UNIT V
ANALYSIS AND VALIDATION

Validating Forensics Data
Objectives

• Determine what data to analyze in a computer forensics investigation
• Explain tools used to validate data
• Explain common data-hiding techniques
• Describe methods of performing a remote acquisition
Determining What Data to Collect and Analyze
Determining What Data to Collect and Analyze

• Examining and analyzing digital evidence depends on:
  – Nature of the case
  – Amount of data to process
  – Search warrants and court orders
  – Company policies

• **Scope creep**
  – Investigation expands beyond the original description

• Right of full discovery of digital evidence
Approaching Computer Forensics Cases

• Some basic principles apply to almost all computer forensics cases
  – The approach you take depends largely on the specific type of case you’re investigating
• Basic steps for all computer forensics investigations
  – For target drives, use only recently wiped media that have been reformatted
    • And inspected for computer viruses
Approaching Computer Forensics Cases (continued)

• Basic steps for all computer forensics investigations (continued)
  – Inventory the hardware on the suspect’s computer and note the condition of the computer when seized
  – Remove the original drive from the computer
    • Check date and time values in the system’s CMOS
  – Record how you acquired data from the suspect drive
  – Process the data methodically and logically
Approaching Computer Forensics Cases (continued)

- Basic steps for all computer forensics investigations (continued)
  - List all folders and files on the image or drive
  - If possible, examine the contents of all data files in all folders
    - Starting at the root directory of the volume partition
  - For all password-protected files that might be related to the investigation
    - Make your best effort to recover file contents
Approaching Computer Forensics Cases (continued)

• Basic steps for all computer forensics investigations (continued)
  – Identify the function of every executable (binary or .exe) file that doesn’t match known hash values
  – Maintain control of all evidence and findings, and document everything as you progress through your examination
Refining and Modifying the Investigation Plan

• Considerations
  – Determine the scope of the investigation
  – Determine what the case requires
  – Whether you should collect all information
  – What to do in case of scope creep

• The key is to start with a plan but remain flexible in the face of new evidence
Using AccessData Forensic Toolkit to Analyze Data

- Supported file systems: FAT12/16/32, NTFS, Ext2fs, and Ext3fs
- FTK can analyze data from several sources, including image files from other vendors
- FTK produces a case log file
- Searching for keywords
  - Indexed search
  - Live search
  - Supports options and advanced searching techniques, such as stemming
Using AccessData Forensic Toolkit to Analyze Data (continued)

Figure 9-1 Viewing live search results in FTK
Using AccessData Forensic Toolkit to Analyze Data (continued)

![Search Options](image)

**Figure 9-2 Selecting search options in FTK**
Using AccessData Forensic Toolkit to Analyze Data (continued)

- Analyzes compressed files
- You can generate reports
  - Using bookmarks
Using AccessData Forensic Toolkit to Analyze Data (continued)

Figure 9-3 Creating a bookmark
Validating Forensic Data
Validating Forensic Data

- One of the most critical aspects of computer forensics
- Ensuring the integrity of data you collect is essential for presenting evidence in court
- Most computer forensic tools provide automated hashing of image files
- Computer forensics tools have some limitations in performing hashing
  - Learning how to use advanced hexadecimal editors is necessary to ensure data integrity
Validating with Hexadecimal Editors

• Advanced hexadecimal editors offer many features not available in computer forensics tools
  – Such as hashing specific files or sectors
• Hex Workshop provides several hashing algorithms
  – Such as MD5 and SHA-1
  – See Figures 9-4 through 9-6
• Hex Workshop also generates the hash value of selected data sets in a file or sector
Validating with Hexadecimal Editors

Figure 9-4 Viewing a file opened in Hex Workshop
Validating with Hexadecimal Editors

Figure 9-5 The Generate Checksum dialog box
Validating with Hexadecimal Editors

Figure 9-5  Hex Workshop displaying the MD5 hash value
Validating with Hexadecimal Editors

• Using hash values to discriminate data
  – AccessData has a separate database, the **Known File Filter (KFF)**
    • Filters known program files from view, such as MSWord.exe, and identifies known illegal files, such as child pornography
  – KFF compares known file hash values to files on your evidence drive or image files
  – Periodically, AccessData updates these known file hash values and posts an updated KFF
Validating with Computer Forensics Programs

- Commercial computer forensics programs have built-in validation features
- ProDiscover’s .eve files contain metadata that includes the hash value
  - Validation is done automatically
- Raw format image files (.dd extension) don’t contain metadata
  - So you must validate raw format image files manually to ensure the integrity of data
Validating with Computer Forensics Programs (continued)

• In AccessData FTK Imager
  – When you select the Expert Witness (.e01) or the SMART (.s01) format
    • Additional options for validating the acquisition are displayed
  – Validation report lists MD5 and SHA-1 hash values