Mobile Forensics Data Acquisition

Asmae El Majdoub[1]*, *Chaimae* Saadi[2], and *Habiba* CHAOUI[1]

[1]System Engineering Laboratory, ADSI team, National School of Applied Sciences, IBN TOFAIL University Kenitra, Morocco
[2] Laboratory of Systems Analysis, Information Processing and Industrial Management, Higher School of Technology of Salé,Mohammed V University in Rabat, Morocco

Abstract. Mobile technology is among the fastest developing technologies that have changed the way we live our lives. And, with the increase of the need to protect our personal information, smartphone companies have developed multiple types of security protection measures on their devices which makes the forensic data acquisition for law enforcement purposes so much harder. As we all know, one of the biggest tasks in mobile forensics investigation is the step of data acquisition, it is the step of extracting all the valuable information that will help the investigators to bring out all the evidences. In this paper, we will explain the traditional forensic data acquisition methods and the impact of encryption and security protection that been implemented in new smartphones on these methods, we will also present some new mobile forensics methods that will help to bypass the security measures in new generation smartphones, and finally, we will propose a new data extraction model using artificial intelligence.

1 INTRODUCTION

Before, everything was quite simple, including mobile devices security; a week PIN, password or pattern were enough to lock your device. With these old security measures, it was very easy for law enforcements to break into mobile devices and collect all the evidences in a forensically sound manner. However, in the last few years, mobile companies have implemented a whole new generation of smartphones that have more security features due to the large amount of information users carry on their devices that needs protection. As a consequence, new mechanisms were designed to improve mobile devices security like the use of passcodes and biometric authentication, and also the incorporation of strong encryption mechanisms to protect the data [1]. All these security improvements present a huge challenge to law enforcement investigators, in view of the fact that data extraction becomes more harder than before. As a result, forensics experts and law enforcement agencies are trying to make every effort to implement new data extraction methods in order to keep up to date with this smartphones security trend.

The most well-known case when broken into a mobile device were a big challenge due to encryption methods was in 2015 when FBI wanted the famous mobile company "Apple" to create a software that would enable the FBI to unlock a the iPhone 5C that belongs to one of the shooters who killed 14 people and injured 22 in a terrorist attack in San Bernardino, California [2]. The iPhone was locked with a password and was set to eliminate all its data after ten failed password attempts; Apple refuses to create the software because they believed that creating a backdoor in their phones for the government would weaken security and could be used by malicious actors [3]. This case shows the world that security measures and encryption make the data extraction from new generation smartphone more complicated; consequently, modern techniques of data acquisition from encrypted devices become an obligation.

2 RELATED WORK

Data acquisition is the process of cloning and copying digital data evidence from mobile devices [4]. In literature, most of researchers focused on old school data acquisition methods which are now considered insufficient with all the security revolution in mobile devices.

In [5], Khawla Abdullah and Andrew Jones have reviewed some of the existing data acquisition methods; they mentioned the manual acquisition method where the investigator can use the phone keypad to extract all the data from the device, it is the simplest technique but it does not preserve the integrity of data and cannot bring out the deleted or the hidden files. Also, they reviewed the logical acquisition technique which can be done by connecting the mobile device to a computer using a cable or Bluetooth and extract all the data by using a software or command line. Then, they have mentioned the physical acquisition, it is defined ad copying the entire physical memory locations of the phone memory chip. Last, they talked about the chip-off method which can be done by getting an image of the internal non-

* Corresponding author: asmae.elmajdoub@uit.ac.ma

volatile memory. Finally, they finished by dividing the data acquisition methods into four levels from the simplest to the complicated and expensive one: manual acquisition, logical acquisition, physical acquisition and chip-off technique.

In [6], the authors provide a comparative analysis between logical and physical data acquisition techniques; they come to an end that the logical acquisition is somehow better because it's easier to use a software to retrieve data from a mobile device than using the physical methods which may cause certain modification to the device.

While the authors in [7] present a very detailed acquisition diagram which contains three cases of mobile forensics:

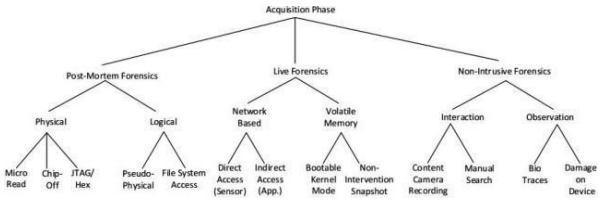

Fig. 1. Detailed acquisition phase

- Post-mortem forensics: known as dead forensics, it can be done on damaged, destroyed or powered-off device, all we need is a copy of the device memory.
  In this situation we use physical or logical extraction techniques.
- Live forensics: consists on gathering data from a running mobile device in the reel time, we can extract information such as process list, the kernel hash table and logs. The authors divided this technique into the network-based and volatile memory subcategories.
- The non-intrusive forensics: the authors describe it as the simplest retrieval method, it can be classified into observation and interaction techniques.

3 MOBILE FORENSICS METHODS

There exist many mobile data acquisition techniques, but first, let's start with the exiting or traditional methods:

3.1 Manual acquisition

The mobile forensic investigator can extract the device's data manually without any cables or platforms just by using the mobile touchscreen [8], this process of manual extraction is simple and applicable to almost every phone. However, the retrieved data using this method is limited and also the process is tedious and take too much time.

3.2 Logical acquisition

This method requires a connection between the mobile device and the forensic workstation. The investigator needs to copy the data to another device using either forensic tools or command line. Yet, logical acquisition often recovers data that actually exist on the mobile device and not the deleted data. [9]

3.3 Physical Acquisition

It is the act of capturing all the data on a physical piece of storage media. An exact copy is made, it is similar to cloning a hard drive. The advantage of this method is that it can capture all data that has been deleted (passwords, files, photos, videos...). The physical extraction leaves no evidence that an investigation was conducted once the extraction is complete. [10]

These old techniques unfortunately are no longer working with the new generation of smartphones that have more advanced security measures, therefor, new techniques have been implemented to bypass mobile devices security.

3.4 Cloud data extraction

Cloud data extraction: with the new smartphones, most information is stored in clouds including passwords, documents, photos, locations…

This method consists to extract the information directly from the cloud without having access to the physical device, it allows to get the reel time data of the suspect [11]. The main technical advantage of this method is that it is platform independent, that means we can have thousands of devices that the cloud can work for all of them. It also helps to bypass such problems as when the device has screen lock passcode and hardware-based encryption or enhanced encryption. [12]

However, the major problem is that in order to download the data from the cloud, the investigator needs the proper credentials, and even if he has them there is the two-factor authentication technique which is an extra layer of protection used to ensure the security of online accounts by using a third part device or a code received by SMS.

Nevertheless, there are several ways to bypass credentials and two-factor authentication by using some commercial forensics tools which have this ability; also, the experts can use phishing techniques, social engineering, brute force and session hijacking techniques [13] to get the code in a forensically sound manner.

3.5 File system extraction

As we all know modern smartphones use file system and all the data is stored in a non-volatile memory. In Android, we have the ext4 file system [14], while in apple devices we find the file system APFS [15]. File System Extraction provides direct access to all data contained in a device without the need for any application, therefore Forensic Tools can access all files contained within a device including database files, system files, and logs. [16]

3.6 Firmware update protocol

With a firmware update, the mobile device is updated with advanced operational instructions without requiring any hardware upgrade [17]. This method is proposed by the authors in [10], it consists on extraction data from the smartphone flash memory that contains user data. Flash memory can only be accessed directly through the firmware update protocol, so here the authors proposed a new way to acquire physical memory by analyzing the commands used in the firmware update process. They have performed four steps to extract data using this method:

- Analysis of firmware update processes and commands via decompiling the bootloader and updating the firmware [10].
- Enter firmware update mode
- Sync the device with the workstation.
- Read flash storage with commands.

3.7 Forensics software tools

There exist many forensics software suites that are available for smartphones and designed specifically for forensic purposes. Investigators must seize, collect, and decrypt evidence from a large number of devices while maintaining integrity. Mobile forensic tools solve these issues. Investigators can retrieve deleted information, analyze and preserve evidence using these specialized tools that may arise during an examination of criminal activity.[18]
Mobile forensics tools can be categorized in two groups:

Table 1. Mobile forensics tools [18]

Open-source tools	▪ MobilEdit: a phone and cloud extractor, data analyzer, and report generator all in one solution It can be used as the only tool in a lab or as an enhancement to other tools due to its data compatibility. ▪ Autopsy: is the first end-to-end open-source digital forensics platform. Built by Basis Technology with the core features you expect in commercial forensic tools. ▪ ibackup extractor: is an efficient application designed to help extracting the relevant information from the backups made to a smartphone.
Commercial tools	▪ Cellebrite UFED: gives you access to the widest range of mobile devices, applications, and public-domain social media platforms to produce meaningful insights quickly. ▪ Oxygen forensics detective: is a highly functional software tool used for digital forensic investigations of mobile devices and cloud data sources. It can be used to acquire data from devices, import backup and images, recover deleted data, etc.

4 SMART EXTRACTION

Despite all the exiting methods, forensics investigators may face many more challenges in the acquirement and analysis of mobile devices forensic data. Therefore, smart extraction using machine learning and AI algorithms is proposed by many researches.

Therefore, we propose a new model of data acquisition from mobile devices using artificial intelligence. Since all the old processes are time consuming when we talk about huge amount of data to extract and analyze. In this method, we will use the machine learning algorithms to train our framework using old cases that have been solved previously.

In the training phase, the framework must be able to detect all the files in a given disk image with their exact path in the file system, it also must have the ability to specify the extracted files type (image, video, text...etc.) using files extensions (.jpg/.png/.txt…etc.). Hence, in the reel data acquisition our framework will be used to these types of cases, so it will be able to extract reel data from the given evidence. Finally, we have to check the extracted data integrity to make sure that we have acquired the right data; to solve this issue, we propose using hash functions to grant the integrity of the full image as well as the extracted files.

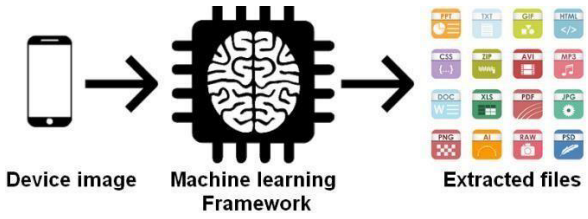

Fig. 2. smart extraction illustration

As we can see in the illustration schema in fig. 2, we enter a device disk image through our proposed machine learning framework so it can give us the extracted files with different types with their exact path.

5 CONCLUSION

Data extraction is the most important phase in mobile forensics, it's where we can acquire all the evidence from a mobile device. Available acquisition methods have many challenges like the security measures and the huge amount of data. Therefore, in this paper, we proposed a new data acquisition model using machine learning and based of solved similar cases, which helps us reduce data extraction time and extract more files than the other extraction methods.

References

1. M. Zinkus, T. M. Jois and M. Green, "Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions," May 27, 2021.
2. https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute, "wikipedia," 2015. [Online].
3. https://www.adn.com/nation-world/2021/04/14/to-unlock-a-terrorists-iphone-the-fbi-turned-to-an-obscure-company-in-australia/. [Online].
4. W. Jansen and R. Ayers, "Guidelines on Cell Phone," *Recommendations of the National Institute of Standards and Technology,* 2007.
5. S. C. Sathe and N. M. Dongre, "Data Acquisition Techniques in Mobile Forensics," in *International Conference on Inventive Systems and Control*, 2018.
6. K. Abdulla and A. Jones, "Forensics data acquisition methods for mobile phones,"in *The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)*, 2012.
7. K. Barmpatsalou, T. Cruz, E. Monteiro and . P. Simoes, "Current and Future Trends in Mobile Device Forensics: A Survey," vol. 51, no. 3, p. 1–31, May 2019.
8. A. Zareen and S. Baig, "Mobile Phone Forensics : Challenges, Analysis and Tools Classification," in *Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, CA, USA , 2010.
9. D. Hariyadi and T. Rochmadi, "Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software," in *IOP Conference Series Materials Science and Engineering* , 2020.
10. S. Jei Yang, J. H. Choi, K. B. Kim and T. Chang, "New acquisition method based on firmware update protocols for Android smartphones," *Digital Investigation,* pp. S68-S76, 9 August 2015.
11. "AcronisCyber Protect Cloud," [Online]. Available: https://www.acronis.com/en-gb/articles/two-factor-authentication/.
12. N. D. W. Cahyani, B. Martini and K.-K. R. Choo, "Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study," in *CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE*, 2016.
13. P. Sharma, D. Arora and T. Sakthivel , "Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications," *Procedia Computer Science,* vol. 167, pp. 907-917, 2020.
14. D. Kim and J. Park, "Forensic Analysis of Android Phone Using Ext4 File System Journal Log," 2012.
15. "Apple Platform Security," [Online]. Available: https://support.apple.com/guide/security/role-of-apple-file-system-seca6147599e/web.
16. A. Fukami, R. Stoykova and Z. Geradts, "A new model for forensic data extraction from encrypted mobile devices," September 2021.
17. R. SAVJANI, "einfochips," [Online]. Available: https://www.einfochips.com/blog/understanding-firmware-updates-the-whats-whys-and-hows/#:~:text=A%20firmware%20update%20will%20upgrade,while%20interacting%20with%20the%20device..
18. R. Lohiya, P. John and P. Shah, "Survey on Mobile Forensics," *International Journal of Computer Applications,* vol. 118, p. 0975 – 8887, 2015.
19. A. EL MAJDOUB, C. SAADI and H. C. CHAOUI, "Mobile Devices Forensics investigation," in *JASTI6*, Sale, 2021.