Graduate Certificate in Forensic and National Security Studies

Digital Forensics and Computer Crime

Digital Forensics and Computer Crime Terminology

Digital forensics is a branch of forensic science focusing on the recovery and investigation of material found in digital devices, often in relation to computer crimes. Understanding the key terms and vocabulary in digital forensics is essential for professionals in the field. Below are some of the most important terms in digital forensics and computer crime investigations.

1. Forensic Investigation

Forensic investigation is the process of collecting, analyzing, and interpreting digital evidence in a manner that preserves its integrity and is admissible in a court of law. It involves following a strict methodology to ensure that the evidence is not contaminated or altered in any way.

2. Chain of Custody

Chain of custody refers to the documentation of the chronological history of the physical or digital evidence, including who collected it, when it was collected, who had custody of it, and where it was stored. Maintaining an unbroken chain of custody is crucial to the admissibility of evidence in court.

3. Digital Evidence

Digital evidence is any information stored or transmitted in digital form that can be used in a legal investigation. This includes data from computers, mobile devices, servers, and other electronic storage media. Examples of digital evidence include emails, text messages, images, and documents.

4. Volatile Data

Volatile data refers to information stored in the computer's memory (RAM) that is lost when the system is powered off. This type of data is crucial in digital forensics investigations as it can provide real-time information about the activities that were taking place on the computer.

5. Non-volatile Data

Non-volatile data is information that is stored on persistent storage devices such as hard drives, solid-state drives, and USB drives. This type of data is retained even when the system is powered off and is the primary focus of digital forensics investigations.

6. Metadata

Metadata is data that describes other data. In digital forensics, metadata provides information about the origin, creation date, author, and other attributes of a file. Analyzing metadata can help investigators

reconstruct the timeline of events and establish the authenticity of digital evidence.

7. File Carving

File carving is a technique used in digital forensics to extract files and data from storage media without relying on the file system. This method is particularly useful when the file system is damaged or corrupted, allowing investigators to recover deleted or hidden files.

8. Steganography

Steganography is the practice of concealing messages or data within other non-secret data. In digital forensics, steganography can be used to hide incriminating information within images, audio files, or other seemingly innocuous files. Detecting steganography requires specialized tools and techniques.

9. Encryption

Encryption is the process of converting data into a code to prevent unauthorized access. In digital forensics investigations, encrypted data can pose a significant challenge as it may be impossible to access without the correct decryption key. Breaking encryption requires advanced technical skills and specialized tools.

10. Malware

Malware, short for malicious software, is any software designed to disrupt, damage, or gain unauthorized access to a computer system. Common types of malware include viruses, worms, trojans, and ransomware. Detecting and analyzing malware is a critical aspect of digital forensics investigations.

11. Rootkit

A rootkit is a type of malware that is designed to hide its presence on a system and provide unauthorized access to the attacker. Rootkits often modify the operating system to evade detection by traditional security tools, making them difficult to detect and remove.

12. Network Forensics

Network forensics is the process of monitoring and analyzing network traffic for the purpose of investigating security incidents and identifying potential threats. This involves capturing and analyzing data packets to reconstruct the sequence of events and identify the source of an attack.

13. Incident Response

Incident response is the coordinated effort to respond to and manage a security incident, such as a data breach or cyber-attack. Digital forensics professionals play a key role in incident response by conducting forensic investigations to identify the cause of the incident and mitigate future risks.

14. Cybercrime

Cybercrime refers to criminal activities carried out using computers or the internet. Common types of

cybercrime include hacking, phishing, identity theft, and online fraud. Digital forensics is essential in investigating and prosecuting cybercrimes to gather evidence and identify perpetrators.

15. Data Breach

A data breach is a security incident in which sensitive or confidential information is accessed or disclosed without authorization. Digital forensics is instrumental in investigating data breaches to determine the extent of the breach, identify the cause, and prevent future occurrences.

16. Expert Witness

An expert witness is a professional with specialized knowledge and experience in a particular field who is called to testify in court as an expert. In digital forensics cases, expert witnesses may provide testimony on the methods used to collect and analyze digital evidence, as well as the findings of their investigations.

17. Forensic Toolkit

A forensic toolkit is a collection of software tools and utilities used by digital forensics professionals to acquire, analyze, and report on digital evidence. These tools may include disk imaging software, data recovery tools, forensic analysis software, and steganography detection tools.

18. Data Preservation

Data preservation is the process of securely storing and protecting digital evidence to prevent tampering, loss, or corruption. This involves creating forensic copies of storage media, documenting the chain of custody, and implementing strict access controls to ensure the integrity of the evidence.

19. Anti-Forensics

Anti-forensics refers to techniques used to thwart or manipulate digital forensic investigations. This may include deleting incriminating data, modifying timestamps, encrypting files, or using steganography to hide information. Digital forensics professionals must be aware of anti-forensic techniques and take steps to counteract them.

20. Data Recovery

Data recovery is the process of retrieving lost, damaged, or deleted data from storage media. In digital forensics, data recovery techniques are used to recover evidence that has been intentionally or unintentionally deleted or altered. This process requires specialized tools and expertise to ensure the integrity of the recovered data.

21. Expert Analysis

Expert analysis in digital forensics involves the interpretation of digital evidence to reconstruct events, identify patterns, and draw conclusions. Digital forensics professionals use their expertise to analyze data from multiple sources and present their findings in a clear and concise manner that is admissible in court.

22. Forensic Report

A forensic report is a detailed document that summarizes the findings of a digital forensics investigation. The report includes information about the evidence collected, the analysis methods used, the conclusions reached, and any recommendations for further action. A well-written forensic report is crucial for presenting evidence in court.

23. Legal Compliance

Legal compliance in digital forensics refers to following established laws, regulations, and guidelines when conducting investigations and handling evidence. Digital forensics professionals must adhere to legal standards to ensure that their findings are admissible in court and that their actions do not violate the rights of individuals.

24. Digital Footprint

A digital footprint is the trail of data left behind by a person's online activities. This includes information such as browsing history, social media posts, emails, and online transactions. Analyzing a digital footprint can provide valuable insights into a person's behavior and activities.

25. Mobile Forensics

Mobile forensics is the branch of digital forensics that focuses on the recovery and analysis of data from mobile devices such as smartphones and tablets. Mobile forensics presents unique challenges due to the variety of devices, operating systems, and applications involved, requiring specialized tools and techniques.

26. Cloud Forensics

Cloud forensics is the process of investigating digital evidence stored in cloud computing environments. This includes data stored in cloud services such as Google Drive, Dropbox, and Microsoft OneDrive. Cloud forensics requires a thorough understanding of cloud technologies and data privacy issues.

27. Digital Signature

A digital signature is a cryptographic technique used to verify the authenticity and integrity of digital documents or messages. Digital signatures provide a way to ensure that a document has not been altered and that it was created by a specific person or entity. Verifying digital signatures is an important aspect of digital forensics.

28. Data Wiping

Data wiping, also known as data erasure, is the process of securely deleting data from storage media to prevent its recovery. Digital forensics professionals may encounter data wiping techniques used by individuals or organizations to conceal evidence of illegal activities. Recovering data from wiped storage media requires specialized tools and expertise.

29. Incident Handling

Incident handling is the process of responding to and managing security incidents in a systematic and coordinated manner. Digital forensics professionals play a key role in incident handling by conducting forensic investigations to identify the cause of the incident, contain the damage, and prevent future incidents.

30. Cybersecurity

Cybersecurity refers to the practice of protecting computer systems, networks, and data from cyber threats. Digital forensics is closely related to cybersecurity, as forensic investigations are often conducted in response to security incidents such as data breaches, malware infections, and unauthorized access attempts.

Conclusion

Understanding the key terms and vocabulary in digital forensics and computer crime investigations is essential for professionals working in this field. From forensic investigation and chain of custody to data recovery and incident handling, digital forensics encompasses a wide range of techniques and methodologies. By mastering these terms and concepts, digital forensics professionals can effectively collect, analyze, and present digital evidence in legal proceedings and contribute to the fight against cybercrime.