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 :19SB701 PATTERN RECOGNITION TECHNIQUES IN CYBER CRIME

IV YEAR / VII SEMESTER

Unit V- **CYBER CRIME**

Topic :The Computer Investigation Process

The Computer Investigation Process

The computer investigation process, also known as digital forensics, involves systematically examining digital devices and data to uncover evidence related to criminal activity, breaches, or other incidents.

This process is crucial for identifying the cause of an incident, understanding its impact, and collecting evidence that can be used in legal proceedings.

1. Preparation

Defining Objectives: Before beginning an investigation, it's essential to clearly define the objectives. This includes understanding the scope of the investigation, what information needs to be gathered, and any legal or regulatory requirements.

Assembling the Team: A skilled team of forensic experts, legal advisors, and IT professionals is gathered. The team should have the necessary tools, knowledge, and authority to conduct the investigation.

Identifying Resources: Ensuring that all necessary tools, software, and hardware for the investigation are available. This may include forensic software for data recovery, imaging tools, and secure storage for evidence.

2. Identification

•**Locating Potential Evidence:** This step involves identifying where the relevant data or evidence might reside. This can include computers, servers, mobile devices, cloud storage, external hard drives, and even network logs.

•**Determining the Type of Data:** Understanding the types of data involved, such as emails, documents, log files, images, or system files. This helps in focusing the investigation on relevant data sources.

3. Collection

Preserving Evidence: To maintain the integrity of the evidence, it's crucial to avoid altering the original data. This is done by creating a forensic image or copy of the data, which can be analyzed without risking contamination of the original evidence.

Data Acquisition: Collecting data from identified sources. This may involve capturing images of hard drives, extracting data from mobile devices, or retrieving data from cloud services. All actions taken during this stage should be carefully documented.

Chain of Custody: Keeping a detailed record of who has handled the evidence and when. This ensures that the evidence is admissible in court and that its integrity is maintained throughout the investigation.

4. Examination

Analyzing Data: Forensic analysts examine the collected data to identify relevant information. This may involve searching for specific keywords, recovering deleted files, or analyzing file metadata. Techniques such as keyword searching, timeline analysis, and file carving are commonly used.

Filtering and Organizing: Once the relevant data is identified, it's filtered and organized in a way that makes it easier to analyze. Irrelevant data is excluded to focus on the critical evidence.

Timeframe Analysis: Investigators often look at timestamps and logs to reconstruct a timeline of events, which can help in understanding the sequence of actions taken by an individual or a system.

5. Analysis

Interpreting Findings: The collected and examined data is analyzed to draw conclusions. This might include identifying the source of an attack, understanding how a breach occurred, or uncovering fraudulent activities.

Correlating Evidence: Investigators correlate the findings with other pieces of evidence to build a coherent narrative. This step may involve comparing data across multiple devices or sources.

Hypothesis Testing: Investigators may develop hypotheses about what happened and test these against the evidence to confirm or refute them.

6. Documentation

Report Preparation: All findings are documented in a detailed report. This report includes a summary of the investigation, the methodologies used, the evidence found, and the conclusions drawn. The report must be clear, concise, and understandable, especially for non-technical audiences, such as legal teams or court officials.

Evidence Logs: Detailed logs of all actions taken during the investigation, including who accessed the data, when, and what was done, are maintained. This ensures transparency and helps defend the investigation's validity if challenged.

7. Presentation

Presenting Findings: If the investigation leads to legal proceedings, forensic experts may be required to present their findings in court. They must be able to explain their methods and conclusions clearly and defend the integrity of their investigation.

Expert Testimony: In some cases, investigators may serve as expert witnesses, providing testimony based on their analysis. This requires a deep understanding of the technical details and the ability to communicate them effectively to judges, juries, or other legal professionals.

8. Review and Feedback

Post-Investigation Review: After the investigation, the team reviews the process to identify any lessons learned. This helps improve future investigations and can lead to updates in procedures or tools.

Updating Policies: Based on the findings, organizations may update their security policies or incident response plans to prevent similar incidents in the future.

Any Query????

Thank you……