additional terms for a protective order**

Pursuant to paragraph (2) of the Order at Dkt. 243 at 7, the government respectfully requests the Court order the following additional terms to a protective Order:

1. The government will provide a computer at the OCRCFL. The computer will have one version of Torrential Downpour installed, *i.e.*

---

than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person without prior order of the Court.

Dkt. 231 at 13.  
U.S. v. Schwier  
3:17-cr-00095-SLG

version 1.23, one of the versions used in this investigation. The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.

2. The only persons who will have access to the computer are Jeffrey Fischbach and Robert Herz (collectively "the defense"). The defense will have access to the computer for 21 consecutive days of testing.
3. The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.
4. The defense may bring digital media, computers, and phones into the room with the computer.
5. The defense will not remove the computer from the OCRCFL. The defense will not copy Torrential Downpour.
6. The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape.
7. The defense will not download or distribute child pornography using the computer. Any downloading of child pornography would constitute a violation of the federal criminal code.

8. All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain the Wireshark data pending further order of the Court.
9. At the conclusion of testing, the FBI will “zip” all the Wireshark files, meaning it will use software to compress them. The FBI will “hash” the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.

The government believes that these restrictions should permit the defense to perform any legitimate testing on Torrential Downpour, while, also, ensuring that the software is not removed from the computer.

The Court is familiar with Wireshark; it is the screen-recording and packet-capturing program the government used during the validation testing previously ordered



by the Court.<sup>4</sup> For the current testing, the preservation of Wireshark data accomplishes two goals. First, it creates some measure of protection against the copying of Torrential Downpour. Second, it protects the integrity of the testing process. To the extent that Mr. Fischbach testifies pursuant to FRE 702, the Wireshark data would be the best possible evidence regarding the testing.

**C) Objections to defense's *ex parte* advocacy.**

In an abundance of caution, and to preserve the record, the government notes that, on record on November 4 and 5, 2019, prior to the Court issuing the Order, the government objected to the Court's consideration of the defense's *ex parte* communication. *See* Dkt 234-1 (redacted version of Mr. Fischbach's declaration). The government respectfully maintains its objections to the Court's consideration of the defense's *ex parte* communications.

On October 17 and 18, 2019, the parties' expert witnesses testified at length. Following that hearing, the Court ordered the government's proposed testing and denied the defense's request that the government produce Torrential Downpour. Dkt. 231. This order made sense in light of the defense's failure to identify the tests and Mr. Fischbach's performance under cross-examination.<sup>5</sup>

Having failed to meet its burden under Budziak at the evidentiary hearing, the defense later submitted, *ex parte*, a Declaration of Jeffrey M. Fischbach, dated October 31,

---

<sup>4</sup> *See* Dkt. 219-1 at para. 3; Dkt. 231 at 12.

<sup>5</sup> "But when asked about the materiality of this information, Mr. Fischbach was only able to speak in vague generalities, claiming attorney-client privilege." Dkt. 231 at 11.

2019, a redacted version of which the government received at Dkt. 234-1. As the Court notes in the Order, “[i]n the redacted copy of Mr. Fischbach’s declaration, the entire description of these four tests and their relevance to the defense are blacked out.” Order at 243 at 6. Thus, it was not until October 31 that the defense identified the tests, long after the government’s opportunity to challenge the merits of Mr. Fischbach’s claims had passed. In this way, the defense achieved, via *ex parte* advocacy, that which it failed to do when Mr. Fischbach was subject to cross-examination in open court.

“[I]n our system, adversary procedures are the general rule and *ex parte* examinations are disfavored.” United States v. Kenney, 911 F.2d 315, 321 (9th Cir. 1990). The “reliability [of evidence is] assessed in a particular manner: by testing in the crucible of cross-examination.” Crawford v. Washington, 541 U.S. 36, 61 (2004). “This open examination of witnesses is much more conducive to the clearing up of truth” because “adversarial testing beats and bolts out the Truth much better.” Id. (internal citations and punctuation omitted). The Supreme Court has described cross-examination as the “greatest legal engine ever invented for the discovery of truth.” Maryland v. Craig, 497 U.S. 836, 846 (1990).

Due to the *ex parte* nature of the defense’s advocacy, the government is ignorant of the four tests, their procedures, goals, scientific validity, and technological requirements. Accordingly, the government has had no opportunity to contest their materiality under United States v. Budziak, 697 F.3d 1105 (9<sup>th</sup> Cir. 2012). As the Court has already

acknowledged<sup>6</sup>, the government has a legitimate interest in protecting Torrential Downpour, pursuant to Roviaro v. United States, 353 U.S. 53 (1957). The government’s interest in protecting, and responsibility to protect, this important tool for investigating child pornography is especially heightened when, as here, the government has been kept ignorant of the tests that the defense is requesting.

Moreover, the secrecy of the tests has complicated the government’s response to the Order. Due to the nationwide importance of protecting Torrential Downpour, while also effectively prosecuting child pornography offenses, the decision regarding how to respond to the Order is not solely that of the U.S. Attorney’s Office for the District of Alaska. Accordingly, in the four working days since the Court issued the Order, the government has conferred with the FBI Office of General Counsel; the Child Exploitation and Obscenity Section of the Criminal Division of the U.S. Department of Justice; another U.S. Attorney’s Office; in addition to personnel involved in this investigation.

//

---

<sup>6</sup> The Court held:

The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that “child pornography distributors could find a way to avoid detection” if the workings of Torrential Downpour were made public, “render[ing] that tool of law enforcement ineffective.” At the evidentiary hearing, Mr. Erdely testified that “to give [the defense] unfettered access to this software puts law enforcement and ten years of development at risk” because it would reveal certain aspects of Torrential Downpour’s operation.

Order Regarding C-3 Motion, Dkt. 231 at 10-11.

U.S. v. Schwier  
3:17-cr-00095-SLG

**D) Conclusion: The computer will be available by November 20, 2019.**

The FBI has advised the undersigned that it can have the computer prepared and in place at the OCRCFL, ready for the defense, by Wednesday, November 20, 2019. The government respectfully requests the Court issue the attached protective order, the terms of which are essential to protect Torrential Downpour, and which should not interfere with any testing by the defense. Absent these protections, the government cannot provide the computer.

The government objects to any additional *ex parte* advocacy by the defense, particularly regarding the terms of the protective order. If necessary, the government can provide an affidavit, or the testimony of a witness, to explain the merits of the terms of the protective order.

RESPECTFULLY SUBMITTED November 15, 2019, in Anchorage, Alaska.

BRYAN SCHRODER  
United States Attorney

s/ Jonas M. Walker  
JONAS M. WALKER  
Assistant U.S. Attorney  
United States of America

**CERTIFICATE OF SERVICE**

I hereby certify that on November 15, 2019, a true and correct copy of the foregoing was served electronically on the following:

Robert M. Herz

s/ Jonas M. Walker  
Office of the U.S. Attorney

U.S. v. Schwier  
3:17-cr-00095-SLG

BRYAN SCHRODER  
United States Attorney

JONAS M. WALKER  
Assistant U.S. Attorney  
Federal Building & U.S. Courthouse  
222 West Seventh Avenue, #9, Room 253  
Anchorage, Alaska 99513-7567  
Phone: (907) 271-5071  
Fax: (907) 271-1500  
Email: jonas.walker@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	No. 3:17-cr-00095-SLG
	)	
MATTHEW WILLIAM SCHWIER,	)	
	)	
Defendant.	)	
_____	)	

**MOTION TO DISMISS COUNTS 1 AND 2  
AND REGULATE PRODUCED DISCOVERY**

The United States, through undersigned Assistant United States Attorney, pursuant to Federal Rules of Criminal Procedure 48 and 16(d), moves the Court for an order dismissing Counts 1 and 2 of the Fourth Superseding Indictment and ordering the defense team to certify that they have destroyed all evidence received relating to Torrential Downpour.

## A) Reasons for dismissal of Counts 1 and 2

BitTorrent is a peer-to-peer network used by computer-savvy individuals to attempt to hide their receipt and collection of child pornography. Law enforcement officers use Torrential Downpour software to identify distributors of child pornography using the BitTorrent network.

In this case, the Court found “persuasive” the government’s evidence that release of Torrential Downpour to the public would undermine the software’s effectiveness as a law enforcement tool. *See* Dkt. 231 at 9-10. Over an approximate four-month period, the government has diligently worked to craft testing environments and protective orders with the goals of, both, protecting Torrential Downpour from disclosure, and, also, permitting the defense to prepare for trial, thereby satisfying both United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012), and Roviaro v. United States, 353 U.S. 53 (1957). The United States proposed three protective orders, or terms for protective orders, (Dockets 244-1, 253-4, and 288-1) in its attempt to achieve those objectives.

At Dkt. 304, the Court denied the government’s third proposed protective order<sup>1</sup>,

---

<sup>1</sup> At the Final Pretrial Conference on January 14, 2020, the Court indicated that it was persuaded by the defense expert’s affidavit (Dkt. 297 at 1-2), which alleged that the government had already released the software by “repeated missteps.”

In an abundance of caution, and to ensure clarity in the record, the government respectfully notes that, to the contrary, the government did not err in producing the virtual machines containing the software; rather, it did so pursuant to the Court’s order at Dkt. 231.

The affidavit at Dkt. 297 is, apparently, referring to virtual machines produced pursuant to the Order at Dkt. 231, which ordered the validation testing in Anchorage and established the original protective order in this case. Specifically, at Dkt. 231 at 12-13, the Court ordered that “the validation process described at Docket 219-1 shall be carried out *U.S. v. Schwier*

3:17-cr-00095-SLG

which, in the opinion of the government's subject-matter experts, proposed terms that were essential to protect Torrential Downpour.

The Court gave the government the alternative to “opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense.” Dkt. 243 at 7. Under FRCrP 48, “[t]he government may, with leave of court, dismiss an indictment, information, or complaint.”

Therefore, pursuant to FRCrP 48, the government respectfully moves the Court to dismiss Count 1 and Count 2 of the Fourth Superseding Indictment.

**B) Destruction of sensitive evidence and vacation of pending discovery orders**

As indicated in Dkt. 310, the government respectfully requests the Court order that the United States does not have to produce a revised redacted version of the Torrential Downpour manual (per Dkt. 306), nor must it produce the software itself (per Dkt. 305). The government respectfully requests the Court order that the defense file certification that Mr. Herz and Mr. Fischbach have destroyed, and will not access in the future, the Torrential Downpour manuals (including sealed Dkt. 299 and Dkt. 300, and the version produced in discovery); and, further, will not access the virtual machines the government produced to

---

for versions 1.15 and 1.23 of the Torrential Downpour software on November 4, 2019, and on November 5, 2019 as necessary.”

Dkt. 219-1 at paragraph 3 includes the following: “Moreover, the computers running the target VM and investigative VM will be available for forensic examination by the defense expert.”

Accordingly, the government lawfully produced, per the Order at Dkt. 231, the virtual machines used during the validation testing that was described at Dkt. 219-1. Those virtual machines contained the software.

U.S. v. Schwier  
3:17-cr-00095-SLG

the defense at the Orange County Regional Computer Forensic Laboratory (OCRCFL), pursuant to the Order at Dkt. 231, and referred to by the defense at Dkt. 297.

RESPECTFULLY SUBMITTED January 23, 2020, in Anchorage, Alaska.

BRYAN SCHRODER  
United States Attorney

s/ Jonas M. Walker  
JONAS M. WALKER  
Assistant U.S. Attorney  
United States of America

### **CERTIFICATE OF SERVICE**

I hereby certify that on January 23, 2020,  
a true and correct copy of the foregoing  
was served electronically on the following:

Robert M. Herz  
Attorney for Defendant

s/ Jonas M. Walker  
Assistant U.S. Attorney  
Office of the U.S. Attorney



BRYAN SCHRODER  
United States Attorney

JONAS M. WALKER  
CHARISSE ARCE  
Assistant U.S. Attorneys  
Federal Building & U.S. Courthouse  
222 West Seventh Avenue, #9, Room 253  
Anchorage, Alaska 99513-7567  
Phone: (907) 271-5071  
Fax: (907) 271-1500  
Email: jonas.walker@usdoj.gov  
charisse.arce@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, )  
)  
Plaintiff, )  
)  
vs. ) No. 3:17-cr-00095-SLG  
)  
MATTHEW WILLIAM SCHWIER, )  
)  
Defendant. )  
\_\_\_\_\_ )

**MOTION FOR PARTIAL RECONSIDERATION REGARDING ORDER  
(Dkt. 254) AND FOR TELEPHONIC PARTICIPATION OF WITNESS AT  
STATUS HEARING**

The United States, by undersigned Assistant United States Attorney, pursuant to L.Civ.R. 7(h)(1)(A), respectfully moves the Court for partial reconsideration of the Order Re Motion for Additional Terms for Protective Order (Dkt. 244) (the “Order,” Dkt. 254), and pursuant to L.Civ.R. 7(i), telephonic participation by a witness. The government

respectfully requests an opportunity to present the testimony of a witness to explain the issues discussed below.

In the 14 days since the Court originally ordered the government to make Torrential Downpour available to the defense (Dkt. 243), the government has diligently worked to craft an appropriate protective order that complies with both United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012), and Roviaro v. United States, 353 U.S. 53 (1957). In an unprecedented development, the United States has agreed to allow a defense expert to test Torrential Downpour outside the presence of a government agent. The government has, in good faith, rapidly proposed two protective orders. Taking into account the defense's objections to the first proposed order (244-1), the government crafted a second proposed protective order (253-4) that allowed internet access, but required Wireshark as a way to protect the software from copying.

**A) Wireshark provides some assurance against software copying, but imposes no costs on the defense.**

The Court held (Order at 2) that FRCrP 16 does not impose a duty on the defense to preserve evidence. The government does not dispute this legal conclusion.

However, the Order overlooked, and did not address, an important reason the government seeks a protective order with Wireshark or another appropriate packet-capture software: *i.e.* detecting digital copying of Torrential Downpour from the TD Computer.

Put another way: there are two potential ways that Torrential Downpour could be compromised at the OCRCFL; first, being physically removed from the OCRCFL; or, second, which is more likely to occur, being digitally copied from the TD Computer onto

other media. The Court has adequately protected Torrential Downpour from being physically removed from the OCRCFL by ordering that the defense will not open, tamper with, or remove the TD Computer from the OCRCFL.

However, the Order provides no way to verify that Torrential Downpour has not been copied from the TD Computer. The risk is that, during testing, the defense could inadvertently copy Torrential Downpour onto the digital media or computers that will be brought into the room with the TD computer. Copying Torrential Downpour would be as easy as copying any file. To be clear, the government is not accusing the defense of intending violate a protective order, or conspiring to violate 18 U.S.C. § 1030, or otherwise attempting to copy the software from the TD Computer. Rather, the government is seeking a reasonable prophylactic measure that will confirm that the software has not been copied.

Mr. Fischbach has, already, lost a hard drive at the OCRCFL in this case. *See* Dkt. 253-2 (email from Joe Monroe, stating “Fischbach advised he was missing an external hard drive that he left in the Defense Review room, during his last visit. We were unable to locate the missing external hard drive”).<sup>1</sup> Given the high importance of protecting Torrential Downpour from disclosure, such negligence is reasonable cause for concern, particularly in light of the government’s evidence that Torrential Downpour must be protected from disclosure.

The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that “child pornography distributors could find a way to avoid detection” if the workings of Torrential Downpour were made

---

<sup>1</sup> The government’s understanding is that Mr. Fischbach insinuated that the OCRCFL was at fault.

public, rendering that tool of law enforcement ineffective. At the evidentiary hearing, Mr. Erdely testified that to give the defense unfettered access to this software puts law enforcement and ten years of development at risk because it would reveal certain aspects of Torrential Downpour's operation. Dkt. 231 at 9-10 (internal punctuation omitted).

Moreover, given his purported experience with classified information, Mr. Fischbach should be comfortable complying with procedures intended to verify that sensitive information is not inadvertently lost during discovery. Indeed, that is the very purpose of the OCRCFL.

Finally, Wireshark provides significant protections for the government, but imposes no costs on the defense. Wireshark will not interfere with any privileged information, because the government will not possess the Wireshark data. Wireshark will not interfere with any testing the defense runs.

The government respectfully requests a status hearing with an opportunity to present the telephonic testimony of a witness who can explain the security value of Wireshark.

**B) The government is working to comply with other aspects of the Order (Dkt. 254).**

The government has identified a computer with specifications similar to the one already in use in this case. Per Mr. Herz's email at Dkt. 253-3, such a computer should satisfy the defense.

The Court ordered the government to "provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements" by the end of one working day. Order at 254. The Court did not define "all applicable TD software documentation." The government is diligently

working to identify a manual for those two versions of Torrential Downpour and redact the privileged information therefrom for discovery.

### **C) Conclusion**

The government respectfully requests the Court schedule a status hearing on November 25 or 26, 2019, at which the government may present the testimony of a witness to briefly explain why Wireshark (or another packet capture program) is important to protect Torrential Downpour from being compromised during testing. In the event that the Court rejects the use of any packet-capture software, the government may request an additional period to propose an alternative technical arrangement that would permit the defense to do testing.

RESPECTFULLY SUBMITTED November 22, 2019, in Anchorage, Alaska.

BRYAN SCHRODER  
United States Attorney

s/ Jonas M. Walker  
JONAS M. WALKER  
Assistant U.S. Attorney  
United States of America

### **CERTIFICATE OF SERVICE**

I hereby certify that on November 22, 2019,  
a true and correct copy of the foregoing  
was served by served through ECF on:

Robert Herz

s/ Jonas M. Walker  
Office of the U.S. Attorney

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, ) No. 3:17-cr-00095-SLG  
)  
Plaintiff, )  
)  
vs. )  
)  
MATTHEW WILLIAM SCHWIER, )  
)  
Defendant. )  
\_\_\_\_\_ )

**[PROPOSED] ORDER GRANTING MOTION FOR  
ADDITIONAL TERMS FOR PROTECTIVE ORDER**

Having duly considered the United States' Motion for Additional Terms for Protective Order and Notice of Compliance with Supplemental Order (the "Motion"), the Court grants the Motion and ORDERS that:

1. The government will provide a computer at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The computer will have one version of Torrential Downpour installed, *i.e.* version 1.23, one of the versions used in this investigation. The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.

//

2. The only persons who will have access to the computer are Jeffrey Fischbach and Robert Herz (collectively “the defense”). The defense will have access to the computer for 21 consecutive days of testing.
3. The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.
4. The defense may bring digital media, computers, and phones into the room with the computer.
5. The defense will not remove the computer from the OCRCFL. The defense will not copy Torrential Downpour.
6. The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape.
7. The defense will not download or distribute child pornography using the computer. Any downloading of child pornography would constitute a violation of the federal criminal code.
8. All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain

the Wireshark data pending further order of the Court.

9. At the conclusion of testing, the FBI will “zip” all the Wireshark files, meaning it will use software to compress them. The FBI will “hash” the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.

The government may provide the computer by November 20, 2019. The government’s compliance with this Order satisfies the government’s obligations under United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).

Moreover, the Court reaffirms its prior protective Order (Dkt. 231), as follows:

Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense’s observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person



without prior order of the Court.

Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this case, provided the materials are filed under seal and/or submitted to the Court for in camera inspection.

Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.

DATED this \_\_\_\_\_ day of November, 2019, at Anchorage, Alaska.

---

UNITED STATES DISTRICT COURT JUDGE

## Validation Report

This document will explain the testing procedure and methodology used to validate the Torrential Downpour v 1.22 investigative tool. Understanding the following terms<sup>1</sup> will be helpful when reading this document as many of them will be mentioned throughout.

### A. GLOSSARY

#### **availability**

The number of complete copies of the torrent contents there are distributed in the part of the swarm you're connected to. The amount of the torrent contents you currently have is included in the availability count. A swarm with no seed and with an availability below 1.0 will likely be unable to finish transferring the complete torrent contents.

#### **byte**

A unit used for measuring the size of data on a computer storage device. Many people confuse "byte" for "bit" when referring to speeds. A byte is composed of 8 bits, so there is a clear distinction, and terminology should not be confused when referring to bytes.

#### **client**

The application a user is using when connected to a swarm. In this case, the application being used to connect to swarms is BitTorrent, so it is the client.

#### **download**

The act of transferring data from another computer onto your own.

#### **firewall**

A barrier (hardware and/or software) that prevents communication to and/or from certain computers, depending on the rules set in the firewall.

#### **hash**

A "fingerprint" of data assumed to be unique to the data. Because of the assumed uniqueness of the data, it is used to verify that a piece of data is indeed uncorrupted (since the corrupted data's hash would not match its expected hash).

#### **hash check**

The comparing of a piece of data's hash with a reference hash in order to verify the integrity of the piece of data.

#### **hashfail**

When a piece fails the hash check used to verify data integrity.

---

<sup>1</sup> This excerpt of definitions of terms was taken directly from the BitTorrent website. These definitions as well as a full list can be found at <http://help.bittorrent.com/customer/portal/articles/179175-glossary>.



**interested**

This word describes the state of a BitTorrent connection. When a peer is interested, it means the peer is interested in the data that the peer on the other end of the connection has and is willing to accept data from the other peer.

**IP address**

A number used to uniquely identify devices on a network.

**LAN IP address (also referred to as a private IP)**

The private, internal IP address that locates a computer on a LAN. A LAN IP address is not visible to users outside of the LAN. As described by RFC 1918, the following ranges are designated as reserved IP addresses for private LANs:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

**P2P (peer-to-peer)**

The use of bandwidth of users using the same peer-to-peer service to perform the functions of the peer-to-peer service or software. Centralized servers are not what keeps P2P networks alive, but rather, the peers themselves.

**payload**

The actual data being transferred from sender to receiver, not counting overhead.

**peer**

A user/client connected to the swarm. People sometimes refer to peers as "leechers," though they also use the same word to refer to its more negative connotation. It's recommended that you use the word "leecher" to strictly refer to people who don't share so to keep the distinction clear and confusion to a minimum.

**piece**

The smallest appreciable unit of data in BitTorrent. The size of pieces can be different depending on the .torrent file in question.

**protocol**

A set of rules and description of how to do things. In the case of the BitTorrent protocol, it is a set of rules describing how BitTorrent clients should communicate and transfer data with each other.

**seed**

A peer with 100% of the data in the torrent contents.

**seeding**

The act of being connected to a swarm as a seed.

**swarm**

The collective group of peers (which includes seeds) that are connected by a common .torrent file.

**torrent**

A small file containing metadata from the files it is describing. In other contexts, it is sometimes used to refer to the swarm connected around that small file.

**upload**

The act of transferring data from your computer onto another.

**B. SETUP:** Note that all software was installed using default setting, except where otherwise noted.

- 1) Both the investigative system and the target system were created using VMWare Workstation Player 15 version 15 build-10952284. This free tool, downloaded from <https://www.vmware.com>, allows for the creation of virtual machines (VMs), which can easily be copied or transferred to other users or systems. As taken from the VMWare website:

*“The isolation and sandbox capabilities of VMware Workstation Player make it the perfect tool to help you learn about operating systems, applications and how they work. Being able to run a server environment on a desktop PC also allows you to explore software and application development in a “real world” environment without interfering with the host desktop.”<sup>2</sup>*

- 2) Windows 10 Pro (64 bit) build 1809 OS Build 17763.253 was chosen as the operating system for both VM’s. Prior to conducting the validation test, Microsoft automatic updates was disabled on both machines. While Torrential Downpour will run on older versions of Windows, Windows 10 was selected as it is the most recent release of the Windows operating system. Torrential Downpour does not operate on other operating systems such as Linux or Mac iOS devices.

- 3) Private Internet Access (PIA) version .81 was used on both VMs. PIA allows for internet connectivity through a virtual private network (VPN):

*“PRIVATE INTERNET ACCESS provides state of the art, multi-layered security with advanced privacy protection using VPN tunneling. Scroll below to the Security Layers section to learn more about each individual layer.*

*Our services have been designed from the ground up to be able to operate using built-in technology pre-existing in your computer or smartphone device.*

---

<sup>2</sup> Quoted from the VMWare website at <https://www.vmware.com/products/workstation-player.html>

*The services operate at the TCP/IP interface level, which means all of your applications will be secured, not just your web browser.”<sup>3</sup>*

4) In order to conduct packet captures to show network traffic, the software tool Wireshark version 2.6.6 was used on both VM’s. This free tool is available for download from <https://www.wireshark.org/>. Wireshark is used to record network traffic (packet captures) on the target machine to show how a standard BitTorrent client, in this case BitTorrent, conducts multisource downloads to obtain a payload. When utilizing Torrential Downpour, Wireshark is used on both the investigative and target VMs to show that the software only conducts single source downloads (SSD).

*“Wireshark is the world’s foremost and widely-used network protocol analyzer. It lets you see what’s happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.”<sup>4</sup>*

Bram Cohen, the architect of the BitTorrent protocol, recommends the use of Wireshark to test BitTorrent applications:

*“When developing a new implementation the Wireshark protocol analyzer and its dissectors for bittorrent can be useful to debug and compare with existing ones.”<sup>5</sup>*

5) To display hash values of created or downloaded files, the program Cyohash version 1.02 was utilized on both VM’s. This tool adds right click functionality to the mouse that allows for hash values to be easily calculated and displayed for individual files. This tool will calculate both the MD5 and SHA1 hash values for a given file.

6) For this validation test, a .torrent file needed to be created to share non-copywritten files on the BitTorrent network. To create this .torrent and to download and share (seed) these files, BitTorrent 7.0 was used.

7) The images used in the creation of the validation torrent were downloaded from <https://www.pexels.com/>:

*“It’s hard to understand complex licenses that is why all photos on Pexels are licensed under the **Creative Commons Zero (CC0) license**. This means the pictures are completely free to be used **for any legal purpose**.*

- *The pictures are **free for personal and even for commercial use**.*

<sup>3</sup> Quoted from the PIA website at <https://www.privateinternetaccess.com/>

<sup>4</sup> Quoted from the Wireshark website at <https://www.wireshark.org/>

<sup>5</sup> Bram Cohen, The BitTorrent Protocol Specification

- You can modify, copy and distribute the photos.
- All without asking for permission or setting a link to the source. So, **attribution is not required**.

*The only restriction is that identifiable people may not appear in a bad light or in a way that they may find offensive, unless they give their consent. You should also make sure the depicted content (people, logos, private property, etc.) is suitable for your application and doesn't infringe any rights.*

*The CC0 license was released by the non-profit organization Creative Commons (CC). Get more information about Creative Commons images and the license on the [official license page](#).”<sup>6</sup>*

Files of various sizes were used for the payload and were saved in a folder named “Validation stock photos”. From there the pictures were arranged randomly in two separate sub directories named “1” and “2” respectively, with one file being left in the root directory. To create the .torrent file itself, the built-in creation tool incorporated into BitTorrent was pointed at the “Validation stock photos” folder. The piece size selected was 1024 kB and a number of trackers were added. No other options were changed.

- 8) For the investigative VM only, Roundup Torrential Downpour version 1.22 (TD) was used. This investigative software is available for law enforcement only and was developed by the University of Massachusetts, Amherst. TD follows the BitTorrent protocol with few exceptions. The first exception is that TD does not take advantage of what is referred to as file swarming. File swarming can speed up the download process by downloading from multiple BitTorrent programs simultaneously. Instead, TD only requests to download pieces from a single IP thereby insuring that any downloaded data came from a single sharing BitTorrent program. Although standard BitTorrent programs will download data from a single IP address if that is the only download candidate available at that moment, TD can *only* download from a single IP address regardless of the number of BitTorrent programs sharing the same data. Secondly, TD cannot share data back to the BitTorrent filesharing network. This is easily accomplished since every piece of data we become in possession of was downloaded from a single IP who would never need those pieces back.
- 9) To view the contents of a .torrent file Roundup Torrent Viewer version 2.3, which is a standalone torrent viewing program, was used on both virtual machines. This program, which was written by the University of Massachusetts, Amherst, reads the data from a .torrent file and presents it in an easy to read format for the user. When directed at a .torrent file, the viewer will display information found within the torrent, which includes the following:

---

<sup>6</sup> Quoted from the Pexels website at <https://www.pexels.com/photo-license/>

- Info Hash
- Number of Pieces
- Files
- Creation Date (GMT)
- Publisher
- Public / Private
- Comment
- Piece Size
- Total Size
- Created By
- Publisher URL
- Files
  - File Name
  - Index Number
  - Size
  - Piece Range
  - Path
- Piece Hashes
- Announce / Announce List
- DHT Nodes

**10)** LibreOffice 6.1.3.2 was used for documentation purposes as it is also a free program which runs on multiple operating systems. It is available for download from <https://www.libreoffice.org/>

**11)** For consistent date and time documentation, the Atomic Clock application written by Timo Partl was downloaded through the Microsoft store and installed on both VMs. Information on Timo Partl can be found at <https://timopartl.com/>

**12)** To capture and record the entire validation process, Camtasia Studio 8 version 8.6.0 (paid version) was used <https://www.techsmith.com/>. During the validation process the recording was conducted in real time and neither the recording of the investigative or target virtual machines was paused or stopped at any time.

**C. METHODOLOGY This validation test was conducted on 01/23/2019. Times listed are Eastern Standard Time (EST).**

- 1) Both the investigative and target virtual machines are started, and the atomic clock program run and placed in the bottom right corner of the screen. Both atomic clocks are compared to verify they are reporting the same time.
- 2) PIA started on both machines and connected to a location which allows for port forwarding.
- 3) **11:24 AM** Screen recording software started for target VM.
- 4) **11:24 AM** Private IP address of ethernet adapter displayed utilizing the Windows command prompt and ipconfig command. Private IP address is documented.

- 5) **11:24 AM** Public IP address for the target VM was displayed by going to the website [www.IPChicken.com](http://www.IPChicken.com) compared to the public IP reported by PIA. Public IP address and port is documented.
- 6) **11:25 AM** Validation .torrent file is opened in Roundup Torrent Viewer, and all information is displayed.
- 7) **11:25 AM** The Wireshark program is run and a packet capture recording of the network traffic is started. The Wireshark recording records all the communication in and out of the target VM. Analysis of this network traffic can be used to identify the communication, and confirm the download was available and conducted through connections with multiple sources as is typical when the data is available from multiple sources. To validate that TD conducts a download from a single BitTorrent program, rather than swarming, would be meaningless if the data was only available from a single BitTorrent program. This validation confirms that even though multiple sources for this data existed, TD will conduct a download from a single IP address.
- 8) **11:25 AM** BitTorrent is started, however no .torrent files are currently loaded into the program. The port number being used by BitTorrent is shown under the preferences of the program. This port number is the same as what is reported by PIA. The option to "Close button closes uT to tray" is disabled.
- 9) **11:26 AM** A standard download is initiated with BitTorrent by loading the .torrent file into the program. During the course of the download, the peers tab is displayed to show simultaneous active connections to multiple peers (swarming). This step documents that the data is available from multiple sources.
- 10) **11:28 AM** Once the payload for the validation torrent is completely downloaded and is displayed as seeding within BitTorrent, the Wireshark capture is terminated and saved onto the desktop of the VM. This packet capture is hashed and displayed using Cyohash. This step was conducted so that any expert will be able to confirm this is an accurate copy of the network traffic recording.
- 11) **11:28 AM** The .torrent file information is displayed from within the BitTorrent program by clicking on the bottom "General" and "Files" tabs. This data can be compared to the data previously displayed by the Torrent Viewer Program.
- 12) **11:28 AM** From within BitTorrent, the downloaded files referenced by the .torrent file are displayed. This is done by right clicking on the entry and selecting "Open Containing Folder". The names, sizes and hash values of each file are shown.
- 13) **11:30 AM** Screen recording the investigative VM is started.
- 14) **11:30 AM** Private IP address of ethernet adapter displayed utilizing the Windows command prompt and ipconfig command. Private IP address is documented.
- 15) **11:30 AM** Public IP address for the target VM was displayed by going to the website [www.IPChicken.com](http://www.IPChicken.com) compared to the public IP reported by PIA. Public IP address and port is documented.
- 16) **11:30 AM** Validation .torrent file is opened in Roundup Torrent Viewer, and all information is displayed.



- 17) **11:31 AM** The Wireshark program is run, and a packet capture recording of the network traffic is started on the investigative VM. The Wireshark recording records all the communication in and out of the investigative VM. Analysis of this network traffic can be used to identify the communication, and confirm the download was available and conducted through a connection with only a single source, even though the download was available from multiple sources as seen above in step 9.
- 18) **11:31 AM** A second Wireshark recording of the network traffic is started on the target VM. This second recording serves to document the investigative download made by TD. Analysis of this Wireshark recording can be used to confirm that all the data being referenced by this .torrent was shared to the investigative computer.
- 19) **11:32 AM** From within BitTorrent on the target VM, the .torrent being seeded<sup>7</sup> is highlighted and the bottom “Peers” tab selected. This is done to display any connections between this BitTorrent client and other BitTorrent clients which are communicating about and /or downloading pieces of this .torrent.
- 20) **11:32 AM** TD program is run, and an investigative download is initiated by loading the .torrent and specifying the IP address and port to connect to. Although this method of initiating an investigation is somewhat manual, TD has the ability to load these investigations into the program and conduct downloads automatically. This can be achieved by specifying an IP address, a range of IP addresses, or a geographic region. To determine the approximate location, TD utilizes the free geolocation database provided by [www.maxmind.com](http://www.maxmind.com). Regardless of the method used to initiate the investigation, only three pieces of information is used by TD: the .torrent identifier (infohash), the IP address and the port.
- 21) **11:32 AM** The date and time of the single source download is documented for both the target and UC VMs.
- 22) **11:32 – 11:33 AM** Once the single source download has completed, the Wireshark captures are stopped on both machines and saved to their respective desktops. Cyohash is used to display the hash values of these captures on both machines. This step was conducted so that any expert will be able to confirm this is an accurate copy of the network traffic recordings.
- 23) **11:33 AM – 11:43 AM** The validation worksheet on the investigative VM is completed. While completing the worksheet, the various log files are displayed as well as the specific file information such as file names, sizes and hash values. These can be compared to the data displayed in the Torrent Viewer Program as well as the information that was displayed on the target VM.
- 24) **11:40 AM** On the target VM the downloaded Validation stock photos folder is copied onto the desktop. A new .torrent file named “New Torrent” is created using this copied folder. This new .torrent is viewed in the torrent viewer program and verified as having the same infohash as the original torrent.
- 25) **11:42 AM** On the target VM, the copied “Validation stock photos” folder located on the desktop is renamed to “Validation stock”.

---

<sup>7</sup> Peers possessing all the pieces of a .torrent that continue sharing that content are referred to as a seed. As a seed, the BitTorrent application will typically connect to other peers in order to share pieces of a .torrent.

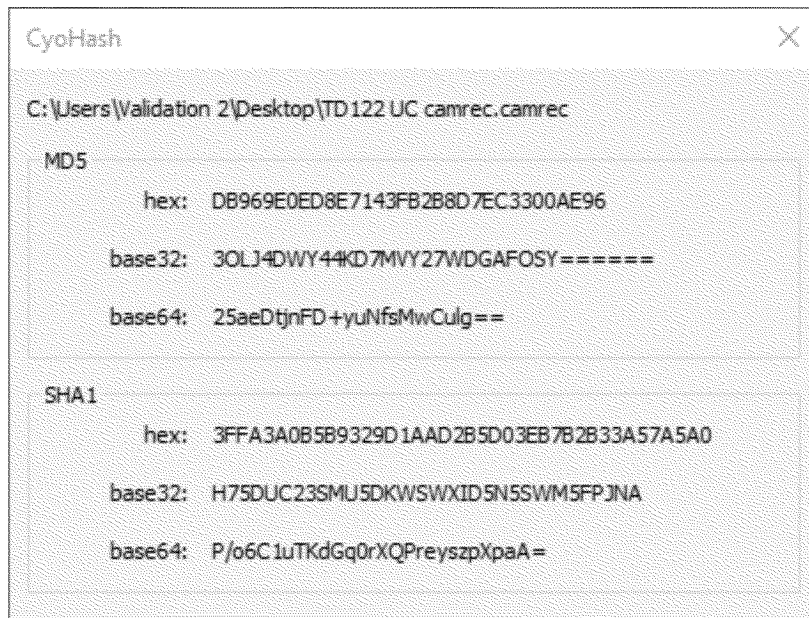
- 26) **11:42 AM** A new .torrent file named "Name Change" is created using the newly renamed "Validation stock" folder. Once created, this new torrent is viewed in the torrent viewer program and shown to calculate a completely different infohash. This is done to show that any changes made to the file names, directories, data etc. will create a completely new .torrent. BitTorrent programs can only communicate and / or share with each other when both programs are communicating about a .torrent with the se infohash.
- 27) **11:43 AM** The validation worksheet is saved and closed and cyohash is used to display the hash values of the worksheet.
- 28) **11:44 AM** A third Wireshark capture of the network traffic is started on the target VM.
- 29) **11:44 AM** A second Wireshark capture of the network traffic is started on the UC VM
- 30) **11:44 AM** On the target VM, the original containing folder for the seeding .torrent (found in the "Downloads" directory) is opened and the top-level directory "Validation stock photos" is renamed to "Validation stock" and BitTorrent is shown to still be displaying the "seeding" message.
- 31) **11:45 AM** Another investigative download of the .torrent from the target VM is attempted.
- 32) **11:45 – 11:46 AM** BitTorrent seeding failure message displayed on target machine. Upon failure, the Wireshark captures on both VMs are terminated and saved to desktop. Both captures are hashed using Cyohash. This step was conducted so that any expert will be able to confirm this is an accurate copy of the network traffic recordings. The purpose of this step is to illustrate that when changes are made to any data referenced by the .torrent at the location where it is shared from, the BitTorrent program quickly recognized the change and therefore stops the seeding (sharing) process.
- 33) **11:46 AM** The top-level directory "Validation stock" is renamed back to its original name of "Validation stock photos". BitTorrent is shown to still be displaying the error message from step 34. The Validation stock photos torrent is selected within the program and the option to "Start" is selected. The error message is shown to change to "Seeding".
- 34) **11:46 AM** A fourth Wireshark recording of the network traffic is started on the target VM.
- 35) **11:47 AM** While BitTorrent is sharing the data, the folder containing the data is moved to a different location (desktop) and BitTorrent is shown to still be "seeding" the files. The purpose of this step is to illustrate that when any data referenced by the .torrent at the location where it is shared from is moved from that shared location, the BitTorrent program quickly recognized the change and therefore stops the seeding (sharing) process.
- 36) **11:48 AM** A third Wireshark recording of the network traffic is started on the UC VM.
- 37) **11:48 AM** Another investigative download of the .torrent from the target VM is attempted.
- 38) **11:48 – 11:49 AM** BitTorrent seeding failure message displayed on target machine. Upon failure, the Wireshark recordings on both VMs are terminated and saved to desktop. Both captures are hashed using Cyohash. This step illustrates what was described in step 35 above
- 39) **11:49 – 11:50 AM** The recordings for both VMs are terminated.

#### **D. CONCLUSIONS**

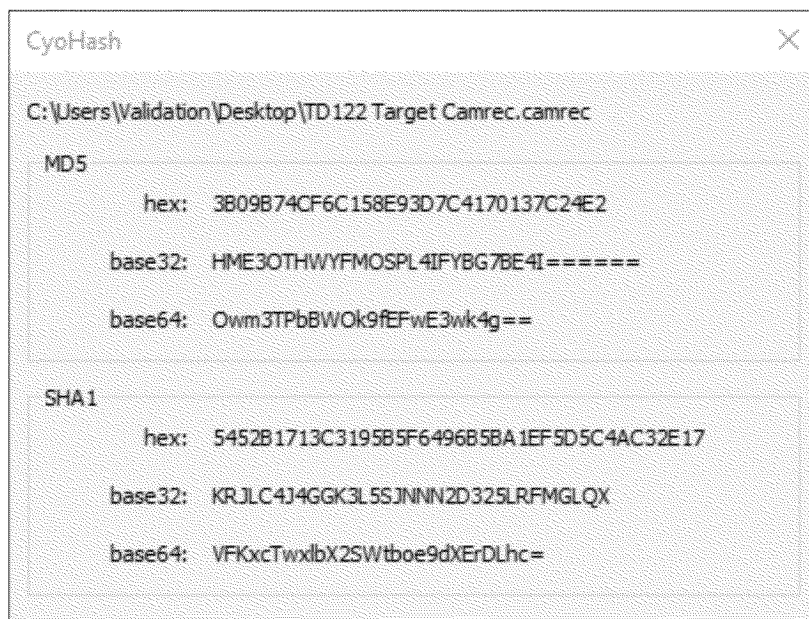
1. TD properly performed an investigative download from a single sharing BitTorrent program, which can be verified through the Wireshark recordings.
2. TD did not share any file data with any other BitTorrent program on the BitTorrent file sharing network.
3. Downloads can only occur when the data remains available in the location where it is being shared from.
4. Data can only be shared when the file(s) and/or directory(s) remained unchanged.
5. Downloads can only occur when two BitTorrent programs are communicating about the same .torrent (having identical infohashes).
6. Understanding the method by which BitTorrent shares data, that being that a .torrent file is a requirement to download any data, the download of unshared files is impossible.
7. All communications to and from the investigative computer were documented with a Wireshark recording (packet capture). Any nefarious activity where Torrential Downpour would send non- standard BitTorrent protocol messages would be exposed in the review of these packet captures.
8. Dates and times are properly recorded in the log files created by the software.
9. The infohash is properly recorded in the log files created by the software.
10. The IP address and port being investigated is properly recorded in the log files created by the software.
11. The IP address of the investigating computer is properly recorded in the log files created by the software
12. Files(s) and paths are properly recorded in the log files created by the software and match what is defined by the .torrent.
13. The data downloaded matched the data being shared on the target computer.
14. Data can only be downloaded while it is being shared by the BitTorrent program. If the data is moved or deleted it immediately ceases.
15. When a change is made to the shared data, even something as minor as renaming a file, the sharing BitTorrent application quickly recognizes the change and stops sharing the data.

#### **E. POST TEST**

- 1) At the conclusion of the validation video, Cyohash was used to hash the original recording files for both the investigative VM (Image 1) and the target VM (Image 2).

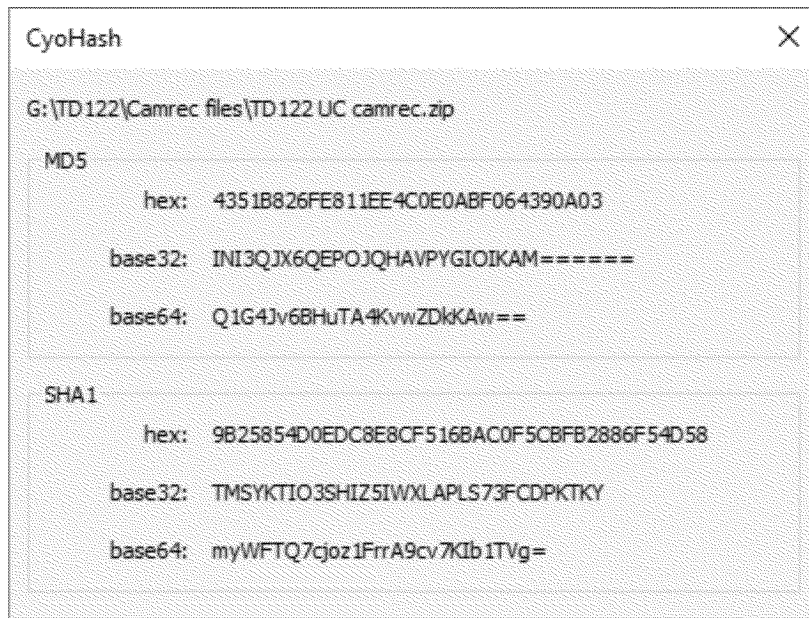


**Image 1** Hash values of recording file of investigative VM

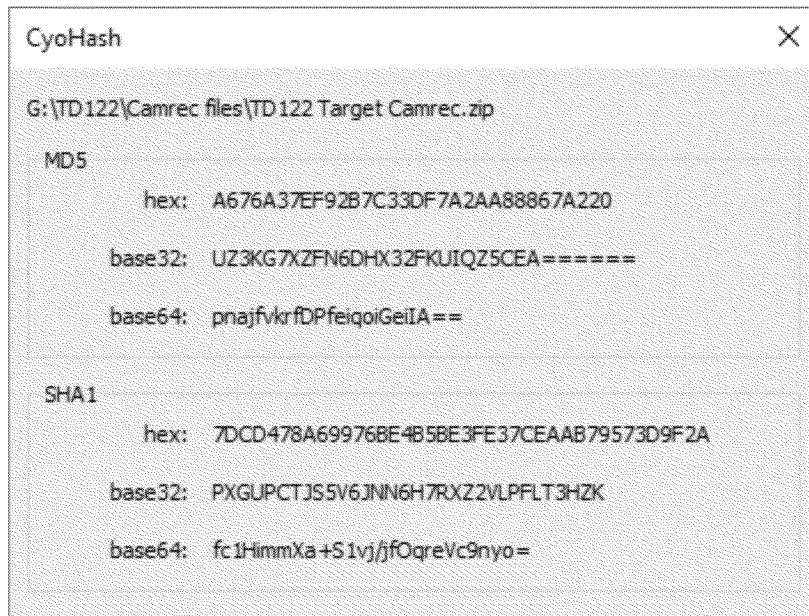


**Image 2** Hash values of recording file of target VM

- 2) Both recording files were then compressed into a .zip format using 7-Zip, and hash values were calculated and documented for these .zip files (images 3 and 4).

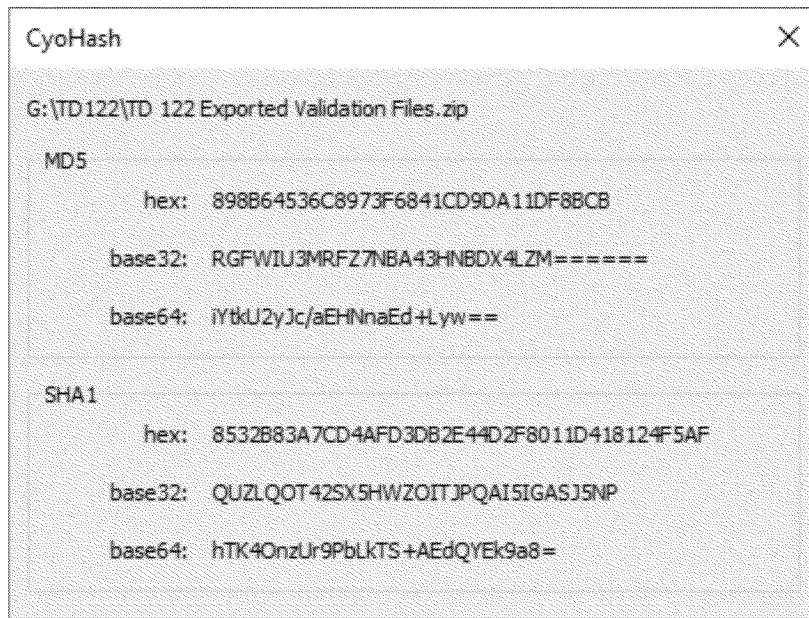


**Image 3** Hash values of compressed investigative VM recording



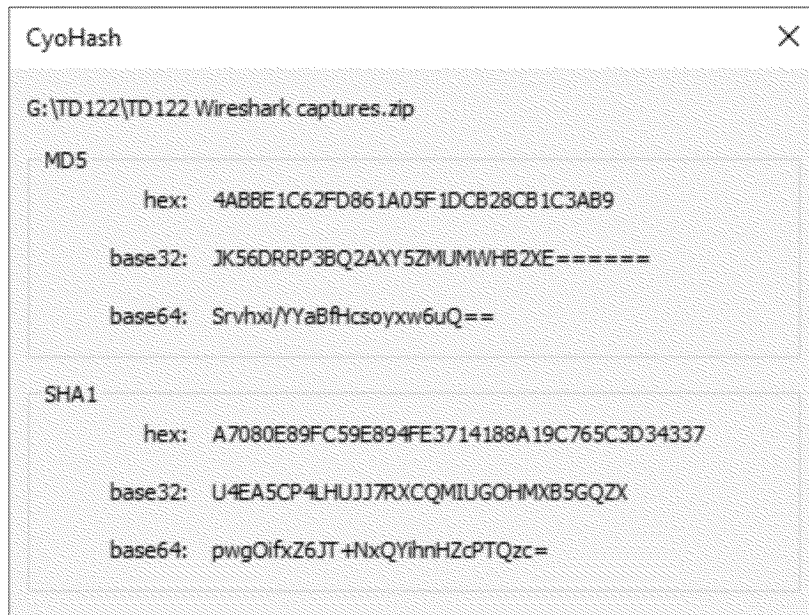
**Image 4** Hash values of compressed target VM recording

- 3) The validation .torrent file, Validation stock pictures folder, and the validation worksheet were transferred from both the investigative VM and target VM to a containing folder outside of the VM's. This containing folder was compressed into a .zip format using 7-Zip and a hash value calculated and documented for the .zip file using Cyohash (Image 5).



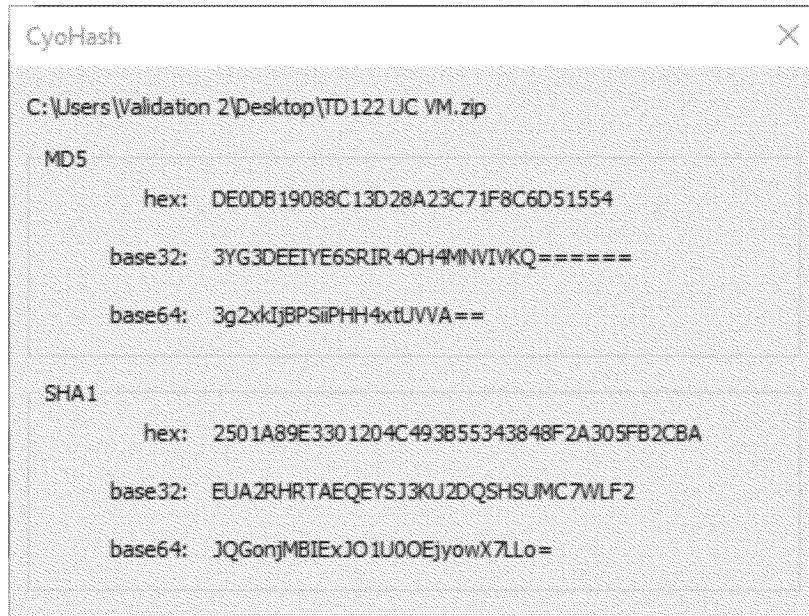
**Image 5** Hash values of the exported validation files from both UC and target VMs

- 4) The Wireshark captures were transferred from both the investigative VM and the target VM into a containing folder outside of the VMs. Once all files were successfully copied the folder was compressed into a password protected .zip file using 7-zip and a hash value was calculated and documented (Images 6). The password used for this .zip file will be included in a separate document.

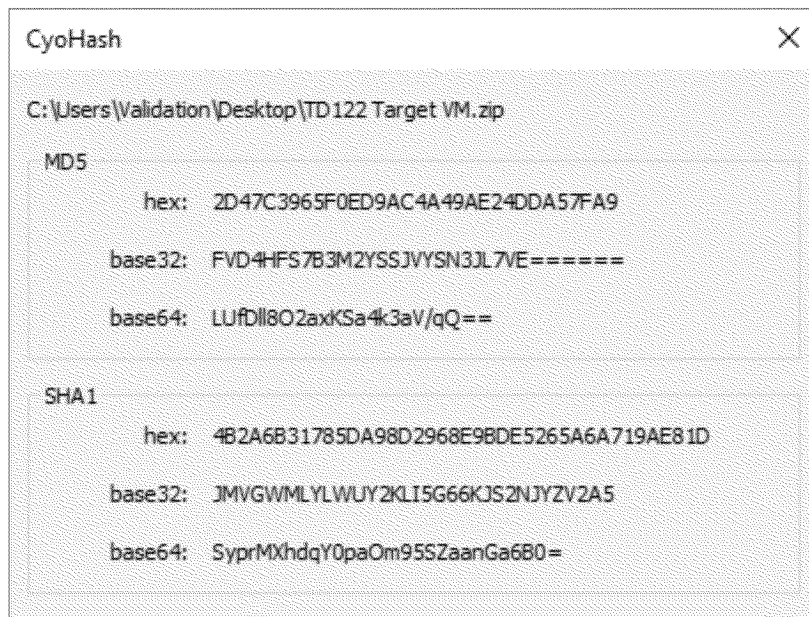


**Image 6** Hash values of compressed Wireshark captures from UC and target VM

- 5) Once all files were copied from both the investigative VM and target VM, they were both shut down, compressed into password protected .zip files using 7-zip and a hash value was calculated and documented for both .zip files (Images 7 and 8). The password used for both .zip files will be included in a separate document.



**Image 7** Hash values of compressed investigative VM



**Image 8** Hash values of compressed target VM

## F. ATTACHMENTS

- i. The BitTorrent Protocol Specification – written by Brian Cohen
- ii. Validation worksheet
- iii. Validation stock photos folder
- iv. Validation .torrent file

- v. Wireshark captures
- vi. Recording files for investigative VM
- vii. Recording files for target VM
- viii. Investigative VM
- ix. Target VM



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW WILLIAM SCHWIER,

Defendant.

Case No. 3:17-cr-00095-SLG

**AMENDED PROTECTIVE ORDER**

For the reason's set forth in the Court's Order re Motions for Reconsideration,<sup>1</sup>:

1. Not later than January 27, 2020, the government will provide a government-owned computer (the "TD Computer") at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The TD Computer shall be configured to the specifications provided by the defense on December 6, 2019.<sup>2</sup>
2. The only non-government persons who will have access to the TD Computer are Jeffrey Fischbach and Robert Herz

---

<sup>1</sup> See Docket 304.

<sup>2</sup> See Docket 280-1 at 1.

(collectively “the defense”).

3. Beginning on January 28, 2020, the defense will have access to the TD Computer for 30 consecutive calendar days of testing Torrential Downpour versions 1.15 and 1.23, the versions used in the investigation in this matter. Actual testing days are expected to be Monday through Friday only, exclusive of federal holidays.
4. Government personnel will have access to the TD Computer only for the purposes of keeping the TD computer secure consistently with OCRFCL standard operating procedures. Government personnel will not observe the defense testing.
5. Installation of Torrential Downpour software onto the TD Computer will occur as follows:
  - a. An FBI agent or Task Force Officer will keep exclusive possession of a USB drive or other removable media containing the Torrential Downpour software, except as provided in (b) and (c) below. The defense will not possess the Torrential Downpour software, other than on the TD Computer, except as provided in (b) and (c) below.

- b. Prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer. The FBI agent or Task Force Officer will remain outside the Defense Review room while Mr. Fischbach installs the software.
    - c. After the installation, Mr. Fischbach will remove the USB drive or other removable media containing the TD Software from the TD Computer and return it to the FBI agent or Task Force Officer.
6. The defense may bring digital media, computers, cell phones, and an internet hotspot (*i.e.* one that is compatible to connect to the TD Computer via WiFi or a network card) into the OCRCFL room with the TD Computer.
7. The defense will only connect to the TD Computer as necessary to complete its testing. The TD Computer may access the internet through the network card or via WiFi.
8. The defense will not remove the TD Computer from the OCRCFL.
9. The defense will not copy Torrential Downpour to any device

other than the TD Computer. The defense will not receive Torrential Downpour source code.

10. Neither the defense nor the TD Computer will have access to law enforcement's database of hash values from known child pornography images, known as "ICAC COPS."
11. The defense will not tamper with or open the TD Computer.
12. The Court reaffirms its prior protective order, entered at Docket 231.

DATED this 13th day of January, 2020, at Anchorage, Alaska.

/s/ Sharon L. Gleason  
UNITED STATES DISTRICT JUDGE

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW WILLIAM SCHWIER,

Defendant.

Case No. 3:17-cr-00095-SLG

**ORDER FOR GOVERNMENT TO REPLY TO DEFENSE’S RESPONSE IN  
OPPOSITION AT DOCKET 248 AND COMPELLING PRODUCTION OF  
VALIDATION TESTING RECORDS**

Before the Court at Docket 244 is the government’s motion proposing additional terms for the protective order governing production of the Torrential Downpour software.<sup>1</sup> Pursuant to the Court’s order at Docket 247, the defense has responded in opposition and filed a redlined copy of the government’s proposed order.<sup>2</sup> The defense disputes several elements of the government’s proposed protective order, including a term that would prohibit internet access during testing.<sup>3</sup> Having reviewed the defense’s opposition, the Court directs the

---

<sup>1</sup> See Docket 231 at 13–14 (entering protective order); see *also* Docket 243 at 8 (allowing government to “propose additional terms to the protective order entered at 231 as warranted”).

<sup>2</sup> Docket 248; see *also* Docket 249 (Decl. of Jeffrey Fischbach in support of Response in Opposition).

<sup>3</sup> Docket 248 at 2–3; see *also* Docket 249 at 5, ¶ 19 (“[I]n order to complete *any* of my proposed tests, and as a requirement of the software itself, I *must* have internet access.” (emphasis in original)); Docket 244 at 4 (proposing that software be tested on computer without access to the internet).

government to file a brief reply, giving special attention to the question of internet access.<sup>4</sup>

The defense's response in opposition also claims that the government has not yet produced the results of the November 4, 2019 validation testing of the Torrential Downpour software.<sup>5</sup> At the November 5, 2019 status conference, the government stated that it believed it could "overnight [the validation data] on Thursday, have it down to the Orange RCFL on Friday, the 8th [of November]."<sup>6</sup> According to the defense, Detective Erdely also indicated that he planned to prepare a report on the validation testing.<sup>7</sup> The Court hereby orders the government to produce to the defense the validation data and Detective Erdely's report immediately or, failing that, to explain why doing so is impossible in its reply.

Accordingly, IT IS ORDERED that the government shall file a reply to the defense's opposition no later than **November 20, 2019 at 5:00 p.m.** IT IS FURTHER ORDERED that the government shall produce the data from the November 5, 2019 Torrential Downpour validation and the accompanying report

---

<sup>4</sup> See L. Crim. R. 47.1(c) ("Unless otherwise ordered by the Court, no reply memorandum will be filed.").

<sup>5</sup> Docket 248 at 4.

<sup>6</sup> Docket 250 at 2:17–22 (Partial Tr. of Nov. 5, 2019 Status Conf.).

<sup>7</sup> Docket 250 at 5–8 (Defense counsel's stating that "Detective Erdely indicated that the earliest he thought he could have a package of data available for release, he wanted time to write a report, the earliest that could be ready would be Friday [November 8, 2019].").

to the Orange RCFL for review by the defense as soon as possible upon receipt of this order. If such production is impossible, the government shall provide an explanation in its reply.

DATED this 19th day of November, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason  
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, )  
 )  
 Plaintiff, )  
 ) Case No. 3:17-cr-00095-SLG-DMS  
 v. )  
 )  
 MATTHEW WILLIAM SCHWIER, )  
 )  
 Defendant. )  
 \_\_\_\_\_ )

**JUDGMENT OF PARTIAL DISCHARGE**

RE: COUNTS 1ssss and 2ssss  
FED.R.CRIM.P. 32(k)(1)

IT APPEARING that the defendant is now entitled to be discharged for the reason that:

X The court has granted the motion of the plaintiff for dismissal without prejudice of the offenses of Possession of Child Pornography and Distribution and Receipt of Child Pornography as charged in counts 1 and 2 of the Fourth Superseding Indictment.

**IT IS THEREFORE ADJUDGED** that the defendant is hereby discharged pursuant to Rule 32(k)(1), Federal Rules of Criminal Procedure.

**DATED** at Anchorage, Alaska, this 3rd day of February, 2020.

S/ Sharon L. Gleason  
Sharon L. Gleason  
United States District Judge

{DISCHARG-PARTIAL.WPD}



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW WILLIAM SCHWIER,

Defendant.

Case No. 3:17-cr-00095-SLG

**ORDER REGARDING C-3 MOTION TO COMPEL DISCOVERY AND  
PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR SOFTWARE**

Before the Court at Docket 199 is Defendant Matthew William Schwier’s C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour Software. The government responded in opposition at Docket 214 and filed supplemental briefing at Docket 219. Mr. Schwier filed supplemental briefing at Docket 221. An evidentiary hearing was held on October 17 and 18, 2019.

**BACKGROUND AND PROCEDURAL HISTORY**

On October 20, 2016, the Federal Bureau of Investigation (“FBI”) used software called “Torrential Downpour” to purportedly identify Mr. Schwier’s computer as possessing child pornography files that were available for download by third parties through BitTorrent, a peer-to-peer file-sharing network.<sup>1</sup> Torrential

---

<sup>1</sup> Docket 199 at 6; Docket 214 at 3. As described by Robert Erdely—offered by the government as an expert witness—a peer-to-peer network “allow[s] individuals unknown to each other and possibly separated by great distances to share files, such as audio and video files, freely.” Docket 214-1 at 2, ¶ 7 (Decl. of Mr. Erdely).

Downpour is a piece of software developed for law enforcement personnel, to allow them to identify BitTorrent users who possess or seek to possess child pornography files.<sup>2</sup> The software operates similarly to other BitTorrent clients—like uTorrent, the program Mr. Schwier allegedly used<sup>3</sup>—with several important differences.<sup>4</sup> Unlike most BitTorrent clients, Torrential Downpour allows law enforcement to download files from a single user,<sup>5</sup> and does not itself share any files downloaded pursuant to an investigation.<sup>6</sup> On October 20, 2016, Torrential Downpour was unable to download the alleged child pornography available for distribution on Mr. Schwier’s computer.<sup>7</sup>

In November 2016, the FBI again used Torrential Downpour to identify Mr. Schwier’s computer as possessing child pornography that was available for download.<sup>8</sup> Over the course of three days, the FBI used Torrential Downpour to

---

<sup>2</sup> Docket 214-1 at 5, ¶ 16.

<sup>3</sup> Docket 214 at 3.

<sup>4</sup> Docket 214-1 at 5–6, ¶¶ 18–20.

<sup>5</sup> Docket 214-1 at 6, ¶ 19. “Traditionally, BitTorrent seeks to download from many sharing computers to speed up the download times.” Docket 214-1 at 6, ¶ 19.

<sup>6</sup> Docket 214-1 at 6, ¶ 20.

<sup>7</sup> Docket 199 at 3–4; Docket 214 at 4.

<sup>8</sup> Docket 199 at 4–6; Docket 214 at 5.

download two files shared by Mr. Schwier's computer, one of which allegedly contained child pornography.<sup>9</sup>

In May 2017, the FBI seized multiple pieces of hardware from Mr. Schwier's home while executing a search warrant.<sup>10</sup> Forensic examination of the hardware identified multiple child pornography files, but could not find the particular files identified or downloaded by Torrential Downpour in October and November 2016.<sup>11</sup>

On August 16, 2017, the grand jury indicted Mr. Schwier on three counts of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2).<sup>12</sup> A September 25, 2017 superseding indictment additionally charged Mr. Schwier with one count of distribution of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).<sup>13</sup> On April 24, 2019, the grand jury returned a Third Superseding Indictment that charged Mr. Schwier with two counts of possession of child pornography and one count of distribution of child pornography.<sup>14</sup>

---

<sup>9</sup> Docket 199 at 6; Docket 214 at 5.

<sup>10</sup> Docket 199 at 6; Docket 214 at 6.

<sup>11</sup> Docket 199 at 7; Docket 214 at 6.

<sup>12</sup> Docket 2.

<sup>13</sup> Docket 40 at 3 (Count 3).

<sup>14</sup> Docket 138. A Second Superseding Indictment had been filed on March 20, 2019. Docket 117.

The FBI's October 20, 2016 use of Torrential Downpour to identify child pornography files on Mr. Schwier's computer forms the basis of Count 1 in the Third Superseding Indictment.<sup>15</sup> The FBI's use of Torrential Downpour to download child pornography from Mr. Schwier's computer in November 2016 forms the basis of Count 2 in the Third Superseding Indictment.<sup>16</sup> Count 3 of the Third Superseding Indictment relates to the child pornography files found during the 2017 physical search of Mr. Schwier's hardware and is not related to the FBI's use of Torrential Downpour.<sup>17</sup>

Mr. Schwier retained Robert M. Herz, his current defense counsel, on March 12, 2018.<sup>18</sup> Mr. Herz retained Jeffrey M. Fischbach as an expert in computer forensics at least as early as November 2018.<sup>19</sup> Despite this, Mr. Herz did not file the instant motion to compel production of the Torrential Downpour software—the

---

<sup>15</sup> Docket 199 at 6; Docket 214 at 3–4.

<sup>16</sup> Docket 199 at 6; Docket 214 at 5.

<sup>17</sup> Docket 138 at 3.

<sup>18</sup> Docket 63.

<sup>19</sup> Docket 203-1 at 2, ¶ 4 (Decl. of Mr. Fischbach) (describing Mr. Fischbach's November 2018 request to review alleged child pornography file downloaded from Mr. Schwier's computer). And Mr. Schwier's supplemental briefing indicates that Mr. Fischbach had begun developing his thoughts about "[t]he circumstances to be tested" should he gain access to Torrential Downpour in May 2019. Docket 221 at 5.

foundation for two counts in the Third Superseding Indictment—until September 12, 2019, one month before trial was scheduled to begin.<sup>20</sup>

### **DISCUSSION**

Mr. Schwier contends that Torrential Downpour “is flawed and should be tested and verified by a third party,” and that the defense requires access to the program in order to effectively cross-examine government witnesses.<sup>21</sup> Mr. Schwier seeks disclosure of an installable copy of Torrential Downpour, along with its user and training manuals.<sup>22</sup> He does not seek disclosure of Torrential Downpour’s source code.<sup>23</sup>

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E)(i), the government must disclose any “books, papers, documents, data . . . or copies or portions” thereof upon the defendant’s request, provided that the item is in the government’s control and is “material to preparing the defense.”<sup>24</sup> “A defendant

---

<sup>20</sup> Docket 199; Docket 175 (setting trial date for October 15, 2019).

<sup>21</sup> Docket 199 at 9.

<sup>22</sup> Docket 199 at 9.

<sup>23</sup> Docket 199 at 9. However, Mr. Fischbach did request a copy of the Torrential Downpour source code during his testimony. Docket 229 at 3:2–18 (Excerpt of 10/17/2019 Evidentiary Hearing Tr.). The Court denies that request for the reasons discussed below.

<sup>24</sup> The defense also bases its motion on the Supreme Court’s decision in *Brady v. Maryland*, 373 U.S. 83 (1963). The Court finds that case inapplicable and denies Mr. Schwier’s motion to the extent it seeks disclosure of Torrential Downpour under *Brady*. See *United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at \*7 (D. Ariz. Feb. 19, 2019) (discussing applicability of *Brady* and finding that

must make a ‘threshold showing of materiality’ in order to compel discovery pursuant” to this rule.<sup>25</sup> “Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.”<sup>26</sup>

In *Budziak*, the Ninth Circuit held that a district court had erroneously denied discovery of EP2P, a piece of investigative software similar to Torrential Downpour.<sup>27</sup> The Circuit concluded that the defendant had demonstrated materiality by “identif[ying] specific defenses to the distribution charge that discovery on the EP2P program could potentially help him develop.”<sup>28</sup> The defense has done the same here; he presented evidence, through the declaration and testimony of Mr. Fischbach, suggesting that Torrential Downpour may have “exploit[ed] vulnerabilities in the [BitTorrent] protocols” to download files that Mr.

---

“[d]efendants have made no showing that Torrential Downpour will prove to be exculpatory or could be used to impeach a government witness”).

<sup>25</sup> *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)).

<sup>26</sup> *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

<sup>27</sup> *Id.* at 1111–12.

<sup>28</sup> *Id.* at 1112.

Schwier had not made available for sharing.<sup>29</sup> Discovery of Torrential Downpour, then, could potentially help Mr. Schwier develop a defense to the distribution charge, as it is based solely on the FBI's use of the program to download files from Mr. Schwier's computer in November 2016.<sup>30</sup> Mr. Fischbach further explained, "it is critical to the defense . . . to understand how this software functions in order to determine its reliability and accuracy in identifying files reported as 'publicly available,'"<sup>31</sup> since Torrential Downpour's alleged October 20, 2016 identification of child pornography files on Mr. Schwier's computer is the sole basis for one of the possession charges.<sup>32</sup>

In light of this, the Court finds that Mr. Schwier has made the threshold showing of materiality required by Rule 16.<sup>33</sup> The Court further finds that the materiality of Torrential Downpour is limited to versions 1.15 and 1.23 of the

---

<sup>29</sup> Docket 200-1 at 7–8, ¶¶ 20–23; see also *Budziak*, 697 F.3d at 1112 (“[The defendant] submitted evidence suggesting that the FBI agents could have used EP2P software to override his sharing settings.”).

<sup>30</sup> See *Budziak*, 697 F.3d at 1112 (“Given that the distribution charge . . . was premised on the FBI's use of the EP2P program to download files from [the defendant], it is logical to conclude that the functions of the program were relevant to his defense.”).

<sup>31</sup> Docket 200-1 at 8, ¶ 24.

<sup>32</sup> Docket 200-1 at 9, ¶ 26; see also *Budziak*, 697 F.3d at 1112 (explaining that “[l]ike the competency of the drug-sniffing dog in [*United States v. Cedano-Areliano*, 332 F.3d 568, 571 (9th Cir. 2003)] the functions of the EP2P software constituted a ‘very important issue’ for Budziak’s defense”).

<sup>33</sup> See *Budziak*, 697 F.3d at 1112.

software—the versions used by the FBI during the events underlying the relevant counts in the Third Superseding Indictment.<sup>34</sup>

The government argues that even if the functionality, reliability, and accuracy of Torrential Downpour is material, disclosure of the software itself should be precluded by what it terms as a “law enforcement privilege.”<sup>35</sup> In *Rovario v. United States*, the Supreme Court recognized the government’s “privilege to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law.”<sup>36</sup> The Supreme Court explained that “no fixed rule with respect to disclosure is justifiable” and directed courts to balance the public interest against the defendant’s right to prepare his case, “taking into consideration the crime charged, the possible defenses, the possible significance of the informer’s testimony, and other relevant factors.”<sup>37</sup> Courts have since applied this law enforcement privilege to investigative software like Torrential Downpour.<sup>38</sup>

---

<sup>34</sup> Docket 229 at 2:6–11.

<sup>35</sup> Docket 214 at 8–11.

<sup>36</sup> 353 U.S. 53, 59 (1957).

<sup>37</sup> *Rovario v. United States*, 353 U.S. 53, 62 (1957).

<sup>38</sup> See, e.g., *United States v. Piroso*, 787 F.3d 358, 365–67 (6th Cir. 2015) (discussing the ShareazaLE software); *United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at \*8 (D. Ariz. Feb. 19, 2019) (discussing Torrential Downpour).



In *United States v. Gonzales*, the U.S. District Court for the District of Arizona recently applied the *Rovario* balancing test to Torrential Downpour, concluding that disclosure of an installable copy of the software to the defense was not warranted:

Child pornography is a scourge, victimizing the most innocent for the basest of reasons. The government has a legitimate interest in preserving its ability to investigate and prosecute distribution of this material—distribution that creates the market and fuels the demand for creation of more child pornography. Agent Daniels testified that the government’s investigative efforts would be severely hampered if a copy of Torrential Downpour got into the wrong hands. Countermeasures could be developed that would thwart law enforcement’s monitoring of the BitTorrent network for suspected child pornography.<sup>39</sup>

The district court in *Gonzalez* did, however, allow the defense’s expert to conduct certain testing of Torrential Downpour in a controlled setting at a secure government facility.<sup>40</sup>

The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that “child pornography distributors could find a way to avoid detection” if the workings of Torrential Downpour were made public, “render[ing]

---

<sup>39</sup> No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at \*8 (D. Ariz. Feb. 19, 2019).

<sup>40</sup> *Id.*; see also *United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 4040531, at \*4–7, \*10 (D. Ariz. Aug. 27, 2019) (specifying which tests the defense was permitted to run). The government’s proposed validation protocol in this case tracks the August 2019 *Gonzalez* testing closely. See Docket 219 at 3 (comparing *Gonzalez* tests and government’s proposed validation protocol); see also Docket 219-1 (government’s proposed validation protocol).

that tool of law enforcement ineffective.”<sup>41</sup> At the evidentiary hearing, Mr. Erdely testified that “to give [the defense] unfettered access to this software puts law enforcement and ten years of development at risk” because it would reveal certain aspects of Torrential Downpour’s operation.<sup>42</sup>

Given the government’s strong interest in retaining control of Torrential Downpour, the Court finds that disclosure of the software itself is not warranted, at least as of this juncture. The government has proposed to allow the defense to examine Torrential Downpour’s operation while it is run by a government expert in a controlled environment.<sup>43</sup> Mr. Erdely testified that this validation process, which includes packet capture by a program called “Wireshark,” would address the defense’s questions about Torrential Downpour’s functionality, accuracy, and ability to exploit vulnerabilities in the BitTorrent protocol.<sup>44</sup>

The Court acknowledges Mr. Schwier’s interest in understanding the operation of Torrential Downpour as it relates to his defense, and the Court concludes based on the present record that the validation process proposed by

---

<sup>41</sup> Docket 214-1 at 7, ¶ 23.

<sup>42</sup> Docket 230 at 8:25–9:2 (Excerpt of 10/18/2019 Evidentiary Hearing Tr.). *But see* Docket 221 at 2–3 (defense argument that Mr. Fischbach is trustworthy and is “a firewall” that will prevent Torrential Downpour’s dissemination to the public).

<sup>43</sup> See Docket 219-1 (proposed validation process).

<sup>44</sup> Docket 230 at 9–17; see *also* Docket 230 at 10:24–11:5 (“[I]f there was a vulnerability and our software was designed to exploit these vulnerabilities, . . . it would be exposed in the Wireshark packet capture.”).

the government is sufficient to meet the defense's needs. Mr. Fischbach had multiple opportunities to identify specific deficiencies in the government's proposed validation protocol, but was not able to do so in a way that persuaded the Court that additional or more extensive testing was necessary.<sup>45</sup> Mr. Fischbach testified that the proposed testing would not show how two features of Torrential Downpour—single-source downloading and the inability to upload—affect the BitTorrent protocol, if at all.<sup>46</sup> But when asked about the materiality of this information, Mr. Fischbach was only able to speak in vague generalities, claiming attorney-client privilege.<sup>47</sup> And while the defense contends that it has begun to formulate tests for Torrential Downpour that may be helpful to the defense, it has not identified these tests or explained how they differ from the government's

---

<sup>45</sup> Docket 230 at 2–8 (Mr. Fischbach discussing the government's proposal). Mr. Fischbach, in his first declaration, expressed a concern that Torrential Downpour was exploiting vulnerabilities in either BitTorrent itself or in BitTorrent clients, such as uTorrent. Docket 200-1 at 7, ¶¶ 20–21. But Mr. Erdely persuasively testified that the specific uTorrent exploit identified by Mr. Fischbach had been resolved in 2014, well before the events of this case. Docket 214-1 at 12, ¶ 33. Moreover, as explained above, Mr. Erdely also persuasively testified that the use of packet capture, as specified in the government's proposed validation protocol, would reveal whether Torrential Downpour exploited any vulnerabilities. Docket 230 at 10:24–11:5.

<sup>46</sup> Docket 230 at 3:20–4:2, 6:3–16.

<sup>47</sup> Docket 230 at 6:24–7:4 (“[T]he findings that we have, and, again, I’m being careful as far as privilege goes, the findings that we have have demonstrated some oddities possibly, but, again, they have to be tested to see if they are associated, but they certainly cause concern.”).

proposed validation protocol, claiming that the defense's proposed testing ideas are confidential attorney work product and subject to the attorney-client privilege.<sup>48</sup>

The Court cannot rule on the materiality of forensic tests that have not been disclosed to it. But the Court will accord the defense one last opportunity to explain what additional testing it is seeking and why. Accordingly, within **seven days of this order**, the defense may file a supplemental declaration of its expert that: (1) explains the specific hypotheses the defense seeks to test; (2) describes with particularity the test(s) the defense seeks to conduct; and (3) identifies the specific hardware and configurations necessary to complete that testing. The declaration shall also clearly explain why the government's proposed validation testing would not be adequate. This declaration may be filed ex parte or redacted, but only to the extent necessary to protect confidential attorney work product and/or privileged attorney-client communications.

### **CONCLUSION**

In light of the foregoing, the motion at Docket 199 is GRANTED IN PART and DENIED IN PART.

IT IS HEREBY ORDERED that the validation process described at Docket 219-1 shall be carried out for versions 1.15 and 1.23 of the Torrential Downpour

---

<sup>48</sup> Docket 221 at 5–6; see *also* Docket 221 at 4 (“The defense in this case wants to run a specific examination to test for a particular hypothesis, a particular condition that the defense believes it may have uncovered.”).

software on November 4, 2019, and on November 5, 2019 as necessary. The validation shall take place in a secure setting at a government location in Anchorage, Alaska that is selected by the government. Defense counsel and Mr. Fischbach may be present and may observe the validation process.

As discussed on the record,<sup>49</sup> the Court further enters a protective order with regard to the validation process as follows:

1. Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person without prior order of the Court.
2. Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this

---

<sup>49</sup> Docket 230 at 8:14–20.

case, provided the materials are filed under seal and/or submitted to the Court for *in camera* inspection.

3. Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.

In the event a timely supplemental expert declaration is filed by the defense, the Court may amend this order as warranted after the government has had an opportunity to respond.

DATED this 24th day of October, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason  
UNITED STATES DISTRICT  
JUDGE

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW WILLIAM SCHWIER,

Defendant.

Case No. 3:17-cr-00095-SLG

**ORDER RE MOTIONS FOR RECONSIDERATION**

Before the Court at Docket 255 and Docket 256 are the government and the defense's respective Motions for Partial Reconsideration of the Court's order at Docket 254.

**BACKGROUND**

The factual background of this case is well known to the parties and is condensed here as relevant to the pending motions. On September 12, 2019, the defense filed a motion seeking the production of the Torrential Downpour software.<sup>1</sup> On October 17 and 18, 2019, the Court heard extensive testimony from government and defense experts regarding the materiality of independent defense testing of the Torrential Downpour software. On October 24, 2019, the Court entered an order that granted in part and denied in part the defense's motion

---

<sup>1</sup> Docket 199.

to compel production of Torrential Downpour.<sup>2</sup> The Court there found that the functionality, reliability, and accuracy of Torrential Downpour were material to Mr. Schwier's defense,<sup>3</sup> but that a validation test performed by the government would be "sufficient to meet the defense's needs" under the balancing test set forth in *Roviaro v. United States*, 353 U.S. 53 (1957).<sup>4</sup>

However, the Court's October 24, 2019, order allowed the defense to file a supplemental declaration of its expert to explain why it believed that additional testing was necessary, and the Court notified the parties that it may amend its order in light of that declaration.<sup>5</sup> On October 31, 2019, the defense filed a supplemental ex parte declaration of Jeffrey M. Fischbach, which described four additional tests he sought to conduct with the Torrential Downpour software.<sup>6</sup> The defense filed a redacted copy of Mr. Fischbach's declaration on the same day, from which it had removed all information claimed as privileged, including the entire

---

<sup>2</sup> Docket 231; *see also* Docket 199 (motion).

<sup>3</sup> Docket 231 at 7–8.

<sup>4</sup> Docket 231 at 10–11. *Roviaro* directs courts determining whether to apply the law enforcement privilege to balance the public interest against the defendant's right to prepare his defense, "taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors." 353 U.S. at 62.

<sup>5</sup> Docket 231 at 12, 14.

<sup>6</sup> Docket 233.



description of the four tests.<sup>7</sup>

On the government's motion,<sup>8</sup> the Court held a brief status conference on November 4, 2019, after which the parties conducted validation testing of Torrential Downpour pursuant to the October 24, 2019 order.<sup>9</sup> The Court held a second status conference the next day, and on November 8, 2019, ordered the production of Torrential Downpour for defense testing at the Orange County Regional Computer Forensics Lab ("OCRCFL"), "limited to the four tests described in Mr. Fischbach's October 31, 2019 declaration."<sup>10</sup>

The Court's November 8, 2019, order allowed the government to "propose additional terms to the protective order entered at Docket 231 as warranted."<sup>11</sup> The government did so on November 15, 2019,<sup>12</sup> and after yet more briefing, on November 22, 2019, the Court entered a supplemental protective order to govern the defense's testing of the Torrential Downpour software.<sup>13</sup> The order required

---

<sup>7</sup> Docket 234.

<sup>8</sup> Docket 235.

<sup>9</sup> Docket 243 at 2.

<sup>10</sup> Docket 243 at 2, 7–8.

<sup>11</sup> Docket 243 at 8.

<sup>12</sup> Docket 244. The defense's Response in Opposition is at Docket 248, and the government's Reply is at Docket 253.

<sup>13</sup> Docket 254. The original protective order is at Docket 244.

the government to provide a computer to run Torrential Downpour (the “TD Computer”), while the defense could bring its own computers to connect to the TD Computer with an internet hotspot.<sup>14</sup> Paragraph 6 of the order provided that “[g]overnment personnel will have access to the TD Computer only for the purposes of starting the TD Computer, entering the password for the defense, and keeping the TD [C]omputer secure consistently with OCRFCL standard operating procedures.”<sup>15</sup> Paragraph 7 required Mr. Fischbach to install Torrential Downpour onto the TD Computer in the presence of an “FBI agent or Task Force Officer.”<sup>16</sup> Paragraph 9 provided that “[t]he TD Computer will contain one network card,” and that “[t]he defense will not make any connections to the TD Computer other than through the network card.”<sup>17</sup> The November 22, 2019 order did not require the defense to use the packet capture program WireShark during its testing of Torrential Downpour.<sup>18</sup>

The government filed a Motion for Partial Reconsideration at Docket 255,

---

<sup>14</sup> Docket 254 at 3, 5.

<sup>15</sup> Docket 254 at 4.

<sup>16</sup> Docket 254 at 4.

<sup>17</sup> Docket 254 at 5. Paragraph 8 of the November 22, 2019, Protective Order specified that the defense would be required to connect to the TD Computer using an internet hotspot “that is compatible to connect to the TD Computer via the network card.” Docket 254 at 5.

<sup>18</sup> Docket 254 at 2.

requesting that the Court require the defense's use of "Wireshark or another appropriate packet-capture software" to detect whether Torrential Downpour had been copied from the TD Computer.<sup>19</sup>

The defense filed its own Motion for Partial Reconsideration at Docket 256, requesting that the Court amend the November 22, 2019, order to allow Mr. Fischbach to enter the password on the TD Computer himself, install Torrential Downpour without supervision, and to "connect to the TD . . . Computer as necessary to complete its testing."<sup>20</sup>

The Court held a hearing on the parties' cross-motions for partial reconsideration on November 26, 2019. At the hearing, the Court ordered the government to file a response to the defense's motion after it had consulted with the FBI.<sup>21</sup> The Court emphasized at that hearing that it was "not asking the government to propose additional testing," but rather was asking the government "to respond to the defense motion for reconsideration . . . and tell [the Court] what you disagree with and agree with."<sup>22</sup> The Court further explained it sought for the

---

<sup>19</sup> Docket 255 at 2–4.

<sup>20</sup> Docket 256; Docket 256-1 at 2–3 (proposed order).

<sup>21</sup> Docket 302 at 6:22–9:9.

<sup>22</sup> Docket 302 at 7:15–19.

government “to respond to this issue of WiFi versus Ethernet, the issue of how many access . . . ports into the computer, the issue of the copying as articulated here, and tell me what the government’s position is on those.”<sup>23</sup> The government responded that the “subject matter experts at the [FBI] . . . [would] need until December 13th to come up with that.”<sup>24</sup>

The Court’s instructions notwithstanding, the government on December 20, 2019, filed a status report that attached an entirely new proposed testing protocol.<sup>25</sup> As correctly observed by the defense, in filing this proposed new protocol, some three months after the defense motion was filed, and two months after the evidentiary hearing, “[t]he government has seemingly repudiated the testing protocol as provided for in the Court’s orders at 231, 243, and 254 the terms of which the government previously had agreed to.”<sup>26</sup> The author of the proposed new protocol is not identified; it appears to have been created by one or more

---

<sup>23</sup> Docket 302 at 8:7–11.

<sup>24</sup> Docket 302 at 8:14–17.

<sup>25</sup> Docket 288. The government’s filing incorrectly states “[a]t the hearing on November 26, 2019, the Court ordered the government to submit a revised protective protocol.” Docket 288 at 2. By filing a new proposed testing protocol with its response to the defense’s Motion for Partial Reconsideration, a full two months after the initial evidentiary hearing regarding defense testing of Torrential Downpour, the government disregarded the Court’s clear instruction on the record to restrict its filing to a direct response to the defense’s reconsideration motion.

<sup>26</sup> Docket 296 at 2.

unidentified FBI agents.<sup>27</sup> The government states that it is willing to provide testimony from unidentified person(s) to explain its new proposal.<sup>28</sup> The defense filed a response to the government's filing at Docket 296 and an accompanying Supplemental Declaration of Mr. Fischbach at Docket 297. Given this record, the Court declines to consider the government's newest proposed protocol.

Separately, December 19, 2020, the government filed a Fourth Superseding Indictment in the case.<sup>29</sup> The new indictment adds a fourth count to the charges against Mr. Schwier: receipt of child pornography on or about November 18, 2015.<sup>30</sup>

## DISCUSSION

The Court will address the parties' respective motions for reconsideration separately, beginning with the defense's motion at Docket 256.

### 1. Defense's Motion at Docket 256

The defense contends that the November 22, 2019, Protective Order

---

<sup>27</sup> See Docket 288-1 at 1 (“[T]he FBI determined the following test conditions are necessary to sufficiently protect the software from unauthorized disclosure.”).

<sup>28</sup> Docket 288 at 2. In a January 13, 2020, Status Report, the government clarified that it would present Detective Erdely “to provide expert testimony regarding the [proposed] Test Environment.” Docket 303 at 2.

<sup>29</sup> Docket 279.

<sup>30</sup> Docket 279 at 3.

contains three “manifest error[s] of fact.”<sup>31</sup> The defense argues that the first of these is “paragraph 9[,] which limits the defense to the use of one port and network connection” on the TD Computer.<sup>32</sup> The defense maintains that this paragraph prohibitively limits Mr. Fischbach’s ability to complete his testing of the software by “prevent[ing] him from installing industry accepted software and hardware as well as well as prevent[ing] him from removing his test results from the [TD Computer] for further examination and analysis on his own equipment.”<sup>33</sup> And Mr. Fischbach states in his declaration that he “need[s] access to multiple computer ports and network connections to run [his] tests.”<sup>34</sup> The government does not meaningfully respond to the defense’s argument. It contends only that the defense’s argument is moot in light of the government’s new proposed testing protocol, which would allow the defense “to use screens, keyboards, and mice.”<sup>35</sup>

Mr. Fischbach, in his declaration, persuasively explains why he requires access to multiple ports on the TD Computer in order to complete the testing

---

<sup>31</sup> Docket 256 at 1–3; see L. R. Civ. P. 7.3(h)(1)(A) (“A court will ordinarily deny a motion for reconsideration absent a showing of . . . [a] manifest error of the law or fact.”).

<sup>32</sup> Docket 256 at 2.

<sup>33</sup> Docket 256 at 2.

<sup>34</sup> Docket 257 at 8, ¶ 5(e); see also *id.* at 2, ¶ 2.

<sup>35</sup> Docket 288 at 3–4. As noted above, the Court declines to address the new protocol, which it considers to be improperly filed.

authorized by previous order of this Court.<sup>36</sup> And the government has not explained how restricting the defense's access to ports on the TD Computer is necessary to protect Torrential Downpour's integrity as a law enforcement tool. The Court will therefore grant the defense's motion to reconsider with respect to paragraph 9 of the November 22, 2019, protective order.

The defense next argues that "Paragraphs 6 and 7 of the . . . [November 22, 2019,] order . . . compromise attorney-client privilege and attorney work product by intruding upon the confidential and independent defense testing process."<sup>37</sup> The defense contends that Paragraph 6's provision that government personnel start and enter the password on the TD Computer "inserts the government into the defense chain of custody and also makes it impossible for Mr. Fischbach to be held accountable for securing either the [Torrential Downpour] software or his own results as the government now has access to defense work product."<sup>38</sup> The defense maintains that "the only person who should have sole access to defense work product is Mr. Fischbach, and as such he should have sole and exclusive

---

<sup>36</sup> Docket 257 at 8, ¶ 5(e); see also *id.* at 2, ¶ 2.

<sup>37</sup> Docket 256 at 3. "The work-product doctrine protects 'from discovery documents and tangible things prepared by a party or his representative in anticipation of litigation.'" *United States v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011) (quoting *Admiral Ins. Co. v. U.S. Dist. Ct.*, 881 F.2d 1486, 1494 (9th Cir. 1989)).

<sup>38</sup> Docket 256 at 3.

possession of any passwords.”<sup>39</sup> In his declaration, Mr. Fischbach explains that under the terms of Paragraph 6, the personnel responsible for powering on and logging into the TD Computer “would be able to see my examination progress each time they have to log me back into the system . . . , as well as hold exclusive possession of the password to access it while I am away.”<sup>40</sup>

The defense further maintains that the way that Mr. Fischbach configures the TD Computer would reveal to a knowledgeable observer information about the type of testing he plans to conduct.<sup>41</sup> The defense therefore contends that Paragraph 7’s provision that an FBI agent may observe Mr. Fischbach install Torrential Downpour onto the TD Computer risks divulging privileged information.<sup>42</sup> Mr. Fischbach states in his declaration that “[a] technically knowledgeable Agent can learn a lot simply from the hardware configuration and setup and the software I am using to perform the tests I need to conduct.”<sup>43</sup>

The government argues in its response that the defense’s assertion of

---

<sup>39</sup> Docket 256 at 3.

<sup>40</sup> Docket 257 at 4, ¶ 5(a).

<sup>41</sup> Docket 256 at 3.

<sup>42</sup> Docket 256 at 3–4.

<sup>43</sup> Docket 257 at 4, ¶ 5(a); see also *id.* at 6, ¶ 5(b) (Mr. Fischbach explaining that configuration of TD Computer would occur before installation of Torrential Downpour and “necessarily make the observing agent privy to attorney client privilege”).



privilege is deficient because “Torrential Downpour is the government’s software”; because “the presence of the computers and software at the OCRCFL [and] Mr. Fischbach’s use of them to prepare for trial . . . are not privileged information”; and because Mr. Fischbach had previously referred to his testing methods as adhering to the “industry standard.”<sup>44</sup> The government’s argument misses the mark. The defense does not claim that Torrential Downpour itself or the mere use of computers or software at OCRCFL constitute privileged work product. Rather, the defense asserts privilege regarding the tests Mr. Fischbach will perform on Torrential Downpour using that hardware and software.<sup>45</sup> The nature of the tests that Mr. Fischbach intends to conduct on Torrential Downpour and the results thereof are clearly privileged.<sup>46</sup> As the government itself notes, “[t]he work-product doctrine covers documents or the compilations of materials prepared by agents of the attorney in preparation for litigation.”<sup>47</sup>

---

<sup>44</sup> Docket 288 at 6–7.

<sup>45</sup> Docket 296 at 8–9.

<sup>46</sup> The Court does not understand Mr. Fischbach to have asserted that the tests themselves were standard, but rather that they complied with industry-accepted standards. See Docket 296 at 9.

<sup>47</sup> Docket 288 at 4 (quoting *United States v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011)); see also *Hernandez v. Tanninen*, 604 F.3d 1095, 1100 (9th Cir. 2010) (“The work product doctrine is a qualified privilege that protects certain materials prepared by an attorney acting for his client in anticipation of litigation.”).

Mr. Fischbach has persuasively explained that granting the government exclusive password access to the TD Computer and allowing government agents to observe his configuration of that computer would compromise privileged attorney work-product. The government has not introduced evidence to the contrary and maintains only that password-protection is necessary to prevent “the defense from bypassing certain,” unspecified, “protections by powering down the computer and then restarting testing without the protections being activated.”<sup>48</sup> The Court finds this vague and unsupported assertion unconvincing and will grant the defense’s motion with respect to Paragraphs 6 and 7 of the November 22, 2019, Protective Order.

Finally, the defense contends that Paragraph 8’s requirement that Mr. Fischbach utilize “an internet hotspot . . . that is compatible to connect to the TD Computer via the network card,” is erroneous because “[t]here is no valid basis to restricting the defense to a wired Ethernet connection.”<sup>49</sup> The defense requests an amendment allowing Mr. Fischbach to connect to the TD Computer using a standard WiFi connection.<sup>50</sup> The government explained at the November 26,

---

<sup>48</sup> Docket 288 at 2–3.

<sup>49</sup> Docket 256 at 4.

<sup>50</sup> Docket 256 at 4.

2019, hearing that the term requiring an ethernet connection had been proposed “because [the government’s] understanding is it would not be possible for [Mr. Fischbach] to use WiFi at the RCFL,” and that “[t]he intent was to identify for him what he would need to do to connect.”<sup>51</sup> The Court concludes from this that Paragraph 8’s Ethernet requirement serves no valid security purpose, and will therefore grant the defense’s motion with respect to the use of WiFi to connect to the TD Computer, to the extent that it is possible to establish a WiFi connection under the OCRCFL’s normal operating procedures.

## **2. Government’s Motion at Docket 255**

The November 22, 2019, Protective Order did not require the defense to use WireShark during its testing of Torrential Downpour. The Court there explained:

The government proposes that the protective order contain a term providing that “[a]ll communications with the Torrential Downpour computer will be preserved via Wireshark.” The defense objects, contending that “[t]he [C]ourt has no more authority under Criminal Rule 16 to impose a duty on the defense to create evidence than it has to impose such a duty on the government.” The Court agrees with the defense on this point, and will not order the defense to use WireShark during its testing of Torrential Downpour.<sup>52</sup>

In its Motion for Partial Reconsideration, the government argues that the protective order “overlooked, and did not address, an important reason the government seeks

---

<sup>51</sup> Docket 302 at 6:13–18.

<sup>52</sup> Docket 254 at 2 (internal citations omitted).

a protective order with Wireshark or another appropriate packet-capture software: *i.e.* detecting digital copying of Torrential Downpour from the TD Computer.”<sup>53</sup>

The Court recognizes the government’s concern that “the defense could inadvertently copy Torrential Downpour” onto their own equipment but will not grant the government’s motion on this basis. However, the Court finds Mr. Fischbach to be responsible and in possession of technical expertise such that he would be unlikely to unwittingly copy Torrential Downpour and remove it from the OCRCFL.<sup>54</sup> And the Court has expressly ordered the defense not to copy Torrential Downpour and expects compliance with that order. The Court sees no reason to revisit its decision regarding WireShark and will therefore deny the government’s Motion for Partial Reconsideration.

### **3. Miscellaneous Issues Raised in the Government’s Response**

In addition to responding to the defense’s motion for partial reconsideration, the government’s response at Docket 288 raises several additional issues. For reasons set out above, the Court will not here consider the government’s new

---

<sup>53</sup> Docket 255 at 2.

<sup>54</sup> A supplemental declaration filed by Mr. Fischbach indicates that the government, itself, believes him to be trustworthy. Mr. Fischbach states that the government inadvertently included two copies of Torrential Downpour on a thumb drive it provided to him on December 6, 2019. Docket 297 at 2, ¶ 2. Mr. Fischbach states that the government, upon realizing this, took no action besides reminding him not to copy the software from the thumb drive. Docket 297 at 2–3, ¶¶ 4–5.

testing protocol, which it proposed a full two months after the Court's first evidentiary hearing regarding the proper environment for defense testing of Torrential Downpour; the Court will, however, address the remaining issues here.

**a. Specifications of TD Computer**

The November 22, 2019, Protective Order clearly outlines the procedure by which the specifications for the TD Computer would be established. The order first requires the government to provide the defense with “all applicable TD software documentation for versions 1.15 and 1.23, *including installation instructions and minimum operating requirements.*”<sup>55</sup> The order next requires the defense to “provide the specifications for the computer that it is seeking for TD testing.”<sup>56</sup> Finally, the order requires the government to “provide a government-owned computer . . . that is configured to specifications that were timely provided by the defense.”<sup>57</sup> Only “[i]f the defense fails to timely provide such specifications,” may “the government . . . select the computer it will provide.”<sup>58</sup>

On November 25, 2019, the government provided the defense with a

---

<sup>55</sup> Docket 254 at 2.

<sup>56</sup> Docket 254 at 2–3.

<sup>57</sup> Docket 254 at 3.

<sup>58</sup> Docket 254 at 3.

redacted user manual for Torrential Downpour version 1.23.<sup>59</sup> Despite the defense's arguments to the contrary,<sup>60</sup> the Court finds that this user manual fulfilled the government's obligation to provide the defense with Torrential Downpour's minimum operating requirements.<sup>61</sup> On December 6, 2019, the Defense timely complied with its obligation to provide the government with system specifications for the TD Computer.<sup>62</sup> Under the terms of the November 22, 2019, Protective Order, the government is now required to provide the defense with a computer that is configured to the specifications supplied by the defense.<sup>63</sup>

The government nevertheless objects to the defense's technical specifications, maintaining that at the November 26, 2019, hearing, "the Court ordered the government to respond to the defense's objections to the computer

---

<sup>59</sup> See Docket 259 (Government's Notice Regarding Partial Compliance with Order (Dkt 254 and Correction of Record). The parties dispute the appropriateness of the government's redactions, see Docket 282 (Defense's C-5 Motion to Compel), an issue which the Court will address in a separate order after reviewing the relevant materials in camera.

<sup>60</sup> See Docket 296 at 12 n.9 ("The government's claim that it provided software specifications seems disingenuous at best.").

<sup>61</sup> Docket 299-1 at 8 (identifying operating system and programming model required to run Torrential Downpour).

<sup>62</sup> Docket 281-2 at 4. At the November 26, 2019, hearing, the Court extended the deadline to provide these specifications from November 27, 2019, to December 6, 2019. Docket 302 at 10:1-13.

<sup>63</sup> Docket 254 at 3.

the government will provide for testing.”<sup>64</sup> The Court disagrees, but has reviewed the transcript for that hearing and understands how the government reached that conclusion.<sup>65</sup> It will therefore address the government’s arguments. The government contends that the defense’s specifications “are not necessary to operate Torrential Downpour or uTorrent software and to conduct the types of industry-standard tests that the government expects the defense will perform.”<sup>66</sup> The government therefore asserts that the defense’s specifications “are unreasonable.”<sup>67</sup> The government provides no evidence, in the form of a declaration or otherwise, to support its contentions.

As the defense notes, the purpose of the TD Computer is to *test* Torrential Downpour, not to operate it.<sup>68</sup> It is therefore understandable that Mr. Fischbach would require more computing power than is necessary to simply operate the

---

<sup>64</sup> Docket 288 at 9.

<sup>65</sup> Docket 302 at 2:5–5:20.

<sup>66</sup> Docket 288 at 11.

<sup>67</sup> Docket 288 at 10. The government further maintains that “[b]ecause the defense has withheld from the government the specific characteristics of its proposed testing, the government cannot know with certainty what the defense’s actual requirements are.” Docket 288 at 10. This argument misunderstands the November 22, 2019 order; that order requires the government to provide a computer consistent with the specifications supplied by the defense, not consistent with what the government determines “the defense’s actual requirements are.” Docket 254 at 2–3.

<sup>68</sup> Docket 296 at 12–13.

software. Mr. Fischbach explains in his declaration that he “specifically chose[]” the specifications to “accommodate the forensic hardware and software [he] need[s] to install in order to both complete [his] testing and assure the [C]ourt that the machine has in no way been compromised during [his] testing, and that no software has been lost, stolen, or compromised.”<sup>69</sup> On this record, the Court finds that the specifications provided by the defense on December 6, 2019, are not only necessary for Mr. Fischbach to conduct his testing of Torrential Downpour, but also promote the government’s interest in ensuring that the testing is secure.

The Court will therefore order the government to provide the defense with a computer that is configured to the specifications identified at Docket 280-1 page 1, pursuant to the November 22, 2019, Protective Order.

**b. Location of Testing**

At the November 26, 2019, hearing, the Court directed the government to address whether the defense’s testing of Torrential Downpour could occur at the Sensitive Compartmented Information Facility (“SCIF”) at the federal building and courthouse in Los Angeles instead of the OCRCFL.<sup>70</sup> Having reviewed the

---

<sup>69</sup> Docket 261 at 7, ¶ 8.

<sup>70</sup> Docket 302 at 9:13–18.



parties' briefing on this issue,<sup>71</sup> the Court finds that it would not be appropriate to relocate testing to the SCIF. The defense notes that "the government has not raised any objection to moving the testing location to the FBI-Wilshire office," which it asserts "would be a more secure location than the RCFL."<sup>72</sup> If the parties can agree to relocate testing to the FBI-Wilshire office, they can notify the Court and the Court will so order. Unless and until such an agreement is reached, testing will be at the OCRCFL.

### CONCLUSION

In light of the foregoing, the government's Motion for Partial Reconsideration at Docket 255 is DENIED. The defense's Motion for Partial Reconsideration at Docket 256 is GRANTED.

The Court will separately issue an amended protective order consistent with this decision.

DATED this 13th day of January, 2020, at Anchorage, Alaska.

s/ Sharon L. Gleason  
UNITED STATES DISTRICT JUDGE

---

<sup>71</sup> See Docket 288 at 7–9; Docket 296 at 9–10.

<sup>72</sup> Docket 296 at 10.

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW WILLIAM SCHWIER,

Defendant.

Case No. 3:17-cr-00095-SLG

**SUPPLEMENTAL ORDER REGARDING C-3 MOTION TO COMPEL  
DISCOVERY AND PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR  
SOFTWARE**

On October 24, 2019, after an evidentiary hearing, the Court entered an order at Docket 231 that granted in part and denied in part Defendant Matthew William Schwier's C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour Software at Docket 199. The Court directed the government to conduct certain validation testing of the Torrential Downpour software in the presence of the defense.<sup>1</sup> The October 24, 2019 order set out the factual background relevant to this issue and it is not repeated here.<sup>2</sup>

The Court's October 24, 2019 order allowed the defense to file a supplemental declaration of its expert to explain why it believed additional testing was necessary, and the Court notified the parties that it may amend its order as

---

<sup>1</sup> Docket 231 at 12–14.

<sup>2</sup> See Docket 231 at 1–12.

warranted in light of that declaration.<sup>3</sup> On October 31, 2019, the defense timely filed a supplemental ex parte declaration of Jeffrey M. Fischbach, offered as a computer forensics expert.<sup>4</sup> The defense filed a redacted copy of Mr. Fischbach's declaration on the same day, from which it had removed all information it claimed as privileged.<sup>5</sup>

On November 1, 2019, the government filed a motion responding to Mr. Fischbach's redacted declaration, asking the Court to either hold an immediate status hearing or issue an order finding that the defense had not shown that additional tests were material.<sup>6</sup>

The Court granted the government's motion and held a brief status conference on November 4, 2019,<sup>7</sup> after which the parties conducted validation testing of the Torrential Downpour software pursuant to the Court's October 24, 2019 order.<sup>8</sup> The Court held a second status conference after the completion of the validation process, on November 5, 2019, at which it notified the parties that it

---

<sup>3</sup> Docket 231 at 12, 14.

<sup>4</sup> Docket 233.

<sup>5</sup> Docket 234.

<sup>6</sup> Docket 235.

<sup>7</sup> Docket 240.

<sup>8</sup> See Docket 231 at 12–13 (ordering government to conduct “the validation process described at Docket 219-1”).

would issue a written order that would address whether additional testing would be ordered in light of Mr. Fischbach's October 31, 2019 declaration.

### **DISCUSSION**

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E)(i), the government must disclose any “books, papers, documents, data . . . or copies or portions” thereof upon the defendant’s request, provided that the item is in the government’s control and is “material to preparing the defense.” “A defendant must make a ‘threshold showing of materiality’ in order to compel discovery pursuant” to this rule.<sup>9</sup> “Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.”<sup>10</sup>

In *United States v. Budziak*, the Ninth Circuit held that a district court had erroneously denied the defense’s request for discovery of EP2P, a piece of investigative software similar to Torrential Downpour.<sup>11</sup> The Circuit concluded that the defendant had demonstrated materiality by “identif[ying] specific defenses to

---

<sup>9</sup> *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)).

<sup>10</sup> *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

<sup>11</sup> *Id.* at 1111–12.

the distribution charge that discovery on the EP2P program could potentially help him develop.”<sup>12</sup> The Circuit cautioned:

In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless[,] . . . especially . . . where . . . a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software.<sup>13</sup>

It explained that “[a] party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately.”<sup>14</sup> In its October 24, 2019 order, the Court found that the functionality, reliability, and accuracy of Torrential Downpour were material to Mr. Schwier’s defense.<sup>15</sup>

However, the government asserted that production of the software was precluded by the law enforcement privilege recognized in *Roviaro v. United States*,

---

<sup>12</sup> *Id.* at 1112. The defendant in *Budziak* “presented evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his ‘incomplete’ folder, making it ‘more likely’ that he did not knowingly distribute any complete child pornography files to [federal] [a]gents.” *Id.* He also “submitted evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings.” *Id.*

<sup>13</sup> *Id.* at 1112–13.

<sup>14</sup> *Id.* at 12 (quoting *United States v. Leibert*, 519 F.2d 542, 547–48 (3rd Cir. 1975)).

<sup>15</sup> Docket 231 at 7–8.

353 U.S. 53 (1957).<sup>16</sup> Balancing the government’s interest against the defendant’s,<sup>17</sup> the Court found in its October 24, 2019 order that based on the record then before it, “the validation process proposed by the government [was] sufficient to meet the defense’s needs.”<sup>18</sup> The Court noted that Mr. Fischbach had spoken only in generalities at the evidentiary hearing about why production of the software for additional testing by him was necessary to the defense.<sup>19</sup> Mr. Fischbach claimed that the defense’s proposed testing ideas were confidential attorney work product and subject to the attorney-client privilege.<sup>20</sup> The Court concluded that it could not “rule on the materiality of forensic tests that have not been disclosed to it.”<sup>21</sup>

In the ex parte portion of his subsequent October 31, 2019 declaration, Mr. Fischbach described four additional tests of the Torrential Downpour software that

---

<sup>16</sup> Docket 214 at 8–11.

<sup>17</sup> See *Roviaro*, 353 U.S. at 62 (directing courts to balance public interest in protecting flow of information to government against defendant’s right to prepare his case, “taking into consideration the crime charged, the possible defenses, the possible significance of the informer’s testimony, and other relevant factors”).

<sup>18</sup> Docket 231 at 10–11.

<sup>19</sup> Docket 231 at 11.

<sup>20</sup> See, e.g., Docket 230 at 6:24–7:4 (Excerpt of October 18, 2019 Hearing Transcript) (“[T]he findings that we have, and again, I’m being careful as far as privilege goes, the findings that we have have demonstrated some oddities possibly, but, again, they have to be tested to see if they are associated, but they certainly cause concern.”).

<sup>21</sup> Docket 231 at 12.

he seeks to conduct at the Regional Computer Forensics Lab (“RCFL”) in Anaheim, California.<sup>22</sup> Mr. Fischbach explained that these four tests are necessary to either develop or rule out specific defense strategies related to Counts 1 and 2 of the Third Superseding Indictment, both of which are premised on the FBI’s use of the Torrential Downpour software.<sup>23</sup>

In the redacted copy of Mr. Fischbach’s declaration, the entire description of these four tests and their relevance to the defense are blacked out.<sup>24</sup> The government argues that “[b]y redacting the tests themselves, the defense has withheld from the government any opportunity to contest the tests, or to agree with them.”<sup>25</sup> The Court acknowledges the government’s concerns and recognizes that in *United States v. Gonzales*, the defense disclosed the actual tests it wanted to run on Torrential Downpour in a way that permitted the government to argue against the testing.<sup>26</sup> Nevertheless, the Court is prepared to balance the defense’s need for the additional testing of Torrential Downpour against the government’s interest in restricting further access to the software.

---

<sup>22</sup> Docket 233-1 at 7–10, ¶ 23; Docket 234-1 at 7–10, ¶ 23 (redacted).

<sup>23</sup> Docket 233-1 at 7–10, 11 ¶¶ 23, 28; Docket 234-1 at 7–10, 11 ¶¶ 23, 28 (redacted); see also Docket 231 at 4 (describing basis of counts in indictment).

<sup>24</sup> Docket 234-1 at 7–10, ¶¶ 23, 28.

<sup>25</sup> Docket 235 at 3.

<sup>26</sup> No. CR-17-01311-001-PHX-DGC, 2019 WL 4040531, at \*4–7 (D. Ariz. Aug. 27, 2019) (describing six tests and government’s objections to their materiality).

Upon review of Mr. Fischbach's October 31, 2019 declaration, the Court concludes that requiring the Torrential Downpour software to be accessible to Mr. Fischbach for the additional testing at the Anaheim RCFL is warranted. In reaching this conclusion, the Court has considered that the government's interest in prosecuting Mr. Schwier for child pornography is not eviscerated by ordering the software's production. The government may opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense. In that event, the government may still proceed on Count 3.<sup>27</sup> The Court also notes that the government would have the opportunity to assert that the conduct alleged in Counts 1 and 2 constitutes relevant conduct for sentencing purposes in the event Mr. Schwier is adjudged guilty on Count 3.

### **CONCLUSION**

In light of the foregoing, the Court supplements its order at Docket 231 as follows:

(1) **Within seven days of the date of this order**, the government shall make the Torrential Downpour software available to Mr. Fischbach and defense counsel at the Regional Computer Forensics Lab in Anaheim, California, for a

---

<sup>27</sup> *United States v. Gonzales*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at \*8 (D. Ariz. Feb. 19, 2019) ("When the two interests come squarely into conflict, the defendant's right to a fair trial should prevail because the government can always choose to protect its investigative technique by dropping the prosecution and due process dictates that a citizen should never be convicted in an unfair trial." (citing *United States v. Turi*, 143 F. Supp. 3d 916, 921 (D. Ariz. 2015))).



period of 21 consecutive days for additional testing. This testing shall be limited to the four tests described in Mr. Fischbach's October 31, 2019 declaration.

(2) The government may propose additional terms to the protective order entered at Docket 231 as warranted.

DATED this 8th day of November, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason  
UNITED STATES DISTRICT JUDGE

Robert M. Herz  
Law Offices of Robert Herz, P.C.  
431 W.7th Avenue, Suite 107  
Anchorage, Alaska 99501  
907-277-7171 Phone  
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

United States of America,                    )  
  )  
  )           Case No. 3:17-cr-0095 SLG-DMS  
  )  
vs.    )  
  )  
Matthew Schwier,                            )  
  )  
  )           Defendant.  
  )  
  )  
\_\_\_\_\_)

**SUPPLEMENTAL DECLARATION OF JEFFREY M. FISCHBACH IN  
SUPPORT OF DEFENDANT’S MOTION FOR PARTIAL  
RECONSIDERATION AT DOC.256**

I, Jeffrey M. Fischbach, declare as follows:

1. In its most recent motion at Doc. 255, the government continues to attempt to impose its self-serving protocols on the defense. This motion, in one stroke, serves to limit the defense to *only* being able to conduct Mr. Erdely’s own “validation”, and prevents the defense from completing its own tests, which the court has already ruled are material. The government’s sole assertion justifying its purported need for Wireshark is to prevent the accidental copying or distribution of its TD software. Implementing the use of WireShark does *nothing* to *actually prevent* the accidental or intentional distribution of its proprietary software. I would also note that, here again, the government makes no effort to even feign concern for potential harm to children -- commensurate with the charges. As such, the government continues to allow me unfettered access to

DECLARATION OF JEFFREY M. FISCHBACH

reb1

alleged child pornography *faciliated* by AUSA Jonas Walker, without so much as a protective order, while he continues to urge the court to impose arbitrary limitations on my ability to conduct tests, which even Walker himself, admits *do not* actually serve to prevent its software from “escaping into the wild”.

2. Specifically, I agree that Wireshark is a very useful tool to observe any nefarious *or* legitimate use of any computer computer IO (input-output) port, including wireless. Since I agree to this premise, it would seem the government’s need to call a witness is unnecessary just to testify to this fact. The government makes no assertion that Wireshark does *anything* to prevent the copying of its software. The fact is that it does not. Its only function is to record the transmission and receipt of data on the host device. According to Wireshark’s own website: “*What is Wireshark? Wireshark® is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network.*” ([https://www.wireshark.org/faq.html#\\_what\\_is\\_wireshark](https://www.wireshark.org/faq.html#_what_is_wireshark)). I agree that Wireshark -- if configured to do so, and if started, and if it is left uninterrupted, *by me* -- will record the [accidental] copying of TD. But only if all those things happen, and only if *I* allow that action to be recorded. What it will also record is every single element of my testing, as data is transmitted for testing purposes, moment-by-moment, in exhaustive detail. And the only way Mr. Walker will have the ability to even make the accusation that TD has been “released to the wild”, intentionally or accidentally, will be for him, or more likely, someone working for him, to decrypt and analyze my detailed recorded work product -- if so ordered by the court. And in doing so the government will have accessed attorney-client privileged data and obtained protected attorney work product information.

3. I am arguably one of the best equipped people on the planet to steal this software without anyone ever being the wiser. And I can do it *while* Wireshark is running. Now after questioning my credentials for almost two hours on the stand, Mr. Walker has pivoted to his “concern” that I might “accidentally” copy the

DECLARATION OF JEFFREY M. FISCHBACH

reb2

software. Perhaps Mr. Walker is prone to accidentally copying or deleting files on his own computer, but I have been working with sensitive files for a quarter-century. Many of the procedures used by the FBI today were first used and instructed by *me*. So long as I have complete and unfettered access to properly determine and configure the equipment I use for these tests, I will take all the aggressive file containment protocols that I *always* use when examining sensitive material. This however, will necessarily require me to configure all equipment myself, and have access to add and remove all necessary software as my time-tested and industry-accepted protocols dictate, which means I will need access to more than one port on the government provided computer. If I am allowed to do this I can safely guarantee the TD software will not be accidentally copied or distributed while under my control. Should I be required to use the computer as dictated by the government, without the ability to install or connect any previously tested and industry accepted software (much of which is specifically designed to protect data from any unintended use) or hardware to *any* port or connector on the computer, as needed, then not only can I not complete my tests, I would not be able to assure the court that all standard precautions had been taken.

4. Mr. Walker brings to the court's attention the theft of a hard drive I left in the *government's* custody, care, and control. In what can only be referred to as an opportunistic loose association with truth, Mr. Walker makes the unsubstantiated and false claim that "Mr. Fischbach has, already, *lost* a hard drive at the OCRCFL in this case." Mr. Walker is well aware, via his intrusive interrogation of my assigned RCFL liaison, Joseph Monroe, that Mr. Monroe did not describe my hard drive as being "lost". He described it as "missing" from the Defense Review room, where I am *required* to keep it, in order to allow me to continue processing data overnight or over the course of several days. Which, in order to complete my work for trial, without delay, is both necessary, and facilitated by the RCFL. Mr. Monroe has documented by email, dated July 2, 2019, his knowledge that the

DECLARATION OF JEFFREY M. FISCHBACH

reb3

processing (long periods of time the computer works without examiner input) of my examinations were ongoing, in my absence. He specifically requested my permission to allow someone to disconnect the equipment, in order for another examiner to use some of it. In an email from Mr. Monroe, solicited by Mr. Walker, documenting his observation of my examination, Mr. Monroe wrote the following: "*Only Fischbach and Herz came back on 25th. Fischbach advised he was missing an external hard drive that he left in the Defense Review room, during his last visit. We were unable to locate the missing external hard drive.*" As Mr. Monroe was aware, that drive was connected to the *government's* work station -- as it was when the work-station was in Anchorage, supervised by Kyle Reardon.

5. Despite my request to use two *significantly more* secure private exam sites -- FBI Wilshire, and Roybal Federal Court's SCIF, both of which I have successfully used many times without incident, and both of which are *significantly* shorter drives for me -- it is Mr. Walker who has insisted that I use the OCRCFL, where he is, apparently, able to maintain a closer watch on my work, and with whom I work. Mr. Walker should know, however, that unlike the FBI and LA SCIF, the OCRCFL offers *only* a shared work space where many different civilians and RCFL personnel come and go and even share much of the same equipment. I would agree that the OCRCFL is a location that *does* risk the possible theft, not only of TD, but of the *entire computer* upon which it is installed. Frankly I am surprised, given the government's purported concern about the security of its TD software that it has not readily accepted my offer for the defense testing to occur in the federal court SCIF. Not only can the OCRCFL not guarantee that items will not be stolen from its own Defense Exam room, it apparently does not take seriously its role in protecting details concerning the use of its defense work environment from the government. What Mr. Walker does not know from his heretofore unjustified intrusion into my RCFL work is whether the

DECLARATION OF JEFFREY M. FISCHBACH

reb4

*missing* drive, taken from the RCFL Defense Review room, when I was not present, was encrypted to secure its contents so that only I could personally decrypt them, or whether that encryption was set to wipe the drive upon unauthorized attempts to open it, or whether the drive had tracking measures installed, or whether that drive has since been found and returned to me thanks to any of the above measures. While Mr. Walker does not have an explanation for how Wireshark *in any way* prevents the theft or accidental copying of its software, (which it emphatically does not,) I can assure that court, given unfettered access to *all* testing equipment, that I *will* guarantee that, in my hands, the software will not escape the OCRCFL. I cannot, however, make the same guarantee for the TD copy the court's order requires be left with FBI or OCRCFL personnel.

6. Much like Mr. Walker knew that Internet access was *required* to test Torrential Downpour, he also knows that it was the RCFL that “lost” a hard drive left in *their* care. He also knows that in order for Wireshark to be used in the way he proposes, I would have to be *trusted*, unmonitored, by myself, to actually configure it the way he wants me to, and to use it, without interruption or log file alteration, to record *all* of my activity on the computer the government will provide. Moreover, like the TD secrets already accidentally exposed to me, and the missing hard drive I reported to the OCRCFL, the only way that the government would even know that their software escaped the RCFL lab is either if *I* can be trusted to report it to them, or if they actually plan on arbitrarily demanding the examination of the Wireshark recording they trusted *me* to make. By which time, given their self-imposed requirements, the software would be irretrievably lost to “the wild”. On the other hand, examination of these Wireshark logs by the government would give them a very complete reenactment of my tests; tests protected by attorney-client privilege and attorney work product doctrine.

7. As noted by the government, the court ordered, “On or before Monday,  
DECLARATION OF JEFFREY M. FISCHBACH

reb5

November 25, 2019, the government will provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements.” And that, “Not later than Wednesday, November 27, 2019, the defense shall provide to the government the specifications for the computer that it is seeking for TD testing.” The court clearly understands my limited ability to determine appropriate specifications for the hardware and equipment I need to test the software, without first being provided any documentation or specifications relating to the software to be tested. In its motion at Dkt. 255 the government has instead chosen to ignore the court’s order to provide complete documentation and equipment specifications, and ignores, as well, the equipment specifications I already provided without the benefit of the materials now ordered by the court. Mr. Walker instead has seemingly made the arbitrary decision to provide a piece of used equipment, similar to the vintage equipment it has already provided to the OCRCFL without any reference to the specifications provided to him by the defense already. Mr. Walker has nowhere in Dkt. 255 explained why the court’s order to provide TD documentation and equipment specifications is unreasonable or untenable. He simply seems to believe that his judgment of what I need to complete my tests supersedes either the court’s or mine.

8. As such, the government has not provided installation instructions or minimum operating requirements, (per my previous requests, or the court's order), with its heavily redacted TD User Manual for version 1.23. At Mr. Walker's request (November 19, 2019 email), the following equipment estimates were provided: Apple Macbook Pro Laptop, 2.8GHz quad-core Intel Core i7

DECLARATION OF JEFFREY M. FISCHBACH

reb6

processor, 64GB memory,, 512GB SSD storage, Thunderbolt / USB-C, WiFi/RJ45. (Updated and summarized here.) While outwardly similar to the equipment Det. Erdely used to perform his "validations", this equipment was specifically chosen, with the expectation that, while accommodating the operating system and software I was able to *observe* Erdely using for his "validations", it should also provide an environment that will accommodate the forensic hardware and software I need to install in order to both complete my testing and assure the court that the machine has in no way been compromised during my testing, and that no software or data has been lost, stolen, or compromised. This hardware has some other very specific capabilities which are routinely utilized by forensic technologists, that are both necessary to complete my tests in time for trial, as well as to secure the equipment, software, and data from theft, intercept or alteration. While it is my usual practice to consult software specifications before choosing hardware, in the absence of court-ordered specifications, *this* hardware is suited to accommodate my anticipated needs for TD testing, as described previously to the court, while allowing me to use industry-standard practices to protect the software, data, and equipment. The equipment Mr. Walker has described in Dkt. 255, is not.

9. The court's order for documentation materials, quoted above, is in no way ambiguous or silent to its documentary requests, nor does it speak to any redactions. Mr. Walker previously claimed, while on record, that no such documents exist, but now he says they need to be redacted. Similarly, after affirming to the court that software change logs did not exist, they suddenly do.

10. The court order to "provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and

DECLARATION OF JEFFREY M. FISCHBACH

reb7



minimum operating requirements,” is clear and unambiguous. However, as he has done previously in this case, Mr. Walker is again opportunistically interpreting the court’s lack of granular specificity to mean “redacted” material, as the government sees fit to define “privileged information”. Again, I remind the court that Mr. Erdely stated under oath that TD’s secret identity was its *only* secret. Yet the government continues to claim that there are other things which the defense should not be able to see. One of those things may be responsible for the reason that TD investigations across the nation have, on several occasions, been inconsistent with the findings of well-tested, industry accepted software and hardware. As is the case herein.

11. Given the necessary access I need to complete my testing on the equipment provided by the government, I will take all necessary software and hardware precautions to restrict copy or dissemination of TD, and to secure my forensic work environment, as has been my standard practice for 25 years.

12. The foregoing statements are true and correct to the best of my knowledge, and I hereby reserve the right to amend them should additional information be made available to me at a later date.

///

///

///

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on November 25, 2019.

A handwritten signature in black ink, appearing to read 'J. Fischbach', with a stylized flourish at the end.

Jeffrey M. Fischbach

DECLARATION OF JEFFREY M. FISCHBACH

reb9

Robert M. Herz  
 Law Offices of Robert Herz, P.C.  
 431 W. 7<sup>th</sup> Avenue, Suite 107  
 Anchorage, Alaska 99501  
 907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT  
 FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

A period of excludable delay under 18 U.S.C. 3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. As of the date of this filing 36 days remain before trial must commence pursuant to the Speedy Trial Act

**SUPPLEMENT TO  
 C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE:  
 TORRENTIAL DOWNPOUR SOFTWARE**

Comes now, Matthew Schwier, by and through counsel, Robert M. Herz of the Law Offices of Robert Herz, P.C. hereby files this supplement pursuant to this court’s oral order from October 3, 2019 at the Final Pre-Trial Conference regarding the testing and protocols discussed in the *U.S. v. Gonzalez, 2:17-cr-001311-DGC*.

**There is no law enforcement privilege that precludes disclosure of material evidence.**

The government argues that *Roviaro v. United States, 353 U.S. 53 (1957)*, gives it a “privilege” not to disclose material evidence to Mr. Schwier. To the contrary, the *Roviaro* Court reversed the defendant’s conviction, finding prejudicial error in the government’s refusal not to disclose the name of its informer who “was the only witness in a position to amplify or contradict testimony of government witnesses.” *Id.* at 64.

The U.S. Supreme Court and the Ninth Circuit have yet to recognize or reject a “law enforcement privilege.” *Shah v. Dept. of Justice, 714 Fed. Appx. 657, 659 n.1 (9<sup>th</sup> Cir. 2017)*. No such privilege exists in *Roviaro*, which instead recognized a

limited “informer’s privilege” that allows the government “to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law.” 353 U.S. at 59.

*Shah* does not consider whether such a privilege would comport with the sixth amendment rights of confrontation and compulsory process and the fifth amendment right to due process. Even in *United States v. Pirosko*, 787 F.3d 358 (6<sup>th</sup> Cir. 2015), where the defendant did not show materiality and the court upheld non-disclosure, the court cautioned that “this conclusion should not be read as giving the government a blank check to operate its file-sharing detection software sans scrutiny. As a general matter, it is important that the government’s investigative methods be reliable, both for individual defendants like Pirosko and for the public at large.” 787 F.3d at 366.

In *Roviaro*, the Supreme Court noted that: “[t]he scope of the privilege is limited by its underlying purpose.” 353 U.S. at 60. Defense counsel does not intend to share the disclosed material with anybody other than his trial team, who often work under protective orders. Thus, there is no danger that child pornography distributors could find a way to avoid detection and thus render that tool of law enforcement ineffective, as the government claims. The government’s argument presumes that somehow there will be wide dissemination of the software to the public. Mr. Fischbach is the firewall. He has previously been granted National Security clearance and no one has suggested he ever violated his oath to maintain those national security secrets. He has been subject to many non-disclosure agreements and protective orders. No one has ever accused him of violating any. Balancing the government’s concerns which do not rise to level of a recognized privilege with those of the defendant which are grounded in the fifth and sixth amendment, the so-called “law enforcement” privilege must give way.

The Court in *Roviaro* also ruled that “[a] further limitation on the applicability of the

privilege arises from the fundamental requirements of fairness. Where the disclosure of an informer's identity, or the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way." 353 U.S. at 60-61. "In these situations the trial court may require disclosure and, if the Government withholds the information, dismiss the action." *Id.* Thus, in *Roviaro*, the Court held that the privilege must give way. Because the informer, John Doe, was the person to whom *Roviaro* was accused of selling heroin, "his identity and testimony [were] highly material" and should have been disclosed. *Id.* at 62-63. The informer was "the sole participant, other than the accused, in the transaction charged" and "the only witness in a position to amplify or contradict the testimony of government witnesses". *Id.* at 64.

The Torrential Downpour software and its associated materials plays the same role in this case that John Doe played in *Roviaro*. The program and its materials constitute "the only witness in a position to amplify or contradict the testimony" of SA Allison, the person who (according to the search warrant affidavit) downloaded child pornography from a remotely located computer on November 22, 2016. Not one scrap of contemporaneous evidence aside from data generated by Torrential Downpour software supports his claim.

**This case is different from Gonzalez, and thus the test(s) that the defense wants to run are different.**

The tests in Gonzalez as designed by the defense retained forensic examiner appeared aimed at answering specific questions pertinent to the facts of that case. In this case there are no .torrents on Mr. Schwier's alleged media that are relevant, and there is no data on the source computer or media that is relevant, unlike in the Gonzalez case. The Gonzalez defense identified nine tests it wanted to conduct in that case. See, *U.S. v. Gonzalez*, 2:17-cr-1311, at Doc. 86, Order of Court, August 27, 2019 at pg.3-4. And while these tests are of some interest, they do not address the specific issues identified in this case by the defense. As to the Gonzalez tests, tests 1 & 2 would not need to be run in this case if the government makes the same concessions it made

in Gonzalez. as described by the court. See, *U.S. v. Gonzalez*, 2:17-cr-1311, at Doc. 86, Order of Court, August 27, 2019 at pg. 8 lines 6-17 and pg.10 lines 6-10. The court also granted the defense request to conduct tests 3 & 4, and the parties agreed to tests 7, 8, & 9. The Gonzalez court noted that the main point of contention between the parties was whether the defense could have access to the ICAC COPS database. *Id.* at pg 3 line 19-21. The defense in this case does not need access to the ICAC COPS database.

The Gonzalez tests largely test the functionality of the software. The defense in this case wants to run a specific examination to test for a particular hypothesis, a particular condition that the defense believes it may have uncovered. And while the defense in this case does not need access to the ICAC COPS database, it does however require that the government provide the .torrents that Torrential Downpour Receptor identified as being files of interest and that were relied upon by SA Allison in conducting his Torrential Downpour searches in October and November of 2016.

**To date no independent third party testing of Torrential Downpour has been done. And the testing done to date does not appear to meet basic scientific standards.**

Mr. Schwier is not aware of any independent third party testing that has been done to date on Torrential Downpour. So far it appears that testing, to the limited extent that it exists, has been conducted by Detective Erdely. He is co-developer of the software and it appears he may have a financial interest and is a beneficiary of financial support provided by DOJ for the software. This appears to include as much as \$4.4 million dollars in the last ten years in grants from the Department of Justice and does not include separate licensing fees received for the software. He has a clear bias and interest to show that the software works, and a clear interest in not releasing the program to anyone who wants to prove it may not work as intended. Indeed, testing by the software's co-developer engenders problems with confirmation bias. This is not how the scientific method works. Erdely's hypothesis is that his software works as advertised. To test this hypothesis the scientific method requires testing the null hypothesis--- testing designed to prove

that the software does not work. If one is using the scientific method one does not design and run tests to show the software works rather you test for failure. Indeed, none of the reported testing appears to comply the the ISO/IEC/IEEE 29119 Software Testing-4: Testing Techniques. This standard is recognized by the National Institute of Standards and Technology (NIST) and by the Department of Justice. See also, National Institute of Standards and Technology, "Methodology Overview," published February 22, 2018 at [<https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-general-0>]. The Erdely testing is designed to prove the functionality of the software, whereas the defense proposed testing will be designed to see it causes one particular or a set of particular circumstances.

**The proposed defense test(s) is subject to attorney-client privilege and attorney work product doctrine. The defense will agree to disclose the particulars to the court in an ex parte proceeding only.**

The circumstances to be tested by the defense team were identified by and during the defense forensic computer examination that has been on-going and largely conducted at the Orange County RCFL since May. It is also based upon information provided by Mr. Schwier to counsel. This examination has allowed Mr. Fischbach to identify specific data and files that are relevant to the proposed testing. Revealing the proposed test(s), and what data it is based upon would reveal attorney work product and attorney client privileged communications. Mr. Schwier will not disclose this information in court to the government, nor is he required to.

In other contexts, such as the issuance of Rule 17 subpoenas, the courts recognize that the defense need not disclose information that reveals attorney-client communications or work product or defense trial strategy. See, e.g., *United States v. McClure*, 2009 W.L. 937502 (E.D. Cal. 2009); *United States v. Crutchfield* ( 2014 W.L. 2569058 (N.D.Cal. 2014). The *McClure* and *Crutchfield* decisions both find that revealing defense trial strategy constitutes good cause for accepting the subpoena application *ex parte*. Local rules in other Districts

within the Ninth Circuit specifically authorize seeking a 17(c) subpoena *ex parte* for good cause and “good cause” is defined as, among other matters, avoiding the revelation of defense trial strategy. Even the trial court’s protective order in *Budziak* (see attached) protected the testing and data generated by the defense tests from disclosure to the government.

In no other forensic field is the defense required to tell the government what independent tests it wants to run on any particular evidence. Whether the evidence is a controlled substance, or a hair, or DNA, so long as the evidence is material to the defense, the defense has a right to test and determine for itself what tests to run. If the results are not favorable the defense is not required to share that information with the government and need not use the results at trial. If the results are favorable the defense has the option of revealing the results and relying on those test results at trial. Of course, here the defense has no way to know in advance what the test results will show and whether the defense will intend to rely upon those results at trial. Mr. Schwier should not be required to disclose that information unless the defense intends to rely upon the evidence at trial. The test results could influence what type of defense Mr. Schwier intends to mount, and could affect his decision to proceed to trial or rather seek some sort of plea agreement. The data being relied upon and the test results are all matters that affect defense strategy, and thus pursuant to the fifth amendment and sixth amendment this information is privileged and not subject to disclosure.

Moreover, in no other defense testing of evidence is the defense required to conduct tests at a government facility. Here, the contraband evidence (actual images of child pornography) is subject to the restrictions imposed by the Adam Walsh act, and that evidence by statute must remain in government custody. The Torrential Downpour software is not contraband and not subject to those strictures. Moreover, the software is not classified as “Confidential Information” covered by the Confidential Information Procedures Act (CIPA) 18 U.S.C. App. 3 et seq. The defense has concerns whether the FBI offices can properly accommodate defense testing without the defense revealing privileged information, due to the



circumstances of the tests proceeding in a government facility. Moreover, Mr. Fischbach will require specific hardware and network configurations to conduct his tests and again the FBI may not be able to accommodate those needs. Mr. Fischbach's laboratory is already configured and set up to accommodate the testing contemplated.

Nevertheless, attached to Mr. Schwir's supplement brief, is a copy of the protective order issued by Judge Whyte in the *Budizak* case after the Ninth Circuit remand. This order fully addresses the government's concern about protecting the software from *public* disclosure. Mr. Schweir respectfully suggests the court largely adopt the terms of this order, with notable exceptions, rather than the one utilized by the court in *Gonzalez*. Paragraph #3 is not applicable to this case and the defense sees no justifiable reason to conduct the testing at a government facility. But the defense does agree with those terms of the *Budziak* Order holding that testing should not occur under the supervision or participation of the government, and that testing and results should remain confidential until the defense indicates that it intends to rely upon the tests and results at trial.

DATED at Anchorage, Alaska, this 15th day of October 2019.

THE LAW OFFICES OF ROBERT HERZ, PC

s/ Robert M. Herz  
431 W. 7<sup>th</sup> Avenue, Suite 107  
Anchorage, Alaska 99501  
Phone 907-277-7171  
Fax 907-277-0281  
[rmherz@gci.net](mailto:rmherz@gci.net)  
AK Bar No. 8706023

**CERTIFICATE OF SERVICE**

I hereby certify that on Oct 15, 2019, a copy of the foregoing Supp to C-3 Motion to Compel was served electronically on Assistant United States Attorney's Office s/ Robert Herz



IN THE SUPERIOR COURT OF THE STATE OF ARIZONA  
IN AND FOR THE COUNTY OF MARICOPA

STATE OF ARIZONA, )  
 )  
 ) PLAINTIFF, )  
 )  
 VS. ) CASE NO. CR2009-114677-001 SE  
 )  
 )  
 ROBERT DEAN MORAN, )  
 )  
 ) DEFENDANT. )  
 )

BEFORE THE HONORABLE ROBERT L. GOTTSFIELD, JUDGE

WEDNESDAY, AUGUST 24, 2011  
2:13 P.M.  
PHOENIX, ARIZONA

REPORTER'S EXCERPTED TRANSCRIPT OF PROCEEDINGS  
TESTIMONY OF ROBERT ERDELY

APPEARANCES:

FOR THE STATE: DANIELLE HARRIS, ESQ.  
DEPUTY COUNTY ATTORNEY  
-AND-  
LISA ANDRUS, ESQ.  
DEPUTY COUNTY ATTORNEY  
301 WEST JEFFERSON STREET,  
2ND FLOOR  
PHOENIX, ARIZONA 85003

FOR THE DEFENDANT: CRAIG C. GILLESPIE, ESQ.  
THE GILLESPIE LAW FIRM, P.C.  
3636 NORTH CENTRAL AVENUE,  
SUITE 150  
PHOENIX, ARIZONA 85012

REPORTED BY:

KIMBERLY D. MC ANDREWS, C.S.R./C.C.R./C.R., R.P.R.  
CALIFORNIA C.S.R. 10755, NEVADA C.C.R. 527,  
ARIZONA C.R. 50652  
REGISTERED PROFESSIONAL REPORTER

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

INDEX

STATE'S WITNESS

ROBERT ERDELY

DIRECT EXAMINATION BY MS. HARRIS

4

P R O C E E D I N G S

AUGUST 24, 2011  
PHOENIX, ARIZONA  
2:13 P.M.

(THE FOLLOWING PROCEEDINGS WERE HAD IN  
OPEN COURT:)

THE COURT: ALL RIGHT. WOULD YOU -- SO WE'RE GOING  
TO GO TO THE OTHER SIDE NOW AND HAVE YOU CALL YOUR WITNESS.

MR. HARRISON: THE STATE CALLS CORPORAL ERDELY TO  
THE STAND.

THE COURT: ALL RIGHT.

(THE CLERK SWORE THE WITNESS.)

THEREUPON--

ROBERT ERDELY,  
WAS CALLED AS A WITNESS BY THE STATE, AND AFTER HAVING BEEN  
FIRST DULY SWORN BY THE CLERK, WAS EXAMINED, AND TESTIFIED AS  
FOLLOWS:

THE WITNESS: I DO.

THE CLERK: OKAY. PLEASE STEP RIGHT OVER THERE.

THE WITNESS: (COMPLYING.)

MR. HARRISON: LET ME KNOW WHEN YOU GET SITUATED.

ALL SET?

THE WITNESS: I'M GOOD.

23 . . . . .  
24 . . . . .  
25 . . . . .

## DIRECT EXAMINATION

1

2 BY MS. HARRIS:

3 Q WOULD YOU PLEASE STATE YOUR NAME FOR THE RECORD.

4 A ROBERT ERDELY.

5 Q AND WHERE DO YOU WORK?

6 A I'M A CORPORAL WITH THE PENNSYLVANIA STATE POLICE.

7 Q OKAY. I DON'T THINK THE MICROPHONE'S CLOSE ENOUGH  
8 TO YOU.

9 THE COURT: PENNSYLVANIA STATE POLICE? OKAY.

10 THE WITNESS: YES, SIR.

11 Q BY MS. HARRIS: ALL RIGHT. AND HOW LONG HAVE YOU  
12 WORKED FOR THE PENNSYLVANIA STATE POLICE?

13 A OVER 19 YEARS.

14 Q AND I'M SURE YOU HAD TO GO THROUGH CERTAIN TRAINING  
15 IN YOUR POSITION WITH THE PENNSYLVANIA STATE POLICE; CORRECT?16 A YES. INITIALLY, WHEN I BECAME A TROOPER, WE GO  
17 THROUGH OUR ACADEMY. SINCE THEN, I'VE BEEN THROUGH NUMEROUS  
18 TRAININGS FOR WHEN I WAS WITH THE VICE UNIT, AND SINCE 2008, I  
19 JOINED THE COMPUTER CRIME UNIT. I'VE BEEN TO EXTENSIVE  
20 TRAINING THROUGHOUT THAT PERIOD, AS WELL UP AND TO THE POINT  
21 APPROXIMATELY FOUR YEARS AGO, WHERE I BECAME THE SUPERVISOR  
22 FOR THE COMPUTER CRIME UNIT FOR THE STATE OF PENNSYLVANIA.23 MS. HARRIS: AND IF I COULD APPROACH THE WITNESS,  
24 JUDGE --

25 THE COURT: SURE.

1 MS. HARRIS: -- WITH WHAT'S MARKED AS EXHIBIT  
2 NUMBER 7.

3 MR. GILLESPIE: (NODS HEAD.)

4 Q BY MS. HARRIS: DO YOU RECOGNIZE THAT?

5 A YES, IT'S MY C.V.

6 Q AND WITHOUT GOING THROUGH EVERYTHING THAT YOU'VE  
7 DONE IN YOUR CAREER AS AN OFFICER, DOES THAT ACCURATELY  
8 REFLECT SOME OF THE INFORMATION THAT YOU HAVE PROVIDED TO THIS  
9 COURT ON YOUR -- BASED ON YOUR TRAINING AND EXPERIENCE?

10 A YES. I HAVE NUMEROUS CISCO CERTIFICATIONS WHICH  
11 DEAL WITH ROUTING AND SWITCH AND HOW THE INTERNET WORKS. I  
12 HAVE VARIOUS MICROSOFT CERTIFICATIONS THAT DEAL WITH OPERATING  
13 SYSTEMS DATABASES AND SYSTEMS OPERATIONS. I'M A SYSTEMS  
14 ENGINEER. I HAVE VARIOUS SECURITY CERTIFICATIONS; CISCO'S ONE  
15 THAT'S SOUGHT AFTER. I HAVE FOUR DIFFERENT FORENSIC  
16 CERTIFICATIONS WHICH ARE CURRENT, AS WELL, WHICH I'VE  
17 ACHIEVED -- FIRST ONE WAS IN 2002, THE LAST ONE WAS IN 2009.

18 Q OKAY. AT THIS POINT --

19 THE COURT: AND WHAT'S THIS EXHIBIT NUMBER?

20 MS. HARRIS: NUMBER 7.

21 JUDGE, AT THIS POINT, THE STATE'S GOING TO MOVE TO  
22 ADMIT EXHIBIT NUMBER 7.

23 THE COURT: DO THAT BY STIPULATION?

24 MR. GILLESPIE: YES, YOUR HONOR.

25 THE COURT: OKAY. WHAT'S THAT? ??

1 MR. GILLESPIE: YES.

2 THE COURT: ADMIT 7.

3 Q BY MS. HARRIS: OKAY. NOT ONLY DO YOU HOLD THOSE  
4 CERTIFICATIONS, DO YOU TEACH COMPUTER OR COMPUTER TRAINING?

5 A YES. I TEACH FOR THE FOX VALLEY TECHNICAL COLLEGE,  
6 I TEACH INTERNET INVESTIGATIONS, PEER-TO-PEER INVESTIGATIONS,  
7 BASICALLY, TEACH TECHNOLOGY TO LAW ENFORCEMENT, AND I'M A  
8 MEMBER OF INTERNATIONAL -- THE INTERPOL WORKING GROUP DEALING  
9 WITH PEER-TO-PEER INVESTIGATIONS AND INVESTIGATIVE TOOLS USED  
10 BY LAW ENFORCEMENT, WHICH IS A WORLDWIDE GROUP OF FOLKS THAT  
11 DEVELOP SOFTWARE TO GIVE LAW ENFORCEMENT THE TOOLS THEY NEED  
12 TO DO THEIR JOB AROUND THE WORLD.

13 Q OKAY. SO NOT ONLY ARE YOU CERTIFIED OR TEACHING IN  
14 THE STATE OF PENNSYLVANIA, YOU'VE TAUGHT THROUGHOUT THE UNITED  
15 STATES; CORRECT?

16 A CORRECT, I'VE SPOKEN IN OTHER COUNTRIES.

17 Q AND I WAS JUST ABOUT TO SAY, AND THEN, THROUGHOUT  
18 THE WORLD?

19 A RIGHT. I WAS IN MOSCOW IN FEBRUARY, PRESENTING TO  
20 THEM.

21 Q OKAY. AND YOU SPECIFICALLY TRAIN ON PEER-TO-PEER  
22 NETWORKS SOME OF -- SOME OF THE TOPICS THAT YOU COVER?

23 A THE MAJORITY OF THE TOPICS DEAL WITH INTERNET  
24 INVESTIGATIONS FOCUSING PRIMARILY ON PEER-TO-PEER FILE SHARING  
25 NETWORKS.



1 Q OKAY. ARE YOU FAMILIAR WITH LIMEWIRE?

2 A YES, I AM.

3 Q OKAY. WHAT -- CAN YOU EXPLAIN TO THE COURT WHAT  
4 THAT IS. I KNOW WE TALKED ABOUT IT A LOT, BUT I DON'T THINK  
5 THERE'S EVER BEEN A FORMAL EXPLANATION ABOUT WHAT LIMEWIRE IS.

6 A LIMEWIRE'S JUST A CLIENT THAT RUNS ON A COMPUTER  
7 SYSTEM THAT ENABLES USERS TO PERFORM SEVERAL FUNCTIONS, THE  
8 FIRST BEING THAT YOU'RE ABLE TO SEARCH FOR FILES. THE  
9 SEARCHING OF THOSE FILES ARE ACTUALLY DONE THROUGH SOMETHING  
10 CALLED AN ULTRAPEER. IT'S JUST A CLIENT ON THE NETWORK THAT  
11 GETS REPROMOTED TO BEING, BASICALLY, A HELPER TO OTHER USERS  
12 ON THIS NETWORK, SO WHEN I EXECUTE A KEYWORD SEARCH, THE  
13 SEARCH IS ACTUALLY GOING THROUGH AN ULTRAPEER, AND THE  
14 ULTRAPEER DIRECTS ME TO FOLKS THAT MAY HAVE FILES THAT MATCH  
15 THE KEYWORDS THAT I USED. THAT'S THE FIRST FUNCTION; AND IF  
16 I'M GOING TO JUST BREAK THIS DOWN INTO THREE BASIC FUNCTIONS,  
17 THAT WOULD BE THE FIRST.

18 Q OKAY.

19 A THE SECOND WOULD BE THE OPTION TO DOWNLOAD FILES, SO  
20 THEN, AT THAT POINT, I HAVE A LIST OF FILES PRESENTED TO ME.  
21 I HAVE TO SELECT WHICH ONES I WANT TO DOWNLOAD. I COULD  
22 COMPARE THAT TO EVEN GOOGLE.

23 YOU OPEN UP A WEB BROWSER, AND YOU TYPE IN WORDS TO  
24 DESCRIBE WHAT YOU'RE LOOKING FOR. YOU'RE GIVEN A SET OF  
25 RESULTS. YOU'RE NOT REALLY -- HAVEN'T GONE AND SEEN THOSE

1 RESULTS YET; HOWEVER, YOU GET A PEEK AT WHAT THEY WOULD  
2 DESCRIBE IF YOU GO THERE --

3 Q OKAY.

4 A -- SO THAT'D BE A GOOD EXAMPLE BECAUSE GOOGLE IS  
5 KIND OF LIKE THAT ULTRAPEER. IT'S THE INDEX SERVER THAT GETS  
6 ME TO THE PLACE I WANT TO GO, SO I SELECT SOMETHING FROM THE  
7 LIST, AND I CHOOSE TO DOWNLOAD IT.

8 THE NORMAL WAY YOU CAN TELL A DOWNLOAD'S HAPPENED IS  
9 THAT IT WILL FIRST TRY TO GET YOU THE FILE FROM THE PERSON  
10 THAT YOU FILE SHARED THAT FILE, WHETHER THAT BE A KEYWORD  
11 SEARCH OR A SINGLE SOURCE DOWNLOAD -- OR I'M SORRY, A BROWSE  
12 HOST, BUT THERE'S SOMETHING ON THIS NETWORK CALLED FILE  
13 SWARMING.

14 Q AND CAN YOU SPELL THAT, SWARMING.

15 A SWARMING IS, LIKE, BEES THAT SWARM, JUST LIKE FILE  
16 SWARMING --

17 THE COURT: OKAY. OKAY.

18 THE WITNESS: -- AND THAT'S WHERE THE COMPUTER THAT  
19 I'VE LOCATED THROUGH THAT KEYWORD SEARCH WILL TELL ME ABOUT  
20 OTHER FOLKS THAT MAY HAVE THAT FILE.

21 THE COURT: LIMEWIRE HAS THE FILE SWARMING OR IT'S  
22 ALREADY ON YOUR COMPUTER?

23 THE WITNESS: LIMEWIRE HAS IT. SO DOES EVERY OTHER  
24 GNUTELLA CLIENT THAT IS FUNCTIONALLY -- FULLY FUNCTIONAL  
25 GNUTELLA CLIENT THAT IS PART OF THE PROTOCOL. THIS IS THE

1 TIME WHEN PARTIAL FILE SHARING OCCURS IS DURING FILE SWARMING.

2 Q BY MS. HARRIS: OKAY. AND BASED ON YOUR KNOWLEDGE  
3 OF THE SOFTWARE AND TRAINING AND EXPERIENCE, THE ONLY TIME  
4 THAT PARTIAL FILE OCCURS IS DURING FILE SWARMING?

5 THE COURT: IS DURING WHAT?

6 MS. HARRIS: DURING FILE SWARMING.

7 THE COURT: OKAY. I GOT IT.

8 THE WITNESS: AND THAT'S JUST WHERE THE NETWORK IS  
9 TRYING TO FIND ME ALL THE PEOPLE THAT HAVE PARTS OF THAT FILE  
10 BECAUSE, THAT WAY, I CAN JUST DOWNLOAD THE FILE MORE QUICKLY  
11 BECAUSE, TYPICALLY, ON THE INTERNET, YOUR DOWNLOAD SPEED IS  
12 FASTER THAN YOUR UPLOAD, SO IF YOU HAVE ONE PERSON OFFERING  
13 THE FILE, IT MAY BE RESTRICTED BASED ON HOW FAR I CAN SEND  
14 INFORMATION OUT TO THE INTERNET.

15 THE COURT: SO DID YOU JUST SAY FILE SWARMING IS  
16 WHERE YOU CAN GET A PARTIAL FILE?

17 THE WITNESS: YES. WHEN YOU GET IT FROM MULTIPLE  
18 SOURCES, THAT'S WHERE YOU'LL GET PIECES OF FILES FROM LOTS OF  
19 PEOPLE, AND THEN, THE PROGRAM WILL KEEP TRACK AND PUT IT BACK  
20 TOGETHER FOR YOU --

21 THE COURT: OKAY.

22 THE WITNESS: -- AND THEN, THE FINAL AREA BEYOND THE  
23 DOWNLOADING IS THE FILE BROWSE. THIS IS A COMPLETELY  
24 DIFFERENT FUNCTION THAN KEYWORD SEARCHES. IT HAS NOTHING TO  
25 DO WITH THE KEYWORD SEARCH, EXCEPT A PERSON YOU'RE BROWSING

1 ALMOST -- USUALLY WOULD HAVE COME THROUGH A KEYWORD SEARCH, SO  
2 AS TAMI LOEHRS DESCRIBED, I DO A KEYWORD SEARCH, AND I SEE A  
3 FILE THAT'S OF INTEREST TO ME, I CAN CHOOSE TO LIST ALL OF THE  
4 SHARED FILES IF THAT FEATURE IS ENABLED ON HIS COMPUTER, SO --  
5 BUT THAT'S SEPARATE AND APART.

6 THE KEYWORD SEARCH GOT ME THERE BECAUSE IT'S TWO  
7 SEPARATE FUNCTIONS. THE KEYWORD SEARCH CAME FROM ULTRAPEER.  
8 HERE IS WHERE I'M DIRECTLY CONNECTING MY COMPUTER TO HIS  
9 COMPUTER, AND THAT'S WHERE THE NAME PEER-TO-PEER COMES FROM.  
10 THERE'S NO INTERMEDIATE AREA; AND THE BROWSE IS FROM PERSON TO  
11 PERSON OR COMPUTER TO COMPUTER, AND -- AND THAT'S ONE OF THE  
12 MOST IMPORTANT THINGS HERE IS THIS FILE BROWSE BECAUSE IT  
13 ENABLES LAW ENFORCEMENT TO SEE FILES THAT ARE COMPLETELY  
14 PRESENT ON A PERSON'S SYSTEM AND BEING SHARED.

15 Q BY MS. HARRIS: OKAY. SO IF I'M UNDERSTANDING --  
16 THE COURT: SO ARE YOU SAYING FILE -- FILE BROWSE  
17 WILL GIVE YOU COMPLETED FILES?

18 THE WITNESS: ABSOLUTELY, SIR.

19 THE COURT: OKAY.

20 Q BY MS. HARRIS: SO I JUST WANT TO MAKE SURE I'M  
21 UNDERSTANDING BECAUSE THAT WAS A LOT TO DIGEST.

22 YOU'VE INDICATED THAT A FILE BROWSE -- IS THAT THE  
23 SAME AS A BROWSE HOST?

24 THE WITNESS: THERE IS THREE DIFFERENT WAYS I MIGHT  
25 REFER TO IT, AS IF I SAID FILE BROWSE, THAT MIGHT HAVE BEEN

1 POORLY WORDED. IT'S A BROWSE HOST OR A DIRECT CONNECT. IN A  
2 LOT OF SOFTWARE, IT'S REFERRED TO AS A BROWSE HOST, BUT IN  
3 LIMEWIRE, IT'S REFERRED TO AS A DIRECT CONNECT, BUT THEY ARE  
4 THE SAME EXACT FUNCTION REGARDLESS OF WHAT YOU CALL IT.

5 Q OKAY. SO IF I'M UNDER -- UNDERSTANDING YOUR  
6 TESTIMONY CORRECTLY, BASED ON YOUR TRAINING AND EXPERIENCE AND  
7 YOUR WORK WITH THE SOFTWARE, A BROWSE HOST IS DIFFERENT THAN A  
8 KEYWORD SEARCH?

9 A ABSOLUTELY DIFFERENT.

10 Q OKAY. AND IF YOU CAN KIND OF GO THROUGH AGAIN  
11 EXACTLY HOW IT'S DIFFERENT, NOW THAT WE'RE ON THE SAME PAGE  
12 ABOUT A BROWSE HOST AND A KEYWORD SEARCH.

13 A SO ONCE YOU HAVE IDENTIFIED A PERSON SHARING A FILE,  
14 WHETHER THAT BE THROUGH A KEYWORD SEARCH OR EVEN IF ANOTHER  
15 OFFICER CALLED ME ON THE PHONE AND SAID, YOU MIGHT WANT TO  
16 LOOK AT THIS I.P. ADDRESS ON THE INTERNET. I COULD JUST  
17 CHOOSE TO USE THIS OPTION, WHICH IS AVAILABLE TO ANYONE USING  
18 GNUTELLA CLIENTS.

19 THE COURT: YOU TALKING ABOUT THE FILE BROWSE  
20 OPTION?

21 THE WITNESS: YEAH; AND, JUDGE, I MIGHT HAVE POORLY  
22 WORDED THAT. IT SHOULD HAVE BEEN BROWSE HOST.

23 THE COURT: OKAY. BROWSE HOST OPTION. OKAY.

24 THE WITNESS: YES, AND EITHER BY ENTERING THE I.P.  
25 ADDRESS OR JUST SELECTING IT FROM THE PROGRAM THROUGH RIGHT

1 CLICKING ON THE FILE, THE END RESULT IS THE SAME, IS THAT MY  
2 COMPUTER CONNECTS TO THEIR COMPUTER, AND IT PRESENTS TO ME A  
3 LIST; AND IT'S A COMPREHENSIVE LIST OF MANY DIFFERENT PIECES  
4 OF INFORMATION, BUT IT WOULD INCLUDE THE FILE NAME, THE SHA-1  
5 HASH VALUE OF THE FILE, FILE SIZE, THE FILE TYPE; AND IT'S  
6 SIGNIFICANT TO LAW ENFORCEMENT BECAUSE THESE ARE WHOLE FILES  
7 ON THEIR COMPUTER AT THAT MOMENT IN TIME THAT ARE BEING  
8 SHARED.

9 IF A PERSON WOULD CHOOSE TO UNSHARE ONE OF THOSE  
10 FILES, IT IMMEDIATELY COMES OFF THE LIST. IT DOES NOT REQUIRE  
11 THE PROGRAM TO BE RESTARTED. IF I WERE TO DELETE A FILE FROM  
12 THAT -- FROM MY LIMEWIRE THAT WAS SHARING CERTAIN FILES -- IF  
13 I DELETED THAT FILE, IT IMMEDIATELY COMES OFF THE LIST AND  
14 ISN'T AVAILABLE FOR SOMEONE TO SEE, SO IT'S VERY SIGNIFICANT  
15 TO LAW ENFORCEMENT.

16 I'VE TRAINED WELL OVER A THOUSAND INVESTIGATORS OVER  
17 THE LAST FEW YEARS, AND I'VE TESTED IT IN EXCESS OF 500 TIMES,  
18 PROBABLY CLOSER TO A THOUSAND. IF YOU CONSIDER, YOU KNOW, I'M  
19 STANDING AT THE FRONT OF THE CLASS OF 30 PEOPLE, PERFORMING  
20 THIS TEST IN A CLASSROOM ENVIRONMENT OVER AND OVER AGAIN, AND  
21 I'VE NEVER SEEN AN INSTANCE WHERE A PARTIAL OR DELETED OR  
22 UNSHARED FILE APPEARS ON THAT LIST. THAT ABSOLUTELY CANNOT  
23 HAPPEN.

24 Q OKAY. SO WHEN DETECTIVE CORDER INDICATES THAT SHE  
25 DID A BROWSE HOST OF THE DEFENDANT'S COMPUTER, IF I'M

1 UNDERSTANDING YOU CORRECTLY, SHE HAD OPPORTUNITY AT THAT POINT  
2 IN TIME TO SEE ALL COMPLETED FILES THAT WERE AVAILABLE FOR  
3 SHARING?

4 A ABSOLUTELY.

5 Q OKAY. NO PARTIAL FILES WOULD HAVE BEEN INCLUDED,  
6 BASED ON YOUR TRAINING AND EXPERIENCE, IN THAT LIST?

7 A ABSOLUTELY CORRECT.

8 Q NOW, IF I'M ALSO UNDERSTANDING YOU CORRECTLY, THE  
9 INFORMATION THAT DETECTIVE CORDER SEES WHEN SHE DOES THE  
10 BROWSE HOST OR A FILE BROWSE IS COMPLETELY OPEN TO THE PUBLIC?

11 A ANYBODY CAN PERFORM THAT FUNCTION --

12 Q OKAY.

13 A -- USING ANY SOFTWARE THAT'S CAPABLE OF DOING A  
14 BROWSE HOST.

15 Q SO IT'S AVAILABLE TO ANYONE THAT'S CAPABLE OF USING,  
16 SAY, FOR INSTANCE, LIMEWIRE OR ONE OF THE OTHER GNUTELLA  
17 PEER-TO-PEER SHARING NETWORKS?

18 A CORRECT. LIMEWIRE AND PHEX ARE THE TWO IN QUESTION  
19 HERE. PHEX WAS HER INVESTIGATIVE TOOL, AND LIMEWIRE WAS THE  
20 PROGRAM THAT THE DEFENDANT WAS USING, IF I'M TO BELIEVE THE  
21 REPORTS THAT I'VE REVIEWED AND PEOPLE I'VE SPOKEN TO.

22 Q OKAY. NOW, BEFORE WE TALK ABOUT PHEX, WHEN YOU DO A  
23 BROWSE HOST, IS IT POSSIBLE TO SEE ANY OTHER PART OF A  
24 PERSON'S COMPUTER SEPARATE AND APART FROM THE FILES THAT THEY  
25 HAVE AVAILABLE FOR SHARING?

1           A       NO.  IT -- IT DISPLAYS TO THE USER THE SHARED FILES.  
2       THAT WOULD INCLUDE -- I COULD PUT THOSE INTO TWO CATEGORIES --  
3       I'LL USE THREE CATEGORIES.  IF ONE WOULD HAVE BEEN  
4       AUTOMATICALLY SHARED BY THE PROGRAM -- FOR INSTANCE, SOME  
5       VERSIONS OF FROSTWIRE WILL AUTOMATICALLY -- I DON'T WANT TO  
6       MISSPEAK.

7                   POTENTIALLY, I'VE SEEN SOME EVIDENCE THAT, MAYBE,  
8       THEY'RE SHARING THE SOFTWARE ITSELF AUTOMATICALLY SO OTHER  
9       PEOPLE CAN GET FROSTWIRE, FOR INSTANCE, SO SOMETHING  
10      AUTOMATICALLY SHARED LIKE THAT.

11                   ANY FILES I TRY TO SHARE BY DRAGGING THEM INTO MY  
12      SHARED FOLDER, WHICH IS DEFINED BY THE PROGRAM IN ITS  
13      SETTINGS; AND THEN, FINALLY, IT'S A DEFAULT FOR, I BELIEVE,  
14      EVERY VERSION OF FOUR THAT I'VE REVIEWED AND ALL VERSIONS OF  
15      FIVE OF LIMEWIRE BECAUSE THERE WAS DIFFERENT VERSION FOURS  
16      THAT WERE AVAILABLE ON LIMEWIRE, AND THEN, THEY JUMPED TO A  
17      WHOLE NEW MAJOR CHANGE; AND THEN, THERE WERE VERSIONS OF FIVE  
18      THAT WERE AVAILABLE ON LIMEWIRE, INCLUDING FROSTWIRE.

19                   THE DEFAULT IS ANYTHING THAT I DOWNLOAD FROM THE  
20      INTERNET IS ALSO SHARED, AND IT KIND OF GOES INTO ITS  
21      CATEGORY, BUT THE USERS OF THIS PROGRAM ARE TOLD THAT THEY'RE  
22      SHARING PROGRAMS AND GIVEN OPTIONS TO NOT SHARE FILES.

23           Q       OKAY.

24                   THE COURT:  SO WHAT DOES BROWSE HOST DO WHAT GOOGLE  
25      DOESN'T?  THAT'S WHAT I'M STILL NOT UNDERSTANDING.



1           THE WITNESS:  JUDGE, I WAS JUST GIVING AN EXAMPLE OF  
2   HOW I'M SEARCHING FOR FILES IN LIMEWIRE AND GETTING A SET OF  
3   RESULTS.  I JUST COMPARED IT TO GOOGLE 'CAUSE GOOGLE'S A  
4   WEBSITE YOU CAN INSERT WORDS THAT YOU'RE SEARCHING FOR, AND  
5   THEN, YOU GET A SET OF RESULTS.  I JUST TRIED TO USE THAT  
6   ANALOGY TO GIVE THE COURT SOME UNDERSTANDING.

7           THE COURT:  SO BROWSE HOST DOESN'T DO ANYTHING THAT  
8   GOOGLE DOES?

9           THE WITNESS:  IT'S JUST TWO DIFFERENT TECHNOLOGIES,  
10  BUT I WAS JUST TRYING TO EXPLAIN, YOU INSERT KEYWORDS, AND  
11  YOU'RE GIVEN A SET OF RESULTS.  THERE ARE TWO SEPARATE THINGS  
12  THAT I TRIED TO JUST COMPARE.

13          THE COURT:  OKAY.

14          Q       BY MS. HARRIS:  AND SO JUST SO WE'RE CLEAR, A  
15  KEYWORD SEARCH IS DIFFERENT FROM A BROWSE HOST?

16          A       ABSOLUTELY.

17          Q       OKAY.

18          A       ONE USES ULTRAPEERS, THE OTHER DOES NOT.

19          Q       SO WHEN YOU DID YOUR GOOGLE ANALOGY, YOU WERE  
20  REFERRING TO TYPING IN KEYWORDS, WHICH WOULD BE SIMILAR TO A  
21  KEYWORD SEARCH?

22          A       CORRECT.

23          Q       AND NOT SIMILAR TO A BROWSE HOST?

24          A       CORRECT.

25          Q       OKAY.  NOW, IS IT YOUR UNDERSTANDING, THEN, LIMEWIRE

1 WAS TAKEN OFFLINE?

2 A YES. I BELIEVE THE WEBSITE ACTUALLY SHUT DOWN,  
3 ALTHOUGH IT WAS -- THERE WAS AN ORDER PRIOR TO THAT,  
4 DECEMBER 31ST OF 2010.

5 Q OKAY. BASED ON YOUR TRAINING AND EXPERIENCE AND  
6 YOUR KNOWLEDGE OF THE SOFTWARE, CAN YOU STILL FIND VERSIONS OF  
7 LIMEWIRE AVAILABLE?

8 A YES.

9 Q HOW?

10 A GO TO GOOGLE AND SEARCH LIMEWIRE DOWNLOAD, AND  
11 YOU'LL BE PRESENTED WITH SITES THAT HAVE VERSIONS, THE SAME  
12 VERSION THAT LIMEWIRE OFFERED UP; HOWEVER, I'VE BEEN  
13 COLLECTING IT FOR YEARS NOW -- COLLECTING ALL THE VERSIONS SO  
14 THAT WE IN LAW ENFORCEMENT, JUST LIKE MISS LOEHR'S SAID, IN HER  
15 LAB, SHE HAS ALL THE DIFFERENT VERSIONS, I'VE DOWNLOADED ALL  
16 THOSE VERSIONS AS THEY BECAME AVAILABLE, SO I HAVE ALL THE  
17 DIFFERENT VERSIONS THAT LIMEWIRE GAVE TO ME, SO I CAN DO  
18 TESTING IN CASES BECAUSE I'VE BEEN TO TRIAL SEVERAL TIMES IN  
19 CASES LIKE THIS WHERE I'M ASKED TO PRESENT AS AN EXPERT, AND  
20 WHAT'S MOST RELEVANT IN A CASE IS THE SOFTWARE THAT THE PERSON  
21 USED, SO I WILL TAKE THAT SOFTWARE AND PREPARE EXHIBITS FOR  
22 COURT, SHOWING THE PROCESS A PERSON WOULD GO TO TO INSTALL THE  
23 SOFTWARE, THE FUNCTIONALITY OF THE SOFTWARE; AND AS IS IN THIS  
24 CASE, THE TESTING OF HOW THE SOFTWARE FUNCTIONS.

25 I KNOW THESE THINGS TO BE TRUE. I TEST THEM OVER

1 AND OVER AGAIN. EVERY TIME I USE A SOFTWARE, IT BECOMES A  
2 TEST BECAUSE I SEARCH FOR FILES AND THEN CHOOSE TO DOWNLOAD  
3 THEM. THE SOFTWARE I USE TELLS ME IF THEY HAVE THE WHOLE FILE  
4 OR NOT, SO I'M ABLE TO SEE THAT AS SOON AS I ATTEMPT TO  
5 DOWNLOAD A FILE.

6 I'VE SEEN HUNDREDS AND HUNDREDS AND HUNDREDS OF  
7 TIMES WHERE I'VE DONE KEYWORD SEARCHES, INITIATE A DOWNLOAD  
8 THROUGH FILE SWARMING. THE FIRST FILE ON MY LIST IS THE FILE  
9 THAT I FOUND VIA THE KEYWORD SEARCH, AND IN PHEX, IT HAS THIS  
10 LITTLE HANDY INDICATOR -- IT'S THIS LITTLE STATUS PROGRESS  
11 BAR-LOOKING THING. IT WILL BE COLORED IN BLUE OR NOT.

12 IF HE HAS IT ALL THE WAY ACROSS, HE HAS THE WHOLE  
13 FILE, AND REASON THAT I KNOW THAT IS THAT'S A TYPE OF  
14 COMMUNICATION THAT HAPPENS ON GNUTELLA. IT IS A DIRECT  
15 CONNECT FROM HIM TO ME, WHERE HE SAID, HEY, I HAVE THE WHOLE  
16 FILE, AND I'VE SEEN THAT HUNDREDS AND HUNDREDS OF TIMES, SO  
17 SEPARATE AND APART FROM THE TESTING I DID IN THIS CASE, MY  
18 EVERYDAY USE OVER YEARS OF USING PHEX, I'VE INDIRECTLY TESTED  
19 THE FACT THAT I HAVE NEVER SEEN A PARTIAL FILE APPEAR AS THAT  
20 SEARCH RESULT, AND IT'S CLEARLY DISPLAYED TO US IN PHEX.

21 Q OKAY. NOW, YOU MENTIONED DIFFERENT VERSIONS OF, FOR  
22 EXAMPLE, LIMEWIRE.

23 IS IT YOUR OPINION THAT DIFFERENT VERSIONS OPERATE  
24 OR CAN FUNCTION DIFFERENTLY?

25 A ABSOLUTELY. THE SOURCE CODE CHANGES OVER TIME.

1 Q OKAY. NOW, YOU MENTIONED PHEX.

2 CAN YOU EXPLAIN TO THIS COURT EXACTLY WHAT PHEX IS.

3 A SO LIMEWIRE IS A GNUTELLA CLIENT THAT SHARES FILES.

4 YOU CAN SEARCH FOR FILES THROUGH IT. YOU CAN GET RESULTS.

5 YOU CAN DOWNLOAD FILES, AND THEN, YOU CAN DO THAT DIRECT

6 CONNECT OR BROWSE HOST.

7 PHEX IS JUST LIKE LIMEWIRE IN THAT IT IS PUBLICLY

8 AVAILABLE. THE SOURCE CODE IS AVAILABLE FOR ANYONE TO REVIEW,

9 JUST LIKE LIMEWIRE, AND IT HAS ALL THE SAME FUNCTIONS. I CAN

10 SEARCH FOR FILES, I CAN GET LISTS OF RESULTS. I CAN CHOOSE TO

11 DOWNLOAD THOSE FILES OR I CAN CHOOSE TO LIST ALL OF A PERSON'S

12 SHARED FILES THROUGH THAT FUNCTION REFERRED TO AS A DIRECT

13 CONNECT.

14 Q OKAY. AND BASED ON YOUR TRAINING AND EXPERIENCE, I

15 BELIEVE YOU'VE ALREADY INDICATED THAT PHEX IS AVAILABLE TO THE

16 GENERAL PUBLIC?

17 A YES, AND AS WELL AS THE SOURCE CODE, AND THAT'S THE

18 INVESTIGATIVE TOOL USED IN THIS CASE.

19 Q WHEN YOU SAY THAT WAS THE INVESTIGATIVE TOOL USED IN

20 THIS CASE, WHAT DO YOU MEAN BY THAT?

21 A WELL -- SO I AM FAMILIAR WITH THE WAY PEER SPECTRE

22 RUNS. IT JUST DOES KEYWORD SEARCHES ON GNUTELLA, AND THEN, IT

23 LOGS ALL THOSE RESULTS FOR INVESTIGATORS TO REVIEW. I COMPARE

24 THAT TO, YOU KNOW, AN ANONYMOUS TIP.

25 Q OKAY.

1           A        I DON'T CARE HOW I'VE LEARNED THAT AN I.P. ADDRESS  
2       MAY OR MAY NOT HAVE CHILD PORNOGRAPHY, BUT I'LL DO A MUCH  
3       BETTER JOB LOOKING AT A LIST PROVIDED BY PEER SPECTRE BECAUSE  
4       THEY'RE LOOKING FOR A SET OF FILES KNOWN TO LAW ENFORCEMENT,  
5       SO IT -- AND IT DOES A SECOND PART.

6                    ALTHOUGH I CAN SEE THE I.P. ADDRESS, WHICH THE I.P.  
7       ADDRESS IS JUST THE INTERNET ADDRESS ASSIGNED TO A COMPUTER ON  
8       THE INTERNET, WHICH IS UNIQUE TO IT.  JUST LIKE A PHONE  
9       NUMBER'S UNIQUE TO A HOME, AN I.P. ADDRESS IS UNIQUE TO A  
10      COMPUTER ON THE INTERNET SOMEWHERE IN THAT POINT IN TIME, SO I  
11      CAN SEE -- IN TELEPHONE AREAS, WE HAVE AREA CODES.  I'M GOING  
12      TO SEE 412, I'M GOING TO THINK PITTSBURGH, BUT IN I.P.  
13      ADDRESSES, I'M GOING TO JUST SEE A BUNCH OF NUMBERS, BUT THERE  
14      ARE WAYS TO TURN THOSE NUMBERS INTO AN APPROXIMATE LOCATION.  
15      THERE'S COMPANIES THAT DO THAT FOR US, SO PEER SPECTRE DOES  
16      THAT FOR US, AS WELL.  IT HELPS US GEO-LOCATE SO WE, AS LAW  
17      ENFORCEMENT, CAN TARGET THE I.P. ADDRESSES THAT MAY HAVE --  
18      MAY OR MAY NOT HAVE CHILD PORNOGRAPHY ON THEIR SYSTEMS, AND  
19      THAT'S MY STARTING POINT, SO WHETHER PEER SPECTRE PRESENTED A  
20      LIST OF RESULTS TO ME -- NOW, I DON'T HAVE TO RUN PEER SPECTRE  
21      TO SEE THE RESULTS.  I JUST LOOK AT THE RESULTS THAT ARE  
22      PRESENTED TO ME THROUGH THIS LAW-ENFORCEMENT-ONLY SYSTEM, SO  
23      IT JUST FEEDS THE PROCESS UP, BUT IT DOESN'T MATTER IF  
24      PEER SPECTRE'S TOLD ME ABOUT IT.  IT DOESN'T MATTER IF I JUST  
25      SAW THE RESULTS ON A WEB PAGE OR SOME OUTPUT OF A PROGRAM.  IT

1 DOESN'T MATTER IF I GOT AN ANONYMOUS CALL ON MY PHONE; IF  
2 SOMEONE RUNNING DOWN THE STREET YELLED OUT AN I.P. ADDRESS AND  
3 SAID, WHY DON'T YOU GO SEE IF HE'S ON LIMEWIRE. IT DOESN'T  
4 MATTER BECAUSE THE MOMENT I PLUG THAT I.P. ADDRESS INTO PHEX,  
5 MY INVESTIGATIVE TOOL, AND INITIATE A BROWSE HOST, WHERE I  
6 DIRECTLY CONNECT TO THE SHARING COMPUTER AND SEE THE LIST OF  
7 HIS WHOLE FILES BEING SHARED WITH -- ALONG WITH THE HASH  
8 VALUE, THAT'S THE INVESTIGATION. I'VE JUST TURNED SOME  
9 ANONYMOUS TIP INTO SOMETHING I CAN SPEAK FIRST PERSON ABOUT IN  
10 ANY REPORT I WRITE OR ANY AFFIDAVIT I HAVE TO AUTHOR.

11 THE COURT: AND, IN GOOD FAITH, YOU CAN SAY WHAT I  
12 SAW IN BROWSE HOST IS NOT PARTIAL, IT'S NOT DELETED, IT'S THE  
13 FULL THING?

14 THE WITNESS: JUDGE, I CAN DO A LIVE DEMONSTRATION  
15 WITH THIS COURT. I CAN MEET WITH THEIR EXPERT ANY TIME OF ANY  
16 DAY FOREVER AND PROVE THAT THIS IS THE CASE.

17 THE COURT: WELL, HOW COULD AN EXPERT -- AN EXPERT  
18 DOING THIS FOR YEARS SAY YOU CAN GET PARTIAL FILES? WHAT --  
19 WHAT COULD SHE BE TALKING ABOUT?

20 THE WITNESS: (NO RESPONSE.)

21 THE COURT: YOU HAVE NO ANSWER?

22 THE WITNESS: SHE COULD NOT HAVE DONE IT ON A TEST.  
23 I DON'T KNOW WHAT SHE DID BECAUSE SHE DIDN'T PUT IT IN HER  
24 REPORT.

25 THE ONE THING THAT THE OFFICER DID IN HER AFFIDAVIT

1 THAT SHE SPECIFICALLY DID 'CAUSE SHE WAS NOT RUNNING  
2 PEER SPECTRE -- SHE DID ONE THING, AND THAT IS USE PHEX TO DO  
3 A BROWSE HOST AND LIST THE SHARED FILES.

4 THIS IS COMMON PRACTICE IN LAW ENFORCEMENT. I TEACH  
5 IT EVERY DAY. I TAUGHT IT A COUPLE WEEKS AGO IN DALLAS, AND I  
6 STILL TEACH IT TO THIS DAY. THIS IS THE INVESTIGATIVE  
7 PROTOCOL USED BY FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT ALL  
8 AROUND THE WORLD.

9 THE COURT: OKAY.

10 Q BY MS. HARRIS: SO IF I'M UNDERSTANDING YOU  
11 CORRECTLY, THE INVESTIGATION DONE BY DETECTIVE CORDER WHERE  
12 SHE USED PEER SPECTRE, YOU'RE ANALOGIZING THAT TO, SAY, AN  
13 ANONYMOUS TIP?

14 A THAT'S CORRECT.

15 Q OKAY. SO IF THERE WAS ANY OTHER WAY, SEPARATE AND  
16 APART FROM PEER SPECTRE, THAT DETECTIVE CORDER COULD HAVE  
17 GOTTEN THIS INFORMATION ABOUT A PARTICULAR I.P. ADDRESS, SHE  
18 COULD HAVE STILL DONE THE EXACT SAME CONNECTION THROUGH PHEX  
19 AND LOCATED THE FILES THAT ARE AVAILABLE FOR SHARING ON THE  
20 DEFENDANT'S COMPUTER?

21 A THAT'S CORRECT. I'VE ACTUALLY SEEN PEOPLE ONLINE AS  
22 I'M SEARCHING GNUTELLA AND CALLED THEM ON THE PHONE AND SAID,  
23 HEY, YOU GOT A BAD GUY ONLINE IN, LET'S SAY, PITTSBURGH,  
24 PENNSYLVANIA AS THAT EXAMPLE. ALL THE INVESTIGATOR HAS TO DO  
25 IS FIRE UP PHEX AND INPUT THE I.P. ADDRESS THAT I TELL HIM

1 OVER THE PHONE AND THEN LIST ALL OF HIS WHOLE SHARED FILES.  
2 THAT'S THE INVESTIGATION.

3 Q OKAY. SO IF I'M UNDERSTANDING YOU CORRECTLY,  
4 INVESTIGATION STARTS THE MOMENT YOU PUT THE I.P. ADDRESS INTO  
5 PHEX AND THEN, YOU DIRECTLY CONNECT?

6 A THAT'S CORRECT.

7 Q OKAY. 'CAUSE AT THAT POINT, YOU CAN SEE ALL  
8 COMPLETED FILES AVAILABLE FOR SHARING?

9 A THAT'S CORRECT.

10 Q AND BASED ON YOUR UNDERSTANDING OF THE FACTS IN THIS  
11 CASE OR THE TESTIMONY GIVEN BY DETECTIVE CORDER IN HER  
12 INTERVIEW, THAT IS WHAT SHE DID IN THIS PARTICULAR CASE?

13 A ABSOLUTELY.

14 Q OKAY. AND NOT ONLY IS THAT WHAT SHE DID IN THIS  
15 PARTICULAR CASE, YOU'VE ACTUALLY HAD AN OPPORTUNITY TO TRAIN  
16 OFFICERS, INCLUDING DETECTIVE CORDER, HAVE YOU NOT?

17 A THAT'S CORRECT.

18 Q OKAY. AND LET'S TALK ABOUT THAT TRAINING, AND THEN,  
19 WE'LL TALK ABOUT YOUR TESTING.

20 WHEN YOU TRAIN AN OFFICER, AND HOW -- YOU'VE BEEN  
21 TRAINING FOR OVER TEN YEARS; IS THAT FAIR TO SAY -- OR ABOUT  
22 TEN YEARS?

23 A OFFICIALLY TEACHING FOR FOX VALLEY TECHNICAL COLLEGE  
24 MAYBE TWO AND A HALF YEARS.

25 Q OKAY.



1           A       HOWEVER, IN MY POSITION IN THE COMPUTER CRIME UNIT,  
2   I HAVE INSTRUCTED OFFICERS THROUGHOUT MY WHOLE COMPUTER CRIME  
3   CAREER, SO I COULD EASILY SAY TEN YEARS WOULD BE A GOOD  
4   ESTIMATE.

5           Q       OKAY.  AND YOU'RE FAMILIAR WITH, OF COURSE,  
6   LIMEWIRE, PHEX, PEER SPECTRE, BUT YOU'RE ALSO FAMILIAR WITH  
7   WYOMING TOOLKIT?

8           A       YES.

9           Q       AND I'M TRYING TO MAKE SURE I COVER EVERYTHING.  
10   CASE MANAGER?

11          A       NO, I'VE NEVER USED CASE MANAGER.

12          Q       OKAY.  SO WE WON'T ASK YOU QUESTIONS ABOUT THE CASE  
13   MANAGER, AT THIS POINT, BUT BASED ON EVERYTHING THAT YOU HAVE  
14   READ, BASED ON YOUR TRAINING AND EXPERIENCE, AND BASED ON THE  
15   TEACHING THAT YOU PROVIDE TO LAW ENFORCEMENT OFFICERS, IS  
16   THERE A REQUIREMENT FOR A LAW ENFORCEMENT OFFICERS TO DO  
17   SINGLE SOURCE DOWNLOADS?

18          A       NO, THERE IS NO REQUIREMENT, AND THE INSTRUCTION WE  
19   GIVE TO THE FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT IS  
20   EXACTLY -- EXACTLY THE OPPOSITE OF THAT.

21                 IT'S PREFERRED -- IF THEY WANT A DISSEMINATION COUNT  
22   IN ALMOST EVERY JURISDICTION THAT I'VE BEEN IN AND WORKED IN,  
23   THERE USUALLY IS A SEPARATE COUNT THAT CAN BE APPLIED FOR  
24   DISSEMINATION OF A FILE VERSUS THE SIMPLE POSSESSION, BUT WHEN  
25   THAT IS NOT POSSIBLE -- AND IT IS NOT ALWAYS POSSIBLE -- THEN

1 THE SECOND BEST THING IS THE BROWSE HOST.

2 Q WHICH IS WHAT DETECTIVE CORDER DID IN THIS CASE?

3 A YES, AND THAT'S THE WAY I TAUGHT IT, YOU KNOW, JUST  
4 A COUPLE WEEKS AGO, AND -- AND SHE DID EVERYTHING, YOU KNOW,  
5 AS WE INSTRUCTED IT TO HAPPEN. AS A MATTER OF FACT, EVERY  
6 STUDENT THAT I TEACH -- AND IT GOES TO MY 500-PLUS TESTS --  
7 THE LAST STEP OF THE CLASS IS A VALIDATION OF THE THINGS I  
8 SAY, SO NOT ONLY DO I KNOW WHAT A BROWSE HOST REPRESENTS,  
9 THERE'S OVER A THOUSAND OFFICERS THAT I'VE TRAINED THAT KNOWS  
10 THAT SAME THING FIRSTHAND.

11 THE COURT: SO YOU'RE SAYING PEER SPECTRE IS KIND OF  
12 ANALOGOUS TO THE ANONYMOUS TIP, BUT THEN, YOU GO TO PHEX AND  
13 BROWSE HOST, AND THAT'S THE INVESTIGATION?

14 THE WITNESS: YES, SIR, THAT'S CORRECT.

15 THE COURT: OKAY.

16 Q BY MS. HARRIS: AND IF I'M UNDERSTANDING YOU  
17 CORRECTLY -- I KNOW YOU SAY THERE IS NO REQUIREMENT.

18 IS THERE ANYTHING IN ANY TRAINING MATERIALS THAT  
19 YOU'VE REVIEWED OVER THE YEARS OR THAT YOU'VE TAUGHT ON THAT  
20 REQUIRES AN OFFICER TO DO A SINGLE SOURCE DOWNLOAD?

21 A NOT REGARDING THE TRAINING I -- I GIVE, NO. I  
22 HAVEN'T BEEN TO ANY TRAINING WHERE THEY TAUGHT THAT YOU HAD TO  
23 DO A SINGLE SOURCE DOWNLOAD. I KNOW THAT, YOU KNOW, IT MAY BE  
24 A POLICY OF A DEPARTMENT SOMEWHERE, THAT THAT'S THE CASE, BUT  
25 IT'S CERTAINLY NOT A REQUIREMENT IN ANY TRAINING I'VE BEEN

1 INVOLVED IN.

2 THE COURT: AND THAT'S NOT BUILT INTO PHEX OR INTO  
3 BROWSE HOST; A SINGLE -- SINGLE SOURCE DOWNLOAD NOT BUILT INTO  
4 ANY OF THAT?

5 THE WITNESS: IT WAS NOT BUILT INTO PHEX. PHEX IS  
6 WHAT WE USE AND WHAT DETECTIVE CORDER USED WHEN WE FIRST  
7 STARTED DOING THESE INVESTIGATIONS BECAUSE IT SHOWED US THE  
8 HASH VALUE AND THE I.P. ADDRESS. IT WAS A VERY GOOD TOOL FOR  
9 LAW ENFORCEMENT 'CAUSE WE COULD SEE THE I.P. ADDRESS AND  
10 DETERMINE WHERE IT'S AT IN THE WORLD.

11 OVER TIME, THERE WERE TOOLS DEVELOPED THAT BASICALLY  
12 MADE IT HARDER FOR LAW ENFORCEMENT BECAUSE INSTEAD OF GETTING  
13 THE FILE VERY QUICKLY FROM MULTIPLE COMPUTERS, WE CHOOSE TO  
14 GET IT FROM A SINGLE COMPUTER, AND THAT'S WHAT TAMI LOEHR'S WAS  
15 REFERRING TO AS A SINGLE SOURCE DOWNLOAD. IT IS A FUNCTION OF  
16 WHAT WE DO TODAY, BUT AT THE TIME THAT DETECTIVE CORDER DID  
17 THIS INVESTIGATION, SHE DID IT EXACTLY AS SHE WAS INSTRUCTED  
18 TO, AND I FIND NO FAULT IN THE PROCESS THAT SHE FOLLOWED  
19 BECAUSE SHE DID NOT HAVE A PROGRAM CAPABLE OF DOING THE SINGLE  
20 SOURCE DOWNLOAD.

21 THE COURT: SO TODAY, WHEN YOU TEACH IT, YOU SAY  
22 IT'S BUILT INTO THE SOFTWARE TODAY?

23 THE WITNESS: YES. AN OFFICER HAS AN OPTION TO DO A  
24 SINGLE SOURCE DOWNLOAD, WE ENCOURAGE IT. IT'S NOT A  
25 REQUIREMENT, AND WE TEACH THEM HOW TO HANDLE THE INVESTIGATION

1 WHEN THEY CAN'T GET A SINGLE SOURCE DOWNLOAD, AND THAT IS TO  
2 DO A BROWSE HOST, WHICH DATES WAY BACK WHEN TO THE TRAINING  
3 THAT TAMI -- SORRY -- DETECTIVE CORDER RECEIVED, AND SHE  
4 FOLLOWED THE PROTOCOL THAT WAS IN PLACE AT THAT TIME.

5 THE COURT: OKAY.

6 Q BY MS. HARRIS: AND I KNOW YOU MENTIONED IT IS NOW,  
7 BUT IT IS -- NOW SINGLE SOURCE DOWNLOAD IS INCLUDED IN THE  
8 PROGRAM THAT YOU RUN.

9 WHEN EXACTLY DID SINGLE SOURCE DOWNLOAD BECOME AN  
10 OPTION IN THE PROGRAM?

11 A AND I'M GOING TO HAVE TO APPROXIMATE. FOR THE TOOL  
12 THAT I'M INVOLVED WITH THE DEVELOPMENT OF, I WOULD SAY  
13 SOMETIME IN 2009, MAYBE JUNE OF 2009.

14 THE COURT: AND WHAT TOOL ARE YOU TALKING ABOUT?  
15 PHEX OR WHAT ARE YOU TALKING ABOUT?

16 THE WITNESS: IT'S A MODIFIED VERSION OF PHEX --

17 THE COURT: OKAY.

18 THE WITNESS: -- WHERE WE'VE ADDED THE OPTION TO DO  
19 A SINGLE SOURCE DOWNLOAD --

20 THE COURT: OH, OKAY.

21 THE WITNESS: -- AND THEN, THERE'S A PROGRAM --

22 THE COURT: SO IT'S AN OPTION, IT'S NOT JUST  
23 AUTOMATIC?

24 THE WITNESS: NO, BECAUSE WE STILL NEED TO BE ABLE  
25 TO DO THE NORMAL DOWNLOAD THAT DETECTIVE CORDER DID. WE STILL

1 USE THE SAME PRACTICE THAT SHE USED BACK IN 2008. WE STILL  
2 USE THAT SAME PRACTICE TODAY BECAUSE WE DON'T RESTRICT THE  
3 OFFICER TO ONLY DO A SINGLE SOURCE DOWNLOAD. THAT'S TO LET  
4 THE OFFICER DO AN INVESTIGATION INTO A DISSEMINATION.

5 WE GIVE THEM THE OPTION TO SEE THAT IT COMES FROM  
6 LOTS OF PEOPLE. WE DON'T CARE WHERE IT COMES FROM, WE JUST  
7 CARE THAT WE GET THE EXACT SAME FILE THAT WAS PRESENTED TO US  
8 IN THAT BROWSE HOST LIST BECAUSE THROUGH ALL THE TESTING I'VE  
9 DONE, I KNOW WITH CERTAINTY EVERY FILE IN THAT LIST ARE WHOLE  
10 FILES SHARED. IF I KNOW THE VALUE OF THE BROWSE HOST, I DON'T  
11 CARE IF YOU DOWNLOAD IT FROM GNUTELLA THE NORMAL WAY; I DON'T  
12 CARE IF I CALL YOU UP ON THE PHONE, AND I GIVE IT TO YOU OR  
13 MAYBE I'VE INVESTIGATED SOMEONE IN THE PAST WHERE WE HAVE THE  
14 VALUE -- WE LOG THE HASH VALUES OF ALL THESE FILES THAT I  
15 USE -- SOMEHOW, SOME WAY, I CAN GET THAT SAME FILE TO DESCRIBE  
16 IT, THAT'S PROBABLE CAUSE ALL DAY LONG.

17 THE COURT: AND YOU KNOW IT'S RELIABLE TO YOU THAT  
18 USER HAS THAT FULL FILE ON HIS MACHINE OR IS THAT TOO MUCH OF  
19 A JUMP?

20 THE WITNESS: NO. I'VE BEEN INVESTIGATING THESE  
21 CASES FOR YEARS. I'VE BEEN INVOLVED IN THE -- HUNDREDS OF  
22 INVESTIGATIONS USING THIS SAME PROCESS. I HAVE NEVER --  
23 AND -- AND IF I DO THE CASE, JUDGE, I'M THE GUY DOING THE  
24 INVESTIGATION, WHERE I'VE BROWSED HIS FILES, I'M THE GUY  
25 WRITING THE AFFIDAVIT TO GET THE SUBSCRIBER FROM THE INTERNET

1 COMPANY, I'M THE GUY THAT DOES THE SEARCH WARRANT, AND I'M THE  
2 GUY THAT DOES THE COMPUTER FORENSICS. I GET TO SEE THE CASE  
3 BEGINNING TO END, SO -- I KNOW MISS LOEHRS HAD DONE THE  
4 FORENSICS ON CERTAIN COMPUTERS, BUT, REALLY, SHE'S MISSING A  
5 BIG PART OF THE PICTURE I'M ABLE TO TAKE FROM BEGINNING TO  
6 END, AND I KNOW OF NO INSTANCE WHERE I HAVEN'T BEEN ABLE TO  
7 FIND THE FILES ON THE COMPUTER AT THE END OF THE -- AT THE END  
8 OF THE INVESTIGATION.

9 I JUST WANT TO QUALIFY THAT ANSWER TO SAY THAT THE  
10 ONLY SCENARIO IS IS WHEN I DON'T FIND THE COMPUTER THAT WAS IN  
11 THE HOUSE THAT DAY, AND WE CAN TELL IN THE FORENSIC WORLD,  
12 THERE ARE INDICATORS OR THINGS THAT I CAN LOOK FOR THAT WILL  
13 TELL ME WITH ALL CERTAINTY THAT'S THE RIGHT COMPUTER.

14 THE COURT: AND BROWSE HOST, IS THAT THE ONE THAT  
15 HAS THE LINE THAT GOES ACROSS AND TELLS YOU IT'S COMPLETE OR I  
16 GOT THAT WRONG?

17 THE WITNESS: NO.

18 THE COURT: WHAT DOES THAT?

19 THE WITNESS: THAT'S DURING KEYWORD SEARCHES.

20 THE COURT: OH.

21 THE WITNESS: IF I CHOSE TO DOWNLOAD THE FILE IN A  
22 NORMAL WAY, AS SOON AS I DOUBLE CLICK THAT FILE AND SAY I WANT  
23 TO DOWNLOAD THE FILE, THE NEXT SCREEN I GO TO IS A DOWNLOAD  
24 SCREEN, WHERE IT LISTS THE I.P. ADDRESS THAT HAS THE FILE, THE  
25 FILE I FOUND DURING THE KEYWORD SEARCH, BUT THERE'S A LITTLE

1 METER THAT TELLS ME WHAT PERCENT OF THE FILE HE POSSESSES, AND  
2 THAT'S WHERE I WAS -- I'M TALKING ABOUT THAT WHOLE OTHER  
3 ELEMENT HERE, THAT KEYWORD SEARCH.

4 THAT'S WHERE I WAS ABLE TO SIT HERE IN THIS COURT  
5 AND SAY I'VE -- I'VE LOOKED AT HUNDREDS OF PEOPLE THAT I'VE  
6 FOUND VIA A KEYWORD SEARCH, AND I'VE NEVER FOUND AN INSTANCE  
7 WHERE HE ONLY HAD PART OF THE FILE, LIKE MISS LOEHRS TESTED.

8 THE COURT: OKAY.

9 (THERE WAS A BREAK IN THE PROCEEDINGS AT  
10 2:47 P.M. UNTIL 3:03 P.M.)

11 THE COURT: ALL RIGHT. BACK ON THE RECORD, ALL  
12 PARTIES AND COUNSEL PRESENT.

13 TURN IT BACK OVER TO MISS HARRIS.

14 Q BY MS. HARRIS: NOW, BEFORE WE TOOK A BREAK,  
15 CORPORAL ERDELY, YOU HAD INDICATED THAT, BASED ON YOUR  
16 TRAINING AND EXPERIENCE, YOU HAVE NOT EVER COME ACROSS A TIME  
17 WHERE A PARTIAL FILE WOULD SHOW AS AVAILABLE FOR SHARING,  
18 SIMILAR TO THAT OF A COMPLETED FILE; RIGHT?

19 AM I MISPHRASING THAT?

20 A NO, IN BOTH THE SEARCH -- KEYWORD SEARCH AND THE  
21 BROWSE HOST; HOWEVER, THE BULK OF MY TESTING WAS WITH THE  
22 BROWSE HOST BECAUSE THAT WAS THE STARTING POINT FOR OUR  
23 INVESTIGATIONS.

24 Q AND I THINK WE ALREADY CLARIFIED THAT'S WHAT  
25 DETECTIVE CORDER DID IN THIS CASE?

1           A        YES, MA'AM.

2           Q        NOW, I KNOW YOU MADE REFERENCE TO WHEN YOU GET A --  
3        SAY, A PARTICULAR FILE.

4                    YOU BROWSE A HOST, YOU FIND A FILE, AND YOU GET --  
5        DOWNLOAD IT, AND YOU GET BITS AND PIECES FROM OTHER PLACES?

6           A        YES.

7           Q        ARE YOU FOLLOWING ME; AND IF I'M UNDERSTANDING YOUR  
8        TESTIMONY CORRECTLY, IT DOESN'T MATTER WHERE THE BITS AND  
9        PIECES COME FROM, AT THAT POINT, YOU'RE JUST TRYING TO COMPARE  
10       IT TO THE FILE YOU SAW WHEN YOU BROWSED THE PERSON YOU  
11       CONNECTED TO?

12          A        THAT'S CORRECT; AND I WENT ONTO SAY IT DOESN'T  
13        MATTER IF I ALREADY HAVE IT. IF I CALL ANOTHER INVESTIGATOR  
14        THAT I KNOW HAS IT OR IF WE GET IT FROM THE PLACE THAT,  
15        NORMALLY, IT'S FOUND, WHICH HAPPENS TO BE GNUTELLA, MY GOAL IS  
16        JUST TO BE ABLE TO COMPARE THE HASH VALUE, THE FILE SIGNATURE  
17        THAT TELLS ME WITH CERTAINTY THIS IS THE SAME FILE HE HAD. I  
18        WANT TO BE ABLE TO DESCRIBE IT IN AN AFFIDAVIT BECAUSE I KNOW  
19        THE MOMENT IN TIME I BROWSED HIM, HE POSSESSED THAT FILE AT  
20        THAT MOMENT IN TIME.

21                   THE COURT: AND IT WAS COMPLETE?

22                   THE WITNESS: AND THAT IT WAS COMPLETE, JUDGE.

23          Q        BY MS. HARRIS: NOW, WHEN YOU SAY HASH VALUE, IS  
24        THAT THE SAME AS A SHA-1 VALUE?

25          A        YES. THERE'S DIFFERENT TYPES OF FILE HASHING. THE



1 TWO BIGGEST OR MOST POPULAR HASH VALUES YOU'LL BE HEARING  
2 ABOUT AND TALKING ABOUT IN COURT WOULD BE AN MD5 HASH OR SHA-1  
3 HASH. YOU HEAR IT ALL THE TIME AS IT RELATES TO COMPUTER  
4 FORENSICS. SHA-1 HASHING IS EVEN MORE UNIQUE AND MORE  
5 SPECIFIC TO A FILE, SO JUST LUCKY FOR LAW ENFORCEMENT THAT THE  
6 PEOPLE WHO DEVELOPED GNUTELLA, WHICH IS THE FILE SHARING  
7 NETWORK THAT LIMEWIRE WORKS ON, THEY HAPPEN TO USE SOME OF THE  
8 STRONGER FILE IDENTIFICATION OR HASHING ALGORITHMS OUT THERE,  
9 SO ME, AS A LAW ENFORCEMENT OFFICER, I CAN LOOK AT THOSE  
10 RESULTS, RELY UPON THOSE RESULTS, AND DO THE INVESTIGATIONS WE  
11 DO.

12 I'M NOT SURE WHO TO THANK, BUT THAT WAS GREAT FOR  
13 LAW ENFORCEMENT.

14 Q SO A SHA-1 WAS EVEN MORE RELIABLE IN YOUR TRAINING  
15 AND EXPERIENCE?

16 A RIGHT. MD5 IS A HUNDRED AND TWENTY-EIGHT BITS LONG,  
17 AND SHA-1 IS A HUNDRED AND SIXTY; JUST -- IT'S A BIGGER SET OF  
18 NUMBERS AND LETTERS REPRESENTING THE SIGNATURE OF A FILE.

19 Q SAY, FOR EXAMPLE, I CHANGE ANY PORTION OF THAT FILE,  
20 BE IT I ALTER THE IMAGE OR ANYTHING LIKE THAT.

21 WOULD THE SHA-1 VALUE OR THE HASH VALUE OF THAT  
22 PARTICULAR FILE CHANGE?

23 A YES, AND IT DOESN'T JUST CHANGE A LITTLE BIT. THIS  
24 IS A -- A FIXED LENGTH IDENTIFIER FOR A FILE OF ANY SIZE, SO  
25 IF I HAD A TEXT DOCUMENT THAT WAS A HUNDRED MILLION CHARACTERS

1 IN LENGTH, AND I CHANGED ONE PERIOD TO A COMMA OUT OF ALL  
2 HUNDRED MILLION CHARACTERS IN THIS FILE, THE HASH VALUE IS  
3 SIGNIFICANTLY DIFFERENT. INSTEAD OF BEING A12B4F, IT'S NOW  
4 SOMETHING COMPLETELY DIFFERENT. IT DOESN'T EVEN LOOK CLOSE TO  
5 WHAT IT USED TO -- WHAT THE VALUE USED TO BE, SO IT'S PRETTY  
6 HARD -- IT'S PRETTY EASY TO RECOGNIZE DIFFERENCES AND PRETTY  
7 HARD TO GET CONFUSED BECAUSE A LITTLE CHANGE IS SIGNIFICANTLY  
8 GOING TO ALTER THE HASH VALUE OF THAT FILE.

9 Q OKAY. SO I JUST WANT TO MAKE SURE I'M UNDERSTANDING  
10 YOUR TESTIMONY CORRECTLY HERE.

11 WHEN -- IN -- SAY, FOR EXAMPLE, IN THIS CASE WHEN  
12 DETECTIVE CORDER DID A BROWSE HOST, AND SHE DIRECTLY CONNECTED  
13 TO THE DEFENDANT, MR. MORAN -- OR HIS COMPUTER --

14 A YES.

15 Q -- I GUESS, IS THE BEST WAY TO PHRASE THAT; SHE  
16 DIRECTLY CONNECTED TO MR. MORAN'S COMPUTER?

17 A CORRECT.

18 Q OKAY. AND WHEN SHE DIRECTLY CONNECTED TO HIS  
19 COMPUTER, AT THAT POINT, SHE THEN DID A BROWSE HOST?

20 A CORRECT.

21 Q WELL --

22 A THE BROWSE HOST DID DIRECTLY CONNECT TO THE COMPUTER  
23 AT MR. MORAN'S HOUSE.

24 Q AND AT THAT POINT, THEN, SHE LOOKED AT THE FILES  
25 THAT HE HAD AVAILABLE FOR SHARING IS THE QUESTION I MEANT TO

1 ASK.

2 A YES, AND IN THAT LIST IS NOT JUST THE FILE NAME. I  
3 THINK, A COUPLE TIMES, THE COURT WAS TOLD JUST THE FILE NAME'S  
4 THERE, BUT IT'S THE FILE NAME AND HASH VALUE.

5 Q OKAY. SO WHEN YOU BROWSE A HOST, YOU SEE THE FILE  
6 NAME, AND YOU SEE THE HASH VALUE OR THE SHA-1 VALUE?

7 A CORRECT. WE CAN USE, IN THIS CASE, THOSE TWO TERMS.  
8 THEY'RE SYNONYMOUS.

9 Q OKAY. AND AT THAT MOMENT, AN INVESTIGATOR IN  
10 GENERAL, AND THEN, DETECTIVE CORDER IN PARTICULAR, IN THIS  
11 CASE, WOULD THEN DOWNLOAD OR TRY TO SEARCH FOR THE SAME SHA-1  
12 VALUE OF -- TO COMPARE IMAGES.

13 IS THAT FAIR TO SAY?

14 A CORRECT. THEY GET IT SOMEHOW, SOME WAY, AND VERIFY  
15 IT'S THE SAME HASH VALUE.

16 Q OKAY. AND ONCE YOU DO THAT, YOU THEN ORDINARILY,  
17 TYPICAL, LAW ENFORCEMENT WOULD HAVE PROBABLE CAUSE?

18 A CORRECT.

19 Q OKAY. AND AT THAT POINT, GENERATE A SEARCH WARRANT?

20 A CORRECT. I'VE DONE MANY, MANY SEARCH WARRANTS  
21 IN-STATE, AND I'VE AUTHORED FEDERAL SEARCH WARRANTS IN  
22 DIFFERENT DISTRICTS IN PENNSYLVANIA AND BEEN -- EVEN PARTS OF  
23 ONES IN OTHER DISTRICTS, AS WELL, AND IT'S A STANDARD PRACTICE  
24 AND USED -- USED TO THIS DAY.

25 Q AND THAT DOESN'T MATTER WHETHER YOU HAVE ONE IMAGE,

1 TEN IMAGES OR 47 IMAGES?

2 A RIGHT. A CRIME'S COMMITTED, AND THIS IS A PLACE WE  
3 NEED TO SEARCH.

4 Q AND YOU'VE HAD AN OPPORTUNITY TO LOOK AT THE SEARCH  
5 WARRANT AFFIDAVIT IN THIS CASE; CORRECT?

6 A YES.

7 Q IS THERE ANYTHING, BASED ON YOUR TRAINING AND  
8 EXPERIENCE, BE IT IN LAW ENFORCEMENT OR YOUR TRAINING AND  
9 EXPERIENCE WITH COMPUTERS AND HOW THE SOFTWARE WORKS, THAT YOU  
10 FOUND MISLEADING ABOUT THE AFFIDAVIT SUBMITTED BY  
11 DETECTIVE CORDER?

12 A NO, ABSOLUTELY NOT. WHEN I WRITE AN AFFIDAVIT FOR A  
13 SEARCH WARRANT, I'M NOT REQUIRED TO PUT IN ALL FACTS. I PUT  
14 IN ENOUGH FACTS TO ESTABLISH PROBABLE CAUSE.

15 IF THERE WAS A REASON WHY I THOUGHT THAT THE  
16 EVIDENCE SOUGHT AFTER WASN'T IN THE LOCATION TO BE SEARCHED, I  
17 WOULDN'T BE APPLYING FOR IT, SO -- MATTER OF FACT, IN MY  
18 WARRANTS, OFTENTIMES, MOSTLY MY FEDERAL WARRANTS, I'LL  
19 ACTUALLY SAY THIS ISN'T EVERY FACT KNOWN TO ME IN THIS CASE,  
20 BUT I'M SIMPLY LAYING OUT THE FACTS NECESSARY TO ESTABLISH  
21 PROBABLE CAUSE.

22 Q OKAY. NOW, YOU'VE HAD AN OPPORTUNITY TO -- NOT  
23 HAVING REVIEWED THE SEARCH WARRANT AFFIDAVIT, YOU'VE HAD AN  
24 OPPORTUNITY TO REVIEW THE TWO AFFIDAVITS BY TAMI LOEHRS, THE  
25 DEFENSE EXPERT?

1           A       YES, MA'AM.

2           Q       OKAY.  AND I WANT TO START WITH -- JUST MAKING SURE  
3 I HAVE IT RIGHT.  HER FIRST --

4           THE COURT:  IT'S EXHIBIT 2?

5           MS. HARRIS:  YEAH, HER FIRST AFFIDAVIT DATED  
6 JANUARY 10TH OF 2010.

7           IF I COULD APPROACH THE WITNESS, JUDGE.

8           THE COURT:  SURE.

9           THE WITNESS:  YES, MA'AM.

10          Q       BY MS. HARRIS:  OKAY.  AND YOU RECALL LOOKING OVER  
11 THAT AFFIDAVIT; CORRECT?

12          A       YES.

13          Q       OKAY.  AND I'M -- YOU WERE PRESENT WHEN I ASKED  
14 MISS LOEHRS ABOUT THE VICTOR SMITH ARTICLE?

15          A       CORRECT.

16          Q       OKAY.  NOW, BASED ON YOUR UNDERSTANDING OF THE  
17 VICTOR SMITH, ARTICLE WHEN YOU DOWNLOAD A FILE, BE IT  
18 CANCELLED OR PARTIAL OR CORRUPTED, DOES THAT DOWNLOAD GO INTO  
19 THE DOWNLOAD.DAT?

20          A       IT GOES DOWN INTO THE DOWNLOAD.DAT AND DOES NOT GO  
21 INTO THE FILEURNS.CACHE.

22          Q       SO WHEN YOU REVIEWED MISS LOEHRS -- AND I'M GOING TO  
23 START WITH THE FIRST ONE, DATED JANUARY 10TH OF 2010, DID YOU  
24 MAKE ANY CONCLUSIONS OR COME TO ANY OPINIONS ABOUT THE  
25 AFFIDAVIT IN REFERENCE TO WHERE FILES GO THAT ARE SHARED OR

1 PARTIAL OR DELETED OR CORRUPTED OR INCOMPLETE?

2 A SO AS LONG AS WE'RE TALKING ABOUT INCOMPLETE  
3 FILES --

4 Q YES.

5 A -- THEN IT GOES INTO THE DOWNLOADS.DAT. ONCE THAT  
6 FILE COMPLETES, IT GOES INTO THE FILEURNS.CACHE.

7 Q OKAY. SO IN OTHER WORDS -- IF I'M UNDERSTANDING  
8 YOUR TESTIMONY CORRECTLY, IN ORDER FOR THE FILE TO SHOW IN THE  
9 FILEURNS.CACHE, IT WOULD HAVE TO BE A COMPLETED FILE?

10 A YES, AND THAT'S WHY I LOOK FOR ENTRIES IN  
11 FILEURNS.CACHE BECAUSE YOU CAN RECOVER THAT OLD INFORMATION  
12 FORENSICALLY, A LOT OF TIMES, AND IT'S SIGNIFICANT BECAUSE OF  
13 THE FINDINGS OF VICTOR SMITH AND MY OWN PERSONAL TESTING,  
14 WHICH I'VE REDONE AND, YOU KNOW, PRESENTED TO YOU.

15 Q OKAY. AND LET'S TALK ABOUT THAT. I'M GOING TO SHOW  
16 YOU WHAT HAS BEEN MARKED AS EXHIBIT NUMBER 1. THAT IS  
17 MISS LOEHR'S AFFIDAVIT DATED MAY 12TH OF 2011.

18 DID YOU HAVE AN OPPORTUNITY TO REVIEW THAT  
19 PREVIOUSLY?

20 A YES.

21 Q OKAY. WHAT CONCLUSIONS OR OPINIONS DID YOU COME TO  
22 IN REGARDS TO THE ASSERTIONS MADE IN THAT AFFIDAVIT IN REGARDS  
23 TO THE TESTING IN LIMEWIRE?

24 A HER TESTING IN LIMEWIRE WAS TROUBLESOME TO ME  
25 BECAUSE THE FIRST THING I NOTICED, WELL, WAS -- I CAN'T SAY

1 FOR CERTAIN IT WAS THE ABSOLUTE FIRST THING I NOTICED, BUT I  
2 NOTICED THAT SHE HAD ONE COMPLETELY DOWNLOADED FILE THAT WAS  
3 BEING SHARED IN AN ENVIRONMENT WHERE SHE'S SUPPOSED TO BE  
4 TESTING AND MAKING AN OPINION AS AN EXPERT, AND THAT WAS  
5 TROUBLESOME TO ME BECAUSE THE DOCUMENTATION IN THE AFFIDAVIT  
6 SAYS THAT SHE HAD A FILE THAT WAS ONLY DOWNLOADED TEN PERCENT,  
7 THE AC/DC FILE.

8 WELL, I KNOW, AND THE EXHIBITS THAT I HAVE HERE IN  
9 MY TESTING KNOW -- SHOWS ME, IN MY DAILY USE OF THE PROGRAM,  
10 THAT LITTLE NUMBER IN THE BOTTOM, THAT ONE THAT WAS CIRCLED  
11 AT --

12 Q IF I COULD -- IF I COULD APPROACH -- SORRY -- WE CAN  
13 PUT IT UP, AND THEN, WE CAN SHOW THE COURT.

14 A OH, THAT'S AN INDICATOR OF A WHOLE FILE THAT'S BEEN  
15 DOWNLOADED AND NOW BEING SHARED. IT DOES NOT GET IMPLEMENTED  
16 WHEN A PARTIAL FILE IS PRESENT, SO IF I'M GOING TO DO A TEST  
17 AND HAVE IT BE A VALID TEST, I CERTAINLY WOULDN'T BE SHARING A  
18 FILE THAT I CAN'T EVEN RECALL WHAT IT WAS FOR.

19 ALL I KNOW IT WAS THE SAME FILE THAT SHE ALLEGES WAS  
20 FOUND BY HER ON ANOTHER COMPUTER. SHE WAS ASKED, AND I WAS  
21 SITTING HERE, AND SHE TESTIFIED SHE DID TESTING ALL DAY DURING  
22 THIS DEMONSTRATION FOR THE FEDERAL PUBLIC DEFENDER'S; I  
23 BELIEVE IT WAS BACK IN APRIL. I WROTE DOWN THE DATE, AND SHE  
24 CAN'T EVEN RECALL WHAT FILE THAT MIGHT HAVE BEEN, BUT EVEN IN  
25 HER OWN TESTIMONY, SHE ACKNOWLEDGES THAT THAT'S A FILE THAT

1 WAS DOWNLOADED COMPLETELY, BEING SHARED AND NOT THE ONE THAT'S  
2 HIGHLIGHTED FOR THE PURPOSES OF HER AFFIDAVIT AND HER  
3 PRESENTATION TO THIS COURT, SO THAT'S TROUBLESOME BECAUSE NOW,  
4 SHE'S GOING TO SAY WITH ALL CERTAINTY THESE ARE THE FACTS, BUT  
5 YET SHE HASN'T PROPERLY DOCUMENTED HER OWN TEST.

6 Q OKAY. IS THERE ANYTHING ELSE ABOUT ANY OTHER  
7 CONCLUSIONS OR OPINIONS YOU CAME TO IN REGARDS TO MRS. LOEHR'S  
8 AFFIDAVIT TO THIS COURT DATED MAY 12TH OF OF 2011?

9 A WELL, SECONDLY, SHE USED LIMEWIRE 4.18.8. SHE USED  
10 A VERSION -- AND I UNDERSTAND THAT SHE HAS TESTIFIED THAT  
11 THESE SLIDES WERE MADE BEFORE SHE KNEW WHAT VERSION WE WERE  
12 TALKING ABOUT, BUT I DON'T KNOW WHY SHE DIDN'T HAVE TIME  
13 BETWEEN WHEN SHE LEARNED UNTIL NOW -- SHE CHOSE TO USE SLIDES  
14 THAT ARE IRRELEVANT BECAUSE SHE USED A WHOLE DIFFERENT VERSION  
15 THAT COULD REACT COMPLETELY DIFFERENTLY THAN THE VERSION IN  
16 QUESTION HERE, WHICH WAS -- WHICH IS LIMEWIRE 4.14.0. THAT IS  
17 THE MOST APPROPRIATE TEST.

18 WHEN I'M VALIDATING SOFTWARE, IF I WANT TO PROVE, AS  
19 A FORENSIC EXAMINER, THAT SOFTWARE WORKS, PART OF WHAT WE DO  
20 IS VALIDATE THAT SOFTWARE. WE USE OTHER PIECES OF SOFTWARE TO  
21 PROVE ITS RELIABILITY, SO I'M SURE MISS LOEHR'S IS FAMILIAR  
22 WITH A PROCESS TO VALIDATE SOFTWARE. HERE, SHE'S COMING TO A  
23 CONCLUSION USING A VERSION OF SOFTWARE THAT IS NOT IN  
24 QUESTION, SO THE MOST APPROPRIATE TEST WOULD HAVE BEEN TO TAKE  
25 SOME TIME, DOWNLOAD LIMEWIRE 4.14.0 AND TRY TO REPLICATE THIS



1 TEST.

2 IN HER TESTIMONY, SHE SAYS THAT SHE CAN'T REPLICATE  
3 IT. I DO RECALL THAT, SO THEN, THE FINAL THING THAT I'D LIKE  
4 TO NOTE ABOUT HER AFFIDAVIT, WHICH IS -- I THINK, MAKES IT NOT  
5 VERY -- IT DOESN'T -- YOU KNOW, I DIDN'T CONSIDER IT MUCH AS  
6 IT RELATES TO THIS CASE BECAUSE SHE FAILED TO TEST THE ONE  
7 THING THAT'S IN QUESTION HERE: SHE FAILED TO TEST THE BROWSE  
8 HOST.

9 I KNOW THAT SHE CANNOT SHOW ME ANY VERSION 4-- LET'S  
10 JUST SAY FROM VERSION 4.14.0 TO 4.18.8 -- SHE CANNOT SET UP AN  
11 ENVIRONMENT WHERE A BROWSE HOST SHOWS PARTIAL FILES, BUT THAT,  
12 I GUESS, WOULDN'T SERVE THEIR POSITION THAT THEY'RE IN TO SHOW  
13 THAT IT WAS A WHOLE FILE, BUT IT WAS COMPLETELY LEFT OUT OF  
14 HER REPORT; AND SHE TESTED IT BEFORE, AND SHE CAME TO THE  
15 CONCLUSION THEY'RE WHOLE FILES.

16 I THINK THAT'S EXTREMELY IMPORTANT FOR THIS COURT TO  
17 CONSIDER, AND SO THAT'S -- I DID THE TESTS IN MY REPORT THAT  
18 WERE THE SAME VERSIONS BEING SHARED -- OR USED BY THE  
19 DEFENDANT IN THIS CASE.

20 Q SO IF I'M UNDERSTANDING YOU CORRECTLY, THE BIGGER  
21 QUESTION IS NOT NECESSARILY TESTING PEER SPECTRE, THE BETTER  
22 PROGRAM TO TEST IN THIS CASE, AS FAR AS WHAT FILES WERE THERE  
23 AND AVAILABLE FOR SHARING WOULD BE THE LIMEWIRE SOFTWARE?

24 A ABSOLUTELY, AND IT'S STILL AVAILABLE IN ITS SOURCE  
25 CODE AND THE PROGRAM. I MEAN, IT'S COMPLETELY THE OPPOSITE OF

1 ANY RATIONAL WAY THAT I WANTED TO TEST SOFTWARE, SO IF I  
2 WANTED TO TEST TO SEE HOW A -- AN E-MAIL SERVER WORKED, SO  
3 WE'RE ALL FAMILIAR ABOUT -- YOU KNOW, E-MAIL AND HOW THE --  
4 THERE ARE SERVERS THAT TRACK THE E-MAIL COMING IN AND GOING  
5 OUT, SO I WANT TO MAKE SURE THAT THAT'S WORKING PROPERLY.

6           WOULD I TAKE EVERY CLIENT THAT EXISTED IN THE WORLD  
7 AND TRY TO SEND AND RECEIVE E-MAIL TO IT? NO, I'D TEST THE  
8 SERVER ITSELF. HERE, WE ARE IN A UNIQUE POSITION TO HAVE THE  
9 EXACT SOFTWARE THAT THE DEFENDANT WAS USING IN THIS CASE, SO  
10 IF SHE NEEDS TO TEST PEER SPECTRE, SHE MIGHT AS WELL TEST  
11 LIMEWIRE, PHEX, BEARSHARE, DEXTERWIRE. I MEAN, I'M NAMING OFF  
12 ALL THESE NAMES, AND I DON'T WANT TO TROUBLE THE COURT  
13 REPORTER, BUT EVERY NEW VERSION OF EVERY GNUTELLA CLIENT NAMED  
14 ON THE PLANET OR MAYBE JUST LOOK AT THE SOURCE CODE THAT TELLS  
15 YOU EXACTLY WHAT A FILE BROWSE REPRESENTS AND KNOW, WITH ALL  
16 CERTAINTY, YOU KNOW WHAT'S HAPPENING IN THE BACKGROUND.

17           TEST LIMEWIRE, DON'T TEST THE SEARCHING CLIENT. THE  
18 SEARCHING CLIENT CAN ONLY SEE WHAT LIMEWIRE SHOWS IT. SHE  
19 WANTS TO MAKE SURE LAW ENFORCEMENT ISN'T DOING ANYTHING THAT  
20 THE GENERAL PUBLIC CAN'T DO. WELL, THE BEST PIECE OF SOFTWARE  
21 TO TEST IS THE CLIENT THAT CHOOSES TO GIVE ME THOSE KEYWORD  
22 SEARCH RESULTS, AND SHE HAS THAT AT HER DISPOSAL; AND IN THIS  
23 PARTICULAR CASE, HE -- SHE'S EVEN IN A MORE UNIQUE POSITION  
24 BECAUSE SHE HAS ACCESS TO THE ACTUAL PROGRAM THE INVESTIGATOR  
25 USED, UNMODIFIED BY LAW ENFORCEMENT. SHE HAS THE SOURCE CODE

1 TO THAT TO LOOK AT, AS WELL, SO SHE HAS ACTUALLY BOTH ENDS OF  
2 THE COMMUNICATION OF THIS INVESTIGATION; AND FROM OCTOBER TO  
3 PRESENT, SHE HASN'T TESTED THAT BY HER OWN TESTIMONY, AND I'VE  
4 TESTED IT FOR YEARS. I KNOW HOW IT OPERATES, AND I TEACH IT,  
5 YOU KNOW, TO PEOPLE ALL AROUND THE WORLD.

6 Q OKAY. SO IF I'M UNDERSTANDING YOU CORRECTLY, THE  
7 PROPER THING, IN YOUR OPINION, WOULD BE TO TEST THE LIMEWIRE  
8 SOFTWARE?

9 A CORRECT; AND ALTHOUGH SHE SAID THROUGHOUT TIME,  
10 SPEAKING HISTORICALLY, SHE'S TESTED LIMEWIRE 4.14.0, I DIDN'T  
11 SEE ANY REFERENCE TO IT IN THE TWO AFFIDAVITS I REVIEWED. I  
12 DID HEAR IN HER TESTIMONY, ALTHOUGH SHE CAN'T RECALL DATES,  
13 TIMES, AND VERSIONS, BUT I'M CERTAIN SHE CANNOT PRESENT TO  
14 THIS COURT LIMEWIRE 4.14.0 SHOWING PARTIAL FILES THAT ARE  
15 BROWSED.

16 Q OKAY. AND WHAT ABOUT PHEX? WOULD THAT ALSO BE  
17 SOMETHING PUBLICLY AVAILABLE THAT YOU WOULD RECOMMEND HER  
18 TESTING TO VALIDATE ANY FILES THAT MAY HAVE OR MAY NOT HAVE  
19 BEEN ON THE DEFENDANT'S COMPUTER?

20 A YES. IT'S AVAILABLE ON THEIR WEBSITE, BOTH THE  
21 BINARY FILE, WHICH IS THE INSTALLER FOR ANY OPERATING  
22 SYSTEM -- IN THIS CASE, SHE WOULD WANT TO TEST THE WINDOWS  
23 VERSION, SINCE THAT'S WHAT DETECTIVE CORDER USED, AND ITS  
24 SOURCE CODE IS AVAILABLE.

25 BOTH LIMEWIRE AND PHEX IS WRITTEN IN JAVA. I HEAR

1 HER SPEAK TO SOME DEGREE ABOUT JAVA AND THE FACT THAT IT'S  
2 HARD TO COMPILE, AND YOU CAN SEE THE SOURCE CODE, SO I KNOW  
3 SHE HAS SOME KNOWLEDGE INTO JAVA PROGRAMMING, BUT IF SHE IS  
4 SKILLED, ANY SKILLED JAVA PROGRAMMER CAN LOOK AT THE SOURCE  
5 CODE AND SEE THAT PEER SPECTRE WOULD NOT SEE ANY OTHER RESULTS  
6 THAN WHAT LIMEWIRE CHOOSES TO SEND OUT AS A SEARCH HIT.

7 THERE IS ONE MORE FLAW IN HER TESTING, IS -- WELL,  
8 NO, I THINK THAT SUMS IT UP. I APOLOGIZE.

9 Q I WANT TO ASK YOU A QUESTION: YOU'RE LOOKING AT THE  
10 SCREEN SHOT ON THE AFFIDAVIT, AND I CAN ZOOM OUT A LITTLE BIT.

11 IN THE AFFIDAVIT -- AND THIS IS ON PAGE 2 OF THE  
12 MAY 12TH AFFIDAVIT -- WHEN YOU LOOK AT THIS SCREEN SHOT,  
13 ORDINARILY, WHEN YOU OPEN UP LIMEWIRE, IS THERE AN OPTION FOR  
14 YOU TO SEE, SAY, FOR EXAMPLE, AN I.P. ADDRESS?

15 A WELL, IN THIS VERSION HERE, THE ONE SHE CHOSE TO  
16 USE, I THINK, BY DEFAULT, IT'S NOT VISIBLE, BUT THERE'S AN  
17 OPTION WHERE YOU COULD RIGHT CLICK ON THE -- ABOVE ALL THOSE  
18 FILE NAMES THAT ARE THERE, THERE'S A BAR, AND IT WOULD  
19 DESCRIBE ON WHAT EACH COLUMN REPRESENTS. IF YOU CLICK ON THAT  
20 BAR, THERE ARE OPTIONS TO SHOW MORE INFORMATION TO THE USER OF  
21 THE PROGRAM.

22 BY DEFAULT, IT'S NOT THERE, BUT IF I WAS GOING TO DO  
23 A TEST -- AND I DID DO A TEST, AND THIS IS WHAT I DID; I CHOSE  
24 TO SHOW THE I.P. ADDRESS THAT WAS SHARING THE FILE, THE FACT  
25 THAT ETHERNET IS THERE OR NOT THERE, I WOULD SUGGEST YOU WOULD

1 HAVE TO GO INTO THE SOURCE CODE TO DEFINE WHAT THAT MEANS; AND  
2 NOT KNOWING EXACTLY HOW THIS -- YOU KNOW, THIS EXAMPLE WAS  
3 LAID OUT, BUT IN A HOTEL ROOM, I CAN -- OR IN A HOTEL  
4 CONFERENCE CENTER, I CAN TELL YOU THAT THERE ARE MANY  
5 COMPUTERS THAT WOULD BE CLASSIFIED AS BEING ON THAT SAME  
6 ETHERNET CONNECTION.

7 IS IT POSSIBLE IT WAS ANOTHER COMPUTER? YES. IS  
8 THERE SOMETHING SHE COULD HAVE DONE THAT WOULD HAVE TAKEN  
9 ABOUT A HALF A SECOND TO IMPLEMENT TO SAY, WITH ALL CERTAINTY,  
10 YES, AND THAT WOULD BE TO DOCUMENT THE INTERNET ADDRESS OF  
11 COMPUTER ONE AND SHOW IT APPEARING IN THE INTERFACE OF  
12 COMPUTER TWO.

13 AGAIN, EVEN IF THAT HAPPENED, I WOULD QUESTION WHY  
14 SHE WOULD USE THAT VERSION TO PRESENT TO THIS COURT BECAUSE  
15 I -- I HAVEN'T SEEN IT.

16 Q AND BY THE 4.18 VERSION, YOU MEAN YOU WOULD QUESTION  
17 WHY SHE USED THAT VERSION IN RELATION TO THE 4.14 VERSION THAT  
18 THE DEFENDANT USED IN THIS CASE?

19 A RIGHT. I WOULD WANT TO TEST THE VERSION IN  
20 QUESTION. JUST LIKE WHEN I VALIDATE SOFTWARE, I VALIDATE THE  
21 SOFTWARE THAT I'M GOING TO USE.

22 Q OKAY. LET'S MAKE REFERENCE TO YOUR TESTING IN THIS  
23 CASE. I WANT TO TALK ABOUT THAT SPECIFICALLY.

24 CAN YOU TALK ABOUT WHEN YOU TESTED VERSION 4.14.

25 A I TESTED IT ON TWO OCCASIONS. I ASSISTED

1 DETECTIVE CORDER AND DETECTIVE LITCHFIELD IN THE FIRST TEST,  
2 AND DETECTIVE LITCHFIELD ACTUALLY DID THE SCREEN CAPTURES --

3 Q OKAY.

4 A -- HOWEVER I WAS THERE PRESENT VIRTUALLY, VIA REMOTE  
5 COMPUTING TECHNOLOGY, WHERE I COULD SEE HIS SCREEN, AND I  
6 COULD MOVE HIS MOUSE OR HE COULD MOVE HIS MOUSE WHILE  
7 EVERYTHING WAS HAPPENING. WE BOTH SAW IT SIMULTANEOUSLY, EVEN  
8 THOUGH I WAS PHYSICALLY LOCATED IN DALLAS ON THAT DAY --

9 Q OKAY.

10 A -- AND THAT WAS ON AUGUST 11TH.

11 Q ALL RIGHT. I WANT TO SHOW YOU WHAT HAS BEEN MARKED  
12 AS EXHIBIT NUMBER 13.

13 MR. GILLESPIE: WAS THIS DISCLOSED TO US?

14 MS. HARRIS: YES, THESE ARE THE SAME SCREEN SHOTS  
15 THAT ARE IN HIS REPORT.

16 Q BY MS. HARRIS: DO YOU RECOGNIZE THAT?

17 A YES. IT WAS MY TESTING THAT I PREPARED, AND IT WAS  
18 IN A REPORT DATED AUGUST -- AUGUST 16TH THAT I GAVE TO YOUR  
19 OFFICE THAT, IN TURN, WAS GIVEN TO THE DEFENSE.

20 ONE CAVEAT IS THAT THE SCREEN SHOTS REGARDING THE  
21 AUGUST 11TH TEST, WHICH IS ALSO IN EVIDENCE, THOSE ARE THE  
22 SCREEN SHOTS THAT DETECTIVE LITCHFIELD ACTUALLY SAID, CAPTURE  
23 THIS PART OF THE SCREEN, BUT I SAT THERE AND WATCHED IT.

24 MR. GILLESPIE: IF I MAY, WHEN ON THE 16TH WERE  
25 THOSE DISCLOSED TO MISS HARRIS? WHAT TIME?

1           THE WITNESS: JUST BEFORE THE END OF THE BUSINESS  
2 DAY. I WAS -- I STAYED UP THE NIGHT OF THE 15TH AND THEN  
3 WORKED ALL DAY THE 16TH, UNTIL -- IT WOULD HAVE BEEN ABOUT  
4 7:30 MY TIME, I THINK, ON THE 16TH, WHICH IS 4:30 HERE, RIGHT?  
5 IT WAS RIGHT BEFORE THE CLOSE OF BUSINESS.

6           MR. GILLESPIE: IF I REMEMBER CORRECTLY, JUDGE, AND  
7 MISS HARRIS, I'M SURE, WILL CORRECT ME IF I'M WRONG, SOME OF  
8 WHAT HE DID WASN'T DISCLOSED TO US UNTIL THE NEXT DAY, WHICH  
9 WOULD HAVE BEEN AFTER THE COURT-IMPOSED DEADLINE.

10          MS. HARRIS: JUDGE, IF I COULD CLARIFY, NONE OF THAT  
11 SUPPLEMENTAL INFORMATION -- BECAUSE LET ME JUST STATE FOR THE  
12 RECORD, WHEN CORPORAL ERDELY DID HIS TESTING, HE PUT IN HIS  
13 REPORT THAT HE WAS GOING TO CONTINUE TO RUN THE TEST UNTIL HE  
14 HAD TO TESTIFY IN COURT.

15          ANYTHING HE GAVE ME AFTER THE 16TH, ALTHOUGH I  
16 DISCLOSED IT TO DEFENSE COUNSEL OUT OF AN ABUNDANCE OF  
17 CAUTION, THE STATE IS NOT PRESENTING. THOSE SCREEN SHOTS ARE  
18 OUT OF HIS REPORT THAT HE PROVIDED TO THE STATE ON  
19 AUGUST 16TH, WHICH WAS DISCLOSED TO DEFENSE COUNSEL.

20          THE COURT: OKAY. ALL RIGHT. I GOT BOTH OF WHAT  
21 YOU'RE SAYING.

22          Q       BY MS. HARRIS: NOW, YOU MADE REFERENCE TO  
23 DETECTIVE LITCHFIELD'S EXAMINATION; CORRECT -- OR THE  
24 EXAMINATION YOU DID IN CONJUNCTION WITH DETECTIVE LITCHFIELD?

25          A       CORRECT, THE TEST WE RAN.

1 Q OKAY.

2 MS. HARRIS: AND BEFORE WE TALK ABOUT THAT, JUDGE, I  
3 WOULD LIKE TO MOVE TO ADMIT EXHIBIT 13.

4 THE COURT: OKAY. FOR PURPOSES OF THE HEARING.  
5 ANY OBJECTION?

6 MR. GILLESPIE: WELL, AGAIN, JUDGE, I WOULD OBJECT  
7 TO ANYTHING THAT WAS DONE AFTER THE COURT-IMPOSED DEADLINE,  
8 WHICH IS, AS I UNDERSTAND IT, A PORTION OF WHAT'S IN  
9 EXHIBIT 13.

10 MS. HARRIS: AND JUST FOR THE RECORD, JUDGE, IT IS  
11 NOT.

12 THE COURT: OKAY. ALL RIGHT. I'LL RULE ON THAT  
13 BEFORE THE CASE IS OVER.

14 GO AHEAD. I'VE GOT NOTES ON WHAT I HAVE TO DO.

15 MS. HARRIS: SO IS IT ADMITTED OR NOT? I'M SORRY.

16 THE COURT: OKAY. GO AHEAD -- NO, IT'S ADMITTED FOR  
17 PURPOSES OF THIS HEARING.

18 MS. HARRIS: OKAY.

19 Q BY MS. HARRIS: I'M GOING TO SHOW YOU WHAT HAS BEEN  
20 MARKED AS EXHIBIT NUMBER 5.

21 DO YOU RECOGNIZE THAT DOCUMENT?

22 A YES, IT'S DETECTIVE -- DETECTIVE LITCHFIELD'S REPORT  
23 OF OUR TEST THAT WE WORKED ON TOGETHER ON AUGUST 11TH OF THIS  
24 YEAR.

25 Q AND DOES THAT REPORT INCLUDE SCREEN SHOTS?



1 A YES, IT DOES.

2 Q OKAY. AND DID YOU HAVE AN OPPORTUNITY TO REVIEW  
3 THOSE SCREEN SHOTS?

4 A YES, I DID.

5 Q OKAY.

6 MS. HARRIS: IF I CAN APPROACH, JUDGE, WITH EXHIBIT  
7 NUMBER 4.

8 THE COURT: YES.

9 Q BY MS. HARRIS: DO YOU RECOGNIZE THIS DOCUMENT?

10 A YES.

11 Q WHAT EXACTLY IS THAT?

12 A THAT'S THE -- THE SCREEN SHOTS, A MORE CLEAR VERSION  
13 OF THEM THAT ARE BLOWN UP BUT ARE IN THAT REPORT.

14 Q OKAY. WHEN YOU SAY, THAT REPORT, YOU'RE REFERRING  
15 TO EXHIBIT NUMBER 5 IN DETECTIVE LITCHFIELD'S REPORT?

16 A YES.

17 MS. HARRIS: AT THIS POINT IN TIME, THE STATE WOULD  
18 MOVE TO ADMIT EXHIBITS -- NUMBER 4 AND EXHIBIT NUMBER 5.

19 THE COURT: ANY OBJECTION?

20 MR. GILLESPIE: COULD I JUST LOOK AT THE EXHIBITS  
21 REAL QUICK, JUDGE?

22 THE COURT: OH, SURE.

23 MR. GILLESPIE: NO OBJECTION FOR PURPOSES OF THIS  
24 HEARING.

25 THE COURT: ALL RIGHT. ADMITTED FOR PURPOSES OF THE

1 HEARING.

2 MS. HARRIS: IF I COULD APPROACH, JUDGE?

3 THE COURT: YEAH.

4 Q BY MS. HARRIS: I'M JUST GOING TO RETRIEVE FROM YOU  
5 EXHIBIT NUMBER 4, I BELIEVE, IS THE SCREEN SHOTS -- OH, NO  
6 EXHIBIT NUMBER 4.

7 A OH.

8 Q OKAY. NOW, I WANT TO START, IF YOU CAN EXPLAIN --  
9 I'M GOING TO GO THROUGH EACH PAGE, STARTING WITH THE FIRST  
10 PAGE OF EXHIBIT NUMBER 4.

11 A I HAVE THOSE IN MINE IN COLOR, ALSO.

12 Q OH, THAT'S WHAT I THOUGHT, BUT...ACTUALLY, LET'S  
13 JUST START WITH YOUR REPORT, EXHIBIT NUMBER 13, YOUR SCREEN  
14 SHOTS.

15 FIRST PAGE, WHAT EXACTLY DOES THIS DEPICT?

16 A THAT'S JUST A SCREEN SHOT OF THE VERSION THAT I WAS  
17 TESTING WITH, AND IT SAYS LIMEWIRE 4.14.0 --

18 Q OKAY.

19 A -- WHICH IS THE VERSION IN QUESTION.

20 Q AND WHEN YOU SAY THE VERSION IN QUESTION, YOU MEAN  
21 THE VERSION USED BY THE DEFENDANT, MR. MORAN?

22 A CORRECT.

23 Q OKAY. I'M GOING TO TRY TO ZOOM IN JUST A LITTLE BIT  
24 SO YOU CAN SEE THIS A LITTLE BIT BETTER.

25 THE SECOND PAGE IS EXHIBIT 13, WHAT DOES THAT

1 DEPICT?

2 A THAT IS A SCREEN SHOT OF THE LOWER LEFT PORTION OF  
3 LIMEWIRE 4.14.0. IF YOU ZOOM IN ALL THE WAY, I CAN DESCRIBE  
4 IT WITHOUT THOSE DOCUMENTS AT THE TOP.

5 Q OKAY.

6 A AND I BELIEVE MISS LOEHRS WAS ASKED THE SAME  
7 QUESTION, BUT THE FIRST ONE THAT LOOKS LIKE A CELL PHONE BAR  
8 IS THE QUALITY OF CONNECTION. BASICALLY, THAT JUST TELLS YOU  
9 YOU'VE CONNECTED TO THOSE ULTRAPEERS, AND THOSE ARE THOSE  
10 COMPUTERS ON THE GNUTELLA NETWORK THAT HELP YOU FIND YOUR  
11 KEYWORD RESULTS.

12 Q AND YOU'RE REFERRING TO THIS RIGHT HERE; CORRECT?

13 A CORRECT.

14 Q AND I'M GOING TO MARK THAT...JUST SO THE RECORD IS  
15 CLEAR, I'M GOING TO MARK THAT IN RED; PUT A RED CIRCLE AROUND  
16 THAT.

17 A THEN, TO THE RIGHT OF THAT, THAT'S A GLOBE, AND  
18 THAT'S A FIREWALL INDICATOR. I DON'T BELIEVE THEIR EXPERT  
19 KNEW WHAT IT WAS, BUT IT'S A GLOBE BECAUSE IT'S UN-FIREWALLED.  
20 MY WINDOWS COMMUNICATION ISN'T IMPEDING -- FIREWALL ISN'T  
21 IMPEDING THIS COMMUNICATION OR PROGRAM. IF I WAS FIREWALLED,  
22 A RED BALL WOULD HAVE APPEARED IN FRONT OF THAT GLOBE.

23 Q AND WHAT DOES FIREWALL MEAN?

24 A A FIREWALL IS SOMETHING THAT RUNS IN YOUR OPERATING  
25 SYSTEM, IF THERE'S ONE INSTALLED, THAT WOULD PREVENT PEOPLE

1 FROM COMING INTO YOUR COMPUTER WHEN THEY'RE UNWANTED;  
2 BASICALLY, IT WOULD BLOCK UNSOLICITED COMMUNICATION FROM  
3 COMING INTO YOUR COMPUTER.

4 Q OKAY. SO RIGHT NEXT TO THE BOX, CLOSEST TO THE LEFT  
5 TO THE SMALL BOX WITH THE EARTH SYMBOL, MEANS EXACTLY WHAT?

6 I KNOW YOU WENT OVER IT.

7 A AN UNFIREWALLED -- THIS APPLICATION IS GOING TO  
8 PROPERLY FUNCTION, AND MY -- AND LET COMMUNICATION INTO IT  
9 LIKE IT'S SUPPOSED TO.

10 Q OKAY. AND THE BOX IMMEDIATELY TO THE RIGHT OF THAT  
11 WITH THE CIRCLE AND THE NUMBER 0 IN IT -- I'M GOING TO SEE IF  
12 I CAN HIGHLIGHT IT THAT BOX.

13 A THAT'S A SHARED FILE INDICATOR, AND IT APPEARS IN  
14 GREEN, AND IT'S A ZERO BECAUSE I HAVE ZERO FULL FILES BEING  
15 SHARED. THAT NUMBER ONLY INCREMENTS IF I HAVE A NEW SHARE --  
16 SHARED FILE; AND WHEN I SAY THAT, I WANT TO QUALIFY THE FACT  
17 THAT A PARTIALLY SHARED FILE DOES NOT CAUSE THAT NUMBER TO BE  
18 INCREMENTED. ONLY A WHOLE FILE THAT'S COMPLETELY DOWNLOADED  
19 THAT WOULD HAVE THAT ENTRY IN THE FILEURNS.CACHE THAT WE'VE  
20 HEARD SO MUCH ABOUT.

21 Q OKAY.

22 THE COURT: SO YOU DON'T HAVE -- YOU ONLY HAVE A ONE  
23 IN THERE IF IT'S A COMPLETED FILE?

24 THE WITNESS: CORRECT.

25 Q BY MS. HARRIS: AND WHEN YOU SAY A COMPLETED FILE,

1 YOU MEAN ONE THAT'S AVAILABLE FOR SHARING SHOULD ANOTHER  
2 PERSON CONNECT TO IT?

3 A AND A COMPLETED SHARE, AND IT'S SHARED. IF I  
4 UNSELECT SHARE, IT WILL GO DOWN TO ZERO.

5 Q OKAY. THE NEXT, WHAT IS THAT?

6 A THAT'S A DOWN GREEN ARROW AND AN UP GREEN ARROW.  
7 THAT'S HOW MUCH TIME YOU'D BE USING FOR THE SHARING OF FILES  
8 OR THE DOWNLOADING OF FILES, SO THE ARROW WOULD INDICATE I'M  
9 USING SO MANY KILOBYTES PER SECOND TO DOWNLOAD MY FILES, AND  
10 THE UP -- TO UPLOAD IN THIS CASE, IF I WAS SHARING CHILD  
11 PORNOGRAPHY, THAT GREEN UP ARROW WOULD HAVE A NUMBER TO THE  
12 RIGHT AND HOW MUCH SPEED OF MY INTERNET CONNECTION WAS BEING  
13 USED FOR SENDING FILES TO OTHER PEOPLE ALL AROUND THE WORLD.

14 Q OKAY. I WANT TO ASK YOU ABOUT THE THIRD PAGE IN  
15 EXHIBIT NUMBER 13. I'M GOING TO LAY IT OUT A LITTLE BIT.

16 WHAT EXACTLY ARE WE LOOKING AT?

17 A THAT'S JUST THE PHEX HOME PAGE. THE HOME PAGE, YOU  
18 CAN GO TO THAT. YOU COULD DOWNLOAD THE SOURCE CODE, AND  
19 INSTALLER IS RIGHT THERE.

20 THIS IS IMPORTANT BECAUSE THIS IS WHAT  
21 DETECTIVE CORDER USED, SO WE CHOSE TO USE AND SET UP THE  
22 ENVIRONMENT JUST AS IT WAS BACK IN 2010 WHEN SHE DID HER  
23 INVESTIGATION.

24 Q OR 2008?

25 A 2008, I'M SORRY.

1 Q I'M GOING TO SHOW YOU THE FOURTH PAGE OF EXHIBIT 13.  
2 EXACTLY WHAT IS THAT?

3 A THAT JUST TELLS YOU ABOUT THE VERSION OF THE  
4 PROGRAM. I DOCUMENTED WHAT VERSION LIMEWIRE WAS USED, SO I  
5 DOCUMENTED WHAT VERSION OF PHEX WAS BEING USED.

6 Q AND THE VERSION OF PHEX THAT WAS BEING USED WAS  
7 3.4.2?

8 A CORRECT.

9 Q OKAY. NOW, I'M GOING TO ZOOM OUT JUST FOR A LITTLE  
10 BIT SO YOU CAN TALK TO US ABOUT THE TESTING YOU DID, AND KIND  
11 OF OUTLINE, AND WE'LL GO THROUGH PIECE BY PIECE AS OUTLINED IN  
12 YOUR EXHIBIT, BUT, FOR RIGHT NOW, I PUT UP PAGE 5 OF  
13 EXHIBIT 13.

14 WHAT ARE WE LOOKING AT HERE?

15 A HERE, I'M JUST SHOWING YOU THE VERSION THAT I'M  
16 USING IN THIS TEST, AND I CHOSE TO DO A SCREEN CAPTURE. IN  
17 THE BACKGROUND, YOU CAN SEE ACTUALLY MY TEST -- SEE MY TEST  
18 ENVIRONMENT TO GIVE AS MUCH INFORMATION TO THE COURT AS  
19 POSSIBLE TO LET THEM KNOW THAT I AM ACCURATELY REPORTING WHAT  
20 I'M SUGGESTING IS IN MY REPORT.

21 YOU CAN SEE THAT LIMEWIRE'S RUNNING IN THE  
22 BACKGROUND, AND YOU CAN SEE THAT THE VERSION THAT I'M USING IS  
23 LIMEWIRE 4.14.0.

24 Q I'M GOING TO SHOW YOU PAGE 6 OF EXHIBIT 13.

25 CAN YOU TELL US WHAT WE'RE LOOKING AT HERE; AND I'M

1 GOING TO SPECIFICALLY ZOOM IN TO YOUR RED ARROW.

2 A SO WE WANTED TO INDICATE THAT PARTIAL FILE SHARING  
3 WAS ENABLED. THAT WAS IMPORTANT BECAUSE A LOT OF THE -- WHY  
4 WE'RE HERE IS ALL ABOUT PARTIAL FILE SHARING, AND WHAT IT IS,  
5 AND WHEN IT'S PRESENTED TO AN INVESTIGATOR, SO WE OPTED TO  
6 LEAVE THAT OPTION ON. EVEN THOUGH IT'S UNCLEAR WHAT HIS  
7 SETTINGS WERE BACK IN 2008, WE CHOSE TO ENABLE PARTIAL FILE  
8 SHARE.

9 Q AND WHEN YOU SAY IT'S UNCLEAR WHAT HIS SETTINGS  
10 WERE, ARE YOU REFERRING TO THE DEFENDANT, ROBERT MORAN?

11 A CORRECT.

12 Q SO THIS PARTICULAR TESTING ENVIRONMENT, YOU  
13 SPECIFICALLY WANTED TO ALLOW THE PARTIAL FILE SHARING JUST SO  
14 YOU COULD TEST THE THEORY THAT'S ULTIMATELY IN QUESTION IN  
15 THIS CASE?

16 A CORRECT.

17 Q OKAY. I'M GOING TO REFER YOU TO PAGE 7, AND I'VE  
18 GOT TO ZOOM OUT SO YOU CAN SEE THAT, AND...I THINK THE BETTER  
19 FOCUS WOULD BE AT THE BOTTOM; IS THAT CORRECT?

20 A IF YOU START AT THE TOP, THE TAB THAT'S HIGHLIGHTED  
21 IN BLUE, YOU CAN MOVE TO THE BOTTOM.

22 Q OKAY. THEN, I'LL ZOOM UP.

23 A YOU CAN ZOOM INTO -- MOVE IT.

24 Q (COMPLYING.)

25 A FIRST THING I DID WAS INITIATED A KEYWORD SEARCH. I

1 BELIEVE THE KEYWORD SEARCH I USED WAS TREE.JPG. I DIDN'T WANT  
2 TO VIOLATE ANY COPYRIGHT LAWS. I LOOKED FOR PICTURES THAT  
3 PEOPLE TAKE THEMSELVES, SO TREE IS THE MOST -- OR FLOWERS ARE  
4 THE MOST INNOCENT THING I COULD THINK TO SEARCH FOR; AND THEN,  
5 BELOW THAT, IF YOU SCROLL DOWN JUST A LITTLE BIT, YOU GET  
6 PRESENTED WITH A BUNCH OF RESULTS, SO AT THIS POINT IN TIME,  
7 THERE'S NOTHING ON, MY GNUTELLA NET HAS TOLD ME.

8 YOU SEARCH FOR TREE.JPG, AND SO HERE ARE A LIST OF  
9 RESULTS THAT YOU CAN CHOOSE FROM. THE NAMES ARE VERY  
10 DESCRIPTIVE; AND THEN, BASED ON THE NAME -- THAT'S REALLY ALL  
11 WE HAVE TO GO ON -- AND THE TYPE OF FILE, WE CHOOSE TO  
12 DOWNLOAD SOMETHING, SO THEN, IF YOU SCROLL DOWN TO THE BOTTOM,  
13 WHAT I CHOSE TO DO IS I CHOSE TO DOWNLOAD FOUR FILES  
14 COMPLETELY AND FOUR FILES PARTIALLY.

15 IF YOU ZOOM TO THE LEFT, WE CAN LOOK AT THE FILES  
16 FIRST, AND YOU CAN SEE THAT THE TOP FOUR, TREE.JPG, THE FOUR  
17 THAT APPEAR AT THE TOP, UNDERNEATH THE NAME COLUMN -- I'M NOT  
18 GOING TO READ THEM ALL. THOSE ARE THE ONES THAT ARE PARTIALLY  
19 DOWNLOADED; AND THEN, THE BOTTOM FOUR, THOSE ARE THE ONES THAT  
20 ARE COMPLETELY DOWNLOADED, AND YOU CAN CONFIRM THAT BY  
21 SCROLLING TO THE RIGHT.

22 Q AND THEN, BEFORE I DO THAT, I'M GOING TO SAY THE  
23 BOTTOM FOUR ARE THE ONES THAT YOU SAY ARE COMPLETELY  
24 DOWNLOADED?

25 A YES.



1 Q SCROLL TO THE RIGHT...

2 A AND THE PROGRESS REPORT INDICATES THAT I HAVE FOUR  
3 COMPLETELY DOWNLOADED FILES, AND IT'S INDICATED BECAUSE THE  
4 STATUS BAR SAYS 100 PERCENT; AND THEN, TO FURTHER ILLUSTRATE  
5 WHAT THAT LOWER CIRCLE MEANS, THE SHARED FILE INDICATOR, IF  
6 YOU SHOW THE GREEN CIRCLE ON THE BOTTOM HERE, YOU CAN SEE THAT  
7 THE INDICATOR IS THAT THERE ARE FOUR SHARED FILES. THE FOUR  
8 PARTIALLY DOWNLOADED FILES DO NOT CAUSE THAT NUMBER TO  
9 INCREMENT.

10 Q AND I'M GOING TO MARK THAT IN BLACK, SO WHEN YOU  
11 REFER TO THIS NUMBER 4, THOSE ARE THE FOUR COMPLETELY  
12 DOWNLOADED FILES?

13 A RIGHT; AND SO NOW, WE HAVE A COMPUTER ON THE  
14 INTERNET, RUNNING THE EXACT SAME VERSION THAT WAS FOUND ON  
15 MR. MORAN'S COMPUTER, WITH FOUR FILES COMPLETELY DOWNLOADED  
16 AND FOUR FILES PARTIALLY DOWNLOADED, SO AT THIS POINT IN TIME,  
17 WE WILL...SHOW...

18 Q (COMPLYING.)

19 A WELL, IT'S JUST SHOWING HERE THAT THEY'RE PAUSED, I  
20 THINK.

21 Q OKAY. AND HERE?

22 A AND THIS IS A BLOW-UP OF THAT SCREEN. I JUST WANTED  
23 THERE TO BE NO MISUNDERSTANDING. THE TOP PORTION OF THIS  
24 SLIDE IS JUST THAT PREVIOUS SLIDE, SHOWING THE BOTTOM FOUR A  
25 HUNDRED PERCENT. IT'S CIRCLED IN RED; AND THEN, THE LOWER

1 SCREEN CAPTURE, I HIGHLIGHT AND CIRCLE IN RED, RATHER, THE  
2 FOUR THAT'S PARTIALLY DOWNLOADED, AND I SET UP MY TEST  
3 ENVIRONMENT TO DO FOUR BECAUSE I JUST DIDN'T WANT TO SAY, AT  
4 TEN PERCENT, IT'S SOMETHING; AT 50 PERCENT, IT'S SOMETHING; I  
5 HAVE THESE FILES PAUSED AND INCOMPLETE IN VARIOUS STAGES OF  
6 THE DOWNLOAD PROCESS, SO I'M NOT JUST TRYING TO SAY, AT TEN  
7 PERCENT, IT'S NOT THERE OR 50. I'VE GOT ONE THAT'S ALMOST  
8 90-SOME PERCENT.

9 WHAT'S THE TOP NUMBER THERE?

10 Q I BELIEVE IT'S 98 PERCENT.

11 A I HAVE ONE FILE THAT'S 98 PERCENT DOWNLOADED, AND IF  
12 ANY PARTIAL FILES ARE GOING TO SHOW UP IN THE BROWSE, IT  
13 SHOULD CERTAINLY BE ONE THAT'S ALMOST COMPLETELY DOWNLOADED,  
14 SO...SO THAT'S OUR TEST ENVIRONMENT SET UP JUST LIKE  
15 MR. MORAN'S COMPUTER --

16 Q OKAY. AND THAT'S PAGE --

17 A -- EXCEPT FOR HE DIDN'T HAVE TREES.

18 Q THAT'S PAGE 9 OF YOUR EXHIBIT 13.

19 I'M GOING TO SHOW YOU PAGE 10 OF EXHIBIT 13.

20 A SO NOW, WE RUN PHEX, AND I IMPLEMENT A BROWSE HOST,  
21 SO IF YOU CAN ZOOM IN AND GO TO THE LEFTMOST COLUMN, THE BLUE  
22 COLUMN, YOU CAN SEE THAT I -- I PUT IN AN I.P. ADDRESS AND  
23 USED A BROWSE HOST FUNCTION IN PHEX, WHICH IS REFERRED TO --  
24 THAT THE EQUIVALENT IN LIMEWIRE IS CALLED DIRECT CONNECT, AND  
25 I JUST PUT THE I.P. ADDRESS OF MY TEST MACHINE IN THERE; AND

1 AS SOON AS I HIT BROWSE HOST, I GOT TO SEE ALL OF THE WHOLE  
2 FILES BEING SHARED, SO IF YOU SCROLL TO RIGHT, AND WE TAKE --  
3 NO, GO LEFT A LITTLE BIT.

4 Q I'M GOING TO ZOOM OUT.

5 A OH, OKAY, BUT THE FILE NAME'S AVANT BARK 5, BARK --  
6 I DON'T KNOW -- AND ANNUL SOMETHING -- THOSE ARE THE FOUR  
7 FILES PRESENTED TO ME; AND IF YOU CAN SOMEHOW PUT THE PRIOR  
8 EXHIBIT ON THERE, YOU'LL SEE THAT THOSE ARE THE HUNDRED  
9 PERCENT DOWNLOADED FILES.

10 Q SORRY.

11 A MAYBE YOU CAN'T.

12 Q YOU CAN IF I ZOOM OUT.

13 A BUT THEY'RE THE SAME FILES THAT WERE A HUNDRED  
14 PERCENT DOWNLOADED.

15 Q LET'S DO IT THIS WAY.

16 A YOU ALMOST HAVE TO LOOK AT THEM, BUT YOU CAN SEE  
17 LMINT BARK 5 -- BARK 5 (PHONETIC). YOU CAN SEE THAT THOSE ARE  
18 THE EXACT SAME FILES. YOU DO NOT SEE THE 98 PERCENT  
19 DOWNLOADED FILES OR ANY OF THE INCOMPLETE.

20 I'VE TRAINED A THOUSAND LAW ENFORCEMENT OFFICERS.  
21 I'VE PRESENTED THINGS OUT OF FORMALIZED TRAININGS FOR  
22 PROSECUTORS, DEFENSE EXPERTS. IT'S ALWAYS THE SAME, AND --  
23 AND I TRY TO HELP THEM UNDERSTAND HOW WE'RE DOING THINGS TO  
24 AVOID HEARINGS SUCH AS THIS.

25 Q OKAY. AND WHEN YOU TALK ABOUT THOSE FOUR COMPLETED

1 FILES, I THINK YOU COMBINED -- I THINK IT'S PAGE 11 OF  
2 EXHIBIT 13, THOSE FOUR COMPLETED FILES?

3 A RIGHT. I PUT THEM TOGETHER FOR YOU SO YOU CAN SEE  
4 IT. THEY'RE ALWAYS THE HUNDRED PERCENT DOWNLOADED COMPLETELY  
5 SHARED FILES.

6 Q OKAY. I'M GOING TO REFER TO PAGE 13.  
7 WHAT EXACTLY ARE WE LOOKING AT HERE?

8 A SO NOW, I HAVE FOUR SHARED FILES. THEY'RE -- THEIR  
9 THEY'RE A HUNDRED PERCENT DOWNLOADED, AND THEY'RE THE ONLY  
10 FILES I SAW ON THAT LIST, SO I WANTED TO IMPLEMENT AN OPTION  
11 WHERE I STOPPED SHARING ONE OF THOSE FILES TO PROVE THE SECOND  
12 HALF OF MY STATEMENT, SO THE ONE THAT BEGINS WITH THE LETTER  
13 "E," I'M NOT GOING TO ATTEMPT TO PRONOUNCE IT, THE BOTTOM  
14 SHARED FILE, I JUST RIGHT CLICKED ON THE FILE AND SAID STOP  
15 SHARING IT --

16 Q OKAY.

17 A -- AND I WANT TO CLARIFY: I DIDN'T RESTART  
18 LIMEWIRE. IT'S RUNNING LIVE IN AN OPERATING SYSTEM. I DIDN'T  
19 HAVE TO DO ANYTHING TO GET IT TO STOP REPORTING AS BEING  
20 SHARED, LIKE HAS BEEN SUGGESTED IN TAMI LOEHRS' AFFIDAVIT. I  
21 HIT STOP SHARING FILE, AND I WOULD ESTIMATE LESS THAN ONE  
22 MINUTE LATER, PROBABLY EVEN LESS THAN THAT, WE DID --  
23 IMPLEMENTED ANOTHER BROWSE HOST: SHOW ME ALL OF YOUR SHARED  
24 FILES.

25 Q AND THAT'S DEMONSTRATED IN THE NEXT EXHIBIT;

1 CORRECT?

2 A CORRECT.

3 Q OKAY.

4 A NOW, WE ONLY HAVE THREE SHARED FILES. THE FILE I'M  
5 NOT SHARING DOES NOT APPEAR IN THE LIST, AND IT GOES -- IT  
6 SUPPORTS MY POSITION. I'VE NEVER KNOWN IT TO NOT BE TRUE  
7 WHOLE FILES BEING SHARED ARE WHAT'S PRESENTED TO YOU DURING A  
8 BROWSE HOST, NOTHING ELSE, SO IF I, AS AN INVESTIGATOR, CAN  
9 DESCRIBE THOSE FILES BASED ON THE HASH VALUE, I'M IN THE DOOR.

10 Q OKAY. AND WHEN YOU SAY HASH VALUE, YOU'RE TALKING  
11 ABOUT THOSE...

12 A (INDICATING.)

13 Q CORRECT...NUMBERS THAT SAY SHA-1 ON THE FAR RIGHT  
14 SIDE OF PAGE 13 OF YOUR EXHIBIT.

15 A CORRECT. NOW -- SO THAT'S THE FINGERPRINT OF THE  
16 FILE. THAT'S THE SHA-1 HASH VALUE WE RELY ON IN FORENSICS ALL  
17 THE TIME; AND IF YOU SCROLL A LITTLE TO YOUR LEFT, THE OTHER  
18 BIG PIECE OF THE ADDRESS IS RIGHT THERE, THE I.P. ADDRESS, AND  
19 IT'S 71.61.71.137; AND SO NOW, I HAVE EVERYTHING I NEED.

20 I KNOW, AT THIS MOMENT IN TIME, A CERTAIN  
21 I.P. ADDRESS IS SHARING COMPLETELY THREE PICTURES OF TREES.  
22 IF THAT WOULD BE CONTRABAND, THEN I WOULD BE...NOT COMPLETE MY  
23 INVESTIGATION, BUT READY TO MOVE FORWARD TO FIGURE OUT WHO THE  
24 SUBSCRIBER OF THAT INTERNET SERVICE IS AND AUTHOR A SEARCH  
25 WARRANT UPON RECEIVING THOSE RESULTS.

1 Q OKAY. AND THAT'S WHAT DETECTIVE CORDER DID IN THIS  
2 CASE?

3 A THAT'S EXACTLY WHAT SHE DID IN THIS CASE.

4 MS. HARRIS: AND JUST FOR THE RECORD, JUDGE, WE'RE  
5 GOING TO HIGHLIGHT THE PORTION IN YELLOW THAT MR. ERDELY WAS  
6 REFERRING TO AS THE I.P. ADDRESS. I'M THEN GOING TO CIRCLE IN  
7 THE PORTION WHERE WE'RE REFERRING TO THE SHA-1 VALUE.

8 Q BY MS. HARRIS: I'M GOING TO SKIP THROUGH A FEW  
9 PAGES, SO THIS IS THE TEST THAT YOU HAD AN OPPORTUNITY TO DO  
10 WITH DETECTIVE LITCHFIELD; CORRECT?

11 A CORRECT.

12 Q AND THAT WAS SIMULTANEOUSLY YOU TWO WORKING IN  
13 CONJUNCTION ON THE COMPUTER?

14 A CORRECT.

15 Q DID YOU THEN DO ANY ADDITIONAL TESTING ON --

16 A YES. I WANTED TO LOOK AT SOME OF OTHER THINGS THAT  
17 WERE STATED IN HER AFFIDAVIT BECAUSE I THOUGHT IT WAS  
18 INCOMPLETE. I DIDN'T WANT TO JUST SAY THAT WITHOUT SOMETHING  
19 TO SUPPORT IT. SOMETHING WE DON'T DO A LOT OF TESTING ON,  
20 ALTHOUGH MY NORMAL USE OF THIS PROGRAM LETS ME TEST WHAT A  
21 KEYWORD RESULT IS.

22 AS I DESCRIBED EARLIER, IT'S NOT SOMETHING I  
23 FORMALLY SIT DOWN IN THE LAB EVERY DAY AND DO BECAUSE WE RELY  
24 ON THE BROWSE HOST. THAT'S MY ANONYMOUS TIP. I'M NOT REALLY  
25 CONCERNED WITH THAT, SO I DID MY TESTING WITH THE EXACT

1 VERSION USED IN THIS CASE.

2 Q AND I'M GOING TO REFER TO PAGE, I BELIEVE, 15 OF  
3 EXHIBIT 13.

4 I'M JUST GOING TO SCROLL OUT; AND YOU AUTHORED --  
5 YOU GENERATED A REPORT IN THIS PARTICULAR CASE IN REGARDS TO  
6 YOUR ADDITIONAL TESTING THAT YOU DID?

7 A RIGHT; AND HERE, I'M JUST SHOWING YOU I'M RUNNING  
8 LIMEWIRE 4.14.0, AND I HAVE IN THE BACKGROUND -- YOU CAN SEE  
9 THAT THERE'S A FILE PARTIALLY DOWNLOADED, BUT THE NEXT SLIDE'S  
10 GOING TO SHOW IT BETTER.

11 Q I WAS JUST ABOUT TO GO THERE. PAGE 16, AND I'LL  
12 ZOOM IN. I'LL START IN WITH THE NAME OF THE FILE, AND THEN,  
13 WE CAN TALK ABOUT WHAT WE SEE HERE.

14 A AND THE NAME IS -- I NAMED THE FILE. IT'S NAMED,  
15 LIKE, CHILD PORNOGRAPHY; HOWEVER, IT'S A FILE THAT I CREATED.  
16 IT'S PUBLICLY AVAILABLE AND NOT COPYWRITTEN --

17 Q OKAY.

18 A -- AND -- AND YOU CAN SEE THAT I'M DOWNLOADING --  
19 DOWNLOADING THE FILE; AND IF YOU SCROLL TO RIGHT, YOU CAN SEE  
20 THAT I HAVE 30 -- MY EYES ARE GONE -- 30 PERCENT DOWNLOADED.

21 Q AND I CAN GO IN A LITTLE BIT MORE.

22 A YEAH, AND THERE'S AN ARROW POINTING TO IT.

23 Q THIRTY PERCENT DOWNLOAD; AND THEN, IT SHOWS THE  
24 SPEED AND THE TIME?

25 A YUP; AND YOU CAN JUST MOVE THROUGH, I GUESS.

1 Q OKAY.

2 (MS. ANDRUS CONFERRING WITH MS. HARRIS.)

3 MS. HARRIS: DO YOU NEED MORE WATER?

4 THE WITNESS: NO, I'M GOOD.

5 Q BY MS. HARRIS: OKAY. WE'RE GOING TO SHOW YOU PAGE  
6 I BELIEVE -- AND YOU CAN LET ME KNOW IF THESE ARE OUT OF  
7 ORDER, BUT I BELIEVE THEY'RE IN ORDER -- THE NEXT PAGE OF YOUR  
8 REPORT.

9 A OKAY. AND I'M JUST INDICATING HOW MUCH IS  
10 DOWNLOADED. IF YOU COULD ZOOM INTO THE -- BELOW THE ARROW, I  
11 CAN SEE IT.

12 Q RIGHT. I KNOW, AT THIS POINT, IT'S A HUNDRED  
13 PERCENT.

14 A OKAY. I HAVE A FILE THAT'S A HUNDRED PERCENT  
15 DOWNLOADED, CORRECT.

16 Q WHAT DOES THIS SCREEN ON PAGE, I BELIEVE, 18 -- WHAT  
17 DOES THIS SCREEN SHOW US -- WHOOPS.

18 A SO I BELIEVE I'M IN THE LIBRARY VIEW. IF YOU ZOOM  
19 IN ABOVE THE ARROW...

20 Q (COMPLYING.)

21 A SO HERE'S THE RELEVANCE AS I TAKE YOU THROUGH THIS:  
22 THE PRIOR SCREEN SHOWED THAT I DOWNLOADED A HUNDRED PERCENT.  
23 I LET IT RUN FOR OVER 24 HOURS. I SEARCHED FOR THAT FILE THAT  
24 I CREATED. I'M THE ONLY ONE IN THE WORLD THAT HAD IT AT THE  
25 MOMENT THAT I CREATED IT, AND I HAD A WHOLE LAB THAT WAS AT MY



1 DISPOSAL AT OUR HEADQUARTERS SEARCH FOR THAT FILE, AND I FOUND  
2 33 INSTANCES WHERE THE FILE WAS SENT OUT, SAYING, YUP, I'M  
3 SHARED; I HAVE THE WHOLE FILE.

4 I SHUT DOWN THE PROGRAM AND THEN STARTED IT BACK UP,  
5 AND IN 15 MINUTES, FROM THIS VIEW IN LIMEWIRE, I SAW THAT I  
6 HAD A THOUSAND FORTY-FOUR HITS, SO JUST 15 MINUTES.

7 Q AND WHY IS THAT SIGNIFICANT?

8 A I'M JUST TRYING TO SHOW HOW QUICKLY THAT THIS FILE  
9 WOULD BE FOUND BECAUSE I USED NAMES OF CHILD PORNOGRAPHY TO  
10 DESCRIBE IT.

11 Q OKAY. AND WHEN YOU SAY NAMES OF CHILD PORNOGRAPHY,  
12 I THINK WE'VE ALREADY KIND OF GONE OVER THIS WITH MISS LOEHR,  
13 BUT SOME OF THOSE TERMS ARE P.T.H.C.; RIGHT?

14 A RIGHT. HUSSYFAN, R@YGOLD; ALL THOSE TERMS THAT I  
15 KNEW USED CHILD PORNOGRAPHY. I ACTUALLY PUT MY BADGE NUMBER  
16 AT THE END. I ALSO KNEW MY HASH VALUE AND FILE NAME THAT I  
17 CREATED AT THAT FILE.

18 Q OKAY. I WANT TO SHOW YOU THE NEXT PAGE OF YOUR  
19 EXHIBIT 13, AND I BELIEVE YOU HIGHLIGHT A BOX IN THE TOP. I  
20 WANT TO SHOW YOU IN THIS SCREEN WHERE YOU CLICK ON  
21 INDIVIDUALLY SHARED FILES.

22 IS THAT THE NEXT SLIDE OR AM I...

23 THE COURT: MAYBE THAT'S OUT OF ORDER.

24 THE WITNESS: DO YOU HAVE A SECOND COPY OF MY...

25 MS. HARRIS: SLIDES?

1 THE WITNESS: -- MY SLIDES. CAN I LOOK AT THEM OR  
2 AM I NOT ALLOWED?

3 MS. HARRIS: I THINK SO. GIVE ME A SECOND.

4 IF I CAN APPROACH...

5 THE COURT: (NO RESPONSE.)

6 MS. HARRIS: THEY CAN BE OUT OF ORDER.

7 THE COURT: REALIZING WE'RE NOT GOING TO GET THROUGH  
8 WITH CROSS, MAYBE NOT EVEN DIRECT, IS THERE ANY WAY, SINCE  
9 WE'VE BEEN USING SKYPE IN THE LAST COUPLE OF TRIALS, SO HE  
10 DOESN'T HAVE TO COME BACK FROM PITTSBURGH, TO JUST DO SKYPE  
11 FOR EVERYTHING ELSE?

12 MS. HARRIS: JUDGE, IT'S MY UNDERSTANDING THAT OUR  
13 OFFICE HAS NO ISSUE AT THIS POINT BRINGING HIM BACK TO  
14 TESTIFY; IT'S JUST A MATTER OF WHEN --

15 THE COURT: OH, OKAY.

16 MS. HARRIS: -- AND IF WE -- THE STATE'S PREFERENCE  
17 WOULD BE, IF POSSIBLE, TO PLOW THROUGH TO TOMORROW, BUT I  
18 UNDERSTAND THAT THERE MAY BE A CONFLICT WITH DEFENSE COUNSEL,  
19 SO WE CAN STOP DETECTIVE -- OR CORPORAL ERDELY'S TESTIMONY AND  
20 THEN RESUME IT UPON HIS RETURN AT A DAY CERTAIN THAT WE'RE  
21 GOING TO TRY TO GET TOGETHER.

22 THE COURT: SURE. YOU HAVE A DATE?

23 THE WITNESS: IT'D BE SOMETIME AFTER MY FRANCE TRIP,  
24 WHICH ENDS ON THE 16TH -- OH, MAYBE NOT.

25 THE COURT: SEPTEMBER?

1 THE WITNESS: YEAH. I GAVE YOU THE DATES; THE 2ND  
2 THROUGH THAT FOLLOWING SATURDAY.

3 MS. HARRIS: WHICH IS, I THINK, THE 10TH OR THE  
4 11TH.

5 THE WITNESS: AND I JUST HAVE TO CHECK MY BOARD  
6 CALENDAR TO SEE IF I CAN COME BACK DOWN HERE.

7 THE COURT: OKAY.

8 THE WITNESS: I CAN LET YOU KNOW. I'LL LET THEIR  
9 OFFICE KNOW BY TOMORROW, IF THAT'S OKAY.

10 THE COURT: OH, SURE, SURE, OKAY, SO I'D HAVE TO  
11 CHECK WITH THE DEFENSE TO SEE IF THEY HAVE A PROBLEM.

12 THE WITNESS: RIGHT.

13 Q BY MS. HARRIS: AND, CORPORAL, IF YOU CAN, LET ME  
14 KNOW -- MAYBE MY PAGES ARE OUT OF ORDER.

15 A NO, THAT'S RIGHT.

16 Q OH.

17 A SO THAT ONE, WHAT I DID FOR MY TEST IS I DELETED THE  
18 FILE --

19 Q OKAY.

20 A -- AND I DID NOT RESTART THE PROGRAM BECAUSE I FOUND  
21 IT 33 TIMES RANDOMLY, LETTING MY WHOLE LAB SEARCH FOR IT OVER  
22 A 24-HOUR PERIOD, SO THEN, I LET IT CONTINUE TO RUN AND SEARCH  
23 AND SEARCH AND SEARCH AND FOUND NO INSTANCE OF THIS FILE  
24 SHOWING UP AS A KEYWORD SEARCH HIT, WHICH IS CONTRADICTIONARY TO  
25 WHAT TAMI LOEHRS SAID IN HER REPORT, SO I HAD A HUNDRED

1 PERCENT DOWNLOADED FILE, FOUND IT 33 TIMES, I ILLUSTRATED TO  
2 THE COURT THAT, JUST RUNNING IT 15 MINUTES.

3 THE WHOLE WORLD SAW IT A THOUSAND FORTY-FOUR TIMES,  
4 BUT THEN, I RUN IT FOR ANOTHER DAY AFTER IT'S DELETED AND THE  
5 COMPUTER'S NOT RESTARTED, AND THAT'S EXACTLY WHAT SHE'S  
6 PRESENTING TO THIS COURT IN HER AFFIDAVIT; THAT IT'S GOING TO  
7 KEEP SAYING, HEY, I'M SHARED. I'M SHARED FOREVER UNTIL I KEEP  
8 RESTARTING LIMEWIRE.

9 I'M JUST WONDERING WHY I WASN'T ABLE TO RECREATE HER  
10 TEST, THAT SAME TEST THAT SHE SAYS, I CAN'T EVEN RECREATE.

11 Q SO WHEN YOU SEE THIS SCREEN, THE EMPTY BOX THAT  
12 INDICATES YOU LOOKED FOR THE FILE THAT WAS DELETED AND IT'S NO  
13 LONGER THERE?

14 A I SEARCHED AND SEARCHED. YOU CAN ALSO CONFIRM IT IN  
15 THE BOX -- THAT CIRCLE WITH THE ZERO IN IT INDICATES THAT IT  
16 WAS NOT BEING SHARED. I DELETED THAT FILE THAT I HAD  
17 PREVIOUSLY BEEN FINDING NO PROBLEM WITH WHATSOEVER.

18 Q OKAY. LET'S TALK ABOUT THE NEXT PAGE.

19 WHAT EXACTLY ARE WE LOOKING AT HERE?

20 A SO THE NEXT FOUR SLIDES -- AND WE CAN SPEED THROUGH  
21 TIME HERE VERY QUICKLY --

22 Q OKAY.

23 A -- IS THAT I JUST CHOSE TO -- THE NEXT HALF OF MY  
24 TEST ON A SEPARATE MACHINE, WITH A SEPARATE COPY OF LIMEWIRE,  
25 SO I'VE GOT THE ONE RUNNING WHERE I'VE NOW DELETED IT, AND I

1 HAVE ANOTHER COMPUTER ALTOGETHER WITH THE SAME VERSION OF  
2 LIMEWIRE INSTALLED, AND I SHOW FOUR SLIDES OF JUST THE PROCESS  
3 OF THIS FILE DOWNLOADING; AND THEN, I STOP IT AT 91 PERCENT,  
4 SO YOU MAY WANT TO JUST JUMP FORWARD TO THE FOURTH SLIDE  
5 THERE --

6 Q YES.

7 A -- AND YOU'LL SEE THAT I DOWNLOADED 91 PERCENT OF  
8 THE FILE USING LIMEWIRE 4.14.0, SO THIS IS MORAN NINE TIMES  
9 MORE -- I HAVE NINE TIMES MORE OF THE FILE THAN TAMI DID IN  
10 HER TEST.

11 I SEARCHED -- I ACTUALLY SEARCHED THE SAME TIME I  
12 WAS SEARCHING, YOU KNOW, IN THIS PREVIOUS TEST. I HAVE A  
13 WHOLE LAB WORTH OF COMPUTERS SEARCHING GNUTELLA AND FOUND NO  
14 INSTANCE OF IT BEING SHARED.

15 Q OKAY. AND THAT'S -- THAT'S DISPLAYED TWO PAGES  
16 LATER ON THIS EXHIBIT, CORRECT, WHEN YOU HAVE THE RED  
17 HIGHLIGHT FOR HITS?

18 A YEAH, ZERO HITS. THE OTHER ONE HAD A THOUSAND  
19 FORTY-FOUR HITS IN 15 MINUTES, SO I HAVE NO HITS.

20 Q SO THE PARTIAL FILE, IF I'M UNDERSTANDING YOUR  
21 TESTIMONY CORRECTLY, THAT YOU DOWNLOADED 95 -- 91 PERCENT DID  
22 NOT SHOW AS AVAILABLE FOR SHARING?

23 A CORRECT. THAT WAS MY TEST.

24 Q AND I BELIEVE YOU HAVE A CLOSE-UP TO -- TO KIND OF  
25 DEMONSTRATE THAT THERE WERE NO HITS, AND NO ONE --

1 A RIGHT.

2 Q -- THAT COULD --

3 A CORRECT.

4 Q -- GET THE FILE?

5 A AND IT WAS NAMED THE SAME WAY. IT'S ACTUALLY THE  
6 SAME FILE THAT YOU FOUND A THOUSAND FORTY-FOUR TIMES ON THE  
7 OTHER SCREEN. IT'S ACTUALLY THE SAME FILE. IT'S NAMED THE  
8 EXACT SAME WAY; VERY, VERY POPULAR TERMS ON GNUTELLA.

9 Q OKAY. AND BY THAT, YOU'RE REFERRING TO THE P.T.H.C.  
10 THAT WE WENT OVER EARLIER?

11 A RIGHT, 15 MINUTES WITH A THOUSAND FORTY-FOUR.

12 Q SO THEN, WHAT DID YOU DO NEXT?

13 I SKIPPED AHEAD ABOUT THREE OR FOUR SLIDES, AND I'M  
14 GOING TO ZOOM OUT JUST A LITTLE BIT.

15 A SO I ACTUALLY PERFORMED THIS TEST TWO WAYS TO TRY  
16 TO -- I DID EVERYTHING I COULD TO REPLICATE WHAT TAMI LOEHRS  
17 HAD PRESENTED TO THIS COURT, SO WITH -- WHEN LIMEWIRE'S  
18 RUNNING, YOU CAN JUST USE -- WITHIN THE PROGRAM LIMEWIRE, AS  
19 YOU -- A FILE'S HIGHLIGHTED, YOU CAN JUST HIT THE DELETE KEY,  
20 AND IT'S GONE. IT'LL SEND IT TO YOUR RECYCLE BIN OR BYPASS  
21 THE RECYCLE BIN AND GO RIGHT INTO THE DELETED SPACE, SO TO  
22 SPEAK, BUT THEN, I ALSO CHOSE TO TRY TO DELETE IT OUTSIDE THE  
23 LIMEWIRE. I JUST USED THE OPERATING SYSTEM AND NAVIGATED TO  
24 WHERE THE FILE LIVES ON THE HARD DRIVE AND DELETED IT THAT  
25 WAY.

1 Q WHY WAS THAT IMPORTANT TO YOU?

2 A WELL, BECAUSE I WANTED TO SHOW THAT REGARDLESS OF  
3 WHETHER I DELETED IT IN THE APPLICATION, WHICH WAS SEVERAL  
4 SLIDES AGO OR IF I DOWNLOAD -- OR IF I DELETED IT OUTSIDE OF  
5 LIMEWIRE, SO LIMEWIRE'S NOT EVEN SMART ENOUGH TO KNOW I  
6 DELETED IT, IT'S GONE; NOW, AM I GOING TO SEE SOME KEYWORD  
7 SEARCH HITS NOW NOW THAT I DELETED IT.

8 Q AND I MEANT TO -- JUST MAKE SURE I HAVE THE NEXT  
9 SLIDE; CORRECT? IS THIS THE NEXT SLIDE THAT YOU'RE SHOWING?

10 A YES; AND BECAUSE I DELETED IT OUTSIDE OF THE  
11 LIMEWIRE PROGRAM ITSELF, YOU KNOW, STILL IN THE INTERFACE,  
12 STILL IN THE INTERFACE, THE FILE IS PRESENTED TO US, BUT I  
13 TRIED TO SPIN THIS IN THE MOST FAVORABLE LIGHT TO THE DEFENSE  
14 AS POSSIBLE AND GIVE EVERY OPPORTUNITY FOR MY TEST TO FAIL, SO  
15 I DID THIS DELETION OF THE FILE AND MADE IT SO THAT IT STAYED  
16 IN THE PROGRAM, AND STILL, I HAD NO SEARCH HIT ON THAT FILE,  
17 WHICH IS NAMED WITH VERY POPULAR TERMS.

18 Q OKAY. AND, I BELIEVE, AFTER THAT, YOU MAKE  
19 REFERENCE TO MISS LOEHRS' SCREEN SHOTS THAT WE HAVE PREVIOUSLY  
20 GONE OVER THAT ARE ATTACHED TO HER AFFIDAVIT; CORRECT?

21 A RIGHT; AND I'VE ALREADY COMMENTED ON THIS --

22 Q RIGHT.

23 A -- BUT SHE -- SHE DOWNLOADED AC/DC VIDEO, I BELIEVE,  
24 OR M.P.3, AND IT'S ONLY DOWNLOADED TEN PERCENT, SO IF YOU ZOOM  
25 INTO THE LOWER LEFT CORNER, MY QUESTION IS...

1 Q WHICH IS PROBABLY DEMONSTRATED ON THE NEXT SLIDE.

2 A YEAH. MY QUESTION IS, WHY IS SHE SHARING A FILE  
3 THAT'S COMPLETELY DOWNLOADED, SO I -- I WANTED TO TEST THAT.  
4 I WANTED TO SEE, CAN I SET UP AN ENVIRONMENT WHERE I HAVE A  
5 FILE PARTIALLY DOWNLOADED THAT HAS A CERTAIN HASH VALUE AND A  
6 CERTAIN FILE NAME, GET THAT SAME FILE AND SHARE IT, COMPLETELY  
7 DOWNLOADED WITH THE SAME FILE NAME AND THE SAME HASH VALUE TO  
8 TRY TO REPLICATE THIS ENVIRONMENT SHE HAD, AS SHE PRESENTED  
9 FOR THE FEDERAL PUBLIC DEFENDERS.

10 Q OKAY. AND BEFORE WE GO OVER THAT, I BELIEVE YOU  
11 PROVIDED --

12 A OH, OH, OH, OKAY.

13 Q -- YOU PROVIDED THIS INFORMATION?

14 A CORRECT.

15 Q CAN YOU EXPLAIN TO THE COURT WHAT WE'RE LOOKING AT  
16 HERE.

17 A SO -- AND THIS -- THIS GOES TO HER MISSPEAKING AND  
18 HER -- I DON'T KNOW WHICH AFFIDAVIT IT WAS; ONE OF HER  
19 AFFIDAVITS WHERE SHE REFERENCED VICTOR SMITH, SO WHAT I DID  
20 WAS I INSTALLED LIMEWIRE, AND I FORENSICALLY LOOKED AT THE  
21 FILEURNS.CACHE.

22 Q AND IS THAT THE SYSTEM OF NUMBERS AND LETTERS THAT  
23 WE SEE IN THE BOTTOM BOX?

24 A IN THE BOTTOM BOX; AND IF YOU ZOOM IN THERE IN THIS  
25 FRESHENED INSTALL OF LIMEWIRE AND SEE NO ACTIVITY, THERE'S



1 ONLY ONE HASH VALUE -- IF YOU GO LEFT --

2 Q GO LEFT?

3 A GO RIGHT.

4 Q GO RIGHT?

5 A I'M SORRY. I'M BACKWARDS -- AND YOU ZOOM IN THERE,

6 THE ONLY REFERENCE TO ANY HASH VALUE IS THIS ONE THAT BEGINS

7 WITH B-- SEE, READ IT HERE...B3G -- COULD YOU SEE, YOUR HONOR,

8 SHA-1, COLON, IT'S THERE BY DEFAULT. IT'S THERE BY DEFAULT IN

9 LIMEWIRE 4.14, FOR WHATEVER REASON. IF YOU SEE IT -- SEE THE

10 WORD SHA-1? THERE'S RED TEXT.

11 Q I SEE THIS.

12 A NOW, MOVE UP...GO LEFT, THERE'S A HASH VALUE. IT'S

13 THERE BY DEFAULT. I'M NOT SHARING. I KNOW IT'S THERE BY

14 DEFAULT, AND I'M SHARING NO FILES, BUT -- SO NOW, WHAT I

15 WANTED TO DO IS I WANTED TO DOWNLOAD PART OF A FILE, WHICH

16 SHOULD BE THE NEXT SLIDE.

17 Q OKAY. I BELIEVE YOU GO BACK TO THE LIMEWIRE VERSION

18 WE USE, WHICH IS 4.14?

19 A CORRECT.

20 Q BUT THEN, YOU GO THREE -- TWO SLIDES LATER, AND --

21 A CORRECT.

22 Q -- YOU'RE DOWNLOADING OR ATTEMPTING TO DOWNLOAD

23 MORNING SNOW AND TREE?

24 A THAT'S CORRECT. I DOWNLOAD MORNING SNOW AND TREE,

25 AND YOU CAN SEE I PAUSED IT AT 28 PERCENT.

1 Q LET ME JUST ZOOM IN A LITTLE BIT.

2 A SO I'VE DOCUMENTED WHAT IT LOOKS LIKE EMPTY, AND  
3 NOW, I DOWNLOAD 28 PERCENT OF A FILE; AND AT THIS POINT, I  
4 KNOW THAT MANY OF THE LIMEWIRE ARTIFACTS GET WRITTEN WHEN YOU  
5 SHUT IT DOWN. IT'S OPERATING, AND IT RUNS THE PROGRAM JUST IN  
6 THE COMPUTER'S MEMORY, AND IT HASN'T WRITTEN IT OUT TO THE  
7 HARD DISK, WHICH IS WHAT WE ANALYZE IN FORENSICS, SO I HAVE TO  
8 SHUT DOWN THE PROGRAM TO MAKE SURE THAT EVERYTHING GETS  
9 WRITTEN TO DISK, SO I SHUT DOWN THE PROGRAM; AND NOW, I  
10 REEXAMINE THAT FILEURNS.CACHE.

11 Q OKAY. AND THAT IS THE NEXT SLIDE. NOW, LET'S --  
12 ACTUALLY, I THINK I'LL KEEP IT WHERE WE WERE 'CAUSE I THINK  
13 YOU HIGHLIGHTED THE SAME.

14 WE'RE STILL IN THE SAME AREA; CORRECT?

15 A IS THAT THE SAME ONE OR THE NEXT ONE?

16 Q THAT WAS THE NEXT.

17 A OH, THAT'S THE NEXT ONE? SO THIS IS AFTER I  
18 DOWNLOAD 28 PERCENT OF A FILE. YOU CAN ONLY SEE THE REFERENCE  
19 THAT SAME SHA, B3, WHATEVER HASH VALUE.

20 MY POINT IN THIS TEST IS THAT A PARTIALLY DOWNLOADED  
21 FILE DOES NOT APPEAR IN THE FILEURNS.CACHE, AND TAMI LOEHRS  
22 SAID IN HER AFFIDAVIT, AND I'VE BEEN FORTUNATE ENOUGH TO HEAR  
23 HER TESTIFY, SHE TESTIFIED UNDER OATH THAT, ABSOLUTELY, FILES  
24 GO IN THERE THAT ARE INCOMPLETE.

25 DOES IT PERTAIN TO THIS CASE SPECIFICALLY? NO.

1 IT -- IT -- I SIMPLY DID THE TEST BECAUSE SHE MADE A STATEMENT  
2 THAT I KNEW WAS WRONG, AND I THINK THAT HER TESTING IS FLAWED  
3 AND, YOU KNOW, INCOMPLETE AND INACCURATE.

4 Q OKAY. SO IN THE NEXT SCREEN, YOU GO TO THE  
5 INCOMPLETE FOLDER; IS THAT CORRECT?

6 A RIGHT; AND -- AND SO THEN, I NAVIGATED TO WHERE THE  
7 DOWNLOADS.DAT WAS --

8 Q OKAY.

9 A -- BECAUSE I HAVE THIS FILE THAT'S 28 PERCENT  
10 DOWNLOADED. I SHUT DOWN LIMEWIRE, AND SO WHERE IS IT -- WHERE  
11 IS IT STORED? WELL, IT'S IN THIS FILE. THIS IS ONE OF THE  
12 FILES THAT MAKES LIMEWIRE WORK, AND I HIGHLIGHTED A CORRECT  
13 PORTION -- I BELIEVE IF YOU ZOOM IN AND KEEP MOVING LEFT A  
14 LITTLE BIT...

15 Q OKAY. THIS PORTION?

16 A -- AND YOU CAN SEE THE PATH OF THE FILES THERE.  
17 DOCUMENTS AND SETTINGS, THAT'S A FOLDER ON YOUR COMPUTER; AND  
18 THEN, ADMIN, THAT'S THE USER NAME OF THE COMPUTER; AND THEN,  
19 INCOMPLETE, SO THAT'S THE PATH TO THE FILE. IT'S REFERRED TO  
20 AS, YOU KNOW, COMPUTER PATH; AND THEN, YOU SEE THE FILE, BUT  
21 THERE'S SOMETHING THAT WAS PUT IN FRONT OF THE FILE NAME, AND  
22 IT'S THE LETTER "J" AND THEN SOME NUMBERS; AND THEN, YOU SEE  
23 THE FILE NAME, WELL, THAT'S HOW LIMEWIRE STORES THOSE  
24 PARTIALLY INCOMPLETE FILES. THEY HAVE THAT T-DASH VALUE, "D,"  
25 BIG LONG FILE NAME.

1 Q OKAY. AND BASED ON YOUR TESTING, THAT FILE DID NOT  
2 SHOW AS AVAILABLE FOR SHARING?

3 A CORRECT. NO, IT DID NOT SHOW. IN ALL MY TESTS, IT  
4 DOESN'T SHOW AVAILABLE FOR SHARING; AND ONE THING SIGNIFICANT  
5 HERE IS HOW IT'S NAMED: I'M AN INCOMPLETE FILE, AND I HAVE  
6 T-DASH, AND THEN, IT'S A BUNCH OF NUMBERS. THOSE NUMBERS  
7 REPRESENT HOW BIG THE FILE WILL BE WHEN IT BECOMES A COMPLETE  
8 DOWNLOAD.

9 IN TAMI LOEHRS' TEST, SHE FOUND A FILE, AC/DC, AND  
10 THERE WAS A NAME; RIGHT? DID IT HAVE A T-DASH VALUE IN FRONT?  
11 IT DIDN'T, SO THE FILE NAME, AS IT'S AN INCOMPLETE VALUE, IS  
12 T-DASH VALUE, AND SHE DID THIS DEMONSTRATION BEFORE A GROUP OF  
13 PEOPLE AND FOUND A FILE THAT DIDN'T HAVE A TEMPORARY FILE  
14 NAME. I WOULD EXPECT THAT EVEN IF LIMEWIRE DID WHAT SHE  
15 SUGGESTED DID, THAT THE NAME WOULD BE COMPLETELY DIFFERENT.

16 Q AND THAT'S REPRESENTED BY THIS "T" I'M GOING TO  
17 HIGHLIGHT HERE, AND I HIGHLIGHTED A FEW OTHER PORTIONS.

18 A RIGHT, AND THAT'S WHAT INDICATES TO LIMEWIRE IT'S A  
19 TEMPORARY FILE. IF IT WAS PREVIEW, IT WOULD HAVE THE WORD  
20 PREVIEW IN FRONT OF IT.

21 Q I'M GOING TO SKIP A COUPLE OTHER SLIDES. I'M JUST  
22 GOING TO MOVE IT UP HERE.

23 CAN YOU EXPLAIN TO US WHAT DID YOU DO HERE.

24 A SO BECAUSE OF HER TEST, THAT I ONLY HAD THOSE FIVE  
25 OR SIX SCREEN SHOTS TO GO BY, I WANTED TO RECREATE AN

1 ENVIRONMENT WHERE I COULD SHARE A WHOLE FILE WITH A CERTAIN  
2 NAME AND THEN HAVE A PARTIAL FILE THERE ALSO, WHICH IS, I  
3 SUGGEST, MAYBE WHAT HAPPENED HERE, AND I WAS ABLE TO DO IT,  
4 SO -- SO IF YOU LOOK AT THE LOWER LEFT-HAND SCREEN OF THIS  
5 EXHIBIT, YOU CAN SEE THAT BEFORE I START DOWNLOADING THIS  
6 FILE, THERE'S A ONE IN THAT CIRCLE.

7 Q RIGHT.

8 A I'VE DOWNLOADED THE WHOLE FILE ALREADY. IT'S IN MY  
9 COMPLETED DOWNLOAD SECTION, AND IT'S ACTIVELY BEING SHARED OUT  
10 OVER THE INTERNET RIGHT NOW. THEN, I TRY TO DOWNLOAD THE SAME  
11 FILE WITH THE SAME FILE NAME AND THE SAME HASH VALUE, AND I  
12 WANTED TO SEE HOW LIMEWIRE WOULD REACT.

13 Q AND HOW DID LIMEWIRE REACT?

14 A IT SAID, HEY, YOU ALREADY HAVE THIS FILE.

15 Q AND IS THAT WHAT IS DEMONSTRATED BY THIS BOX THAT  
16 HAS WARNING ON IT?

17 A CORRECT, AND IT ASKS ME WHAT I WANT TO DO, AND I  
18 TOOK THE DEFAULT OPTION, WHICH IS OVERWRITE.

19 Q OKAY. AND WHAT DOES THAT MEAN?

20 A SO IT JUST MEANS THAT ONCE THIS FILE THAT I ALREADY  
21 HAVE COMPLETES DOWNLOADING, IT'S GOING TO OVERWRITE WHAT I  
22 ALREADY HAVE, BUT WHAT I'VE DONE IS CREATED AN ENVIRONMENT  
23 WHERE I HAVE A FILE THAT'S COMPLETELY DOWNLOADED WITH A  
24 CERTAIN NAME AND HASH VALUE; AND NOW, I HAVE A COPY OF THAT  
25 SAME FILE IN ITS INCOMPLETE STATE --

1 Q OKAY.

2 A -- AND THAT IS ONE EXPLANATION AS TO WHY TAMI LOEHRS  
3 MAY HAVE FOUND HER FILE THAT WAS DOWNLOADED TEN PERCENT.

4 Q AND BY THAT, YOU'RE REFERRING TO THE ONE SHARED FILE  
5 THAT WAS COMPLETELY DOWNLOADED?

6 A THAT SHE CAN'T REMEMBER WHAT IT WAS.

7 Q I'M GOING TO SKIP THROUGH THE NEXT SLIDE...THE NEXT  
8 SLIDE DEMONSTRATES, I BELIEVE, IT'S 27 PERCENT DOWNLOADED;  
9 CORRECT?

10 A RIGHT. THAT'S THE FILE THAT I WAS IN THE PROCESS OF  
11 DOWNLOADED -- DOWNLOADING. IT'S A DUPLICATE FILE, I HAVE A  
12 WHOLE FILE, AND I HAVE A PART OF A FILE, AND THE NEXT SCREEN  
13 KIND OF TELLS THE TALE.

14 Q AND JUST TO CLARIFY, YOU KNOW YOU HAVE A WHOLE FILE  
15 BECAUSE YOU HAVE ONE COMPLETED FILE AVAILABLE FOR SHARING AS  
16 INDICATED BY THIS ONE BOX IN THE LOWER LEFT CORNER?

17 A RIGHT; AND WHEN YOU GO TO THE NEXT SLIDE, IT'S EVEN  
18 MORE APPARENT --

19 Q OKAY.

20 A -- BECAUSE NOW, I'M GOING TO SHOW YOU THAT WHOLE  
21 FILE, EVEN THOUGH I HAVE ONE IN THE PROCESS OF BEING  
22 DOWNLOADED, INCOMPLETE --

23 Q RIGHT.

24 A -- HERE'S THE WHOLE FILE, AND LOOK AT THE HITS  
25 COLUMN IN THE UPPER RIGHT. IT'S BEING SHARED.

1 Q OKAY. SO THE ONE COMPLETED FILE THAT'S DEMONSTRATED  
2 BY THE ZERO -- I MEAN, THE 1 IN THE BOTTOM LEFT CORNER IS  
3 COMPLETE AND AVAILABLE FOR SHARING?

4 A RIGHT; AND THIS IS DONE WITH THE VERSION THAT'S IN  
5 QUESTION HERE, NOT 4.18.8. I DIDN'T TAKE THE TIME TO TEST  
6 THAT VERSION AS OF YET IN THIS -- IN THIS EXACT PROCESS THAT I  
7 FOLLOWED FOR THE VERSION THAT'S IN QUESTION IN THIS CASE, THE  
8 MORAN INVESTIGATION.

9 Q SO YOU USED THE VERSION THAT THE DEFENDANT USED IN  
10 THIS CASE?

11 A RIGHT.

12 Q AND THAT DETECTIVE CORDER OBSERVED?

13 A CORRECT.

14 Q OKAY. AND LET'S TALK ABOUT THE LAST PAGE OF YOUR  
15 EXHIBIT.

16 WHAT ARE WE LOOKING AT HERE?

17 A SO THEN, I SHOWED YOU A -- IF YOU SCROLL OVER TO THE  
18 LEFT, THIS IS THE -- NO, TO THE -- LEFT.

19 IS THAT THE RIGHT OR LEFT?

20 Q LEFT.

21 A I'M SORRY. IS THAT RIGHT -- OR THE OTHER WAY.

22 Q I THINK YOUR LEFT IS MY RIGHT.

23 A I WANT YOU TO GO TO YOUR LEFT.

24 Q MY LEFT IS HERE.

25 A YEAH. SCROLL DOWN.

1 Q (COMPLYING.)

2 A YOU CAN SEE HOW IT SAYS, INCOMPLETE FILES.

3 Q YES.

4 A I'M JUST SHOWING YOU THAT THIS IS THAT INCOMPLETE  
5 FILES THAT IS COEXISTING WITH THE COMPLETED FILE, NO PROBLEM;  
6 AND IF YOU SCROLL OVER TO THE HITS COLUMN, IT'S STILL A ZERO,  
7 SO MY COMPUTER'S RESPONDING I HAVE A FILE BECAUSE I HAVE A  
8 COMPLETED FILE, BUT HERE, I HAVE CREATED AN ENVIRONMENT WHERE  
9 I'M, YOU KNOW, REPORTING OUT TO THE NETWORK THAT I HAVE A  
10 CERTAIN FILE, BUT IT'S RESPONDING TO THE WHOLE FILE, NOT THE  
11 PARTIAL FILE.

12 Q OKAY. SO IF I'M UNDERSTANDING YOUR TESTIMONY  
13 CORRECTLY, AS DEMONSTRATED BY THE LAST PAGE IN YOUR SLIDE, YOU  
14 DOWNLOADED A COMPLETE FILE; THEN, YOU WENT BACK AND ATTEMPTED  
15 TO DOWNLOAD THE SAME FILE ONLY 27 PERCENT, I BELIEVE, IS WHAT  
16 YOUR TESTING --

17 A RIGHT.

18 Q -- DEMONSTRATED; AND YOU TRIED TO MAKE THAT PARTIAL  
19 FILE THAT YOU DOWNLOADED 27 PERCENT AVAILABLE FOR SHARING?

20 A RIGHT.

21 Q AND WHEN YOU MADE IT AVAILABLE FOR SHARING, YOU WERE  
22 SHOWING NO HITS, MEANING, NO ONE WAS THERE OR NO ONE -- IT  
23 COULDN'T BE SHARED TO ANYBODY?

24 A CORRECT. THE MOST IMPORTANT PART OF THIS LAST  
25 PROCESS IS TRY TO EXPLAIN, AND I DIDN'T HAVE THE LUXURY OF



1 SPEAKING WITH TAMI LOEHRS WHEN I WAS DOING THIS. ALL I COULD  
2 DO IS READ HER REPORT, TRY TO EXPLAIN THE ANOMALY THAT I SAW  
3 HERE: HEY, WAIT A MINUTE. SHE'S SHARING THAT ONE FILE. I  
4 KNOW THAT ONE INDICATOR SHOULD BE A ZERO WHEN SHE HAS THIS  
5 AC/DC ALREADY DOWNLOADED, SO I KNEW MY QUESTION TO HER WAS  
6 WHAT IS THAT FILE, AND I SAT AND LISTENED TO HER TESTIMONY,  
7 AND SHE SAID, I DON'T KNOW.

8 Q AND THAT'S IN DIRECT REFERENCE TO THIS PARTICULAR  
9 SCREEN SHOT FROM MISS LOEHRS' TESTING?

10 A RIGHT. SHE HAD A SHARED FILE, EVEN THOUGH SHE'D  
11 ONLY DOWNLOADED TEN PERCENT OF A FILE "A," TO HAVE A  
12 SCIENTIFIC TEST PERFORMED, SHE SHOULD BE ABLE TO REPLICATE THE  
13 TEST: I CAN REPLICATE MY TEST; AND "B," I NEED TO DOCUMENT IT  
14 WELL SO THAT IT'S BEING TOLD TO THE COURT HERE.

15 SHE HAS NO IDEA WHAT SHE'S SHARING, AND SHE'S  
16 REPRESENTING IT AS PROOF POSITIVE AND TAKING A POSITION IN  
17 SOMETHING THAT SHE CAN'T RECREATE BY HER OWN TESTIMONY.

18 Q NOW, YOU ADMIT YOU'RE FAMILIAR WITH PEER SPECTRE,  
19 AND YOU KNOW THE REASON, HAVING SAT HERE THROUGH TESTIMONY IN  
20 THIS CASE, AS TO WHY DEFENSE COUNSEL PURPORTS TO NEED THE  
21 SOFTWARE.

22 DO YOU, AS A LAW ENFORCEMENT OFFICER AND A TRAINER  
23 ON THIS MATERIAL, SEE ANY HARM IN PROVIDING THE PEER SPECTRE  
24 SOFTWARE?

25 A ABSOLUTELY.

1 Q AND WHAT IS THAT HARM?

2 A I DO NOT WANT TO GIVE ANY SOFTWARE THAT I HAVE THAT  
3 IS TRICKS OF THE TRADE, SO TO SPEAK, BUT -- YOU KNOW, TO THE  
4 DEFENSE.

5 IT IS LAW ENFORCEMENT SENSITIVE. IT'S WHAT WE'RE  
6 USING TO IDENTIFY THESE POTENTIAL TARGETS. IT'S PART OF A  
7 SYSTEM AND ISN'T -- SO IT'S IMPORTANT TO ME TO KEEP THAT IN  
8 LAW ENFORCEMENT'S HANDS. THIS IS ALREADY, YOU KNOW, I KNOW,  
9 F.B.I. EP2P TOOL. THEY WANTED THAT, AND THEY WEREN'T ABLE TO  
10 GET THAT IN THE NINTH CIRCUIT HERE, BUT WE'RE IN A UNIQUE  
11 SITUATION WHERE THEY'RE ASKING FOR SOMETHING THAT DOESN'T  
12 MATTER.

13 I DON'T WANT THEM TO HAVE IT BECAUSE IT'S HOW WE  
14 OPERATE. IT'S LAW ENFORCEMENT SENSITIVE. IT OPERATES IN A  
15 CERTAIN AUTOMATED WAY, BUT AT THE END OF THE DAY, IT CANNOT  
16 SEE ANY SEARCH HITS EXCEPT FOR WHAT LIMEWIRE 4.14.0 WILL SEND  
17 TO IT.

18 IF I WAS ON THE DEFENSE SIDE, AND I WAS THEIR  
19 EXPERT, I WOULD HAVE LIMEWIRE 4.14.0 AND SEE BY LOOKING AT THE  
20 SOFTWARE AND THE SOURCE CODE WHAT RESULTS IT WILL ISSUE OUT TO  
21 ANY CLIENT, PEER SPECTRE OR BEARSHARE OR LIMEWIRE. THEY CAN  
22 ANSWER ALL QUESTIONS WITH A PIECE OF SOFTWARE THEY ALREADY  
23 HAVE; AND AS IT RELATES TO OTHER ARGUMENTS I'M AWARE OF IN  
24 COURTS, YOU KNOW, THE INVESTIGATIVE TOOL THAT THE F.B.I. USES,  
25 EP2P, THE NINTH CIRCUIT SAID THE DEFENSE WAS NOT ENTITLED TO

1 IT, BUT THEY'RE IN A UNIQUE SITUATION. THEY ACTUALLY HAVE  
2 ACCESS TO THE SOURCE CODE AND THE PROGRAM USED IN THIS CASE.  
3 THEY HAVE MORE IN THIS INVESTIGATION THAN IN THAT NINTH  
4 CIRCUIT CASE, AND YET, THEY CHOSE TO NOT EVEN LOOK AT THE  
5 SOFTWARE THAT THEY HAVE AVAILABLE TO THEM TODAY.

6 Q IS IT THAT SOFTWARE BEING LIMEWIRE AND PHEX?

7 A LIMEWIRE AND PHEX SOURCE CODE IS AVAILABLE TO ANYONE  
8 WHO WANTS IT.

9 Q NOW, I KNOW YOU MENTIONED YOU, AS A LAW ENFORCEMENT  
10 OFFICER, WOULD NOT WANT THE DEFENSE TO HAVE THE TRICKS OF THE  
11 TRADE.

12 DO ANY OTHER LAW ENFORCEMENT OFFICERS FEEL THE SAME  
13 WAY THAT YOU DO?

14 A ABSOLUTELY. I'M A DEVELOPER OF A PROGRAM FOR LAW  
15 ENFORCEMENT, AND I WILL CONTINUE TO MAKE MYSELF AVAILABLE TO  
16 FIGHT THIS BECAUSE WE ARE USING OPEN SOURCE PROGRAMS AND JUST  
17 TWEAKING THEM TO HELP INVESTIGATORS, BUT THE BASIC FUNCTIONING  
18 OF PEER SPECTRE, OF THE MODIFIED PHEX VERSION I'M INVOLVED  
19 WITH OR THE EP2P TOOL, IS THAT IT OPERATES THE SAME WAY; AND  
20 AT THE END OF THE DAY, ANYTHING THE DEFENSE WOULD EVER NEED TO  
21 ANSWER WHAT IT WAS ABLE TO COLLECT CAN BE FOUND IN THE CLIENT  
22 OR THE SUSPECT IN THAT CASE OR THE ACCUSED IN THAT CASE WAS  
23 RUNNING, AND THAT'S ALL THEY NEED TO ANSWER THEIR QUESTIONS,  
24 SO I DON'T WANT SOME DEFENSE EXPERT OR DEFENSE ATTORNEY  
25 WRITING A PAPER EDUCATING THE POTENTIAL TARGETS WE WOULD HAVE

1 IN THE FUTURE ON HOW WE'RE DOING OUR JOB.

2 I DON'T WANT THEM TO KNOW HOW I AM CONDUCTING MY  
3 INVESTIGATIONS SO WE CAN CONTINUE TO SAVE CHILDREN AND NOT  
4 HAVE THEM BE ABUSED BY PEOPLE ON -- THROUGH THE -- THE ABUSE  
5 THAT HAPPENS THROUGH CHILD PORNOGRAPHY IN ITSELF AND --  
6 CONSIDERING THESE ARE LIVE VICTIMS OUT THERE BEING ABUSED.

7 Q IF THIS INFORMATION WERE DISCLOSED, COULD THAT  
8 AFFECT THE WAY LAW ENFORCEMENT OPERATES IN REGARDS TO THEIR  
9 INVESTIGATION IN COMPUTER CRIMES?

10 A YES; AND -- AND ON TOP OF THAT IS THEY DON'T NEED IT  
11 TO PERFORM THE TEST THAT THEY'RE ASKING TO TEST, THEY NEED TO  
12 TEST LIMEWIRE.

13 (MS. ANDRUS CONFERRING WITH MS. HARRIS.)

14 Q BY MS. HARRIS: AND WHAT ABOUT -- SEPARATE AND APART  
15 FROM THE PEER SPECTRE, WHAT ABOUT THE TRAINING MATERIALS AND  
16 THE MANUALS THAT GO ALONG WITH THE SOFTWARE? IS THERE ANY  
17 HARM IN DISSEMINATING THAT INFORMATION?

18 A THOSE ARE METHODS THAT WE USE TO INVESTIGATE PEOPLE  
19 ONLINE. THERE'S NO NEED FOR THEM TO HAVE THAT. I'M SITTING  
20 HERE, TESTIFYING THAT STILL, TO THIS DAY, WE FOLLOW THE SAME  
21 PROTOCOL THAT THE DETECTIVE USED IN THIS CASE. IT DOESN'T  
22 SERVE ANY PURPOSE WHATSOEVER. THEY NEED TO LOOK AT THE  
23 LIMEWIRE AND ANALYZE THE VERSION OF THE PROGRAM THAT DEFENDANT  
24 WAS USING.

25 I DON'T WANT THEM TO KNOW HOW WE -- YOU KNOW, HOW WE

1 CONNECT TO THEM. MAYBE WE TRY TO INITIATE A CHAT -- I'M JUST  
2 MAKING THINGS UP FOR SAKE OF ARGUMENT. WHATEVER PROCESS IS,  
3 AND WHATEVER INVESTIGATIVE PROTOCOL WE FOLLOW, I DON'T WANT  
4 THE DEFENSE TO KNOW -- IF PART OF OUR PROTOCOL IS THAT WE WILL  
5 ALWAYS TRY TO CHAT WITH A PERSON, I DON'T WANT THEM TO KNOW  
6 THAT WE ALWAYS TRY TO CHAT WITH A PERSON SO THEY CAN PUBLISH  
7 THIS TO THE PUBLIC AND MAKE CRIMINALS AWARE THIS IS HOW LAW  
8 ENFORCEMENT OPERATES.

9 Q ARE THERE OTHER THINGS OR OTHER INFORMATION OR  
10 TECHNIQUES INCLUDED IN THESE MANUALS, SEPARATE AND APART FROM  
11 HOW THIS SOFTWARE FUNCTIONS; FOR EXAMPLE, HOW TO DO CERTAIN  
12 INVESTIGATIVE TECHNIQUES?

13 I BELIEVE YOU KIND OF MADE REFERENCE TO IT, AS FAR  
14 AS INITIATING CHATS AND THAT TYPE OF THING.

15 A YES. I MEAN, I DON'T KNOW WHAT ALL'S IN ALL THE  
16 MANUALS -- THE MANUALS THAT I'M INVOLVED WITH. I DON'T KNOW  
17 WHAT MANUALS SHE HAS. I DON'T KNOW WHAT THE WYOMING PROTOCOL  
18 GAVE TO HER, BUT IT IS VERY POSSIBLE -- I KNOW THAT, AS A  
19 WHOLE, IT TEACHES AN INVESTIGATOR FROM THE GROUND UP WHAT  
20 GNUTELLA IS, AND HOW TO DO THIS INVESTIGATION, HOW TO COLLECT  
21 THE EVIDENCE, AND THINGS OF THAT NATURE THAT DOESN'T  
22 PERTAIN -- OR DOES -- I DON'T BELIEVE SHOULD BE AVAILABLE TO  
23 THE DEFENSE, AND IT ISN'T RELEVANT. THEY HAVE EVERYTHING THEY  
24 NEED.

25 Q IS IT POSSIBLE THAT IT COULD CONTAIN HOW TO

1 INTERVIEW A SUSPECT IN REGARDS TO FILES OR INFORMATION YOU  
2 RECEIVED ON LIMEWIRE?

3 A ABSOLUTELY.

4 Q AND WOULD THAT BE DAMAGING TO YOU AS A LAW  
5 ENFORCEMENT OFFICER?

6 A CORRECT. I WOULDN'T WANT -- I WOULDN'T WANT SOMEONE  
7 TO KNOW THE INTERVIEWING TECHNIQUES THAT I USE TO ELICIT A  
8 CONFESSION.

9 MS. HARRIS: I HAVE NO FURTHER QUESTIONS, YOUR  
10 HONOR.

11 THE COURT: ALL RIGHT. THANK YOU.

12 IS THIS THE BEST TIME TO JUST STOP NOW AND COME BACK  
13 TO -- ANOTHER DAY? I'M ASSUMING BOTH COUNSEL WILL CHECK WITH  
14 EACH OTHER AND GIVE US A TIME. IF I'M IN A TRIAL, WE'LL JUST  
15 TAKE A DAY RECESS.

16 MS. HARRIS: THANK YOU, JUDGE.

17 THE WITNESS: THANK YOU, YOUR HONOR.

18 THE COURT: THANK YOU. THANKS, EVERYONE.

19 MS. HARRIS: AND, JUDGE, JUST FOR THE RECORD, I  
20 BELIEVE DEFENSE COUNSEL SAID THAT HE WAS AVAILABLE ON MONDAY.  
21 I WILL CLEAR MY CALENDAR AND BE AVAILABLE ON MONDAY SO THAT WE  
22 CAN TIE UP THE REMAINING WITNESSES THAT ARE ACTUALLY HERE IN  
23 ARIZONA SO THAT ALL WE WOULD HAVE LEFT IS CORPORAL ERDELY.

24 THE COURT: OKAY. WE'LL START AT 10:30 MONDAY.

25 IS THAT OKAY? ELEVEN?

1 MR. GILLESPIE: ACTUALLY, I HAVEN'T CHECKED MY  
2 CALENDAR, BUT I CAN DO THAT RIGHT NOW.

3 THE COURT: OKAY. LET US KNOW.

4 MR. GILLESPIE: YES, SIR.

5 THE COURT: WE'VE GOT IT DOWN FOR 10:30 MONDAY. LET  
6 US KNOW IF THAT'S NOT GOING TO GO.

7 OKAY. WE'RE AT RECESS. EVERYBODY RELAX.

8 (THERE WAS A BREAK IN THE PROCEEDINGS AT  
9 4:19 P.M. UNTIL 4:20 P.M.)

10 MS. HARRIS: I WANT TO CLARIFY A POINT BECAUSE I  
11 WANT TO MAKE SURE WE'RE ALL ON THE SAME PAGE, AS FAR AS THE  
12 ORDER THAT WE HAVE LEFT. I BELIEVE DEFENSE COUNSEL WANTED TO  
13 CALL DETECTIVE LITCHFIELD, AND THE STATE HAD --

14 THE COURT: ON MONDAY?

15 MS. HARRIS: ON MONDAY; AND THEN, THE STATE -- IF  
16 DEFENSE IS DONE WITH THAT PORTION OF THEIR QUESTIONING, THE  
17 STATE HAS A WITNESS, DETECTIVE BALE (PHONETIC), WHO IS THE  
18 INVESTIGATOR ON THE ROBISON CASE, AND WE WANT TO GET THROUGH  
19 THOSE TWO, IF WE CAN, ON MONDAY, BUT I BELIEVE -- AND I JUST  
20 WANT TO MAKE SURE -- AFTER WE ARE DONE WITH THOSE WITNESSES,  
21 THAT WILL JUST LEAVE CORPORAL ERDELY AND MRS. LOEHRS.

22 THE COURT: OKAY. AND YOU BUY THAT?

23 MR. GILLESPIE: AS FAR AS I KNOW. I MEAN, WE HAVE  
24 THE RIGHT TO CALL MISS LOEHRS IN REBUTTAL --

25 MS. HARRIS: RIGHT.

1 MR. GILLESPIE: -- SO...

2 THE COURT: SURE.

3 MR. GILLESPIE: -- AS FAR AS I KNOW, I THINK THAT  
4 WOULD CONCLUDE THE EVIDENCE.

5 THE COURT: AND, SERIOUSLY, IF BOTH BOTH OF YOU WANT  
6 TO CONSIDER TO STIPULATE THAT PROGRAM ABOUT WE'VE BEEN USING  
7 IT, PEOPLE IN FLORIDA, ALL OVER THE PLACE -- THEY'VE BEEN  
8 TESTIFYING IN ACTUAL JURY TRIALS...

9 MR. GILLESPIE: USING WHICH PROGRAM?

10 THE COURT: SKYPE. WE'VE GOT THE SKYPE EXPERT IN  
11 TOWN. HE COMES -- I DON'T KNOW WHERE HE COMES FROM.

12 DO YOU KNOW WHO THAT WAS, THE SKYPE CLERK?

13 THE CLERK: THE SKYPE GUY? I HAVE NO IDEA...

14 THE COURT: BE SURE AND THINK OF SKYPE. IT'S SO  
15 MUCH CHEAPER.

16 MS. HARRIS: I DO NOT HAVE THAT. I BELIEVE COUNSEL  
17 HAD THAT.

18 THE CLERK: COUNSEL, COPY OF THE AFFIDAVIT OF SEARCH  
19 WARRANT, EXHIBIT 3, I'M MISSING IT.

20 MR. GILLESPIE: (COMPLYING.)

21 THE COURT: THANK YOU VERY MUCH.

22 MS. HARRIS: NO PROBLEM.

23 THE COURT: OKAY. SOMETHING ELSE YOU WANTED ON THE  
24 RECORD.

25 OKAY. WHAT ELSE?



1 MS. ANDRUS: JUDGE, I THINK MY -- THIS IS JUST SO  
2 THAT I UNDERSTAND. I UNDERSTOOD THAT, EITHER YESTERDAY OR THE  
3 DAY BEFORE, YOU SAID THAT, AFTER THE EXPERTS TESTIFY, THAT YOU  
4 WOULD ALLOW EACH PARTY TO RECALL EACH EXPERT.

5 THE COURT: SURE.

6 MS. ANDRUS: OKAY. SO IN KEEPING WITH THAT, CAN  
7 WE -- WHEN WE BLOCK OFF THE TIME, CAN WE HAVE AT LEAST -- I  
8 MEAN, I THINK IT'LL TAKE AT LEAST ONE DAY BECAUSE WE HAVE  
9 CROSS AND, POTENTIALLY CALLING MISS LOEHRS AGAIN, AND THEN,  
10 POTENTIALLY CALLING CORPORAL ERDELY AGAIN; POSSIBLY TWO OR  
11 THREE DAYS.

12 THE COURT: WHATEVER TIME YOU NEED, WE'RE GOING TO  
13 GIVE YOU.

14 MS. ANDRUS: WE JUST DIDN'T WANT TO MESS WITH YOUR  
15 TRIAL SCHEDULE, BUT WE WANT TO MAKE SURE WE'RE NOT MESSING UP  
16 MISS LOEHRS' TIME OR CORPORAL ERDELY'S TIME, IF THE COURT HAS  
17 OTHER STUFF...

18 THE COURT: YOU'LL GIVE US THOSE DATES AS SOON AS  
19 POSSIBLE, WE'LL JUST MAKE OURSELVES AVAILABLE. IT IS  
20 IMPORTANT.

21 MR. GILLESPIE: IT IS IMPORTANT.

22 I GUESS WE'RE PROBABLY NOT ON THE RECORD.

23 ALL OF THIS IS COMING AT US AT THE LAST MINUTE. WE  
24 WOULD LIKE TO DO SOME ADDITIONAL TESTING NOW, AND I WOULD LIKE  
25 YOU TO ALLOW US TO DO THAT SO THAT WE COULD PRESENT THAT IN

1 OUR CROSS-EXAMINATION AND REBUTTAL.

2 THE COURT: YEAH, I DON'T EVEN HAVE A PROBLEM WITH  
3 THAT, BUT BOTH SIDES COULD DO MORE TO REBUT THE EXPERTS.

4 MR. GILLESPIE: OKAY.

5 MS. HARRIS: JUDGE, I DO HAVE A PROBLEM WITH THAT.  
6 WE'RE GOING TO EXTEND THIS HEARING INTO INFINITY ON PEOPLE  
7 DOING TESTS AND RETESTS.

8 WE DID IMPOSE A DEADLINE ON TESTING. I BELIEVE  
9 DEFENSE COUNSEL KNEW WHAT THE ISSUE WAS BECAUSE THEY RETAINED  
10 MISS LOEHRS TO SET FORTH THE TESTING. CORPORAL ERDELY  
11 PROVIDED INFORMATION THAT WAS COUNTER TO THAT, SO I BELIEVE  
12 IT'S UP TO THE JUDGE TO THEN DETERMINE WHICH VERSION HE IS  
13 RELYING ON MORE AND MORE CREDIBLE TO MAKE A RULING, SO TO KEEP  
14 DOING ADDITIONAL TESTING TO INFINITY, AT THIS POINT, WE WOULD  
15 THEN BE EXTENDING THIS HEARING MORE THAN JUST THE DAY OR TWO  
16 REMAINING IN THE FUTURE; WE'LL BE DOING ANOTHER FOUR OR FIVE  
17 DAYS ON TESTING AND RETEST, SO MY CONCERN IS THIS WILL BE  
18 DRAGGING OUT, AND WE'LL KEEP INCURRING NOT ONLY EXPENSES BUT  
19 WASTING TIME: CORPORAL ERDELY'S TIME, MRS. LOEHRS' TIME.

20 I WOULD LIKE TO TRY TO GET THIS HEARING AND THE  
21 RECORD AS CLEAR AS POSSIBLE, BUT I AM ALSO CONCERNED WITH  
22 ADDITIONAL TESTING WILL COME ADDITIONAL TESTIMONY. NOT JUST  
23 REBUTTAL TESTIMONY BUT TESTIMONY THAT CAN GO ON FOR WEEKS AND  
24 WEEKS AT A TIME.

25 THE COURT: WELL, I'LL PLAY THAT BY EAR BECAUSE

1 THINGS WEREN'T DISCLOSED FOR EACH SIDE. I WANT TO GET THE  
2 CORRECT ANSWER FOR THE APPELLATE COURT. WE'LL SEE HOW IT  
3 GOES.

4 MR. GILLESPIE: VERY FINE.

5 (WHEREUPON, THE PROCEEDINGS CONCLUDED AT  
6 4:26 P.M.)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

CERTIFICATE OF REPORTER

I, KIMBERLY D. MC ANDREWS, OFFICIAL REPORTER IN THE SUPERIOR COURT OF THE STATE OF ARIZONA, IN AND FOR THE COUNTY OF MARICOPA, DO HEREBY CERTIFY THAT I MADE A SHORTHAND RECORD OF THE PROCEEDINGS HAD AT THE FOREGOING ENTITLED CAUSE, AT THE TIME AND PLACE HEREINBEFORE STATED;

THAT SAID RECORD IS FULL, TRUE, AND ACCURATE;

THAT THE SAME WAS THEREAFTER TRANSCRIBED UNDER MY DIRECTION; AND

THAT THE FOREGOING EIGHTY-NINE (89) TYPEWRITTEN PAGES CONSTITUTE A FULL, TRUE, AND ACCURATE TRANSCRIPT OF SAID RECORD, ALL TO THE BEST OF MY KNOWLEDGE AND ABILITY.

DATED AT PHOENIX, ARIZONA, THIS 11TH DAY OF SEPTEMBER, 2011.

/S/ KIMBERLY D. MC ANDREWS  
KIMBERLY D. MC ANDREWS,  
C.S.R./C.C.R./C.R., R.P.R.

KIMBERLY D. MC ANDREWS, C.S.R./C.C.R./C.R., R.P.R.

UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF WISCONSIN  
GREEN BAY DIVISION

-----

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	Case No. CR 18-157
	)	Green Bay, Wisconsin
vs.	)	
	)	August 14, 2019
THOMAS J. OWENS,	)	1:35 p.m.
	)	
Defendant.	)	

-----

**TRANSCRIPT OF EVIDENTIARY HEARING**  
BEFORE THE HONORABLE WILLIAM C. GRIESBACH  
UNITED STATES CHIEF DISTRICT JUDGE

APPEARANCES:

For the Plaintiff

UNITED STATES OF AMERICA:

United States Dept of Justice  
(ED-WI)

By: DANIEL R. HUMBLE

Office of the US Attorney - 205

Doty St - Ste 301

Green Bay, WI 54301

Ph: 920-884-1066

Fax: 920-884-2997

Daniel.Humble@usdoj.gov

For the Defendant

THOMAS J. OWENS:

(Present)

Pruhs & Donovan SC

By: CHRISTOPHER D. DONOVAN

757 N Broadway - Ste 401

Milwaukee, WI 53202

Ph: 414-221-1950

Fax: 414-221-1959

donovanc34@hotmail.com

U.S. Official Transcriber:

JOHN T. SCHINDHELM, RMR, CRR,

Transcript Orders:

WWW.JOHN SCHINDHELM.COM

Proceedings recorded by electronic recording,  
transcript produced by computer aided transcription.



TRANSCRIPT OF PROCEEDINGS

Transcribed From Audio Recording

\* \* \*

1  
2  
3  
4 THE CLERK: The Court calls Case 18-CR-157, United  
01:42 5 States of America vs. Thomas J. Owens for an evidentiary  
6 hearing. May I have the appearances, please?

7 MR. HUMBLE: Dan Humble for the Government, along with  
8 Misha Linsmayer (phonetic) from our office, Your Honor.

9 THE COURT: Good afternoon.

01:43 10 MR. DONOVAN: Attorney Chris Donovan appearing on  
11 behalf of Mr. Owens who is here in person on my right. And  
12 then, also to my immediate right is our expert, Peyton Engel.

13 THE COURT: Okay. Good afternoon.

14 So we have put this on for a hearing on the motion to  
01:44 15 disclose investigative BitTorrent software and related  
16 documents. And the government has opposed the motion on the  
17 basis of the law enforcement privilege?

18 MR. HUMBLE: Yes, Your Honor.

19 THE COURT: Or investigation privilege?

01:45 20 And so the -- I guess, what do you -- Mr. Donovan,  
21 it's your motion, how would you plan on proceeding?

22 MR. DONOVAN: Your Honor, what I envision is I would  
23 call my expert. I think that we have at least the initial  
24 burden under Rule 16 to show that the requested material is  
01:45 25 material to preparing our defense.

1 THE COURT: Uh-huh.

2 MR. DONOVAN: And then I think the burden on the law  
3 enforcement privilege would fall to the government, so they can,  
4 you know, carry that burden when they call their witness.

01:46 5 THE COURT: That sounds good. Go ahead. You may call  
6 your witness.

7 MR. DONOVAN: Do you want him up on the witness stand?

8 THE COURT: Oh, yeah.

9 MR. DONOVAN: Okay.

01:46 10 THE CLERK: Please raise your right hand.

11 Do you solemnly swear the testimony you are about to  
12 give today is the truth, the whole truth and nothing but the  
13 truth so help you God?

14 THE WITNESS: I do.

01:46 15 THE CLERK: Please state and spell your first and last  
16 name for the record.

17 THE WITNESS: My name is Peyton Engel, that's  
18 P-e-y-t-o-n, E-n-g-e-l.

19 THE COURT: Thank you, Mr. Engel.

01:48 20 Go ahead, Mr. Donovan, you may proceed.

21 MR. DONOVAN: Thank you, Your Honor.

22 PEYTON ENGEL, DEFENSE WITNESS, DULY SWORN

23 DIRECT EXAMINATION

24 BY MR. DONOVAN:

01:48 25 Q. Good afternoon, Mr. Engel. I just want to run through a few

1 background questions with you. Can you state your education  
2 background?

3 A. I have a bachelor's degree in Russian from Grinnell College,  
4 a master's in Russian literature from the University of  
01:53 5 Wisconsin-Madison, and a JD from the University of  
6 Wisconsin-Madison.

7 Q. And can you do a brief overview of your work history?

8 A. Yes. In about 1997, I went into the field of IT networking,  
9 the bottom having fallen out of the Russian literature market.  
01:53 10 And I specialized in computer security for about 16 years. And  
11 that included doing forensic investigations and incident  
12 response.

13 Q. And where do you work now?

14 A. I currently work for a law firm in Madison, Wisconsin that's  
01:54 15 called Hurley Burish.

16 Q. And can you just give a brief on overview, not necessarily  
17 maybe listing everything, but some examples of your  
18 certifications and continuing education in the computer field.

19 A. I routinely provide training. So I speak at conferences and  
01:58 20 at trainings, for example, for the state public defender, mostly  
21 regarding how to work with computer experts, how litigators  
22 should work with computer experts.

23 I maintain the CISSP -- that's Certified  
24 Information -- CISSP, Certified Information Systems Security  
01:58 25 Professional certification -- which is sort of a broad or a



1 generalist security certification but it's, for better or worse,  
2 one of the standard ones that people obtain in the field. It  
3 includes some requirements for forensics and incident response  
4 knowledge as well.

01:59 5 Q. Thank you. You mentioned that you train other professionals  
6 in this area, correct?

7 A. Yes.

8 Q. And so you've spoken at different conferences?

9 A. Yes.

01:59 10 Q. And do you also have some published works?

11 A. Yes.

12 Q. Can you give an example of a few of those?

13 A. The most recent one was an article on cell phone forensics  
14 and that appeared in The Champion, which is the National  
01:59 15 Association of Criminal Defense Lawyers publication.

16 Q. And you've testified in court before?

17 A. Yes.

18 Q. And related to, again, computer issues?

19 A. Yes. I've appeared as an expert witness. This is my first  
02:06 20 venture into federal court, but I've appeared as an expert at  
21 trial and at evidentiary hearings in a number of state court  
22 proceedings.

23 Q. Can you give a rough estimate?

24 A. My affidavit actually lists some specific ones. I've  
02:06 25 probably appeared in 10 or so, 10 or 12. And then I've been an

1 expert in dozens more, but those haven't gone to trial.

2 Q. Okay, thank you. Okay. Have you also done some prior work  
3 for law enforcement before?

4 A. Once in a while. The most notable incident was -- well,  
02:07 5 never been deputized or anything like that, but in the course of  
6 my work I've assisted -- the FBI was the most notable, in an  
7 industrial espionage case down in Madison.

8 Q. So is it fair to say you've worked on both the defense side  
9 and law enforcement?

02:08 10 A. Yes, though heavily more on the defense side.

11 Q. Correct. Okay. Okay. Can you kind of explain what a  
12 peer-to-peer network is and how it operates?

13 A. Sure. A peer-to-peer -- well, the standard architecture on  
14 the internet is what's called a client server architecture. You  
02:09 15 have a centralized resource, say a website or something like  
16 that, that many people want to access. And so they'll use a  
17 client piece of software like a web browser to see the web  
18 server. And that shares this one central resource among many  
19 other users.

02:09 20 A peer-to-peer architecture is just a different  
21 arrangement. Instead of having one central resource, resources  
22 are distributed across the network and users share and consume  
23 on an as-needed basis.

24 Q. And to access a peer-to-peer network you have to download  
02:09 25 like a special type of software?

1 A. Yes. There's usually a peer-to-peer client software  
2 involved.

3 Q. Can you explain what open source software would be versus  
4 not open source?

02:10 5 A. Sure. Software is developed by programmers. And  
6 programmers write in a computer language. So, for example, C or  
7 Java. And that language is compiled -- the C or Java code  
8 itself is not what the computer runs. It's compiled and  
9 generated into an executable program for the computer. But that  
02:11 10 code that the programmers write is called the source code.

11 Closed source software means it's not publicly  
12 accessible. Open source software means that the source code is  
13 available for others to review or potentially update and modify.

14 Q. So would most of these peer-to-peer programs be open source  
02:13 15 software?

16 A. There's a variety. There are -- so, for example, at issue  
17 in this case is BitTorrent. There are both open and closed  
18 source BitTorrent clients.

19 Q. Okay. Now, is it your experience and knowledge that all  
02:14 20 software is subject to having bugs or errors or malfunctions in  
21 it?

22 A. Yes. This is a universal truth. I mean, not all software  
23 has tons of bugs. Some is sounder than others. But sort of the  
24 gold standard for software bug-trimming would be avionics  
02:16 25 software. And we've just recently seen the 737 Max disasters.

1 So it's a certainly heavily reviewed, heavily audited code that  
2 didn't function as expected.

02:16 3 Q. So even commercial products like Microsoft Word or Excel or  
4 other, you know, highly common programs have bugs and errors,  
5 correct?

6 A. Yes. And these are systems that are wildly deployed, you  
7 know, used by many, and there's a robust system for reporting  
8 issues and, you know, having them escalated and filtered through  
9 technical support. But I still get updates from Microsoft  
02:20 10 probably twice a month.

11 Q. Can you explain a little bit more about like how they're  
12 addressed? So, for example, is there things called "patches"  
13 that fix errors?

14 A. Right. A "patch" is a term for usually a small update to a  
02:20 15 piece of software. So there are patches. And then larger  
16 things might be called "service packs." These are basically  
17 usually small executable pieces of code that are delivered and  
18 they update some aspect of a piece of software that's been  
19 deployed out in the field.

02:21 20 Q. Now, do most programs also go through what's called "beta  
21 testing"?

22 A. Yes. Generally there's a beta phase before it's sent into  
23 full production.

24 Q. Could you explain what a beta test would be?

02:21 25 A. Sure. So a beta testing happens when people think the

1 software is pretty much done and more or less ready to deploy.  
2 They'll deploy it in a way that generally more sophisticated  
3 users who would be good at spotting issues and good at reporting  
4 the issues, have a chance to tinker with the software and to use  
02:24 5 it and get the hang of it before it gets a general release.

6 Q. Is it kind of fair to say they kind of put it through its  
7 paces before it becomes generally used?

8 A. That's the idea of beta testing.

9 Q. And just to be clear, are most beta testers outside the  
02:25 10 entity or the company that made the software?

11 A. That depends on the kind of software and who the eventual  
12 user base is. Probably in the world at large, yes, but for any  
13 given project it might be different.

14 Q. Now, can you describe briefly what the interface would look  
02:25 15 like on a peer-to-peer program?

16 A. Well, it's usually a graphical user interface these days.  
17 There's a way of searching for -- let's restrict ourselves to  
18 peer-to-peer file sharing programs. There are other things out  
19 there, but there would be an interface for searching for the  
02:26 20 type of file you want to find.

21 So, for example, if I want to download the latest Star  
22 Wars movie or something like that, there would be a place to  
23 type in what I'm searching for and a place to see results and  
24 select which ones I wanted to obtain.

02:26 25 Q. So there would be like a search bar that you could type in

1 like a text search, for example?

2 A. Yeah. I mean, something -- something like that is present  
3 somewhere along the way. Different clients will look different,  
4 but, yes, that functionality is there in one form or another.

02:27 5 Q. Can users also search by hash values if they would know the  
6 hash value of the particular file that they want?

7 A. It would be strange for a user to even understand what a  
8 hash value is. I have no -- I mean, there's no reason the  
9 software couldn't support that, but for someone to sit and enter  
02:27 10 a 48-digit hexadecimal numbers -- I wouldn't think most users  
11 would do that.

12 Q. And maybe just to make sure everyone's on the same page, can  
13 you briefly explain what a hash value is?

14 A. Right. So a hash value, sometimes people call it the  
02:28 15 "digital fingerprint" of a file. So suppose you have two files  
16 and you want to know if they're the same. Rather than go and  
17 bit-by-bit compare them, you can pass them each through a  
18 certain kind of mathematical function, called a "hash function,"  
19 and you obtain a number. And if those two numbers are the same,  
02:28 20 then the chances are astronomically small that the two files are  
21 different. And so a hash value is sort of a shorthand for  
22 identifying a file or a piece of a file.

23 Q. Now, you've reviewed the pleadings in this case, correct?

24 A. Yes. At least the initial ones.

02:29 25 Q. Including the government's response brief --

1 A. Yes.

2 Q. -- to our motion to compel?

3 Now, they raise this concern about if the program's  
4 turned over that, you know, hash tags could be manipulated to  
02:30 5 change and then they'd be harder to detect. Right? Do you  
6 remember -- do you recall that?

7 A. I do recall that.

8 Q. Okay. Now, why in your opinion would that be a red-herring  
9 argument?

02:30 10 A. For a couple of reasons. First, I presume, but do not know,  
11 that the database of known hash values is separate from the  
12 program itself. So one could look at the program without  
13 necessarily seeing the full list of things that it looks for.

14 Second, the government discloses hash values every  
02:31 15 time it applies for a search warrant. You see not only the hash  
16 value of the file that they say they've obtained, but also the  
17 file name that is associated with it. So it's not that any  
18 individual hash value is that big a secret.

19 Third, it's possible for anyone on the internet to go  
02:31 20 ahead and change a single bit in a file today without the  
21 software having been disclosed. And that would change the hash  
22 value and it would no longer trigger the automated alerts that  
23 the Torrential Downpour software generates.

24 That's something that could happen today for free and  
02:33 25 without any -- you know, without any need for knowledge of the

1 code base.

2 But fourth, that would actually reduce the ability to  
3 share or at least the ease with which people are sharing  
4 contraband materials on the internet because of all the hash  
02:33 5 value changes -- values change. Then the Torrent clients won't  
6 know how to find the software for the images or movies or  
7 whatever it is they're downloading anymore because the whole  
8 thing is premised on a shared, you know, set of hash values.

9 So, yes, that could happen. But it doesn't seem to me  
02:34 10 to be either a realistic possibility or one that would -- I  
11 mean, it would actually probably cut down on the sharing of  
12 child pornography on the internet.

13 Q. Now, you talked earlier about source code versus the program  
14 itself, right?

02:34 15 A. Yes.

16 Q. Can you explain what concerns there might be about turning  
17 over source code?

18 A. So the gold standard for understanding how a piece of  
19 software works is to review the source code. You get to see  
02:34 20 pretty much everything it's capable of. And you can then see  
21 all of the inputs that it takes and all of the ways in which it  
22 gives output and all of the logic that it operates on. So the  
23 concern there would be that by knowing that, one would know  
24 something that couldn't otherwise be known.

02:36 25 So, for example, from time to time, and I believe in



1 this case, the government raises the concern that this kind of  
2 disclosure would impede future or ongoing investigations. So I  
3 can think of a couple ways that that might happen.

4 One is, that we know from reading the warrants here  
02:37 5 and in other cases, that RoundUp pretends to be sharing files in  
6 order not to get kicked off the network or throttled from being  
7 able to download files.

8 If it were the case that RoundUp always shared the  
9 same list of files, that might be a way of recognizing RoundUp  
02:39 10 and people who wanted to avoid being tagged by it would simply  
11 hang up the phone whenever something sharing those files  
12 connected.

13 Another thing might be that -- and this is  
14 hypothetical. I don't know this because I haven't had access to  
02:40 15 the source code. But another thing might be that if the system  
16 is designed so that -- to prevent law enforcement in one  
17 jurisdiction from accidentally investigating other users of  
18 RoundUp in another jurisdiction, maybe there's something about  
19 the way that it establishes its connection or operates -- or  
02:41 20 interacts with the systems it's investigating that could be  
21 recognized. That would be another sort of handshake signature  
22 that you could figure out this is RoundUp connecting to me and  
23 then hang up the phone again.

24 That would be -- those would be two ways that I can  
02:41 25 think of that would be potentially problematic.

1 Q. Now, those concerns wouldn't be raised if it was just  
2 getting access to the program and not the source code, correct?

3 A. Well, it would be less of a concern. It would sort of  
4 depend on how the program operates and what we'd be able to  
02:43 5 observe about it.

6 Q. Fair enough. I understand, again, you obviously don't have  
7 access to the program so you can't say for sure.

8 Okay. And I just want to clarify one thing. When you  
9 say RoundUp, you're using that interchangeably with Torrential  
02:43 10 Downpour?

11 A. Yes. I am sorry. That's a habit that I have. The  
12 investigative software, which is RoundUp-like, which is used on  
13 BitTorrent, is called "Torrential Downpour" from what I've read.

14 Q. Okay. So going back to peer-to-peer network I guess  
02:44 15 architecture. So it's a decentralized network, correct?

16 A. Yes.

17 Q. And this would be to allow sharing more efficiently and  
18 faster than if it was just in a centralized network?

19 A. Right. So the problem that the designers were attempting to  
02:45 20 solve was, how do we exchange large files that aren't hosted at  
21 some giant file repository like a Google Docs or something like  
22 that? How do we just trade large files on the internet?

23 And the issue is that when we purchase a connection to  
24 the internet from our internet service provider, whether it's  
02:46 25 AT&T or Comcast or whatever it is, the connection we get is

1 generally what's called asymmetrical. Meaning that we can  
2 download things much faster than we can upload them. Because  
3 the people who provision those circuits realize correctly that  
4 for most people's purposes that's the right way to do it. Most  
02:46 5 people are much more interested in downloading things than they  
6 are in uploading things.

7           So you might get, say, from a Spectrum, Charter  
8 Spectrum account you might get 200 megabits downstream to your  
9 house so can watch Netflix on several TVs at once, but you might  
02:46 10 only get, you know, 30 or 50 megabits upstream. So the problem  
11 is if -- let's say you and I want to exchange a file -- well, I  
12 want to get a file from you. I'm limited. Even though I can  
13 download things with blazing speed, I'm limited to getting the  
14 file by the fastest speed that you can upload. And so that  
02:49 15 makes things crawl to a halt, and it also means you can't be  
16 sharing multiple files at once, et cetera.

17           So the insight of BitTorrent is, hey, why don't we  
18 chop the files up. Why don't we have the files stored on  
19 multiple systems around the internet, or at least realize that  
02:49 20 they are stored in multiple systems around the internet, chop  
21 them up into segments, and I can grab one segment from system A,  
22 one segment from system B, one segment from system C, and then  
23 get the benefit of my fast bandwidth by being able to download  
24 from several sources at once and you get the file faster that  
02:50 25 way.

1 Q. Can you describe briefly how computers connect to the  
2 internet and maybe also discuss what an IP address is?

3 A. Sure. So one of the hard problems in computing in the '70s  
4 was how do we get computers to talk to each other. And what  
02:51 5 came out of this, the sort of system that emerged and towers  
6 above all others today is what's called the "internet protocol."  
7 It's a series of rules or standards by which one communicates on  
8 the internet.

9 And one of the challenges that it solves is how do we  
02:52 10 route a message. So let's say we have a network that spans the  
11 nation or even the world, how do I get a message from one  
12 computer to another?

13 And so the way this is accomplished is via IP  
14 addresses and routing protocols. But for the purposes of this  
02:53 15 conversation, every machine that is connected to the internet is  
16 assigned or associated with at least one IP address.

17 And when we are -- you can think of -- as the machine  
18 sends messages across the internet, you can think of this as  
19 being like the send and return addresses on a mail envelope. It  
02:53 20 has a "destination" IP address, each message does, and a "sent  
21 from" IP address. And so that when the guy at the other end of  
22 the connection gets the message, he knows where to reply to.

23 So IP addresses are distributed more or less  
24 geographically. So we can -- by IP address, we can draw some  
02:54 25 inferences about where a system is located in the physical world

1 and which internet service provider allocates it. And this is  
2 what allows investigators, when they find an IP address that  
3 they think is associated with a crime, they can get an  
4 administrative subpoena or some other mechanism that compels the  
02:54 5 relevant internet service provider to disclose the identity of  
6 the subscriber who was using that IP address at the time.

7 Q. Okay. So I'd like to talk a little bit about how  
8 BitTorrent's a little different than maybe perhaps other  
9 peer-to-peer programs. So you've talked about these little  
02:55 10 pieces of a file. Would those be called "torrents"?

11 A. So a torrent -- at least the way I think of it is, there's a  
12 thing called a "torrent file" which is kind of like a recipe for  
13 obtaining and assembling a given set of contents.

14 So, again, let's use the example of the latest Star  
02:56 15 Wars movie. It would list the -- for each segment of the file  
16 some directions for where to find that and how to, once you've  
17 got all the segments, how to assemble that into the finished  
18 product.

19 Q. And then -- so a torrent is basically a map that then helps  
02:57 20 the computer receiving these different pieces to assemble them,  
21 correct?

22 A. Right. It tells you -- it's kinda like a recipe. It tells  
23 you what ingredients to get and how to put them together.

24 Q. Okay. And, again, BitTorrent is decentralized? There's no  
02:57 25 central server or hierarchy, correct?

1 A. Yes.

2 Q. Okay. I'd like to talk now about Torrential Downpour, or  
3 what you call RoundUp, and how it modifies the normal BitTorrent  
4 program. Okay? So first off, Torrential Downpour is not open  
02:58 5 source, correct?

6 A. Correct. The source code is secret.

7 Q. So, not publicly available from any other source, right?

8 A. Correct.

9 Q. Do you know anything about I guess the origin or who created  
02:58 10 these programs?

11 A. There are publications available, some of them authored by  
12 the gentleman at the prosecution table, that describe its  
13 creation. It's a collaboration between law enforcement and some  
14 computer scientists.

02:59 15 Q. Okay.

16 A. I couldn't name them right off the top of my head.

17 Q. And that's fine. I'm not asking you to name them.

18 There's certain things we do know about Torrential  
19 Downpour that is different than the normal BitTorrent program,  
02:59 20 correct?

21 A. Yes.

22 Q. Okay. Is one of the differences what's called single source  
23 downloading?

24 A. Yes. As I described earlier, the goal of BitTorrent was to  
02:59 25 allow people to obtain files in pieces from multiple sources.

1 That was the point of it.

2 For law enforcement purposes, though, in order to  
3 prove that a user has the entirety of one file, it's necessary  
4 to get all of the segments from that one target computer. So  
03:00 5 one of the things that RoundUp is designed to do is obtain an  
6 entire download from a single source.

7 So it's speaking the BitTorrent protocol, but doing so  
8 in a way that sort of subverts the purpose of it. It's not  
9 breaking any rules, but it's definitely doing something out of  
03:01 10 the ordinary and deviating from the BitTorrent standard.

11 Q. And again, this isn't something a normal BitTorrent user  
12 would do or how it would operate.

13 A. It's not something a normal BitTorrent user would probably  
14 want to do, since it just makes things go more slowly. But,  
03:01 15 yes, standard BitTorrent software would not be capable of doing  
16 this.

17 Q. Now, you mentioned earlier that it also might basically fake  
18 file share so it doesn't get throttled down on the network. Can  
19 you explain that a little bit more?

03:02 20 A. So one of the things that people quickly discovered when the  
21 BitTorrent standard was first developed is that people would do  
22 what's called "leaching." They would come and download a bunch  
23 of stuff, but they wouldn't be sharing anything. So they would  
24 be consuming BitTorrent resources but not contributing back.

03:02 25 So various efforts were made to force people to share

1 at least what they had downloaded, and maybe other things as  
2 well, so that they weren't just a drag on the network; so that  
3 they're contributing.

03:05 4 And so what you see is clients that aren't sharing  
5 anything won't get preferential treatment in terms of downloads.  
6 They won't get necessarily access. Their ability to download  
7 will be throttled.

8 Q. And why would law enforcement not want to be participating  
9 in the sharing?

03:05 10 A. Well, there are a couple of reasons. One would be, they  
11 don't want to commit any crimes.

12 The other one -- I mean, that's probably the major  
13 one. But they probably also want to appear as though at least  
14 from time to time they are sharing contraband because then  
03:11 15 they'll get more interesting connections inbound to them.

16 Q. And do you have any I guess speculation on how they could  
17 hold themselves out as sharing when they're not, in fact,  
18 sharing?

19 A. Oh, you simply respond to search queries saying, yeah, I've  
03:11 20 got this or -- you know, I don't know the exact dimensions of  
21 the protocol that they're speaking. You know, I don't know  
22 exactly what messages they're sending, but they can advertise  
23 what they've got.

24 Q. Now, another difference is, does Torrential Downpour run  
03:13 25 automatically?



1 A. Yes. We've learned -- well, automatically. Presumably a  
2 user launches it initially. So it's maybe not fully automated.  
3 But once it's on, it just sits and runs. It runs around the  
4 clock, unattended.

03:13 5 Q. And do we know how that actually is carried out or what  
6 means are used to do that, or is that something, again, that you  
7 don't know?

8 A. I mean, I presume, without firsthand knowledge, that it just  
9 sits in a lab somewhere and runs. It gets set up and launched  
03:14 10 like any other process and it's left running and then people  
11 check on it from time to time to see what it's found.

12 Q. Okay. Does Torrential Downpour also generate special data  
13 logs?

14 A. Yes, it does.

03:14 15 Q. Now, how would we judge the reliability of those logs that's  
16 generated by the same program that we don't have access to?

17 A. I -- well, without access I have no objective way of judging  
18 the accuracy of the logs.

19 So, for example, I've seen log files and they  
03:15 20 oftentimes will describe events that can be verified via other  
21 means; for example, in the context of a criminal case.

22 But what we don't know -- there's sort of confirmation  
23 bias here. What we don't know is how many log files are  
24 generated that don't result in prosecutions, or how many  
03:15 25 warrants are executed that don't result -- based on those log

1 files that don't result in prosecutions. We don't have access  
2 to that information so there's -- we don't have a way of  
3 evaluating whether the system is accurate in general or not.

03:16 4 Q. Does this kind of maybe implicate that you'd have a false  
5 positive? Is there -- can you describe what a false positive  
6 might be in computer --

7 A. Sure. In testing -- in general, any time you have a test to  
8 look for a condition, there are two kinds of errors that you are  
9 worried about. One is a false positive result. In other words,  
03:16 10 the system, whatever it may be, falsely reports the condition  
11 exists. The other one is a false negative. The condition  
12 falsely reports -- or, I'm sorry, the test falsely reports that  
13 the condition does not exist.

14 And these are things which are tracked very carefully.  
03:17 15 For example, in medical testing, you know, you have a test which  
16 is 99 percent accurate for finding this kind of cancer. What  
17 they mean is there's 1 percent that they're getting either false  
18 positives or false negatives and, you know, giving a  
19 misdiagnosis potentially on that basis.

03:18 20 So here as well we know of times when the system has  
21 given positive alerts, but we only know the ones that resulted  
22 in prosecutions. So we don't know the false-positive rate or  
23 the false-negative rate of Torrential Downpour.

24 Q. And the logs themselves again don't shed any light on that,  
03:18 25 correct?

1 A. Right. They -- they report what the software reported.  
2 They're a record of what the software reported.

3 And there's -- the logs themselves, you know, purport  
4 to be accurate records of events that the software engaged in,  
03:22 5 but we have no way -- or at least I have no way of verifying  
6 their accuracy.

7 Other than, I will say, from time to time there are  
8 events in a log that can actually be correlated with records of  
9 events elsewhere or other sources of information.

03:22 10 Q. Well, let's talk about this case. So, for example, one way  
11 that this supposed single-source download could have been  
12 verified was that the image that the program said it downloaded  
13 was found later on Mr. Owens' computer, correct?

14 A. Correct.

03:23 15 Q. And in this case did that happen?

16 A. There was -- to my recollection there was an image that the  
17 Torrential Downpour reported a single source download of and  
18 that image was not found on any of the media seized.

19 Q. Is another difference between Torrential Downpour and the  
03:24 20 public version of the program is that Torrential Downpour can  
21 get information from target computers like, for example, the  
22 version that's being run of the program?

23 A. Torrential Downpour is a BitTorrent client in the sense that  
24 it speaks the BitTorrent protocol, but it's really a  
03:24 25 surveillance tool. It's designed for gathering information to

1 be used in prosecution, and so it makes records of all kinds of  
2 information that would be of no interest to the average  
3 BitTorrent user: IP addresses, software versions, segments of  
4 files and so forth.

03:25 5 All of that information is used to a greater or lesser  
6 extent by a BitTorrent client, but it's not exposed to the user.  
7 The user has no knowledge of it. The user just says, "ah, my  
8 file got here" and is happy with that.

9 So that's -- that's a difference between Torrential  
03:25 10 Downpour and other BitTorrent software, is that the other  
11 BitTorrent software is designed for transferring files,  
12 Torrential Downpour is designed for supporting interdiction.

13 Q. Okay. Is there any other I guess major differences you're  
14 aware of that Torrential Downpour might have that the public  
03:25 15 program doesn't?

16 A. I don't believe it's an issue in this case, but I have from  
17 time to time in warrant applications seen statements to the  
18 effect that Torrential Downpour is capable of tagging a target  
19 system.

03:30 20 So one of the other problems that can happen is in say  
21 a home network there might be multiple devices, tablets, phones,  
22 computers, these days thermostats, alarm systems, et cetera,  
23 that all use the internet for communications. And so one of the  
24 problems is, well, how do we know which of these devices was the  
03:31 25 one that was on the BitTorrent network?

1           And so presumably this involves the placement in a log  
2 file somewhere of some piece of information that would be  
3 uniquely identifying the system as this is the one to which law  
4 enforcement connected. But I'm not aware of that being in play  
03:31 5 in this case.

6 Q. Would a tag, if it was placed on a target computer, possibly  
7 be in a nonshared portion of the target computer?

8 A. It would possibly be there, yes. I don't know the exact  
9 mechanism of tagging. But like I said, I assume it's probably  
03:31 10 in a log file somewhere.

11 Q. And again, without access to the program it's impossible to  
12 say.

13 A. A tag might be discernible, but, yes, it would be much  
14 easier to figure it out if we had access to the program.

03:32 15 Q. Okay. Okay. So, now, in this case you were hired by me,  
16 correct?

17 A. Correct.

18 Q. And you reviewed all the digital evidence that was made  
19 available by law enforcement.

03:32 20 A. Yes.

21 Q. And so did that include a mirror-image of the computer hard  
22 drive --

23 A. Yes.

24 Q. -- that was seized from the search warrant?

03:32 25 A. It did.

1 Q. And also was there several thumb drives?

2 A. Yes.

3 Q. Okay. And again, you also reviewed I think you said the  
4 pleadings, like the indictment?

03:33 5 A. Yes.

6 Q. And also the police reports.

7 A. Yes.

8 Q. And the search warrant, correct?

9 A. Yes.

03:33 10 Q. Okay. Now, after you reviewed all of this material did you  
11 have several questions that caused you concern?

12 A. One that I recall was that at least some of the single  
13 source downloads seemed to happen quite quickly. It's not rare  
14 to see single source downloads or logs of single source  
03:34 15 downloads -- I've never seen the single source download  
16 itself -- but Torrential Downpour logs that describe single  
17 downloads that take hours, or even maybe span more than a day.

18 Here at least some of them -- and I don't recall the  
19 exact timeframes without refreshing my recollection, but some of  
03:36 20 them were quite quick, on the order of less than a minute or  
21 maybe even seconds.

22 Q. And why would that be unusual?

23 A. Well, again, the nature of the single source download is  
24 that because you're downloading from a single source, you are  
03:39 25 subject to whatever the upstream bandwidth limitations of that

1 source are. So that's why it sometimes takes a while to get  
2 files, because you're pulling it from a system that's only  
3 uploading very efficiently. It's maybe not the only consumer of  
4 that upstream bandwidth and, in any case, it's limited by that  
03:40 5 pipe size.

6 Q. Was another one of your concerns about what the search  
7 warrant meant when it said that law enforcement's investigative  
8 focus was directed to Mr. Owens' IP address?

9 A. Right. So search warrant applications derived from  
03:40 10 Torrential Downpour information are generally worded pretty  
11 obliquely, I assume in order to avoid divulging sensitive  
12 information about the software.

13 So I don't have any idea what it means to turn one's  
14 investigative focus, what actions that implies. I mean,  
03:42 15 presumably at any point in an investigation one's focus is  
16 somewhere, but I don't know what it means to turn one's  
17 investigative focus towards a certain IP address. I mean,  
18 obviously it means I've seen an alert and so I'm taking an  
19 interest in the IP address, but I don't know what actions the  
03:42 20 investigator takes.

21 I also don't know concretely, you know, in technical  
22 terms what it means to be associated with a certain hash value.  
23 That would be another -- you know, we just don't know precisely  
24 what it is that Torrential Downpour is basing its alerts on. We  
03:43 25 know the kind of stuff it is, but not exactly what.

1 Q. And, again, to be clear, this could have been the program by  
2 itself running automated that, you know, focused its  
3 investigation or, you know, thought that this target computer  
4 was associated with a torrent, not necessarily a person sitting  
03:43 5 there looking over it, correct?

6 A. Yeah. Based on what I have read in this case and in others,  
7 I think it's rare for someone to just sit there watching  
8 Torrential Downpour. What happens is they get a bunch of --  
9 they come back in the morning, probably see a bunch of log files  
03:44 10 and then start digging on those.

11 Q. So in a sense, as far as the actual transactions that occur  
12 between Torrential Downpour and the remote client or the target  
13 computer, would it be fair to say that really the program's the  
14 only witness to what happened at that point.

03:44 15 A. Yeah, I think that's a good analogy. The process of  
16 identifying IP addresses in the language of the warrant  
17 associated with a piece of contraband and conducting the single  
18 source download is probably entirely automated and, you know,  
19 was done unattended by a human.

03:45 20 Q. Could the term "associated with a torrent" just means that  
21 the target computer says, hey, I have this torrent or this map  
22 to a file and not necessarily the file itself?

23 A. I assume it means either I have it or I want it, and I don't  
24 know for sure which.

03:46 25 Q. But, again, could it be that it doesn't necessarily have the



1 file; it's just saying that it has the information or the  
2 request for the file?

3 A. Oh, certainly. It might even be a false statement.

4 It's possible to imagine that someone, for example,  
03:46 5 Torrential Downpour might untruthfully advertise what they have.

6 Q. Okay. Did you also have concerns when the search warrant  
7 said that Mr. Owens' computer connected to law enforcement's  
8 computer and what that might mean?

9 A. Yeah, I would be curious to know exactly what that means and  
03:47 10 what caused it to do so.

11 Q. Okay.

12 MR. DONOVAN: And, Judge, I'm getting towards the end  
13 of my questions for Mr. Engel.

14 BY MR. DONOVAN:

03:47 15 Q. So I guess I'd like to kinda conclude with, you know, why  
16 you feel you need access to Torrential Downpour to answer all  
17 these questions or to answer some of these concerns in the case.

18 So would it be fair to say that you need access to the  
19 program to confirm whether Torrential Downpour actually  
03:49 20 conducted a single source download the way that it says it does?

21 A. Right. I don't think -- I mean, the time of that particular  
22 single source download has come and gone. But I don't have any  
23 way to verify how reliably Torrential Downpour conducts single  
24 source downloads. So that would be one of the things that I  
03:49 25 would want to observe is sort of, in a controlled environment,

1 does it reliably get all of a file from a single source when it  
2 reports that it's doing so.

3 Q. And this would be important because whether or not the  
4 entire file came from Mr. Owens' computer versus from multiple  
03:50 5 computers, would obviously bear on his intent or his knowledge  
6 of what occurred, correct?

7 A. I don't know so much knowledge as just actual possession.  
8 If someone has a piece of a file, that's different from having  
9 the whole file.

03:50 10 Q. And, again, that's, again, also maybe different from having  
11 just the torrent for the file.

12 A. Correct.

13 Q. Okay. Because, again, normal peer-to-peer protocol would be  
14 a download from multiple sources, not just one. So that would  
03:51 15 be pretty crucial to try to figure out.

16 A. Right. So presumably the authors of Torrential Downpour  
17 overrode that default behavior of the BitTorrent software. And  
18 the question is, did they do a perfect job of that or not.

19 Q. Okay. Are you also interested in knowing what network  
03:51 20 traffic is monitored to identify potential target computers?

21 A. Yes. I would be interested to know the specific sorts of  
22 messages that Torrential Downpour inspects.

23 We know that it discriminates between network messages  
24 that involve hash values that are related to contraband. In  
03:52 25 order to do that, it's gotta be looking at the pool of messages

1 in general and then it alerts on the ones that are presumably --  
2 their hash values are in a database of known bad files.

3 But, so it's -- effectively it's looking at all of the  
4 traffic and then discriminating. It's only alerting on some of  
03:52 5 it.

6 Q. So correct me if I'm wrong, but it sounds like it could be  
7 doing like a dragnet search of all traffic across a peer-to-peer  
8 network, at least in maybe a certain geographic area, to then  
9 narrow down to what it thinks is contraband images or videos?

03:53 10 A. Right. In order to discriminate between contraband and  
11 noncontraband, it has to get all of the messages. It doesn't  
12 see all of the BitTorrent traffic in the entire world, but it  
13 certainly sees whatever is in its neighborhood and what it --  
14 you know, whatever its peers are interacting with. And it then  
03:53 15 sifts through that to look for ones that are, you know,  
16 potentially bad.

17 Q. And this could maybe be important, for example, for raising  
18 Fourth Amendment concerns?

19 A. Well, one interesting question is, okay, there's this  
03:54 20 database of -- of known hash values. How do things get --  
21 what's the process for adding things to that database? How  
22 rigorously are they vetted? Is the database --

23 I mean, it's also easily possible to imagine this  
24 database being used for discovering things other than child  
03:57 25 pornography. You could use it to look for hashes that are

1 associated with, say, recipes for bombs or things like that.  
2 It's not just a -- it's a Swiss army knife tool in the right  
3 hands.

4 And so, I mean, I'm not a criminal law practitioner so  
03:57 5 I'll leave the Fourth Amendment arguing to you, but, yes, it  
6 seems to me that this is -- the fact that it looks at both  
7 legitimate and non-legitimate traffic in order to figure out  
8 what the non-legitimate traffic is, you know, that is -- that  
9 seems invasive to me. But, again, I'm -- that's not the part  
03:58 10 I'm an expert on.

11 Q. Now, you also want to -- and we've talked about this a  
12 little bit already with the false positives, but you want to be  
13 able to have access to the program to test its accuracy and  
14 reliability in how it carries out its methods, correct?

03:58 15 A. Correct.

16 Q. All right. And this would be important because every  
17 software program has certain parameters and instructions that  
18 should be followed to make sure it's being used correctly.

19 A. Right. So the analogy I would make here is to say a radar  
03:58 20 gun or a breathalyzer. These are tools that are used to  
21 establish probable cause to charge people with crimes or at  
22 least ordinance violations. And, but we know that they have to  
23 be calibrated a certain way and they have to be used correctly.  
24 And so defense attorneys routinely verify that that has been  
03:59 25 done. You know, it is a defense in many cases if the equipment

1 was not operated correctly.

2 And we have no way of knowing what questions to even  
3 ask here, because we don't know how the software is set up, how  
4 the software is installed, what the correct way of operating the  
04:00 5 software is. Those are all things that are opaque to us. And  
6 so we don't have any way of evaluating or even properly  
7 questioning a prosecution witness about whether that took place  
8 in this case or not.

9 Q. Could you just describe briefly for the Court, if you were  
04:00 10 able to get access to the program, like what are some of the  
11 things that you might try to do or try to -- you know, what kind  
12 of tests might you run?

13 A. Well, one of them would be just what's called packet  
14 capturing or packet sniffing. I would attempt to watch from a  
04:00 15 nearby place on the network a single source download and see if  
16 indeed it all came from a single source. Probably do that a few  
17 times just to verify that it doesn't every so often grab a piece  
18 from elsewhere.

19 I would also watch when the software generates an  
04:01 20 alert what traffic caused it to do that. That would -- those  
21 would be things that would help me understand what it's doing  
22 under the hood. And that's kind of the goal here.

23 Q. Now, would it matter where you did this testing or review,  
24 whether it was at, you know, your own facility, your office  
04:01 25 versus perhaps in a law enforcement office?

1 A. I have no, you know -- it would be more convenient at my  
2 office, but I have no, you know, principled objection to doing  
3 it elsewhere.

4 I would say that if it were at another facility, I'd  
04:01 5 probably want to schedule more than one visit because I assume I  
6 would spend a fair amount of time getting up to speed on just  
7 what -- how I would do the tests there. You know, what's  
8 available to me in terms of network ports or, you know, power  
9 outlets, you know, sort of mundane things like that. Also, just  
04:02 10 learning how to -- I've never seen the software. I don't know  
11 what it looks like. I don't know the first thing about how to  
12 launch it or do anything like that. So I'd need a little time  
13 to just get oriented, and then I'd also need time to do the  
14 tests.

04:02 15 So doing it at my leisure at my own facility would  
16 make that easier, but it's not impossible to do it elsewhere.  
17 I'd just need the requisite degree of access.

18 Q. Now, would you view it as a problem if this was done  
19 pursuant to a protective order where you can't disseminate or  
04:02 20 discuss or otherwise disclose the program to anybody else except  
21 for me?

22 A. No, I believe we've even proposed that.

23 Q. So you would obviously -- I mean, you're a practicing lawyer  
24 in Wisconsin, correct?

04:03 25 A. I am.

1 Q. You value your law license. You wouldn't do anything to  
2 violate an order, right?

3 A. I'd do my best to avoid that.

04:03 4 Q. Okay. Another reason that you might want access to the  
5 program would be, again, to ensure that it -- when it identifies  
6 a computer as flagged for possessing a torrent, okay? That that  
7 is maybe different than an actual child pornography image or  
8 video, right?

04:03 9 A. Right. Now, this would be probably a dicey thing to test,  
10 since I don't possess any child pornography and have no  
11 intention of doing so, so we'd probably have to set up some way  
12 of having a known, you know, safe file, you know, some dummy  
13 file that we could pretend was something, you know, that  
14 Torrential Downpour would alert on. So we'd want to see when  
04:04 15 that file gets shared what is it that triggers Torrential  
16 Downpour to alert and do the log entries that it creates  
17 accurately reflect the condition that was present on the  
18 network.

04:04 19 Q. You mentioned earlier, but I just want to maybe clarify this  
20 a little bit more. So it's virtually impossible for us as the  
21 defense to prepare any sort of cross-examination of government  
22 witnesses about how this program is used or whether it was used  
23 correctly or within the right parameters, right?

04:04 24 A. The best we have right now is what's in warrant applications  
25 and then a few inferences we can draw from there.

1           There's a little bit of literature, you know,  
2 presentations that one can download, but there's really not  
3 much -- we don't have access to documentation about the system.  
4 We certainly don't have the source code. No one outside of law  
04:05 5 enforcement to my knowledge has seen a working copy of the  
6 software.

7           We get conceptually what it is, and we understand that  
8 a system could be built to do what it claims it does, we just  
9 have no way of verifying it. And that makes it hard to know  
04:05 10 what questions to ask, again, about whether the system was  
11 properly installed, was it properly operated, what network  
12 environment does it require in order to function correctly, did  
13 it have that at the time. These are all questions we don't --  
14 since we don't know information about the guts of the system, we  
04:05 15 don't know what questions to ask. And we could ask a question,  
16 but we wouldn't know whether the answer was helpful or not.

17 Q. So would it be fair to say that your opinion is we are  
18 basically at the mercy of the government right now of what they  
19 say it does and doesn't do without independently verifying it?

04:05 20 A. Very much so. The -- we have nothing -- we just are -- we  
21 either take on faith what's in the warrant application or we  
22 don't.

23 Q. And so there's really been no -- again, as far as you're  
24 aware, and this is anywhere in the country -- any adversarial  
04:06 25 testing of this program.



1 A. I am not aware of any. There are a couple of competitors to  
2 Torrential Downpour also which are closely guarded. I'm aware  
3 of efforts in various courtrooms to get varying degrees of  
4 access to Torrential Downpour and other systems. I'm unaware of  
04:07 5 someone getting unrestricted access to do just sort of thorough  
6 testing.

7 Q. And lastly, would it be important to gain access to the  
8 program so that we can perhaps try to figure out why the file  
9 that the program said it downloaded twice over the course of two  
04:07 10 different days is not located on Mr. Owens' computer?

11 A. Well, what we could do -- I mean, we know that the program  
12 said it downloaded those things, and we know that the file was  
13 not present at the time when the computer was seized. We can  
14 think of a variety of explanations for why that might be the  
04:08 15 case. Inspecting the software would help us evaluate sort of  
16 which inferences are more plausible versus less plausible.

17 MR. DONOVAN: Your Honor, I believe I'm done. If I  
18 could just check my notes for a quick minute here to see if I  
19 missed anything.

04:08 20 (Brief pause.)

21 MR. DONOVAN: Your Honor, I have no further questions.

22 THE COURT: Okay. Mr. Humble?

23 CROSS-EXAMINATION

24 BY MR. HUMBLE:

04:12 25 Q. Mr. Engel, you mentioned your background and training. Have

1 you had any or received any training in BitTorrent file sharing  
2 for the networks?

3 A. Other than experiential testing, no.

4 Q. Okay. And you also mentioned that it sounds like what you  
04:13 5 learned you learned from reading the literature and also doing?

6 A. Yes. For better or worse, people of my vintage typically  
7 the courses weren't available at the time when we needed to  
8 learn things, so we had to just go do it.

9 Q. Okay. And you mentioned that some of the literature upon  
04:13 10 which you relied to teach yourself was authored by this  
11 gentleman sitting next to me; is that correct?

12 A. Yes. You have next to you one of the probably half dozen  
13 people in the world who knows most about the software.

14 Q. Okay. So if he helped teach you about what you know about  
04:14 15 BitTorrent, do you have reason to trust his -- distrust his  
16 expertise in this area with regard to BitTorrent Torrential  
17 Downpour or Torrential Downpour Receptor?

18 A. Curious question. I don't distrust him. No, I have no  
19 reason to distrust him. I mean, I don't think he's trying to  
04:14 20 fool anybody. I just don't have any objective way of verifying  
21 any of the facts in this case.

22 Q. But, again, what you've learned about this essentially, at  
23 least in part, you've learned from this gentleman. So you would  
24 rely on his expertise in what you're testifying to here today  
04:14 25 essentially.

1 A. In part, yes.

2 Q. And you referred to this in your -- in your affidavit as  
3 "RoundUp" and you clarified "Torrential Downpour." It's  
4 actually Torrential Downpour Receptor, were you aware of that?

04:15 5 A. I'm aware of that term as well.

6 Q. Can you tell the Court the difference between Torrential  
7 Downpour and Torrential Downpour Receptor?

8 A. Not with specificity I cannot.

9 Q. Okay. And when you had the opportunity to review the logs  
04:15 10 and the imaging of the computer, you said that you never found  
11 this image that is alleged in the indictment; is that correct?

12 A. That image as far as I could tell was not present on the  
13 computer.

14 Q. And I said "image" and earlier you said "image," but  
04:15 15 actually, more correctly, it's a movie.

16 A. Yes. Yes.

17 Q. Okay. So you didn't find this movie, but you did review the  
18 logs, correct?

19 A. Yes.

04:15 20 Q. And those logs did reflect that I believe there were 226  
21 portions that made up the movie for lack -- I say "portions" for  
22 lack of a better term?

23 A. I'm taking your word for the number 226. But, yes, the  
24 movie was reflected in the logs.

04:17 25 Q. And this will probably be an exhibit soon, but this log

1 essentially shows all 226 portions of that movie are going into  
2 the computer of Mr. Owens; is that correct?

3 A. That log is a document that speaks for itself. I don't have  
4 a way of assessing its accuracy, but it has entries that appear  
04:17 5 to be what you describe.

6 Q. Do you have a way of proving inaccuracies in the log?

7 A. No.

8 Q. Okay. With regard to your review of the logs and the mirror  
9 imaging of Mr. Owens's computer, did you find evidence that that  
04:17 10 movie had been on Mr. Owens's computer?

11 A. I saw an indication that it may have been there, yes.

12 Q. And did you find indications that that particular movie with  
13 that particular hash value may have actually been on Mr. Owens's  
14 computer at different times throughout 2018, 2016, 2017?

04:18 15 A. I don't believe -- or at least I don't recall, sitting here  
16 today, seeing anything that gave me a sense of the time at which  
17 it may or may not have been there. I did find a reference to  
18 the file name, but that's all I recall finding.

19 Q. Okay. And in looking at, again, the evidence, the computer,  
04:18 20 the forensic evidence, were you able to establish essentially  
21 any evidence -- or did you observe any evidence that the file  
22 had been there prior to Mr. Owens's computer connecting with law  
23 enforcement?

24 A. Again, I don't recall what I saw being associated with a  
04:19 25 time. So I'm not -- one can always imagine a forensic analyst

1 smarter than oneself, so I'm not saying that there was  
2 definitively no such evidence. I just -- what I recall was  
3 seeing a reference to the file name and I did not recall that  
4 having any kind of timestamp on it.

04:19 5 Q. And in reviewing that information did you -- well, I'll just  
6 ask you: Do you know what program Mr. Owens used to establish  
7 peer-to-peer communication?

8 A. It's in my notes, but I don't recall if it was Micro-Torrent  
9 or what.

04:22 10 Q. Okay. And did you see any evidence when you were reviewing  
11 the forensic materials that Mr. Owens had downloaded a  
12 peer-to-peer program very close in time to when he connected  
13 with law enforcement?

14 A. There was peer-to-peer software installed. That would have  
04:22 15 had a timestamp on it. I don't recall sitting here right now  
16 the proximity. I could refresh my recollection and I would -- I  
17 don't -- I don't have any reason to dispute it.

18 Q. Do you recall in reviewing that information that that  
19 particular movie with its 226 portions was -- that there was  
04:23 20 evidence that it was on Mr. Owens's computer after he  
21 established contact with law enforcement?

22 A. Again, the evidence I saw for the existence of that file, I  
23 don't recall any time data associated with it. So, no, I don't.  
24 All I saw was the file name.

04:23 25 Q. Well, let me ask you this. If -- if there was evidence that

1 this particular movie was on Mr. Owens's computer prior to  
2 connecting with law enforcement, and there was -- and I'm just  
3 asking you to go with the question -- and there was evidence  
4 that this particular movie was on Mr. Owens's computer after  
04:23 5 connecting with law enforcement, would that be pretty good  
6 evidence that that particular movie had been on Mr. Owens's  
7 computer?

8 A. If there was -- if there was evidence that the file was  
9 present before connecting with law enforcement and evidence that  
04:23 10 the file was connected -- was present after connecting to law  
11 enforcement, would I infer that the file was present?

12 Q. Yes.

13 A. Yes. If the file was present it was present.

14 Q. So people can delete files, correct?

04:24 15 A. Correct.

16 Q. And you've been on other child pornography cases. You've  
17 testified you've done the research, looked at the forensics,  
18 correct?

19 A. Yes.

04:24 20 Q. Have you seen other instances where individuals who have  
21 contraband or child pornography have deleted the images after  
22 viewing them?

23 A. I have seen instances --

24 Well, let me answer it -- a two-part answer to that.

04:24 25 The short answer is, of course, people delete files from time to

1 time. And sometimes you'll find traces of files in unallocated  
2 space and those are presumably deleted files.

3 I am also aware of times when, as here, in the warrant  
4 application there's a report of a single source download of a  
04:25 5 file and we don't find it present on the target system when we  
6 go to analyze it. I don't know why that is. Deletion is one  
7 possible explanation, but another one would be a false positive.

8 Q. This is going to come across very crude, because it is  
9 crude, but it's a term that you may be familiar with and I'm  
04:25 10 going to ask you: Have you -- are you familiar with the term  
11 "pump and dump"?

12 A. No, I'm not.

13 Q. Not with regard to child pornography or the downloading of  
14 child pornography?

04:25 15 A. That is -- that's not one I've encountered.

16 Q. Okay. In reviewing the forensic evidence here in this  
17 particular case, was there a question in your mind that it was  
18 Mr. Owens's computer who initiated contact with law enforcement?

19 A. I don't know of a way from the forensic image to determine  
04:26 20 that. So it wasn't a question I particularly investigated  
21 because I had no idea how to investigate it.

22 So I -- I'm not sure what would cause a computer to  
23 connect to a law enforcement computer just in the abstract. So  
24 in that sense I wonder about it, but it was not something that I  
04:26 25 investigated.

1 Q. Are you familiar with the term "seeding"?

2 A. Yes.

3 Q. Could you describe for the Court what seeding is?

4 A. In broad terms it's advertising the presence of files so  
04:27 5 that you can -- you're participating in the network and people  
6 know that you've got either whole files or at least segments of  
7 files that others might want.

8 Q. And seeding essentially -- well, sometimes, if not most  
9 times, seeding is done by someone who already possesses an image  
04:27 10 or a movie; isn't that correct?

11 A. My understanding -- yes. Yes, that's correct.

12 THE COURT: This is s-e-e-d-i-n-g?

13 MR. HUMBLE: Yes. Seeding as in -- S, yeah.

14 THE COURT: As in lawn seed.

04:27 15 MR. HUMBLE: Yes, correct.

16 BY MR. HUMBLE:

17 Q. So that seems counterintuitive. If someone already has the  
18 movie, why are they offering it out to the world?

19 A. That's sort of the economic principle that's central to  
04:27 20 BitTorrent. What one downloads one ought to offer for sharing.  
21 And that's sort of how the BitTorrent network maintains itself  
22 as an efficient distributor of files.

23 Q. So essentially that almost certainly is why the term is  
24 called seeding. So you just keep distributing and distributing  
04:28 25 and distributing because you're hoping it's going to come back



1 to you.

2 A. Not the same file, but --

3 Q. Not the same file, correct.

4 A. Yes.

04:28 5 Q. Same genre.

6 A. Well, genre even -- I think it's just bandwidth. I don't  
7 know that it discriminates by subject matter so much as just if  
8 you're not offering things, then you're kind of a jerk user of  
9 the system and you shouldn't get the benefit of it.

04:28 10 Q. Okay. And what is swarming?

11 A. Swarming is another feature of -- I think it was first in  
12 Gnutella. It's a way of boosting the performance of downloads  
13 of certain files. I'm afraid, sitting here right now, I can't  
14 go into much more detail than that. I don't recall exactly how  
04:29 15 swarming works on BitTorrent.

16 MR. HUMBLE: I don't have any further questions,  
17 Your Honor.

18 THE COURT: Mr. Donovan?

19 MR. DONOVAN: Just a couple follow-up, Your Honor.

04:29 20 REDIRECT EXAMINATION

21 BY MR. DONOVAN:

22 Q. So, Mr. Humble asked you about how part of your knowledge  
23 and expertise of BitTorrent is based on the government's  
24 witness, correct?

04:29 25 A. Or documents authored by him. I've never met him before

1 today.

2 Q. Correct, I'm sorry. To be more precise, documents authored  
3 by him.

4 A. Yes.

04:29 5 Q. And again, I just wanted to clarify, there is no independent  
6 access to this program.

7 A. That's correct.

8 Q. And so anything that's known about this program is either  
9 what is chosen to be shared by its authors, including the  
04:30 10 government witness, or that comes out through litigation.

11 A. Yes.

12 Q. Like, for example, in case decisions or, you know, opinions  
13 and orders, things like that.

14 A. Yes. And one can glean tidbits here and there from things  
04:30 15 like warrant applications.

16 Q. So I guess my question -- you might be -- you know, where  
17 else could you go to learn about this? Other than perhaps  
18 publications by the government witness.

19 A. If I knew of another place I'd go there.

04:30 20 Q. Okay. The government asked you questions about whether you  
21 have any reason to doubt that the logs are inaccurate. Okay?

22 Again, why can't you assess the logs separate from the  
23 program?

24 A. Well, the log is just a text file. Sitting at my computer  
04:31 25 with a Notepad application, I can make a text file that says

1 darned near anything. I don't think the government is  
2 generating false text files. That's not -- I'm not that much of  
3 a conspiracy theorist. But it seems to me antithetical to the  
4 idea of criminal defense that we should just take it at face  
04:31 5 value. It seems that we should be able to do some investigation  
6 of the degree to which it accurately reflects the events that  
7 it's reported.

8 Q. Would it be fair to say that if there's problems within the  
9 program itself then there might be problems within the logs  
04:31 10 themselves?

11 A. Right. That's the old "computer garbage in/garbage out"  
12 theory. If the software does not function as designed, then  
13 there's no reason to expect that the logs would be better than  
14 the program itself.

04:32 15 Q. You testified that again you reviewed the forensic evidence  
16 available in this case personally.

17 A. Yes.

18 Q. And you found indications of perhaps the file name of the  
19 movie that was supposedly downloaded on Mr. Owens' computer.

04:32 20 A. Correct.

21 Q. But no actual file.

22 A. Correct.

23 Q. And I apologize, I forget, did you find any indications of a  
24 hash for that movie?

04:32 25 A. I did not.

1 Q. Okay. Now, part of these peer-to-peer programs would be,  
2 again, a search function where like a term could be entered,  
3 correct?

4 A. Yes.

04:32 5 Q. And so would that be part of a Torrent? So like could a  
6 search term or a function be part of a Torrent that might be on  
7 the computer? Meaning that, you know, it might say it's looking  
8 for or has information on it but, again, doesn't have the file  
9 itself?

04:33 10 A. Yes. One can find, for example, Torrent files on a  
11 computer, but not the -- not the movies or images or whatever  
12 that the torrent files would enable you to acquire.

13 Q. Okay. And so, again, you said one explanation could be, as  
14 you acknowledged, that the user deleted the file, right?

04:33 15 A. Yes.

16 Q. But another explanation could be, again, this idea of a  
17 false positive that perhaps Torrential Downpour reporting a  
18 single source download was just wrong; that there -- you know,  
19 it reports a download, but there never was a file there to  
04:34 20 download from.

21 A. Correct.

22 Q. Okay.

23 MR. DONOVAN: I don't have any other questions,  
24 Your Honor.

04:34 25 THE COURT: Okay. Thank you, Mr. Engel. You can step

1 down.

2 (Witness excused at 2:44 p.m.)

3 THE COURT: How about a short break. Do you have -- I  
4 mean, are we in a rush because a witness has to catch something  
04:34 5 or get out of here or --

6 MR. ERDELY: 6:45.

7 MR. HUMBLE: We've got some time, Your Honor.

8 THE COURT: 6:45?

9 MR. HUMBLE: It's Green Bay, we can get him over  
04:34 10 there.

11 THE COURT: 20 minutes.

12 (Recess taken at 2:45 p.m., until 2:58 p.m.)

13 THE CLERK: Please raise your right hand.

14 Do you solemnly swear the testimony you are about to  
07:17 15 give is the truth, the whole truth and nothing but the truth so  
16 help you God?

17 THE WITNESS: I do.

18 THE COURT: Please state and spell your first and last  
19 name for the record.

07:17 20 THE WITNESS: Robert Erdely, E-r-d-e-l-y.

21 THE COURT: Thank you, Mr. Erdely.

22 Go ahead, Mr. Humble, you may proceed.

23 MR. HUMBLE: Thank you. May I approach the witness,  
24 Your Honor?

07:18 25 THE COURT: You may.

1 ROBERT ERDELY, GOVERNMENT WITNESS, DULY SWORN

2 DIRECT EXAMINATION

3 BY MR. HUMBLE:

4 Q. Mr. Erdely, I'm just going to hand you what's been marked as  
07:18 5 Exhibit 1, can you just tell me what that is?

6 A. It's a copy of my CV.

7 (TRANSCRIBER NOTE: Mr. Humble not near a microphone.)

8 Q. [Indiscernible]?

9 A. I did.

07:19 10 MR. HUMBLE: [Indiscernible].

11 MR. DONOVAN: No objection.

12 THE COURT: 1 is received.

13 (Exhibit 1 received in evidence.)

14 BY MR. HUMBLE:

07:19 15 Q. If you could go ahead and just inform the Court, what is  
16 your background, who is your employer, how long have you been  
17 employed, that kind of thing?

18 A. I worked for the Pennsylvania State Police until I retired  
19 in 2012. The last five years of that career I supervised the  
07:20 20 Computer Crime Unit. And it was during my time with Computer  
21 Crime Unit that I worked on the development of these tools with  
22 the University.

23 And, April 2012 I retired and the very next day I  
24 started with the Indiana County Detectives Bureau where I kept  
07:20 25 the same role - computer crime investigations, which is both the

1 investigative piece and the forensic analysis piece.

2 So as part of that and my time with Computer Crime  
3 Unit, I went through various trainings, conferences and such  
4 where I was able to acquire professional certifications. For  
07:21 5 instance, the CISSP certification the defense expert was  
6 speaking of, I obtained that.

7 I'm a Microsoft certified systems engineer, a Cisco  
8 certified networking professional.

9 I went through the certification process for four --  
07:25 10 four different certification processes for computer forensics.  
11 And, again, just the ongoing training day to day.

12 As it relates to peer-to-peer, much of my training  
13 came from the University, the researchers, the professors and  
14 Ph.D.'s that did the research into the network so I could learn  
07:26 15 exactly how it operates.

16 Q. Okay. Just total, how many years have you been dealing in  
17 investigating computer crimes?

18 A. I started with the Computer Crime Unit October 1998 to  
19 present.

07:26 20 Q. Okay. And is it fair to say that now you split your time  
21 between investigations and training and testifying?

22 A. Correct. I do trainings for the Internet Crimes Against  
23 Children Task Force, for the FBI's Violent Crimes Task Force,  
24 their international task force. I've done a training for  
07:27 25 Interpol and various different countries. I provided this

1 technology beyond the United States.

2 Q. So as you say, you've trained on BitTorrent and the  
3 investigative use of BitTorrent in other countries. How many  
4 countries use this investigative Torrential Downpour?

07:28 5 A. We last checked, over 60 countries used our investigative  
6 systems.

7 Q. And if you could just kind of describe for the judge when --  
8 in defense affidavit and probably in your resume, it references  
9 Amherst is where this particular software was developed. Sounds  
07:28 10 like you were in on the ground floor. Can you explain that to  
11 the Court?

12 A. Yes. Initially there was research done by a professor from  
13 University of Massachusetts Amherst, and a professor from  
14 Georgetown University. That was the initial discussions as to  
07:29 15 where we move next as law enforcement for investigations.

16 After that, I worked, you know, day in and day out  
17 with the senior programmer at University of Massachusetts  
18 Amherst where we did the development of the software.

19 Q. So you didn't author the software.

07:29 20 A. No. I was part -- the development team was myself and the  
21 senior programmer from UMass.

22 There's a lot of back-end work that relate to other  
23 aspects and other networks that we investigate that I programmed  
24 in that area. I'm a Microsoft data -- Certified Database  
07:29 25 Administrator, so I work with the databases and things like



1 that, as well as the actual individual testing of the software  
2 before it's deployed.

3 Q. Okay. So fair to say you're very familiar with Torrential  
4 Downpour.

07:30 5 A. Yes.

6 Q. Okay. And Torrential Downpour Receptor?

7 A. Yes, sir. Those are two separate programs. And this case  
8 relates to one, which is Torrential Downpour Receptor,  
9 specifically version 1.50.

07:30 10 Q. Okay. We've heard about the basics of BitTorrent from the  
11 defense expert. Is there anything that you want to clarify or  
12 put a little more focus on for the Court with regard to how that  
13 operates?

14 A. Just quickly a high-level -- I just want to make sure the  
07:31 15 Court has a good understanding as to how things worked.

16 BitTorrent is different as was already described. One  
17 of the major differences is that the torrent file that we've  
18 heard about is a set of instructions on how to get the actual  
19 files that they describe.

07:31 20 Well, you have to search outside websites or get them  
21 from other people. The BitTorrent software, although it gives  
22 you a mechanism to type and search as described, I just wanted  
23 to clarify the BitTorrent file sharing network doesn't have a  
24 searching component built in. When I type in the little search  
07:32 25 field in this program, which is my BitTorrent software,

1 typically what happens is a web browser just pops up and starts  
2 giving you your search results. Well, you could have skipped  
3 that whole step and just went to your web browser, opened up  
4 Google, and started searching that way.

07:32 5 So I just wanted to be clear that there is no  
6 mechanism to search by file name within the BitTorrent file  
7 sharing network. So that was a little bit different.

8 The second -- so after I get the instructions I search  
9 the internet and I find a torrent file that describes the  
07:33 10 content I'm looking for. Then you load that torrent --

11 Q. Can I just stop you there?

12 A. Yes.

13 Q. We're talking in the abstract. What might one put into this  
14 to find the type of movie or image they are looking for?

07:33 15 A. "Jurassic Park movie torrent."

16 Q. Okay.

17 A. If I just use those four key words I would be presented with  
18 lots of sites that have these instruction files, these torrent  
19 files that would enable me to download Jurassic World or any of  
07:34 20 the other new movies that are out there. But you have to start  
21 by finding these instructions outside of the BitTorrent file  
22 sharing network is my point.

23 Q. Okay. So now I found these websites, and I'm assuming the  
24 same holds for erotica or child pornography or any type of other  
07:34 25 file?

1 A. Yes, sir.

2 Q. I found this, I found what I want, how do I go about getting  
3 it with the BitTorrent?

4 A. So now what happens is you load that torrent file into your  
07:34 5 BitTorrent program. Much like if you wanted to open up a Word  
6 document. You can either double-click it and it will launch the  
7 program and load the Word file you were trying to view. Well,  
8 with BitTorrent it's similar, I can double-click the torrent  
9 file and, assuming there's an association between those two, it  
07:35 10 just opens up my BitTorrent program and starts working.

11 Or you could have it already open and choose the  
12 drop-down file, open, and you just navigate to that torrent file  
13 which are the instructions. But in either case, once the  
14 torrent file, the instruction gets loaded into the program,  
07:35 15 searching does happen. And what searching happens is, that now  
16 my computer, running a BitTorrent piece of software that has  
17 instructions loaded, it goes out to the BitTorrent network.

18 There's indexing that happens. So the BitTorrent  
19 network keeps track of who is associated with which torrent.  
07:36 20 Because if I load a torrent, I need to find other people that  
21 have some or all of that material to share with me. I just  
22 started, I have nothing to share.

23 So the BitTorrent network does that all by itself.  
24 And it's just a search for a torrent that I've now loaded into  
07:36 25 my program which is different than initially finding that

1 torrent. They are two separate things.

2 Q. So when you say it does it all by itself -- I guess that was  
3 a corny commercial where they said "set it and forget it"? I  
4 mean, is that what we're talking about? You've already told it  
07:36 5 what you want and you can just walk away and it's going to ask  
6 all of the people all over the world through the internet to  
7 give you pieces of what you want?

8 A. Correct. I load it into my program, assuming that all the  
9 [Indiscernible] are in place, it's going to learn a list of IP  
07:37 10 addresses that potentially -- that have shown this association,  
11 they've communicated on the BitTorrent network asking about the  
12 same torrent file. So they basically are matchmakers at this  
13 point. The BitTorrent network says this is the torrent you're  
14 looking for, I understand that, here's a list of 40 or 50 IP  
07:37 15 addresses that also show that association.

16 Well, at the point -- and this is very important -- at  
17 the point in time where my computer has interacted with the  
18 BitTorrent file sharing network and expressed interest in this  
19 torrent file, which is identified through caching like the Court  
07:38 20 has already heard, a very unique way to identify content.

21 So it will keep track of the fact that I asked that  
22 question. So my computer had -- my BitTorrent software, I  
23 loaded a torrent file into it, I've made an inquiry to the  
24 network, now the network knows about me. I have an association.  
07:38 25 And it could be me, Rob Erdely the law enforcement officer, or

1 any other BitTorrent user in the world.

2           So the next thing that happens is, I will start trying  
3 to connect people to get pieces of the file or files -- because  
4 it could be one file or many files described by a torrent -- and  
07:39 5 hopefully get to connect to people. And at the point in time we  
6 connect, what happens with this BitTorrent file sharing network,  
7 there's some handshaking that goes on. It's just a computer  
8 term, but basically we're just gonna have a little conversation  
9 before we start creating data. And one of the very first things  
07:39 10 that happens is, regardless of whether I initiated the  
11 connection to you or you initiated the connection to me, we  
12 first have to agree upon one thing: That we're talking about  
13 the same torrent.

14           And the torrent's identified through something called  
07:39 15 an "info hash," but very simply it's a very, very, very unique  
16 way to identify it. It's more unique than DNA is to the human  
17 body. That's how unique it is.

18           So we agree we're talking about the same torrent. And  
19 then the next thing that happens is, both computers, regardless  
07:40 20 of -- if I contacted you because I needed pieces of data, or if  
21 you contacted me because you needed pieces of data, in either  
22 case both sides are required to report, "These are the pieces I  
23 have to share," and the other side says, "These are the pieces I  
24 have to share."

07:40 25           Because BitTorrent is built on the premise it's a

1 tit-for-tat exchange. You're supposed to be able to give pieces  
2 of data to a person that is connected to you to download data,  
3 as well as receive. You're supposed to give and get, all  
4 through the same connection. And it's an automatic thing that  
07:41 5 happens.

6 Q. Let me ask -- let me stop you there. Sorry.

7 Do I always need to go to 50 or 100 different people  
8 to get little pieces? Can I not just get the Jurassic Park  
9 movie I want from one person?

07:41 10 A. You could and do at times on the BitTorrent network using  
11 any software, not law enforcement, nothing specific. The  
12 network allows for the entire content to be downloaded from a  
13 single IP address.

14 But, it is true that you will speed up your download  
07:42 15 times if you reach out to two, three, four, 10 or 20 different  
16 computers, because all of them could be giving you data at the  
17 same time.

18 But, just to put it in perspective, if I'm -- if I  
19 load a torrent into my BitTorrent program and I'm seeking to  
07:42 20 download that material and there's only one person online that  
21 has it available at that moment in time, then the entire  
22 download happens from a single sharing computer. It's nothing  
23 unique to law enforcement software that downloads happen from a  
24 single sharing client.

07:43 25 Additionally, if you think about the person that had

1 to create this collection of data to share, no one else in the  
2 world has it. I'm creating this unique collection of files. So  
3 there's a process within your BitTorrent software to create that  
4 instruction file, that torrent file. So when I start sharing  
07:43 5 that torrent file out and people want to start downloading it,  
6 there's only one person in the world that has that collection of  
7 files, me, the creator, until I start sharing it out.

8 So my point is, the fact that law enforcement does a  
9 download from a single sharing IP address is not unique to law  
07:44 10 enforcement. It happens naturally on the BitTorrent file share  
11 network on a daily basis. So....

12 Q. So is that the conclusion of your overview of BitTorrent?

13 A. No. So then I just learned to go a step further. There was  
14 already a definition given for seeding and I just want to make  
07:50 15 sure the Court understands exactly what seeding is.

16 So if I loaded a torrent into my BitTorrent software  
17 and I downloaded everything, now I have all the files that are  
18 described by that torrent file. I need nothing more. That's  
19 the moment in time you become a seed. If you are seeding a  
07:50 20 torrent, you're in a position where you've -- you possess it  
21 all. And you're staying online for the purpose of continuing to  
22 seed the data, like a farmer in a field throwing seeds to grow  
23 his crops. Because a torrent and its associated data will only  
24 be available assuming there's enough BitTorrent programs online  
07:50 25 around the world that have those pieces to share.

1 Well, so now that I have it all, this is the point  
2 that I'm trying to bring out, I am making myself --

3 (TRANSCRIBER NOTE: Witness moves away from microphone  
4 or microphone not functioning.)

07:51 5 -- available to anybody looking for that torrent and I  
6 will share the data for them. But it's important to understand  
7 this. I'm not just sitting here passively waiting for people to  
8 find their way through the internet to connect to my computer.

9 That certainly is one of the two possibilities.  
07:51 10 Someone loads a torrent, they want to find a down -- someone to  
11 download it from, the BitTorrent network, the index tells them  
12 about my IP address, so they connect to me. And I'll give them  
13 the pieces they request.

14 Again, I don't need anything, I have everything, so  
07:52 15 that whole tit for tat stage is gone, it's out the window. But  
16 there's another thing that happens, and a lot of people don't  
17 realize it [Indiscernible].

18 I don't just sit there as a seed on the BitTorrent  
19 network when I have everything and just sit passively waiting.  
07:53 20 No. I created the index and look for people that are still in  
21 need of some of this material I have. I'm being overly helpful.  
22 I will make outbound connections from my computer -- when I say  
23 "I," I'm talking about the BitTorrent [Indiscernible] I  
24 apologize. I'm not trying to infer that the person  
07:53 25 [Indiscernible] to make it happen. But the BitTorrent network,



1 I'm a seed, will continually query the network looking for new  
2 IP addresses that are in need of data. And I'm going to deliver  
3 it to them. I'm going to knock on the door and say, "I heard  
4 you need some of this data" and offer it up to them.

07:54 5 So it makes outbound connections to computers all  
6 around the world and it continues to share, and it didn't  
7 require that computer to reach into my BitTorrent software and  
8 make the request. I'm delivering it to you. It's home delivery  
9 so to speak.

07:55 10 Q. Okay. So when all this is happening, this happens  
11 automatically if the computer is on and connected to the  
12 internet?

13 A. Correct. As long as it's connected to the internet and it's  
14 running the BitTorrent software and until the person chooses to  
07:55 15 stop the sharing or seeding process, it would continue operating  
16 that batch.

17 Q. And the handshake, the handshake takes place mutually, for  
18 lack of a better image, outside of each computer? I mean, no  
19 one's intruding each other's computer to go ahead and do that,  
07:56 20 is it?

21 A. No, it's expected. The two computers have something called  
22 a TCP connection. It just -- think of it like a tunnel. There  
23 isn't a connection established or even a phone call. I pick up  
24 the phone and I dial your number and you have a phone, we have  
07:56 25 an established connection, I can talk to you and you can talk to

1 me. That's what happens on BitTorrent.

2 So either I connect to the computer or the computer  
3 connects to me, but at that point we have this open line of  
4 communication. And again, the first thing that's gonna happen  
07:57 5 is, we're going to agree that we both are talking about the same  
6 torrent. Because if we're not, the conversation's over. He  
7 could have stopped sharing. He could have stop [Indiscernible]  
8 seeding [Indiscernible].

9 The next thing that happens is handshake. And that's  
07:58 10 where one BitTorrent program can talk to the other BitTorrent  
11 program and tell each other: I'm running a BitTorrent program  
12 called BitComet, and I could respond I'm running a BitTorrent  
13 program called UTorrent. Those are both real clients. So  
14 that's part of the handshake.

07:58 15 It's available to any program. As a matter of fact,  
16 the off-the-shelf, so to speak, clients tell you that. Or if  
17 there's a tab that says peers and you can see their IP address,  
18 you can see the version of software that they told us that they  
19 were running. It's part of the normal everyday communication,  
07:59 20 that handshaking. It tells us what networking port they listed  
21 on, all those sorts of information.

22 Q. Okay. So Torrential Downpour Receptor, which is the program  
23 we're talking about here with regard to Mr. Owens, how does that  
24 differ from the BitTorrent -- or does it differ from the  
08:00 25 BitTorrent that you just described?

1 A. Well, it's using just the functions I just described.  
2 Obviously we're law enforcement, that's not a surprise. But the  
3 way BitTorrent -- I'm sorry, Torrential Downpour Receptor works  
4 is that it searches for torrents files, the instructions, that  
08:00 5 are known to law enforcement. And who is the person that  
6 decides whether it is something we search for or not? It's me.

7 And we learn that through the hashing of the files and  
8 comparing it to other [Indiscernible] location of files we know  
9 about, or at times I actually have to physically download the  
08:01 10 file and look at them and say that's an eight-year-old, it's a  
11 sex offense, we're going to include this on the torrents that we  
12 investigate.

13 We do not listen in -- listen or monitor or try to  
14 discern one type of traffic from another. We simply search for  
08:01 15 a torrent to learn the IP addresses of other -- others who have  
16 shown an association with that torrent, and we receive the  
17 search results relating to what IPs are present. We do not -- I  
18 don't even know how you would do that -- sit there and somehow  
19 sniff out or monitor all BitTorrent traffic. It's a  
08:02 20 decentral -- decentralized network. That would be an incredibly  
21 difficult thing to do if it's possible at all.

22 We are just doing the same messages out that any  
23 BitTorrent program would give and receiving responses back.  
24 [Indiscernible] receptors you need, because all we're doing is  
08:03 25 searching for torrents that relate to child exploitation and

1 then we sit there. We just sit. We're gonna sit and wait.

2 And because I searched for that torrent, remember, the  
3 BitTorrent file sharing network knows my IP address  
4 [Indiscernible], my law enforcement IP. And the BitTorrent  
08:03 5 network is going to tell others about me. I'm just gonna sit  
6 and wait.

7 And that's what happened in this case. The suspect  
8 computer or the user's computer, however you want to define  
9 that, loaded a torrent into their BitTorrent program. The first  
08:04 10 step happens where they inquire on the network [Indiscernible],  
11 what IPs might I connect to that also have an association with  
12 this torrent? And the suspect computer learns my law  
13 enforcement IP address and he, or she, connects to us.

14 That's analogous to the drug dealer driving his car to  
08:04 15 the police station, going to the front desk and, any police  
16 officers here want to buy crack? Because that's what happened.  
17 The suspect computer arrived to law enforcement's computer, the  
18 TCP connection happens, we both agree that we're willing to talk  
19 about the same exact precise torrent, and now both sides, the  
08:05 20 person that contacted the investigator and the investigator  
21 contacted the person who established the connection, we get to  
22 talk freely about that torrent. What pieces do you have to  
23 share, the law enforcement computer can ask the suspect  
24 computer, and vice versa.

08:06 25 So we're law enforcement, we do not share. And we

1 don't even have to lie. They ask us what pieces we have to  
2 share, we say zero. We have none. That's a completely  
3 acceptable message on the BitTorrent file sharing network. And  
4 then the sharing computer will tell us what pieces they have to  
08:06 5 share.

6 So here's what happened in this case as  
7 [Indiscernible] reading the law. The suspect computer was  
8 seeding. They had all the pieces. They didn't need anything  
9 from law enforcement. They connected to us through the overly  
08:07 10 helpful image sharing, like I previously described, and once we  
11 were connected we just started asking for the pieces of the data  
12 that the sharing client was making available. And all that gets  
13 memorialized in a log file by Torrential Downpour Receptor.

14 Q. Okay. And you've reviewed those log files prior to your  
08:07 15 testimony here today?

16 A. Yes, I have.

17 Q. And we've brought a couple with us?

18 A. Yes. The two in question that were two downloads of the  
19 same file spanning two different days.

08:08 20 Q. Okay.

21 MR. HUMBLE: May I approach, Your Honor?

22 THE COURT: You may.

23 MR. HUMBLE: And counsel has these.

24 BY MR. HUMBLE:

08:08 25 Q. Handing you what's been marked Exhibits 2 and 3, they seem

1 to be quite similar, could you explain to the Court what they  
2 are and why they're different?

3 A. Well, this is two different investigative sessions. Every  
4 investigative session -- every time we accept a connection from  
08:08 5 a person -- a person's computer, it gets compartmentalized in  
6 its own folder. It lives all by itself.

7 And on two different dates, the same IP address  
8 connected to the law enforcement computer, possessing all of the  
9 content in complete possession of this movie file, and offered  
08:09 10 to share it because that computer was, quote-unquote, seeding.

11 And that's what happened in these cases. And the  
12 reason there's two log files is because the first investigation  
13 began on May 21st, 2018. The download happened quite quickly,  
14 as the Court's already heard. And then the next day on May  
08:09 15 22nd, the early-morning hours of May 22nd, that computer still  
16 had that material to share and was still offering to share it to  
17 the world. Just fortunate for law enforcement that that  
18 computer chose to connect to law enforcement's instance of the  
19 BitTorrent piece of the file.

08:10 20 MR. HUMBLE: May I approach again, Your Honor? I'm  
21 sorry.

22 THE COURT: You may.

23 BY MR. HUMBLE:

24 Q. I'm going to hand you exact duplicates of what you have  
10:25 25 there so the Court has a copy and [Indiscernible].

1 A. Thank you.

2 Q. And obviously these are detailed logs. So I don't want you  
3 necessarily to dwell on each line, but there's highlighted  
4 portions.

10:25 5 Could you explain for the Court the significance of  
6 the highlighted sections, why you chose to highlight those and  
7 what that essentially means with regard to the program and the  
8 memorialization of the program?

9 A. Sure. And so just for the sake of being on the same log at  
10:25 10 the same time, let's just describe a download dated May 21st,  
11 2018.

12 Q. Which will be Exhibit 2.

13 A. Which is Exhibit -- I don't have -- yeah.

14 Q. You don't have that.

10:26 15 A. Okay, Exhibit 2. So if we all look at that one, then I can  
16 explain the highlighted portion.

17 So on May 20th of -- the first highlighted portion on  
18 page 1, it says, "Remote client at IP address 104.11.97.37 has  
19 connected to us."

10:26 20 Again, there's two possibilities why some BitTorrent  
21 computer would connect to us. That's either, A, he's seeking to  
22 find pieces he's yet missing, but he'd still share what he had,  
23 or he's seeding. I have it all, I want to be overly helpful,  
24 I'm going to give this data freely to anyone on the BitTorrent  
10:27 25 file share.

1           So I know that a computer is connected to me, but I'm  
2 not really sure why until we start communicating. So the second  
3 highlighted area, "info hash sent by remote client."

4           So the computer that connected to us has to tell us  
10:28 5 why are you even talking to me. Well, I'm talking to you about  
6 a very specific torrent, and that has a hash value, it's called  
7 an info hash, uniquely identifying that torrent. There can be  
8 no duplicate. It's the same -- the odds are astronomical, it's  
9 one -- it's two to the hundred and sixtieth power, or one in 1.4  
10:29 10 quindecillion, which is one with 48 trailing numbers. It's a  
11 very, very large number.

12 Q. So that number that begins 0833, that is the hash value?

13 A. That's the info hash.

14 Q. Info hash?

10:29 15 A. It's the hash of the information, the instructions unique to  
16 that torrent. And that's going to be the only payload or  
17 content it could describe is that file that it was meant to help  
18 you download.

19 Q. And that second highlighted portion appears to be occurring  
10:30 20 at essentially the same exact time as the initial connection?

21 A. Yes, it happens. We're talking about computers. It happens  
22 very, very quickly. Right.

23 Q. Okay. So what's that next highlighted portion mean?

24 A. The next thing that happens is, handshake data. And this is  
10:30 25 where the computer that is connected to us is telling us more



1 information.

2 Now, we know the torrent that they connected to us  
3 about, but in the extended handshake it's telling us things like  
4 they're listening port. So if we ever wanted to connect back to  
10:30 5 them, you need to know not only just an IP address but also a  
6 networking port. So P equals and then you see a number, that's  
7 their networking port.

8 REQQ, that stands for request Qs. It tells us how many  
9 pieces are we -- I'm sorry, how many packets are we permitted to  
10:31 10 ask for at any given moment in time. If it's included, we're  
11 supposed to abide by that value and we do. And you'll see that  
12 here in a minute.

13 It tells us the version of software they're running.  
14 This is something they offered to us in the extended handshake.  
10:32 15 It's given to any BitTorrent client, not just us.

16 And then it actually tells us our IP address, your IP.  
17 That means they're detailing in the handshake who they connected  
18 to. Just so there's no misunderstanding, I meant to connect to  
19 -- whatever IP address was listed. That would have been the law  
10:32 20 enforcement officer.

21 And then the next highlighted portion is why I know it  
22 was seeding and needed no data from law enforcement or it would  
23 even think to ask for any data from law enforcement or any other  
24 BitTorrent client, because the next section says remote client  
10:33 25 has all 226 pieces. You have to download 226 pieces of data

1 before you would be in possession of the entire movie file.

2 Q. And I'm sorry to interrupt, but you'd have to -- based on  
3 what you previously said, you'd have to do that 50 pieces -- 50  
4 packets at a time?

10:34 5 A. 50 packets at a time is how you have to request them, yes.

6 Q. Okay.

7 A. So, and just to put it in context, that's about 50 -- just  
8 over 50 megabytes. So it's actually a small file as far as  
9 movies go on BitTorrent. 50 megabytes is not that large.

10:46 10 There's hundreds of megabytes of data that's shared in a single  
11 movie file.

12 Q. So here we've been talking about abstract kind of strings of  
13 alphanumeric -- alphanumeric strings, it looks like in the next  
14 highlighted portion we're actually start talking about the  
10:47 15 movie's name that you would see on the computer?

16 A. Correct. Now, it's inside of the torrent. The instruction  
17 files knows how to name it. It takes the name of the creator.  
18 Whoever first shared this content on the BitTorrent file sharing  
19 network, it takes that name.

10:48 20 Q. Okay.

21 A. And the file name is -- and it's long, I don't know -- it's  
22 on everyone's sheet of paper. 022 Asian-VPHC. It appears in  
23 the quotes. That's the file name.

24 Q. Okay.

10:49 25 A. And then the downloads begin in the next highlighted

1 section, it says, "Sent 50 requests." Well, that's because of  
2 the extended handshake. The sharing client that came to us to  
3 share child pornography said you're allowed to ask for 50  
4 packets at a time. So that's what we did. We asked for 50  
10:56 5 packets.

6 And then we started asking for the packets and they  
7 get received, line by line. I've requested a packet, it's  
8 received. I requested a packet, it's received. Had to happen  
9 226 times before the investigator would have the entire payload.

10:57 10 So....

11 Q. And are -- on the next -- geez, I don't know how many pages,  
12 17 pages long -- in the next series of pages, is that what  
13 you're detailing, that each piece going up to 226 --

14 A. Correct.

10:57 15 Q. -- this log reflects that it's been successfully received?

16 A. Correct, yeah. And it's just a couple minutes is all that  
17 it took. And then you don't see any more highlighting until  
18 page 11 of 17.

19 So, to put it in context, a computer on the BitTorrent  
11:30 20 file sharing network came to us and we agreed we're willing to  
21 talk about the same info hash, the same form.

22 We asked for pieces of data. Now, you notice in the  
23 extended handshake it never told us 226, did it? It didn't say  
24 anything about 226 pieces or even the file name of this file.

11:31 25 It's because both ends of the communication has this instruction

1 file. It's required. Without a torrent file, you can't  
2 download on the BitTorrent network. You can't just, you know,  
3 wander around on someone's computer and say I think I want to  
4 download that. It just doesn't work that way.

11:32 5 It only works because we have the same instructions  
6 file. And also included --

7 So, well, let me back up. So for the -- for the  
8 sharing computer to say I have piece zero through piece 225,  
9 which is 226 pieces, tells me right away he's got the torrent,  
11:32 10 he has to have the torrent, because I have my copy and sure  
11 enough, there's 226 pieces. Either that or it was a really good  
12 guess.

13 But now I named the file like the instructions says,  
14 but I've downloaded those 226 pieces. And where I'm going is,  
11:33 15 on page 11 where that highlighting [Indiscernible], that's a  
16 hashing that happens on every piece of data shared. And it  
17 comes up with that fingerprint, digital fingerprint as the  
18 defense expert described. It's actually a SHA-1 hash. Secure  
19 hashing algorithm version 1 hash is what BitTorrent uses.

11:33 20 And it calculates the hash value, the signature for  
21 all 226 pieces. And so now what happens is, we are going to  
22 compare those hash values and make sure it matches what is in  
23 the instruction file of the torrent.

24 We had data set, we calculated the fingerprint, we  
11:35 25 look inside the torrent and it matches. I got the right piece

1 of data. It has to be the right piece of data.

2 So for it to not -- for the computer that connected to  
3 us offering to share this torrent file to have guessed that it's  
4 226 pieces and responded to our 226 requests for data, have that  
11:36 5 computer give us that data and then match 226 SHA-1 hash values  
6 is inconceivable. The computer had to be in possession of that  
7 file and the instruction file, the torrent file, for what I  
8 described to have just happened. It's an impossibility. The  
9 computer had to have had it.

11:36 10 Q. And to be clear, that computer came to you. So Mr. Owens  
11 came to you.

12 A. Correct. And when you say "you," you mean the  
13 investigator --

14 Q. I mean the investigator, I'm sorry.

11:37 15 A. But, yes, the investigator running our software -- just  
16 because we searched for the torrent, like any other BitTorrent  
17 program searches for download candidates, that was enough to  
18 make us associated with the torrent that suspects were any  
19 computer on the BitTorrent network comes to law enforcement's  
11:37 20 version just the same way they would go to any other BitTorrent  
21 program [Indiscernible]: Bitcom, uTorrent, Sherazel (phonetic),  
22 there's a ton of them out there.

23 Q. And that was Exhibit 2. Exhibit 3 we don't really probably  
24 need you to walk through, but why are there two exhibits? This  
11:38 25 one reflects a date of May 22nd.

1 A. Yes. It was -- the Torrential Downpour Receptor is  
2 configured by the end-user and you can specify what IPs you'd  
3 like to investigate.

4 For instance, if I was a law enforcement officer at a  
10:55 5 university and I knew all of the University's IP addresses, I  
6 could say just -- I want to investigate any of these IPs.

7 And with Torrential Downpour Receptor, if any computer  
8 having that IP address comes to me offering to sell me drugs in  
9 my analogy, or give me child pornography, then I would accept  
10:55 10 that connection. I don't care about people in Russia or Spain  
11 or France coming to my computer, I care about people in my  
12 jurisdiction.

13 Or, the other possibility in the configuration, is I  
14 specify by geographic region. And I think the Court's already  
10:56 15 heard some of that through the defense expert. But it's  
16 publicly available. You can go to lots of places on the  
17 internet and you punch in an IP address and it will approximate  
18 what city and state that that IP is being used in. And that's  
19 just an effort for law enforcement to try to do investigations  
10:56 20 in their primary jurisdiction and not poaching in someone  
21 else's, so to speak.

22 Q. And so you reviewed the defense expert's affidavit.

23 A. Yes.

24 Q. And in there, in paragraph 24 essentially he asked what does  
10:57 25 it mean to direct investigative focus. Is that what you're

1 saying, this program directs the investigative focus by saying I  
2 want to do this in Wisconsin, or I want to do it in northeast  
3 Wisconsin, or this particular series of IP addresses?

4 A. Yes. It's user configurable. And it does run -- I  
10:57 5 configure it, I launch it, and it's set to investigate people in  
6 Wisconsin. And it's ignoring all the other connection attempts  
7 to us.

8 If I have a connection attempt from an IP address and  
9 it approximates the location as being in Spain, I just refuse  
10:58 10 that connection. I'm only accepting connections from the  
11 Wisconsin area, if that's how I configured it. And that's how  
12 you direct your investigative focus to a particular region, by  
13 their IP addresses, or straight up with their IP address if I  
14 knew that range off the [Indiscernible].

11:01 15 Q. And are those the settings that the investigator would be  
16 able to essentially input?

17 A. That, a license, their name. Things of that nature. But  
18 there is no setting that would enable them to -- enable a  
19 feature that would be harmful or would make the software not  
11:02 20 work properly.

21 Q. Or I want to go after this particular person or just white  
22 males in a certain area, those aren't variables that this  
23 program allows?

24 A. No, it's geographic region or IP address. And then you can  
11:03 25 further restrict it. Although I'm sort of the gatekeeper as it

1 relates to what torrents do the systems seek out on the network.

2 I can't define what's illegal in every state in the  
3 U.S., let alone every country in the world. I include torrents  
4 to be investigated that presumably would have some violation  
11:03 5 somewhere. It relates to child exploitation.

6 For instance, I could include pictures and movies of  
7 17-year-olds engaged in sex, which is child pornography  
8 federally and child pornography in Pennsylvania, where I'm from;  
9 but in Connecticut, it's 16 or under.

11:04 10 So the onus is on the investigator to look at what's  
11 downloaded and determine, yes, this violates our statute,  
12 [Indiscernible]. But we don't just sit there and sniff and  
13 listen to every piece of BitTorrent communication and try to  
14 discern as the defense expert --

11:05 15 And, you know, obviously he hasn't seen the software,  
16 but we aren't sitting there sniffing on the network or listening  
17 and trying to discern this is child pornography and this is not.  
18 No. We have the torrent. We're like every other BitTorrent  
19 client. We reach out to the index, the matchmaker as I  
11:05 20 described it earlier, and they provide us with IPs. That's it.

21 There's no listening for movie files, for anything  
22 else; it's just the predesignated torrents in the system. We're  
23 very refined. We're not searching for everything, we're looking  
24 for a very specific subset of data.

11:06 25 Q. And to be clear, in this particular case Mr. Owens came to



1 law enforcement.

2 A. Correct. But let me just say that if he had come to law  
3 enforcement and it wasn't one of the torrents we had chosen to  
4 investigate, it would have ended there as well. Because we're  
11:06 5 not going to talk to a person about it.

6 The other configuration I was leading towards -- and,  
7 sorry, that was a little long-winded -- is that the end-user, if  
8 they download material and they determine this is not violating  
9 my statute in Connecticut, because it has to be under 16, they  
11:07 10 have a mechanism to exclude those in future investigations. So  
11 they can further refine it even more than the work that I've  
12 done trying to identify the torrents leading to be investigated  
13 by law enforcement.

14 Q. Okay. You had the opportunity to view the imaging of  
11:08 15 Mr. Owens's computer I believe yesterday in my office, correct?

16 A. Yes.

17 Q. Okay. And I'll ask you what I asked the defense expert, did  
18 you find any artifacts or evidence that this particular file had  
19 been on Mr. Owens' computer?

11:08 20 A. Yes. The torrent which points to a file, yes, that both the  
21 torrent and the file was on the system in -- excuse me -- in  
22 three different areas.

23 Q. Okay. And did you print off basically information that  
24 would reflect that that we can show to the Court and provide to  
11:09 25 counsel?

1 A. Yes, I did.

2 MR. HUMBLE: May I approach, Your Honor?

3 THE COURT: You may, uh-huh.

4 BY MR. HUMBLE:

11:10 5 Q. I've handed you what have been marked Exhibits 4, 5 and 6.

6 Could you just identify those and tell the Court what they are?

7 A. Yes. These are just one portion of the forensic analysis.

8 4 relates to installed programs.

9 5 relates to torrent files.

11:11 10 6 relates to MRUs, or most recently used entries, from  
11 the registry.

12 Q. Okay. And did you create these?

13 A. I created this printout, but the forensic -- it was part of  
14 the forensic [Indiscernible].

11:11 15 Q. Sorry, that was imprecise. You created the images.

16 A. Yes.

17 Q. And that captures what you're trying to show here?

18 A. Yes.

19 Q. Okay. I'm going to switch those out, those duplicates, so  
11:12 20 that the Court can follow along.

21 Now, I guess start with the first one which I believe  
22 is No. 4?

23 A. Correct. So --

24 Q. Sorry. Could you just explain the significance of why  
11:12 25 that's highlighted and what that reflects?

1 A. Yes. But before I get there, I just want to go back to this  
2 log file where the computer that connected to the law  
3 enforcement reported what software they were running. And they  
4 reported it as being BitComet Version 1.50, which was  
11:13 5 highlighted in yellow in those two exhibits we just went  
6 through.

7 So the first thing I would look at would be to see if  
8 there is a BitTorrent -- BitComet program installed, and sure  
9 enough, BitComet Version 1.50 was installed. And  
11:13 10 coincidentally, or not coincidentally, it was installed on May  
11 20th at 9:07 -- I don't have my glasses on, I believe that's  
12 right -- p.m.

13 So that's the date, the day before the investigation  
14 happened. So the user of this computer installed BitComet  
11:14 15 Version 1.50 the day before the investigation happened and was  
16 memorialized in these logs. So that's the first -- that would  
17 be Exhibit 4.

18 MR. DONOVAN: Your Honor, if I may, I would like to  
19 interpose an objection. I think this is getting a little far  
11:14 20 afield of the relevance of this hearing which is whether or not  
21 we should have access to the program.

22 It sounds to me like he's trying to establish guilt  
23 based on he had the program on this date, it was installed on a  
24 certain date, then I guess there was, you know, torrents  
11:15 25 downloaded.

1           It just seems like this is kind of far afield of where  
2 we should be for today.

3           MR. HUMBLE: Except, Your Honor, that the defense  
4 expert places great significance on the fact that he did not  
11:16 5 find that particular file on the defendant's computer or in  
6 multimedia. So I think it is certainly relevant that there was  
7 strong evidence, which he also testified he did not find  
8 necessarily, to show that this was there both before and after  
9 law enforcement had any interaction with Mr. Owens's computer.

11:16 10           THE COURT: Overruled. And I assume we'll get to the  
11 law enforcement privilege later. But this is kind of the  
12 preliminary steps of how it works, as I understand it. And  
13 it's -- I see this as testimony intended to show that the  
14 defense is not in need of the software or the computer -- the  
11:16 15 other materials sought. Now, that's arguable, I agree, and  
16 certainly you'll be able to cross-examine and argue on that.  
17 But at this point I think this testimony is relevant, so  
18 overruled.

19 BY MR. HUMBLE:

11:17 20 Q. Okay. So, now, essentially he -- if this reflects that  
21 [Indiscernible] the tool that was used to knock on law  
22 enforcement's computer essentially and say I'm gonna give you  
23 this, that's reflected on No. 4?

24 A. Correct. Because the file wasn't found, the next thing I  
11:17 25 want to know as a forensic expert, okay, if it isn't there

1 today, deletion being a common thing we all do, let's show  
2 whether or not it was there during the investigation, which is  
3 what this was meant to do. So the software reported to law  
4 enforcement was installed the day before the investigation took  
11:18 5 place. That's the relevance of that exhibit.

6 Q. And how about Exhibit 5, what's the relevance of --

7 A. 5 is the torrent file named by its info hash. So if you  
8 looked at the detailed log with the highlights that we went  
9 through, remembering the first step is to agree that we're  
11:18 10 talking about the same torrent file, that's step number 1.

11 Because if we can't agree that it's the same torrent, I'm done  
12 talking to you.

13 If you look at the entry on Exhibit 5, the longest  
14 cell, it starts "Partition 4 Microsoft NTFS." But if you look  
11:20 15 at the next row down all the way to the end, you see a string of  
16 numbers and letters, 0833, and then at the end it ends in 3C0, I  
17 believe.

18 If you marry that up with the log, that's the exact  
19 same info hash. So there's a date and time affixed to that.

11:21 20 May 20th at 9:29. So we're talking 22 minutes after he  
21 installed BitComet -- he or she, the user of the computer --  
22 20-some minutes later the torrent was downloaded and loaded into  
23 BitComet. Why do I know that? Because the path of where that  
24 torrent was found would only get there if you loaded the torrent  
11:22 25 into the BitTorrent program. Otherwise it would just be sitting

1 in my downloads directory or on my desktop or someplace I chose  
2 to save it. That's a hidden directory for applications to store  
3 data they're using. So I know he downloaded the torrent and  
4 loaded it into BitComet for it to be there.

11:22 5 Q. And what is the --

6 A. And that's the day before the investigation, to put it in  
7 perspective, May 20th at 9:29 p.m.

8 Q. Okay. And the next exhibit, what is the significance of  
9 that?

11:22 10 A. Well, this is most recently used. And when you touch files  
11 and you access files, it will keep a record of that. And on May  
12 22nd, a file with the exact same file name as the one sent from  
13 the suspect computer to the law enforcement computer, is there.  
14 And that's dated May 22nd at 1:38 a.m.

11:23 15 So the second investigation occurred on May 22nd at  
16 3 a.m. So it's just an hours apart. It's still there so it's  
17 being shared all the way from the 20th, when he started  
18 downloading it, through the 22nd when the second undercover  
19 session happened.

11:23 20 And I also note that in the exhibit where the torrent  
21 was found, this -- there was more than one instance of him  
22 having that torrent. There was one that dated all the way back  
23 to January of 2016. And so what we are seeing more and more --  
24 because I still do investigations beyond the development aspect  
11:24 25 of my position -- more and more with the speed of the internet

1 and the efficiency of BitTorrent, not everyone keeps every file  
2 they download. They download it, they look at it, and at some  
3 point in time after that they delete it because it's so easy to  
4 get it again.

11:24 5 And there's -- there's a reference to that same  
6 torrent file all the way back to January of 2016. So that makes  
7 me fall on the side of the fence that these files were getting  
8 deleted as opposed to it was never there. It was clearly there.  
9 That's what these forensic artifacts show.

11:25 10 Q. And correct me if I'm wrong, the log that we went through  
11 previously, that's what law enforcement has -- receives,  
12 correct?

13 A. Right. This is the memorialization of the events that took  
14 place during the investigation made by Torrential Downpour  
11:25 15 Receptor.

16 Q. And 4, 5, 6 were taken from the image -- the imaging of the  
17 defendant's computer.

18 A. Yes, that's correct. That's a seized device.

19 Q. So these aren't married -- these are two opposite ends  
11:25 20 essentially matching up.

21 A. Correct. Everything's lining up.

22 And I could have stopped just by reading this log.  
23 There is no way that a computer at that IP address didn't  
24 possess that data, to be able to give me 226 pieces that match  
11:26 25 the right hash file. The computer had to be in possession of

1 that data to send it, and this just further confirms it.

2 Q. Okay. So let's get to law enforcement privilege then.

3 What's the harm in allowing testing to occur with  
4 regard to Torrential Downpour Receptor?

11:27 5 A. Well, it has access. In order to run it you have to have a  
6 license, first of all. That license is controlled by the system  
7 I'm the administrator of.

8 And when you have a license to the software, it's  
9 designed to download child pornography. And so you put in a  
11:29 10 license and you specify an IP address or geographic region,  
11 child pornography will be downloaded, because people will arrive  
12 to our computer and offer to share child pornography with us.  
13 So it exposes each and every torrent file we're investigating.

14 Again, to know the info hash of these torrents could  
11:29 15 be harmful to law enforcement because if that gets out --  
16 although, you know, people can promise never to release it, you  
17 can't un-ring the bell. Once it's out it's done. We have to  
18 start from scratch.

19 It's taken eight years to amass what we have here  
11:29 20 today. At least eight. I can't remember the exact days when we  
21 started, but it was at least eight years to get where we are  
22 today.

23 It exposes the files we investigate and their hash  
24 [Indiscernible].

11:30 25 It exposes law enforcement contact information of



1 investigators who are investigating individual IP addresses.  
2 These are active investigation.

3 It exposes the IP address -- other IP addresses  
4 associated with the torrents that we investigate. So, in other  
11:30 5 words, these have yet to be investigated. There are just so  
6 many people on BitTorrent sharing child pornography, we cannot  
7 get to them all. I've trained personally hundreds, maybe  
8 upwards towards a thousand investigators, and we can't come  
9 close to getting all the people sharing child pornography on the  
11:31 10 BitTorrent file sharing network. And I'm not even talking about  
11 all the other areas that we can investigate.

12 So -- and finally, I mean, aspects of the system,  
13 you're basically dropping a civilian in the mix of a raid  
14 briefing. These are -- the system is designed to connect law  
11:38 15 enforcement officers that have similar investigations based on  
16 their IP addresses, they're in some stage of investigation, the  
17 system alerts them of that, and you're dropping a civilian in  
18 the middle of a raid briefing. If you're taking something  
19 technology and trying to relate it to something real world, it  
11:39 20 would be an equivalent.

21 Q. Were you saying raid, r-a-i-d briefing?

22 A. Raid like a search warrant.

23 Q. Okay.

24 A. Is what I was referring to.

11:39 25 Q. Okay. So, let me ask you, with regard -- in your opinion,

1 as someone who helped develop this program and obviously has a  
2 lot of familiarity with it, is Torrential Downpour Receptor so  
3 different from other BitTorrent programs that there is a strong  
4 need for the defense to have this before they could  
11:41 5 cross-examine somebody on the operations of this particular  
6 BitTorrent?

7 A. The only point of confusion that I could see the defense  
8 expert having, which he now has the answer to, was why a  
9 computer would connect to us. He gave a definition of seeding.  
11:41 10 And I don't know that he had a full understanding of what  
11 seeding actually was.

12 But now with that question answered, this is -- this  
13 is BitTorrent talk. This is not Torrential Downpour Receptor  
14 talk. I mean, anyone should be able to look at this and see  
11:42 15 that data was sent and it matches the corresponding hash  
16 [Indiscernible]. The defense expert has the ability to look at  
17 the torrent which is part of discovery, open it up and see all  
18 of the hash values of all those 226 pieces, see that they were  
19 verified, could even take the original file and hash those  
11:44 20 individual segments to make sure that they do, in fact, belong  
21 to that file, none of which requires our software.

22 This is -- this is a law enforcement BitTorrent piece  
23 of software that, yes, employs the ability to download from a  
24 single IP address as opposed to from multiples. Well, that's  
11:45 25 law enforcement being more restrictive on itself.

1 I could get it really fast, but I'm willing to wait.  
2 But it's not something unique to law enforcement software. A  
3 download from a single sharing IP happen all the time.

4 So I don't believe that there is a need to confirm it  
11:45 5 when we've detailed it as specifically as we have. This is all  
6 information, as the defense expert said, that any BitTorrent  
7 client would know. But whether or not it chooses to display it  
8 to the user, and certainly probably wouldn't memorialize it to a  
9 log file like this, but it is to aid the prosecution, but it's  
11:46 10 also letting the defense expert know exactly what happened at  
11 what moment in time.

12 And he can confirm these things through the forensic  
13 analysis, as I did. I spent 10 or 15 minutes and found these  
14 three items. There's probably much more on there that I didn't  
11:46 15 look at, and to have the torrent file and the data, that should  
16 be sufficient.

17 Q. In your expert opinion, if there had been a bug or a glitch  
18 in the software, would that be reflected in the things that  
19 you've reviewed prior to your testimony here today?

11:47 20 A. Yes. I mean, I would get the bug reports. I would know if  
21 there was a bug report. If people are continually downloading  
22 files and they didn't come from the sharing computer, I would  
23 know to seek that out.

24 But it's a very simple process. As the defense expert  
11:47 25 said, the IP addresses have a source and destination IP right in

1 every packet of data. It's not hard to discern where it came  
2 from. And we just memorialize that in this document.

3 And, again, that IP address came to us. Just like if  
4 you visit a web page, that web server knows your IP address  
11:48 5 immediately. Well, the suspect computer came to us. We  
6 documented the IP address, we allowed the communication to  
7 happen, and then we received the data they wanted to share with  
8 us.

9 Q. Would you -- based on your knowledge of Torrential Downpour  
11:48 10 Receptor, would you describe it as bug-ridden or buggy as I  
11 guess software people say?

12 A. No. Early on in its early stages of development we had the  
13 source code looked at, and there was one issue -- and this is  
14 eight years ago -- where we weren't accounting for long file  
11:49 15 names that exceeded 260 -- or the path and file name to exceed  
16 260 characters, that was fixed, and that was the end of the bugs  
17 as it relates to downloading.

18 BitTorrent is a very, very light-weight small  
19 protocol. A BitTorrent program like BitTorrent or uTorrent are  
11:50 20 like a couple megabytes. It's the size of a single picture.  
21 It's not a ton of code that could be bug-ridden like the defense  
22 expert's example of an operating system or Microsoft Word that  
23 are millions of lines of codes. We're talking about 2 megabytes  
24 of programming.

11:50 25 So, but that was fixed eight or more years ago, the

1 long file name issue, and all that would have done was shut the  
2 program down. It wouldn't have collected erroneous information.

3 And the fact that BitTorrent relies on SHA-1 hashing,  
4 which is extremely accurate, you're not going to get the false  
11:52 5 positives because we're confirming the data through hashing, the  
6 same thing forensic examiners use to confirm I'm working from an  
7 exact duplicate of the hard drive seized. We rely on it day in  
8 and day out. Well, BitTorrent does as well. And through  
9 hashing, short of SHA-1 hashing failing, which is very, very  
11:52 10 accurate, you're not going to get a [Indiscernible] false  
11 positive.

12 MR. HUMBLE: Judge, I don't have any further  
13 questions.

14 THE COURT: Mr. Donovan?

11:53 15 MR. HUMBLE: Could I just ask that those exhibits be  
16 received, Your Honor?

17 THE COURT: 1 through 6 received.

18 I take it there's no objection.

19 MR. DONOVAN: Well, Your Honor, I mean, we didn't see  
11:53 20 Exhibits 4, 5 and 6 before today, but, I mean, no objection as  
21 far as --

22 THE COURT: I don't think they existed before today.  
23 It sounds like they were run off today. Is that right, Mr. --

24 MR. HUMBLE: Was it this morning or last night? Last  
11:54 25 night perhaps.

1 THE WITNESS: To be clear, this is the forensic report  
2 of the forensic examiner. This is the material that was --

3 MR. HUMBLE: Yeah, it's been provided, just not the  
4 exhibit --

11:54 5 THE COURT: Okay.

6 MR. DONOVAN: Your Honor, we don't deny that the  
7 forensic material was provided, but, I mean, it's large. It's  
8 very voluminous. And we did not see these exact references  
9 until today.

11:54 10 THE COURT: Yeah. But you had access to the hard  
11 drive or the computer --

12 MR. DONOVAN: Correct, yes.

13 THE COURT: -- evidence from which this was taken.  
14 I'll overrule the objection and 1 through 6 are  
11:55 15 received.

16 (Exhibits 1-6 received in evidence.)

17 MR. DONOVAN: Thank you.

18 CROSS-EXAMINATION

19 BY MR. DONOVAN:

11:57 20 Q. Good afternoon. Getting towards the evening here shortly.

21 Okay. So you have testified that you were part of the  
22 original development for all of these types of programs,  
23 correct?

24 A. Yes.

11:57 25 Q. And it's been kind of an evolution from probably -- I don't

1 know if Gnutella was maybe the first iteration all the way up  
2 through now BitTorrent. Right?

3 A. There are many file-sharing networks that we have  
4 investigative tools for.

11:59 5 Q. Can you I guess more precisely describe your role? Because  
6 you said you didn't do any of the actual programming, correct?

7 A. I didn't write Torrential Downpour Receptor, the program  
8 being used. I did programming on the back end and testing of  
9 the software. But with the other tools there are programming  
11:59 10 elements that I did participate in, it's just not with  
11 Torrential Downpour Receptor. The physical program sitting on  
12 the investigator's computer, how it logged search results and  
13 things like that I was involved.

14 Q. Okay. How long did the development take of Torrential  
11:59 15 Downpour?

16 A. From the point in time where we first talked about it at the  
17 University of Massachusetts to releasing the first version, it  
18 was well over a year. Maybe more.

19 Q. And maybe this is a good time, can you explain the  
12:00 20 difference between Torrential Downpour and Torrential Downpour  
21 Receptor?

22 A. Torrential Downpour wasn't used in this case and it doesn't  
23 sit and wait for suspect computers to arrive to our computer.  
24 It's the complete opposite of that.

12:00 25 So Receptor sits and listens passively for people

1 coming and knocking on our door asking to share torrents that we  
2 know that involve child exploitative material.

3           Torrential Downpour makes outbound connections trying  
4 to connect to somebody that may or may not be sharing child  
12:01 5 pornography.

6           That's the big difference. We sit passively and wait  
7 for the suspect to come to us.

8 Q. Is the only way you know which one was used in this case is  
9 from reviewing the logs? Or did you talk directly to the law  
12:01 10 enforcement officers who ran this?

11 A. Well, the log certainly tells us -- that's the whole purpose  
12 of putting on the first line the software that's used. But  
13 beyond that, through networking I can tell that.

14           In the extended handshake he tells us what his listing  
12:02 15 port is. So if I were to connect to him, I would connect into  
16 that port. I know we're getting kind of technical. But you can  
17 see at the top, he connected to us because it's an outbound  
18 port. There's a specific range of ports. Of the 65,000  
19 ports -- there's more than 65,000 ports available to use --  
12:02 20 there's a set of ports set aside just for making outbound  
21 connections.

22           So it's proof that the suspect computer connected to  
23 us. The networking ports alone tell you that. And the software  
24 that we indicate we were using at the top of the log indicate  
12:03 25 that. That's the only functionality it has, is to receive an



1 inbound connection which triggers an investigation.

2 Q. But, again, you would agree that the logs are a subset of  
3 the program, correct?

4 A. The --

12:03 5 Q. They're generated by the program.

6 A. They're generated by the program, I agree with that.

7 Q. And so the information that comes from the program dictates  
8 what's on the logs.

9 A. Correct.

12:03 10 Q. In other words, the logs aren't an independent check or  
11 verification of anything, it's a subset of the program that  
12 we're talking about.

13 A. Correct. The computer comes to us, we see the IP address,  
14 we memorialize it in the log. Correct. Which is Windows,  
12:04 15 actually.

16 Q. What language is Torrential Downpour Receptor written in?

17 A. C#.

18 Q. Okay. And so obviously this involved, you know, computer  
19 scientists and software developers and other people besides  
12:06 20 yourself to put it together, correct?

21 A. Me and one guy, Brian Lang.

22 Q. Okay. Oh, just the two of you.

23 A. Yes. And it's not -- it was written by the ground up from  
24 the university. It was not a modified version of an existing

12:07 25 program. So that was incorrect information the Court had heard.

1 It was written by the University of Massachusetts Amherst. And  
2 the team of developers beyond the initial research is me and  
3 that one individual.

12:08 4 Q. Okay. Now, you've reviewed the pleadings in this case,  
5 right?

6 A. Yes. Well, I've read the defense expert's report/affidavit.

7 Q. Did you read any of the motions filed by either me or the  
8 government?

9 A. I did not. They were already filed and done before I even  
12:08 10 had communicated with the office. I don't believe I -- I did  
11 have a copy of the police officers' report. I never had a copy  
12 of the search warrant. And then obviously I have the two  
13 detailed logs.

14 Q. So, sir, are you aware that the government has said that  
12:08 15 basically the investigator in this case accessed BitTorrent like  
16 a normal or average user of the program? I'm talking about the  
17 normal BitTorrent program, not the law enforcement program.

18 A. Can you repeat that? I don't want to --

19 Q. Are you aware that the government's characterized law  
12:09 20 enforcement's use of BitTorrent here as a normal or average  
21 user?

22 A. I am now, I wasn't before. But I don't feel that that's  
23 inaccurate.

24 Q. You don't feel that's inaccurate.

12:09 25 A. No, we follow the protocol. And just like any other program

1 can receive an inbound connection and download any or all of  
2 that data, we did the exact same thing except we memorialize the  
3 data and we don't share.

12:10 4 Q. Well, there's -- I mean, there's a lot of other things that  
5 the program does the public version doesn't, right?

6 A. (No response.)

7 Q. And I can give examples.

8 A. Okay.

12:10 9 Q. Would you agree that, again, it does single source  
10 downloads?

11 A. Correct. The general public does that as well.

12 Q. And I understand you testified that that could also happen  
13 in the public if there was only one computer sharing this one  
14 file that could be a single source, but your program doesn't  
12:11 15 even when there's multiple sources available which would be  
16 contrary to the normal protocol, right?

17 A. Our program I'm sure it happens every time, but it happens  
18 naturally every day on the internet.

19 Q. But yours insures it only happens on single source  
12:12 20 downloads.

21 A. Right.

22 Q. Right? It wouldn't do any good to get multi-source  
23 downloads and then try to figure out who to attribute this to,  
24 right?

12:12 25 A. That would be counterproductive. It would add a burden to

1 law enforcement.

2 Q. And your program -- and I think you testified earlier that  
3 it doesn't fake file share, it just says it has no pieces to  
4 share, right?

01:09 5 A. Because we have no pieces to share we appropriately say we  
6 have no pieces to share.

7 Because the computer -- since we're employing a single  
8 source download, every piece of data we have received came from  
9 the computer that connected to us. So there is no need for us  
01:09 10 to ever share any data back because everything we have come from  
11 the sharing computer.

12 Q. Well, I understand, too, you don't want to share contraband,  
13 correct?

14 A. Correct.

01:10 15 Q. Okay. How do you then -- so the program does something to  
16 stay on the BitTorrent network and not get kicked off, right?

17 A. That doesn't exist. And I don't -- I'm not sure what the  
18 defense expert was talking about.

19 Q. Well, have you heard the term "throttling" before?

01:10 20 A. Yes, you can throttle. That's not being kicked off the  
21 network.

22 Q. Oh.

23 A. So, in other words, there are incentives. If you share, if  
24 you employ that tit-for-tat exchange, so I'm giving pieces as  
01:11 25 I'm getting pieces, you're -- the allocated bandwidth you're

1 given is increased. So I might get that file a little quicker.

2 But, to not share, I'm still able to download and I'm  
3 not kicked off the network and I'm not fake file sharing.

4 Q. Okay. I'm sorry, I don't mean to be imprecise. I didn't  
01:11 5 mean to say kicked off the network. But you could get throttled  
6 if you're not sharing, right?

7 A. You could receive your downloads slower than other  
8 BitTorrent clients.

9 Q. But here you testified that based on the logs these  
01:12 10 downloads actually occurred pretty quickly.

11 A. Correct. Because the client didn't need any pieces for us.  
12 The tit-for-tat exchange was gone. That, on top of the fact it  
13 was an AT&T U-verse connection, which has a large amount of  
14 upload bandwidth which is the one exception. AT&T U-verse and  
01:12 15 Verizon Fios have huge upstream bandwidths. So what the defense  
16 expert was describing really doesn't apply because the  
17 connections are so fast. But it's only a 15-megabyte movie, so  
18 I expect it to happen fairly quickly with the speed of the  
19 internet today.

01:13 20 Q. So just to be clear, is your testimony that the program does  
21 not do anything to stay on the network that an average user  
22 couldn't do? To avoid being throttled or --

23 A. I don't even understand what you mean by on the network.  
24 Because you're on the network every time you load a torrent file  
01:14 25 into your program. You don't get kicked off. A user can choose

1 to share the data with you slower. And, yes, that is part of  
2 the incentive scheme for this give-to-get scenario on  
3 BitTorrent. But it doesn't preclude you from getting everything  
4 without sharing one single bit of data, which happens naturally  
01:14 5 every day on the network.

6 Q. So does Torrential Downpour do anything to avoid throttling?  
7 I shouldn't say kicked off. Avoid throttling for not sharing.

8 A. No. We properly say we have nothing to share at the  
9 beginning of the session. And then if ever we're asked again,  
01:14 10 if we handshake again, which happens sometimes, we would report  
11 what pieces we did have to share.

12 Again, the sharing client gave us every piece we  
13 possess. There is no need for him to ever request that back  
14 from us. So this whole tit-for-tat exchange and the throttling,  
01:15 15 as you put it, of the bandwidth doesn't really come into play in  
16 this case specifically because they were seeding. They had all  
17 of the content. There is no need to throttle data. Its purpose  
18 in life when it's seeding is sharing the data proactively out to  
19 the network to keep that data alive on the BitTorrent network.  
01:15 20 So throttling really isn't in play when there's a seed.

21 Q. Is it ever in play, though? I mean, it's not in play in  
22 this case, but can it ever be in play that you get throttled?

23 A. Oh, absolutely. Again, if I never share a piece of data,  
24 which we don't, I will never benefit from added bandwidth from  
01:16 25 the sharing client.

1           Additionally, clients at times, depending on --  
2           there's so many variables to go into, but depending on how  
3           popular the torrent is, they could actually share with me for a  
4           period of time and then disconnect from me. And then later, as  
01:17 5           any BitTorrent client would, you can reconnect and ask for  
6           additional pieces. Again, I'm in the same situation.

7           Q. So I'm not trying to belabor this, but, again, not in this  
8           case, but does Torrential Downpour Receptor ever do anything to  
9           not get throttled in general to be able to keep up fast --

01:17 10          A. No.

11          Q. -- and do what it wants to do?

12          A. To the contrary. We get throttled is what I'm trying to  
13          say. We didn't here because --

14          Q. Okay.

01:17 15          A. -- he was seeding. But there is no secret mechanism to keep  
16          us getting data faster than we deserve to get it. It doesn't  
17          exist. And I wasn't trying to avoid the answer --

18          Q. Okay. It's fine. I apologize. I probably wasn't being  
19          precise enough.

01:18 20                        Torrential Downpour Receptor again generates these  
21          specialized data logs that you've talked about which the normal  
22          program doesn't do, correct?

23          A. Correct.

24          Q. Okay.

01:18 25          A. It's information known by the programs, but there would be

1 no purpose for BitComet to write out a log like this.

2 Q. And it conducts searches against the hash library, you've  
3 talked about, right?

4 A. (No response.)

01:19 5 Q. Again -- in other words, you have a set of hash values that  
6 you are looking for torrents that report having an association  
7 with them, correct?

8 A. Correct. We're searching for a torrent exactly like any  
9 other program out there. As soon as a torrent gets loaded into  
01:19 10 BitComet, which is the program in question here, it actually  
11 searches for download candidates.

12 And that's what we do. We physically load a torrent  
13 into Torrential Downpour Receptor, and then it searches the  
14 network for download candidates. It's exactly the same.

01:20 15 Q. Now, to be clear -- to be clear, when you say "we" it's  
16 actually you. You maintain control exclusively of the database,  
17 or library, whatever you want to call it, of all these hash  
18 values you're looking for, right?

19 A. What torrents we search for I'm in control over. What is  
01:20 20 being searched for by the investigator is an actual torrent file  
21 being loaded into Torrential Downpour Receptor like any other  
22 program. We're just excluding the commercial movies and the  
23 commercial music and the illegal, you know, copyrighted programs  
24 that are traded on BitTorrent and we're only focusing on child  
01:21 25 exploitation material.



1 Q. Again, that you decide on, correct?

2 A. I decide on what is to be searched for. The investigator  
3 decides on what to use as probable cause for a charge.

4 Q. Okay.

01:21 5 A. And they make suggestions. They will submit torrents to me  
6 to be evaluated to be included into our system.

7 Q. Can you describe a little bit about how the program is set  
8 up by someone who's got a license and is trained to do this?

9 A. Sure. It has an installer file just like any other program.  
01:21 10 You double-click an installer file. It will ask you some  
11 questions. Some questions already have answers to them. But it  
12 will ask you to input your name. There are options to put in  
13 your email address. But you have to have a license number to  
14 run it or else it won't function.

01:22 15 So we control who has a license. So if the software  
16 gets out there it's nonfunctional without the license, it will  
17 do nothing.

18 You will specify with Receptor what geographic region  
19 you'd like to investigate. Or you could express it by the  
01:22 20 physical IP address or a range of IP addresses, which is the  
21 trigger to the program to decide whether to, as the investigator  
22 put I think, direct his investigative focus towards a particular  
23 IP or not. It's based on his settings. He's told the computer  
24 investigate these IPs or just investigate people in Wisconsin as  
01:23 25 opposed to anywhere in the world.

1           And there are settings regarding how long should we  
2 wait for the download to complete. Because we're not gonna wait  
3 forever. And so we can just stop the investigation after a  
4 predetermined period of time. The default I think is four  
01:24 5 hours.

6 Q. And this program can run automatically, right, after it's  
7 set up and configured?

8 A. Correct. You're going to configure it and set it up and  
9 it's going to search for torrents and receive those inbound  
01:24 10 connections automatically. The logs get written out  
11 automatically as well.

12 Q. So does the investigator typically just check the results  
13 like every day, every week, every month? Like how does that  
14 work?

01:24 15 A. Well, I can't speak for every investigator, but on every  
16 shift of my work I check my logs.

17 Q. Okay. Okay. So going back to the logs that have been  
18 introduced as Exhibits -- I believe 2 and 3, how do those logs,  
19 for example, like establish by themselves that Torrential  
01:25 20 Downpour Receptor doesn't invade, for example, the shared space  
21 of a computer?

22 A. Well, it basically comes down to -- well, first the suspect  
23 computer comes to [Indiscernible]. That's the first piece.

24           The second piece is just to understand BitTorrent, if  
01:25 25 you understand the BitTorrent set of rules that have to be

1 followed and how it functions, it's -- what you're describing is  
2 impossible.

3 I can't -- if I wanted to download -- excuse me, I'm  
4 sorry.

01:25 5 If I wanted to download a file from some unshared  
6 location on the computer, I can't even do that because both the  
7 sharing computer and the investigating computer -- or in another  
8 way I could say that as any two BitTorrent programs -- would  
9 require that you have the exact same torrent file.

01:26 10 I can't -- there's no function within BitComet, which  
11 is what was used on the suspect computer in this case, there is  
12 no ability to download anything. We can only receive what the  
13 sharing computer permits us to get.

14 Q. So is your answer that the program just can't do it and,  
01:27 15 therefore, that's why it's not on the logs? Is that --

16 A. It's -- yeah. Not even BitComet. Any BitTorrent program on  
17 this planet require a torrent file on both sides with that  
18 really unique identifier. I have no way to know where these  
19 files are on the suspect computer, let alone create a torrent  
01:28 20 file, load it into his BitTorrent program, just so that I could  
21 then investigate him with our BitTorrent software. There's just  
22 no mechanism. You'd have to show that there was a flaw in  
23 BitComet at Version 1.50 that allowed some crazy intrusion like  
24 you're describing, but that doesn't exist.

01:29 25 Q. Are there any other types of logs generated besides what's

1 been entered as exhibits or is that the comprehensive log?

2 A. This is the comprehensive log. There's also a net -- a  
3 netstat. Because for reasons just like this, there's a Windows  
4 program that will record TCP connections.

01:29 5 And earlier as I was describing how the suspect  
6 computer connected to the law enforcement computer, it was  
7 through something called a TCP connection. And Windows has a  
8 utility that will track all of the TCP connections between my  
9 computer and other computers. So we run this netstat program,  
01:30 10 this windows program that has nothing to do with us and our  
11 development, to confirm, to give corroborative evidence that,  
12 yes, this other program came to the same conclusion as us that  
13 there was an active TCP connection between us and the suspect  
14 computer.

01:31 15 So there's the netstat log. There's a summary log  
16 which is just less verbose than the detailed log. There is the  
17 torrent info.txt file which gives you all of the information  
18 inside of the torrent that is used to calculate that unique  
19 identifier, that info hash I spoke of.

01:32 20 There's two XML files that contain data and I don't  
21 remember them off -- the names off the top of my head. Those  
22 XML files are just data that help us evaluate the case more  
23 quickly.

24 It's the same data that you're finding in the detailed  
01:32 25 log in other areas. We have a program that helps us parse

1 through that and realize information. So that's what those XML  
2 files are for. And then you have the actual downloaded material  
3 which is in a download directory.

4 So that's the output of the software, all those items.

01:33 5 Q. Are there any other either libraries or software packages  
6 that the program relies upon or uses?

7 A. No. Actually there's no libraries. Everything was written  
8 from the ground up. There was a point in time I think he was  
9 using an open source library, but he ceased using that years  
01:34 10 ago.

11 Q. So is it like -- I mean, I'm not trying to be too basic  
12 here, but is it literally like one file, the program? Like one  
13 application file? Or does it have associated files with it?

14 A. Yeah. I mean, you're gonna install a program and it's one  
01:34 15 file to start the installation, but it's just not a single file  
16 that makes it work. There's configuration files and such.

17 For instance, when you're inputting the settings on  
18 who you want to investigate, that has to be stored somewhere.  
19 There's other associated files [Indiscernible].

01:35 20 Q. Okay. Is Torrential Downpour Receptor actively maintained?

21 A. Yes. It's worked on and maintained by the University, who  
22 is the owner of the software. It still exists. And, you know,  
23 there may be features we want added to it. That programmer is  
24 still available to accommodate law enforcement requests.

01:36 25 Q. How about like, are there patches done to it occasionally?

1 A. Oh, there's new versions released to implement new features  
2 that we want to make law enforcement's job easier in evaluating  
3 the case. There's so many people on BitTorrent sharing child  
4 pornography that we want to try to get the most egregious stuff  
01:37 5 first. Those are the changes that are being made in the new  
6 release.

7 Q. Is it your testimony that there's really only been one bug  
8 with this program since the time it was developed?

9 A. That's the only bug that I know of that relates to single  
01:37 10 source downloading, and it was reviewed -- it was the long file  
11 names, which was handled.

12 Q. Who found that or who reviewed that?

13 A. Before the FBI would let the -- their agents use the  
14 software, which we had already bought through a grant, and they  
01:38 15 did an independent validation of the method in which we do  
16 single source downloading to confirm that we don't share, which  
17 obviously law enforcement can't become part of the problem, and  
18 that it does employ properly as [Indiscernible].

19 Q. I don't know suppose that FBI validation is publicly  
01:39 20 available.

21 A. No. I mean, the purpose of them doing it was to permit the  
22 agents to use the software we developed. And now they've  
23 abandoned their own programs and just use the whole  
24 [Indiscernible] that make --

01:40 25 Q. But again, that's not something that we can look at, that

1 validation.

2 A. I don't have it. I've read it once, and that's why I know  
3 that was the bug that was seen and fixed immediately. And,  
4 again, I'm the administrator of the entire system still to this  
01:41 5 day. It's housed by the Pennsylvania State Police in a computer  
6 center and I would receive those bug reports. I don't know of  
7 any other bug that would affect [Indiscernible].

8 Q. So you're the only person that would get reported to if  
9 there was a problem?

01:41 10 A. Me or the developer. If any other instructor would receive  
11 it, it has to come to me eventually, or the programmer.

12 Q. So how often typically is it updated?

13 A. The version that's current -- I don't think there was any  
14 release in the last six, eight, ten months maybe. There may be  
01:42 15 some years where there were a couple releases. Because we,  
16 again, they're feature enhancements, not changing the method in  
17 which we single source download. But we may want to be able to  
18 flag the most egregious torrent as opposed to torrents that have  
19 pictures of kids modeling adult lingerie or something like that.

01:42 20 Q. Well, that would just be more updating the hash database,  
21 right?

22 A. No, that's updating the program and how you look at it.

23 Q. Okay.

24 A. How you look at the data.

01:43 25 Q. What type of network connectivity does it require?

1 A. It uses TCP communication for the file transfers.

2 TCP, Your Honor, is transmission control protocol.

3 And it's, again, that type of internet traffic that I compared  
4 to like a phone call. You dial a number, you say hello, hello.

01:43 5 There's error correction, all kinds of things.

6 Some of the indexing that BitTorrent uses also uses  
7 UDP packets, which are connectionless packets. And that's for  
8 once you load the torrent, so that you can get those IPs of  
9 people associated with the torrent. That comes via UDP

01:44 10 depending on which index you're connecting to. So it uses both  
11 TCP and UDP networking.

12 Q. Do you test to determine whether it's operating correctly  
13 from time to time?

14 A. Yes. You test it at the conclusion of every class with the  
01:44 15 students. I test it before the release of the software.  
16 There's a validation process.

17 Q. So you've done that testing in the past. You say you do it  
18 every class that you teach?

19 A. Yeah, at the conclusion of the class we go through a  
01:44 20 process. Because it's automated the end-user in the class,  
21 we'll go through a validation process.

22 So, for instance, if we're gonna rely upon a log as  
23 the basis to get a subpoena for a subscriber or eventually a  
24 search warrant, then that investigator needs to trust that the  
01:45 25 logs' dates and times are correct.



1           So we have a computer that's sharing content and a  
2 computer that is investigating. And we show both screens. And  
3 as -- as events happened we confirm that the dates and times in  
4 the log are correct. We confirm that the IP address purported  
03:11 5 in the log is correct. Because we're controlling both sides of  
6 the communication, so we know the sharing computer's IP and the  
7 investigating computer's IP.

8           We verify that it properly weights out the info hash  
9 of the torrent in question, and that it dates and timestamps  
03:12 10 appropriately throughout that log.

11           And then, finally, it calculates the MD5 and SHA-1  
12 hash at the conclusion of the transfer.

13 Q. So in this training or this validation testing you just  
14 described, you're controlling both computers, correct?

03:13 15 A. Correct.

16 Q. Are you actually transferring child pornography or is it  
17 just a benign file of something else?

18 A. It's a benign file.

19 Q. So why couldn't that be done for the defense?

03:13 20 A. Well, it exposes all those other things to our system.

21           Again, once you have a license to our software, you  
22 see active investigations, you see contact information for the  
23 investigators, you would learn all of our hash values, all the  
24 info hashes of the torrents. But it is possible to set up a  
03:14 25 torrent with data that is not child pornographic, but it takes

1 my involvement.

2 Q. Well, in fact, so you've done that before for the defense  
3 counsel, right?

4 A. Done what?

03:14 5 Q. A demonstration or a validation testing.

6 A. I've done demonstrations. But when I do demonstrations I  
7 can just actually -- I can actually just transfer child  
8 pornography. In my test I run the system, I actually download  
9 [Indiscernible] log. I don't have to show them the movie file  
03:15 10 that gets downloaded. But additionally, we have offered a  
11 validation test -- although it's in-house, we've offered a  
12 validation test I think for [Indiscernible].

13 Q. So you have offered some access before to defense counsel,  
14 right?

03:16 15 A. Not to the software. A validation test which is documented.

16 The whole process, like I describe to our students,  
17 we'll test the software so they can be comfortable with the  
18 dates and times, the logs, what's logged. There's a whole  
19 validation process. And just like the students would see, both  
03:18 20 the sharing computer and the investigating computer, we do that  
21 with video screen recording. So visually you can see that the  
22 software is connected to the sharing computer. The logs are  
23 shown. And so you can verify the dates and times are accurate.  
24 And then, finally, there's a packet capture.

03:18 25 As the defense brought out, that can be used to prove

1 single source downloading, which is the only thing that I saw  
2 other than the questions he had in his report was more of a  
3 what-if scenario, what if it was downloaded from someone else.

03:19 4 So that's the only thing I really saw in his report  
5 that was any question as to the reliability of our software  
6 short of not finding a file, but clearly it was there.

7 So that packet capture is proof of single source  
8 downloading as your own expert said.

03:20 9 Q. But you've never let anybody do a packet capture, you never  
10 let anyone have hands on the program. The most you've ever done  
11 is let them just watch your demonstration controlled on both  
12 ends from you.

13 A. Correct.

14 Q. Or by you.

03:20 15 A. It's documented in such a way it couldn't be altered. Hash  
16 values of all the elements of the tests are recorded and seen  
17 visually and memorialized [Indiscernible].

18 Q. Has the government asked you to be able to do that here  
19 today, you know, in this case?

03:21 20 A. No, the government never -- again, I got involved in this  
21 case I think after the motion -- the pending responses or  
22 motions were filed. It's only been a couple weeks that I've  
23 been involved in the case.

03:22 24 Q. All right. So when you do a single source download from the  
25 IP address that you identify as a target computer, okay? Do you

1 know how long at that point that the source computer had that  
2 file?

03:22 3 A. No. If you had search results, a history recorded, you  
4 could have an idea of about how long. But normal BitTorrent  
5 communication, no, would not tell you that.

6 Q. And you didn't know -- you wouldn't know where they got it  
7 from, where the source computer might have gotten it from in the  
8 first place, right?

03:23 9 A. No. No. I mean, that's true with file sharing as a  
10 whole --

11 Q. Okay.

12 A. -- across the board, yeah.

13 Q. So it could have been downloaded by that source computer as  
14 a single file or it could have been downloaded in a batch. I  
03:23 15 think you testified earlier that you can download, you know,  
16 multiple files at one time, right?

17 A. Yes. Some torrents describe one file, as it was in this  
18 case, or it could be dozens or more.

03:26 19 Q. So it could be a situation where a user of a computer is  
20 downloading dozens of files, a whole batch of files and, you  
21 know, maybe one of it or some of it's child pornography, the  
22 rest is legal material.

23 A. That's certainly possible. That's the whole purpose --  
24 that's why we get search warrants and do an interview.

25 Q. Right.

1 A. Because we'll never know that before the search warrant  
2 and -- we're dealing with the internet here.

3 Q. So I think you testified earlier -- so you say that it  
4 doesn't sniff data across the network in total, but you must be  
03:32 5 doing some sort of narrowing-down or winnowing process that only  
6 gets you what you're looking for which means by definition  
7 you're excluding other things, right?

8 A. No. I have a torrent. Although I'm the gatekeeper of all  
9 the torrents, each investigator has a physical torrent. They  
03:32 10 load it into a physical BitTorrent program, Torrential Downpour  
11 Receptor. It searches for download candidates and then it  
12 receives search results.

13 Done. That's it. But that's every BitTorrent client.  
14 That's different than saying like with a wiretap, a phone  
03:33 15 wiretap, you're listening to all conversations in and out. With  
16 a packet capture, as the defense expert described, that's  
17 listening to all the communication on a wire.

18 Here we are searching, issuing a search request to  
19 find IPs and receiving results and recording it. That's it.  
03:33 20 It's not like we're listening on the internet for any time any  
21 BitTorrent communication happens and I can somehow magically  
22 discern one from the other. That's not at all what happens. We  
23 just search and receive results. That's it.

24 MR. DONOVAN: Your Honor, if I could have one minute  
03:38 25 to consult with my expert.

1 (Brief pause.)

2 MR. DONOVAN: Your Honor, I don't have any further  
3 questions.

4 THE COURT: Mr. Humble, anything else?

03:38 5 MR. HUMBLE: No, Your Honor.

6 EXAMINATION

7 BY THE COURT:

8 Q. Mr. Erdely, you said that one of the concerns about allowing  
9 an expert to share or look at some of these things is that it  
03:38 10 would expose hash values?

11 A. Correct. It would expose -- it's taken years to amass the  
12 instruction files, those torrent files that law enforcement are  
13 seeking out. If any of that --

14 Q. Aren't those -- I thought those were publicly available.

03:39 15 A. They are publicly available. They're not -- but what the  
16 public doesn't know is what areas we, law enforcement, exist in.  
17 We're looking for these 500,000, 2,000 torrents. To put that  
18 out there would give them the key to not get caught. We'd have  
19 to start from scratch.

03:39 20 Q. Okay. So you don't want them to know what you're looking  
21 for.

22 A. Correct.

23 Q. The other thing is, now, Exhibits 2 and 3, the logs, are  
24 essentially downloads of the exact same video?

03:39 25 A. Yes, sir. That computer was online sharing it over two

1 days.

2 Q. Why -- I thought -- you know, if you put out the request,  
3 why does it pull in from the same person twice?

4 A. And actually you can -- there are settings to avoid that.

03:40 5 If you downloaded the whole torrent from somebody --

6 Q. Yeah.

7 A. -- in our software you can say don't try to download again.

8 But, I believe your question is more about why would -- why

9 would the same computer come to us to be overly helpful and

03:46 10 share the whole file with us the second time when they had just

11 done it the day before. Is that summarizing --

12 Q. Yes. And your initial log says we don't have any of it.

13 A. Right.

14 Q. But by that time, the time the second download happens, you

03:47 15 have it all.

16 A. Right. But that's a whole other investigative session. So,

17 to remember, and we haven't really talked about it in this

18 hearing much, IPs are dynamic. They change. I could have one

19 IP address today and another IP address tomorrow. There is

03:47 20 nothing that is going to enable me to know, even though it's the

21 same IP address, a day later. I don't know for certain it's the

22 same individual.

23 Q. Okay.

24 A. They're dynamic and can change daily or even hourly.

03:48 25 Q. Now, we just have the logs that came from the IP address of

1 the defendant. In this same investigative session is it likely  
2 that this search or this -- not so much a search, but they  
3 received -- after inputting this torrent, this hash value --  
4 received a number of other hits as well where there were other  
03:48 5 individuals now that they followed up on?

6 A. Yes. So the software isn't going to just sit there and  
7 investigate one person at a time.

8 Q. Right.

9 A. There are different programming threads that you could have  
03:48 10 multiple investigations going on at any given time. So, for  
11 instance, I could have through my web browser five tabs open  
12 with five different web pages.

13 Q. Uh-huh.

14 A. But tab 5 doesn't somehow get mixed up with tab 1. I see  
03:49 15 MSN here, I see CNN there.

16 Same concept. And Windows controls that. It's not  
17 even -- if there was an error in that, you would need to go to  
18 Microsoft and say why aren't you controlling your TCP  
19 connection.

03:49 20 Q. Yeah.

21 A. But it's separate tunnels, so to speak, separate TCP  
22 connections, so one would never get mixed up with another one or  
23 Windows is failing.

24 Q. And then lastly, I think you've covered this, but you said  
03:50 25 you had that bug maybe eight years ago or whatever and the



1 result of it was it just didn't work. It wasn't that it gave  
2 false information, it just doesn't work. Is that --

3 A. Right. It would just cause the program to stop working  
4 because -- to put it in context, Windows allows for, you know,  
03:50 5 the folder, all the folders and sub folders and the file name  
6 can't exceed 260 characters.

7 Q. Uh-huh.

8 A. So the programmer said, okay, we're gonna limit it to 260  
9 characters. That's what Windows says. But the problem is other  
03:50 10 operating systems like a UNIX or Linux environment or Mac can  
11 have even longer extensions, so we had to account for that.

12 So programmatically they're accounting for the fact  
13 that some of these paths and file names could exceed 260, which  
14 doesn't make Windows happy, but we had to account for it because  
03:51 15 BitTorrent is not just unique to a Windows computer, it runs on  
16 Mac and Linux and all these other operating systems.

17 But that was the extent of the bug. And you're right,  
18 Your Honor, it would just shut the program down. It didn't  
19 collect false information or give us false negatives or  
03:51 20 positives, it just shut down. So that's a case I will never  
21 investigate.

22 THE COURT: Okay. Any follow-up?

23 MR. HUMBLE: No, Your Honor.

24 THE COURT: All right.

03:54 25 MR. DONOVAN: I do have just a little follow-up based

1 on some of these questions and answers. And I appreciate it,  
2 Your Honor.

3 FURTHER CROSS-EXAMINATION

4 BY MR. DONOVAN:

03:54 5 Q. You would agree that an info hash is different than a hash  
6 value for a file, correct?

7 A. It is certainly different.

8 Q. So the info hash is just saying, hey, I've got this  
9 information and you want it or vice versa, and we're going to  
03:54 10 now have this handshake and hookup, right?

11 A. Well, it's more specific than a file hash. I just want to  
12 be clear. Info hash is different. It's a hash with  
13 information. But the information in hashes are the file names,  
14 the file sizes, the SHA-1 hash of every piece. So indirectly  
03:58 15 the info hash actually defines the material being traded,  
16 whether that be one file or 100 files. So it's better than a  
17 file hash.

18 Q. Okay. So that's -- so an info hash is different than a file  
19 hash, right?

03:59 20 A. Yes.

21 Q. And then a file hash is different than the file itself,  
22 right?

23 A. It's the fingerprint or signature of the data.

24 Q. But it's not the thumb, it's the thumb's fingerprint, right?

03:59 25 So it's not the same thing.

1 A. (No audible response.)

2 Q. So, in other words, if you can get a file hash, does that  
3 give you the file?

4 A. No. The file hashing is a unidirectional thing.

04:00 5 Q. It's an algorithm, right?

6 A. Right.

7 Q. It's a 40-digit hexadecimal whatever, it's not the file  
8 itself, correct?

9 A. Correct.

04:00 10 Q. Okay.

11 A. The hash points to the file.

12 Q. Now, I think you testified earlier and correct me if I'm  
13 wrong, the name of the file is inside the torrent, right?

14 A. Yes. And the [Indiscernible].

04:02 15 Q. Okay. And so, for example, like on Exhibit I believe it  
16 was -- let me just make sure I'm getting this one right.

17 So on Exhibit 5 I believe, where it says "torrent file  
18 fragments," right?

19 A. Yeah.

04:02 20 Q. And it has the -- you know, the name right there under the  
21 name column.

22 A. Yes.

23 Q. Starting, you know, "022Asian," okay?

24 A. Yes.

04:02 25 Q. And then in the source column it's got the hash file

1 torrent, right?

2 A. It's -- basically what it's done is it's named the torrent  
3 by its info hash.

04:03

4 Q. Right. So that name is inside, like you said, the hash.  
5 It's part of the information that's in the hash file.

6 A. It's part of the information in the hash, so, yes.

7 Q. But again, that's not the file itself.

8 A. That is not the file --

04:03

9 Q. And you don't contest again that the file that supposedly  
10 was downloaded here two days in a row wasn't recovered later,  
11 right?

12 A. I don't contest that. Although the other exhibit shows it  
13 was there, the MRU. That's the file, that's not the torrent.

04:03

14 Most recently used, which was Exhibit 6, show you that  
15 file name including its extension. That's when you open the  
16 file in a video player, for instance. And that was on May 22nd,  
17 after the first investigation and just before the second  
18 investigation. MRU is the file.

04:04

19 Q. Yeah. Gotcha. Now, you talked about false positives. You  
20 would agree that just because a false positive might be rare,  
21 it's not impossible, right?

22 A. Well, statistically speaking it's 1 and 1.4 quindecillion  
23 or two to the 160th power.

04:06

24 Q. That's of two hash values not matching, that's not the same  
25 thing as whether or not there might be a false positive in a

1 software, which is a type of malfunction or bug in the software,  
2 correct?

3 A. Right.

4 Q. So I'm not asking the odds of two hash values matching,  
04:07 5 which I understand is an impossibly high number, I'm saying that  
6 just because a false positive might be rare within this program  
7 that we don't have access to, doesn't mean it's impossible.

8 A. (No audible response.)

9 Q. And I can --

04:07 10 A. There's so many areas a false positive could be, you'd need  
11 to define that further. Because the data we receive as hashed,  
12 it's impossible -- or at least two to the 160th power that that  
13 is not the data that belongs to the torrent.

14 Q. Let me put it -- can I put it this way? Okay. So you have  
04:08 15 these hash values which are indicators of the file on the  
16 computer, right?

17 A. Are we -- the info hash of a torrent, is that what we're  
18 talking about?

19 Q. Or the torrent. The torrent is not the file itself, it's an  
04:08 20 indicator of the file, right?

21 A. It's the instructions to download file.

22 Q. Okay. And we also have like this, you know, again most  
23 recently used whatever with, you know, the extension, right?  
24 But again, it's not the file itself.

04:09 25 A. That's the file itself was touched which caused an entry,

1 MRU entry.

2 Q. But an MRU entry is not the file.

3 A. No, no, no, you're right.

4 Q. Okay.

04:09 5 A. It's just proof that the file was there.

6 Q. And you've speculated that the reason the file isn't there  
7 and only these indicators are there is because perhaps it was  
8 deleted, right?

9 A. Correct.

04:10 10 Q. And that's possible. It's also possible it was a false  
11 positive; that the program reported the file as being there and  
12 it really wasn't. I'm not asking again about hash matches or --  
13 I'm saying is that possible?

14 A. It's not possible because the detailed log -- there's no way  
04:11 15 he could have sent us 226 pieces with the corresponding hash  
16 values unless it was present at that moment in time on his  
17 computer. So this, I say, no, it's impossible.

18 Q. I'd like to ask you a hypothetical. Okay? Let's say the  
19 Torrential Downpour Receptor, just like every other computer  
04:12 20 program, whether it's Windows, Microsoft Excel, you name it,  
21 whatever, has a bug in it. And I understand you said there was  
22 only one. Let's say it has a bug in it, okay? And it's not  
23 performing properly. Those log files are generated from the  
24 program, correct?

04:12 25 A. Correct.

1 Q. So if there was a problem with the program there could also  
2 be a problem with those log files.

3 A. I don't -- I agree that if there's a problem with the  
4 program it could affect the log file. But what it couldn't do  
04:12 5 is make 226 pieces match. There's no possibility that the  
6 computer at that IP address didn't possess that whole file  
7 because he shared 226 matching pieces. It's not a possibility.

8 Q. But the log files which says it matched 226 pieces, fair?

9 A. It is what it says, yes.

04:16 10 Q. Okay.

11 A. And so we would have had to get wrong and have it match 226  
12 times. It's just inconceivable to me. I don't know how to  
13 better answer your question. I apologize.

14 Q. I guess my final question would be: So a false positive is  
04:17 15 possible.

16 A. Anything's possible. But statistically speaking, I don't  
17 believe it happened here.

18 Q. I understand.

19 MR. DONOVAN: I don't have any other questions,  
04:17 20 Your Honor.

21 THE COURT: All right. Thank you, Mr. Erdely.

22 THE DEFENDANT: Thank you, Your Honor.

23 (Witness excused at 4:42 p.m.)

24 THE COURT: Mr. Donovan, what would you like to do?

04:20 25 MR. DONOVAN: Well, Your Honor, I'm kinda torn.

1 Obviously I think this is complicated stuff. I think we've  
2 learned a lot today. I know my expert whispered to me that he's  
3 learned a lot today. So I think we might have some of our  
4 questions answered, but not all of them.

04:20 5 THE COURT: I'm -- you know, when you have an expert  
6 like Mr. Erdely come in, I don't get this stuff much, I don't  
7 think the government wants to produce him over and over and  
8 over, so it probably makes sense for me to write something. And  
9 if I'm going to write something on this, I think you should tell  
04:21 10 me what you -- your position after hearing the evidence.

11 MR. DONOVAN: Well, and that's what I was getting  
12 towards, is I'm -- I think I'm leaning towards I'd like to get  
13 the transcripts, have some time to review those, I guess do a  
14 follow-up, you know, brief or, you know, position.

04:22 15 THE COURT: Transcripts? Can't you give me something  
16 faster? I mean, this case has been --

17 MR. DONOVAN: I know.

18 THE COURT: This is an 18 -- when was this filed, back  
19 in July of last year? And there were a lot of delays in getting  
04:22 20 you as much as we did get. Then you got an expert.

21 MR. DONOVAN: I understand, Your Honor. And I do  
22 appreciate the Court's patience with this case because, again,  
23 at least from my perspective, this has been complicated and  
24 difficult to work through even with the expert because, again,  
04:23 25 we have an asymmetry of information here trying to figure out



1 what's going on.

2 THE COURT: What makes this case unique? I mean, we  
3 have all these child pornography cases. Is it just that he's  
4 charged with distribution and the files he was charged with  
04:23 5 distributing weren't found on the -- the files themselves were  
6 no longer -- or not found on his computer?

7 MR. DONOVAN: I think that's exactly right. I think  
8 what the big difference we have here is that they're pretty  
9 convinced that it must be because it was deleted. Okay?  
04:24 10 We're --

11 THE COURT: There were a lot of files that were on the  
12 computer, correct? I mean, there's possession charges here.

13 MR. DONOVAN: Yes, later. Yes. Count 2 relates to  
14 the search warrant and the stuff that came from the search  
04:26 15 warrant. That's a simple possession charge. Has no mandatory  
16 minimum.

17 Count 1 relates only to these two downloads from  
18 Torrential Downpour Receptor. And that's what was not located  
19 on the media. And so --

04:27 20 THE COURT: Did you know that there was -- 4, 5 and 6  
21 showed that it was on the -- or at least there's pretty good  
22 evidence that --

23 MR. DONOVAN: Well, again, these are artifacts. You  
24 know, these are indicators, these aren't the files. I mean,  
04:27 25 this is -- this is what I was trying to get on my rebuttal

1 questions there.

2 THE COURT: Yeah.

3 MR. DONOVAN: 4, 5 and 6 show things taken from the  
4 system through a -- basically a forensic program, right? And  
04:27 5 they're indicators of the file, they're not the file. I don't  
6 think it's being disputed here and I think he even admitted  
7 on --

8 THE COURT: So I guess my question is: Is this more a  
9 question of the search or are we beyond that now and this is a  
04:28 10 question of just your ability to assert your defense and --

11 MR. DONOVAN: I think it's two things. I think, one,  
12 it's the ability to properly prepare for trial, should there be  
13 a trial here, of the government witness who ran this program and  
14 says that these things were downloaded because, again, they're  
04:28 15 not later recovered, okay?

16 So the only evidence that the government's going to  
17 present about that is what this program did and what it  
18 supposedly observed and downloaded and generated logs about and  
19 all of that. That's how they're going to prove Count 1.

04:28 20 They're not going to prove Count 1 because it was  
21 located later on his computer. Count 1 is a distribution charge  
22 that carries a five-year minimum, so that's obviously the one  
23 that we're more concerned about.

24 And, I would also mention, Your Honor, what happened  
04:29 25 in Count 1 during this program running is the sole basis of the

1 search warrant that is then later used to form the basis of  
2 Count 2, to go get the warrant executed, locate whatever they  
3 locate and then charge possession.

4 So I think it relates more directly to Count 1, and I  
04:30 5 think that's what makes this case more unique than other cases  
6 where they do later recover the file or whatever. But it also  
7 does impact Count 2. And it impacts it on I think several  
8 levels, but definitely preparing for trial and cross-examining  
9 the government --

04:30 10 THE COURT: Are you suggesting that the program  
11 actually puts child pornography on the defendant's computer?

12 MR. DONOVAN: No. I don't think we have any  
13 indication of that. I'm not going to advance that. I asked a  
14 couple questions about that.

04:30 15 Again, I think the question for Count 1 is could this  
16 be a false positive, which is why it's not there when they go  
17 back later to look, versus he deleted it.

18 THE COURT: So even if it's a false positive, let's  
19 say, it's still probable cause.

04:31 20 MR. DONOVAN: Yes.

21 THE COURT: So --

22 MR. DONOVAN: So in that case it could still support  
23 Count 2. But then it would not support Count 1 because that  
24 would mean that it was never there. Count 1 is that he, on a  
04:31 25 specific date, distributed this specific file.

1 THE COURT: Well, they'd still get to a jury on  
2 Count 1 because they'd certainly be able to argue from the logs  
3 and the search of the computer, the mirrored computer, the data  
4 they have there; that he actually possessed it, he just deleted  
04:31 5 it.

6 MR. DONOVAN: Yes, I think that could get to the jury.  
7 That could be arguable. That's where we're handicapped because  
8 we don't have access to this program and can't question its  
9 reliability, accuracy. I mean, this is the problem.

04:31 10 Everything, with all due respect to the government witness,  
11 is --

12 THE COURT: Okay. Let's say it takes a week to get a  
13 transcript. When will I see your brief?

14 MR. DONOVAN: Well, Your Honor, I'm on vacation from  
04:32 15 August 23rd until September 2nd, so I think that's the day  
16 before Labor Day. I mean, I'll do it as fast as I can after  
17 that, but my, you know --

18 THE COURT: Okay. So how about September 10th. 15th?

19 MR. DONOVAN: Sure. I'm assuming that the transcript  
04:32 20 hopefully comes through.

21 THE COURT: September 15th for your brief, Mr. Humble?

22 MR. HUMBLE: Whatever you'd like, Judge.

23 I'll just say, we were told -- and I know it's on the  
24 recordings -- repeatedly when we were having these continued --  
04:32 25 what am I -- adjournments to --

1 THE COURT: Status conferences.

2 MR. HUMBLE: Correct. -- that this was dispositive;  
3 that there wasn't going to be a trial. I understand --

4 THE COURT: This motion would be dispositive.

04:33 5 MR. HUMBLE: I understand things change.

6 THE COURT: Yeah.

7 MR. HUMBLE: But it was repeatedly asserted by counsel  
8 that this was dispositive, that there wasn't going to be a  
9 trial, but this was the issue that we were basically going to  
04:33 10 battle out. Now that's not what I'm hearing. So....

11 THE COURT: Well, my sense is if he's -- if the  
12 motion's denied am I likely to see a -- then it's probably not a  
13 trial.

14 MR. DONOVAN: Well, that's exactly what I meant when I  
04:33 15 said dispositive before. Obviously if we don't get this, that  
16 changes things drastically I think from our perspective and then  
17 it probably -- yeah, I don't know at that point how we could  
18 effectively even prepare for trial. If it's granted, then that  
19 would be a different story because then we could actually maybe  
04:34 20 get even further answers than what we've gotten so far.

21 THE COURT: Yeah. 30 days after his. And the sooner  
22 the better. And then if you want to reply, 10 days later,  
23 Mr. Donovan.

24 MR. DONOVAN: Okay.

04:34 25 THE COURT: And I appreciate this is delayed, but I

1 take it there's been compliance. There's no noncompliance with  
2 conditions of bail as with most of these cases?

3 MR. DONOVAN: Correct, he's been --

4 THE COURT: And frankly I -- you know, this is very  
04:34 5 unusual. If the government needs to go through this on every  
6 child pornography case, that's -- we're going to see far fewer.  
7 You can't -- and the government has made the effort of calling  
8 an expert who frankly is acknowledged as the expert on this  
9 program. So I think since they've made that record I'll try and  
04:35 10 give you something that will have some value.

11 MR. DONOVAN: Thank you. I would just note September  
12 15th's a Sunday. Can we do September 16th which is Monday?

13 THE COURT: Sure. Any day I selected that is a  
14 weekend, take the next day.

04:35 15 MR. DONOVAN: Okay, thank you.

16 THE COURT: All right. Anything else today?

17 MR. HUMBLE: Not from the government.

18 THE COURT: All right. Thank you, all.

19 MR. HUMBLE: Thank you.

04:36 20 UNIDENTIFIED SPEAKER: Thank you, Your Honor.

21 (Hearing adjourned at 4:49:46 p.m.)

22 \* \* \*

23

24

25

C E R T I F I C A T E

I, JOHN T. SCHINDHELM, RMR, CRR, Official Court Reporter and Transcriptionist for the United States District Court for the Eastern District of Wisconsin, do hereby certify that the foregoing pages are a true and accurate transcription of the audio file provided in the aforementioned matter to the best of my skill and ability.

Signed and Certified August 30, 2019.

/s/John T. Schindhelm

John T. Schindhelm

John T. Schindhelm, RPR, RMR, CRR  
United States Official Reporter  
517 E Wisconsin Ave., Rm 236,  
Milwaukee, WI 53202  
Website: WWW.JOHNSCHINDHELM.COM



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

I N D E X

<u>WITNESS</u>	<u>EXAMINATION</u>	<u>PAGE</u>
PEYTON ENGEL, DEFENSE WITNESS		
	DIRECT EXAMINATION BY MR. DONOVAN.....	3
	CROSS-EXAMINATION BY MR. HUMBLE.....	37
	REDIRECT EXAMINATION BY MR. DONOVAN.....	45
ROBERT ERDELY, GOVERNMENT WITNESS		
	DIRECT EXAMINATION BY MR. HUMBLE.....	50
	CROSS-EXAMINATION BY MR. DONOVAN.....	90
	EXAMINATION BY THE COURT.....	114
	FURTHER CROSS-EXAMINATION BY MR. DONOVAN.....	118

\*\*\*\*\*

E X H I B I T S

<u>NUMBER</u>	<u>DESCRIPTION</u>	<u>OFFERED</u>	<u>ADMITTED</u>
1	Erdely CV.....	50	50
1	CV of Robert Erdely.....	90	90
2	Investigative log for download 5/21/18.....	90	90
3	Investigative log for download 5/22/18.....	90	90
4	Installed Programs.....	90	90
5	Torrent Files.....	90	90
6	MRU Recent Files and Folders.....	90	90