2.3. Current Computer Forensics Tools: Software/ Hardware Tools

Evaluating Digital Forensics Tool Needs

- Consider open-source tools; the best value for as many features as possible
- Questions to ask when evaluating tools: – On which OS does the forensics tool run – What file systems can the tool analyze?
  - Can a scripting language be used with the tool to automate repetitive functions?
  - Does it have automated features?
  - What is the vendor's reputation for providing support?

Types of Digital Forensics Tools

- Hardware forensic tools
  – Range from single-purpose components to complete computer systems and servers
- Software forensic tools – Types
- Command-line applications
- GUI applications
  – Commonly used to copy data from a suspect's disk drive to an image file

Tasks Performed by Digital Forensics Tools

- Follow guidelines set up by NIST's Computer Forensics Tool Testing (CFTT) program
- ISO standard 27037 states: Digital Evidence First Responders (DEFRs) should use validated tools
- Five major categories:
  - Acquisition
  - Validation and verification
  - 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, live, and memory acquisitions
  - 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

You can view the contents of a raw image file with any hexadecimal editor

  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - Remote acquisition of files is common in larger organizations
- Popular tools, such as AccessData and EnCase, can do remote acquisitions of forensics drive images on a network

Validation and Verification

– Validation

- A way to confirm that a tool is functioning as intended

– Verification

- Proves that two sets of data are identical by calculating hash values or using another similar method
- A related process is filtering, which involves sorting and searching through investigation findings to separate good data and suspicious data.

– Subfunctions

- Hashing

  – CRC-32, MD5, SHA-1 (Secure Hash Algorithms)
- Filtering

– 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

- 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

Extraction

- Recovery task in a digital investigation
- Most challenging of all tasks to master
- Recovering data is the first step in analyzing an investigation's data

Subfunctions of extraction

- Data viewing
- Keyword searching
- Decompressing or uncompressing
- Carving
- Decrypting
- Bookmarking or tagging

- **Keyword search** speeds up analysis for investigators
- 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
    - Methods of reconstruction
  - Disk-to-disk copy
  - Partition-to-partition copy
  - Image-to-disk copy
  - Image-to-partition copy
  - Rebuilding files from data runs and carving – To re-create an image of a suspect drive
  - Copy an image to another location, such as a partition, a physical disk, or a virtual machine
  - Simplest method is to use a tool that makes a direct disk-to-image copy

  Examples of disk-to-image copy tools:
  - Linux dd command
  - ProDiscover
  - Voom Technologies Shadow Drive

Reporting

- To perform a forensics disk analysis and examination, you need to create a report
- Subfunctions of reporting
  - Bookmarking or tagging
  - Log reports
  - Report generator
- Use this information when producing a final report for your investigation

Function	ProDiscover Basic	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
Acquisition				
Physical data copy	✓	✓	✓	✓
Logical data copy	✓	✓	✓	
Data acquisition formats	✓	✓	✓	✓
Command-line processes				✓
GUI processes	✓	✓	✓	✓
Remote acquisition		✓	✓	✓
Validation and verification				
Hashing	✓	✓	✓	✓
Verification	✓	✓	✓	✓
Filtering		✓	✓	✓
Analyzing file headers		✓	✓	✓
Extraction				
Data viewing	✓	✓	✓	✓
Keyword searching	✓	✓	✓	✓
Decompressing			✓	✓
Carving		✓	✓	✓
Decrypting		✓	✓	
Bookmarking	✓	✓	✓	✓
Reconstruction				
Disk-to-disk copy	✓	✓	✓	✓
Partition-to-partition copy	✓	✓	✓	✓
Image-to-disk copy	✓	✓	✓	✓
Image-to-partition copy	✓	✓	✓	✓
Disk-to-image copy	✓	✓	✓	✓
Rebuilding files	✓	✓	✓	✓
Reporting				

Fig: Comparison of forensic tool functions

- Considerations
  - Flexibility
  - Reliability
  - Future expandability
- Create a software library containing older versions of forensics utilities, OSs, and other programs

Forensics Software Tools

- The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux

Command-line Forensics Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems
- Norton DiskEdit
- One of the first MS-DOS tools used for computer investigations
- Command-line tools require few system resources
- Designed to run in minimal configurations
- Current programs are more powerful and have many more capabilities

Linux Forensics Tools

- **UNIX** has been mostly replaced by Linux
  - **–** You might still encounter systems running UNIX
- **Linux** platforms are becoming more popular with home and business end users
- **SMART**
  - Designed to be installed on numerous Linux versions
  - Can analyze a variety of file systems with SMART
  - Many plug-in utilities are included with SMART
  - Another useful option in SMART is its hex viewer
- **Helix 3**
  - One of the easiest suites to begin with
  - You can load it on a live Windows system
- Loads as a bootable Linux OS from a cold boot

  **Some international courts have not accepted live acquisitions as a valid forensics practice

- **Kali Linux**
  - Formerly known as BackTrack

- Includes a variety of tools and has an easy-to-use KDE interface

- **Autopsy and SleuthKit**
  - Sleuth Kit is a Linux forensics tool
  - Autopsy is the GUI browser interface used to access Sleuth Kit's tools

Other GUI Forensics Tools

- GUI forensics tools can simplify digital forensics investigations
- Have also simplified training for beginning examiners
- Most of them are put together as suites of tools
- **Advantages**
  - Ease of use
  - Multitasking
  - No need for learning older OSs
- **Disadvantages**
  - Excessive resource requirements
  - Produce inconsistent results – Create tool dependencies
- Investigators' may want to use only one tool
- Should be familiar with more than one type of tool

Forensics Hardware Tools

- Technology changes rapidly
- Hardware eventually fails
  – Schedule equipment replacements periodically
- When planning your budget consider:
  - Amount of time you expect the forensic workstation to be running
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement

Forensic Workstations

- Carefully consider what you need
  - Categories

    -Stationary workstation
  - Portable workstation
  - Lightweight workstation
- Balance what you need and what your system can handle
  - Remember that RAM and storage need updating as technology advances
- Police agency labs
  - Need many options
  - Use several PC configurations
- Keep a hardware library in addition to your software library
- Private corporation labs
  - Handle only system types used in the organization
- Some vendors offer workstations designed for digital forensics
- Examples
  - F.R.E.D. unit from Digital Intelligence
  - Hardware mounts from ForensicPC
- Having vendor support can save you time and frustration when you have problems
- Can mix and match components to get the capabilities you need for your forensic workstation **Using a Write-Blocker**
- **Write-blocker**
  - Prevents data writes to a hard disk
- **Software-enabled blockers**
  - Typically run in a shell mode (Windows CLI)
  - Example: PDBlock from Digital Intelligence
- **Hardware options**
  - Ideal for GUI forensic tools

- Act as a bridge between the suspect drive and the forensic workstation

- You can navigate to the blocked drive with any application
- Discards the written data
  - For the OS the data copy is successful
- Connecting technologies – FireWire

  USB 2.0 and 3.0

  SATA, PATA, and SCSI controllers

Recommendations for a Forensic Workstation

- Determine where data acquisitions will take place
- With Firewire and USB write-blocking devices
  - You can acquire data easily with Digital Intelligence FireChief and a laptop computer
  - FireWire
- If you want to reduce hardware to carry:
  - WiebeTech Forensic DriveDock with its regular DriveDock FireWire bridge or the Logicube Talon
- Recommendations when choosing stationary or lightweight workstation:
  - Full tower to allow for expansion devices
  - As much memory and processor power as budget allows
  - Different sizes of hard drives
  - 400-watt or better power supply with battery backup
  - External FireWire and USB 2.0 ports
  - Assortment of drive adapter bridges
  - Ergonomic keyboard and mouse
  - A good video card with at least a 17-inch monitor
  - High-end video card and dual monitors
- If you have a limited budget, one option for outfitting your lab is to use highend game PCs

Validating and Testing Forensic Software

It is important to make sure the evidence you recover and analyze can be admitted in court

- You must test and validate your software to prevent damaging the evidence

Using National Institute of Standards and Technology Tools

- NIST publishes articles, provides tools, and creates procedures for testing/validating forensics software
- Computer Forensics Tool Testing (CFTT) project
  - Manages research on computer forensics tools
- NIST has created criteria for testing computer forensics tools based on:
  - Standard testing methods
    - ISO 17025 criteria for testing items that have no current standards
- Your lab must meet the following criteria
  - Establish categories for digital forensics tools
  - Identify forensics category requirements
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results
- ISO 5725 - specifies results must be repeatable and reproducible
- NIST created the National Software Reference Library (NSRL) project
  - Collects all known hash values for commercial software applications and OS files
- Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)
  - Helps filtering known information
  - Can use RDS to locate and identify known bad files

Using Validation Protocols

- Always verify your results by performing the same tasks with other similar forensics tools
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how forensics tools work

- One way to compare results and verify a new tool is by using a disk editor
  – Such as Hex Workshop or WinHex
- Disk editors do not have a flashy interface, however they:
  - Are reliable tools
  - Can access raw data
- Computer Forensics Examination Protocol
  - Perform the investigation with a GUI tool
  - Verify your results with a disk editor
  - Compare hash values obtained with both tools
- Digital Forensics Tool Upgrade Protocol – Test
- New releases
- OS patches and upgrades
  – If you find a problem, report it to forensics tool vendor
- Do not use the forensics tool until the problem has been fixed
  - Use a test hard disk for validation purposes
  - Check the Web for new editions, updates, patches, and validation tests for your tools.