Postgraduate Certificate in Network Security

Digital Forensics

Digital Forensics is a branch of forensic science focused on the recovery and investigation of material found in digital devices. It involves the identification, preservation, examination, analysis, and presentation of digital evidence from computers, networks, and electronic storage devices. The main goal of digital forensics is to uncover and document evidence that can be used in legal proceedings.

Digital forensics plays a crucial role in Network Security by helping organizations investigate and respond to cyber incidents, such as data breaches, malware infections, and unauthorized access. It provides valuable insights into the extent of an attack, the methods used by the attacker, and the impact on the organization's systems and data.

Key Terms and Vocabulary:

1. Forensic Investigation: The process of collecting, preserving, analyzing, and presenting digital evidence in a way that maintains its integrity and admissibility in court.

2. Chain of Custody: The documented record of individuals who have had custody of a piece of evidence. It ensures that the evidence has not been tampered with or altered.

3. Volatility: The tendency of digital evidence to change or be lost over time, especially in volatile memory (RAM). Volatile data must be captured and preserved quickly to prevent loss.

4. File System: The structure used by operating systems to store, organize, and retrieve files on a storage device. Common file systems include NTFS, FAT, exFAT, and HFS+.

5. Metadata: Data that provides information about other data. It includes file creation dates, modification dates, file size, and user access logs.

6. Hash Value: A unique alphanumeric string generated by applying a hash function to a set of data. It is used to verify the integrity of files and ensure they have not been altered.

7. Incident Response: The process of responding to and managing a security incident. It involves identifying the incident, containing the damage, eradicating the threat, and recovering from the attack.

8. Live Forensics: The process of collecting and analyzing digital evidence from a running system without shutting it down. It allows investigators to capture volatile data and conduct real-time analysis.

9. Steganography: The practice of concealing messages or files within other files to avoid detection. Digital forensics tools are used to detect and extract hidden data.

10. Malware Analysis: The process of analyzing malware samples to understand their behavior, functionality, and impact. It helps in developing countermeasures and preventing future infections.

11. Rootkit: A type of malicious software that gives attackers privileged access to a computer or network. Rootkits are difficult to detect and remove using traditional antivirus tools.

12. Chain of Custody: The process of documenting the handling of evidence from the time it is collected until it is presented in court. It ensures the integrity and admissibility of the evidence.

13. Computer Forensics: The application of forensic techniques to investigate digital devices and recover digital evidence. It involves the analysis of hard drives, memory cards, and other storage media.

14. Network Forensics: The process of monitoring and analyzing network traffic to identify security incidents, investigate attacks, and gather evidence. It helps in understanding how an attacker breached a network and what data was compromised.

15. Mobile Device Forensics: The investigation of smartphones, tablets, and other mobile devices to recover data, messages, call logs, and other digital evidence. It is essential for solving crimes and corporate investigations.

16. Forensic Toolkit (FTK): A popular digital forensics tool used to collect, analyze, and preserve digital evidence. It allows investigators to search for keywords, recover deleted files, and create forensic reports.

17. EnCase: Another widely used digital forensics tool that provides investigators with the ability to acquire, analyze, and report on digital evidence. It supports a wide range of file systems and devices.

18. File Carving: The process of extracting files from a storage device without relying on the file system. It is used to recover deleted or damaged files that cannot be accessed through traditional means.

19. Memory Forensics: The analysis of volatile memory (RAM) to extract information about running processes, network connections, and other activities. It helps in identifying malware and understanding system behavior.

20. Network Packet Analysis: The examination of network packets to identify patterns, anomalies, and security incidents. It enables investigators to reconstruct network activities and determine the source and impact of an attack.

21. Encryption: The process of converting data into a secure format to prevent unauthorized access. Encryption is used to protect sensitive information during transmission and storage.

22. Decryption: The process of converting encrypted data back into its original, readable format. Decryption keys are required to unlock encrypted files and messages.

23. Forensic Imaging: The process of creating a bit-by-bit copy of a storage device for forensic analysis. It ensures that the original evidence remains intact while investigators work with the copy.

24. Write Blocker: A hardware device or software tool used to prevent data from being written to a storage device during the forensic imaging process. It ensures the integrity of the evidence.

25. Time Stamping: The process of recording the date and time when a piece of evidence was collected or

an event occurred. Time stamps are used to establish the timeline of an investigation.

26. Virtual Machine Forensics: The analysis of virtual machines to recover digital evidence and investigate security incidents. It involves examining virtual disks, snapshots, and configurations.

27. Cloud Forensics: The investigation of data stored in cloud services to uncover evidence of cybercrime or unauthorized access. It involves retrieving logs, metadata, and user activity.

28. Mobile Application Forensics: The examination of mobile applications to identify security vulnerabilities, data leakage, and privacy issues. It helps in understanding how apps handle user data.

29. Forensic Report: A detailed document that summarizes the findings of a digital forensic investigation. It includes information about the evidence collected, analysis performed, and conclusions drawn.

30. Expert Witness: A qualified professional who testifies in court about digital forensics findings. Expert witnesses provide testimony based on their knowledge, experience, and analysis of the evidence.

By mastering the key terms and vocabulary of digital forensics in the context of network security, students in the Postgraduate Certificate in Network Security program will be equipped to effectively investigate cyber incidents, analyze digital evidence, and strengthen the security posture of organizations.