Professional Certificate in Digital Forensics Fundamentals

Legal and Ethical Issues

Adware: Software that displays advertisements on a user's device, often as part of a free or low-cost application. Adware can be legitimate, but it can also be malicious, displaying unwanted ads or tracking user activity without consent.

Anti-forensics: Techniques used to evade or impede digital forensics investigations, such as data hiding, data destruction, or tampering with forensic tools.

Autopsy: A digital forensics tool used for data acquisition, analysis, and reporting. Autopsy can be used to investigate various types of digital devices, including computers, mobile devices, and external storage media.

BitLocker: A full disk encryption feature included in Microsoft Windows operating systems. BitLocker can help protect data at rest by encrypting the entire hard drive, making it more difficult for unauthorized users to access sensitive information.

Chain of custody: The documentation and tracking of evidence from the time it is collected to the time it is presented in court. Maintaining a proper chain of custody is essential for ensuring the integrity and admissibility of evidence in legal proceedings.

Computer Fraud and Abuse Act (CFAA): A United States federal law that criminalizes unauthorized access to computers and networks, as well as the transmission of malicious code or the intentional damage of data.

Data carving: A digital forensics technique used to recover deleted or damaged files by analyzing the raw data on a storage device. Data carving can be used to recover files that have been intentionally deleted or have become corrupted due to hardware or software failures.

Digital evidence: Any data or information that is stored or transmitted in digital form and can be used as evidence in a legal proceeding. Digital evidence can include emails, text messages, social media posts, files, and other types of data.

Electronic Discovery (eDiscovery): The process of identifying, preserving, collecting, and producing electronically stored information (ESI) in response to a legal request or lawsuit. eDiscovery can involve a wide range of digital devices and data types, including email, social media, cloud storage, and mobile devices.

Encryption: The process of converting plaintext (unencrypted) data into ciphertext (encrypted) data using an encryption algorithm and a secret key. Encryption can help protect sensitive data from unauthorized access, interception, or theft.

Evidence tampering: The act of altering, modifying, or destroying evidence in order to obstruct justice or

manipulate the outcome of a legal proceeding. Evidence tampering is a serious criminal offense and can result in severe penalties, including fines and imprisonment.

Forensic image: A bit-for-bit copy of a digital device's storage media, including all data and metadata, that is used for digital forensics investigations. Forensic images are created using specialized tools and software and are admissible as evidence in legal proceedings.

GDPR: The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

Hashing: A one-way mathematical function that maps data of arbitrary size to a fixed-size hash value. Hashing is used in digital forensics to verify the integrity of data and to create unique identifiers for digital evidence.

Incident response: The process of identifying, investigating, containing, and mitigating security incidents, such as data breaches, cyber attacks, or unauthorized access. Incident response plans should be developed and tested in advance to ensure a swift and effective response to security incidents.

IP address: A unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. IP addresses can be used to identify the location and owner of a device and are often used as evidence in digital forensics investigations.

JavaScript: A popular programming language used for creating interactive web pages and applications. JavaScript can be used for legitimate purposes, but it can also be abused for malicious purposes, such as injecting malware or conducting phishing attacks.

Keylogger: A type of malware that records keystrokes on a user's device, often with the intent of stealing passwords or other sensitive information. Keyloggers can be installed manually or remotely and can be difficult to detect and remove.

Live analysis: The process of analyzing a digital device while it is still running and in use, as opposed to creating a forensic image and analyzing it offline. Live analysis can be useful for identifying and mitigating active threats, but it can also pose risks to the integrity of evidence.

Malware: Short for "malicious software," malware is any type of software that is designed to harm or exploit a user's device or network, such as viruses, worms, Trojans, ransomware, or spyware.

Mobile device forensics: The process of collecting, analyzing, and preserving data from mobile devices, such as smartphones, tablets, and GPS devices, for use in digital forensics investigations.

Network forensics: The process of analyzing network traffic and data to identify security threats, anomalies, or policy violations. Network forensics can involve monitoring live network traffic or analyzing captured network packets.

Password cracking: The process of attempting to guess or recover a user's password, often using specialized

software or hardware. Password cracking can be used for legitimate purposes, such as recovering lost or forgotten passwords, but it can also be used for malicious purposes, such as gaining unauthorized access to a system or network.

Penetration testing: The process of testing a system or network for vulnerabilities and weaknesses by simulating real-world attacks. Penetration testing can help identify potential security risks and provide recommendations for mitigation.

Registry analysis: The process of analyzing the Windows Registry, a hierarchical database that stores configuration settings and other information for the Windows operating system and installed applications. Registry analysis can be used to identify system changes, software installations, user activity, and other relevant information.

Reverse engineering: The process of analyzing a software program, hardware device, or other technology in order to understand its design, functionality, or vulnerabilities. Reverse engineering can be used for legitimate purposes, such as software debugging or security research, but it can also be used for malicious purposes, such as creating malware or circumventing copy protection.

SQL injection: A type of cyber attack that exploits vulnerabilities in web applications that use SQL databases. SQL injection attacks can allow attackers to inject malicious SQL code into a database, allowing them to extract, modify, or delete sensitive data.

Steganography: The practice of hiding secret data or messages within seemingly innocuous files or media, such as images, audio, or video. Steganography can be used for legitimate purposes, such as watermarking or copyright protection, but it can also be used for malicious purposes, such as hiding malware or transmitting sensitive information.

Triage: The process of quickly assessing and prioritizing digital evidence based on its relevance and importance to an investigation. Triage can help investigators focus their efforts on the most promising leads and avoid wasting time on irrelevant or redundant data.

Volatility: The property of digital evidence that refers to its tendency to change or disappear over time. Volatile data, such as network connections, running processes, or memory contents, can be lost or altered if not collected and analyzed quickly and accurately.

Whitelisting: The practice of allowing only explicitly approved software or applications to run on a device or network. Whitelisting can help prevent the execution of malware or other unauthorized software, but it can also be time-consuming and require careful maintenance.