The Effects of a Factory Reset on an iPhone 8 Plus

By

Lindsey M. Ridderman
B.S. Criminal Justice
Ferris State University, 2018

Advisor:
Dr. Greg Gogolin
Full Professor
Information Security and Intelligence

Spring Semester, 2018
Ferris State University
Big Rapids, MI

Table of Contents

Page

List of Tables

Abstract

With the rapid evolution of the Apple iPhone and the high rate of cybercrime it seems impossible to keep up on the everchanging security features the iPhone provides and how safe user data is. Currently, the iPhone 8 Plus is at its peak, therefore, it is important to understand what happens with data on the device before and after a device factory reset. To analyze this data, the mobile forensic toolkits, Cellebrite UFED Physical Analyzer and MSAB XRY software are used. The aim of this study is to test two iPhone 8 Plus devices using the mentioned software to answer research questions determining what information can be viewed before and after a factory reset is performed and a comparison of results from the two toolkits being used.

The Effects of a Factory Reset on an iPhone 8 Plus

Chapter 1: Introduction

Introduction

The personal data stored on an iPhone is said to be stored at the highest security of any other phone brands currently on the market. Is the data being stored on the new iPhone 8 Plus as secure as the public is led to believe? From iMessage, photos, and phone calls to downloaded applications such as Snapchat and WhatsApp, the amount of data being stored every minute is never ending. Also, what happens when the phone user factory resets their device? Is that data still available when a phone dump is performed? There are many questions revolving around what happens to data and what can be seen when an extraction takes place. From both a personal and professional standpoint it is beneficial to know what information may forever be stored on an iPhone 8 Plus device.

Background

Why is it important to understand how secure data stored on an iPhone 8 Plus is? There is more than one answer to this question. Not only do consumers using these phones want to know how secure their data is, but law enforcement and other government agencies should be aware of what information may or may not be found on a device. Also, when thinking about what is done with an iPhone after it is refurbished and sold again, whose information may still be found on the phone? What if the phone is involved in some sort of criminal activity and a phone extraction is done? The questions are endless with what could happen if data that is supposedly wiped is left out there. Solid information regarding what happens when a factory reset is performed on an iPhone 8 Plus is limited and even more limited on what is found through a phone dump using Cellebrite or XRY technology software. There has been research showing the results of earlier versions of the iPhone, but since the iPhone 8 Plus is still in the beginning stages of use there are not many studies to support these questions.

Statement of the Problem

What happens with phone data has proven to be important in the security of user information. It has also been shown that wiping an iPhone may not actually wipe the phone as users are led to believe. Therefore, the most logical way to determine what data can be viewed on an iPhone 8 Plus before and after a factory reset is done by loading the two new iPhone 8 Plus devices fresh out of the factory box with various types of data. This information can be iMessages, phone calls, voicemails, photos, videos, notes, etc. as well as information from phone applications such as Snapchat and WhatsApp. Once a significant amount of data has been loaded onto the phones they are tested using the Cellebrite and XRY software.

Purpose of the Study

The purpose of this study is to determine what personal information can be viewed when performing an extraction on two iPhone 8 Plus's both before and after a device factory reset. The objective of this study will be to compare the results from two mobile forensics toolkits, Cellebrite UFED Physical Analyzer and MSAB's XRY software. The results will provide much needed information regarding what happens to data that is said to be "wiped" from an iPhone 8 Plus.

Rationale

It is well known that cell phone users and government agencies alike are interested in knowing what happens with iPhone 8 data after it has been factory reset. The goal of the study is to determine what data may still be left on an iPhone 8 Plus once a factory reset has been done. This is important to know for user privacy and for law enforcement knowledge.

Research Questions

1. Determine what information can be viewed during an extraction before a factory reset is performed on an iPhone 8 Plus.
2. Determine what information, if any, can be viewed during an extraction after a factory reset has been performed on an iPhone 8 Plus.
3. Develop comparisons of information gathered through the extractions using Cellebrite UFED Physical Analyzer and MSAB XRY software.

Nature of the Study

The methodology to complete the objectives and answer research questions will be done by conducting a study. This will be an exploratory study using qualitative measures, meaning a descriptive content analysis will be reported based on the findings throughout the study.

Significance of the Study

From a personal perspective, this study is interesting in the sense that I am an iPhone 8 user and to see what information would be viewable through an extraction will provide a great amount of insight into what I should be aware of. The applications that were used on the phones are all applications that I use in my everyday life. The messaging application WhatsApp, is known to be popular among college campuses and other various networks of people around the world who are out of range of cell phone service or want a faster way to group chat with various types of providers (“Most popular messaging…,” 2018). It would be beneficial to know how secure those messages are after performing a factory reset on the phone.

From a professional perspective, the study of iPhones is always a popular topic being that the Apple encryption policies are known to be the strongest amongst cell phone providers. Apple builds “encryption, on-device intelligence, and other tools” into their products that let the user share data on their own terms (“iOS security,” 2018). It would be beneficial for professional teams to know what information may still be gathered using the defined software if an iPhone 8 has been factory reset before entering the possession of law enforcement.

Definition of Terms

UFED – Universal Forensic Extraction Device

XRY software – Digital forensic software used by Police, Law Enforcement, Military, and Government Intelligence Agencies.

.UFD – The extraction file that is created once an extraction is complete using the Cellebrite UFED software.

.ZIP – archived collection of one or more files and/or folders that is compressed into one single file.

.IMG – complete disc image files.

.BIN – binary image of a CD or DVD that can be opened by creating a new text document.

SQLite – “an in-process library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine (“About SQLite,” n.d.).”

Snapchat – a social media application that allows users to send images and chat messages to other users.

WhatsApp – messaging application used around the world for people to communicate in a reliable and secure way (“About WhatsApp,” n.d.).

Faraday bag – bag that an electronic device may be stored in to block cell signal (Gogolin, 2013).

Assumptions and Limitations

The assumptions in this exploratory study are that the iPhones will be loaded with enough data to complete the study and all necessary extractions will be performed. It is assumed that the extractions using both Cellebrite and XRY will provide results to answer the established research questions. The limitations may be that there is no way to know for sure what type of results will come from the extractions. The research may be limited if the results do not turn out as planned. The time frame to load data onto the devices is also limited which may affect the amount of data that can result from the study.

Chapter 2: Literature Review

Researching factory resets regarding the iPhone 8 Plus proved to be lacking in relevant information. However, there are studies out there with information regarding earlier versions of the iPhone as well as Android devices. There is also a large amount of information about what data may be found on devices when using the Cellebrite or XRY software to perform an extraction. Along with information regarding the tools used to perform extractions, information regarding the digital forensic process and what data can be found on a mobile device are of importance to research.

Glisson, Storer, Mayall, Moug, and Grispos (2011) examined what a mobile phone may reveal about a person in their article, *Electronic retention: what does your mobile phone reveal about you?* The study investigates how much information may still be available on a phone that has been refurbished and re-sold to other mobile devices users. The authors pointed out that mobile devices may belong to multiple owners over the lifetime and users tend to keep phones for an estimated 20.5 months before replacing. To conduct their experiment, refurbished devices were obtained from an eBay online auction site and a local pawn shop. Among the 49 devices obtained, an iPhone 3G and HTC Touch Dual were included.

Glisson et al. (2011) tested their devices using three different mobile forensic toolkits – Cellebrite UFED Version 1.1.3.8, XRY Forensics' Examination Kit Version 5.1, and Radio Tactics' Aceso Version 5.0.4.2. The results of the study showed that all 49 devices that were tested showed information still present which included calls, contacts, emails, messages, and other potentially sensitive data. Deleted artifacts were also recovered through the extraction process from 15 of the mobile devices. These results showed that either the mobile devices users were not attempting to wipe their information before re-selling on the market or their attempts to wipe the devices failed. Whichever may be true, it is a consensus that personal data is almost always left on a phone.

To understand the study being conducted on the iPhone 8 Plus devices it is necessary to understand how Cellebrite UFED Physical Analyzer works as well as MSAB's XRY software. To conduct an extraction on an iOS device using Cellebrite the UFED Physical Analyzer software must be used. When the iOS device is connected to the software, UFED will automatically select which extraction method is appropriate for the device ("Cellebrite iOS physical…," 2011). Once the necessary method of extraction is chosen, the decoding process will begin, which translates raw data from the device to a recognizable format within the UFED software ("Cellebrite iOS physical…," 2011). Concerns about whether the decoding process may miss information depends on the software programming, but with Cellebrite's access to the manufacturers mobile devices and device carriers it is easier for the UFED software to decode information ("Cellebrite iOS physical…," 2011). This is one reason Cellebrite has become a top software to use for digital forensic investigations.

UFED Physical Analyzer can identify application data files such as WhatsApp, Viber, Twitter, and Facebook from file extractions of Android or Blackberry smartphones. In iOS devices, UFED can identify the SQLite database files of the same applications ("Cellebrite iOS physical…," 2011). However, if the application is not a well-known application that UFED is programed to look for it will most likely not find the database since there are many applications available. Since UFED can identify these application database files it is a strong tool to use for the study. WhatsApp is one of the applications being tested in the experiment.

Cellebrite explains that after an extraction is complete, the UFED software will generate an extraction file as well as a .UFD text file that will notify UFED Physical Analyzer what type of extraction the file is. With logical extractions, a .ZIP file is also created, and an .IMG and .BIN file for physical extractions. Along with the extraction files created, UFED Physical Analyzer will also create a report which varies in delivery depending on the type of extraction that was done.

The other digital forensic tool being utilized in this study is MSAB's XRY software that extracts data from electronic devices using the Windows operating system. It is important to use two different tools for this study to compare the results of each software and analyze which one will extract more data or if they turn out the same. To perform data extractions using this software it is necessary to obtain the XRY software, XRY license, XRY key, and any cables that are necessary to connect the devices being extracted ("Retrieving data from…," 2014). Types of devices that XRY can extract information from include cell phones, GPS units, music players and tablets. There are three types of extractions that may be done using the XRY program – XRY Logical, XRY Physical, and XRY Complete ("Retrieving data from…," 2014).

A logical extraction will communicate with the operating system and recover most live data from the device, which to put into perspective, is equivalent to examining every screen available on the phone manually and taking record of what was found ("Retrieving data from…," 2014). A physical extraction is more advanced than logical and will recover all available raw data from the device, which also includes deleted data. There are two stages involved in a physical extraction, the first being the initial device 'dump' where the raw data is recovered followed by the second stage of 'decoding', which is the XRY software turning the data into human readable form, the same as Cellebrite decoding the raw data from extractions ("Retrieving data from…," 2014). A physical extraction is the best choice when dealing with phones that are security locked or a phone without a SIM Card. Lastly, the complete extraction is a combination of both logical and physical. This means with one extraction there is a strong possibility of recovering all data found on the device.

To conduct an extraction on an iOS device using the XRY software, the first step is to connect the device to the software using either the USB cable or XRY Communications Unit, next the Micro Systemation USB Key must be plugged into another USB port. Once the XRY application is opened, find the extract data option, identify the device, choose the extraction method, click “Trust” when the iOS device asks if the computer is to be trusted, and the extraction process will then begin (“Retrieving data from…,” 2014). The wizard will then analyze the data and decode it in a readable format and an .XRY file will automatically open in a new window. Cellebrite and XRY look different, but in the general sense of things complete the same tasks as one another. Both tools will extract data from iOS devices and create a readable format to be analyzed.

For this study, the digital forensic process is of importance to research to know what should be done in the case of seizing a phone for examination. The book, *Digital Forensics Explained*, authored by Dr. Greg Gogolin (2013), has a chapter focused on mobile forensics which provides a solid description of the forensic process. One of the first things to consider when talking about mobile forensics is that there are many tools that can be used, and every tool has different characteristics. It is also important to consider the difference in handheld devices and computers, for example forensics on a handheld device is done with active imaging while a computer is done with bit stream imaging (Gogolin, 2013).

The next thing to remember during the forensic process is that mobile devices have the possibility of being remotely modified or wiped, which means precautions need to be taken to avoid this from happening otherwise all digital evidence may be gone. There are a few different options to avoid this problem, the first being putting the device in airplane mode which will take the phone off any wireless networks. Another option would be to utilize a Faraday bag, which is a bag that the device can be placed into that blocks the cell signal (Gogolin, 2013).

Lastly, the investigator must understand a few different things concerning mobile devices. The first being what information may be found on a mobile device, which includes provider/carrier information, phone information such as voice calls, SMS, and MMS messages. Also, the SIM card will hold a large amount of information as well as any media cards that may be present (Gogolin, 2013). The investigator also needs to know how mobile devices work, radio waves connecting to cell phone towers, and the different generations of cell phone technology (Gogolin, 2013). All information the investigator should be aware of is important in the forensic investigation to determine where/when different messages, calls, apps, etc. were used on the device. To conduct a strong digital forensic investigation the previously mentioned steps should be followed.

In Schwamm and Rowe's article, *Effects of the Factory Reset on Mobile Devices,* it was found that data files were left on both Android and iPhone devices that had been factory reset (2014). The Cellebrite UME-36 Pro Universal Memory Exchanger 1.2.2.3 hardware and Cellebrite UFED Physical Analyzer 3.7.2.0 were used to conduct the experiment as well as the Oxygen Forensic suite (Schwamm & Rowe, 2014). To conduct the experiment, an Apple iPhone 4S and Android Samsung Galaxy SIII were loaded with data including web history, pictures, link files, zip files, YouTube video views, and note entries. Each of these was manually documented as to remember which files and places had been visited to compare when conducting the extraction analysis.

The phones used for this experiment were not connected with a cell phone provider, so messaging and voice call services were not utilized. This is an aspect that the current experiment being conducted will address since cell phone provider services are available for use. For the Android results, the number of recovered files pre-reset was 5,141 and 3,578 files post-reset with 3,292 files being an exact match with pre-reset content (Schwamm & Rowe, 2014). The results of the iPhone test returned results of 61,276 files recovered pre-reset and 43,165 files recovered post-rest (Schwamm & Rowe, 2014). Of the files recovered post-reset, 42,728 were exact matches for both path and contents. The results of this study proved that not everything thought to be wiped during a factory reset is. The iPhone reset proved to wipe far more data than did the Android, but there were still some files leftover.

The experiment conducted by Schwamm and Rowe followed similar steps as the current experiment being conducted, with differences in tools being used for analysis, the type of devices being used, and the type of content being analyzed. The iPhone test showed that the AES-256 encryption Apple claimed to use for protecting user data did not encrypt all data that should have been. Since Apple still uses the same type of encryption hardware, it is assumed that the same problem may occur during the iPhone 8 Plus experiment when a factory reset is performed. For the protection of user data, the authors mentioned that a few different steps should be taken to ensure a phone being given away or sold is clear of user data. Schwamm and Rowe suggested following the steps which include performing the device factory reset, manually delete remaining files – making sure to check in unconventional places where the files could have moved, deleting cached files, history, cookies, etc., and removing the SIM card or other removable storage (2014).

The recommendations from the previous study touch on an important subject, removing the SIM (Subscriber Identity Module) card before giving the phone away or selling. The article, *Forensic Investigation of SIM Card*, authored by Ibrahim, Al Naqbi, Iqbal, and AlFandi (2016) delve into detail of what information may be obtained from a SIM card extraction. The SIM card holds an immense amount of personal data that a phone user would not want other people having access to. Since cybercrime is a growing problem around the world it is important to know where user data goes and what is stored, especially if that phone lands in the wrong hands and is later used in a cyber investigation.

Ibrahim et al. (2016) mentioned that the SIM card from a phone holds a vast amount of personal identity data such as the name of the subscriber registered to a cell phone network, contacts, messages, calls, locations, and other user data that is of a personal nature. For the study, an Apple iPhone 4S was used along with an Android Samsung Galaxy SIII with their respective SIM cards. Since iPhones do not allow directly saving to the SIM, the authors manually moved the SIM to a Nokia device and loaded data. To conduct the analysis of the SIM cards the following commercial and open source tools were used – EnCase Forensics, MOBILedit, Mobile Phone Examiner, Oxygen Forensic_Suite, Paraben SIM Card Seizure, pySIM, SIMBrush, SIMScan, UFED Cellebrite, USIMdetective, and XRY.

The results obtained by Ibrahim et al. (2016) showed that Paraben SIM Card Seizure, Quantaq USIMDetective, and XRY were the most beneficial tools in extracting SIM card data. Some of the data that was found through extraction included the Last Area Code and Routing Area Location, Temporary Mobile Subscriber Identity, and International Mobile Subscriber Identifier. With the results of this experiment, it is more proof that extreme caution needs to be taken when wiping a device for any after-market use that is going to another user other than the one who purchased the device.

Chapter 3: Methodology

Description of Methodology

The iPhone 8 Plus study being conducted is considered exploratory. An exploratory study is used for topics that are somewhat new and although iPhones in general are not new, the iPhone 8 Plus is and not many experiments have been conducted concerning the factory reset on this particular version. For this study, information is gathered about the forensic process, related studies, and the tools being used to complete the study which are Cellebrite UFED Physical Analyzer Version 7.0.0.108 and MSAB XRY Version 7.0.1 software. Data is also loaded onto two iPhone 8 Plus phones and dumped into the mobile forensic software for analysis. Therefore, in the long run this is an exploratory study because it is concerning a new topic and a great deal of information is being gathered and evaluated.

Design of the Study

For this study, two iPhone 8 Plus phones were utilized. Both phones were loaded with data, which included iMessages, voice calls, camera photos, notes, Safari search history/favorites, Snapchat, and WhatsApp data. The phones communicated back and forth to one another to get the messages, calls, Snapchat, and WhatsApp information loaded. After a sufficient amount of data was loaded onto both phones they were connected to the Cellebrite and XRY software to conduct an extraction. The steps to completing a Cellebrite UFED Physical Analyzer extraction are as follows:

1. Open UFED Physical Analyzer
2. Select the ‘Extract’ drop down menu
3. Choose ‘iOS device extraction’
4. Connect the iOS device, making sure it is on and unlocked

5. Choose ‘Advanced Logical Extraction’
6. The connected iOS device should be recognized
7. Follow prompts to complete the extraction, once completed the .UFD file will be available for viewing in UFED Physical Analyzer

The steps to completing an extraction in XRY are as follows:

1. Open XRY extraction software
2. Choose the ‘extract’ option
3. Connect iOS device and wait for the software to recognize the device
4. Choose the extraction method
5. On the iOS device choose ‘Trust’ when prompted if the device is trusted on the computer
6. Follow the steps to complete the extraction
7. Once the extraction is complete a file will be created that can be saved and viewed to analyze

After completing the extraction process for the iPhones once all data has been loaded it is time to factory reset the devices. The factory reset is done by entering the general settings area of the iPhone and scrolling down to the bottom of the options where it says ‘Reset’, from there choose the option of ‘Erase All Content and Settings’ to fully wipe the phone of the present data. Once this process has been completed the iPhone will ask you the basic questions to use/setup the phone, which must be done to complete the final extractions. After going through the basics, the phone is ready to be connected to Cellebrite and XRY for the post-reset extractions. The post-reset extractions follow the same process as did the pre-reset extractions. Once all extractions have been completed it is time to analyze the data through the tools available through Cellebrite and XRY, UFED Physical Analyzer and XAMN, respectively.

Data Analysis

The results from the exploratory study will be analyzed as soon as all extractions have taken place using both the Cellebrite and XRY mobile forensic toolkits. The results from the extractions will provide information valuable to answering the previously stated research questions. All questions being explored can be answered by analyzing the data that is shown through the mobile extractions such as what files are able to be viewed before and after a device factory reset. The data collected from the extractions will be kept for at a period of at least six months to account for sufficient time in completing the analysis of data obtained through the iPhone dumps.

Chapter 4: Results

iPhone Results Using Cellebrite

Of the ten iPhone features that were examined before and after a factory reset on the iPhone 8 Plus, it appears that all user data entered by the user was wiped as the factory reset claims to do. Before a factory reset, the extraction from Cellebrite shows that the items that were simply "deleted" from the phone are still available for viewing. The table below shows the number of files that were found on iPhone 1 before and after using factory reset option using Cellebrite UFED Physical Analyzer for the extraction.

Table 1 *iPhone 1 Cellebrite Extraction Results*

Type of File	Count Before Reset	Count After Reset
Cookies	511	4
Web Bookmarks	14	N/A
iMessage Chats	50 (1 deleted)	N/A
Call Log	29 (2 deleted)	N/A
Notes	4	N/A
Images	964	1
Device Locations	314	N/A
Safari Web History	173 (73 deleted)	N/A

Note. The number of files present on the iPhone 1 using the Cellebrite UFED Physical Analyzer software.

Cookies. Before the factory reset Cellebrite software recovered 511 cookies on iPhone 1, while the post-reset returned 4 cookies. The cookies found before the reset contained information that was searched by the user. The cookies found post-reset appear to be all from apple.com, which brings the conclusion that they are default cookies on the device from setting the iPhone up.

Web bookmarks. Pre-reset showed that Cellebrite recovered 14 web bookmarks from Safari and the post-reset extraction brought back 0 hits for recovery.

iMessage chats. Pre-reset showed 5 iMessage chat sessions with a total of 50 messages and 1 deleted chat. Post-reset extraction recovered 0 iMessage chat sessions.

Call log. Pre-reset showed 29 items in the call log with 2 deleted. The post-reset recovered 0 items in the call log.

Notes. Pre-reset showed 4 notes in the Apple installed application, while the post-reset recovered 0 notes in the application.

Images. Pre-reset recovered 964 images from the device. The post-reset recovered 1 image that is the default background image on the device.

Device locations. Pre-reset returned 314 locations while there were 0 recovered post-reset.

Safari web history. Pre-reset recovered 173 search histories with 73 deleted. The post-reset did not recover any search history.

WhatsApp and Snapchat. The WhatsApp data is presented in an interesting way through UFED, the contents from the app are displayed within databases and it is necessary to determine what information is connected through different databases. Such as one database for the application will show the phone numbers associated with the messages and another database will show the messages. Before the factory reset all messages that were sent using the app are displayed, but after the factory reset none of the information can be viewed and there is no trace of the app being installed. As with the WhatsApp app, the data from Snapchat is displayed through databases as well. However, photos sent through the app cannot be viewed unless there is a state or federal warrant obtained (“Snapchat law enforcement…,” 2016).

iPhone 2 Results Using Cellebrite

For the second iPhone used in the experiment, the results proved to be the same as the first device. Of the ten iPhone features that were analyzed, the user data recovered through the Cellebrite UFED Physical Analyzer extraction was wiped from the device and not present on the extraction post-reset.

Table 2 *iPhone 2 Cellebrite Extraction Results*

Type of File	Count Before Reset	Count After Reset
Cookies	654	2
Web Bookmarks	6	N/A
iMessage Chats	3	N/A
Call Log	22 (1 deleted)	N/A
Notes	45 (1 deleted)	N/A
Images	111	1
Device Locations	3	N/A
Safari Web History	802 (47 deleted)	N/A

Note. The number of files present on iPhone 2 using the Cellebrite UFED Physical Analyzer software.

Cookies. Before the factory reset, the extraction recovered 654 cookies, while post-reset showed 2 cookies still available. The cookies that were still able to be viewed were from Apple and had to do with activating the iPhone.

Web bookmarks. Pre-factory reset recovered 6 bookmarks from Safari, while post-reset did not recover any bookmarks.

iMessage chats. Pre-reset recovered 3 iMessage chats with 45 messages while post-reset did not recover any chats.

Call log. Pre-reset recovered 22 calls with 1 deleted and post-reset did not recover any calls.

Notes. Pre-reset recovered 3 notes with 1 deleted and post-reset did not recover any notes.

Images. Pre-reset recovered 111 images while post-reset recovered 1 image. The image recovered post-reset was the default background image on the device.

Device locations. Pre-reset recovered 3 locations found on the device, while post-reset did not recover any.

Safari web history. Pre-reset recovered 802 items in the Safari history with 47 deleted items. The post-reset did not recover any search history.

WhatsApp and Snapchat. As previously explained in the results for the iPhone 1 extraction, the data for the WhatsApp application is viewed using databases rather than be presented outright for the analyst. Snapchat is also

iPhone 1 Results Using XRY

The results from the XRY extraction proved to be nearly identical to Cellebrite number wise with the files that were present before and after a factory reset. The following table shows the numbers in relation to iPhone 1 and the XRY extraction.

Table 3 *iPhone 1 XRY Extraction Results*

Type of File	**Count Before Reset**	**Count After Reset**
Cookies	518	7
Web Bookmarks	16 (2 deleted)	N/A
iMessage Chats	50 (1 deleted)	N/A
Call Log	29 (1 deleted)	N/A
Notes	4	N/A
Images	966	1
Device Locations	168	N/A
Safari Web History	183 (120 deleted)	N/A

Note. The number of files recovered on iPhone 1 using the MSAB XRY software.

The results from the iPhone 1 phone extractions recovered all user data that was placed on the phone prior to a factory reset, but post-reset only returned items for cookies and images. In comparison to the Cellebrite results, XRY recovered more files for cookies, bookmarks, images, and Safari web history.

Cookies. Before the factory reset, the extraction recovered 518 cookies, while post-reset showed 7 cookies still available. The cookies that were still able to be viewed were from Apple and had to do with activating the iPhone.

Web bookmarks. Pre-factory reset recovered 16 bookmarks with 2 deleted from Safari, while post-reset did not recover any bookmarks.

iMessage chats. Pre-reset recovered 50 iMessage chats with 1 deleted, while post-reset did not recover any chats.

Call log. Pre-reset recovered 29 calls with 1 deleted and post-reset did not recover any calls.

Notes. Pre-reset recovered 4 notes while post-reset did not recover any notes.

Images. Pre-reset recovered 966 images while post-reset recovered 1 image. The image recovered post-reset was the default background image on the device.

Device locations. Pre-reset recovered 168 locations found on the device, while post-reset did not recover any.

Safari web history. Pre-reset recovered 183 items in the Safari history with 120 deleted items. The post-reset did not recover any search history.

WhatsApp and Snapchat. As previously explained in the results for the iPhone 1 extraction, the data for the WhatsApp application is viewed using databases rather than be presented outright for the analyst as well as Snapchat data.

iPhone 2 Results Using XRY

Table 4 *iPhone 2 XRY Extraction Results*

Type of File	Count Before Reset	Count After Reset
Cookies	669 (2 deleted)	3
Web Bookmarks	7 (1 deleted)	N/A
iMessage Chats	45	N/A
Call Log	24 (1 deleted)	N/A
Notes	3	N/A
Images	113	1
Device Locations	1	N/A
Safari Web History	408 (64 deleted)	N/A

Note. The number of files recovered iPhone 2 using the MSAB XRY software.

As with the first iPhone tested using XRY software, there seems to be no indication that user files were left on the phone after a device factory reset. Also, as with iPhone 1 the results of the extractions in comparison with Cellebrite returned more files with XRY for cookies, bookmarks, images, and history.

Cookies. Before the factory reset, the extraction recovered 669 cookies with 2 deleted, while post-reset showed 3 cookies still available. The cookies that were still able to be viewed were from Apple and had to do with activating the iPhone.

Web bookmarks. Pre-factory reset recovered 7 bookmarks from Safari with 1 deleted, while post-reset did not recover any bookmarks.

iMessage chats. Pre-reset recovered 45 iMessage chats, while post-reset did not recover any chats.

Call log. Pre-reset recovered 24 calls with 1 deleted and post-reset did not recover any calls.

Notes. Pre-reset recovered 3 notes and post-reset did not recover any notes.

Images. Pre-reset recovered 113 images while post-reset recovered 1 image. The image recovered post-reset was the default background image on the device.

Device locations. Pre-reset recovered 1 location found on the device, while post-reset did not recover any.

Safari web history. Pre-reset recovered 408 items in the Safari history with 64 deleted items. The post-reset did not recover any search history.

WhatsApp and Snapchat. As previously explained in the results for the iPhone 1 extraction, the data for the WhatsApp application is viewed using databases rather than be presented outright for the analyst as well as Snapchat data.

Chapter 5: Summary of Findings

The exploratory study conducted on two iPhone 8 Plus devices proved to show that when a factory reset is done the information entered by the device user is wiped as the reset is supposed to do. For both iPhones tested, there were very few files found on the phone through the extractions and those files were related to the activation of the device. The only features that were tested that showed files after the factory reset were cookies and images. The XRY software recovered more files pre and post-reset than did Cellebrite for both iPhones. After conducting research on other studies and material out there, the results are surprising that there is no trace of the user data on the extractions.

Some items that could be of interest for further study would be exploring the private browsing mode on the Safari internet application. When the user is in private mode there is supposedly no history saved to the phone, but it could very well show up on an extraction. Further study could also be done to determine if more data were loaded onto the iPhone for a longer period of time would the results still turn out to be the same. Another application that would be interesting to study would be Viber, which is another messaging application that is popular amongst students as well as professionals that can be used around the world the same as WhatsApp.

References

"About SQLite." *About SQLite*, www.sqlite.org/about.html.

"About WhatsApp." *WhatsApp.com*, www.whatsapp.com/about/.

Cellebrite iOS device physical extraction manual. 22 Nov. 2011, www.mcsira.com/WEB/8888/NSF/Web/3128/UFEDFAQ/Manuals/iOSPhysicalUserManual.pdf.

Glisson, W., Storer, T., Mayall, G., Moug, I., & Grispos, G. (2011). Electronic retention: What does your mobile phone reveal about you? International Journal of Information Security, 10(6), 337-349.

Gogolin, G. (2013). *Digital forensics explained*. Boca Raton, FL: CRC Press.

Ibrahim, N., Al Naqbi, N., Iqbal, F., & AlFandi, O. (2016). Forensic investigation of SIM card. Proceedings of the Conference on Digital Forensics, Security and Law, 219-233.

iOS security. Jan. 2018, www.apple.com/business/docs/iOS_Security_Guide.pdf.

Most popular messaging apps 2018. (2018). Retrieved April 02, 2018, from https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Retrieving data from apple iOS devices using XRY. (2014, December). Retrieved from https://www.champlain.edu/Documents/LCDI/Apple_iOS_Tutorial_Final_PDF.pdf

Riqui Schwamm, & Neil C. Rowe. (2014). Effects of the factory reset on mobile devices. Journal of Digital Forensics, 9(2), 205-220.

Snapchat law enforcement guide. 11 Oct. 2016, storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf.