Professional Certificate in Digital Forensics Fundamentals

Mobile Device Forensics

ACPO: Association of Chief Police Officers. A set of guidelines for digital forensics, including mobile device forensics, that outlines best practices for handling and analyzing digital evidence.

ADFS: Active Directory Federation Services. A software component developed by Microsoft that can be used for authentication and authorization of users in a forensic examination of mobile devices.

ADB: Android Debug Bridge. A command-line tool used to communicate with Android devices for the purpose of debugging and data collection in a mobile device forensics examination.

Android: A popular mobile operating system developed by Google. Forensic examinations of Android devices involve analyzing data stored on the device, as well as data stored in the cloud.

Application data: Data stored by mobile apps, including user-generated content, settings, and preferences. Application data can provide valuable evidence in a mobile device forensics examination.

Backup: A copy of data stored on a mobile device, often in the cloud. Backups can be a rich source of evidence in a mobile device forensics examination.

BIOS: Basic Input/Output System. The firmware that initializes hardware and loads the operating system on a computer or mobile device. In a mobile device forensics examination, the BIOS can provide information about the device's hardware and configuration.

Bitlocker: A full disk encryption feature in Microsoft Windows. Bitlocker can be used to protect data on a mobile device, making it inaccessible without the encryption key.

Bluetooth: A wireless technology used for short-range communication between devices. Bluetooth data can provide evidence in a mobile device forensics examination.

Cache: Temporary data stored by a mobile device or app for quick access. Cache data can provide valuable evidence in a mobile device forensics examination.

Chip-off: A mobile device forensics technique that involves removing the memory chip from a device and reading the data directly from the chip. Chip-off is a destructive process that can damage the device.

Cloud forensics: The process of collecting and analyzing data stored in the cloud, including data associated with mobile devices. Cloud forensics can provide valuable evidence in a mobile device forensics examination.

CPU: Central Processing Unit. The primary component of a computer or mobile device that performs calculations and executes instructions. The CPU can provide information about the device's hardware and configuration in a mobile device forensics examination.

CPU registers: Small amounts of memory used by the CPU to store data and instructions. CPU registers can provide valuable evidence in a mobile device forensics examination.

Data acquisition: The process of collecting data from a mobile device for analysis in a forensic examination. Data acquisition can involve physical, logical, or over-the-air methods.

Data carving: The process of extracting data from a mobile device by searching for specific data patterns or signatures. Data carving can be used to recover deleted data.

Data extraction: The process of extracting data from a mobile device for analysis in a forensic examination. Data extraction can involve physical, logical, or over-the-air methods.

Data image: A bit-for-bit copy of a mobile device's data, including deleted data. Data images can be created using physical or logical acquisition methods.

Data partition: A logical division of a mobile device's storage space. Data partitions can provide evidence in a mobile device forensics examination.

Data remnants: Data that remains on a mobile device after an attempt to delete it. Data remnants can provide valuable evidence in a mobile device forensics examination.

Deleted data: Data that has been removed from a mobile device, but may still be recoverable. Deleted data can provide valuable evidence in a mobile device forensics examination.

Digital evidence: Any data that can be used as evidence in a legal proceeding. Digital evidence can include data from mobile devices, computers, and other digital sources.

Dual-persona: A mobile device configuration that separates personal and work data into separate partitions or containers. Dual-persona devices can provide additional security for sensitive data.

Encryption: The process of converting data into a code that cannot be read without the decryption key. Encryption can be used to protect data on a mobile device.

File system: The structure used to organize data on a mobile device's storage. The file system can provide evidence in a mobile device forensics examination.

File system artifacts: Data stored by the file system that can provide evidence in a mobile device forensics examination. File system artifacts can include metadata, such as file creation and modification dates.

Firewall: A security system that monitors and controls incoming and outgoing network traffic. Firewalls can be used to protect data on a mobile device.

Forensic image: A bit-for-bit copy of a mobile device's data, including deleted data. Forensic images can be created using physical or logical acquisition methods.

Geolocation data: Data that can be used to determine the physical location of a mobile device. Geolocation data can provide valuable evidence in a mobile device forensics examination.

Hash value: A unique value calculated from data that can be used to verify the integrity of the data. Hash values can be used to ensure that data has not been altered during a mobile device forensics examination.

iCloud: A cloud storage and computing service developed by Apple. iCloud can be a rich source of evidence in a mobile device forensics examination.

iOS: A mobile operating system developed by Apple. Forensic examinations of iOS devices involve analyzing data stored on the device, as well as data stored in the cloud.

Jailbreak: The process of removing restrictions on an iOS device to allow for the installation of unauthorized software. Jailbreaking can provide access to data that is not normally accessible in a mobile device forensics examination.

JTAG: Joint Test Action Group. A mobile device forensics technique that involves connecting to a device's JTAG interface to extract data. JTAG can be used to extract data from devices that cannot be accessed using other methods.

Logical acquisition: The process of collecting data from a mobile device using the device's operating system or file system. Logical acquisition is a non-destructive process that does not modify the device's data.

Malware: Software designed to harm a mobile device or steal data. Malware can provide valuable evidence in a mobile device forensics examination.

Mobile device management (MDM): A system used to manage and secure mobile devices in an enterprise environment. MDM can provide additional security for sensitive data.

Mobile forensics: The process of collecting and analyzing data from a mobile device for use as evidence in a legal proceeding. Mobile forensics can involve physical, logical, or over-the-air methods.

Mobile operating system: The software that runs on a mobile device and manages its hardware and software resources. Mobile operating systems can provide evidence in a mobile device forensics examination.

NAND flash memory: A type of non-volatile memory used in mobile devices. NAND flash memory can provide evidence in a mobile device forensics examination.

Network forensics: The process of collecting and analyzing data transmitted over a network for use as evidence in a legal proceeding. Network forensics can provide valuable evidence in a mobile device forensics examination.

Over-the-air (OTA) acquisition: The process of collecting data from a mobile device wirelessly, without physical access to the device. OTA acquisition can be used to collect data from devices that are not physically accessible.

Partition: A logical division of a mobile device's storage space. Partitions can provide evidence in a mobile device forensics examination.

Physical acquisition: The process of collecting a bit-for-bit image of a mobile device's data, including deleted data. Physical acquisition is a destructive process that can damage the device.

RAID: Redundant Array of Independent Disks. A storage technology that combines multiple physical disks into a single logical unit. RAID can