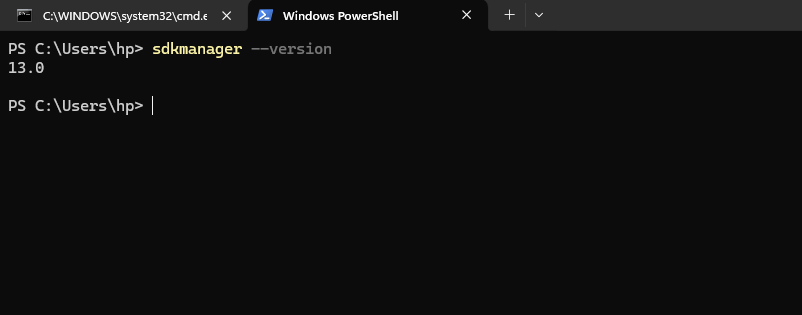
ADB Installation

The first step of the process is to install adb by installing SDK manager via android studio. To comfirm the installation, run “sdkmanager --version” as shown below to get the version of my SDKManager.

Process 

Reveal hidden developer options

|  |  |
| --- | --- |
| Step | Action |
| Step 1 | Go to Settings |
| Step 2 | About phone |
| Step 3 | Tap on “Build number” seven times  A box will appear with a notification that developer options is enables |
| Step 4 | Return to the previous screen to find Developer options |

Enable Android Debugging Bridge (ADB)

Now that the developer option has been enabled, access the developer options menu. In this menu set Android Debugging Bride (ADB) also known as USB debugging to communicate with the device.

Connect the phone to my computer using a USB.

|  |  |
| --- | --- |
| Step | Action |
| Step 1 | To connect the android device to the computer, use the Micro USB cable.  The standard USB end goes to the computer and the Micro USB connects to the Android device. |
| Step 2 | Allow USB debugging prompt that is shown when the android device is connected to the computer |

ADB Devices command

Type “adb devices” to get the unique serial number of the connected devices and the connection state as shown below.

|  |  |
| --- | --- |
| Step | Action |
| Step 1 | Open the administrator command prompt located at C:\WINDOWS\system32\cmd.exe |
| Step 2 | Type the command “ADB Devices” as shown here    The output is the unique serial number and the state of the device. |

Run “adb backup –all” to extract all the data from the android device and authorize the client to proceed with the backup and a file called backup.ab will be created.

Convert the resultant backup.ab to a .tar for easy extraction using android-backup-processor software.

Findings

Open source tools for mobile device forensics

1. Autopsy: Although primarily known as a digital forensics platform for analyzing hard drives and media images, Autopsy also supports mobile device analysis. It allows you to analyze data from various mobile platforms, including Android and iOS devices. Autopsy provides features such as timeline analysis, keyword search, file carving, and integrated hash databases. It belongs to logical extraction category.

Uses:

* Autopsy offers features such as timeline analysis, keyword search, file carving, and integrated hash databases, making it suitable for comprehensive forensic examinations.
* It provides a user-friendly interface and supports plugins for extending functionality.

Limitations:

* While Autopsy supports mobile device analysis, it may not have as extensive mobile-specific features compared to dedicated mobile forensic tools.
* Its mobile device analysis capabilities might not be as advanced or specialized as those found in tools specifically designed for mobile forensics.

1. MobSF (Mobile Security Framework): MobSF is an automated mobile application (Android and iOS) security testing, vulnerability scanning, and analysis tool. It supports dynamic analysis, static analysis, and web API testing of mobile apps. While its primary focus is on security testing, MobSF can also be used for forensic analysis of mobile applications. It belongs to

Uses:

* MobSF is primarily designed for security testing and vulnerability scanning of mobile applications, but it can also be used for forensic analysis.
* It supports dynamic analysis, static analysis, and web API testing of Android and iOS apps, providing insight into potential security issues and vulnerabilities.
* MobSF can assist in analyzing mobile apps for malicious behavior or privacy violations, which can be relevant in forensic investigations.

Limitations:

* While MobSF offers some forensic analysis capabilities, it may lack the depth and breadth of features compared to tools specifically dedicated to mobile device forensics.
* Its focus on security testing means that it may not provide all the features required for comprehensive forensic examinations, such as advanced data extraction and analysis.

1. Andriller: Andriller is a tool for Android smartphone forensic analysis. It enables examiners to extract data such as call logs, messages, contacts, photos, videos, and more from Android devices. Andriller supports various extraction methods, including physical extraction, logical extraction, and file system extraction. It also provides built-in analysis features for examining extracted data.

Uses:

* It supports various extraction methods, including physical extraction, logical extraction, and file system extraction, allowing examiners to access different types of data from Android devices.
* Andriller provides built-in analysis features for examining extracted data, such as call logs, messages, contacts, photos, videos, and more.

Limitations:

* As a tool focused on Android device forensics, Andriller may not support iOS devices or provide features tailored to iOS forensic analysis.
* Its capabilities may be limited to what is possible through software-based extraction methods, and it may not support advanced techniques such as chip-off or JTAG forensics.

1. XRY: XRY is a popular mobile forensics tool developed by MSAB. While the commercial version of XRY is widely used in law enforcement and digital forensic investigations, MSAB also provides a free version called XRY Photon for non-commercial use. XRY Photon offers basic mobile device forensic capabilities, allowing users to extract data from Android and iOS devices, including call logs, messages, contacts, and more. This belongs to physical and logical extraction techniques of device forensics.

Uses:

* It supports data extraction from both Android and iOS devices, including call logs, messages, contacts, and more.
* XRY provides advanced features for forensic analysis, such as physical extraction methods and support for a wide range of mobile device models.

Limitations:

* While XRY Photon offers basic mobile device forensic capabilities for free, the full commercial version of XRY may be required for advanced features and support.
* XRY's free version may have limitations compared to the commercial version, such as fewer supported devices or extraction methods.
* As a commercial tool, the free version may lack certain features or updates available in the paid version, and it may not receive the same level of support or maintenance.