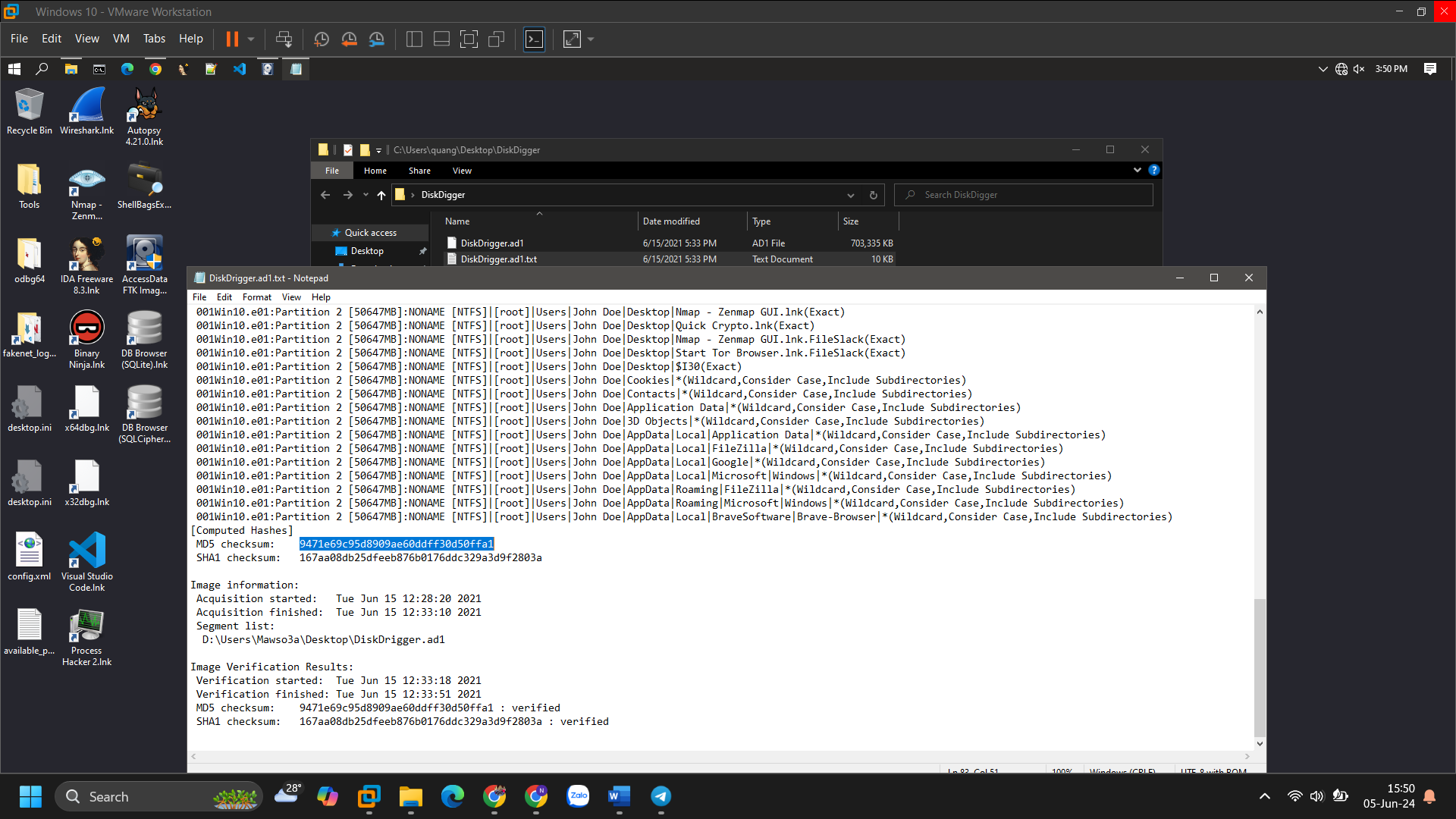
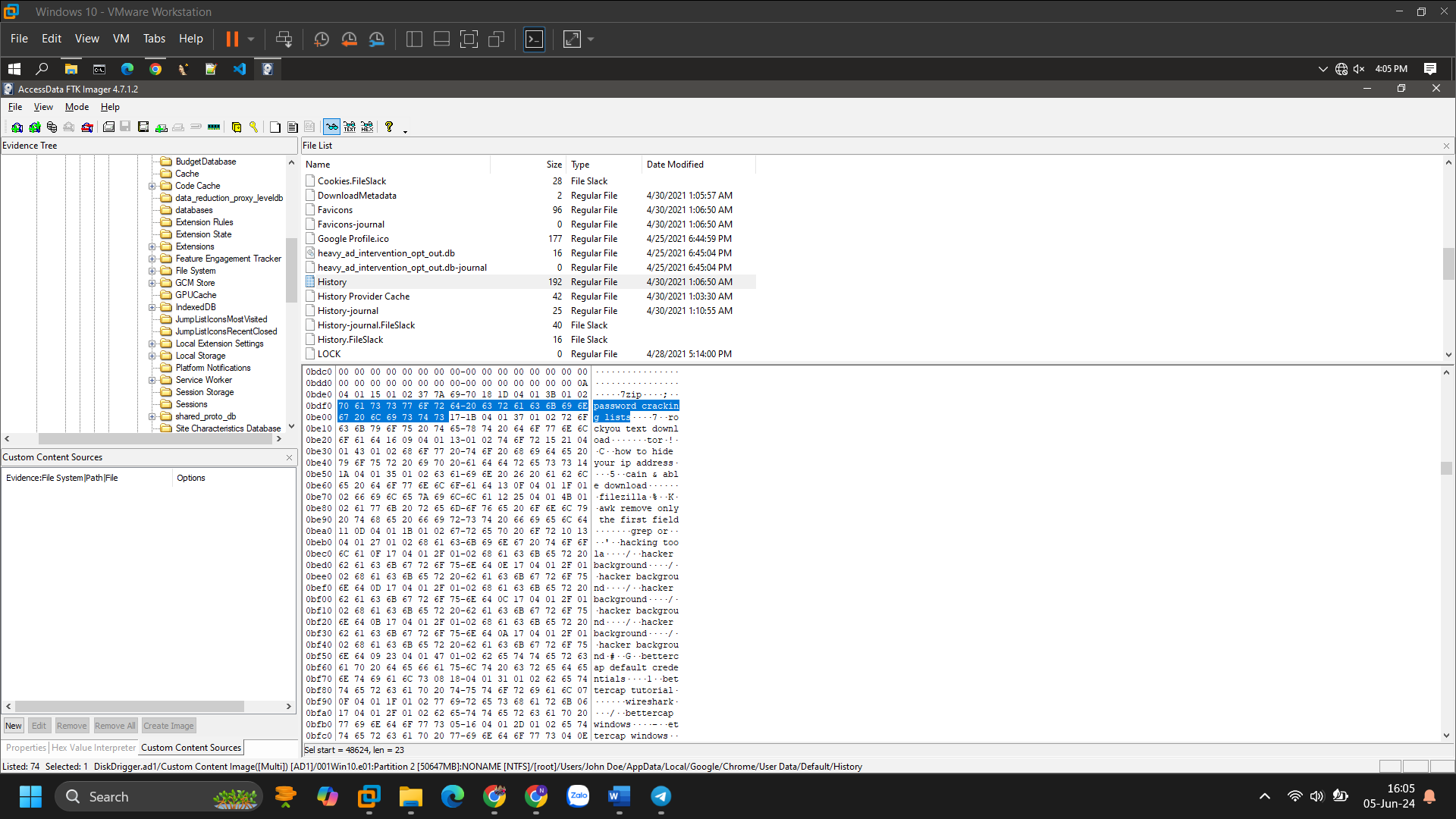
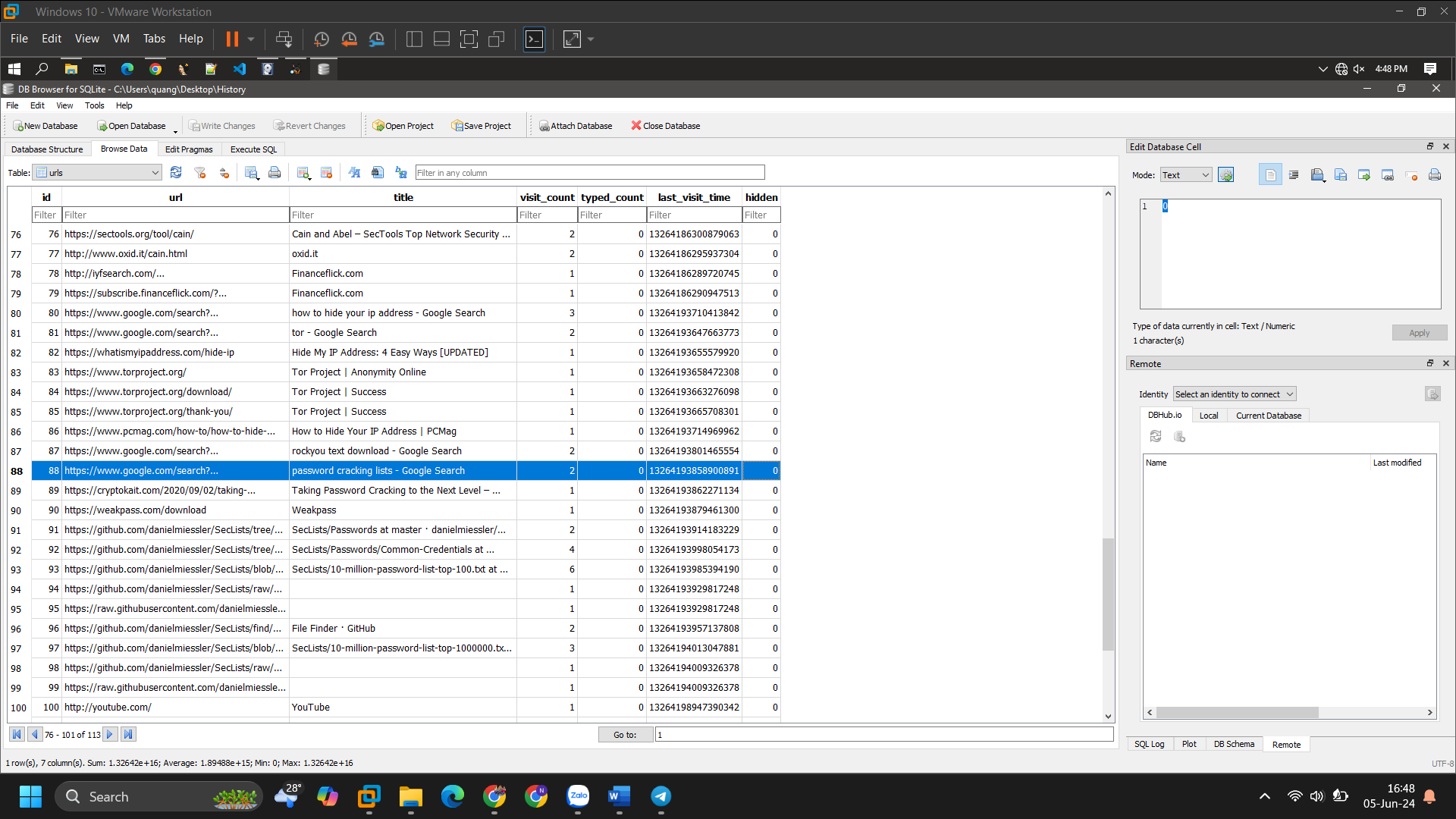
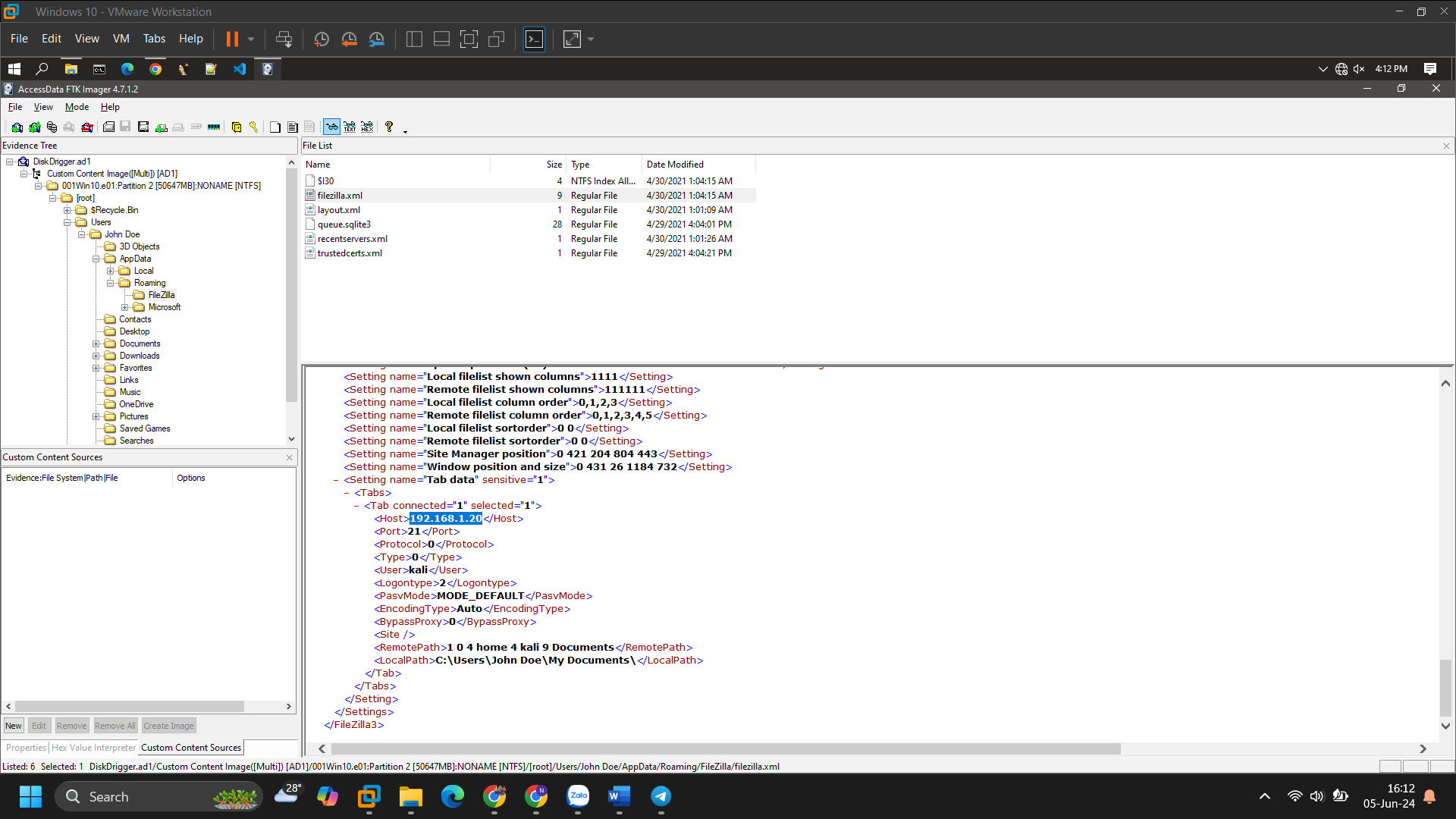
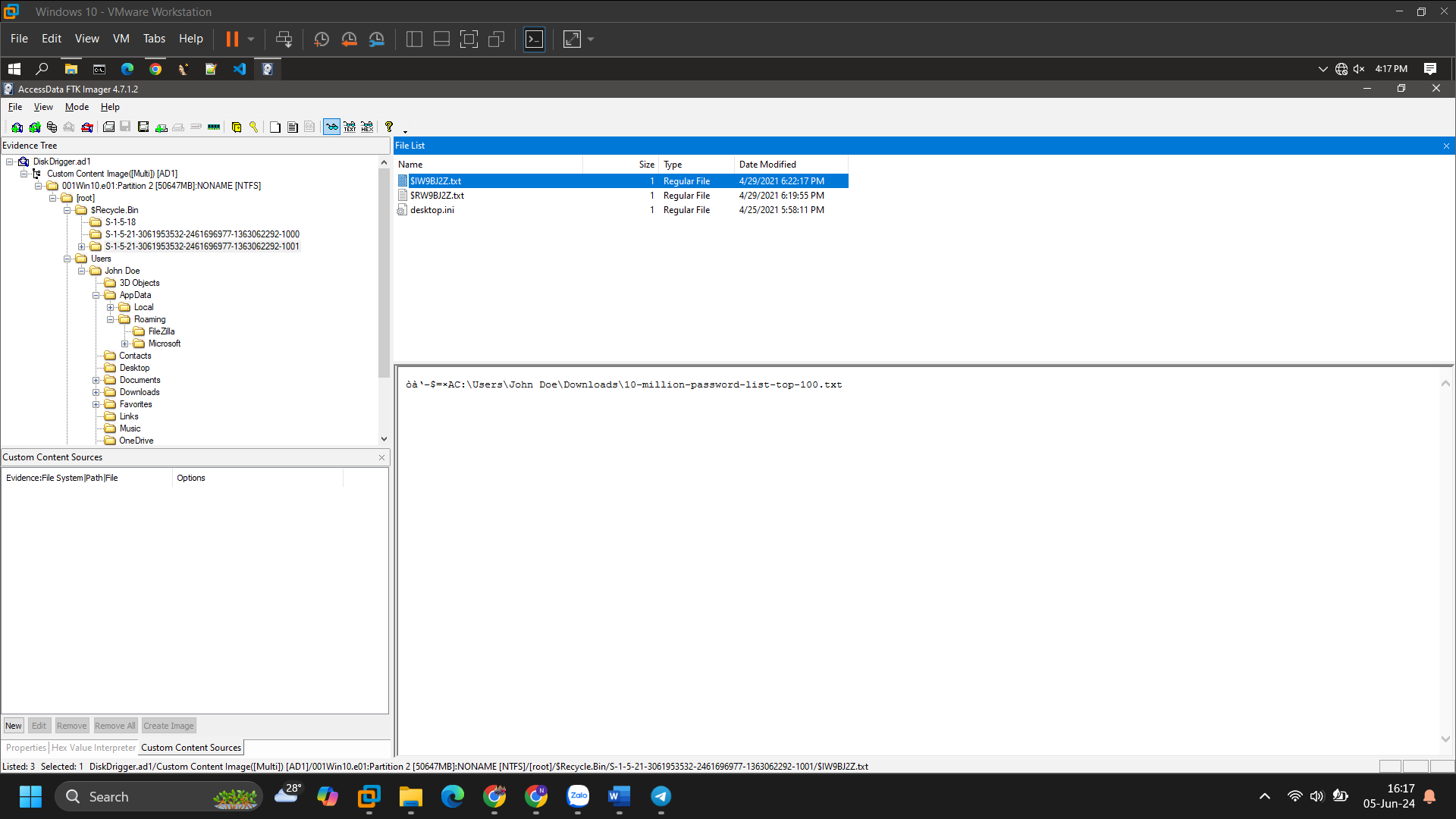
https://cyberdefenders.org/blueteam-ctf-challenges/africanfalls/

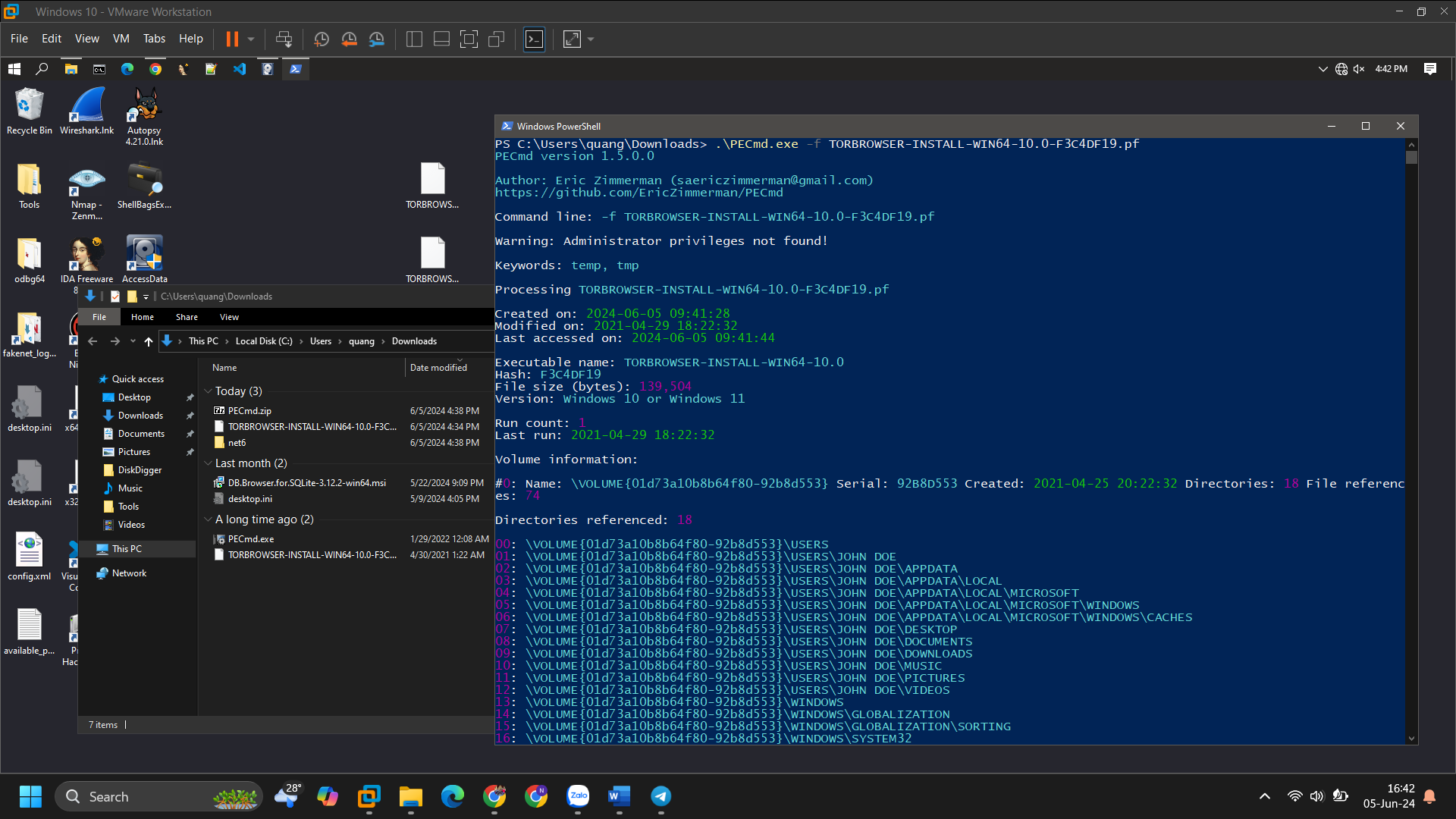
Q1. Giá trị băm MD5 của đĩa là 9471e69c95d8909ae60ddff30d50ffa1, nằm trong file DiskDrigger.ad1.txt.  


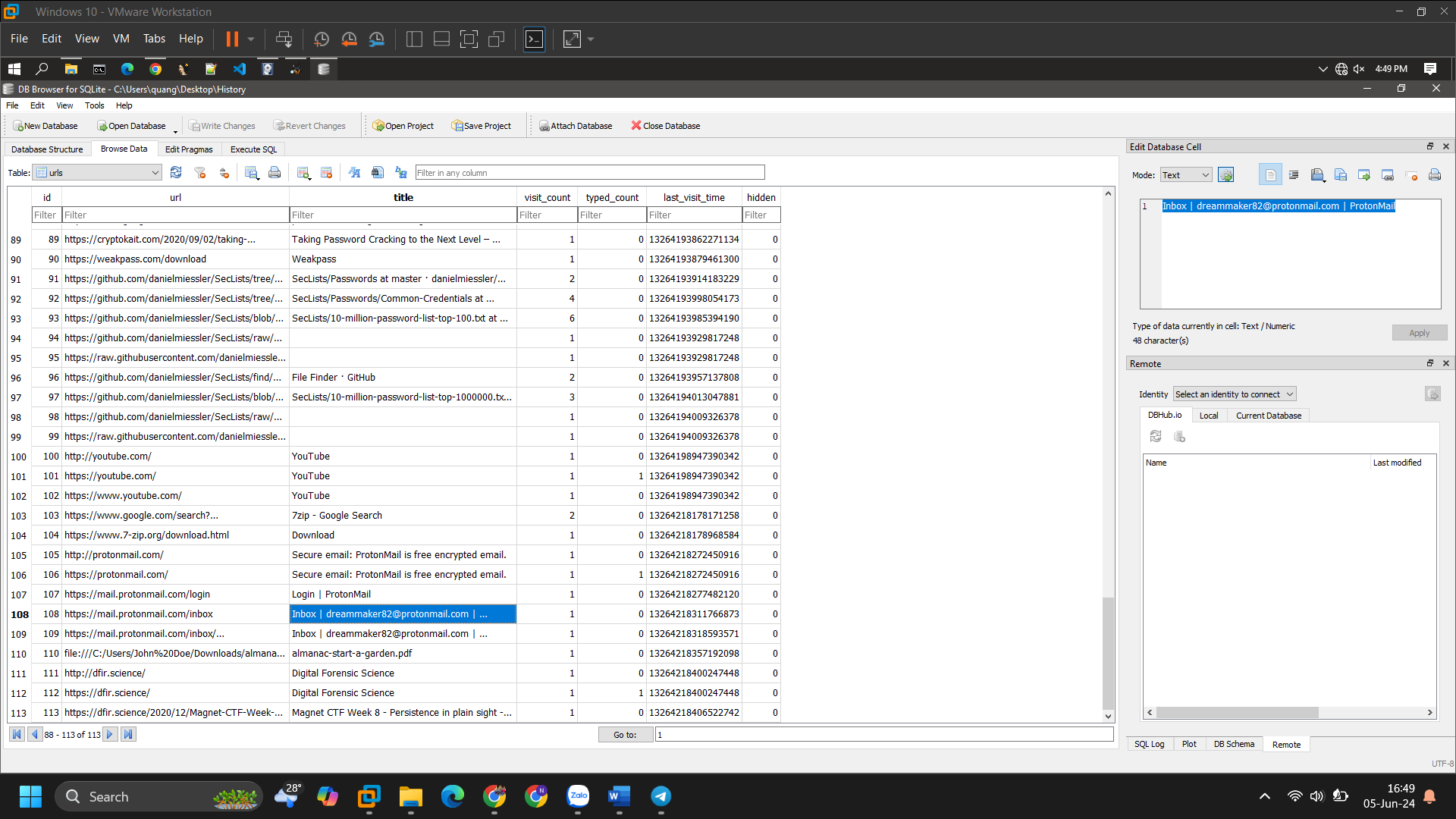
Q2. Mục C:\Users\John Doe\AppData\Local\Google\Chrome\User Data\Default\History lưu trữ dữ liệu về hành vi sử dụng Google Chrome của máy tính.

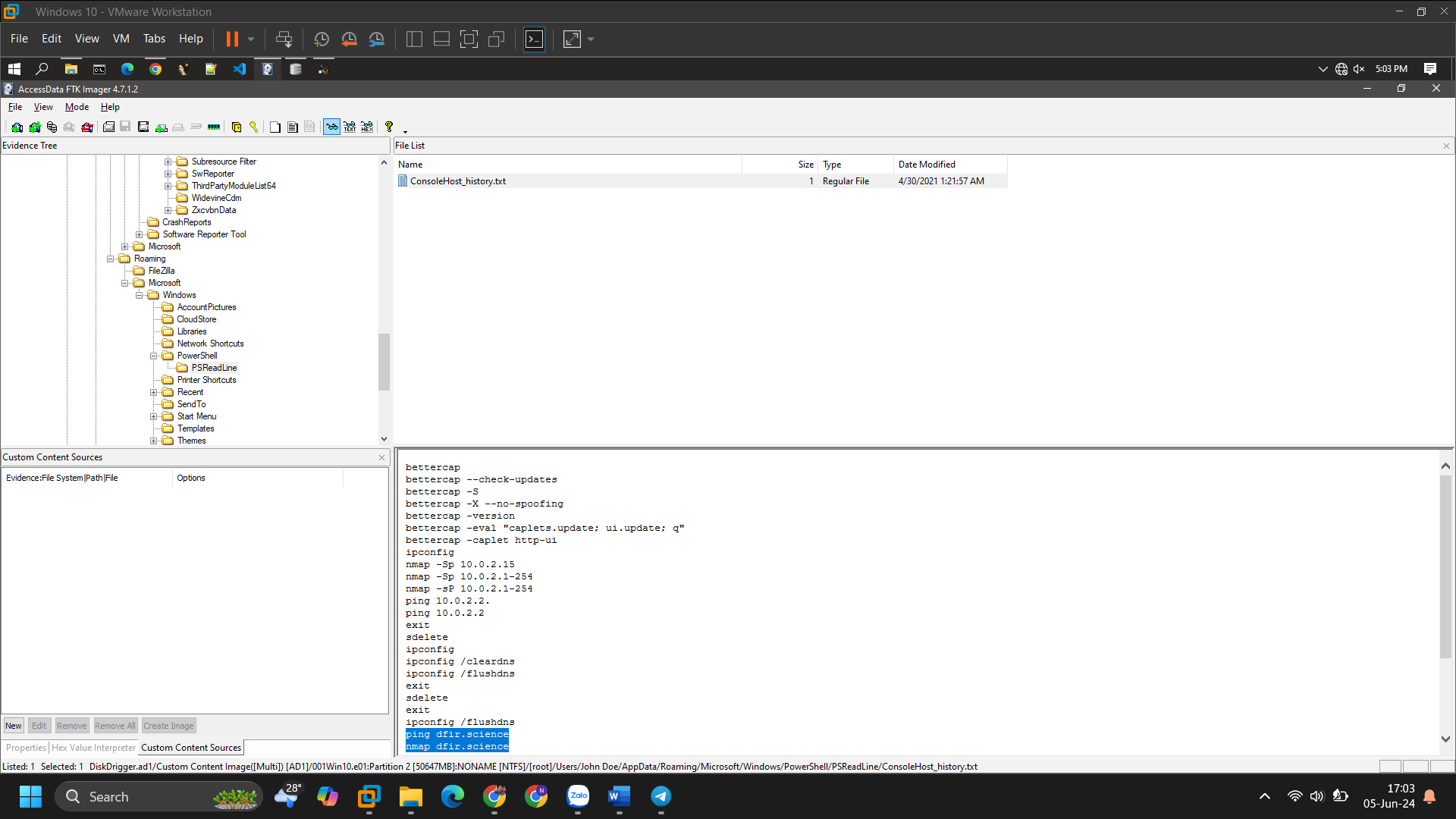
Đưa file History vào SQLite bảng urls. Bảng urls sẽ lưu lại các thông tin website trên Google Chrome. Đối với trường hợp này, kẻ tấn công đã tìm kiếm cụm từ password cracking lists. Với website epochconverter.com/webkit, kiểm tra 13264193858900891 ra đúng thời gian 2021-04-29 18:17:38.  


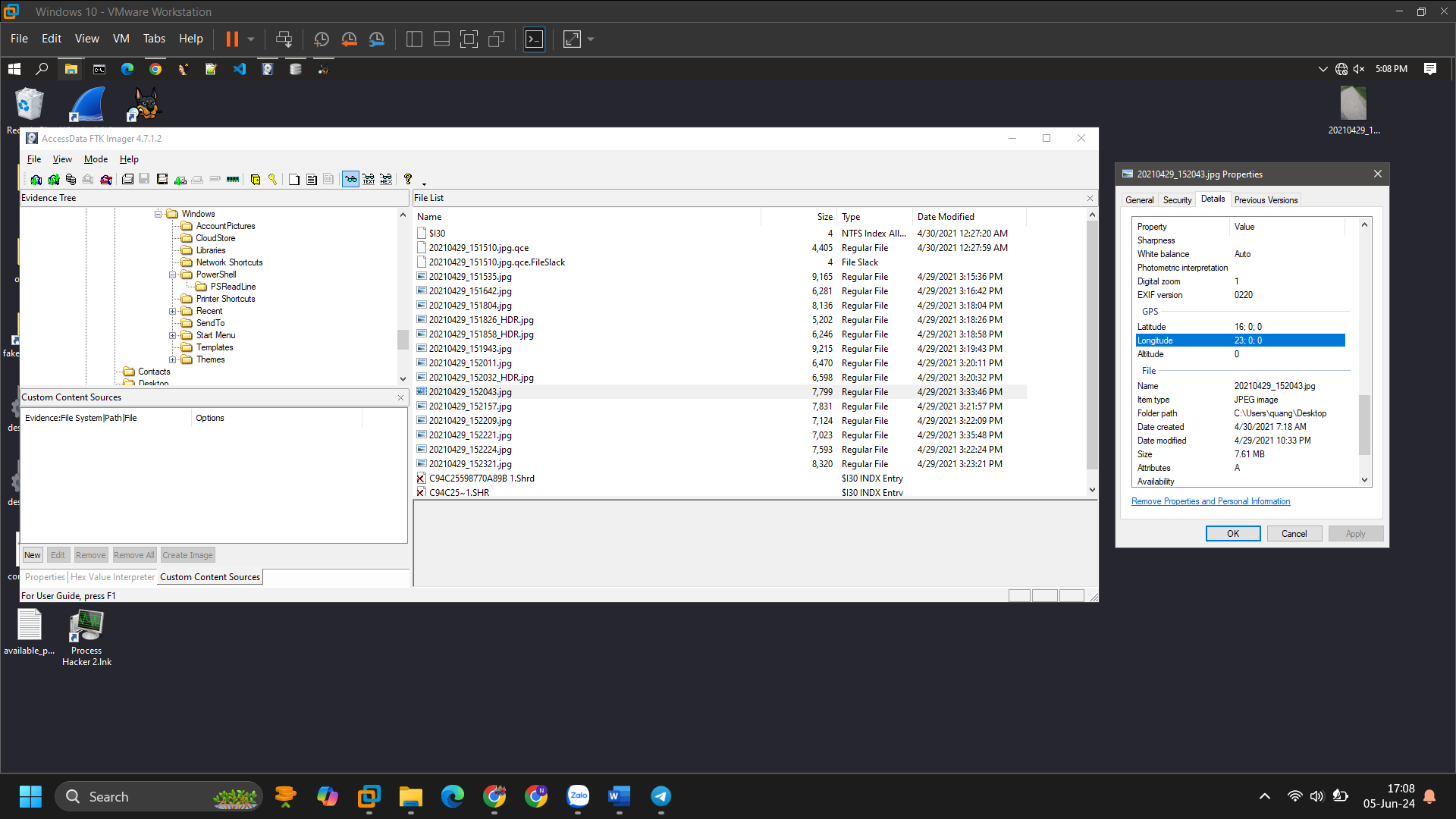
Q3. Kiểm tra các phần mềm đã cài đặt. Mục C:\Users\John Doe\AppData\Roaming\FileZilla\filezilla.xml lưu lại thông tin của máy chủ. Địa chỉ IPv4 của máy chủ FTP mà kẻ tấn công nhắm tới là 192.168.1.20 thông qua cổng 21.  


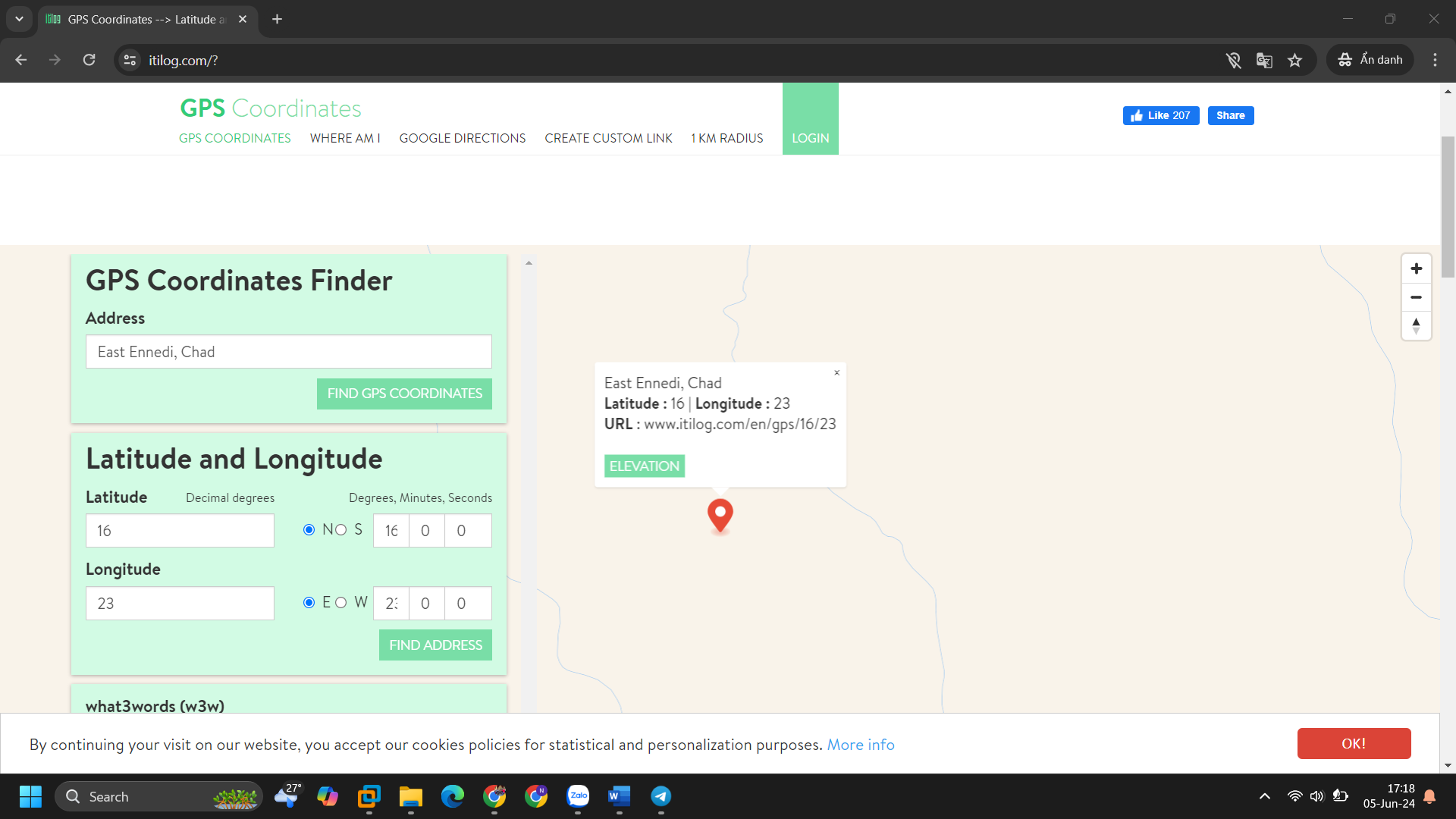
Q4. Để biết list mật khẩu bị xóa vào thời gian nào, cần kiểm tra mục C:\$Recycle.Bin\S-1-5-21-3061953432-2461696977-1363062292-1001\. List mật khẩu mà kẻ tấn công đã sử dụng bị xóa vào ngày 2021-04-29 18:22:17.  


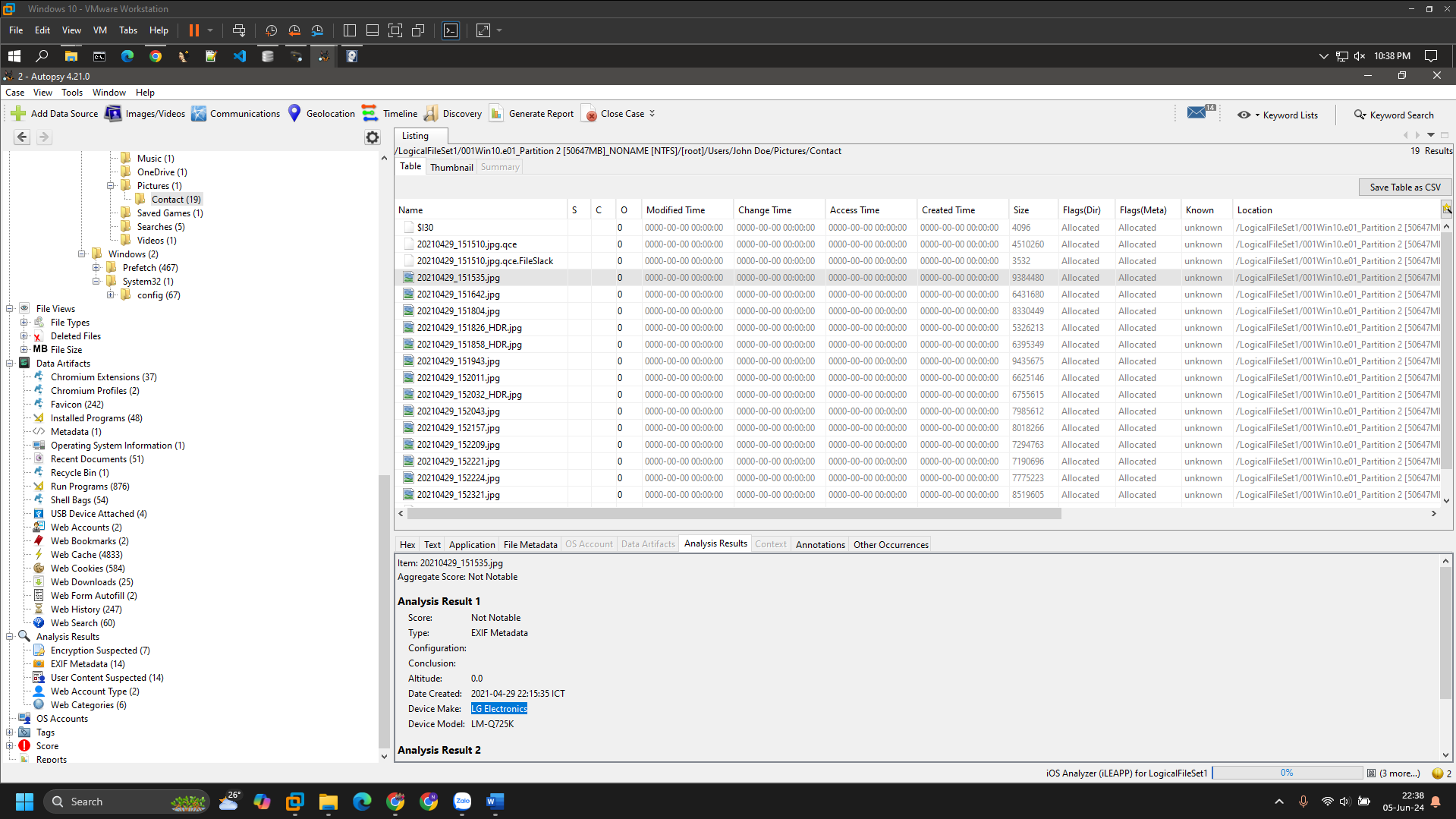
Q5. Các tệp tìm nạp được liên kết với phần mềm từ ổ đĩa sẽ lưu trữ trong Prefetch để khởi động nhanh hơn. TORBROWSER-INSTALL-WIN64-10.0-F3C4DF19.pf & TORBROWSER-INSTALL-WIN64-10.0-F3C4DF19.pf.FileSlack là 2 tệp được hướng tới.   
Sử dụng PECmd để đọc 2 tệp này. Tor Browser được chạy 0 lần trên máy tính. Bởi vì người dùng không khởi chạy TOR Installer nên không có tệp tìm nạp để chạy TOE Browser.  


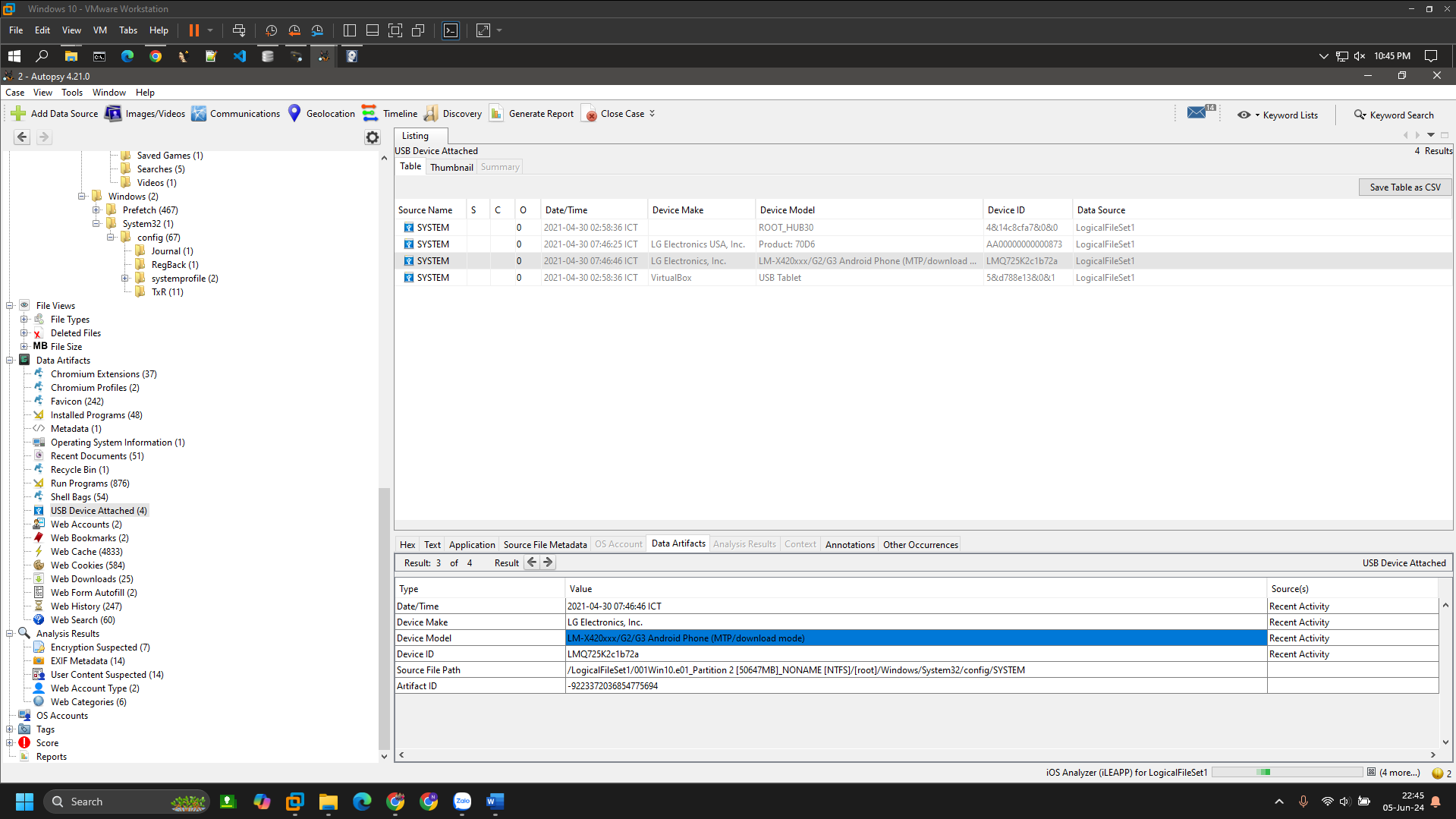
Q6. Trong SQLite ở bảng urls, địa chỉ email của kẻ tấn công là dreammaker82@protonmail.com.  


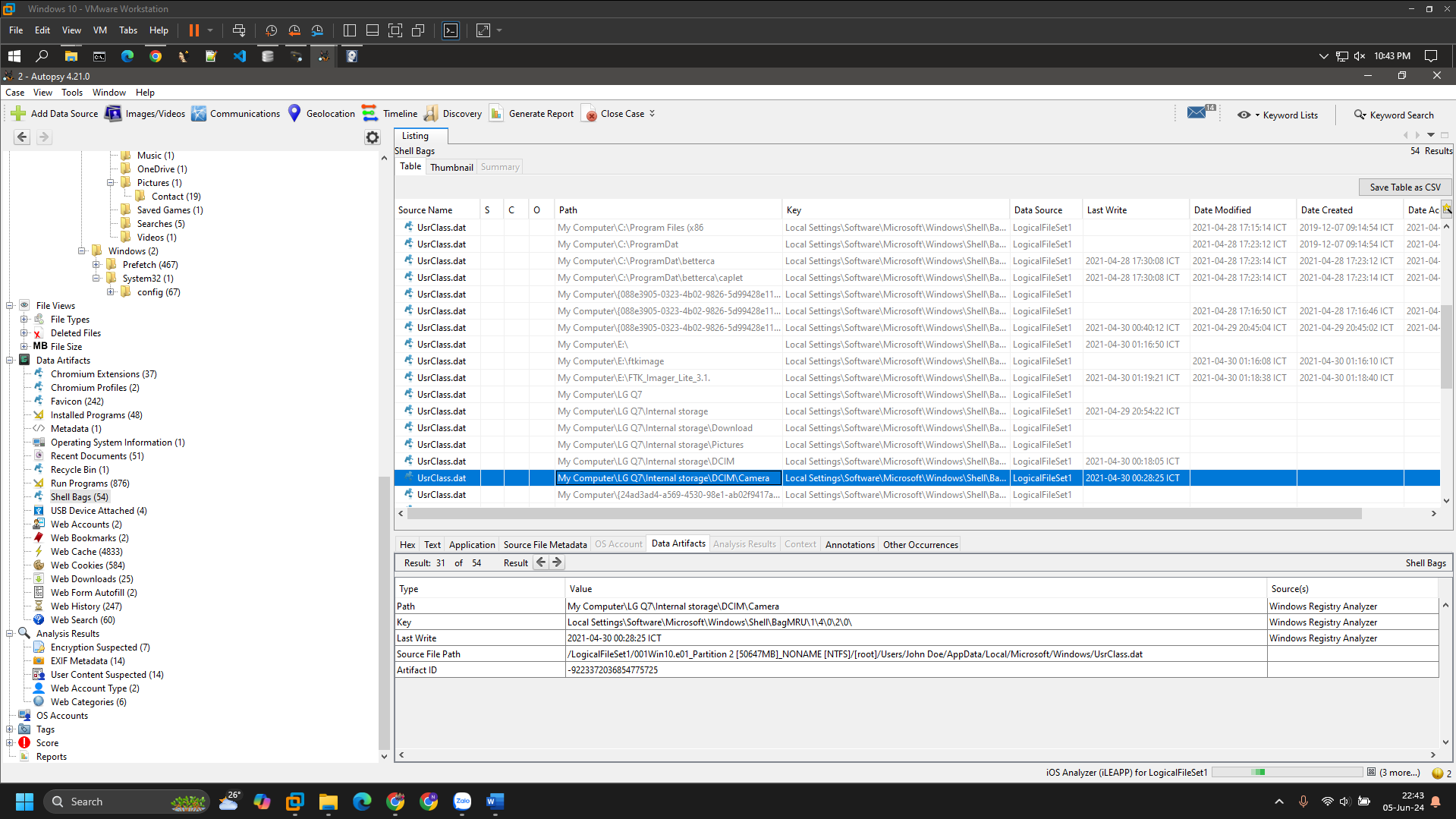
Q7. Để quét được cổng chúng ta có thể hướng tới nmap. Nmap là chương trình quét cổng chạy trên môi trường dòng lệnh nên ta hướng tới mục mục C:\Users\John Doe\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost\_history.txt\, là mục lưu trữ lịch sử sử dụng dòng lệnh trên PowerShell. Mục tiêu của kẻ tấn công là dfir.science.   


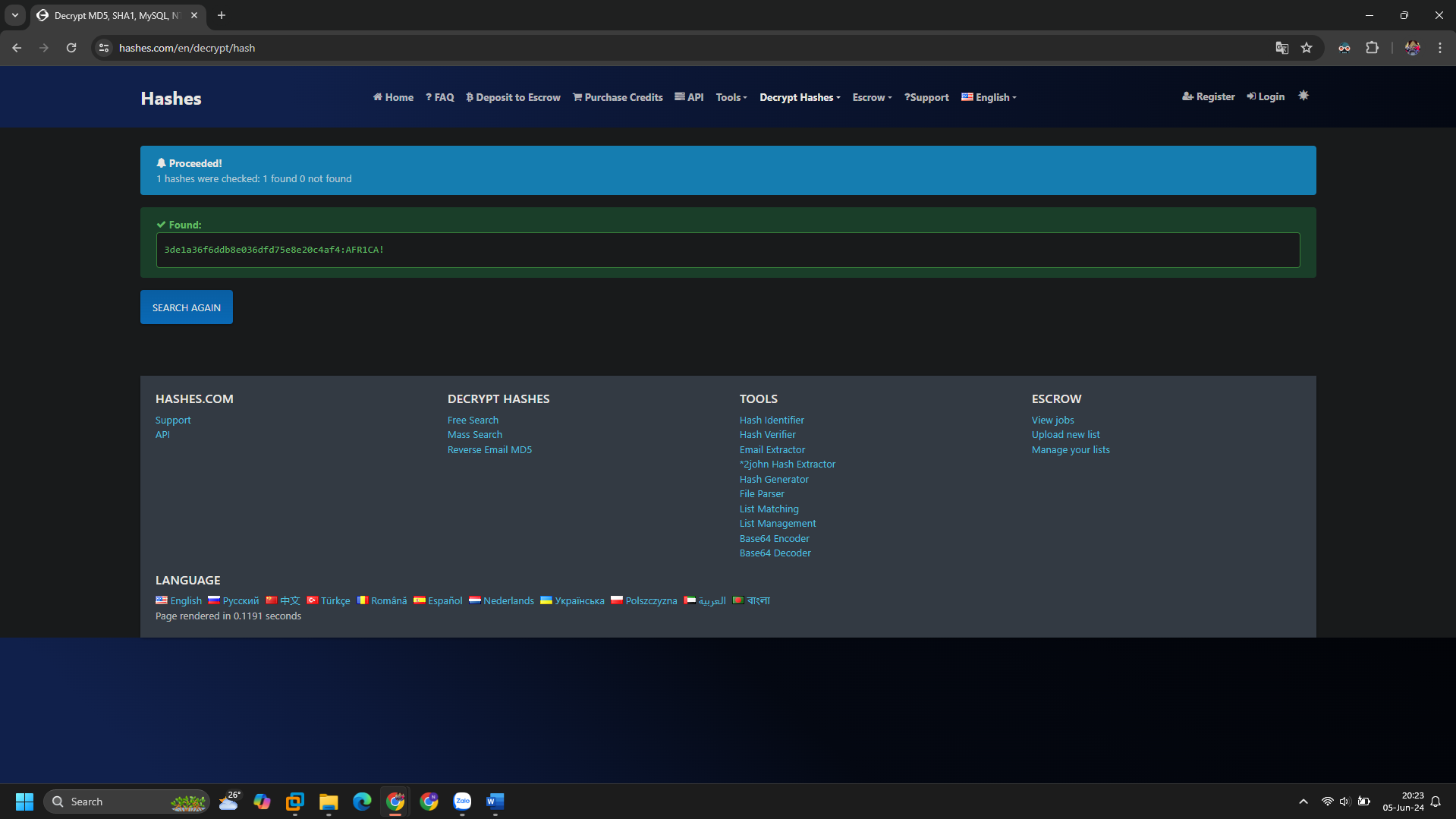
Q8. Xác định file hình ảnh nằm ở mục C:\Users\John Doe\Pictures\Contact\. Kiểm tra Latitude 16;0;0 và Longitude 23;0;0 của bức ảnh 20210429\_152043.jpg.   


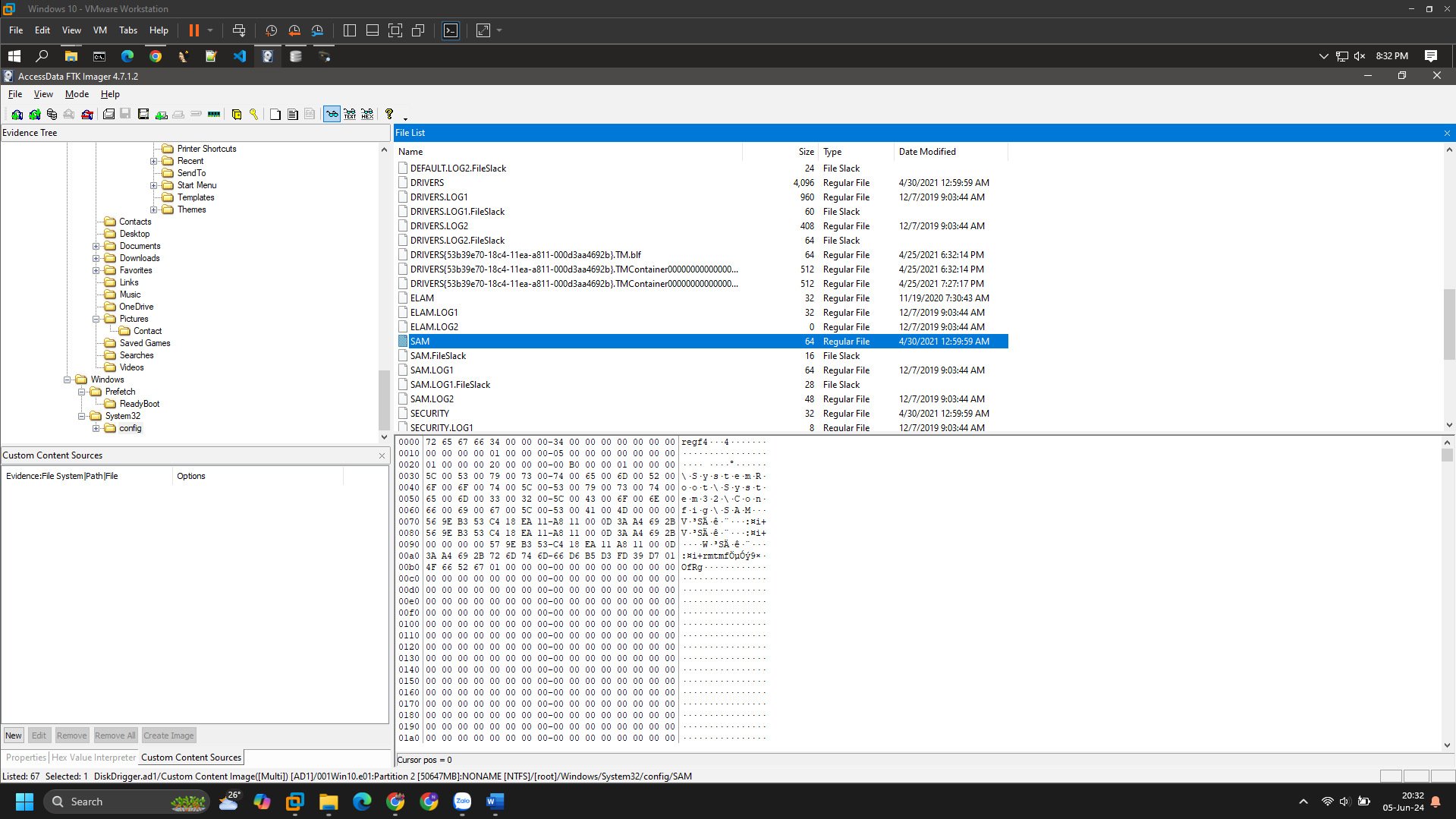
Website itilog.com sẽ cung cấp địa chỉ bức ảnh đó. Bức ảnh "20210429\_152043.jpg" được cho là được chụp ở Chad (Zambia).  


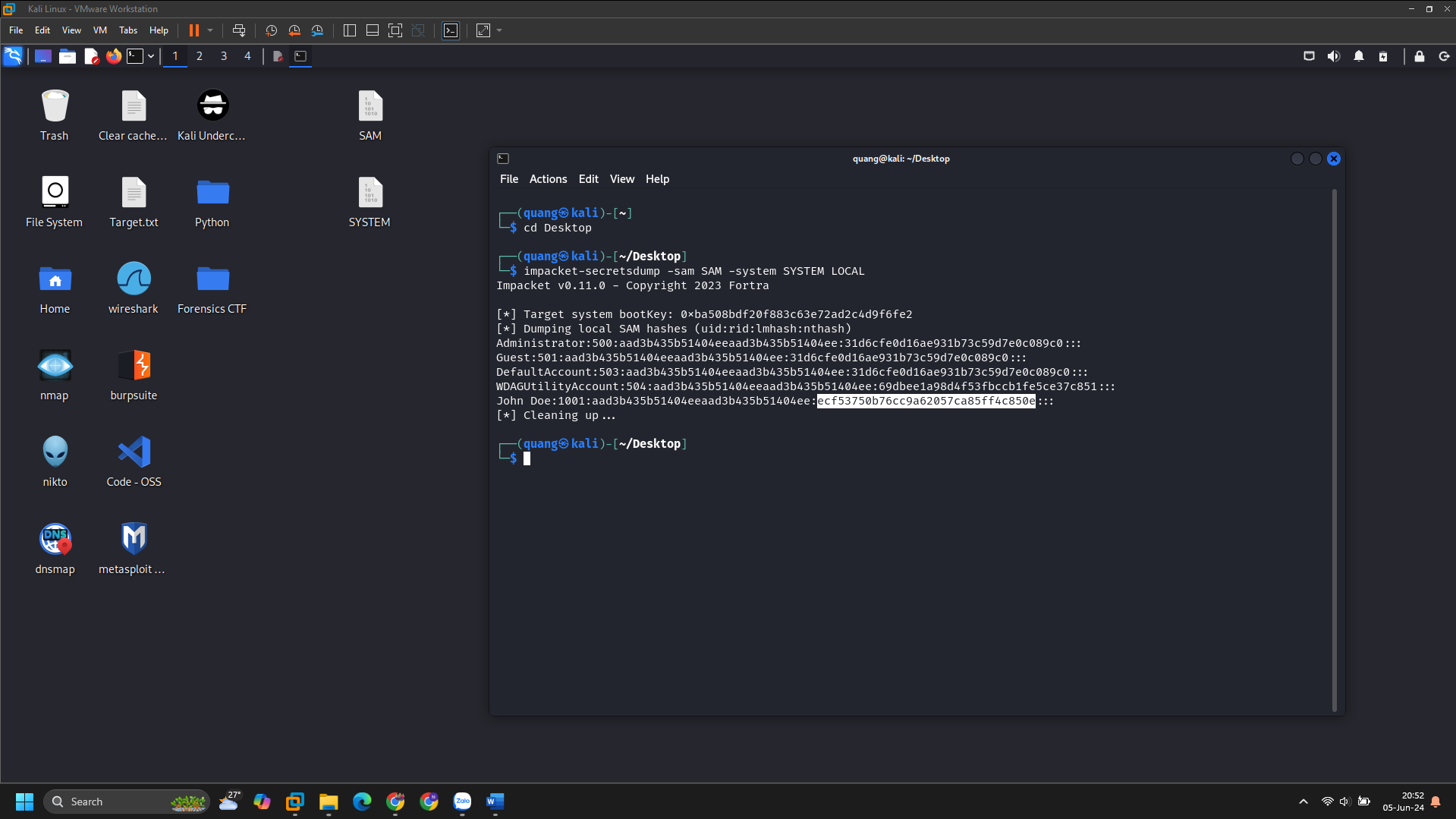
Q9. Hình ảnh "20210429\_151535.jpg" hiện nằm ở thư mục Pictures\contact.  
****

Kiểm tra các thiết bị đã cắm qua USB thông qua Autopsy USB Device Attached, có điện thoại LG được kết nối với máy tính trong trạng thái Download mode, nghĩa là các file từ điện thoại LG sẽ tải về máy tính.  


Shell Bags sẽ ghi lại các logs hoạt động của điện thoại LG đó. LG Q7\Internal storage\DCIM\Camera là nơi hình ảnh "20210429\_151535.jpg" được tải về tới thư mục Pictures\contact. ****

Q10. Anon:1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E2 là hàm băm sử dụng thuật toán NTLM. Với hashes.com, mật khẩu của người dùng là AFR1CA!.   


Q11. Mật khẩu Windows được lưu ở mục C:\Windows\System32\config. Chú ý tới file SAM và SYSTEM. SAM và SYSTEM là 2 file hash được mã hóa bởi thuật toán băm NTLM.   


Lấy đoạn mã hash của 2 file SAM và SYSTEM bằng câu lệnh impacket-secretsdump -sam SAM -system SYSTEM LOCAL.  


Với hashes.com hoặc tool crack Hashcat: hashcat -m 1000 -a 3 "ecf53750b76cc9a62057ca85ff4c850e" -o result.txt (-m 1000 là NTLM), đoạn hash ecf53750b76cc9a62057ca85ff4c850e là ctf2021.  
