UNIT 1

Understanding Computer Forensics

1. **Computer Forensics Basics**:
    - A branch of digital forensics focused on recovering, analyzing, and preserving digital evidence for legal or organizational investigations.
    - Tools like **EnCase**, **FTK**, and **Autopsy** help extract evidence without altering it.
2. **Cybercrimes and Investigation**:
    - Cybercrimes include hacking, phishing, identity theft, and fraud.
    - Investigation steps:
        - Identify the crime and its scope.
        - Preserve evidence using tools like write blockers.
        - Analyze data for clues about the attacker or methods used.
        - Document findings for court or organizational reports.
3. **Digital Evidence**:
    - Can include files, emails, chat logs, and metadata (timestamps, geolocation).
    - Characteristics:
        - Must remain unaltered.
        - Can be volatile (e.g., RAM data) and requires immediate preservation.
    - Bitstream imaging ensures a complete copy of the original data.
4. **Forensic Readiness**:
    - Preparing to handle incidents by:
        - Setting up logging systems.
        - Training staff on evidence collection.
        - Establishing legal-compliant procedures.
5. **Incident Response**:
    - Steps include preparation, detection, containment, eradication, recovery, and post-incident review.
    - Example: Isolating a compromised system to prevent further damage.
6. **Role of SOC**:
    - The **Security Operations Center** (SOC) monitors systems, detects threats, and supports forensic investigations.

7. **Forensic Investigator's Role**:
    - Responsible for collecting, analyzing, and presenting evidence while maintaining a proper chain of custody to ensure its validity.

Computer Forensics Investigation Process

1. **Importance of the Process**:
    - Ensures evidence is admissible in court.
    - Identifies vulnerabilities to improve security.
2. **Pre-Investigation Phase**:
    - Define forensic policies, prepare tools, and train teams.
    - Establish protocols for evidence storage and handling.
3. **First Response**:
    - Secure the scene (physical or digital).
    - Document system states and collect volatile data immediately (e.g., RAM, running processes).
4. **Investigation Phase**:
    - **Collection**: Gather evidence like logs, hard drives, and network traffic.
    - **Analysis**: Use tools to uncover activity timelines, deleted files, and attacker methods.
    - **Documentation**: Maintain detailed records of every action taken during the process.
    - **Reporting**: Summarize findings for stakeholders or legal authorities.

Important MCQ

1. **What is the primary goal of computer forensics?**
   a) Create new software
   b) Protect personal data
   c) Recover and analyze digital evidence
   d) Design computer systems
   Answer: c

2. **Which tool is commonly used for digital forensics?**
   a) Wireshark
   b) EnCase
   c) Metasploit
   d) Nessus
   Answer: b

3. **What is the first step in a forensic investigation?**
   a) Analysis
   b) Documentation
   c) Evidence collection
   d) Incident identification
   Answer: d

4. **What does the chain of custody refer to?**
   a) Securing a crime scene
   b) Handling evidence to maintain its integrity
   c) Documenting legal procedures
   d) Storing data backups
   Answer: b

5. **Which of the following is a volatile source of digital evidence?**
   a) RAM
   b) Hard drives
   c) USB drives
   d) Cloud storage
   Answer: a

6. **What is forensic readiness?**
   a) Preparing evidence for court
   b) Training personnel to handle incidents
   c) Preparing an organization to collect and handle evidence efficiently
   d) Conducting mock cyberattacks
   Answer: c

7. **Which phase involves isolating a compromised system during an incident?**
   a) Recovery
   b) Containment
   c) Eradication
   d) Preparation
   Answer: b

8. **What type of evidence includes emails, logs, and chat messages?**
   a) Metadata
   b) Volatile evidence
   c) Digital evidence
   d) Physical evidence
   Answer: c

9. **What is a bitstream copy?**
   a) A selective copy of files
   b) An exact duplicate of all data on a drive
   c) A network traffic log
   d) A backup of volatile data
   Answer: b

10. **Which of the following is NOT a step in incident response?**
    a) Preparation
    b) Containment
    c) Eradication
    d) Encryption
    Answer: d

11. **What is the role of the SOC in computer forensics?**
    a) Develop malware analysis tools
    b) Monitor and analyze security events
    c) Create encryption protocols
    d) Design operating systems
    Answer: b

12. **Which of the following is NOT a cybercrime?**
    a) Hacking
    b) Phishing
    c) Identity theft
    d) Software development
    Answer: d

13. **Which phase focuses on preventing future incidents after a breach?**
    a) Eradication
    b) Recovery
    c) Post-incident review
    d) Containment
    Answer: c

14. **What is the primary characteristic of digital evidence?**
    a) Easily manipulated
    b) Non-volatile
    c) Can be altered without detection
    d) Must remain unchanged for admissibility
    Answer: d

15. **What is the purpose of write blockers in forensics?**
    a) To create backups
    b) To prevent data on the evidence drive from being modified
    c) To analyze network traffic
    d) To encrypt collected evidence
    Answer: b

16. **Which forensic tool is open-source?**
    a) EnCase
    b) FTK
    c) Autopsy
    d) Nessus
    Answer: c

17. **Which of the following is an example of metadata?**
    a) File size
    b) Email content
    c) System logs
    d) Timestamps
    Answer: d

18. **What is the purpose of the investigation phase in forensics?**
    a) Train investigators
    b) Document legal processes
    c) Collect, analyze, and report evidence
    d) Recover lost data
    Answer: c

19. **What is the first priority during first response in computer forensics?**
    a) Collect evidence
    b) Power down the system
    c) Secure the scene and preserve evidence
    d) Analyze network logs
    Answer: c

20. **What is the main goal of containment in incident response?**
    a) Remove malware
    b) Prevent further damage
    c) Document the incident
    d) Recover lost files
    Answer: b

21. **What does a forensic investigator do during the recovery phase?**
    a) Secure evidence
    b) Restore systems to normal operation
    c) Collect volatile data
    d) Encrypt recovered files
    Answer: b

22. **Which type of evidence disappears when a system is powered off?**
    a) Hard disk data
    b) RAM data
    c) USB drive data
    d) Browser cookies
    Answer: b

23. **What is the key legal requirement for digital evidence?**
    a) It must be encrypted.
    b) It must be verifiable and unaltered.
    c) It must be backed up.
    d) It must be stored on a hard drive.
    Answer: b

24. **What is the primary use of forensic reports?**
    a) Guide network administrators
    b) Provide legal evidence and findings
    c) Train employees
    d) Develop incident response plans
    Answer: b

25. **Which phase involves removing malware from infected systems?**
    a) Containment
    b) Eradication
    c) Recovery
    d) Detection
    Answer: b

26. **What is the role of the pre-investigation phase?**
    a) Collect digital evidence
    b) Train employees and define procedures
    c) Analyze data logs
    d) Restore affected systems
    Answer: b

27. **What is forensic readiness designed to improve?**
    a) System recovery speed
    b) Evidence collection and handling efficiency
    c) Network traffic analysis
    d) Data encryption standards
    Answer: b

28. **What is the purpose of post-incident reviews?**
    a) Identify mistakes and improve future responses
    b) Encrypt evidence
    c) Recover deleted files
    d) Train new employees
    Answer: a

29. **Which of the following is NOT part of the forensic investigation process?**
    a) Evidence collection
    b) Analysis
    c) Reporting
    d) System updates
    Answer: d

30. **What is the significance of timestamps in forensics?**
    a) They encrypt files.
    b) They verify the origin of evidence.
    c) They provide a timeline of activities.
    d) They store user credentials.
    Answer: c