"MOBILE FORENSICS DIFFERENT TOOLS AND TECHNIQUES"

[1]KU. ANJALI M. GAHALOD
Shree H.V.P. Mandal's, D. C. P. E an Autonomous College, P. G. Department of Computer Science And Technology, Amravati, India
anjaligahelod@gmail.com

[2]KU. SURUCHI M. TINKHEDE
Shree H.V.P. Mandal's, D. C. P. E an Autonomous College, P. G. Department of Computer Science And Technology, Amravati, India

[3]KU. RASIKA D. BAGAL
Shree H.V.P. Mandal's, D. C. P. E an Autonomous College, P. G. Department of Computer Science And Technology, Amravati, India
rasikabagalamt23@gmail.com

[4]KU. SHRADDHA R. KADODE
Shree H.V.P. Mandal's, D. C. P. E an Autonomous College, P. G. Department of Computer Science And Technology, Amravati, India
shraddhakadode76@gmail.com

[5]PROF. N. V. WANKHADE
Shree H.V.P. Mandal's, D. C. P. E an Autonomous College, P. G. Department of Computer Science And Technology, Amravati, India
nitinvwankhade@gmail.com

ABSTRACT: *Mobile forensics is a branch of digital forensics related to the recovery of digital evidence from mobile devices. Forensically sound is a term used extensively in the digital forensics community to qualify and justify the use of particular forensic technology or methodology. Mobile technology is among the fastest developing technologies that have changed the way we live our daily lives. Over the past few years, mobile devices have become the most popular form of communication around the world. However, bundled together with the good and advanced capabilities of the mobile technology, mobile devices can also be used to perform various activities that may be of malicious intent or criminal in nature. This makes mobile devices a valuable source of digital evidence. For this reason, the technological evolution of mobile devices has raised the need to develop standardized investigation process models and procedures within the field of digital forensics. Advances in semiconductor technologies related to mobile phones and the increase of computing power of mobile phones led to an increase of functionality of mobile phones while keeping the size of such devices small enough to fit in a pocket. This led mobile phones to become portable data carriers. This in turn increased the potential for data stored on mobile phone handsets to be used as evidence in civil or criminal cases. This paper examines the nature of some of the newer pieces of information that can become potential evidence on mobile phones. It also highlights some of the weaknesses of mobile forensic toolkits and procedures.*

***Keywords*:** Digital Forensics, Mobile Forensics, Anti-Forensics, Mobile Anti-Forensics Counter-Forensics, Android Forensics, Android anti-forensics, Android, Phone, Forensics.

1. INTRODUCTION

Mobile Forensics is a branch of Digital Forensics and it is about the acquisition and the analysis of mobile devices to recover digital evidences of investigative interest. When we talk about Mobile Forensics generally, we use the term "Forensically Sound", commonly used in the forensic community to define the application of methods and techniques, which respect the international guidelines for acquisition, and examination of mobile devices. The principles for the correct application of Forensically Sound techniques assume the primary purpose, which is the preservation and the possibility of non-contamination of the state of things. All the phases, from the acquisition to forensics analysis of the mobile device, have to totally avoid non-alteration of the examined device. This process is not easy at all, particularly in mobile devices. The continuous evolution of mobile devices technology, allows the commercialization of new mobile phones, which creates new digital investigations problems. Hardware and software for these type of mobile device analysis are numerous, but none is able to give an integrated solution for the acquisition and the forensic analysis of all Smartphone.

Furthermore, mobile devices are able to contain plenty of digital information, almost like a computer, so not only a call log or SMS messages as old mobile phones. Many of the digital information in a Smartphone is reliant on applications installed on it, which evolve in such a variety that analysis software are not able to support them completely. Often the data acquisition from a mobile device is not compatible with some parameters, which defines a Forensically Sound method. In other words to have access to the mobile device it is necessary to use communication vectors, boot loader and other agents which are installed in the memory to enable the communication between the mobile phone and the instrument that we use for the acquisition and so it I s not possible to use a write blocking option. Often we resort on modify the device configuration for acquisition, but this operation risks to invalidate the evidence in the Court, even though all the techniques are always well-documented.

As much as possible it is always fundamental to respect the international guidelines on mobile forensic to ensure the evidence integrity and the repeatability of the forensic process. A fundamental aspect on device preservation at the crime scene is evidence collection on site; that is the preservation of the device found turned on, safeguarding it from Wi-Fi signals, telecommunication systems, GPS signals and keeping the battery on charge. This is required to avoid its shutdown and the loss of important information such as a PIN.

Nowadays, mobile device use is as pervasive as it is helpful, especially in the context of digital forensics, because these small-sized machines amass huge quantities of data on a daily basis, which can be extracted to facilitate the investigation. Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions.

2. MOBILE FORENSICS

There are four steps of standard procedure including preservation, acquisition, analysis, and reporting according to NIST standard mobile forensic procedure. Besides, digital evidence requires four characters that are testability, acceptance, error rate, credibility, and clarity. Here is the explaining of preservation, acquisition, analysis, and reporting.

Preservation: Digital evidence is easily damaged by external factors, such as packaging, transportation, storage etc.; therefore, the evidence must be well-preserved to ensure its accuracy.

Acquisition: That acquired digital evidence by examiner from target mobile must be complete and analyzable and able to be presented by reporting.

Analysis: After forensic examiner receives the evidence result, analysis will be done in different way depending on the situation. The main purpose is to look for potential data connected to digital evidence to enhance the reality of evidence.

Reporting. Detailed conclusion will be presented in reporting including detailed acquisition procedure and result to reveal the original scene.

3. WHAT TOOLS & TECHNIQUES ARE COMMONLY USED IN MOBILE FORENSICS?

Forensic software tools are continually developing new techniques for the extraction of data from several cellular devices. The two most common techniques are physical and logical extraction. Physical extraction is done through JTAG or cable connection, whereas logical extraction occurs via Bluetooth, infrared, or cable connection. There are various types of tools available for mobile forensic purposes. They can be categorized as open source, commercial, and non-forensic tools. Both non-forensic and forensic tools frequently use the same techniques and protocols to interact with a mobile device.

3.1 Tools Classification System: Forensic analysts must understand the several types of forensic tools. The tools classification system offers a framework for forensic analysts to compare the acquisition techniques used by different forensic tools to capture data. Figure 1 shows the system:

Figure 1: Mobile Device Tool Classification System

3.2 Manual Extraction

The manual extraction technique allows investigators to extract and view data through the device's touch screen or keypad. At a later stage, this data is documented photographically. Furthermore, manual extraction is time-consuming and involves a great probability of human error. For example, the data may be accidentally deleted or modified during the examination.

3.3 Logical Extraction

In this technique, the investigators connect the cellular device to a forensic workstation or hardware via Bluetooth, Infrared, RJ-45 cable, or USB cable. The computer using a logical extraction tool sends a series of commands to

the mobile device. As a result, the required data is collected from the phone's memory and sent back to the forensic workstation for analysis purposes.

3.4 Hex Dump

A hex dup, also called physical extraction, extracts the raw image in binary format from the mobile device. The forensic specialist connects the device to a forensic workstation and pushes the boot-loader into the device, which instructs the device to dump its memory to the computer. This process is cost-effective and supplies more information to the investigators, including the recovery of phone's deleted files and unallocated space.

3.5 Chip-Off

The chip-off technique allows the examiners to extract data directly from the flash memory of the cellular device. They remove the phone's memory chip and create its binary image. This process is costly and requires an ample knowledge of hardware. Improper handling may cause physical damage to the chip and renders the data impossible to retrieve.

3.6 Micro Read

This process involves interpreting and viewing data on memory chips. The investigators use a high-powered electron microscope to analyze the physical gates on the chips and then convert the gate level into 1's and 0's to discover the resulting ASCII code. This process is expensive and time-consuming. Also, it requires an ample knowledge of hardware and file systems. There is no tool available for micro read The article Introduction to forensic analysis for mobile devices considers different aspects related to this subject, such as methodologies, phases of the process and the complications inherent therein. When carrying it out, bearing in mind first and foremost the phases of acquisition and analysis of the evidence, it is necessary to know a wide range of methods, techniques and tools as well as the criteria necessary for being able to evaluate the suitability of using one versus another. In this article we will address these issues.

Broadly speaking there are 3 different methods of extracting evidence: physical acquisition, logical acquisition and file system acquisition.

• Physical acquisition: this is commonly the most used method. It consists of making an identical replica of the original, thereby preserving all potential evidence. This procedure has the advantage of it being possible to search for deleted elements. Its main disadvantage is its complexity compared to the other methods and the time that it takes to carry it out.

• Logical acquisition: this consists in making a copy of the objects stored on the device. This makes use of the mechanisms implemented natively by the manufacturer, that is, those that are normally used to synchronize the terminal with a computer so that the desired information is requested from the mobile device's operating system. It has the advantage of being a much simpler process than the previous one, although it does not allow a great amount of information to be accessed.

• File system acquisition: this allows all visible files to be obtained through the file system, which does not include deleted files or hidden partitions. Depending on the type of investigation, it may be sufficient to use this method, which is less complex than physical acquisition.

3.7 Forensic Process

The forensics process for mobile devices broadly matches other branches of digital forensics; however, some particular concerns apply. Generally, the process can be broken down into three main categories: seizure, acquisition, and examination/analysis. Other aspects of the computer forensic process, such as intake, validation, documentation/reporting, and archiving still apply.

3.8 Seizure

Seizing mobile devices is covered by the same legal considerations as other digital media. Mobiles will often be recovered switched on; as the aim of seizure is to preserve evidence, the device will often be transported in the same state to avoid a shutdown, which would change files.[10] In addition, the investigator or first responder would risk user lock activation. Even so, there are two disadvantages to this method. First, it renders the device unusable, as its touch screen or keypad cannot be used. Second, a device's search for a network connection will drain its battery more quickly. While devices and their batteries can often be recharged, again, the investigator risks that the phone's user lock will have activated. Therefore, network isolation is advisable either through placing the device in Airplane Mode, or cloning its SIM card (a technique which can also be useful when the device is missing its SIM card entirely).

3.9 Acquisition

The second step in the forensic process is acquisition, in this case usually referring to retrieval of material from a device (as compared to the bit-copy imaging used in computer forensics).Due to the proprietary nature of mobiles it is often not possible to acquire data with it powered down; most mobile device acquisition is performed live. With more advanced Smartphone using advanced memory management, connecting it to a recharger and putting it into a faraday cage may not be good practice. The mobile device would recognize

the network disconnection and therefore it would change its status information that can trigger the memory manager to write data.

Most acquisition tools for mobile devices are commercial in nature and consist of a hardware and software component, often automated.

3.10 Examination and Analysis

As an increasing number of mobile devices use high-level file systems, similar to the file systems of computers, methods and tools can be taken over from hard disk forensics or only need slight changes.

Different software tools can extract the data from the memory image. One could use specialized and automated forensic software products or generic file viewers such as any hex editor to search for characteristics of file headers. The advantage of the hex editor is the deeper insight into the memory management, but working with a hex editor means a lot of handwork and file system as well as file header knowledge. In contrast, specialized forensic software simplifies the search and extracts the data but may not find everything.. Since there is no tool that extracts all possible information, it is advisable to use two or more tools for examination.

3.11 The Android Anti-Forensics Technique

In this section, the proposed technique is described. It makes it possible to modify and delete in a secure and selective way the digital evidence on a device with the Android OS, without using any cryptographic additions or low-level medications on the kernel. It is difficult to apply the anti-forensics techniques used for magnetic supports to NANDs flash memories. NANDs differ from hard drives in both the technology they use to store data as well as the algorithms they use to manage and access them. NANDs maintain a layer of indirection between the logical block addresses that computer systems use to access data and the raw flash addresses which identify physical storage. The layer of indirection enhances NAND performance and reliability by both hiding the idiosyncratic interface of the flash memory and managing its limited lifetime.

3.12 Anti-Forensic Tools

Anti-Forensic is a quite young and immature discipline even more if we consider the Mobile Environment (ME); regarding ME, a number of difficulties and issues during forensics analysis are still to overcome hence the possible shapes of AF techniques are continuously and rapidly evolving. Currently, there is no unique and standard definition of AF, while several definitions exist and focus on different and specific aspects. Among those, some focuses on breaking forensic tools or avoiding the detection of evidence while some others relate AF to system intrusions.

However, in accordance with, in this paper we consider AF to be any attempts to compromise the availability or usefulness of evidence in the forensic process. The availability of the evidence can be compromised by preventing its creation, hiding its existence and by manipulating the evidence as well; the usefulness can be compromised by deleting the evidence or by tampering its integrity. By the comprehension and the study of the AF techniques, a number of useful conclusions and guidelines can be drawn, in order to improve and harden the currently used forensic tools and techniques.

4. RELATED WORK

Forensics on mobile devices has become important that several researchers have worked on it such as [13], [14], [15], [16] and [19]. As for Smartphone's, the statistics of mobile operating system from December 2014 until February 2015showed that Android is the top mobile operating system followed by iOS and other mobile operating systems. The digital forensic community faces a constant challenge to stay abreast of the latest technologies that may be used to expose relevant clues in an investigation [9] and [10].Extracting data from smart phones is challenging. Unlike personal computers that have limited number of major operating system vendors, there are countless manufacturers of Smartphone's and mobile devices with their own proprietary technology and formats.

The way that Android manufacturers fragmented its operating system introduces difficult factor. On the Apple iOS, its security proving is so effective that bypassing the PIN is a challenge for digital forensics investigators [18].

5. CONCLUSION

Variety of conducted research on Android, and in general, mobile forensics, as well as undergoing standardization attempts indicate that the area is under continuous development. The work presented in this paper provided a comprehensive review of the state-of-the-art research in the field of Android forensics, as well as a classification of important Android anti-forensic techniques. Extraction of data, at least from iOS devices is a moving target, a mouse and cat game where the protection mechanisms are getting sufficiently strong, relying on a bit by bit dump is no longer practical. The same phenomena is seen on PCs and laptops with disk encryption enabled, with the major difference being that iOS devices have protection on by default.

6. REFERENCES

[1]. A. Simao A, F. Sicoli, L. Melo. F Deus, JR Sousa, "Acquisition and analysis of digital evidence in android Smart phones", International Journal of Forensic Computer Science, Vol. 6, No. 1, pp. 28–43, 2011.

[2]. Y. Lai, C. Yang, C. Lin, T. Ahn, "Design and implementation of mobile forensic tool for android smart

phone through cloud computing". In International Conference on Hybrid Information Technology, pp. 196-203. Springer Berlin Heidelberg, 2011.

[3]. A. Distefano, G. Mea, F. Pace, "Android ant forensics through a local paradigm", Digital Investigation 7, pp. S83-S94, 2010.

[4]. G. Kessler, "Anti-forensics and the digital investigator", In Proceedings of the 5th Australian digital forensics conference, December 2007.

[5]. https://eforensicsmag.com

[6]. https://link.springer.com

[7]. www.engpaper.com

[8]. https://pdfs.semanticsscholar.org

[9]. https://en.wikipedia.org

[10]. https://www.certsi.es
[11].https://www.forensicsmag.com
[12].https://resources.infosecinstitute.com

[13] Mubarak Al-Hadadi and Ali Al-Shidhani, Smartphone Forensics Analysis: A case study, International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.ISBN: 978-1-4673-8499-5©2015 IEEE 131

[14] Alexios Mylonas, Vasilis Meletiadis, Bill Tsoumas, Lilian Mitrou and Dimitris Gritzalis, "Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition.", a chapter in Information Security and Privacy Research, Vol 376, pp 249-260, Springer Berlin Heidelberg, 2012.

[15] Jeff Lessard, Gary C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations", Scale Digital Evidence Forensics Journal Vol.4, September 2010.

[16] Muhammad Faheem, N-A. Le-Khac, Tahar Kechadi, "Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool", Journal of Information Security, 2014.

[17]Jackson, W., Can digital forensics keep up with Smartphone Tech? Retrieved on 2 April from http://gcn.com/Articles/2014/06/16/forensics-technologyrace.

[18] Networkworld.com, 2015 "Getting Forensics data off Smartphone's and Tablets can be Tough", http://www.networkworld.com/article/2160656/smartphones/gettingforensics-Data-off-Smartphone's--tablets-can-be-tough--experts-say.html,Retrieve 12 March 2015

[19] Martin, A., "Mobile Device Forensic", SANS Forensics White paper, Retrieved on 10 April, 2015 from http://digitalforensics.sans.org/community/papers/gcfa/mobile-deviceforensics