SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

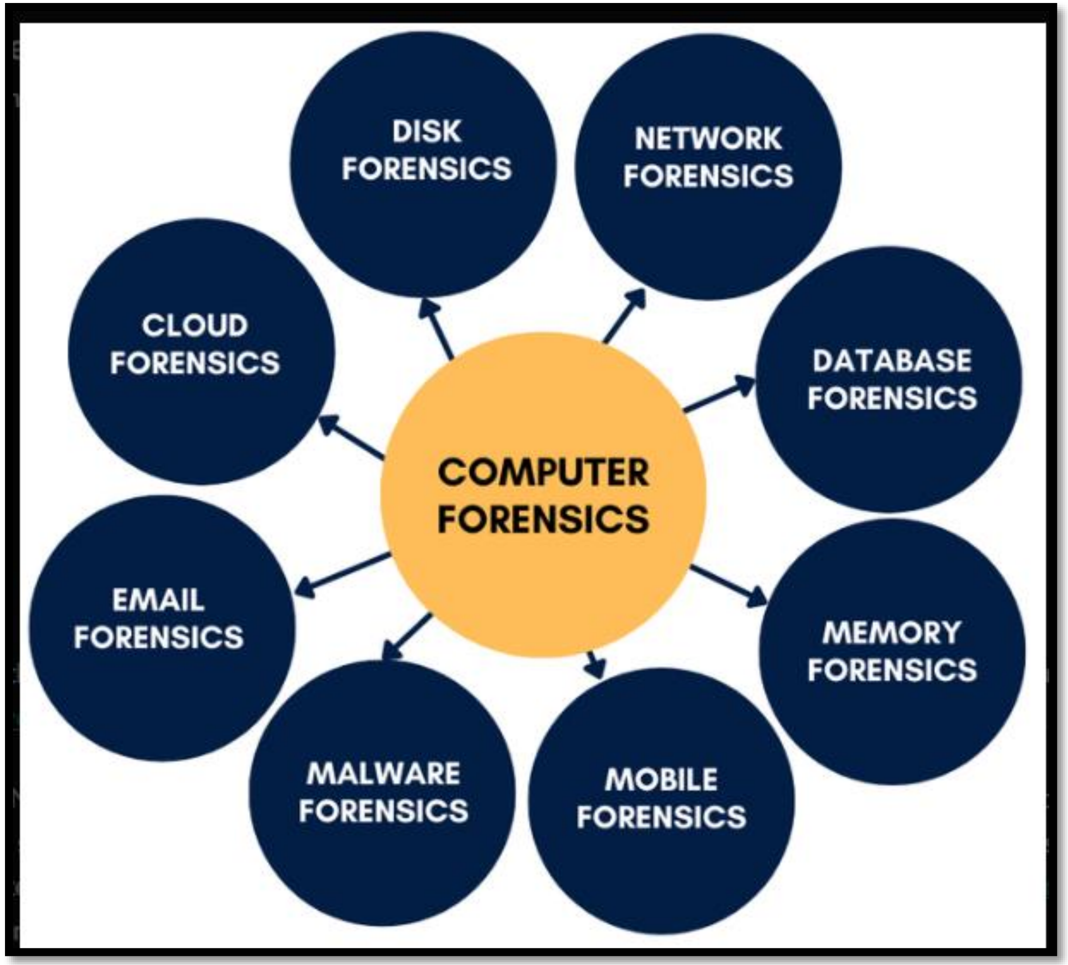
III YEAR / VI SEMESTER

Unit III- INTRODUCTION TO COMPUTER FORENSICS

Topic : Types of CF Techniques

Types of Computer Forensic

Computer forensics involves various techniques to investigate digital crimes and security incidents. These techniques help in collecting, analyzing, and preserving electronic evidence



Types of Computer Forensic

- **Disk Forensics:** It is the process by which experts take data recovered from physical storage devices such as hard disks, SSDs, USB flash drives, and memory cards with disc judges to recover deletions and hidden partitions.
- **Network Forensics:** Network forensics simply implies the investigation of network traffic to collect evidence regarding security incidents on systems, unauthorized access, or any other malicious activity that occurred in the system. Network forensics involves intercepting and capturing data packets and then analyzing their source to decipher cyber-attack origins, trace communication patterns, or gather some details about an incident.
- **Database Forensics:** It is the process of collection of information that is contained in a database, both data and related metadata. It uses the electronic data that is present in a database to detect any crime that had occurred, reconstruct the hints obtained, and solve the cases.
- **Memory Forensics:** Memory forensics focuses on the collection of information in a computer's volatile memory (RAM) and cache to extract information that is either active or in hibernation. It includes information like encryption keys, open network connections, and active programs that would not be available on conventional disk forensics.

Types of Computer Forensic

•**Mobile Forensics:** The procedure involves using special software with functions of extracting, investigating, and recovering (searching, analyzing, recovering, isolating) the data that is stored on Devices (i.e., smartphones, tablets, and GPS devices). In this process, investigations are recovering and breaking down the different data sets such as in/out text messages, phone calls, and any other data Tags. Lastly, these investigators search through data from other places where the offender was, such as location information and digital artifacts in the phones.

•**Malware Forensics:** The aim of malware forensics is finding, examining, and tracking down the attacking malware. The code is carefully examined to detect the various types of malicious programs that are stored in software e.g. trojan horses, ransomware, adware, viruses, etc to protect the software installed in the system. Researchers employ various techniques to examine malware samples to uncover their actions and effects on compromised and corrupt systems. Through comprehensive malware analysis including code structure, encoding techniques, and propagation methods, it is up to cybersecurity analysts to trace the attacks back to the source, mitigate the risks, and improve the cyber defenses.

Types of Computer Forensic

Email Forensics: It is the recovery and analysis of emails and information to collect digital evidence as findings to crack crimes and certain incidents. It can include schedules and contacts.

•**Cloud Forensics:** Cloud forensics is another discipline within digital forensics. It covers operations of finding, saving, investigating, and presenting cloud data in a court of law or any other matters that require investigation. It is about finding evidence that is stored in the cloud environment infrastructures by the name Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. In investigations of internal or external data breaches, improper access to the cloud platforms, or policy violations taking place on the cloud platform, investigators gather related evidence.

Types of Computer Forensic

1. Disk Forensics - Investigating storage media for deleted or hidden files.
2. Network Forensics - Analyzing network traffic for security breaches.
3. Memory Forensics - Examining volatile memory for live attack traces.
4. Mobile Forensics - Extracting data from smartphones and tablets.
5. Email Forensics - Investigating email headers and attachments.
6. Malware Forensics - Analyzing malicious software behavior and code.
7. Cloud Forensics - Collecting and analyzing cloud-based data.
8. **Database Forensics -** Analyzing database records and logs for manipulation or data theft.
9. **IoT Forensics -** Investigating digital evidence from **smart devices (CCTV, IoT sensors, smart home systems).**
10. **OS Forensics -** Investigating operating system artifacts (Windows Registry, event logs).

Any Query????

Thank you……