MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Forensics on a Mobile Device, Tools and Limitations

Hassan M*

Digital Forensics and Cybersecurity, John Jay College, USA

***Corresponding author:** Mohammed Hassan, Digital Forensics and Cybersecurity, John Jay College, NY, USA, Email: mhassan@jjay.cuny.edu

Mini Review

Volume 6 Issue 3

Received Date: September 03, 2021

Published Date: September 23, 2021

DOI: 10.23880/ijfsc-16000240

Abstract

In modern days, individuals are deeply attached to their mobile devices. Like many other benign tools, mobile devices are often used for criminal purposes. Such devices can be confiscated at the crime scene, or at a later point in time. Then it's typically examined by forensics expert to extract and retrieve usable information. While technically a mobile phone is a computer by definition, performing forensic examination is quite challenging from a typical desktop or laptop computer systems. In this paper, we explore such challenges, discuss limitations and speculate what the future might be.

Keywords: Android; Forensics; IOS; Linux; Command; Security; Data; Cloud; Analysis

Introduction

When we say mobile device, we think of a handheld device, most often a phone. While there were many flavors and iterations in the past, these days' choices are rather limited. One has to choose either Apple iOS device or Google Android based device whereas just a few years ago, one was able to choose between these two plus – Blackberry, Symbian, Windows Mobile, Palm OS etc. This paper will focus on the most prevalent mobile OS in the market today which is Android. It was based on Linux, developed by Google. Because of its openness, choices of devices and manufacturers, it quickly became very popular worldwide. Android offers devices on all spectrum including high and low end. The underlying operating system is still android.

While the OS remains same, the performance obviously varies. Furthermore, some manufacturers also add their own tweaks, enhancements to differentiate from other vendors. This presents another challenge because ongoing software update may not be available for all devices. Bigger companies are able to support their devices for few years while smaller companies phones barely received any software updates. Subsequent versions of Android addresses this problem by making core components modular, meaning you could technically be running an older build of Android with more recent versions of core components. It's not a perfect solution but much better than what was available in the past. Furthermore, cell phones have undergone a significant transformation. Initially they were just some devices to talk to another party but with advancement in technology, devices became much more capable and usage expanded to – online shopping, watching movies, surf the web, send/receive emails [1].

Anatomy of a Mobile Device

A mobile device is a miniature computer. It has same core components as a normal desktop or laptop computer. They are equipped with a storage device, a CPU, ram, screen, modem and other components. The capacities and capabilities vary by price. For example, higher end Android devices tend to cost more since they generally use latest mobile CPU, modem, and high resolution screen. Low end Android hardware tend to come with less capable CPU, mediocre storage and so on. What they have in common is the operating system – Android. Due to price differences, the OS is often outdated on low end hardware because manufacturers of such devices offer little to no updates. Larger companies tend to support their devices for few years with software updates. The OS version plays a big factor in forensics work. As we know vulnerabilities are generally patched as they are discovered. In addition, Android has gone through several iterations and with each release of the OS, security has been

tightened. The RAM on a phone works much like their PC counterpart. While modern phones are removing it, some phones are equipped with external storage slot. Such storage cards are easy to capture.

Required Tools

- USB C / Micro USB wire
- DD
- NC
- Busybox
- Android SDK
- Manufacturer driver

Capturing Data for Analysis

An actual law enforcement forensic case will involve several steps such as:
Intake > Identification > Preparation > Isolation > Processing > Verification > Reporting > Presentation > Archiving [2].

In this scenario, we will use a very simple use case of capturing a rooted Android device image. Depending on the model, one needs to have a micro usb or USB C type cable. Additionally, one must also have necessary software such as device drivers, Android Studio kit installed on the system. Most Android devices will be recognized but some might require additional software drivers' specific to manufacturer.

For a rooted (*where privileges can be elevated as needed*) and "busybox" installed device, after enabling debugging in Android settings, one can connect the cable and open command prompt on Windows or Terminal on Linux, then run this command:
adb shell //starts the a session on the mobile device
cat /proc/partitions //lists partitions, we care about the swap and the entire mmcblk0 device

On the host PC, we need to setup a way to receive incoming data from the device. To accomplish this, we setup a tcp transfer on port 8888 with this command:
adb forward tcp:8888 tcp:8888
We now use dd to start transferring images:
dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888
Additionally, we need to define a save location:
nc 127.0.0.1 8888 > device_image.dd
This will store captured image, which can then be further analyzed with tools such as Autopsy, EnCase etc.

Challenges

This is just one of several ways images can be captured from a rooted mobile system. The keyword here is "rooted". Generally an Android device is NOT rooted, meaning privileges can't be elevated. One must exploit some vulnerabilities to weaken system security and gain root privilege. Often, rooted devices void warranty, fails to receive over-the-air updates. While older versions of Android can be rooted without too much effort, newer versions of Android are bit more challenging to root.

Even if the device in question runs a vulnerable version of android that can be potentially rooted, the rooting process itself makes few changes on the OS. This puts the integrity or pureness of evidence into question because of rooting modification. One of the fundamental requirements of any forensic work is not to contaminate evidence. Here, we shouldn't be tampering with evidence for convenience.

In such cases, we must look for alternative methods to extract and capture data/image without any modification on file system. We have to look at commercial offerings. Generally these kinds of specialized forensic tool are out of scope of average consumers due to few factors – price, availability. Due to sensitivity, there may be restrictions in selling to general public. Therefore such tools may be offered to authorized officials or governing bodies. For instance - Mobil Edit, Device Seizure, Cellebrite offer specialized forensic tools. Other tools include:

	CDMA	GSM	iDen	SIM	Logical Dump	Physical Dump
BitPim	X				X	
Data Pilot Secure View 3	X	X				
Paraben Device Seizure	X	X	X	X	X	X
SIMCon				X		
Iden Media Manager			X			
Manufacturer / Other	X	X	X	X		
Cellebrite	X	X	X	X	X	X
CellDEK	X	X	X	X	X	X
Oxygen Forensic Suite	X	X		X	X	X
XRY / XACT	X	X	X	X	X	X

Table 1: Cellular phone tool matrix [3].

Few other factors can determine which approach to take including the chosen method of acquisition. Sometimes manual may be acceptable, then logical but for stringent requirement, we may need to perform a full physical acquisition.

As mentioned, devices today are much more secured in general. For instance, most devices have biometric protection these days. Once we've gone past the typical lock screen, image capturing may become more problematic especially if the device is encrypted. Some screen locked devices are set to erase themselves after several attempts of incorrect password or PIN. We must remember that fact, otherwise we run the risk of erasing crucial evidence. While rooting a device will make forensic work a lot easier, it does require permission from court. The other challenge is that rooting method may not be available for that specific device.

Artifacts, what to look for?

In addition to captured image, what else is interesting? The SIM card can potentially contain contacts, some messages. There are SIM card readers that can extract this kind of information without too much efforts. Some modern phones are using embedded SIM, meaning it can't be physically separated. When examining retrieved photos, we should look at metadata, GPS tags. These can reveal interesting information which can then be correlated with other artifacts. GPS data can be highly useful in determining location of a device at a crime scene. However, it doesn't conclusively prove that the owner was present, it merely indicates the device was there. Savvy criminals can also tamper with GPS related settings to confuse device sensors and fill with inaccurate location data. Hard artifacts include device SN (often IMEI number), SIM card number, make and model number.

Assuming we have access to the device, we can now investigate what cloud accounts have been setup, what's being uploaded, and where. In other words, presence of apps such as box, onedrive, indicates content is being uploaded [4].

Recommendation

While this example outlines the process of creating an image for a rooted device, if we were to perform an actual forensic investigation, we have to exercise caution. We have to create a chain of custody document, evidence list. The device itself must be secured in a Faraday cage. Also the forensic workstation or laptop must be properly configured and secured. This station should be isolated and disconnected from networks of any kind. The objective is to protect integrity of all devices. Recovered files/content must be documented with hash values. We must remember, a cell phone is an electronic device. Therefore temperature, humidity, low battery can all affect the device. In terms of acquisition, if physical is not possible, one should explore logical data acquisition because it too can reveal very valuable artifacts such as – SMS, call history, application data, media, system logs etc.

References

1. Doherty Eamon P (2013) The Cell Phone. Digital Forensics for Handheld Devices. CRC Press, pp: 332.
2. Murphy Cynthia A (2009) Developing Process for Mobile Device Forensics, pp: 1-9.
3. Kessler G (2010) Cell Phone Analysis: Technology, Tools, and Processes.
4. (2014) Live imagining an Android device. Free Android Forensics.