COMP 2555 Principles of Computer Forensics

Lecture 15

Ramki Thurimella, PhD

Overview

- Midterm grades will be given on Wed
- Project 3 on backup to be assigned on Wed
- Cover Chapter 7 Duplication & Preservation of Digital Evidence
- Start Chapter 8 Computer Image Verification & Authentication

Emergency Guidelines

- Don’t operate the subject computer
- Don’t solicit the assistance of the resident “computer expert.”
- Don’t evaluate employee email unless corporate policy allows it

Scientific Evidence Standards

- Federal Rules of Evidence (FRE) 401 Relevancy Test
  - "Relevant evidence" evidence having any 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 evidence.

Scientific Evidence Standards (cont.)

- Daubert Standard (supersedes Frye)
- Trial judges must evaluate whether the testimony is both "relevant" and "reliable", a two-pronged test of admissibility:

  1) The relevancy prong: Whether or not the expert's evidence "fits" the facts of the case, e.g. an astronomer might tell the jury if it had been a full moon on the night of a crime. However, the astronomer would not be allowed to testify if the fact that the moon was full was not relevant to the issue at hand in the trial.

  2) The reliability prong: The Supreme Court explained that in order for expert testimony to be considered reliable, the expert must have derived his or her conclusions from the scientific method:
  - Empirical testing: the theory or technique must be falsifiable, refutable, and testable.
  - Subjected to peer review and publication.
  - Known or potential error rate and the existence and maintenance of standards concerning its operation.
  - Whether the theory and technique is generally accepted by a relevant scientific community.

Scientific Evidence Standards (cont.)

- Marx Standard
  - Can the technique and its results be explained with sufficient clarity and simplicity so that the court and the jury can understand its plain meaning? This is just the Marx standard, which is assumed to be incorporated in Daubert as it was with Frye.

Scientific Evidence Standards (cont.)

- Coppolino standard (Coppolino v. State 1968)
  - The court allows a novel test or piece of new, sometimes controversial, science on a particular problem at hand if an adequate foundation can be laid even if the profession as a whole isn't familiar with it.

Representational Accuracy

- In the context of scientific evidence standards,
  - No need to present all the originals
  - If data from a computer or similar device
    - Any printout is acceptable

Evidence Processing Steps

- Collect volatile data
- Shut down
- Document hardware configuration
- Transport to secure location
- Take an image
- Compute hash values of data on the drive
- Document the system data and time
- Make a list of keywords to be searched

Evidence Processing Steps (cont.)

- Evaluate the swap file
- Evaluate file slack
- Evaluate unallocated space (erased files)
- Search files, slack, and unallocated for keywords
- Document file names, dates, and times
- Identify file, program, and storage anomalies
- Evaluate program functionality
- Document your findings
- Retain copies of software used

Evidence Processing in Detail

- Take photos
  - screen image
  - Hardware
  - Label wires
- Time is of the essence:
  - Password-protected screen might activate

Evidence Processing in Detail (cont.)

- Document the system date and time settings
- Given the size of hard drives, one can only do searches on keywords
  - Make a list
  - Need a good search engine
- Add more keywords to supplement the previous ones to search the unallocated space
- Sort files
  - By name
  - By last accessed times
  - Size
  - Type

Evidence Processing in Detail (cont.)

- Search will fail on
  - Encrypted files
  - Compressed files
  - Graphic images
- Look for hidden partitions
- If a destructive process is found, proves willfulness
- Duplication of software process
  - Keep tools used
  - Software evolves and might not have access to older versions

Legal aspects

- Chain of custody shows how
  - Evidence was collected
  - Analyzed
  - Preserved
- Therefore, requires a proof that
  - No information has been added or deleted
  - A complete copy was made
  - A reliable copying process was used
  - All media was secured

Legal aspects (cont.)

- Logs, otherwise considered hearsay, are admissible as long as they are collected *in the course of regularly conducted business activity*
- Digitally sign the logs

Legal aspects (cont.)

- Key to establishing a user has no right to privacy (CERT advisory suggestion)
  - This system is for the use of authorized user only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel.
  - In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored

Legal aspects (cont.)

- Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials

Legal aspects (cont.)

- Supreme Court ruling in O'connor v. Ortega
  - The legality of workplace monitoring depends on
    - Whether policies exist
    - Whether those policies have been clearly communicated to employees

Legal aspects (cont.)

- Incident coordinator, must record at a minimum
  - Who initially reported, when, and circumstances surrounding the incident
  - Details of the initial assessment
  - Names of the persons conducting the investigation
  - The case number
  - Reasons for the investigation

Legal Aspects (cont.)

- List of all computers, tag numbers, along with complete system information
- Network diagrams
- Applications running on these systems
- A copy of the use policy for these systems
- List of admins responsible
- Details list of steps
- ACLs of who had access
- Separate notebooks for diff incidents
- No spiral bounds

Legal Aspects (cont.)

- Encase v. freeware?
- Store in a secure area with
  - Video surveillance
  - Access control cards