Инженерный вестник Дона, №2 (2019)
ivdon.ru/ru/magazine/archive/n2y2019/5766

Mobile forensic tools and techniques: Android data security

A. Mentsiev, M.T. Alams

Chechen State University, Grozny

University of Jos, Nigeria

Abstract: Undoubtedly, today mobile phones have become an integral part of people's lives. Having set up access rights to our phone, we are sure about the safety of data, but also we need to know that data from smartphones can be obtained in full by digital forensic investigators. Even deleted data can be restored by the tools of these specialists. Digital forensic experts and investigators have a wide range of multifunctional and narrow-profile tools that allow you to "extract" digital data from almost any device. This article analyzes various types of mobile device memory on the Android platform, from which experts get data, tools and methods for obtaining information from mobile phones.
Keywords: android, digital forensics, database, computer security, Cellebrite, Oxygen.

Introduction

Android is an operating system for smartphones, tablets, e-books, digital players, game consoles, netbooks, smart books, Google glasses and other devices. It is based on the Linux kernel and has its own Java implementation from Google. It was originally developed by Android Inc., which was then bought by Google. Subsequently, Google launched an alliance Open Handset Alliance (OHA), which is now engaged in supporting and further development of the platform. Android allows you to create Java-based applications that control the device via Google-designed libraries. Android Native Development Kit lets import (but not debug) libraries and application components written in C and other languages.

85% out of sold smartphones, in the second quarter of 2014, was on Android operating system. [1]

As Android gained popularity, there also began to appear a lot of cases related to hacking into the system, data stealing and its modification. To prevent illegal activities, developers are creating tools to protect your data and restore it. Mainly, people engaged in this area are specially trained investigators who use special digital forensics tools, which help extract or recover some digital evidence.

Mobile forensics is another sort of acquisition digital evidence where the data is recovered from a mobile device. It depends on evidence extraction from the internal memory of a mobile device when there is the ability to get to information. Mobile device technologies are experiencing rapid development lately. There are various software tools available to recover and investigate mobile phone information. Each one has its set of advantages and disadvantages (limitations).

There are a lot of tools used in mobile forensics to expertise any mobile device. It should be emphasized that all of these tools are divided into two types. The first type is tools that have no relation to the type of mobile device. These tools are usually installed on your computer and deal with images of mobile devices involved in this investigation. [3]

This type of tools includes such well-known tools such as Cellebrite, Oxygen Forensics Suite, Mobile Phone Examiner Plus, Xry and so on. There are also tools that focus on a specific type of a mobile device, for example, for Apple products Lantern and Elcomsoft iOS Forensic Toolkit. [5]

The second type is tools directly mounted on the mobile device. These tools do not have the same options as the desktop application. They are inferior in functionality and are able to work only with certain resources. This is due to the fact that mobile devices still do not have sufficient performance characteristics to perform forensics analysis and investigations, but these applications are strong in certain areas. These include such applications as Data Recovery, SMS Backup and Restore and so on.

These apps and tools are vital for mobile forensic investigation to get digital evidence that could be later utilized as part of a legal case. [4, 7]

Different areas of forensics investigation using Android

Today, mobile devices have become an integral part of our lives. These small electronic devices are aware of their owner’s almost everything: location, meeting, photos, videos, bank details, messages, contacts and more. Besides, the mobile

devices include corporate information, information about other people and sensitive information. Loss of data can lead to bad consequences. That is why mobile forensics is so on demand today.

According to Hoog, 2011, there are three essential ways to approach forensics on an Android device. They are SD Card investigation, Logical and Physical acquisition. [2]

A primary objective in digital forensics is to keep out any changes of the target device by the inspector. On the other hand, mobile phones do not have usual hard drives which could be shutdown, connected with a forensics tool and then imaged in a forensically sound manner. Here the final result is that the forensics tool changes the Android device. Inspectors must utilize their caution when analyzing a mobile device and if the gadget is changed, the investigator must clarify how it was altered and why that decision was made. [5,6]

SD Card Analysis. Almost every Android gadget accompanies an external SD Card for keeping information. After getting and securing an Android gadget, an inspector ought to disconnect the SD Card and procedure it in the standard way. In this case, the card should be formatted with a Fat32 file system.

Logical Analysis. The logical analysis of an Android gadget is the strategy we suggested first. This system includes duplicating a little Android Forensics tool to the device, launching the tool, and afterward deleting it from the gadget. This kind of tools capture the following data: history logs of browser, call logs, external media, audio, and music, MMS, Contacts, SMS and more. [10]

Physical Analysis. Sometimes, a larger examination is needed in mobile forensics.

For this purpose, we have a method of physical acquisition, when an image of the full system is taken. This strategy obliges root benefits on the gadget and can yield a lot of data. [8,9]

This system will give a scientific image of the different client information segments. These segments utilize the open source framework Yaffs2 (Yet Another Flash File System 2) and is one of the huge difficulties with the Android platform.

Difference between Logical and Physical Analysis

Android forensic methods are either logical or physical. A logical strategy concentrates designated data and is normally attained by getting to the file system. Assigned data essentially implies that the information is not erased and it is accessible. One exemption to this definition is the thing that some files, for example, an SQLite database, could be designated furthermore still contain erased records in the database. While restoring the erased information obliges special tools and methods, it is conceivable to restore the erased information from a logical acquisition.

Physical systems, then again, focus on the physical stockpiling medium straightforwardly and do not depend on the record framework itself to get to the information. There are favorable circumstances to this approach; the most noteworthy one is that physical systems likely give access to huge measures of erased information. File systems frequently just check information as erased or outdated, and don't really delete the capacity medium unless required. Since the physical forensic strategies give immediate access to capacity medium, it is conceivable to recoup both the distributed and the unallocated (erased or old) information.

Obviously, the examination of an Android physical procurement is for the most part significantly more troublesome and tedious. Likewise, the physical procedures are harder to execute and stumbles could leave the gadget blocked off.

In Android forensics, the most widely recognized logical method does not by any means give immediate access to the file system and it truly works at a more unique and less powerful level than customary logical systems, which can get all non-erased information specifically from the file system. This method, which

depends on the Content Providers incorporated with the Android platform and SDK, is successful in creating some essential forensic data, however just a small amount of the information accessible on the framework.

In Android forensics, the most widely recognized logical method does not by any means give immediate access to the file system and it truly works at a more unique and less powerful level than customary logical systems, which can get all non-erased information specifically from the file system. This method, which depends on the Content Providers incorporated with the Android platform and SDK, is successful in creating some essential forensic data, however just a small amount of the information accessible on the framework.

References

1. Ahmed, Rizwan & Dharaskar, Rajiv. Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective. 2008. pp. 312-323.

2. Andrew Hoog. Investigation, Android Forensics. Analysis and Mobile Security for Google Android. 2011, pp. 195-284.

3. Himanshu Srivastava, Shashikala Tapaswi, "Logical acquisition and analysis of data from android mobile devices", Information & Computer Security, 2015. Vol. 23 Issue: 5, pp.450-475.

4. Lai Y., Yang C., Lin C., Ahn T. Design and Implementation of Mobile Forensic Tool for Android Smart Phone through Cloud Computing. In: Lee G., Howard D., Ślęzak D. (eds) Convergence and Hybrid Information Technology. ICHIT 2011. Communications in Computer and Information Science, vol 206. Springer, Berlin, Heidelberg. 2011. pp. 196-203.

5. Venkateswara Rao V. and Chakravarthy A. S. N. "Survey on Android Forensic Tools and Methodologies." International Journal of Computer Applications (0975 – 8887), Volume 154 – No.8, November 2016. pp. 17-21.

6. Magomedov I.A. Inženernyj vestnik Dona (Rus). 2018. №2. URL: ivdon.ru/en/magazine/archive/N2y2018/5009

7. Pritykin F.N., Nebritov V.I. Inženernyj vestnik Dona (Rus). 2016. №1. URL: ivdon.ru/en/magazine/archive/n1y2016/3506

8. McFarland, R. (2017). Introduction to Mobile Forensics - Android OS. [online] The Cyber Security Place. URL: thecybersecurityplace.com/introduction-mobile-forensics-android-os/ [Accessed 17 Mar. 2019].

9. Messmer E. (2012). Getting forensics data off smartphones, tablets can be tough, experts say. [online] Network World. URL: networkworld.com/article/2160656/getting-forensics-data-off-smartphones--tablets-can-be-tough--experts-say.html [Accessed 12 Mar. 2019].

10. Pub P. (2019). Mobile Forensics and Android Security. [online] AndroidPub. URL: android.jlelse.eu/mobile-forensics-and-android-security-c3d6aaceb2b [Accessed 12 Mar. 2019].