8. Evaluation and Presentation

Digital Forensics and Cybercrime course

Prof. Zanero

The evaluation phase

- Need to match the **evidence elements** (~facts) with the required legal elements to support (or negate) a legal theory
- E.g. the law punishes “willingly detaining child pornography”?
  - Child pornography: we can scan drives for images, and then have (if needed) a doctor attest to the age of subjects
  - Willingly detaining: we can use elements like access dates, conservation in folders, sorting...

Items to evaluate

- The elements to support the indictment
- Alternative explanations to the elements
- Analyzing what can be said, what cannot, and what further experiments would be needed to say more
  - The latter is important to analyze whether these experiments will be performed by the counterpart, and whether performing them or asking for them to be performed entails risk

Relationship with lawyers

- Lawyers own the choice of defense strategy
  - They may ask for the expert's counsel
  - But the expert must yield to them
- Lawyers own the relationship with the client
  - Experts should never tarnish this relationship
  - If you are unable to do this, you need to resign
- Lawyers (and customer) pay your bill, but do not dictate what you write or say
  - You should always write and say only that of which you are personally convinced
  - You may be asked to omit a finding, as long as this omission is not the same as lying.

Relationship with the customer

- The expert assists one of the parts in the judgment
  - Mandate: finding what helps the customer
- This is not the same as “helping someone escape law”: this is part of the due process of applying law
- “Process truth” is not the same as historical truth

Relationship with prosecutors/police

- Assisting the prosecutors or the police does not entail moral superiority
- Still very important to stick to science and facts
- Important not to get your words or thoughts shaped by “justice”

Evaluation: analyzing the documents

- A key component of the evaluation process is reviewing documents and evidence already presented in the proceedings
  - In particular, written reports of other expert witnesses and investigators
- What to look for:
  - Technical/factual errors (or omissions)
  - Unclear reasoning, methodologies or descriptions
  - Suggestive writing
  - Opinions and hypotheses not clearly distinct from facts and not substantiated

Typical technical and factual errors

- Acquisition
  - Search and seizure: process, chain of custody, seals,
  - Description of seized/analyzed materials: serial numbers, etc
  - Hashing/cloning procedure (e.g. use of write blockers)
- Analysis
  - Steps where hashing was not verified
  - Proprietary programs; bugs and vulnerabilities
  - Description of the process
  - Technical mistakes (of course!)

Typical presentation errors

- No exploration of alternative hypotheses
  - What **else** could explain the facts? What's the best alternative theory?
  - Cliché: trojan defense
- Is the presentation neutral or biased?
- Can we find counter-examples for some of the assumptions?
- Are there missing explanations that we can provide in order to shift the understanding of the judge?

Presentation: writing your report

- First and foremost **be clear**
  - Focused on the items you want to explain, concise
  - If in national language: do not exceed in english terminology
  - All technical terminology must be explained, if necessary in a footnote
  - You need to be **simple** without being **simplistic** and without giving the reader the (right) impression that you are simplifying things for them
- You must explain **why** what you are saying is relevant **to the reader** (i.e. the judge). **It is not obvious to them!**

How not to write a report

- Don’t be apodictic: “This does not work”. Why doesn’t it? Maybe it’s obvious to you but not to the reader
- Don’t suggest, don’t use innuendo
- Don’t be too technical, you will not sound more expert, you will be ignored
- Don’t show bias or solidarity with your client, with the aggrieved party or the victim, you are a scientist and must be cold and factual
- Don’t show excessive deference to the judge
- No sarcasm (but if you are **very** sure of yourself and you want to aim low, you can use a little bit of irony)
- Don’t use weak arguments if you have more solid ones

Structure of a report

- Model it on a scientific paper or report
  - Introduction - tell them what you are going to say
  - Facts
  - Discussion and analysis - each block with a small introduction saying what you want to explain and a conclusion summarizing what you just describe
  - Final conclusions where you leave out any doubtful statement: just distilled, iron truth
- Structure it like an obstacle course, each obstacle a little taller than the previous one
  - Make the judge sweat to ignore all of your obstacles

Structure of a report (example)

1. Foreword
   - I have examined these documents and these evidence sources
   - I was asked to report on X
2. Introduction
   - In this report, we are going to show A, B, C, D, and these are all related to the question X because…
3. Acquisition issues
   - Preliminarily, we want to observe the following on acquisition…
   - Hashes were not computed, **and therefore** this, this and this could have happened (don't stop at "computed." and don't count on chain of custody)

Structure of a report (example)

4. On the technical analysis
   - **Even ignoring** all of our fundamental issues with the evidence integrity…
   - The connection was not from A to B, but rather to C, this changes the reconstruction like this, and also makes these paragraphs of the adversarial report wrong (don't stop at "C.")
   - **Even ignoring** these factual errors, the evidence is not best explained as the adversary did, but rather is much more compatible with these other explanations
   - The following experiment has not been performed, or the following evidence is missing, and it could...

Structure of a report (example)

5. Conclusions
   - **(the only thing most judges will consider)**
   - In this report we have shown
     - Evidence was not properly acquired and **thus these manipulations may have contaminated it**
     - Item I did not happen as described, making conclusion C completely wrong (don't fix it for them)
     - Theory T fits the facts better
     - Nobody checked if F was true or false, which could have led to G
   - **We must therefore conclude that … (one strong, inevitable phrase)**

Testimony as a witness

- In many jurisdictions the expert may just submit a report, but **may** be called as witness
- In others, like in Italy, they **must** be called as a witness and then can submit their report
- In most jurisdictions, the expert witness provides a **sworn testimony** and can commit **perjury**
- This means that, depending on jurisdiction, an expert witness cannot lie or claim confidentiality or professional secrecy

Direct examination

- Usually you are called by your side and thus proceed to friendly direct examination
  - Prepare: have a script with your side's lawyer
  - Be clear and very helpful
  - Make sure you explain everything to the judge
  - Take your time (but don't overdo it)
  - In some jurisdictions (including Italy) judge can ask questions of their own: prepare; check previous records of the judge
- Relax and don't be nervous, because you now need to stand cross-examination

Cross examination

- Examination by the counterpart is less friendly, sometimes downright hostile
  - Prepare: check previous records of the lawyer, prosecutor or judge
  - Use your report as a shield and as a way to get time and think about the answer
  - Be curt if you can: “yes” “no”
  - If you cannot, be very complex and difficult to understand
  - If unexpectedly a question is positive, immediately go back to being extremely clear and helpful
  - Don’t get angry
  - Don’t be surprised if your competency is called into question