Guide to Computer Forensics and Investigations Sixth Edition

Chapter 6
Current Digital Forensics Tools

Objectives

- Explain how to evaluate needs for digital forensics tools
- List some considerations for digital forensics hardware tools
- Describe methods for validating and testing forensics 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
  - *Range from $300 up*
  - 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

All tools used should be well tested

- *All computer forensics tools, both hardware and software, perform specific functions. These function can be grouped into* Five major categories:
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting

Tasks Performed by Digital Forensics Tools (Cont)

- **Acquisition**
  - Making a copy of the original drive

- Acquisition subfunctions:
  - Physical data copy
  - Logical data copy - *logical partition*
  - Data acquisition format – *raw data format*
  - GUI acquisition
  - Remote, live (*logon*), and memory acquisitions

Tasks Performed by Digital Forensics Tools (Cont)

- Acquisition (cont'd)
  - 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

Tasks Performed by Digital Forensics Tools (Cont)

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

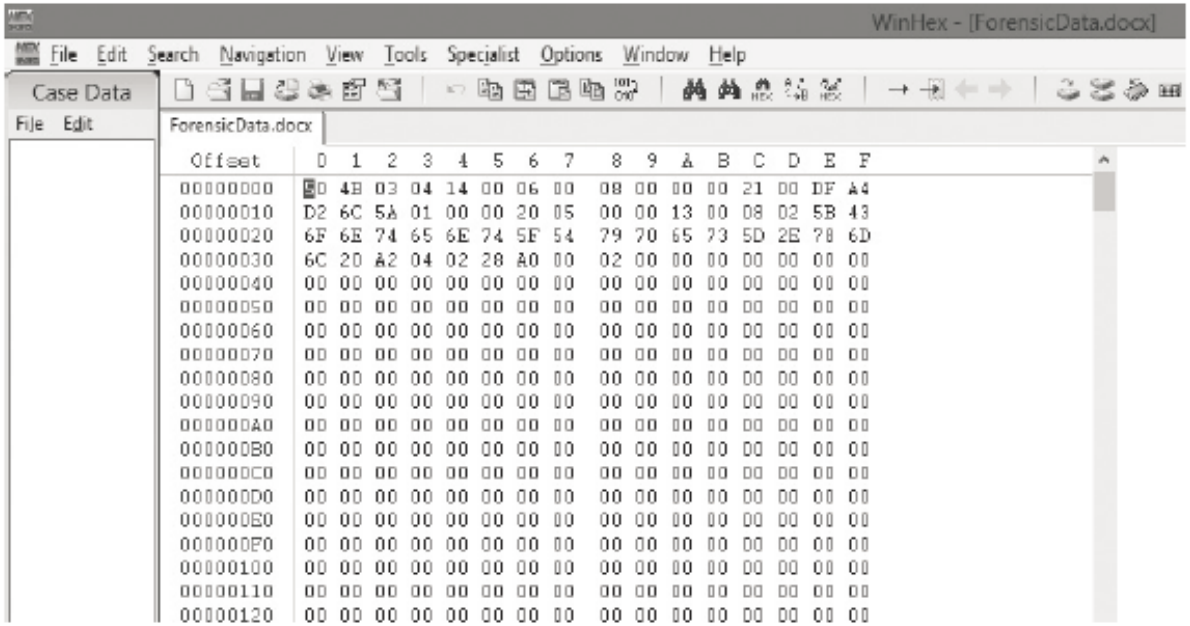


Figure 6-1 Viewing data in WinHex

Courtesy of X-Ways AG, *www.x-ways.net*

Tasks Performed by Digital Forensics Tools (Cont)

- Acquisition (cont'd)
  - Creating smaller segmented files is a typical feature in vendor acquisition tools – *segmented files are smaller and therefore can be stored in smaller media*
  - 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

Tasks Performed by Digital Forensics Tools (Cont)

- Validation and Verification
  - **Validation**
    - A way to confirm that a tool is functioning as intended – *ensuring the integrity of data being copied*
  - **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

Tasks Performed by Digital Forensics Tools (Cont)

- Validation and verification (cont'd)
  - Subfunctions of validation and verification include:-
    - Hashing – *ensure data hasn't been changed*
      - CRC-32, MD5, SHA-1 (Secure Hash Algorithms)
    - Filtering – *To separate good files and files need to be investigated*
      - Based on hash value sets
    - Analyzing file headers – *To check on change file type*
      - 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

Tasks Performed by Digital Forensics Tools (Cont)

- Validation and discrimination (cont'd)
  - 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

Tasks Performed by Digital Forensics Tools (Cont)

- **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

Tasks Performed by Digital Forensics Tools (Cont)

- **Extraction** (cont'd)
  - Subfunctions of extraction
    - Data viewing – *Different tools provide different way of viewing data*
    - Keyword searching – *A good function but if wrong key word is used may produce "noise"*
    - Decompressing or uncompressing
    - Carving - *Reconstructing fragments of files*
    - Decrypting – *Can be a potential problem for investigation*
    - Bookmarking or tagging
  - **Keyword search** speeds up analysis for investigators

Tasks Performed by Digital Forensics Tools (Cont)

- **Extraction** (cont'd)
  - 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**

Tasks Performed by Digital Forensics Tools (Cont)

- **Reconstruction**
  - Re-create a suspect drive to show what happened during a crime or an incident – *Another reason is to create a copy of suspect drive for other investigators*
  - 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

Tasks Performed by Digital Forensics Tools (Cont)

- **Reconstruction** (cont'd)
  - 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

Tasks Performed by Digital Forensics Tools (Cont)

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

Considerations for Tools

- Considerations
  - Flexibility
  - Reliability
  - Future expandability

- Create a software library containing older versions of forensics utilities, OSs, and other programs

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

Other GUI Forensics Tools (Cont)

- Disadvantages
  - Excessive resource requirements – *i.e PC RAM*
  - Produce inconsistent results - *Because of the type of OS used. 32 bits OS vs 64 bits OS*
  - Create tool dependencies
    - Investigators' may want to use only one tool – *Refuse to change*
    - Should be familiar with more than one type of tool

Digital 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 – *how often does it fail?*
  - Consultant and vendor fees – *support the h/w*
  - Anticipate equipment replacement – *the more you use, the more the equipment will breakdown*

https://blog.inkjetwholesale.com.au/

Forensic Workstations

- Carefully consider what you need
- Categories
  - Stationary workstation
  - Portable workstation
  - Lightweight workstation

Ref: http://forensic.acmeportable.com

- Balance what you need and what your system can handle
  - Remember that RAM and storage need updating as technology advances

Forensic Workstations (Cont)

- Police agency labs
  - Need many options
  - Use several PC configurations – *due to diverse investigations*
- Keep a hardware library in addition to your software library
- Private corporation labs
  - Handle only system types used in the organization

Forensic Workstations (Cont)

- Building a forensic workstation is not as difficult as it sounds
  - Advantages
    - Customized to your needs
    - Save money
  - Disadvantages
    - Hard to find support for problems
    - Can become expensive if careless

Ref : https://digitalintelligence.com

- Also need to identify what you intend to analyze

Recommendations for a Forensic Workstation

- Some vendors offer workstations designed for digital forensics
- 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
- Determine where data acquisitions will take place – *i.e acquire data in the field, may want to carry something light*

Recommendations for a Forensic Workstation (Cont)

- 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

Recommendations for a Forensic Workstation (Cont)

- Recommendations when choosing stationary or lightweight workstation (cont'd):
  - 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 high-end game PCs – *can perform well with modifications!*

Using a Write-Blocker

- **Write-blocker**
  - Prevents data writes to a hard disk
    - *A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data.*

- Software-enabled blockers
  - Typically run in a shell mode (Windows CLI)
    - Example: PDBlock from Digital Intelligence

Ref: https://www.cru-inc.com

- Hardware options
  - Ideal for GUI forensic tools
    - *They prevent Windows or Linux from writing data to the blocked drive.*
  - Act as a bridge between the suspect drive and the forensic workstation

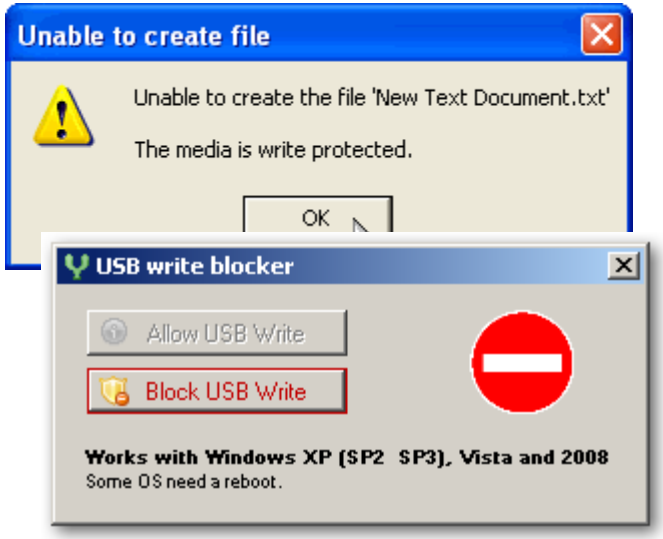
Using a Write-Blocker (Cont)

- You can navigate to the blocked drive with any application – *no problem accessing the blocked drive's applications after write-blocker is installed.*

- 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

Ref : http://blog.zoller.lu



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

Using National Institute of Standards and Technology Tools (Cont)

- Your lab must meet the following criteria for tool testing
  - Establish categories for digital forensics tools
  - Identify forensics category requirements
  - Develop test assertions :
    - *Based on the requirements, create tests to test tool's capability*
  - Identify test cases
  - Establish a test method
  - Report test results
- **ISO 5725** - specifies results must be repeatable and reproducible

Using National Institute of Standards and Technology Tools (Cont)

- 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
    - *This could help to speed up investigation time*
  - 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 editor can be used to view data on a disk in its raw format.*

Using Validation Protocols (Cont)

- 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

Using Validation Protocols (Cont)

- Digital Forensics Tool Upgrade Protocol – *To ensure evidence data will not be corrupted, we need to:-*
  - Test
    - New releases (*Tools*)
    - 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

Summary

- Consult your business plan to get the best hardware and software
- Computer forensics tools functions
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting
- Maintain a software library on your lab

Summary

- Computer Forensics tools types
  - Software
  - Hardware
- Forensics software
  - GUI
- Forensics hardware
  - Customized equipment – *Make one yourself*
  - Commercial options – *Buy off the shelf*
  - Include workstations and write-blockers
- Always run a validation test when upgrading your forensics tools