Computer Forensics

Week 5: Current Digital Forensics Tools

Kumi University
Lecturer: Lemi Agrey Oliver
codingissweet@gmail.com

Content

- ❑ Introduction to digital forensic tools
- ❑ Evaluating Digital Forensics Tool Needs
- ❑ Digital Forensics Software Tools
- ❑ Digital Forensics Hardware Tools.
- ❑ Validating and Testing Forensics Software

Recap of last week

- Last week, we discussed about file systems, exploring their definition and crucial role in organizing data effectively. We then shift our focus to the common file systems used in Windows environments, including FAT32, NTFS, and exFAT, discussing their features and limitations.
- Next, we took a deep dive into the NTFS (New Technology File System) structure, understanding how it manages files, directories, and metadata. We explore the NTFS disk structures, highlighting the Master File Table (MFT) and its pivotal role in file system operations. Additionally, we examine disk allocation methods and how NTFS optimizes storage for improved performance.
- Further more, we explored the importance of whole disk encryption for data security, introducing BitLocker Drive Encryption in Windows as a powerful tool for encrypting entire disk volumes.

Recap of last week+

- We discuss the benefits and challenges of whole disk encryption, emphasizing its role in protecting sensitive data.
- Finally we introduce the concept of virtualization and its myriad benefits for testing and development. We provide a step-by-step guide to creating a virtual machine using popular virtualization platforms like Hyper-V or VirtualBox.
- The lecture provided a comprehensive overview of file systems, disk structures, encryption, virtualization, and best practices, equipping you with the knowledge and tools to manage data effectively in Windows environments.
- This week we shall discuss about the current digitals tools.

Introduction to digital forensic tools

- There are a multitude of forensic software tools and services available to the forensic examiner [1]
- Digital forensics tools are software applications used to collect, preserve, extract, analyze, and document digital evidence from electronic devices and digital media.
- These tools play a crucial role in cybercrime investigations, incident response, and legal proceedings.
- Examples of these tools includes Digital Forensics Framework (DFF), Write blockers, X-Ways Forensics, Open Computer Forensics Architecture, Forensic Toolkit (FTK) and many others

Evaluating Digital Forensics Tool Needs

- Develop a business plan to justify obtaining digital forensics hardware and software. Consider open-source tools that may offer technical support to maximize value.
- Evaluate tools based on:
  - ✓ Compatibility with different operating systems
  - ✓ Versatility across Windows, Linux, and macOS
  - ✓ Ability to analyze various file systems like FAT, NTFS, and Ext4
  - ✓ Support for scripting languages to automate tasks
  - ✓ Automated features that can reduce analysis time
  - ✓

Evaluating Digital Forensics Tool Needs +

- ✓ Vendor's reputation for providing product support or the quality of support forums for open-source tools

- ❖ Consider the operating systems and file types you'll be analyzing when choosing tools.
- ❖ Look for specialized tools if you need to analyze specific file types, such as Microsoft Access or SQL Server databases, or email messages.
- ❖ Keep an open mind and compare different platforms and applications for various tasks. Consider exploring alternatives to Windows tools, such as Linux and macOS platforms

Hardware Forensic tools

❖Hardware forensics tools are specialized devices used in digital forensics to acquire and analyze data from physical hardware components. These tools are designed to extract information from various types of devices, including computers, mobile phones, and storage devices.

Examples of Hardware Forensic tools

❖**Forensic Workstations,** specialized computers designed for digital forensic analysis, equipped with high-performance components and forensic software.

❖**Disk Imaging Devices**, These devices are used to create forensic images of storage devices, including hard drives, solid-state drives (SSDs), and USB drives, preserving the original data for analysis.

Hardware Forensic tools+

- **JTAG/Chip-Off Tools,** used in mobile forensics, these tools allow investigators to extract data from mobile devices' memory chips directly, bypassing the device's operating system.
- **Logic Analyzers**, These tools are used to capture and analyze digital signals in hardware components, helping in the analysis of embedded systems and other hardware devices.
- **Bus Analyzers**, Used to monitor and analyze data traffic on buses, such as USB, SATA, and PCIe, these tools can help in identifying and analyzing data transfers between hardware components.
- **Device Disassemblers**, used in cases where physical disassembly of a device is required, these tools help in accessing and extracting data from internal components.

Hardware Forensic tools++

- **Circuit Debuggers**, used to analyze and debug circuits in hardware devices, these tools can be helpful in identifying and analyzing malicious hardware modifications.
- **Media Storage Devices,** used to securely store forensic images and other digital evidence, ensuring chain of custody and integrity of the data.

Write-blocker

- A write-blocker is essential for a forensic workstation as it protects evidence disks by preventing data from being written to them. There are software and hardware write-blockers, each functioning differently.
- **Software Write-Blockers**, Software write-blockers like PDBlock from Digital Intelligence typically run in a shell mode and change interrupt-13 of a workstation's BIOS to prevent writing to a specified drive. They sound an alarm if an attempt is made to write data to the blocked drive but can only run in true DOS mode, not in a Windows CLI.
- **Hardware Write-Blockers,** Hardware write-blockers act as a bridge between the suspect drive and the forensic workstation, allowing you to start the OS as usual. They are ideal for GUI forensics tools and prevent Windows or Linux from writing data to the blocked drive.

Write-blocker

- Functionality of Write-Blockers: In a Windows environment, a write-blocker installed on an attached drive makes the drive appear as any other attached disk. While Windows applications show that data copy is successful, the write-blocker actually discards the written data, effectively writing to null.
- Types of Write-Blocking Devices: Write-blocking devices connect to a computer through FireWire, USB 2.0 and 3.0, SATA, PATA, and SCSI controllers. They allow for the removal and reconnection of drives without shutting down the workstation, saving time in processing the evidence drive.
- Vendor Offerings: Various vendors offer write-blocking devices, and specifications can be found on the CFTT website.

Write-blocker++

- Figure 1: A portable Tableau forensic write-blocker attached to a hard disk drive[2]

Software Forensics Tools

- Software forensics tools are applications designed to assist in digital forensic investigations by analyzing digital artifacts, recovering deleted files, and extracting valuable information from various sources.
- These tools are used to examine digital devices such as computers, smartphones, and storage media

Examples of Forensic Software tools

- Autopsy, An open-source digital forensics platform that supports disk imaging, file analysis, and case management. It is widely used for analyzing disk images and files, recovering deleted files, and examining file metadata.

Software Forensics Tools+

- **EnCase Forensic,** a popular commercial digital forensics tool used for acquiring, analyzing, and reporting on digital evidence. It supports a wide range of file systems and can analyze various types of digital artifacts.
- **Forensic Toolkit (FTK), a** comprehensive forensic analysis tool that helps in analyzing digital evidence from computers and mobile devices. It includes features for disk imaging, file analysis, keyword searching, and email analysis.
- **Volatility**, an open-source memory forensics framework used for analyzing volatile memory (RAM) in computer systems. It helps in extracting information such as running processes, network connections, and other system activities.
-

Software Forensics Tools++

- **Wireshark,** a popular network protocol analyzer used for capturing and analyzing network traffic. It helps in identifying unauthorized access, network intrusions, and other suspicious activities.
- **Cellebrite UFED,** A mobile forensics tool used for extracting data from mobile devices like smartphones and tablets. It can extract call logs, messages, app data, and other relevant information from mobile devices.

Tasks Performed by Digital Forensics Tools

- Digital forensics tools perform a variety of tasks to help investigators analyze digital evidence and reconstruct digital incidents. These tasks includes Acquisition, Validation and verification, Extraction, Reconstruction and Reporting

Acquisition

- Acquisition is the initial step in digital forensics, involving copying the original drive to preserve the data.
- Subfunctions in acquisition include physical and logical data copies, data acquisition formats, and command-line and GUI acquisitions.

Acquisition+

- ISO standard 27037 emphasizes the importance of DEFR competency and validated tools in data acquisition.
- Documentation of the acquisition process is crucial, including the rationale behind decisions.
- Decision-making flowcharts help determine whether to copy an entire disk or focus on specific areas.
- Some software suites have separate tools for acquiring images, while hardware devices can also be used.
- Hardware devices like Tableau TD2 and Logicube Talon have built-in software for data acquisition.
- Two types of data-copying methods are used: physical copying of the entire drive and logical copying of a disk partition.
- Logical acquisition is preferred for encrypted drives to ensure readable data.

Acquisition++

- Disk acquisition formats vary, with raw data format being a bit-for-bit copy and vendor-specific formats also used.
- Remote acquisition of files is common in larger organizations using tools like AccessData and EnCase.

Validation and verification

- Validation and verification functions in digital forensics are crucial and work together. Validation confirms that a tool functions correctly, while verification ensures that two sets of data are identical, often done using hash values.
- Filtering is a related process that involves sorting and searching through investigation findings to separate good data from suspicious data, which is enabled by validating tools and verifying data.
- To validate a tool, forensic images are used from sources like NIST's CFTT or the Scientific Working Group on Digital Evidence (SWGDE), which provide expected results for different scenarios.

Validation and verification+

- Verification of data copying compares the original drive with the image, often using hashing algorithms like MD5 or SHA-1.
- Filtering separates known good data (OS files, common applications) from suspicious data using hash values or file headers.
- The National Software Reference Library (NSRL) provides known file hashes for various OSs, applications, and images, aiding in filtering known good files.
- Digital forensics tools can integrate known good file hash sets and compare them with file hashes from a suspect drive to quickly eliminate irrelevant data.

Validation and verification+

- Analyzing and verifying header values for known file types is another way to filter data, as file headers can reveal the true file type despite incorrect file extensions.
- Viewing file headers using a hexadecimal editor can help identify files that have been altered intentionally, improving the filtering process.

Extraction

- Extraction in digital forensics refers to the process of retrieving data from digital devices and storage media for analysis. This step is crucial for collecting evidence in Investigations.
- Subfunctions of Extraction:
- Data Viewing: Tools provide ways to view data, including logical drive structures such as folders and files, as well as allocated and unallocated disk areas.
- Keyword Searching: Tools support searching for keywords of interest to speed up analysis, including the use of word lists created for specific cases.
- Decompressing or Uncompressing: Tools can handle compressed files and zip archives, applying the correct algorithm for uncompressing files.
-

Extraction+

- Carving: Also known as salvaging, this involves reconstructing fragments of deleted files from unallocated disk space, often done manually or using GUI tools with built-in carving functions.
- The process of carving involves searching a data stream for file headers and magic values, determining (or guessing) the file end point, and saving this substream out into a carved file[3]
- Decrypting: Tools can recover and decrypt data from encrypted files or systems, which can be a major challenge in investigations.

Extraction++

- **Data Recovery and Reconstruction,** investigators use extraction to recover and reconstruct data, including deleted files and fragmented data, from digital devices and storage media.
- **Keyword Searching and Filtering,** tools enable searching for keywords and filtering data to separate good data from suspicious data, improving the efficiency of the analysis process.
- **Encryption Challenges**, decrypting encrypted files and systems is challenging, but tools have features for generating potential password lists and attempting password recovery using rainbow tables and brute-force attacks.
- **Bookmarking or Tagging**, investigators use bookmarks to tag evidence for later reference, often used in report generation to produce technical reports of examination findings.

Reconstruction

- The reconstruction function in a forensics tool is used to recreate a suspect drive to understand what occurred during a crime or incident. It can also be used to create a copy of the drive for other investigators or to restore a compromised drive.

Methods of Reconstruction:

- Disk-to-disk copy: Copying one disk directly to another.
- Partition-to-partition copy: Similar to disk-to-disk copy, but copying partitions instead of entire disks.
- Image-to-disk copy: Copying an image of a disk to another disk.
- Image-to-partition copy: Copying an image of a disk to a partition.
- Disk-to-image copy: Copying a disk directly to an image file.
- Rebuilding files from data runs and carving: Reconstructing files from data fragments and using carving techniques.

Reconstruction+

Drive Reconstruction Methods:

- Using the same make and model disk as the suspect disk, which was more common in the past but is rarely used now.
- Copying an image to another location, such as a partition, physical disk, or virtual machine.
- Direct disk-to-image copy using tools like Linux dd command, which produces uncompressed files.
- Tool-specific Formats: Some tools have proprietary formats that can only be restored by the same application that created them, while others can convert files to formats like .E01 or .001 for use in different tools.

Reconstruction++

- Time-critical Cases and Shadowing Drives: In cases like kidnapping or homicides, shadowing drives can be useful. This involves connecting a suspect's drive to a read-only port and another drive to a read-write port using a hardware device like Voom Technologies Shadow Drive.
- All data that would normally be written to the suspect’s drive is redirected to the shadow drive, allowing investigators to access and run applications on the suspect’s drive without compromising evidence.

Reporting

❖ Creating a report is essential for disk analysis and examination in forensics. Previously, this process involved manual data copying and extraction, followed by compiling evidence into a report using separate programs. Challenges arose with nonprintable file data, such as databases and graphics, making insertion into reports difficult.

❖ **Modern Reporting Tools**: Newer forensics tools can generate electronic reports in various formats like word-processing documents, HTML, and PDF files. This advancement has simplified and streamlined the reporting process.

- **Subfunctions of Reporting**:
  - ✓ **Bookmarking or Tagging**: Identifying and marking evidence during extraction for inclusion in the report.

Reporting+

- ✓ **Log Reports**: Recording investigator activities and incorporating bookmarked evidence.
- ✓ **Timelines**: Creating timelines of events based on the evidence.
- ✓ **Report Generator**: Using built-in tools to generate reports in different formats.

❖ **Documentation and Validation**: It's crucial to document the steps taken to acquire data from a suspect drive, often done through log reports. These reports serve as documentation of the examination process and can be useful for peer review or if the examination needs to be repeated.

❖ **Tool-specific Features**: Tools like EnCase, FTK, OSForensics, ILookIX, and X-Ways Forensics offer report generators and the ability to display bookmarked evidence. However, investigator reports are still necessary to provide detailed explanations and insights beyond what automated reports can offer.

Validating and Testing Forensics Software

- Validating and testing forensics software is crucial to ensure its reliability and accuracy in handling digital evidence.
- This involves confirming that the software functions as intended and meets the specified requirements. It ensures that the tool behaves correctly in various scenarios.
- Testing involves using the software in simulated or real-world scenarios to evaluate its performance, accuracy, and effectiveness. This includes checking for bugs, errors, and vulnerabilities.
- Various tools and methods are used for validation and testing, including creating test cases, using validation suites, and comparing results against known standards and benchmarks.

Validating and Testing Forensics Software +

- It's important to document the results of validation and testing, including any issues or discrepancies found. This documentation helps in improving the software and providing evidence of its reliability.
- Forensics software often needs to comply with specific standards, such as ISO/IEC 27037, which provides guidelines for digital evidence acquisition and analysis.
- Validation and testing are ongoing processes, and software developers should continuously update and improve their tools based on feedback and new findings.

Validating and Testing Forensics Software++

- Your lab must meet the following criteria and keep accurate records so that when new software and hardware become available, testing standards are in place for your lab[3]
- Establish categories for digital forensics tools—Group digital forensics software according to categories, such as forensics tools designed to retrieve and trace e-mail.
- Identify forensics category requirements—For each category, describe the technical features or functions a forensics tool must have.
- Develop test assertions—Based on the requirements, create tests that prove or disprove the tool's capability to meet the requirements.

Validating and Testing Forensics Software+++

- Identify test cases—Find or create types of cases to investigate with the forensics tool, and identify information to retrieve from a sample drive or other media. For example, use the image of a closed case file created with a trusted forensics tool to test a new tool in the same category and see whether it produces the same results.
- Establish a test method—Considering the tool's purpose and design, specify how to test it.
- Report test results—Describe the test results in a report that complies with ISO 17025, which requires accurate, clear, unambiguous, and objective test reports.

Summary

- We have reached the conclusion of our lecture for this week on digital forensics tools. Let's recap the key points covered:
- **Introduction to Digital Forensic Tools**: We started by defining digital forensic tools and providing a brief overview of their importance in investigations.
- **Criteria for Selecting a Digital Forensic Tool**: We discussed the criteria that should be considered when selecting a digital forensic tool, emphasizing the importance of choosing the right tool for the specific requirements of an investigation.

Summary

- We categorized forensic tools into hardware and software tools and provided examples of each. For example, software tools include forensic imaging tools, data recovery tools, and analysis tools, while hardware tools include write blockers and forensic workstations.
- We then introduced the concept of a write blocker, which can be either in software or hardware form. We explained that a write blocker is used during data acquisition to prevent the alteration of forensic evidence, ensuring its integrity.
- Furthermore, we discussed the tasks performed by digital investigators, which can be summarized as follows:
  - ✓ Acquisition: Collecting digital evidence in a forensically sound manner.
  - ✓ Validation and Verification: Ensuring that the collected evidence is valid and reliable.

Summary

- ✓ Extraction: Extracting relevant information from the collected evidence.
- ✓ Reconstruction: Reconstructing events based on the extracted information.
- ✓ Reporting: Documenting findings and presenting them in a clear and concise manner.

❖ Finally, we delved into the importance of validating and testing forensic tools to ensure their reliability and accuracy in forensic investigations.

❖ In conclusion, understanding digital forensic tools and their proper use is essential for conducting effective digital investigations and ensuring that evidence is admissible in court.

❖ Next week we shall discuss about Linux and Macintosh File Systems

Reference

[1] Laykin, E. (2013). *Investigative computer forensics: the practical guide for lawyers, accountants, investigators, and business executives*. John Wiley & Sons.

[2] Wikimedia. (n.d.). https://upload.wikimedia.org/wikipedia/commons/8/8e/Portable_forensic_tableau.JPG

[3] Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning.

[4] Cory A ,. Harlan C ,. (2011) *Digital Forensics with Open Source Tools, Elsevier*, Inc.