**Digital Forensics –** Computer or digital forensics is a scientific method of investigation and analysis to gather evidence from digital media i.e., computers, mobile phones, servers, or network . It is primarily used for two separate purposes, **investigation, and data recovery.**

**Investigation-** first of all, the suspect is identified and his personal computer or cell phone is confiscated. A computer forensics professional searches 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 may be

- documents,

-browsing information

- even metadata can be used by prosecution to create a compelling case against the suspect.

Metadata describes how, when and by whom a particular set of data was collected, and how the data is formatted.

• Metadata is created when files are created and when edited

**Data Recovery-**

When it comes to data recovery, forensics professionals can take broken hard drives, crash servers and other compromised devices and retrieve the data that was previously lost.

**Steps in Computer Forensics (Process)**

1. **Identification-** it includes identification of evidence, where it is stored and how it is stored. It also includes identification of the resources that are required to carry out this process.
2. **Preservation-** it is ensured that data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.
3. **Analysis-** tools and techniques are identified. Data is processed through different tools and techniques. Interpret analysis and draw conclusion on the basis of evidence found.
4. **Documentation-** it includes documentation of the crime scene along with photographing, sketching and crime scene mapping.
5. **Presentation-** it is the process of summarization and explanation of conclusion based on collected facts.

**Types of Digital Forensics**

**Disk Forensics:**

It deals with extracting data from storage media by searching active, modified, or deleted files.

**Network Forensics:**

It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

**Wireless Forensics:**

It is a division of network forensics. The main aim of wireless forensics is to offer the tools need to collect and analyze the data from wireless network traffic.

**Database Forensics:**

It is a branch of digital forensics relating to the study and examination of databases and their related metadata (when and who has created the data, where it is stored and how it is stored).

**Malware Forensics:**

This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

The term payload is used to describe what a virus, worm or Trojan is designed to do on a victim's computer.

payload of malicious programs includes damage to data, theft of confidential information and damage to computer-based systems or processes.

**Email Forensics**

Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

**Memory Forensics:**

It deals with collecting data from system memory (HDD, system registers, cache, ) in raw form and then carving the data from Raw dump (to find a meaningful result from raw data).

**Mobile Phone Forensics:**

It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

**Advantages of Digital forensics**

* To ensure the integrity of the computer system.
* To produce evidence in court, which can lead to the punishment of the culprit.
* It helps the companies to capture important information if their computer systems or networks are compromised.
* Efficiently tracks down cybercriminals from anywhere in the world.
* Helps to protect the organization’s money and valuable time.
* Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal actions in the court.

**Disadvantages of Digital Forensics**

* Digital evidence accepted into court. However, it must be proved that there is no tampering.
* Legal practitioners must have extensive computer knowledge
* If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
* Lack of technical knowledge by the investigating officer might not offer the desired result (result of investigation depends on the capability of the investigating officer)

**Digital Signature**

A sender sends encrypted message to an intended receiver. If the sender also wishes to send evidence of his identity to the receiver, he encrypts a piece of information that makes sense to both, using his private key and sends it to the receiver. This encrypted piece of information is called the digital signature. Receiver uses sender's public key to decrypt sender's digital signature and to retrieve the information. If this information decrypts sensibly, receiver can be sure of the identity of the sender because digital signature must have been created using the private key that pairs with sender's public key.

This can also be used to ensure that the sender does not repudiate at a later stage. The piece of information that makes sense to both is in fact related to the actual message that is the subject of transmission.

Diagram

Description automatically generated

The piece of information is called the message digest and is generated from the actual message using some algorithm that the parties agree upon. One-way hash function is generally used as the algorithm for the creation of message digest.

* Sender generates message digest from the message, using one-way hash function as the algorithm.
* The sender encrypts message digest, using his private key and product is called digital signature.
* Sender sends digital signature to the receiver over the Internet.
* Receiver then does two things:
* Receiver recovers message digest by decrypting the digital signature using sender's public key.
* Receiver generates message digest by applying one-way hash function to the message that has also arrived.
* Receiver compares the two versions of message digest.

If the two versions of message digest are same, sender must have signed it and receiver can be sure of sender's identity. This also means that the sender cannot later deny having sent the message (sender cannot repudiate) because he must have signed the message digest.