UNIT 3

Data Acquisition and Duplication

1. **Data Acquisition Fundamentals**:
   - Involves collecting digital evidence in a manner that preserves its integrity.
   - Key practices include ensuring a proper chain of custody and using write blockers to prevent data modification.
2. **Data Acquisition Methodology**:
   - Identification: Determine what data needs to be collected.
   - Acquisition: Use forensic tools (e.g., FTK Imager, EnCase) to create exact copies or disk images.
   - Documentation: Record details of the acquisition process for legal purposes.
3. **Prepare an Image for Examination**:
   - Use hashing algorithms like MD5 or SHA-256 to verify that the forensic image is identical to the original source.
   - Tools like Autopsy or ProDiscover analyze the image while maintaining data authenticity.

Windows Forensics

1. **Collect Volatile and Non-Volatile Information**:
   - **Volatile Information**: Temporary data like active processes, network connections, and RAM contents. Tools like Volatility or DumpIt capture these details.
   - **Non-Volatile Information**: Data stored on disk, including files, registry entries, and logs.
2. **Perform Windows Memory and Registry Analysis**:
   - **Memory Analysis**: Extract data from memory dumps, such as malware traces, encryption keys, and passwords.
   - **Registry Analysis**: Investigate registry entries to uncover user activities, installed software, and connected USB devices.

3. **Examine the Cache, Cookie, and History Recorded in Web Browsers**:
    - Browsers save cache (temporary files), cookies (session data), and history (visited URLs).
    - Forensic analysis can reveal visited websites, login details, and timestamps.
4. **Examine Windows Files and Metadata**:
    - Analyze system files (e.g., SAM, SYSTEM, NTUSER.DAT) to retrieve user accounts, device configurations, and activity logs.
    - Metadata provides information like file creation and modification dates, revealing patterns of use.
5. **Understand Text-Based Logs and Windows Event Logs**:
    - **Text-Based Logs**: Contain plain text records of application or system activity.
    - **Windows Event Logs**: Structured logs categorized into Application, Security, and System events, aiding in tracking unauthorized access or system errors.

Important MCQ

1. What is the primary goal of data acquisition in computer forensics?
   a) Modifying evidence
   b) Preserving evidence integrity
   c) Deleting unnecessary files
   d) Compressing large files
   Answer: b) Preserving evidence integrity

2. Which of the following tools is commonly used for creating forensic images?
   a) Volatility
   b) FTK Imager
   c) Metasploit
   d) Wireshark
   Answer: b) FTK Imager

3. What is the role of a write blocker during data acquisition?
   a) It blocks unauthorized access to logs.
   b) It prevents modification of source data.
   c) It compresses files for faster processing.
   d) It decrypts encrypted files.
   Answer: b) It prevents modification of source data.

4. What does a hash function like MD5 or SHA-256 ensure during data acquisition?
   a) Data compression
   b) Evidence authenticity
   c) File encryption
   d) File accessibility
   Answer: b) Evidence authenticity

5. Which of the following is considered volatile information?
   a) RAM contents
   b) System logs
   c) Hard drive data
   d) Registry entries
   Answer: a) RAM contents

6. What tool can be used to analyze memory dumps in Windows forensics?
   a) EnCase
   b) Volatility
   c) Autopsy
   d) Metasploit
   Answer: b) Volatility

7. Which file stores user account information on a Windows system?
   a) SYSTEM
   b) NTUSER.DAT
   c) SAM
   d) CONFIG
   Answer: c) SAM

8. What does the Windows registry primarily store?
   a) System logs
   b) User preferences and system settings
   c) Temporary files
   d) Internet history
   Answer: b) User preferences and system settings

9. What is the main purpose of a forensic disk image?
   a) To improve system performance
   b) To create a backup of files
   c) To replicate data for investigation
   d) To hide sensitive files
   Answer: c) To replicate data for investigation

10. What is the term for temporary files stored by web browsers?
    a) Cookies
    b) Cache
    c) Logs
    d) Metadata
    Answer: b) Cache

11. Which log type in Windows records unauthorized access attempts?
    a) Application log
    b) Security log
    c) System log
    d) Text-based log
    Answer: b) Security log

12. What type of data does non-volatile storage typically contain?
    a) Temporary processes
    b) File system data
    c) Open network connections
    d) Memory snapshots
    Answer: b) File system data

13. Which forensic tool is used to analyze browser artifacts like cookies and history?
    a) Wireshark
    b) FTK Imager
    c) Browser History Examiner
    d) Volatility
    Answer: c) Browser History Examiner

14. What is metadata in file forensics?
    a) Hidden content in files
    b) File properties such as creation and modification dates
    c) Network configurations
    d) User account information
    Answer: b) File properties such as creation and modification dates

15. What type of log contains information about application errors?
    a) Security log
    b) Application log
    c) System log
    d) Volatile log
    Answer: b) Application log

16. Which command is used to create a disk image in Linux?
    a) dd
    b) cat
    c) ls
    d) mkdir
    Answer: a) dd

17. What is the purpose of volatile data collection in forensics?
    a) To retrieve long-term stored data
    b) To capture data lost after power shutdown
    c) To extract web browsing history
    d) To identify metadata of files
    Answer: b) To capture data lost after power shutdown

18. What Windows artifact stores user login details and preferences?
    a) SAM file
    b) NTUSER.DAT
    c) SYSTEM registry hive
    d) Application logs
    Answer: b) NTUSER.DAT

19. What is a common method to verify the integrity of a forensic image?
    a) File comparison
    b) Hash comparison
    c) Memory analysis
    d) Registry editing
    Answer: b) Hash comparison

20. What does a cookie primarily store in web browsers?
    a) Visited URLs
    b) User session data
    c) Downloaded files
    d) Temporary scripts
    Answer: b) User session data

21. What is the main function of Windows Event Viewer?
    a) To edit registry entries
    b) To analyze system performance
    c) To review system and application logs
    d) To manage user accounts
    Answer: c) To review system and application logs

22. Which file type is used for booting Windows?
    a) Boot.ini
    b) SAM
    c) NTUSER.DAT
    d) Event Logs
    Answer: a) Boot.ini

23. What command displays active network connections in Windows?
    a) ipconfig
    b) netstat
    c) ping
    d) tracert
    Answer: b) netstat

24. What registry hive stores information about hardware configurations?
    a) HKEY_LOCAL_MACHINE
    b) HKEY_CURRENT_USER
    c) HKEY_USERS
    d) HKEY_CLASSES_ROOT
    Answer: a) HKEY_LOCAL_MACHINE

25. What is the forensic importance of browser cache?
    a) It stores system logs.
    b) It records browsing activity and downloaded content.
    c) It encrypts user data.
    d) It retrieves deleted files.
    Answer: b) It records browsing activity and downloaded content.

26. What type of storage is affected by a system shutdown?
    a) Non-volatile storage
    b) Volatile storage
    c) File systems
    d) Hard disks
    Answer: b) Volatile storage

27. What log is analyzed to detect user logins and logouts?
    a) Application log
    b) Security log
    c) System log
    d) Network log
    Answer: b) Security log

28. What is the function of the SYSTEM registry file?
    a) Stores user account information
    b) Tracks system configuration details
    c) Logs browser history
    d) Stores metadata of files
    Answer: b) Tracks system configuration details

29. What forensic tool allows deep analysis of Windows registry?
    a) Autopsy
    b) Registry Explorer
    c) FTK Imager
    d) Metasploit
    Answer: b) Registry Explorer

30. Why is an image created for forensic examination?
    a) To improve system speed
    b) To analyze data without altering the original evidence
    c) To delete irrelevant data
    d) To compress files for storage
    Answer: b) To analyze data without altering the original evidence