Chapter 9

Evidence Handling

Ed Crowley

Spring 10

Topics

- Evidence Defined
- Best Evidence
- Original Evidence
- Evidence Handling Procedures

Intro

- If a computer security incident leads to a court proceeding, the digital evidence and documents obtained may be used as trial exhibits.

What is Evidence?

- According to the Federal Rules of Evidence (FRE), relevant evidence is defined as any information:

  "having a tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the information." (FRE401)

  - Anything of probative value, meaning it proves something or helps prove something relevant to the case.
  - See also the online manual:

    "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Proceedings".

`http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm`

Best Evidence Rule

- The best evidence rule essentially requires that, absent some exceptions in order to prove its contents the original of a writing or recording must be admitted in court.

Rule 1001 (3) provides:

- “[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original”.

Informal rule

- Best evidence is the most complete copy of evidence that we have obtained that is closest linked to the original evidence.

Original Evidence

- To ensure due diligence, it is prudent to always assume a case will end up in a judicial proceedings.
  - Handle evidence accordingly.

Original evidence

- The original copy of the evidence media provided by a client/victim.

Best evidence

- Original duplication of the evidence media, or the duplication most closely linked to the original evidence.

Challenges of Evidence Handling

- Failure to adequately document the response to a computer security incident.
- Properly retrieved evidence requires a paper trail.
- Properly collecting evidence is a big challenge
  - Must be authenticated at a judicial proceedings and
    1. Chain of custody for the evidence must be maintained.

Authentication of Evidence

- The FRE, as well as many state laws, define computer data as “writings and recordings”.
- Before they may be introduced into evidence, documents and recorded material must be authenticated.
  - Authentication, defined in FRE 901(a) basically means that whomever collected the evidence should testify during direct examination that the information is what the proponent claims.
  - You meet the demands of authentication by ensuring that whomever collected the evidence is a matter of record.

Chain of Custody

- Maintaining chain of custody requires that collected evidence be stored in a tamper proof manner.
  - Not to be accessed by unauthorized individuals.
- You need to maintain positive control (evidence within your possession or within your sight at all times) of all best evidence.
  - Until it can be hand carried or shipped to evidence custodians for proper storage.
- Your organization's best evidence should always be stored within a safe or storage room that is inaccessible to anyone other than the appointed evidence custodian(s).
  - Area referred to as an evidence safe

Evidence Custodians

- Any employee can collect and transport evidence, but only evidence custodians can inventory evidence and ensure it is properly stored.

Evidence custodians required to:

- At all times, know the location of all best evidence
- For areas that store best evidence, maintain custody of all keys and lock combinations
- Document all receipt and transfers of best evidence.
- If your organization's evidence handling procedures are ever challenged, you will need to provide testimony to defend your practices.

Evidence Validation

- For each file, generate a MD5/SHA-1 hash
  - Performed at file acquisition time.

Evidence Handling Procedures

- Examine drive contents
- Take digital photos
- Fill out evidence tag
- Label all media
- Store best evidence copy of evidence media in your evidence safe
- Evidence custodian enters a record of the best evidence into the evidence log.

- All examinations are performed on a forensic copy of the best evidence (working copy).

Evidence custodian:

- Ensures that backup copies of best evidence are created.
- Ensures that all disposition dates are met.
- Performs a monthly audit to ensure all of the best evidence is present, properly stored, and labeled.

Evidence System Description

Prior to gathering electronic evidence, the following should be recorded:

- Individuals who:
  - Occupy office or room where the original evidence is found.
  - Have access to the area where the original evidence is found.
- Users who could actually access the system
- Physical computer location
- State of the system
  - System BIOS Time/date
  - Network connections
  - Processes and ports
  - Attached system peripherals.
- Individuals present at the time of the forensic duplication
- Serial numbers, models, makes of HD and system components.

Digital Photos

Photograph the evidence system.

- Ensure against damage claims.
  - Establish what was connected and part of system.
- Capture current configuration
- Good idea to photograph all network and phone connections, as well as everything else…

Evidence Tags

Include the following information:

- Place of persons from whom the item was received
- If the item requires consent to search
- Description of item taken
- If the item is a storage device, information contained within
- Date and time when item was taken
- Full name and signature of individual initially receiving the evidence
- Case and tag number related to evidence

Evidence Labels

- If labeling original evidence, suggested that you mark your initials and data on original drive.
- Case number and evidence tag number
- Date and time evidence was collected
- Brief description of items contained within the envelope

Other

Evidence storage

- At the very least, the container must be able to show signs of tampering by parties outside the chain of custody.
- Evidence must also be protected from alteration by the environment.
- Shipping
- Evidence must be packaged in a tamper proof, static proof, padded container and shipped via a carrier that provides tracking capability.

Evidence Safe

- Prevents tampering or unauthorized access to the documents, data, or physical evidence that may be critical to your case.

Evidence Log

- Contains a complete inventory of all the evidence contained within the safe.

Working Copies

- If your organization has numerous initial responders that perform forensic duplications and then forward their duplications to an evidence custodian, a good policy is to have those investigators be responsible for making the working copies of the best evidence.

Evidence Backups and Disposition

- In order to minimize impact from equipment failure or natural disasters, it is prudent to create backups of all electronic evidence.
  - Store redundant backups in separate locations.
- Initial disposition occurs when the final investigative report has been completed and the analysis is finished.
- Final disposition of evidence occurs five years from the date a case was initially opened unless otherwise directed by law, the court, or some deciding body.

Evidence Custodian Audits

- Evidence custodians should perform a monthly audit to ensure that all best evidence is present, properly stored, and labeled.
- For evidence related forms, (from Foundstone) see Appendix B in the Mandia text.

Questions?