

# BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 2: Hard Drive Forensics

GVHD: Đoàn Minh Trung

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đại Nghĩa	21521182	21521182@gm.uit.edu.vn
2	Phạm Hoàng Phúc	21521295	21521295@gm.uit.edu.vn
3	Lê Xuân Sơn	21521386	21521386@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%
4	Bài tập 4	100%
5	Bài tập 5	100%
6	Bài tập 6	100%
7	Challenge	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## Câu 1:

New Case Information

Steps

1. Case Information

2. Optional Information

Case Information

Case Name:

Base Directory: 

Browse

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

## Chọn ổ đĩa

Add Data Source

Steps

1. Select Host

2. Select Data Source Type

3. Select Data Source

4. Configure Ingest

5. Add Data Source

Select Data Source

Local Disk: 

Select Disk

Timezone:

☐ Ignore orphan files in FAT file systems  
(faster results, although some data will not be searched)

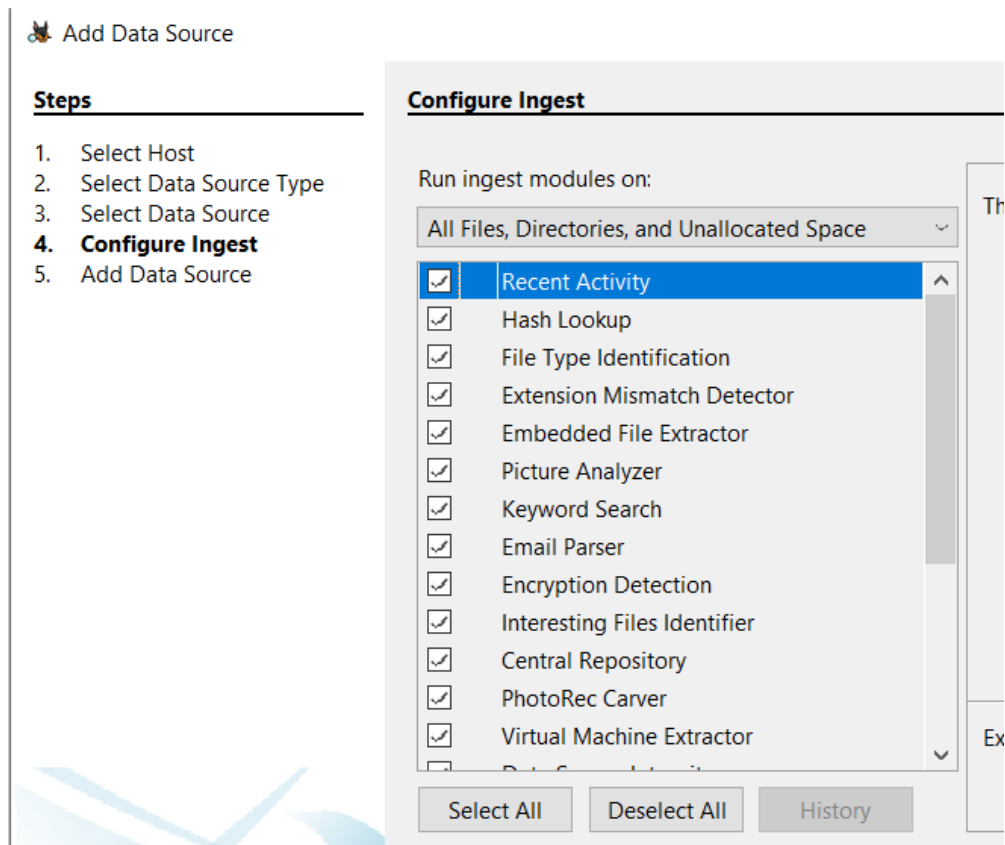
☐ Make a VHD image of the drive while it is being analyzed  

Browse

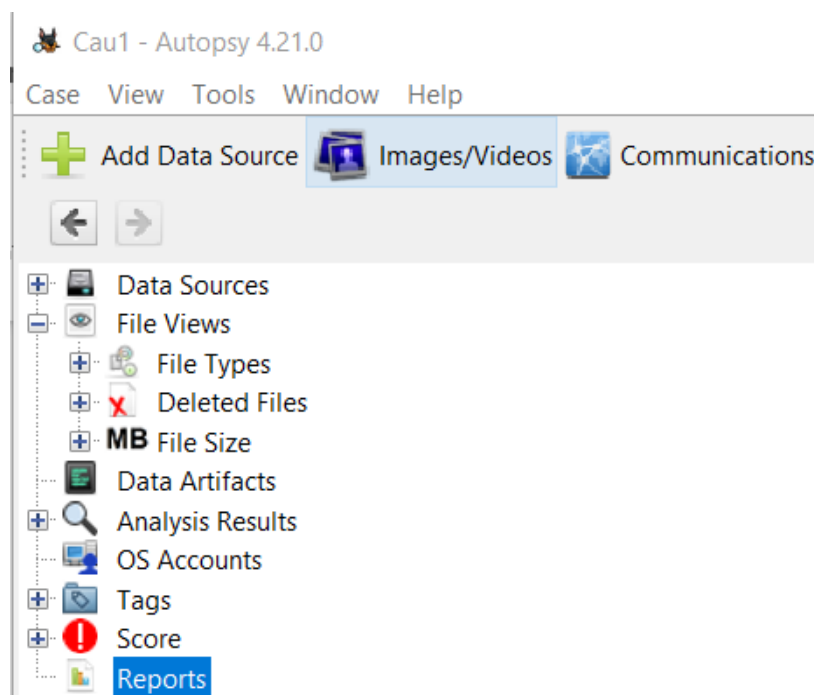
☐ Update case to use VHD file upon completion  
Note that at least one ingest module must be run to create a complete copy

Sector Size:

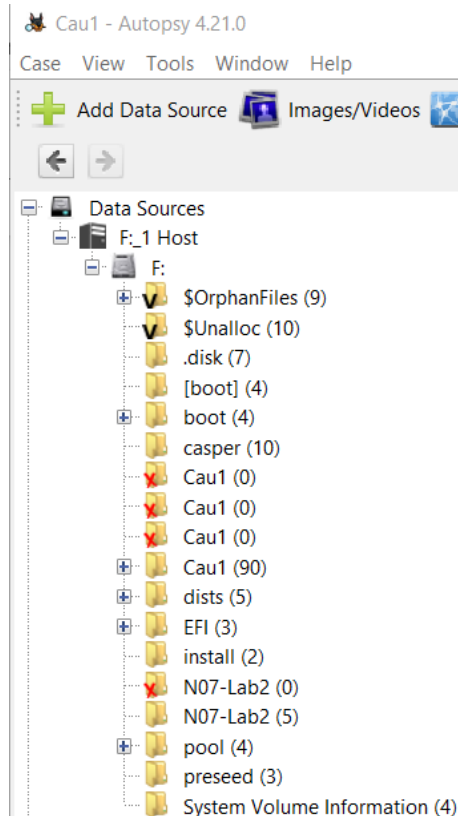
## Chọn các module phân tích



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

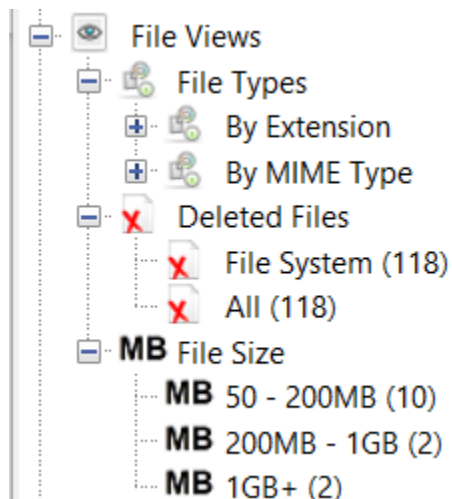


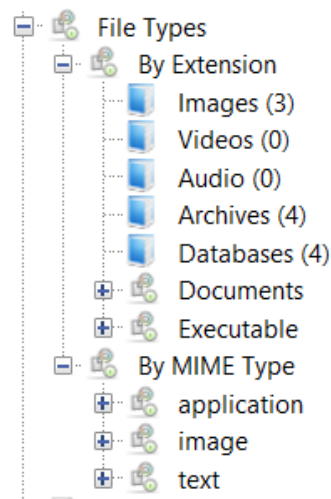
Data Sources: Nơi lưu ổ đĩa được dump ra, ta có xem thông tin cây thư mục



File View: xem tất cả file có trong ổ đĩa, file được phân loại dựa theo:

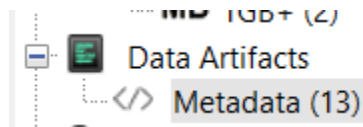
- +File Types: Dựa theo đuôi file (by extension) và theo signature (by MIME type)
- +Delete Files: Xem tất cả file đã bị xóa
- +File Size: Phân loại dựa trên kích cỡ file





Data Artifacts:

Metadata: danh sách các metadata của file

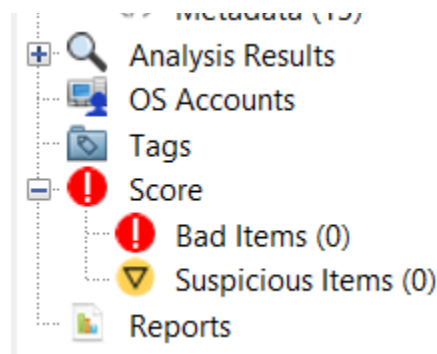


Analysis Result: Lưu kết quả phân tích liên quan đến thông tin được dump

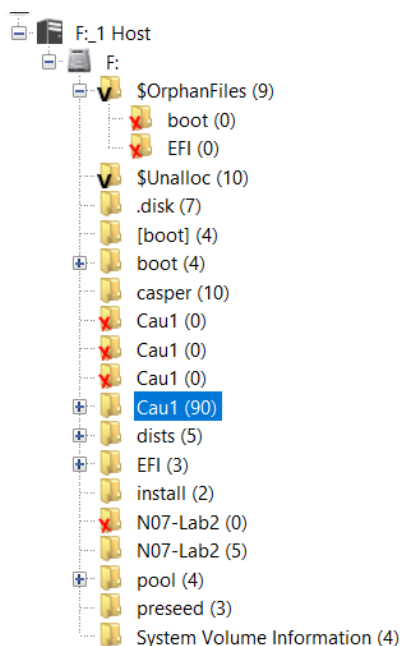
OS Account: Các accounts tồn tại trong hệ điều hành

Tags: Các tags được gắn nhãn từ trước đó

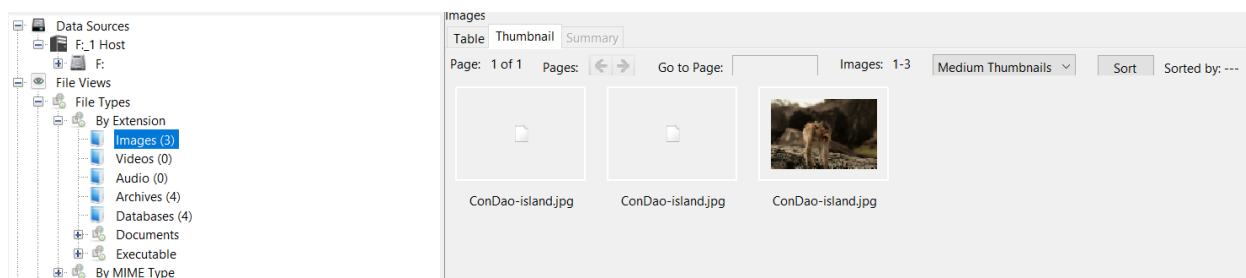
Reports: Các bản báo cáo được lưu lại trước đó



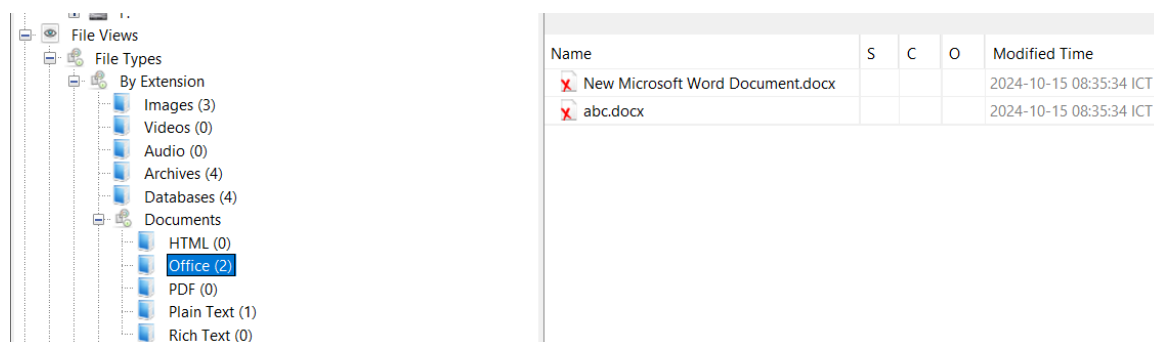
-Tìm thư mục có nhiều File nhất trong Filesystem



-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

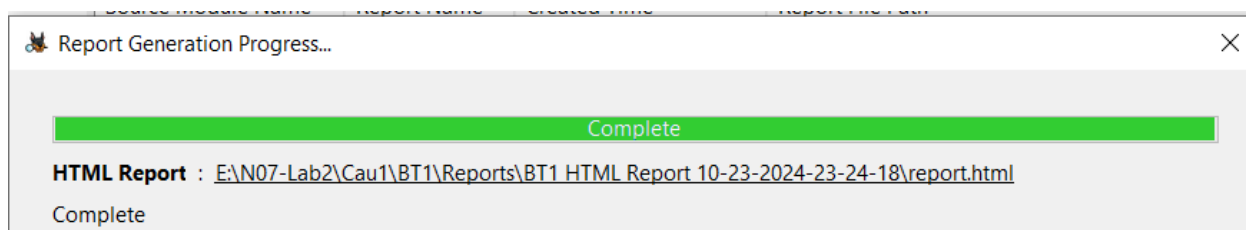


Số lượng file pdf và doc



-Generate report

HTML



Report Navigation

- Case Summary
- ★ Data Source Usage (1)
- Metadata (13)
- ★ Tagged Files (0)
- ★ Tagged Images (0)
- ★ Tagged Results (0)

## Autopsy Forensic Report

HTML Report Generated on 2024/10/23 23:24:18

Case: BT1  
Number of data sources in case: 1

### Image Information:

F:

Timezone: Asia/Saigon  
Path: \\F:

### Software Information:

Autopsy Version:	4.21.0
Android Analyzer Module:	4.21.0
Android Analyzer (aLEAPP) Module:	4.21.0
Central Repository Module:	4.21.0
DJI Drone Analyzer Module:	4.21.0
Data Source Integrity Module:	4.21.0
Email Parser Module:	4.21.0
Embedded File Extractor Module:	4.21.0
Encryption Detection Module:	4.21.0

Đánh giá: Xem được các trường dữ liệu trong AutoSpy với giao diện trực quan hơn so với trong app. Ngoài ra còn có thể xem được phiên bản cụ thể của các tool, plugin được dùng trong quá trình thực hiện điều tra.

## EXCEL

Report Generation Progress...

Complete

Excel Report : E:\N07-Lab2\Cau1\BT1\Reports\BT1 Excel Report 10-23-2024-23-25-12\Excel.xlsx

Complete

Summary		
Case Name:	BT1	
Number of data sources in case:	1	

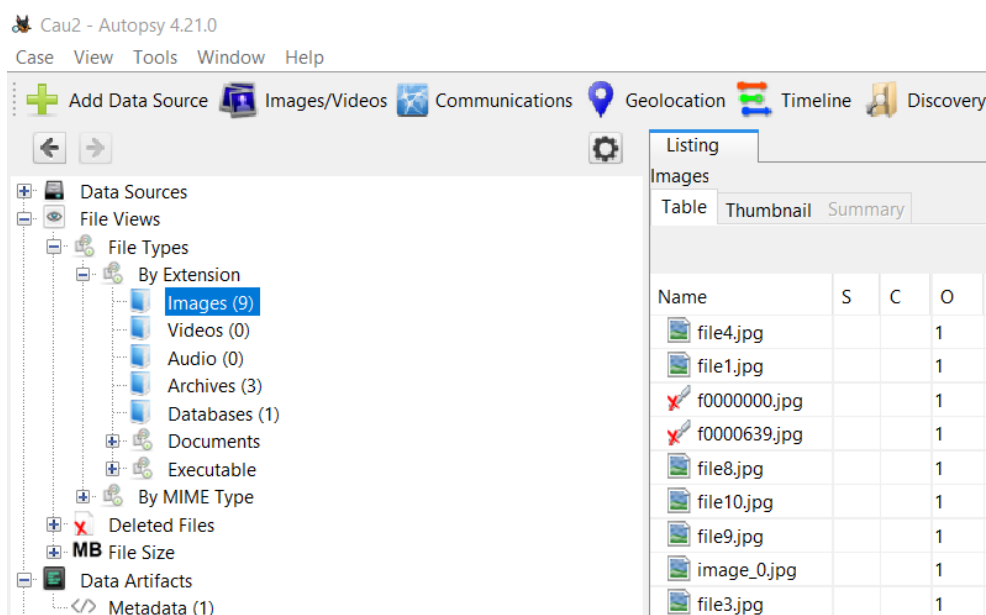
A	B	C	D	E	F	G	H
Date Created	Date Modified	Last Printed Date	Owner	Program Name	User ID	Version	Source File
1999-06-21 09:15:32 ICT	2024-09-11 11:15:42 ICT	1999-07-26 11:07:16 ICT	b-tina	Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Blockchain/Week01-Blockchain network Overview.pptx
1999-06-21 09:15:32 ICT	2024-09-19 03:59:43 ICT	1999-07-26 11:07:16 ICT	b-tina	Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Blockchain/Week02-03-Blockchain network architecture.pptx
1999-06-21 09:15:32 ICT	2024-10-03 04:51:55 ICT	1999-07-26 11:07:16 ICT	b-tina	Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Blockchain/Week04-05-Smart Contract-R2.pptx
1999-06-21 09:15:32 ICT	2024-10-03 04:51:55 ICT	1999-07-26 11:07:16 ICT	b-tina	Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Blockchain/Week04-05-Smart Contract-R3.pptx
1999-06-21 09:15:32 ICT	2024-10-17 04:49:00 ICT	1999-07-26 11:07:16 ICT	b-tina	Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Blockchain/Week06-Application domains (P1).pptx
2006-08-16 00:00:00 ICT	2024-09-07 04:52:45 ICT			Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Đồ án chuyên ngành/Đồ án chuyên ngành.pptx
2006-08-16 00:00:00 ICT	2024-09-28 05:21:16 ICT			Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Đồ án chuyên ngành/Update_Week3-4.pptx
2013-09-16 14:47:59 ICT	2013-10-02 10:40:42 ICT					1.4	/img_F:/Quản lý rủi ro/ISO-IEC_27002-2013_Code-of-Practice.pdf
2013-09-26 23:45:02 ICT	2013-10-03 05:59:15 ICT					1.4	/img_F:/Quản lý rủi ro/ISO IEC 27001-2013.pdf
2024-04-07 17:51:00 ICT	2024-09-13 15:45:00 ICT		Phạm Hoàng Phúc	Microsoft Office Word	Phạm Hoàng Phúc		/img_F:/Đồ án chuyên ngành/IDS_LAB.docx
2024-05-21 17:58:17 ICT	2024-09-20 16:17:21 ICT		Phạm Hoàng Phúc	Microsoft Office PowerPoint	Phạm Hoàng Phúc		/img_F:/Đồ án chuyên ngành/Wazuh_topology.pptx
2024-05-28 18:53:00 ICT	2024-06-14 05:37:00 ICT		ADMIN	Microsoft Office Word	ADMIN		/img_F:/Đồ án chuyên ngành/ATMNC.docx
2024-10-18 10:31:00 ICT	2024-10-18 12:56:00 ICT		Phạm Hoàng Phúc	Microsoft Office Word	Phạm Hoàng Phúc		/img_F:/Đồ án Forensics/Anti disk and Image file forensics.docx

Đánh giá: File report dạng Excel được chia thành nhiều sheet tương ứng với nhiều trường dữ liệu. Không trực quan bằng file report HTML.

Không có phần summary các version tool, plugin, không đầy đủ bằng file report HTML.

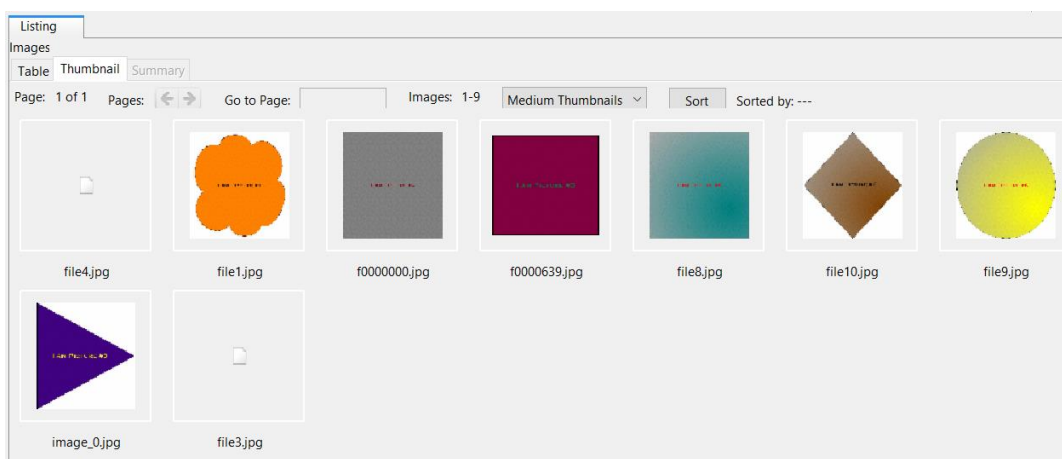
## Câu 2:

Vào File Views -> File Types -> By extension -> Chọn Images



Có tổng cộng 9 bức ảnh





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

file4.jpg - Properties	
Properties	
Name	file4.jpg
S	(No Property Editor)
C	NO_COMMENT
O	1
Modified Time	2004-06-10 14:38:06 ICT
Change Time	2004-06-10 10:28:22 ICT
Access Time	2004-06-10 10:28:22 ICT
Created Time	2004-06-10 10:28:20 ICT
Size	189021
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/invalid/file4
MD5 Hash	c8de721102617158e8492121bdad3711
SHA-256 Hash	0da94b7a5d24696f7dca510255493ca4e5ae
MIME Type	application/octet-stream
Extension	jpg
file4.jpg	

file1.jpg - Properties

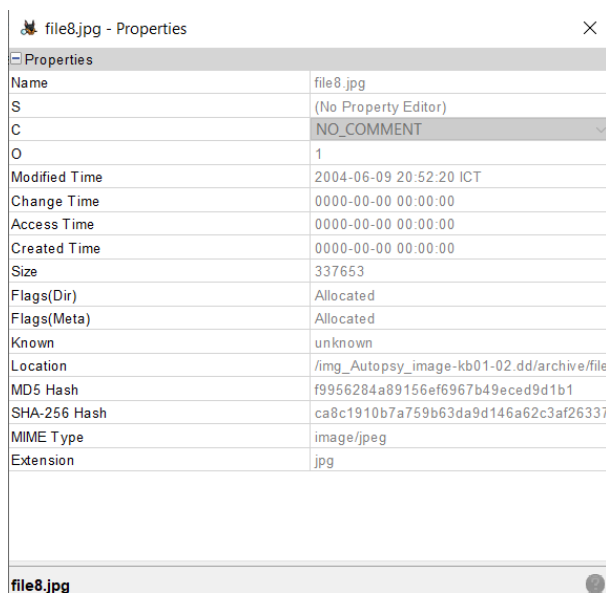
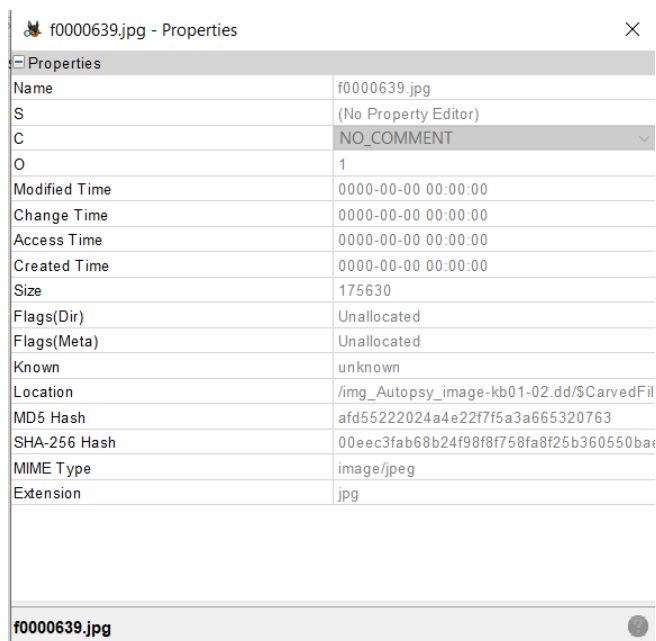
Properties	
Name	file1.jpg
S	(No Property Editor)
C	NO_COMMENT
O	1
Modified Time	2004-06-10 13:59:40 ICT
Change Time	2004-06-10 10:27:36 ICT
Access Time	2004-06-10 10:27:36 ICT
Created Time	2004-06-10 10:27:36 ICT
Size	274260
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/alloc/file1.j
MD5 Hash	75b8d00568815a36c3809b46fc84ba6d
SHA-256 Hash	2a082002a5d42b716b7934a23371ceb0bae
MIME Type	image/jpeg
Extension	jpg

file1.jpg

f0000000.jpg - Properties

Properties	
Name	f0000000.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	326859
Flags(Dir)	Unallocated
Flags(Meta)	Unallocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/\$CarvedFi
MD5 Hash	0c452c5800fcfa7c66027ae89c4f068a
SHA-256 Hash	e09242768c1f897f197bd499042511b105c2
MIME Type	image/jpeg
Extension	jpg

f0000000.jpg



file10.jpg - Properties	
Properties	
Name	file10.jpg
S	(No Property Editor)
C	NO_COMMENT
O	1
Modified Time	2004-06-10 08:54:53 ICT
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	208919
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/archive/file
MD5 Hash	c476a66ccdc2796b4f6f8e27273dd788
SHA-256 Hash	81f5733ec0a6053ef00351503e8264550f485
MIME Type	image/jpeg
Extension	jpg
file10.jpg	

file9.jpg - Properties	
Properties	
Name	file9.jpg
S	(No Property Editor)
C	NO_COMMENT
O	1
Modified Time	2004-06-09 20:53:32 ICT
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	292813
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/archive/file
MD5 Hash	c5a6917669c77d20f30ecb39d389eb7d
SHA-256 Hash	522443d66dfdf4d1a88e36721f6f74458c508
MIME Type	image/jpeg
Extension	jpg
file9.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
MD5 Hash	936d202fbedecbe64b42c5f3d03233e5
SHA-256 Hash	3a3f2e50f1eefb0f19ec4c3b0c69dd4f0d5158
MIME Type	image/jpeg
Extension	jpg

image\_0.jpg

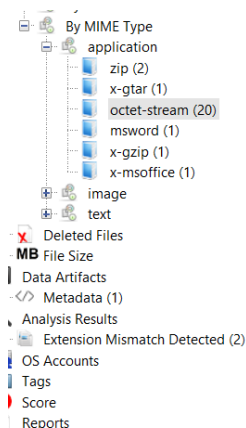
file3.jpg - Properties

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	1ba4e91591f0541eda255ee26f7533bc
SHA-256 Hash	f1684e96895d2970dbda0f95786f8b41109c7
MIME Type	text/plain
Extension	jpg

file3.jpg

Ngoài ra, nếu vào File Types -> By MIME Type -> octet-stream, ta sẽ tìm thấy file11.dat

Đây là 1 file ảnh được ẩn bằng cách chèn thêm byte vào file. Dấu hiệu để nhận biết đây là một file ảnh là vì file có chứa byte JFIF - byte này luôn xuất hiện ở các file ảnh ở trên.



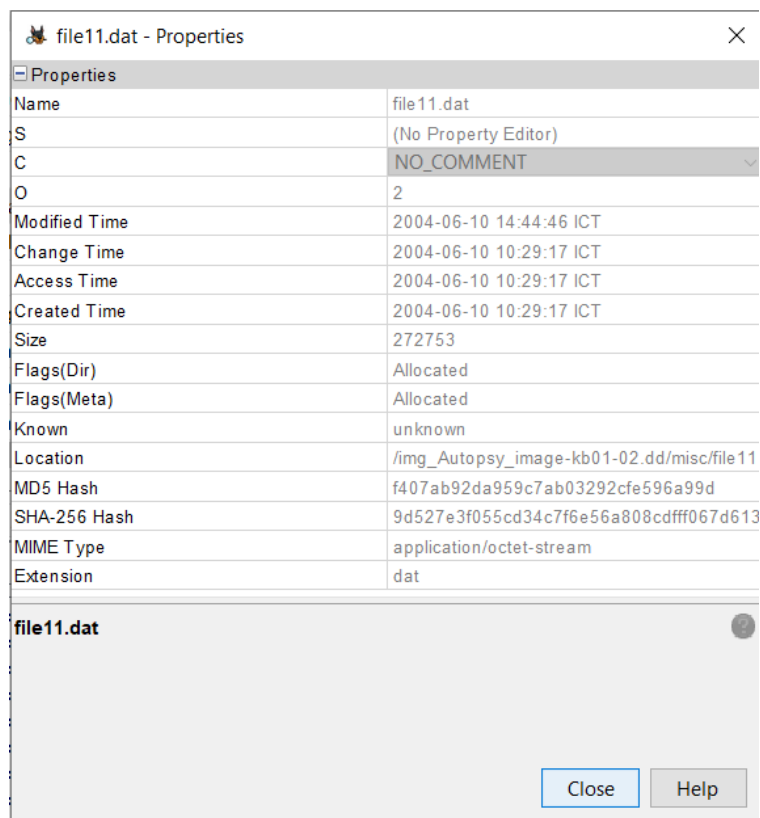
Name	S	C	O	Modified Time	Change Time	Access Time
\$Volume				2004-06-10 10:22:22 ICT	2004-06-10 10:22:22 ICT	2004-06-10 10:22:22 ICT
file4.jpg			2	2004-06-10 14:38:06 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:22 ICT
file5.rtf			2	2004-06-10 14:41:54 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT
file11.dat			2	2004-06-10 14:44:46 ICT	2004-06-10 10:29:17 ICT	2004-06-10 10:29:17 ICT
file13.dll			2	2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT
INFO2			2	2004-06-10 10:59:31 ICT	2004-06-10 10:59:31 ICT	2004-06-10 10:59:31 ICT
tracking.log			2	2004-06-10 10:44:37 ICT	2004-06-10 10:44:37 ICT	2004-06-10 10:44:37 ICT
random8.dat			2	2004-06-09 21:06:22 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00
random10.dat			2	2004-06-10 09:18:41 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00
random9.dat			2	2004-06-09 21:17:38 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other C
Page: 1 of 17	Page	Go to Page: 1	Jump to Offset	Launch					

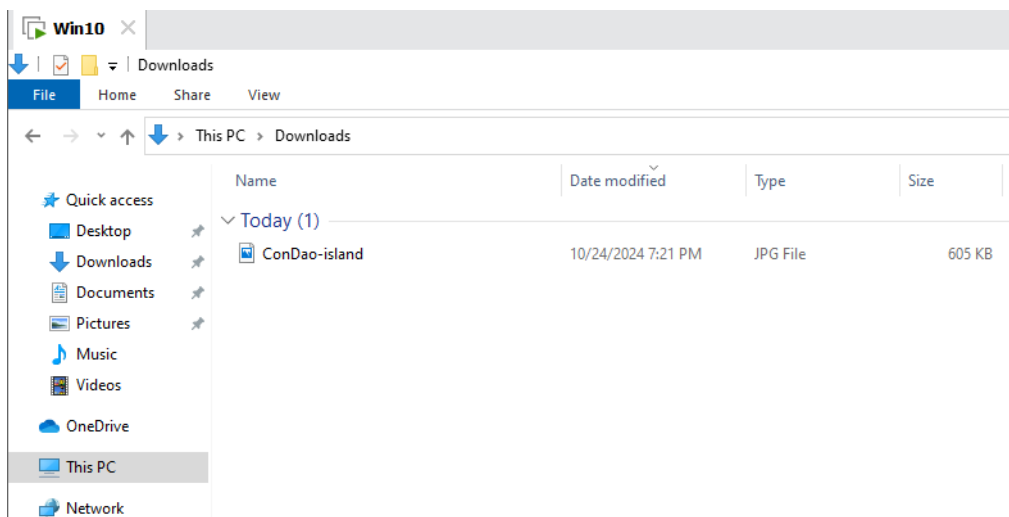
```
0x0000005a0: 62 1B B2 2F FA C6 5F 0C 78 8A 01 B3 C4 EF 8C 23 b./...x.....#
0x0000005b0: B2 5B 49 B0 8F C8 10 F4 38 9B 7E 65 57 94 6C 3F .[I....8.-eW.1?
0x0000005c0: 30 D7 21 81 AB F4 F2 34 61 C7 42 1D F3 04 0B 37 0!....4a.B....7
0x0000005d0: EC 0D 4A EC 73 3F 10 00 CB FF 04 86 7D BF 7A 20 .J.s?.....}.z
0x0000005e0: 2A 23 62 7F 4C 34 E3 C5 AA 86 E3 29 D6 F0 48 83 *#b.L4.....).H.
0x0000005f0: BD 2C 69 01 17 0F S6 3D DC S6 7B 2C 6F 79 E0 BC .,1...V=.{,oy..
0x000000600: 8C EF 90 4C E3 CF 03 A3 C3 9C 3C 15 9E 7A 17 07 ...L.....<..z...
0x000000610: FB 34 EC 0B 9D 5A 51 EE 51 7A A0 64 55 0F 92 E6 .4...2Q.Qz.dU...
0x000000620: EE E0 D4 AA FF D8 FF E0 00 10 4A 46 49 46 00 01 .....Jfif...
0x000000630: 01 00 00 01 00 01 00 00 FF DB 00 43 00 01 01 01 .....C.....
0x000000640: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....C.....
```

### Thông tin file

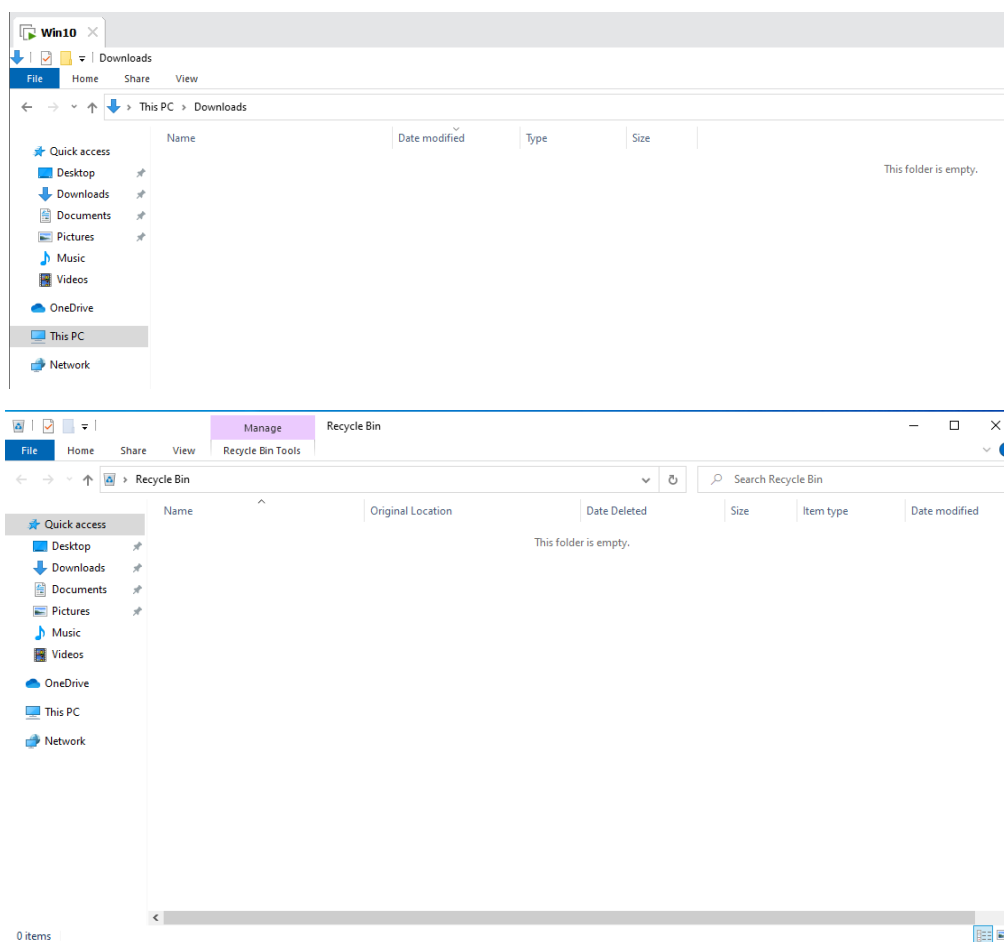


### Câu 3:

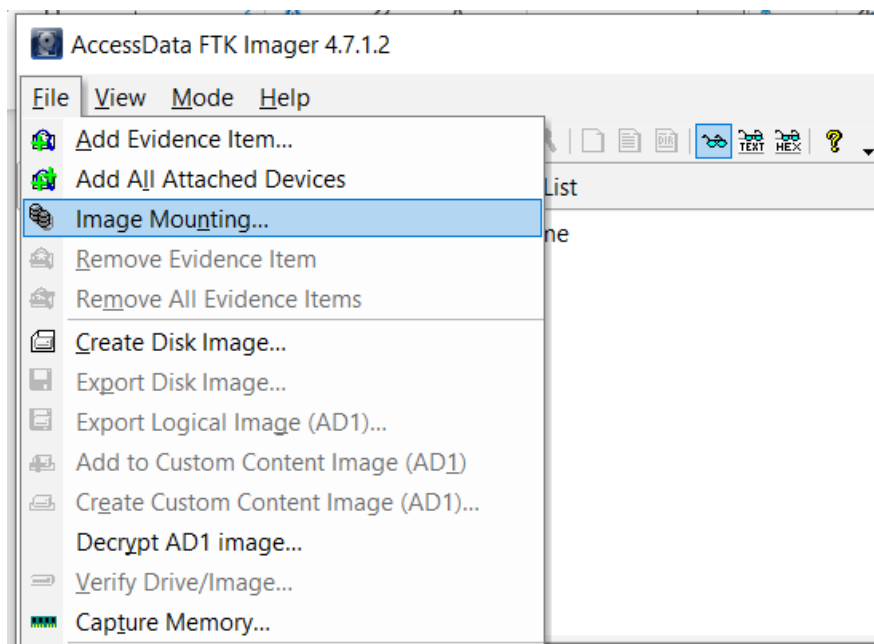
Tải file ảnh về và đổi tên file thành ConDao-island



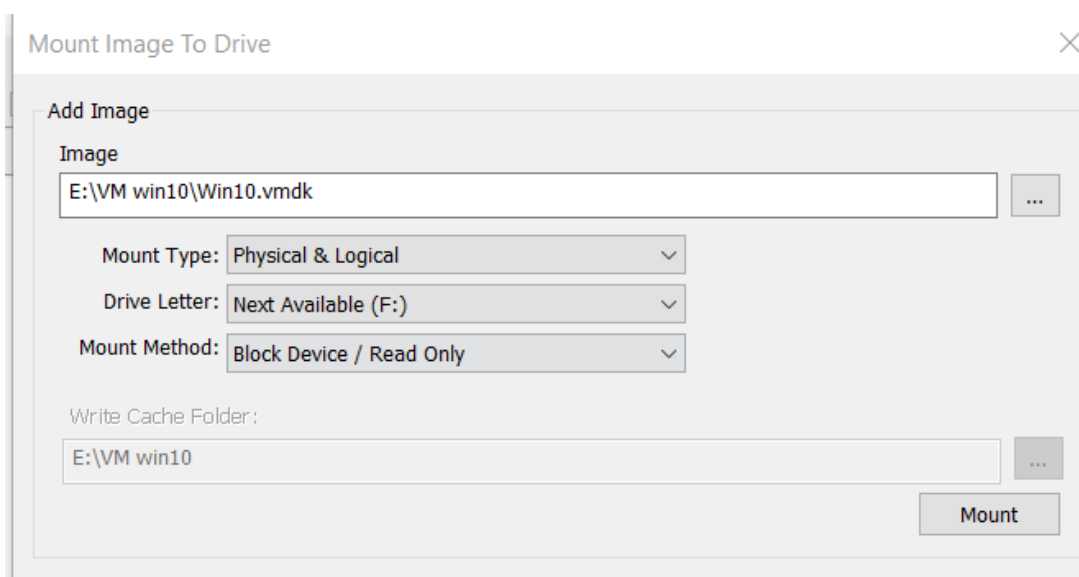
Xóa file ảnh, xóa cả trong Recycle Bin



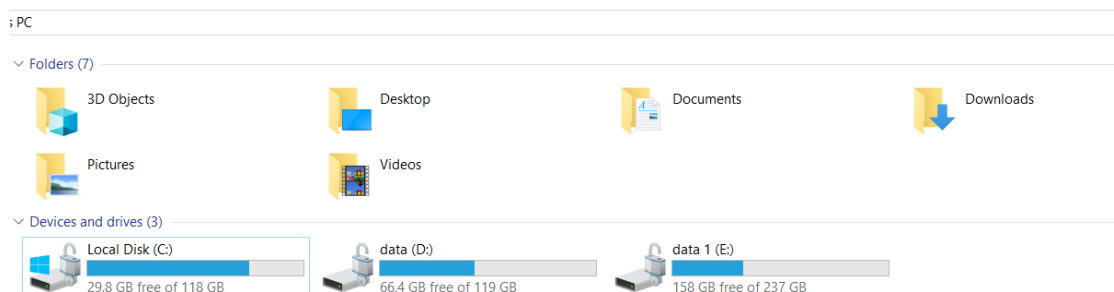
Mở công cụ FTK Imager, vào File -> Image mounting



Tiến hành Mounting

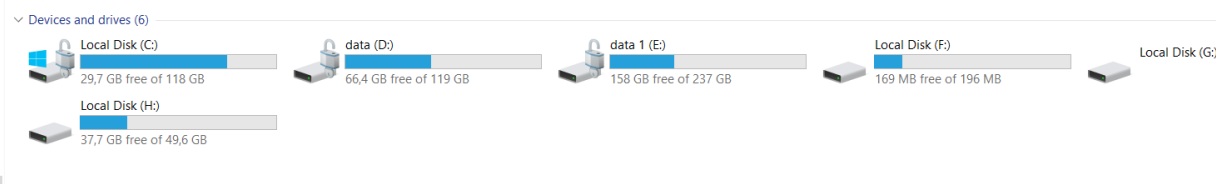


Trước khi mount

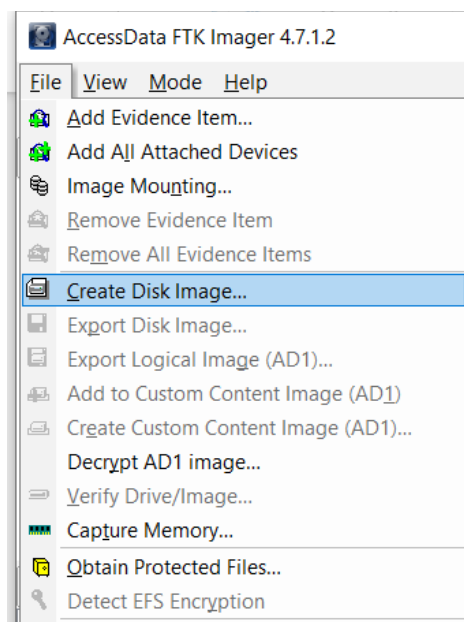


Sau khi mount

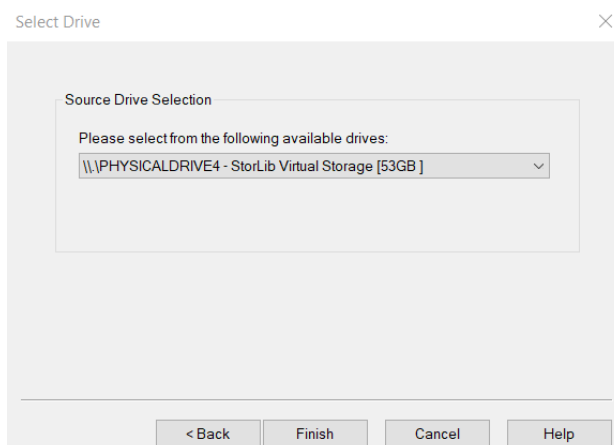




Chọn Create Disk Image

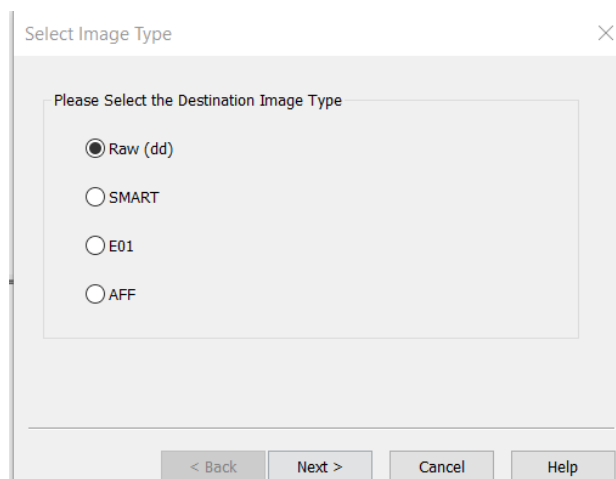


Chọn ổ đĩa cần dump dữ liệu



Nhấn Add để thêm các trường thông tin:

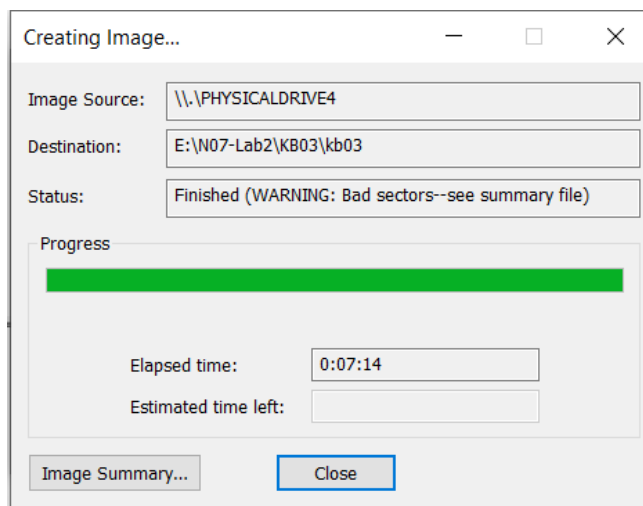
Chọn Raw dd



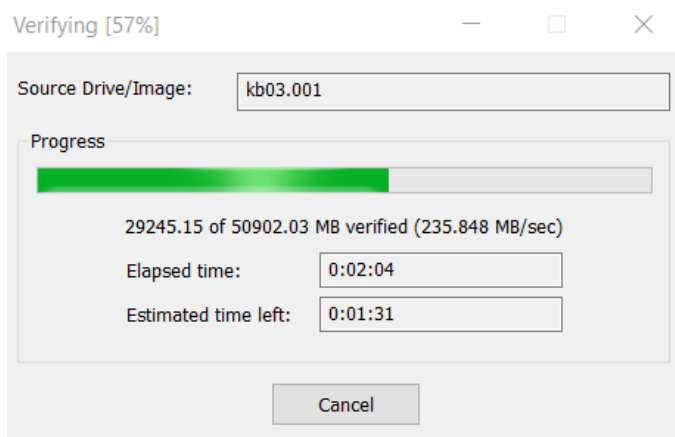
Thêm các thông tin về evidence

Thêm thông tin vị trí lưu trữ image

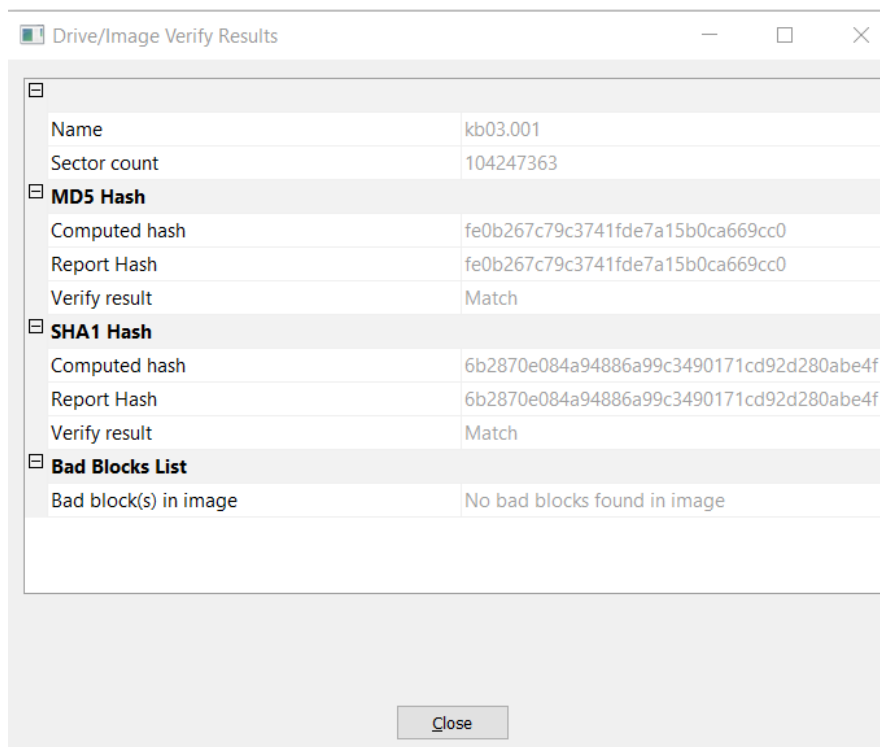
Thực hiện tạo image



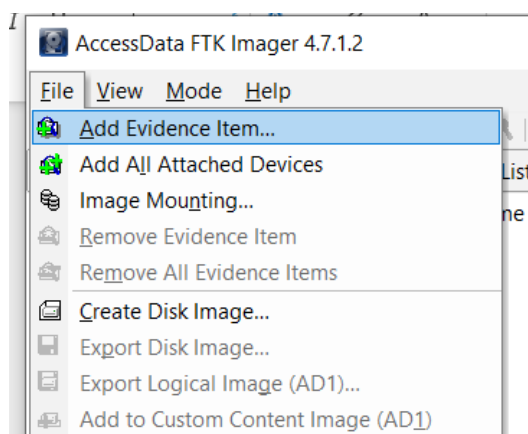
Thực hiện quá trình verify



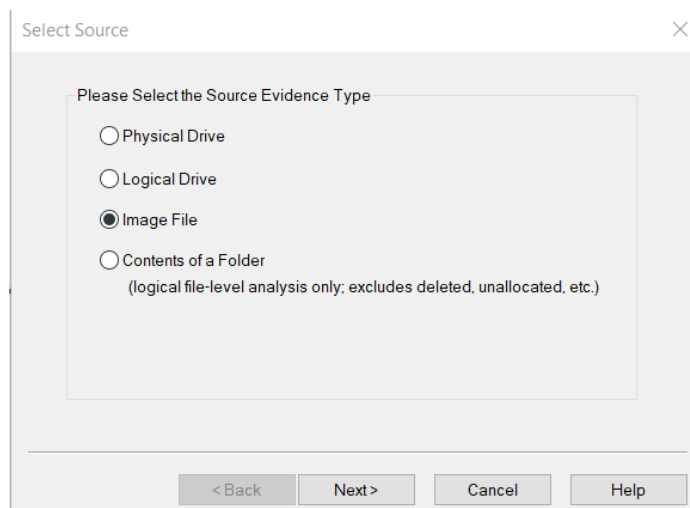
Kết quả



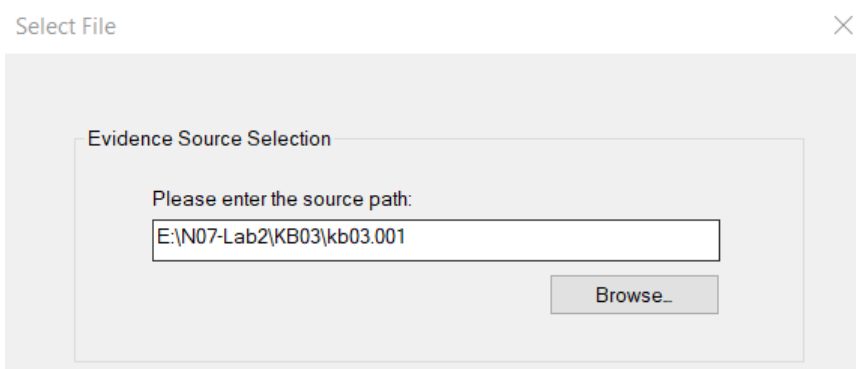
Thực hiện Add evidence



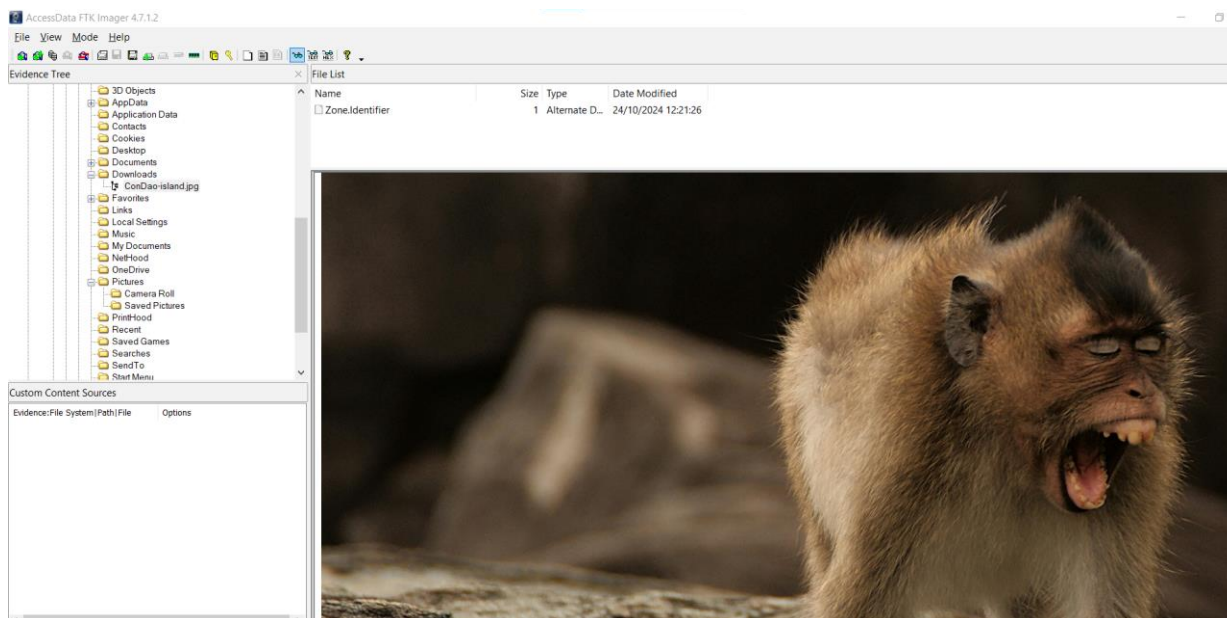
Chọn Image file



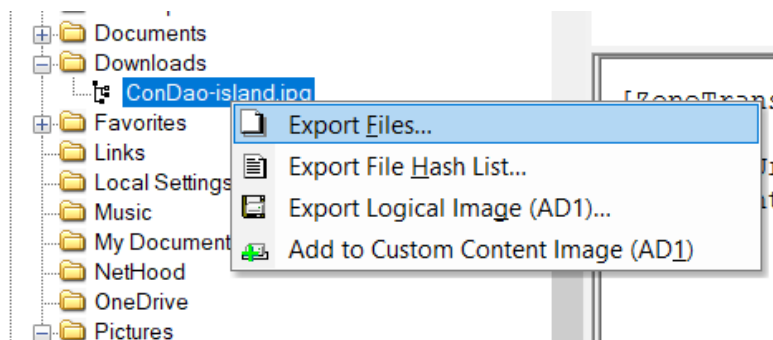
Chọn file kb03.001



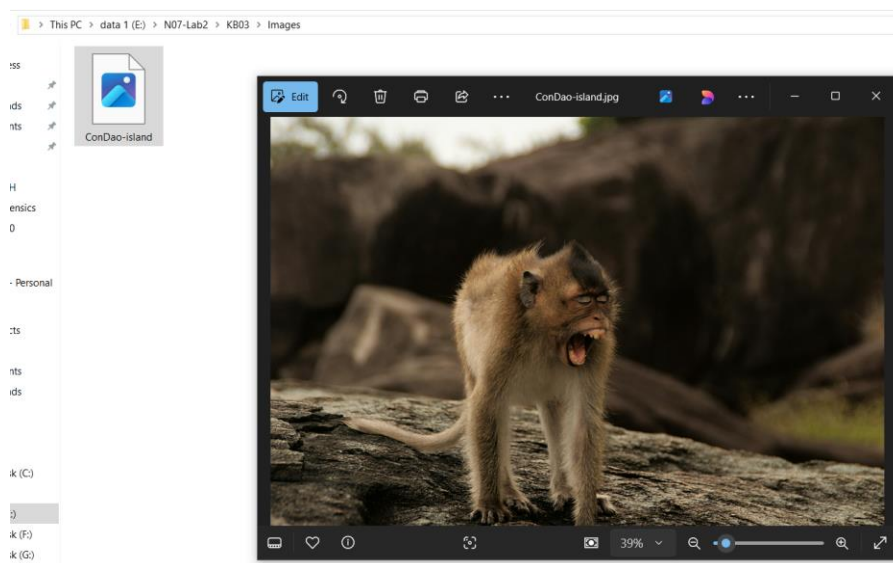
Ta tìm được ảnh ConDao-island đã bị xóa



Sử dụng tính năng Export Files để xuất file ảnh.



Lưu file ảnh vào thư mục KB3/Images



Kiểm tra giá trị hash MD5 của file ảnh vừa được phục hồi



So sánh với file ảnh gốc, ta thấy rằng mã hash của 2 file này là hoàn toàn trùng khớp

Input


  
marek-michalsky-uXPBXlruX5o-unsplash.jpg

Output

f0ab37fc67beeb2c23ffc7f4482dc834

Mình chứng làm bài

```

Command Prompt
C:\Users\ADMIN>dir E:\N07-Lab2\KB03\Images | findstr "ConDao-island"
24/10/2024  19:21          619.289 ConDao-island.jpg

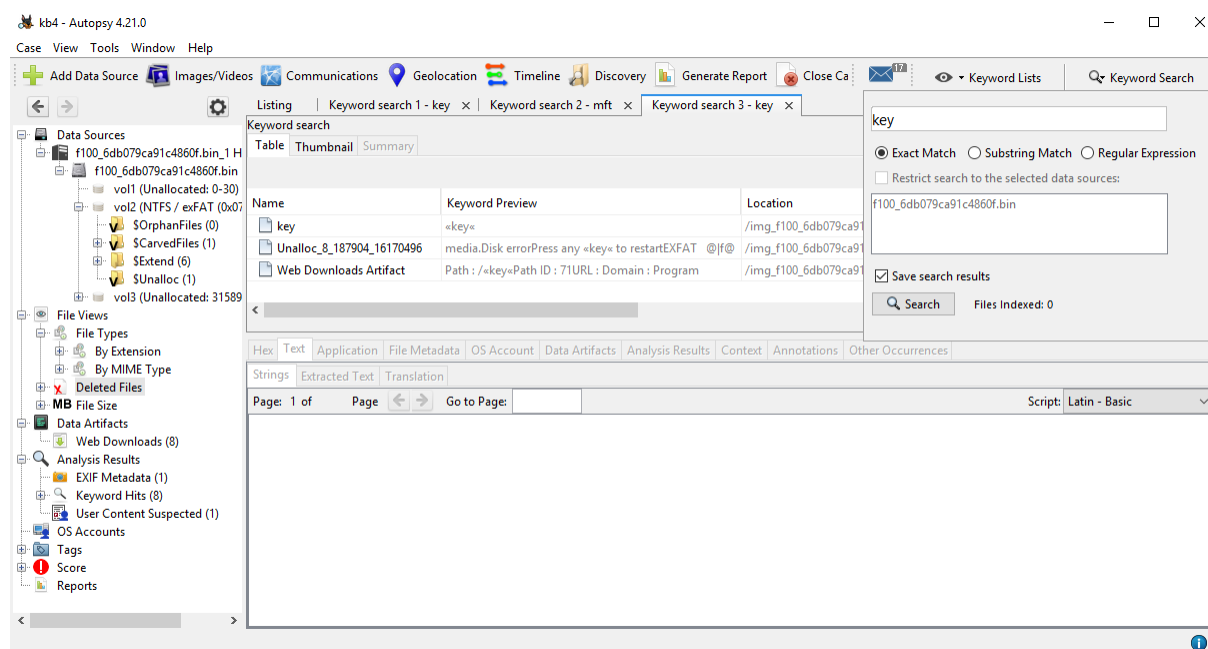
C:\Users\ADMIN>date /t
24/10/2024

C:\Users\ADMIN>echo "N07"
"N07"

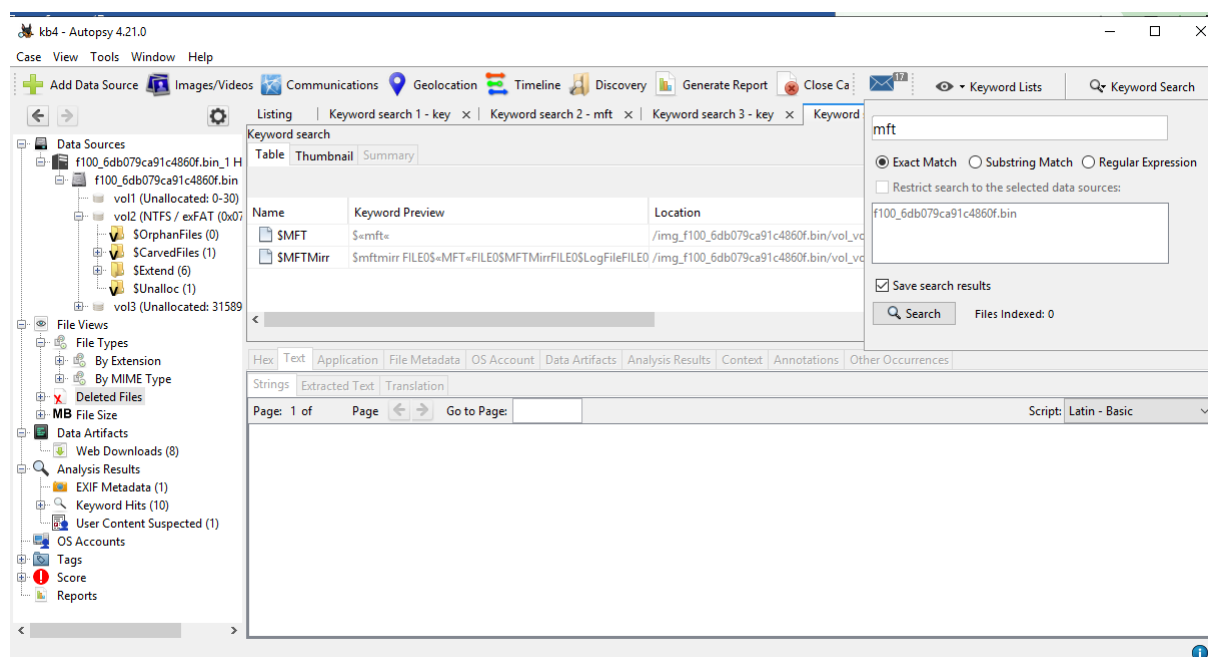
C:\Users\ADMIN>
    
```

## Câu 4:

Trước tiên ta sẽ tìm bằng từ khoá key, ta tìm được các 3 file có chứa từ khoá key





Trong lab hướng dẫn có gợi ý về file MFT, vì vậy em tiếp tục tìm file mft, có được 2 file có key là mft, 1 file MFT.



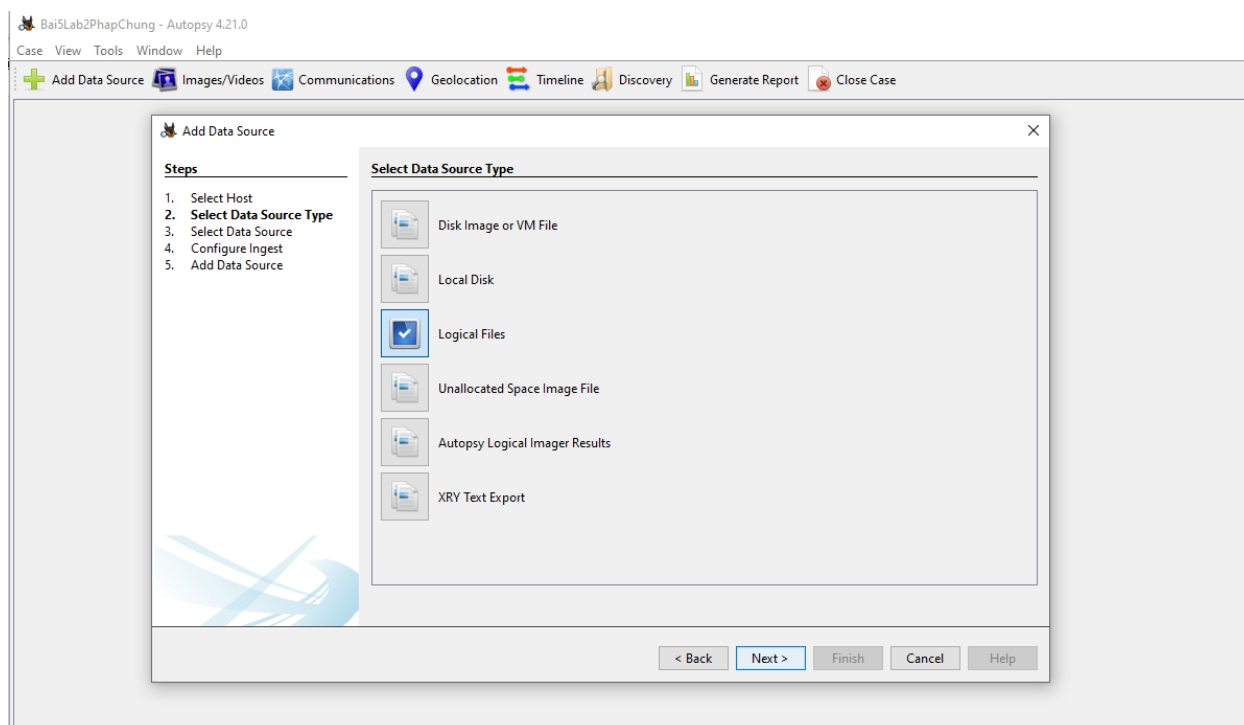
Tìm kiếm trong file MFT ta có thể tìm ra được từ khoá key trong mã hex của file:



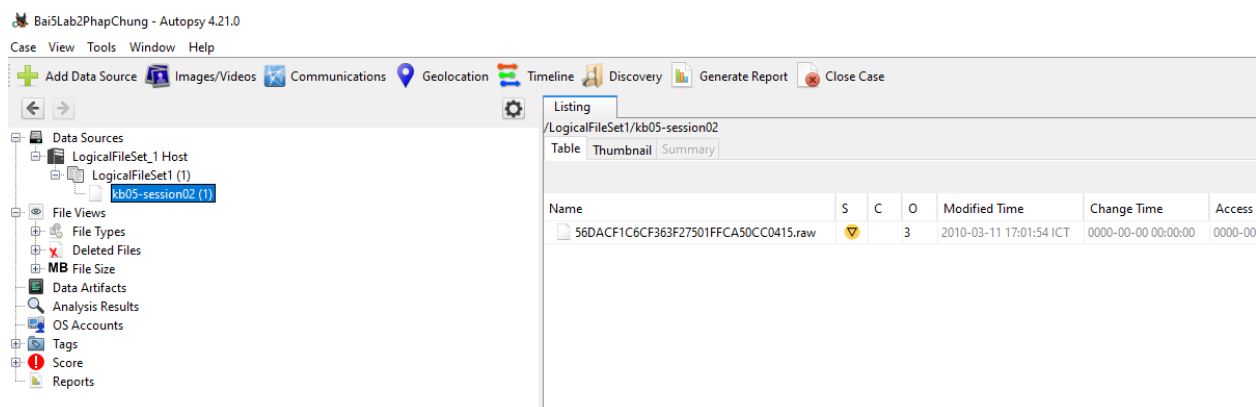
Page: 3 of 16	Page	 	Go to Page: 3	Jump to Offset	<input type="text"/>	Launch in HxD
<hr/>						
0x00009890:	00 00 00 00	00 00 00 00	30 00 00 00	60 00 00 00	.....0.....	
0x000098a0:	00 00 00 00	00 00 02 00	48 00 00 00	18 00 01 00	.....H.....	
0x000098b0:	05 00 00 00	00 00 05 00	E0 77 98 B1	EA F6 CA 01	.....w.....	
0x000098c0:	E0 77 98 B1	EA F6 CA 01	E0 77 98 B1	EA F6 CA 01	.w.....w.....	
0x000098d0:	E0 77 98 B1	EA F6 CA 01	00 00 00 00	00 00 00 00	.w.....	
0x000098e0:	00 00 00 00	00 00 00 00	20 00 00 00	00 00 00 00	.....	
0x000098f0:	03 03 6B 00	65 00 79 00	80 00 00 00	48 00 00 00	..k.e.y.....H...	
0x00009900:	00 00 18 00	00 00 01 00	00 00 00 00	18 00 00 00	.....	
0x00009910:	6E 00 6F 00	74 00 64 00	65 00 6C 00	65 00 74 00	n.o.t.d.e.l.e.t.	
0x00009920:	65 00 64 00	2C 00 6E 00	65 00 76 00	65 00 72 00	e.d.,.n.e.v.e.r.	
0x00009930:	65 78 69 73	74 65 64 0D	0A 00 00 00	00 00 00 00	existed.....	
0x00009940:	80 00 00 00	58 00 00 00	00 0F 18 00	00 00 03 00	...X.....	

**Câu 5:**

Đầu tiên em chọn option Logical Files để thực hiện đọc file kb05-session02:

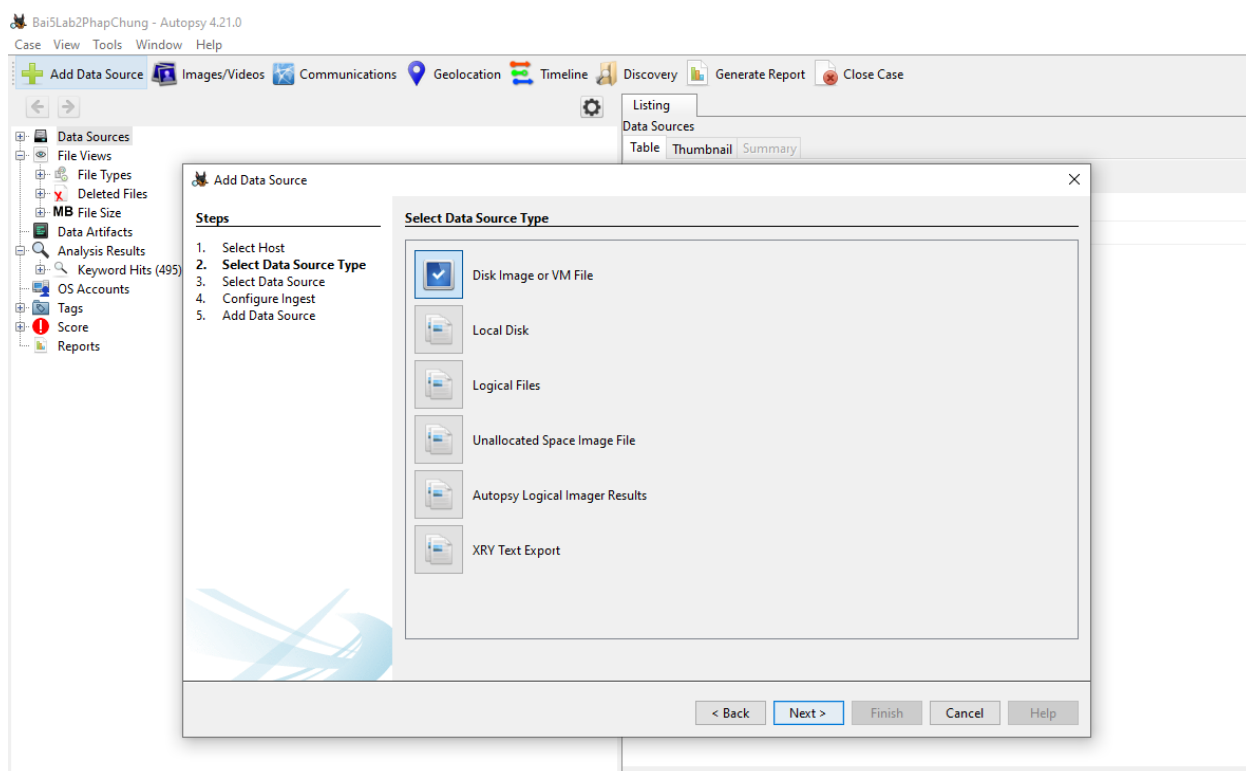


Kết quả nhận được như sau:

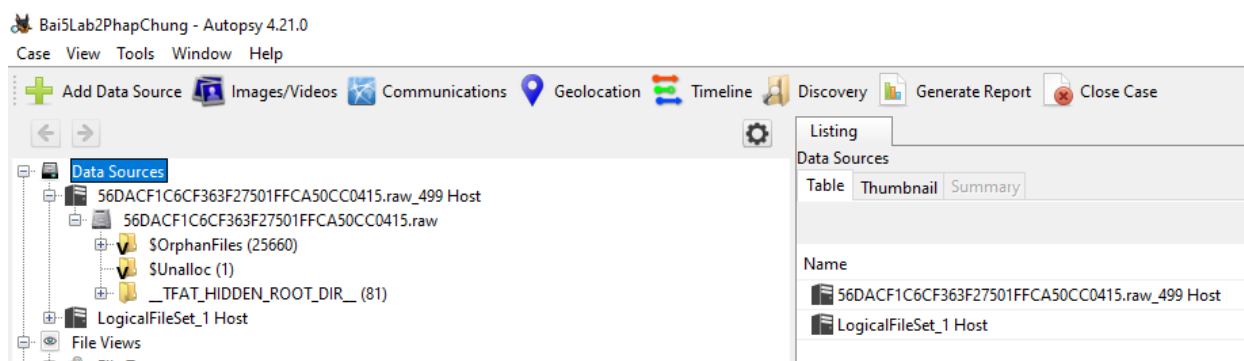


Em thấy rằng có file 56DACF1C6CF363F27501FFCA50CC0415.raw nên đã extract nó ra (vì với file kb05-session02 hiện tại đang mở em không thể tìm được bất cứ thông tin gì cho kết quả trong file này).

Vì là file raw nên em sẽ mở nó bằng option Disk Image ở VM File:

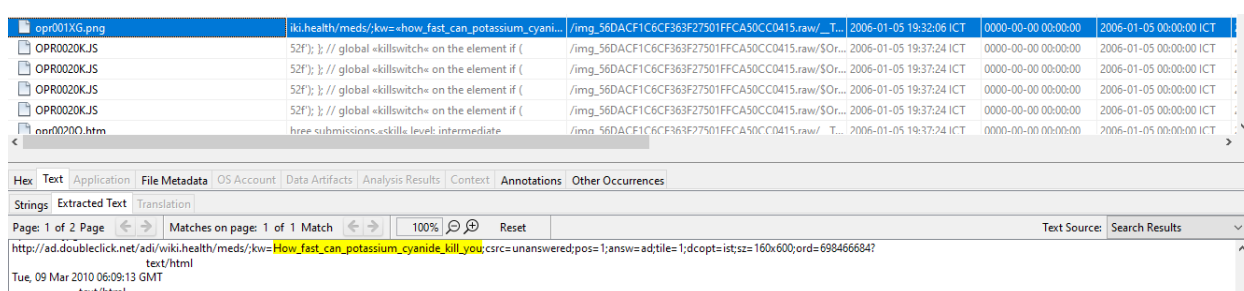


Kết quả nhận được như sau:



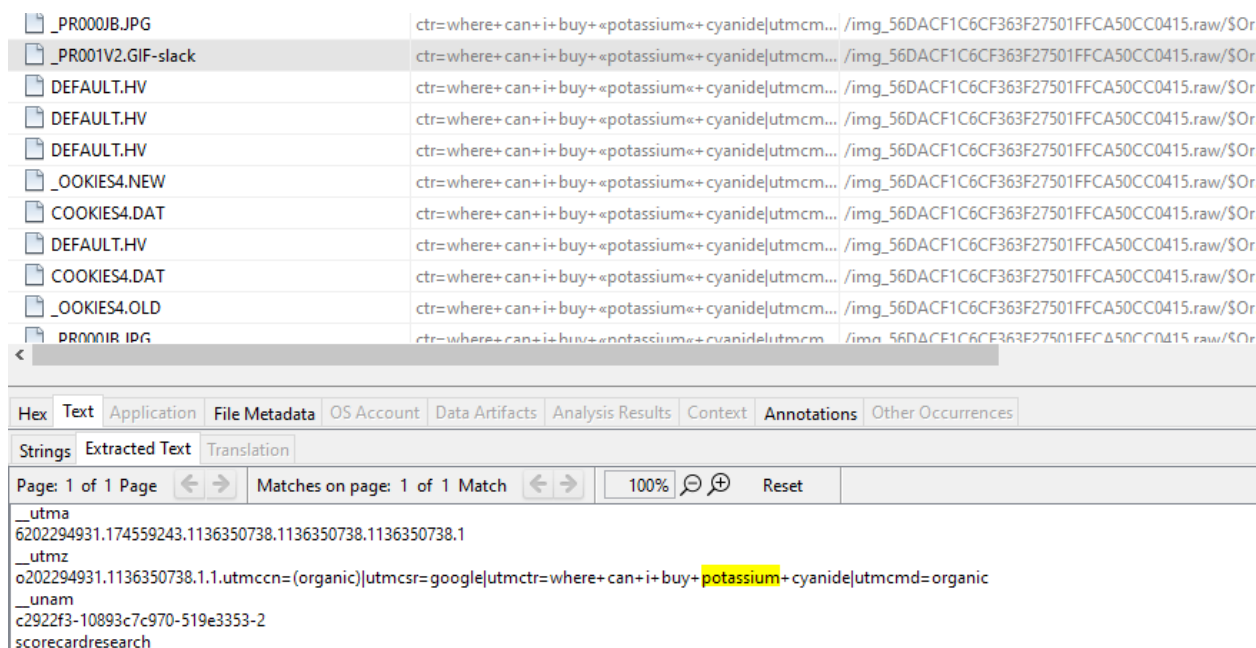
Bây giờ em sẽ tiến hành tìm kiếm chứng cứ, bởi vì nghi người này chết do tự tử nên sẽ có các keywords tìm kiếm khả thi như sau: 'dead', 'suicide', 'kill', 'gun', 'medicine', 'depression',.....

Lần lượt thử qua hết các keywords thì em có phát hiện ở keyword 'kill':



Ở đây em tìm được dòng chữ “How\_fast\_can\_potassium\_cyanide\_kill\_you” từ một trang quảng cáo hiển thị tới nạn nhân.

Đã có được 1 phần manh mối nên em tiếp tục tìm kiếm tiếp 2 từ khóa 'potassium' và 'cyanide':



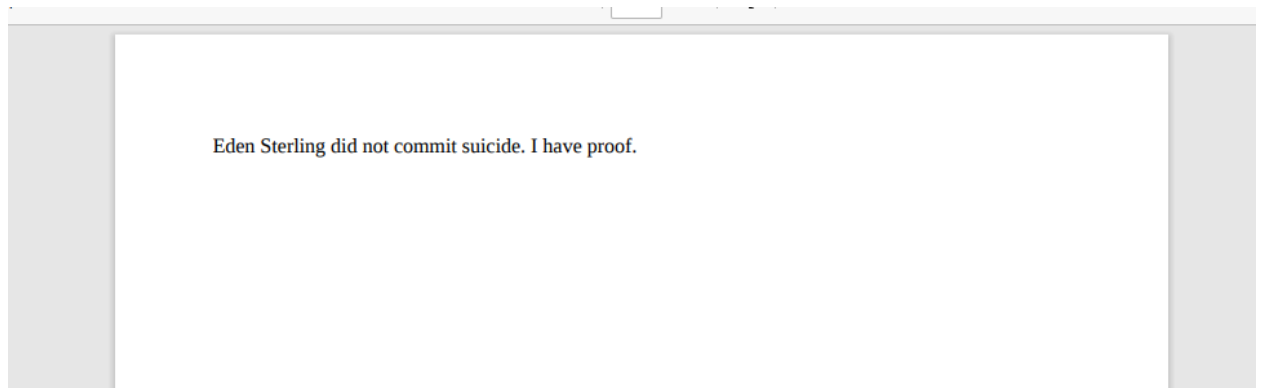
Ngay từ từ khóa đầu tiên với 'potassium', em đã tìm được thông tin là nạn nhân search dòng chữ “where can I buy potassium cyanide” trên mạng.

Vậy thì có thể kết luận được rằng là ban đầu người nạn nhân này đã thấy 1 quảng cáo về việc potassium cyanide giết người nhanh như thế nào, và sau đó nhờ vào thông tin ấy thì người này đã tìm kiếm để tìm ra nơi mua potassium cyanide để phục vụ cho mục đích muốn tự tử của mình.

Vì vậy kết luận tình nghi trước đó đã đúng.

**Câu 6:**

Sau khi mở file pdf đã cho, em chỉ nhận được dòng chữ như sau:



Không thể tìm gì được hơn, nên em nghĩ rằng đã có file ẩn nằm trong file pdf này (bởi mặc dù chỉ có 1 dòng chữ thôi nhưng file lại nặng tới gần 76mb), vì thế mà em sẽ tiến hành phân tích sâu hơn vào file pdf này thông qua công cụ trong kali linux:

```

nghianguyen@kali: ~/PhapChung/ThucHanh2
File Actions Edit View Help

(nghianguyen@kali)-[~/PhapChung/ThucHanh2]
$ exiftool kb06-session02.pdf
ExifTool Version Number      : 12.67
File Name                    : kb06-session02.pdf
Directory                    : .
File Size                     : 77 MB
File Modification Date/Time   : 2024:10:14 09:58:50+07:00
File Access Date/Time        : 2024:10:23 02:05:07+07:00
File Inode Change Date/Time   : 2024:10:23 02:05:07+07:00
File Permissions              : -rwxrw-rw-
File Type                     : PDF
File Type Extension           : pdf
MIME Type                     : application/pdf
PDF Version                   : 1.4
Linearized                    : No
Create Date                   : 2014:12:10 23:00:19-08:00
Author                        : A. M.
Creator                       : Writer
Producer                      : LibreOffice 4.2
Language                      : en-US
Page Count                    : 1

(nghianguyen@kali)-[~/PhapChung/ThucHanh2]
$ binwalk kb06-session02.pdf

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0             0x0            PDF document, version: "1.4"
147           0x93          Zlib compressed data, default compression
10606238      0xA1D69E      JB00T STAG header, image id: 2, timestamp 0x932212B9, image size: 1178501565 bytes, image JB00T checksum: 0x
3DE, header JB00T checksum: 0x4343
39724507      0x25E25DB     xz compressed data
39767781      0x25ECE5E5     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

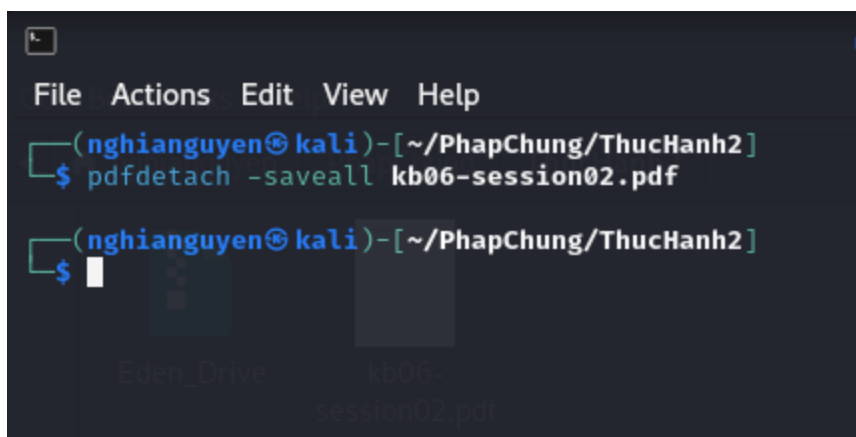
```

Chạy binwalk thì em thấy được có rất nhiều file nén chứa trong pdf, đặc biệt là định dạng nén xz và một số dữ liệu Zlib. Sau đó em chạy lại lệnh binwalk với option -e để extract các file nén này ra:

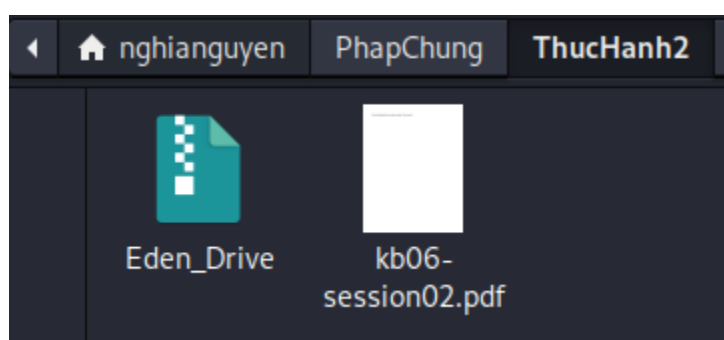
```
(nghianguyen@kali)-[~/PhapChung/ThucHanh2]
$ binwalk -e kb06-session02.pdf
```

DECIMAL	HEXADECIMAL	DESCRIPTION
147	0x93	Zlib compressed data, default compression
39724507	0x25E25DB	xz compressed data
39767781	0x25ECE5	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
40961161	0x2710489	xz compressed data
41004599	0x271AE37	xz compressed data
41046840	0x2725338	xz compressed data
41135276	0x273ACAC	xz compressed data
41151673	0x273ECB9	xz compressed data
41193670	0x27490C6	xz compressed data
41280298	0x275E32A	xz compressed data
41321656	0x27684B8	xz compressed data
41364898	0x2772DA2	xz compressed data
41451786	0x278810A	xz compressed data
41476074	0x278DFEA	xz compressed data
41518769	0x27986B1	xz compressed data
41606844	0x27ADEBC	xz compressed data

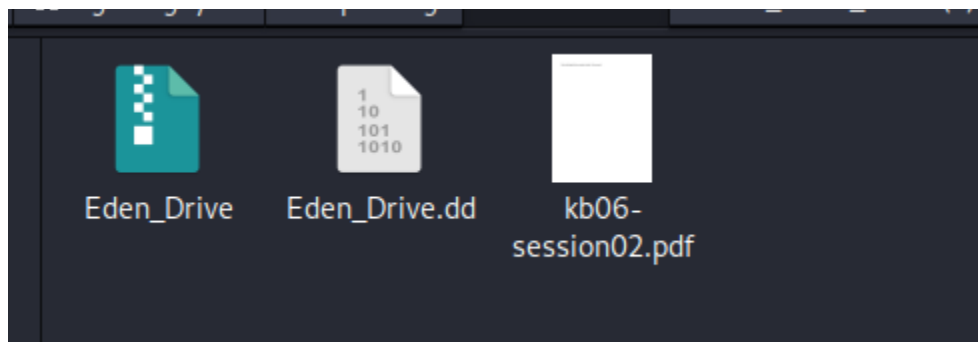
Cách này có vẻ không hiệu quả lắm, nên em đã sử dụng sang công cụ pdfdetach (thuộc gói Poppler-utils):



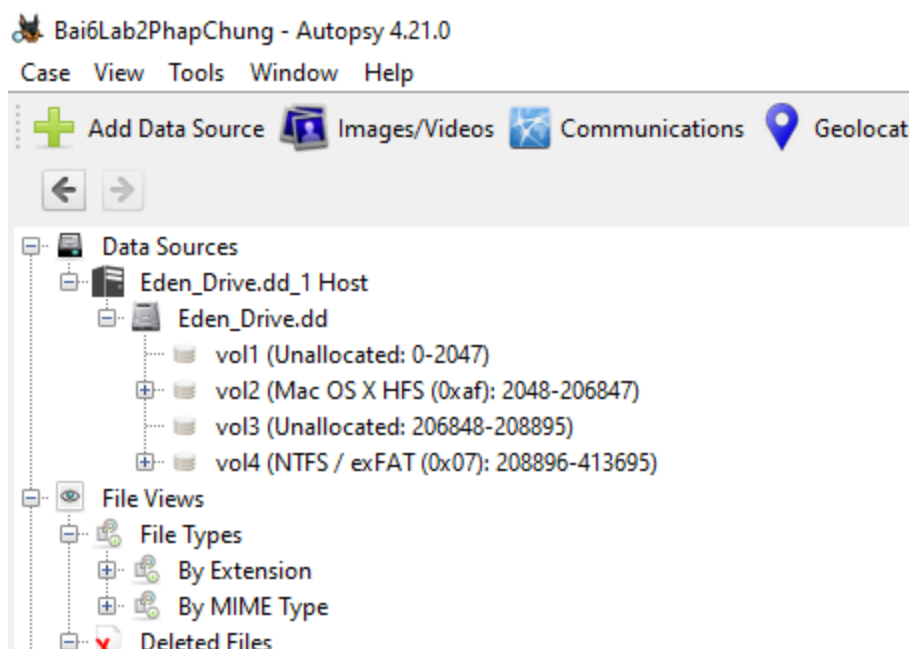
Kết quả nhận được:



Đây là 1 file zip tên Eden\_Drive, vậy đúng là thứ mà em đang cần tìm, tiếp theo em sẽ giải nén nó ra:

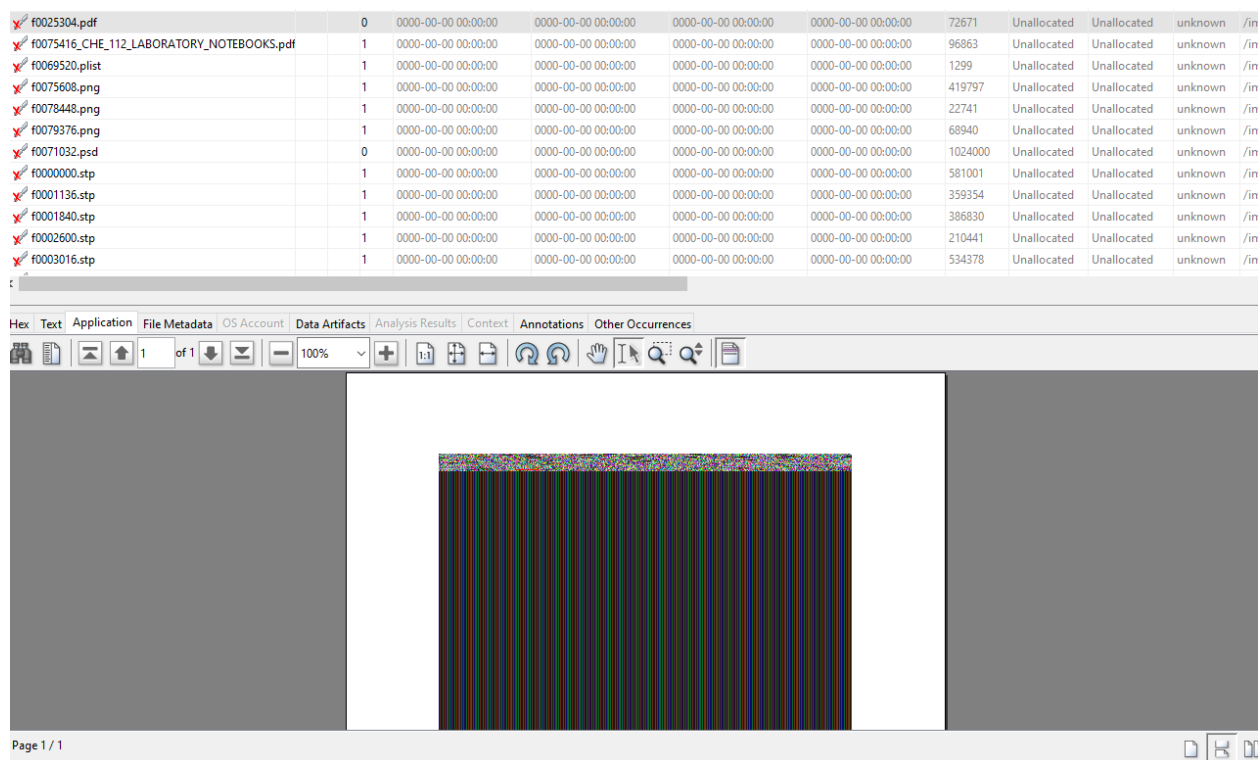


Giải nén xong thì nhận được file với đuôi .dd, đây là file đĩa, em sẽ lấy nó về máy chính và phân tích sâu hơn:



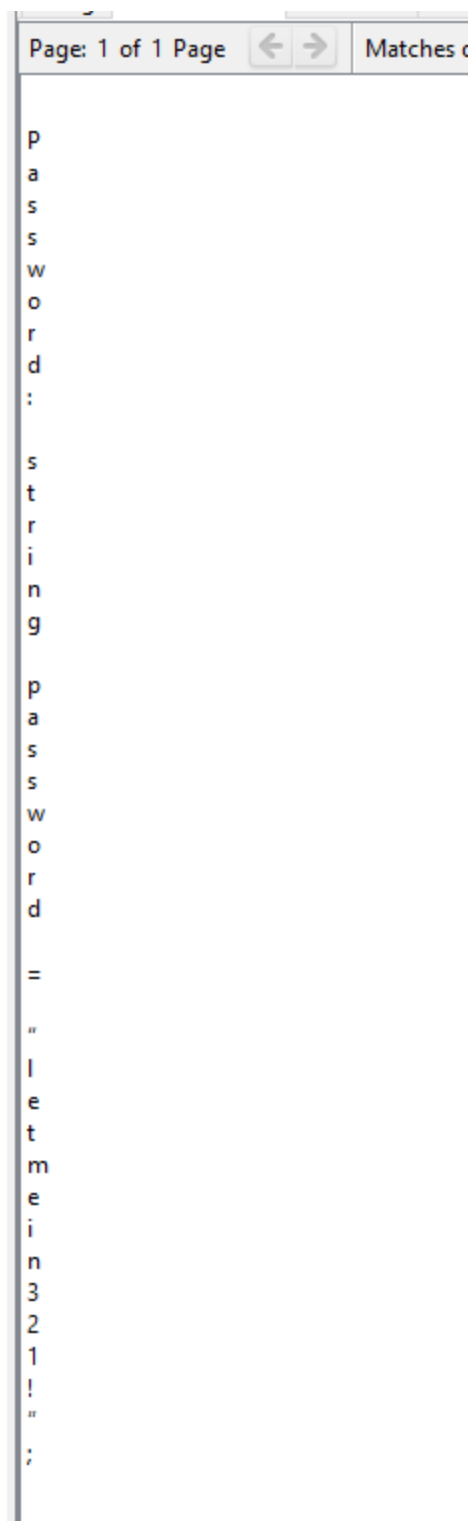
## Task1:

Vì đã có hint là 1 file pdf đã xóa, nên em sẽ vào mục Deleted Files để tìm kiếm:









Em thấy có dòng password như trên, nó khớp với lại hint thầy đã cho “(password: letme\*\*\*\*\*)”. Vì vậy pass tài khoản truyền thông xã hội của Eden chính là “letmein321!”;

Task2:

Vì đã có gợi ý là “Nancy”, nên em sẽ tiến hành search keyword này:

Keyword search 10 - Nancy x		
Keyword search		
Table	Thumbnail	Summary
Name	Keyword Preview	Location
9188107.ico	-----author: «nancy»content-type: appli	/img_Eden_Drive.dd/vol_vol
Unalloc_433_50847744_105902080	<rdf:li>«nancy»</rdf:li>	/img_Eden_Drive.dd/vol_vol
Metadata Artifact	2:50:53 ictowner : «nancy»date modified : 201	/img_Eden_Drive.dd/vol_vol
Metadata Artifact	2:50:53 ictowner : «nancy»date modified : 201	/img_Eden_Drive.dd/vol_vol
f0075416_CHE_112_LABORATORY_NOTEBOOKS.pdf	-----author: «nancy»content-type: appli	/img_Eden_Drive.dd/vol_vol

Em tìm được các file như trên, với author là Nancy:

Unalloc_433_50847744_105902080	<rdf:li>«nancy»</rdf:li>
Metadata Artifact	2:50:53 ictowner : «nancy»date modified
Metadata Artifact	2:50:53 ictowner : «nancy»date modified
f0075416_CHE_112_LABORATORY_NOTEBOOKS.pdf	-----author: «nancy»content-type:

<

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContext

StringsExtracted TextTranslation

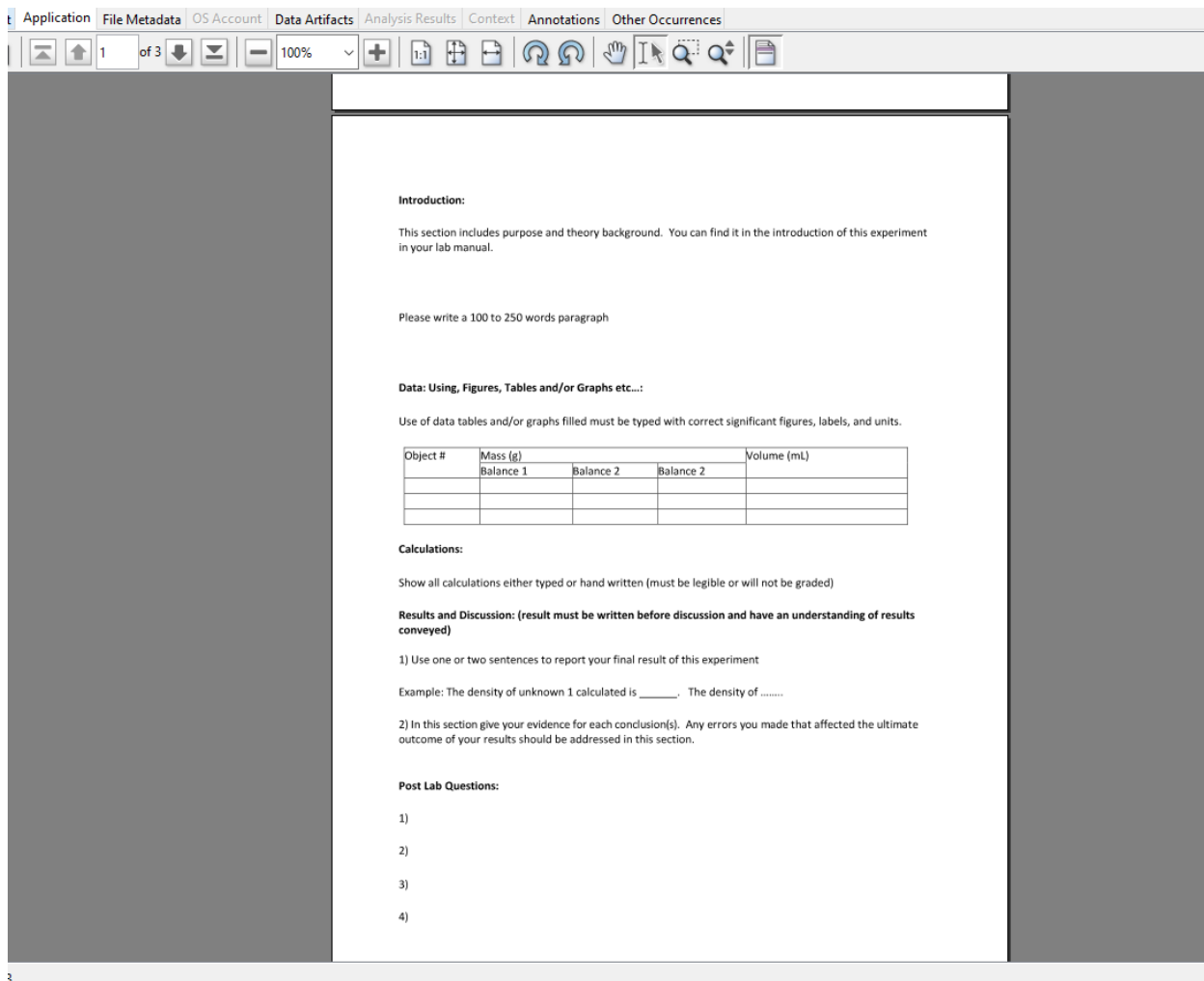
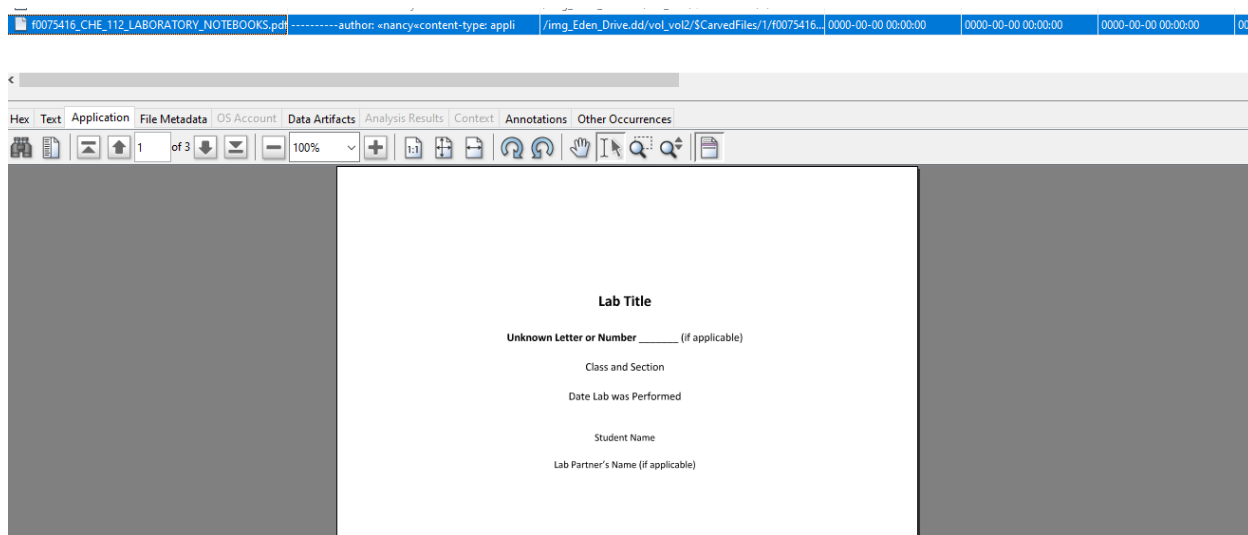
Page: 1 of 1 Page<=>Matches on page: 1 of 5 Match<=>100%🗨️🔍

Author: Nancy

Content-Type: application/pdf

Creation-Date: 2014-06-16T22:50:53Z

Nội dung file là:



Points per area	1	2	3	4
	Beginning or incomplete	Developing	Accomplished	Exemplary
Introduction	Very little background information provided or information is incorrect	Some introductory information, but still missing some major points	Introduction is nearly complete, missing some minor points	Introduction complete and well-written; provides all necessary background principles for the experiment
Data including Figures, Graphs, Tables, etc.	Figures, graphs, tables contain errors or are poorly constructed, have missing titles, captions or numbers, units missing or incorrect, etc.	Most figures, graphs, tables OK, some still missing some important or required features	All figures, graphs, tables are correctly drawn, but some have minor problems or could still be improved	All figures, graphs, tables are correctly drawn, are numbered and contain titles/captions.
Calculations	All or most of the calculations are either done incorrectly; little understanding of the mathematical concepts of the lab. No units or correct significant figures	Some of the calculations have been done properly; partial understanding of the mathematical concepts of the lab.	Almost all calculations are done properly and all calculations are given to the proper number of significant figures and units.	All calculations are done properly and results have the proper number of significant figures and units.
Discussion	Very incomplete or incorrect interpretation of trends and comparison of data indicating a lack of understanding of results	Some of the results have been correctly interpreted and discussed; partial but incomplete understanding of results is still evident	Almost all of the results have been correctly interpreted and discussed, only minor improvements are needed	All important trends and data comparisons have been interpreted correctly and discussed, good understanding of results is conveyed
Results and Discussion (result must be written before discussion)	Very incomplete or incorrect interpretation of trends and comparison of data indicating a lack of understanding of results	Some of the results have been correctly interpreted and discussed; partial but incomplete understanding of results is still evident	Almost all of the results have been correctly interpreted and discussed, only minor improvements are needed	All important trends and data comparisons have been interpreted correctly and discussed, good understanding of results is conveyed
Appearance and formatting	Sections out of order, too much handwritten copy, sloppy formatting	Sections in order, contains the minimum allowable amount of handwritten copy, formatting is rough but readable	All sections in order, formatting generally good but could still be improved	All sections in order, well-formatted, very readable

Nhìn vào thì có vẻ đây là một file lab mẫu để điền vào, liên quan đến một môn học khoa học (CHE 112). Nội dung của tệp này liên quan đến các thí nghiệm và hướng dẫn về cách ghi lại dữ liệu, xử lý tính toán, và trình bày kết quả thí nghiệm.

Vậy từ đây có thể kết luận rằng đây là tập tin có nội dung liên quan đến nơi Eden làm việc và học tập (f0075416\_CHE\_112\_LABORATORY\_NOTEBOOKS.pdf) và người viết nội dung trong đó chính là Nancy.

### Task 3:

Để tìm transaction, như trong gợi ý có đề cập, em tiến hành sử dụng Keyword Lists và tích vào mục Credit Card Numbers:

Đây là các kết quả trả về, em không biết phải dựa vào cột nào để xác định thời gian, có 2 cột em phân vân như sau:

Em sẽ sử dụng đại cột Created Time để làm thời gian, và em thấy có rất nhiều file có mốc thời gian tương đồng, nhưng mà cũ nhất sẽ là các file vào 2014-12-04 13:33:57 ICT :

Em cũng không thật sự biết đây có phải là 1 giao dịch không, khi mà nhìn vào file này thì nó có vẻ giống như các file sử dụng trong hệ thống CAD (Computer-Aided Design) để mô tả dữ liệu liên quan đến thiết kế sản phẩm.

Báo cáo môn học  
HOC KỲ I – NĂM HỌC 2024-2025

2929189.STEP	oint ('none', ( 5.461000000000002100, 2.2860000000000000... /img_Eden_Drive.dd/vol_vol4/my_cad/2929189.STEP	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	529
3214154.STEP	5345774306977500, 0.0154816347119433460=0, 0.0161... /img_Eden_Drive.dd/vol_vol4/my_cad/3214154.STEP	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	400
3242066.STEP	4875671926780300, 2.748690687499441200, 2.250000... /img_Eden_Drive.dd/vol_vol4/my_cad/3242066.STEP	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	172
3266025.STEP	oint ('none', ( 5.996446609406704400, 5.9964466094... /img_Eden_Drive.dd/vol_vol4/my_cad/3266025.STEP	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	229
3368181.STEP	3426311271131000, 4.420708734667987200, -3.525000... /img_Eden_Drive.dd/vol_vol4/my_cad/3368181.STEP	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	809
3381193.STEP	tesian_point", (-0.497592363336099, 2.040196519937... /img_Eden_Drive.dd/vol_vol4/my_cad/3381193.STEP	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	562
3420797.STEP	int ('none', ( -5.218629150101522300, 6.200000000000... /img_Eden_Drive.dd/vol_vol4/my_cad/3420797.STEP	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	347

<

>

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 1 of 8    Result    < >									
Accounts									
Type	Value							Source(s)	
Account Type	CREDIT_CARD							Keyword Search	
ID	461000000000002100							Keyword Search	
Keyword	461000000000002100							KeywordSearch	
Card Number	461000000000002100							KeywordSearch	
Card Scheme	visa							Keyword Search	
Card Type	credit							Keyword Search	
Bank Name	SIMMONS FIRST NATIONAL BANK							Keyword Search	
Phone Number	8002722102							Keyword Search	
Country	US							Keyword Search	
Set Name	Credit Card Numbers							Keyword Search	
Keyword Preview	oint ('none', ( 5.461000000000002100, 2.2860000000000000... /img_Eden_Drive.dd/vol_vol4/my_cad/2929189.STEP							Keyword Search	
Keyword Search Type	2							Keyword Search	
Source File Path	/img_Eden_Drive.dd/vol_vol4/my_cad/2929189.STEP								
Artifact ID	-9223372036854766917								

Nó có thời gian khởi tạo là 2014-12-04 13:39:34 ICT.

Em nghĩ rằng thời gian đó là thời gian cho giao dịch cũ nhất.

#### Task 4:

Ở task 3, trong lúc tìm kiếm giao dịch cũ nhất thì em cũng đã tìm thấy thông tin của 1 tài khoản ngân hàng:

2929189.STEP

oint ('none', ( 5.461000000000002100, 2.2860000000000000... /img\_Eden\_Drive.dd/vol\_vol4/my\_cad/2929189.STEP

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

529

<

>

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Result: 1 of 8

Result

Accounts

Type	Value	Source(s)
Account Type	CREDIT_CARD	Keyword Search
ID	461000000000002100	Keyword Search
Keyword	461000000000002100	KeywordSearch
Card Number	461000000000002100	KeywordSearch
Card Scheme	visa	Keyword Search
Card Type	credit	Keyword Search
Bank Name	SIMMONS FIRST NATIONAL BANK	Keyword Search
Phone Number	8002722102	Keyword Search
Country	US	Keyword Search
Set Name	Credit Card Numbers	Keyword Search
Keyword Preview	oint ('none', ( 5.461000000000002100, 2.2860000000000000... /img_Eden_Drive.dd/vol_vol4/my_cad/2929189.STEP	Keyword Search
Keyword Search Type	2	Keyword Search
Source File Path	/img_Eden_Drive.dd/vol_vol4/my_cad/2929189.STEP	
Artifact ID	-9223372036854766917	

#### Task 5:







Để tìm file secret.txt thì em đã search keyword với từ “secret”, nhận được các kết quả như sau:

Listing

Keyword search 26 - secret X

Keyword search

TableThumbnailSummary

Name	Keyword Preview	Location	Modified Time	Change Time
 \$LogFile	secret~1.docfile0«secret.docx0«secret~1.doc(8'8@	/img_Eden_Drive.dd/vol_vol4/\$LogFile	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT
 \$MFT	file0844930file0«secret.docx0«secret~1.docsecret	/img_Eden_Drive.dd/vol_vol4/\$MFT	2014-11-28 03:51:26 ICT	2014-11-28 03:51:26 ICT
 secret.docx	«secret.docx«	/img_Eden_Drive.dd/vol_vol4/secret.docx	2014-12-04 13:40:32 ICT	2014-12-04 13:40:32 ICT
 secret.docx-slack	«secret.docx«-slac	/img_Eden_Drive.dd/vol_vol4/secret.docx-slack	2014-12-04 13:40:32 ICT	2014-12-04 13:40:32 ICT
 secret.docx:secret.txt	«secret.docx«:secret.tx	/img_Eden_Drive.dd/vol_vol4/secret.docx:secret.txt	2014-12-04 13:40:32 ICT	2014-12-04 13:40:32 ICT
 4443268.userprefs	¿te puedo decir el «secreto» a ti? _____	/img_Eden_Drive.dd/vol_vol4/my_stuff/4443268.userp...	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT

Em thấy có 1 file tên là secret.docx:secret.txt, nhấn vào xem file:

secret.docx:secret.txt	«secret.docx«:secret.tx	/img_Eden_Drive.dd/vol_vol4/secret.docx:secret.txt	2014-
4443268.userprefs	¿te puedo decir el «secreto» a ti? _____	/img_Eden_Drive.dd/vol_vol4/my_stuff/4443268.userp...	2014-

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 2 Match

100%

Reset

secret.docx:secret.txt, I think someone may be after me. - Eden

-----METADATA-----]

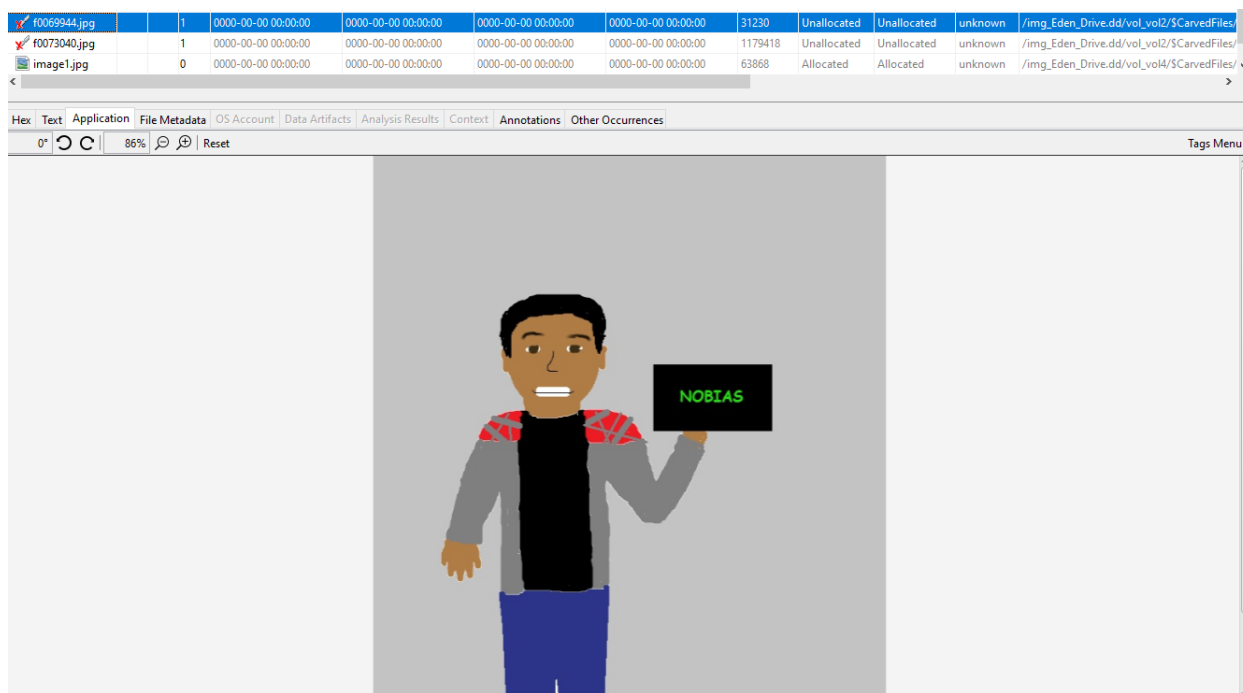
Vậy nội dung mà Eden để lại chính là “I think someone may be after me. – Eden”.

#### Task 6:

Để tìm hình thì em vào mục File Views -> File Types -> By Extension -> Images.

Sau khi xem qua các ảnh thì em có thấy một ảnh như này:





Nó có chữ Nobias, thế nên em nghĩ đây chính là ảnh mà đề bài yêu cầu cần tìm.

### CTF Dear Diary:

Tải file mà chall cho về và giải nén:

```
(kali@kali)~[/Downloads]
$ wget https://artifacts.picoctf.net/c_titan/63/disk.flag.img.gz
--2024-10-24 02:52:09-- https://artifacts.picoctf.net/c_titan/63/disk.flag.img.gz
Resolving artifacts.picoctf.net (artifacts.picoctf.net) ... 13.225.4.125, 13.225.4.99, 13.225.4.126, ...
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|13.225.4.125|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68353329 (65M) [application/octet-stream]
Saving to: 'disk.flag.img.gz'

disk.flag.img.gz      100%[=====] 65.19M  1.42MB/s  in 47s
2024-10-24 02:52:57 (1.40 MB/s) - 'disk.flag.img.gz' saved [68353329/68353329]

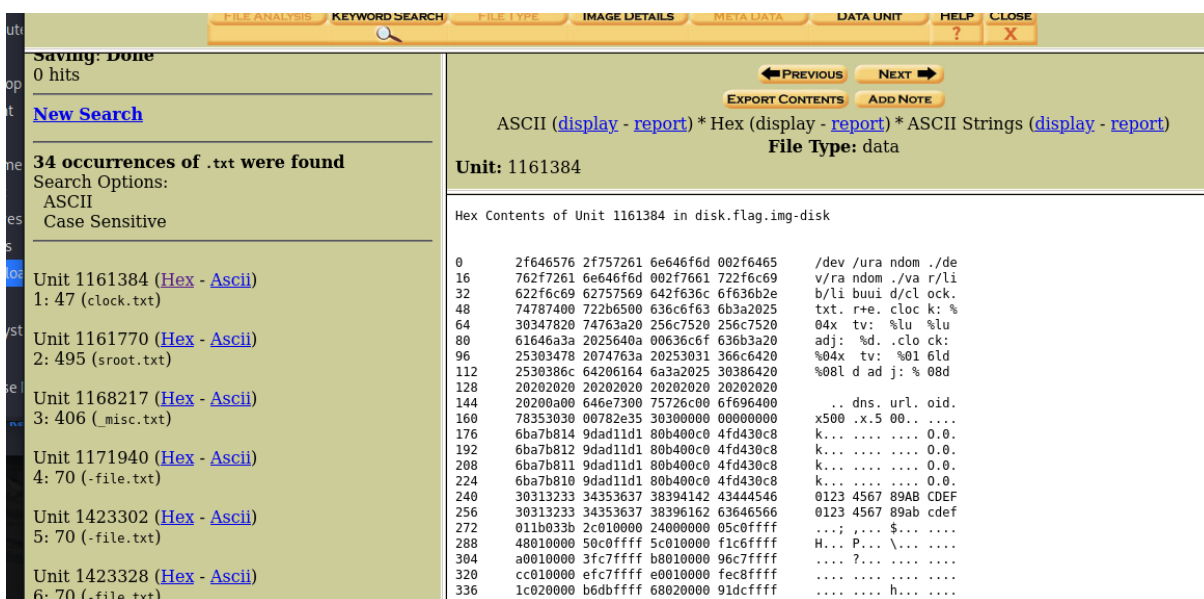
(kali@kali)~[/Downloads]
$ gunzip -d disk.flag.img.gz

(kali@kali)~[/Downloads]
$
```

Ta sẽ dùng autopsy được cho cùng trên distro kali 2024 để làm. Sau khi cho file vào phân tích, ta sẽ tìm các file .txt để xem có flag không.



Ta tìm được rất nhiều file txt nhưng không có file nào có vẻ chứa hay nói về flag.



Tuy nhiên, sau khi kiểm tra các file -file.txt, ta có thể thấy các mảnh nhỏ của flag trong từng file, ví dụ như chữ pic này là một mảnh của picoCTF {}, là định dạng flag của picoCTF.

```

Unit 1171940 (Hex - Ascii)
4: 70 (-file.txt)

Unit 1423302 (Hex - Ascii)
5: 70 (-file.txt)

Unit 1423328 (Hex - Ascii)
6: 70 (-file.txt)

Unit 1423344 (Hex - Ascii)
7: 70 (-file.txt)

```

Hex Contents of Unit 1423344 in disk.flag.img-disk

0	32070000	0c000102	2e000000	cc000000	2...
16	0c000202	2e2e0000	33070000	18000d01	...
32	666f7263	652d7761	69742e73	68000000	forc e-wa it.s h...
48	34070000	38001201	696e6e6f	63756f75	4... 8... inno cuou
64	732d6669	6c652e74	78740000	00000000	s-fi le.t xt.. ....
80	00000000	00000000	00000000	00000000	...
96	00000000	00000000	35070000	8c030301	... 5... .....
112	70696300	00000000	00000000	00000000	pic. .... .....
128	00000000	00000000	00000000	00000000	...
144	00000000	00000000	00000000	00000000	...
160	00000000	00000000	00000000	00000000	...

Thật vậy, ở file tiếp theo ta có thể tìm được phần còn lại là Oct. Cứ như vậy, ta tìm hết các mảnh flag rồi ghép lại với nhau.

```

Unit 1423328 (Hex - Ascii)
6: 70 (-file.txt)

Unit 1423344 (Hex - Ascii)
7: 70 (-file.txt)

Unit 1423356 (Hex - Ascii)
8: 70 (-file.txt)

```

Hex Contents of Unit 1423356 in disk.flag.img-disk

0	32070000	0c000102	2e000000	cc000000	2...
16	0c000202	2e2e0000	33070000	18000d01	...
32	666f7263	652d7761	69742e73	68000000	forc e-wa it.s h...
48	34070000	1c001201	696e6e6f	63756f75	4... inno cuou
64	732d6669	6c652e74	78740000	35070000	s-fi le.t xt.. 5...
80	a8030301	6f435400	00000000	00000000	... oCT. .... .....
96	00000000	00000000	00000000	00000000	...
112	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	...

```

Unit 1423328 (Hex - Ascii)
6: 70 (-file.txt)

Unit 1423344 (Hex - Ascii)
7: 70 (-file.txt)

Unit 1423356 (Hex - Ascii)
8: 70 (-file.txt)

Unit 1423374 (Hex - Ascii)
9: 70 (-file.txt)

```

Hex Contents of Unit 1423374 in disk.flag.img-disk

0	32070000	0c000102	2e000000	cc000000	2...
16	0c000202	2e2e0000	33070000	18000d01	...
32	666f7263	652d7761	69742e73	68000000	forc e-wa it.s h...
48	34070000	28001201	696e6e6f	63756f75	4... inno cuou
64	732d6669	6c652e74	78740000	00000000	s-fi le.t xt.. ....
80	00000000	00000000	35070000	9c030301	... 5... .....
96	467b3100	00000000	00000000	00000000	F{1. .... .....
112	00000000	00000000	00000000	00000000	...
128	00000000	00000000	00000000	00000000	...
144	00000000	00000000	00000000	00000000	...
160	00000000	00000000	00000000	00000000	...
176	00000000	00000000	00000000	00000000	...

```

Unit 1423392 (Hex - Ascii)
10: 70 (-file.txt)

Unit 1423410 (Hex - Ascii)
11: 70 (-file.txt)

Unit 1423422 (Hex - Ascii)
12: 70 (-file.txt)

```

Hex Contents of Unit 1423392 in disk.flag.img-disk

0	32070000	0c000102	2e000000	cc000000	2...
16	0c000202	2e2e0000	33070000	18000d01	...
32	666f7263	652d7761	69742e73	68000000	forc e-wa it.s h...
48	34070000	1c001201	696e6e6f	63756f75	4... inno cuou
64	732d6669	6c652e74	78740000	35070000	s-fi le.t xt.. 5...
80	a8030301	5f353300	00000000	00000000	... _53. .... .....
96	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	...

```

Unit 1423410 (Hex - Ascii)
11: 70 (-file.txt)

Unit 1423422 (Hex - Ascii)
12: 70 (-file.txt)

```

Hex Contents of Unit 1423410 in disk.flag.img-disk

0	32070000	0c000102	2e000000	cc000000	2...
16	0c000202	2e2e0000	33070000	18000d01	...
32	666f7263	652d7761	69742e73	68000000	forc e-wa it.s h...
48	34070000	28001201	696e6e6f	63756f75	4... inno cuou
64	732d6669	6c652e74	78740000	00000000	s-fi le.t xt.. ....
80	00000000	00000000	35070000	9c030301	... 5... .....
96	335f6e00	00000000	00000000	00000000	3_n. .... .....
112	00000000	00000000	00000000	00000000	...
128	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	...

```

Unit 1423410 (Hex - Ascii)
11: 70 (-file.txt)

Unit 1423422 (Hex - Ascii)
12: 70 (-file.txt)

```

Hex Contents of Unit 1423422 in disk.flag.img-disk

0	32070000	0c000102	2e000000	cc000000	2...
16	0c000202	2e2e0000	33070000	18000d01	...
32	666f7263	652d7761	69742e73	68000000	forc e-wa it.s h...
48	34070000	1c001201	696e6e6f	63756f75	4... inno cuou
64	732d6669	6c652e74	78740000	35070000	s-fi le.t xt.. 5...
80	a8030301	346d3300	00000000	00000000	... 4m3. .... .....
96	00000000	00000000	00000000	00000000	...
112	00000000	00000000	00000000	00000000	...
128	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	...

```

Unit 1423410 (Hex - Ascii)
11: 70 (-file.txt)
Unit 1423422 (Hex - Ascii)
12: 70 (-file.txt)
Unit 1423440 (Hex - Ascii)
13: 70 (-file.txt)

```

16	00000202	2e2e0000	33070000	18000001	....	....	3...	....
32	666f7263	652d7761	69742e73	68000000	forc	e-wa	it.s	h...
48	34070000	28001201	696e6e6f	63756f75	4...	(...	inno	cuou
64	732d6669	6c652e74	78740000	00000000	s-fi	le.t	xt..	....
80	00000000	00000000	35070000	9c030301	....	....	5...	....
96	355f3800	00000000	00000000	00000000	5_8.	....	....	....
112	00000000	00000000	00000000	00000000	....	....	....	....
128	00000000	00000000	00000000	00000000	....	....	....	....
144	00000000	00000000	00000000	00000000	....	....	....	....
160	00000000	00000000	00000000	00000000	....	....	....	....

```

Unit 1423440 (Hex - Ascii)
13: 70 (-file.txt)
Unit 1423452 (Hex - Ascii)
14: 70 (-file.txt)
Unit 1423470 (Hex - Ascii)
15: 70 (-file.txt)

```

0	32070000	0c000102	2e000000	cc000000	2...	....	....	....
16	0c000202	2e2e0000	33070000	18000d01	....	....	3...	....
32	666f7263	652d7761	69742e73	68000000	forc	e-wa	it.s	h...
48	34070000	1c001201	696e6e6f	63756f75	4...	(...	inno	cuou
64	732d6669	6c652e74	78740000	35070000	s-fi	le.t	xt..	5...
80	a8030301	30643200	00000000	00000000	....	0d2.	....	....
96	00000000	00000000	00000000	00000000	....	....	....	....
112	00000000	00000000	00000000	00000000	....	....	....	....
128	00000000	00000000	00000000	00000000	....	....	....	....
144	00000000	00000000	00000000	00000000	....	....	....	....

```

Unit 1423452 (Hex - Ascii)
14: 70 (-file.txt)
Unit 1423470 (Hex - Ascii)
15: 70 (-file.txt)
Unit 1423488 (Hex - Ascii)
16: 70 (-file.txt)

```

HEX CONTENTS OF UNIT 1423470 IN DISK:flag.img-1423470

0	32070000	0c000102	2e000000	cc000000	2...	....	....	....
16	0c000202	2e2e0000	33070000	18000d01	....	....	3...	....
32	666f7263	652d7761	69742e73	68000000	forc	e-wa	it.s	h...
48	34070000	28001201	696e6e6f	63756f75	4...	(...	inno	cuou
64	732d6669	6c652e74	78740000	00000000	s-fi	le.t	xt..	....
80	00000000	00000000	35070000	9c030301	....	....	5...	....
96	34623300	00000000	00000000	00000000	4b3.	....	....	....
112	00000000	00000000	00000000	00000000	....	....	....	....

```

Unit 1423488 (Hex - Ascii)
16: 70 (-file.txt)
Unit 1423500 (Hex - Ascii)
17: 70 (-file.txt)

```

32	666f7263	652d7761	69742e73	68000000	forc	e-wa	it.s	h...
48	34070000	1c001201	696e6e6f	63756f75	4...	(...	inno	cuou
64	732d6669	6c652e74	78740000	35070000	s-fi	le.t	xt..	5...
80	a8030301	307d0000	00000000	00000000	....	0}	....	....
96	00000000	00000000	00000000	00000000	....	....	....	....
112	00000000	00000000	00000000	00000000	....	....	....	....
128	00000000	00000000	00000000	00000000	....	....	....	....

Từ các mảnh nhỏ ta thu được flag của chall là: picoCTF{1\_533\_n4m35\_80d24b30}

## Description

If you can find the flag on this disk image, we can close the case for good!

Download the disk image [here](#).

1.602 users solved



52%

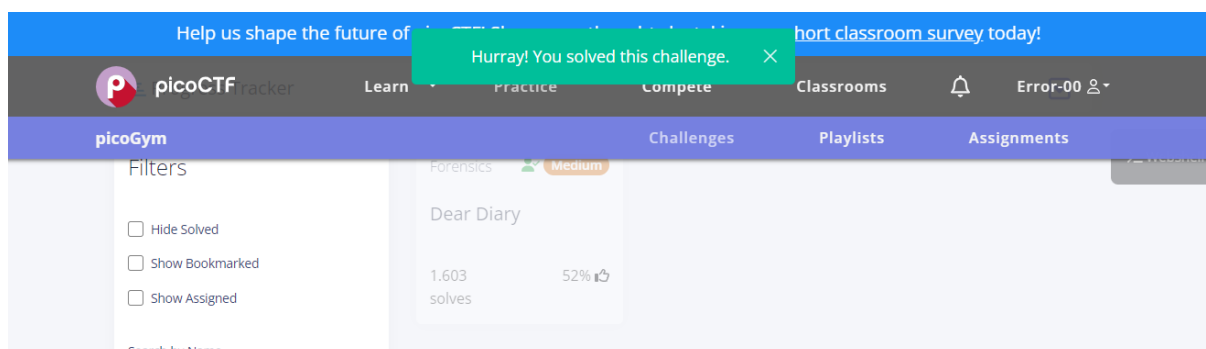
Liked



picoCTF{1\_533\_n4m35\_80d24b30}

Submit  
Flag

Ta nhập flag vào và đó là flag đúng



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

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).
- Ví dụ: [NT101.K11.ANTT]-Exe01\_Group03.*
- 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 nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

### Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

**HẾT**