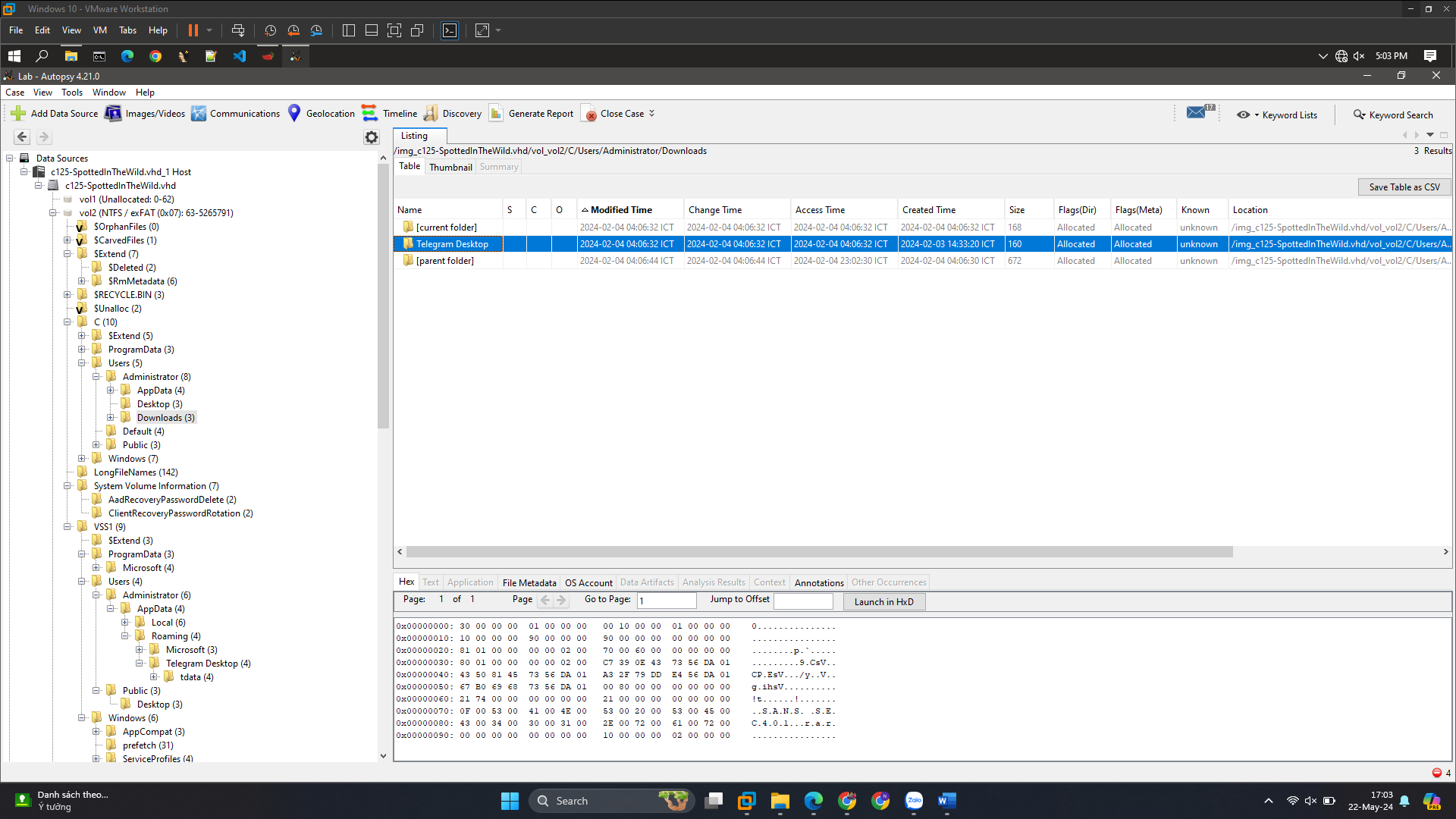
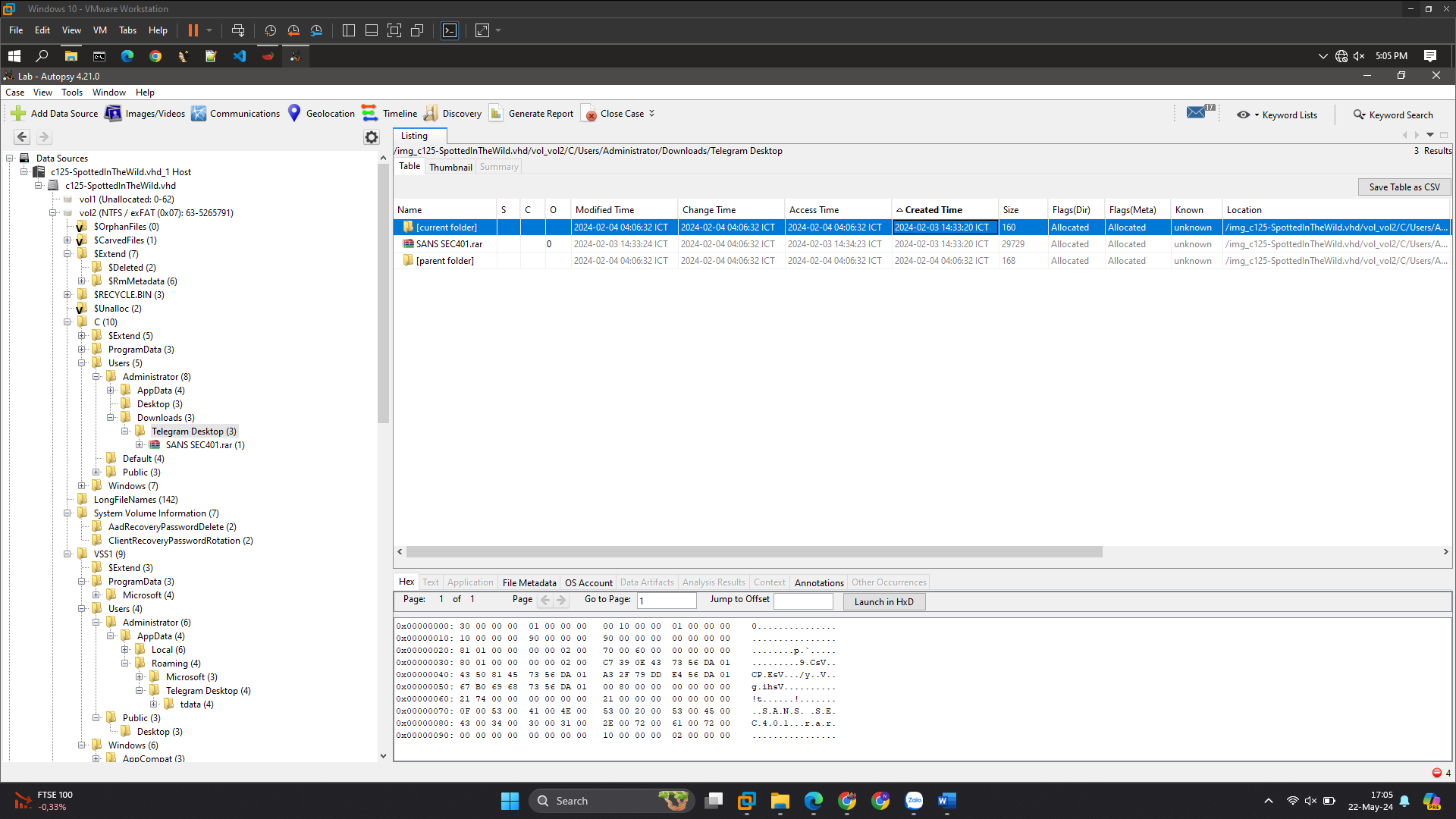
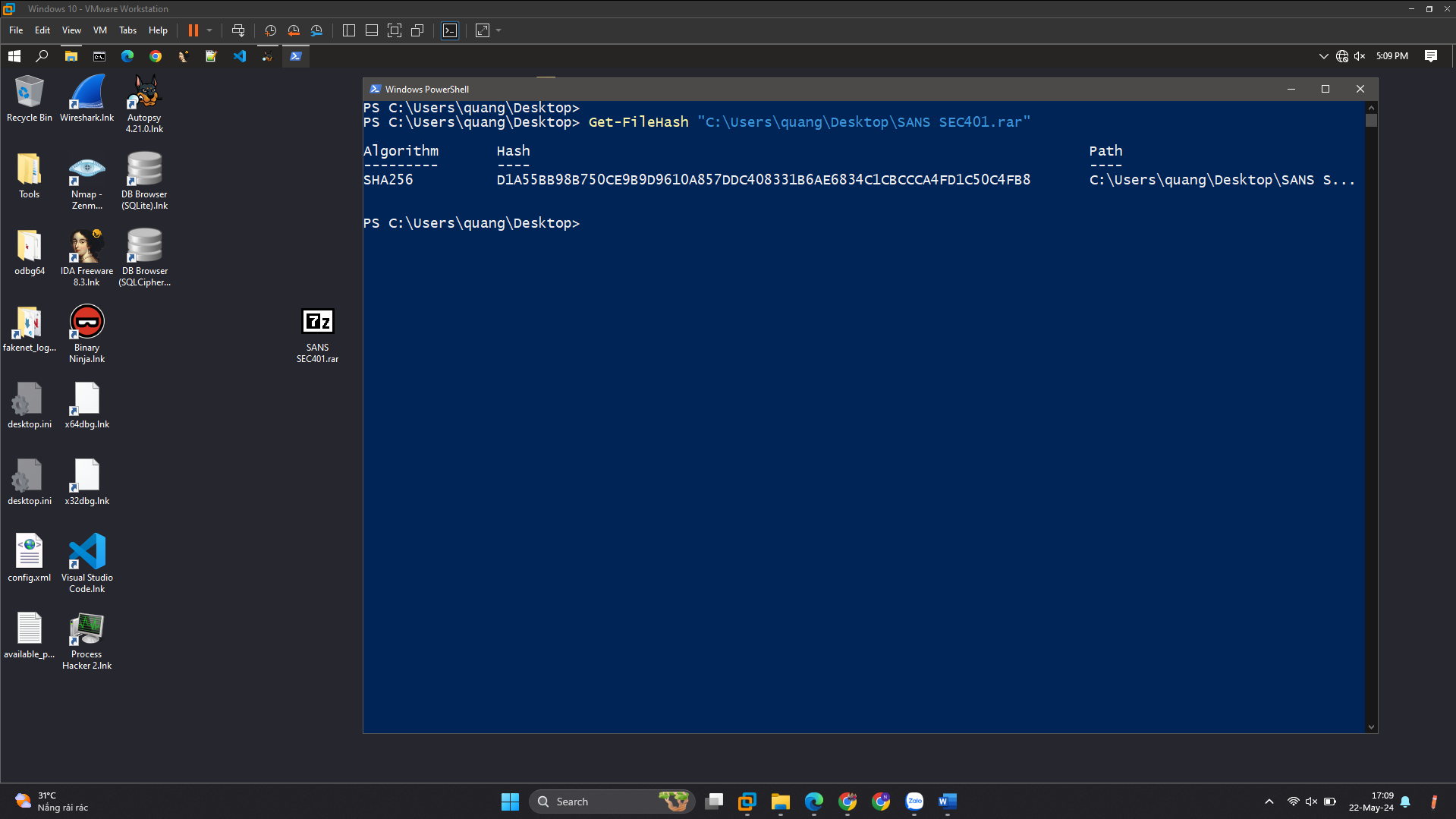
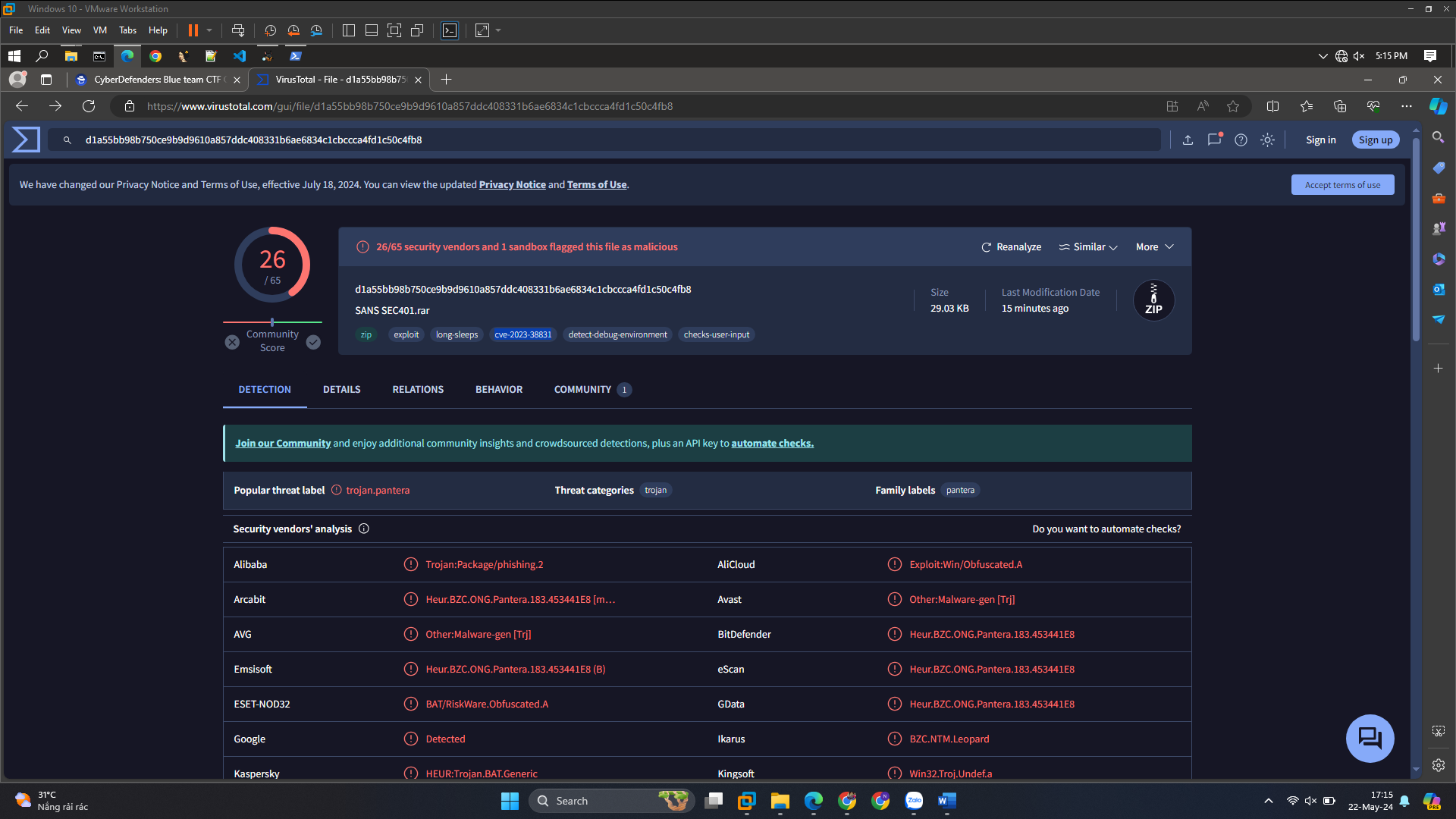
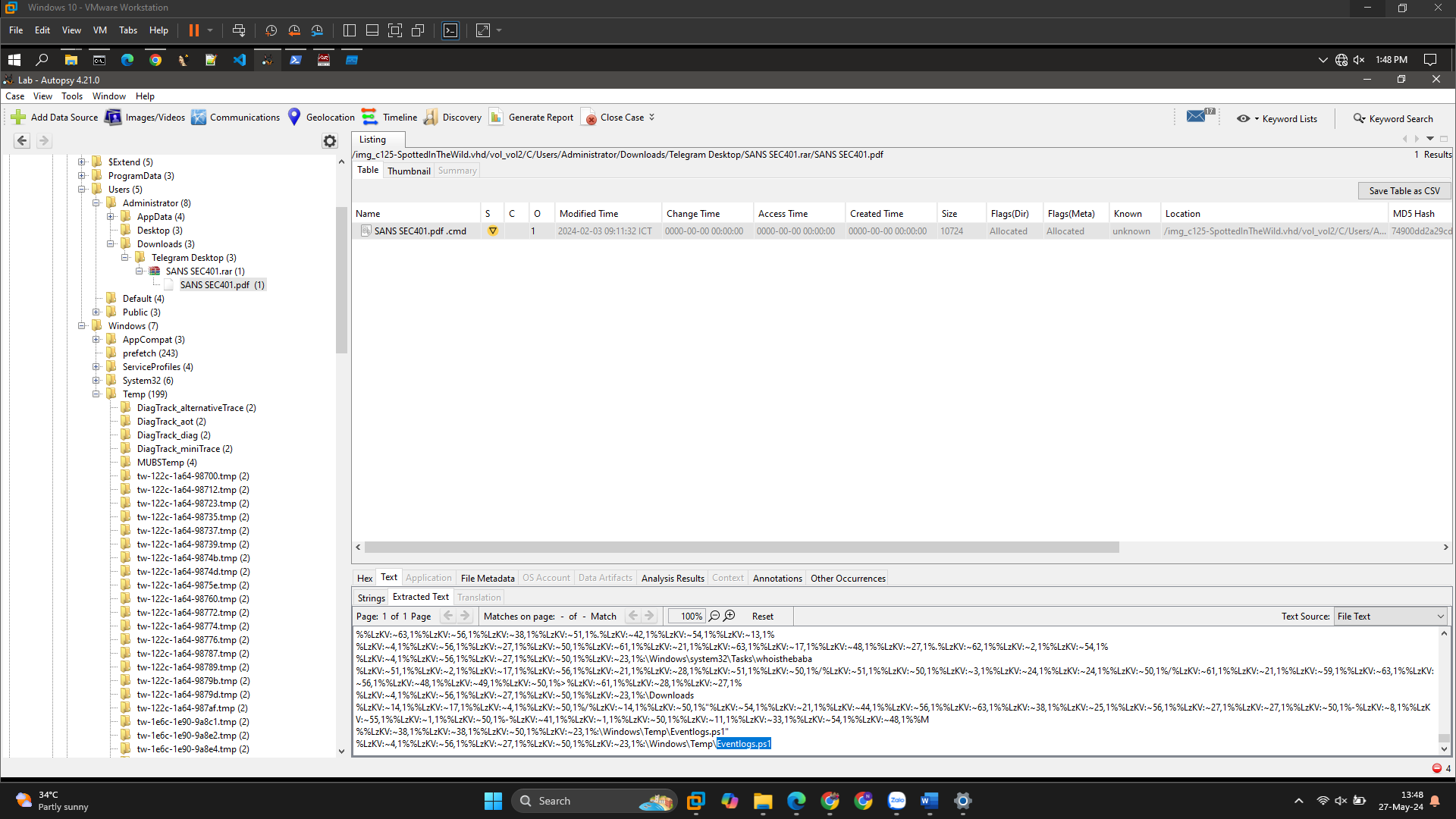
<https://cyberdefenders.org/blueteam-ctf-challenges/spottedinthewild/>

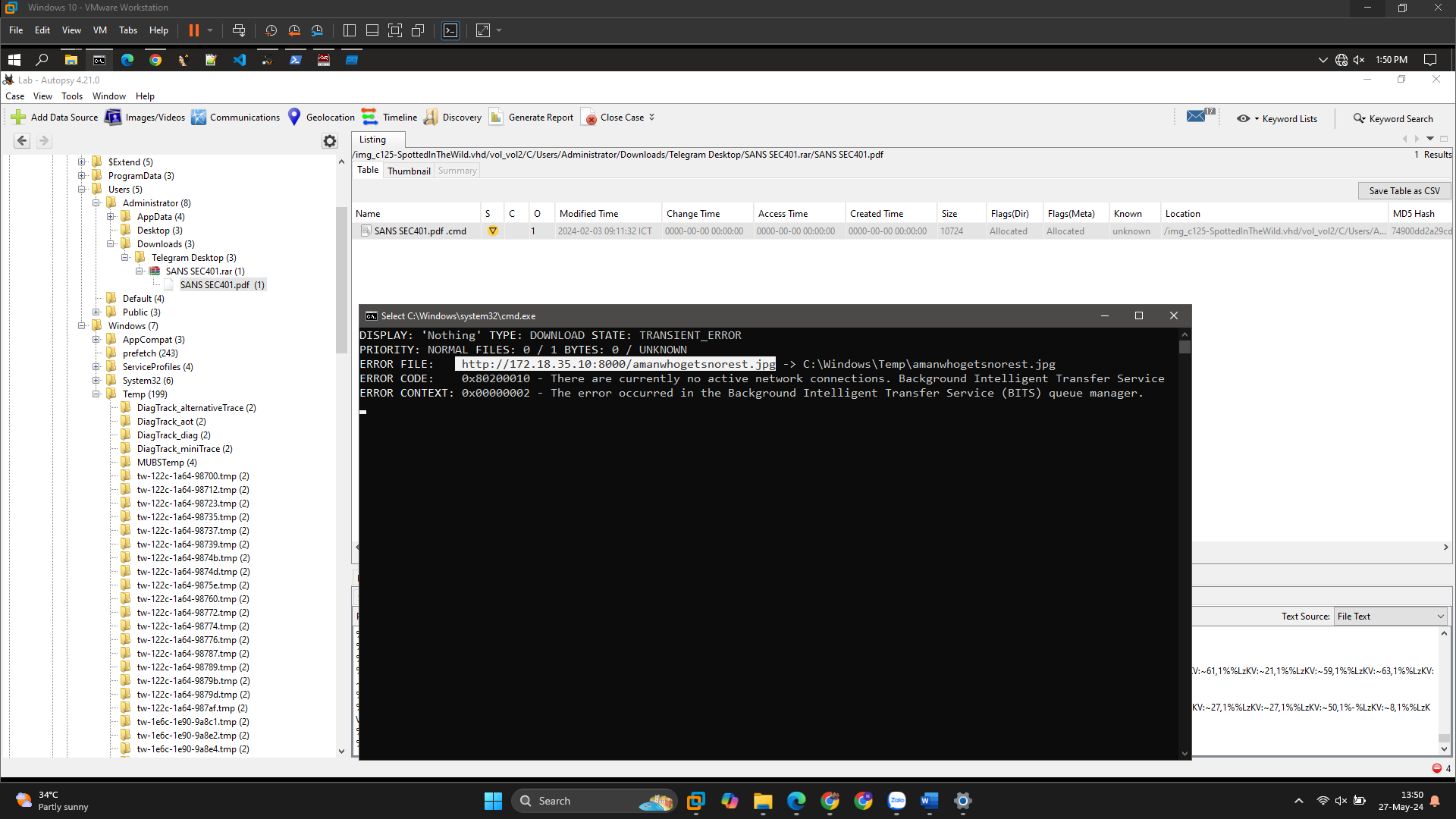
Q1. Mô phỏng một cuộc tấn công mã độc trong ngân hàng FinTrust, cần tìm hiểu xem tệp độc hại nào đã được tải xuống máy. Trong thư mục Downloads, Telegram là khởi đầu của cuộc tấn công, trong Telegram đó có thể đã bị gắn mã độc.  


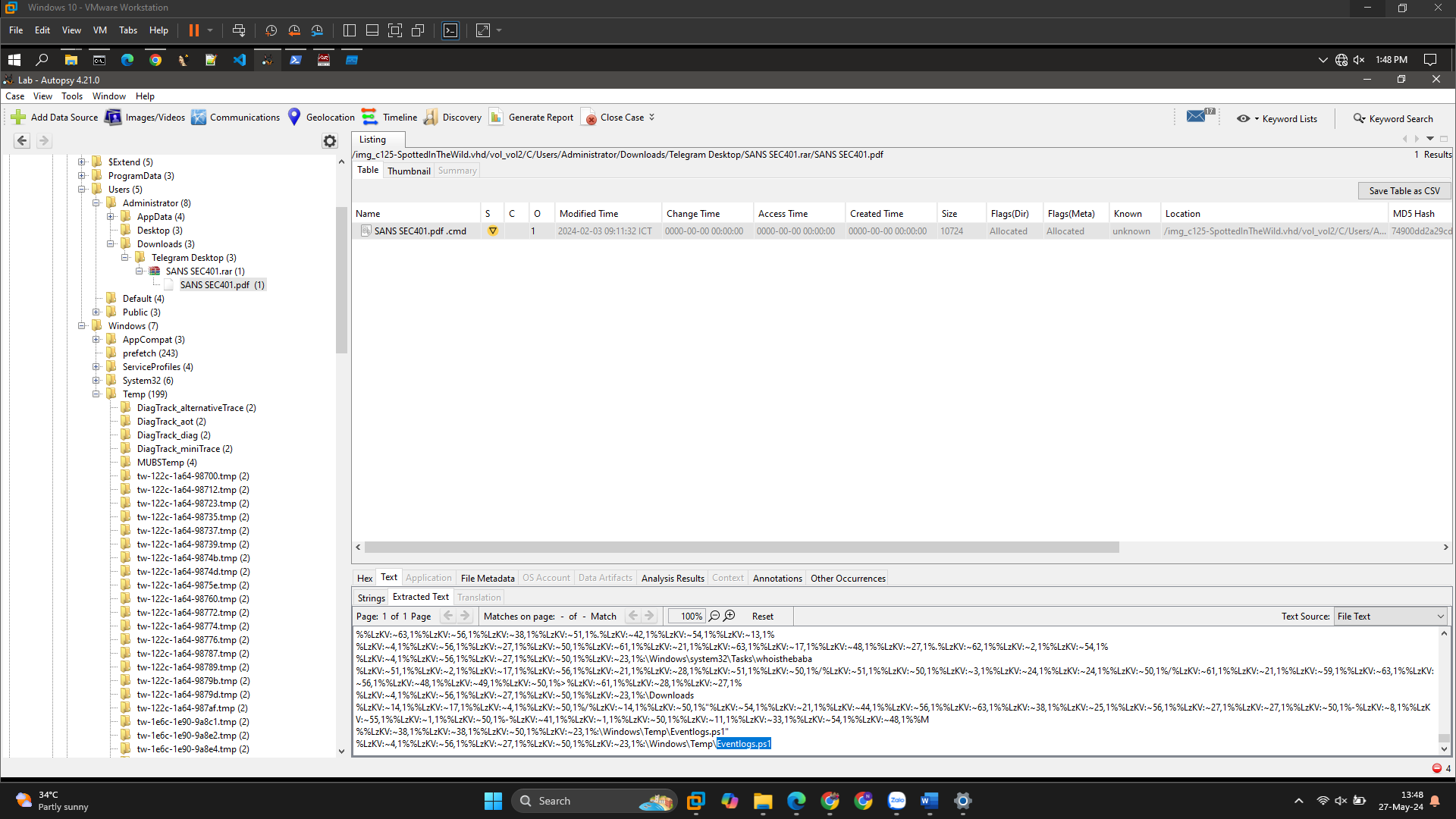
Q2. Thời gian bắt đầu của cuộc tấn công dựa vào thời gian của file mã độc được tải xuống. Bên trong folder Telegram Desktop, có ghi lại mốc thời gian bắt đầu tấn công là 2024-02-03 07:33:20 UTC.  


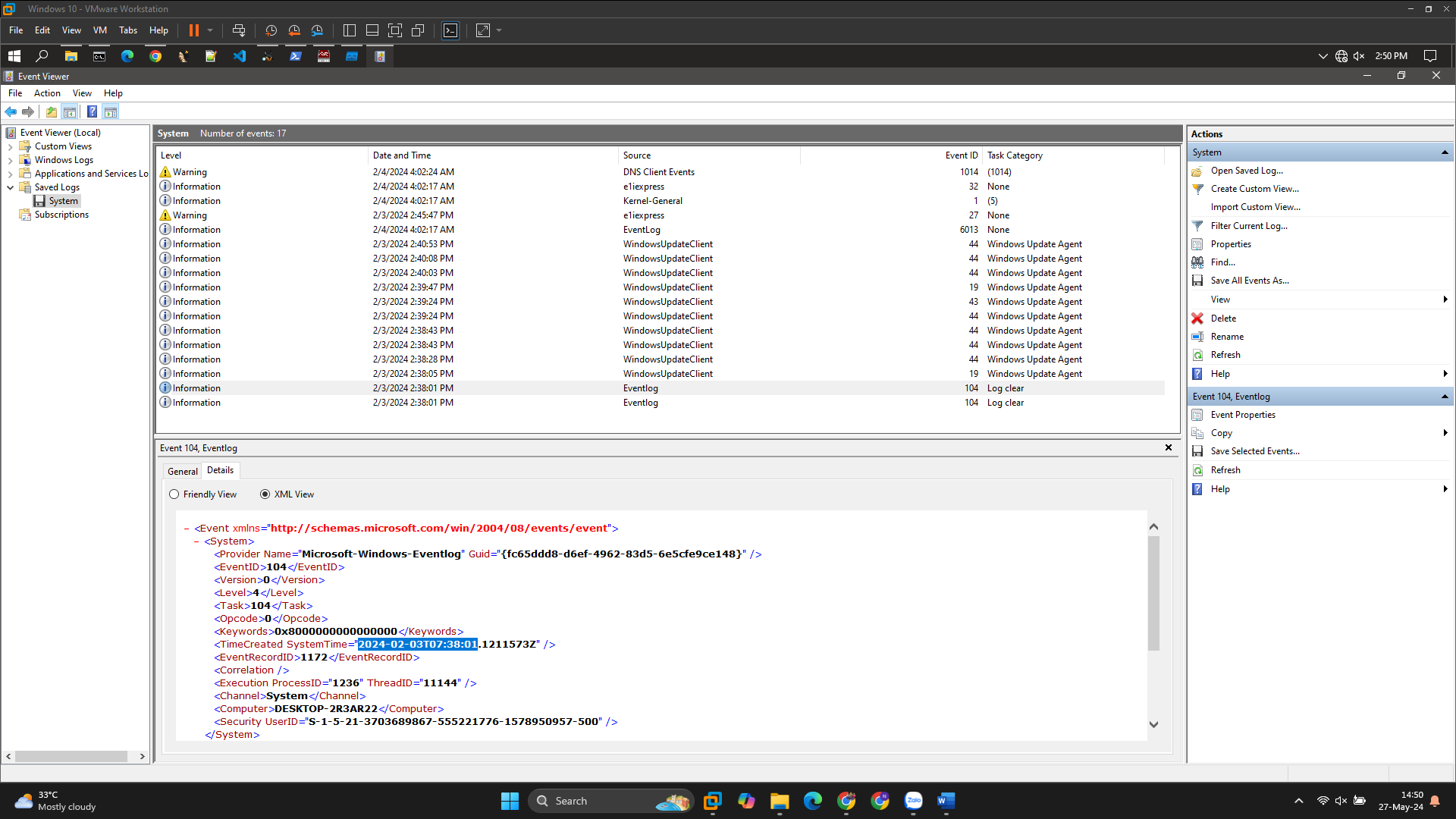
Q3. Để tìm mã CVE của tệp độc hại SANS SEC401.rar trong folder Telegram đó, cần biết đoạn hash của file nén SANS SEC401.   


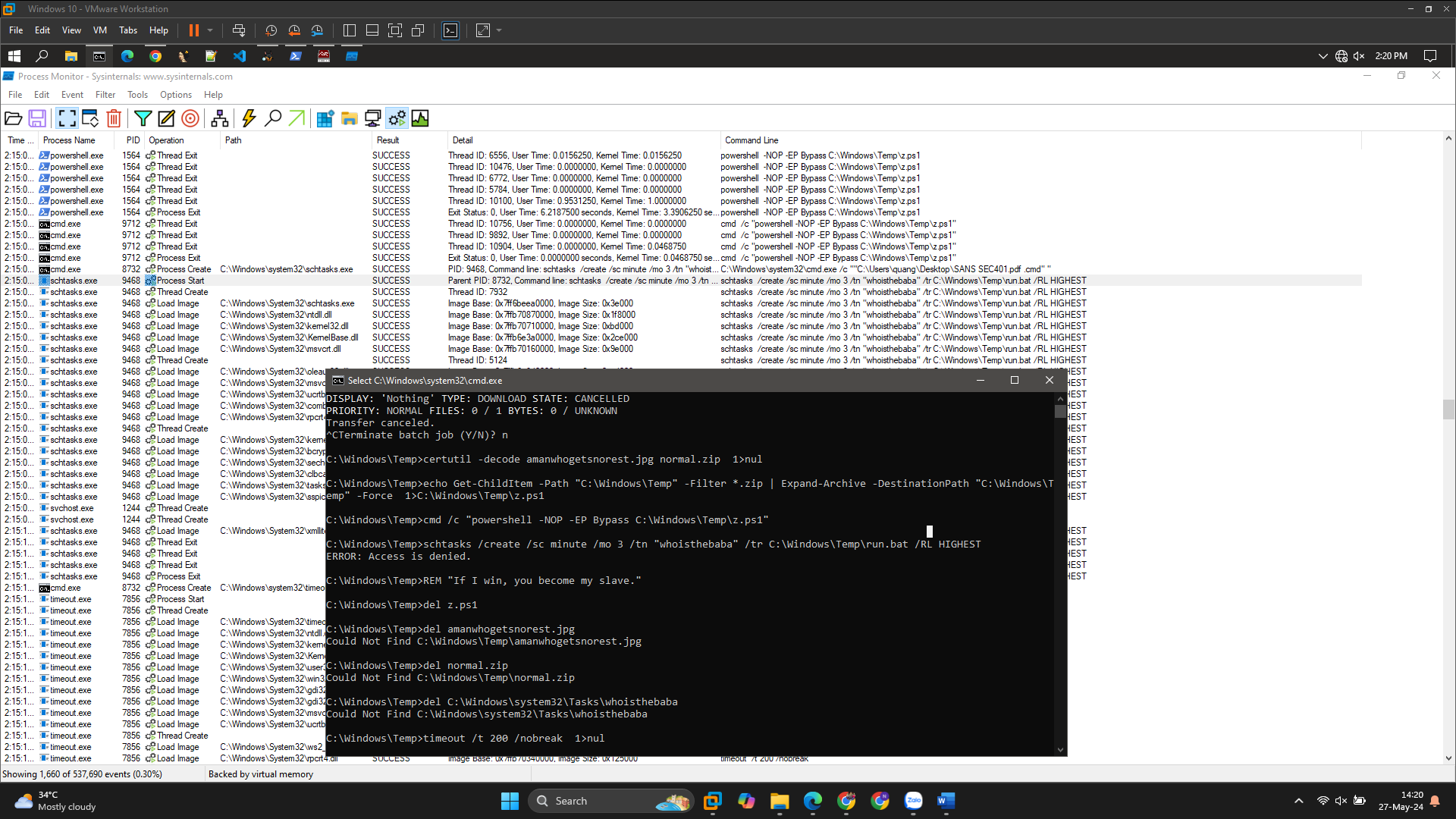
Sau đó, tìm kiếm đoạn hash D1A55BB98B750CE9B9D9610A857DDC408331B6AE6834C1CBCCCA4FD1C50C4FB8 trên VirusTotal. Sau khi scan, VirusTotal trả về kết quả mã CVE của SANS SEC401.rar là CVE-2023-38831.  


Q4. Bên trong file nén SANS SEC401.rar, có SANS SEC401.pdf .cmd có thể là một file đáng ngờ với đuôi .cmd. Với việc sử dụng cmd, nó có thể thực thi mã độc theo ý muốn của kẻ tấn công bằng các câu lệnh với mục đích tải file mã độc khác, che giấu hoạt động, tấn công duy trì…  


Q5. Sau khi SANS SEC401.pdf .cmd khởi chạy, file đó sẽ tải mã độc tiếp theo thông qua đường link của kẻ tấn công gán vào, đó là URL <http://172.18.35.10:8000/amanwhogetsnorest.jpg>.  


Q6. Để kẻ tấn công che giấu hoạt động, chúng đã gắn 1 script powershell vào SANS SEC401.pdf .cmd chạy song song. **Eventlogs.ps1 đã được thực thi trong quá trình** SANS SEC401.pdf .cmd đang chạy, để khi nạn nhân có kiểm tra Event Viewer sẽ không thấy hoạt động của chúng. ****

Q7. Trong thư mục C:\Windows\System32\winevt\logs, có file System.evtx là Event log file. Event log sẽ lưu lại lịch sử tấn công, trong đó có mốc thời gian xóa dấu vết của file mã độc đó. Mốc thời gian đó là 2024-02-03 07:38:01.  


**Q8. Sử dụng Procmon để xem các câu lệnh đã được thực thi. Kẻ tấn công sẽ duy trì quyền truy cập vào máy, mỗi lần máy tính nạn nhân được bật thì mã độc sẽ được thực thi, bằng cách chèn câu lệnh schtasks /create /sc minute /mo 3 /tn "whoisthebaba" /tr C:\Windows\Temp\run.bat /RL HIGHEST trong** SANS SEC401.pdf .cmd. ****

**Q9. Nơi kẻ tấn công đã lưu trữ dữ liệu đã thu thập nằm ở bộ nhớ lưu trữ tạm thời của máy nạn nhân. Đa số hoạt động và trạng thái của máy tính nạn nhân đều được lưu trên bộ nhớ lưu trữ tạm thời này để đảm bảo tính sẵn sàng cho việc phân tích và tấn công. Đường dẫn của file lưu trữ dữ liệu là C:\Users\Administrator\AppData\Local\Temp\BL4356.txt.**