UNIT I: INTRODUCTION TO DIGITAL FORENSIC

1.1 Learning Objectives

After completion of this unit, we will be able to:

- Learn What is Digital Forensic and types
- Know the past and evolution of digital forensics
- Describe various types of cybercrime
- Realize the benefits of computer forensics
- Identify about forensics readiness
- Implement forensics readiness plan

1.2 Introduction

Digital forensics, the art of recovering and analysing the contents found on digital devices such as desktops, notebooks/netbooks, tablets, smartphones, etc., was little-known a few years ago. However, with the growing incidence of cybercrime, and the increased adoption of digital devices, this branch of forensics has gained significant importance in the recent past, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations.

As a rule of thumb, "Forensic is the scientific tests or techniques used in connection with the detection of crime." - ***Wikipedia***.

Case Scenario

Suppose Mr X is the computer forensics investigator in Odisha and he has been appointed to inspect data-stealing case in an MNC in Bhubaneswar. The general manager of the organization has confidence in that some of his employees are involved in the case including the network crack and the transfer of the confidential data. Mr X has started his investigation, Analyze, Evaluate the case and collected the evidence and then he submitted his final report to the Authority. According to the report, four employees were found accountable for data theft/ data-stealing. Based on this report, a case has been lodged against them.

In the situation mentioned above, the organization was the client, Mr X was the service provider and the service that was being provided is called computer forensics & digital investigation services.

1.3 Definition of Computer Forensics

Computer Forensics is the process of using scientific techniques during the identification, collection, examination and reporting the evidence to the court. So what computer forensics is all about?

According to Dr H.B. Wolfe, computer forensics is, "A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media that can be presented in a court of law in a coherent and meaningful format."

If we further define computer forensics then, it is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.

Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.

The scope of computer forensics is not limited to investigating a crime only. Apart from this, computer forensics can be used for:

- Data recovery
- Log monitoring
- Data acquisition (from the retired or damaged devices)
- Fulfil the compliance needs

1.4 Cybercrime

Computer crime, or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Dr. Debarati Halder and Dr K. Jaishankar define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation-state is sometimes referred to as cyberwarfare.

Digital forensics is traditionally associated with criminal investigations and, as you would expect, most types of investigation centre on some form of computer crime. This sort of crime can take two forms; computer-based crime and computer-facilitated crime.

1.4.1 Computer-based crime

This is criminal activity that is conducted purely on computers, for example, cyber-bullying or spam. As well as crimes newly defined by the computing age it also includes traditional crime conducted purely on computers (for example, child pornography).

1.4.2 Computer facilitated crime

Crime conducted in the "real world" but facilitated by the use of computers. A classic example of this sort of crime is a fraud: computers are commonly used to communicate with other fraudsters, to record/plan activities or to create fraudulent documents.

Not all digital forensics investigations focus on criminal behavior; sometimes the techniques are used to incorporate (or private) settings to recover lost information or to rebuild the activities of employees.

1.5 Evolution of Computer Forensics

Most of the experts agree that the field of computer forensics began to develop more than 40 years ago.

By the 1970s, electronic crimes were increasing, especially in the financial sector. Most computers in this era were mainframes, used by trained people with specialized skills who worked in finance, engineering, and academia. White-collar fraud began when people in these industries saw a way to make money by manipulating computer data. One of the most well-known crimes of the mainframe era is the one-half cent crime. Banks commonly tracked money in accounts to the third decimal place or more. They used and still use the "rounding

up" accounting method when paying interest. If the interest applied to an account resulted in a fraction of a cent, that fraction was used in the calculation for the next account until the total resulted in a whole cent. It was assumed that sooner or later every customer would benefit.

Some computer programmers corrupted this method by opening an account for themselves and writing programs that diverted all the fractional monies into their accounts. In small banks, this practice amounted to only a few hundred dollars a month. In large banks with many branch offices, however, the amount reached hundreds of thousands of dollars.

The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents.

In 1984, FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.

By the early 1990s, specialized tools for computer forensics were available. In 1988, the International Association of Computer Investigative Specialists (IACIS), an international non-profit corporation composed of volunteer computer forensic professionals introduced training on software for forensics investigations. However, no commercial GUI software for computer forensics was available until ASR Data created Expert Witness for Macintosh. This software could recover deleted files and fragments of deleted files. One of the ASR Data partners later left and developed EnCase, which has become a popular computer forensics tool.

It was followed by the formation of International Organization on Computer Evidence (IOCE) in 1995, which aims to brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

With the rise in cybercrime, the G8 nations realized the importance of computer forensics, and in 1997 declared that - Law enforcement personnel must be trained and equipped to address high-tech crimes. In 1998, G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. In the same year, INTERPOL Forensic Science Symposium was held. The First FBI Regional Computer Forensic Laboratory established in 2000 at San Diego.

As computer technology continued to evolve, more computer forensics software was developed. "ILook", is a Cyber forensic tool maintained by the IRS Criminal Investigation Division and limited to law enforcement, can analyze and read special files that are copies of a disk. Access Data Forensic Toolkit (FTK) has become a popular commercial product that performs similar tasks in the law enforcement and civilian markets.

Computers are getting more powerful day by day, so the field of computer forensics must rapidly evolve. Previously, we had many computer forensic tools that were used to apply forensic techniques to the computer. However, we have listed a few best forensic tools that are promising for today's computers:

- SANS SIFT
- ProDiscover Forensic
- Volatility Framework
- The Sleuth Kit (+Autopsy)
- CAINE (Computer Aided Investigative Environment)
- Xplico
- X-Ways Forensics

In this material, we will try to discuss as many tools as possible but you should also refer to trade publications and Web sites, such as www.ctin.org (Computer Technology Investigators Network) and www.usdoj.gov (U.S. Department of Justice), to stay updated.

1.6 Different types of digital forensics

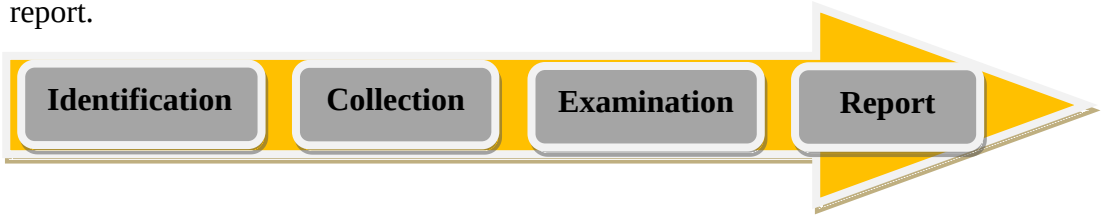
Digital forensics is a constantly evolving scientific field with many sub-disciplines. Some of these sub-disciplines are:

1) **Computer Forensics**: the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.
2) **Network Forensics**: the monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.
3) **Mobile devises Forensics**: the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.
4) **Digital Image Forensics**: the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
5) **Digital Video/Audio Forensics:** the collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
6) **Memory forensics:** the recovery of evidence from the RAM of a running computer, also called live acquisition.
7) **Cloud Forensics:** Cloud Forensics is actually an application within Digital Forensics which oversees the crime committed over the cloud and investigates on it.

1.7 Stages of Computer Forensics Process

The overall computer forensics process is sometimes viewed as comprising of four stages:

- **Assess the situation/ Identification:** Analyze the scope of the investigation and the action to be taken.
- **Acquire the data/ Collection:** Gather, protect, and preserve the original evidence.
- **Analyze the data/Examination:** Examine and correlate digital evidence with events of interest that will help you make a case.
- **Report the investigation:** Gather and organize collected information and write the final report.



Assess the situation/ Identification