IoT Forensics

For this lab we are looking into IoT devices and how to use them for investigations. IoT devices have a lot of data that can provide insight and answer important questions to the investigation.

We start with loading the FTK Imager from the desktop and choosing file, add evidence item then select image file, next, and browse. We go to the evidence repository and inside the lab 15 folder choosing the lab15-1.img inside and clicking open and finish. Then we expand the lab15-1.img, then NONAME, root, media, and click on images then photos before closing media. We expand apps, com.samsung.shealth, click data and highlight .shealth.db and .shealth.db-journal right clicking then hitting export files. Going through the evidence repository we open the for lab 15 folder and create a new folder called Exports where we make another folder called lab15\_1 and hit ok. Now we expand, com.samsung.wemail, data and open dbspace exporting the two files found there, .wemail.db and .wemail.db-journal into the same folder from last time. The process repeats with com.samsung.w-launcher-app > data, exporting .favorite\_apps.db and its journal to the folder. Now we minimize FTK Imager and open DB Browser(SQLite) on the desktop and click open database selecting .shealth.db and open. Click the browse data and select shealth\_profile, once inside right click on birthday and click edit display format, choosing Java epoch (milliseconds) to date from the menu and click ok, repeat this with the timestamp column. At table, click on shealth\_pedometer\_history in the drop down menu, repeat with shealth\_heartrate\_log. Hit open database and go back to the previously used folder choosing .wemail.db and hit open then browse data. Change table to EmailNotiInfo then hit view and remove items three and four from the view. Right click the column header mDateTime and click edit display format, select Unix epoch to date and hit ok. Now we go back to open database and follow the path back to the lab15\_1 and select .favorite\_apps.db and click open then browse data. Then we go back to FTK Imager and click file, add evidence item, image file, next, browse, and go to for lab 15, lab 15\_2 and select the Lab15-2.E01 and hit open then finish. In the evidence tree we expand our new file, then userdata, NONAME, root, data, com.amazon.imp, and click databases selecting the map\_data\_storage\_v2.db file and its journal and hiting right click, export files, where we go back to exports and make a new folder, lab15\_2 and hit ok. Closing data, we expand misc and hit wifi clicking the file wpa\_supplicant.conf, then we click networkHistory.txt, hex view, show text only, fit to window, and then minimize the misc folder. Now we follow the path, davs > wakeword > models > 20190519001356\_ebe924fc869415c9f291b7b81670a32d and click the file op.cfg.json. Then we move back to the DB Browser(SQLite), open database, go to lab15\_2 in exports and select map\_data\_storage\_v2.db and hit open.

The lab was quite informative of how to handle databases as we had yet to look at them. There was a lot of repeating steps to make sure we got all of the files we needed. Overall, it was an interesting lab to work through.

Section 1 Step 44 output

A screenshot of a computer

Description automatically generated

Section 2 Step 24 output

A screenshot of a computer

Description automatically generated

Mobile Forensic Analysis

This lab is to help us understand how to get digital evidence through a smartphone. These days phones hold a large amount of information about our lives so they are great for an investigation.

We start by opening autopsy 4.13 from the taskbar and selecting new case giving the name FOR\_LAB\_016, hit next then enter examiner information and the number as NDG016 and hit finish. On add data source we click disk image or vm file, next, browse, and follow the path, Home > csi > Desktop > Evidence Files > FOR\_LAB\_016 selecting the file Lab16.001 and click open, next, deselect all, exif parser and android analyzer, next, then finish. Expand data sources, lab10.001, vol15, data, com.android.providers.settings, and click on databases then the file settings.db, application, and choosing system then secure in table. Minimize the com.android.providers.settings folder and expand com.google.android.gms and open shared\_prefs clicking the file checkin.xml and the text tab. Then we expand the folder com.google.android.gm, click databases, [mailstore.cfttmobile1@gmail.com.db](mailto:mailstore.cfttmobile1@gmail.com.db), and application, selecting messages in table. Right click on dateSentMs and dateReceivedMs column headers and choose display as, date then move on to the table attachments. Moving on we expand com.google.android.apps.maps, databases, and click the file da\_destination\_history, and in table application and destination\_history. Time column header can be changed to date as previously done. Now we move on to expand misc, click wifi, wpa\_supplicant.conf, text tab. The next set is expanding system, clicking file SimCard.dat then text tab. Now we can minimize the data sources tab and expand results, extracted content, and click call logs, then installed programs, then messages.

This lab gave something to think about as our phones have so much information on them that can be found through these methods. The lab let us see the calls, settings, and messages which can hold a lot of information. This was a fun lab overall and I quite enjoyed it.

Section 1 Step 37

A screenshot of a computer

Description automatically generated

Section 2 Step 6

A screenshot of a computer

Description automatically generated