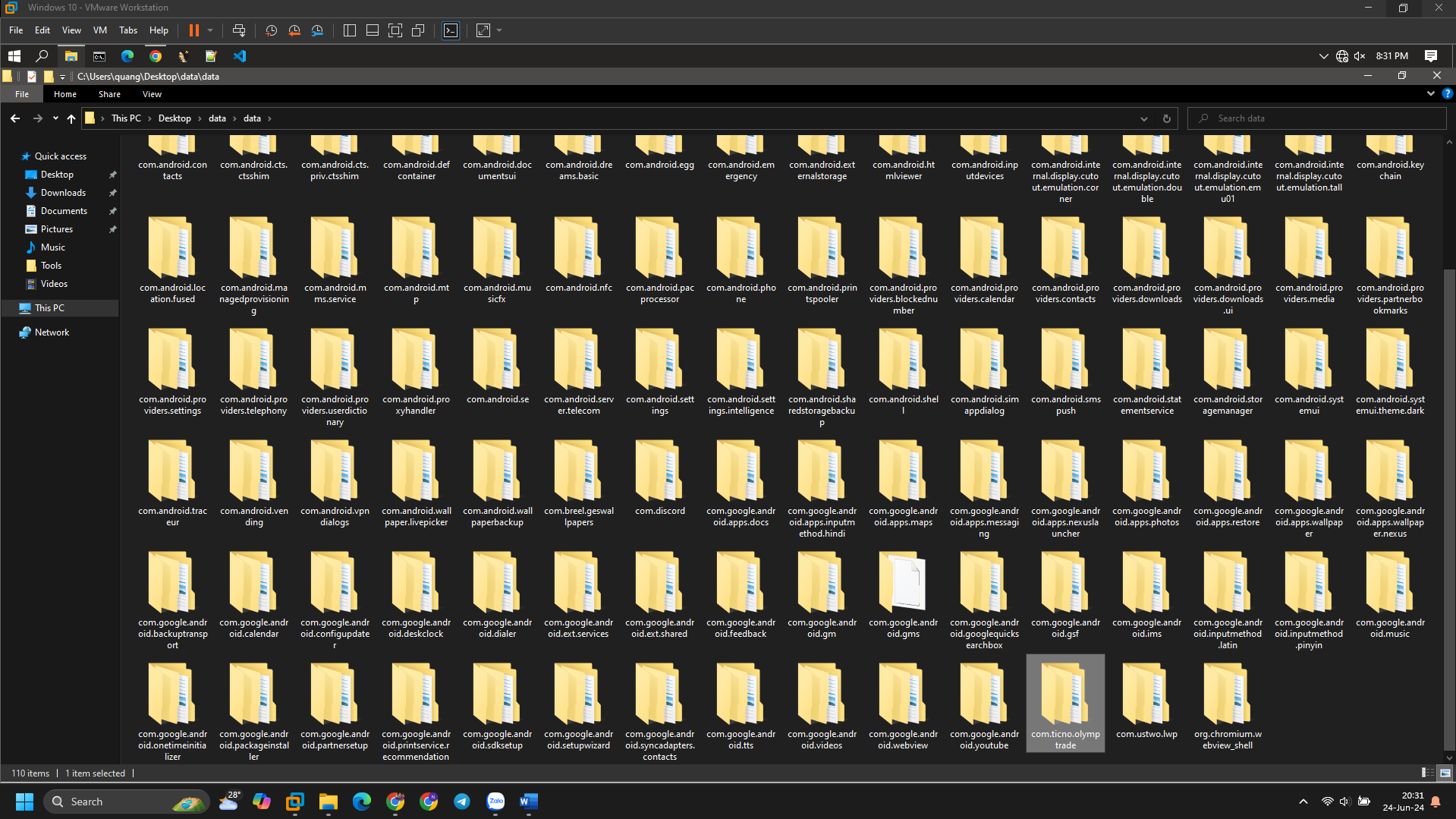
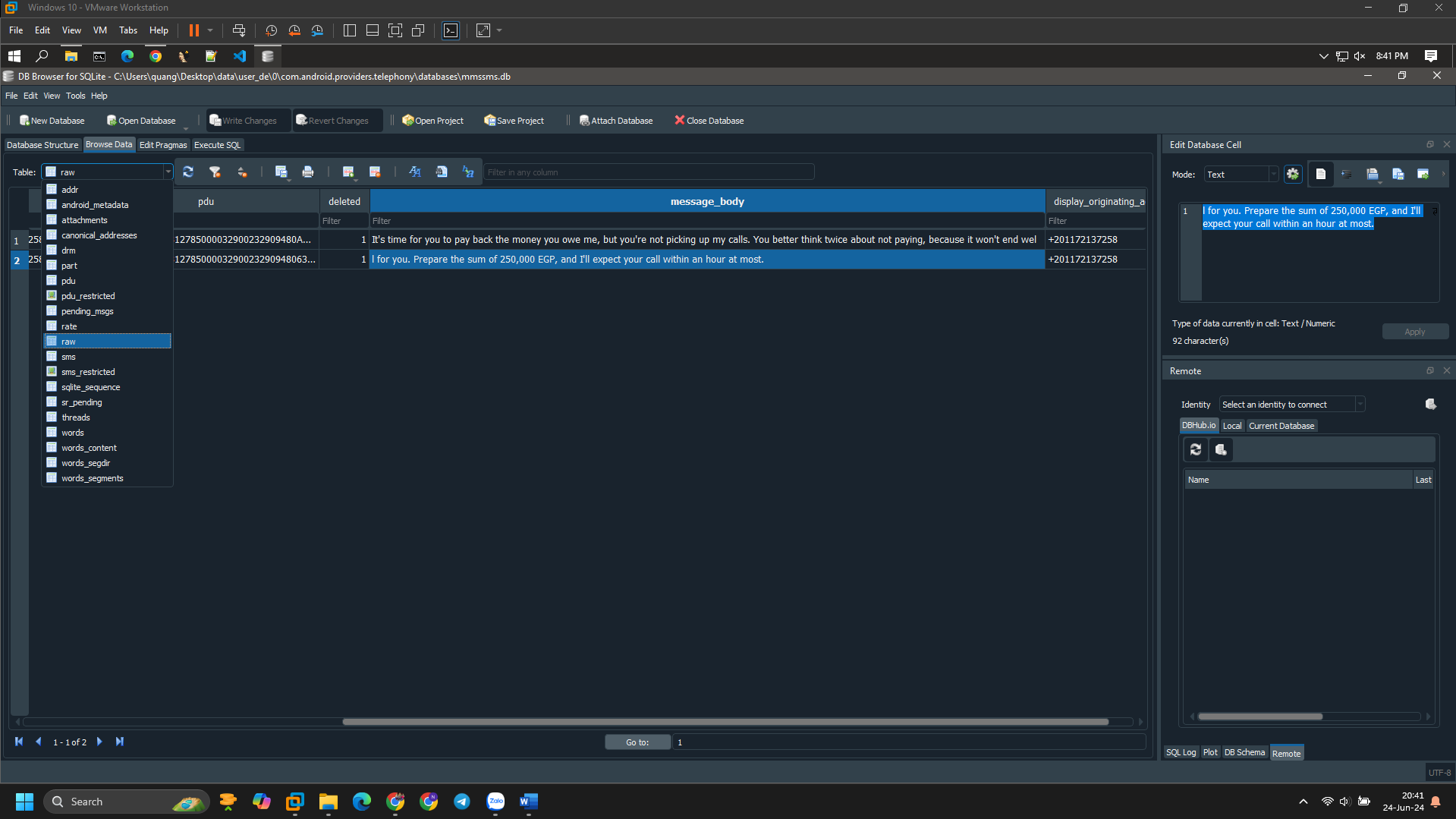
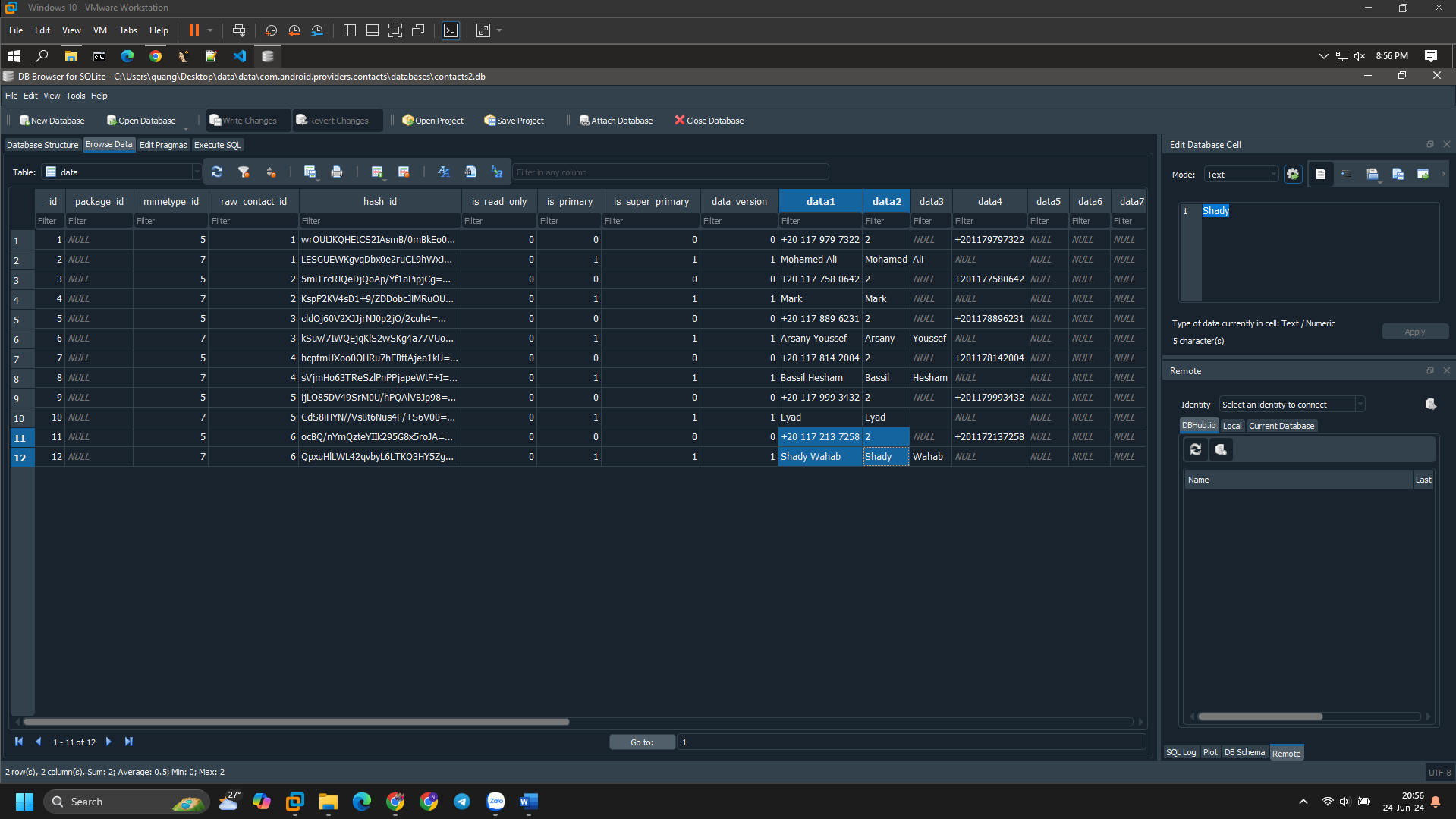
<https://cyberdefenders.org/blueteam-ctf-challenges/the-crime/>

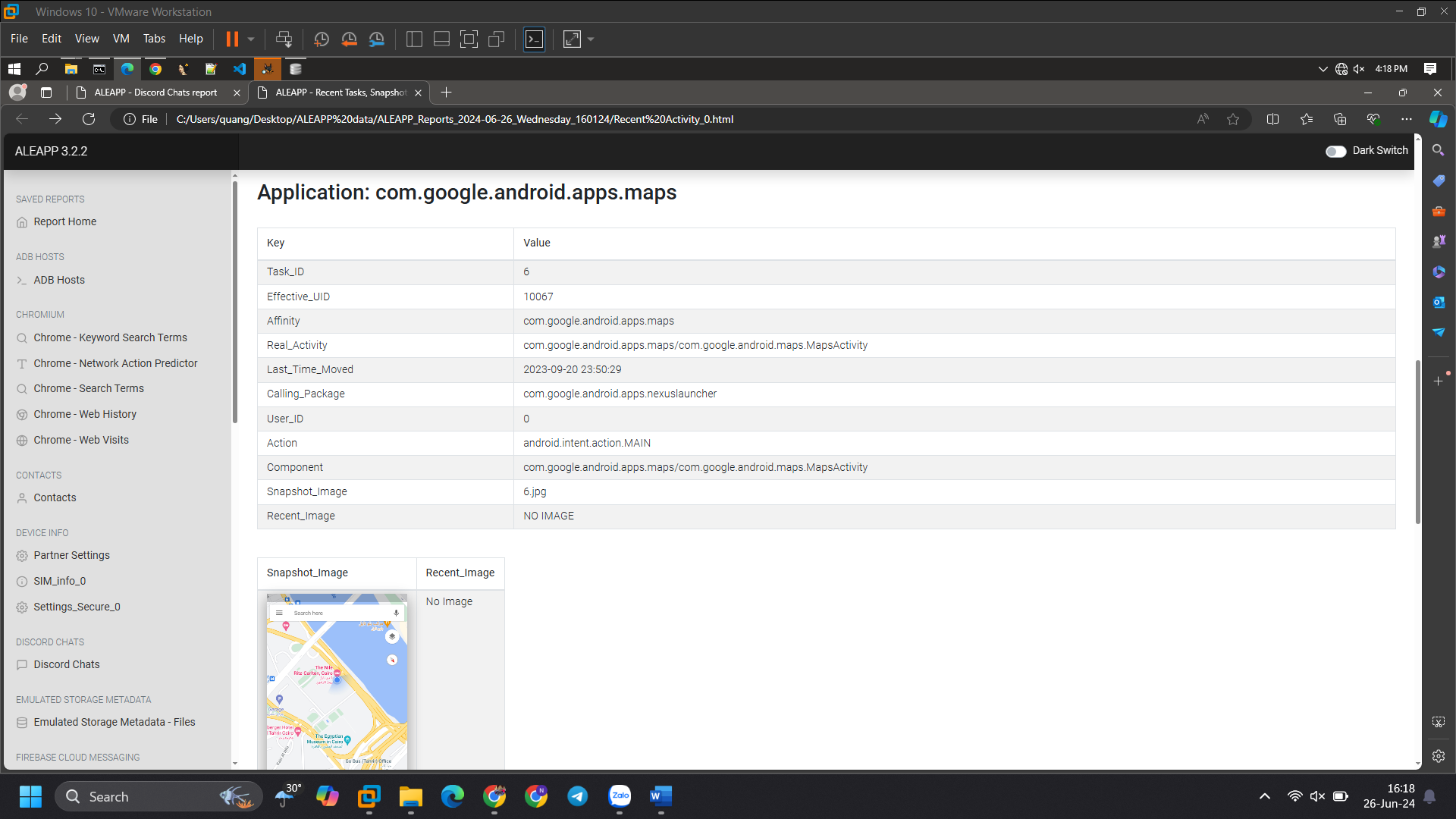
Q1. Dựa trên lời kể của các nhân chứng và những người thân cận với nạn nhân, nạn nhân quan tâm đến đầu tư và giao dịch. Nạn nhân đã đầu tư toàn bộ số tiền của mình và mắc nợ. Olymp Trade chính là ứng dụng Android dùng để đầu tư và giao dịch. Olymp Trade nằm trong mục /data/com.ticno.olymptrade.  


Q2. Theo lời khai của người bạn thân của nạn nhân: “Khi chúng tôi ở cùng nhau, bạn tôi nhận được nhiều cuộc gọi mà anh ấy đều không trả lời. Anh ấy nói mình nợ người gọi rất nhiều tiền nhưng hiện tại không có khả năng trả”. Nạn nhân nợ người này 250.000 Bảng Ai Cập. Cơ sở dữ liệu lưu trữ các tin nhắn trên Android là /data/user\_de/0/com.android.providers.telephony/databases/mmssms.db bảng Raw.

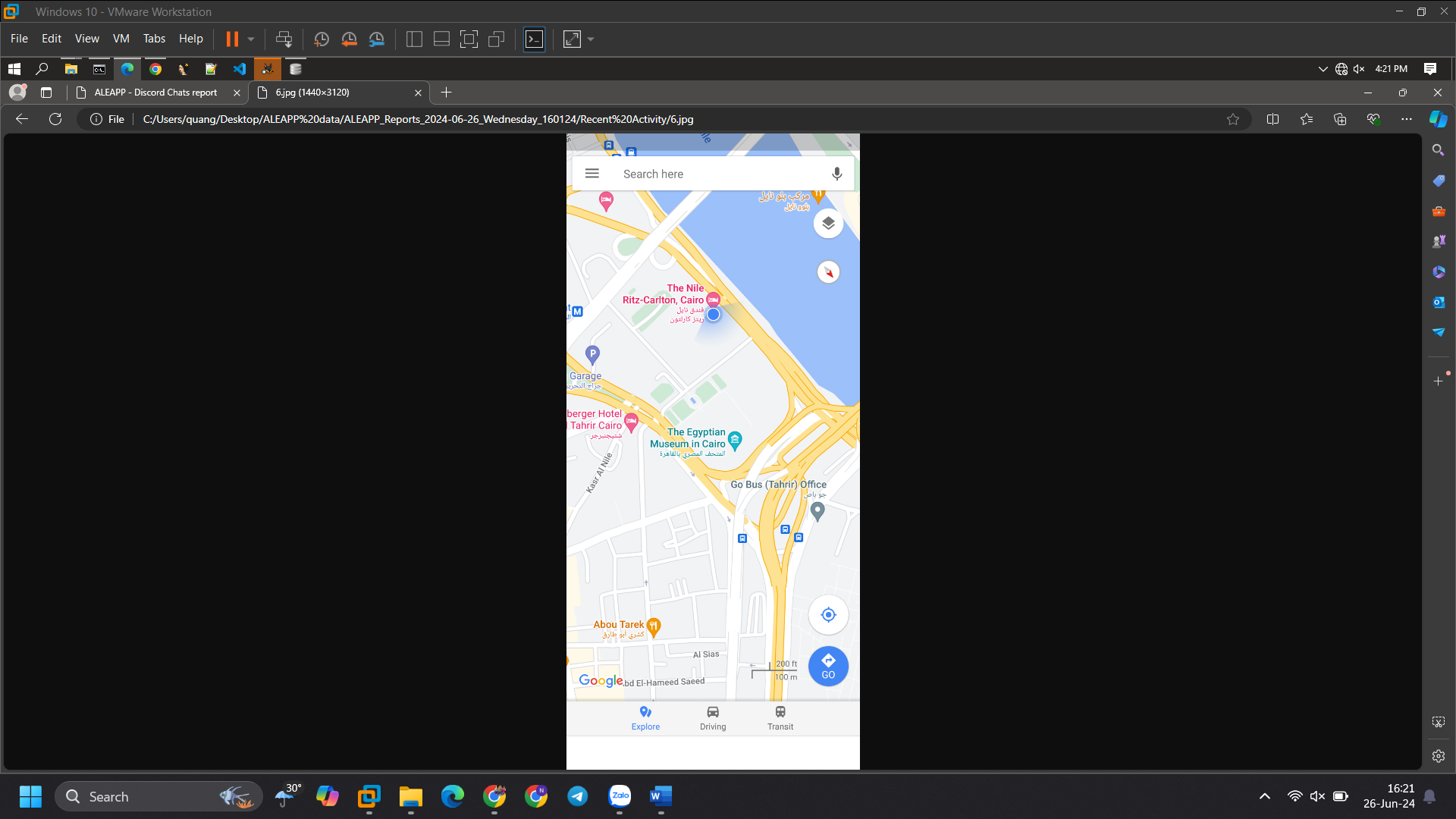


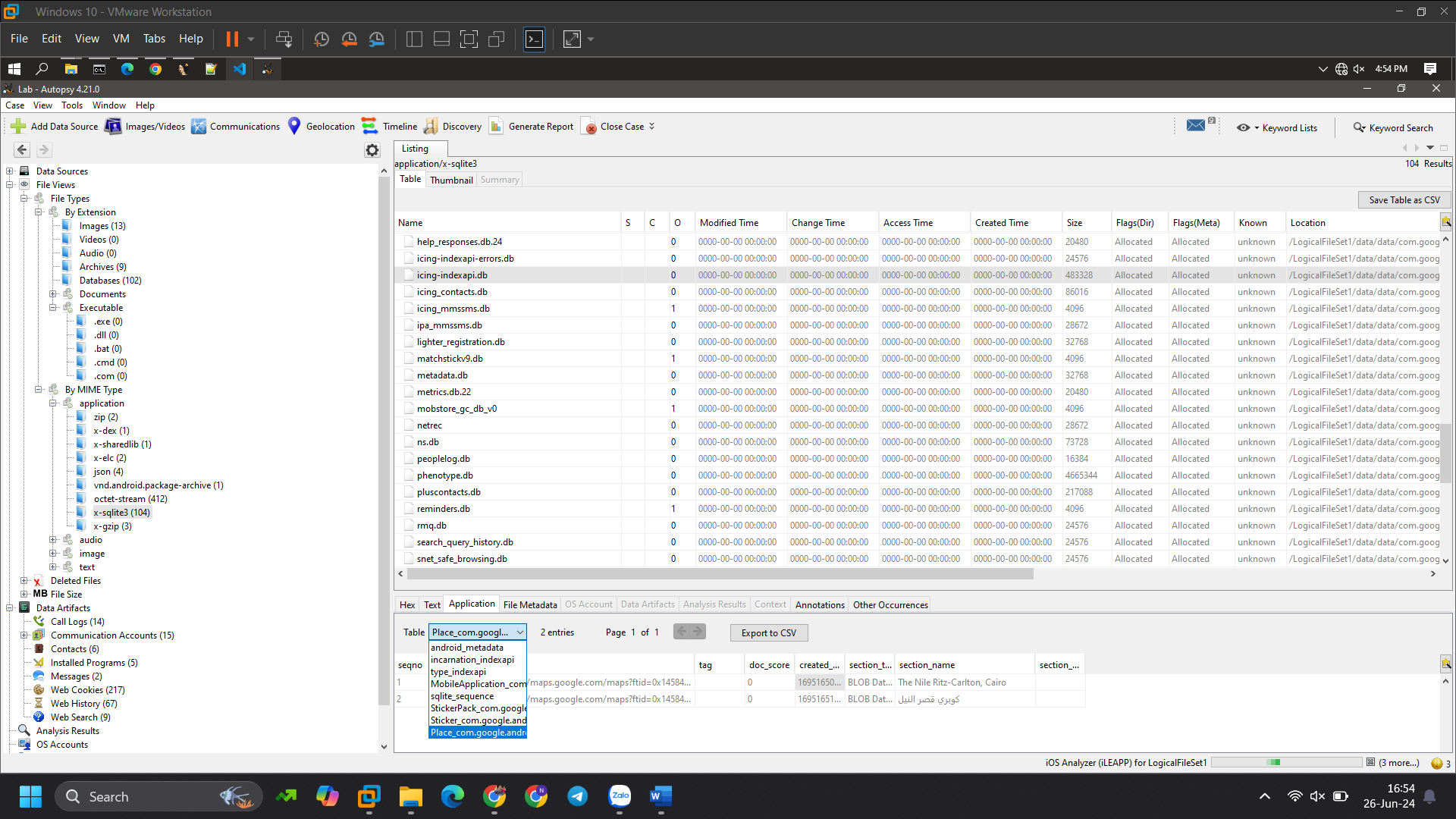
Q3. Người nợ tiền của nạn nhân tên là Shady Wahab. Theo cơ sở dữ liệu mmssms.db, +201172137258 là đầu số điện thoại của nạn nhân bị nợ tiền, với đầu số +20 là của Ai Cập. Sử dụng DB Browser for SQLite, chúng ta chuyển sang cơ sở dữ liệu danh bạ của Android là /data/com.android.providers.contacts/databases/contacts2.db bảng data. Tại đây, số điện thoại +201172137258 tương ứng với tên danh bạ Shady Wahab.  


Q4. Căn cứ qua lời khai của gia đình nạn nhân, họ cho biết, ngày 20/9/2023, nạn nhân rời khỏi nơi ở mà không thông báo cho ai về đích đến. Theo như tìm hiểu trên điện thoại, lúc đó nạn nhân ở The Nile Ritz-Carlton. Với câu này, ta sẽ sử dụng AleappGUI để tìm kiếm địa chỉ của điện thoại. Kiểm tra file Recent Activity\_0.html do AleappGUI xuất ra, ta thấy có 3 ảnh chụp màn hình.

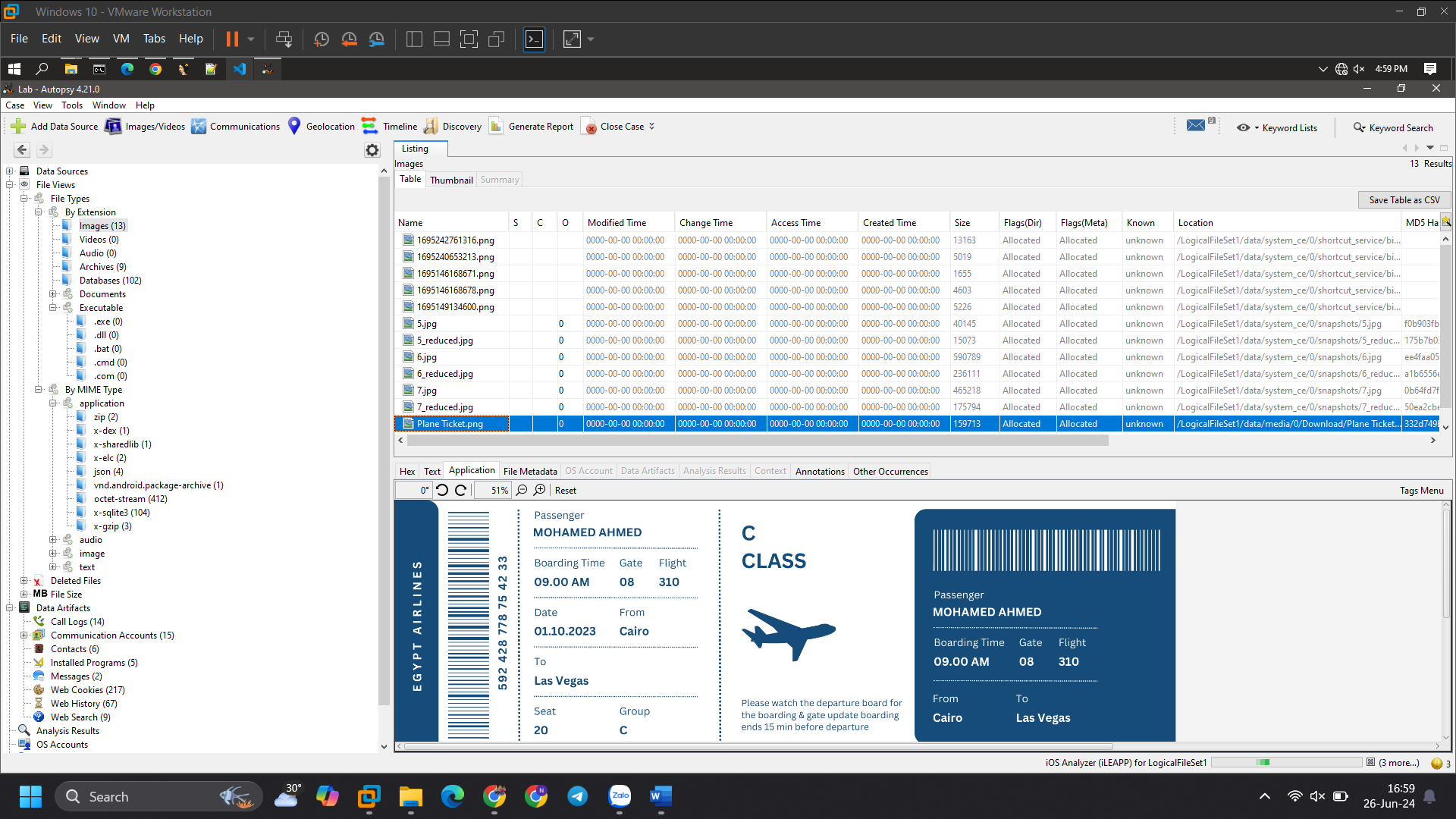


Có 1 ảnh chụp màn hình liên quan tới bản đồ. Tại đây, Aleapp đã đưa ra ảnh chụp màn hình do nạn nhân đã chụp, đó là địa chỉ của nạn nhân được hiện tại địa điểm The Nile Ritz-Carlton.



Hoặc sử dụng Autopsy mục x-sqlite3, trong này ta nhắm tới cơ sở dữ liệu icing-indexapi.db. Tại bảng Place\_com.google.android…, có lưu chính xác 2 địa chỉ mà nạn nhân đã tới, địa chỉ đầu tiên là The Nile Ritz-Carlton.  


Q5. Thám tử tiếp tục cuộc điều tra bằng cách thẩm vấn tiền sảnh khách sạn. Họ cho anh biết nạn nhân đã đặt phòng 10 ngày và có lịch bay sau đó. Điều tra viên cho rằng có thể nạn nhân đã lưu thông tin vé vào điện thoại. Nạn nhân đã đi Las Vegas. Trên Autopsy, tìm tới mục Image, file Plane Ticket.png. Nạn nhân đã đi từ Cairo, Ai Cập tới Las Vegas lúc 09:00 sáng.



Q6. Sau khi kiểm tra các cuộc trò chuyện trên Discord của nạn nhân, chúng tôi phát hiện ra nạn nhân đã hẹn gặp một người bạn tại một địa điểm cụ thể. Nơi hai người đó gặp nhau là The Mob Museum.

Kiểm tra file Discord Chats.html do AleappGUI xuất ra, ta thấy đoạn chat của 2 người. Theo như phân tích của Aleapp, Username rob1ns0n đã hẹn infern0\_o ở The Mob Museum.  
