

INCIDENT RESPONSE & DIGITAL FORENSICS

REPORT OF THE FORENSIC INVESTIGATION ON HEISENBERG'S ANDROID PHONE

BY

JIWUEZE BRIGHT CHUKWUEBUKA

SUBMITTED TO

THE DEPARTMENT OF CYBER SECURITY

**HOCHSCHULE DER BAYERISCHEN WIRTSCHAFT
(HDBW)**

**IN PARTIAL FULFILMENT FOR THE AWARD OF M.SC IN
CYBER SECURITY**

On 20th July 2021, at about 7pm, Heisenberg was arrested by the police and was charged with the offense of car theft.

He had an android phone that was presented for forensic investigations.

I used the following tools for the investigations.

- ALEAPP ANDROID FORENSIC TOOL: An open-source forensic tool designed to extract evidence from android phones, it uploads the extracted information and displays it on a web browser. <https://github.com/abrignoni/>
- AUTOPSY: A digital platform that provides graphical interface for forensic investigation. <https://www.autopsy.com/>

INVESTIGATION DETAILS

This phase contains answers to questions outlined for the investigation process.

Firstly, I uploaded the extracted folder to ALEAP, and it opened automatically on a web browser, where I got a user interface to commence my investigation.

Understand that ALEAP as well as AUTOPSY interfaces have two divisions. From the viewer's perspective, the left side of the screen are directories you can click on to perform searches, while the right side of the screen will always provide answers to your searches.

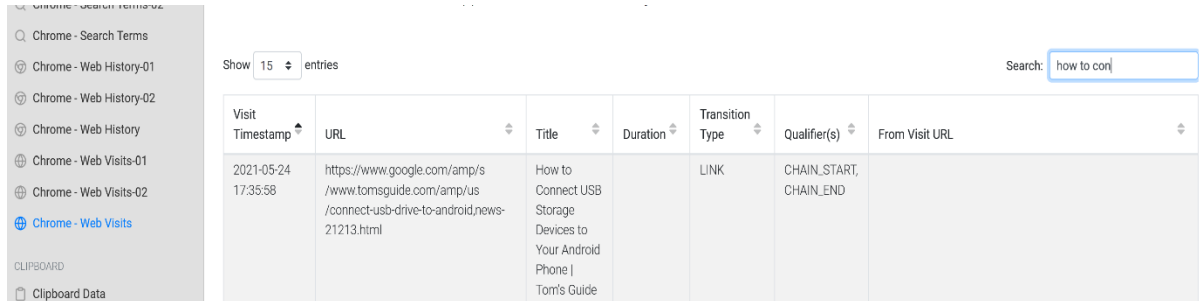
1. What Gmail account is set up on the device?

Clicking on the [Gmail-Active](#) directory, I got the active Gmail account associated with the device. heisenbergcarro@gmail.com

Gmail - Active report	
Total number of entries: 1	
Gmail - Active located at: C:\Users\chukw\Desktop\android dump\ALEAPP_Reports_2024-01-23_Tuesday_142225\temp\Dump\data\data\com.google.android.gm\shared_prefs\Gmail.xml	
Show 15 entries	Search:
Active Gmail Address	
heisenbergcarro@gmail.com	
Active Gmail Address	

2. Which website did Heisenberg look for with regards to guidance on how to mount a USB drive on his phone? (The answer should be the full website i.e www.XX.com).

I clicked on the [Chrome-Web Visits](#) directory, and typed the keyword as shown in the picture below. With this, I got the answer to the question to be www.tomsguide.com

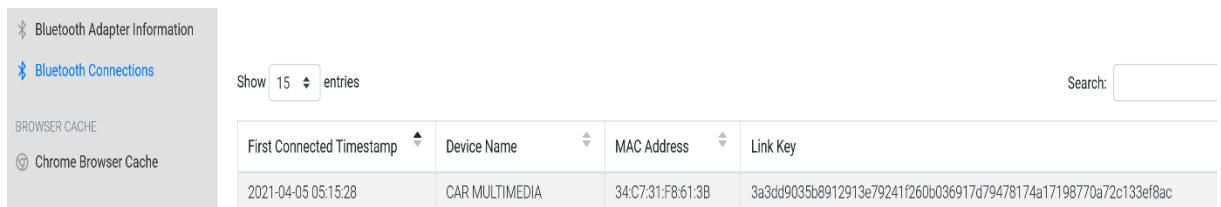


The screenshot shows the 'Chrome - Web Visits' directory in a forensic tool. A search bar on the right contains the text 'how to con'. The main table displays search results with columns: Visit Timestamp, URL, Title, Duration, Transition Type, Qualifier(s), and From Visit URL. One result is visible for a visit on 2021-05-24 at 17:35:58 to a URL from tomsguide.com, with the title 'How to Connect USB Storage Devices to Your Android Phone | Tom's Guide'.

Visit Timestamp	URL	Title	Duration	Transition Type	Qualifier(s)	From Visit URL
2021-05-24 17:35:58	https://www.google.com/amp/s/www.tomsguide.com/amp/us/connect-usb-drive-to-android/news-21213.html	How to Connect USB Storage Devices to Your Android Phone Tom's Guide		LINK	CHAIN_START, CHAIN_END	

3. What is the Bluetooth MAC Address of the first vehicle Heisenberg's Android was connected to?

I clicked on the [Bluetooth connections](#) directory where I found all the connections the android phone made through Bluetooth. I checked the first car it connected to, and found this MAC address attached to it 34:C7:31:F8:61:3B



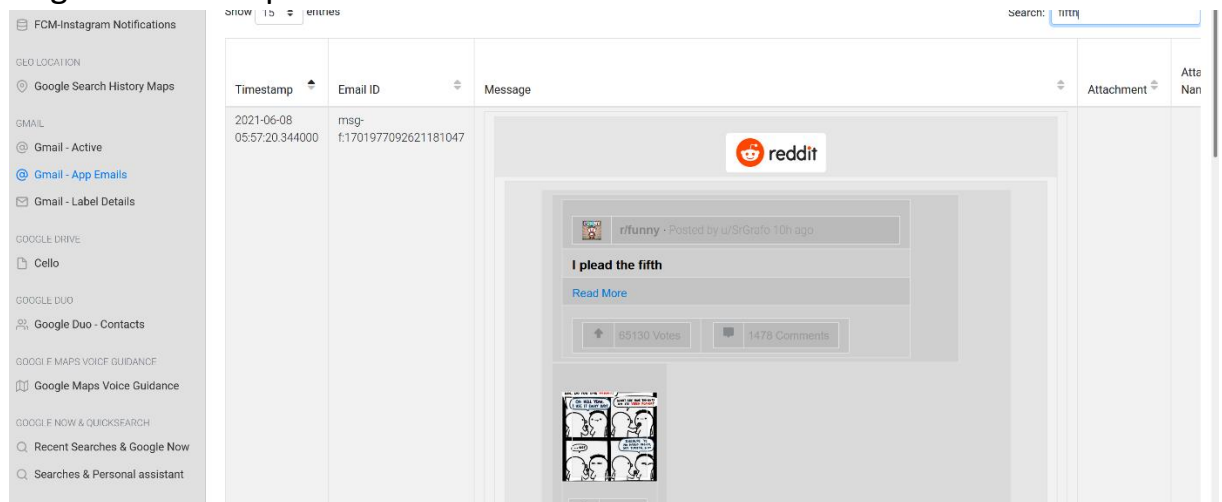
The screenshot shows the 'Bluetooth Connections' directory. The main table displays search results with columns: First Connected Timestamp, Device Name, MAC Address, and Link Key. The first entry shows a connection on 2021-04-05 at 05:15:28 to a device named 'CAR MULTIMEDIA' with MAC address 34:C7:31:F8:61:3B.

First Connected Timestamp	Device Name	MAC Address	Link Key
2021-04-05 05:15:28	CAR MULTIMEDIA	34:C7:31:F8:61:3B	3a3dd9035b8912913e79241f260b036917d79478174a17198770a72c133ef8ac

4. Who was the originator (friendly name) of the phrase "I plead the fifth" used on Heisenberg's Android?

I clicked on the [Gmail-App Email](#) directory, and typed the keyword as shown in the picture below. I got the answer to the friendly name of the

originator of the phrase to be reddit.



- Which applications did Heisenberg use to secure (hide) files and/or pictures?

[HideX – Locked Apps](#) is one of the directories provided by the extracted information. More research on HideX shows that it can be used to lock apps on android phones for security purposes. So, the answer to the question is HideX.

- What is the date and time of Heisenberg's confession/arrest? (Format YYYY-MM-DD HH:MM:SS).

This question was a tough one because it took a lot of time for me to assume what could be an indication of human arrest in an android phone. Firstly, I went through all written conversations both sent and received, I saw the date and time Heisenberg's android phone was blocked from receiving SMS, I suspected that action to have some connection with the arrest. I clicked on [Google Photo – Local Media](#) directory to search for captured events that occurred within that time frame Heisenberg's android phone was blocked from receiving SMS. Inside that directory, I saw a one-minute video that was taken using the android phone camera at this date and time "2021-07-20 19:03:34".

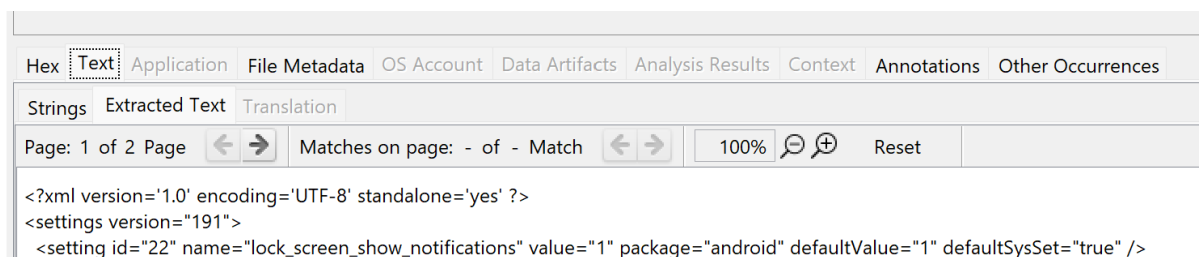
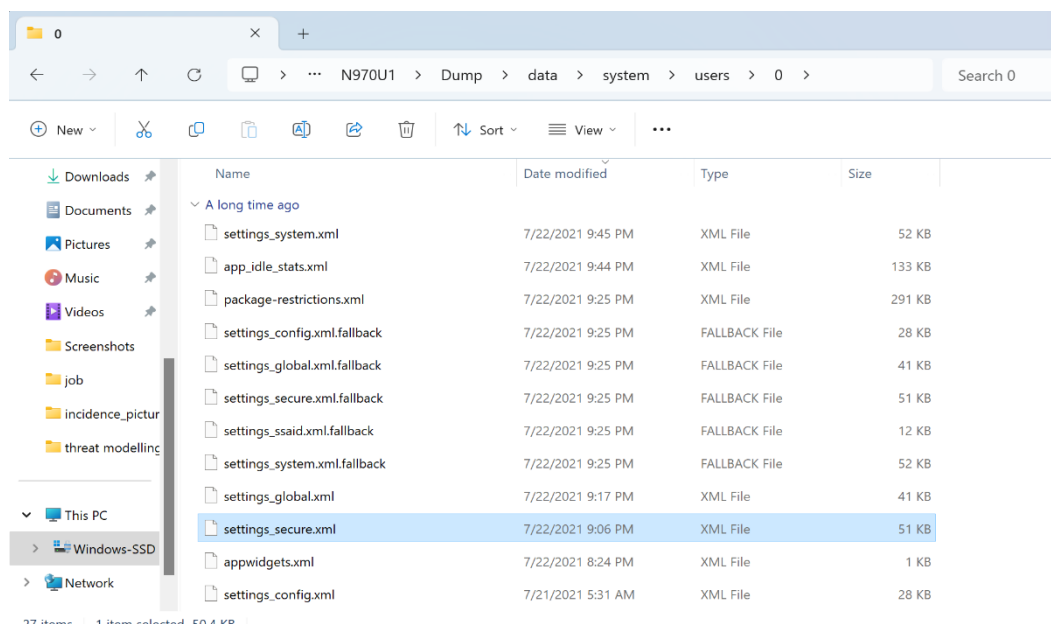
Google Photos - Local Media	2021-07-20 19:03:34	20210720_150222.mp4	/storage/emulated/0/DCIM/Camera	2021-07-20 15:03:34	-4	1080	1920	152589241	C
			/20210720_150222.mp4						

That was the last video captured by the android camera, and it happened an hour before the message blocking was activated. Though the tools I

was using were not able to play the video, but the time of the video record is an indication showing an event that happened prior to the arrest.

7. Notifications were visible on the lock screen while Heisenberg's Android was locked. What is the file that stores the Notification settings? Only the file name is needed.

I resolved this question using AUTOPSY. But first, I searched manually through the extracted folder in my local computer for all the files containing settings relating to notification and security and tried reading their contents using AUTOPSY. This file [settings_secure.xml](#) when uploaded in AUTOPSY, gave me clearer information about what I am looking for as recorded in the second image below, that makes it the answer.



8. Which website was accessed by the user on Heisenberg's Android using DuckDuckGo?

For this question, I clicked on the [Installed Apps](#) directory, DuckDuckGo was one of the apps installed on the android phone. This app is used to

visit websites in an anonymous mode. I tried to perform a keyword search with those websites listed in the answer options, but none provided a history to prove website visitation, and that makes the answer to be “None of the above”.

9. When and in which city (the name of the city he was in at that time) did Heisenberg search for rental properties on his Android? (Answer Format: YYYY-MM-DD HH:MM:SS NameOfCity).

To solve this question, I first got the date and time of the search by clicking on the [Chrome – Search Terms -01](#) directory, then typed the keyword search as shown in the picture below.

Chrome - Network Action Predictor	Show 15 entries	Search: rent
Chrome - Offline Pages-01		
Chrome - Offline Pages-02		
Chrome - Offline Pages		
Chrome - Search Terms-01		
Chrome - Search Terms-02		
Chrome - Search Terms		
Chrome - Web History-01		
Chrome - Web History-02		

Last Visit Time	Search Term	URL	Title	Visit Count
2021-05-16 04:26:51	properties for rent near me	https://www.google.com/search?q=properties+for+rent+near+me&oeq=properties+for+rent+&aqs=chrome..69l57j0l4.11105j0j4&client=ms-android-samsung-gn-rev1&sourceid=chrome-mobile&ie=UTF-8	properties for rent near me - Google Search	0
Last Visit Time	Search Term	URL	Title	Visit Count

To know the city the search was made, I tried to search other directories for other events that also took place on the same day. Clicking on [Geodata](#) directory, I saw some events that happened that same day on this latitude 37.34929656982422 and longitude -80.53861999511719, though the name of the city attached to it was Newport, but it was still not the correct answer. I searched other related directories as shown in the picture below where I noticed that Blacksburg is another city that falls within same latitude and longitude, this gave me the answer.

GEO LOCATION	Directions	Latitude	Longitude	To Latitude	To Longitude
Google Search History Maps	https://google.com/maps/dir/35.2949622;-80.7504288/Blacksburg,+VA/data=!4m13!4m12!1m1!4e1!1m9!1m1!1s0x884d950adc06dccc3:0x86ceb8ea4842da2d!2m2!1d-80.4139393!2d37.2295733!2m2!6e0!7e2!3e0	35.2949622	-80.7504288	37.2295733	-80.4139393
GMAIL					

10. Heisenberg was looking for cars. Which vehicle did he not search for?

To solve this question, I searched for email replies related to car searches in the [Gmail – Email App](#) directory. Other cars listed in the option appeared on the search, but I didn’t see Ford Escape, that makes it the answer among the options.

11. How many times did Heisenberg’s Android power off due to the battery being fully depleted between May and August? The answer must be an integer (i.e 4).

Android phones are being powered using batteries. So, once the battery gets fully depleted, it goes off because of lack of power. As shown in the picture below, if you count the number of times the android device went off because of no power, you will see that it is 10, and that is the answer.

Search:

Timestamp (Local)	Timezone Offset	Action	Reason
2021-05-01 06:04:43	-0400	SHUTDOWN	no power
2021-05-05 04:15:14	-0400	REBOOT	recovery
2021-05-10 07:07:32	-0400	SHUTDOWN	no power
2021-05-18 22:33:26	-0400	SHUTDOWN	no power
2021-05-25 15:43:16	-0400	SHUTDOWN	no power
2021-06-06 05:14:56	-0400	SHUTDOWN	no power
2021-06-10 11:47:37	-0400	SHUTDOWN	no power
2021-06-21 03:19:04	-0400	SHUTDOWN	no power
2021-06-22 14:10:26	-0400	REBOOT	recovery-update
2021-06-28 23:18:32	-0400	REBOOT	recovery
2021-06-30 15:16:31	-0400	SHUTDOWN	no power
2021-07-04 19:47:09	-0400	SHUTDOWN	no power
2021-07-08 02:31:52	-0400	SHUTDOWN	no power
Timestamp (Local)	Timezone Offset	Action	Reason

12. On Heisenberg’s Android, where else can you find the IMSI number on the device, other than the Checkin.xml file?

This question seems not be complicated for me because the files listed in the answer options have something in common that is in relationship with the SIM network used in the android phone. Netpolicy.xml (Network policies), mmssms.db (SMS & MMS), telephony.db (database that contains sim card information). So, the sim card IMSI number can be found in all of them.

CONCLUSION

I performed forensic investigations on Heisenberg android phone to acquire evidence to back up the accusation on him. The suspect was arrested for a criminal offence relating to car theft.

In the forensic report, according to the SMS messages found in the phone, it shows that prior to Heisenberg arrest, he was planning to hand over a 2014 Hyundai Sonata to a prospective buyer. Also, there was a particular one-minute video found in his android phone which was recorded prior to his arrest, I recommend further investigations to know what happened in that recorded video camera.

The beauty of forensic investigations can never be overemphasized because most crime in this era are committed through digital communication. Therefore, performing forensic investigations can produce proof of what exactly happened and how it happened.