

# Expert Evidence in Practice

# Expert witness for prosecution

- Prosecution seizes equipment and maintains relevant information about its owner, state (powered-on or off), location, etc.
- Each equipment is bagged, tagged and identifiable
  - Forensic disk image is made for analysis
  - Original device is repacked for archiving
- Expert witness has access to copies of devices

# Expert witness for prosecution

- In contact with the primary investigator, need to know
  - Why raid took place
  - Overview of computer and devices where data is stored
  - Idea of the technical capability of the suspects
  - Keyword searches based on the user skills
- Part of the investigation team
  - See things differently than a police officer
  - They advise the police officer

# Expert witness for Defence

- Things are different
  - Only come to know when contacted by a defence lawyer
  - Have initial information
  - Suitable financial arrangements need to be agreed with the client
  - Major focus is on testing of the evidence

# Expert witness for Defence

- Expert work has to be on the basis of the court proceeding
  - Presentation and cross examined
  - Explain the strengths and weaknesses of the prosecution evidence
    - Statistically, most often prosecutions have strong cases.
    - If evidence is overwhelming – then you may advise the defendant to plead guilty
  - Jurists may not know much about computers
    - They need to clearly see what they can agree on

# Illustrative real case studies in practice

# Case 1: Illegal sexual images

- Prosecution found indecent sexual images of children on someone's computer.
- Upon careful examinations and correlations of relevant evidence, such as pictures, logs and emails, defence forensic expert was able to show that
  - Pictures were not knowingly downloaded from a particular adult website.
- Case collapsed.

# Expert advice

- It is essential to confine yourself to the scope of your area of expertise and not to cross its boundaries.
- After examining someone's computer, a Digital Forensics Expert may make statements about hidden indecent sexual pictures of children found on its hard disk but should not make statements relating to whether somebody is a paedophile because this is outside the expert's domain.
- In some countries, however, an expert has to be specifically registered as an expert by an independent body before they can give evidence.



## Case 2: Images of terrorists

- Prosecution found images of well known terrorists on someone's computer.
- Upon careful examinations and correlations of relevant evidence, such as images, logs, cache and browsing histories, defence forensic expert was able to show that
  - Pictures were not deliberately downloaded from specific terrorist websites.
- Case collapsed.

## Case 3: Time stamps

- Using different forensic tools, prosecution and defence obtained contradicting versions of the timeline of events involving mobile evidence.
- Upon careful examinations, both parties agree that the evidence could not be relied upon.
- Prosecution won the case but on the basis of other evidence.

## Case 4: Print spooler

- Accused: is a minority police officer who had a troubled relationship with some of his colleagues
- Prosecution charge: accused sent a racist document to himself to implicate his colleagues of racist behaviours
- Evidence: Printer spool file & its size
- Defence: computer forensics expert was able to show that the size of the printer spool file did not relate to the document sent
- Outcome: prosecution case collapsed. This had big political implications at the time.

Thank you!