Cross Examination of Digital Experts

1. **Introduction**
    a. Basic concepts of cross that apply across digital fields
        i. Strategic plan: to attack or not to attack
        ii. Challenge the applicability in your case
        iii. Challenge the science
        iv. Challenge the expert's qualifications and bias

2. **Cell Site Evidence**
    a. Strategic plan:
        i. How much does the location matter?
        ii. Is there an alternate explanation for client's location?
        iii. Can you use the location data to help you?
    b. Expand your thinking - look at a greater timeline than the prosecution
        i. Finding patterns
        ii. Look for times when client was in same location that is innocent

C. When the prosecution generalizes - specify
    I. The prosecutor will pick and and choose and put your client in the area
    Ii. The area contains a lot of things - where exactly is the tower?

D. cell site evidence is VERY far from specific
    I. expanding the area
    Ii. explaining the direction of the towers

E. The science - it isnt - its tech and hard to challenge
    I. better to cast doubt on the accuracy
    Ii. Find "jumps" - data that makes no sense

3. **Cell Phone Forensics**

A. Cellebrite
    a. The science and how to challenge it
        i. How does it work?
        ii. Discovery
            1. CelleBrite "extraction summary report" (usually) a .pdf, .xls, or .html file). This isgenerated by the UFED software but can be controlled by the DT and should accompany folders containing the data described in the report.
            2. The investigating detectives "summary report." This is generally a typewritten description of the request, the search

performed/actions taken, and the results. It should mention the ADA requesting the search, the nature of the investigation, and the voucher numbers of the items searched.

3. Handwritten “lab notes.” These are handwritten notes that should accompany the “summary report” and should describe the dates/times each action was taken and the results.
4. The “Forensic Mobile Phone Submission form.” This is the request by the DA to the DT examining the mobile device.
5. Grand Jury Minutes from the Investigating detective. It is usually a combination of the AO and the DT examining the device that make out the basis for the warrant.
6. The search warrant or consent/written consent to search form.
7. Photographs of the device.

iii. What can be extracted - live data vs hidden
   1. Live data = typical user info SMS, MMS, video, email, etc
   2. Hidden data = typical user cannot see e.g. web history, email headers, picture data

Iii. Type of extraction matters -
   1. Logical image extraction = picture of all live data
   2. File system extraction = copy of all live files and all hidden data

Iv. What was extracted and what was reported?
   1. The investigator can control was is extracted
      a. By type - SMS, apps, MMS, emails etc.
      b. By time frame
      c. Review contents of report to determine what if any limitations were placed on the search
   2. How does this impact your case?
      A. Is there missing data
      B. Did client communicate over multiple mediums - e.g. SMS and MMS within one text feature

b. The expert - qualifications
   i. Expert or fact
   ii. Ayers, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 (Revision 1May, 2014).

iii. CelleBrite currently has four levels of certifications in addition to miscellaneous certifications. These include:
    1. beginner - The CelleBrite Mobile Forensic Fundamentals Online course (CMFF);
    2. intermediate - The CelleBrite Certified Logical Operator (CCLO)
    3. advanced- The CelleBrite Certified Physical Analyst (CCPA) and
    4. highest level- The CelleBrite Certified Mobile Examiner(CCME).

B. What's on my phone?
1. Apps
2. Location data
    a. Google map tracking
3. The CLOUD!

4. **<u>Computer forensics</u>**
a. What matters? - Typically any offense includes demonstration of knowledge or intent
b. As an average computer user what do you know is on your drive?
    i. Human searches - discerning them from other searches
        1. URL = google/yahoo/bing
        2. If it doesn't - what is it? Might not be a person generated search

    ii. Beware of cookies!
        1. Explain cookies in a way the jury can understand: e.g. you searched for a pair of black boots on Zappos, the next time you sign into Facebook you see an ad for black boots. Those are cookies.
        2. Stored in the browser without your knowledge
        3. Look at searches in combination with cookies - is there an innocent explanation?
            a. Gov says client charged with sexual assault possessed 370 images of vaginas - how to explain?
            b. Client's wife searched "symptoms vaginal pain"
            c. All but 2 of the images are contained in cookies

C. Don't forget the obvious -
    i. Who has access to the computer
    Ii. Was the image or other file sent to the person?

Iii. Auto save and cloud uploads? Settings and knowing control