## Digital Forensics and Incident Response

**🔑Digital Forensics: -**

“Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.”

* It is a science of finding evidence from digital media like a computer, mobile phone, server, or network.
* It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.
* Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

**🏮Objectives of computer forensics: -**

Here are the essential objectives of using Computer forensics:

* It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
* It helps to postulate the motive behind the crime and identity of the main culprit.
* Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
* Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
* Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
* Producing a computer forensic report which offers a complete report on the investigation process.
* Preserving the evidence by following the chain of custody.

**🏮Challenges faced by Digital Forensics:-**

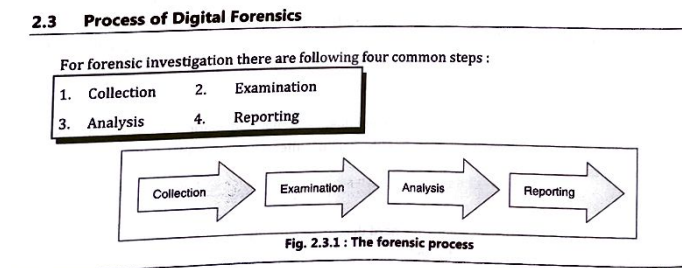
Here, are major challenges faced by the Digital Forensic:

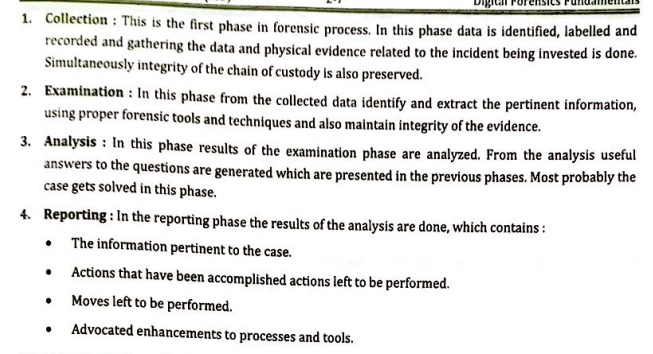
* The increase of PC’s and extensive use of internet access
* Easy availability of hacking tools
* Lack of physical evidence makes prosecution difficult.
* The large amount of storage space into Terabytes that makes this investigation job difficult.
* Any technological changes require an upgrade or changes to solutions.

**📍TYPES:**

1. **Disk Forensic**s: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
2. **Network Forensics**: It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
3. **Database Forensics**: It deals with the study and examination of databases and their related metadata.
4. **Malware Forensics**: It deals with the identification of suspicious code and studying viruses, worms, etc.
5. **Email Forensics**: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
6. **Memory Forensics:** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
7. **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.

**📍Process of Digital forensics:**





**📍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.

**Tools for Memory:**

* Volatility
* WindowsSCOPE
* Tools for Mobile Device :
* MicroSystemation XRY/XACT

**📕APPLICATIONS:**

* Intellectual Property theft
* Industrial espionage
* Employment disputes
* Fraud investigations

**📍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.

**📍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.

