Forensic Duplication and Acquisition:

Forensic Duplication:

- Forensic duplication, also known as forensic imaging or forensic copying, is a crucial process in digital forensics.
- It involves creating an exact replica or duplicate of a digital storage device, such as a hard drive, solid-state drive (SSD), or a memory card, in a forensically sound manner.
- Forensic duplicates are created to preserve the original data in its unaltered state so that it can be analyzed without the risk of contamination
- The purpose of forensic duplication is to preserve the integrity of the original evidence while allowing investigators to examine and analyze the data without affecting the original source.

Here are some of the benefits of using forensic duplicates:

- Preserves the original data in its unaltered state
- Prevents the original data from being altered
- Allows for analysis of the original data without the risk of contamination
- Is admissible in court

Here are some of the challenges of using forensic duplicates:

- Can be time-consuming and expensive to create
- Requires specialized tools and techniques
- Can be difficult to verify the integrity of the duplicate.

Types of Forensic Duplicates

There are three main types of forensic duplicates:

1. Physical duplicates: This is a bit-by-bit copy of the original digital media, including all data, metadata, and system information. Physical duplicates are created using specialized forensic software and hardware, such as write-blockers, to ensure that the original data is not altered or destroyed during the duplication process.

2. Logical duplicates: This is a copy of the logical structure of the digital media, which includes the file system and directory structure. Logical duplicates are used to recover deleted files or to analyze the file system of the digital media. Logical duplicates are created using specialized software that reads the file system and creates a copy of the file system information.

3. Partial duplicates: This is a selective copy of the digital media, which includes only the relevant data for the investigation. Partial duplicates are used when the digital media is too large to acquire or when only a specific portion of the data is relevant to the investigation. Partial duplicates can be created using specialized software that allows forensic analysts to select and extract specific data from the digital media.

Each type of forensic duplicate has its own advantages and disadvantages, and the type of duplicate used depends on the specific requirements of the investigation. Forensic analysts must select the appropriate type of duplicate to ensure that the integrity of the data is preserved and that the evidence will be admissible in court.

Some common **techniques** of forensic duplication include:

1. Bit-stream Imaging: This is a method of creating a bit-by-bit copy of the original storage device, including unallocated space and deleted files.
2. Live Duplication: This technique involves copying active data on a running system to a separate storage device or destination, without shutting down the system.
3. Logical Duplication: This technique involves copying only the relevant data files, directories, or partitions of a storage device to a separate storage device or destination.
4. Remote Duplication: This technique involves remotely copying data from a system or storage device over a network to a separate storage device or destination.
5. Targeted Duplication: This technique involves copying only specific files or data that are relevant to the investigation.

🚀 Forensic duplication tools

Forensic duplication tools, also known as forensic imaging tools, are software or hardware solutions used in digital forensics to create forensic copies or duplicates of digital storage media such as hard drives, solid-state drives (SSDs), USB drives, memory cards, and optical discs.

These tools play a critical role in the preservation and analysis of digital evidence, ensuring the integrity and accuracy of the original data.

Here are a few commonly used forensic duplication tools:

- **FTK Imager**: FTK Imager, developed by AccessData, is a widely used tool for creating forensic images. It allows forensic investigators to acquire data from various sources, including hard drives, memory, and removable media. FTK Imager can create forensic images in various formats, including EnCase, raw dd, and SMART.
- **EnCase**: EnCase Forensic, developed by Guidance Software (now part of OpenText), is a comprehensive forensic software suite that includes a duplication feature. EnCase allows investigators to create forensic images, perform evidence preservation, and analyze digital evidence. It supports a wide range of storage media and offers advanced features for data recovery and analysis.
- **dd**: dd is a command-line tool available in most Unix-based operating systems. It is a simple and powerful utility for creating disk images. With dd, forensic investigators can create bit-for-bit copies of disks or partitions. It can also convert between different image formats and perform other data manipulation tasks.
- **Paladin Forensic Suite**: Paladin Forensic Suite is a Linux-based live forensic environment that includes various tools for digital forensics, including imaging and duplication utilities. It provides a user-friendly interface and supports a wide range of hardware devices.
- **Tableau Forensic Duplicators**: Tableau produces a range of hardware-based forensic duplicators, such as the Tableau TD3 and Tableau TD2u. These devices are used for duplicating storage media quickly and efficiently. They offer features like write-blocking and hashing to ensure the integrity of the copied data.

🚢Data Acquisition:

- Data acquisition refers to the process of collecting digital data from electronic devices for forensic analysis.
- The process of data acquisition is becoming increasingly accurate, simple, and versatile.

There are two types of data acquisition: static and live/volatile data acquisition.

⚓ static

- Static data refers to nonvolatile data, which does not change its state even after the system is shut down.
- Dead acquisition refers to the process of extracting and gathering these data in an unaltered manner from storage media. Sources of nonvolatile data include hard drives, DVD-ROMs, USB drives, flashcards, smart-phones, and external hard drives.
- This type of data exists in the form of emails, word processing documents, web activity, spreadsheets, slack space, swap files, unallocated drive space, and various deleted files.
- Investigators can repeat the dead acquisition process on well-preserved disk evidence.

Static data recovered from a hard drive include the following:

- ♣ Temporary (temp) files
- ♣ System registries
- ♣ Event/system logs
- ♣ Boot sectors
- ♣ Web browser cache
- ♣ Cookies and hidden files

live data:

- The live data acquisition process involves the collection of volatile data from devices when they are live or powered on.
- Volatile information, as present in the contents of RAM, cache, DLLs, etc. is dynamic, and is likely to be lost if the device to be investigated is turned off.
- It must therefore be acquired in real time.
- Examination of volatile information assists in determining the logical timeline of a security incident and the users that are likely to be responsible for it.

Depending on the source from which they are obtained, volatile data are of two types:

♣ System data

System information is the information related to a system, which can serve as evidence in a security incident. This information includes the current configuration and running state of the suspect computer. Volatile system information includes system profile (details about configuration), login activity, current system date and time, command history, current system uptime, running processes, open files, startup files, clipboard data, users logged in, DLLs, and shared libraries. The system information also includes critical data stored in the slack spaces of the hard disk drive.

♣ Network data

Network information is the network-related information stored in the suspect system and connected network devices. Volatile network information includes open connections and ports, routing information and configuration, ARP cache, shared files, and services accessed.

Express the differences between static acquisition and live acquisition?

	Static Acquisition	Live Acquisition
Definition	Copying data from a storage device that is powered off or not in use	Copying data from a storage device that is currently in use
Device state	Device is powered off or not in use	Device is running and in use
Data integrity	Data is not being modified during the acquisition process	Data may be modified during acquisition due to system activities or processes
Data volatility	Data is not volatile and remains unchanged	Data is volatile and may change during the acquisition process
Evidence admissibility	More likely to be admissible in court due to the static nature of the acquisition	May be challenged in court due to potential modifications to data during acquisition
Acquisition time	Generally quicker as device is not in use	May take longer due to potential system activities and processes
Data recovery	More challenging to recover deleted or damaged data	Easier to recover deleted or damaged data due to the device being in use
Suitable for	Suitable for devices that are not in use, or for backup and archival purposes	Suitable for devices that are actively being used or for acquiring volatile data
Examples of tools	dd, FTK Imager	FTK Imager, EnCase, AccessData, X-Ways Forensics

Network forensics

Network forensics is a subcategory of digital forensics that essentially deals with the examination of the network and its traffic going across a network that is suspected to be involved in malicious activities, and its investigation for example a network that is spreading malware for stealing credentials or for the purpose analyzing the cyber-attack.

As the internet grew cybercrimes also grew along with it and so did the significance of network forensics, with the development and acceptance of network-based services such as the World Wide Web, e-mails, and others.

With the help of network forensics, the entire data can be retrieved including messages, file transfers, e-mails, and, web browsing history, and reconstructed to expose the original transaction.

For identifying the attacks investigators must understand the network protocols and applications such as web protocols, Email protocols, Network protocols, file transfer protocols, etc.

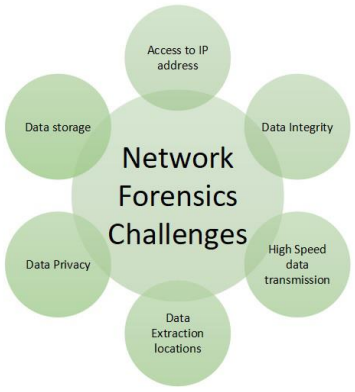
Processes Involved in Network Forensics:

Some processes involved in network forensics are given below:

1. **Identification**: In this process, investigators identify and evaluate the incident based on the network pointers.
2. **Safeguarding**: In this process, the investigators preserve and secure the data so that the tempering can be prevented.
3. **Accumulation**: In this step, a detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
4. **Observation**: In this process, all the visible data is tracked along with the metadata.
5. Investigation: In this process, a final conclusion is drawn from the collected shreds of evidence.
6. **Documentation**: In this process, all the shreds of evidence, reports, conclusions are documented and presented in court.

Challenges in Network Forensics:

- The biggest challenge is to manage the data generated during the process.
- Intrinsic anonymity of the IP.
- Address Spoofing.



Advantages:

- Network forensics helps in identifying security threats and vulnerabilities.
- It analyzes and monitors network performance demands.
- Network forensics helps in reducing downtime.
- Network resources can be used in a better way by reporting and better planning.
- It helps in a detailed network search for any trace of evidence left on the network.

Disadvantage:

The only disadvantage of network forensics is that It is difficult to implement.

Wireshark:

Wireshark is an open-source network monitoring tool. We can use Wireshark to capture the packet from the network and also analyze the already saved capture.

Wireshark can be installed through the below commands in Ubuntu.

```
$ sudo apt-get install wireshark [This is for installing Wireshark]
```

Once Wireshark is launched, we can select the interface where we want to capture, and Wireshark window looks like below

There are three sections inside Wireshark

- Packet List
- Packet Details
- Packet Bytes

Packet List: This section displays all packets captured by Wireshark. We can see the protocol column for the type of packet.

Packet Details: Once we click on any packet from Packet List, packet details show supported networking layers for that selected packet.

Packet Bytes: Now, for the selected field of the selected packet, hex (default, It can be changed to binary also) value will be shown under the Packet Bytes section in Wireshark.

OR

1. Install and launch Wireshark on your computer.

2. Select the network interface you want to capture traffic from, and click on the "Start" button to begin capturing packets.

3. Analyze the captured packets in real-time to identify any suspicious network activity or anomalies.

4. Use Wireshark's built-in filtering and search features to search for specific network traffic patterns or data, such as IP addresses, protocols, or keywords.

5. Save the captured packets to a file for further analysis and investigation.

6. Use Wireshark's packet analysis features to examine the saved capture file in detail, including analyzing packet headers, payloads, and metadata.

7. Use the information obtained from the packet analysis to reconstruct the network traffic and determine the sequence of events that occurred during the incident.