**Sipna College of Engineering & Technology,Amravati**

**Department Computer Science and Engineering**

**List Of Practical**

# 1.Introduction to Digital Forensics.

# Aim:Introduction to Digital Forensics

**Theory:**

Digital Forensic: 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.

## **Process of Digital forensics**

Digital forensics entails the following steps:

* Identification
* Preservation
* Analysis
* Documentation
* Presentation

### **Identification**

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

### **Preservation**

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

### **Analysis**

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

### **Documentation**

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

### **Presentation**

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson’s terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

## **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 offers 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.

### **Malware Forensics:**

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

### **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 (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

### **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.

## **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.

## **Example Uses of Digital Forensics**

In recent time, commercial organizations have used digital forensics in following a type of cases:

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

## **Advantages of Digital forensics**

Here, are pros/benefits of Digital forensics

* To ensure the integrity of the computer system.
* To produce evidence in the 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 action’s in the court.

## **Disadvantages of Digital Forensics**

Here, are major cos/ drawbacks of using Digital Forensic

* Digital evidence accepted into court. However, it is must be proved that there is no tampering
* Producing electronic records and storing them is an extremely costly affair
* Legal practitioners must have extensive computer knowledge
* Need to produce authentic and convincing evidence
* 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

**Conclusion**:Thus,We have to study the introduction of digital forensics.