Challenge: The Crime Lab

Platform: CyberDefenders

Category: Endpoint Forensics

Difficulty: Easy

Tools Used: ALEAPP

Summary: This lab involved analysing an Android device using a forensic tool called ALEAPP. This is honestly one of the coolest labs I have done, I really enjoyed messing around with ALEAPP and seeing all that could be extracted by the tool. For those interested in mobile device forensics, I recommend giving this challenge a shot.

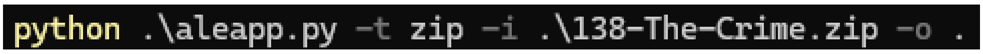
Scenario: We're currently in the midst of a murder investigation, and we've obtained the victim's phone as a key piece of evidence. After conducting interviews with witnesses and those in the victim's inner circle, your objective is to meticulously analyse the information we've gathered and diligently trace the evidence to piece together the sequence of events leading up to the incident.

Based on the accounts of the witnesses and individuals close to the victim, it has become clear that the victim was interested in trading. This has led him to invest all of his money and acquire debt. Can you identify the SHA256 of the trading application the victim primarily used on his phone?

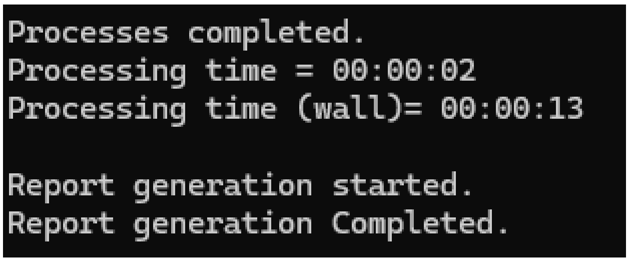
In order to answer this question, we need to install a tool called ALEAPP (Android Logs Events and Protobuf Parser). ALEAPP is an open-source analysis tool for Android devices. To install this tool, execute the following commands (in my case, I used Windows 11):

- git clone https://github.com/abrignoni/ALEAPP.git
- pip3 install -r requirements.txt

Before we execute ALEAPP against the given file, make sure to unzip the password protected lab zip file, and zip it again but without a password. After doing so, we can then execute the following command:

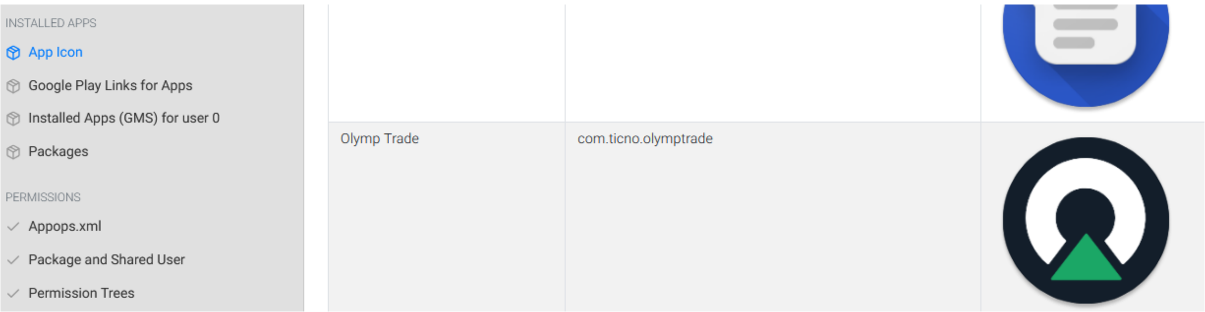


```
python .\aleapp.py -t zip -i .\138-The-Crime.zip -o .
```



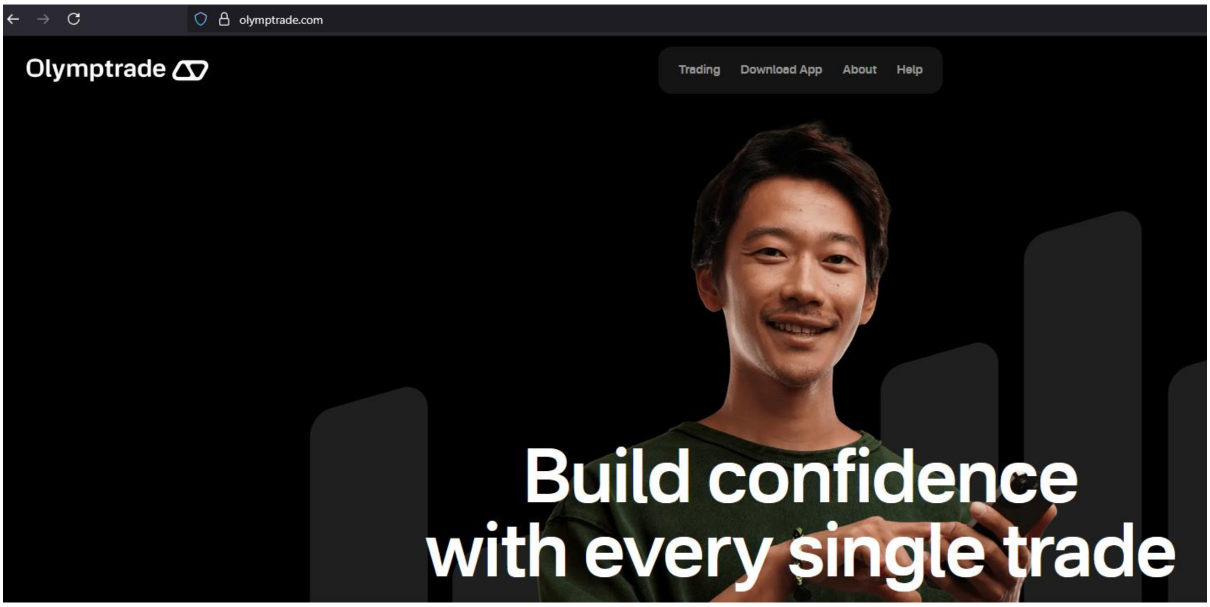
```
Processes completed.
Processing time = 00:00:02
Processing time (wall)= 00:00:13

Report generation started.
Report generation Completed.
```

Once completed, ALEAP creates a directory that contains all the extracted information. I am focusing on the index.html file. If you navigate to the App Icon section, we can see that this device had Olymp Trade installed:

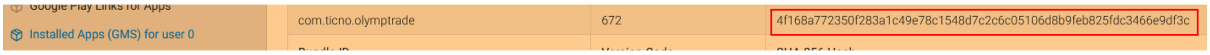


Olymp Trade	com.ticno.olymptrade	

Olymp Trade is an online trading platform:



You can find the SHA256 hash for this app in the Installed Apps (GMS) for user 0 section:

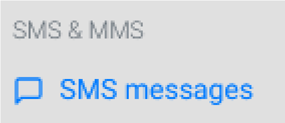


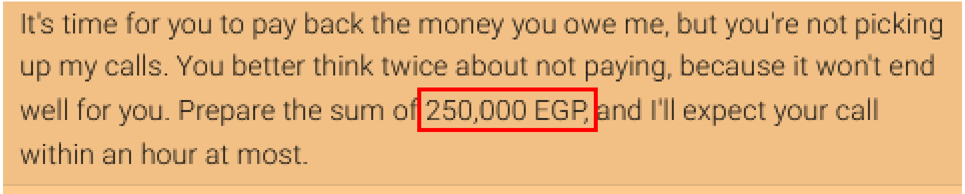
com.ticno.olymptrade	672	4f168a772350f283a1c49e78c1548d7c2c6c05106d8b9feb825fdc3466e9df3c

Answer: 4f168a772350f283a1c49e78c1548d7c2c6c05106d8b9feb825fdc3466e9df3c

According to the testimony of the victim's best friend, he said, "While we were together, my friend got several calls he avoided. He said he owed the caller a lot of money but couldn't repay now". How much does the victim owe this person?

Under the SMS messages section, you can find one SMS message:



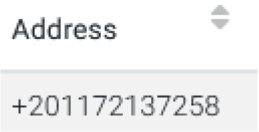


It's time for you to pay back the money you owe me, but you're not picking up my calls. You better think twice about not paying, because it won't end well for you. Prepare the sum of 250,000 EGP, and I'll expect your call within an hour at most.

Answer: 250000

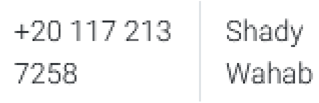
What is the name of the person to whom the victim owes money?

Under the "SMS messages" section, you can see the source phone number of a message:



Address
+201172137258

If you then navigate to the "Contacts" section, you can find the display name associated with this number:

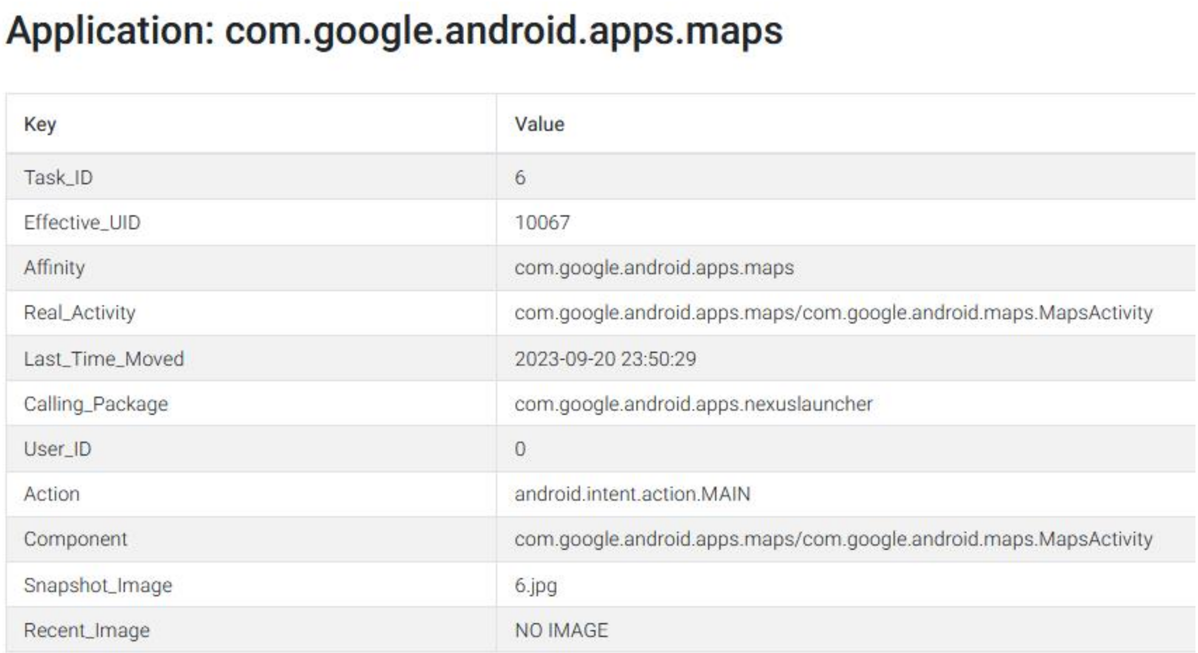


+20 117 213 7258	Shady Wahab

Answer: Shady Wahab

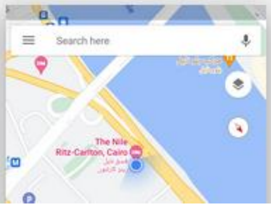
Based on the statement from the victim's family, they said that on September 20, 2023, he departed from his residence without informing anyone of his destination. Where was the victim located at that moment?

If you navigate to the "Recent Activity 0" section, we can see a snapshot image from google maps:



Application: com.google.android.apps.maps

Key	Value
Task_ID	6
Effective_UID	10067
Affinity	com.google.android.apps.maps
Real_Activity	com.google.android.apps.maps/com.google.android.maps.MapsActivity
Last_Time_Moved	2023-09-20 23:50:29
Calling_Package	com.google.android.apps.nexuslauncher
User_ID	0
Action	android.intent.action.MAIN
Component	com.google.android.apps.maps/com.google.android.maps.MapsActivity
Snapshot_Image	6.jpg
Recent_Image	NO IMAGE

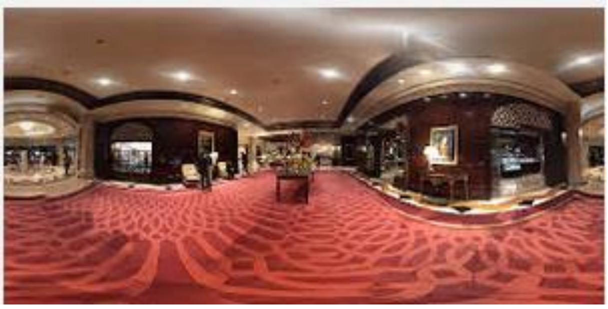
Snapshot_Image	Recent_Image
	No Image

If you open the image, you can see that the victim was located at The Nile Ritz-Carlton.

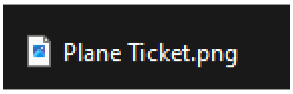
Answer: The Nile Ritz-Carlton

The detective continued his investigation by questioning the hotel lobby. She informed him that the victim had reserved the room for 10 days and had a flight scheduled thereafter. The investigator believes that the victim may have stored his ticket information on his phone. Look for where the victim intended to travel.

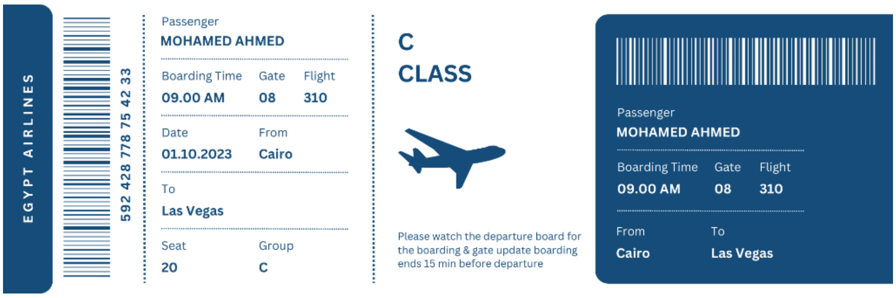
Within the “Image Manager Cache” section, I can see photos from google maps that appear to be of a casino within Las Vegas:



Alternatively, if you navigate to \138-The-Crime\temp_extract_dir\data\media\0\Download, you can see an image called “Plane Ticket.png”:



Plane Ticket.png



EGYPT AIRLINES

592 428 778 75 42 33

Passenger
MOHAMED AHMED

Boarding Time 09.00 AM
Gate 08
Flight 310

Date 01.10.2023
From Cairo

To
Las Vegas

Seat 20
Group C

C
CLASS

Please watch the departure board for the boarding & gate update boarding ends 15 min before departure

Passenger
MOHAMED AHMED

Boarding Time 09.00 AM
Gate 08
Flight 310

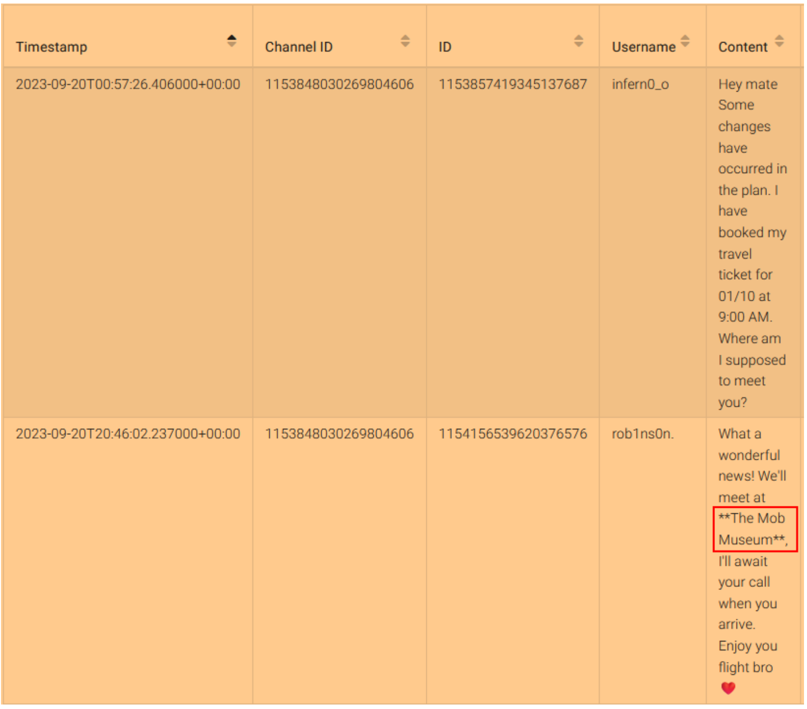
From Cairo
To Las Vegas

As you can see, this is a plane ticket to Las Vegas, which suggests that MOHAMED AHMED was intending to travel to Vegas.

Answer: Las Vegas

After examining the victim's Discord conversations, we discovered he had arranged to meet a friend at a specific location. Can you determine where this meeting was supposed to occur?

ALEAP has an entire section dedicated to Discord Chats. Within this section, it was able to extract two messages, one being a reply containing a location to meet:



Timestamp	Channel ID	ID	Username	Content
2023-09-20T00:57:26.406000+00:00	1153848030269804606	1153857419345137687	infern0_o	Hey mate Some changes have occurred in the plan. I have booked my travel ticket for 01/10 at 9:00 AM. Where am I supposed to meet you?
2023-09-20T20:46:02.237000+00:00	1153848030269804606	1154156539620376576	rob1ns0n.	What a wonderful news! We'll meet at **The Mob Museum**, I'll await your call when you arrive. Enjoy you flight bro ❤️

Answer: The Mob Museum