

Mobile Device Forensics

CA2 – Open Source Assignment

By Dean xxxxxxxxx

B0009xxxxxx

Department of Informatics
School of Informatics and Engineering
Technological University of xxxxxxxxx
xxxxxxxxxxxxxxxxxx

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
          Mobile Device Forensics
              Michael xxxxxxxx
```

10/11/2019

Plagiarism Declaration

TECHNOLOGICAL UNIVERISTY xxxxxxxxxxxxxx
DEPARTMENT OF INFORMATICS
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
LECTURER: MICHAEL xxxxxxxxxxxxxx

DECLARATION ON PLAGIARISM

I declare that the work I/We am (are) submitting for assessment by the Institute examiner(s) is entirely my (our) own work, except where the author or source has been duly referenced and attributed.

I confirm that this material has not been previously submitted for a degree or any other qualification at xxxxxxxxx or any other institution. I further confirm that I have read and understood the Institute policy on plagiarism in assignments and examinations (3AS08.doc) and that I am not, so far as I am aware, in breach of any of these regulations.

Signed: Dean xxxxxxxxxxxxxx

Date: 10/11/2019

Table of Contents

Plagiarism Declaration	2
Introduction	4
Lab Requirements	4
Lab Goals	4
The Image	4
Acquiring the Image	6
Setting up the software	7
Questions for the Investigator	13
Example Investigation Report	14
Case Reference	14
Chain of Custody	14
Hash Checking	14
Device Information	14
Hardware Identification	14
File Systems	15
Automatic tagged information for analysis	16

Introduction

The purpose of this assignment is to create a lab session for future students to be able to understand a new system or technology for the analysis of mobile devices, be it GPS, Tablets or Mobile Devices. The idea is to be informative and easy to follow for a student to understand what they are looking at and what data is available to the user for analysis

The purpose of this lab is to understand the analysis purpose of analyzing mobile images and what information that can be found, these included some of the following items

- Text Messages
- Email Messages
- Passwords
- Usernames
- Call Log
- Photos and Metadata

Lab Requirements

There are not many requirements needed to be able to complete the lab

- windows 7 64bit or Windows 10 64bit
- 7zip
- Downloaded Image – “In Zip”
- Download Tool – “In Zip”

Lab Goals

These are the goals of completing this lab

- Have an understanding of how Cellebrite images look
- Have an understanding of finding information in a Mobile Image
- Have an understanding of the Analysis processes

The Image

The image of the Mobile device came from the California Cybersecurity Institute using a closed sourced tool called Cellebrite from a Physical Samsung CDMA SM-J320VPP Galaxy J3 2016 mobile device, the tool used is only for making an Image of the device, the image was then uploaded to the California Cybersecurity Institute website as a training aid for forensic use.

They also offer free software by Cellebrite that is available upon request called Reader, within the download image you get a copy of the Reader software that can be used for analysis of the file.

This download for both the image and the software is available from the following location

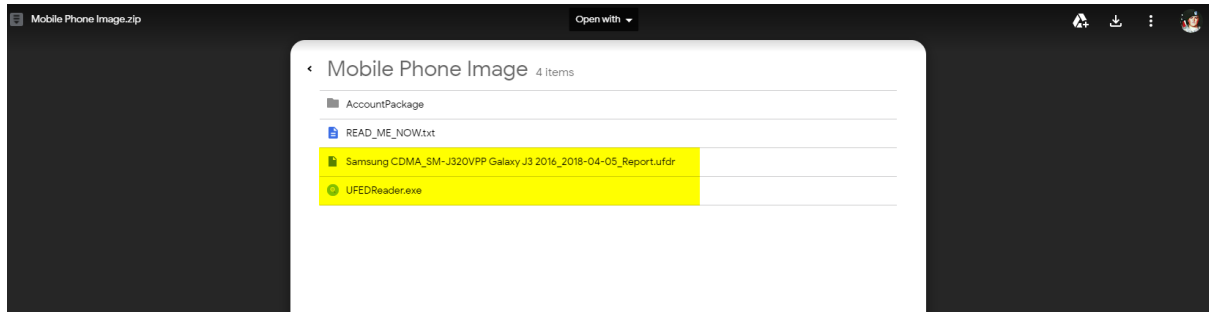
xx.com

I choose to use this image from a professional tool because; I was unable to find a spare mobile device or digital unit that I could use for testing, the reason I chose this image from multiple others that are available for forensics training online, is that this is an image populate with data for forensics analysis training, with a narrative that can allow an investigator to analysis the data and follow the trail of information that is found in the system.

Since Cellebrite is a common tool for Law Enforcement and some corporate level forensic investigation and the tool for capture the image is straight forward and requires little interaction from the investigator, the benefit of this is that there are FreeWare and open source alternatives to analysing these images, even ones provided by Cellebrite for educational use.

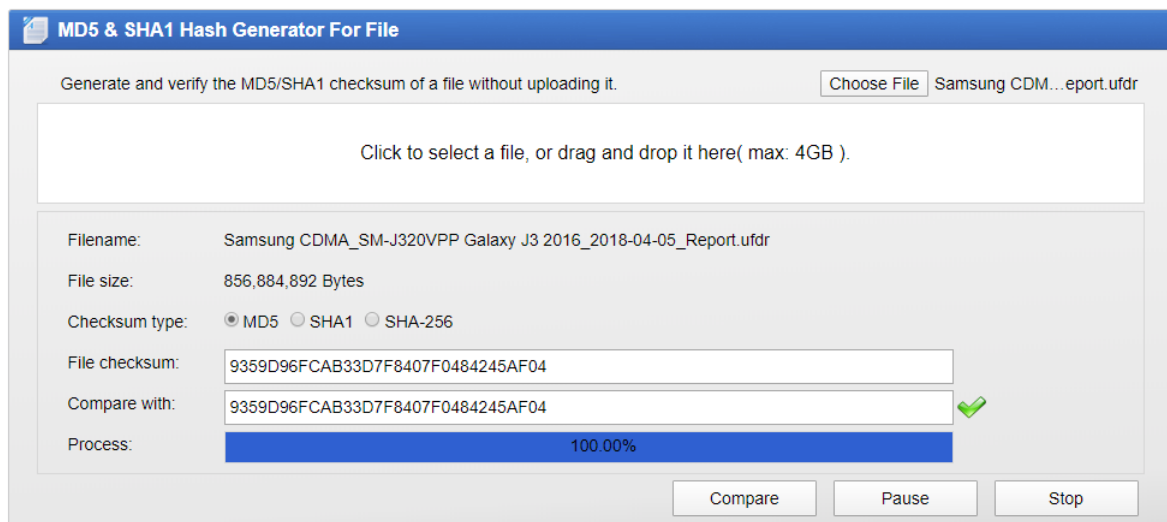
Acquiring the Image

The Image can be downloaded from the California Cybersecurity Institute at the following link
XX the files needed are the .ufdr image and the
UFEDReader.exe, the reader is used for reading images captured from Cellebrite systems.



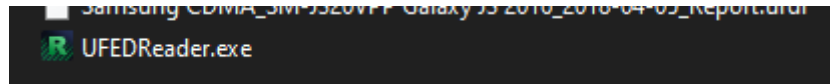
The READ_ME_NOW.txt contained the original hash file during the original capture comparing with that hash we can see the image hasn't been modified using an OnlineMD5 checker

OnlineMD5

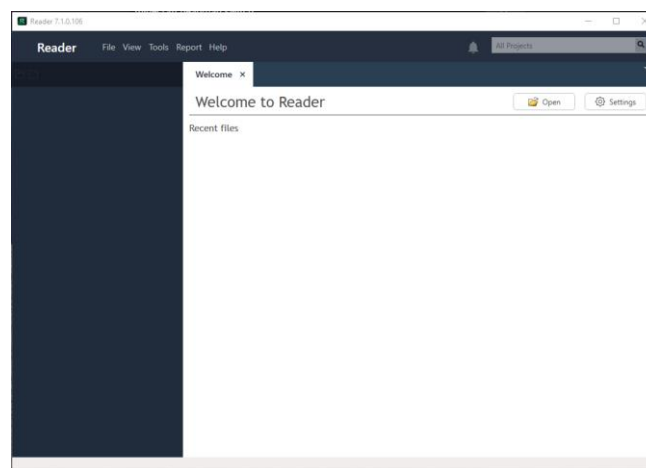


Setting up the software

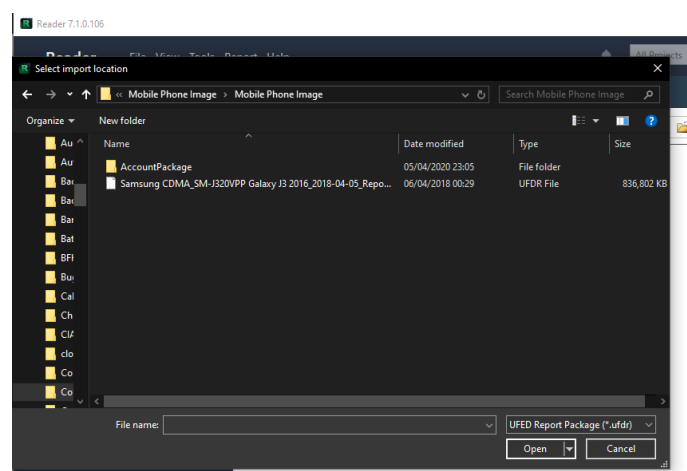
The reader is portable and doesn't not require a virtual machine or to be installed on the host system, it's just a case of running the .exe



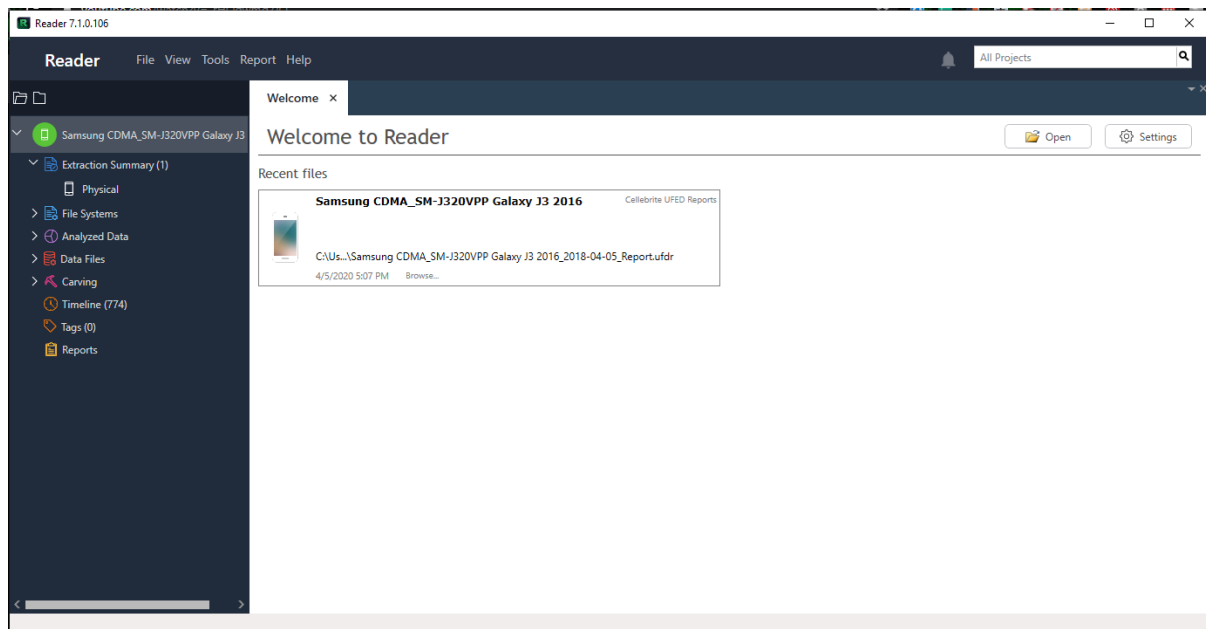
Upon running the software, you will be presented with a blank screen where you can choose to open an image to be analyzed by the investigator, this can be done by clicking the Open button or going to file and clicking the open option



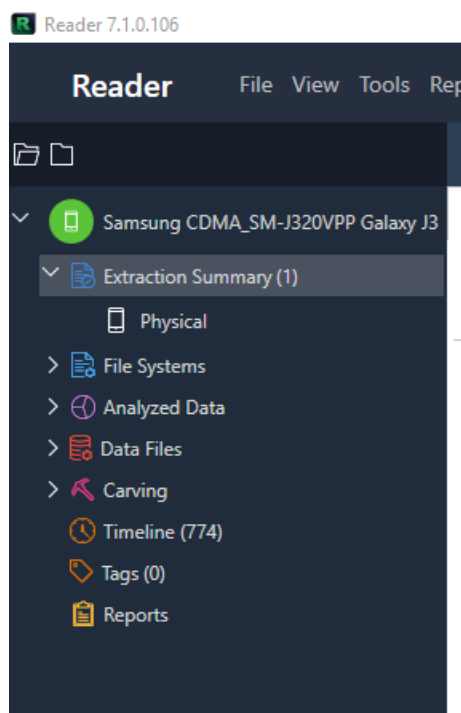
Then use the pop out navigation window to move to the location of the .ufdr image for analysis, and opening it with the open button.



Opening the image depending on the system can be a fast or slow process, on it loads you will be displayed a window that looks like the image bellow, and this will show the open image and multiple options that can be used to view the information. The software is very intuitive and simple to use for all users

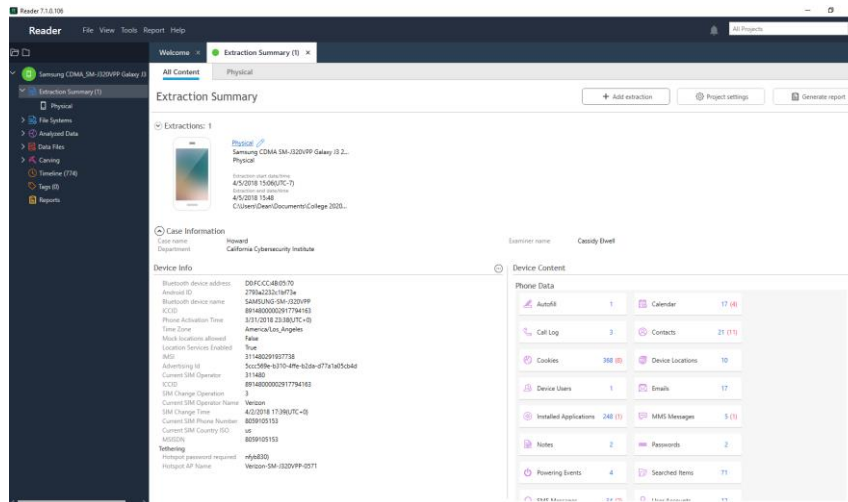


Taking a look at the options available we can see them bellow, each section breaks down different parts of the device and how it can be used to analysis the information, The main menu looks like the image bellow showing the sub sections that can be chosen by the user



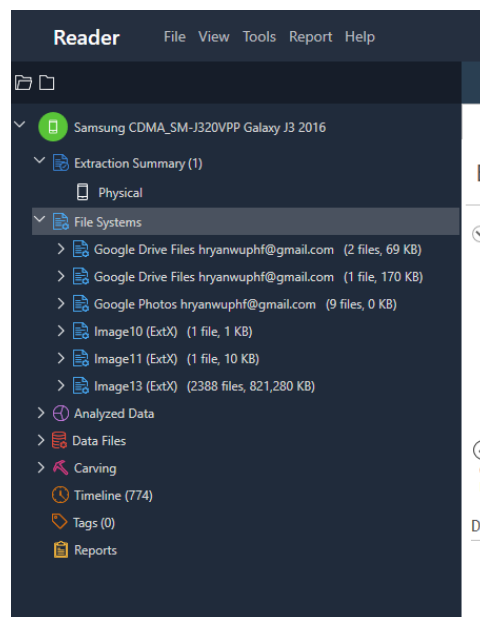
Extraction Summary

Under the extraction summary section we can see the details that can be found of the device, these are made easily readable to be able to find the details needed for the investigation. The information that can be seen is common details such as mobile carrier, Mac addresses of hardware such as the wireless card and the Bluetooth card



File System

Under the file system section we can use the collections of files found on the system, this includes file systems such as Google Drive, Dropbox and other system that would contain files



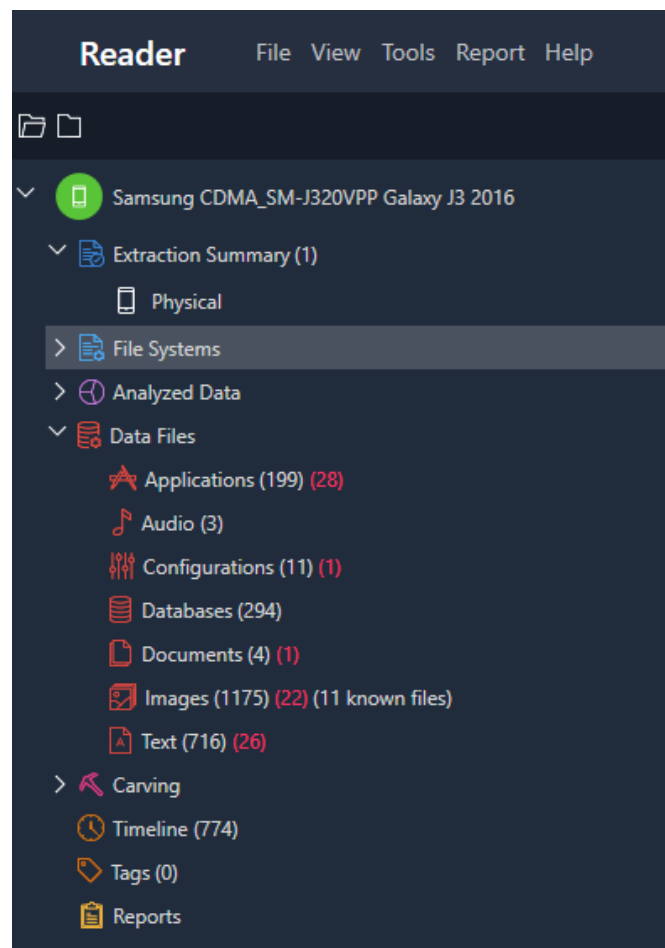
Analyzed Data

Similar to other applications Reader does automatic analysis of files and lists files with common extensions and hashes for easy analysis. This includes Autofill data, Calendar data, Cookies, Web History and makes this data easily readable and viewable to the investigator



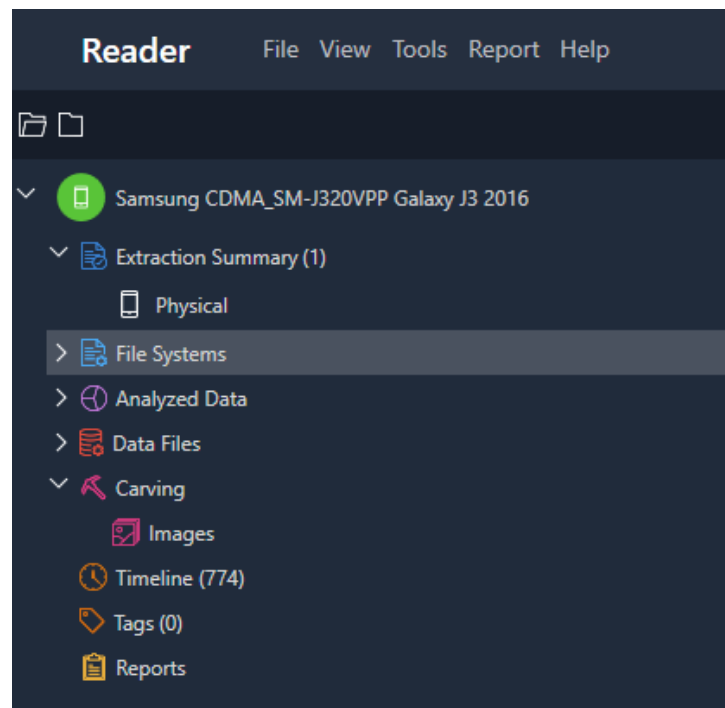
Data Files

Under the Data Files section we can use the collections of files that contain data with known extensions, this would be photos, audio tracks, database files, PDF's and documents. This section makes the analysis of files on the system easier for the investigator to be able to see all data files that are included on the system

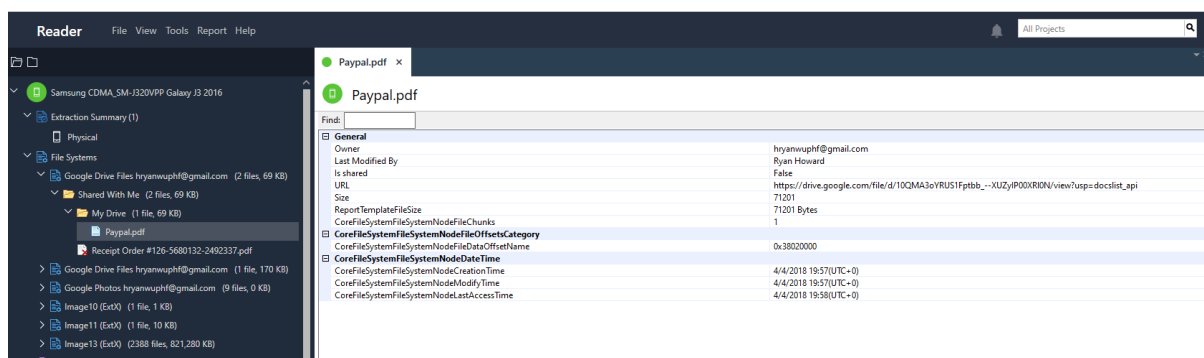


Carving

Under the Carving section we can see that that was removed and deleted data by the phone user, in this case we can see that there was deleted images found on the device, these are listed under the images category, if it was documents it would be found under a category called documents



Deleted files shows up with a red X over the file, this can be seen in the file system below, here you can see the deleted file Receipt Order that was deleted, is available in the structure section but you can see that it is deleted. This file will also be listed in the file carving section.



Questions for the Investigator

1. What was the File's MD5

2. What is your Chain of Custody

3. What are the Physical addresses associated with the device

4. What Usernames are found on the device

5. What is the SSID of the Wi-Fi the phone is connected to

6. What account is linked to the Google Drive account

7. What game can be found as an in the MMS

8. How many Files were deleted

9. What files was downloaded on 04/04/2018 12:57:33

10. What Does the evidence here suggest is happening

Example Investigation Report

Here we will do a sample investigation of the given image

Case Reference

Case Name	Investigator	Location
Howard	Dean xxxxxxxx	Home Lab

Chain of Custody

This is the full chain of custody from the original image provided till it was received and investigated by the investigator

DATE	TIME	TO	FROM	Transferred By
05/04/2018	15:06 PM	Cassidy Elwell	Cassidy Elwell	Original Image Captured
13/04/2020	14:20 PM	Dean	Cassidy Elwell	Download Via Secure Upload
13/04/2020	15:51 PM	Dean	Dean	Transfer of Data to Secure Lab

Hash Checking

Here we can see the hashes of image, from originally been taken and from the downloaded image this is to confirm the image was not tampered with

DATE	TYPE	HASH
05/04/2018	MD5	9359D96FCAB33D7F8407F0484245AF04
13/04/2020	MD5	9359D96FCAB33D7F8407F0484245AF04

Device Information

Here we can see the device information of the system that the image was taken from

Brand	Model	Time Zone	Version
Samsung	Galaxy SM-J320VPP 2016	America's / Los Angeles (UTC-7)	Android 7.1

Hardware Identification

Here we can see the identification information of the device hardware, this can be used to get an idea of what portion of the device traffic came from

Hardware	Identification
Bluetooth device address	D0:FC:CC:4B:05:70
Android ID	2793a2232c1bf73e
Bluetooth device name	SAMSUNG-SM-J320VPP
Phone Activation Time	3/31/2018 23:38(UTC+0)
Time Zone	America/Los_Angeles
Mock locations allowed	False
Location Services Enabled	True
IMSI	311480291937738
Advertising Id	5ccc569e-b310-4ffe-b2da-d77a1a05cb4d
Current SIM Operator	311480






SIM Change Operation	3
Current SIM Operator Name	Verizon
SIM Change Time	4/2/2018 17:39(UTC+0)
Current SIM Phone Number	8059105153
Current SIM Country ISO	Us
MSISDN	8059105153
Hotspot password required	nfyb830)
Hotspot AP Name	Verizon-SM-J320VPP-0571

File Systems

In this section we can see the location of files on the system, this includes location such as cloud storage

Image	Name
1	Google Drive Files hryanwuphf@gmail.com
2	Google Drive Files hryanwuphf@gmail.com
3	Google Photos hryanwuphf@gmail.com
4	Image 10 (ExtX)
5	Image 11 (ExtX)
6	Image 13 (ExtX)

Autofill data

		#				Type	TimeStamps	Source	Key	Value
	<input checked="" type="checkbox"/>	1					04/04/2018 11:22:11(UTC-7)	Chrome	zipCity	93410

Calendar Entries

Calendar (17)

Table Search

#			Subject	Location	Event Position	Attendees	Details
1			Precinct Appoi...	San Luis Obispo, California, Unit...		hryanwuphf@gmail.com hryanwuphf@gmail.com	To see detaile
2			Your Geek Squ...	255 Madonna Rd, San Luis Obis...			If you're dropp
3			Check Email for...				
4			Put together G...				
5			Hear from Dwi...				
6			Wait for more...				
7			Complete Xbox...				
8			Call Mom				
9			Check that all e...				
10			Call Kelly				
11			Create Watch...				
12			Create Minecra...				
13			Create Grand T...				
14			Call in Sick to...				
15			Test				
16			3469p30crf6ljn...	k36spm6so68ob56dk6ie1k75gjc...			nct Appointment
17			k36spm6so68ob...	1k75gjcjr9odtimsq36d5j6ecom.a...			nct Appointment

Calendar Entry
Go to

Category: hryanwuphf@gmail.com
Subject: Precinct Appointment
Start Date: 05/04/2018 12:00:00(UTC-7)
End Date: 05/04/2018 13:00:00(UTC-7)
Reminders: 05/04/2018 11:30:00(UTC-7)
Priority:
Status:
Class:
Repeat Rule:
Repeat Until:
Repeat Day:
Repeat Interval:
Extraction: Physical
Source file:

Attendees

hryanwuphf@gmail.com

hryanwuphf@gmail.com

Details

To see detailed information for automatically created events like this one, download the official Google Calendar app for your Android phone or tablet. <https://www.google.com/calendar/android>

This event was created from an email you received in Gmail. https://mail.google.com/mail/?extsrc=cal&plid=ACUX6DNw_jBKP8HODcQ_6fhFta3dhSavi-8jVM4

Map

Location: San Luis Obispo, California, United States, 93405
Event Position:

Subject	Location	Attendees	Details	Start date	End Date
Precinct Appointment	San Luis Obispo, California, United States, 93405	hryanwuphf@gmail.com	To see detailed information for automatically created events like this one, download the official Google Calendar app for your Android phone or tablet. https://www.google.com/calendar/android This ev...	05/04/2018 12:00:00(UTC-7)	05/04/2018 13:00:00(UTC-7)
Your Geek Squad Reservation	255 Madonna Rd, San Luis Obispo, CA 93405		If you're dropping off a device with us, remember to back up your files beforehand. Also, don't forget to bring in any accessories involved with the problem you're having. See you soon!	05/04/2018 12:00:00(UTC-7)	05/04/2018 12:20:00(UTC-7)
Check Email for Paypal Payment				04/04/2018 10:00:00(UTC-7)	04/04/2018 11:00:00(UTC-7)
Put together Grand Theft Auto V with "damaged" disc for jhal from eBay				04/04/2018 08:19:48(UTC-7)	
Hear from Dwight about "free" packing by materials				04/04/2018 08:19:02(UTC-7)	
Wait for more people to take the bait and buy my "products"				04/04/2018 08:18:33(UTC-7)	
Complete				04/04/20	

Xbox 360 sleeves for Grand Theft Auto V, Minecraft, Watch Dogs				18 08:17:56(UTC-7)	
Call Mom				04/04/2018 08:15:24(UTC-7)	
Check that all emails forwarding from techie6739@gmail.com				03/04/2018 09:38:13(UTC-7)	
Call Kelly				03/04/2018 09:21:11(UTC-7)	
Create Watch Dogs Item				03/04/2018 09:20:45(UTC-7)	
Create Minecraft Item				03/04/2018 09:20:27(UTC-7)	
Create Grand Theft Auto V Item				03/04/2018 09:17:57(UTC-7)	
Call in Sick to Work				03/04/2018 09:00:00(UTC-7)	
Test				02/04/2018 11:39:39(UTC-7)	
3469p30crf6lnj0rj6cl		k36spm6so68ob56dk6ie1k75gjcr9odtimsq36d5j6e_Preci	nct AppointmentSan Luis Obispo, California, United States, 93405To see detailed information for automatically created events like this one, download the official Google		

GPS	04/04/2018 11:49:14(UTC-7)	(35.262584, -120.677709)	http://maps.google.com/?cid=10904070324379996883	Chipotle Mexican Grill
GPS	04/04/2018 11:43:32(UTC-7)	(35.258855, -120.687006)	0:0	1179 Atascadero St, San Luis Obispo, CA 93405
Image	16/02/2018 19:00:19	(35.280105, -120.663279)		20180216_761345.jpg
Image	14/02/2018 17:00:57	(35.258855, -120.687006)		20180214_124635.jpg
Image	01/12/2017 10:00:35	(35.258855, -120.687006)		20171201_945638.jpg
GPS			Best Buy, 255 Madonna Rd, San Luis Obispo, CA 93405	
GPS			Chipotle Mexican Grill, 297 Madonna Rd, San Luis Obispo, CA 93401	
GPS		(35.280105, -120.663279)		
GPS		(35.258855, -120.687007)		

Emails

There were multiple emails, the contents of the email take up too much time in the response, email contents contain information regarding online sales through eBay, and having GeekSquad appear for the system repair. These emails have details such as that could be used to cross reference details against other found information

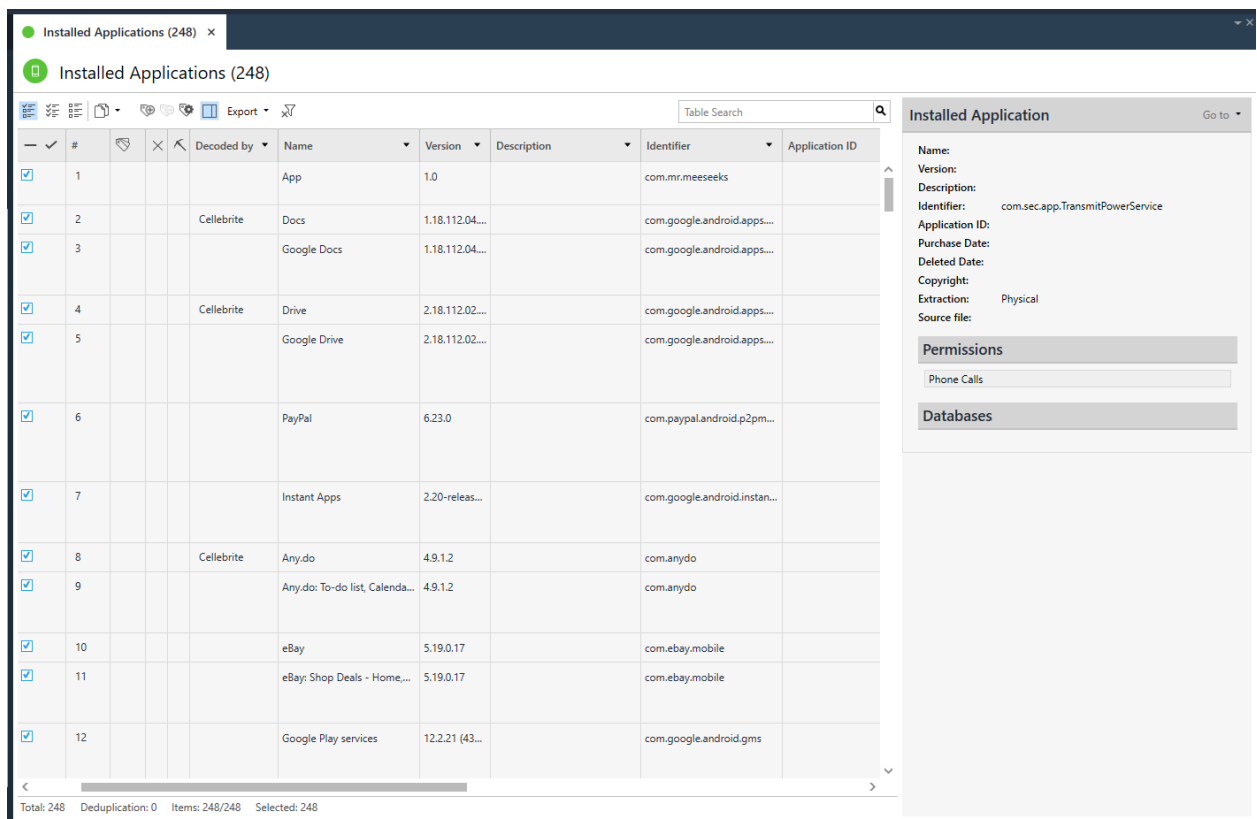
Timestamp	Subject	Source	From	To	Attachement
05/04/2018 11:02:59(UTC-7)	Reminder: You're close to tech bliss	Gmail	GeekSquad@emailinfo.geeksquad.com	HRYANWUPHF@gmail.com	
04/04/2018 18:43:09(UTC-7)	Check your Google	Gmail	no-reply@accounts.google.com	hryanwuphf@gmail.com	

	Account security status				
04/04/2018 12:01:33(UTC-7)	Your Precinct reservation is just around the corner	Gmail	GeekSquad@emailinfo.geekquad.com	HRYANWUPHF@gmail.com	
04/04/2018 11:28:46(UTC-7)	An event from Gmail has been added to your Google Calendar	Gmail	calendar-noreply@google.com	hryanwuphf@gmail.com	
04/04/2018 11:28:39(UTC-7)	Your Precinct reservation is confirmed	Gmail	GeekSquad@emailinfo.geekquad.com	HRYANWUPHF@gmail.com	
04/04/2018 11:27:03(UTC-7)	Information regarding your Best Buy account	Gmail	BestBuyInfo@emailinfo.bestbuy.com	hryanwuphf@gmail.com	
03/04/2018 12:38:09(UTC-7)	Fwd: Congratulations, your item sold!	Gmail	techie6739@gmail.com	hryanwuphf@gmail.com	YES
03/04/2018 11:49:03(UTC-7)	Fwd: Congratulations, Steve, your item has been listed.	Gmail	techie6739@gmail.com	hryanwuphf@gmail.com	
03/04/2018 11:45:17(UTC-7)	Answer 2 questions and get 50% off Any.do Premium	Gmail	newcustomers@any.do	hryanwuphf@gmail.com	
03/04/2018 11:36:37(UTC-7)	Fwd: Congratulations,		techie6739@gmail.com	hryanwuphf@gmail.com	YES

	Steve, your item has been listed.				
03/04/2018 10:53:25(UTC-7)	Fwd: Congratul ations, Steve, your item has been listed.		techie6739@gmail.com	hryanwuphf@gmail.co m	
02/04/2018 19:23:29(UTC-7)	Fwd: Your Amazon.c om order of "(25) Empty Standard.. ." has shipped!		techie6739@gmail.com	hryanwuphf@gmail.co m	YES
02/04/2018 18:54:44(UTC-7)	Fwd: Activate your new account		techie6739@gmail.com	hryanwuphf@gmail.co m	
02/04/2018 17:49:41(UTC-7)	Ryan, finish setting up your Google Photos account		noreply-photos@google.com	hryanwuphf@gmail.co m	
02/04/2018 11:40:41(UTC-7)	Welcome to Any.do!		feedback+welcome@e- mail.any.do	hryanwuphf@gmail.co m	
31/03/2018 17:59:02(UTC-7)	Critical security alert		no- reply@accounts.google.com	hryanwuphf@gmail.co m	
31/03/2018 17:56:03(UTC-7)	Ryan, welcome to your new Google Account		andy-noreply@google.com	hryanwuphf@gmail.co m	

Installed Applications

There are over 248 installed applications available in this image, searching through the installed applications there were no applications that would come in interest as the apps where all default applications that comes with the device



MMS Messages

There were 5 MMS messages stored on the image they included contact regarding XBOX information

Timestamp	Source	From	To	Message
05/04/2018 09:20:03(UTC-7)		8053031855		Just have to place in the Xbox 360 case and we are good to go on a couple orders! I will bring them by today for you to slip them past your boss.

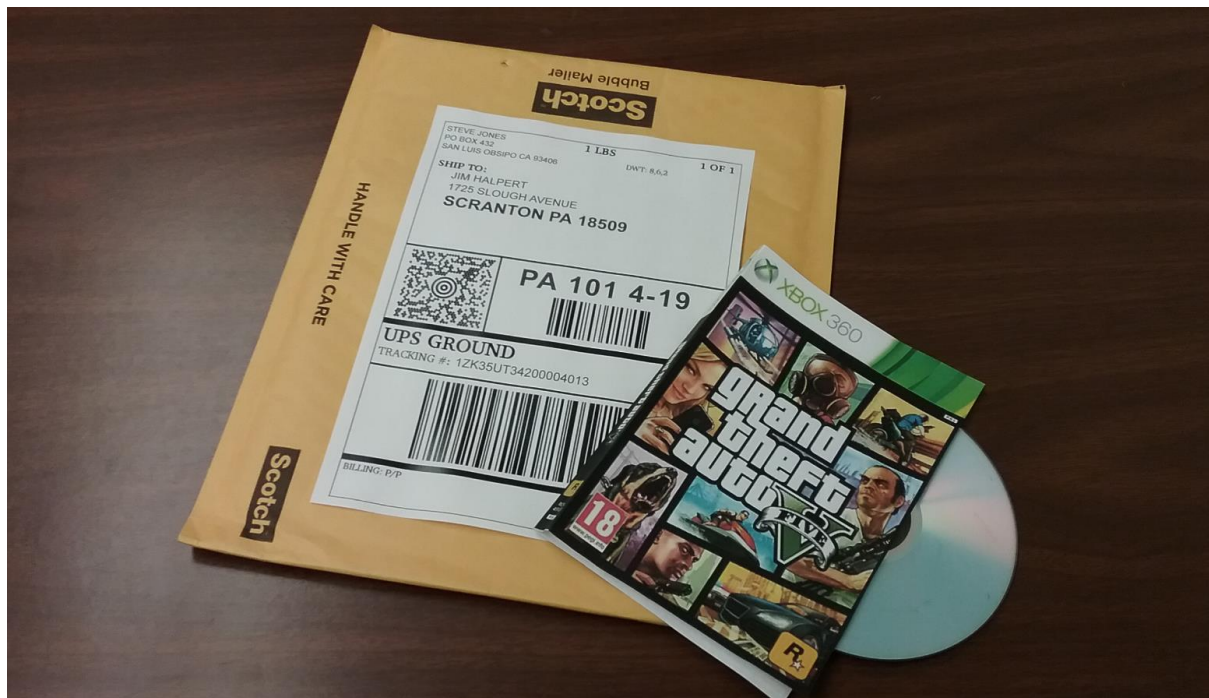
Below is the attachment for the text message, it contained the address for Jim Halpert of 1725 Slough Avenue, Scranton PA, 18509



The address that was on the envelope was not found using google maps

Timestamp	Source	From	To	Message
05/04/2018 09:20:03(UTC-7)	Verizon Message+	+18059105153	+18053031855	Just have to place in the Xbox 360 case and we are good to go on a couple orders! I will bring them by today for you to slip them past your boss.

Below is the attachment for the text message, it contained the address for Jim Halpert of 1725 Slough Avenue, Scranton PA, 18509



Timestamp	Source	From	To	Message
04/04/2018 08:58:22(UTC-7)		8053031855	8059105153	This file contained an Application as a .zip that was un- openable

Below is the attachment for the text message, it contained a box of what looks like postage envelopes



Timestamp	Source	From	To	Message
04/04/2018 08:58:22(UTC-7)	Verizon Message+	+18053031855	+18059105153	This file contained an Application as a .zip that was un-openable

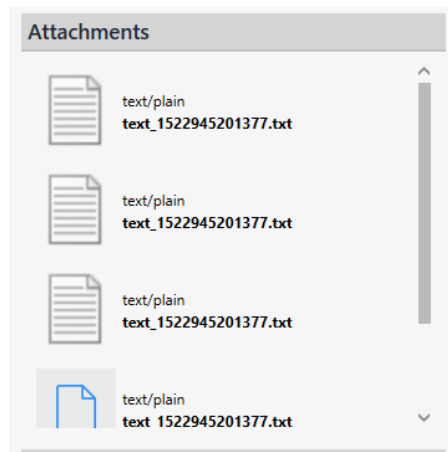
Below is the attachment for the text message, it contained a box of what looks like postage envelopes



Timestamp	Source	From	To	Message
DELETED				<p>Just have to place in the Xbox 360 case and we are good to go on a couple orders! I will bring them by today for you to slip them past your boss.</p> <p>Just have to place in the Xbox 360 case and we are good to go on a couple orders! I will bring them by today for you to slip them past your boss.</p> <p>Just have to place in the Xbox 360 case and we are good to go on a couple orders! I</p>

				will bring them by today for you to slip them past your boss.
--	--	--	--	---

Below is the attachment for the text message, it contained a box of what looks like postage envelopes



The text files that were attached to this MMS message contained the data of the past text messages.

Notes

Creation	Modification	Title	Message	App
04/04/2018 08:23:15(UTC -7)	04/04/2018 08:35:29(UTC -7)	eBay Scammin g Notes	- Make closing dates soon after posted as the pressure makes people fall for the scam (ie. Grand Theft Auto V) - Prices should be low enough to entice buyers but high enough for profit - Use high quality photos and official product descriptions - Ensure bubbles in bubble mailer are mostly popped to back up the fact that the disc is damaged - Use P.O. Box to send from, fake name, and dummy email address	Samsun g Notes
02/04/2018 11:40:23(UTC -7)	02/04/2018 11:46:22(UTC -7)	Notes on eBay Privacy	http://www.dummies.com/business/online-business/ebay/protecting-your-privacy-on-ebay/ Use a non-personal email and username to ensure privacyCreate a PayPal account for transfer of moneyRather than home phone number, provide eBay with a cellphone numberGuard your password	Samsun g Notes

Stored Passwords

Bellow you can see stored password hashes on the system; this includes the google logins and wireless keys that are also stored on the system

Account	Stored Data	Service
Dunder MifflAN	edbcd67794d89228e8c532e1c3461c5bd008bf86cea99601c82b9341bb7531b2	WIFI
hryanwuphf@gmail.com	aas_et/AKpplNYZID3LOe9XdOwgZTYTQCT-N9NoTZv4Y9vLWE0wZyCK8bGYKfti_MtBrIRRByeb8UxfQgONV7kiJcYRJTRnGQadCEfhzTdyVxG3bhmcDTlgqYIyQDtFZKhWoo_fvg==	com.google

Search Items

There where multiple searches saved from google searches, most where the same queries or junk data queries, but there were some interesting ones that will be listed below these searches where related to scamming on eBay and location addresses

Timestamp	Queried	Source
05/04/2018 11:02:59(UTC-7)	255 MADONNA RD SAN LUIS OBISPO CA	Gmail
04/04/2018 11:43:32(UTC-7)	1179 Atascadero St, San Luis Obispo, CA 93405	Google Maps
04/04/2018 11:28:39(UTC-7)	255 MADONNA RD SAN LUIS OBISPO CA	Gmail
04/04/2018 11:19:55(UTC-7)	watch dogs xbox 360 printable cover	Chrome
03/04/2018 11:49:03(UTC-7)	2145 Hamilton Avenue, San Jose, CA 95125	Gmail
02/04/2018 18:54:44(UTC-7)	2211 N. First St., San Jose, CA 95131	Gmail
02/04/2018 17:49:41(UTC-7)	1600 Amphitheatre Parkway, Mountain View, CA 94043	Gmail
02/04/2018 11:30:07(UTC-7)	protecting privacy on ebay	Chrome
02/04/2018 11:17:36(UTC-7)	scams on ebay	Chrome
31/03/2018 17:56:03(UTC-7)	1600 Amphitheatre Parkway, Mountain View, CA 94043	Gmail

SMS Messages

There were 34 SMS messages saved on the device, I will paste bellow messages that maybe of interest during the investigation, they include whether they were deleted and the contact at which they were sent to this information can be used to cross references conversations along with past searches and locations

Contact	Timestamp	Message	Deleted
8053031855	05/04/2018 09:32:15(UTC-7)	Great! I'm excited to hear about the profit. I will make sure the packages get through.	
8053031855	05/04/2018 09:21:19(UTC-7)	Looks like we should be reaching a couple hundred for this week and last.	YES
+18059105153	04/04/2018	Good. I switched to Xbox 360 games	

	09:56:34(UTC-7)	on eBay now.	
8053031855	04/04/2018 09:18:11(UTC-7)	What is the new product you are using to profit on eBay anyways?	

User Accounts

There are multiple user accounts configured on the device, these can be seen below they contain information such as accounts used and where they are used and in some cases it contains passwords

Name	Username	Password	Service
	hryanwuphf@gmail.com		
	hryanwuphf@gmail.com	aas_et/AKppINyZID3LOe9XdOwgZTYTQCT-N9NoTZv4Y9vLWE0wZyCK8bGYKFti_MtBrIRRBByeb8UxfQgONV7kiJcYRJTRnGQadCEfhzTdyVxG3bhmcDTlgqYlyQDtFZKhWoo_fvg==	com.google
	hryanwuphf@gmail.com		com.anydo.account
	vnd.sec.contact.phone		vnd.sec.contact.phone
	primary.sim.account_name		vnd.sec.contact.sim
	vnd.sec.contact.agg.account_name		vnd.sec.contact.agg.account_type
	hryanwuphf@gmail.com		Gmail
	hryanwuphf@gmail.com		Google Maps
	8059105153		MMS
	hryanwuphf@gmail.com		Google Drive
hryanwuphf@gmail.com	1522691789490		Google Client ID
Ryan Howard	hryanwuphf@gmail.com		Google Photos

Web History

There were over 196 entries into the Web History, the information. The searches were Google Calendar, BestBuy, Geek squad, Amazon, Game Cover art, PayPal, eBay and a Website for looking up scammers on eBay and the scams they have run. This information also includes dates of the search and where the information was saved to.

Web History (196)

Table Search

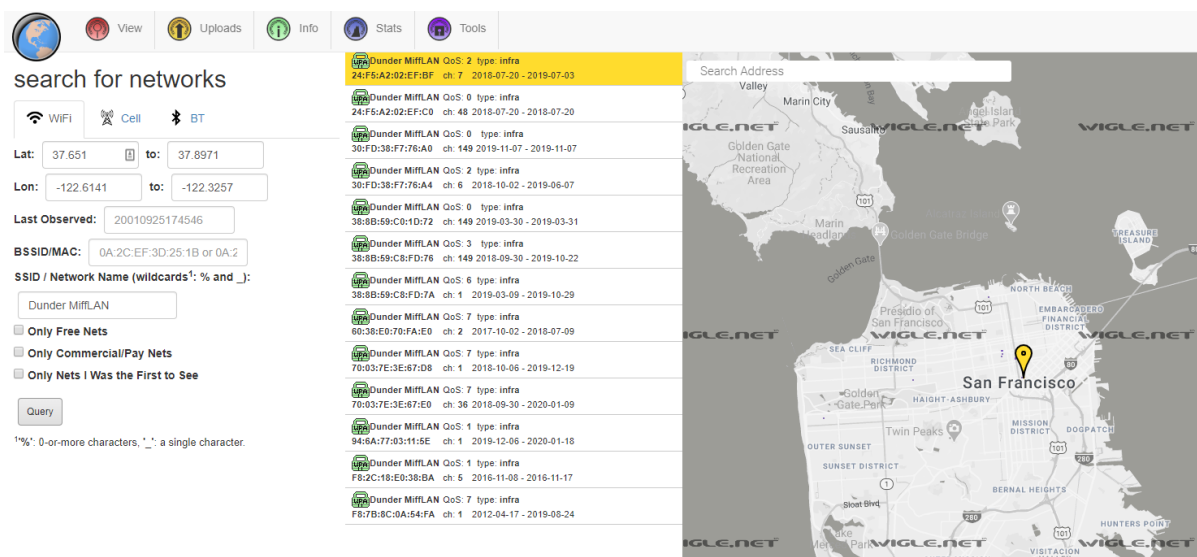
	✓	#		×	↶	↓ Last Visited	Title	URL
<input checked="" type="checkbox"/>		1				04/04/2018 11:37:31(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		2				04/04/2018 11:37:29(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		3				04/04/2018 11:37:27(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		4				04/04/2018 11:37:25(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		5				04/04/2018 11:37:24(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		6				04/04/2018 11:37:22(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		7				04/04/2018 11:37:19(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		8				04/04/2018 11:37:13(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		9				04/04/2018 11:37:09(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		10				04/04/2018 11:37:06(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		11				04/04/2018 11:37:02(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		12				04/04/2018 11:37:00(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		13				04/04/2018 11:36:59(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		14				04/04/2018 11:36:56(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		15				04/04/2018 11:36:55(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		16				04/04/2018 11:36:49(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		17				04/04/2018 11:29:58(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		18				04/04/2018 11:29:55(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&output=xml
<input checked="" type="checkbox"/>		19				04/04/2018 11:29:47(UTC-7)	https://calendar.google.com/calendar/r/eventedit?text=Your+G	https://calendar.google.com/calendar/r/eventedit?text=Your+G
<input checked="" type="checkbox"/>		20				04/04/2018 11:29:45(UTC-7)	https://calendar.google.com/calendar/r/eventedit?text=Your+G	https://calendar.google.com/calendar/r/eventedit?text=Your+G
<input checked="" type="checkbox"/>		21				04/04/2018 11:29:45(UTC-7)	https://calendar.google.com/calendar/render?action=TEMPLATE	https://calendar.google.com/calendar/render?action=TEMPLATE

Wireless Network

There is only one entry the WiFi with no security key, this can be seen bellow, but can be used to check against other information found

SSID	Security Mode
Dunder Mifflan	WPA-PSK

Checking this SSID against a tool called Wingle, we can see it belongs to a location in California that matches up with other data



Files on the systems

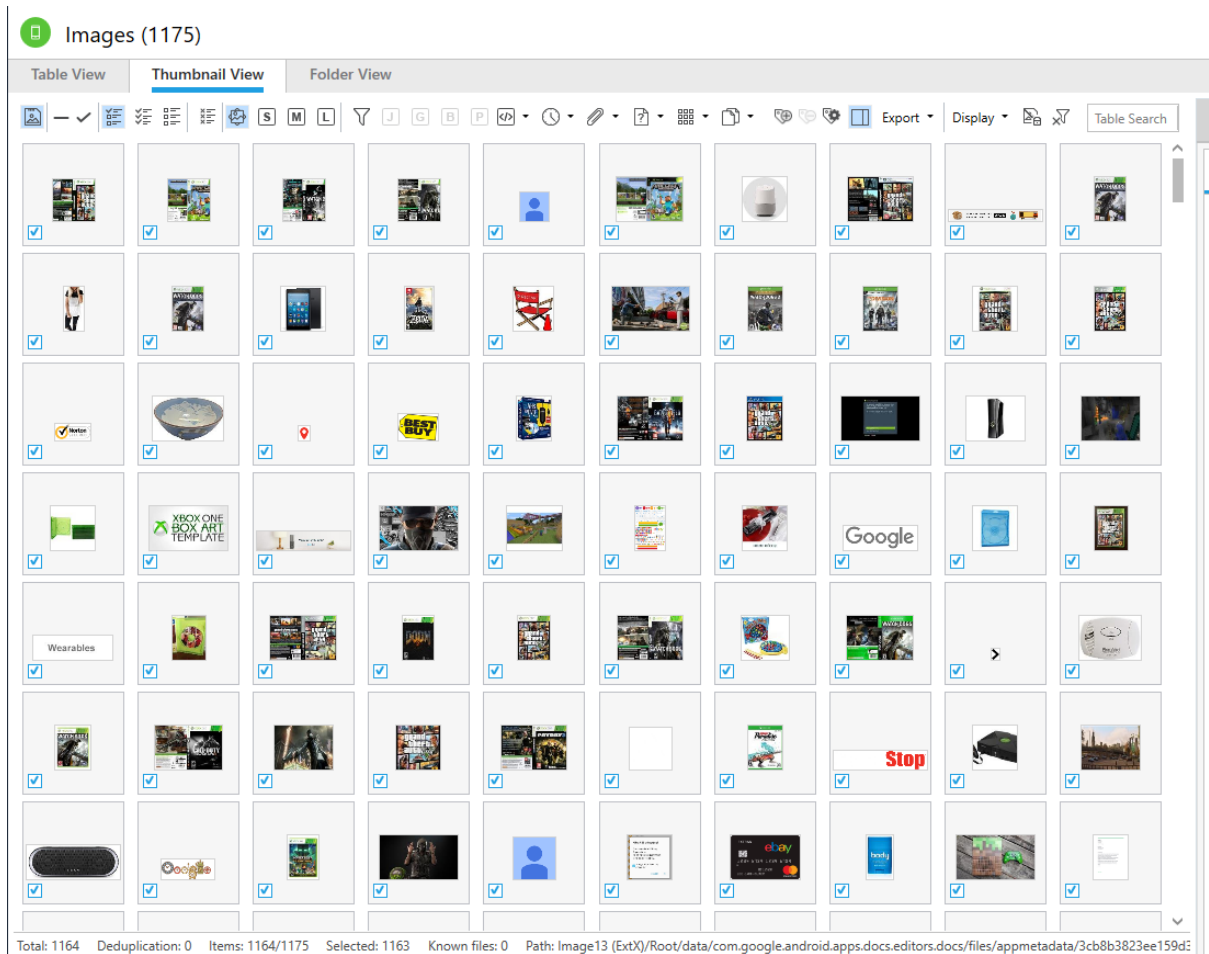
There were 4 documents found on the system these documents included a PayPal statement and receipts, these documents will be listed below, they included the documents location, creation and modification date if they were modified by the user.

Name	Path	Created	Modified
0_a3a23708-d8a7-4008-870a-d83ed0a7399c_blob	Image13 (ExtX)/Root/data/com.google.android.apps.docs/files/shiny_blobs/blobs/0_a3a23708-d8a7-4008-870a-d83ed0a7399c_blob	04/04/2018 12:58:46(UTC-7)	04/04/2018 12:58:53(UTC-7)
Paypal.pdf	Google Drive Files hryanwuphf@gmail.com/Shared With Me/My Drive/Paypal.pdf	04/04/2018 12:57:33(UTC-7)	04/04/2018 12:57:33(UTC-7)
Receipt Order #126-5680132-2492337.pdf	Google Drive Files hryanwuphf@gmail.com/Shared With Me/My Drive/Receipt Order #126-5680132-2492337.pdf	02/04/2018 19:25:10(UTC-7)	02/04/2018 19:25:10(UTC-7)
Receipt Order #126-5680132-2492337.pdf	Google Drive Files hryanwuphf@gmail.com/Shared With Me/Receipt Order #126-5680132-2492337.pdf	02/04/2018 19:24:46(UTC-7)	02/04/2018 19:24:46(UTC-7)

Images

There was over 1175 images on the device, 22 of these images were deleted, from analysis a lot of these images seem to be cached from websites the user was viewing. The images found show that the user was looking at multiple forms of video game covers and CD covers, these could be related

to messages found that would indicate a user was printing the covers. In the image data there is metadata and creation and modification data for each image that is on the system



Investigators notes:

From the information provided in the image, there are certain factors that are interloped, these factors include the production of fake CD's using copywriter material that is been sold on online stores such as eBay. It is highly probable that owner of this phone could be involved in online scamming due to the evidence that is portrayed in this image, but that is up for the detective involved to decided.