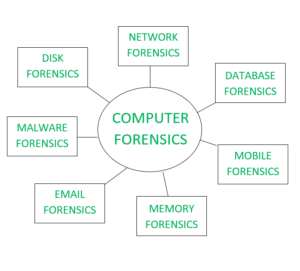
**Introduction of Computer Forensics**

**INTRODUCTION**

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it. 

**TYPES**

* Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
* Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
* Database Forensics: It deals with the study and examination of databases and their related metadata.
* Malware Forensics: It deals with the identification of suspicious code and studying viruses, worms, etc.
* Email Forensics: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
* Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
* Mobile Phone Forensics: It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.



**CHARACTERISTICS**

* Identification: Identifying what evidence is present, where it is stored, and how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
* Preservation: Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
* Analysis: Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
* Documentation: A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
* Presentation: All the documented findings are produced in a court of law for further investigations.



**PROCEDURE:**

The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene. Then the court warrant is obtained for the seizure of the evidence which leads to the seizure of the evidence. The evidence are then transported to the **forensics lab** for further investigations and the procedure of transportation of the evidence from the crime scene to labs are called chain of custody. The evidence are then copied for analysis and the original evidence is kept safe because analysis are always done on the copied evidence and not the original evidence.

The analysis is then done on the copied evidence for suspicious activities and accordingly, the findings are documented in a nontechnical tone. The documented findings are then presented in a court of law for further investigations.

**Some Tools used for Investigation:**

Tools for Laptop or PC –

* **COFFEE –** A suite of tools for Windows developed by Microsoft.
* **The Coroner’s Toolkit –** A suite of programs for Unix analysis.
* **The Sleuth Kit –** A library of tools for both Unix and Windows.

**APPLICATIONS**

* Intellectual Property theft
* Industrial espionage
* Employment disputes
* Fraud investigations
* Misuse of the Internet and email in the workplace
* Forgeries related matters
* Bankruptcy investigations
* Issues concerned the regulatory compliance

**Advantages of Computer Forensics :**

* To produce evidence in the court, which can lead to the punishment of the culprit.
* It helps the companies gather important information on their computer systems or networks potentially being compromised.
* Efficiently tracks down cyber criminals 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 action’s in the court.

**Disadvantages of Computer Forensics :**

* Before the digital evidence is accepted into court it must be proved that it is not tampered with.
* Producing and keeping electronic records safe is expensive.
* Legal practitioners must have extensive computer knowledge.
* Need to produce authentic and convincing evidence.
* If the tool used for digital forensics is not according to specified standards, then in a court of law, the evidence can be disapproved by justice.
* A lack of technical knowledge by the investigating officer might not offer the desired result.