Mobile Forensics: A comprehensive analysis

Natália Freitas[1]

[1] Lusófona University, Porto - Portugal
natyrf2000@gmail.com

Abstract. The objective of this paper is to analyze different attacks and techniques when it comes to digital forensic analysis. There are different threats, some with more associated dangers, which are described in depth throughout this work. The techniques detailed are compared with real-life practical cases. There are many people using popular messaging apps, which consequently comes with an increase in the number of attacks with this technology.
This in turn, increases the potential of certain data to be used in court, becoming important evidence, which creates the need for investigators to use specific mobile forensic techniques: however, this is not always possible due to numerous restrictions in the field. The paper is focused on these topics, based on the research of scientific papers. The conclusion is that this area of study has yet to grow, to become something with a larger impact, more commonly used.

Keywords: digital forensic, mobile, messaging apps, analysis, court evidence.

1 Introduction

Nowadays, our world is surrounded by technology, and this inevitably brings a new branch of studies and work on our everyday life. In this case, Forensic Science has the need to "evolve" into something else, so it can answer to different problems associated with technology. In brief, Forensic Science focuses on gathering and examining information about an event or crime. When it comes to analyzing digital information, this is known as digital forensics, and nowadays it applies to computers, mobile phones, tablets, or any electronic devices. So, Mobile Forensics is a branch of digital forensics, and consists of methods that describe how to take evidence from phones and how to analyze the information [1]. It can involve real-life implications or happen solely on the online ground.

Mobile devices aren't foolproof, and they can be exploited in different ways, even without tampering with them: their usage as it is can be malicious. They can hold photos, location access, or even just messaging apps, which can contain sensitive information, for example.

They can also propagate malware, to steal the sensitive information mentioned above.

These dangers and actual crimes bring up the need of using different forensic tools, which have several constrains that can difficult this work: hardware differences, security settings, and even the cost [2]

2

Starting with section 2, general attacks/threats on mobile devices are described, including how to prevent and detect them.

Next up, section 3 focuses on the proposed forensic model for mobile forensics, and section 4 compares the previously mentioned model with others that are used on the field.

Following this, section 5 presents a practical case, based on research on WhatsApp data extraction methods, and section 6 contains all the conclusions and reflections achieved after finishing this work.

Finally, section 7 includes all the references used throughout this paper.

b

2 Different Threats on Smart Devices

Mobile platforms are regularly attacked and targeted due to their security issues, and here are different types of threats that we can face when it comes to Smart Devices:

2.1 General Threats

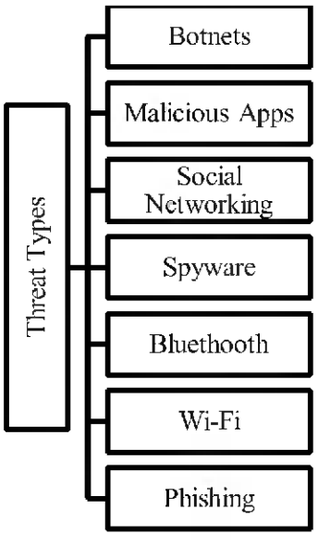

Fig. 1. Threat Types

Botnets:

.

They are networks that are formed by malware-compromised machines, usually used to conduct large-scale illegal activities. [3]

These are also called "zombie systems" and each zombie represents each individual connected computer. They can cause Denial of Service attacks or send spam, usually without the owner of the device noticing these actions.

Malicious Applications:
. Attackers can transfer malicious attacks with the form of apps usually seen as "ordinary", such as games, so the user downloads them, without knowing what the app really does on their device.

Social Networking:
. Social networks have made it easier for attackers to spread their malicious links, on which people click out of pure curiosity or are unable to identify that it's a malicious link.

Spyware:
. Spyware is malicious software with actions of different levels of maliciousness, and it attempts to monitor the behavior of users. The collected information is sent back, where it might be used for targeted ads, or marketing studies [4].
Moreover, the malware authors can see messages, hear calls, and track GPS information from the owner of the device.

Bluetooth:
. The Cabir worm is one of the first that propagated through Bluetooth, even though the users have their settings configured properly.

Wi-Fi:
. The attacker intercepts connections between Wi-Fi hotspots and smart devices, taking advantage of the latter.

Phishing:
. Phishing attacks usually target vulnerabilities that are present due to human factors [5].
Mobile phishers use vulnerable telephone connections, for example, through emails, SMS, or even MMS [6]

2.2 Preventive Measures

To mitigate malware and app abuse, there should some measures applied to each one of the threats.

Application Developers. They must make sure that the app is properly coded when it comes to security issues and include encryption on their services [6].

Smartphone User Level. To avoid certain situations, the user should be informed on these matters, at least on the surface. This gives the user the general sense to examine if the permissions requests are trustworthy or not when installing an app, for example. They should also have good security options on their device [6].

2.3 Malware Detection Techniques

These are generally classified into 3 types:

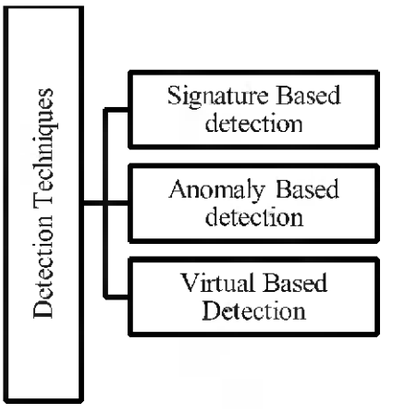

Fig. 2. Malware Detection Techniques

Intrusion detection and Prevention System (IDPS) has three main stages:

1. System details: network, application, OS behavior, etc.
2. Monitored data re-analyzed: allows the investigator to identify malicious occurrences.
3. Collect detected malicious data and initiate preventive measures, such as shutting down the devices or locking systems [6].

3 Proposed mobile forensics model

This model for mobile forensics is based on the most important phases for mobile forensics but there isn't a forensics model that is accepted or considered "correct", since different models can be applied to different situations.

3.1 Preparation:

This is the most important phase, as it allows the investigators to discover the nature of the case, and with this the team starts setting up their workstation. They also have a briefing on the situation, and they should be aware of different devices, their general hardware and software configurations of the ones involved. [7]

3.2 Handling Evidence & Securing the evidence:

This step is focused on making sure that the device found has the proper authorizations for the team to start investigating: if this isn't assured, there might be data losses. [1]

Accordingly, there are some important guidelines and challenges associated with this step:

Acquisition. Performing this at the scene avoids problems such as battery depletion, damage and more. First, it's determined if the device has been identified and next, if the device is on, there's only the need to bypass PIN/password [8].

There are various issues that can come up during acquisition:

- Selection of the Correct Acquisition Tool (experimenting with different tools to find out which one works best with certain devices is something recommended) [8][9]
- PIN/Password bypass (can be obtained from the service provider) [8] [9]

3.3 Documentation

This phase is connected to all the others since the investigators should document everything throughout the investigation and consequently, the documentation should include:

- Legal Authority letter
- Photographs and manual documents of digital evidence
- Information about the mobile device if obtained from owner
- Report of the findings
- Chain of Custody
- Formulated strategy for the investigation

3.4 Preservation

The phase of preservation aims to keep the evidence's integrity. Having in mind that we are dealing with electronic devices, it's important to know that humidity and other factors might have an adverse impact and therefore jeopardize the entire investigation, so there are some special arrangements to overcome these "challenges":

- Phone found in a liquid (battery should be removed, and the device should be sealed in an appropriate container) [8][9]

- Identification of Phone (the team should discover the type of device, operating system, and other attributes, to find out how to create a forensic copy of the contents of the device) [8][9]
- On-Off State Challenge (depending on the power state, there are different approaches) [8]

3.5 Examination and Analysis

The aim of this phase is to make the evidence visible: we might have a ton of information, but if it isn't properly arranged, it won't make much sense.

With this, the investigators analyze all the data to figure out which pieces can be used as evidence, and after determining what data is relevant, there is a data retrieval process.

Analysis is seen as technical review and recreating the crime scene is part of it. It allows for the investigators to basically do a timeframe analysis, since it might have a significant impact on the judgement.

As the final step, there is the making of a comprehensive report, which includes everything from the beginning to the end, with the results. [2][7]

3.6 Presentation

The court depends on this phase, and it consists of presenting the final report to the court of law. Nevertheless, if the report has any flaws when it comes to evidence, a culprit may be released, and the report itself might be challenged during its presentation, by the other side. In brief, the documentation must be solid at this time.

3.7 Review

This is the final phase, and it's dedicated to the investigators, as it allows them to improve their analytical skills. All the steps mentioned above are analyzed.

4 Comparison with other Models

The following table compares the model from above with others, specifically the phases that they include.

Table 1. Comparison of Proposed Model with others

Proposed Model	NIST Guidelines	DEFSOP	Model for Windows devices	HDFI model
Preparation	-	+	+	+
Handling Evidence & Securing the evidence	+	-	-	-
Data Acquisition	+	+	+	+
Documentation	+	-	+	+
Preservation	+	-	+	+
Examination and Analysis	+	+	+	+
Presentation	+	+	+	+
Review	-	-	+	-

This shows how there are different approaches (none of which are wrong) and they are applied to different situations. The proposed model has the advantage of including all the phases, which makes the investigations more concise.

5 Practical case with the usage of research tools

WhatsApp is one of the many existing messaging apps, and it has been equipped with an encryption feature [2]. There are many threats when it comes to the use of these apps, which were detailed before in this paper, so we can take a simple example: a pedophile can use this app to conduct his wrong-doings and even have incriminating conversations, and once he is pressed with charges, the investigators need to extract information from the app. This creates the need of using an extraction tool for WhatsApp.

5.1 Research Tools

(The hardware and software used to experiment on the extraction of WhatsApp Artifacts from an Android-based device can be seen in Table 2.) [2]

Table 2. Research tools and devices

No.	Tool and Device	Information
1	Samsung Galaxy S4 GT-19500	Smartphone used in the experiment
2	WhatsApp	Messaging App
3	Workstation with and operating system for Windows	Computer for extraction and analysis
4	USB Cable	Connects device and computer
5	Android Debugging Bridge	Software that supports communication
6	WhatsApp Key/DB Extractor	Extraction Tool
7	Belkasoft Evidence	Extraction and Analysis Tool
8	SQLite Studio	Analysis Tool

5.2 Results

When using the Belkasoft Evidence Software, the investigators can retrieve videos, images, and document artifacts. When it comes to the WhatsApp Key/DB extractor, the investigators only managed to retrieve text message artifacts and images, including information such as the message sender, message content, and time of sending or receiving the messages.

Both the extractions were repeated to ensure the results are similar and based on the results they have different strengths. WhatsApp Key/DB extractor dominates when it comes to retrieving text messages and the information associated with them, and Belkasoft Evidence excels in the extraction abilities for images, videos, and documents. [2]

Table 3. Forensic Tools Comparison

Artifact Type	Belkasoft Evidence	WhatsApp Key/DB Extractor
Text Message	-	+
Image	+	+
Video	+	-
Document	+	-

All this reinforces the idea that using different research tools is beneficial, since it allows us to obtain more concise and detailed evidence.

6 Conclusion

Technology became part of our life, and it's being used all the time: for the good and the bad. There are countless attacks that can be carried out, and technology only opens the possibilities.

People with malicious intent will always find new ways of getting their way, and Mobile Forensics aims to recover digital evidence to put an end to their antics. It might have similar processes to Digital Forensics, but it has its own peculiarities that are vital.

Subsequently, the need of having tools capable of extracting data or deleted data is also very real. A suspect in a trial might even delete the data in a phone that connects him with some sort of offense and being able to give evidence of his actions is important to have him prosecuted.

7 References

1. Lohiya, Ritika & John, Priya & Shah, Pooja. (2015). Survey on Mobile Forensics. International Journal of Computer Applications. 118. 6-11. 10.5120/20827-3476.
2. Umar, Rusydi & Riadi, Imam & Zamroni, Guntur. (2018). Mobile Forensic Tools Evaluation for Digital Crime Investigation. International Journal on Advanced Science, Engineering, and Information Technology. 8. 949-955. 10.18517/ijaseit.8.3.3591.
3. Silva, Sergio & Silva, Rodrigo & Pinto, Raquel & Salles, Ronaldo. (2013). Botnets: A survey. Computer Networks. 57. 378 403. 10.1016/j.comnet.2012.07.021.
4. Egele, Manuel & Kruegel, Christopher & Kirda, Engin & Yin, Heng & Song, Dawn. (2007). Dynamic Spyware Analysis.. 233-246.
5. Khonji, Mahmoud & Iraqi, Youssef & Jones, Andy. (2013). Phishing Detection: A Literature Survey. IEEE Communications Surveys &amp Tutorials. PP. 1-31. 10.1109/SURV.2013.032213.00009.
6. Duraisamy, Balaganesh & Chakrabarti, Amlan & Midhunchakkaravarthy, Divya. (2018). Smart Devices Threats, Vulnerabilities and Malware Detection Approaches: A Survey. European Journal of Engineering Research and Science. 3. 7. 10.24018/ejers.2018.3.2.302.
7. Sadiq M, Iqbal MS, Naveed K, Sajad M (2016) MOBILE DEVICES FORENSICS INVESTIGATION: PROCESS MODELS AND COMPARISON. ISJ Theoretical & Applied Science, 01 (33): 164-168.
8. Raghav, Shivankar & Saxena, Ashish. (2009). Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition. 5 - 8. 10.1109/SCORED.2009.5443431.
9. Ayers, R., Brothers, S. and Jansen, W. (2014), Guidelines on Mobile Device Forensics, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-101r1
10. "CWAGWEB – Best Practices for Seizing Eletronic Evidence" https://www.cwag-web.org/wp-content/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf, last access 15/12/2021
11. Dawson, Maurice & Wright, Jorja & Omar, Marwan. (2016). Mobile Devices: The Case for Cyber Security Hardened Systems. 10.4018/978-1-4666-8751-6.ch047.
12. Marturana, Fabio & Bertè, Rosamaria & Me, Gianluigi & Tacconi, Simone. (2011). A Quantitative Approach to Triaging in Mobile Forensics. 10.1109/TrustCom.2011.75.

10

13. Alhassan, John & Oguntoye, R. & Misra, Sanjay & Adewumi, Adewole & Maskeliunas, Rytis & Damasevicius, Robertas. (2018). Comparative Evaluation of Mobile Forensic Tools. 10.1007/978-3-319-73450-7_11.