Forensic Analysis on Android Mobile Devices

What types of forensic data resides on Android mobile devices?

British Columbia Institute of Technology

Forensic Investigation – Computer Crime

Graduation Project Proposal

Harry Taheem

March 7, 2015

Version 2

Table of Contents

Abstract

The study assessed the top four mobile forensics solutions to understand the type of information that can be extracted from mobile devices. These days' mobile devices have become very common among most individuals. However, many are not aware of the type of sensitive data and information that is stored on these devices. And, what may happen if that data falls into the hands of someone with ill intentions. Law enforcement has been struggling with crimes related to getting evidence off mobile devices to prove many case in the court of law. Along with that, law enforcement has not being able to gain enough skills and knowledge to uncover evidence off criminal's mobile devices. The study was conducted with common mobile devices that are used these days. It will define and list out all types of sensitive information that can be obtained off newer mobile devices in a very detailed manner. And, will educate not just law enforcement, but create awareness for the mobile users within the general public.

1. Introduction

The purpose of this study is to determine the amount of data that can be accessed and recovered off of an Android mobile device. These days' mobile devices carry a large amount of data such as media which contains images and videos. Also, data such as call logs and text messages are also stored on the devices. Furthermore, the World Wide Web can be accessed from these devices, which leads to the fact that many applications can be downloaded on to the mobile devices. Most mobile devices can store and hold up to and over 192GB worth of data. What once was known as a cellular device used only to make voice calls is now a mini hand held computer that each user carry's around with them. That means all of their data resides on their mobile device and if it falls into the wrong hands the data could be misused or used against the device owner.

The main goal in this study is to find out how much information can be recovered from a mobile device. And, how can someone misuse this stored information if they were to illegally access and get ahold of an Android mobile device. These devices store very sensitive information such as Wi-Fi network passwords, social media logins, email access, GPS locations coordinates and banking information details and so forth. Therefore, these mobile devices have become a security risk for the average user. And, the majority of the mobile users have no idea how harmful the data can be if used against them. However, many mobile users are unaware of how serious the security breaches may be, and as to what type of damage can be caused by them. Therefore, that means a person may access the usernames and passwords to Wi-Fi networks, personal email addresses and social media logins. Then someone that

attempts and is able to steal another person's mobile device would be able to mine out all this data. So in the long run anyone that owns and uses a mobile device would be at the same risk.

2. Benefits of the study

The benefits of the study will further help mobile users understand how un-safe their data is on their own mobile devices. But, it will also help provide other solutions to fix these weaknesses or create other controls to mitigate the security risks. Businesses that store trade secret data or other vital and sensitive data documents may think twice. Business documents could cause long term problems for a business in the case where an employee has their mobile device stolen. The mobile device engineers also may use this study to possibly find alternative methods to encrypt or secure data in a form where only the device owner could ever retrieve the data from it. Another possible idea for mobile engineers is to create a device that doesn't store information for too long.

The study will also provide benefits to law enforcement, as it has become quite common to use mobile devices as forensic evidence in criminal and civil court cases. Therefore, the information in this study will allow law enforcement to understand what type of data can be extracted and how they can best use this data in a court of law. Lastly, another benefit would be for the mobile device consumers. If a mobile device user were to lose access to their device by forgetting their password. Then they would have a method to be able to once again re-gain access to their mobile device. And, be able to extract their lost data and retrieve it, so that they do not lose important data such as their contact lists, important messages or documents with sensitive information.

3. Literature Review

There are other similar studies that have been conducted to understand what types of forensic evidence can be obtained from mobile devices. (Glisson, 2011) has a similar study, which looks at collecting mobile devices from various places such as eBay, Craigslist and local pawn shops. Their study also performs a mobile forensic analysis on 49 mobile devices. In total 11,135 data artifacts were found from these devices. The information found was listed in a form of severity, which consisted of how dangerous or harmful the information was in terms of causing harm to the previous owner's privacy. The type of information found were images, text messages, browser web history and list of contacts. All this information was deleted by the previous mobile device owners. However, the researchers were able to recover this deleted data that most mobile users think would have been deleted. The study concluded with the facts after analyzing all of the recovered data that potential future work needs to be done in order to ensure confidentiality for mobile user's personal stored data. The overall message of the study brings

awareness to the second hand sellers' market for mobile devices. And, that a mobile seller may be selling not just their device, but the information and also comes along with it. The same concept in terms of what types of forensic data that is found is similar to the objectives of this new study that is currently being researched.

A similar study completed by (Storer, 2010) also analyzed investigating information discovered from re-sold mobile devices. The study ran a phase of acquisition of all of the mobile devices through eBay. The next phase moved into the investigation phase, which applied the use of forensic applications to extract data from the mobile devices. In this study in order to verify data integrity, the researchers conducted the test twice in order to match up their findings. This then allowed them to verify if the data they extracted could be extracted again to prove that the experiment functions properly. In order to help further studies continue their own research. The findings and results were put in a database created by the researchers in order for others to match their own research conclusions. The study was conducted in late 2010, which is one reason why a new update study needs to be done. The new study then would show any new forensic tool improvements, as well as improvements in obtaining and recovering more detailed data.

A research study by (Mutawa, 2012), looks at the forensic analysis of social networking application on mobile devices. This applies to the current study since it also includes social media applications that will be placed on the mobile device. The research study of (Mutawa, 2012) looks at potential evidence on mobile devices that make use of social media. The study found that a lot of the social media data was not only stored on the social media website such as Facebook. But, that much of that same data is also stored on the users own mobile device.

4. Methodology

The project will be conducted through an experimental design, which will focus on a forensic examination on a select Android mobile device. Two types of mobile forensic software will also be utilized in order to gain access to the mobile device and extract the data from it. The assumption is that there is data stored on mobile phones, and that it can be accessed by someone that has enough knowledge to break into a mobile device and obtain all data on it. The role of the researcher is to use their forensic analysis skills to determine the best methods and procedures to obtain data from the mobile device.

The data gathering steps will be in phases, where the first phase looks at populating the data on the phone. This will create a simulation of actual activity taking place on a normal mobile device. The second phase regards obtaining and securing the mobile device. The next phase conducted will concentrate on extracting the data from the mobile device in a few different manners. The extraction will

take a physical, and logical image of the devices storage system. Later, the software will also aim at bypassing the mobile device password/login lock. The phase also aims at gathering files and data that can be accessed normally by a user that are already stored on the device. The third phase will look at finding deleted data and recovering it such as deleted images and text messages.

Another aspect that will be inspected is the use of recovering any passwords of existing Wi-Fi networks, and mobile applications such as Facebook. Afterwards the final phase will be introduced, and all of the data will be analyzed to come to a conclusion as to what type of information was obtained. After all of the phases have been completed the procedure for analyzing the data and what type of information was found and can be found will be listed. And, this is the section that will disclose what types of information was found and will be placed in a selected set of categories.

There will be set categories that will depict each category of data found as a security risk of High, Medium and Low in terms of how dangerous the obtained information may be. The impact of the research findings will help create awareness for all mobile users in terms of what type of data is stored on their device. Some data that users may think is deleted may still reside on the device and could possibly be recoverable by a person that has the knowledge and tools to do so. The other benefit would be that the study may lead to question how better information could be stored securely on mobile devices. This means that in the future based off the weaknesses found newer and more innovative methods could be integrated to allow better encryption of stored data on mobile devices.

In order to validate data and its integrity at the minimum two types of mobile software will be used to extract data from the mobile devices. Therefore, the assumption is that both mobile forensic software toolkits should be able to extract similar data. And, if both programs are able to extract the exact same data information, then the assumption is that the data is valid since it was extracted both times by both toolkits. Furthermore, the data can also be verified to see if the parameters such as date, time, etc… make sense to be in a format that fits a logical format. Lastly, the experiment will be conducted twice in order to see if the data extracted is the same and can be matched from each attempt.

4.1 – Test environment and requirements

Prior to conducting the mobile forensic analysis, a PC machine will have all of the mobile forensic software and toolkits installed ahead of time. Network access will be needed to connect to a Wi-Fi connection. The following is the list of all hardware and software that will be needed to conduct the research study.

- A Samsung Galaxy Note 4 and Samsung S 3 mobile devices
- Cellebrite mobile forensic software analysis toolkit

- Oxygen Forensics Suite
- Faraday bag
- MobilEDIT mobile forensic software analysis toolkit
- Andriller Forensics Extracting Software
- USB drive to store all of the extracted data on to

4.2 Phase 1 – Data Population

The devices will not need any data populated, as the devices that will be acquired will have pre-existing data on them. In order to make the study as real as possible, the mobile devices will be end up being devices that someone has already used for a while. The devices will be bought from craigslist and/or borrowed from random users, who have no problem lending their older phones that they no longer use any more. Using this technique saves additional work required to generate false information and makes it much less real in terms of user activity. Now with devices that users have utilized as most normal users would, it provides for more real and life like data on the mobile devices.

4.3 Phase 2 – Obtaining the Device

This phase regards obtaining the device with the assumption that the device has been left behind by its owner. This will simulate a real life situation that would occur if a device was stolen by an individual. A Faraday bag will be used to transport the device to the testing lab. The point of the bag is to block any cellular signal and service from the device to a cellular tower. This way the device owner would not be able to remotely wipe the phone data. And, it will preserve the integrity of the data on the mobile device. The following lists the steps for this phase in more detail. Figure 1.2 displays a visual representation of the below processes.

1. The device will be placed on a table in a computer lab with the battery being charged over 60%.

2. The device then will be placed off standby mode and put into Flight mode to be sure any network connection established is turned off. This is so that no one may remotely wipe the device.

3. The device then will be secured in a Faraday bag and will be sealed to prevent any wireless signal from making contact with the mobile device.

4. The device will be transported to a computer testing lab to run forensic tools to extract any data that resides on the device.

4.3 Phase 3 – Analyzing the Device

Once the device has been secured and has no access to any signal from its carrier. The device will then be ready to connect to the lab testing PC for data extraction. Special mobile forensic software will be used to analyze the data on the device. Cellebrite and MobilEdit will be used as the mobile forensic software to extract and analyze the data from the mobile device. The device needs to be checked to see if a connection can be made to remotely wipe the device from an online resource website. The remote wipe test will confirm that the device has no connection to any network or wireless carrier while it is held in the lab. The data will first look at a Physical level acquisition of data stored on the mobile device. The second part will examine a Logical acquisition of data stored on the mobile device. Lastly, the final step will examine manually viewing data stored on the device through the user interface. Figure 1.3 displays a visual representation of the below processes.

1. Keep the device stored in the Faraday bag, and examine to double check that it has sufficient battery life of over 60%. Connect a charging unit so the battery does not die.

2. Setup the mobile forensic software on the PC lab machines. Connect the mobile device to the PC lab machine through a USB and Micro wire.

4.3.1 - Physical level acquisition

4. The device will have a physical drive acquisition conducted through the software, and the data will be saved on a PC hard drive.

4.3.2 – Manual access to device

6. Use the software to bypass the login screen since the device will be locked with a pattern lock.

7. The data on the PC hard drive then will be analyzed and investigated to see what types of data can be seen, what type of data is hidden and what information it contains.

8. The device will be manually checked by swiping on it to view the menu.

9. Applications will be clicked on to open them and to see if they are active and logged in.

10. If the applications allow access, then all data that can be accessed will be tried and seen.

4.4 Phase 4 – Review of the Findings

In this phase all of the data findings will be organized and structured to allow for the researcher to examine the data that is present. The data will then be listed and organized according to its level of severity in terms of how much of a security hazard and risk the information can pose. Figure 1.4 displays a visual representation of the below processes.

1. Analyze the Physical acquisition drive to reveal and uncover hidden/deleted files, as well as other data such as usernames and passwords. Also look for images, contacts, text messages and other data.

2. Analyze the applications manually in order to recover any authentication credentials such as account login information. Also look for images, contacts, text messages and other visible data.

4.5 Phase 5 – Document all results and conclusions

The last phase will list all of the details in the research in terms of all tools used and data that was found. It will also display all of the data findings, and conclusions made from the results that were found. The study will also help pose questions on other factors that were missed or conducted for future studies. The study may leave room for potential future work. It will include all of the data in visual forms and organize all of the findings in severity groups.

Short falls

The research project has a few short falls when it comes down to extracting data from the mobile device. Some mobile forensic software will extract data that another type of mobile forensic software may miss. This is one reason why some analysts will use multiple mobile forensic tools to extract data in case

one tool misses some vital information. Since this project is not heavily funded, and some of the top most best mobile forensic tools costs well over ten thousand dollars. There may be some data that does not get extracted by the tools used in this study.

Some other limitations to the study are that the study will only look at mobile devices using the Android operating system. Therefore, the research may not be as useful for IPhone or BlackBerry mobile users and devices. The concepts will be the same however; the methods used in the experimental design will be significantly different. The mobile forensic software used also will differ slightly, as certain software is better suited for Apple products over Android products.

The study also may not fully follow laws that would allow the data to be admissible in court. Certain parts of the study may cause some data to be modified or altered such as when bypassing a password lock on a mobile device. Most techniques used to bypass the lock require the use of making changes to the mobile device in terms of deleting the password lock file. Therefore, in a court of law there it may be a factor that could cause the forensic evidence to be thrown out. However, hopefully this study will show that if the only alternative is to make a small change to the system file in order to bypass the lock. Then that it should be allowed as a mobile forensic practice and be admissible in court.

5. Mobile Forensics Analysis

5.1 Android Background Information

It is important to learn and understand how the Android file system functions before diving into any forensic analysis. The Android system is based off Linux, where each file defines its own set rules for management and who is able to gain access to it. For example, the system files can only be accessed and modified by a root user. Any other user will not be able to access those files at all. This measure is in place by the operating system in order to keep the device secure from authorized access to system files. The last thing anyone wants is a phone that can be modified by any user and any person that uses it.

Android Debug mode will be used in this study, as it is a means for most developers to gain access to the mobile device. There are sections that a normal user will not have access too. In the case of Debug mode, it was specifically made for developers so they could test out their custom made applications. Android Debug mode also known as ADB is used by developers for software support.

Additionally, physical extraction will also take place, which is a bit by bit copy that not only includes allocated data. But, also all unallocated data where deleted files may be present. This will be used in the study, as it will allow for the use of finding hidden or deleted information on the mobile devices. File carving is a method known to be used to uncover data. It also allows for recovering deleted

or hidden data on a storage device. Some of the forensic tools presented in this study will have the capability to help the analyst file carve through lots of data.

Data is stored in partitions and each partition has its own role.

Partitions on an Android device

system	Has bulk of the platform including the root filesystem
boot	default bootimage
recovery	Recover boot image
cache	Could store temporary app data
misc	Some say it is for controlling device modes etc .Not very clear
data	contains user installed apps and data for the apps.

Figure 5.1

5.2 Phase 1 – Android Devices to be studied

Figure 5.2

For the purpose of this study a few different devices were used in the experiment. The primary devices used were a Samsung Galaxy Note 2 and a Samsung Galaxy S3 mobile device. A few secondary devices were also used such as two Motorola Razors. For a small portion of breaking lock codes a few older Motorola Razor mobile devices were used. Though the Motorola devices are not Android based, they were used to study the actual concept of being able to bypass locked mobile devices. Fortunately, data was already present on all of the devices, and therefore, no data needed to be populated manually. Many apps were already pre-existing, as it made known by the previous owners that there would be some form of residual data present.

5.3 Phase 2 – Obtaining the Device

Figure 5.3

The device was 60% charged and acquired from a forensic lab. It was placed in Airplane mode and was placed in a faraday bag. This prevents the device from connecting to its carrier network or any other network. The device then was transferred to a personal lab that was setup with various types of forensic software. Another reason why this step is necessary is so that the mobile device cannot be remotely wiped by someone. If there is a steady network connection, then someone such as the device owner could potentially remotely wipe the mobile device. And, this would make recovery of any forensic data much more difficult if not impossible.

Figure 5.3.1

The faraday bag is shown in Figure 5.3, and the mobile device was placed into the bag. Each mobile device that was tested was placed into this Faraday bag. This was to be sure it would not be able to reach or connect to any type of carrier network connection what so ever.

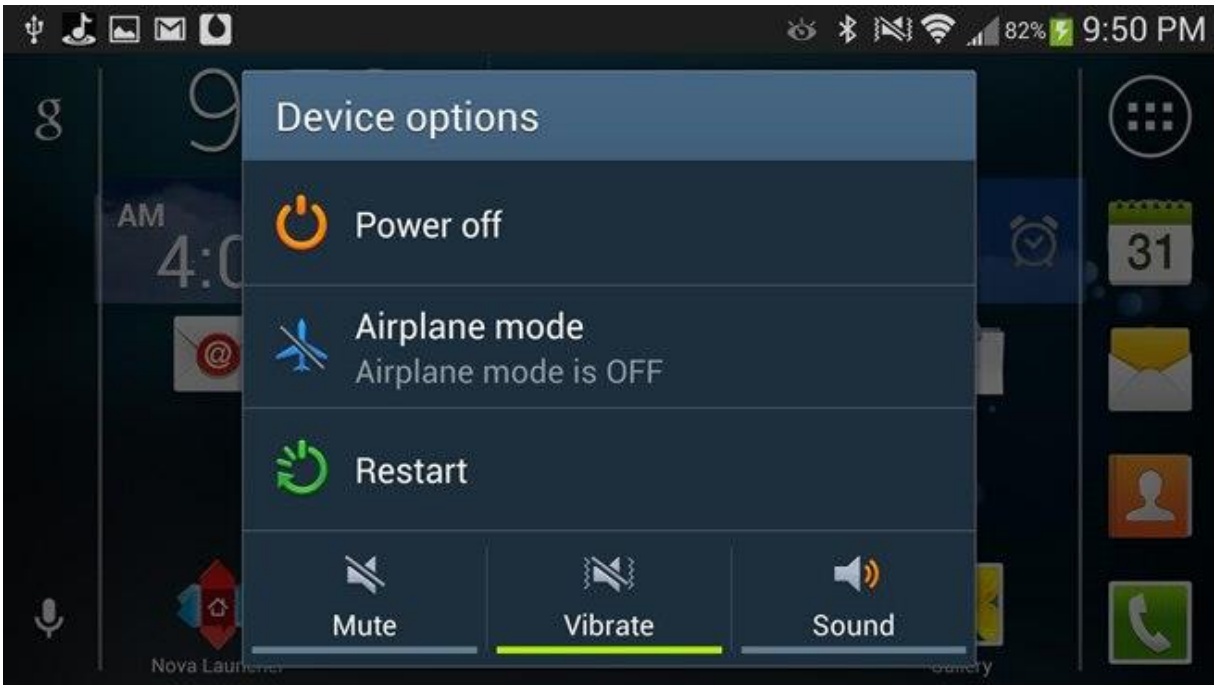


Figure 5.3.2

Also, to be extra cautious, the device was also put into Airplane mode. This mode can be enabled even if the device is locked, as no password or pass lock credentials is needed. You may simply hold down the power button till a “Device options” menu pops up as shown in Figure 5.3.2. From here clicking on the Airplane mode button puts it into Airplane mode. And, this will disable all network connectivity on the mobile device including Bluetooth, Wi-Fi and Data.

5.4 Phase 3 – Analyzing the Device

In this stage a dew different types of forensic software tools were used to extract information from the devices. The tools also were used to break into locked phones, and to gain access to the device. The tools that were used are Andriller, Cellebrite, MobilEDIT and Oxygen Forensics. The study will be able to uncover which tools were able to gain the most information. But, also will allow an analyst to verify the integrity of the data and, that the information found was also found by another forensic tool.

5.4.1 Andriller Analysis

Andriller is a fairly new forensic tool that has been released recently. It was created by a single developer as a project for fun, but slowly has led to becoming one of the cheapest priced and efficient android forensic tools out on the market. The software has a free trial for thirty days to really see how the software functions. For this tool to function you must have a rooted mobile android device. Or, a mobile device that has USB debug mode enabled. Otherwise, Andriller will not work unless and give out an error message till one of the requirements is met. In the case of this study we are assuming that USB Debug mode is enabled on the device when it is acquired.

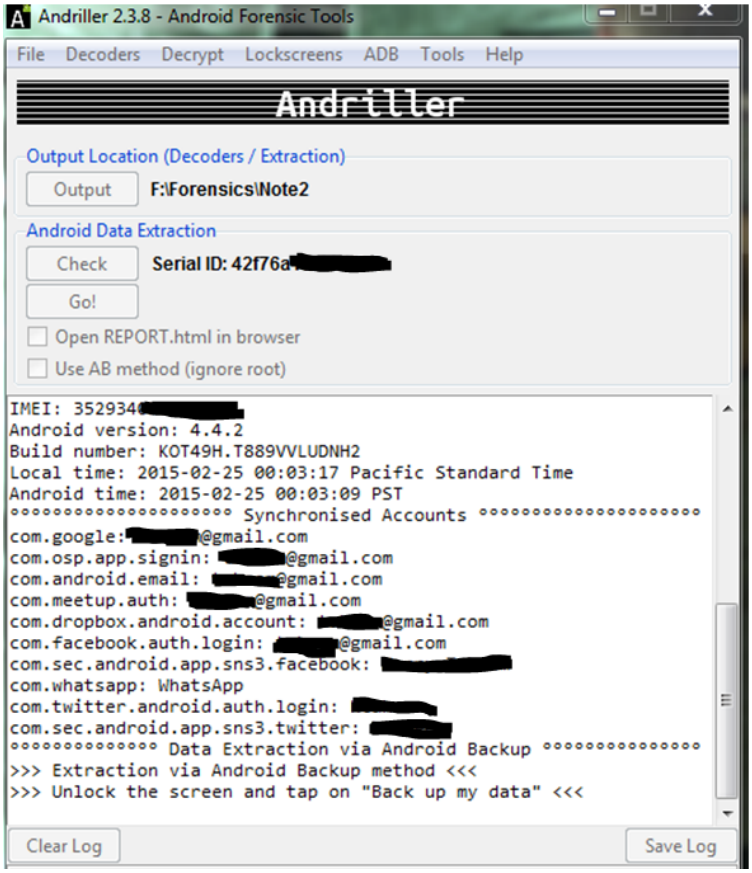


Figure 5.4

The software will list all the processes as it goes along scanning and extracting all of the information. Some of the information has been hidden in order to protect the privacy of the device owners. The concept however still remains the same for any other device that has any information extracted through Andriller.

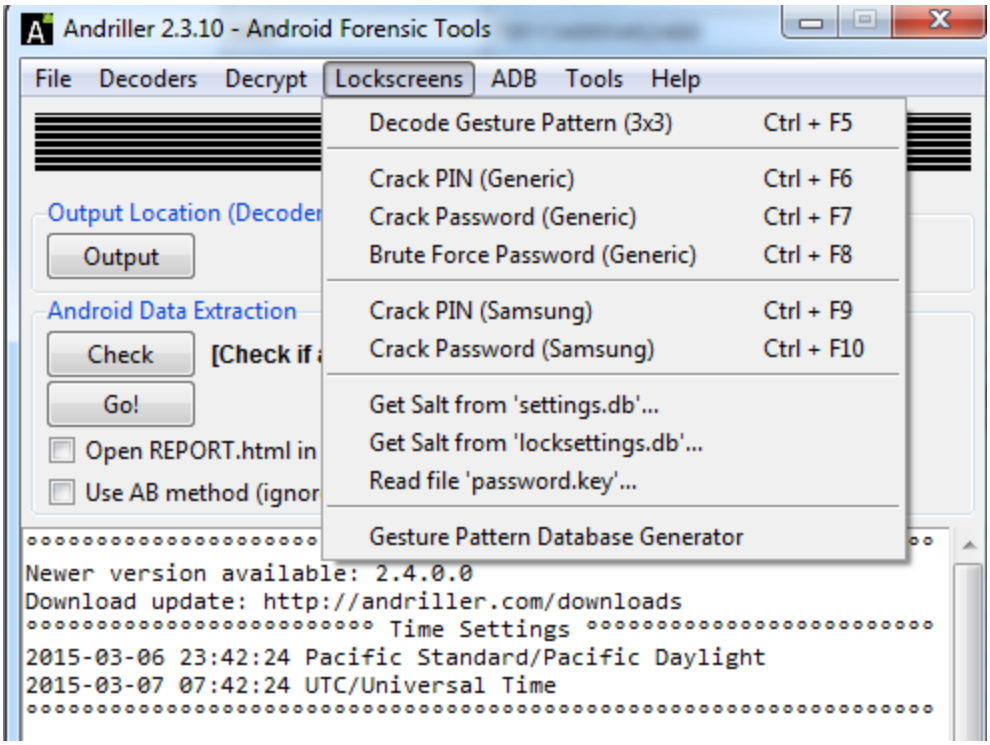


Figure 5.4.1

Andriller is able to break through locked screens with a password, gesture patterns, or PIN's enabled. Most mobile devices these days will have some sort of lock on it to prevent unauthorized access. However, if the phone is rooted, then Andriller is able to crack and break into the mobile device. In the case of this study we do not have root access to any of the mobile devices. Therefore, there will be no method to test or analyze any of the lock screen bypassing tools as shown in Figure 5.4.1. However, if there was root access, the analyst would be able to download the appropriate password.key or gesture.key files. These files then would be loaded into Andriller and allow the software to run different patterns and selections till it finds the correct gesture, PIN code or password that device owner has assigned or normally uses.

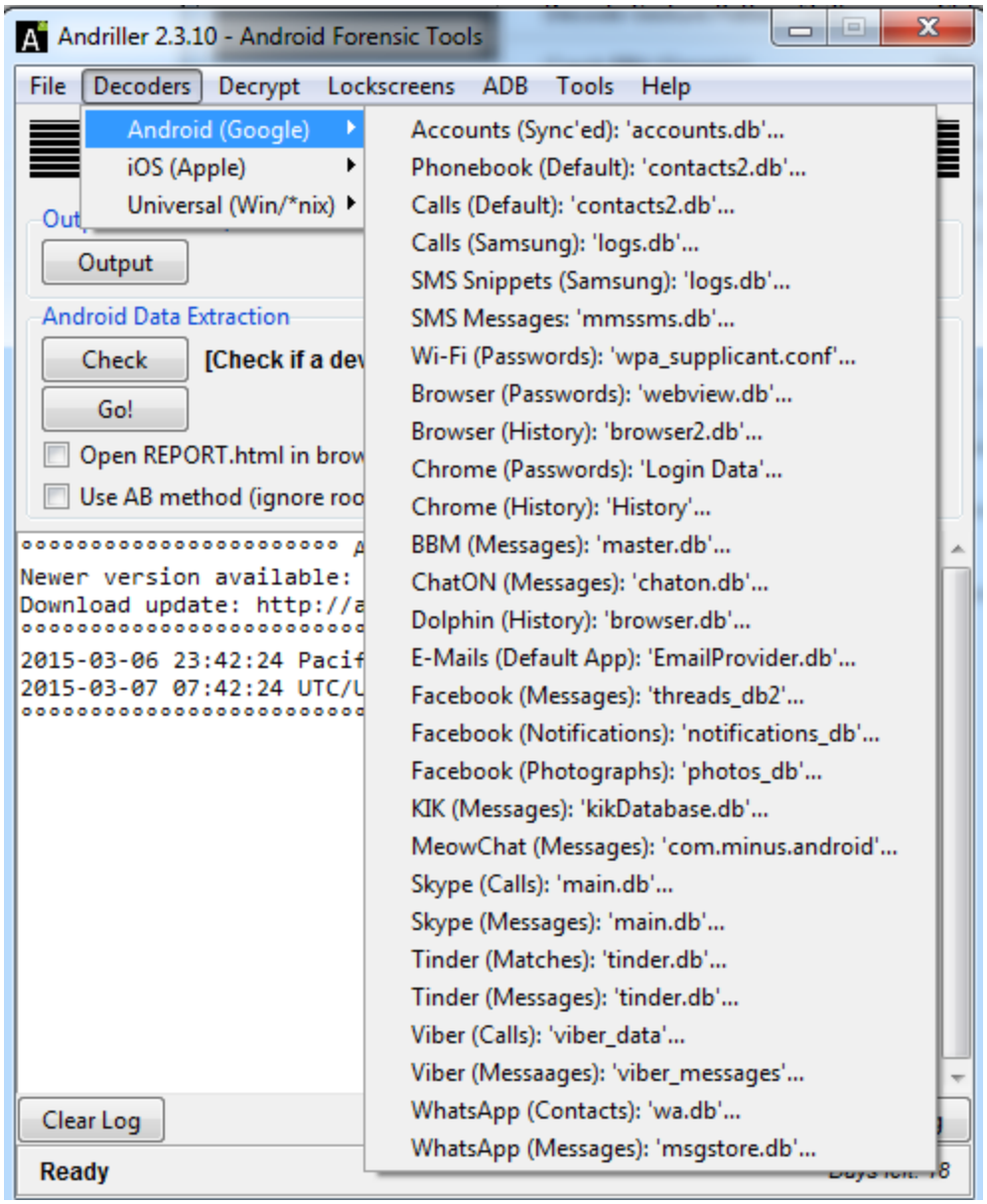


Figure 5.4.2

Figure 5.4.2 shows the list of applications that Andriller is able to decode and extract off a mobile device. However, not all of them can be extracted, as some applications will need root access. In the case of this study ADB, which is also known as USB debug mode access is used and the phone is not rooted. This means that only certain application data will be extracted depending on what type of access is needed to obtain the information. For example, WhatsApp chat messages may be extracted, however, since there is no root access to grab the encryption keys from the system files. The forensic tool will not be able to decrypt the WhatsApp chat logs.

In order to run the analysis, the mobile device is connected through a USB connection from the mobile device to the PC. Andriller is run on the PC and the “Check” button is clicked to verify that Andriller can connect to the mobile device. From there once the device is recognized it will list RSA key as shown in figure 5.4.2. This occurs so the PC and mobile device can create a secure connection. And, it allows the analyst to gain comfort in knowing the transmission is secure and specifically between only the PC and mobile device.

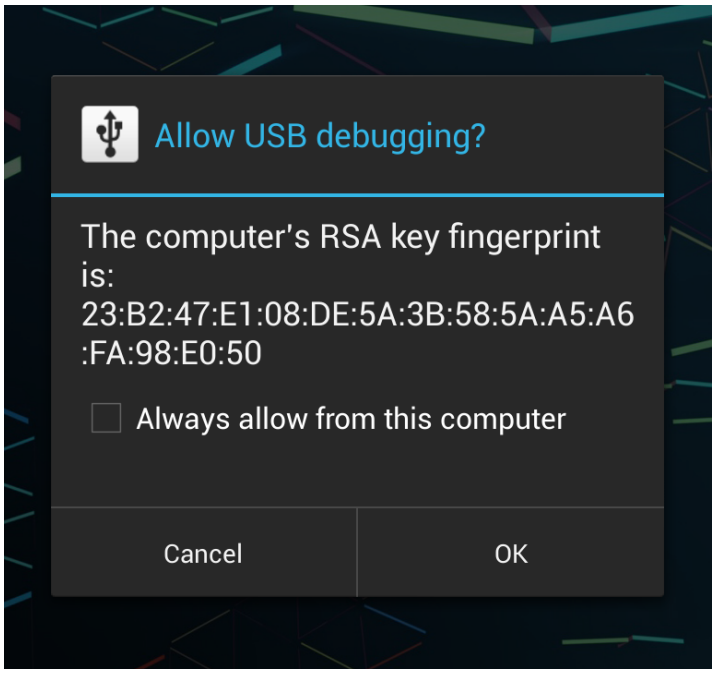


Figure 5.4.3

Click okay to allow the PC machine to connect to the mobile device through USB debug mode. Now, going back to Andriller, the “Go” button is clicked on to start the extraction process. All of the information from the mobile device now will slowly get extracted, as the process will take quite a lot of time. Once the extraction process has fully completed a completed message will appear on Andriller.

 # This report was generated using Andriller version 2.3.8 on 2015-01-25 00:03:17 Pacific Standard Time #

[Andriller Report] SAMSUNG SGH-T889V | IMEI:785134965462486

Type	Data
ADB serial:	42f88a1699fe9fe7
Shell permissions:	shell
Manufacturer:	SAMSUNG
Model:	SGH-T889V
IMEI:	785134965462486
Android version:	4.4.2
Build name:	KOT49H.T889VVLUDNH2
Local time:	2015-01-25 00:03:17 Pacific Standard Time
Android time:	2015-01-25 00:03:09 PST
Accounts:	com.google: vancouver_hitman@gmail.com com.osp.app.signin: vancouver_hitman@gmail.com com.android.email: vancouver_hitman@gmail.com com.meetup.auth: vancouver_hitman@gmail.com com.dropbox.android.account: vancouver@gmail.com com.facebook.auth.login: vancouver_hitman@gmail.com com.sec.android.app.sns3.facebook: Henry Wilson com.whatsapp: WhatsApp com.twitter.android.auth.login: hwilson com.sec.android.app.sns3.twitter: hwilson
System:	Wi-Fi Passwords (7)
Web browser:	Android Web Browser History (119)
Android E-mail:	Android E-mails (2)
Communications data:	Samsung SMS Snippets (479)
Applications data:	Tinder Matches (48)
Applications data:	Tinder Messages (662)

 # http://andriller.com #

Figure 5.4.4

Once Andriller completes its extraction it will present the analyst with a report page as shown in Figure 5.4.4. From here on the analyst can click on the links to view the detailed reports. The reports will also be shown further below in greater detail.

Wifi Passwords

 # This report was generated using Andriller #

[Wi-Fi Passwords]

SSID	Password	Management
Starbucks	Kingsway	WPA-PSK2
Home	password	WPA-PSK2
Admin's Network	llikecheese5467	WPA-PSK
7Y5HH	W3lc0m3t0H3ll23	WEP
BCITLab	m59dj58dutn5455	WPA-PSK2
Langara	L5nY7K3B449LoP	WPA-PSK2
Mayan Resort	Enj0yY0ur$tay4550	WPA-PSK2

http://andriller.com

Figure 5.4.5

Wifi passwords were found on all of the Samsung mobile devices. And, it seems that the passwords are not encrypted in any manner. The Wireless network name (SSID) is listed, as well as the password (pre-shared key). It also lists the type of encryption used for the wireless connection. Overall, this report shows that obtaining wireless passwords is fairly easy, and can allow you to enter into any of these wireless networks fairly easily. This makes it easier for a hacker to steal a mobile device, extract the Wi-Fi passwords. And, then potentially head out close to the device owners home to connect to their wireless network. After that, the hacker could potentially run all sorts of attacks on the network, or even sniff out all of the network data. Sniffing network data simple refers to the fact that someone is able to read all data that is sent through the network. So usernames, passwords, credit card numbers and other valuable personal information could potentially be stolen and obtained by the hacker.

Browsing History

 # This report was generated using Andriller #

[Android Web Browser History]

Page title	URL	Time	Frequency
Celeb Star Signs: Gemini	http://www.chacha.com/gallery/1949/celeb-star.....urus/14916	2013-02-14 04:30:57 UTC	1
Celeb Star Signs: Gemini	http://www.chacha.com/gallery/1949/celeb-star.....urus/14915	2013-02-14 04:30:50 UTC	1
http://t.co/cltBmDTi	http://t.co/cltBmDTi	2013-02-14 04:29:48 UTC	2
Canucks Mobile	http://canucksmobile.com/streaming/geo_target.php	2013-02-10 04:00:59 UTC	1
Zoosk, The Romantic Social Network(™)	https://t.zoosk.com/mkt/000112/402/?from=AM_W.....ailypix.me	2013-02-09 00:26:53 UTC	2
http://t.co/sFjPRSRr	http://t.co/sFjPRSRr	2013-02-09 00:26:18 UTC	2
Vancouver, Canada Tomorrow's Weather Forecast - AccuWea.....	http://m.accuweather.com/en/ca/vancouver/v5z/.....2&p=samand	2013-02-09 00:20:56 UTC	5
Vancouver, Canada Daily Weather Forecast - AccuWeather.com	http://m.accuweather.com/en/ca/vancouver/v5z/.....3&p=samand	2013-02-09 00:20:55 UTC	3
Vancouver, Canada Current Weather Report - AccuWeather.com	http://m.accuweather.com/en/ca/vancouver/v5z/.....6?p=samand	2013-02-09 00:20:54 UTC	3
Windows 8 no mouse response desktop and IE 10	http://social.technet.microsoft.com/Forums/en.....59fc00b351	2013-02-08 19:08:08 UTC	3
Chrysler Canada | Home of Chrysler, Jeep, Dodge, RAM	http://www.chrysleroffers.ca/mobile/en?utm_ca.....320_50_NID	2013-02-07 06:03:14 UTC	2

Figure 5.4.6

Andriller is also able to find and include web browser history in its report. This report is from all browser types, such as the default Samsung browser, as well as Google Chrome, Firefox and many others. The report lists the Website Page Title, the URL to that website, the time it was last accessed, and the frequency of times the page was visited by the user. This information would be very useful for forensic investigations if someone was visiting a particular website relating to certain subject matter pertaining to a case.

Android Emails

 # This report was generated using Andriller #

[Android E-mails]

Protocol	Address	Port	Login	Password
imap	imap.gmail.com	993	vancouver_hitman@gmail.com	B9F6PFP0oPK+wbL15tElsS==
smtp	smtp.gmail.com	465	vancouver_hitman@gmail.com	B9F6PFP0oPK+wbL15tElsS==

#	From	To	Subject	Content (snippet)	Attachments	Time
27	vancouver_hitman@gmail.com Henry WIlson	gossipgurl99@gmail.com	(no subject)	Sent from Samsung Mobile	content://media/external/images/media/164	2013-02-24 11:55:37 UTC
26	vancouver_hitman@gmail.com Henry Wilson	gossipgurl99@gmail.com	(no subject)	Sent from Samsung Mobile	content://media/external/images/media/135	2013-01-15 00:33:38 UTC

Figure 5.4.7

Andriller also has a report on all of the email accounts on the mobile device. As well as the emails recently sent and received by the user. The details in the report are listed with the sender and recipients email addresses, the content of the email, any attachments that were included, and the time it was sent or received.

SMS - Text Messages

 # This report was generated using Andriller #

[Samsung SMS Snippets]

#	Number	Name	Snippet	Type	Time
12762	+17787776590	Jake	Hahahaha	Inbox	2015-02-25 01:23:34 UTC
12761	+17787776590	Jack	Let's fight today, Metro town station midnight!	Sent	2015-02-25 01:17:06 UTC
12755	6045635522	Dr Chod	I just left you a message (18s). Call 00021 to lis	Inbox	2015-02-23 21:16:09 UTC
12750	6044350699		I just left you a message (13s). Call 00025 to lis	Inbox	2015-02-22 23:54:42 UTC
12746	+17783458150		No just sell them	Inbox	2015-02-22 07:26:36 UTC
12745	7783458150		Hi do you also rotate and change tires	Sent	2015-02-22 07:16:51 UTC
12742	+16048373921	Mom	Come home for dinner I made KFC finger licking good.....	Sent	2015-02-22 03:44:37 UTC
12722	+16043373493	Homie J	I got the weed and guns you wanted homie	Sent	2015-02-15 02:12:13 UTC

Figure 5.4.8

There is a report also generated for all SMS - Text messages on the mobile devices. The report lists the phone number, the context of the text messages, as well as if it was sent or received, and at what time. This allows a forensic analyst to map out relationships with the mobile device owner with the contacts.

Tinder - Matches

 # This report was generated using Andriller #

[Tinder Matches]

Picture	Name	Gender	User ID	When Matched	Last Activity
	Linda	Female	53cc97dfb94rt19c384900b3	2014-08-17 17:23:53	2014-11-25 03:05:45
	Jasmine	Female	53e3cd8c8c3dh78d0504d956	2014-08-17 17:32:52	2014-08-20 06:44:41
	Alanna	Female	5295384dgk58171467000054	2014-08-21 03:18:20	2014-08-21 06:04:58
	Kala	Female	532ec763fg8b7df45b000bbf	2014-09-01 08:32:20	2014-09-04 05:48:33
	Taryn	Female	5340dd9dg6hjb9be11002671	2015-02-09 21:38:38	2015-02-18 01:53:56

Figure 5.4.9

Andriller was able to extract information from Tinder, a dating application used by the user. It lists the pictures of matches the user got, the name of the person, when they matched and were last active on the application. The important part here is the User ID, as it could be used to target individuals through the Tinder systems. And, it could pose as a security risk for these Tinder matches. Additionally, there have been many cases of abuse, kidnap or rape from women that have used this app. Therefore, by being able to extract and recover forensic data on Tinder matches and chats. Law enforcement would have some evidence to back up a case where a woman might have been abuse by someone she met on Tinder.

Tinder – Conversations

 # This report was generated using Andriller #

[Tinder Messages]

From (sender)	Matched with	Message	Time (Local)
Jason (ID:53efe3fl768f2db149be1635)	**Linda** (ID:53cc97f5b94b9k40u84900b3)	BLOCK*	2014-11-25 03:05:45
Jason (ID:53efe3fl768f2db149be1635)	**Linda** (ID:53cc97f5b94b9k40u84900b3)	Glrl call me gangstaz!	2014-08-18 05:51:13
Linda (ID:53cc97f5b94b9k40u84900b3)	**Linda** (ID:53cc97f5b94b9k40u84900b3)	So many gangsters on tinder!	2014-08-18 05:24:35
Linda (ID:53cc97f5b94b9k40u84900b3)	**Linda** (ID:53cc97f5b94b9k40u84900b3)	Hi Jason	2014-08-18 05:24:16
Jason (ID:53efe3fl768f2db149be1635)	**Linda** (ID:53cc97f5b94b9k40u84900b3)	Hey Linda. So listen u n me weed 420 dat shit in ma car! yeaaaaaaa	2014-08-18 03:16:15
Jason (ID:53efe3fl768f2db149be1635))	**Jasmine** (ID:53e3cd8c8ck5978d0504d956)	What you up to now did the boss let you out or did you break out!	2014-08-20 06:44:41
Jason (ID:53efe3fl768f2db149be1635)	**Jasmine** (ID:53e3cd8c8ck5978d0504d956)	damn gurl u work? I sit at da crib be playin ma playstation 4	2014-08-20 06:44:17
Jasmine (ID:53e3cd8c8ck5978d0504d956)	**Jasmine** (ID:53e3cd8c8ck5978d0504d956)	Dude ive been busy with work	2014-08-20 06:43:06
Jason (ID:53efe3fl768f2db149be1635)	**Jasmine** (ID:53e3cd8c8ck5978d0504d956)	Omg your fake!	2014-08-20 06:40:56

Figure 5.4.10

Lastly, the report also included information regarding not only the Tinder matches. But, all of the conversations the user has on Tinder with the name of the match, the message and times it was sent or received. This type of information once again could be seen and viewed as valuable information in a forensic investigation for law enforcement.

Short Falls

One major short fall is that Andriller can only extract information if you actually have access to it. By that, it means you must be able to get past the locked screen (password, gesture, PIN code etc...). Otherwise, the software cannot extract any data at all, as it either needs debug mode enabled or root access on the mobile device. And, the only method to enable debug mode is to already have access to the devices menu. The only other way data can be extracted is if the device has been rooted. If the device is rooted, then Andriller is able to obtain the maximum amount of data, which essentially is just about everything on the mobile device.

For future improvements, one wish would be that the software is able to automatically able to gain root access to the mobile device. It would provide a most useful feature, and would make this one of the best Android Mobile forensic tools out there. If Andriller can root a device, then the software can gain pure access to the whole device and all parts of it without any access limitations or restrictions. Lastly, Andriller

should add in a database viewer, so that an analyst is able to sift through any application data that may have no report generated on it.

5.4.2 MobilEDIT Analysis

MobilEDIT is known more for its capabilities to provide backup solutions for mobile devices. However, there is an extended edition which also provides forensic tools for law enforcement and forensic analysts.

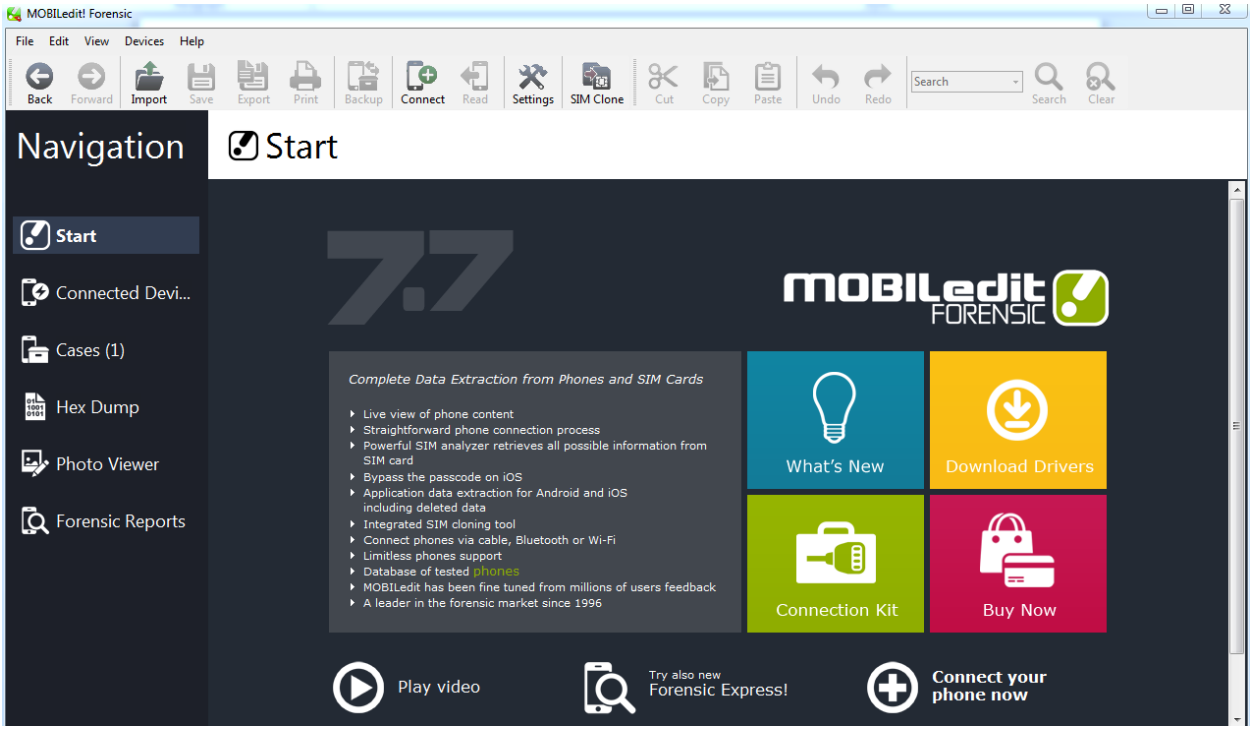


Figure 5.4.11

When MobilEDIT is opened it will display many options as shown in Figure 5.4.11. Once the mobile device has been plugged into the PC USB device. The next step is to click on “Connect your phone now”, and this will start the extraction process.

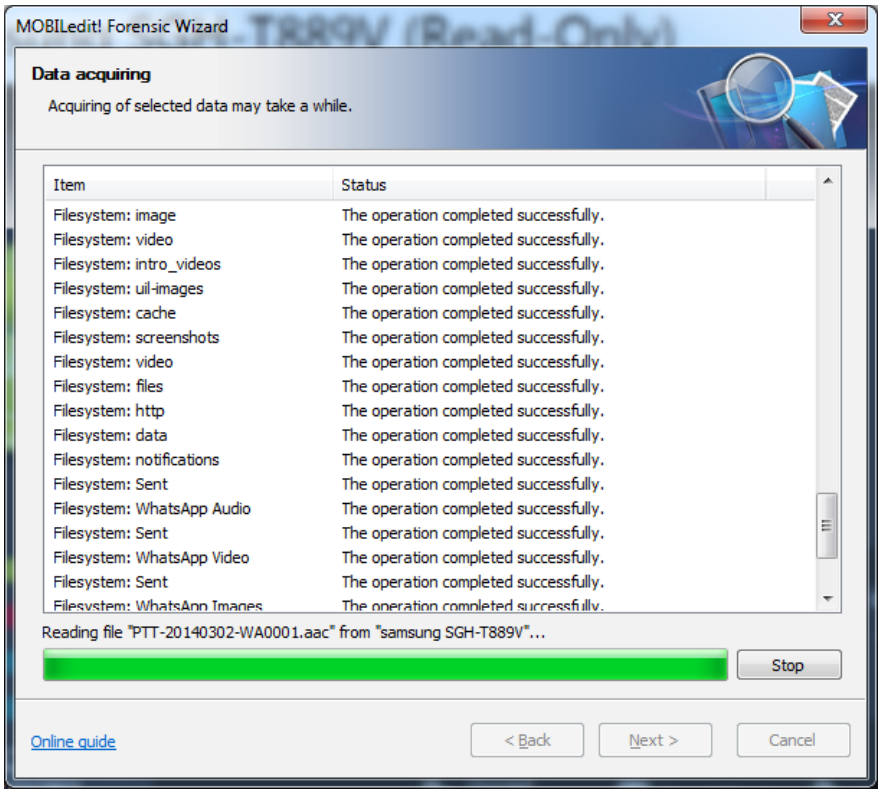


Figure 5.4.12

As the extraction takes place details will be listed of the types of items, files, folders and applications that are being extracted from the mobile device. This process will take quite a lot of time, as the forensic tool will dive deep into the mobile device to grab as much data as it can access and reach. The more data that is on the mobile device, the longer it will take to extract it. For example, if there are many emails stored on the device with large attachments. Then the extraction process will take much longer, as it has to extract all of the large attachments along with the emails. Many chat logs also for applications such as WhatsApp are fairly large. Therefore, the extraction process can take a large amount of time to complete.

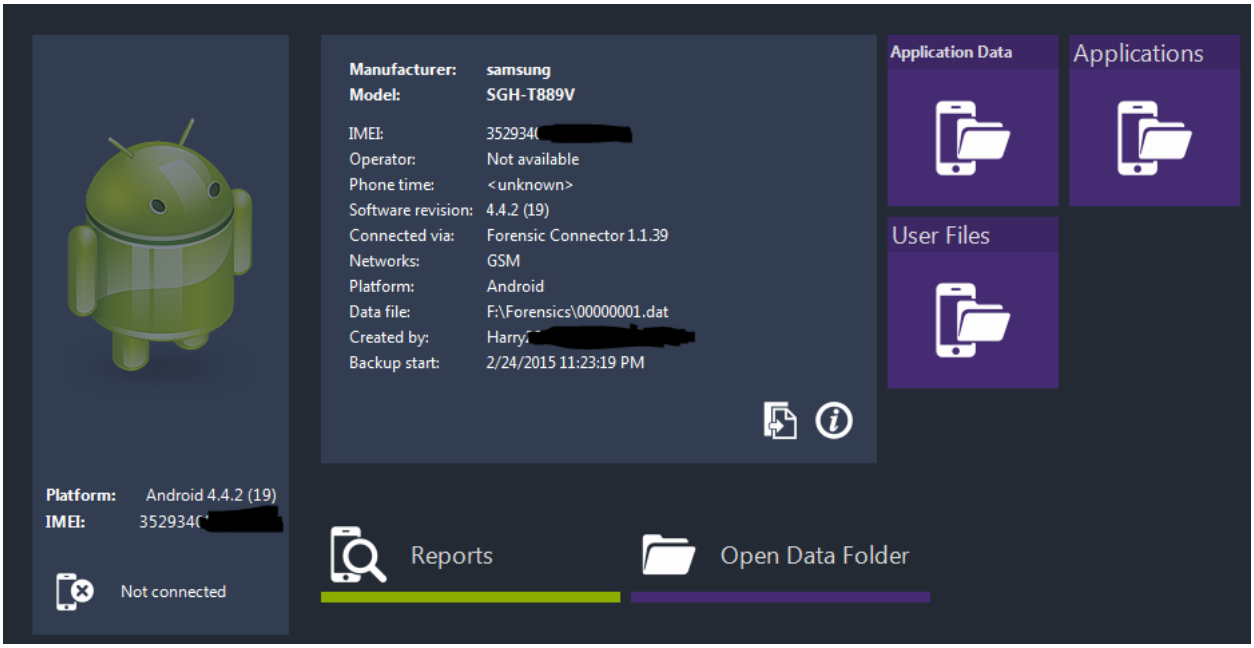


Figure 5.4.13

Once all of the data has been extracted from the mobile and the process has completed. The analysis page will pop up displaying information about the mobile device as shown in Figure 5.4.13. From here the User Files button is selected to view files on the device.

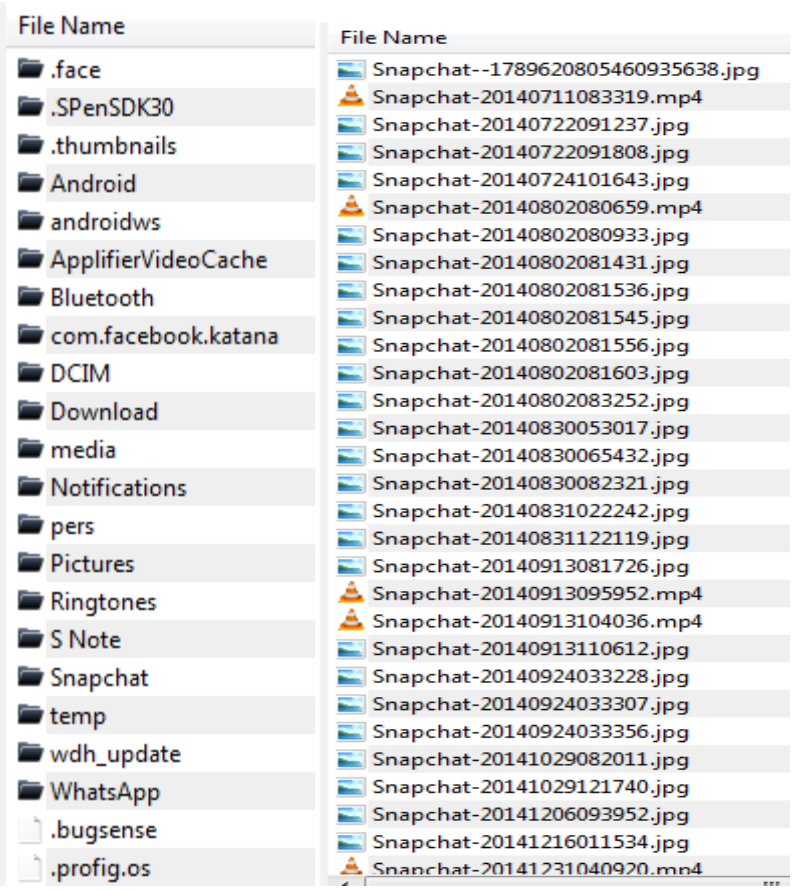


Figure 5.4.14

The User Files shows a list of folders and data that was extracted from the mobile device. As an example, the Snapchat application folder was selected. Once within the folder a list of images and videos can be seen. And, these images and videos can be opened up to be viewed for any type of evidence.

Applications

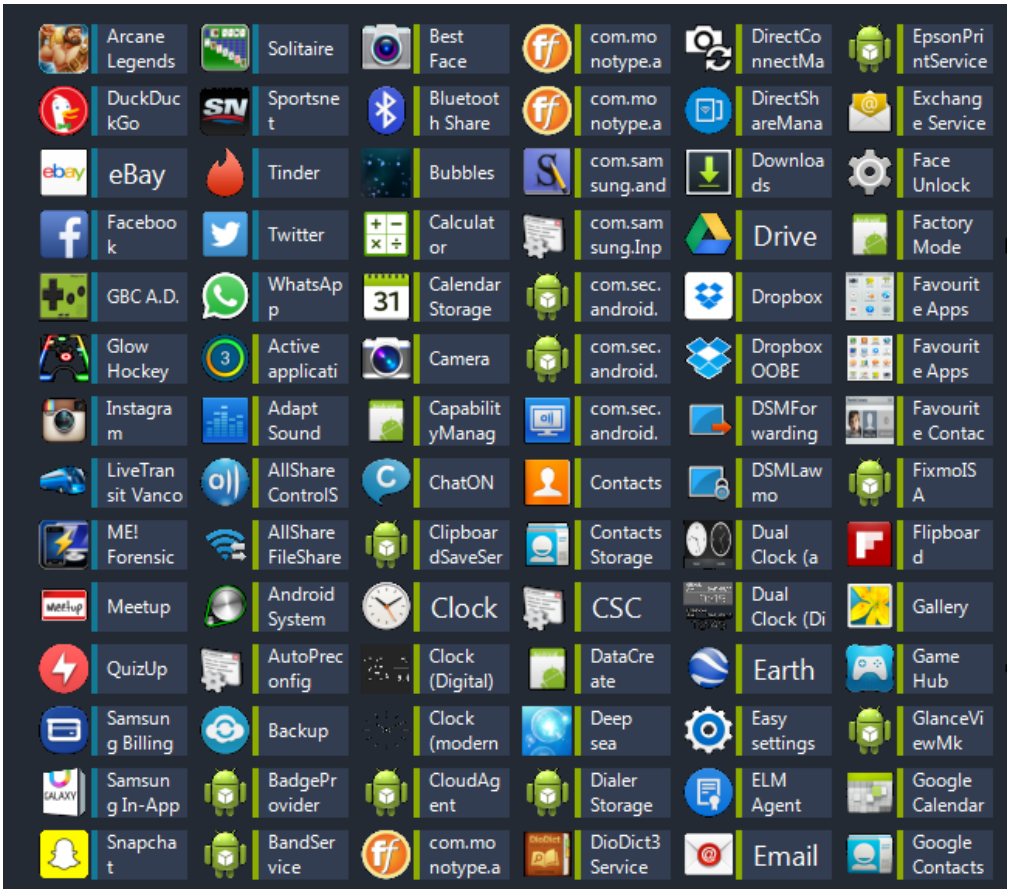


Figure 5.4.15

Clicking on the Applications button will display a list of all applications on the device as shown in Figure 5.4.15. And, all of these apps can be backed up for safe keeping. The purpose here is to understand what types of applications reside on the device, as it will lead the analyst to further dig out information on select or all apps. The analyst may be looking for a specific type of application. This option makes a great way to map out the applications and possible type of information on the mobile device.

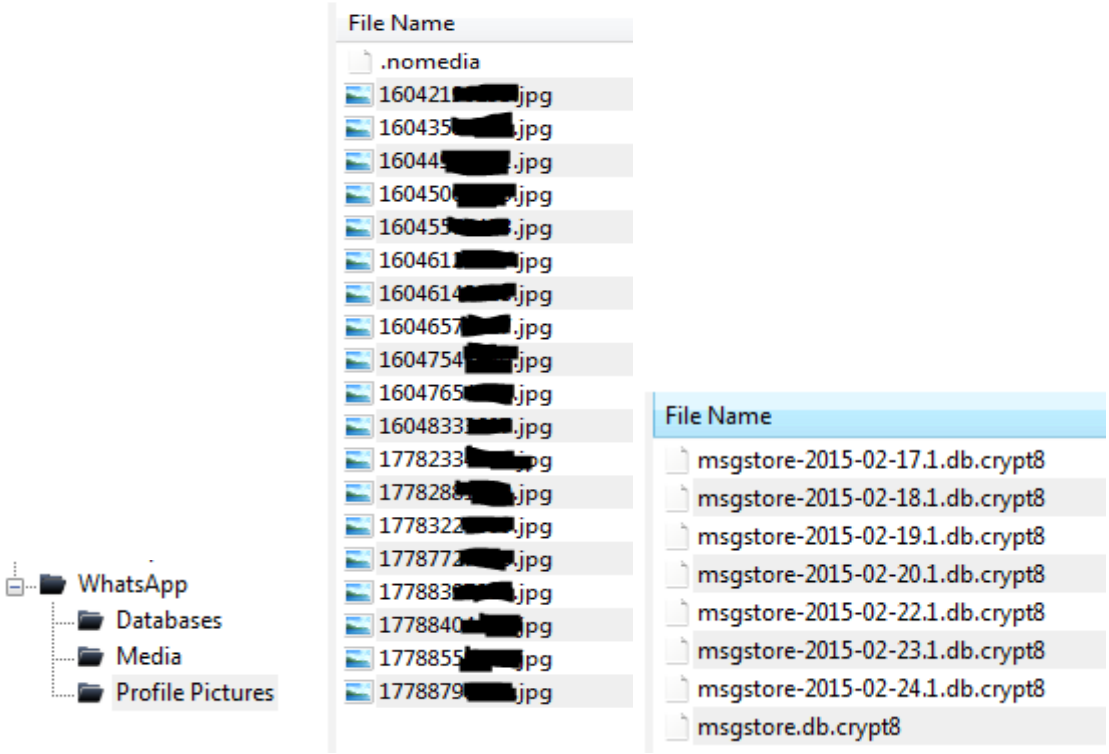


Figure 5.4.16

Another application that showed up is called WhatsApp. The profile pictures of the users contact members are stored on the device. Therefore, an analyst would be able to possibly get a visual on who the user interacted with on WhatsApp. The biggest issue is that the WhatsApp chat logs are all encrypted, and cannot be read by any normal database viewer. In this case the WhatsApp encrypted logs cannot provide much help. However, if you mix muliple tools such as Andriller and MobilEDIT. Then the analyst may be able to decrypt the WhatsApp chats, as Andriller provides the capability to decypt WhatsApp messages. Though the analyst will need root access to obtain the msgstore files and the encrypted key file from the device.

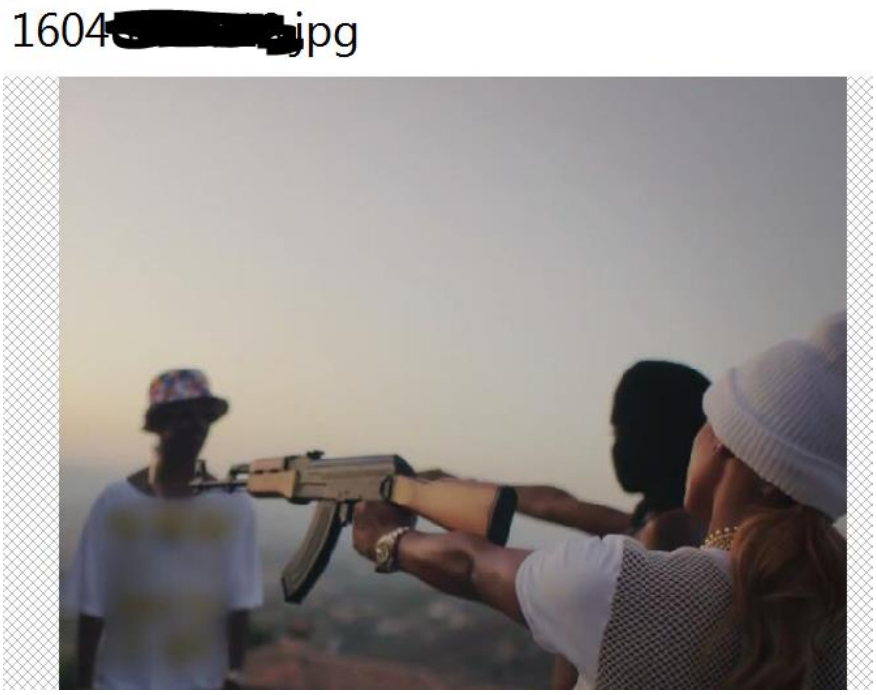


Figure 5.4.17

Even though the chat logs are encrypted, the profile pictures are not. And, this can still be used as good evidence. The pictures are also named with the convention of the contacts phone number. Therefore, the image can always be traced back to a phone number being used on WhatsApp. In the example of Figure 5.4.17, the number was hidden for privacy reasons.

Short falls

Similarly to all of the other mobile forensic tools, MOBILedit also needs USB debug mode enabled or a rooted mobile device. Otherwise, it cannot perform any useful tasks such as extracting any important data off a mobile device. Therefore, the device has to be rooted or in debug mode. And, many mobile devices will not incorporate either of those methods by default. There is no database viewer though an analyst can view the physically extracted information in a HEX editor. But, a database viewer would be ideal to make it easier for an analyst to be able to dig deeper into the databases of each application. Overall, this forensic tool is best for creating backups of mobile devices. As it is fairly limited in its forensic capabilities for anyone that would wish to perform major forensic techniques.

5.4.3 Cellebrite

One of the better and more efficient forensic tools out on the market is called Cellebrite. This is a tool that seems to be widely used by law enforcement, as well as by many top forensic businesses and companies. The more positive thought regarding Cellebrite is that it does have a list of all of the supported phones and models the device supports. Cellebrite is also known to be able to bypass locked phones and can break into devices to gain access. Law enforcement at times may have no way to get the password or unlock codes to mobile devices. Therefore, a tool like Cellebrite comes in handy to gain access to the device and extract important information. The Cellebrite device used in this study is not the current version. As there is a newer UFED device released by Cellebrite. Therefore, the study will have some limitations with Cellebrite gathering data on the newer mobile devices.

Figure 5.4.18

Figure 5.4.19

The Cellebrite device has access to all types of USB to phone connectors. There is a USB wire provided by Cellebrite for practically every type of mobile device out on the market. The mobile forensic device can save extracted data to a USB for viewing on a normal computer machine. This way data extraction can be done on the spot rather than having to take the mobile device into a lab. Cellebrite provides practically every possible USB wire to connect any mobile device with its forensic device. In the case of this study wire #100 was used to connect to the Samsung S3 and Note 2 devices.

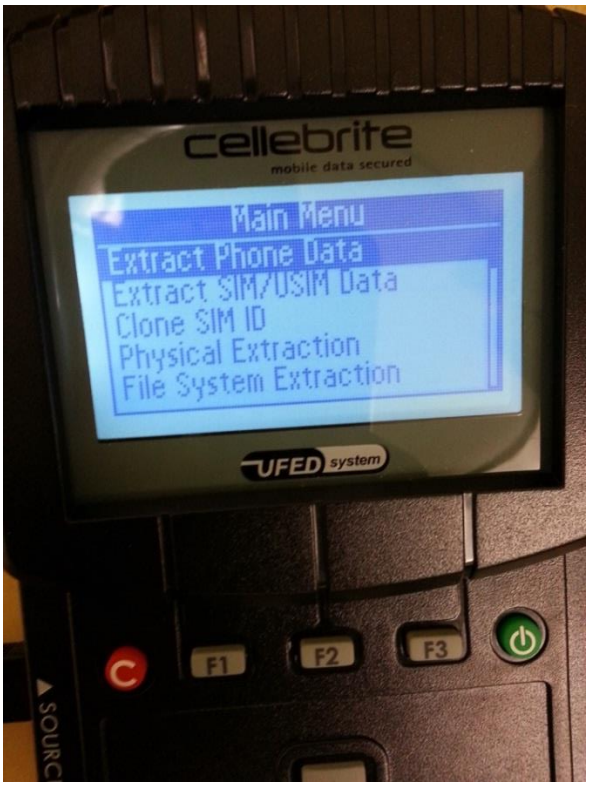


Figure 5.4.20

Once the Cellebrite UFED device has been turned on, a menu will appear on the screen. The steps to connect a mobile device to the Cellebrite device are fairly straight forward. The first step is to connect the mobile device to the Source connection on the Cellebrite device via USB. The second step is to insert a USB drive on the Target port of the Cellebrite device. The important factor here is that the USB drive is equal to or larger than the size of the mobile devices internal storage drive. An easy way to identify the size of the internal storage drive is to take out the batter cover and battery. Below the battery, there is information listing the model number. If the model number is searched on Google, it will lead to a specifications website, which will list all of the details regarding the mobile device. In the case of this study, a 64GB DURACELL USB drive was used to store all of the extracted data from the mobile device.

Figure 5.4.21

In figure 5.4.21 the mobile device is an older Motorola Razr mobile device, which happens to use a 4 digit PIN to unlock the device and again access to it. Newer devices also use a PIN system, but now may use more than four numbers for a PIN. The password function was not supported for the Samsung S3 mobile device. Therefore, for the purpose of this study and general curiosity, the experiment was done with an older mobile device. The mobile device is connected once again via USB to the Cellebrite system. In the menu the “Password” option is selected. This then runs the password PIN scan, which will process and complete within a very short time frame.

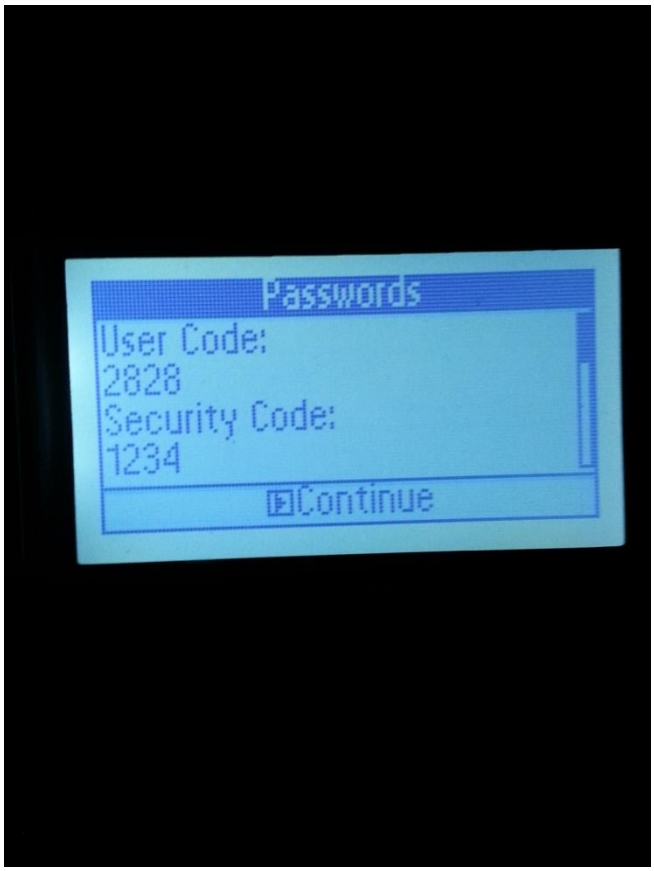


Figure 5.4.22

Once the PIN code has been found, it will display it on the Cellebrite device as the “User Code”. This can then be used to enter into the mobile device to gain access to it. Most new mobile devices do not just use a PIN any longer. And, therefore, this technique may no longer work for newer phones. The new types of pass locks are Gesture patterns, PIN’s and alphanumerical passwords.

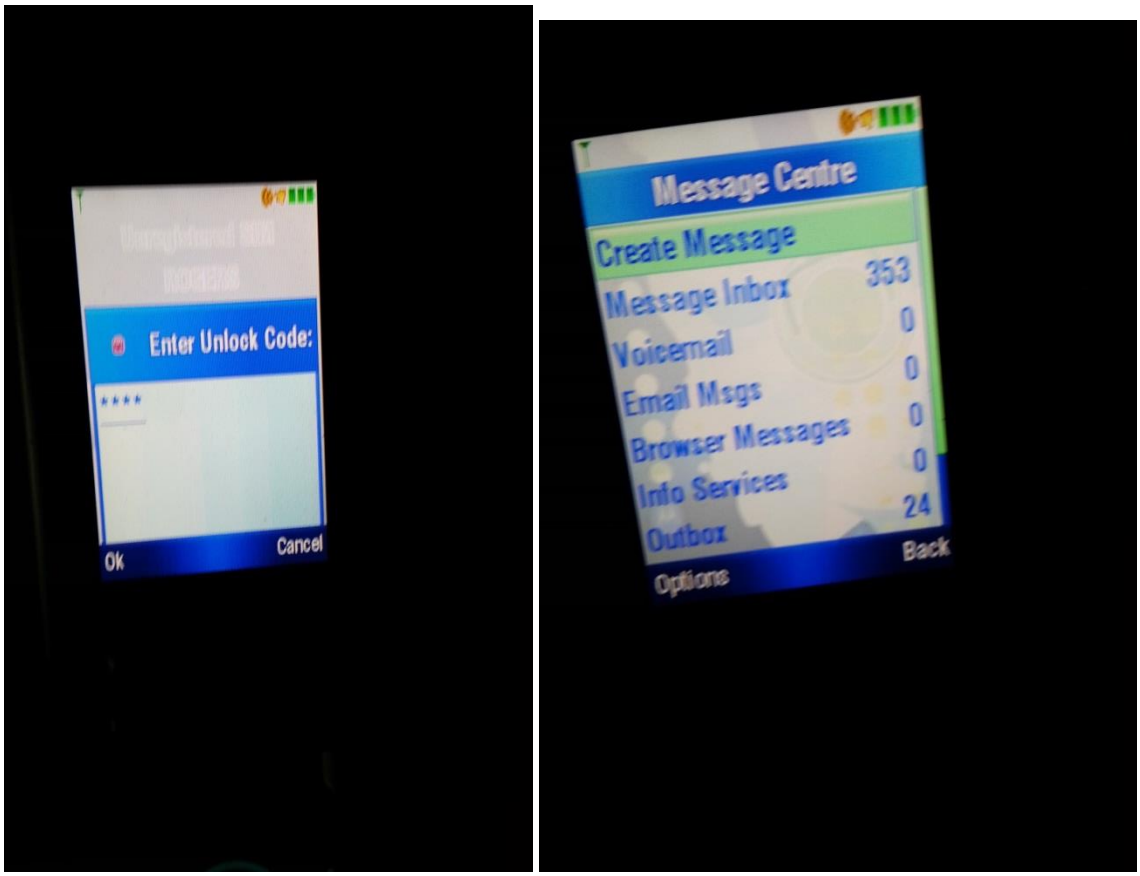


Figure 5.4.23

Now, the extracted PIN password can be entered into the mobile device. As it should now allow access to get through the PIN lock code. And, as Figure 5.4.23 , it shows access to the mobile device. Cellebrite was able to break through unlock PIN codes for older Motorola Razr phones. This then gives the forensic analyst access to the device, and allows them to enable USB or Debug mode on the mobile device. It also allows for being able to manually view the device data.

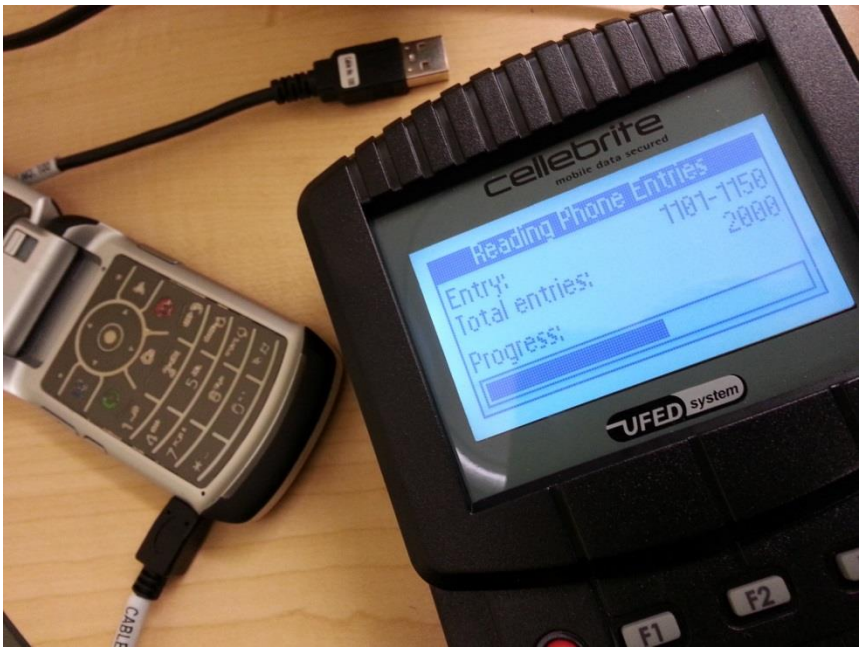


Figure 5.4.24

The device will also display the data progress bar as it is being extracted along with the total progress. Once the device has completed the extraction it will display a completed message. The next step is to take the USB drive and view the data on it from any computer machine that has a web browser.

Phone Examination Report Properties

Selected Manufacturer:	Samsung GSM
Selected Model:	SIII
Detected Manufacturer:	"Samsung"
Detected Model:	"MODEL=SIII"
Revision:	"JFJKN5_00.0E.00R"
MEID:	268435385411319326 (HEX: A4678002ACB81E)
GSM MIN:	6049255341
MDN:	6049255341
User Code:	8342
Extraction start date/time:	26/01/15 20:01:51
Extraction end date/time:	26/01/15 20:04:09
Phone Date/Time:	06/01/80 00:01:35 (GMT)
Connection Type:	USB Cable
UFED Version:	Software: 2.2.5.0 UFED , Full Image: 1.0.2.9 , Tiny Image: 1.0.2.1
UFED S/N:	5568592

Phone Examination Report Index

Contacts	Selected
SMS - Text Messages	Selected
Calendar/Notes/Tasks	Selected
Call Logs	Selected
MMS - Multimedia Messages	Not Supported
Email Messages	Not Supported
Instant Messages	Not Supported
Images	Selected
Ringtones	Selected
Audio	Selected
Video	Not Supported
Databases	Not Supported

Figure 5.4.25

Cellebrite will automatically generate a report onto a USB device. The information then can be viewed by opening the Report.html file with any web browser. It will load all of the relevant documents in a web browser for the analyst. It lists important information about the device itself, such as the model number, type, and other details. It also lists what type of information was extracted from the device, such as SMS test messages, contacts, call logs etc….

Phone Contact List

Phone Contacts

Total Entries: 12
PBB MD5 Hash: D479F53D6650901C8856AFB70CD1DC02
PBB SHA256 Hash: 34514FFD 95DE4EA 922586B 2FBB6E5 65806B3 CAB056C 58C4AEF 38D13DF ADC3340

#1	**Jake Evans** (Memory: Phone)
Mobile:	16042578896

#2	**Biggie** (Memory: Phone)
Mobile:	17789996327

#3	**Homie J** (Memory: Phone)
Mobile:	17789426678

#4	**Ralph** (Memory: Phone)
Mobile:	16048135744

#5	**Bj** (Memory: Phone)
Mobile:	16044753899

Figure 5.4.26

A list of all phone contacts is shown in a separate report indicating the names and numbers of all contacts on the mobile device. The details are very brief, but it allows for a forensic analyst to map out contacts and phone numbers.

SMS – Text Messages

Phone SMS - Text Messages

SMS MD5 Hash: 53363621FCF102C42C0D1CB8AA3A3AEC

SMS SHA256 Hash: ADE55AB0 B2F10B4 D7F8D9A 83BE7B1 B4AC39A 6957909 B3E708E 8EA44F3 907660C

#	Number	Name	Date & Time	SMSC	Status	Folder	Storage	Type	Text
1	17787776590	Jake	N/A		Inbox	Inbox	Unknown	Incoming	Hahahaha
2	17787776590	Jack	N/A		Sent	Sent	Unknown	Outgoing	Let's fight today, Metro town station midnight!
3	6045633522	Dr Chod	N/A		Inbox	Inbix	Unknown	Incoming	I just left you a message (18s). Call 00021 to lis
4	6044350699	N/A	N/A		Inbox	Inbox	Unknown	Incoming	I just left you a message (13s). Call 00025 to lis
5	+17783458150	N/A	N/A		Inbox	Inbox	Unknown	Incoming	No just sell them
6	7783458150	N/A	N/A		Sent	Sent	Unknown	Outgoing	Hi do you also rotate and change tires
7	16048373921	Mom	N/A		Sent	Sent	Unknown	Outgoing	Come home for dinner I made KFC finger licking good....
8	16043373493	Homie J	N/A		Sent	Sent	Unknown	Outgoing	I got the weed and guns you wanted homie

Figure 5.4.27

A list of all SMS text messages is shown in a separate report indicating the names, phone numbers, if the text is incoming or outgoing, and content of the text messages on the mobile device.

Images

Images

#	Information	MetaData	Image
1	File Name: Photo 0001.jpg File Path: picture File Size: 66927 Bytes File Date/Time: 17/12/14 17:33:05 MD5: 6A684141A7295006E122F285F70AD112 SHA256: 5EE11C0A 94558E2 2CD82F3 50B204D 18AC889 1DA26ED B6E55A4 523A54C 3A5B97C	Resolution: 72x72 (unit: inch) Pixel Resolution: 640x480 Camera Make: Motorola Camera Model: VGA Date/Time: 2014:12:17 22:33:20	

Figure 5.4.28

A list of all SMS text messages is shown in a separate report indicating the names, numbers, incoming, outgoing and content of the text messages on the mobile device. The details of the image are listed, such as the length, width and resolution of the image, as well as the date and time of when it was taken.

Short falls

Cellebrite, while it has many upsides, it was not the best with extracting application data. This also could be due to the fact that this was the older Cellebrite model. The newer UFED may possibly be built and able to detect certain or all types of apps. However, for this study Cellebrite provided only basic forensic information from all mobile devices. Therefore, if basic details such as text messages and call logs are needed, then this device seems to do a great job. However, if analysis on applications needs to be done or emails need to be extracted. Then, this device lacks in that department quite a bit, and would probably not be the most useful tool to use for an investigation.

5.4.4 Oxygen Forensics Analysis

Oxygen Forensics is a whole forensic suite which comes with various types of different forensic tools. When you first load the software, it will install certain mobile device drivers automatically so it can communicate with the mobile device right from the start.

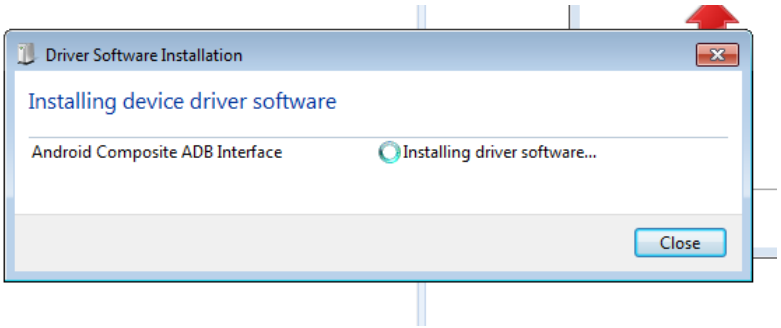


Figure 5.4.29

The great thing about Oxygen Forensic is that it comes with a whole list of all drivers for various mobile devices. Therefore, you can run an analysis offline and need no Internet access to download any additional drivers. This makes this software convenient for forensic analyst that need to work offline or away from a forensic lab. The mobile device is connected to the PC machine through a USB cable. Then Oxygen Forensics is run on the PC machine. It will automatically pick up and identify the mobile device. And, it will ask to confirm if the user wishes to have the mobile device connect to the PC workstation. Once the user accepts the connection, the software will start to extract all data from the mobile device.

Oxygen Forensics also has an option to try to root the mobile device in order to bypass the locked screen. In the case of the study, the devices were not used through that option. There is a risk of

destroying the mobile device when rooting it. Oxygen Forensics also mentioned this when trying to root the mobile device. For the purpose of the study and with limited resources, the mobile devices were not rooted and no attempt was made to root them.

Figure 5.4.30

Now, once the mobile device has been hooked up via USB from the mobile device to the computer workstation. The software will automatically pick it up and ask to confirm if wants the users to extract the data. Once yes has been selected, it will start to process and extract all of the data. The time it took was quite a while, as there was lots of data to be extracted. And, Oxygen forensics seems to do a very detailed search for data on the mobile device.

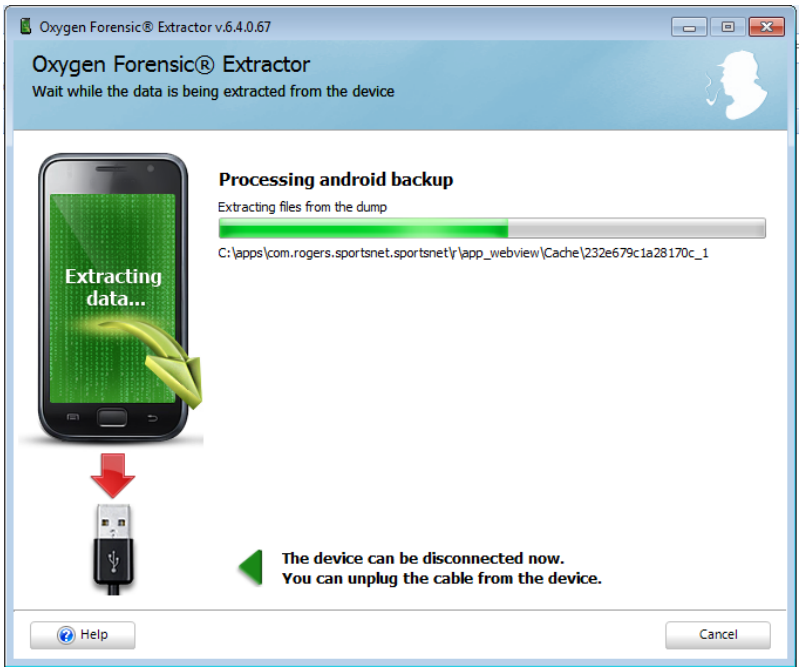


Figure 5.4.31

The software will first make a backup of the mobile device in case something goes wrong with the extraction process. This way if the device ever needed to be restored, then there is a copy of the mobile device information to revert it back to its normal prior state.

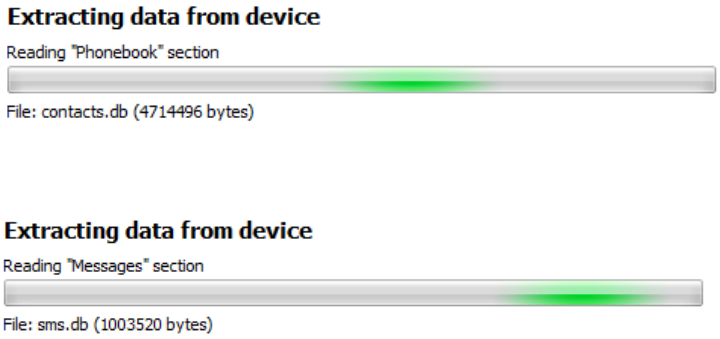


Figure 5.4.32

The various steps will extract different portions of data within the mobile device. The mobile devices contacts, text messages and various application data will be extracted in separate instances. Each extraction will list details of what the software is reading off the device. And, the extraction can take quite a while to complete.

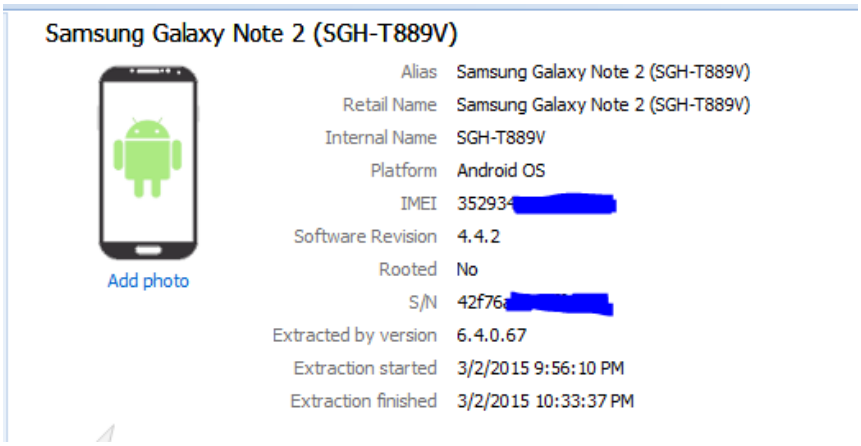


Figure 5.4.33

Once the software tool has completed the extraction process it will display a section as shown in Figure 5.4.33. The details of the mobile device are listed, such as the IMEI number, if the device is rooted, the type of device and the software revision number. All of this information is important, as it can be used to further find more information relating the device to its owner.

The type of data that was extracted through Oxygen Forensic is the following:

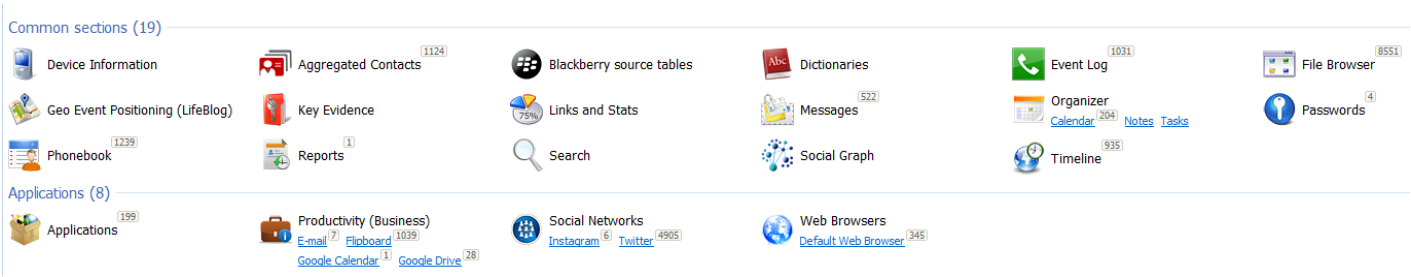


Figure 5.4.34

Wifi Passwords

Figure 5.4.35

Wi-Fi passwords were easily found listing the wireless network name (SSID) along with the password to that network.

Browser History

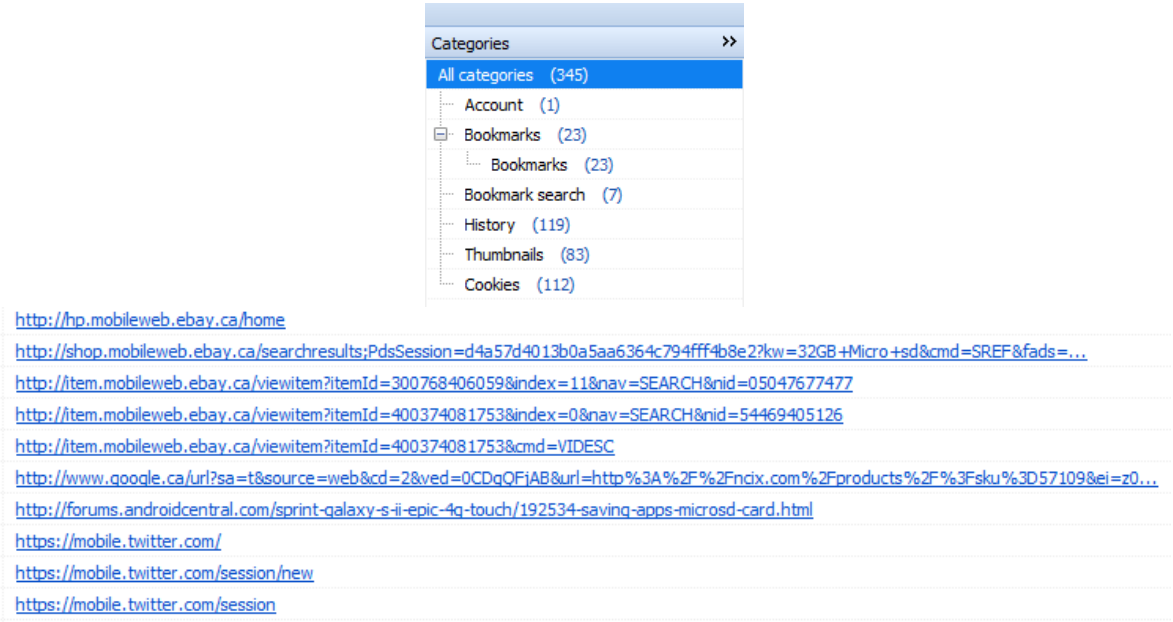


Figure 5.4.36

The browser history was easily found and broken down into detailed fields, such as Account name, bookmarks, history, thumbnails and cookies. All of this information can help an analyst track a user's online behavior and activities.

Phone Contacts

Photo	Contact	Internet	Phones	Caller groups	Data source	Last contacted	SHA-2 Hash
			+1778233[redacted]			UTC: 7/17/2014 9:40:03 PM	
	Devon	Instant messenger: 177823[redacted]@s.wh...	Mobile: +17782334[redacted]		Account name: WhatsApp		4d6e9218e76e17db61d9d6[redacted]
	Devon		Mobile: +1778233[redacted]		Account name: primary.sim.account_...		8771c784c28e8c354370850[redacted]

						9 missed				
☑	Andrew	+1604506[redacted]604506[redacted]	Call	41	41 12 incoming 18 outgoing 11 missed	0	01.08.2014 18:46	15.02.2015 16:58	10:40:03 incoming: 07:45:13 outgoing: 02:54:50

Figure 5.4.37

The phone contacts was easily found and broken down into detailed fields, such as contact name, phone number, and when the user last contacted them.

Call Logs

Type	Time stamp	Remote party	Contact name	Subject	Call duration
Voice	Device time: 3/2/2015 5:53:00 PM UTC: 3/3/2015 1:53:00 AM	604432[redacted]	604432[redacted]		00:01:13
Voice	Device time: 3/2/2015 5:51:21 PM UTC: 3/3/2015 1:51:21 AM	+164770[redacted]	+164770[redacted]		00:01:07
Voice	Device time: 3/2/2015 4:36:27 PM UTC: 3/3/2015 12:36:27 AM	+1647706[redacted]	+1647700[redacted]		00:01:06

Figure 5.4.38

The call logs are also included in the final report and display the time stamp of the calls, the phone number of the party calling and receiving the call, as well as the call duration time.

SMS/Text Messages

				SMS	SMS - Inbox	+1604825[redacted]	+1604825[redacted]	Device time: 11/26/2014 5:23:53 PM UTC: 11/27/2014 1:23:53 AM	Have the grill though	f67464b9d68bdc2ee7e42d5e34[redacted]
				SMS	SMS - Inbox	+1604825[redacted]	+1604825[redacted]	Device time: 11/26/2014 5:22:48 PM UTC: 11/27/2014 1:22:48 AM	Just sold on the weekend.	46ecacc48ef304428d25b7671d80[redacted]
				SMS	SMS - Sent	+1604825[redacted]	+1604825[redacted]	Device time: 11/26/2014 5:22:13 PM UTC: 11/27/2014 1:22:13 AM	Do you still happen to have the front bumper or gr	225fb5eed2db872e2ea76ad339[redacted]

Figure 5.4.39

All of the Text messages were also extracted listing the recipient and sender of the messages. Also included is the subject of the messages and the time it was sent or received on the mobile device.

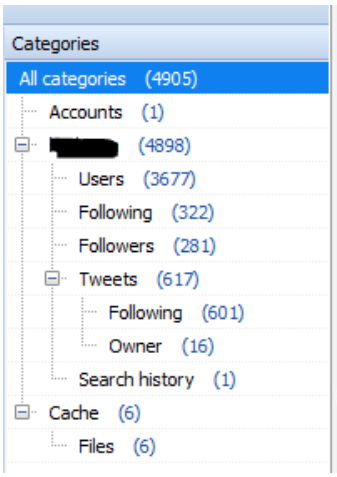
Application data

		Name	Identifier	Container	SHA-2 Hash
		Twitter	com.twitter.android	C:\apps\com.twitter.android	3208bad6ef84ceb909287fba6675291c17606f364aac4f417672b[redacted]
		Flipboard	flipboard.app	C:\apps\flipboard.app	890134d6e3024ef5b70b7b417e2f5d8f4c52786df6b50335bda[redacted]
		com.sec.android.provider.logsprovider	com.sec.android.provider.logsprovider	C:\apps\com.sec.android.provider.logsprovider	3adc228cc86dedc921cee091325a382a5f46fbd877845846d4ea[redacted]
		Web Browser	com.android.browser	C:\apps\com.android.browser	29b13227b7df55da8ed62073abf1228312160a5dc15f8957e3e[redacted]
		Media	com.android.providers.media	C:\apps\com.android.providers.media	56d1cb93c5c6fe6b71dace4b1bbdce4124077e24340fba786778[redacted]
		Google Drive	com.google.android.apps.docs	C:\apps\com.google.android.apps.docs	e92a314181f93c03b1d9930acf71ade974fee9c71043f0a885f5b[redacted]
		Downloads	com.android.providers.downloads	C:\apps\com.android.providers.downloads	ec43659e1327c2f6acf3c98504039e3d5c62003c36c63039ba3c[redacted]
		E-mail	com.android.email	C:\apps\com.android.email	2ce3531e29a52fbe87f5cd91527b90beeb846d48dd3b6df41c279[redacted]
		Instagram	com.instagram.android	C:\apps\com.instagram.android	9b2a21d60138fd1e5c232aca24baeee583163617a82acf05dbbfe[redacted]
		Google Calendar	com.android.providers.calendar	C:\apps\com.android.providers.calendar	0098615af0c7e70ff3e13d4583096e21a102ebdf006bedcb213be[redacted]
		android	android	C:\apps\android	12e2266cfe8d7dae46b2e4e6b6a82e6ce91187ebb1e576dcf1e2[redacted]
		android.googleSearch.googleSearchWidget	android.googleSearch.googleSearchWidget	C:\apps\android.googleSearch.googleSearchWidget	32314ebece3d22caaf3c690b0edf8095cdc25b90c98c8ee4778268[redacted]
		com.android.apps.tag	com.android.apps.tag	C:\apps\com.android.apps.tag	ea66be1f580caf17aeb05d131ac830cc25c05ec5658d82ea093c4[redacted]
		com.android.calendar	com.android.calendar	C:\apps\com.android.calendar	aad5d9b808ea4d353a7b88a4cda6b6e1d6594230f91ef26cfb68[redacted]

Figure 5.4.40

Finally, there is a list of all applications that are on the mobile device. Some applications are known well or are extremely popular. And, in that case Oxygen Forensics has built reports on certain applications. For the non-popular applications, Oxygen Forensics allows the analyst to view all of the application data within its database. This method allows the analyst to dig into the database to view the type of data that is stored per an application.

Twitter



nationalpost	National Post	Canada	News, analysis & commentary by the National Post. The Post on Twitter: http://natpo.st/mRz43J | Post Staff http://natpo...
jackieelule	Just Jackie ❤	N/A	living life day by day ❤
issssabellaaa	N/A	NY // august 28, 2013≡	"please dont fondle austin"
CoachKen41	Ken Armstrong	Metro Vancouver, Canada	Husband, Father, Lawyer, Little League BC Umpire Consultant, soccer coach, former baseball coach & Van 2010 Olympic vol...
ginalimp	Gina L.	Kentucky	Nurse Aide, Independant Beachbody Coach, Fun, Goofy, Silly, Lovable, Just Me! 3
Shaggyshan	Shaggy Shan	Toronto	Steven Shanahan, writer of Silly Kingdom, Shrub Monkeys, Tatterhood, Buttons & Jim, Fairy Market, Radio Adrift, hosts S...

Figure 5.4.41

Since twitter is a fairly common application known and used on mobile devices. Oxygen forensics has built a method to detect for any Twitter application data on mobile devices during extraction. The report displays all of the twitter accounts on the device, how many followers and users are being followed. It also lists all of the users' tweets, search history and files such as images that were posted on the users Twitter account.

Instagram

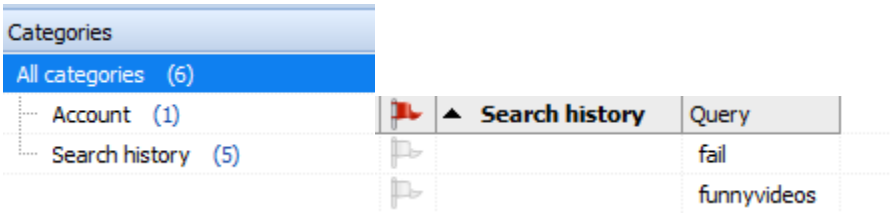
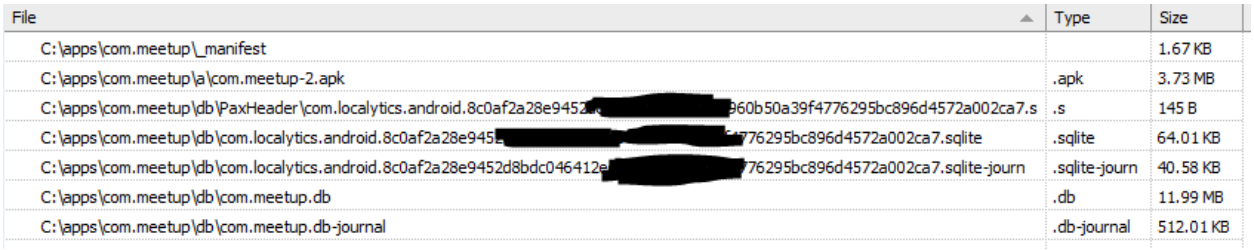


Figure 5.4.42

Instagram also is a fairly popular application on most mobile devices. And, it seems that Oxygen Forensics also notices this app and creates a report on it. The report lists the account name, and all of the search history.

Meetup



File	Type	Size
C:\apps\com.meetup_manifest		1.67 KB
C:\apps\com.meetup\a\com.meetup-2.apk	.apk	3.73 MB
C:\apps\com.meetup\db\PaxHeader\com.localytics.android.8c0af2a28e9452[redacted]960b50a39f4776295bc896d4572a002ca7.s	.s	145 B
C:\apps\com.meetup\db\com.localytics.android.8c0af2a28e945[redacted]776295bc896d4572a002ca7.sqlite	.sqlite	64.01 KB
C:\apps\com.meetup\db\com.localytics.android.8c0af2a28e9452d8bdc046412e[redacted]76295bc896d4572a002ca7.sqlite-journ	.sqlite-journ	40.58 KB
C:\apps\com.meetup\db\com.meetup.db	.db	11.99 MB
C:\apps\com.meetup\db\com.meetup.db-journal	.db-journal	512.01 KB

Figure 5.4.43

The figure 5.4.43 above shows the database and files for the application called meetup. Now to get more information regarding the application, there is a method to view and search through the application database. There is a way to click on the ".db" file and open it in a database viewer such as SQLite Viewer. The database viewer will allow the analyst to find other data within the database. And, this is a good way to find sensitive information that may otherwise not be found automatically by the forensic tool.

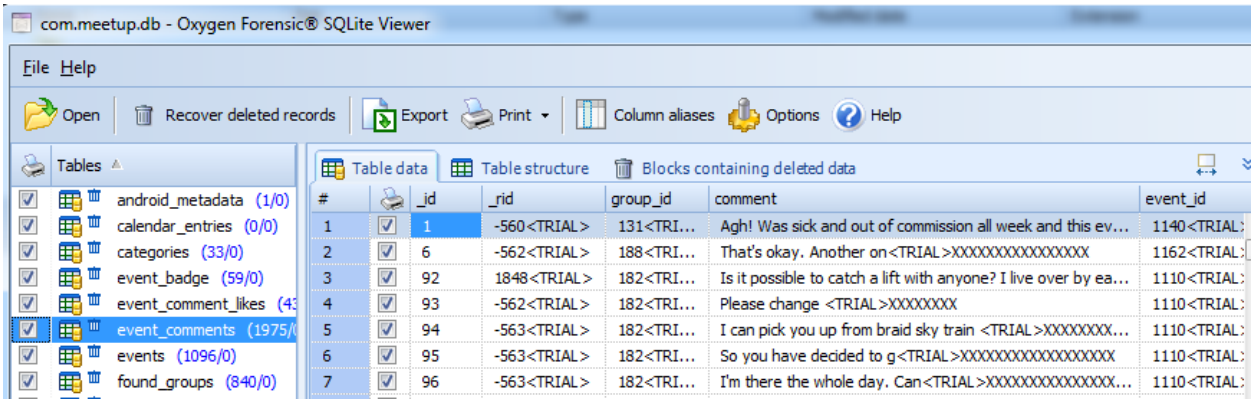


Figure 5.4.44

The other great feature that Oxygen Forensic brings to the table is the SQi Database Viewer. Application data is all stored as a database on the mobile devices. This creates a mechanism to view the schematic, schema and data within this database. However, much of it must be deciphered by the analyst, as the data will not be placed in an easy to read report or form.

Short Falls

Oxygen Forensics was able to get the most data out of all of the forensic tools. However, it was only able to provide reports on certain popular applications. Many other applications requires much more work for the forensic analyst. The databases are available for the analyst to search through for additional information. However, it would save much more time if more common application reports were generated after the extraction. Another issue is that Oxygen Forensics was not able to decrypt any of the WhatsApp chat logs that it had found. If there was some sort of mechanism or decryption setting, then it would provide much more help when trying to access encrypted chat logs for certain applications.

5.5 Manual Extraction

Figure 5.4.45

In the case when no forensic tools are available, or the tools are not able to extract any mobile data. The last resort is to manually bypass the pass lock and view the data on the mobile device. The downside to this type of analysis is that you will most likely modify information on the mobile device. And, this type of analysis may not be forensically sound in the court of law. By viewing information on a mobile device, copying or reading information can cause data to become modified. And, therefore there could be a loss or corruption of data on the device. This type of extraction should normally be never done unless access is needed to certain applications. For example, access might be needed to the users Facebook account. However, the password may not be known or stored on the device. Yet, the application could still be logged and signed into the Facebook account. Therefore, entering into the phone and clicking on the Facebook app would then give the forensic analyst the ability to access the users Facebook account.

7. Review of Findings

Overall, based off the study and experiment conducted it was found that Oxygen Forensic was the best forensic software tool to extract data from an Android mobile device. It was able to provide the most useful information, as well as allowing a method to go in and find data for yourself through its database viewer. It also has a method built in to possibly root or gain access to locked devices. However, the equipment available for this study did not allow for the ability to take a risk of rooting the phone. As rooting a mobile device can also cause it to cease to function if done incorrectly.

I also did not find any data for stored GPS location data. This could be data that is stored under certain apps, which the forensic software tools could not extract due to insufficient permissions and access. The study also never looked at analyzing rooted android mobiles devices, as it's possible more

data could've been extracted or seized. Lastly, there was no forensic analysis done on the RAM on any of the mobile devices. To gain access to the ram normally root access is needed. There is a good chance that sensitive and useful information is stored in RAM. And, therefore, further studies need to be done to uncover findings within the RAM of mobile devices.

8. Conclusion

The overall security for most android mobile devices is pretty good. Unless the mobile device has been rooted, or has debug mode enabled. It is fairly secure from having any of its content and data exposed to strangers. It also makes it very difficult for law enforcement to perform any sort of forensic analysis on android devices. Hopefully, as time goes on the forensic tools will find methods to temporarily gain root access. As this would allow forensic analyst to get the information they need from the mobile devices. The last problem posed is the fact that possible future mobile devices may come pre-encrypted. This would mean that not even the mobile device manufactures would have access to decrypt any of the data on mobile devices. And, this further provides larger and more difficult problems for law enforcement. However, the current tools do provide fairly excellent options and definitely can provide evidence in court regarding information stored on mobile devices.

Definitions

Cellebrite: A type and name of mobile forensic software used worldwide to extract and analyze data from mobile devices.

Faraday Bag: A plastic bag that is made of material that blocks airwaves and other wireless signals. It creates a seal around an object to block it from any wireless signal reception.

Logical Acquisition: A copy of multiple file structures on a single hard drive storage space. Such as C: drive, D: drive, E: drive.

MobilEdit: A type and name of mobile forensic software used worldwide to extract and analyze data from mobile devices.

Physical Acquisition: A copy of the whole hard drive storage space with everything as one whole file or set of data.

User Interface: The design and look that is seen for an application. In this case it is the screen shown for a mobile device and how things are displayed on the phone.

References

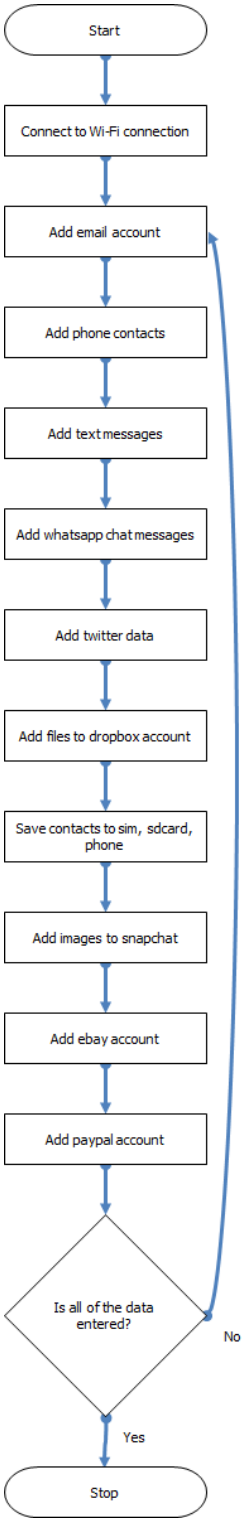
Ahmed R, V Dharaskar R. (2010). Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective. p. 312-323. Amravati University, India.

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; Vol. 10 Issue 6, p337

Al Mutawa N, Al Awadhi I, Baggili I, Marrington A. (2011). Forensic analysis of social networking applications on mobile devices. p. s24-s33. Abu Dhabi, UAE.

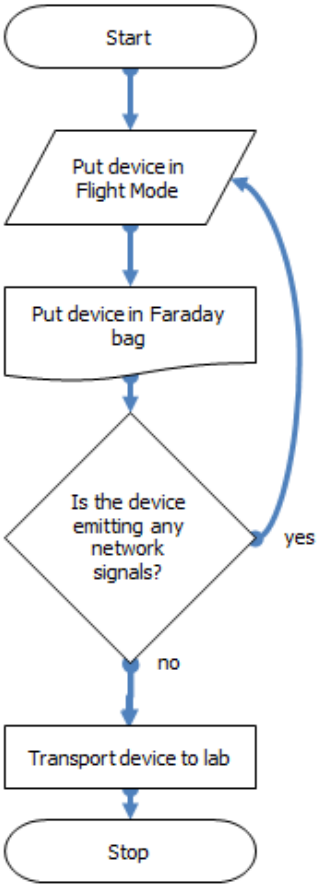
Storer T, Glisson W, Grispos G. (2010). Investigating Information recovered from Re-sold Mobile Devices. p. 1-2. University of Glasgow, Glasgow England.

Appendices



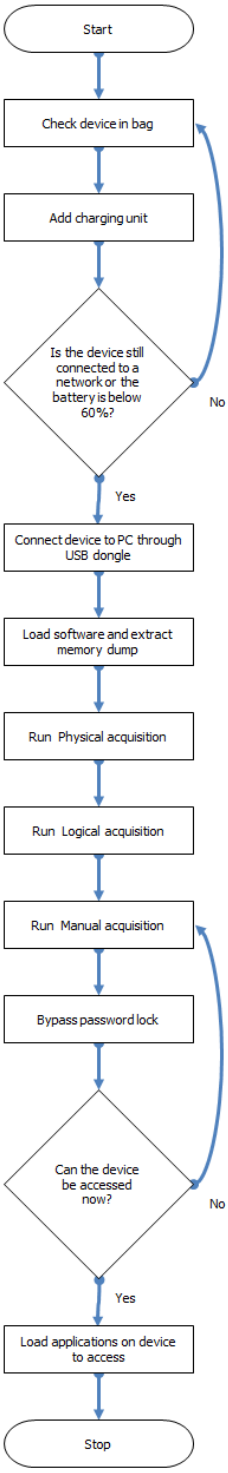
Phase 1

Figure 1.1



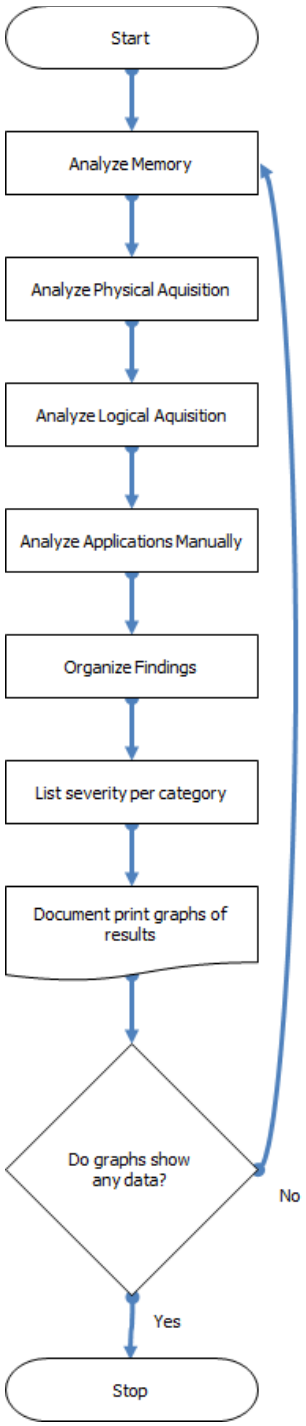
Phase 2

Figure 1.2



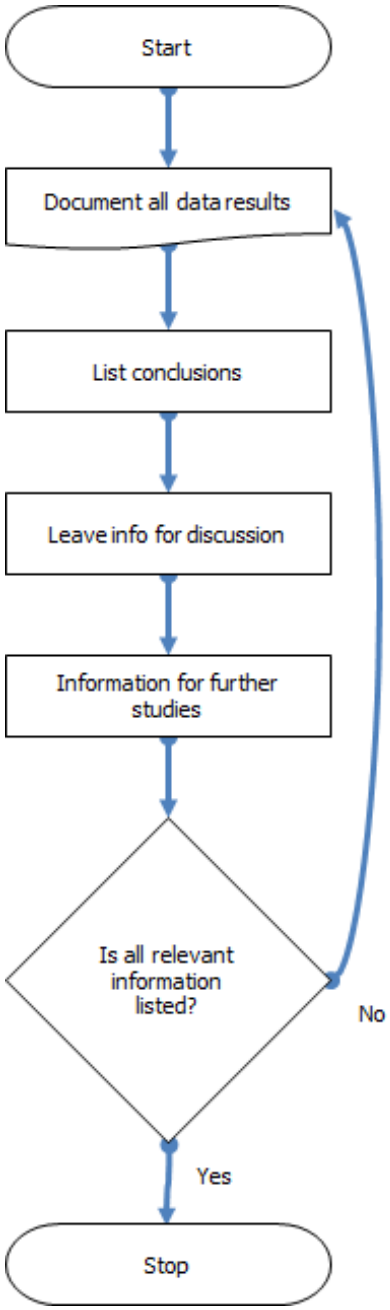
Phase 3

Figure 1.3



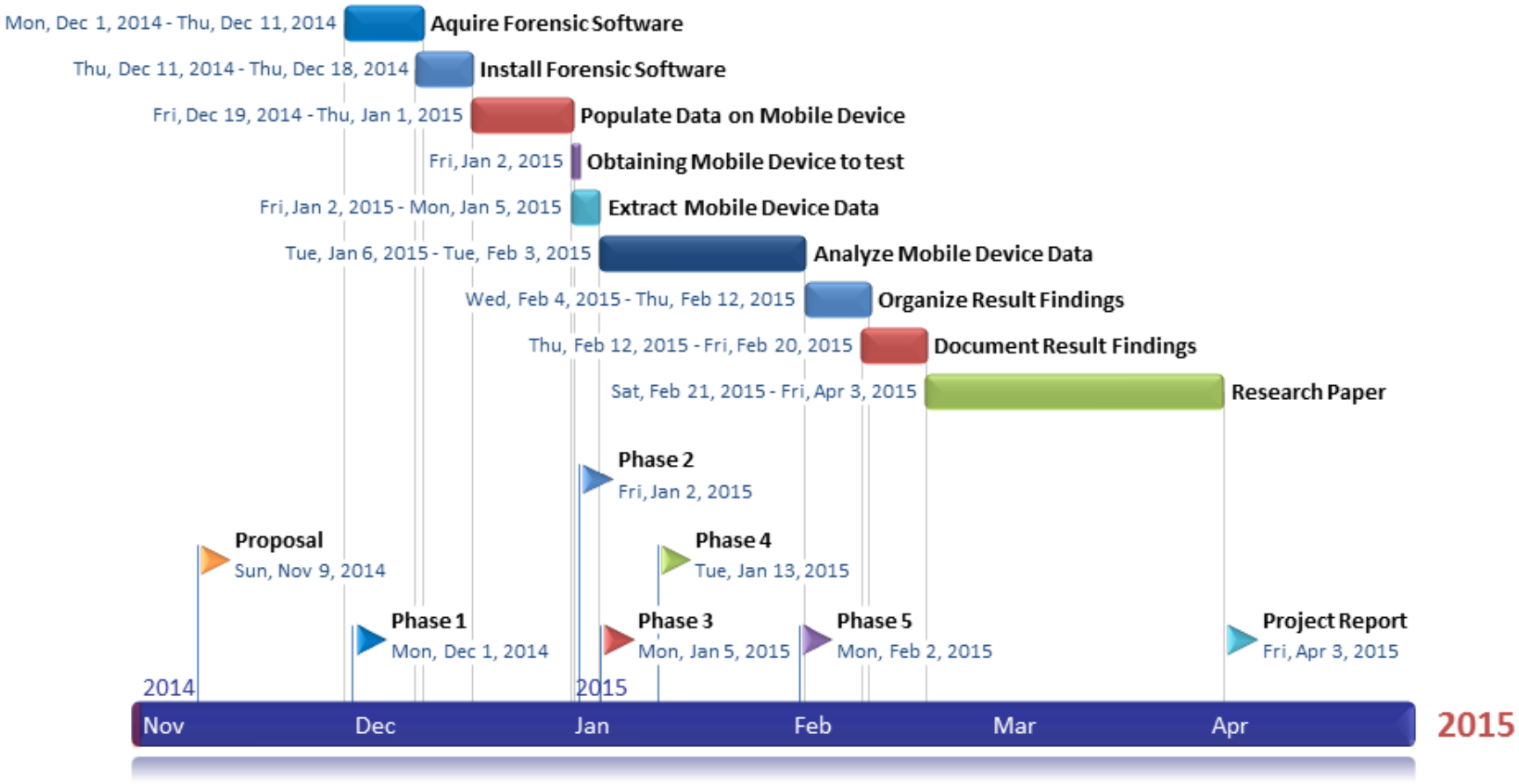
Phase 4

Figure 1.4

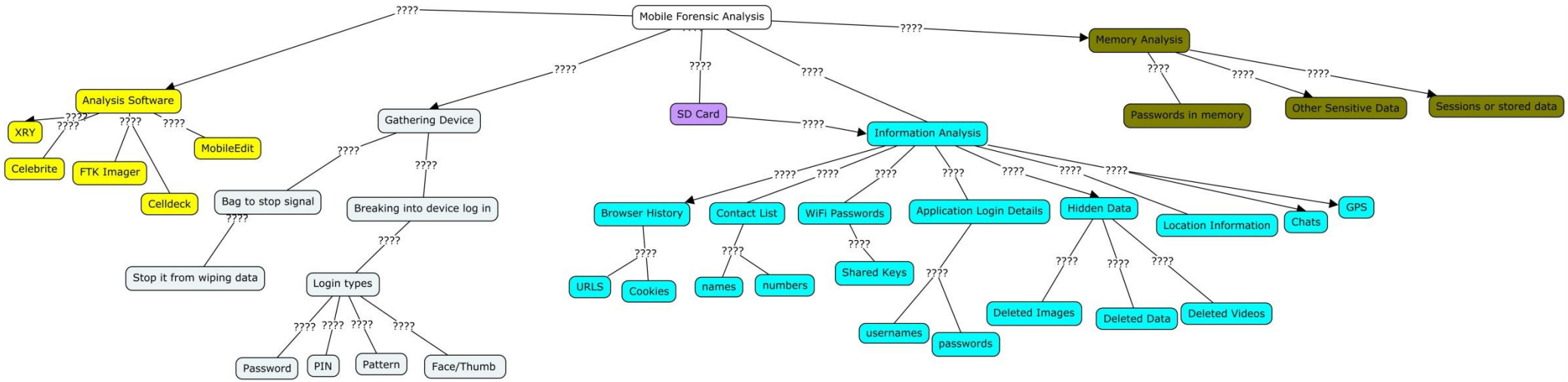


Phase 5

Figure 1.5


Mon, Dec 1, 2014 - Thu, Dec 11, 2014
Aquire Forensic Software
Thu, Dec 11, 2014 - Thu, Dec 18, 2014
Install Forensic Software
Fri, Dec 19, 2014 - Thu, Jan 1, 2015
Populate Data on Mobile Device
Fri, Jan 2, 2015
Obtaining Mobile Device to test
Fri, Jan 2, 2015 - Mon, Jan 5, 2015
Extract Mobile Device Data
Tue, Jan 6, 2015 - Tue, Feb 3, 2015
Analyze Mobile Device Data
Wed, Feb 4, 2015 - Thu, Feb 12, 2015
Organize Result Findings
Thu, Feb 12, 2015 - Fri, Feb 20, 2015
Document Result Findings
Sat, Feb 21, 2015 - Fri, Apr 3, 2015
Research Paper
Phase 2
Fri, Jan 2, 2015
Proposal
Sun, Nov 9, 2014
Phase 4
Tue, Jan 13, 2015
Phase 1
Mon, Dec 1, 2014
Phase 3
Mon, Jan 5, 2015
Phase 5
Mon, Feb 2, 2015
Project Report
Fri, Apr 3, 2015
2014
2015
Nov
Dec
Jan
Feb
Mar
Apr
2015

GANTT CHART



CMAP – Brainstorming Ideas & Concepts