# Mobile Forensics

Taylor Bauer, Jason Delaney, and Michael Lee

COM-452-CA01

1 November 2018

Abstract

Nowadays, many mobile devices have become a valuable asset for people to use for their benefits. These same devices have also proved to be involved in many crimes and investigations. In mobile forensics, many tools and techniques help encrypt data and display proper evidence. Specifically, the operating system of a phone show to contain memory where many criminals try to gain access. If people are not careful, that data can be used to commit acts of terrorism or even invade private information that can harm innocent people.

# Mobile Forensics

Mobile forensics describes “the science behind recovering digital evidence from mobile phones” (Bommisetty 8). Cell phones and other mobile technology are considered to be reliable resources that changed the way that people communicate, think, and see the world from a different perspective. However, some criminals display their ruthless endeavors to gain access to critical data for their desires. With technology advancing, crime has turned to the world of mobile technology. Without precautions, this can lead to the misuse of technology that “can deliberately target civilians and non-combatants” (Cahyani 1). With the help of forensic investigators, they can access data by using the right tools, demonstrating their unique ways of seeking sufficient evidence. To see the world from a forensic specialist’s point of view, one must come to the understanding of the operating system of mobile devices, the possible acts that imply to crime and terrorism, and the proper uses of many mobile forensic tools.

The iOS is the primary operating system when it comes to any device that Apple makes. This operating system comes with two types of memory, volatile and non-volatile. Volatile memory deletes when the power disconnects from the device. RAM is an example of volatile memory. RAM is important because it is used to store critical parts of the operating system or application. RAM can contain usernames, passwords, and encryption keys. All of this information stored in the RAM is crucial to a lot of investigations, but there is currently no tool around to acquire RAM from an iPhone. NAND is an example of non-volatile memory, and it does not lose data every time the phone reboots. NAND flash is the main storage area and contains system files and user data. NAND memory is cheap and can hold a lot of data; this makes it ideal for mobile devices.

A type of data acquisition is called a physical acquisition. The goal of this is to perform a bit by bit copy of NAND memory. The physical acquisition has the highest success rate in recovering data from iOS devices. As time goes by security features are improving on iPhones, so it makes it harder to retrieve data through physical acquisition. At the moment there are two ways of doing this, and they are via a custom ramdisk and via jailbreaking.

The first method is physical acquisition via a custom ramdisk. The process involves getting access to the file system by loading a ramdisk into memory. Once loaded into the memory, physical acquisition exploits a weakness in the boot process while it is in DFU mode. This ramdisk will contain forensic tools that are needed to dump the file system over a USB. The good thing about using a ramdisk is that it will not alter data and none of the user data on the phone deletes. When an investigator sits down, they will load a custom ramdisk via USB to access the file system. The iPhone will try to stop this, but there is an exploit in the DFU.

The second method of data acquisition is via jailbreak. Jailbreak works when the device is not vulnerable to the DFU exploit. When an examiner jailbreaks an iPhone, they are looking to be able to install tools onto the phone that would not usually install. Most of the time when an iPhone encounters jailbreaking, it is done using redSn0w or evasi0n. During the jailbreaking process, changes made to the device cause a risk to data on the device. Jailbreaking is mostly a last resort after trying to exploit the system. While jailbreaking the device everything must be well documented so that all evidence will stand in court. It is also important to note that an iPhone that is protected by a passcode cannot encounter jailbreaking, which would make it impossible to perform physical acquisition on the device. The raw disk image file that is obtained while jailbreaking is encrypted. The only way to decrypt it is to receive the encryption

key in the device's UID key. Although many functions make the operating system unique, they can be lead in the wrong hands if not being too careful.

When discussing the crimes that are involved with mobile devices, many circumstances display too many problems. For instance, the idea behind cyberstalking is referred to "online harassment [where it escalates] into real-life stalking." Many types of victims get involved through phone calls, text messages, threatening emails, or even recorded videos. It is amazing how a majority of them do not feel the need to report it. The majority of the time, a cyber stalker's identity is usually concealed and will display fake names, identities. The most difficult problem of identifying a suspect is that it is "all-but-impossible to determine the true identity of the source" and it can often be very frustrating (Pattanari). A cyberstalker can remain anonymous, which gives an advantage. An unknown stalker can be anyone from former lovers or friends to teenagers that play jokes or strangers.

Many cybercriminals feel that they have the authority over others, which leads investigators for their demands to solve problems. Mobile phones continue to grow and become a part of society. Fortunately, this can lead to an open escalation of terrorist activities if people are not too careful. Terrorism is described as the act "of violence by groups or individuals pursuing political objectives" (Cahyani 240). According to the information and communications technologies (ICT), it can become linked to many technological resources and tools where information can be managed and used for manual manipulation. With the information that can be essential, there have been many methods that are used to keep the message from being revealed. Methods such as steganography are used to conceal important information "within digital objects, such as text, image or audio" (Cahyani 242). These kinds of methods lead to illegal communication and difficult clarification.

In many ways, there are many mobile phone crimes contain vast amounts of information that can be beneficial for many forensic investigators. Every mobile phone has their memory storage based on their operating system. When an investigator is working on a case, they pick up the nearest mobile device that may contain potential data needed to have substantial evidence. According to Paul Luehr, former federal prosecutor and supervisor, he stated that text messages are still in the data of phones. He clarified that to regain deleted messages, "you really need to have access to one or more physical devices." One phone may hold the data, but it might take more than one device to prove that there is some communication. John J. Carney explained that deleted text messages are "still in there, it's simply marked as 'erased'…it's possible to go in there and collect them" (Evans). Generally, cell phones will still contain data and will determine the right data by the right mobile investigator. Though forensic specialist can uncover data from mobile devices, it is vital for them to use the right tools to get what is required.

The Elcomsoft iOS Forensic Toolkit is a set of tools specifically designed to acquire forensic evidence off iOS devices. Although, depending on the iOS version the phone may need to be jailbroken. EFIT has an expansive list of abilities it can extract device secrets such as passwords and encryption keys, retrieve bit-for-bit pictures that are in the device file system, and lastly decrypt images. It also has an accountability feature built in which logs everything on the mobile device that works. The accountability feature is vital for forensic investigators since keep track of your actions is a necessity. Only a few years ago, these tools were only allowed to law enforcement; however, now the public can buy them.

The Oxygen Forensic Suite 2014 is a forensic tool that works with all mobile devices smartphones, PDA's, even tablets. Oxygen Forensic Suite 2014 is the most advanced when it comes to diversity; it supports more than 7,700 different types of software. The list of extraction

tools is jaw-dropping, it can extract data from the “phonebook with assigned photos, calendar events and notes, call logs, messages, camera snapshots, video and music, voicemails, passwords, dictionaries, geopositioning data, Wi-Fi points with passwords and coordinates, IP connections, locations, navigation applications, device data, factory installed and third-party applications” (Bommisetty, S., Tamma, R., & Mahalik, H., 2014). A major benefit is that this tool will automatically import all information to a database of your choosing. In this way, forensic investigators will have an entire database of evidence that makes management much more comfortable. The major downside to this tool is price, just one license to use this software costs as much as 3,000 dollars.

The Cellebrite UFED Physical Analyzer is a tool is only available to security organizations, anti-terrorism groups, and law enforcement. It can be useful for more than 5,320 different mobile devices. These devices include regular phones, smartphones, PDA’s, and any mobile tablet. Cellebrite UFED Physical Analyzer strives at physical and advanced logical acquisition, retrieving data through file system acquisition. UFED Physical Analyzer also can reveal important information such as disk images, keychain items, device passwords, and data from applications. Lastly, it can retrieve all the data from a system then dump it into another forensic tool that may be easier to examine data.

The Paraben iRecovery Stick is a very affordable piece of equipment, knowing it is a unique forensic tool. It is software that installs on to a USB drive, after plugging it into any iOS device you will be able to access the user’s data directly from either iTunes or from the device itself. The Paraben iRecovery Stick can only support the logical acquisition, which is why the method is so affordable. It “can recover data such as messages, contacts, call history, internet

history, and calendar events" (Bommisetty 154). With one hundred and twenty-nine dollars, this tool works on Windows.

Mobile forensics proved to be more than capable of finding evidence in many mobile devices and demonstrated proper techniques to of a threat when not dealt with appropriately. Many people in this world are not aware of the many possibilities that mobile devices can uphold other than memory. It is clear that technology today is something that cannot underestimate nor to be considered a minor problem. With potential cyber stalkers and criminals continuing to grow, the world of data has proven to become a more significant challenge. Fortunately, many forensic specialists will uncover data to ensure to find evidence with the right tools and information.

References

Bommisetty, S., Tamma, R., & Mahalik, H. (2014). *Practical Mobile Forensics*. Birmingham, UK: Packt Publishing. Retrieved from https://saintleo.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=816517&site=ehost-live&scope=site

Cahyani, N., Rahman, N., Glisson, W., & Choo, K.-K. (2017). The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Storage Service and Communication Apps. *Mobile Networks & Applications*, *22*(2), 240–254. https://doi-org.saintleo.idm.oclc.org/10.1007/s11036-016-0791-8

Evans, J. B. (2016, June 02). Cell Phone Forensics: Powerful Tools Wielded By Federal Investigators. Retrieved November 1, 2018, from https://news.law.fordham.edu/jcfl/2016/06/02/cell-phone-forensics-powerful-tools-wielded-by-federal-investigators/

Hoog, A., & McCash, J. (2011). *Android Forensics : Investigation, Analysis and Mobile Security for Google Android*. Waltham, MA: Syngress. Retrieved from https://saintleo.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=407913&site=ehost-live&scope=site

Pettanari, D. (n.d.). Cyberstalking investigation and prevention. Retrieved November 1, 2018, from http://www.crime-research.org/library/Cyberstalking.htm

Strozier, C., Ware, J. G., Crime and Justice News, & Justice News. (2015, April 02). Stalking by Cellphone. Retrieved November 1, 2018, from https://thecrimereport.org/2015/04/02/2015-04-stalking-by-cellphone/