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 COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

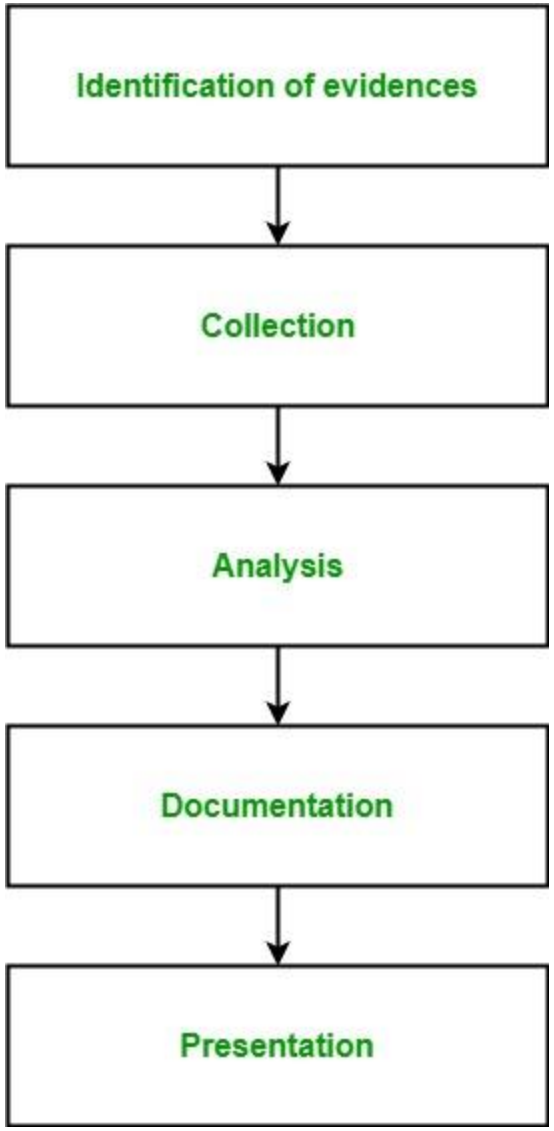
II YEAR / IV SEMESTER

Unit V- CYBER ANALYSIS

Topic 1 : Digital forensics

DIGITAL FORENSICS

- Digital forensics is the process of **storing, analyzing, retrieving,** and **preserving electronic data** that may be useful in an investigation.
- It includes data from hard drives in **computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices.**
- The process's goal of digital forensics is **to collect, analyze, and preserve evidence**.


Identification of evidences
Collection
Analysis
Documentation
Presentation

Steps of Digital Forensics

Identification:

- This is the initial stage in which the individuals or devices to be analyzed are identified as likely sources of significant evidence.

Preservation:

- It focuses on safeguarding relevant electronically stored information (ESI) by capturing and preserving the crime scene, documenting relevant information such as visual images, and how it was obtained.

Analysis:

- It is a methodical examination of the evidence of the information gathered. This examination produces data objects, including system and user-generated files, and seeks specific answers and points of departure for conclusions.

Documentation:

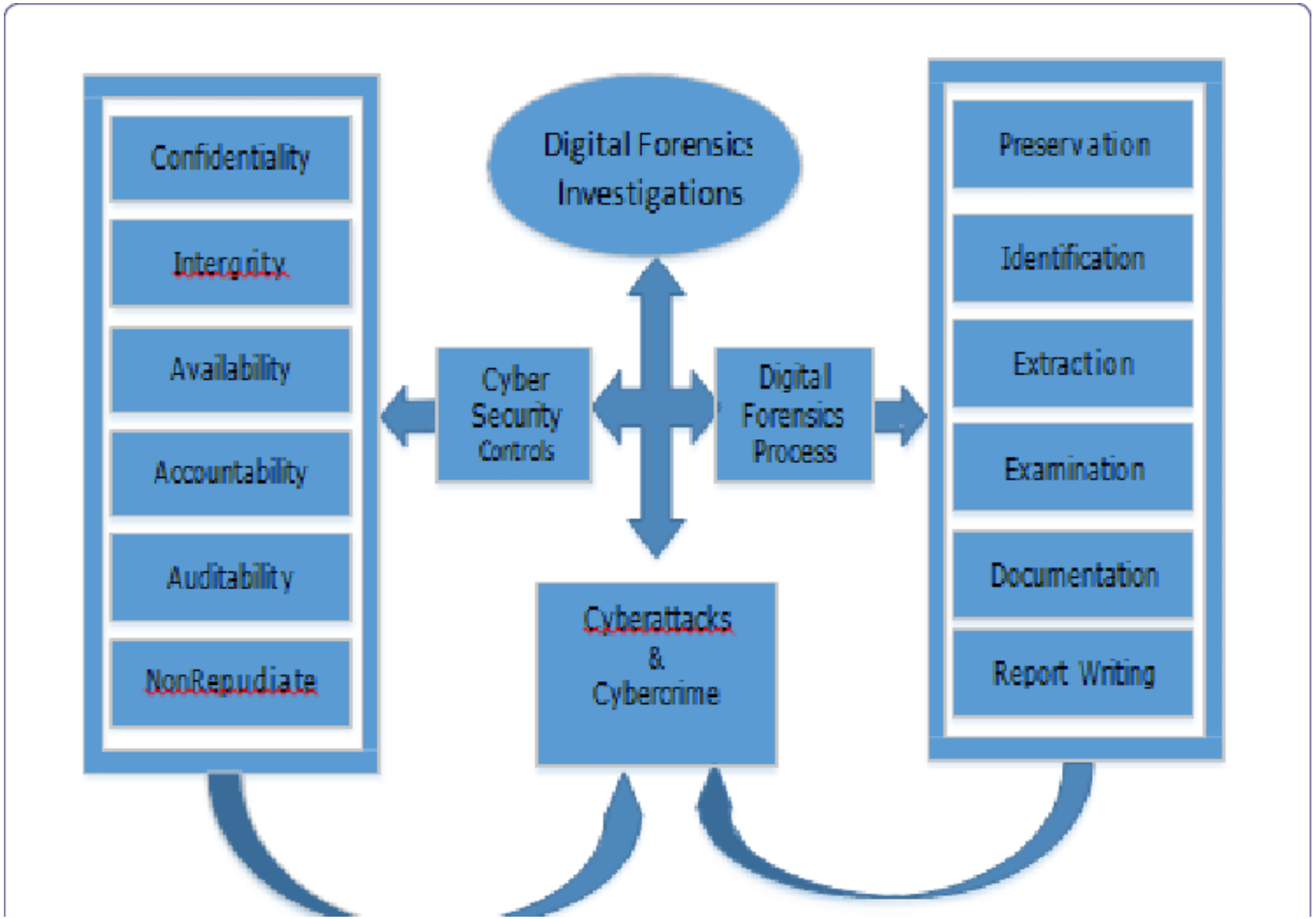
- These are tried-and-true procedures for documenting the analysis's conclusions, and they must allow other competent examiners to read through and duplicate the results.

Presentation:

- The collection of digital information, which may entail removing electronic devices from the crime/incident scene and copying or printing the device(s), is critical to the investigation.

Objectives of Digital Forensics

- It aids in **the recovery, analysis, and preservation of computers** and *related materials* for the investigating agency to present them as evidence in a court of law
- It aids in **determining the motive for the crime** and the identity of the primary perpetrator
- **Creating procedures at a suspected crime scene** to help ensure that the digital evidence obtained is not tainted
- **Data acquisition and duplication:** The process of recovering deleted files and partitions from digital media in order to extract and validate evidence
- Assists you in quickly **identifying evidence and estimating the potential impact** of malicious activity on the victim
- Creating a computer forensic report that provides comprehensive information on the investigation process
- Keeping the evidence safe by adhering to the chain of custody


Confidentiality
Intergrity
Availability
Accountability
Auditability
NonRepudiate
Digital Forensics Investigations
Cyber Security Controls
Digital Forensics Process
Cyberattacks & Cybercrime
Preservation
Identification
Extraction
Examination
Documentation
Report Writing

Types of Digital Forensics

Computer forensics

- It analyzes digital **evidence obtained from laptops, computers, and storage media** to support ongoing investigations and legal proceedings.

Mobile Device Forensics

- It entails obtaining **evidence from small electronic devices** such as personal digital assistants, mobile phones, tablets, sim cards, and gaming consoles.

Network Forensics

- Network or cyber forensics depends on the data **obtained from monitoring and analyzing cyber network activities** such as attacks, breaches, or system collapse caused by malicious software and abnormal network traffic.

Digital Image Forensics

- This sub-specialty focuses on the extraction and analysis of digital images to verify authenticity and metadata and determine the history and information surrounding them.

Digital Video/Audio Forensics

- This field examines audio-visual evidence to determine its authenticity or any additional information you can extract, such as location and time intervals.

Memory Forensics

- It refers to the recovery of information from a running computer's RAM and is also known as live acquisition.

Advantages of Digital Forensics

- Enables Digital Evidence Analysis
- Aids in the Identification of Criminals
- It Is Capable of Recovering Deleted Data
- Enlightens on How Crimes Are Committed
- It Has the Potential to Be Used to Prevent Future Crimes

Disadvantages of Digital Forensics

- Prolonged Procedure
- Requires Specialized Knowledge and Skills
- Can Be Costly
- Obtaining Evidence May Necessitate a Court Order

Any Query????

Thank you……