Mobile Device Forensics: Challenges and Best Practices in Evidence Extraction

Felix Monteiro
felix.monteiro@pt.ey.com

***Abstract*—The proliferation of mobile devices has led to increased cybercrimes involving these devices, making mobile forensics an essential aspect of digital forensics investigations. Mobile forensics involves acquiring, preserving, analyzing, and reporting digital evidence on mobile devices. However, this process is complicated by the ever-changing technology, the range of mobile devices and operating systems, and the diverse types of data and evidence that can be stored on these devices.**

Mobile devices are also exposed to various threats, such as malware, spyware, and ransomware, which can undermine their security and make it more challenging to extract evidence. This article provides an overview of mobile forensics, including the mobile forensics process, the threats to mobile devices, and the challenges digital forensics experts face when extracting evidence from these devices. By understanding these challenges and best practices in mobile forensics, digital forensics investigators can effectively extract evidence from mobile devices and enhance their investigation processes.

I. Introduction

With the widespread adoption of mobile devices, digital forensics experts face new challenges in investigating cybercrimes and extracting evidence from these devices. Mobile forensics has become crucial in digital forensics investigations, as smartphones and tablets store a wealth of personal and sensitive information.

The mobile forensics process involves acquiring, preserving, analysing, and reporting digital evidence found on mobile devices. However, the process is complicated by the ever-evolving technology, the variety of mobile devices and operating systems, and the different data types and evidence found on these devices. Moreover, mobile devices are increasingly becoming a target for cybercriminals, and the threats to mobile devices are constantly evolving. These threats can include malware, spyware, and ransomware, which can compromise the device's security and make it more challenging to extract evidence. This article aims to provide an overview of mobile forensics, including the mobile forensics process, the threats to mobile devices, and the challenges digital forensics experts face in extracting evidence from these devices. By understanding the challenges and best practices in mobile forensics, digital forensics investigators can better navigate this complex field and effectively extract evidence from mobile devices.

II. Mobile Forensics

Digital Forensics is the process of uncovering and analysing electronically stored data. This process aims to preserve pieces of evidence in their original form using a court-accepted methodology [1]. If properly collected, this data can prove or confirm past events.

Mobile forensics is a subtype of digital forensics that focuses on retrieving evidence from mobile devices such as smartphones and tablets.

Although computers are the standard example of personal digital storage nowadays, individuals rely more on mobile devices for sending, receiving, and searching data, making these devices the primary holders of significant evidence that investigators may utilise.

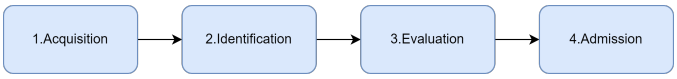

Fig. 1. Computer Forensic Investigation Process

The reasons for applying mobile forensics differ from context to context. In a military environment, mobile forensics gathers the intelligence necessary to plan military operations or stop dangerous attacks. From a business perspective, it might be necessary to conduct an investigation requiring mobile evidence to prove intellectual property theft. Through the eyes of a Law enforcement agent, mobile forensics presents the advantage of using digital data to discover evidence in all kinds of legal cases [2].

III. Mobile Forensics Process

A. Computer Forensic Investigation Process

The FBI created the first model destined to examine digital evidence in 1984, Computer Forensic Investigation Process (CFIP), presented in 1995 by M. M. Pollitt [3]. This model is composed of the following four phases:

1) **Acquisition** - Data acquired must answer three main questions: what can be sized (legally), from whom and from where. These questions should be answered taking into consideration the concerned authorities.
2) **Identification** - This phase can be divided into three subprocesses: defining the form of data, defining the data's logical position and placing the identified data (information) into its correct context (evidence).
3) **Evaluation** - This phase relates to the collected data's legal context. This phase aims to determine whether the collected data is relevant and can be used as legitimate evidence in the specific ongoing case.
4) **Admission** - the final phase consists of admitting the data as legal evidence and presenting it to the court of law. [4]

B. Intrusion Kill Chain

To perform a forensic analysis on any digital device, an investigator must be able to think like an attacker. This need was already acquired by the military forces when performing offensive operations. In any cyber attack, the objective is to move laterally inside the environment or violate a system's confidentiality, integrity, or availability.

A kill chain is a process first analysed by the U.S. military forces used to engage an adversary to create desired effects. In such a military context, the steps of this process were: to find

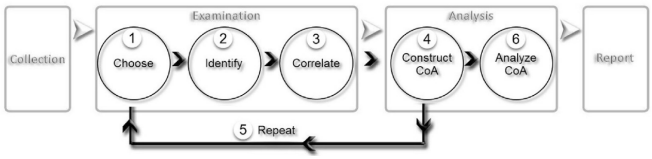

Fig. 2. D4I step-by-step instructing method [6]

the adversary, fix their location, track and observe, target with a suitable weapon, engage the target and assess the effects.

In cyber security and presented by Lockheed Martin [5], these kill chain models were adapted to serve computer network intrusions. The intrusion kill chain phases are:

1) **Reconnaissance** - Attackers usually scan the internet to find and gather information about their target. Resources are websites, email addresses, social relationships or information on specific technologies.
2) **Weaponization** - Building an attack deliverable. An exploit into a deliverable payload using automated tools, typically using client application data files such as PD or Microsoft Office documents.
3) **Delivery** - Transmission of the previously built weapon into the target environment, usually using email attachments, websites and USB removable media.
4) **Exploitation** - The intrusion code is triggered when the deliverable is located in the victim's host. These deliverables can target a vulnerable application or operating system or exploit the victim directly.
5) **Installation** - To maintain continued access inside the victim's environment, the attackers must install a remote access trojan or backdoor.
6) **Command and Control (C2)** - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. Advanced persistent threat malware provides full access inside the target environment.
7) **Actions on Objectives** - This is the final phase, and it is only now that the intruders can progress to achieve their initial objectives. Such objectives can be data exfiltration or violations of data integrity or availability.

C. D4I-Digital forensics framework

The D4I framework is a semi-automatic method for investigating cyber attacks, which can be used regardless of the attack's type, nature, or level of sophistication. This framework complements and improves existing digital forensics processes rather than replacing them.

Digital forensics examiners can use their preferred digital forensics processes alongside D4I during the examination and analysis phases.

The framework consists of two main pillars: a categorization of artefacts and their mapping to the intrusion kill chain; this way, digital forensics examiners are able to identify all of the traces/artifacts that the attack has left/created in each phase of the kill chain, and a step-by-step instruction method, as shown in Figure 2, for examination and analysis based on the previous categorization and mapping of the artefacts [6].

Each examination and analysis phase consists of the following six steps:

1) **Choose** - Choose a kill chain phase.
2) **Identify** - Identify all artefacts belonging to the specific kill chain phase based on the artefact categorisation.
3) **Correlate** - Find and match correlations between the artefacts of that kill chain phase with other kill chain phases.
4) **Construct Chain of correlated Artifacts (CoA)** - Document every correlation found and add it to a chain of correlations.
5) **Repeat** - Repeat the last four steps for all kill chain phases.
6) **Analyze CoA** - Finally, analyse the chain of correlated artefacts and conclude if it describes an attack. Remember that an attack should follow the phases of the kill chain.

D. Unified Security Framework

Since specific mobile device security measures often present problems in software integration, usability and administration, *NIST* has developed a unified security framework that addresses several mobile security aspects. The framework supports multiple policy contexts [7]. The managed security aspects are the following:

- **User Authentication** - In case a mobile device gets lost or stolen, the authentication of that device becomes the first line of defence. Multiple authentication modes are recommended(e.g. Face ID plus PIN code) to make the attacker work harder.
- **Content Encryption** - In case the first line of defence gets breached and the authentication method of the device is compromised, encryption plays a vital role in maintaining classified information secure.
- **Policy Controls** - When the two past measures fail, and the device is considered active, the scope of the attack is immense. Policy rules enforced in the various device programs can present a barrier for the attacker. These policies can be associated with higher access privileges and protect critical components from modification or unauthorized access.

IV. Challenges in Mobile Forensics

Even with all the presented frameworks, mobile forensics has unique challenges that investigators must consider.

A. Signals

Several policies can be implemented on a mobile device to destroy data; such policies can be implemented locally or remotely. After acquiring the digital mobile evidence, one must isolate the device and block every incoming and outgoing signals to ensure data is not remotely modified or destroyed. A standard method is using Radio Frequency, for example, a Faraday bag. A Faraday bag contains multiple metallic layers that block wireless signals. However, generally, examiners isolate a mobile device from network connectivity by placing the device in "aeroplane mode". Powering off the device to isolate it from the network can pose the risk of engaging authentication mechanisms or altering the device's current state by activating other security protocols that can make data inaccessible [8].

B. Cloud storage

Apple and Android phones require users to create a respective iCloud or Google account. These services backup the user's files and data to the provider's cloud servers. Because of these automatic services, the investigator should restrict direct interaction with the device unless in a controlled and prepared environment.

C. Equipment

Equipment used in forensics examination processes must be well considered by investigators. They must ensure the use of suitable versions of tools relating to the requirements of hardware, firmware, or software of the device. For example, data cables can differ from manufacturer to manufacturer. Removable media cards containing essential data should be extracted from the device before being examined [9]. An examiner should never insert an identity module or any card into the device with the risk of losing or altering data.

D. Operating systems

When analysing a mobile device, an investigator must identify and document its Operating system. There are two leading mobile operating systems: iOS and Android.

iOS is a mobile operating system created and developed by Apple. All mobile devices that use these operating systems employ hardware and software encryption. If the device has at least one authentication method (password/passcode/FaceID), the device's owner needs to supply the information required to gain access to the device; otherwise, the investigator may not be able to access the data. If the device is found, unlock the examiner that found it should take steps to prevent its locking [8].

Android is a Linux-based mobile operating system developed by Google. Unlike iOS, Android is offered on devices by different manufacturers and multiple companies. The Android device may or may not utilise hardware and software encryption. If the examiner encounters an authentication method, it must bypass it to access the data.

V. Mobile Forensics Tools

A. Oxygen Forensic Detective

Oxygen Forensic is an all-in-one forensic software platform built to extract, decode and analyze data from multiple digital sources: mobile and IoT devices, device backups, UICC and media cards, drones, and cloud services [10].

This study presents several functionalities of this tool essential for a forensics investigation. Oxygen Forensic has a built-in Cloud data recovery called the *Oxygen Forensic Cloud Extractor*, allowing data collection from Google, Microsoft, Apple, Dropbox, WhatsApp, Facebook, and IMAP accounts. It has built-in contact aggregation that identifies linked suspect profiles from all sources, including app accounts. The *Common Contacts* functionality displays the most frequently communicated with individuals between multiple device owners, allowing the investigator to determine the suspect the investigation should concentrate on. With the tool's file browser and timeline, it is possible to map images quickly and, most importantly, any geolocation containing app data. The built-in SQLite Viewer decodes and recovers deleted data from the primary database and associated write-ahead logs. It shows what time and day of the week the user was the most active allowing the investigator to conclude the most common manner the device is being utilized [11]. Overall a very updated and complete forensic software platform.

B. Cellebrite UFED

Cellebrite UFED is another mobile forensic software that allows examiners to extract, analyse, and report data from various mobile devices, including smartphones, tablets, and GPS units. It is widely regarded as one of the leading mobile forensic tools on the market and is used by law enforcement agencies, digital forensics experts, and other professionals worldwide.

One of the main strengths of Cellebrite UFED is its ability to support a wide range of mobile devices, including those running on iOS, Android, BlackBerry, and other operating systems. This allows examiners to collect data from various devices, even those that may be older or less commonly used.

Cellebrite UFED also offers a range of powerful features, including extracting logical and physical data from devices, recovering deleted data, and analysing information such as call logs, text messages, and social media activity. The software also includes various analysis tools, such as timeline analysis and keyword searching, to help examiners identify essential data and connections [12].

In terms of usability, Cellebrite UFED offers a user-friendly interface that allows examiners to quickly and easily navigate through the software and perform tasks such as device acquisition and data analysis. The software also includes various reporting options, allowing examiners to create customised reports that can be easily shared with other investigation team members or presented in court [13].

Overall, Cellebrite UFED is a powerful and versatile mobile forensic tool that offers a wide range of features and supports various mobile devices. While it may be more expensive than some other mobile forensic tools on the market, its reputation and track record make it a solid choice for professionals in the field.

C. MSAB's XRY

XRY is a mobile forensic software tool designed specifically for digital investigations involving mobile devices. The software is developed by MSAB, a company specialising in digital forensics solutions, and is widely used by law enforcement agencies, government organisations, and other professionals in the field.

The XRY software ensures the integrity of information by excluding all risks of tampering with evidence. The process is fully traceable so that the integrity of the evidence is assured. Most devices contain multiple storage resources and unique operating systems. The XRY software supports more than 10,000 different mobile devices, including smartphones, GPS navigation systems, 3G modems and tablets like the iPad. Through an intuitive interface, the XRY application provides a fast and efficient way to analyse mobile devices.

The XRY Logical package analyses and retrieves the current data from the device, screen by screen. The Physical XRY package founds deleted data by bypassing the operating system and retrieving all the device's raw decoded data. The XRY Complete package combines the last two packages, allowing the retrieval and analysis of all available data from a mobile device [14].

Overall, XRY is a powerful and reliable mobile forensic tool that offers a range of features and capabilities for digital investigations involving mobile devices. While it may be more expensive than other tools on the market, its comprehensive capabilities and reputation make it a solid choice for professionals in the field.

VI. Conclusion

Mobile devices are a rich source of digital evidence, and their prevalence in our daily lives has made mobile forensics an essential component of digital forensics investigations. However, the mobile forensics process presents unique challenges that digital forensics experts must overcome to extract reliable evidence from mobile devices.

As discussed in this article, these challenges include the rapid pace of technological change, the variety of mobile devices and operating systems, and the evolving threats to these devices. The complexity of the mobile forensics process also requires digital forensics experts to follow strict legal and ethical standards in evidence collection and analysis. To overcome these challenges, digital forensics experts must stay abreast of the latest technologies and best practices in mobile forensics. They must also collaborate with other experts, including law enforcement agencies, legal professionals, and software vendors, to develop effective strategies for extracting evidence from mobile devices.

In conclusion, mobile forensics is a required field in digital forensics investigations. By understanding the challenges and best practices in mobile forensics, digital forensics experts can effectively extract evidence from mobile devices and enhance their investigation processes.

References

[1] J. Eichbaum, "Five continual challenges with smartphone forensics," *MSAB*, 2019. [Online]. Available: https://www.msab.com/blog/five-continual-challenges-with-smartphone-forensics/

[2] "Mobile forensics – definition, uses, and principles," 2022. [Online]. Available: https://www.geeksforgeeks.org/mobile-forensics-definition-uses-and-principles/

[3] M. M. Pollitt, "Computer forensics: An approach to evidence in cyberspace," 1995.

[4] S. Tahiri, "Mobile forensics: Investigation process model," 2016. [Online]. Available: https://resources.infosecinstitute.com/topic/mobile-forensics-investigation-process-model/

[5] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Lockheed Martin Corporation*, Last accessed on 06 of March 2023. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[6] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4i - digital forensics framework for reviewing and investigating cyber attacks," *Elsevier*, 2019. [Online]. Available: https://www.nist.gov/publications/d4i-digital-forensics-framework-reviewing-and-investigating-cyber-attacks

[7] "Mobile devices unified security framework," 2016. [Online]. Available: https://csrc.nist.gov/Projects/Mobile-Security-and-Forensics/Mobile-Devices

[8] I. M. P. F. T. Sub-Group, "Guidelines for digital forensics first responders," *Interpol*, 2021.

[9] K. D. Lutes and R. P. Mislan, "Challenges in mobile phone forensics," *Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA)*, 2008.

[10] O. Forensic, "Oxygen forensic® detective," Last accessed 08 March 2023. [Online]. Available: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective

[11] F. Focus, "Oxygen forensic detective from oxygen forensics," 2016. [Online]. Available: https://www.forensicfocus.com/reviews/oxygen-forensic-detective-from-oxygen-forensics/

[12] R. Ammerman, "A basic review of mobile device data collection with cellebrite ufed," 2020. [Online]. Available: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective

[13] F. Focus, "Cellebrite's ufed cloud analyzer product review," 2016. [Online]. Available: https://www.forensicfocus.com/reviews/cellebrites-ufed-cloud-analyzer-product-review/

[14] E. C. Forensics, "Xry mobile forensic," Last accessed 08 March 2023. [Online]. Available: https://www.forensicfocus.com/reviews/xry-v9-3-from-msab/