Mission Name

DataCardForensics

History Background

Claire found Ethan at Skytech, interrogating to a suspected information trader on the black market. The suspect (SkytechMole named Anderson) is connected, and Claire acquire his datacard.

Technical High-Level Overview

A file system is provided that is linked to an Android evidence. The aim is to get a location, in this case in South America (Paraguay).
Player will have to Android filesystem in order to find out two parameters: latitude and longitude. These parameters can be found analysing chat apps and performing a file decryption.

Short Description

You´re going to analyse Skytech Mole´s datacard, your goal is to find a location in terms of latitude and longitude.

Mission Description

An Android file system is provided that is linked to the datacard. You´re going to analyse this Skytech Mole´s datacard and your goal is to find a location in terms of latitude and longitude at Paraguay. Keep in mind, this time it was used other App to send the location. If you have to use passwords to open files with passwords, use numbers only.

Location

SYLVARCON | SKYTECH HQ

Tools

- SQLITE Studio: database to read SQLITE databases.
- ALEAPP - https://github.com/abrignoni/ALEAPP

Questions

Which is the Android Bluetooth MAC Address?

- 04:B1:A1:9B:3B:C2

How many searches were executed on “Google Play” App?

- 3

Which is the gmail account used on the Android device?

- anderson.vegax37@gmail.com

Items

1. Analyse Gmail messages on the SQLITE database called bigTopDataDB.-596317436
2. Analyse Gmail attachments on the SQLITE database called metadata.-596317436.db
3. Analyse Pictures attached, locate the name of the street on Paraguay, follow to last picture using Google Maps, and locate a possible password based on numbers.

Write Up

First of all, player should unzip evidence provided, and the use ALEAPP app to parse Android File System:

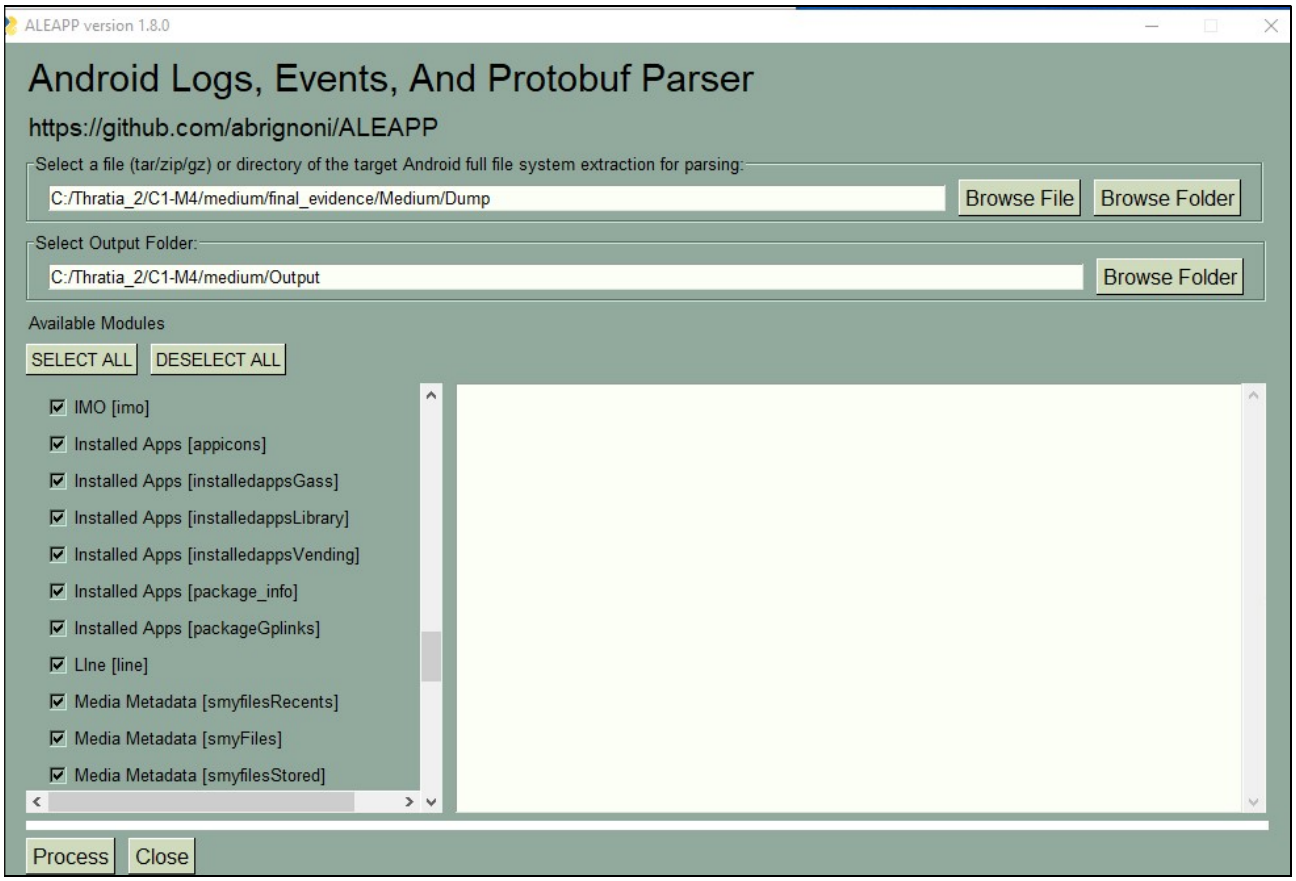


Figure 1

Select all options, and finally select “Process”.

Once ALEAPP has finished, ALEAPP will show this message:

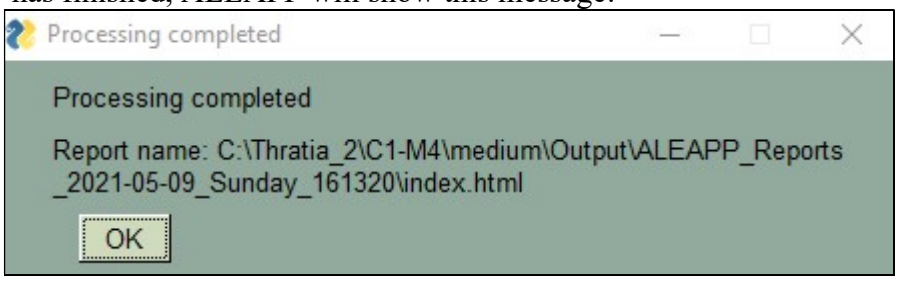


Figure 2

Open index.html

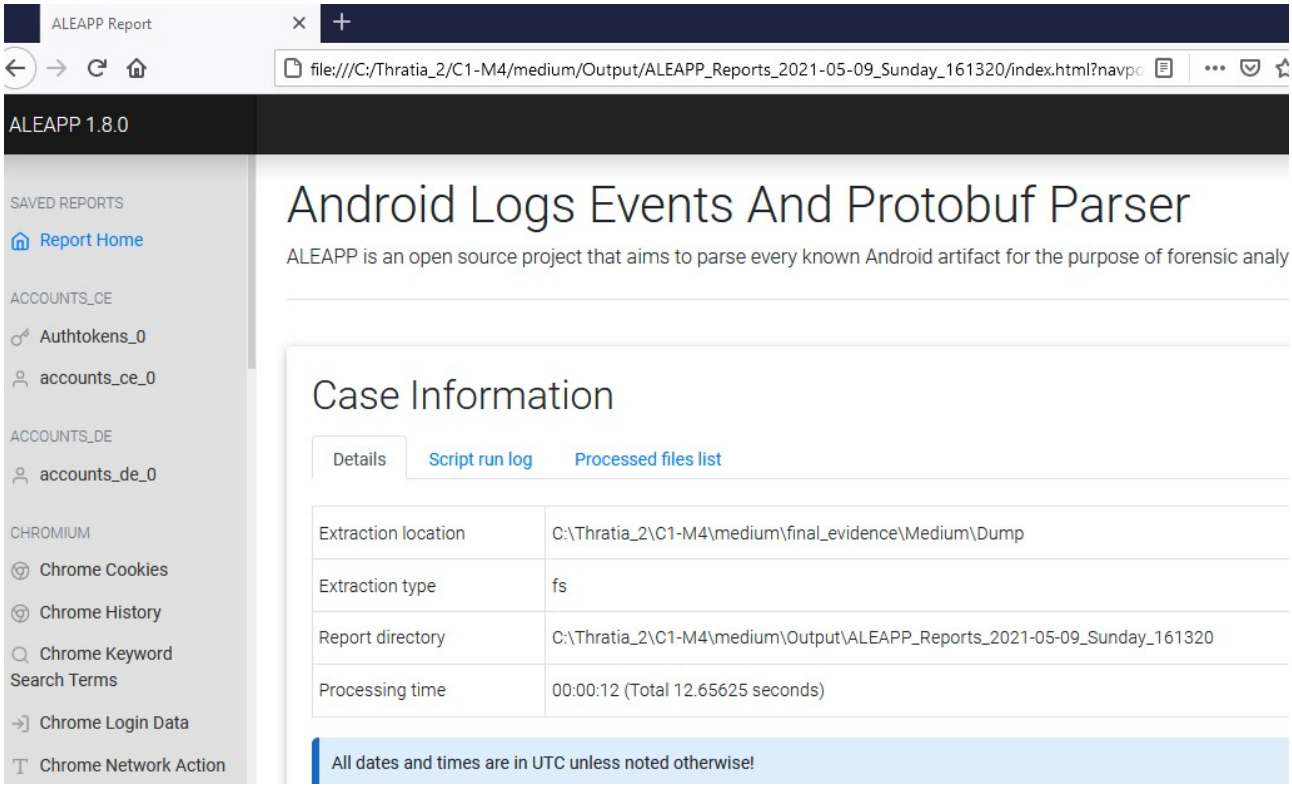


Figure 3

The first clue would be to analyse accounts inside Android filesystem:

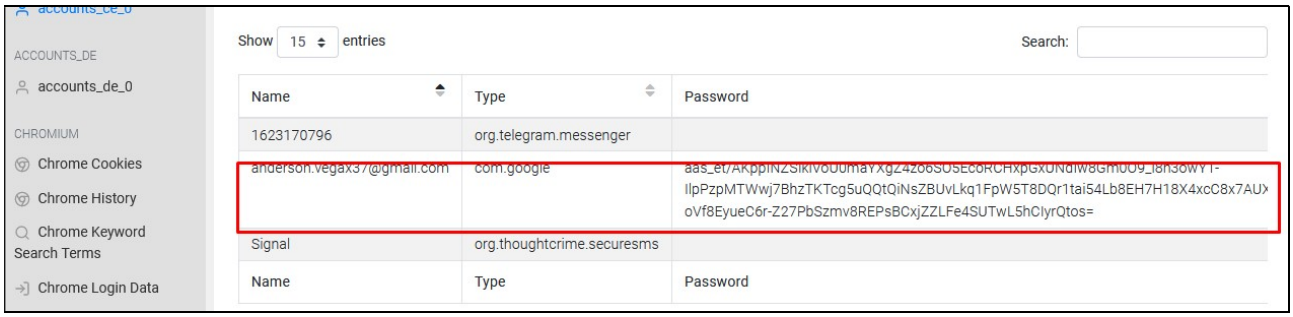


Figure 4

At this time, player must analyse Gmail. Challenge description indicates that it´s mandatory to analyse other APP, so considering medium challenge was Skype and Telegram apps, right now it´s Gmail. Android Gmail is located at: \data\data\com.google.android.gm\

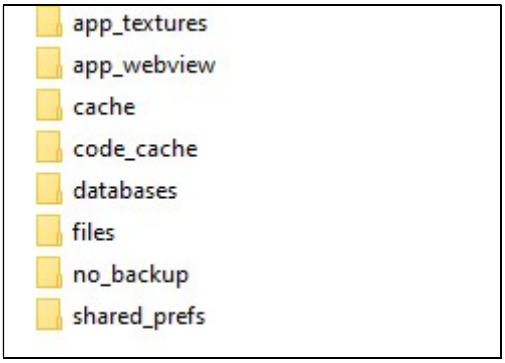


Figure 5

Emails messages could be found at the following SQLite database: \data\data\com.google.android.gm\databases\bigTopDataDB.-596317436

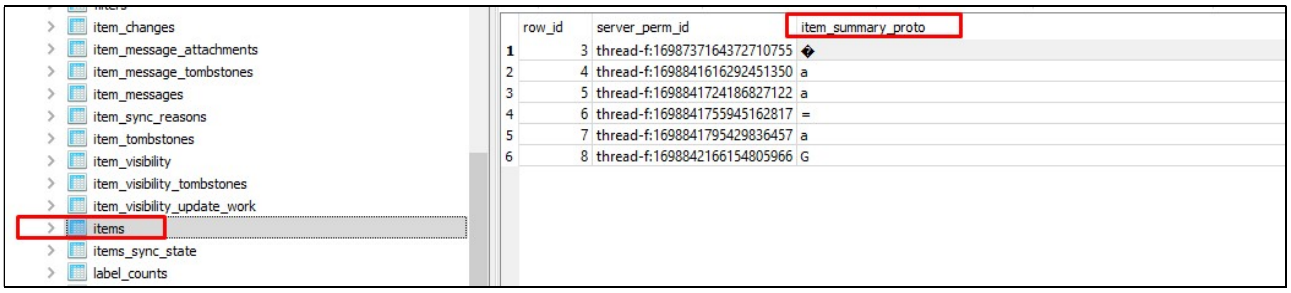


Figure 6

Messages could be found on table items and column item_summary_proto.

To perform a deep analyse, export table, selecting on the same table “export”.

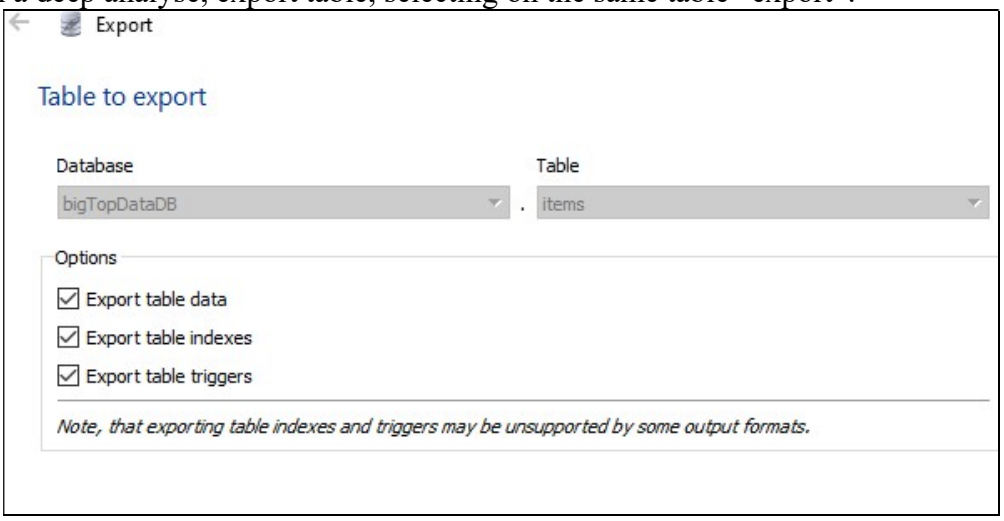


Figure 7

Fill the name and the path to export results:

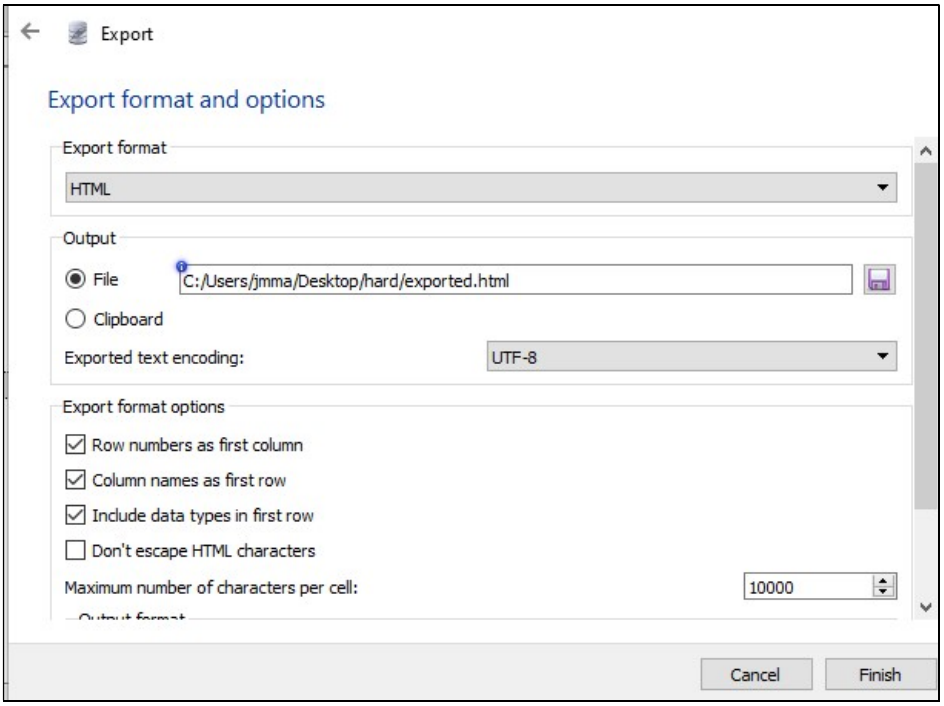


Figure 8

Player should identify messages inside it:

row_id INTEGER	server_perm_id TEXT	item_summary_proto BLOB	rec TE
3	thread-f:1698737164372710755	thread-f:1698737164372710755 9Anderson, termina de configurar tu nueva cuenta de Google Hola, Anderson: Te damos la bienvenida a Google. Con tu nueva cuenta, puedes acceder a productos, aplicaciones y servicios de Google. Aquí tienes algunos consejos para empezar. Comprueba que tus /UC*?h	
4	thread-f:1698841616292451350	a thread-f:1698841616292451350 Picture 1"Sent with ProtonMail Secure Email. /h	
5	thread-f:1698841724186827122	a thread-f:1698841724186827122 Picture 2"Sent with ProtonMail Secure Email. /h	
6	thread-f:1698841755945162817	= thread-f:1698841755945162817 Picture 3 /h	
7	thread-f:1698841795429836457	a thread-f:1698841795429836457 Picture 4"Sent with ProtonMail Secure Email. /h	
8	thread-f:1698842166154805966	G thread-f:1698842166154805966 Location /: /h	

Figure 9

This is the other database called metadata with attachments: **metadata.-596317436.db.** At this point, player must analyse attachments to get a latitude and longitude:

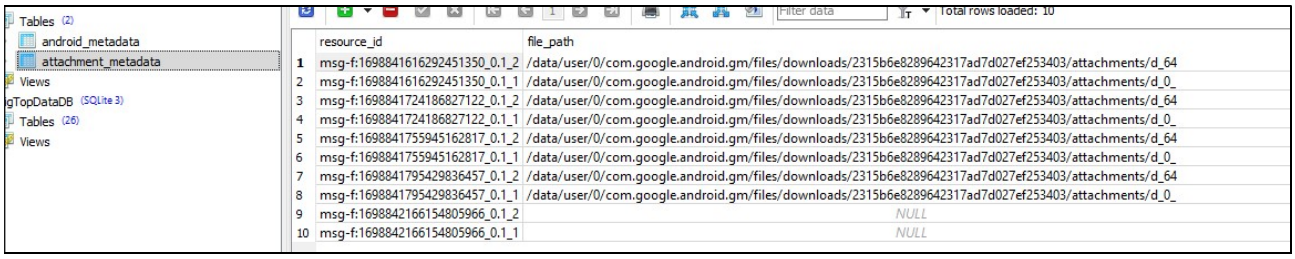
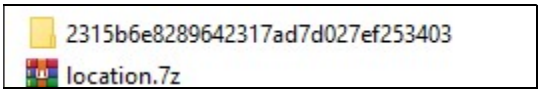


Figure 10

So attachments could be found here: data\data\com.google.android.gm\files\downloads



There is a file called location.7z with password, the goal is to identify the password keep in mind, that there were emails with pictures: Picture 1, Picture 2, Picture 3, Picture 4.

Picture 1

data\data\com.google.android.gm\files\downloads\2315b6e8289642317ad7d027ef253403\attachments\d_0_0_4b9ea1e9_ca2ff541_e9f5b089_73e52cd5_7cf11e8a

Figure 11

Picture 2

\data\data\com.google.android.gm\files\downloads\2315b6e8289642317ad7d027ef253403\attachments\d_0_0_59f0f674_33cf3071_d236eb3d_685be6ac_2eb11204

Figure 12

Picture 3

\data\data\com.google.android.gm\files\downloads\2315b6e8289642317ad7d027ef253403\attachments\d_0_0_36cc71e0_d70ff4ba_a1347a3b_dce824ac_6a8bcc27

Figure 13

Picture 4

\data\data\com.google.android.gm\files\downloads\2315b6e8289642317ad7d027ef253403\attachments\d_0_0_dce4dc09_be44aa78_c7c0a015_5f08b9d7_b1aabee7

Figure 14

Picture 1 and Picture 2 have the same street name:

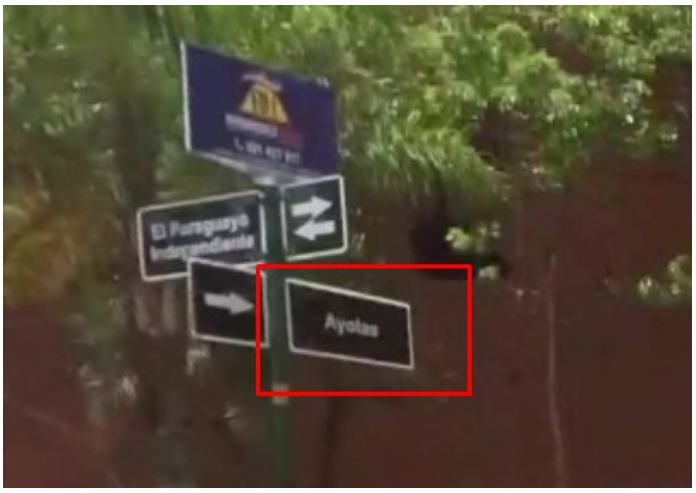


Figure 15

Figure 16

Cosidering, challenge description, Ayolas Street is located in Paraguay.

Player has to follow this street on Google Maps with street view and follow the pictures along Ayolas Street.

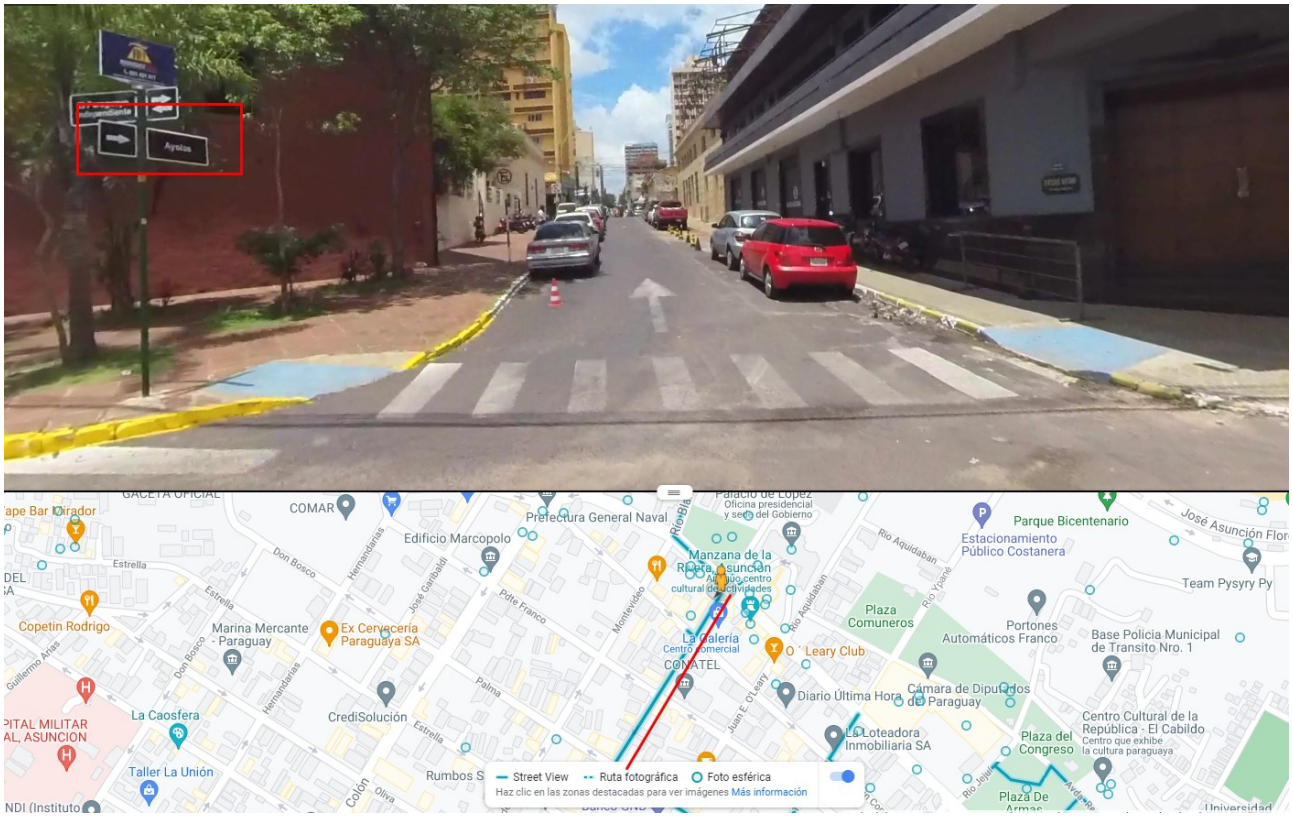


Figure 17

Picture 1:
https://www.google.es/maps/@-25.2776292,-57.6380814,3a,48.8y,213.02h,88.84t/data=!3m9!1e1!3m7!1sAF1QipNlrhT8pcSnfuCVq8rM1SQ5U-h3Ai_ud75gujEx!2e10!7i7680!8i3840!9m2!1b1!2i37

Picture 2
https://www.google.es/maps/@-25.2781339,-57.6383761,3a,75y,300.63h,91.18t/data=!3m7!1e1!3m5!1sAF1QipMR5v6D1AnR4rjjLjcJNhaQYiflrg_5CGEBXGDb!2e10!3e12!7i7680!8i3840

Picture 3
https://www.google.es/maps/@-25.2785229,-57.6385725,3a,75y,222.75h,89.8t/data=!3m10!1e1!3m8!1sAF1QipM01Yxc6fffmzE55dfqM8lLoIPZRhBCDgyNf-Pe!2e10!3e12!7i7680!8i3840!9m2!1b1!2i37

Picture 4

https://www.google.es/maps/@-25.2788295,-57.6387403,3a,75y,201.05h,90.77t/data=!3m10!1e1!3m8!1sAF1QipM0m2CiXTJDNAfMCB91cYobNG19Tr5p15XMnaxZ!2e10!3e12!7i7680!8i3840!9m2!1b1!2i37

Figure 18

Player has to locate all possible passwords in this picture, especially in the red square, and player must consider to locate numbers (challenge description)

https://www.google.es/maps/@-25.2788877,-57.6387783,3a,25.2y,266.22h,94.84t/data=!3m10!1e1!3m8!1sAF1QipM4yqKdAkoNPJ_DnwLdYFVxRtf0vf4NGcWpO5Dt!2e10!3e12!7i7680!8i3840!9m2!1b1!2i37

Figure 19

Finally, to open location.7Z player must use just numbers 880000.

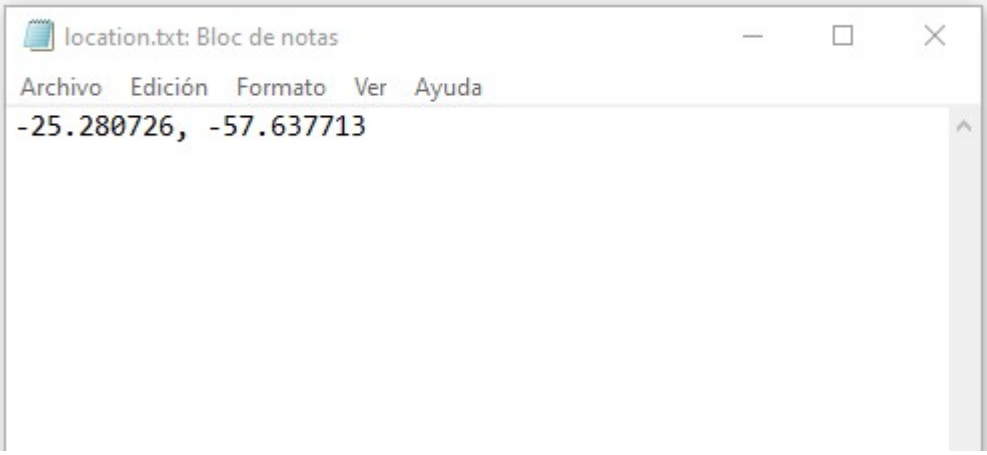


Figure 20

Flag Information

Flag{Latitude: -25.280726| Longitude: -57.637713 }