# What is Digital Forensic :

Digital forensics is the process of storing, analyzing, retrieving, and preserving electronic data that may be useful in an investigation. It includes data from hard drives in computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices. The process's goal of digital forensics is to collect, analyze, and preserve evidence.

# What are uses of Digital Forensic :

Computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device. Often, computer forensics is used to uncover evidence that could be used in a court of law.
Computer forensics also encompasses areas outside of investigations. Sometimes professionals in this field might be called upon to recover lost data from drives that have failed, servers that have crashed or operating systems that have been reformatted.

Computer forensics is primarily used for two separate purposes, investigation and data recovery. Here's a brief summary of how each is handled by professionals within the field.

## Investigations

Computer forensics can be an essential facet of modern investigations. When a crime is committed and an investigation is started, one of the more common places to look for clues is the computer or cell phone of a suspect. This is where a computer forensics professional enters the picture.

When a suspect has been identified and their personal computer or cell phone taken into evidence, a computer forensics professional goes searching for data that is relevant to the investigation. When searching for information, they need to be careful to follow detailed procedures that allow their findings to be used as evidence. The information they uncover, whether it be documents, browsing information or even metadata, may then be used by prosecution to create a compelling case against the suspect.

### Data Recovery

Aside from working to collect evidence, computer forensics professionals can also work in data recovery. When it comes to data recovery, forensics professionals can take broken hard drives, crashed servers and other compromised devices and retrieve the data that was previously lost. This is valuable for anyone who has lost important data outside of uncovering criminal evidence, such as businesses who have experienced a system crash.

## Difference between Computer Forensics vs. Cyber Security

To those outside the profession, computer forensics and cyber security can seem rather similar. Both deal with criminals and computers, but despite this initial similarity, the function of each practice differs greatly.

To recap, computer forensics is focused largely on data recovery. The data recovered is often used as evidence in criminal trials, but sometimes is recovered for companies after a data loss incident. Additionally, the criminals that computer forensics professionals investigate are not always cybercriminals. Because almost everyone uses a computer, there is often valuable information on their personal device that can contribute to an investigation.

Cyber security, on the other hand, is more concerned with defense. Cyber security professionals work under a variety of job titles, but nearly all of them work to build networks and systems that are secure from potential attackers. Sometimes they use hacking to test their own networks or the networks of a client to find areas of weakness and bolster them.

## Steps of Digital Forensics

The steps involved in the Digital Forensic is as follows:

### Identification

This is the initial stage in which the individuals or devices to be analyzed are identified as likely sources of significant evidence.

### Preservation

It focuses on safeguarding relevant electronically stored information (ESI) by capturing and preserving the crime scene, documenting relevant information such as visual images, and how it was obtained.

### Analysis

It is a methodical examination of the evidence of the information gathered. This examination produces data objects, including system and user-generated files, and seeks specific answers and points of departure for conclusions.

### Documentation

These are tried-and-true procedures for documenting the analysis's conclusions, and they must allow other competent examiners to read through and duplicate the results.

### Presentation

The collection of digital information, which may entail removing electronic devices from the crime/incident scene and copying or printing the device(s), is critical to the investigation.

## Objectives of Digital Forensics

Knowing the primary objectives of using digital forensics is essential for a complete understanding of what is digital forensics:

- It aids in the recovery, analysis, and preservation of computers and related materials for the investigating agency to present them as evidence in a court of law
- It aids in determining the motive for the crime and the identity of the primary perpetrator
- Creating procedures at a suspected crime scene to help ensure that the digital evidence obtained is not tainted
- Data acquisition and duplication: The process of recovering deleted files and partitions from digital media in order to extract and validate evidence
- Assists you in quickly identifying evidence and estimating the potential impact of malicious activity on the victim
- Creating a computer forensic report that provides comprehensive information on the investigation process
- Keeping the evidence safe by adhering to the chain of custody.

## Types of Digital Forensics

As digital data forensics evolves, several sub-disciplines emerge, some of which are listed below:

### Computer Forensics

It analyzes digital evidence obtained from laptops, computers, and storage media to support ongoing investigations and legal proceedings.

### Mobile Device Forensics

It entails obtaining evidence from small electronic devices such as personal digital assistants, mobile phones, tablets, sim cards, and gaming consoles.

### Network Forensics

Network or cyber forensics depends on the data obtained from monitoring and analyzing cyber network activities such as attacks, breaches, or system collapse caused by malicious software and abnormal network traffic.

### Digital Image Forensics

This sub-specialty focuses on the extraction and analysis of digital images to verify authenticity and metadata and determine the history and information surrounding them.

### Digital Video/Audio Forensics

This field examines audio-visual evidence to determine its authenticity or any additional information you can extract, such as location and time intervals.

### Memory Forensics

It refers to the recovery of information from a running computer's RAM and is also known as live acquisition.

## Challenges Faced by Digital Forensics

Due to the evidentiary nature of digital forensic science, rigorous standards are required to withstand cross-examination in court. Challenges faced by digital forensics are:

- Extracting data from locked, or destroyed computing devices is one of the challenges that digital forensic investigators face
- Finding specific data entries within massive amounts of data stored locally or in the cloud
- Keeping track of the digital chain of custody
- Ensuring data integrity throughout an investigation

## Advantages of Digital Forensics

The following are some advantages of digital forensics:

- Enables Digital Evidence Analysis

Computer forensics uses investigation and analysis techniques to collect and preserve evidence from a specific computing device to present it in court.

- Aids in the Identification of Criminals

Law enforcement officers can frequently track down suspects and piece evidence together to prosecute them by analyzing data on computers and other digital devices.

- It Is Capable of Recovering Deleted Data

One advantage of using computer forensics to recover deleted data is that it is relatively simple to do. Most of the time, all you need is the right software and a little know-how.

- Enlightens on How Crimes Are Committed

Computer forensics can shed light on how crimes are committed by analyzing digital evidence.

- It Has the Potential to Be Used to Prevent Future Crimes

Law enforcement can better target their investigative efforts if they understand how criminals use computers to commit crimes.

## Disadvantages of Digital Forensics

The following are some disadvantages of digital forensics:

- Prolonged Procedure

Computer forensics is a lengthy process. Data collection and analysis can take days or weeks.

- Requires Specialized Knowledge and Skills

Computer forensics is a process that collects, examines, and reports digital evidence using specialized skills and knowledge.

- Can Be Costly

Computer forensics can be costly because it requires specialized equipment and software and is frequently performed by a specialist.

- Obtaining Evidence May Necessitate a Court Order

Obtaining the evidence may necessitate a court order. It means there could be a delay in getting the evidence, giving the perpetrator time to destroy or tamper with it.

- Evidence Can Be Easily Destroyed or Manipulated

One of the most severe issues with computer forensics is the ease with which evidence can be destroyed or tampered with. Even if investigators successfully recover deleted files or damaged hard drives, there is no guarantee that the evidence has not been tampered with.

## When Is Digital Forensics Used in a Business Setting?

Digital forensics is an integral part of the Incident Response process for businesses. Forensic Investigators identify and document details of a criminal incident as evidence for law enforcement. The rules and regulations that govern this process are frequently helpful in proving innocence or guilt in a court of law.

## Who Is a Digital Forensics Investigator?

A digital forensics investigator wants to follow the evidence and solve a crime virtually.

Assume a company suffers a security breach, resulting in stolen data. In this case, a computer forensic analyst would investigate how the attackers gained access to the network, where they went on the network, and what they did, whether they stole information or planted malware. In such cases, a digital forensic investigator's role is to recover data such as photos, documents, and emails from hard drives and any other data devices that store data such as flash drives that have been damaged, deleted, or otherwise manipulated.

## History of Digital Forensics

The following is a brief history of digital forensics:

The term "digital forensics" is relatively new, having first appeared in the late 1900s after being known as "computer forensics." The first group of computer forensic analysts consisted of law enforcement officers who enjoyed playing with computers. The Federal Bureau of Investigation (FBI) established the Computer Analysis and Response Team (CART) in 1984, followed by the Metropolitan Police in the United Kingdom a year later.

At the turn of the century, law enforcement, investigators, and specialists recognized the need for standard techniques, procedures, and protocols in digital forensics and other forensic sciences. Many informal guidelines were used until discussions and conferences were held to establish computer forensic methodology and practices on what computer forensics is today.

## Phases of Digital Forensics

The following are the phases of digital forensics:

### Phase I - Initial Response

The first response is the action taken immediately following a security incident. The nature of the incident heavily influences it.

### Phase II - Seizure and Search

During this phase, the professionals look for the devices used in the crime. These devices were then carefully seized to extract information from them.

### Phase III - Gather Evidence

Following the search and seizure phase, professionals collect data using the acquired devices. They have well-defined forensic methods for handling evidence.

### Phase IV: Protect the Evidence

The forensic team should have access to a secure location where they can store the evidence. They determine whether the information gathered is correct, authentic, and accessible.

### Phase V - Data Collection

Data acquisition is when Electronically Stored Information (ESI) from suspected digital assets is retrieved. It aids in gaining insights into the incident, whereas an improper process can alter the data, jeopardizing the evidence's integrity.

### Phase VI - Data Analysis

The accountable staff scans the acquired data to identify the evidentiary information that can be presented to the court during data analysis. This phase involves examining, identifying, separating, converting, and modeling data to convert it into useful information.

### Phase VII - Evidence Evaluation

The evidence assessment process connects the evidential data to the security incident. Based on the scope of the case, a thorough assessment should be performed.

### Phase VIII - Reporting and Documentation

It is the post-investigation phase, which includes reporting and documenting all findings. In addition, the report should contain sufficient and acceptable evidence following the court of law.

### Phase IX - Testify as an Expert Witness

Forensic investigators should approach the expert witness to confirm the evidence's accuracy. An expert witness is a professional who investigates a crime to obtain evidence.

## What Are Digital Forensics Tools?

Digital forensic tools were developed to examine data on a device without causing damage to it. Digital forensic tools can also assist ICT managers in proactively identifying risk areas. Digital forensic tools are currently classified as digital forensic open-source tools, digital forensic hardware tools, and various others.

Popular instruments include:

- Forensic disc controllers: enable the investigator to read the data from a target device while preventing it from being modified, corrupted, or erased.
- Hard-drive duplicators: enable the investigator to copy data from a suspect thumb drive, hard drive, or memory card to a clean drive for analysis.
- Password recovery devices: crack password-protected storage devices using machine learning algorithms.

Here are some of the most popular digital investigation tools:

1 .Disk Analysis: Autopsy/Sleuth Kit Autopsy and Sleuth Kit are the most well-known forensics toolkits in digital forensics. The sleuth kit is command line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI based system that uses the sleuth kit behind the scenes.

2. Image Creation: FTK imager As autopsy does not have image creation functionality, so another tool need to be used. FTK manager is free software. It can be used to create disk images which can be analyzed using autopsy/sleuth kit.

3. Memory Forensic: Volatility For analysis of volatile memory, the most well-known and popular tool is volatility. It is open source, free and supports third party plugins. Volatility foundation holds annual contest for users to develop the useful extension to the framework.

4. Mobile Forensic: Cellebrite UFED A mobile-focused forensic tool might be a useful acquisition as growing importance of mobile forensic. Cellebrite UFED is the best commercial tool for mobile forensics and it supports various platforms and boasts exclusive tools for mobile device analysis.

5.Netwok Analysis: Wireshark Wireshark is most popular and widely used tool for network traffic analysis. It is free and open source, offers study for many different types of network traffic. Wireshark has easy to use GUI for traffic analysis and include wide range of functionality. It supports live traffic capture files for analysis.