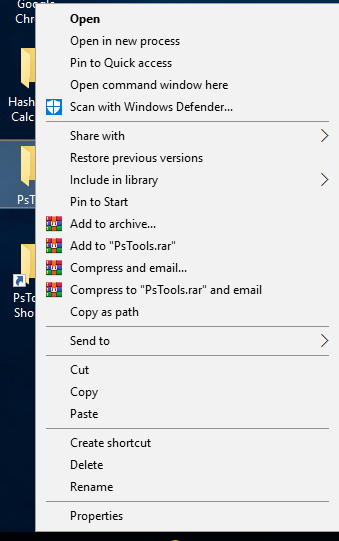
**Module 6: Windows Forensics**

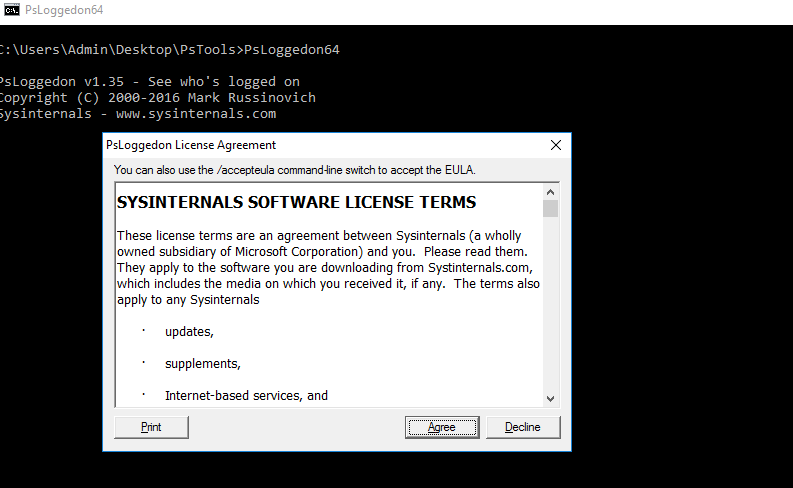
# **Lab 1: Acquiring Volatile Information from a Live Windows System**

## **Task 1: Gather Information About Logged On Users**

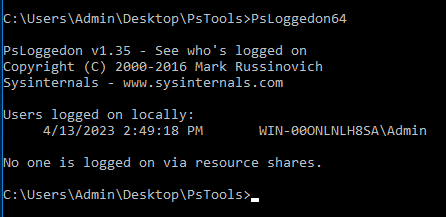
1. Đăng nhập vào máy ảo Windows Server 2016 và Windows 10
2. Trong máy ảo Windows Server 2016, điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Volatile Data Acquisition Tools.
3. Chọn thư mục PsTools, giữ phím Shift trên bàn phím, nhấp chuột phải vào thư mục đã chọn, sau đó chọn Open command window here từ menu ngữ cảnh

****

1. Thao tác trên sẽ khởi chạy Command Prompt hiển thị đường dẫn của PsTools. Nhập PsLoggedon64.exe và nhấn Enter.
2. Cửa sổ PsLoggedon License Agreement sẽ xuất hiện. Nhấn Agree để tiếp tục.

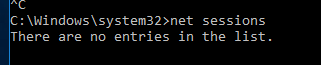


1. Lúc này, cửa sổ Command Prompt sẽ hiển thị hai kết quả: Users Logged on locally (ở đây, người dùng cục bộ là Administrator của máy cục bộ) và Users Logged on via resource shares (trong trường hợp này, không có người dùng nào đăng nhập thông qua chia sẻ tài nguyên; do đó, kết quả hiển thị null trong phần Users Logged on via resource shares).

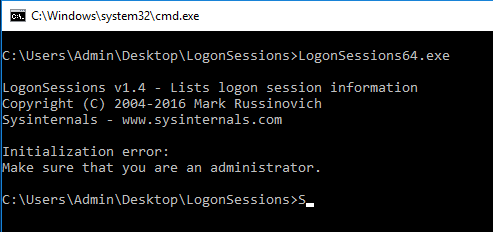


1. Bây giờ, hãy đóng cửa sổ Command Prompt và khởi chạy nó với tư cách Administrator bằng cách nhấp chuột phải vào nút Start (nút biểu tượng Windows) rồi nhấp vào Command Prompt (Admin). Bây giờ chúng ta sẽ chạy lệnh net session, lệnh này sẽ liệt kê địa chỉ IP của tất cả các phiên kết nối trên máy chủ (ở đây là Windows Server 2016), lệnh đã liệt kê địa chỉ IP của máy ảo Windows 10 như hình dưới đây ảnh chụp màn hình:

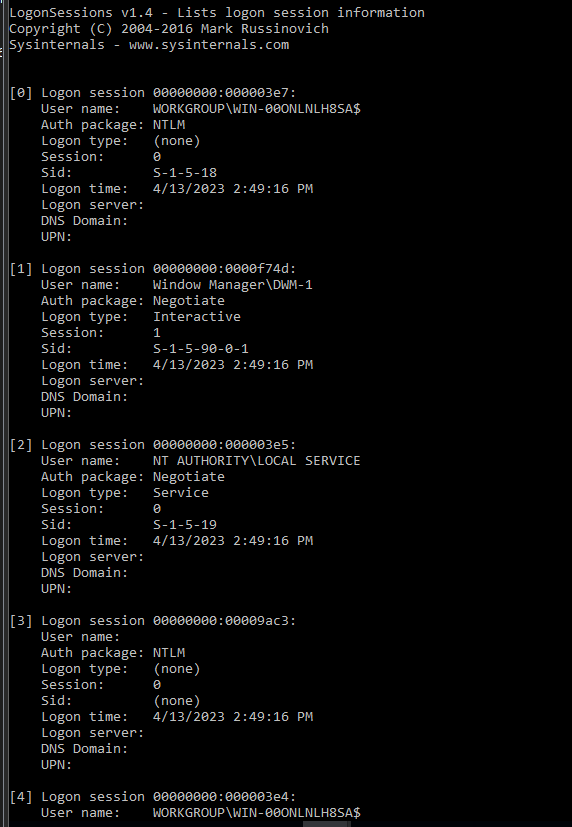
Lưu ý: Lệnh net session chỉ có thể chạy trên máy ảo Windows Server 2016 và kết quả có thể khác trong môi trường lab của bạn



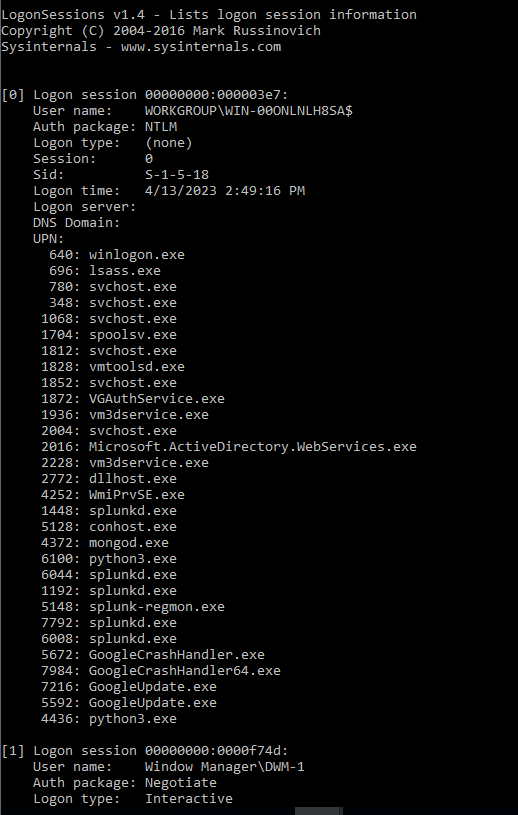
1. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Volatile Data Acquisition Tools, chọn thư mục LogonSessions, giữ phím Shift trên bàn phím, nhấp chuột phải vào thư mục đã chọn và chọn Open command window here từ menu ngữ cảnh.
2. Thao tác trên sẽ khởi chạy Command Prompt với đường dẫn LogonSessions. Nhập LogonSessions64.exe và nhấn Enter.



1. Cửa sổ LogonSessions License Agreement sẽ xuất hiện. Nhấn Agree để tiếp tục.
2. Lúc này tiện ích sẽ liệt kê các phiên đăng nhập đang hoạt động



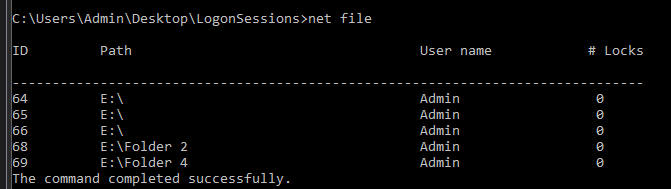
1. Để liệt kê các phiên đăng nhập, loại của chúng và các quy trình chạy bên dưới chúng, hãy sử dụng khóa chuyển -p kết hợp với LogonSessions64.exe. Tất cả các quy trình đang chạy được liên kết với mỗi phiên sẽ được hiển thị trong phần UPN như trong ảnh chụp màn hình:

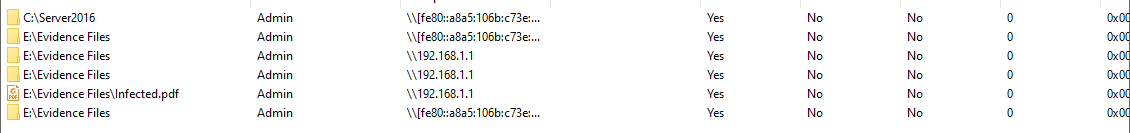
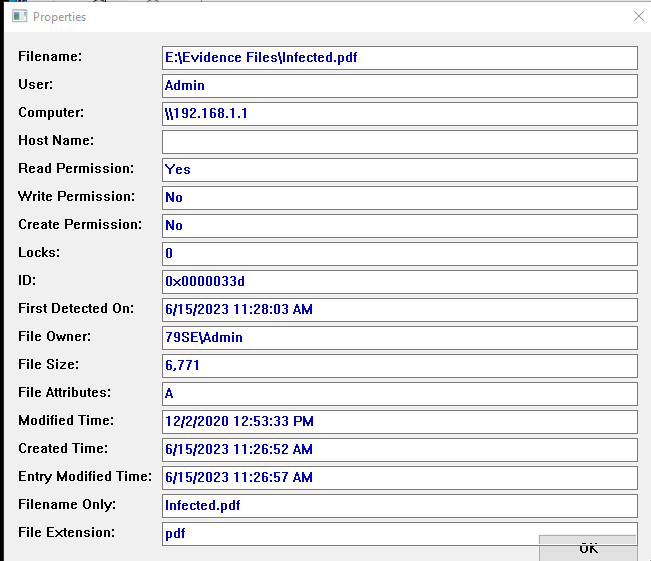


1. Đóng Command Prompt

## **Task 2: Gather Information About Shared Files**

1. Bây giờ, chúng tôi sẽ sử dụng tiện ích net file để truy xuất thông tin liên quan đến tất cả các tệp được chia sẻ đang mở đối với máy ảo Windows Server 2016. Trước khi bạn bắt đầu tác vụ này, hãy chuyển sang máy ảo Windows 10 và mở Z:\.
2. Chuyển về máy ảo Windows Server 2016. Để chạy lệnh net file, hãy khởi chạy command prompt bằng cách nhấp chuột phải vào nút Start rồi nhấp vào Command Prompt (Administrator). Trong cửa sổ Command Prompt, gõ net file và nhấn Enter.
3. Lệnh net file lúc này sẽ hiển thị Đường dẫn của thư mục dùng chung từ máy cục bộ được các máy khác truy cập (ở đây là máy ảo Windows 10); nó cũng hiển thị Username của tài khoản người dùng đang truy cập từ xa vào thư mục dùng chung cùng với ID và Locks được liên kết với thư mục dùng chung như trong ảnh chụp màn hình:

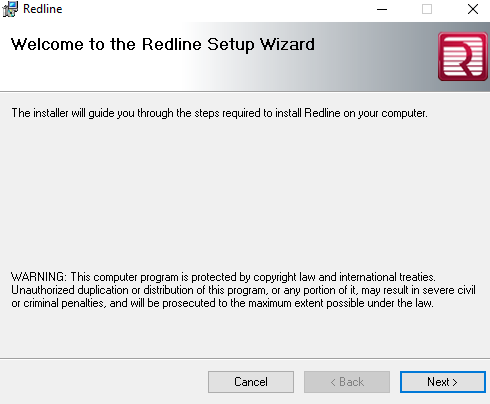


1. Để phân tích sâu hơn, bạn có thể sử dụng NetworkOpenedFiles để lấy thêm thông tin về network folder/drive dùng chung, chẳng hạn như IP Address, Host Name và Permissions
2. Trước khi chạy NetworkOpenedFiles, hãy chuyển sang máy ảo Windows 10 và điều hướng đến Z:\Evidence Files để tìm tệp Infected.pdf. Mở tệp Infected.pdf
3. Bây giờ, để chạy NetworkOpenedFiles, hãy quay lại máy ảo Windows Server 2016, điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Volatile Data Acquisition Tools\NetworkOpenedFiles và nhấp đúp vào NetworkOpenedFiles.exe
4. Cửa sổ NetworkOpenedFiles xuất hiện, hiển thị các thư mục và tệp được chia sẻ đã được truy cập, chẳng hạn như CHFI-Tools, Evidence Files và Infected.pdf, cùng với thông tin như IP Address của máy tính mà chúng đã được mở từ xa, User (tên của tài khoản người dùng) truy cập vào các thư mục và (các) tệp và Host Name của máy tính mà các thư mục và (các) tệp được liệt kê đã được mở (trong trường hợp này, phần Host Name sẽ phản ánh tên máy ảo Windows 10). Bấm đúp vào C:\CHFI-Tools\Evidence Files\Infected.pdf.
5. Cửa sổ Properties sẽ mở ra, hiển thị tất cả các chi tiết liên quan đến tệp Infected.pdf
6. Theo cách này, bạn cũng có thể xác định các tệp/thư mục khác hiện đang mở trên máy chủ.

# **Lab 2: Investigating Forensics Image of Windows RAM**

## **Task 1: Perform Malware Analysis Using Redline**

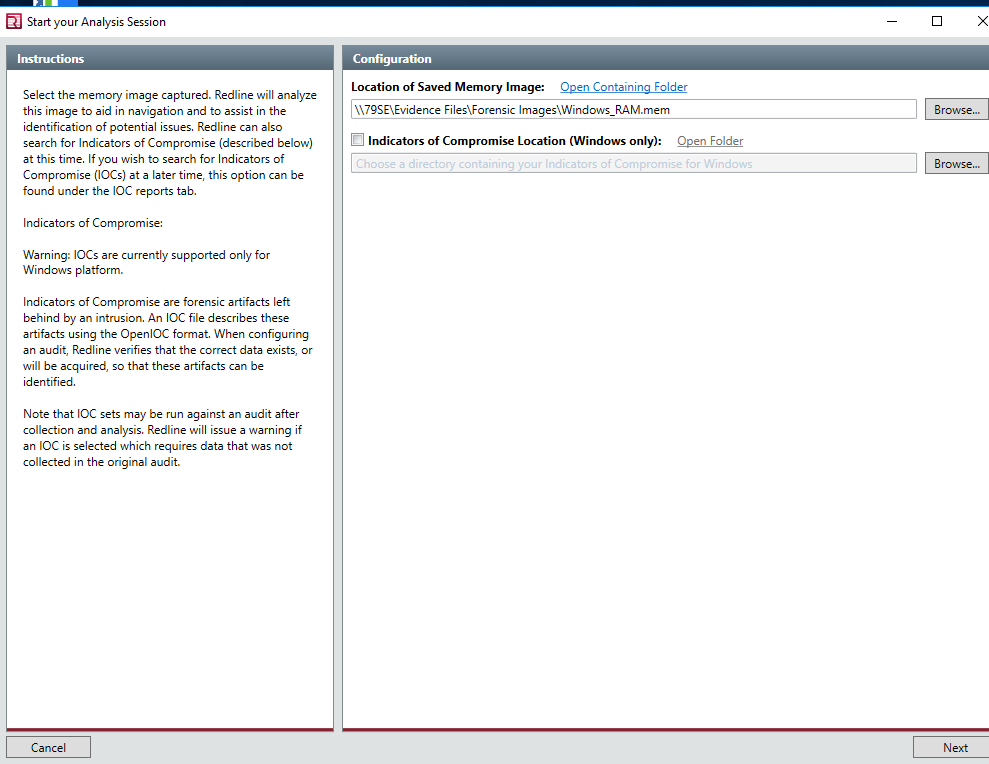
1. Đăng nhập vào máy ảo Windows Server 2016.
2. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Memory Forensics Tools\Redline, bấm đúp vào Redline-2.0.msi và làm theo các bước cài đặt hướng dẫn để cài đặt ứng dụng



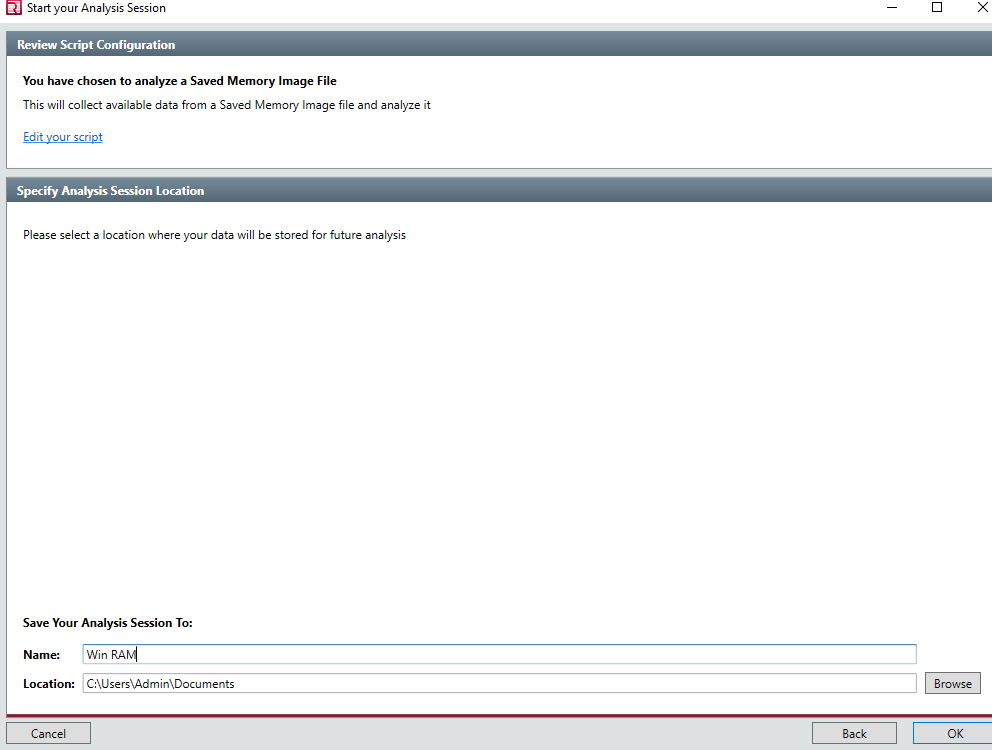
1. Sau khi hoàn tất cài đặt, nhấp vào biểu tượng Windows ở góc dưới bên trái màn hình, sau đó nhấp vào biểu tượng Redline để khởi chạy ứng dụng
2. Cửa sổ chính của công cụ Redline xuất hiện. Trong lab này, chúng ta sẽ kiểm tra một hình ảnh bộ nhớ. Vì vậy, hãy di con trỏ chuột qua phần Analyze Data và nhấp vào From a Saved Memory File



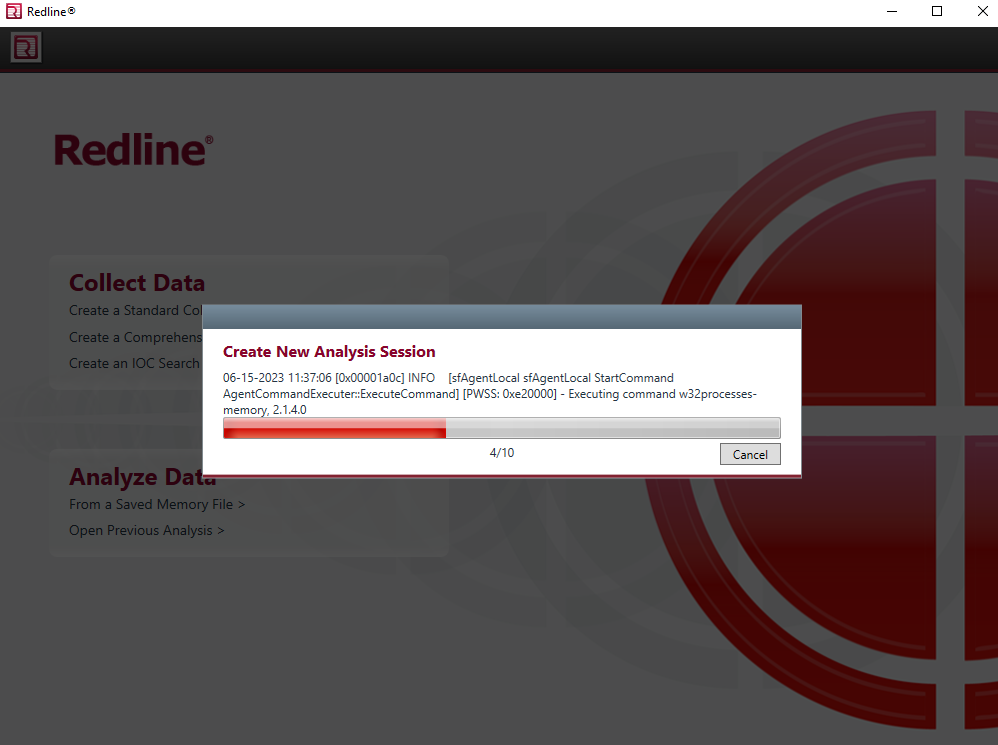
1. Cửa sổ Start your Analysis Session của bạn xuất hiện. Tại đây, bạn cần chỉ định vị trí của hình ảnh bộ nhớ mà bạn muốn kiểm tra. Vì vậy, hãy nhấp vào nút Browse



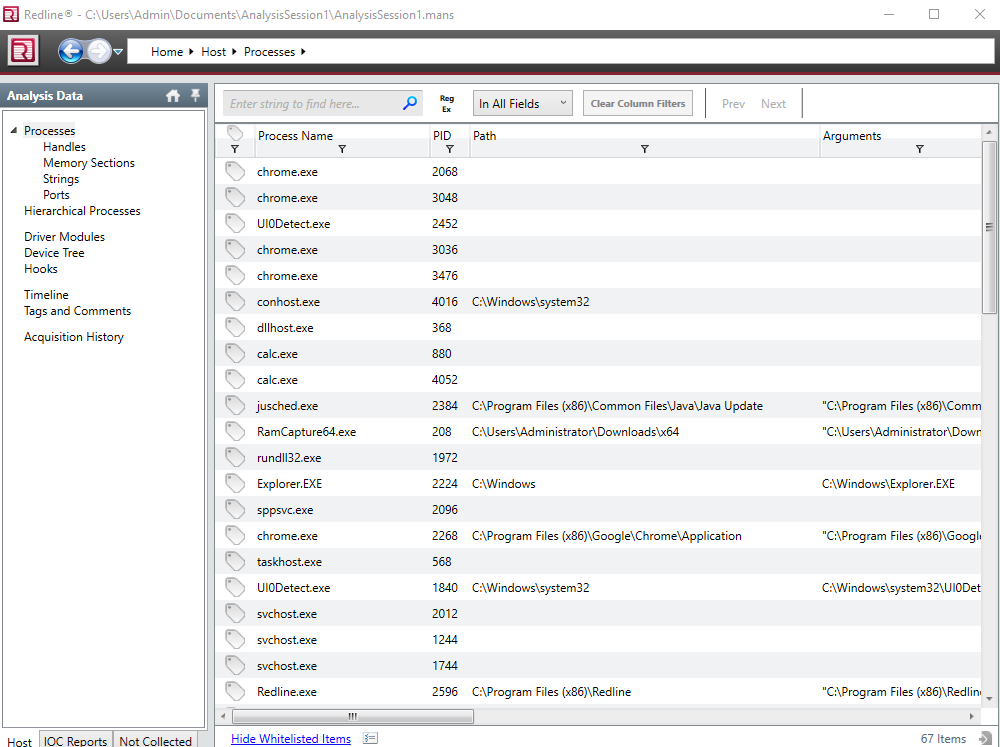
1. Cửa sổ Open xuất hiện. Điều hướng đến C:\CHFI-Tools\Evidence Files\Forensic Images, chọn All Files từ danh sách thả xuống loại tệp, chọn Windows\_RAM.mem và nhấp vào Open
2. Tệp hiện đã được thiết lập để phân tích. Bấm Next.
3. Bây giờ, bạn phải chỉ định tên cho phiên phân tích và vị trí lưu phiên. Trong lab này, chúng ta đặt tên cho phiên phân tích là Windows Ram Analysis và vị trí mặc định, ví dụ: C:\Users\Administrator\Documents.
4. Nhấn OK để tiếp tục.



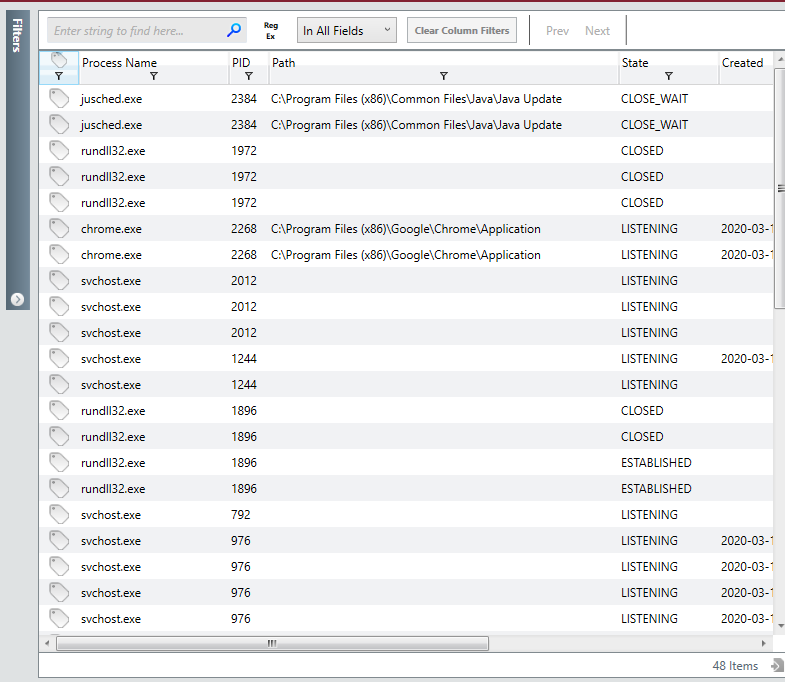
1. Redline bắt đầu phân tích tệp hình ảnh và mất khoảng 60 phút để hoàn thành quá trình phân tích



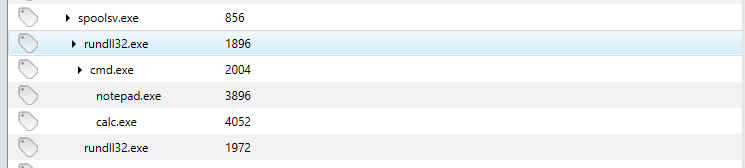
1. Sau khi tạo phiên phân tích, cửa sổ sau sẽ xuất hiện. Bấm đúp vào Processes trong khung bên trái để xem tất cả các tiến trình được ghi trên hình ảnh.
2. Redline hiển thị tất cả các tiến trình được ghi trong RAM như trong ảnh chụp màn hình sau:



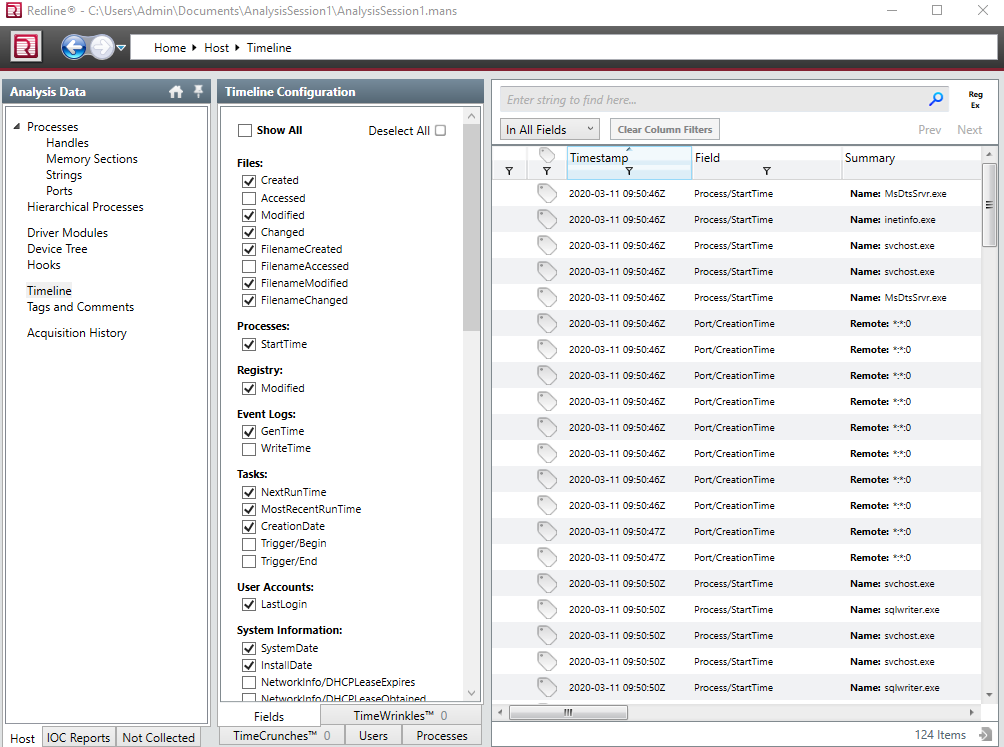
1. Kiểm tra các tiến trình có thể giúp điều tra viên xác định xem có bất kỳ tiến trình đáng ngờ nào đang chạy trên máy hay không. Tuy nhiên, nếu họ không xác định được bất kỳ tiến trình nào như vậy, họ có thể kiểm tra các kết nối mạng trên bằng chứng để xác định bất kỳ hoạt động bất thường nào.
2. Nhấp vào Ports ở khung bên trái. Phần Ports xuất hiện trong khung bên phải, hiển thị tất cả các kết nối mạng và tiến trình được liên kết với chúng. Bỏ ghim phần Filters để hiển thị rõ ràng phần Ports.
3. Kiểm tra phần Ports để tìm bất kỳ điểm bất thường nào trong mạng. Bạn sẽ quan sát thấy rằng một quá trình có tên rundll32.exe được kết nối với IP từ xa 172.20.20.21 trên cổng 4444 và kết nối đã bị đóng.
4. Cuộn xuống phần này để tìm bất kỳ kết nối bất thường nào khác. Trong khi cuộn xuống, bạn sẽ quan sát thấy rằng quá trình tương tự rundll32.exe tồn tại với PID 1896, được kết nối với IP 172.20.20.21 trên cổng 4444, nhưng trạng thái kết nối ESTABLISHED và đang hoạt động, điều này đáng ngờ.



1. Để phân tích sâu hơn, chúng ta sẽ đến phần Hierarchical Processes, nơi liệt kê các tiến trình cha và con. Nhấp vào Hierarchical Processes trong ngăn bên trái.
2. Phần Hierarchical Processes xuất hiện ở khung bên phải, hiển thị các tiến trình theo cấu trúc phân cấp, như minh họa trong ảnh chụp màn hình sau:



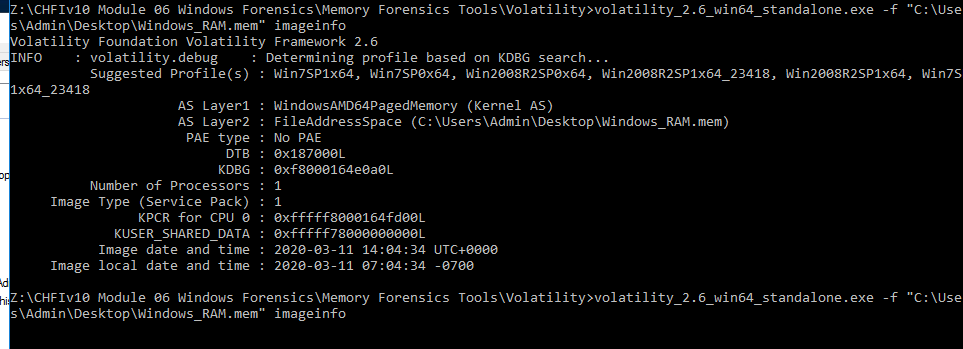
1. Ảnh chụp màn hình ở trên cho thấy tiến trình rundll32.exe mà chúng tôi đã xác định trong các bước trước đó có tiến trình mẹ spoolsv.exe và tiến trình con cmd.exe. Từ tiến trình con cmd.exe, hai tiến trình đã được thực hiện: notepad.exe và calc.exe.
2. Phát hiện trên chỉ ra rằng tiến trình spoolsv.exe đã bị xâm nhập, dẫn đến việc tạo ra các tiến trình con rundll32.exe và cmd.exe. Các tiến trình notepad.exe và calc.exe sau đó được thực thi từ cmd.exe, tương ứng với Command Prompt.
3. Để xem dòng thời gian của các sự kiện được ghi trên RAM, hãy nhấp vào Timeline ở khung bên trái. Thao tác này sẽ hiển thị dòng thời gian của các hoạt động, như được hiển thị trong ảnh chụp màn hình sau:



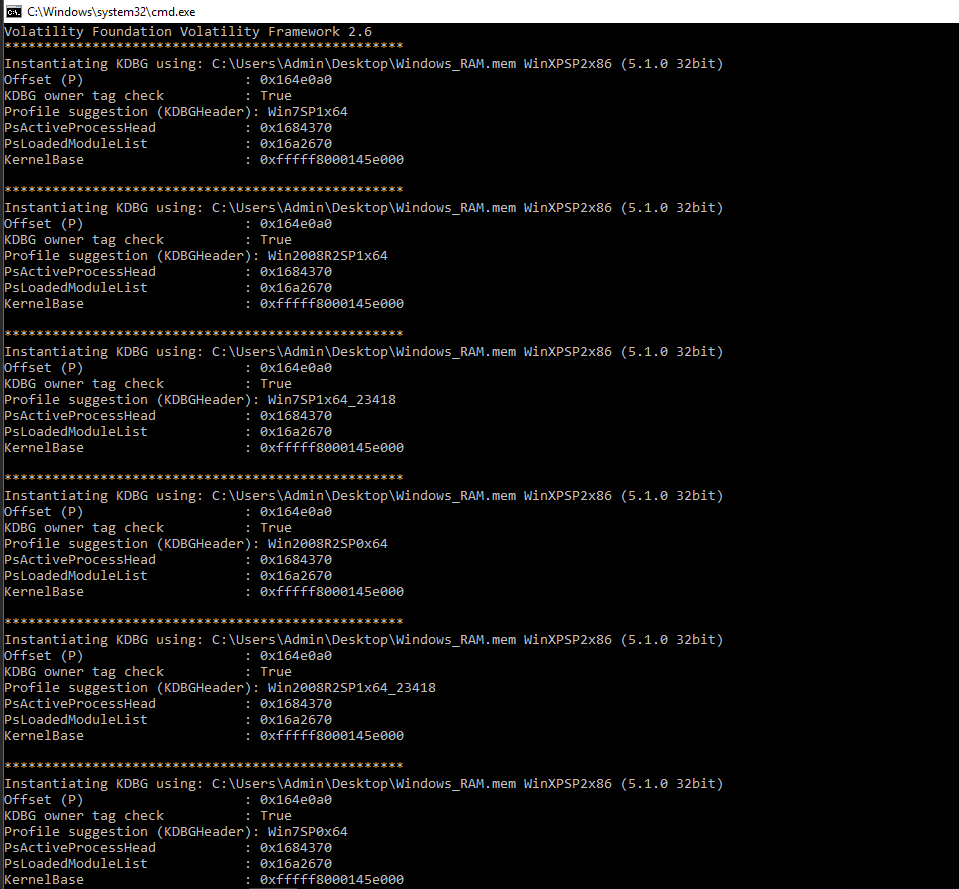
1. Đóng ứng dụng

## **Task 2: Perform RAM Analysis Using Volatility Framework**

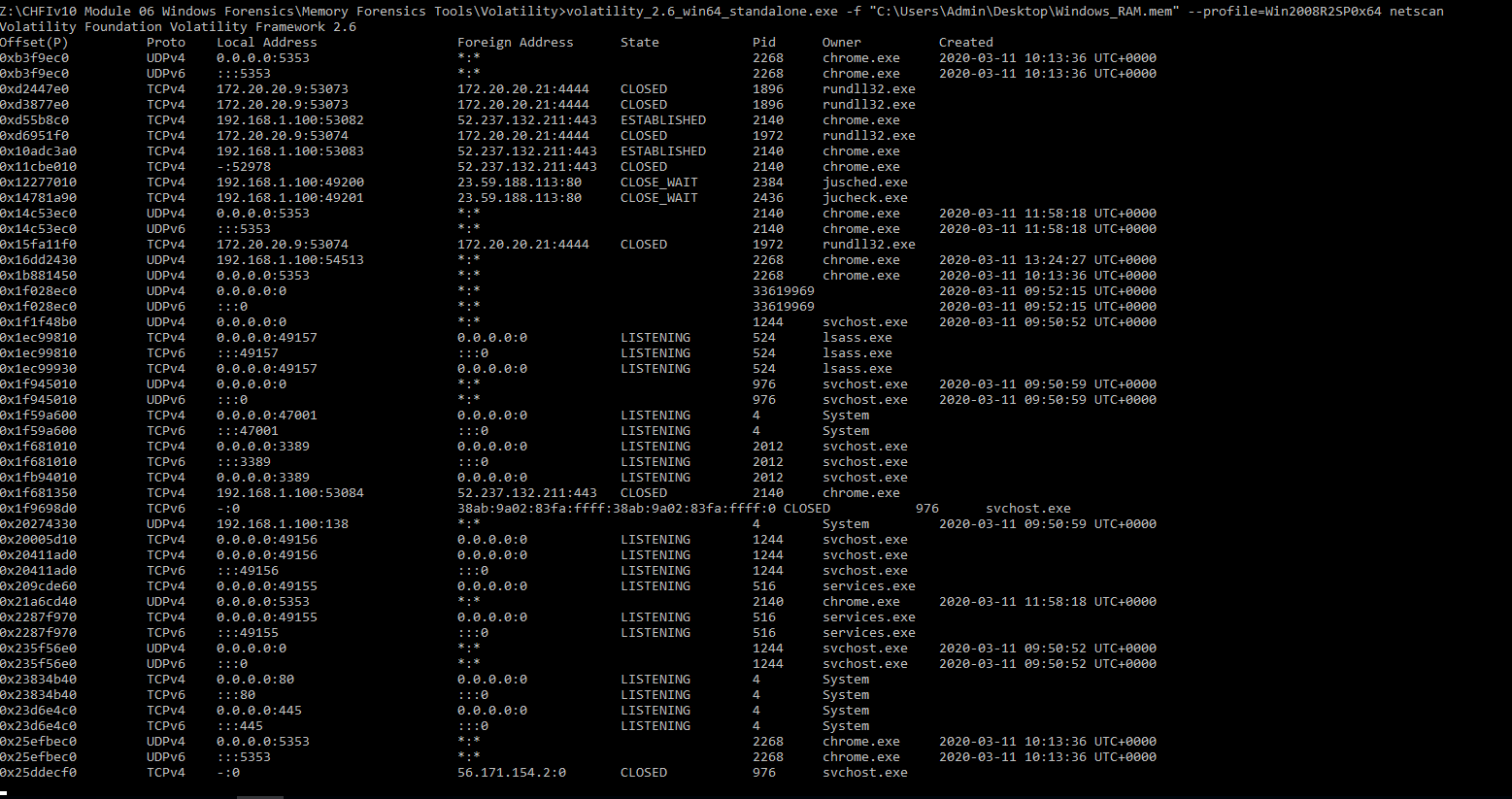
1. Bây giờ, chúng ta sẽ phân tích hình ảnh bằng Volatility framework.
2. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Memory Forensics Tools, chọn thư mục Volatility, giữ phím Shift và nhấp chuột phải vào thư mục đã chọn.
3. Chọn Open command window here từ menu ngữ cảnh.
4. Command Prompt xuất hiện với đường dẫn được đặt thành C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Memory Forensics Tools\Volatility. Trong lab này, chúng tôi sẽ phân tích Windows\_RAM.mem có tại C:\CHFI-Tools\Evidence Files\Forensic Images.
5. Nhiệm vụ đầu tiên của chúng tôi là lấy thông tin về hình ảnh. Plugin imageinfo của Volatility giúp truy xuất thông tin này. Vì vậy, hãy nhập Volity\_2.6\_win64\_standalone.exe -f "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows\_RAM.mem" imageinfo trong Command Prompt và nhấn Enter
6. Volatility phân tích tệp hình ảnh và hiển thị thông tin của nó như trong ảnh chụp màn hình sau:



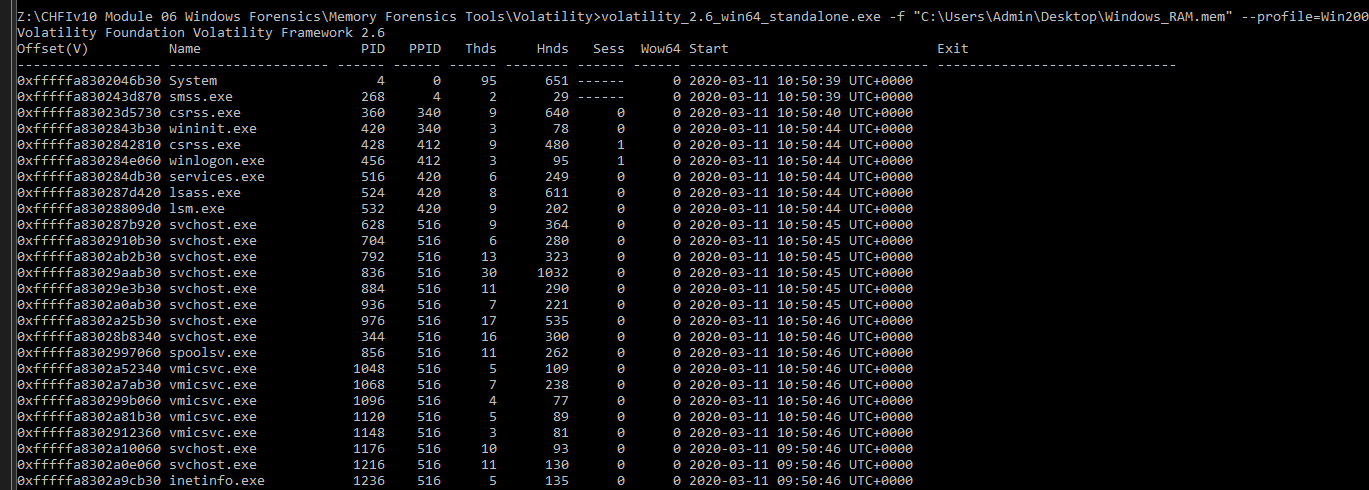
1. Ngoài ra, bạn có thể sử dụng plugin kdbgscan để quét trình gỡ lỗi kernel và liệt kê các cấu hình được đề xuất. Để sử dụng plugin, hãy nhập Volatility\_2.6\_win64\_standalone.exe -f "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows\_RAM.mem" kdbgscan trong Command Promptvà nhấn Enter. Volatility phân tích tiêu đề kdbg và liệt kê các cấu hình có thể, như trong ảnh chụp màn hình:



1. Volatility hiển thị danh sách các hồ sơ được đề xuất. Chúng ta phải chọn một cấu hình từ danh sách có thể gần giống với cấu hình trên RAM. Trong lab này, chúng tôi sẽ chọn Win2008R2SP0x64.
2. Vì chúng tôi đã tìm thấy một cấu hình phù hợp, bây giờ chúng tôi sẽ xem các kết nối mạng được liên kết với máy được ghi lại trong hình ảnh. Để xem các kết nối mạng, Volatility\_2.6\_win64\_standalone.exe Files\Forensic gõ lệnh Images\Windows\_RAM.mem" -f "C:\CHFI-Tools\Evidence --profile=Win2008R2SP0x64 netscan trong Command Prompt và nhấn Enter.



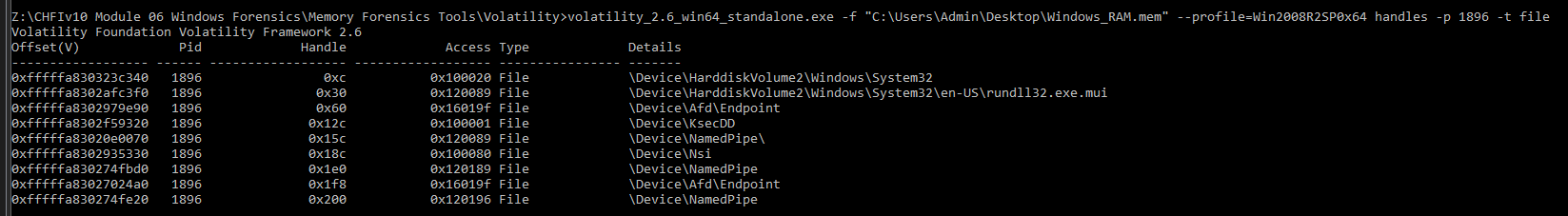
1. Ảnh chụp màn hình ở trên cho thấy một tiến trình có tên rundll32.exe đã thiết lập kết nối mạng với máy nghi ngờ, nhưng kết nối đã bị đóng. Các PID cho tiến trình là 1972 và 1896. Bây giờ chúng ta sẽ xem liệu có bất kỳ kết nối đang hoạt động nào với cùng một tiến trình hay không.
2. Cuộn xuống cửa sổ Command Promptđể phát hiện bất kỳ kết nối đang hoạt động nào với rundll32.exe. Chúng ta có thể quan sát một kết nối đang hoạt động bằng rundll32.exe với PID 1896, như trong ảnh chụp màn hình sau
3. Từ ảnh chụp màn hình ở trên, có thể suy ra rằng quá trình rundll32.exe đã được bắt đầu nhiều lần. Trong khi kết nối liên quan đến PID 1972 bị đóng, kết nối với PID 1896 đang hoạt động. Dựa trên thông tin này, chúng tôi sẽ tiến hành điều tra thêm.
4. Bạn có thể quan sát tiến trình tương tự trong danh sách tiến trình bằng cách đưa ra lệnh sau: Volatility\_2.6\_win64\_standalone.exe -f "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows\_RAM.mem" profile=Win2008R2SP0x64 pslist.
5. Volatility liệt kê tất cả các tiến trình như trong ảnh chụp màn hình sau



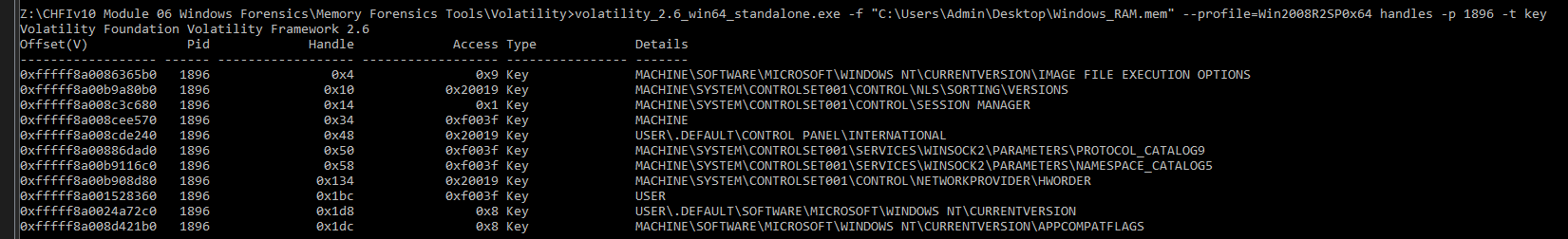
1. Cuộn xuống danh sách để tìm tiến trình rundll32.exe, được quan sát thấy trong các kết nối mạng được liệt kê trước đó



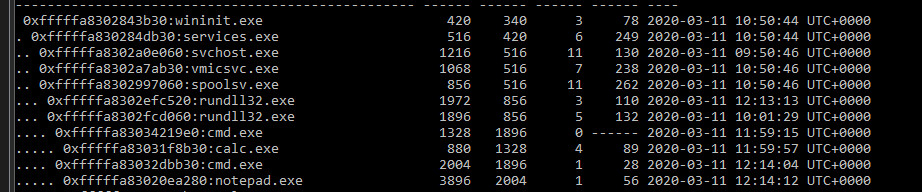
1. Dựa trên tiến trình, bây giờ bạn có thể liệt kê các tệp và sổ đăng ký được sử dụng bởi nó. Để xem các tệp được sử dụng bởi tiến trình , hãy nhập Volity\_2.6\_win64\_standalone.exe -f "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows\_RAM.mem" --profile=Win2008R2SP0x64 handle -p 1896 -t file và nhấn Enter



1. Để xem các sổ đăng ký được liên kết với tiến trình, hãy nhập Volatility\_2.6\_win64\_standalone.exe -f "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows\_RAM.mem" --profile=Win2008R2SP0x64 handle -p 1896 -t key và bấm phím Enter.



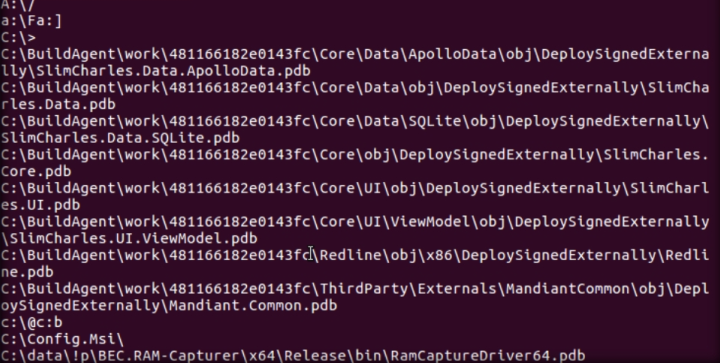
1. Để liệt kê cây tiến trình chứa tiến trình rundll32.exe, hãy nhập Volatility\_2.6\_win64\_standalone.exe -f "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows\_RAM.mem" --profile=Win2008R2SP0x64 pstree.
2. Điều này liệt kê cây tiến trình liên quan đến rundll32.exe, như thể hiện trong ảnh chụp màn hình sau:



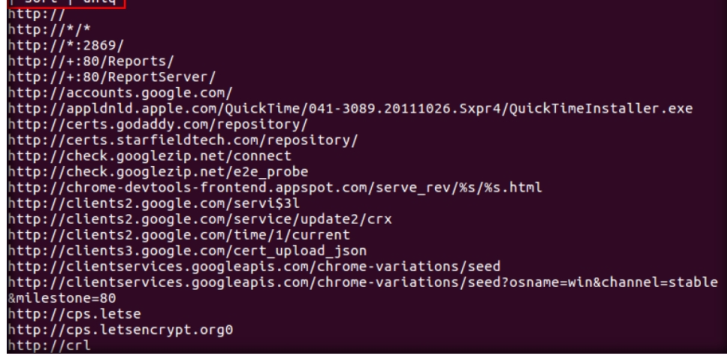
1. Trong ảnh chụp màn hình ở trên, 1 biểu thị luồng tiến trình đầu tiên và 2 biểu thị luồng thứ hai.
2. Trong 1, chúng ta có thể quan sát dòng tiến trình dưới dạng spoolsv.exe -> rundll32.exe -> rundll32.exe -> cmd.exe -> calc.exe. Tiến trình rundll32.exe đầu tiên (PID: 1972) bị đóng, trong khi tiến trình rundll32.exe thứ hai (PID: 1896) bắt đầu sau đó, với dòng tiến trình sau: spoolsv.exe -> rundll32.exe -> cmd.exe -> (notepad.exe và calc.exe đều có nguồn gốc từ cmd.exe).
3. Điều này chỉ ra rằng tiến trình rundll32.exe bắt nguồn từ tiến trình spoolsv.exe và đến lượt nó, tạo ra một tiến trình con có tên cmd.exe, từ đó máy tính và notepad được khởi tạo.
4. Theo cách này, chúng ta có thể sử dụng Volatility để kiểm tra ảnh RAM. Ngoài các plugin được trình bày trong các bước trên, bạn có thể sử dụng các plugin như malfind, arp, ifconfig và lsof để thu thập thông tin bổ sung

## **Task 3: Examine RAM Dump Using Strings**

1. Hình ảnh RAM cũng có thể được kiểm tra bằng cách sử dụng tiện ích dòng lệnh chuỗi trong Ubuntu. Tiện ích này giúp bạn lấy thông tin chẳng hạn như tệp/thư mục nằm trên máy cũng như URL và IP được lưu trữ trên đĩa, có thể giúp điều tra viên xác định thông tin có giá trị.
2. Đăng nhập vào máy ảo Ubuntu Forensics.
3. Nhấp vào biểu tượng Tệp trong bảng Trình khởi chạy để khởi chạy Trình quản lý tệp
4. Cửa sổ File Manager xuất hiện, trỏ đến thư mục Home. Nhấp vào chfi-tools đã đánh dấu trên thư mục 10.0.0.16.
5. Thư mục CHFI-Tools xuất hiện trong cửa sổ, như trong ảnh chụp màn hình sau:
6. Bây giờ, hãy vào Evidence Files Forensic Images. Bạn sẽ có thể xem tệp Windows\_RAM.mem trong hình ảnh. Sao chép tập tin này.
7. Điều hướng đến thư mục Home và dán tệp.
8. Bây giờ, hãy nhấp vào biểu tượng Terminal từ bảng khởi chạy để khởi chạy terminal dòng lệnh.
9. Khởi chạy thiết bị đầu cuối dòng lệnh. Bạn cần có quyền root trong thiết bị đầu cuối để cài đặt ứng dụng.
10. Vì vậy, hãy gõ sudo su và nhấn Enter. Bạn sẽ được nhắc nhập mật khẩu. Nhập toor làm mật khẩu và nhấn Enter.
11. Bây giờ, bạn sẽ vào thiết bị đầu cuối gốc, như thể hiện trong ảnh chụp màn hình sau
12. Để liệt kê tất cả các tập tin và thư mục, gõ chuỗi Windows\_RAM.mem | grep -i "^[az]:\\\\" | sắp xếp | uniq và nhấn Enter.
13. Điều này sẽ hiển thị tất cả các tệp và thư mục được lưu trữ trên máy nghi ngờ, như trong ảnh chụp màn hình sau



1. Chúng ta phải kiểm tra đầu ra để xem có bất kỳ tệp đáng ngờ nào được tìm thấy trên máy không.
2. Để trích xuất tất cả các URL được lưu trữ trong máy nghi ngờ, hãy nhập lệnh: strings Windows\_RAM.mem | egrep "^https?://" | sắp xếp | duy nhất
3. Lệnh liệt kê tất cả các URL đã truy cập trong đầu ra của nó, như thể hiện trong ảnh chụp màn hình



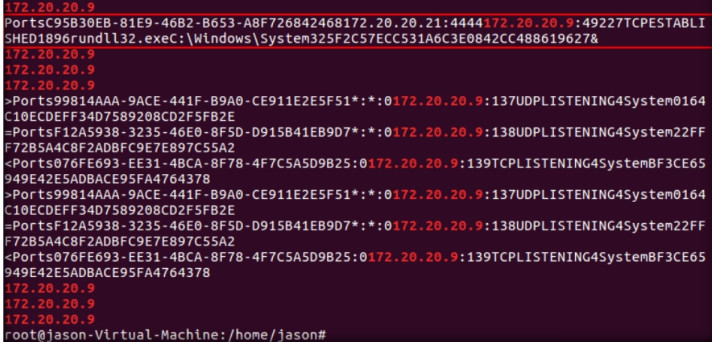
1. Chúng tôi phải kiểm tra đầu ra để xác định sự hiện diện của bất kỳ URL đáng ngờ nào trên máy.
2. Kiểm tra địa chỉ IP có thể giúp chúng tôi xác định xem có bất kỳ kết nối độc hại nào được liên kết với máy hay không. Để xem địa chỉ IP, gõ chuỗi Windows\_RAM.mem | egrep -oE '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3} ' và nhấn Enter.
3. Lệnh Strings trích xuất tất cả các mục được liên kết với địa chỉ IP và các mục bổ sung có định dạng địa chỉ IP, ví dụ: [octet.octet.octet.octet], như minh họa trong ảnh chụp màn hình sau:



1. Cuộn xuống kết quả để tìm bất kỳ mục nhập địa chỉ IP hợp pháp nào được ghi trên hình ảnh.



1. Nếu bạn tìm thấy một mục có thể tiết lộ thông tin liên quan đến cuộc điều tra, bạn có thể sử dụng lệnh strings để xem thông tin đó.
2. Trong bài lab này, chúng ta sẽ sử dụng địa chỉ IP của máy (trong trường hợp này là 172.20.20.9) để lọc dữ liệu chứa địa chỉ này. Vì vậy, hãy gõ chuỗi Windows\_RAM.mem | ví dụ: "172.20.20.9" và nhấn Enter. Điều này kiểm tra hình ảnh để lọc tất cả các mục có chứa địa chỉ IP như trong ảnh chụp màn hình sau

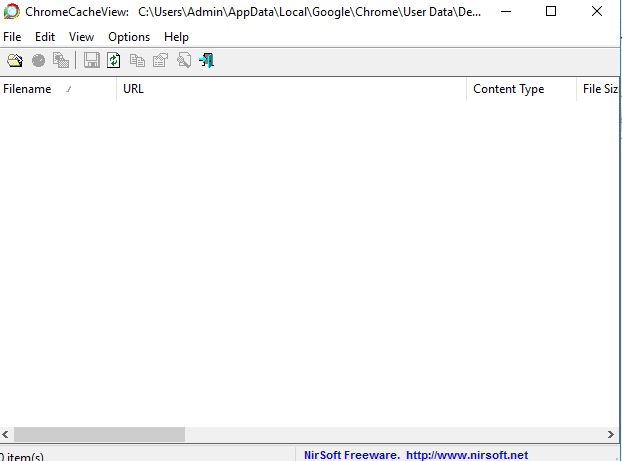


1. Giải mã mục trên cho thấy kết nối mạng đã được thiết lập với máy đang được điều tra, tức là 172.20.20.9 từ 172.20.20.21 qua cổng số. 4444. Quá trình liên kết với kết nối là rundll32.exe nằm trong C:\Windows\System32.
2. Theo cách này, hình ảnh RAM đóng vai trò là bằng chứng quan trọng để khám phá dữ liệu quan trọng trong quá trình điều tra

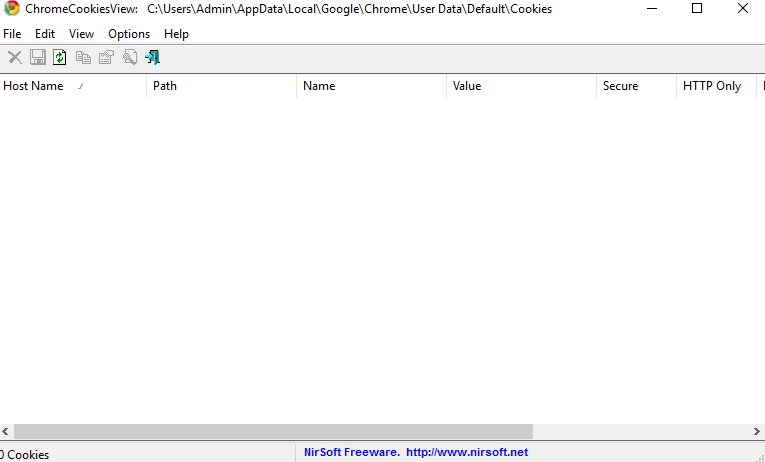
# **Lab 3: Examining Web Browser Aritfacts**

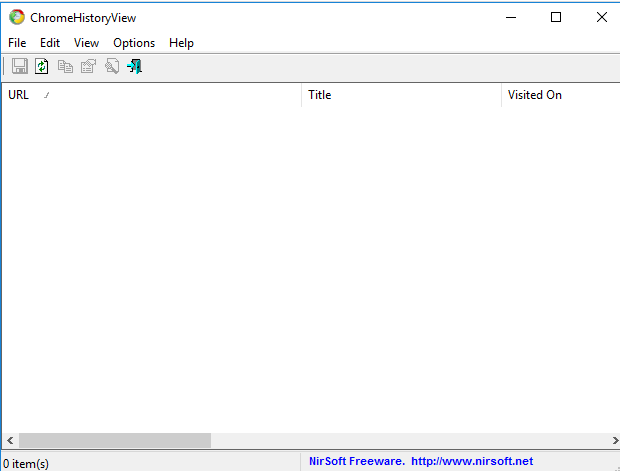
## **Task 1: Retrieving Artifacts from Google Chrome**

1. Đăng nhập vào máy ảo Windows Server 2016
2. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Browser Analysis Tools\Google Chrome.
3. Trong thư mục Google Chrome, bạn sẽ tìm thấy các thư mục dành cho ba công cụ: ChromeCacheView, ChromeHistoryView và ChromeCookiesView.
4. Trước tiên, hãy mở thư mục công cụ ChromeCacheView và khởi chạy ChromeCacheView.exe.
5. Công cụ hiển thị các thông tin như Tên tệp, URL, Loại nội dung, Kích thước tệp, Truy cập lần cuối, Thời gian hết hạn, Thời gian máy chủ, Tên máy chủ, Phản hồi của máy chủ và Địa chỉ IP của máy chủ.



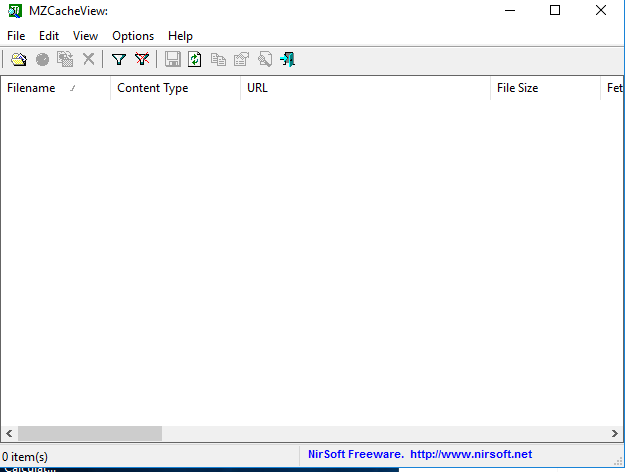
1. Bây giờ, hãy đóng cửa sổ ChromeCacheView, điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Browser Analysis Tools\Google Chrome\ChromeCookiesView và khởi chạy ChromeCookiesView.exe.
2. Công cụ hiển thị các thông tin như Tên máy chủ, Đường dẫn, Tên, Giá trị, Bảo mật, Chỉ HTTP, Truy cập lần cuối, v.v. cho mỗi trang web đã truy cập



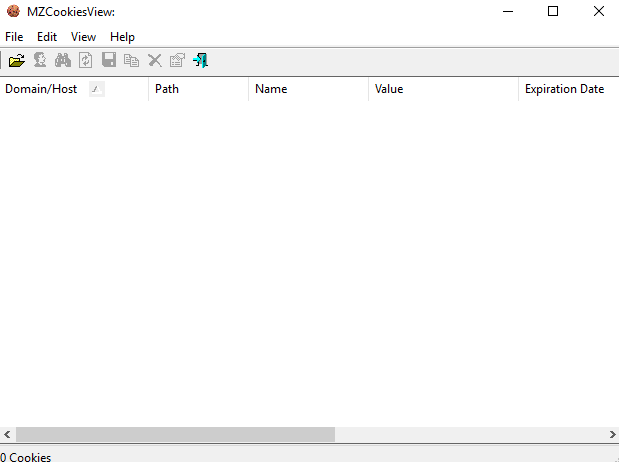
1. Bây giờ, hãy đóng cửa sổ ChromeCookiesView, điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Browser Analysis Tools\Google Chrome\ChromeHistoryView và khởi chạy ChromeHistoryView.exe.
2. ChromeHistoryView hiển thị các thông tin như URL, Tiêu đề, Ngày truy cập, Số lượt truy cập, ID truy cập, Tệp lịch sử, v.v. cho mỗi cookie.
3. Theo cách này, bạn có thể xem các tạo phẩm của trình duyệt Chrome để phát hiện bất kỳ mục đáng ngờ nào trong lịch sử duyệt web.

## **Task 2: Retrieving Artifacts from Mozilla Firefox**

1. Tương tự, chúng tôi sẽ trích xuất các tạo phẩm của trình duyệt Firefox.
2. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Browser Analysis Tools\Mozilla Firefox.
3. Trong thư mục Mozilla Firefox, bạn sẽ tìm thấy các thư mục dành cho ba công cụ: MZCacheView, MZHistoryView và MZCookiesView.
4. Đầu tiên, mở thư mục MZCacheView và khởi chạy MZCacheView.exe.
5. MZCacheView hiển thị các thông tin như Tên tệp, Loại nội dung, URL, Kích thước tệp, Số lần tìm nạp, Sửa đổi lần cuối, Đã tìm nạp lần cuối, Thời gian hết hạn, Tên máy chủ, Phản hồi của máy chủ, Thời gian máy chủ, Mã hóa nội dung, Tên bộ đệm, Tệp bị thiếu, Kiểm soát bộ đệm, v.v. cho mỗi tệp bộ đệm.



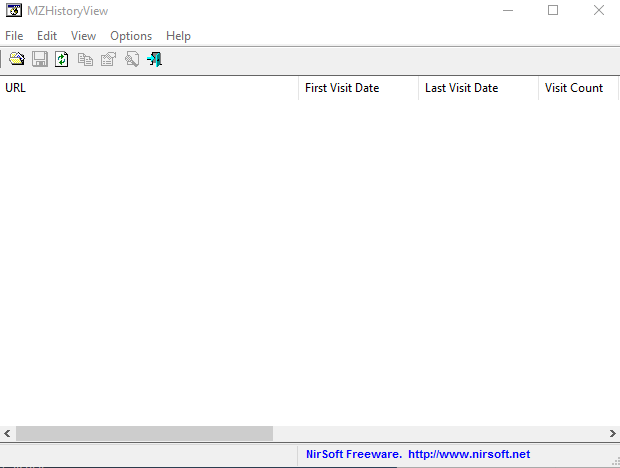
1. Đóng cửa sổ MZCacheView. Bây giờ, điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Browser Analysis Tools\Mozilla Firefox\MZCookiesView và khởi chạy mzcv.exe.
2. Khi khởi chạy, cửa sổ ứng dụng MZCookiesView sẽ xuất hiện, hiển thị danh sách tất cả các cookie đã được tạo bởi các lượt truy cập của người dùng vào các trang web khác nhau. Nó cũng sẽ hiển thị các thông tin như Tên miền/Máy chủ, Đường dẫn, Tên, Giá trị, Ngày hết hạn, Bảo mật (Có/Không), Truy cập lần cuối, Thời gian tạo, v.v. cho mỗi cookie.



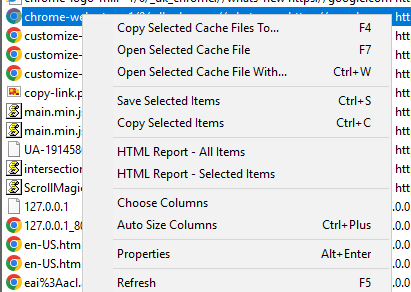
1. Bây giờ, hãy đóng cửa sổ MZCookiesView, điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Browser Analysis Tools\Mozilla Firefox\MZHistoryView và khởi chạy MozillaHistoryView.exe.
2. Khi khởi chạy MZHistoryView.exe, trước tiên, ứng dụng sẽ mở cửa sổ Chọn tên tệp lịch sử. Trong cửa sổ này, bạn sẽ thấy đường dẫn thư mục mặc định được cung cấp trong trường đối với nút dấu chấm lửng. Để đường dẫn thư mục được đặt thành mặc định. Tất cả các tùy chọn khác được bỏ chọn theo mặc định. Để các tùy chọn được đặt thành mặc định và sau đó nhấp vào OK, như thể hiện trong ảnh chụp màn hình



1. Lúc này, cửa sổ ứng dụng chính sẽ xuất hiện, hiển thị các thông tin như URL, Ngày truy cập đầu tiên, Ngày truy cập lần cuối, Số lượt truy cập, Người giới thiệu, Tiêu đề, Loại lượt truy cập, v.v. cho mỗi trang web đã truy cập, như minh họa trong ảnh chụp màn hình



1. Theo cách này, bạn có thể xem các tạo phẩm của trình duyệt Mozilla Firefox để phát hiện bất kỳ mục đáng ngờ nào trong lịch sử duyệt web
2. Để lưu các thành phần lạ liên quan đến bất kỳ trình duyệt nào, bất kể chúng là tệp bộ đệm, tệp lịch sử duyệt web hay cookie, hãy chọn các mục chứa dữ liệu bằng chứng, nhấp chuột phải, sau đó chọn tùy chọn Lưu các mục đã chọn từ menu ngữ cảnh.



1. Cửa sổ Chọn tên tệp để lưu sẽ xuất hiện, hiển thị vị trí mặc định nơi tệp sẽ được lưu. Vị trí mặc định sẽ là thư mục công cụ tương ứng trong C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Browser Analysis Tools. Bạn cũng có thể chọn một vị trí khác để lưu tệp. Trong cửa sổ Select a filename to save, tùy theo yêu cầu của bạn mà đặt tên cho file (ở đây là Mozilla Browsing History) để lưu rồi nhấn Save. Tệp sẽ được lưu vào vị trí mặc định/đã chọn dưới dạng tệp .txt.



1. Theo cách này, bạn có thể xem các tạo phẩm của trình duyệt để phát hiện bất kỳ mục đáng ngờ nào trong lịch sử duyệt web trong quá trình điều tra.

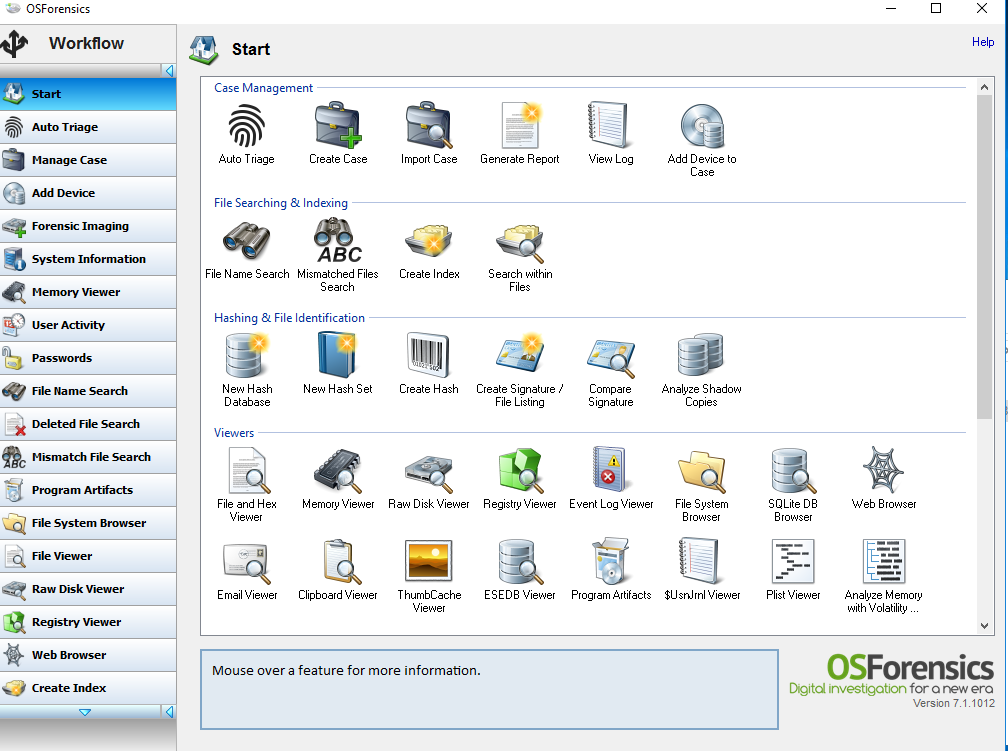
# **Lab 4: Discovering and Extracting Forensic Data from Computers**

## **Task 1: Creating a New Case**

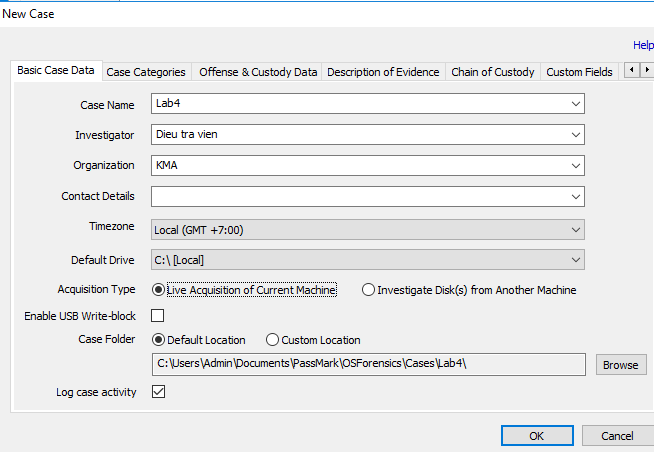
1. Đăng nhập vào máy ảo Windows Server 2016.
2. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Windows Forensics Tools\OSForensics, bấm đúp vào osf.exe để khởi chạy thiết lập và làm theo hướng dẫn cài đặt theo trình hướng dẫn để hoàn tất cài đặt công cụ
3. Trong bước cài đặt cuối cùng, hãy đánh dấu vào tùy chọn Khởi chạy OSForensics và nhấp vào Kết thúc.
4. OSForensics GUI xuất hiện cùng với cửa sổ bật lên PassMark OSForensics. Trong cửa sổ bật lên, nhấp vào Tiếp tục sử dụng Phiên bản dùng thử.



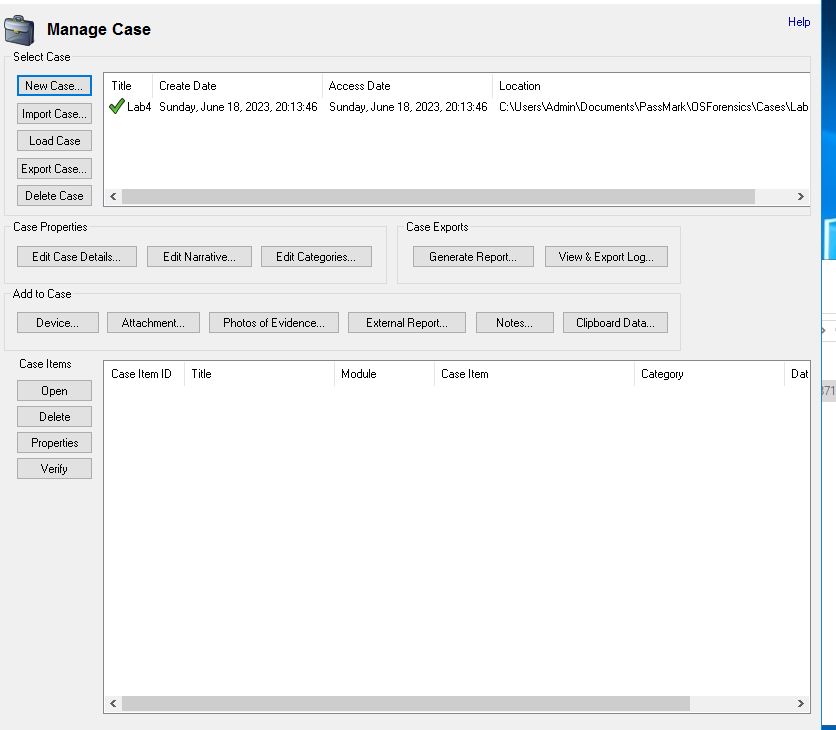
1. Nhiệm vụ đầu tiên của chúng ta là tạo một trường hợp bằng công cụ này. Nhấp vào biểu tượng Tạo trường hợp trong cửa sổ chính của công cụ để tạo trường hợp mới



1. Cửa sổ Trường hợp mới xuất hiện; điền vào các trường bắt buộc trong cửa sổ. Đảm bảo rằng bạn chọn nút radio cho tùy chọn Thu nhận trực tiếp máy hiện tại trong danh mục Loại thu nhận. Bạn có thể chọn lưu thư mục trường hợp mới ở vị trí Mặc định hoặc Tùy chỉnh. Nhấp vào OK.

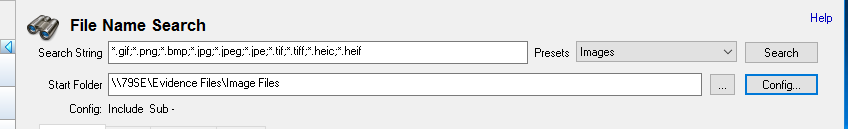


1. Một trường hợp mới được tạo như trong ảnh chụp màn hình bên dưới

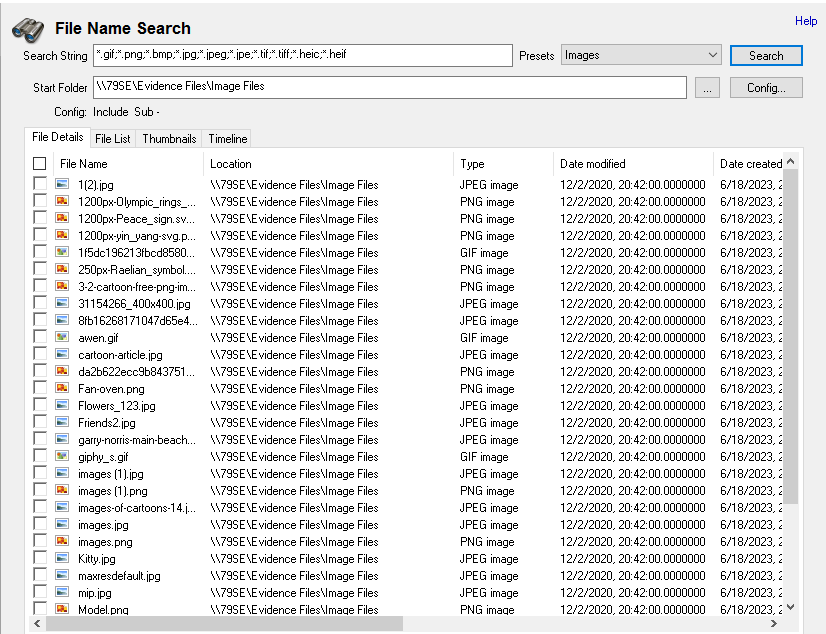


## **Task 2: File Name Search**

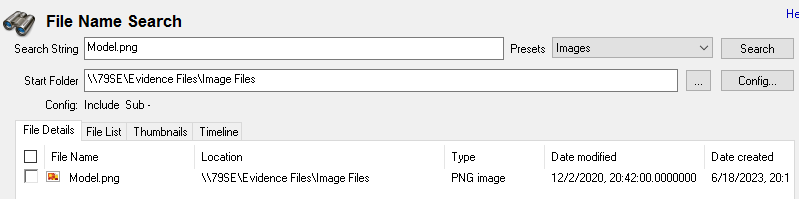
1. Công cụ OSForensics có thể giúp điều tra viên tìm kiếm và định vị các tệp trên hệ thống. Để bắt đầu tìm kiếm tệp, hãy nhấp vào Tìm kiếm tên tệp trong ngăn bên trái của cửa sổ.
2. Để xác định vị trí tệp, nhập tên tệp hoặc phần mở rộng của nó vào trường Chuỗi tìm kiếm bên dưới phần Tìm kiếm tên tệp. Ngoài ra, bạn có thể chọn loại tệp từ danh sách thả xuống Cài đặt sẵn.
3. Trong lab này, chúng tôi sẽ tìm kiếm các tệp hình ảnh. Vì vậy, hãy chọn tùy chọn Hình ảnh từ danh sách thả xuống Cài đặt sẵn.
4. Trong trường Start Folder, chỉ định đường dẫn để tìm kiếm tệp hình ảnh bằng cách nhấp vào nút dấu chấm lửng và chọn vị trí (ở đây, chúng tôi chỉ định vị trí C:\CHFI-Tools\Evidence Files\Image Files để tìm kiếm hình ảnh trong Nó). Sau đó, nhấp vào nút Tìm kiếm



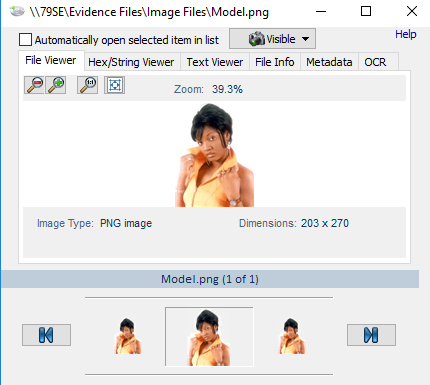
1. Phần Tìm kiếm tên tệp hiện hiển thị danh sách các tệp có trong vị trí đã chọn, như thể hiện trong ảnh chụp màn hình bên dưới. Theo mặc định, công cụ hiển thị các tệp này trong tab Chi tiết tệp. Bạn cũng có thể xem danh sách các tệp này trong tab Danh sách tệp và Hình thu nhỏ bằng cách nhấp vào chúng.



1. Ngoài ra, nếu bạn chỉ muốn tìm kiếm một hình ảnh duy nhất trên toàn bộ hệ thống, hãy chọn Hình ảnh từ menu thả xuống Cài đặt sẵn, nhập tên của tệp hình ảnh mong muốn vào trường Chuỗi tìm kiếm, sau đó nhấp vào Tìm kiếm, như minh họa trong ảnh chụp màn hình bên dưới. Ở đây, chúng tôi đang tìm kiếm tệp hình ảnh JPEG có tên Kitty.



1. Công cụ sẽ tìm kiếm tệp hình ảnh được chỉ định và hiển thị kết quả tìm kiếm trong phần Tìm kiếm tên tệp trong tab Chi tiết tệp. Kết quả tìm kiếm sẽ được hiển thị cùng với đường dẫn/vị trí lưu trữ tệp tìm kiếm.
2. Để xem ảnh, nhấp đúp vào ảnh. Công cụ sẽ hiển thị hình ảnh thông qua cửa sổ bật lên, như trong ảnh chụp màn hình sau

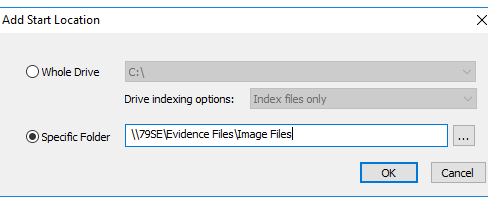


## **Task 3: Creating Index**

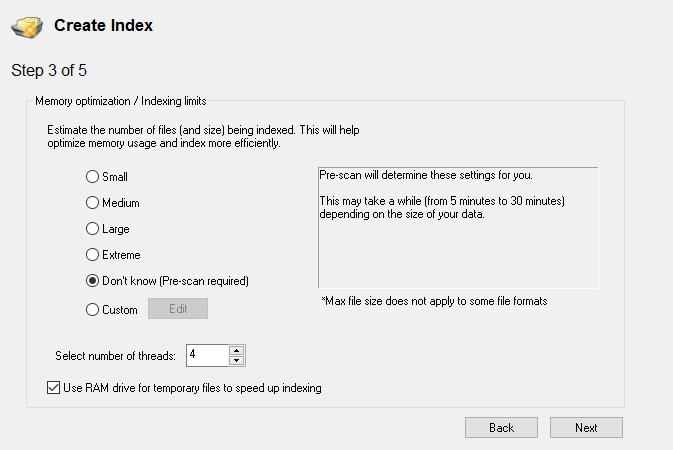
1. Bây giờ chúng ta sẽ tiến hành nhiệm vụ tạo chỉ mục cho các tệp. Ở đây, chúng tôi chứng minh việc tạo chỉ mục cho các tệp hình ảnh. Tạo một chỉ mục các tệp giúp các nhà điều tra đẩy nhanh quá trình tìm kiếm tệp của họ.
2. Để bắt đầu tạo chỉ mục cho các tệp, nhấp vào Tạo chỉ mục trong ngăn bên trái của cửa sổ công cụ.
3. Phần Tạo chỉ mục xuất hiện ở khung bên phải. Trong phần này, chọn tùy chọn Sử dụng các loại tệp được xác định trước để tạo chỉ mục và kiểm tra các tùy chọn bắt buộc được liệt kê bên dưới để chọn loại tệp mà bạn muốn lập chỉ mục (ở đây, chúng tôi đã chọn tùy chọn Hình ảnh). Sau đó, nhấp vào Tiếp theo



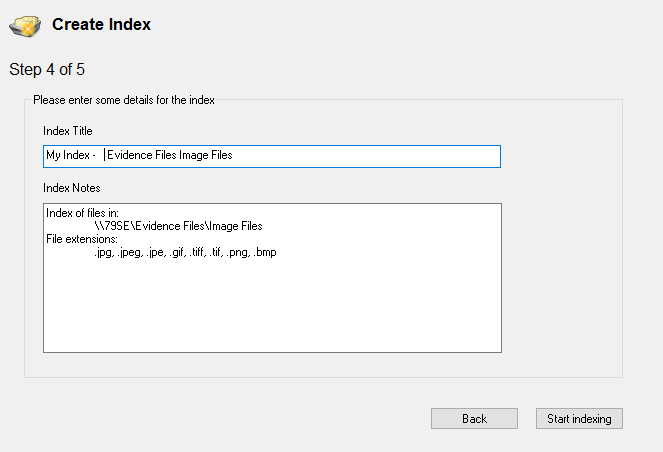
1. Bây giờ, hãy nhấp vào nút Thêm để chọn ổ đĩa đích hoặc thư mục chứa các tệp mà bạn muốn lập chỉ mục được lưu trữ
2. Khi bạn nhấp vào nút Thêm, cửa sổ bật lên Thêm vị trí bắt đầu xuất hiện. Từ cửa sổ bật lên này, chọn nút radio Thư mục cụ thể và nhấp vào nút dấu chấm lửng để cung cấp đường dẫn đến thư mục đích. Đối với lab này, hãy chọn thư mục C:\CHFI-Tools\Evidence Files\Image Files và nhấp vào nút OK.



1. Thư mục Bắt đầu hiện đã được định cấu hình. Bấm tiếp.
2. Trong Bước 3 của trình hướng dẫn, chọn tùy chọn Không biết (Yêu cầu quét trước), đảm bảo rằng tùy chọn Sử dụng ổ đĩa RAM cho các tệp tạm thời để tăng tốc độ lập chỉ mục được chọn và nhấp vào Tiếp theo



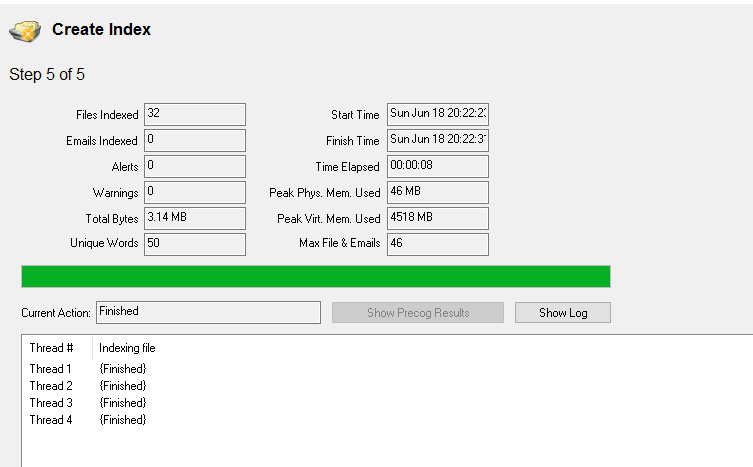
1. Trong Bước 4 của trình hướng dẫn, hãy chỉ định Tiêu đề Chỉ mục (ở đây, chúng tôi đã chỉ định Tiêu đề Chỉ mục là Trường hợp 75), nhập Ghi chú Chỉ mục (tùy chọn), sau đó bấm Bắt đầu Lập chỉ mục



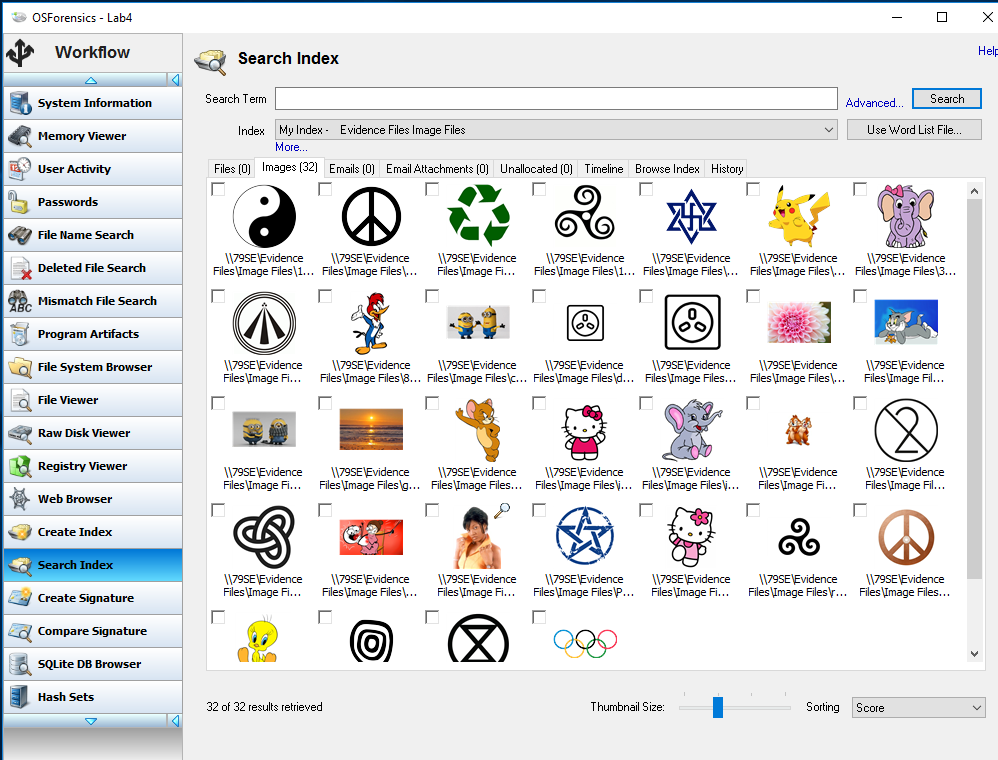
1. Bây giờ, ứng dụng sẽ bắt đầu thực hiện quét trước trên thư mục đã chỉ định.



1. Sau khi lập chỉ mục hoàn tất, ứng dụng sẽ thay đổi trạng thái của quá trình lập chỉ mục thành Đã hoàn thành, như có thể thấy trong trường Hành động hiện tại



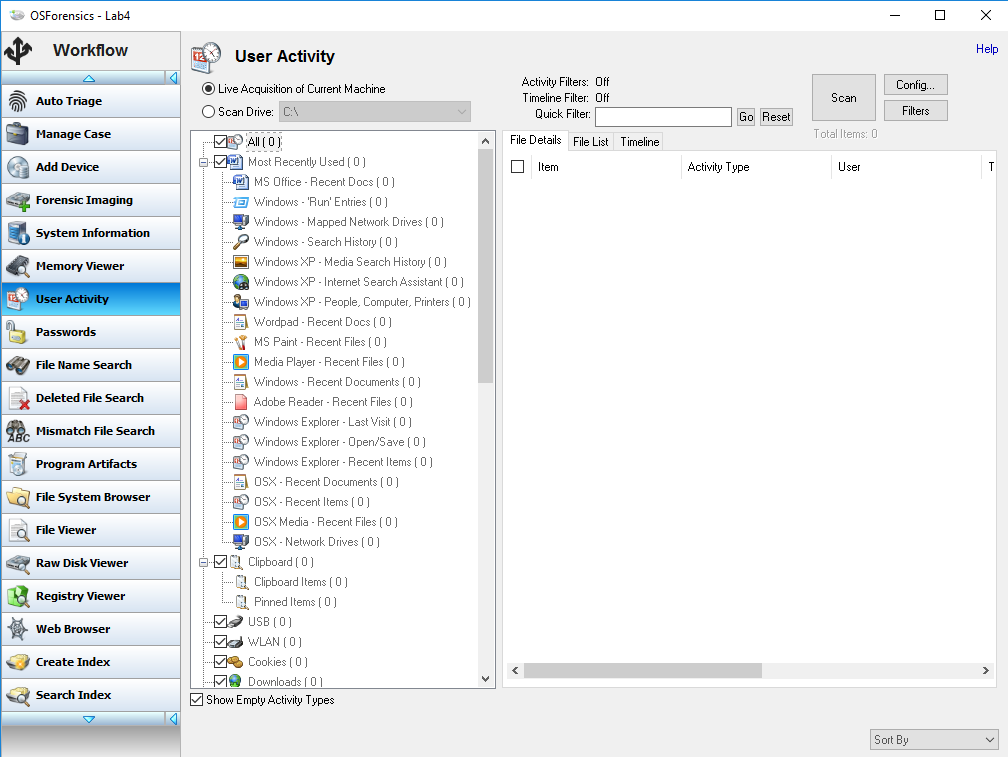
1. Bây giờ chúng ta sẽ tìm kiếm các tệp được lập chỉ mục. Để tìm kiếm các tệp được lập chỉ mục, hãy chọn Tìm kiếm Chỉ mục từ ngăn bên trái của cửa sổ công cụ. Phần Chỉ mục tìm kiếm hiện xuất hiện trong cửa sổ công cụ. Trường chỉ mục ở trên cùng hiển thị tên của trường hợp chúng tôi đã tạo (tức là Trường hợp 75). Nhấp vào Tìm kiếm. Công cụ sẽ tải các tệp hình ảnh mà bạn đã lập chỉ mục trong tab Hình ảnh.



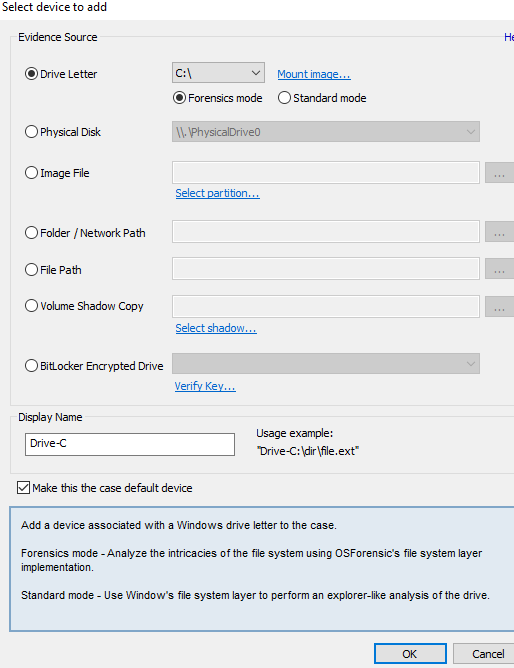
1. Tương tự, bạn cũng có thể lập chỉ mục các tệp khác như email và tìm kiếm chúng bằng tùy chọn Chỉ mục tìm kiếm. Trong trường hợp đó, các email được lập chỉ mục sẽ được hiển thị trong tab Email.

## **Task 4: Searching User’s Recent Activities**

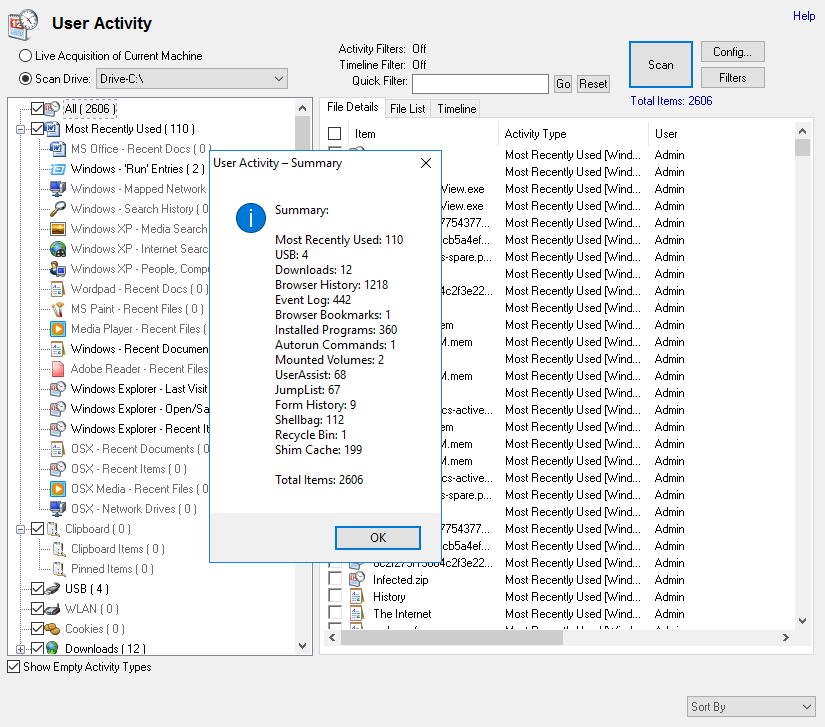
1. Bây giờ, chúng tôi sẽ thu thập tất cả các hoạt động của người dùng đã xảy ra trên hệ thống.
2. Nhấp vào Hoạt động của người dùng ở khung bên trái để quét các bằng chứng như các trang web đã duyệt, ổ USB, các bản tải xuống gần đây và mạng không dây
3. Trong bài lab này, chúng ta sẽ quét các hoạt động diễn ra trong ổ C:. Chọn nút radio Scan Drive, đảm bảo rằng ổ C: được chọn từ menu thả xuống Scan Drive, sau đó nhấp vào Scan để quét các hoạt động như trang web đã duyệt, ổ USB, tải xuống gần đây và mạng không dây trong ổ.



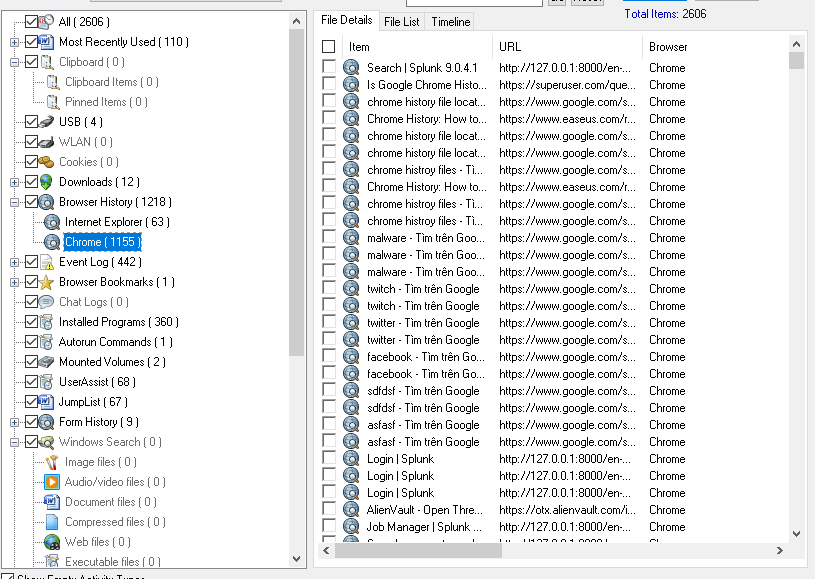
1. Nếu xuất hiện cửa sổ Chọn thiết bị để thêm, bấm OK



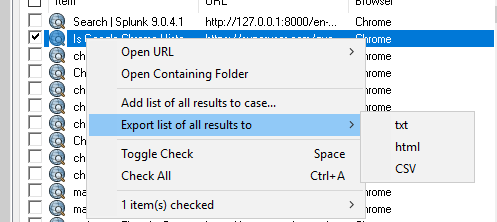
1. Ứng dụng cần một chút thời gian để quét và sau khi hoàn tất quá trình quét, cửa sổ Hoạt động của người dùng - Tóm tắt bật lên, hiển thị bản tóm tắt thông tin liên quan đến hoạt động của người dùng như Lịch sử trình duyệt, Tải xuống, Chương trình được sử dụng gần đây nhất và Đã cài đặt. Bấm OK để đóng Hoạt động người dùng – Tóm tắt.



1. Nếu bạn muốn lưu bất kỳ thông tin nào về hoạt động của người dùng ở trên trên hệ thống của mình, chẳng hạn như Lịch sử trình duyệt, thì hãy cuộn xuống danh sách các mục trong ngăn bên trái bên dưới tùy chọn Quét ổ đĩa và mở rộng nút Lịch sử trình duyệt. Chọn trình duyệt mà bạn muốn truy xuất lịch sử (Ở đây chúng tôi chọn Chrome). Lịch sử trình duyệt liên quan đến trình duyệt này sẽ được hiển thị trong ngăn bên phải của cửa sổ công cụ



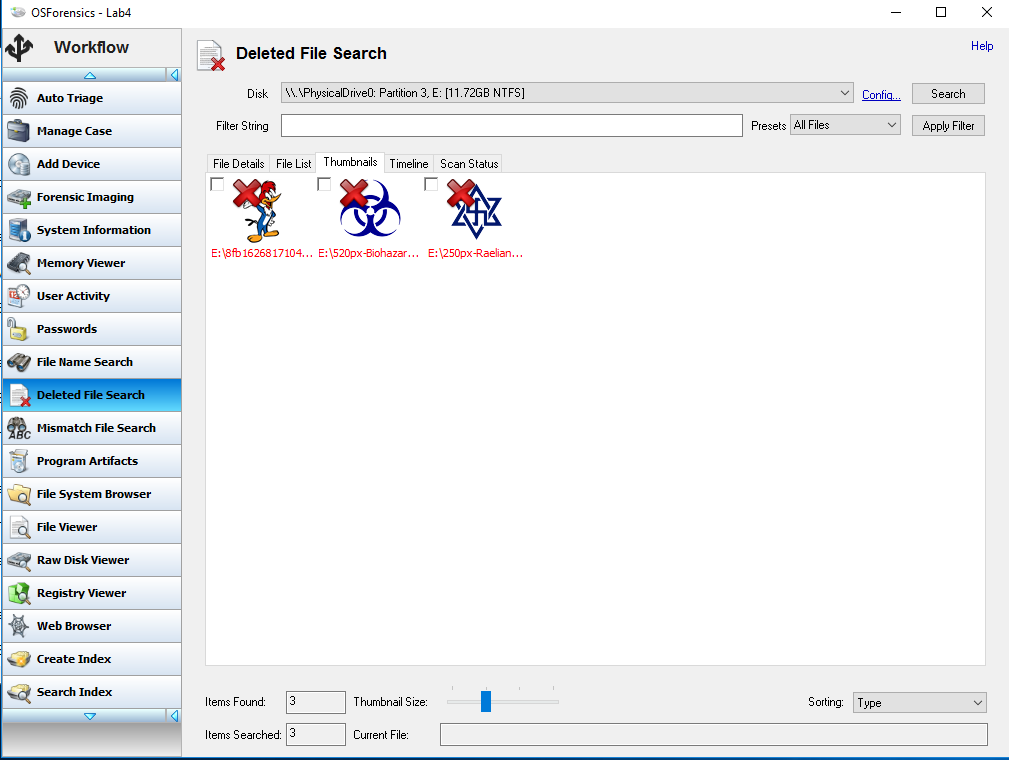
1. Để truy xuất toàn bộ lịch sử trình duyệt, hãy chọn bất kỳ tệp nào trong khung bên phải và nhấp chuột phải vào tệp đó. Từ menu ngữ cảnh, nhấp vào Xuất danh sách tất cả kết quả sang và từ menu thả xuống kết quả, nhấp vào txt.



1. Một cửa sổ Export List to... sẽ xuất hiện. Điều hướng đến C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Cas e 75, đặt tên cho tệp (ở đây, chúng tôi đặt tên là Lịch sử duyệt web) và nhấp vào Lưu để xuất lịch sử duyệt web
2. Lịch sử sẽ được xuất và lưu vào tệp văn bản. Điều hướng đến thư mục trường hợp và bấm đúp vào tệp Lịch sử duyệt web để xem thông tin được lưu trữ trong đó.
3. Bây giờ chúng ta sẽ kiểm tra cách khôi phục các tệp đã xóa bằng công cụ này

## **Task 5: Searching Deleted Files**

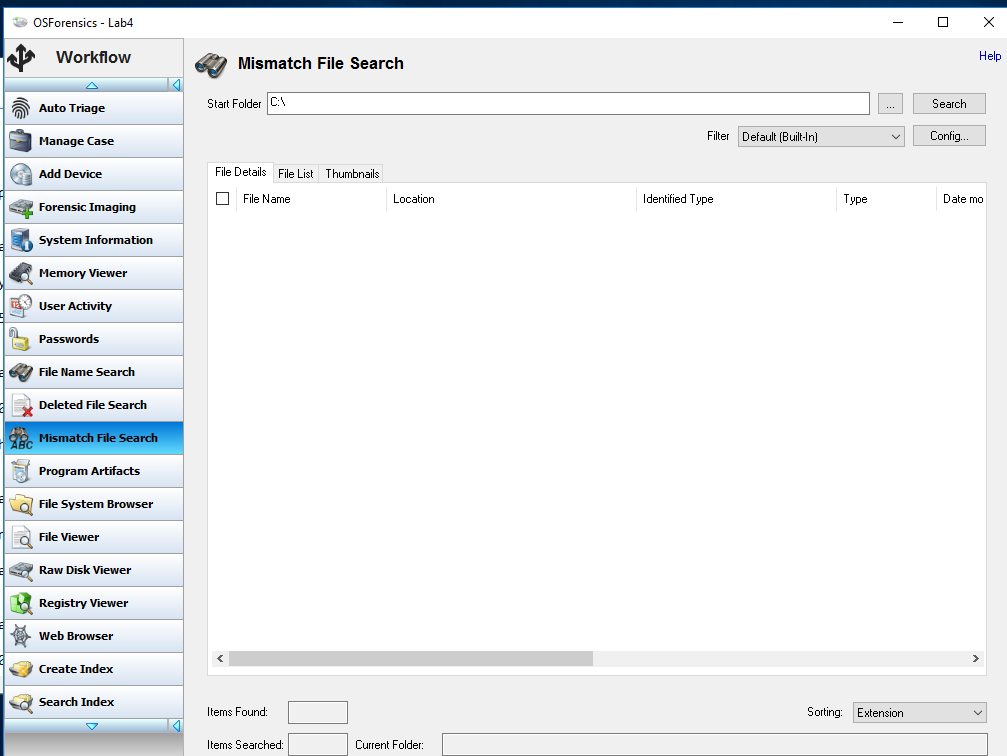
1. Để khôi phục các tệp đã xóa từ hệ thống tệp, nhấp vào Tìm kiếm tệp đã xóa trong ngăn bên trái, chọn đĩa mà bạn muốn thực hiện tìm kiếm tệp đã xóa từ menu thả xuống Đĩa (ở đây, chúng tôi đang chọn Phân vùng 1, C :) và nhấp vào nút Tìm kiếm
2. Ứng dụng sẽ chạy quét trên ổ đĩa đã chọn, truy xuất các tệp đã xóa và hiển thị chúng trong tab Hình thu nhỏ được hiển thị trong ảnh chụp màn hình sau:



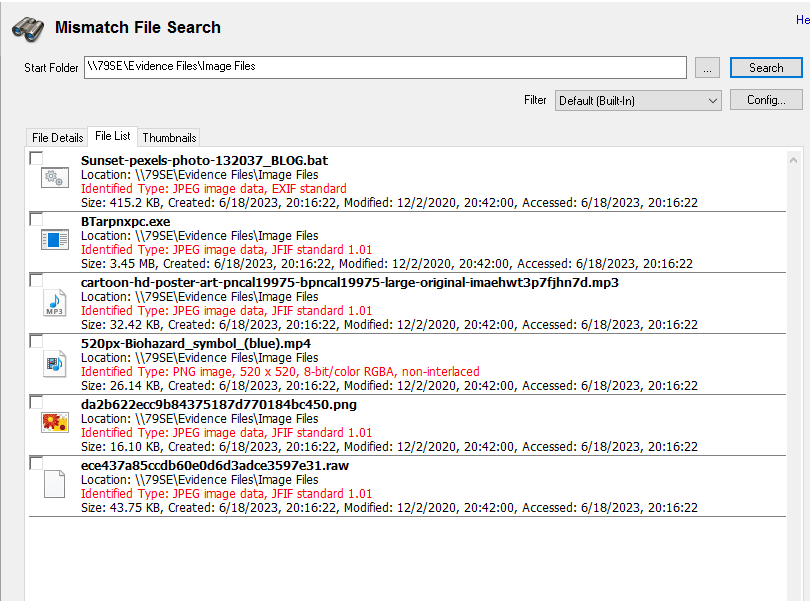
1. Để lưu và xem nội dung của các tệp đã xóa đã được công cụ truy xuất, hãy làm theo tiến trình tương tự như được mô tả trong các bước trên và đặt tên cho tệp được xuất là Tệp đã xóa được phục hồi

## **Task 6: Searching Mismatch Files**

1. Bây giờ chúng tôi sẽ phát hiện các tệp có phần mở rộng không khớp. Đối với điều này, chúng tôi sẽ sử dụng tính năng Tìm kiếm tệp không khớp. Tính năng này hữu ích trong trường hợp kẻ tấn công đã lưu tệp độc hại vào hệ thống bằng cách sửa đổi phần mở rộng của chúng.
2. Để định vị các tệp có nội dung không khớp với phần mở rộng tệp, hãy nhấp vào Tìm kiếm tệp không khớp trong ngăn bên trái của cửa sổ công cụ. Công cụ sẽ hiển thị phần Tìm kiếm tệp không khớp trong khung bên phải, như trong ảnh chụp màn hình

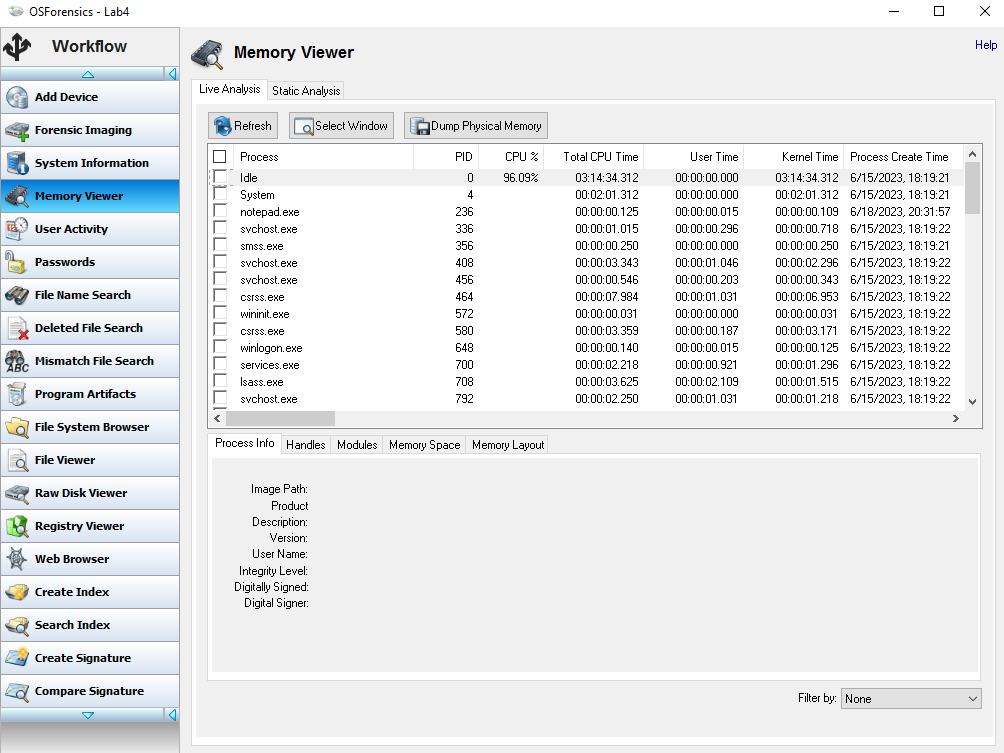


1. Nhấp vào nút Dấu ba chấm liên quan đến trường Thư mục Bắt đầu để cung cấp vị trí trong đó các tệp có phần mở rộng không khớp sẽ được tìm kiếm. Đối với tác vụ này, chúng tôi sẽ tìm kiếm các tệp có phần mở rộng không khớp trong thư mục Tệp hình ảnh. Vì vậy, hãy điều hướng đến C:\CHFI-Tools\Evidence Files\Image Files và nhấp vào nút Tìm kiếm
2. Công cụ sẽ quét thư mục đã chọn và hiển thị tất cả các tệp có phần mở rộng không khớp trong tab Chi tiết tệp theo mặc định. Nhấp vào tab Danh sách tệp để dễ dàng xem các tệp và thông tin chi tiết của chúng như trong ảnh chụp màn hình sau:

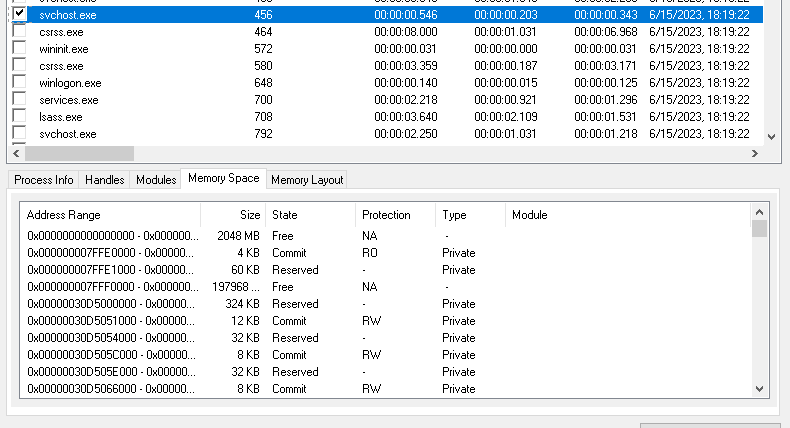


## **Task 7: Viewing Active Processes Running on the Computer Memory**

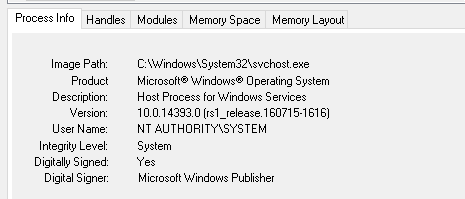
1. Bây giờ chúng ta sẽ tiến hành công việc xem các tiến trình đang chạy trên hệ thống.
2. Để xem các tiến trình đang chạy trên hệ thống, hãy nhấp vào Memory Viewer ở khung bên trái của cửa sổ công cụ. Lúc này công cụ sẽ hiển thị phần Memory Viewer.



1. Chọn một Tiến trình từ danh sách các tiến trình đang chạy, sau đó chọn tab Dung lượng bộ nhớ để xem toàn bộ chi tiết bộ nhớ của tiến trình đó



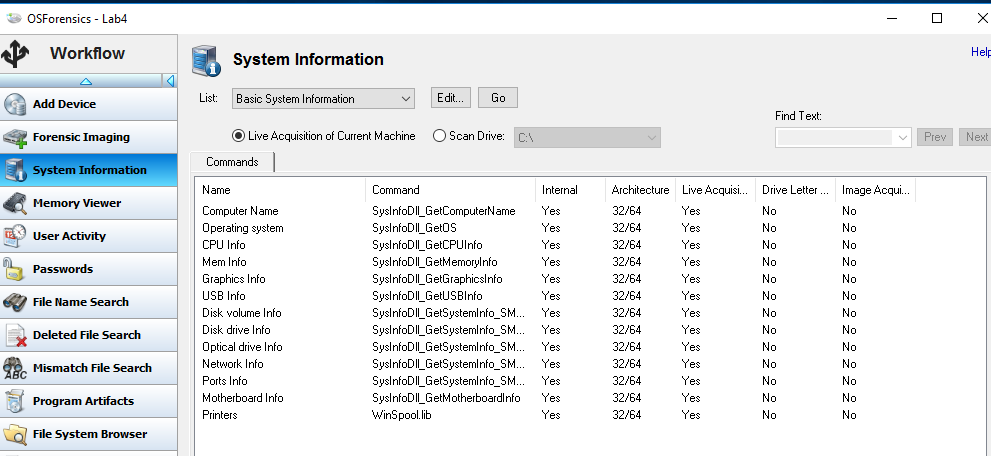
1. Để xem thông tin tiến trình liên quan đến tệp đã chọn, nhấp vào tab Thông tin tiến trình. Thông tin liên quan đến quá trình đó sẽ được hiển thị như trong ảnh chụp màn hình



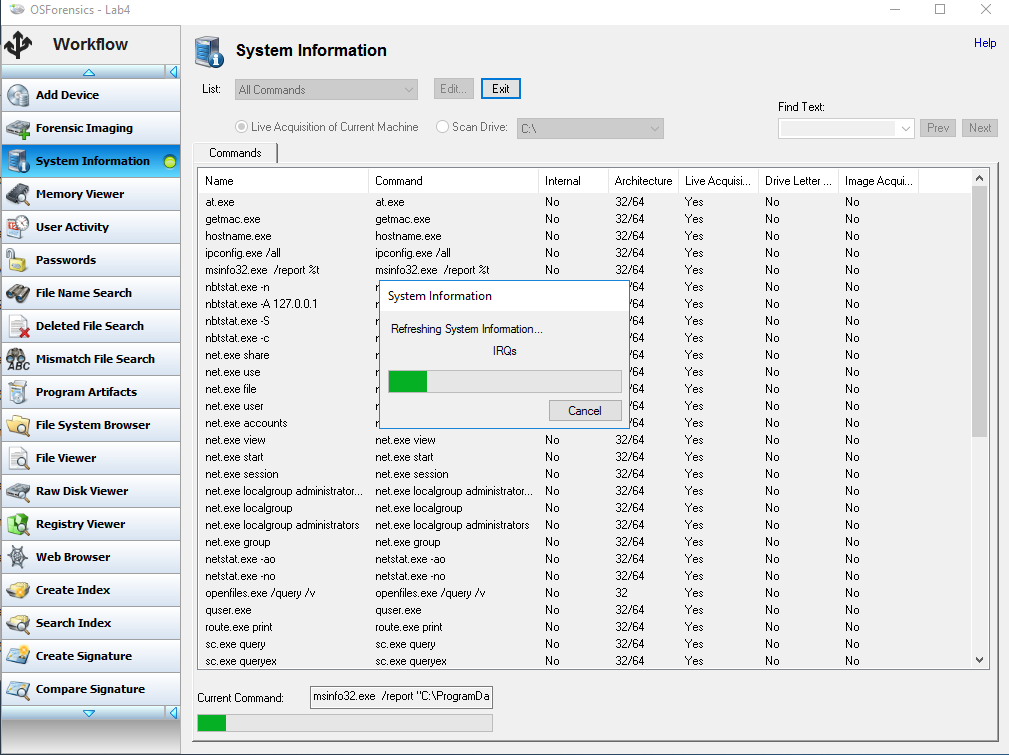
1. Bây giờ chúng ta sẽ tiến hành công việc xem thông tin hệ thống.

## **Task 8: Viewing System Information**

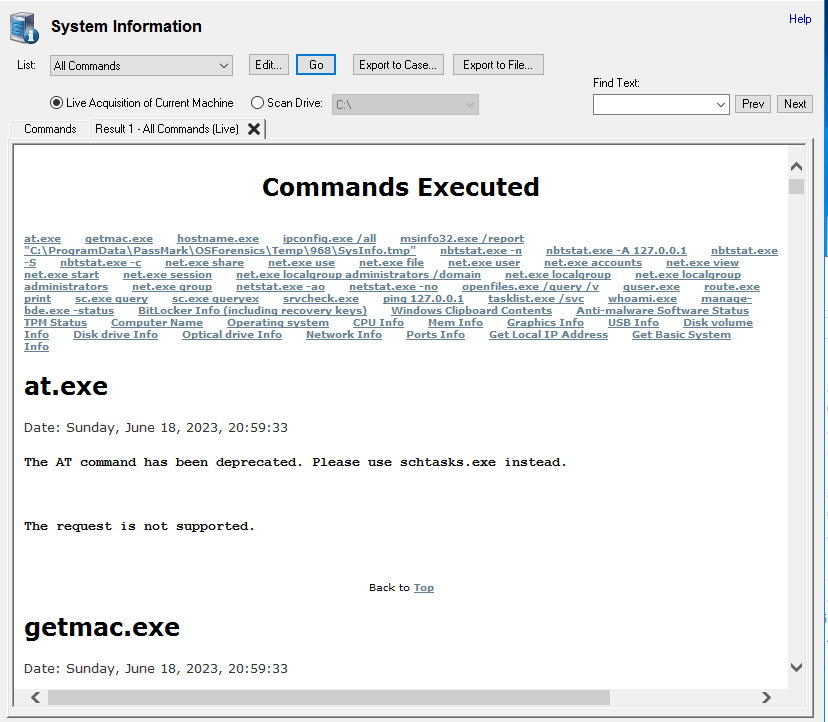
1. Để truy xuất thông tin chi tiết về các thành phần cốt lõi của hệ thống, hãy nhấp vào Thông tin Hệ thống. Công cụ sẽ hiển thị phần Thông tin hệ thống.



1. Từ menu thả xuống Danh sách, chọn bất kỳ tùy chọn nào dựa trên loại thông tin bạn muốn truy xuất và sau đó nhấp vào Bắt đầu. Các tùy chọn được hiển thị trong menu thả xuống danh sách là Lệnh DOS cơ bản, Thông tin hệ thống cơ bản, Thông tin hệ thống từ sổ đăng ký, Phát hiện BitLocker, Khôi phục khóa BitLocker, Tập lệnh Python và Tất cả các lệnh.
2. Ở đây, chúng tôi chọn Tất cả các lệnh từ menu thả xuống Danh sách. Đảm bảo rằng nút radio chống lại tùy chọn Live Acquisition of Current Machine được chọn và sau đó nhấp vào Go

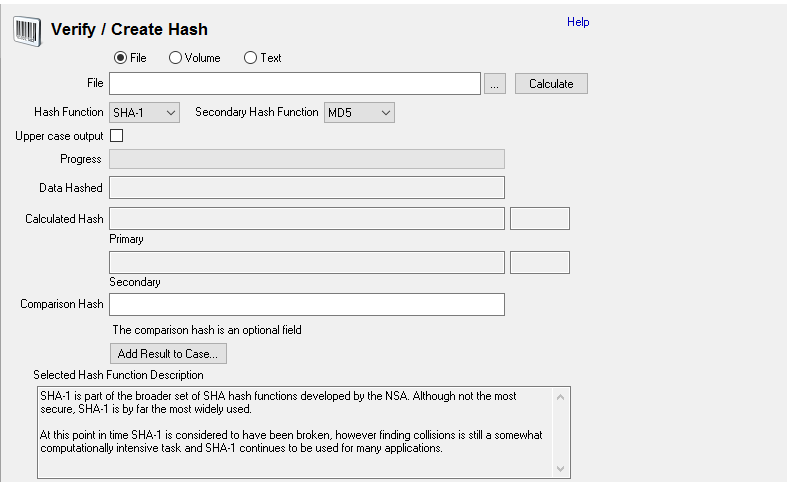


1. Vì chúng tôi đã chọn tùy chọn Tất cả các lệnh nên khi nhấp vào Bắt đầu, ứng dụng sẽ hiển thị tất cả các lệnh đã được thực thi trên hệ thống và kết quả đầu ra tương ứng của chúng trong tab Kết quả 1 – Tất cả các lệnh (Trực tiếp), như thể hiện trong ảnh chụp màn hình sau:

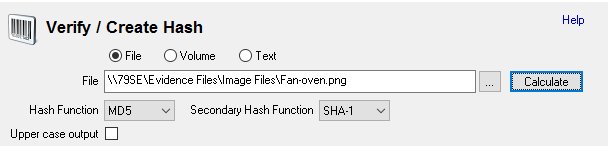


## **Task 9: Verifying File Integrity**

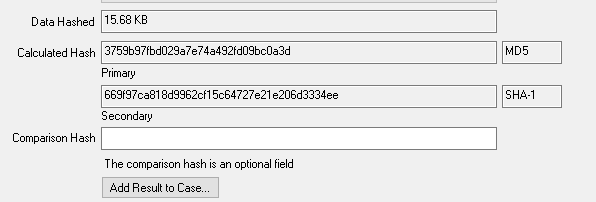
1. Bây giờ chúng ta sẽ tiến hành nhiệm vụ xác minh tính toàn vẹn của tệp bằng cách tính giá trị băm của chúng.
2. Để xác minh tính toàn vẹn của tệp bằng cách tính giá trị băm của chúng, hãy nhấp vào Xác minh/Tạo Hash từ ngăn bên trái của cửa sổ. Lúc này phần Verify/Create Hash sẽ xuất hiện trong cửa sổ. Đảm bảo rằng tùy chọn Tệp được chọn.



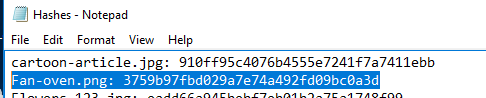
1. Nhấp vào nút Ellipsis để chỉ định một Tệp để tính giá trị băm của nó. Ở đây, chúng tôi chỉ định tệp Friends2.jpg từ vị trí C:\CHFI-Tools\Evidence Files\Image Files\Friends2.jpg để tính giá trị băm của nó. Từ danh sách thả xuống Hàm băm, chọn MD5 và từ danh sách thả xuống Hàm băm phụ, chọn SHA1. Sau đó, nhấp vào Tính toán



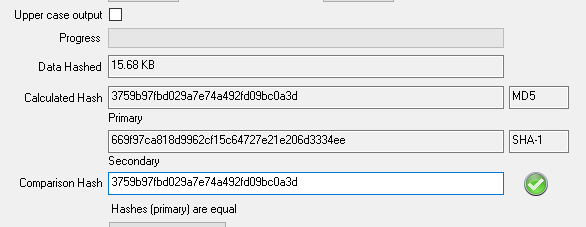
1. Giá trị băm của tệp xuất hiện trong phần Hàm băm được tính toán trong cả hai trường Hàm băm chính (MD5) cũng như Hàm băm phụ (SHA-1), như minh họa trong ảnh chụp màn hình sau:



1. Để xác minh tính toàn vẹn của tệp Friends2.jpg, chúng ta có thể nhập giá trị băm có sẵn của nó vào trường Băm so sánh. Điều hướng đến C:\CHFI-Tools\Evidence Files\Image Files và mở tệp Hashes.txt, tệp này chứa các giá trị băm có sẵn của một số tệp hình ảnh. Sao chép giá trị băm cho tệp Friends2.jpg



1. Bây giờ, dán giá trị băm đã sao chép của tệp Friends2.jpg vào trường Băm so sánh. Bạn sẽ thấy một dấu kiểm xuất hiện trên trường Băm so sánh, cho biết rằng các giá trị băm MD5 đã được tính toán và tồn tại trước đó của tệp đã chọn khớp với nhau. Điều này ngụ ý rằng tính toàn vẹn của tệp còn nguyên vẹn

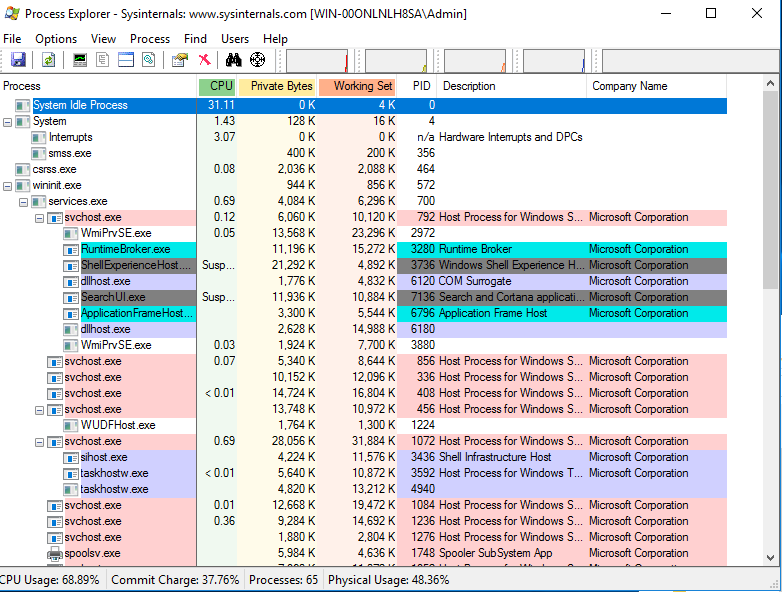


1. Theo cách này, bạn có thể thực hiện điều tra trên hệ thống hoặc các thư mục và phân vùng trong hệ thống để thu thập dữ liệu quan tâm cho điều tra số

# **Lab 5: Extracting Information about Loaded Processes on a Computer**

## **Task 1: Viewing System Information**

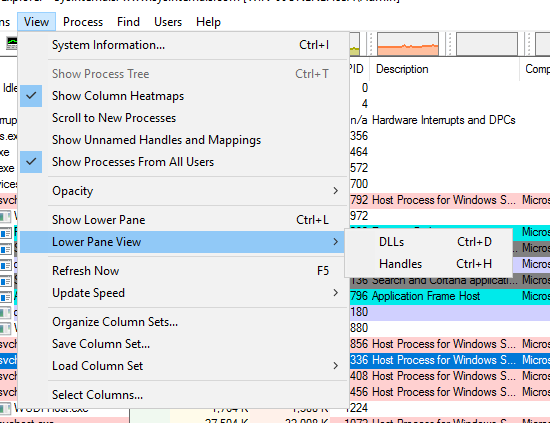
1. Đăng nhập vào máy ảo Windows Server 2016
2. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Windows Forensics Tools\Process Explore
3. Bấm đúp vào tệp procexp.exe và chấp nhận thỏa thuận cấp phép.
4. GUI Process Explorer xuất hiện, hiển thị chi tiết của tất cả các tiến trình đang chạy trên máy, như minh họa trong ảnh chụp màn hình



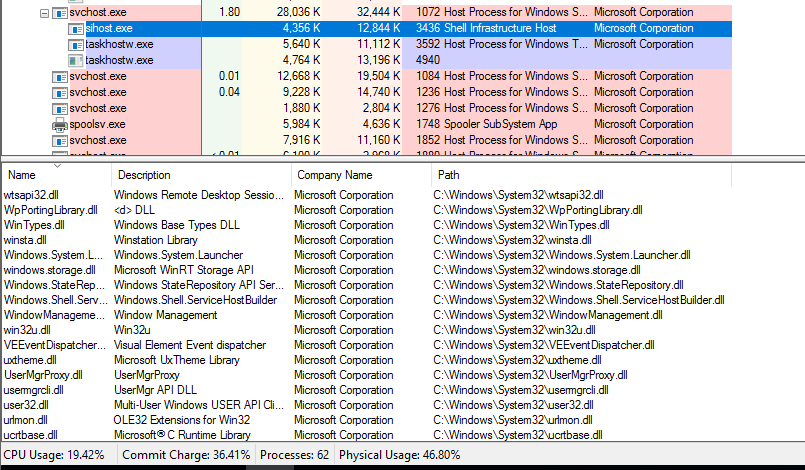
1. Process Explorer liệt kê tất cả các tiến trình đang chạy trong khung bên trái và chi tiết của từng tiến trình (chẳng hạn như mức sử dụng CPU và PID) trong khung bên phải.

## **Task 2: Viewing DLLs**

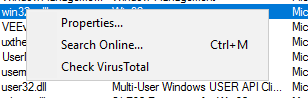
1. Để xem các tệp DLL, nhấp vào biểu tượng Xem DLL từ thanh công cụ hoặc điều hướng đến View Lower Pane Xem DLL từ thanh Menu.



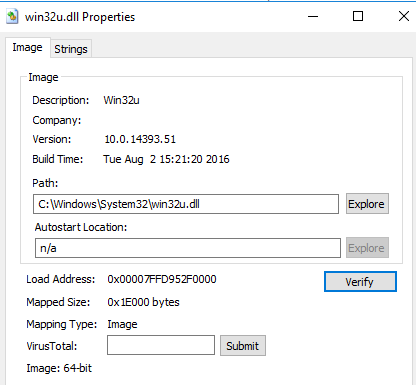
1. Cửa sổ Process Explorer bây giờ sẽ có một khung bên trên liệt kê các tiến trình và thông tin chi tiết của chúng và một khung bên dưới trống. Từ ngăn phía trên, chọn một tiến trình mà bạn muốn xem các tệp DLL. Bây giờ, bạn sẽ có thể xem danh sách các tệp DLL cho tiến trình đó ở khung bên dưới/dưới cùng của cửa sổ.



1. Để xem các thuộc tính DLL, chọn một DLL, chọn Thuộc tính DLL từ thanh Menu hoặc nhấp chuột phải vào DLL cần thiết từ danh sách DLL được hiển thị cho một tiến trình và chọn Thuộc tính....



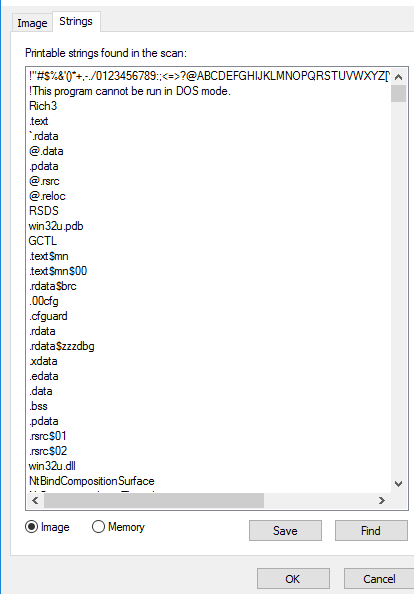
1. Thực hiện bước trên sẽ hiển thị các thuộc tính DLL trong tab Hình ảnh và Chuỗi.



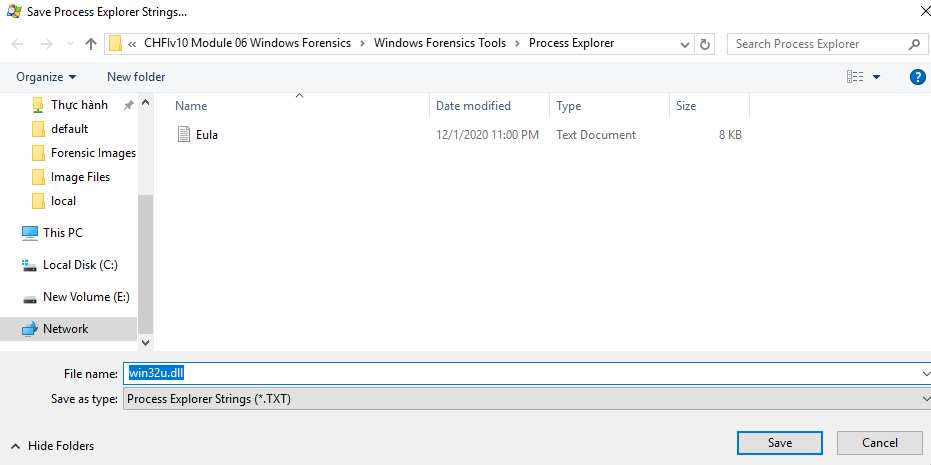
1. Tab Hình ảnh chứa các chi tiết của DLL như tên công ty, phiên bản và đường dẫn.
2. Nhấp vào Xác minh để kiểm tra chữ ký của tiến trình
3. Khi nhấp vào Xác minh, nếu tên của công ty là Microsoft Windows thì quá trình này được xác định là hợp pháp, như minh họa trong ảnh chụp màn hình



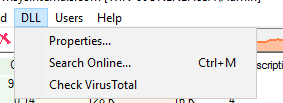
1. Bây giờ, hãy nhấp vào tab Chuỗi. Tab này liệt kê bất kỳ chuỗi Unicode nào được tìm thấy trong tiến trình đã chọn. Kiểm tra nội dung trong tab này giúp bạn tìm xem tiến trình có liên quan đến bất kỳ phần mềm độc hại nào không.
2. Khi bạn nhấp vào tab Chuỗi, bạn sẽ có hai tùy chọn để kiểm tra: chuỗi Hình ảnh và Bộ nhớ. Nhấp vào nút radio Hình ảnh hoặc Bộ nhớ ở cuối cửa sổ để xem hình ảnh hoặc chuỗi ký ức.

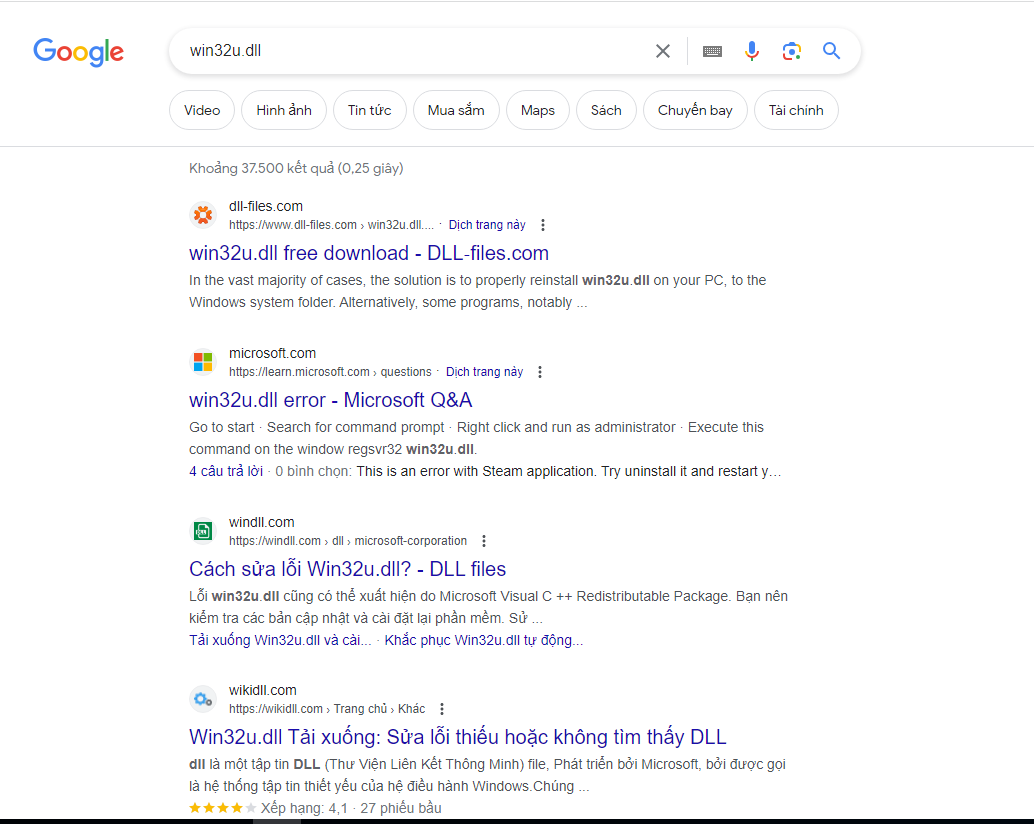


1. Bạn cũng có thể lưu chuỗi Hình ảnh và/hoặc Bộ nhớ ở định dạng tệp văn bản. Trong lab này, chúng tôi đang lưu chuỗi Hình ảnh. Để lưu chuỗi Hình ảnh, hãy đảm bảo rằng nút radio Hình ảnh được chọn rồi nhấp vào nút Lưu.
2. Khi nhấp vào Save, cửa sổ Save Process Explorer Strings... xuất hiện. Chỉ định một vị trí (ở đây, Máy tính để bàn) để lưu tệp và nhấp vào Lưu.



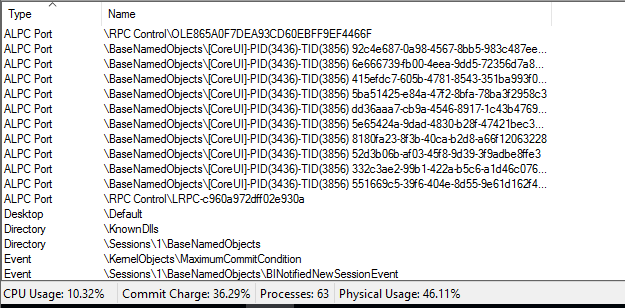
1. Khi lưu tệp, nhấp vào OK trong cửa sổ Thuộc tính của DLL để đóng tệp
2. Tùy chọn Search Online tìm kiếm DLL đã chọn trên internet bằng cách khởi chạy Trình duyệt Internet
3. Để tìm kiếm trực tuyến, chọn một DLL, nhấp chuột phải vào nó và chọn DLL Search Online... từ thanh Menu



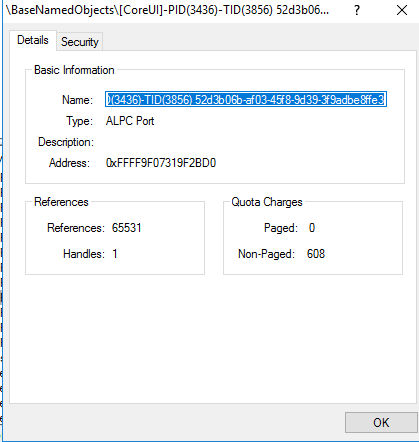


1. Để xem các handle của một process, chọn process và chọn View Lower Pane View Handles từ thanh Menu.

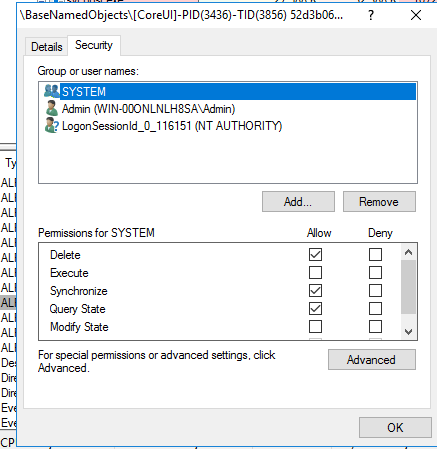




1. Để xem các thuộc tính của handle, click chuột phải vào handle cần chọn và chọn Properties, hoặc chọn handle cần thiết rồi chọn Handle Properties từ thanh Menu



1. Cửa sổ Thuộc tính xuất hiện cho tay cầm đã chọn. Tab Chi tiết hiển thị thông tin cơ bản về tay cầm đã chọn



1. Tab Bảo mật hiển thị mức độ bảo mật được chỉ định cho từng nhóm hoặc người dùng cho bộ điều khiển đã chọn.
2. Nhấn OK để đóng cửa sổ Properties.
3. Theo cách này, bạn có thể xem tất cả các tiến trình cũng như các DLL liên quan và các xử lý của chúng bằng cách sử dụng Process Explorer. Trong quá trình điều tra số, công cụ này rất hữu ích để kiểm tra một tiến trình (bất kỳ tiến trình độc hại nào, nếu được tìm thấy) và phân tích các tệp DLL và phần xử lý liên quan của nó.

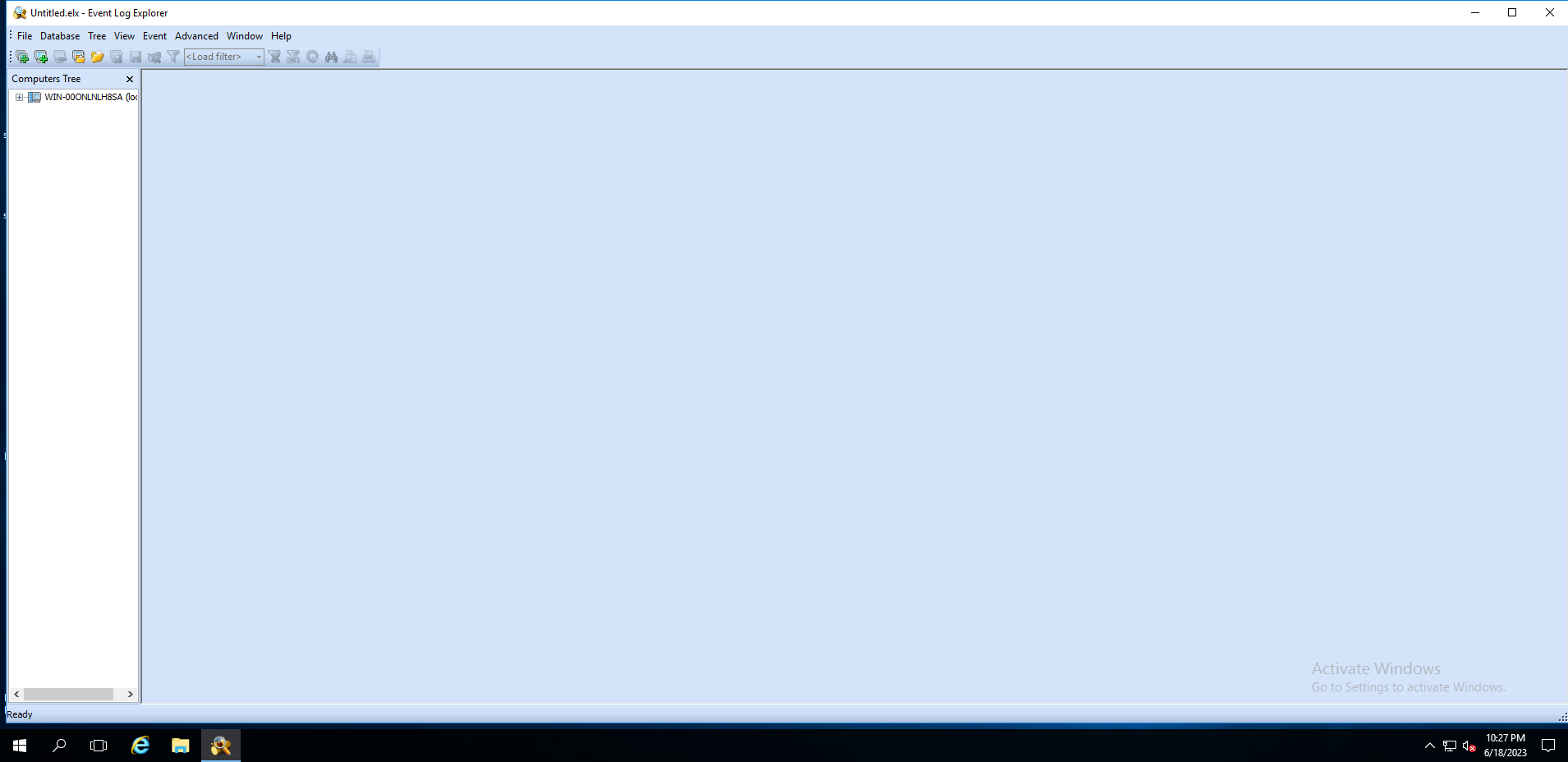
# **Lab 6: Viewing, Monitoring, and Analyzing Events Occurred on a Windows Machine**

## **Task 1: Installing and Launching Event Log Explorer**

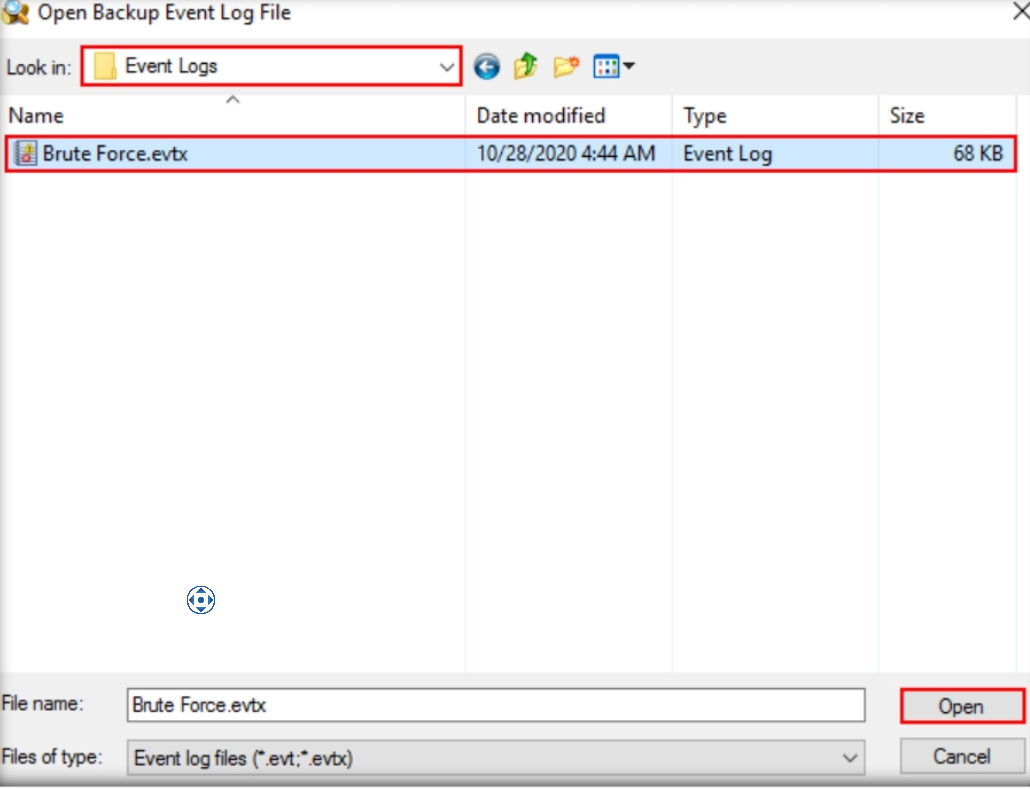
1. Đăng nhập vào máy ảo Windows Server 2016.
2. Điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Windows Forensics Tools\Event Log Explorer và bạn sẽ thấy tệp elex\_setup.exe.
3. Nhấp đúp vào elex\_setup.exe để khởi chạy cài đặt. Chọn ngôn ngữ là tiếng Anh, chấp nhận thỏa thuận cấp phép và làm theo các bước cài đặt hướng dẫn để cài đặt ứng dụng.
4. Ở bước cài đặt cuối cùng, đánh dấu chọn Launch Event Log Explorer và nhấn Finish.
5. Khi hoàn tất cài đặt, một cửa sổ trình duyệt sẽ tự động mở ra, hiển thị trang web eventlogxp.com. Đóng cửa sổ trình duyệt. Ngoài cửa sổ trình duyệt, bạn cũng sẽ thấy cửa sổ bật lên Event Log Explorer xuất hiện sau khi hoàn tất cài đặt công cụ; trong cửa sổ bật lên này, đảm bảo rằng tùy chọn Tiếp tục đánh giá được chọn rồi bấm OK.
6. Cửa sổ chính của Event Log Explorer mở ra, hiển thị một khu vực xem nhật ký trống và ngăn Cây máy tính ở bên trái, hiển thị tên máy ảo Windows Server 2016 của bạn ở trên cùng.
7. Chúng tôi sẽ sử dụng tệp bằng chứng Brute Force.evtx để kiểm tra nhật ký sự kiện đã được ghi lại trên máy chủ (ở đây, máy ảo Windows Server 2016).

## **Task 2: Uploading the Evidence File (Event Log File)**

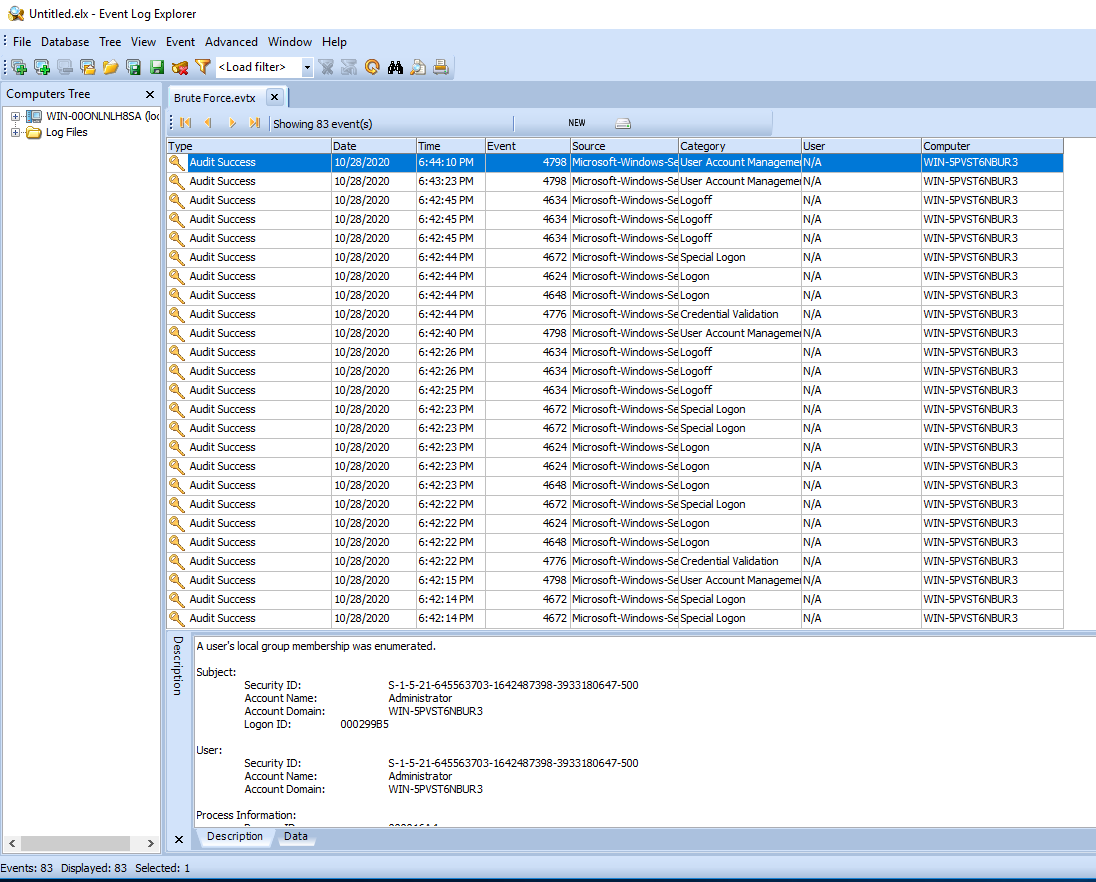
1. Nhấp vào biểu tượng Mở tệp nhật ký sự kiện ở đầu cửa sổ bên dưới thanh menu, như được đánh dấu trong ảnh chụp màn hình bên dưới



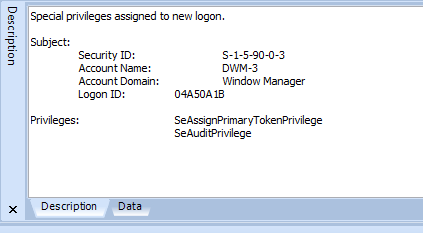
1. Một cửa sổ Open Backup Event Log File xuất hiện. Điều hướng đến C:\CHFI-Tools\Evidence Files\Event Logs, chọn tệp Brute Force.evtx, sau đó nhấp vào Mở, như được chỉ ra trong ảnh chụp màn hình sau:



1. Ứng dụng Event Log Explorer bây giờ sẽ tải tệp nhật ký đã chọn và hiển thị các mục nhật ký của nó trong ngăn bên phải của cửa sổ ứng dụng, như được chỉ ra trong ảnh chụp màn hình sau

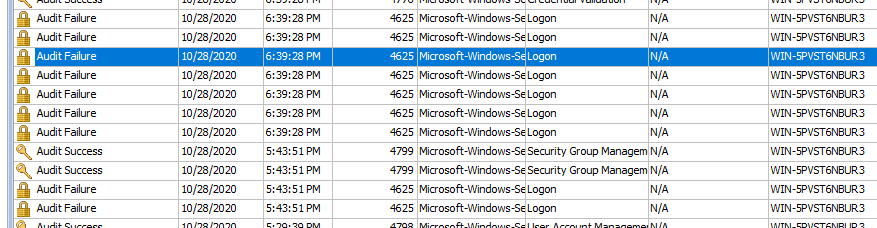


1. Nếu bạn muốn biết một sự kiện bảo mật cụ thể nói về điều gì, hãy chọn nó. Mô tả liên quan đến sự kiện đó sẽ được hiển thị trong ngăn Mô tả ở phần dưới của cửa sổ. Tại đây, khi chọn một trong các nhật ký sự kiện bảo mật, chúng tôi thấy rằng hệ thống đã cố xác thực thông tin đăng nhập cho tài khoản của Administrator

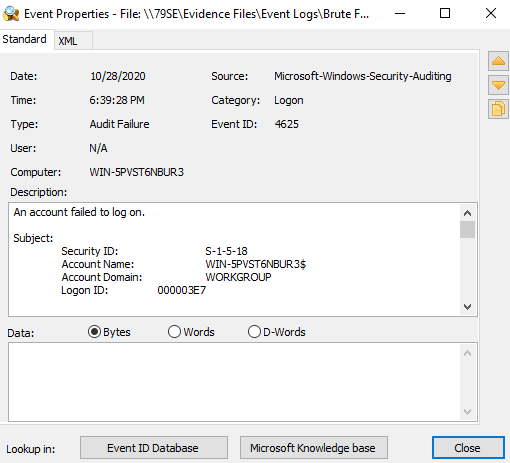


## **Task 3: Examining Audit Failure Events**

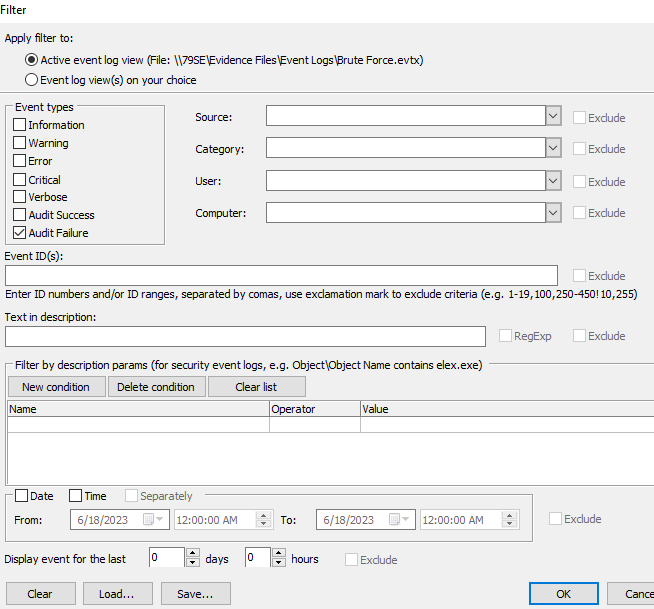
1. Bây giờ, cuộn xuống các sự kiện. Bạn sẽ có thể thấy một loạt các sự kiện Lỗi kiểm tra, như được hiển thị trong ảnh chụp màn hình sau:



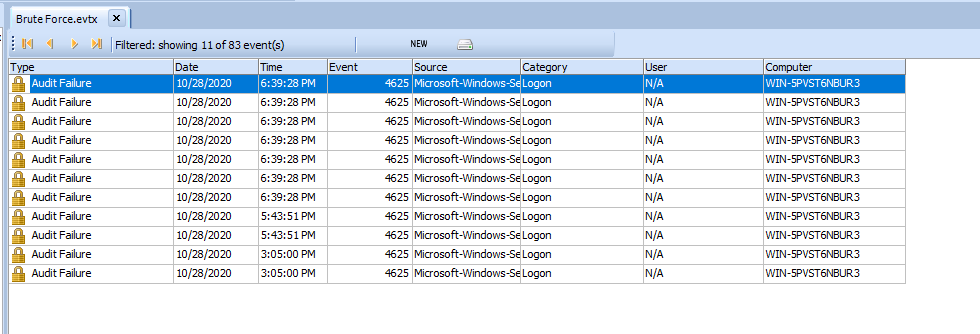
1. Để xem thông tin chi tiết liên quan đến sự kiện Audit Failed, nhấp đúp vào sự kiện. Công cụ sẽ hiển thị chi tiết của sự kiện trong cửa sổ Thuộc tính sự kiện. Tại đây, chúng tôi nhấp đúp vào sự kiện Lỗi kiểm tra đầu tiên được liệt kê ở đầu ngăn xếp trong ảnh chụp màn hình ở trên. Cửa sổ Thuộc tính sự kiện hiển thị một lần đăng nhập không thành công, được ghi lại với ID sự kiện 4625.



1. Trong một kịch bản thời gian thực, số lượng sự kiện được ghi lại có thể rất lớn và việc kiểm tra thủ công từng sự kiện và xác định các sự kiện đáng ngờ/độc hại có thể khá khó khăn.
2. Vì vậy, chúng tôi sẽ áp dụng bộ lọc cho các sự kiện bảo mật để kiểm tra tất cả các lần đăng nhập không thành công. Để áp dụng bộ lọc, hãy đóng cửa sổ Thuộc tính sự kiện rồi nhấp vào biểu tượng bộ lọc bên dưới thanh menu, như được đánh dấu trong ảnh chụp màn hình sau:
3. Một cửa sổ Bộ lọc sẽ mở ra. Trong cửa sổ này, chỉ chọn tùy chọn Kiểm tra lỗi trong khi bỏ chọn tất cả các tùy chọn khác trong phần Loại sự kiện. Sau đó, nhấp vào OK



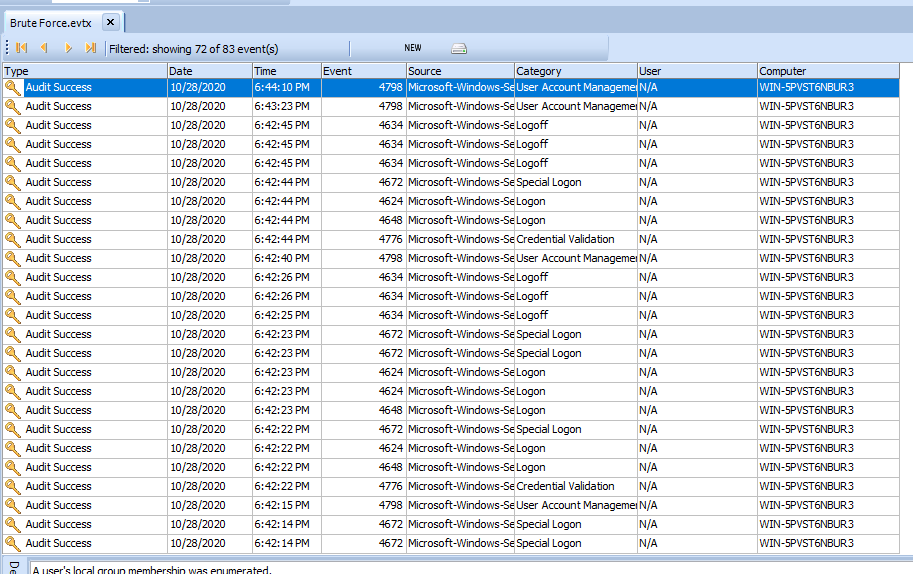
1. Bây giờ, ứng dụng sẽ chỉ hiển thị các sự kiện Kiểm tra lỗi trong ngăn bên phải của cửa sổ công cụ. Bạn có thể xem mô tả của sự kiện đã chọn trong ngăn Mô tả. Khung Mô tả, như được thấy trong ảnh chụp màn hình bên dưới, hiển thị như sau:
2. Dòng đầu tiên hiển thị thông báo có nội dung Không đăng nhập được tài khoản, ngụ ý rằng người dùng đã cố đăng nhập vào máy cục bộ nhưng đăng nhập không thành công.
3. Phần Chủ đề chứa Tên tài khoản của máy cục bộ (WIN-5PVST6NBUR3) mà lần đăng nhập đã được thực hiện.
4. Phần Tài khoản đăng nhập không thành công chứa Tên tài khoản là Administrator, là tên người dùng trên máy cục bộ. Do đó, chúng tôi có thể suy luận rằng tài khoản có tên người dùng Administrator đã được nhắm mục tiêu.



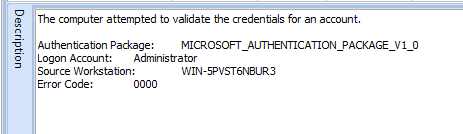
1. Trong ảnh chụp màn hình ở trên, hãy lưu ý rằng bảy sự kiện Lỗi kiểm tra đầu tiên từ trên cùng có cùng dấu thời gian, tức là 4:39:28 sáng (Dấu thời gian quan sát được trong môi trường lab của bạn có thể khác với dấu thời gian được minh họa trong lab này). Do đó, khi chúng tôi kiểm tra chi tiết của từng sự kiện trong số sáu sự kiện Lỗi kiểm tra khác có cùng dấu thời gian trong ngăn Mô tả bằng cách chọn tuần tự từng sự kiện, chúng cho thấy một lần đăng nhập không thành công, như đã thấy ở bước trên.
2. Bây giờ, chúng ta sẽ kiểm tra các sự kiện Audit Success, ghi nhớ dấu thời gian mà chúng phản ánh

## **Task 4: Examining Audit Success Events**

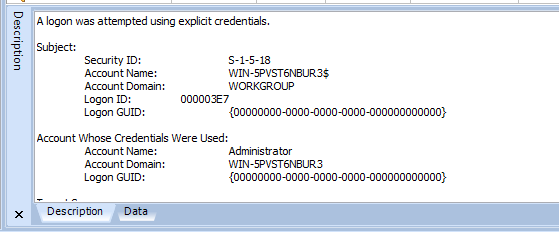
1. Vì vậy, hãy nhấp vào biểu tượng bộ lọc ở trên cùng. Cửa sổ Bộ lọc sẽ xuất hiện như đã thấy trước đó. Trong cửa sổ Bộ lọc, chỉ chọn tùy chọn Kiểm tra thành công trong khi bỏ chọn tất cả các tùy chọn khác trong phần Loại sự kiện. Sau đó, nhấp vào OK
2. Bây giờ, ứng dụng sẽ liệt kê tất cả các sự kiện Audit Success trong ngăn bên phải của cửa sổ, như minh họa trong ảnh chụp màn hình sau



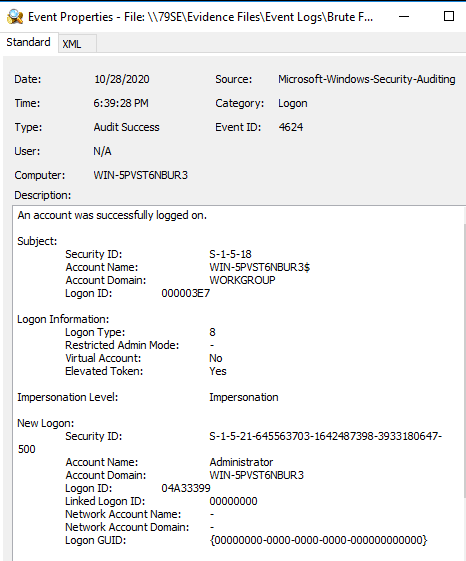
1. Từ quan sát trước đây của chúng tôi, chúng tôi biết rằng nhiều sự kiện Lỗi kiểm tra cho thấy các lần đăng nhập không thành công có dấu thời gian là 4:39:28 AM. Bây giờ, chúng ta cần bắt đầu kiểm tra các sự kiện Kiểm toán thành công bắt đầu vào hoặc sau 4:39:28 sáng.
2. Cuộn xuống trong ngăn bên phải của cửa sổ để xem các sự kiện Kiểm tra thành công có dấu thời gian 4:39:28 AM. Chúng ta cần bắt đầu kiểm tra các nhật ký sự kiện này bắt đầu với sự kiện Kiểm tra thành công đầu tiên có dấu thời gian là 4:39:28 sáng.
3. Chọn sự kiện Kiểm tra thành công đầu tiên với ID sự kiện 4776. Ngăn Mô tả của nó cho thấy máy tính đã cố xác thực thông tin đăng nhập cho Administrator tài khoản trên máy cục bộ (được xác định là WIN-5PVST6NBUR3), như được chỉ ra trong ảnh chụp màn hình bên dưới. Điều này ngụ ý rằng nỗ lực đăng nhập vào máy cục bộ của người dùng đã được xác thực.



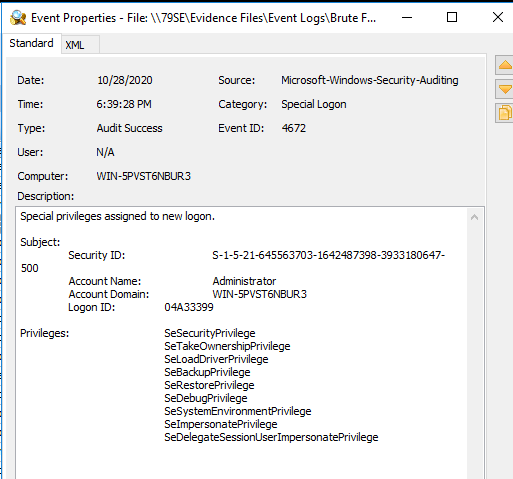
1. Bây giờ, hãy chọn sự kiện Kiểm tra thành công ở trên sự kiện hiện được chọn và giữ dấu thời gian giống như đã đề cập trước đó. Ngăn Mô tả của nó tiết lộ rằng một lần đăng nhập đã được thử bằng thông tin xác thực rõ ràng trên máy cục bộ, như được chỉ ra trong ảnh chụp màn hình bên dưới. Điều này ngụ ý rằng một nỗ lực đăng nhập bằng thông tin xác thực đăng nhập rõ ràng, rõ ràng có thể đã được thực hiện trên máy cục bộ. Điều này có thể xảy ra khi kẻ tấn công/người dùng độc hại đã nắm giữ thông tin xác thực đăng nhập cho một máy cục bộ.



1. Bây giờ, hãy chọn sự kiện Audit Success ở trên sự kiện hiện được chọn và giữ dấu thời gian đã đề cập trước đó. Ngăn Mô tả của nó cho biết rằng một tài khoản đã được đăng nhập thành công. Tiếp tục cuộn xuống trong ngăn Mô tả sẽ hiển thị tên tài khoản (ở đây, đó là Administrator) đã đăng nhập thành công, được biểu thị qua các ảnh chụp màn hình bên dưới:



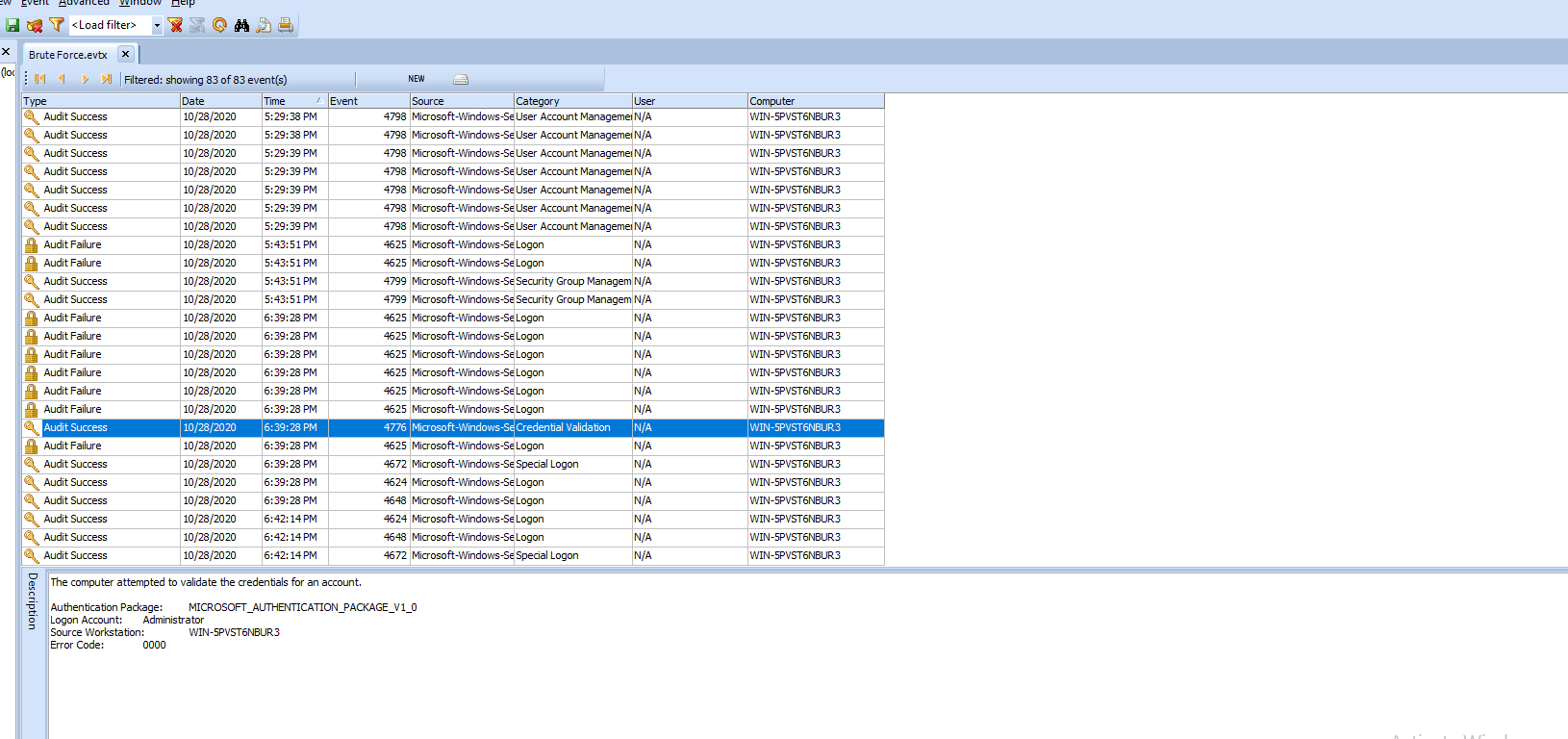
1. Bây giờ, hãy chọn sự kiện Audit Success ở trên sự kiện hiện được chọn và giữ dấu thời gian đã đề cập trước đó. Trường Danh mục của nó đề cập đến Đăng nhập Đặc biệt. Khung Mô tả cho sự kiện này, ở trên cùng, hiển thị rằng các đặc quyền đặc biệt đã được gán cho lần đăng nhập mới, như được chỉ ra trong ảnh chụp màn hình bên dưới. Điều này ngụ ý rằng người dùng đáng ngờ đã đăng nhập có thể đã đạt được các đặc quyền nâng cao trên máy cục bộ



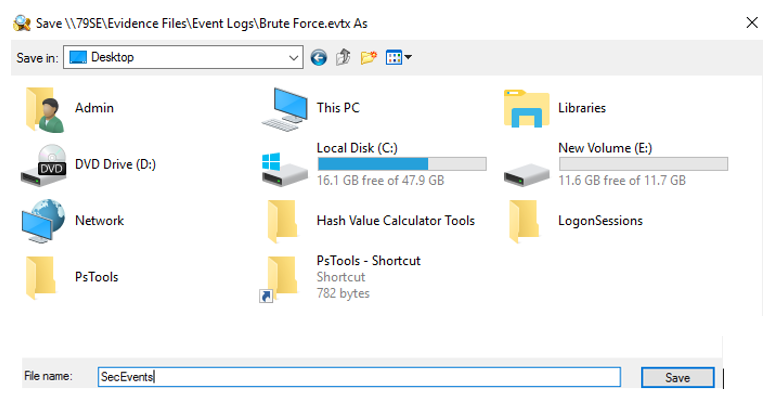
1. Tất cả những phát hiện trên cho thấy rằng một nỗ lực đăng nhập thành công đã xảy ra trên máy cục bộ sau nhiều lần thử đăng nhập thất bại lặp đi lặp lại. Cả hai sự kiện đăng nhập thất bại và thành công đều xảy ra liên tiếp vì cả hai đều phản ánh cùng một dấu thời gian. Đây là dấu hiệu mạnh mẽ của một cuộc tấn công vũ phu.
2. Bây giờ, chúng ta sẽ lưu nhật ký sự kiện Kiểm tra Thất bại và Kiểm tra Thành công mà chúng ta vừa kiểm tra.

## **Task 5: Saving the Event Logs**

1. Trước khi lưu nhật ký sự kiện, hãy nhấp vào biểu tượng Bộ lọc ở trên cùng. Trong cửa sổ Bộ lọc xuất hiện, chỉ chọn các tùy chọn Kiểm tra thành công và Kiểm tra thất bại trong phần Loại sự kiện trong khi bỏ chọn tất cả các tùy chọn khác. Sau đó, nhấp vào OK, như được chỉ ra trong ảnh chụp màn hình
2. Bây giờ, bạn sẽ thấy cả hai sự kiện Kiểm tra thành công và Kiểm tra thất bại được liệt kê trong ngăn bên phải của cửa sổ, như được chỉ ra trong ảnh chụp màn hình bên dưới:



1. Bây giờ, để lưu tệp nhật ký sự kiện, hãy vào Tệp -> Lưu nhật ký dưới dạng... -> Lưu nhật ký sự kiện (Sao lưu)..
2. Một cửa sổ Lưu sẽ xuất hiện. Điều hướng đến vị trí bạn muốn lưu tệp nhật ký. Ở đây, chúng tôi đang lưu tệp trên Máy tính để bàn. Đặt tên cho tệp nhật ký (ở đây, chúng tôi đặt tên là Nhật ký sự kiện bảo mật) và nhấp vào Lưu.



1. Để xem tệp nhật ký sự kiện bảo mật đã lưu, bạn có thể mở trực tiếp tệp đó trong Trình xem sự kiện từ vị trí bạn đã lưu tệp. Ngoài ra, bạn có thể truy cập nó từ cửa sổ công cụ Event Explorer bằng cách vào File Open Log File Standard (legacy)
2. Tương tự, bạn cũng có thể kiểm tra nhật ký sự kiện ứng dụng và nhật ký sự kiện hệ thống bằng cách sử dụng các tệp nhật ký đã ghi lại các sự kiện đó. Trong lab này, chúng tôi chỉ sử dụng tệp Brute Force.evtx, tệp này hiển thị các sự kiện bảo mật.
3. Theo cách này, bạn có thể kiểm tra các sự kiện Windows thông qua Event Log Explorer.

# **Lab 7: Performing Digital Forensic Investigation on a Computer**

## **Task 1: Viewing System Information**

## **Task 2: Perform Data Acquisition**

## **Task 3: Create Disk Image**

## **Task 4: Use Nigilant32 to Preview the Hard Disk**

## **Task 5: Examine a File**

## **Task 6: Recovering Deleted Files**

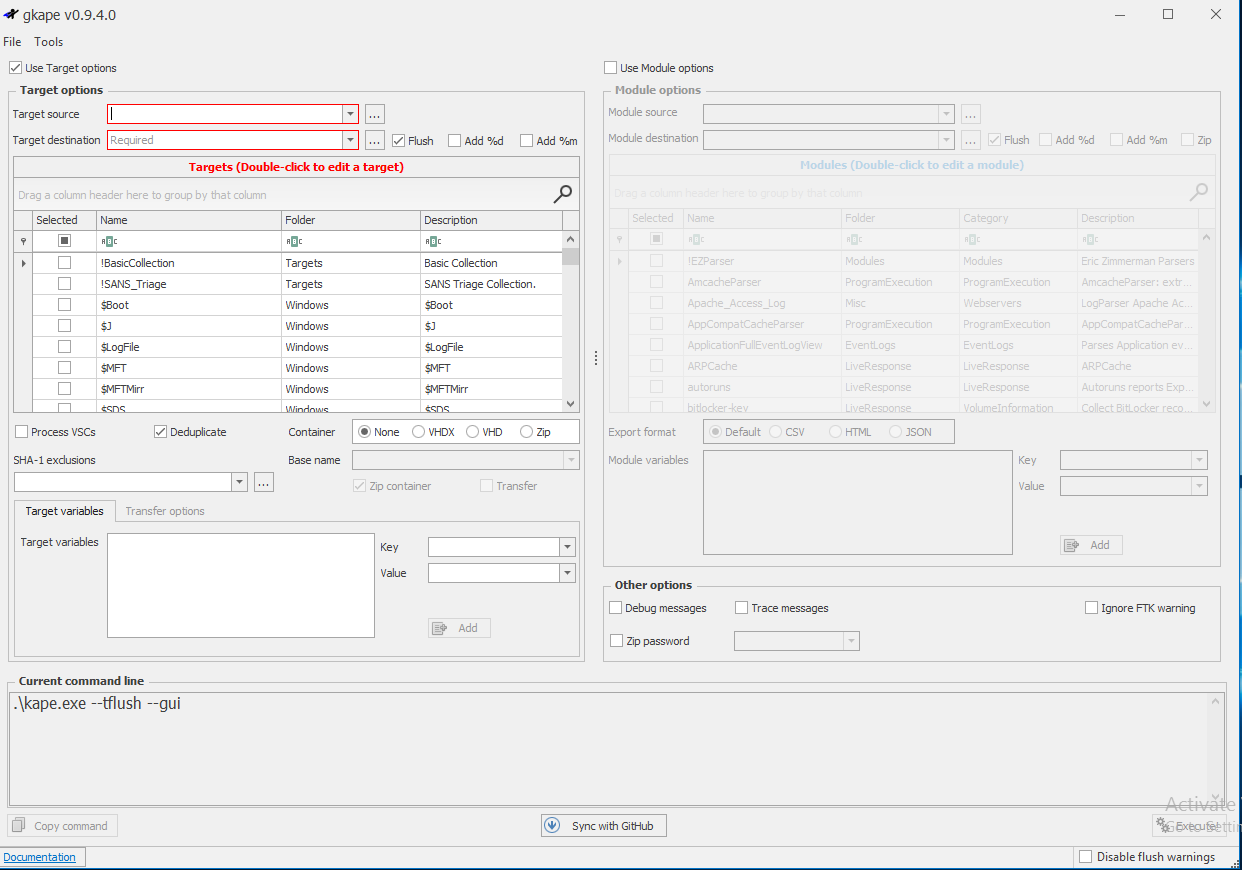
## **Task 7: Browsing Contents on a Hard Drive**

## **Task 8: Scanning for Pictures**

# **Lab 8: Collecting and Parsing Forensic Artifacts on a Live Windows Machine**

## **Task 1: Open Kape and Explore Its Components**

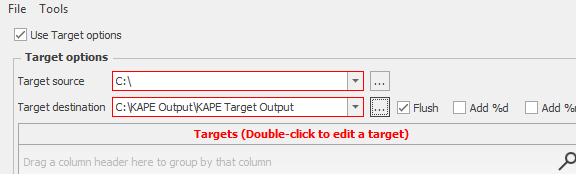
* 1. Trong lab này, chúng tôi sẽ trình bày cách thực hiện thu thập và xử lý hiện vật trực tiếp thông qua công cụ KAPE.
  2. Trước khi bắt đầu bài lab này, hãy đảm bảo rằng bạn đã cài đặt ứng dụng Microsoft Office trên máy của mình.
  3. Đăng nhập vào máy ảo Windows Server 2016.
  4. Mở File Explorer, điều hướng đến C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\ Windows Forensics Tools\KAPE và nhấp đúp vào gkape.exe.
  5. GUI KAPE xuất hiện, như trong ảnh chụp màn hình bên dưới:
  6. Trước khi tiến hành lab, điều quan trọng cần lưu ý là các thành phần khác nhau của công cụ. Phía trên bên trái có một mục có tên Sử dụng tùy chọn Mục tiêu. Khi mục nhập đó được chọn, nó sẽ bật tất cả các tùy chọn Mục tiêu được nhúng vào công cụ, như minh họa trong ảnh chụp màn hình bên dưới
  7. Khi kiểm tra mục Sử dụng tùy chọn Mục tiêu, chúng tôi thấy các trường và tùy chọn sau được bật trên công cụ:
     1. Nguồn mục tiêu: Tại đây, bạn có thể chỉ định ký tự ổ đĩa mà bạn muốn thu thập các tệp từ đó. Trong lab này, chúng tôi sẽ chọn C: hoặc ổ đĩa hệ thống
     2. Đích đích: Đây là vị trí lưu trữ các tệp đã thu thập. Đối với bộ sưu tập trực tiếp, nó thường bao gồm đường dẫn đến ổ đĩa ngoài. Tuy nhiên, vì đây là kịch bản alab, chúng tôi sẽ lưu các kết quả đầu ra của công cụ trong chính ổ C:.
     3. Mục tiêu: Đây là vị trí mà từ đó bạn có thể chọn các loại tệp mà công cụ sẽ thu thập. Nó bao gồm một danh sách đầy đủ các Mục tiêu mà bạn có thể chọn và chỉnh sửa theo yêu cầu của từng trường hợp.
     4. Loại bỏ trùng lặp: Với tùy chọn này được chọn, KAPE sẽ xóa mọi tệp trùng lặp bằng cách khớp các giá trị băm SHA 1 của chúng. Tùy chọn này đã được chọn theo mặc định.
     5. Bộ chứa: Trường này xác định định dạng mà tệp sẽ được thu thập. Các định dạng có sẵn để sử dụng là VDHX, VHD và Zip.
     6. Xóa: Tùy chọn này xóa hoặc xóa nội dung của Đích đích trước khi thu thập bất kỳ dữ liệu nào. Tùy chọn này được kiểm tra theo mặc định.
  8. Ngay bên cạnh các tùy chọn Mục tiêu là một mục có tên Sử dụng các tùy chọn Mô-đun. Khi bật mục nhập này, bạn sẽ thấy tất cả các tùy chọn Mô-đun được nhúng trong công cụ, như minh họa trong ảnh chụp màn hình bên dưới



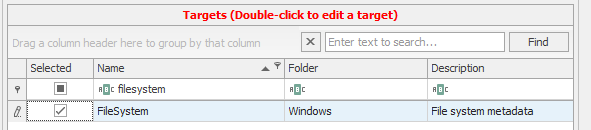
* 1. Khi kiểm tra mục Sử dụng tùy chọn Mô-đun, chúng tôi thấy các phần và tùy chọn Mô-đun sau được bật trên công cụ:
     1. Nguồn mô-đun: Ở đây, đường dẫn của Đích đích nơi bạn đã sao chép các tệp phải được đề cập.
     2. Đích mô-đun: Tại đây, đường dẫn thư mục sẽ được chỉ định nơi lưu các bản sao được phân tích cú pháp của các tệp Đích.
     3. Mô-đun: Phần này chứa tên của các Mô-đun thuộc về các tệp thực thi cụ thể, sử dụng các tệp Mục tiêu đã chọn sẽ được phân tích cú pháp. Các tệp thực thi này được lưu trữ trong thư mục bin của công cụ KAPE
     4. Xả: Tùy chọn Xả được chọn theo mặc định. Nó xóa nội dung của đích Đích/Mô-đun trước khi lưu trữ/phân tích cú pháp bất kỳ dữ liệu nào.
     5. Định dạng xuất: Phần này chỉ định định dạng mà dữ liệu được phân tích cú pháp sẽ được tạo. Tùy chọn mặc định là định dạng CSV, cùng với HTML và JSON.
  2. Ngay bên dưới các tùy chọn Mục tiêu và Tùy chọn Mô-đun, bạn sẽ thấy phần Dòng lệnh hiện tại và các nút khác:
     1. Dòng lệnh hiện tại: Đây là phần dòng lệnh của công cụ. Bất kỳ lệnh nào được cung cấp trong công cụ đều được ghi lại trong phần này.
     2. Sao chép lệnh: Nút này giúp sao chép lệnh từ dòng lệnh hiện tại và chạy nó trên Command Prompt.
     3. Đồng bộ hóa với GitHub: Nhấp vào nút này sẽ rút ra các Mục tiêu và Mô-đun được cập nhật từ kho lưu trữ GitHub. Tuy nhiên, các tệp thực thi cần thiết cần phải được tải xuống và đặt vào thư mục KAPE/bin theo cách thủ công.
     4. Thực thi!: Khi chọn tất cả các Mục tiêu/Mô-đun mong muốn và đặt đường dẫn thư mục cho các nguồn và đích của Mục tiêu và Mô-đun, bạn có thể nhấp vào nút Thực thi! nút để thực hiện lệnh

## **Task 2: Create Target and Module Destination Folders and Acquire Target Files**

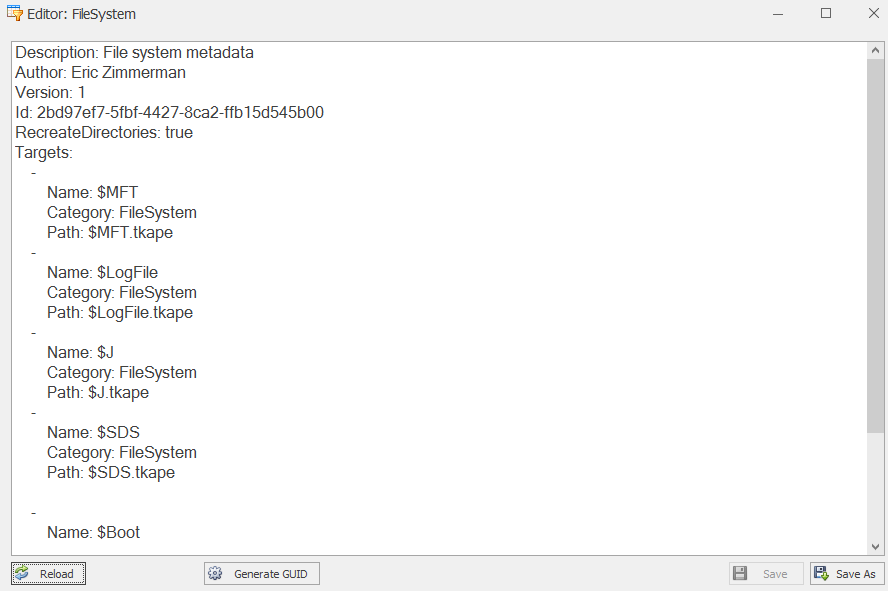
* 1. Bây giờ, chúng ta cần tạo các thư mục đích Mục tiêu và Mô-đun, các thư mục này sẽ được yêu cầu khi chạy công cụ.
  2. Thu nhỏ cửa sổ KAPE GUI. Mở File Explorer, điều hướng đến This PC Local Drive (C:) và tạo một thư mục mới có tên KAPE Output.
  3. Bây giờ, vào bên trong thư mục KAPE Output. Tạo hai thư mục có tên là Đầu ra mục tiêu KAPE (thư mục này sẽ được sử dụng làm đích Mục tiêu) và Đầu ra mô-đun KAPE (thư mục này sẽ được sử dụng làm đích Mô-đun)
  4. Bây giờ, chúng ta có thể tạo tệp Target bằng cách sao chép tệp từ máy. Để làm như vậy, hãy quay lại cửa sổ KAPE GUI.
  5. Đảm bảo rằng mục Sử dụng tùy chọn Mục tiêu được chọn. Để chọn thư mục nguồn Đích, bấm vào Dấu ba chấm (...) bên cạnh.



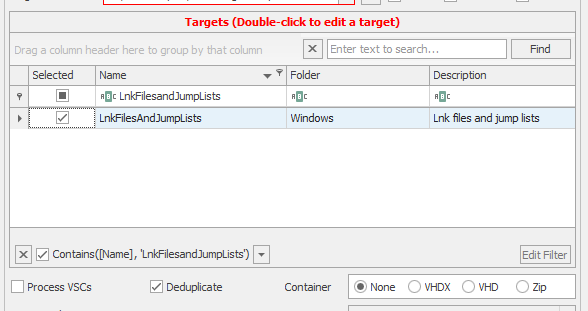
* 1. Cửa sổ Browse for Folder xuất hiện. Chọn Đĩa cục bộ (C:) và Nhấp vào OK.
  2. Tương tự, để đặt thư mục Đích đến, nhấp vào nút Dấu ba chấm (...) bên cạnh. Khi cửa sổ Browse For Folder xuất hiện, điều hướng đến Local Disk (C:) KAPE Output KAPE Target Output. Sau khi hoàn tất, bấm OK.
  3. Trong phần Mục tiêu, chúng tôi sẽ chọn Mục tiêu liên quan đến Hệ thống tệp, tệp LNK và Danh sách nhảy. Để tìm các Mục tiêu liên quan đến Hệ thống tệp, hãy đặt con trỏ bên dưới trường Tên bên cạnh các chữ cái RBC và nhập Hệ thống tệp. Sau khi tìm thấy mục Mục tiêu có tên Hệ thống tệp, hãy chọn hộp kiểm được liên kết với mục đó.
  4. Bây giờ, nhấp đúp vào mục Target có tên FileSystem để xem nội dung của nó hoặc chỉnh sửa nó



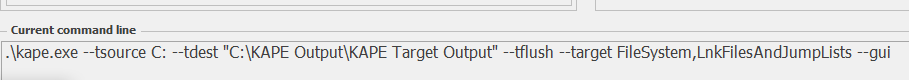
* 1. Cửa sổ Editor: FileSystem mở ra, như minh họa trong ảnh chụp màn hình bên dưới:



* 1. Tại đây, bạn có thể thấy các tệp trong hệ thống tệp NTFS mà Mục tiêu đã chọn sẽ sao chép:
     1. $MFT: Còn được gọi là Bảng tệp chính, tệp này chứa một loạt thuộc tính cho từng tệp trong hệ thống tệp được chỉ định và có giá trị pháp lý tối đa.
     2. $LogFile: Tệp này theo dõi các thay đổi được thực hiện trong hệ thống tệp NTFS
     3. $J: Tệp này là một phần của tệp $UsnJrnl, bao gồm nội dung của nhật ký thay đổi.
     4. $SDS: Còn được gọi là Luồng mô tả bảo mật, tệp này lưu trữ danh sách tất cả các Bộ mô tả bảo mật trong ổ đĩa NTFS.
     5. $Boot: Đây là bản sao tệp của khu vực khởi động của ổ đĩa NTFS được chỉ định.
     6. $T: Tệp này thuộc dữ liệu tệp TxF Old Page Stream (TOPS). Nó bao gồm luồng dữ liệu $T, chứa dữ liệu về các tệp bị ghi đè một phần.
  2. Đóng cửa sổ Editor: FileSystem. Bây giờ, trong phần Mục tiêu, xóa ô RBC, nhập LnkFilesAndJumpLists và chọn hộp kiểm được liên kết với LnkFilesAndJumpLists. Mục Mục tiêu này sẽ sao chép các tệp LNK và Danh sách Nhảy từ ổ đĩa được chỉ định
  3. Đảm bảo rằng các tùy chọn Xóa trùng lặp và Xóa trùng lặp được chọn và giữ cho Vùng chứa được chọn là Không có



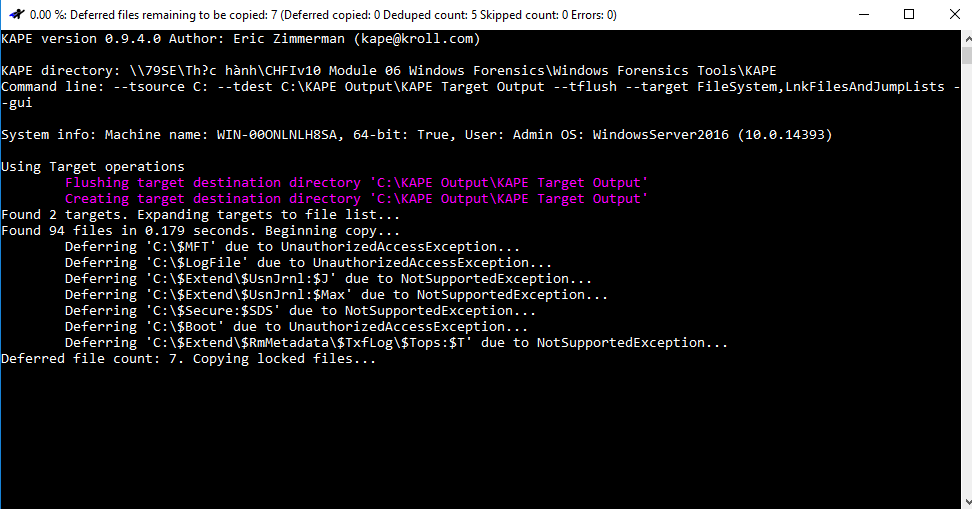
* 1. Khi cả hai mục Mục tiêu được chọn, phần Dòng lệnh hiện tại sẽ xuất hiện như trong ảnh chụp màn hình sau

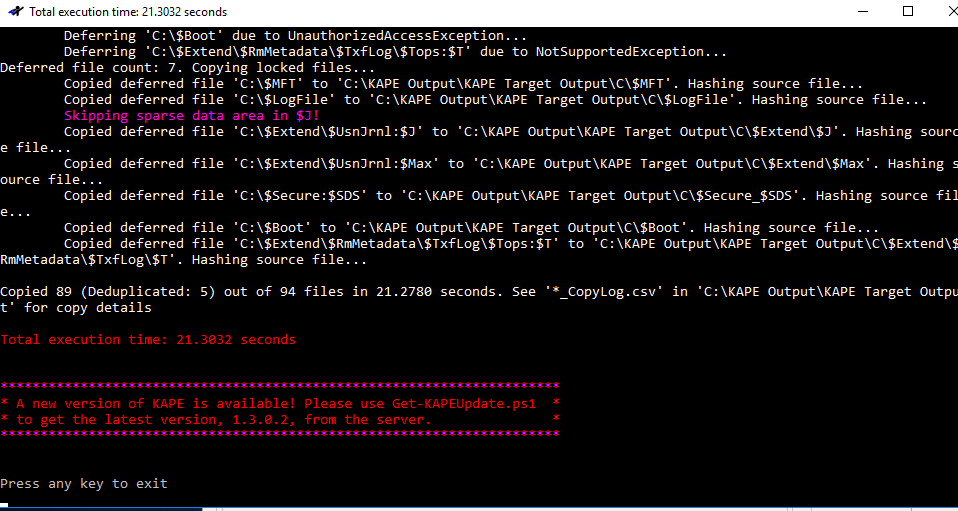


* 1. Trong phần được tô sáng của ảnh chụp màn hình ở trên, tham số --tsource chỉ định thư mục nguồn Đích và tham số --tdest xác định đường dẫn của thư mục đích Đích. Tham số --tflush cho biết rằng tùy chọn Flush đã được chọn, tham số --target hiển thị các mục Mục tiêu đã chọn và tham số --gui cho biết rằng lệnh sẽ được thực thi bằng GUI của công cụ.
  2. Khi tất cả các tùy chọn Mục tiêu đã được định cấu hình, hãy nhấp vào nút Thực thi! Cái nút

Lưu ý: Nếu có CẢNH BÁO PHÁ HỦY DỮ LIỆU! cửa sổ hiện ra, nhấn OK để tiếp tục.

* 1. Lúc này, công cụ sẽ mở một cửa sổ dòng lệnh hiển thị tiến trình của các tệp Mục tiêu được sao chép. Khi tất cả các tệp Mục tiêu đã chọn được sao chép vào thư mục Đích, công cụ sẽ nhắc bạn nhấn phím bất kỳ để thoát

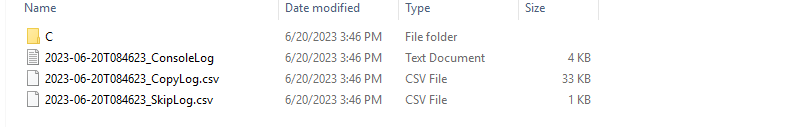




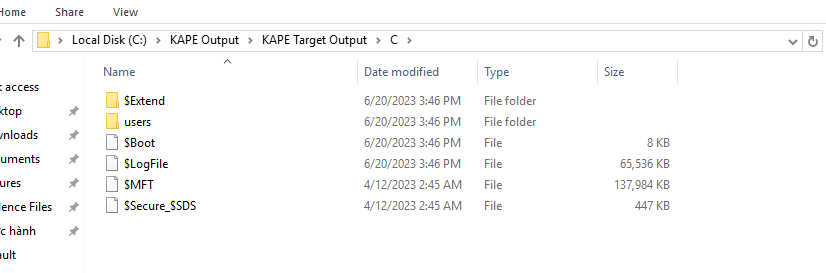
* 1. Nhấn phím bất kỳ để thoát khỏi cửa sổ dòng lệnh. Thu nhỏ cửa sổ ứng dụng KAPE.

## **Task 3: Check the Acquired Target Files in Target Destination Folder**

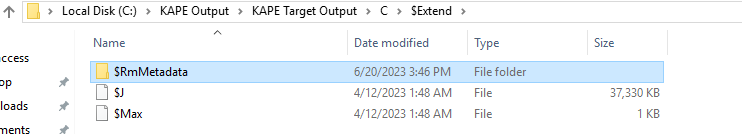
* 1. Bây giờ, hãy mở File Explorer và điều hướng đến C:\KAPE Output\KAPE Target Output. Bạn sẽ thấy một thư mục có tên C, cùng với ba tệp, như trong ảnh chụp màn hình bên dưới



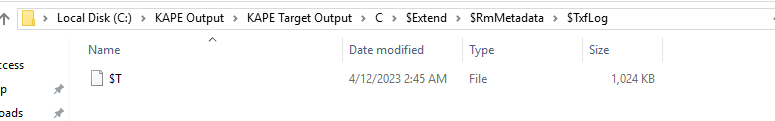
* 1. Tất cả các tệp trong phần được tô sáng của ảnh chụp màn hình ở trên đều bắt đầu bằng ngày mà các tệp Mục tiêu được sao chép từ máy, theo sau là một số ký tự chữ và số. Tệp 2020-10-16T181354\_ConsoleLog.txt chứa thông tin giống như thông tin được hiển thị trong cửa sổ dòng lệnh, tệp 2020-10-16T181354\_CopyLog.csv bao gồm thông tin về các tệp Mục tiêu đã được sao chép và tệp 2020-10- 16T181354\_SkipLog.csv bao gồm thông tin về các tệp Mục tiêu đã bị công cụ bỏ qua trong các thao tác Mục tiêu.
  2. Để xem các mục đã sao chép, nhấp đúp vào Cfolder. Bạn sẽ thấy một số tệp đã sao chép, cụ thể là $Boot, $LogFile, $MFT và $Secure\_$SDS và hai thư mục: $Extend và người dùng.



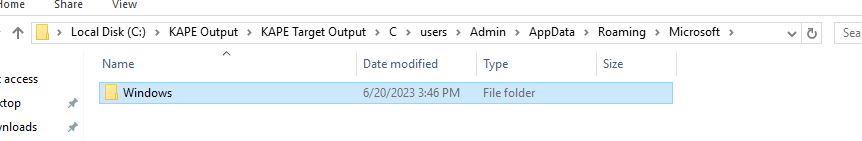
* 1. Bạn cũng sẽ thấy các tệp $J và $Max cũng như thư mục có tên $RmMetadata khi nhấp đúp vào thư mục $Extend.



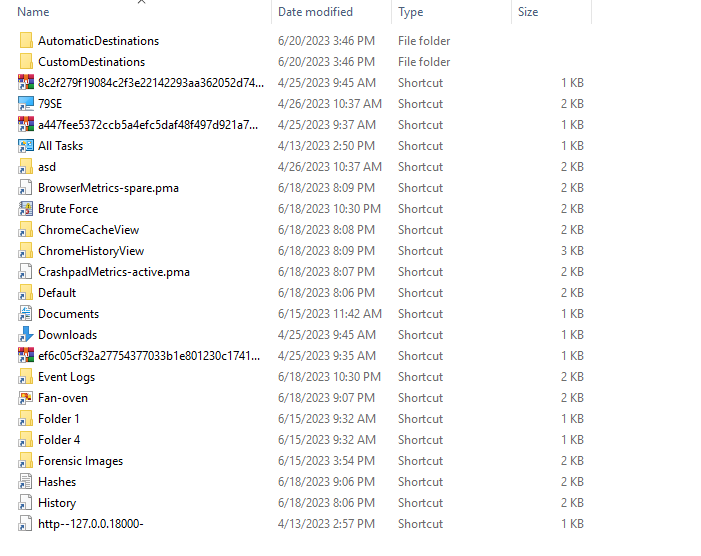
* 1. Bây giờ, điều hướng đến $RmMetadata -> $TxfLog. Bạn sẽ thấy tệp $T ở đó



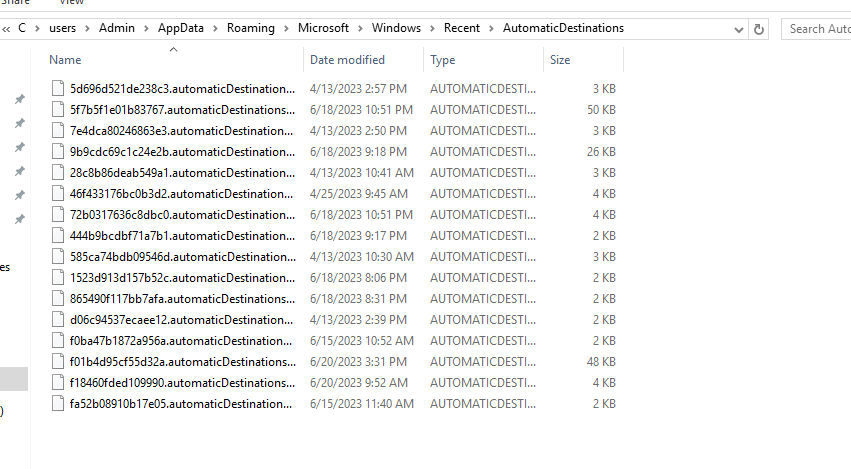
* 1. Trở lại thư mục C bên trong thư mục KAPE Target Output. Bây giờ, điều hướng đến users\Administrator\AppData\Roaming\Microsoft. Bạn sẽ thấy hai thư mục ở đó: Office và Windows.

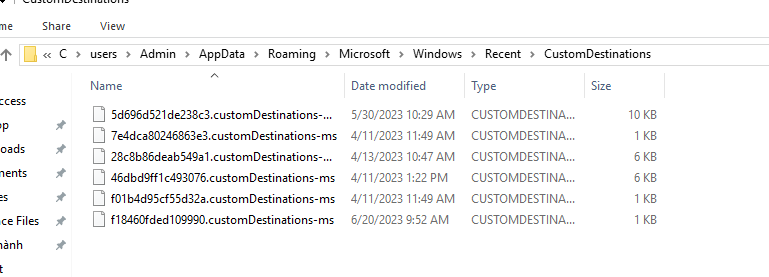


* 1. Trong đường dẫn C:\KAPE Output\KAPE Target Output\C\users\Administrator\AppData\Roaming\Microsoft\Office\Rec ent, bạn sẽ thấy danh sách các tệp LNK được sao chép từ máy của bạn



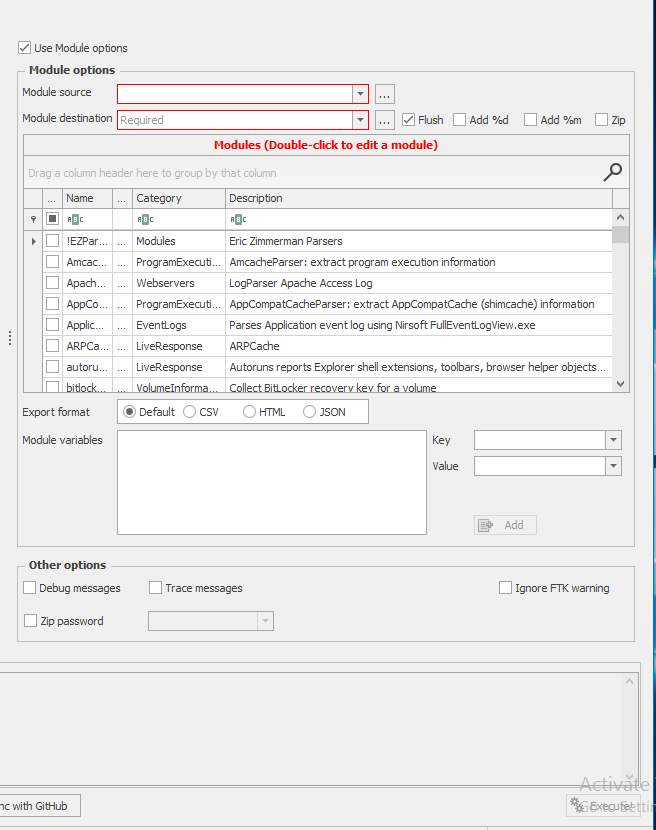
* 1. Bây giờ, quay lại thư mục Microsoft và điều hướng đến Windows\Recent. Bạn sẽ thấy hai thư mục có tên AutomaticDestinations và CustomDestinations (A) chứa danh sách tất cả các tệp Jump List, cùng với danh sách các tệp LNK (B).
  2. Vào cả hai thư mục AutomaticDestination và CustomDestination để xem danh sách các tệp Jump List đã sao chép, như thể hiện trong ảnh chụp màn hình sau:



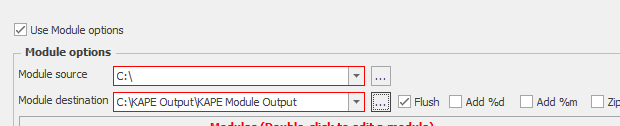


## **Task 4: Parse the Acquired Target Files in the Module Section in KAPE**

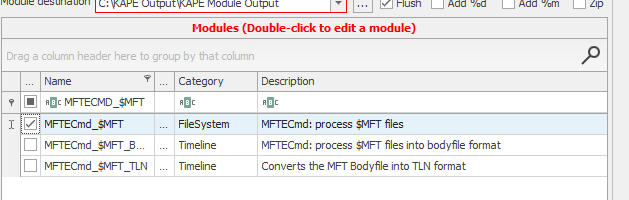
* 1. Vì các tệp Mục tiêu đã chọn đã được mua, bây giờ chúng tôi sẽ sử dụng cùng một ứng dụng để phân tích các tệp này và kiểm tra nội dung của chúng. Để làm như vậy, hãy tối đa hóa cửa sổ KAPE GUI.
  2. Đảm bảo rằng bạn đã bỏ chọn tùy chọn Sử dụng mục tiêu ở góc trên cùng bên trái của công cụ. Điều này sẽ vô hiệu hóa tất cả các tùy chọn Mục tiêu. Bây giờ, hãy nhấp vào Sử dụng tùy chọn Mô-đun để kích hoạt nó, như thể hiện trong ảnh chụp màn hình bên dưới:
  3. Bây giờ, hãy nhấp vào nút Dấu ba chấm (...) bên cạnh Nguồn mô-đun để chọn nguồn



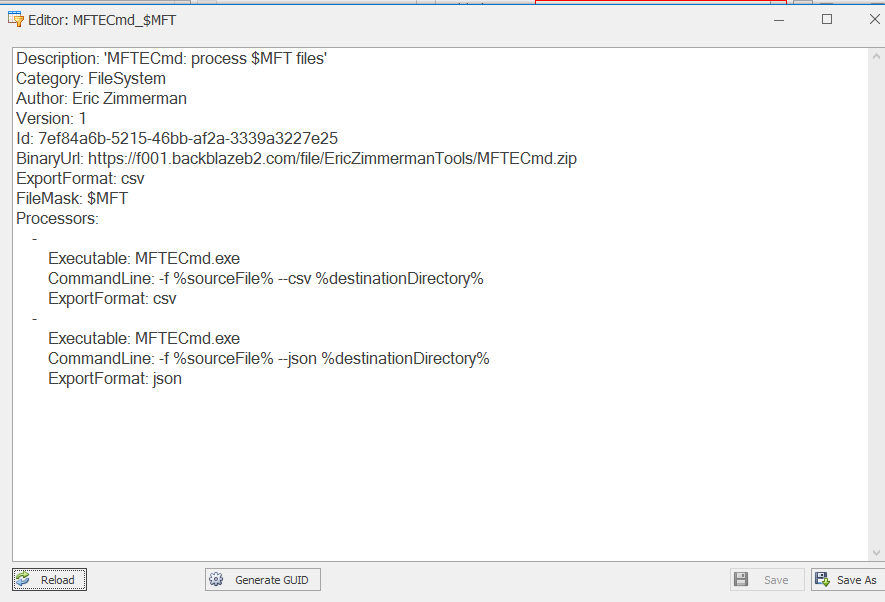
* 1. Cửa sổ Browse for Folder xuất hiện. Điều hướng đến Ổ đĩa cục bộ (C:) KAPE Output KAPE Target Output và chọn nó. Điều này sẽ cho phép bạn phân tích cú pháp các tệp Mục tiêu đã thu được. Sau khi cấu hình, bấm OK.
  2. Bây giờ hãy nhấp vào nút Dấu ba chấm (...) bên cạnh Điểm đến mô-đun



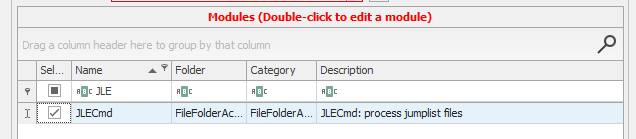
* 1. Trên cửa sổ Browse for Folder xuất hiện tiếp theo, điều hướng đến Local Drive (C:) -> KAPE Output -> KAPE Module Output, chọn nó và nhấn OK
  2. Bây giờ, chúng tôi sẽ chọn Mô-đun từ phần Mô-đun, sử dụng phần mà chúng tôi muốn phân tích các tệp Mục tiêu của mình. Trong lab này, chúng tôi sẽ trình bày cách phân tích cú pháp tệp Mục tiêu $MFT, cùng với các tệp LNK và Danh sách Nhảy có được trong thư mục Đầu ra Mục tiêu KAPE.
  3. Để phân tích tệp $MFT Target, chúng tôi sẽ chọn một Mô-đun có tên MFTECmd\_$MFT. Vì vậy, trong phần Mô-đun, hãy đặt con trỏ bên dưới phần Tên bên cạnh các chữ cái RBC và nhập MFTECmd\_$MFT. Khi Mô-đun có cùng tên xuất hiện, hãy chọn hộp kiểm được liên kết với mô-đun, như minh họa trong ảnh chụp màn hình bên dưới
  4. Bây giờ, nhấp đúp vào mô-đun MFTECmd\_$MFT để xác định tệp thực thi nào sẽ chạy qua Mô-đun để phân tích cú pháp tệp Mục tiêu $MFT.



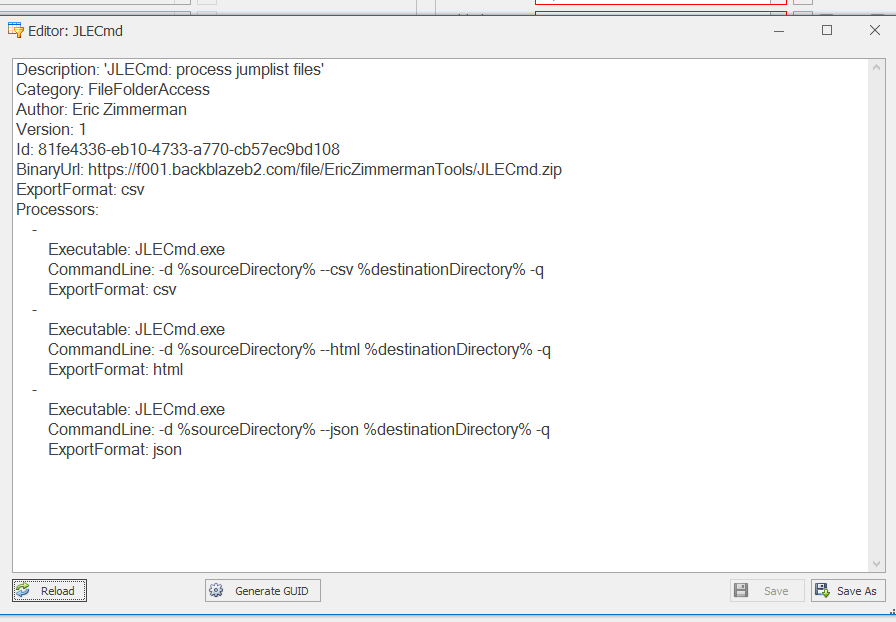
* 1. Cửa sổ Editor: MFTECmd\_$MFT mở ra. Nó cho thấy rằng Mô-đun đã chọn sẽ sử dụng tệp MFTECmd.exe để phân tích cú pháp tệp $MFT, cùng với Dòng lệnh và Định dạng xuất khẩu.



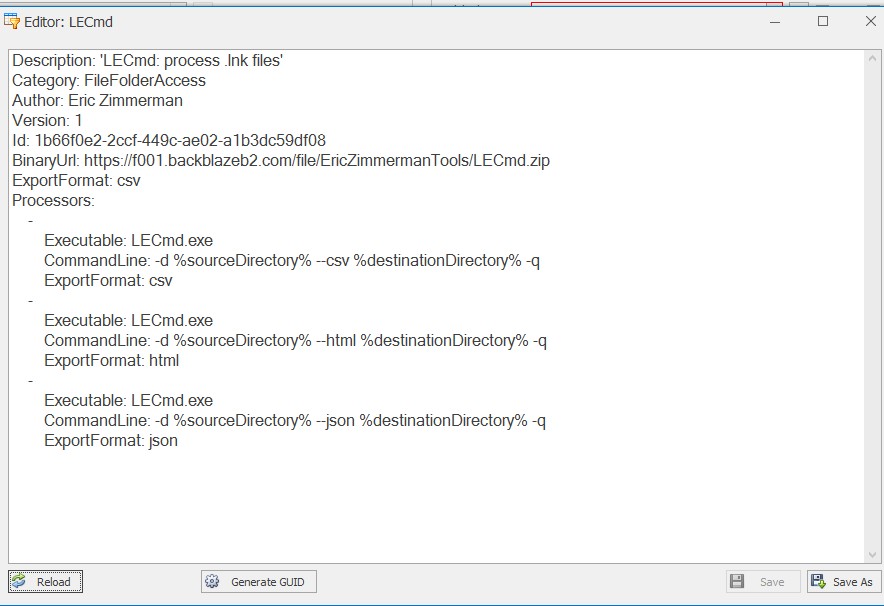
* 1. Đóng cửa sổ MFTECmd\_$MFT. Bây giờ, chúng tôi sẽ chọn một Mô-đun để phân tích Danh sách Nhảy được lưu trữ trong thư mục Đầu ra Mục tiêu KAPE. Đối với Danh sách Nhảy, hãy nhập JLECmd. Một mục Mô-đun có cùng tên sẽ xuất hiện. Chọn hộp kiểm được liên kết với mô-đun rồi bấm đúp vào nó để xem tên của tệp thực thi có trong Mô-đun đó.



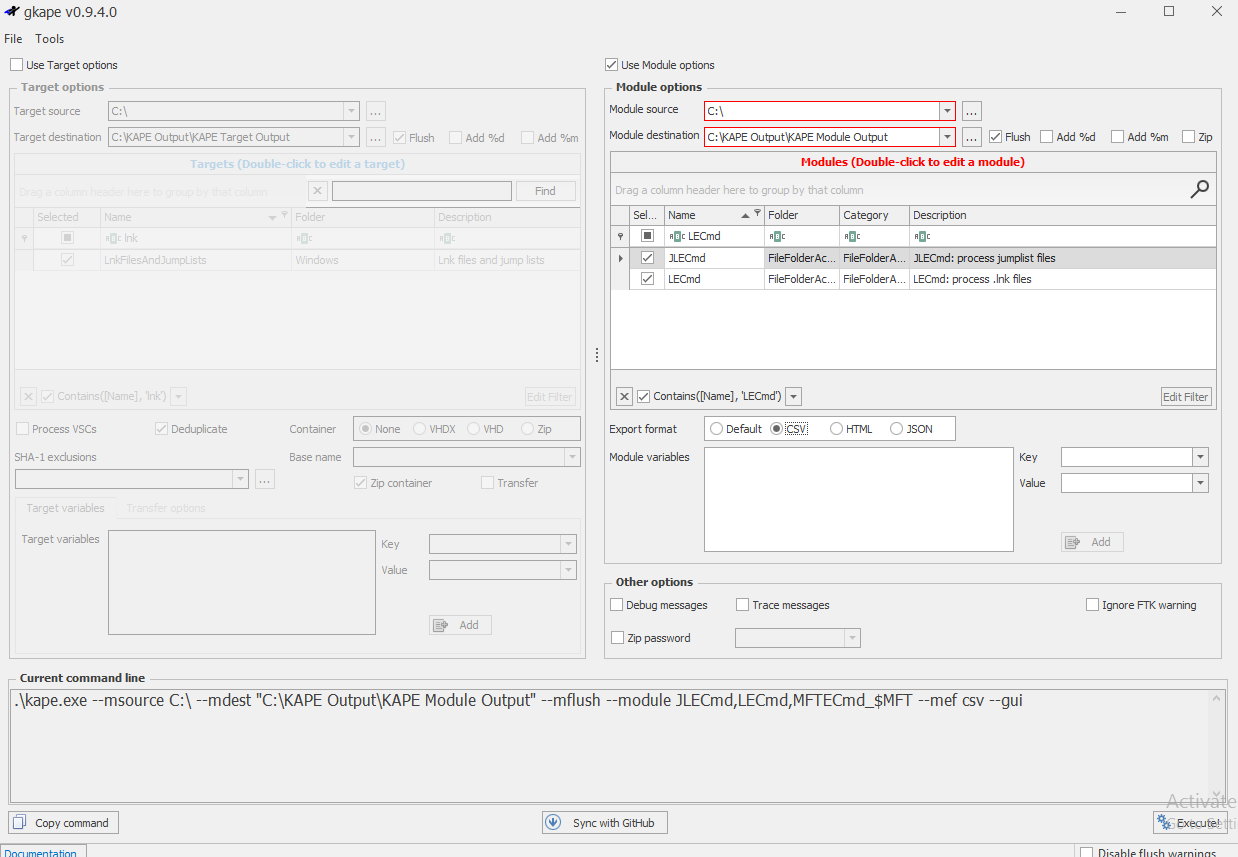
* 1. Cửa sổ Editor: JLECmd mở ra. Nó cho thấy rằng tên thực thi được sử dụng để phân tích cú pháp các tệp Danh sách nhảy là JLECmd.exe, cùng với Dòng lệnh và Định dạng xuất khẩu.



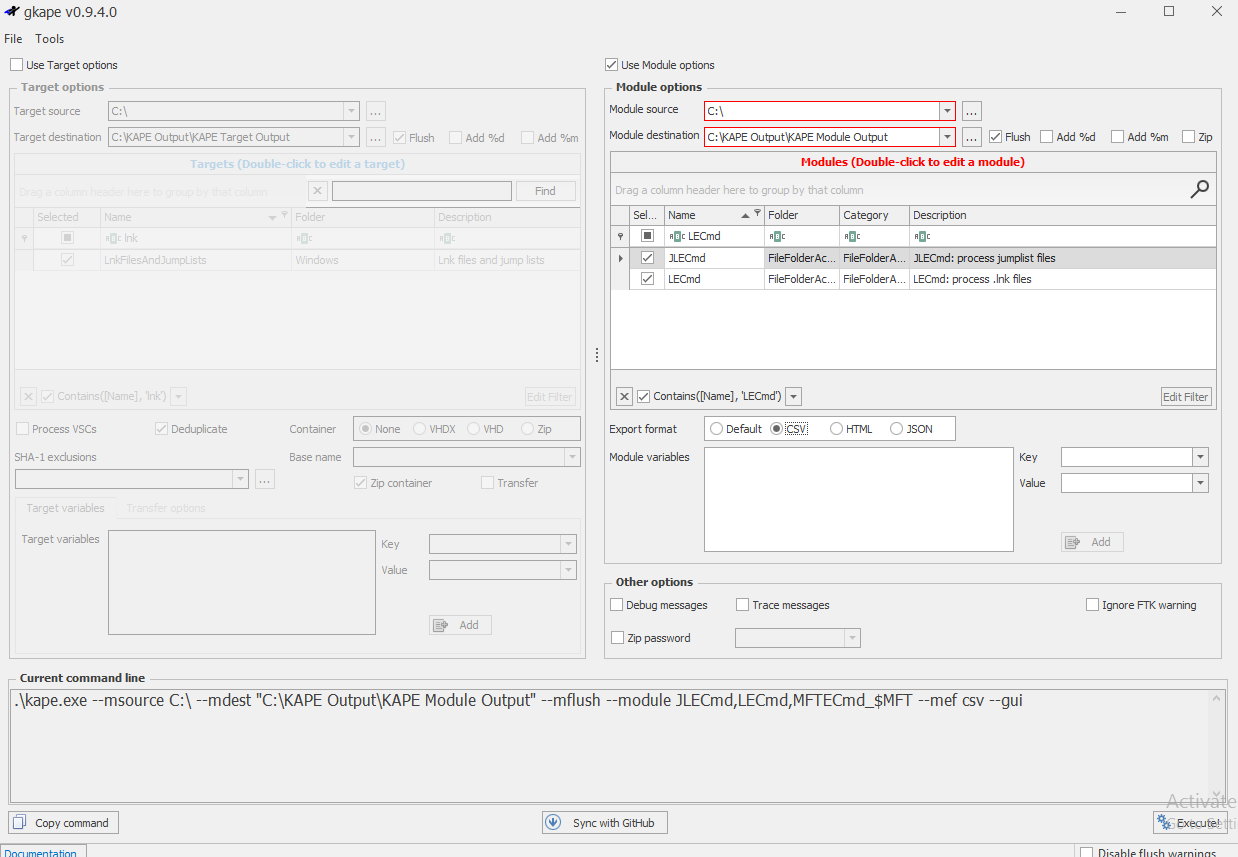
* 1. Đóng cửa sổ Editor: JLECmd. Nhập LECmd và chọn hộp kiểm cho mục nhập Mô-đun có cùng tên khi nó xuất hiện. Bây giờ, bấm đúp vào mục nhập. Mô-đun này sẽ được sử dụng để phân tích cú pháp các tệp LNK trong thư mục KAPE Target Output
  2. Cửa sổ Editor: LECmd xuất hiện hiển thị tên thực thi là LECmd.exe, cùng với CommandLine và ExportFormat



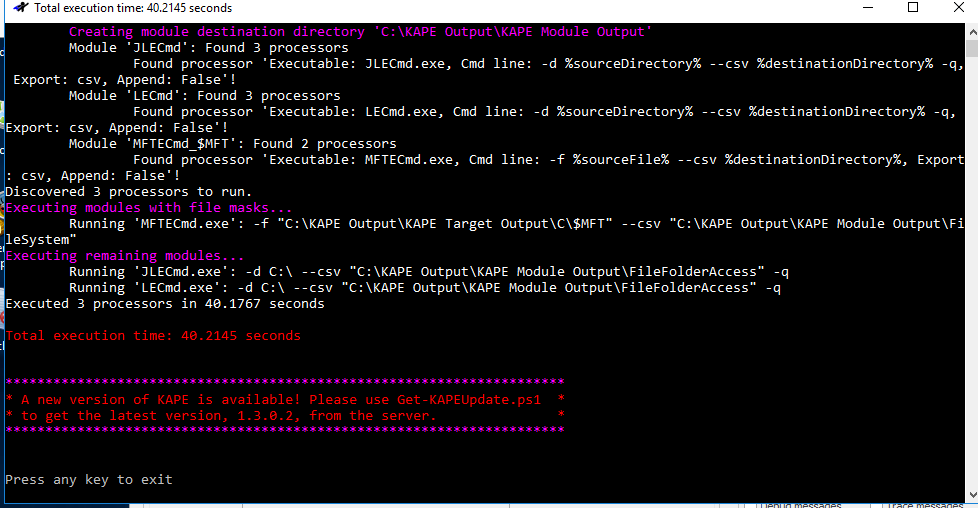
* 1. Đóng cửa sổ Editor: LECmd. Tất cả các Mô-đun cần thiết đều được chọn. Đảm bảo rằng tùy chọn Xóa được chọn và chọn CSV làm định dạng Xuất như trong ảnh chụp màn hình bên dưới:



* 1. Với tất cả các cấu hình được thực hiện trong phần Mô-đun, dòng lệnh Hiện tại sẽ như sau



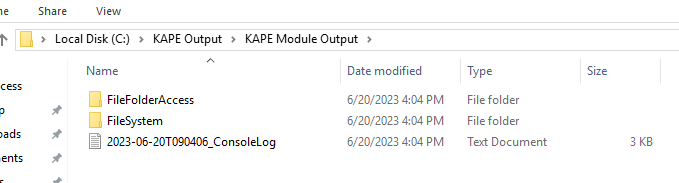
* 1. Trong phần được đánh dấu của Dòng lệnh hiện tại như minh họa ở trên, tham số - -msource phản ánh đường dẫn của thư mục nguồn Mô-đun đã chọn, tham số --mdest hiển thị đường dẫn của thư mục đích Mô-đun đã chọn, --mflush cho biết rằng nội dung của thư mục đích Mô-đun đã chọn sẽ bị xóa trước khi phân tích cú pháp, tham số --module hiển thị các Mô-đun được chọn, tham số --mef hiển thị định dạng Xuất được chọn và --gui hiển thị rằng dòng lệnh sẽ được thực thi thông qua giao diện KAPE.
  2. Sau khi đã định cấu hình và xem lại, nhấp vào nút Thực thi! cái nút.
  3. Bây giờ, công cụ sẽ mở một cửa sổ dòng lệnh hiển thị tiến trình của các Mô-đun đang chạy đối với các tệp Mục tiêu được lưu trữ trong thư mục Đầu ra Mục tiêu KAPE. Khi phân tích cú pháp xong, công cụ sẽ nhắc bạn nhấn phím bất kỳ để thoát khỏi cửa sổ dòng lệnh



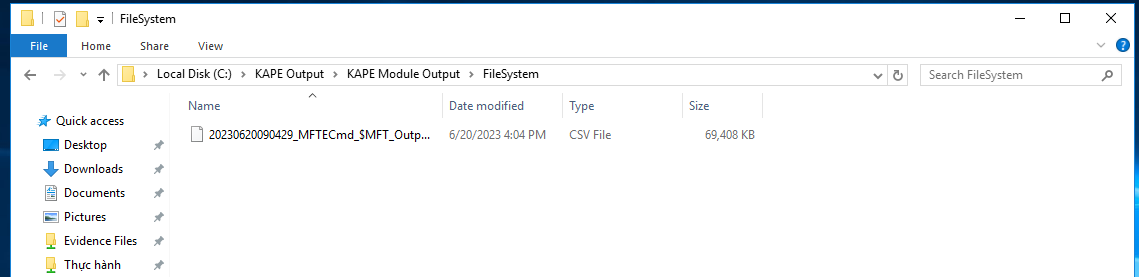
* 1. Nhấn phím bất kỳ và nhấn Enter để thoát khỏi cửa sổ dòng lệnh. Thu nhỏ cửa sổ KAPE GUI

## **Task 5: Examine the Parsed Files Stored in the Module Destination Folder**

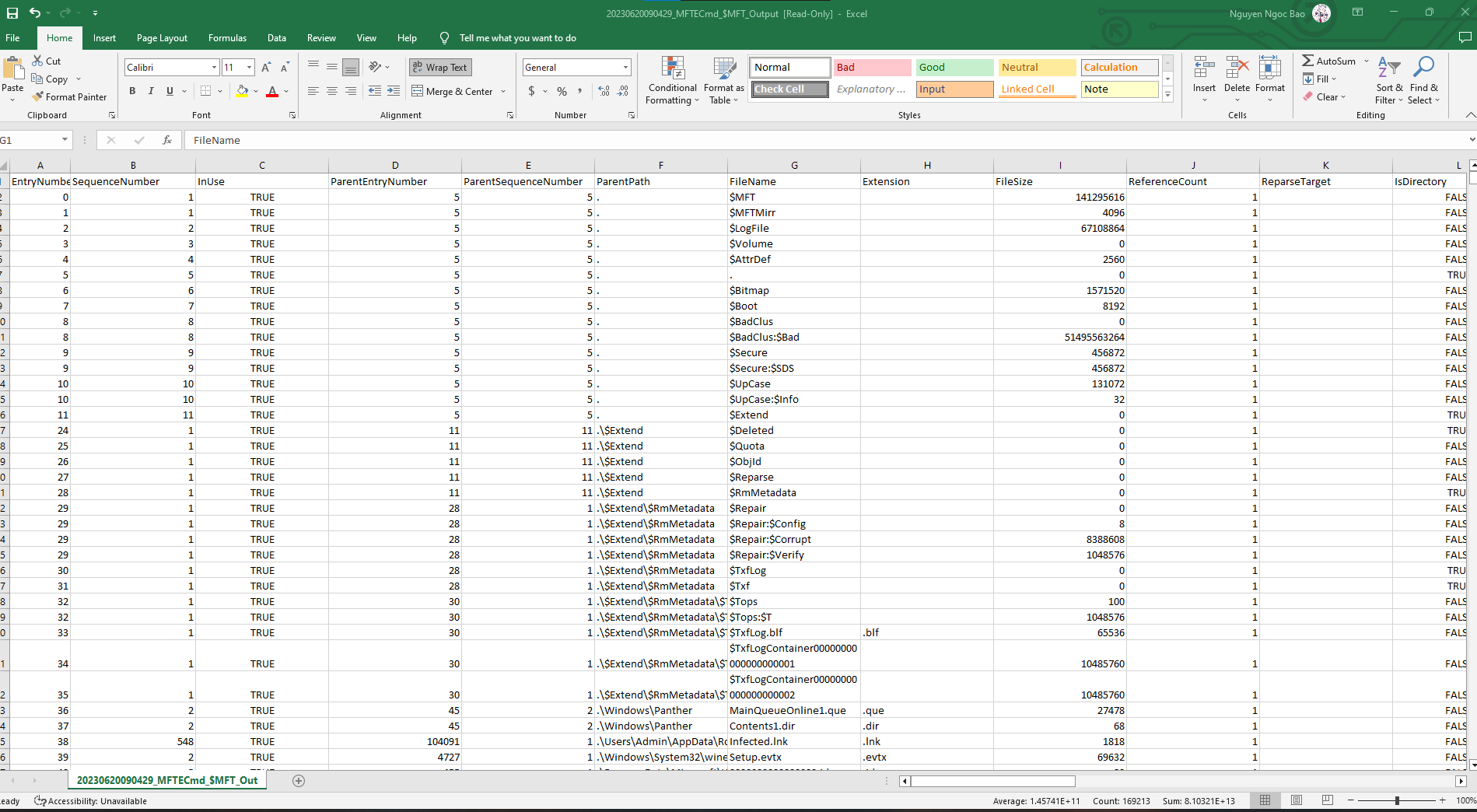
* 1. Bây giờ, hãy mở File Explorer và điều hướng đến C:\KAPE Output\KAPE Module Output. Bạn sẽ thấy hai thư mục: FileFolderAccess và FileSystem, cùng với một tệp văn bản có tên 2020-10-16T182016\_ConsoleLog.txt, như minh họa trong ảnh chụp màn hình bên dưới



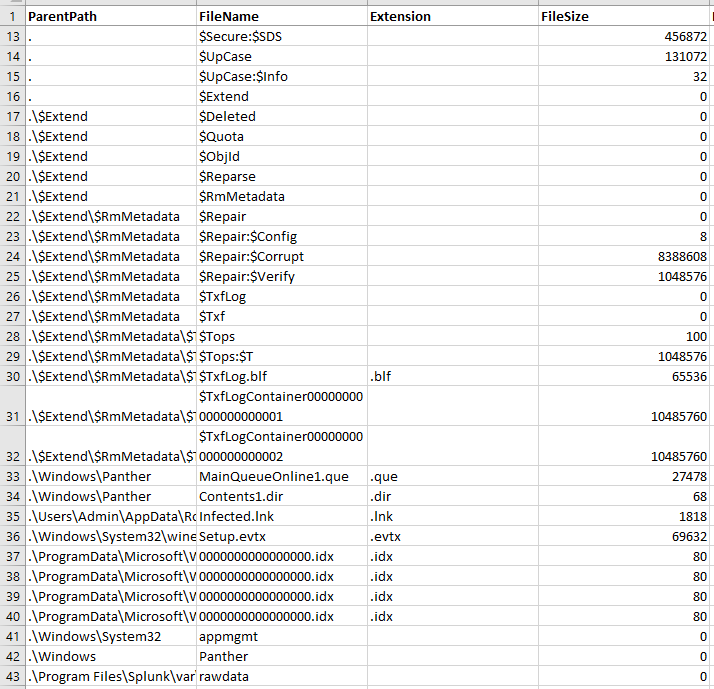
* 1. Nhấp đúp vào thư mục FileSystem và bạn sẽ thấy tệp có tên 20201016182035\_MFTECmd\_$MFT\_Output.csv. Đây là tệp CSV được tạo sau khi phân tích cú pháp tệp Mục tiêu $MFT



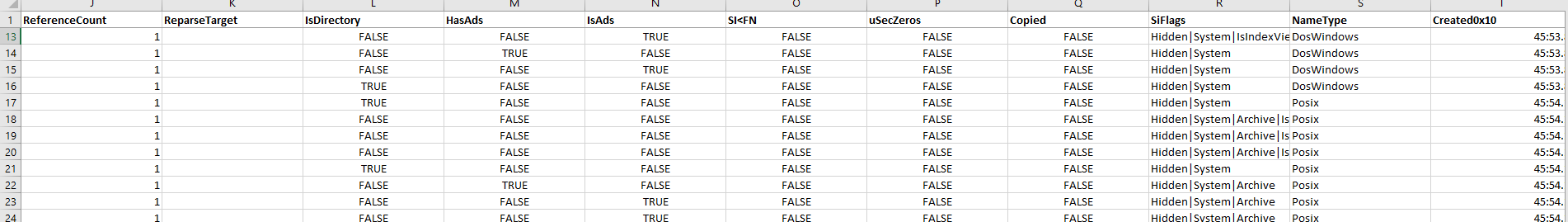
* 1. Nhấp đúp vào tệp CSV để mở và xem nội dung của nó



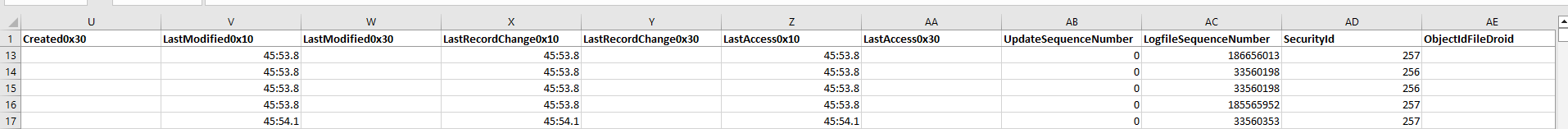
* 1. Chọn toàn bộ hàng trên cùng, chuyển đến tab Lượt xem, nhấp vào Freeze Panes và chọn Freeze Top Row từ trình đơn thả xuống.
  2. Đảm bảo rằng hàng trên cùng được chọn. Bây giờ, hãy quay lại Tab Trang chủ. Nhấp vào Bicon để xem hàng trên cùng được in đậm.
  3. Cuộn xuống để xem tất cả các tệp bên trong các tệp $MFT. Kéo thanh cuộn ngang sang bên phải để tìm nhiều mục nhập đáng chú ý về các tệp được phản ánh trong tệp $MFT đã phân tích cú pháp, chẳng hạn như ParentPath (A) hoặc vị trí của chúng trong hệ thống tệp NTFS, Tên tệp hoặc tên của các tệp (B), Tiện ích mở rộng (C) và Kích thước tệp (D) của chúng



* 1. Khi kéo thanh cuộn ngang sang bên phải, bạn sẽ thấy Created0x10 (E) và Created0x30 (F), đại diện cho ngày và giờ tạo của bất kỳ tệp nào; LastModified0x10 (G) và LastModified0x30 (H), đại diện cho ngày và giờ sửa đổi lần cuối của bất kỳ tệp nào; và LastRecordChange0x10 (I) và LastRecordChange0x30 (J), đại diện cho ngày và giờ khi bất kỳ thay đổi nào được ghi lại trong bất kỳ tệp nào



* 1. Khi kéo thanh trượt ngang sang bên phải, bạn có thể quan sát các mục nhập khác như LastAccess0x10 (K) và LastAccess0x30 (L), đại diện cho ngày và giờ truy cập cuối cùng của bất kỳ tệp nào, cùng với UpdateSequenceNumber (M), LogFileSequenceNumber (N) và SecurityId (O)



* 1. Các mục nhập này rất quan trọng theo quan điểm forensic vì bạn có thể xác định và kiểm tra lần truy cập cuối cùng và thời gian sửa đổi của bất kỳ tệp cụ thể nào trong hệ thống tệp NTFS của máy nghi ngờ. Tệp $MFT cũng chứa thông tin về các tệp bị xóa và việc kiểm tra nó có thể giúp khôi phục các tệp đó
  2. Sau khi kiểm tra các mục nhập, hãy đóng tệp 20201016182035\_MFTECmd\_$MFT\_Output.csv.
  3. Trên File Explorer, điều hướng đến C:\KAPE Output\KAPE Module Output\FileFolderAccess và bạn sẽ thấy ba tệp .csv: 20201016112054\_AutomaticDestinations.csv và 20201016112055\_CustomDestinations.csv chứa thông tin về Danh sách nhảy được phân tích cú pháp và 20201016112056\_LECmd\_ Đầu ra.csv, mà chứa thông tin chi tiết về các tệp LNK được phân tích cú pháp từ thư mục KAPE Target Output
  4. Đầu tiên chúng ta sẽ kiểm tra các tệp Jump List trong tệp 20201016112054\_AutomaticDestination.csv. Bấm đúp vào tệp để mở và xem nội dung của nó.
  5. Một số mục nhập đáng chú ý được tìm thấy trong tệp 20201016112054\_AutomaticDestination.csv là SourceFile hoặc đường dẫn của nguồn Mô-đun (A), SourceCreated, SourceModified, SourceAccessed (B) thông tin APPId (C), đường dẫn của Danh sách nhảy mục tiêu (D) , Ngày và giờ TargetCreated, TargetModified và TargetAccessed (E) và Kích thước tệp (F), như minh họa trong ảnh chụp màn hình bên dưới
  6. Sau khi hoàn thành việc kiểm tra Danh sách nhảy trong AutomaticDestination, hãy đóng tệp .csv.
  7. Khi mở tệp 20201016112055\_CustomDestinations.csv, bạn sẽ nhận được loại thông tin tương tự như trong tệp 20201016112054\_AutomaticDestinations.csv.
  8. Kiểm tra tất cả Danh sách Nhảy trong 20201016112055\_CustomDestinations.csv và đóng tệp mà không lưu.
  9. Bây giờ, hãy mở tệp 20201016112056\_LECmd\_Output.csv. Bạn sẽ thấy các mục nhập đáng chú ý như SourceFile (A), SourceCreated, SourceModified và SourceAccessed–dấu thời gian liên quan (B), TargetCreated, TargetModified và TargetAccessed–liên quan đến Dấu thời gian (C), Kích thước tệp (D), Đường dẫn tương đối Mục tiêuMFTEntryNumber (E), TargetIDAbsolutePath ( F), (G), TargetMFTSequenceNumber (H), MachineID (I) và MachineMACAddress (J), như minh họa trong ảnh chụp màn hình bên dưới:
  10. Việc kiểm tra các mục này về tệp LNK và Danh sách nhảy có thể cung cấp thông tin hữu ích về các hoạt động của người dùng trên hệ thống.
  11. Do đó, bạn có thể sử dụng công cụ KAPE để thu thập và xử lý dữ liệu có giá trị về mặt pháp lý cũng như đẩy nhanh quá trình điều tra.