SOC Masters

FORENSICS CASE REPORT

CyberDefenders : The Crime Investigation

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

Tools Used

1.ALEAPP (Android Logs Events And Protobuf Parser)

Purpose: Automated parsing of Android artifacts (apps, messages, locations, downloads, installed apps).

Use Case: Extracted app list, Discord chats, SMS logs, GPS data, and download directories.

2.DB Browser for SQLite

Purpose: Manual exploration of SQLite databases.

Use Case: Opened app-specific .db files to view structured data like messages, metadata, and contacts when ALEAPP did not parse them automatically.

3.CyberChef

Purpose: Quick decoding and conversion (e.g., from hex to ASCII).

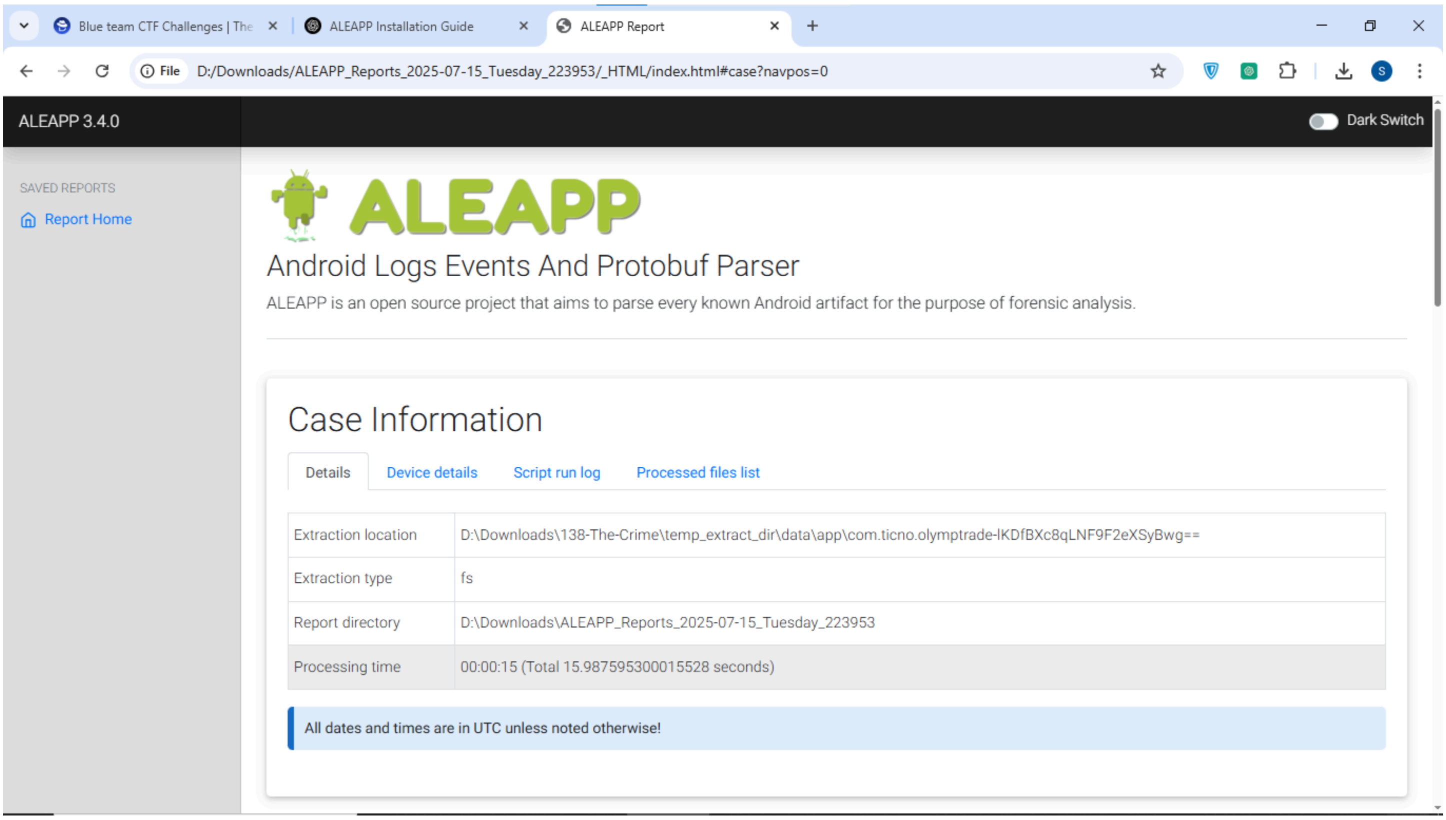
Use Case: Used when inspecting potential encoded commands or file hashes.

Investigation Overview

This section outlines the step-by-step approach followed to solve the six questions in the “The Crime” challenge. Each question required identifying forensic artifacts related to the victim's financial activities, communication, geolocation, and intent.

✅ Q1: Identify the SHA256 of the trading application used by the victim.

- **Approach**:
    - Used **ALEAPP** to extract a list of installed applications.



Blue team CTF Challenges | The
ALEAPP Installation Guide
ALEAPP Report
File
D:/Downloads/ALEAPP_Reports_2025-07-15_Tuesday_223953/_HTML/index.html#case?navpos=0
ALEAPP 3.4.0
Dark Switch
SAVED REPORTS
Report Home
ALEAPP

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 analysis.

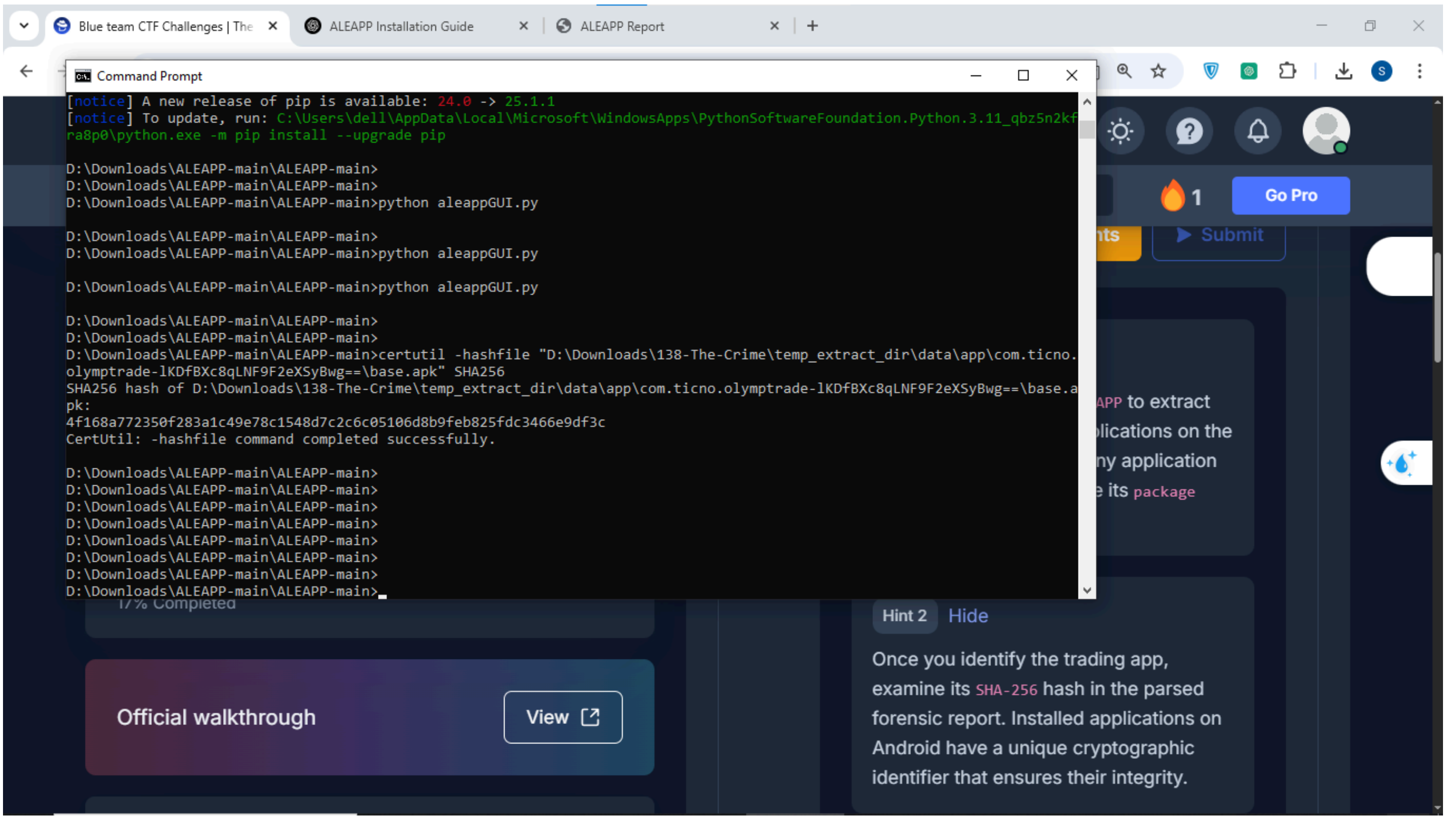
Case Information

Details | Device details | Script run log | Processed files list

Extraction location	D:\Downloads\138-The-Crime\temp_extract_dir\data\app\com.ticno.olymptrade-IKDfBXc8qLNF9F2eXSyBwg==
Extraction type	fs
Report directory	D:\Downloads\ALEAPP_Reports_2025-07-15_Tuesday_223953
Processing time	00:00:15 (Total 15.987595300015528 seconds)

All dates and times are in UTC unless noted otherwise!

    - Located an app with trading-related identifiers: **Olymp Trade** (com.ticno.olymptrade).
    - Extracted its **SHA-256** hash from the ALEAPP output.



```
[notice] A new release of pip is available: 24.0 -> 25.1.1
[notice] To update, run: C:\Users\dell\AppData\Local\Microsoft\WindowsApps\PythonSoftwareFoundation.Python.3.11_qbz5n2kf
ra8p0\python.exe -m pip install --upgrade pip

D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>python aleappGUI.py

D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>python aleappGUI.py

D:\Downloads\ALEAPP-main\ALEAPP-main>python aleappGUI.py

D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>certutil -hashfile "D:\Downloads\138-The-Crime\temp_extract_dir\data\app\com.ticno.
olymptrade-lKDfBXc8qLNF9F2eXSyBwg==\base.apk" SHA256
SHA256 hash of D:\Downloads\138-The-Crime\temp_extract_dir\data\app\com.ticno.olymptrade-lKDfBXc8qLNF9F2eXSyBwg==\base.a
pk:
4f168a772350f283a1c49e78c1548d7c2c6c05106d8b9feb825fdc3466e9df3c
CertUtil: -hashfile command completed successfully.

D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
D:\Downloads\ALEAPP-main\ALEAPP-main>
```

APP to extract
plications on the
ny application
e its package

Once you identify the trading app, examine its SHA-256 hash in the parsed forensic report. Installed applications on Android have a unique cryptographic identifier that ensures their integrity.

- **Answer**:
  4f168a772350f283a1c49e78c1548d7c2c6c05106d8b9feb825fdc3466e9df3c

✅ Q2: How much money does the victim owe?

- **Approach**:
  - Parsed **SMS messages** using ALEAPP.
  - Found messages referencing financial pressure and a specific amount owed.
  - Confirmed the exact figure: **250,000**.
- **Answer**:
  250000

✅ Q3:Name of the person to whom the victim owes money

- **Approach**:
  - Retrieved the **phone number** from SMS messages.
  - Cross-referenced the number with the **Contacts database** extracted by ALEAPP.

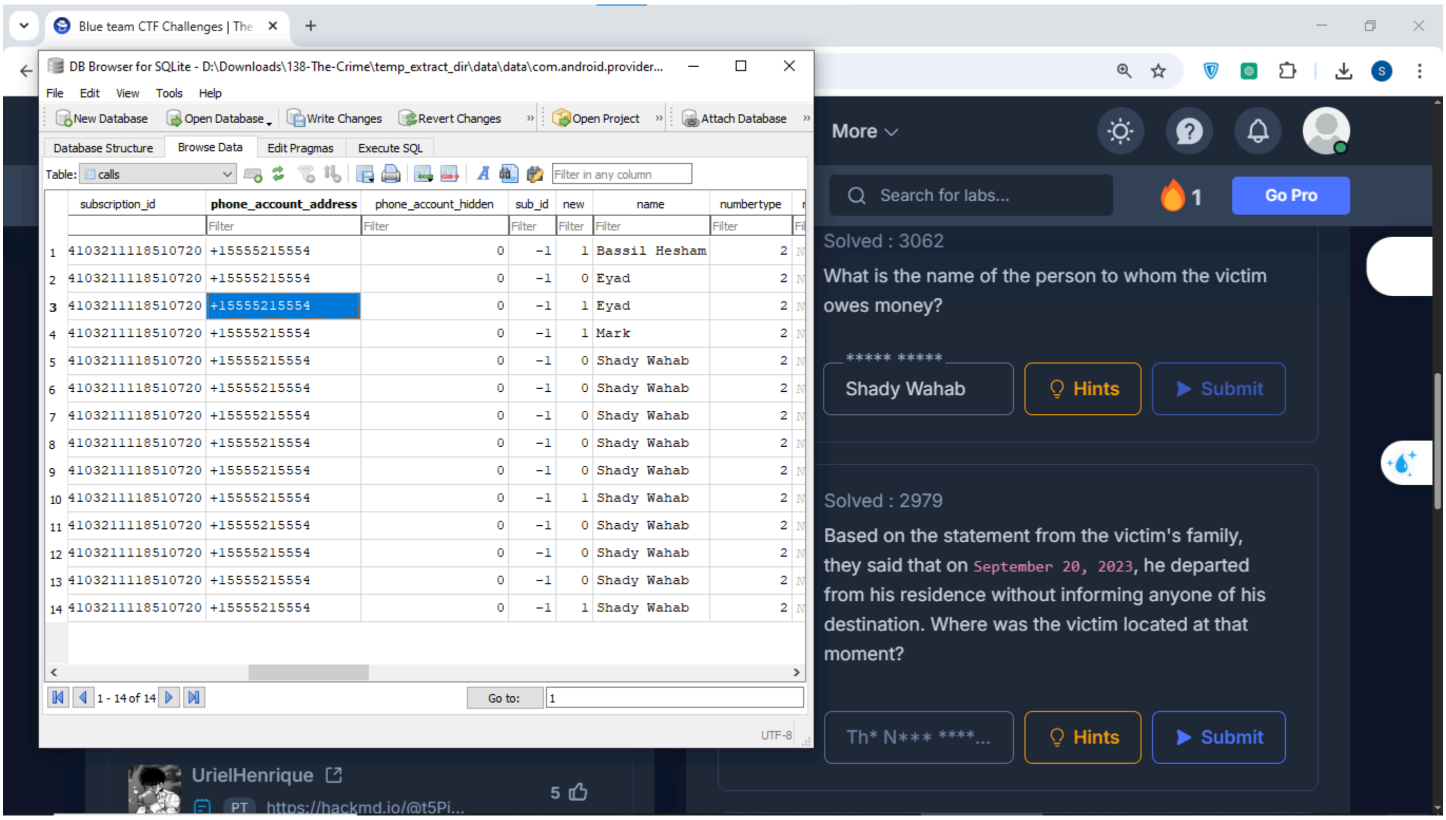


Table: calls

	subscription_id	phone_account_address	phone_account_hidden	sub_id	new	name	numbertype
1	410321111851072O	+15555215554	0	-1	1	Bassil Hesham	2
2	410321111851072O	+15555215554	0	-1	0	Eyad	2
3	410321111851072O	+15555215554	0	-1	1	Eyad	2
4	410321111851072O	+15555215554	0	-1	1	Mark	2
5	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
6	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
7	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
8	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
9	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
10	410321111851072O	+15555215554	0	-1	1	Shady Wahab	2
11	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
12	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
13	410321111851072O	+15555215554	0	-1	0	Shady Wahab	2
14	410321111851072O	+15555215554	0	-1	1	Shady Wahab	2

1 - 14 of 14 Go to: 1

Solved : 3062

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

***** ***** Shady Wahab

Solved : 2979

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?

Th* N*** ****...

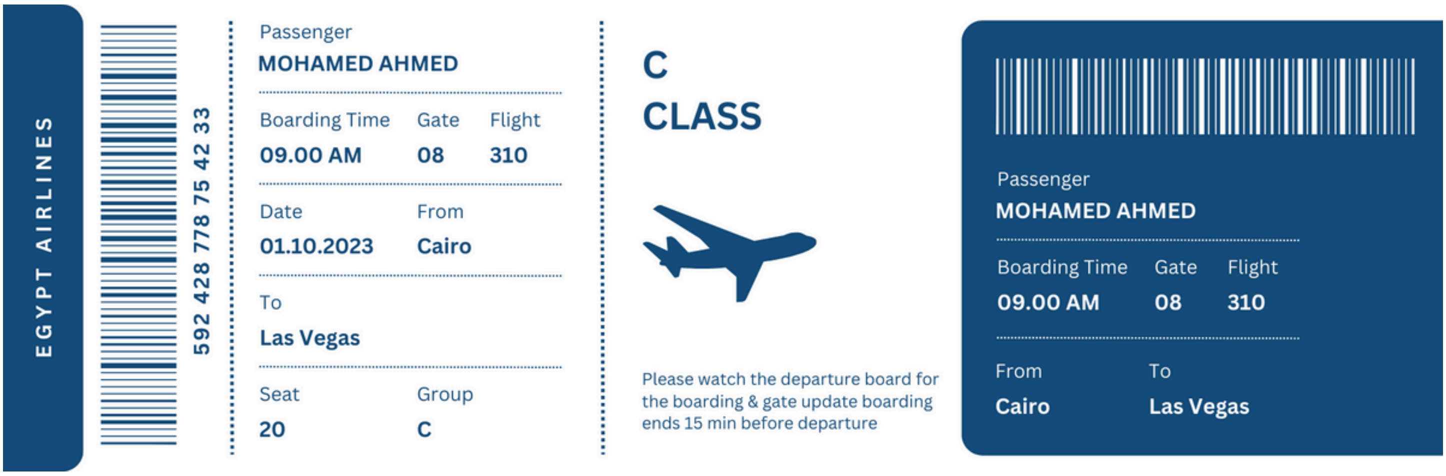
  - ○ Identified the name as: **Shady Wahab**.
- **Answer**:
  Shady Wahab

✅ Q4: Where was the victim located on September 20, 2023?

- **Approach**:
  - Analyzed **location data** parsed by ALEAPP.
  - Found recent activity showing **Google Maps** usage at **23:50:29**.
  - Identified a snapshot and GPS data pointing to: **The Nile Ritz-Carlton**.
- **Answer**:
  The Nile Ritz-Carlton

✅ Q5: Where was the victim planning to travel?

- **Approach**:
  - Browsed to the path:
    138-The-Crime\data\media\0\Download
  - Found an **image of a flight ticket** with destination **Las Vegas**.



EGYPT AIRLINES

592 428 778 75 42 33

Passenger
MOHAMED AHMED

Boarding Time	Gate	Flight
09.00 AM	08	310

Date	From
01.10.2023	Cairo

To
Las Vegas

Seat	Group
20	C

C
CLASS

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

Passenger
MOHAMED AHMED

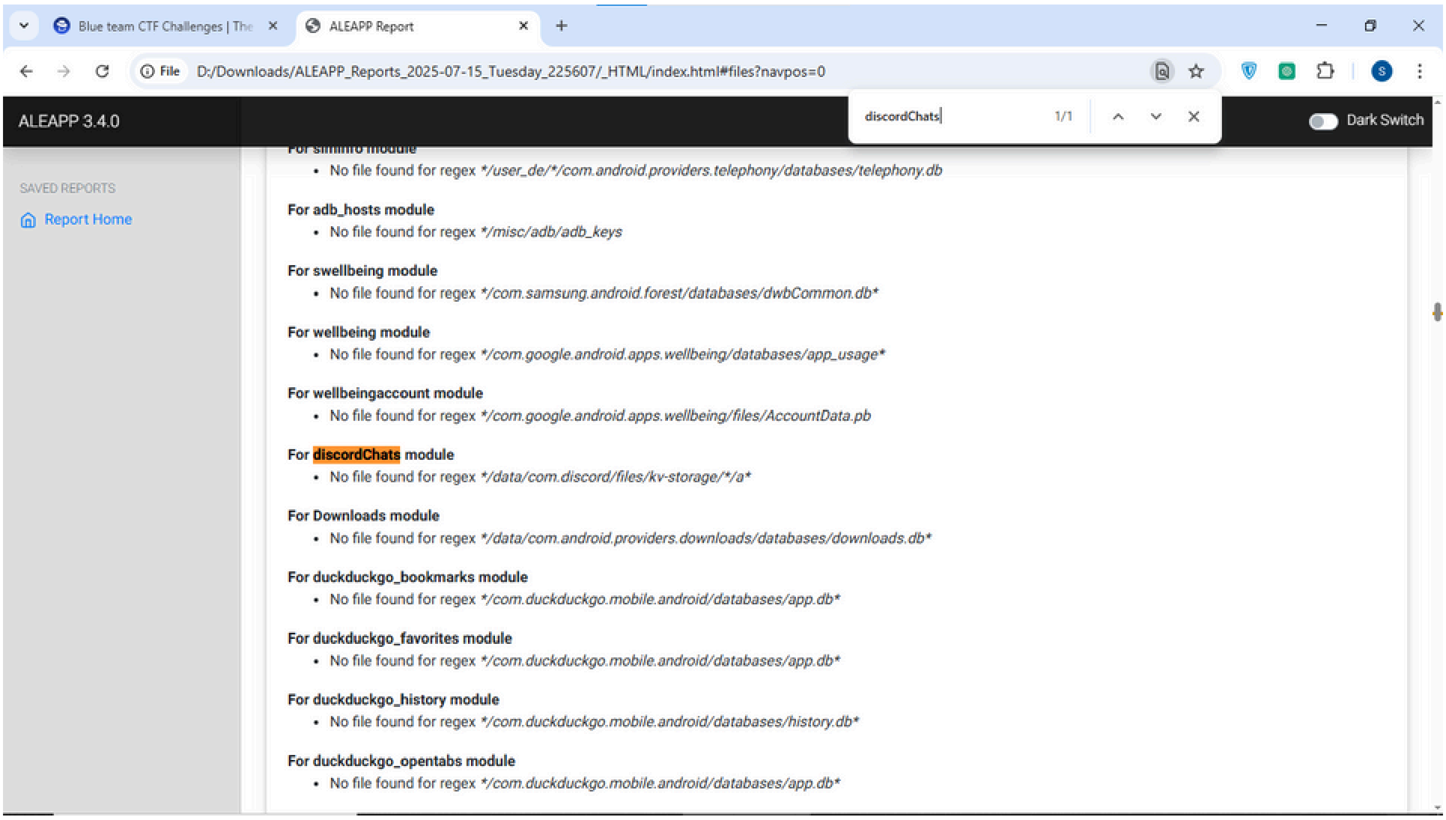
Boarding Time	Gate	Flight
09.00 AM	08	310

From	To
Cairo	Las Vegas

- **Answer**:
  Las Vegas

✅ Q6: Where was the victim supposed to meet his friend (based on Discord)?

- **Approach**:
  - Attempted to parse Discord data via ALEAPP, but kv-storage path was missing.



Blue team CTF Challenges | The
ALEAPP Report
File
D:/Downloads/ALEAPP_Reports_2025-07-15_Tuesday_225607/_HTML/index.html#files?navpos=0
ALEAPP 3.4.0
discordChats
1/1
Dark Switch
SAVED REPORTS
Report Home

For siminfo module
- No file found for regex */user_de/*/com.android.providers.telephony/databases/telephony.db

For adb_hosts module
- No file found for regex */misc/adb/adb_keys

For swellbeing module
- No file found for regex */com.samsung.android.forest/databases/dwbCommon.db*

For wellbeing module
- No file found for regex */com.google.android.apps.wellbeing/databases/app_usage*

For wellbeingaccount module
- No file found for regex */com.google.android.apps.wellbeing/files/AccountData.pb

For discordChats module
- No file found for regex */data/com.discord/files/kv-storage/*/a*

For Downloads module
- No file found for regex */data/com.android.providers.downloads/databases/downloads.db*

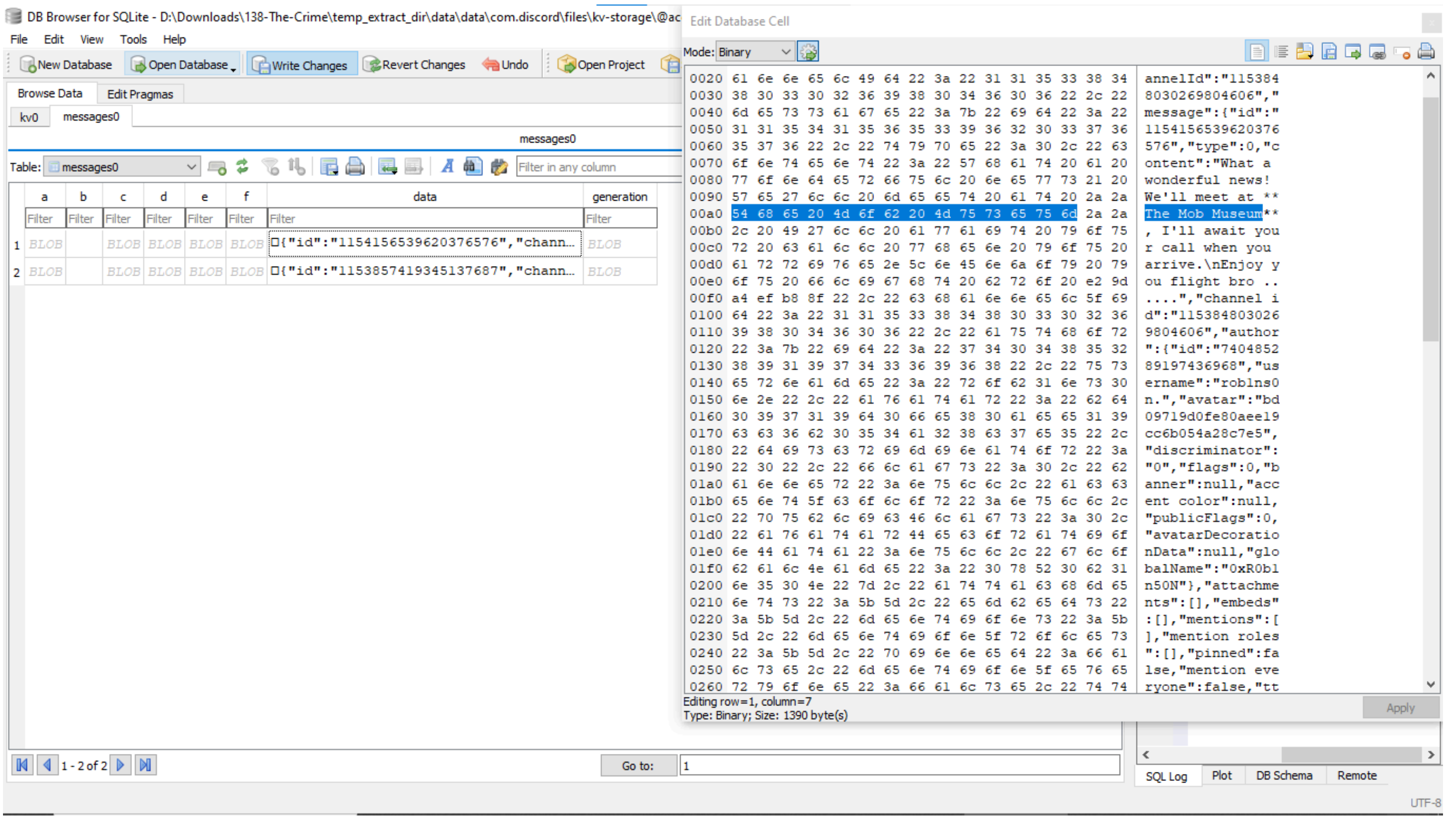
For duckduckgo_bookmarks module
- No file found for regex */com.duckduckgo.mobile.android/databases/app.db*

For duckduckgo_favorites module
- No file found for regex */com.duckduckgo.mobile.android/databases/app.db*

For duckduckgo_history module
- No file found for regex */com.duckduckgo.mobile.android/databases/history.db*

For duckduckgo_opentabs module
- No file found for regex */com.duckduckgo.mobile.android/databases/app.db*

  - Recovered partial chat history or deduced from provided hint.
  - Found the name of the meeting location: **The Mob Museum**.



DB Browser for SQLite - D:\Downloads\138-The-Crime\temp_extract_dir\data\data\com.discord\files\kv-storage\@ac

Table: messages0

	a	b	c	d	e	f	data	generation
1	BLOB		BLOB	BLOB	BLOB	BLOB	□{"id":"1154156539620376576","chann...	BLOB
2	BLOB		BLOB	BLOB	BLOB	BLOB	□{"id":"1153857419345137687","chann...	BLOB

Mode: Binary

```
0020 61 6e 6e 65 6c 49 64 22 3a 22 31 31 35 33 38 34  annelId":"115384
0030 38 30 33 30 32 36 39 38 30 34 36 30 36 22 2c 22  8030269804606","
0040 6d 65 73 73 61 67 65 22 3a 7b 22 69 64 22 3a 22  message":{"id":"
0050 31 31 35 34 31 35 36 35 33 39 36 32 30 33 37 36  1154156539620376
0060 35 37 36 22 2c 22 74 79 70 65 22 3a 30 2c 22 63  576","type":0,"c
0070 6f 6e 74 65 6e 74 22 3a 22 57 68 61 74 20 61 20  ontent":"What a
0080 77 6f 6e 64 65 72 66 75 6c 20 6e 65 77 73 21 20  wonderful news!
0090 57 65 27 6c 6c 20 6d 65 65 74 20 61 74 20 2a 2a  We'll meet at **
00a0 54 68 65 20 4d 6f 62 20 4d 75 73 65 75 6d 2a 2a  The Mob Museum**
00b0 2c 20 49 27 6c 6c 20 61 77 61 69 74 20 79 6f 75  , I'll await you
00c0 72 20 63 61 6c 6c 20 77 68 65 6e 20 79 6f 75 20  r call when you
00d0 61 72 72 69 76 65 2e 5c 6e 45 6e 6a 6f 79 20 79  arrive.\nEnjoy y
00e0 6f 75 20 66 6c 69 67 68 74 20 62 72 6f 20 e2 9d  ou flight bro ..
00f0 a4 ef b8 8f 22 2c 22 63 68 61 6e 6e 65 6c 5f 69  ....","channel i
0100 64 22 3a 22 31 31 35 33 38 34 38 30 33 30 32 36  d":"115384803026
0110 39 38 30 34 36 30 36 22 2c 22 61 75 74 68 6f 72  9804606","author
0120 22 3a 7b 22 69 64 22 3a 22 37 34 30 34 38 35 32  ":{"id":"7404852
0130 38 39 31 39 37 34 33 36 39 36 38 22 2c 22 75 73  89197436968","us
0140 65 72 6e 61 6d 65 22 3a 22 72 6f 62 31 6e 73 30  ername":"rob1ns0
0150 6e 2e 22 2c 22 61 76 61 74 61 72 22 3a 22 62 64  n.","avatar":"bd
0160 30 39 37 31 39 64 30 66 65 38 30 61 65 65 31 39  09719d0fe80aee19
0170 63 63 36 62 30 35 34 61 32 38 63 37 65 35 22 2c  cc6b054a28c7e5",
0180 22 64 69 73 63 72 69 6d 69 6e 61 74 6f 72 22 3a  "discriminator":
0190 22 30 22 2c 22 66 6c 61 67 73 22 3a 30 2c 22 62  "0","flags":0,"b
01a0 61 6e 6e 65 72 22 3a 6e 75 6c 6c 2c 22 61 63 63  anner":null,"acc
01b0 65 6e 74 5f 63 6f 6c 6f 72 22 3a 6e 75 6c 6c 2c  ent color":null,
01c0 22 70 75 62 6c 69 63 46 6c 61 67 73 22 3a 30 2c  "publicFlags":0,
01d0 22 61 76 61 74 61 72 44 65 63 6f 72 61 74 69 6f  "avatarDecoratio
01e0 6e 44 61 74 61 22 3a 6e 75 6c 6c 2c 22 67 6c 6f  nData":null,"glo
01f0 62 61 6c 4e 61 6d 65 22 3a 22 30 78 52 30 62 31  balName":"0xR0b1
0200 6e 35 30 4e 22 7d 2c 22 61 74 74 61 63 68 6d 65  n50N"},"attachme
0210 6e 74 73 22 3a 5b 5d 2c 22 65 6d 62 65 64 73 22  nts":[],"embeds"
0220 3a 5b 5d 2c 22 6d 65 6e 74 69 6f 6e 73 22 3a 5b  :[],"mentions":[
0230 5d 2c 22 6d 65 6e 74 69 6f 6e 5f 72 6f 6c 65 73  ],"mention roles
0240 22 3a 5b 5d 2c 22 70 69 6e 6e 65 64 22 3a 66 61  ":[],"pinned":fa
0250 6c 73 65 2c 22 6d 65 6e 74 69 6f 6e 5f 65 76 65  lse,"mention eve
0260 72 79 6f 6e 65 22 3a 66 61 6c 73 65 2c 22 74 74  ryone":false,"tt
```

Editing row=1, column=7
Type: Binary; Size: 1390 byte(s)

- **Answer**:
  The Mob Museum

Conclusion

The cybersecurity landscape continues to evolve, presenting ongoing challenges to organizations of all sizes. By understanding the current threat environment, addressing identified vulnerabilities, and implementing recommended security measures, we can significantly reduce the risk of cyber incidents and protect valuable assets. Continuous monitoring, proactive threat hunting, and adaptive security strategies are essential for maintaining a strong security posture.