# iPhone Forensics

Jaclyn Sottilaro

Monica Figueroa-Santos

Antonina Spinella

Saint Leo University

## Abstract

With an ever-growing evolution on technology, the use of smartphones is becoming increasingly common. But smartphones are still complicated from the forensic point-of-view. Various versions of operating systems exist in many devices, which leave smartphones looking very complicated. Every manufacturer has its own security algorithm and own terms and conditions when creating a mobile operating system. Every day encryption is becoming increasingly complex for forensic analyzers during investigations. iPhones and iPads are using iOS which cover Users Privacy and Security on the top level of their architecture. Investigating such devices can be extremely complicated because every single file on the device is encrypted. Cybercriminals use the latest technology to commit crimes, and cybercriminals are only increasing in the near future. This paper covers forensic-safe methods that can be achieved on iOS devices.

iPhone forensics is basically the knowledge of the hardware and software of the iOS device with the ability to extract and decipher data from an iPhone successfully. The iOS architecture plays a huge role between the applications that one can see from their phone screens to the hardware underneath. The applications communicate with the hardware through a "well-defined system interface that protects [the] applications from hardware changes" (Parmar & Sheth, 2018). This system interface is essential because it makes it easier to extract data. There are two different ways that data can be extracted from an iPhone, and that is either physically or logically. Logical extraction is the preferred method because physical extraction requires the iPhone to be jailbroken. Jailbroken iPhones can run software and perform many things that normal iPhones cannot, one can install apps and modify their iPhone in ways that is unauthorized by the creators of Apple, all of which is perfectly legal. A downfall to jailbroken iPhones is that they are not protected by the tough security protections applied by Apple. Logical extractions are performed using customized tools. These tools are Linux based and programmed using Python programming. Python is an "open source cross-platform framework [that] supports windows and Linux environment[s]" (Parmer & Sheth, 2018). These customized tools run on iOS devices without the need of jailbreaking by authorizing other software access the filesystem easily. These tools can also back up the device to make separate copies to work on in case of a forensic investigation. All the files extracted are SHA1 hash value of the original file. Not all tools have the capability of extracting data from iOS devices without the need for jailbreaking. "There is no question of integrity here" (Parmer & Sheth, 2018), coming from a forensic point of view all findings can be presented in a professional manner. Meaning all evidence should be valid as well as liable to be presented in a judicial proceeding.

The use of iPhones has grown more and more over the years. One would never realize, but these devices contain so much information that can be helpful in an investigation. Data on smartphones is highly volatile. One cannot just copy the contents of the memory because the data is encrypted, and the operating system of the phone restricts running any applications that have not been signed by Apple. With every releases of new phones or operating systems, many problems arise. This article discusses the design and implementation of digital forensic software for iPhones. It goes into depth on how to extract data and recover images while a cell phone is locked. It uses libimobiledevice to extract phone calls, text messages, photos, and a lot more information. “The increasing trend of safety and criminal issues has made the development of iPhone forensics become a must.” (Chen, Tso, Yang 2013).

iPhones have many different functions. From the internet, GPS, digital cameras, multi-media and it has a higher volume of storage space and diverse apps. So, one can say that a cell phone is a personal database. IOS is the operating system developed by Apple for smart devices. As illustrated in figure 1, the iOS is made up of four layers: The Cocoa Touch, the Media Layer, the Core Service, and the Core OS Layer. The system all together takes up about one GB memory stick volume. The Core OS is the bottom and is responsible for the foundation of the operating system which what the other layers sit on. It oversees managing memory, taking care of file system tasks, handling networking and other tasks. The core service contains the fundamental system services that all applications use. The media layer contains the graphics, audio, and video technologies. The Cocoa Touch layer, which is the top, contains the key frameworks for building iOS applications. That includes the basic application infrastructure and

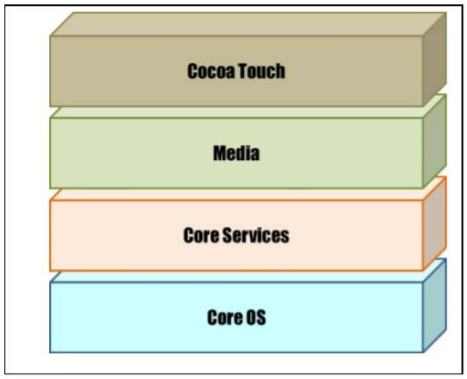


**Figure 1. iOS Layers**

support for key technologies such as multitasking, touch-based input, push notifications, and many high-level system services.

The data on iPhones is kept as an electronic record. Forensic personnel investigate the digital evidence, which is all the data extracted from mobile phones. This includes phone calls, phone logs, text messages, emails, media files, and GPS. Mobile forensics procedures are divided into four phases: Preservation, Acquisition, Examination and Analysis, and Reporting. Following these steps can help to recover digital evidence from a mobile device. Preservation is the first step; it is to ensure identify or search for possible existing digital evidence storage devices. Digital evidence must be kept in its original form, or else it will be unusable in court. Acquisition is the removal of digital data from digital devices through reading database files or images. Examination and analysis are two steps. Examination reveals the collected data and analysis combines the collected digital evidence with the highly related evidence. Reporting takes the analysis of digital evidence and builds a report to represent. “Digital evidence is abstract and is stored in the binary condition in electronic devices.” (Chen, Tso, Yang 2013). Gathering evidence can be very tricky because no evidence can be damaged. If the phone is turned off, it is best to leave it that way because if turned back on risk of data overriding is possible. “Libimobiledevice is a kind of open source software library for iOS devices like the iPhone.” (Chen, Tso, Yang 2013). Libimobiledevice does not depend on the current iOS special database to jailbreak and remove the system files in the device. Libimobiledevice can use a USB connection as well. As seen in figure 2, once the iPhone is connected to

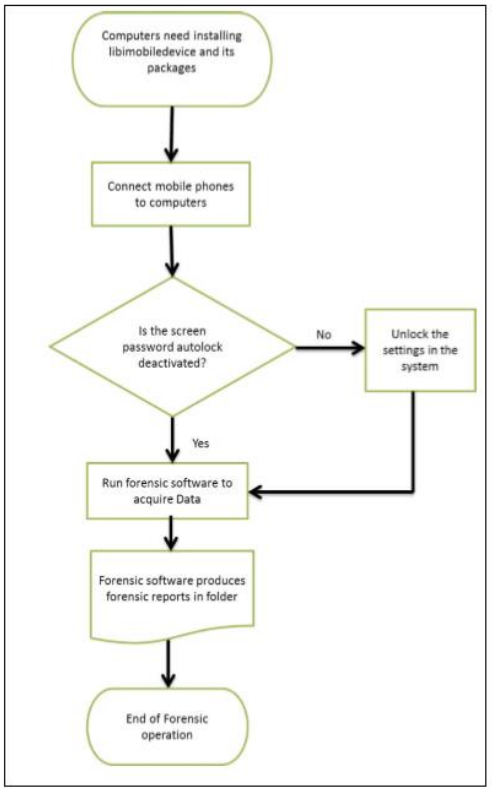


**Figure 2. Operation Process**

Libimobiledevice, the investigation can begin. The password must be on autoblock, if not the settings must be modified. Once finished, the forensic software can be running to acquire data. One can run “Acquire Data” to finish the process. Using “Examine the Acquired Data” examines the information inside of the iPhone. Use “examine the recovered data” to see any deleted data. Once the software finishes, a file folder will appear that includes all the data from the phone. Investigators can open this folder and begin to examine the found data.

Mobile devices such as the iPhone are quickly taking over the newer generation in the mobile phone market. The iPhone is believed to be an essential phone due to its capabilities of executing many operations if not doing many tasks (Al-Hajri, Sansurooah, 2008). Like other technology, this device is used for illegal and legal activities. Hence the probable risks aren’t restricted to materials that are illegal, which could be any of the following: images, audios, documents, and malicious propaganda (Al-Hajri, Sansurooah, 2008). The iPhone tool can be the strongest hacking device if its functions are customized to act with malevolent intent. It is principal to have a good forensic methodology to obtain and examine extracted data (Al-Hajri, Sansurooah, 2008).

There are two forensic extraction methods logical and physical. The logical approach explains the software tools for data recovery (Al-Hajri, Sansurooah, 2008). The physical approach deals with using tools to view the data extraction in the memory chip (Al-Hajri, Sansurooah, 2008). Some tools in the logical approach are ibrickr 0.91, pwnage, Xpwn, and data carving tool. Ibrickr 0.91 opens the firmware. Afterward, the individual should run the application, connect the iPhone and dock. Pwnage works to break the iPhone by changing the bootloader (Al-Hajri, Sansurooah, 2008). Xpwn is an open source tool that arranges proprietary img3 formats in disks stored in RAM (Al-Hajri, Sansurooah, 2008). The RAM disk has to

convert primarily, which bring the need for the encryption key and the vector initial (Al-Hajri, Sansurooah, 2008). Lastly, data carving is the practice of removing or withdrawing a group of data from a bigger set of data. This technique happens during an investigation that is digital where unallocated files are examined. It is essential to have the data craving tool when it comes to retrieving deleted files. Under the physical approach are the JTAG method, JTAG testing pins, and memory removal stages. JTAG (Joint Test Action Group) was made to find solutions for problems with the boards of the logic/circuit. It is used for the construction of a good forensic picture that is incorporated in the memory chips when dealing with compact devices like the iPhone (Al-Hajri, Sansurooah, 2008). JTAG also talks about the borderline control scan which has the serial procedure for board examination. The testing pins are TCK/CLOCK, TMS/MODE, TDI/DATA INPUT, TDO/DATA OUTPUT, and TRST/REST; they play an essential role during the processes (Al-Hajri, Sansurooah, 2008). Lastly, the removal memory stages are (1) de-soldering the chip, (2) getting the chip ready for processing, and (3) the flash reader of memory (Al-Hajri, Sansurooah, 2008).

# References

Al-Hajri, H., & Sansurooah, K. (2008). Australian Digital Forensics Conference. *iPhone Forensics Methodology and Tools*. Retrieved October 1, 2018

Chen, C., Tso, R., & Yang, C. (2013). 2013 Eighth Asia Joint Conference on Information Security. *Design and Implementation of Digital Forensic Software for iPhone.* doi:10.1109/asiajcis.2013.21

Parmar, P., & Sheth, R. (2018). International Journal of Scientific Research in Science and Technology, 4(9). *Logical acquisition of iPhone without Jail Breaking*. doi:10.1018/ijsrst.2018