CAL POLY

California Cybersecurity Institute

Windows and Android Forensics
CCIC Training

Chapter 0: Preamble

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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 https://cci.calpoly.edu/events/ccic/2019-df-downloads.

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

Android Forensics

1. QuickHash GUI
2. Google Map Creation
3. Thunderbird Mail

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

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 cci@calpoly.edu.

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 1: Introduction

Cassidy Elwell and James Poirier

April 2019 (Version 2)

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 www.cci.calpoly.edu), 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 off-eBay 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.

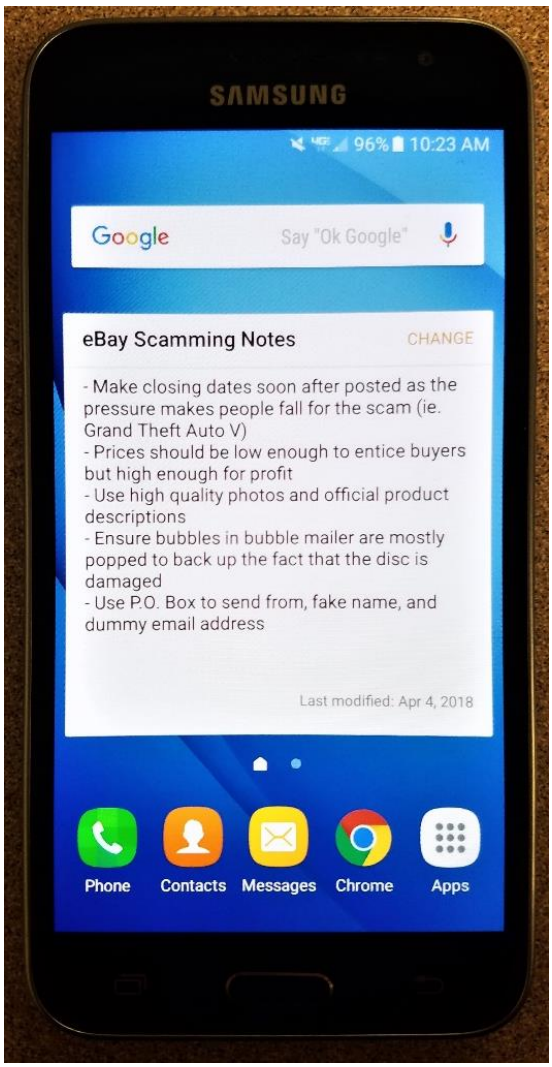
Since the discovery, eBay has continued to watch the suspect's seller account. Geek Squad has contacted the San Luis Obispo Police Department to arrest and prosecute Howard for theft.

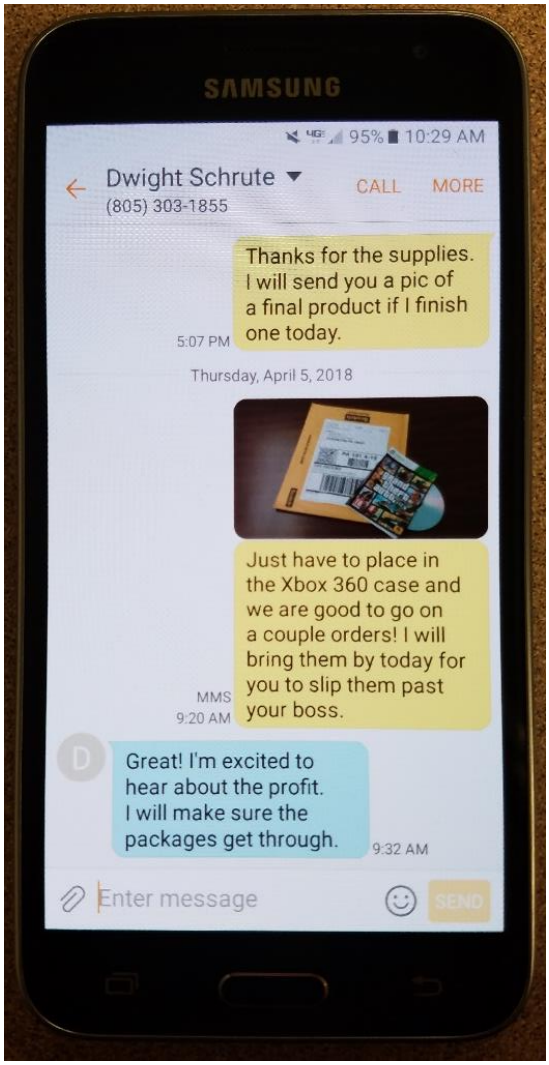
On April 5th, Ryan Howard was detained by Best Buy security as he attempted to pick up his mobile device from the Geek Squad Service's associate who had been solving a technical glitch Howard claimed to be having on his device.

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:





CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 2: Secure the Device

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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.

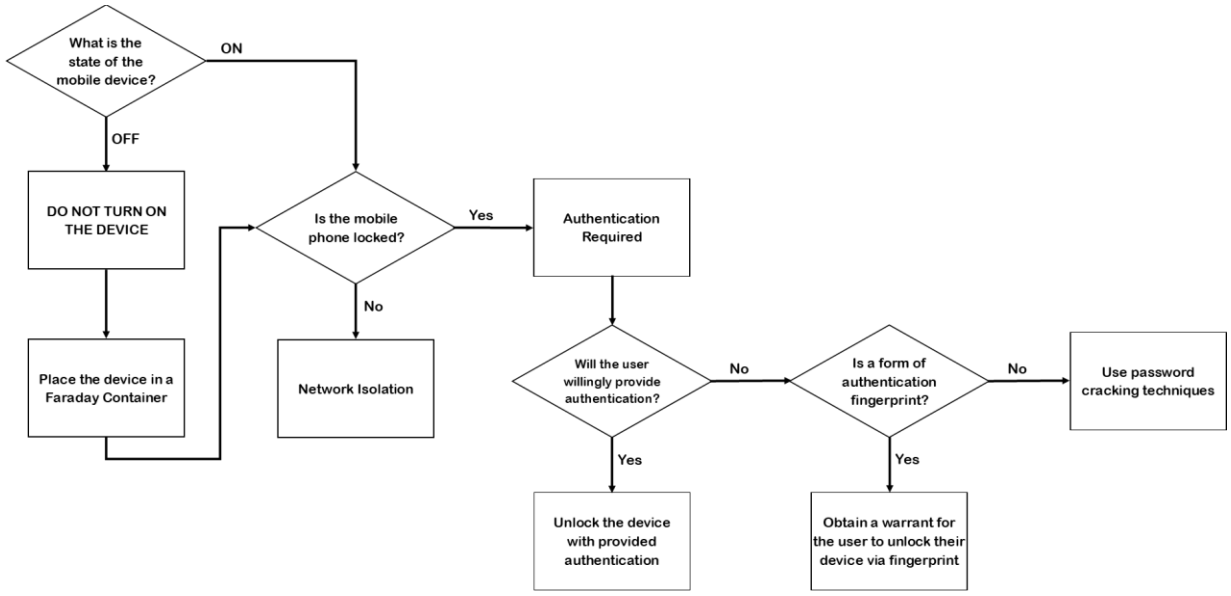


Figure 2-1: Properly Handling a Mobile Device Flowchart

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).

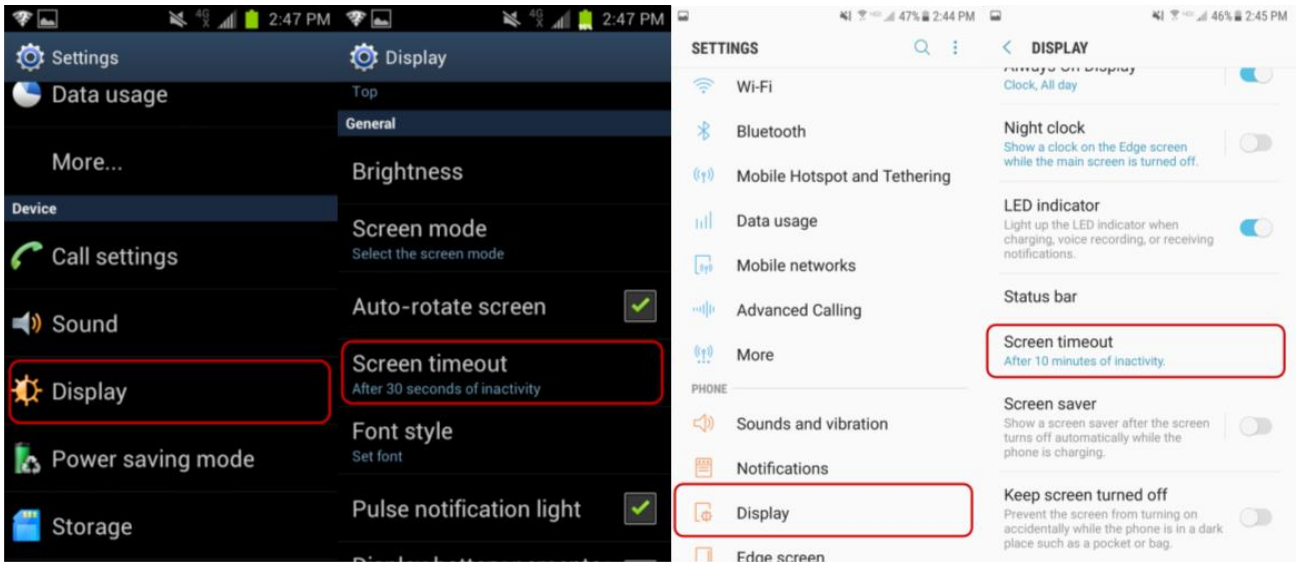


Figure 2-2: Version 4.2 (Jelly Bean) vs Version 7 (Nougat) "Screen timeout" within "Display"

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.

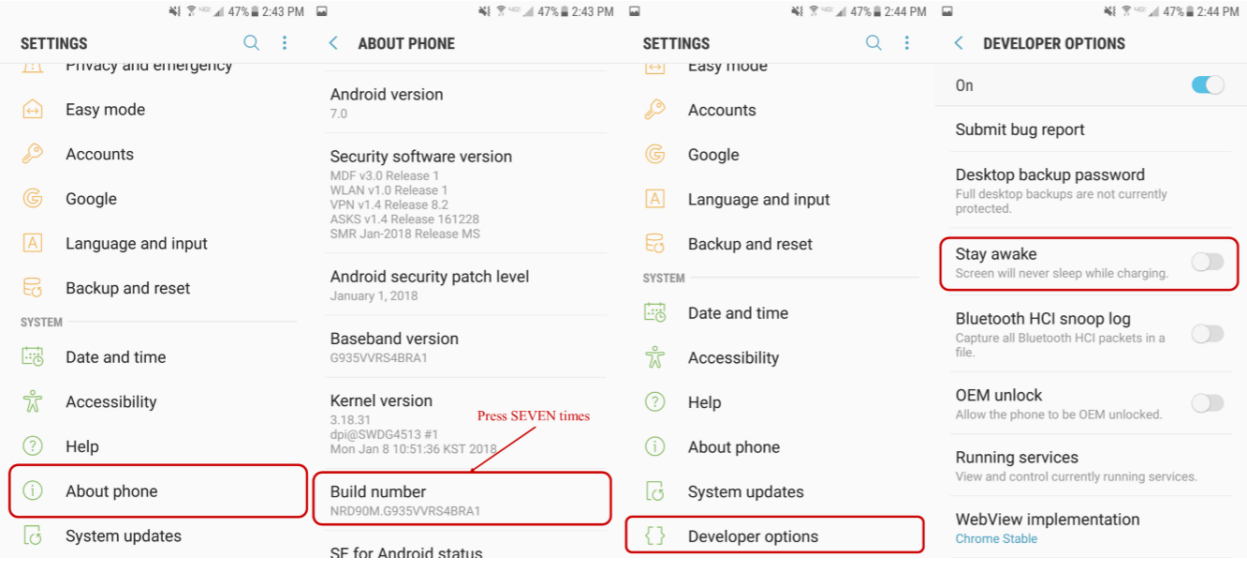


Figure 2-3: Version 7 (Nougat) “Stay awake” with “Developer options” Enabled

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."

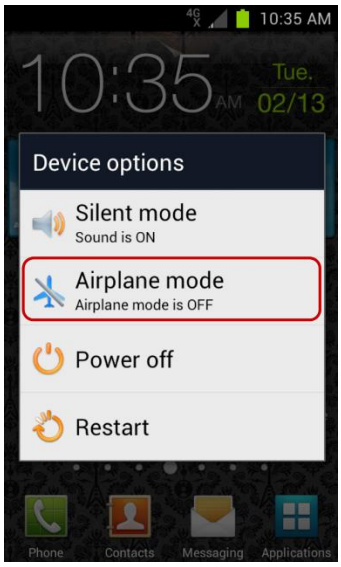


Figure 2-4: Version 4.2 (Jelly Bean) "Airplane mode" from Pop-Up Menu

- 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.

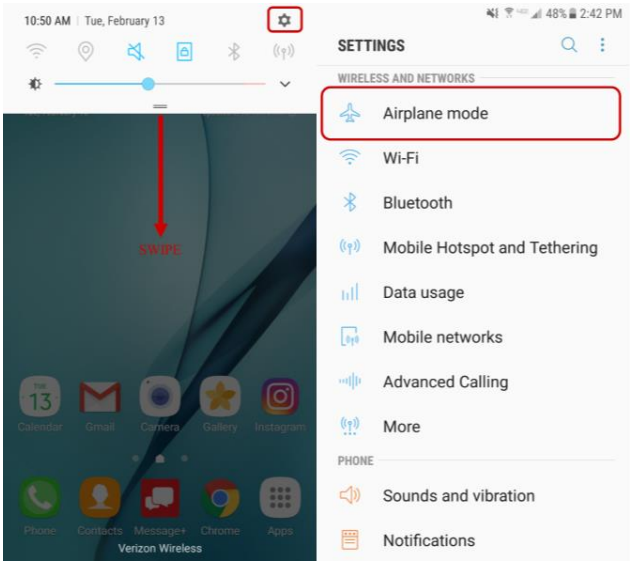


Figure 2-5: Version 7 (Nougat) “Airplane mode” from Swipe Menu

- 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.

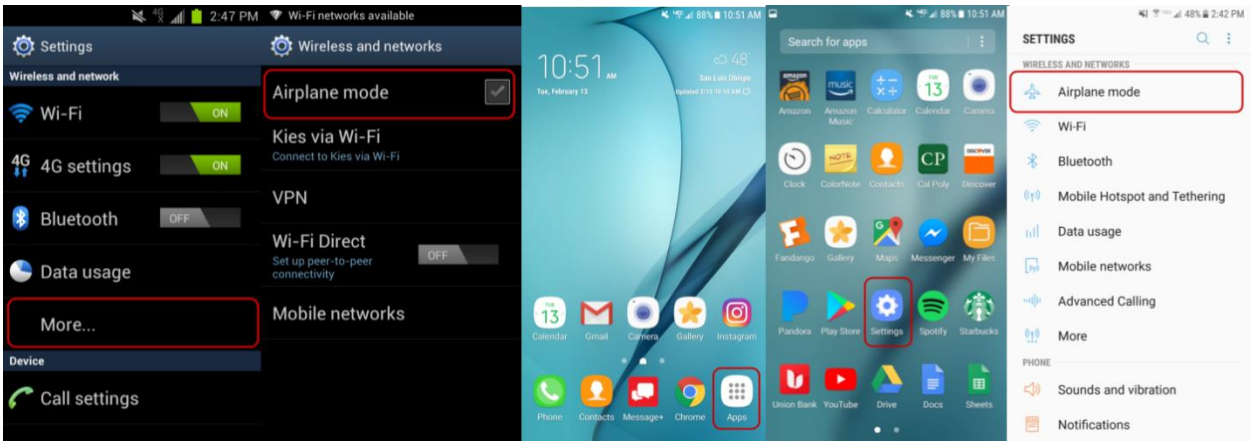


Figure 2-6: Version 4.2 (Jelly Bean) vs Version 7 (Nougat) “Airplane mode” from Settings

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

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

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

Cassidy Elwell and James Poirier

May 2019 (Version 2)

3

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.

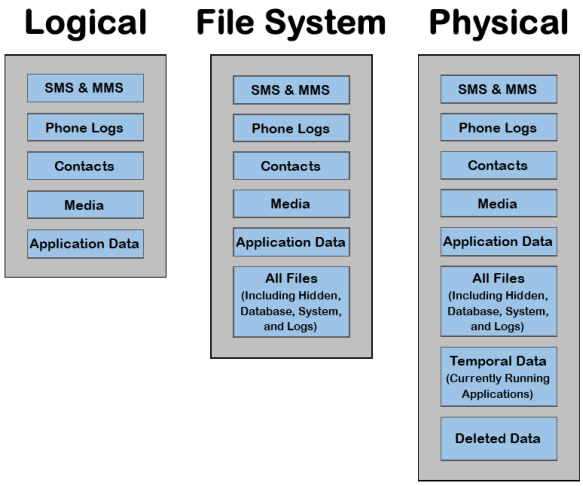


Figure 3-1: Logical vs File System vs Physical Extraction

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.

Figure 3-3: File System Extraction

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 "read-only" 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.

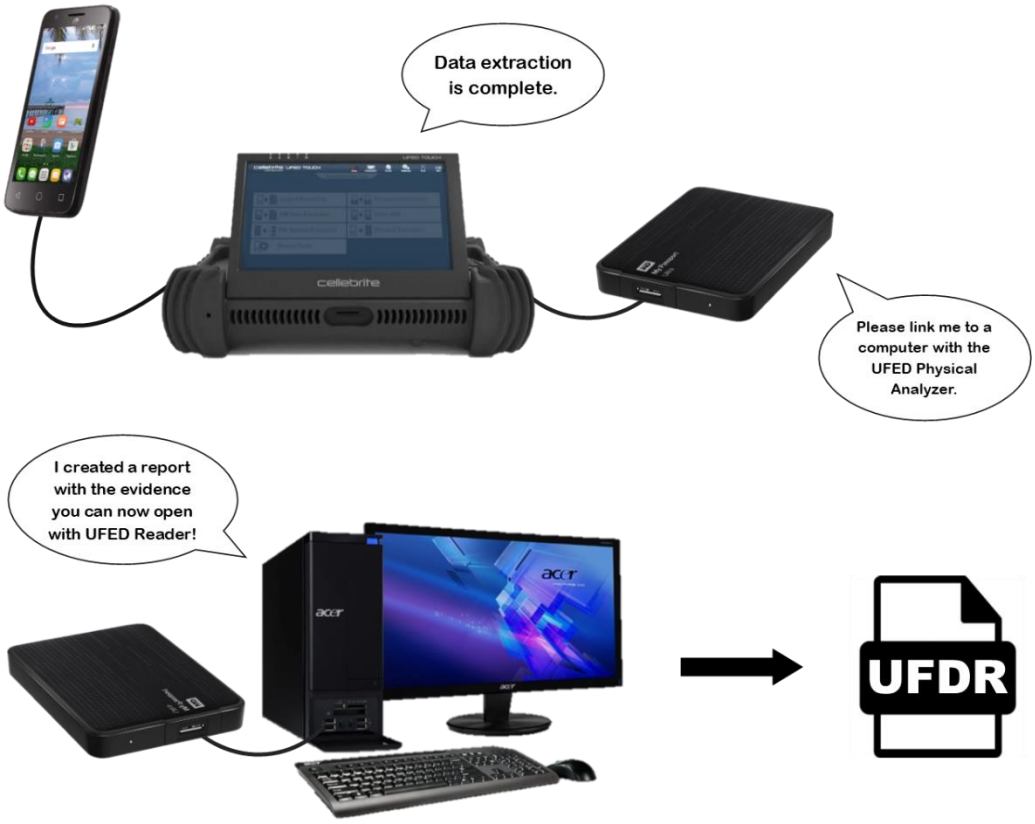


Figure 3-5: Use UFED Software Following Data Extraction

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 4: Verify the Forensics Image

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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.

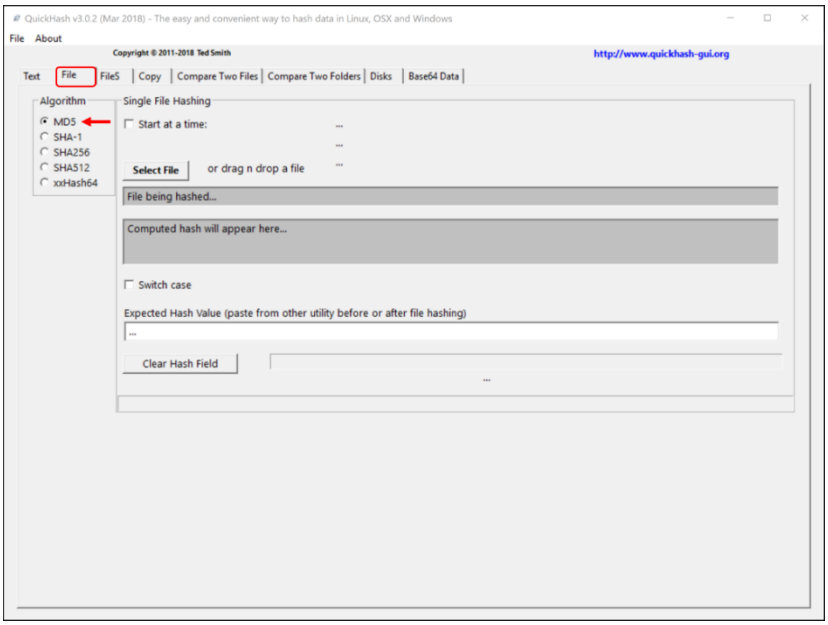


Figure 4-1: QuickHash GUI Single File MD5

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).

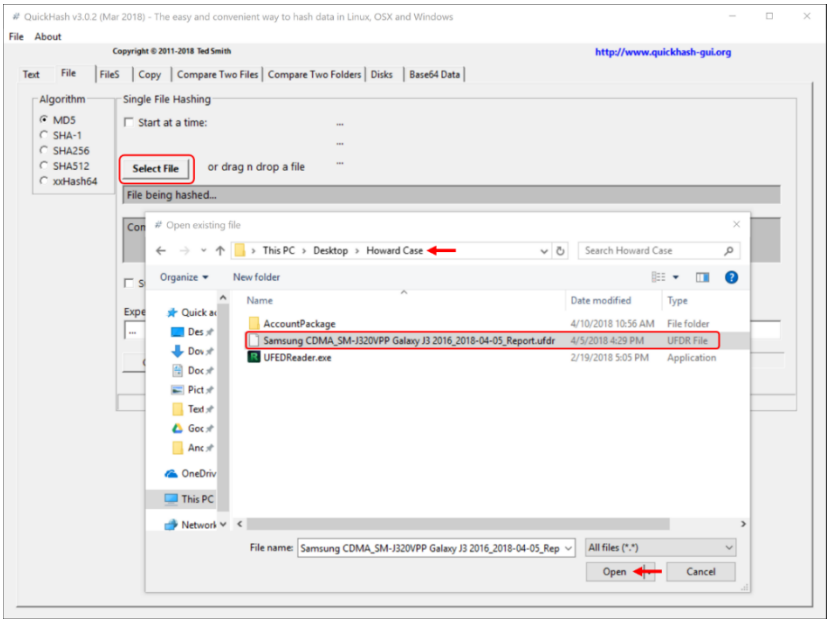


Figure 4-2: Select the .UFDR File for MD5 Hash Calculation

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

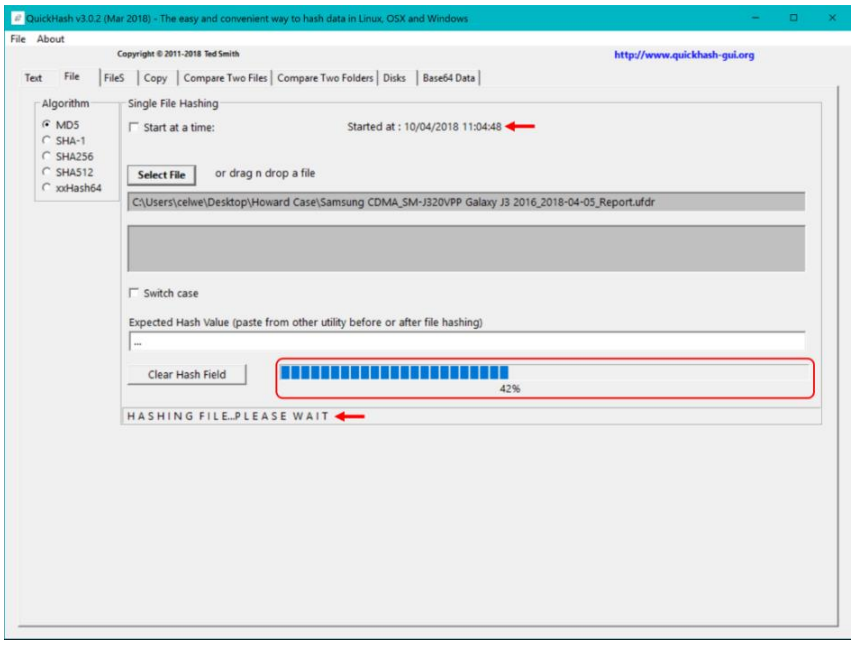


Figure 4-3: Hash Calculation Begins and the Timestamp is Displayed

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.

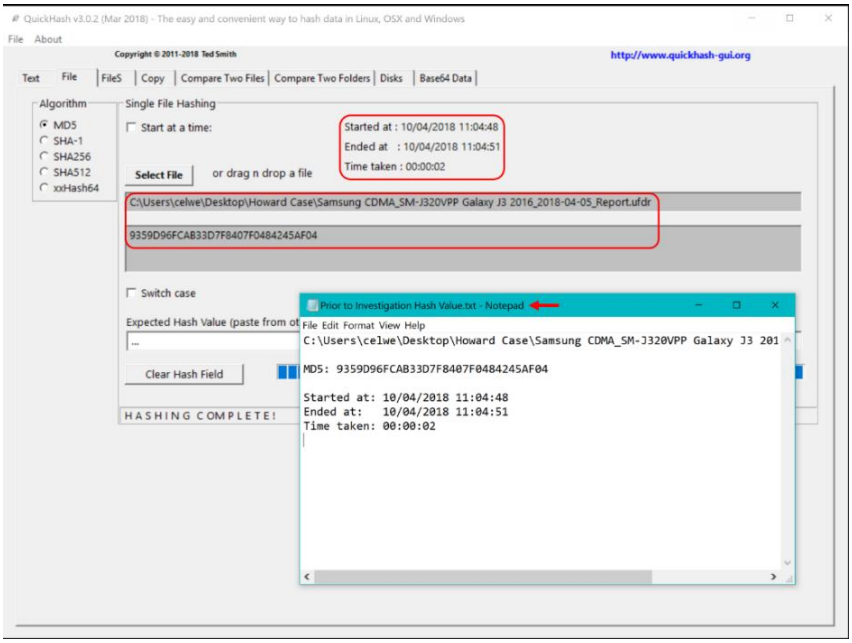


Figure 4-4: Record the MD5 Hash to be Verified Post-Investigation

Following Completion of Investigation

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

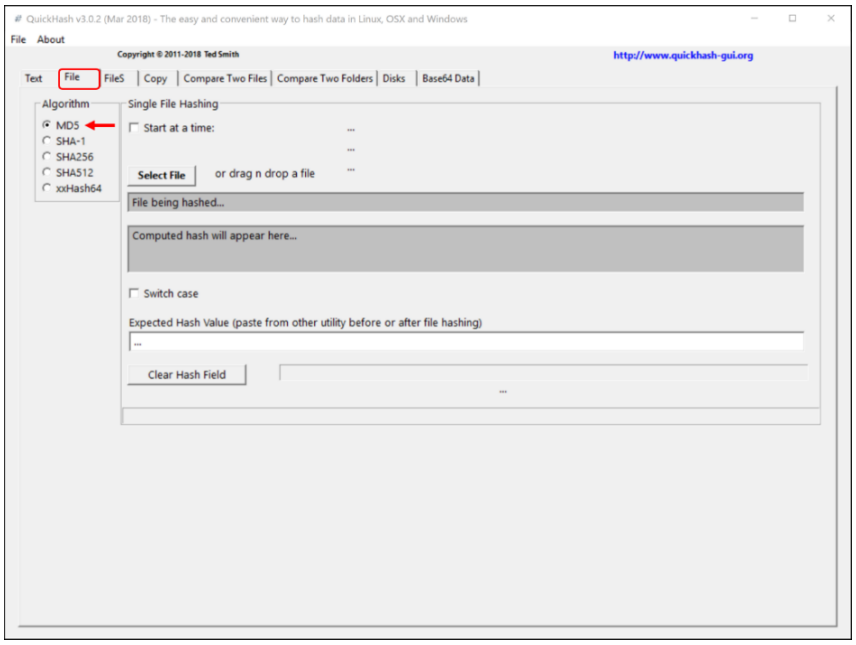


Figure 4-5: QuickHash GUI Single File MD5

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.

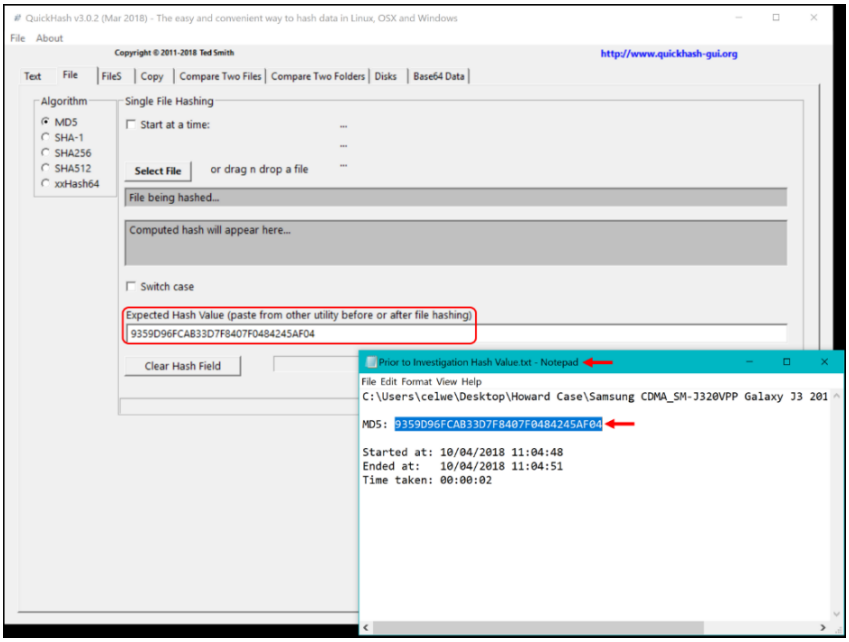


Figure 4-6: Place Recorded MD5 Hash from Pre-Investigation in the Expected Hash Value Box

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).

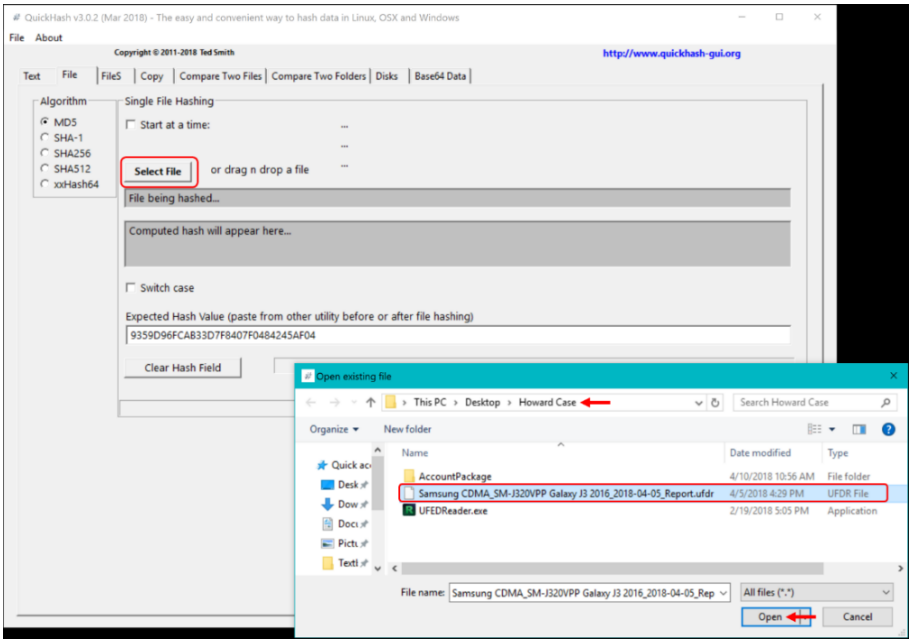


Figure 4-7: Select the .UFDR File for MD5 Hash Calculation and Comparison

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

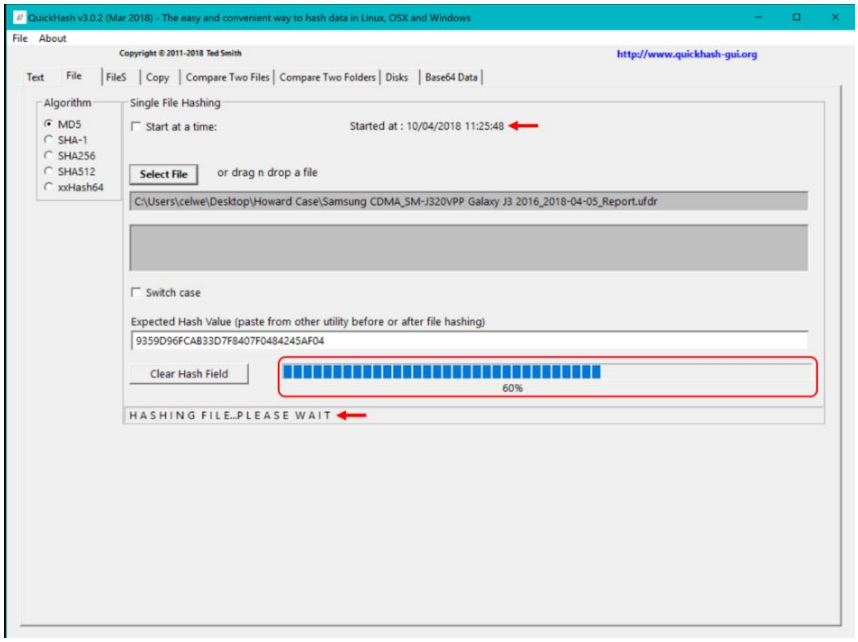


Figure 4-8: Hash Calculation Begins and the Timestamp is Displayed

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.

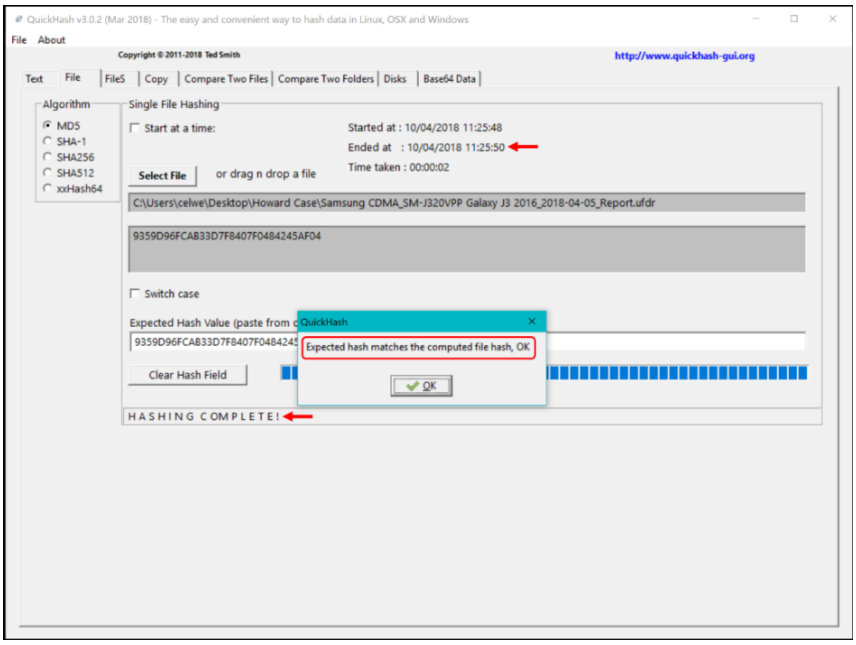


Figure 4-9: Hash Comparison is Complete and Pop-Up Window Indicates an Identical Match

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

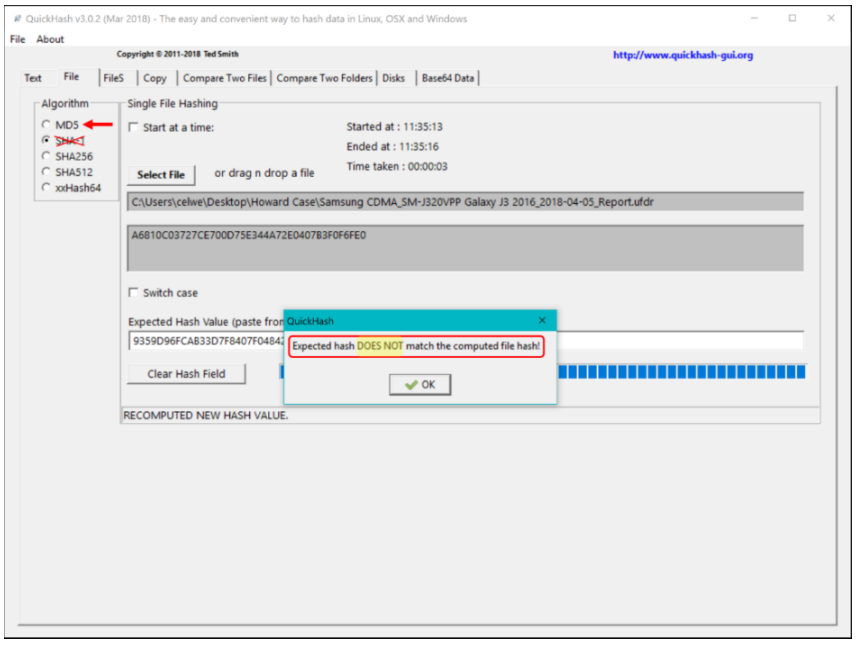


Figure 4-10: Check Selected Algorithm if Hash Comparison Indicates NOT Identical Match

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 5: UFED Reader Basics

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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").

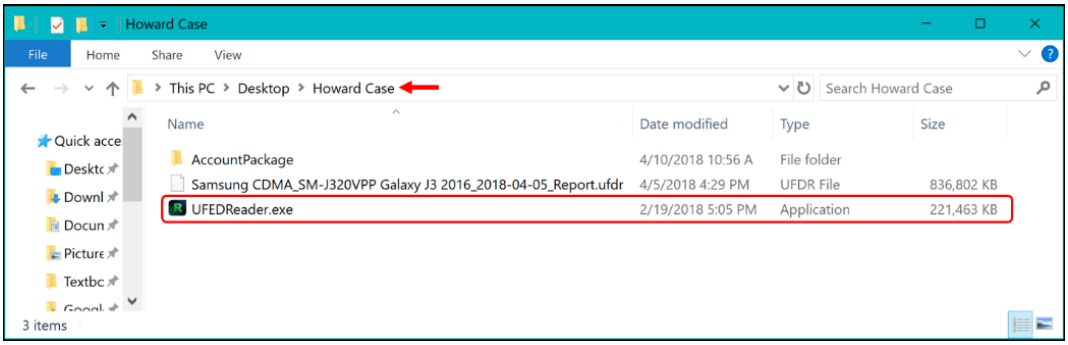


Figure 5-1: To View Evidence with UFED Reader, Double Click on the Executable File "UFEDReader"

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.

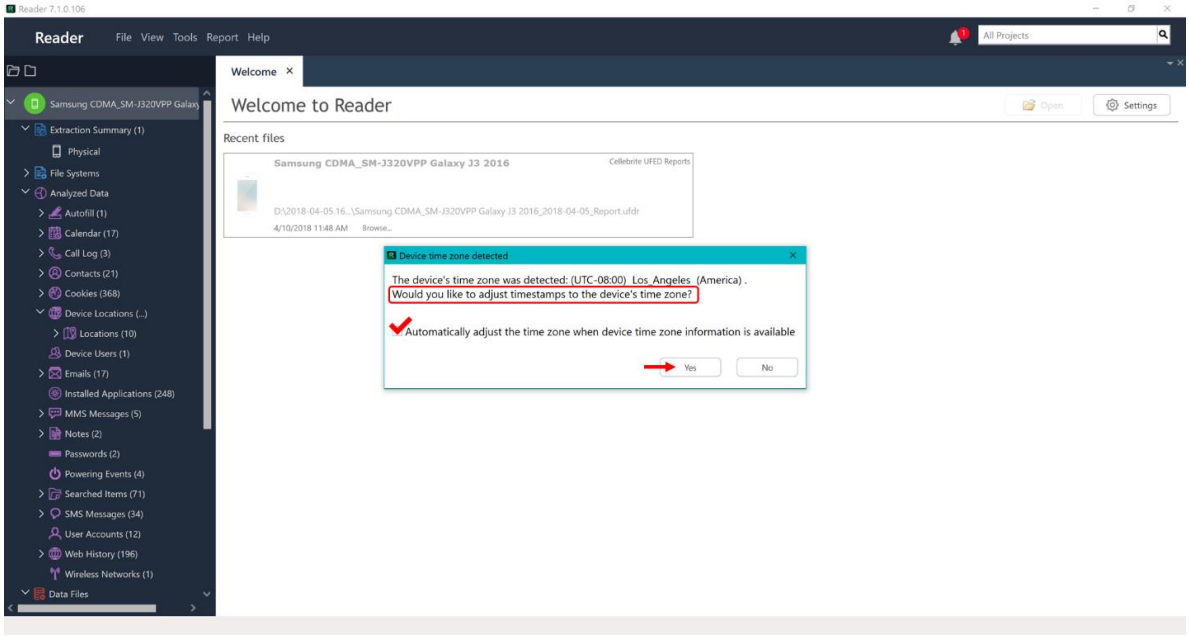


Figure 5-2: Check and Click Yes If You Are Asked About Using the Device's Time Zone

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.

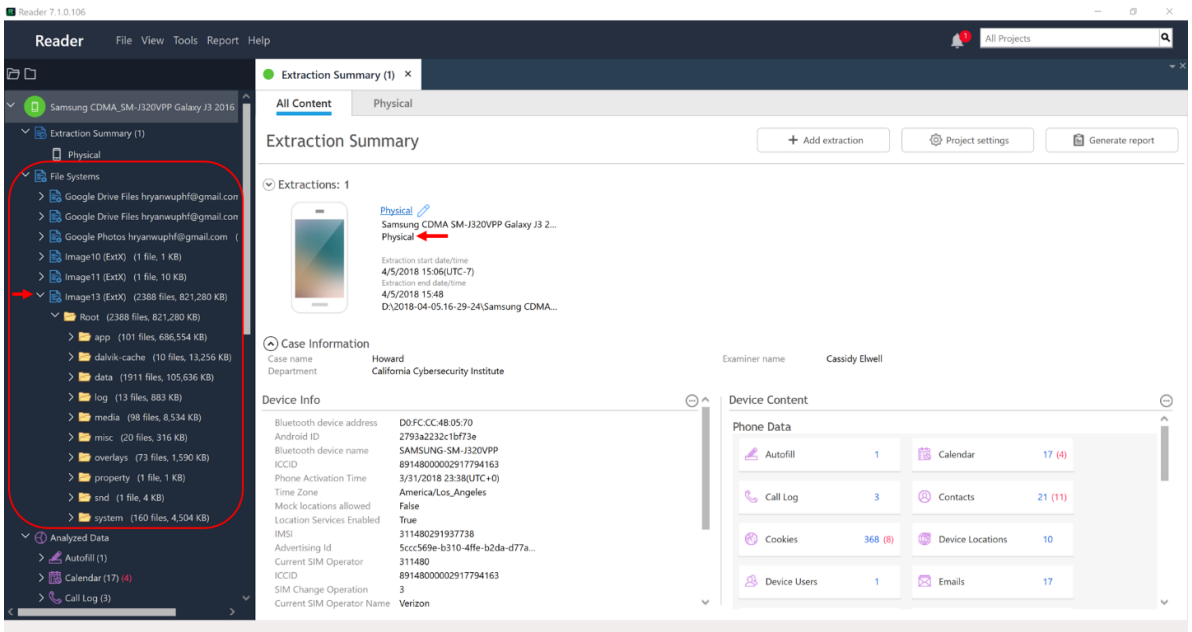


Figure 5-3: The File Systems Tab is an Exact Copy of the Device's Memory

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.

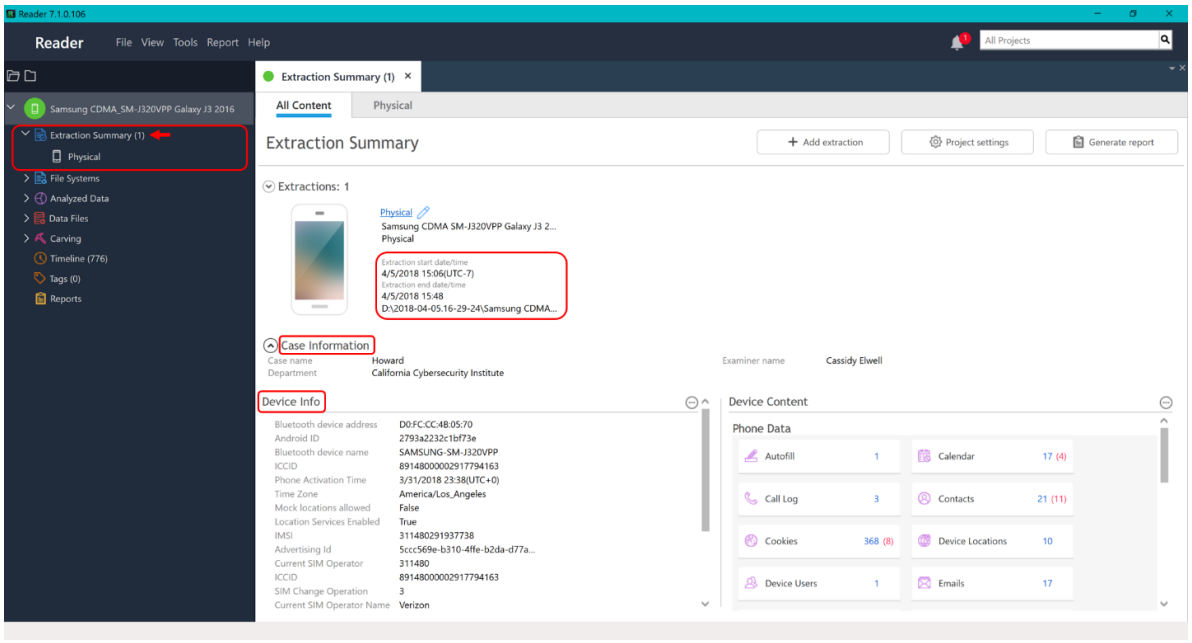


Figure 5-4: The Extraction Summary Tab is Useful for Information About the Device, Case, and Extraction Technique

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.

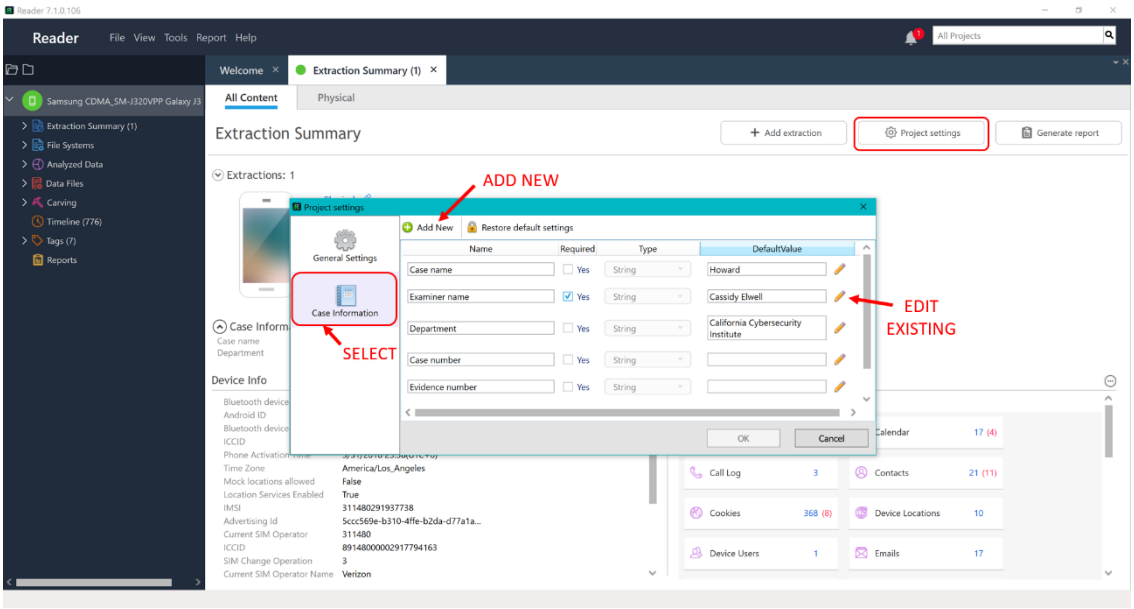


Figure 5-5: Project Settings Menu Allows for Editing of Case Information

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.

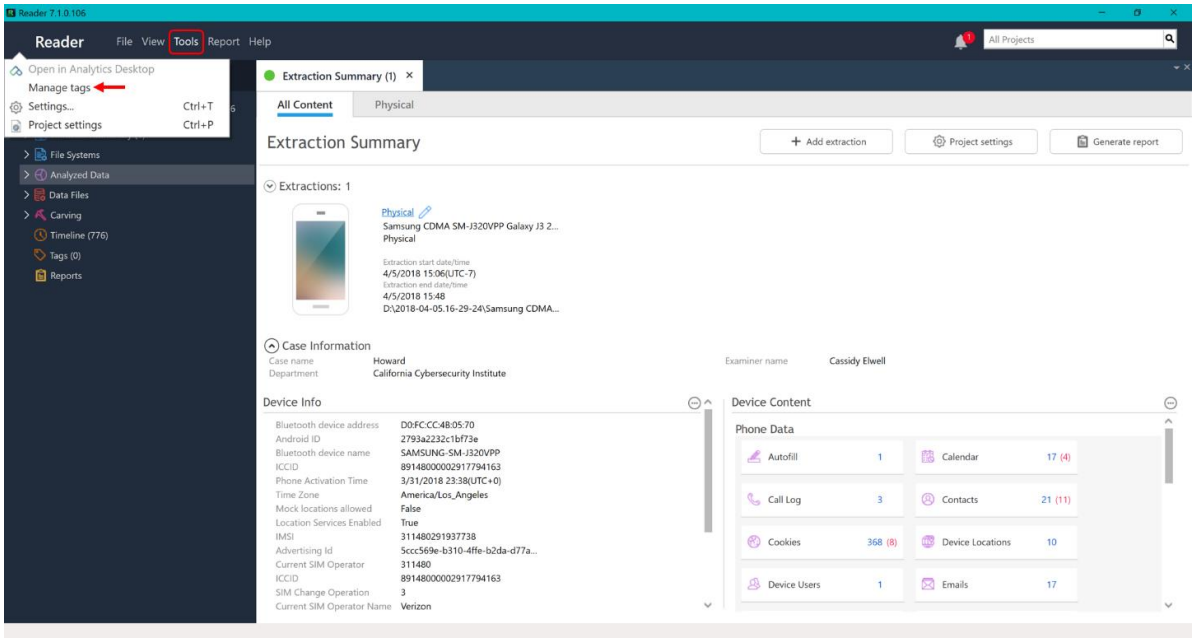


Figure 5-6: To Edit Tags for Investigation, Click Manage Tags in the Toolbar

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.

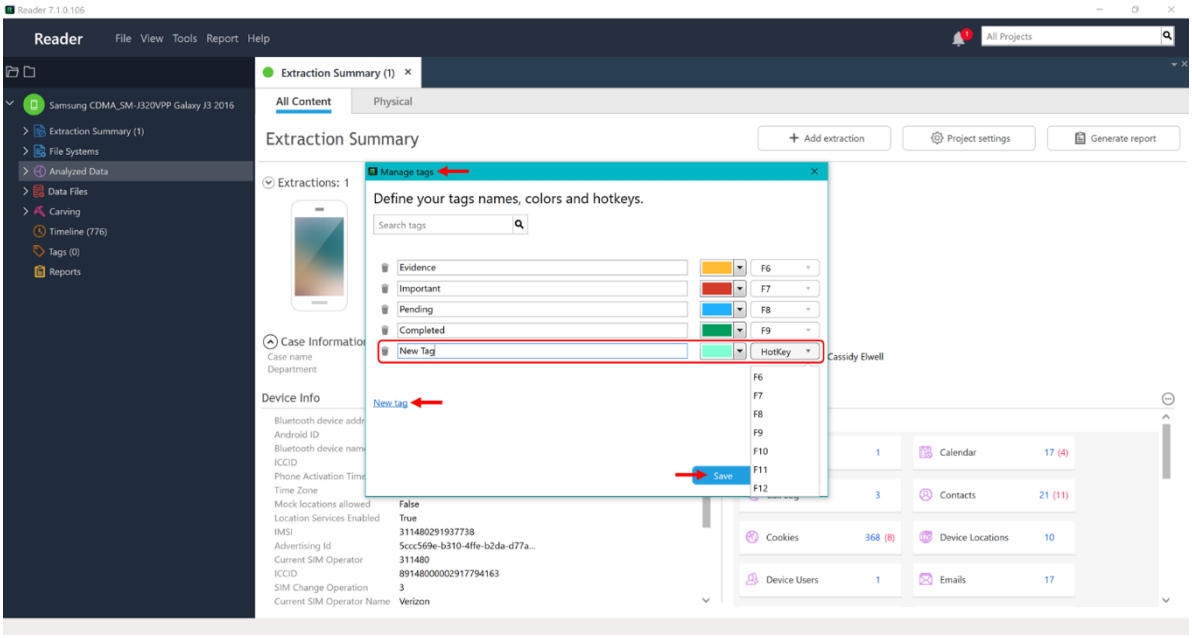


Figure 5-7: When Creating a Tag, Options Include Name, Color, and HotKey

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.

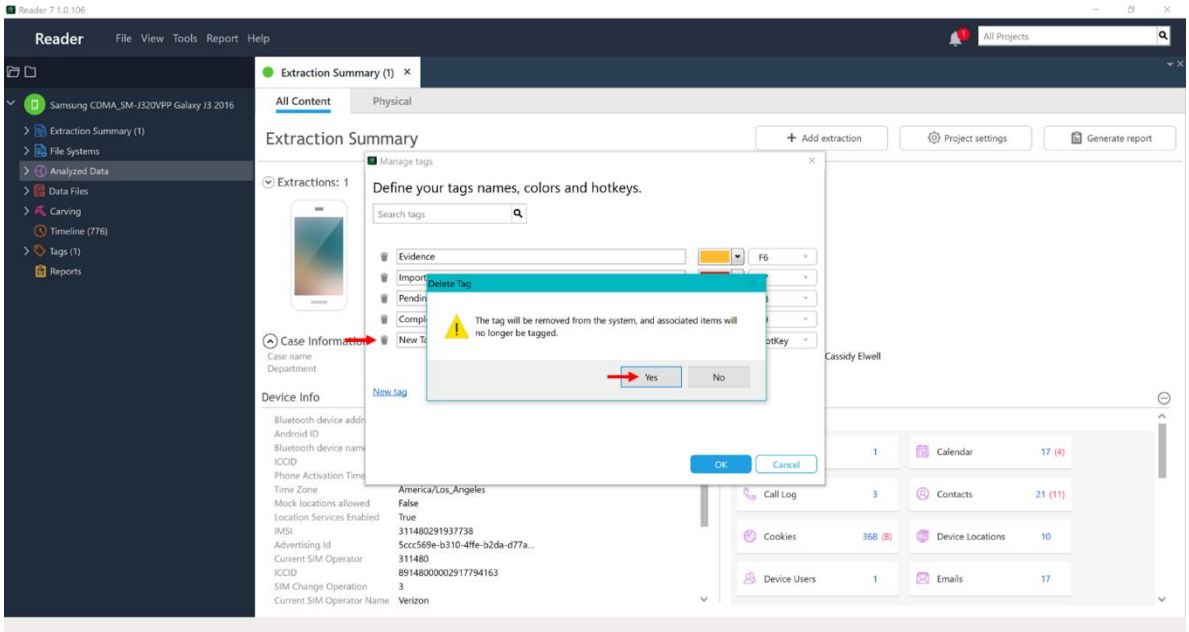


Figure 5-8: Delete a Tag By Simply Clicking the Trash Can Icon

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.

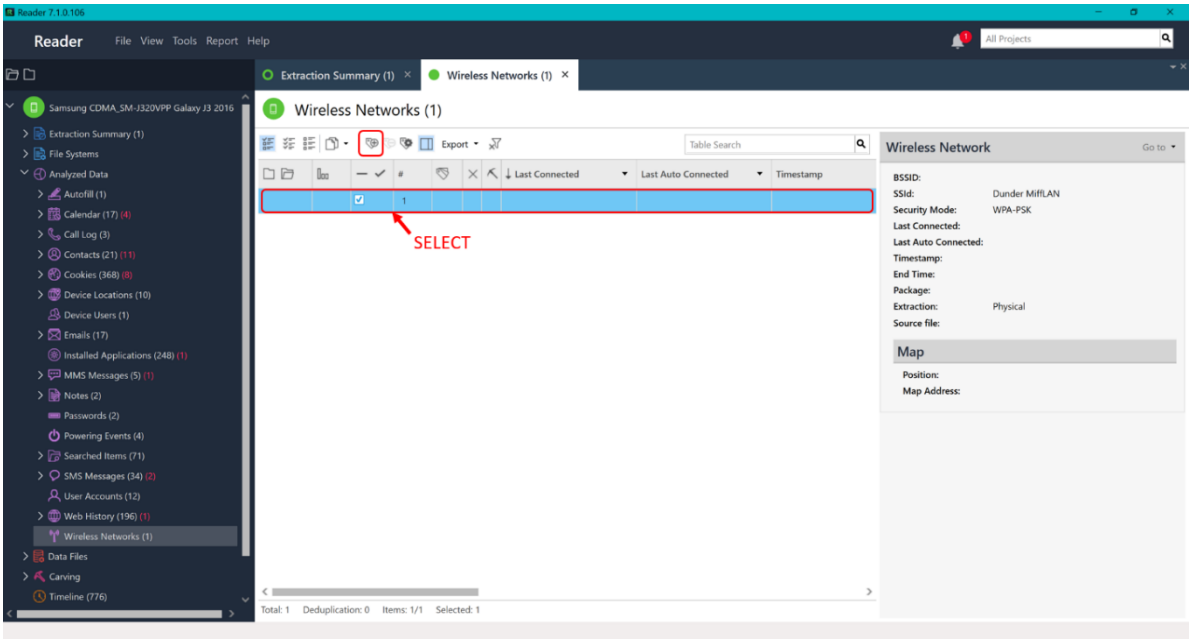


Figure 5-9: Begin By Selecting File(s) and Clicking the Plus Tag Button

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.

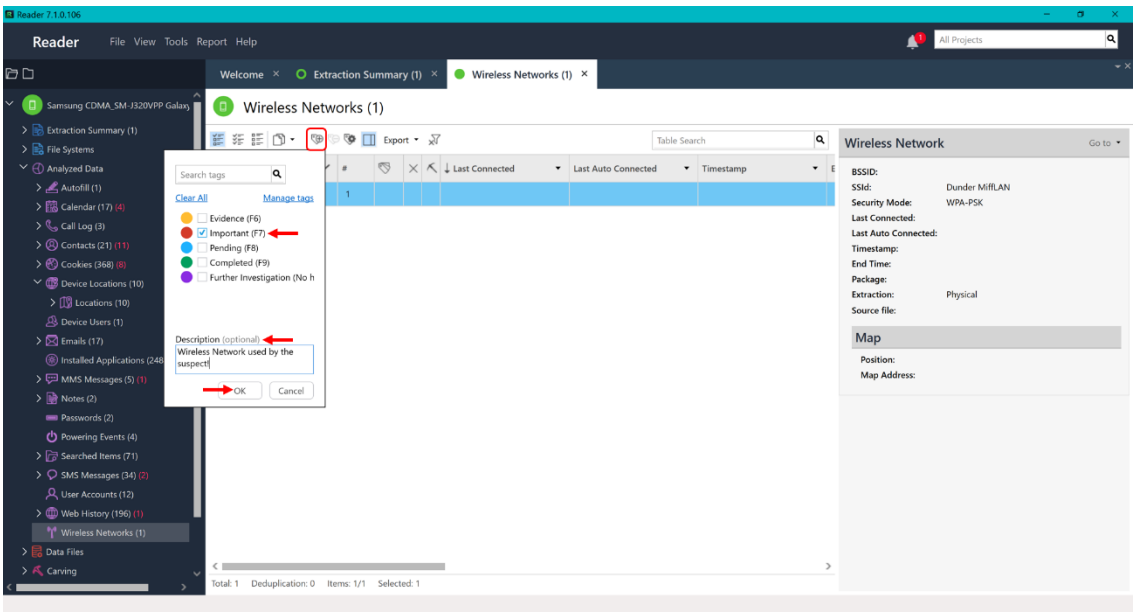


Figure 5-10: Select the Tag You Want to Use and Add an Optional Description

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.

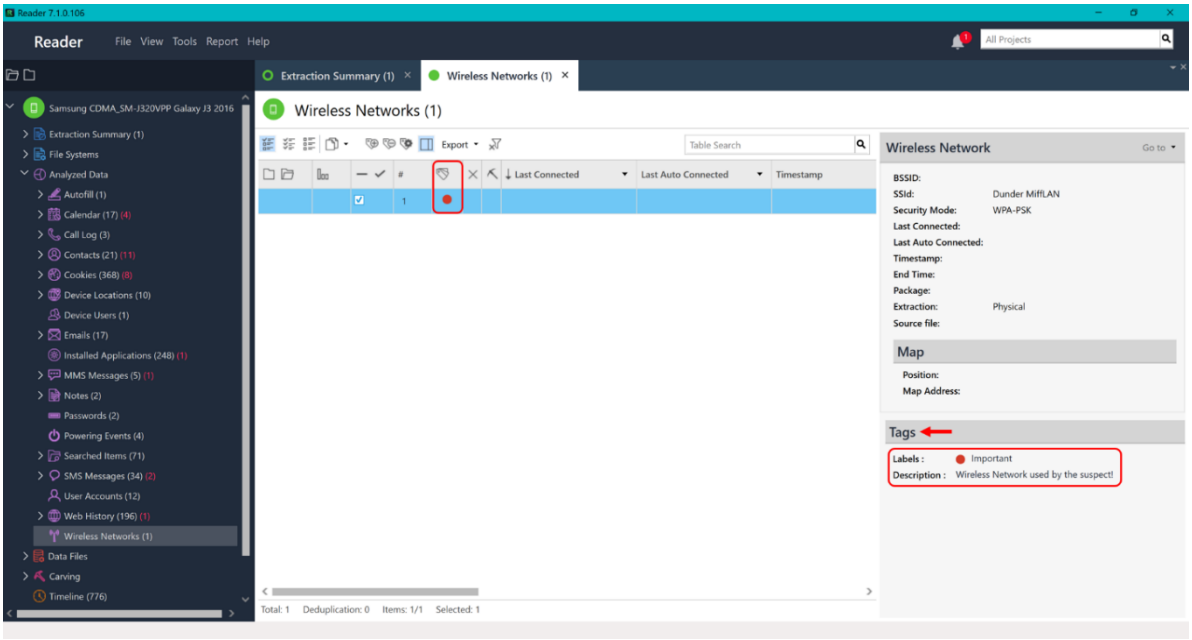


Figure 5-11: The Tag Will Be Represented in the File's Row and the Right Detail Pane

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.

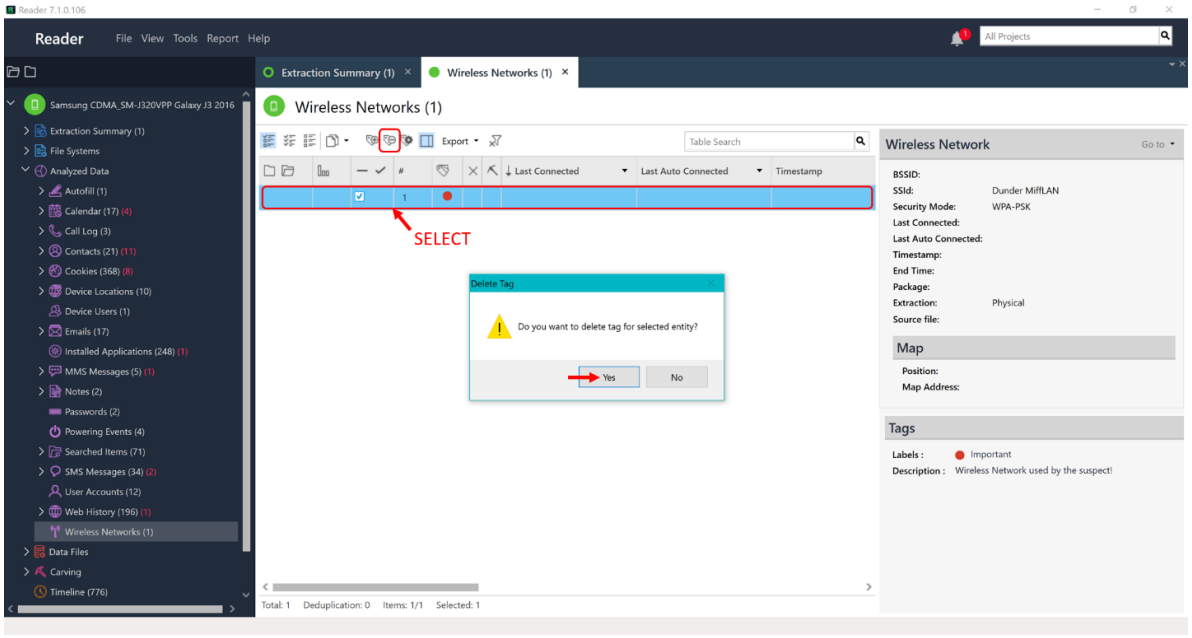


Figure 5-12: Begin By Selecting File(s) and Clicking the Minus Tag Button

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.

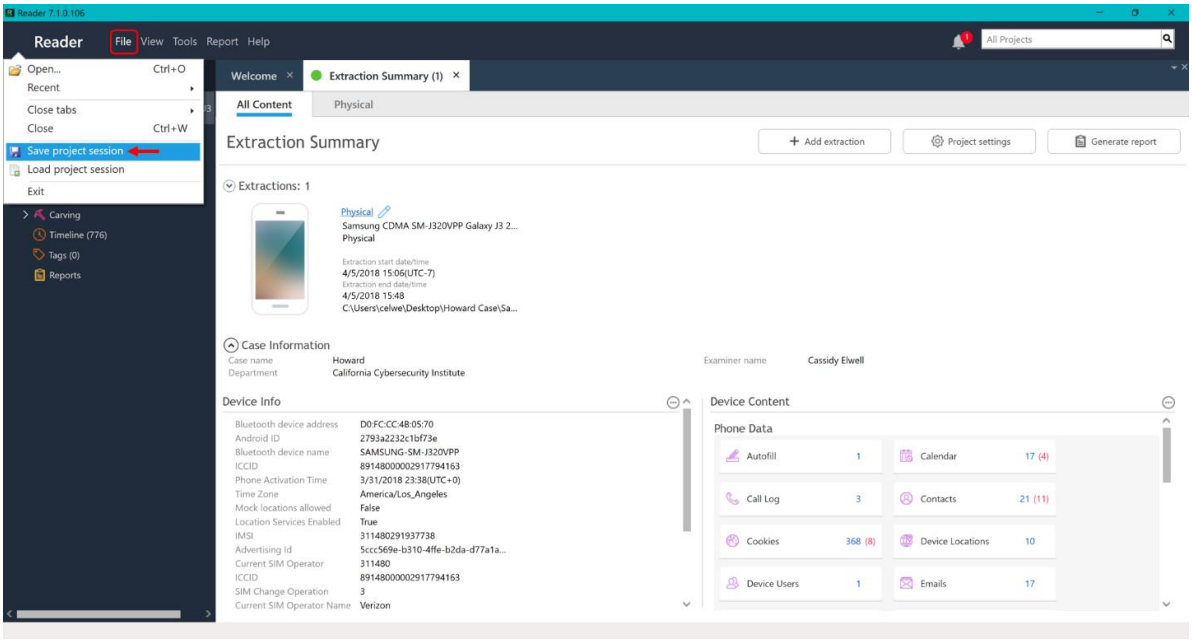


Figure 5-13: Remember to Save Your Session Using the Toolbar Before Exiting UFED Reader

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.

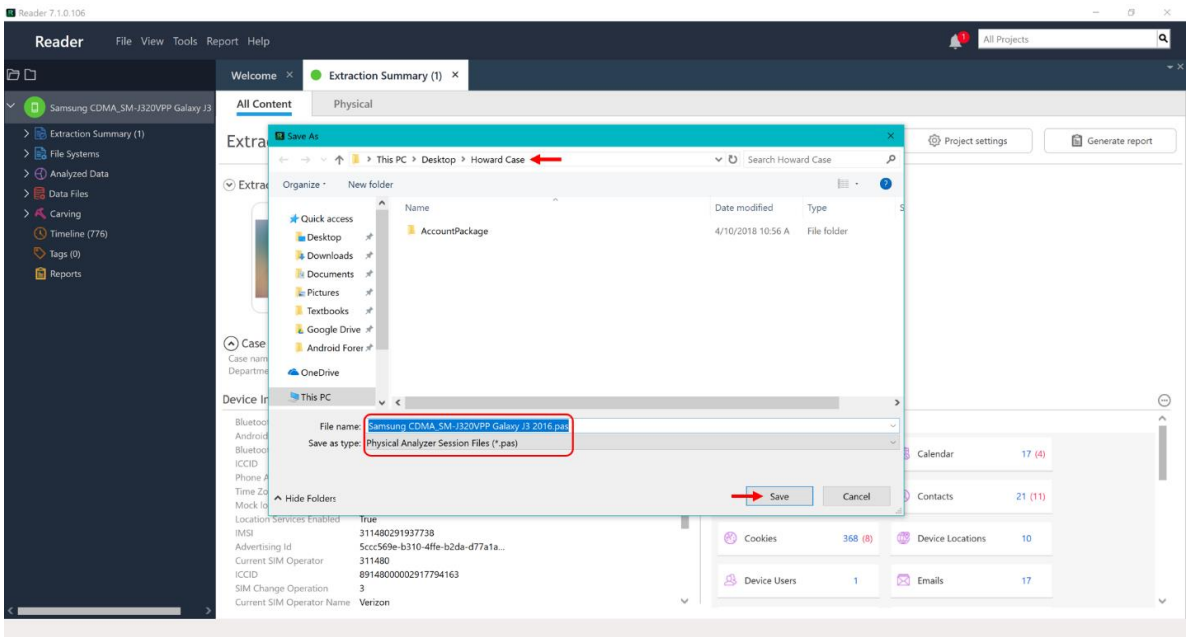


Figure 5-14: Ensure You Select to Save the Project Session Within the Same Location as the .UFDR File

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.

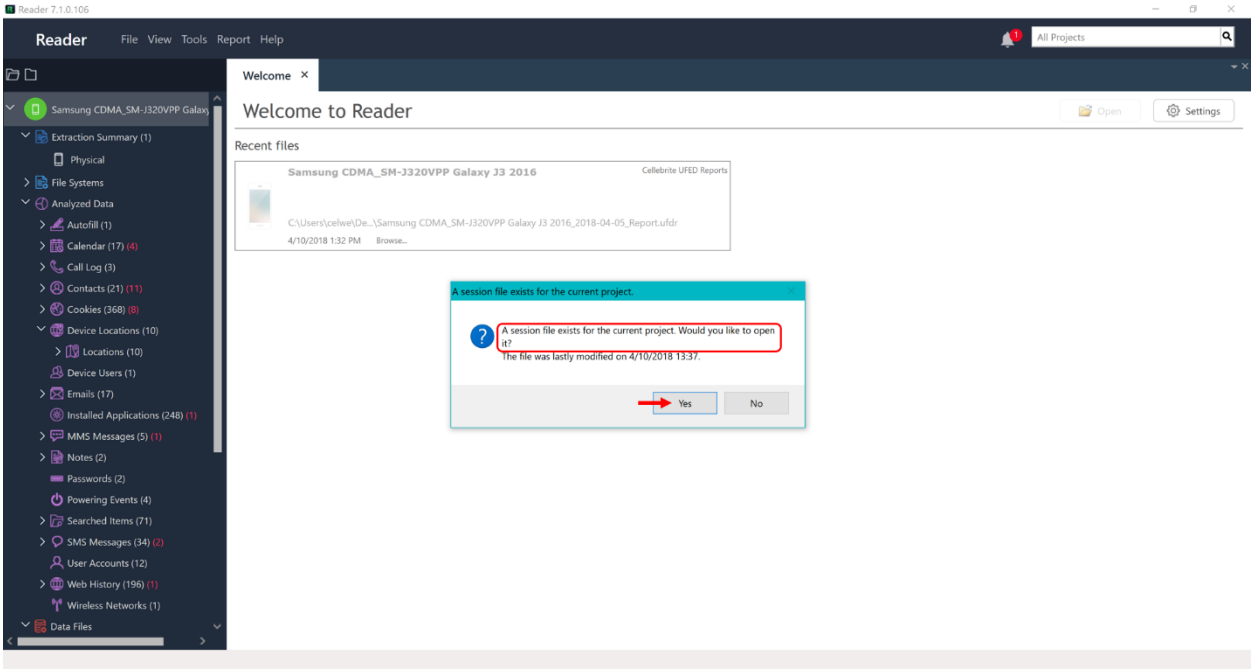


Figure 5-15: Reopen the Case the Same as Before and Select Yes When Asked If You Want to Load Your Project Session

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.

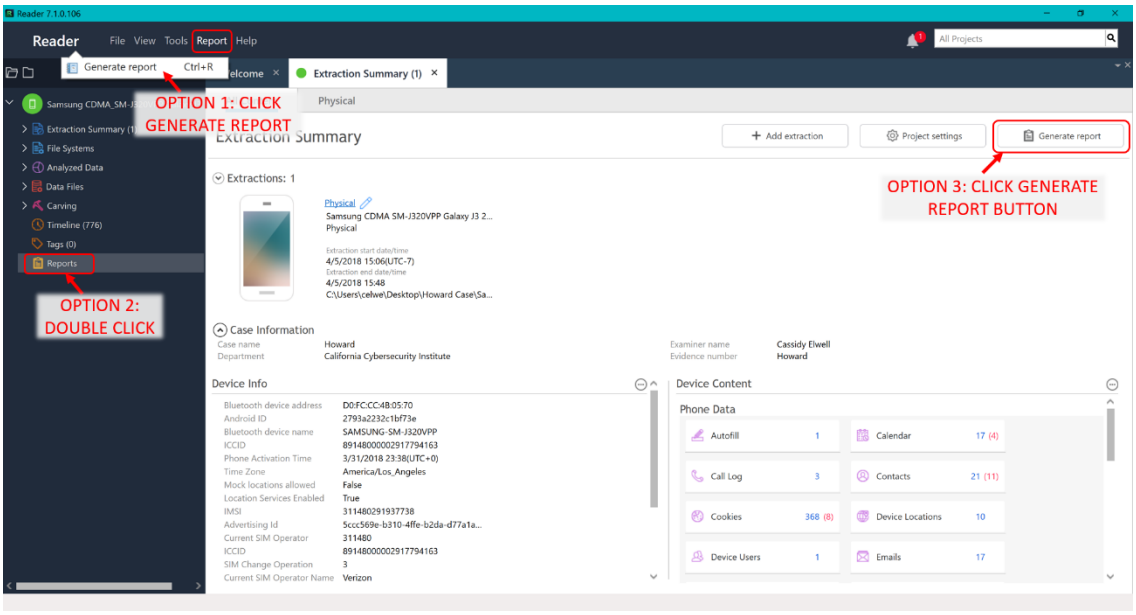


Figure 5-16: Open the Generate Report Menu

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.

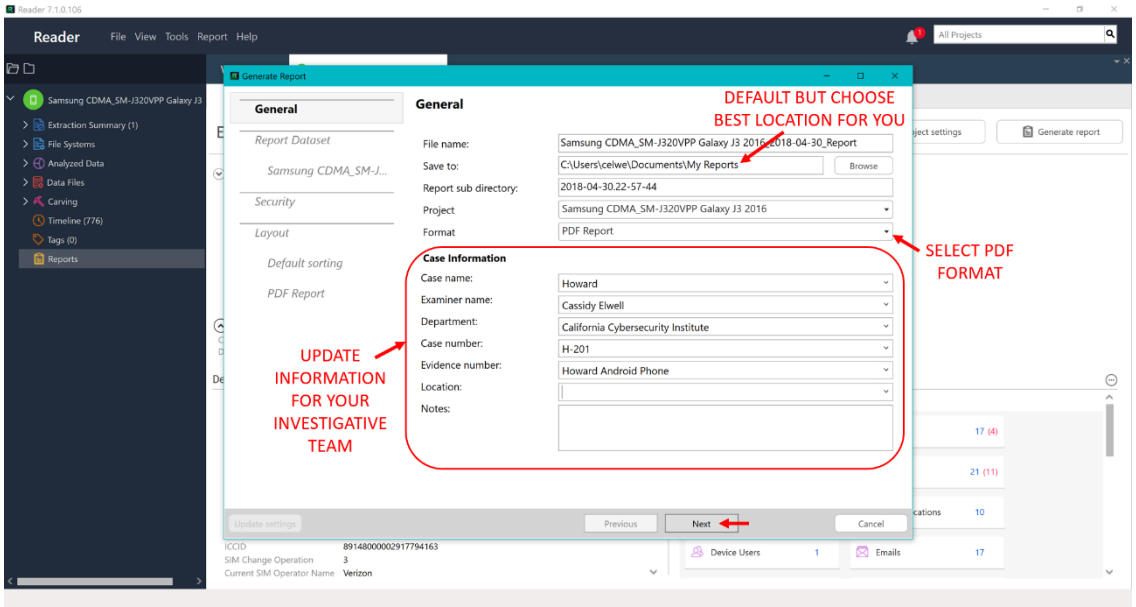


Figure 5-17: Update Case and Investigation Information and Select PDF for Report Format

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.

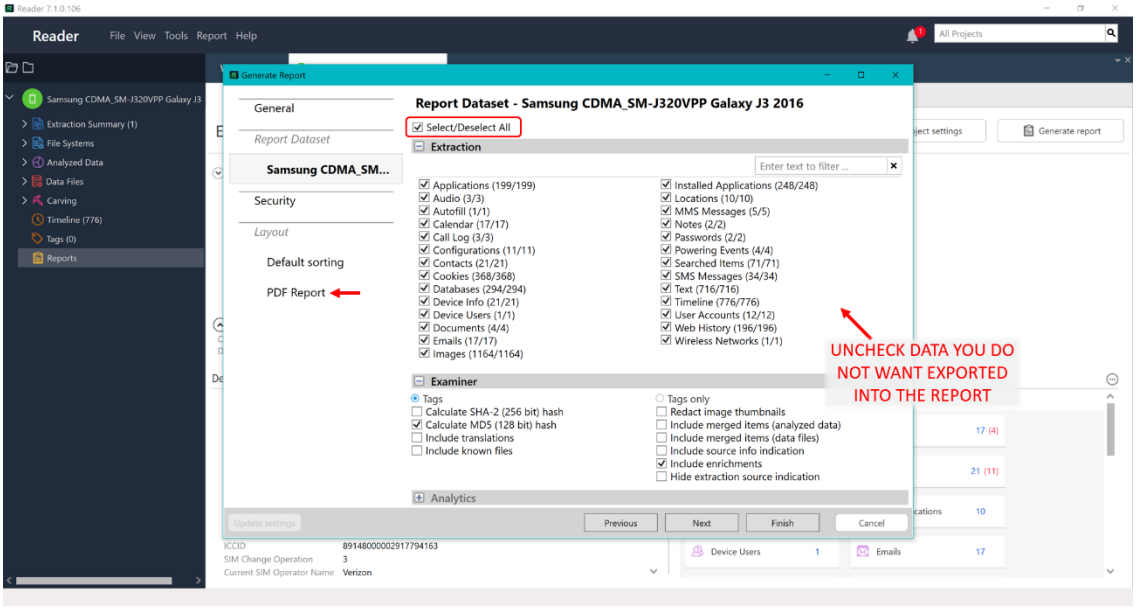


Figure 5-18: Select Data to be Included in the Generated Report

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.

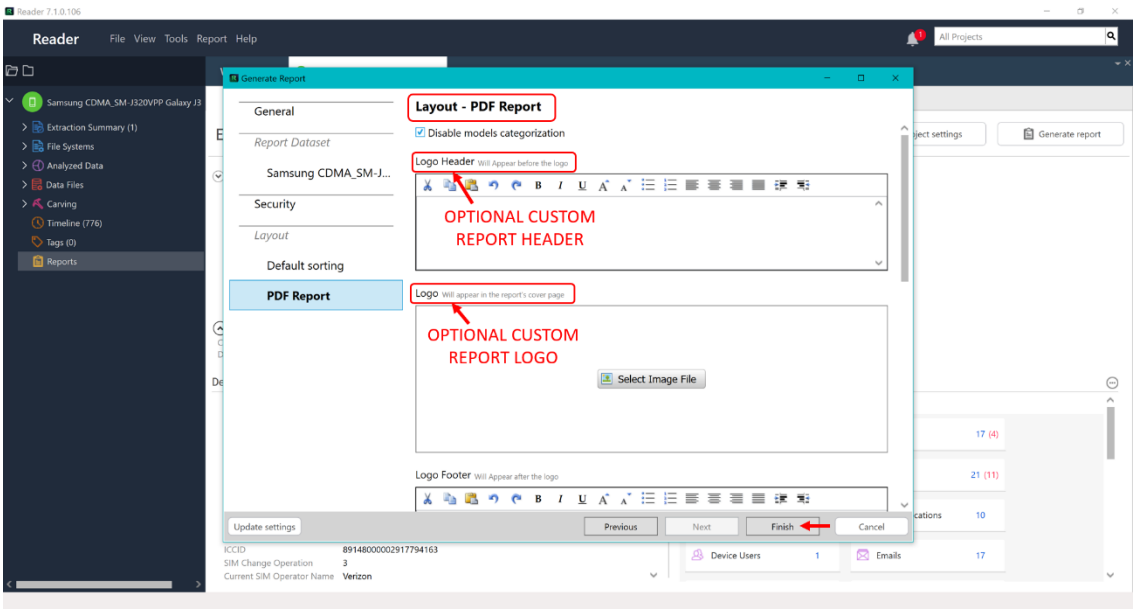


Figure 5-19: Optional Custom Header and Logo Options for PDF Report

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.

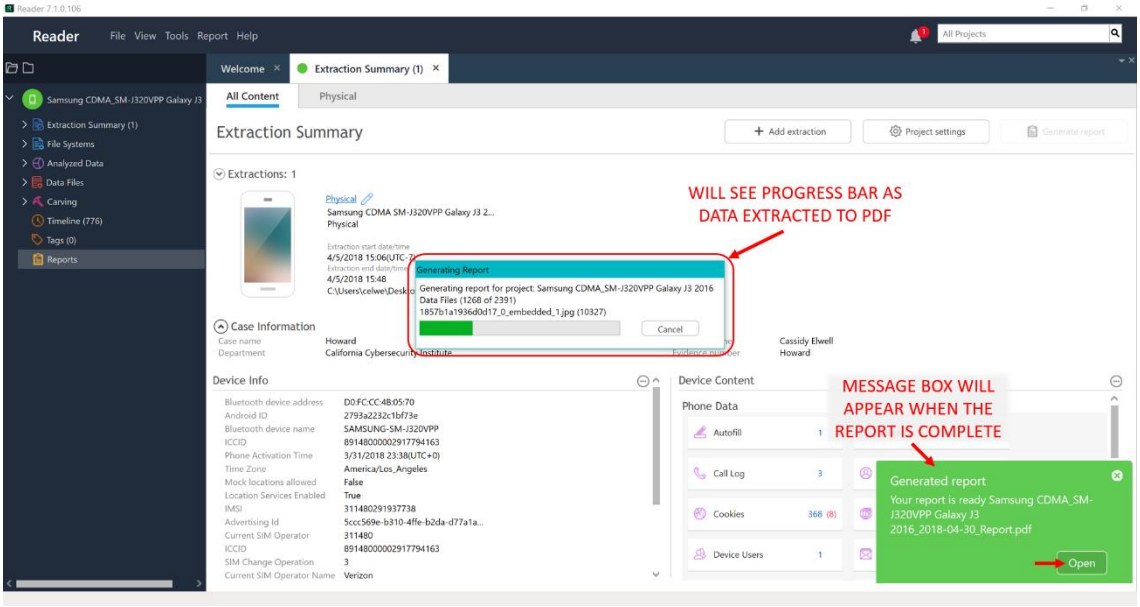


Figure 5-20: Report Creation in Process with Green Pop-Up Showing Completion

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.

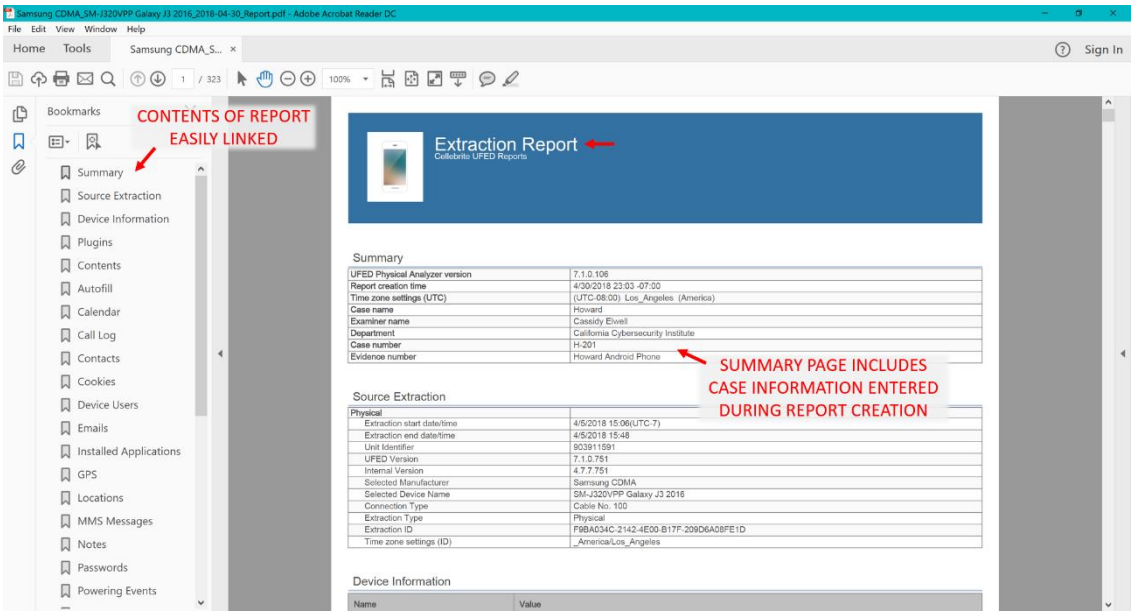


Figure 5-21: Open the Extraction Report and Contents will be Easily Linked

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 6: Lock/Home Screen Captures and Personal Files

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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.

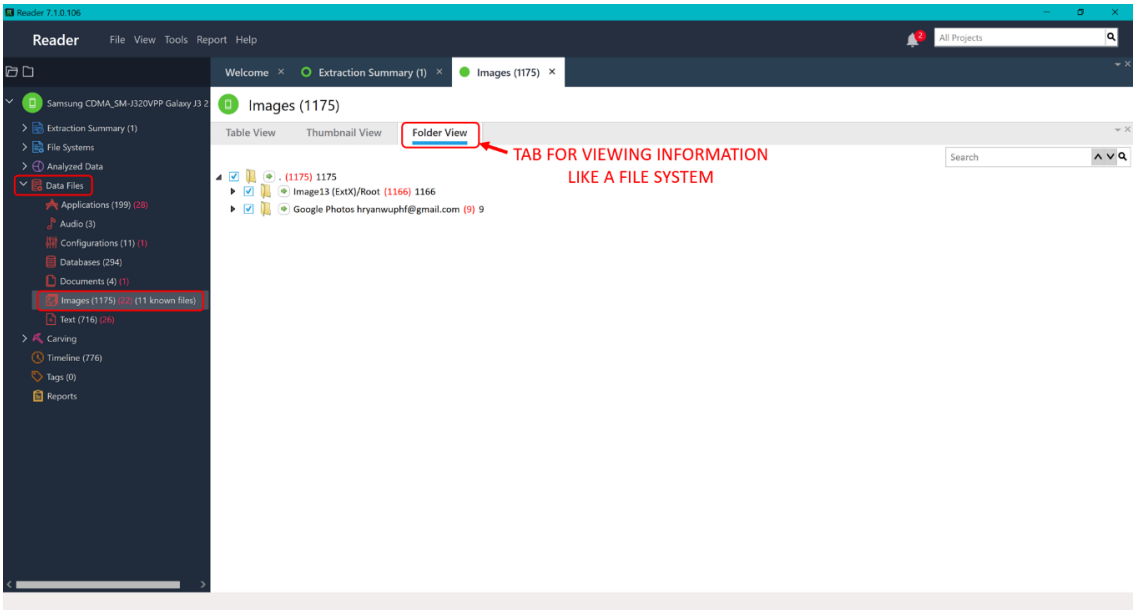


Figure 6-1: View the Images Within Android File System in the Data Files Tab

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."

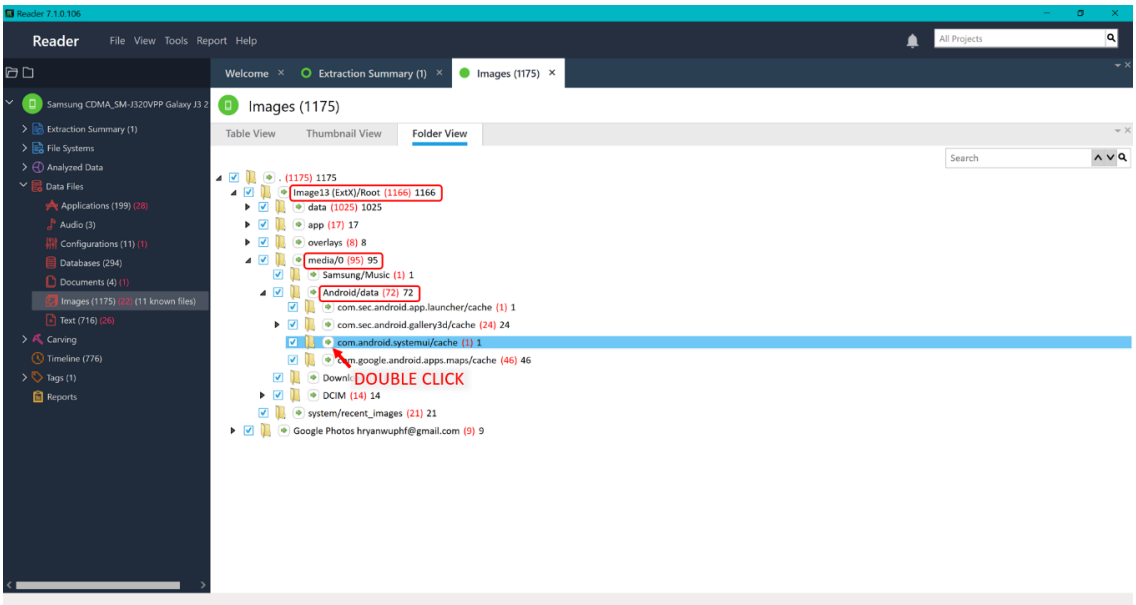


Figure 6-2: Screen Capture of the Device's Lock Screen is Stored Within Media

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.

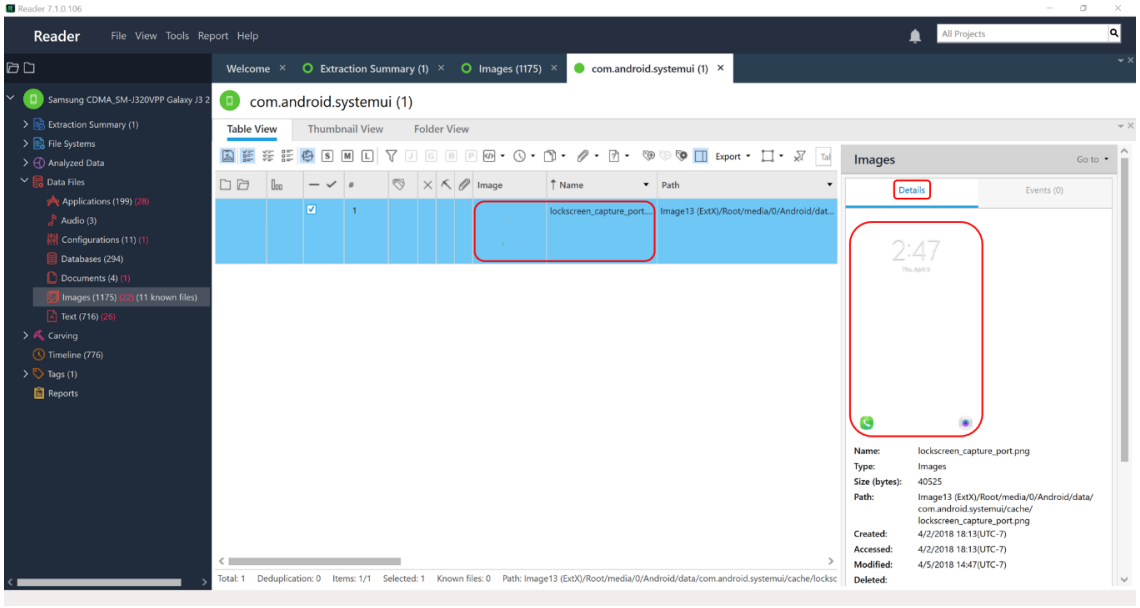


Figure 6-3: Lock Screen Capture for Ryan Does Not Differ from the Android Default

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.”

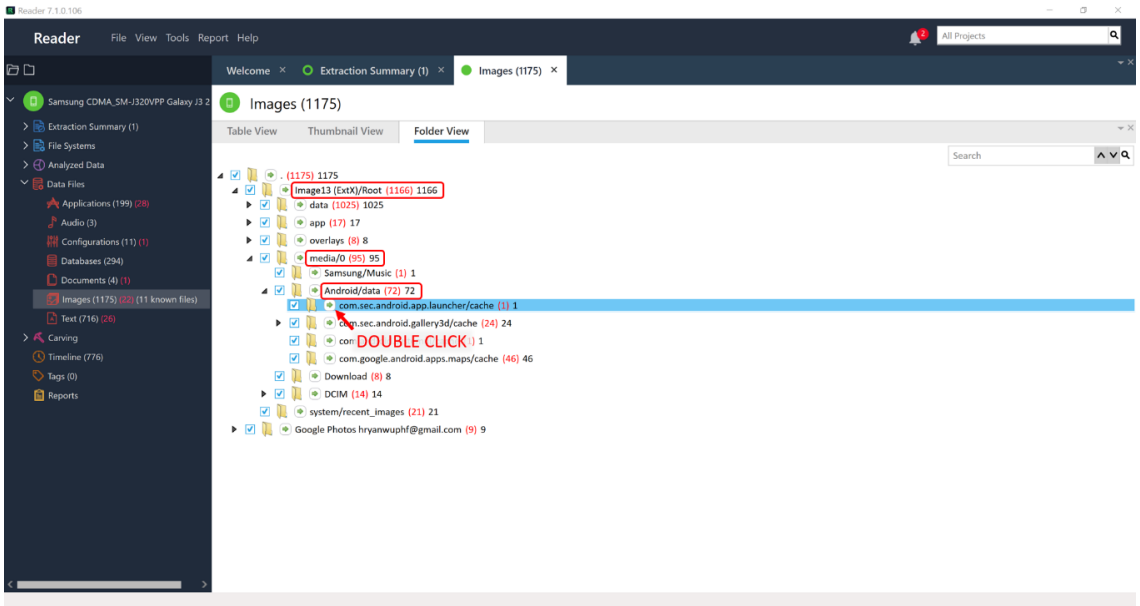


Figure 6-4: Screen Capture of the Device's Home Screen is Stored Within Media

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.

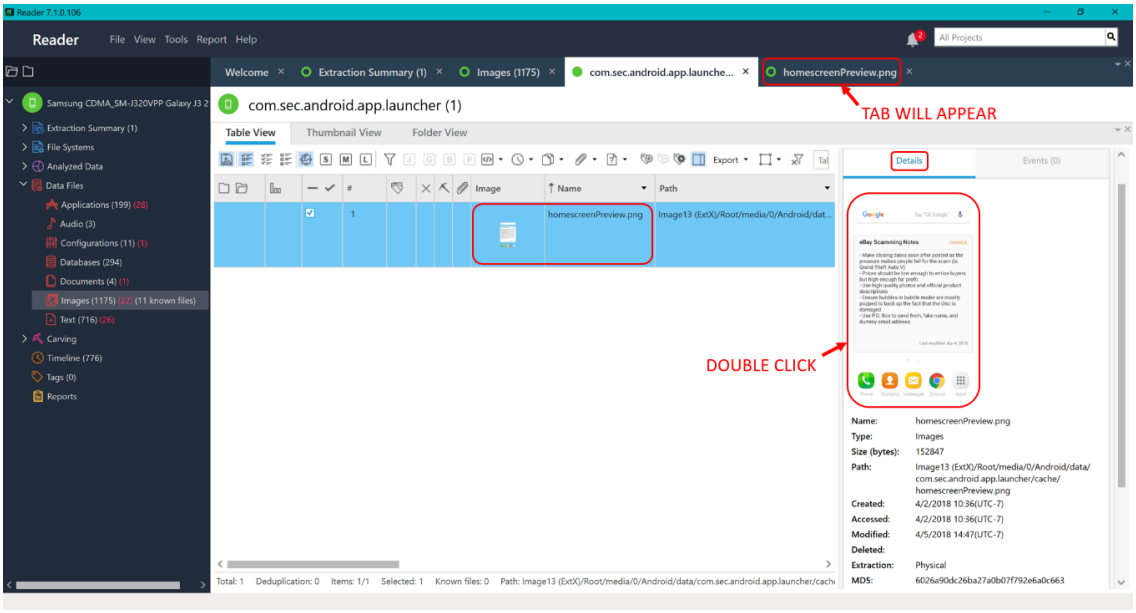


Figure 6-5: Home Screen Capture for Ryan Includes a Widget with Evidence

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.

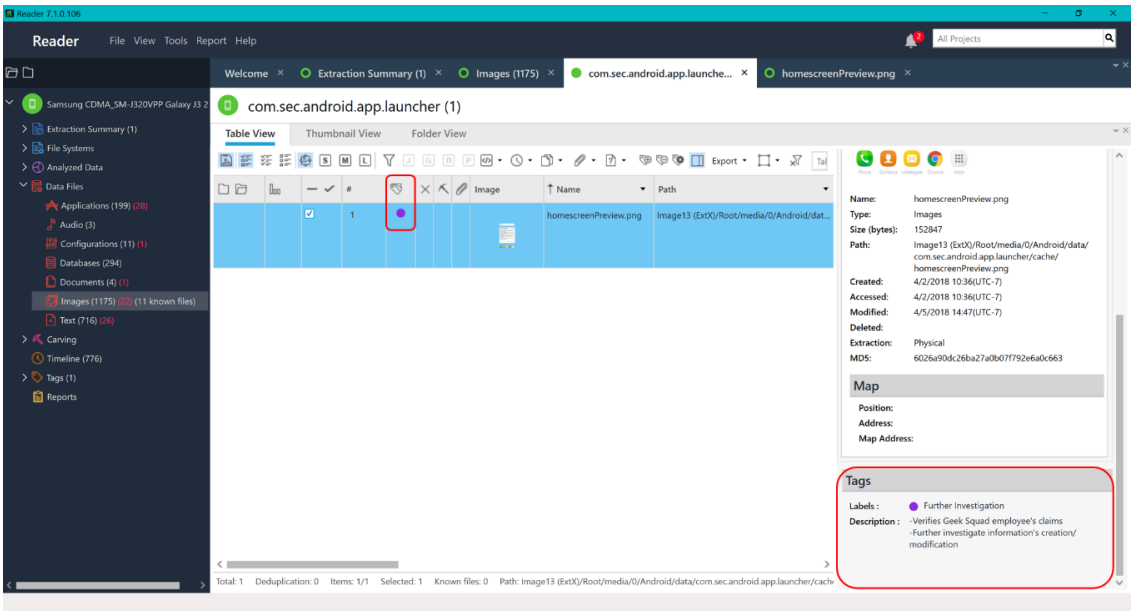


Figure 6-6: Tag the Home Screen Capture for Future Access and Investigation

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.

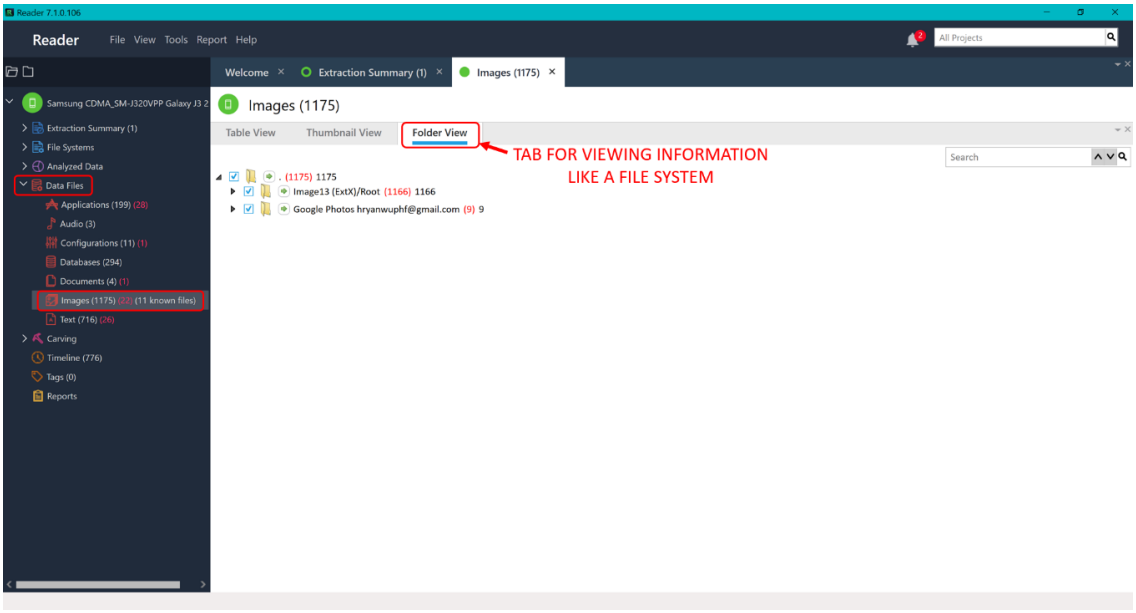


Figure 6-7: View the Images Within Android File System in the Data Files Tab

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."

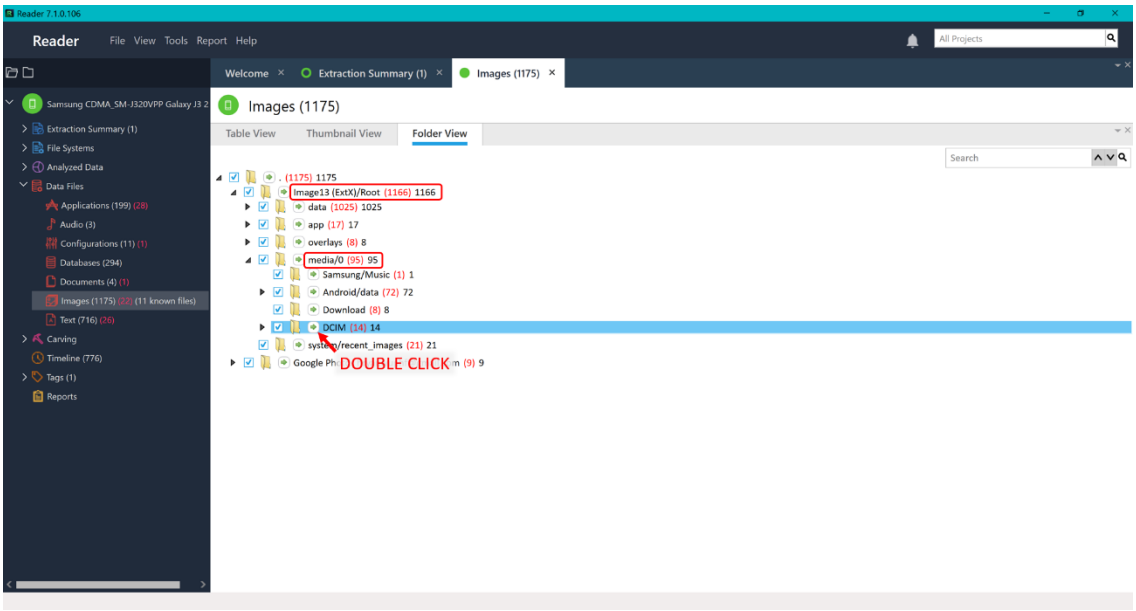


Figure 6-8: Media Gallery Photos Including Those Taken with the Device's Camera are Stored in DCIM

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.

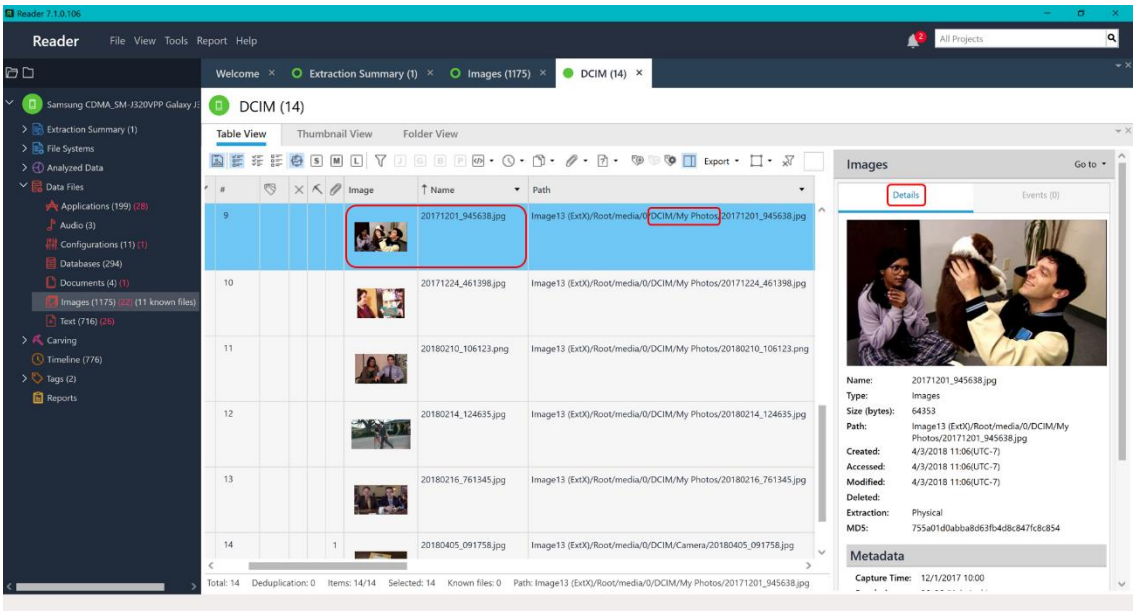


Figure 6-9: Personal and Downloaded Images Further Analyzable Within the Details Pane

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.

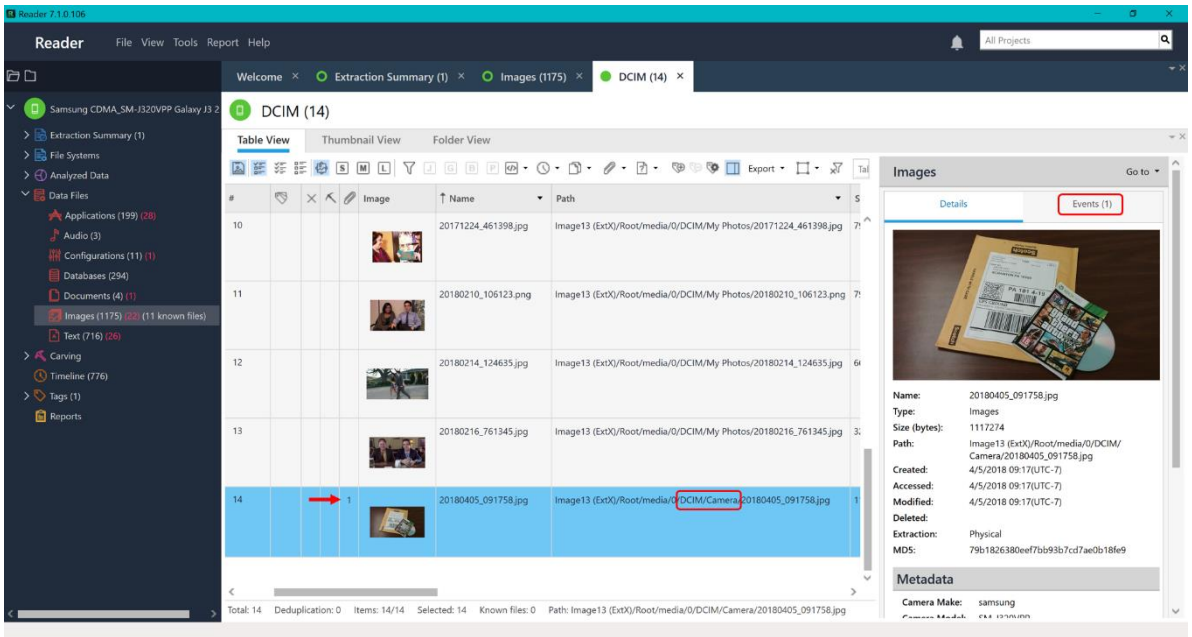


Figure 6-10: Image Labeled with an Event was Often Sent or Received Through Form of Communication

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.

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

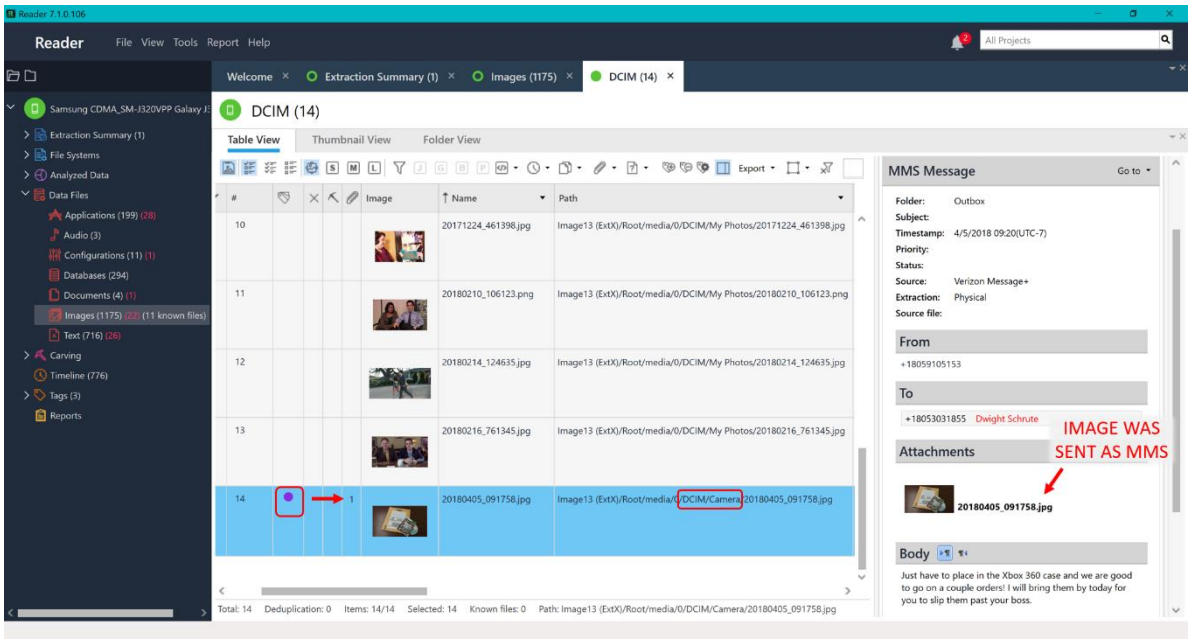


Figure 6-11: Event of the Image was a MMS Message to Dwight Schrute

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.”

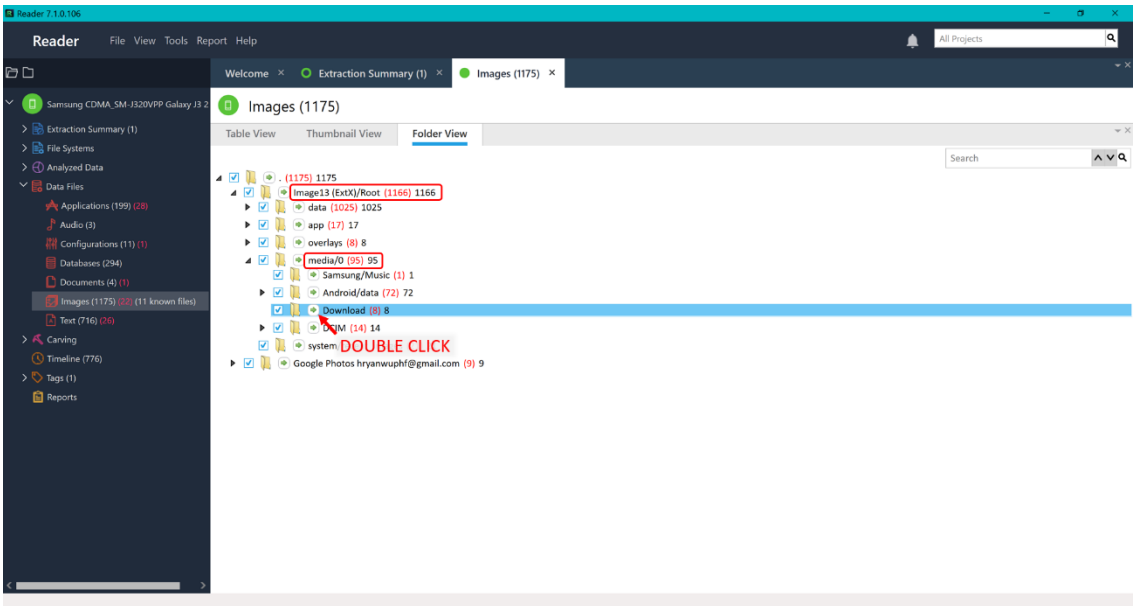


Figure 6-12: Downloaded Photos are Stored Within the Android File System's Media Folder

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.”

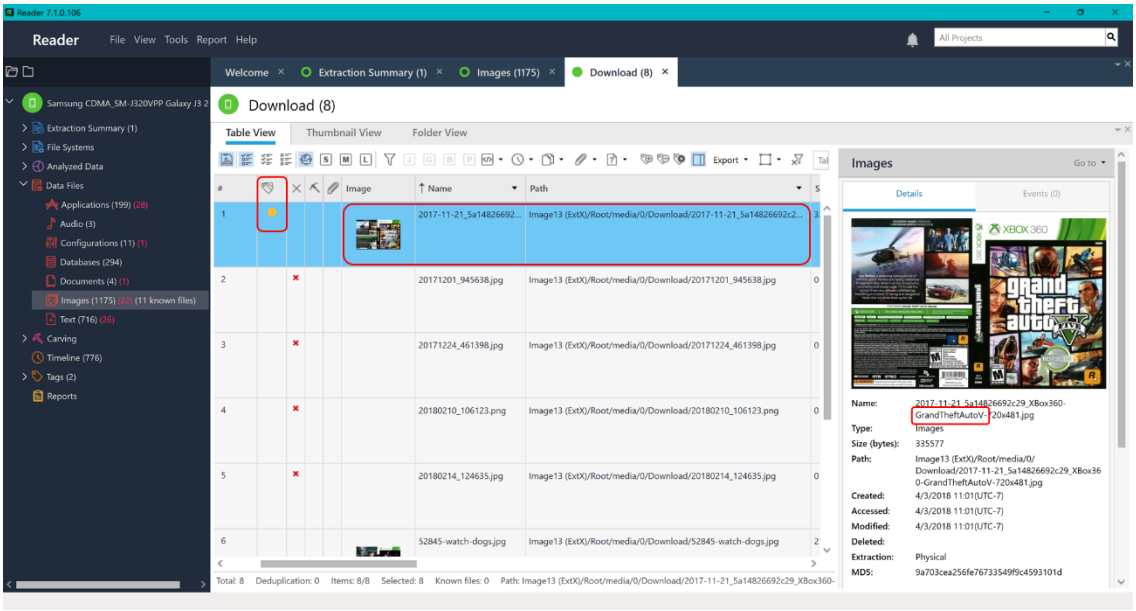


Figure 6-13: Ryan's Downloaded Photos are Purely Xbox 360 Game Sleeves

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.

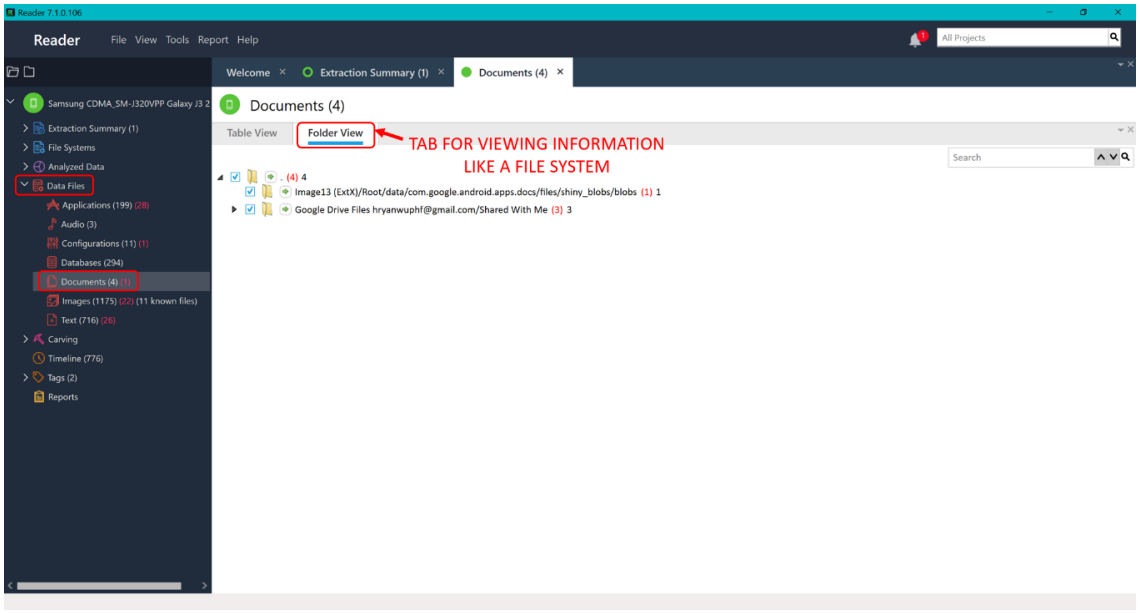


Figure 6-14: View the Images Within Android File System in the Data Files Tab

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."

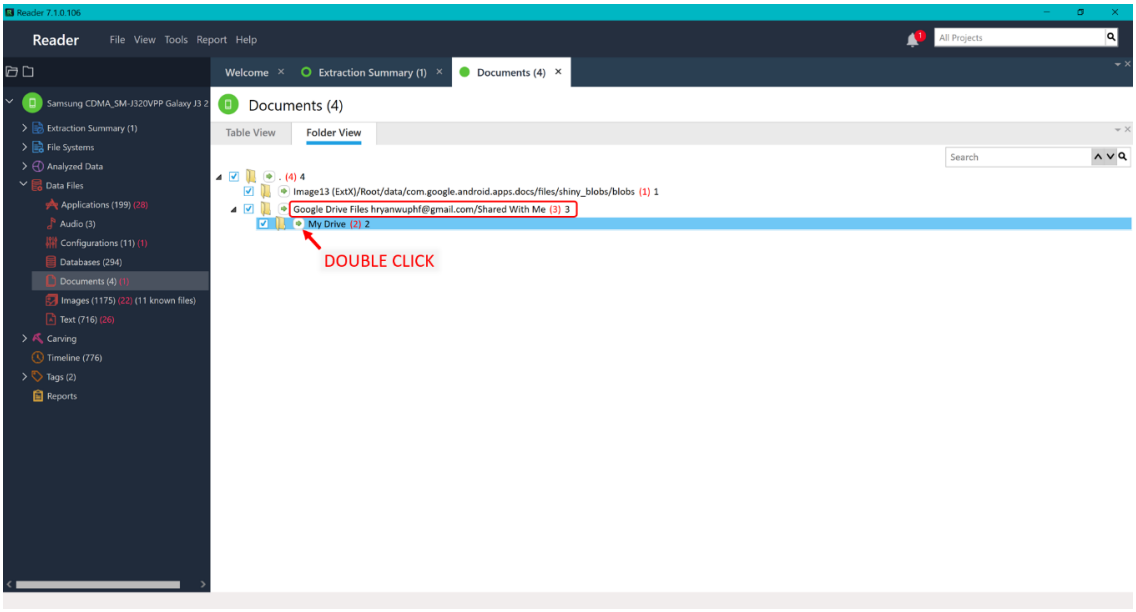


Figure 6-15: My Drive Documents within Ryan's hryanwuphf@gmail.com Google Account

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.

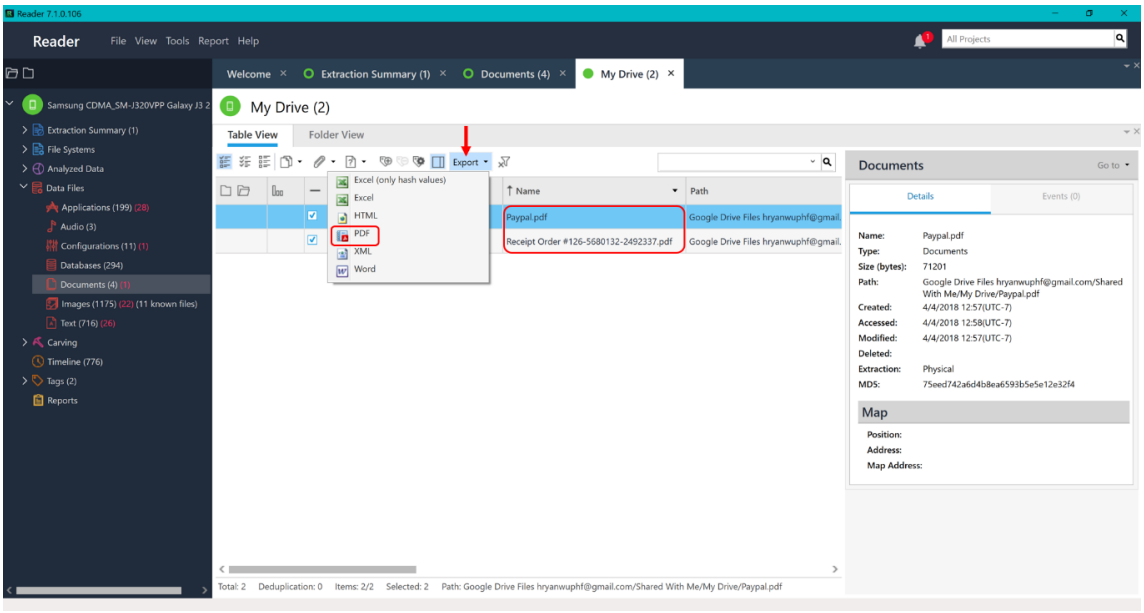


Figure 6-16: View Documents from the Device by Exporting a Report

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.

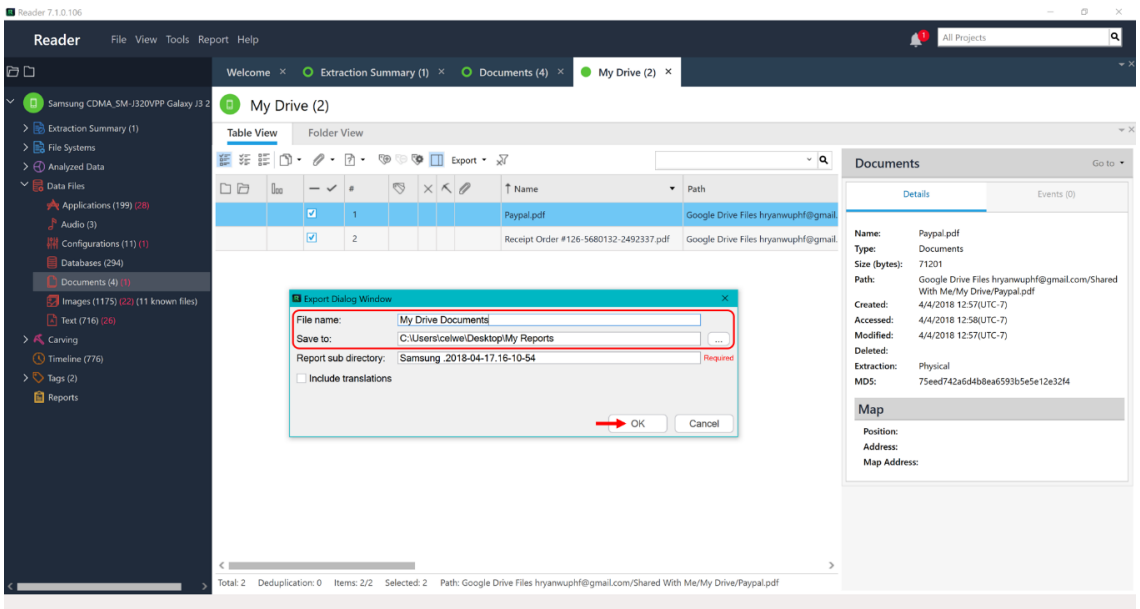


Figure 6-17: Export Window Specifications Should be Changed EXCEPT for the Report Sub Directory

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/`

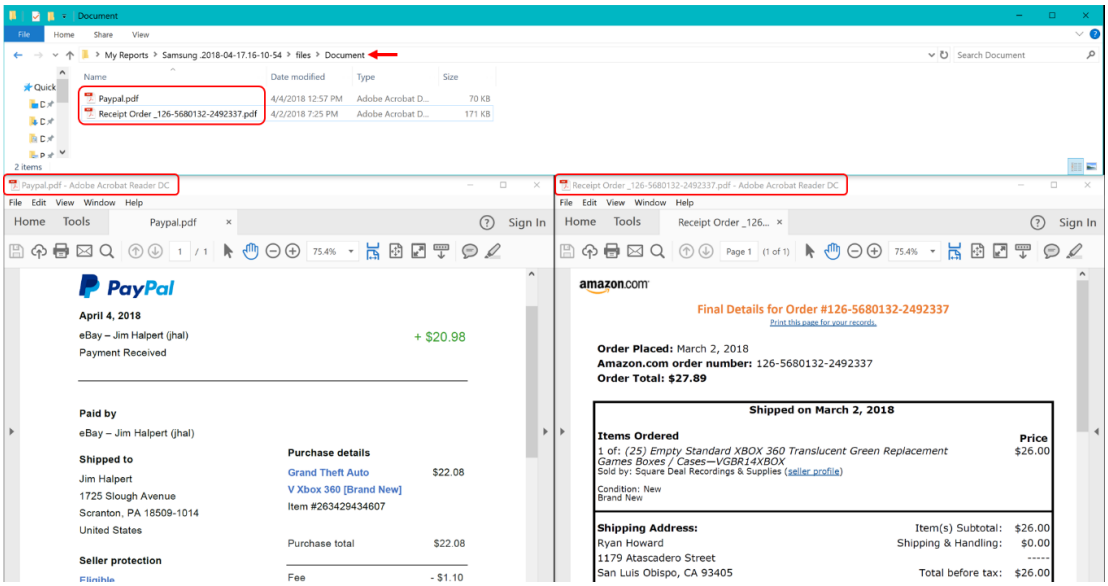


Figure 6-18: Open the Exported Paypal and Amazon Receipts from Ryan's My Drive

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.

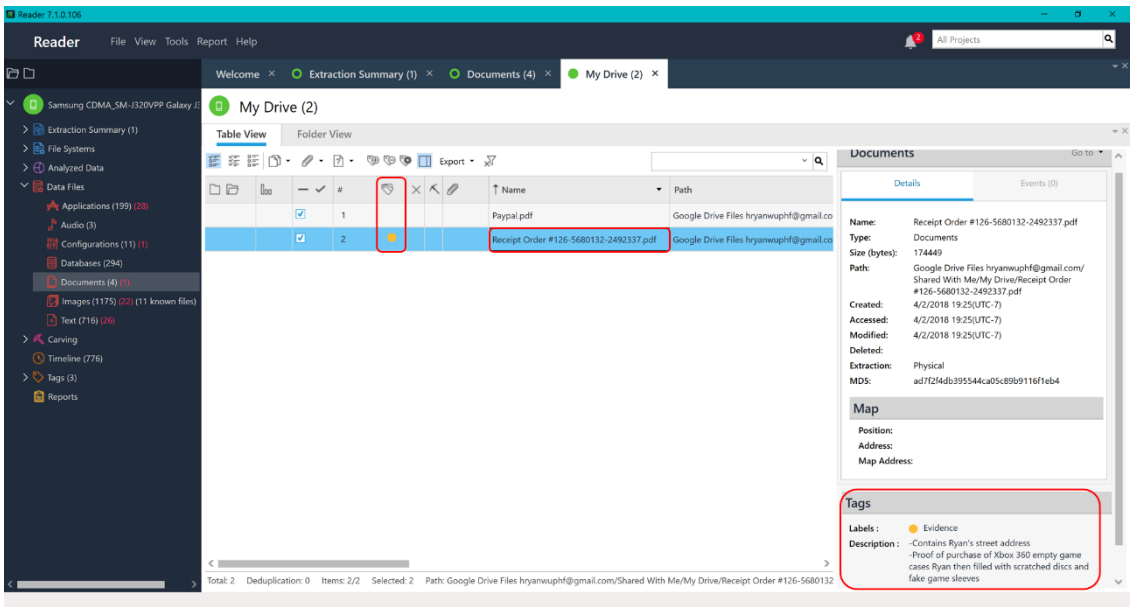


Figure 6-19: Tag Amazon Receipt Containing Address and Proof of Xbox 360 Cases Purchase

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/
```

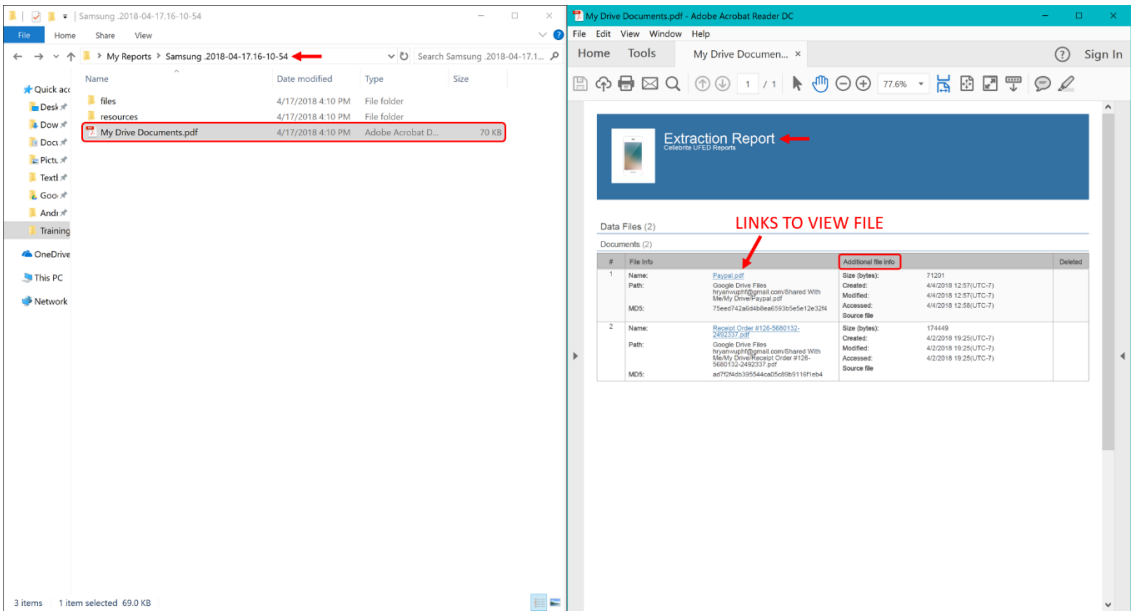


Figure 6-20: Extraction Report of My Drive Documents Includes Metadata from Device

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 7: Installed Applications

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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.

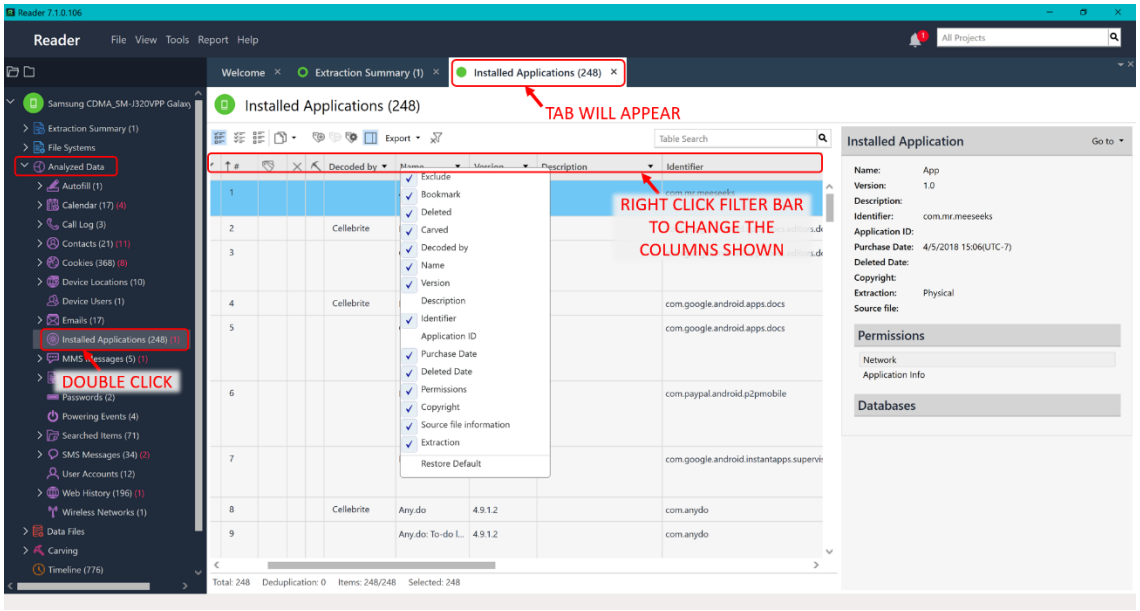


Figure 7-1: Extensive Installed Applications List

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.

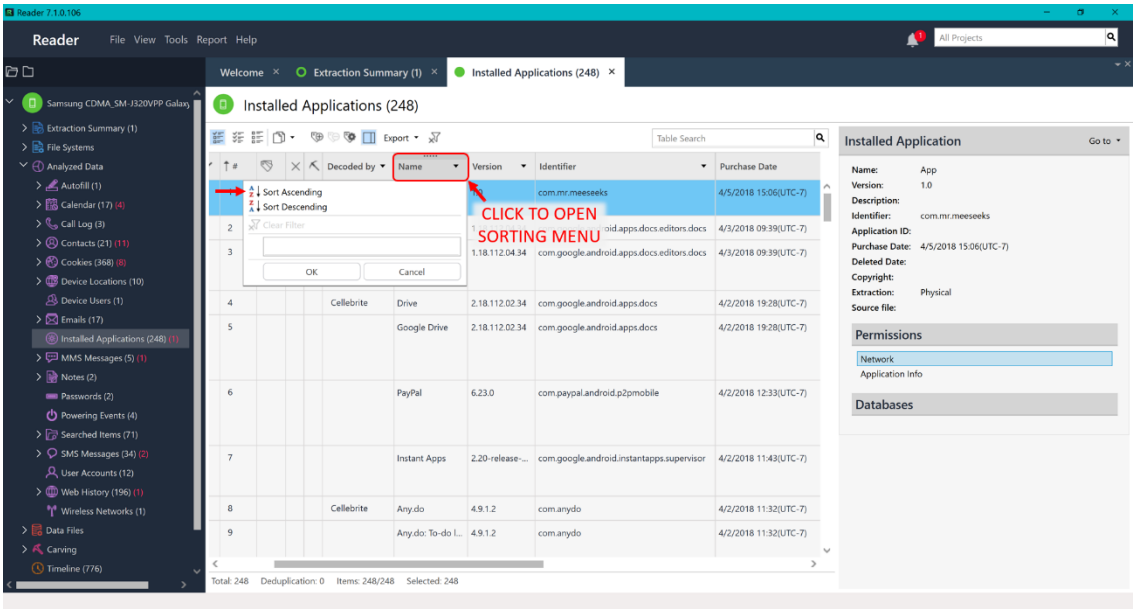


Figure 7-2: Ascending Sort Allows for Separation Between User and Android Background Applications

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.

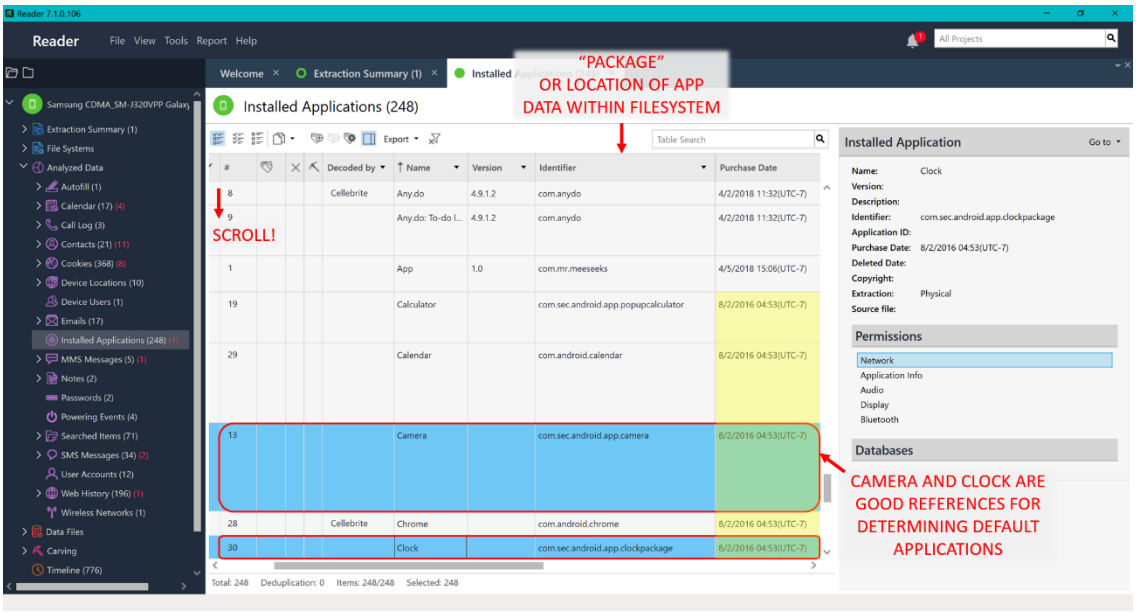


Figure 7-3: Examine Applications Further by Package Name and Determine Default Applications with Timestamps

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."

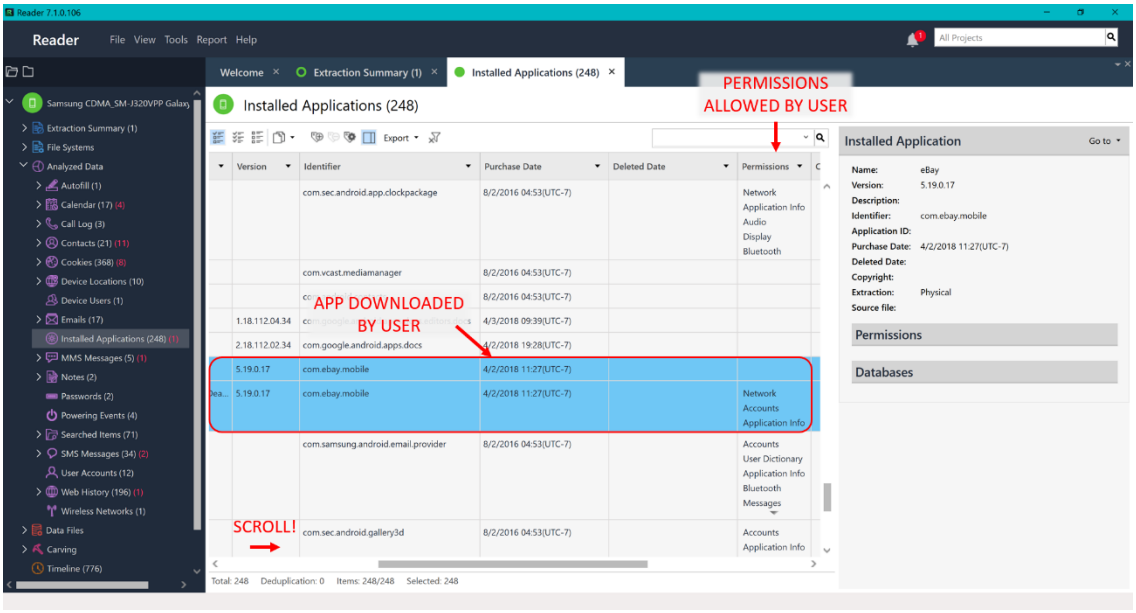


Figure 7-4: Permissions Can Provide Additional Details About the Applications Use

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

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 8: Contacts, Phone, and Messaging

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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.

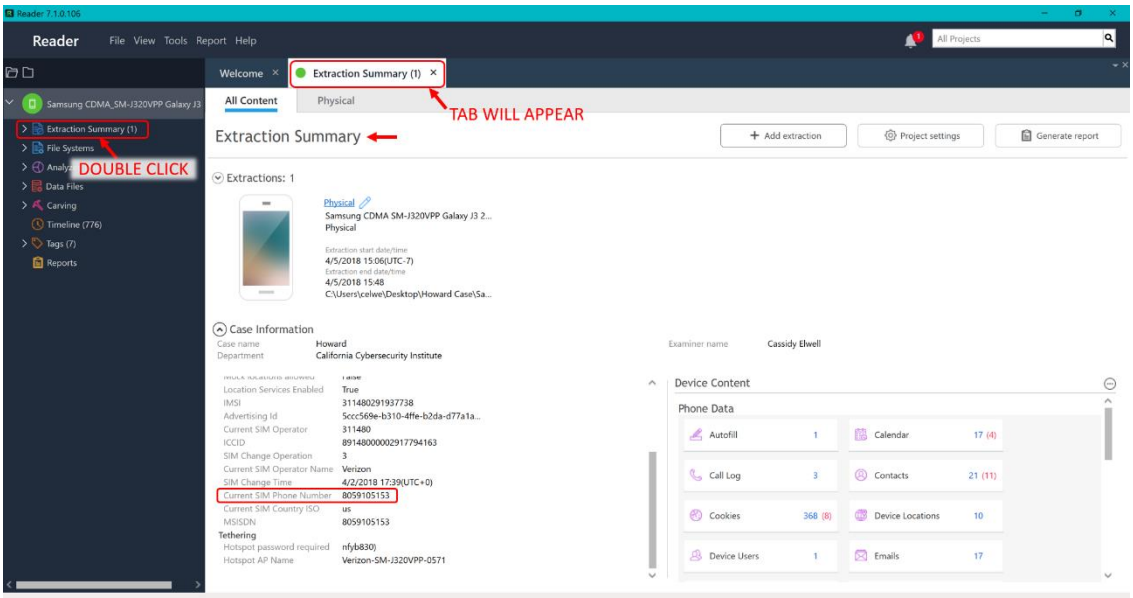


Figure 8-1: Extraction Summary Contains Device's Phone Number

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.

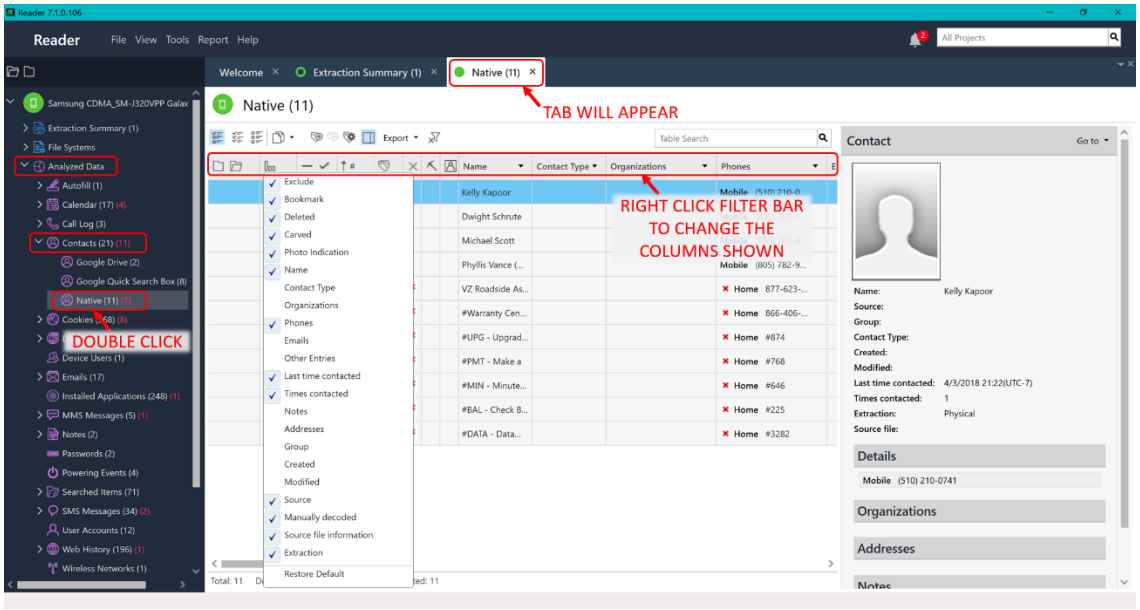


Figure 8-2: Native Device Contacts Listed

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.

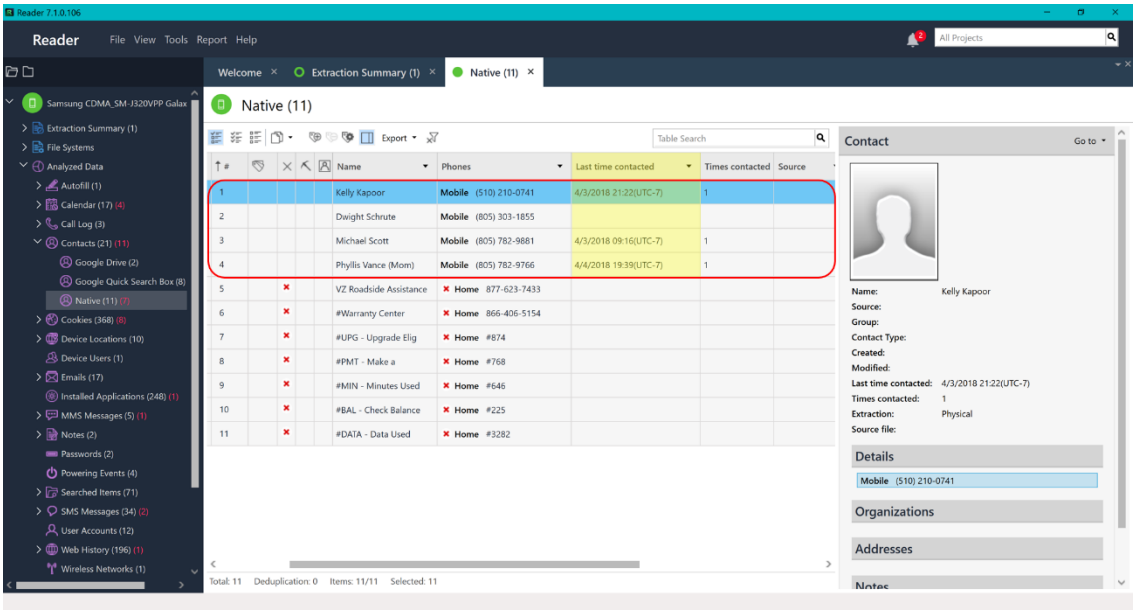


Figure 8-3: Timestamp of Last Contacted is Stored within Native Contacts Data

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.

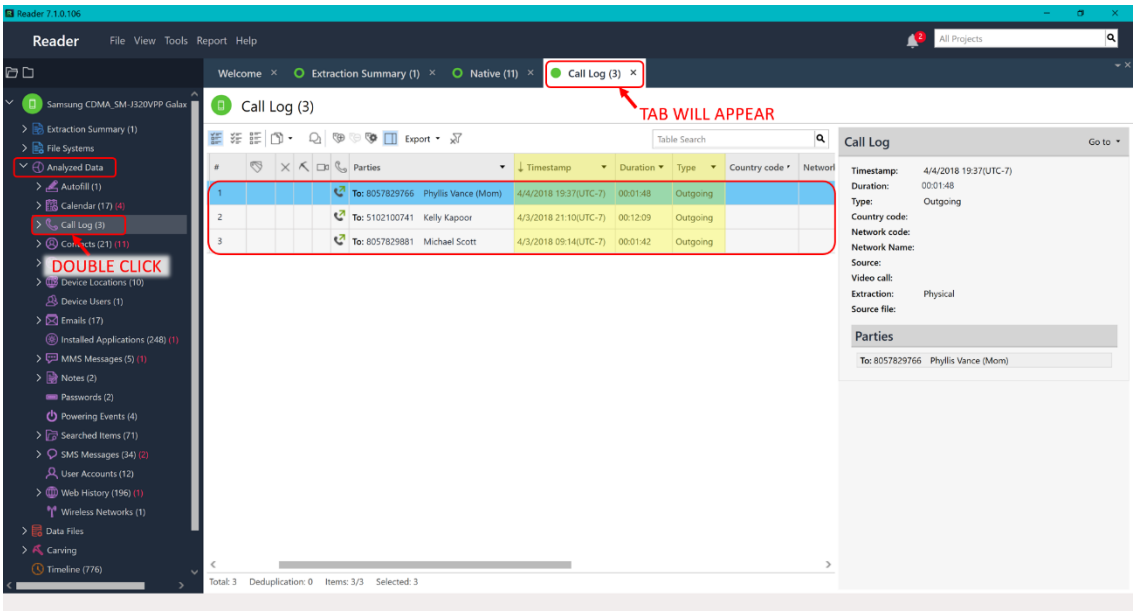


Figure 8-4: Call Log with Timestamp and Duration

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).

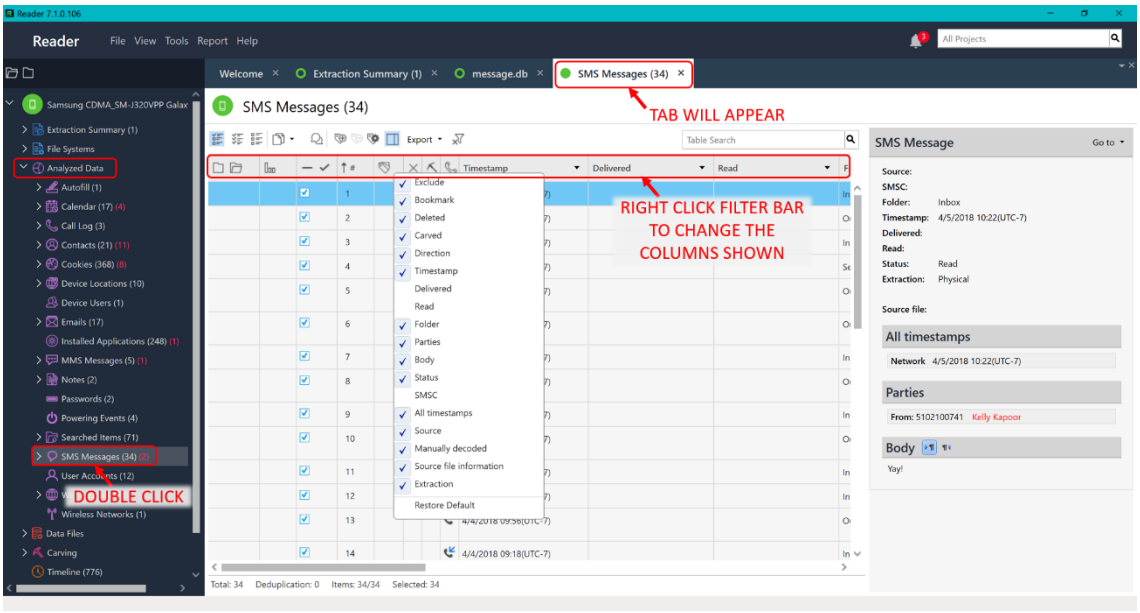


Figure 8-5: SMS Messages are Cross-Referenced and Filterable

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.

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

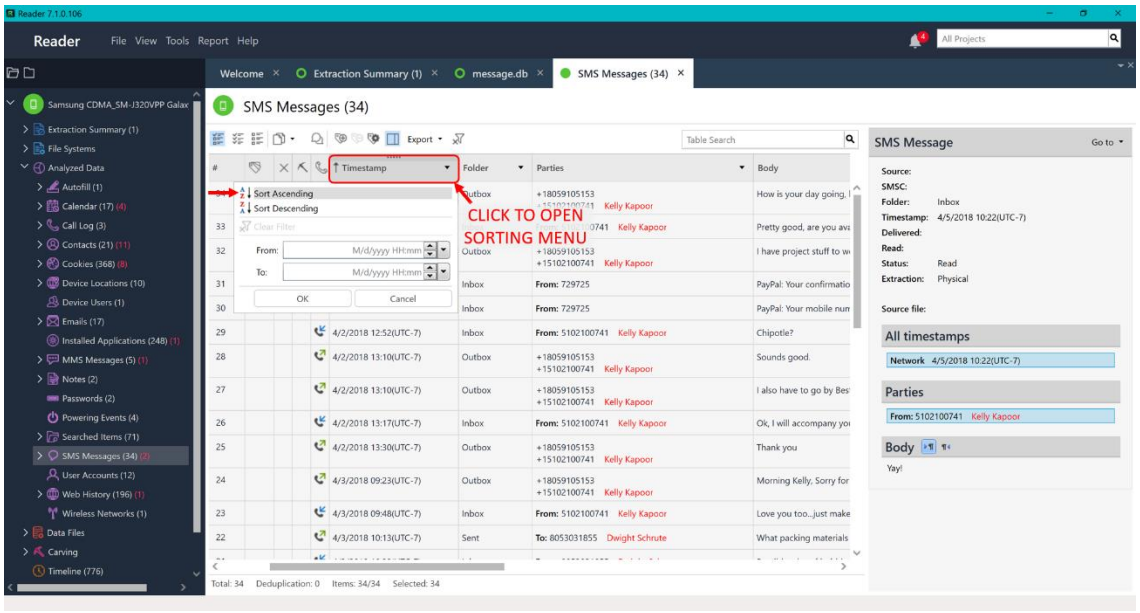


Figure 8-6: Sort SMS Messages into Ascending Timestamp Order

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.

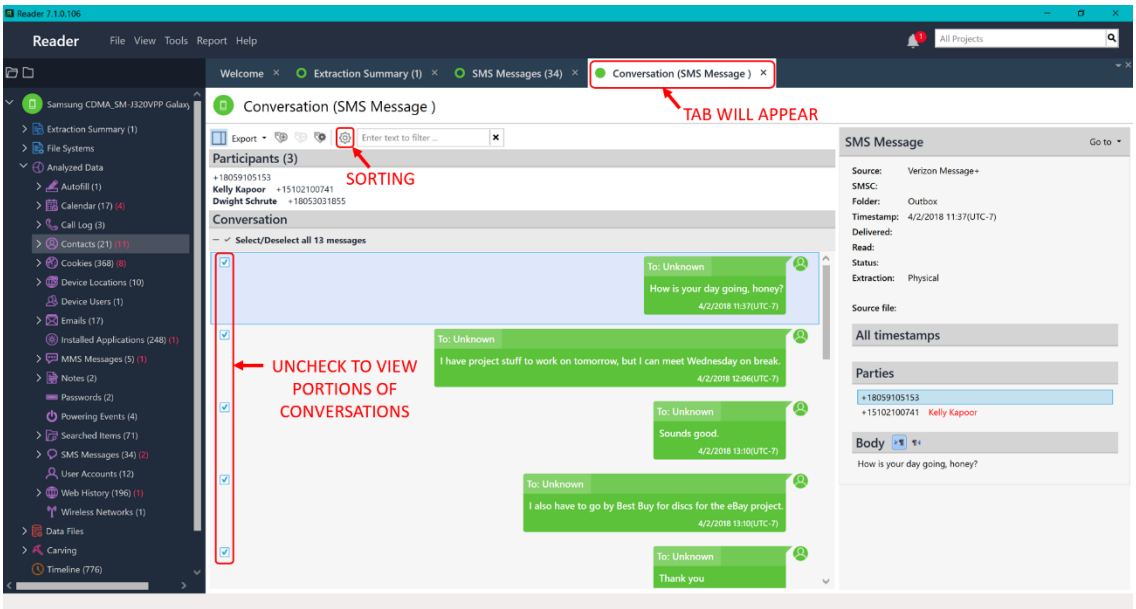


Figure 8-7: Conversation View of SMS Messages

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.

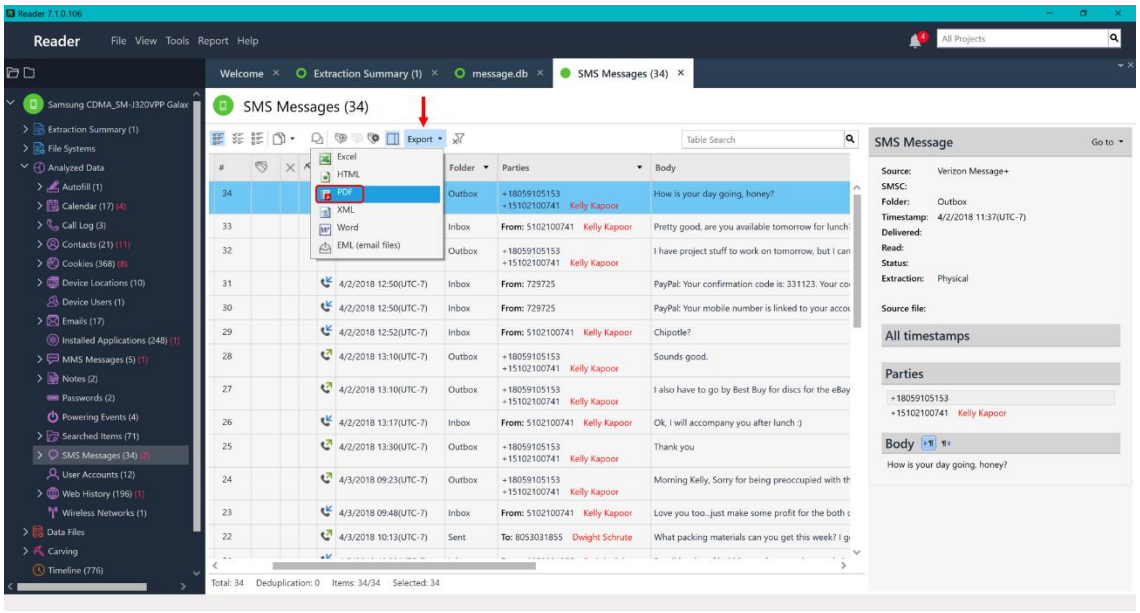


Figure 8-8: Exporting SMS Messages is an Option for Ease of Investigation

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/
```

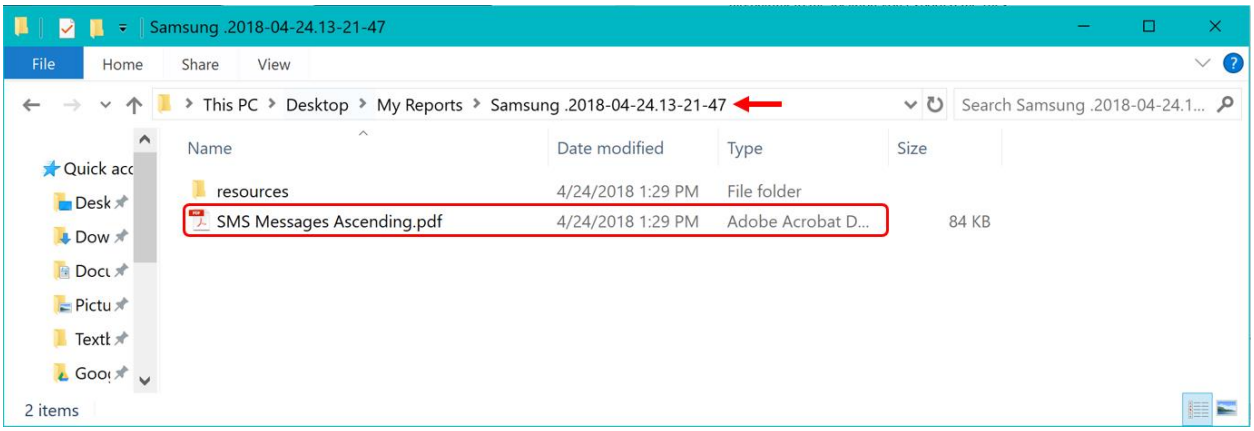


Figure 8-9: Navigate to Exported Report and Open

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."

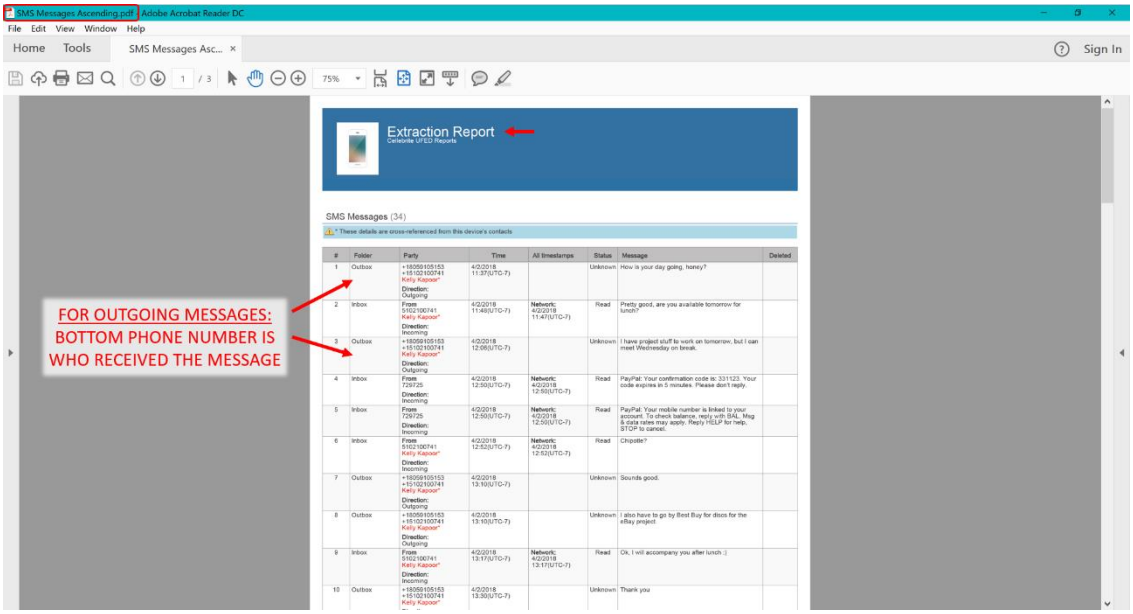


Figure 8-10: Extraction Report of SMS Messages from Device (in Ascending Order)

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).

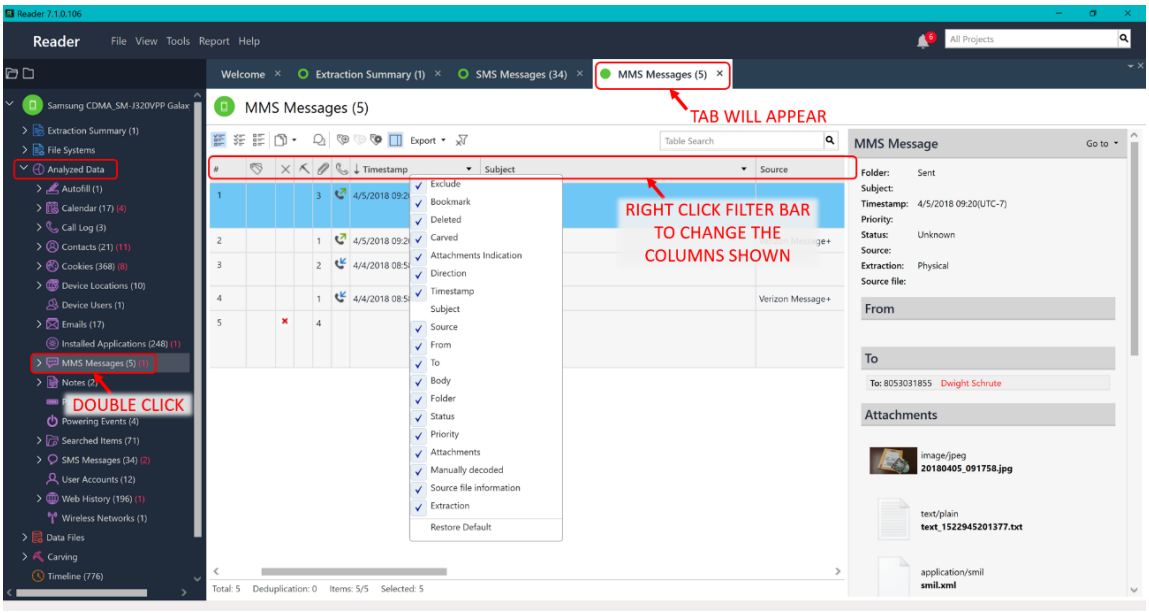


Figure 8-11: MMS Messages are Cross-Referenced and Filterable

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."

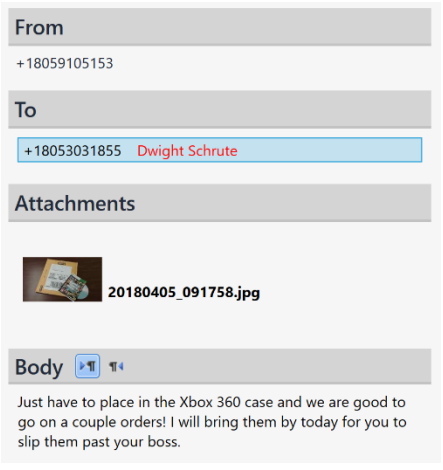


Figure 8-12: MMS Messages from Ryan's Device in Correspondence with Dwight Schrute

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.

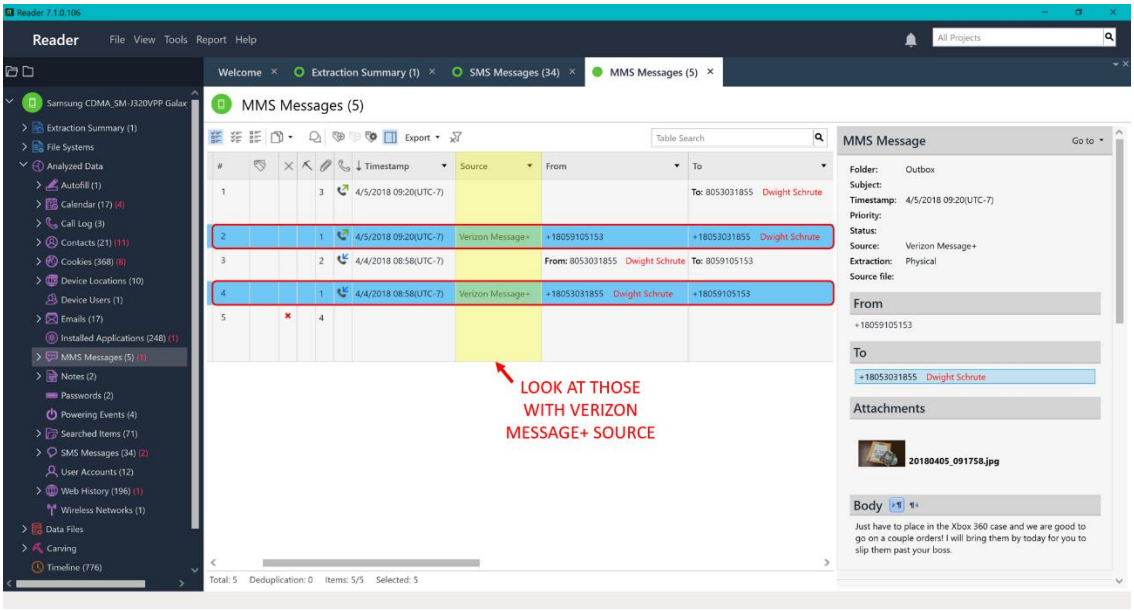


Figure 8-13: Examine the MMS Messages with Verizon Messages+ as a Source

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 9: Location Data

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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/
```

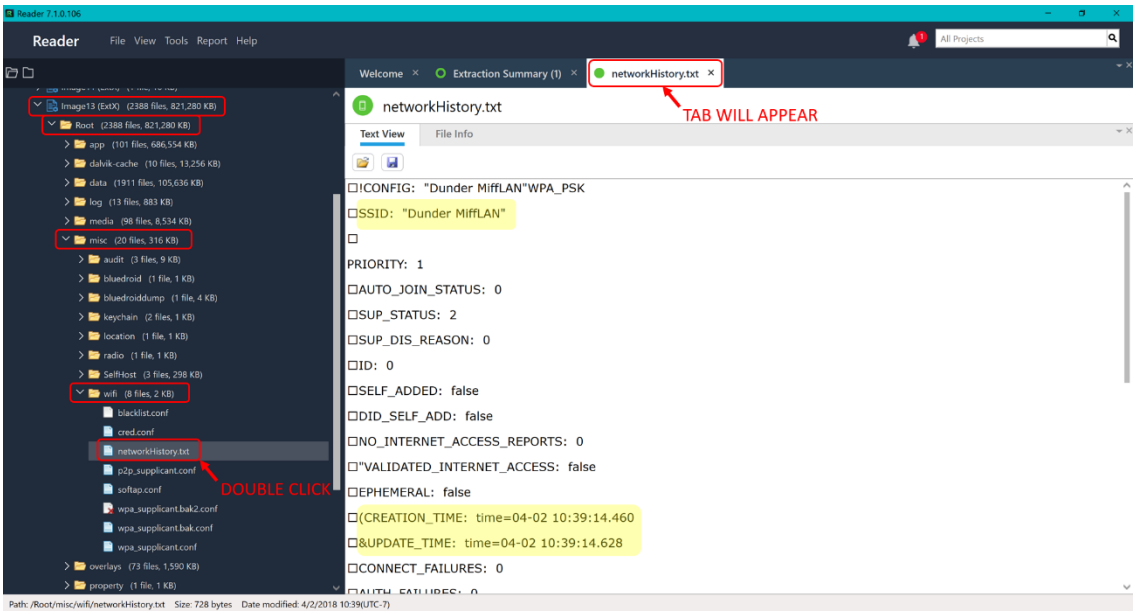


Figure 9-1: Ryan's Wireless SSID with Creation Time

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.

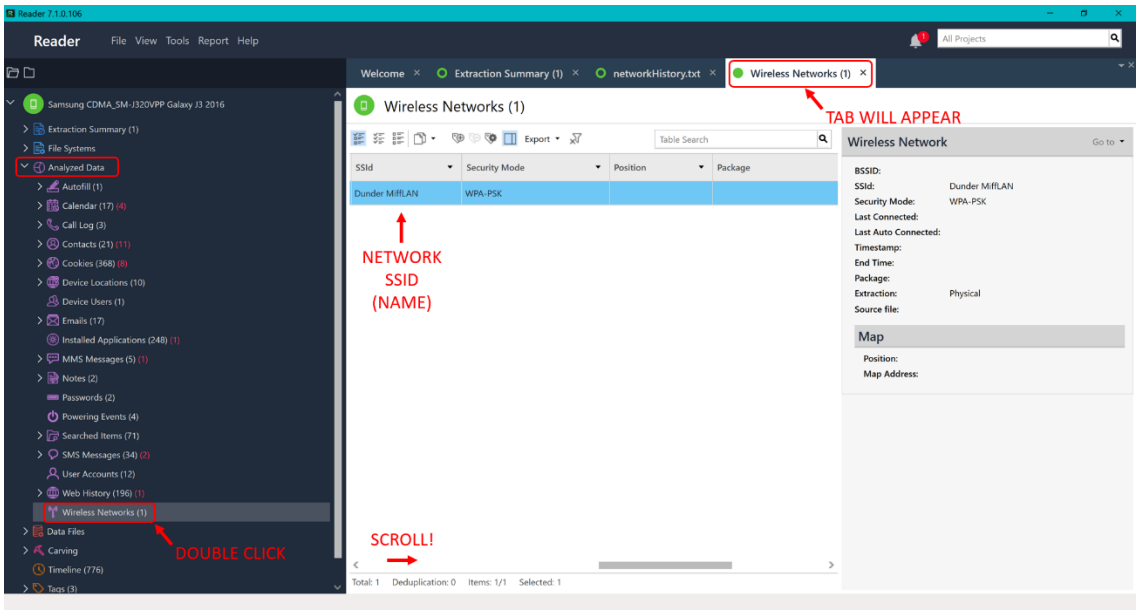


Figure 9-2: Another Location to View ONLY the SSID of Wireless Networks

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/`

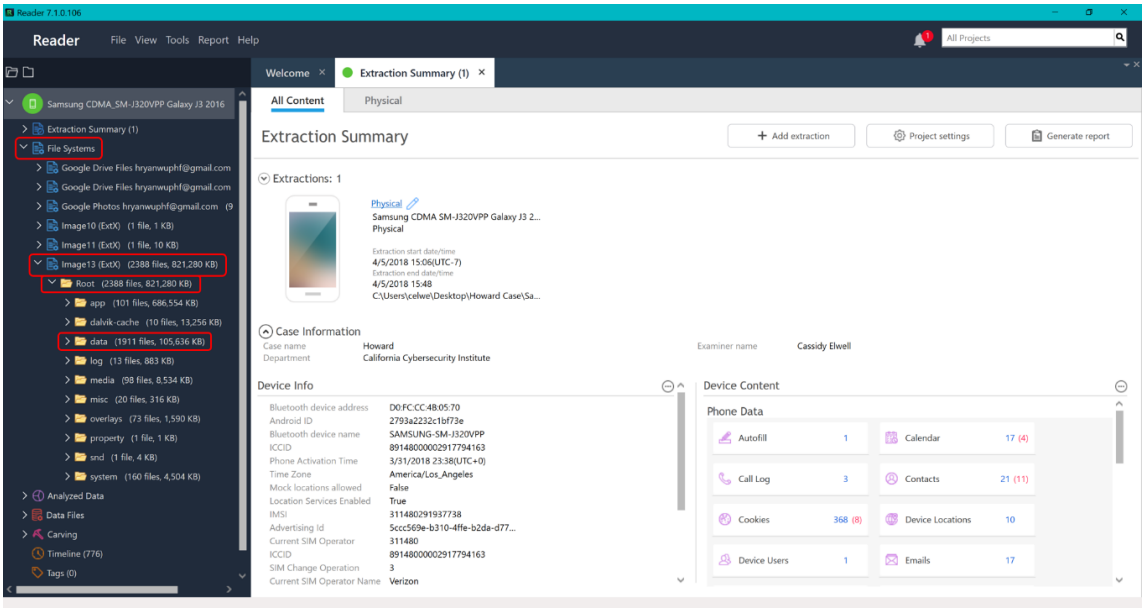


Figure 9-3: Navigation to Data Folder Containing Android Packages for Applications

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.

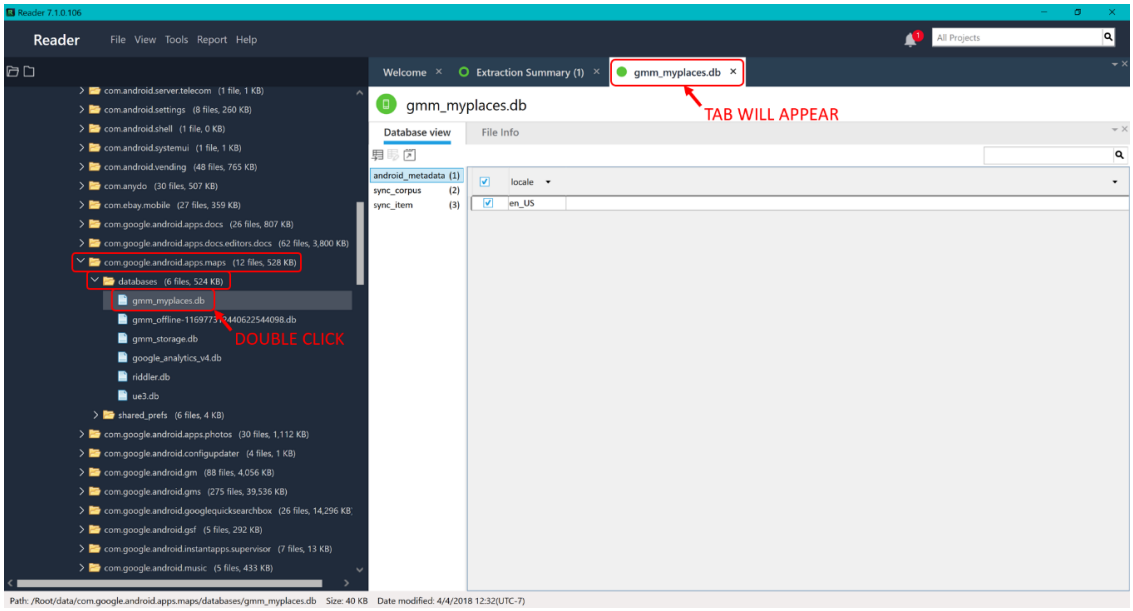


Figure 9-4: Ryan's Google Maps Places Database

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.

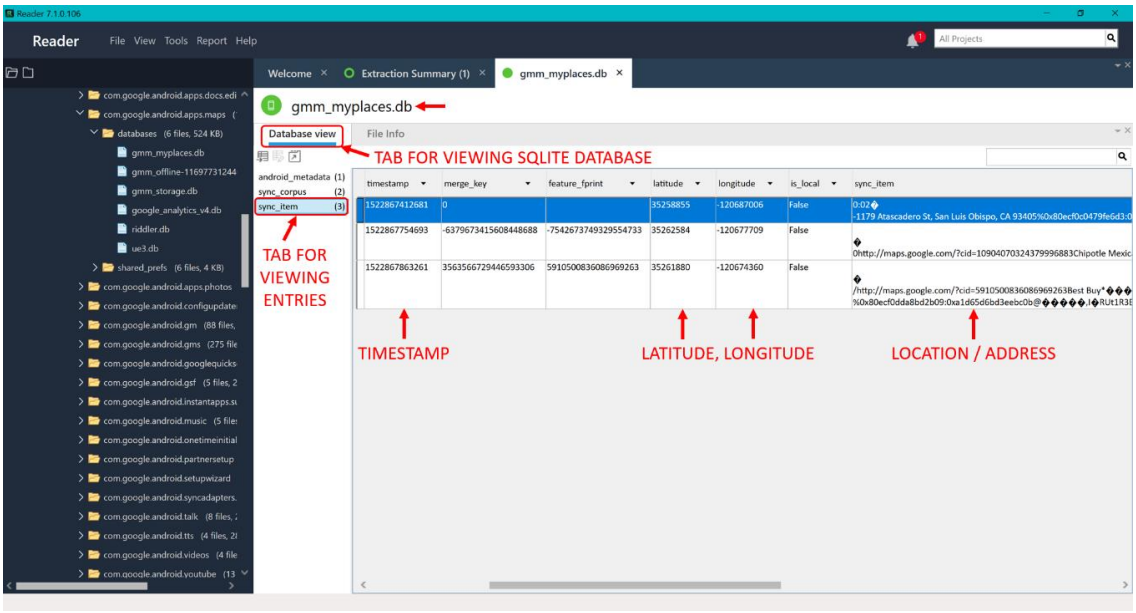


Figure 9-5: Viewing Database Entries Displays Timestamp, Latitude, Longitude, and Location/Address for Each Entry

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.

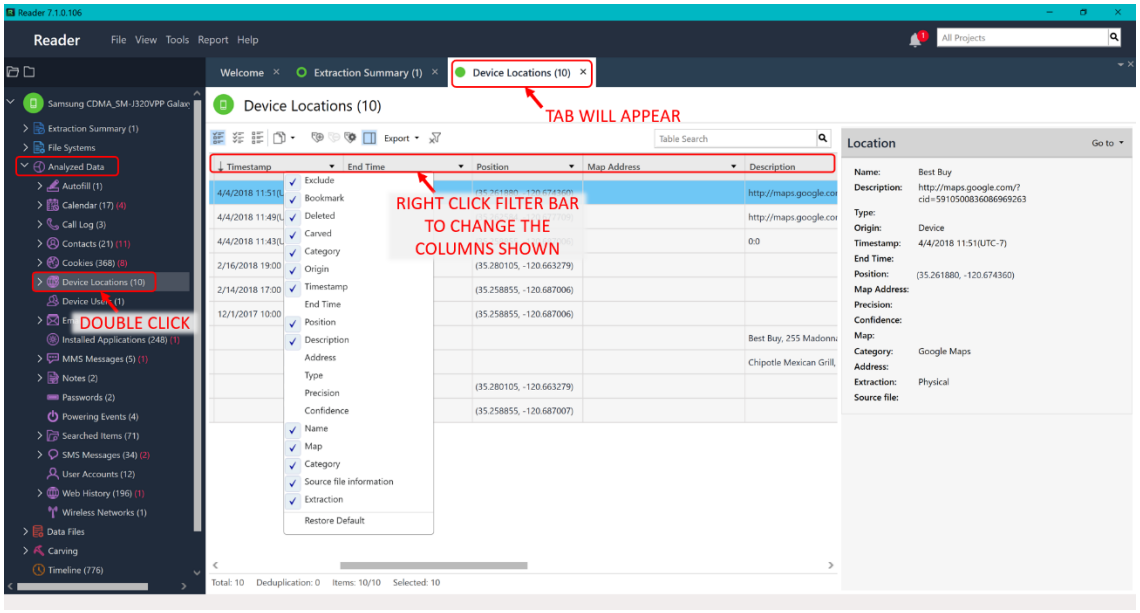


Figure 9-6: Ryan's Device Locations Displayed Collectively

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
```

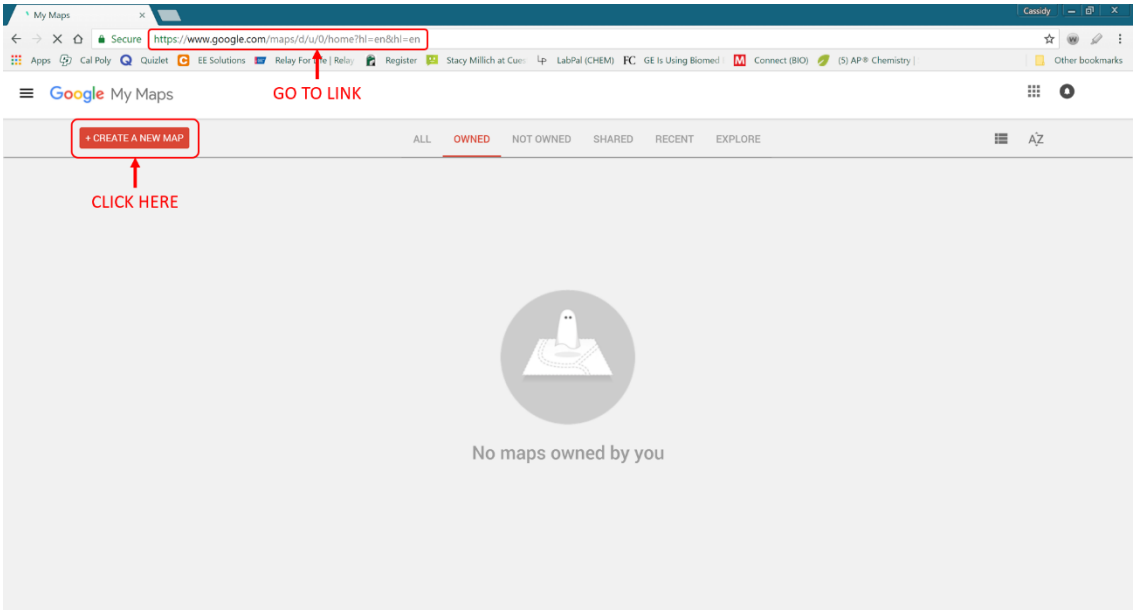


Figure 9-7: Create a New Map with Google

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.

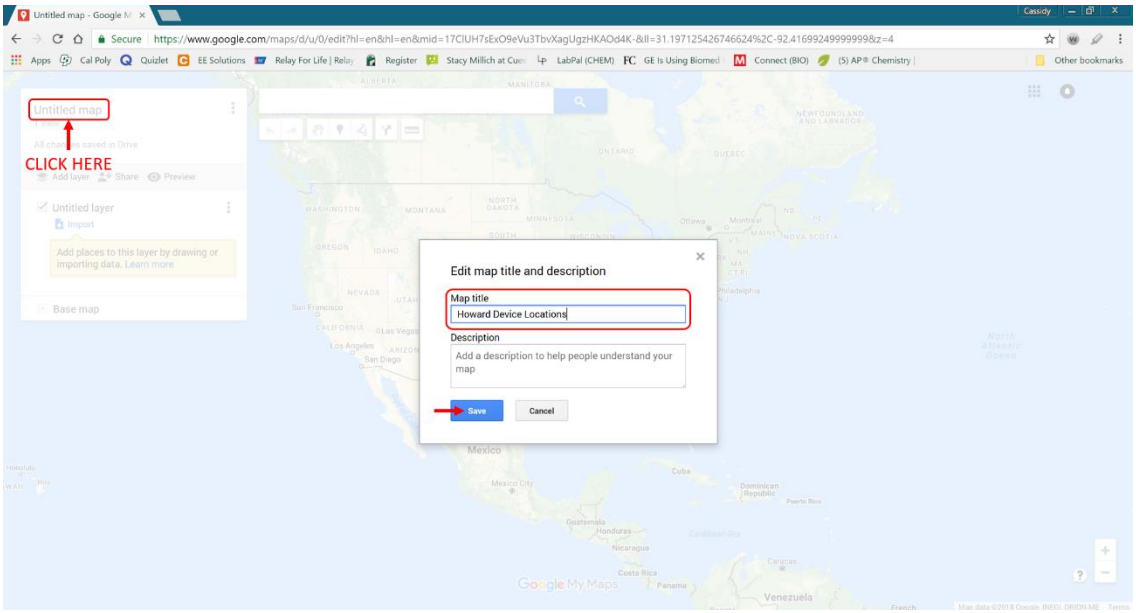


Figure 9-8: Name the Created Map such as "Howard Device Locations"

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

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

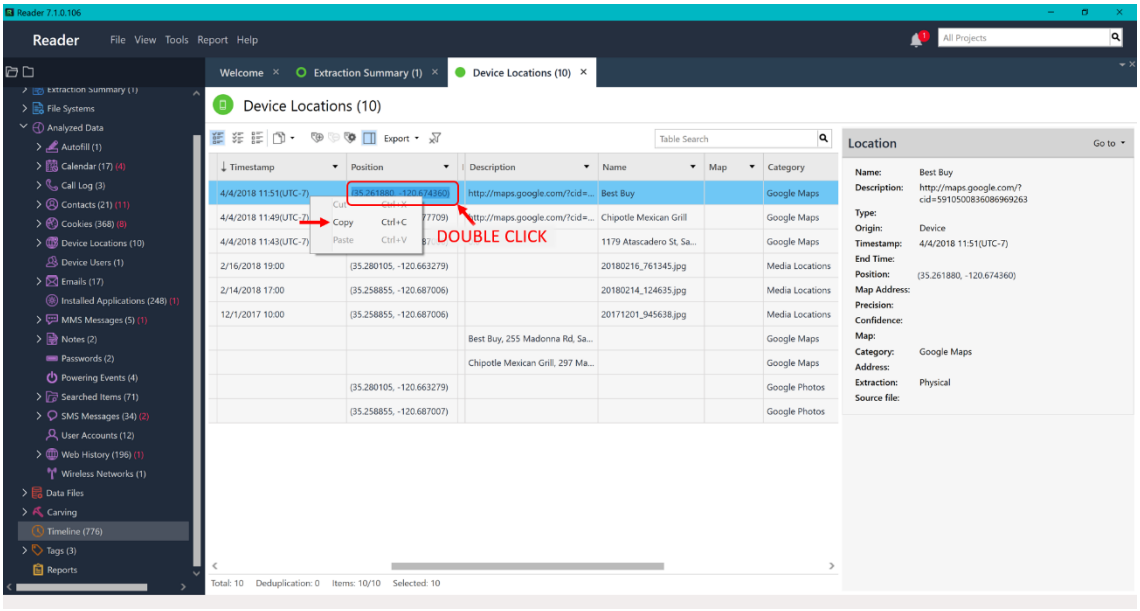


Figure 9-9: Copy Information of Entries from UFED Reader

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.

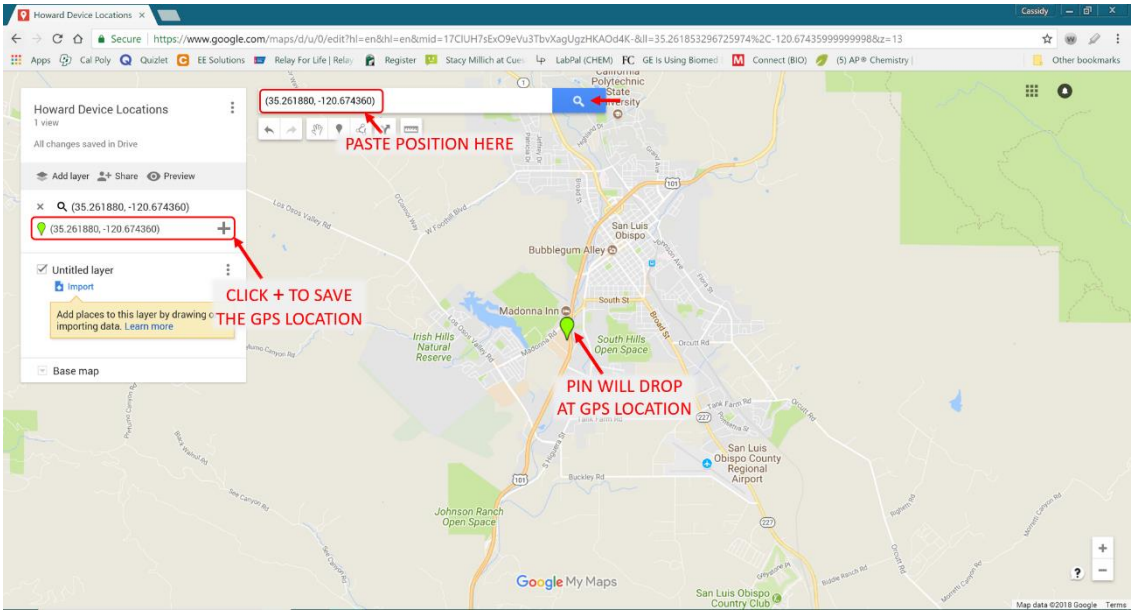


Figure 9-10: Paste Information in Created Map and Save GPS Location Pin

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.

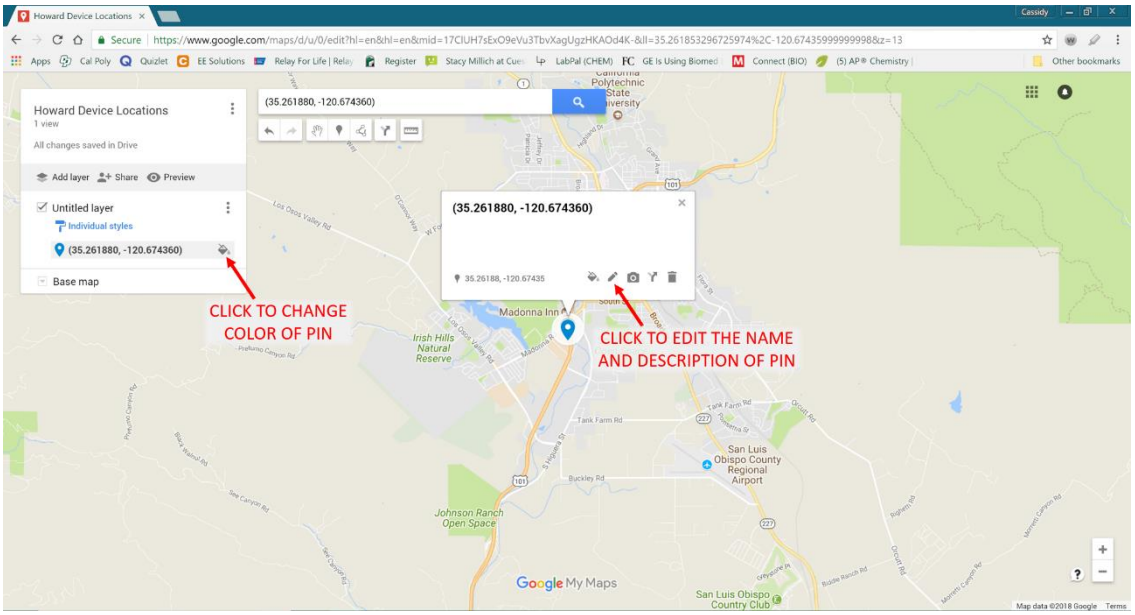


Figure 9-11: Select the Pin and Edit Details to Allow Proper Labeling

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.

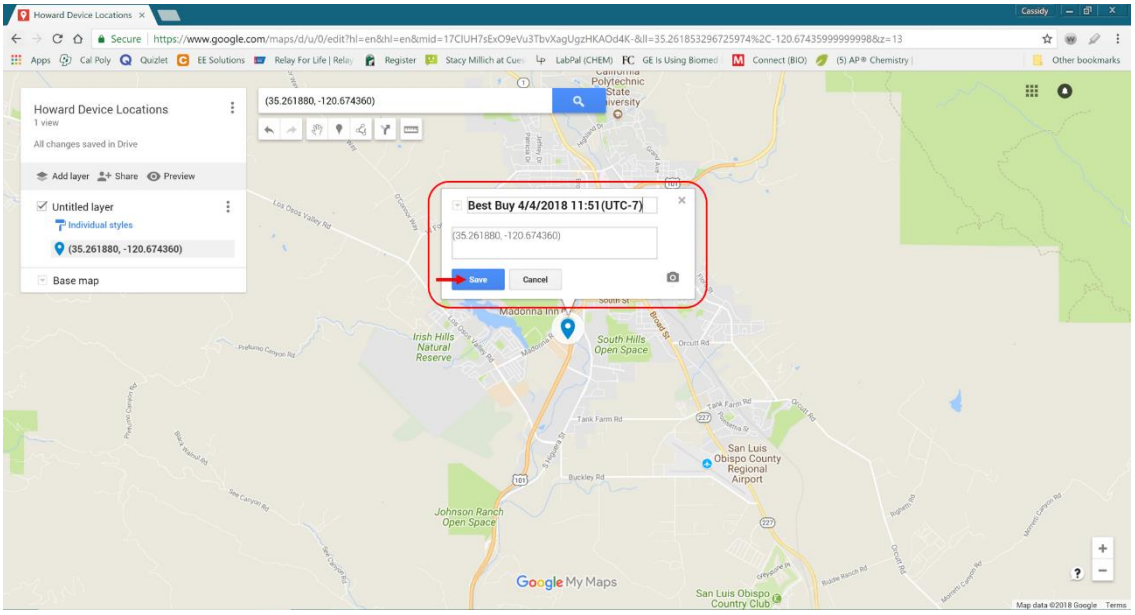


Figure 9-12: Label the Pin with Name, Timestamp, and Position with GPS Location Entry Information

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.

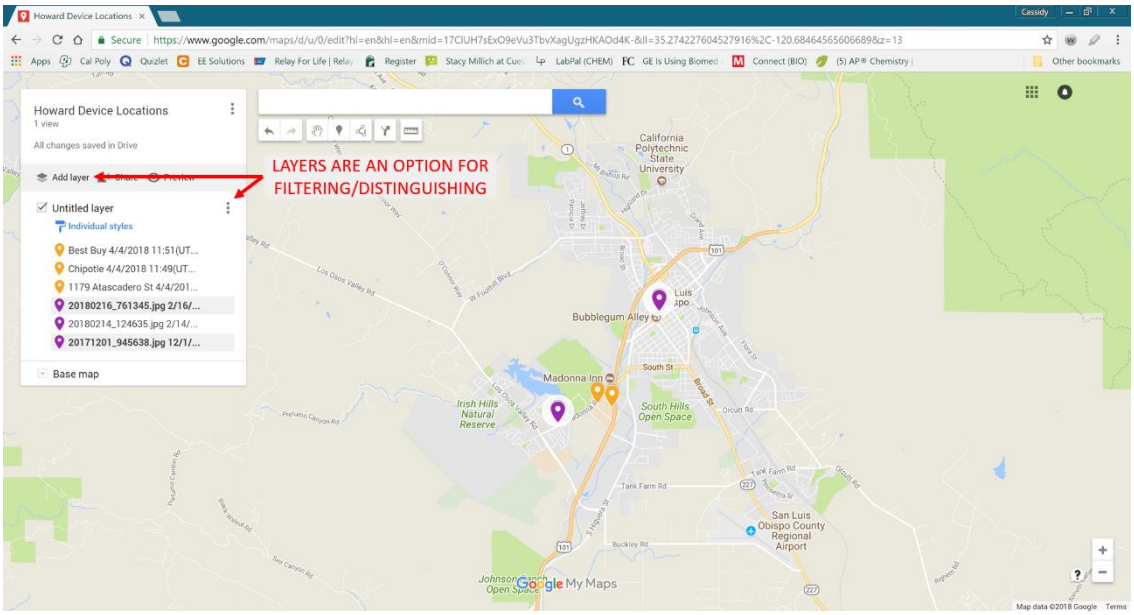


Figure 9-13: Created Map of Howard Device Locations and Layer Option Shown

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

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

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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:

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

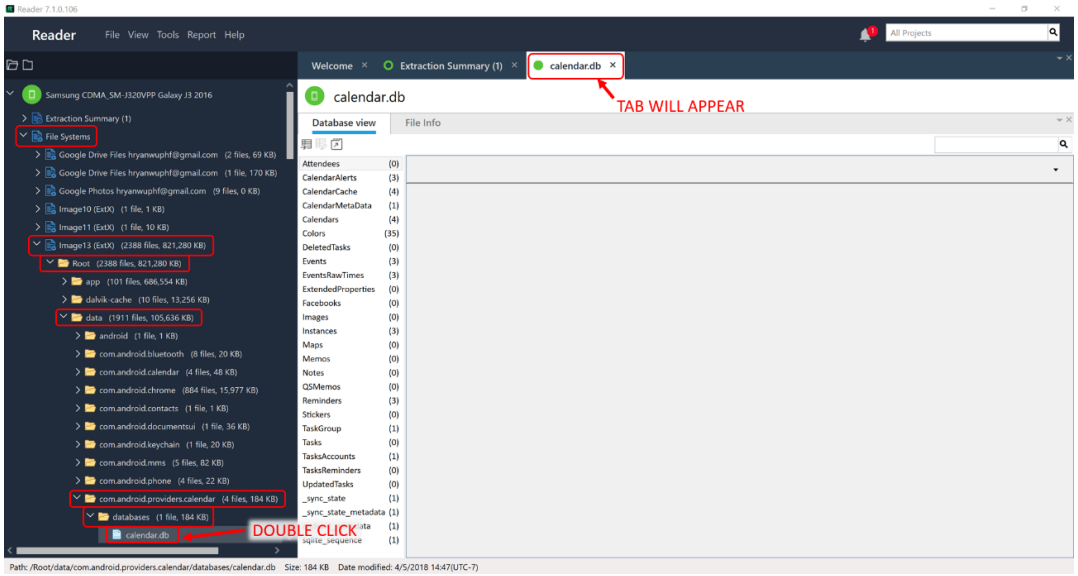


Figure 10-1: Calendar Data Including Associated Accounts and Saved Events

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."

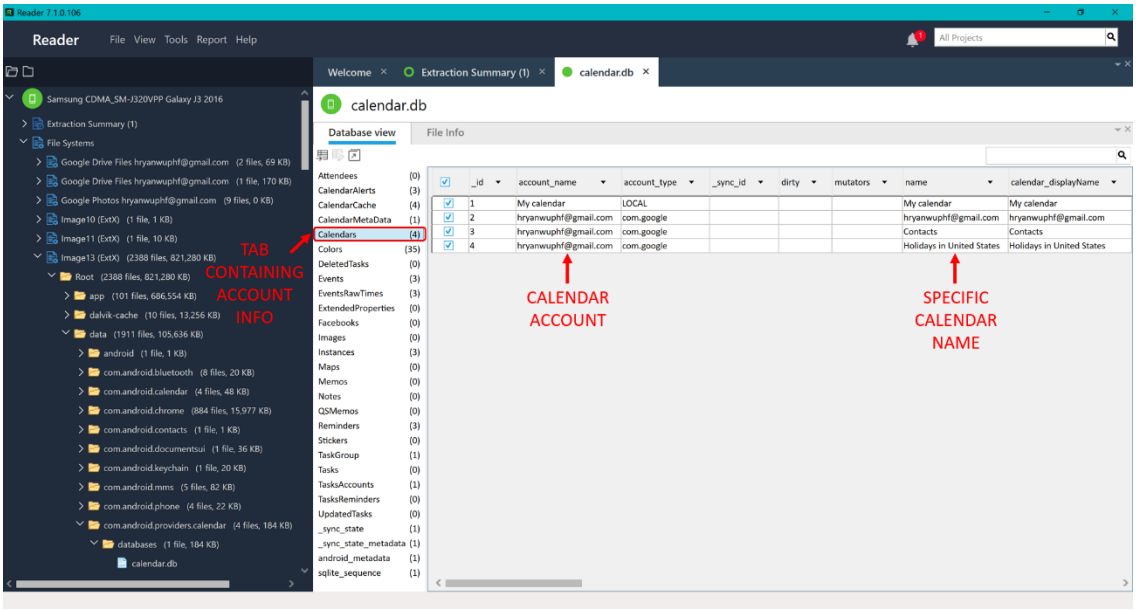


Figure 10-2: Calendar Accounts Logged into and the Specific Associated Calendars

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).

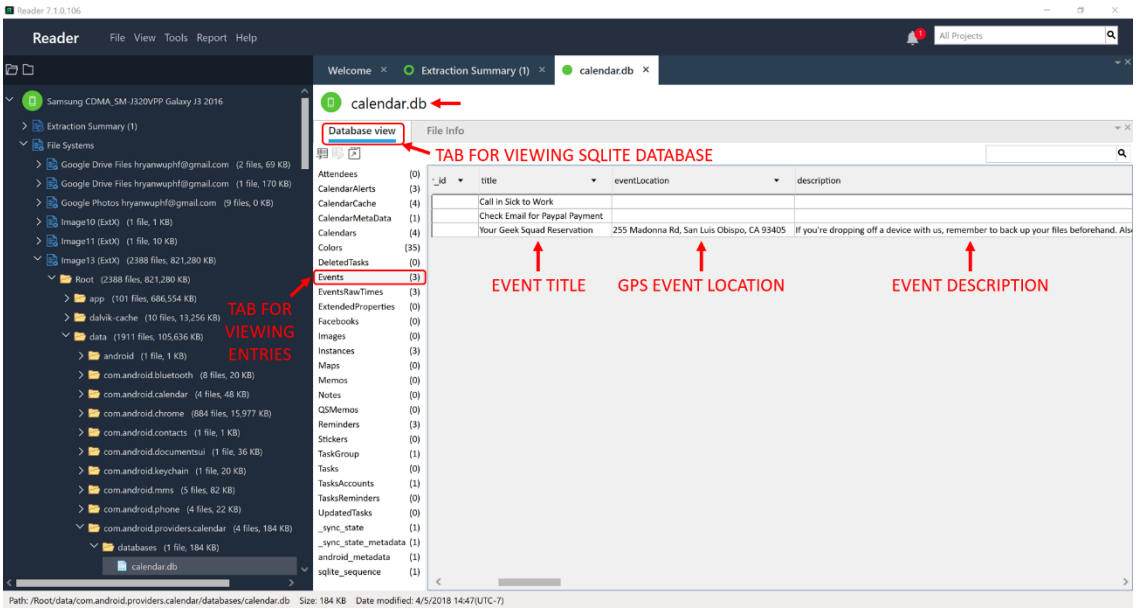


Figure 10-3: Viewing Database Entries Displaying Title, Location, and Description of Each Event

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.

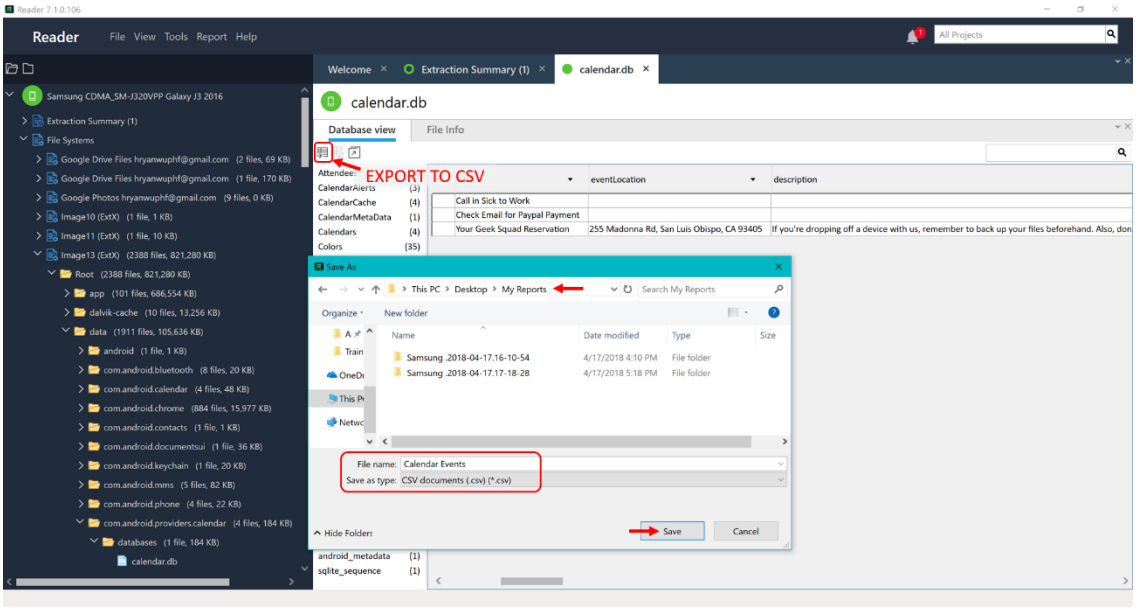


Figure 10-4: Export SQLite Database to CSV Containing Calendar Events

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.

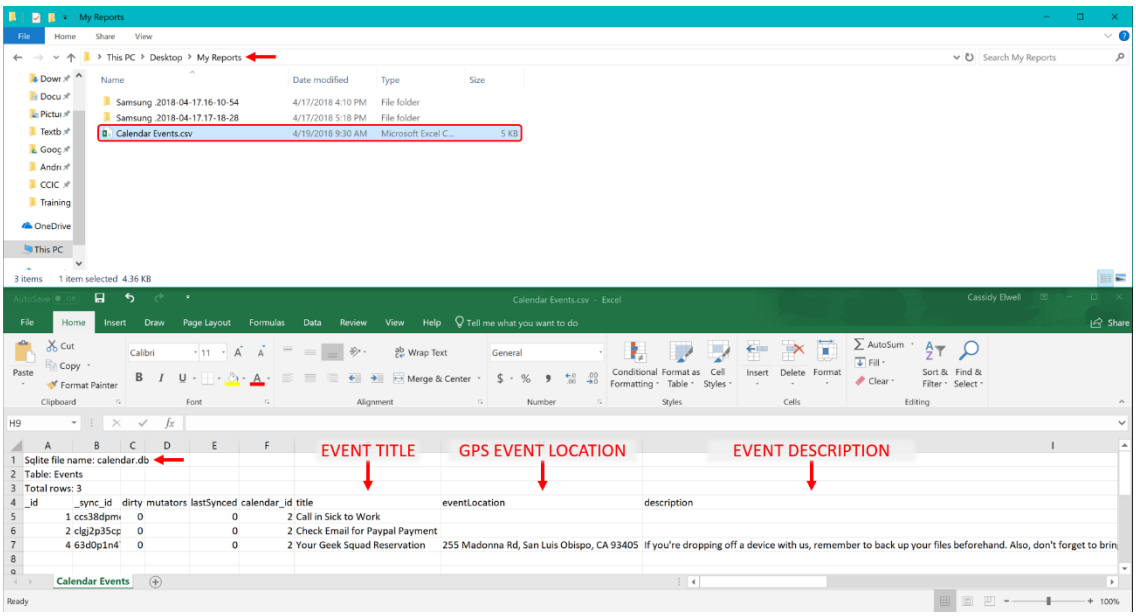


Figure 10-5: Open and View the Exported Calendar Data Easily with Microsoft Excel

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.

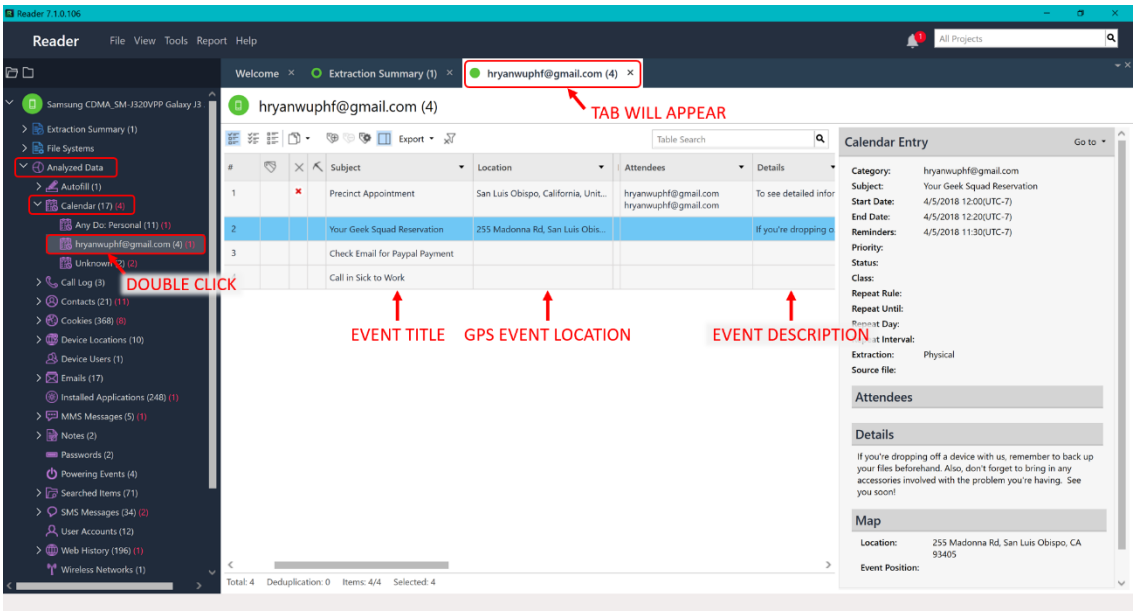


Figure 10-6: Another Location to View Calendar Data from Gmail Account(s)

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/
```

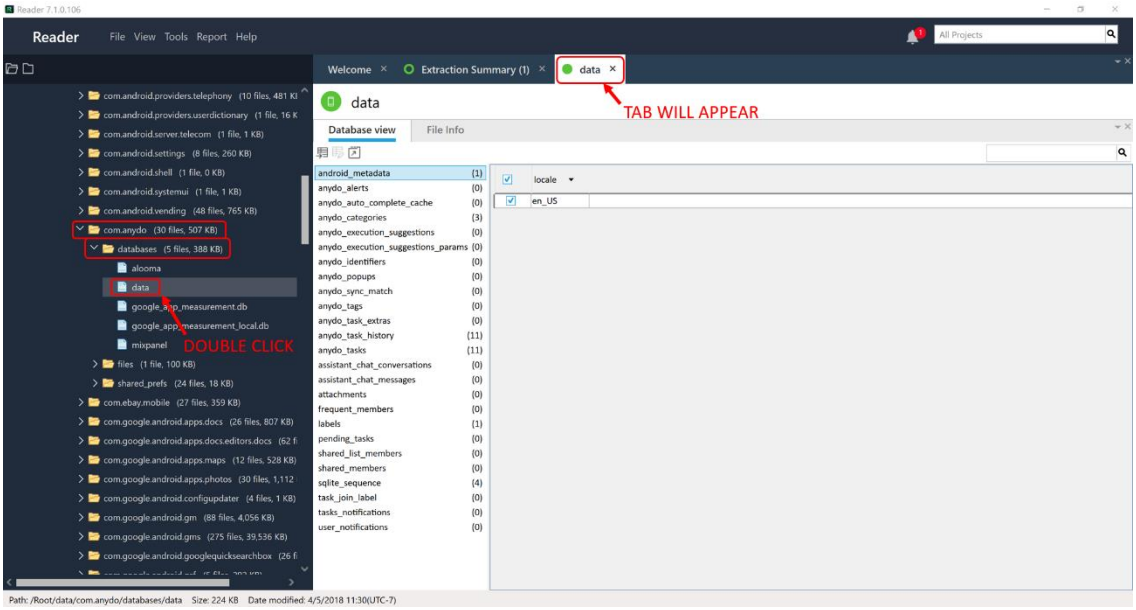


Figure 10-7: Any.do List Application Data for Ryan

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.

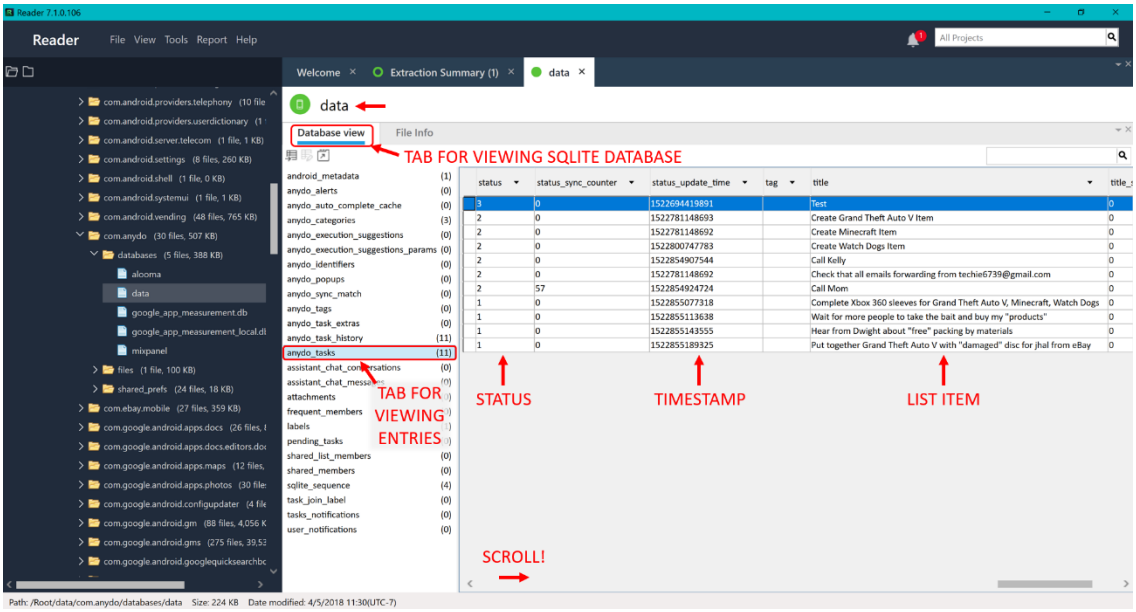


Figure 10-8: Each Any.do Task is Stored with its Creation Time and Status

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.

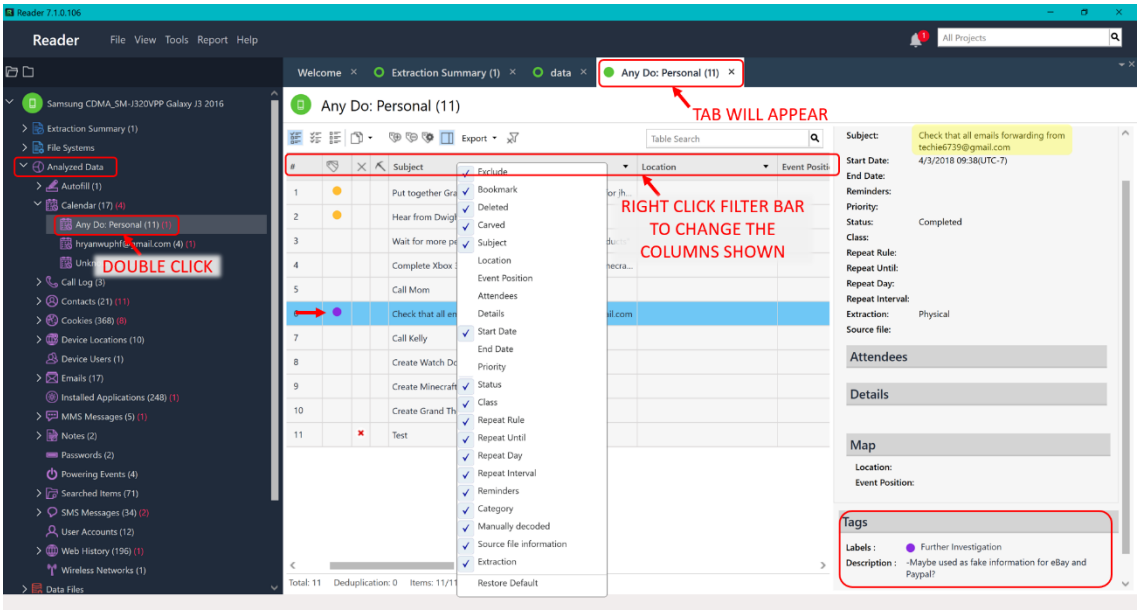


Figure 10-9: Another Location for Viewing (and Filtering) Any.do Tasks

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/`

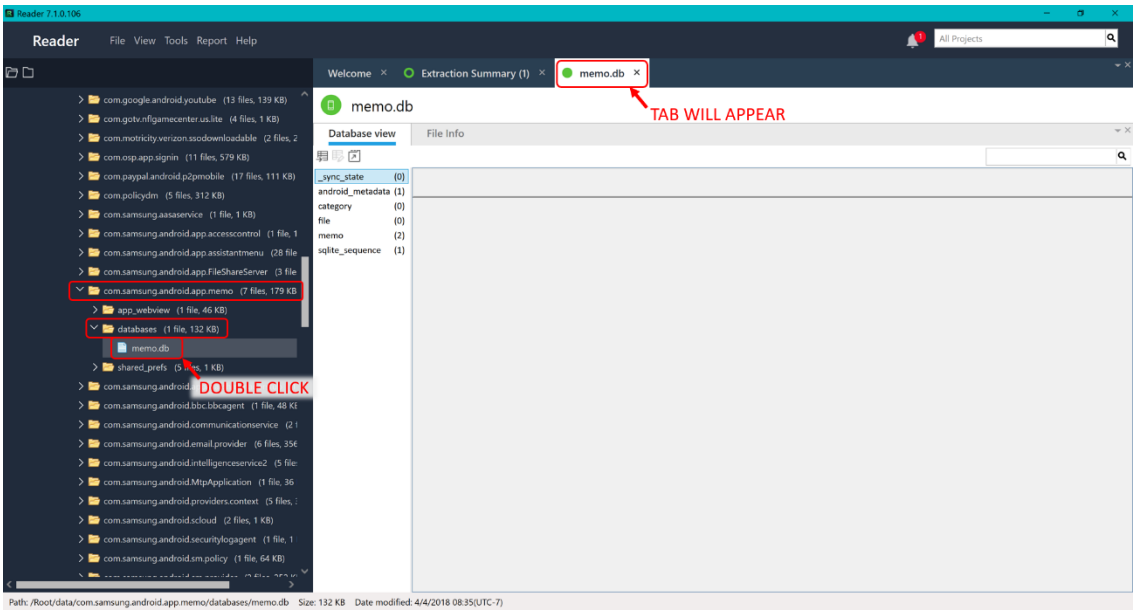


Figure 10-10: Samsung Notes SQLite within File System

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.

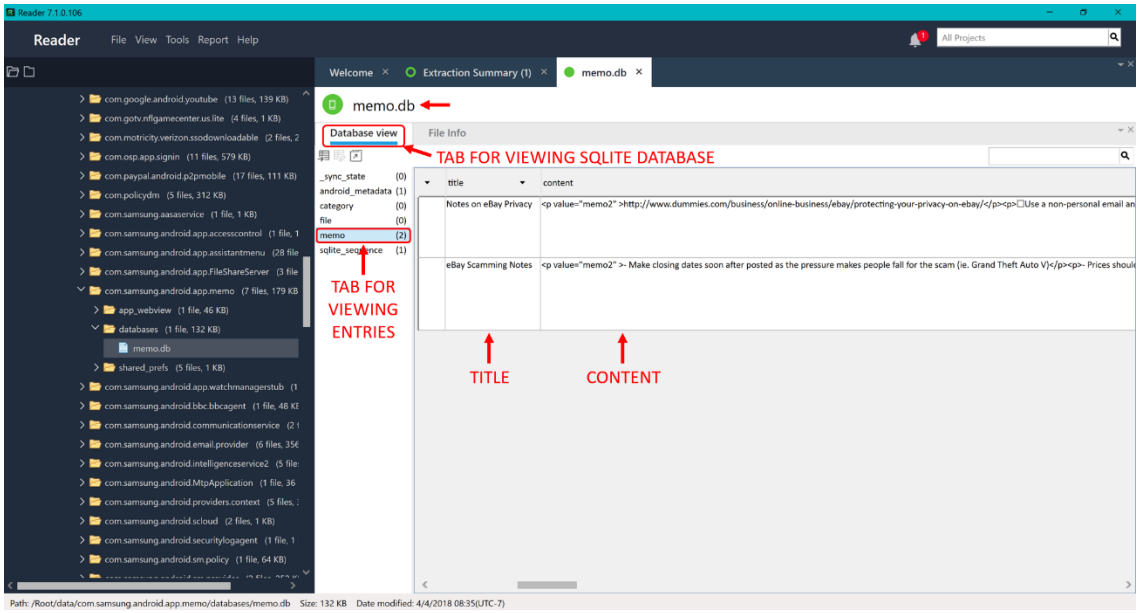


Figure 10-11: Individual Memos Stored within Samsung Notes by Ryan

This information can also be viewed within:

```
/Analyzed Data/Notes/Samsung Notes/
```

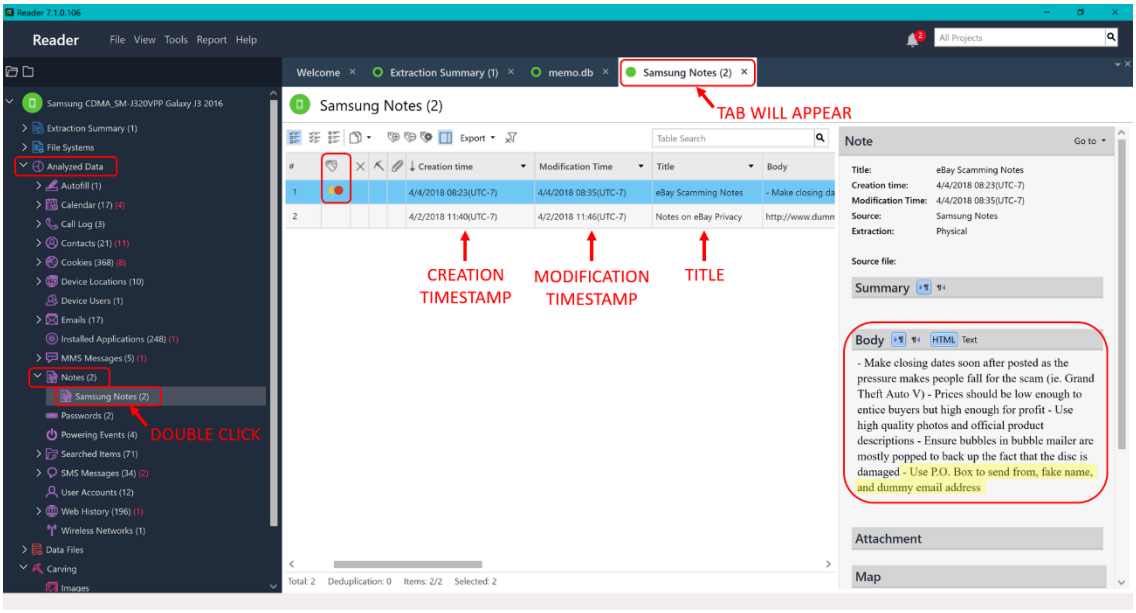


Figure 10-12: Ryan's Samsung Notes Contains Investigation Critical Information

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.

CAL POLY

California Cybersecurity Institute

Android Forensics CCIC Training

Chapter 11: Email and Internet History

Cassidy Elwell and James Poirier

May 2019 (Version 2)

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/
```

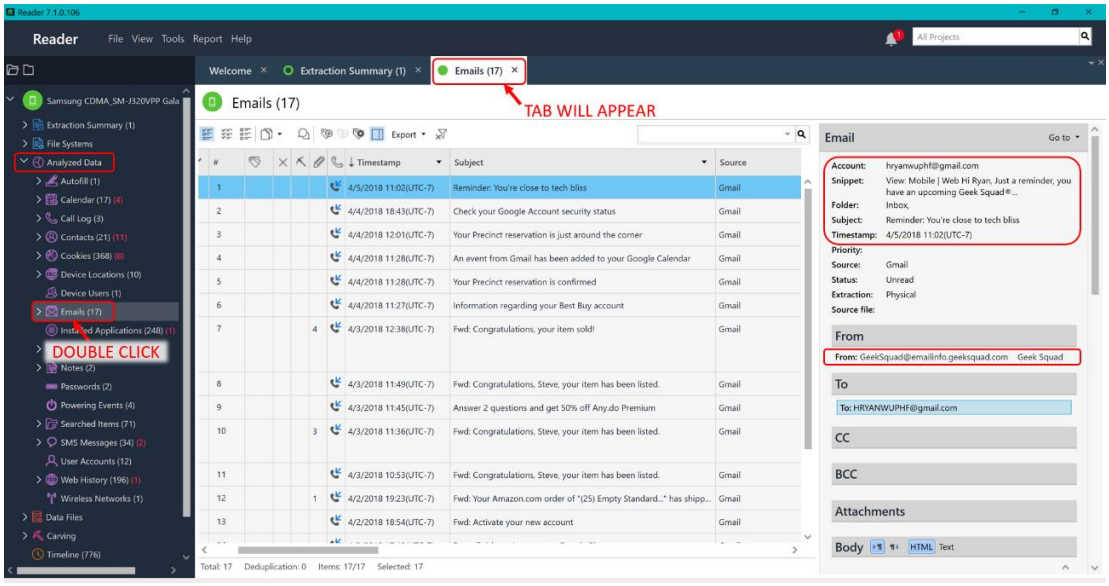


Figure 11-1: Emails are Listed in a Filterable Table

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.

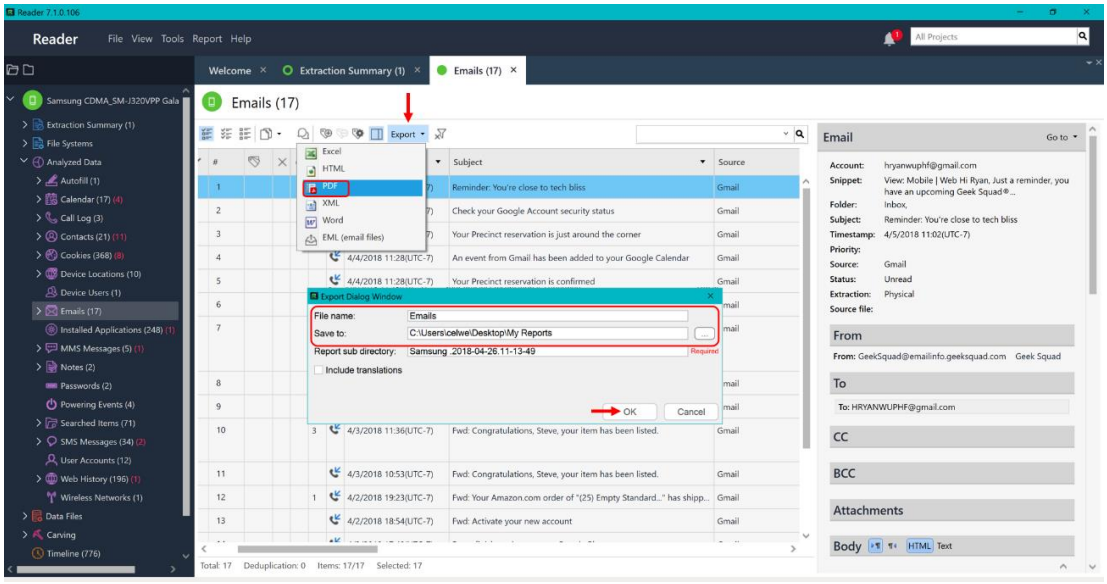


Figure 11-2: Export Emails for Investigation as Formatted on Device

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.”

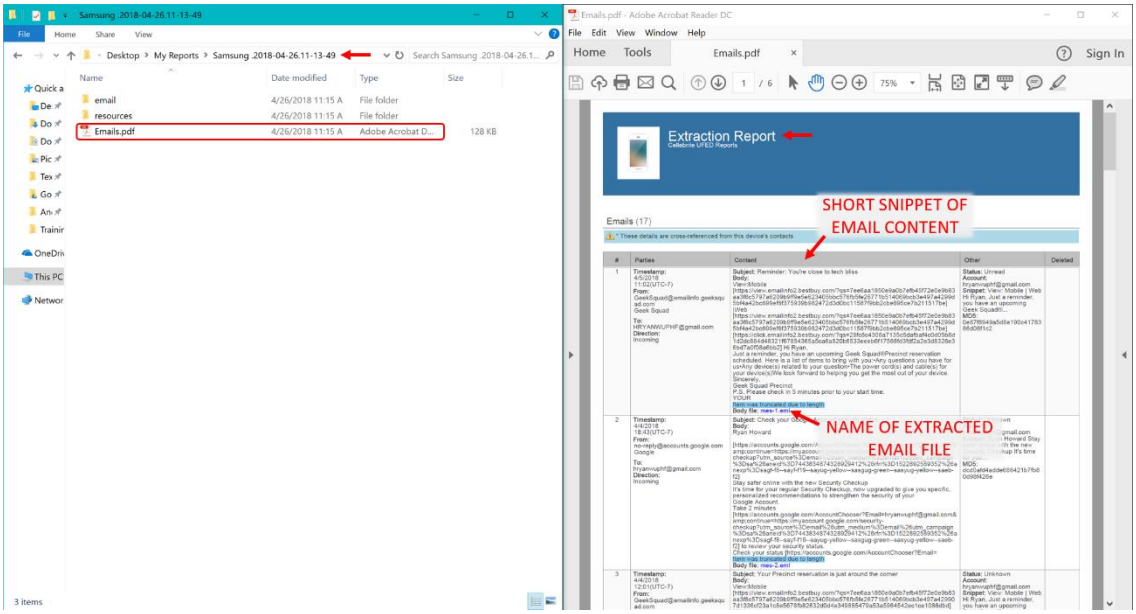


Figure 11-3: Extraction Report of Emails from Device

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.

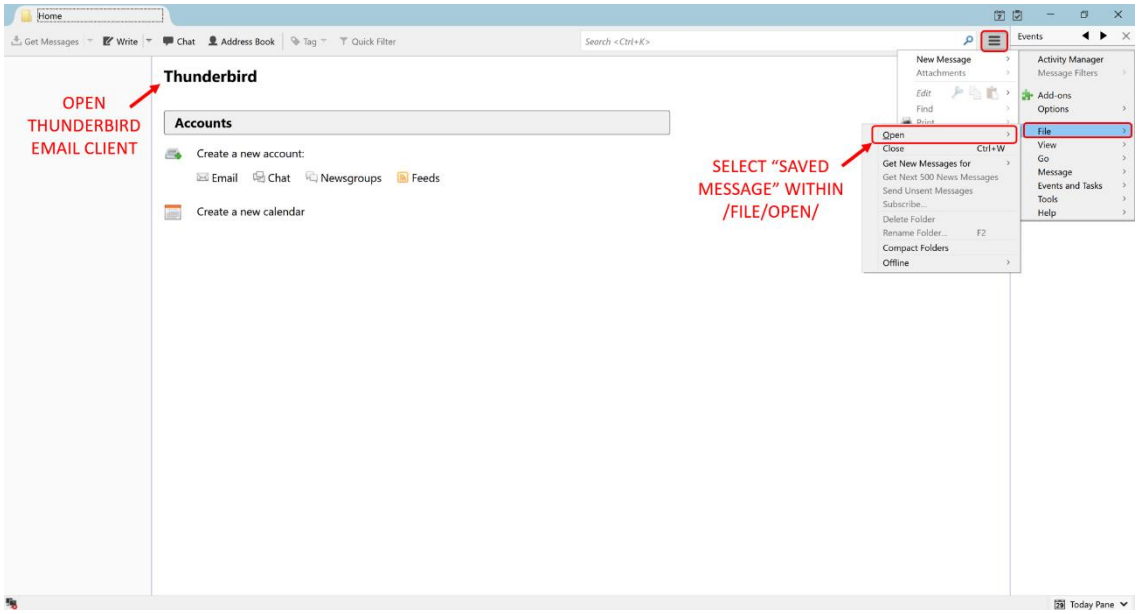


Figure 11-4: Thunderbird Mail Opening a Saved Message

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/`

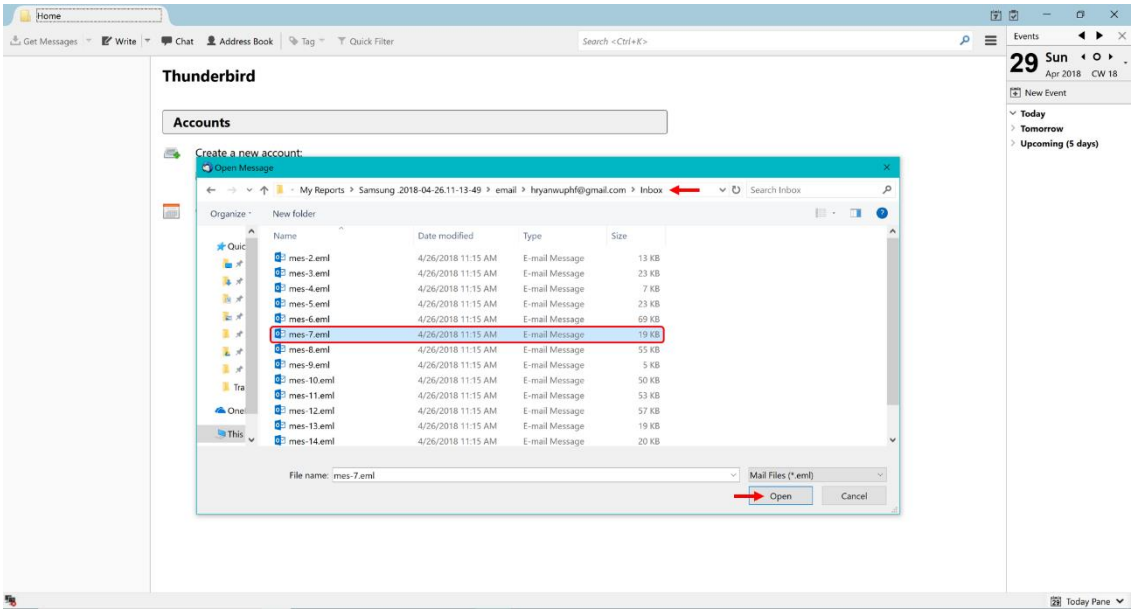


Figure 11-5: Select the Saved Message of Interest in Thunderbird Mail

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.

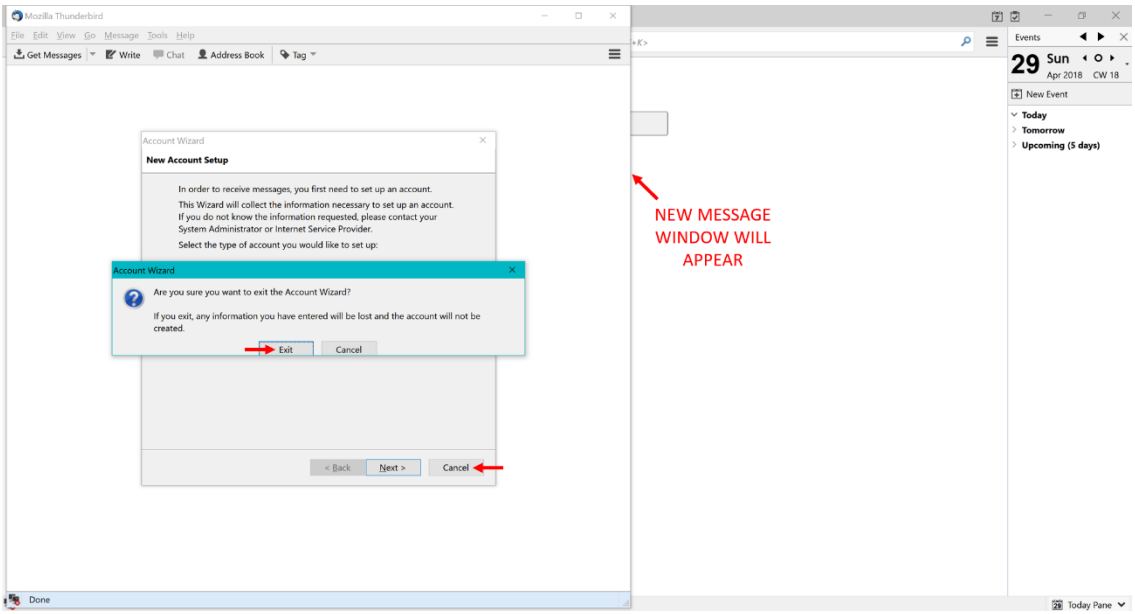


Figure 11-6: By-Pass Logging into Email Account in Thunderbird

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.

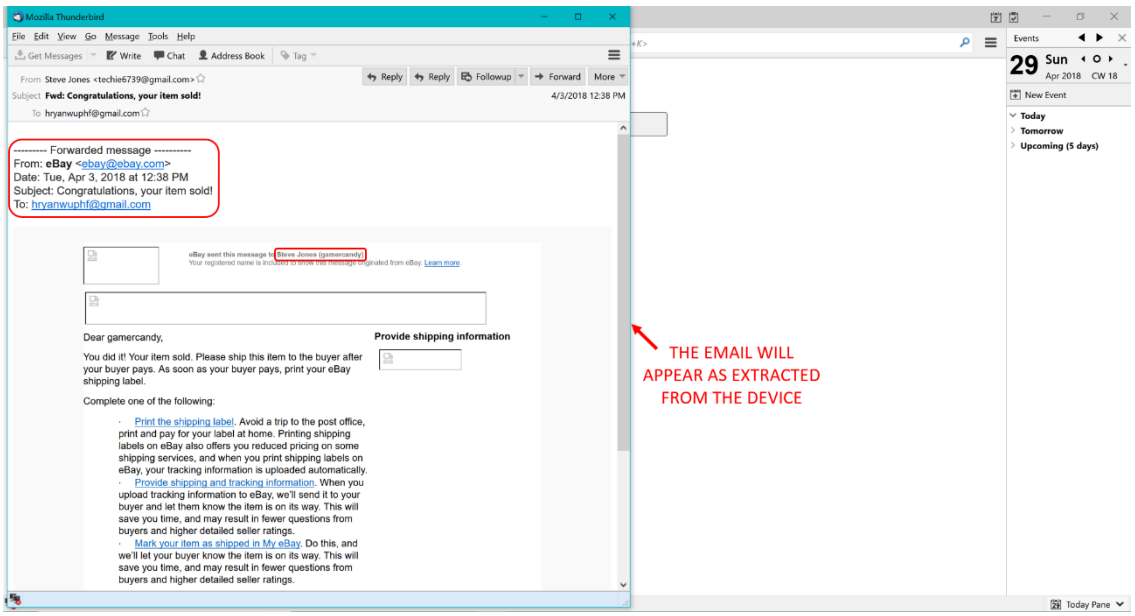


Figure 11-7: Email Message 7 From Inbox Displaying eBay Fake Information

Internet History

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

```
/Analyzed Data/Web History/
```

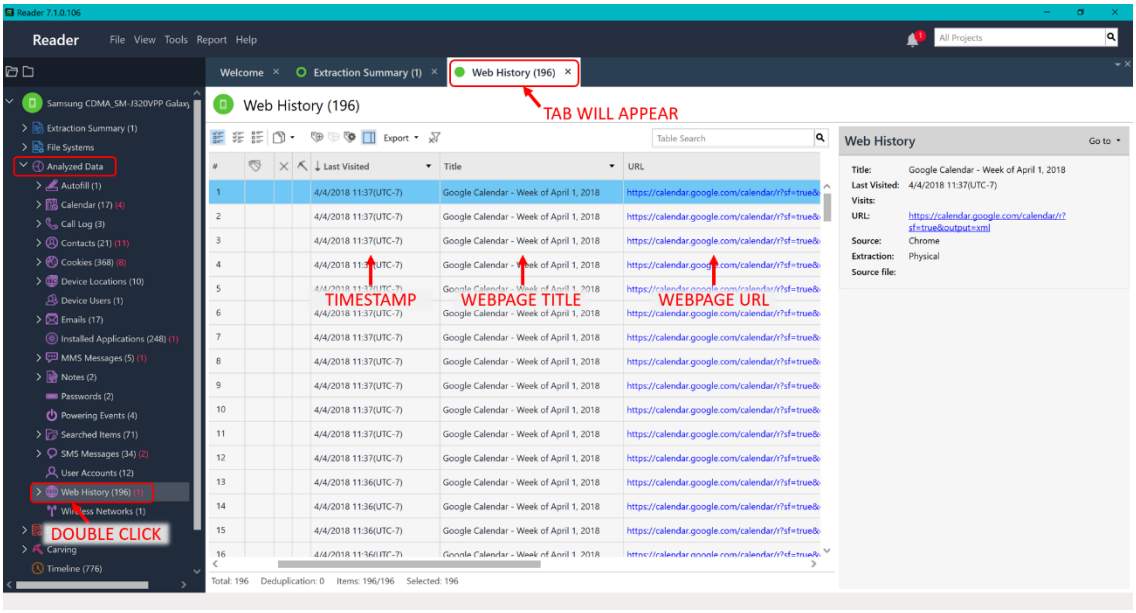


Figure 11-8: Web History Includes Webpages Visited with the Title and URL

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.

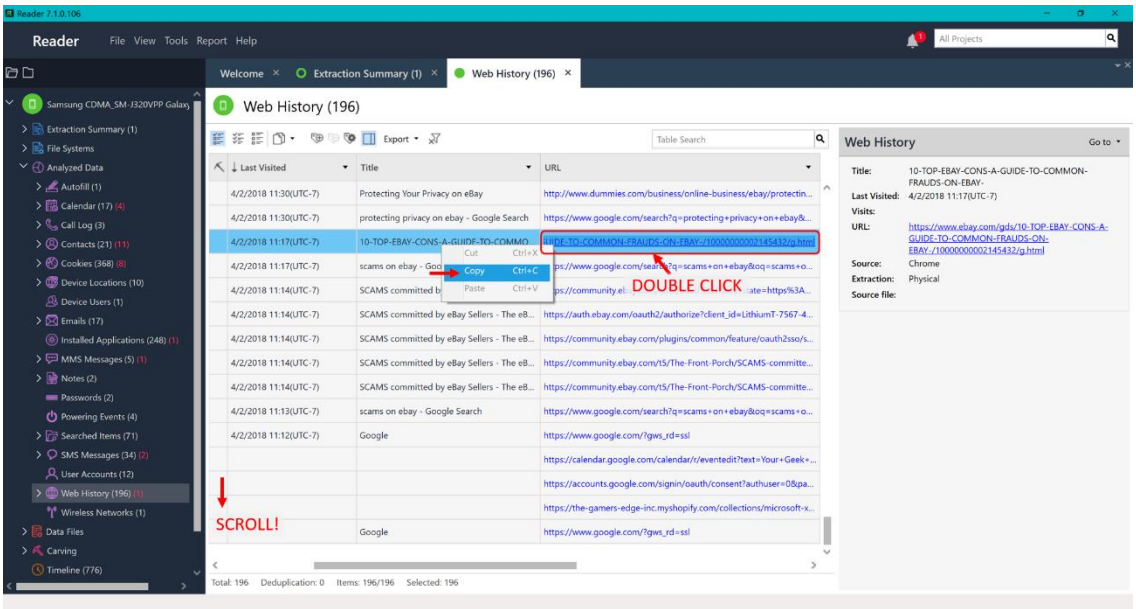


Figure 11-9: Double Click on the URL to Copy the Visited Webpage

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.

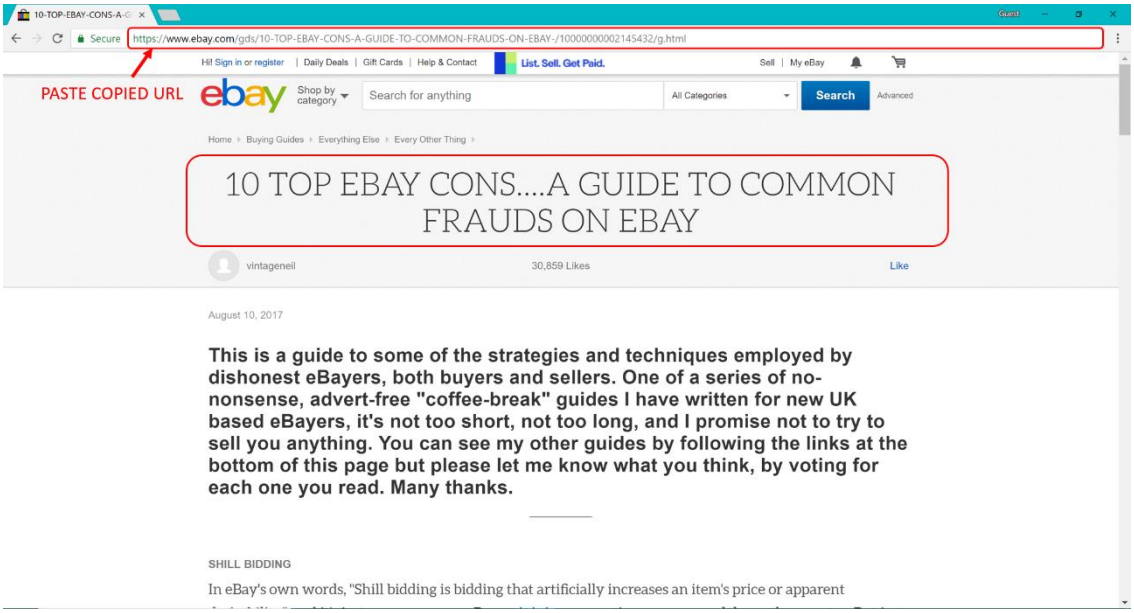


Figure 11-10: Paste the Copied Webpage URL into a Browser to View

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

```
/Analyzed Data/Searched Items/
```

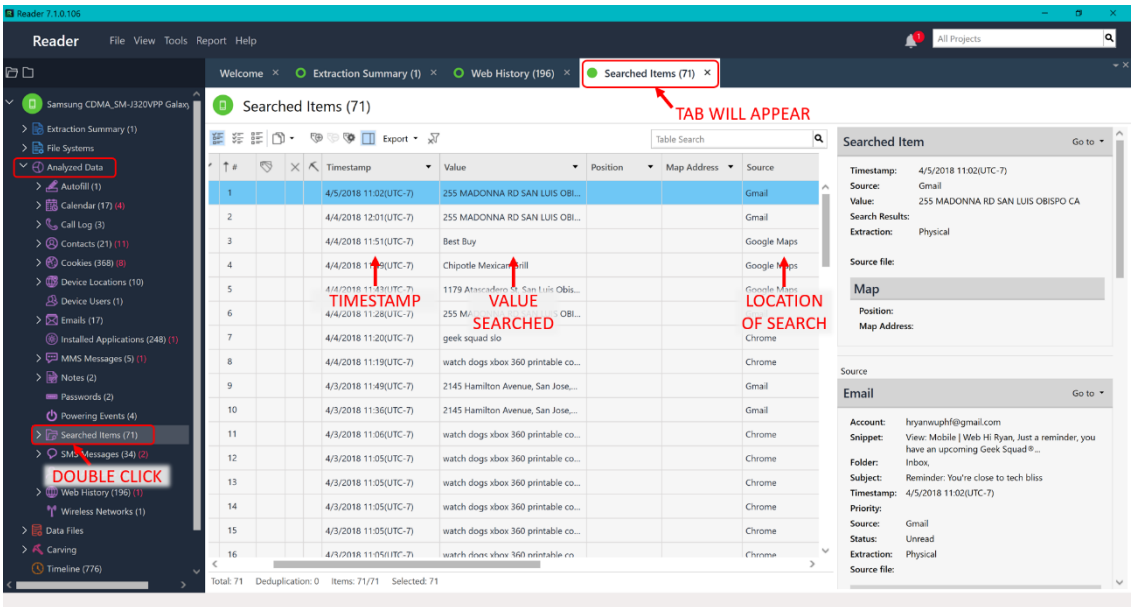


Figure 11-11: Items Searched within Applications are Stored

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.

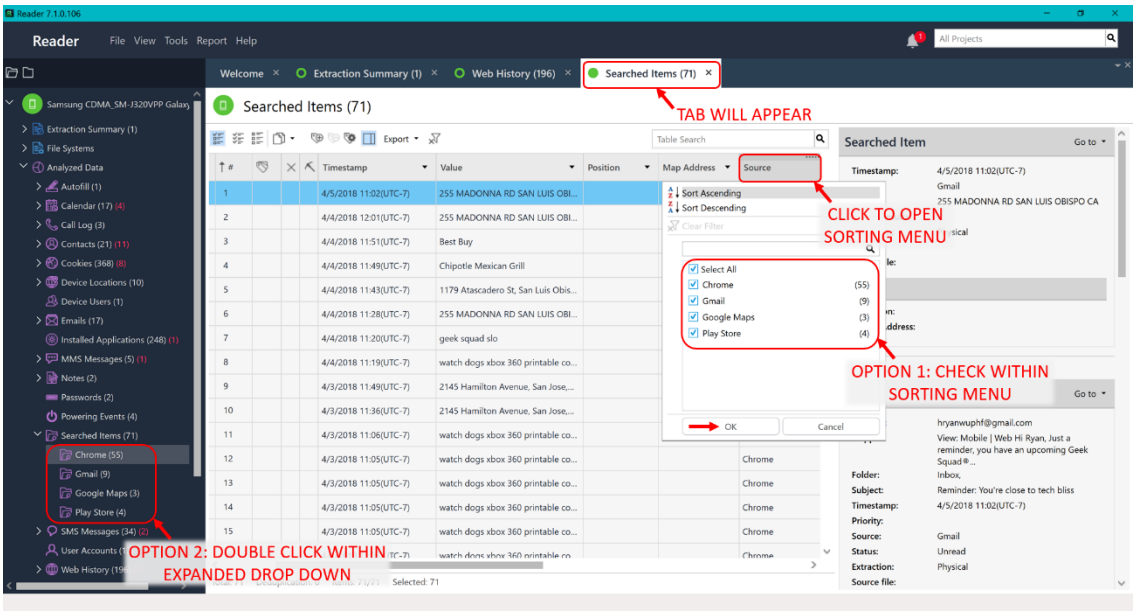


Figure 11-12: Two Options for Sorting Searched Items