Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

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 Tấn 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 02	100%
3	Kịch bản 04	100%
4	Kịch bản 05	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.

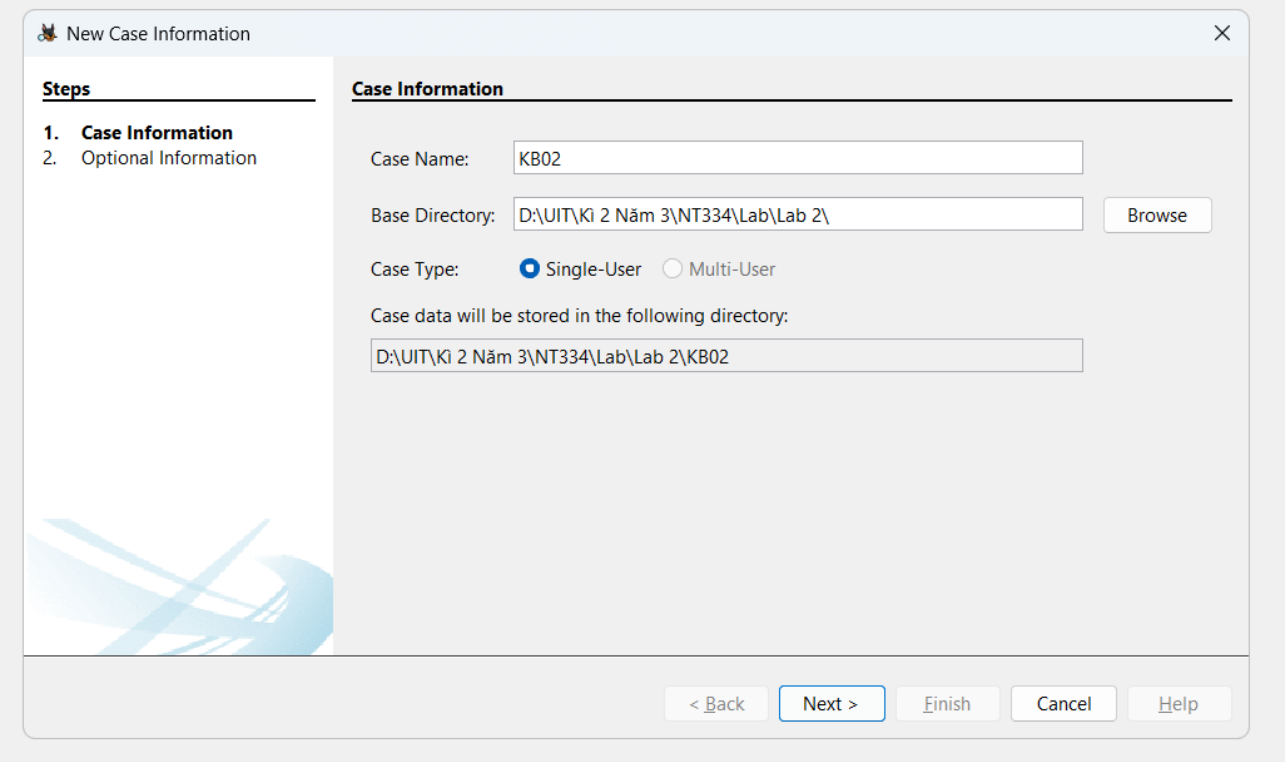
Các file .dd thường được sử dụng trong các hoạt động như phục hồi dữ liệu từ ổ đĩa hỏng, sao lưu toàn bộ hệ thống hoặc phân tích số học. Các chuyên gia có thể sử dụng các hình ảnh đĩa để khám phá dữ liệu và điều tra vụ việc mà không làm thay đổi nội dung gốc của ổ đĩa.

=> 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.

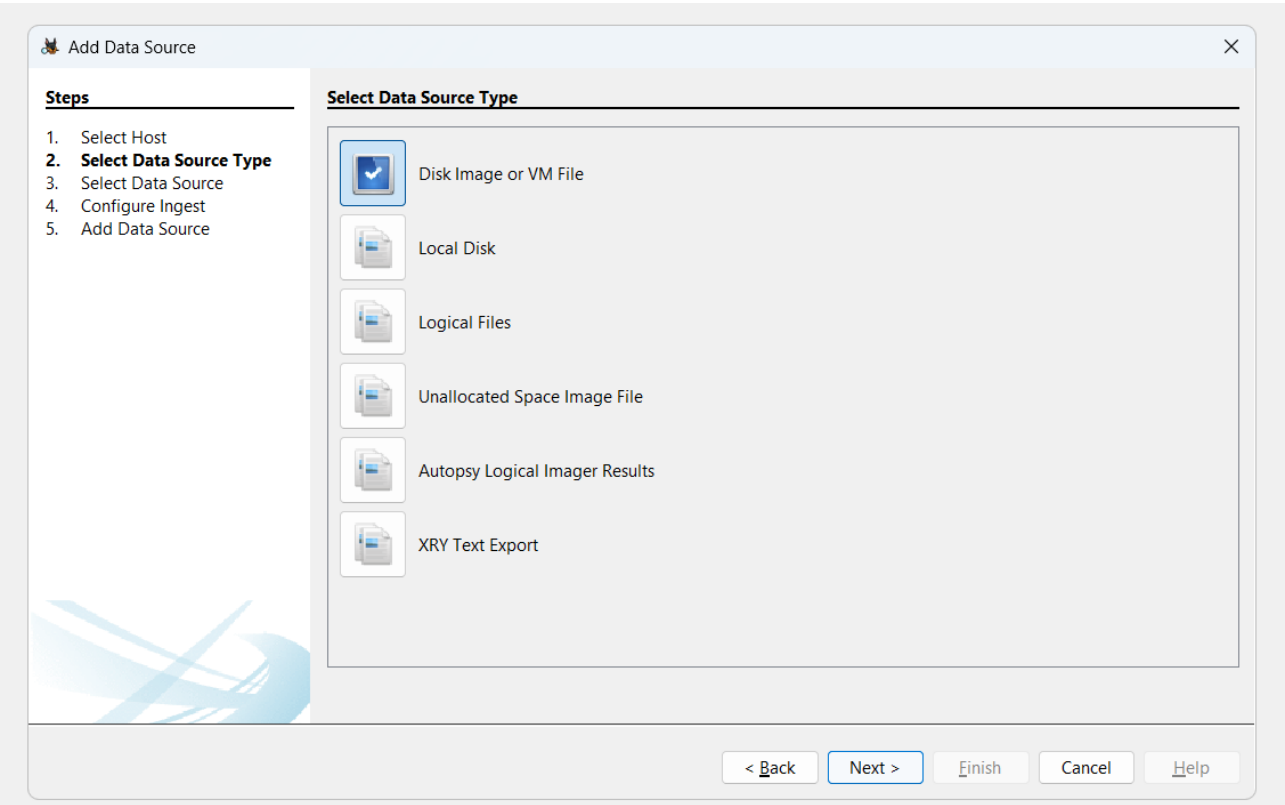
1. **Kịch bản 01**
2. **Kịch bản 02**

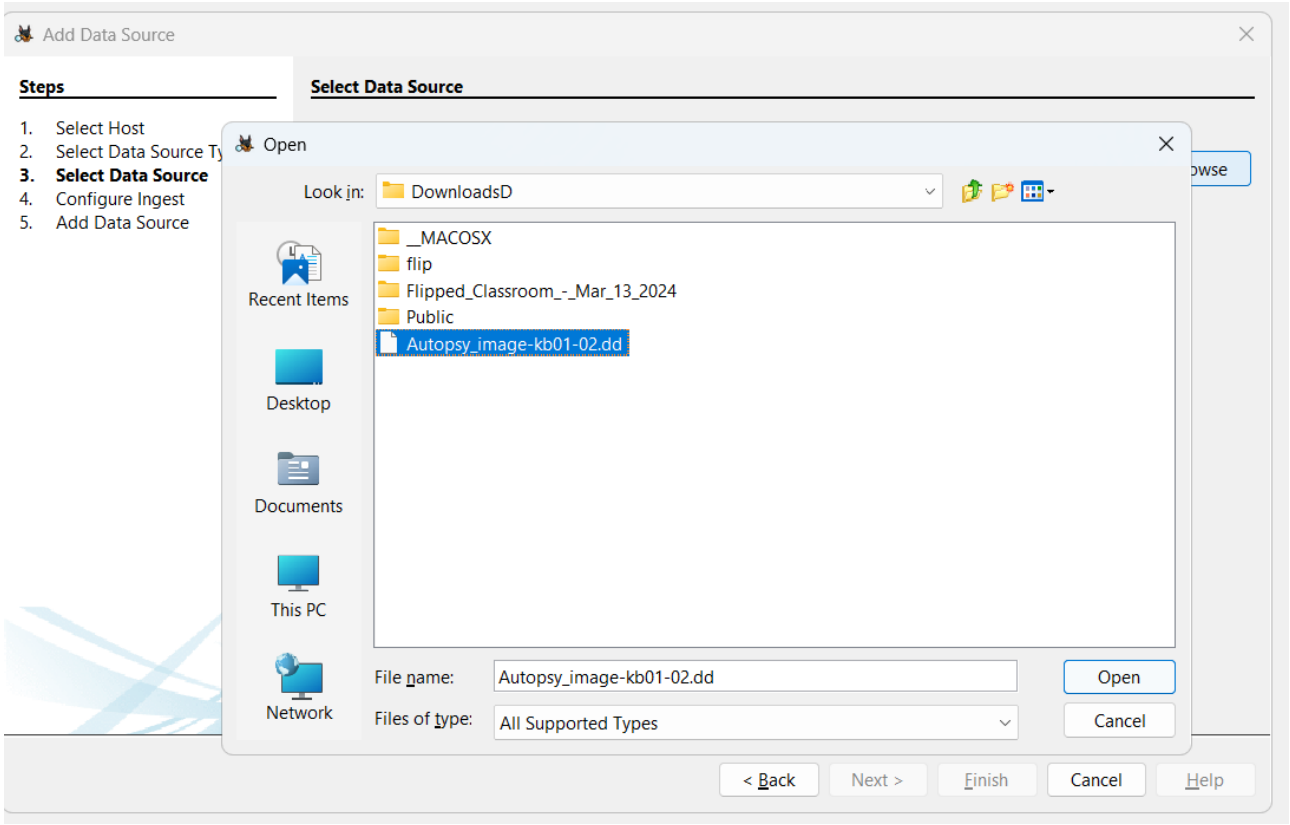
> **Kịch bản 02. Thực hiện phân tích dựa trên tài nguyên được cung cấp.**
>
> Tài nguyên: tải về theo link sau: https://goo.gl/MRLtj4

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

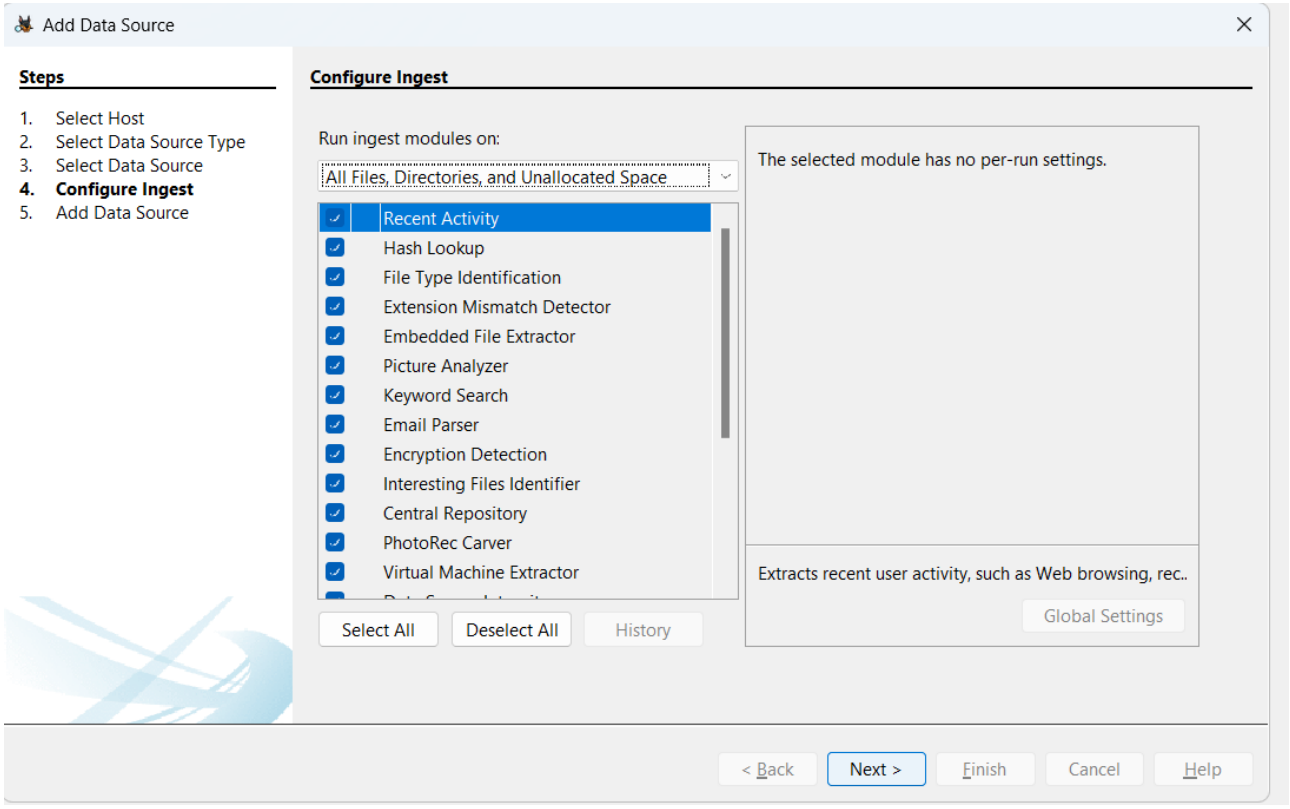


- Tại Add data source, chọn Disk Image or VM File và chọn path tới file tài nguyên cho sẵn





- Chọn các module cần phân tích

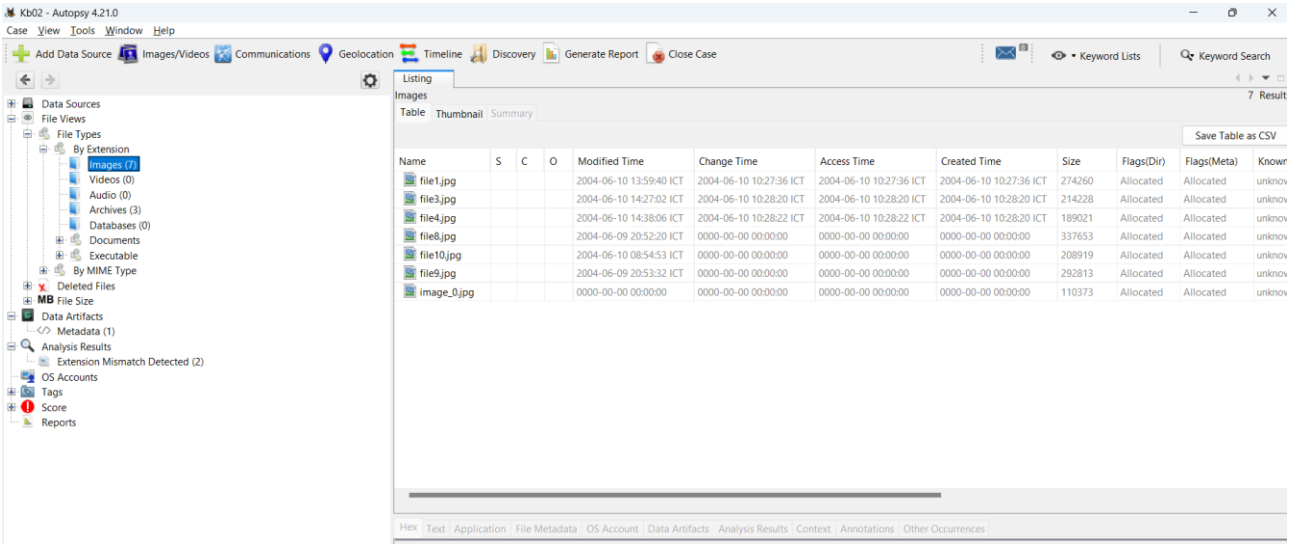


- Vào File Views, nơi hiển thị các thông tin chi tiết thông tin của các file chứa trong Filesystem.

+ Hãy tìm tất cả những hình ảnh có trọng ổ đĩa đã cho.

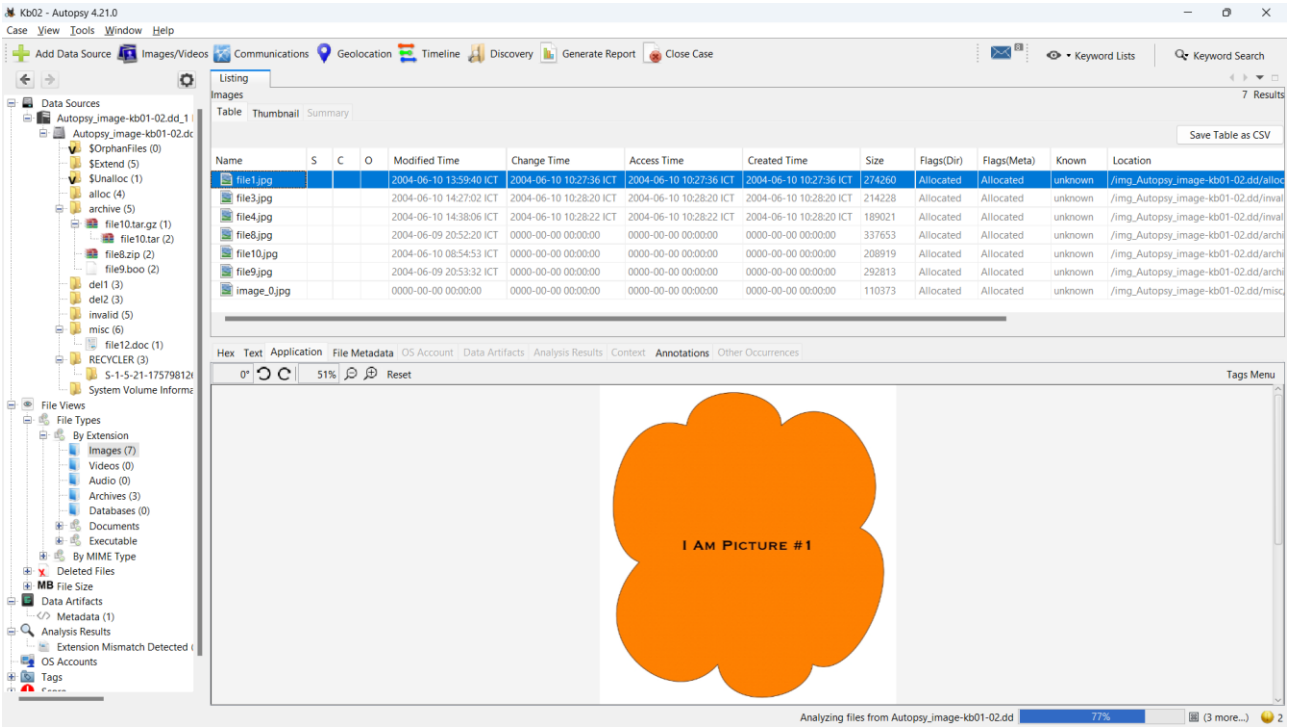
File Views -> File Types -> By Extension -> Images

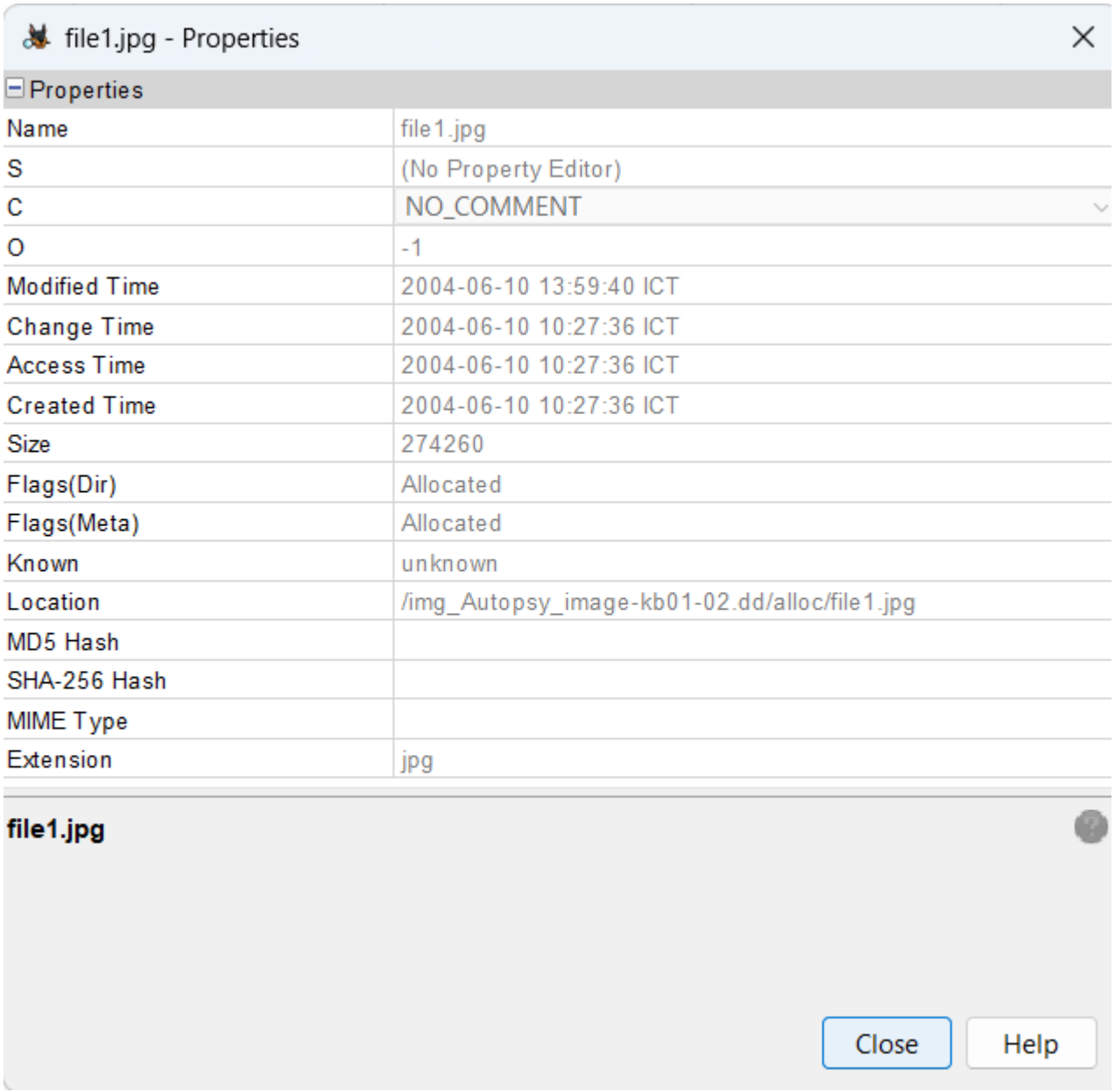
Ngoài ra còn tìm được các file ảnh khác trong thư mục deleted file, trong file1.jpg có file2.dat, trong executable → .dll cũng có.



+ 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 …

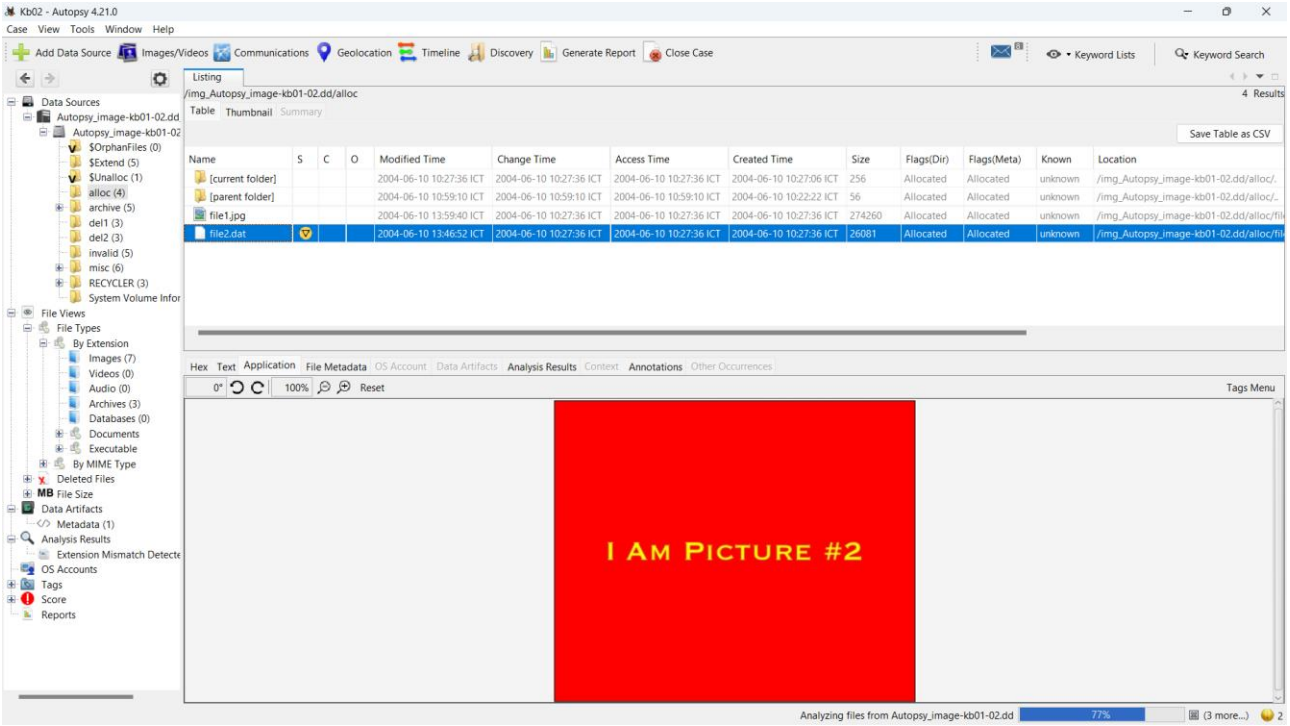
Thông tin file ảnh file1.jpg

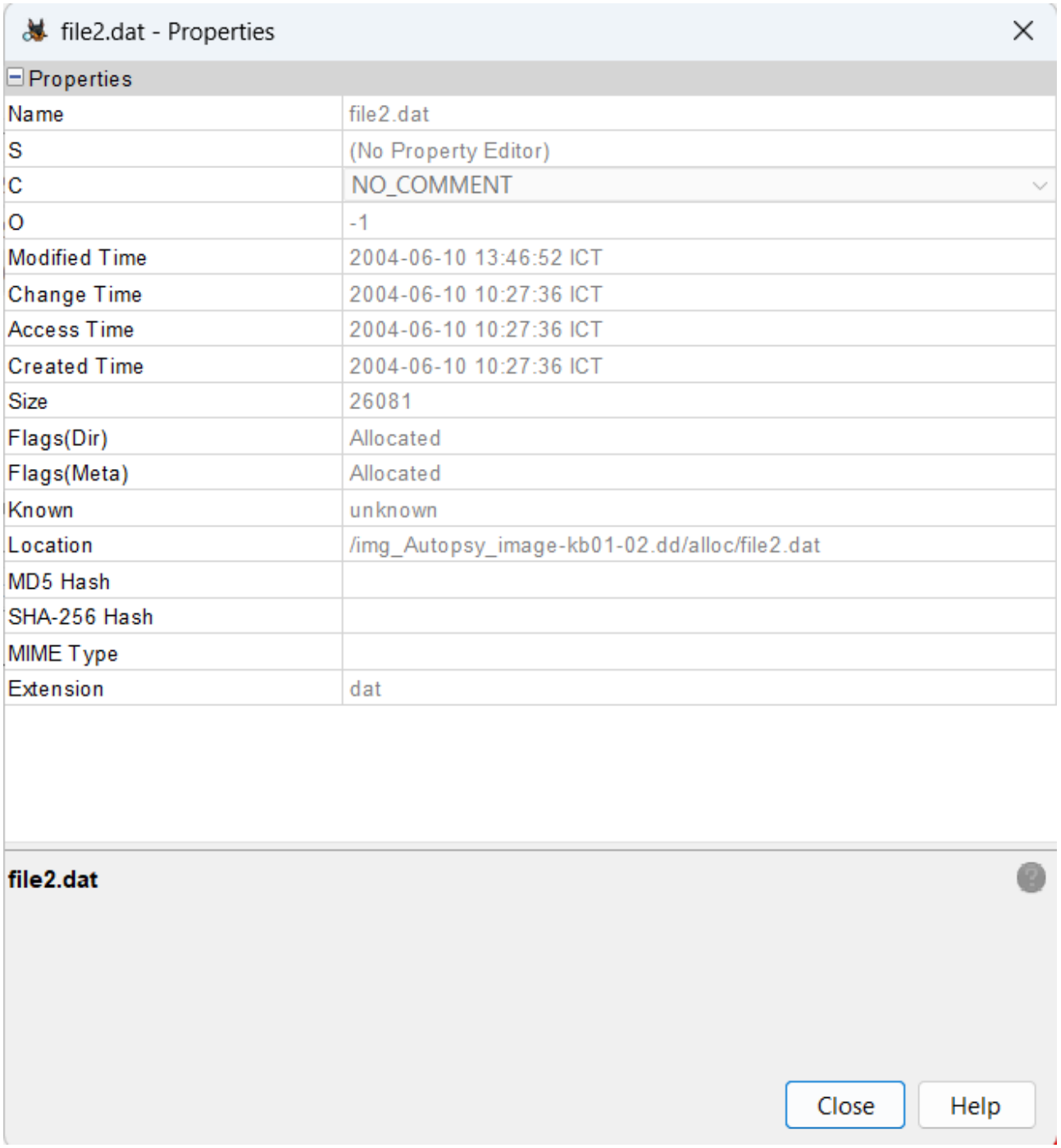




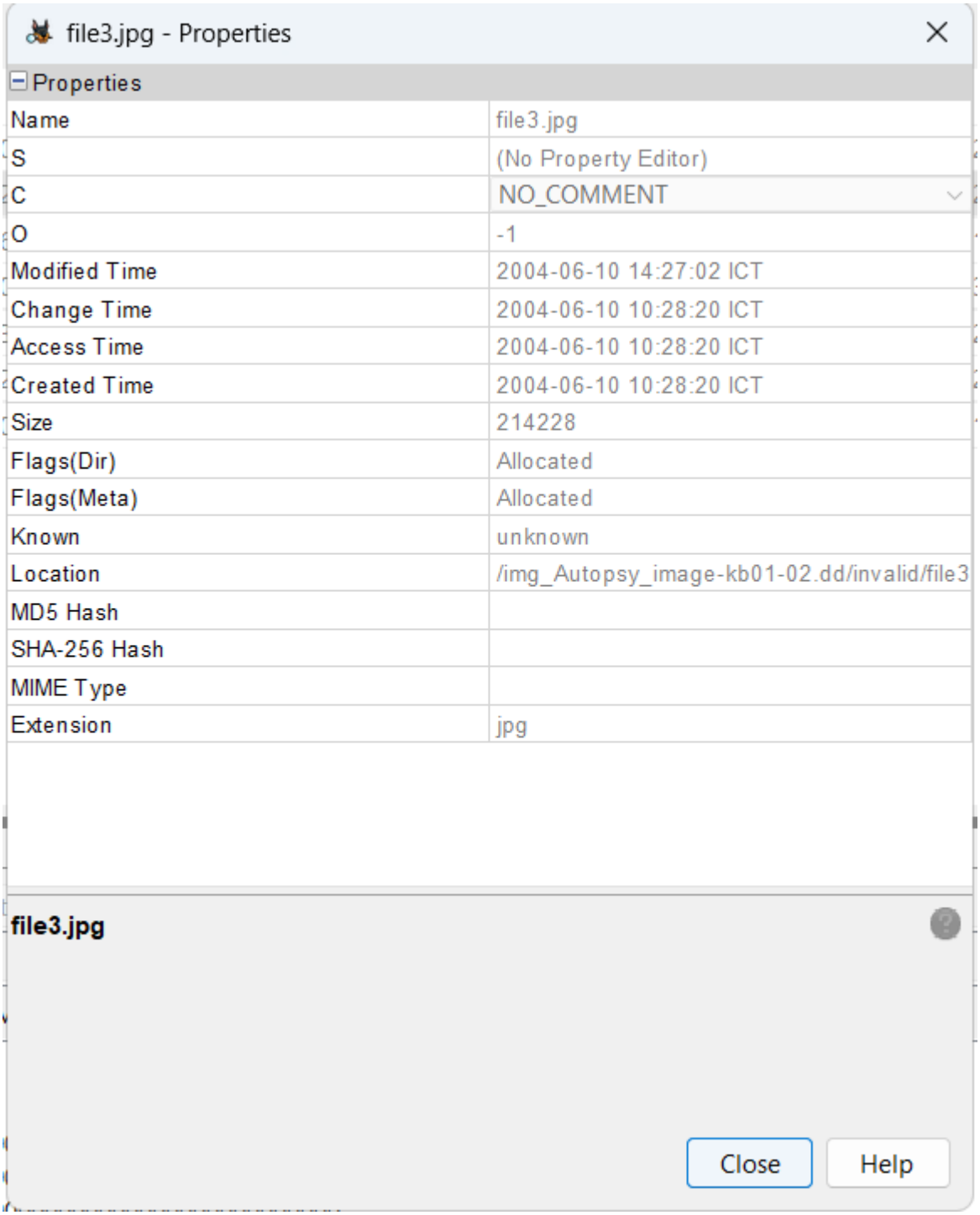
Trong file1.jpg ta view File in dictionary sẽ thấy file2.dat

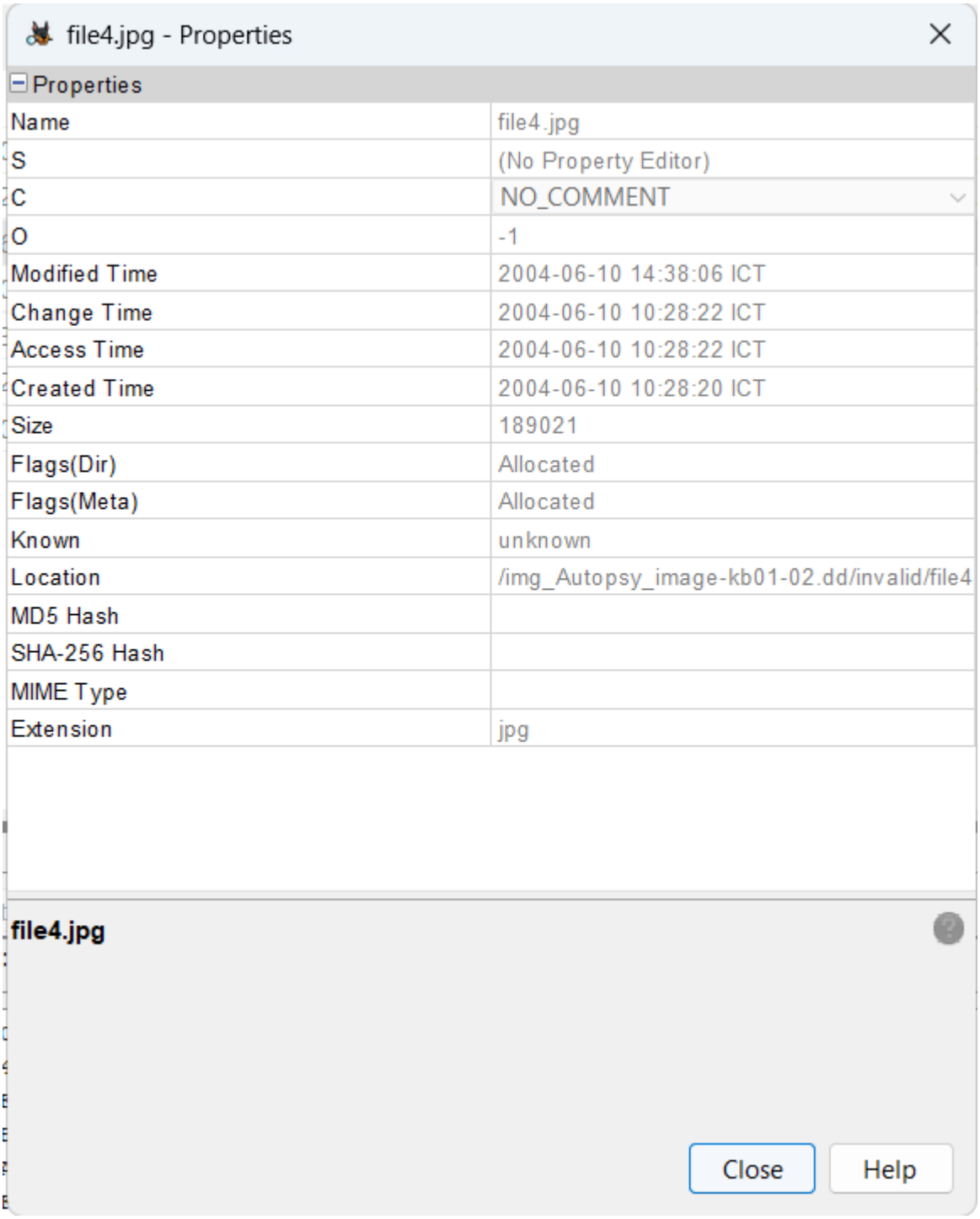
Thông tin file2.dat


Kb02 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_Autopsy_image-kb01-02.dd/alloc
4 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Location
[current folder] 2004-06-10 10:27:36 ICT 2004-06-10 10:27:36 ICT 2004-06-10 10:27:36 ICT 2004-06-10 10:27:06 ICT 256 Allocated Allocated unknown /img_Autopsy_image-kb01-02.dd/alloc/.
[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/alloc/..
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/file1.jpg
file2.dat 2004-06-10 13:46:52 ICT 2004-06-10 10:27:36 ICT 2004-06-10 10:27:36 ICT 2004-06-10 10:27:36 ICT 26081 Allocated Allocated unknown /img_Autopsy_image-kb01-02.dd/alloc/file2.dat
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Reset
Tags Menu
I AM PICTURE #2
Analyzing files from Autopsy_image-kb01-02.dd
77%
(3 more...)

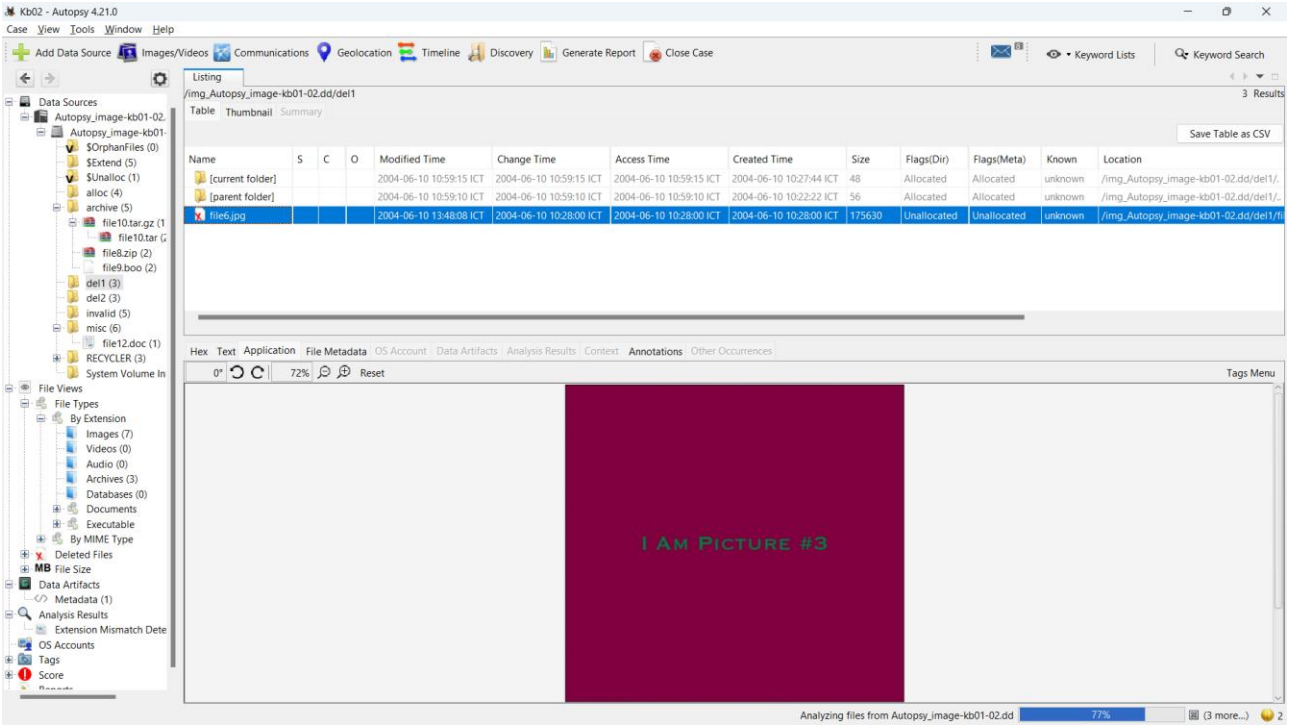


Thông tin file ảnh file3.jpg

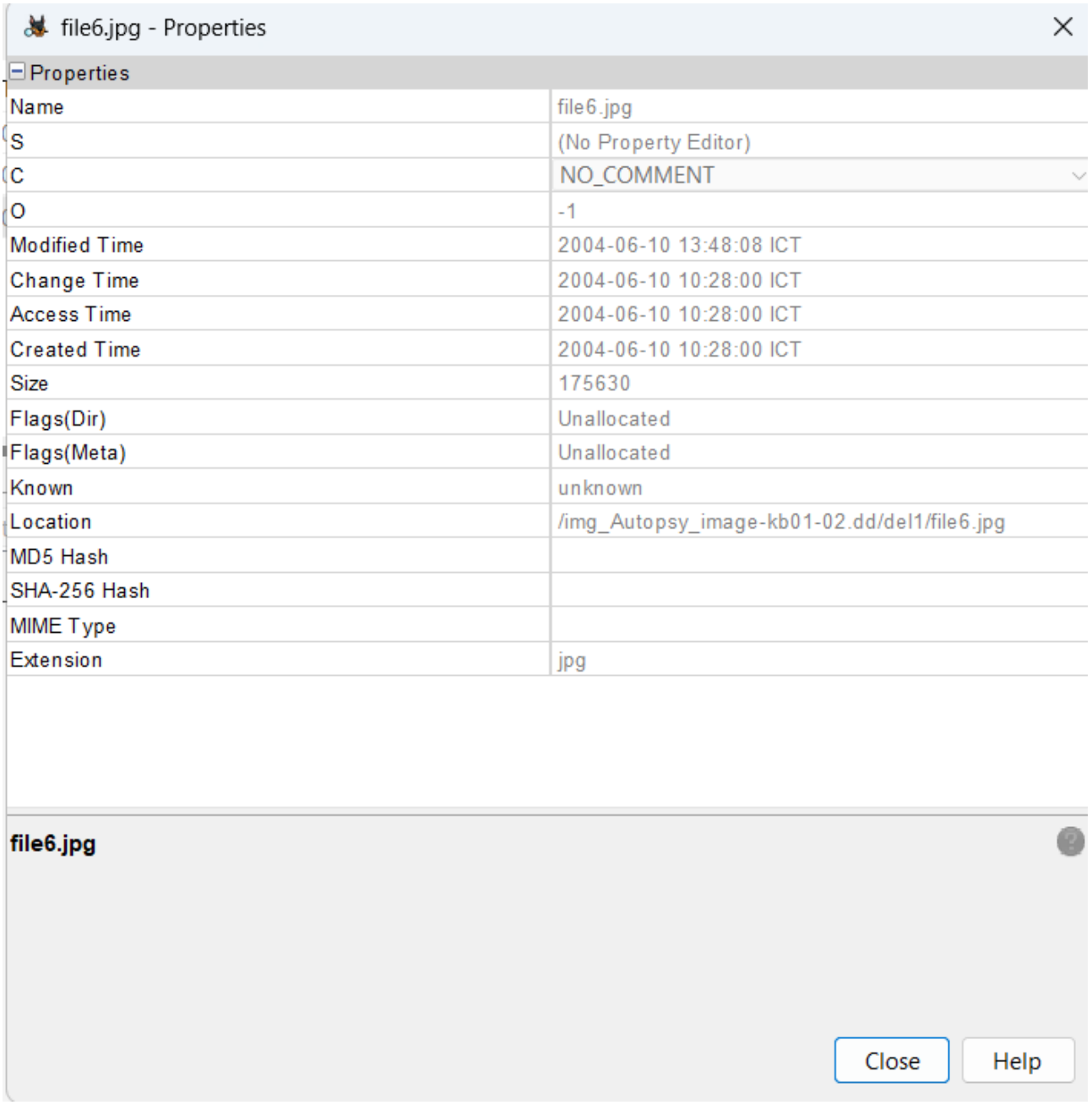

file3.jpg - Properties
Properties
Name file3.jpg
S (No Property Editor)
C NO_COMMENT
O -1
Modified Time 2004-06-10 14:27:02 ICT
Change Time 2004-06-10 10:28:20 ICT
Access Time 2004-06-10 10:28:20 ICT
Created Time 2004-06-10 10:28:20 ICT
Size 214228
Flags(Dir) Allocated
Flags(Meta) Allocated
Known unknown
Location /img_Autopsy_image-kb01-02.dd/invalid/file3
MD5 Hash
SHA-256 Hash
MIME Type
Extension jpg
file3.jpg
Close
Help



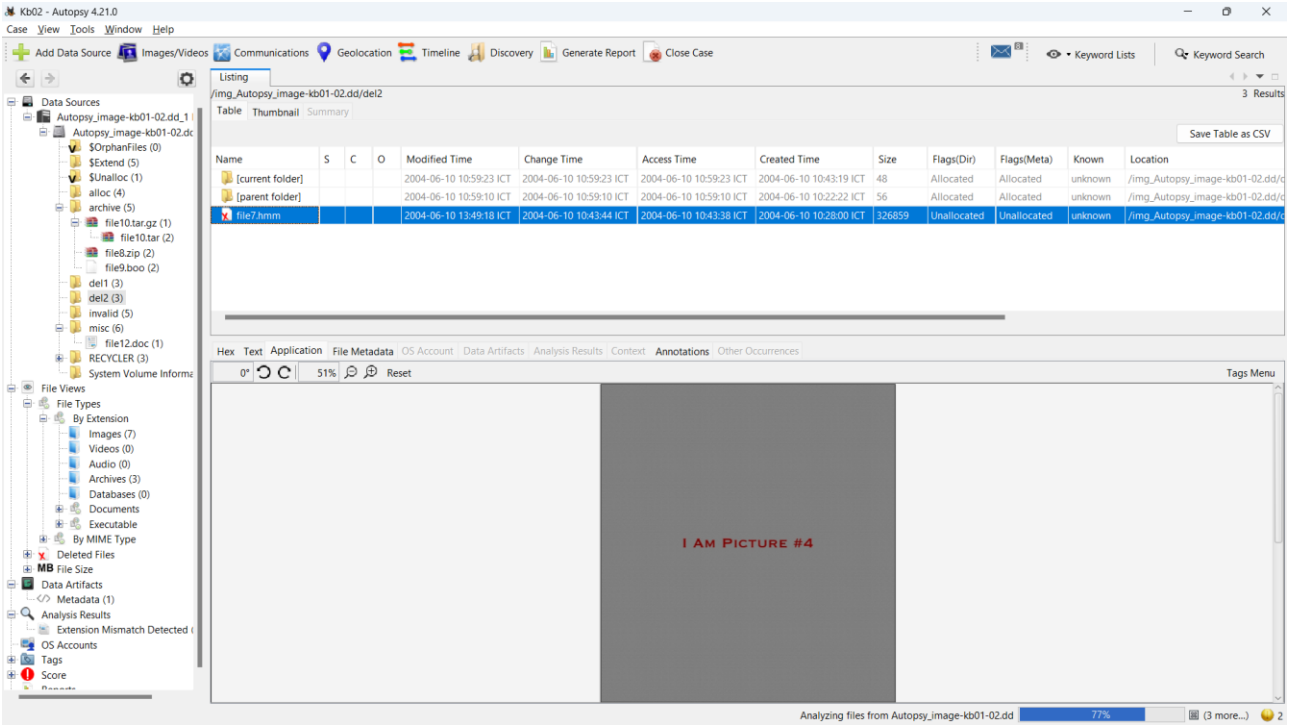
Tìm trong del1 ta thấy file6.jpg



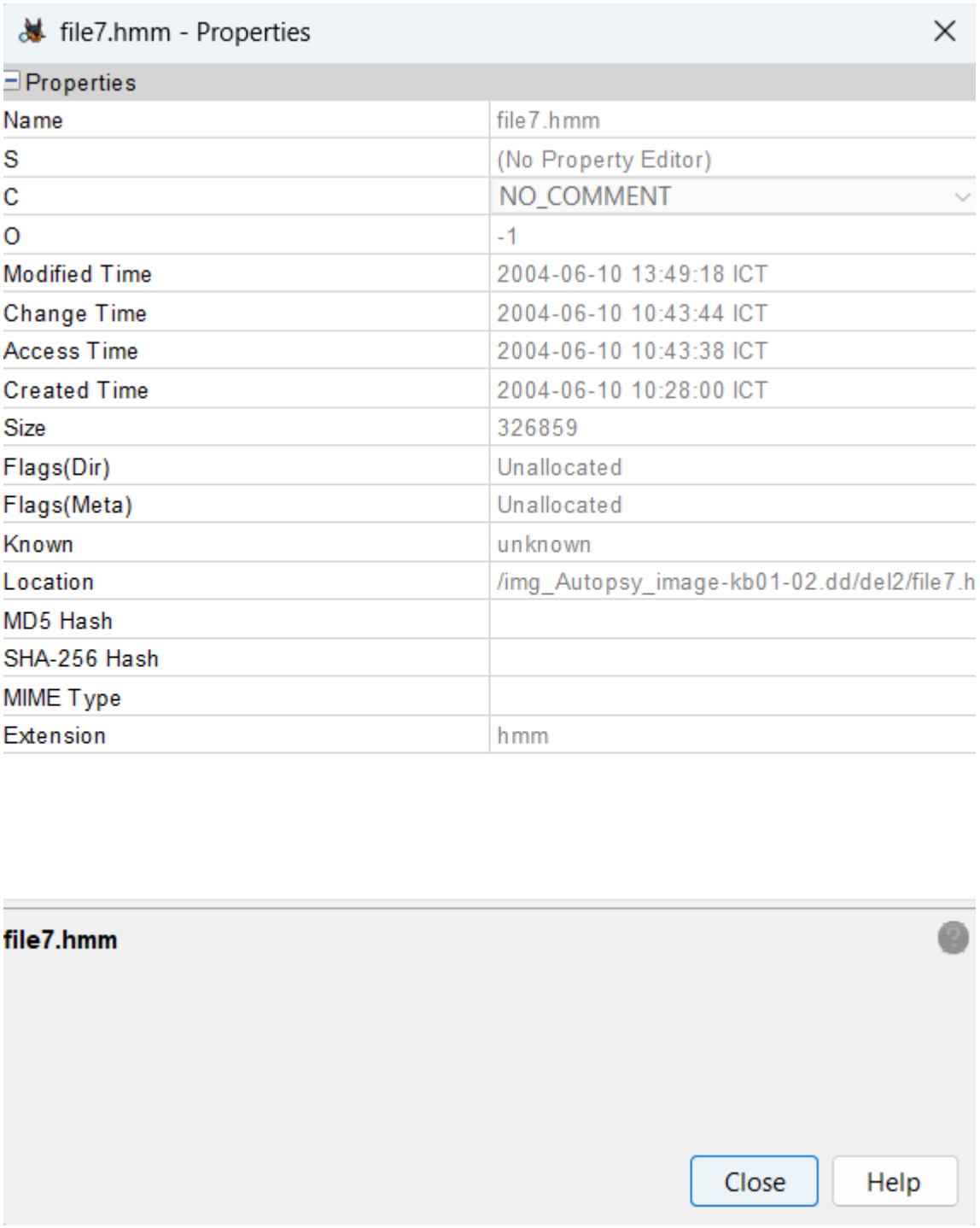
Thông tin file6.jpg



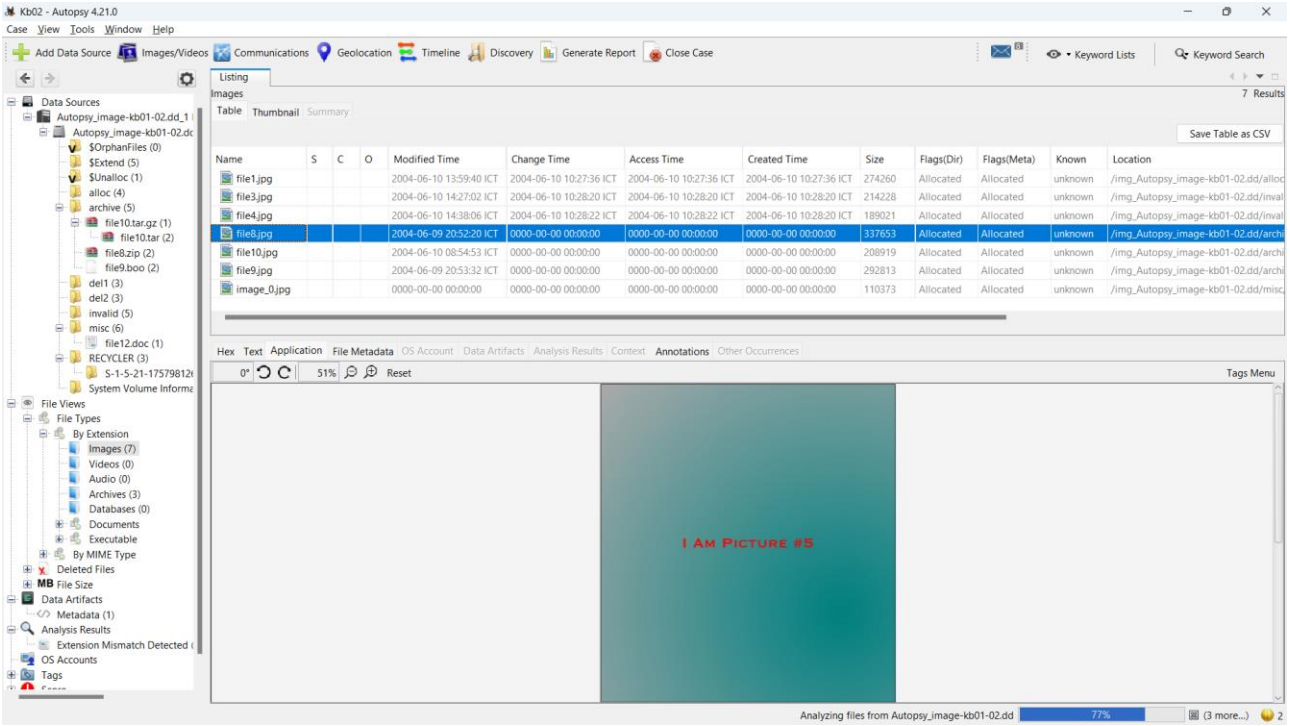
Tìm trong del2 thấy file7.hmm

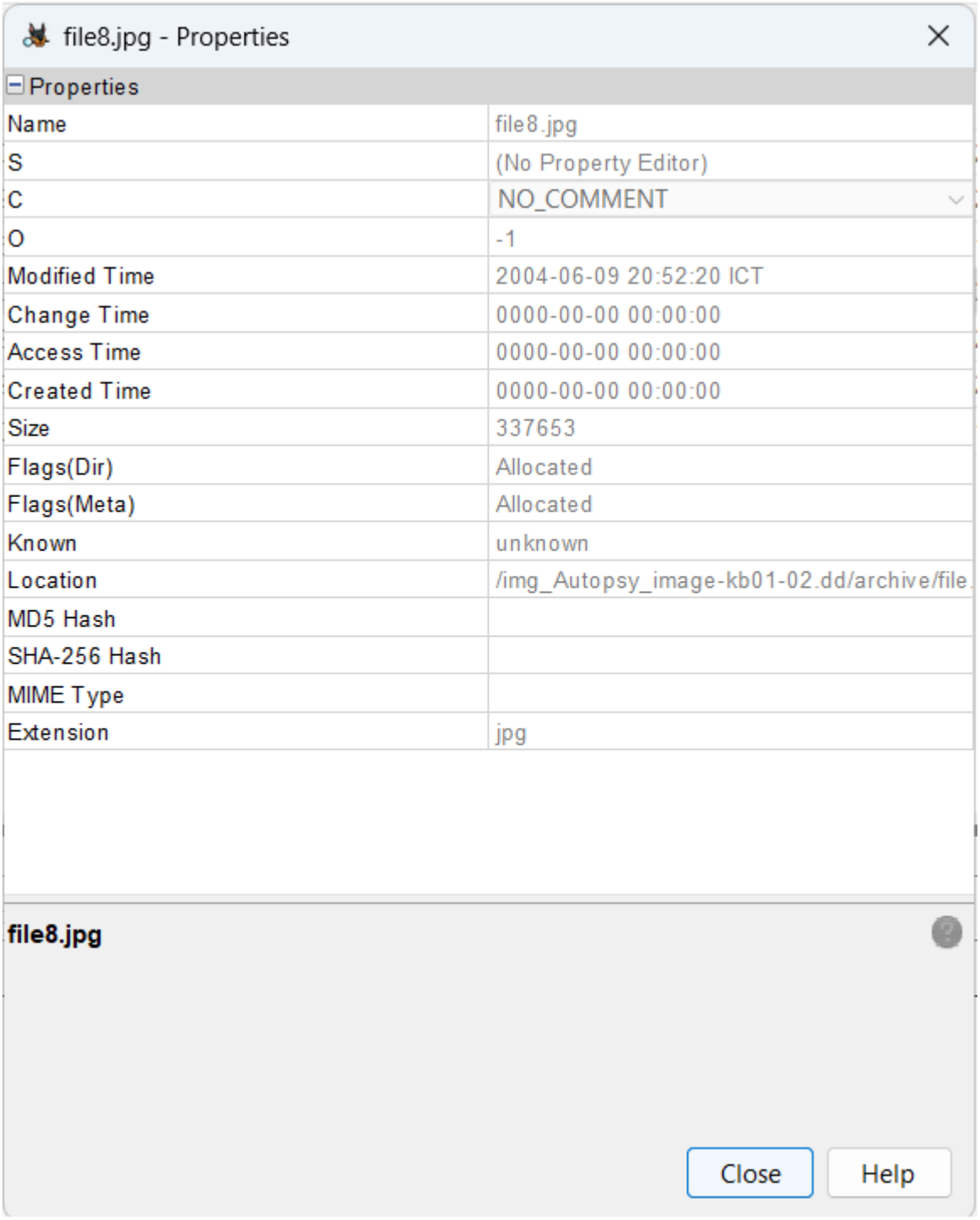


Thông tin file file7.hmm

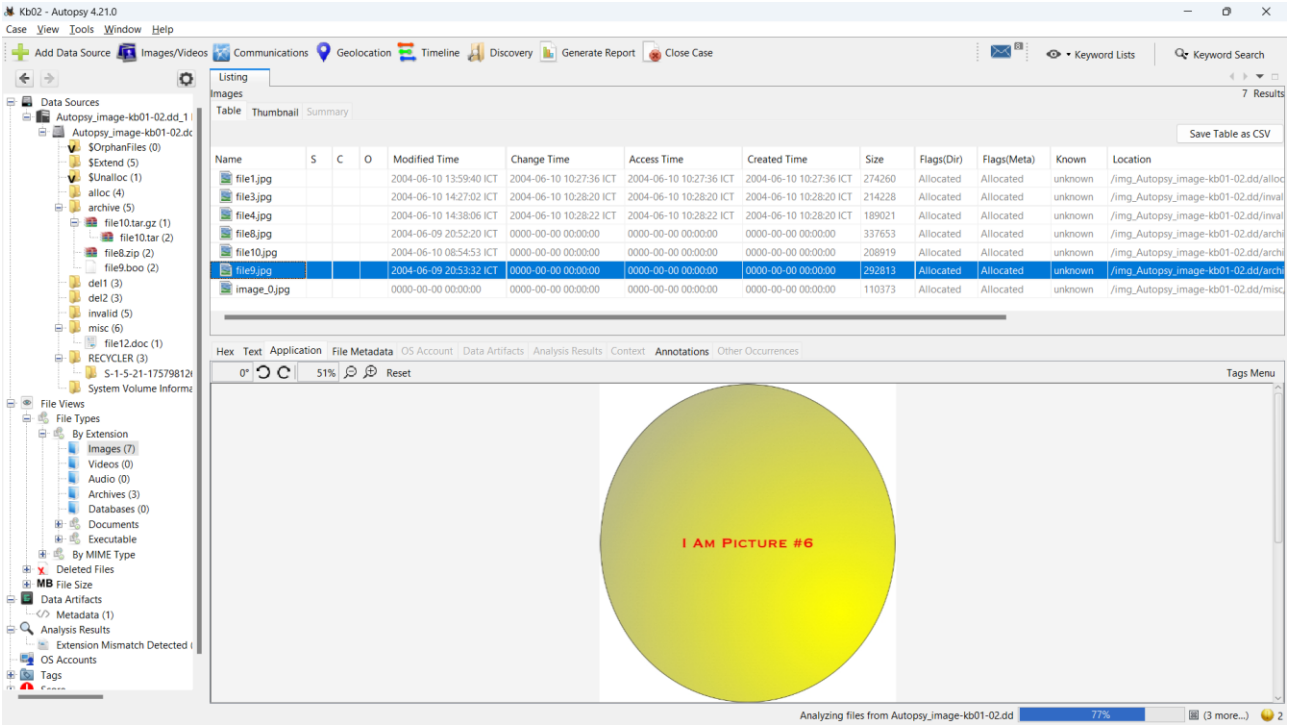


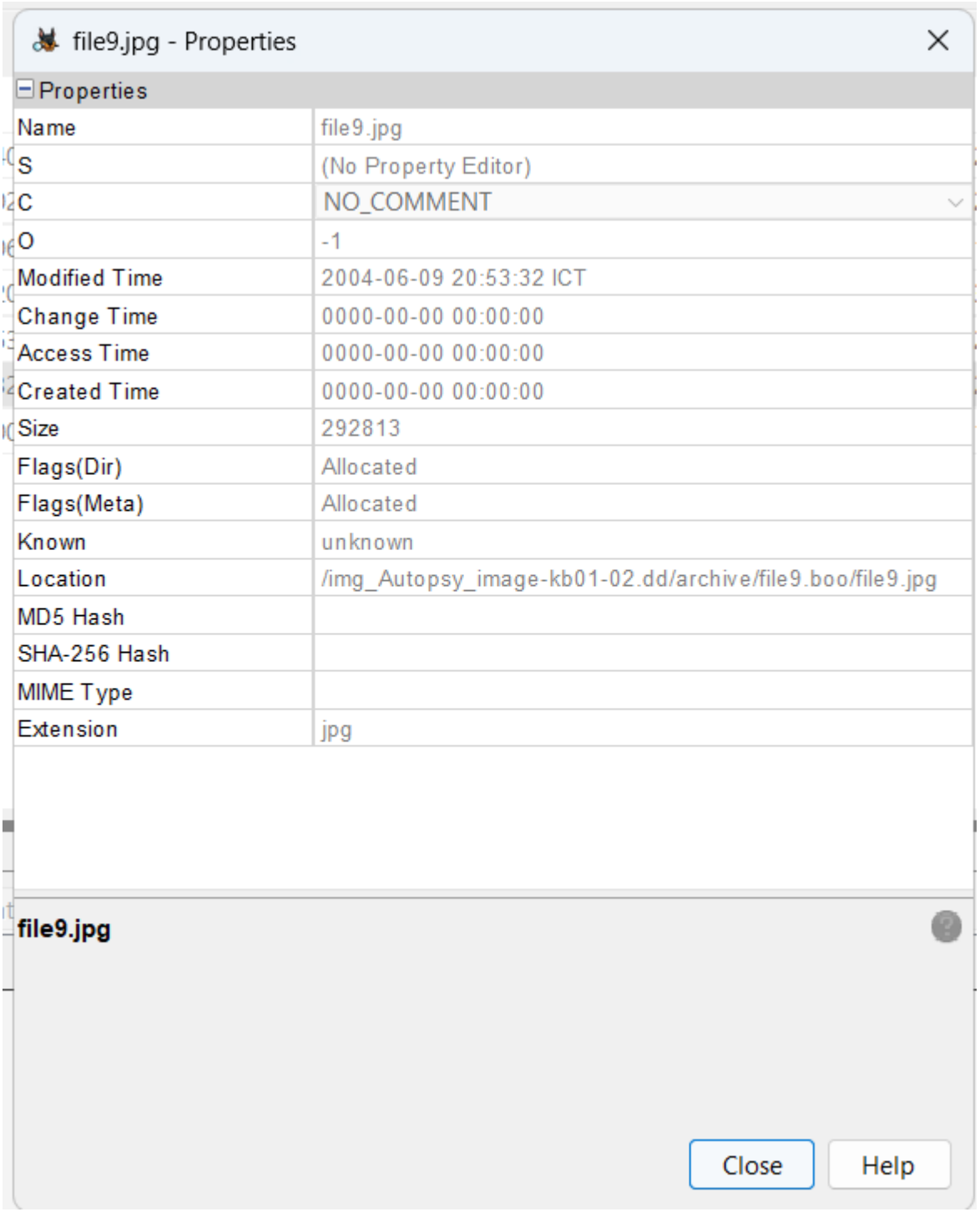
Thông tin file8.jpg


Kb02 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Images
7 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
file1.jpg
file3.jpg
file4.jpg
file8.jpg
file10.jpg
file9.jpg
image_0.jpg
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Reset
Tags Menu
I Am Picture #5
Analyzing files from Autopsy_image-kb01-02.dd
77%
(3 more...)

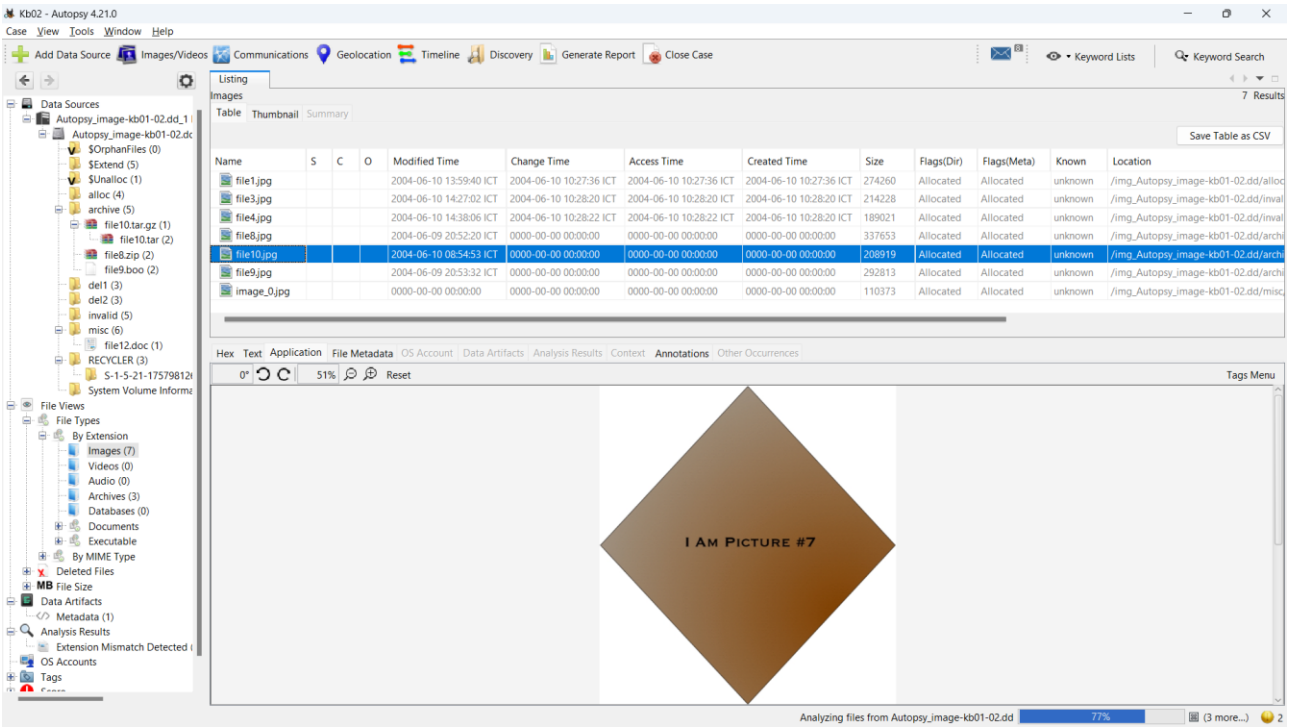


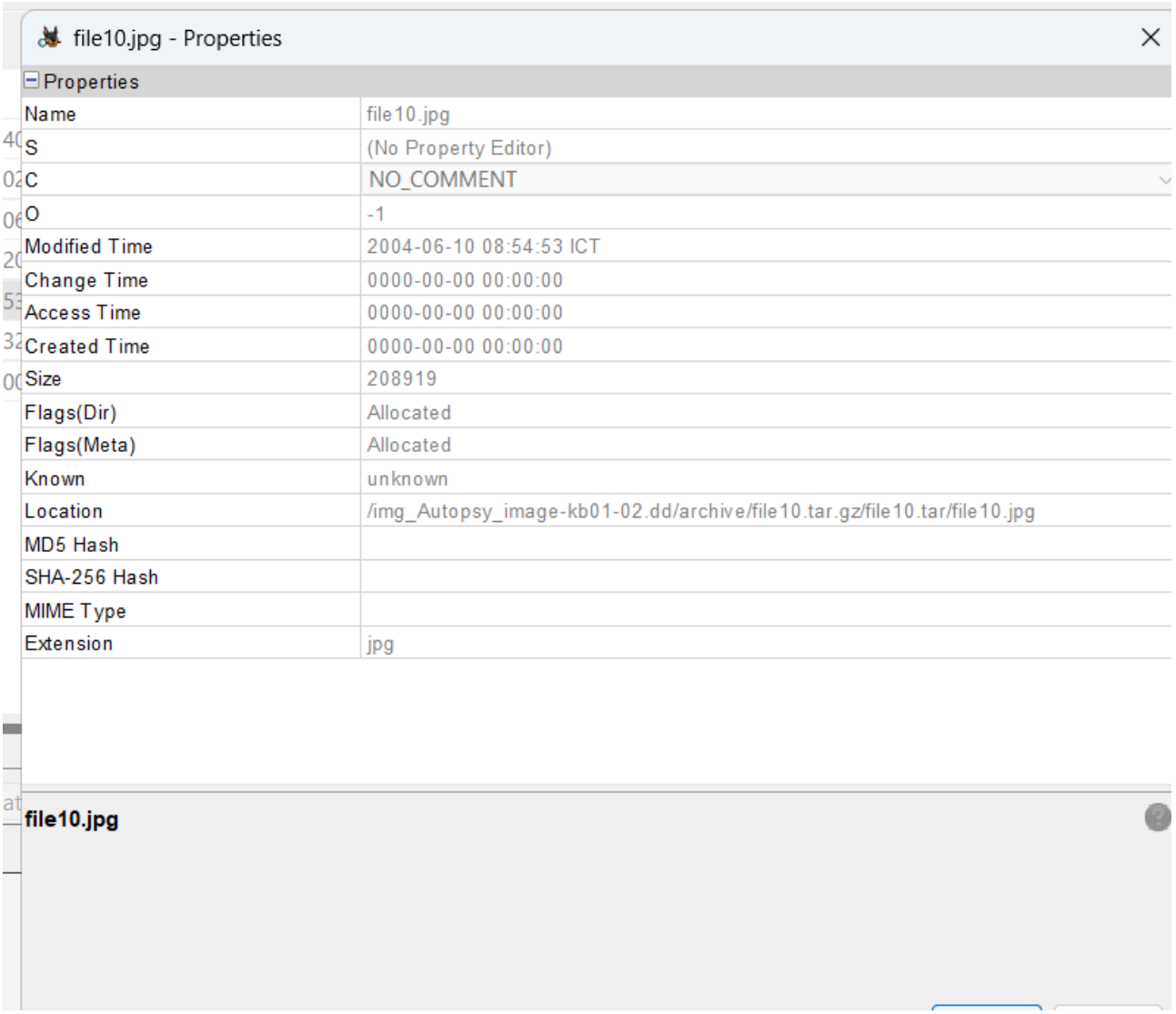
Thông tin file9.jpg


Kb02 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Images
7 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
file1.jpg
file3.jpg
file4.jpg
file8.jpg
file10.jpg
file9.jpg
image_0.jpg
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Reset
Tags Menu
I Am Picture #6
Analyzing files from Autopsy_image-kb01-02.dd
77%
(3 more...)

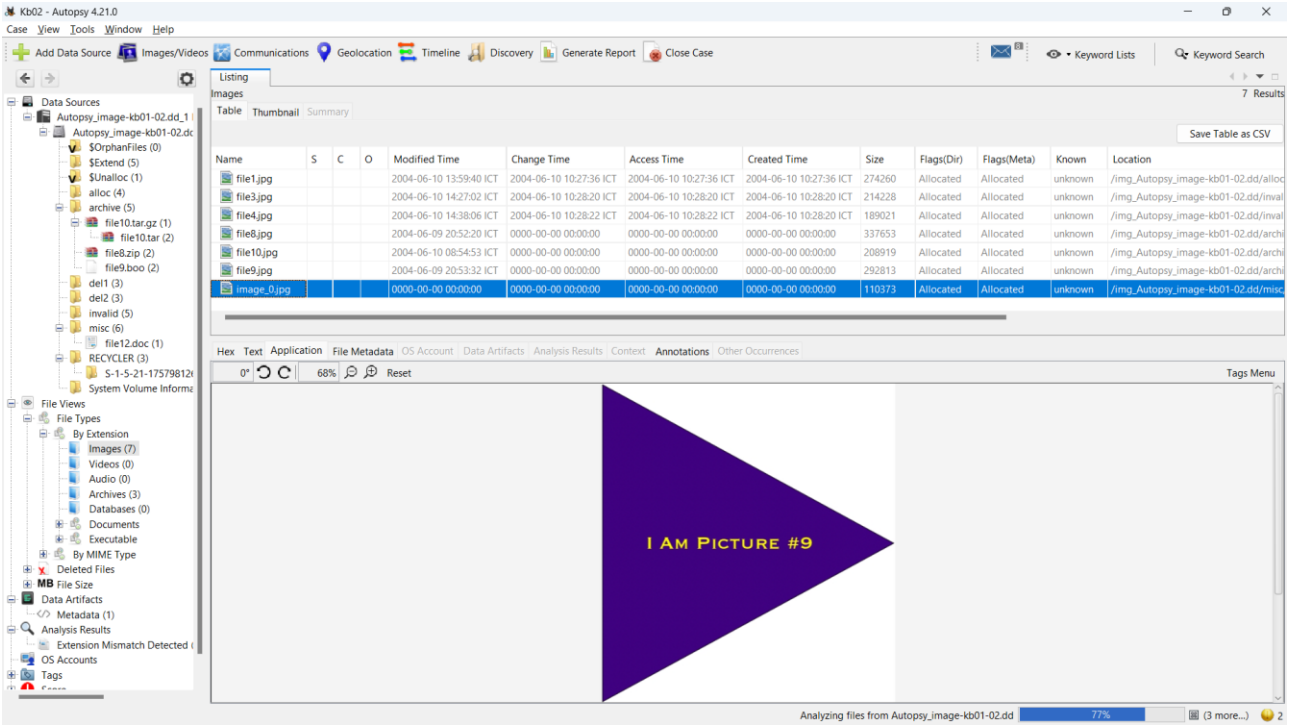


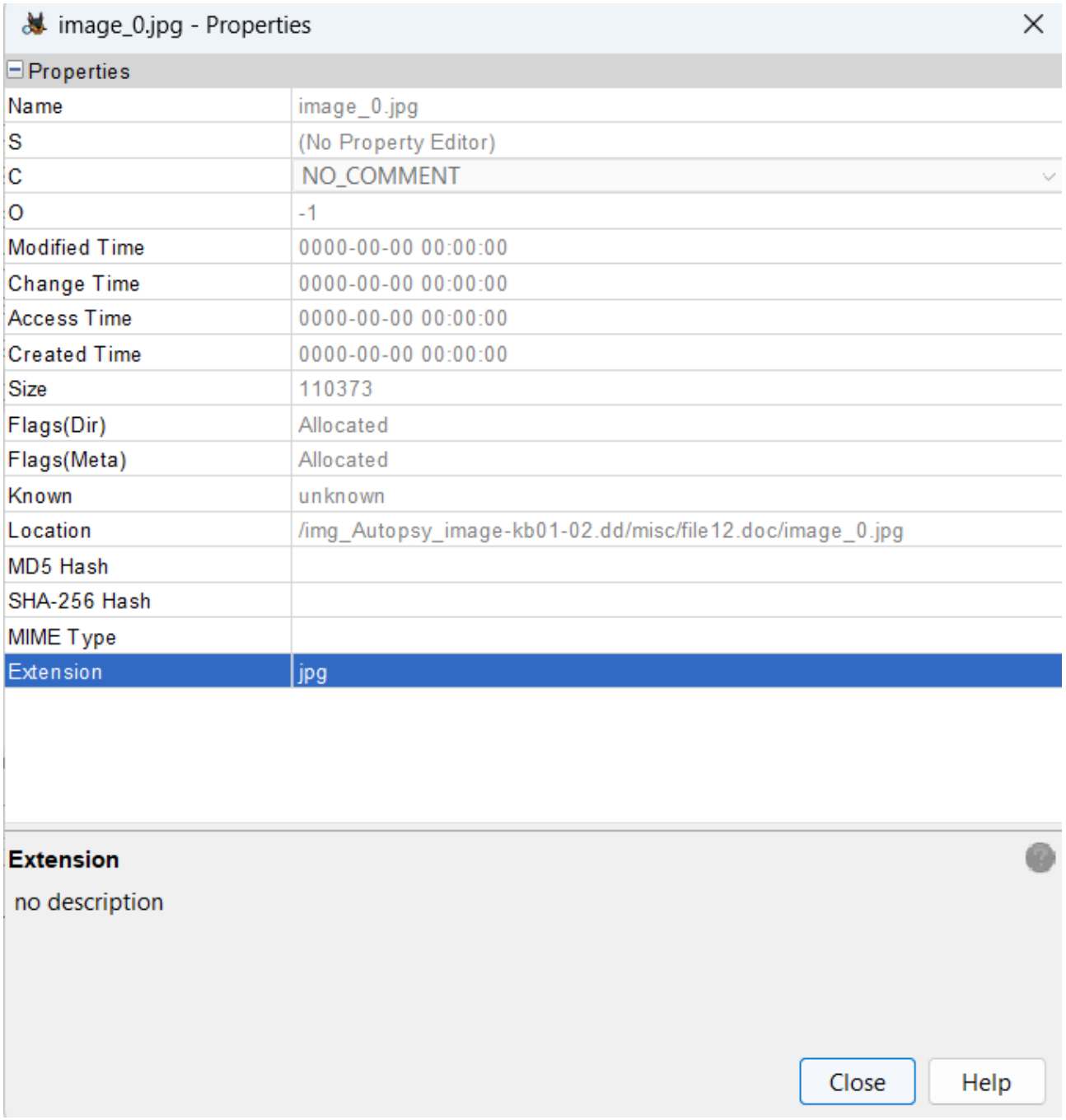
Thông tin file10.jpg


Kb02 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Images
7 Results
Table Thumbnail Summary
Save Table as CSV
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/inval
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/inval
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
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Reset
Tags Menu
I Am Picture #7
Analyzing files from Autopsy_image-kb01-02.dd
77%
(3 more...)
Data Sources
File Views
File Types
By Extension
Images (7)
Videos (0)
Audio (0)
Archives (3)
Databases (0)
Documents
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Metadata (1)
Analysis Results
OS Accounts
Tags

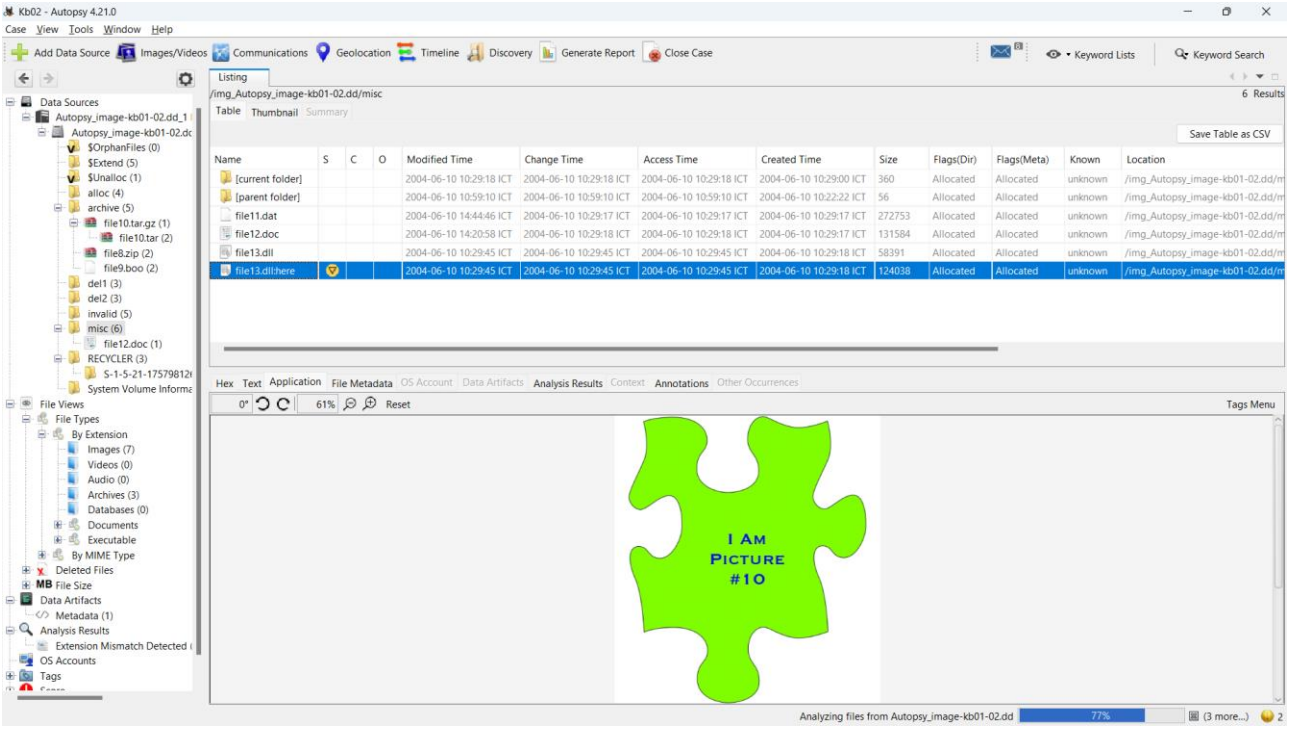


Thông tin file ảnh image0.jpg


Kb02 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Images
7 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
file1.jpg
file3.jpg
file4.jpg
file8.jpg
file10.jpg
file9.jpg
image_0.jpg
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Reset
Tags Menu
I AM PICTURE #9
Analyzing files from Autopsy_image-kb01-02.dd
77%
(3 more...)



Tìm được picture 10 trong thư mục misc



Link drive file hình ảnh:
https://drive.google.com/drive/folders/1NSz8va4VEgd92ns95DQf4ZjHwYB1pHwx

Kịch bản 4

Kịch bản 04. Thực hiện phân tích:

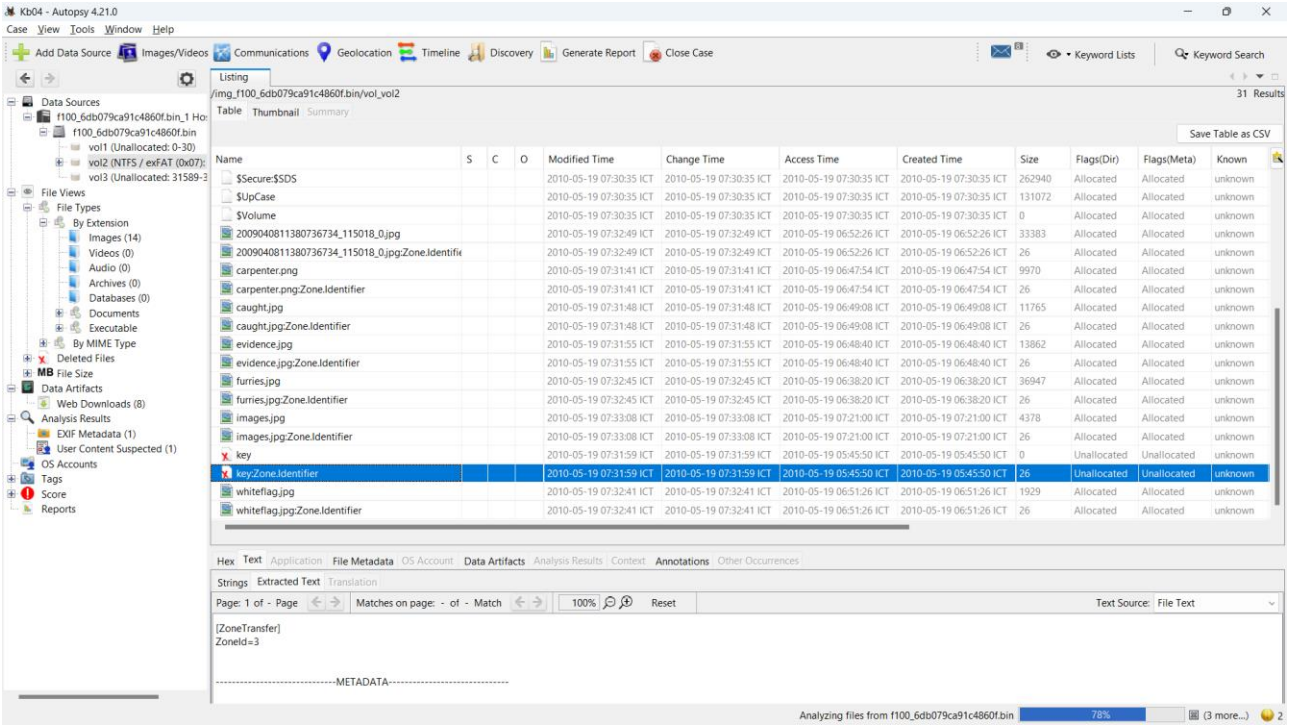
- Tài nguyên: kb04-session02.bin.gz
- Tìm thông tin có liên quan đến từ khóa "key" trong dữ liệu được cung cấp.

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

Đáp án:

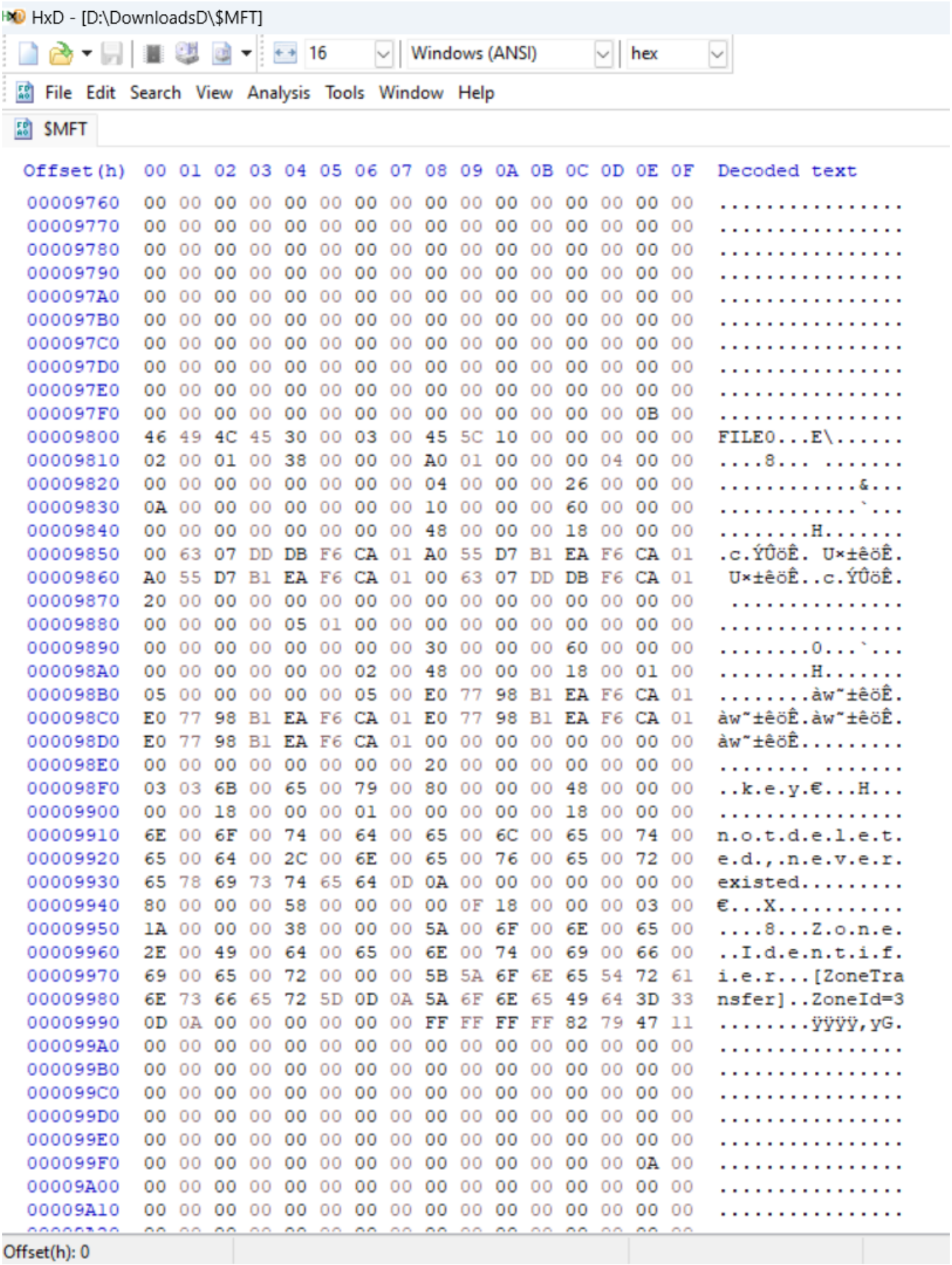
- Tiến hành phân tích sử dụng Autopsy

Tìm key và thấy key đã bị xóa



- 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 Lauch 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”


HxD - [D:\DownloadsD\$MFT]
16
Windows (ANSI)
hex
File Edit Search View Analysis Tools Window Help
$MFT
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 ....
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 00 ....8... ....
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 00 48 00 00 00 18 00 00 00 ....H.......
00009850 00 63 07 DD DB F6 CA 01 A0 55 D7 B1 EA F6 CA 01 .c.ÝÛöÊ. U×±êöÊ.
00009860 A0 55 D7 B1 EA F6 CA 01 00 63 07 DD DB F6 CA 01 U×±êöÊ..c.ÝÛöÊ.
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 00 30 00 00 00 60 00 00 00 ....0...`...
000098A0 00 00 00 00 00 00 02 00 48 00 00 00 18 00 01 00 ....H.......
000098B0 05 00 00 00 00 00 05 00 E0 77 98 B1 EA F6 CA 01 ....àw˜±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 àw˜±êöÊ.........
000098E0 00 00 00 00 00 00 00 00 20 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 00 18 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 00 ....8...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 11 ....ÿÿÿÿ,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 0A ....
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 ....
Offset(h): 0

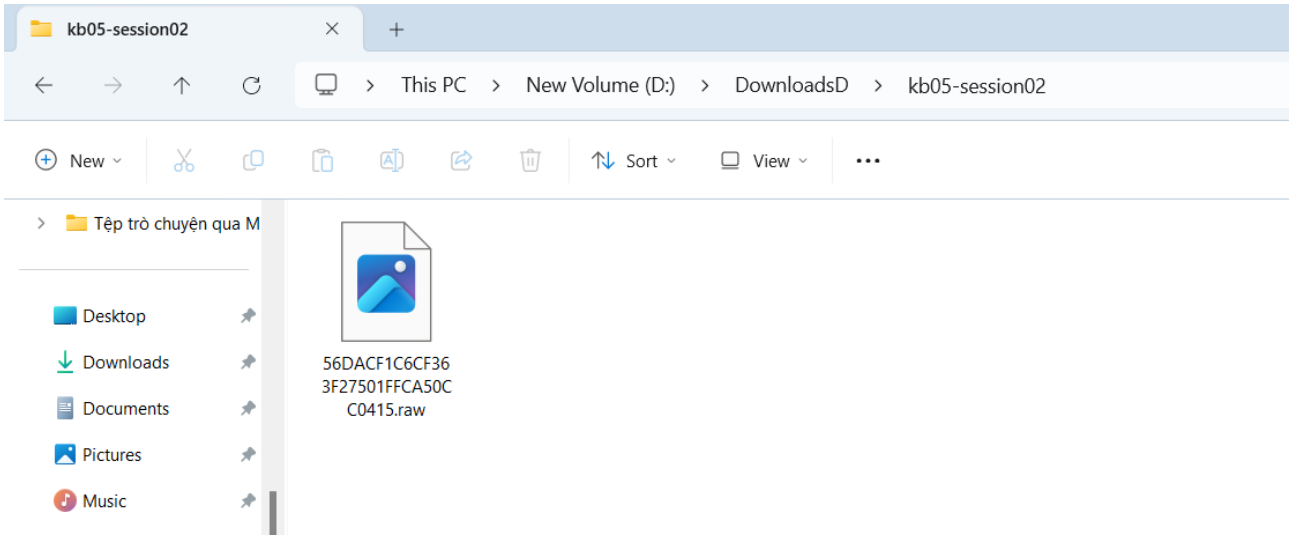
Kịch bản 5

Kịch bản 05. Thực hiện phân tích:

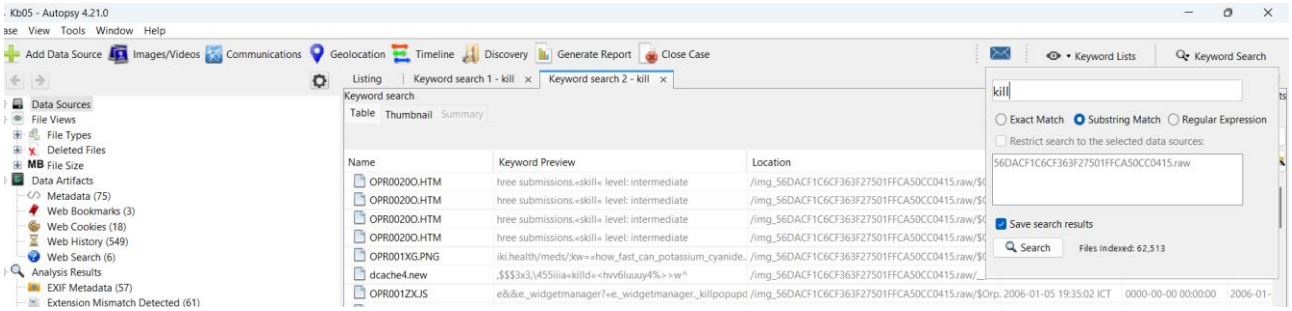
- Tài nguyên: kb05-session02
- Cảnh sát phát hiện một vụ án tình nghi một người đàn ông chết do tự tử. Bằng chứng thu được từ máy tính nạn nhân được gửi cho điều tra viên. Đóng vai làm nhân viên điều tra, hãy tìm manh mối xác định liệu kết luận tình nghi này có đúng hay không.

Đáp án:

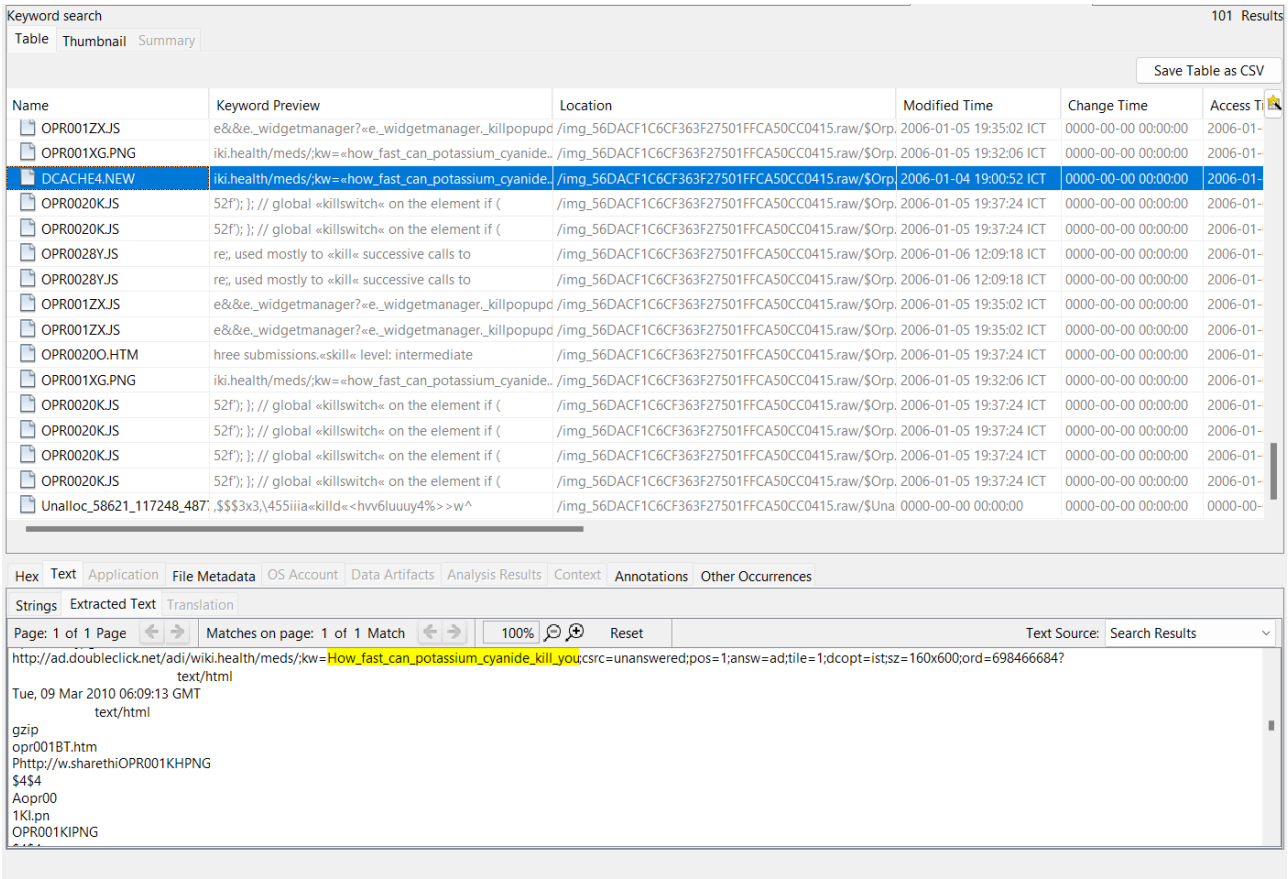
Đổi file kb05-session02 thành file zip rồi extract ra và phân tích với autospy.



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

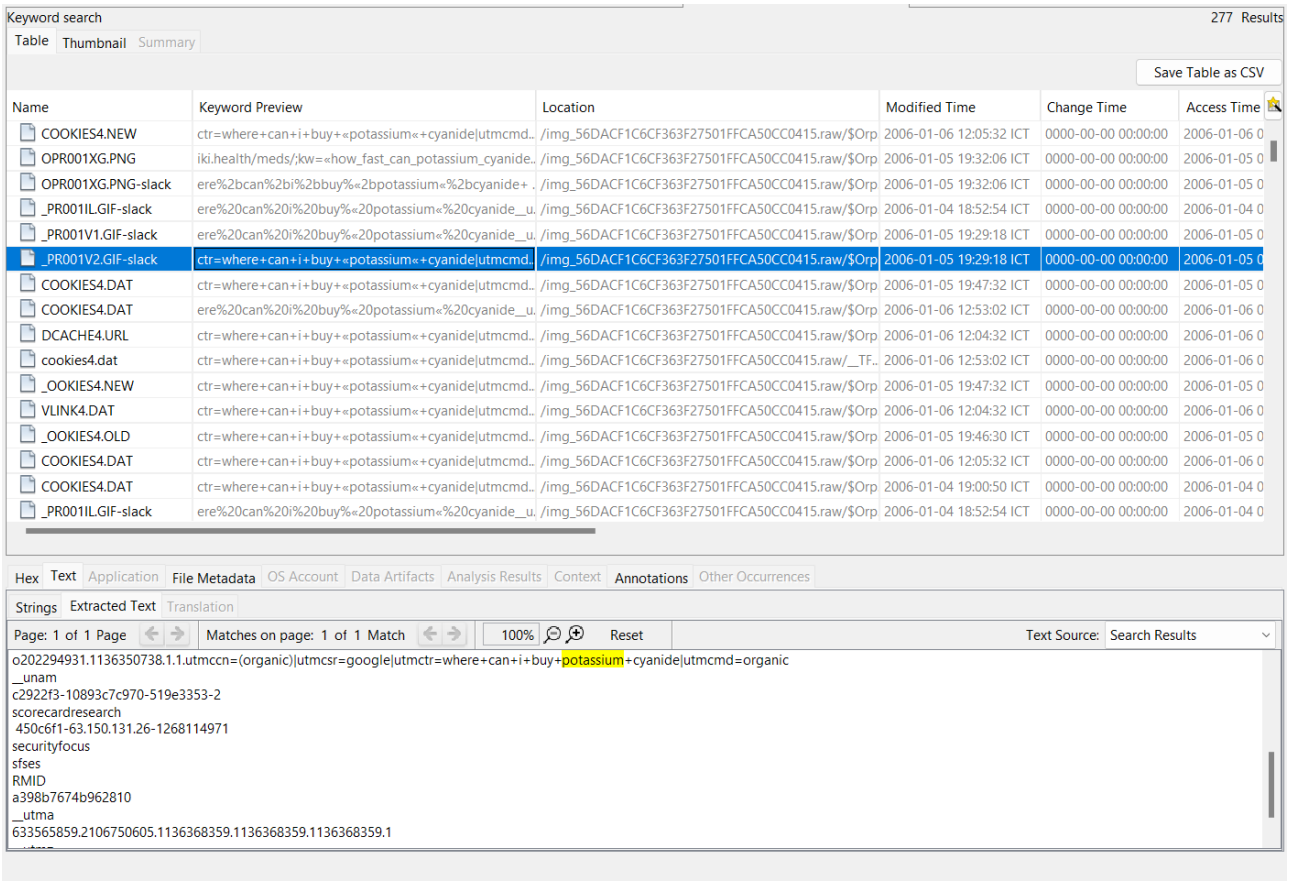


- Ta thấy người đàn ông có tìm kiếm 1 thông tin đại khái là cách chất độc cyanide có thể giết ta trong bao lâu(How_fast_can_potassium_cyanide_kill_you) ở 1 trang tìm kiếm tên là "doubleclick.net".



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

Tiếp tục tìm thử thông tin về potassium.



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

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

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

  Ví dụ: [NT101.H11.1]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT