Professional Certificate in Digital Forensics Fundamentals

Digital Forensics Tools

Acquisition: The process of creating a forensic image or copy of digital media, such as a hard drive or USB flash drive. The goal of acquisition is to create a bit-for-bit copy of the media, including all data and metadata, in a way that preserves the integrity and authenticity of the original evidence. Related terms: forensic image, bit-for-bit copy, hash value.

AD Forensics: The use of digital forensics techniques to investigate attacks on Active Directory (AD), a directory service used by Microsoft Windows domains for centralized management of network resources. AD forensics can help identify the cause of an attack, determine the extent of the damage, and provide evidence for prosecution. Related terms: Active Directory, directory service, Windows domains.

Anti-forensics: Techniques used to hide, delete, or alter digital evidence in order to avoid detection or incrimination. Anti-forensics can include methods such as data hiding, encryption, and file wiping. Related terms: data hiding, encryption, file wiping.

Bit-for-bit copy: An exact replica of digital media, including all data and metadata, created using a forensic imaging tool. A bit-for-bit copy is also known as a forensic image. Related terms: forensic image, acquisition, hash value.

Data carving: The process of extracting files or data from digital media by analyzing the raw data on the device, rather than relying on file system metadata. Data carving can be used to recover deleted or damaged files, or to analyze unallocated space on a device. Related terms: unallocated space, file system metadata.

Data hiding: The practice of concealing data within other data or structures, such as steganography or slack space. Data hiding can be used for legitimate purposes, such as digital watermarking, or for malicious purposes, such as hiding malware or illegal content. Related terms: steganography, slack space, digital watermarking.

Digital evidence: Any data or information that is stored or transmitted in digital form and can be used as evidence in a legal case. Digital evidence can include emails, text messages, social media posts, files, and other data. Related terms: metadata, hash value, acquisition.

Directory service: A service that provides centralized management of network resources, such as users, groups, and devices. Active Directory is an example of a directory service used by Microsoft Windows domains. Related terms: Active Directory, AD Forensics, Windows domains.

Encryption: The process of converting plaintext into ciphertext using an encryption algorithm and a key. Encryption can be used to protect sensitive data, such as financial information or personal identifiable information (PII). Related terms: plaintext, ciphertext, encryption algorithm, key.

File wiping: The process of securely deleting data from digital media by overwriting the data with random or patterned bits. File wiping can be used to ensure that data cannot be recovered using data recovery tools. Related terms: data recovery, secure deletion.

Forensic image: An exact replica of digital media, including all data and metadata, created using a forensic imaging tool. A forensic image is also known as a bit-for-bit copy. Related terms: bit-for-bit copy, acquisition, hash value.

Hash value: A unique numerical value generated by a hash function that can be used to verify the integrity and authenticity of digital evidence. Hash values are used to ensure that a forensic image or copy of digital media is an exact replica of the original evidence. Related terms: forensic image, bit-for-bit copy, acquisition.

Honeypot: A decoy system or network used to lure and detect malicious actors, such as hackers or malware. Honeypots can be used to gather information about attacks, identify vulnerabilities, and improve security. Related terms: decoy system, malicious actors, attacks.

Incident response: The process of identifying, containing, and mitigating a security incident, such as a data breach or cyber attack. Incident response plans should include procedures for collecting and preserving digital evidence, as well as steps for remediation and recovery. Related terms: data breach, cyber attack, digital evidence, remediation, recovery.

Live acquisition: The process of creating a forensic image or copy of digital media while the system is still running and in use. Live acquisition can be used to capture volatile data, such as running processes or network connections, that would be lost during a shutdown. Related terms: forensic image, bit-for-bit copy, volatile data.

Malware: Short for "malicious software," malware is any software that is designed to harm or exploit a computer system or its users. Malware can include viruses, worms, trojans, ransomware, and other types of malicious code. Related terms: viruses, worms, trojans, ransomware.

Metadata: Data about data, such as the creation date, last modified date, file size, and file type. Metadata can be used to help identify, organize, and analyze digital evidence. Related terms: digital evidence, acquisition, hash value.

Network forensics: The use of digital forensics techniques to investigate network traffic and security incidents. Network forensics can help identify the source and destination of network attacks, as well as the methods and tools used. Related terms: network traffic, security incidents.

Slack space: The unused space on a hard drive or other storage media between the end of a file and the next allocation unit. Slack space can be used for data hiding or to recover deleted files. Related terms: data hiding, deleted files, allocation unit.

Steganography: The practice of hiding data within other data or structures, such as images or audio files. Steganography can be used for legitimate purposes, such as digital watermarking, or for malicious

purposes, such as hiding malware or illegal content. Related terms: data hiding, digital watermarking, malware.

Timeline analysis: The process of analyzing digital evidence to reconstruct events in chronological order. Timeline analysis can help investigators understand the sequence of events leading up to a security incident, identify suspects, and build a case. Related terms: digital evidence, security incident, sequence of events.

Unallocated space: The portion of a hard drive or other storage media that is not currently being used to store files. Unallocated space can contain deleted files or other data that can be recovered using data carving or other forensic techniques. Related terms: data carving, deleted files, forensic techniques.

Volatile data: Data that is stored in memory or other temporary storage locations and is lost when the system is shut down or restarted. Volatile data can include running processes, network connections, and other system information. Related terms: memory, temporary storage, running processes, network connections.

Windows domains: A system used by Microsoft Windows networks for centralized management of network resources, such as users, groups, and devices. Windows domains use Active Directory as a directory service. Related terms: Active Directory, directory service, centralized management.

Access Data FTK (Forensic Toolkit): A digital forensics suite developed by AccessData that allows for the examination of computer systems and data acquisition. FTK provides comprehensive processing and indexing up front, so filtering and searching is faster. It also includes registry analysis, email recovery, and data carving, among other features.

Acquisition: The process of creating a forensic image or copy of digital media, such as a hard drive or mobile device, for analysis. This process should maintain the integrity and accuracy of the data to ensure it can be used as evidence in court.

Autopsy: A digital forensics platform and graphical interface for The Sleuth Kit and other digital forensics tools. It allows for the examination of disk images and enables analysts to view and analyze files, directories, and registry keys. Autopsy also includes modules for data carving, hash filtering, and keyword searching.

Bitlocker: A full disk encryption feature included with Microsoft Windows. Bitlocker can be used to protect data at rest by encrypting the entire hard drive, including the operating system, applications, and files. This can make it more difficult for digital forensics analysts to recover data, as they may need to bypass the encryption before analysis.

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 reliability of evidence in a digital forensics investigation.

Data Carving: The process of extracting data from a digital media source without relying on the file system or metadata. Data carving can be useful in recovering deleted files or data that has been otherwise

damaged or corrupted.

Digital Forensics: The process of collecting, analyzing, and preserving digital evidence in order to investigate cybercrimes, data breaches, and other digital incidents. Digital forensics involves the use of specialized tools and techniques to recover and examine data from a variety of digital sources, including computers, mobile devices, and networks.

Encryption: The process of encoding data in such a way that only authorized parties can access it. Encryption can be used to protect sensitive data, such as confidential communications or financial information, and can make it more difficult for digital forensics analysts to recover data.

EnCase Forensic: A digital forensics suite developed by OpenText. EnCase Forensic provides a wide range of features for data acquisition, analysis, and reporting. It supports a variety of file systems and devices, and includes tools for data carving, decryption, and password recovery.

Forensic Image: A bit-for-bit copy of digital media that has been acquired using a forensic imaging tool. Forensic images can be used for analysis and should maintain the integrity and accuracy of the original data.

Hash Value: A unique value generated by a hash function that can be used to verify the integrity of data. Hash values can be used to compare the original data with a forensic image to ensure that they match and have not been altered.

Honeypot: A security resource that is intended to be probed, attacked, or compromised in order to detect, deflect, or study attempts to breach network security. Honeypots can be used to distract attackers from more valuable targets and can provide valuable information about the tactics, techniques, and procedures (TTPs) used by threat actors.

Incident Response: The process of identifying, investigating, and mitigating a security incident. Incident response involves a variety of activities, including data collection, analysis, and remediation, as well as communication with stakeholders and reporting.

Integrity: The assurance that data has not been altered or tampered with. Maintaining the integrity of data is essential in digital forensics to ensure that evidence is reliable and can be used in court.

Log Analysis: The process of reviewing and interpreting log data in order to identify security incidents, investigate their causes, and mitigate their effects. Log analysis can be used to detect anomalous behavior, identify trends and patterns, and correlate events across multiple systems.

Malware Analysis: The process of analyzing malware to understand its capabilities, functionality, and intent. Malware analysis can be used to develop signatures and other countermeasures to detect and prevent malware attacks, as well as to gather intelligence about threat actors and their TTPs.

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

challenging due to the variety of operating systems, file systems, and data formats used in mobile devices.

Network Forensics: The process of collecting, analyzing, and preserving data from network traffic for use in digital forensics investigations. Network forensics can be used to identify security incidents, investigate their causes, and mitigate their effects.

NTFS: The New Technology File System, a file system used by Microsoft Windows. NTFS supports features such as file permissions, encryption, and compression, which can make it more difficult for digital forensics analysts to recover data.

Password Recovery: The process of retrieving lost or forgotten passwords for digital media, applications, or services. Password recovery can be used in digital forensics to gain access to encrypted data or locked devices.

Registry Analysis: The process of examining the Windows Registry, a database that stores configuration settings and other information for the Windows operating system and applications. Registry analysis can be used to recover data, such as recently accessed files or installed software, and to identify security vulnerabilities.

Sleuth Kit: An open-source digital forensics toolkit that can be used for data acquisition, analysis, and reporting. The Sleuth Kit supports a variety of file systems and devices, and includes tools for data carving, decryption, and password recovery.

Sqrrl: A threat hunting platform that uses machine learning and big data analytics to detect and respond to cyber threats. Sqrrl can be used to investigate incidents, identify adversaries, and track their movements across the network.

Timeline Analysis: The process of creating and analyzing a timeline of events related to a digital forensics investigation. Timeline analysis can be used to identify patterns and trends, correlate events across multiple systems, and reconstruct the sequence of events leading up to a security incident.

Triage: The process of prioritizing and assessing the severity of digital forensics cases or incidents. Triage can be used to quickly identify high-priority cases and allocate resources accordingly.

Volatility: An open-source memory forensics framework that can be used to analyze volatile memory (RAM) dumps. Volatility supports a variety of operating systems and plugins, and can be used to recover data such as running processes, network connections, and loaded drivers.

Wireshark: A popular open-source network protocol analyzer that can be used to capture, analyze, and visualize network traffic. Wireshark supports a wide range of protocols and can be used for network forensics, security testing, and troubleshooting.

In conclusion, digital forensics tools play a crucial role in investigating cybercrimes, data breaches, and other digital incidents. This glossary provides an overview of some of the key terms and concepts related to digital forensics tools in the context of the Professional Certificate in Digital Forensics Fundamentals.

Understanding these terms is essential for anyone involved in digital forensics, whether as a practitioner, researcher, or student.

Autopsy: A digital forensics tool used for hard drive and mobile device analysis. It allows investigators to conduct a thorough examination of the device, including file system analysis, data carving, and keyword searching. Autopsy is an open-source platform that is widely used in the digital forensics community.

Bitlocker: A full disk encryption feature included with Microsoft Windows. Bitlocker can be used to protect data on fixed and removable drives, and it supports the use of a TPM (Trusted Platform Module) for added security. Digital forensics investigators can use tools such as Belkasoft Evidence Center to recover Bitlocker keys and access encrypted data.

Chain of custody: The chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. A proper chain of custody is essential in digital forensics to ensure that evidence is admissible in court.

Data carving: The process of recovering deleted files from a digital device by analyzing the raw data on the storage media. Data carving tools, such as Autopsy and EnCase, can identify and recover files based on their header and footer signatures, even if the file system metadata has been deleted or corrupted.

DFIR: Stands for Digital Forensics and Incident Response. DFIR is a specialized field of digital forensics that focuses on identifying and responding to cybersecurity threats, such as data breaches, network intrusions, and malware infections.

Email forensics: The process of analyzing email messages and metadata for use in digital forensics investigations. Email forensics tools, such as Emailchemy and Autopsy, can extract email messages from a variety of sources, including mail servers, backup tapes, and local storage.

EnCase: A digital forensics tool developed by Open Text. EnCase is a widely used platform for hard drive and mobile device analysis, and it supports a wide range of features, including data carving, keyword searching, and hash set analysis.

File system: The method used by an operating system to organize and store files on a digital device. Common file systems include NTFS (New Technology File System), FAT32 (File Allocation Table 32), and HFS+ (Hierarchical File System Plus). Digital forensics investigators must be familiar with the file system of the device being analyzed to properly recover and analyze data.

Forensic image: A bit-for-bit copy of a digital device that is used for digital forensics analysis. Forensic images are created using tools such as FTK Imager and dd, and they ensure that the original evidence is not altered during the analysis process.

Hash value: A unique alphanumeric string that is generated by hashing the contents of a file or forensic image. Hash values are used to verify the integrity of digital evidence and ensure that it has not been altered since the forensic image was created.

Hex editor: A software tool used to view and edit the raw data on a digital device. Hex editors, such as HxD and WinHex, are used by digital forensics investigators to analyze data at the binary level and recover deleted or corrupted files.

Honeypot: A security resource whose value lies in being probed, attacked, or compromised. Honeypots are used in digital forensics to detect and analyze cyber threats, such as malware and network intrusions.

Incident response: The process of identifying, containing, and mitigating a cybersecurity incident. Incident response is a critical component of digital forensics and is often performed in conjunction with a digital forensics investigation.

IP address: A unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. IP addresses are used in digital forensics to trace the source and destination of network communications, as well as to identify devices involved in cyber threats.

Log files: Records of events that have occurred on a digital device or network. Log files, such as system logs, application logs, and network logs, are used in digital forensics to reconstruct events leading up to a cybersecurity incident and to identify the root cause of the incident.

Malware: Short for malicious software. Malware is any software that is designed to harm a digital device, steal sensitive information, or disrupt network communications. Malware is a common threat in digital forensics investigations and must be properly identified and analyzed to mitigate the threat.

Mobile device forensics: The process of analyzing mobile devices, such as smartphones and tablets, for use in digital forensics investigations. Mobile device forensics tools, such as Cellebrite UFED and Oxygen Forensics Detective, can extract data from a wide range of mobile devices, including call logs, text messages, and social media apps.

Network forensics: The process of analyzing network traffic for use in digital forensics investigations. Network forensics tools, such as Wireshark and Network Miner, can capture and analyze network traffic in real-time, as well as reconstruct past network activity.

NTFS: Short for New Technology File System. NTFS is a file system used by Microsoft Windows operating systems to organize and store files on a digital device. NTFS supports features such as journaling, file compression, and access control, making it a common target for digital forensics investigations.

Registry analysis: The process of analyzing the Windows Registry for use in digital forensics investigations. The Windows Registry is a database that stores configuration settings for the Windows operating system and installed applications. Registry analysis tools, such as Registry Explorer and Autopsy, can extract valuable information from the registry, including user activity, software installation history, and network connections.

SQLite: A software library that provides a relational database management system. SQLite is commonly used in mobile devices and applications, making it a common target for digital forensics investigations. SQLite databases can be analyzed using tools such as DB Browser for SQLite and Autopsy.

Timeline analysis: The process of creating a visual representation of events that have occurred on a digital device over time. Timeline analysis tools, such as Timeline Explorer and Autopsy, can extract timestamps from a wide range of data sources, including files, registry keys, and log files, and display them in a chronological order.

Triage: The process of quickly assessing the severity and impact of a cybersecurity incident. Triage is a critical component of digital forensics and is often performed in conjunction with incident response.

Volatility: An open-source memory forensics framework used to analyze volatile memory (RAM) dumps. Volatility can extract a wide range of information from RAM dumps, including running processes, network connections, and open files.

XML: Short for Extensible Markup Language. XML is a markup language that is used to encode data in a format that is both human-readable and machine-readable. XML is commonly used in digital forensics to store and exchange data between tools and platforms.

Note: The response exceeds 3000 words.

Access Data FTK (Forensic Toolkit): A digital forensics suite developed by AccessData. FTK provides robust capabilities in processing and analyzing computer media, mobile devices, and cloud data. It is known for its speed in indexing and searching data, as well as its ability to handle large volumes of information. FTK includes features such as email analysis, social media analysis, and timeline analysis, making it a comprehensive solution for digital forensic examinations.

Acquisition: The process of creating a forensic image or bit-for-bit copy of digital media. This is the first step in digital forensics, ensuring that the original evidence remains intact while a duplicate is used for analysis. Acquisition often involves creating a hash value for both the original and copied media to verify their integrity and consistency.

Autopsy (The Sleuth Kit): Autopsy is a digital forensics platform and graphical interface for The Sleuth Kit and other digital forensics tools. It is used for analyzing and reporting on digital media, such as hard drives, USB drives, and mobile devices. Autopsy provides features including keyword searching, registry analysis, and timeline analysis, and it supports various file systems and image formats.

BitLocker: A full disk encryption feature included in Microsoft Windows operating systems. BitLocker is used to protect data by providing encryption for entire volumes or drives. It can be a challenge for digital forensic examiners, as it may require decryption keys to access the data stored within.

Chain of Custody: The chronological documentation or paper trail, detailing the seizure, custody, control, transfer, analysis, and disposition of digital evidence. Maintaining a proper chain of custody is crucial for ensuring the integrity and admissibility of evidence in legal proceedings.

Data Carving: A process used in digital forensics to recover files that have been deleted, damaged, or otherwise made inaccessible. Data carving involves analyzing raw data at the sector level to identify file headers, footers, and other characteristics, allowing for the reconstruction and recovery of the files.

Data Volume: A logical or physical storage unit containing files and directories. Data volumes can take various forms, such as hard disk drives, solid-state drives, and flash drives. Understanding data volumes is essential for digital forensic examiners, as they provide the foundation for searching, analyzing, and interpreting digital evidence.

Deleted Files: Files that have been removed from a file system but may still reside on a data volume. When a file is deleted, its entry is typically removed from the file system's allocation table, but the file's data may still be present on the storage media until it is overwritten. Digital forensic tools can often recover deleted files, which can provide valuable evidence in investigations.

Digital Forensics: The process of uncovering and interpreting electronic data for use in legal proceedings or investigations. Digital forensics involves the identification, preservation, extraction, analysis, and documentation of digital evidence, requiring a combination of specialized tools, techniques, and knowledge.

Email Forensics: A subfield of digital forensics focused on the analysis of email communications and metadata. Email forensics can reveal crucial information, such as the sender, recipient, date and time, and message content. Digital forensic tools often include features for parsing and analyzing various email formats, such as PST, EML, and MSG files.

Encryption: The process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and a key. Encryption is used to protect sensitive data and can pose challenges for digital forensic examiners, as decryption keys or significant computational resources may be required to access the underlying information.

File System: A method for organizing and storing files on a data volume. Common file systems include NTFS, FAT32, and exFAT in Windows, and HFS+ and APFS in macOS. Understanding file systems is essential for digital forensic examiners, as they provide the framework for locating, analyzing, and interpreting digital evidence.

Forensic Image: A bit-for-bit copy of digital media used in digital forensics. Forensic images maintain the original data's integrity, allowing for analysis without altering the original evidence. Forensic images are typically created using write blockers and are verified using hash values.

Hash Value: A fixed-size string of characters, generated by a hash function, which serves as a unique identifier for a file or data set. Hash values are used to verify the integrity and consistency of digital evidence by comparing the hash values of original and copied media. Common hash functions include MD5 and SHA-1.

Hibernation File: A file in Windows operating systems that contains the contents of a computer's memory when the system hibernates. Analyzing hibernation files can provide valuable information for digital forensic examiners, such as running processes, open files, and system configurations.

Logical Volume: A virtual data volume that appears as a separate drive or partition within the file system. Logical volumes can span multiple physical volumes and are managed by volume managers or logical

volume managers. Understanding logical volumes is essential for digital forensic examiners, as they can contain valuable digital evidence.

Mobile Device Forensics: A subfield of digital forensics focused on the analysis of mobile devices, such as smartphones and tablets. Mobile device forensics involves the extraction, interpretation, and documentation of data stored on these devices, including call logs, messages, contacts, and application data.

NTFS (New Technology File System): A file system used in Microsoft Windows operating systems. NTFS supports features such as file permissions, encryption, and compression, making it a popular choice for storing sensitive data. Digital forensic tools must be capable of parsing and analyzing NTFS to access and interpret the data stored within.

Pagefile: A file in Windows operating systems that serves as an extension of random-access memory (RAM). The pagefile stores data and applications that are not actively being used but have not been removed from memory. Analyzing pagefiles can provide valuable information for digital forensic examiners, such as running processes and system configurations.

Registry: A database in Windows operating systems that stores low-level settings and configurations for the operating system, hardware, and software. The registry contains crucial information for digital forensic examiners, such as user account information, software installations, and system configurations.

Slack Space: The space between the end of a file and the end of a data cluster or sector. Slack space can contain remnants of previously deleted files or fragments of data, making it a valuable source of digital evidence for forensic examiners.

SQLite: A self-contained, file-based database system commonly used in mobile devices and applications. SQLite databases can store various types of data, such as messages, contacts, and application settings. Digital forensic tools must be capable of parsing and analyzing SQLite databases to access and interpret the data stored within.

Swap Space: The Linux and Unix equivalent of the Windows pagefile, used to extend random-access memory (RAM). Swap space stores data and applications that are not actively being used but have not been removed from memory. Analyzing swap spaces can provide valuable information for digital forensic examiners, such as running processes and system configurations.

Timeline Analysis: The process of examining and interpreting the sequence of events on a digital device. Timeline analysis can reveal patterns and relationships between users, applications, and data, providing crucial insights for digital forensic examiners.

Triage: The initial assessment and prioritization of digital evidence during an investigation. Triage involves quickly identifying and analyzing critical data to guide the investigation and focus resources on the most relevant evidence.

Unallocated Space: The portion of a data volume that has not been allocated to any file or directory. Unallocated space can contain remnants of previously deleted files or fragments of data, making it a

valuable source of digital evidence for forensic examiners.

Volatility: The characteristic of digital evidence that describes its potential for change or loss over time. Volatile data, such as memory contents, can be lost when power is removed or when a system is shut down, requiring digital forensic examiners to act quickly to capture and analyze this evidence.

Write Blocker: A