Current Computer Forensics Tools

Objectives

- Explain **how to evaluate needs** for computer forensics tools
- Describe available computer forensics **software** tools
- List some considerations for computer forensics **hardware** tools
- Describe **methods for validating and testing** computer forensics tools

Evaluating Computer Forensics Tool Needs

Evaluating Computer Forensics Tool Needs

- Look for versatility, flexibility, and robustness
  - OS
  - File system(s)
  - Script capabilities
  - Automated features
  - Vendor's reputation for support
- Keep in mind what application files you will be analyzing - Microsoft Access databases, E-mail Message

Types of Computer Forensics Tools

- **Hardware forensic tools**
  - Range from single-purpose components to complete computer systems and servers
    - Write Blocker to Forensic workstation
- **Software forensic tools**
  - Specialized to perform one task to many different tasks
  - SafeBack, a command-line disk acquisition tool
  - Pro-Discover, forensics acquisition and analysis functions
  - Types
    - Command-line applications
    - GUI applications
  - Software tools are Commonly used to copy data from a suspect's disk drive to an image file

Tasks Performed by Computer Forensics Tools

- Five major categories:
  - Acquisition
  - Validation and discrimination
  - Extraction
  - Reconstruction
  - Reporting

Acquisition

- Making a copy of the original drive
- Acquisition subfunctions:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote acquisition
  - Verification

Acquisition (continued)

- Two types of data-copying methods are used in software acquisitions:
  - Physical copying of the entire drive
  - Logical copying of a disk partition
- The formats for disk acquisitions vary
  - From raw data to vendor-specific proprietary compressed data
  - The contents of a raw image file can be read with any hexadecimal editor

Acquisition (continued)

- Creating smaller segmented files is a typical feature in vendor acquisition tools
- Make it easier to store acquired data on smaller media, such as CD-Rs or DVD-Rs.
- All computer forensics acquisition tools have a method for verification of the data-copying process
  - That compares the original drive with the image
  - MD5, SHA

Validation and discrimination

- **Validation**
  - Ensuring the integrity of data being copied
- **Discrimination** of data
  - Involves sorting and searching through all investigation data

Validation and discrimination (continued)

- Subfunctions
  - Hashing
    - CRC-32, MD5, Secure Hash Algorithms
  - Filtering
    - Known system files can be ignored
    - Based on hash value sets
  - Analyzing file headers
    - Discriminate files based on their types
- National Software Reference Library (NSRL) has compiled a list of known file hashes
  - For a variety of OSs, applications, and images

Validation and discrimination (continued)

- Many computer forensics programs include a list of common header values
  - With this information, you can see whether a file extension is incorrect for the **file type**
- Most forensics tools can identify **header values**

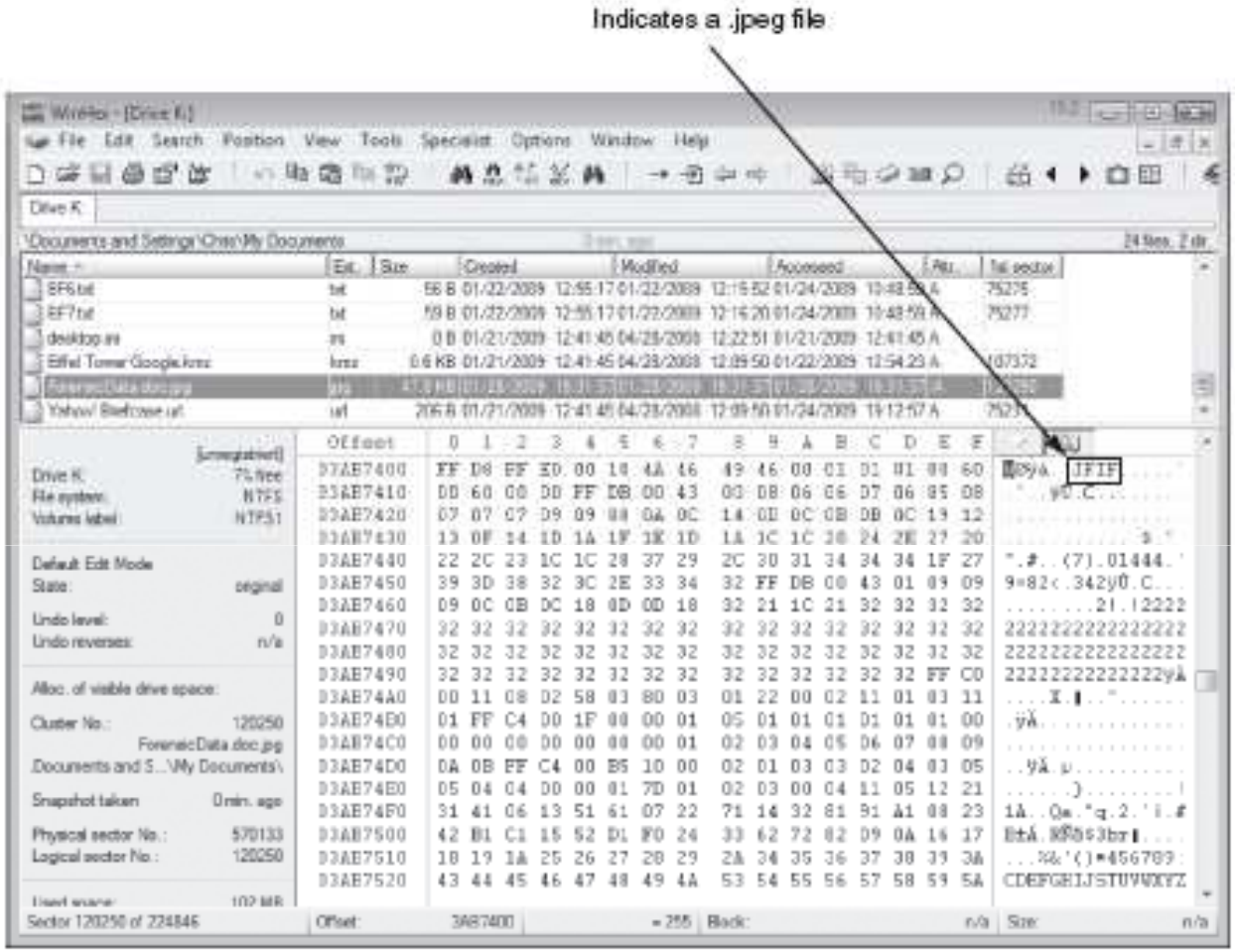

Figure 7-3 The file header indicates a .jpeg file

Extraction

- Recovery task in a computing investigation
- Most demanding of all tasks to master
- Recovering data is the first step in analyzing an investigation’s data

Extraction (continued)

- Subfunctions
  - Data viewing
  - Keyword searching
  - Decompressing
  - Carving (reconstructing file fragments)
  - Decrypting
  - Bookmarking
- **Keyword search** speeds up analysis for investigators

Figure 7-7 Data-carving options in FTK

Extraction (continued)

- From an investigation perspective, encrypted files and systems are a problem
- Many password recovery tools have a feature for generating potential password lists
  - For a **password dictionary attack**
- If a password dictionary attack fails, you can run a **brute-force attack**

Reconstruction

- Re-create a suspect drive to show what happened during a crime or an incident
- Subfunctions
  - Disk-to-disk copy (dd command, H/W & S/W tools)
  - Image-to-disk copy
  - Partition-to-partition copy
  - Image-to-partition copy
- This is easiest if a matching blank hard disk is available, same make and model

Reconstruction (continued)

- Some tools that perform an image-to-disk copy:
  - SafeBack
  - SnapBack
  - EnCase
  - FTK Imager
  - ProDiscover
- Shadowing technique – Read from suspect drive and write to another drive(shadow drive)
  - Used to demonstrate in court how criminal activity was carried out

Reporting

- To complete a forensics disk analysis and examination, you need to create a report
- Earlier - Manual examination, paper report
- Subfunctions
  - Log reports (tools records activities the investigator performed)
  - Report generator (EnCase, ProDiscovery,FTK)
- Use this information when producing a final report for your investigation

Other Considerations for Tools

- Considerations
  - Flexibility
  - Reliability
  - Expandability
  - Keep a library with older version of your tools
- Create a software library containing older versions of forensics utilities, OSs, and other programs