Mission Name

DataCardForensics_Android

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.

Location

SYLVARCON | SKYTECH HQ

Tools

- SQLITE Studio
- ALEAPP

Questions

Which is the Telegram user ID of Anderson?

- 1623170796

Which is the MAC Address of the Android device?

- fc:b4:e6:d5:1e:15

Which is the device ID of the Android device?

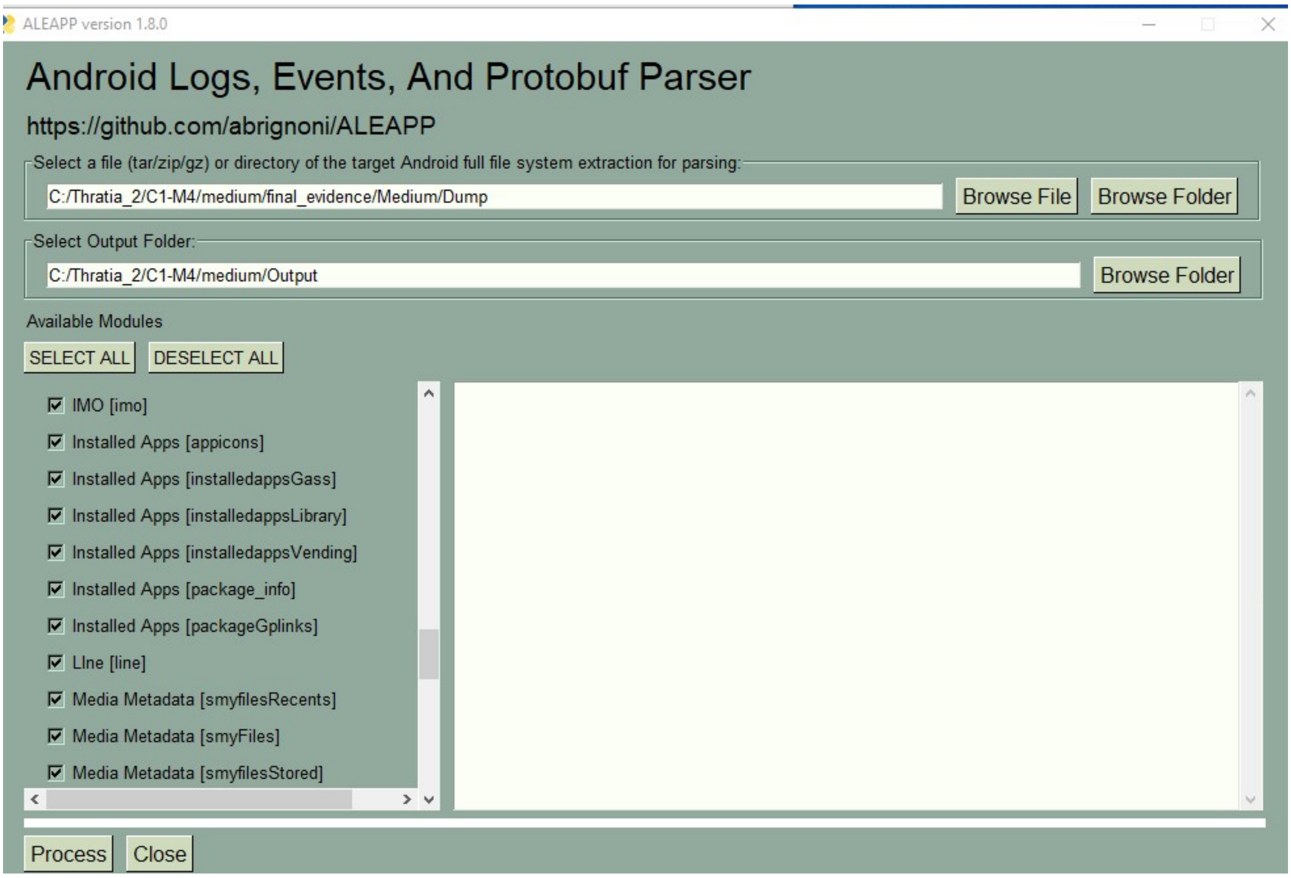
- 5af0678c46197d1

Hints

1. List Apps installed on the device.
2. Analyse Skype chats
3. To locate the password necessary to open the file, analyse Android Application Activity pictures.

Write Up

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



ALEAPP version 1.8.0

Android Logs, Events, And Protobuf Parser

https://github.com/abrignoni/ALEAPP

Select a file (tar/zip/gz) or directory of the target Android full file system extraction for parsing:

C:/Thratia_2/C1-M4/medium/final_evidence/Medium/Dump

Select Output Folder:

C:/Thratia_2/C1-M4/medium/Output

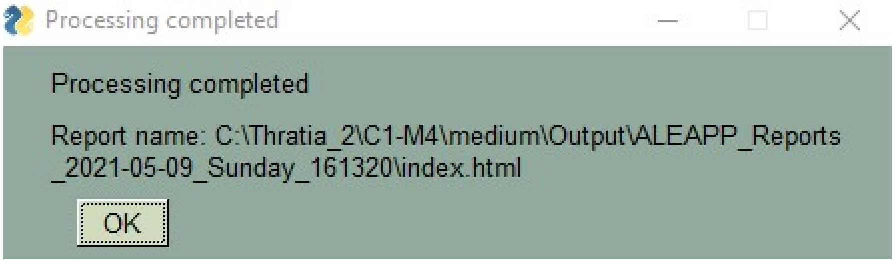
Available Modules

- ☑ IMO [imo]
- ☑ Installed Apps [appicons]
- ☑ Installed Apps [installedappsGass]
- ☑ Installed Apps [installedappsLibrary]
- ☑ Installed Apps [installedappsVending]
- ☑ Installed Apps [package_info]
- ☑ Installed Apps [packageGplinks]
- ☑ LIne [line]
- ☑ Media Metadata [smyfilesRecents]
- ☑ Media Metadata [smyFiles]
- ☑ Media Metadata [smyfilesStored]

Figure 1

Select all options, and finally select “Process”.

Once ALEAPP has finished, ALEAPP will show this message:

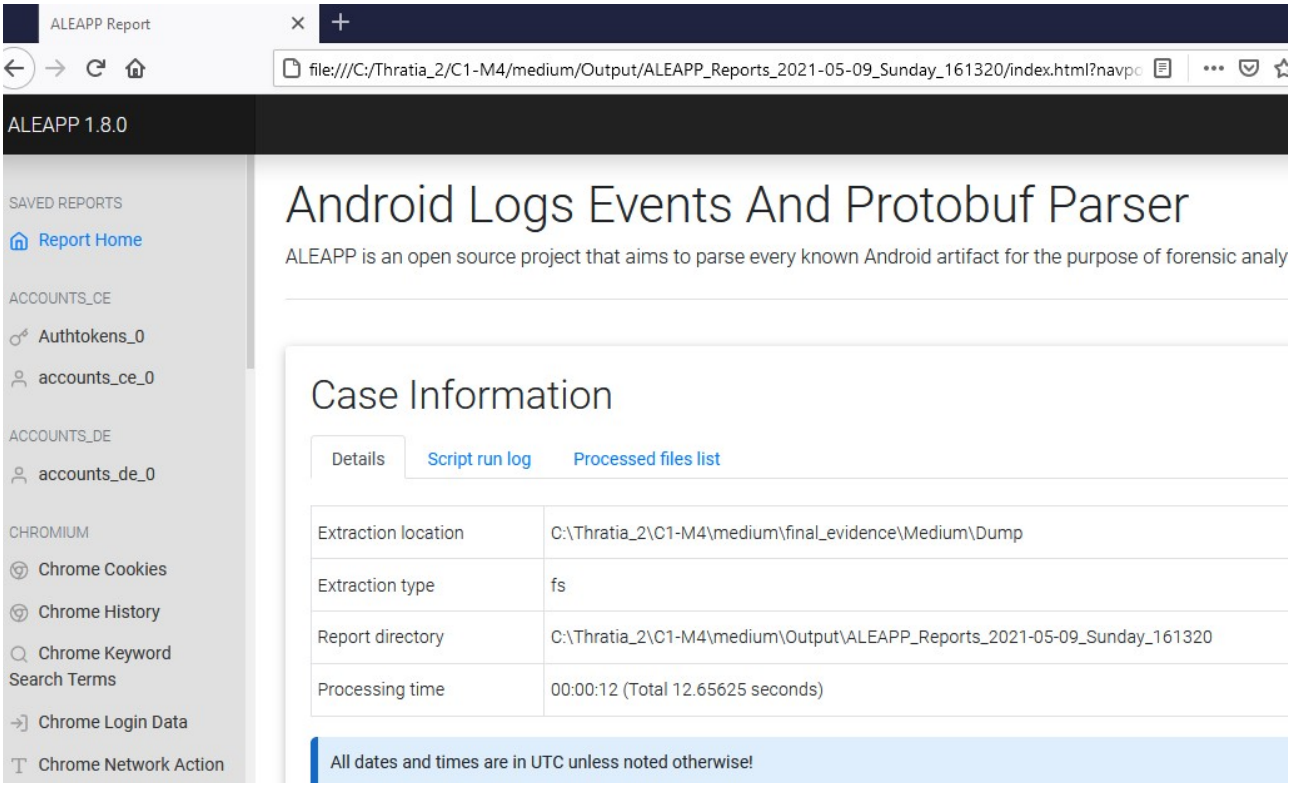


Processing completed

Report name: C:\Thratia_2\C1-M4\medium\Output\ALEAPP_Reports_2021-05-09_Sunday_161320\index.html

Figure 2

Open index.html



Android Logs Events And Protobuf Parser

ALEAPP is an open source project that aims to parse every known Android artifact for the purpose of forensic analy

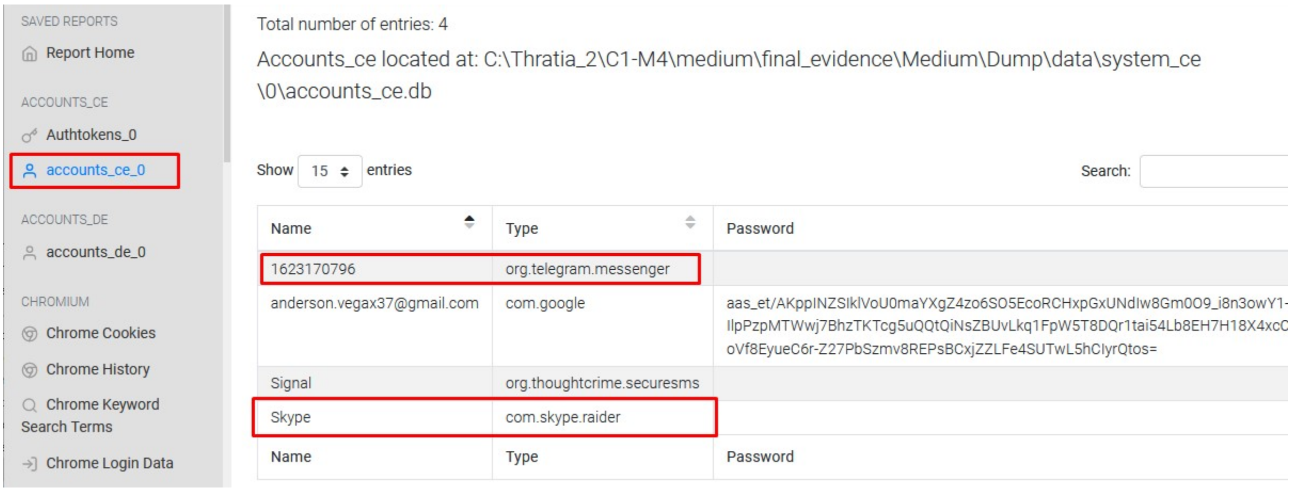
Case Information

Extraction location	C:\Thratia_2\C1-M4\medium\final_evidence\Medium\Dump
Extraction type	fs
Report directory	C:\Thratia_2\C1-M4\medium\Output\ALEAPP_Reports_2021-05-09_Sunday_161320
Processing time	00:00:12 (Total 12.65625 seconds)

All dates and times are in UTC unless noted otherwise!

Figure 3

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



Total number of entries: 4

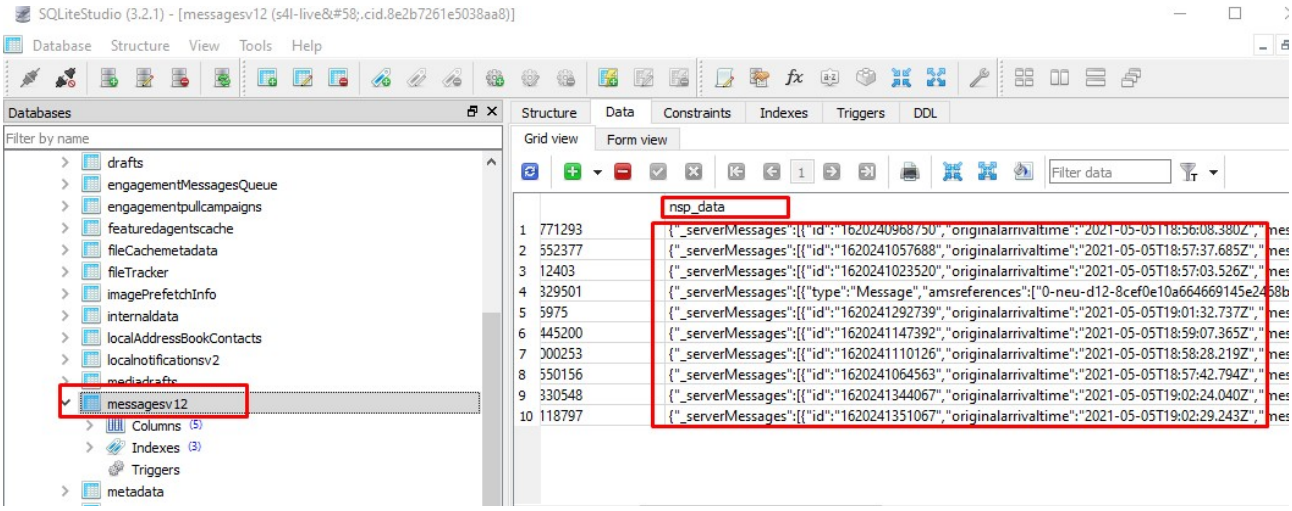
Accounts_ce located at: C:\Thratia_2\C1-M4\medium\final_evidence\Medium\Dump\data\system_ce \0\accounts_ce.db

Show 15 entries Search:

Name	Type	Password
1623170796	org.telegram.messenger	
anderson.vegax37@gmail.com	com.google	aas_et/AKppINZSIklVoU0maYXgZ4zo6SO5EcoRCHxpGxUNdIw8Gm0O9_i8n3owY1-IlpPzpMTWwj7BhzTKTcg5uQQtQiNsZBUvLkq1FpW5T8DQr1tai54Lb8EH7H18X4xcC oVf8EyueC6r-Z27PbSzmv8REPsBCxjZZLFe4SUTwL5hClyrQtos=
Signal	org.thoughtcrime.securesms	
Skype	com.skype.raider	
Name	Type	Password

Figure 4

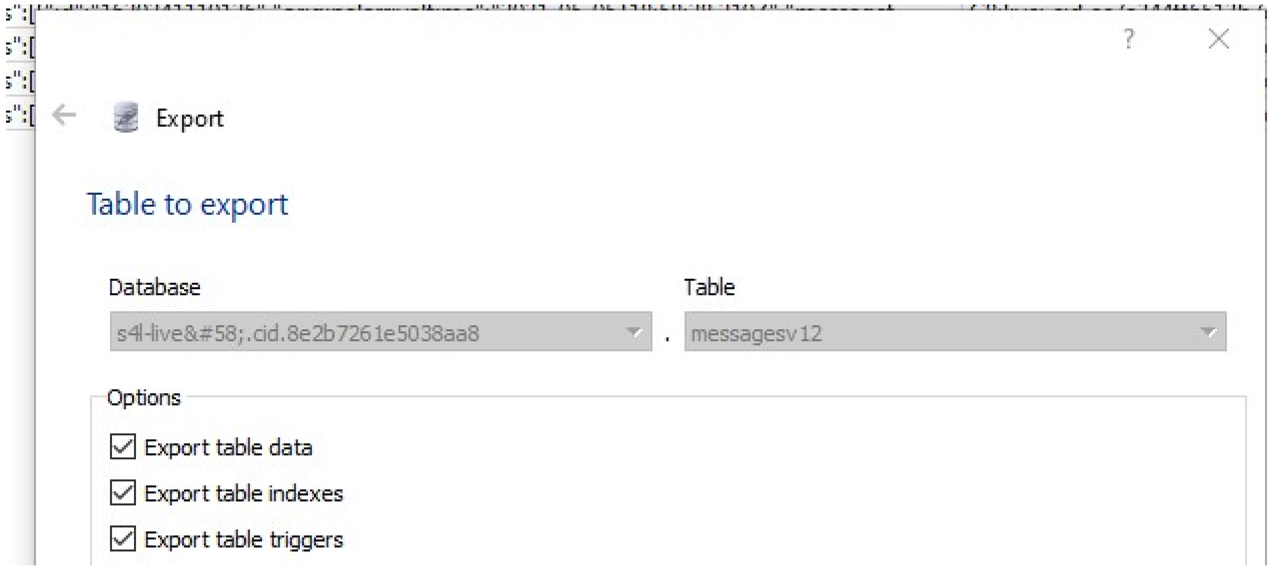
At this time, player must analyse Skype and Telegram chats, to locate any clue related to latitude or longitude. To analyse Skype, player must open SQLITE database located at: Dump\data\data\com.skype.raider\databases\s4l-live&#58;.cid.8e2b7261e5038aa8.db



		nsp_data
1	771293	{"_serverMessages":[{"id":"1620240968750","originalarrivaltime":"2021-05-05T18:56:08.380Z"," mes
2	552377	{"_serverMessages":[{"id":"1620241057688","originalarrivaltime":"2021-05-05T18:57:37.685Z"," mes
3	12403	{"_serverMessages":[{"id":"1620241023520","originalarrivaltime":"2021-05-05T18:57:03.526Z"," mes
4	329501	{"_serverMessages":[{"type":"Message","amsreferences":["0-neu-d12-8cef0e10a664669145e2458b
5	5975	{"_serverMessages":[{"id":"1620241292739","originalarrivaltime":"2021-05-05T19:01:32.737Z"," mes
6	445200	{"_serverMessages":[{"id":"1620241147392","originalarrivaltime":"2021-05-05T18:59:07.365Z"," mes
7	000253	{"_serverMessages":[{"id":"1620241110126","originalarrivaltime":"2021-05-05T18:58:28.219Z"," mes
8	550156	{"_serverMessages":[{"id":"1620241064563","originalarrivaltime":"2021-05-05T18:57:42.794Z"," mes
9	330548	{"_serverMessages":[{"id":"1620241344067","originalarrivaltime":"2021-05-05T19:02:24.040Z"," mes
10	118797	{"_serverMessages":[{"id":"1620241351067","originalarrivaltime":"2021-05-05T19:02:29.243Z"," mes

Figure 5

Messages could be found on table messagesv12 and column nsp_data. To perform a deep analyse, export table, selecting on the same table "export".



Export

Table to export

Database: s4l-live&#58;.cid.8e2b7261e5038aa8

Table: messagesv12

Options

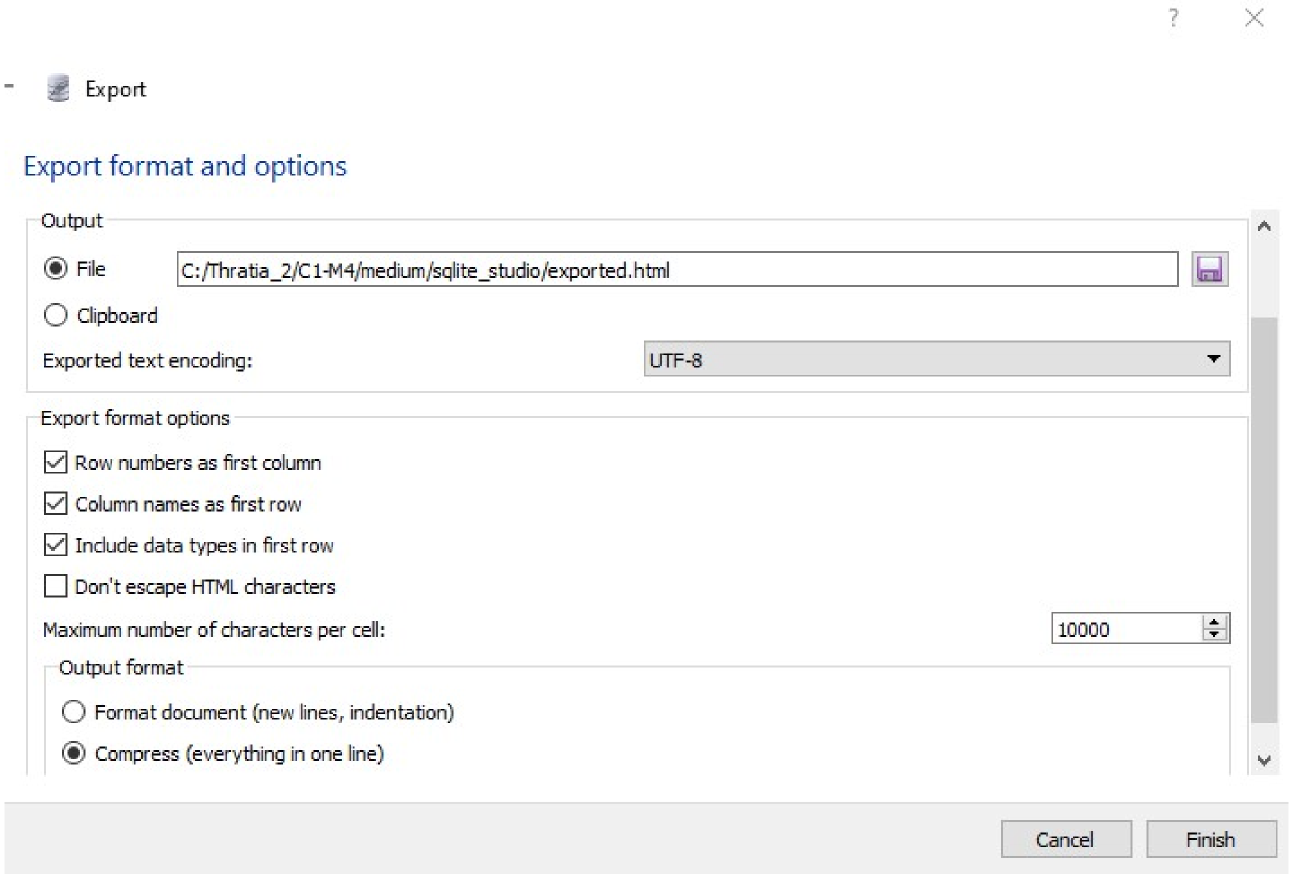
☑ Export table data

☑ Export table indexes

☑ Export table triggers

Figure 6

Fill the name and the path to export results:



Export

Export format and options

Output

● File C:/Thratia_2/C1-M4/medium/sqlite_studio/exported.html

○ Clipboard

Exported text encoding: UTF-8

Export format options

☑ Row numbers as first column

☑ Column names as first row

☑ Include data types in first row

☐ Don't escape HTML characters

Maximum number of characters per cell: 10000

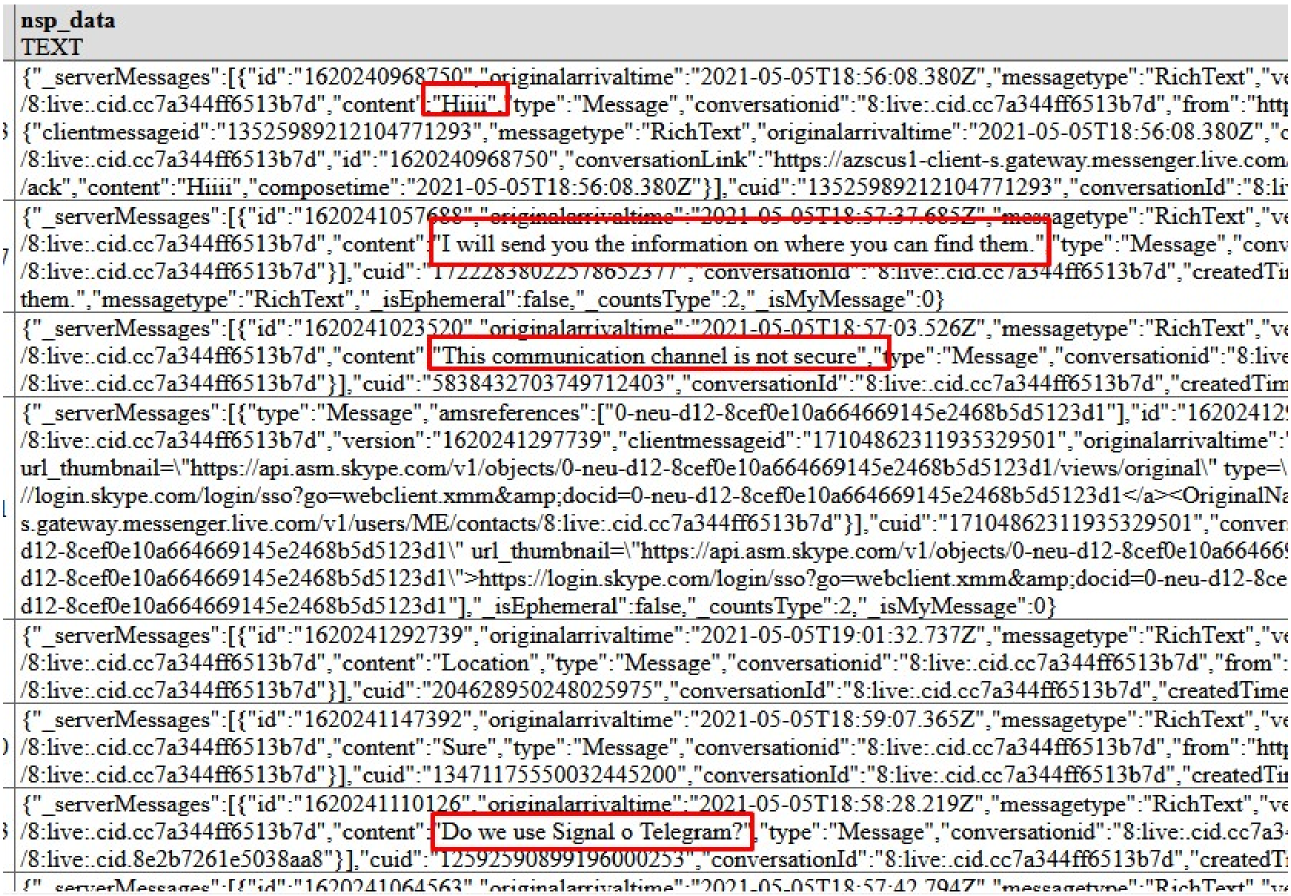
Output format

○ Format document (new lines, indentation)

● Compress (everything in one line)

Figure 7

Player should identify messages inside it:



```
nsp_data
TEXT
{"_serverMessages":[{"id":"1620240968750","originalarrivaltime":"2021-05-05T18:56:08.380Z","messagetype":"RichText","ve
/8:live:.cid.cc7a344ff6513b7d","content":"Hiiii","type":"Message","conversationid":"8:live:.cid.cc7a344ff6513b7d","from":"http
{"clientmessageid":"13525989212104771293","messagetype":"RichText","originalarrivaltime":"2021-05-05T18:56:08.380Z","c
/8:live:.cid.cc7a344ff6513b7d","id":"1620240968750","conversationLink":"https://azscus1-client-s.gateway.messenger.live.com
/ack","content":"Hiiii","composetime":"2021-05-05T18:56:08.380Z"}],"cuid":"13525989212104771293","conversationId":"8:li
{"_serverMessages":[{"id":"1620241057688","originalarrivaltime":"2021-05-05T18:57:37.685Z","messagetype":"RichText","ve
/8:live:.cid.cc7a344ff6513b7d","content":"I will send you the information on where you can find them.","type":"Message","conv
/8:live:.cid.cc7a344ff6513b7d"}],"cuid":"17222838022578652377","conversationId":"8:live:.cid.cc7a344ff6513b7d","createdTi
them.","messagetype":"RichText","_isEphemeral":false,"_countsType":2,"_isMyMessage":0}
{"_serverMessages":[{"id":"1620241023520","originalarrivaltime":"2021-05-05T18:57:03.526Z","messagetype":"RichText","ve
/8:live:.cid.cc7a344ff6513b7d","content":"This communication channel is not secure","type":"Message","conversationid":"8:live
/8:live:.cid.cc7a344ff6513b7d"}],"cuid":"5838432703749712403","conversationId":"8:live:.cid.cc7a344ff6513b7d","createdTim
{"_serverMessages":[{"type":"Message","amsreferences":["0-neu-d12-8cef0e10a664669145e2468b5d5123d1"],"id":"16202412
/8:live:.cid.cc7a344ff6513b7d","version":"1620241297739","clientmessageid":"17104862311935329501","originalarrivaltime":
url_thumbnail=\"https://api.asm.skype.com/v1/objects/0-neu-d12-8cef0e10a664669145e2468b5d5123d1/views/original\" type=\
//login.skype.com/login/sso?go=webclient.xmm&amp;docid=0-neu-d12-8cef0e10a664669145e2468b5d5123d1</a><OriginalNa
s.gateway.messenger.live.com/v1/users/ME/contacts/8:live:.cid.cc7a344ff6513b7d"}],"cuid":"17104862311935329501","conver
d12-8cef0e10a664669145e2468b5d5123d1\" url_thumbnail=\"https://api.asm.skype.com/v1/objects/0-neu-d12-8cef0e10a66466
d12-8cef0e10a664669145e2468b5d5123d1\">https://login.skype.com/login/sso?go=webclient.xmm&amp;docid=0-neu-d12-8ce
d12-8cef0e10a664669145e2468b5d5123d1"],"_isEphemeral":false,"_countsType":2,"_isMyMessage":0}
{"_serverMessages":[{"id":"1620241292739","originalarrivaltime":"2021-05-05T19:01:32.737Z","messagetype":"RichText","ve
/8:live:.cid.cc7a344ff6513b7d","content":"Location","type":"Message","conversationid":"8:live:.cid.cc7a344ff6513b7d","from":
/8:live:.cid.cc7a344ff6513b7d"}],"cuid":"2046289502480259 75","conversationId":"8:live:.cid.cc7a344ff6513b7d","createdTime
{"_serverMessages":[{"id":"1620241147392","originalarrivaltime":"2021-05-05T18:59:07.365Z","messagetype":"RichText","ve
/8:live:.cid.cc7a344ff6513b7d","content":"Sure","type":"Message","conversationid":"8:live:.cid.cc7a344ff6513b7d","from":"http
/8:live:.cid.cc7a344ff6513b7d"}],"cuid":"13471175550032445200","conversationId":"8:live:.cid.cc7a344ff6513b7d","createdTi
{"_serverMessages":[{"id":"1620241110126","originalarrivaltime":"2021-05-05T18:58:28.219Z","messagetype":"RichText","ve
/8:live:.cid.cc7a344ff6513b7d","content":"Do we use Signal o Telegram?","type":"Message","conversationid":"8:live:.cid.cc7a3
/8:live:.cid.8e2b7261e5038aa8"}],"cuid":"12592590899196000253","conversationId":"8:live:.cid.cc7a344ff6513b7d","createdT
{"_serverMessages":[{"id":"1620241064563","originalarrivaltime":"2021-05-05T18:57:42.794Z","messagetype":"RichText","ve
```

Figure 8

Keep in mind Skytech´s mole is Anderson with Skype ID **8e2b7261e5038aa8**

live:.cid.cc7a344ff6513b7d
05/05/2021 18:56:08
Hiiii

live:.cid.cc7a344ff6513b7d
05/05/2021 18:57:03
This communication channel is not secure

live:.cid.cc7a344ff6513b7d
05/05/2021 18:57:37
I will send you the information on where you can find them.
live:.cid.8e2b7261e5038aa8
05/05/2021 18:57:44
Ok

live:.cid.8e2b7261e5038aa8
05/05/2021 18:58:30

Do we use Signal o Telegram?

live:.cid.cc7a344ff6513b7d
05/05/2021 18:59:07
Sure

live:.cid.cc7a344ff6513b7d
05/05/2021 19:01:32
Location

live:.cid.cc7a344ff6513b7d
05/05/2021 19:01:37

live:.cid.cc7a344ff6513b7d shared Location.7z with the conversation

live:.cid.cc7a344ff6513b7d
05/05/2021 19:02:24
Password through another channel

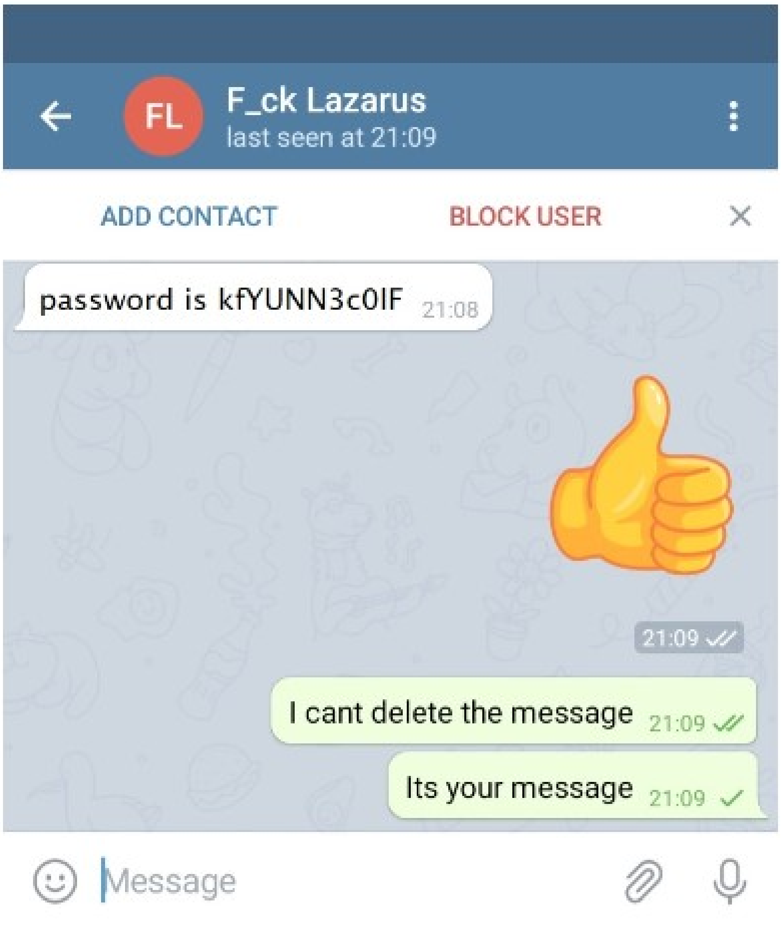
live:.cid.8e2b7261e5038aa8
05/05/2021 19:02:31
Ok

Checking previous conversation, there is a file called Location.7z sent by the other person to Anderson, a they are talking about a Password. Files on Skype APP, are downloaded here:

- \data\media\0\Download\Location.7z

And it´s necessary to know the password to open the file “Location.7z”. Player must analyse all chats to identify password, but the clue to get the password is a picture located Dump\data\system_ce\0\snapshots\41.jpg. This is an image of the telegram conversation where you can see that there is a password.

This image is real, and it is made by Android in the context of **Android Application Activity.**



password is kfYUNN3c0lF 21:08

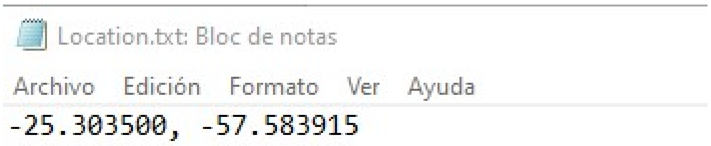
21:09

I cant delete the message 21:09

Its your message 21:09

Figure 9

So, finally player will able to open Location.7z an get latitude and longitude:


Location.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda

```
-25.303500, -57.583915
```

Figure 10

Flag Information

flag{Latitude: -25.303500 | Longitude: -57.583915 }