

Android Forensics

(Part 1)



Contents

- Introduction to Android Forensics
- Challenges in mobile forensics
- Seizure and Isolation
- Gathering Information on Device Accessibility
- Prerequisites
- Types of Acquisition
- Operating Modes of Android
- Rooting Android Phone



Introduction to Android Forensics

- Mobile forensics is a branch of digital forensics that is evolving in today's digital era
- It is constantly changing as new phones are released and operating systems are updated
- Android forensics deal with extracting, recovering, and analysing data present on an Android device through various techniques under **forensically sound** conditions
- Due to the open nature of the Android operating system, these forensic techniques and methods can apply to more than just mobile phones
- It can be refrigerators, vehicle entertainment units, televisions, watches, and many more devices that run Android Operating Systems (OS)



Challenges in mobile forensics

- The wide range of operating systems and device models
- Preventing Data Alterations on mobile devices
- Inherent security features
- Legal issues



Seizure and Isolation

- Note location from where mobile has been collected.
- Take the picture using camera and take picture of the location
- Chain of Custody
 - Is a document to maintain each record of the Digital evidence from the collection to presentation
 - Another part of documentation is taking pictures (photographs) of the crime scene, capturing the original state of the mobile device, as well as the make, model, serial number, IMEI number or operating system version .which would help during the acquisition phase and need to be captured as well
- Take the picture of the mobile phone before starting any progress
- Request for Pin, Pattern, Passwords, SIM pin
- Check for any Unified Endpoint Management solutions
- Note the status of the device
 - Whether it's powered off or on
 - If it is power on then, check the battery status, network status
 - Check where the screen is locked
- Search/request for the SIM and if any cables are located around



Seizure and Isolation (Cont'd)

Isolation Techniques (If the device is ON)

- Activate Airplane mode
- Check and manually disable, if necessary, “hotspots” or any GPS locations, the Wi-Fi and Bluetooth toggles (these may be left on even in Airplane mode if the user enabled Wi-Fi once in that mode)
- Do not remove the SIM or SD card at this point
- Connect the phone to a power bank
- If you have a Faraday bag handy, place the phone along with the adapter and charger into the Faraday bag

Faraday bag

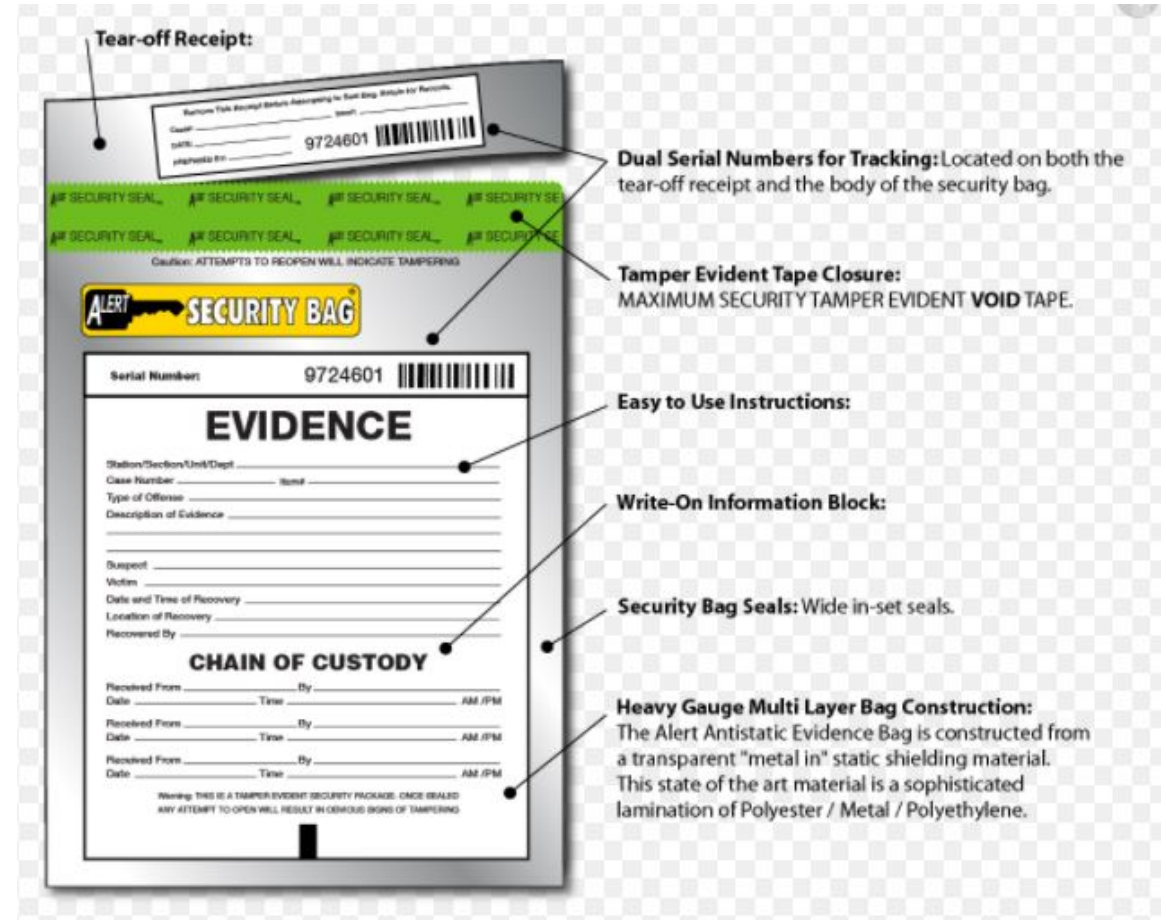


Seizure and Isolation (Cont'd)



Isolation Techniques (If device is OFF, DO NOT turn ON.)

- Place it in an Evidence Bag or Box
- If you have a Faraday bag handy, place the phone along with the adapter and charger into the Faraday bag
- Bring it back to Forensic Lab
- Back in the Forensic Lab
- You will want to, Write-protect the SD card, remove the SIM card
- Do a proper acquisition of both SIM and SD card.
- As mentioned phones cannot always be left powered off during acquisition of the phone
- You will have to turn on the phone if necessary, and treat it as if it was turn on and apply the Isolation Techniques, mentioned in the earlier slides



Seizure and Isolation(Cont'd)

Forensic acquisition

- is the process of acquiring the original evidence in a forensically sound manner while maintaining the integrity of it
- This process is also known as “Imaging”
- It can be done on site (at the scene) and can also be done off-site (in the lab)

Hashing

- Done after acquisition of device
- Hashing is the method used to prove the integrity of the evidence
- MD5 or SHA are widely used algorithms to calculate the Hash values
- Hash values should be documented as well to maintain record of the Digital evidence.



Gathering Information on Device Accessibility

- Android Mobile device acquisition depends on the following factors for data collection

Factors

- Android Version
- Device Security
 - Pattern
 - PIN
 - Password
 - Fingerprint
 - Face Recognition mechanism
 - Bluetooth Device Lock & Unlock



Gathering Information on Device Accessibility (Cont'd)

Factors

- Device accessibility
 - Non-Root Access
 - Root Access

Mode of Transfers

- The following mediums can be utilized to acquire a mobile device which depends on availability and device status:
 - USB Connectivity
 - **Bluetooth**: Mobile acquisition can be performed by utilizing Android Debugging bridge(ADB) via bluetooth connection
 - **Wireless**: Both mobile device and acquisition machine has to be connected to same wifi network. Device acquisition can be performed by using android device bridge via WiFi

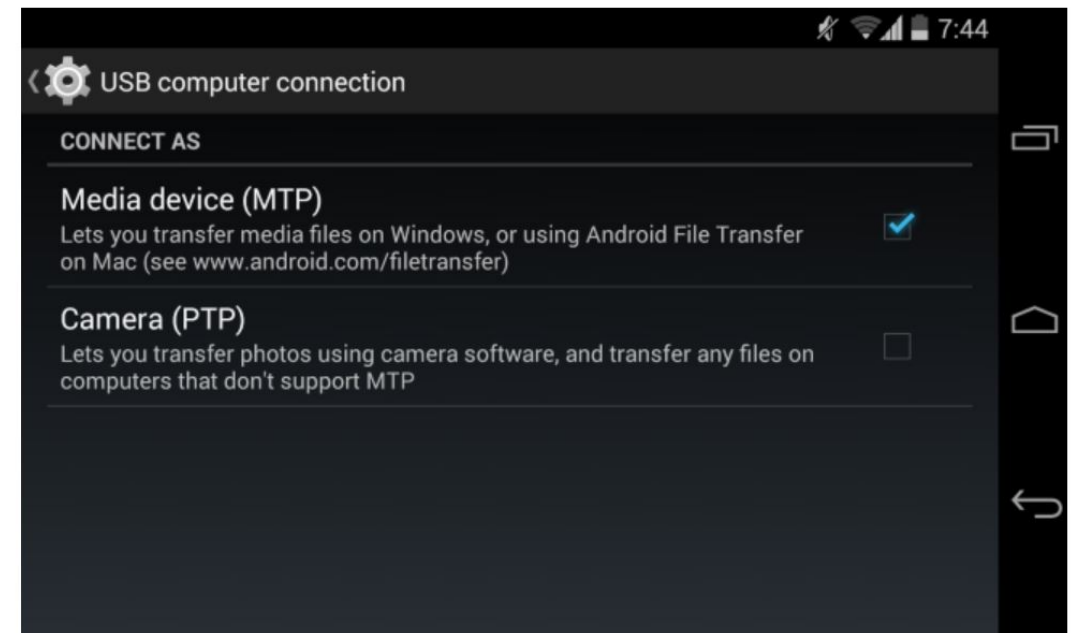


Prerequisites

- This pre-requisites is either done during or before acquisition

Media Transfer Protocol (MTP)

- Allows media files to be transferred automatically to and from portable device
- Ensured for uninterrupted device acquisition



MTP Reference



Prerequisites (Cont'd)

Enabling USB debugging

- USB debugging is a developer option which enables analysis machine to establish connection with the device via Android Debug Bridge (ADB)
- ADB it acts as a bridge between computer and the mobile phone
- To communicate with the phone from the computer, we do it via ADB
- To work with ADB, USB debugging options should be enabled on the phone

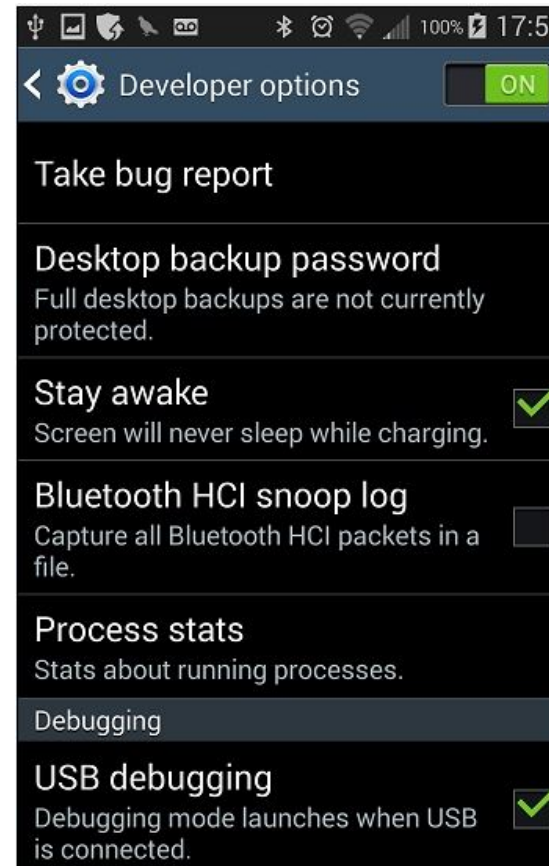
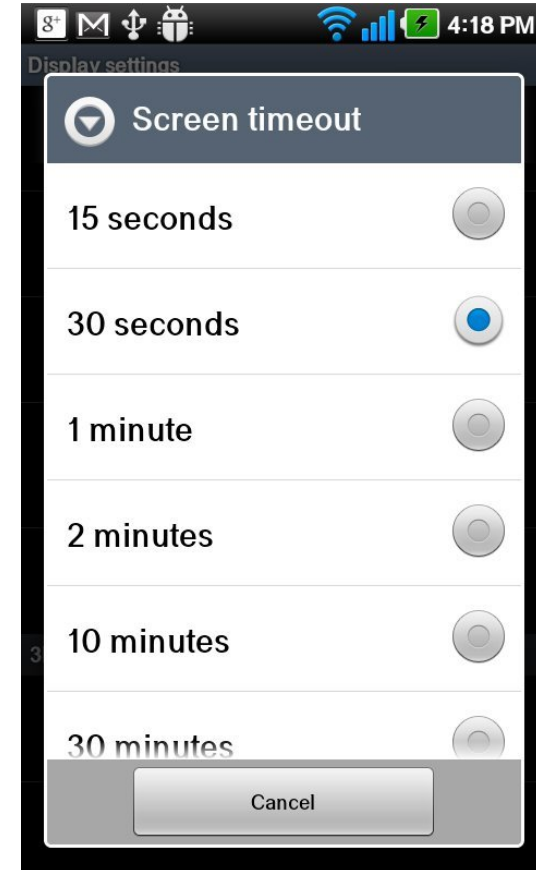
Android version	Steps
V 5.0 and Above	1. Goto Settings > About Phone > Build number > Tap it 7 times to become developer;
	2. Again go to Settings > Developer Options > Check and allow USB Debugging.
V 4.2,4.3 and 4.4	1. Goto Settings > About Phone > Build number > Tap it 4-5 times to become developer;
	2. Again go to Settings > Developer Options > Check and allow USB Debugging.
V 3.0 to 4.1	1. Goto Settings > Developer Options > Enable and Allow USB Debugging.
V 2.0 to 2.3	1. Go to Settings > Applications > Development > USB Debugging.



Prerequisites (Cont'd)

Enable Stay Awake/Increase Screen Time

- Enabling this option and charging the device will make the device stay awake which means that, it doesn't get locked
- In Android devices, this option is usually found under ***Settings / Developer*** options



Types of Acquisition



Logical

SMS

Contact

Call Logs

Media

App Data

File System

SMS

Contact

Call Logs

Media

App Data

Files

Hidden Files

Physical

SMS

Contact

Call Logs

Media

App Data

Files

Hidden Files

Deleted Data

Types of Acquisition (Cont'd)

Advance Logical

- Combines both Logical and File System extraction methods

Manual

- The examiner uses the user interface of the phone to browse and investigate
- No special tools or techniques are required
- Manual Extraction of Chat messages (Screen Shots, export to external media)
- limitation is that only the files and data visible through the normal user interface
- Data extracted through other methods can also be verified using this
- Very easily modify data on the device

Brute Force

- offensive techniques like password cracking, patterns, pins, Rooting the device



Operating Modes of Android

Three (3) operating modes

- Android Safe mode, Recovery Mode and Fastboot Mode

Android Safe mode

- safe mode builds a clean and secure environment
- Third-party apps are disabled and greyed out
- Troubleshoot smartphone's problems, like restarting itself, lagging, freezing, battery issues, or data disappearing, are caused by third-party applications or not



Operating Modes of Android (Cont'd)

Android Recovery Mode

- Recovery is an Android-based, lightweight runtime environment which is separate from and parallel to the main Android operating system
- There are mainly two kinds of recoveries: **stock recovery** and **custom recovery**.
- In recovery mode, you will get some advanced options
- There are several custom recovery images available in the market today, such as ClockworkMod Recovery, TeamWin Recovery Project



Operating Modes of Android (Cont'd)

Android Fastboot Mode

- Fastboot is a tool/protocol that comes with the Android SDK (software developer kit) package
- Which can be used to re-flash partitions on Android device
- It is an alternative to recovery mode for doing installations and updates
- Fastboot mode can be used for unlocking the bootloader for certain Android device models



Rooting Android Phone

- Rooting is the process of letting the users of Android phones gain the highest privilege i.e. Root user privilege on an Android Phone
- Android is based on Linux as discussed. Thus, gaining root access is same as gaining root user access or administrative access on Linux OS
- However, from a forensic point of view, the main reason for rooting is to gain access to those parts of the system that are normally not accessible
- Most of the public root tools will result in a permanent root. In this, the changes persist even after rebooting the device.
- In the case of a temporary root, the changes are lost once the device reboots
- Temporary roots should always be preferred over permanent for forensic acquisition
- Note* it easily modify data on the device



Summary

- Android is a rapid evolving operating system, hence the methods and acquisition methods will keep changing on the basis of device & data access it is providing. Thus Challenges will be faced
- The basic device acquisition & data collection practices mentioned will remain constant for Android devices
- Android Forensic Investigation requires an investigator to be proficient regarding acquisition, extraction and analysis of evidence
- The methods involved and the amount of data collected while performing device acquisition, can become a crucial pointer determining extraction of artifacts leading towards discovering an evidence

