Computer Forensics

Week 2: Data Acquisition

Lecturer: Lemi Agrey Oliver

Email: codingissweet@gmail.com

Kumi University

www.kumiuniversity.ac.ug

Content

- ❑ Introduction to data acquisitions
- ❑ Storage formats
- ❑ Partitioning and Formatting Procedure
- ❑ DD Command
- ❑ Image capture with FTK Imager Lite
- ❑ Steps to follow when validating data Acquisition
- ❑ Characteristics of hashing algorithms
- ❑ Validation tools
- ❑ Remote acquisition tools
- ❑ Network acquisition
- ❑ Methods of Remote Acquisition
- ❑ etc

Introduction to Data Acquisition

- Acquisition of evidence is the first most important step in any digital forensic case. It is described as collecting data for further investigation[2]
- In computer forensics arena, data acquisition refers to the process of collecting digital data with the aim of presenting it as evidence
- There are two types of data acquisition in forensics which are live acquisition and static acquisition
- Our focus in this lecture will be on static acquisition. Live acquisition will be discussed in the future lectures
- Its important to mention however that the focus of acquisition is shifting towards live acquisition due to the whole disk encryption challenge with modern operating systems, coupled to acquisition of data that is in the volatile memory

Introduction to Data Acquisition+

- The requirements and the process of acquisition in both live and static acquisition are similar except that
- In static acquisition, a second copy made after the first static acquisition produces the same results,
- Live acquisition produces different results each time an acquisition is been made from the state data source
- The aim of static acquisition is to preserve the electronic evidence
- Learn to use different acquisition tools to ensure the integrity of the acquisition tool selected
- Some of those tools will be mention but will by no means be an exhaustive list

Understanding Storage Formats for Digital Evidence

- There are basically three acquisition data formats as can be seen below
  - ✓ Raw format
  - ✓ Advanced Forensic Format
  - ✓ Proprietary format
- **Raw format**
  - ✓ Refers to the bit by bit copying of data from one disk to an other
- **Merits**
  - ✓ Fast data transfer
  - ✓ Ability to overlook data errors on the source disk
  - ✓ Can be easily read by most forensic tools

Understanding Storage Formats for Digital Evidence+

❑ Demerits of the Raw Format

- ✓ Requires a disk that is either larger than the source or at least of the same size
- ✓ Ignores the marginal sectors on the source disk meaning that the degree of retry is minimum

❑ Advanced Forensic Format[1]

- ✓ Capable of producing compressed or uncompressed image files
- ✓ No size restriction for disk-to-image files
- ✓ Space in the image file or segmented files for metadata
- ✓ Simple design with extensibility
- ✓ Open source for multiple computing platforms and OSs
- ✓ Internal consistency checks for self-authentication

Understanding Storage Formats for Digital Evidence++

❑Proprietary format

- ✓Proprietary format refers to a file format specification that is proprietarily owned by an individual enterprise or group and there is no attempt for an openness standard and documentation by the confession.
- ✓This is highly closed data that may turn not easy to reach by the forensic analysts and getting specialized software or tools in the retrieval and analysis of data that was archived inside such formats.
- ✓In case of any need, reverse engineering, or use by the vendor's proprietary software that supports access to the fact, be it in the data structure or content, support may be put into use.

Understanding Storage Formats for Digital Evidence++

- Examples of proprietary format includes EnCase Evidence File Format (.E01), AccessData Forensic Toolkit Image (.AD1, X-Ways Forensics Disk Image (.E01), etc
- Merits of Proprietary format
  - ✓ Proprietary formats are often designed to work seamlessly with a particular software or platform, which can lead to more efficient and accurate data acquisition.
  - ✓ Proprietary formats may include built-in security features that help protect the integrity and confidentiality of the acquired data.

Understanding Storage Formats for Digital Evidence+++

- ✓ Vendors of proprietary software may offer customization options for their formats, allowing users to tailor data acquisition processes to their specific needs.
- ✓ Users of proprietary formats may have access to technical support from the software vendor, which can be helpful in troubleshooting issues and ensuring successful data acquisition.
- ✓ While proprietary formats may not be compatible with all software applications, they are often compatible with the software provided by the vendor, ensuring a smooth data acquisition process.
- ✓ Proprietary formats may offer advanced features and functionality that are not available in standard or open formats, allowing for more comprehensive data acquisition.

Understanding Storage Formats for Digital Evidence++++

- Demerits of Proprietary format
  - ✓ Users may become dependent on a specific software vendor's tools and formats, limiting their ability to switch to alternative solutions in the future.
  - ✓ Proprietary software and formats often require the purchase of licenses, which can be expensive, especially for organizations that require multiple licenses or use the software on a large scale.
  - ✓ Proprietary formats may not be compatible with other software or systems, making it difficult to share or transfer data between different platforms.

Understanding Storage Formats for Digital Evidence++++

- ✓ If a software vendor discontinues support for a proprietary format, users may no longer be able to access or use data stored in that format, leading to data loss or obsolescence.
- ✓ There is a risk that proprietary formats may not be well-documented or standardized, which can make it difficult to verify the integrity of the acquired data or to ensure its long-term preservation.
- ✓ While proprietary formats may include security features, they may also be more vulnerable to security risks, as their inner workings are not as transparent as open formats.

Understanding case information and legal issues[3]

- What is the nature of the investigation? Is it a narcotics case, homicide, or employee misconduct? As you hear this information, you formulate your plan on how you want to proceed.
- What digital evidence do you expect to find at the scene? There can be situation where the investigator is only looking for a single laptop and we found multiple laptops, multiple desktops, and many mobile devices.
- What is the legal justification? For law enforcement—what is the rationale behind the search? Consent? A search warrant? It doesn't matter whether it is written consent or a written search warrant
- As a government and corporate digital forensic investigator, I have had limits on what I can search for or view on digital devices many times.
- Who are the subjects and suspects and what roles do they play in the investigation? Now, depending on your role, you may or may not have any contact with the subjects and suspects involved.

Determining the Best Acquisition Method

- As already discussed in the earlier slides, the two types of acquisitions are live acquisition and static acquisition
- Static acquisition is basically carried out on systems that were seizure during search and seizure will live acquisition is carryout one running systems or programs
- Even thought preference is given to static acquisition, however a number of factors sometimes hinders it for example evidence from password protected or encrypted systems might be easy to acquire when the computer is left on by the suspects
- Also acquiring RAM data can only be possible when the computer is still powered on. This is because RAM is a volatile memory

Determining the Best Acquisition Method

- It then can not go without saying that, the acquisition method basically depends on the nature of the case and the circumstance at hand
- It is worthwhile to mention that Elcomsoft Forensic Disk Decryptor can be used to decrypt encrypted disk

Factors to consider when selecting an Acquisition method

- **Volatility of Evidence (Live vs. Dead Acquisition),** Consider whether a live or dead acquisition is more appropriate. Live acquisitions are performed on running systems and capture volatile data, such as open network connections and running processes. Dead acquisitions are conducted on powered-off systems and provide a static snapshot.
- **Nature of the Case(Criminal vs. Civil Cases),** the nature of the case may influence the acquisition method. Criminal cases may require more rigorous procedures, while civil cases might have different requirements.
- **Device Type (Computers vs. Mobile Devices),** different acquisition methods may be suitable for computers, mobile devices, or other digital storage media. For example, mobile devices often require specialized tools and techniques.

Factors to consider when selecting an Acquisition method+

- **Admissibility,** ensure that the chosen acquisition method complies with legal standards and is admissible in court. Follow proper procedures, maintain chain of custody, and adhere to relevant laws and regulations.
- **Preservation of Evidence, u**se write-blocking devices or techniques to ensure the integrity of the original evidence. This prevents any unintentional modifications during the acquisition process.
- **Time Constraints(Speed vs. Precision),** Consider the urgency of the investigation and whether a quick acquisition is necessary. In some cases, a rapid acquisition may be more appropriate, while in others, a more thorough and time-consuming process may be required.

Factors to consider when selecting an Acquisition method++

- **Available Tools and Expertise,** Choose acquisition tools that are well-established, widely accepted in the forensic community, and appropriate for the specific device or storage media.
- Consider the expertise of the forensic examiner in using specific tools and techniques. The examiner's familiarity with the tools can impact the efficiency and reliability of the acquisition.
- **Remote vs. On-Site Acquisition,** In cases where on-site access is challenging, remote acquisition methods may be considered.

Factors to consider when selecting an Acquisition method++

- **Data Encryption,** Dealing with encrypted devices requires additional considerations. Determine whether to acquire the encrypted data itself or acquire it after decryption, considering legal and technical aspects.
- **Documentation and Reporting,** Document the acquisition process thoroughly, including the tools used, settings applied, and any issues encountered. This documentation is crucial for transparency and future verification.
- **Budget Constraints,** Consider budget constraints when choosing acquisition tools and methods. There are both commercial and open-source tools available, and the choice may depend on the available resources.
- **Post-Acquisition Verification,** After acquiring the data, verify its integrity using hash values. This ensures that the acquired data matches the original source and hasn't been altered.

Others considerations in the choice of Forensic tools

- The size of the disk of the suspect's device
- Whether the source disk is retainable as evidences or supposed to be returned
- Time available for the acquisition of the digital evidence
- The location of the digital evidence source

Methods of forensic data acquisition

- There are several methods for acquiring forensic data, each with its own advantages and disadvantages depending on the specific situation and needs of the investigation.
- **The four methods are**
- **Creating a disk to image file**, this process involves capturing an exact copy of a storage device, like a hard drive, USB stick, or memory card, preserving all its data, including used, unused, and deleted files
- **Creating disk to disk**, this involves copying all the data, including operating systems, files, settings, and even unused space, from the source disk to the target disk

Methods of forensic data acquisition+

- **Creating a logical disk-to-disk or disk-to-data file,** involves copying only specific files and folders from a storage device instead of capturing the entire drive like a disk image.
- **Creating a sparse data copy of a file or folder,** involves replicating only the parts of the original file that actually contain data, leaving all unused portions "empty" or filled with predefined values (usually zeros).

Acquisitions based on the Acquisition types

Physical acquisition

- **Bit-stream disk-to-image**, This is the most common method and involves creating an exact, bit-by-bit copy of the entire storage device, including used, unused, and deleted data. It ensures the highest level of data integrity but requires significant storage space and can be slow.
- **Logical acquisition**, this method copies only specific files and folders that are relevant to the investigation. It's faster and saves storage space but risks missing crucial evidence if not carefully targeted.
- **Selective acquisition**, This involves acquiring specific data types like email, web browsing history, or chat logs. It offers fine-grained control but requires knowledge of the target data and potential issues with legal admissibility

Acquisitions based on the Acquisition types+

Live acquisition

- Memory acquisition, This captures the RAM content of a running system, preserving volatile data like active processes and network connections. It's crucial in incident response but requires specialized tools and expertise.
- Network acquisition, This captures network traffic flowing through a device or network segment, helping investigate cyberattacks or data exfiltration. It requires network monitoring tools and understanding of potential legal implications.

Acquisitions based on the Acquisition types++

Cloud acquisition

- **API-based acquisition**, Many cloud providers offer APIs for forensic data retrieval, allowing access to specific user data like emails or documents. It's convenient but subject to provider terms and potential legal challenges.
- **Web browser download**, In some cases, cloud data can be downloaded directly through the web browser, but this might not capture all relevant information and metadata.

Acquisitions based of the Acquisition types++++

Mobile device acquisition

- **Physical acquisition**, Similar to computers, bit-stream or logical acquisitions can be performed on mobile devices. Specialized tools and procedures are often needed.
- **Logical acquisition**, Mobile forensics tools extract specific data like contacts, messages, and call logs. Consider potential limitations and legal implications.

Contingency Planning for Image Acquisitions

- Dealing with electronic evidence involves essential responsibilities to protect it from loss and ensure the integrity of the investigative process.
- Contingency planning is necessary to address probable software or hardware failures during data acquisition, curtailing risks and ensuring the effectiveness of forensic investigations.
- Duplicate imaging is a standard practice in digital forensics to mitigate the risk of data loss or corruption during acquisition.
- Notwithstanding time and resource limitations, the effort to create identical images is invaluable in safeguarding the integrity of evidence.

Contingency Planning for Image Acquisitions+

Utilizing Multiple Imaging Tools

- Employing multiple imaging tools, such as FTK Imager Lite and X-Ways Forensics, enhances data acquisition reliability.
- Different tools utilize varying methods to copy data, providing redundancy and ensuring comprehensive coverage of the digital evidence

Considerations for Single Tool Usage

- In scenarios where only one imaging tool is available, making two images using the same tool is recommended, especially for critical investigations.
- Utilizing different compression settings for each image can further diversify redundancy measures.

Contingency Planning for Image Acquisitions++

Addressing Host Protected Area (HPA) Challenges

- Some acquisition tools may not copy data within the Host Protected Area (HPA) of a disk drive, necessitating alternative solutions.
- Hardware acquisition tools, like Belkasoft or ILookIX IXImager, equipped with write-blockers, offer access to HPA, ensuring comprehensive data acquisition.

Challenges of Whole Disk Encryption

- Whole disk encryption, such as BitLocker, poses challenges for static acquisitions, requiring decryption keys for access.
- Contingency planning involves strategies to deal with encrypted drives, including manual decryption processes and utilizing specialized tools like Elcomsoft Forensic Disk Decryptor.

Contingency Planning for Image Acquisitions+++

- In criminal investigations, obtaining decryption keys may be challenging due to suspects' reluctance to cooperate, necessitating alternative approaches.
- Understanding legal considerations surrounding decryption processes is crucial to navigate potential legal hurdles effectively.
- Effective data acquisition in digital forensics requires meticulous planning and proactive measures to address potential challenges.
- By implementing redundancy measures, leveraging diverse imaging tools, and staying abreast of encryption technologies, forensic investigators can enhance the integrity and efficacy of their investigations.

Utilizing Acquisition Tools for Digital Forensics

- Forensic acquisition tools play a pivotal role in extracting evidence from suspect drives in digital forensics investigations.
- This session will explore the significance of acquisition tools, their usage with different operating systems, and the deployment of forensic boot CDs/USB drives for data acquisition

Windows-Based Acquisition Tools

- Many forensics software vendors offer acquisition tools designed for Windows platforms, simplifying the process of evidence extraction.
- Utilizing hot-swappable devices like USB-3, FireWire 1394A/B, or SATA enhances convenience and flexibility during data acquisition.

Utilizing Acquisition Tools for Digital Forensics+

Challenges with Windows and Linux OSs

- Windows and Linux operating systems pose challenges in maintaining evidence integrity due to automatic drive mounting processes.
- To prevent contamination, employing well-tested write-blocking hardware devices is crucial, although acceptance varies among jurisdictions
- Some older Windows and Linux tools may not be able to acquire data from a disk’s HPA.

Utilizing Acquisition Tools for Digital Forensics++

Mini-WinFE Boot CDs and USB Drives

- A Mini-Windows Forensic Environment (Mini-WinFE) is a lightweight forensic boot disk or USB drive that is specifically designed to provide forensic capabilities without altering or compromising the target system.
- It allows forensic examiners to boot a live Windows environment from external media, enabling them to perform various forensic tasks, such as acquiring data, analyzing systems, and conducting investigations.

Creating Mini-WinFE

- **Choose a Compatible Version,** Mini-WinFE is typically built using a stripped-down version of a Windows operating system. Choose a Windows version that is compatible with the forensic tools you intend to use.

- **Select Forensic Tools,** Determine the forensic tools you want to include in your Mini-WinFE. Commonly used tools may include imaging tools, file analysis utilities, and network analysis software.

- **Prepare the Bootable Media,** Mini-WinFE can be created on a bootable CD/DVD or a USB drive. Choose the media type based on your preferences and the available hardware

Creating Mini-WinFE Boot CD

- **Use ISO Creation Software,** Download and use ISO creation software to compile the necessary files, including the stripped-down Windows OS and selected forensic tools, into a bootable ISO image.
- **Burn ISO to CD/DVD,** Once the ISO image is created, burn it to a CD/DVD using a disc burning tool. Ensure that the CD/DVD is bootable, allowing the system to start from it.

Creating Mini-WinFE Boot USB Drive

- **Prepare USB Drive,** Format the USB drive, ensuring it is large enough to accommodate the Mini-WinFE files. Make the USB drive bootable using tools like Rufus or Win32 Disk Imager.

Creating Mini-WinFE Boot USB Drive

- **Copy Files,** Copy the Mini-WinFE files, including the stripped-down Windows OS and forensic tools, onto the bootable USB drive. Ensure the necessary boot files are in the correct locations.
- **Verify Bootability,** Test the bootable USB drive on a test system to ensure it starts properly. Adjust configurations or files as needed to resolve any boot issues.

Using Mini-WinFE

- **Boot from CD or USB,** Insert the Mini-WinFE CD or plug in the USB drive into the target system. Boot the system from the CD or USB drive to launch the Mini-WinFE environment.
- **Perform Forensic Tasks,** Use the Mini-WinFE environment to perform various forensic tasks, such as acquiring disk images, analyzing files, and conducting live system investigations.
- **Preserve Evidence,** When performing forensic tasks, adhere to best practices for evidence preservation. Minimize changes to the target system, use write-blocking when necessary, and document all actions taken.

Using Mini-WinFE+

- **Generate Reports,** Document the findings and actions taken during the forensic analysis. Create detailed reports that can be used in legal proceedings.
- Linux OS offers features suitable for digital forensics, particularly data acquisitions.
- Older Linux versions can access a drive that isn't mounted, allowing physical access for reading data.
- Forensic Linux Live CDs are recommended for acquiring USB drives without a write-lock switch.

Linux Live CD Distributions for Digital Forensics

- Linux Live CD distributions provides useful tools for digital forensics work, offering extra utilities not normally found in standard Linux distributions.
- These distributions are designed to safeguard the integrity of connected storage media during data acquisition and analysis.
- Linux Live CDs are ISO images that can be burned to a CD or DVD.
- Some distributions are tailored for Linux OS recovery, while others are specifically crafted for digital forensics tasks.

Linux Live CD Distributions for Digital Forensics+

- Certain Linux ISO images are purpose-built for digital forensics, containing tools and configurations optimized for acquiring and analyzing data.
- These distributions ensure that connected storage media, such as USB drives, remain unmounted or mounted as read-only to preserve data integrity.

Examples of Linux distributions for forensics

- Penguin Sleuth Kit, CAINE (Computer Aided Investigative Environment), Deft, Kali Linux (formerly BackTrack), Knoppix, SANS Investigate Forensic Toolkit (SIFT)

Creating and Using Linux Live CDs

- Download the desired ISO image and burn it to a CD/DVD using burner software like Roxio or Nero.
- Ensure the CD/DVD is bootable by following instructions in the burner software's Help menu.
- Alternatively, use a USB drive by transferring the ISO image using tools like ISO to USB.
- Test the Live CD on your workstation by booting from it, checking the BIOS settings to prioritize booting from the CD/DVD drive.
- Linux Live CDs load the operating system into the computer's RAM, which may affect performance, especially when using GUI tools.
- Troubleshoot any video display issues by trying different computers with various video cards.

Preparing a Target Drive for Acquisition in Linux

- Preparing a target drive for acquisition in Linux involves partitioning and formatting it, ensuring compatibility with forensic analysis tools.
- This section outlines the step-by-step process for partitioning and formatting a Microsoft FAT drive from a Linux environment.
- Linux OS offers tools to modify non-Linux file systems like Microsoft FAT and NTFS.
- While Linux can format and read FAT file systems by default, the NTFS-3G driver enables mounting and writing data to NTFS partitions.

Partitioning and Formatting Procedure

- **Boot Linux and Connect the Drive,** Ensure Linux is running, and connect the USB, FireWire, or SATA external drive.
- **Access Shell Prompt,** Open a shell window if not already available.
- **Switch to Superuser (Root) Mode,** Type **su** and enter the root password to gain superuser privileges.
- **List Connected Disk Devices,** Use the command **fdisk -l** to list all connected disk devices.
- **Partition the Disk Drive,** use **fdisk /dev/sda** to access the disk for partitioning.

Partitioning and Formatting Procedure+

- **Create a New Partition,** select options to create a new primary partition on the disk.
- **Change Partition to FAT32 File System,** Use the command **t** to change the partition type to Windows 95 FAT32 file system.
- **Save Partition Changes,** Save the changes made by typing **w** and pressing Enter.
- **Format the Partition,** Use **mkfs.msdos -vF32 /dev/sda1** to format the partition as FAT32.
- **Close Shell Session,** Type **exit** to close the shell window.

Acquiring Data with dd in Linux

- Acquiring data from a suspect computer is a critical aspect of forensic analysis.
- In Linux environments, the **dd** command plays a central role in this process by facilitating the extraction of raw data from storage devices.

Prerequisites for Data Acquisition

- Before performing data acquisition with **dd**, ensure the following
- A forensics Linux Live CD is available.
- An external drive (USB, FireWire, or SATA) for storing acquired data.
- Knowledge of how to configure the suspect computer's BIOS to boot from the Linux Live CD.
- Familiarity with relevant shell commands for data acquisition.

Understanding the dd Command

- The **dd** command, short for "data dump," is a versatile tool available on UNIX and Linux distributions.
- It operates at a low level, bypassing file system structures to read and write data directly from/to storage devices.

Caution and Considerations

- Extreme caution is advised when using the **dd** command to prevent data loss or corruption.
- Mistakes such as reversing input/output fields can lead to irreversible damage to original evidence drives.

Using dd for Data Acquisition

- **Preparation,** Boot the suspect computer from a Linux Live CD and connect the external drive.
- **Accessing Shell Prompt,** If not already at a shell prompt, enter superuser mode and list connected drives using **fdisk -l**.
- **Creating a Mount Point,** Make a directory in **/mnt** for the target drive partition.
- **Mounting the Target Drive,** Use **mount -t vfat /dev/sda5 /mnt/sda5** to mount the target drive partition.
- **Navigating to Target Drive,** Change the default directory to the mounted target drive using **cd /mnt/sda5**.
- **Performing Data Acquisition,** Use **dd** in conjunction with **split** to create segmented volumes for acquiring data from the suspect drive.
- **Completing Acquisition,** After acquiring data, dismount the target drive using **umount /dev/sda5**.

Overview of FTK Imager Lite

- FTK Imager Lite is a component of the AccessData Forensic Toolkit, offering robust features for forensic data acquisitions.
- Unlike the licensed version, FTK Imager Lite is free and does not require a USB dongle for licensing.
- It supports various file formats, including AccessData .ad1, EnCase .e01, and raw format files, enabling comprehensive analysis of evidence disks.

Capturing an Image with AccessData FTK Imager Lite

- Acquiring digital evidence is a critical step in forensic investigations. AccessData FTK Imager Lite is a powerful tool designed to capture images of suspect drives, facilitating the preservation and analysis of evidence.
- In this lecture, we'll explore the steps involved in using FTK Imager Lite to create disk images.

Connecting the Suspect Drive

- **Documenting Chain of Evidence,** before proceeding, ensure proper documentation of the chain of evidence for the drive intended for acquisition.

Capturing an Image with AccessData FTK Imager Lite+

- **Drive Removal and Configuration,** safely remove the drive from the suspect's computer, and for IDE drives, configure jumpers as necessary.
- **Connection to Write-Blocker,** Connect the suspect drive to a USB or FireWire write-blocker device to prevent any alterations to the data during acquisition.
- **Creating Storage Folder,** establish a storage folder on the target drive, typically on the C drive, ensuring sufficient free space for the acquired data.

Steps for Image Capture with FTK Imager Lite

- **Boot Forensic Workstation,** Start the forensic workstation using an installed write-blocker device to maintain data integrity.
- **Connect Devices,** Connect the evidence drive to the write-blocking device and the target drive to a USB external drive if needed.
- **Launching FTK Imager Lite,** Start FTK Imager Lite and proceed with the acquisition process.
- **Selecting Source Drive,** Choose the source drive from which the image will be captured.

Steps for Image Capture with FTK Imager Lite+

- **Image Creation,** Configure image settings, including verification options and image type (e.g., Raw dd format).
- **Specifying Destination,** Select the location to save the image file, ensuring adequate space and adjusting fragment size if necessary.
- **Initiating Acquisition,** Start the acquisition process and monitor its progress.
- **Verification and Completion,** Review the verification results after completion to ensure the integrity of the acquired image.

Validating Data Acquisitions

- Ensuring the integrity of digital evidence is paramount in computer forensics. Validation of data acquisitions is crucial to maintaining the reliability of evidence.
- In this section, we'll delve into various tools and methods used to validate digital evidence

Steps to follow when validating data Acquisition

- Perform checks to ensure that the data acquired is complete and accurate. This can include comparing checksums or hash values of the acquired data with the original data to detect any changes.
- Verify that the data acquired matches the expected data. This can involve comparing the acquired data with known good data or using other validation techniques to ensure the correctness of the acquired data.

Steps to follow when validating data Acquisition+

- Check the metadata associated with the acquired data to ensure that it is accurate and complete. This can include verifying timestamps, file sizes, and other relevant metadata.
- Ensure that the acquired data is consistent across different sources or components. This can involve checking for duplicate data, inconsistent data formats, or other inconsistencies.
- Validate the acquired data against predefined criteria or rules to ensure that it meets the required quality standards. This can include checking for data outliers, anomalies, or other issues that may affect the data quality.

Steps to follow when validating data Acquisition++

- If applicable, perform data sampling to validate the acquired data. This involves selecting a subset of the data and validating it to ensure that it is representative of the entire dataset.
- Maintain a log of all data acquisitions and validation activities, including details such as the date and time of acquisition, the source of the data, and any validation results.
- Whenever possible, use automated tools and scripts to validate data acquisitions. This can help streamline the validation process and reduce the risk of human error.

Understanding Hashing Algorithms

- A hashing algorithm is a cryptographic function that takes an input and returns a fixed-size string of bytes, which typically represents a 'digest' or 'hash' of the input.
- Hashing algorithms are designed to be fast to compute and deterministic, meaning the same input will always produce the same hash value.
- Hashing algorithms generate unique digital fingerprints, or hash values, for data sets such as files or disk drives.
- Even minor alterations in data result in vastly different hash values, ensuring integrity.
- Though rare, collisions—where different data produces the same hash value—can occur with MD5 and SHA-1 algorithms but are generally not a concern for forensic examinations.

Characteristics of hashing algorithms

- **Deterministic,** given the same input, a hashing algorithm will always produce the same output. This property is essential for verifying data integrity and authenticity.
- **Fixed Output Size,** Hash functions produce a fixed-size output, regardless of the size of the input. For example, the SHA-256 hashing algorithm always produces a 256-bit hash value.
- **Irreversibility,** Hash functions are designed to be irreversible, meaning it should be computationally infeasible to reverse-engineer the original input from the hash value.
- **Collision Resistance,** A good hashing algorithm should be resistant to collisions, which occur when two different inputs produce the same hash value. This property is crucial for maintaining the integrity of hashed data.

Validation Tools

- **Byte-by-Byte Comparison,** Programs like X-Ways Forensics, X-Ways WinHex, and IDM Computing Solution's UltraCompare allow for detailed comparison of data files.
- **Linux Validation Methods,** Linux provides built-in utilities like md5sum and sha1sum for hashing files, partitions, or entire disk drives.
- Commands like **dd** and **dcfldd** in Linux offer options for data validation, utilizing hashing algorithms.
- **Validating dd-Acquired Data,** Using commands like **md5sum**, hash values for segmented volumes of a suspect drive can be computed and compared to validate data integrity.

Validation Tools+

- **Validating dcfldd-Acquired Data, dcfldd** incorporates validation options like **hash** and **hashlog**, allowing for the creation of hash output files during acquisition.
- The **vf** option verifies image files against the original medium for non segmented acquisitions.
- **Windows Validation Methods,** Unlike Linux, Windows lacks built-in hashing tools, but third-party programs like OSForensics, Autopsy, EnCase, and FTK offer various validation techniques.

Using Remote Network Acquisition Tools

- Recent advancements in forensic tools have introduced the capability to remotely acquire disk data or fragments, providing forensic examiners with enhanced flexibility and efficiency.
- Remote acquisition tools enable the connection to a suspect computer over a network, allowing data retrieval without physical access.
- These tools vary in functionality, from requiring manual intervention on the suspect computer to secretly acquiring data through encrypted links.

Methods of Remote Acquisition

ProDiscover Incident Response

- Integrates as a network intrusion analysis tool, allowing remote acquisitions.
- Requires the installation of the PDServer remote agent on the suspect computer.
- Offers features such as capturing volatile system state information and analyzing running processes remotely.
- Remotely view and listening to IP ports
- Run hash comparison

Methods of Remote Acquisition+

EnCase Endpoint Investigator

- Developed by Guidance Software, facilitates remote acquisition and analysis.
- Supports multiple operating systems and file systems, enabling wide-ranging investigations.

R-Studio Network Edition

- Designed for data recovery, can remotely access networked systems and recover various file systems.
- Creates raw format acquisitions for forensic analysis.

Methods of Remote Acquisition++

WetStone US-LATT PRO

- Connects to networked computers remotely and performs live acquisitions of connected drives
- Part of a suite of forensic tools developed by WetStone.

F-Response

- Vendor-neutral remote access utility compatible with any digital forensics program.
- Sets up a secure, read-only connection to remote computers, allowing access to raw data.

Summary

- In this week's lecture we discussed what an acquisition is, the different data formats, discussing the merits and demerits of each of these formats ,we further looked at the types of acquisitions which we identified as live acquisition and static acquisition. We then went further to look at the different acquisition methods, contingency planning, acquisitions tools and many others.
- Next week we shall now draw our attention to Processing Crime and Incident Scenes. See you there

Reference

1. Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning. Page 175
2. Moric, Z., Redzepagic, J., & Gatti, F. (2021). ENTERPRISE TOOLS FOR DATA FORENSICS. *Annals of DAAAM & Proceedings*.
3. Oettinger, W. (2020). *Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing Ltd.