FORENSICS V2 LAB SERIES

Lab 15: IoT Forensics

Document Version: 2021-01-11

Contents

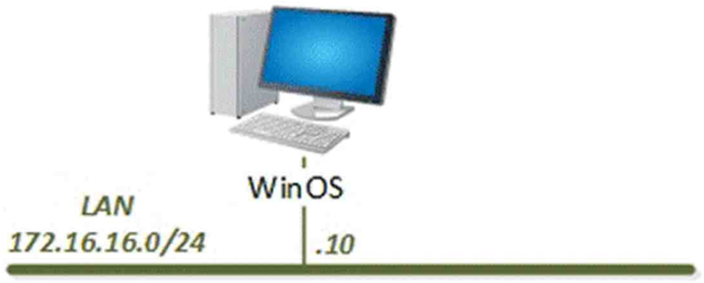
Introduction

With the rise of IoT devices, a new avenue of investigation has been opened. IoT devices store lots of data that help to provide insight into people's behavior and can be used on their own or coupled with other artifacts to answer important questions in investigations.

Objectives

- Learn what IoT devices are
- Learn how to interpret the data captured from IoT devices

Lab Topology



Lab Settings

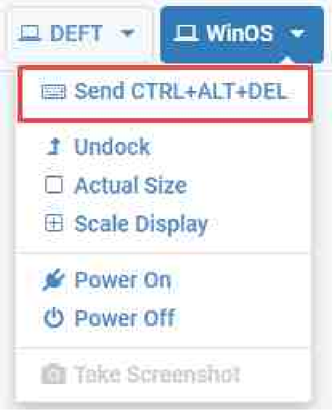
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

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 Files of Interest in a Smart Watch

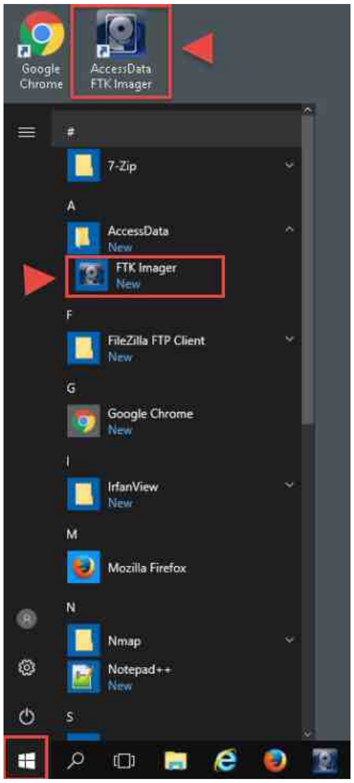
IoT devices consist of a wide variety of electronic devices that are connected to the internet and receive, store, process, and send information in different ways. A lot of the data is never stored on the device, however, but we still find information that is very sensitive, which means it is very helpful for investigations. In this lab, we will guide you through the basic analysis of data from two (2) different IoT devices. They are an Echo Dot and a Samsung Smartwatch.

1. To begin, launch the WinOS virtual machine to access the graphical login screen.
   a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.

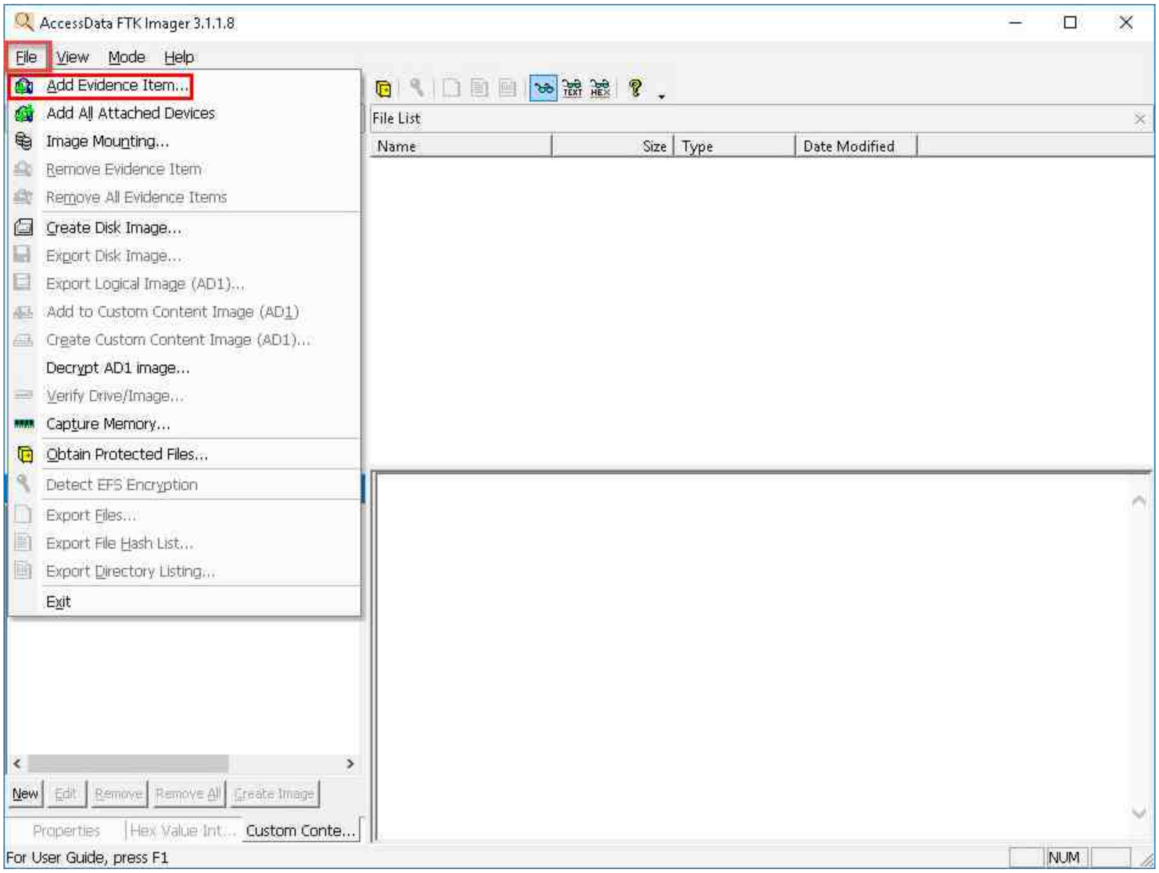


   b. Log in as `Administrator` using the password: `Train1ng$`

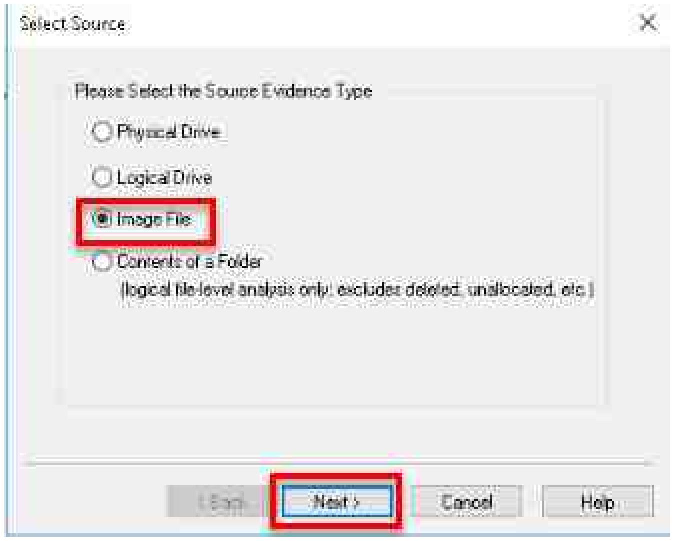
2. Once you are logged into the VM, launch the FTK Imager program from the Windows menu by navigating to Start Menu > AccessData > FTK Imager. Alternatively, you can open FTK Imager from the Desktop by clicking the icon called AccessData FTK Imager:



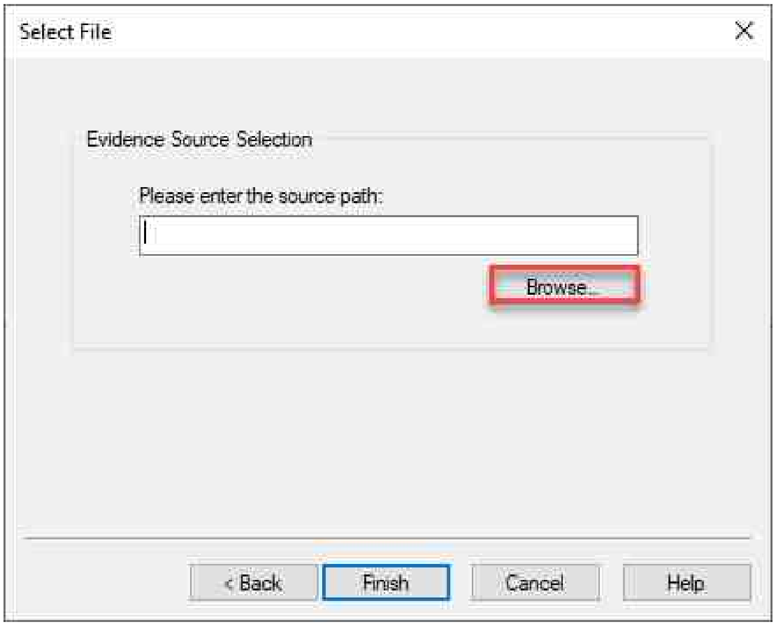
3. You should already be familiar with FTK Imager from our previous labs. In this exercise, we will learn how to navigate to the registry files' locations using some preconfigured Forensic Evidence Files (FEF). Let us begin by loading a FEF. To do this click the File menu option to open the File dropdown menu, then click the Add Evidence Item option from the dropdown menu. It is the first item on the menu, as highlighted below.



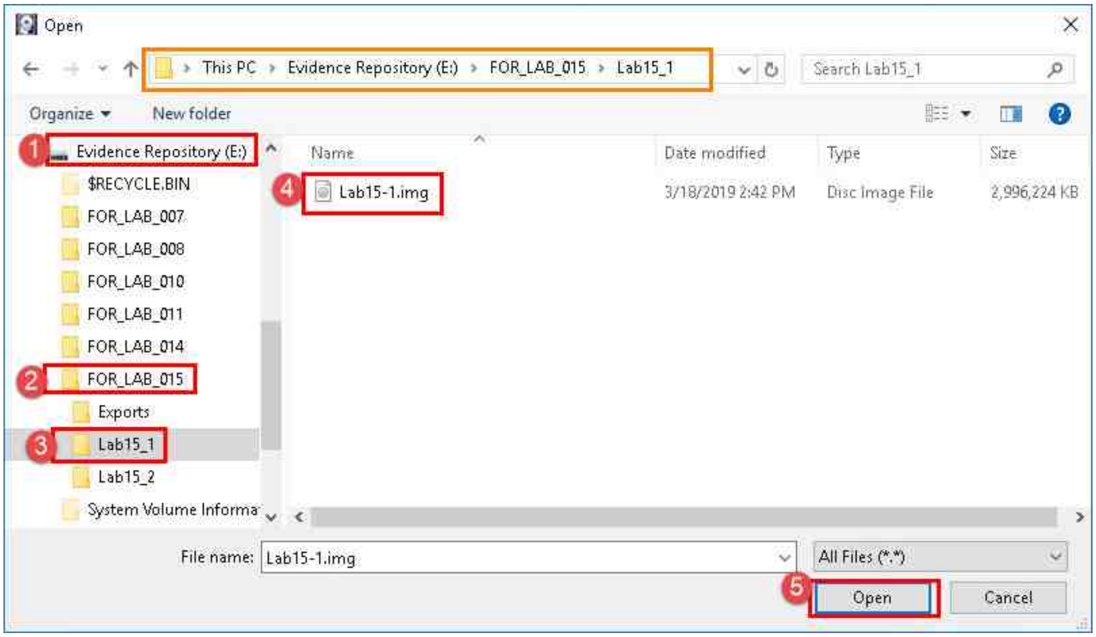
4. You will be brought to the Select Source window. Let us select Image File and click Next as highlighted below.


Select Source
Please Select the Source Evidence Type
○ Physical Drive
○ Logical Drive
● Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help

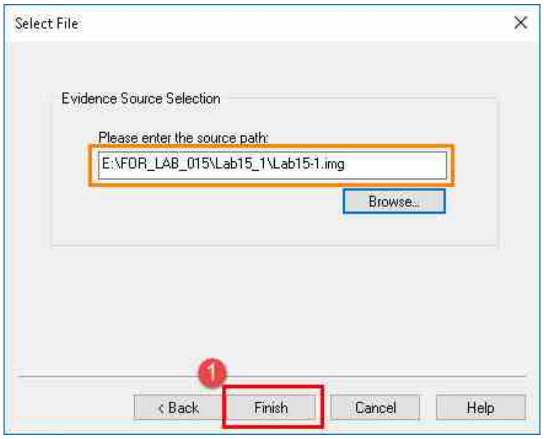
5. In the Select File window, click Browse highlighted in red in the screenshot below. This will open the Select File window, which will allow you to browse to the appropriate FEF.



6. You are now at the Select File window. Browse to This PC > Evidence Repository (E:) > FOR_LAB_015 and double-click the folder called Lab15_1. This will open the folder revealing the FEF called Lab15-1.img. Select the file called Lab15-1.img and click the Open button as highlighted in items 1, 2, 3, 4, and 5 below.

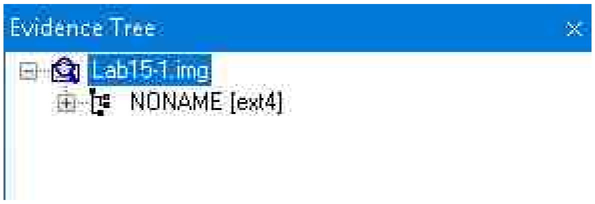


7. Review the source path of the file called Lab15-1.img. In the Select File window, click Finish highlighted in red in the screenshot below. This will take you back to FTK Imager's main window.

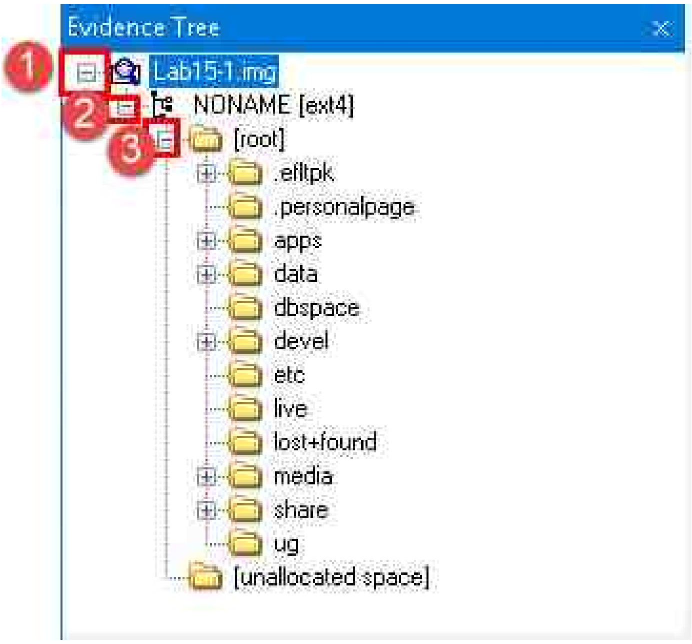


E:\FOR_LAB_015\Lab15_1\Lab15-1.img

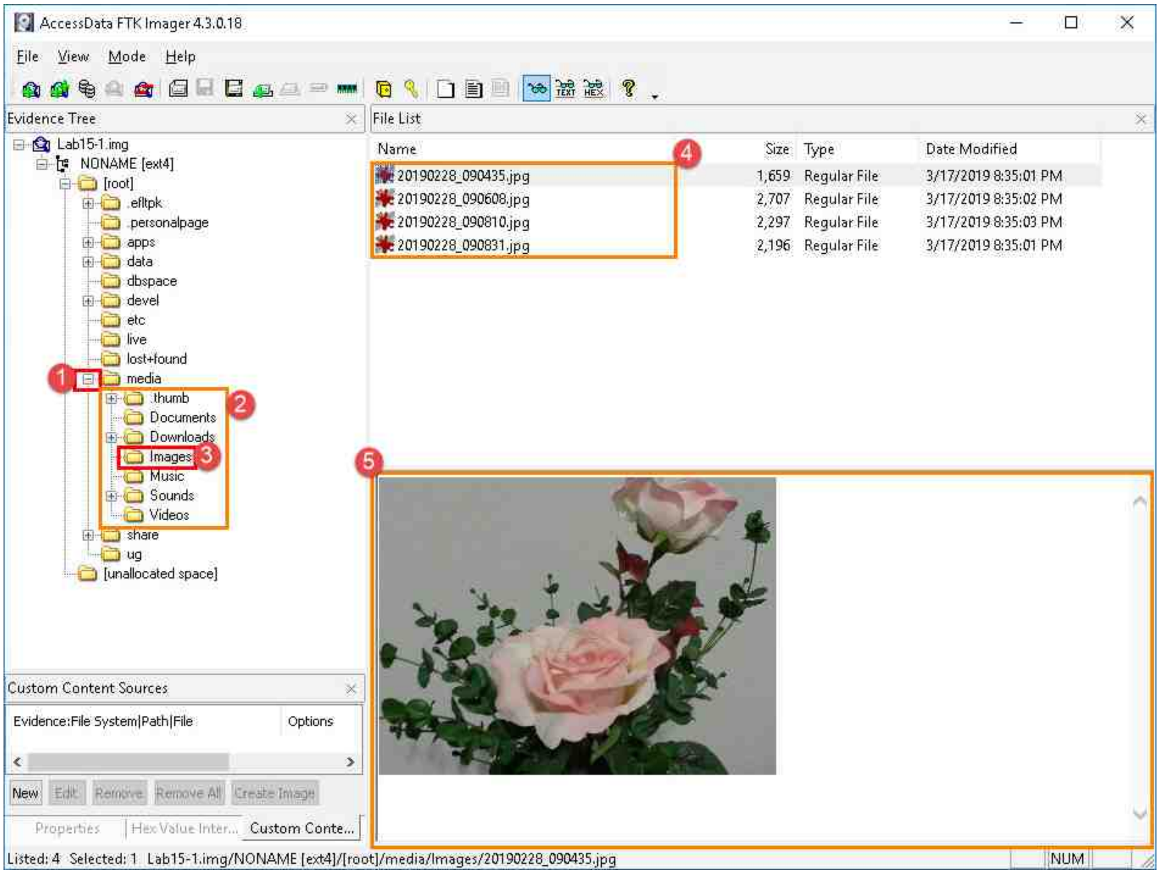
8. If you did everything correctly, you will now be back at FTK Imager's main window with Lab15-1.img listed under the Evidence Tree pane. From the Evidence Tree pane, click the tree item Lab15-1.img highlighted below. This will select the image you are going to peruse.



9. We will now browse the FEF and view its contents. To begin, click the + sign beside the hard drive you added called Lab15-1.img, as seen in item 1 below. This will expand the tree and display the file system on the drive called NONAME [ext4]. The Ext4 file system is a file system that is associated with Linux operating systems, and Android file systems use it as well. Based on this observation, we can quickly assume that this smartwatch uses the Android operating system. Let us dig further by clicking the + sign beside NONAME [ext4], as seen in item 2 below. Next, let us expand the folder called root by clicking the + sign beside it, as seen in item 3 below.



10. Now look at the folder structure and see if there are any folders that you are familiar with. Take the media folder, for example. This folder is typically found on Android phones and extended storage devices like MicroSD cards used within Android phones. Let us look at this folder's contents first. Begin by expanding the media folder by clicking the + beside the media folder, as seen in item 1 below. As you can see in item 2, there are 7 folders within this media folder. This is the location for different media files stored and accessed by the device. Look at the Images folder by clicking it, as seen in item 3 below. This will reveal 4 image files in the File List pane in item 4 below. Click each one to view the content in the View pane in item 5 below. These images that you are accessing are files that have been synchronized with a smartphone. A bonus with these devices is that they may have data on them that may have been deleted from the original device.

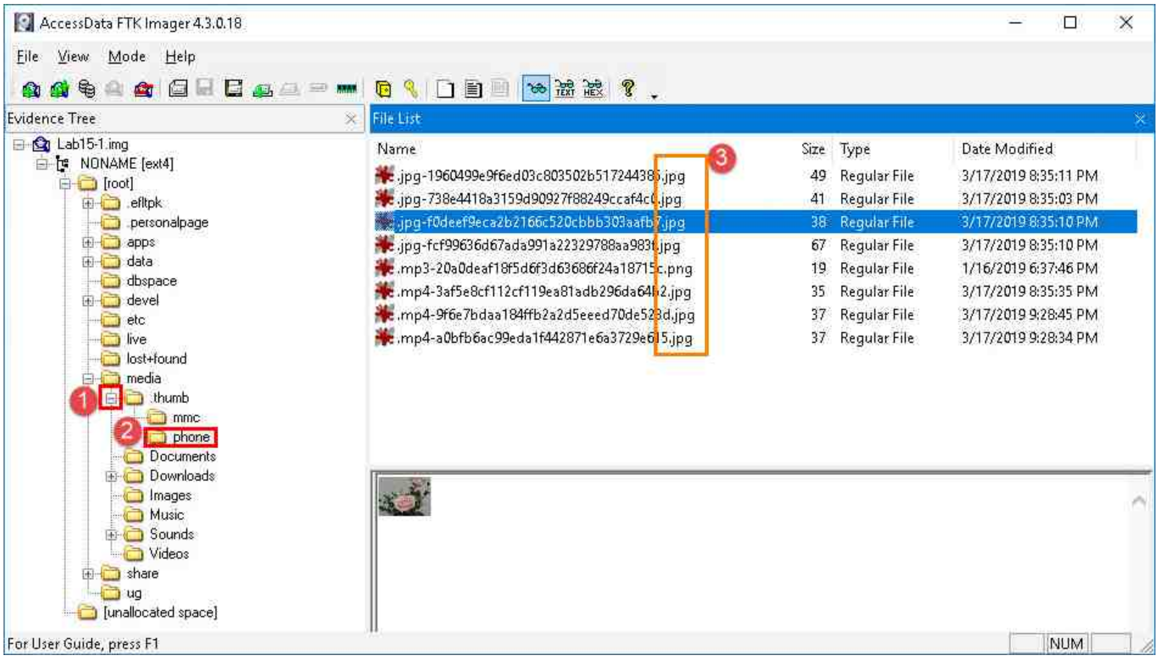


Name	Size	Type	Date Modified
20190228_090435.jpg	1,659	Regular File	3/17/2019 8:35:01 PM
20190228_090608.jpg	2,707	Regular File	3/17/2019 8:35:02 PM
20190228_090810.jpg	2,297	Regular File	3/17/2019 8:35:03 PM
20190228_090831.jpg	2,196	Regular File	3/17/2019 8:35:01 PM

Listed: 4 Selected: 1 Lab15-1.img/NONAME [ext4]/[root]/media/Images/20190228_090435.jpg

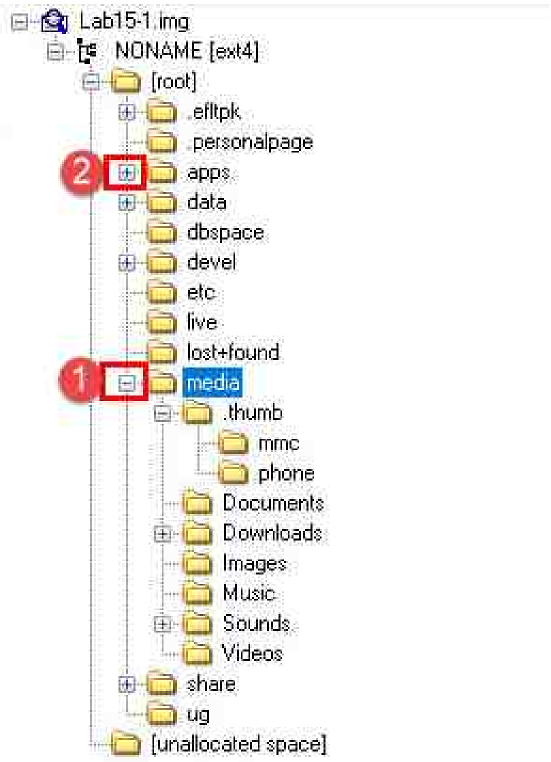
If the displayed image appears too large, press Ctrl + scroll wheel to zoom out or Ctrl + minus (-).

11. Let us take a look at the folder called .thumb. It is a hidden folder, and it contains thumbnails taken from pictures and videos synched with the smartwatch. Navigate to .thumb > phone by clicking the + sign beside each folder, as seen in items 1 and 2 below. You will see a list of files appear in the File List pane bearing names that start with an extension, as seen in item 3 below. The extension refers to the file extension of the file that the thumbnail was created from. If you click the files that begin with .jpg, you will see the same pictures that you looked at in the Images folder. This location is important because there is a chance that you can find thumbnails of files that have been deleted. There are also mp4 thumbnails for videos and even thumbnails for mp3 files that have embedded album cover images. Feel free to review the other files and folders within the media folder. When you are done, we will move on to some databases.

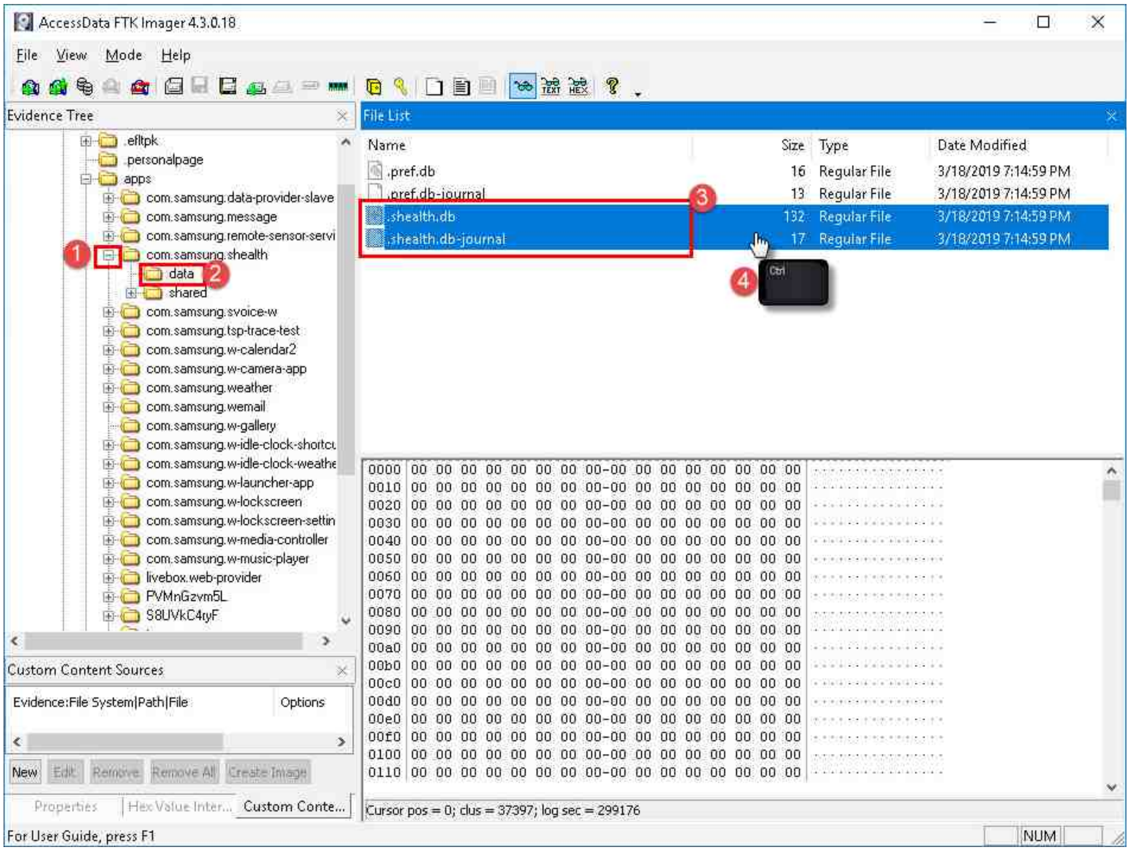


Name	Size	Type	Date Modified
.jpg-1960499e9f6ed03c803502b517244386.jpg	49	Regular File	3/17/2019 8:35:11 PM
.jpg-738e4418a3159d90927f88249ccaf4c0.jpg	41	Regular File	3/17/2019 8:35:03 PM
.jpg-f0deef9eca2b2166c520cbbb303aafb7.jpg	38	Regular File	3/17/2019 8:35:10 PM
.jpg-fcf99636d67ada991a22329788aa983f.jpg	67	Regular File	3/17/2019 8:35:10 PM
.mp3-20a0deaf18f5d6f3d63686f24a18715c.png	19	Regular File	1/16/2019 6:37:46 PM
.mp4-3af5e8cf112cf119ea81adb296da64b2.jpg	35	Regular File	3/17/2019 8:35:35 PM
.mp4-9f6e7bdaa184ffb2a2d5eeed70de523d.jpg	37	Regular File	3/17/2019 9:28:45 PM
.mp4-a0bfb6ac99eda1f442871e6a3729e615.jpg	37	Regular File	3/17/2019 9:28:34 PM

12. Let us export some SQLite database files and review them using DB Browser. Begin by contracting the media folder by clicking the – sign beside it, as seen in item 1 below. Now expand the folder called apps by clicking the + sign as seen in item 2 below.



13. Let us export the health data first. To do this, expand the folder called com.samsung.shealth by clicking the + beside it, as seen in item 1 below. Next, click the folder called data to reveal its contents in the File List pane as seen in items 2 and 3 below. We will be exporting the files called .shealth.db and .shealth.db-journal. Begin this process by highlighting both files. This can be done by holding the Ctrl key and clicking both files, as seen in item 4 below.

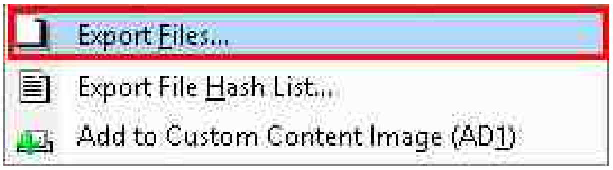


Name	Size	Type	Date Modified
.pref.db	16	Regular File	3/18/2019 7:14:59 PM
.pref.db-journal	13	Regular File	3/18/2019 7:14:59 PM
.shealth.db	132	Regular File	3/18/2019 7:14:59 PM
.shealth.db-journal	17	Regular File	3/18/2019 7:14:59 PM

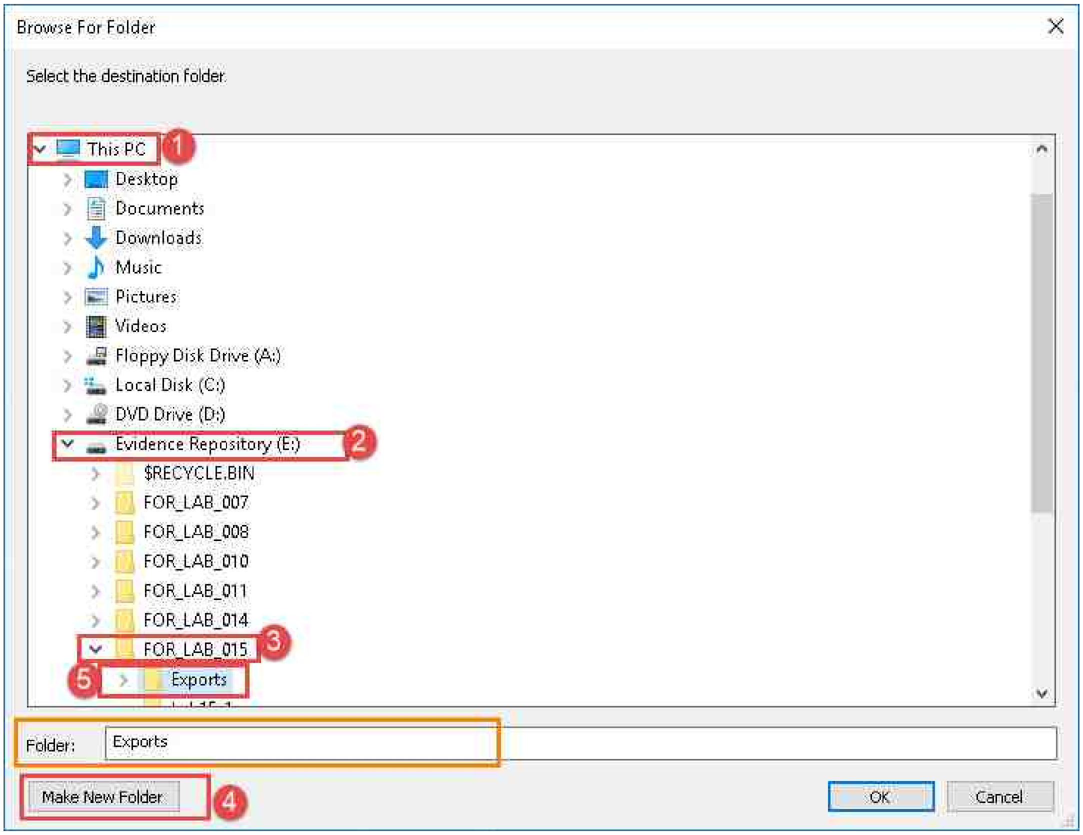
```
0000 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Cursor pos = 0; clus = 37397; log sec = 299176

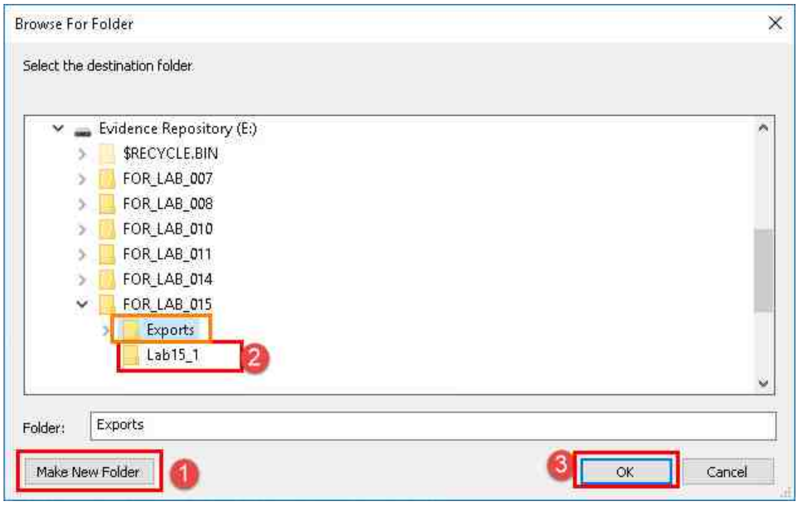
14. Now that the files are highlighted, right-click on the highlighted files, and click Export Files from the context menu that appears.



15. The Browse For Folder window will appear, allowing you to browse to the location where you want to put the files. Navigate to ThisPC > Evidence Repository (E:) as seen in items 1 and 2 below. Once there, click the folder called FOR_LAB_015 and then click the Make New Folder button as seen in item 4 below. This will create a new folder. Name this folder Exports, as seen in item 5 below.



16. Click the folder called Exports to highlight it and then click the Make New Folder button once more to create a subfolder as seen in item 1. Name this new folder `Lab15_1` as seen in item 2, and then click it again to select it. Once that is done, click OK, as seen in item 3 below.

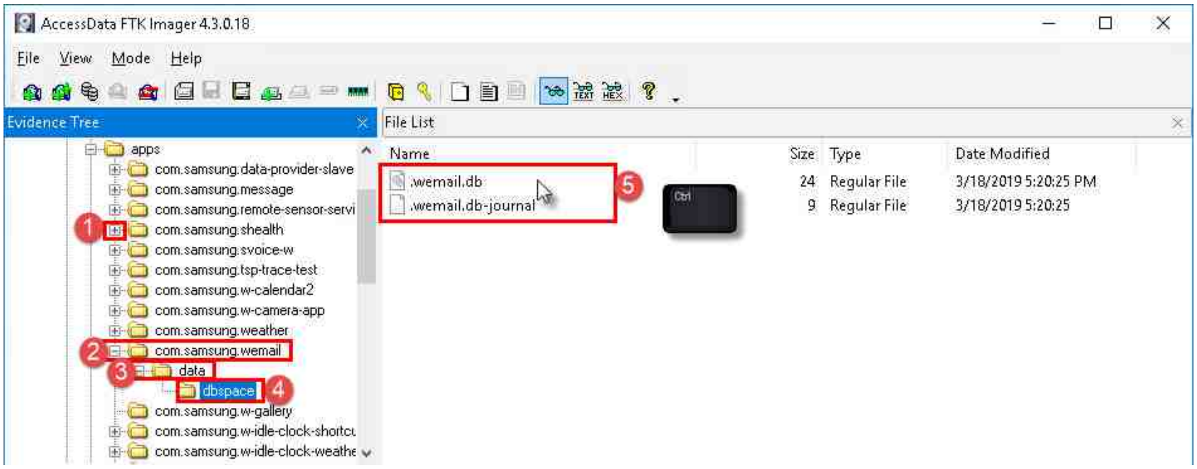


Browse For Folder

Select the destination folder

Folder: Exports

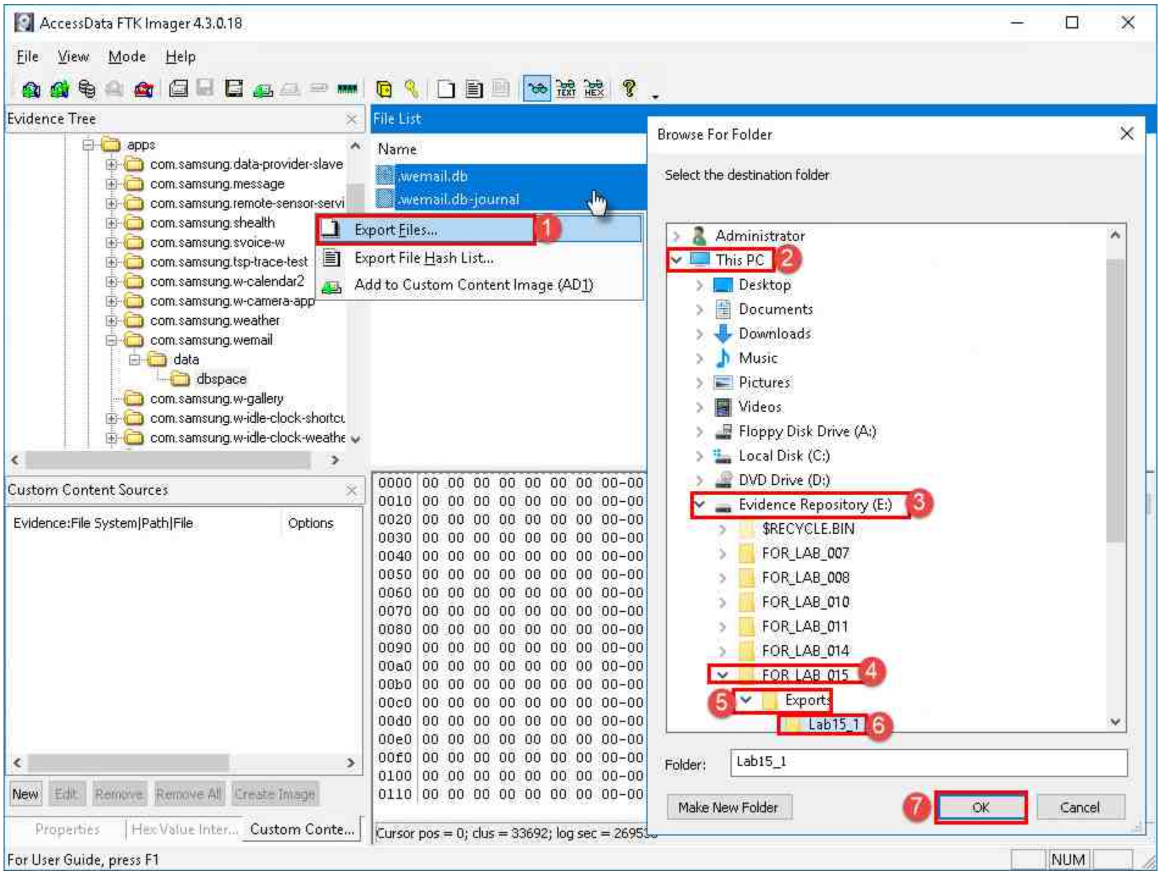
17. Let us get another database file called the .wemail.db. Begin by clicking the – sign beside com.samsung.shealth, as seen in item 1 below. Next, click the + signs beside com.samsung.wemail > data > dbspace, as seen in items 2, 3 and 4 below. Once there, highlight the 2 files called .wemail.db and .wemail.db-journal by holding the Ctrl key and clicking them as seen in item 5.



AccessData FTK Imager 4.3.0.18

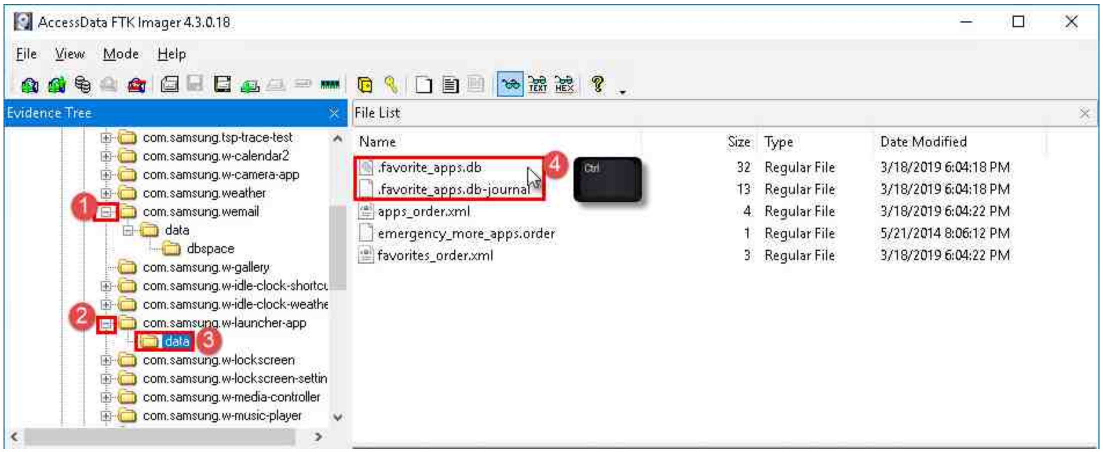
Name	Size	Type	Date Modified
.wemail.db	24	Regular File	3/18/2019 5:20:25 PM
.wemail.db-journal	9	Regular File	3/18/2019 5:20:25

18. Let us export these files to the same folder as before. Right-click on the highlighted file(s) and click the Export Files button from the context menu that appears as seen in item 1. This will open the Browser For Folder window. Navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_015 > Exports as seen in items 2, 3, 4 and 5 below. Click the folder called Lab15_1 to select it, and then click OK, as seen in items 6 and 7 below.



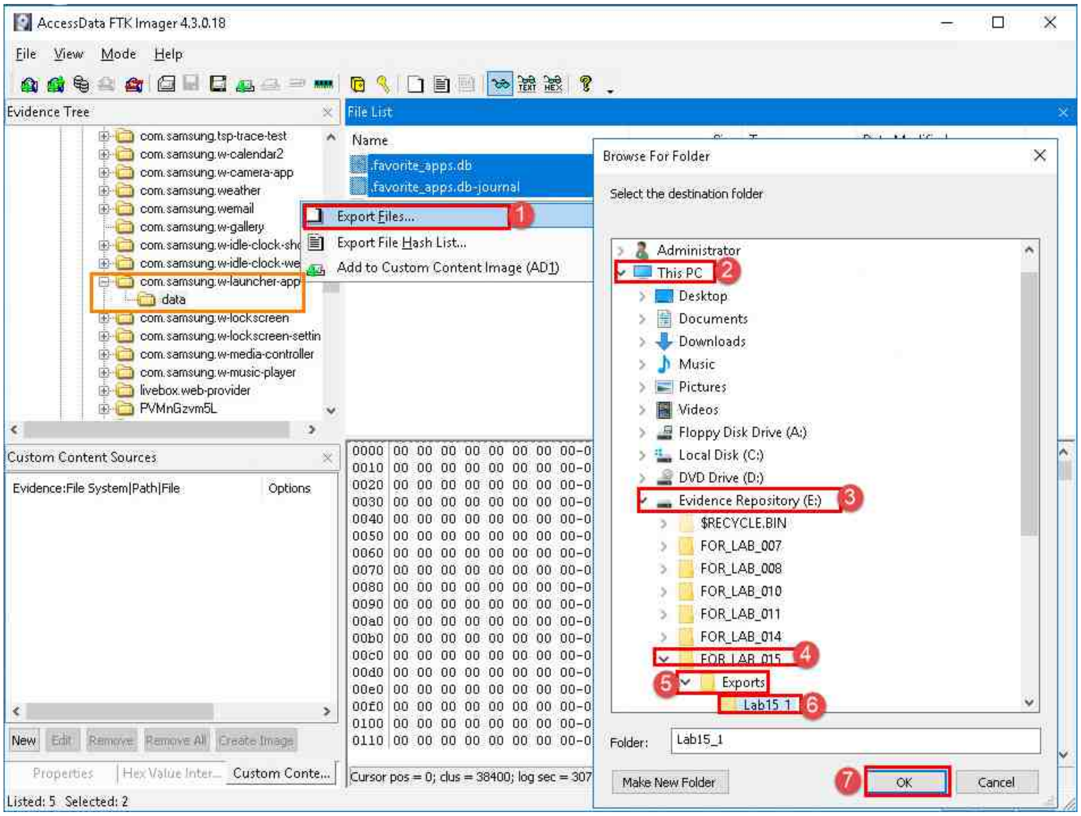
```
0000 00 00 00 00 00 00 00 00-00
0010 00 00 00 00 00 00 00 00-00
0020 00 00 00 00 00 00 00 00-00
0030 00 00 00 00 00 00 00 00-00
0040 00 00 00 00 00 00 00 00-00
0050 00 00 00 00 00 00 00 00-00
0060 00 00 00 00 00 00 00 00-00
0070 00 00 00 00 00 00 00 00-00
0080 00 00 00 00 00 00 00 00-00
0090 00 00 00 00 00 00 00 00-00
00a0 00 00 00 00 00 00 00 00-00
00b0 00 00 00 00 00 00 00 00-00
00c0 00 00 00 00 00 00 00 00-00
00d0 00 00 00 00 00 00 00 00-00
00e0 00 00 00 00 00 00 00 00-00
00f0 00 00 00 00 00 00 00 00-00
0100 00 00 00 00 00 00 00 00-00
0110 00 00 00 00 00 00 00 00-00
```

19. The last database we will export is called .favorite_apps.db. Begin by clicking the – sign beside com.samsung.wemail as seen in item 1 below. Next, click the + signs beside com.samsung.w-launcher-app > data, as seen in items 2 and 3 below. Once there, highlight the 2 files called .favorite_apps.db and .favorite_apps.db-journal by holding the Ctrl key and clicking them, as seen in item 4.

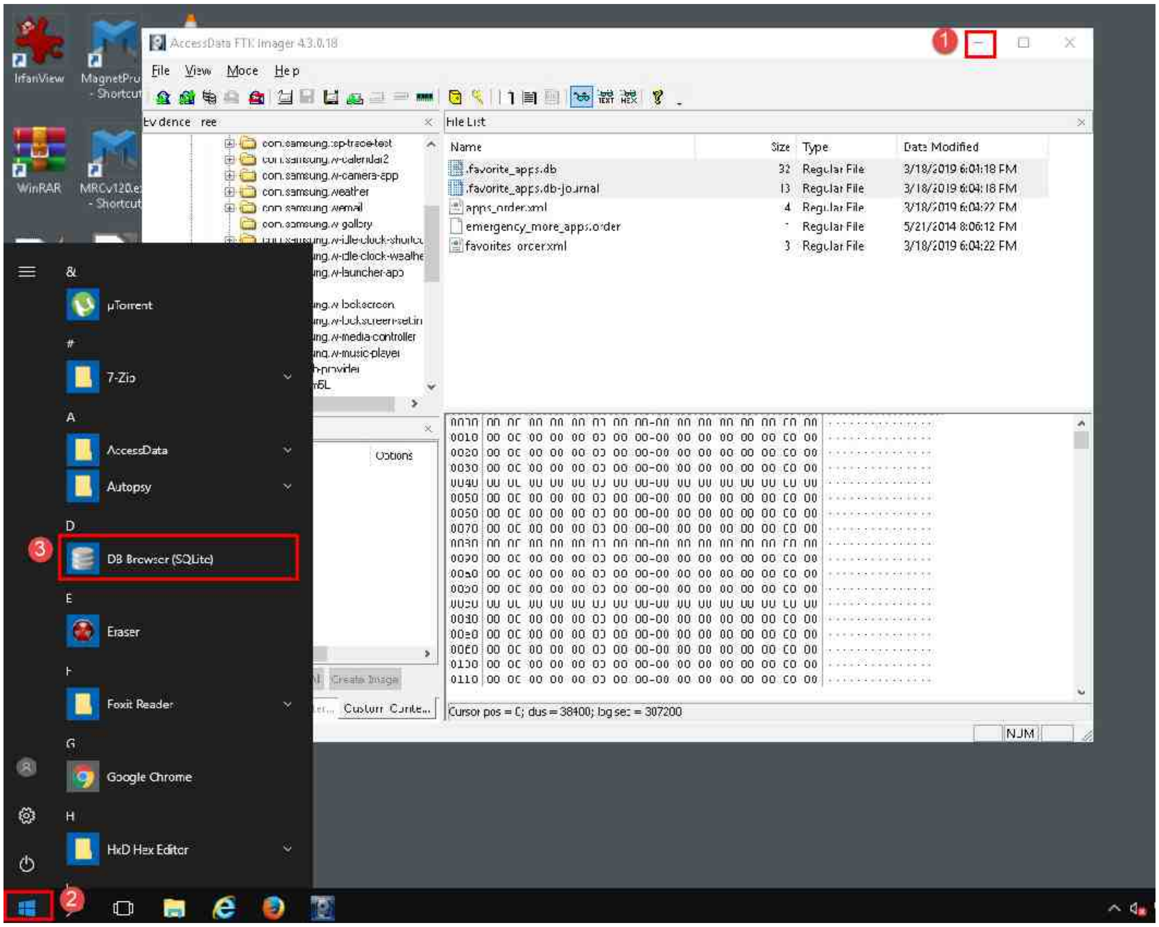

AccessData FTK Imager 4.3.0.18
File View Mode Help
Evidence Tree
com.samsung.tsp-trace-test
com.samsung.w-calendar2
com.samsung.w-camera-app
com.samsung.weather
1
com.samsung.wemail
data
dbspace
com.samsung.w-gallery
com.samsung.w-idle-clock-shortcu
com.samsung.w-idle-clock-weathe
2
com.samsung.w-launcher-app
data
3
com.samsung.w-lockscreen
com.samsung.w-lockscreen-settin
com.samsung.w-media-controller
com.samsung.w-music-player
File List
4
Ctrl

Name	Size	Type	Date Modified
.favorite_apps.db	32	Regular File	3/18/2019 6:04:18 PM
.favorite_apps.db-journal	13	Regular File	3/18/2019 6:04:18 PM
apps_order.xml	4	Regular File	3/18/2019 6:04:22 PM
emergency_more_apps.order	1	Regular File	5/21/2014 8:06:12 PM
favorites_order.xml	3	Regular File	3/18/2019 6:04:22 PM

20. Let us export these files to the same folder as before. Right-click on the highlighted file(s) and click the Export Files button from the context menu that appears, as seen in item 1. This will open the Browser For Folder window. Navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_015 > Exports as seen in items 2, 3, 4, and 5 below. Click the folder called Lab15_1 to select it, and then click OK as seen in items 5 and 6 below.



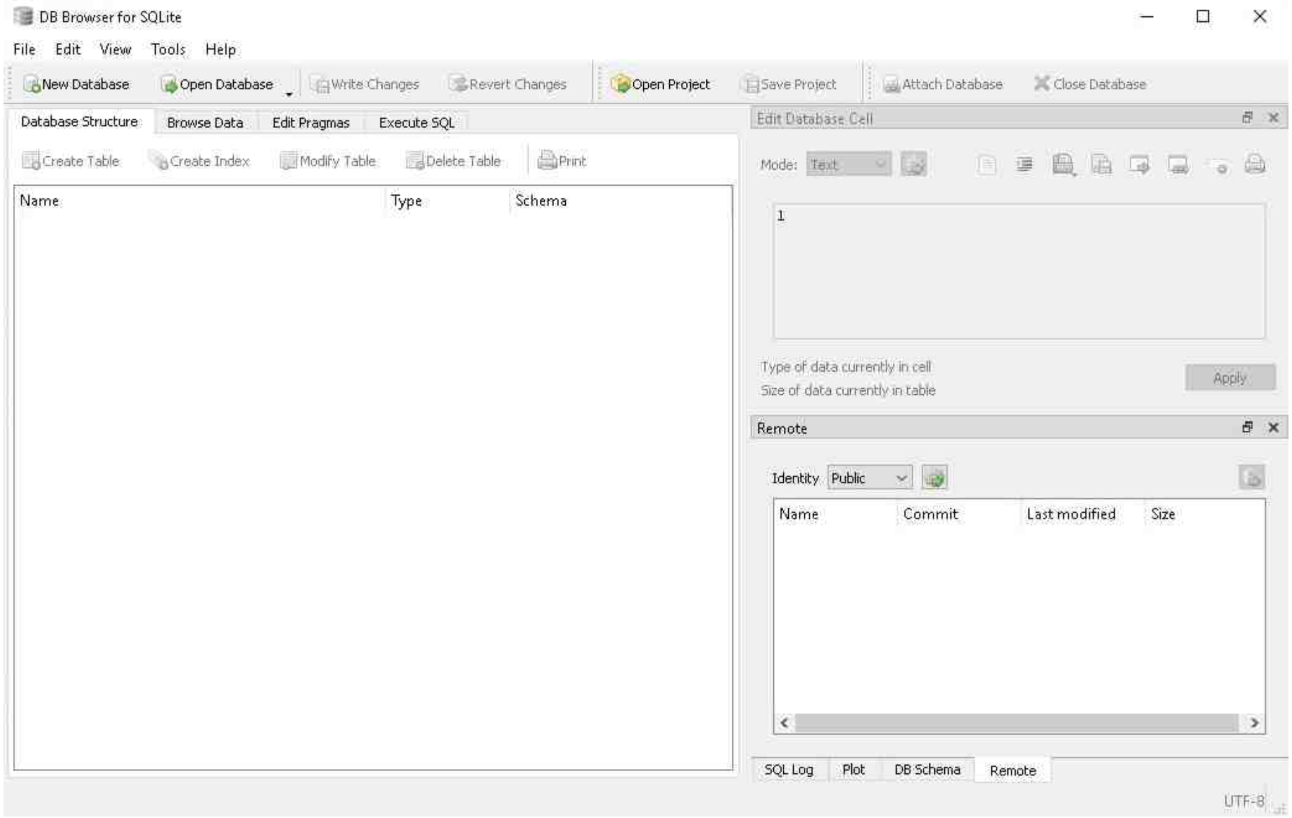
21. Now that we have all 3 files exported, let us look at the data they contain. We will be using DB Browser for SQLite.
22. The DB Browser for SQLite software is a powerful database browser that allows you to easily view the contents of SQLite databases. Let us open it and jump right in to learn some of the features we will be using. Minimize FTK Imager and open DB Browser for SQLite by navigating to Start > DB Browser (SQLite) as seen in items 1, 2 and 3 below. Alternatively, you can open the application from the icon on the desktop.



Name	Size	Type	Date Modified
.favorite_apps.db	32	Regular File	3/18/2019 6:01:18 PM
.favorite_apps.db-journal	13	Regular File	3/18/2019 6:04:18 PM
apps_order.xml	4	Regular File	3/18/2019 6:04:22 PM
emergency_more_apps.order	1	Regular File	5/21/2014 8:06:12 PM
favorites_order.xml	3	Regular File	3/18/2019 6:04:22 PM

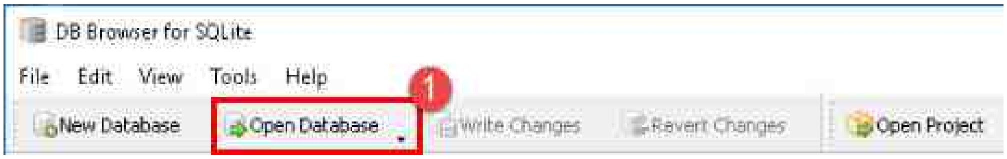
Cursor pos = 0; clus = 38400; log sec = 307200

23. Once the program opens, you will be presented with the main GUI. The table below the following screenshot provides details about some of the features we will be using.

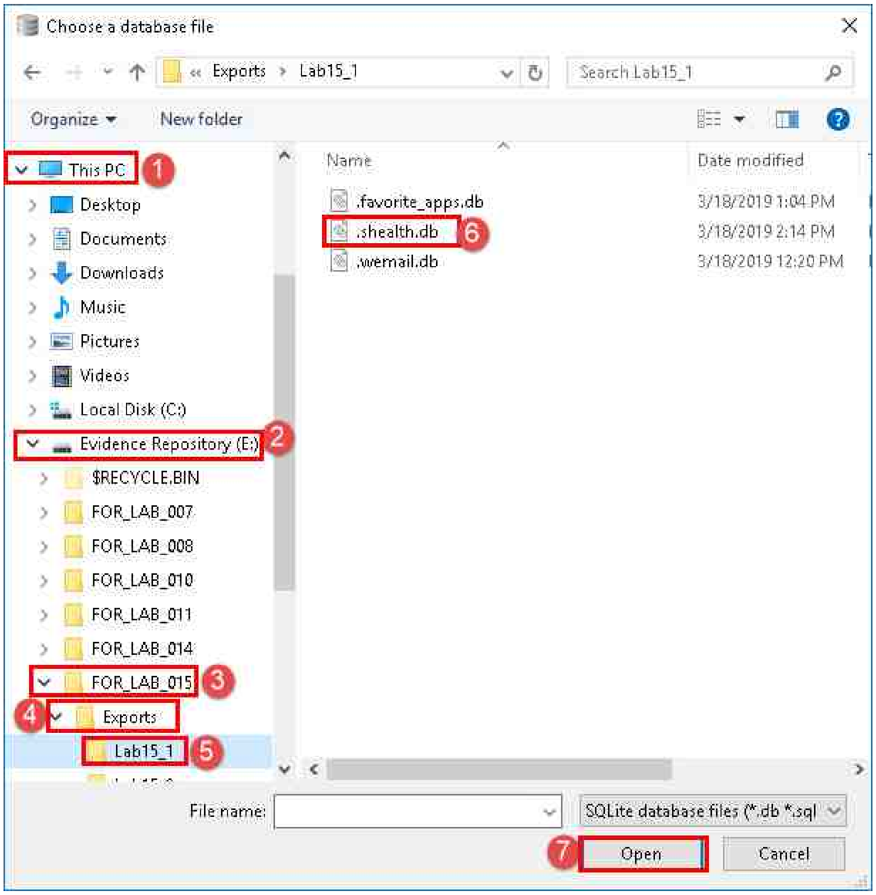


1	Open Database	This option allows you to browse to the location of the database file
2	Browse Data tab	This is the tab that allows you to navigate the different tables and view their data
3	Table area	This area is where the data is displayed
4	Menu bar	This area has a wide variety of options such as changing the view area, creating, editing, and opening databases, and providing help
5	Data View	Displays the data in a selected cell

24. Let us open the first database file we exported, .shealth.db. Do this by clicking the Open Database button seen in item 1 below. This will open the Choose a database file window.



25. In the Choose a database file window, navigate to This PC > Evidence Repository > FOR_LAB_015 > Exports > Lab15_1 as seen in items 1, 2, 3, 4, and 5 below. Once there, select the file called .shealth.db by clicking it and then click Open as seen in items 6 and 7 below.



26. The database file will be loaded. You can verify this by looking at the path and filename at the top bar of the window seen in item 1 below. Now select the Browse Data tab as seen in item 2 below to switch to the table view. Now let us select a different table by clicking the Table dropdown menu and clicking shealth_profile as seen in items 3 and 4 below.

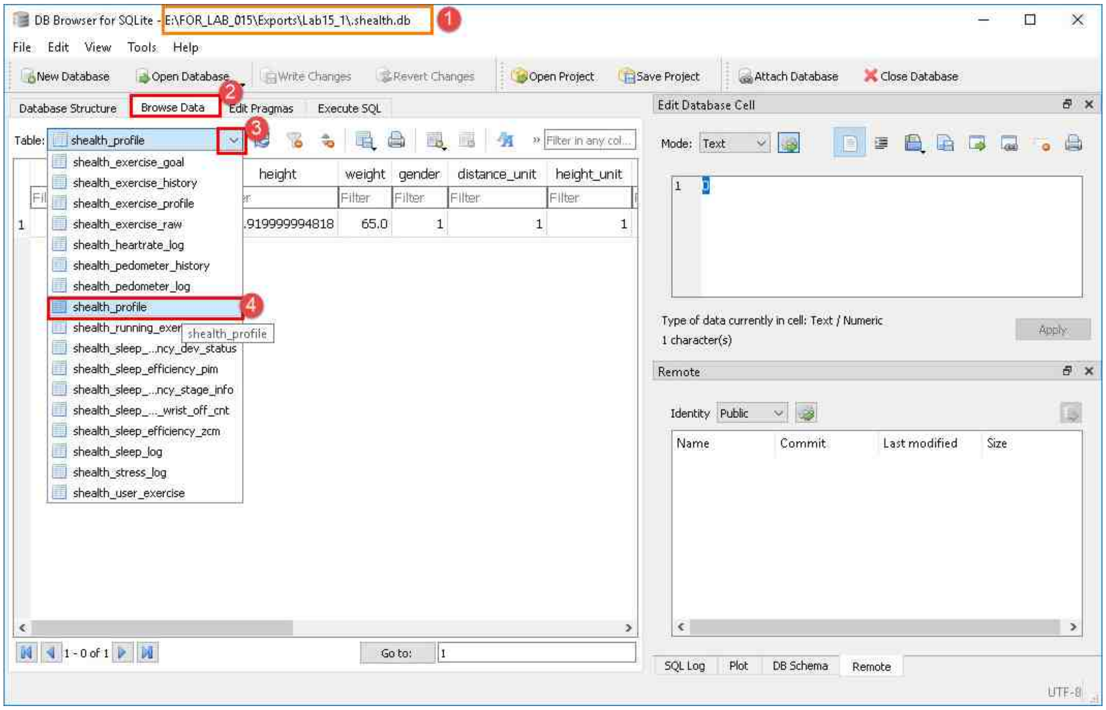


Table: shealth_profile

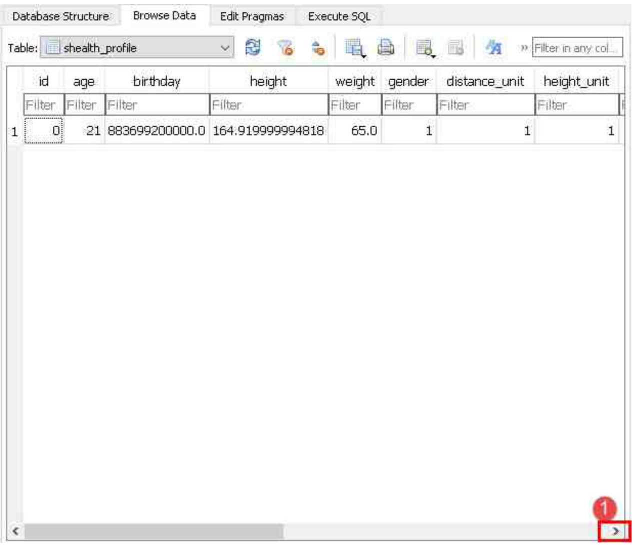
- shealth_exercise_goal
- shealth_exercise_history
- shealth_exercise_profile
- shealth_exercise_raw
- shealth_heartrate_log
- shealth_pedometer_history
- shealth_pedometer_log
- shealth_profile
- shealth_running_exer
- shealth_sleep_...ncy_dev_status
- shealth_sleep_efficiency_pim
- shealth_sleep_...ncy_stage_info
- shealth_sleep_..._wrist_off_cnt
- shealth_sleep_efficiency_zcm
- shealth_sleep_log
- shealth_stress_log
- shealth_user_exercise

	height	weight	gender	distance_unit	height_unit
1	.919999994818	65.0	1	1	1

1 - 0 of 1

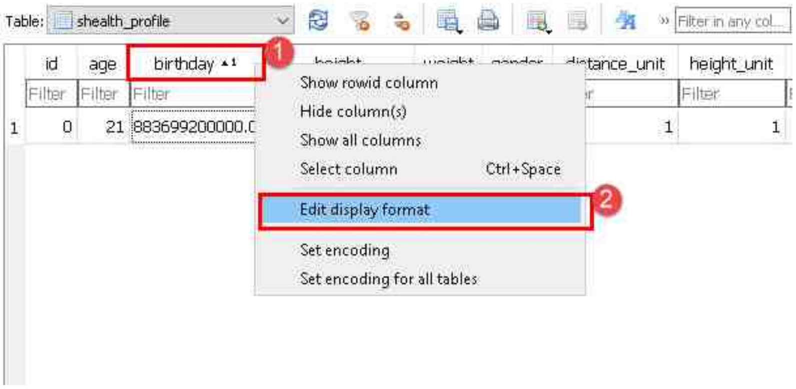
Type of data currently in cell: Text / Numeric
1 character(s)

27. You will now be taken to the health profile created by the user. As you can see from the names of the columns and the data in the row, there is attribution data such as the user's age, birthday, height, weight, pedometer goal, and even the date the profile was created. You can scroll to the right by clicking the arrow as seen in item 1 or by dragging the scroll bar.

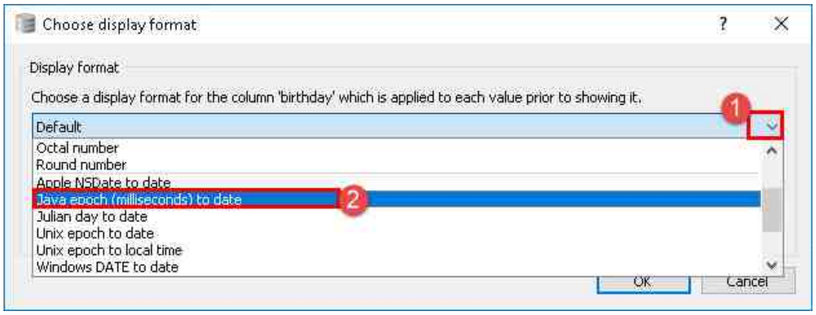


	id	age	birthday	height	weight	gender	distance_unit	height_unit
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	0	21	883699200000.0	164.919999994818	65.0	1	1	1

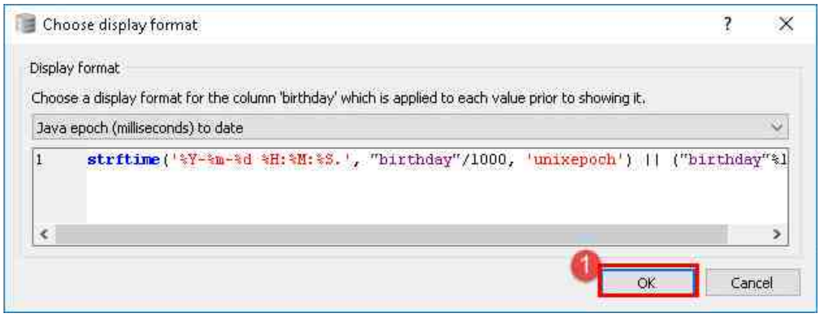
28. The dates and times are stored in Unix Time. Let us convert it to see the date of birth of the user. Do this by right-clicking on the column heading birthday and clicking the Edit display format option from the context menu as seen in items 1 and 2 below.



29. The Choose display format window will appear. Click the dropdown menu as seen in item 1 and select Java epoch (milliseconds) to date from the menu seen in item 2 below.



30. Once done, click OK as seen in item 1 to convert the data in the column. This will immediately display the birthday in a more familiar format, as you can see in item 2.


Choose display format
?
×
Display format
Choose a display format for the column 'birthday' which is applied to each value prior to showing it.
Java epoch (milliseconds) to date
1
OK
Cancel

```
strftime('%Y-%m-%d %H:%M:%S.', "birthday"/1000, 'unixepoch') || ("birthday"%1
```

31. Now scroll to the right using the scroll bar or arrow seen in item 1 below and repeat the above steps to convert the timestamp column seen in item 2 below. This is the creation date of the profile; note this date.

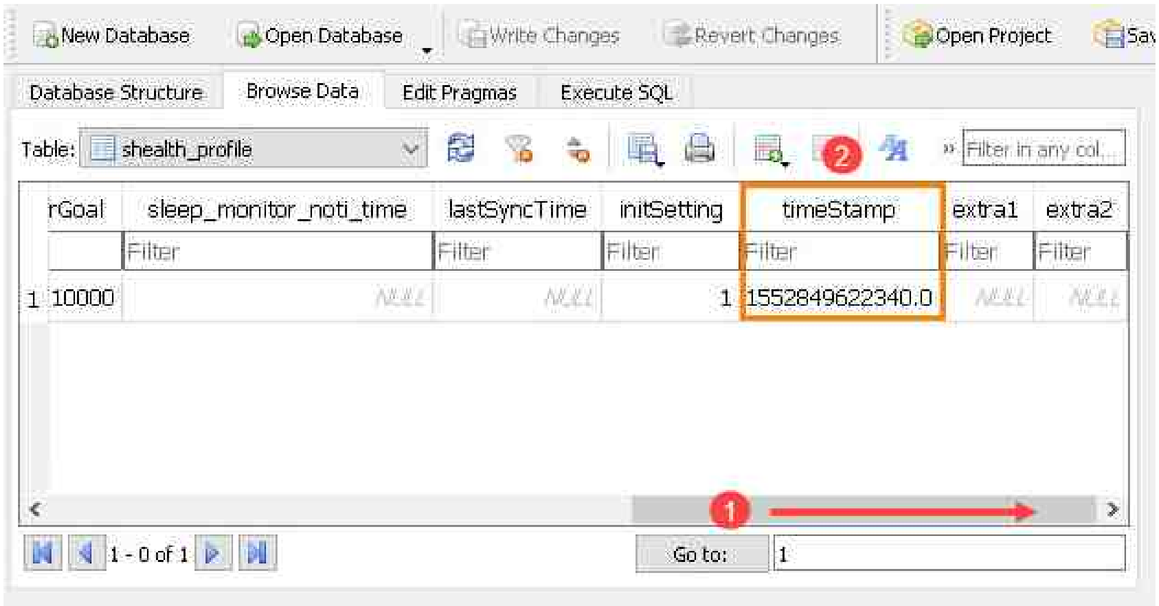


Table: shealth_profile

	rGoal	sleep_monitor_noti_time	lastSyncTime	initSetting	timeStamp	extra1	extra2
		Filter	Filter	Filter	Filter	Filter	Filter
1	10000	NULL	NULL	1	1552849622340.0	NULL	NULL

32. Let us look at the pedometer data. Do this by selecting the shealth_pedometer_history table from the Table dropdown menu as seen in items 1 and 2. As you can see from this table, we can tell whether the user was running or walking and how many steps they took on specific dates. You can also learn the distance and the estimated number of calories burned.

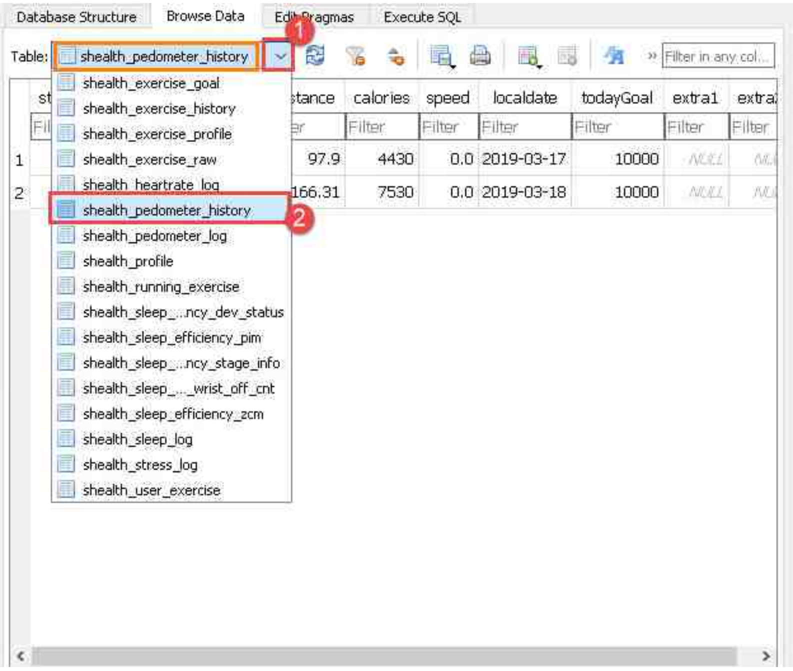
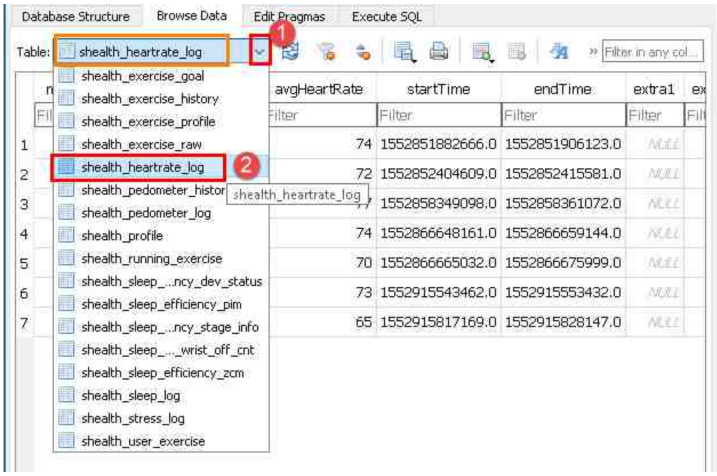


Table: shealth_pedometer_history

	st	stance	calories	speed	localdate	todayGoal	extra1	extra
	Fil	er	Filter	Filter	Filter	Filter	Filter	Filter
1		97.9	4430	0.0	2019-03-17	10000	NULL	NU
2		166.31	7530	0.0	2019-03-18	10000	NULL	NU

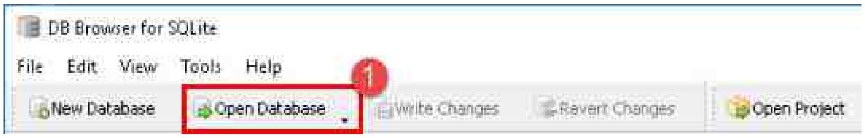
33. The last table we will look at is the log for the pedometer. To do this, click shealth_heartrate_log from the Table dropdown menu, as seen in items 1 and 2 below. This table is associated with the user's heart rate and can tell how fast their heart was beating on a specific date. This data is great when compared to the pedometer data to determine if an accelerated heart rate is the result of an activity such as running or something else.



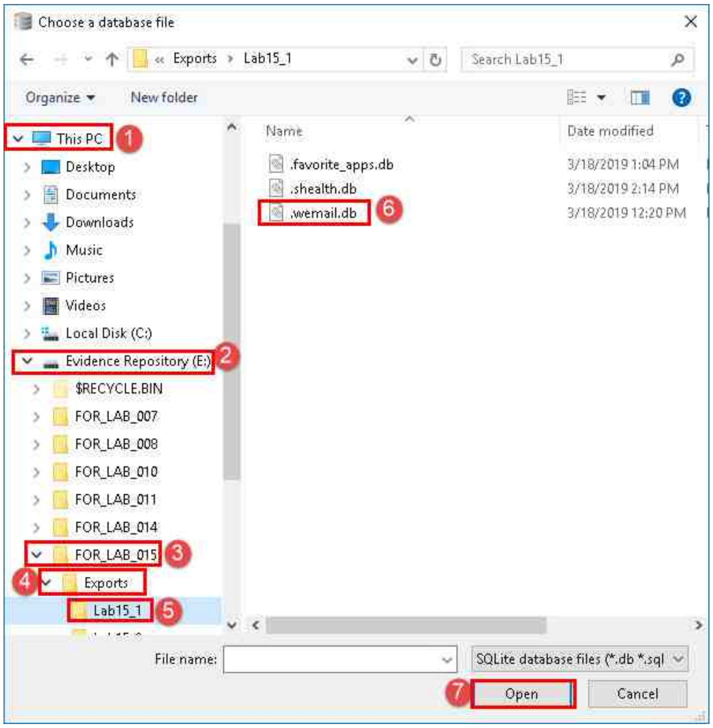
	avgHeartRate	startTime	endTime	extra1
	Filter	Filter	Filter	Filter
1	74	1552851882666.0	1552851906123.0	NULL
2	72	1552852404609.0	1552852415581.0	NULL
3	77	1552858349098.0	1552858361072.0	NULL
4	74	1552866648161.0	1552866659144.0	NULL
5	70	1552866665032.0	1552866675999.0	NULL
6	73	1552915543462.0	1552915553432.0	NULL
7	65	1552915817169.0	1552915828147.0	NULL

As previously mentioned, the dates and times are stored in Unix Time. Please change the displayed format option to Java epoch (milliseconds) to date, using the steps outlined at No. 27, where applicable.

34. As you can see from the table, the data lists the average heart rate and can also contain the minimum and maximum rates over time. It also lists the start time and end time in epoch time as well. Convert these times and note them.
35. Next, look at another database file we exported. This is the .wemail.db file. Open it by clicking the Open Database button seen in item 1 below. This will open the Choose a database file window.

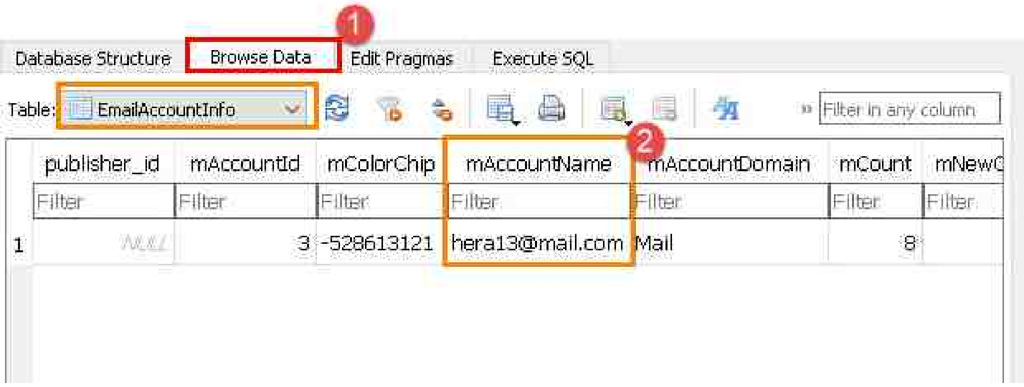


36. In the Choose a database file window, navigate to ThisPC > Evidence Repository > FOR_LAB_015 > Exports > Lab15_1 as seen in items 1, 2, 3, 4, and 5 below. Once there, select the file called .wemail.db by clicking it and then click Open as seen in items 6 and 7 below.



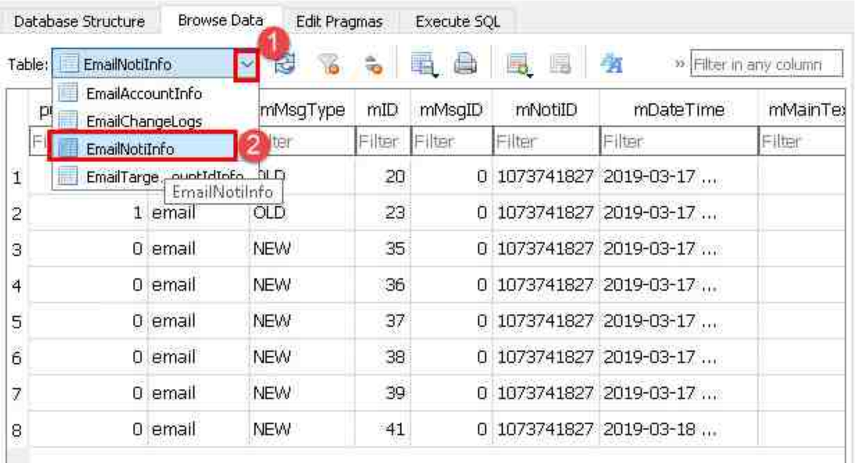
Name	Date modified
.favorite_apps.db	3/18/2019 1:04 PM
.shealth.db	3/18/2019 2:14 PM
.wemail.db	3/18/2019 12:20 PM

37. Now select the Browse Data tab as seen in item 1 below to switch to the table view. The first table you will see is the EmailAccountInfo table, and it contains the email data for the associated user. As you can see in item 2 below, the Account name is an email address hera13@mail.com.



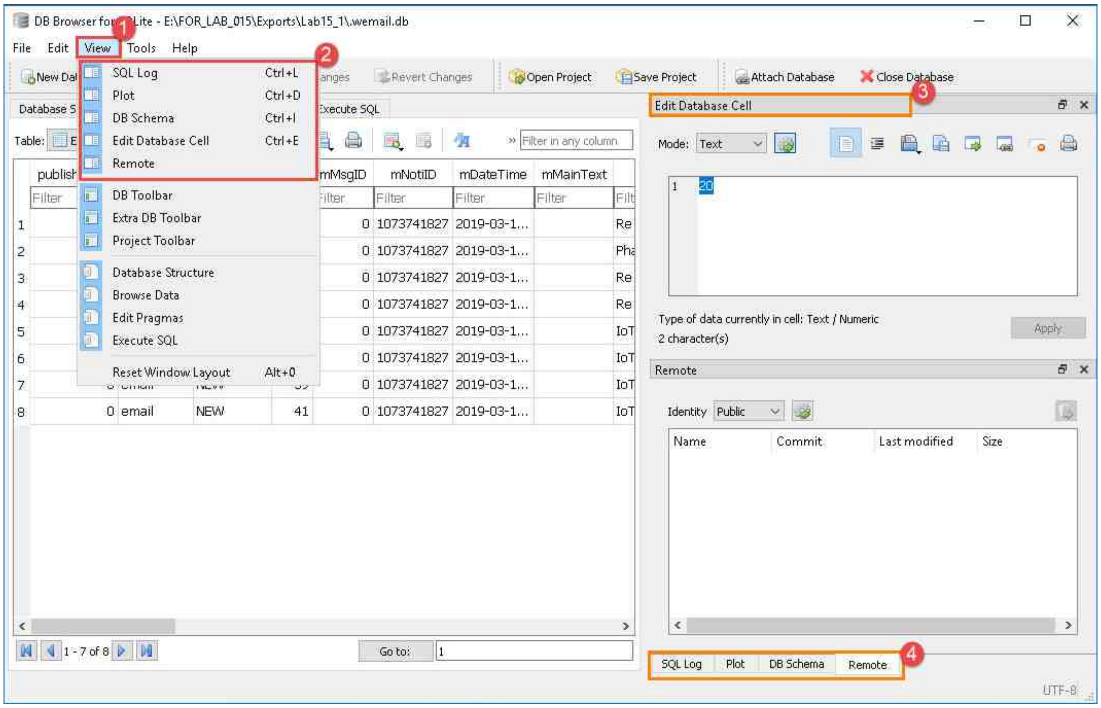
	publisher_id	mAccountId	mColorChip	mAccountName	mAccountDomain	mCount	mNewC
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	NULL	3	-528613121	hera13@mail.com	Mail	8	

38. Let us look at another table in this database. This is the EmailNotiInfo table, and it stores the notifications that appear when the synchronized cell phone receives an email or other message. This is very helpful because you can see some of the message's content. To access this table, click EmailNotiInfo from the Table Dropdown menu, as seen in items 1 and 2 below.



	pl...		mMsgType	mID	mMsgID	mNotiID	mDateTime	mMainTex
	Fi...		...ilter	Filter	Filter	Filter	Filter	Filter
1			OLD	20	0	1073741827	2019-03-17 ...	
2	1	email	OLD	23	0	1073741827	2019-03-17 ...	
3	0	email	NEW	35	0	1073741827	2019-03-17 ...	
4	0	email	NEW	36	0	1073741827	2019-03-17 ...	
5	0	email	NEW	37	0	1073741827	2019-03-17 ...	
6	0	email	NEW	38	0	1073741827	2019-03-17 ...	
7	0	email	NEW	39	0	1073741827	2019-03-17 ...	
8	0	email	NEW	41	0	1073741827	2019-03-18 ...	

39. For the next step, you will need a full view of the DB Browser to examine the full table. Let us disable the default features before proceeding. Start by selecting View from the navigation panel, as seen in item 1 below. Then click each feature separately to have them disabled or use their unique shortcut keys (Ctrl+Letter) to achieve the same results as seen in item 2 below. Items 3 and 4 are the features we are removing from view ONLY.



					mMsgID	mNotiID	mDateTime	mMainText	
1					0	1073741827	2019-03-1...		Re
2					0	1073741827	2019-03-1...		Pha
3					0	1073741827	2019-03-1...		Re
4					0	1073741827	2019-03-1...		Re
5					0	1073741827	2019-03-1...		IoT
6					0	1073741827	2019-03-1...		IoT
7					0	1073741827	2019-03-1...		IoT
8	0	email	NEW	41	0	1073741827	2019-03-1...		IoT

40. As you can see from the table that appears, there is a lot of data captured here. Let us convert the dates for this table but be aware that this table stores dates in a slightly different format. Begin by right-clicking the column header called mDateTime and then select Edit display format from the context menu that appears.

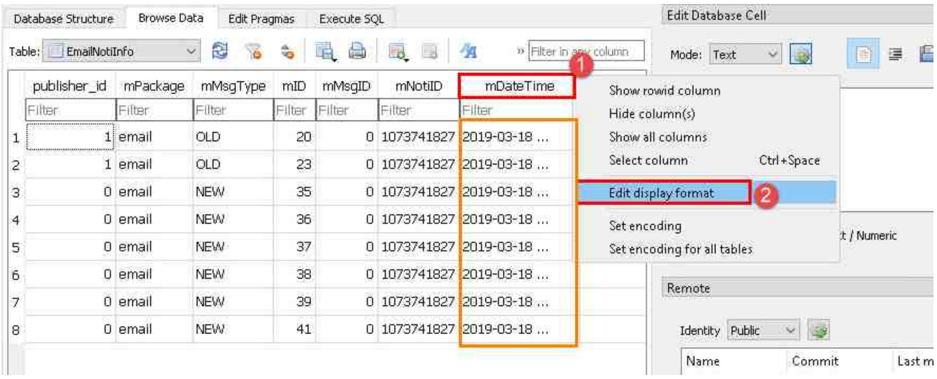


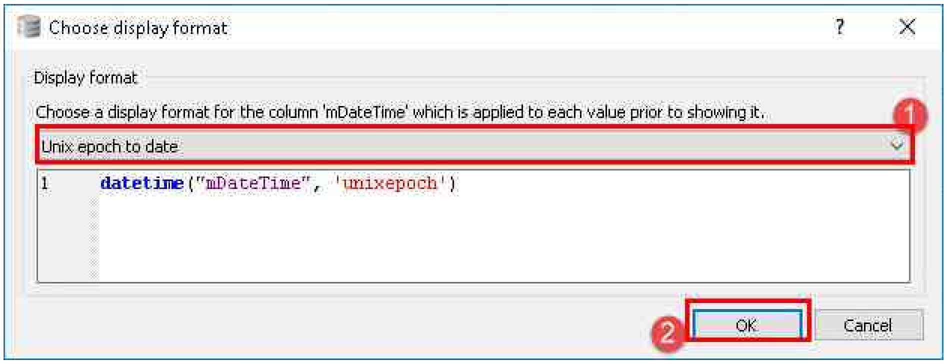
Table: EmailNotiInfo

Mode: Text

Identity: Public

	publisher_id	mPackage	mMsgType	mID	mMsgID	mNotiID	mDateTime
1	1	email	OLD	20	0	1073741827	2019-03-18 ...
2	1	email	OLD	23	0	1073741827	2019-03-18 ...
3	0	email	NEW	35	0	1073741827	2019-03-18 ...
4	0	email	NEW	36	0	1073741827	2019-03-18 ...
5	0	email	NEW	37	0	1073741827	2019-03-18 ...
6	0	email	NEW	38	0	1073741827	2019-03-18 ...
7	0	email	NEW	39	0	1073741827	2019-03-18 ...
8	0	email	NEW	41	0	1073741827	2019-03-18 ...

41. When the Choose display format window appears, select Unix epoch to date from the dropdown menu as seen in item 1 and then click OK as seen in item 2 below.

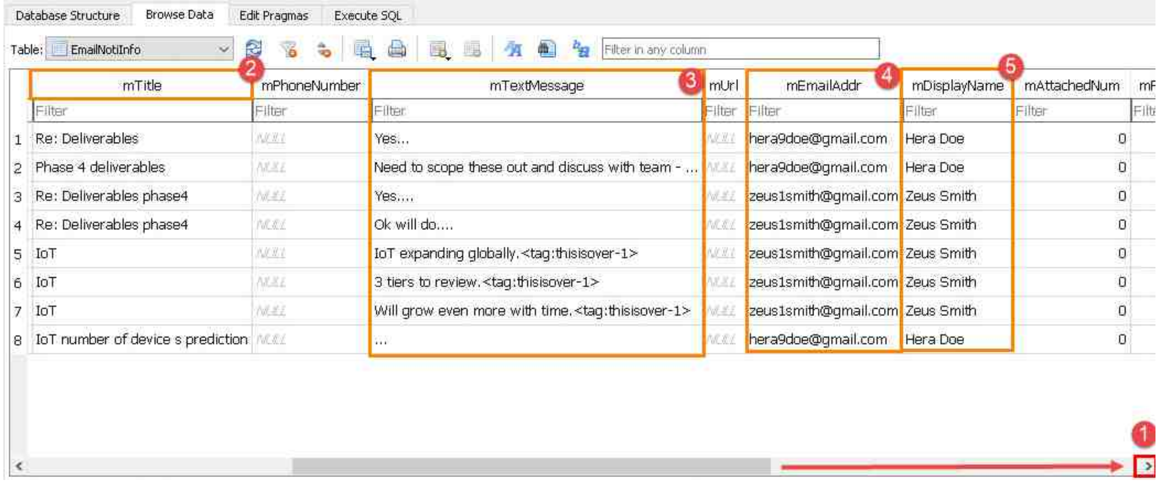


Choose a display format for the column 'mDateTime' which is applied to each value prior to showing it.

Unix epoch to date

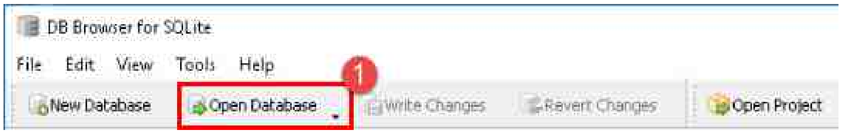
```
datetime("mDateTime", 'unixepoch')
```

42. Now that the dates are changed, let us look at some more data. Scroll to the right by clicking the horizontal arrow as seen in item 1 below or by using the scroll bar and stop at the column called mTitle, seen in item 2 below. As you can see, this column contains the messages' subject. Next is the mTextMessage column that contains the body of the message seen in item 3 below. The column called mEmailAddr contains the message sender's email address, and right beside it is the display name in the mDisplayName column seen in items 4 and 5 below.

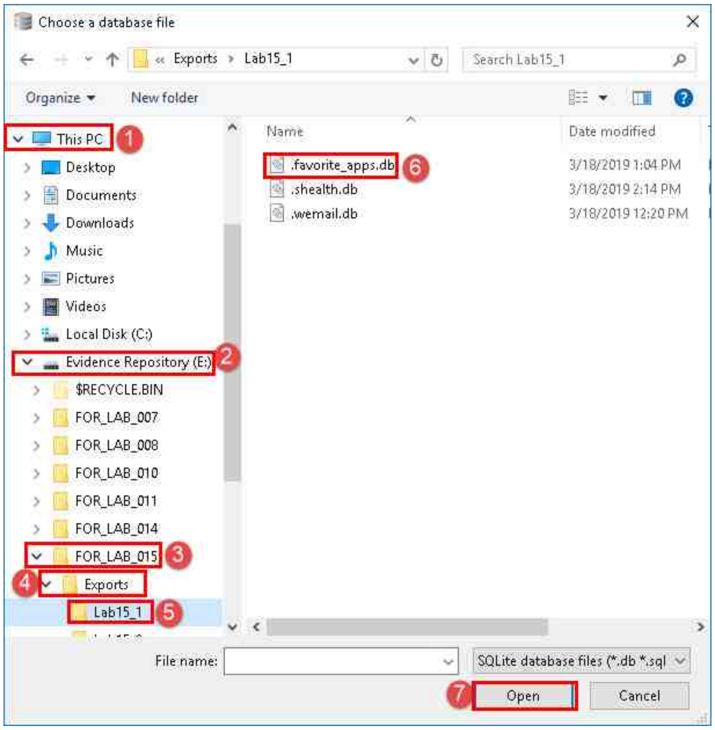


	mTitle	mPhoneNumber	mTextMessage	mUrl	mEmailAddr	mDisplayName	mAttachedNum	mF
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filte
1	Re: Deliverables	NULL	Yes...	NULL	hera9doe@gmail.com	Hera Doe	0	
2	Phase 4 deliverables	NULL	Need to scope these out and discuss with team - ...	NULL	hera9doe@gmail.com	Hera Doe	0	
3	Re: Deliverables phase4	NULL	Yes....	NULL	zeus1smith@gmail.com	Zeus Smith	0	
4	Re: Deliverables phase4	NULL	Ok will do....	NULL	zeus1smith@gmail.com	Zeus Smith	0	
5	IoT	NULL	IoT expanding globally.<tag:thisisover-1>	NULL	zeus1smith@gmail.com	Zeus Smith	0	
6	IoT	NULL	3 tiers to review.<tag:thisisover-1>	NULL	zeus1smith@gmail.com	Zeus Smith	0	
7	IoT	NULL	Will grow even more with time.<tag:thisisover-1>	NULL	zeus1smith@gmail.com	Zeus Smith	0	
8	IoT number of device s prediction	NULL	...	NULL	hera9doe@gmail.com	Hera Doe	0	

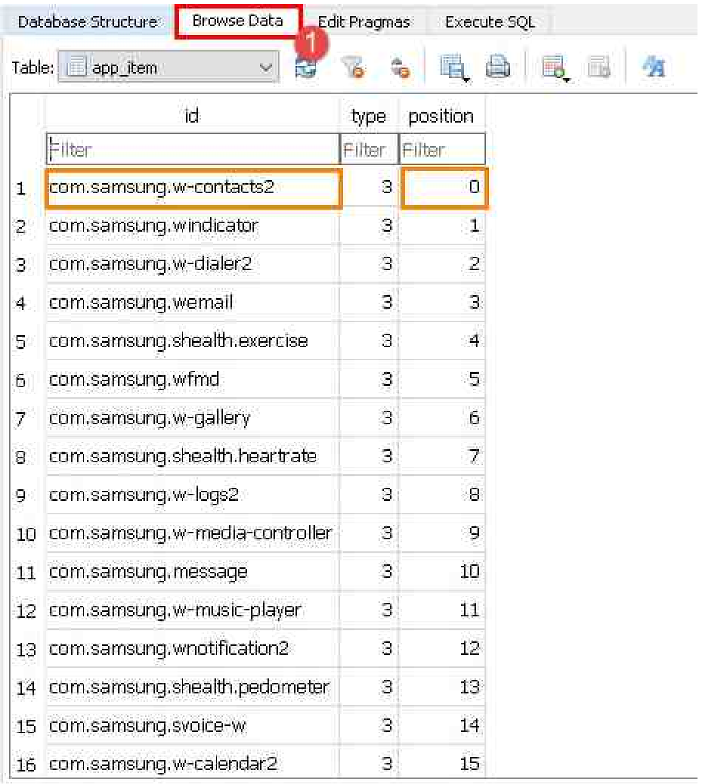
43. As you can see, this database is full of great information. Let us look at one last database file. The .favorite_apps.db file stores data about the most recently used applications. Open it by clicking the Open Database button seen in item 1 below. This will open the Choose a database file window.



44. In the Choose a database file window, navigate to ThisPC > Evidence Repository > FOR_LAB_015 > Exports > Lab15_1 as seen in items 1, 2, 3, 4, and 5 below. Once there, select the file called .favorite_apps.db by clicking it and then click Open as seen in item 6 below.



45. Now select the Browse Data tab as seen in item 1 below to switch to the table view. The table we will look at is the app_item table and is the first one you should see by default. This table provides a list of the apps on the device, and the position of the most recently used app is always 0.

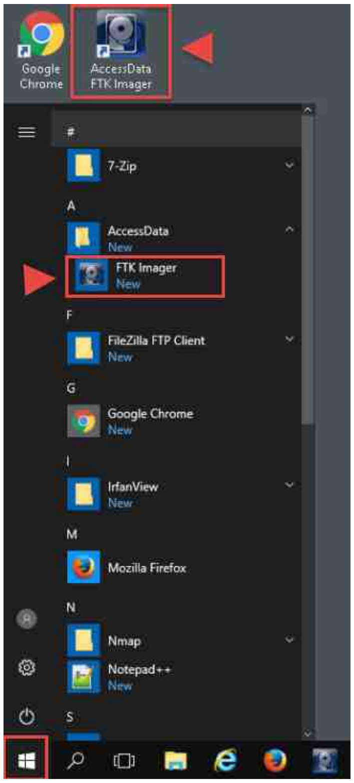


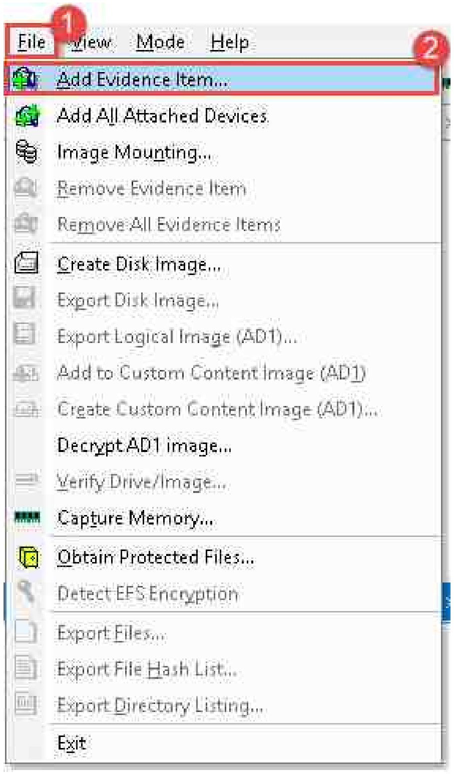
	id	type	position
	Filter	Filter	Filter
1	com.samsung.w-contacts2	3	0
2	com.samsung.windicator	3	1
3	com.samsung.w-dialer2	3	2
4	com.samsung.wemail	3	3
5	com.samsung.shealth.exercise	3	4
6	com.samsung.wfmd	3	5
7	com.samsung.w-gallery	3	6
8	com.samsung.shealth.heartrate	3	7
9	com.samsung.w-logs2	3	8
10	com.samsung.w-media-controller	3	9
11	com.samsung.message	3	10
12	com.samsung.w-music-player	3	11
13	com.samsung.wnotification2	3	12
14	com.samsung.shealth.pedometer	3	13
15	com.samsung.svoice-w	3	14
16	com.samsung.w-calendar2	3	15

46. You can tell from the type of data we have been finding that these devices contain very detailed and sensitive personal information. This data can be used in a variety of ways to tie a person to specific actions, a location, or a device. We will now look at the data within the Echo Dot device in the next exercise.

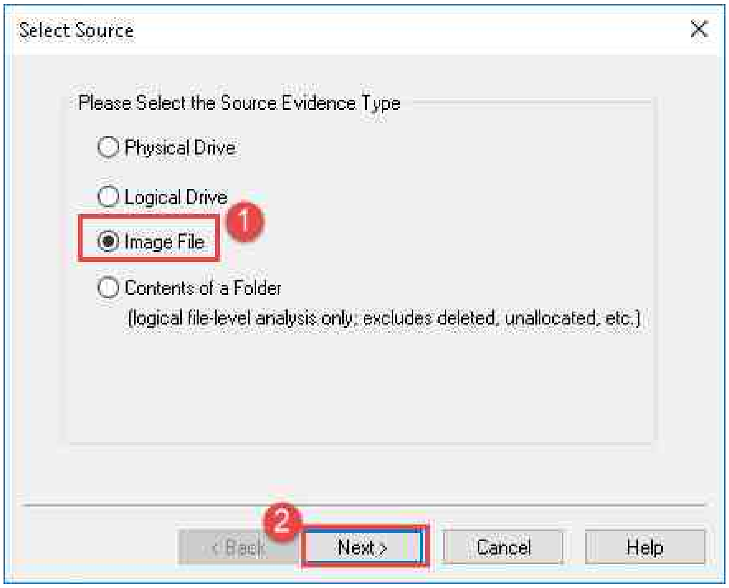
2 Identifying Files of Interest in an Echo Dot Device

1. Let us look at another IoT device. This time, we will look at the Amazon Echo Dot device. This is a smart home speaker that performs searches and controls other devices using voice commands. This device is very important in investigations because of the amount of information contained within them. Let us dig in and see what we find. FTK Imager should still be open; if not, reopen it and click the File menu option to open the File dropdown menu, then click the Add Evidence Item option from the dropdown menu. It is the first item on the menu, as highlighted below.





2. You will be brought to the Select Source window. Let us select Image File and click Next as highlighted at items 1 and 2 below.


Select Source

Please Select the Source Evidence Type

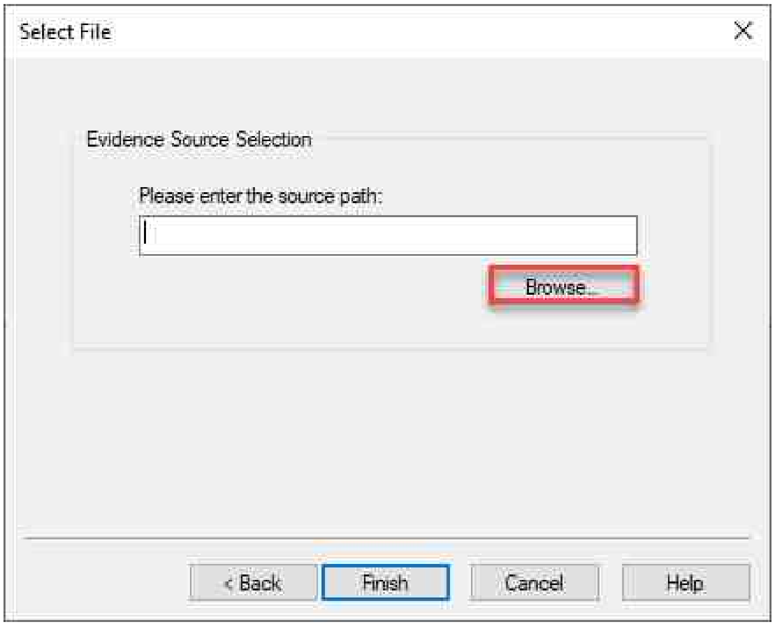
○ Physical Drive

○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

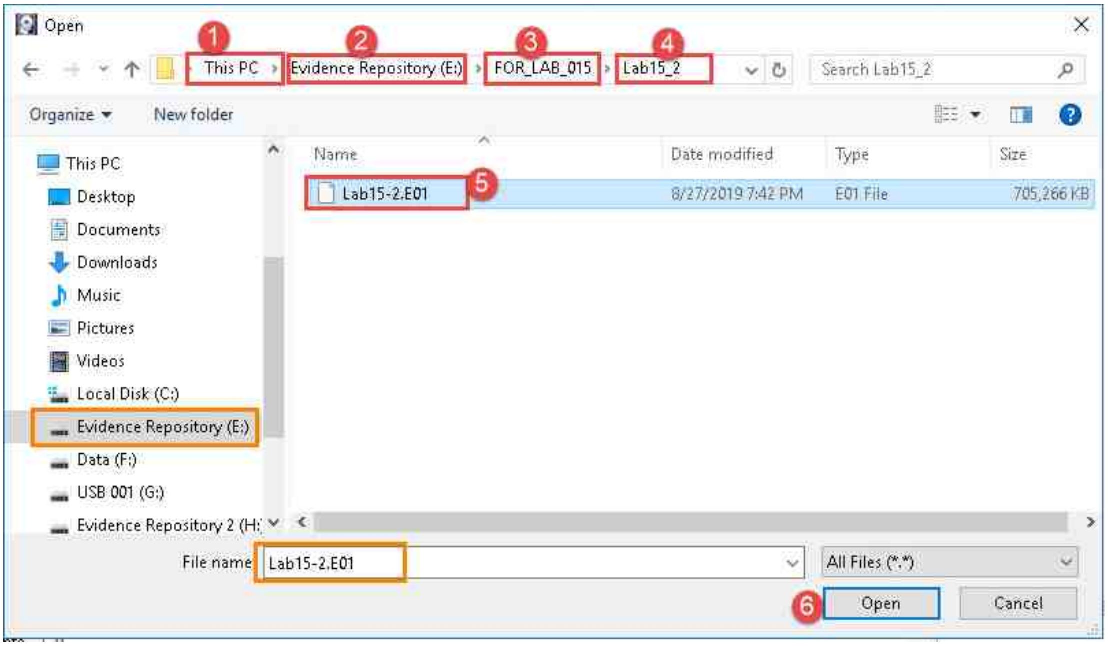
3. In the Select File window, click Browse highlighted in red in the screenshot below. This will open the Select File window, which will allow you to browse to the appropriate FEF.


Select File

Evidence Source Selection

Please enter the source path:

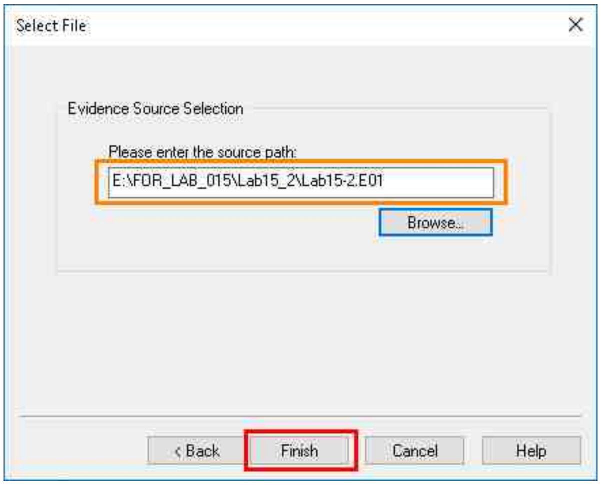
4. You are now at the Select File window. Browse to This PC > Evidence Repository (E:) > FOR_LAB_015 and double click the folder called Lab15_2. This will open the folder revealing the FEF called Lab15-1.img. Select the file called Lab15-2.E01 and click the Open button as highlighted in items 1 thru 6 below.



Name	Date modified	Type	Size
Lab15-2.E01	8/27/2019 7:42 PM	E01 File	705,266 KB

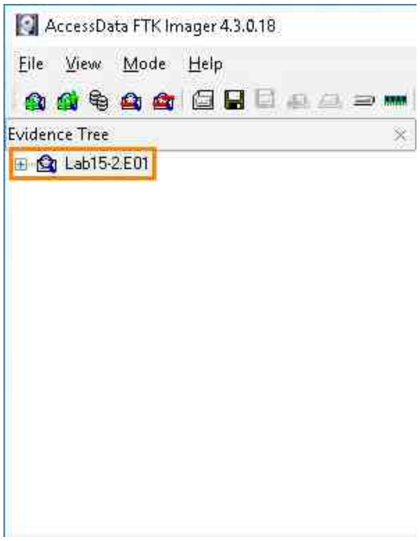
File name: Lab15-2.E01

5. Review the source path of the file called Lab15-2.E01. In the Select File window, click Finish highlighted in red in the screenshot below. This will take you back to FTK Imager's main window.

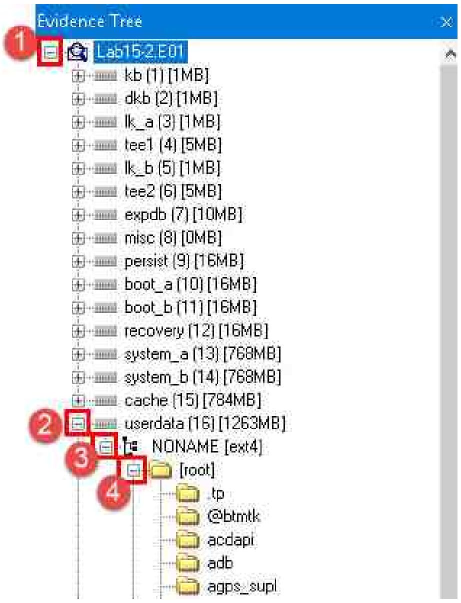


Please enter the source path: E:\FOR_LAB_015\Lab15_2\Lab15-2.E01

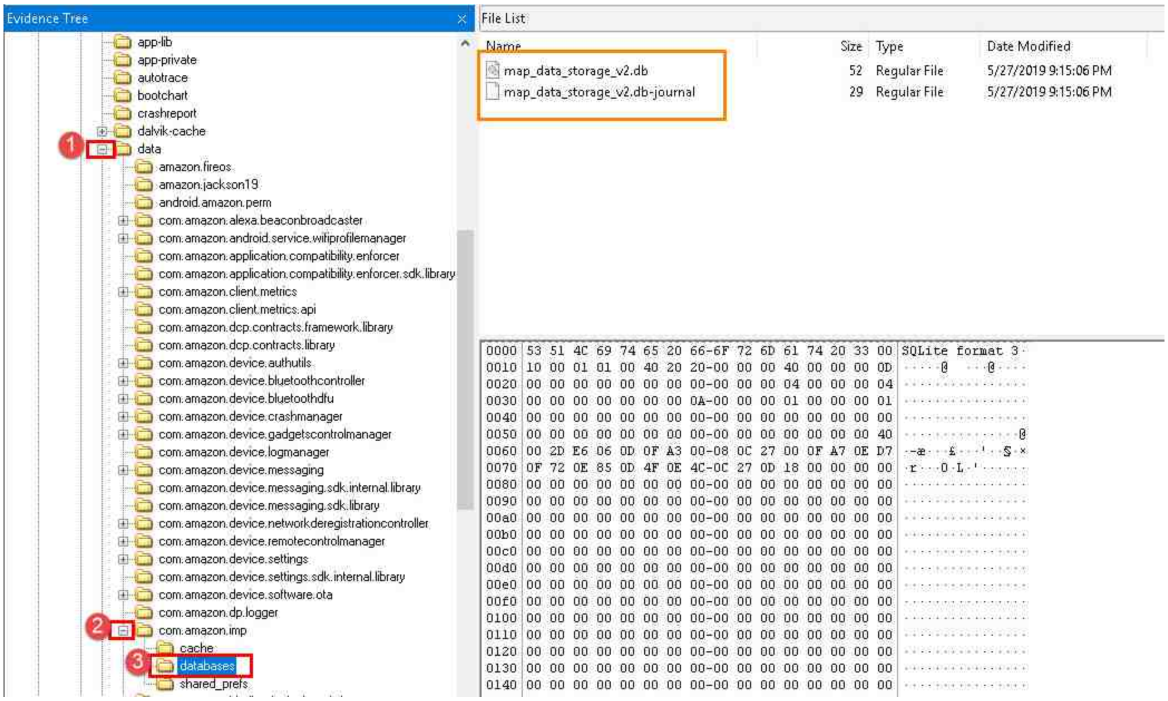
6. If you did everything correctly, you will now be back at FTK Imager's main window with Lab15-2.E01 listed under the Evidence Tree pane. From the Evidence Tree pane, click the tree item Lab15-2.E01 highlighted below. This will select the image you are going to peruse.



7. We will now browse the FEF and view its contents. To begin, click the + sign beside the FEF you added called Lab15-2.E01, as seen in item 1 below. This will expand the tree and display all logical partitions. Let us look at the one called userdata (16) [1263MB]. Click the + sign beside userdata (16) [1263MB] as seen in item 2 below. Next, let us expand the folder called NONAME [ext4] by clicking the + sign beside it, as seen in item 3 below. Like the watch we examined, this device also uses ext4 for some of its partitions. Finally, let us expand the folder called [root] by clicking the + sign beside it, as seen in item 4 below.



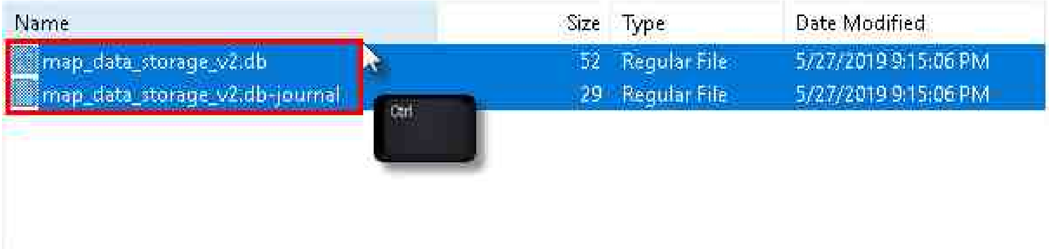
8. Now let us look for some information about the user. There are several files that store data about the user. We will look at the one called map_data_storage_v2.db. Navigate to this file by clicking the + signs beside the following folders data > com.amazon.imp > databases, as seen in items 1, 2, and 3 below.


Evidence Tree
app-lib
app-private
autotrace
bootchart
crashreport
dalvik-cache
1
data
amazon.fireos
amazon.jackson19
android.amazon.perm
com.amazon.alexa.beaconbroadcaster
com.amazon.android.service.wifiprofilemanager
com.amazon.application.compatibility.enforcer
com.amazon.application.compatibility.enforcer.sdk.library
com.amazon.client.metrics
com.amazon.client.metrics.api
com.amazon.dcp.contracts.framework.library
com.amazon.dcp.contracts.library
com.amazon.device.authutils
com.amazon.device.bluetoothcontroller
com.amazon.device.bluetoothdfu
com.amazon.device.crashmanager
com.amazon.device.gadgetscontrolmanager
com.amazon.device.logmanager
com.amazon.device.messaging
com.amazon.device.messaging.sdk.internal.library
com.amazon.device.messaging.sdk.library
com.amazon.device.networkderegistrationcontroller
com.amazon.device.remotecontrolmanager
com.amazon.device.settings
com.amazon.device.settings.sdk.internal.library
com.amazon.device.software.ota
com.amazon.dp.logger
2
com.amazon.imp
cache
3
databases
shared_prefs
File List

Name	Size	Type	Date Modified
map_data_storage_v2.db	52	Regular File	5/27/2019 9:15:06 PM
map_data_storage_v2.db-journal	29	Regular File	5/27/2019 9:15:06 PM

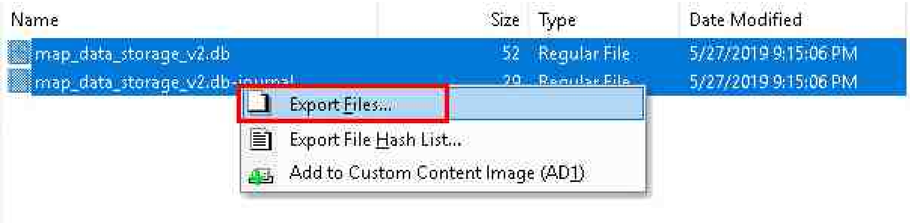
```
0000 53 51 4C 69 74 65 20 66-6F 72 6D 61 74 20 33 00 SQLite format 3·
0010 10 00 01 01 00 40 20 20-00 00 00 40 00 00 00 0D ·····@   ···@····
0020 00 00 00 00 00 00 00 00-00 00 00 04 00 00 00 04 ················
0030 00 00 00 00 00 00 00 0A-00 00 00 01 00 00 00 01 ················
0040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 40 ···············@
0060 00 2D E6 06 0D 0F A3 00-08 0C 27 00 0F A7 0E D7 ·-æ···£···'··§·×
0070 0F 72 0E 85 0D 4F 0E 4C-0C 27 0D 18 00 00 00 00 ·r···O·L·'······
0080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

9. We will be exporting the files called map_data_storage_v2.db and map_data_storage_v2.db-journal. Begin this process by highlighting both files. This can be done by holding the Ctrl key and clicking both files, as seen in item 1 below.



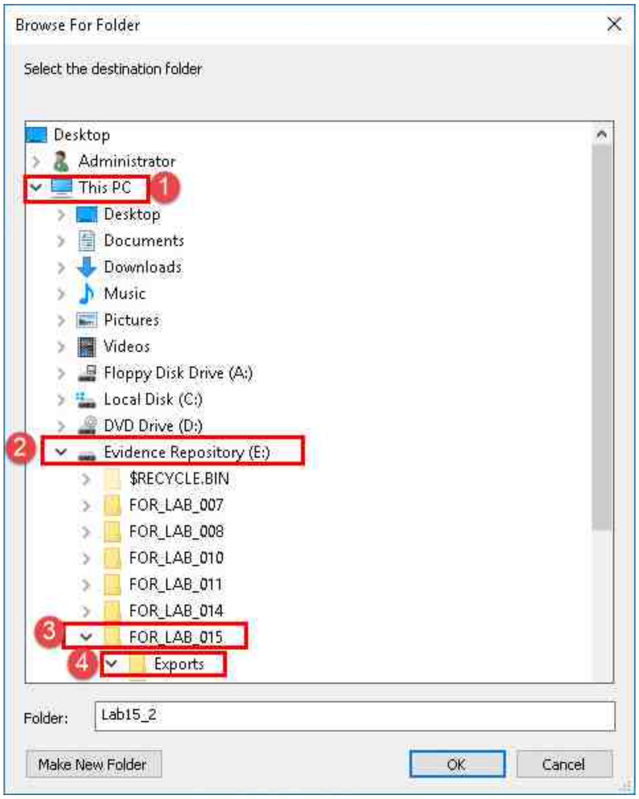
Name	Size	Type	Date Modified
map_data_storage_v2.db	52	Regular File	5/27/2019 9:15:06 PM
map_data_storage_v2.db-journal	29	Regular File	5/27/2019 9:15:06 PM

10. Now that the files are highlighted, right-click on the highlighted files, and click Export Files from the context menu that appears.



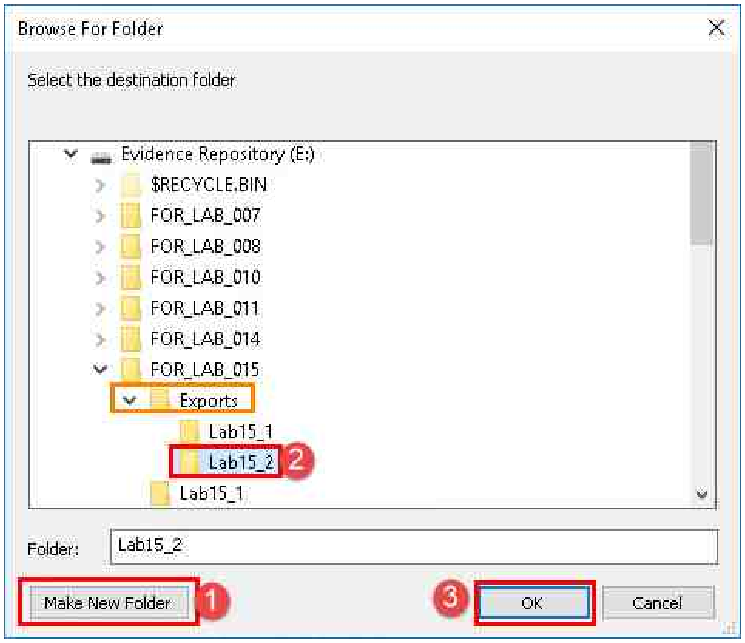
Name	Size	Type	Date Modified
map_data_storage_v2.db	52	Regular File	5/27/2019 9:15:06 PM
map_data_storage_v2.db-journal	29	Regular File	5/27/2019 9:15:06 PM

11. The Browse For Folder window will appear, allowing you to browse to the location where you want to put the files. Navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_015 > Exports as seen in items 1, 2, 3 and 4.

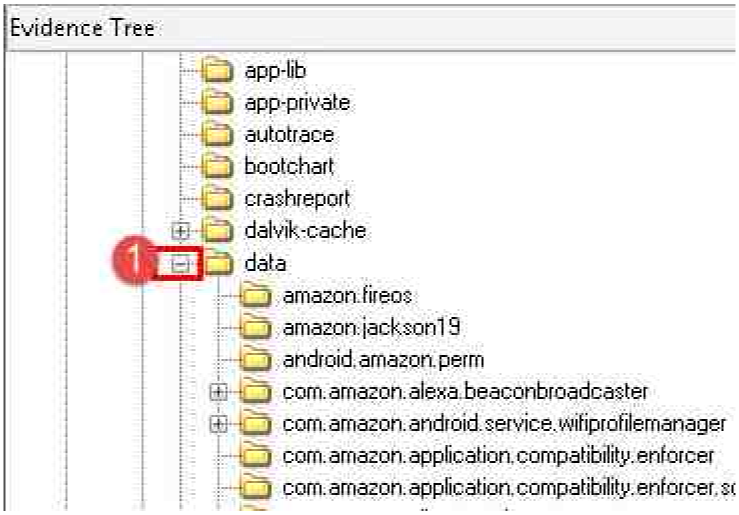


Folder: Lab15_2

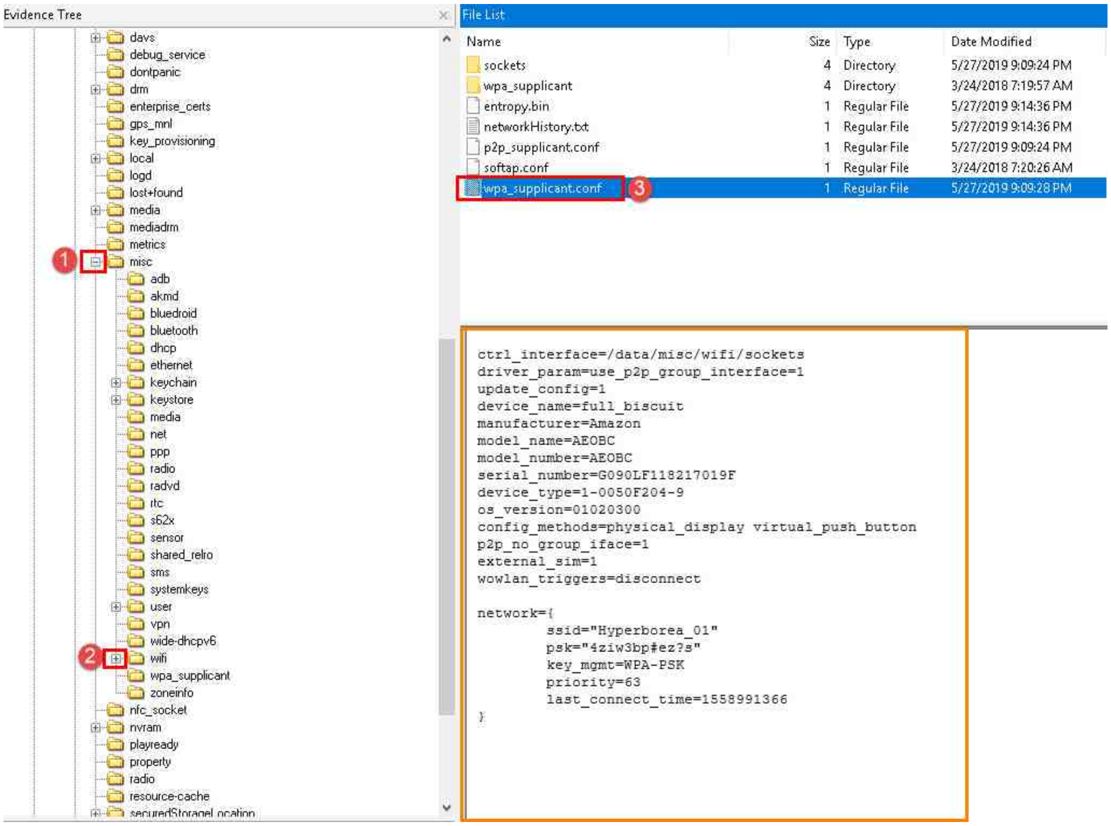
12. Now that you have the Exports folder selected. Click the Make New Folder button, as seen in item 1 below. This will create a new folder. Name this folder `Lab15_2` as seen in item 2 below. Finally, click OK, as seen in item 3 below.



13. Now that that file is exported, let us look at some other files. We will check out the WiFi settings. Begin by contracting the data folder by clicking the – sign beside the folder as seen in item 1 below.


Evidence Tree
app-lib
app-private
autotrace
bootchart
crashreport
dalvik-cache
1
data
amazon.fireos
amazon.jackson19
android.amazon.perm
com.amazon.alexa.beaconbroadcaster
com.amazon.android.service.wifiprofilemanager
com.amazon.application.compatibility.enforcer
com.amazon.application.compatibility.enforcer.sc

14. Now click the + sign beside the following folders misc > wifi as seen in items 1 and 2 below. Once there, click the file called wpa_supplicant.conf that appears in the File List pane, as seen in item 3 below.

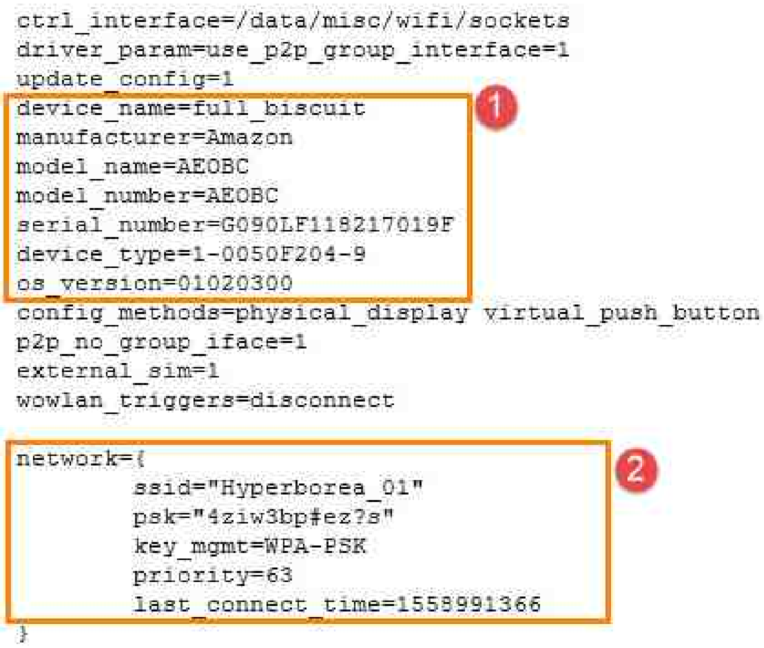


Name	Size	Type	Date Modified
sockets	4	Directory	5/27/2019 9:09:24 PM
wpa_supplicant	4	Directory	3/24/2018 7:19:57 AM
entropy.bin	1	Regular File	5/27/2019 9:14:36 PM
networkHistory.txt	1	Regular File	5/27/2019 9:14:36 PM
p2p_supplicant.conf	1	Regular File	5/27/2019 9:09:24 PM
softap.conf	1	Regular File	3/24/2018 7:20:26 AM
wpa_supplicant.conf	1	Regular File	5/27/2019 9:09:28 PM

```
ctrl_interface=/data/misc/wifi/sockets
driver_param=use_p2p_group_interface=1
update_config=1
device_name=full_biscuit
manufacturer=Amazon
model_name=AEOBC
model_number=AEOBC
serial_number=G090LF118217019F
device_type=1-0050F204-9
os_version=01020300
config_methods=physical_display virtual_push_button
p2p_no_group_iface=1
external_sim=1
wowlan_triggers=disconnect

network={
        ssid="Hyperborea_01"
        psk="4ziw3bp#ez?s"
        key_mgmt=WPA-PSK
        priority=63
        last_connect_time=1558991366
}
```

15. As you can see in the View pane, the contents of this file are stored in plain text and reveal a lot of data. As you can see in item 1 below, the device's codename is full_biscuit and the serial number, model number, and OS version are listed here. In item 2 it gets more interesting as we can see the SSID (name) of the last connected WiFi, the passphrase, the key strength, and the time that the last connection was made. The time is stored in Unix Time. The fact that this information is stored in plain text is convenient because many times users reuse passphrases for other services. The network name and passphrase can also be used to associate a user with a specific WiFi router. This means, if the router is a standard router that is stationary, then the user was within the proximity at the specific date and time of the last connection.

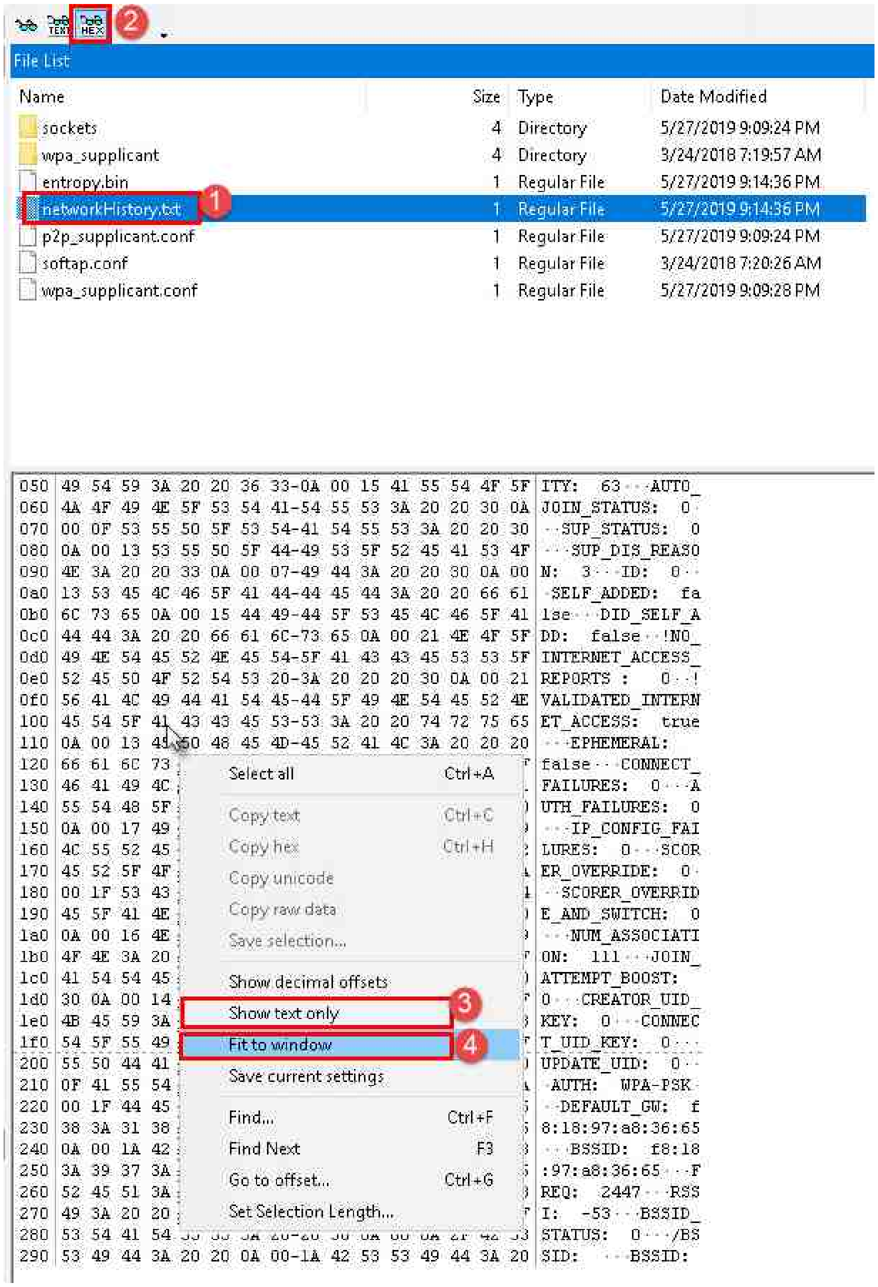


```
ctrl_interface=/data/misc/wifi/sockets
driver_param=use_p2p_group_interface=1
update_config=1
device_name=full_biscuit
manufacturer=Amazon
model_name=AEOBC
model_number=AEOBC
serial_number=G090LF118217019F
device_type=1-0050F204-9
os_version=01020300
config_methods=physical_display virtual_push_button
p2p_no_group_iface=1
external_sim=1
wowlan_triggers=disconnect

network={
        ssid="Hyperborea_01"
        psk="4ziw3bp#ez?s"
        key_mgmt=WPA-PSK
        priority=63
        last_connect_time=1558991366
}
```

Make a note of these details.

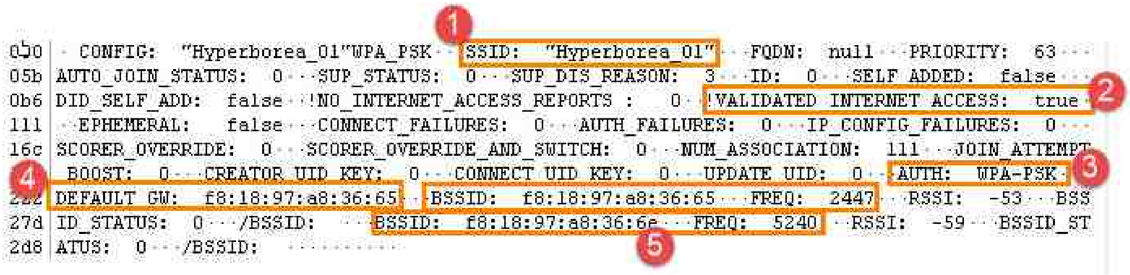
16. Let us look at another file that stores data about the WiFi history. This file is called networkHistory.txt and is in the same folder as the file we just examined called wpa_supplicant.conf. Access it by clicking networkHistory.txt in the File List pane, as seen in item 1 below. To view the contents of this file in FTK Imager, click the Hex view icon from the toolbar as seen in item 2 below. Next, right-click anywhere in the View Pane and select Show text only and Fit to window to make the data more manageable, as seen in items 3 and 4 below.



Name	Size	Type	Date Modified
sockets	4	Directory	5/27/2019 9:09:24 PM
wpa_supplicant	4	Directory	3/24/2018 7:19:57 AM
entropy.bin	1	Regular File	5/27/2019 9:14:36 PM
networkHistory.txt	1	Regular File	5/27/2019 9:14:36 PM
p2p_supplicant.conf	1	Regular File	5/27/2019 9:09:24 PM
softap.conf	1	Regular File	3/24/2018 7:20:26 AM
wpa_supplicant.conf	1	Regular File	5/27/2019 9:09:28 PM

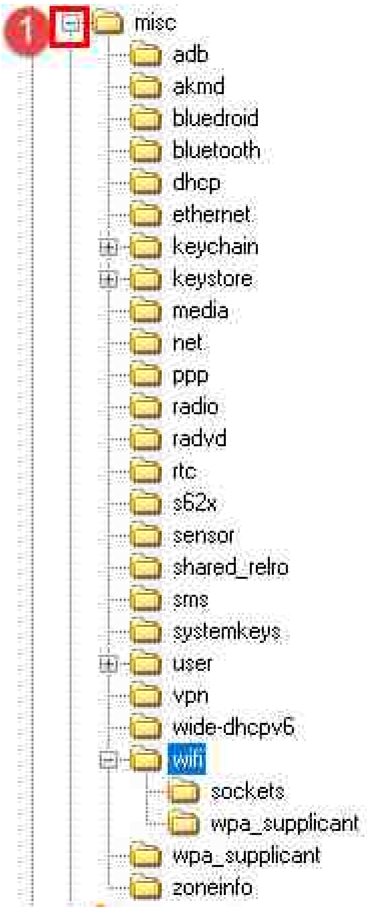
```
050  49 54 59 3A 20 20 36 33-0A 00 15 41 55 54 4F 5F  ITY:  63···AUTO_
060  4A 4F 49 4E 5F 53 54 41-54 55 53 3A 20 20 30 0A  JOIN_STATUS:  0·
070  00 0F 53 55 50 5F 53 54-41 54 55 53 3A 20 20 30  ··SUP_STATUS:  0
080  0A 00 13 53 55 50 5F 44-49 53 5F 52 45 41 53 4F  ···SUP_DIS_REASO
090  4E 3A 20 20 33 0A 00 07-49 44 3A 20 20 30 0A 00  N:  3···ID:  0··
0a0  13 53 45 4C 46 5F 41 44-44 45 44 3A 20 20 66 61  ·SELF_ADDED:  fa
0b0  6C 73 65 0A 00 15 44 49-44 5F 53 45 4C 46 5F 41  lse···DID_SELF_A
0c0  44 44 3A 20 20 66 61 6C-73 65 0A 00 21 4E 4F 5F  DD:  false··!NO_
0d0  49 4E 54 45 52 4E 45 54-5F 41 43 43 45 53 53 5F  INTERNET_ACCESS_
0e0  52 45 50 4F 52 54 53 20-3A 20 20 20 30 0A 00 21  REPORTS :   0··!
0f0  56 41 4C 49 44 41 54 45-44 5F 49 4E 54 45 52 4E  VALIDATED_INTERN
100  45 54 5F 41 43 43 45 53-53 3A 20 20 74 72 75 65  ET_ACCESS:  true
110  0A 00 13 45 50 48 45 4D-45 52 41 4C 3A 20 20 20  ···EPHEMERAL:
120  66 61 6C 73                                      false···CONNECT_
130  46 41 49 4C                                      FAILURES:  0···A
140  55 54 48 5F                                      UTH_FAILURES:  0
150  0A 00 17 49                                      ···IP_CONFIG_FAI
160  4C 55 52 45                                      LURES:  0···SCOR
170  45 52 5F 4F                                      ER_OVERRIDE:  0·
180  00 1F 53 43                                      ··SCORER_OVERRID
190  45 5F 41 4E                                      E_AND_SWITCH:  0
1a0  0A 00 16 4E                                      ···NUM_ASSOCIATI
1b0  4F 4E 3A 20                                      ON:  111···JOIN_
1c0  41 54 54 45                                      ATTEMPT_BOOST:
1d0  30 0A 00 14                                      0···CREATOR_UID_
1e0  4B 45 59 3A                                      KEY:  0···CONNEC
1f0  54 5F 55 49                                      T_UID_KEY:  0···
200  55 50 44 41                                      UPDATE_UID:  0··
210  0F 41 55 54                                      ·AUTH:  WPA-PSK·
220  00 1F 44 45                                      ··DEFAULT_GW:  f
230  38 3A 31 38                                      8:18:97:a8:36:65
240  0A 00 1A 42                                      ···BSSID:  f8:18
250  3A 39 37 3A                                      :97:a8:36:65···F
260  52 45 51 3A                                      REQ:  2447···RSS
270  49 3A 20 20                                      I:  -53···BSSID_
280  53 54 41 54                                      STATUS:  0···/BS
290  53 49 44 3A 20 20 0A 00-1A 42 53 53 49 44 3A 20  SID:  ···BSSID:
```

17. As you can see, the contents of this file reveal data about the network connections this device has made. The data highlighted in item 1 is the BSSID of the router, as we saw in the previous file. Next, in item 2 is Validated Internet Access entry. This tells you whether the device successfully connected to the internet through that access point. Next, let us look at the data highlighted in item 3. This is the authentication method and tells what security protocol the device uses. In item 4 is the MAC address of the default gateway. Finally, the data highlighted in item 5 are the MAC addresses of the 2.4Ghz and 5Ghz BSSIDs.

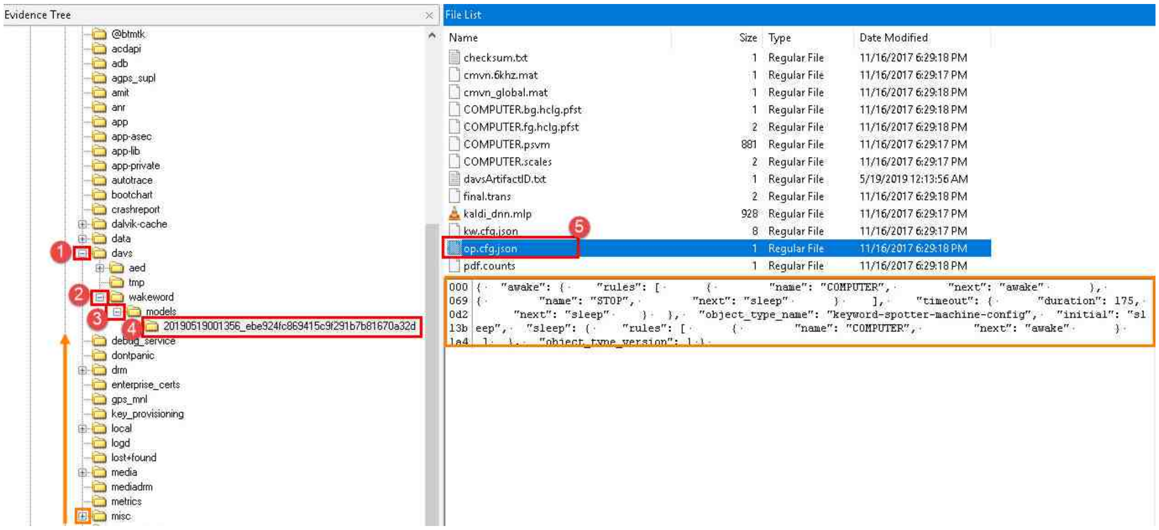


```
050   CONFIG:  "Hyperborea_01"WPA_PSK   SSID:  "Hyperborea_01"   FQDN:  null   PRIORITY:  63   
05b AUTO_JOIN_STATUS:  0   SUP_STATUS:  0   SUP_DIS_REASON:  3   ID:  0   SELF ADDED:  false   
0b6 DID_SELF_ADD:  false  !NO_INTERNET_ACCESS_REPORTS :   0  !VALIDATED INTERNET ACCESS:  true 
111   EPHEMERAL:   false   CONNECT_FAILURES:  0   AUTH_FAILURES:  0   IP_CONFIG_FAILURES:  0   
16c SCORER_OVERRIDE:  0   SCORER_OVERRIDE_AND_SWITCH:  0   NUM_ASSOCIATION:  111   JOIN_ATTEMPT
     BOOST:  0   CREATOR UID KEY:  0   CONNECT UID KEY:  0   UPDATE UID:  0   AUTH:  WPA-PSK 
222 DEFAULT GW:  f8:18:97:a8:36:65   BSSID:  f8:18:97:a8:36:65   FREQ:  2447   RSSI:  -53   BSS
27d ID_STATUS:  0   /BSSID:     BSSID:  f8:18:97:a8:36:6e   FREQ:  5240   RSSI:  -59   BSSID_ST
2d8 ATUS:  0   /BSSID:           
```

18. Let us look at another piece of information. This is the “wake word” and is the command that the device listens for to begin working. Let us navigate there by first contracting the folder called misc by clicking the – sign beside it, as seen in item 1 below.



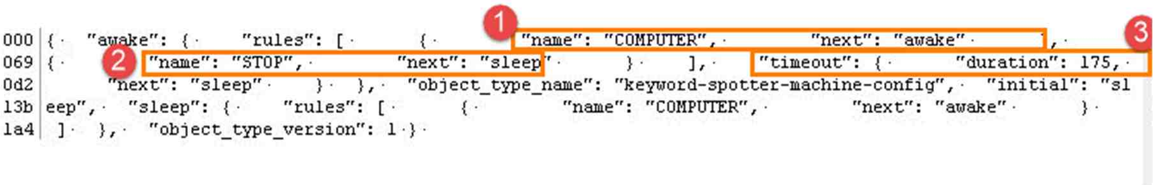
19. Now, navigate to the following folders by clicking the + sign beside them davs > wakeword > models > 20190519001356_ebe924fc869415c9f291b7b81670a32d as seen in items 1, 2, 3, and 4 below. Now click the file called op.cfg.json as seen in item 5 as seen below.



Name	Size	Type	Date Modified
checksum.txt	1	Regular File	11/16/2017 6:29:18 PM
cmvn.6khz.mat	1	Regular File	11/16/2017 6:29:17 PM
cmvn_global.mat	1	Regular File	11/16/2017 6:29:18 PM
COMPUTER.bg.hclg.pfst	1	Regular File	11/16/2017 6:29:18 PM
COMPUTER.fg.hclg.pfst	2	Regular File	11/16/2017 6:29:18 PM
COMPUTER.psvm	881	Regular File	11/16/2017 6:29:17 PM
COMPUTER.scales	2	Regular File	11/16/2017 6:29:17 PM
davsArtifactID.txt	1	Regular File	5/19/2019 12:13:56 AM
final.trans	2	Regular File	11/16/2017 6:29:18 PM
kaldi_dnn.mlp	928	Regular File	11/16/2017 6:29:17 PM
kw.cfg.json	8	Regular File	11/16/2017 6:29:17 PM
op.cfg.json	1	Regular File	11/16/2017 6:29:18 PM
pdf.counts	1	Regular File	11/16/2017 6:29:18 PM

```
000 { ·  "awake": { ·    "rules": [ ·       { ·         "name": "COMPUTER", ·        "next": "awake" ·      }, ·
069 { ·          "name": "STOP", ·          "next": "sleep" ·      } ·    ], ·    "timeout": { ·       "duration": 175, ·
0d2        "next": "sleep" ·    } ·  }, ·  "object_type_name": "keyword-spotter-machine-config", ·  "initial": "sl
13b eep", ·  "sleep": { ·    "rules": [ ·       { ·         "name": "COMPUTER", ·         "next": "awake" ·      } ·
1a4  ] ·  }, ·  "object_type_version": 1 · } ·
```

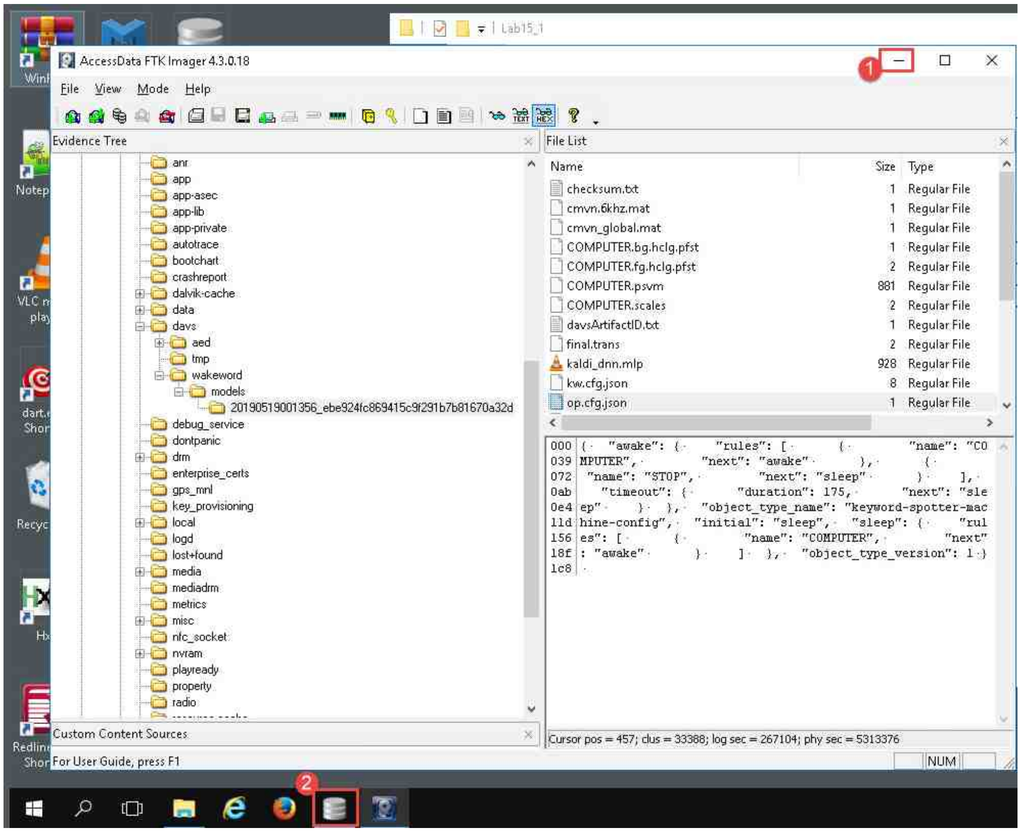
20. Now, look at the data that populates the View Pane. As you can see in item 1 below, the wake word for the device is COMPUTER. This means the user would need to say the word computer for the device to respond. The data highlighted in item 2 is the word STOP, and that puts the device to sleep. Highlighted in item 3 is the length of time in minutes that the device will sleep after receiving the voice command.



```
000 { ·  "awake": { ·    "rules": [ ·       { ·       "name": "COMPUTER", ·          "next": "awake" ·      ], ·
069 { ·      "name": "STOP", ·          "next": "sleep" ·         } ·    ], ·   "timeout": { ·      "duration": 175, ·
0d2          "next": "sleep" ·      } ·  }, ·  "object_type_name": "keyword-spotter-machine-config", ·  "initial": "sl
13b eep", ·  "sleep": { ·    "rules": [ ·       { ·         "name": "COMPUTER", ·         "next": "awake" ·      } ·
1a4  ] ·  }, ·  "object_type_version": 1 · } ·
```

21. This data can help to attribute a user to the device by testing their knowledge of its voice commands.

22. Now let us look at the database that we exported. This is the database file called map_data_storage_v2.db. Let us begin by minimizing FTK Imager and reopening DB Browser (SQLite).

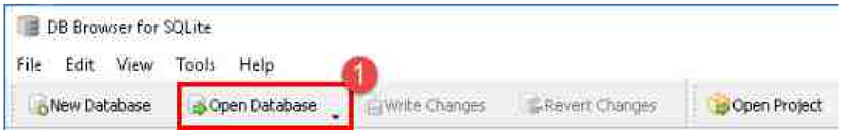


Name	Size	Type
checksum.txt	1	Regular File
cmvn.6khz.mat	1	Regular File
cmvn_global.mat	1	Regular File
COMPUTER.bg.hclg.pfst	1	Regular File
COMPUTER.fg.hclg.pfst	2	Regular File
COMPUTER.psvm	881	Regular File
COMPUTER.scales	2	Regular File
davsArtifactID.txt	1	Regular File
final.trans	2	Regular File
kaldi_dnn.mlp	928	Regular File
kw.cfg.json	8	Regular File
op.cfg.json	1	Regular File

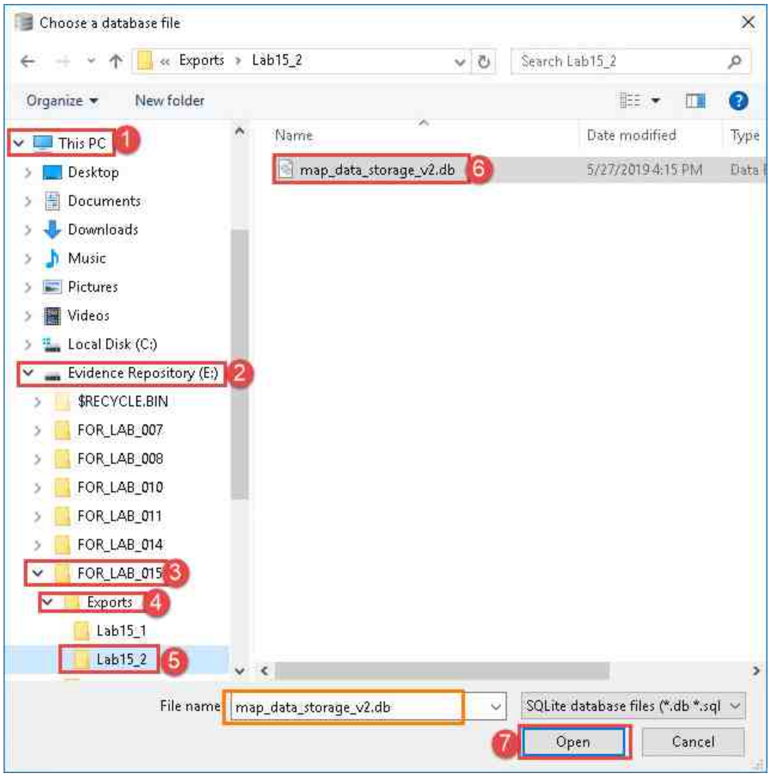
```
000 {·  "awake": {·    "rules": [·      {·         "name": "CO
039 MPUTER",·         "next": "awake"·       },·      {·
072  "name": "STOP",·         "next": "sleep"·      }·    ],·
0ab    "timeout": {·      "duration": 175,·      "next": "sle
0e4 ep"·    }·  },·  "object_type_name": "keyword-spotter-mac
11d hine-config",·  "initial": "sleep",·  "sleep": {·    "rul
156 es": [·      {·         "name": "COMPUTER",·         "next"
18f : "awake"·       }·    ]·  },·  "object_type_version": 1·}
1c8 ·
```

Cursor pos = 457; clus = 33388; log sec = 267104; phy sec = 5313376

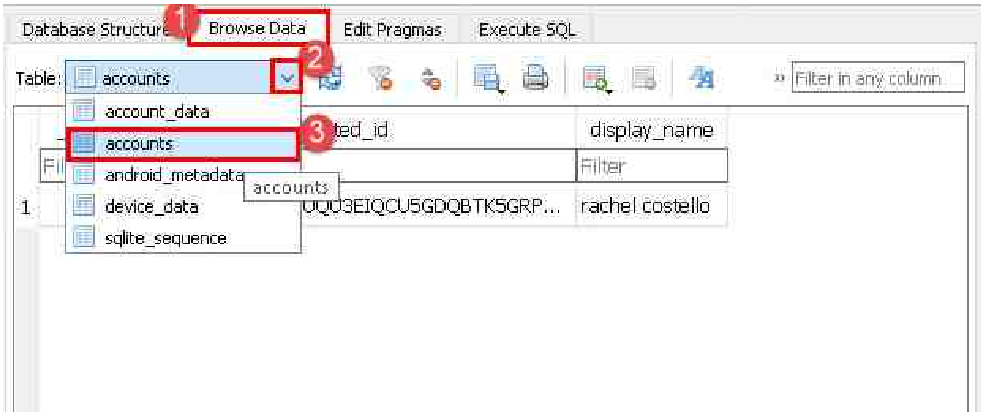
23. Once the DB Browser (SQLite) GUI appears, click the Open Database button seen in item 1 below. This will open the Choose a database file window.



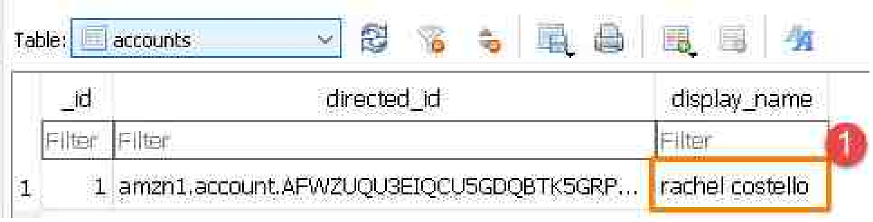
24. In the Choose a database file window, navigate to ThisPC > Evidence Repository > FOR_LAB_015 > Exports > Lab15_2 as seen in items 1, 2, 3, 4 and 5 below. Once there, select the file called map_data_storage_v2.db by clicking it and then click Open as seen in items 6 and 7 below.



25. Now select the Browse Data tab as seen in item 1 below. The table that you will see is the account_data table. It contains a list of different types of data, but we will not be reviewing this data in this lab; instead, let us switch to the accounts table by clicking it from the Table dropdown menu as seen in items 2 and 3 below.

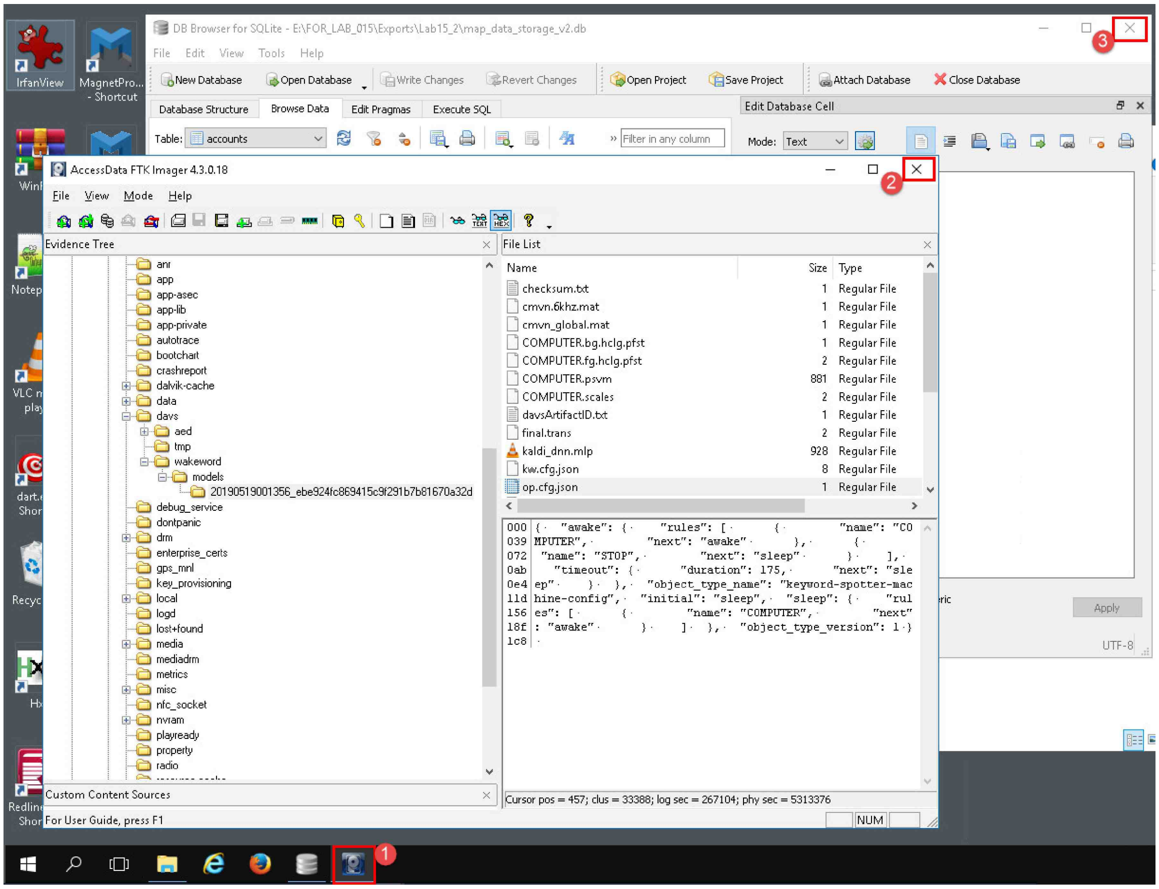


26. In this table, you will see a list of the users that are associated with this device. As you can see in the screenshot, there is only one account listed here. The name that the user entered is listed under the display_name column in item 1 below; assume that name is the amazon account ID that is used to connect to Amazon's servers. This information is very sensitive and can be used to tie this device with data found on the cloud sources associated with this account. Examining the cloud source will be done in a more advanced class, however.



	_id	directed_id	display_name
	Filter	Filter	Filter
1	1	amzn1.account.AFWZUQU3EIQCU5GDQBTK5GRP...	rachel costello

27. We are now at the end of this lab. Feel free to examine the image using FTK Imager or another tool to see if you can find more information about the device and its activities. Once you are done, close all the programs you used by clicking the X at the top-right corner of each window.



Name	Size	Type
checksum.txt	1	Regular File
cmvn.6khz.mat	1	Regular File
cmvn_global.mat	1	Regular File
COMPUTER.bg.hclg.pfst	1	Regular File
COMPUTER.fg.hclg.pfst	2	Regular File
COMPUTER.psvm	881	Regular File
COMPUTER.scales	2	Regular File
davsArtifactID.txt	1	Regular File
final.trans	2	Regular File
kaldi_dnn.mlp	928	Regular File
kw.cfg.json	8	Regular File
op.cfg.json	1	Regular File

```
000 {·  "awake": {·    "rules": [·      {·        "name": "CO
039 MPUTER",·         "next": "awake"·       },·      {·
072  "name": "STOP",·         "next": "sleep"·      }·    ],·
0ab    "timeout": {·      "duration": 175,·      "next": "sle
0e4 ep"·    }·  },·  "object_type_name": "keyword-spotter-mac
11d hine-config",·  "initial": "sleep",·  "sleep": {·    "rul
156 es": [·      {·        "name": "COMPUTER",·        "next"
18f : "awake"·      }·    ]·  },·  "object_type_version": 1·}
1c8 ·
```

Cursor pos = 457; clus = 33388; log sec = 267104; phy sec = 5313376