

# Windows and Android Forensics CCIC Training

Chapter 0: Preamble

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 0

# **Preparing for the CCIC 2019**

The 2019 California Cyber Innovation Challenge (CCIC) will be hosted by the California Cybersecurity Institute (CCI) on June 21-23. Training is provided for the DFC at <u>https://cci.calpoly.edu/events/ccic/2019-df-downloads</u>.

As part of the DFC, teams will be presented with a case where digital AND physical evidence will have to be collected, verified, analyzed, and a criminal case will have to be assembled on a timeline and presented to a judge. Digital forensics, critical thinking, teamwork and communication skills will all be tested as part of this event.

In preparation of the DFC, it is highly recommended that the DFC training is completed by all team members. The Windows and Android Forensics CCIC Trainings are designed to take an inexperienced high school student about 22-27 hours to complete. However, the trainings can be split amongst team members to be specialized within areas of Windows and Android Forensics resulting in about 6-8 hours per student.

The DFC training serves as a primer - which covers the necessary skills for teams to compete in the challenge. However, there will be portions of the DFC that will NOT be covered by the DFC training, and your team's ability to handle these unexpected challenges will be a part of your team's overall success.

#### What is Digital Forensics and how will it be used in the CCIC 2019?

Digital Forensics is a subset of the field of forensics science and has evolved out of computer forensics as digital devices now not only include computers, but other digital devices. Nearly all modern day crimes now have a digital element. However, there is a large divide between the number of law enforcement officers with formal training in Digital Forensics and the number of crimes with a digital element. The DFC is designed to highlight some of these challenges and we believe serves as an example of how "human" cyber problems can be.

Digital Forensics can be broken down into multiple stages, which include:

- 1. Seizure Focusing on the preservation of evidence to be legally permissible in court
- 2. Acquisition Ensuring evidence is forensically sound (authentic and not tampered with)
- 3. Analysis Identifying the evidence and establishing a timeline for the crime
- 4. Reporting Putting together a concrete case, often for a non-technical audience

#### Seizure

After an introduction of the DFC on June 24th, teams will be issued a blanket warrant for searching allocated space(s) to search and seize digital evidence. Please refer to the Windows and Android Forensics CCIC Trainings on the proper seizure of evidence

#### Acquisition

The acquisition stage of the DFC will be aided by "forensics technicians." Teams that seize a piece of digital evidence will be turning these devices to a "forensic technician" in exchange for a USB drive with a forensics image (creating a forensics image may take several hours). Drive hashes should still be verified upon receipt of the forensics image and once again at the end of the Analysis phase. The Windows and Android Forensics CCIC Trainings will help prepare teams in this regard, but the DFC will provide forensics images to all competitors to avoid long imaging durations.

#### Analysis

Due to the complexity of the field of Digital Forensics, the DFC's evidence will focus mostly on Windows and Android-based forensics and serves as the bulk of the training. Note that there will be some physical evidence and other digital elements as part of the DFC which will require teams to be able to integrate evidence from multiple sources.

#### Reporting

After the Analysis phase, teams will have to make an oral presentation (aided by a presentation slide deck, if desired) to a series of judge advocates. The report should focus on the "Who, What, Where, When, and How" will/did this crime take place, and provide evidence supporting these findings. Additionally, teams will be asked to provide recommendations for remediation - what should be done at the outcome of their findings.

## **Open-Source Tools for Trainings**

All tools utilized in these training manuals are open-source and therefore available for download through the links provided.

Prior to starting the trainings, you will want to install/have access to the following tools on your PC:

#### **Windows Forensics**

- 1. <u>Autopsy</u> and/or Sleuthkit
- 2. <u>Registry Explorer</u>
- 3. Ophcrack v 3.7 and Vista Free Table
- 4. Autopsy's Multi Content Viewer 3rd Party Plugin
- 5. <u>DCode v 4.2</u>
- 6. JumpLister v 1.1.0
- 7. <u>USB Historian v 1.3</u>
- 8. <u>SkypeLogView v 1.55</u>
- 9. <u>7Zip v 16.04</u>
- 10. USB Deview

#### **Android Forensics**

- 1. QuickHash GUI
- 2. Google Map Creation
- 3. <u>Thunderbird Mail</u>

Additionally, you may want to download the Windows and Android Forensics CCIC Training manuals and training images located at: <u>http://cci.calpoly.edu/ccic</u>.

**Note:** UFED Reader is a free program provided with the creation of an extraction report and therefore is not an executable which can be downloaded online.

### **Recommended Training Schedule**

It is recommended that all team members complete all training materials. The following is a recommended training schedule, assuming that team training session are each about 1-2 hours long:

#### Windows Forensics

- Chapters 1-4 Introduction, Starting a Case, Drive Geometry, Image Verification, Registry
- Chapter 5 Windows File Overview
- Chapter 6 Recent Files
- Chapters 7-8 Recycle Bin, External Storage Devices
- Chapter 9 Email
- Chapters 10-11 Internet History, Chat Logs
- Chapter 12 Hidden Data
- Chapter 13 Installed Programs
- Chapter 14 Legality, Reporting
- Appendices, as time allows

#### **Android Forensics**

- Chapters 1-3 Introduction, Secure the Device, Data Extraction with UFED
- Chapters 4-6 Image Verification, UFED Reader Basics, Lock/Home Screens, Personal Files
- Chapters 7-9 Installed Applications, Contacts, Phone, Messaging, Location Data
- Chapter 10-11 Calendar, To-do Lists, Notes, Email, Internet History
- Appendices, as time allows

**Note:** Android Forensics Chapter 3 on Data Extraction with UFED is for your team's knowledge of understanding the mobile forensics process. You will exchange any mobile phone(s) for a USB drive containing a physical data extraction during the competition.

The training manuals will be available to all teams during the competition, but familiarity with the topics in the training manuals will greatly impact your team's performance. It is therefore also recommended immediately prior to the CCIC that individual team members are assigned to "own and review" one or more of Chapters 6-14 of Windows Forensics and Chapters 4-11 of Android Forensics.

## Questions

If you have any questions about the CCIC, or the CCI in general, please do not hesitate to email us at <u>cci@calpoly.edu</u>.



## **Android Forensics CCIC Training**

## Chapter 1: Introduction

Cassidy Elwell and James Poirier April 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 1

# Introduction

For the CCIC Event, your team will be asked to do analysis on a variety of devices as a part of a digital forensics challenge. This documentation on Android mobile forensics, in addition to the Windows computer forensics documentation (located at <u>www.cci.calpoly.edu</u>), will show you how to conduct analysis on digital evidence obtained from an Android mobile phone and the legalities behind seizing and searching digital evidence. In this training, you will walk through the Ryan Howard case. The scenario is as follows:

## **Ryan Howard Scenario**

eBay routinely reviews customer business practices to ensure they are within policies such as "Offers to Buy or Sell Outside of eBay Policy," "Excessive Shipping Charges Policy," and "Avoiding eBay Fees Policy." Within the last month, several accounts were flagged based on behavior which indicated offeBay transactions were being offered. These sellers have been put under strict surveillance, but no action has been taken against their accounts, yet. Shortly after this review, eBay received contact from Best Buy's Geek Squad Services about an individual suspected of manufacturing and selling fraudulent Xbox video games through eBay.

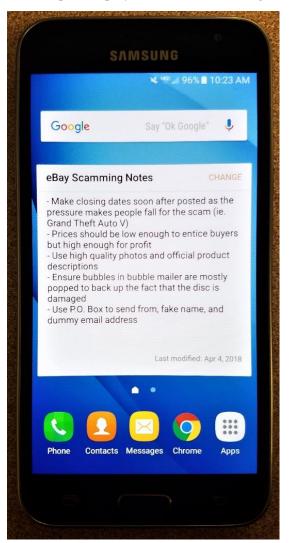
Since the discovery, eBay has continued to watch the suspect's seller account. Geek Squad has contacted the San Luis Obispo Police Department to arrest and prosecute Howard for theft.

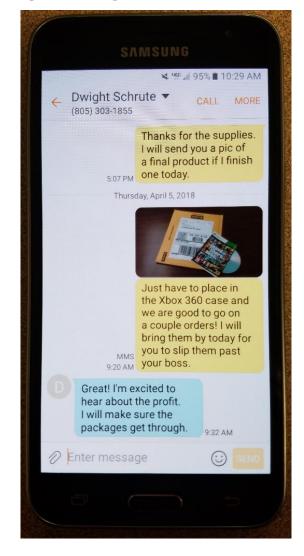
On April 5<sup>th</sup>, Ryan Howard was detained by Best Buy security as he attempted to pick up his mobile device from the Geek Squad Service's associate who had been solving a technical glitch Howard claimed to be having on his device.

San Luis Obispo Police Department Officer Diaz interviewed Howard and he denied all allegations. A search warrant was obtained, even though Howard consented, to search his mobile device, as the device may contain incriminating evidence.

You have been provided with a UFED physical extraction of his mobile device. Based on the search warrant, you are authorized to search for any information or communication associated with creating, selling, and profiting from fraudulent product transactions on eBay.

The Geek Squad employee found the following on the suspect's mobile phone:







## **Android Forensics CCIC Training**

## Chapter 2: Secure the Device

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 2

## **Secure the Device**

## Introduction

With mobile devices constantly updating how they store and access data, first responders often do not know how to properly handle devices. It is critical to have protocols in place on how to handle devices, depending on their state, prior to the analyst receiving it. In this chapter, you will learn the critical details behind ensuring a seized mobile device's evidence remains forensically sound and accessible to you as a forensic examiner.

### **Properly Handling a Seized Device**

The first observation to be made when a mobile device is seized from a crime scene should be to determine whether the device is ON or OFF. This is important in determining what action should be taken to ensure the device cannot be wiped remotely or authentication cannot be surpassed. Use the flowchart below (Figure 2-1) on how to approach properly handling a mobile device.

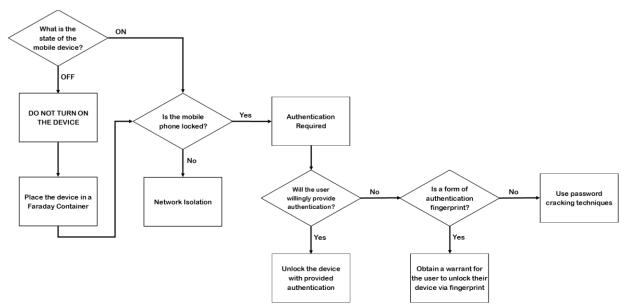


Figure 2-1: Properly Handling a Mobile Device Flowchart

### **Authentication Required**

Locked devices are very common due to security and privacy being widely important to device users, both consumer and commercial. With security awareness continuing to be on the rise, individuals are ensuring their devices require a passcode of some type. Device manufacturers are constantly adding additional security options with hardware and software updates. For example, newer mobile devices have the option of facial recognition and fingerprint lock types. These types are deemed more secure than the average four number pin or swipe pattern passcodes.

When finding a device, the most important thing to consider is if there is an opportunity available to disable or surpass the passcode created by the suspect. This is another situation where minimal changes to the settings of the device need to be made to ensure full access to the data. Therefore, quick action is required for a device found unlocked as there is a short window of time (on average user have set to 30-60 seconds) of full access capabilities before the device will lock and request the passcode once again. There are two options in this situation:

1. Increase the time before the screen locks and execute minimal activity on the device as to remain having accessibility. This typically can be accomplished by locating the "Settings" application on the device, selecting "Display," and then changing the value of "Screen timeout." Change the value to the max selection available (often 10 minutes).

😵 🔤 🛛 🔌 🐇 🚛 📋 2:47 PM	🏶 🖬 🛛 🔌 🐇 📶 🚊 2:47 PM		⊴ 47% ≣ 2:44 PM	⊇ ¥I જ ∞ al 469	%≣ 2:45 PM
🤯 Settings	🧑 Display	SETTINGS	Q :	< DISPLAY	
S Data usage	Тор	🤶 Wi-Fi		Clock, All day	
	General	Bluetooth		Night clock	
More	Brightness	(()) Mobile Hotspot and	Tethering	Show a clock on the Edge screen while the main screen is turned off.	
evice	Caraan mada	Data usage		LED indicator Light up the LED indicator when	
Call settings	Screen mode Select the screen mode	Mobile networks		charging, voice recording, or receiving notifications.	
Sound	Auto-rotate screen 🗹	Advanced Calling		Status bar	
	Screen timeout	((t) More	(	Screen timeout After 10 minutes of inactivity.	
🗘 Display	After 30 seconds of inactivity	PHONE		Screen saver	
	Font style	Sounds and vibratio	n	Show a screen saver after the screen turns off automatically while the	
🏡 Power saving mode	Set font	Notifications		phone is charging.	
<b>Storage</b>	Pulse notification light	Display		Keep screen turned off Prevent the screen from turning on accidentally while the phone is in a dark	
	Sind data -	Edge screen		place such as a pocket or bag.	

Figure 2-2: Version 4.2 (Jelly Bean) vs Version 7 (Nougat) "Screen timeout" within "Display"

2. Enable "Stay Awake" using Developer options and connect the device to be charged which will result in the device never sleeping. First, the Developer options will need to be enabled on the device by selecting "About phone" within the "Settings" application and then locating the "Build number." Then press on the "Build number" seven times in a row which will add "Developer options" to the "Settings" application. Now select "Developer options" and agree to the pop-up window. Lastly, enable the "Stay awake" toggle and connect the device to a power source.

Note: "Stay Awake" may not be a capability on all devices, depending on the manufacturer.

¥€ 😤 🖙 ⊿í 47% 🗎 2:43 Pi	M 🖬 🙀 😤 🖅 🖼 47% 🛢 2:43 PM	I 🖬 👫 😤 🖅 🖬 47% 🚊 2:44 PM	🖬 🕷 😤 ™ 🗐 47% 🖹 2:44 PM
SETTINGS Q :	< ABOUT PHONE	SETTINGS Q :	< DEVELOPER OPTIONS
Envacy and emergency		→ Easy mode	On 🔹
🔂 Easy mode	Android version 7.0	🖉 Accounts	Submit bug report
Accounts	Security software version	G Google	
Google	MDF v3.0 Release 1 WLAN v1.0 Release 1 VPN v1.4 Release 8.2 ASKS v1.4 Release 161228	A Language and input	Desktop backup password Full desktop backups are not currently protected.
A Language and input	SMR Jan-2018 Release MS	Backup and reset	Stay awake
	Android security patch level	SYSTEM	Screen will never sleep while charging.
Backup and reset	January 1, 2018	Date and time	Bluetooth HCI snoop log
Date and time	Baseband version G935VVRS4BRA1	* Accessibility	Capture all Bluetooth HCI packets in a file.
Second Accessibility	Kernel version 3.18.31 Press SEVEN times	? Help	OEM unlock Allow the phone to be OEM unlocked.
? Help	dpi@SWDG4513 #1 Mon Jan 8 10:51:36 KST 2018	(i) About phone	Running services
(i) About phone	Build number	J System updates	View and control currently running services.
	NRD90M.G935VVRS4BRA1		WebView implementation
System updates	SE for Android status	Developer options	Chrome Stable

Figure 2-3: Version 7 (Nougat) "Stay awake" with "Developer options" Enabled

In the case that such an opportunity does not present itself, obtaining the passcode information from the device's user can be accomplished (Figure 2-1) with a warrant or using password cracking techniques, as necessary.

#### **Network Isolation**

When a mobile device is seized from a crime scene, it is priority to ensure that the device is isolated from all mobile data and Wi-Fi connections. If this is not done immediately, a suspect could remote wipe their device resulting in the worst-case scenario for you as a forensic examiner: device evidence is unrecoverable. Remote wipes can be accomplished by a suspect via internet connections, SMS, or through third party applications and pre-created cloud backups.

However, when accomplishing network isolation, a forensics investigator's goal is to maintain the integrity of the data on the mobile device for analysis, nothing more than minimal changes should be made. There are a variety of solutions to establish network isolation of a device, but often the best option is to place the device in Airplane mode. The settings may vary slightly depending on the Android device, but the approach should be about the same:

• Press and hold the Power button until a pop-up menu appears and select "Airplane mode."



Figure 2-4: Version 4.2 (Jelly Bean) "Airplane mode" from Pop-Up Menu

• Swipe down from the top of the screen and select the gear icon in the far-right corner. This will open the "Settings" application. Now, select either "Airplane mode" or the wireless option (such as "Wireless" or "Wi-Fi") near the top.

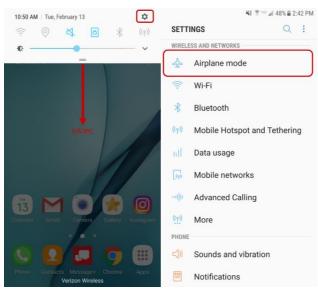


Figure 2-5: Version 7 (Nougat) "Airplane mode" from Swipe Menu

• Press Menu or Apps from the home screen and then select the "Settings" application. Now, select either "Airplane mode" or the wireless option (such as "Wireless" or "Wi-Fi") near the top.



Figure 2-6: Version 4.2 (Jelly Bean) vs Version 7 (Nougat) "Airplane mode" from Settings

The advantages to using Airplane mode to isolate a device include maintaining active data and applications as well as ensuring disconnection form mobile data and Wi-Fi connections. The main disadvantage to this technique is that full access to the device is required. While some may argue that another disadvantage is the modifications you are making to the device, this is not the case as the minimal modifications to the settings of the device do not affect the integrity of the data itself. These changes, however, should be logged in case notes to include the original state of the device, the changes made, the outcome, and why the changes were required.

#### **Device Cables**

While most kits used for extracting data from mobile devices include the necessary cables, it is still necessary to seize any cable pertinent to a seized mobile device. This is due to the possibility that the suspect's device is a newer model. Therefore, charging and connectivity may require a special cable that the forensics kit has not yet acquired. This can significantly change the outcome of the evidence, especially if you are going to do analysis on temporal data (currently running applications), not to mention that the device needs to be charged and without the proper cable, it will lose power. For example, the Google Pixel 2 and Samsung Galaxy S8 (Figure 2-7) have upgraded from micro USB to USC-C cabling.



Figure 2-7: Micro-USB vs USB-C Cables https://www.youtube.com/watch?v=gVU\_9MZ6zME



## **Android Forensics CCIC Training**

Chapter 3: Data Extraction with Universal Forensic Extraction Device (UFED)

> Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

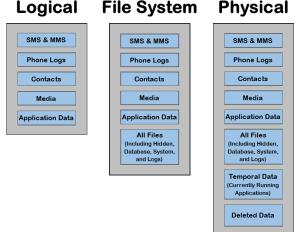
# 5

# **Data Extraction with Universal Forensic Extraction Device (UFED)**

## Introduction

The Universal Forensic Extraction Device (UFED) is a small hand-held, easy-to-use device that extracts data from mobile phones. An examiner can simply plug in the mobile device and a flash drive or external hard drive to download a portion of or an exact copy of the device's memory. From the display screen of the UFED, the examiner may select a data extraction technique, specific data to extract or not to extract, and the location for the extracted data.

There are three types of techniques used to extract data from an Android device: logical, file system, and physical. Each of these techniques can be accomplished with a Universal Forensic Extraction Device (UFED), which is created and maintained by Cellebrite. In this chapter, you will learn about each of the types of data extraction. You will be provided a physical extraction for the CCIC event.



**File System** Physical

Figure 3-1: Logical vs File System vs Physical Extraction

### Logical Extraction Technique

A logical extraction is the quickest and most supported method amongst mobile devices. The UFED device uses an API (Application Programming Interface) to connect and request information from the file system through the device's operating system. After connecting and loading the API, the UFED makes "read-only" API calls to seize allocated data to extract any files that have not be deleted and are accessible to the file system. Therefore, the typical data from a logical extraction would be any data that a third-party application could get access to such as text messages, contacts, media, etc.



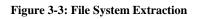
Figure 3-2: Logical Extraction

However, this method of extraction is the most limited out of the three, due to the technique being dependent on the API's available scope (authentication) of information. The API may not have authorization to content within all default and third-party applications. Therefore, to access the content within this category, an examiner would need to access the data in question through the file system directly using another technique. For example, this issue often occurs when devices do not have a common interface such as with email records (Gmail, iCloud Mail by Apple, Samsung Email, third-party email applications).

## File System Extraction Technique

A File System extraction is an extension of the logical extraction that allows the examiner to examine the file system as a whole, rather than just snippets of data. This can include some hidden and deleted data if the method of storing such data was chosen to be a database or logs within the file system. Also, the examiner will have more detailed information from default and third-party applications such as web history, EXIF data about emails and media, and Google Maps destination history.





This method of extraction does require decoding of system and database files since the data is raw, but this is not a concern for basic applications as the UFED Physical Analyzer automatically performs the decryption. Since there are millions of applications on the Google Play Store alone, Cellebrite can only provide programming to decode a portion of applications which include the most popular amongst users (such as Gmail, Facebook, Skype, Twitter, Any.do). Even so, examiners will have access to both the raw and decrypted versions (where plausible) of the device's file system for analysis.

### **Physical Extraction Technique**

A physical extraction is the most extensive method, but with the least support. This method provides an examiner with an exact copy of the device's memory, for better interpretation of the data. Mobile devices are designed to allow the insertion of bootloaders (fragments of code) into their RAM when booted into "recovery mode." Typically, this capability is used by manufacturers and carriers to upgrade software or change service providers on a device. With forensics analysis, a similar technique is used by the UFED in which a bootloader is inserted to cease the regular booting procedure into the operating system and execute "read-only" actions on the device. With this method, an examiner has access to the data in a logical extraction in addition to deleted files, system files, and temporal data (currently running applications).



Figure 3-4: Physical Extraction

This method creates an exact copy of the device, making it the most useful technique for examiners to complete analysis. Examiners can access GPS locations, wireless networks, and Bluetooth connections because they have access to databases stored within the file system itself. The UFED Physical Analyzer is a program that will automatically decode the portion of applications it is capable of processing, similar to the File System extraction method. Therefore, examiners will still have access to both the raw and decrypted versions (where plausible) of the device's file system for analysis as before.

#### Are bootloaders forensically sound?

Yes, the bootloaders used by Cellebrite devices are forensically sound due to in-house creation and "readonly" execution. Cellebrite designs its bootloaders for each device framework with the possible varieties of hardware, drivers, and memory kept in mind to provide a quick analysis that is repeatable. Data integrity is maintained because the Cellebrite bootloader will only execute "read-only" actions and removes itself from the device after completion of the process. In most cases, the Cellebrite bootloader can extract data despite security mechanisms (including a passcode-protected device) because the bootloader is only requesting "read-only" permissions of the memory.

#### What if a bootloader is not available for the device?

With some newer devices, the capability to utilize bootloaders is locked from users, therefore requiring the device to be rooted temporarily to access data. Such a "temporary rooting" is accomplished by the UFED device uploading a Cellebrite client onto the device to extract data. In this situation, the client will write itself to the data partition to the next available unallocated space. This action does not, however, render the analysis no longer forensically sound, as long as carefully documented and the UFED device is set by default to uninstall after extraction. However, this setting can be changed if examiners, or their superiors, desire the client to remain on the device as proof of method. Otherwise, any additional writing of data to a device will be predetermined and must be confirmed by the examiner before the UFED device will take any further actions.

## **UFED Physical Analyzer & Reader**

When the data extraction is complete, regardless of the technique utilized, the UFED will produce a .UFD (text) file to be opened with the UFED Physical Analyzer program on a computer. This file contains information regarding the extraction process (including the UFED serial number, date and time the process occurred, and hash values) and references to the extracted device data. These references are to .ZIP files for a logical extraction and .IMG or .BIN for a physical extraction. Finally, the UFED Physical Analyzer is used to create a report with the extracted data in the form of a UFED Report Package (.UFDR file). The .UFDR is an executable file that uses the UFED Reader program (a free application) to view the data, continue forensic analysis, and generate a PDF or HTML readable report.

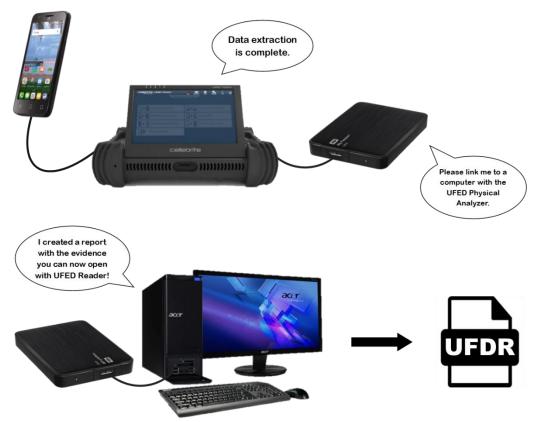


Figure 3-5: Use UFED Software Following Data Extraction



# **Android Forensics CCIC Training**

## Chapter 4: Verify the Forensics Image

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 4

# **Verify the Forensics Image**

## Introduction

Before you even begin your analysis, you always want to first establish a solid foundation. To do so, you want to verify the forensic image's validity by checking its hash value. A hash value is basically the fingerprint of the file. The odds of two MD5 hash values for two different files being the same is 2128. By checking the hash value of the forensic image and comparing it to the hash value when it was imaged, you are confirming that the evidence has not been corrupted or tampered with. This becomes a vital piece of information later when you are being questioned on the integrity of the image and if you missed any partitions or data. The hash value should be checked once again after investigation is complete to ensure that you haven't unintentionally changed your evidence.

## QuickHash GUI

The information that the UFED Reader contains is slightly limited due to its purpose being a free-ware tool for sharing analysis reports with other investigators. If you want to calculate the hash values of your evidence to ensure a forensically sound investigation, you will need to use another tool. For this case, you are going to use a tool called QuickHash GUI. You can download it from:

https://quickhash-gui.org/downloads/

#### **Prior to Beginning Investigation**

Open the QuickHash GUI tool and click on the File tab. Select MD5 from the Algorithm options.

About	r 2018) - The easy and convenient way to hash data in Linux, OSX and Windows	-		×
	opyright © 2011-2018 Ted Smith http://	www.quickhash-gui.org		
ext File File	6 Copy Compare Two Files Compare Two Folders Disks Base64 Data			
Algorithm	Single File Hashing			
<ul> <li>MD5 </li> <li>SHA-1</li> <li>SHA256</li> <li>SHA512</li> <li>xxHash64</li> </ul>	Start at a time:     Select File or drag n drop a file <sup></sup>			
· AATIBATION	File being hashed			
	Computed hash will appear here			
	Switch case     Expected Hash Value (paste from other utility before or after file hashing)			
	Expected Hash value (paste from other utility before or after file hashing)		_	
	Clear Hash Field			

Figure 4-1: QuickHash GUI Single File MD5

Click the button Select File and navigate to where the folder is containing your evidence (extracted data) and select the image file with extension UFDR. Click Open when you are done to start the process.

**Note:** You do NOT want to select "UFEDReader.exe" or files with the extension PAS. These files do not contain any of the evidence of interest, but rather only data to run the forensics software and maintain your overlay of forensic tags (to be explained in Chapter 5).

0	apyright © 2011-2018 Ted Smith	http://www.qu	ickhash-gui.org	
t File FileS	Copy Compare Two Files Compare Two Folders Disks Base64 Data			
Algorithm	Single File Hashing			
@ MD5	□ Start at a time:			
C SHA-1				
C SHA256 C SHA512	Select File or drag n drop a file			
C xxHash64	Select File or drag n drop a file			
	File being hashed			
	Con # Open existing file		×	-
	← → v ↑ → This PC > Desktop > Howard Case ← v ♂	Search Howard Ca	se "Ø	
	□ S Organize ▼ New folder		• 🔟 🕜	
	Expe A Quick ad	Date modified	Туре	
	Des      AccountPackage		File folder	
	Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_Report.ufdr UFEDReader.exe	4/5/2018 4:29 PM 2/19/2018 5:05 PM	UFDR File Application	
	Doc #	2/19/2010 3/03 PM	Application	
	Fict 🖈			
	Ted 🖈			-
	💪 Goc 🖈			
	Anc #			
	CneDriv			
	This PC			
	→ Network × <		>	
	File name: Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_Rep	All files (*.*)	~	
	Samsung CDMA_SM-J320VPP Galaxy J3 2010_2018-04-05_Kep	V All thes (1.7)	~	

Figure 4-2: Select the .UFDR File for MD5 Hash Calculation

You will begin to see the tool's progress in calculating the hash value below and then displayed in the gray shaded box.

QuickHash v3.0.2 (Mar 2018) - The easy and convenient way to hash data in Linux, OSX and Windows	-		×
File About			
Copyright © 2011-2018 Ted Smith http:/	/www.quickhash-gui.org		
Text File FileS Copy Compare Two Files Compare Two Folders Disks Base64 Data			
Algorithm Single File Hashing			
<sup>C</sup> MD5 <sup>C</sup> Start at a time:               Started at : 10/04/2018 11:04:48 <sup>C</sup> SHA256			
C SHA512 Select File or drag n drop a file			
C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_Report.u	ldr		
		-	
☐ Switch case			
Expected Hash Value (paste from other utility before or after file hashing)			
Clear Hash Field			
42%			
HASHING FILEPLEASE WAIT 🛻			

Figure 4-3: Hash Calculation Begins and the Timestamp is Displayed

Following the investigation, you will need to prove your case is forensically sound. Open a text editing program such as Notepad (https://notepad-plus-plus.org/). Copy the MD5 hash and the timestamps specified by the tool. Save this file for future reference.

	Copyright © 2011-2018 Ted Smith http://www.quickhash-gui.org
File Fil	ileS Copy Compare Two Files Compare Two Folders Disks Base64 Data
Algorithm	Single File Hashing
MD5 SHA-1 SHA256 SHA512 xxHash64	Start at a time:         Started at : 10/04/2018 11:04:48           Ended at : 10/04/2018 11:04:51         Time taken : 00:00:02
	C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_Report.ufdr
	9359D96FCAB33D7F8407F0484245AF04
	Switch case <ul> <li>Whot to Investigation Hash Value tot - Notepool</li> <li>             Expected Hash Value (paste from of File Edit Format View Help             <li>             C:\Users\climetaive\Desktop\Howard Case\Samsung CDMA_SM-J320VPP Galaxy J3 201             </li> <li>             Clear Hash Field             </li> <li>             MASHING COMPLETE!             </li> <li>             Tame taken: 00:00:02             </li> </li></ul>

Figure 4-4: Record the MD5 Hash to be Verified Post-Investigation

#### Following Completion of Investigation

Open the QuickHash GUI tool and click on the File tab. Select MD5 from the Algorithm options.

# QuickHash v3.0.2 (Ma	2018) - The easy and convenient way to hash data in Linux, OSX and Windows		- 0	1	$\times$
File About					
	opyright © 2011-2018 Ted Smith	http://www.quickhash-gui.or	9		
Text File File	6 Copy Compare Two Files Compare Two Folders Disks Base64 Data				
Algorithm	Single File Hashing				
	Select File or drag n drop a file				
C xxHash64				- 1	
	File being hashed				
	Computed hash will appear here				
	Switch case     Expected Hash Value (paste from other utility before or after file hashing)				
	······································			-	
	, Clear Hash Field				

Figure 4-5: QuickHash GUI Single File MD5

Copy and paste the MD5 hash from the beginning of your investigation into the Expected Hash Value textbox. This will have the QuickHash GUI tool compare the hash values, looking for an identical match, to indicate whether the investigation was forensically sound.

Algorithm Single File Hashing Single File Hashing Start at a time:		Copyright © 2011-2018 Ted Smith http://www.quickhash-gui.org
Image: Start at a time:	xt File File	eS Copy Compare Two Files Compare Two Folders Disks Base64 Data
C SH41 SH425 SH425 Setet File or drag n drop a file <sup>−</sup> File being hashed. Computed hash will appear here Switch case Spected Hash Value (paste from other utility before or after file hashing) 9350096FCAB3D07F8407F0484245AF04 Clear Hash Field Clear Hash Field Clear Hash Field File fail format View Help C:\Users\colwe\Desktop\Howard Case\Samsung CDMA_SM-3320VPP Galaxy 33 MDS: 935096FCAB3D07F8407F0484245AF04 Started at: 10/04/2018 11:04:48 Ended at: 10/04/2018 11:04:51 Time taken: 00:00:02	Algorithm	Single File Hashing
Select File or drag n drop a file " File being hashed.          Computed hash will appear here         Switch case         Expected Hash Value (pasts from other utility before or after file hashing)         9390906FCA83207F8407F0484245AF04         Clear Hash Field         Pior to Investigation Hash Value Ltt. Notepad         Clear Hash Field         Pior to Investigation Hash Value Ltt. Notepad         File Edit format View Help         Cilvare's Localway Desktop/Howard Case\Samsung CDMA_SM-3320VPP Galaxy 33         MD5:       95507648226AF04         Started at:       10/04/2018 11:04:48         Ended at:       10/04/2018 11:04:51         Time taken:       00:00:02	C SHA-1	□ Start at a time:
Computed hash will appear here  Switch case Expected Hash Value (paste from other utility before or after file hashing) 355096FCA83D7F8407F0048245AF04  Clear Hash Field  File fait format Vew Heip C: \Users\celwe\Desktop\Howard Case\Sansung CDMA_SM-J320VPP Galaxy J3 NDS: 3150906FCA93D7F6403F07F048245AF04  Started at: 10/04/2018 11:04:48 Ended at: 10/04/2018 11:04:51 Time taken: 00:00:02	C SHA512	
□       Switch case         □       □		File being hashed
Clear Hash Value (paste from other ublity before or after file hashing) 9350096FCA83307F8407F0484245AF04  Clear Hash Field  File Gilt Format View Heip C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-J3280VPP Galaxy J3 NDS: 9350006FCA83B3D7E8407F0484245AF60  Started at: 10/04/2018 11:04:88 Ended at: 10/04/2018 11:04:51 Time taken: 00:00:92		Computed hash will appear here
9339096FCA833D7F8403F04484245AF04         Clear Hash Field         File Edit Format View Help         C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-3320VPP Galaxy 33         MD5:       9350964CA83205F407F0484245AF00         Started at:       10/04/2018 11:04:48         Ended at:       10/04/2018 11:04:51         Time taken:       00:00:02		
Clear Hash Field Fie Edit format View Heip C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-3320VPP Galaxy 33 MDS: 2350006fcCAB3007E04082245Af60 Started at: 10/04/2018 11:04:48 Ended at: 10/04/2018 11:04:51 Time taken: 00:00:02		
Clair Hain THEIL       File Edit Format View Help         C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-J320VPP Galaxy J3         MD5:       2350006FC403307F8407F04882265AF00         Started at:       10/04/2018 11:04:48         Ended at:       10/04/2018 11:04:51         Time taken:       00:00:02		9359D90FCAB33D/16840/F0484245AF04
Started at: 10/04/2018 11:04:48 Ended at: 10/04/2018 11:04:51 Time taken: 00:00:02		File Edit Format View Help C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-J328VPP Galaxy J2
		Started at: 10/04/2018 11:04:48 Ended at: 10/04/2018 11:04:51



Click the button Select File and navigate to where the folder is containing your evidence and select the image file with extension UFDR. Click Open when you are done to start the process.

**Note:** Remember you do NOT want to select "UFEDReader.exe" or files with the extension PAS. Those files do not contain any of the evidence of interest, but rather only data to run the forensics software and maintain your overlay of forensic tags (to be explained in Chapter 5).

# QuickHash v3.0.2 (Ma	ar 2018) - The easy and convenient way to	hash data in Linux, OSX and Windows	- 🗆 ×	£
File About				
	Copyright © 2011-2018 Ted Smith	http://www.quickhash-gui	.org	
Text File File	S Copy Compare Two Files Com	pare Two Folders   Disks   Base64 Data		
Algorithm	Single File Hashing			
	☐ Start at a time:	50 50		
C SHA512 C xxHash64	Select File or drag n drop a	file		
	File being hashed			
	Computed hash will appear here			
	Switch case Expected Hash Value (paste from of	ther utility before or after file hashing)		
	9359D96FCAB33D7F8407F0484245			
	Clear Hash Field	Open existing file		×
		$\leftarrow$ $\rightarrow$ $\checkmark$ 📩 $\diamond$ This PC $\Rightarrow$ Desktop $\Rightarrow$ Howard Case 🛶 $\checkmark$ ඊ	Search Howard Ca	ise "P
		Organize 👻 New folder	BER	- 🔳 🔞
		A Name	Date modified	Туре
		Desk # CountPackage	4/10/2018 10:56 AM	File folder
		Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_Report.ufdr	4/5/2018 4:29 PM	UFDR File
		<ul> <li>↓ Dook # ■ ■ UFEDReader.exe</li> <li>B Doct # ■</li> <li>■ Fict.#</li> <li>■ Text!# ↓ &lt;</li> </ul>	2/19/2018 5:05 PM	Application
				· · · · ·
		File name: Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_Rep	<ul> <li>All files (*.*)</li> </ul>	~
			Open 🔶	Cancel

Figure 4-7: Select the .UFDR File for MD5 Hash Calculation and Comparison

You will begin to see the tool's progress in calculating the hash value below and then displayed in the gray shaded box.

# QuickHash v3.0.2 (M	r 2018) - The easy and convenient way to hash data in Linux, OSX and Windows			×
File About				
	Copyright © 2011-2018 Ted Smith	http://www.quickhash-gui.org		
Text File File	S Copy Compare Two Files Compare Two Folders Disks Base64 Data			
Algorithm	Single File Hashing			
MD5     SHA-1     SHA256     SHA25     SHA55     SHA55     SHA55     SHA55	□ Start at a time: Started at : 10/04/2018 11:25:48 ←			
C SHA512 C xxHash64	Select File or drag n drop a file			
1 XXHasho4	C:\Users\celwe\Desktop\Howard Case\Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_R	eport.ufdr		
	Switch case     Expected Hash Value (paste from other utility before or after file hashing)			
	9359D96FCAB33D7F8407F0484245AF04			
	3555050FCA8550FF040FF040FF04		_	
	Clear Hash Field 60%			
	HASHING FILEPLEASE WAIT 🗲			-

Figure 4-8: Hash Calculation Begins and the Timestamp is Displayed

Upon completion of the hash value and comparing it to the MD5 provided, a pop-up window will appear verifying whether the hashed values were indeed identical.

# QuickHash v3.0.2 (Ma	r 2018) - The easy and convenient way to hash data in Linux, OSX and Windows	- 0	$\times$
File About			
	Copyright © 2011-2018 Ted Smith	http://www.quickhash-gui.org	
Text File File	5 Copy Compare Two Files Compare Two Folders Disks Base64 Data		
Algorithm	Single File Hashing		11
Algorithm G MD5 C SHA-1 C SHA256 C SHA512 C xxHash64	Single File Hashing	2 ←	-

Figure 4-9: Hash Comparison is Complete and Pop-Up Window Indicates an Identical Match

**Note:** If your pop-up window states the hash values DO NOT match, check that you selected MD5 as the Algorithm of choice.

	r 2018) - The easy and convenient way to hash data in Linux, OSX and Windows	- 0	×
File About	opyright © 2011-2018 Ted Smith	http://www.quickhash-gui.org	
Text File File	S Copy Compare Two Files Compare Two Folders Disks Base64 Data		
Algorithm	Single File Hashing		
Algorithm C MD5 G SHA256 C SHA256 C SHA512 C xoHash64	Single File Hashing   Start at a time:  Start at at in:  Start at at at in:  Start at at at in:  Start at	18-04-05_Report.ufdr	_

Figure 4-10: Check Selected Algorithm if Hash Comparison Indicates NOT Identical Match



## **Android Forensics CCIC Training**

## Chapter 5: UFED Reader Basics

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 5

# **UFED Reader Basics**

## Introduction

The evidence provided for you is a physical extraction completed by a Universal Forensic Extraction Device (UFED) as discussed in Chapter 3. A forensics report (UFDR) was generated containing all evidence which is accessible to you through the open-source UFED Reader program. In this chapter, you are going to properly open the case evidence, explore the menus with information, and create and remove tags for important file(s). While you search through the evidence in the software and add tags, your work will be saved. This allows you to reopen the case later to look through the evidence again if necessary.

## Accessing Case Evidence

To begin your investigation of the mobile phone evidence, open your case by double clicking (executing) the UFED Reader executable file ("UFEDReader.exe").

File Home	Share View					$\sim$ (
← → ✓ ↑ 🖡 > This PC > Desktop > Howard Case <del>←</del>			ن v	Search Howard Case		م ر
A Quick acce	Name	Date modified	Туре	S	ize	
Desktc *	AccountPackage	4/10/2018 10:56 A	File fold	folder		
	Samsung CDMA_SM-J320VPP Galaxy J3 2016_2018-04-05_Report.ufdr	4/5/2018 4:29 PM	UFDR F	ile	836,802 KB	
👃 Downl 🖈	UFEDReader.exe	2/19/2018 5:05 PM	Applica	ition	221,463 KB	]
🖪 Docun 🖈						
Nicture 🖈						
📜 Textbc 🖈						
items						

Figure 5-1: To View Evidence with UFED Reader, Double Click on the Executable File "UFEDReader"

**Note:** Do NOT delete or separate any of the files within the folder containing the evidence (extracted data). These files must be within the same file location in order to open your case properly and not have your access to the evidence revoked.

When the case fully loads, a pop-up window should appear asking if you would like to adjust the timestamps to the device's time zone. Check the box and click Yes.

Reader 7.1.0.106		- 0 ×
Reader File View Tools R		All Projects
80	Welcome ×	• ×
✓	Welcome to Reader	📑 Open 🔞 Settings
<ul> <li>Extraction Summary (1)</li> <li>Physical</li> <li>Re Systems</li> <li>Analyzed Data</li> <li>Analyzed Data</li> <li>Anototic (1)</li> <li>Calledge (3)</li> <li>Contacts (2)</li> <li>Contacts (2)</li> <li>Contacts (2)</li> <li>Contacts (2)</li> <li>Contacts (10)</li> <li>Device Unations ()</li> <li>[1] Locations (10)</li> <li>[2] Device Unations ()</li> <li>[3] Device Unations (248)</li> <li>[4] MASS Messages (5)</li> <li>[4] MASS Messages (5)</li> <li>[5] Notes (2)</li> <li>Passwords (2)</li> <li>[6] Passwords (2)</li> <li>[7] Searched Items (71)</li> </ul>	Welcome to Reader         Recent files         Samsung CDMA_SH-3320VPP Galaxy 33 2016         Dt/2018 04.05.16.\Samsung CDMA_SH-320VPP Galaxy 33 2016,2018 04.05,Beportuide:         4/10/2018 1148 AM         Howse         Image: Comparison of the device's time zone?         Would you like to adjust timestamps to the device's time zone?         Automatically adjust the time zone when device time zone information is available         Image: Weight of the device's time zone information is available	Open Settings
<ul> <li>SMS Messages (34)</li> <li>User Accounts (12)</li> <li>Web History (196)</li> <li>Wireless Networks (1)</li> </ul>		
V B Data Files V V V V V V V V V V V V V V V V V V V		

Figure 5-2: Check and Click Yes If You Are Asked About Using the Device's Time Zone

Due to this being a physical extraction, the evidence you have been given is an exact copy of the device's memory to allow for a complete interpretation of the data. Therefore, by expanding the File Systems tab in the left main menu, you will see images of each portion of the memory listed. With the number of files shown per image, you as the examiner are aware of the main memory used for the device. For this case, the main memory is "Image13 (ExtX)" which contains the Android Root files.

Reader File View Tools Rep	oort Help					All Proje	ects	c
	Extraction Summar	ry (1) ×						
Samsung CDMA_SM-J320VPP Galaxy J3 20	All Content	Physical						
<ul> <li>Extraction Summary (1)</li> <li>Physical</li> </ul>	Extraction Sur	mmary		+ Add extra	action	Project settings	🔓 Ger	nerate report
Bie Systems     Bie Systems     Bie Google Drive Files hryanwuph@gmail.     Bie Google Drive Files hryanwuph@gmail.com     Bie Google Photos hryanwuph@gmail.com     Bie Image10 (ExtX) (1 file, 11 K8)     Bie Image11 (ExtX) (288 files, 821,280 K8	con m (	Ethodical Constraints of the second s						
Root (2388 files, 821,280 KB)		bite to or other bit of bit barround and and						
<ul> <li>Proot (2388 hiles, 821,280 KB)</li> <li>Proot (2088 hiles, 686,554 KB)</li> <li>Proot (10 files, 13,256 KB)</li> <li>Proot (10 files, 105,636 KB)</li> </ul>		Howard California Cybersecurity Institute		Examiner name Cas	sidy Elwell			
> 📄 app (101 files, 686,554 KB) > 📄 dalvik-cache (10 files, 13,256 K	(B) Case name	Howard	⊖≙	Examiner name Cas Device Content	sidy Elwell			
<ul> <li>&gt; = app (101 files, 686,554 KB)</li> <li>&gt; = dalvik-cache (10 files, 13,256 K</li> <li>&gt; = data (1911 files, 105,636 KB)</li> <li>&gt; = log (13 files, 883 KB)</li> <li>&gt; = media (98 files, 8,534 KB)</li> </ul>	(B) Case name Department Device Info Bluetooth device addres	- Howard California Cybersecurity Institute 55 D0 FCCC:48.05:70			sidy Elwell			
<ul> <li>&gt; app (101 files, 686,554 KB)</li> <li>&gt; advik-cache (10 files, 13,256 K</li> <li>&gt; adata (1911 files, 105,636 KB)</li> <li>&gt; log (13 files, 883 KB)</li> </ul>	(B) Case name Department Device Info	Howard California Cybersecurity Institute		Device Content	sidy Elwell	🔞 Calendar	17 (4)	
<ul> <li>app (101 files, 686,554 KB)</li> <li>dahvik-cache (10 files, 132.56 K</li> <li>data (1911 files, 105,658 KB)</li> <li>moda (18 files, 883 KB)</li> <li>moda (28 files, 8,534 KB)</li> <li>moda (26 files, 136 KB)</li> <li>overlays (73 files, 1,590 KB)</li> <li>overlays (174 files, 1,590 KB)</li> <li>snd (1 file, 4 KB)</li> </ul>	Gase name Department      Device Info      Bluetooth device addres Android ID      Bluetooth device name     ICID      Phone Activation Time     Time Zone     Mock locations allowed	Howard California Cybensecurity Institute 55 DDFC CC 48:05:70 2793-32232-CH73a SAMSUNG-SM-J320VPP 69:140000029:17794163 3;4712/012 2:340(UT-0) America/Loc_Angeles False		Device Content Phone Data		Calendar (2) Contacts	17 (4) 21 (11)	
<ul> <li>&gt; app (101 files, 666,554 KB)</li> <li>&gt; adalvik-cache (10 files, 13,256 K</li> <li>&gt; adalvik-cache (10 files, 13,256 K</li> <li>&gt; ad log (13 files, 883 KB)</li> <li>&gt; media (98 files, 6,354 KB)</li> <li>&gt; meis (20 files, 313 KB)</li> <li>&gt; property (1 file, 1 KB)</li> </ul>	(3) Case name Department Device Info Bluetooth device addres Android ID Bluetooth device name ICCID Phone Activation Time Time Zone	Howard California Cybensecurity Institute 55 DDFC CC 48:05:70 2793-32232-CH73a SAMSUNG-SM-J320VPP 69:140000029:17794163 3;4712/012 2:340(UT-0) America/Loc_Angeles False		Device Content Phone Data	1			

Figure 5-3: The File Systems Tab is an Exact Copy of the Device's Memory

Also, the Extraction Summary tab is a useful location which displays Extraction, Case, and Device information. For example, this is the window in which you can locate the device's phone number.

Reader 7.1.0.106								– ø ×
Reader File View Tools Report H	Help					All Projec	ts	٩
60	Extraction Summary (1	×						<del>~</del> ×
Samsung CDMA_SM-J320VPP Galaxy J3 2016	All Content Phy.	sical						
Extraction Summary (1)     Physical	Extraction Summ	ary		+ Add extrac	tion	Project settings	E	Generate report
<ul> <li>De Fale Systems</li> <li>Ch Analyzed Data</li> <li>Data Files</li> <li>X. Carving</li> <li>Timeline (776)</li> <li>Tags (0)</li> <li>Reports</li> </ul>	Sa Ph Case Information Case name How	rskal msung CDMA SM-J320VPP Galaxy J3 2 sical answers med denotione 2018 15 66/LTC-7) strong on diagnome 2018-04-05.16-29-24/Samsung CDMA rd mid mid CDMA-SM-SM-SM-SM-SM-SM-SM-SM-SM-SM-SM-SM-SM-	D	aminer name Cassi	dy Elwell			
	Device Info		$\odot$ $\triangleq$	Device Content				
	Bluetooth device address Android ID Bluetooth device name ICCID Phone Activation Time Time Zone Mock locations allowed Location Services Enabled IMSI Advertsing Id Current Sind Operator ICCID Sind Change Operation Current Sind Operator Name	D0-FC-CC-88:05-70 2793a-2322-1677a 801-4800002917794163 357/2018 23:80(TC-40) Americal-0x_Angeles Faise True 31:480/201937738 51:480/201937738 31:480 801-4800002917794163 3 Verizon	v	Phone Data Autofil Cookies Brockers Phone Data	1 3 368 (8) 1	Calendar       O       Contacts       O       Device Locations       Emails	17 (4) 21 (11) 10 17	, v

Figure 5-4: The Extraction Summary Tab is Useful for Information About the Device, Case, and Extraction Technique

This window can also be used to access the menu for editing Case Information, such as Examiner Name(s) and Department. To access the menu, click the Project Settings button and then select Case Information. You can edit and add fields as you please which will then display in the Extraction Summary after clicking OK.

Reader File View Tools R									All Proj	ects	
	Welcome × 🥚 E	xtraction Summa	ry (1) ×								
Samsung CDMA_SM-J320VPP Galaxy J3	All Content I	Physical									
Extraction Summary (1)	Extraction Sum	nmary					+ Add extraction		Project settings		Generate report
🕣 Analyzed Data 👼 Data Files			, ADD I	NEW							
🕻 Carving 🕅 Timeline (776)	- B Proj	ect settings	🗘 Add New 🔒 Restore det	the set				×			
		÷	Name	Required	Туре		DefaultValue	^			
Reports	G	ieneral Settings	Case name	Ves	String		Howard	/			
	_	111	Examiner name	Ves	String		Cassidy Elwell	14			
	Case Inform	ase Information	Department	Yes	String		California Cybersecurity Institute	1	EXISTING		
	Department	SELECT	Case number	Ves	String			/			
	Device Info		Evidence number	Ves	String			/			
	Bluetooth device Android ID		<					■ > <sup>~</sup>			
	Bluetooth device ICCID						ОК Са	ncel	Calendar	17 (4)	
	Phone Activation Time Zone Mock locations allowed	America/Los_A False				e	。Call Log 3	8	Contacts	21 (11)	
	Location Services Enable IMSI	311480291937	1738 D-4ffe-b2da-d77a1a		- 1	C	Cookies 368 (8	, @	Device Locations	10	
	Advertising Id										

Figure 5-5: Project Settings Menu Allows for Editing of Case Information

**Note:** The Analyzed Data and Data Files tabs will be explored more thoroughly in upcoming chapters as you complete your detailed investigation.

## **Tagging Evidence**

When you find files or information that is evidence or requires further investigation, it is best practice to place tag on the items. This is also a great practice to allow you as an investigator to "annotate" the evidence with notes for yourself or another examiner in the future.

**Note:** Tag data will be included into any generated report(s) with the tag name, timestamp, and the item(s). This information will be included at the end of the report in a Tags section and is represented throughout the report with a colored tag symbol in the right-most column of the listed evidence.

#### **Manage Tags**

Open the Manage tags window to create or edit the name, color, and keyboard shortcut of tags by clicking Tools ► Manage tags or the icon containing a tag and gear in the tool bar.

**Note:** The UFED Reader program already has tags named Evidence, Important, Pending, and Completed as defaults which you can use.

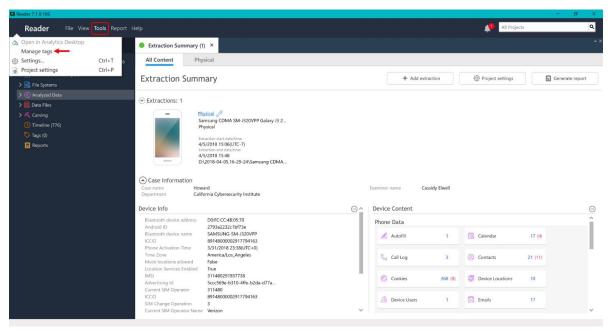


Figure 5-6: To Edit Tags for Investigation, Click Manage Tags in the Toolbar

To create a new tag, select the New tag link and a blank row will appear. You can then utilize the text box, color drop down, and HotKey drop down to choose the characteristics desired. Click Save following your changes.

Reader File View Tools Report Help 🔊 🔊 All Projects	٩
Extraction Summary (1) ×	
Content of the second of	
IMSI     311440221937283     Image: Cookies     368 (8)     Image: Cookies     368 (8)     Image: Cookies     10       Advertising M     Screent SIM Operator     3114400     114602-1461-b2da-d77a     Image: Cookies     368 (8)     Image: Cookies     10       ICCD     89144800002917794163     Image: Cookies     1     Image: Cookies     1     Image: Cookies     1       Still Change Operator Name     Verizon     Verizon     Verizon     Verizon     1     Image: Cookies     1	Ŷ

Figure 5-7: When Creating a Tag, Options Include Name, Color, and HotKey

Tags can also be deleted by clicking the trash can icon to the left of the listed tag.

**Note:** This will not delete any evidence associated with this tag. However, the associated items will no longer be tagged and any descriptions associated erased.

Reader 7.1.0.106					- 6 ×
Reader File View Tools Report	Help			All Projects	٩
80	Extraction Summary (1)	) ×			
Samsung CDMA_SM-J320VPP Galaxy J3 2016	All Content Phys	sical			
Extraction Summary (1)	Extraction Summ	ary	+ Add extraction	Project settings	Generate report
<ul> <li>See Tele Systems</li> <li>See Tele Systems</li> <li>See Tele Systems</li> <li>See Tele Systems</li> <li>See Carving</li> <li>Connecting (776)</li> <li>See Tags (1)</li> <li>See Reports</li> </ul>	© Extractions: 1 Def	Yes No	F6 * * s * stKey * Cassidy Elwell		Θ
	Mock locations allowed Location Services Enabled IMSI Advertising Id Current SIM Operator ICCID	5ccc569e-b310-4fte-b2da-d77a 311480 89148000002917794163 3	Cancel 1 Call Log 3 Cookies 368 (8) Device Users 1	Contacts 2     Device Locations	17 (6) 1 (11) 10 17

Figure 5-8: Delete a Tag By Simply Clicking the Trash Can Icon

#### Tag File(s)

Select the file(s) you want to tag and click the icon of a tag and plus sign in the toolbar. For example, let's say you want to tag the file which includes the name of the Wireless Network used by the device.

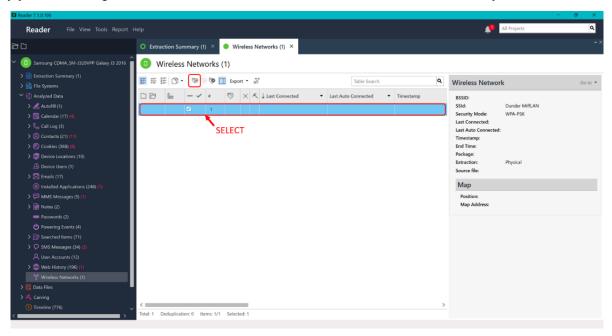


Figure 5-9: Begin By Selecting File(s) and Clicking the Plus Tag Button

**Note:** If you are unable to click on the icon and you have multiple files selected, it is likely because a specific file within the selected already has at least one tag. Since the UFED Reader program does not allow this action, you will need to unselect the already tagged file and tag it separately after tagging the rest collectively.

A mini tag window will appear for you to choose which of your created tags to use. Check one or more tags for the file(s). There is also an optional Description textbox where you can put any notes you desire about the specific file or group of files. Click OK once you are done.

Reader 7.1.0.106			- a ×
Reader File View Too		All Projects	٩
60	Welcome × O Extraction Summary (1) × O Wireless Networks (1) ×		<del>~</del> ×
✓ □ Samsung CDMA_SM-J320VPP Gala	Wireless Networks (1)		
>          Extraction Summary (1)           >          File Systems           >          Analyzed Data           >          Manalyzed Data           >          Scalendar (17) [6]           >          Scalendar (17) [7]           >          Scalendar (17) [7]		Wireless Network  sscience sscience sscience sscience sscience science	Go to •
<sup>↑</sup> Wireless Networks (1) <sup>→</sup> B Data Files <sup>→</sup> Carving <sup>→</sup>	Total: 1 Deduplication: 0 Items: 1/1 Selected: 1		

Figure 5-10: Select the Tag You Want to Use and Add an Optional Description

You will see the color of the tag(s) added in the Tags column of the piece(s) of evidence. In addition, the details panel to the right will gain a Tags section containing the tag(s) color, name, and any entered description.

🖬 Reader 7.1.0.106		— c	× ĸ
Reader File View Tools Report I	łeip	All Projects	٩
60	Extraction Summary (1) ×      Wireless Networks (1) ×		÷ ×
Samsung CDMA_SM-J320VPP Galaxy J3 2016	Wireless Networks (1)		
> 🕞 Extraction Summary (1) > 💼 File Systems	羅 ※ 詳 ①・ 物 物 例 面 Export ・ 叔 Table Search Q	Wireless Network	Go to 🔹
<ul> <li>✓ (2) Analyzed Data</li> <li>&gt; ∰ Autoff (1)</li> <li>&gt; % callendar (17) (4)</li> <li>&gt; % Callendar (17) (4)</li> <li>&gt; % Contacts (21) (11)</li> <li>&gt; % Contacts (26) (6)</li> <li>&gt; % Device Locations (10)</li> <li>. Device Locations (10)</li> </ul>	Image: Solution of the second seco	BSSID: Sside: Under MiffLAN Security Mode: W/A-FSK Last Connected: Last Auto Connected: Times: Package: Extra connected: Source file: Physical Source file: Position: Map Address:	
Passocids (2)     Downing Events (4)     Downing Events (4)     Downing Events (4)     Downing Events (4)     Downing Events (14)     Downing Events (15)     Downing Events (15)     Dota Files     Caning     Connelline (776)     C	Total: 1. Deduplication: 0. Items: 1/1. Selected: 1.	Tags  Labels: Important Description: Wireless Network used by the suspect	

Figure 5-11: The Tag Will Be Represented in the File's Row and the Right Detail Pane

#### Remove Tag(s)

Select the file(s) you want to remove a tag from and click the icon of a tag and minus sign in the toolbar. For example, let's say you decided that the Wireless Network used by the device did not fit the chosen tag so you want it removed.

**Note:** Any notes you have written in the Description of a tag will be DELETED as well, so ensure the information does not need to be maintained or recovered.

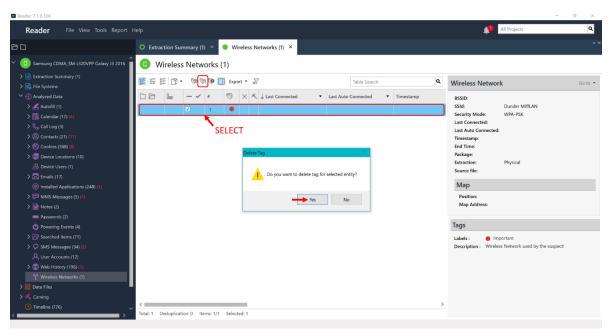


Figure 5-12: Begin By Selecting File(s) and Clicking the Minus Tag Button

## Saving Session and Reopening Case

After adding tags or descriptions to file(s) within the case evidence, you will want to save to ensure this data is kept upon the close of the UFED Reader program. To do so, begin by clicking File ► Save project session.

Reader 7.1.0.106		- 0 ×
Reader File View Tools Report Help		All Projects Q
Open         Ctrl+O         Welcome         Extra           Recent         ,         .<	ction Summary (1) ×	* x
Close tabs , 3 All Content Phy	sical	
Close Ctrl+W		
Save project session 🛻 Extraction Summ	ary +	Add extraction 🔞 Project settings 📓 Generate report
Exit		
	rsical //	
Sa	msung CDMA SM-J320VPP Galaxy J3 2 ysical	
Tags (0)		
Reports 4/	raction start date/time 5/2018 15:06(UTC-7)	
4/	raction end date/time 5/2018 15:48	
c	Users\celwe\Desktop\Howard Case\Sa	
Case Information     Case name     How     Department     Califi	ard Examiner name small Cybersecurity Institute	Cassidy Elwell
Device Info	💬 \land 🔰 Device Content	Θ
Bluetooth device address	D0:FC:CC:48:05:70 Phone Data	1
Android ID Bluetooth device name	2793a2232c1bf73e SAMSUNG-SM-J320VPP & Autofill	1 🔀 Calendar 17 (4)
ICCID	89148000002917794163	1 Calendar 17 (4)
Phone Activation Time Time Zone	3/31/2018 23:38(UTC+0) America/Los_Angeles Call Log	3 (2) Contacts 21 (11)
Mock locations allowed Location Services Enabled	False Can Log	
IMSI	311480291937738	368 (8)      Device Locations 10
Advertising Id Current SIM Operator	Sccc569e-b310-4ffe-b2da-d77a1a	
ICCID	89148000002917794163 . Device Users	1 🖂 Emails 17
SIM Change Operation Current SIM Operator Name	3	V

Figure 5-13: Remember to Save Your Session Using the Toolbar Before Exiting UFED Reader

Select the location for the file to be the same as where the case's .UFDR file and the UFED Reader executable are being saved (should be default location). The project session will be saved as a PAS file.

Reader File View		All Projects	
3	Welcome × 😑 Extraction Summary (1) ×		
Samsung CDMA_SM-J320VPP	Galaxy J3 All Content Physical		
Extraction Summary (1)	Extra Save As	×       Project settings	Generate report
File Systems	← → ∨ ↑ 🖡 > This PC > Desktop > Howard Case 🖛	✓ ひ Search Howard Case タ	
Analyzed Data	Extra     Organize - New folder	i≣ • <b>()</b>	
房 Data Files Carving	^ Name	Date modified Type S	
Carving	Quick access     AccountPackage	4/10/2018 10:56 A File folder	
Tags (0)	Desktop # Accountrackage		
Reports	Documents *		
	📕 Pictures 🖈		
	Extbooks 🖈		
	Google Drive *     Android Forer *		
	Case nam		
	Device Ir This PC 🗸 🧹	>	
	Bluetoo File name: Samsung CDMA_SM-J320VPP Galaxy J3 2016.pas	~	
	Bluetoo Save as type: Physical Analyzer Session Files (*.pas)	Calendar 17 (4	4)
	ICCID Phone A		
	Time Zo Mock lo	Save Cancel Contacts 21 (11	1)
	Location Services Enabled True		
	IMSI 311480291937738 Advertising Id 5ccc569e-b310-4ffe-b2da-d77a1a	Cookies 368 (8) Covice Locations 10	
	Current SIM Operator 311480 ICCID 89148000002917794163		
	SIM Change Operation 3	A Device Users 1 Emails 17	
	Current SIM Operator Name Verizon	V	

Figure 5-14: Ensure You Select to Save the Project Session Within the Same Location as the .UFDR File

When you want to reopen your case evidence, open your case by double clicking (executing) the UFED Reader executable file ("UFEDReader.exe") just as you did before. You will then see a new pop-up window asking if you would like to open a session file for the current case. Click Yes and continue with your investigation.

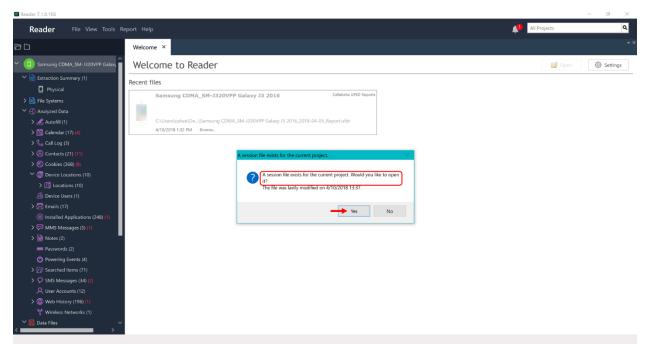


Figure 5-15: Reopen the Case the Same as Before and Select Yes When Asked If You Want to Load Your Project Session

## Reporting

Following the completion of your investigation, you will likely need to create a report containing all or particular sections of evidence to provide to court or other examiners. To do so, you have three options:

- 1. Click Report ► Generate report in the main toolbar.
- 2. Double click the Reports tab in the left main menu.
- 3. Click the Generate report button within the Extraction Summary window.

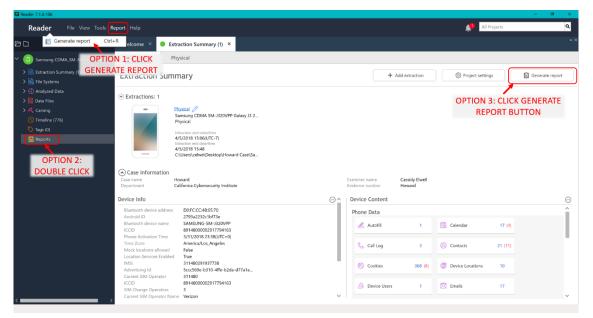


Figure 5-16: Open the Generate Report Menu

Within the Generate Report menu, edit the information to reflect your investigation team and choose PDF as the Format for the extraction report. Click Next when you are done.

Reader 7.1.0.106			– a ×
Reader File View Tools Report Help		All Projects	م
Generate Report		x	
<ul> <li>Samsung CDMA, SM J320/VPP Calaxy J1</li> <li>Statuton Summary (1)</li> <li>Report Dataset</li> <li>Samsung CDMA, SM-Statuton</li> <li>Samsung CDMA, SM-Statuton</li></ul>	Report sub directory: Project Format Case name: Earniner name: Department: Case number: Evidence number: Location: Notes:	DEFAULT BUT CHOOSE BEST LOCATION FOR YOU         Samsung CDMA, SM J320VPP Galaxy J3 2016         Samsung CDMA, SM J320VPP Galaxy J3 2016         Calibod-30, 22-57-44         Samsung CDMA, SM J320VPP Galaxy J3 2016         PDF Report         Howard         California Cybersecurity Institute         H-201         Howard Android Phone         17 (e)         218-04 - 0.22 - 57-44         Samsung CDMA, SM J320VPP Galaxy J3 2016         PDF Report         SELECT P         FormA         California Cybersecurity Institute         1-201         17 (e)         218-01         218-02         218-02         218-02         218-02         128-02         129-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02         120-02	4)
Update settings ICCID 8914800 SM Change Operation 3 Current SIM Operator Name Verition	00002917794163	Previous Next Cancel catons 10	

Figure 5-17: Update Case and Investigation Information and Select PDF for Report Format

Now, select the extracted data you want included in the report and click "PDF Report" to the left.

You can choose to only extract the data which you tagged in the UFED Reader program with the "Tags only" option. This is a good option for examining and presenting the most critical evidence in your case.

Reader 7.1.0.106						– a ×
Reader File View Tools Report				4	All Projects	٩
	Generate Report		-	• • ×		~ ×
Gamsung CDMA_SM-J320VPP Galaxy J3     Betraction Summary (1)     Betraction Summary (1)	General Report Dataset	Report Dataset - Samsung	CDMA_SM-J320VPP Galaxy J3 2016	a)	ect settings	Generate report
> 🕙 Analyzed Data	Samsung CDMA_SM		Enter text to filt	er 🗙		
<ul> <li>K Carving</li> <li>Timeline (776)</li> </ul>	Security	<ul> <li>Applications (199/199)</li> <li>Audio (3/3)</li> <li>Autofill (1/1)</li> <li>Calendar (17/17)</li> </ul>	<ul> <li>✓ Installed Applications (248/248)</li> <li>✓ Locations (10/10)</li> <li>✓ MMS Messages (5/5)</li> <li>✓ Notes (2/2)</li> </ul>			
Tags (0)	Layout Default sorting	<ul> <li>Call Log (3/3)</li> <li>Configurations (11/11)</li> <li>Contacts (21/21)</li> </ul>	<ul> <li>✓ Passwords (2/2)</li> <li>✓ Powering Events (4/4)</li> <li>✓ Searched Items (71/71)</li> </ul>			
િ	PDF Report	<ul> <li>✓ Cookies (368/368)</li> <li>✓ Databases (294/294)</li> <li>✓ Device Info (21/21)</li> <li>✓ Device Users (1/1)</li> <li>✓ Documents (4/4)</li> </ul>	<ul> <li>✓ SMS Messages (34/34)</li> <li>✓ Text (716/716)</li> <li>✓ Timeline (776/776)</li> <li>✓ User Accounts (12/12)</li> <li>✓ Web History (196/196)</li> </ul>	×		
Joe		<ul> <li>✓ Emails (17/17)</li> <li>✓ Images (1164/1164)</li> </ul>	Mirelass Naturatis (1(1)		ATA YOU DO	
De		Examiner			EXPORTED	
		<ul> <li>Tags</li> <li>Calculate SHA-2 (256 bit) hash</li> </ul>	Tags only Redact image thumbnails		E REPORT	î
		Calculate MD5 (128 bit) hash Include translations Include known files	<ul> <li>Include merged items (analyzed da</li> <li>Include merged items (data files)</li> <li>Include source info indication</li> </ul>	ta)	17 (4)	
			✓ Include enrichments ☐ Hide extraction source indication		21 (11)	
		Analytics				
			Previous Next Finish	Cancel	ations 10	
2	CCID         891480000029           SIM Change Operation         3           Current SIM Operator Name         Verizon	17794163	A Device Users 1	🔀 Emails	17	U
<	current silvi Operator Name Venzon					÷

Figure 5-18: Select Data to be Included in the Generated Report

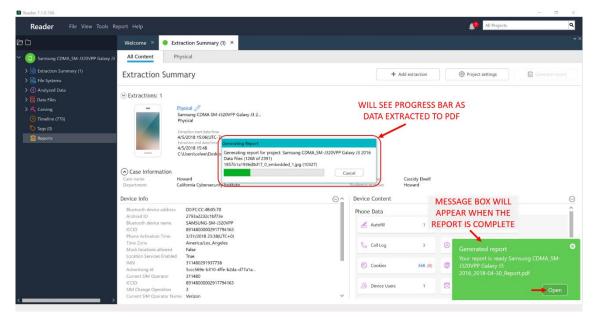
**Note:** The reason you skipped to the "PDF Report" portion of the Generating Report menu is because the options in between should be left at their default values for our purposes.

The "PDF Report" section allows you to add/edit custom headers and logos to the report in order to reflect your investigation team. This is optional, but a great way to personalize the extracted report. Click Finish when you are done.

Reader 7.1.0.106				- 0 ×
Reader File View Tools Reg			All Projects	٩
60	Generate Report	- 0	×	~ ×
<ul> <li>Samung CDMA, SM J320VPP Galaxy J3</li> <li>Bata Statistics Summary (1)</li> <li>Bata File Systems</li> <li>C) Analyzed Data</li> <li>Bata Files</li> <li>Caring</li> <li>Tendine (776)</li> <li>Tegic (0)</li> <li>Reports</li> </ul>	C C C C C C C C C C C C C C C C C C C	Layout - PDF Report Disable models categorization Cogo Header We Agene before the layout OPTIONAL CUSTOM REPORT HEADER OPTIONAL CUSTOM REPORT LOGO Select Image File Logo Footer Will Agener after the layout Mark and an and a state of the layout Previous Next Field of Carcel	iect settings	Generate report
<	ICCID 891480000029 SIM Change Operation 3 Current SIM Operator Name Verizon	17794163	nails 17	v

Figure 5-19: Optional Custom Header and Logo Options for PDF Report

The report creation process will begin, and you will see a progress bar appear. When the report is completely generated and saved to your computer, a green pop-up will appear in the lower right-hand corner with the option to Open. You may click to Open the report here or expand the Reports tab in the left main menu which will now contain your report (and any additional reports you chose to create).



Note: Exported data reports will NOT be listed in this section, ONLY fully generated reports will be.

Figure 5-20: Report Creation in Process with Green Pop-Up Showing Completion

When opening the generated report, the Summary page will be displayed containing the investigative team and case information you specified earlier and a list of the contents of the report easily linked.

Edit View Window Help					_
ne Tools Samsung CDN	MA_S ×				⑦ Sig
		100% - 🗟 🗗 🐺 🗩 🖉			
	T SES R OOO				
Bookmarks CONTEN	NTS OF REPORT	-			
E- R EAS	SILY LINKED	Extraction	Report 🔶		
- /		Cellebrito UFED Report			
🔲 Summary 🦰	<u>^</u>				
Source Extraction					
A					
Device Information					
D Plugins					
		Summary			
Contents		UFED Physical Analyzer version	7.1.0.106		
Autofill		Report creation time	4/30/2018 23:03 -07:00		
н		Time zone settings (UTC)	(UTC-08:00) Los_Angeles (/	America)	
🔲 Calendar		Case name Examiner name	Howard Cassidy Elwell		
Call Log		Department	Cassidy Erweil California Cybersecurity Instit	ule	
M Call Log		Case number	H-201		
Contacts	4	Evidence number	Howard Android Phone	SUMMARY PAGE INCLUDES	
Cookies					
Cookies		Comment Endersteiner		CASE INFORMATION ENTERED	
Device Users		Source Extraction		DURING REPORT CREATION	
		Physical Extraction start date/time	4/5/2018 15:06(UTC-7)	DURING REPORT CREATION	
Emails		Extraction end date/time	4/5/2018 15:48		
Installed Applications		Unit Identifier	903911591		
		UFED Version	7.1.0.761		
GPS GPS		Internal Version Selected Manufacturer	4.7.7.751 Samsung CDMA		
Locations		Selected Device Name	SM-J320VPP Galaxy J3 2016		
M Locations		Connection Type	Cable No. 100		
MMS Messages		Extraction Type	Physical		
		Extraction ID Time zone settings (ID)	F9BA034C-2142-4E00-B17F- America/Los Angeles	209D6A08FE1D	
Notes		L Time zone setungs (ID)	[_America/Los_Angeles		
Passwords					
		Device Information			
Powering Events					
-	~	Name	/alue		

Figure 5-21: Open the Extraction Report and Contents will be Easily Linked



## **Android Forensics CCIC Training**

Chapter 6: Lock/Home Screen Captures and Personal Files

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 6

## Lock/Home Screen Captures and Personal Files

## Introduction

Users can save their pictures, documents, and videos to a variety of applications on mobile devices. However, you always want to first check the Android default media folder within the file system since a large majority of users store data in within its Documents and DCIM folders. You also want to look at the Downloads folder and any cloud storage user folders. These folders will sometimes show what personal data the user downloaded or uploaded.

In addition, Android automatically stores screen captures of the device's lock and home screens in its file system. These screen captures are used by Android for user interface functionality, but for a forensic examiner they can potentially provide additional evidence if widgets were being utilized by the user.

#### Lock and Home Screen Captures

Expand the Data Files tab in the left main menu and click Images. In the opened window, select to view the information like it does in the Android file system by clicking the Folder View tab.

Note: It's recommended to collapse folder contents to simplify the process of locating correct file paths.

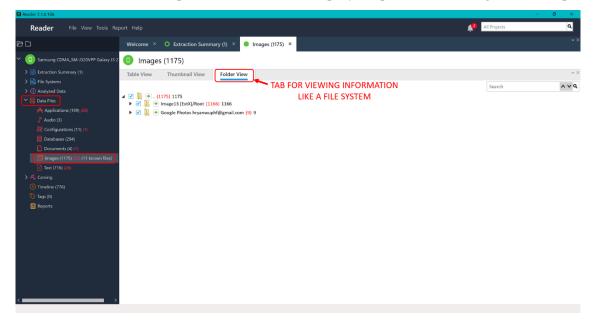


Figure 6-1: View the Images Within Android File System in the Data Files Tab

To view a screen capture of the Android device's Lock screen, navigate within Images to:

/Image13(ExtX)/Root/media/0/com.android.systemui/cache/

Click the green arrow beside the folder named "com.sec.android.app.launcher/cache."

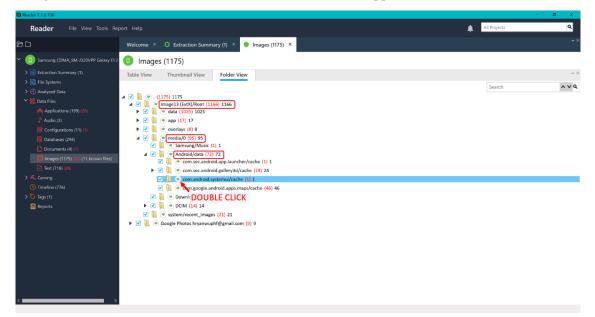


Figure 6-2: Screen Capture of the Device's Lock Screen is Stored Within Media

A table will then be displayed which contains the image "lockscreen\_capture\_port.png."

Ryan did not change his device from the default contents for the Lock screen, therefore no additional information is acquired here for the investigation.

Reader 7.1.0.106															-	o ×
Reader File View Tools Re	port Help												1	All Projects		٩
80	Welcor	me × (	O Extra	iction Sum	mary (1)		O Ima	iges (1175)	) × 😑 com.andr	oid.system	nui (1) ×					
Samsung CDMA_SM-J320VPP Galaxy J3 2	🕕 c	om.and	roid.s	ystemui	(1)											
Extraction Summary (1)      Extraction Summary (1)      Extraction Summary (1)	Table V	/iew	Thumb	nail View		der Vie										<i></i>
> 🕤 Analyzed Data	國際	35 BE 🤇	5 S	ML	7	GB	ΡØ	• () •	D• Ø• 2•	G () ()	🦻 🔲 Export 🔹 🛄	• 📈 Tal	Images			Go to 🝷
🗡 🐻 Data Files		0:0	- ~		⊗ >	KO	🖉 Imag	je	† Name	▼ Path		•	Det	ails	Events (0)	
📌 Applications (199) (28) المحمد المحمد			<b>V</b>	1					lockscreen_capture_po	ort Image	e13 (ExtX)/Root/media/0/	Android/dat		_		_
Configurations (11) (1)													( a.	x-7		- 1
Databases (294)													2:	<u>/ </u> /		- 1
Documents (4) (1)																- 1
Images (1175) (22) (11 known files)																- 1
> K Carving																- 1
( Timeline (776)																- 1
> 🏷 Tags (1)																- 1
💼 Reports																- 1
													3	۲		- 1
													Name:	lockscreen_captur	e_port.png	- 1
													Type: Size (bytes):	Images 40525		_
													Path:	Image13 (ExtX)/Re	oot/media/0/Android/d	iata/
														com.android.syste lockscreen_captur	e_port.png	
														4/2/2018 18:13(U 4/2/2018 18:13(U		
	<	n de l'este					610	Dark Inc.			ta da ser esta de la como	>	Modified:	4/5/2018 14:47(U		
× • • • • • • • • • • • • • • • • • • •	iotal: 1	Decuplicatio	n: U Ite	ms: 1/1 Se	nected: 1	Known	n files: 0	Path: Ima	ge13 (ExtA)/Root/media/	)/Android/d	data/com.android.systemu	ii/cacne/locksc	Deleted:			~

Figure 6-3: Lock Screen Capture for Ryan Does Not Differ from the Android Default

However, it is likely Ryan made edits to the Home screen of his device for ease of access to information.

To view a screen capture of the Android device's Home screen, navigate within Images to:

/Image13(ExtX)/Root/media/0/com.sec.android.app.launcher/cache/

Click the green arrow beside the folder named "com.sec.android.app.launcher/cache."

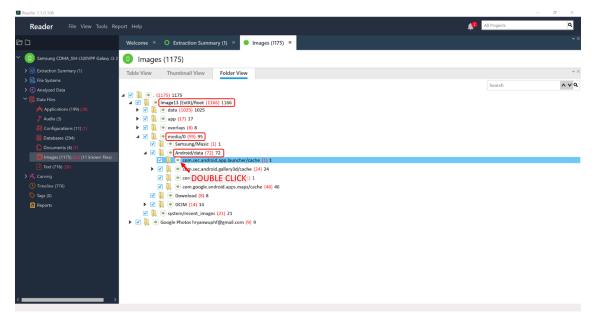


Figure 6-4: Screen Capture of the Device's Home Screen is Stored Within Media

A table will then be displayed which contains the image "homescreenPreview.png." To magnify the capture, double click on the thumbnail in the right Details pane. Another tab will appear with the image.

It appears that your inference was correct as Ryan has included a Samsung Notes widget on the Home screen containing "eBay Scamming Notes." Observe that Ryan mentions "Grand Theft Auto V" as an example, using official high-quality photos/descriptions, and fake personal identification information.

Note: This piece of evidence also verifies original accusations made by the Geek Squad employee.

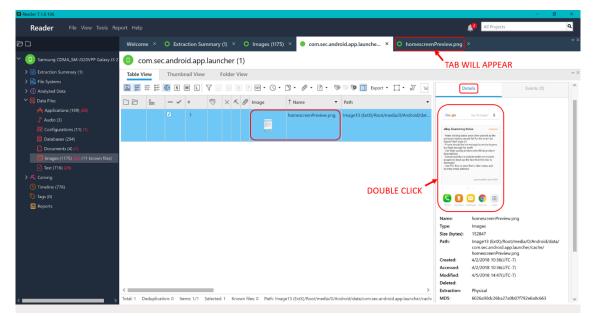


Figure 6-5: Home Screen Capture for Ryan Includes a Widget with Evidence

This is a file of interest for further investigation in Chapter 10 as the information pertains to Notes and Lists by Ryan, therefore the file should be tagged with "Further Investigation" and a detailed description.

Reader File View Tools	in point in cip												All Projects
Ċ	Welcor	me ×	O Extra	action Sur	nmary (1)	× O Im	ages (1175	i) × 😑 com	n.sec.andro	id.app.launche >	o homescreen	Preview.png	×
Samsung CDMA_SM-J320VPP Galaxy J	3 2 🕕 o	om.se	c.andro	id.app	launche	er (1)							
	Table \	/iew	Thumb	nail View	Fold	er View							
		¥ #	🚱 S	ML	7 D G			B. A.	- F20	🗐 🧐 🔲 Export •	· 🛛 • 📈 🖬		
		\$5 <u>85</u>	161 3					L	U • 💚	🗇 🎯 🛄 Export -	, ∐ , ×ı lai		estapet Crome Appe
		Doo	- ~		$\otimes$ $\times$	K 🖉 Ima	ge	† Name	•	Path	•	Name:	homescreenPreview.png
Applications (199) (28)			<b>Z</b>	1	•			homescreenPre	wiew.png	Image13 (ExtX)/Root/n	nedia/0/Android/dat	Type:	Images
Audio (3) Configurations (11) (1)					$\Box$							Size (bytes):	152847
Databases (294)												Path:	Image13 (ExtX)/Root/media/0/Android/data/ com.sec.android.app.launcher/cache/
Documents (4) (1)												Created:	homescreenPreview.png 4/2/2018 10:36(UTC-7)
Images (1175) (22) (11 known files)												Accessed:	4/2/2018 10:36(UTC-7)
Text (716) (26)												Modified: Deleted:	4/5/2018 14:47(UTC-7)
												Extraction:	Physical
() Timeline (776)												MD5:	6026a90dc26ba27a0b07f792e6a0c663
> 🏷 Tags (1)												Map	
💼 Reports												Position:	
												Address:	
												Map Addre	55:
												Tags	
												Labels :	<ul> <li>Further Investigation</li> </ul>
												Description :	-Verifies Geek Squad employee's claims
													-Further investigate information's creation/ modification
	<										>		

Figure 6-6: Tag the Home Screen Capture for Future Access and Investigation

### **Personal Images**

Expand the Data Files tab in the left main menu and click Images. In the opened window, select to view the information like it does in the Android file system by clicking the Folder View tab.

Note: It's recommended to collapse folder contents to simplify the process of locating correct file paths.

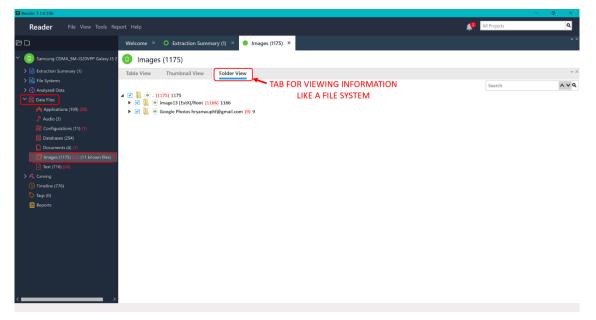


Figure 6-7: View the Images Within Android File System in the Data Files Tab

To view the images located in the Media Gallery of the device, navigate within Images to:

```
/Image13(ExtX)/Root/media/0/DCIM/
```

Click the green arrow beside the folder named "DCIM."

Reader 7.1.0.106		– ø ×
Reader File View		All Projects
60	Welcome × O Extraction Summary (1) × Images (1175) ×	• X
Samsung CDMA_SM-J320V	PP Galaxy J3 2 🕕 Images (1175)	
> 📄 Extraction Summary (1)	Table View Thumbnail View Folder View	* X
> 📄 File Systems		Search A V Q
>	🔺 🗹 📜 🐵 . (1175) 1175	Senen
🗡 🔀 Data Files	▲ ▼ ↓ ● Image13 (ExtX)/Root (1166) 1166	
Applications (199) (28)	▶ 🗹 🛄 💌 data (1025) 1025	
P Audio (3)	🕨 🗹 📜 💿 app (17) 17	
Configurations (11) (1)	▶ ☑ 📜 💿 overlays (8) 8	
Databases (294)	⊿ 🗹 📜 (⊕ (media/0 (95) 95) ☑ 📜 (⊕ Samsung/Music (1) 1	
Documents (4) (1)	Android/data (72) 72	
Images (1175) (22) (11 k	nown files)	
A Text (716) (26)	CIM (14) 14	
> 🔨 Carving	🗹 📜 🐵 system/recent_images (21) 21	
C Timeline (776)	🕨 🗾 间 Google Phi DOUBLE CLICK m (9) 9	
> 🏷 Tags (1)		
💼 Reports		
(		

Figure 6-8: Media Gallery Photos Including Those Taken with the Device's Camera are Stored in DCIM

A table will then be displayed which contains all images stored within the Media Gallery, including the default Camera folder and folders created by the user.

Ryan appears to have created a folder called "My Photos" for personal images with family and friends.

Reader 7.1.0.106						– ø ×
Reader File View Tools I	Report Help				All Projects	٩
60	Welcome ×	O Extraction Sur	nmary (1) × O Images (117	5) × 🔵 DCIM (14) ×		
Samsung CDMA_SM-J320VPP Galaxy J		(14)				
> 📄 Extraction Summary (1)	Table View	Thumbnail View	Folder View			* X
> 📄 File Systems > 🕣 Analyzed Data		🗐 S M L	7 ] G B P Ø• ()	- 🖞 • 🖉 • 🕲 🕲 🧐 🛄 Export • 🔲 • 📈	Images	Go to 🔹 🏠
Y 🔀 Data Files	• # 👳	X K 🖉 Image	† Name 🝷	Path 👻	Details	Events (0)
Applications (199) (28) Audio (3) Configurations (11) (1) Databases (294)	9		20171201_945638.jpg	Image13 (ExX)/Root/media/00CIM/My Photos 20171201_945638jpg		
Cocuments (4) (1)	10		20171224_461398.jpg	Image13 (ExXX)/Root/media/0/DCIM/My Photos/20171224_461398.jpg		
<ul> <li>K Carving</li> <li>Timeline (776)</li> <li>Tags (2)</li> <li>Reports</li> </ul>	11		20180210_106123.png	Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180210_106123.png	Name:         20171201_945638.jpg           Type:         Images	11 2
	12		20180214_124635.jpg	Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180214_124635.jpg	Size (bytes):         64353           Path:         Image13 [Ext0]/Root/mst           Photos/20171201_94563         Created:           4/3/2018 11:06(UTC-7)         Accessed:	
	13		20180216_761345.jpg	Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180216_761345 jpg	Modified: 4/3/2018 11:06(UTC-7) Deleted: Extraction: Physical MD5: 755a01d0abba8d63fb4d	18c847fc8c854
	14	1	20180405_091758.jpg	Image13 (ExtX)/Root/media/0/DCIM/Camera/20180405_091758.jpg	Metadata	
<	✓ Dedup	lication: 0 Items: 14/14	Selected: 14 Known files: 0 Pa	th: Image13 (ExtX)/Root/media/0/DCIM/My Photos/20171201_945638.jpg	Capture Time: 12/1/2017 10:00	~

Figure 6-9: Personal and Downloaded Images Further Analyzable Within the Details Pane

Scroll through Ryan's DCIM images and you will notice that "20180405\_091758.jpg" has an "Event" associated with it. The UFED Reader program has an Events pane which includes additional information if the data file was sent or received through a channel of communication.

Select the "20180405 091758.jpg" image and then click the Events tab in the right pane.

Reader File View Tools Re	port Heij						<u></u>			All Projects	
ב	Welco	me ×	O Extr	action Summa	ry (1) × O Images	s (11	75) × 🔵 DCIM (14) ×				
Samsung CDMA_SM-J320VPP Galaxy J3 2	0		(14)								
	Table	View	Thum	onail View	Folder View						
	国新	va- 0=-				0	• 🕥 • 🖉 • 😨 • 🐨 🐨 🔲 Export • 🎞 • 📈				
Analyzed Data		AE 85	12 8	MUV		0	• D • Ø • D • @ • @ D Export • D • x/	Tal	Images		Go to
🚼 Data Files	8	1	XKØ	Image	† Name	٠	Path •	s	Deta	ils Events (	1)
Applications (199) (28) P. Audio (3)	10				20171224_461398.jpg		Image13 (ExtX)/Root/media/0/DCIM/My Photos/20171224_461398jpg	7! ^			
<ul> <li>Databases (294)</li> <li>Documents (4) (1)</li> <li>Images (1175) (22) (11 known files)</li> <li>Text (716) (26)</li> </ul>	11				20180210_106123.png		Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180210_106123.png	g 7:		Particular and Partic	
K Carving () Timeline (776) Tags (1)	12				20180214_124635.jpg		Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180214_124635 jpg	64	Name: Type:	20180405_091758.jpg Images	
n Arports	13				20180216_761345.jpg		Image13 (ExX)/Root/media/0/DCIM/My Photos/20180216_761345 jpg	3:	Size (bytes): Path: Created:	117274 Image13 (ExtX)/Root/media/0/DC Camera/20180405_091758.jpg 4/5/2018 09:17(UTC-7)	IM/
	14				20180405_091758.jpg		Image13 (ExX)/Root/media/0 <mark>f0CIM/Camera</mark> 20186405_091758.jpg	1	Accessed: Modified: Deleted: Extraction: MD5:	4/5/2018 09:17(UTC-7) 4/5/2018 09:17(UTC-7) Physical 79b1826380eef7bb93b7cd7ae0b	18fe9
	<							~	Metadata		

Figure 6-10: Image Labeled with an Event was Often Sent or Received Through Form of Communication

As in most cases with images, you will see the "Event" is a MMS Message. Ryan sent this image to an individual labeled in his contacts as "Dwight Schrute" with a SMS Message on 4/5/2018.

Reader 7.1.0.106								- a :
Reader File View Tools R	Report Help						All Projects	٩
ð 🗅	Welcome	× O Extra	ction Summary (1	I) × O Images (1175	5) × 🖲 DCIM (14) ×			
Samsung CDMA_SM-J320VPP Galaxy JE		Л (14)						
> 📄 Extraction Summary (1)	Table View	Thumbr	nail View Fo	older View				
> 📑 File Systems > 🕙 Analyzed Data		ii 🙆 s (	m C 7 /	G 8 P Ø • () •	🗂 • 🖉 • 🗟 • 🕲 🕫 🚺 Export • 🗔 • 📈 🗌	11	MMS Message	Go to 🝷
🗡 🛃 Data Files	• # ₹	SXX0	/ Image	† Name 🔹	Path •		Folder: Outbox	
Applications (199) (28) Audio (3) Configurations (11) (1) Databases (294)	10			20171224_461398.jpg	Image13 (ExXX)/Root/media/0/DCIM/My Photos/20171224_461398.jpg	~	Subject: Timestamp: 4/5/2018 09:20(UTC-7) Priority: Status: Source: Verizon Message+	
Databases (294)     Documents (4) (1)     Images (1175) (12) (11 known files)     Text (716) (26)	11			20180210_106123.png	Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180210_106123.png		Extraction: Physical Source file:	
> K Carving (1) Timeline (776)	12		2000	20180214_124635.jpg	Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180214_124635.jpg		+18059105153	
> 🚫 Tags (3)			- A				То	
💼 Reports	13			20180216_761345.jpg	Image13 (ExtX)/Root/media/0/DCIM/My Photos/20180216_761345.jpg		+18053031855 Dwight Schrute	IMAGE WAS
			A THE R			Ľ.	Attachments	SENT AS MMS
	14	••		20180405_091758.jpg	Image13 (ExtX)/Root/mediar400(M/Camera20180405,091758 jpg		20180405_091758.jpg	
	< Total: 14 Dedi	uplication: 0 Ite	ems: 14/14 Select	ed: 14 Known files: 0 Pat	> th: Image13 (ExtX)/Root/media/0/DCIM/Camera/20180405_091758.jpg		Just have to place in the Xbox 360 case to go on a couple orders! I will bring the you to slip them past your boss.	

Tag this image file as "Further Investigation" with a description. You will do further analysis on SMS and MMS Messaging in Chapter 8.

Figure 6-11: Event of the Image was a MMS Message to Dwight Schrute

In addition, to view the images downloaded to the device per the user, navigate within Images to:

```
/Image13(ExtX)/Root/media/0/Download/
```

Click the green arrow beside the folder named "Download."

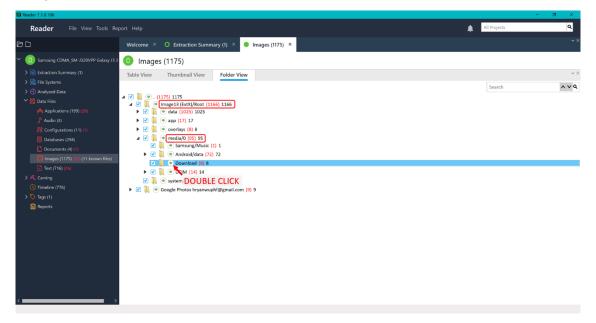


Figure 6-12: Downloaded Photos are Stored Within the Android File System's Media Folder

A table will then be displayed which contains all images downloaded and therefore stored in the media Downloads folder.

You found previously that "Grand Theft Auto V" was possibly a scam Ryan used due to the widget notes from the Lock screen capture. It looks like this is the official high-quality image he was utilizing for eBay, so this should be tagged as "Evidence."

Reader 7.1.0.106								- a	×
Reader File View Tools Rep							All Pro	jects	۹
60	Welcon	ne × OEx	raction Summar	y (1) × O Images (1	175) × 🖲 Download (8) ×				
<ul> <li>Samsung CDMA_SM-J320VPP Galaxy J3 2</li> <li>Extraction Summary (1)</li> </ul>		ownload (8							_ ~
<ul> <li>File Systems</li> <li>Analyzed Data</li> </ul>	Table V	iew Thun	bnail View	Folder View	)• 🕥 • 🖉 • 🖗 • 🐨 🐨 🛄 Export • 🎞 •	x7 Tal	Images	Go to 💌	î
Data Files Applications (199) (28)	•	🔊 × K (	Image		Path	▼ s	Details	Events (0)	1
Audio (3) Configurations (11) (1) Databases (294)	1	•		2017-11-21_5a14826692	Image13 (ExtX)/Root/media/0/Download/2017-11-21_5a1482669	3: ^		* XBOX 360	
Documents (4) (1) Documents (4) (1) Images (1175) (22) (11 known files) Text (716) (26)	2	×		20171201_945638.jpg	Image13 (ExtX)/Root/media/0/Download/20171201_945638.jpg	0	A the target of targe		
> 🐔 Carving () Timeline (776) > ) Tags (2) () Reports	3	×		20171224_461398.jpg	Image13 (ExtQ)/Root/media/0/Download/20171224_461398.jpg	0			
	4	×		20180210_106123.png	Image13 (ExtX)/Root/media/0/Download/20180210_106123 png	0	GrandTheft Type: Images Size (bytes): 335577	5 <u>a1482</u> 6692c29_XBox360- utoV-120x481.jpg X)/Root/media/0/	l
	5	×		20180214_124635.jpg	Image13 (ExtX)/Root/media/0/Download/20180214_124635.jpg	0	Download/2	017-11-21_5a14826692c29_XBox36 tAutoV-720x481,jpg 01(UTC-7) 01(UTC-7)	
< >	6 < Total: 8	Deduplication: 0	Items: 8/8 Selecte	52845-watch-dogs.jpg d: 8 Known files: 0 Path:	Image13 (ExtX)/Root/media/0/Download/52845-watch-dogs.jpg Image13 (ExtX)/Root/media/0/Download/2017-11-21_5a14826692	2 > 22	Deleted: Extraction: Physical	5fe76733549f9c4593101d	~

Figure 6-13: Ryan's Downloaded Photos are Purely Xbox 360 Game Sleeves

Also, observe that this image appears to match the Xbox 360 game sleeve shown in the photo Ryan sent MMS to Dwight Schrute. It appears Grand Theft Auto V is a common eBay scam selection for Ryan, which therefore could be easily traceable.

### **Personal Documents**

Expand the Data Files tab in the left main menu and click Documents. In the opened window, select to view the information like it does in the Android file system by clicking the Folder View tab.

Note: It's recommended to collapse folder contents to simplify the process of locating correct file paths.

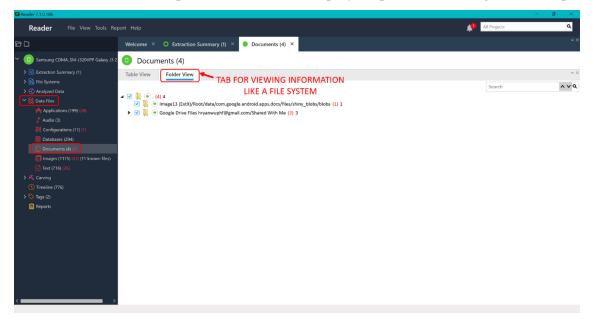


Figure 6-14: View the Images Within Android File System in the Data Files Tab

To view the documents located in the local Google Drive of the device, navigate within Documents to:

```
/Google Drive Files/My Drive/
```

Click the green arrow beside the folder named "My Drive."

Reader 7.1.0.106		– ø x
Reader File View Tools		All Projects
60	Welcome × O Extraction Summary (1) × O Documents (4) ×	
Samsung CDMA_SM-J320VPP Galax	yJ32 🕕 Documents (4)	
> 🛃 Extraction Summary (1)	Table View Folder View	~ X
> 📑 File Systems		Search
> 🕣 Analyzed Data	🔺 🗹 📜 🐵 . (4) 4	Senen
Y 🛃 Data Files	<ul> <li>Image13 (ExtX)/Root/data/com.google.android.apps.docs/files/shiny_blobs/blobs (1) 1</li> </ul>	
Applications (199) (28)	🔺 🗹 📜 🕐 Google Drive Files hryanwuphf@gmail.com/Shared With Me (3) 3	
Audio (3)	✓ 📙 • My Drive (2) 2	
Configurations (11) (1)		
Databases (294)	DOUBLE CLICK	
Documents (4) (1)		
💹 Images (1175) (22) (11 known file	(in the second se	
Text (716) (26)		
Carving		
C Timeline (776)		
> 🏷 Tags (2)		
Reports		
<		

Figure 6-15: My Drive Documents within Ryan's hryanwuphf@gmail.com Google Account

A table will then be displayed which contains all documents stored within the My Drive of Ryan's Google account. To view the content of individual Ryan's document's, you need to export the files.

Click the Export drop down in the tool bar and then PDF.

Reader 7.1.0.106		- o ×
Reader File View Tools Re		All Projects
60	Welcome × O Extraction Summary (1) × O Documents (4) × O My Drive (2) ×	
<ul> <li>Constraints of the second se</li></ul>	Welcome ×       Extraction Summary (1) ×       Documents (4) ×       My Drive (2) ×         Image: State of the stat	Decales     Constant Cons
		Map Address:
	<pre></pre>	

Figure 6-16: View Documents from the Device by Exporting a Report

Change the File name to "My Drive Documents" and specify Save To as a folder called "My Reports" on your Desktop.

Do NOT change the Report Sub Directory as the automatic name includes the timestamp of the generated report. Click OK when you are done.

Reader 7.1.0.106 Reader File View Tools	Report Help	,											All Projec	- 0 ×
<del>)</del> []	Welcor	me ×	O Extr	action S	ummar	y (1)		Documents (4)	× 🕚 My Drive (2)	×				
Samsung CDMA_SM-J320VPP Galaxy J	3 2 🕕 N	∕ly Dri	ive (2)						_					
	Table \	View	Folder	View										
	XEE XEE	ii D	• Ø•	7 -	، چ	۰	Export	• <sub>X</sub> 7			~ <b>Q</b>	Documen	nts	Go to
	00	000	- ~		$\bigtriangledown$	×	K ()	† Name		• Path			Details	Events (0)
Applications (199) (28)				1				Paypal.pdf		Google Drive	e Files hryanwuphf@gmail.	<u> </u>		
P Audio (3)			<b>v</b>	2				Receipt Ord	er #126-5680132-2492337.pd	f Google Drive	e Files hryanwuphf@gmail.	Name:	Paypal.pdf	
Databases (294)												Type: Size (bytes):	Documents 71201	
												Path:	Google Drive Fi	iles hryanwuphf@gmail.com/Share
🛃 Images (1175) (22) (11 known files)			🖪 Export Di	ialog Wind	low					×		Created:	With Me/My Di 4/4/2018 12:57	
			File name	c	My	/ Drive	Documer	nts				Accessed:	4/4/2018 12:58	
			Save to:		_			sktop\My Reports	1			Modified: Deleted:	4/4/2018 12:57	(UTC-7)
			Report sul			imsung	.2018-04	-17.16-10-54		Required		Extraction:	Physical	
> 🏷 Tags (2)			Include	translati	ons							MD5:	75eed742a6d4l	b8ea6593b5e5e12e32f4
💼 Reports												Map		
									> ок	Cancel		Position:		
											·	Address:		
												Map Addre	HSS:	
	<										>			
	> Total: 2	Deduplic	ation: 0 It	tems: 2/2	Selecte	ed: 2	Path: Goo	gle Drive Files hrya	nwuphf@gmail.com/Shared V	Vith Me/My Drive	/Paypal.pdf			

Figure 6-17: Export Window Specifications Should be Changed EXCEPT for the Report Sub Directory

Open the "Paypal.pdf" and "Receipt Order #126-5680132-2492337.pdf" from Ryan's My Drive with Adobe Acrobat Reader (get.adobe.com/reader/) by navigating to the location you exported the files:

.../Desktop/My Reports/Samsung .2018-04-17.16-10-54/files/Document/

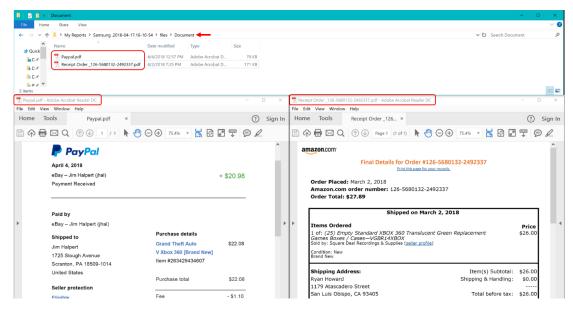


Figure 6-18: Open the Exported Paypal and Amazon Receipts from Ryan's My Drive

Observe that the Paypal document is a receipt for a Paypal payment from Jim Halpert for Grand Theft Auto V on eBay. This is proof that Ryan is selling scam copies of Grand Theft Auto V for profit.

Observe that the Receipt Order #126-5680132-2492337 document is a receipt for an Amazon order by Ryan for empty Xbox 360 game cases. You should note Ryan's home address is 1179 Atascadero Street in San Luis Obispo.

Tag the Amazon receipt as "Evidence" with description like given in figure below.

Reader File View Tools												All Projec	ts
Ċ	Welcor	me ×	O Extr	action	Summar		< O Do	cuments (4) × 🛛 My Drive (2)	×				
Samsung CDMA_SM-J320VPP Galaxy .	JE 🕕 N	/ly Driv	e (2)										
	Table \	/iew	Folder	View									
	-				-			-		[a]	Documen	ts	Go to
Analyzed Data	111 VIII	≣ D•	0 -	7 -	T T	9	Export •	×.		~ Q			
	00	Oco	- ~	#	1	×	K Ø	† Name	•	Path	De	rtails	Events (0)
Applications (199) (28)	_		✓	1				Paypal.pdf		Google Drive Files hryanwuphf@gmail.co			
					•						Name: Type:	Receipt Order # Documents	126-5680132-2492337.pdf
				2	Ē	J		Receipt Order #126-5680132-2492337	.pdt	Google Drive Files hryanwuphf@gmail.co	Size (bytes):	174449	
Databases (294)											Path:		les hryanwuphf@gmail.com/
Documents (4) (1)												Shared With Me #126-5680132-	e/My Drive/Receipt Order 2492337.pdf
💹 Images (1175) (22) (11 known files)											Created:	4/2/2018 19:25	
											Accessed: Modified:	4/2/2018 19:25 4/2/2018 19:25	
											Deleted:	4/2/2010 15.25	010-1)
											Extraction:	Physical	
											MD5:	ad7f2f4db3955	44ca05c89b9116f1eb4
💼 Reports											Map		
											Position:		
											Address:		
											Map Addre	ss:	
											Tags		
											Labels :	Evidence	
											Description :	-Contains Ryan's	street address
	<									2		-Proof of purcha	se of Xbox 360 empty game filled with scratched discs and

Figure 6-19: Tag Amazon Receipt Containing Address and Proof of Xbox 360 Cases Purchase

In addition, the exported files' information, including timestamps, path, and hash value, can be found within the generated report in this case named "My Drive Documents." This report is located at:

```
.../Desktop/My Reports/Samsung .2018-04-17.16-10-54/
  Image: Samsung .2018-04-
             Share
                  View
                                                                                      File Edit View Wi
                                                                                          Home Tools My Drive Documen... ×
                           sung .2018-04-17.14
                                                                                                                                                                       ? Sign In
          My Reports > :
                                         10-54 ┥
                                                                                      Q
                                                                      Size
                                          Date modified
                                                        Туре
                                                                                          🖺 🗇 🖶 🖂 Q. 🗇 🕘 1 / 1 🖡 🖑 🖂 🕀 77.6% 🔹 📙 🛃 🎔 🗩 🖉
 📌 Quick acc
           🖡 files
                                          4/17/2018 4:10 PM File folder
  Desk 🖈
                                              2018 4:10 PM
  Dow 🖈 🐚 Doci 🖈
          👎 My Driv
                                                                                                         ie Pictu 🖈
  🕹 Goo 🖈
                                                                                                                    LINKS TO VIEW FILE
                                                                                              Data Files (2
 🧎 Training
 🐴 OneDrive
                                                                                              # File Info
 Name
Path:
                                                                                                                Google Drive Files
hryanwuphf@gmai
Me/My Drive/Pavo
 📌 Network
                                                                                                   Nam
                                                                                                                 hryanwuphf@gmail.
Me/My Drive/Receip
3 items 1 item selected 69.0 KB
```

Figure 6-20: Extraction Report of My Drive Documents Includes Metadata from Device



## **Android Forensics CCIC Training**

## Chapter 7: Installed Applications

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 7

## **Installed Applications**

## Introduction

By looking at the applications installed by the user, you as a forensic examiner can get a better idea of how and what they utilized on their phone. If the user had pictures, documents, and videos, how are they viewed and edited? If the user wanted to remain organized with lists and notes, how are they created and maintained? If the user wants to email and message other individuals, how is the communication viewed, sent, and received?

In this chapter, you will be examining the Android-provided list of installed applications. Applications are almost never the same (with the exception of default applications), so the information about how they were used will be stored differently. It is also possible that the storing of information may change between versions of the application. You can research the application online and test how evidence is being stored by downloading the application onto a virtual machine.

To view a list of ALL applications installed on the device (default and user downloaded), navigate to:

```
/Analyzed Data/Installed Applications/
```

You can examine the right pane for a summary of the information within each entry. If you would like to view the information collectively for all entries, right click on the filter bar to change the columns which are shown. In this case, the blank columns for the device which should be unchecked are Description and Application ID.

Reader File View Tools F	eport help							All Projects	4
	Welcome × O	Extraction Sum	mary (1) 🛛 🤘	Installed Application	s (248) ×				
Samsung CDMA_SM-J320VPP Galaxy	Installed A	Applications	(248)	TAB	WILL APPE	AR			
Extraction Summary (1) File Systems	籠 🎕 🏗 🔘 •	🔞 🗇 🐼 🔟	Export • 📈			able Search	Installed App	plication	Go to
Analyzed Data	r ↑# 🕾 🗙	K Decoded by	Namo 🔻	Vorcion - Descrip	tion -	Identifier	Name:	Арр	
> 🛃 Autofill (1) > 🛗 Calendar (17) (4)	1		Exclude     Bookmark		×	COM ME MORSON AS A COMMENSATION OF THE CARE OF THE CAR	Version: Description:	Арр 1.0	
> Call Log (3)	2	Cellebrite	Deleted     Carved		т		Identifier: Application ID:	com.mr.meeseeks	
<ul> <li>Cookies (368) (8)</li> <li>Cookies (268) (8)</li> <li>Cookies (268) (10)</li> </ul>	3		Version	Υ Υ	CO	LUMNS SHOWN editors.de	Purchase Date: Deleted Date: Copyright:	4/5/2018 15:06(UTC-7)	
Bevice Users (1)     Emails (17)	4	Cellebrite	Description	•		com.google.android.apps.docs	Extraction: Source file:	Physical	
<ul> <li>Mais (17)</li> <li>Installed Applications (248) (1)</li> <li>MMS Ressages (5) (1)</li> </ul>	5		Application	Date		com.google.android.apps.docs	Permission Network		
<ul> <li>DOUBLE CLICK</li> <li>Passwords (2)</li> <li>Powering Events (4)</li> </ul>	6		Permission     Copyright     Source file	5		com.paypal.android.p2pmobile	Application In Databases		
	7		Extraction     Restore De	fault		com.google.android.instantapps.supervi:			
Wireless Networks (1)	8	Cellebrite	Any.do	4.9.1.2		com.anydo			
Data Files	9		Any.do: To-do I	. 4.9.1.2		com.anydo			
K Carving						>	/		

Figure 7-1: Extensive Installed Applications List

Before beginning your analysis, sort the applications by name to separate those used by the user and run by Android for functionality. Click the Name column title and then Sort Ascending in the pop-up menu.

Reader File View Tools R	eport Hel										All Projects	٥
0	Welco		Extraction Sum	mary (1) 🛛 🥌	Installed App	plications (248) ×						
Samsung CDMA_SM-J320VPP Galaxy	<b>O</b> II	nstalled A	Applications	(248)								
> 📄 Extraction Summary (1)	<b>XE</b> XE	ED.	🐨 🕫 🔲	Export • J7		Table	Search		۹	Installed Ap	uliantian	Go to
> 📑 File Systems	Ger VI-	- D	Ф () Ф <u>Ш</u> (						-	Installed Ap	plication	Go to
' 🕣 Analyzed Data	1 †#	🖉 🗙	K Decoded by ▼	Name 🔻	Version 💌	Identifier	•	Purchase Date		Name:	App	
> 柔 Autofill (1) > 臨 Calendar (17) (4)		Sort Ascend			N.	com.mr.meeseeks		4/5/2018 15:06(UTC-7)	î	Version: Description:	1.0	
> Call Log (3)		Clear Filter	naing		CLICK	TO OPEN				Identifier:	com.mr.meeseeks	
> @ Contacts (21) (11)	2				SORTIN	IG MENU	ors.docs	4/3/2018 09:39(UTC-7)		Application ID:		
> 🚯 Cookies (368) (8)	3				1.18.112.04.34	com.google.android.apps.docs.edite	ors.docs	4/3/2018 09:39(UTC-7)		Purchase Date: Deleted Date:	4/5/2018 15:06(UTC-7)	
>   Device Locations (10)			ок 📃 📃	Cancel						Copyright:		
A Device Users (1)	4		Cellebrite	Drive	2 18 112 02 34	com.google.android.apps.docs		4/2/2018 19:28(UTC-7)		Extraction:	Physical	
> 🖂 Emails (17)	5									Source file:		
Installed Applications (248) (1)	5			Google Drive	2.18.112.02.34	com.google.android.apps.docs		4/2/2018 19:28(UTC-7)		Permission	ns	
> 💬 MMS Messages (5) (1)										Network		
> 🔛 Notes (2)										Application In	nfo	
m Passwords (2)	6			PayPal	6.23.0	com.paypal.android.p2pmobile		4/2/2018 12:33(UTC-7)		Databases		
Powering Events (4)										Databases		
> 🕞 Searched Items (71)												
> 🗘 SMS Messages (34) (2)	7			Instant Apps	2.20-release	com.google.android.instantapps.sup	pervisor	4/2/2018 11:43(UTC-7)				
Q User Accounts (12)												
> (1) Web History (196) (1)	_											
<sup>9</sup> <sup>4</sup> Wireless Networks (1)	8		Cellebrite	Any.do	4.9.1.2	com.anydo		4/2/2018 11:32(UTC-7)				
Data Files	9			Any.do: To-do I	4.9.1.2	com.anydo		4/2/2018 11:32(UTC-7)				
									~			
🕓 Timeline (776) 🗸 🗸			on: 0 Items: 248/2						>			

Figure 7-2: Ascending Sort Allows for Separation Between User and Android Background Applications

Now, scroll down until you reach the first application with a Name value. Applications without a Name value, for the most part, are background applications utilized by Android and therefore not executed or controlled by the user.

The Identifier column lists what is known as the application's package name, a unique Android ID that looks like a Java package name such as com.myapplicationname. This also represents the name of the file location which stores the data required to run the application. For example, the Any.do application's package name is "com.anydo" and its stored data is located at "/Image13(ExtX)/Root/data/com.anydo/."

When you are examining the installed applications from the device, use known default applications, such as Camera and Clock, to identify which specific applications were downloaded from the Google Play Store by the user. In this case, you see the Camera and Clock applications were installed (by Android) on 8/2/2016 at 4:53. Not only do we know the device was activated on 3/31/2018 from the Extraction Summary under Device Info, but also a large variety of the applications have the exact same timestamp. Therefore, with examination you can identify which applications the user downloaded specifically and further investigate associated data by navigating to the provided package name.

Reader File View Tools R				Extraction Sumn		Installed A	"PACKAGE	<b>,</b>		1	All Projects	
	Welco	me ×	0	Extraction Sumn	nary (1) 🛛 🥌	Installed A	OR LOCATION C	F APP				
Samsung CDMA_SM-J320VPP Galaxy	🔲 lı	nstalle	ed A	Applications (	248)		DATA WITHIN FILE	SYSTEM				
Extraction Summary (1)	<b>新</b> ※	EN		🐨 河 🐨 🔲 E	west v			Table Search	۹		n	-
📑 File Systems	80- VD-	8=   LP		Ф ( <b>П</b> р	dour . Xi		•	lable search	~	Installed Ap	plication	Go
Analyzed Data	r =	$\bigtriangledown$	×	K Decoded by ▼	† Name ▼	Version	• Identifier	<ul> <li>Purchase</li> </ul>	Date	Name:	Clock	
> 🛃 Autofill (1)	8			Cellebrite	Any.do	4.9.1.2	com.anydo	4/2/2018	11:32(UTC-7)	Version:		
> 📆 Calendar (17) (4)	<b>+</b> .				Any.do: To-do I	4912	com.anydo	4/3/2018	11:32(UTC-7)	Description: Identifier:	com.sec.android.app.clockpackage	
> 📞 Call Log (3)	SCRC	111			Phily.uo. 10-001	4.3.1.2	contanyuo	4/2/2010	11.52(010-7)	Application ID:	consecurationapperocepaceage	
> (2) Contacts (21) (11)	Jene										8/2/2016 04:53(UTC-7)	
> 🕙 Cookies (368) (8)	1				App	1.0	com.mr.meeseeks	4/5/2018	15:06(UTC-7)	Deleted Date: Copyright:		
>      OB Device Locations (10)	_									Extraction:	Physical	
A Device Users (1)	19				Calculator		com.sec.android.app.popupcal	ulator 8/2/2016	04:53(UTC-7)	Source file:		
> 🖾 Emails (17)										Permission	26	
Installed Applications (248) (1)	29				Calendar		com.android.calendar	8/2/2016	04:53(UTC-7)		15	
> 💬 MMS Messages (5) (1) > 📄 Notes (2)										Network Application Ir	fo	
<ul> <li>Passwords (2)</li> </ul>										Audio		
Powering Events (4)										Display		
> 🕞 Searched Items (71)	13				Camera		com.sec.android.app.camera	8/2/2016	04:53(UTC-7)	Bluetooth		
SMS Messages (34) (2)							competantionaloppicamera		01.55(0101)	Databases		
Q User Accounts (12)												
> (1) Web History (196) (1)											AND CLOCK ARE	
Wireless Networks (1)										GOOD	REFERENCES FOR	
Data Files	28			Cellebrite	Chrome		com.android.chrome	8/2/2016	04:53(UTC-7)	DETERM	/INING DEFAULT	
K Carving	30				Clock		com.sec.android.app.clockpack	age 8/2/2016	04:53(UTC-7)	AP	PLICATIONS	

#### Figure 7-3: Examine Applications Further by Package Name and Determine Default Applications with Timestamps

Observe the installation of the Any.do To-do List and Task application. You will further investigate the information stored by the application such as to-do lists and notes in Chapter 10 and therefore the file should be tagged as "Evidence" and "Further Investigation."

Lastly, you can scroll to the right to identify the permissions allowed by the user for each application. This can be useful in making more in-depth inferences about the user's utilization of the installed application.

Figure 7-4 also shows an example of a non-default application installed and utilized by the user. Notice the timestamp is not 8/2/2016 at 4:53 and that the application is eBay which directly pertains to this investigation regarding accusations of eBay scams by Ryan. This application is also important so the file should be tagged as "Evidence."

	w	elcome ×	O Extraction Summary (1) × 🧧	nstalled Applications (248)	×	PERMISSION	IS	1		
Samsung CDMA_SM-J320VPP Galaxy		Installed	Applications (248)		ALL	OWED BY L	ISER	2		
Extraction Summary (1) File Systems	201 201	# E D•	🐨 河 🧐 🚺 Export 🔹 📈			· ·	۹	Installed App	lication	Go t
Analyzed Data	•	Version 🔻	Identifier •	Purchase Date	Deleted Date	Permissions 🔻	c	Name:	eBay	
>			com.sec.android.app.clockpackage	8/2/2016 04:53(UTC-7)		Network Application Info Audio Display Bluetooth	^	Version: Description: Identifier: Application ID: Purchase Date: Deleted Date:	5.19.0.17 com.ebay.mobile 4/2/2018 11:27(UTC-7)	
> 😳 Cookies (368) (8)			com.vcast.mediamanager	8/2/2016 04:53(UTC-7)				Copyright:		
Device Ocations (10)     Device Users (1)     Device Users (1)     Emails (17)			"APP DOWNLOADED	8/2/2016 04:53(UTC-7)				Extraction: Source file:	Physical	
<ul> <li>Emails (17)</li> <li>Installed Applications (248) (1)</li> </ul>		1.18.112.04.34	DIUSEN	4/3/2018 09:39(UTC-7)				Permission	s	
> F MMS Messages (5) (1)	_	2.18.112.02.34	com.google.android.apps.docs	4/2/2018 19:28(UTC-7)						
> 📦 Notes (2)		5.19.0.17	com.ebay.mobile	4/2/2018 11:27(UTC-7)				Databases		
Passwords (2)	Dea	5.19.0.17	com.ebay.mobile	4/2/2018 11:27(UTC-7)		Network Accounts Application Info				
<ul> <li>&gt; [27] Searched Items (71)</li> <li>&gt; Q SMS Messages (34) (2)</li> <li>Q. User Accounts (12)</li> <li>&gt; (20) Web History (196) (1)</li> <li>* Wireless Networks (1)</li> </ul>			com.samsung.android.email.provider	8/2/2016 04:53(UTC-7)		Accounts User Dictionary Application Info Bluetooth Messages	I			
🖥 Data Files 🔻		SCROLL!	com.sec.android.gallery3d	8/2/2016 04:53(UTC-7)		Accounts Application Info	~			

Figure 7-4: Permissions Can Provide Additional Details About the Applications Use

In addition, observe that the default messaging application appears to be Verizon Messages+ due to no additional messaging applications being installed by the user.



## **Android Forensics CCIC Training**

Chapter 8: Contacts, Phone, and Messaging

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 8

## **Contacts, Phone, and Messaging**

## Introduction

Phones are likely to contain more personal information than an individual's laptop or wallet. They contain every person you keep contact information for, phone number you have called, SMS and MMS message you have sent, and so much more. Therefore, a suspect's phone is often critical in providing evidence towards an investigation.

While users can choose from a myriad of applications to utilize for sending messages, most choose the default messaging application provided by their manufacturer/carrier. In this chapter, you will examine the device's contacts, call logs, and messages which, in this case, includes the Verizon Messages+ app.

**Note:** For reference in this chapter, visit the Extraction Summary window and locate "Current SIM Phone Number" under Device Info. In this case, Ryan's phone number is 8059105153.

Reader File Vie					🚺 🍂	Projects	4
כ	Welcome × 💽 Extraction Summary (1) ×						
Samsung CDMA_SM-J320	OVPP Galaxy J3 All Content Physical	TAB WILL APPEAR					
Extraction Summary (1)	Extraction Summary -		+ Add	d extraction	Project setting	ngs	Generate report
Analyze DOUBLE	CLICK Structions: 1						
Carving Timeline (776)	Physical      Samsung CDMA SM-J320VP     Physical	PP Galaxy J3 2					
Tags (7)	Physical Extraction start date/time						
Reports	4/5/2018 15:06(UTC-7) Extraction end date/time						
	4/5/2018 15:48 C:\Users\celwe\Desktop\Hov	ward Case\Sa					
	4/5/2018 15:48 C:\Users\celwe\Desktop\Hov	ward Case\Sa					
	4/5/2018 15:48 C\USers\celwe\Desktop\Hov Ocase Information Case name Howard		Examiner name Ca	ssidy Elwell			
	Class Information			ssidy Elwell			
	Ad/S2018 15-88     CUbertiveleve/Deaktop\Hov     Case Information     Case name     Deaktment     California Cybersecurity Institu      Location Services Enabled     True     Mol 31146/2291937738	te	Device Content	ssidy Elwell			
	Ads/2018 15-88     CUlterrivice/wn/Dexktop/Hox     Case Information     Case name     Howard     Department     California Cybersecurity Institu      Location Services Enabled     Tate     M31     311440291937738     Advertising Id     Sccc658e-b310-dffe-b2     Current SM Operator     31140	ne da-d77a1a		ssidy Elwell	Calendar	17 (4)	
	Ads/2018 15-88     CUlterriveleve/Deaktop/Hox     Case Information     Case name     East name     East name     California Cyberacurity Institu     California Cyberacurity Institu     Cata constraints     California State     California Cyberacurity Institu     Cata constraints     Sint Advertising Id     Caccose State     Corternet Sint Operator     Sint Advertising Id     CCO     Sint Advertising Id     CCCO     Sint Advertising Id     Sint Advertising Id     CCCO     Sint Advertisi	ne da-d77a1a	Device Content     Phone Data     Autofil			17 (4)	
	Ads/2018 15.48     CUlterrivice/wn/Dexktop/Hox     Cale Information     Cale anime Howerd     Department California Cybersecurity Institu     Cale anime Supervise Enabled     True     MSI 311440291937738     Advertising Id Sccc6569-b310-dfftee3     Current SM Operator 311440     ICOD     Sin 4000002917734163     Sin 4000002917734     Sin 400000291774     Sin 4000000291774     Sin 4000000000000000000000000000000000000	ne da-d77a1a	<ul> <li>Device Content</li> <li>Phone Data</li> </ul>		Calendar Contacts	17 (4) 21 (11)	
	4/5/2018 15.48 C/Users/ice/we/Dexktop/Hox Cose name Howerd Department California Cybersecurity Institu California Cybersecurity Institu Coston Services Enabled Tore MSI 311440291937738 Advertising Id Sccc658+310-4ffecb Corrent SM Operator 31140 ICOD 91400002017734163 SM Change Operation 3 Corrent SM Operator Name Version SM Change Operation 3 Corrent SM Operator Name Version SM Change Minone August 105131 Corrent SM Operator Name Version SM Change Tore SM	ne da-d77a1a	Device Content     Phone Data     Autofil	1			
	4/s/2018 15.48     C.\Usernikelwe\Desktop\Hoi     Case Information     Case name     Department     Califormation     Case name     Department     Califormation     Top     Case Information     Top     Top     Case Information     Top     Correct State     Correct     Sin Change Operation     Sin Change Time     CA/22018 1739UTc+0     Correct State Topole     Correct     Corr	ne da-d77a1a	Device Content     Phone Data     Autofil     Gal Log	1	③ Contacts	21 (11)	

Figure 8-1: Extraction Summary Contains Device's Phone Number

### Contacts

To view the Contacts stored in the device, navigate to:

```
/Analyzed Data/Contacts/Native/
```

You can examine the right pane for a summary of the information within each entry. If you would like to view the information collectively for all entries, right click on the filter bar to change the columns which are shown. In this case, the blank columns for the device which should be unchecked are Contact Type, Organizations, Emails, Other Entries, Notes, Addresses, Group, Created, and Modified.

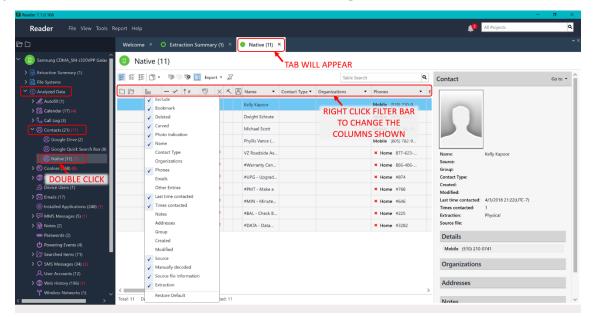


Figure 8-2: Native Device Contacts Listed

**Note:** In addition, the timestamp of last contacted and the number of times contacted are stored in each "Native" contact file. It is important to be aware that the timestamp does include messaging and phone calls as forms of contact, however the number of times contacted ONLY represents the number of phone calls.

When examining the contacts, focus your attention to those contact files known as "Native" (those stored by the Contacts application). This is because those within "Google Quick Search Box" are just shortcut files to the "Native" contacts and "Google Drive" stored contacts, in this case, contains no additional data.

Reader File View Tools F	keport I	ieip									All Projects	
	Weld	ome ×	O Ext	raction Summary (1) ×	Native (11) ×							
Samsung CDMA_SM-J320VPP Galax	0	Native (	11)									
Extraction Summary (1)	<b>8</b> #1 \$3	::D-	₹⊕ (	🖯 🧐 🔲 Export 🔹 🔬	7		Tab	le Sear	ch	۹	Contract	
🖹 File Systems	_						Idu	ve sean		~	Contact	Go to
🕄 Analyzed Data	†≠	$\otimes$ $\times$	KA	Name 👻	Phones	٠	Last time contacted	*	Times contacted	Source		
> 🛃 Autofill (1)	1			Kelly Kapoor	Mobile (510) 210-0741		4/3/2018 21:22(UTC-7)		1			
> 🛗 Calendar (17) (4)	2			Dwight Schrute	Mobile (805) 303-1855							
> 📞 Call Log (3) Y (Q) Contacts (21) (11)	3			Michael Scott	Mobile (805) 782-9881		4/3/2018 09:16(UTC-7)		1			
Google Drive (2)	· ·											
Google Drive (2)     Google Quick Search Box (8)	4			Phyllis Vance (Mom)	Mobile (805) 782-9766		4/4/2018 19:39(UTC-7)		1			
Native (11) (7)	5	×		VZ Roadside Assistance	× Home 877-623-7433						Name: Kelly Kapoor	
> 🛞 Cookies (368) (8)	6	×		#Warranty Center	× Home 866-406-5154						Source: Group:	
>      Device Locations (10)	7	×		#UPG - Upgrade Elig	× Home #874						Contact Type:	
A Device Users (1)	8	×		#PMT - Make a	× Home #768						Created:	
> 🖂 Emails (17)		×		#MIN - Minutes Used	× Home #646						Modified: Last time contacted: 4/3/2018 21:22	(UTC-7)
Installed Applications (248) (1)	-	×									Times contacted: 1	
> 💬 MMS Messages (5) (1)	10			#BAL - Check Balance	× Home #225						Extraction: Physical	
> 🔛 Notes (2)	11	×		#DATA - Data Used	× Home #3282						Source file:	
Passwords (2)											Details	
O Powering Events (4)											Mobile (510) 210-0741	
> 🕞 Searched Items (71)											o 1.2	
SMS Messages (34) (2) User Accounts (12)											Organizations	
> (User Accounts (12)											Addresses	
Wireless Networks (1)	<		_				_			>		

Figure 8-3: Timestamp of Last Contacted is Stored within Native Contacts Data

To view the Call Log that includes both outgoing and incoming phone calls for the device, navigate to:

```
/Analyzed Data/Call Log/
```

This is the best option for viewing and examining all phone calls due to the UFED Reader program automatically cross-referencing from the device's Contacts (as you just examined) and formatting the phone data into a filterable table as shown.

Reader File View Tools R		elp										4	2 All Projects	C
	Welc	ome × (	O Extract	on Summary (1) 🛛 ×	O Native (1	1) × 🔵 Call I	.og (3)	×						
Samsung CDMA_SM-J320VPP Galax		Call Log	(3)					TAR	WILL A	PPEAR				
Extraction Summary (1)	NE SE	ED.	0	河 🔯 🔲 Export 🔹	27				e Search		۹	Call Log		Go to
File Systems												Call Log		Go to
Analyzed Data	#	$\otimes$ $\times$	< □ €	Parties	•	↓ Timestamp	• 0	Ouration 🔻	Туре 🔻	Country code '	Networl	Timestamp:	4/4/2018 19:37(UTC-7)	
> 🛃 Autofill (1)	1		e	To: 8057829766 Phyllis	s Vance (Mom)	4/4/2018 19:37(UT	C-7) 0	0:01:48	Outgoing			Duration: Type:	00:01:48 Outgoing	
> 🛗 Calendar (17) (4)	2		e	To: 5102100741 Kelly	Kapoor	4/3/2018 21:10(UT	C-7) 0	0:12:09	Outgoing			Country code:	outgoing	
> (a) Contacts (21) (11)	3		C.	To: 8057829881 Micha	el Scott	4/3/2018 09:14(UT	c-7) 0	0:01:42	Outgoing			Network code: Network Name:		
> DOUBLE CLICK > @ Device Locations (10)												Source: Video call: Extraction:	Physical	
<ul> <li>A Device Users (1)</li> <li>&gt;</li></ul>												Source file:		
<ul> <li>Emails (17)</li> <li>Installed Applications (248) (1)</li> </ul>												Parties		
> F MMS Messages (5) (1)													6 Phyllis Vance (Mom)	
> 🕞 Notes (2)												101005102510	o Thyno Yance (moni)	
Passwords (2)														
O Powering Events (4)														
> 🕞 Searched Items (71)														
> 🗘 SMS Messages (34) (2)														
오 User Accounts (12)														
> (1) Web History (196) (1)														
۹۴ Wireless Networks (1)														
Data Files														
🕓 Timeline (776) 🗸 🗸	<										>			

Figure 8-4: Call Log with Timestamp and Duration

### Messaging

If you would like to examine SMS and MMS Messages through the File System, see Appendix D.

In this section, you will utilize the Analyzed Data provided by the UFED Reader program for viewing and examining messages due to its automatic cross-referencing from the device's Contacts and filterable table formatting.

### SMS (Text)

To view the SMS Messages sent and received on the device, navigate to:

```
/Analyzed Data/SMS Messages/
```

You can examine the right pane for a summary of the information within each entry. If you would like to view the information collectively for all entries, right click on the filter bar to change the columns which are shown. In this case, the blank columns for the device which should be unchecked are Delivered, Read, and SMSC (this data is placed under the Folder and Status columns instead).

Reader File View Tools	Report Help									All Projects	c
D	Welcome ×	O Extr	action S	ummary	(1) × O message.dl	5 × 💽 S	MS Messages (34) ×				
Samsung CDMA_SM-J320VPP Galax     Samsung CDMA_SM-J320VPP Galax	🕕 SMS N	/lessage	s (34)				ТАВ	WILL APPEAR			
<ul> <li>Extraction Summary (1)</li> <li>File Systems</li> </ul>	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	) • Q	T 🗇 🐨	ا 🔟 🤨	Export • 📈			Table Search	٩	SMS Message	Go to
<ul> <li>✓ O Analyzed Data</li> <li>✓ A Antolff (1)</li> <li>&gt; ∅ Antolff (1)</li> <li>&gt; ∅ Contacts (2) (1)</li> <li>&gt; ∅ Contacts (2) (1)</li> <li>&gt; ∅ Cookes (368) (8)</li> <li>&gt; ∅ Device Locations (10)</li> <li>. ∅ Devi</li></ul>			T       1       2       3       4       5       6       7       8       9       10       11		X S Trestamp Exclude Bookmark Deleted Carved Direction Timetsamp Delivered Read Folder Parties Body Status SMSC All timestamps Source file information	n           n	TO C	Read ICK FILTER BAR HANGE THE MNS SHOWN		Source: SMSC: Folder: inbox Timestamp: 4/5/2018 10:22(UTC-7) Delivered: Rad: Statu: Read Extraction: Physical Source file: All timestamps Network 4/5/2018 10:22(UTC-7) Parties From: 5102100741 Kelly Kapoor Body X T+	
> (III) W DOUBLE CLICK		<ul> <li>Image: Constraint of the second second</li></ul>	12	<ul> <li>Image: A start of the start of</li></ul>	Extraction Restore Default	יז ד) סוב-ז)			In Or	,	
Data Files  Carving  Timeline (776)	<	V	14		4/4/2018 09:18	UTC-7)			ln V		

Figure 8-5: SMS Messages are Cross-Referenced and Filterable

Examine the messages in chronological order to find Dwight Schrute's connection to the eBay scam and Kelly Kapoor's encouragement for the profit.

To sort the SMS Messages in order of sent and received, click the Timestamp column title and then Sort Ascending in the pop-up menu. You should now see a message to Kelly Kapoor at the top of the table.

۵	We	lcome ×	O Ext	raction Summary (1) $\times$	message.db	SMS Messages (34)	×			
Samsung CDMA_SM-J320VPP Galax	0	SMS M	essage	es (34)						
Extraction Summary (1)	XE :	E E D	. 0	1 Export •	∽		Table Search	٩		
> 📄 File Systems	1000 ·	ve av LP		de de 🛄 expore	C1		lable search	<b>_</b>	SMS Message	Go to
Y 🕜 Analyzed Data		⊗ ×	KG	† Timestamp 🔹	Folder 🔹	Parties	•	Body	Source:	
> 🔏 Autofill (1)		Sort Asce	nding		Qutbox	+18059105153		How is your day going, I	SMSC:	
> 🛗 Calendar (17) (4)		Z Sort Desc	ending		CLICK TO	OPEN Kelly Kapoor			Folder: Inbox Timestamp: 4/5/2018 10:22(UTC-7)	
> 📞 Call Log (3)	33	Clear Filte			SORTING	From 510210741 Kelly Kappor		Pretty good, are you ava	Delivered:	
>	32	From:		M/d/yyyy HH:mm 🖨 🔹	Outbox	+18059105153		I have project stuff to w	Read:	
> 🕙 Cookies (368) (8)		To:		M/d/yyyy HH:mm 🚔 💌		+15102100741 Kelly Kapoor			Status: Read	
> (10) Device Locations (10)	31				Inbox	From: 729725		PayPal: Your confirmatio	Extraction: Physical	
A Device Users (1)	30		ОК	Cancel	Inbox	From: 729725		PayPal: Your mobile num	Source file:	
> 🔀 Emails (17)	29		er	4/2/2018 12:52(UTC-7)	Inbox	From: 5102100741 Kelly Kapoor		Chipotle?	All timestamps	
Installed Applications (248) (1)				4/2/2018 13:10(UTC-7)						
> 💬 MMS Messages (5) (1)	28			4/2/2018 13:10(UTC-7)	Outbox	+18059105153 +15102100741 Kelly Kapoor		Sounds good.	Network 4/5/2018 10:22(UTC-7)	
> 🔛 Notes (2)	27		3	4/2/2018 13:10(UTC-7)	Outbox	+18059105153		I also have to go by Bes'	Parties	
Passwords (2)						+15102100741 Kelly Kapoor				
O Powering Events (4)	26		CK.	4/2/2018 13:17(UTC-7)	Inbox	From: 5102100741 Kelly Kapoor		Ok, I will accompany you	From: 5102100741 Kelly Kapoor	
Searched Items (71)     Q SMS Messages (34) (2)	25		2	4/2/2018 13:30(UTC-7)	Outbox	+18059105153		Thank you	Body 🕅 🅫	
Q User Accounts (12)			-			+15102100741 Kelly Kapoor			Yayi	
> (12) Web History (196) (1)	24		C	4/3/2018 09:23(UTC-7)	Outbox	+18059105153 +15102100741 Kelly Kappor		Morning Kelly, Sorry for		
Wireless Networks (1)	23		Ľ	4/3/2018 09:48(UTC-7)	Inbox	From: 5102100741 Kelly Kapoor		Love you toojust make		
> R Data Files				4/3/2018 10:13(UTC-7)						
> K Carving	22			4/3/2018 10:13(UTC-7)	Sent	To: 8053031855 Dwight Schrute		What packing materials		

Or, to access the conversation view, click the speech bubble icon in the tool bar.

Figure 8-6: Sort SMS Messages into Ascending Timestamp Order

Either way, you can easily traverse through the conversations in this window through either the table (as shown in Figure 8-6) or conversation view (as shown in Figure 8-7).

**Note:** With conversation view, a new tab will appear with the SMS messages reformatted like conversation speech bubbles. The messages can be changed between ascending and descending order by clicking the gear icon or unchecking SMS messages to view only a portion of conversations.

Reader 7.1.0.106		– o ×
Reader File View Tools F		All Projects
26	Welcome × O Extraction Summary (1) × O SMS Messages (34) × O Conversation (SMS Message ) ×	
Samsung CDMA_SM-J320VPP Galaxy	Conversation (SMS Message )     TAB WILL APPEAR	
Extraction Summary (1)	Export - 🕲 🗇 🔯 Enter text to filter 🗙	SMS Message Go to -
> 📄 File Systems <ul> <li>C) Analyzed Data</li> </ul>	Participants (3)	
<ul> <li>Analyzed Data</li> <li>Autofill (1)</li> </ul>	+18059105153 SORTING	Source: Verizon Message+ SMSC:
> 孟 Autofill (1) > 關 Calendar (17) (4)	Kelly Kapoor +15102100741 Dwight Schrute +18053031855	SMSC: Folder: Outbox
> Eis Calendar (17) (4) > 📞 Call Log (3)	Conversation	Timestamp: 4/2/2018 11:37(UTC-7)
> (G) Call Log (3)	− ✓ Select/Deselect all 13 messages	Delivered:
> (3) Contacts (21) (11)		Read: Status:
> (10) Cookies (366) (8)	To: Unknown	Extraction: Physical
Device Locations (10)     Device Users (1)	How is your day going, honey?	
Emails (17)	4/2/2018 11:37(UTC-7)	Source file:
<ul> <li>Installed Applications (248) (1)</li> </ul>	To: Unknown	All timestamps
MMS Messages (5) (1)		
> Notes (2)	UNCHECK TO VIEW I have project stuff to work on tomorrow, but I can meet Wednesday on break.  4/2/2018 12:06(UTC-7)	Parties
Passwords (2)	PORTIONS OF	+18059105153
O Powering Events (4)	CONVERSATIONS To: Unknown	+15102100741 Kelly Kapoor
> For Searched Items (71)	Sounds good.	
> Q SMS Messages (34) (2)	4/2/2018 13:10(UTC-7)	Body 📧 🕫
Q User Accounts (12)		How is your day going, honey?
> (1) Web History (196) (1)	To: Unknown	
1 Wireless Networks (1)	I also have to go by Best Buy for discs for the eBay project.	
> Data Files	4/2/2018 13:10(UTC-7)	
> K Carving	To: Unknown	
C Timeline (776)		
>`	Thank you 🗸	

Figure 8-7: Conversation View of SMS Messages

As another option for investigating messages and for use in proving your case in court, you can export the SMS Messages by clicking the Export drop down in the tool bar and then PDF.

Change the File name to "SMS Messages Ascending" and specify Save To as a folder called "My Reports" on your Desktop.

Do NOT change the Report Sub Directory as the automatic name includes the timestamp of the generated report. Click OK when you are done.

Reader File View Tools	Report Help					All Projects C
D	Welcome × O	Extraction Summary (1) ×	O mes	sage.db × 🥚 SMS Messages	(34) ×	
Samsung CDMA_SM-J320VPP Galax	SMS Mest	sages (34)				
<ul> <li>Extraction Summary (1)</li> <li>Estile Systems</li> </ul>	₩ % # D•	Q 🐨 🐨 💖 🛄 Export	· 📈		Table Search	SMS Message Go to
🕙 Analyzed Data	# 🛇 ×	HTML	Folder 🔻	Parties •	Body	Source: Verizon Message+
> 🛃 Autofill (1) > 🐻 Calendar (17) (4)	34	PDF XML	Outbox	+ 18059105153 + 15102100741 Kelly Kapoor	How is your day going, honey?	SMSC: Folder: Outbox
> 🍆 Call Log (3)	33	Word	Inbox	From: 5102100741 Kelly Kapoor	Pretty good, are you available tomorrow for lunch	Timestamp: 4/2/2018 11:37(UTC-7) Delivered:
> 🛞 Contacts (21) (11) > 🛞 Cookies (368) (8)	32	EML (email files)	Outbox	+ 18059105153 + 15102100741 Kelly Kapoor	I have project stuff to work on tomorrow, but I can	Read: Status:
>	31	4/2/2018 12:50(UTC-7)	Inbox	From: 729725	PayPal: Your confirmation code is: 331123. Your co	Extraction: Physical
용 Device Users (1)	30	4/2/2018 12:50(UTC-7)	Inbox	From: 729725	PayPal: Your mobile number is linked to your accou	Source file:
Emails (17) Installed Applications (248) (1)	29	4/2/2018 12:52(UTC-7)	Inbox	From: 5102100741 Kelly Kapoor	Chipotle?	All timestamps
> 💬 MMS Messages (5) (1)	28	4/2/2018 13:10(UTC-7)	Outbox	+18059105153 +15102100741 Kelly Kapoor	Sounds good.	Parties
<ul> <li>&gt; Motes (2)</li> <li>Passwords (2)</li> </ul>	27	4/2/2018 13:10(UTC-7)	Outbox	+18059105153 +15102100741 Kelly Kappor	I also have to go by Best Buy for discs for the eBay	+18059105153
Overing Events (4)	26	4/2/2018 13:17(UTC-7)	Inbox	From: 5102100741 Kelly Kapoor	Ok, I will accompany you after lunch :)	+15102100741 Kelly Kapoor
Searched Items (71)     Q SMS Messages (34) (2)	25	4/2/2018 13:30(UTC-7)	Outbox	+ 18059105153 + 15102100741 Kelly Kappor	Thank you	Body 114 How is your day going, honey?
오 User Accounts (12) > @) Web History (196) (1)	24	4/3/2018 09:23(UTC-7)	Outbox	+18059105153 +15102100741 Kelly Kapoor	Morning Kelly, Sorry for being preoccupied with th	How is your day going, noney?
M Wireless Networks (1)	23	4/3/2018 09:48(UTC-7)	Inbox	From: 5102100741 Kelly Kapoor	Love you toojust make some profit for the both c	
📕 Data Files	22	4/3/2018 10:13(UTC-7)	Sent	To: 8053031855 Dwight Schrute	What packing materials can you get this week? I ge	
Carving	<i></i>				· · · · · · · · · · · · · · · · · · ·	

Figure 8-8: Exporting SMS Messages is an Option for Ease of Investigation

**Note:** For the SMS Messages to appear in ascending order in the exported report, you must filter BEFORE exporting.

Open the "SMS Messages Acending.pdf" with Adobe Acrobat Reader (get.adobe.com/reader/) by navigating to the location you exported the files:

```
.../Desktop/My Reports/Samsung .2018-04-24.13-21-47/
         ₹ Samsung .2018-04-24.13-21-47
       Home
                Share
                        View
          \uparrow
                This PC > Desktop > My Reports > Samsung .2018-04-24.13-21-47 +
                                                                                            ✓ ♥ Search Samsung .2018-04-24.1...
                 Name
                                                       Date modified
                                                                                           Size
                                                                         Туре
  📌 Quick acc
                 resources
                                                       4/24/2018 1:29 PM
                                                                         File folder
   🗖 Desk 🖈
                 📜 SMS Messages Ascending.pdf
                                                       4/24/2018 1:29 PM
                                                                         Adobe Acrobat D...
                                                                                                84 KB
  👃 Dow 🖈
  Doci 🖈
  Pictu 🖈
  📕 Textl 🖈
  👃 Gooi 🖈 🗸
                                                                                                                         2 items
```

Figure 8-9: Navigate to Exported Report and Open

This Extraction Report contains all data associated with the SMS Messages extracted from the device. As you investigate the messages, remember to return back to the UFED Reader program and tag the messages of particular interest as "Evidence."

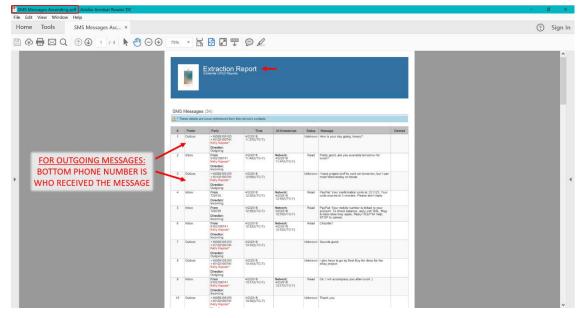


Figure 8-10: Extraction Report of SMS Messages from Device (in Ascending Order)

### MMS (Multimedia)

To view the MMS Messages sent and received on the device, navigate to:

```
/Analyzed Data/MMS Messages/
```

You can examine the right pane for a summary of the information within each entry. If you would like to view the information collectively for all entries, right click on the filter bar to change the columns which are shown. In this case, the blank column for the device which should be unchecked is Subject (not commonly used in messaging).

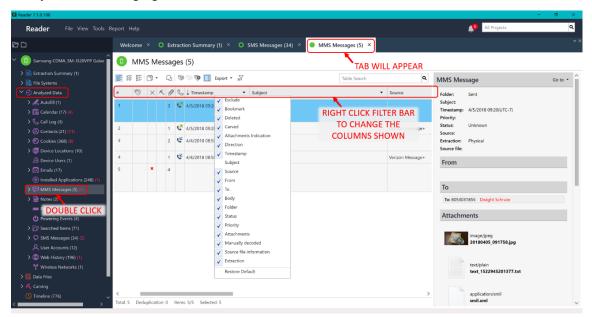


Figure 8-11: MMS Messages are Cross-Referenced and Filterable

Examine the multimedia that was attached to messages between Ryan and Dwight. You should begin to see the pieces coming together of Ryan's overall conspiracy as he communicates with Dwight Schrute to take advantage of his post office position to obtain free packaging and ship packages for free. These files should be tagged as "Evidence" and "Important."





Figure 8-12: MMS Messages from Ryan's Device in Correspondence with Dwight Schrute

When examining the MMS Messages, focus your attention to those messages with a Source of "Verizon Message+." This is because the other representations are duplicates of the messages which contain an additional .XML file used for proper viewing of the multimedia attachment.

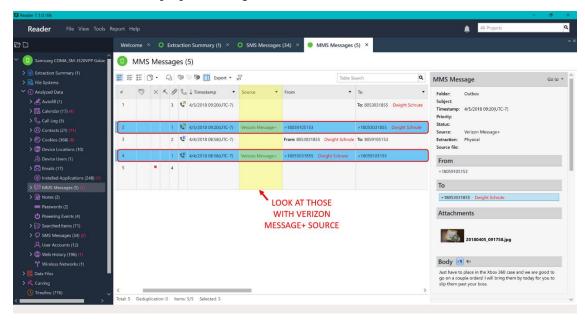


Figure 8-13: Examine the MMS Messages with Verizon Messages+ as a Source



## **Android Forensics CCIC Training**

### Chapter 9: Location Data

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 9

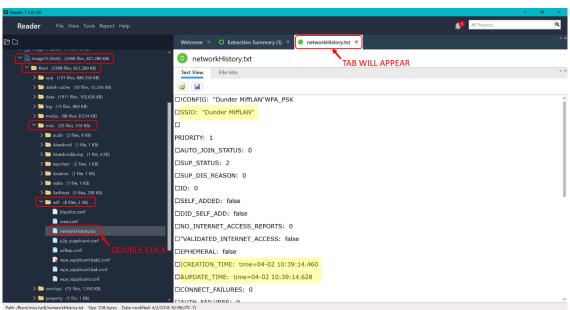
## **Location Data**

### Introduction

The integration of Wireless and Global Position System (GPS) functionality into mobile phones is certainly a technological innovation that has changed the field of Digital Forensics. Mobile phones use Wireless to receive high-speed internet (Wi-Fi) and communicate with external devices, such as printers and headphones (Bluetooth), within a particular area. This data can become extremely helpful for analysis when the user allows their device to connect to any open connections automatically, therefore resulting in location storing of frequently visited places. GPS also allows investigators to collect data from position-aware applications such as point-to-point directions through Google Maps, find location elements embedded within the metadata of files, and more interesting uses as applications continue to further incorporate use of location data. In this chapter, you will obtain all GPS location information within the device and learn how to map the locations collectively using Google.

### Wireless

To view the SSID of the Wireless Network utilized by the device and when the network was first connected to, navigate within File Systems to:



/Image13(ExtX)/Root/misc/wifi/networkHistory.txt/

Figure 9-1: Ryan's Wireless SSID with Creation Time

This information can also be viewed within:

/Analyzed Data/Wireless Networks/

Note: The Creation Date is NOT always viewable in this window, therefore follow Figure 9-1 above.

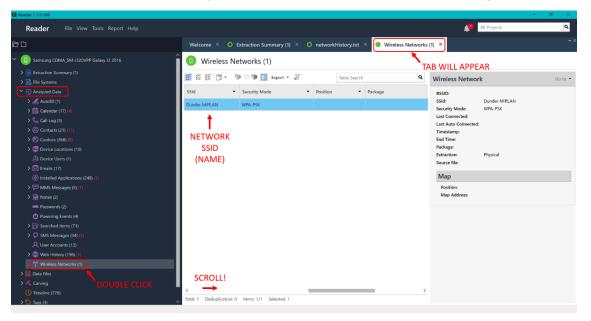


Figure 9-2: Another Location to View ONLY the SSID of Wireless Networks

### **Global Positioning System (GPS)**

### **Google Maps**

To analyze Google Map's Places data (Ryan's labeled places such as Home, Work, and Visited), navigate within File Systems to:

/Image13(ExtX)/Root/data/com.google.android.apps.maps/databases/

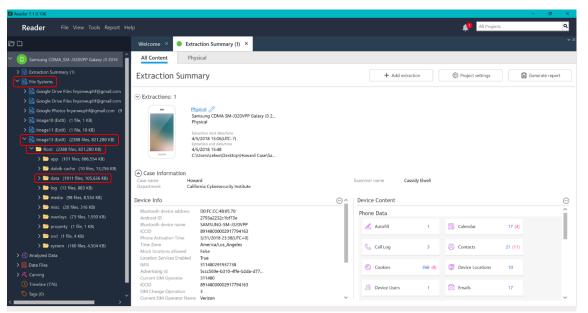


Figure 9-3: Navigation to Data Folder Containing Android Packages for Applications

Double click "gmm\_myplaces.db" within the databases folder. You should see a new tab and window appear to the right with the contents of the SQLite database gmm\_myplaces.

Reader 7.1.0.106			– ø ×
Reader File View Tools Report Help		All Projects	٩
80	Welcome × O Extraction Summary (1) × 🔵 gmm_myplaces.db ×		÷×
> 📂 com.android.server.telecom (1 file, 1 KB) 🛛 🔥			
> image: provide the setting (8 files, 260 KB)	gmm_myplaces.db		
> 🗁 com.android.shell (1 file, 0 KB)	Database view File Info		
> 🗁 com.android.systemui (1 file, 1 KB)			٩
> 🗁 com.android.vending (48 files, 765 KB)			-
> 🗁 com.anydo (30 files, 507 КВ)	sync_corpus (2)		•
> 🗁 com.ebay.mobile (27 files, 359 KB)	sync_item (3) en_US		
> 🗁 com.google.android.apps.docs (26 files, 807 KB)			
> 🗁 com.google.android.apps.docs.editors.docs (62 files, 3,800 KB)			
💙 🗁 com.google.android.apps.maps (12 files, 528 KB)			
🗡 🗁 databases (6 files, 524 KB)			
📄 gmm_myplaces.db			
gmm_offline-116977312440622544098.db			
gmm_storage.db DOUBLE CL/CK			
google_analytics_v4.db			
📄 riddler.db			
📄 ue3.db			
> 🗁 shared_prefs (6 files, 4 KB)			
> 🗁 com.google.android.apps.photos (30 files, 1,112 KB)			
> 🗁 com.google.android.configupdater (4 files, 1 KB)			
> 🚞 com.google.android.gm (88 files, 4,056 KB)			
Com.google.android.gms (275 files, 39,536 KB)			
> image: com.google.android.googlequicksearchbox (26 files, 14,296 KB)			
> >> com.google.android.gsf (5 files, 292 KB)			
> Com.google.android.instantapps.supervisor (7 files, 13 KB)			
> 🗁 com.google.android.music (5 files, 433 KB) 🗸 🗸			

c /Root/data/com.google.android.apps.maps/databases/gmm\_myplaces.db Size: 40 KB Date modified: 4/4/2018 12:32(UTC-7)

Figure 9-4: Ryan's Google Maps Places Database

To view the contents of the database, click the Database view tab and then "sync\_item." In the window, a list of SQLite database entries will appear with the timestamp, latitude, longitude, and location/address.

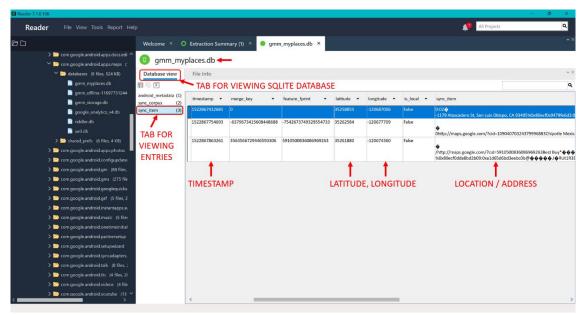


Figure 9-5: Viewing Database Entries Displays Timestamp, Latitude, Longitude, and Location/Address for Each Entry

### **File Metadata**

GPS locations are stored as metadata within documents, photos, and videos when location is enabled on the device. In Ryan's case, he had a few photos stored within the Media Gallery on the phone.

To view all files containing GPS location metadata, navigate to:

```
/Analyzed Data/Device Locations/
```

You can examine the right pane for a summary of the information within each entry. If you would like to view the information collectively for all entries, right click on the filter bar to change the columns which are shown. In this case, the blank columns for the device which should be unchecked are End Time, Address, Type, Precision, and Confidence.

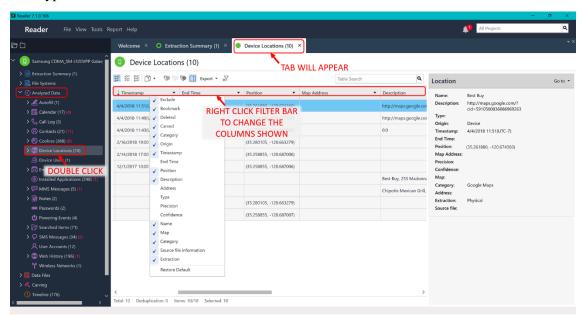


Figure 9-6: Ryan's Device Locations Displayed Collectively

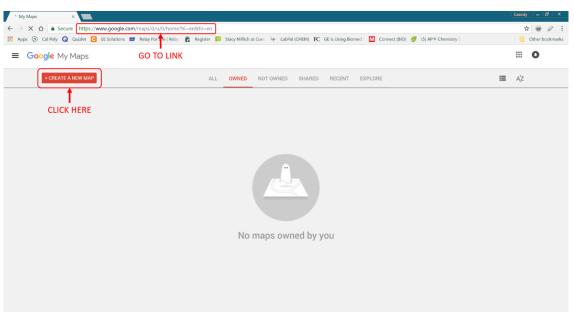
Observe that the location includes those discussed in Ryan's SMS messages and used for shipping items.

**Note:** This view collectively shows ALL device locations, therefore it also includes the data from Google Maps My Places.

### **Creating Map of GPS Locations**

As an investigator, creating a collective map with all device GPS locations is a great way to see patterns and commonly visited places.

To do so, visit open this link in a browser, sign into your Google account, and click Create a New Map:



www.google.com/maps/d/u/0/home?hl=en&hl=en

Figure 9-7: Create a New Map with Google

Begin by clicking "Untitled Map" and renaming the map based on the case, such as "Howard Device Locations." Click Save when you are done and the created map will be saved within your Google Drive.

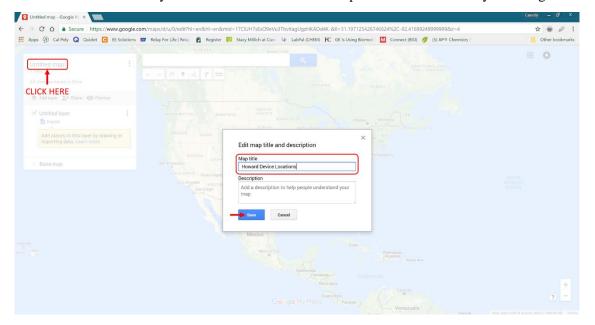


Figure 9-8: Name the Created Map such as "Howard Device Locations"

Now return to the UFED Reader program and double click on the first Position under Device Locations. Right click and select Copy.

10	Welcome × O Extrac	tion Summary (1) ×	Device Locations (10) ×						
Extraction Summary (1)     Extraction Summary (1)	Device Location	ns (10)							
	# # # # M. 00 00					•	_		
> 🛃 Autofill (1)	🗜 🗄 🗄 🖸 • 🗇 🕫	😻 🔲 Export • 📈		Table Sea	irch	٩	Location		Go to
> 🛗 Calendar (17) (4)	↓ Timestamp •	Position •	Description •	Name -	Map 🔻	Category	Name:	Best Buy	
	4/4/2018 11:51(UTC-7)	(35.261880. +120.674360)	http://maps.google.com/?cid=	Best Buy		Google Maps	Description:	http://maps.google.com/? cid=5910500836086969263	
>      O Contacts (21) (11)	4/4/2018 11:49(UTC-7)	nt Cul+X 20y Ctrl+C 77709)	attp://maps.google.com/?cid=	Chipotle Mexican Grill		Google Maps	Type:	cid=5910500836086969263	
Cookies (368) (8) Bevice Locations (10)			UBLE CLICK	1179 Atascadero St. Sa.		Google Maps	Origin: Timestamp:	Device 4/4/2018 11:51(UTC-7)	
Device Users (1)	2/16/2018 19:00	(35,280105, -120,663279)		20180216_761345.jpg		Media Locations	End Time:	4/4/2018 11:51(UTC-7)	
> 🔀 Emails (17)								(35.261880, -120.674360)	
(#) Installed Applications (248) (1)	2/14/2018 17:00	(35.258855, -120.687006)		20180214_124635.jpg		Media Locations	Map Address: Precision:		
> 💬 MMS Messages (5) (1)	12/1/2017 10:00	(35.258855, -120.687006)		20171201_945638.jpg		Media Locations	Confidence:		
> 📑 Notes (2)			Best Buy, 255 Madonna Rd, Sa			Google Maps	Map:		
			Chipotle Mexican Grill, 297 Ma			Google Maps	Category: Address:	Google Maps	
Overing Events (4)		(35.280105, -120.663279)				Google Photos	Extraction:	Physical	
> 🕞 Searched Items (71)						-	Source file:		
> Q SMS Messages (34) (2)		(35.258855, -120.687007)				Google Photos			
Q User Accounts (12)									
> (1) Web History (196) (1)									
Y Wireless Networks (1) > ■ Data Files									
> 🐔 Carving									
() Timeline (776)									
> 🏷 Tags (3)									

**Note:** Double clicking cells within tabs of Analyzed Data will allow you to copy the contained information.

Figure 9-9: Copy Information of Entries from UFED Reader

Paste the copied Position into the search bar and click the magnifying glass symbol. You will see a pin drop at the latitude longitude location and it listed in the left menu.

Click the plus sign next to the listed pin to save it to the map.

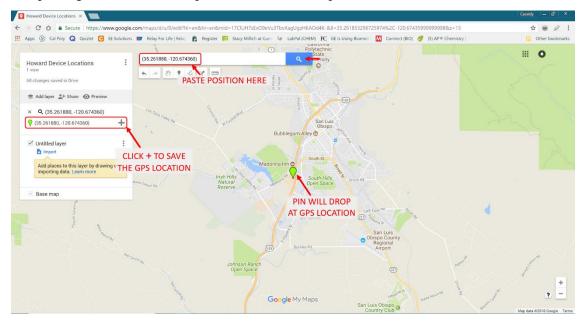


Figure 9-10: Paste Information in Created Map and Save GPS Location Pin

Click on the pin and then the edit button, which looks like a pencil.

**Note:** You also have the option to change the color of the pin for filtering and distinguishing GPS locations for your investigation.

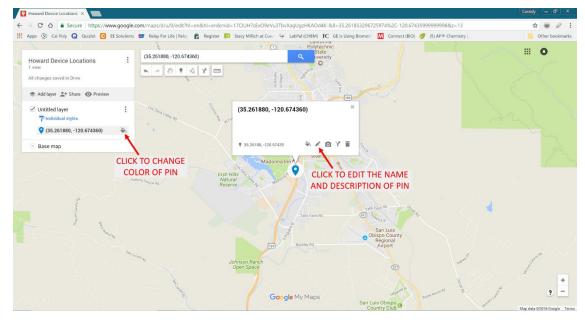


Figure 9-11: Select the Pin and Edit Details to Allow Proper Labeling

Next, label the pin to include the Name, Timestamp, and Position of the entry and click Save.

For example, a great labeling system is to list the Name and Timestamp in the Title text box and the Position in the Description textbox. This will display the most important information (Name and Timestamp) in the left menu listed beside its pin.

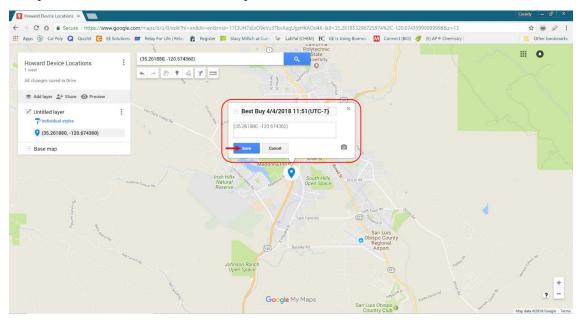


Figure 9-12: Label the Pin with Name, Timestamp, and Position with GPS Location Entry Information

Repeat this process for the remainder of the Positions under Device Locations.

In this example shown, all Positions are placed as pins with the Google Maps data colored in orange and the File Metadata colored in purple.

**Note:** Layers are another option for filtering and distinguishing GPS locations. To use layers, just click Add Layer and customize each layer using the three dots menu buttons.

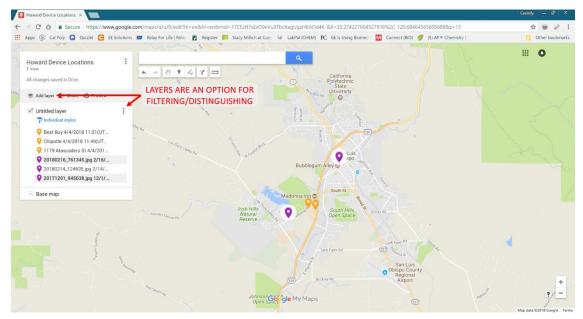


Figure 9-13: Created Map of Howard Device Locations and Layer Option Shown



## **Android Forensics CCIC Training**

Chapter 10: Calendar, To-do Lists, and Notes

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 10

## **Calendar, To-do Lists, and Notes**

### Introduction

When examining Ryan's installed programs and Home screen capture, you noticed his use of Calendar, Any.do, and a Samsung Notes widget. It is always important to check calendar and listing applications because they show the suspect's daily activities and recorded thoughts. This information can assist you in creating a timeline of evidence and viewing possibly important information the suspect needed to note. In this chapter, you will investigate the device's default calendar application and the user downloaded Any.do and Samsung Notes applications.

### Calendar

To view events and accounts associated with the Calendar application, navigate within File Systems to:

Reader 7.1.0.106		-	σ×
Reader File View Tools Report Help		All Projects	٩
60	Welcome ×	O Extraction Summary (1) × 🕒 calendar.db ×	
Y 🔲 Samsung CDMA_SM-J320VPP Galaxy J3 2016	calenda	dar.db	
> 📑 Extraction Summary (1)	Database view		
🗡 📄 File Systems			
> 🗟 Google Drive Files hryanwuphf@gmail.com (2 files, 69 KB)	期時区		۹
> R Google Drive Files hryanwuphf@gmail.com (1 file, 170 KB)	Attendees	(0)	•
See Google Photos hryanwuph@gmail.com (9 files, 0 KB)	CalendarAlerts CalendarCache	(3)	
	CalendarCache CalendarMetaData	(4)	
> 📑 Image10 (ExtX) (1 file, 1 KB)	Calendars	(4)	
> 📄 Image11 (ExtX) (1 file, 10 KB)	Colors	(35)	
Image13 (ExtX) (2388 files, 821,280 KB)	DeletedTasks	(0)	
Root (2388 files, 821,280 KB)	Events	(3)	
> 🗁 app (101 files, 686,554 KB)	EventsRawTimes	(3)	
> advik-cache (10 files, 13,256 KB)	ExtendedProperties		
✓ → data (1911 files, 105,636 KB)	Facebooks Images	(0) (0)	
	Instances	(3)	
> 🗁 android (1 file, 1 KB)	Maps		
Com.android.bluetooth (8 files, 20 KB)	Memos		
Com.android.calendar (4 files, 48 KB)	Notes	(0)	
> 🗁 com.android.chrome (884 files, 15,977 KB)	QSMemos	(0)	
> improvement contacts (1 file, 1 KB)	Reminders	(3)	
> tomancrosoconacta (Time, Tico)	Stickers	(0)	
	TaskGroup	(1)	
Com.android.keychain (1 file, 20 KB)	Tasks TasksAccounts	(0) (1)	
Com.android.mms (5 files, 82 KB)	TasksReminders	(1)	
Com.android.phone (4 files, 22 KB)	UpdatedTasks	(0)	
Y 🔄 com.android.providers.calendar (4 files, 184 KB)	_sync_state		
🗠 🗁 databases (1 file, 184 KB)	_sync_state_metadat	data (1)	
	LE CLICK ata squite_sequence		
Path: /Root/data/com.android.providers.calendar/databases/calendar.db Size	: 184 KB Date modifi	dified: 4/5/2018 14:47(UTC-7)	

/Image13(ExtX)/Root/data/com.android.providers.calendar/calendar.db/

Figure 10-1: Calendar Data Including Associated Accounts and Saved Events

To view the contents of the database beginning with the account(s) information, click the Database view tab and then Calendars. In the window, a list of SQLite database entries will appear listing the accounts logged into on Ryan's device and the specific calendars created within each account.

You should see and note that Ryan's personal Google account is "hryanwuphf@gmail.com."

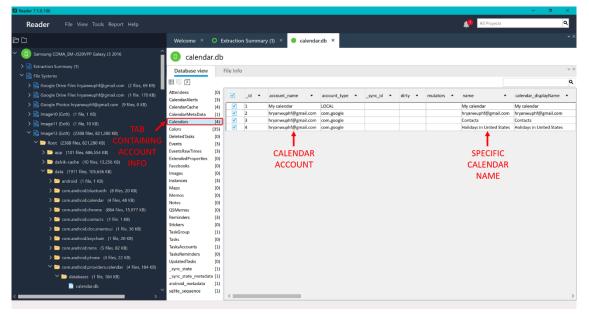


Figure 10-2: Calendar Accounts Logged into and the Specific Associated Calendars

To view the event detail contents of the database, click the Database view tab and then Events. In the window, a list of SQLite database entries will appear with the event's title and the GPS location and description (if applicable).

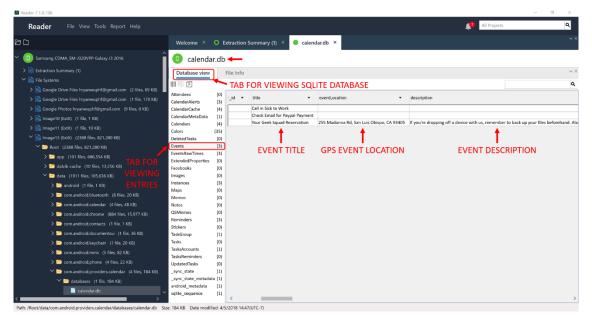


Figure 10-3: Viewing Database Entries Displaying Title, Location, and Description of Each Event

You may find it helpful to export the calendar data to a .CSV file which can be parsed with Microsoft Excel. To do so, click the left-most button with the symbol of a table. Change the File Name to be "Calendar Events" and Save to the folder created earlier called "My Reports" on your Desktop.

Reader 7.1.0.106	- a	×
Reader File View Tools Report Help	All Projects	٩
<b>P</b> D	Welcome × O Extraction Summary (1) × e calendar.db ×	-×
	Calendar.db      Database view     File Info      Celendar.db      C	<ul> <li>×</li> <li>Q</li> <li>Also, don</li> </ul>
<ul> <li>dahki-scale (10 fires, 13.258 (8))</li> <li>dahki-scale (10 fires, 155.364 K8)</li> <li>android (1 fire, 168)</li> <li>comandroid:Interform (84 fires, 24 K8)</li> <li>comandroid:Anore (84 fires, 15.977 K8)</li> <li>comandroid:Anore (84 fires, 25 K8)</li> <li>comandroid:Anore (1 fire, 164 K8)</li> <li>calendards</li> </ul>	Organize*     New folder       Image: Size     Name       Image: Size     Size	>

Figure 10-4: Export SQLite Database to CSV Containing Calendar Events

Double click the "Calendar Events.csv" file after navigating to /Desktop/My Reports/ to open the data in Microsoft Excel. You should see the SQLite file name listed first of the extracted file "calendar.db" followed by the specific Table name "Events" and each of the entries within the table.

**Note:** This is a great option for easily viewing SQLite Databases you would like to further investigate. You can click the Export to CSV button while viewing any .DB file within File Systems.

🕞 📕 👻 My Reports					- 0
file Home Share View					
> -> -> -> -> -> -> -> -> -> -> -> ->	<b>—</b>			v Ö +	Search My Reports
Dowr A Name	Date modified Type	Size			
Docu 🖈 🔋 Samsung .2018-04-17.16-10-54	4/17/2018 4:10 PM File folder				
Pictur # Samsung .2018-04-17.10-10-54	4/17/2018 5:18 PM File folder				
Textb      Textb      Textb	4/19/2018 9:30 AM Microsoft Exce	el C 5 KB			
€ Gooc #					
Andro#					
Training					
CneDrive					
This PC					
¥					
toSave 💽 🖬 🐬 🦿 🔹	Formulas Data Review View Hel	Calendar Events.csv - Excel		Cass	idy Elwell 💷 — 🗆
ioSave 💿 🖬 5 👌 • Re Home Insert Draw Page Layout		IP 🗘 Tell me what you want to do		∑ AutoSum · A	idy Elwell 📧 – 🗆
ooseve € cm 🛛 🖶 S 💸 * Re Home Insert Draw Page Layout 🕌 & Cut En Copy -	Ă = = → Wrap T	Hp Q Tell me what you want to do Text General •		∑ AutoSum · A ▼ Fill · Z▼	idy Elwell 📧 – 🗆
colare ● ○ 日 5	Ă = = → ↔ ab Wrap T	Hp Q Tell me what you want to do Text General •	onal Format as Cell Insert: Delete Form	∑ AutoSum · A ▼ Fill · Z▼	idy Elwell 📧 – 🗆
cSave ● cri	Ă = = → Wrap T	Ip     Q Tell me what you want to do       Text     General       Condition     Q Condition		The second seco	idy Elwell 📧 – 🗆
International Constraints of the second seco	À = = → the Wrap T A = = → the Wrap T A = = = → the the Merge	Ip          ⊋ Tell me what you want to do        Text     General       & Condition       & Condition       & Condition       & Condition	ing * Table * Styles * *	at	idy Elwell 📧 – 🗆
In the second se	À = = → the Wrap T A = = → the Wrap T A = = = → the the Merge	Ip          ⊋ Tell me what you want to do        Text     General       & Condition       & Condition       & Condition       & Condition	ing * Table * Styles * *	at	idy Elwell 📧 – 🗆
All and a set of the	A     =     =     * <td>IP         Q Tell me what you want to do           Text         General         -           &amp; Center         \$ - %         \$ 16 degrees           G         Number         6</td> <td>ing * Table * Styles * * Styles Cells</td> <td>Z AutoSum · A v Fill · Sort &amp; Find &amp; Clear · Fitter · Select · Editing</td> <td>idy Elwell 📧 – 🗆</td>	IP         Q Tell me what you want to do           Text         General         -           & Center         \$ - %         \$ 16 degrees           G         Number         6	ing * Table * Styles * * Styles Cells	Z AutoSum · A v Fill · Sort & Find & Clear · Fitter · Select · Editing	idy Elwell 📧 – 🗆
All B C D E E	A     =     =     * <td>Ip          ⊋ Tell me what you want to do        Text     General       &amp; Condition       &amp; Condition       &amp; Condition       &amp; Condition</td> <td>ing * Table * Styles * *</td> <td>Z AutoSum · A v Fill · Sort &amp; Find &amp; Clear · Fitter · Select · Editing</td> <td>idy Elwell 📧 – 🗆</td>	Ip          ⊋ Tell me what you want to do        Text     General       & Condition       & Condition       & Condition       & Condition	ing * Table * Styles * *	Z AutoSum · A v Fill · Sort & Find & Clear · Fitter · Select · Editing	idy Elwell 📧 – 🗆
Action of the second s	A     =     =     * <td>IP         Q Tell me what you want to do           Text         General         -           &amp; Center         \$ - %         \$ 16 degrees           G         Number         6</td> <td>ing * Table * Styles * * Styles Cells</td> <td>Z AutoSum · A v Fill · Sort &amp; Find &amp; Clear · Fitter · Select · Editing</td> <td>idy Elwell 📧 – 🗆</td>	IP         Q Tell me what you want to do           Text         General         -           & Center         \$ - %         \$ 16 degrees           G         Number         6	ing * Table * Styles * * Styles Cells	Z AutoSum · A v Fill · Sort & Find & Clear · Fitter · Select · Editing	idy Elwell 📧 – 🗆
A B C D E Solution Calabar de Ca	A     □     □     ②     ②     Wrap 1       A     □     □     □     ○     ○     ○       Algument     Algument     Image: Algument     Image: Algument	Q Tall me what you want to do      Ext.     General     S + % 9 % 48     Kunber      GPS EVENT LOCATION	ing - Table - Styles	Z AutoSum · A v Fill · Sort & Find & Clear · Fitter · Select · Editing	idy Elwell 📧 – 🗆
A B C D E Solution Calabar de Ca	A     □     □     ②     ②     Wrap 1       A     □     □     □     ○     ○     ○       Algument     Algument     Image: Algument     Image: Algument	Q Tall me what you want to do  Rext General     S - % 9 % 48 Condition     Kumber      GPS EVENT LOCATION	ing * Table * Styles * * Styles Cells	Z AutoSum · A v Fill · Sort & Find & Clear · Fitter · Select · Editing	idy Elwell 📧 – 🗆
totare of the file name: calendar.db ← Total: was: Jack book to the file name: calendar.db ← Total: w	A     ■     ● </td <td>Q Tell me what you want to do      Text     General     S - % 9 % 48     Kunber      GPS EVENT LOCATION  eventLocation</td> <td>ing - Table - Styles</td> <td>Z AutoSum · A v Fill · Sort &amp; Find &amp; Clear · Fitter · Select · Editing</td> <td>idy Elwell 📧 – 🗆</td>	Q Tell me what you want to do      Text     General     S - % 9 % 48     Kunber      GPS EVENT LOCATION  eventLocation	ing - Table - Styles	Z AutoSum · A v Fill · Sort & Find & Clear · Fitter · Select · Editing	idy Elwell 📧 – 🗆
A     B     C     C       A     B     C     Draw     Page Layout       Calbin     11     A       B     I     U     -       Cipboard     Formation     Formation       Cipboard     C     E       Solite file name:     calbin     11       A     B     C     D       Fable:     Events     Total rows: 3       Id     _yymc_ild     dirty mutators lastSynedd of 1	A B B B B B B B B B B B B B B B B B B B	Q Tell me what you want to do  Text General Generad General General General General General General General Gener	escription	∑ AutoSum · Ar P T Fill · Soft & Fild & Filter · Soft & Fild & Filter · Soft & Fild & Filter · Solect · Edding	koy Dwell 🖄 – C
A     B     C     A       A     B     C     C       Calibria     11     A       B     I     U       Cupboard     Fort       Table: Events     Fort       Table: Events     Table: Starter       IcalBin     0	A B B B B B B B B B B B B B B B B B B B	Q Tell me what you want to do  Text General Generad General General General General General General General Gener	escription	∑ AutoSum · Ar P T Fill · Soft & Fild & Filter · Soft & Fild & Filter · Soft & Fild & Filter · Solect · Edding	koy Dwell 🖄 – C
File     Home     Insert     Draw     Page Layout       So Cut     Calibrit     11     A       So Cut     Format Printer     Fort       Cutpboard     A     B     C       D Esolite file name: calendar db     Table: Events       Total rows: 3     Total rows: 3     Total rows: 3       I d calibrit     0     0	A B B B B B B B B B B B B B B B B B B B	Q Tell me what you want to do  Text General Generad General General General General General General General Gener	escription	∑ AutoSum · Ar P T Fill · Soft & Fild & Filter · Soft & Fild & Filter · Soft & Fild & Filter · Solect · Edding	koy Dwell 🖄 – C

Figure 10-5: Open and View the Exported Calendar Data Easily with Microsoft Excel

This information can also be viewed within:

```
/Analyzed Data/Calendar/hryanwuphf@gmail.com/
```

Observe how the calendar events validate other pieces of evidence to assist in forming a timeline. For example, "Call in Sick to Work" occurs on 4/3/2018 at 9AM as does his phone call to Michael Scott and "Check Email for Paypal Receipt" is validated by the Paypal document located in Ryan's downloads.

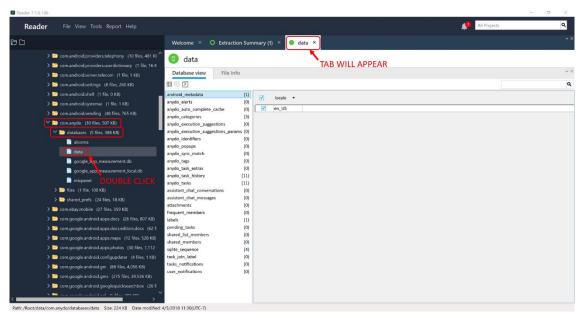
Reader 7.1.0.106										- a
Reader File View Tools Rep									4	1 All Projects
ם כ	Weld	come	× c	) Extraction Summary (1) $ imes$	hryanwuphf@gmail.com (	4) ×				
Samsung CDMA_SM-J320VPP Galaxy J3 .	Î	hrya	nwup	ohf@gmail.com (4)	TA TA	B WI	LL APPEAR			
> 📄 Extraction Summary (1)	100 M	EE	<u>اگا</u> -	🕲 🗇 🧐 🔲 Export 🔹 📈			Table Search	٩	Calendar Ent	rv Go to
> 📑 File Systems	June 1								Calendar Ent	19 0010
✓ ④ Analyzed Data	#	S	××	Subject	Location	Attend	dees 👻	Details	Category:	hryanwuphf@gmail.com
> 《 Autofill (1) ~ 臨 Calendar (17) (4)	1		×	Precinct Appointment	San Luis Obispo, California, Unit		vuphf@gmail.com vuphf@gmail.com	To see detailed infor	Subject: Start Date: End Date:	Your Geek Squad Reservation 4/5/2018 12:00(UTC-7) 4/5/2018 12:20(UTC-7)
Any Do: Personal (11) (1)	2			Your Geek Squad Reservation	255 Madonna Rd, San Luis Obis			If you're dropping o	Reminders:	4/5/2018 12:20(0TC-7) 4/5/2018 11:30(UTC-7)
hryanwuphf@gmail.com (4) (1)	3			Check Email for Paypal Payment					Priority:	
🔛 Unknown (2) (2)	-			Call in Sick to Work					Status: Class:	
> Call Log (3) DOUBLE CL	ICK								Repeat Rule:	
> (2) Contacts (21) (11)				T	T			T	Repeat Until:	
> 🕙 Cookies (368) (8)				EVENT TITLE	GPS EVENT LOCATIO	NC	EVEN	IT DESCRIP	Repeat Day:	
>    Device Locations (10)				EVENT THEE			EVE!	T DESCRIT	Extraction:	Physical
									Source file:	
Installed Applications (248) (1)									Attendees	
<ul> <li>MMS Messages (5) (1)</li> </ul>									Attenuees	
> Notes (2)									Details	
Passwords (2)										ing off a device with us, remember to back up
(D) Powering Events (4)									your files before	ehand. Also, don't forget to bring in any
> 🕞 Searched Items (71)									accessories invo you soon!	olved with the problem you're having. See
> SMS Messages (34) (2)										
									Map	
> (1) Web History (196) (1)									Location:	255 Madonna Rd, San Luis Obispo, CA 93405
1 Wireless Networks (1)	<							>	Event Position	
>	Total: 4	Dedu	plication	1: 0 Items: 4/4 Selected: 4						

Figure 10-6: Another Location to View Calendar Data from Gmail Account(s)

Next, you will examine the Any.do application contents, as you discovered in Chapter 7 that it was specifically installed by the user.

### **List Applications**

To view Ryan's To-do lists through the Any.do application, navigate within File Systems to:



/Image13(ExtX)/Root/data/com.anydo/databases/data/

Figure 10-7: Any.do List Application Data for Ryan

To view the specific tasks on the created lists, click the Database view tab and then "anydo\_tasks." In the window, a list of SQLite database entries will appear listing the status, timestamp of creation, and list item. Scroll to almost the end of the SQLite columns listed for this information.

The Status of the task will be represented by an integer: 1 – Not Completed, 2 – Completed, 3 – Deleted.

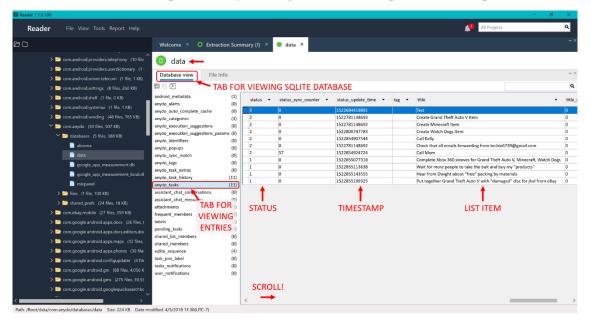


Figure 10-8: Each Any.do Task is Stored with its Creation Time and Status

Note: The timestamp of when an item was marked completed is NOT stored by the application.

This information can also be viewed within:

/Analyzed Data/Calendar/Any Do: Personal/

You can examine the right pane for a summary of the information within each entry. If you would like to view the information collectively for all entries, right click on the filter bar to change the columns which are shown. In this case, the blank columns for the device which should be unchecked are Location, Event Position, Attendees, Details, End Date, and Priority.

Reader 7.1.0.106							All Projects
Reader File View Tools Report Help							All Projects
D	Welcome × (	Extraction Su	mmary (1) × O data ×	Any Do: Personal (11) ×			
Samsung CDMA_SM-J320VPP Galaxy J3 2016	Any Do:	Personal (11	)	TAB WILL	APPFAR		
Extraction Summary (1)     Brile Systems	₩ % E 🗅 •	()) ()) ()) ())	Export • 📈	Table Search	٩	Subject:	Check that all emails forwarding from techie6739@gmail.com
✓ ⊕ Analyzed Data	# 🕾 ×	Subject	Z Exclude	▼ Location ▼	Event Positi	Start Date: End Date:	4/3/2018 09:38(UTC-7)
> 🛃 Autofill (1)	1	Put together Gr	V Bookmark	ior ih		Reminders:	
~ 闘 Calendar (17) (4)	2	Hear from Dwig	✓ Deleted	<b>RIGHT CLICK FILTER</b>	BAR	Priority:	
🛗 Any Do: Personal (11) (1)	-		✓ Carved	TO CHANGE TH	E	Status:	Completed
mail.com (4) (1)	3	Wait for more p	🖌 Subject	COLUMNS SHOW	/N	Class: Repeat Rule:	
	4	Complete Xbox	Location	hecra		Repeat Until:	
> 📞 Call Log (3)	5	Call Mom	Event Position			Repeat Day:	
> (2) Contacts (21) (11)		Check that all e	Attendees Details	il.com		Repeat Interval: Extraction:	Physical
> 🕙 Cookies (368) (8)			✓ Start Date	ii.com		Source file:	Physical
>	7	Call Kelly	End Date				
A Device Users (1)	8	Create Watch D				Attendees	
> 🖂 Emails (17)	9	Create Minecrat	V Status				
Installed Applications (248) (1)	10	Create Grand T	✓ Class			Details	
> 💬 MMS Messages (5) (1)			🗸 Repeat Rule				
> 🔐 Notes (2)	11 ×	Test	🗸 Repeat Until			Map	
Passwords (2)			V Repeat Day			Location:	
O Powering Events (4)			<ul> <li>Repeat Interval</li> </ul>			Event Position	n:
> 🕞 Searched Items (71)			<ul> <li>Reminders</li> </ul>				
> O SMS Messages (34) (2)			Category     Manually decoded			Tags	
Q User Accounts (12)			Source file information			-	Contraction in the second second
> (iii) Web History (196) (1)			<ul> <li>Extraction</li> </ul>		,		<ul> <li>Further Investigation</li> <li>Maybe used as fake information for eBay and</li> </ul>
↑ Wireless Networks (1) > ■ Data Files	< Total: 11 Deduplicat	ion: 0 Items: 11/1	· ·		,		Paypal?

Figure 10-9: Another Location for Viewing (and Filtering) Any.do Tasks

After filtering, observe the tasks connecting with other evidence within documents and messages. Tag these tasks as "Evidence." Most importantly, notice Ryan's completed task of forwarding all emails from "techie6739@gmail.com" and tag it as "Further Investigation." Email will be examined in Chapter 11.

### Notes

To view Ryan's Samsung Notes taken, navigate within File Systems to:

/Image13(ExtX)/Root/data/com.samsung.android.app.memo/databases/memo.db/

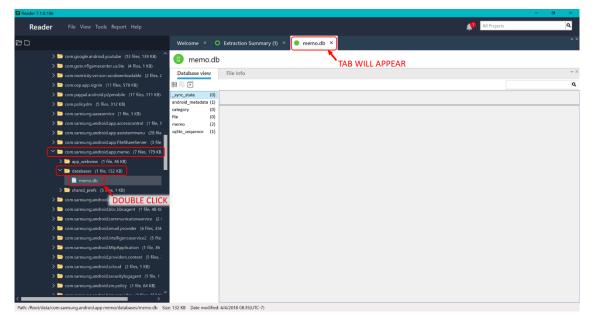


Figure 10-10: Samsung Notes SQLite within File System

To view each individual note, click the Database view tab and then "memo." In the window, a list of SQLite database entries will appear listing the memo title and content. Scroll to view timestamps.

**Note:** Viewing Samsung Notes data is best within Analyzed Data due to the ability to display the text in a more readable format.

							– a ×
Reader File View Tools Report Help					1	All Projects	٩
60	Welcome × O	Extraction Summary (1)	× 🖲 memo.db ×				≁×
> © com goople android youtube (13 files, 139 kB) > © com goople android youtube (13 files, 148) > © com noticity written sadownicable (2 files, 2 kB) > © com noticity written sadownicable (2 files, 2 kB) > © com spapal android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © com samung android appmentale (17 files, 179 kB) > © databases (16 file, 128 kB) > © databases (16 file, 128 kB) > © databases (16 file, 128 kB) > © com samung android dappmethramagentub (1 > © com samung android scient(2) (2 file, 14 kB) > © com samung android scient(2) (2 file, 14 kB) > © com samung android scient(2) (2 file, 14 kB) > © com samung android scient(2) (2 file, 14 kB) > © com samung android scient(2) (2 file, 14 kB) > © com samung android scient(2) (2 file, 14 kB) > © com samung android scient(2 file,	memo.db     Database view     very     very	File Info  TAB FOR VIEV  title  Notes on eBay Privacy  eBay Scarming Notes  tritle		www.dummies.com/business/onii			

Figure 10-11: Individual Memos Stored within Samsung Notes by Ryan

This information can also be viewed within:

/Analyzed Data/Notes/Samsung Notes/

Reader 7.1.0.106										-	a ×
Reader File View Tools Report Help									<b>4</b> 2	All Projects	٩
60	Wel	come		0 8	Extraction Summary (1) $\times$	O memo.db × 🧔 s	Samsung Notes (2) ×				
Samsung CDMA_SM-J320VPP Galaxy J3 2016	0	Sam	nsun	g N	otes (2)		TAB V	VILL APPE	٨R		
> 🕞 Extraction Summary (1) > 📑 File Systems	111 111	F 85	۵.	9	🖲 🗐 🧐 🛄 Export 🔹 📈		Table Search	٩	Note		Go to *
✓ ᠿ Analyzed Data	8	1	$\times$	ĸ		Modification Time •	Title 👻	Body	Title:	eBay Scamming Notes	
> 🖉 Autofil (1)	1				4/4/2018 08:23(UTC-7)	4/4/2018 08:35(UTC-7)	eBay Scamming Notes	- Make closing da	Creation time: Modification Time:	4/4/2018 08:23(UTC-7) 4/4/2018 08:35(UTC-7)	
> 🛗 Calendar (17) (4) > 📞 Call Log (3)	2				4/2/2018 11:40(UTC-7)	4/2/2018 11:46(UTC-7)	Notes on eBay Privacy	http://www.dumm	Source:	Samsung Notes	
> (2) Contacts (21) (11) > (3) Cookies (368) (8)					1	1	1		Extraction: Source file:	Physical	
>      @ Device Locations (10)						MODIFICATION	I TITLE		Summary 时	14	- L
B Device Users (1) > ⊠ Emails (17)					TIMESTAMP	TIMESTAMP					_
<ul> <li>Installed Applications (248) (1)</li> </ul>									Body 🛐 🕫	HTML Text	
> 💬 MMS Messages (5) (1)									- Make closing	dates soon after posted as the	
✓										people fall for the scam (ie. C Prices should be low enough	
Samsung Notes (2) Passwords (2)									entice buyers b	ut high enough for profit - Us	
Overing Events (4) DOUBLE CLICK										otos and official product insure bubbles in bubble mails	er are
> 🕞 Searched Items (71)									mostly popped	to back up the fact that the dis	sc is
> 🖓 SMS Messages (34) (2)										P.O. Box to send from, fake n	ame,
오 User Accounts (12)									and dummy em	ail address	
> (1) Web History (196) (1)											
1 Wireless Networks (1)									Attachment		
	<							>			
✓ ▲ Carving Images ✓	Total: 2	Ded	uplicati	on: 0	Items: 2/2 Selected: 2			/	Map		~
Ref Images											

Figure 10-12: Ryan's Samsung Notes Contains Investigation Critical Information

Examine the contents of the memos taken by Ryan and you should see a red flag in the last sentence of "eBay Scamming Notes" that fake information was used for selling online. Tag this file as "Evidence" and "Important." This would explain the use of "techie6739@gmail.com" rather than "hryanwuphf@gmail.com." In Chapter 11, Email and Internet History will be examined to validate this evidence.



## **Android Forensics CCIC Training**

Chapter 11: Email and Internet History

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 11

## **Email and Internet History**

### Introduction

Email and Internet History can be critical to your investigation as you need to know who the user is communicating with, what sites were being visited and information being searched for, and if data was being exchanged or downloaded. Earlier in this case, you found files in the Downloads folder and mentions of Ryan using fake personal details and email account for his eBay scam. Where did these files come from and what fraudulent information has he been using to fuel his scam?

You will address each of these questions in this chapter and have a better understanding of email and internet history. In this examination, you will recover email through the applications users utilize to view the data on mobile devices, such as Samsung Email or Gmail. Internet history will be examined collectively from the variety of popular and built-in browser applications through the UFED Reader program's Analyzed Data.

### Email

To view the Emails stored in the device, navigate to:

/Analyzed Data/Emails/

Reader File View Tools									All Projects
	Wel	come ×		Extrac	tion Summary (1) 🛛 🤇	Emails (17) ×			
Samsung CDMA_SM-J320VPP Gala	0	Emails	(17)	1		TAB WILL APPEAR			
🗟 Extraction Summary (1)		E IE O	• 1	2 3	🖲 똇 🚺 Export • 🗙		~ Q	Email	Go to
Analyzed Data		1	×	0	<pre>₲ ↓ Timestamp •</pre>	Subject 👻	Source	Account:	hrvanwuphf@gmail.com
> 🛃 Autofill (1)	1			1	4/5/2018 11:02(UTC-7)	Reminder: You're close to tech bliss	Gmail _	Snippet:	View: Mobile   Web Hi Ryan, Just a reminder, you have an upcoming Geek Squad®
> 🔞 Calendar (17) (4)	2				4/4/2018 18:43(UTC-7)	Check your Google Account security status	Gmail	Folder:	Inbox,
> 📞 Call Log (3) > @ Contacts (21) (11)	-				4/4/2018 12:01(UTC-7)	Your Precinct reservation is just around the corner	Gmail	Subject:	Reminder: You're close to tech bliss 4/5/2018 11:02(UTC-7)
<ul> <li>(c) Contacts (21) ((1)</li> <li>(c) Cookies (368) (8)</li> </ul>					4/4/2018 11:28(UTC-7)	An event from Gmail has been added to your Google Calendar	Gmail	Priority:	. 4/3/2010 11:02(010-1)
Device Locations (10)								Source:	Gmail
A Device Users (1)	5				4/4/2018 11:28(UTC-7)	Your Precinct reservation is confirmed	Gmail	Status: Extraction:	Unread Physical
> 🔀 Emails (17)	6				4/4/2018 11:27(UTC-7)	Information regarding your Best Buy account	Gmail	Source file:	
Instated Applications (248) (1)	7			4	4/3/2018 12:38(UTC-7)	Fwd: Congratulations, your item sold!	Gmail	From	
DOUBLE CLICK								From: Geel	kSquad@emailinfo.geeksquad.com Geek Squad
> 📄 Notes (2)	8				4/3/2018 11:49(UTC-7)	Fwd: Congratulations, Steve, your item has been listed.	Gmail	То	
Passwords (2)     Powering Events (4)	-							0.00	
Powering Events (4)     Powering Events (71)	9				4/3/2018 11:45(UTC-7)	Answer 2 questions and get 50% off Any.do Premium	Gmail	To: HRYAI	NWUPHF@gmail.com
SMS Messages (34) (2)	10			3	4/3/2018 11:36(UTC-7)	Fwd: Congratulations, Steve, your item has been listed.	Gmail	сс	
Q User Accounts (12)									
💮 Web History (196) (1)	11				4/3/2018 10:53(UTC-7)	Fwd: Congratulations, Steve, your item has been listed.	Gmail	BCC	
Mireless Networks (1)	12			1	4/2/2018 19:23(UTC-7)	Fwd: Your Amazon.com order of *(25) Empty Standard* has shipp	Gmail		
Data Files	13				4/2/2018 18:54(UTC-7)	Fwd: Activate your new account	Gmail	Attachr	nents
					.v	1	· · · ·		T T+ HTML Text

Figure 11-1: Emails are Listed in a Filterable Table

To open emails as formatted when received/sent on the device, you can export the Emails by clicking the Export drop down in the tool bar and then PDF.

Change the File name to "Emails" and specify Save To as a folder called "My Reports" on your Desktop.

Do NOT change the Report Sub Directory as the automatic name includes the timestamp of the generated report. Click OK when you are done.

B Reader 7.1.0.106							- 0 X
Reader File View Tools	Report Help					All Projects	٩
80	Welcome × O	Extraction Summary (1) ×	🗧 Emails (17) 🛛 ×				
Samsung CDMA_SM-J320VPP Gala	Emails (17)						
> 🛃 Extraction Summary (1) > 📑 File Systems	≝ ≋ E Ø• j	Q 🕲 🕫 💖 🔲 Export •	7		~ <b>Q</b>	Email	Go to 🔹 🏠
✓ ④ Analyzed Data	• • 🔊 × •	Excel	▼ Subject	• Source		Account: hryanwuphf@gmail.	:om
> 🔏 Autofill (1)	1	PDF	7) Reminder: You're close to tech bliss	Gmail	<u></u>	Snippet: View: Mobile   Web H have an upcoming G	li Ryan, Just a reminder, you
> 📴 Calendar (17) (d) > 📞 Call Log (3)	2	MIL Word	7) Check your Google Account security status	Gmail		Folder: Inbox, Subject: Reminder: You're clo	
> (a) Contacts (21) (11)	3	EML (email files)	7) Your Precinct reservation is just around the co	rner Gmail		Timestamp: 4/5/2018 11:02(UTC-	7)
> 🕙 Cookies (368) (8)	4	4/4/2018 11:28(UTC-	7) An event from Gmail has been added to your	Google Calendar Gmail		Priority: Source: Gmail	
>      Orice Locations (10)	5	4/4/2018 11:28(UTC-	7) Your Precinct reservation is confirmed	Gmail		Status: Unread	
A Device Users (1)	6	Export Dialog Window		×		Extraction: Physical	
> 🔀 Emails (17)	0	File name: Ema	ils	mail	_	Source file:	
Installed Applications (248) (1)	7	Save to: C:\U	sers\celwe\Desktop\My Reports	mail		From	
> 💬 MMS Messages (5) (1)		Report sub directory: Sam	sung .2018-04-26.11-13-49	Required		From: GeekSquad@emailinfo.geel	ksquad.com Geek Squad
> 📄 Notes (2)		Include translations			_	-	
Passwords (2)	8			mail		То	
O Powering Events (4)	9			OK Cancel mail		To: HRYANWUPHF@gmail.com	
> 🕞 Searched Items (71) > 🛇 SMS Messages (34) (2)	10	3 🕊 4/3/2018 11:36(UTC-	7) Fwd: Congratulations, Steve, your item has be	en listed. Gmail		сс	
Q User Accounts (12)							
> 🍈 Web History (196) (1)	11	4/3/2018 10:53(UTC-	7) Fwd: Congratulations, Steve, your item has be	en listed. Gmail		BCC	
M Wireless Networks (1)	12	1 🕊 4/2/2018 19:23(UTC-	Pwd: Your Amazon.com order of "(25) Empty :	Standard" has shipp Gmail			
> 🔀 Data Files	13	4/2/2018 18:54(UTC-	7) Fwd: Activate your new account	Gmail		Attachments	
> K Carving	<	•			>	Body 💌 🕫 HTML Text	
<	Total: 17 Deduplication:	0 Items: 17/17 Selected: 17					~ ~

Figure 11-2: Export Emails for Investigation as Formatted on Device

**Note:** If you would prefer for the Emails to be sorted differently when exported, be sure to sort the data by clicking on the proper column prior to choosing to export to a PDF.

Open the "Emails.pdf" with Adobe Acrobat Reader (get.adobe.com/reader/) by navigating to the location you exported the files:

.../Desktop/My Reports/Samsung .2018-04-26.11-13-49/

A short snippet of each email's content will be displayed with its metadata (timestamp, sender, receiver) and the name of extracted email file. If you scroll through the emails, you will find forwarded eBay emails regarding listed/sold items. One of particular interest is "mes-7.eml."

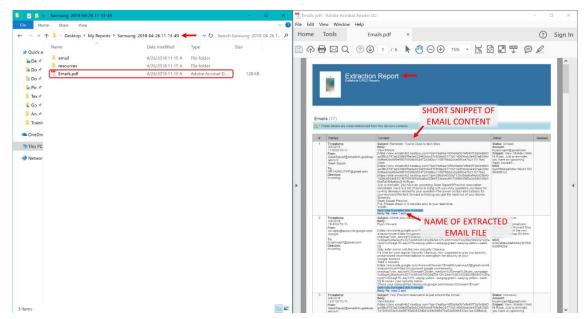


Figure 11-3: Extraction Report of Emails from Device

To investigate this email thoroughly and view it as formatted on the device, you will use a tool called Thunderbird Mail. You can download it from:

https://www.thunderbird.net/en-US/

Open Thunderbird Mail and click on the menu icon. Click File ► Open ► Saved Message.

OPEN Accounts Accounts OPEN IUNDERBIRD	Home			۲ ا		; (
AUNDERBIRD MAIL CLIENT MAIL CLIENT MAIL CLIENT Create a new account: Email C that C Newsgroups Feeds Create a new calendar Create a			Seerch <ctri+k></ctri+k>	New Message Attachments Edit $P$ is in a	Activity Man Message Filt	ager
	THUNDERBIRD EMAIL CLIENT	Create a new account:	MESSAGE" WI	Close Cut+W Close Cut+W Get New Mesages Send Ursent Mesages Send Ursent Mesages Delete Folder Delete Folder Rename Folder. F2 Compact Folders	File View Go Message Events and T Tools	asks

Figure 11-4: Thunderbird Mail Opening a Saved Message

Navigate within the folder containing the "Emails.pdf" Extraction Report, select the file name you are interested in inspecting. Click OK when you are done:

.../email/hryanwuphf@gmail.com/Inbox/mes-7.eml/

Thu	nderbird						29 Sun • 0 Apr 2018 CW
Ac	counts						✓ Today > Tomorrow
-	Create a new a				~	×	> Upcoming (5 days)
	← → × /	↑ 🧵 · My Reports > Samsur	ig.2018-04-26.11-13-49 ≥ em	ail > hryanwuphf@gn	nail.com > Inbox 🔫	- → O Search Inbox	
	Organize -	New folder					
ULLC .	organize						
	# Quic	Name	Date modified	Туре	Size		
		2 mes-2.eml	4/26/2018 11:15 AM	E-mail Message	13 KB		
		2 mes-3.eml	4/26/2018 11:15 AM	E-mail Message	23 KB		
		2 mes-4.eml	4/26/2018 11:15 AM	E-mail Message	7 KB		
	<u>ik</u> #	2 mes-5.eml	4/26/2018 11:15 AM	E-mail Message	23 KB		
	1 A	🔄 mes-6.eml	4/26/2018 11:15 AM	E-mail Message	69 KB		
	1.1	🔄 mes-7.eml	4/26/2018 11:15 AM	E-mail Message	19 KB		
	2.1	ames-8.eml	4/26/2018 11:15 AM	E-mail Message	55 KB		
	1 1	mes-9.eml	4/26/2018 11:15 AM	E-mail Message	5 KB		
	Tra	🛂 mes-10.eml	4/26/2018 11:15 AM	E-mail Message	50 KB		
		a mes-11.eml	4/26/2018 11:15 AM	E-mail Message	53 KB		
	Cone One	a mes-12.eml	4/26/2018 11:15 AM	E-mail Message	57 KB		
	🕒 This 🖉	a mes-13.eml	4/26/2018 11:15 AM	E-mail Message	19 KB		
	· · · · ·	2 mes-14.eml	4/26/2018 11:15 AM	E-mail Message	20 KB	×	
		File name: mes-7.eml				<ul> <li>Mail Files (*.eml)</li> </ul>	
		rite name. mes-ritemi					
						Open Cancel	

Figure 11-5: Select the Saved Message of Interest in Thunderbird Mail

System Administrator or Internet Service Provider. WIND Select the type of account you would like to set up:	🗵 🗹 — 🗇 🔿
Account Wigard       X         Mex Account Stup       In order to receive messages, you first need to set up an account.         This Wigard will collect the information necessary to set up an account.       In order to receive messages, you first need to set up an account.         Type do not know the information necessary to set up an account.       System Administrator or Internet Service Provider.         System Administrator or Internet Service Provider.       Select the type of account you would like to set up:         More Wolf       X         If you cail, any information you have entered will be lost and the account will not be created.       Exit         Exit       Cancel	P  ≡ Events  ▲ ►
There have a second sec	EESSAGE W WILL PEAR

You will see a new message window appear, however the tool will request that you login to your email account. To by-pass this, click the Cancel button and then the Exit button in the additional pop-up.

Figure 11-6: By-Pass Logging into Email Account in Thunderbird

The email message you chose to open will display in the message window with From, Subject, To, and the timestamp in the information bar above the email contents. Below the information bar, you can examine the contents of the selected email as viewed on the device.

In this chosen email, you will notice Ryan was utilizing fake personal information for his eBay account: "Steve Jones techie6739@gmail.com." Therefore, this email file should be tagged as "Evidence" and "Important" as it confirms the previous information found within his personal files and notes.

🕥 Mozilla Thunderbird		– 🗆 ×		17	10 - 0 ×
<u>File Edit View Go M</u> essage <u>T</u> ools <u>H</u> elp			15	= م	Events
🖞 Get Messages 🔻 🖿 Write 🔎 Chat 👤 Address Book 🛛 📎 Tag 👻		≡			29 Sun ( 0 ) .
From Steve Jones <techie6739@gmail.com>☆</techie6739@gmail.com>	↔ Reply ↔ Reply 🕏 Followup	→ Forward More			29 Apr 2018 CW 18
Subject Fwd: Congratulations, your item sold!		4/3/2018 12:38 PM			New Event
To hryanwuphf@gmail.com ப					√ Today
From: eBay <ebay com="" webay=""> Date: Tue, Apr 3, 2018 at 12:38 PM Subject: Congratulations, your term solid To: Invanwub/If@cmail.com Dear gamercandy, You did If Your item sol. Please ship this item to the buyer. You did If Your item and . Please ship this item to the buyer. You did If Your item and . Please ship this item to the buyer. You did If Your item and . Please ship this item to the buyer. You did If Your item and . Please ship this item to the buyer of physics and the shipping label. Complete one of the following: Provide shipping and Inaking in this hipping label. Provide shipping and Inaking in this item to the buyer. Provide shipping and inaking in this item to the buyer of the shipping and Inaking information. Who we have the Bay your tracking information is upoaded automation. Provide shipping and Inaking information. Who save you time, and may result in fewer questions for buyers and hipping label and hipping labels on the limit is no is year. Mark your item as a thoged in My eBay. Do this, as we life item to note the tem is on its way. This save you time, and may result in fewer questions for buyers and hipping labels in a things.</ebay>	Provide shipping information fler lice, ne on ally. you aff a d d		THE EMAIL WILL APPEAR AS EXTRACTED FROM THE DEVICE		) Tanorow ) Upcoming (5 days)
(%)			1		🔄 Today Pane 🗸

Figure 11-7: Email Message 7 From Inbox Displaying eBay Fake Information

### **Internet History**

To view the Web History stored in the device, navigate to:

/Analyzed Data/Web History/

Reader File View Tools I	Report H						All Projects	٥
2	Weld	ome ×	O Extraction Summary (1)	× 🧶 Web History (196) ×				
Samsung CDMA_SM-J320VPP Galaxy	0	Web Hi	istory (196)		APPEAR			
Extraction Summary (1)		100						
File Systems	85 VS	::: D	• 🐨 🗇 😻 🔲 Export •	×i	Table Search	Web Hist	ory	Go to
🖌 🕣 Analyzed Data		1 N	K ↓ Last Visited	<ul> <li>Title</li> </ul>	• URL	Title:	Google Calendar - Week of April 1, 2018	
> 🛃 Autofill (1)	1		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&		: 4/4/2018 11:37(UTC-7)	
> 🗱 Calendar (17) (4)	2					Visits: URL:	https://calendar.google.com/calendar/r?	
> 📞 Call Log (3)	2		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&		sf=true&output=xml	
>	3		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&	Source: Extraction:	Chrome Physical	
> 🕙 Cookies (368) (8)	4		4/4/2018 11:3 (UTC-7)	Google Calendar - Wheek of April 1, 2018	https://calendar.googn.com/calendar/r?sf=true&	Source file:		
Device Locations (10)	5		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
A Device Users (1)	6		4/4/2018 11:37(UTC-7)	WEBPAGE TITLE Google Calendar - Week of April 1, 2018	WEBPAGE URL https://calendar.google.com/calendar/r?sf=true&/			
> 🔀 Emails (17)	<u> </u>							
Installed Applications (248) (1)	<u> </u>		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
> 💬 MMS Messages (5) (1)	8		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
<ul> <li>Notes (2)</li> <li>Passwords (2)</li> </ul>	9		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
Passwords (2)  Powering Events (4)	10		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
> C Searched Items (71)	11		4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
> Q SMS Messages (34) (2)	12							
Q User Accounts (12)			4/4/2018 11:37(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
> (1) Web History (196) (1)	13		4/4/2018 11:36(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
<sup>14</sup> Wirkless Networks (1)	14		4/4/2018 11:36(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
	15		4/4/2018 11:36(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/r?sf=true&			
Carving	16		4/4/2018 11:36(UTC-7)	Google Calendar - Week of April 1, 2018	https://calendar.google.com/calendar/i?sf=true&	~		

Figure 11-8: Web History Includes Webpages Visited with the Title and URL

Double click on the URL of interest under Web History. Right click and select Copy.

**Note:** Double clicking cells within tabs of Analyzed Data will allow you to copy the contained information.

	Welcome × O Extractio	n Summary (1) 🛛 🧶 Web History (	196) ×			
Samsung CDMA_SM-J320VPP Galax	0 Web History (196	)				
房 Extraction Summary (1) 📄 File Systems	₩#ED• ®®®	Export • 📈	Table Search	Q Web His	story	Go to
🕣 Analyzed Data	$\prec$ $\downarrow$ Last Visited $\bullet$	Title 👻	URL -	Title:	10-TOP-EBAY-CONS-A-GUIDE-TO-COMMO	N-
> 🛃 Autofill (1)	4/2/2018 11:30(UTC-7)	Protecting Your Privacy on eBay	http://www.dummies.com/business/online-business/ebay/protectin.	A Last Visite	FRAUDS-ON-EBAY- ed: 4/2/2018 11:17(UTC-7)	
> 🛗 Calendar (17) (4)	4/2/2018 11:30(UTC-7)	protecting privacy on ebay - Google Search	https://www.google.com/search?g=protecting+privacy+on+ebay8	Visits:		
> 📞 Call Log (3) > (A) Contacts (21) (11)	4/2/2018 11:17(UTC-7)	10-TOP-EBAY-CONS-A-GUIDE-TO-COMMO	HIDE-TO-COMMON-FRAUDS-ON-FRAY-/1000000002145432/g htm	URL:	https://www.ebay.com/gds/10-TOP-EBAY-C GUIDE-TO-COMMON-FRAUDS-ON-	ONS-A-
> 🛞 Contacts (21) (11)	4/2/2018 11:17(UTC-7)	Cut Ctrl+X		Source:	EBAY-/1000000002145432/g.html Chrome	
>   Device Locations (10)			DOUDLE CLICK	Extraction		
A Device Users (1)	4/2/2018 11:14(UTC-7)	Scaling committee 0		Source file	e:	
> 🖂 Emails (17)	4/2/2018 11:14(UTC-7)	SCAMS committed by eBay Sellers - The eB	https://auth.ebay.com/oauth2/authorize?client_id=LithiumT-7567-4.			
Installed Applications (248) (1)	4/2/2018 11:14(UTC-7)	SCAMS committed by eBay Sellers - The eB	https://community.ebay.com/plugins/common/feature/oauth2sso/s.			
> 💬 MMS Messages (5) (1)	4/2/2018 11:14(UTC-7)	SCAMS committed by eBay Sellers - The eB	https://community.ebay.com/t5/The-Front-Porch/SCAMS-committe.			
> 📑 Notes (2)	4/2/2018 11:14(UTC-7)	SCAMS committed by eBay Sellers - The eB	https://community.ebay.com/t5/The-Front-Porch/SCAMS-committe.			
Passwords (2)     Powering Events (4)	4/2/2018 11:13(UTC-7)	scams on ebay - Google Search	https://www.google.com/search?q=scams+on+ebay&oq=scams+o.			
> C Searched Items (71)	4/2/2018 11:12(UTC-7)	Google	https://www.google.com/?gws_rd=ssl			
> Q SMS Messages (34) (2)			https://calendar.google.com/calendar/r/eventedit?text=Your+Geek+			
은 User Accounts (12)	1		https://accounts.google.com/signin/oauth/consent?authuser=0&pa.			
> 🍈 Web History (196) (1)	1		https://the-gamers-edge-inc.myshopify.com/collections/microsoft-x.			
Wireless Networks (1)	SCROLL!	2. 2		1		
B Data Files		Google	https://www.google.com/?gws_rd=ssl			

Figure 11-9: Double Click on the URL to Copy the Visited Webpage

Paste the webpage URL you copied into a browser such as Google Chrome or Internet Explorer.

In this case, you will see a webpage regarding eBay frauds which directly relates to the accusations against Ryan. As you examine the Web History, remember to tag files as "Evidence," "Important," and "Further Investigation" as necessary.

10-TOP-EBAY-CONS-A-G ×						Gent – a ×
← → C ≜ Secure https://www.	bay.com/gds/10-TOP-EBAY-CONS-A-	GUIDE-TO-COMMON-FRAUDS	-ON-EBAY-/1000000002145432/g	html		:
/	Hi! Sign in or register   Daily Deals	Sift Cards   Help & Contact	List. Sell. Get Paid.	Sell   MyeBay	<b>♦</b> /Ħ	
PASTE COPIED URL	EDAV Shop by -	Search for anything		All Categories - Searc	Advanced	
,	Home + Buying Guides + Everything I	Else + Every Other Thing +				
(	10 TOP F	RAY CONS	S A GUID	E TO COMM		
		FRAC	JDS ON EB.	AY		
	vintageneil		30,859 Likes		Like	
	August 10, 2017					
	This is a guide to dishonest eBaye nonsense, adver based eBayers, i sell you anything bottom of this pa each one you rea	( y to at the				
	shill bidding In eBay's own words, "Sl	nill bidding is bidding	that artificially increase	s an item's price or apparent		

Figure 11-10: Paste the Copied Webpage URL into a Browser to View

To view the Searched Items stored in the device, navigate to:

Reader File View Tools Report Help										All Projects			
	Welco	me ×	О Е	xtraction Summary (1) $\times$	• O Web History (196) ×	Searche	d Ite	ems (71) ×					
Samsung CDMA_SM-J320VPP Galaxy		Search	ed Ite	ems (71)			1		L APPEAR				
Extraction Summary (1)	🎬 語 🏗 🗅 • 🕲 🤍 💖 🔲 Export • 📈						Гт	Table Search	٩	Searched Item Go to			
File Systems										Searcheum	1011 0010		
Analyzed Data	<b>1</b> ↑ #	S	× ^	Timestamp •	Value	Position	•	Map Address 🔻	Source	Timestamp: Source: Value:	4/5/2018 11:02(UTC-7)		
> 柔 Autofill (1) > 關 Calendar (17) (4)	1			4/5/2018 11:02(UTC-7)	255 MADONNA RD SAN LUIS OBI				Gmail		Gmail 255 MADONNA RD SAN LUIS OBISPO CA		
> Ego Calendar (17) (4)	2			4/4/2018 12:01(UTC-7)	255 MADONNA RD SAN LUIS OBI				Gmail	Search Result	s:		
> @ Contacts (21) (11)	3			4/4/2018 11:51(UTC-7)	Best Buy				Google Maps	Extraction:	Physical		
> 🚯 Cookies (368) (8)	4			4/4/2018 1 +9(UTC-7)	Chipotle Mexican rill				Google Maps	Source file:			
>   Device Locations (10)	-												
A Device Users (1)	5			4/4/2018 11:43(UTC-7) TIMESTAMP	1179 Atascadero St. San Luis Obis VALUE					Map			
> 🖂 Emails (17)	6			4/4/2018 11:28(UTC-7)	255 MA				OF SEARCH	Position: Map Addres			
Installed Applications (248) (1)	7			4/4/2018 11:20(UTC-7)	geek squad slo				Chrome				
> 💬 MMS Messages (5) (1)	8			4/4/2018 11:19(UTC-7)	watch dogs xbox 360 printable co				Chrome				
> 🔛 Notes (2)	9			4/3/2018 11:49(UTC-7)	2145 Hamilton Avenue, San Jose				Gmail	Source			
m Passwords (2)	-									Snippet:	Go to		
O Powering Events (4)	10			4/3/2018 11:36(UTC-7)	2145 Hamilton Avenue, San Jose,				Gmail		hryanwuphf@gmail.com		
Searched Items (71)	11			4/3/2018 11:06(UTC-7)	watch dogs xbox 360 printable co				Chrome		View: Mobile   Web Hi Ryan, Just a reminder, y		
> O SM5 Messages (34) (2)	12			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co				Chrome		have an upcoming Geek Squad ® Inbox,		
DOUBLE CLICK	13			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co				Chrome		Reminder: You're close to tech bliss		
> (()) Web History (196) (1)	14			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co				Chrome	Timestamp: Priority:	4/5/2018 11:02(UTC-7)		
Y Wireless Networks (1)	15			4/3/2018 11:05(UTC-7)					Chrome		Gmail		
S Data Files -					watch dogs xbox 360 printable co						Unread		
Carving	< 16			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co				Chrome >	Extraction: Source file:	Physical		

/Analyzed Data/Searched Items/

Figure 11-11: Items Searched within Applications are Stored

To sort the Searched Items by the location of the search, you have two options:

- 1. Click the Source column title and then check the locations you want to view in the pop-up menu.
- 2. Expand the Searched Items selection within the Analyzed Data menu and double click the location you want to view.

Note: Option 1 is the best choice if you want to examine more than one location of searched items.

	Welco	ome ×	0 6	extraction Summary (1)	× O Web History (196) ×	Search	ned Ite	tems (71) ×						
Samsung CDMA_SM-J320VPP Galaxy	20VPP Galaxy 🗍 📵 Searched Items (71)													
Extraction Summary (1) File Systems	<b>**</b>	# D	• 3	🕀 河 😵 🔲 Export 🕶 🖌	<i>র</i>		1	Table Search	٩	Searched Item	Searched Item Go to			
Analyzed Data	†#	1	×ĸ	Timestamp •	Value 👻	Position	•	Map Address 🔻 Source		Timestamp:	4/5/2018 11:02(UTC-7)			
> 🛃 Autofill (1)	1			4/5/2018 11:02(UTC-7)	255 MADONNA RD SAN LUIS OBI			A ↓ Sort Ascending	≺		Gmail			
> 🛗 Calendar (17) (4)	2			4/4/2018 12:01(UTC-7)	255 MADONNA RD SAN LUIS OBL			Z Sort Descending	Ċ	LICK TO OP	255 MADONNA RD SAN LUIS (	OBISPO CA		
> 📞 Call Log (3)	-								-					
> (2) Contacts (21) (11)	3			4/4/2018 11:51(UTC-7)	Best Buy				51					
> 🚱 Cookies (368) (8)	4			4/4/2018 11:49(UTC-7)	Chipotle Mexican Grill			Select All		le:				
Device Locations (10)	5			4/4/2018 11:43(UTC-7)	1179 Atascadero St, San Luis Obis			Chrome		(55)				
A Device Users (1) > ⊠ Emails (17)	6			4/4/2018 11:28(UTC-7)	255 MADONNA RD SAN LUIS OBI			Google Maps		(9) (3) m:				
<ul> <li>Emails (17)</li> <li>Installed Applications (248) (1)</li> </ul>	7			4/4/2018 11:20(UTC-7)	geek squad slo			✓ Play Store		(4) ddress:				
> 💬 MMS Messages (5) (1)	8			4/4/2018 11:19(UTC-7)	watch dogs xbox 360 printable co					_				
> 📄 Notes (2)	9									OPTION 1	: CHECK WITHIN			
Passwords (2)				4/3/2018 11:49(UTC-7)	2145 Hamilton Avenue, San Jose,					SOR	TING MENU	Go to		
Overing Events (4)	10			4/3/2018 11:36(UTC-7)	2145 Hamilton Avenue, San Jose,			ок	Cano		hryanwuphf@gmail.com			
Searched Items (71)	11			4/3/2018 11:06(UTC-7)	watch dogs xbox 360 printable co				Cano	cel	View: Mobile   Web Hi Ryan, Ju			
Chrome (55)	12			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co			Chrome			reminder, you have an upcomi Squad ®	ng Geek		
Gmail (9)	13			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co			Chrome		Folder:	Inbox,			
Google Maps (3)	14			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co			Chrome		Subject: Timestamp:	Reminder: You're close to tech 4/5/2018 11:02(UTC-7)	DIISS		
Play Store (4)										Priority:				
> Ø SMS Messages (34) (2)	15			4/3/2018 11:05(UTC-7)	watch dogs xbox 360 printable co			Chrome		Source: Status:	Gmail Unread			

Figure 11-12: Two Options for Sorting Searched Items