

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



RyanNgCT Inc.

SECURING WITH AI

Ryan Ng (Leader)

Ezra Ho

Hannah Leong

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.



Dated 11 November 2021

Ng Chin Tiong Ryan

Table Of Contents

Introduction of Assignment (Fictitious Case)	4
Description of work	4
Resources (hardware and software)	4
Set-up and Functionality of Tools	6
Extraction using Andriller	6
Reporting using aLEAPP	7
Whatsapp Viewer messages	10
Investigation using Autopsy Android Modules	14
Investigation of Key Artifacts using the Tools	19
Images	19
Keyword Searches	23
Extension Mismatch	26
Whatsapp Information	28
General Phone Information	31
SQLite Spy and Editors	31
Calendar	37
Examination of Artifacts using ALEAPP	40
Whatsapp	40
Google Chrome History	41
Craigslist / Jobs / Housing	41
Knee Pain / Clinic	42
ImgBB.com	43
Google Maps	44
Google Keep - Notes Report	46
Installed Apps	50
Chat Timeline of events	51
Justification of Preference of Forensic Tools and Recommendations	53
Conclusion	54
References/Appendices	55

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)

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)

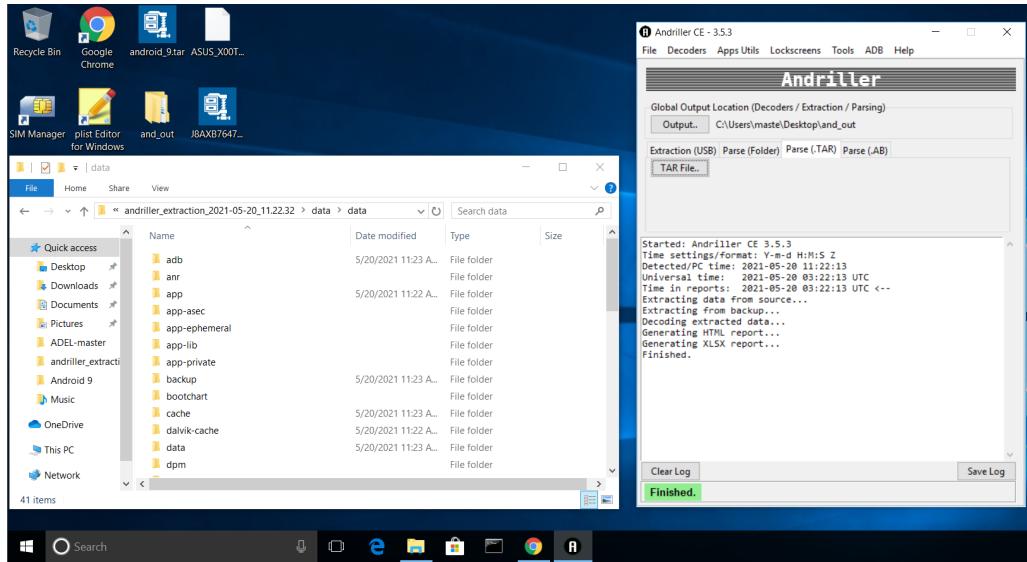
Evidence Source:

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



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.

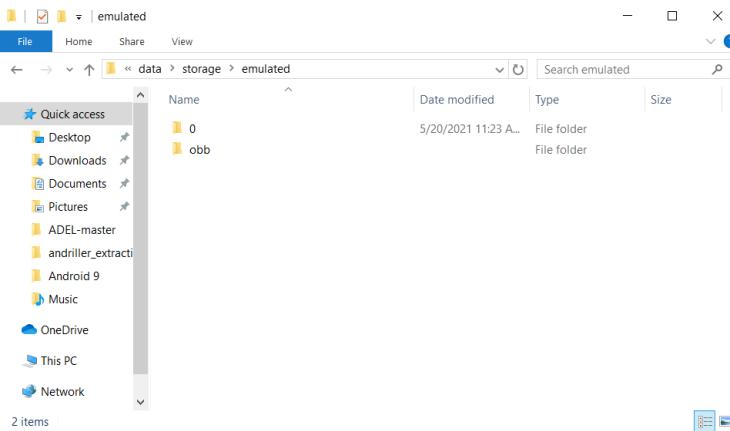


Open andriller and select an output file and using the Parse (TAR) tab, select **J8AXB7647798GRJ-20210421_0920.tar** (not the ASUS belkasoft image) on the Desktop and the tool will automatically start processing and generate another file with outputs and reports.

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.

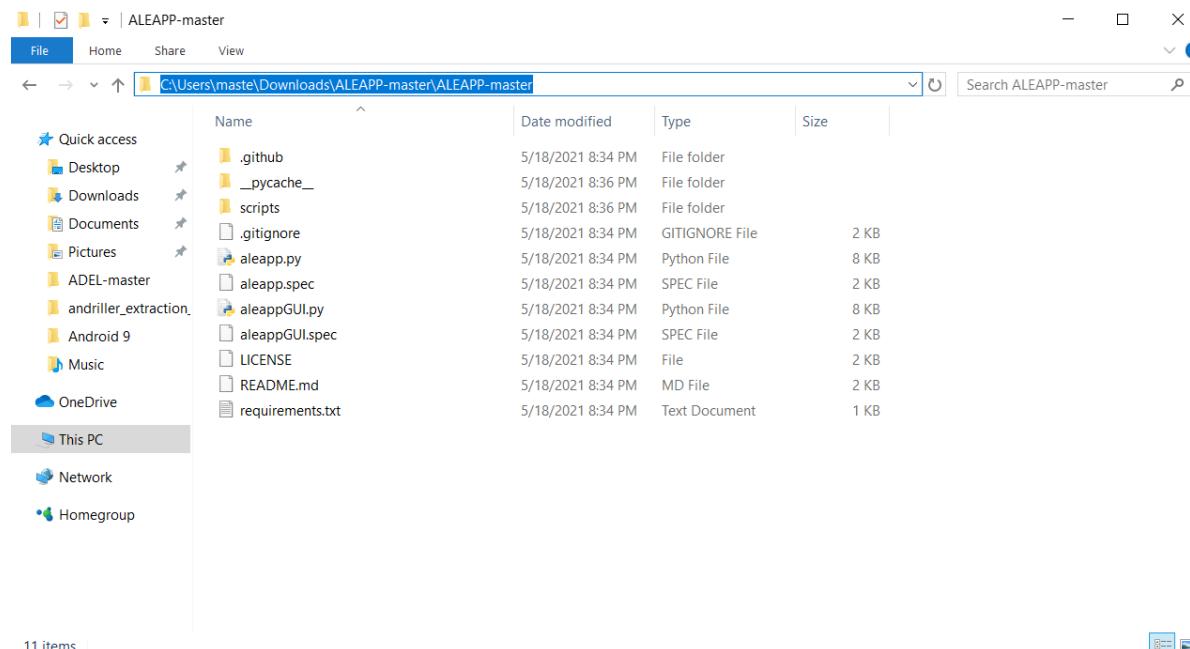
We also can see that some artifacts reside in `andriller_extraction_<date_timestamp>\data\storage\emulated` as shown below.

Open Source (Academic Usage)

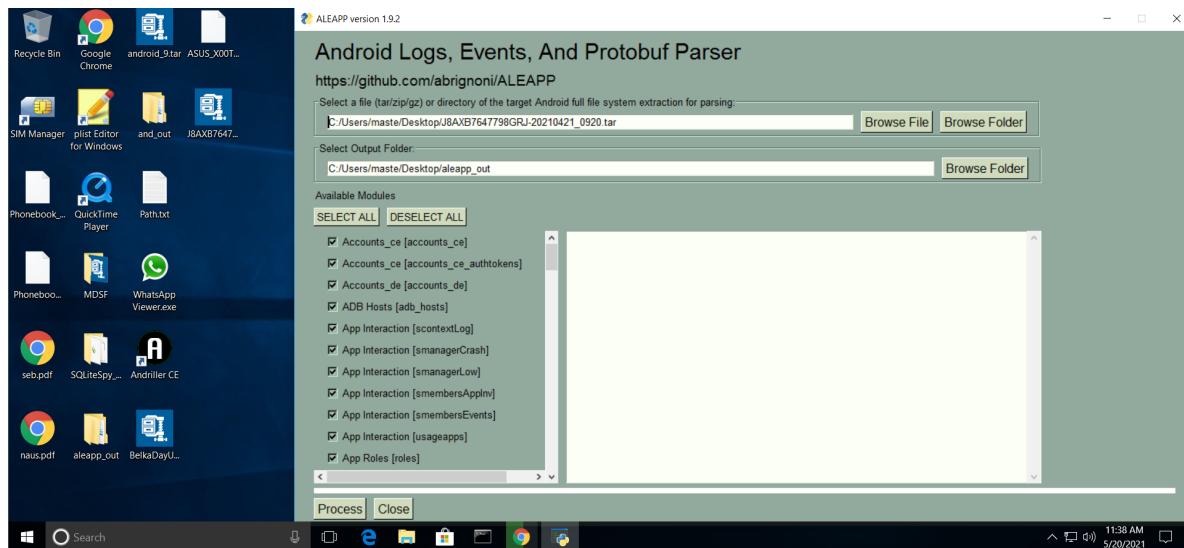


b) Reporting using aLEAPP

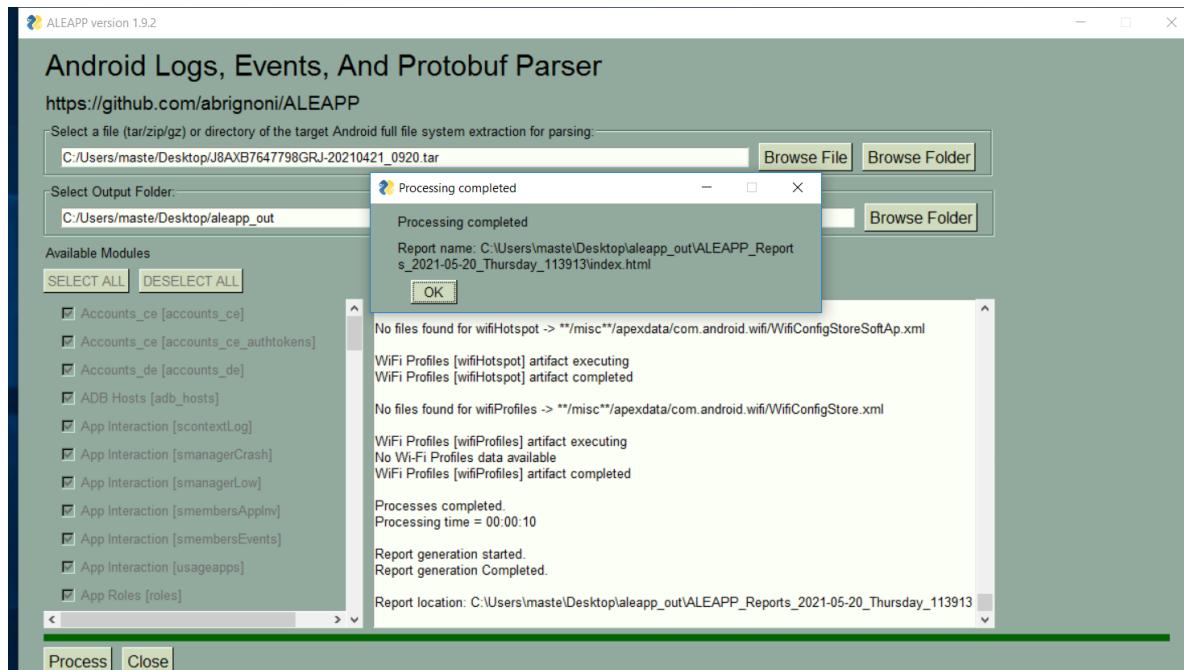
For Windows, navigate to the directory where aLEAPP was installed and copy the path. Open up a command prompt and navigate there, following which we will launch a GUI instance. (For linux, since the tool should be automatically added to \$PATH upon installation and setting up dependencies, we can just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



Open Source (Academic Usage)



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.

Open Source (Academic Usage)

The screenshot shows the ALEAPP software interface. On the left is a sidebar with various forensic analysis categories like SAVED REPORTS, ADB HOSTS, ACCOUNTS_CE, and CHROMIUM. The main area displays 'Android Logs Events And Protobuf Parser' and 'Case Information'. Under 'Case Information', there are tabs for Details, Device details, Script run log, and Processed files list. The 'Details' tab shows system information: Android version per Usagestats: 9, Codename per Usagestats: REL, Build version per Usagestats: cee0d3f014, Bluetooth name: ASUS_X00TDB, and Bluetooth address: 22:22:11:96:C1:49. At the bottom right, a message says 'Thank you for using ALEAPP'.

The screenshot shows the ALEAPP software interface with the title 'ALEAPP - Chrome History report'. The sidebar includes categories like CHROME HISTORY, CONTACTS, DEVICE INFO, GOOGLE PLAY, and INSTALLED APPS. The main area displays a table of Chrome history entries. The columns are Last Visit Time, URL, Title, Visit Count, and Hidden. The data shows several visits to Google search results for 'phoenix news', news sites like ABC15.com, FOX10Phoenix.com, and Craigslist.org, and a geo.craigslist.org entry.

Last Visit Time	URL	Title	Visit Count	Hidden
1601-01-01 00:00:00	https://www.google.com/search?q=phoenix+news&oq=phoenix+news&aqs=chrome..69i57j0i433j0i131i433j2.2569j0j7&sourceid=chrome-mobile&ie=UTF-8	phoenix news - Google Search	3	0
1601-01-01 00:00:00	https://www.abc15.com/	Phoenix, Arizona News and Weather ABC15 Arizona	1	0
1601-01-01 00:00:00	https://www.fox10phoenix.com/	FOX 10 Phoenix	2	0
1601-01-01 00:00:00	https://www.google.com/search?q=craigslist&oq=craig&aqs=chrome.1.69i57j0i433i457j0i402l2j0i131i433.1905j0j7&sourceid=chrome-mobile&ie=UTF-8	craigslist - Google Search	1	0
1601-01-01 00:00:00	https://www.craigslist.org/	craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	1	0
1601-01-01 00:00:00	https://geo.craigslist.org/	craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	1	0

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.

Open Source (Academic Usage)

ALEAPP 1.9.2

INSTALLED APPS

- Google Play Searches
- Google Play Links for Apps
- Installed Apps (GMS)**
- Installed Apps (Vending)
- Packages

PERMISSIONS

- Package and Shared User
- Permission Trees
- Permissions
- Runtime Permissions_0

SQlite JOURNALING

- Strings - SQLite Journal & WAL

USAGE STATS

- OS Version

Dark Switch

Bundle ID	Content
com.android.chrome	
com.android.vending	
com.cmidevelop.whatshack	
com.google.android.apps.turbo	
com.google.android.apps.wellbeing	
com.google.android.googlequicksearchbox	
com.google.android.keep	
com.google.android.soundpicker	
com.google.android.tts	
com.topjohnwu.magisk	
com.whatsapp	
net.mullvad.mullvadvpn	
org.thoughtcrime.securesms	

Search: []

11:42 AM 5/20/2021

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.

ALEAPP 1.9.2

PACKAGES

PERMISSIONS

- Package and Shared User
- Permission Trees
- Permissions
- Runtime Permissions_0

SQlite JOURNALING

- Strings - SQLite Journal & WAL

USAGE STATS

- OS Version
- UsageStats_0

WELLBEING

- Account Data

Events

WHATSBAPP

- WhatsApp - Contacts
- WhatsApp - Messages**

WIFI PROFILES

- Wi-Fi Hotspot

Dark Switch

Send Timestamp	Received Timestamp	Message ID	Recipients	Direction	Content	Group Sender	Attachment
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg-fna.whatsapp.net/d/f/AqKKbaPHuHXMNjqMYBPKRpdFTyxS3aiRnNmRenc
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg-fna.whatsapp.net/d/f/AqWHRSLkThAbkx8IOCaMW
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg-fna.whatsapp.net/d/f/Ap2hVbW3De_BidKFkUVgS7AvbDymv5StXl
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg-fna.whatsapp.net/d/f/Asamds9jQBZzOXQhb7Rwsys4
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg-fna.whatsapp.net/d/f/AijxXQgiyMVA3cx9zmRdfvv7L
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg-fna.whatsapp.net/d/f/Aj9u6j0TcJsaCoJqYpArhJWCo-4UXTpSpF
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg.whatsapp.net/d/f/aiUMMMSwTqRekVJL_TxFGzam1C
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg.whatsapp.net/d/f/AneGc_HsuIsA1xdftYQmUhqdDLk
2020-05-19 09:28:20	2020-05-19 09:28:20	status@broadcast	status@broadcast	0	0@s.whatsapp.net		https://mmg.whatsapp.net/d/f/AvZMhdzCY_6DCtV75deWYNl_CRI
2020-05-19 09:29:43	2020-05-19 09:29:43	18084826999@s.whatsapp.net	18084826999@s.whatsapp.net	1	18084826999@s.whatsapp.net		https://mmg.whatsapp.net/d/f/AgZc7vePdW_AVb_UvMw3ixQnOc
2020-05-19 09:29:43	2020-05-19 09:29:43	18084826999@s.whatsapp.net	18084826999@s.whatsapp.net	1	18084826999@s.whatsapp.net		https://mmg.whatsapp.net/d/f/AgZc7vePdW_AVb_UvMw3ixQnOc
2020-05-19	2020-05-19	18084826999@s.whatsapp.net	18084826999@s.whatsapp.net	0	18084826999@s.whatsapp.net	https://mmg.whatsapp.net/d/f/Asyt47chtaEUitm3ANLRd4pkJuh	

Search: []

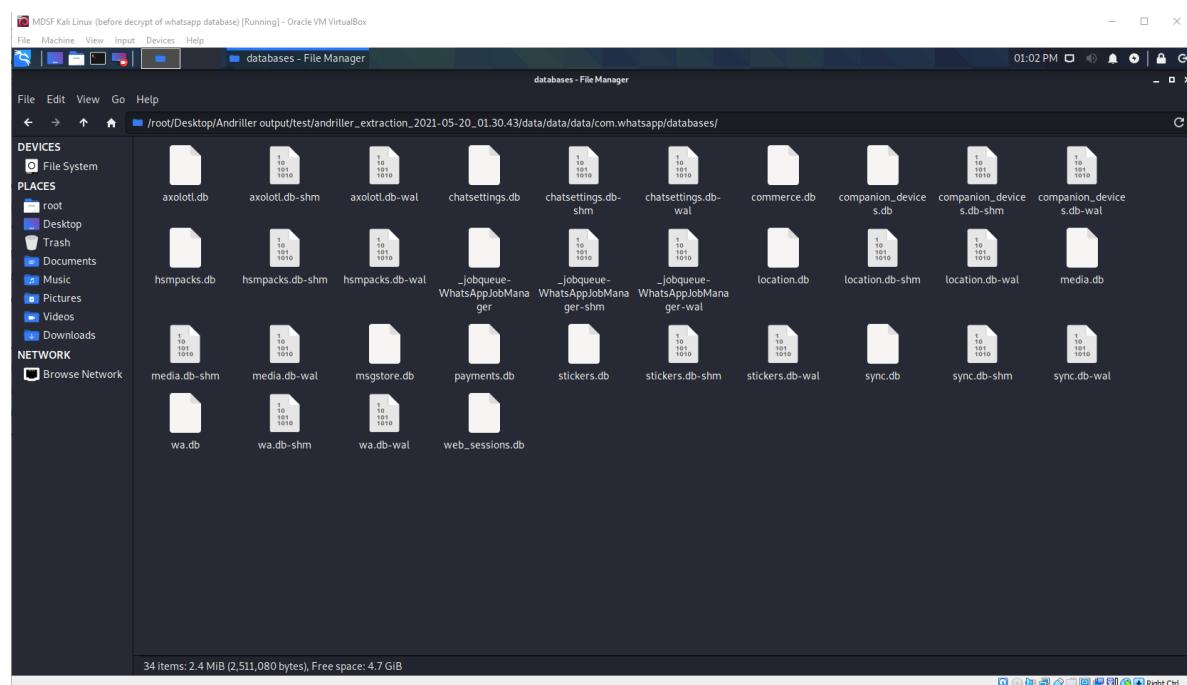
11:46 AM 5/20/2021

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

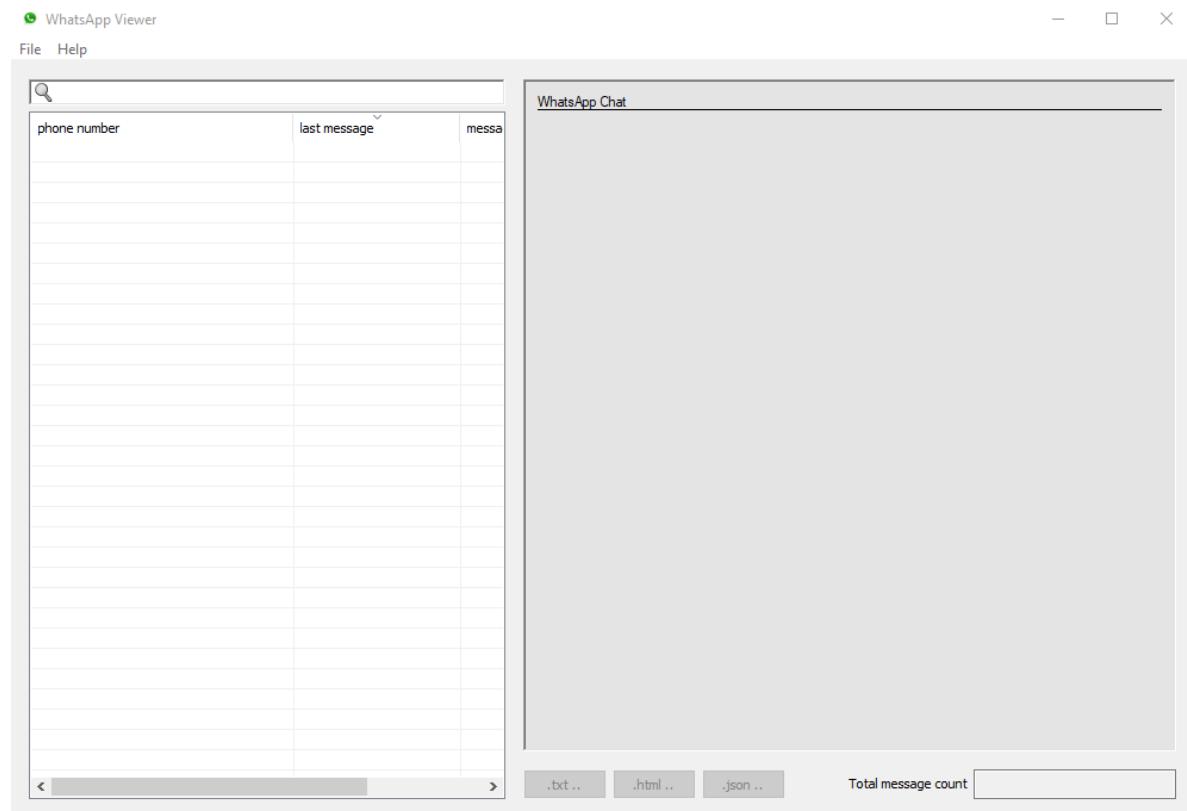
WhatsApp Viewer is a simple Windows tool that allows us to display chats from android phones through the msgstore.db file which is where chat history is stored. It also has the capability of decrypting any WhatsApp encrypted files like .crypt5, .crypt7, .crypt8, .crypt12 and .crypt1. It does so by using 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/com.whatsapp/databases/**.



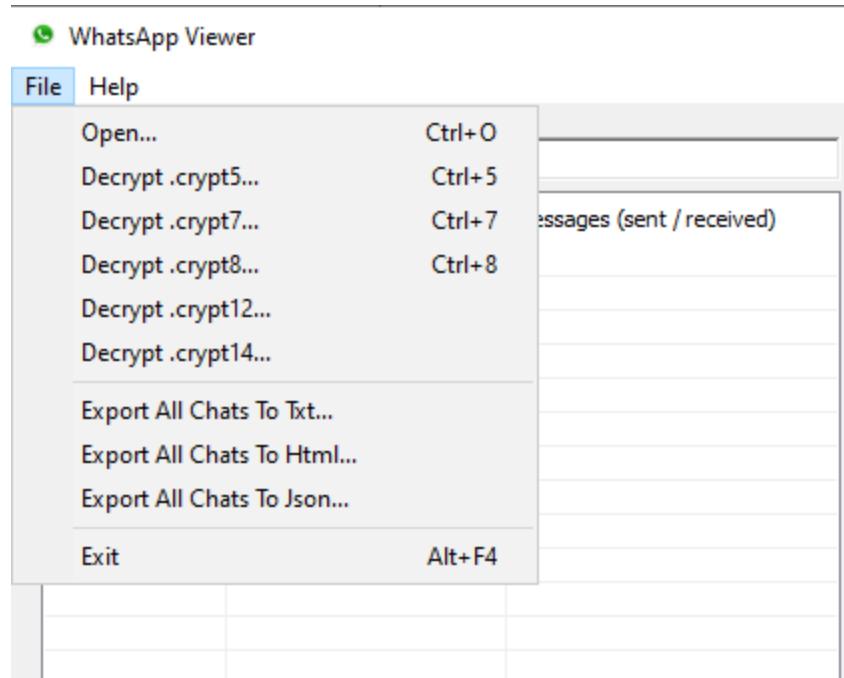
If a linux machine is being used, like in the picture above, the file would need to be transferred over to a windows machine. On the windows machine, double click WhatsApp Viewer.exe and the UI should open with two panes as follows.

Open Source (Academic Usage)



RyonNoCT Inc.

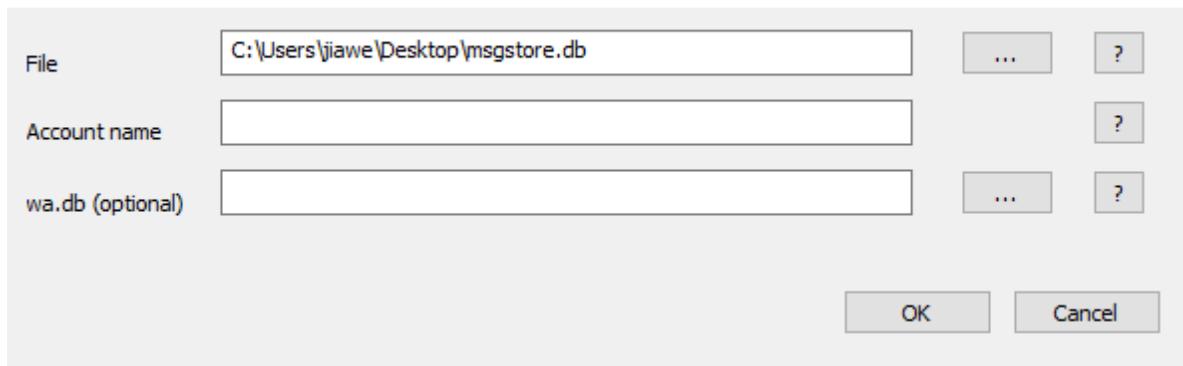
When we click on the file tab we can see all the options available to us. For this example we will just click open since decrypting would not be required, however, should decrypting be required, the key file should also be obtained (should be found in the WhatsApp Directory).



Here we select the file and click OK.

Open Source (Academic Usage)

Open WhatsApp Database



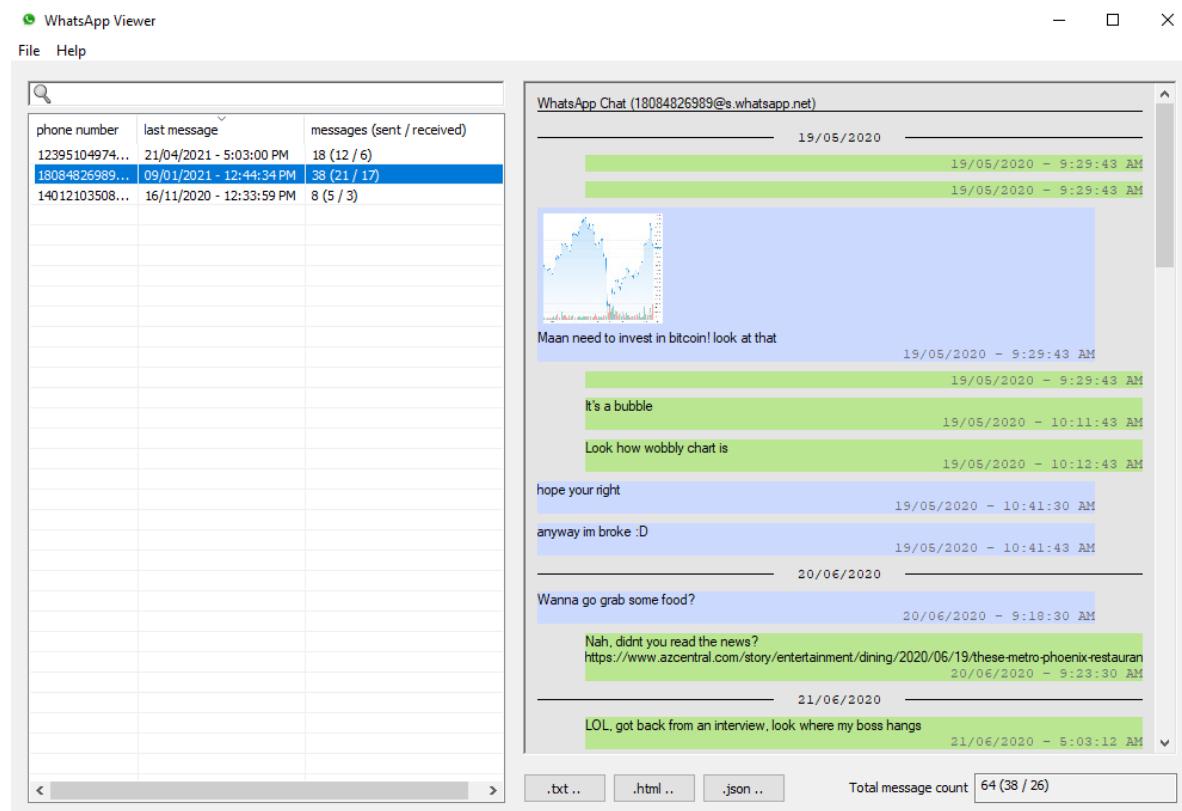
The chat history of all the messages should pop up on the left.

The application window has a title bar with a green icon, 'WhatsApp Viewer', and standard window controls. The menu bar includes 'File' and 'Help'. On the left is a search bar and a table listing contacts:

phone number	last message	messages (sent / received)
12395104974...	21/04/2021 - 5:03:00 PM	18 (12 / 6)
18084826989...	09/01/2021 - 12:44:34 PM	38 (21 / 17)
14012103508...	16/11/2020 - 12:33:59 PM	8 (5 / 3)

The main area is titled 'WhatsApp Chat' and is currently empty. At the bottom are buttons for '.txt ..', '.html ..', '.json ..', and a total message count of '64 (38 / 26)'.

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.



d) Investigation using Autopsy Android Modules

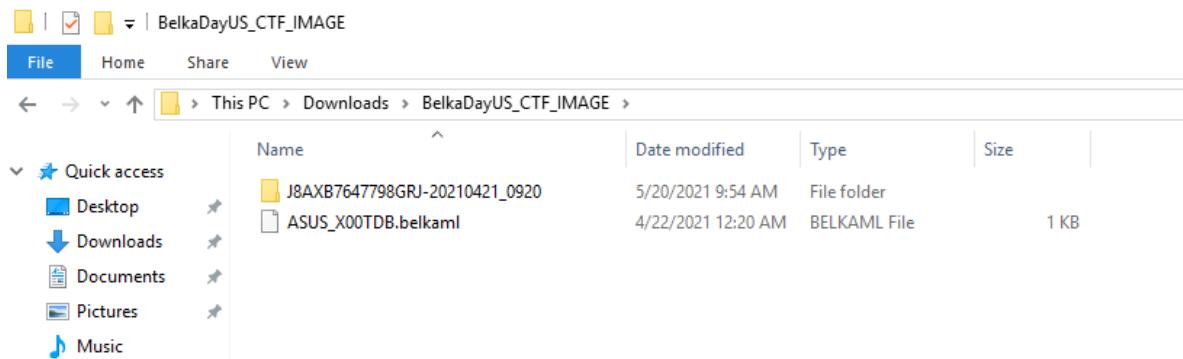
This will help us to more easily correlate the messages and media to quickly establish the communications exchanged. Using Autopsy on a Windows 10 virtual machine, we can also view the full and thorough analysis of the data contained within the ASUS phone. Although Autopsy is mainly used for computer 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.

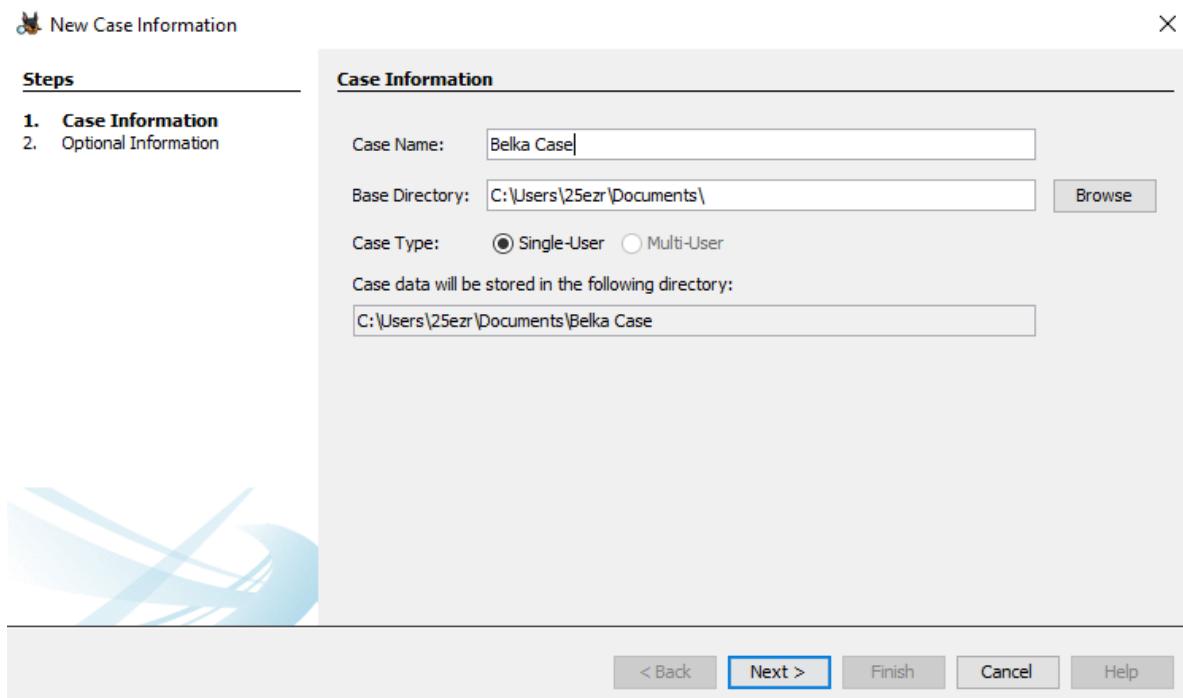
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
J8AXB7647798GRJ-20210421_0920.tar *	1,673,574,400	?	WinRAR archive	4/22/2021 12:20 AM	D8F5C0B0
ASUS_X00TDB.belkaml *	694	647,506,144	BELKAML File	4/22/2021 12:20 AM	1A53D73E

Open Source (Academic Usage)

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.

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

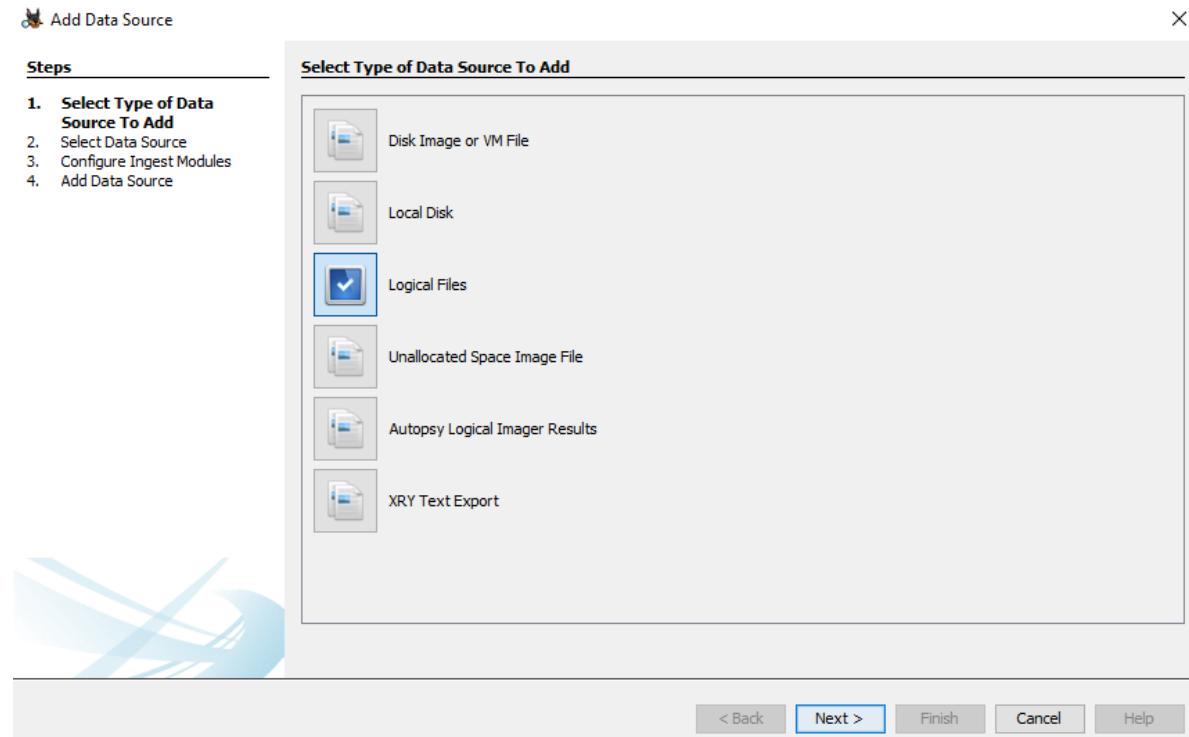
Organization

Organization analysis is being done for:



Open Source (Academic Usage)

Select “Logical Files”

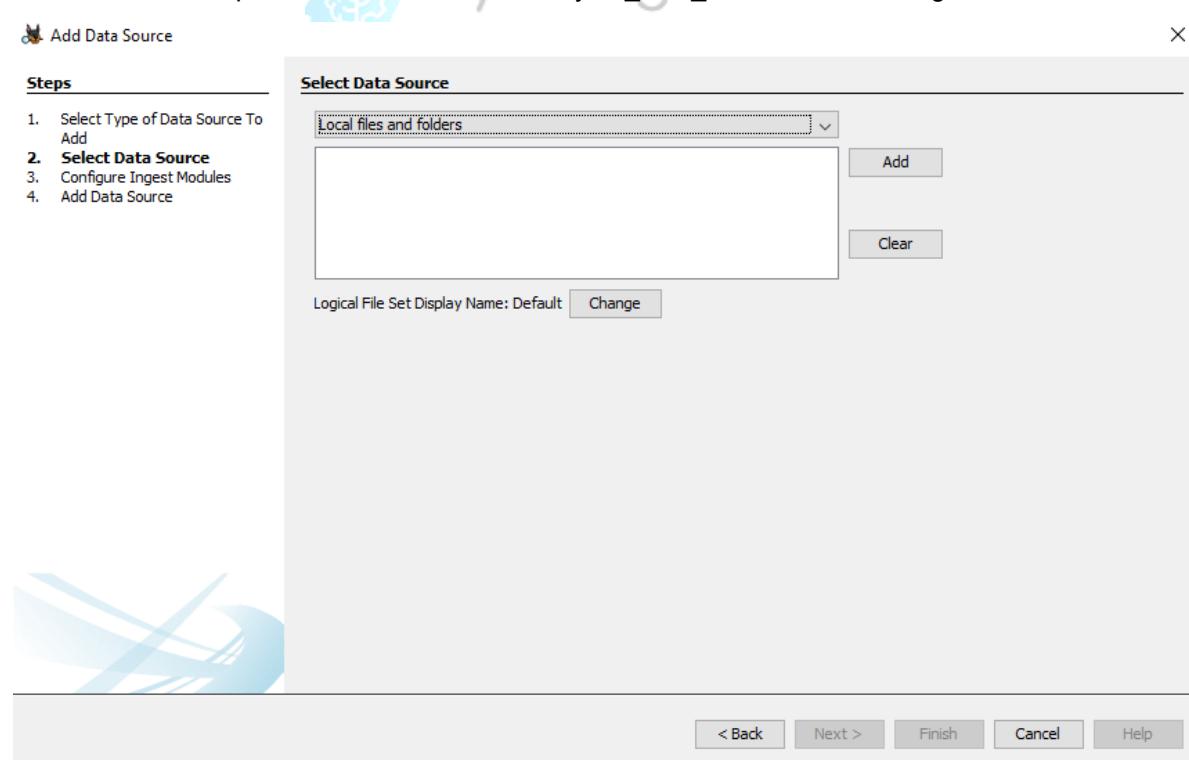


The screenshot shows the 'Select Type of Data Source To Add' step of the 'Add Data Source' wizard. On the left, a sidebar lists steps: 1. Select Type of Data Source To Add, 2. Select Data Source, 3. Configure Ingest Modules, 4. Add Data Source. Step 1 is bolded. The main area shows a list of data source types with icons:

- Disk Image or VM File
- Local Disk
- Logical Files** (selected, indicated by a blue checkmark icon)
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

At the bottom are buttons: < Back, Next >, Finish, Cancel, Help.

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



The screenshot shows the 'Select Data Source' step of the 'Add Data Source' wizard. On the left, a sidebar lists steps: 1. Select Type of Data Source To Add, 2. **Select Data Source**, 3. Configure Ingest Modules, 4. Add Data Source. Step 2 is bolded. The main area shows a 'Select Data Source' dialog with a dropdown menu set to 'Local files and folders'. Below it is a list box containing no items, with an 'Add' button to its right. At the bottom is a 'Logical File Set Display Name: Default' field with a 'Change' button.

At the bottom are buttons: < Back, Next >, Finish, Cancel, Help.

Open Source (Academic Usage)

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.

Select Local Files or Folders

Look in: BelkaDayUS_CTF_IMAGE

J8AXB7647798GRJ-20210421_0920

ASUS_X00TDB.belkaml

Recent Items

Desktop

Documents

This PC

Network

File name: C:\Users\25ezr\Downloads\BelkaDayUS_CTF_IMAGE

Select

Cancel

Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Local files and folders

C:\Users\25ezr\Downloads\BelkaDayUS_CTF_IMAGE

Add

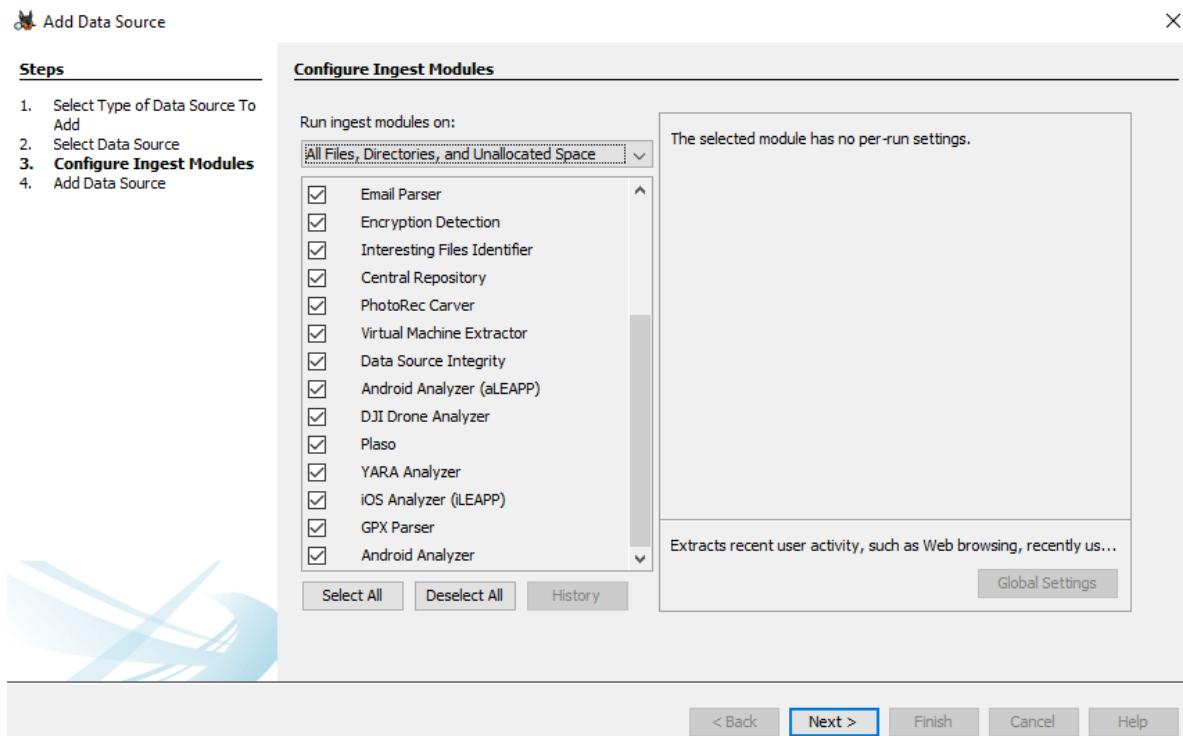
Clear

Logical File Set Display Name: Default Change

< Back Next > Finish Cancel Help

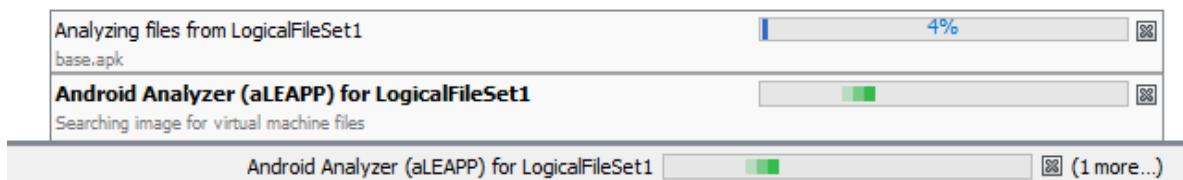
Open Source (Academic Usage)

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.

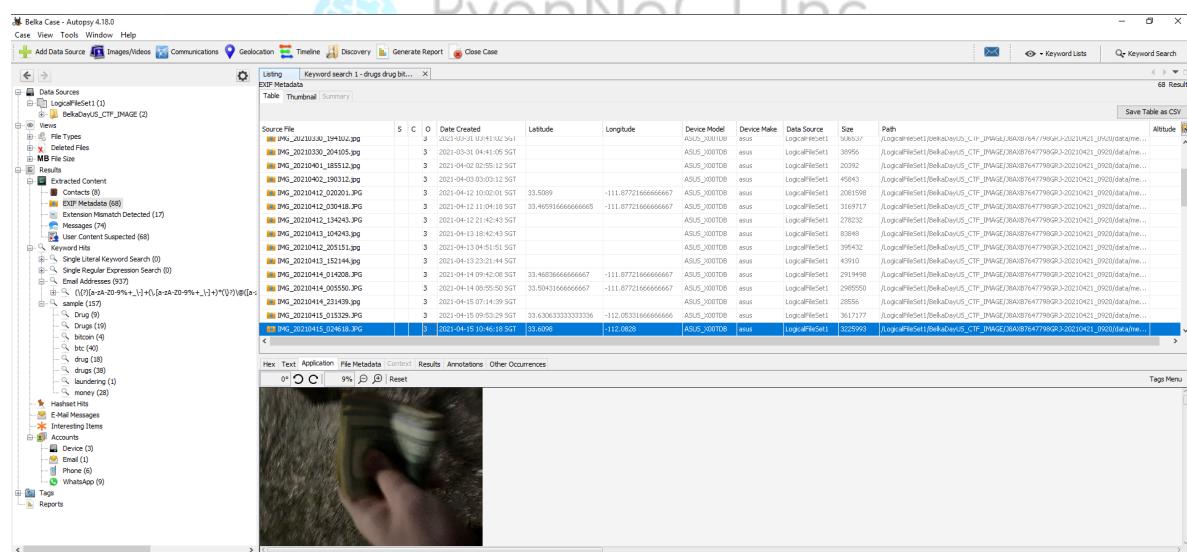
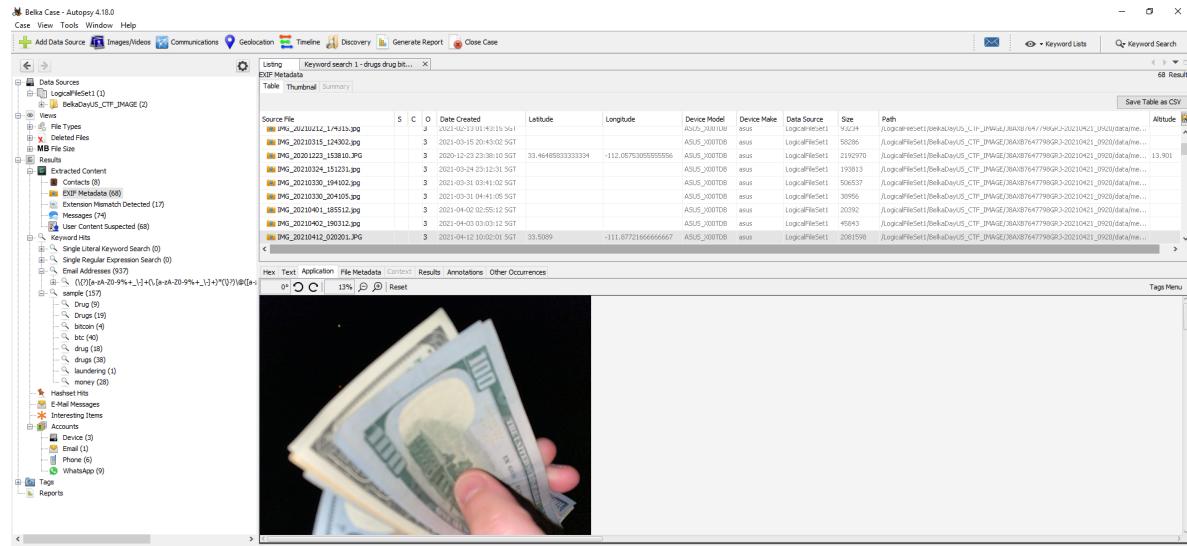


Investigation of Key Artifacts using the Tools

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.

Open Source (Academic Usage)

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.

BelkaSoft Drug Dealing - Autopsy 4.18.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

File Types Deleted Files All (0) MB File Size MD5 Hashes Extracted Content EODF Metadata (68) Extension Mismatch Detected (17) User Content Suspected (68) Keyword Search Single Literal Keyword Search (0) Single Regular Expression Search (0) Email Addresses (861) Hardened Hts Encrypted Images Interesting Items Accounts Tags Reports

Autopsy 4.18.0 - Keyword search 1-drugs bit... | 68 Results

Save Table as CSV

Latitude Longitude

Source File S C O Date Created Device Model Device Make Data Source Size Path

IMG_20210415_200443.jpg	1	2021-04-15 04:04:14.5GT	ASUS_X00TDB	asus	LogicalFileSet1	165109	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20210402_190312.jpg	1	2021-04-03 08:03:12.5GT	ASUS_X00TDB	asus	LogicalFileSet1	59543	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20210412_202010.JPG	1	2021-04-12 10:00:10.5GT	ASUS_X00TDB	asus	LogicalFileSet1	2081598	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st... 33.5089
IMG_20210415_024618.JPG	1	2021-04-15 04:46:18.5GT	ASUS_X00TDB	asus	LogicalFileSet1	3225993	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st... 33.6098

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Balka Case - Autopsy 4.18.0 | 68 Results

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

File Types Deleted Files All (0) MB File Size Results Extracted Content Content (9) Extension Mismatch Detected (17) Messages (74) User Content Suspected (68) Keyword Search Single Literal Keyword Search (0) Single Regular Expression Search (0) Email Addresses (937) Hardened Hts Encrypted Images Interesting Items Accounts Tags Reports

Autopsy 4.18.0 - Keyword search 1-drugs bit... | 68 Results

Save Table as CSV

Latitude Longitude

Source File S C O Date Created Latitude Longitude Device Model Device Make Data Source Size Path

IMG_20200624_151231.jpg	3	2020-06-24 15:12:31.5GT	ASUS_X00TDB	asus	LogicalFileSet1	1460947	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201113_140215.jpg	3	2021-01-13 22:00:15.5GT	ASUS_X00TDB	asus	LogicalFileSet1	62942	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20202212_170315.jpg	3	2021-03-13 01:43:15.5GT	ASUS_X00TDB	asus	LogicalFileSet1	93234	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20203515_120302.jpg	3	2021-03-15 20:43:02.5GT	ASUS_X00TDB	asus	LogicalFileSet1	58286	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201223_153010.JPG	3	2020-12-23 23:30:10.5GT	ASUS_X00TDB	asus	LogicalFileSet1	2192970	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st... 13.901
IMG_20201224_151231.jpg	3	2021-02-24 23:12:31.5GT	ASUS_X00TDB	asus	LogicalFileSet1	193813	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201330_194022.jpg	3	2021-03-01 03:41:02.5GT	ASUS_X00TDB	asus	LogicalFileSet1	506337	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201401_185120.jpg	3	2021-03-01 04:51:20.5GT	ASUS_X00TDB	asus	LogicalFileSet1	39594	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201401_185120.jpg	3	2021-03-01 04:51:20.5GT	ASUS_X00TDB	asus	LogicalFileSet1	45044	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201402_190312.jpg	3	2021-03-03 03:00:12.5GT	ASUS_X00TDB	asus	LogicalFileSet1	3109717	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201412_020301.JPG	3	2021-04-12 10:00:01.5GT	ASUS_X00TDB	asus	LogicalFileSet1	2081598	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st... 33.5089
IMG_20201412_020310.JPG	3	2021-04-12 11:00:10.5GT	ASUS_X00TDB	asus	LogicalFileSet1	3225993	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st... 33.6098
IMG_20201412_140423.jpg	3	2021-04-13 10:40:43.5GT	ASUS_X00TDB	asus	LogicalFileSet1	83048	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20201412_205151.jpg	3	2021-04-13 09:51:51.5GT	ASUS_X00TDB	asus	LogicalFileSet1	395432	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...

Hex Text Application File Metadata Context Results Annotations Other Occurrences

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

Autopsy 4.18.0 - Keyword search 1-drugs bit... | 68 Results

Save Table as CSV

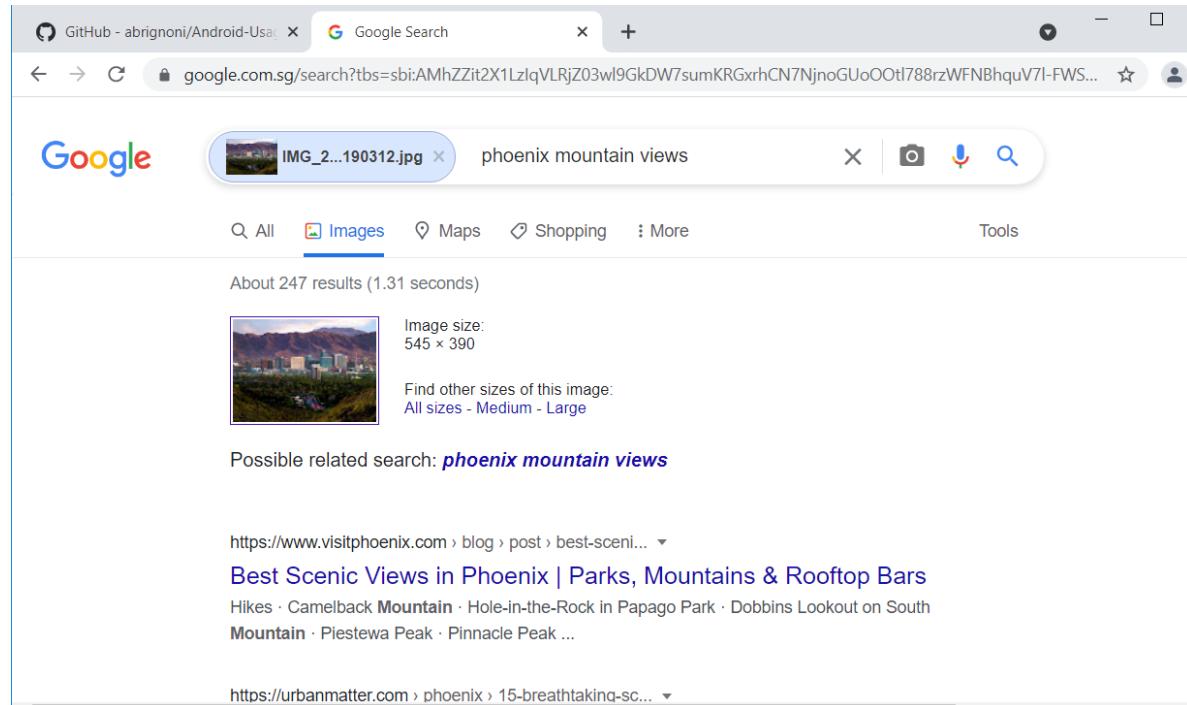
Latitude Longitude

Source File S C O Date Created Device Model Device Make Data Source Size Path

IMG_20210415_200443.jpg	1	2021-04-16 04:04:14.5GT	ASUS_X00TDB	asus	LogicalFileSet1	165109	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20210402_190312.jpg	1	2021-04-03 08:03:12.5GT	ASUS_X00TDB	asus	LogicalFileSet1	59543	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st...
IMG_20210412_202010.JPG	1	2021-04-12 10:00:10.5GT	ASUS_X00TDB	asus	LogicalFileSet1	2081598	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st... 33.5089
IMG_20210415_024618.JPG	1	2021-04-15 04:46:18.5GT	ASUS_X00TDB	asus	LogicalFileSet1	3225993	/LogicalFileSet1/38AxB76477799GRJ-20210421_0920.tar/st... 33.6098

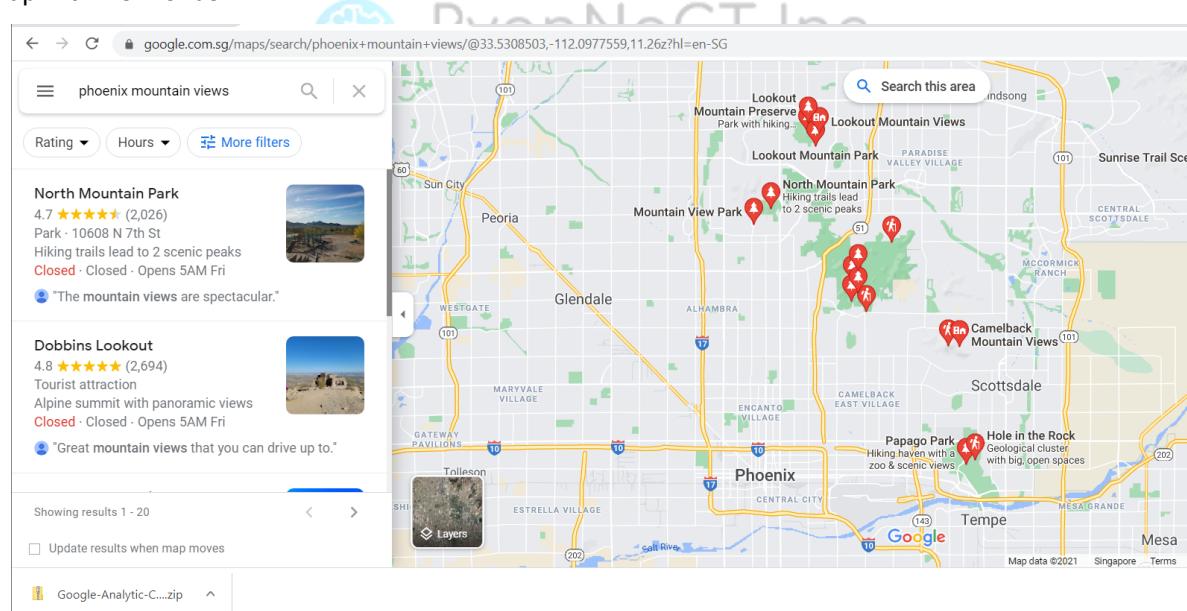
Hex Text Application File Metadata Context Results Annotations Other Occurrences

Open Source (Academic Usage)



Google Images search results for "phoenix mountain views". The search bar shows "IMG_2...190312.jpg" and "phoenix mountain views". The results page shows a thumbnail image of a city skyline with mountains. Below the thumbnail, it says "Image size: 545 x 390" and "Find other sizes of this image: All sizes - Medium - Large". Possible related search: [phoenix mountain views](#). Below the search bar, it says "About 247 results (1.31 seconds)". There are links to "https://www.visitphoenix.com" and "https://urbanmatter.com".

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



Google Maps search results for "phoenix mountain views". The search bar shows "phoenix mountain views". The map displays several locations marked with red pins, including Lookout Mountain Park, North Mountain Park, and Papago Park. Each location has a callout box with a thumbnail image and a brief description. For example, North Mountain Park is described as having hiking trails leading to 2 scenic peaks and being closed. Dobbins Lookout is described as having panoramic views and being a tourist attraction. The map also shows major roads like I-10, I-17, and I-101, as well as various neighborhoods and landmarks.

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

Open Source (Academic Usage)

The screenshot shows a Google search results page. At the top, there are two tabs: "GitHub - abrignoni/Android-Usac" and "Google Search". The search bar contains the query "phoenix townhomes". Below the search bar, there are several navigation links: "All", "Images" (which is underlined), "Maps", "Shopping", and "More". A "Tools" link is located on the right side. The main content area displays the search results. It starts with a thumbnail image of a townhome complex, followed by the text "Image size: 411 x 411" and a link to "Find other sizes of this image: All sizes - Small - Medium - Large". Below this, a link to "Possible related search: phoenix townhomes" is shown. The first result is a link to "https://www.apartments.com > Townhomes > Arizona". The second result is "Townhomes for Rent in Phoenix, AZ - Apartments.com" with a snippet about 136 available units. The third result is "https://www.zillow.com > phoenix-az > rent-townhomes". The fourth result is "Townhomes For Rent in Phoenix AZ - 40 Rentals | Zillow" with a snippet about checking rentals and getting tours.

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

The screenshot shows a Google search results page for "headquarters make a wish phoenix". The interface is similar to the previous one, with tabs for GitHub, Google Search, and the search term "headquarters make a wish phoenix". The "Images" tab is selected. The results show a thumbnail of a building at sunset, with the text "Image size: 882 x 588" and a link to "Find other sizes of this image: All sizes - Small - Medium - Large". Below this, a link to "Possible related search: headquarters make a wish phoenix" is provided. The first result is a link to "https://wish.org > arizona > our-chapter". The second result is "Our Chapter - Make-A-Wish® Arizona" with a snippet about serving the state of Arizona and granting wishes. The third result is "https://www.worldwish.org > contact". The fourth result is "Contact - Make-A-Wish International" with a snippet about Suite 305, Phoenix, Arizona, 85016.

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 screenshot shows the Autopsy interface with a keyword search results table. The search term 'Drug Dealer' is entered in the search bar. The results table has two columns: 'Name' and 'Keyword Type'. The results are as follows:

Name	Keyword Type
drugs	Exact Match
drug	Exact Match
heroin	Exact Match
high	Exact Match
meth	Exact Match
crack	Exact Match

Below the table, there is a note: "Restrict search to the selected data sources: logicalFileSet1". There is also a checkbox for "Save search results". The status bar at the bottom right shows the date and time: 12:20 PM 5/20/2021.

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).

This screenshot shows the same Autopsy interface with a keyword search for 'Drug Dealer'. The results table shows the following data:

Name	Files with Hits
crack (1)	1
drugs (9)	9
drug (19)	19
heroin (1)	1
high (98)	98
meth (5)	5

The status bar at the bottom right shows the date and time: 12:24 PM 5/20/2021.

Open Source (Academic Usage)

base.apk | 4 | new one //This involves «drugs», weapons or regulated | drugs | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | LogicalFileSet1/BelkaDayUS_CTF_1.M

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 84 of 125 Page ⏪ ⏩ Matches on page: 1 of 1 Match ⏪ ⏩ 100% ⏪ ⏩ Reset Text Source

y WhatsApp groupsLLThis invite link no longer works, please contact your bank to get a new one..//This involves **drugs**, weapons or regulated goods##This is abusive, harmful or illegal
This is fraud or a scamXThis is not a verified merchant. For your security, payments to them cannot exceed \$150.VVThis is not your username or pin. This name will be visible to your WhatsApp contacts.
This is spam4This is the default WhatsApp wallpaper48This is the official business account of
WhatsApp



Open Source (Academic Usage)

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.

Page: 1 of 8 Page	Matches on page: 1 of 8 Match	100%	Reset
Text Source: Search Results			
5 1 17693117cfda_997057a5f5b3a3edc 1M8c0mUDRL179EGHBZ9ygOpIZcVEDUvtOp1D68zQnqQVG_aTK4OU9kJF0jC_BPRFkS0 0 Drugs Drugs 0 4194304 0 0 1 1 horatio0.42k@gmail.com 0 0 0 1608785168577 1619903272735 1619903272447 1608785221019 0 0 7 0 0 6 1 178dc9ab8f2_887ba0e332f2f380c 178HE7381WCVw12enH6GE8GmwsVclzQuFqiChLN7-cuHUKILoyVWi3D8N11C4138c1dLaKg 0 Side hustle Side hustle 0 5242880 0 0 1 1 horatio0.42k@gmail.com 0 0 0 1605723905026 1619903272849 1619903272265 1608726871203 0 0 13 0 0			

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.

Page: 1 of 2 Page	Matches on page: 1 of 1 Match	100%	Reset
Text Source: Search Results			
22 6t164o9hcopm0bb2cqy62b3970cm2b3p23134b3m74e68e9p61qmaphc6c 0 0 Take drugs 1 0 1608681600000 Zulu PID 1 0 0 1 0 FREQ=DAILY,UNTIL=20210223T070000Z,NKST=G 1614150000000 1 0 1 1 horatio0.42k@gmail.com 0 6t164o9hcopm0bb2cqy62b3970cm2b3p23134b3m74e68e9p61qmaphc6c@google.com 0 "3239783694586000" 0			

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

Phone Numbers	Name	Keyword Type
<input type="checkbox"/>	drugs	Exact Match
<input type="checkbox"/>	drug	Exact Match
<input type="checkbox"/>	bitcoin	Exact Match
<input type="checkbox"/>	btc	Exact Match
<input checked="" type="checkbox"/> sample	laundering	Exact Match
<input type="checkbox"/>	money	Exact Match

Restrict search to the selected data sources:
LogicalFileSet1

Save search results

Files Indexed: 7,324

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.

Page: 1 of 1 Page	Matches on page: 1 of 11 Match	100%	Reset
Text Source: Search Results			
https://phoenix.craigslist.org/ev1/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/7306534288.html - wtf?? https://phoenix.craigslist.org/ev1/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 6 0 0 1605723905064 1605723954982 0 0 10 1			

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

Listing	boss	Table	Thumbnail	Summary	Save Table as CSV				
Source File	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time	Change Time	File Path
shortcuts.xml				1 .whatsapp.html title=Boss title=0 textId=0	boss	2021-04-21 01:40:40 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\874779\^
wa.db				1 74 3 Boss 2 -1 1 1620120483787 Boss	boss	2021-04-19 18:04:13 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
base.vdex				1 boostedFieldboost@image:boss@boundingBox@pns@... boss	boss	2021-04-18 15:34:59 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
t_en-us_2021-04-25_371253341_100000_index.bin				1 the super bowel firstboss@most powerful doctor in	boss	2021-04-18 22:44:42 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
dialer.db-wal				1 Health CenterBossBossArnie6023... boss	boss	2021-04-20 04:43:44 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
dialer.db				1 4073-3-BH4HD.37894-2B4504D @Boss 0 162005973... boss	boss	2020-12-19 06:28:40 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
contacts2.db				1 0 0 0 0 Boss 40 0 Boss B 2.0 boss	boss	2021-04-20 18:26:19 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
msgstore.db				1 interview, look where my boss hangs 159266992000 200	boss	2021-04-18 21:47:06 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
current_configuration.bin				1 hubbylovelovermanagerBossmothermommemommy	boss	2021-04-19 20:21:55 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
icong_contacts.db-wal				1 37894-2B454D@BossBossBoss+1 239-510-4974+1 (239) boss	boss	2021-04-19 05:10:36 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779
gservices.db-wal				1 op;Riley Touch;Tambour;@BOS5;Touch;TH247;YOU;GUESS boss	boss	2021-04-20 10:03:28 SGT	0000-00-00:00:00:00	0000-00-00:00:00:00	[LogicalFileSet1]\38A\8746779

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



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.

Open Source (Academic Usage)

Screenshot of a digital forensics tool interface showing EXIF metadata for a photo. The table lists file details such as source, date created, device model, make, size, path, latitude, longitude, and ownership status.

Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size	Path	Latitude	Longitude	S	C	O
IMG_021041/_5892.jpg	0			2021-04-18 07:58:02 SGT	ASUS_X00TDB	asus	LogicalFileSet1	149KB	/LogicalFileSet1/8A/B/b9/ /989a/J-021041/_5892.jpg			0		
IMG_20210412_030418.JPG	0			2021-04-12 11:04:18 SGT	ASUS_X00TDB	asus	LogicalFileSet1	3169717	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...	33.465916666666665	-111.87721666666667	0		
IMG_20210416_023643.JPG	0			2021-04-16 10:36:43 SGT	ASUS_X00TDB	asus	LogicalFileSet1	500792	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...	33.506003333333336	-111.87721666666667	0		
IMG_20210416_004343.JPG	0			2021-04-16 08:43:43 SGT	ASUS_X00TDB	asus	LogicalFileSet1	3446592	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...	33.39855	-111.87721666666667	0		
IMG_20210324_151231.jpg	0			2021-03-24 23:12:31 SGT	ASUS_X00TDB	asus	LogicalFileSet1	193813	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...			0		
IMG_20210401_185512.jpg	0			2021-04-02 02:55:12 SGT	ASUS_X00TDB	asus	LogicalFileSet1	20392	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...			0		
IMG_20210412_205151.jpg	0			2021-04-13 04:51:51 SGT	ASUS_X00TDB	asus	LogicalFileSet1	395432	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...			0		
IMG_20210330_204105.jpg	0			2021-03-31 04:41:05 SGT	ASUS_X00TDB	asus	LogicalFileSet1	38956	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...			0		
IMG_20210212_174315.jpg	0			2021-02-13 01:43:15 SGT	ASUS_X00TDB	asus	LogicalFileSet1	93234	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...			0		
IMG_20200824_151231.jpg	1			2020-08-24 23:12:31 SGT	ASUS_X00TDB	asus	LogicalFileSet1	1460847	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...			1		
IMG_20201223_153810.JPG	1			2020-12-23 23:38:10 SGT	ASUS_X00TDB	asus	LogicalFileSet1	2192970	/LogicalFileSet1/8A/B7647799GRJ-20210421_0920.tar/st...	33.464858333333334	-112.0575305555556	1		

Below the table is a preview window showing a portrait photo of a man with a beard. At the bottom, there is a status bar indicating "Analyzing files from LogicalFileSet1" and a zoom level of 100%.

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.



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.

The screenshot shows the Belkasoft Drug Dealing - Autopsy 4.18.0 interface. The main window displays a list of found files, with a total of 481 results. The search query used is: `(\{\})|(x-a-20-9%+,-1)+,(x-a-20-9%+,-1)+|(\{\})#((x-a-20-9)[(x-a-20-9)]*(x-a-20-9))|,(x-a-2) [2,4]`. The results include various file types such as PDFs, images, and documents, many of which are related to WhatsApp or Google services. A sidebar on the left shows categories like File Types, Deleted Files, and User Content Suspected. A bottom status bar indicates the date and time: 5/20/2021 12:15 PM.



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 screenshot shows the Belka Case - Autopsy 4.18.0 interface. The top navigation bar includes Case, View, Tools, Window, Help, and a Keyword Lists section. Below the navigation is a toolbar with icons for Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, and Close Case.

The main workspace displays a search results table titled "Listing" with a "Keyword search : drugs drug bit...". The table has columns for Source File, Hash, Type, Account Type, ID, Data Source, and a "Save Table as CSV" button. A "Thumbnail" view is also available.

The left sidebar contains a tree view of the investigation, including sections for Data Sources (LogicalFileSet (1)), File Types (Word (1), PDF (1), Deleted Files (1), MB file size (1)), Extracted Content (Extracted Content (8)), Contacts (8), EXP Metadata (68), Extended Filesystem Detected (17), Messages (26), User Content Suspected (1), and a large section for Keyword Hunt (Single Literal Keyword Search (0), Single Regular Expression Search (0), Single Regular Expression Search (0)).

The central pane shows the search results for the keyword "drugs drug bit...". The results include various URLs from forums like 4chan and imgur, discussing topics such as Bitcoin, sex games, and upload issues. The results are paginated at 1 of 2 pages.

Open Source (Academic Usage)

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

This screenshot shows a timeline analysis interface with the following details:

- View Mode:** Details
- Date/Time:** 2020-12-23 23:38:10 to 2021-03-19 02:03:43
- Event Type:** Event Log (Evt), WhatsApp Message (Messages)
- Description:**
 - 2020-12-23 23:38:10: asus : ASUS_X00TDB : IMG_20201223_153810.JPG
 - 2020-12-23 23:38:10: asus : ASUS_X00TDB : IMG_20201223_153810.JPG
 - 2021-01-09 11:01:32: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : fuck you!
 - 2021-01-09 11:01:45: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : I HAD to buy bitcoin this summer
 - 2021-01-09 11:01:59: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : if you hadn't discouraged me with your fuckin Bubbles I would've been 5 times richer
 - 2021-01-09 12:44:34: WhatsApp Message : Outgoing to 180842699@atsapp.net : \U0001f917
 - 2021-01-13 22:02:15: asus : ASUS_X00TDB : IMG_20210113_140215.jpg
 - 2021-01-13 22:02:15: asus : ASUS_X00TDB : IMG_20210113_140215.jpg
 - 2021-02-13 01:40:15: asus : ASUS_X00TDB : IMG_20210212_174315.jpg
 - 2021-02-13 01:40:15: asus : ASUS_X00TDB : IMG_20210212_174315.jpg
 - 2021-03-15 20:40:02: asus : ASUS_X00TDB : IMG_20210315_124002.jpg
 - 2021-03-15 20:40:02: asus : ASUS_X00TDB : IMG_20210315_124002.jpg
 - 2021-03-19 01:25:12: WhatsApp Message : Outgoing to 12395104974@atsapp.net : -0.088 btc sent your way. tx 348266821fe7ea8b2fb4a42bbae4ae0cd251733aa2b29e5d675c7451197ca2
 - 2021-03-19 01:25:12: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : -0.088 btc sent your way. tx 348266821fe7ea8b2fb4a42bbae4ae0cd251733aa2b29e5d675c7451197ca2
 - 2021-03-19 02:03:43: WhatsApp Message : Outgoing to 12395104974@atsapp.net : Nice, thanks. Got it
- Tags:** 141 events
- Annotations:** None
- Attachments:** None
- Original Text:** -0.088 btc sent your way. tx 348266821fe7ea8b2fb4a42bbae4ae0cd251733aa2b29e5d675c7451197ca2

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.

This screenshot shows a timeline analysis interface with the following details:

- View Mode:** Details
- Date/Time:** 2020-12-23 23:38:10 to 2021-03-19 02:03:43
- Event Type:** Event Log (Evt), WhatsApp Message (Messages)
- Description:**
 - 2020-12-23 23:38:10: asus : ASUS_X00TDB : IMG_20201223_153810.JPG
 - 2020-12-23 23:38:10: asus : ASUS_X00TDB : IMG_20201223_153810.JPG
 - 2021-01-09 11:01:32: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : fuck you!
 - 2021-01-09 11:01:45: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : I HAD to buy bitcoin this summer
 - 2021-01-09 11:01:59: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : if you hadn't discouraged me with your fuckin Bubbles I would've been 5 times richer
 - 2021-01-09 12:44:34: WhatsApp Message : Outgoing to 180842699@atsapp.net : \U0001f917
 - 2021-01-13 22:02:15: asus : ASUS_X00TDB : IMG_20210113_140215.jpg
 - 2021-01-13 22:02:15: asus : ASUS_X00TDB : IMG_20210113_140215.jpg
 - 2021-02-13 01:40:15: asus : ASUS_X00TDB : IMG_20210212_174315.jpg
 - 2021-02-13 01:40:15: asus : ASUS_X00TDB : IMG_20210212_174315.jpg
 - 2021-03-15 20:40:02: asus : ASUS_X00TDB : IMG_20210315_124002.jpg
 - 2021-03-15 20:40:02: asus : ASUS_X00TDB : IMG_20210315_124002.jpg
 - 2021-03-19 01:25:12: WhatsApp Message : Outgoing to 12395104974@atsapp.net : -0.088 btc sent your way. tx 348266821fe7ea8b2fb4a42bbae4ae0cd251733aa2b29e5d675c7451197ca2
 - 2021-03-19 01:25:12: WhatsApp Message : Incoming from 69982102-ed09-4ea9-a964-d871fcafae628 : -0.088 btc sent your way. tx 348266821fe7ea8b2fb4a42bbae4ae0cd251733aa2b29e5d675c7451197ca2
 - 2021-03-19 02:03:43: WhatsApp Message : Outgoing to 12395104974@atsapp.net : Nice, thanks. Got it
- Tags:** 141 events
- Annotations:** None
- Attachments:** None
- Original Text:** -0.088 btc sent your way. tx 348266821fe7ea8b2fb4a42bbae4ae0cd251733aa2b29e5d675c7451197ca2

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).

Open Source (Academic Usage)

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

The screenshot shows two main sections of the aLEAPP 1.9.2 interface:

- OS Version report:** This section displays the Android version details. The total number of entries is 3. The OS Version is located at C:\Users\maste\Desktop\aleapp_out\ALEAPP_Reports_2021-05-20_Thursday_113913\temp\data\system\usagestats\0\version. The table shows the following data:

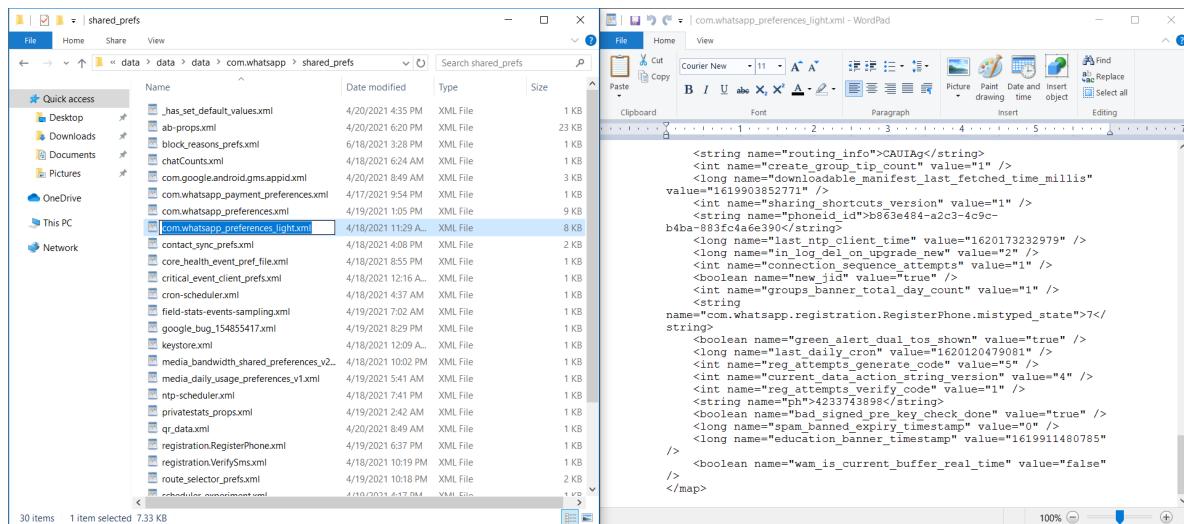
Key	Value
Android Version	9
Build version	cae0d3f014
Codename	REL
- Case Information:** This section provides details about the device. It includes:
 - Android version per Usagestats: 9
 - Codename per Usagestats: REL
 - Build version per Usagestats: cae0d3f014
 - Bluetooth name: ASUS_X00TDB
 - Bluetooth address: 22:22:11:96:C1:49

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,

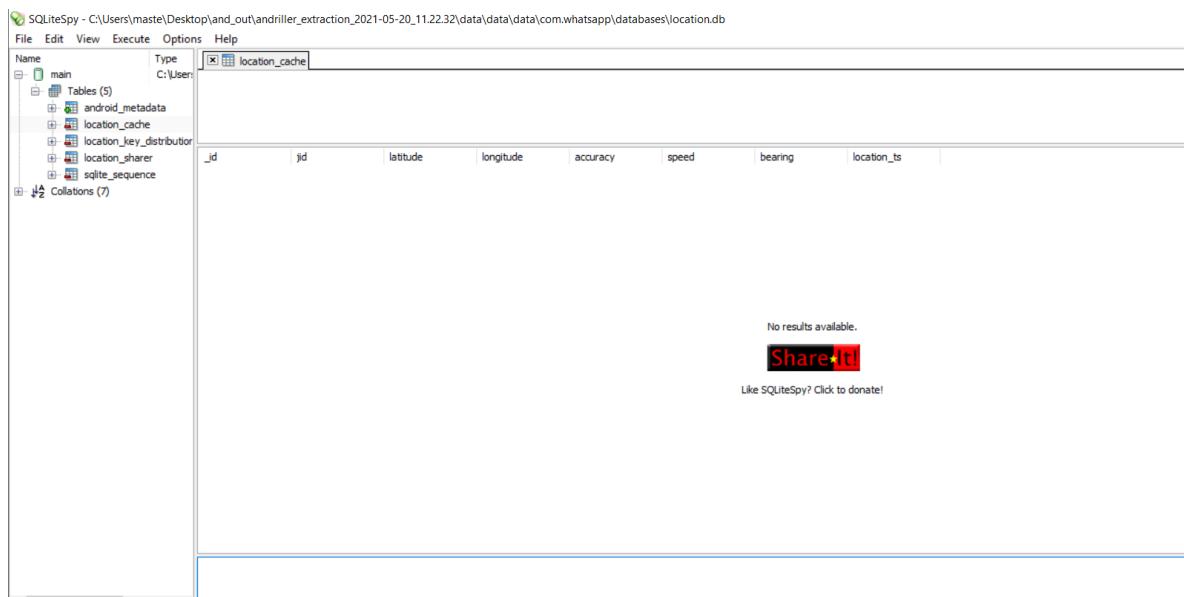
SQLite Spy and Editors

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.

Open Source (Academic Usage)



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 as follows: "<contact_number>@s.whatsapp.net"

Open Source (Academic Usage)

The screenshot shows the SQLiteSpy application interface. The left pane displays a tree view of tables in the 'main' database, including 'away_messages', 'call_log', 'chat', 'chat_list', 'conversion_tuples', 'deleted_chat_job', 'frequent', and 'frequents'. The 'frequents' table is selected, and its data is shown in a grid on the right. The grid has columns: '_id', 'jid', 'type', and 'message_count'. The data is as follows:

_id	jid	type	message_count
1	18084826989@s.whatsapp.net	0	16
2	18084826989@s.whatsapp.net	1	2
3	14012103508@s.whatsapp.net	0	3
5	12395104974@s.whatsapp.net	0	11

Below the grid, there is a smaller window showing the value '1'.

Time: 0.37 ms | 4 returned | SQLite 3.7.8

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)

Open Source (Academic Usage)

The screenshot shows the WhatsApp Viewer interface. On the left is a list of phone numbers with their last message times and message counts. On the right is a detailed view of a specific WhatsApp Chat (ID: 12395104974@.whatsapp.net) from April 12, 2021. The messages are color-coded by sender (green for me, blue for others). A red arrow points to a message from 'Sony! I forgot to take one :((('.

Phone Number	Last Message	Count
12395104974@.whatsapp.net	4/12/2021 - 5:03:00 PM	18 (12)
18084826989@.whatsapp.net	1/9/2021 - 12:44:34 PM	38 (21)
14012103508@.whatsapp.net	11/16/2020 - 12:33:59 PM	8 (5 /)

WhatsApp Chat (12395104974@.whatsapp.net)

- ~0.088 btc sent your way, tx 34826682f1e7a3b2ba482baa4aac0cd25173aa2b29ac5d2675c7451f97ca2
- Nice, thanks. Got it
- <https://ibb.co/album/RThva>
- There are not enough pics.
- Sony! I forgot to take one :(((
- Dont make me suspect you
- Today's photos. All in place <https://ibb.co/album/AMoXhs>
- <https://ibb.co/album/ASpEB>
- payment of 0.0913 btc should be on ur wallet now
- Appreciated
- I see a bit less than that.

Total message count: 64 (38 / 26)

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

The screenshot shows the SQLiteSpy interface with the database file C:\Users\mate\Desktop\and_out\andriller_extraction_2021-05-20_11.22.32\data\data\com.whatsapp\database/msgstore.db. The 'messages' table is selected, showing a list of messages with columns like _id, key_remote_id, key_from_me, key_id, needs_push, data, timestamp, media_url, media_mime_type, media_wa_type, media_size, and media_name. A red arrow points to a message from 'Boss' at timestamp 1589851283000. A green circle highlights the row for message ID 13.

Name	Type	Value
message_system_bubble	object	
message_system_chat_o	object	
message_system_device	object	
message_system_error	object	
message_system_group	object	
message_system_inbox_x	object	
message_system_number	object	
message_system_photo	object	
message_system_value_x	object	
message_template	object	
message_template_button	object	
message_template_quote	object	
message_text	object	
message_thumbnail	object	
message_thumbnal	object	
message_u_elements	object	
message_u_elements_re	object	
message_y_card	object	
message_y_card_id	object	
message_yview_once_me	object	
messages	object	
messages_fts	object	
messages_fts_content	object	
messages_fts_segdr	object	
messages_fts_segments	object	
messages_hydrated_four	object	
messages_links	object	
messages_quotes	object	
messages_quotes_pymw	object	
messages_vcards	object	
messages_vcards_ids	object	
missed_call_log_notifications	object	

Time: 2.03 ms 75 returned SQLite 3.7.8

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)

Open Source (Academic Usage)

The screenshot shows the SQLiteSpy interface with the database file 'com.whatsapp/databases/wa.db' open. The left sidebar lists tables such as main, android_metadata, sqlite_sequence, system_contacts_version, wa_contacts, wa_bit_profiles, wa_bit_profile_categories, wa_bit_profile_hours, wa_bit_profile_websites, wa_bit_list, wa_contact_storage_usage, wa_contacts, wa_group_add_black_list, wa_group_admin_settings, wa_group_descriptions, wa_last_entry_point, wa_props, wa_vnames, and wa_vnames_localized. The right pane displays the 'wa_contacts' table with the following data:

_id	jid	status@broadcast	is_whatsapp_user	status	status_timestamp	number	raw_contact_id	display_name	ph...	company	phone_label	unseen_msg_c
1	status@broadcast	1	Hey there! I am using WhatsApp.	0	+18084826889	1	Anne	2	Alice			
3	1808482689@.whatsapp.net	1		0	+16023448011	5	Valleywise Heal...	2				
4	16023448011@.whatsapp.net	0		0	+12395104974	3	Boss	2				
5	12395104974@.whatsapp.net	1	Hey there! I am using WhatsApp.	0								
6	1401210350@.whatsapp.net	1	Hey there! I am using WhatsApp.	0								

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 screenshot shows the SQLiteSpy interface with the database file 'com.android.chrome\app_chrome\Default\History' open. The left sidebar lists tables such as main, downloads, downloads_slices, downloads_url_chains, keyword_search_terms, meta, segment_usage, segments, sqlite_sequence, typed_url_sync_metadata, urls, visit_source, visits, and visit_uris. The right pane displays the 'segments' table with the following data:

id	name	url_id
1	http://imgbb.com/	38
2	http://maps.google.com/	43
3	http://pornhub.com/	47
4	http://lb.co/upload	79
5	http://imgbb.com/upload	81

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).

The screenshot shows the imgbb.com website. At the top, there are navigation links for 'About', 'EN', and 'imgbb'. On the right, there are buttons for 'Upload', 'Sign in', and 'Create account'. Below the header, a large text area says 'Upload and share your images.' with a sub-instruction 'Drag and drop anywhere you want and start uploading your images now. 32 MB limit. Direct image links, BBCode and HTML thumbnails.' A blue 'START UPLOADING' button is centered below this text.

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).

Name	Type	File	
main	Table	C:\User	
Tables (12)			
downloads	Table		
downloads_slices	Table		
downloads_ur_chans	Table		
keyword_search_terms	Table		
meta	Table		
segment_usage	Table		
segments	Table		
sqlite_sequence	Table		
typed_url_sync_metadata	Table		
urls	Table		
visit_source	Table		
visits	Table		
Collations (7)			
urls	Table		
id	url	title	
visit_count	typed_count	last_visit_time	
hidden			
1 https://www.google.com/search?q=ph... phoenix news - Google Search	3	0	0
2 https://www.abc15.com/ Phoenix, Arizona News and Weather ABC15 Arizona	1	0	0
3 https://www.fox10phoenix.com/ FOX 10 Phoenix	2	0	0
4 https://www.google.com/search?q=crai... craigslist - Google Search	1	0	0
5 https://www.craigslist.org/ craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	1	0	0
6 https://geo.craigslist.org/ craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	1	0	0
7 https://phoenix.craigslist.org/ craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	2	0	0
8 https://phoenix.craigslist.org/d/jobs/se... craigslist: phoenix, AZ jobs, apartments, for sale, services, community, and events	2	0	0
9 https://phoenix.craigslist.org/ph/etc/d... ▶ PART TIME DRIVER IMMEDIATE START \$1,000 BONUS ★ - et cetera -...	1	0	0
10 https://phoenix.craigslist.org/ph/etc/d... phoenix jobs "temp job" - craigslist	2	0	0
11 https://phoenix.craigslist.org/ph/etc/d... +Deliver with DoorDash and Earn Up to \$19 /Hr * - et cetera - job...	1	0	0
12 https://phoenix.craigslist.org/ph/etc/d... phoenix jobs "temp job" - craigslist	2	0	0
13 https://phoenix.craigslist.org/ph/fab/d... +Deliver with DoorDash and Earn Up to \$19 /Hr * - general labor - job...	1	0	0
14 https://phoenix.craigslist.org/ph/etc/d... phoenix jobs "temp job" - craigslist	1	0	0
15 https://phoenix.craigslist.org/ph/etc/d... phoenix jobs "temp job" - craigslist	1	0	0
16 https://phoenix.craigslist.org/ph/etc/d... phoenix jobs "temp job" - craigslist	2	0	0
17 https://phoenix.craigslist.org/v/fab/d/... The Hiring Event at Chevy Is Blooming! Full Time Benefits Included!...	1	0	0
18 https://phoenix.craigslist.org/ph/etc/d... phoenix jobs "temp job" - craigslist	2	0	0
19 https://phoenix.craigslist.org/ph/fab/d... Earn Up To \$19/Hr - Be Your Own Boss - DoorDash Driver - food /...	1	0	0
20 https://phoenix.craigslist.org/ph/etc/d... phoenix jobs "real estate" - craigslist	2	0	0
21 https://phoenix.craigslist.org/housing... phoenix housing "real estate" - craigslist	4	0	0
22 https://phoenix.craigslist.org/ph/etc/d... Phoenix Home In Good Condition - real estate - by owner - apartment...	1	0	0
23 https://phoenix.craigslist.org/v/reb/d... Home for Sale in Buckeye, (480 284/1980) - real estate - by broker -...	1	0	0
phoenix jobs "temp job" - craigslist			

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.

_id	key	value
-2140311132	timezoneDatabaseVersion	2020d
-495220580	timezoneInstancesPrevious	America/Phoenix
1126213331	timezoneType	home
1167965829	timezoneInstances	America/Phoenix

In addition, we can also see the calendar schedule.

_id	_sync_id	dirty	mutators	calendar_id	title	eventLocation	description	eventColor	even
1	60ggpp661h3eb965h6zb9k6...	0	0	1	Pay rent	Local Wendy's			
2	6djhkhcor6z829n9qgq6970...	0	0	1	Gym leg day	1625 W Comeback Rd			
3	6cp4dhkpc62bb6c4o9zb9k6...	0	0	1	Gym back/core day	1625 W Comeback Rd			
4	689jedc6sc4qd9j9;4q9p965h...	0	0	1	Gym chest day	1625 W Comeback Rd			
5	61jaep250a30b9nhqgq69kcl...	0	0	1	Spanish class	5107 N 7th St #2			
6	cdf3ge96t832969nmab9k6...	0	0	1	Job interview	33.46116965354126, -112.09162528863925			
7	75geob56gpb4713b9k6...	0	0	1	Dad's bd	Di vany coffee karaoke			
8	646ae1ckdgfb9ndqgb9kcl...	0	0	1	Pizza delivery	33°32'56.2"N 112°06'22.5"W			
9	6kogedp60a2b9p93eb9kseq...	0	0	1	Barber	Bethany Marketplace			
10	6qogmap9mch3b9qckq4b9k6...	0	0	1	Kitten feeding	33.52837064473933, -111.99877430841748			
11	6qogmap9mch3b9qckq4b9k6...	0	0	1	Job interview at Flower Child	100 E Comeback Rd			
12	6qogjac32cb2b670q7ab9k...	0	0	1	Pizza delivery	33°32'16.4"N 112°07'11.9"W			
13	65h2c965pm6bb5b57073b9k...	0	0	1	Swag up	Christown spectrum			
14	71j38p174n3d9n174mb9k...	0	0	1	Swag up	Christown spectrum			
15	cdf7ob36430b4e4b96b9k...	0	0	1	Pick groceries	5838 W Olive Ave Ste c101			
16	74o36d2653abb1clm4b9k6...	0	0	1	Date, Marie	33.4490116, -112.0778212, 14.56			
17	cd3acp653b9g6g6tb9k6fh...	0	0	1	Pizza delivery	33.508146, -112.148462			
18	cpgn8p1m71g12b9k616zb9k...	0	0	1	kitten feeding	33.512097861571306, -112.05513469849355			
19	c40sae626aa30bb4c56zb9k...	0	0	1	Date w Isabella	33.4490116, -112.0778212, 14.56			
20	60538c34cp6p9b6t6b9k6...	0	0	1	Doctor's appointment	2601 E. Roosevelt St.			
21	6dhy1p668p6bb5b2zb9k...	0	0	1	Take drugs				
22	6t649p26phn69p706zb9k...	0	0	1	Job interview at GameStop	1703 W Bethany Home Rd			

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.

_id	user_id	uid	root_alias	cert_path	cert_serial
1	0	10010	GoogleCloudKe...	30 82 08 5D 30 82 05 1A 30 82 03 02 A0 03 02 01	10005

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.

Hex to ASCII Text Converter

Enter hex bytes with any prefix / postfix / delimiter and press the *Convert* button.

(e.g. 45 78 61 6d 70 6C 65 21):

Paste hex numbers or drop file

30 82 08 5D 30 82 05 1A 39 82 30 02 A0 03 02 01

Character encoding

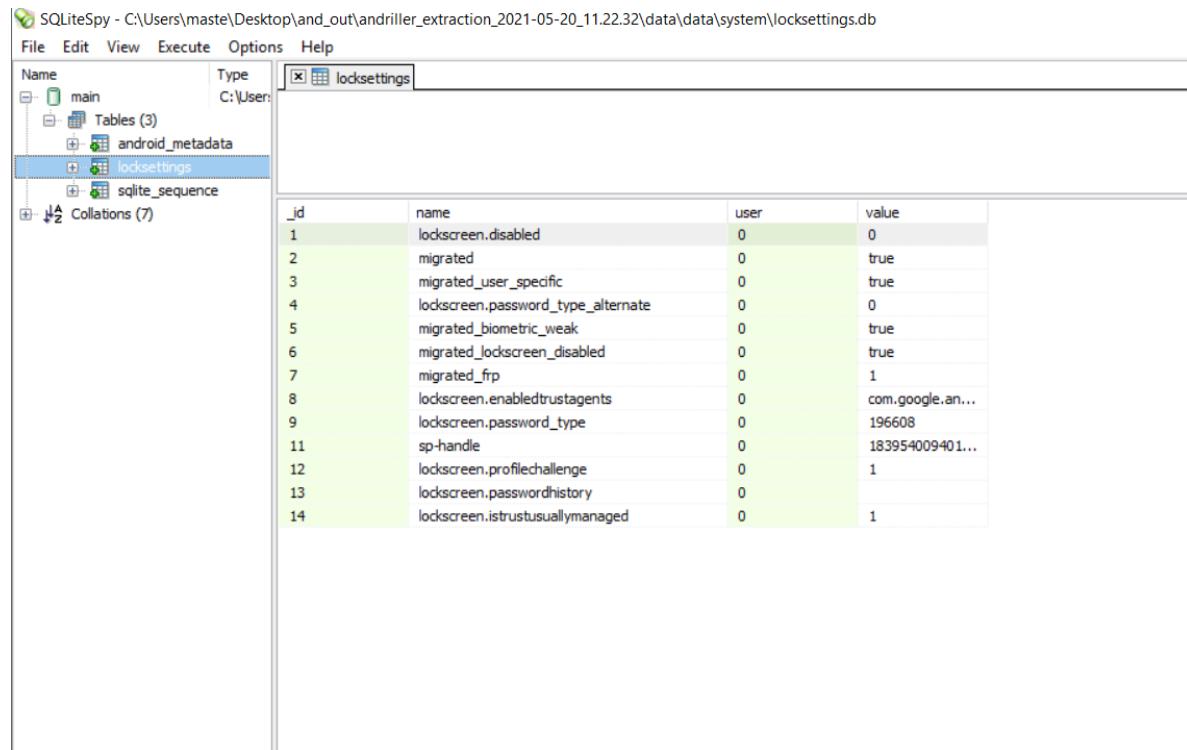
ASCII

Convert Reset Swap

Inc. THAI

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

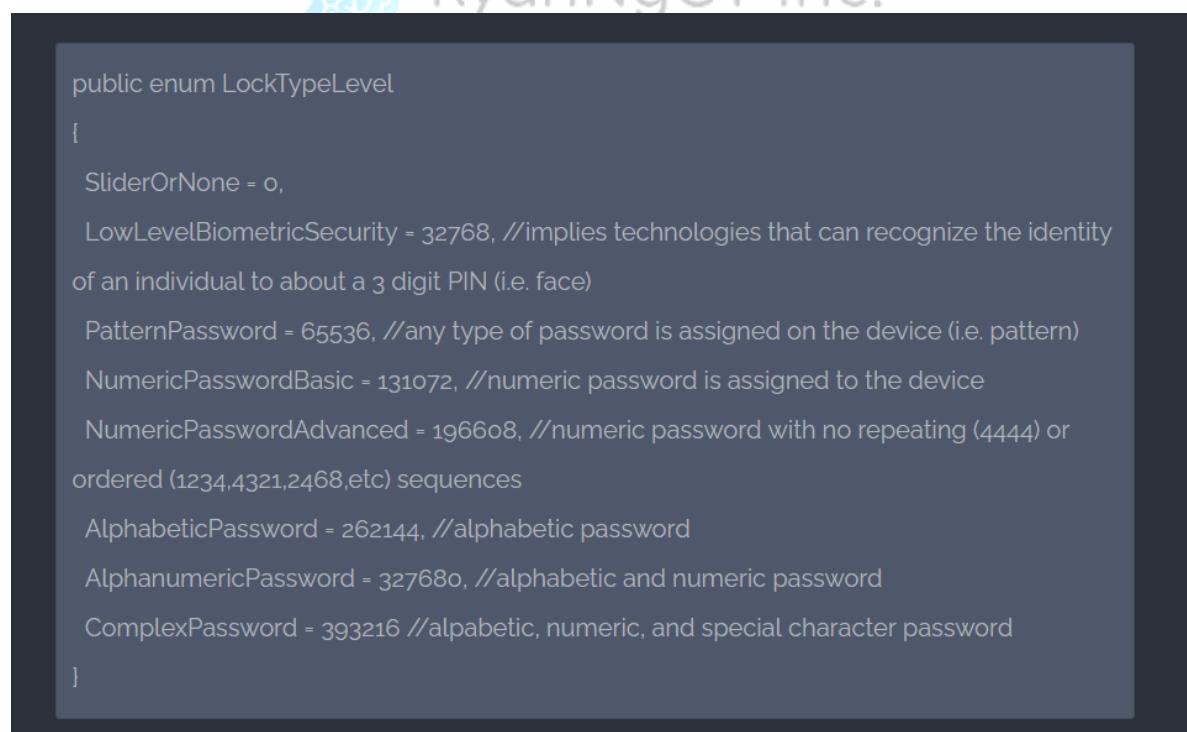
Open Source (Academic Usage)



The screenshot shows the SQLiteSpy application interface. The left pane displays the database schema with tables: main, android_metadata, locksettings, and sqlite_sequence. The right pane shows the contents of the locksettings table.

_id	name	user	value
1	lockscreen.disabled	0	0
2	migrated	0	true
3	migrated_user_specific	0	true
4	lockscreen.password_type_alternate	0	0
5	migrated_biometric_weak	0	true
6	migrated_lockscreen_disabled	0	true
7	migrated_frp	0	1
8	lockscreen.enabledtrustagents	0	com.google.an...
9	lockscreen.password_type	0	196608
11	sp-handle	0	183954009401...
12	lockscreen.profilechallenge	0	1
13	lockscreen.passwordhistory	0	
14	lockscreen.istrustusuallymanaged	0	1

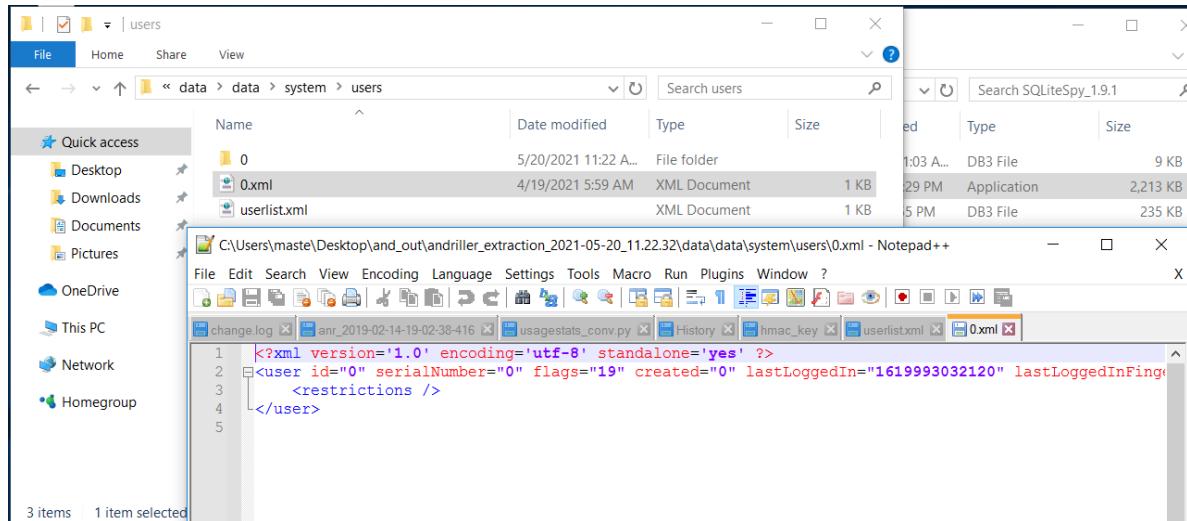
The data show that the lockscreen is enabled but with a weak migrated biometric lock. Referring to this article below and the password type, it is likely that a numeric password or pin was used (without repetition of numbers).



```
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.

Version	Name	User Status	Country Code	Mobile Number
2.21.8.17	Derek Hor	Hey there! I am using WhatsApp.	1	4233743898
			Country Code	Mobile Number

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)

Send Timestamp	Received Timestamp	Message ID	Recipients	Direction	Content	Group Sender	Activate Go to Sett
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 34826682fe7aa8b2fba482baa4aac0cd251733aa2b29ac5d2675c7451f97ca2	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://bb.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://bb.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://bb.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://bb.co/album/Y0vt6f	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://bb.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://bb.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	

Google Chrome History

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/ ?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/ ?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/ ?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/ ?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/rea/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.

1601-01-01 00:00:00	https://www.google.com/search?q=my+knee+hurts&rlz=1C1GCEUwAEAYADICAAQsQMyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAOgQIABBD0gQILhBD0gsILhCxAxDHA RC0JaoGCAAQBXAeOgUILhCxAz0CC046BwgUELEDEENQnxlY8Czg5TjoAHAAeACAAeACIAGEEEJIBazt0ugBAKABAcABAQ&scilnt=mobile-gws-wiz-serp#sbffu=1&rlz=my%20knee%20hurts	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&rlz=1C1GCEUwAEAYADICAAQsQMyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAOgQIABBD0gQILhBD0gsILhCxAxDHA RC0JaoGCAAQBXAeOgUILhCxAz0CC046BwgUELEDEENQnxlY8Czg5TjoAHAAeACAAeACIAGEEEJIBazt0ugBAKABAcABAQ&scilnt=mobile-gws-wiz-serp#sbffu=1&rlz=my%20knee%20hurts	my knee hurts - Google Search	1
1601-01-01 00:00:00	https://www.google.com/search?q=knee+clinic+phoenix&rlz=1C1GCEUwAEAYADICAAQsQMyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAOgQIABBD0gQILhBD0gsILhCxAxDHA RC0JaoGCAAQBXAeOgUILhCxAz0CC046BwgUELEDEENQnxlY8Czg5TjoAHAAeACAAeACIAGEEEJIBazt0ugBAKABAcABAQ&scilnt=mobile-gws-wiz-serp#sbffu=1&rlz=my%20knee%20hurts	knee clinic phoenix - Google Search	2

Open Source (Academic Usage)

1601-01-01 00:00:00	https://www.google.com/search?q=knee+clinic+phoenix&ei=hqKQYJ6pJcTU9APXlamgCA&oq=knee+clinic+phoenix&gs_lcp=ChNtb2JpbGUTZ3dzLXdpe1zZXJwEAMyB0gheKAEBMgUIIRCgATIFCEQqw16BaAEEe6BQgpELEDogIJKToCAAQ6gIQjwE6BaAEEem6AggAOgsILhCXDHARCIajpCFAAQOkQl6BQgAELEDogglCxAxCDAToECAAOQjpCFAAQyQM6CAgUEmcBEK8BQgc1ABDJAXANQgIABAN0gqILhDHARCVARCTAjpCFAAQOkhAEogkIABDJAXAVWEB46BwgheA0QgAe6CAgheBYQHRAeOggIBABAIEAOQHjpCFAAQhgNQKRZT7Y8BYKGTAWgGcAF4AIAB2gKIAy0kgEGMl0xNS44mAEEoAEBsAESyAEiWAEB&client=mob ille-gws-wiz-serp#ip=1&sfbou=1&p=knee%20clinic%20phoenix	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=ChNtb2JpbGUTZ3dzLXdpe1zZXJwEAMyB0gheKAEBMgUIIRCgATIFCEQqw16BaAEEe6BQgpELEDogIJKToCAAQ6gIQjwE6BaAEEem6AggAOgsILhCXDHARCIajpCFAAQOkQl6BQgAELEDogglCxAxCDAToECAAOQjpCFAAQyQM6CAgUEmcBEK8BQgc1ABDJAXANQgIABAN0gqILhDHARCVARCTAjpCFAAQOkhAEogkIABDJAXAVWEB46BwgheA0QgAe6CAgheBYQHRAeOggIBABAIEAOQHjpCFAAQhgNQKRZT7Y8BYKGTAWgGcAF4AIAB2gKIAy0kgEGMl0xNS44mAEEoAEBsAESyAEiWAEB&client=mob ille-gws-wiz-serp#ip=1&sfbou=1&p=knee%20clinic%20phoenix	knee clinic phoenix - Google Search	1
1601-01-01 00:00:00	https://www.google.com/search?q=phoenix+clinic&ei=p6KQYJ27BznIOPEPj-GksAw&oq=phoenix+cli&gs_lcp=ChNtb2JpbGUTZ3dzLXdpe1zZXJwEAEYADfCAAQkQlyAggAMgIIADICCAAYAggAMgIIADICCAAYAggA0gQIABBH0gIKToF0CQkQsQM6CAgAEo0CEiB0gqILhCRAhCTAjpCC4QxwEQow16CvguELEDEMcBEKM0C0gQlABBD0gUiABCxAz0ECC4QQzohCAAQsQM0QzohFCC4QsQM0xwxEQwxEQkQl6DgguELEDEIMBEMC0ggIABCxAdJAzoFOAAQkgM6CgggELEDEIMBEEM6BwgueLEDEEM6CQgUEmcBEK8B0gIIJjoOCC4QsQM0xwxEQwxEQkQl6DgguELEDEIMBEMC0ggIABCxBU1QWOZFYKZnsAJwAxgAHLAogBxxmSAQuyLtcuNjgBAKABAbEgBCMABAQ&scilent=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.imgur.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

Open Source (Academic Usage)

1601-01-01 00:00:00	https://horatio420.imgur.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/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

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

Open Source (Academic Usage)

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!1s0x872b6d94fe06ba2d0x248453ff6ed539ad	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!1s0x872b13f49a3cd2b1:0x2cf437234cb6e56e	Pho 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/@33.525515,-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,-112.1157363,13z	OZ Bar - Google Maps	1
1601-01-01 00:00:00	https://www.google.com/maps/place/Redbox,+West+Bethany+Home+Road,Glendale,+AZ/@33.52452,-112.09845,17z/data=!4m2!3m1!1s0x872b132b2ace7cab:0x3dc0d8797e1cb658f	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/@33.664504,-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/@33.487751,-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,-112.21166176,17z/data=!4m2!3m1!1s0x872b6ccb9a5f0b9:0xa784537d2ce36ba	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,-112.21174988,17z/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!1s0x872b6cc72fd82455:0xd091c37c71a38c3	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.

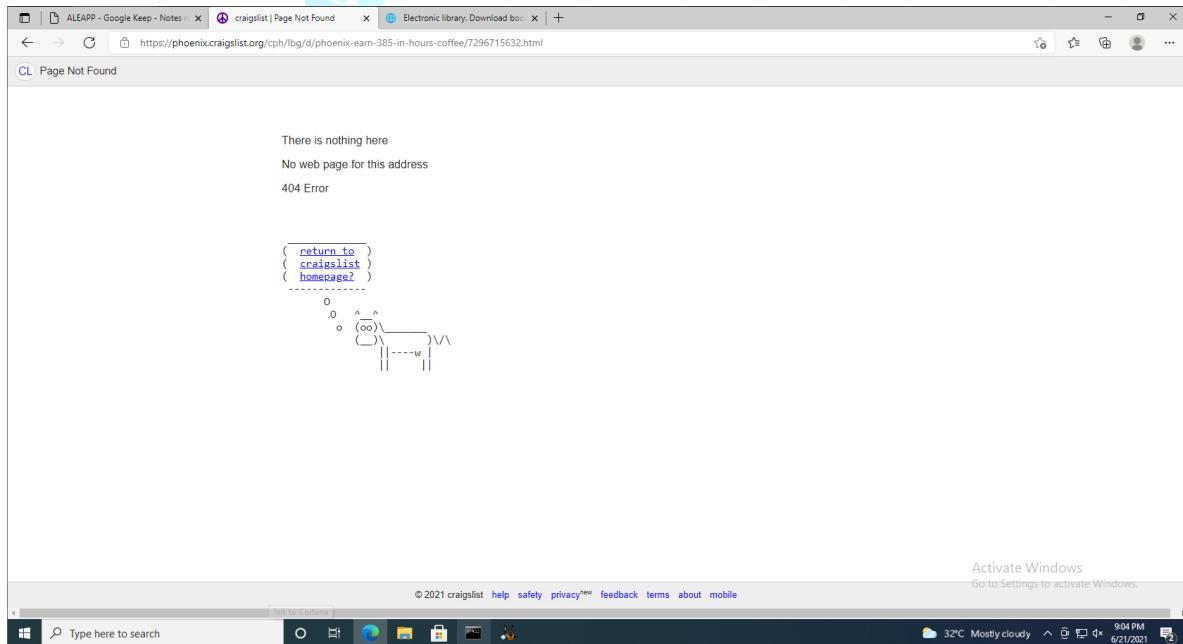
Google Keep - Notes report

Total number of entries: 6

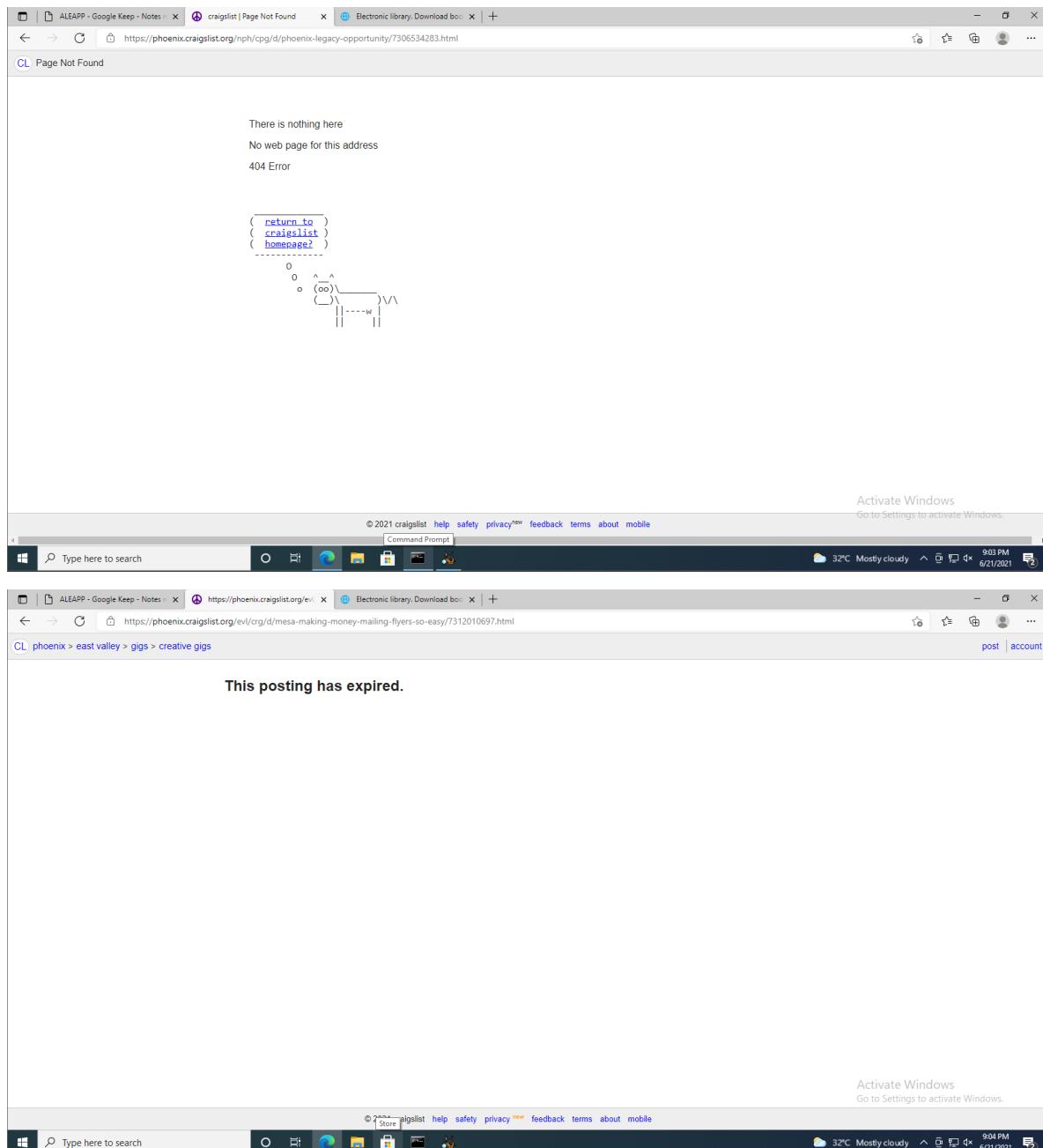
Google Keep - Notes located at: C:\Users\25ezr\Downloads\BelkaDayUS_CTF_IMAGE\V8AXB7647798GRJ-20210421_0920\data\data\com.google.android.keep\databases\keep.db

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	horatio.042k@gmail.com	Side hustle	\$400 in 2 hours. drugs again? wtf?? easy but low paid night job	\$400 in 2 hours. drugs again? wtf?? easy but low paid night job	False	horatio.042k@gmail.com
2020-12-17 07:57:13	2020-12-17 07:57:13	1	horatio.042k@gmail.com		04049 19810 47697 72485 91554 88046	04049 19810 47697 72485 91554 88046	False	horatio.042k@gmail.com
2020-12-24 04:46:05	2020-12-24 04:47:58	5	horatio.042k@gmail.com	Drugs	Chondroitin Sulfate 600mg - 2 per day PERCUTANE Pain Relief Cream - evening	Chondroitin Sulfate 600mg - 2 per day PERCUTANE Pain Relief Cream - evening	False	horatio.042k@gmail.com
2021-01-12 11:54:49	2021-01-12 11:54:49	3	horatio.042k@gmail.com	Secrets	762-n1BHKYU_L_&7JK7Dx2Pj#HkUNT_~TTJWuSx4'Zl 4pf5p@C@EXZ4RH puJ87RHMfbU3Vz_Pbf+~	762-n1BHKYU_L_&7JK7Dx2Pj#HkUNT_~TTJWuSx4'Zl 4pf5p@C@EXZ4RH puJ87RHMfbU3Vz_Pbf+~	False	horatio.042k@gmail.com
2021-01-14 13:46:21	2021-01-14 13:46:39	4	horatio.042k@gmail.com		https://bok.co/	https://bok.co/	False	horatio.042k@gmail.com
2021-04-15 19:43:54	2021-04-15 19:47:12	2	horatio.042k@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	horatio.042k@gmail.com

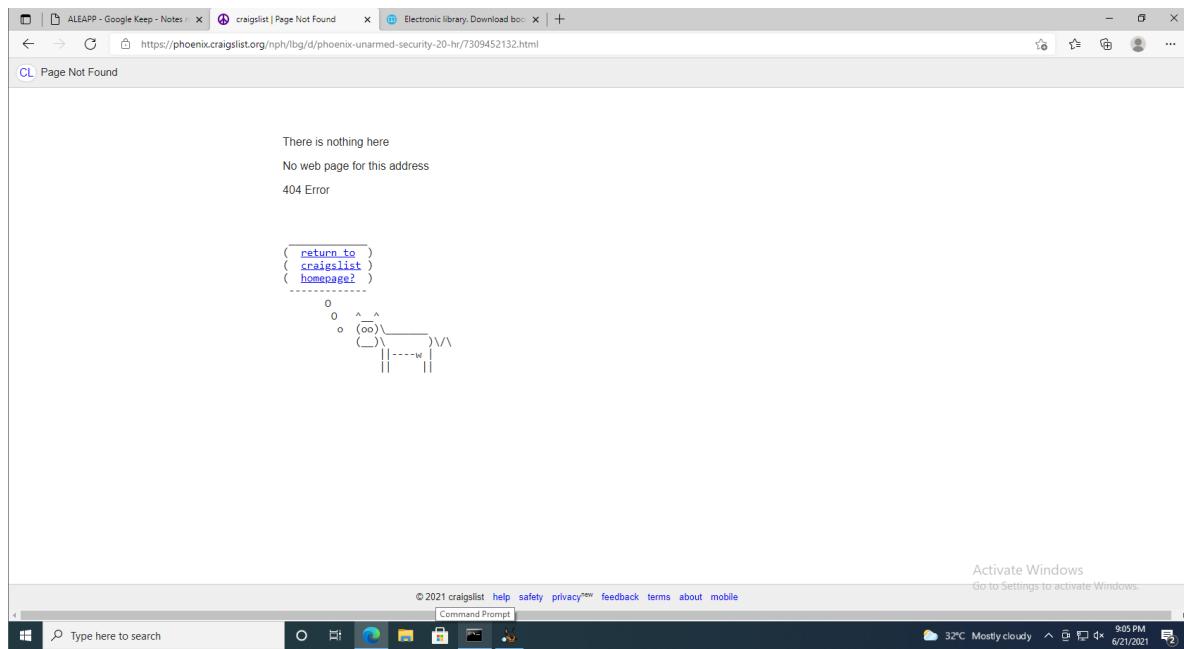
The first note contained 4 links relating to the job listings he found on Craigslist within Phoenix, AZ. However, all the links were already invalid.



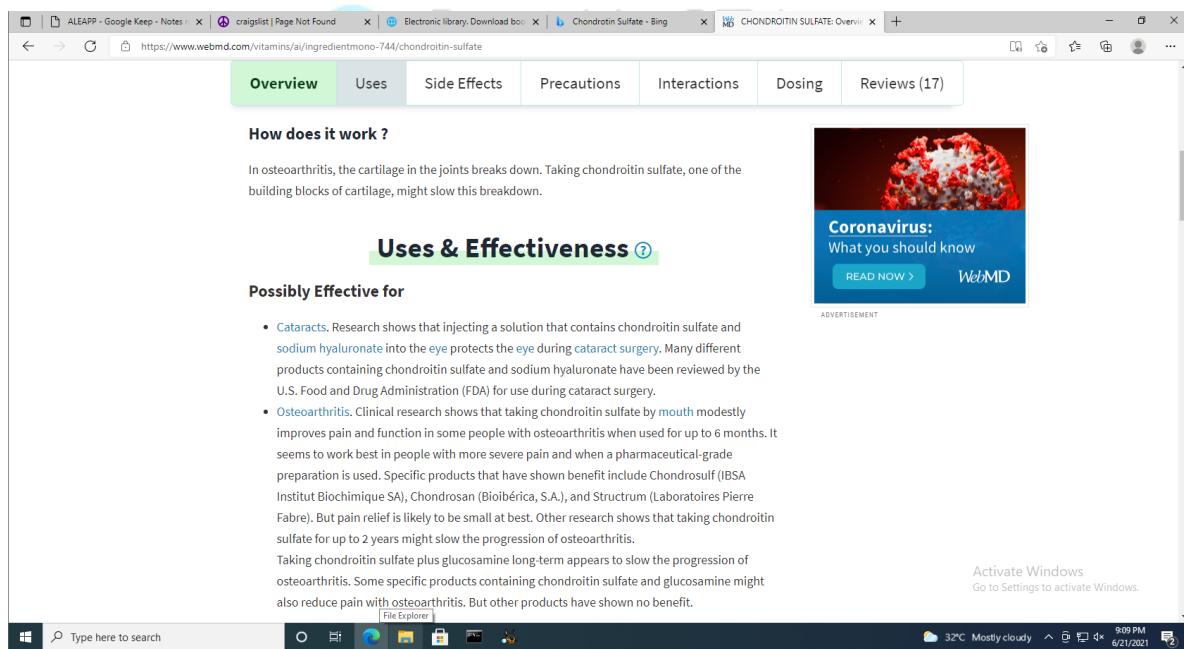
Open Source (Academic Usage)



Open Source (Academic Usage)



The third note contains a drug called “Chondroitin 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.

Open Source (Academic Usage)

The screenshot shows a web browser window with multiple tabs open. The active tab is for the Z-Library website, which is described as "The world's largest ebook library". The page includes a search bar with options for "General Search" and "Fulltext Search", and a "Search" button. Below the search bar, there is a "Most Popular" section displaying several book covers, including "My Policeman" by Bethan Roberts, "SOCIAL PSYCHOLOGY" by Daniel W. Fazio et al., "KINGDOM OF THE WICKED" by K.W. Jeter, and "EGO IS THE ENEMY" by Ryan Holiday. To the right of the search area, there is a sidebar with a weather forecast for 32°C Mostly cloudy and a link to activate Windows. The browser's address bar shows the URL https://sg1lib.org. The taskbar at the bottom of the screen includes icons for the Start button, search, Task View, File Explorer, Edge browser, Google Play Store, and Settings.



Open Source (Academic Usage)

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/AKppINYYFUljXGrlyBoYjmCfROE86YrKCZSGRhNvpclFQ1odXCxzPRjykxNjvrwDGOX3skvwhQ93ETrqS1Dc9TleY9SpfxNueck5oc3Ne7R3j7_paY0JJSQCucRkwPVK52bN9sQL45qHMvlspqROCPihuakcKlk8-YbgBtzYH93qeNv9a8tWalYwxQWNgD_z_3pqXPi	
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).

The screenshot shows the ALEAPP 1.9.2 application interface. On the left, there is a sidebar with the following menu items: CONTACTS, DEVICE INFO, GOOGLE PLAY, INSTALLED APPS, PERMISSIONS, and a few collapsed sections. The 'INSTALLED APPS' section is currently selected and expanded, showing a list of installed applications under the 'Bundle ID' heading. The listed apps include com.android.chrome, com.android.vending, com.cmidevelop.whatshack, com.google.android.apps.turbo, com.google.android.apps.wellbeing, com.google.android.googlequicksearchbox, com.google.android.keep, com.google.android.soundpicker, com.google.android.tts, com.topjohnwu.magisk, com.whatsapp, net.mullvad.mullvadvpn, and org.thoughtcrime.securesms.

Bundle ID
com.android.chrome
com.android.vending
com.cmidevelop.whatshack
com.google.android.apps.turbo
com.google.android.apps.wellbeing
com.google.android.googlequicksearchbox
com.google.android.keep
com.google.android.soundpicker
com.google.android.tts
com.topjohnwu.magisk
com.whatsapp
net.mullvad.mullvadvpn
org.thoughtcrime.securesms

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?
						Nah, didnt you read the news? https://www.accentral.com/story/entertainment/dining/2020/06/19/these-metro-phoenix-restaurants-closed-permanently-due-covid-19/3211019001/
msgstore.db	WhatsApp Message	2020-06-20 09:23:30 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	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!



Open Source (Academic Usage)

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.

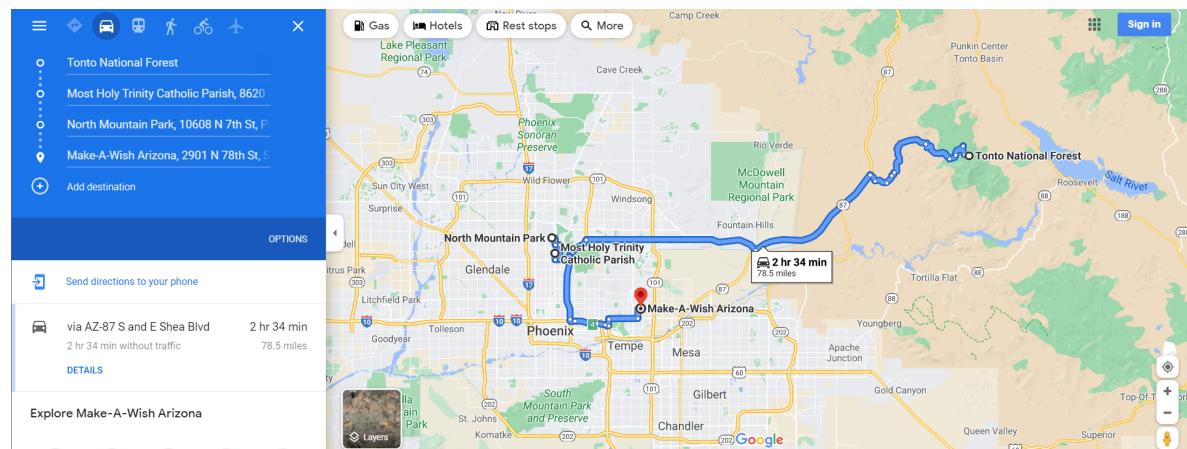
Source File	Message Type	Date/Time	Direction	From Phone Number	To Phone Number	Data Source
msgstore.db	WhatsApp Message	2021-01-09 11:01:45 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fcfa6a628	I HADD to buy bitcoin this summer
msgstore.db	WhatsApp Message	2021-01-09 11:01:59 SGT	Incoming	18084826989@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fcfa6a628	i hadn't discouraged me with your fuckin Bubbles I wouldve been 5 times ricerr
msgstore.db	WhatsApp Message	2021-01-09 12:44:34 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fcfa6a628	18084826989@s.whatsapp.net	↖(˘)↖

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.

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-d871fcfa6a628	12395104974@s.whatsapp.net	LogicalFileSet1
						*.088 btc sent your way, tx 34826682f1e7aa8b2fba482baa4aac0cd25173aa2b29a5d2675
msgstore.db	WhatsApp Message	2021-03-19 01:25:12 SGT	Incoming	12395104974@s.whatsapp.net	69982102-ea09-4ea9-a964-d871fcfa6a628	7451f97ca2
msgstore.db	WhatsApp Message	2021-03-19 02:03:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fcfa6a628	12395104974@s.whatsapp.net	Nice, thanks. Got it
msgstore.db	WhatsApp Message	2021-04-12 18:26:32 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fcfa6a628	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-d871fcfa6a628	There are not enough pics.
msgstore.db	WhatsApp Message	2021-04-14 02:26:43 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fcfa6a628	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-d871fcfa6a628	Dont make me suspect you
msgstore.db	WhatsApp Message	2021-04-14 04:27:17 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fcfa6a628	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-d871fcfa6a628	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-d871fcfa6a628	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-d871fcfa6a628	12395104974@s.whatsapp.net	Appreciated
msgstore.db	WhatsApp Message	2021-04-16 04:27:27 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fcfa6a628	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-d871fcfa6a628	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-d871fcfa6a628	yes.
msgstore.db	WhatsApp Message	2021-04-16 18:35:30 SGT	Outgoing	69982102-ea09-4ea9-a964-d871fcfa6a628	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-d871fcfa6a628	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-d871fcfa6a628	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-d871fcfa6a628	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>

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.

Conclusion

ORIGINAL

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.



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/>



END