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:-

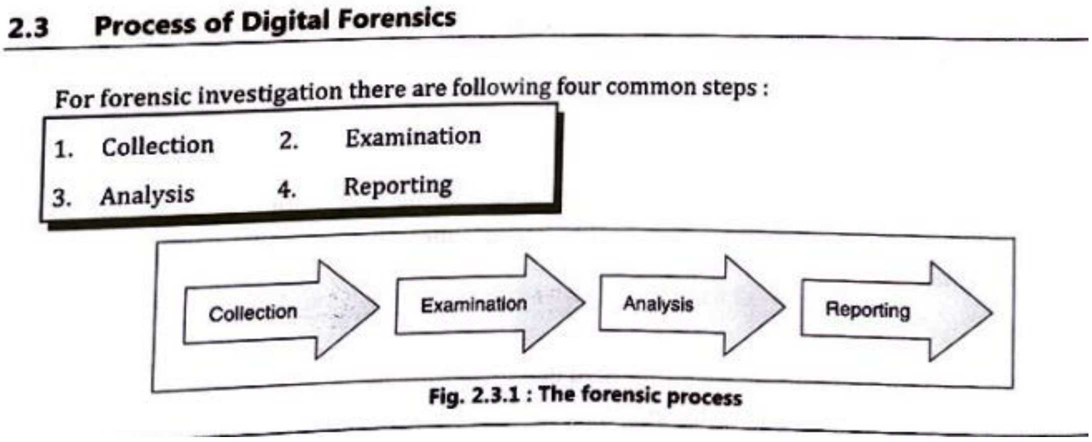
Here, are major challenges faced by the Digital Forensic:

- 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:



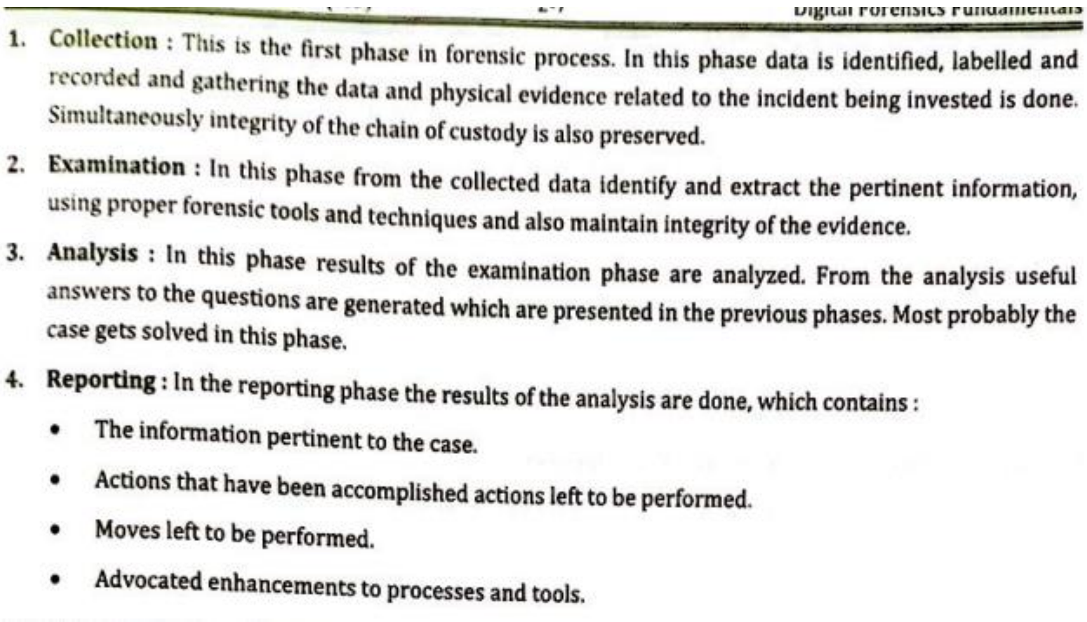
2.3 Process of Digital Forensics

For forensic investigation there are following four common steps :

1. Collection
2. Examination
3. Analysis
4. Reporting

Collection
Examination
Analysis
Reporting

Fig. 2.3.1 : The forensic process



1. **Collection :** This is the first phase in forensic process. In this phase data is identified, labelled and recorded and gathering the data and physical evidence related to the incident being invested is done. Simultaneously integrity of the chain of custody is also preserved.
2. **Examination :** In this phase from the collected data identify and extract the pertinent information, using proper forensic tools and techniques and also maintain integrity of the evidence.
3. **Analysis :** In this phase results of the examination phase are analyzed. From the analysis useful answers to the questions are generated which are presented in the previous phases. Most probably the case gets solved in this phase.
4. **Reporting :** In the reporting phase the results of the analysis are done, which contains :
   - The information pertinent to the case.
   - Actions that have been accomplished actions left to be performed.
   - Moves left to be performed.
   - Advocated enhancements to processes and tools.

📍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:

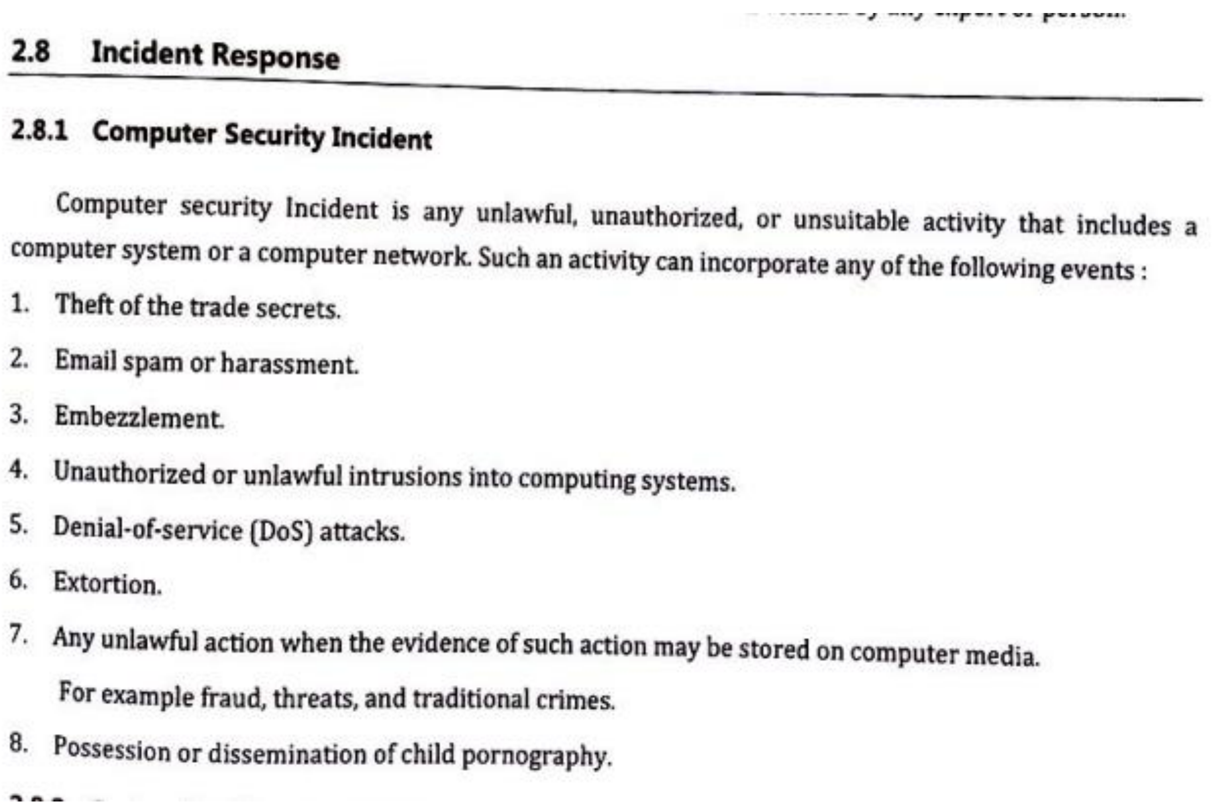
- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations

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.



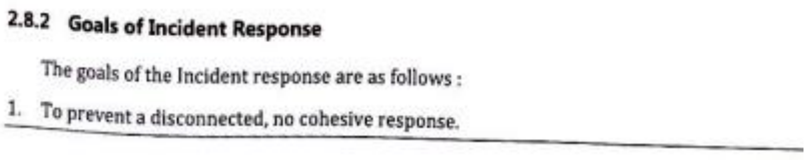
2.8 Incident Response

2.8.1 Computer Security Incident

Computer security Incident is any unlawful, unauthorized, or unsuitable activity that includes a computer system or a computer network. Such an activity can incorporate any of the following events :

1. Theft of the trade secrets.
2. Email spam or harassment.
3. Embezzlement.
4. Unauthorized or unlawful intrusions into computing systems.
5. Denial-of-service (DoS) attacks.
6. Extortion.
7. Any unlawful action when the evidence of such action may be stored on computer media.

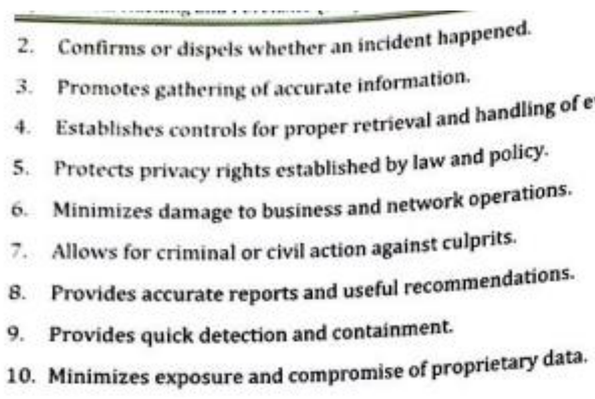
   For example fraud, threats, and traditional crimes.
8. Possession or dissemination of child pornography.



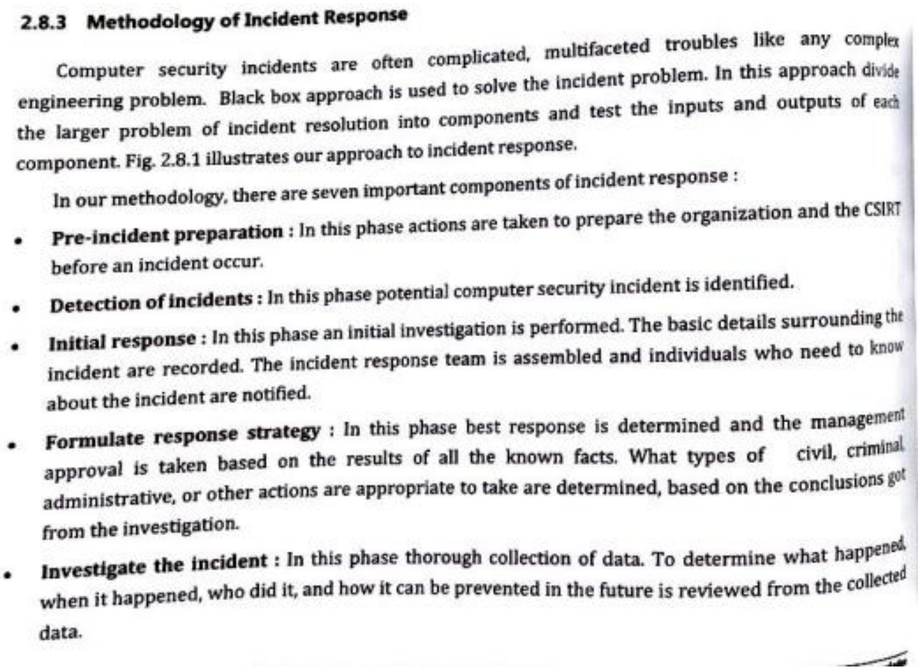
2.8.2 Goals of Incident Response

The goals of the Incident response are as follows :

1. To prevent a disconnected, no cohesive response.



2. Confirms or dispels whether an incident happened.
3. Promotes gathering of accurate information.
4. Establishes controls for proper retrieval and handling of evidence.
5. Protects privacy rights established by law and policy.
6. Minimizes damage to business and network operations.
7. Allows for criminal or civil action against culprits.
8. Provides accurate reports and useful recommendations.
9. Provides quick detection and containment.
10. Minimizes exposure and compromise of proprietary data.

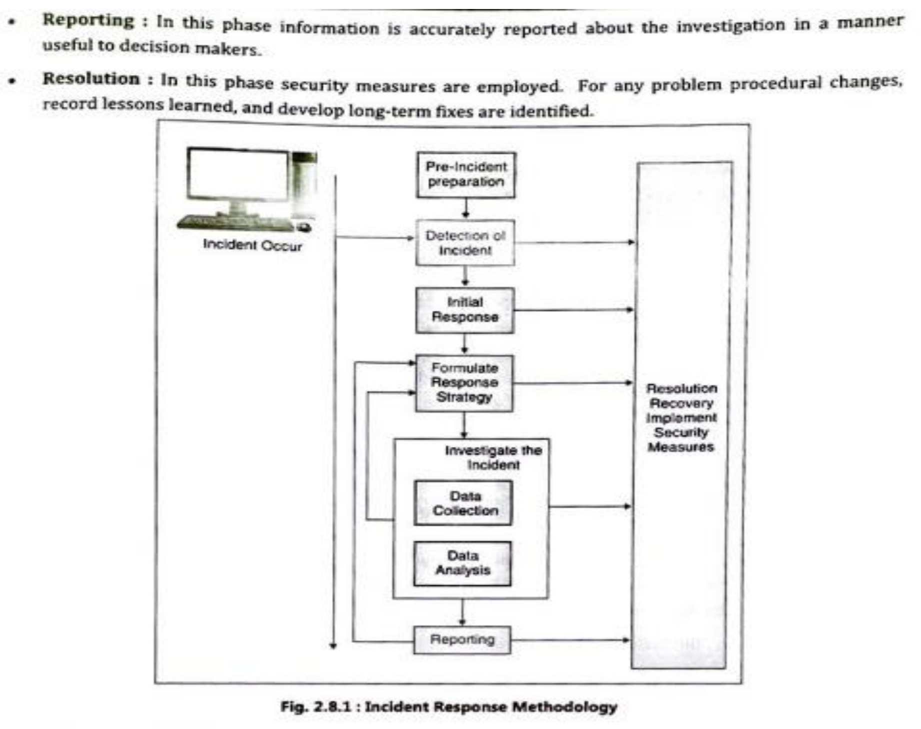


2.8.3 Methodology of Incident Response

Computer security incidents are often complicated, multifaceted troubles like any complex engineering problem. Black box approach is used to solve the incident problem. In this approach divide the larger problem of incident resolution into components and test the inputs and outputs of each component. Fig. 2.8.1 illustrates our approach to incident response.

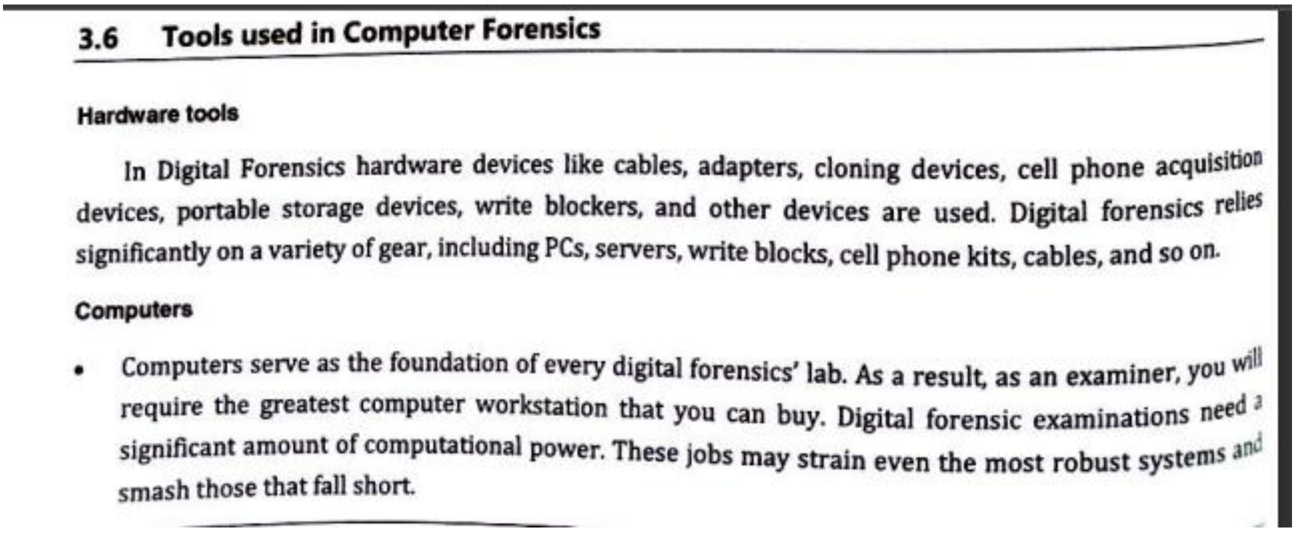
In our methodology, there are seven important components of incident response :

- **Pre-incident preparation :** In this phase actions are taken to prepare the organization and the CSIRT before an incident occur.
- **Detection of incidents :** In this phase potential computer security incident is identified.
- **Initial response :** In this phase an initial investigation is performed. The basic details surrounding the incident are recorded. The incident response team is assembled and individuals who need to know about the incident are notified.
- **Formulate response strategy :** In this phase best response is determined and the management approval is taken based on the results of all the known facts. What types of civil, criminal, administrative, or other actions are appropriate to take are determined, based on the conclusions got from the investigation.
- **Investigate the incident :** In this phase thorough collection of data. To determine what happened, when it happened, who did it, and how it can be prevented in the future is reviewed from the collected data.



- **Reporting :** In this phase information is accurately reported about the investigation in a manner useful to decision makers.
- **Resolution :** In this phase security measures are employed. For any problem procedural changes, record lessons learned, and develop long-term fixes are identified.

Fig. 2.8.1 : Incident Response Methodology



3.6 Tools used in Computer Forensics

Hardware tools

In Digital Forensics hardware devices like cables, adapters, cloning devices, cell phone acquisition devices, portable storage devices, write blockers, and other devices are used. Digital forensics relies significantly on a variety of gear, including PCs, servers, write blocks, cell phone kits, cables, and so on.

Computers

- Computers serve as the foundation of every digital forensics' lab. As a result, as an examiner, you will require the greatest computer workstation that you can buy. Digital forensic examinations need a significant amount of computational power. These jobs may strain even the most robust systems and smash those that fall short.