

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 02 (Session 02)

Tên chủ đề: Điều tra bộ nhớ lưu trữ (Hard Drive Forensics)

GVHD: Đoàn Minh Trung

Ngày báo cáo: 25/03/2024

Nhóm: 07

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đình Bảo Long	21522303	21522303@gm.uit.edu.vn
2	Nguyễn Tân Phát	21522447	21522447@gm.uit.edu.vn
3	Ngô Minh Thiên	21522623	21522623@gm.uit.edu.vn
4	Đào Vĩnh Thịnh	21522632	2152632@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Các câu hỏi trên lớp	100%
2	Kịch bản 01	100%
3	Kịch bản 02	100%
4	Kịch bản 03	100%
5	Kịch bản 04	100%
6	Kịch bản 05	100%
7	Kịch bản 06	100%

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành,

BÁO CÁO CHI TIẾT

Các câu hỏi yêu cầu:

Hard drive

Một ổ cứng (hard drive) là một thiết bị lưu trữ dữ liệu dùng để lưu trữ và truy cập vào các tệp tin và thông tin.

Có 2 loại:

- + Ổ cứng cơ học (hard disk drive - HDD)
- + Ổ cứng thể rắn (solid-state drive - SSD)

Partition

Một phân vùng (partition) là một phần hoặc một khu vực được xác định trên một ổ cứng hoặc thiết bị lưu trữ khác, được sử dụng để tổ chức và quản lý dữ liệu.

Các phân vùng cho phép chia nhỏ không gian lưu trữ của ổ cứng thành nhiều phần riêng biệt, mỗi phần có thể được sử dụng như một ổ cứng độc lập.

Việc phân vùng ổ cứng giúp tăng cường tổ chức và quản lý dữ liệu, cũng như cải thiện hiệu suất hệ thống.

Vd: Ổ cứng như một tủ lưu trữ lớn, và các phân vùng như các ngăn nhỏ bên trong tủ đó

File system (windows linux macos)

Trong hệ điều hành Windows, Linux và macOS, file system là cách thức tổ chức và quản lý các tệp và thư mục trên ổ đĩa hoặc thiết bị lưu trữ. Mỗi hệ điều hành có các file system riêng biệt.

Các file system đóng vai trò quan trọng trong việc xác định cách dữ liệu được lưu trữ, truy cập và quản lý.

Chúng cung cấp các tính năng như phân quyền, mã hóa, kiểm tra lỗi, và hỗ trợ dung lượng lớn cho các tệp và thư mục.

Các hệ thống file thường được sử dụng trên mỗi nền tảng:

- Windows:
 - NTFS (New Technology File System): Là file system mặc định cho hệ điều hành Windows từ Windows NT 3.1 trở đi. Nó hỗ trợ các tính năng như phân quyền, nén dữ liệu, mã hóa và ghi nhật ký.
- Linux:
 - Ext4 (Fourth Extended File System): Là phiên bản tiếp theo của hệ thống file Ext3 và là hệ thống file mặc định cho nhiều bản phân phối Linux hiện đại. Nó cung cấp tính năng mở rộng dung lượng lớn, hỗ trợ file lớn và hỗ trợ journaling.
 - XFS (X File System): Một hệ thống file khác được sử dụng phổ biến trong môi trường Linux, đặc biệt là cho các hệ thống lưu trữ lớn.
- macOS:
 - APFS (Apple File System): Được giới thiệu bởi Apple vào năm 2017, APFS thay thế cho HFS+ và cung cấp nhiều tính năng hiện đại như mã hóa, snapshots và quản lý dung lượng hiệu quả hơn.

Dictionaries

Trong lĩnh vực computer forensics, "dictionaries" thường được sử dụng để ám chỉ các tập hợp các từ, cụm từ hoặc mẫu dữ liệu được sử dụng để thực hiện các phân tích trên dữ liệu số. Dictionaries có thể được áp dụng trong nhiều trường hợp khác nhau trong forensics, bao gồm:

1. Tìm kiếm từ khóa: Dictionaries có thể chứa danh sách các từ khóa, cụm từ hoặc mẫu dữ liệu đặc biệt mà nhà điều tra muốn tìm kiếm trong dữ liệu số. Điều này có thể bao gồm các từ khóa liên quan đến hoạt động phạm pháp, như mã độc, tên tệp, tên người dùng, địa chỉ IP, v.v.
2. Phát hiện tệp và dữ liệu quan trọng: Trong quá trình điều tra, dictionaries có thể được sử dụng để tìm kiếm các loại tệp cụ thể (ví dụ: hình ảnh, video) hoặc dữ liệu quan trọng (ví dụ: số thẻ tín dụng, số điện thoại) để định danh hoặc phân loại các thông tin quan trọng.
3. Phân loại và phân tích dữ liệu: Dictionaries có thể được sử dụng để phân loại dữ liệu theo loại (ví dụ: hình ảnh, văn bản, âm thanh) hoặc tính chất (ví dụ: tệp tin quan trọng, dữ liệu được mã hóa) để hỗ trợ việc phân tích và hiểu về dữ liệu đang được xem xét.
4. Xác định đặc điểm của dữ liệu: Bằng cách sử dụng dictionaries, nhà điều tra có thể xác định các đặc điểm đặc trưng của dữ liệu, ví dụ: mã độc có dạng cụ thể, mẫu mã hash của các tệp tin độc hại, hoặc cấu trúc của một loại tệp tin cụ thể.

Như vậy, dictionaries trong ngữ cảnh computer forensics là các tập hợp dữ liệu được tổ chức và sử dụng để hỗ trợ việc phân tích, định danh và hiểu về dữ liệu số trong quá trình điều tra tội phạm máy tính.

Files

Files (tệp tin) là đơn vị lưu trữ thông tin trong máy tính, chứa dữ liệu như văn bản, hình ảnh, âm thanh, video, hoặc mã nguồn chương trình. Mỗi file có tên duy nhất để xác định và truy cập.

Các files có thể được tổ chức thành các thư mục để quản lý và tổ chức dữ liệu một cách cấu trúc hóa.

Có thể read-write? Khi từ windows sang macos và ngược lại

Có, có thể đọc và ghi file từ một hệ điều hành vào hệ điều hành

Nhưng cần lưu ý:

- Hỗ trợ định dạng file:
Hệ điều hành Linux thường hỗ trợ đọc và ghi vào các định dạng file phổ biến như NTFS và FAT32, mà là các định dạng file phổ biến trên hệ điều hành Windows. Tuy nhiên, một số định dạng file đặc biệt hoặc mới hơn có thể cần cài đặt thêm phần mềm hoặc driver để hỗ trợ đọc và ghi.
- Phần mềm hỗ trợ:
Có một số phần mềm và công cụ trong Linux giúp đọc và ghi vào các định dạng file của Windows, chẳng hạn như NTFS-3G cho việc đọc và ghi vào ổ đĩa NTFS.

Ngược lại, Samba có thể được sử dụng để chia sẻ file giữa Linux và Windows thông qua mạng, cho phép các máy tính chạy Linux và Windows có thể truy cập và ghi vào các file trên máy tính của nhau thông qua giao thức mạng SMB/CIFS.

- Đảm bảo an toàn:

Khi đọc hoặc ghi vào file từ một hệ điều hành sang hệ điều hành khác, cần chú ý để tránh gây hỏng dữ liệu hoặc mất mát thông tin. Đảm bảo sao lưu dữ liệu quan trọng trước khi thực hiện các thao tác này.

=> Việc đọc và ghi file từ Linux sang Windows và ngược lại là hoàn toàn khả thi, nhưng cần sử dụng các công cụ và phương tiện phù hợp để đảm bảo tương thích và an toàn.

File .dd ?

File có phần mở rộng .dd thường là các hình ảnh đĩa được tạo ra bằng các công cụ như dd trong Unix. Các hình ảnh này là bản sao chính xác bit-by-bit của toàn bộ nội dung của một ổ đĩa hoặc phân vùng, bao gồm cả dữ liệu và cấu trúc đĩa như bảng phân vùng.

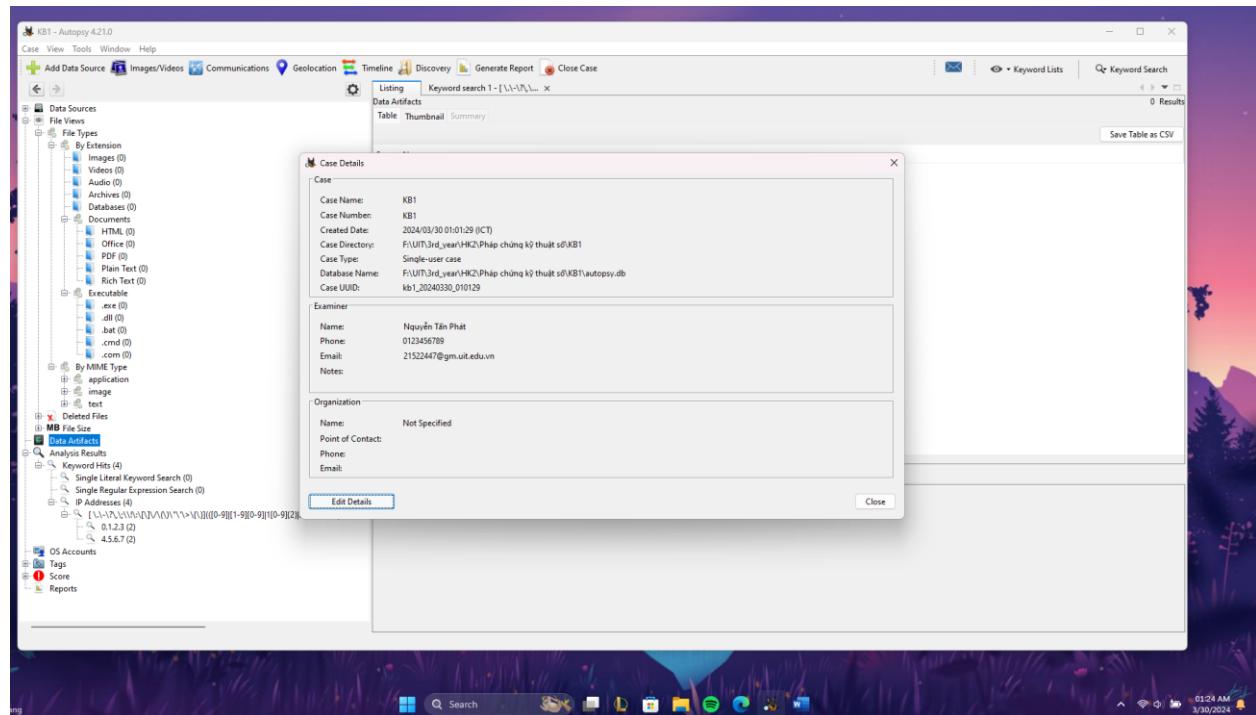
Công cụ dd cho phép người dùng tạo ra các hình ảnh đĩa với độ chính xác cao, bao gồm cả các phần không được sử dụng của ổ đĩa, làm cho các file .dd rất hữu ích trong việc sao lưu và phục hồi dữ liệu, vì chúng bao gồm toàn bộ nội dung của ổ đĩa mà không bỏ lỡ bất kỳ phần nào.

Các file .dd thường được sử dụng trong các hoạt động như phục hồi dữ liệu từ ổ đĩa hỏng, sao lưu toàn bộ hệ thống hoặc phân tích số học. Các chuyên gia có thể sử dụng các hình ảnh đĩa để khám phá dữ liệu và điều tra vụ việc mà không làm thay đổi nội dung gốc của ổ đĩa.

=> file .dd là các hình ảnh đĩa chứa bản sao chính xác của toàn bộ nội dung của một ổ đĩa hoặc phân vùng, được sử dụng rộng rãi trong việc sao lưu, phục hồi dữ liệu và phân tích số học.

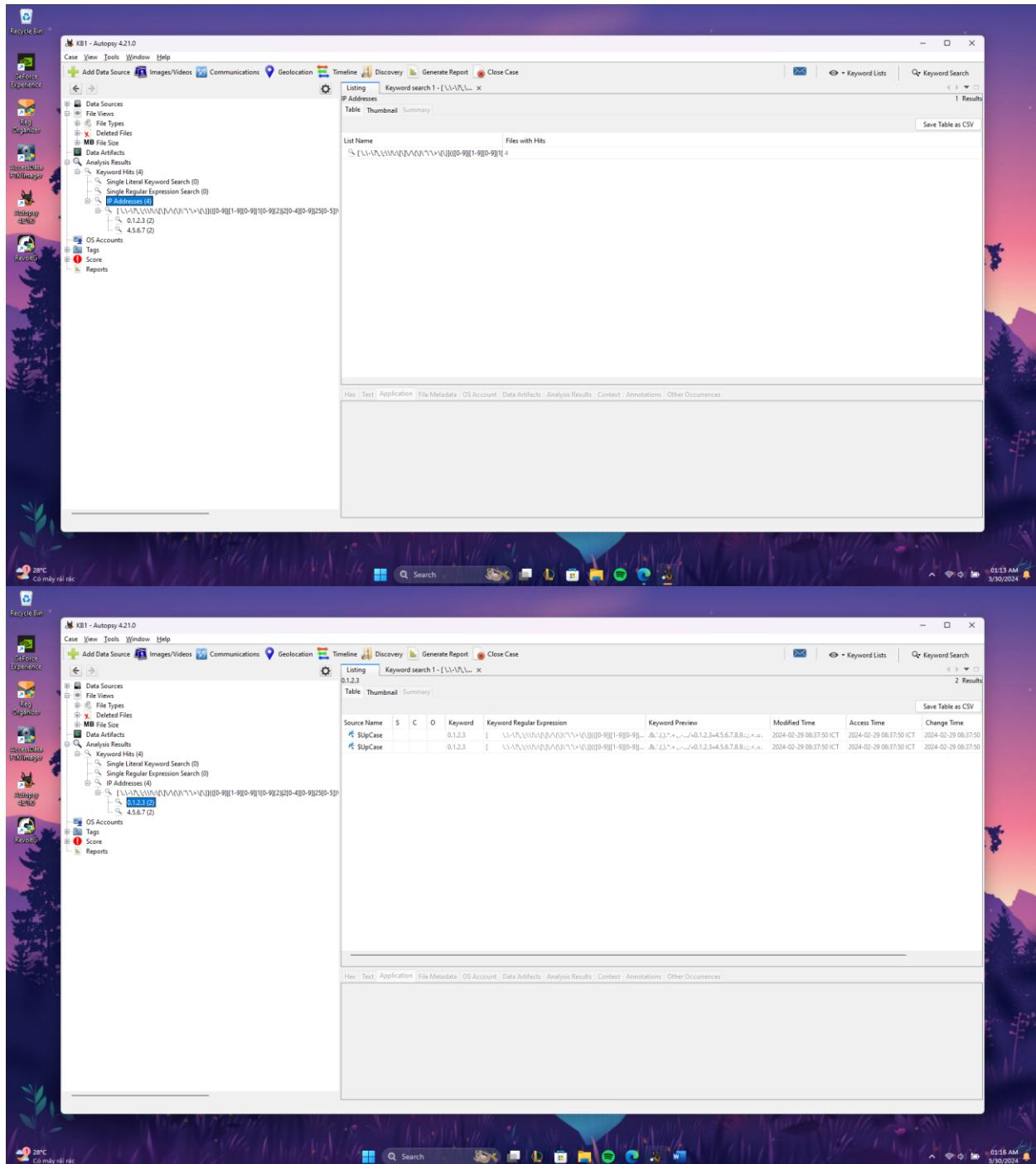
1. Kịch bản 01

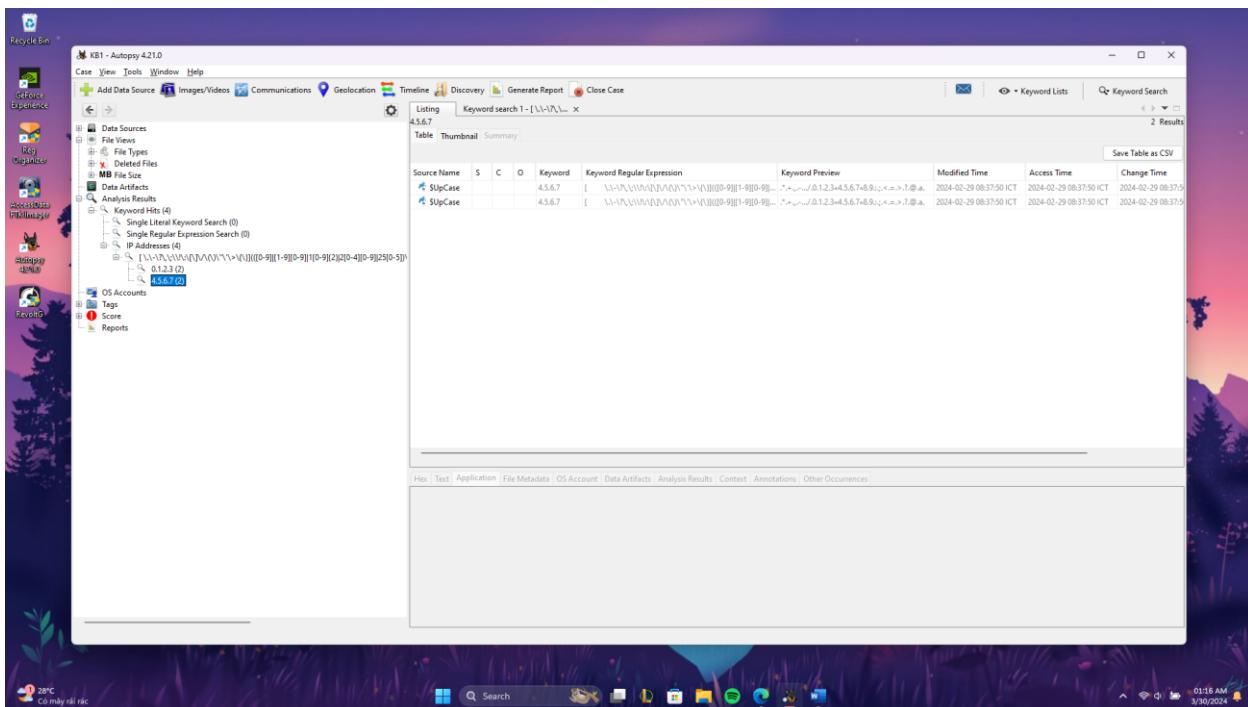
Case detail:



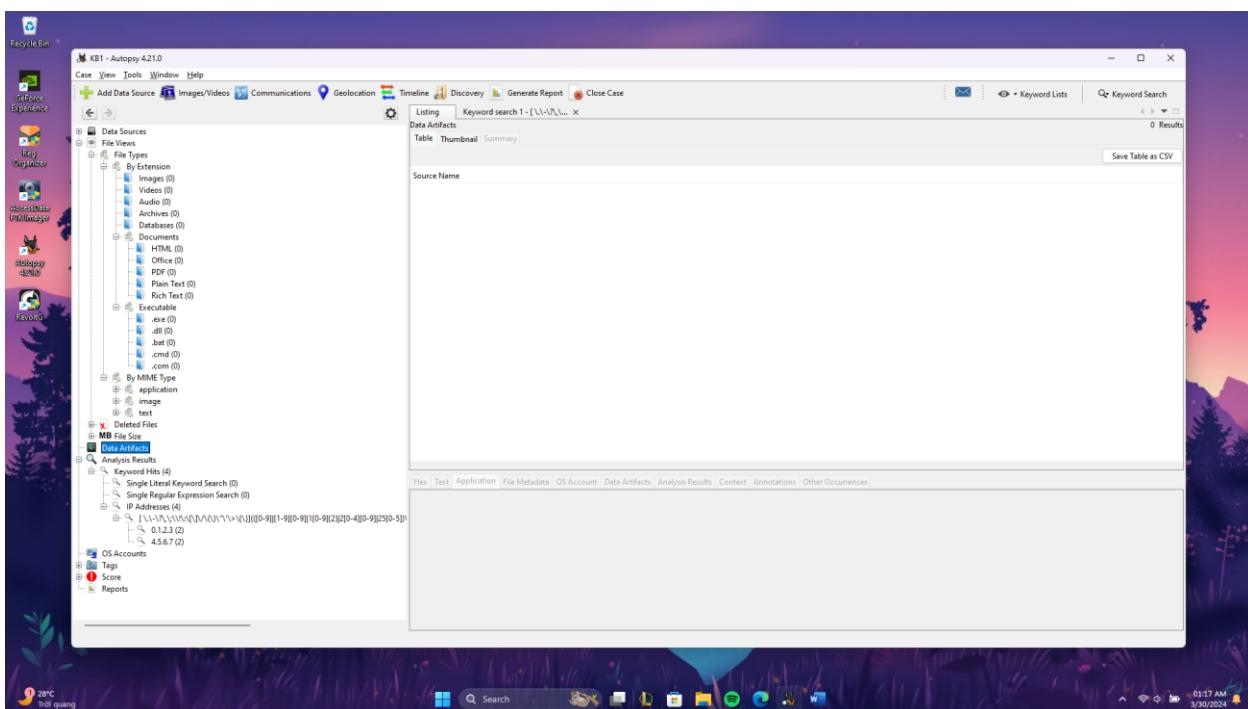
- Chọn tìm các số điện thoại và địa chỉ IP có trong Filesystem

Kết quả: có 2 địa chỉ IP

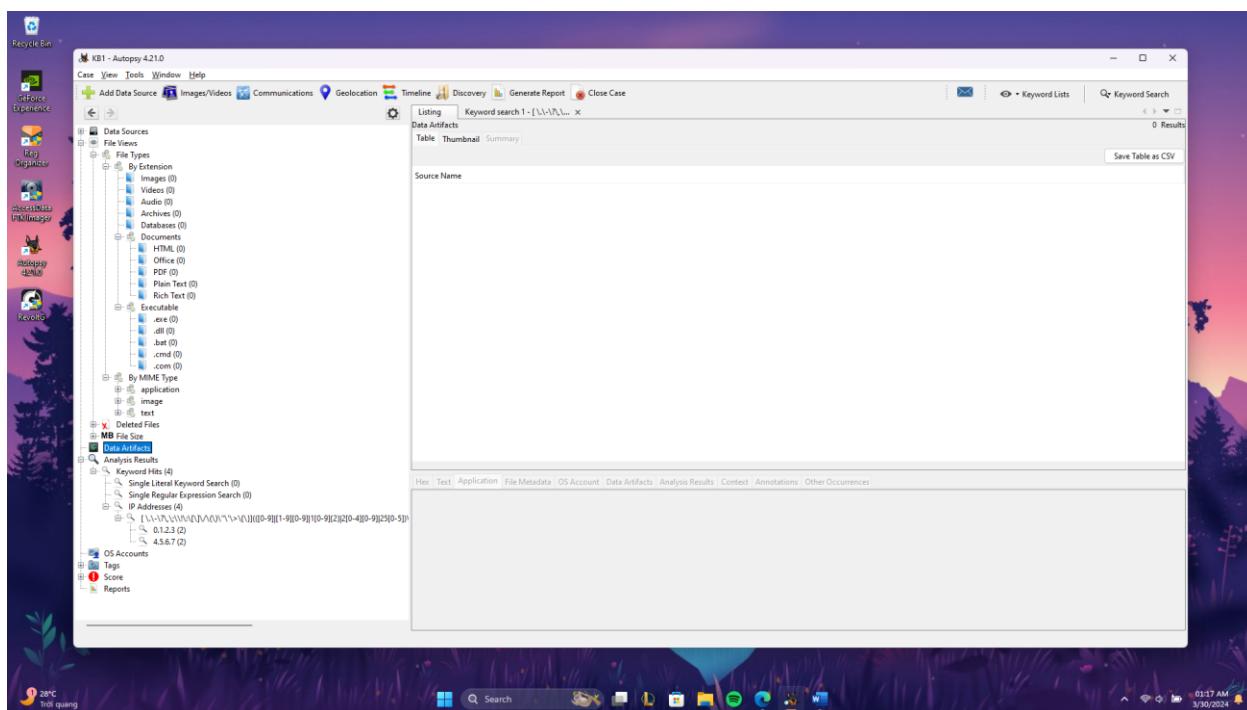




- Thực hiện việc xem xét toàn bộ Filesystem, xem xét các lựa chọn nằm ô phía bên trái của màn hình.



- Tìm thư mục có nhiều File nhất trong Filesystem.

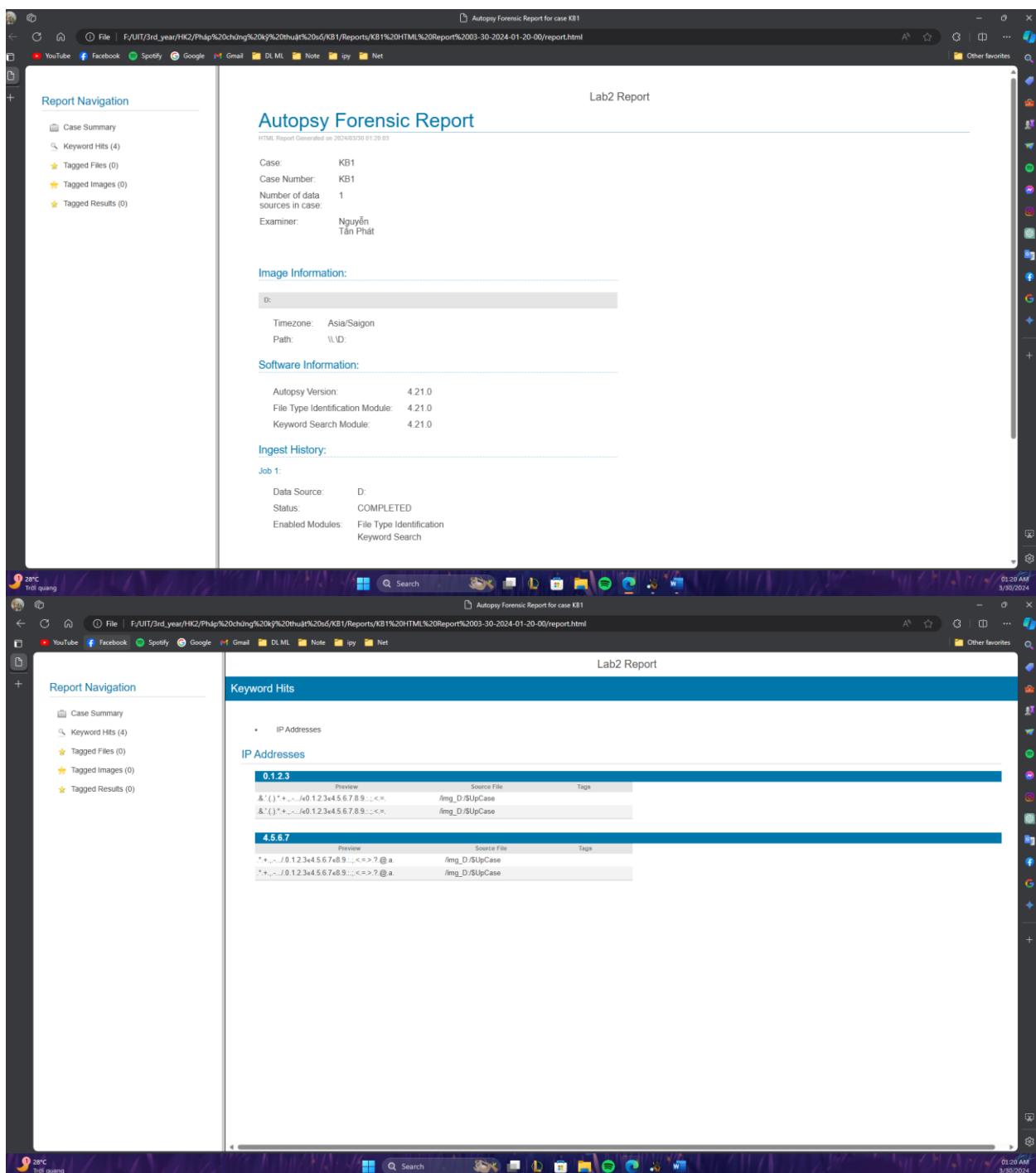


- Xem các file hình ảnh chứa trong Filesystem bằng chế độ view Thumbnail. Xác định số lượng các files dạng doc và pdf chứa trong Filesystem.

Vì Filesystem không có file hình ảnh hay bất kì file gì nên không thể xem được

- Sử dụng nút "Generate Report" để tạo ra báo cáo dạng HTML và Excel, xem nội dung báo cáo trong mục Report. Nếu nhận xét, kết luận về nội dung của báo cáo.

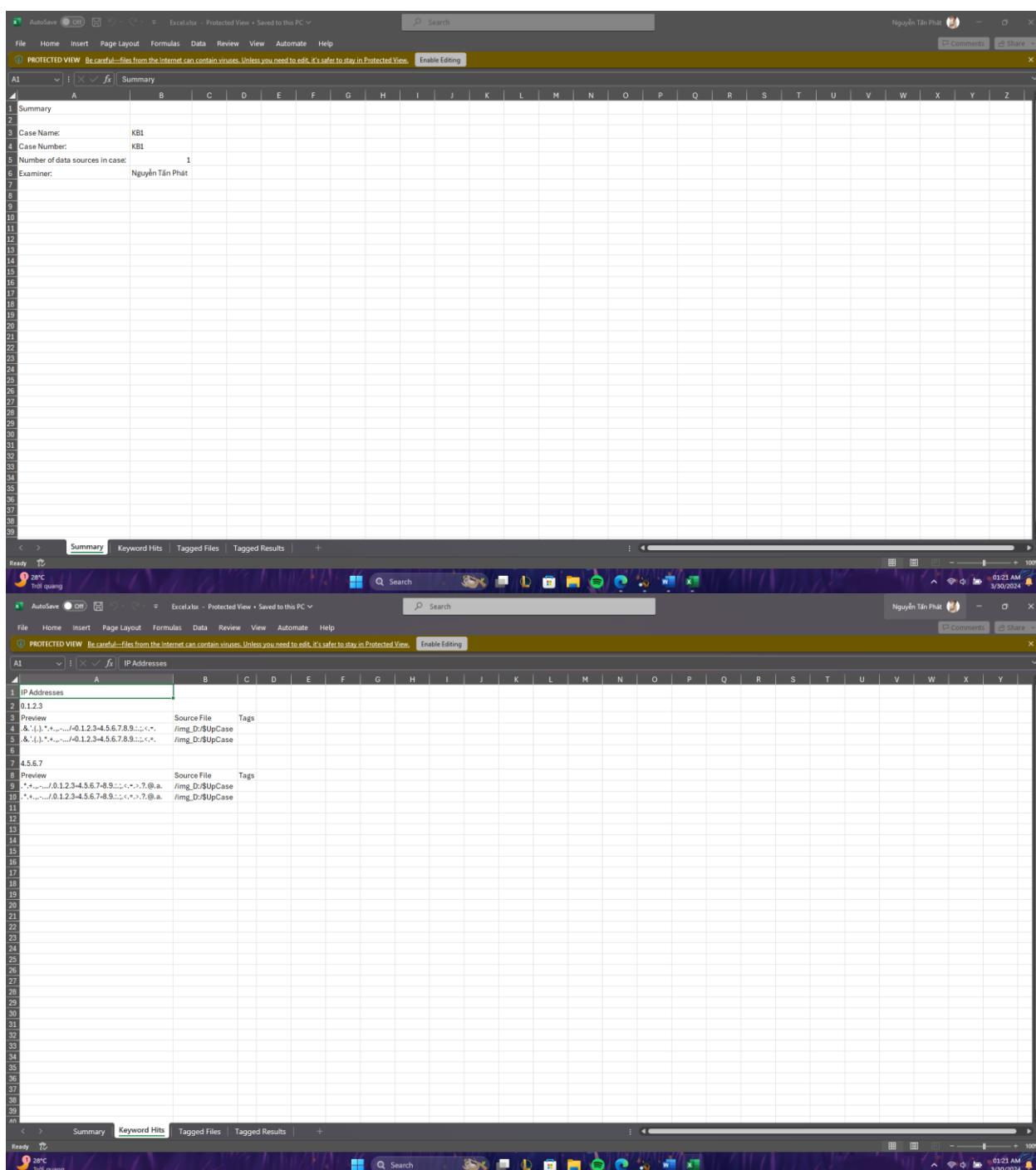
Nội dung báo cáo trong dạng file HTML ngắn gọn, tập trung vào kết quả được phân tích từ Analysis Modules và Keyword Search



The screenshot displays two windows of the Autopsy Forensic Report interface. The top window shows the 'Lab2 Report' section, which includes a 'Report Navigation' sidebar with options like Case Summary, Keyword Hits (4), Tagged Files (0), Tagged Images (0), and Tagged Results (0). The main content area shows the 'Autopsy Forensic Report' header, case details (Case: KB1, Case Number: KB1, Number of data sources in case: 1, Examiner: Nguyễn Tân Phát), and sections for Image Information, Software Information, and Ingest History. The bottom window shows the 'Keyword Hits' section, specifically the 'IP Addresses' tab, displaying two entries:

Preview	Source File	Tags
&('.)*+,-./0.1.2.3x4.5.6.7.8.9...<@.;	/Img_D/\$UpCase	
&('.)*+,-./0.1.2.3x4.5.6.7.8.9...<=.	/Img_D/\$UpCase	

Nội dung report trong file Excel hiển thị ra nhiều sheet khác nhau, kết quả cũng giống như của report HTML

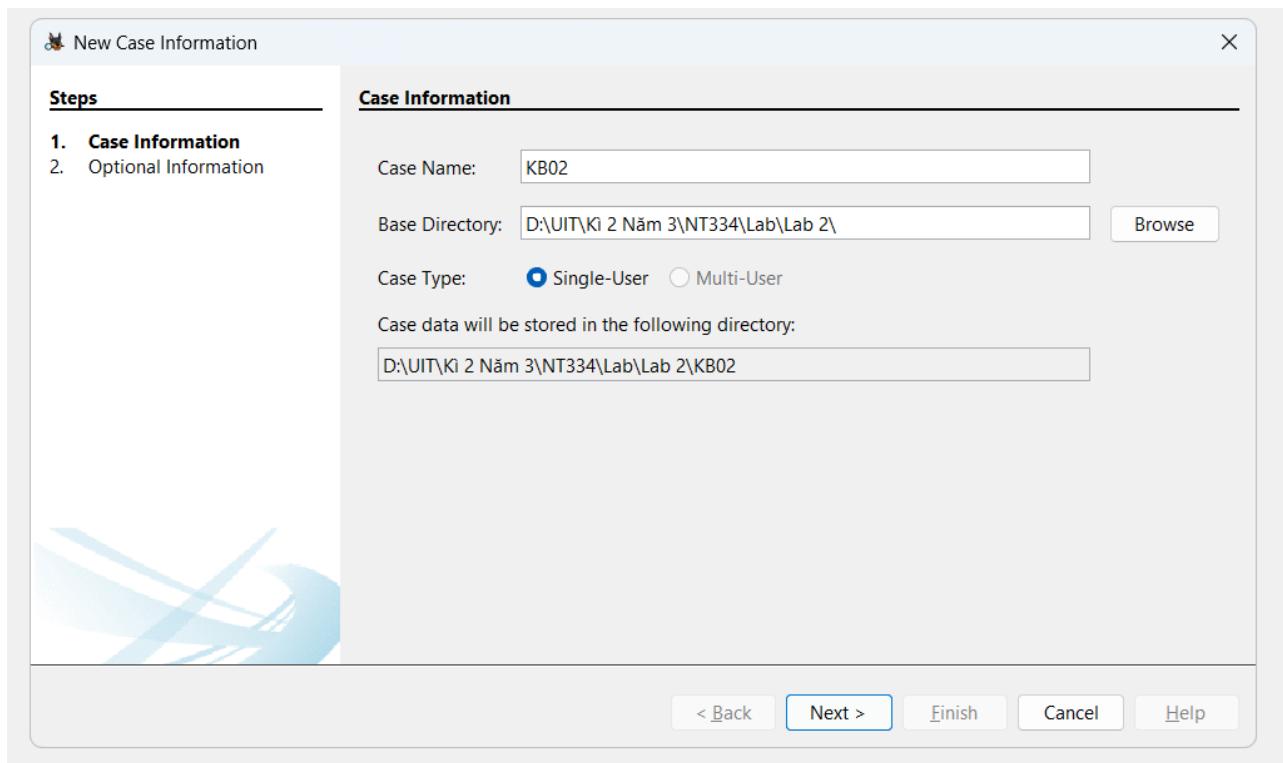


2. Kịch bản 02

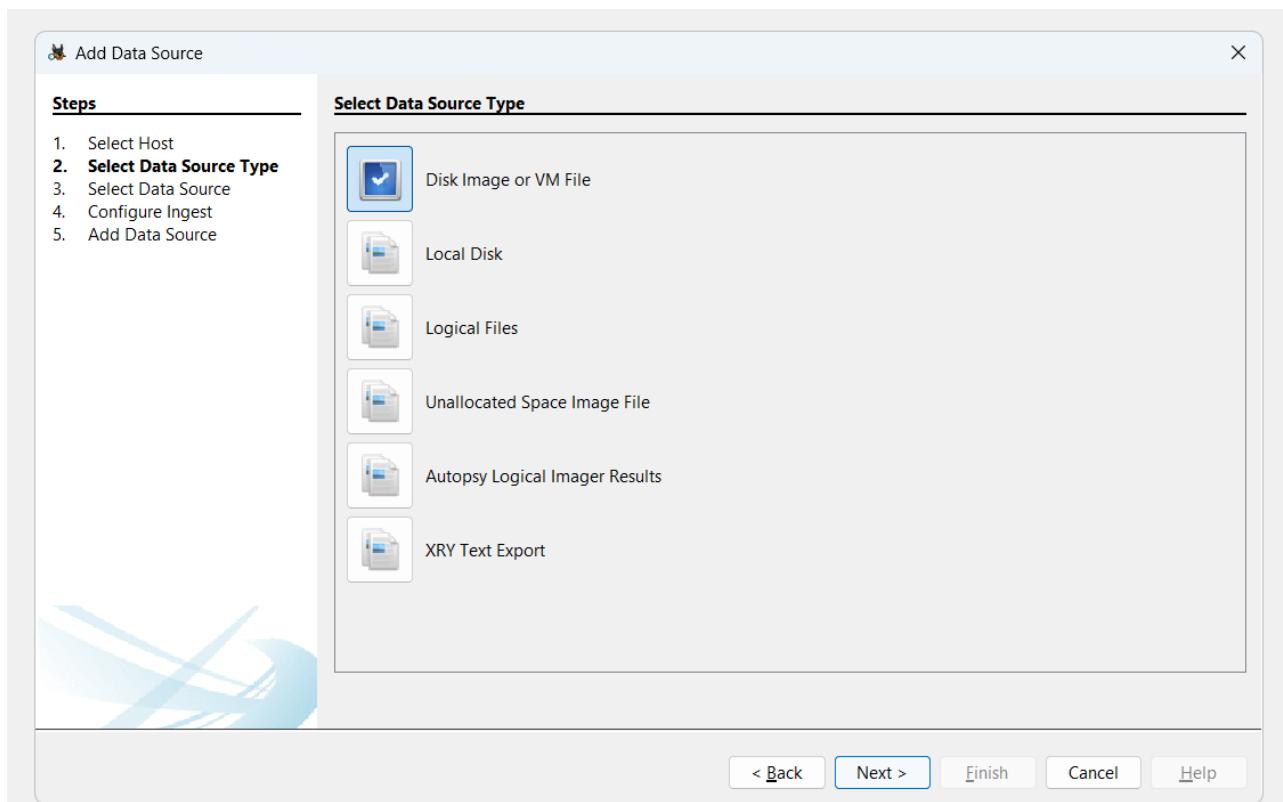
Kịch bản 02. Thực hiện phân tích dựa trên tài nguyên được cung cấp.

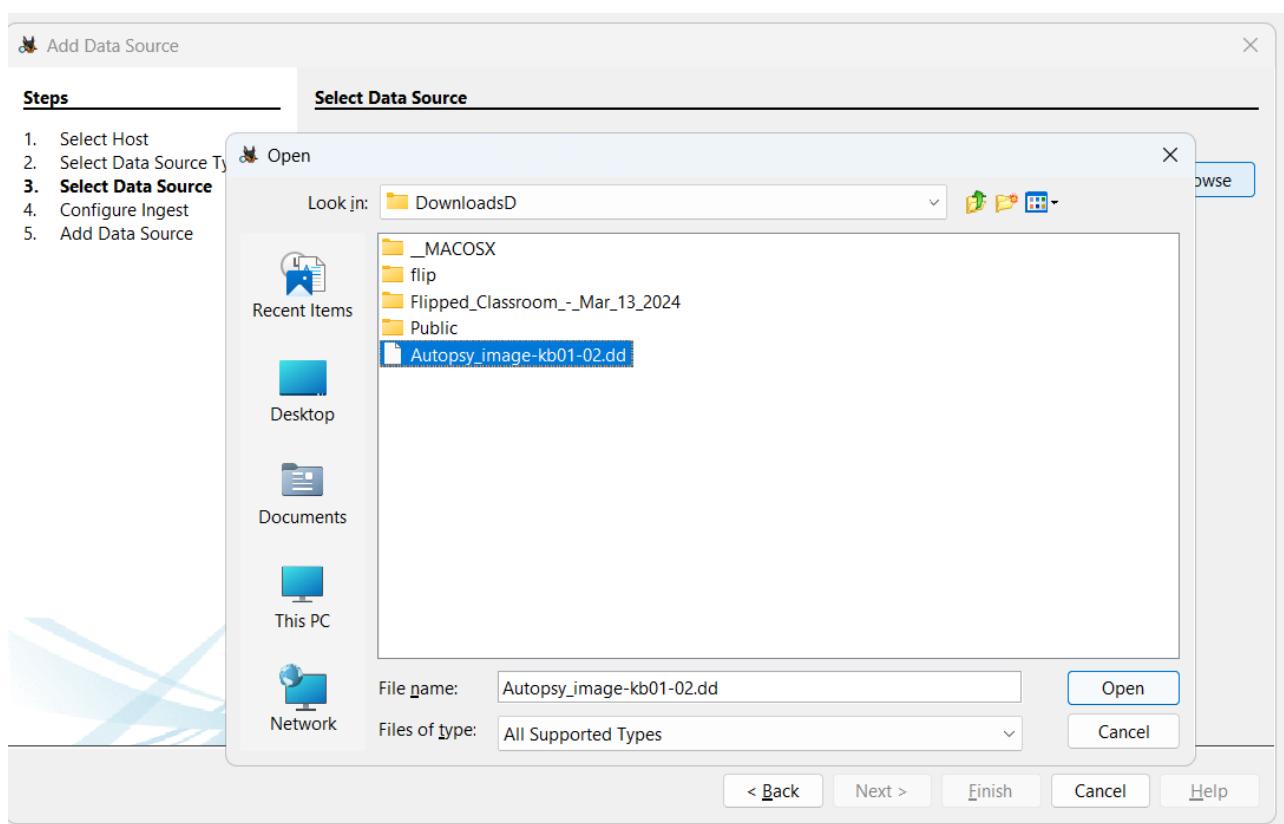
Tài nguyên: tải về theo link sau: <https://goo.gl/MRLtj4>

- Mở Autopsy -> New Case -> set case name để tạo case mới

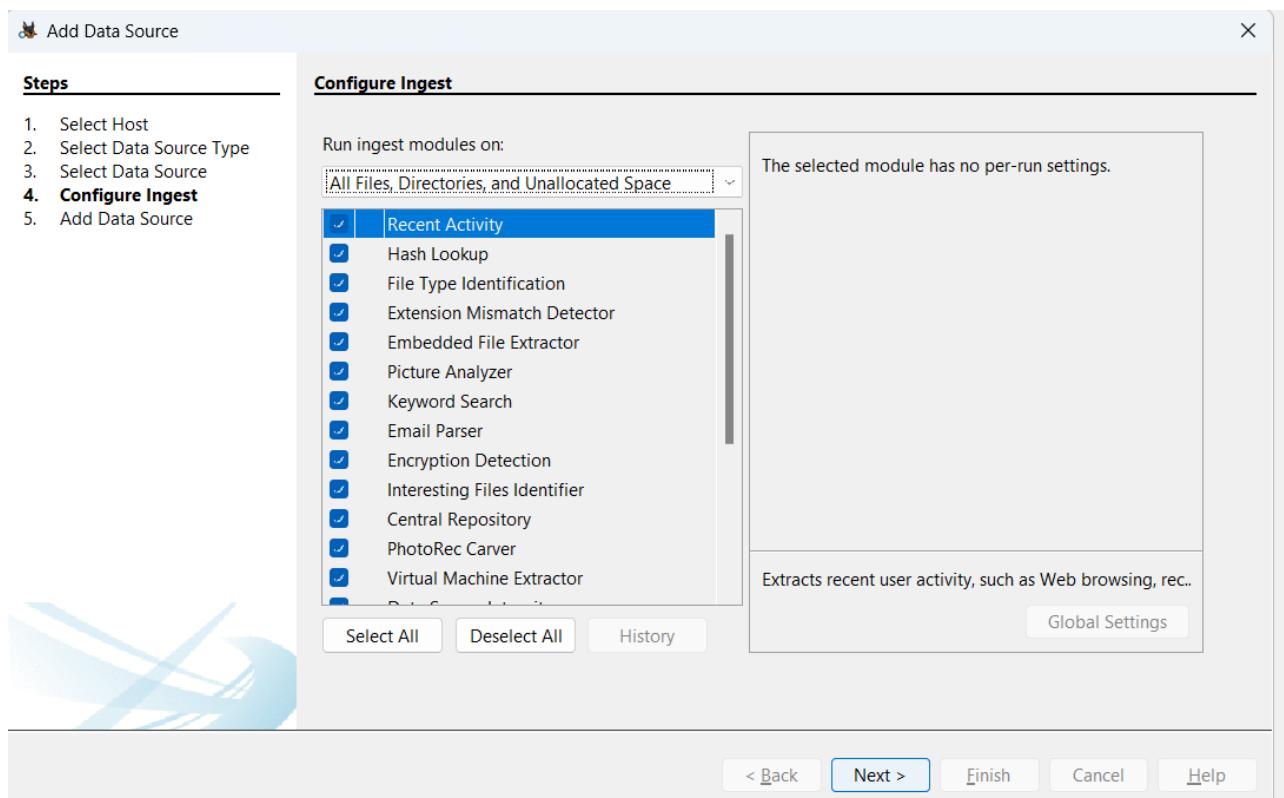


- Tại Add data source, chọn Disk Image or VM File và chọn path tới file tài nguyên cho sẵn





- Chọn các module cần phân tích



- Vào File Views, nơi hiển thị các thông tin chi tiết thông tin của các file chứa trong Filesystem.

Session 01: Memory Forensics

+ Hãy tìm tất cả những hình ảnh có trong ô đĩa đã cho.

File Views -> File Types -> By Extension -> Images

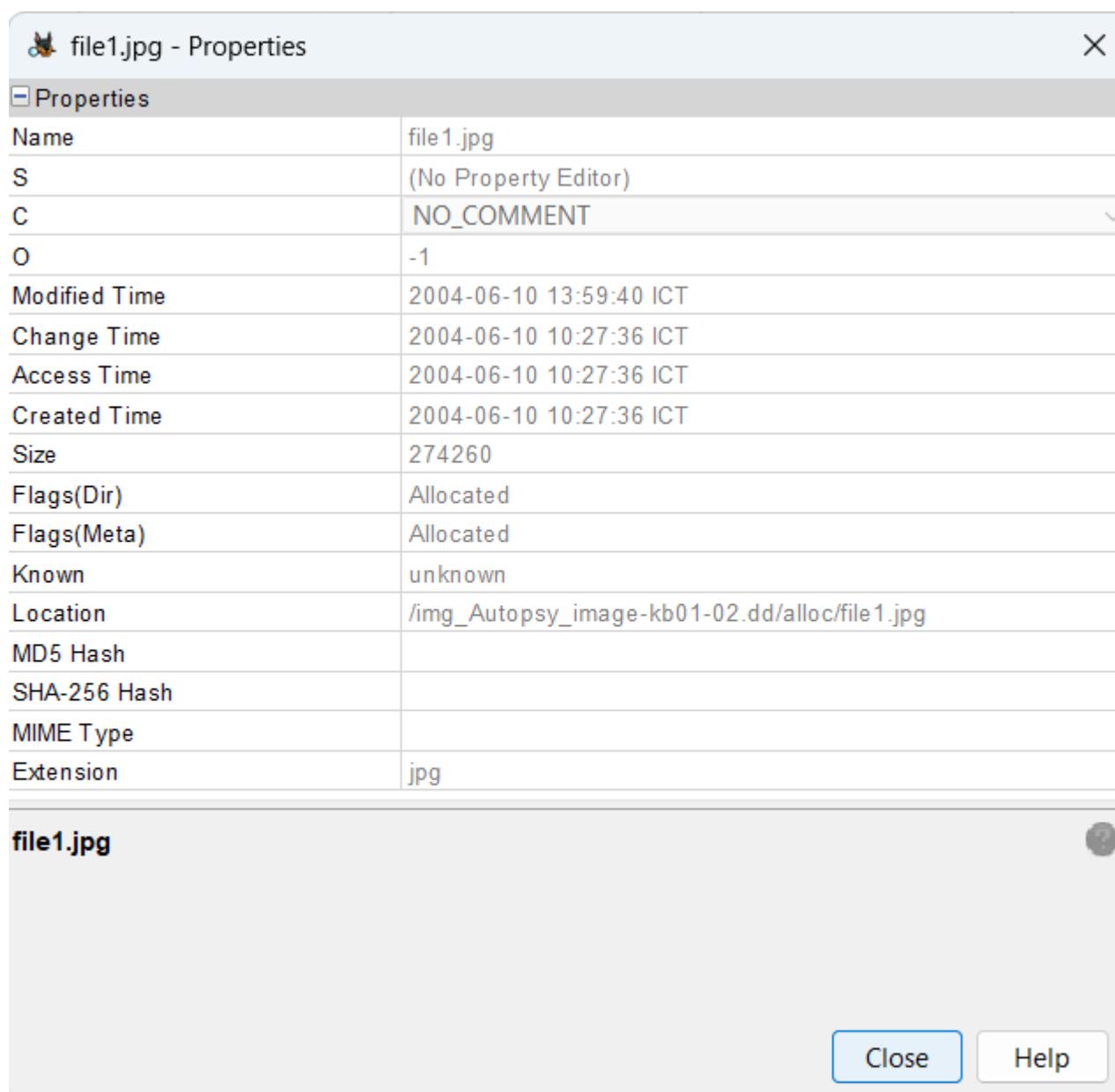
Ngoài ra còn tìm được các file ảnh khác trong thư mục deleted file, trong file1.jpg có file2.dat, trong executable → .dll cũng có.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
file1.jpg				2004-06-10 13:59:40 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	274260	Allocated	Allocated	unknow
file3.jpg				2004-06-10 14:27:02 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	214228	Allocated	Allocated	unknow
file4.jpg				2004-06-10 14:38:06 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:20 ICT	189021	Allocated	Allocated	unknow
file8.jpg				2004-06-09 20:52:20 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	337653	Allocated	Allocated	unknow
file10.jpg				2004-06-10 08:54:53 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	208919	Allocated	Allocated	unknow
file9.jpg				2004-06-09 20:53:32 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	292813	Allocated	Allocated	unknow
image_0.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	110373	Allocated	Allocated	unknow

+ Với mỗi file hình ảnh tìm được, liệt kê tất cả các thông tin liên quan đến file đó: tên file, loại file, size, thời gian tạo, xoá, sửa, MD5, kích thước hình ảnh ...

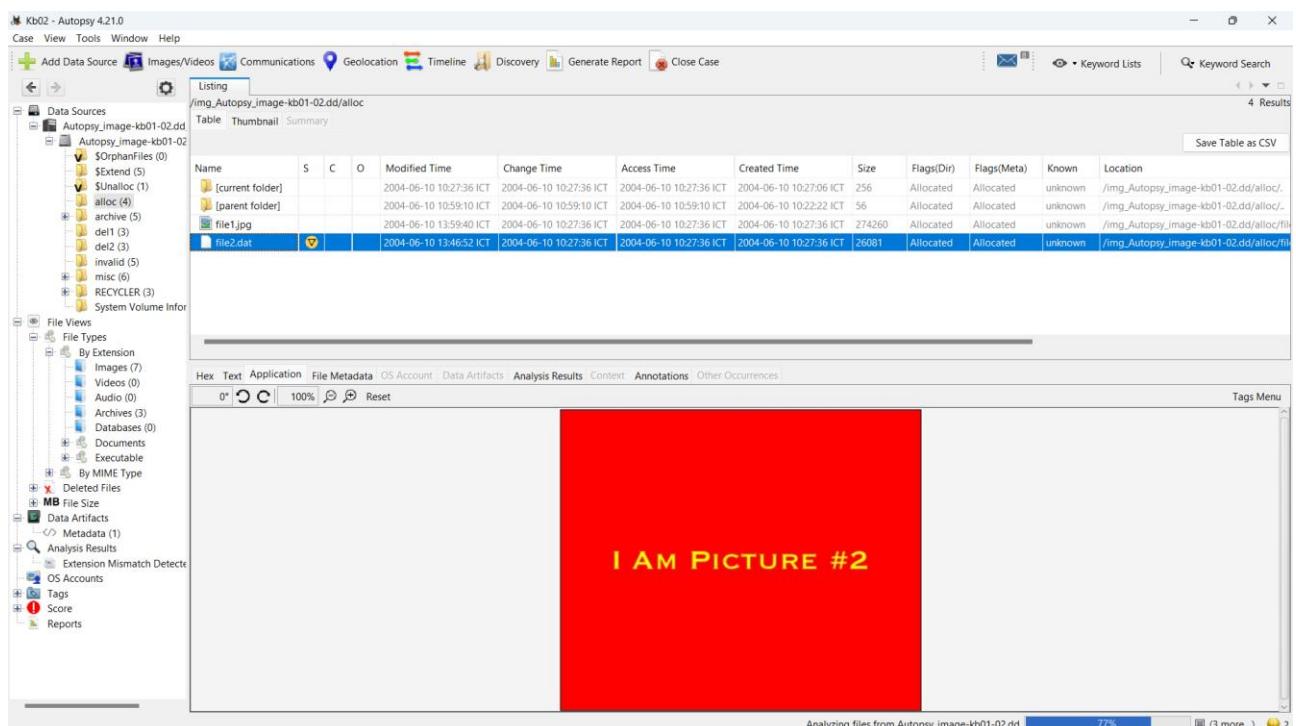
Thông tin file ảnh file1.jpg

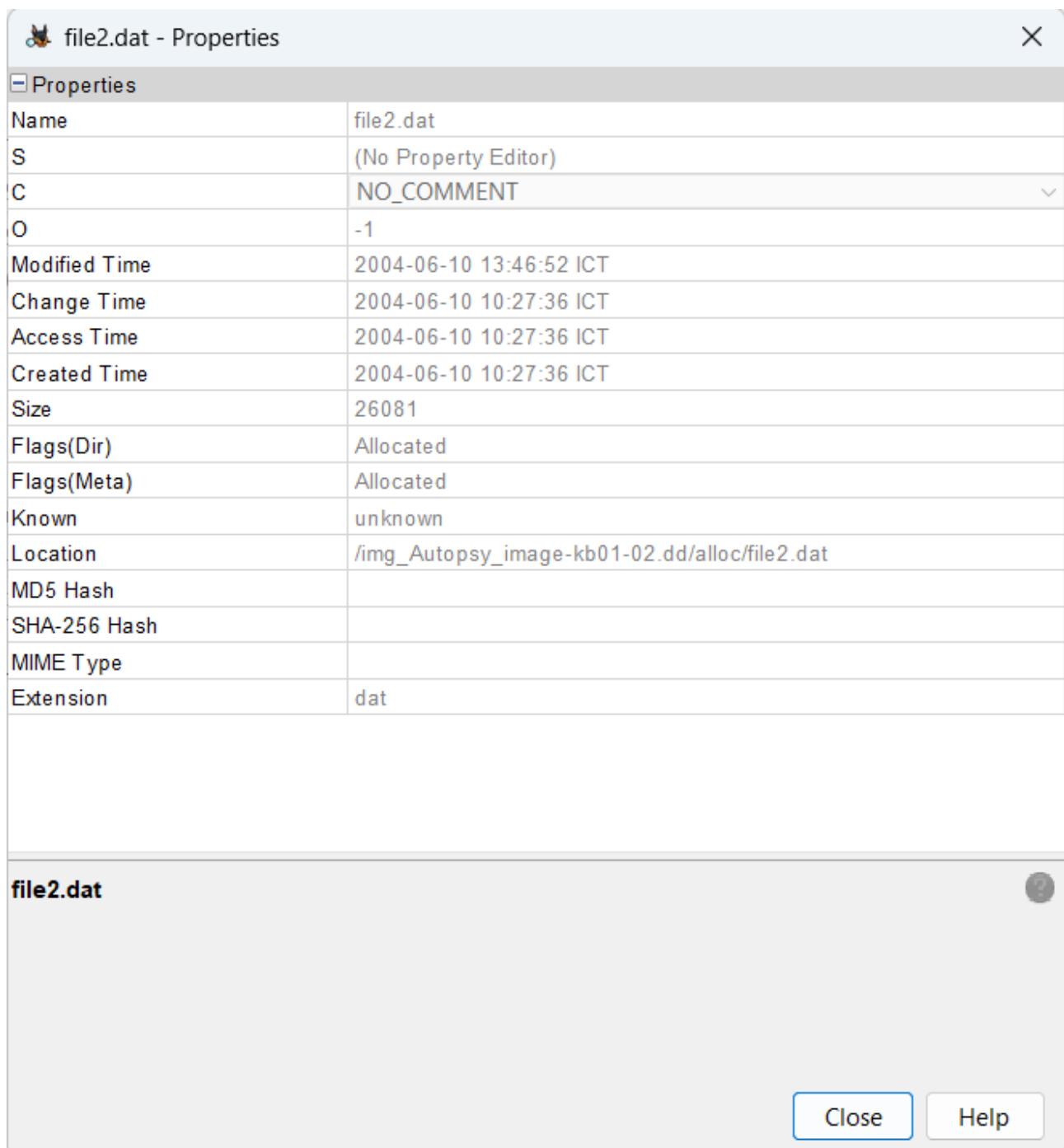
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
file1.jpg				2004-06-10 13:59:40 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	274260	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/alloc
file3.jpg				2004-06-10 14:27:02 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	214228	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/inv
file4.jpg				2004-06-10 14:38:06 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:20 ICT	189021	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/archi
file8.jpg				2004-06-09 20:52:20 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	337653	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/archi
file10.jpg				2004-06-10 08:54:53 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	208919	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/archi
file9.jpg				2004-06-09 20:53:32 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	292813	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/archi
image_0.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	110373	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/misc



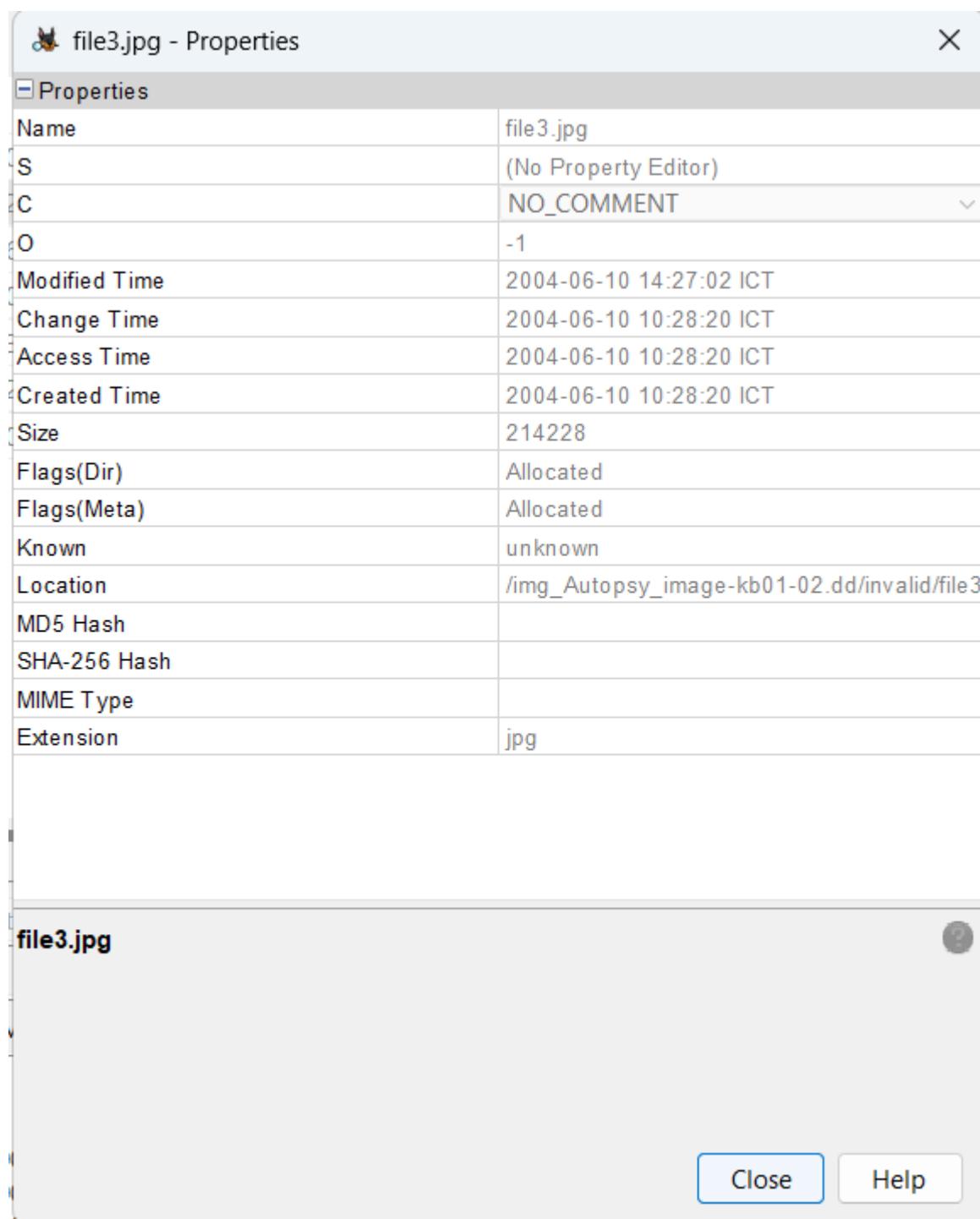
Trong file1.jpg ta view File in dictionary sẽ thấy file2.dat

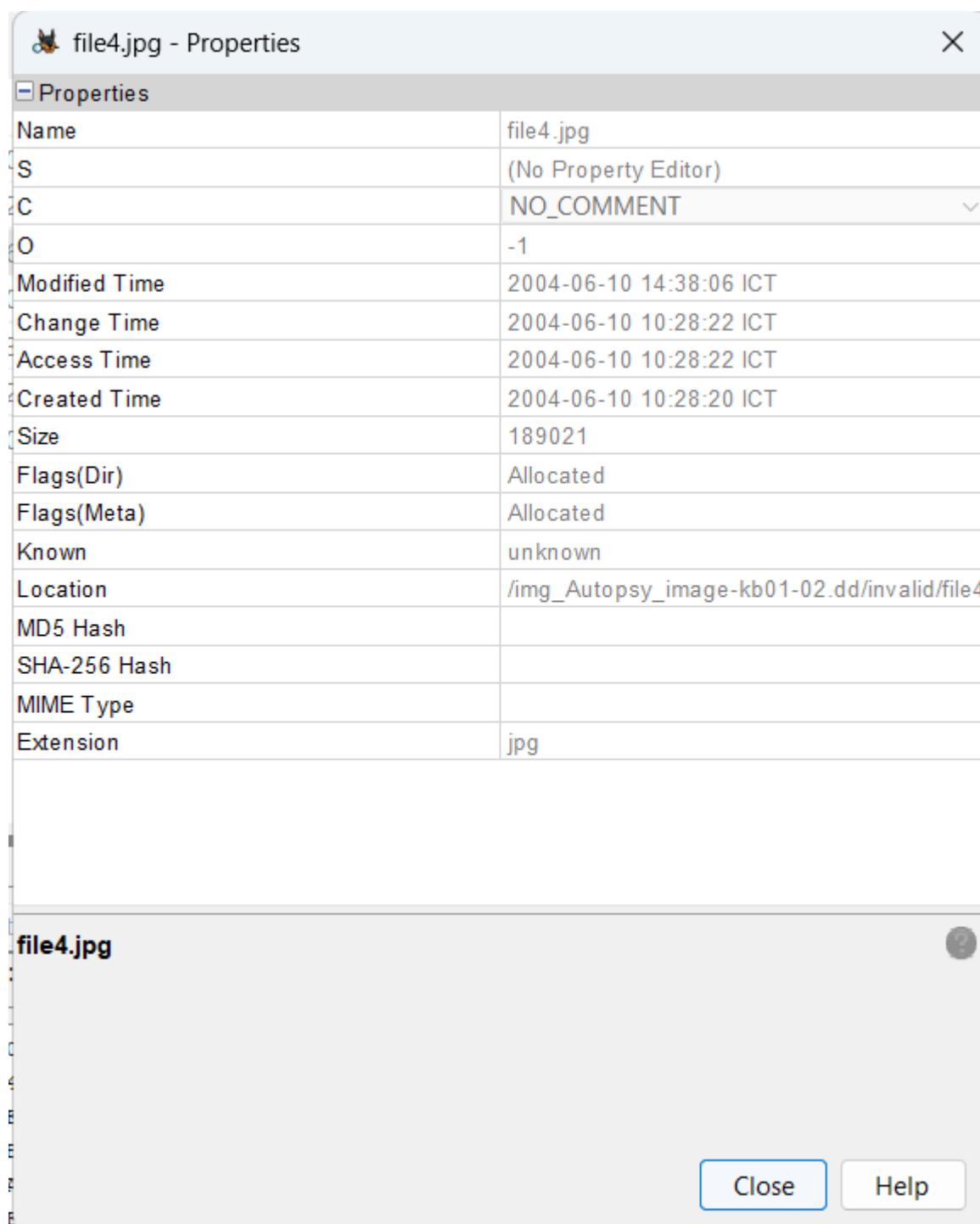
Thông tin file2.dat



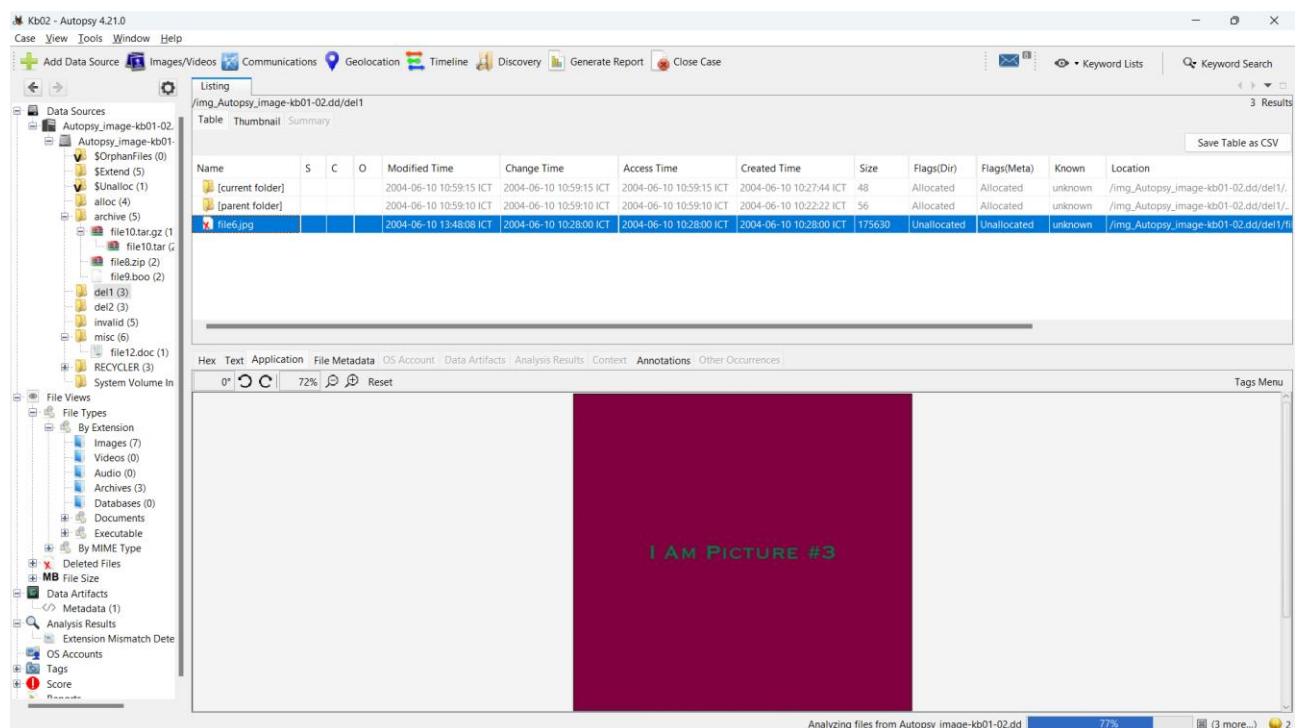


Thông tin file ảnh file3.jpg





Tìm trong dell1 ta thấy file6.jpg



Thông tin file6.jpg

 file6.jpg - Properties

Properties	
Name	file6.jpg
S	(No Property Editor)
C	NO_COMMENT
O	-1
Modified Time	2004-06-10 13:48:08 ICT
Change Time	2004-06-10 10:28:00 ICT
Access Time	2004-06-10 10:28:00 ICT
Created Time	2004-06-10 10:28:00 ICT
Size	175630
Flags(Dir)	Unallocated
Flags(Meta)	Unallocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/del1/file6.jpg
MD5 Hash	
SHA-256 Hash	
MIME Type	
Extension	jpg

file6.jpg



Tìm trong del2 thấy file7.hmm

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, including 'Autopsy Image-kb01-02.dd_1' which contains various files like 'file10.tar.gz', 'file8.zip', and 'file7.hmm'. The main pane shows a table of file metadata for 'file7.hmm' and other folders. Below the table is a preview area with the text 'I AM PICTURE #4'. At the bottom, a progress bar indicates 'Analyzing files from Autopsy_image-kb01-02.dd' at 77% completion.

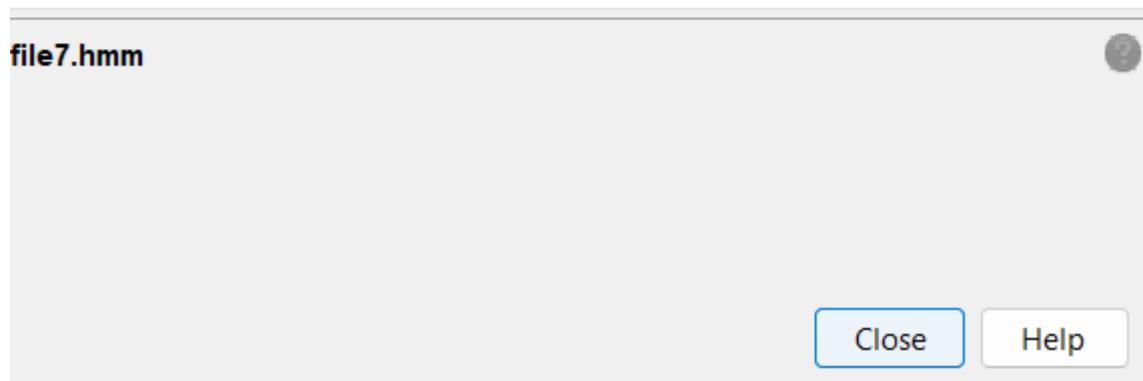
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2004-06-10 10:59:23 ICT	2004-06-10 10:59:23 ICT	2004-06-10 10:43:19 ICT	2004-06-10 10:43:19 ICT	48	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/c...
[parent folder]				2004-06-10 10:59:10 ICT	2004-06-10 10:59:10 ICT	2004-06-10 10:59:10 ICT	2004-06-10 10:22:22 ICT	56	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/c...
file7.hmm				2004-06-10 13:49:18 ICT	2004-06-10 10:43:44 ICT	2004-06-10 10:43:38 ICT	2004-06-10 10:28:00 ICT	326859	Unallocated	Unallocated	unknown	/img_Autopsy_image-kb01-02.dd/c...

Thông tin file file7.hmm

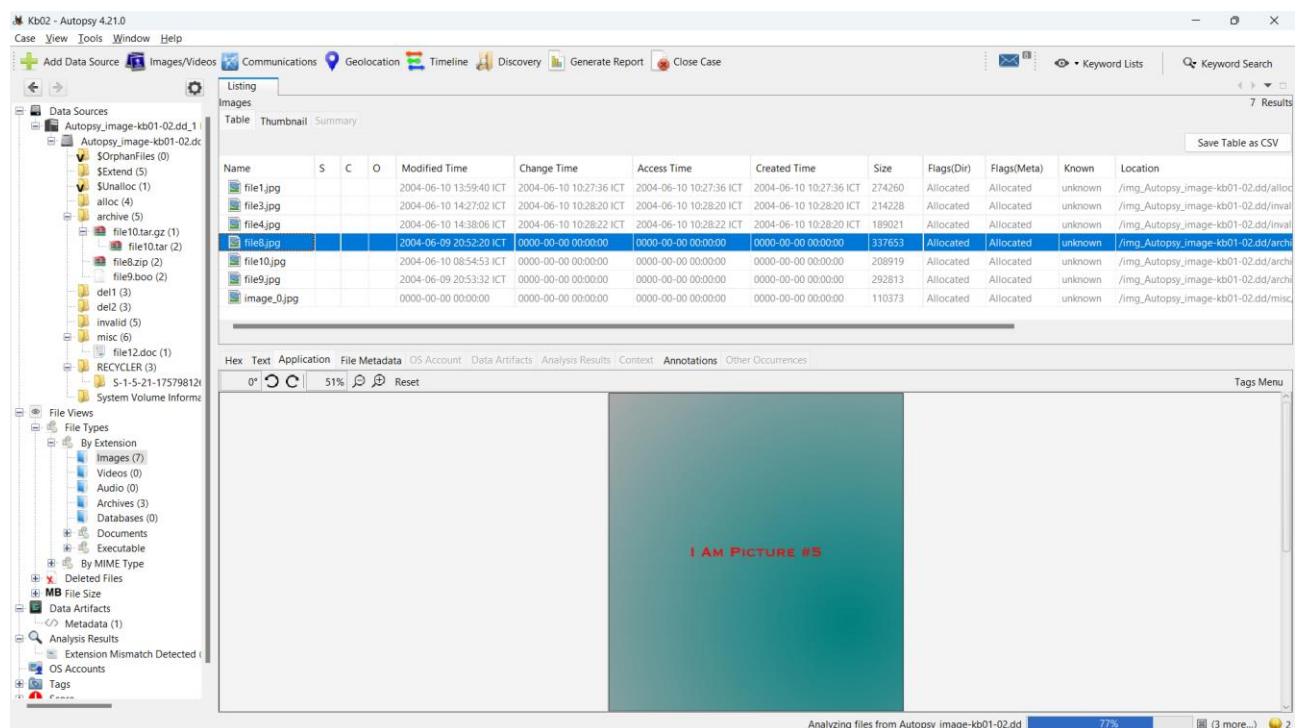
 file7.hmm - Properties X

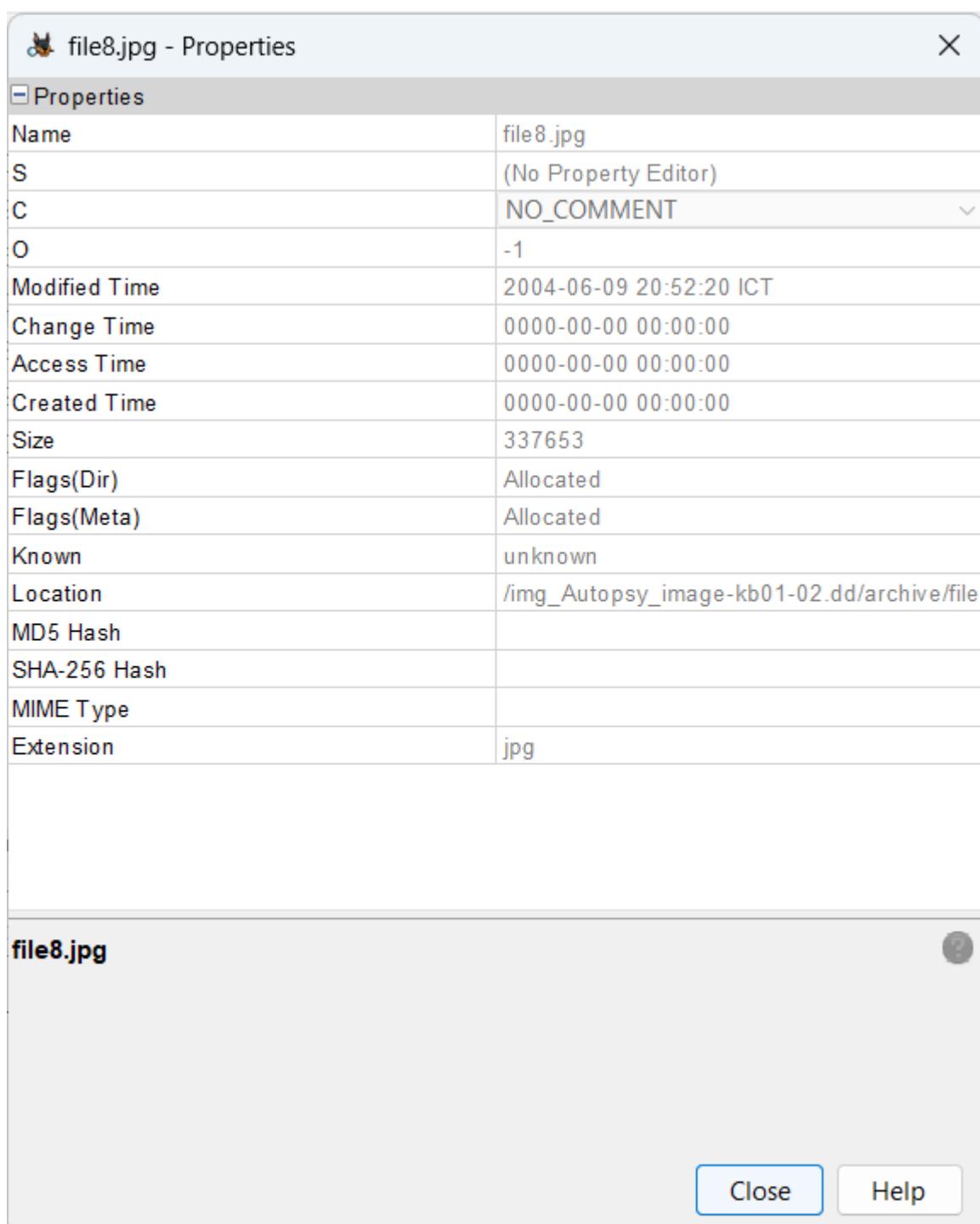
Properties

Name	file7.hmm
S	(No Property Editor)
C	NO_COMMENT
O	-1
Modified Time	2004-06-10 13:49:18 ICT
Change Time	2004-06-10 10:43:44 ICT
Access Time	2004-06-10 10:43:38 ICT
Created Time	2004-06-10 10:28:00 ICT
Size	326859
Flags(Dir)	Unallocated
Flags(Meta)	Unallocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/del2/file7.h
MD5 Hash	
SHA-256 Hash	
MIME Type	
Extension	hmm

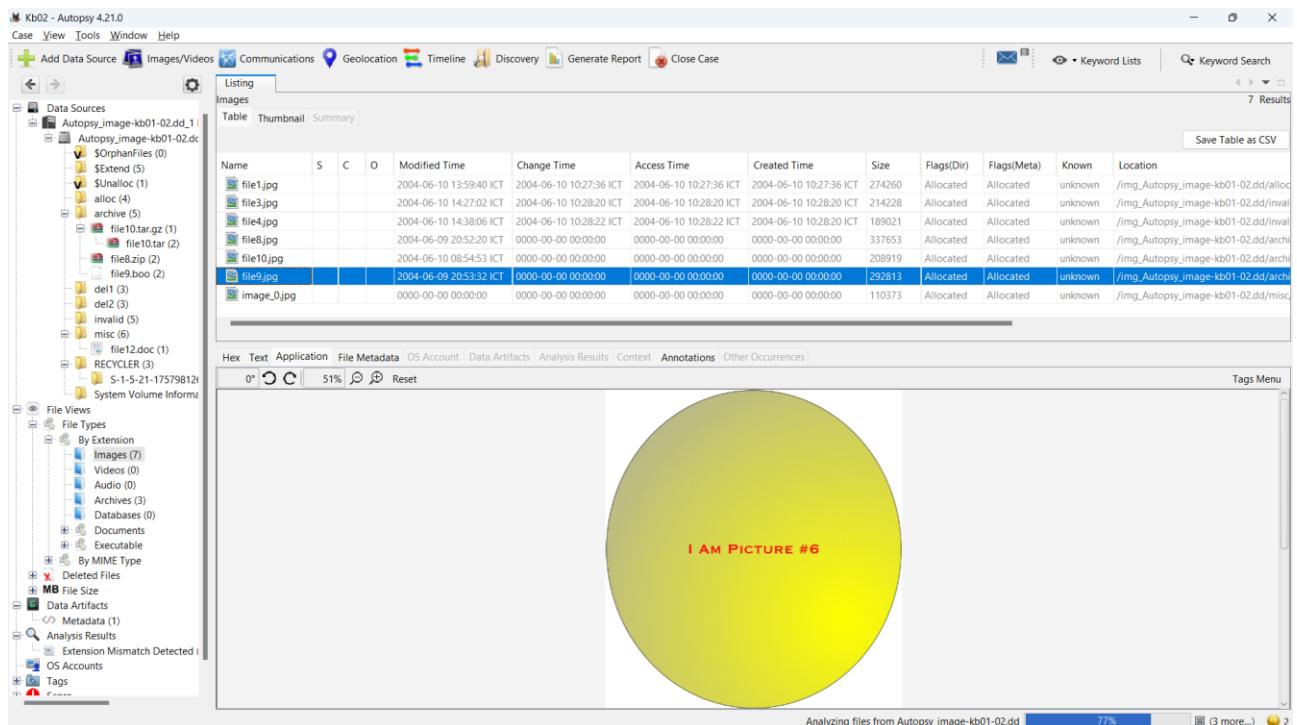


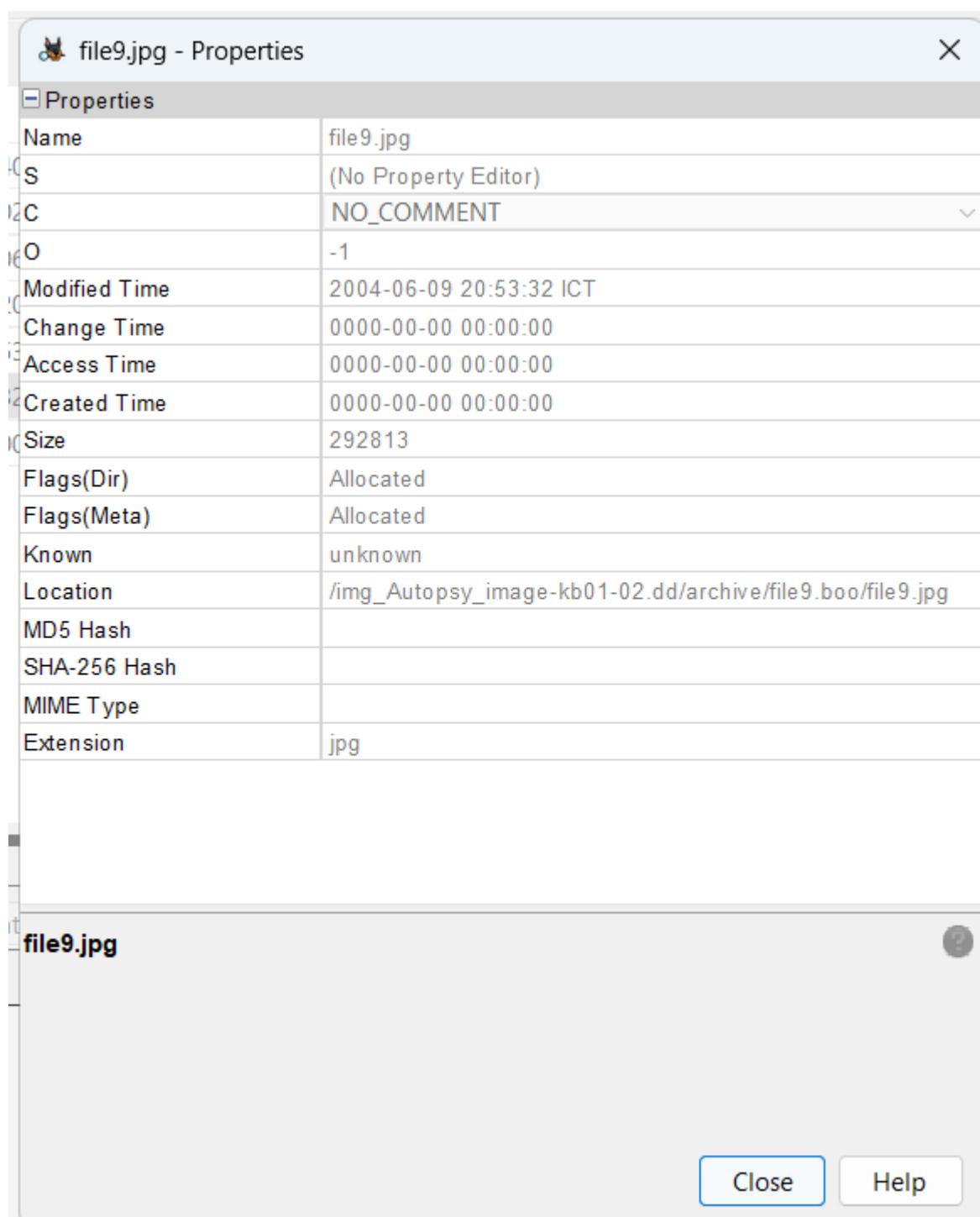
Thông tin file8.jpg



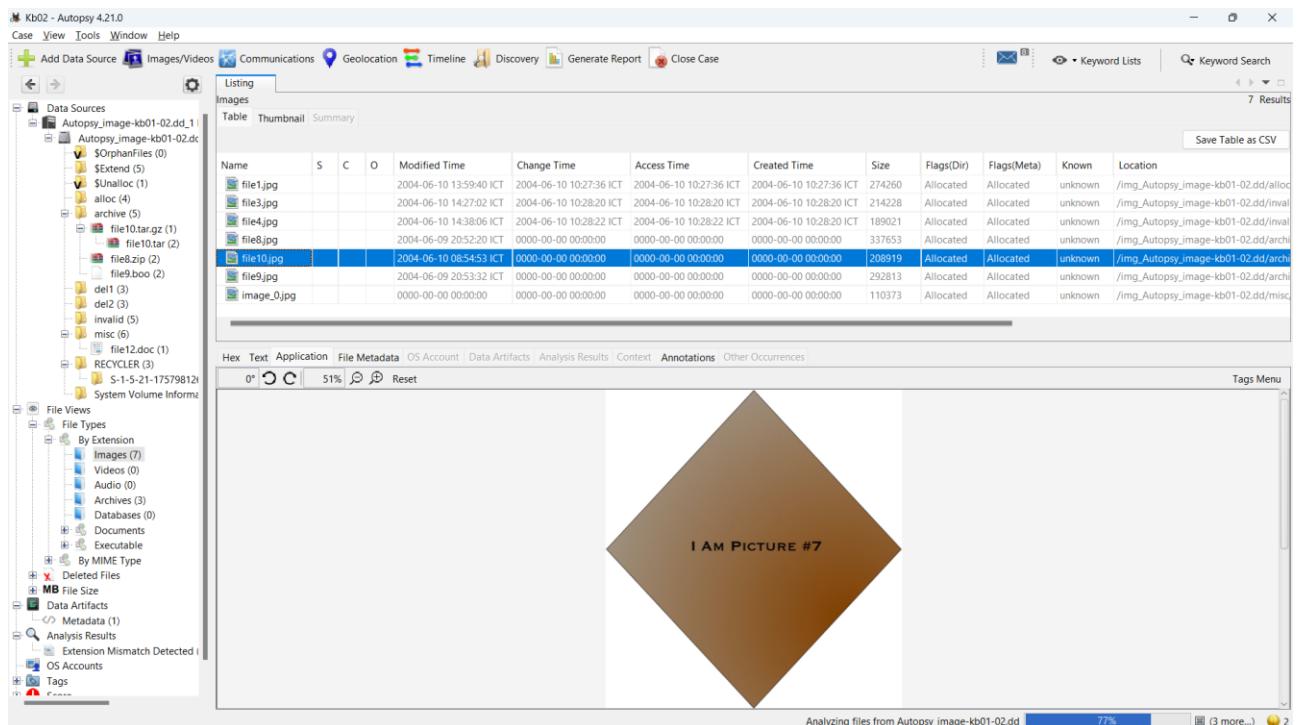


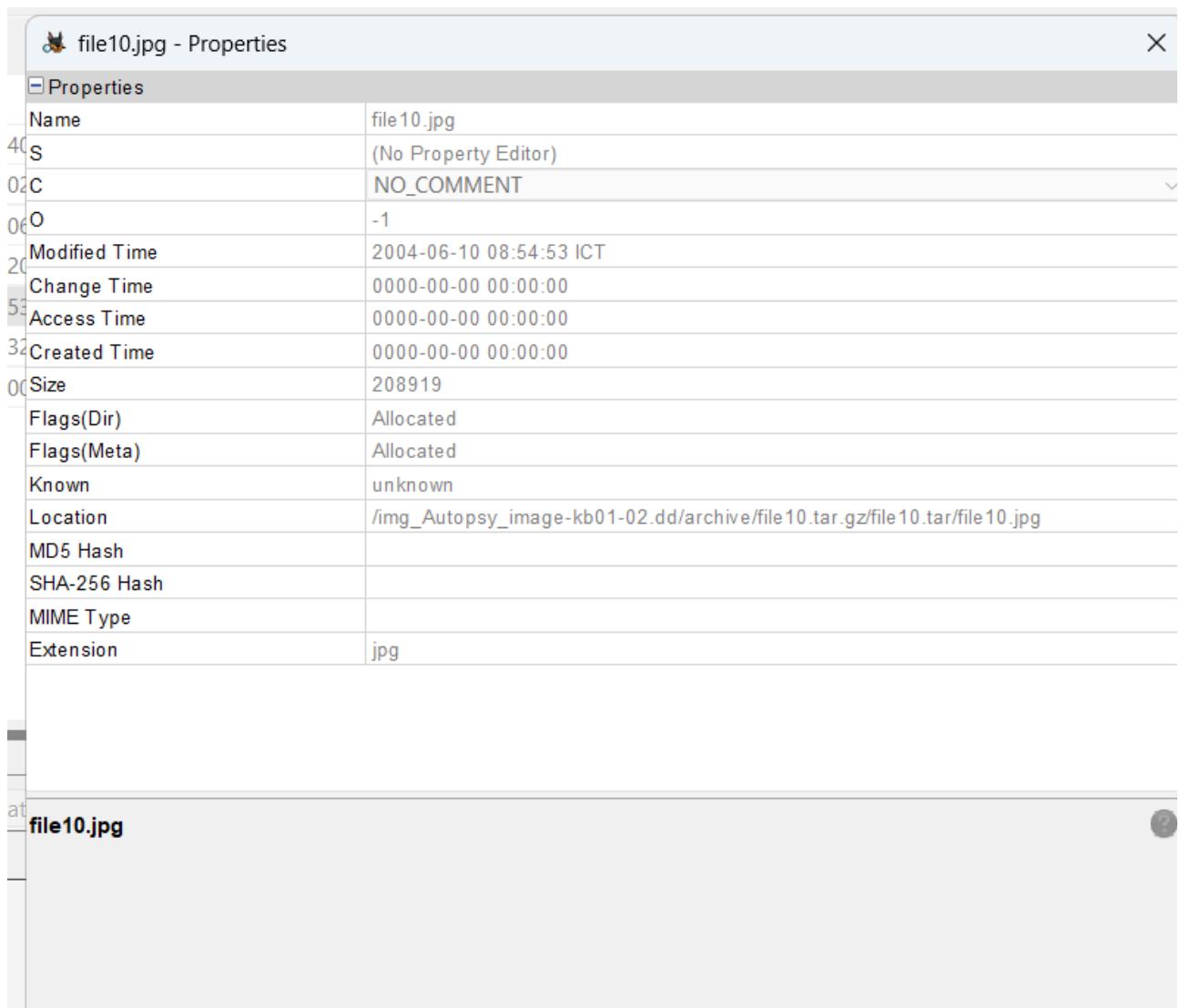
Thông tin file9.jpg



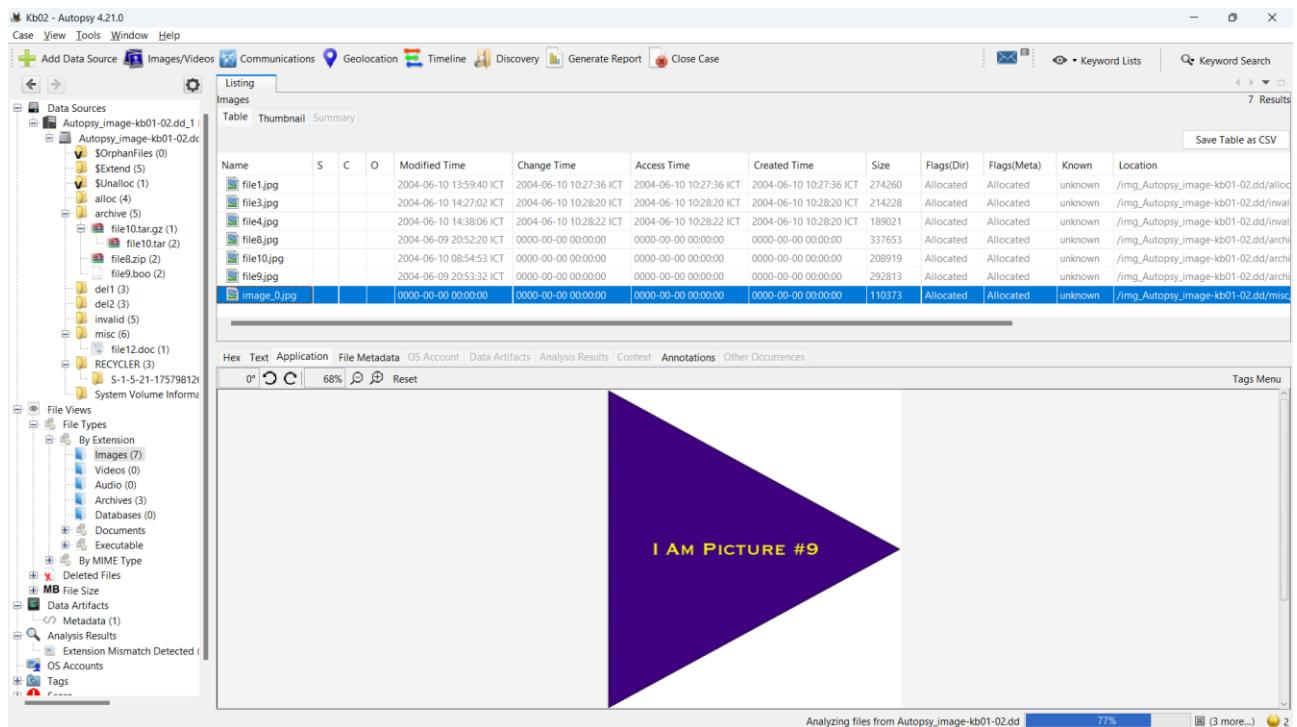


Thông tin file10.jpg





Thông tin file ảnh image0.jpg



image_0.jpg - Properties	
Properties	
Name	image_0.jpg
S	(No Property Editor)
C	NO_COMMENT
O	-1
Modified Time	0000-00-00 00:00:00
Change Time	0000-00-00 00:00:00
Access Time	0000-00-00 00:00:00
Created Time	0000-00-00 00:00:00
Size	110373
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/misc/file12.doc/image_0.jpg
MD5 Hash	
SHA-256 Hash	
MIME Type	
Extension	jpg
Extension	
no description	
Close Help	

Tìm được picture 10 trong thư mục misc

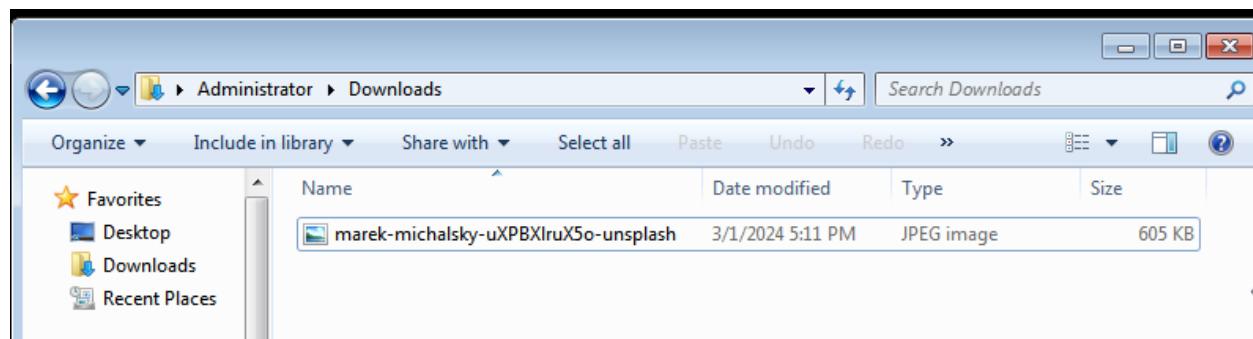
Kết quả phân tích file hình ảnh:

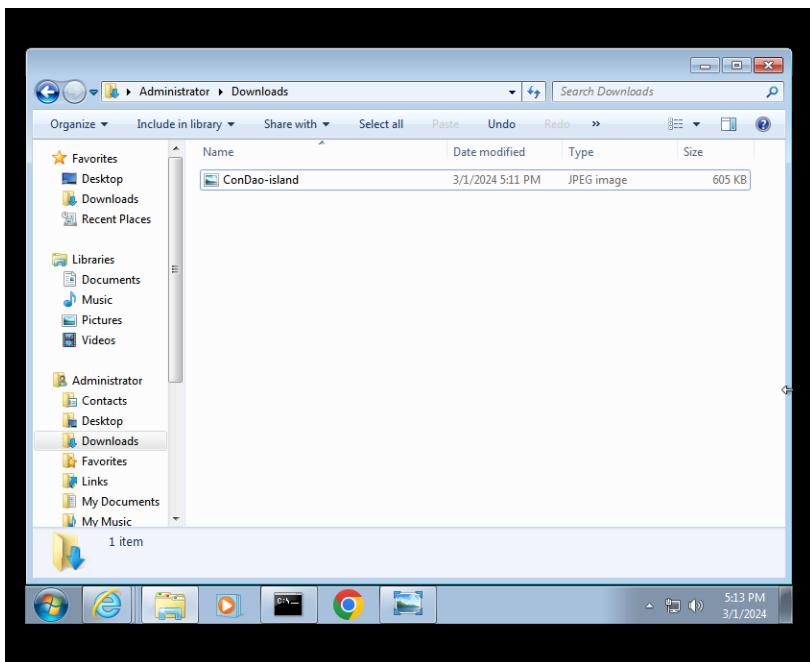
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2004-06-10 10:29:18 ICT	2004-06-10 10:29:18 ICT	2004-06-10 10:29:00 ICT	2004-06-10 10:29:00 ICT	360	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/m
[parent folder]				2004-06-10 10:59:10 ICT	2004-06-10 10:59:10 ICT	2004-06-10 10:59:22 ICT	2004-06-10 10:59:22 ICT	56	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/m
file11.dat				2004-06-10 14:44:46 ICT	2004-06-10 10:29:17 ICT	2004-06-10 10:29:17 ICT	2004-06-10 10:29:17 ICT	272753	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/m
file12.doc				2004-06-10 14:20:58 ICT	2004-06-10 10:29:18 ICT	2004-06-10 10:29:18 ICT	2004-06-10 10:29:17 ICT	131584	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/m
file13.dll				2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	2004-06-10 10:29:18 ICT	58391	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/m
file13.dlhere				2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	2004-06-10 10:29:18 ICT	124038	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.dd/m

Link drive file hình ảnh:

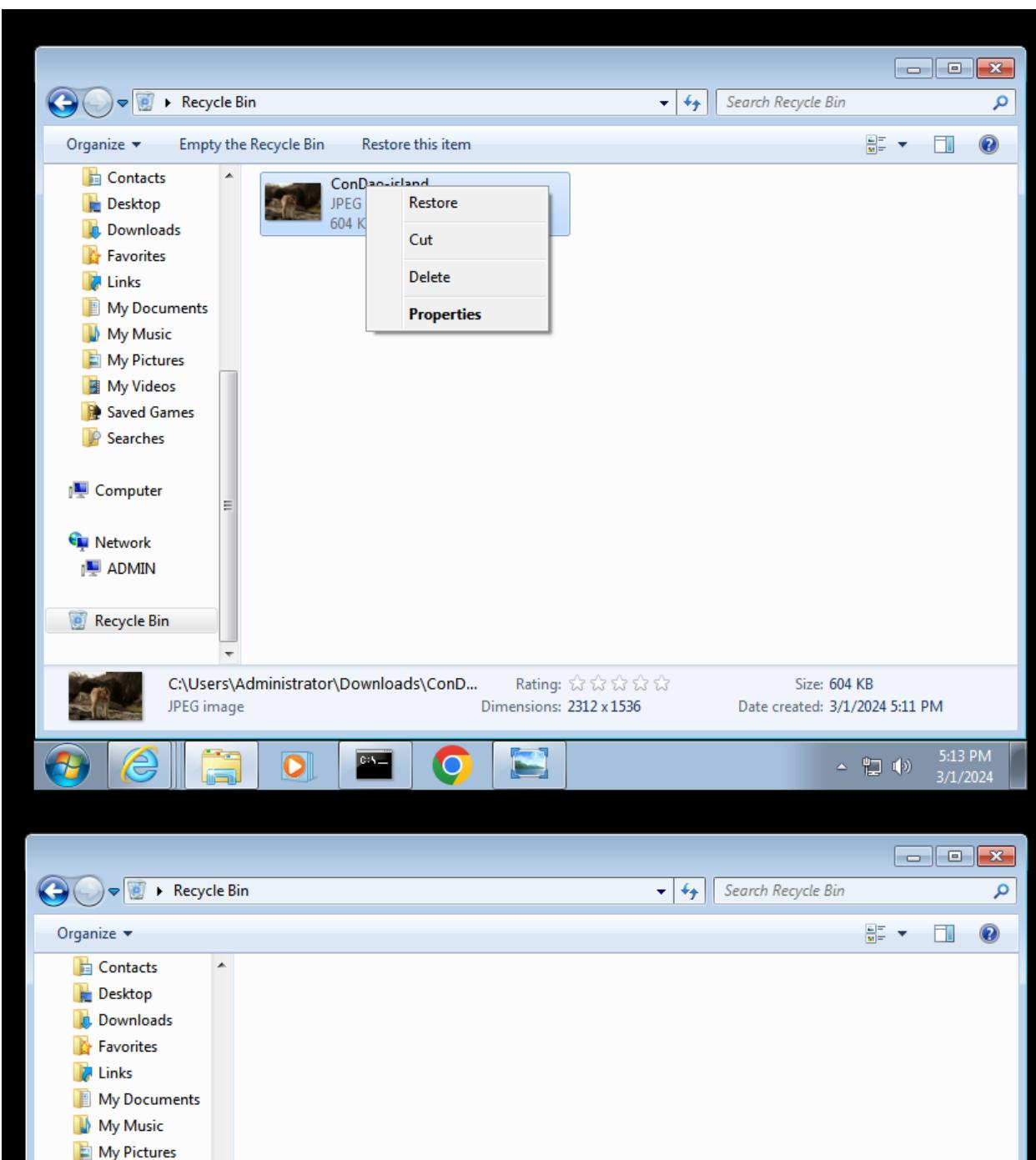
<https://drive.google.com/drive/folders/1NSz8va4VEgd92ns95DQf4ZjHwYB1pHwx>

Kích bản 3

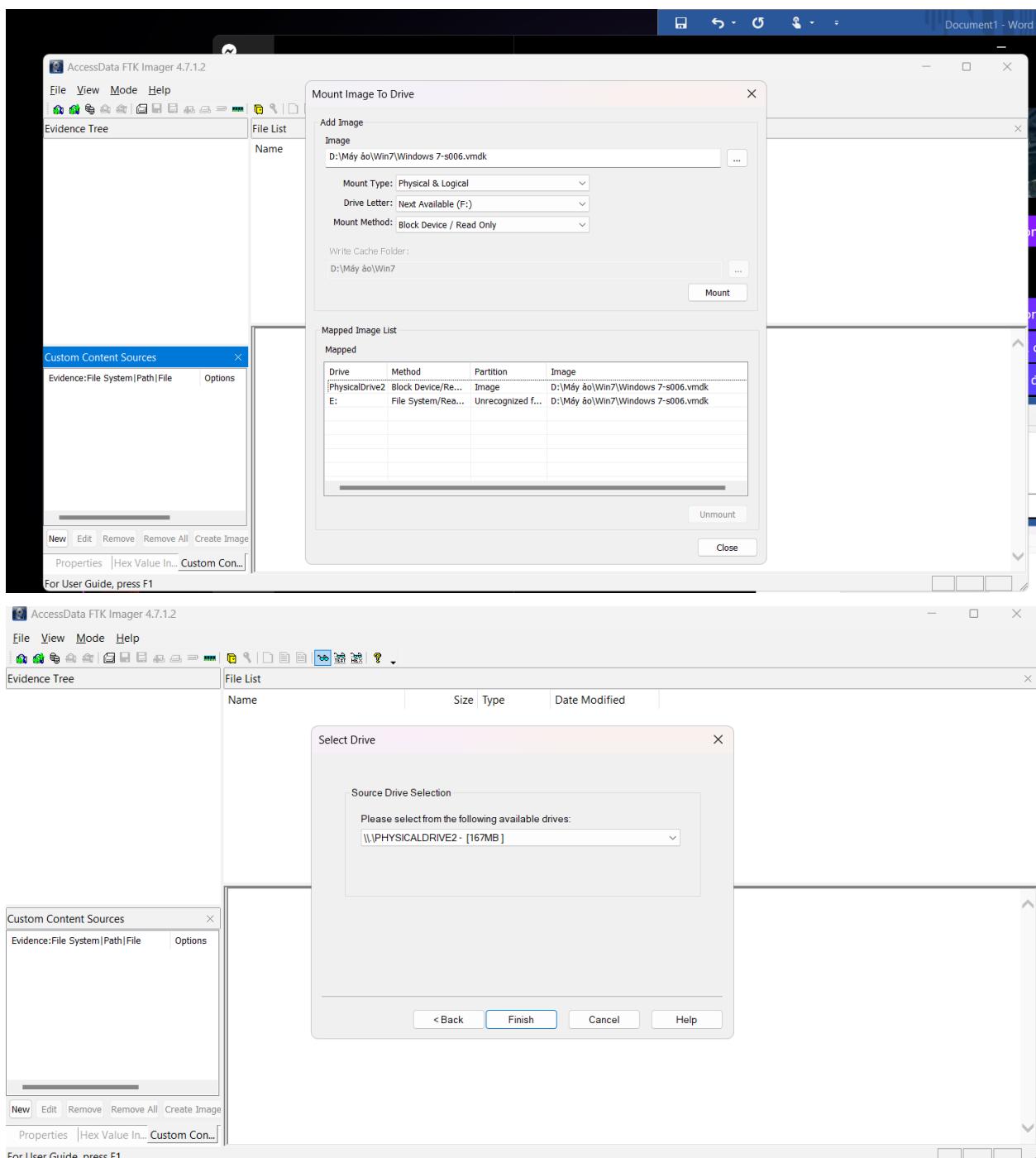




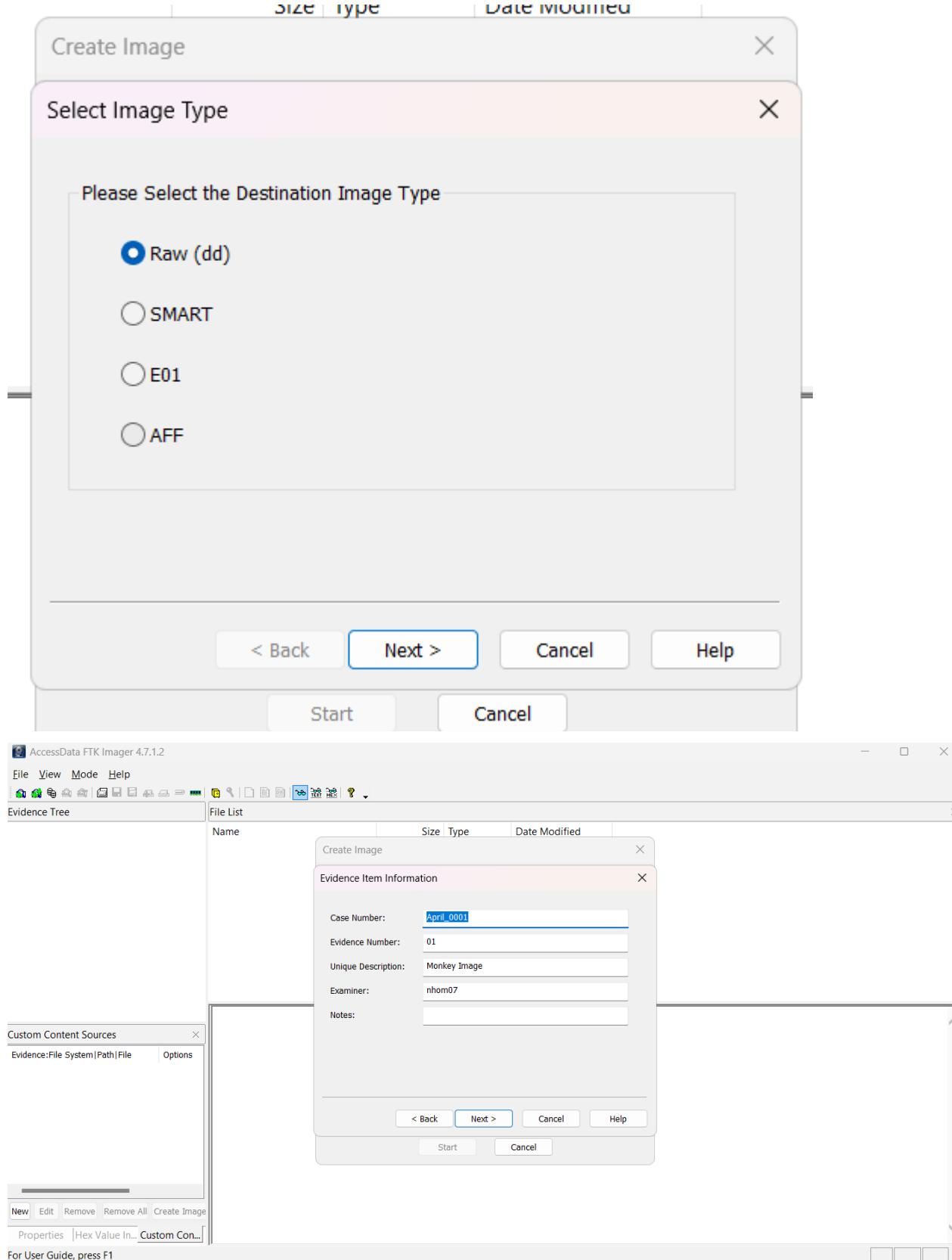
Tải ảnh về và đặt tên theo yêu cầu.

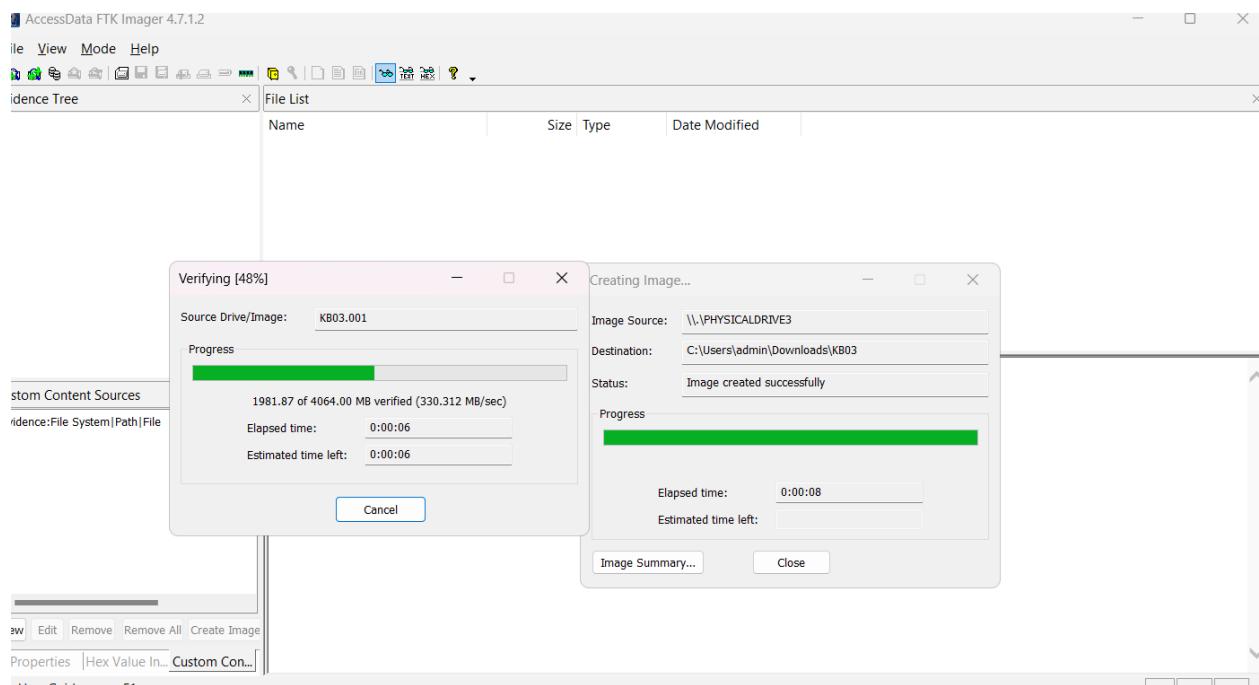


Xóa ảnh sau đó xóa trong thùng rác

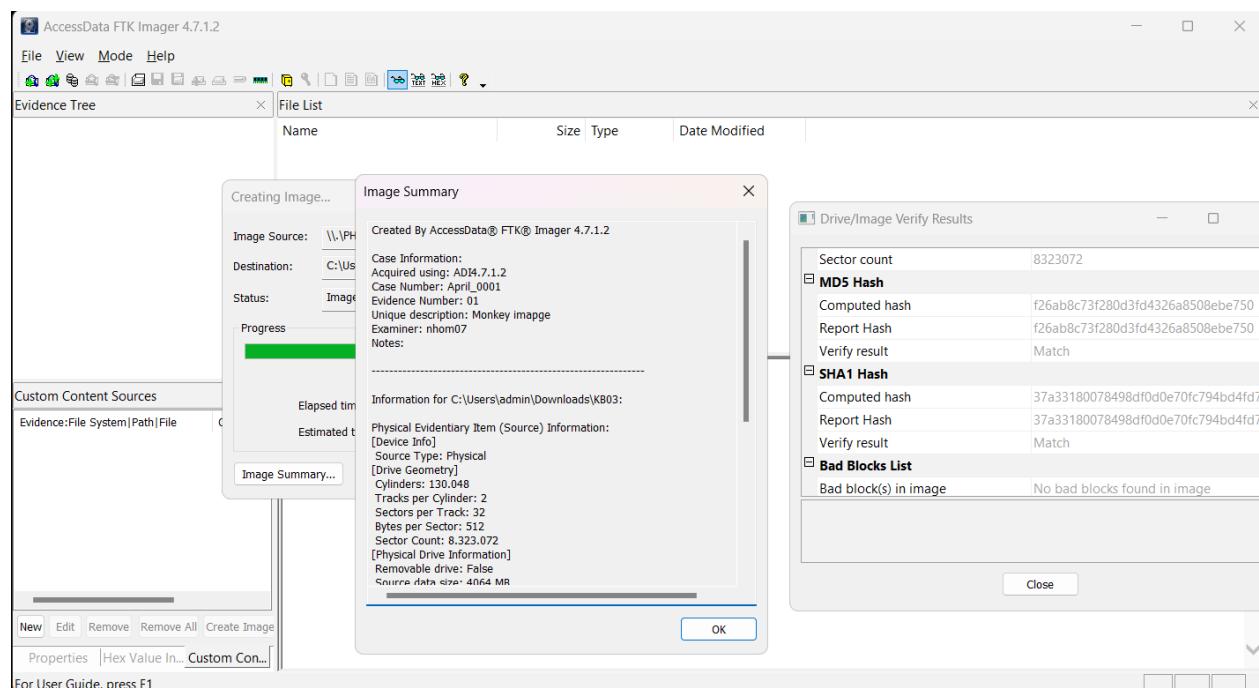


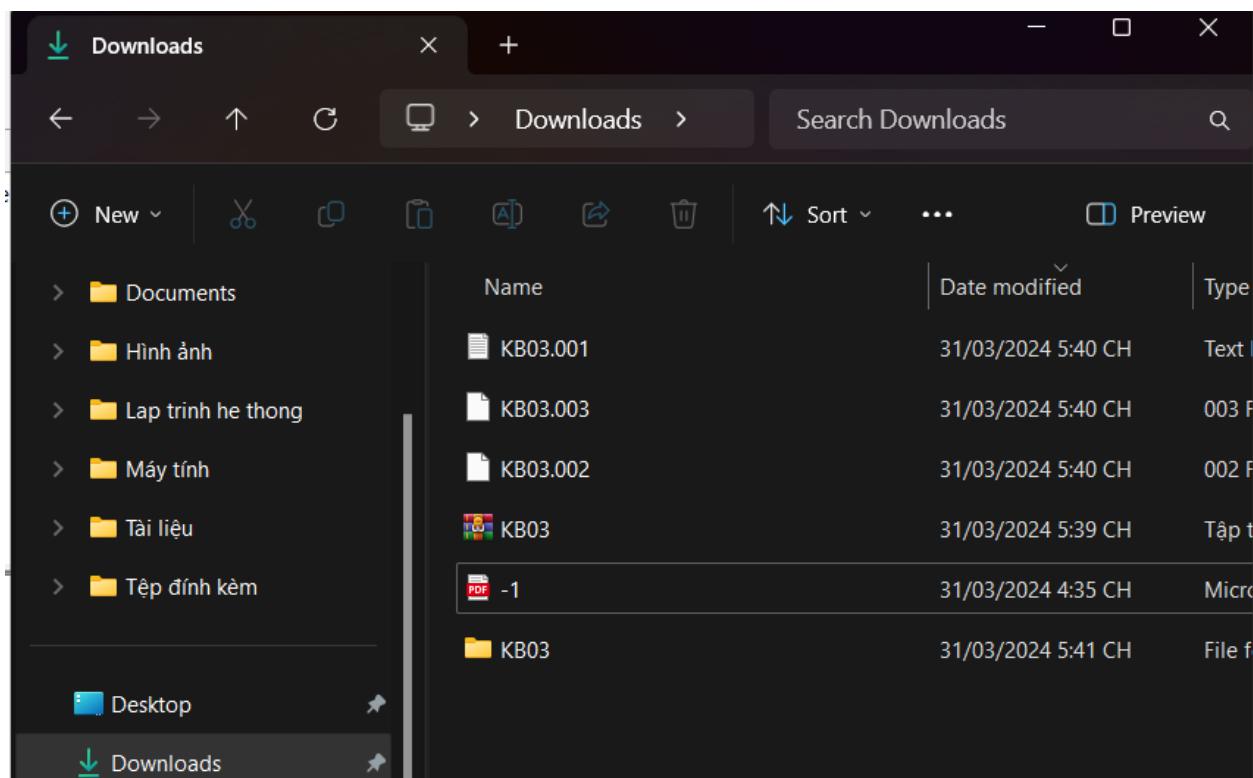
- Tạo một ảnh đĩa -định dạng Raw (dd) sau khi xóa file ảnh trên



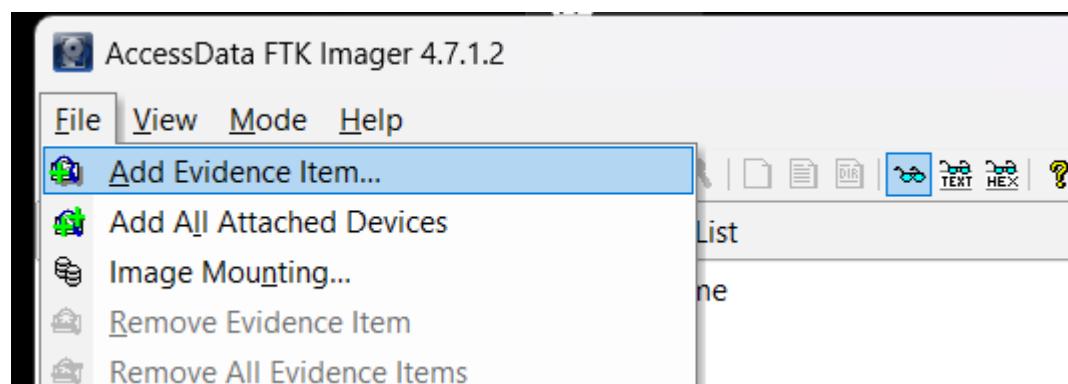


- Ta lưu vào 1 folder và đặt tên là KB3

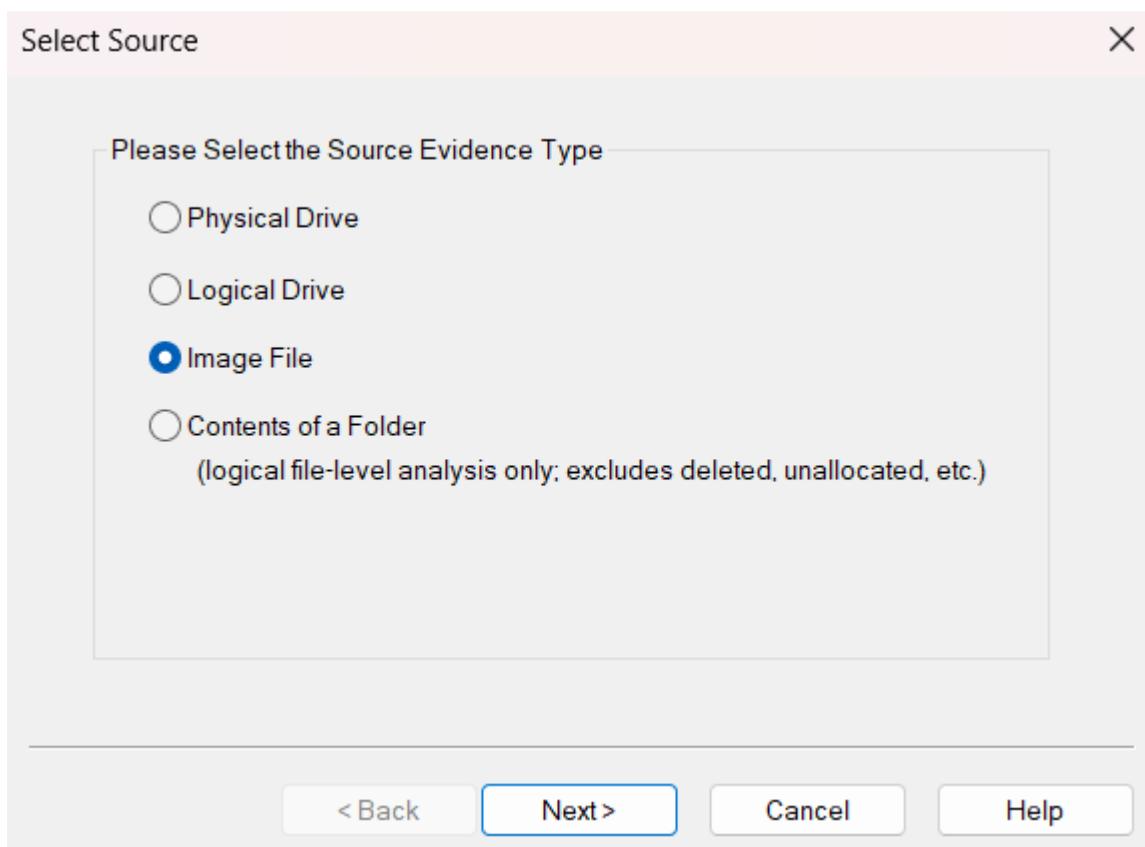




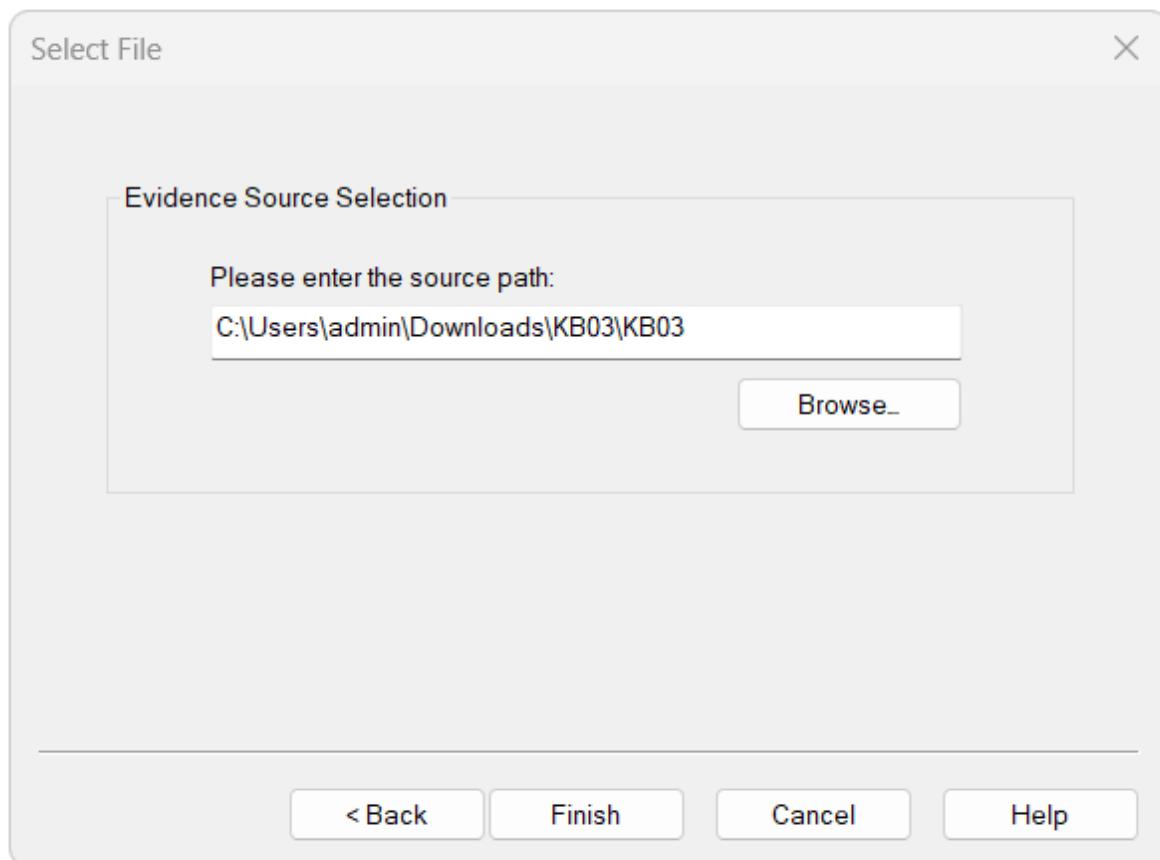
- Trong thư mục KB3 vừa tạo chứa disk image ta vừa tạo

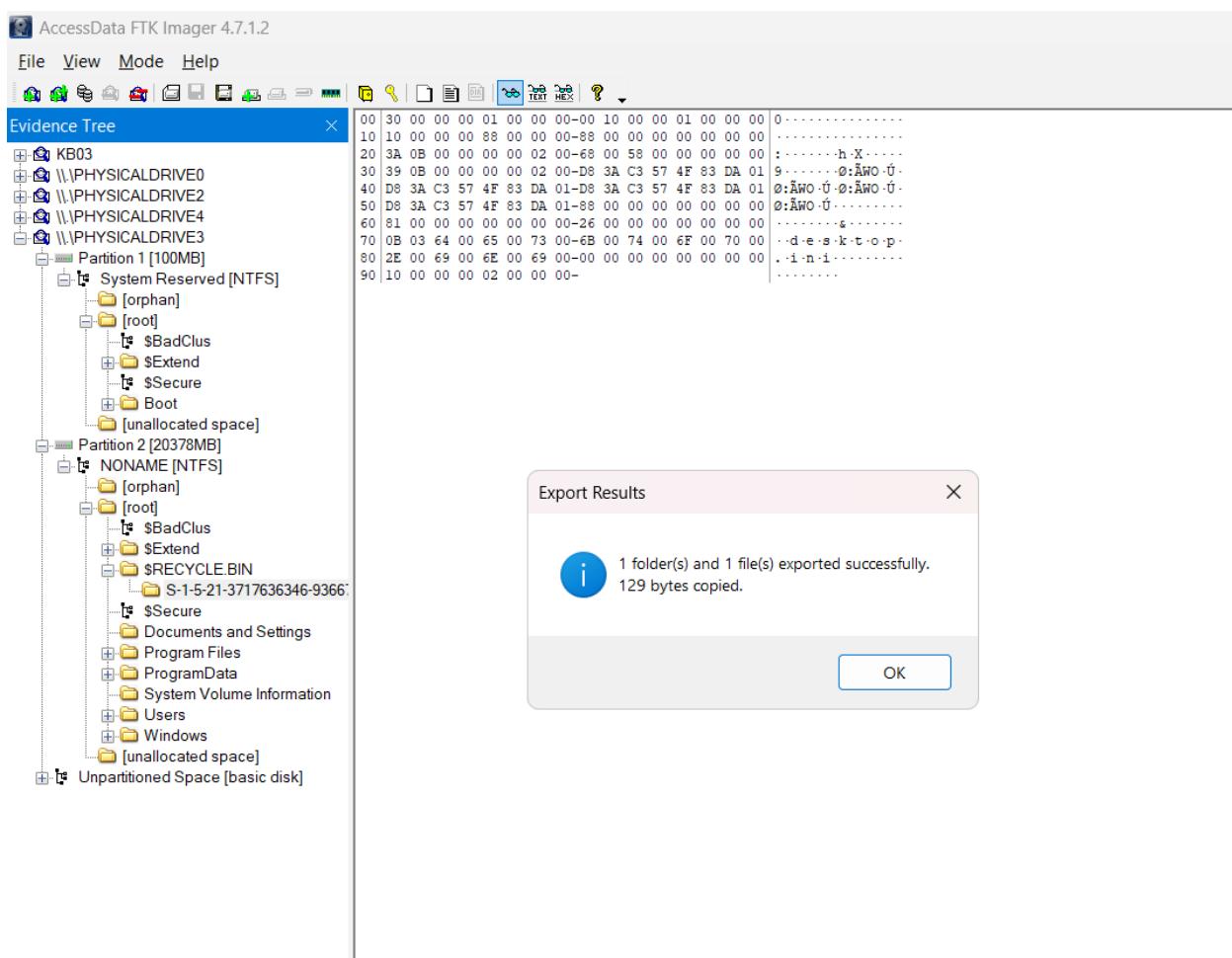
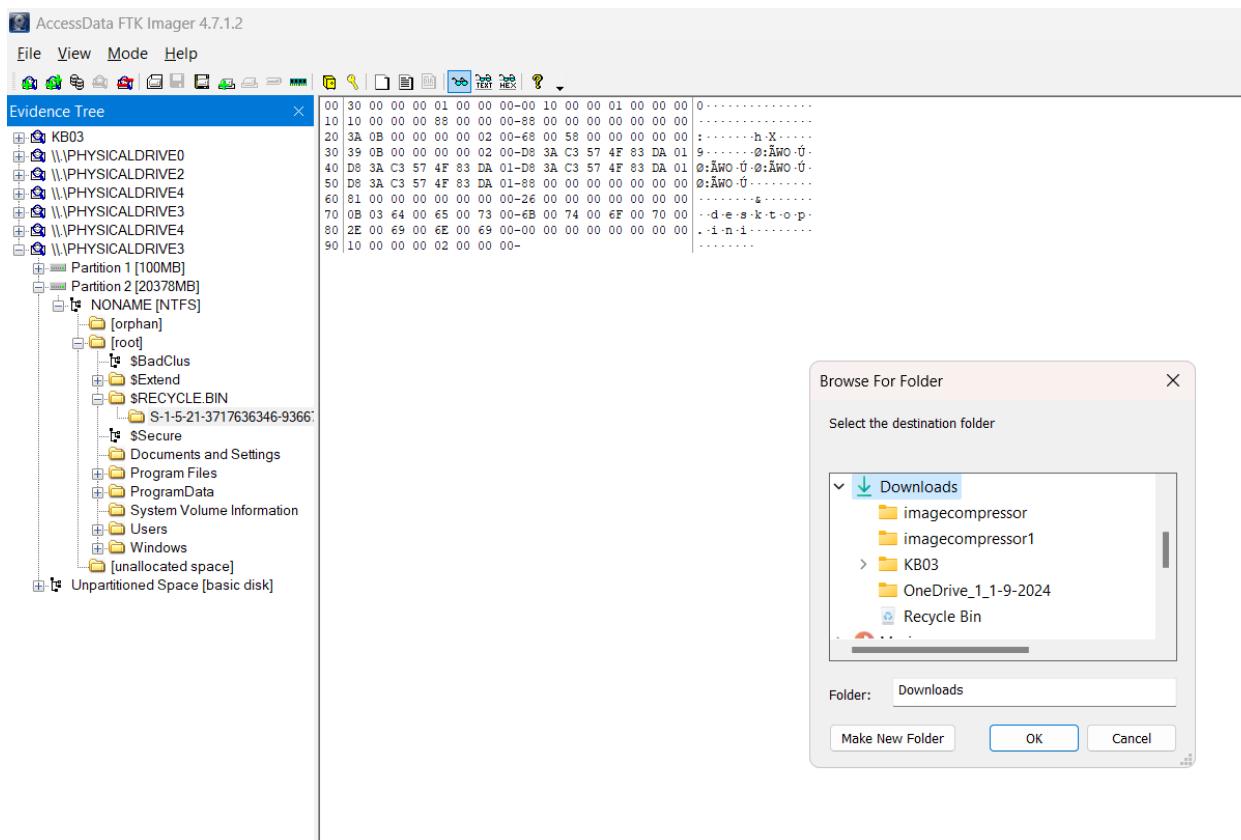


- Để thêm bằng chứng ta chọn file -> add evidence item
- Chọn image file



- Ta chọn disk image vừa tạo trong folder KB03

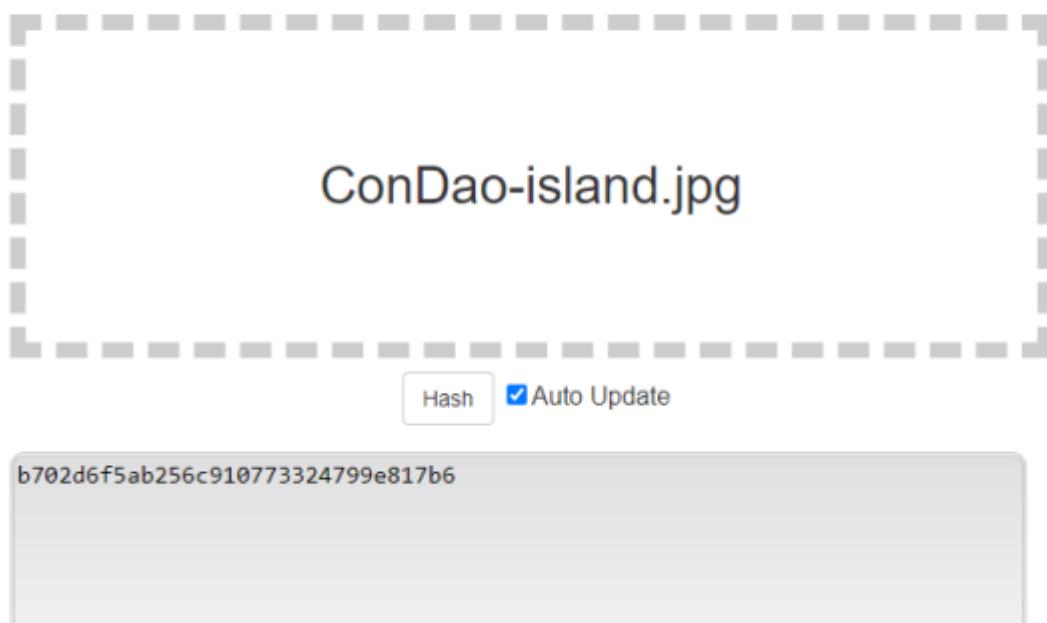




- Tìm được ảnh đã bị xóa trên ổ đĩa. Tiến hành sử dụng tính năng phục hồi file ảnh đã bị xóa (tính năng Export Files),

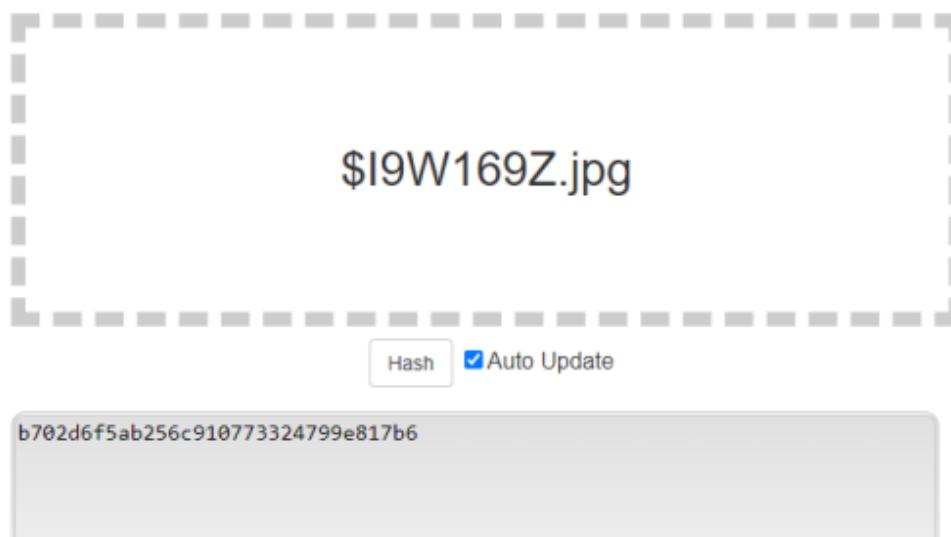
MD5 File Checksum

MD5 online hash file checksum function



MD5 File Checksum

MD5 online hash file checksum function



Kịch bản 4

Kịch bản 04. Thực hiện phân tích:

- Tài nguyên: kb04-session02.bin.gz
- Tìm thông tin có liên quan đến từ khóa “key” trong dữ liệu được cung cấp.

Gợi ý: Tìm hiểu các Master File Table (MFT), mmls, dd, strings, foremost/scalpel

Đáp án:

- Tiến hành phân tích sử dụng Autopsy

Tìm key và thấy key đã bị xóa

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
\$Secure\$\$SDS				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	262940	Allocated	Allocated	unknown
\$UpCase				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	131072	Allocated	Allocated	unknown
\$Volume				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	0	Allocated	Allocated	unknown
2009040811380736734_115018_0.jpg				2010-05-19 07:32:49 ICT	2010-05-19 07:32:49 ICT	2010-05-19 06:52:26 ICT	2010-05-19 06:52:26 ICT	33383	Allocated	Allocated	unknown
2009040811380736734_115018_0.jpg\$Zone.Identifier				2010-05-19 07:32:49 ICT	2010-05-19 07:32:49 ICT	2010-05-19 06:52:26 ICT	2010-05-19 06:52:26 ICT	26	Allocated	Allocated	unknown
carpenter.png				2010-05-19 07:31:41 ICT	2010-05-19 07:31:41 ICT	2010-05-19 06:47:54 ICT	2010-05-19 06:47:54 ICT	9970	Allocated	Allocated	unknown
carpenter.png\$Zone.Identifier				2010-05-19 07:31:41 ICT	2010-05-19 07:31:41 ICT	2010-05-19 06:47:54 ICT	2010-05-19 06:47:54 ICT	26	Allocated	Allocated	unknown
caught.jpg				2010-05-19 07:31:48 ICT	2010-05-19 07:31:48 ICT	2010-05-19 06:49:08 ICT	2010-05-19 06:49:08 ICT	11765	Allocated	Allocated	unknown
caught.jpg\$Zone.Identifier				2010-05-19 07:31:48 ICT	2010-05-19 07:31:48 ICT	2010-05-19 06:49:08 ICT	2010-05-19 06:49:08 ICT	26	Allocated	Allocated	unknown
evidence.jpg				2010-05-19 07:31:48 ICT	2010-05-19 07:31:48 ICT	2010-05-19 06:49:08 ICT	2010-05-19 06:49:08 ICT	13862	Allocated	Allocated	unknown
evidence.jpg\$Zone.Identifier				2010-05-19 07:31:55 ICT	2010-05-19 07:31:55 ICT	2010-05-19 06:48:40 ICT	2010-05-19 06:48:40 ICT	26	Allocated	Allocated	unknown
furries.jpg				2010-05-19 07:32:45 ICT	2010-05-19 07:32:45 ICT	2010-05-19 06:38:20 ICT	2010-05-19 06:38:20 ICT	36947	Allocated	Allocated	unknown
furries.jpg\$Zone.Identifier				2010-05-19 07:32:45 ICT	2010-05-19 07:32:45 ICT	2010-05-19 06:38:20 ICT	2010-05-19 06:38:20 ICT	26	Allocated	Allocated	unknown
images.jpg				2010-05-19 07:33:08 ICT	2010-05-19 07:33:08 ICT	2010-05-19 07:21:00 ICT	2010-05-19 07:21:00 ICT	4378	Allocated	Allocated	unknown
images.jpg\$Zone.Identifier				2010-05-19 07:33:08 ICT	2010-05-19 07:33:08 ICT	2010-05-19 06:49:08 ICT	2010-05-19 06:49:08 ICT	26	Allocated	Allocated	unknown
key				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45:50 ICT	2010-05-19 05:45:50 ICT	0	Unallocated	Unallocated	unknown
key.Zone.Identifier				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45:50 ICT	2010-05-19 05:45:50 ICT	26	Unallocated	Unallocated	unknown
whiteflag.jpg				2010-05-19 07:32:41 ICT	2010-05-19 07:32:41 ICT	2010-05-19 06:51:26 ICT	2010-05-19 06:51:26 ICT	1929	Allocated	Allocated	unknown
whiteflag.jpg\$Zone.Identifier				2010-05-19 07:32:41 ICT	2010-05-19 07:32:41 ICT	2010-05-19 06:51:26 ICT	2010-05-19 06:51:26 ICT	26	Allocated	Allocated	unknown

- Tuy nhiên, NTFS có một thành phần thú vị: Master File Table (MFT) , được hiển thị trong hệ thống tệp NTFS dưới dạng \$ MFT . Tiến hành xem xét nó vì nó có thể vẫn chứa các phần của tệp đã xóa.

- Sử dụng chức năng Launch in HxD, sau đó thực hiện tìm kiếm với từ khóa “key”. Và ta đã đọc tìm được nội dung của file key: “notdeleted, neverexisted”

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00009760	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00009770	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00009780	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00009790	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000097A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000097B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000097C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000097D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000097E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000097F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0B	00
00009800	46 49 4C 45 30 00 03 00 45 5C 10 00 00 00 00 00	FILE0...E\.....
00009810	02 00 01 00 38 00 00 00 A0 01 00 00 00 04 00 008.....
00009820	00 00 00 00 00 00 00 00 04 00 00 00 26 00 00 00&....
00009830	0A 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00`....
00009840	00 00 00 00 00 00 00 48 00 00 00 18 00 00 00 00H.....
00009850	00 63 07 DD DB F6 CA 01 A0 55 D7 B1 EA F6 CA 01	.c.ÝÙöÊ. U×±êöÊ.
00009860	A0 55 D7 B1 EA F6 CA 01 00 63 07 DD DB F6 CA 01	U×±êöÊ..c.ÝÙöÊ.
00009870	20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00009880	00 00 00 00 05 01 00 00 00 00 00 00 00 00 00 00
00009890	00 00 00 00 00 00 00 30 00 00 00 60 00 00 00 000....`....
000098A0	00 00 00 00 00 02 00 48 00 00 00 18 00 01 00 00H.....
000098B0	05 00 00 00 00 05 00 E0 77 98 B1 EA F6 CA 01àw~±êöÊ.
000098C0	E0 77 98 B1 EA F6 CA 01 E0 77 98 B1 EA F6 CA 01	àw~±êöÊ.àw~±êöÊ.
000098D0	E0 77 98 B1 EA F6 CA 01 00 00 00 00 00 00 00 00 00	àw~±êöÊ.....
000098E0	00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
000098F0	03 03 6B 00 65 00 79 00 80 00 00 00 48 00 00 00	..k.e.y.€...H...
00009900	00 00 18 00 00 00 01 00 00 00 00 18 00 00 00 00
00009910	6E 00 6F 00 74 00 64 00 65 00 6C 00 65 00 74 00	n.o.t.d.e.l.e.t.
00009920	65 00 64 00 2C 00 6E 00 65 00 76 00 65 00 72 00	e.d.,.n.e.v.e.r.
00009930	65 78 69 73 74 65 64 0D 0A 00 00 00 00 00 00 00	existed.....
00009940	80 00 00 00 58 00 00 00 00 0F 18 00 00 00 03 00	€...X.....
00009950	1A 00 00 00 38 00 00 00 5A 00 6F 00 6E 00 65 008...Z.o.n.e.
00009960	2E 00 49 00 64 00 65 00 6E 00 74 00 69 00 66 00	..I.d.e.n.t.i.f.
00009970	69 00 65 00 72 00 00 00 5B 5A 6F 6E 65 54 72 61	i.e.r...[ZoneTra
00009980	6E 73 66 65 72 5D 0D 0A 5A 6F 6E 65 49 64 3D 33	nsfer]..ZoneId=3
00009990	0D 0A 00 00 00 00 00 00 FF FF FF FF 82 79 47 11ÿÿÿ,yG.
000099A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000099B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000099C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000099D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000099E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000099F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0A 00
00009A00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00009A10	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Offset(h): 0

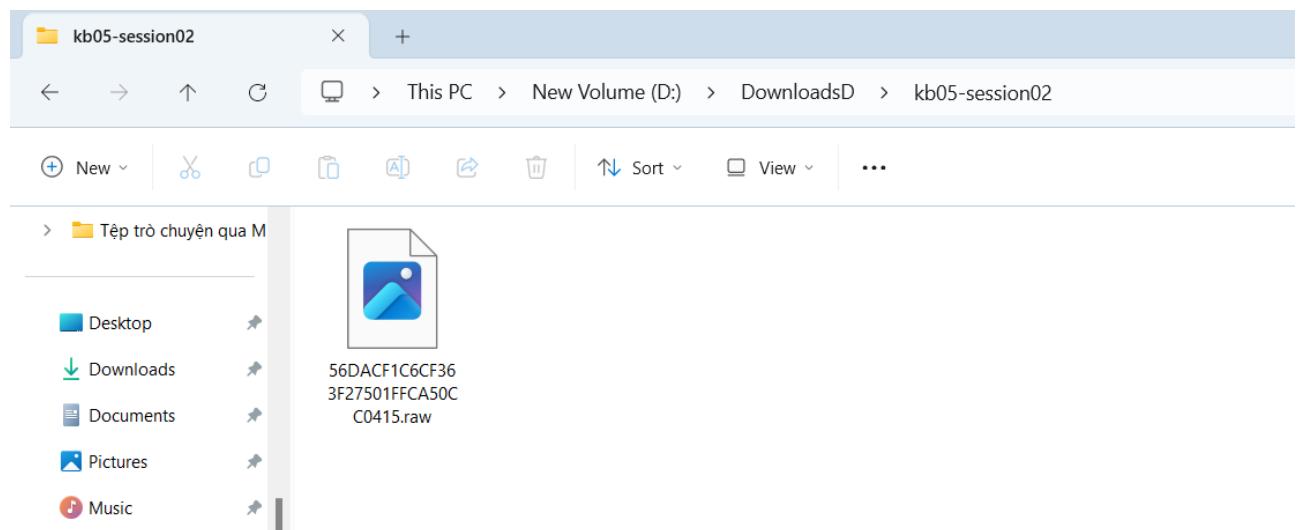
Kích bản 5

Kịch bản 05. Thực hiện phân tích:

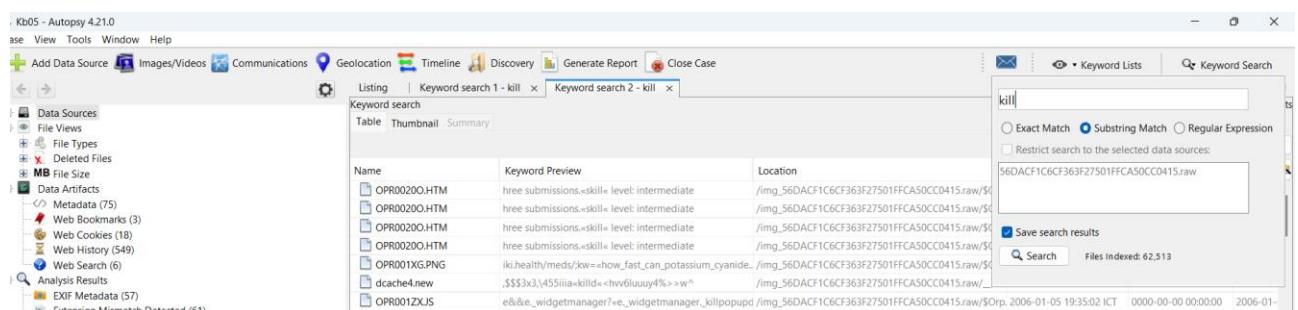
- Tài nguyên: kb05-session02
- Cảnh sát phát hiện một vụ án tình nghi một người đàn ông chết do tự tử. Bằng chứng thu được từ máy tính nạn nhân được gửi cho điều tra viên. Đóng vai làm nhân viên điều tra, hãy tìm manh mối xác định liệu kết luận tình nghi này có đúng hay không.

Đáp án:

Đổi file kb05-session02 thành file zip rồi extract ra và phân tích với autopsy.



- Thực hiện tìm kiếm các từ liên quan đến chết hoặc tự tử như là kill, dead, ... bằng option substring.



- Ta thấy người đàn ông có tìm kiếm 1 thông tin đại khái là cách chất độc cyanide có thể giết ta trong bao lâu(How_fast_can_potassium_cyanide_kill_you) ở 1 trang tìm kiếm tên là “doubleclick.net”.

Keyword search

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
OPR001ZXJS	e&&e._widgetmanager?«e._widgetmanager._killpopupd	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:35:02 ICT	0000-00-00 00:00:00	2006-01-	
OPR001XG.PNG	iki.health/meds/kw=«how_fast_can_potassium_cyanide..	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-	
DCACHE4.NEW	iki.health/meds/kw=«how_fast_can_potassium_cyanide..	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-04 19:00:52 ICT	0000-00-00 00:00:00	2006-01-	
OPR0020KJS	52f}; }; // global «killswitch» on the element if (/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-	
OPR0020KJS	52f}; }; // global «killswitch» on the element if (/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-	
OPR0028YJS	re;, used mostly to «kill» successive calls to	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-	
OPR0028YJS	re;, used mostly to «kill» successive calls to	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-	
OPR001ZXJS	e&&e._widgetmanager?«e._widgetmanager._killpopupd	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:35:02 ICT	0000-00-00 00:00:00	2006-01-	
OPR001ZXJS	e&&e._widgetmanager?«e._widgetmanager._killpopupd	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:35:02 ICT	0000-00-00 00:00:00	2006-01-	
OPR00200.HTM	hree submissions.«skill» level: intermediate	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-	
OPR001XG.PNG	iki.health/meds/kw=«how_fast_can_potassium_cyanide..	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-	
OPR0020KJS	52f}; }; // global «killswitch» on the element if (/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-	
OPR0020KJS	52f}; }; // global «killswitch» on the element if (/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-	
OPR0020KJS	52f}; }; // global «killswitch» on the element if (/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-	
OPR0020KJS	52f}; }; // global «killswitch» on the element if (/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-	
Unalloc_58621_117248_487.\$\$.3x3,\455iiia«killd«<hv6luuy4%>w^	/img_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Una 0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-	

Save Table as CSV

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: 1 of 1 Match

Text Source: Search Results

```
http://ad.doubleclick.net/adi/wiki.health/meds/kw=How_fast_can_potassium_cyanide_kill_you;csrc=unanswered;pos=1;answ=ad;tile=1;dcopt=ist;sz=160x600;ord=698466684?
text/html
Tue, 09 Mar 2010 06:09:13 GMT
text/html
gzip
opr001BT.htm
Http://w.sharethiOPR001KHPNG
$4$4
Aopr00
1Klpn
OPR001KIPNG
...
```

Có lẽ như người dùng này dự kiến kết liễu bản thân bằng potassium cyanide (Kali cyanide)

Tiếp tục tìm thử thông tin về potassium.

Keyword search						277 Results
Table	Thumbnail	Summary	Save Table as CSV			
Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	
COOKIES4.NEW	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-06 12:05:32 ICT	0000-00-00 00:00:00	2006-01-06 0	2006-01-06 0	
OPR001XG.PNG	iki.health/meds/kw=«how_fast_can_potassium_cyanide.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 0	2006-01-05 0	
OPR001XG.PNG-slack	ere%2bcan%2bi%2bbuy%2bpotassium%2bcyanide+.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 0	2006-01-05 0	
_PR001L.GIF-slack	ere%20can%20i%20buy%20potassium%20cyanide_u.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-04 18:52:54 ICT	0000-00-00 00:00:00	2006-01-04 0	2006-01-04 0	
_PR001V1.GIF-slack	ere%20can%20i%20buy%20potassium%20cyanide_u.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-05 19:29:18 ICT	0000-00-00 00:00:00	2006-01-05 0	2006-01-05 0	
_PR001V2.GIF-slack	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-05 19:29:18 ICT	0000-00-00 00:00:00	2006-01-05 0	2006-01-05 0	
COOKIES4.DAT	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-05 19:47:32 ICT	0000-00-00 00:00:00	2006-01-05 0	2006-01-05 0	
COOKIES4.DAT	ere%20can%20i%20buy%20potassium%20cyanide_u.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-06 12:53:02 ICT	0000-00-00 00:00:00	2006-01-06 0	2006-01-06 0	
DCACHE4.URL	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-06 12:04:32 ICT	0000-00-00 00:00:00	2006-01-06 0	2006-01-06 0	
cookies4.dat	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw _TF..	2006-01-06 12:53:02 ICT	0000-00-00 00:00:00	2006-01-06 0	2006-01-06 0	
_OOKIES4.NEW	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-05 19:47:32 ICT	0000-00-00 00:00:00	2006-01-05 0	2006-01-05 0	
VLINK4.DAT	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-06 12:04:32 ICT	0000-00-00 00:00:00	2006-01-06 0	2006-01-06 0	
_OOKIES4.OLD	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-05 19:46:30 ICT	0000-00-00 00:00:00	2006-01-05 0	2006-01-05 0	
COOKIES4.DAT	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-06 12:05:32 ICT	0000-00-00 00:00:00	2006-01-06 0	2006-01-06 0	
COOKIES4.DAT	ctr=where+can+i+buy+«potassium»+cyanide utmcmd.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-04 19:00:50 ICT	0000-00-00 00:00:00	2006-01-04 0	2006-01-04 0	
_PR001IL.GIF-slack	ere%20can%20i%20buy%20potassium%20cyanide_u.. /img_56DACE1C6CF363F27501FFCA50CC0415.raw \$Orp	2006-01-04 18:52:54 ICT	0000-00-00 00:00:00	2006-01-04 0	2006-01-04 0	

Ta thấy được thông tin người này đang tìm mua potassium cyanide với thông tin
where+can+i+buy+potassium+cyanide.

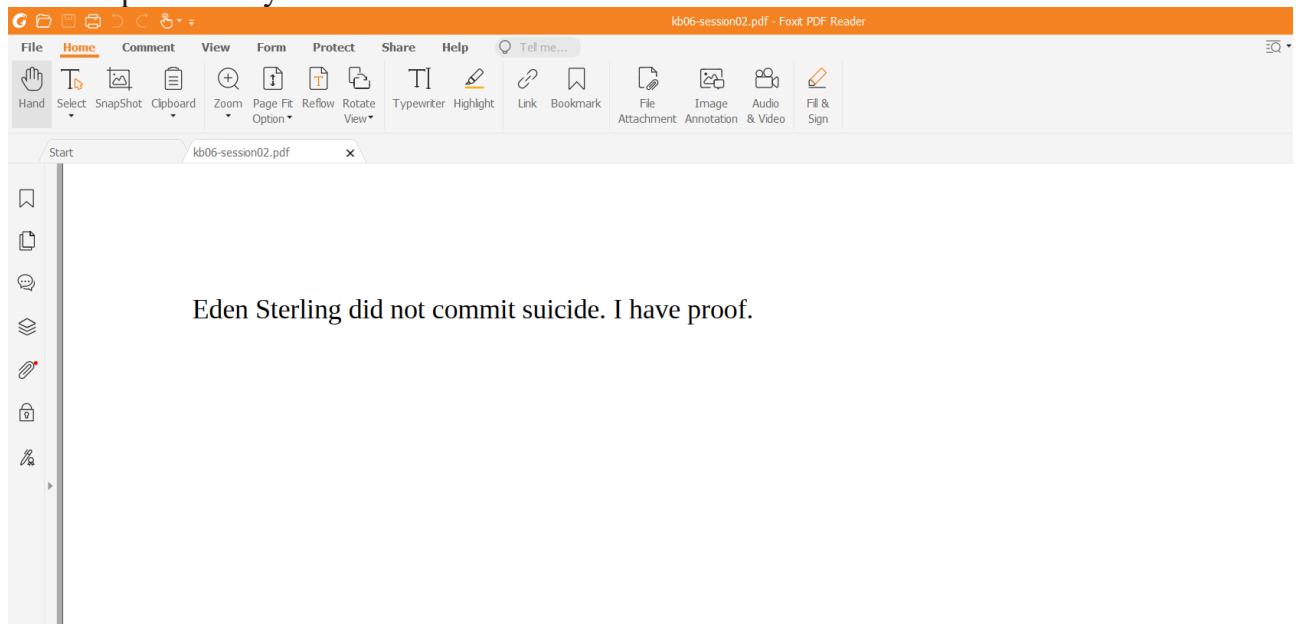
Vậy ta kết luận là ông này tự tự bằng potassium cyanide.

Kịch bản 06:

Kịch bản 06. Thực hiện phân tích:

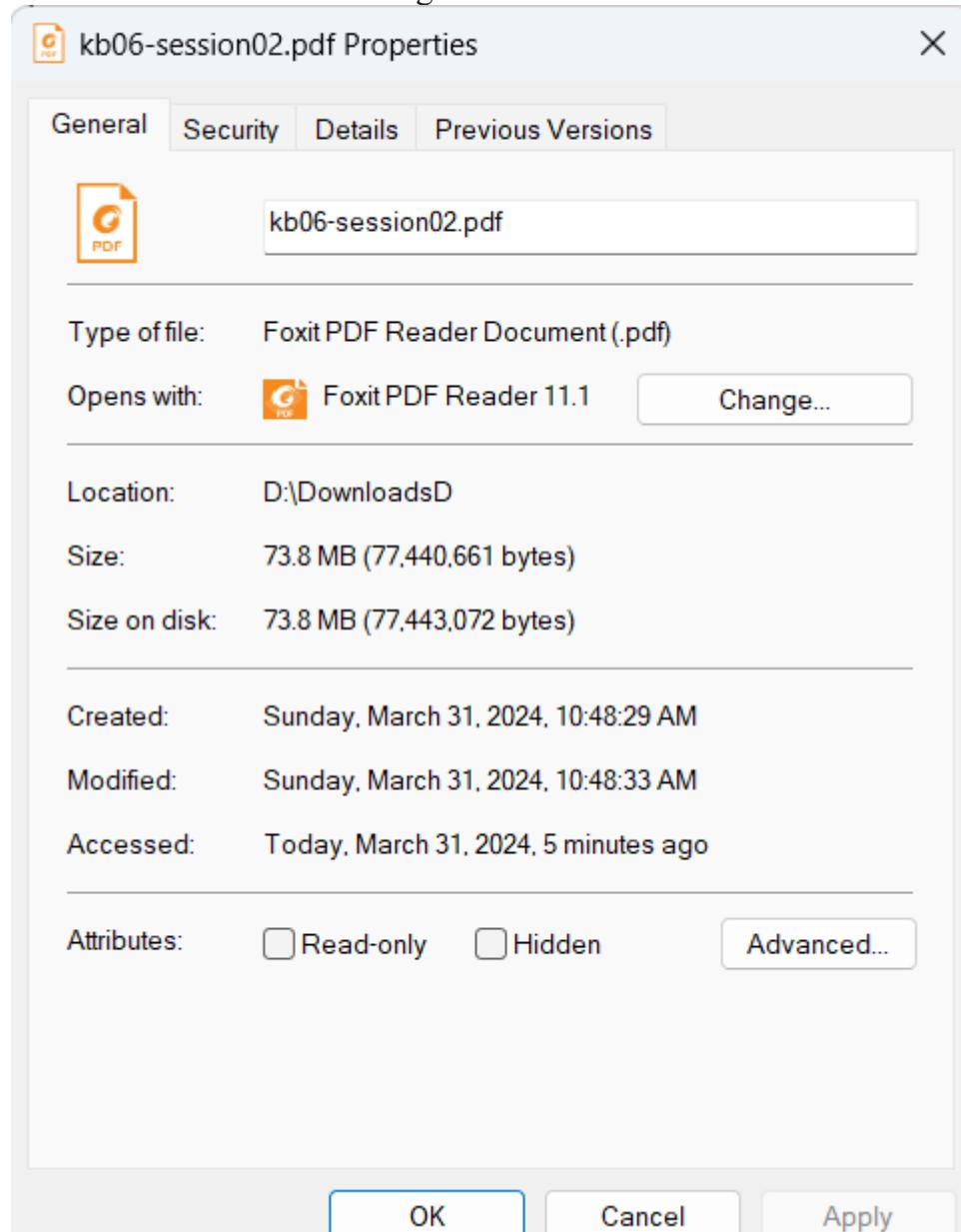
- Tài nguyên: kb06-session02.pdf
- Chúng tôi đảm nhiệm vai trò là đội ngũ điều tra viên pháp y trong vụ án tự tử của một thanh niên tên là Eden (đã đổi tên nạn nhân). Anh ta được tìm thấy trong tình trạng đã chết bên ngoài ngôi nhà của mình. Từ những gì đội cảnh sát có thể phục hồi, có vẻ như Eden đã trèo lên mái nhà ba tầng của mình và nhảy xuống vào ban đêm. Eden là một lập trình viên thực sự tài năng tại trường trung học Hacker. Anh ấy luôn có điểm số cao nhất trong lớp. Tuy nhiên, vào đầu ngày hôm nay nhóm điều tra nhận được một tập tin đính kèm pdf có kích thước lớn đáng ngờ, được gửi tới bằng một thư điện tử ẩn danh. Trong bức thư này, chúng tôi cũng nhận được cảnh báo rõ ràng là không được mở trực tiếp tệp tin đính kèm, cũng như gửi nó cho ai khác (thí dụ như chuyên gia điều tra pháp chứng kỹ thuật số có chuyên môn cao như các bạn). Đội ngũ điều tra pháp y của chúng tôi hoàn toàn xuất thân từ những sinh viên đại học tốt nghiệp ngành hóa học và sinh học; do đó không có kiến thức liên quan đến điều tra kỹ thuật số. Tuy nhiên, trong trường hợp này, việc điều tra một bằng chứng đáng ngờ từ tập tin đính kèm đáng ngờ này dường như là một manh mối mới. Chúng tôi không thể cung cấp cho nhóm điều tra của các bạn thêm nhiều thông tin khác liên quan đến vụ án, do chính sách bảo mật và kiểm duyệt thông tin được đưa ra bởi hiệu trưởng của ngôi trường mà Eden theo học. Chúng tôi không được phép hỏi các học sinh khác quá nhiều về thông tin liên quan tới Eden, cũng như cha mẹ của anh ta không cho phép phân tích thêm về các vật dụng cá nhân của anh ấy (máy tính xách tay, điện thoại di động, v.v.). Tất cả chúng ta có là tập tin đính kèm đáng ngờ. Hãy điều tra các thông tin liên quan đến vụ án này theo một số câu hỏi gợi ý sau:

Mở file pdf thì thấy



Thử check size của file pdf này thì thấy tới gần 74MB mặc dù chỉ có một dòng như trên nén

có thể là có file ẩn ở bên trong



Dùng binwalk để kiểm tra và trích xuất các file ẩn bên trong ra.

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PDF document, version: "1.4"
147	0x93	Zlib compressed data, default compression
39724507	0x25E25DB	xz compressed data
39767781	0x25ECEE5	xz compressed data
39820771	0x25F9DE3	xz compressed data
39820951	0x25F9E97	xz compressed data
39899694	0x260D22E	xz compressed data
39935872	0x2615F80	xz compressed data
40009219	0x2627E03	xz compressed data
40013387	0x2628E4B	xz compressed data
40092191	0x263C21F	xz compressed data
40128120	0x2644E78	xz compressed data
40205040	0x2657AF0	xz compressed data
40209788	0x2658D7C	xz compressed data
40249502	0x266289E	xz compressed data
40329277	0x267603D	xz compressed data
40375259	0x26813DB	xz compressed data
40416593	0x268B551	xz compressed data
40503101	0x26A073D	xz compressed data
40518625	0x26A43E1	xz compressed data
40559387	0x26AE31B	xz compressed data
40643923	0x26C2D53	xz compressed data
40687748	0x26CD884	xz compressed data
40729959	0x26D7D67	xz compressed data
40817626	0x26ED3DA	xz compressed data
40834367	0x26F153F	xz compressed data
40875601	0x26FB651	xz compressed data

Ta thấy đa số các file giống nhau và đa số là file junk. Thấy có vài file zlib lạ lạ và một file 93 không rõ extension là gì

Session 01: Memory Forensics

```
(lixsong㉿kali)-[~/Downloads/_kb06-session02.pdf.extracted]
$ ls
25E25DB 267603D.xz 2725338 2707D5C.xz 28CD89B 29A917E.xz 2ABA087 2B33655.xz 2C55F6A 2D0700E.xz 2DBA582 2E23B18.xz 2EBCC34
25E25DB.xz 26813DB 2725338.xz 27DE061 28CD89B.xz 29BCADE 2ABA087.xz 2B30586 2C55F6A.xz 2D18CFA 2DBA582.xz 2E2E1AB 2EBCC34.xz
25ECE5 268B551 273ACAC.xz 27F21E8 28CD08.xz 29D1B61 2ABD46F.xz 2B30586.xz 2C9557E 2D18CFA.xz 2DC3B57 2E2E1AB.xz 2EC9F9A
25ECE5.xz 268B551.xz 273ACAC.xz 27F21E8.xz 28E19DF 2901B61.xz 2AC5D1D 2B4878D.xz 2CA3D4D 2D08371.xz 2DC3B57.xz 2E4038A 2EC9F9A.xz
25F9DE3 268B551.xz 273ECB9 27F21E8.xz 28E19DF 2901B61.xz 2AC5D1D 2B4878D.xz 2CA3D4D 2D08371.xz 2DC46E9 2E4038A.xz 2ED3804
25F9DE3.xz 26A073D 273ECB9.xz 28075C1 28E19DF.xz 29E6F01 2AC5D1D.xz 2B5015E 2CA3D4D.xz 2D2C429 2DCA0E9.xz 2E4E46C 2ED3804.xz
25F9E97 26A073D.xz 27490C6 28075C1.xz 28F0816 29E6F01.xz 2ACF983 2B5015E.xz 2CA4E9D 2B2C429.xz 2DD3BC6 2E4E46C.xz 2EDABE5
25F9E97.xz 26A43E1 27490C6.xz 281FB01 28F0816.xz 2A005F2 2ACF983.xz 2B59D5F 2CA4E9D.xz 2D3DD50 2D03BC6.xz 2E5B746 2EDABE5.xz
260D22E 26A43E1.xz 275E32A 2831B 28F0816.xz 2903B1D 2A005F2.xz 2AD4AB4 2B59D5F.xz 2CA6C7 2B30050.xz 2DDC495 2E5B746.xz 2EE442F
260D22E.xz 26A43E1.xz 275E32A.xz 2831B 28F0816.xz 2903B1D.xz 2A0B740 2AD4AB4.xz 2B5E014 2AD4C67.xz 2D04982 2DC495.xz 2E5F7F3 2EE442F.xz
2615F80 26AE31B 27684B8 283414C.xz 29174C9 2A0B740.xz 2AE479F 2B5E014.xz 2C8C40D 2D49D82.xz 2D37C9 2E5F7F3.xz 2EF0285
2615F80.xz 26C2053 27684B8.xz 283B0CE 29174C9.xz 2A1FA14 2B5E014.xz 2C8C40D.xz 2D49D82.xz 2D37C9.xz 2E60622 2EF0285.xz
2627E03 26C2053.xz 2772D2 283B0CE.xz 292A9F0 2A1FA14.xz 2AF2C01 2B69914.xz 2B8C445 2D58601.xz 2DEC3AF 2E06022.xz 2EFC163
2627E03.xz 26CD884 2772D2.xz 2849C94 292A9F0.xz 2A326CE 2AF2C01.xz 2B77A43 2B8C445.xz 2D69F54 2D58601.xz 2E06022.xz 2EFC163.xz
2628E4B 26CD884.xz 278810A 28588A3 2939DE2 2A326CE.xz 2AF2C01.xz 2B77A43.xz 2CC6423 2D69F54.xz 2DDEFD8 2E7AFB4.xz 2F03E94
2628E4B.xz 26D0767 278810A.xz 28588A3.xz 2939DE2.xz 2A4346A 2AFDC77.xz 2B897865 2CC6423.xz 2D784BF 2DDEFD8.xz 2E866FA 2F03E94.xz
263C21F 26D0767.xz 278DFFEA 28588A3.xz 294DE72 2A4346A.xz 2B897865.xz 2CD82A6 2D784BF.xz 2D80758 2DFCB46.xz 2E8FC28 93
263C21F.xz 26ED3DA 278DFFEA.xz 286A9F5 294DE72.xz 2A588DA 2B0E0A2.xz 2B8B762D 2CD82A6.xz 2D80758 2DFCB46.xz 2E8FC28 93
264E478 26ED3DA.xz 27986B1 286A9F5.xz 2962CFA 2A588DA.xz 2B16953 2B8B762D.xz 2CE2504 2D80758.xz 2E098B4 2E8FC28.xz 93.zlib
264E478.xz 26F153F 27ADEBC 2787E02 28777E 2A6BAED 2B16953.xz 2B8B762D.xz 2CE2504.xz 2D80758.xz 2E098B4.xz 2E96091
2657A0 26F153F.xz 27ADEBC.xz 2787E02.xz 28777E 2A6BAED.xz 2B20155 2B8D73C3 2CEC94A 2D80758.xz 2E111DE 2E96091.xz
2657A0.xz 26FB651 27ADEBC 2892351 297877E 2A81051 2B20155.xz 2BF72F5 2CEC94A.xz 2D8A716 2E111DE.xz 2EA1523
2658D7C 26FB651.xz 27B7C3E 2892351.xz 298E575 2A81051.xz 2B25A16 2BF72F5.xz 2CF950C 2D8A716.xz 2E15846 2E1523.xz
2658D7C.xz 2710489 27B7C3E.xz 28A25AF 298E575.xz 2A9631C 2B25A16.xz 2C1638E 2CF950C.xz 2D9801C.xz 2E1FAB0 2EAD75
266289E 2710489.xz 27C2DD5 28A25AF.xz 29A13E9 2A9631C.xz 2B2EB3B 2D0666A 2D9801C.xz 2E1FAB0 2EAD75.xz
266289E.xz 271AE37 27C2DD5.xz 28B7DEC 29A13E9.xz 2AA808 2B2EB3B.xz 2C361BC 2D0666A.xz 2D9801C.xz 2E1FAB0 2EAD75
267603D 271AE37.xz 27D7D5C 28B7DEC.xz 29A917E 2AA808.xz 2B33655 2C361BC.xz 2D0700E 2D9801C.xz 2E1FAB0 2EAD75
267603D.xz 27D7D5C.xz 29A917E 2AA808.xz 2B33655 2C361BC.xz 2D0700E 2D9801C.xz 2E1FAB0 2EAD75.xz
```

Thứ extract file lạ nhất là 93 thì ta có file Eden_Drive.dd

```
(lixsong㉿kali)-[~/Downloads/_kb06-session02.pdf.extracted]
$ file 93
93: 7-zip archive data, version 0.3
```

```
(lixsong㉿kali)-[~/Downloads/_kb06-session02.pdf.extracted]
$ 7z e 93
7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=C.UTF-8 Threads:128 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 77422710 bytes (74 MiB)

Extracting archive: 93
-- 
Path = 93
Type = 7z
Physical Size = 77422710
Headers Size = 122
Method = LZMA2:26
Solid = -
Blocks = 1
```

```
2F106A2.xz
93
93.zlib
Eden_Drive.dd
```

Đã có image rồi sẽ chuyển sang window và dùng autopsy phân tích.

The screenshot shows the Autopsy Forensic Browser interface. At the top, it displays a table of file metadata with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), and Known. The table lists various system files like \$Bitmap, \$Boot, \$LogFile, etc., and a file named secret.docx. A specific row for secret.docx is selected, showing its full path as /img_Eden_Drive.dd/vol_0/vol4/secret.docx and its contents as secret.secret.txt. Below the table, there's a search bar with the query "I think someone may be after me. - Eden". The search results pane shows the text "I think someone may be after me. - Eden" and a section titled "-----METADATA-----".

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
\$Bitmap				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	3200	Allocated	Allocated	unkno
\$Boot				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	8192	Allocated	Allocated	unkno
\$LogFile				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2097152	Allocated	Allocated	unkno
\$MFT				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	262144	Allocated	Allocated	unkno
\$MFTMirr				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	4096	Allocated	Allocated	unkno
\$Secure:\$SDS				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	263392	Allocated	Allocated	unkno
\$UpCase				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	131072	Allocated	Allocated	unkno
\$UpCase:\$Info				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	32	Allocated	Allocated	unkno
\$Volume				2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT	0	Allocated	Allocated	unkno
368896				2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	36864	Unallocated	Unallocated	unkno
376538				2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	36864	Unallocated	Unallocated	unkno
447761				2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	36864	Unallocated	Unallocated	unkno
545316				2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	36864	Unallocated	Unallocated	unkno
844930				2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	35807	Unallocated	Unallocated	unkno
secret.docx				2014-12-04 13:40:32 ICT	2014-12-04 13:40:32 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	11433	Allocated	Allocated	unkno
secret.docx:secret.txt				2014-12-04 13:40:32 ICT	2014-12-04 13:40:32 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	41	Allocated	Allocated	unkno

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page < > Matches on page: - of - Match < > 100% ⌂ ⌃ Reset Text Source: File Text

I think someone may be after me. - Eden

-----METADATA-----

Ta phân tích và tìm thấy có 1 file secret.docx.secret.txt với nội dung là

I think someone may be after me. - Eden

Kết luận: Có thể có ai đã theo dõi Eden và đã ám sát anh ấy.