UNIT IV

EVIDENCE COLLECTION AND FORENSICS TOOLS

Processing Crime and Incident Scenes

Objectives

- Explain the **rules** for digital evidence
- Describe how to **collect** evidence at private-sector incident scenes
- Explain **guidelines for processing** law enforcement crime scenes
- List the steps in **preparing** for an evidence search
- Describe how to **secure** a computer incident or crime scene
- Explain guidelines for **seizing** digital evidence at the scene
- List procedures for **storing** digital evidence
- Explain how to **obtain a digital hash**
- Review a case to identify requirements and plan your investigation

Identifying Digital Evidence

- **Digital evidence**
  - Can be any information stored or transmitted in digital form
- Scientific Working Group on Digital Evidence (SWGDE)
- International Organization on Computer Evidence (IOCE)
- General task
  - **Identify, Collect, preserve, document, Analyze, identify, organize, Rebuild**
- Collecting computers and processing an incident must be done **systematically**
- Handle all evidence consistently
- Comply with rules - Follow latest rules

Understanding Rules of Evidence

- Computer records are usually divided into:
  - **Computer-generated records**
    - Records (data) the system maintains - **Log files**
    - **records** are authentic If the program that created the output **is functioning correctly**
  - **Computer-stored records**
    - Records person creates and saves on a computer - **Word doc, spreadsheet**
    - the person offering must demonstrate that a person created the data and the data is reliable and trustworthy—in other words, that **it wasn’t altered** when it was acquired or afterward

Collecting Evidence in Private-Sector Incident Scenes

- Private-sector organizations include:
  - Businesses and government agencies that aren’t involved in law enforcement
- Agencies must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws and make certain documents available as public records
- ISPs can investigate computer abuse committed by their employees, but not by customers

Processing Law Enforcement Crime Scenes

- Be familiar with criminal rules
- Understand how a search warrant works
- Probable cause
- The Fourth Amendment states that only warrants “particularly describing the place to be searched, and the persons or things to be seized” can be issued
- Innocent information
- limiting phrase
- Plain view doctrine
- “Knock and announce”

Preparing for a Search

- **Identifying the Nature of the case**
- **Identifying the Type of Computing**
- **Determining Whether You Can Seize a Computer**
- **Obtaining a Detailed Description of the Location**
- **Determining Who Is in Charge**
- **Using Additional Technical Expertise**
- **Determining the Tools You Need**
- **Preparing the Investigation Team**

Securing a Computer Incident or Crime Scene

- Goals
  - **Preserve** the evidence
  - Keep information **confidential**
- Define a secure perimeter
  - Use yellow barrier **tape**
  - Legal authority: keep **unnecessary people out** but don’t obstruct justice or fail to comply with police officers

- Professional curiosity can destroy evidence
  - Involves police officers and other professionals who aren’t part of the crime scene processing team

Seizing Digital Evidence at the Scene

- Law enforcement can seize evidence
  - With a proper warrant
  - Follow standards

Processing an Incident or Crime Scene

- Guidelines
  - Keep a journal to document
  - Secure the scene - Remove people
  - Take video and still recordings
  - Sketch the incident
  - Check computers as soon as possible
    - Perform a live acquisition if possible
    - perform a normal shutdown, to preserve log files
    - Save data from current applications as safely as possible
    - Record all active windows or shell sessions
    - Photograph the screen
  - Bag and tag the evidence
  - Look for information related to the investigation
  - Collect documentation and media related to the investigation

Processing an Incident or Crime Scene

- Processing Data Centers with RAID Systems
  - Sparse acquisition
- Using a Technical Advisor
- Documenting Evidence in the Lab
  - Record your activities and findings
- Processing and Handling Digital Evidence
  - Maintain the integrity

Storing Digital Evidence

- The media you use to store digital evidence usually depends on how long you need to keep it
  - CD-Rs or DVDs
  - Magnetic tapes

Obtaining a Digital Hash

- Cyclic Redundancy Check
- Message Digest 5 (MD5)
- Secure Hash Algorithm version 1 (SHA-1)
- Nonkeyed hash set
- Keyed hash set
- Three rules for forensic hashes:
  - You can’t predict the hash value of a file or device
  - No two hash values can be the same
  - If anything changes in the file or device, the hash value must change