Technische Universität Wien

188.922 Digital Forensics

Lecturers: Dipl.Inf. (FH) Karsten Theiner and DI Dr. Martin Schmiedecker

Teaching Assistant: Christoph Kraus

Assignment 3: Smartphones

Bruno André Moreira Rosendo

e12302727

Due Date: December 20, 2023

Submitted: December 18, 2023

Contents

1 Purpose

This assignment was designed to support the investigation into someone known as Heisenberg, who was arrested for allegedly dealing with stolen cars. The focus of the task was to analyze Heisenberg's smartphone as part of this process. This assignment was undertaken as part of a Digital Forensics course, wherein students were assigned the role of forensic analysts responsible for conducting this fictional investigation.

To kickstart the process, the students were given an image containing the file system of Heisenberg's Android phone. The goal is to use this image to answer a few questions that are proposed about the case, which are detailed in section 3.

This project's primary challenge is acquiring proficiency in the techniques for retrieving, analyzing, and documenting information from a smartphone file system. The Cellebrite Reader and ALEAPP software tools were suggested for the analysis, providing hands-on experience in digital forensics for the participating students.

2 Procedure

After downloading and extracting the smartphone's image, and prior to anything else, it is important to hash the image to guarantee that any modifications made to it do not alter its content in any manner. To ensure the ability to return to the initial state, one option could be to redownload it; however, a safer approach is to duplicate its contents into a new file. The hashes of both files were stored and compared throughout the investigation:

```
md5sum smartphone-image.zip > hash.txt
md5sum smartphone-image-copy.zip > hash-copy.txt
cat hash.txt
XX  smartphone-image.zip
cat hash-copy.txt
XX smartphone-image-copy.zip
```

After hashing the image, the first actions involved using the Cellebrite Reader (v7.59.0.36) and ALEAPP (v3.1.9) tools to scrutinize the smartphone. The generated reports from these tools were subsequently utilized in the investigation to address the questions outlined in the assignment.

3 Analysis

The subsequent section responds to all the assignment's specific questions and assesses the results of the investigation according to the reports generated in section 2.

3.1 Are there clues or evidence for Heisenberg dealing with (stolen) cars?

There are numerous compelling indicators strongly suggesting Heisenberg's involvement with cars, and there is specific evidence hinting at the potential theft of these cards. Utilizing ALEAPP to inspect the applications installed on his phone (Figure 1), we can discern the presence of the following suspicious apps by searching the app ID in Google Play:

- **Cartomizer - Wheels Visualizer:** Enables the visualization of wheels on personal vehicles, implying a connection to the trade of cars.
- **Autotrader, CARFAX, CarGurus:** Apps designed for buying and selling used cars. The simultaneous use of multiple apps suggests Heisenberg's involvement in the car trade.
- **Car info - Car Data, Cars Specs:** A comprehensive database providing information about various car models.
- **Instant Checkmate Search:** One among several apps installed for conducting background checks on individuals, potentially used to vet potential car buyers.
- **BlueDriver OBD2 Scan Tool:** An app offering detailed information about car models, including specific mechanical details.
- **ORTO:** An app allowing the scanning of car plates for information on car history and ownership.

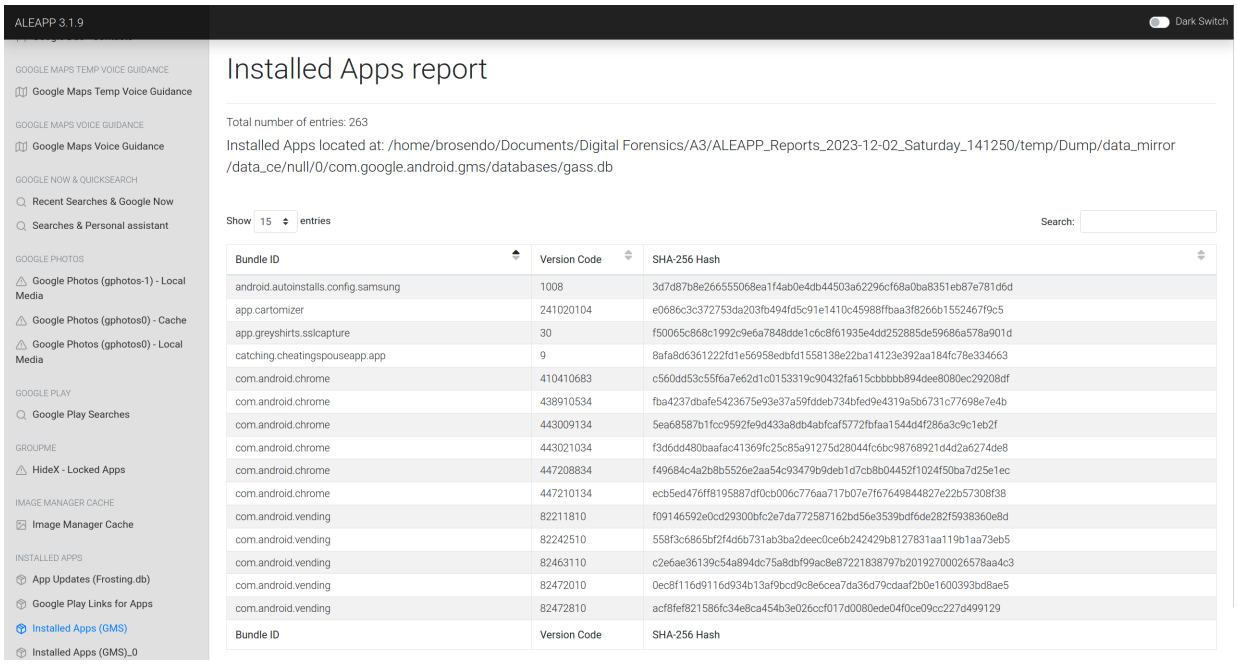


Figure 1: ALEAPP's report showing the apps installed on the smartphone

Additionally, examining his text messages with potential buyers further confirms his involvement in dealing cars, as illustrated in Figure 3.

Furthermore, insights into Heisenberg's financial challenges emerge, providing a potential explanation for his engagement with stolen cars. Notably, he had installed money-saving apps such as **T-Mobile Tuesdays** and **Upside: Fuel Rewards Cash Back**. Accessing his email history (Figure 4) reveals his exploration of new avenues to generate income. He was also searching the web for cheap OBD scanners, revealing his interest in car trading and low amount of cash (Figure 5).

Finally, it is noteworthy that he had installed an app named **Cheating Spouse Catching**, suggesting potential issues in his personal life and raising concerns about his mental health.

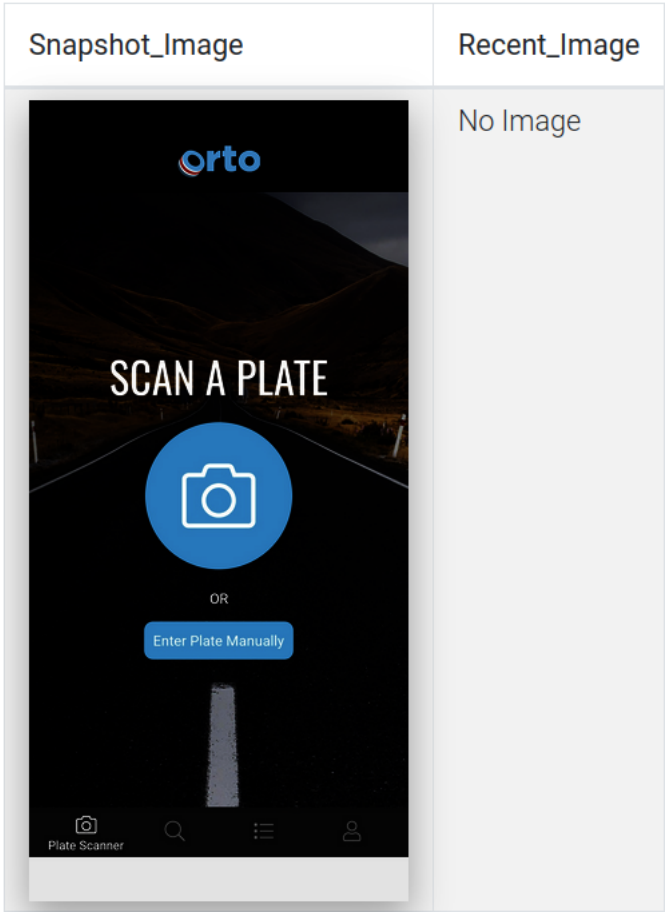


Figure 2: A snapshot of the app ORTO, used by Heisenberg

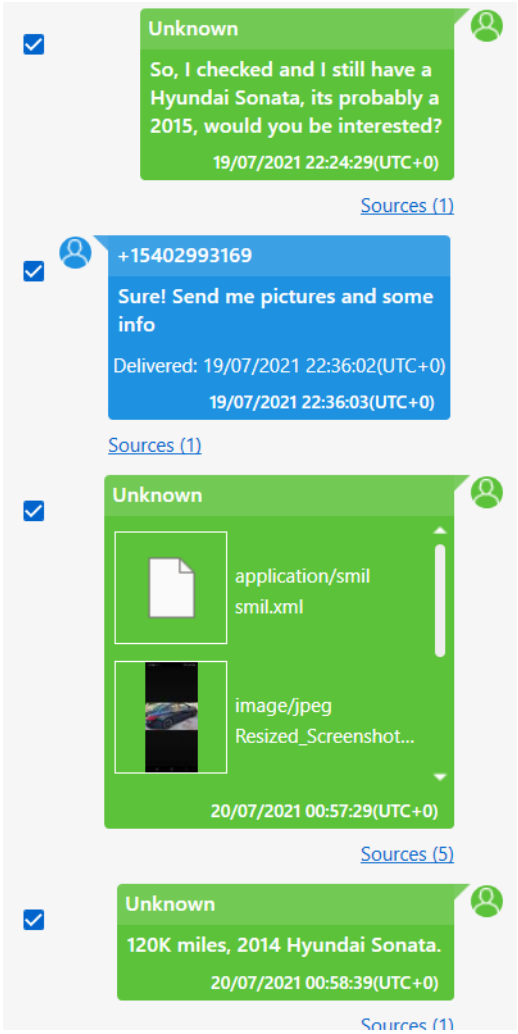


Figure 3: An SMS conversation with a potential car buyer, exported from Cellebrite Reader

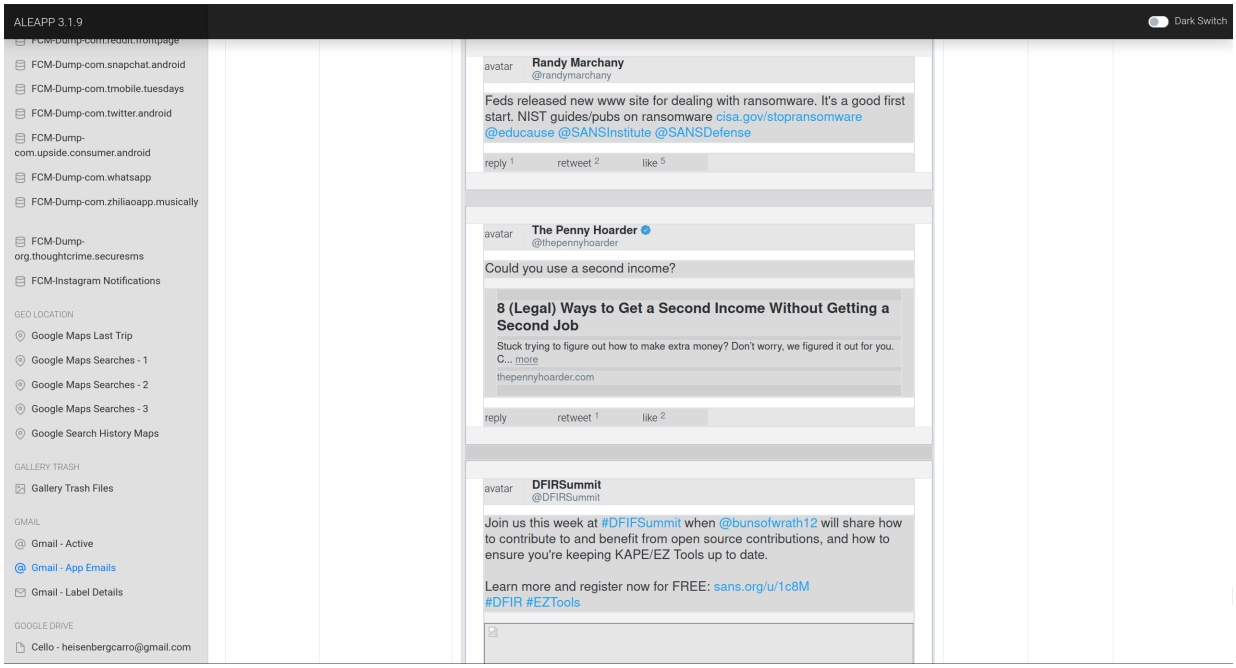


Figure 4: ALEAPP's email report showing activity on a Tweet related to extra income

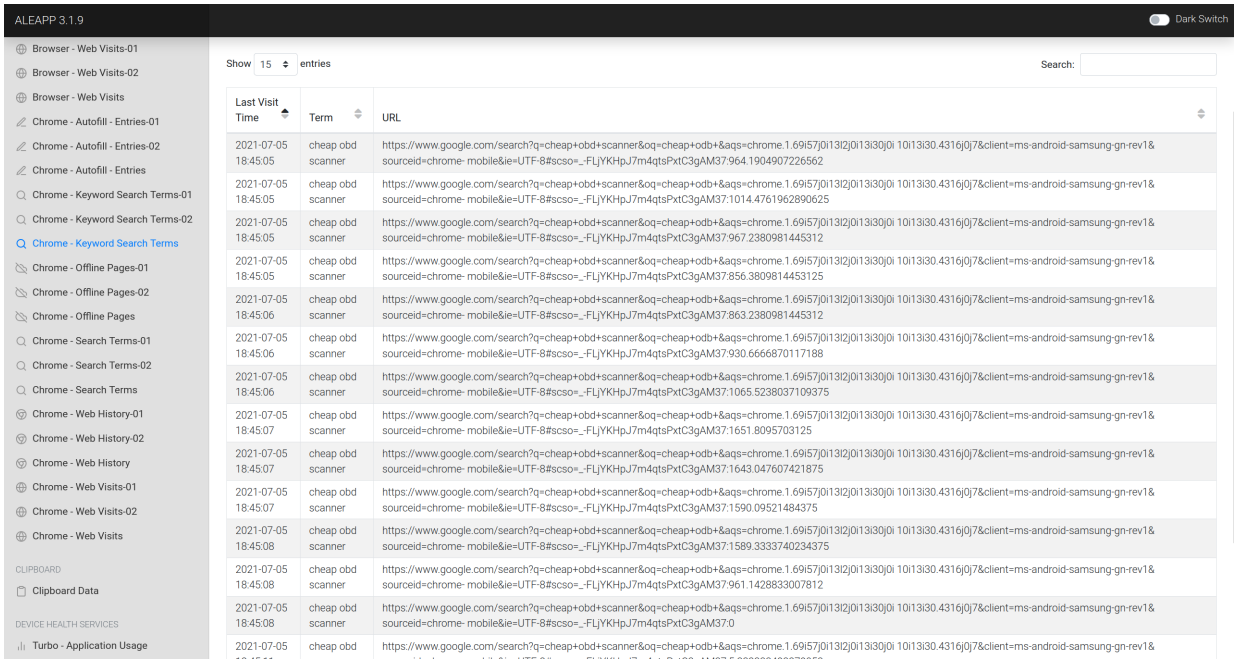


Figure 5: Web search revealing interest to buy a cheap OBD scanner

3.2 Heisenberg used his cellphone during the arrest. Did he create any recordings of the arrest?

Yes, by searching for videos recorded on the day of the arrest (20-07-2021) using Cellebrite Reader, a recording made during the arrest can be easily located. In this video, Heisenberg mistakenly believed that the police woman was a potential buyer for the car he possessed. When confronted, he attempted to deny his involvement with the stolen car, attributing the blame to someone named Beth. The recording is stored on his phone in the directory *"/Dump/data/media/0/DCIM/Camera/20210720_150222.mp4"*. A screenshot of the video is provided in Figure 6. The hash of the video is *"1fb629ceb7e03948032448b6af978c94"*. Note that it is also possible to find texts between Heisenberg and Beth, so the investigation should analyze her in the future as well.

3.3 Are there any hints that the police did not quite follow best practices in handling the cellphone during/after the arrest? If so, what did they do wrong?

Following the arrest and the seizure of the smartphone, standard protocols dictate isolating the phone to minimize external interactions. This typically involves implementing measures such as enabling airplane mode, removing the SIM card, and restricting access to various functionalities like Wi-Fi, mobile data, GPS, and Bluetooth. Additionally, shielding the device from external communications, for example, by using a Faraday bag, is a possible practice. If the device remains unused and lacks password protection, it is also advisable to turn it off.

However, it appears that these standard practices were not followed by the police, as there is significant phone activity observed after the arrest. Notably, activities such as Google Maps usage and geolocation information indicate that GPS and Wi-Fi connectivity

Figure 6: Screenshot of the video recorded during the arrest

were not prevented (Figure 7). Moreover, there is evidence of pictures being taken and USB devices connected (figures 8 and 9), as evident from the system logs, even after the phone was taken into custody for investigation. This oversight could potentially compromise the integrity of the evidence stored on the smartphone.

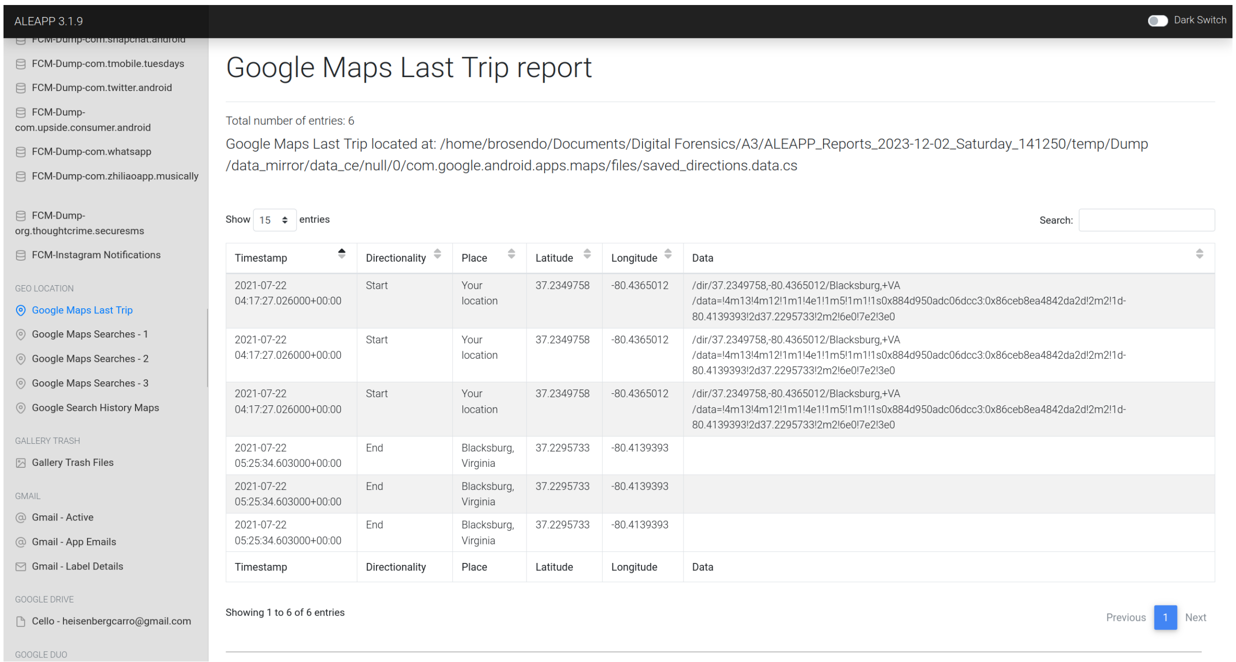
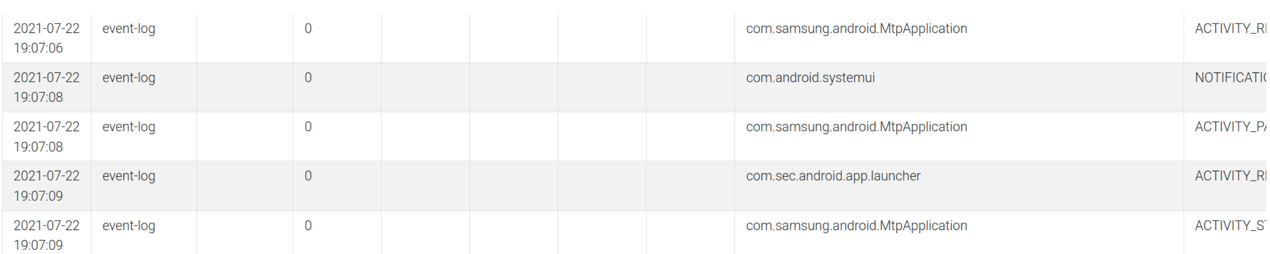


Figure 7: Evidence showing Google Maps information being tracked after the arrest



2021-07-22 19:07:06	event-log		0					com.samsung.android.MtpApplication	ACTIVITY_RI
2021-07-22 19:07:08	event-log		0					com.android.systemui	NOTIFICATIO
2021-07-22 19:07:08	event-log		0					com.samsung.android.MtpApplication	ACTIVITY_PA
2021-07-22 19:07:09	event-log		0					com.sec.android.app.launcher	ACTIVITY_RI
2021-07-22 19:07:09	event-log		0					com.samsung.android.MtpApplication	ACTIVITY_S

Figure 8: System logs showing USB media activity after the arrest

com.samsung.android.MtpApplication	ACTIVITY_RESUMED	com.samsung.android.MtpApplication.USBConnection
com.android.systemui	NOTIFICATION_INTERRUPTION	
com.samsung.android.MtpApplication	ACTIVITY_PAUSED	com.samsung.android.MtpApplication.USBConnection
com.sec.android.app.launcher	ACTIVITY_RESUMED	com.android.launcher3.uioverrides.QuickstepLauncher
com.samsung.android.MtpApplication	ACTIVITY_STOPPED	com.samsung.android.MtpApplication.USBConnection

Figure 9: System logs showing USB media activity after the arrest

3.4 Are there any clues for Heisenberg taking an interest in cryptocurrency?

Yes, we can find emails and Twitter activity related to cryptocurrencies, such as Bitcoin, Dogecoin and NFTs, as shown in figures 10 and 11.

3.5 Did Heisenberg use any apps for file hiding or encryption?

Indeed, a manual inspection of the apps installed on Heisenberg's smartphone uncovered an application that disguises as a calculator. Contrary to its appearance, the primary function of this app is to hide other apps, files, and web history by securing them behind a secret code within the calculator interface. The app in question can be identified by its ID among the installed apps: *"com.flatfish.cal.privacy"*.

Another suspicious app associated with encryption is named *"Packet Capture"*, which aims to capture encrypted SSL packets through a man-in-the-middle attack. While this doesn't involve file hiding, it does raise concerns about potential nefarious activities on Heisenberg's part.

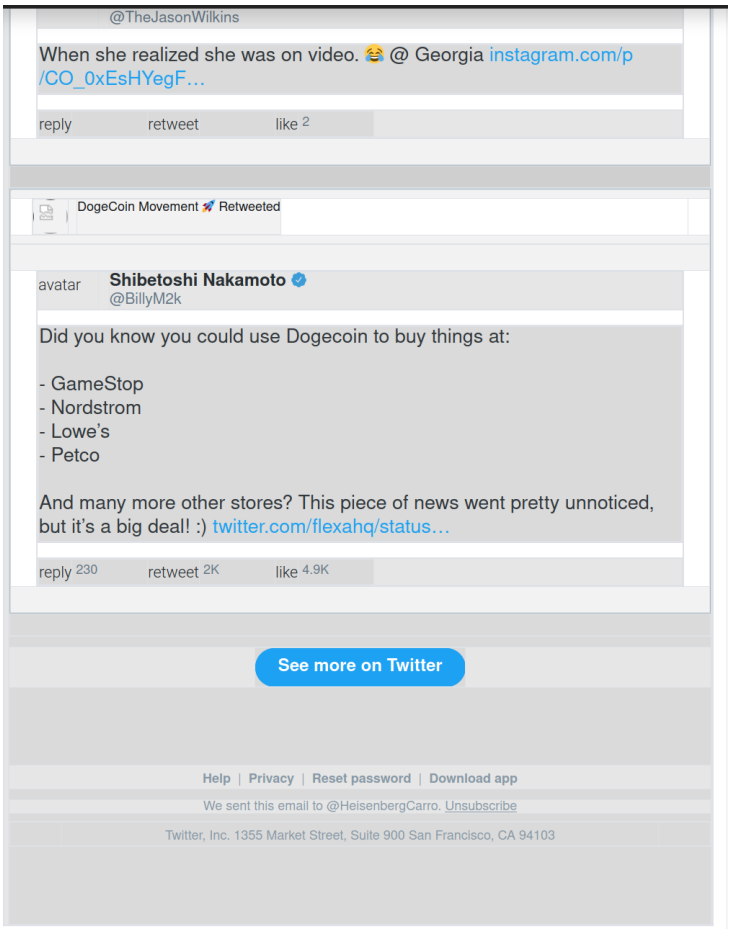


Figure 10: Twitter activity on Dogecoin

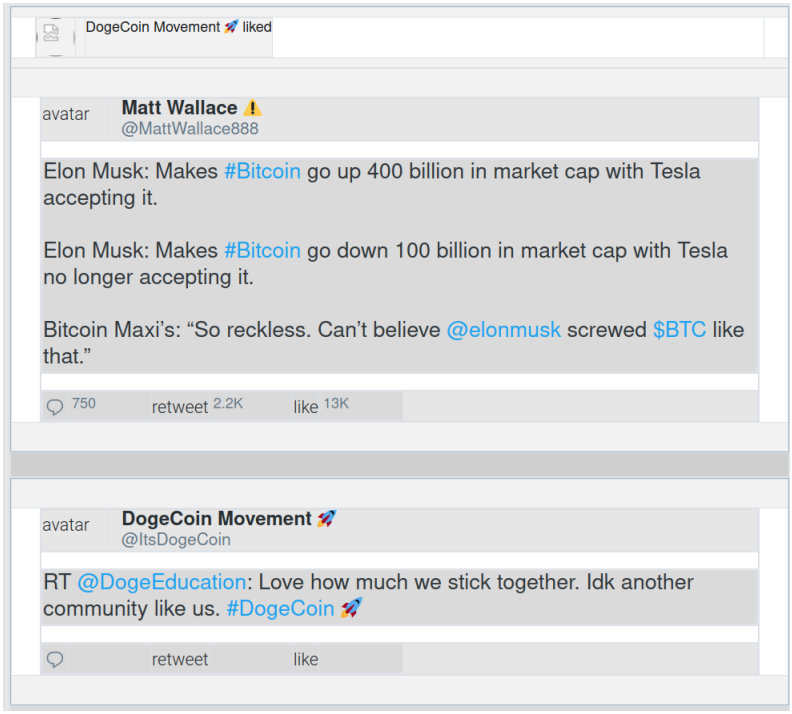


Figure 11: Twitter activity on Bitcoin and Dogecoin

3.6 Are there any clues for Heisenberg connecting or planning to connect external drives to his Cellphone?

Indeed, there is evidence of web searches indicating Heisenberg's interest in connecting a USB storage device to his smartphone, as depicted in Figure 12. Additionally, his search history includes queries for a micro USB adapter, suggesting a potential intention to facilitate the connection of the USB device, as illustrated in Figures 13 and 14.

3.7 Was the image with the MD5 hash "066858f4b1971b0501b9a06296936a34" hidden by Heisenberg? If yes, what app was used?

In Cellebrite Reader, searching for the file hash yields a result associated with the HideX application's cache directory, indicating that Heisenberg hid the file. The file is located at

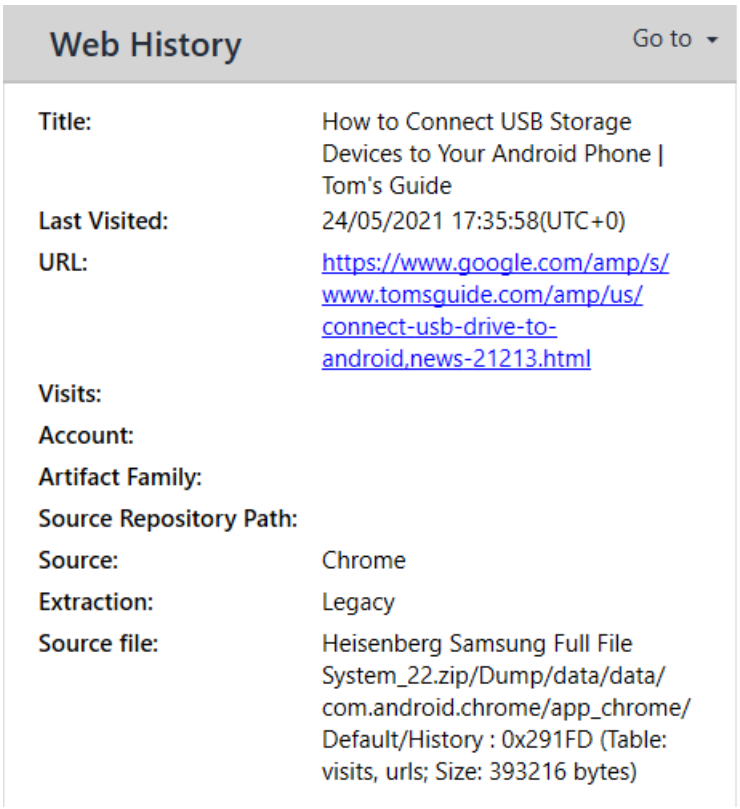


Figure 12: Web search for how to connect a USB storage device to an Android phone

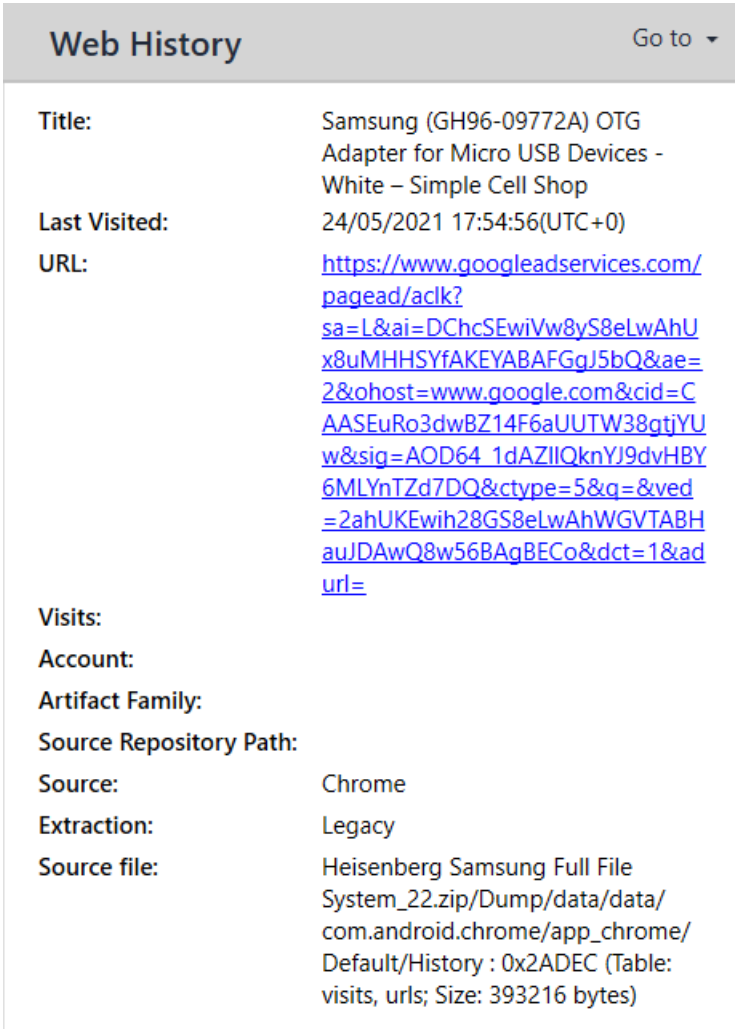


Figure 13: Web search for a potential micro USB adapter

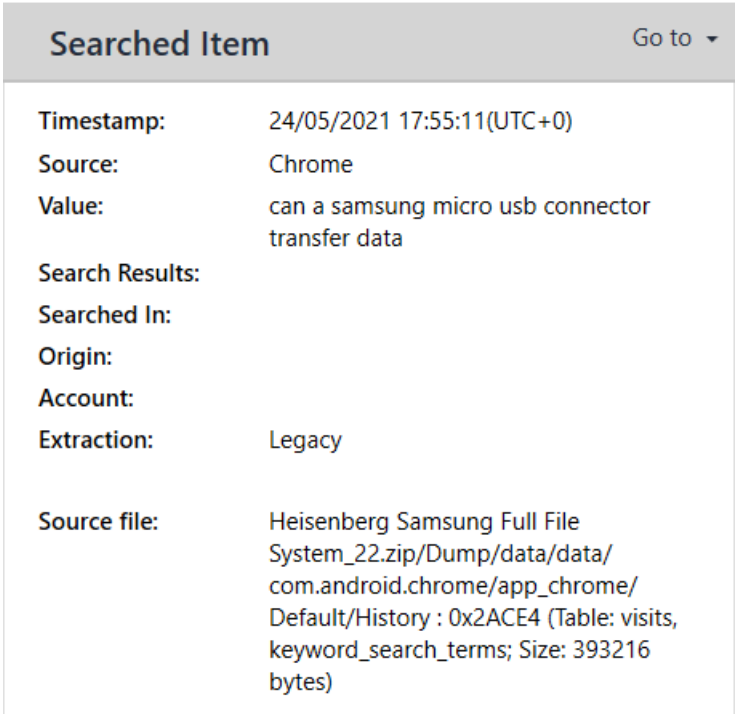


Figure 14: Web search to check if a micro USB connector can transfer data

"/Dump/data/data/com.flatfish.cal.privacy/cache/image_manager_disk_cache/7ae6e97ba4ad0d693413273d6e270a412af3331a9c96c7a9049e3ae9b6047c9d.0". It is an image depicted in Figure 15.

3.8 Where did Heisenberg plan to meet with the owner of the telephone number "+15402993169"?

The planned meeting location can be ascertained by examining SMS messages between Heisenberg and the owner of the phone number. In one of the texts, detailed in Figure 16, it is revealed that they intended to meet at the Washington Street Tennis Courts. Additionally, it is noteworthy that the owner of this number is the same police officer who arrested him on the 20th of July.

Figure 15: The image hidden by Heisenberg using the HideX calculator

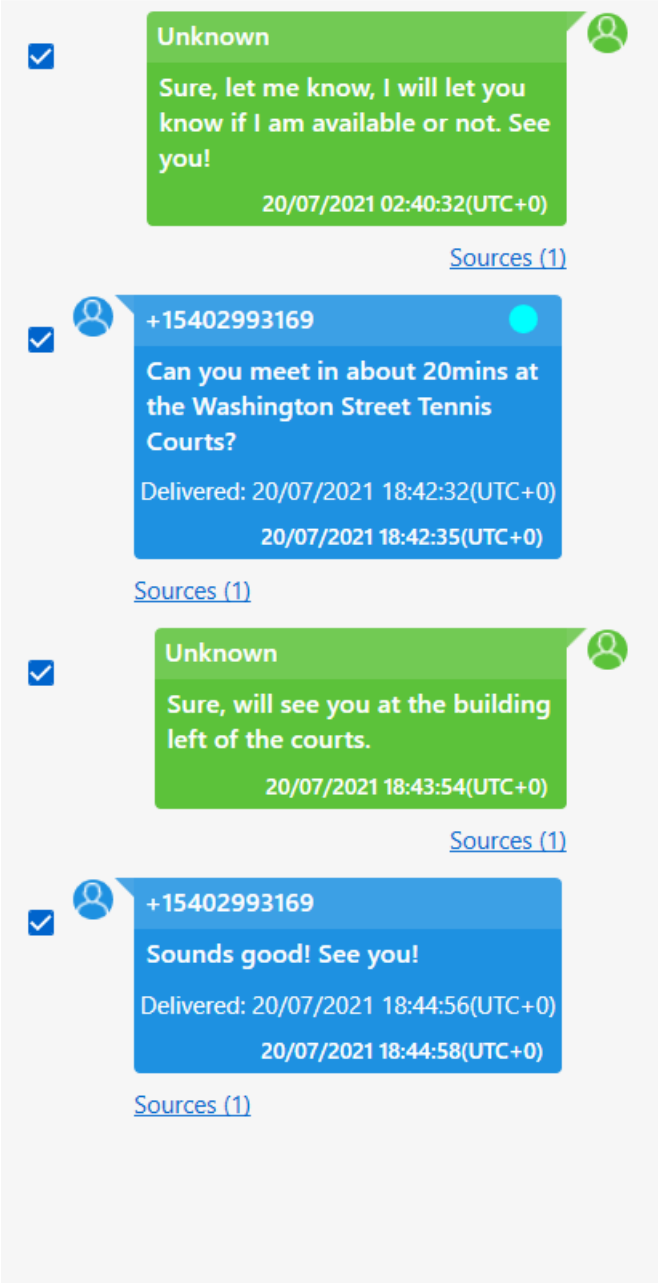
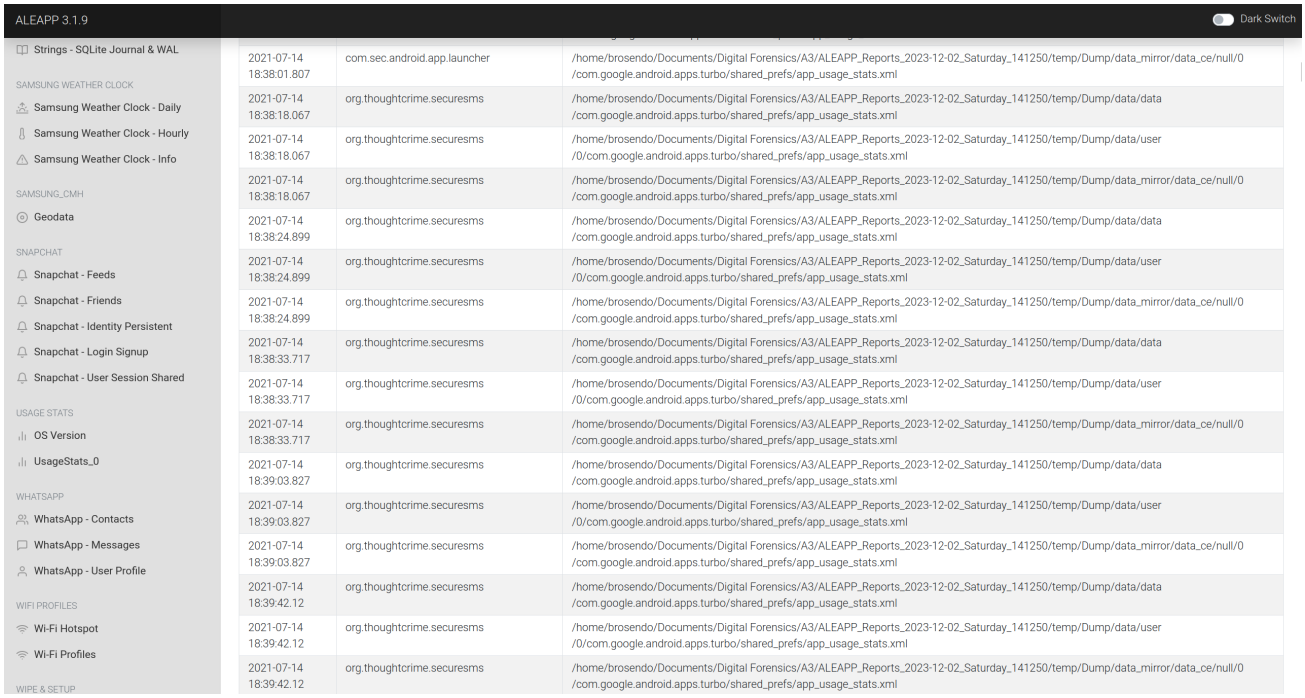


Figure 16: SMS messages revealling the meeting place between Heisenber and the cop

3.9 At which time(s) did Heisenberg actively use the Signal app on 2021-07-14?

To begin, it is essential to note that Signal's app ID is *"org.thoughtcrime.securesms."* Leveraging this information, ALEAPP was utilized to investigate app activity, revealing a substantial amount of activity between 18:38 and 18:40. This timeframe strongly indicates an exchange of messages. The corresponding evidence is presented in Figure 17.



2021-07-14 18:38:01.807	com.sec.android.app.launcher	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:18.067	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:18.067	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:18.067	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:24.899	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:24.899	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:24.899	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:33.717	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:33.717	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:38:33.717	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:39:03.827	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:39:03.827	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:39:03.827	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:39:42.12	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:39:42.12	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
2021-07-14 18:39:42.12	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml

Figure 17: ALEAPP's report showing Signal's activity