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 I- NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

Topic : Introduction to Cyber Forensic and Data Security

Overview of Cyber forensics: Definition and Importance

Cyber forensics, also known as computer forensics, is the practice of investigating and analyzing digital evidence to identify, preserve, recover, and present data in a manner that is legally admissible.
It is a critical field in the modern era, where technology plays a significant role in both personal and professional aspects of life.

Cyber forensics involves applying investigative techniques to digital devices like computers, smartphones, servers, and cloud systems to uncover evidence related to cybercrimes or digital incidents.

It helps law enforcement agencies and private organizations investigate cybercrime, identify perpetrators, and prevent future attacks.

Process in Cyber Forensics

•**Identification**: Recognizing potential digital evidence.

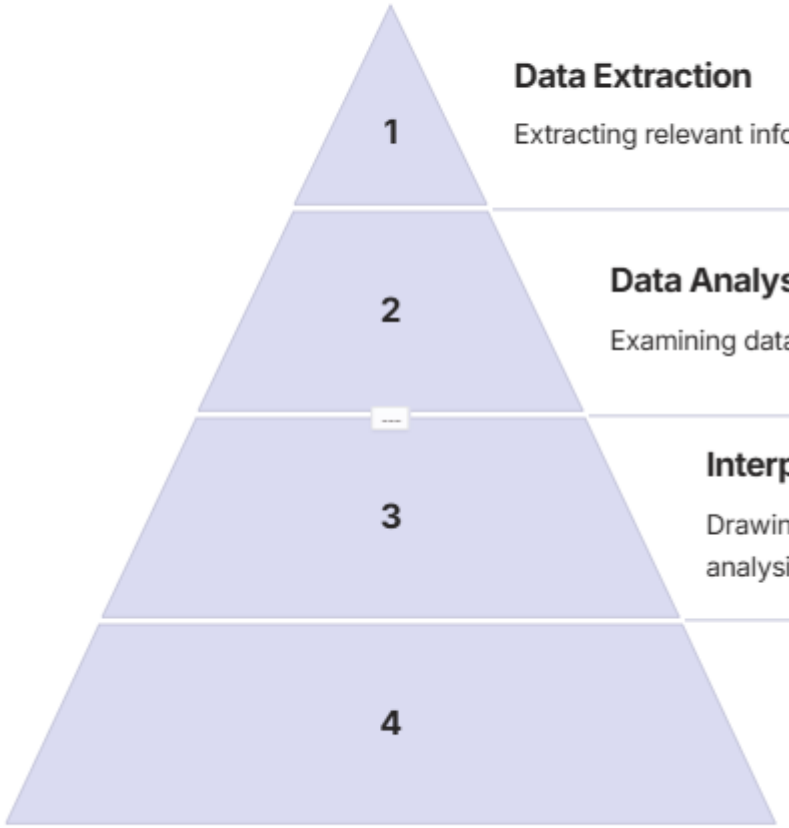
•**Preservation**: Securing and isolating evidence to prevent tampering.

•**Analysis**: Extracting meaningful information using tools and techniques.

•**Documentation**: Recording findings systematically for reporting.

•**Presentation**: Preparing evidence for court or stakeholders.

Forensic Analysis of Digital Evidence



Data Extraction

Extracting relevant information from data files and artifacts.

Data Analysis

Examining data for patterns, anomalies, and evidence of malicious activity.

Interpretation

Drawing conclusions and forming opinions based on the evidence analysis.

Reporting

Documenting findings and presenting them in a clear and concise manner.

Types of Cyberforensic Investigations

Malware Analysis

Investigating malicious software, including viruses, ransomware, and trojans.

Network Intrusion

Examining network traffic and logs to identify unauthorized access or malicious activity.

Data Breach

Investigating the theft or unauthorized disclosure of sensitive information.

Intellectual Property Theft

Tracking down the theft of copyrighted or trademarked content.

Cyber Forensic Tools and Technologies

1

Disk Imaging Tools

Creating bit-by-bit copies of hard drives for analysis.

2

Network Monitoring Tools

Capturing and analyzing network traffic to identify suspicious activity.

3

Data Recovery Tools

Recovering deleted files and data from damaged storage devices.

4

Forensic Analysis Software

Analyzing digital evidence for patterns, anomalies, and clues.

Applications and Challenges

Applications:

- Investigating cybercrimes.
- Recovering lost or corrupted data.
- Strengthening cybersecurity defenses.
- Assisting law enforcement and legal systems.

Challenges:

- Handling large volumes of data.
- Adapting to rapidly evolving technology.
- Ensuring data privacy and compliance with laws.

Any Query????

Thank you……