

# Computer Forensics



## Chapter 23

### Background

- **Forensics**
  - The application of scientific knowledge to legal problems.
- **Computer forensics**
  - Preservation, identification, documentation, and interpretation of computer data.
  - Conducted for three purposes:
    - Investigating and analyzing computer systems as related to violation of laws.
    - Investigating and analyzing computer systems for compliance with an organization's policies.
    - Incident Response- Investigating computer systems that have been remotely attacked.



## Background

---

- Computer forensics actions
  - May deal with legal violations
  - Investigations could go to court.
  - Minor procedural missteps have significant legal consequences.



## Computer Forensics

---

- The preservation, identification, documentation, and interpretation of computer data
- Reasons to perform computer forensics
  - Investigate systems as related to violation of laws
  - Ensure compliance with organization's policies
  - Investigate systems victimized by remote attacks
- Be aware of legal implications and seek counsel when needed

## Incident Response Cycle

- Discover and report
  - Administer an incident response reporting process
- Confirm
  - Specialists review incident report and confirm occurrence
- Investigate
  - Response team investigates incident in detail
- Recover
  - Systems and applications returned to operational status
- Lessons learned
  - Action items to correct weaknesses and make improvements

## Incident Response Cycle (*continued*)





## Evidence

---

- Evidence
  - Documents, verbal statements, and material objects admissible in a court of law.
  - Critical to convince management, juries, judges, or other authorities that some kind of violation has occurred.
  
- Computer evidence
  - More challenging since data cannot be perceived with physical senses.
  - One can see printed characters, but cannot see the bits where that data is stored.
  - Often of concern to auditors.
  - Good auditing techniques recommend accessing the original data or a version as close as possible to the original data.



## Standards for Evidence

---

- Credibility standards:
  - **Sufficiency:** The evidence must be convincing or measure up without question.
  - **Competency:** The evidence must be legally qualified and reliable.
  - **Relevancy:** The evidence must be material to the case or have a bearing on the matter at hand.



## Types of Evidence

- **Direct evidence**
  - Oral testimony that proves a specific fact, such as an eyewitness' statement.
- **Real evidence**
  - Physical evidence that links the suspect to the scene of a crime.
- **Documentary evidence**
  - Evidence in the form of business records, prints, and manuals.
- **Demonstrative evidence**
  - Used to aid the jury and can be in the form of a model, experiment, or chart, offered to prove that an event occurred.



## Three Rules Regarding Evidence

- **Best Evidence Rule**
  - Courts prefer original evidence rather than a copy to ensure no alteration of the evidence has occurred.
- **Exclusionary Rule**
  - Must have been gained in accordance with all laws
- **Hearsay Rule**
  - Hearsay is second-hand evidence
  - Second-hand evidence may not be allowed
  - However, Important as most computer-generated evidence is classified as second-hand



## Collecting Evidence

- Credibility of evidence relies on proper
  - Acquisition
  - Identification
  - Protection against tampering
  - Transportation
  - Storage

Important



## Acquiring Evidence

- Data should be gathered as quickly as possible.
  - Attacker may attempt to cover their tracks.
  - Data may be tampered with or destroyed.
- Search under the keyboard, desktop storage areas, and cubicle bulletin boards for relevant information
- Secure Floppy disks, CDs, flash memory cards, USB drives, tapes, and other removable media
- Request and maintain copies of logs
  - Most Internet service providers (ISPs) protect logs that could be subpoenaed.
- Photographs or videotapes
  - Include operating computer screens and hardware components from multiple angles.
  - Photograph internal components before removing them for analysis.




## Acquiring Evidence

- When an incident occurs and the computer being used needs to be secured, the following two things should be considered:
  - Whether or not it should be turned off.
  - Whether or not it should be disconnected from the network.



## Acquiring Evidence

- Option 1: Freezing the current state of the computer
  - Some forensics professionals state that the plug should be pulled in order to freeze the current state of the computer.
  - However, this results in the loss of data associated with an attack from the machine. This may also result in the loss of any data in RAM.
  - Further, it may corrupt the computer's file system and could call into question the validity of the findings.
- Option 2: Shutting down or restarting the system
  - A software bomb
  - Management's reluctance
- Therefore, from an investigative perspective, either of the courses may be correct or incorrect, depending on the circumstances surrounding the incident.

- 
- Acquiring evidence:
    - **Never examine a system with the utilities provided by that system.**
    - Always use utilities that have been verified as correct and uncorrupted.
    - Do not open any files, or start any applications.
    - Document the current memory, swap files, running processes, and open files.
    - Unplug the system from the network, and immediately contact the management.
    - Follow the Computer Incidence Response Team (CIRT) procedures.
    - Capture and secure mail, Domain Name Service (DNS), and other network service logs on supporting hosts.



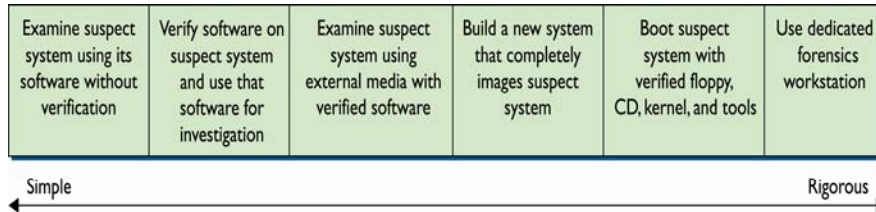
## Volatility of Data

1. Data can be very volatile
2. Forensics experts debate about the best ways to approach securing the data.
3. In general data can be classified from the most volatile to the most persistent as follows:
  - CPU storage (registers/cache)
  - System storage (RAM)
  - Kernel tables
  - Fixed media
  - Removable media
  - Output/hardcopy



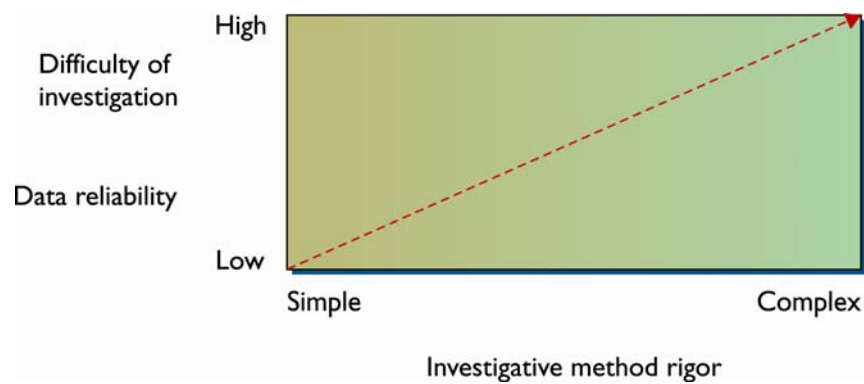
## Investigative Method Rigor

There are many investigative methods.  
The figure shows the range of investigative methods from simple to more rigorous



## Investigative Method Rigor (*continued*)

- There is a relationship between the complexity of the investigation and both the reliability of the forensic data and the difficulty of investigation.





## Identifying Evidence

- Must be properly marked when collected
  - Be methodical.
  - Work in teams rather than individually.
    - Do not collect evidence by yourself—have a second person witness the actions.
  - Keep thorough logs during seizure and analysis.
- Characteristics of proper record keeping
  - Labels are difficult to remove and match log book.
  - Identifies the who, what, when, where, and why related to the collected evidence.
- The information should be specific enough for recollection later in the court.
  - Log other identifying marks, such as device make, model, serial number, and cable configuration or type.
  - Note any type of damage to the piece of evidence.



## Protecting Evidence

- Protect evidence from electromagnetic or mechanical damage.
  - Ensure that the evidence is not tampered, damaged, or compromised by the procedures used during the investigation.
  - Do not damage evidence – Avoids liability problems later.
  - Protect evidence from extremes in heat and cold, humidity, water, magnetic fields, and vibration.
  - Use static-free evidence protection gloves, not standard latex gloves.
  - Seal the evidence in a proper container with evidence tape.



## Transporting Evidence

---

- Properly log in and out of controlled storage.
- Chain of custody must be maintained.
- Ensure evidence is properly packaged.



## Storing Evidence

---

- Evidence
  - Static-free bags
  - Foam packing material
  - Cardboard boxes
- Evidence room
  - Restricted access
  - Entry-logging capability
  - Camera monitoring



## Conducting the Investigation

- Never analyze the original target system.
  - Make multiple images of original to be used to analyze and authenticate the data.
  - Use a system specially designed for forensics examination.
- Keep thorough and precise notes of all actions.
  - Notes may become evidence in case.
- Conduct analysis in a controlled environment with:
  - Strong physical security
  - Minimal traffic
  - Controlled access



## Conducting the Investigation

- Unless there are specific tools to take forensic images under Windows, DOS should be used for imaging process instead of standard Windows.
- Boot it from a floppy disk or a CD, and have only the minimal amount of software installed to preclude propagation of a virus or the inadvertent execution of a Trojan horse or other malicious program.
- Windows can then be used to examine copies of the system.



## Conducting the Investigation

- Each investigation is different. Given below is an example of a comprehensive investigation.
  - Remove the hard disk and label it – use an anti-static or static-dissipative wristband and mat before beginning the investigation.
  - Identify the disk type (IDE, SCSI, or other type).
    - Log the disk capacity, cylinders, heads, and sectors.
  - Image the disk with a bit-level copy, sector by sector – this will retain deleted files, unallocated clusters, and slack space.



## Conducting the Investigation

- More steps in the process:
  - Make three or four copies of the drive.
  - Check the disk image to make sure there were no errors during the imaging process.
  - Before analyzing, generate a message digest for all system directories, files, disk sectors, and partitions.
  - Inventory all files on the system.
  - Document the system date and time.



## Chain of Custody

---

- Accounts for all persons who handled or had access to the data
- Answers the following evidence questions:
  - Who collected it?
  - When and from where was it collected?
  - Where and how it was stored?
  - Who had control or possession of it?



## Steps in Chain of Custody

---

1. Record each item collected as evidence.
2. Write a description of it in the documentation.
3. Store evidence in labeled containers.
4. Record all hash values in the documentation.
5. Securely transport evidence to storage facility.
6. Obtain signature of the person who accepts it.
7. Provide controls to prevent access to it.
8. Securely transport evidence to court.



## Free Space vs Slack Space

- When a user deletes a file, the file is not actually deleted.
- Instead, a pointer in a file allocation table is deleted.
- A second file that is saved in the same area does not occupy as many sectors as the first file – there will be a fragment of the original file.
  
- Free Space:
  - The sector that holds the fragment of this file is referred to as free space because the operating system marks it usable when needed.
    - When the operating system stores something else in this sector, it is referred to as allocated.
  - Unallocated sectors still contain the original data until the operating system overwrites them.



## Slack Space

- When a file is saved to a storage media, the operating system allocates space in blocks of a predefined size, called sectors.
- The size of all sectors is the same on a given system or hard drive.
- Even if a file contains only 10 characters, the operating system will allocate a full sector of say 1,024 bytes—the space left over in the sector is slack space.
- **It is possible for a user to hide malicious code, tools, or clues in slack space, as well as in the free space.**
- Slack space from files that previously occupied that same physical sector on the drive may contain information.
- Therefore, an investigator should review slack space using utilities that can display the information stored in these areas.



## Message Digest and Hash

---

- Applies a mathematical operation to data.
  - Creates a unique number (hash) based on the data.
- Hash should be applied to each file and log.
  - Should be written to write-once media.
  - Provides ability to “bag and tag” evidence.
  - Proves whether data has been changed or not.



## Do Not Modify Data

---

- The hash tool is applied to each file or log and the message digest value is noted in the investigation documentation.
  - When the case goes to trial, the investigator may need to run the tool on the files or logs again to demonstrate they have not been altered.
  - The logs may also need to be written to a write-once media, such as a CD-ROM.





## Analysis

- After successfully imaging the drives to be analyzed and calculating and storing the message digests, the investigator begins the analysis.
  
- In general, the following steps will be involved:
  - Check the Recycle Bin for deleted files.
  - Check the Web browser history files and address bar histories.
  - Check the Web browser cookie files.
  - Check the Temporary Internet Files folder.
  - Search files for suspect character strings.
  - Search the slack and free space for suspect character strings as described previously.

Important



## Remediation After an Attack

1. Steps to take once an incident has been responded to and the initial investigation completed
  1. Place the system behind a firewall.
  2. Reload the OS.
  3. Run virus/malware scanners.
  4. Install security software.
  5. Remove unneeded services and applications.
  6. Apply all patches.
  7. Restore the system from backup.