CS593: Digital Forensics

Lecture 2: Digital Forensics Concepts

D. Kevin McGrath

Thursday, July 6, 2023

Outline

- What is digital forensics?
- Principles of the scientific method.
- Relevance and quality of evidence.

What is Digital Forensics?

- *Forensics*: The application of science to legal problems and investigations.
- *Digital forensics*: A branch of forensics involving the recovery and investigation of digital evidence.
- *Digital evidence*: Data stored or transmitted using a digital device that are relevant to a legal investigation.

Subdisciplines of Digital Forensics

- *Computer forensics*: forensics related to individual computers.
- *Network forensics*: forensics related to network components.
- *Mobile device forensics*: forensics related to cell phones, tablets, GPS devices, etc.

Professions that Use Digital Forensics

- Digital forensics examiners.
- Lawyers.
- Network security analysts.
- Military intelligence.
- Data recovery specialists.
- Software engineers (writing digital forensics tools).
- Librarians/archivists.

Scientific Method

- Make observations and learn background.
- Form hypothesis.
- Experiment.
- Analyze results.
- Draw conclusions and report findings.

Selecting a Good Hypothesis

- A scientific hypothesis should be:
  - *Falsifiable*: It must be possible to show the hypothesis to be false, by some feasible test.
  - *Consistent*: The hypothesis must be consistent with all previous observations.
  - *Simple*: Other considerations being equal, a simpler hypothesis should be preferred.

Designing Good Tests for Digital Forensics

- Should have a high chance of refuting or confirming the hypothesis.
- Must be tractable.
- Should use sound techniques.
- Could be passive examination or active experimentation (live or online forensics).

Refutation

- *Refutation*: Tests to confirm the hypothesis should include tests to try to refute the hypothesis.
- *Confirmation bias*: We tend to design tests more likely to confirm our assumptions.
- Should not conclude guilt unless all other viable explanations are refuted.

Example

- Hypothesis: “Adam downloaded illegal content from website X.”
- Evidence of guilt: “Network analysis shows him downloading data from site X.”
- Refutation evidence: “Further examination shows the data were served through a banner ad while Adam was shopping for yarn for his kitten orphanage.”

Reporting and Testimony

- Digital forensics reports should target general lay audience; assume no background.
- Should never explicitly assert a party is guilty or innocent.
  - Only present and explain evidence.
  - Deciding on guilt is up to judges and juries.
  - Tell a story, but leave the conclusion blank.

Circumstantial vs. Direct Evidence

- *Direct evidence* shows that an event occurred.
- *Circumstantial evidence* implies that an event occurred, but other explanations are possible.
- Multiple pieces of circumstantial evidence must be corroborated to form a direct link.

Circumstantial Digital Evidence

- Digital evidence is usually circumstantial.
- Digital evidence links computers to events.
- Linking a person to an event requires additional evidence.
- E.g., digital evidence directly links a computer to an event, but only circumstantially links the computer's owner to the event.

Forensic Soundness

- *Forensically sound* is roughly equivalent to “best practice.”
- Document all steps in handling and analyzing evidence.
- Ensure evidence is not damaged/altered.
- Analysis must be objective and unbiased.
- Unrelated to distinction between circumstantial and direct evidence.

Evidence Integrity

- Should ensure evidence is not damaged or altered.
- Any alteration must be precisely documented.
- Avoid loss of evidence.
- Avoid introducing artifacts that may confuse investigation.

Cryptographic Hash Functions

- Take arbitrary input, output a fixed-sized hash value.
  - Collision resistance.
  - Pre-image resistance.
  - Second pre-image resistance.
- Evidence integrity can be verified by re-computing crypto hash and comparing the earlier and later hashes.

Chain of Custody

- Documentation of every person who handles the evidence.
- Several people will likely handle the evidence before the digital forensics examiner does.
- Incomplete documentation could result in inadmissible evidence.

Summary

- What is digital forensics?
- Scientific method.
- Evidence principles.

Videos about Forensics

- Google TechTalk on “A Geek’s Guide to Digital Forensics” (56 minutes): https://www.youtube.com/watch?v=rPd-HiEvhhw&feature=youtu.be
- Mikko Hypponen TED talk on the general state of cyber crime (18 minutes): http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net?language=en

Questions?