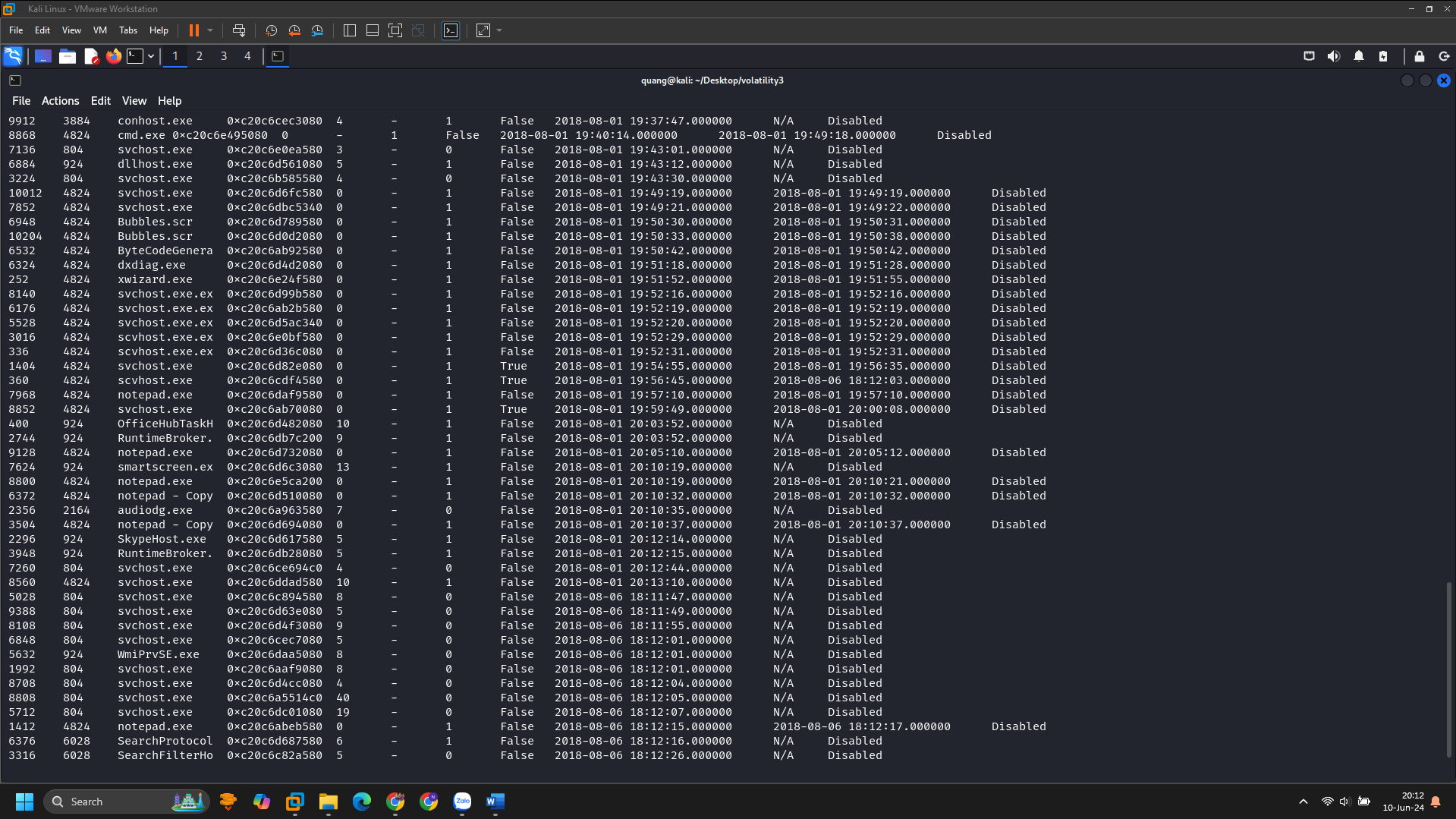
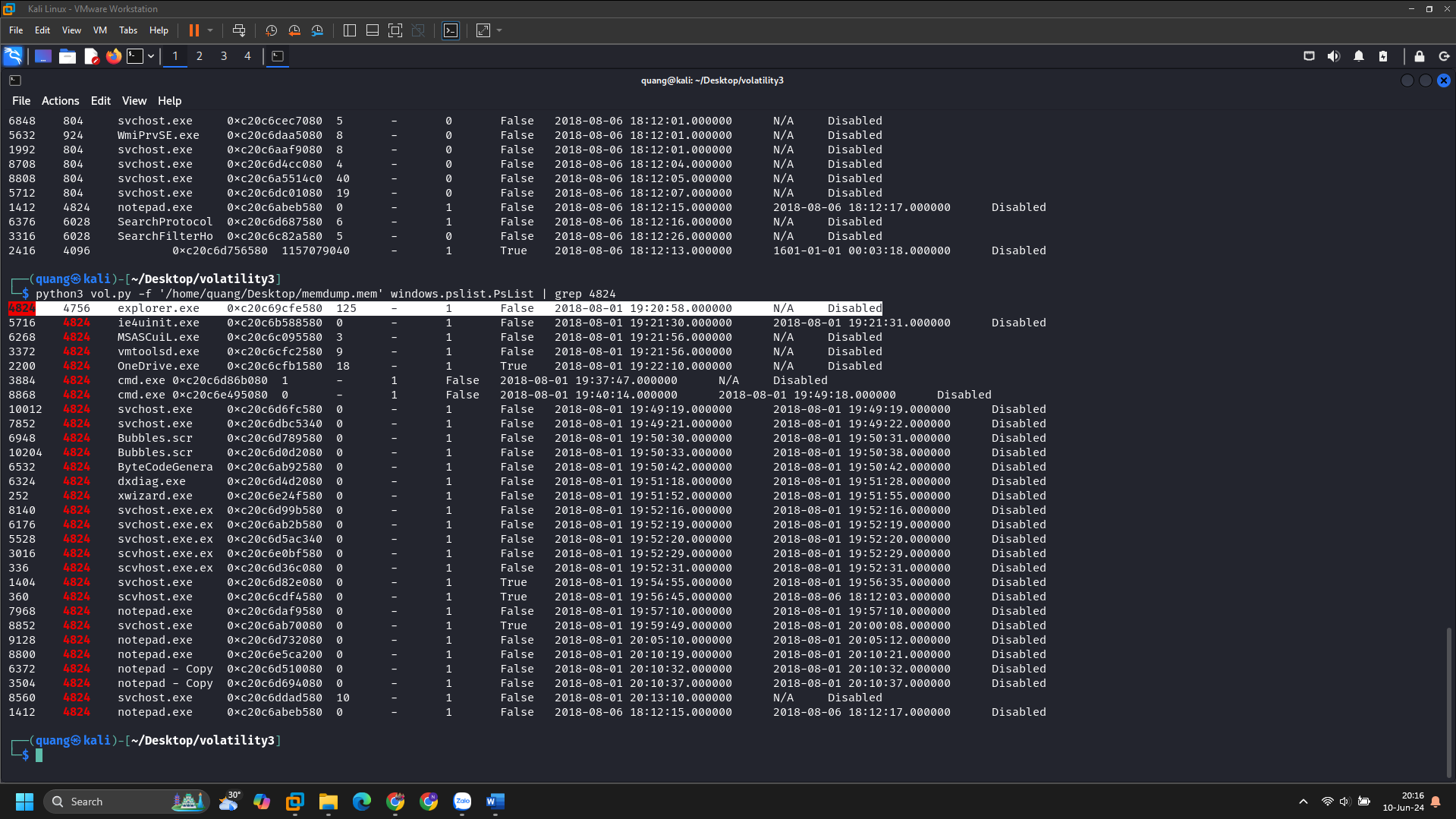
<https://cyberdefenders.org/blueteam-ctf-challenges/nintendohunt/>

Q1. ID tiến trình của tiến trình độc hại hiện đang chạy là 8560.

Sử dụng câu lệnh python3 vol.py -f memdump.mem windows.pslist.PsList để xem các tiến trình đang chạy trên máy tính bị tấn công. Ta thấy có khá nhiều tiến trình khả nghi trên PPID 4824, đặc biệt là svchost.exe.exe vì có 2 đuôi exe, nên thử xác định xem ID 4824 đó cụ thể ra sao.

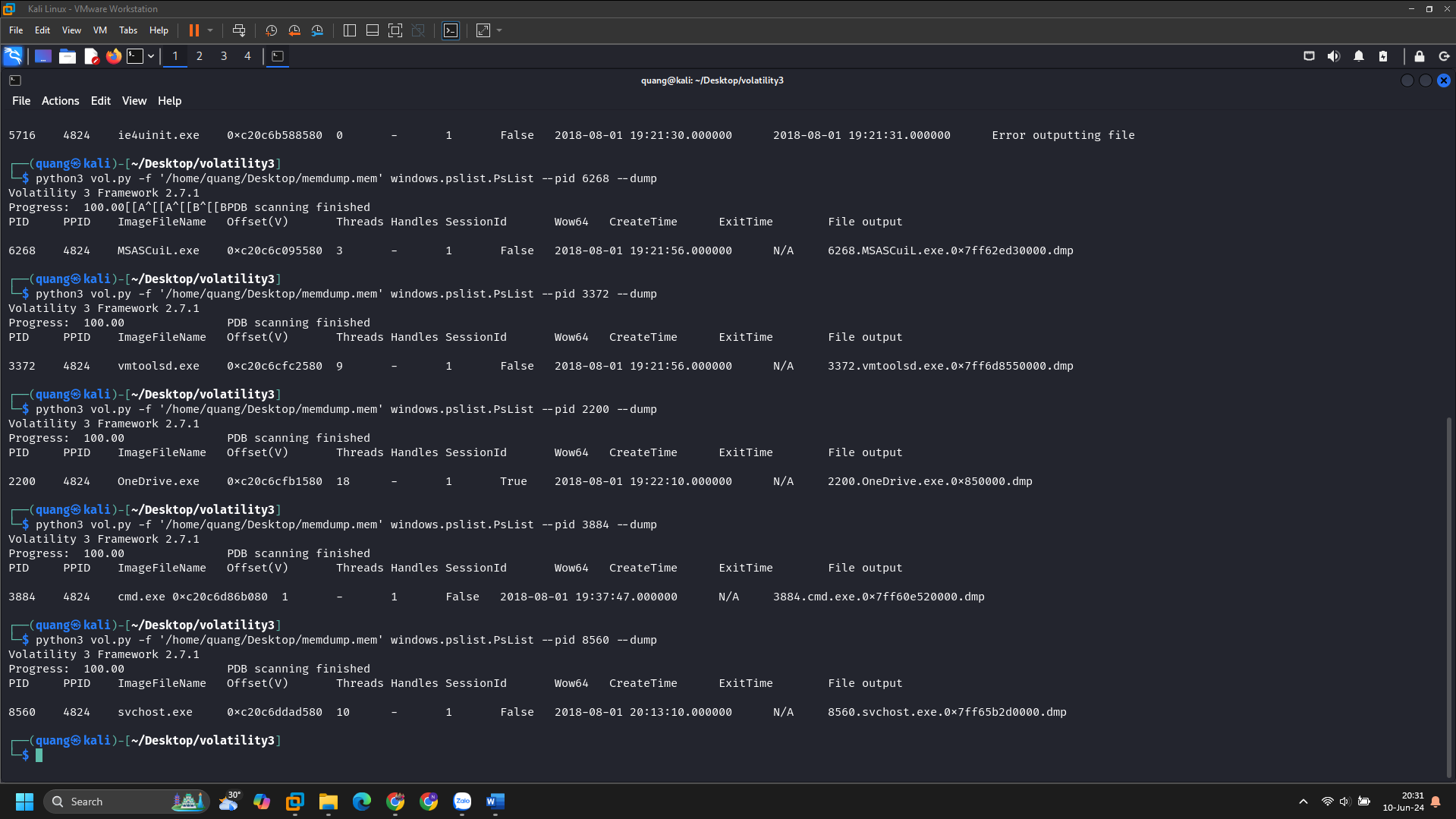


Sử dụng câu lệnh python3 vol.py -f memdump.mem windows.pslist.PsList | grep 4824 để tìm ra các tiến trình có PPID là 4824. Nếu PID tiến trình 4824 là Explorer thì đó là điều không bình thường vì tất cả các tiến trình trước đó đã ngừng hoạt động. Explorer là chương trình quản lý các folder của Windows, đồng thời hiển thị giao diện đồ họa GUI Windows tương tác với người dùng.



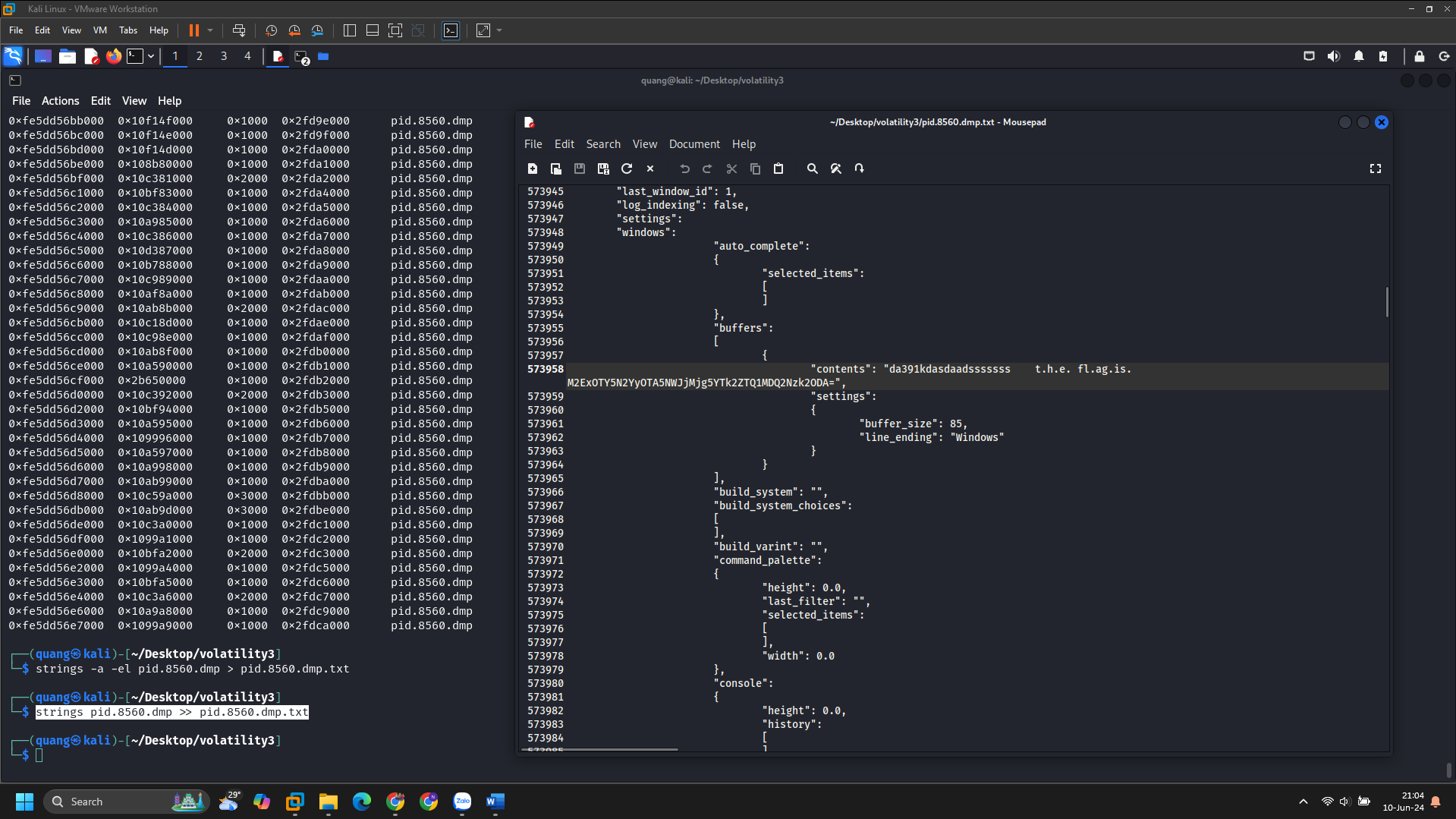
Kiểm tra từng PID một trong danh sách đã được lọc bởi PPID 4824, xem nếu có giá trị băm thì đó là PID của tiến trình độc hại đó, bởi các câu lệnh:

python3 vol.py -f memdump.mem windows.pslist.PsList --pid XXXX –dump, với XXXX là PID tiến trình. Qua đó chỉ có tiến trình 8560 có giá trị hash.

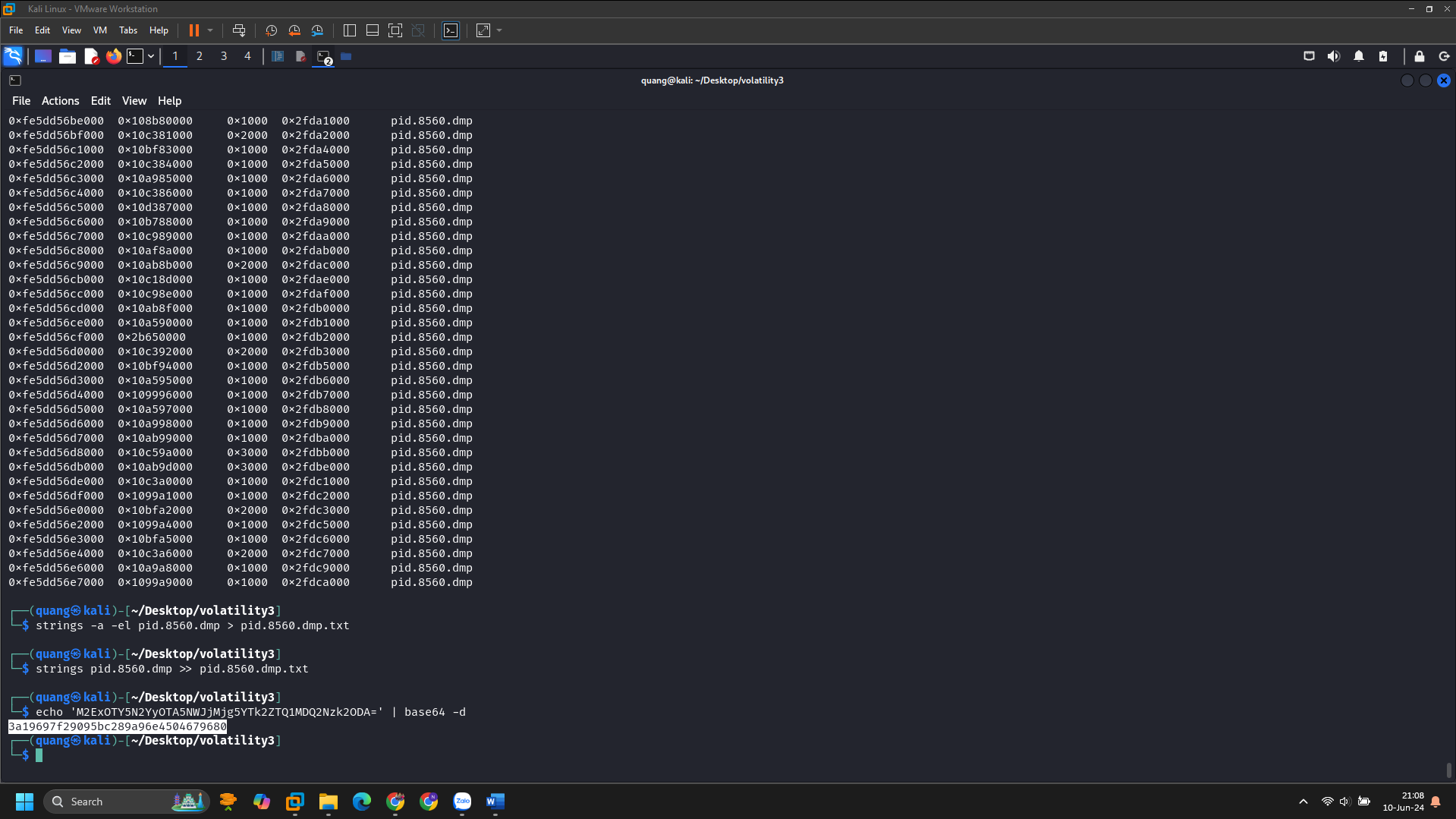


Q2. Hash md5 ẩn trong bộ nhớ tiến trình độc hại 8560 là 3a19697f29095bc289a96e4504679680.

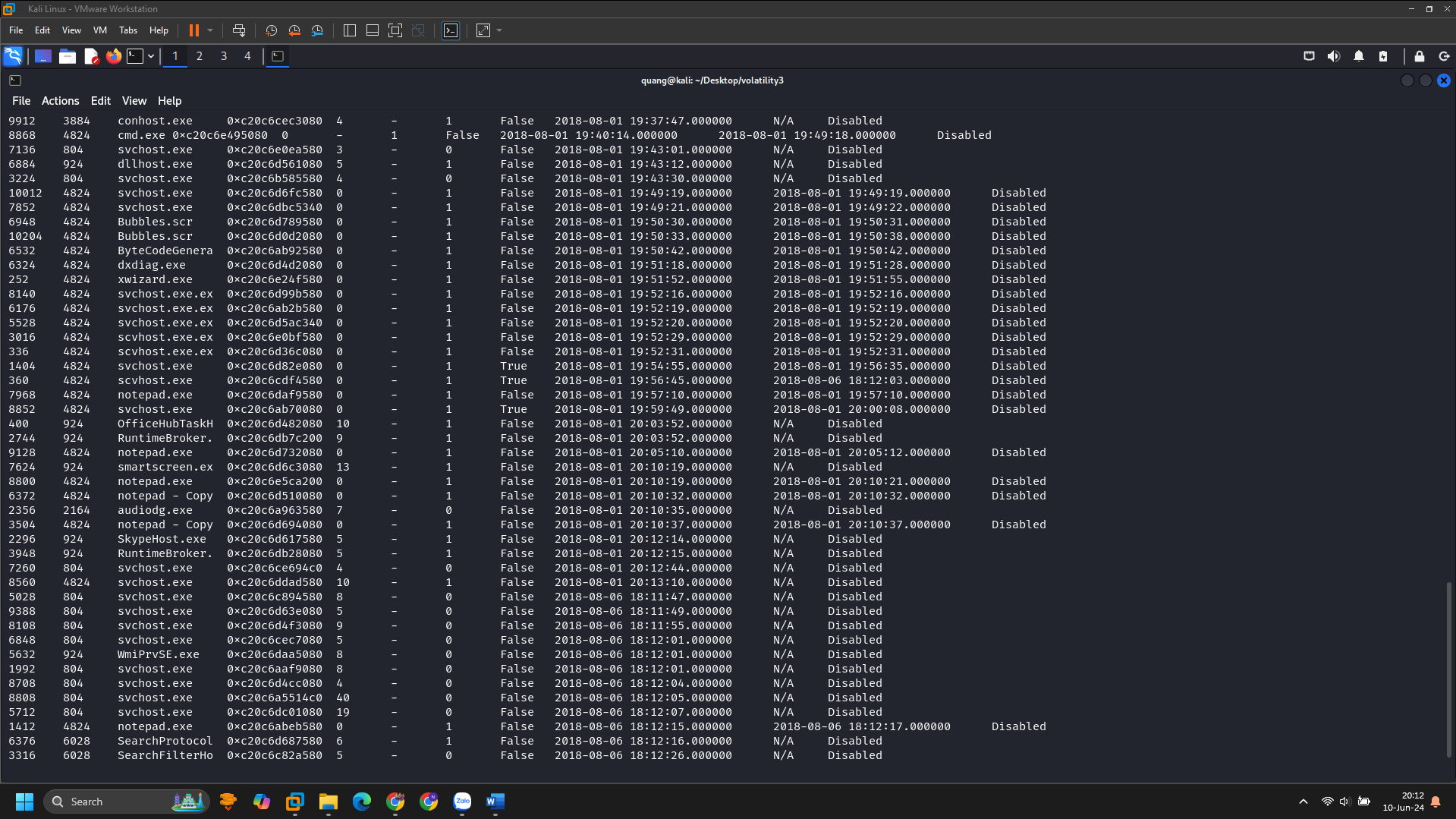
Sử dụng câu lệnh python3 vol.py -f memdump.mem windows.memmap.Memmap --pid 8560 --dump để dump các memory page của PID 8560. Sau khi ra pid.8560.dump, phân tích file dump bằng câu lệnh strings pid.8560.dmp >> pid.8560.dmp.txt.



Ở đây có 1 đoạn mã M2ExOTY5N2YyOTA5NWJjMjg5YTk2ZTQ1MDQ2Nzk2ODA= được xác định mã hóa theo dạng Base64. Với câu lệnh echo 'M2ExOTY5N2YyOTA5NWJjMjg5YTk2ZTQ1MDQ2Nzk2ODA=' | base64 -d, ta đã có đoạn hash là 3a19697f29095bc289a96e4504679680.

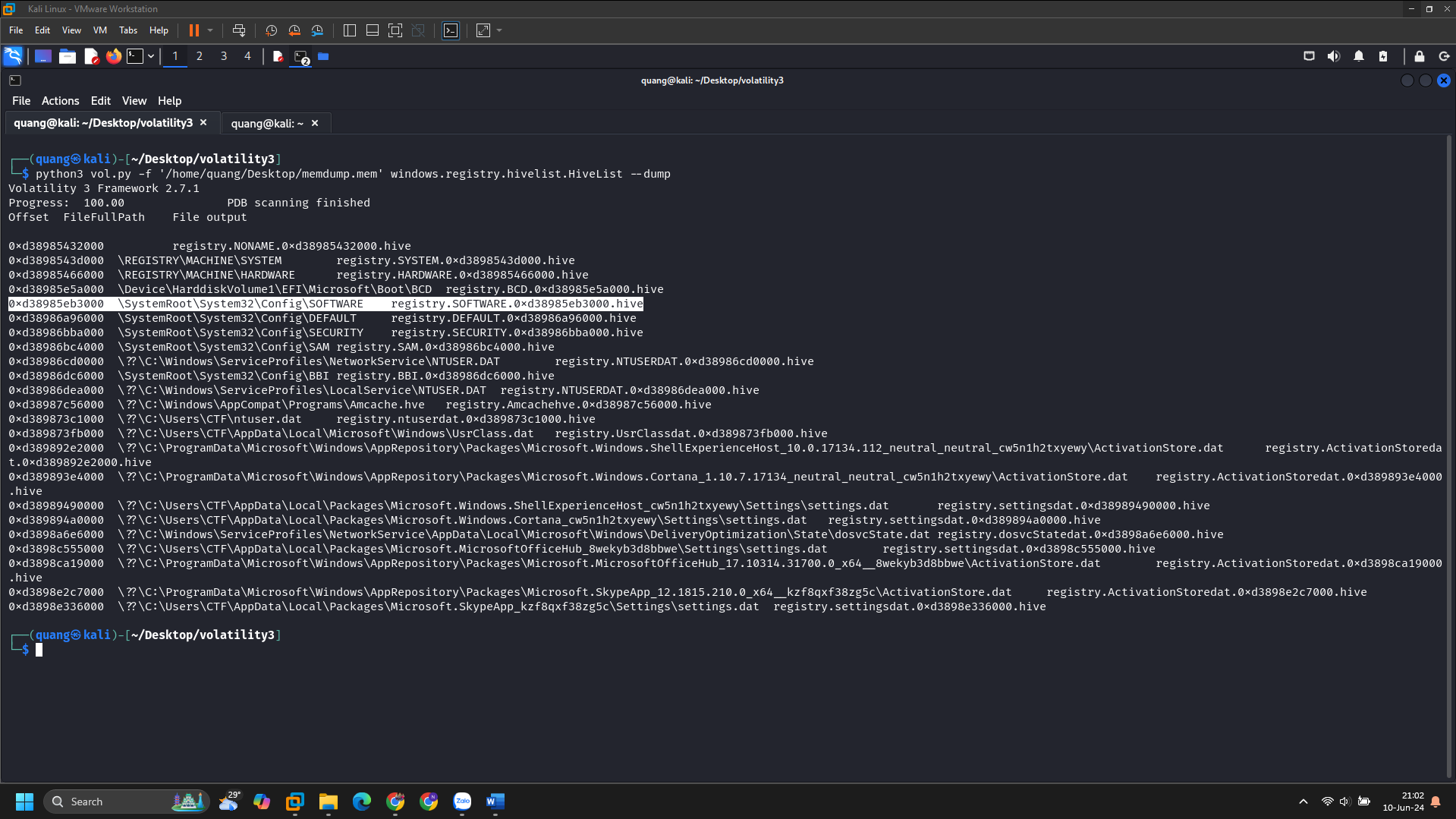


Q3. Tên tiến trình của tiến trình gốc độc hại là Explorer, bởi khi chạy câu lệnh python3 vol.py -f memdump.mem windows.pslist.PsList | grep 4824, Explorer là nơi khởi chạy tiến trình độc hại 8560 từ PPID 4824.

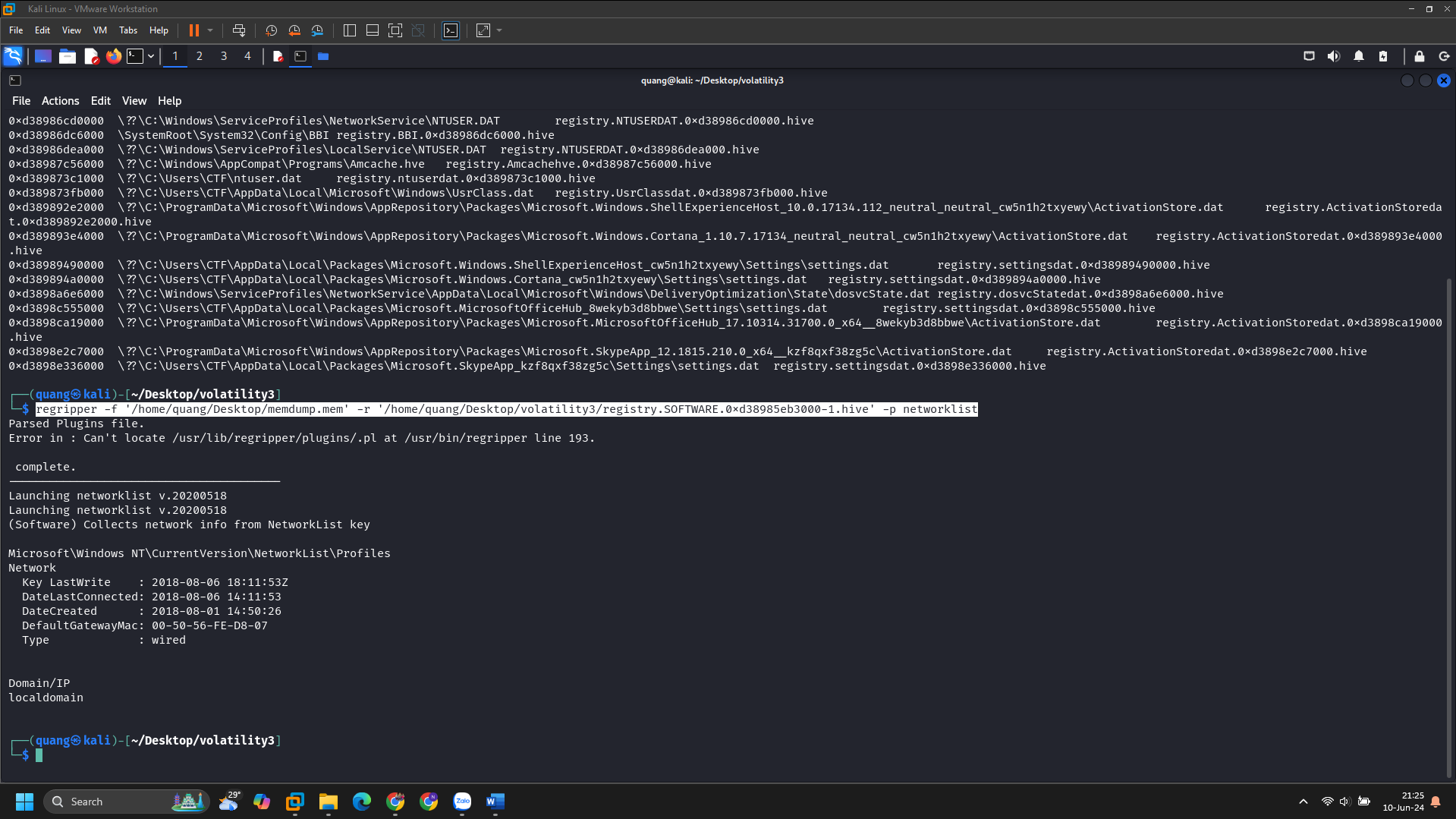


Q4. Địa chỉ MAC của cổng mặc định của máy này là 00:50:56:FE:D8:07.

Sử dụng câu lệnh python3 vol.py -f memdump.mem windows.registry.hivelist.HiveList --dump để xem Software registry của máy tính bị tấn công. Sau khi chạy câu lệnh trên, 1 loạt file .hive được xuất ra và ta sẽ xác định file SOFTWARE.

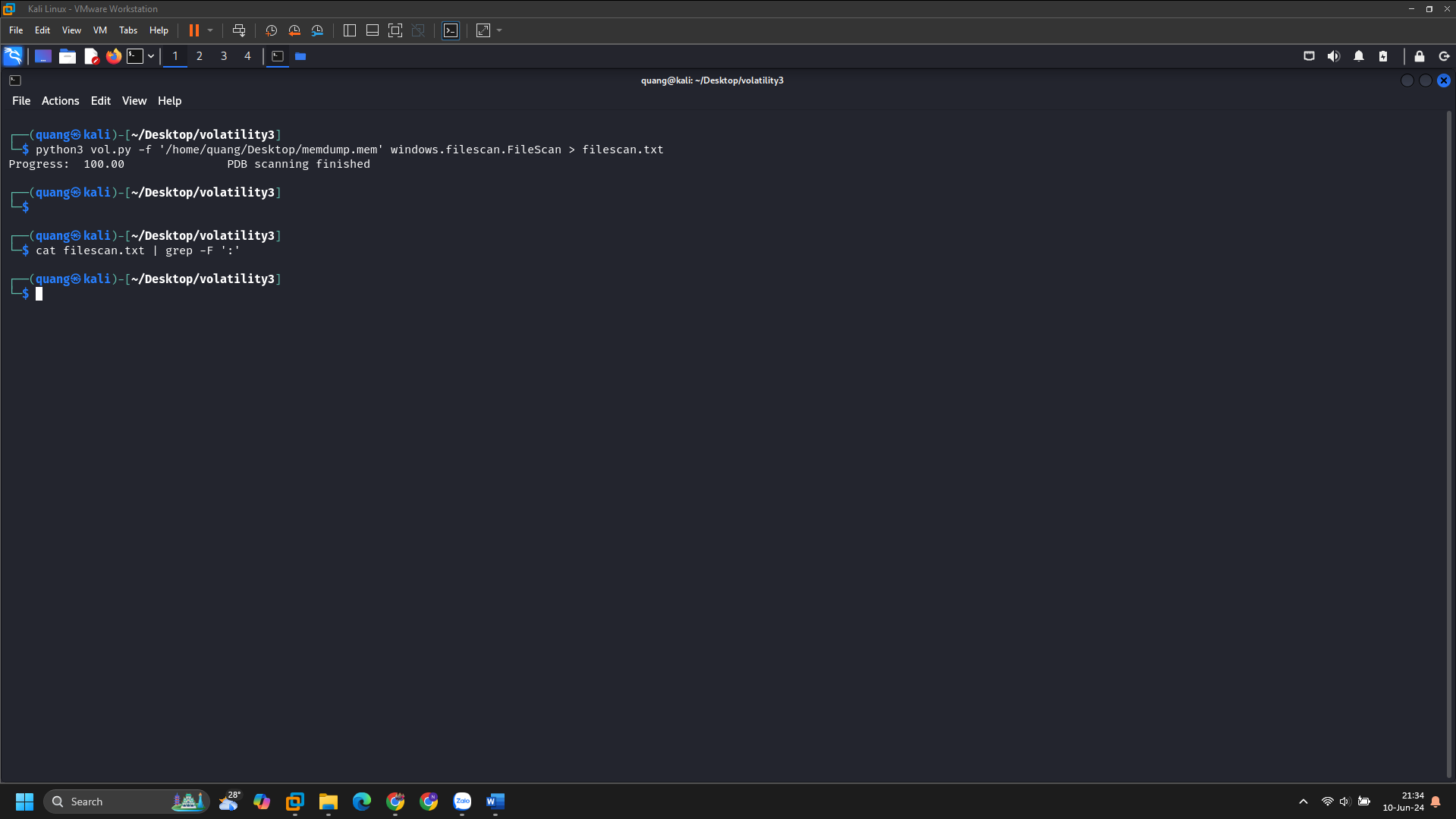


Sử dụng câu lệnh regripper -f memdump.mem -r registry.SOFTWARE.0xd38985eb3000-1.hive -p networklist để kiểm tra địa chỉ MAC của máy bị tấn công. Tại đây RegRipper hiển thị địa chỉ MAC của máy bị tấn công là 00-50-56-FE-D8-07.



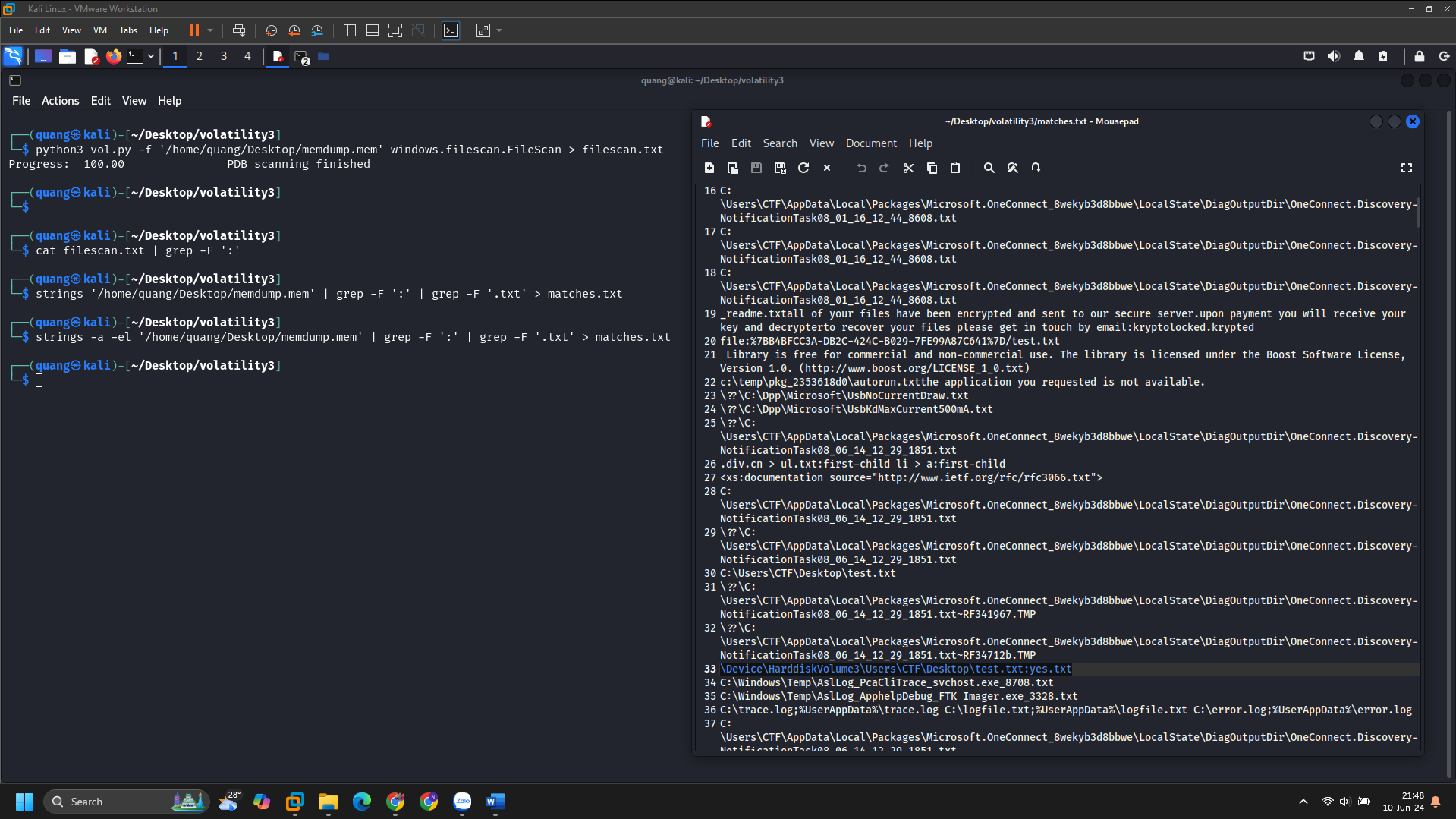
Q5. Tên của file bị ẩn trong luồng dữ liệu thay thế là yes.txt.

Ta sẽ sử dụng plugin FileScan, và tìm các file có liên quan kết thúc bằng “:” và xuất thành file, sử dụng câu lệnh python3 vol.py -f memdump.mem windows.filescan.FileScan > filescan.txt. Sau đó kiểm tra xem có tệp nào kết thúc bằng “:” không.

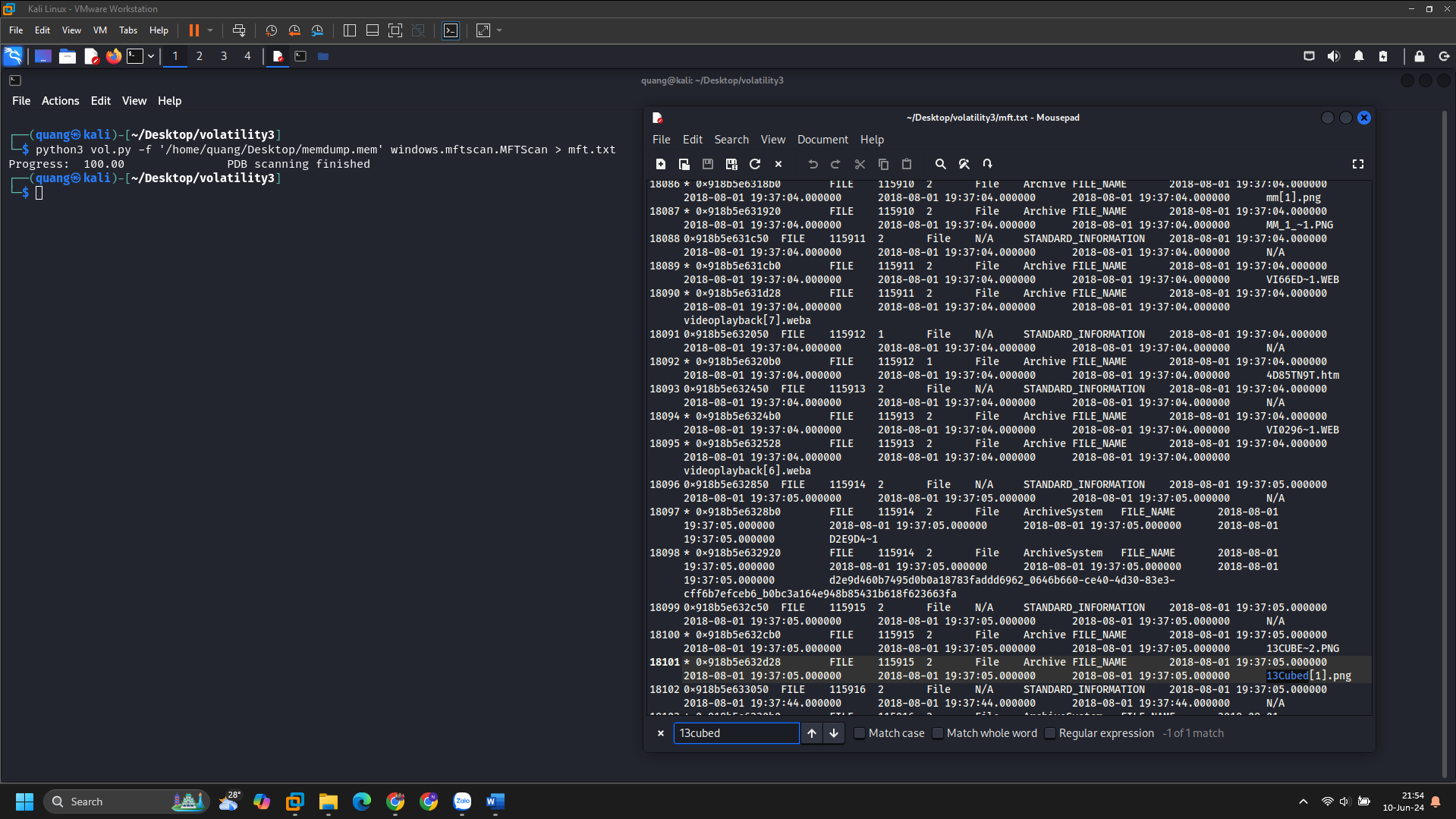


Tiếp đó, phân tích file memdump.mem lọc ra các file kết thúc bởi “:” và “.txt”, đồng thời xuất ra file để thuận tiện tìm, bằng câu lệnh strings -a -el memdump.mem | grep -F ':' | grep -F '.txt' > matches.txt.

Địa chỉ file bị ẩn trong luồng dữ liệu là \Device\HarddiskVolume3\Users\CTF\Desktop\test.txt:yes.txt.



Q6. Để tìm đường dẫn được tạo khi truy cập vào trang web, cần xem xét thời điểm nào mà máy tính đó truy cập vào trang web đó. Dữ liệu này được lưu trữ lại trong bảng MFT. Sử dụng plugin MFTScan: python3 vol.py -f memdump.mem windows.mftscan.MFTScan > mft.txt để tìm các dữ liệu MFT. Tuy nhiên plugin này chỉ trả về tên file 13Cubed[1].png. Thế nên ta sẽ sử dụng Volatility2 được viết bởi python2.



Đây là máy tính chạy Windows 10, phiên bản kernel và bản dựng 6.4.17134. Sử dụng câu lệnh   
python2 vol.py -f memdump.mem --profile=Win10x64\_17134 mftparser > mft.txt. Đường dẫn đó là: C:\Users\CTF\AppData\Local\Packages\MICROS~1.MIC\AC\#!001\MICROS~1\Cache\AHF2COV9\13cubed[1].htm.  
