Complexities and Evolutions in Forensic Analysis of Mobile Applications

Tiago Daniel dos Santos Martins [0000-0002-4308-9821]

University Lusófona of Porto, 4000-098 Porto, Portugal
tiagomartins98@gmail.com

Abstract: Smartphones have become a standard in modern times, almost everyone has one, and some even require one to do their work. These devices have much personal information on them. They can have anything from our text messages, call records, bank logins, and any other accounts that we use, be it from a social network or otherwise. In recent years, as technology evolved, we started noticing a rise in privacy concerns and security features. As a result, mobile application forensics has become increasingly complex, and the trend shows no slowing down in sight. The implementation of encryption on storage or communications, more strict permission systems, and protected system partitions makes the forensic process more complicated and time-consuming. Forensics is a vital part of law enforcement work because, many times, it is necessary to analyze the device of a suspected criminal as part of the investigation. The purpose of this paper is to evaluate how mobile application forensics has evolved and what complexities can arise from the process. Firstly, we will review the steps of examining a device, what methods the analysts use, and each one's advantages and disadvantages. Finally, we will evaluate how this process has changed, what complications have emerged from security measures implemented by device manufactures or users, and what strategies were created by analysts to overcome these problems.

Keywords: Smartphones, Mobile Applications, Forensic Analysis, Technical Complexities, Forensic Techniques Evolution.

1 Introduction

Mobile forensics, a digital forensics branch, is defined as the science of recovering digital evidence from mobile phones under forensically sound conditions using accepted methods [1].

10.11228/dpsc.03.01.008

Table 1. Number Of Smartphone & Mobile Phone Users Worldwide (Billions) [2]

Year	Number of smartphones	Number of mobile phones
2019	3.2	4.7
2018	2.9	4.6
2017	2.7	4.4
2016	2.5	4.3

As we can see in the table above (Table 1), there are many phones globally, but we also use them for everything. They became our preferred way of digital communication [3]. We make calls, send text messages or instant messages, take pictures, record video or audio, read email, browse the news, login into our bank, the list goes on forever. When dealing with smartphones, besides de data on the device itself, it is almost sure that we might leverage some credentials to access further information stored in the cloud, like social media or email accounts. Maybe cloud storage was syncing with the device [4].

This data can usually be recovered and analyzed to redact a report, summarizing the recovered information more comfortable to read and accessible format [1]. The recovered data is crucial for law enforcement, as it can be useful in an ongoing investigation or as evidence in a court of law. As with other forensics procedures, specific guidelines and conditions must be fulfilled for the data to be considered valid evidence [1],[5].

Previously, obtaining the device's data was easy. The first generations of mobile phones had practically no security measures, and permission systems were lax. Nowadays, it is a whole different story [6]. Nowadays, device manufactures have implemented file-based encryption [7], sometimes even full disk encryption [8], more restrictive permissions [9], complex password requirements, fingerprint readers, and many more security and privacy-related features. There is also a plethora of new applications for communication with enhanced security features, as opposed to the classic text message or phone call [10],[11],[12].

To better understand how mobile forensics works and how it evolved to overcome new problems, we will examine the procedures involved in smartphone forensic analysis. We will talk about the necessary steps, the different methods available, and the guidelines to ensure that our data is valid. After we understand how it all works, we will review what complications have appeared in recent years, how they affect the forensics process, and what solutions have analyst came up with to overcome them.

2 The Forensic Analysis of Smartphones

2.1 Device Seizure

There is a crucial moment in smartphone forensics before the device even reaches the lab. When the court issues a warrant, law enforcement detains the suspect and immediately confiscates any electronic devices called a seizure [13]. The devices are physically seized and isolated from any radio signal, mainly if found in an on-state during a raid [4].

10.11228/dpsc.03.01.008

The objective of isolation is to preserve as much evidence as possible from the device. We accomplish it by blocking network access to prevent network-related anti-forensics countermeasures implemented by the suspect [1] or any data from being overwritten [14]. There are a variety of isolation methods, but these three are the most popular ones:

- Enabling "Airplane Mode" – requires physically interacting with the device. Therefore, it is not always an option, and we also risk losing data or locking the device because of some security measures put in place by the owner [1].
- Turning off the device – will block it from connecting to any network, but there is a very high chance that it locks the device [1].
- Faraday containers – using these is the best option, as we are not required to interact with the device. They use a unique material that attenuates, not block, radio signals, but they deplete the battery faster [1].

These isolation measures are temporary, and now the seized devices must be taken to the lab, where there is a permanent isolation solution [14]. We are also required to keep the devices charged to prevent a lockdown [14].

2.2 The Forensic Analysis Process

When the devices arrive at the lab, we place them in permanent isolation. It can range from a little shielded container to an entire room [14]. The latter is preferred as it allows analysts to work freely.

We will now review the process of smartphone forensic analysis using the Harmonized Mobile Forensic Investigation Process Model [15], comprised of seven layers or phases:

1. Preparation.
2. Preservation.
3. Data Acquisition.
4. Examination.
5. Analysis.
6. Reporting.
7. Presentation.

10.11228/dpsc.03.01.008

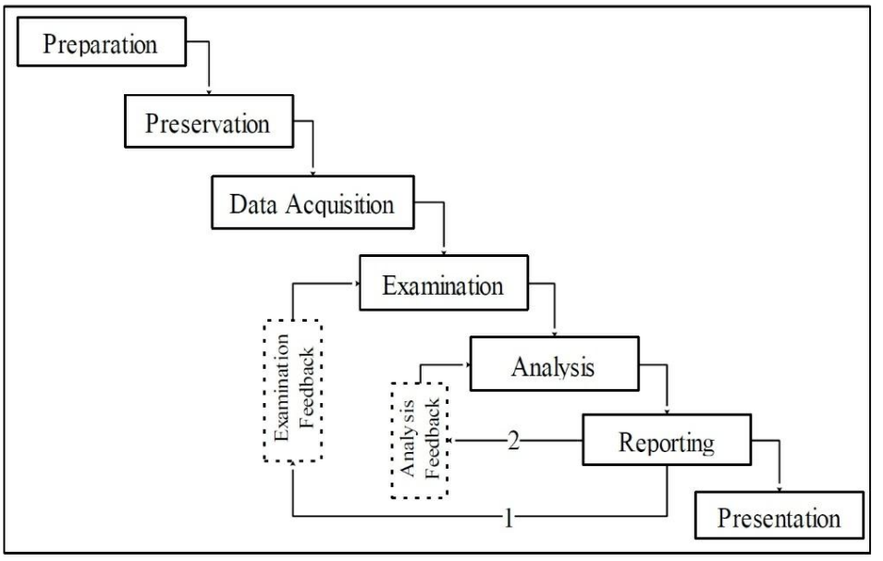

Fig. 1. Harmonized Mobile Forensic Investigation Process Model [15]

Preparation. This phase refers to creating a clean and isolated forensic environment to conduct the investigation. A clean environment is vital to guarantee that our evidence is not contaminated with evidence from another investigation, while the isolation is crucial to prevent any data loss. We also define what verified forensic techniques we will use and how the device will be isolated [1],[15].

Before we do anything to the device, we must first correctly identify it and catalog it. This way, we can avoid any mix-ups and choose which techniques and tools we use more efficiently.

Preservation. This phase refers to the process of preserving the integrity of the device and its data [15]. This phase is significant, as any tampering, be it accidentally or intentionally, can compromise the validity of the evidence on the device [1],[14].

We calculate the hashes[1] of all the files present on the device to later compare with those from extracted files, ensuring data integrity. We also take note of all the file timestamps for later comparison.

Data acquisition. This phase refers to acquiring, sometimes called extracting, the device's data, and any digital identifiers [15]. This phase is the most crucial in the whole process [14], and there are various techniques and tools available to analysts.

It is also vital to ensure a tool is compatible with the device and has a consistent output, and we do this by using it on another device of the same make and model [14]. The tool must block the operating system from updating any file timestamps or any

[1] Bit string with fixed size calculated using one-way hashing algorithms

writing operation. Otherwise, we would compromise data integrity or overwrite some crucial information, invalidating the evidence.

Examination. This phase refers to examining the acquired data to ensure its authenticity and not being tampered with in any way [15]. We compare file hashes and timestamps with the previously calculated ones to guarantee that any tampering has occurred and that file integrity remains unviolated.

Analysis. This phase refers to analyzing the examined data from the previous phase. We usually use special forensic tools to reconstruct the device's activities and recover who, when, and where these activities happened.

In modern devices running Android or iOS, this usually means sifting through many SQLite databases [14], [15]. These are the preferred method to store application data, including system ones like messages, calls, and contacts, which nowadays run on top of applications. Even though databases can have many lines, they have the advantage of providing access to deleted data sometimes.

Other file types such as images, videos, and documents may be significant for investigations and serve as direct evidence in court, but log files more often than not represent a treasure chest of past activities [4],[16]. These log files can include user authentication events, permission changes, unique identifiers generated by applications, application usage telemetry, geolocation information, network activity, deleted file names, and many other useful data. The best thing about log files is that everything has a timestamp.

The forensic tools are a huge help in sorting, filtering, and searching through all this data, sometimes even alert analysts of any interesting information.

Reporting. This phase refers to documenting or reporting all investigation steps [1],[15]. This phase has two feedback processes: the examination feedback and the analysis feedback [15].

In the examination feedback, we re-integrate and re-evaluate the information to revise any discrepancies or update the examination process [15]. In the analysis feedback, we re-analyze the information outputted from the examination feedback [15].

If we find any discrepancy in any of these feedback processes, we must repeat the process chain from the point we returned to [15], as shown in the flowchart represented in figure 1.

Presentation. This phase refers to the process of presenting our findings to law enforcement. As previously stated, these findings can be used as evidence in a court of law or to help in an ongoing investigation [1],[15]. This phase is the final one in a forensic investigation.

10.11228/dpsc.03.01.008

2.3 Data Acquisition Techniques and Tools

The data acquisition phase is the most critical part of the forensic analysis process [14]. We will examine what techniques are available to analysts and what tools they can use in each one.

The first technique is the simplest one, but it is usually only used when there is a need to access any stored information immediately. It is called manual acquisition, and this technique involves physically interacting with the device like in a standard operation scenario [17],[18].

The second one is called logical acquisition, a technique that involves making a bit-by-bit copy of the device's logical stored objects [17]. This technique is also the most used when performing forensic investigations, but it has some limitations [18]. Unfortunately, we cannot access deleted data, bypass security locks, or recover any information from damaged devices [18]. As for the tools available to conduct a logical acquisition, there are many options, but we will give only a few examples, as other products in the market do the same thing:

- ADB[2] – This tool can be used with the Android operating system and only if we can enable USB debugging on the device. Another problem is that we have limited access to the device's data, like not accessing applications that use restful encryption, meaning that the application stored data is encrypted [17].
- Backup analysis tools – There are third party tools out there capable of creating an image of the device in an external location that we can later open and analyze [17].
- AFLogical – This is a free tool available on GitHub to extract data on content providers, like SMS/MMS, call logs, contacts, or calendar [17].
- Commercial tools – There are many commercial tools by companies like Cellebrite, MOBILedit, viaForensic, MSAB, and many more [17]. Because these tools follow the same principles as the free ones, they suffer from the same caveats. The advantage of these tools is that they automate most of the process, are updated more frequently, and present the retrieved information in a much more organized manner.

The third technique at the disposal of analysts is the physical acquisition, and with it, we can make a bit-by-bit copy of the whole device, including system partitions [15]. With this technique, we can bypass security locks, recover from damaged devices, or even access deleted data since the operating system does not erase it but instead marks it as available space for overwriting [17]. As with the previous technique, this one presents a limitation, and that is the requirement to have admin or root privileges on the device [17]. For this technique, analysts can use hardware-based methods or software-based methods, in contrast to the previous technique where only software-based methods are available [17]. The methods and tools we can use for physical acquisition are:

- JTAG – This is a hardware method that relies on specifications for PCB[3] testing and debugging developed by the Joint Test Action Group. With this method, we can create images of the device's chips and retrieve their content [17].

[2] Android Debug Bridge
[3] Printed Circuit Board

10.11228/dpsc.03.01.008

- Chip-off – This is a hardware method that involves removing NAND[4] chips and resoldering them into another device, but this method can easily damage the chip's connectors [17]. This method is useful when extracting data of a damaged device or to bypass security locks [18].
- Software acquisition – There are multiple applications on the market to make a physical acquisition through software, both free and paid. However, we must root and enable USB debugging on Android devices or jailbreak iOS devices [17]. We can achieve this using exploits develop by security researchers, the same exploits people use for device customization or to run homebrew[5], and involves typically unlocking the bootloader and flashing a custom recovery or some other form of firmware exploiting [19]. The main difference between free and commercial products is that the paid solutions vendors often automate getting those admin privileges and displaying the retrieved information in a more organized manner.

3 Complications and Evolutions of the Smartphone Forensic Process

We will now talk about problems analysts face and solutions they come up with for those problems, some of which we have already mentioned in this paper. We will also be able to see the evolution of this process. Nowadays, both consumers and companies are more concerned with their privacy and security, so device manufacturers start incorporating more security measures [6]. It is important to note that these measures were implemented with security in mind, not to hinder forensic analysis purposely. The exploits used by forensic analysts are also available to hackers or any other threat actor for that matter.

The first complication worthy of mention is the implementation of security locks, as they effectively block the amount of data acquisition in most cases [17]. To overcome this problem, forensic analysts started exploiting privilege escalation vulnerabilities to perform physical acquisitions, thereby making a full copy of the device's memory and, consequently, bypassing the security lock [18].

In response to the bypasses mentioned above, some developers started making their security locks and encrypting the applications' stored data. However, as seen in recent news regarding Signal, forensic software vendors can sometimes bypass the encryption [20]. If this is possible, it can be because of poor coding of the encryption algorithm or improper storage of encryption keys, leading to possible brute-force attacks or key extraction.

To prevent privilege escalation by modifying the device's firmware, manufacturers started 006Cocking down partitions and making the user environment less permissive. One security measure was to lock the bootloader[6], preventing the overwriting of system

[4] Nonvolatile flash memory

[5] Software produced by hobbyists and amateur developers targeting proprietary hardware platforms

[6] Bootloader is a piece of code that runs before any operating system is running

10.11228/dpsc.03.01.008

partitions [21]. We must exploit the bootloader somehow to be unlocked [19], as the normal unlock procedure, even with an unlock code provided by the manufacturer, usually erases the device. After the bootloader is unlocked, it is required to flash a custom recovery, only after we can proceed with the physical acquisition [17]. Furthermore, it is worth mentioning that recently it was disclosed an iOS vulnerability at the hardware level, the now-famous checkm8 exploit [22]. A vulnerability of this severity means that any device with this specific hardware configuration and chip firmware can be exploited and is impossible to patch.

Following the same line of thought of application developers, device manufactures started implementing full disk encryption [8] or file-based encryption [7]. The use of encryption complicates things, even when using a physical acquisition technique, requiring further brute-forcing of the encryption keys.

As described in the section about device seizure, we can prevent security locks and device encryption if we seize them in an on-state [1]. By capturing a device while the user is using it, w can prevent it from being locked, and because it is operating normally, the data is currently unencrypted. Now that the device is in the authorities' hands, it is essential to keep it isolated from any network [1], and the battery charged [14].

The last complication we will talk about is anti-forensic countermeasures. To prevent any data from being overwritten or remotely erased, it is crucial to implement isolation measures on the seized devices [1] and to ensure that the battery never dies [14], basically the same solution described in the paragraph above and in the device seizure section.

4 Conclusion

In conclusion, we can see that smartphone forensics is a robust and well-defined process, but as with everything in science, still lacking some improvement and optimization. We learned how we conduct this process and how it has evolved, clearly seeing how increasingly complex it became for analysts. We also learned what complications we can encounter when performing a forensic investigation and what strategies analysts have created to overcome them, even though some problems still have no answer.

In summation, as with everything in the field of cybersecurity, smartphone forensics is a never-ending cat and mouse game. When someone discovers a new exploit, the manufacturer quickly comes up with a solution to prevent that exploit. It is up to the perfect coordination between law enforcement and forensic analysts to create new strategies and tools to solve these problems and keep the cyber world safe while not undermining everyday users' privacy.

References

1. Ayers, R., Jansen, W., Brothers, S.: Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). NIST Spec. Publ. 1, 85 (2014).
2. How Many People Have Smartphones Worldwide (Nov 2020), https://www.bankmycell.com/blog/how-many-phones-are-in-the-world, last accessed 2020/11/09.

3. Brunty, J.: Mobile device forensics: Threats, challenges, and future trends. In: Digital Forensics: Threatscape and Best Practices. pp. 69–84. Elsevier (2016).
4. Sharma, P., Arora, D., Sakthivel, T.: Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications. In: Procedia Computer Science. pp. 907–917. Elsevier B.V. (2020).
5. Ahmed, R., Dharaskar, R. V: Mobile Forensics : an Overview , Tools , Future trends and Challenges from Law Enforcement perspective. Online. 312–323 (2008).
6. Chernyshev, M., Zeadally, S., Baig, Z., Woodward, A.: Mobile Forensics: Advances, Challenges, and Research Opportunities. IEEE Secur. Priv. 15, 42–51 (2017).
7. File-Based Encryption | Android Open Source Project, https://source.android.com/security/encryption/file-based, last accessed 2020/11/11.
8. Encryption | Android Open Source Project, https://source.android.com/security/encryption, last accessed 2020/11/11.
9. Product Partitions | Android Open Source Project, https://source.android.com/devices/bootloader/partitions/product-partitions, last accessed 2020/11/14.
10. Google is rolling out end-to-end encryption for RCS in Android Messages beta - The Verge, https://www.theverge.com/2020/11/19/21574451/android-rcs-encryption-message-end-to-end-beta, last accessed 2020/11/20.
11. Signal becomes European Commission's messaging app of choice in security clampdown - The Verge, https://www.theverge.com/2020/2/24/21150918/european-commission-signal-encrypted-messaging, last accessed 2020/11/11.
12. Zoom Finally Has End-to-End Encryption. Here's How to Use It | WIRED, https://www.wired.com/story/how-to-enable-zoom-encryption/, last accessed 2020/11/18.
13. Manendra Sai, D., G K Prasad, N.R., Dekka, S.: The Forensic Process Analysis of Mobile Device. Int. J. Comput. Sci. Inf. Technol. 6, 4847–4850 (2015).
14. Raghav, S., Saxena, A.K.: Mobile forensics: Guidelines and challenges in data preservation and acquisition. In: SCOReD2009 - Proceedings of 2009 IEEE Student Conference on Research and Development. pp. 5–8 (2009).
15. Al-Dhaqm, A., Razak, S.A., Ikuesan, R.A., Kebande, V.R., Siddique, K.: A Review of Mobile Forensic Investigation Process Models. IEEE Access. 8, 173359–173375 (2020).
16. Sathe, S.C., Dongre, N.M.: Data acquisition techniques in mobile forensics. Proc. 2nd Int. Conf. Inven. Syst. Control. ICISC 2018. 280–286 (2018).
17. Alghafli, K.A., Jones, A., Martin, T.A.: Forensics data acquisition methods for mobile phones. 2012 Int. Conf. Internet Technol. Secur. Trans. ICITST 2012. 265–269 (2012).
18. Do, Q., Martini, B., Choo, K.K.R.: A cloud-focused mobile forensics methodology. IEEE Cloud Comput. 2, 60–65 (2015).
19. Signal App Crypto Cracked, Claims Cellebrite - Security Boulevard, https://securityboulevard.com/2020/12/signal-app-crypto-cracked-claims-cellebrite/, last accessed 2020/12/19.
20. Locking/Unlocking the Bootloader | Android Open Source Project, https://source.android.com/devices/bootloader/locking_unlocking, last accessed 2020/12/19.
21. Yu, M., Zhuge, J., Cao, M., Shi, Z., Jiang, L.: A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. Futur. Internet. 12, 1–23 (2020).