



FORENSICS V2 LAB SERIES

Lab 16: Mobile Forensic Analysis

Document Version: 2021-01-11

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and other countries. Google is a registered trademark of Google, LLC. Amazon is a registered trademark of Amazon in the United States and other countries.

Contents

| | |
|---|----|
| Introduction | 3 |
| Objectives..... | 3 |
| Lab Topology | 4 |
| Lab Settings | 5 |
| 1 Identifying and Extracting Mobile Artifacts | 6 |
| 2 View the extracted mobile artifacts | 28 |

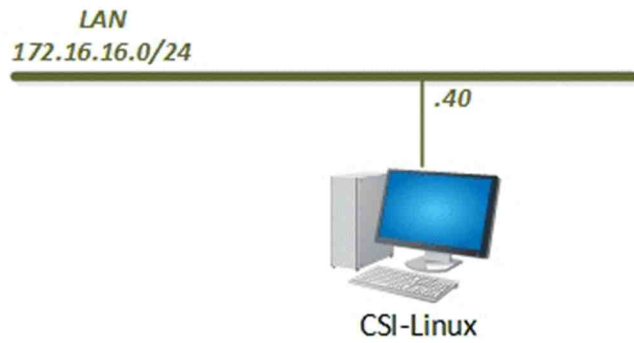
Introduction

If there ever is a digital evidence source that can tell a story of its owner, then that source is a smartphone. This module will teach how to access the insurmountable amount of data stored within android smartphones

Objectives

-) Learn to identify device details
-) Learn how to find different types of data in databases
-) Learn how to navigate an Android file system

Lab Topology



Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

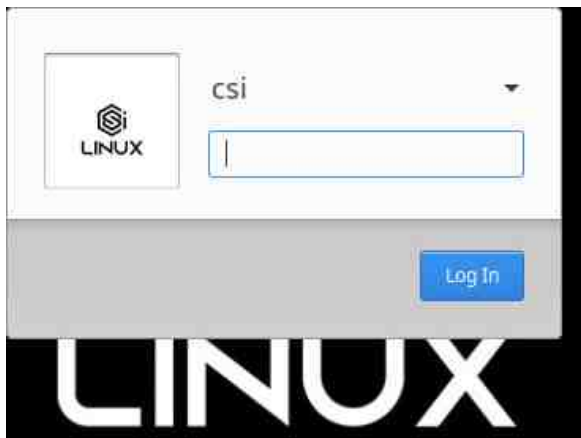
| Virtual Machine | IP Address / Subnet Mask | Account (if needed) | Password (if needed) |
|-----------------|--------------------------|---------------------|----------------------|
| Caine | 172.16.16.30 | caine | Train1ng\$ |
| CSI-Linux | 172.16.16.40 | csi | csi |
| DEFT | 172.16.16.20 | deft | Train1ng\$ |
| WinOS | 172.16.16.10 | Administrator | Train1ng\$ |

1 Identifying and Extracting Mobile Artifacts

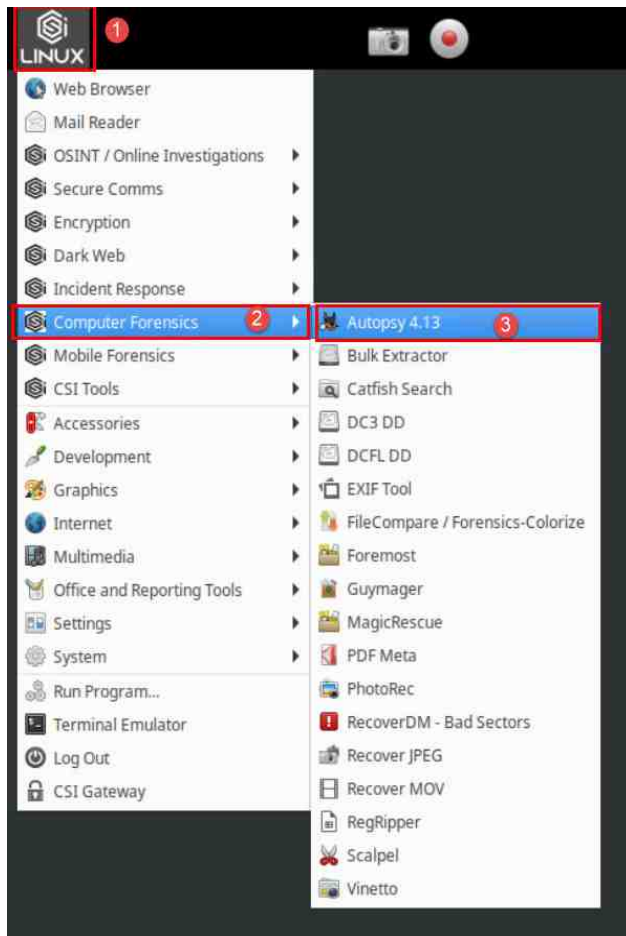
Mobile forensics is one of the most popular categories of digital forensics. It has earned its popularity due to the significance of the data that is created on these devices. They can tell a user's location, associates, likes, or dislikes, and much more. In this lab, we will take you through a physical image of a Samsung Galaxy S2 device and show you just how much data can be extracted using free tools and some know-how. The physical image is the best extraction you can get from a cell phone and is akin to a physical image of a hard drive. Many phones currently in use only support logical or advanced logical extractions, which provide access to a lot of system data; however, the physical is much more complete as it includes data in deleted space. Whenever possible, always try to get a physical image. We will be using Autopsy to process and review the data from the phone.

Let us get started by opening Autopsy and loading a FEF.

1. To begin, launch the CSI-Linux virtual machine to access the graphical login screen. Log in as `csi` using the password: `csi`



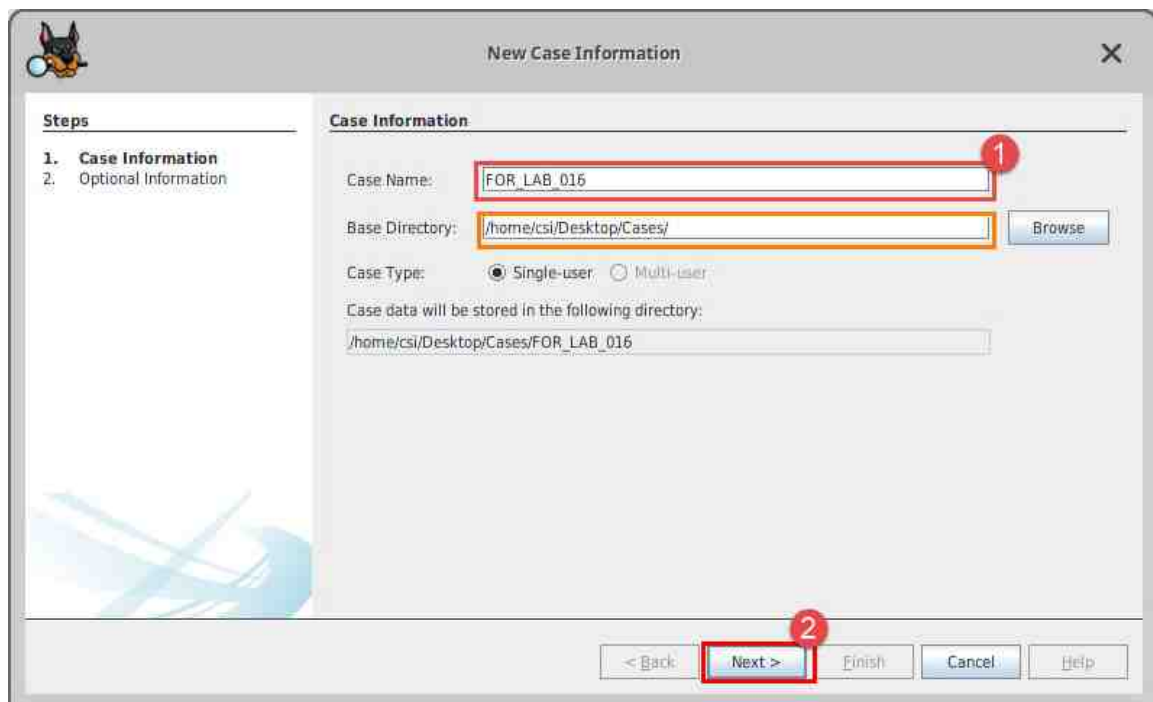
2. Once you are logged into the VM, launch the Autopsy program from the Start menu by navigating to Application Menu (Top left corner) > Computer Forensics > Autopsy 4.13. Alternatively, you can open Autopsy from the taskbar by clicking the Autopsy icon.



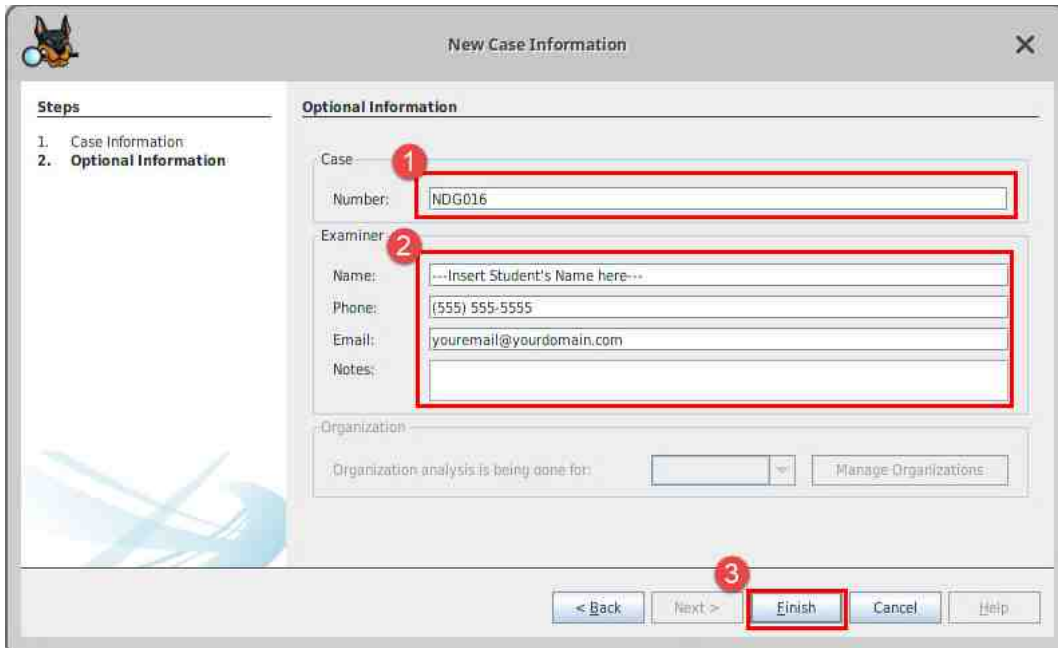
- Since you are already familiar with Autopsy, let us jump right in by creating a new case. In Autopsy, click the New Case option from the welcome screen as seen in item 1 OR Select > New Case, equally you can press Ctrl+N as highlighted in items 2 and 3 below. This will open the New Case Information window.



- In the New Case Information window, enter FOR_LAB_016 in the Case Name field. The Base Directory field is used to choose the location of the case folder. Let us leave that default selection and click Next as highlighted items 1 and 2 below.

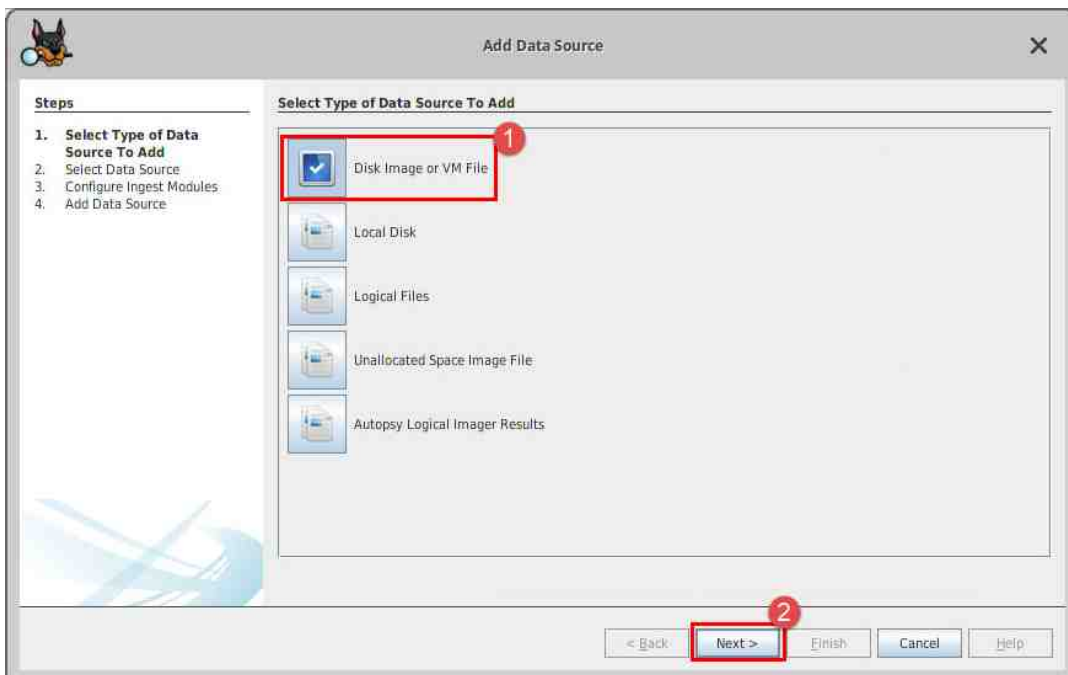


- The next window in the New Case wizard is the Optional information window. Here you can type more information about the case and examiner. Fill in the information as seen in the fields below, and then click Finish when you are done. Remember, the Name field highlighted within the examiner section should contain your name.



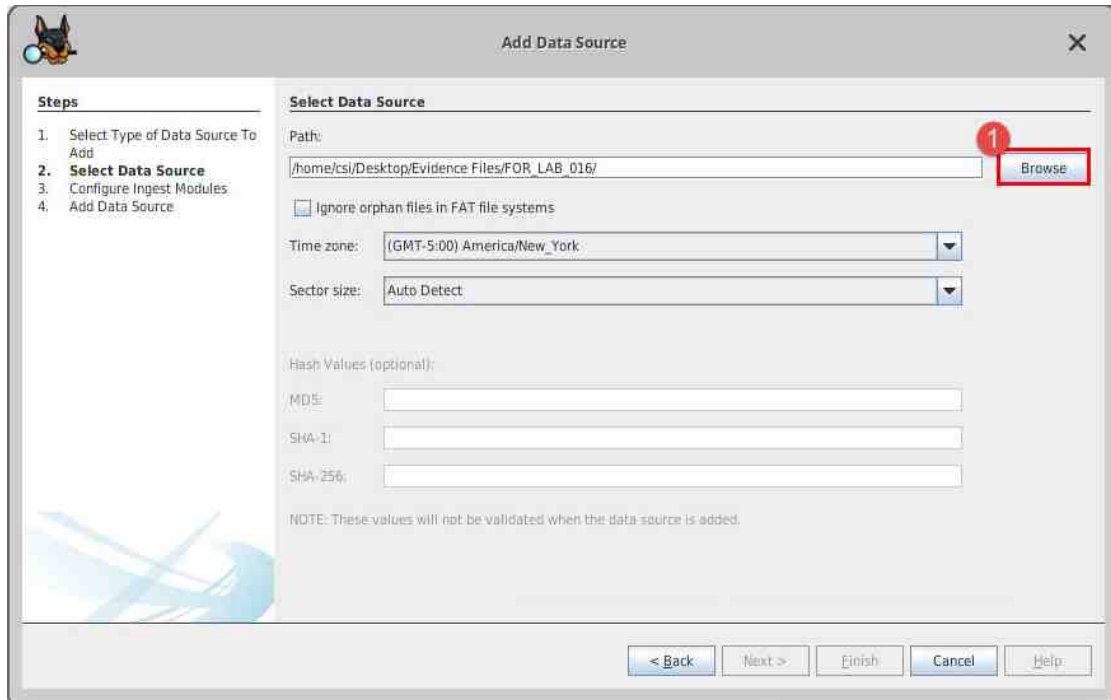
The screenshot shows the 'New Case Information' window with the 'Optional Information' tab selected. The 'Steps' pane on the left shows '2. Optional Information' as the current step. The main area contains several input fields: 'Case Number' (labeled 1) with the value 'NDG016'; 'Examiner Name' (labeled 2) with the placeholder '---Insert Student's Name here---'; 'Examiner Phone' with the value '(555) 555-5555'; 'Examiner Email' with the value 'youremail@yourdomain.com'; and an empty 'Examiner Notes' field. Below these is an 'Organization' section with a dropdown menu and a 'Manage Organizations' button. At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish' (labeled 3), 'Cancel', and 'Help'.

- You will now be taken to the Add Data Source window. Here you can choose between different evidence sources. In this exercise, we will be using a Forensic Evidence File (FEF) so let us select Disk Image or VM file and click Next as highlighted items 1 and 2 below.

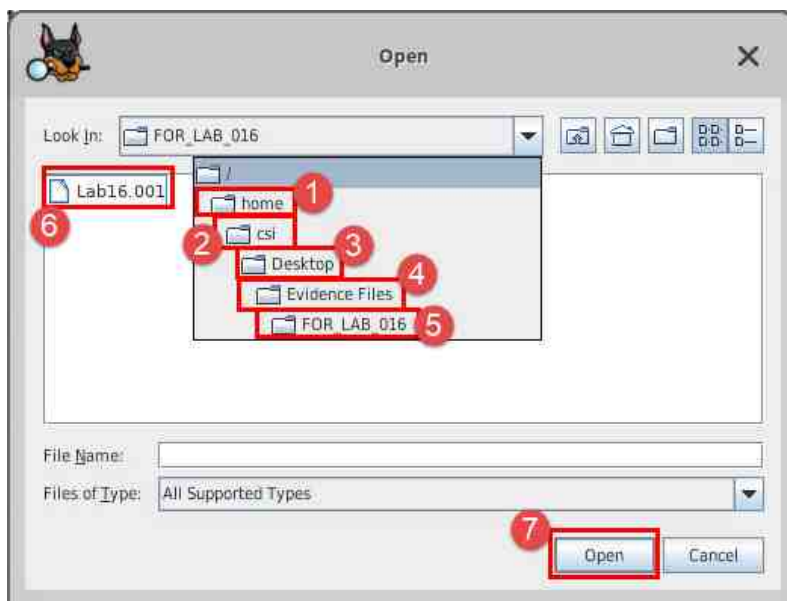


The screenshot shows the 'Add Data Source' window. The 'Steps' pane on the left shows '1. Select Type of Data Source To Add' as the current step. The main area is titled 'Select Type of Data Source To Add' and contains a list of options: 'Disk Image or VM File' (labeled 1), 'Local Disk', 'Logical Files', 'Unallocated Space Image File', and 'Autopsy Logical Imager Results'. The 'Disk Image or VM File' option is selected with a blue checkmark. At the bottom, there are navigation buttons: '< Back', 'Next >' (labeled 2), 'Finish', 'Cancel', and 'Help'.

- The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.

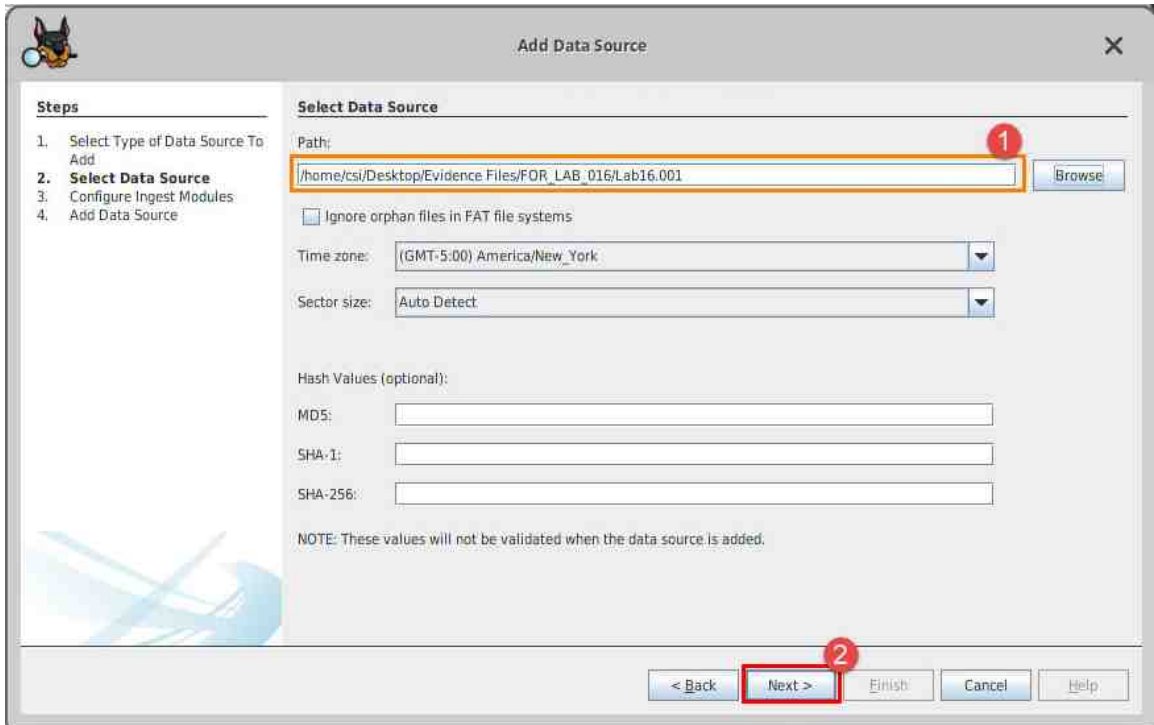


- In the Open window, browse to Home > csi > Desktop > Evidence Files > FOR_LAB_016 and click the file called Lab16.001¹ and then click Open as highlighted in items 1 – 7 below.



¹The FEF of the cellphone that we use in this lab is from the NIST Computer Forensic Reference Data Sets (CFReDS).
<https://www.cfreds.nist.gov/mobile/index.html>

9. The image path will now appear in the Path field highlighted as item 1 below. We will leave the other options as-is for now and click Next highlighted as item 2 below.

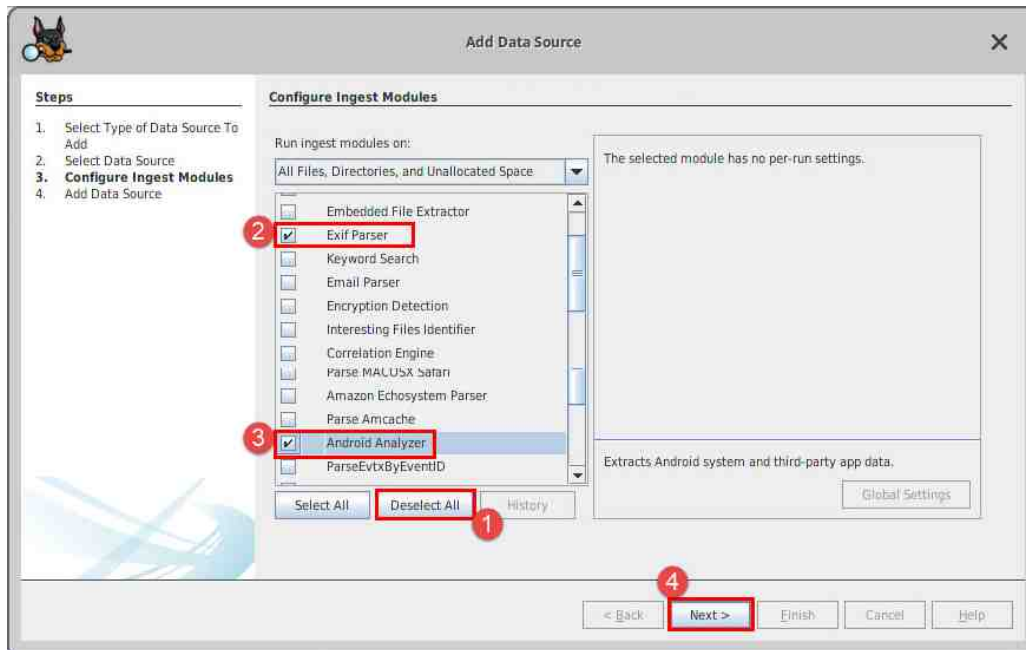


The screenshot shows the 'Add Data Source' dialog box. On the left, a 'Steps' list shows four steps: 1. Select Type of Data Source To Add, 2. **Select Data Source**, 3. Configure Ingest Modules, and 4. Add Data Source. The main area is titled 'Select Data Source'. It contains a 'Path:' label followed by a text field containing the path '/home/csi/Desktop/Evidence Files/FOR_LAB_016/Lab16.001'. A red box labeled '1' highlights this text field. To the right of the text field is a 'Browse...' button. Below the path field is a checkbox labeled 'Ignore orphan files in FAT file systems'. Further down are two dropdown menus: 'Time zone:' set to '(GMT-5:00) America/New_York' and 'Sector size:' set to 'Auto Detect'. Below these are three text fields for 'Hash Values (optional)': 'MD5:', 'SHA-1:', and 'SHA-256:'. At the bottom of the main area is a note: 'NOTE: These values will not be validated when the data source is added.' At the bottom of the dialog box are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A red box labeled '2' highlights the 'Next >' button.

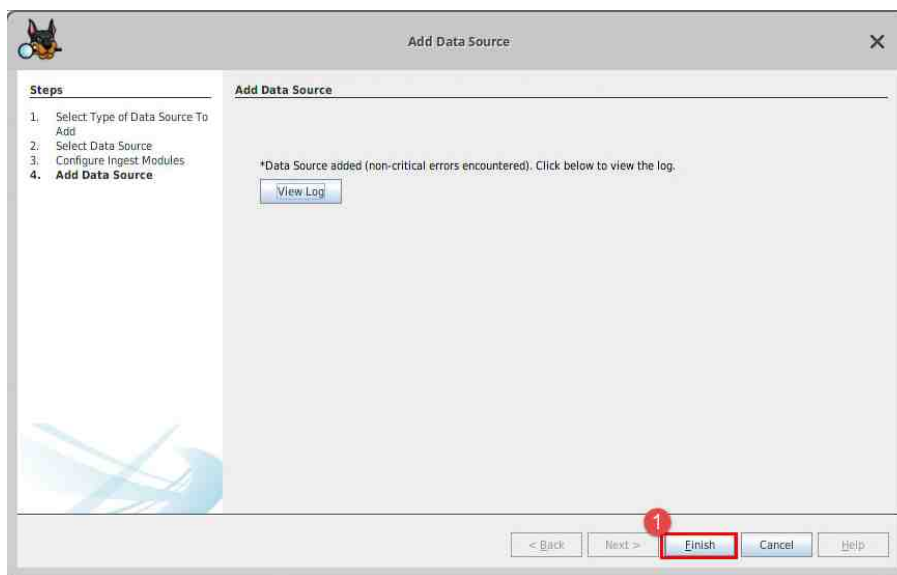


Time zone is an important aspect to any forensic investigation. Feel free to adjust the time zone to match your respective time zones.

10. You will be taken to the Configure Ingest Modules step of the case creation process. We will be using some Ingest Modules in this exercise, so uncheck any selected Ingest Module by clicking the Deselect All button as seen in item 1. Next, click the checkbox beside the following Ingest Modules: Exif Parser and Android Analyzer, as highlighted in items 2 and 3 below. Once you have selected all the Ingest Modules, click Next as seen in item 4.

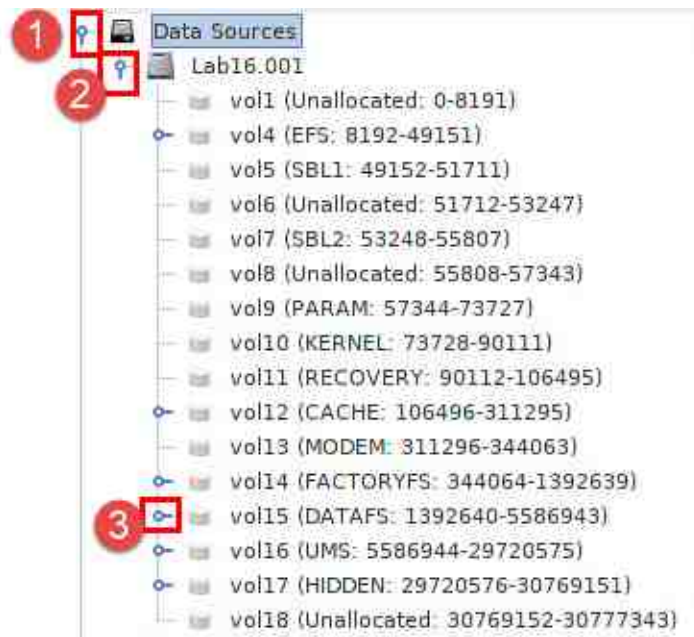


11. In the final window in the Add Data Source process, click Finish, as highlighted below.

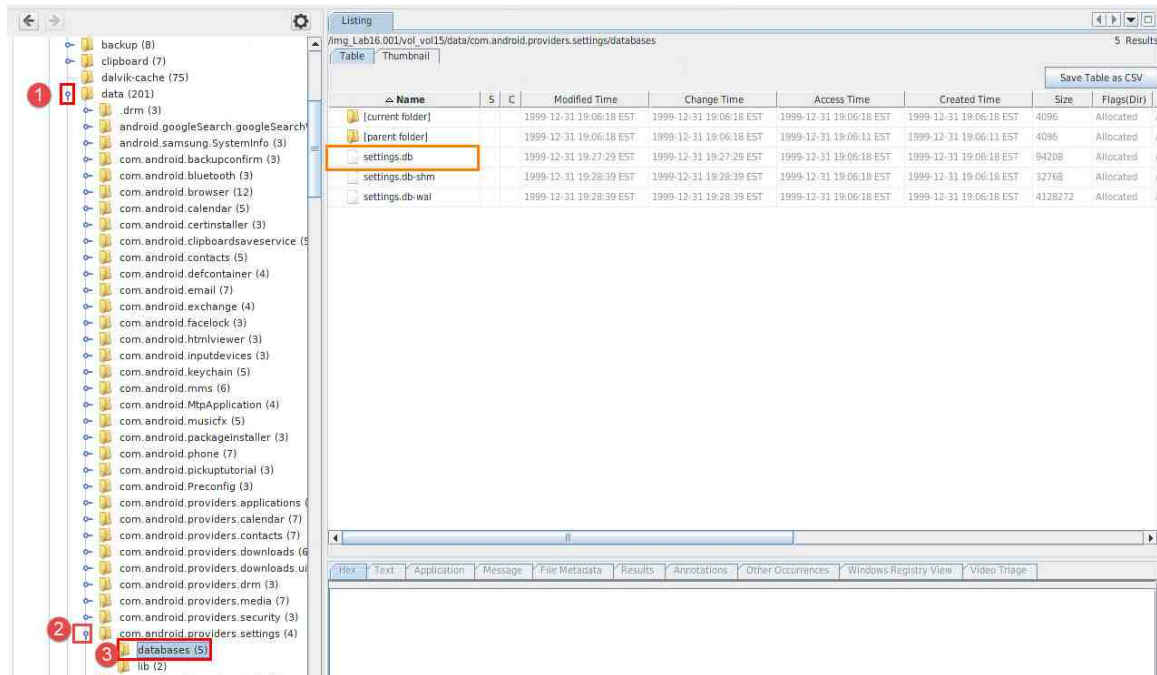


Pay attention to the status bar in the bottom-right corner to determine when the Ingest Modules are done running. Proceed once the processing is done.

12. You will now be taken to the Autopsy main window. Here we can navigate the data partition of the phone to identify some common artifacts. To begin, click the blue pin beside Data sources, which will expand and reveal the FEF as seen in item 1 below. Next, click the blue pin beside Lab16.001 to view the partitions on the drive as seen in item 2 below. In physical images of Android devices, you will see many partitions. This image has 18 partitions, but we will focus on the data within one, which is volume 15 (vol15) – the data partition. Let us expand vol15 by clicking the blue pin beside it as seen in item 3 below. Within vol15, you are now able to see several folders that we can navigate. These folders contain valuable system and user information.

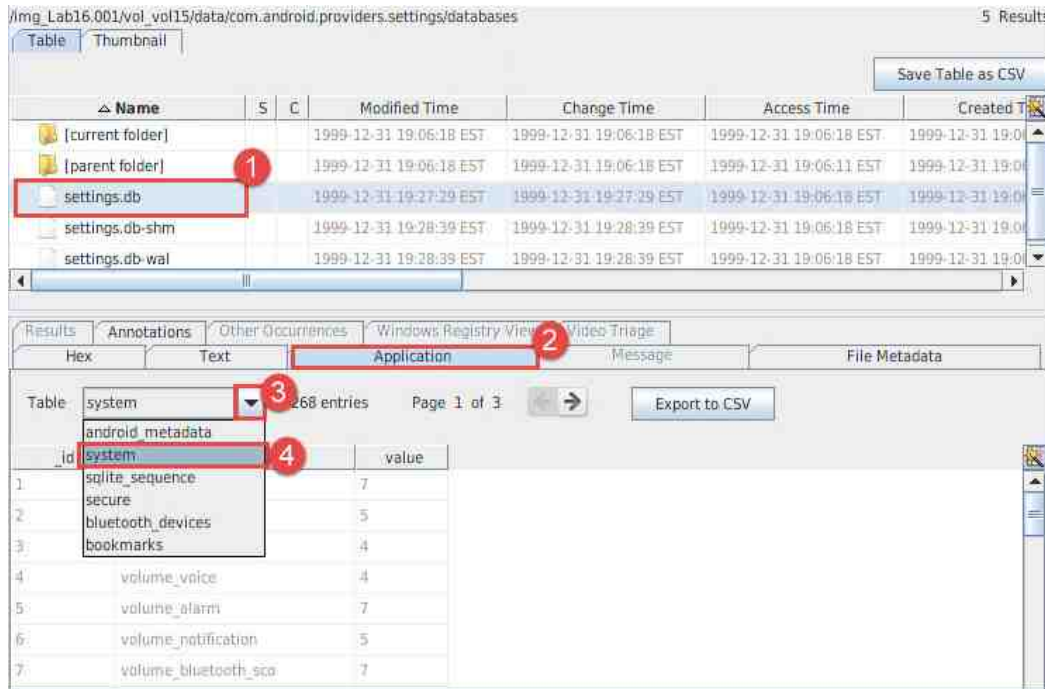


13. Most of the data that is valuable to forensic examiners in an android device can be found in databases and config files. Let us look for a few useful artifacts that can help us learn more about the device. Click the blue pin beside the following folders data > com.android.providers.settings > databases seen in items 1, 2, and 3 below. Inside the databases folder, you will find the settings.db file. Let us look at some of the data it stores.



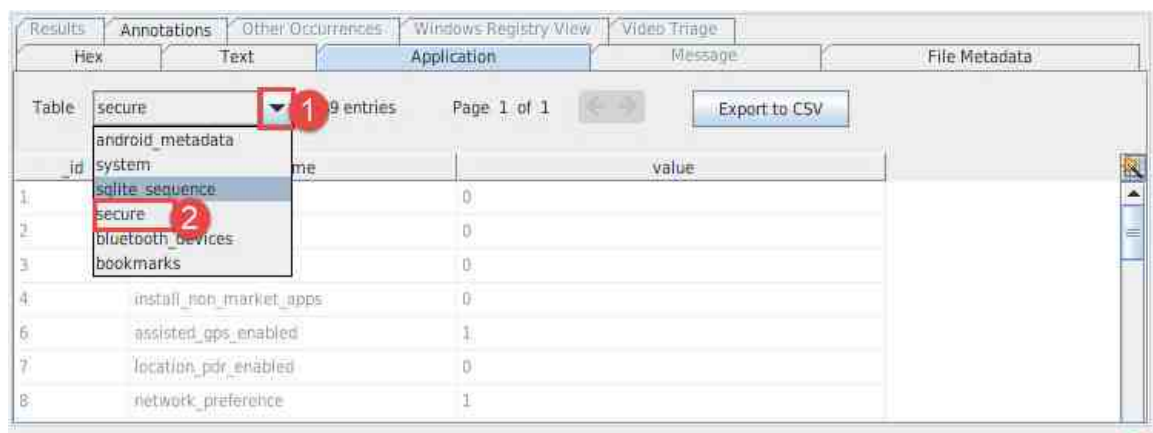
Autopsy creates references to the current folder and parent folder within the File List pane.

14. Click the settings.db file, as seen in item 1 below. Next, click the Application tab seen in item 2 to view it using Autopsy's database viewer. Now click the Table dropdown arrow and select System as seen in items 3 and 4 below.



This table reveals device system settings such as the sound settings, the airplane mode settings, driving mode settings, and other options. This information will not be necessary in every investigation but is useful to know since it can provide hints about the phone's state and expected behavior. Take some time to review the options you see here.

15. Let us look at the security settings now. Begin by clicking the Table dropdown menu and selecting secure from the list, as seen in items 1 and 2 below.



16. This table contains network preferences and security options. Look at the first 4 rows highlighted in item 1.

| _id | name | value |
|-----|-------------------------|-------|
| 1 | bluetooth_on | 0 |
| 2 | data_roaming | 0 |
| 3 | data_roaming_1 | 0 |
| 4 | install_non_market_apps | 0 |
| 6 | assisted_gps_enabled | 1 |
| 7 | location_poi_enabled | 0 |
| 8 | network_preference | 1 |



The settings can tell whether the device's Bluetooth and data roaming were enabled. It also can tell whether non-market applications can be installed to the phone. This is a helpful setting when determining whether a device was compromised.

17. Let us scroll down to row 17 using the scroll bar seen in item 1 or the mouse wheel. This row tells whether backups are enabled for this device.

| _id | name | value |
|-----|-------------------------|--|
| 15 | cdma_cell_broadcast_sms | 1 |
| 16 | mock_location | 0 |
| 17 | backup_enabled | 0 |
| 18 | backup_transport | com.google.android.backup/BackupTransportService |
| 19 | mount_play_not_snd | 1 |
| 20 | mount_ums_autostart | 0 |
| 21 | mount_ums_prompt | 1 |

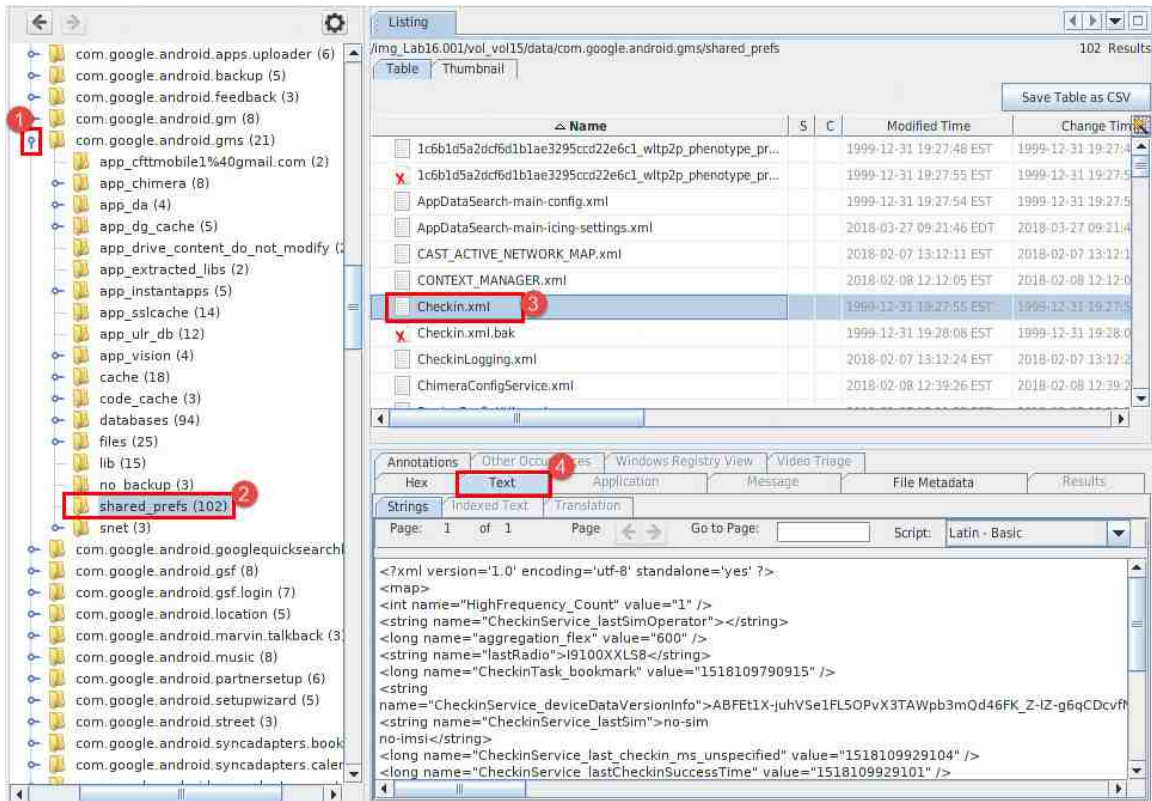
18. Let us scroll a little further and stop scrolling when you can see both rows 29 and 34 as seen in item 1. Row 29 is the `lockscreen.disabled` setting and can tell whether the phone's lock screen was enabled. The fact that this value is 0 indicates that the phone's lock screen was enabled at the time of extraction. Now, look at row 34 `lockscreen.options`, which has `enable_facelock`. This indicates that the phone had face unlock enabled. There are several more settings and options related to security and network settings in this table. Feel free to scroll through and identify some familiar ones.

| _id | name | value |
|-----|------------------------------------|--|
| 27 | speak_password | 0 |
| 28 | accessibility_script_injection_url | https://ssl.gstatic.com/accessibility/javascript/android/... |
| 29 | lockscreen.disabled | 0 |
| 31 | netstats_enabled | 1 |
| 32 | wifi_max_dhcp_retry_count | 9 |
| 33 | usb_setting_mode | 0 |
| 34 | lockscreen.options | enable_facelock |
| 35 | lock_motion_tilt_to_unlock | 0 |
| 36 | lockscreen.visible_motions | 3 |

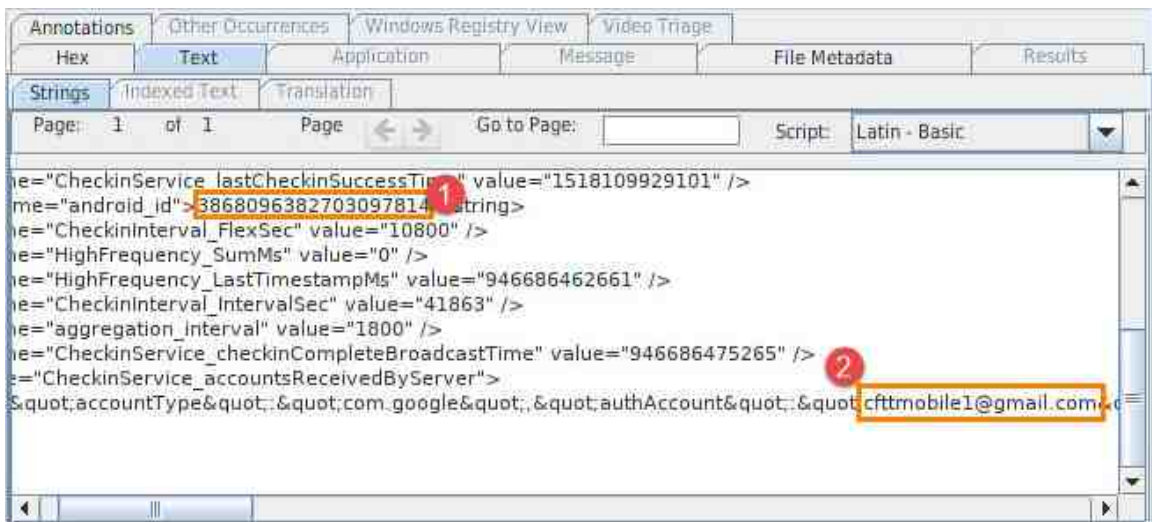
19. Now let us look at some device information in the `checkin.xml` file. To do this, first contract the folder called `com.android.providers.settings` by clicking the blue pin beside it as seen in item 1.



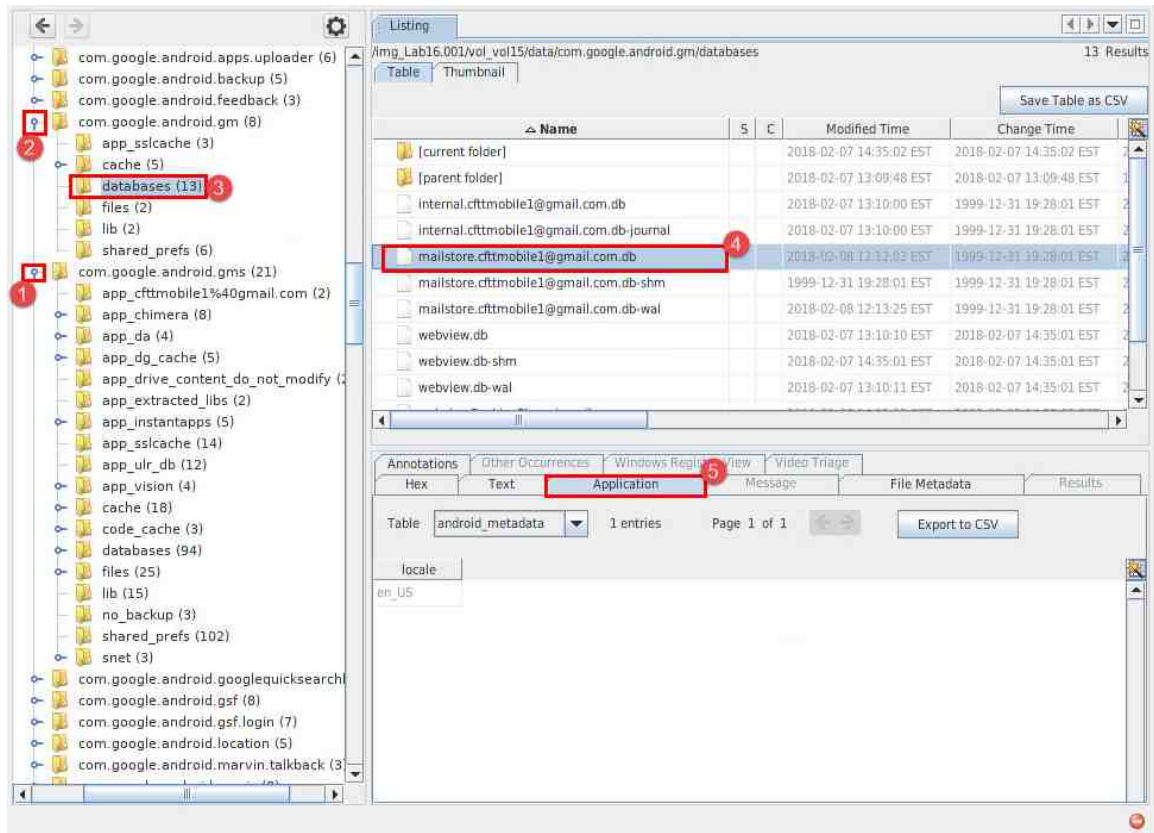
20. Next, click the blue pin beside the following folders com.google.android.gms > shared_prefs seen in items 1 and 2 below. Once there, click the file called checkin.xml and then click the Text tab as seen in items 3 and 4.



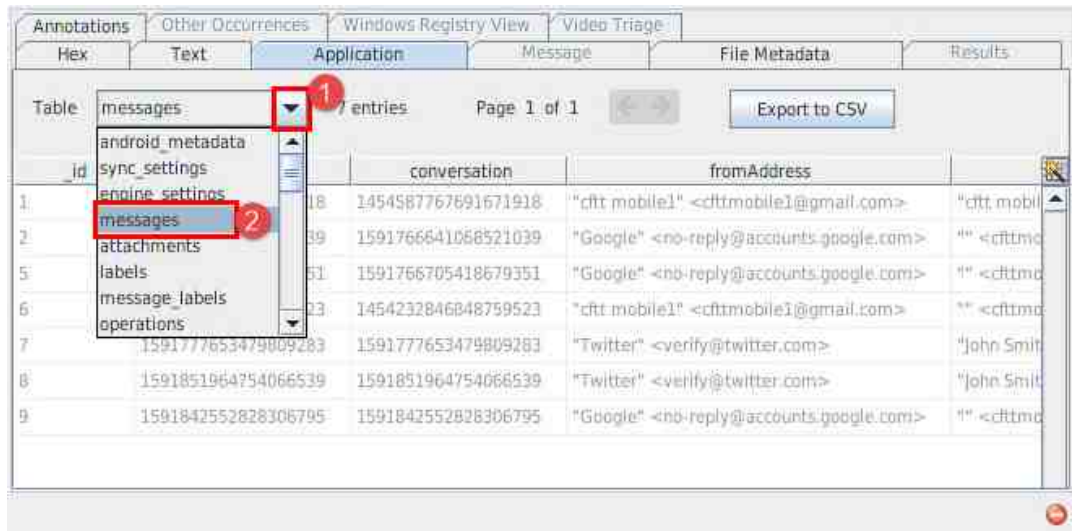
21. In this file, we can find information about the phone, such as its International Mobile Equipment Identity (IMEI) seen in item 1 below. This number can be used to find specific details about the phone as it is unique to this device. If you scroll to the bottom of this window, you will also see the Gmail account associated with the device, as seen in item 2 below. This information helps in the steps to tie a user to the device.



22. Since we found an email address, let us look to see if there is any information about the emails for the account. Let us navigate to the Gmail database. To begin, contract the folder called com.google.android.gms by clicking the blue pin beside it as seen in item 1. Next, click the blue pins beside the following folders com.google.android.gm > databases seen in items 2 and 3 below. Once there, click the file called mailstore.cfttmobile1@gmail.com.db and then click the Application tab as seen in items 4 and 5.



23. Let us look at the email message data for the account cftmobile1@gmail.com. Begin by clicking the Table dropdown menu and selecting messages from the list, as seen in items 1 and 2 below.



24. The table that appears contains fragments of the emails that are in the account. Let us look at some of the columns that make up this table. The first column, _id seen in item 1 is the unique identifier for each message in this table. The messageid seen in item 2 is the unique identifier for each message, and the conversation seen in item 3 column contains the unique identifier for each thread. These values help to keep track of messages and can be referenced by other tables in the database. The fromAddress and toAddress seen in item 4 are the sender and recipient of each message.

Table

messages

7 entries

Page 1 of 1

Export to CSV

| id | messageid | conversation | fromAddress | toAddresses | ccAddresses | bccAddress.. |
|----|---------------------|---------------------|---|--------------------------------------|-------------|--------------|
| 1 | 1454587767691671918 | 1454587767691671918 | "cft mobile1" <cftmobile1@gmail.com> | "cft mobile1" <cftmobile1@gmail.com> | | |
| 2 | 1591766641068521039 | 1591766641068521039 | "Google" <no-reply@accounts.google.com> | ** <cftmobile1@gmail.com> | | "Google" |
| 5 | 1591766705418679351 | 1591766705418679351 | "Google" <no-reply@accounts.google.com> | ** <cftmobile1@gmail.com> | | "Google" |
| 6 | 1454232846848759523 | 1454232846848759523 | "cft mobile1" <cftmobile1@gmail.com> | ** <cftmobile1@gmail.com> | | |
| 7 | 159177653479809283 | 159177653479809283 | "Twitter" <verify@twitter.com> | "John Smith" <cftmobile1@gmail.com> | | |
| 8 | 1591851964754066539 | 1591851964754066539 | "Twitter" <verify@twitter.com> | "John Smith" <cftmobile1@gmail.com> | | |
| 9 | 1591842552828306795 | 1591842552828306795 | "Google" <no-reply@accounts.google.com> | ** <cftmobile1@gmail.com> | | "Google" |

25. Let us scroll to the right until you get to the dateSentMs and dateReceivedMs columns, as seen in item 1. These columns contain the dates and times that the messages were sent, as seen in item 2. To convert them, you can right-click in the column and navigate to Display as > Date as seen in items 3 and 4.

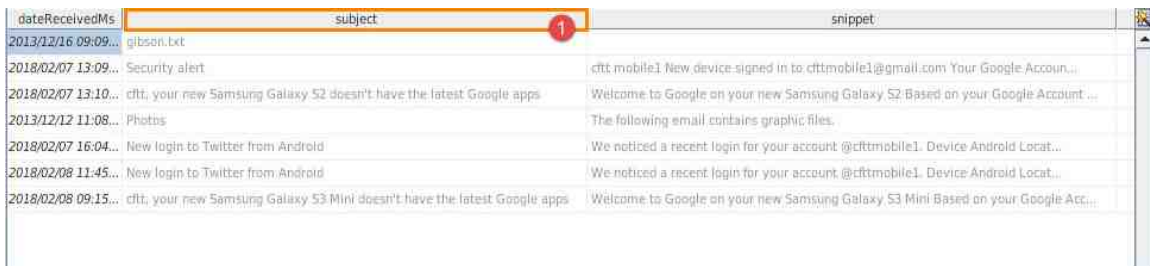


| replyToAddresses | dateSentMs | dateReceivedMs | subject |
|---|---------------|----------------|---|
| "Google" <no-reply@accounts.google.com> | 1518026961000 | 1518026961000 | gibson.txt |
| "Google" <no-reply@accounts.google.com> | 1518026961000 | 1518026961000 | ... |
| | 1386864516000 | 1386864516287 | Photos |
| | 1518037464000 | 1518037465357 | New login to Twitter from Android |
| | 1518108333000 | 1518108334315 | New login to Twitter from Android |
| "Google" <no-reply@accounts.google.com> | 1518099294000 | 1518099358252 | cftt, your new Samsung Galaxy S3 Mini doesn't have the latest Google apps |



Scrolling can be a little tricky. If you have difficulty scrolling across select any of the cells and use the arrow keys to navigate you way across.

26. The next column called subject, seen in item 1 is the subject of the email. Right beside that is the column called snippet. This column contains message fragments. Here you can see the first part of the email messages in this Gmail account.



| dateReceivedMs | subject | snippet |
|---------------------|---|---|
| 2013/12/16 09:09... | gibson.txt | |
| 2018/02/07 13:09... | Security alert | cftt mobile1 New device signed in to cfttmobile1@gmail.com Your Google Account... |
| 2018/02/07 13:10... | cftt, your new Samsung Galaxy S2 doesn't have the latest Google apps | Welcome to Google on your new Samsung Galaxy S2 Based on your Google Account ... |
| 2013/12/12 11:08... | Photos | The following email contains graphic files. |
| 2018/02/07 16:04... | New login to Twitter from Android | We noticed a recent login for your account @cfttmobile1. Device Android Locat... |
| 2018/02/08 11:45... | New login to Twitter from Android | We noticed a recent login for your account @cfttmobile1. Device Android Locat... |
| 2018/02/08 09:15... | cftt, your new Samsung Galaxy S3 Mini doesn't have the latest Google apps | Welcome to Google on your new Samsung Galaxy S3 Mini Based on your Google Acc... |



While they are not the complete emails, it is really great that we can find information such as subject, sent received, attachments etc.

27. Let us look at another table in this database. Navigate to the attachments table by clicking the Table dropdown menu and selecting attachments from the list, as seen in items 1 and 2 below.

Table

attachments

18 entries

Page 1 of 1

Export to CSV

id

android_metadata

sync_settings

engine_settings

messages

attachments

labels

message_labels

operations

messages_messageId

messages_...

originExtras

desiredRen...

automatic

downloade...

downloadId

stat...

| | | | | | | | | | | |
|---|--|--|---------------------|-----|---|------|---|------|----|-----|
| 1 | | | 1454587767691671918 | 0.1 | 1454587767691671918_1454587767691671918_0.1 | BEST | 0 | BEST | -1 | 200 |
| 2 | | | 1454587767691671918 | 0.1 | 1454587767691671918_1454587767691671918_0.1 | BEST | 0 | BEST | -1 | 200 |
| 3 | | | 1454587675735835686 | 0.1 | 1454587675735835686_1454587675735835686_0.1 | BEST | 0 | BEST | -1 | 200 |
| 4 | | | 1454587675735835686 | 0.1 | 1454587675735835686_1454587675735835686_0.1 | BEST | 0 | BEST | -1 | 200 |
| 5 | | | 1454587598156294665 | 0.1 | 1454587598156294665_1454587598156294665_0.1 | BEST | 0 | BEST | -1 | 200 |
| 6 | | | 1454587598156294665 | 0.1 | 1454587598156294665_1454587598156294665_0.1 | BEST | 0 | BEST | -1 | 200 |
| 7 | | | 1454587536384287494 | 0.1 | 1454587536384287494_1454587536384287494_0.1 | BEST | 0 | BEST | -1 | 200 |
| 8 | | | 1454587536384287494 | 0.1 | 1454587536384287494_1454587536384287494_0.1 | BEST | 0 | BEST | -1 | 200 |
| 9 | | | 1454587450178213811 | 0.1 | 1454587450178213811_1454587450178213811_0.1 | BEST | 0 | BEST | -1 | 200 |

28. This table contains details about the attachments associated with the emails in this database. We will only focus on a few columns in this table. The first 3 columns are familiar to us as we saw something similar in the messages database. As you can see, the messageId and conversation columns have similar values to the ones in the messages table. This is because the attachments table associates the attachments listed here, with the matching email messages. The row called _id is unique to this table, however.

| _id | messages.conversation | messages.messageId | messages... | originExtras | desiredRen... | automatic | downloade... | downloadId | stat... |
|-----|-----------------------|---------------------|-------------|---|---------------|-----------|--------------|------------|---------|
| 1 | 1454587767691671918 | 1454587767691671918 | 0.1 | 1454587767691671918_1454587767691671918_0.1 | BEST | 0 | BEST | -1 | 200 |
| 2 | 1454587767691671918 | 1454587767691671918 | 0.1 | 1454587767691671918_1454587767691671918_0.1 | BEST | 0 | BEST | -1 | 200 |
| 3 | 1454587675735835686 | 1454587675735835686 | 0.1 | 1454587675735835686_1454587675735835686_0.1 | BEST | 0 | BEST | -1 | 200 |
| 4 | 1454587675735835686 | 1454587675735835686 | 0.1 | 1454587675735835686_1454587675735835686_0.1 | BEST | 0 | BEST | -1 | 200 |
| 5 | 1454587598156294665 | 1454587598156294665 | 0.1 | 1454587598156294665_1454587598156294665_0.1 | BEST | 0 | BEST | -1 | 200 |
| 6 | 1454587598156294665 | 1454587598156294665 | 0.1 | 1454587598156294665_1454587598156294665_0.1 | BEST | 0 | BEST | -1 | 200 |
| 7 | 1454587536384287494 | 1454587536384287494 | 0.1 | 1454587536384287494_1454587536384287494_0.1 | BEST | 0 | BEST | -1 | 200 |
| 8 | 1454587536384287494 | 1454587536384287494 | 0.1 | 1454587536384287494_1454587536384287494_0.1 | BEST | 0 | BEST | -1 | 200 |
| 9 | 1454587450178213811 | 1454587450178213811 | 0.1 | 1454587450178213811_1454587450178213811_0.1 | BEST | 0 | BEST | -1 | 200 |

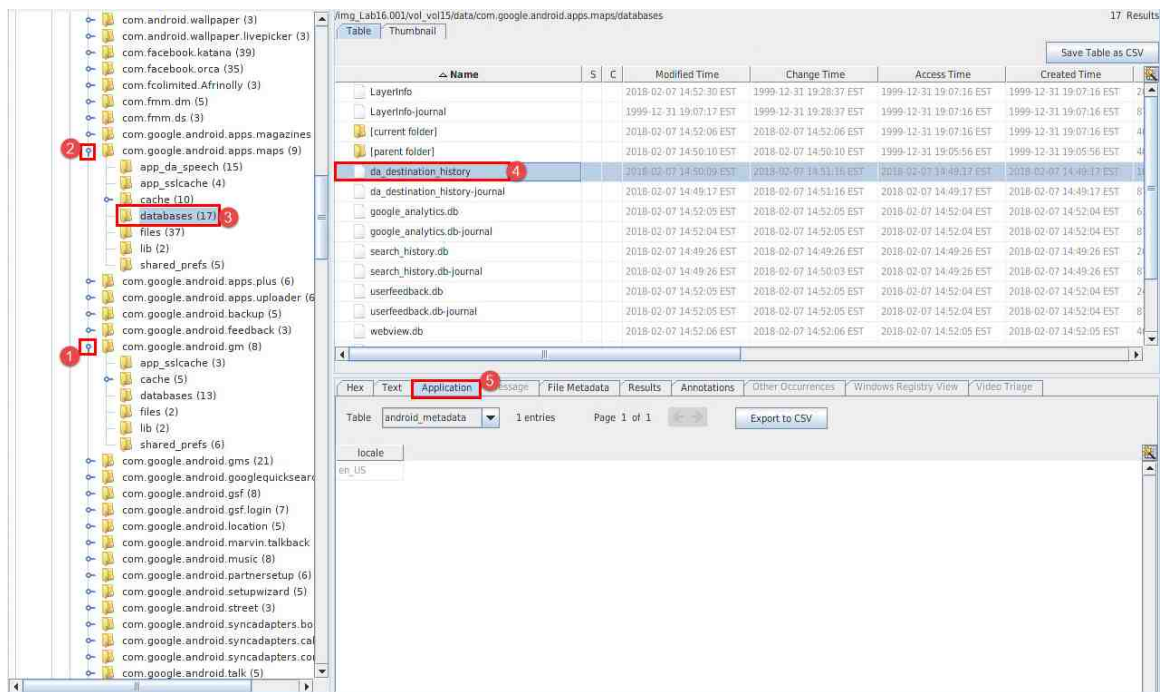
29. Let us scroll to the right until you get to the column called filename, as seen in item 1. This column contains the names and storage locations of the attachments. This is extremely helpful in tracking where a file came from, as you can trace it back using the message and conversation IDs.

| Ren... | automatic | downloade... | downloadId | status | saveToSd | filename | priority | mimeType |
|--------|-----------|--------------|------------|--------|----------|--|----------|-----------------|
| 0 | BEST | -1 | 200 | 0 | 0 | gibson.txt | 0 | text/plain |
| 0 | BEST | -1 | 200 | 1 | 0 | file:///storage/sdcard0/Download/gibson.txt | 0 | text/plain |
| 0 | BEST | -1 | 200 | 1 | 0 | forensics.pdf | 0 | application/pdf |
| 0 | BEST | -1 | 200 | 1 | 0 | file:///storage/sdcard0/Download/forensics.pdf | 0 | application/pdf |
| 0 | BEST | -1 | 200 | 0 | 0 | french.mp3 | 0 | audio/mpeg |
| 0 | BEST | -1 | 200 | 1 | 0 | file:///storage/sdcard0/Download/french.mp3 | 0 | audio/mpeg |
| 0 | BEST | -1 | 200 | 0 | 0 | chare.wav | 0 | audio/x-wav |
| 0 | BEST | -1 | 200 | 1 | 0 | file:///storage/sdcard0/Download/chare.wav | 0 | audio/x-wav |
| 0 | BEST | -1 | 200 | 0 | 0 | hinder.mp4 | 0 | video/mp4 |



Select any of the cells and use the arrow keys to navigate your way across until you reach the column.

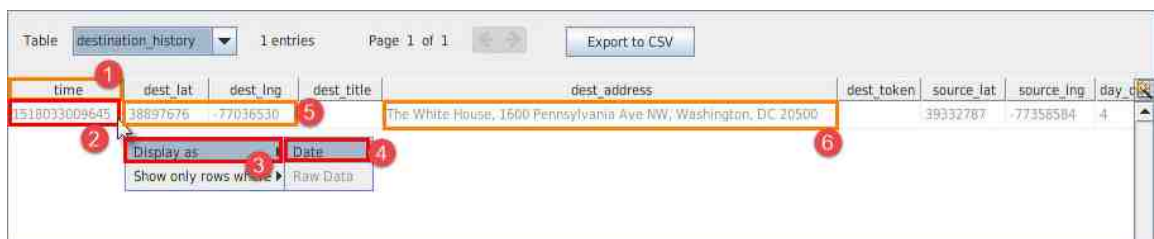
30. The next interesting artifact we will look at is Google Maps' navigation history. This database file can provide information about the user's previous trips plotted by Google Maps. To begin, contract the folder called com.google.android.gm by clicking the blue pin beside it as seen in item 1. Next, click the blue pins beside the following folders com.google.android.apps.maps > databases seen in items 2 and 3 below. Once there, click the file called da_destination_history and then click the Application tab as seen in items 4 and 5.



31. Let us look at the navigation data for the user. Begin by clicking the Table dropdown menu and selecting destination_history from the list as seen in items 1 and 2 below.



32. This table contains one entry, but this entry contains lots of detail. Let us look at some of the columns. The first column, seen in item 1, is time and can be converted to a human-readable date by right-clicking in the column and selecting Display as > Date as seen in items 2, 3, and 4 below. The time in this entry is when the navigation began. Next to the time are the latitude and longitude entries in the columns called dest_lat and dest_lng highlighted in item 5. The data in these columns plot the specific location of the destination. Next up is the destination address called dest_address seen in item 6. This is the address that the user navigated to.



33. Finally, if you scroll to the right, you will see the source latitude and longitude columns called `source_lat` and `source_lng` seen in item 1 below. This is the location that the user started navigating from.

Table

destination_history

1 entries

Page 1 of 1

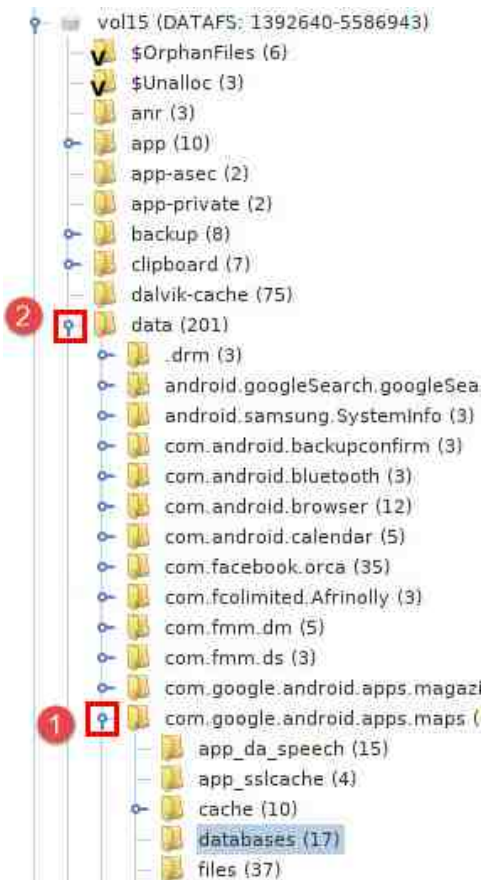
Export to CSV

| dest_lat | dest_lng | dest_title | dest_address | dest_token | source_lat | source_lng | day_of_week | hour_of_day |
|----------|-----------|------------|---|------------|------------|------------|-------------|-------------|
| 38897676 | -77036530 | | The White House, 1600 Pennsylvania Ave NW, Washington, DC 20500 | | 39332787 | -77358584 | 4 | 14 |

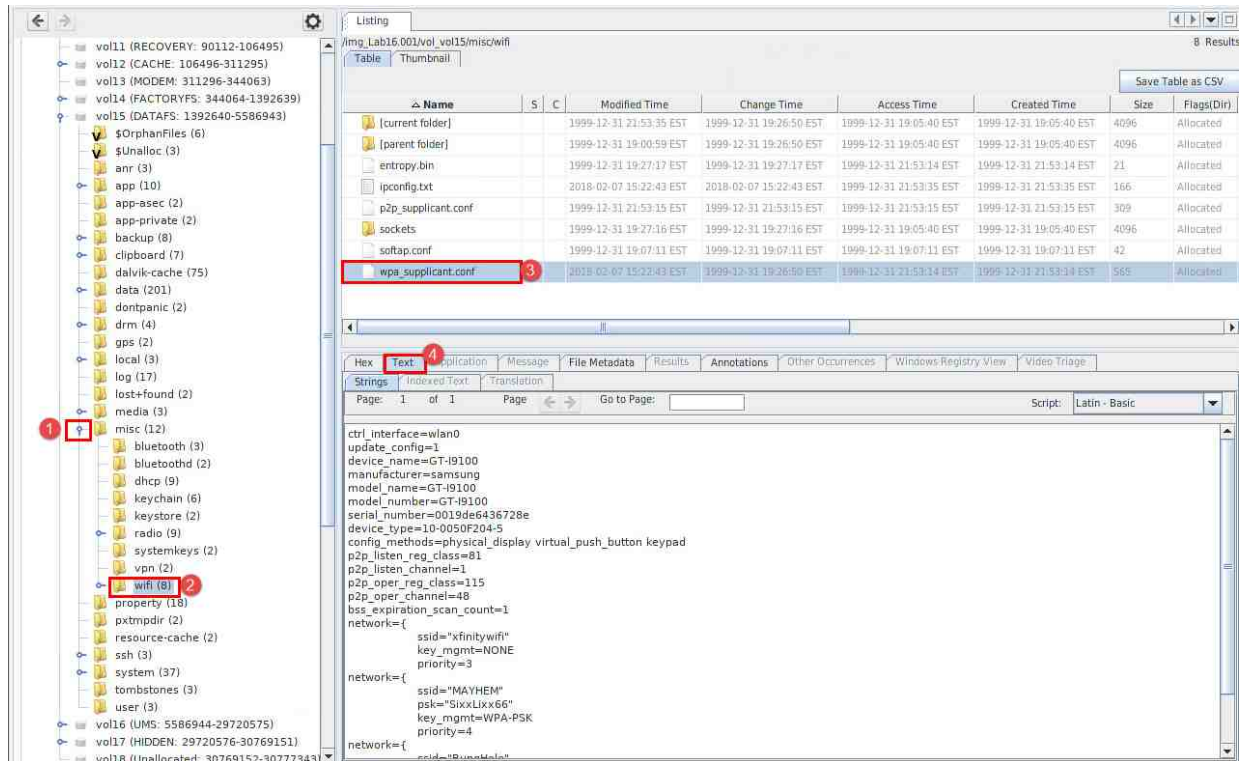


The information we identified in this database is helpful since it helps you to keep track of the user's travels.

34. We will look at two more data types and then move on to the calls and messages. Let us start with the Wi-Fi data. To begin, contract the folders called `com.google.android.apps.maps` and `data` by clicking the blue pins beside them as seen in items 1 and 2.



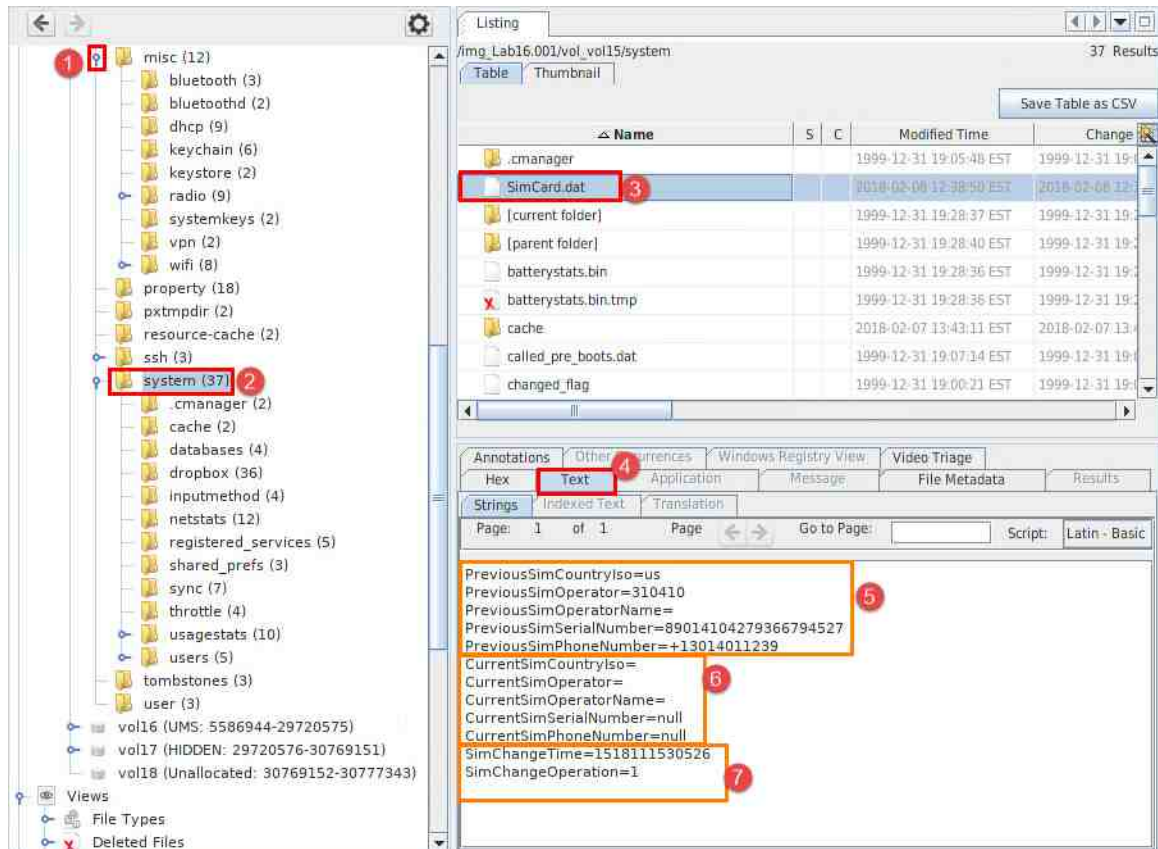
35. Next, click the blue pins beside the following folders misc > wifi seen in items 1 and 2 below. Once there, click the file called wpa_supplicant.conf and then click the Text tab as seen in items 3 and 5.



36. This configuration file contains information about the wireless adapter and the cell phone as well. Look at the data highlighted in item 1. Here, you can see the wireless interface, the device model, manufacturer, and serial number in hexadecimal. In item 2, you will find the saved Wi-Fi connections, including their SSID, encryption type (if any), and the passphrase.



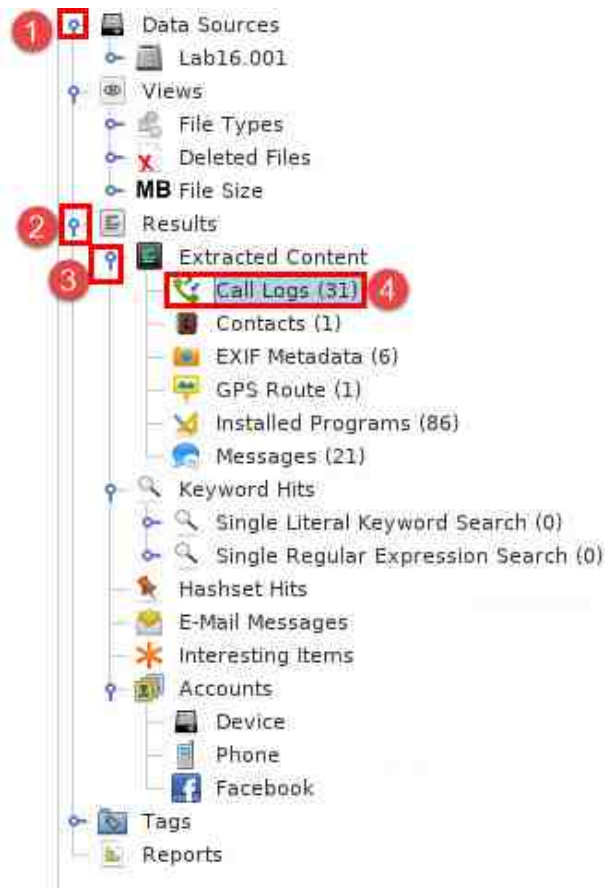
37. Let us look at one last network connection artifact. This is the SIM Card data. To begin, contract the folder called misc by clicking the blue pin beside it, as seen in item 1. Next, click the folder called System, as seen in item 2 below. Once there, click the file called SimCard.dat and then click the Text tab, as seen in items 3 and 4. As you can see in item 5, the details of the previous SIM card are listed here. It provides the Integrated Circuit Card Identifier (ICCID) and the phone number as well as details about the SIM operator and the country. The details of the current SIM card, if applicable, can be seen in item 6. In item 7, the Unix time that the SIM card was changed/removed.



38. So far, we have looked at lots of different database and configuration files and seen the way the types of data inside them. In the next exercise, we will take a quick look at the processed data that the ingest modules uncovered.

2 View the extracted mobile artifacts

1. We will look at the artifacts that this tool extracted for us and see what databases the information was pulled from. Let us begin by contracting the tree item called Data Sources by clicking the blue pin beside it, as seen in item 1. Next, click the blue pins beside the following tree items Results > Extracted Content seen in items 2 and 3 below. This will expand and reveal several items. Let us start by clicking Call Logs as seen in item 4 below.



- The call logs will appear in the Listing pane. Let us look at the columns. The first column called Source File seen in item 1 is the file that the call logs were taken from. This file is the logs.db and is located at (DataPartition)/data/com.sec.android.provider.logsprovider/databases/. The column called To Phone Number, seen in item 2, contains the phone number that received the call. The two columns to the right of that, called Start Date/Time and End Date/Time, seen in item 3, are the start and end dates and times of each call. The next column is the one called Direction, seen in item 4, tells whether the call was outgoing or incoming. Next is the Name column seen in item 5 and is populated with a contact name if it is saved/known by the device.

Call Logs 31 Results

Table Thumbnail Save Table as CSV

| Source File | S | C | To Phone Number | Start Date/Time | End Date/Time | Direction | Name | Data |
|-------------|---|---|-----------------|-------------------------|-------------------------|-----------|--------------|------|
| logs.db | | | 2402528734 | 2018-02-07 14:33:04 EST | 2018-02-07 14:33:04 EST | Outgoing | | Lab1 |
| logs.db | | | 2402528734 | 2018-02-07 14:29:37 EST | 2018-02-07 14:29:37 EST | Outgoing | | Lab1 |
| logs.db | | | 2402528734 | 2018-02-07 14:27:40 EST | 2018-02-07 14:27:40 EST | Outgoing | | Lab1 |
| logs.db | | | | 2018-02-07 14:25:34 EST | 2018-02-07 14:25:34 EST | Incoming | | Lab1 |
| logs.db | | | | 2018-02-07 14:24:00 EST | 2018-02-07 14:24:00 EST | Incoming | | Lab1 |
| logs.db | | | | 2018-02-07 14:22:56 EST | 2018-02-07 14:22:56 EST | Incoming | | Lab1 |
| logs.db | | | | 2018-02-07 14:22:15 EST | 2018-02-07 14:22:15 EST | Incoming | | Lab1 |
| logs.db | | | 2402528734 | 2018-02-07 14:20:56 EST | 2018-02-07 14:20:56 EST | Outgoing | | Lab1 |
| logs.db | | | 7691234560 | 2018-02-07 14:20:56 EST | 2018-02-07 14:20:56 EST | Outgoing | Jimi Hendrix | Lab1 |

Results Annotations Other Occurrences Windows Registry View Video Triage

Hex Text Application Message File Metadata

Result: 2 of 36 Result < > Call Logs

| Type | Value | Source(s) |
|------------------|---|----------------|
| To Phone Number | 2402528734 | Android Analyz |
| Start Date/Time | 2018-02-07 14:33:04 | Android Analyz |
| End Date/Time | 2018-02-07 14:33:04 | Android Analyz |
| Direction | Outgoing | Android Analyz |
| Name | | Android Analyz |
| Source File Path | /img_Lab16.001/vol_vol15/data/com.sec.android.provider.logsprovider/databases/logs.db | |
| Artifact ID | -9223372036854775805 | |

3. Scroll to the right of this window using the scroll bar to see the last column called From Phone Number, seen in items 1 and 2.

| To Phone Number | Start Date/Time | End Date/Time | Direction | Name | Data Source | From Phone Number |
|-----------------|-------------------------|-------------------------|-----------|--------------|-------------|-------------------|
| 2402528734 | 2018-02-07 14:33:04 EST | 2018-02-07 14:33:04 EST | Outgoing | | Lab16.001 | |
| 2402528734 | 2018-02-07 14:29:37 EST | 2018-02-07 14:29:37 EST | Outgoing | | Lab16.001 | |
| 2402528734 | 2018-02-07 14:27:40 EST | 2018-02-07 14:27:40 EST | Outgoing | | Lab16.001 | |
| | 2018-02-07 14:25:34 EST | 2018-02-07 14:25:34 EST | Incoming | | Lab16.001 | +12402528734 |
| | 2018-02-07 14:24:00 EST | 2018-02-07 14:24:00 EST | Incoming | | Lab16.001 | +12402528734 |
| | 2018-02-07 14:22:56 EST | 2018-02-07 14:22:56 EST | Incoming | | Lab16.001 | +12402528734 |
| | 2018-02-07 14:22:15 EST | 2018-02-07 14:22:15 EST | Incoming | | Lab16.001 | +1121611611 |
| 2402528734 | 2018-02-07 14:20:56 EST | 2018-02-07 14:20:56 EST | Outgoing | | Lab16.001 | |
| 7691234560 | 2018-02-07 14:20:56 EST | 2018-02-07 14:20:56 EST | Outgoing | Jiml Hendrix | Lab16.001 | |



This column tells the phone number that initiated the call. This data can always be verified by navigating to the source or by clicking the Application tab, which will open the database file.

4. Let us look at two more data categories. Click Installed Programs as seen in item 1. The list of installed programs will appear in the Listing pane. Let us look at the columns. The first column, seen in item 2, is the Source File and tells the name of the file that the data is pulled from. The column seen in item 3 is the name of the program. Finally, in item 4, is the Date/Time column that can tell when each specific program was installed. Scroll through the list and see if you are familiar with any of the programs.
5. Make a note of all the social media applications installed on the device.

←

→

⚙

Data Sources

Lab16.001

Views

File Types

Deleted Files

MB File Size

Results

Extracted Content

Call Logs (31)

Contacts (1)

EXIF Metadata (6)

GPS Route (1)

Installed Programs (86)

Messages (21)

Keyword Hits

Single Literal Keyword Search (0)

Single Regular Expression Search

Hashset Hits

E-Mail Messages

Interesting Items

Accounts

Device

Phone

Facebook

Tags

Reports

Listing

Installed Programs

TableThumbnail

Save Table as CSV

| Source File | S | C | Program Name | Data Source | S | C | Date/Time |
|-------------|---|---|-----------------------------------|-------------|---|---|-----------|
| library.db | | | com.folimited.Afrinolly | Lab16.001 | | | |
| library.db | | | com.google.android.apps.magazines | Lab16.001 | | | |
| library.db | | | com.google.android.voicesearch | Lab16.001 | | | |
| library.db | | | com.samsung.groupcast | Lab16.001 | | | |
| library.db | | | com.sec.android.app.clockpackage | Lab16.001 | | | |
| library.db | | | com.sec.android.app.launcher | Lab16.001 | | | |
| library.db | | | com.sec.android.app.music | Lab16.001 | | | |
| library.db | | | com.sec.android.app.samsungapps | Lab16.001 | | | |
| library.db | | | com.sec.android.inputmethod | Lab16.001 | | | |
| library.db | | | com.sec.chaton | Lab16.001 | | | |

Results

Annotations

Other Occurrences

Windows Registry View

Video Triage

Hex

Text

Application

Message

File Metadata

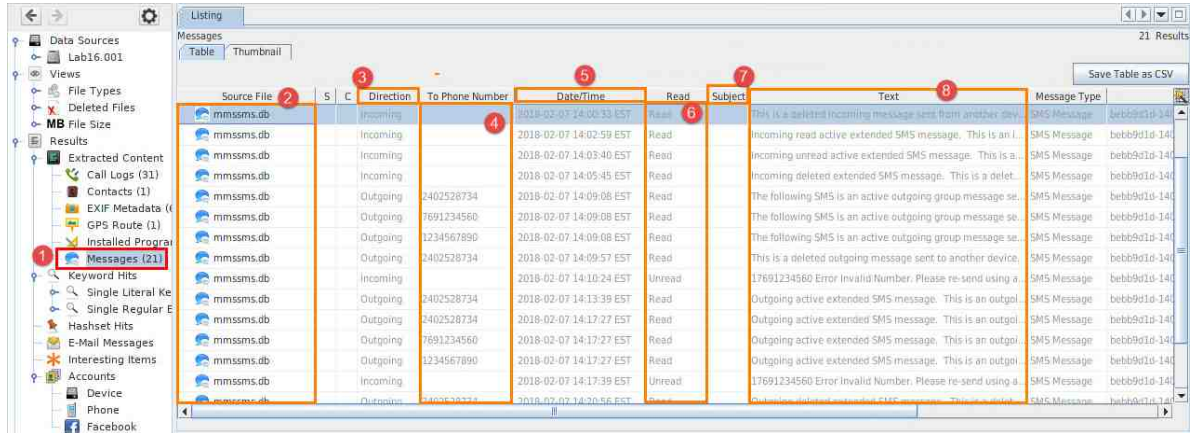
Result: 5 of 86

Result

Installed Programs


| Type | Value | Source(s) |
|------------------|---|-----------------|
| Program Name | com.google.android.apps.magazines | Android Install |
| Source File Path | /img_Lab16.001/vol_15/data/com.android.vending/databases/library.db | |
| Artifact ID | 9223372036854775732 | |

6. The last artifact we will review is the Messages category. To access this, click Messages as seen in item 1. Like before, the results will appear in the Listing pane and the first column seen in item 2 is the Source File. The column called Direction, seen in item 3, contains the direction of each message like in the call logs. The next column, To Phone Number, as seen in item 4, lists the destination phone number of the message. The column that follows, seen in item 5, is the Date/Time column. This tells the date and time the message was received. Next is the Read status column, seen in item 6. This tells whether the message was opened or not. The column called Subject, seen in item 7, lists the subject of the message if one is given. Finally, item 8 is the Text column, and it contains the body of the message.



| Source File | Direction | To Phone Number | Date/Time | Read | Subject | Text |
|-------------|-----------|-----------------|-------------------------|--------|---------|--|
| mmsms.db | Incoming | | 2018-02-07 14:05:33 EST | Read | | This is a deleted incoming message sent from another device. |
| mmsms.db | Incoming | | 2018-02-07 14:02:59 EST | Read | | Incoming read active extended SMS message. This is an i... |
| mmsms.db | Incoming | | 2018-02-07 14:03:40 EST | Read | | Incoming unread active extended SMS message. This is a... |
| mmsms.db | Incoming | | 2018-02-07 14:05:45 EST | Read | | Incoming deleted extended SMS message. This is a delet... |
| mmsms.db | Outgoing | 2402528734 | 2018-02-07 14:09:08 EST | Read | | The following SMS is an active outgoing group message se... |
| mmsms.db | Outgoing | 7691234560 | 2018-02-07 14:09:08 EST | Read | | The following SMS is an active outgoing group message se... |
| mmsms.db | Outgoing | 1234567890 | 2018-02-07 14:09:08 EST | Read | | The following SMS is an active outgoing group message se... |
| mmsms.db | Outgoing | 2402528734 | 2018-02-07 14:09:57 EST | Read | | This is a deleted outgoing message sent to another device. |
| mmsms.db | Incoming | | 2018-02-07 14:10:24 EST | Unread | | 17691234560 Error Invalid Number. Please re-send using a... |
| mmsms.db | Outgoing | 2402528734 | 2018-02-07 14:13:39 EST | Read | | Outgoing active extended SMS message. This is an outgoi... |
| mmsms.db | Outgoing | 2402528734 | 2018-02-07 14:17:27 EST | Read | | Outgoing active extended SMS message. This is an outgoi... |
| mmsms.db | Outgoing | 7691234560 | 2018-02-07 14:17:27 EST | Read | | Outgoing active extended SMS message. This is an outgoi... |
| mmsms.db | Outgoing | 1234567890 | 2018-02-07 14:17:27 EST | Read | | Outgoing active extended SMS message. This is an outgoi... |
| mmsms.db | Incoming | | 2018-02-07 14:17:39 EST | Unread | | 17691234560 Error Invalid Number. Please re-send using a... |
| mmsms.db | Outgoing | 2402528734 | 2018-02-07 14:20:56 EST | Read | | Outgoing active extended SMS message. This is an outgoi... |

7. Let us scroll to the right using the scroll bar, seen in item 1. You will see the Message Type column, seen in item 2, which tells whether this is a Short Message Service (SMS) message or a Multimedia Message (MMS) since this database can contain both. The column to the right of that, seen in item 3, is called Thread ID and contains an identifier that is used to link messages to a specific thread, as we discussed when we were looking at the email fragments. The last column, called From Phone Number, seen in item 4, lists the sender's phone number.



| Text | Message Type | Thread ID | Data Source | From Phone Number |
|--|--------------|--|-------------|-------------------|
| This is a deleted incoming message sent from another device. | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-1 | Lab16.001 | +12402528734 |
| Incoming read active extended SMS message. This is an i... | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-1 | Lab16.001 | +12402528734 |
| Incoming unread active extended SMS message. This is a... | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-1 | Lab16.001 | +12402528734 |
| Incoming deleted extended SMS message. This is a delet... | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-1 | Lab16.001 | +12402528734 |
| The following SMS is an active outgoing group message se... | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-2 | Lab16.001 | |
| The following SMS is an active outgoing group message se... | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-2 | Lab16.001 | |
| The following SMS is an active outgoing group message se... | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-2 | Lab16.001 | |
| This is a deleted outgoing message sent to another device. | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-1 | Lab16.001 | |
| 17691234560 Error Invalid Number. Please re-send using a... | SMS Message | bebb9d1d-1406-4177-ac92-ef5d74972623-3 | Lab16.001 | +1121611611 |

8. As you can see from the long list of databases and the data within them, there are many important artifacts that can help to confirm or deny certain findings. We did not review files that are stored on this device but feel free to review them. You can find things like photographs taken, files downloaded, deleted files, and hidden data. In a more advanced course, we can go in-depth into some more useful artifacts that are not readily available or easy to interpret.
9. You are now at the end of the lab. Please close the program by clicking the X at the top-right corner.

