The Crime Lab (Cyber Defenders) - Walkthrough

Tuesday, September 24, 2024 4:22 PM

Story:
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 analyze the information we've gathered and diligently trace the evidence to piece together the sequence of events leading up to the incident.

Q1: 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 which trading application the victim primarily used on his phone?

- I initially parsed all the Android data using ALEAPP and received a detailed report.
  In the 'Installed Apps' section, I found several apps, one of which referenced the trading app 'Olymp Trade'.

Installed Apps report

Total number of entries: 5

Installed Apps located at: C:\Users\FlareVM\Desktop\data\data\com.google.android.gms\databases\gass.db

Show 15 entries Sea

Bundle ID	Version Code	SHA-256 Hash
com.discord	194017	cb8511953a2b33be0a5291dd2af23fecdcd02a9df7b1752aa549bea89d3aad30
com.discord	186011	bc85ef24fbf124c7fae1614a49265467b7cb70d04e6da79da92ea2bcaedf09cc
com.discord	149011	70526fd3a0f9d795984157bc06e1baa6f4685bd8f893c6fd2fa359b72fa655e4
com.google.android.youtube	1419573700	fb09675ed6b64e56319cc85d956f194319f5faa41be6e010dbf1c1f021f2c033
com.ticno.olymptrade	672	4f168a772350f283a1c49e78c1548d7c2c6c05106d8b9feb825fdc3466e9df3c
Bundle ID	Version Code	SHA-256 Hash

Q2: 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?

- In the 'SMS Messages' section, I found a message from the number '+201172137258'. The message body read: '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.'
  This indicates that the victim was in debt for 250,000 EGP.

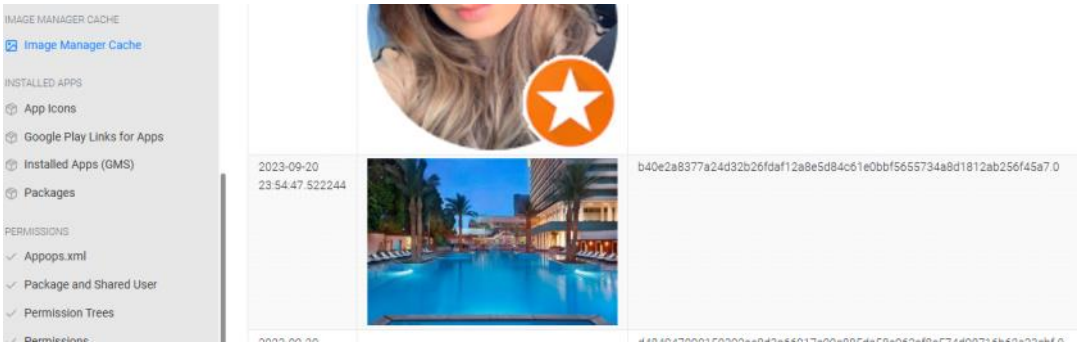
Q3: What is the name of the person to whom the victim owes money?

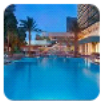
- I searched for the attacker's number in the 'Contacts' section and found his phone number listed under the name 'Shady Wahab'.

vnd.android.cursor.item/phone_v2	+20 117 213 7258	Shady Wahab	+20 117 213 7258		\\?\C:\Users\FlareVM\Desktop\data\data\com.android.providers.contacts\databases\contacts2.db

Q4: 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?

- I navigated through the 'Image Manger Cache' and found a photo of an hotel on the data the victim disappeared.
  I took the hotel to Google and found the name of the hotel.

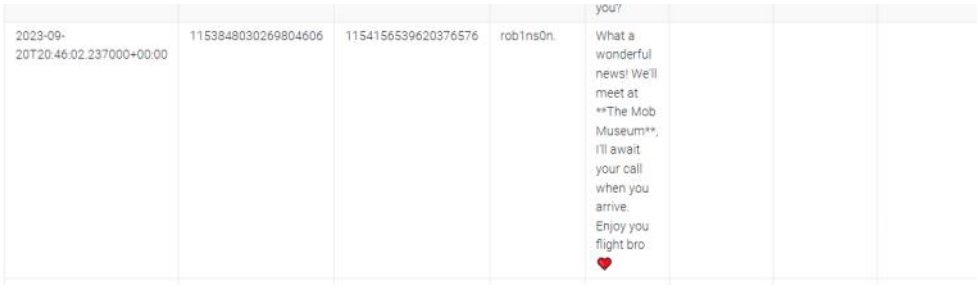




The Nile Ritz-Carlton Cairo- Cairo, Egypt Hotels- Deli

Q5: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.

- I noticed a discord chat between the victim to other person, I identified they will meet at 'The Mob Museum' which located in 'Las Vegas'



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 ❤️

Q6: 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?

- We already found it in the question above.