Open Source (Academic Usage)

Mobile Device Security & Forensics

Year 3 (2021/22), Semester 5

SCHOOL OF INFOCOMM TECHNOLOGY

Diploma in Information Security & Digital Forensics

ASSIGNMENT WRITEUP

Android Forensics for Drug Dealing Activities

By Team da-droid

Ryan Ng (Leader)

Ezra Ho

Hannah Leong

Team_dadroid_2021_NP_CSF

Open Source (Academic Usage)

Disclaimer

While this work has been made openly available and open source, the author and his teammates **DO NOT** condone plagiarism in any form. Any attempt to cite or reference material used contained herein should be made clearly as published. By viewing this document, you consent to all the rules as spelt out above.

We would like to thank Belkasoft and its partners for making available material that we could use as “evidence” to base our case on, as well as external resources used, together with the teaching faculty at Ngee Ann Polytechnic for ideas to go about conducting the forensic investigation.

RyanNgCT Inc.
SECURING WITH AI

Dated 11 November 2021

Ng Chin Tiong Ryan

Open Source (Academic Usage)

Table Of Contents

RyanNgCT Inc. SECURING WITH AI

ORIGINAL
Open Source (Academic Usage)

1. Introduction of Assignment (Fictitious Case)

A man was detained on the street because he looked suspicious, walking around late at night with a backpack in the middle of a suburban area. The police found traces of drugs on his seemingly empty backpack. The man had an Android phone with him, which was later imaged in a digital forensics lab.

Now, you and your group of forensic examiners from the National Crime Agency, UK are tasked with identifying if the person has any connections to the local drug ring they have been tracking for over three years. Your colleague has performed a logical acquisition of the image and handed your team a copy of it. You are to use widely available open-source Android Forensic Tools for this investigation.

2. Description of work

In this project, we plan to use available open-source mobile forensic tools to simulate conducting a real-life case of a forensic investigation with regards to the mobile phone on the Android platform. The suspect and his accomplice have been suspected to be involved with drug dealing and money laundering. We plan to examine photos, messages and web history to determine if that is the case.

3. Resources (hardware and software)

RyanNgCT Inc.
SECURING WITH AI

Windows or Linux-based Virtual Machine is recommended, performing forensic examination on the host machine is also possible, but VM gives the ease of cleanup.

Recommended Minimum Hardware: 3GB RAM and 60GB free hard disk space

Tools used:

- **Android Logs Events And Protobuf Parser (aLEAPP)** to create reports on various common artifacts found in the evidence image.
- **Andriller** for unzipping and parsing of .tar image
- **Whatsapp Viewer** for decoding and viewing whatsapp message db
- **Autopsy - with Android Module** for in-depth analysis of the phone content
- **SQLite Spy** for parsing databases and sqlite file formats

Open Source (Academic Usage)

Dependencies Needed:

- Python3 added to path (use pip install functionality for dependencies) -- more specific to examination on Windows
- Various dependencies on the github pages of the tools
- 7zip (optional)

Evidence Source:

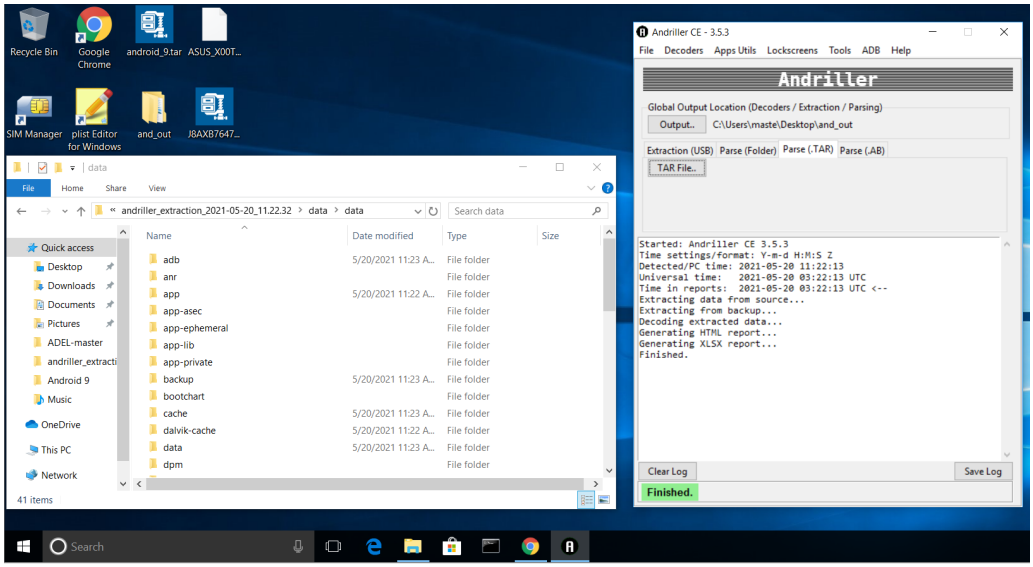
- https://belkasoft.com/ctf/ : Android Image from BelkaSoft CTF in May 2020

RyanNgCT Inc.
SECURING WITH AI

Open Source (Academic Usage)

4. Set-up and Functionality of Tools

a) Extraction using Andriller



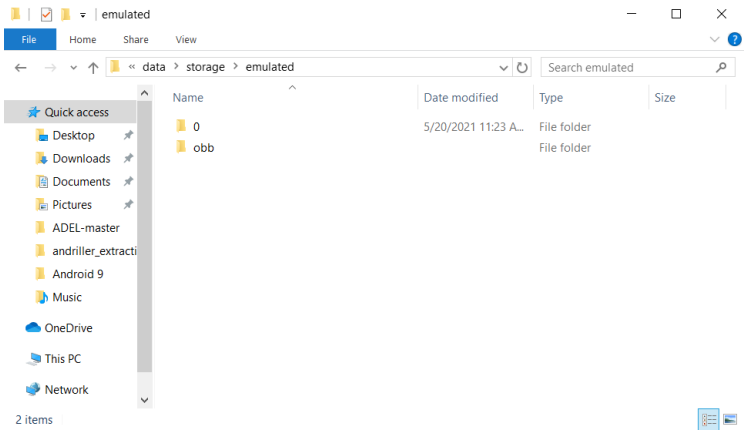
First, download the evidence from the link mentioned above and then extract it using 7-zip on the vm. Now we have the compressed .tar file. We can then proceed to use Andriller to extract it. Create 2 empty directories, one for the output of andriller and another for aleapp later on.

RyanNgCT Inc.
SECURING WITH AI

Open andriller and select an output file and using the Parse (TAR) tab, select **J8AXB7647798GRJ-20210421_0920.tar** (not the ASUS belkasoft image) on the Desktop and the tool will automatically start processing and generate another file with outputs and reports.

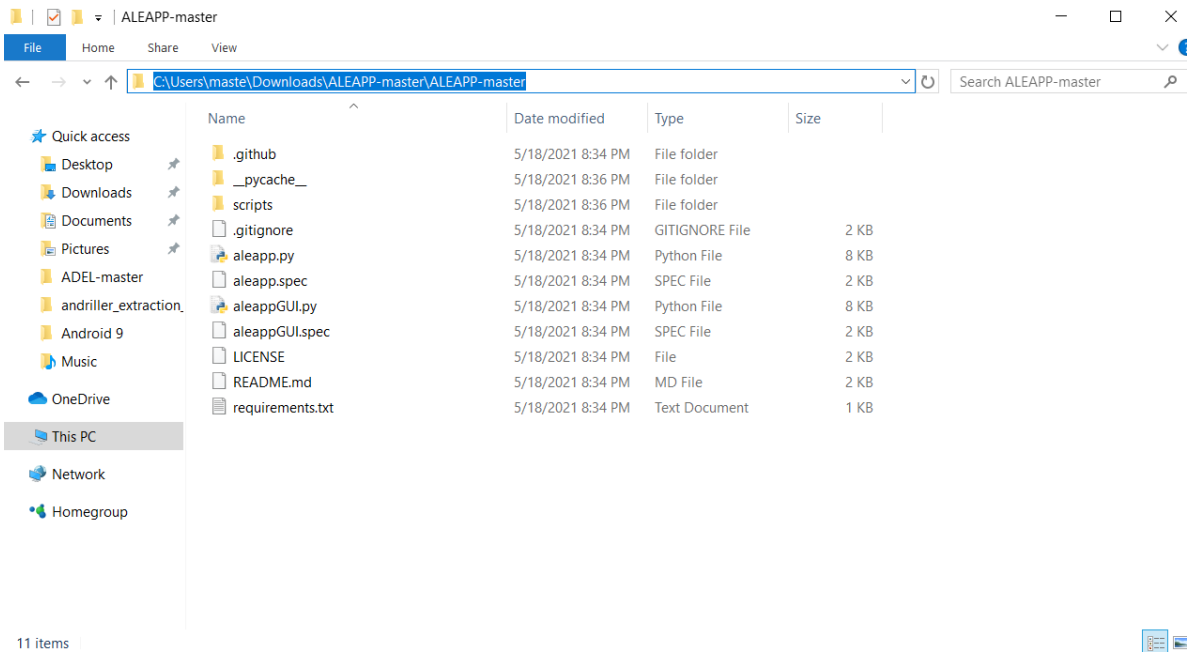
Once complete, navigate to <output_directory>\andriller_extraction_<date_timestamp>\data\data to verify the following folders have been created as in the extracted image.

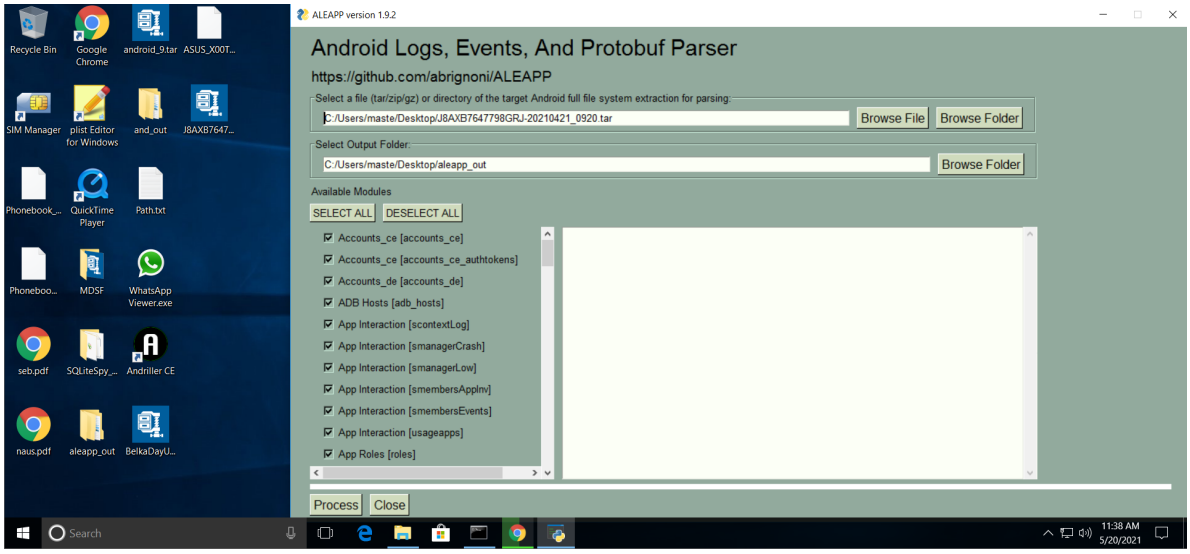
We also can see that some artifacts reside in andriller_extraction_<date_timestamp>\data\storage\emulated as shown below.



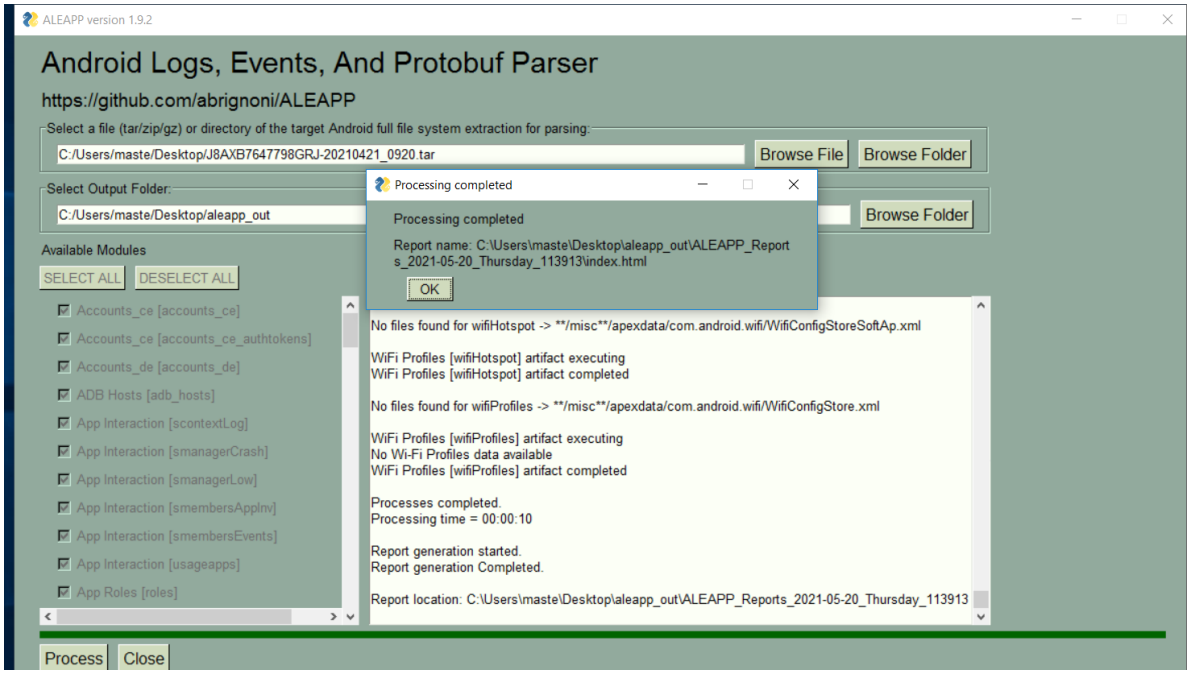
b) *Reporting using aLEAPP*

For Windows, navigate to the directory where aLEAPP was installed and copy the path. Open up a command prompt and navigate there, following which we will launch a GUI instance. (For linux, since the tool should be automatically added to $PATH upon installation and setting up dependencies, we can just launch the GUI from the current working directory)

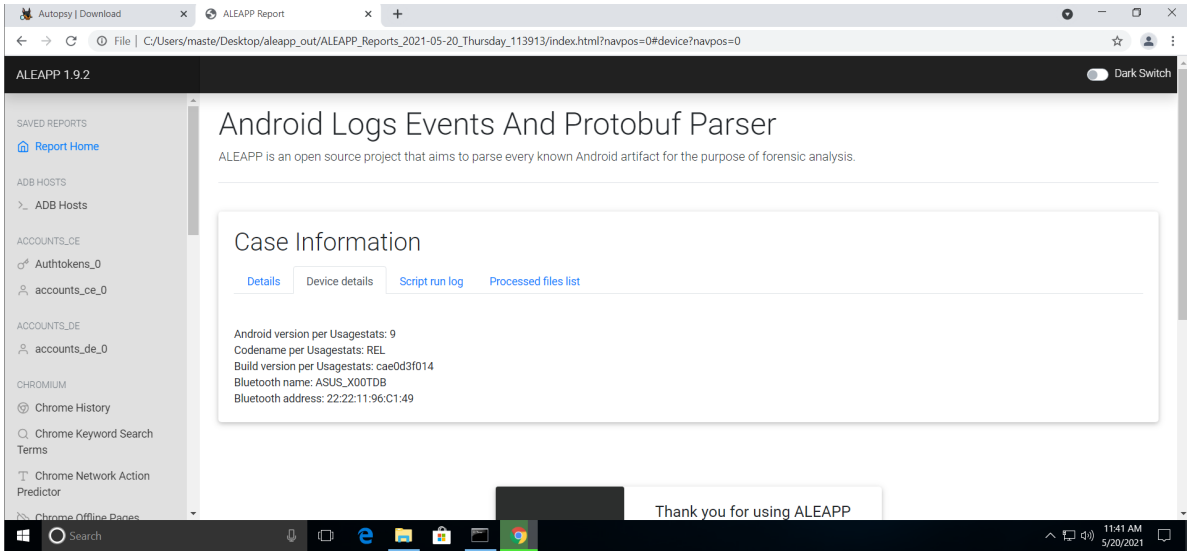


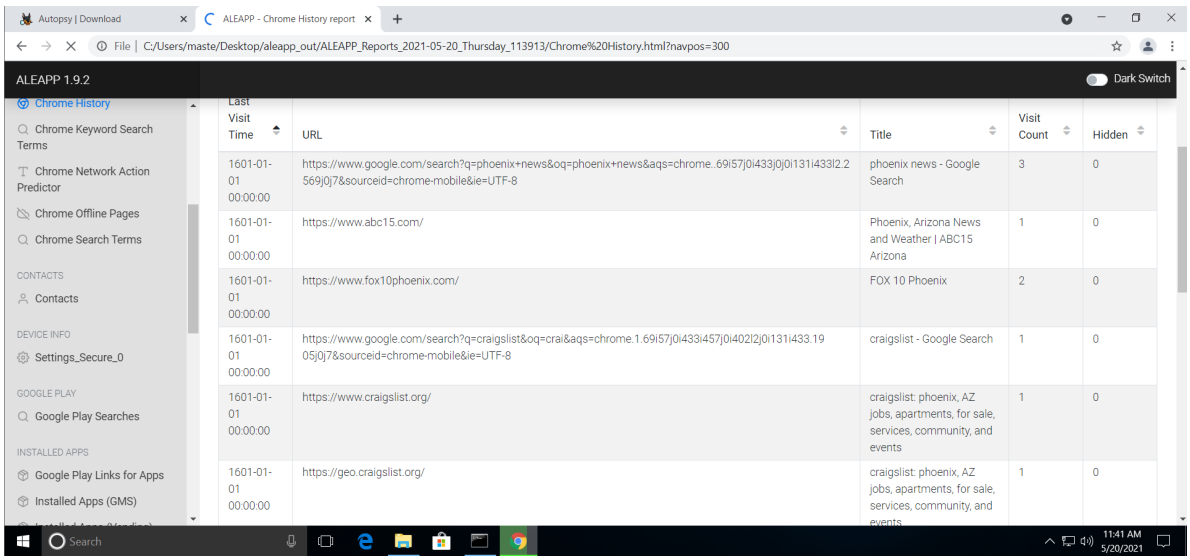


Navigate to and select the tar file for processing (leave the default--all options selected), select the corresponding output folder and hit Process. ALEAPP will use the relevant modules to extract the information that it is built to parse if they are present.

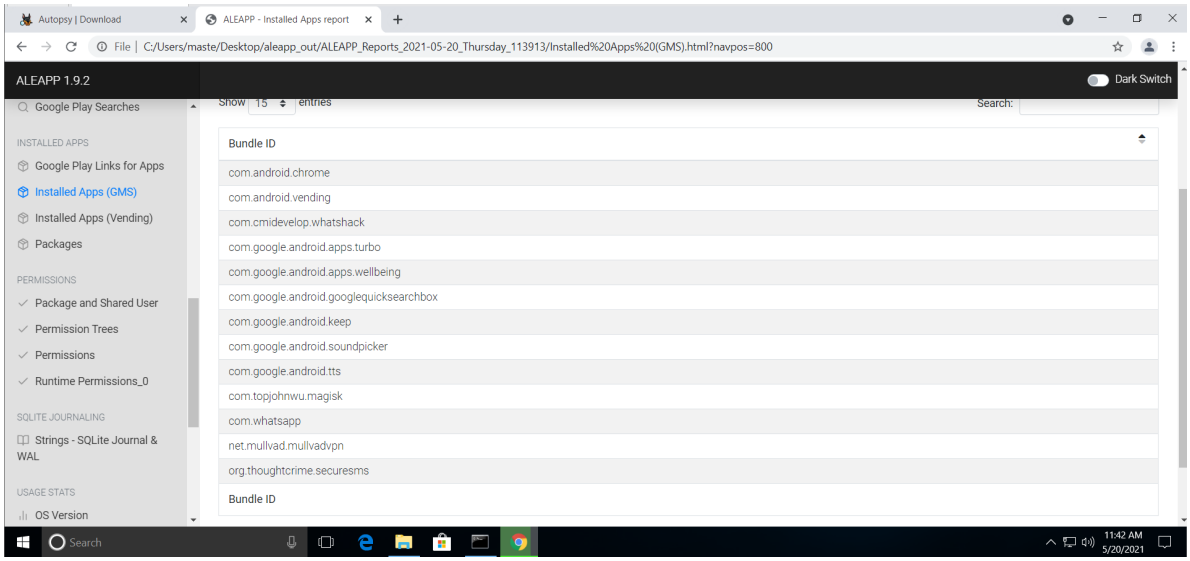


Once the processing is complete, you can select “OK” on the pop-up, which opens the output report (in the default browser), which contains and details the common evidence found in android devices. The report gives information pertaining to contacts, messaging applications, SIM cards, phone model and make etc.

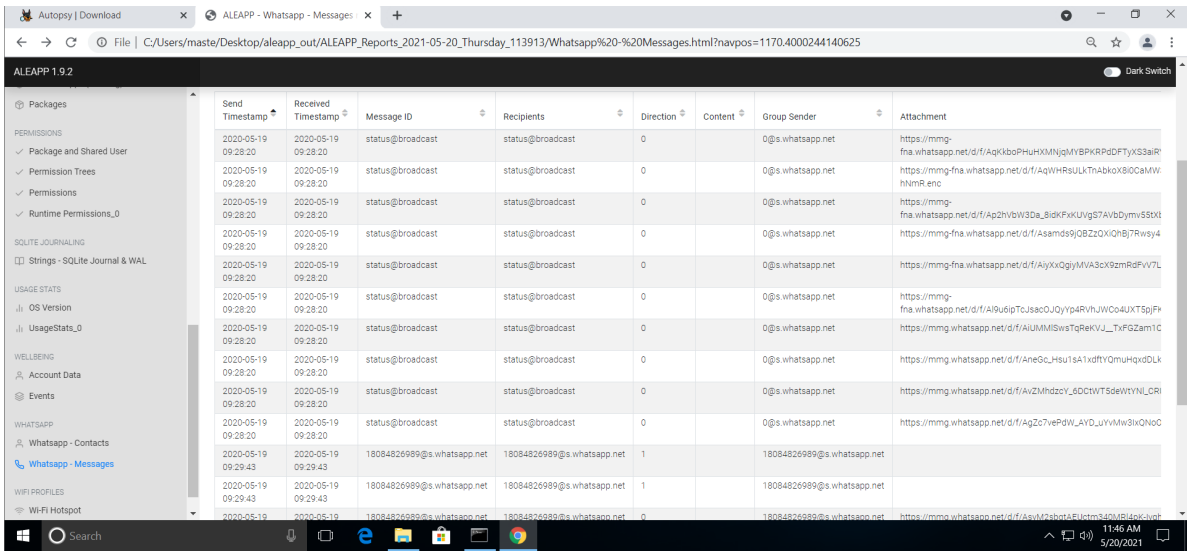




We found out there were some interesting URLs in the extracted chrome history, which we might want to do a more in-depth investigation into later on.



We can also see a very minimal installation of applications (default apps are probably removed)--in this case chrome, whatsapp and thoughtcrime securesms are worth looking into. We hypothesize that this is likely a burner phone since there are minimal applications used.

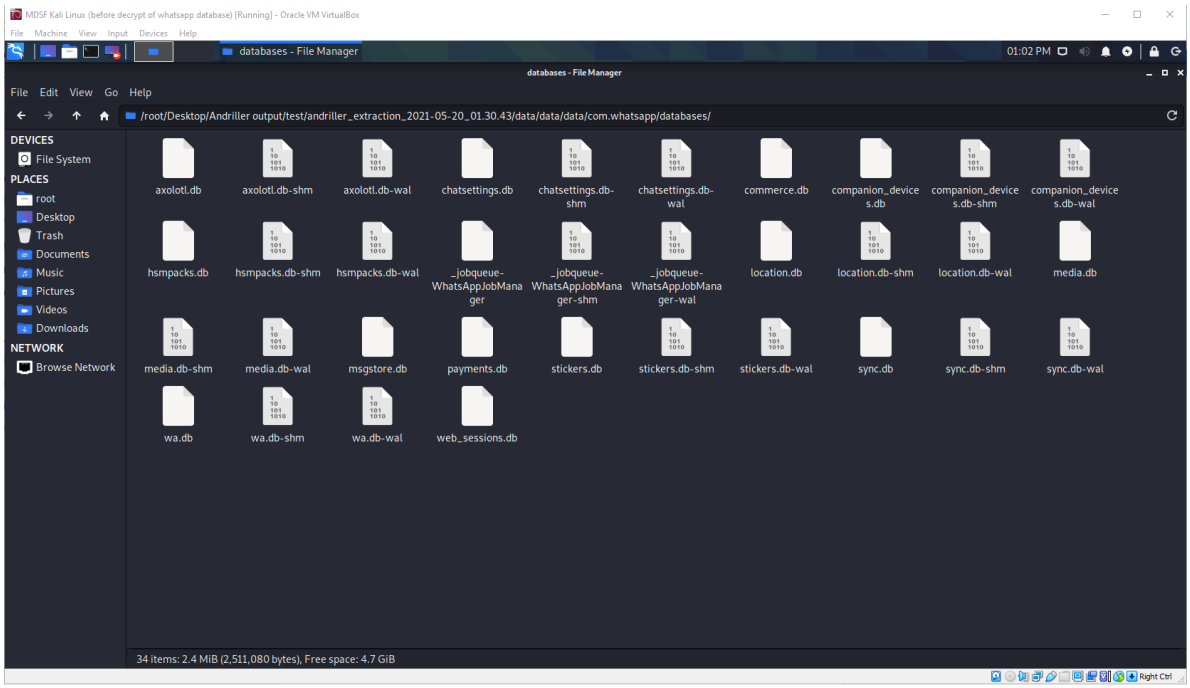


There are also interesting Whatsapp contacts and messages worth looking into. To get a more visual view, we will use Whatsapp Viewer, which uses a GUI.

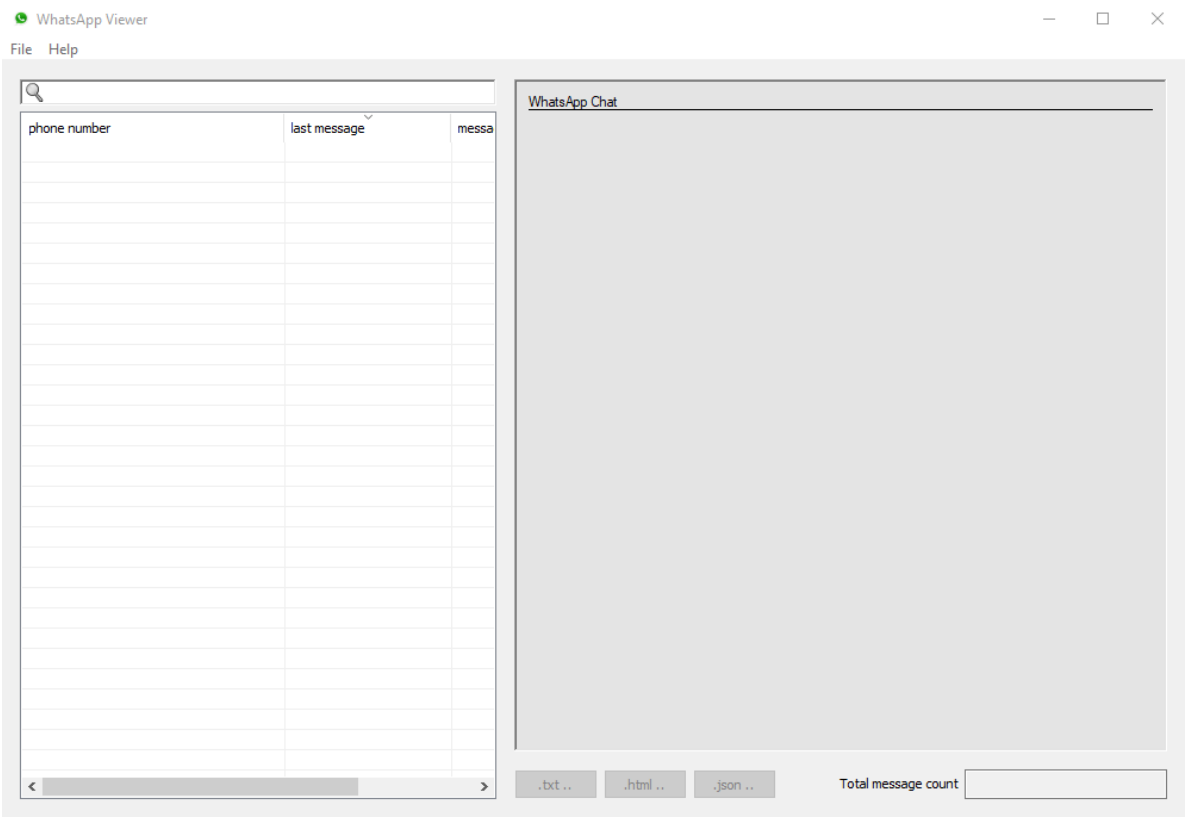
c) *Whatsapp Viewer messages*

WhatsApp Viewer is a simple Windows tool that allows us to display chats from android phones through the msgstore.db file which is where chat history is stored. It also has the capability of decrypting any WhatsApp encrypted files like .crypt5, .crypt7, .crypt8, .crypt12 and .crypt1. It does so by using the key file to decrypt messages. In this example however, decrypting the file would not be required. It displays the chat history in the order that it was sent and also shows it in a neat GUI - just like how it is viewed in WhatsApp itself.

First, we need to get the msgstore.db file from the image that was extracted using andriller previously. We need to navigate to where the msgstore.db file is located, which is ***/data/data/data/com.whatsapp/databases/***.

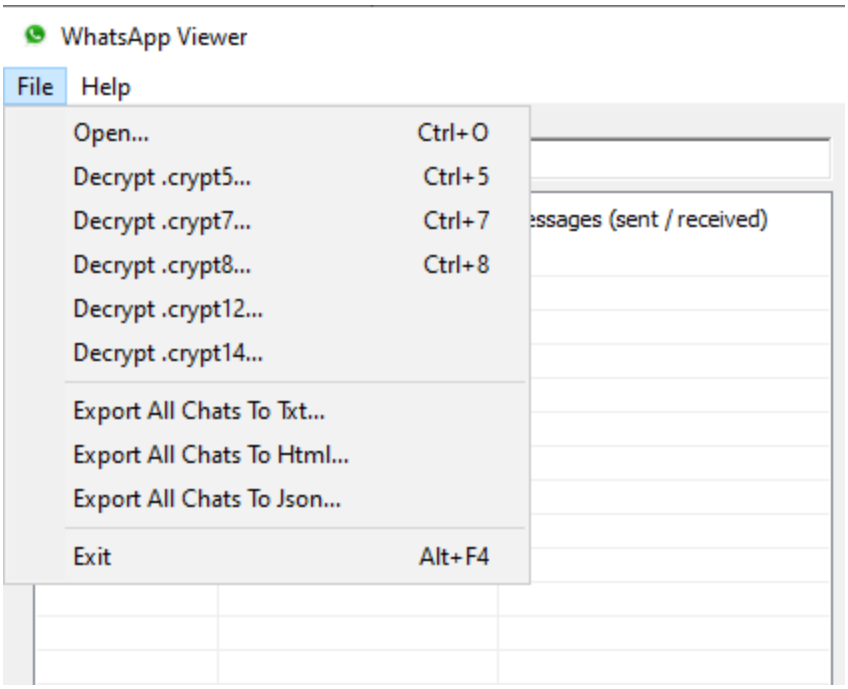


If a linux machine is being used, like in the picture above, the file would need to be transferred over to a windows machine. On the windows machine, double click WhatsApp Viewer.exe and the UI should open with two panes as follows.

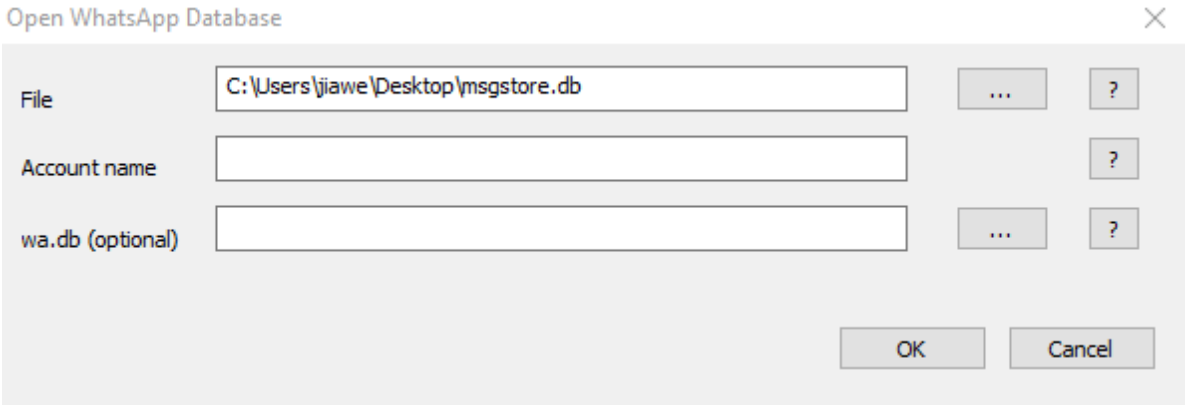


RyonNgCT Inc.

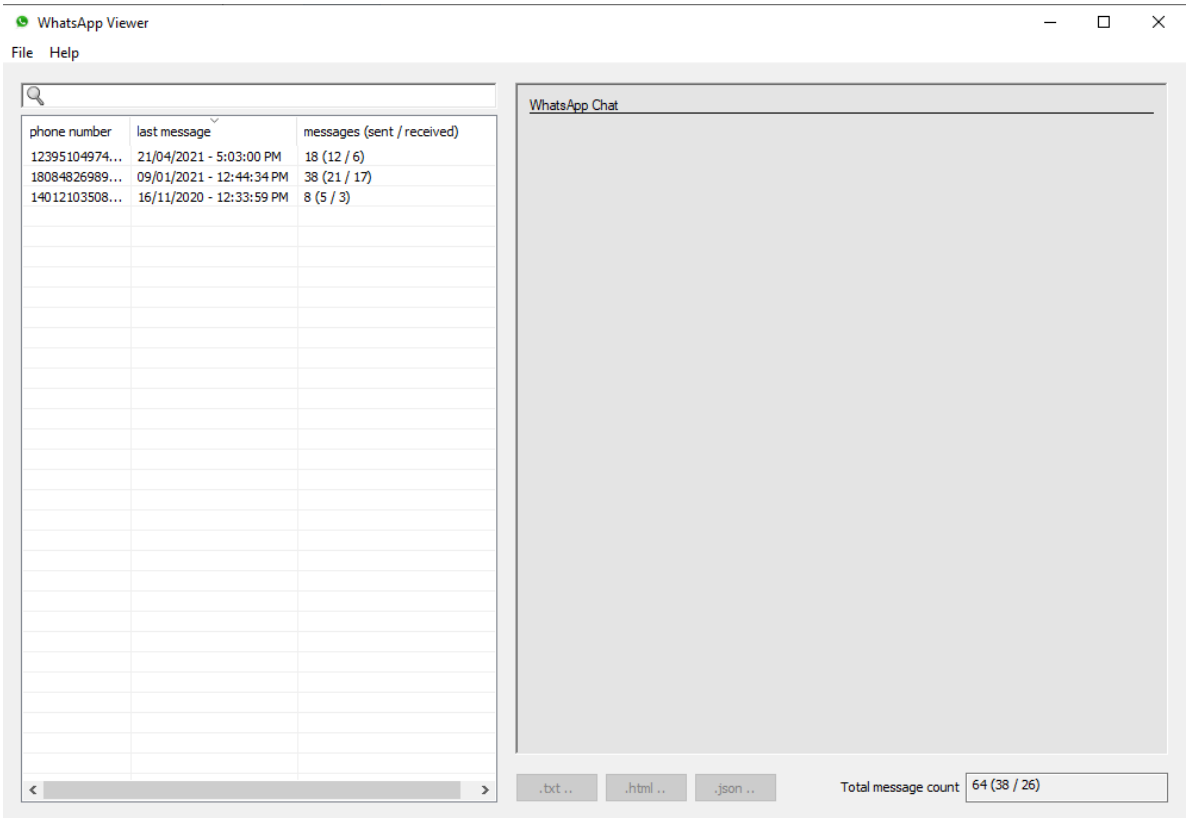
When we click on the file tab we can see all the options available to us. For this example we will just click open since decrypting would not be required, however, should decrypting be required, the key file should also be obtained (should be found in the WhatsApp Directory).



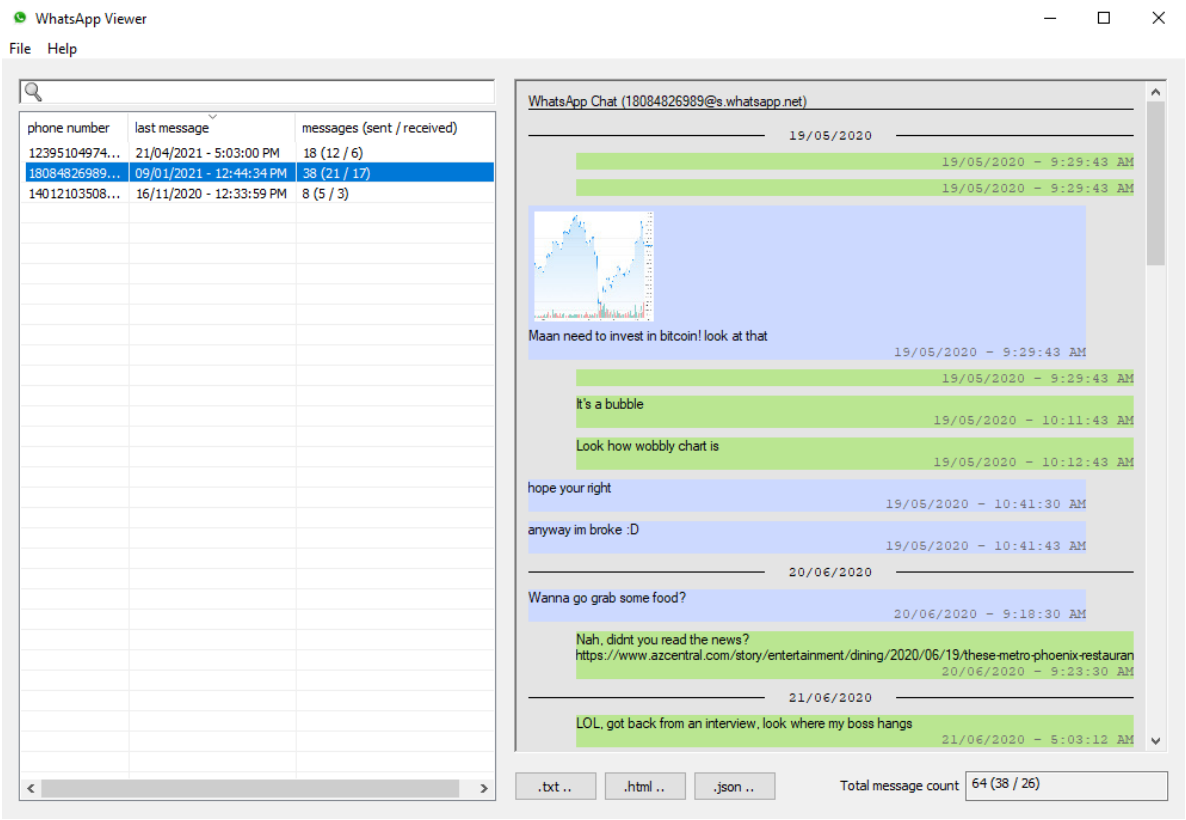
Here we select the file and click OK.



The chat history of all the messages should pop up on the left.



Clicking any one of the chats will display it in a nice GUI like how it was sent in WhatsApp itself. Any previously sent pictures will also be displayed.

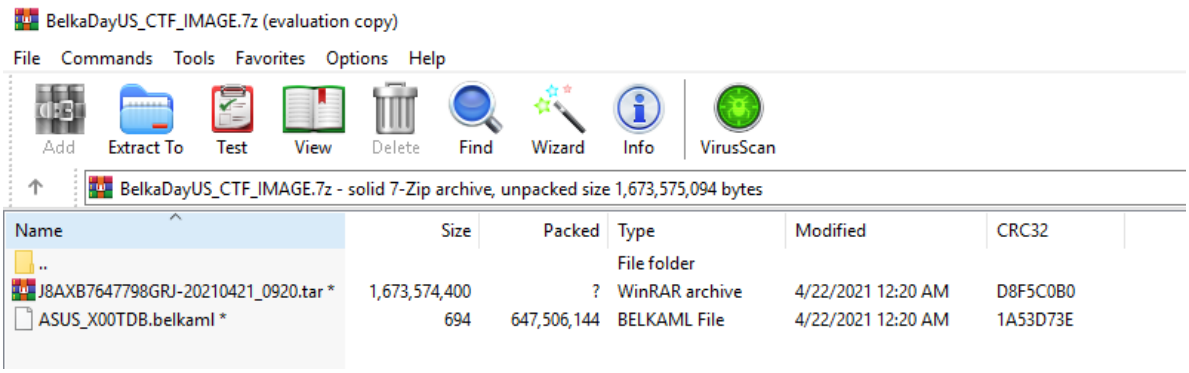


RyanNgCT Inc.
SECURING WITH AI

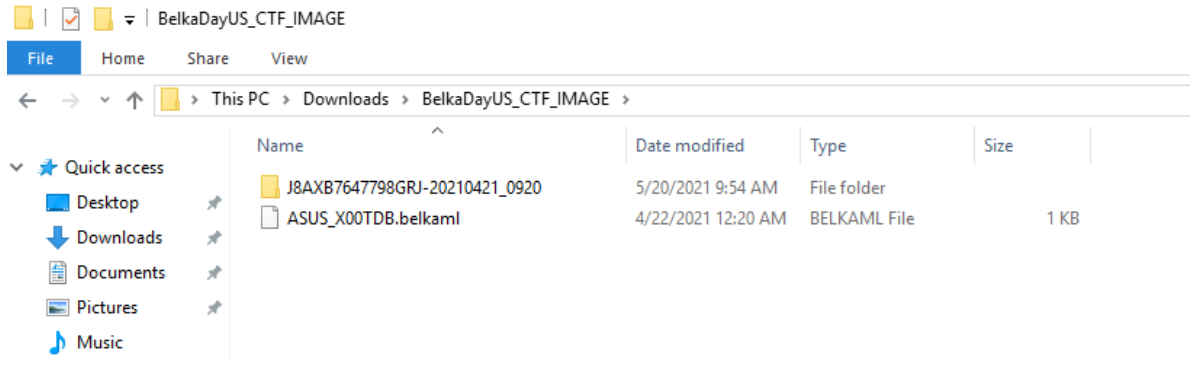
d) *Investigation using Autopsy Android Modules*

This will help us to more easily correlate the messages and media to quickly establish the communications exchanged. Using Autopsy on a Windows 10 virtual machine, we can also view the full and thorough analysis of the data contained within the ASUS phone. Although Autopsy is mainly used for computer forensics and not for mobile forensics, there is an Android Module which was also used in order for us to analyze and obtain the data as shown. Using Autopsy is also a method to confirm and cross-check the evidence and report with the other softwares used, ensuring that results shown are consistent despite using different tools.

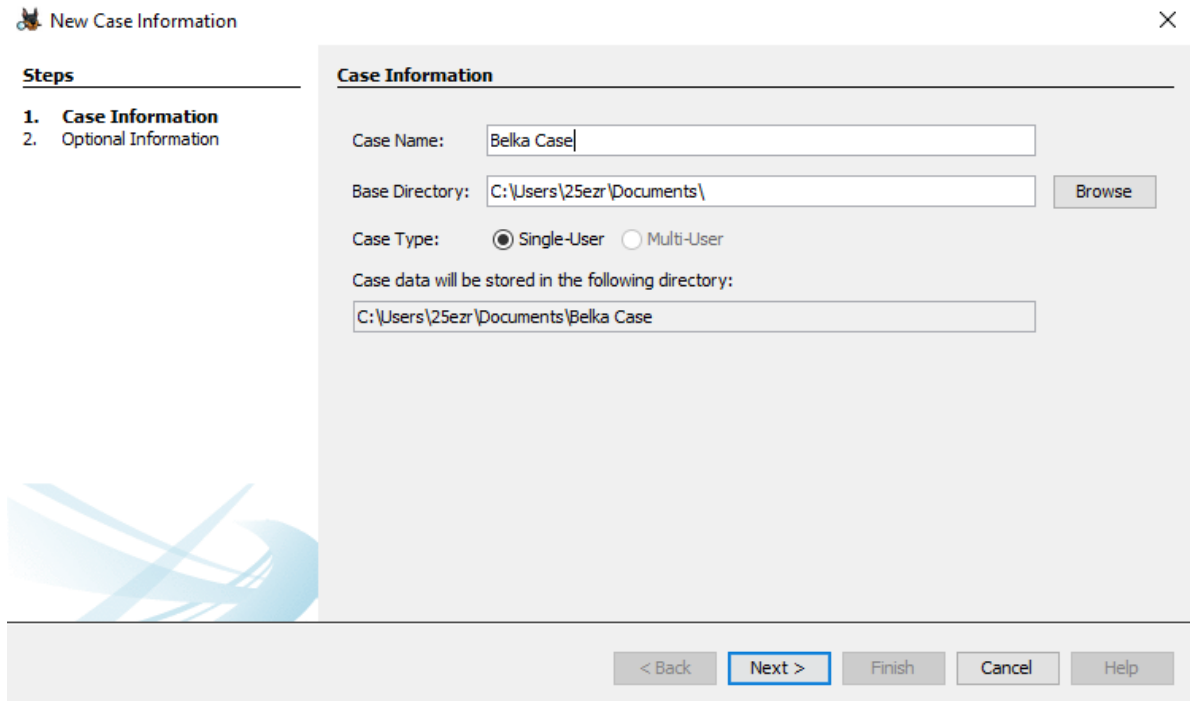
Firstly, we download the evidence file from Belkasoft (https://belkasoft.com/ctf/) called "BelkaDayUS_CTF_IMAGE". Once the downloaded image has been extracted, it will display 2 items inside. One is "ASUS_X00TCB.belkaml" and the other is the "J8AXB7647798GRJ-20210421_0920.tar" file.



Proceed to parse the .tar file to obtain a folder as shown in the image below. (In Linux we can extract it using *tar -xvzf <filename>*)

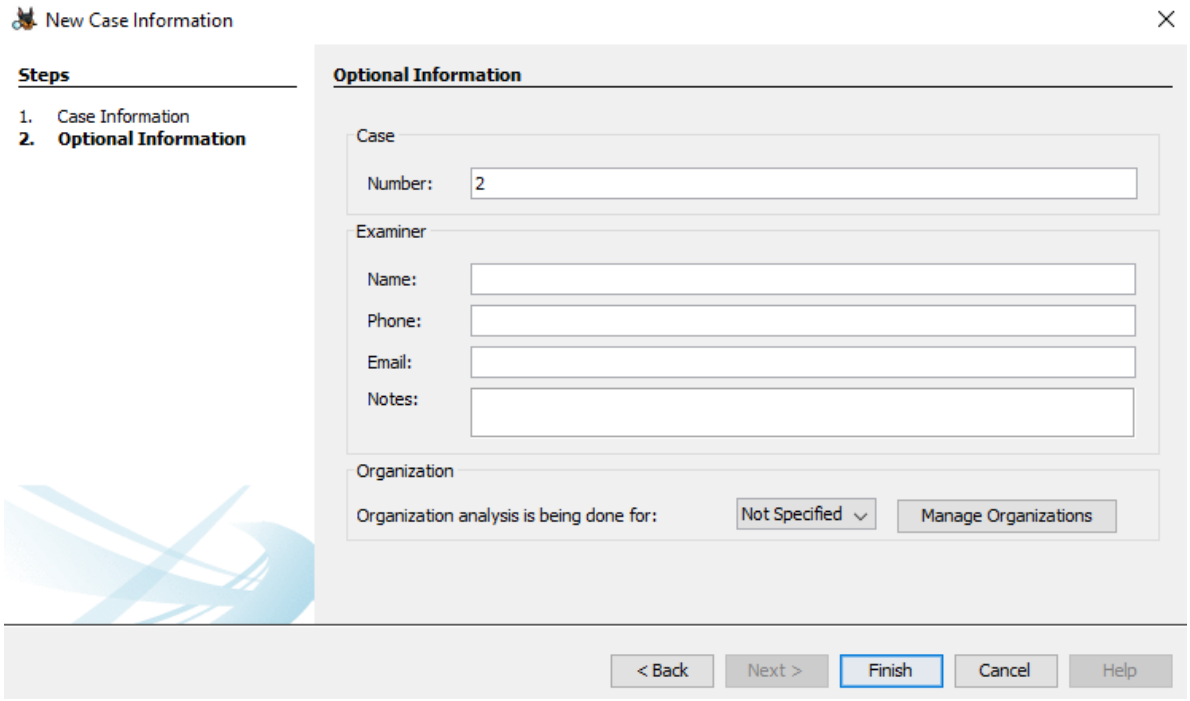


Launch Autopsy and open a new case.



Enter a case number.

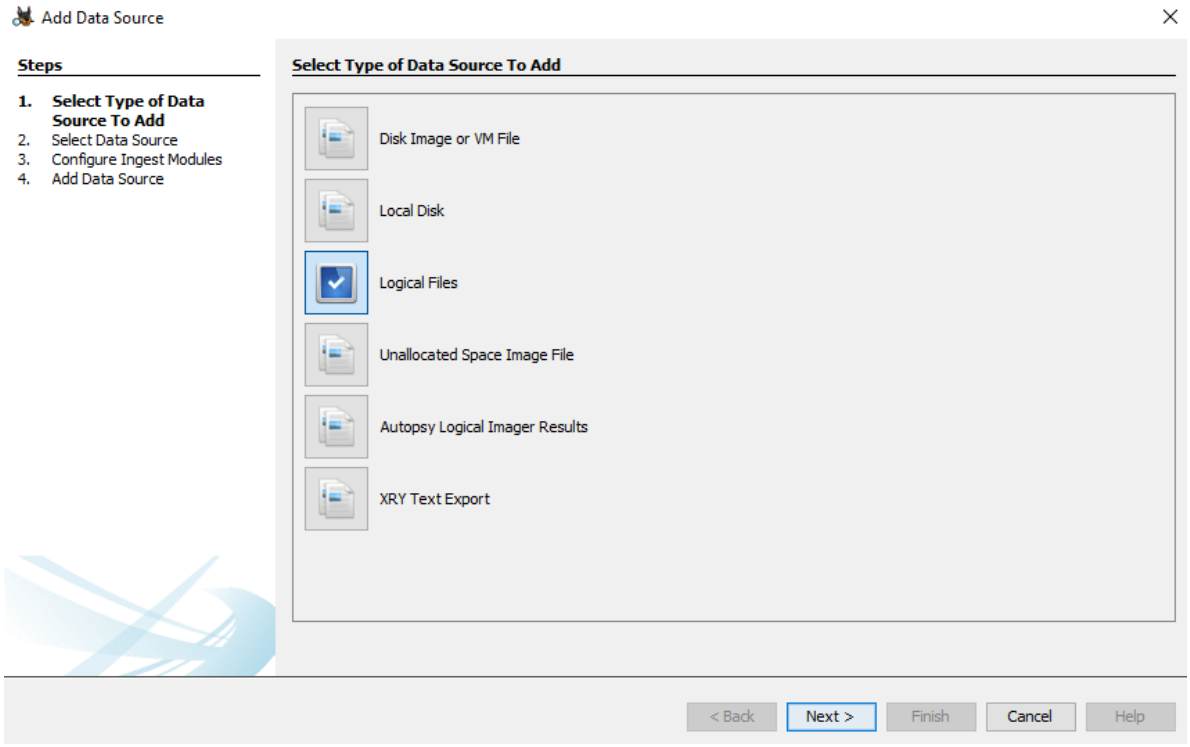
Open Source (Academic Usage)



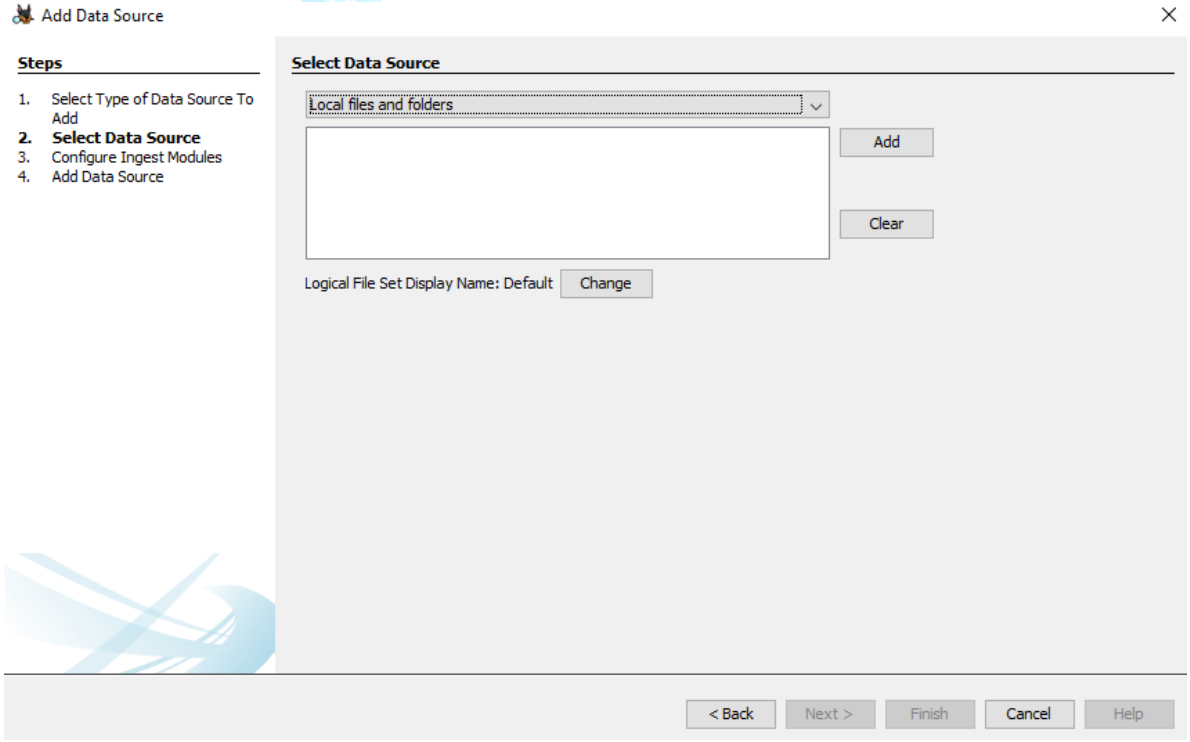
RyanNgCT Inc.
SECURING WITH AI

Open Source (Academic Usage)

Select “Logical Files”

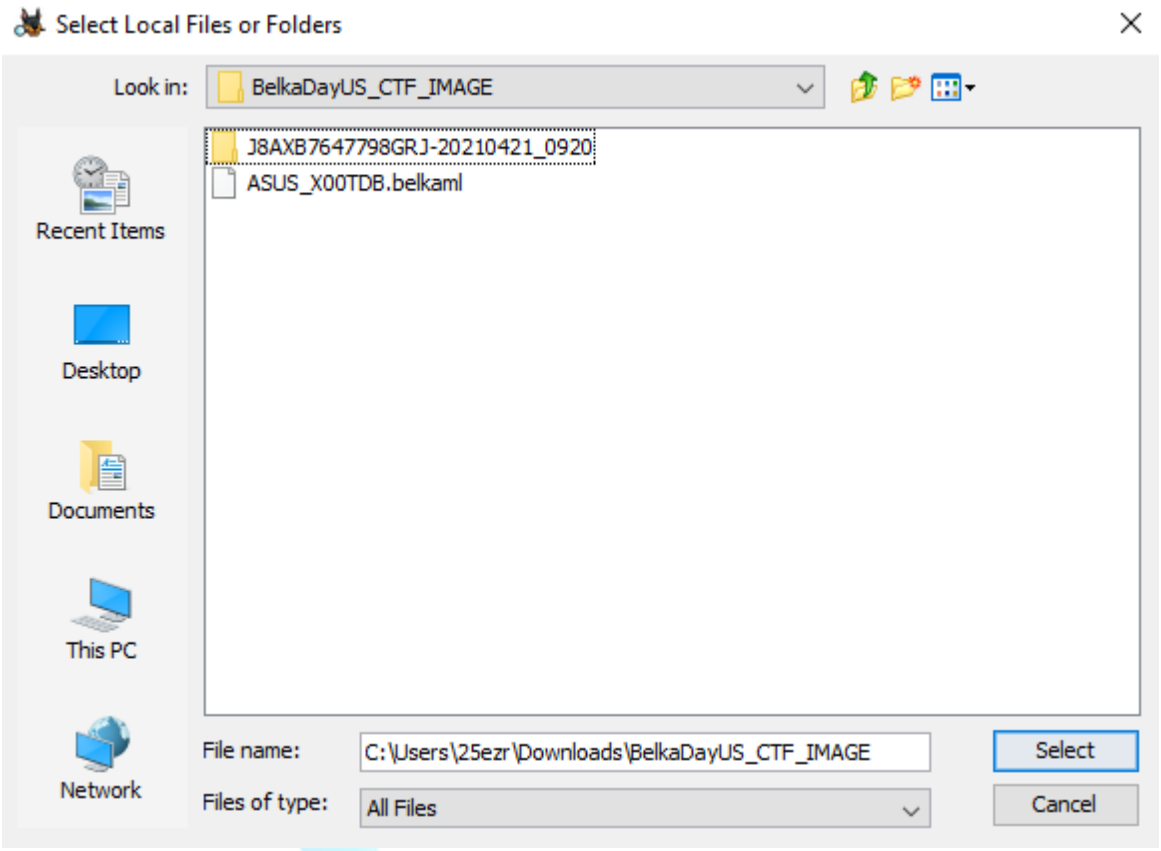


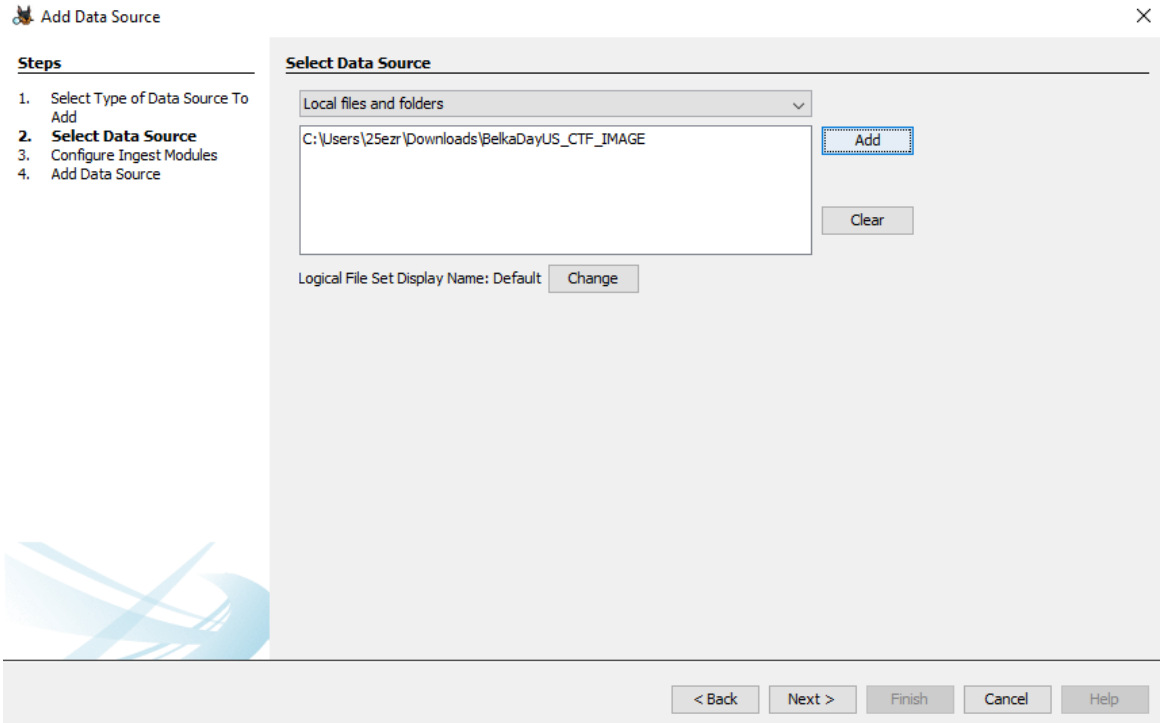
Click on “Add” and proceed to add the “BelkaDayUS_CTF_IMAGE” as the image.



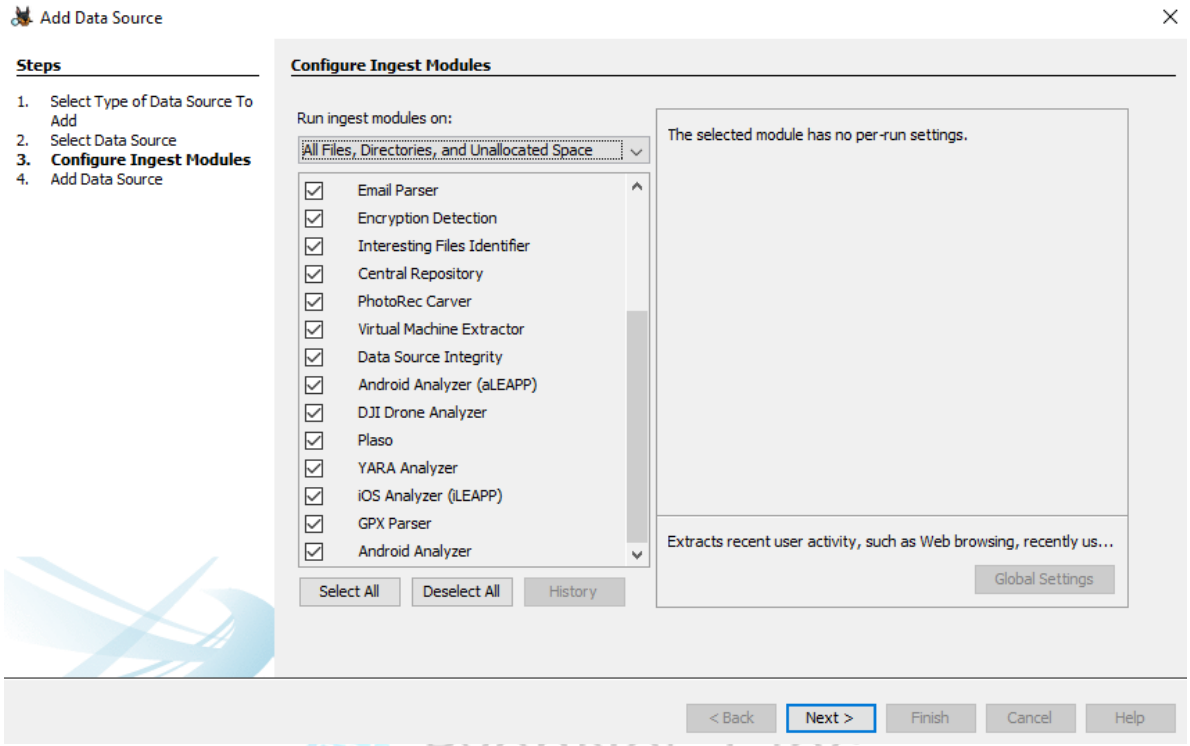
Team_dadroid_2021_NP_CSF

Click on “Select” and ensure that it is the image file that is being ingested, not the “ASUS_X00TCB.belkaml” and the other is “J8AXB7647798GRJ-20210421_0920” folder.



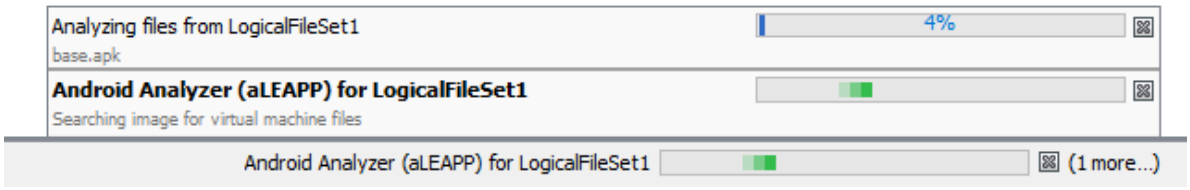


Ensure that the Android Analyzer checkbox is ticked to allow the modules to be run on the image afterwards. This is to allow for specialized extraction of android-related artifacts which Autopsy can parse.



Click on “Next” to start the ingest process.

The ingest process will begin, please let it fully load until completion before beginning analysis.

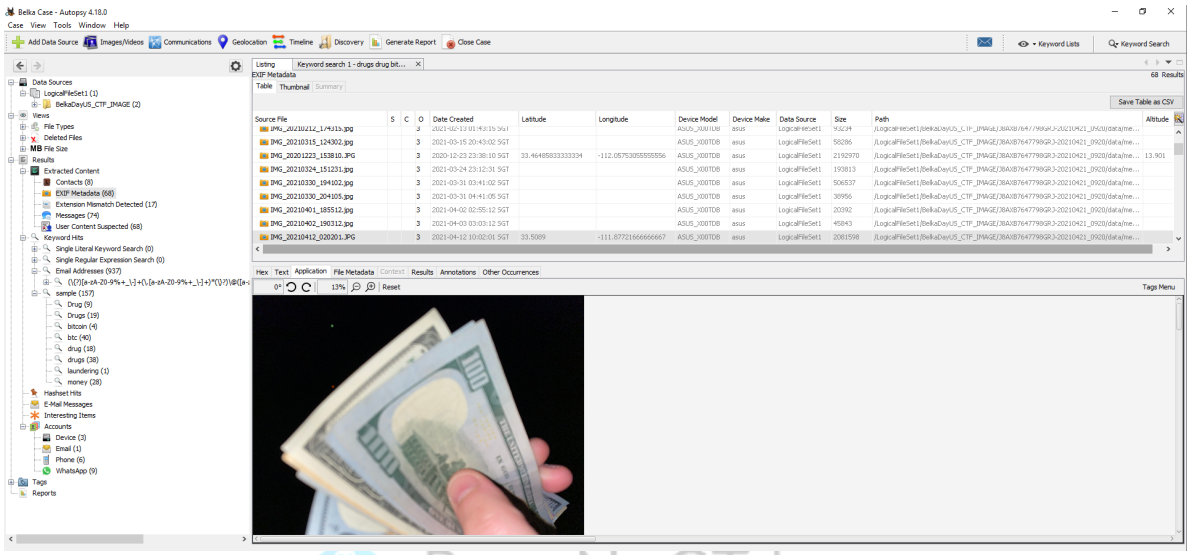


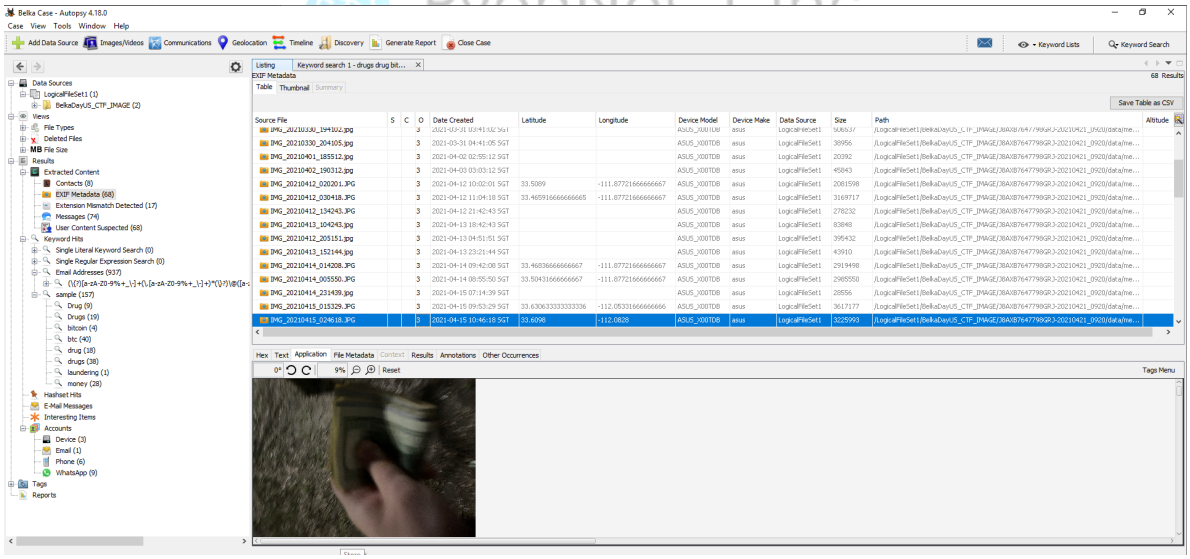
Investigation of Key Artifacts using the Tools

We will now proceed on to use the various tools to gather incriminating evidence on the case.

1. Images

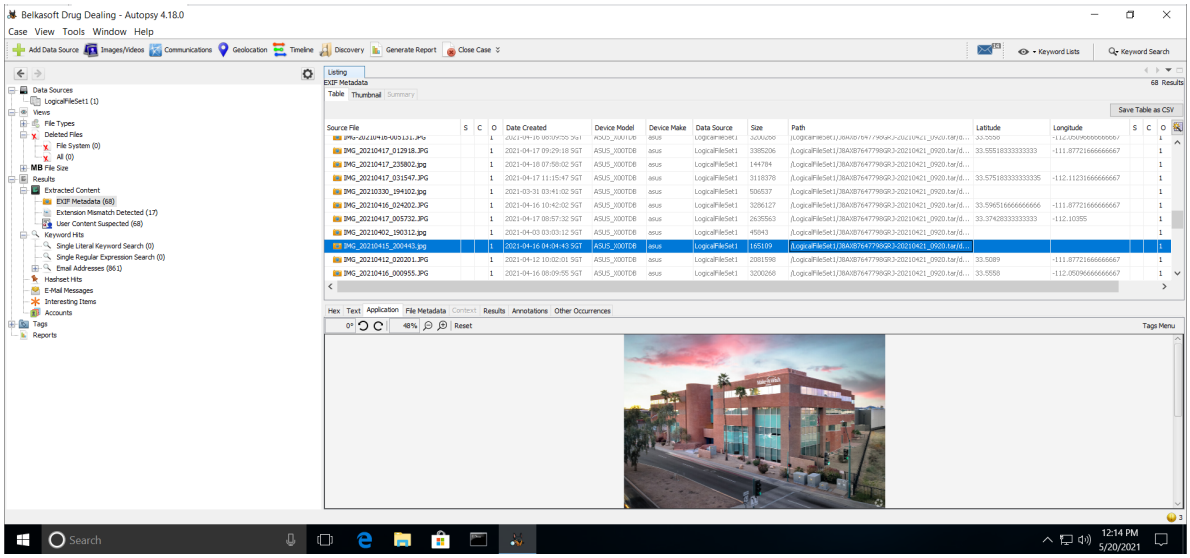
When initially analyzing the images, we realised that there are a lot of screenshots of bank notes, which might suggest that the suspect could be involved in money laundering or drug-related activities.

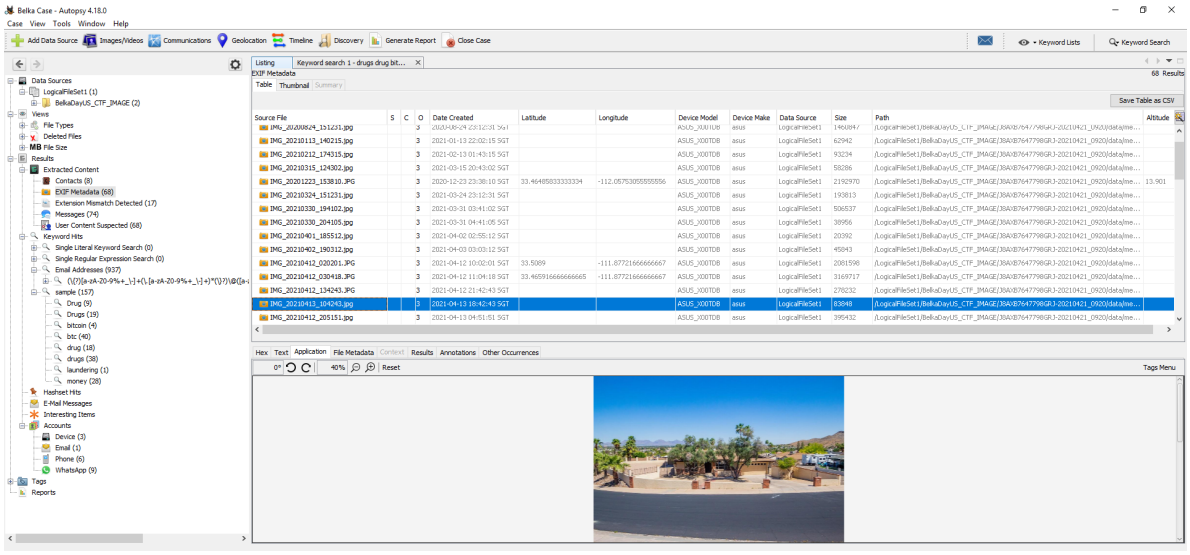




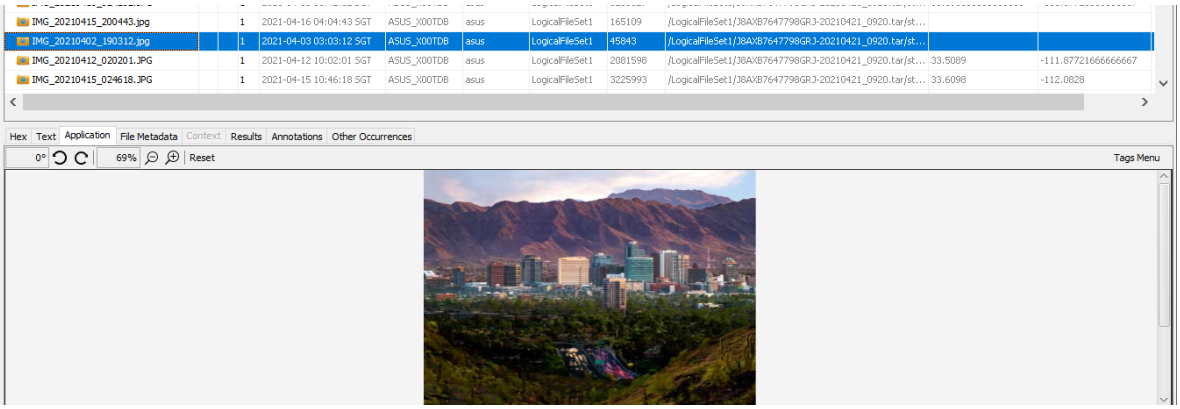
Pictured above is another image of possibly the suspect holding bank notes as found in the Exif Metadata tab in autopsy.

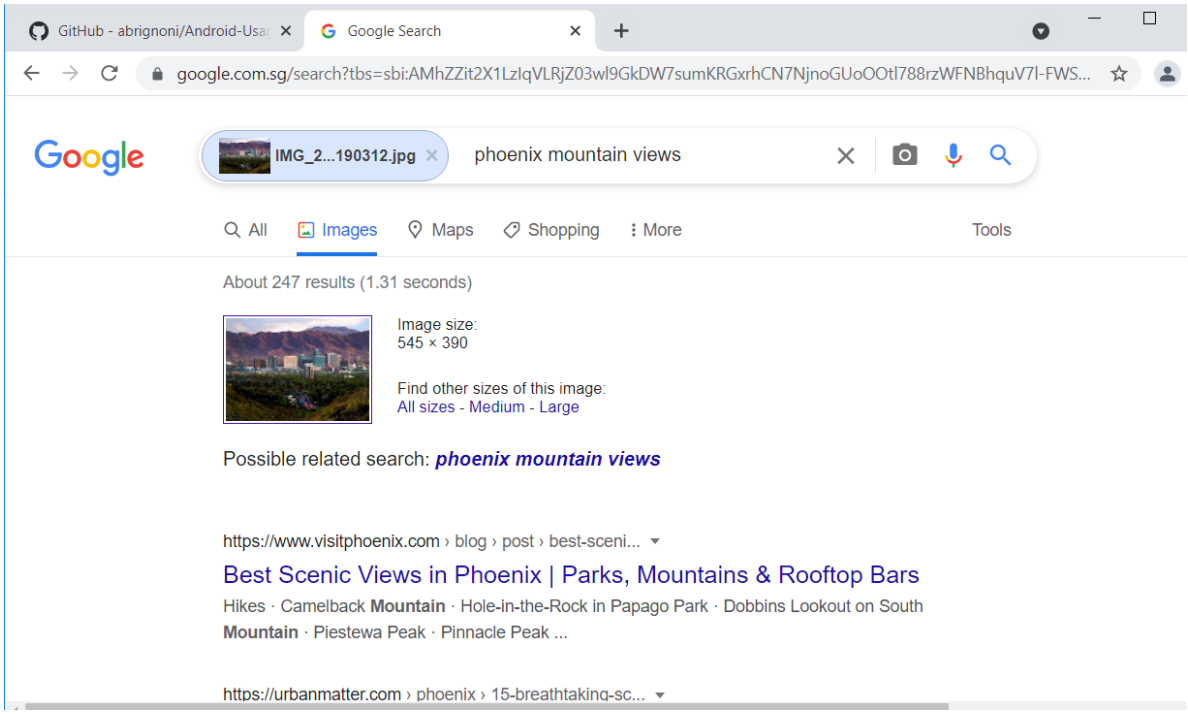
There were also images of places, likely the meet up points for selling and distributing drugs. We plan to perform reverse search using the images to determine the locations and subsequently help police to establish a pattern if any.



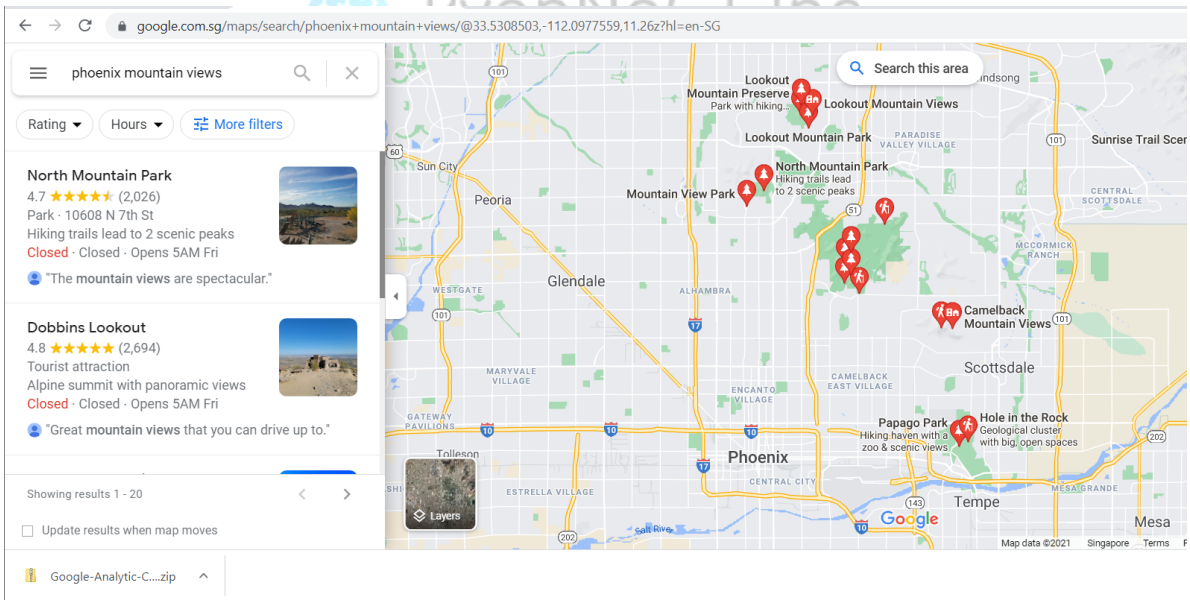


A reverse search for the image below found that it was located in Phoenix Mountain Views.

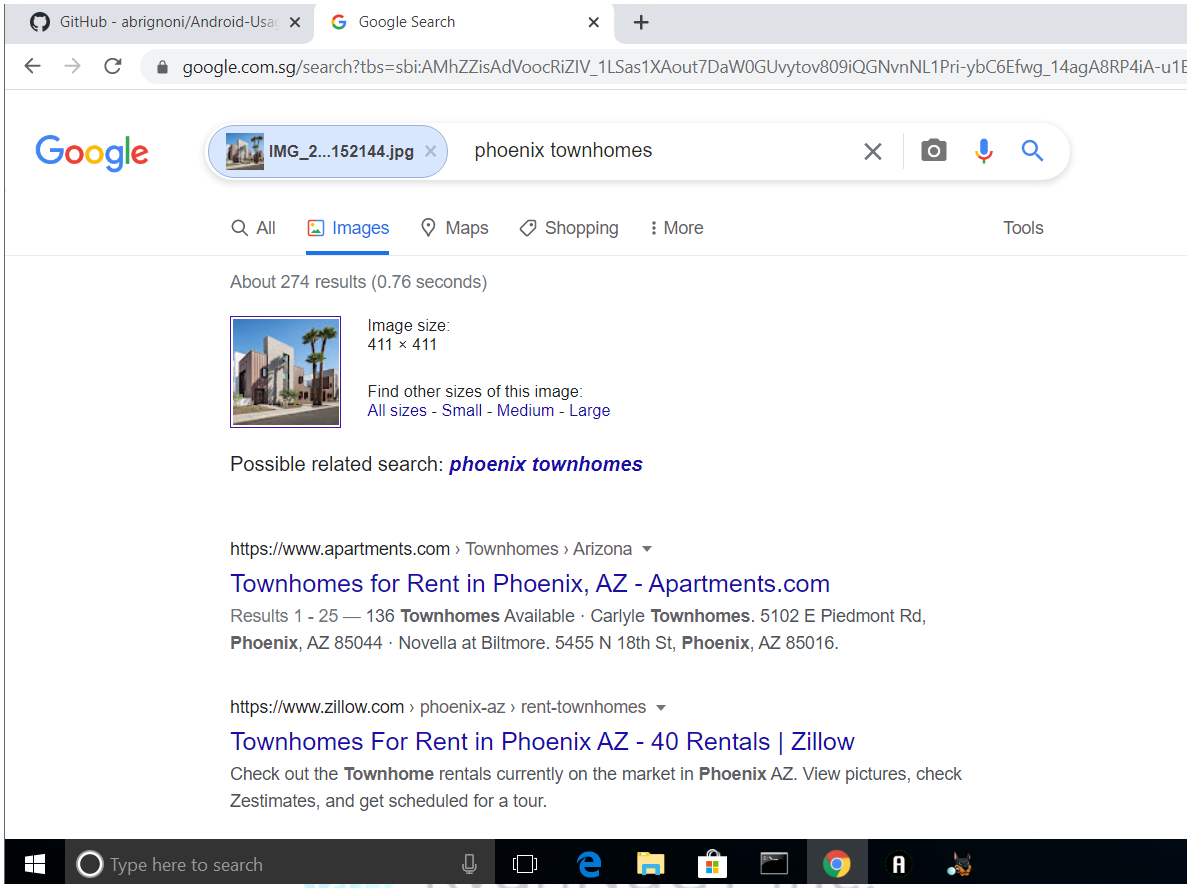




Using Google maps, we can narrow down the search scope to where Derek may have possibly met up with his friends.

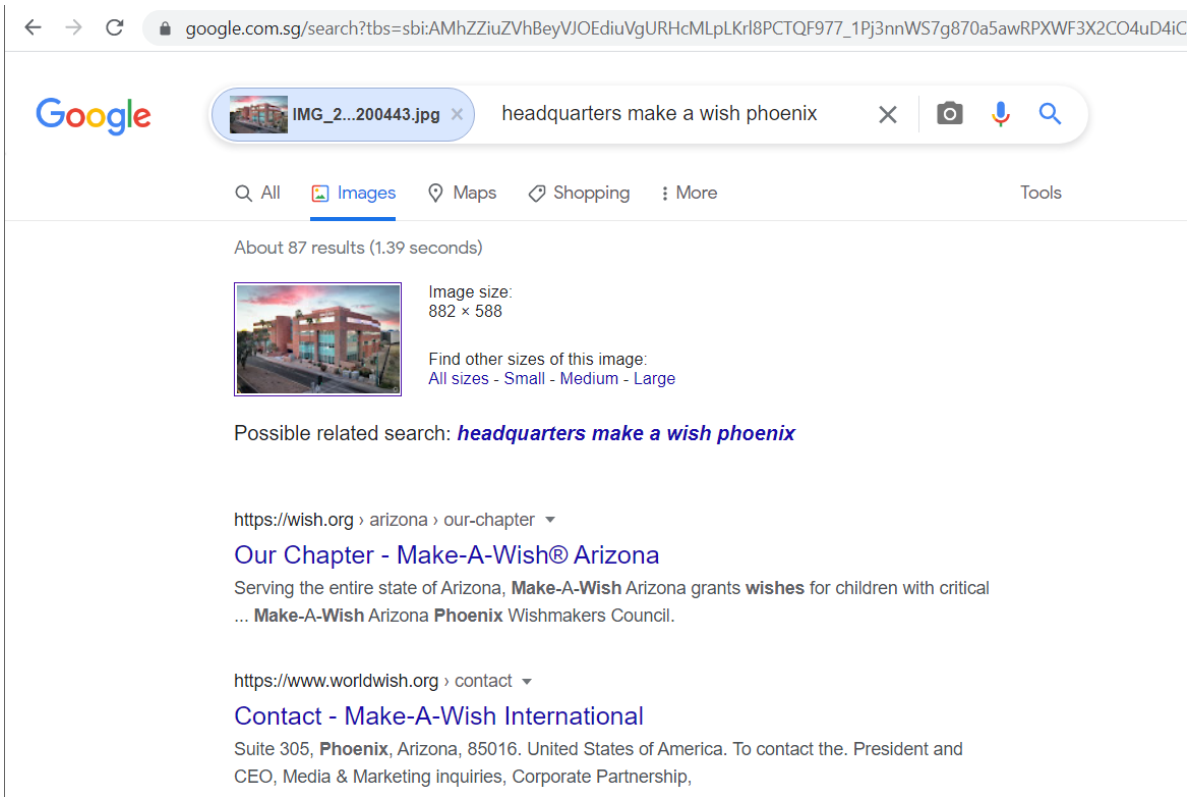


Furthermore, other images were linked to apartments around the area.



SECURING WITH AI

There is also another image that discloses exactly where they met (has the sign and name of the location).

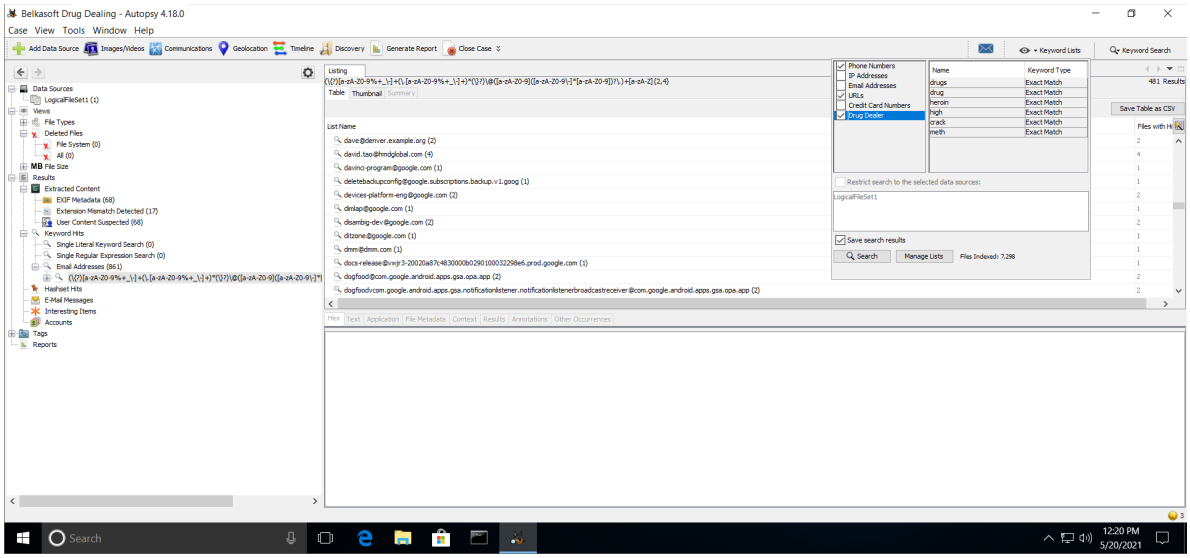


Thus, if police or law enforcement were to set up an ambush to arrest the rest of his accomplices, they could do so at the places mentioned above or the screenshots of the other images in his phone using Google Images Reverse Search Mechanism to predict patterns in meetup locations and cordon off the respective areas.

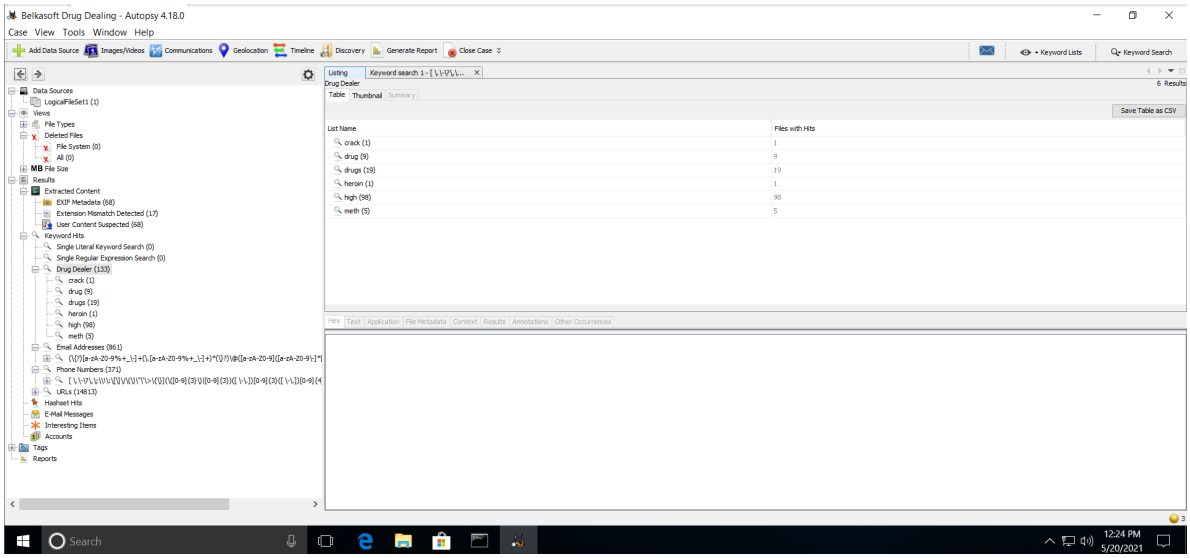
2. Keyword Searches

We will now be using Autopsy's keyword search feature for a more in-depth search for possible evidence/data in the logical image.

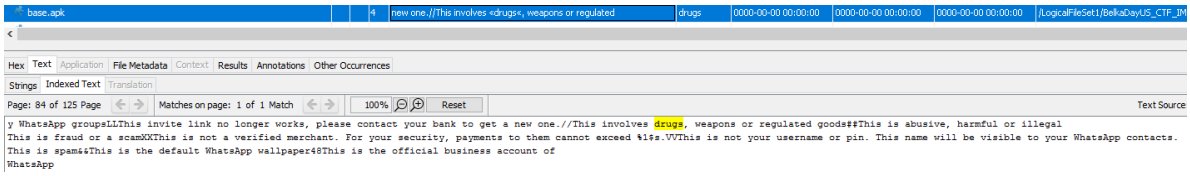
Using a keyword search for different drug names yields the following output:



The results showed that there were mentions of common terms used in the drug dealing trade that might be of interest to police (and some which are specific to the case).

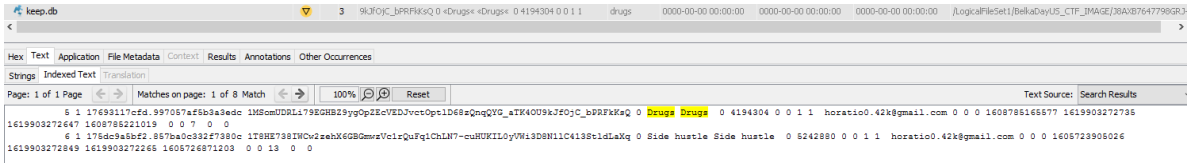


Open Source (Academic Usage)

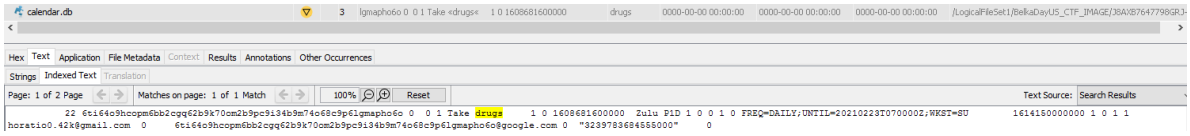


RyanNgCT Inc.
SECURING WITH AI

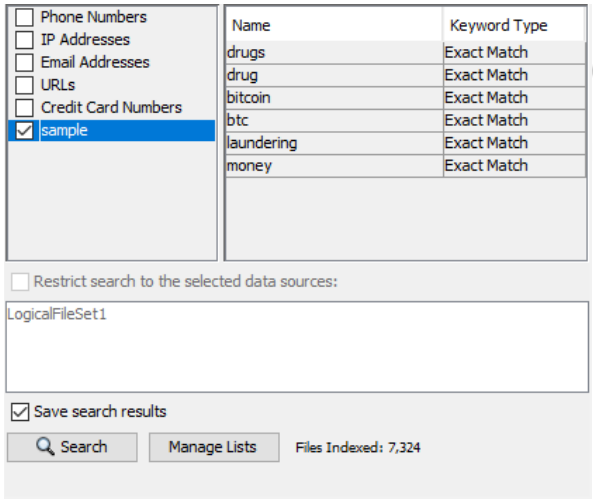
An email, horatio0.42k@gmail.com, appears in this search (after using the email address regex match) and can be seen encouraging the owner of the phone to pursue drug smuggling as a side hustle. This might potentially be the “Boss”. This statement will be re-evaluated later once we uncover more information.



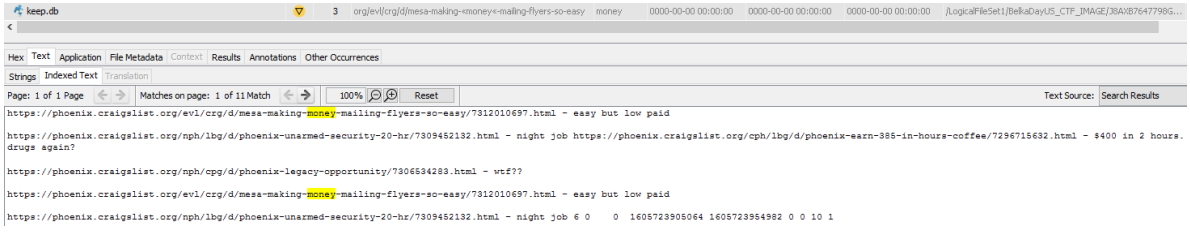
More evidence points to the phone owner being a drug dealer as her phone calendar has an event which is called “Take drugs”, possibly indicating that she was supposed to go and collect drugs to be sold to potential customers.



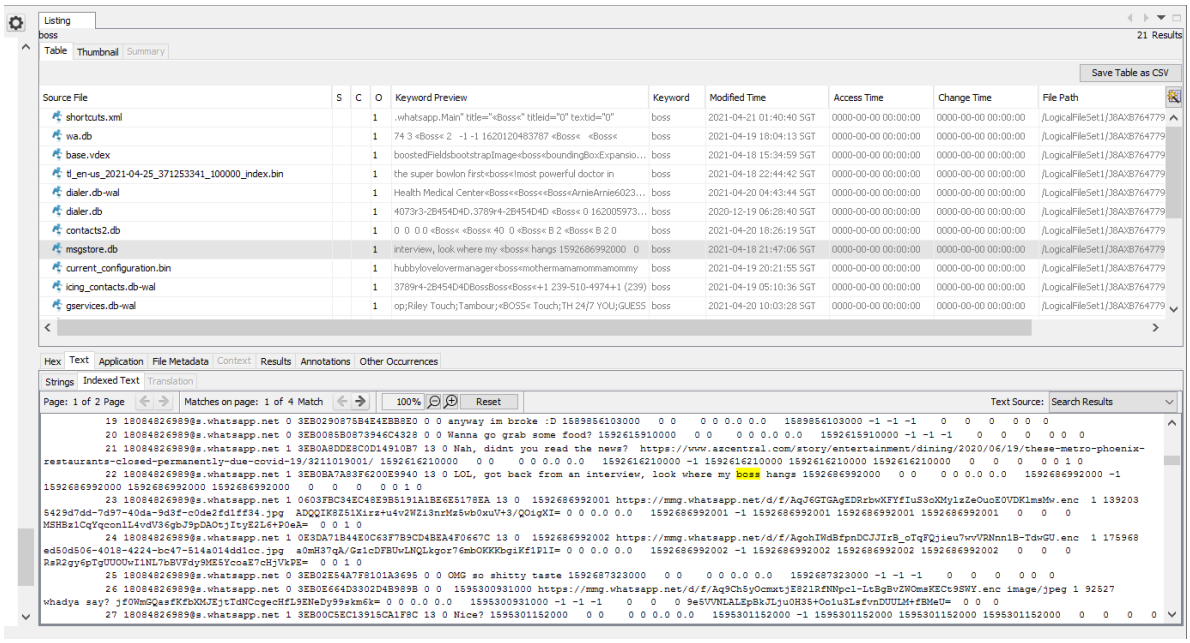
More keywords were used to find more information regarding the information we have gathered thus far.



Other keywords were used and it produced this result as shown in the image below. The image shows that the owner of the phone was looking for a side job and has decided to keep certain links related to side jobs.



Since we found conversations in Whatsapp with the alias of “Boss”, we also used this keyword in our second keyword search.

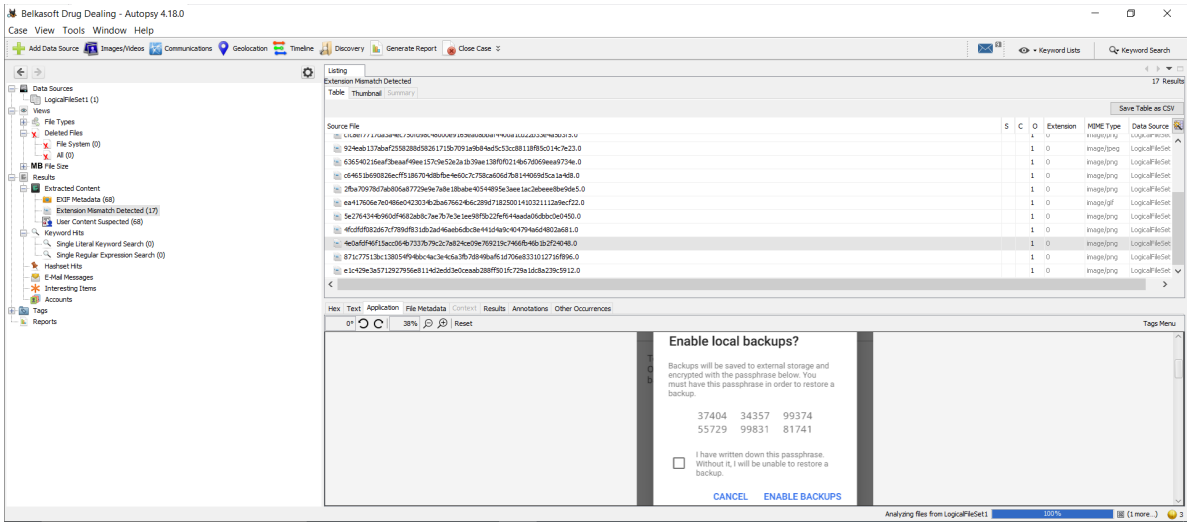


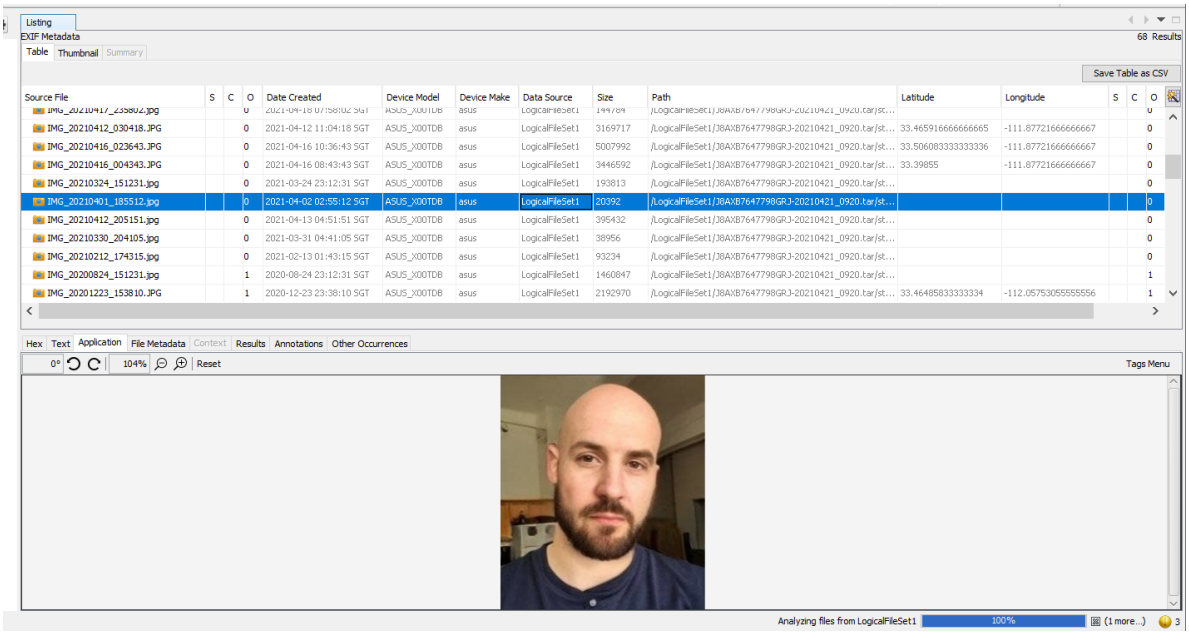
Diving into the details of the keywords search, we can find entries which match the messages extracted using Whatsapp Viewer.

RyanNgCT Inc.
SECURING WITH AI

3. Extension Mismatch

The suspect also likely performed local backups (in extension mismatch tab), because it is unlikely that such an image is currently in Autopsy’s database (format in which these codes are saved in). There were also many suspicious images of money, bitcoin and a face (which kept showing up), and google backup codes, which might help the police in their investigations. The codes specifically could be used to login to gmail accounts to gain access to messages or plans formulated there.



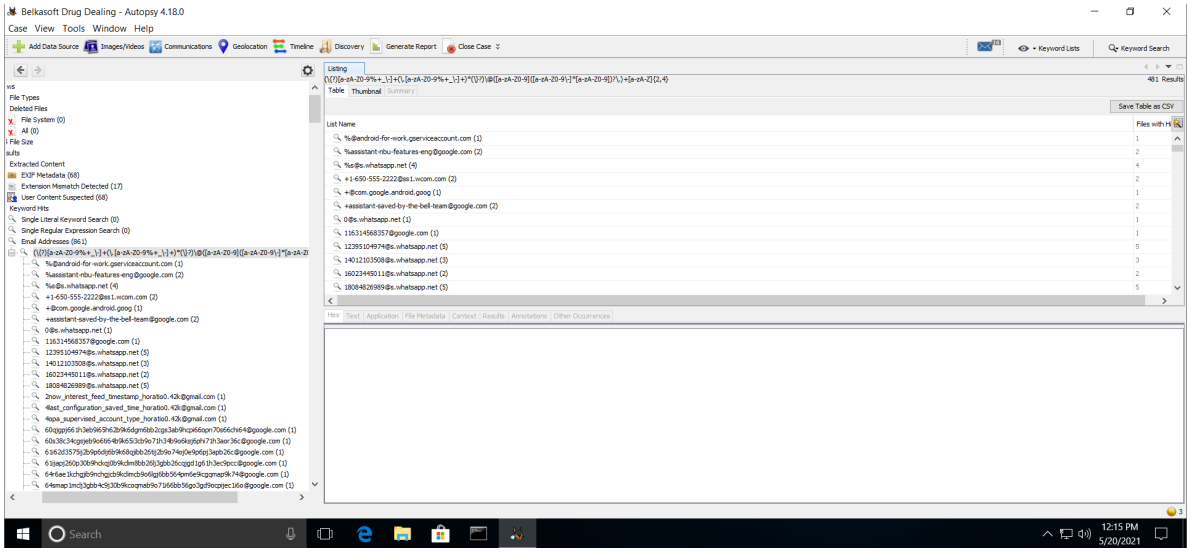


We can use this face to conduct a reverse search in a local or international police or immigration database to try to ascertain the identity of the individual in the photo.

RyanNgCT Inc.
SECURING WITH AI

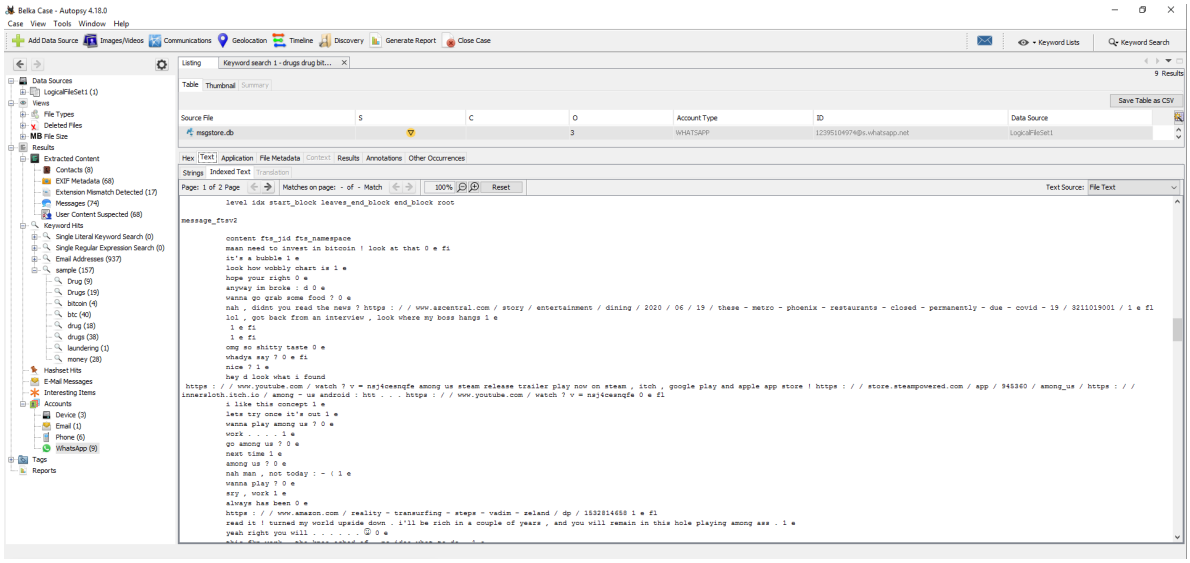
4. Whatsapp Information

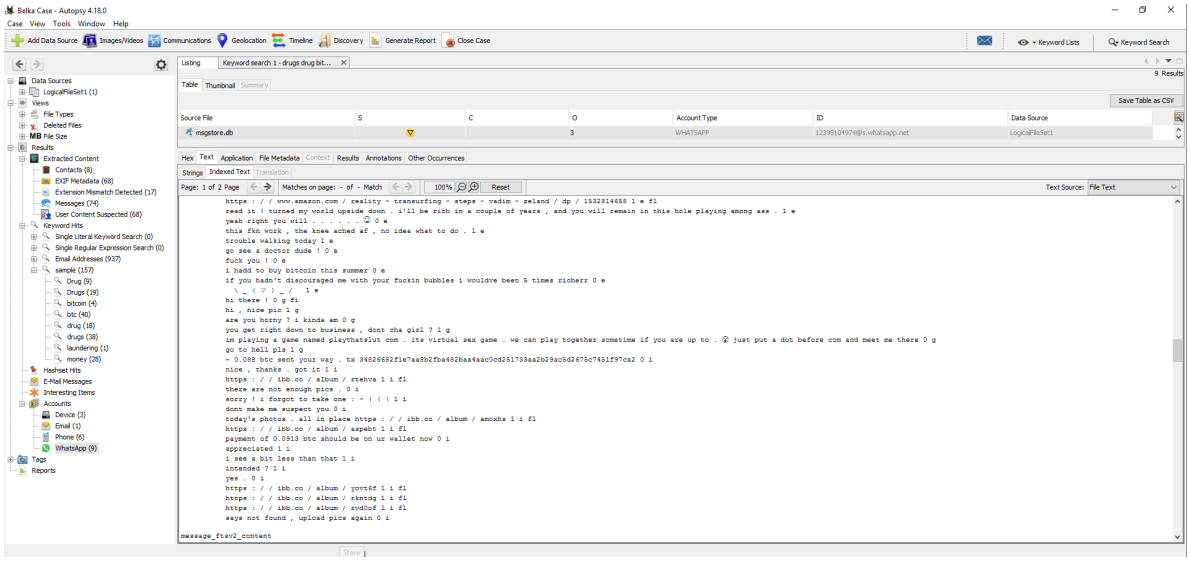
Below is some information on Whatsapp, email and apps installed as filtered by the email regex syntax of the keyword search. This might be useful later on the investigation, especially email, since it may not be directly accessible through the phone (suspect might not have logged in there), and if that is the case, then the officers would have to find ways to be able to access it, as there might be critical evidence there.



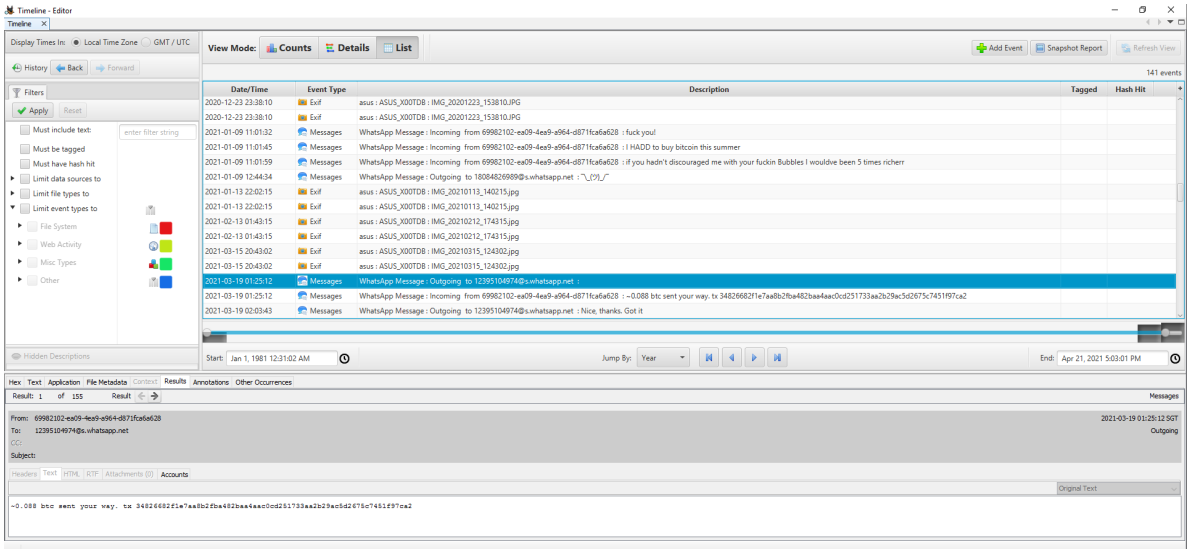
RyanNgCT Inc.
SECURING WITH AI

The two images below contain the whatsapp messages exchanged between “Boss” and the phone owner, these can be again correlated with the extracted images from WhatsApp Viewer.

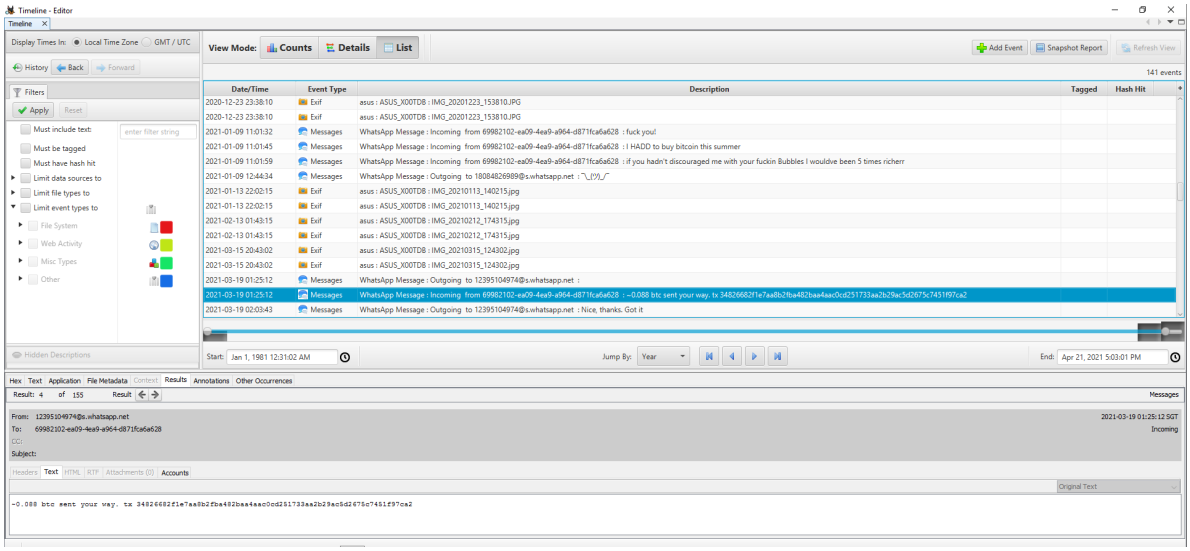




The image below shows the owner of the phone sending roughly 0.088 bitcoin (btc) to “Boss”.



This next image also shows “Boss” sending roughly 0.088 bitcoin (btc) back to the owner of the phone at exactly the same time. → he probably copied and sent the same message back to double check because it was the same authentication code.

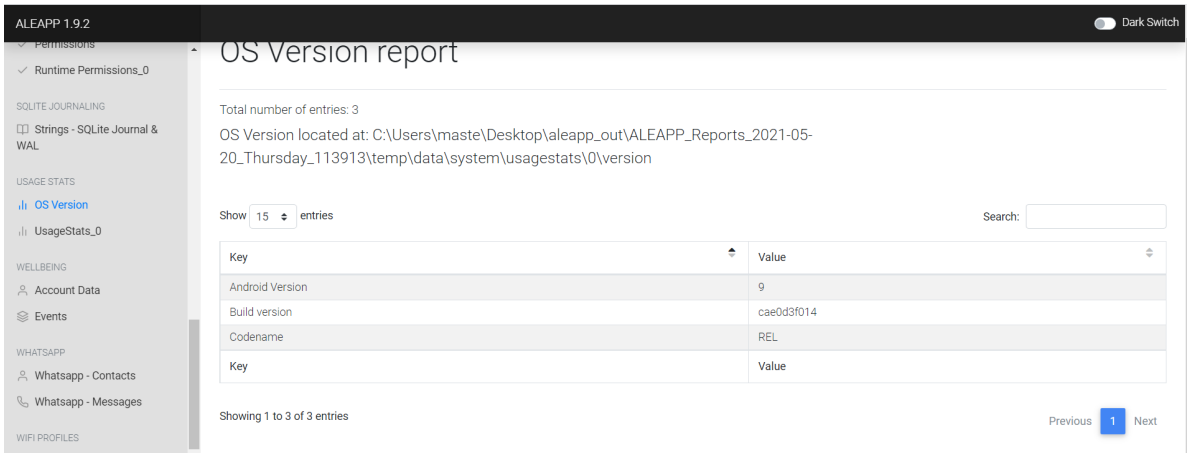


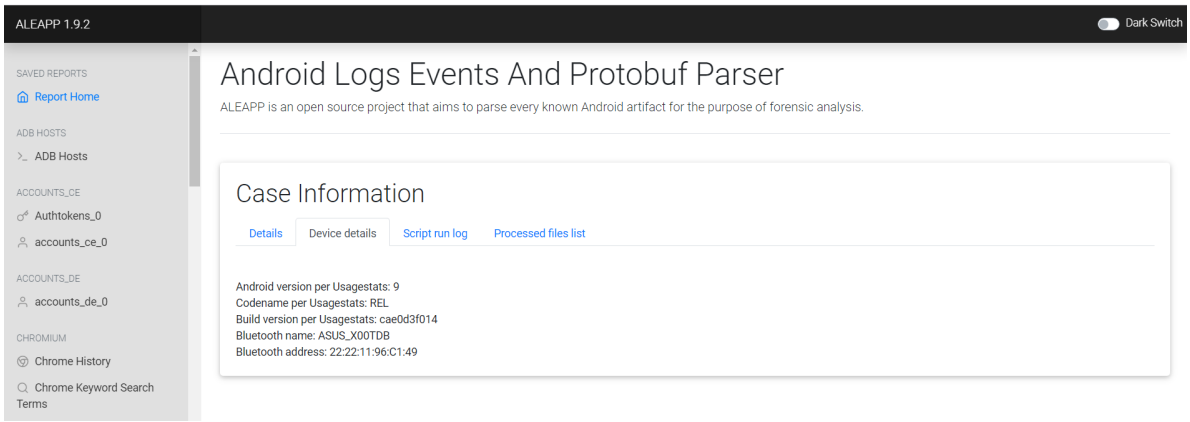
From this transactions and interactions we can determine that there was probably some form of illegal money transfer between two parties (i.e. the Boss paid the suspect for a job done).

General Phone Information

Using the generated aLEAPP report, we can also determine some information based on what was parsed by the aLEAPP engine.

OS and build

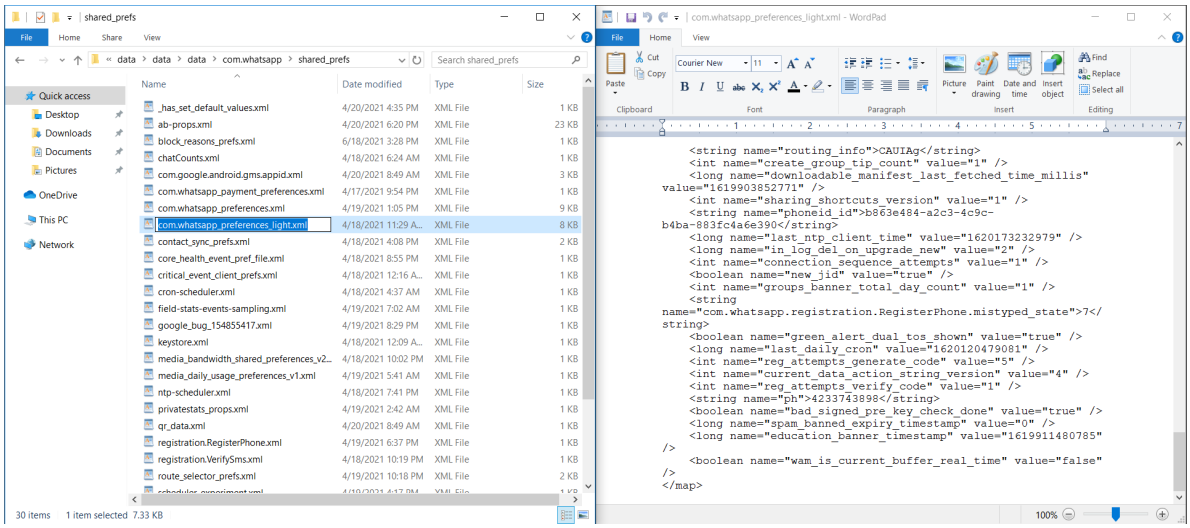




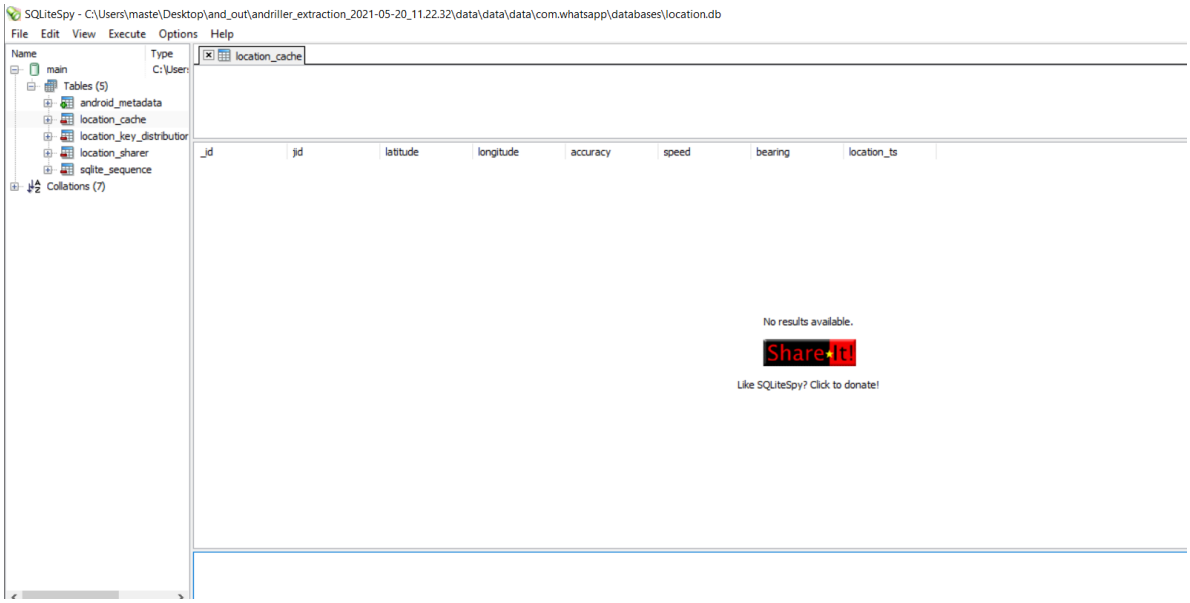
Based on the above information, we can determine that the phone is using Android 9 OS and its OEM is ASUS based on the Bluetooth name.We can also view the build version,

SQLite Spy and Editors

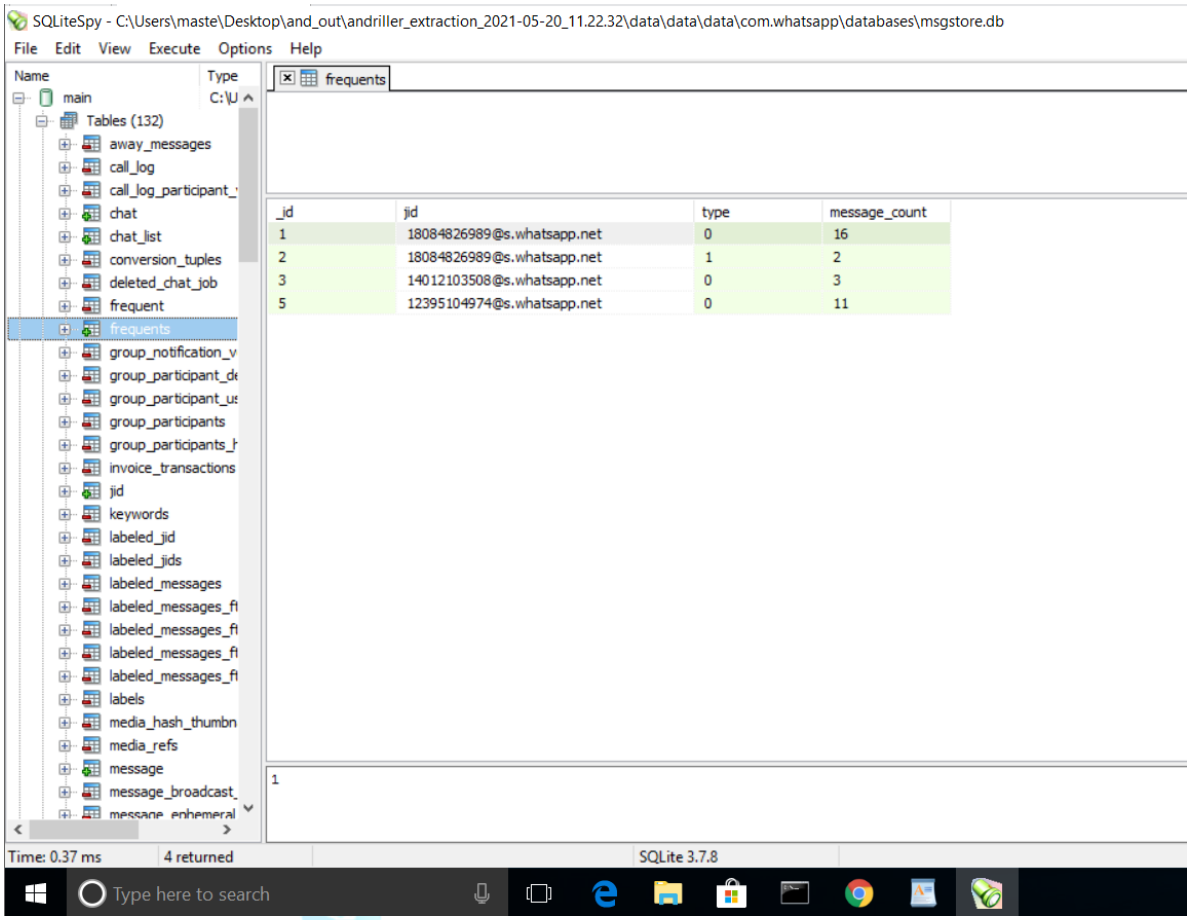
We are also able to extract the user's real name by parsing the xml file /data/data/com.whatsapp/shared_prefs/com.whatsapp_preferences_light.xml in a text editor of choice (in this case it is in the tag **push_name)**. Since **registration_biz_registered_on_device** is false, we can also conclude that the suspect uses the normal whatsapp application, not the corporate variant of Whatsapp for Business.



In trying to parse the location of the user using whatsapp, we were unable to recover any useful information.



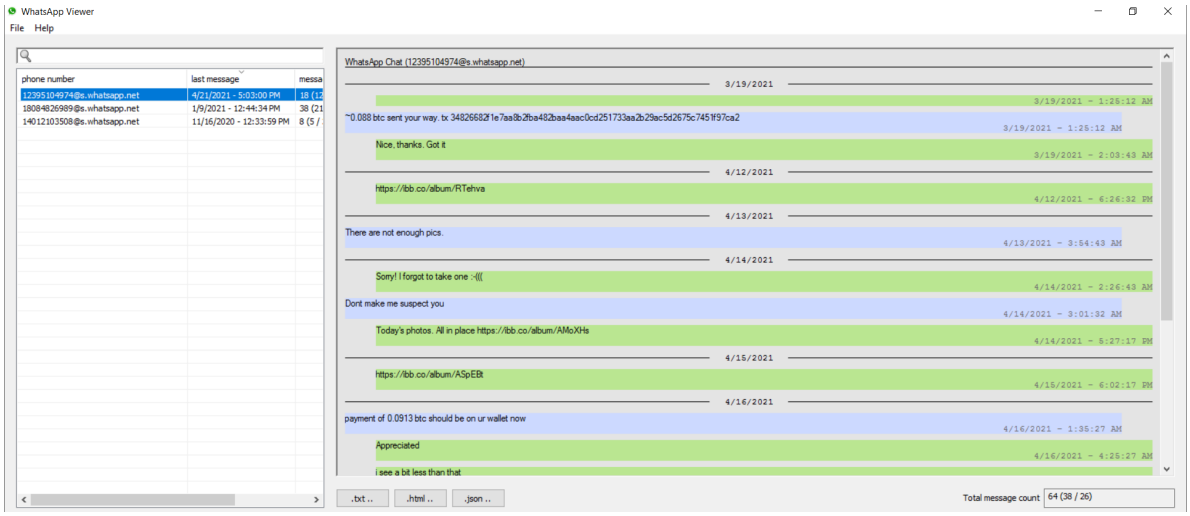
We are also able to view the frequent contacts of the suspect as shown below in the msgstore.db. The jid includes the mobile number of the contact (the format is a follows: “<contact_number>@s.whatsapp.net”



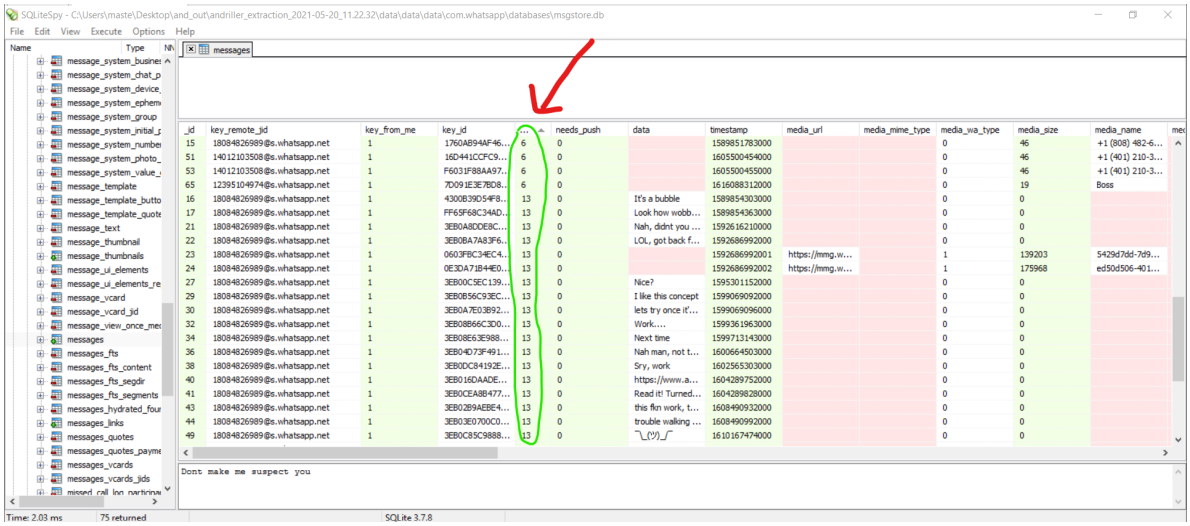
SECURING WITH AI

Since read receipts are turned on but the status of the messages cannot be seen in Whatsapp Viewer, we can obtain them by comparison when we open msgstore.db (could be tedious). Looking at the status column, we can cross check the following status codes with the messages (using the common WhatsApp forensic artifacts link in the Appendix).

'5'=received at the destination,
'6'=control message, '13'=message opened by the recipient (read)

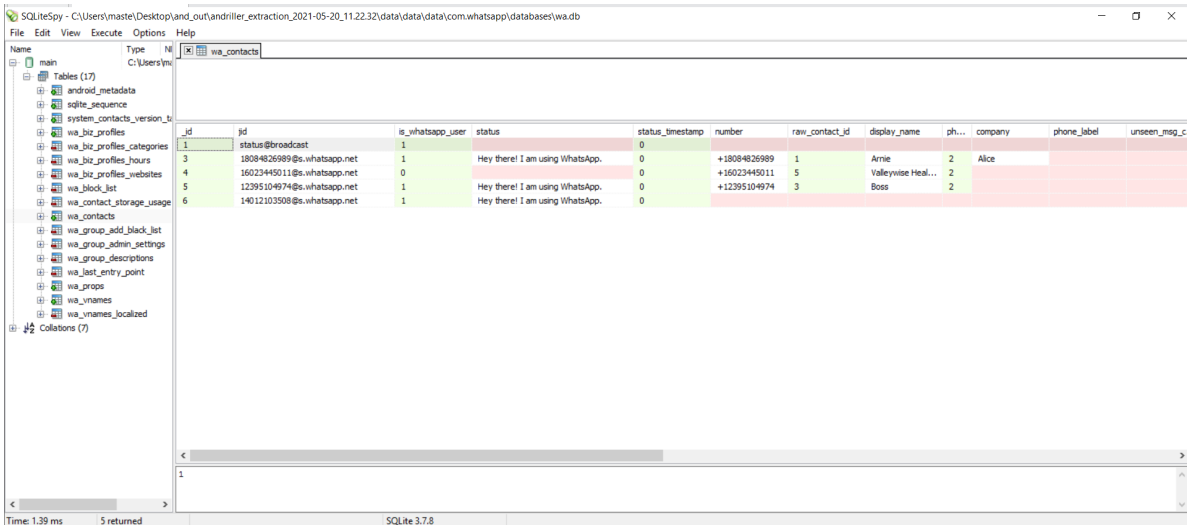


We can also counter check the messages sent in whatsapp viewer and the status codes as parsed by SQLiteSpy.



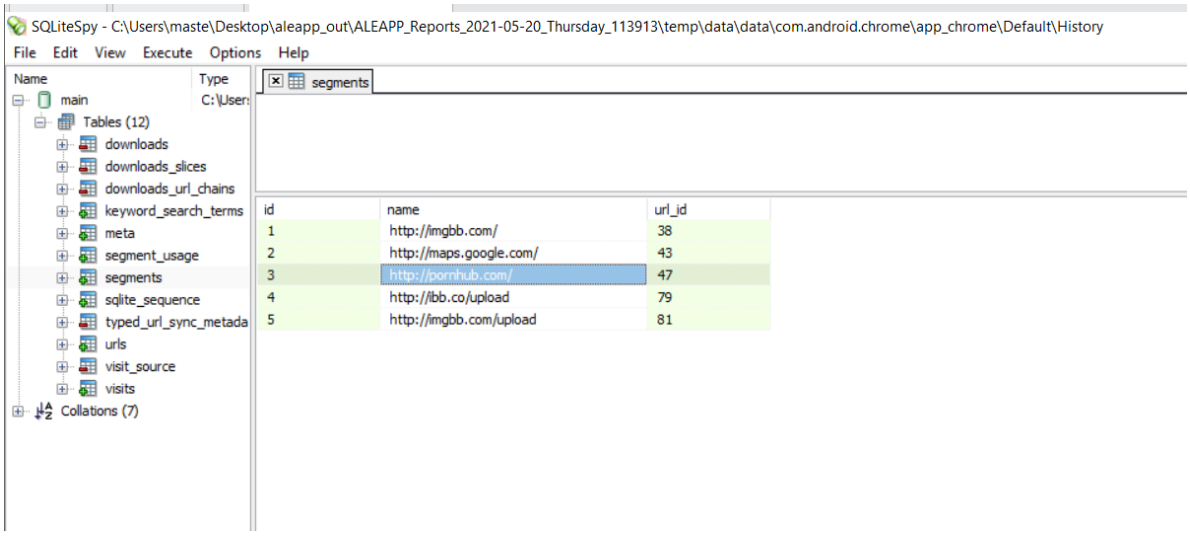
This is most likely useful if we want to determine if the user claims to be ignorant about a read message, since we have digital evidence to prove otherwise.

In wa.db, we can also find other evidences like the contact's names, order/position in the Whatsapp contact list, their status and Company Name if any (provided they use Whatsapp for business)

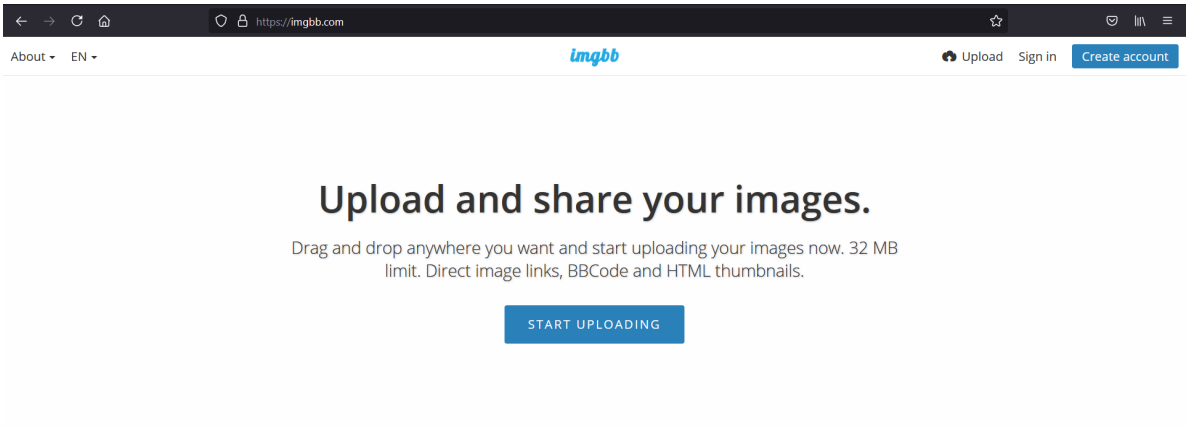


We were also able to extract his search history (what he typed using the keypad)

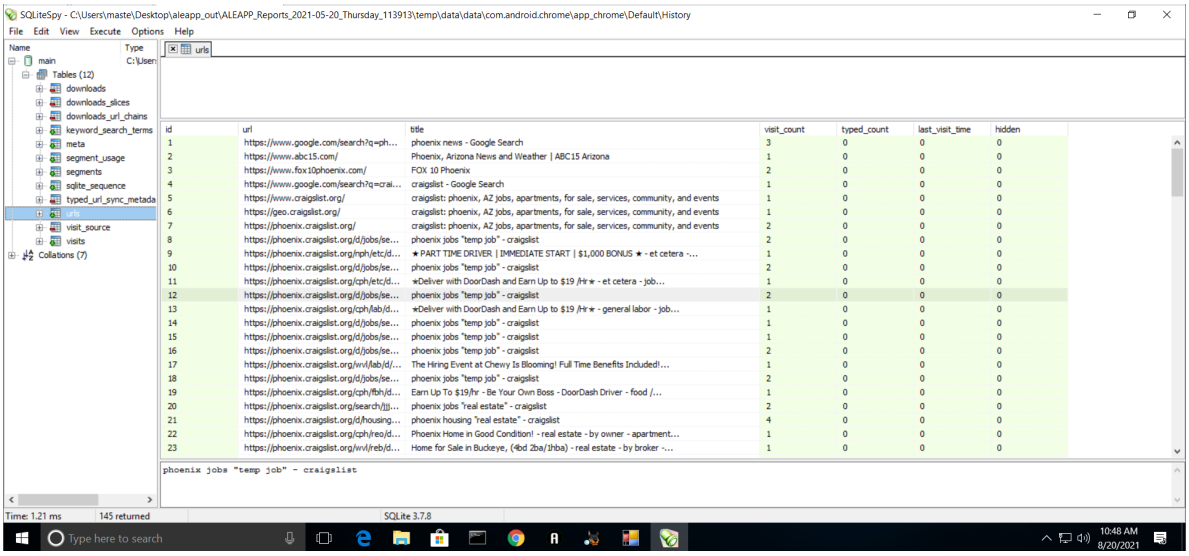
by navigating to C:\Users\maste\Desktop\aleapp_out\ALEAPP_Reports_2021-05-20_Thursday_113913\temp\data\data\com.android.chrome\app_chrome\Default and selecting the History file to be viewed with SQLiteSpy (under the segments SQLite table) in the mobile chrome browser.



The owner had used this free online image sharing software although the images were no longer available at time of the investigation (probably image upload service with deletion functionalities after a period of time).

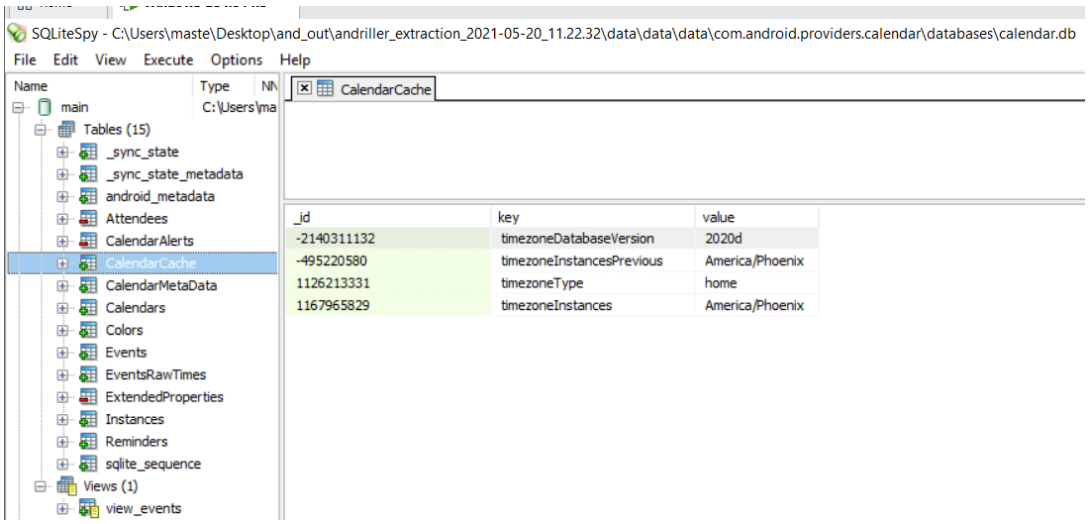


We can also view all the websites he visited with the title which helps to describe what the weblink may be about, to provide clues on his intent and activities, since web history reveals a lot about a person (similar to what was displayed in the ALEAPP report).

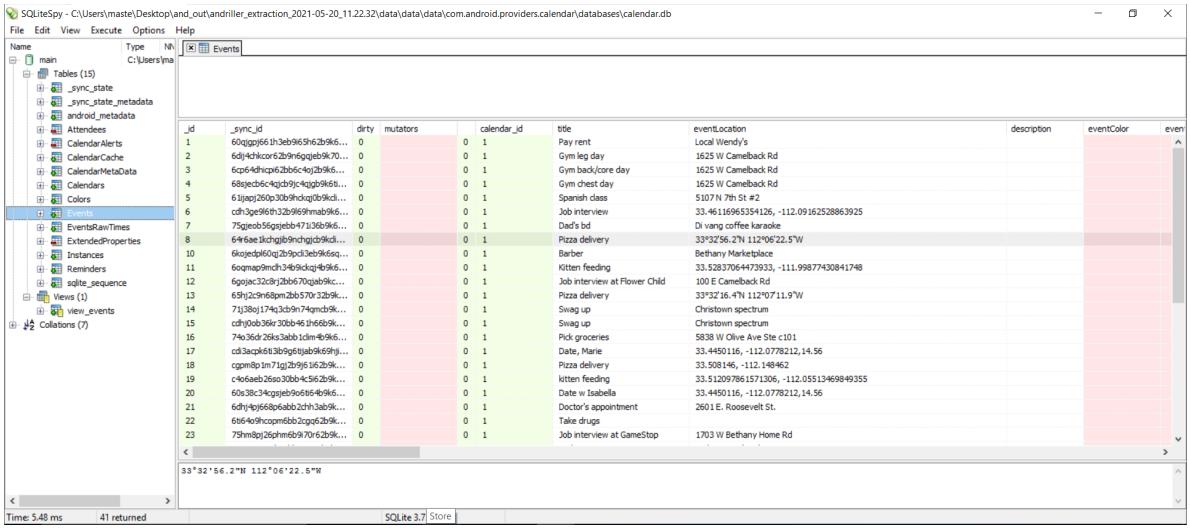


Calendar

Opening the calendar database in SQLiteSpy, we can determine the country and region the suspect is based in since the timezone is set to America/Phoenix.



In addition, we can also see the calendar schedule.

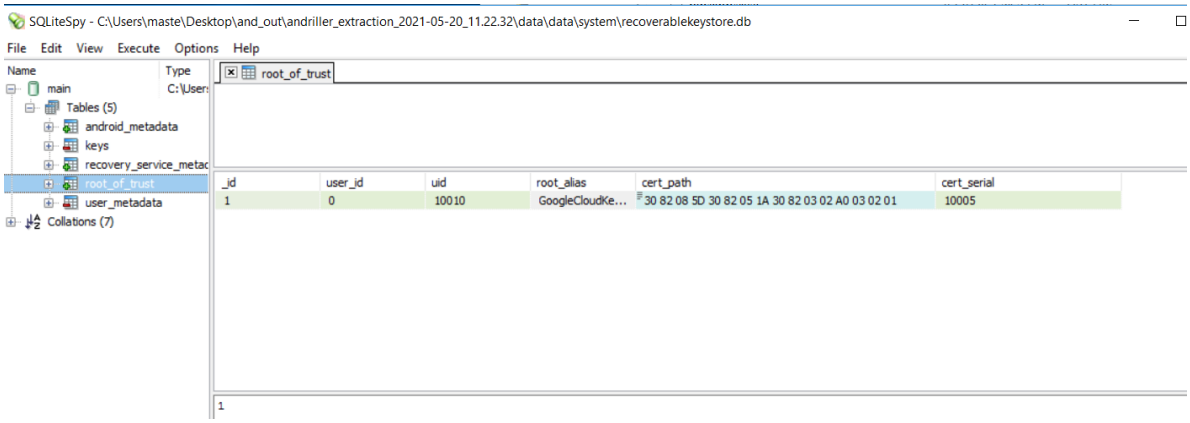


We can reorder the columns so that the GUI shows dtstart (datetime start) and dtend (datetime end) and then thereafter use a UTC time converter like the one below to determine the date and time of the event on the calendar:

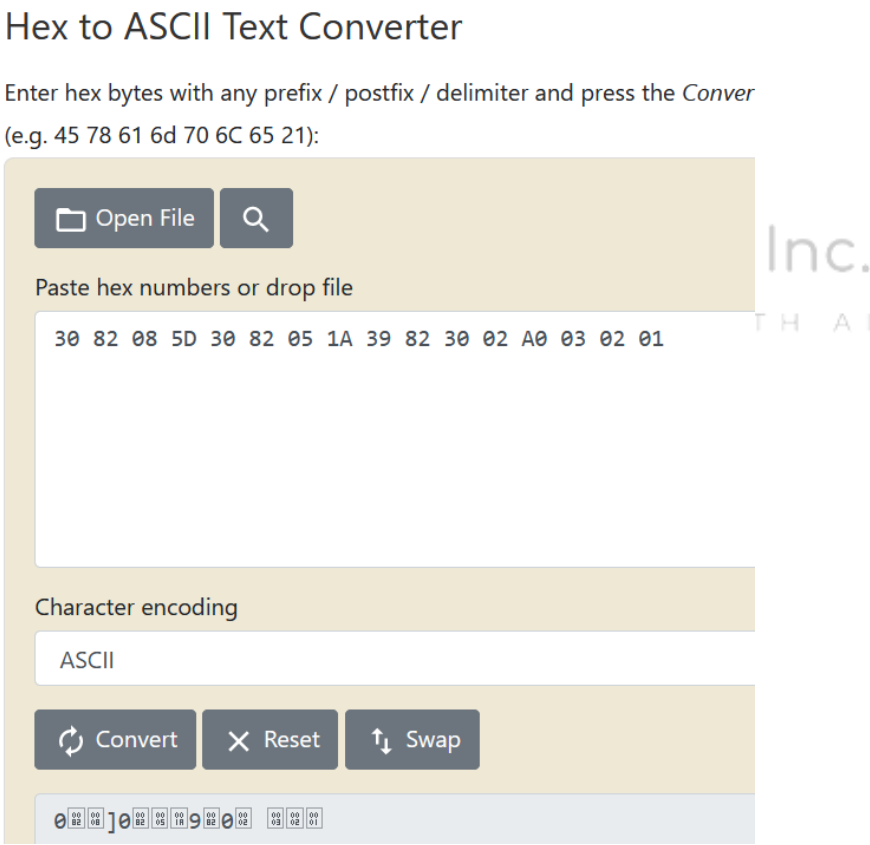
https://www.epochconverter.com/

This confirms our hypothesis based on the evidence which we processed through reverse search that he is likely to be residing in Phoenix.

However, this may be time consuming and a better option might be to use Belkasoft X as an alternative (recommended for this evidence), which has these features built in.

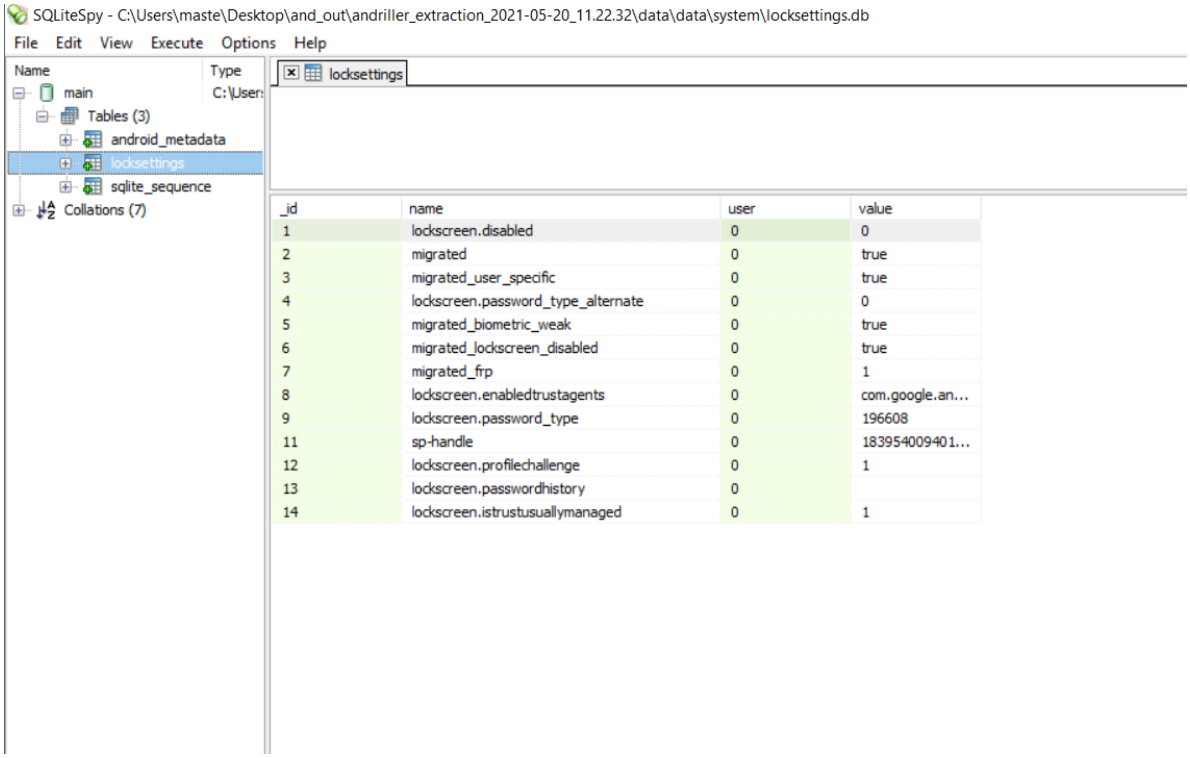


Based on the image above, under /data/system, we are able to view that the Google Cloud Key has indeed been activated with the certificate path included. However, no useful information is gathered when we try to convert this to ASCII text.



In addition, we also find important information in the same directory when the phone was imaged.

Open Source (Academic Usage)



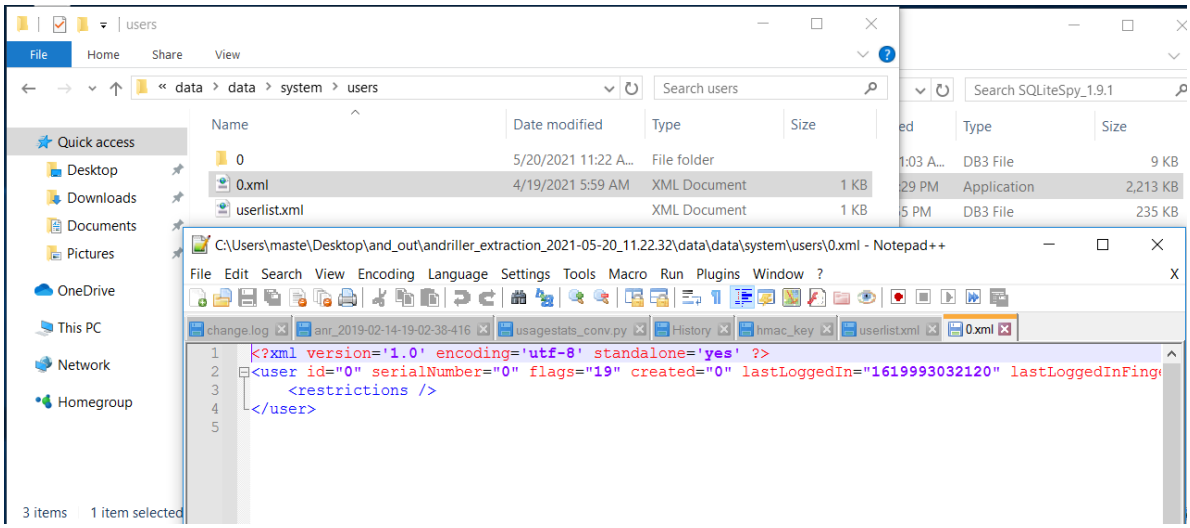
The data show that the lockscreen is enabled but with a weak migrated biometric lock. Referring to this article below and the password type, it is likely that a numeric password or pin was used (without repetition of numbers).

RyanNgCT Inc.

```
public enum LockTypeLevel
{
  SliderOrNone = 0,
  LowLevelBiometricSecurity = 32768, //implies technologies that can recognize the identity of an individual to about a 3 digit PIN (i.e. face)
  PatternPassword = 65536, //any type of password is assigned on the device (i.e. pattern)
  NumericPasswordBasic = 131072, //numeric password is assigned to the device
  NumericPasswordAdvanced = 196608, //numeric password with no repeating (4444) or ordered (1234,4321,2468,etc) sequences
  AlphabeticPassword = 262144, //alphabetic password
  AlphanumericPassword = 327680, //alphabetic and numeric password
  ComplexPassword = 393216 //alpabetic, numeric, and special character password
}
```

https://blog.mptolly.com/determining-the-type-of-security-lock-settings-on-an-android-device-in-xamarin/

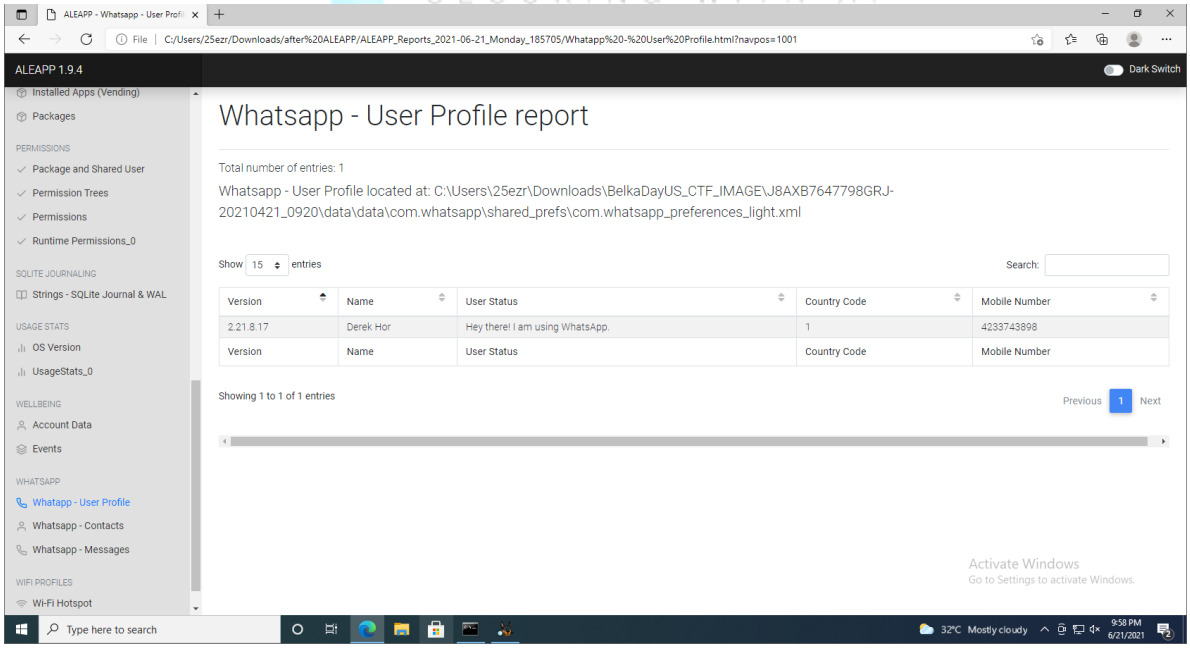
We can also determine the last time he logged into the phone using this information.



Examination of Artifacts using ALEAPP

Whatsapp

We discovered the Whatsapp User Profile using ALEAPP. The name of the suspect is Derek Hor and his mobile number is +1 4233743898. His Whatsapp version is 2.21.8.17.



We have also found Whatsapp messages which could be between the suspect and the boss, asking him to send images taken that day. All of the images were possibly uploaded through ibb.com as shown by the interaction and the links within the content in the image below.

Open Source (Academic Usage)

2021-03-19 01:25:12	2021-03-19 01:25:12	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	0	~0.088 btc sent your way. tx 34826682f1e7aa8b2fba482baa4aac0cd251733aa2b29ac5d2675c7451f97ca2	12395104974@s.whatsapp.net
2021-03-19 02:03:43	2021-03-19 02:03:43	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	Nice, thanks. Got it	12395104974@s.whatsapp.net
2021-04-12 18:26:32	2021-04-12 18:26:32	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	https://ibb.co/album/RTehva	12395104974@s.whatsapp.net
2021-04-13 03:54:43	2021-04-13 03:54:43	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	0	There are not enough pics.	12395104974@s.whatsapp.net
2021-04-14 02:26:43	2021-04-14 02:26:43	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	Sorry! I forgot to take one :-(((	12395104974@s.whatsapp.net
2021-04-14 03:01:32	2021-04-14 03:01:32	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	0	Dont make me suspect you	12395104974@s.whatsapp.net
2021-04-14 17:27:17	2021-04-14 17:27:17	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	Today's photos. All in place https://ibb.co/album/AMoXHs	12395104974@s.whatsapp.net
2021-04-15 18:02:17	2021-04-15 18:02:17	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	https://ibb.co/album/ASpEBt	12395104974@s.whatsapp.net
2021-04-16 01:35:27	2021-04-16 01:35:27	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	0	payment of 0.0913 btc should be on ur wallet now	12395104974@s.whatsapp.net
2021-04-16 04:25:27	2021-04-16 04:25:27	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	Appreciated	12395104974@s.whatsapp.net
2021-04-16 04:28:27	2021-04-16 04:28:27	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	i see a bit less than that	12395104974@s.whatsapp.net
2021-04-16 04:28:33	2021-04-16 04:28:33	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	intended?	12395104974@s.whatsapp.net
2021-04-16 04:52:43	2021-04-16 04:52:43	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	0	yes.	12395104974@s.whatsapp.net
2021-04-16 18:35:30	2021-04-16 18:35:30	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	https://ibb.co/album/YOvt6f	12395104974@s.whatsapp.net
2021-04-17 19:15:00	2021-04-17 19:15:00	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	https://ibb.co/album/RKntdG	12395104974@s.whatsapp.net
2021-04-18 19:11:34	2021-04-18 19:11:34	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	1	https://ibb.co/album/rvD0OF	12395104974@s.whatsapp.net
2021-04-21 17:03:00	2021-04-21 17:03:00	12395104974@s.whatsapp.net	12395104974@s.whatsapp.net	0	says Not found, upload pics again	12395104974@s.whatsapp.net
Send Timestamp	Received Timestamp	Message ID	Recipients	Direction	Content	Group Sender

Activate
Go to Sett

Google Chrome History

RyanNoCT Inc
SECURING WITH AI

We are unable to tell the order of events as the date and time of the restored search history was somewhat corrupted or not picked up well when parsing. However, we assumed that the Google Maps search history had to be the last one to be searched as the suspect was caught and arrested for drug charges.

Craigslist / Jobs / Housing

Least recently, he was searching Craigslist for housing and jobs.

1601-01-01 00:00:00	https://www.craigslist.org/	craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	1
1601-01-01 00:00:00	https://geo.craigslist.org/	craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/	craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	2
1601-01-01 00:00:00	https://phoenix.craigslist.org/d/jobs/search/jjj?query=temp%20job&sort=rel	phoenix jobs "temp job" - craigslist	2
1601-01-01 00:00:00	https://phoenix.craigslist.org/nph/etc/d/phoenix-part-time-driver-immediate/7314484634.html	★ PART TIME DRIVER	IMMEDIATE START	$1,000 BONUS ★ - et cetera -...	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/d/jobs/search/jjj?s=120&query=temp%20job&sort=rel	phoenix jobs "temp job" - craigslist	2
1601-01-01 00:00:00	https://phoenix.craigslist.org/cph/etc/d/phoenix-deliver-with-doordash-and-earn/7314006988.html	★Deliver with DoorDash and Earn Up to $19 /Hr★ - et cetera - job...	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/d/jobs/search/jjj?s=240&query=temp%20job&sort=rel	phoenix jobs "temp job" - craigslist	2
1601-01-01 00:00:00	https://phoenix.craigslist.org/cph/lab/d/phoenix-deliver-with-doordash-and-earn/7311241557.html	★Deliver with DoorDash and Earn Up to $19 /Hr★ - general labor - job...	1

Open Source (Academic Usage)

1601-01-01 00:00:00	https://phoenix.craigslist.org/d/jobs/search/jjj?s=480&query=temp%20job&sort=rel	phoenix jobs "temp job" - craigslist	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/d/jobs/search/jjj?s=600&query=temp%20job&sort=rel	phoenix jobs "temp job" - craigslist	2
1601-01-01 00:00:00	https://phoenix.craigslist.org/wvl/lab/d/goodyear-the-hiring-event-at-chewy-is/7306911572.html	The Hiring Event at Chewy Is Blooming! Full Time Benefits Included!...	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/d/jobs/search/jjj?s=720&query=temp%20job&sort=rel	phoenix jobs "temp job" - craigslist	2
1601-01-01 00:00:00	https://phoenix.craigslist.org/cph/fbh/d/phoenix-earn-up-to-19-hr-be-your-own/7306035666.html	Earn Up To $19/hr - Be Your Own Boss - DoorDash Driver - food /...	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/search/jjj?query=real+estate&sort=rel	phoenix jobs "real estate" - craigslist	2
1601-01-01 00:00:00	https://phoenix.craigslist.org/d/housing/search/hhh?query=real%20estate&sort=rel	phoenix housing "real estate" - craigslist	4
1601-01-01 00:00:00	https://phoenix.craigslist.org/cph/reo/d/phoenix-phoenix-home-in-good-condition/7316513953.html	Phoenix Home in Good Condition! - real estate - by owner - apartment...	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/wvl/reb/d/home-for-sale-in-buckeye-4bd-2ba-1hba/7314124792.html	Home for Sale in Buckeye, (4bd 2ba/1hba) - real estate - by broker -...	1
1601-01-01 00:00:00	https://phoenix.craigslist.org/cph/reb/d/phoenix-home-for-sale-in-phoenix/7316507468.html	Home for sale in Phoenix - real estate - by broker - apartment real...	1

Knee Pain / Clinic

At one point in time, he was searching for clinics in Phoenix, AZ. It was specifically for his knee. It can be assumed that he suffered an injury on the knee.

RyanNoCT Inc
SECURING WITH AI

1601-01-01 00:00:00	https://www.google.com/search?q=my+knee+hurts&ei=faKQYKLqOZXa9AOr1rrYCw&oq=my+knee+&gs_lcp=ChNtb2Jpb GUtZ3dzLXdpei1zZXJwEAEYADIFCAAQsQMyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAOgQIABBDOgQILhBDOgsILhCxAxDHA RCjAjoGCAAQBxAeOgUILhCxAzoCCC46BwguELEDEENQnxlY8CZg5TJoAHAAeACAAaACiAGEEJIBAzItOJgBAKABAcABAQ&sclien t=mobile-gws-wiz-serp	my knee hurts - Google Search	4
1601-01-01 00:00:00	https://www.mayoclinic.org/diseases-conditions/knee-pain/symptoms-causes/syc-20350849	Knee pain - Symptoms and causes - Mayo Clinic	1
1601-01-01 00:00:00	https://www.google.com/search?q=my+knee+hurts&ei=faKQYKLqOZXa9AOr1rrYCw&oq=my+knee+&gs_lcp=ChNtb2Jpb GUtZ3dzLXdpei1zZXJwEAEYADIFCAAQsQMyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAOgQIABBDOgQILhBDOgsILhCxAxDHA RCjAjoGCAAQBxAeOgUILhCxAzoCCC46BwguELEDEENQnxlY8CZg5TJoAHAAeACAAaACiAGEEJIBAzItOJgBAKABAcABAQ&sclien t=mobile-gws-wiz-serp#sbfbu=1&pi=my%20knee%20hurts	my knee hurts - Google Search	1
1601-01-01 00:00:00	https://www.google.com/search?q=knee+clinic+phoenix&ei=hqKQYJ6pJcTU9APXlamgCA&oq=knee+clinic+phoenix &gs_lcp=ChNtb2JpbGUtZ3dzLXdpei1zZXJwEAMyBQghEKABMgUIIRCgATIFCCEQqwI6BAgAEEc6BQgpELEDOgIIKTolCAAQ6gIQ jwE6BAgAEEM6AggAOgsILhCxAxDHARCjAjoFCAAQkQI6BQgAELEDOggILhCxAxCDATobECAAQCjoFCAAQyQM6CAguEMcBEK8BOgcI ABDJAxANOgQIABANOgoILhDHARCvARANOgsILhDHARCvARCTAjoGCAAQFhAeOgkIABDJAxAWEB46BwghEAoQoAE6CAghEBYQHRAe OggIABAIEA0QHjoFCAAQhgNQkRZY7Y8BYKGTAWgGcAF4AIAB2gKIAYg0kgEGMi0xNS44mAEAoAEBsAESyAEIwAEB&sclient=mob ile-gws-wiz-serp	knee clinic phoenix - Google Search	2

Team_dadroid_2021_NP_CSF

1601-01-01 00:00:00	https://www.google.com/search?q=knee+clinic+phoenix&ei=hqKQYJ6pJcTU9APXlamgCA&oq=knee+clinic+phoenix&gs_lcp=ChNtb2JpbGUtZ3dzLXdpei1zZXJwEAMyBQghEKABMgUIIRCgATIFCCEQqwI6BAgAEEc6BQgpELEDOgIIKToICAAQ6gIQjwE6BAgAEEM6AggAOgsILhCxAxDHARCjAjoFCAAQkQI6BQgAELEDOggILhCxAxCDAToECAAQCjoFCAAQyQM6CAguEMcBEK8BOgcIABDJAxANOgQIABANOgoILhDHARCvARANOgsILhDHARCvARCTAjoGCAAQFhAeOgkIABDJAxAWEB46BwghEAoQoAE6CAghEBYQHRAeOggIABAIEA0QHjoFCAAQhgNQkRZY7Y8BYKGTAWgGcAF4AIAB2gKIAYg0kgEGMi0xNS44mAEAoAEBsAESyAEIwAEB&sclient=mobile-gws-wiz-serp#ip=1	knee clinic phoenix - Google Search	4
1601-01-01 00:00:00	https://www.mayoclinic.org/biographies/spangehl-mark-j-m-d/bio-20054096	Mark J. Spangehl, M.D. - Doctors and Medical Staff - Mayo Clinic	1
1601-01-01 00:00:00	https://www.cucchettiorthopedics.com/	Brad A. Cucchetti, DO: Orthopedic Surgeon Phoenix, AZ	1
1601-01-01 00:00:00	https://www.google.com/search?q=knee+clinic+phoenix&ei=hqKQYJ6pJcTU9APXlamgCA&oq=knee+clinic+phoenix&gs_lcp=ChNtb2JpbGUtZ3dzLXdpei1zZXJwEAMyBQghEKABMgUIIRCgATIFCCEQqwI6BAgAEEc6BQgpELEDOgIIKToICAAQ6gIQjwE6BAgAEEM6AggAOgsILhCxAxDHARCjAjoFCAAQkQI6BQgAELEDOggILhCxAxCDAToECAAQCjoFCAAQyQM6CAguEMcBEK8BOgcIABDJAxANOgQIABANOgoILhDHARCvARANOgsILhDHARCvARCTAjoGCAAQFhAeOgkIABDJAxAWEB46BwghEAoQoAE6CAghEBYQHRAeOggIABAIEA0QHjoFCAAQhgNQkRZY7Y8BYKGTAWgGcAF4AIAB2gKIAYg0kgEGMi0xNS44mAEAoAEBsAESyAEIwAEB&sclient=mobile-gws-wiz-serp#ip=1&sbfbu=1&pi=knee%20clinic%20phoenix	knee clinic phoenix - Google Search	1
1601-01-01 00:00:00	https://www.google.com/search?q=phoenix+clinic&ei=p6KQYJ27BZnI0PEPj-GksAw&oq=phoenix+cli&gs_lcp=ChNtb2JpbGUtZ3dzLXdpei1zZXJwEAEYADIFCAAQkQIyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAOgQIABBHOgIIKToFCCkQsQM6CAgAEOoCEI8BOggILhCRAhCTAjoIEC4QxwEQowI6CwguELEDEMcBEKMCOgQIABBDOgUIABCxAzoEEC4QQzoHCAAQsQMQzoFCC4QsQM6CwguELEDEJECEJMCOggIABCxAxDJAzoFCAAQkgM6CgguELEDEMcBEK8BOgIILjoOEC4QsQMQxwEQrwEQkQI6DggueLEDEIMBEMcBEK8BUI1QWOZfYKZnaAJwAXgAgAHLAogBxxmSAQUyLTcuNJgBAKABAbABE8gBCMABAQ&sclient=mobile-gws-wiz-serp	phoenix clinic - Google Search	4
1601-01-01 00:00:00	https://thecoreinstitute.com/location/north-phoenix-clinic/	North Phoenix Clinic | Phoenix, AZ | The CORE Institute	1
1601-01-01 00:00:00	https://valleywisehealth.org/locations/comprehensive-health-center-phoenix/	Valleywise Comprehensive Health Center - Phoenix - Valleywise Health	1

ImgBB.com

It is mainly used for free image hosting and sharing service, upload pictures and photos. This website can be found numerous times by the suspect as seen in the Google Chrome history below. As this is a drug case, these images could possibly be the images of evidence of the drugs being delivered or has been prepared. I have tried to access the website to obtain the images, but none of the links are valid as we suspect that the images have been taken down.

1601-01-01 00:00:00	http://imgbb.com/	ImgBB — Upload Image — Free Image Hosting	1
1601-01-01 00:00:00	https://imgbb.com/	ImgBB — Upload Image — Free Image Hosting	2
1601-01-01 00:00:00	https://imgbb.com/login	Sign in — ImgBB	1
1601-01-01 00:00:00	https://imgbb.com/#google_vignette	Horatio420 (horatio420) — ImgBB	1
1601-01-01 00:00:00	https://horatio420.imgbb.com/	Horatio420 (horatio420) — ImgBB	2
1601-01-01 00:00:00	https://ibb.co/album/RTehva	12 — ImgBB	2
1601-01-01 00:00:00	https://imgbb.com/upload	Upload your images	8
1601-01-01 00:00:00	https://ibb.co/LZTgT2s	IMG-20210412-020201 — ImgBB	2
1601-01-01 00:00:00	https://ibb.co/R7XrPjN	IMG-20210412-030418 — ImgBB	2

1601-01-01 00:00:00	https://horatio420.imgbb.com/albums	Horatio420 (horatio420) — ImgBB	7
1601-01-01 00:00:00	https://ibb.co/album/AMoXHs	14 — ImgBB	2
1601-01-01 00:00:00	https://ibb.co/4pgZzS2	IMG-20210414-005550 — ImgBB	2
1601-01-01 00:00:00	https://ibb.co/Y02ZVgt	IMG-20210414-014208 — ImgBB	2
1601-01-01 00:00:00	https://ibb.co/album/ASpEBt	15 — ImgBB	2
1601-01-01 00:00:00	https://ibb.co/L03WFGh	IMG-20210415-015329 — ImgBB	2

By using the Chrome Network Action Predictor Report, we are able to tell that the person was in contact and has been using the Img.bb platform to send and presumably receive images from Horatio. The evidence gathered can be seen below.

Total number of entries: 120

Chrome Network Action Predictor located at: C:\Users\25ezr\Downloads\BelkaDayUS_CTF_IMAGE\J8AXB7647798GRJ-20210421_0920\data\data\com.android.chrome\app_chrome\Default\Network Action Predictor

Show All entries Search: ho

User Text	URL	Number of Hits	Number of Misses
i	https://horatio420.imgbb.com/	0	2
ib	https://horatio420.imgbb.com/	0	1
ibb	https://horatio420.imgbb.com/	0	1
ibb.	https://horatio420.imgbb.com/	0	1
im	https://horatio420.imgbb.com/	0	1
img	https://horatio420.imgbb.com/	0	1
imgbb.com	https://horatio420.imgbb.com/	0	1
imgbb.com/	https://horatio420.imgbb.com/	0	1
User Text	URL	Number of Hits	Number of Misses

Google Maps

There are many web history contents, mostly involving Google Maps such as the ones shown below. The images could possibly serve as evidence that he was a delivery driver of some sort. Many of the locations are mainly situated in Phoenix, Arizona, which we can presume is to be the area he is situated at.

1601-01-01 00:00:00	https://www.google.com/maps/place/Sugar+Sweet+Bakery+Company,+2007+W+Bethany+Home+Rd,+Phoenix,+AZ+85015/@33.5237564,-112.1024752,17z/data=!4m2!3m1!1s0x872b6d94fe06ba2d:0x248453ff6ed539ad	Christown Spectrum - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Christown+Spectrum,+1607+W+Bethany+Home+Rd,+Phoenix,+AZ+85015/@33.521846,-112.095291,17z/data=!4m2!3m1!1s0x872b13f49a3cd2b1:0x2cf437234cbae56e	Phở 602 - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Ph%E1%BB%9F+602,+6135+N+35th+Ave+UNIT+121,+Phoenix,+AZ+85017/@33.5255115,-112.1304472,17z/data=!4m2!3m1!1s0x872b6cb1dd67c699:0xb71e7ae552b6e304	546 W Southern Hills Rd - Google Maps	2
1601-01-01 00:00:00	https://www.google.com/maps/place/Walgreens,+4249+W+Glendale+Ave,+Phoenix,+AZ+85051/@33.5379144,-112.1508397,17z/data=!4m2!3m1!1s0x872b6b671c4bbac3:0x8540b32be7180462	Bakery Arizona - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Bakery+Arizona,+2647+W+Glendale+Ave,+Phoenix,+AZ+85051/@33.5377414,-112.1158806,17z/data=!4m2!3m1!1s0x872b6cc11fdfa553:0xf41e74c4c311017d	Bakery Arizona - Google Maps	2
1601-01-01 00:00:00	https://www.google.com/maps/place/Bakery+Arizona,+2647+W+Glendale+Ave,+Phoenix,+AZ+85051/@33.5378198,-112.1157363,17z/data=!4m2!3m1!1s0x872b6cc11fdfa553:0xf41e74c4c311017d	Redbox, West Bethany Home Road, Glendale, AZ - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/search/Redbox,+West+Bethany+Home+Road,+Glendale,+AZ/@33.5378198,-112.115 7363,13z	OZ Bar - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/OZ+Bar,+1804+W+Bethany+Home+Rd,+Phoenix,+AZ+85015/@33.52452,-112.09845,17z/data=!4m2!3m1!1s0x872b132b2ace7cab:0x3dcd8797e1cb658f	Stinkweeds Record Store - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Stinkweeds+Record+Store,+12+W+Camelback+Rd,+Phoenix,+AZ+85013/@33.5095482,-112.0746469,17z/data=!4m2!3m1!1s0x872b12c04c782a29:0x468f84b0e20be28e	Christian Life Church - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Christian+Life+Church,+3946+W+McDowell+Rd,+Phoenix,+AZ+85009/@33.4664504,-112.1450457,17z/data=!4m2!3m1!1s0x872b1478e9a7d7f9:0xf9c0bba9c83e4842	Jiffy Lube - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Jiffy+Lube,+1645+N+51st+Ave,+Phoenix,+AZ+85035/@33.4677439,-112.1687751,17z/data=!4m2!3m1!1s0x872b145f915475b9:0xcaea7b566004963e	Super gasoline - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Super+gasoline,+5835+N+27th+Ave,+Phoenix,+AZ+85017/@33.5238266,-112.1166176,17z/data=!4m2!3m1!1s0x872b6ccba9a5f0b9:0x4a784537d2ce36ba	Beer, Wine, Smoke, Liquor - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Beer,+Wine,+Smoke,+Liquor,+6024+N+23rd+Ave,+Phoenix,+AZ+85015/@33.5249335,-112.1086966,17z/data=!4m2!3m1!1s0x872b6db663cc7a43:0xb6c21c31dc506d70	Clean Freak - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Clean+Freak,+2942+N+16th+St,+Phoenix,+AZ+85016/@33.4814487,-112.0480096,17z/data=!4m2!3m1!1s0x872b1330ae958e97:0x75838eae2f82c062	Desert Financial Credit Union - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Desert+Financial+Credit+Union,+1630+E+Camelback+Rd+Ste.+110,+Phoenix,+AZ+85016/@33.5104039,-112.0470312,17z/data=!4m2!3m1!1s0x872b0d602db80c1b:0x781145b0bb60cf9b	Exclusive Automotive Diagnostic - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Exclusive+Automotive+Diagnostic,+7011+N+19th+Ave,+Phoenix,+AZ+85021/@33.539081,-112.099179,17z/data=!4m2!3m1!1s0x872b7530dae557b7:0x5bd311825587be0d	Club Silverado - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Club+Silverado,+6108+N+27th+Ave,+Phoenix,+AZ+85017/@33.5254477,-112.1174988,17z/data=!4m2!3m1!1s0x872b6cca3c951bf9:0xa850a346d6f702e8	AiNT NICKS TAVERN - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/AiNT+NICKS+TAVERN,+6840+N+27th+Ave,+Phoenix,+AZ+85017/@33.537987,-112.1171128,17z/data=!4m2!3m1!1s0x872b6cc72fd82455:0x4d091c37c71a38c3	Google Maps	3

Google Keep - Notes Report

In this report, we can see the date and time of the notes creation, which is earliest on top and latest changes at the bottom. It shows that Horatio created the notes and was the last editor of it. It also confirms that the knee pain was due to the job he took up in Phoenix, Arizona as he has pain relief cream written in his notes.

Google Keep - Notes report

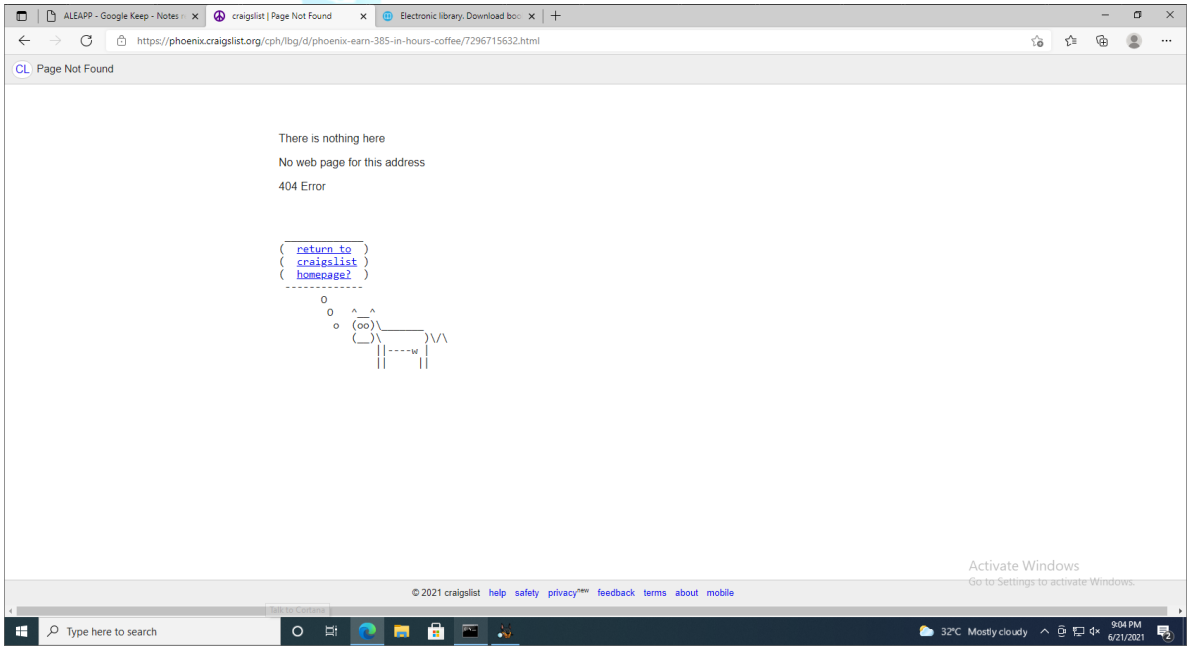
Total number of entries: 6

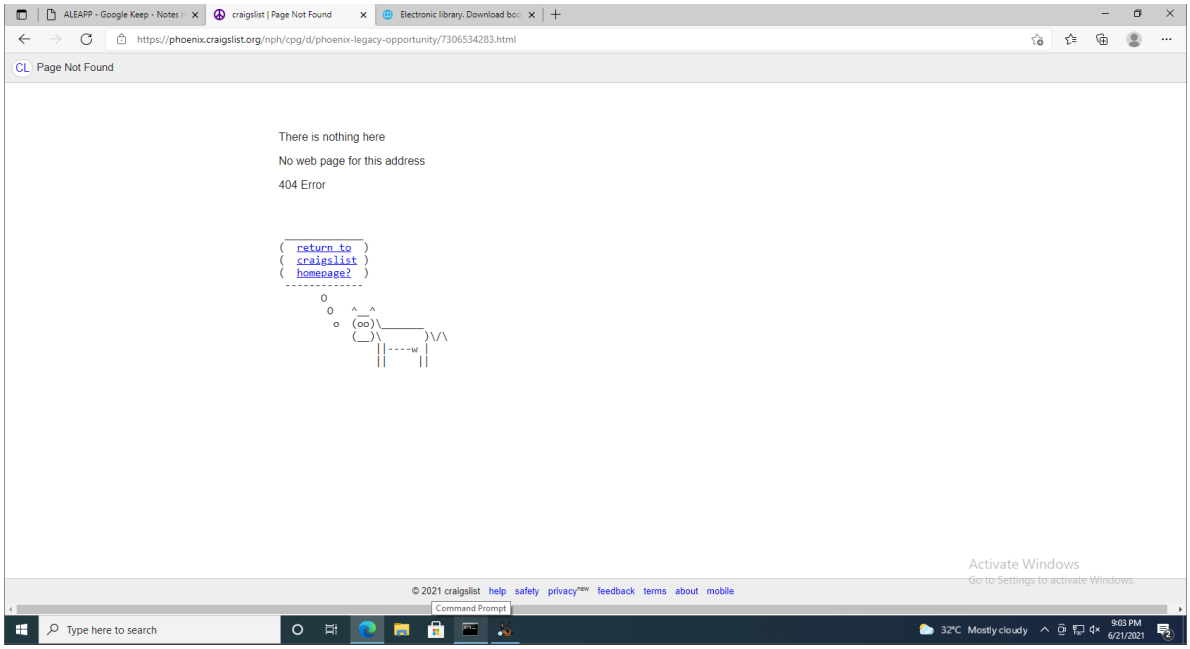
Google Keep - Notes located at: C:\Users\25ezr\Downloads\BelkaDayUS_CTF_IMAGE\J8AXB7647798GRJ-20210421_0920\data\data\com.google.android.keep\databases\keep.db

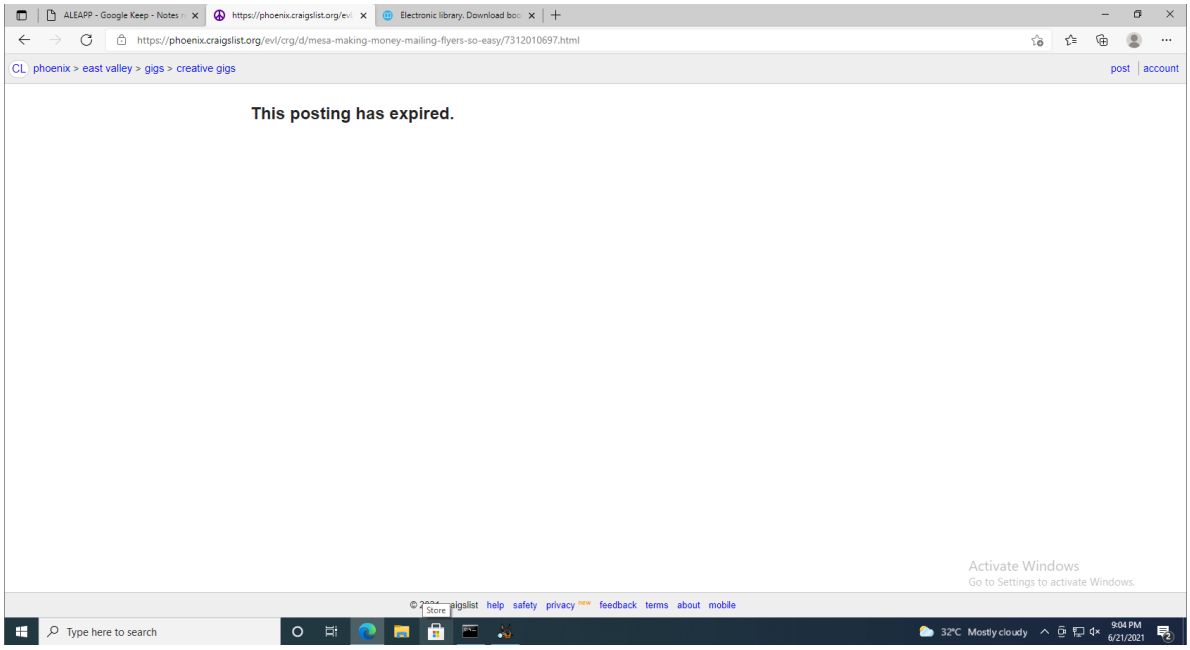
Show 15 entries Search:

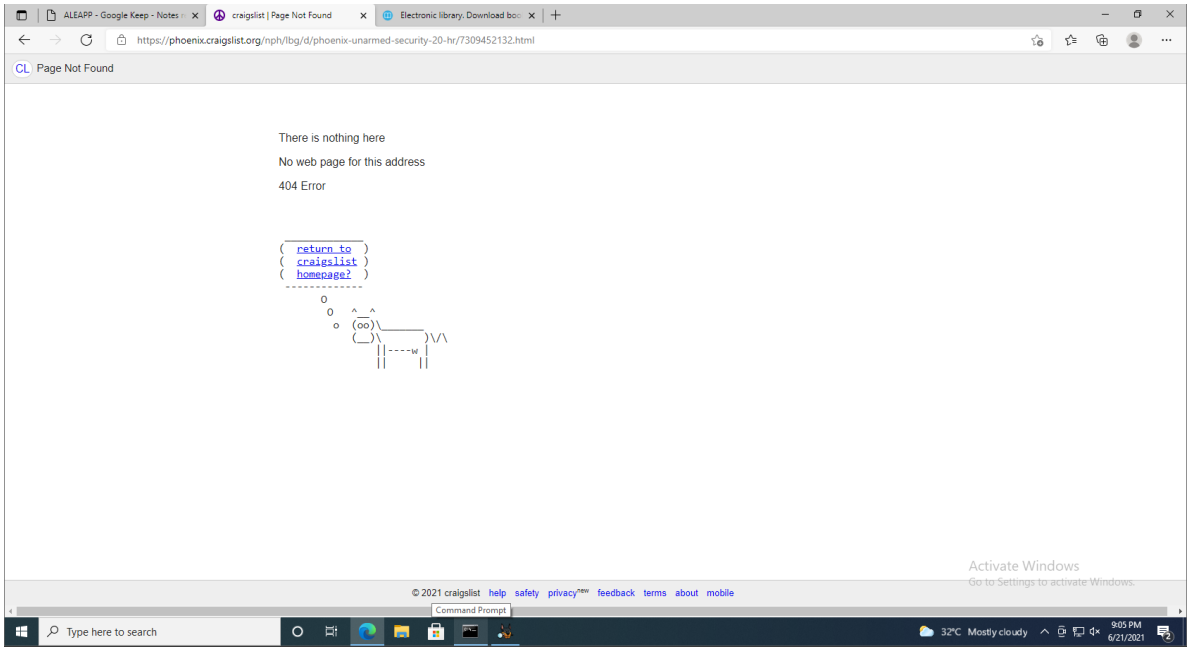
Notes Creation Time	Notes Last Modified Time	List Parent ID	Creator Email	Title	Text	Synced Text	Is deleted	Last Modifier Email
2020-11-18 18:25:05	2020-11-18 18:25:54	6	horatio0.42k@gmail.com	Side hustle	https://phoenix.craigslist.org/cph/lbg/d/phoenix-earn-385-in-hours-coffee/7296715632.html - $400 in 2 hours. drugs again? https://phoenix.craigslist.org/nph/cpg/d/phoenix-legacy-opportunity/7306534283.html - wtf?? https://phoenix.craigslist.org/evl/crg/d/mesa-making-money-mailing-flyers-so-easy/7312010697.html - easy but low paid https://phoenix.craigslist.org/nph/lbg/d/phoenix-unarmed-security-20-hr/7309452132.html - night job	https://phoenix.craigslist.org/cph/lbg/d/phoenix-earn-385-in-hours-coffee/7296715632.html - $400 in 2 hours. drugs again? https://phoenix.craigslist.org/nph/cpg/d/phoenix-legacy-opportunity/7306534283.html - wtf?? https://phoenix.craigslist.org/evl/crg/d/mesa-making-money-mailing-flyers-so-easy/7312010697.html - easy but low paid https://phoenix.craigslist.org/nph/lbg/d/phoenix-unarmed-security-20-hr/7309452132.html - night job	False	horatio0.42k@gmail.com
2020-12-17 07:57:13	2020-12-17 07:57:13	1	horatio0.42k@gmail.com		04049 19810 47697 72485 91554 88046	04049 19810 47697 72485 91554 88046	False	horatio0.42k@gmail.com
2020-12-24 04:46:05	2020-12-24 04:47:58	5	horatio0.42k@gmail.com	Drugs	Chondrotin Sulfate 600mg - 2 per day PERCUTANE Pain Relief Cream - evening	Chondrotin Sulfate 600mg - 2 per day PERCUTANE Pain Relief Cream - evening	False	horatio0.42k@gmail.com
2021-01-12 11:54:49	2021-01-12 11:54:49	3	horatio0.42k@gmail.com	Secrets	?62l-=NBhKYUL_&7J'K7Dx2 P'J=#HxUNT_^TTJWu$X4'Zl 4pf3p*C@cEXZ24nH puj87RHhfBtJ*3xYz_Pblfr+	?62l-=NBhKYUL_&7J'K7Dx2 P'J=#HxUNT_^TTJWu$X4'Zl 4pf3p*C@cEXZ24nH puj87RHhfBtJ*3xYz_Pblfr+	False	horatio0.42k@gmail.com
2021-01-14 13:46:21	2021-01-14 13:46:39	4	horatio0.42k@gmail.com		https://b-ok.cc/	https://b-ok.cc/	False	horatio0.42k@gmail.com
2021-04-15 19:43:54	2021-04-15 19:47:12	2	horatio0.42k@gmail.com	Grocery	Milk Honey Eggs Beer 6pack Ham Water Toilet paper Smith sweet	Milk Honey Eggs Beer 6pack Ham Water Toilet paper Smith sweet	False	horatio0.42k@gmail.com
Notes Creation Time	Notes Last Modified Time	List Parent ID	Creator Email	Title	Text	Synced Text	Is deleted	Last Modifier Email

The first note contained 4 links relating to the job listings he found on Craigslist within Phoenix, AZ. However, all the links were already invalid.

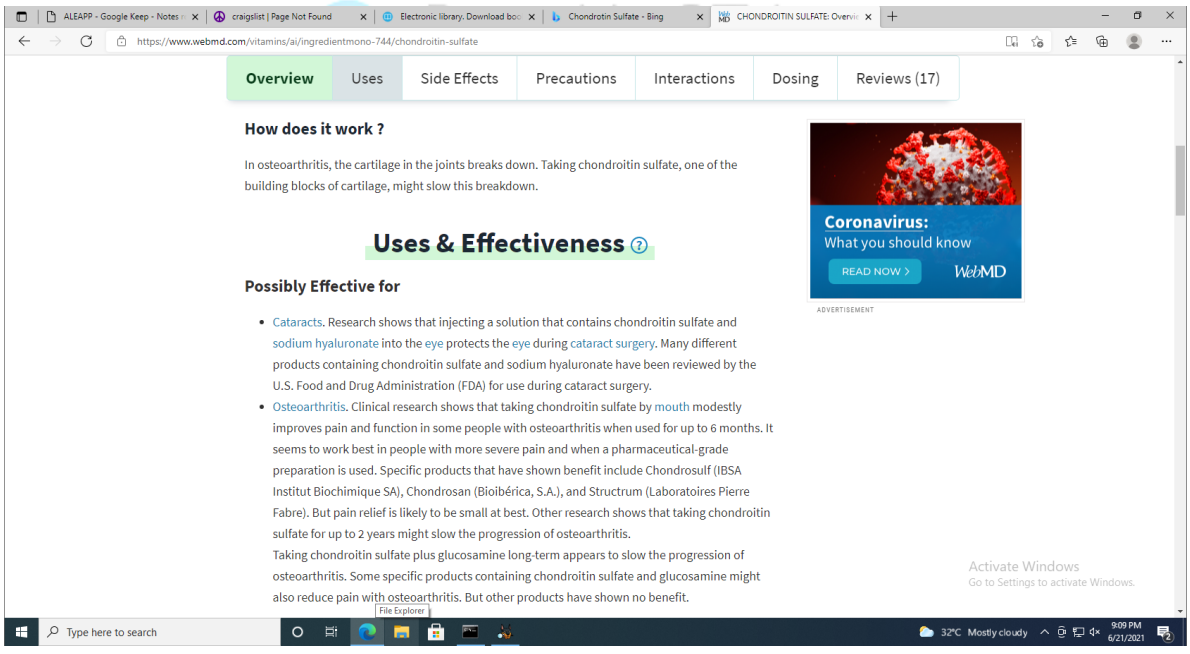



craigslist | Page Not Found
https://phoenix.craigslist.org/nph/cpg/d/phoenix-legacy-opportunity/7306534283.html
Page Not Found
There is nothing here
No web page for this address
404 Error
(return to craigslist homepage?)
© 2021 craigslist help safety privacy feedback terms about mobile
Activate Windows
Go to Settings to activate Windows.
Command Prompt
Type here to search
32°C Mostly cloudy
9:03 PM
6/21/2021

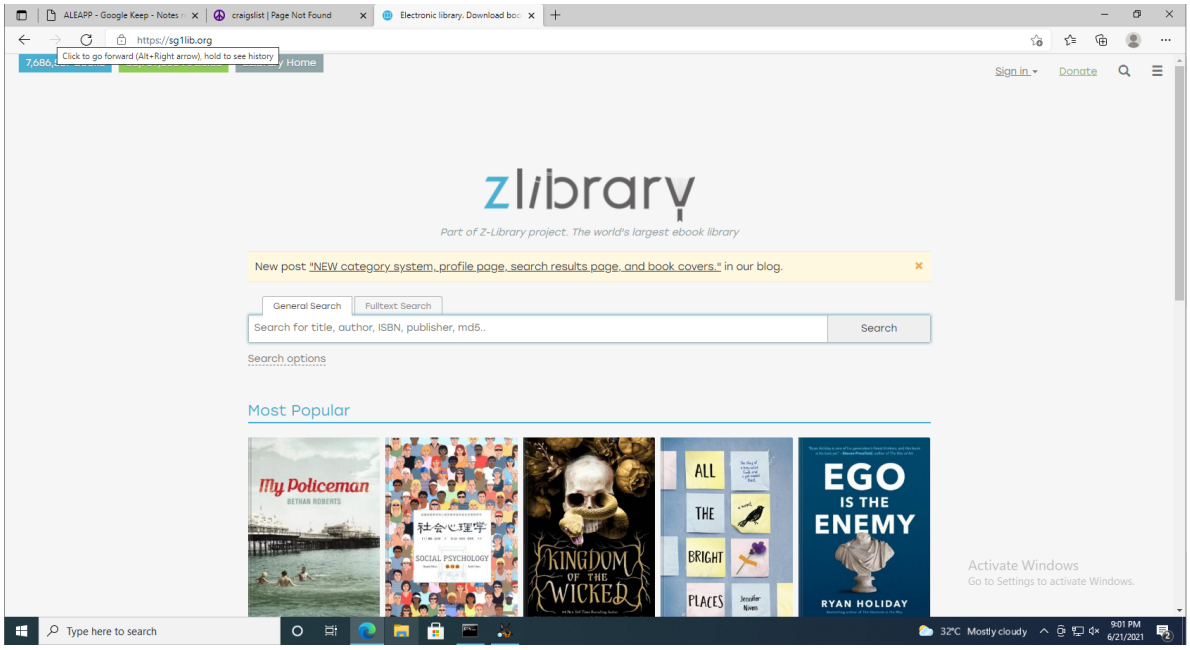

https://phoenix.craigslist.org/evl/crg/d/mesa-making-money-mailing-flyers-so-easy/7312010697.html
phoenix > east valley > gigs > creative gigs
post | account
This posting has expired.
help safety privacy feedback terms about mobile
Activate Windows
Go to Settings to activate Windows.
Store
Type here to search
32°C Mostly cloudy
9:04 PM
6/21/2021



The third note contains a drug called “Chondrotin Sulfate”, and it is used to treat osteoarthritis as the cartilage breaks down. The reference link can be found in this website: https://www.webmd.com/vitamins/ai/ingredientmono-744/chondroitin-sulfate and this could be used to treat Derek’s knee issue.

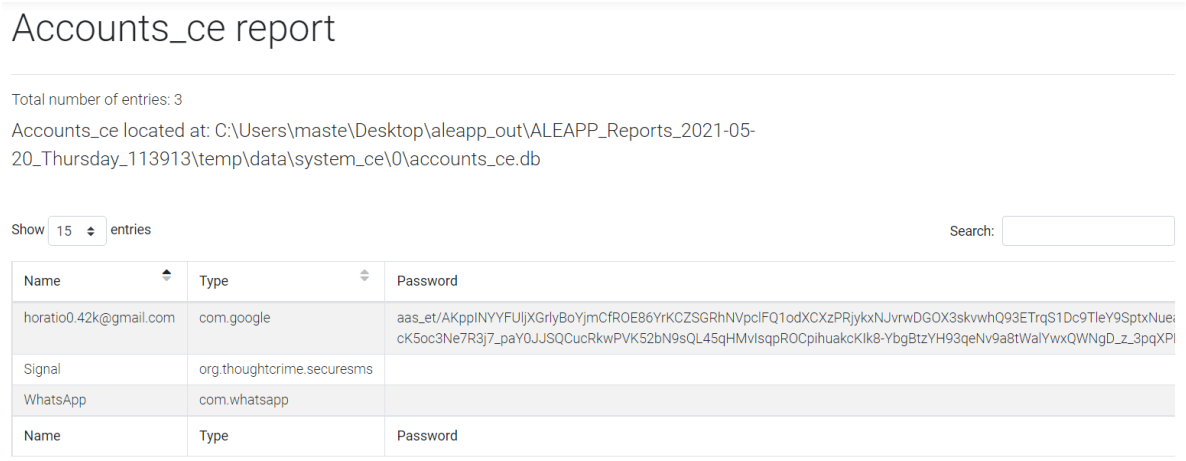


The link in the notes “https://b-ok.cc/” directs to Z-library, which is the world’s largest ebook library. He might have used this for browsing books but we could not gather much more information so we decided to forgo this information source.



RyanNgCT Inc.
SECURING WITH AI

Most probable accounts (to be searched for artifacts)



Accounts_ce report

Total number of entries: 3

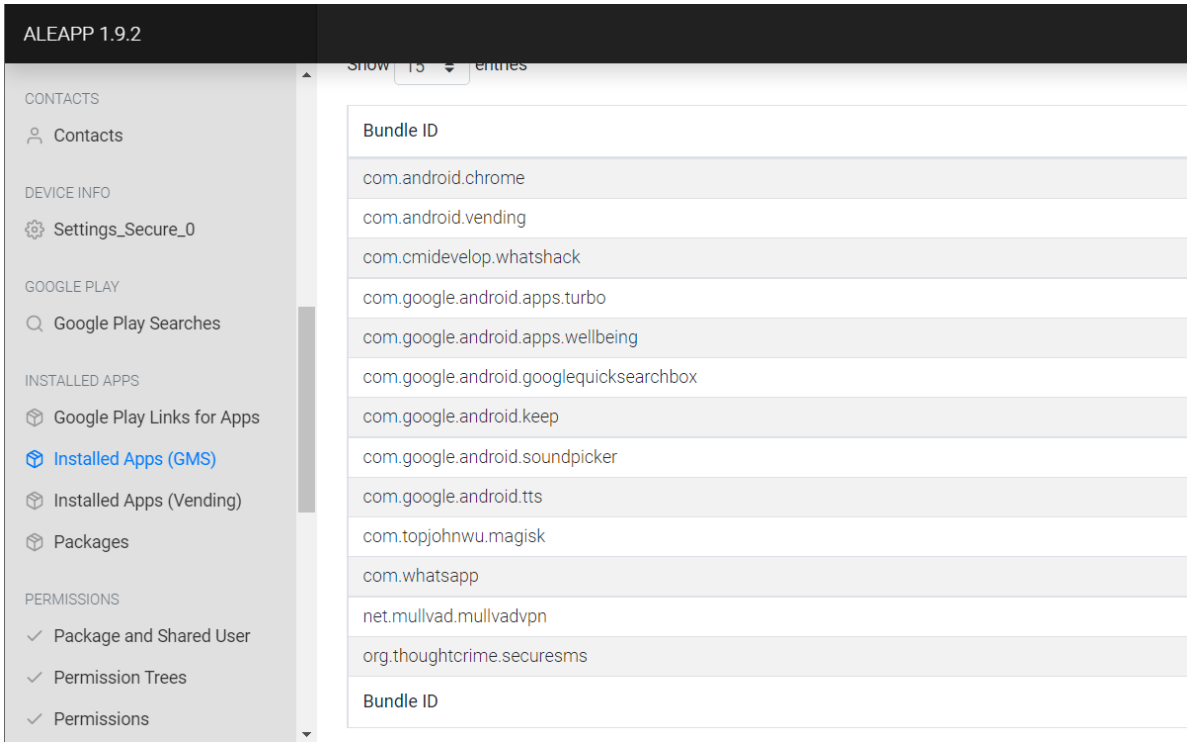
Accounts_ce located at: C:\Users\maste\Desktop\aleapp_out\ALEAPP_Reports_2021-05-20_Thursday_113913\temp\data\system_ce\0\accounts_ce.db

Show 15 entries Search:

Name	Type	Password
horatio0.42k@gmail.com	com.google	aas_et/AKppINYYFUljXGrlyBoYjmCfROE86YrKCZSGRhNVpclFQ1odXCXzPRjykxNJvrwDGOX3skvwhQ93ETrqS1Dc9TleY9SptxNue cK5oc3Ne7R3j7_paY0JJSQCucRkwPVK52bN9sQL45qHMvIsqpROCpihuakcKIk8-YbgBtzYH93qeNv9a8tWalYwxQWNgD_z_3pqXPl
Signal	org.thoughtcrime.securesms	
WhatsApp	com.whatsapp	
Name	Type	Password

Installed Apps

ALEAPP also provides a list of installed apps based on the contents of /data/data, from the list, we can research some common artifacts that might be worth looking into based on the applications installed (specific to the phone).



Chat Timeline of events

Initially, Derek was just chatting with a person we are assuming is his friend/accomplices, later we found out that the name of the person is Arnie after we matched the contact number with the information from the forensic evidence. They were talking casually about eating together, and him stating that he is broke, and talking to Arnie regarding his boss.

Source File	Message Type	Date/Time	Direction	From Phone Number	To Phone Number	Data Source
msgstore.db	WhatsApp Message	2020-05-19 10:11:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	It's a bubble
msgstore.db	WhatsApp Message	2020-05-19 10:12:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	Look how wobbly chart is
msgstore.db	WhatsApp Message	2020-05-19 10:41:30 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	hope your right
msgstore.db	WhatsApp Message	2020-05-19 10:41:43 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	anyway im broke :D
msgstore.db	WhatsApp Message	2020-06-20 09:18:30 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	Wanna go grab some food?
msgstore.db	WhatsApp Message	2020-06-20 09:23:30 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	Nah, didnt you read the news? https://www.azcentral.com/story/entertainment/dining/2020/06/19/these-metro-phoenix-restaurants-closed-permanently-due-covid-19/3211019001/
msgstore.db	WhatsApp Message	2020-06-21 05:03:12 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	LOL, got back from an interview, look where my boss hangs
msgstore.db	WhatsApp Message	2020-06-21 05:03:12 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	LogicalFileSet1
msgstore.db	WhatsApp Message	2020-06-21 05:03:12 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	LogicalFileSet1
msgstore.db	WhatsApp Message	2020-06-21 05:08:43 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	OMG so shitty taste
msgstore.db	WhatsApp Message	2020-07-21 11:08:51 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	LogicalFileSet1
msgstore.db	WhatsApp Message	2020-07-21 11:12:32 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	Nice?

Derek then began explaining to Arnie that he was not able to play the Among Us mobile game due to work. The texts received were on 6th September 11:08 am, 10th September 12:38 pm, 21st September 12:38 pm and 13th October 12:38 pm respectively. Each of the time, Derek was not able to play due to his work. The final text in the image below shows that Arnie seems to be rather frustrated by the situation that Derek is always at work when Arnie texts, unable to play or spend time anymore.

Source File	Message Type	Date/Time	Direction	From Phone Number	To Phone Number	Data Source
msgstore.db	WhatsApp Message	2020-09-06 11:08:53 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	Wanna play among us?
msgstore.db	WhatsApp Message	2020-09-06 11:12:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	Work....
msgstore.db	WhatsApp Message	2020-09-10 12:38:43 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	Go among us?
msgstore.db	WhatsApp Message	2020-09-10 12:45:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	Next time
msgstore.db	WhatsApp Message	2020-09-21 12:38:43 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	among us?
msgstore.db	WhatsApp Message	2020-09-21 13:01:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	Nah man, not today :-(
msgstore.db	WhatsApp Message	2020-10-13 12:38:43 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	Wanna play?
msgstore.db	WhatsApp Message	2020-10-13 13:01:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	Sry, work
msgstore.db	WhatsApp Message	2020-10-13 13:18:43 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	always has been

The above details were more trivial matters that did not arouse suspicion thus artifacts here are not worth further investigation.

On 21st November 2020, Derek texted Arnie again regarding his knee, indicating he had trouble walking. Arnie suggested that he went to see the doctor. The images below show the exchange of their conversation and an x-ray scan of his knee.

Source File	Message Type	Date/Time	Direction	From Phone Number	To Phone Number	Data Source
msgstore.db	WhatsApp Message	2020-12-21 03:02:12 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	this fkn work, the knee ached af, no idea what to do.
msgstore.db	WhatsApp Message	2020-12-21 03:03:12 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	trouble walking today
msgstore.db	WhatsApp Message	2020-12-21 03:09:43 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	go see a doctor dude!

Then on 9th January 2021, Derek's friend complained to him regarding cryptocurrency and how rich Arnie would be if bitcoin had been purchased beforehand. Derek returned a shrug emoji as a reply.

Source File	Message Type	Date/Time	Direction	From Phone Number	To Phone Number	Data Source
msgstore.db	WhatsApp Message	2021-01-09 11:01:45 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	I HADD to buy bitcoin this summer
msgstore.db	WhatsApp Message	2021-01-09 11:01:59 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	if you hadn't discouraged me with your fuckin Bubbles I wouldve been 5 times richerr
msgstore.db	WhatsApp Message	2021-01-09 12:44:34 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	18084826989@s.whatsapp.net	¯_(ツ)_/¯

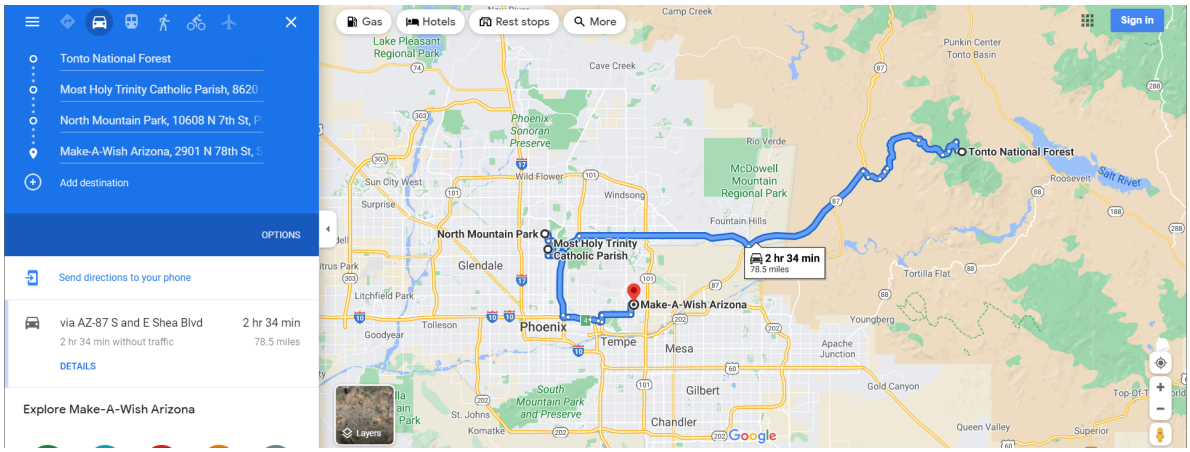
Finally, here is where we think Derek started his job as an illegal drug dealer. It started on 19th March 2021 when he sent images to a contact number called Boss, as saved in his contact list. The exchanged messages here do not tell the full story as we believe that they might have interacted in real life to talk about the business. We also have reason to believe that Derek met Boss through cryptocurrency as he sent Boss a link to Img.bb website a month after they initially made contact on Whatsapp. Img.bb was used to upload images of successful drug trading and was used by Boss to monitor Derek, ensuring all dealings were made fairly and paid in full. This can be seen by the number of pictures with money contained in Derek's phone when it was obtained for forensic evidence.

We know from the text messages that Derek's first successful deal was on 12th April 2021, and his last trade was on 21st April 2021, before he was caught by the police. Although all the links to Img.bb website have since been deleted, we have reason to believe that it is the platform used by the both of them to exchange information such as clients, locations and amount of money for each trade. This would have given them enough privacy and secrecy to perform their business quietly, avoiding attention of the state police.

RyanNgCT Inc.

Source File	Message Type	Date/Time	Direction	From Phone Number	To Phone Number	Data Source
msgstore.db	WhatsApp Message	2021-03-19 01:25:12 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	LogicalFileSet1
msgstore.db	WhatsApp Message	2021-03-19 01:25:12 SGT	Incoming	12395104974@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	~0.088 btc sent your way. tx 34826682f1e7aa8b2fba482baa4aac0cd251733aa2b29ac5d2675c7451f97ca2
msgstore.db	WhatsApp Message	2021-03-19 02:03:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	Nice, thanks. Got it
msgstore.db	WhatsApp Message	2021-04-12 18:26:32 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	https://ibb.co/album/RTehva
msgstore.db	WhatsApp Message	2021-04-13 03:54:43 SGT	Incoming	12395104974@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	There are not enough pics.
msgstore.db	WhatsApp Message	2021-04-14 02:26:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	Sorry! I forgot to take one :-(((
msgstore.db	WhatsApp Message	2021-04-14 03:01:32 SGT	Incoming	12395104974@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	Dont make me suspect you
msgstore.db	WhatsApp Message	2021-04-14 17:27:17 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	Today's photos. All in place https://ibb.co/album/AMoXHs
msgstore.db	WhatsApp Message	2021-04-15 18:02:17 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	https://ibb.co/album/ASpEBt
msgstore.db	WhatsApp Message	2021-04-16 01:35:27 SGT	Incoming	12395104974@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	payment of 0.0913 btc should be on ur wallet now
msgstore.db	WhatsApp Message	2021-04-16 04:25:27 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	Appreciated
msgstore.db	WhatsApp Message	2021-04-16 04:28:27 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	i see a bit less than that
msgstore.db	WhatsApp Message	2021-04-16 04:28:33 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	intended?
msgstore.db	WhatsApp Message	2021-04-16 04:52:43 SGT	Incoming	12395104974@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	yes.
msgstore.db	WhatsApp Message	2021-04-16 18:35:30 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	https://ibb.co/album/YOvt6f
msgstore.db	WhatsApp Message	2021-04-17 19:15:00 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	https://ibb.co/album/RKntdG
msgstore.db	WhatsApp Message	2021-04-18 19:11:34 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fca6a628	12395104974@s.whatsapp.net	https://ibb.co/album/rvD0OF
msgstore.db	WhatsApp Message	2021-04-21 17:03:00 SGT	Incoming	12395104974@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fca6a628	says Not found, upload pics again

Possible Travel Timeline (Based on images in DCIM/Camera)

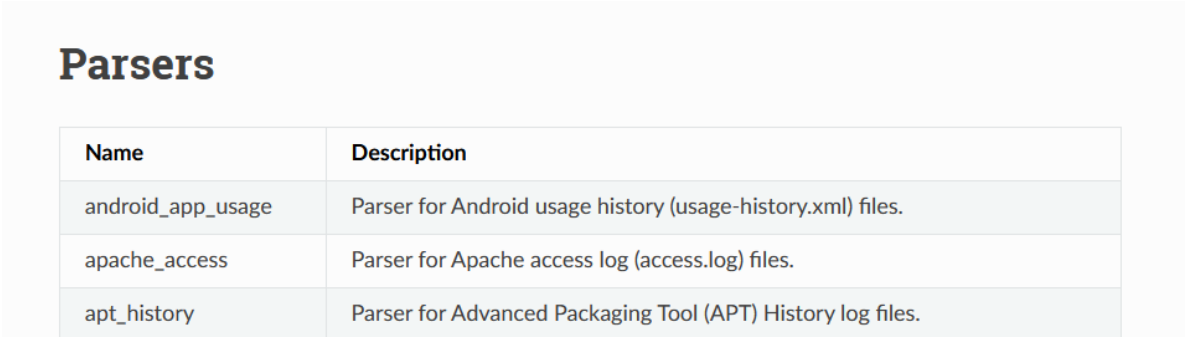


Open Source (Academic Usage)

Based on the images he searched, he could have visited these 4 locations, although we could not find an exact correlation between the places and the texts as none of their names were mentioned.

Justification of Preference of Forensic Tools and Recommendations

Due to the lack of commercial tools to use when coming up with the assignment (would probably be possible if this case scenario was under Singapore's/the US' jurisdiction), we went to source for multiple open source tools, as they were free and widely available to use, in order to extract evidence, since every tool has its own specialities and some had weaknesses. Ultimately, it was up to us as forensic analysts to correlate the data and make sense of what happened as well as formulate a timeline. We tried using plaso to parse the data but there were some errors that arose (e.g. the android_app_usage file was not present to be parsed).



Parsers

Name	Description
android_app_usage	Parser for Android usage history (usage-history.xml) files.
apache_access	Parser for Apache access log (access.log) files.
apt_history	Parser for Advanced Packaging Tool (APT) History log files.

In addition, we also tried to use additional tools to try to parse this directory (/data/system/usagestats) like this parser but could not seem to get it to work: https://github.com/abrignoni/Android-Usagestats-XML-Protobuf

RyanNgCT Inc. THAI

However, commercial tools like Belkasoft X would have saved much time as it is able to parse multiple formats and correlate the evidence on our behalf. One other disadvantage is that since we did not have the physical device for examination, deleted files in slack space might be missed, which means we might have left out critical evidence that would have helped to more concretely prove the intentional obstruction of justice through evidence deletion. Thus we might want to venture into physical acquisition if it is possible too.

It would also have been useful to have a multi-purpose tool, somewhat like Autopsy but with integration of features for correlation like Whatsapp Viewer and reporting like ALEAPP, since we often had to correlate evidence ourselves to prove the hypothesis.

Our biggest challenge was finding the right tools for the right purpose since not all the open source tools available on Github were well-maintained or usable.

ORIGINAL

Conclusion

Based on the evidence that we have gathered from his mobile device, we can incriminate Derek Hor with drug dealing offences. We also have found evidence that Derek was looking for a high paying, highly flexible job due when he stumbled upon the advertisement for the drug delivery job. Screenshots of bank notes were obtained from his mobile device, assuming those were the deleted images we were not able to find from Img.bb. There were also images of buildings, which we

Open Source (Academic Usage)
assumed were the meetup locations for him to conduct the exchange of drugs and money. We have evidence that Derek has been participating in drug related activities such as delivery and possession of drugs, as well as taking pictures of them as proof of delivery on img.bb according to WhatsApp messages on the mobile device.

RyanNgCT Inc.
SECURING WITH AI

References/Appendices

Forensic Tools:

1. aLEAPP : https://github.com/abrignoni/ALEAPP
2. Andriller: https://github.com/den4uk/andriller
3. WhatsApp Viewer:
    a. https://andreas-mausch.de/whatsapp-viewer/
    b. https://github.com/andreas-mausch/whatsapp-viewer/
4. Autopsy: https://www.digitalforensics.com/blog/android-forensic-analysis-with-autopsy/

Evidence Source: https://belkasoft.com/ctf/

General References:

1. https://blog.group-ib.com/whatsapp_forensic_artifacts
2. https://www.cellebrite.com/en/hex-diving-the-easy-way-to-uncover-hidden-forensic-artifacts/

RyanNgCT Inc.
SECURING WITH AI

END