

# 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.ANTT.1

STT	Họ và tên	MSSV	Email
1	Lê Huy Hiệp	21522067	<a href="mailto:21522067@gm.uit.edu.vn">21522067@gm.uit.edu.vn</a>
2	Nguyễn Trần Duy Anh	20520393	<a href="mailto:20520393@gm.uit.edu.vn">20520393@gm.uit.edu.vn</a>

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 1 (đã nộp trên lớp)	100%
2	Kịch bản 2 (đã nộp trên lớp)	100%
3	Kịch bản 3	100%
4	Kịch bản 4	100%
5	Kịch bản 5	100%
6	Kịch bản 6	100%
7	Encrypted Disk	100%
8	Timestomp	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

### Mục lục

Kịch bản 03 .....	3
Kịch bản 04: .....	18
Kịch bản 05 .....	20
Kịch bản 06 .....	21
Encrypted Disk: .....	33
Timestomp .....	37
<b>YÊU CẦU CHUNG.....</b>	<b>44</b>

## BÁO CÁO CHI TIẾT

Kịch bản 03. Thực hiện phân tích theo kịch bản mô tả sau:

- Trên máy tính/máy ảo windows thực hiện tải về hình ảnh và đặt tên ConDao-island.

Liên kết tải: <https://unsplash.com/photos/uXPBXlruX5o>

- Thực hiện xóa file ảnh vừa tạo, xóa trong Recycle Bin.

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

- Case Number: April\_0001

- Evidence Number: 01

- Unique Description: Monkey Image

- Examiner: Your Name (tên của nhóm)

- Tạo một thư mục điều tra dùng cho kịch bản này: KB03, chứa ảnh đĩa đã tạo.

- Thực hiện điều tra, tìm ảnh đã bị xóa trên ổ đĩa bằng công cụ FTK Imager. Sử dụng tính năng phục hồi file ảnh đã bị xóa (tính năng Export Files), lưu trữ file này trong thư mục KB03\images.

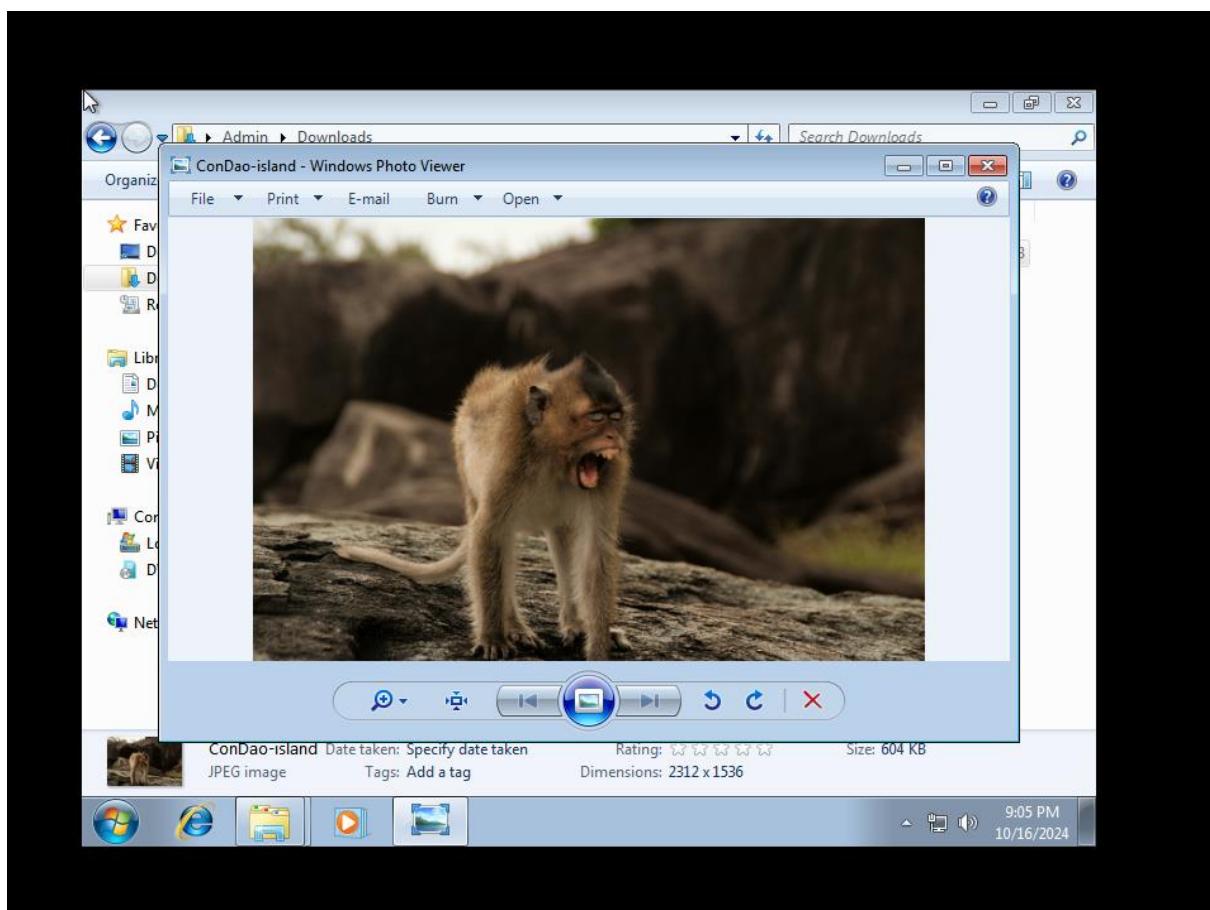
- Kiểm tra giá trị hash MD5 của file ảnh vừa được phục hồi với file gốc ban đầu. Yêu cầu: Các nhóm thực hiện chụp màn hình terminal sau khi hoàn thành điều tra bằng cách gõ các câu lệnh sau:

```
dir D:\KB03 | findstr "ConDao-island"
```

```
date /t
```

```
echo "Tên nhóm"
```

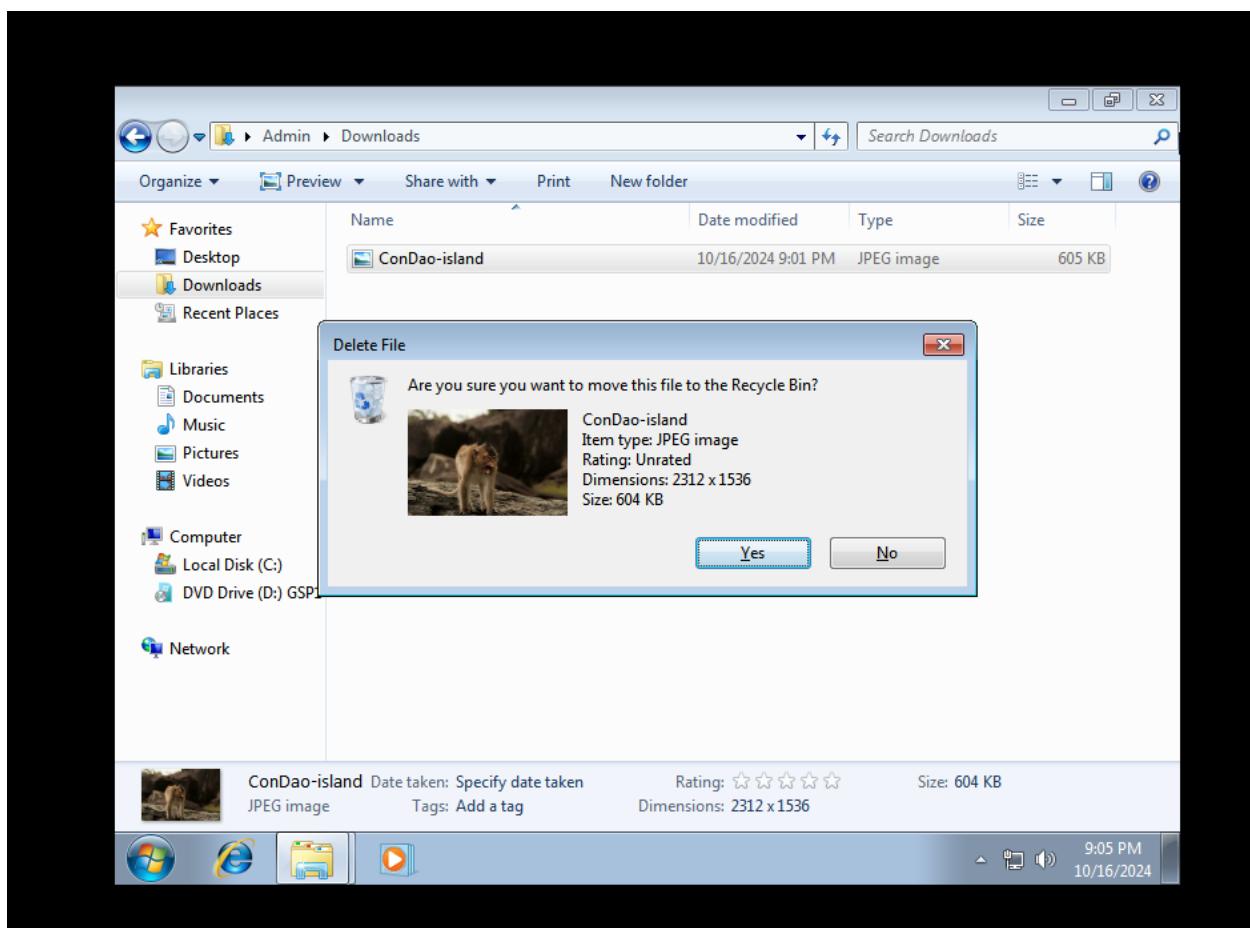
Tải file về sau đó đổi tên thành “ConDao-island”



Xóa file;

## Lab 2: Hard Drive Forensics

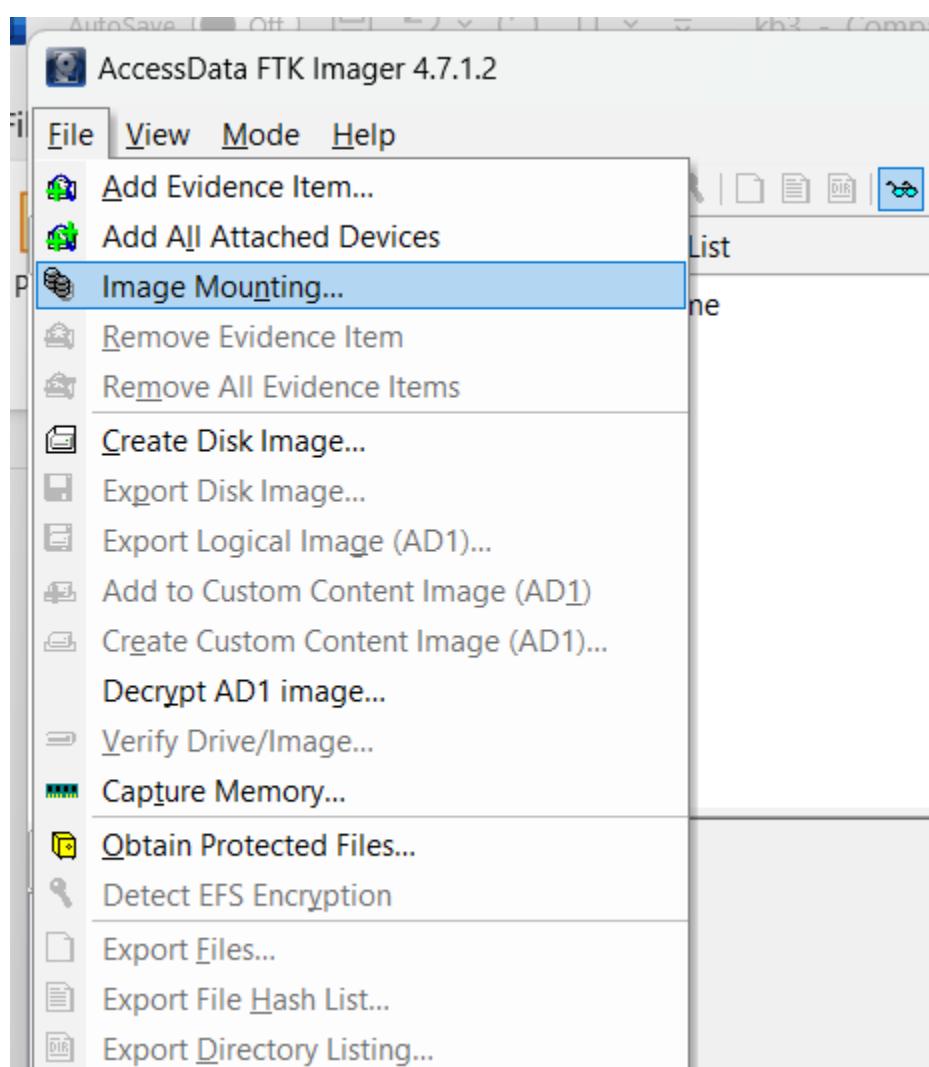
5



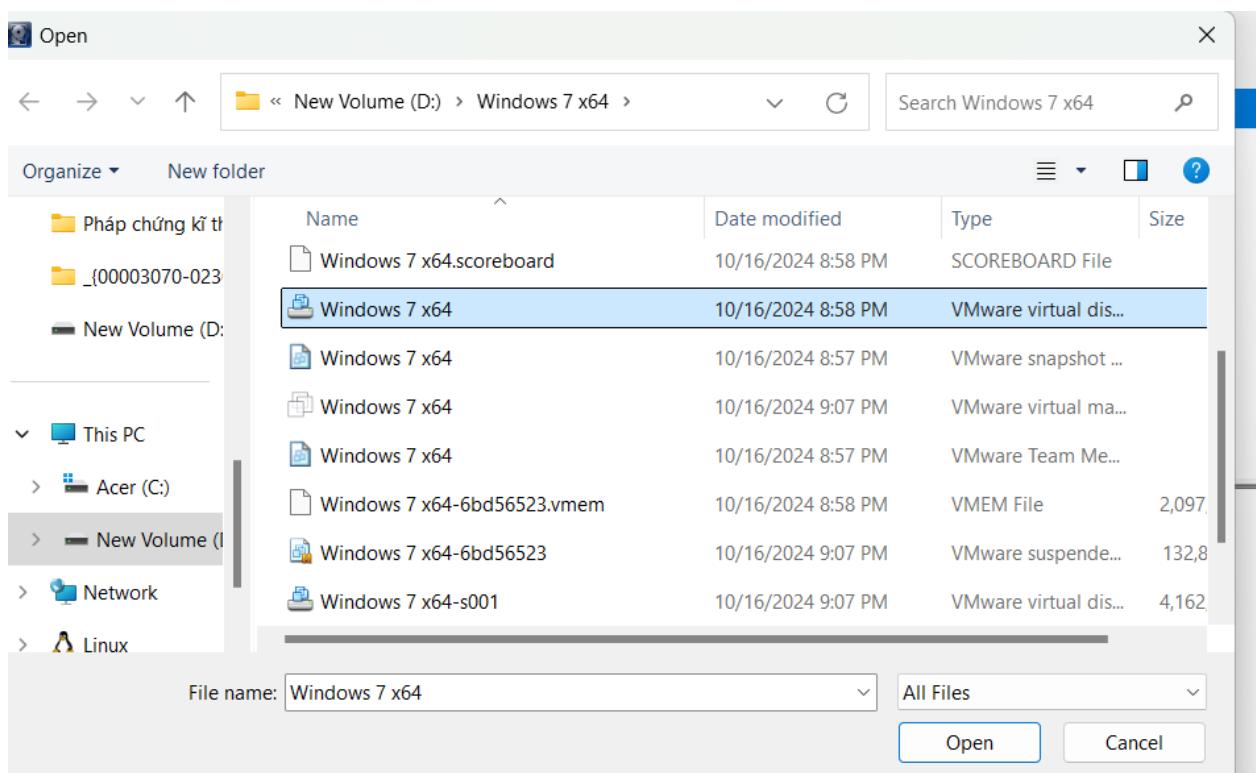
Gắn (mounting) file ảnh của ổ đĩa (disk images) vào máy tính phân tích:

## Lab 2: Hard Drive Forensics

6



## Lab 2: Hard Drive Forensics



Sau khi mount xong;

## Lab 2: Hard Drive Forensics



Mount Image To Drive

Add Image

Image: D:\Windows 7 x64\Windows 7 x64.vmdk

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder: D:\Windows 7 x64

Mount

Mapped Image List

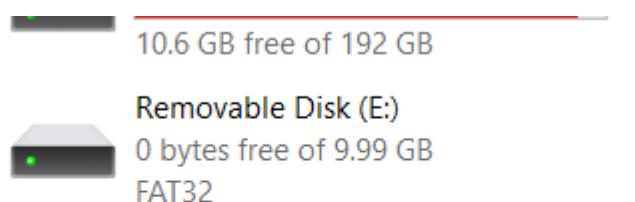
Mapped

Drive	Method	Partition	Image
PhysicalDrive1	Block Device/Re...	Image	D:\Windows 7 x64\Windows 7 x64.vmdk
E:	File System/Rea...	Partition 1 [10...]	D:\Windows 7 x64\Windows 7 x64.vmdk

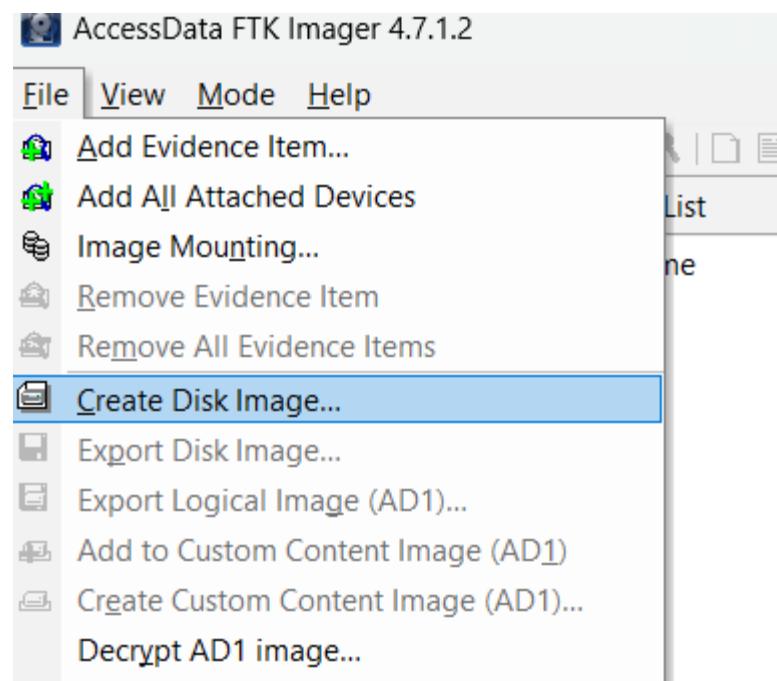
Unmount

Close

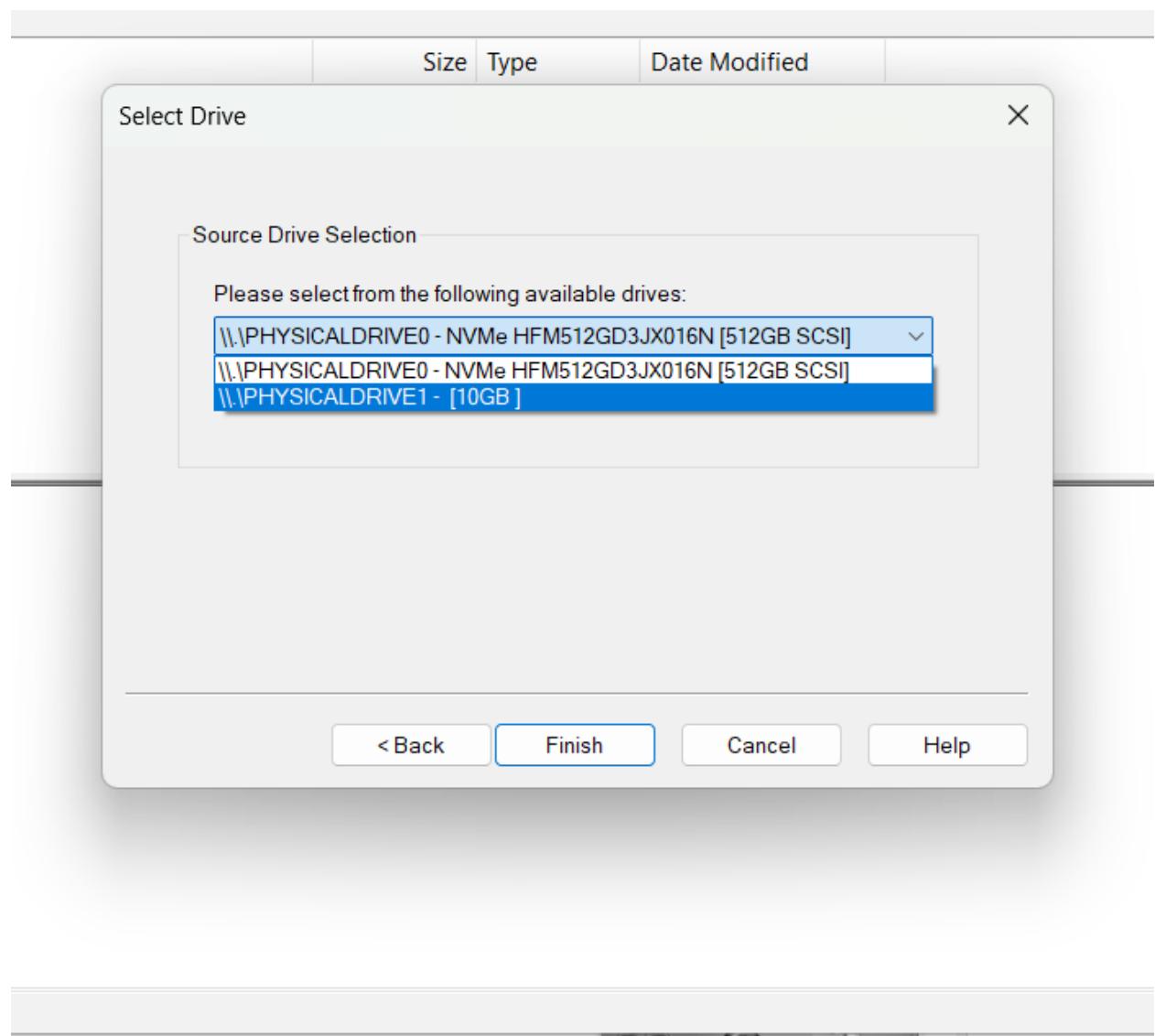
Lúc này tại This PC:



Thực hiện tạo ảnh đĩa:



Chọn PHYSICALDRIVE1 chính là ổ E



Nhập thông tin

Evidence Item Information X

Case Number:	April_0001
Evidence Number:	01
Unique Description:	Monkey Image
Examiner:	N03
Notes:	

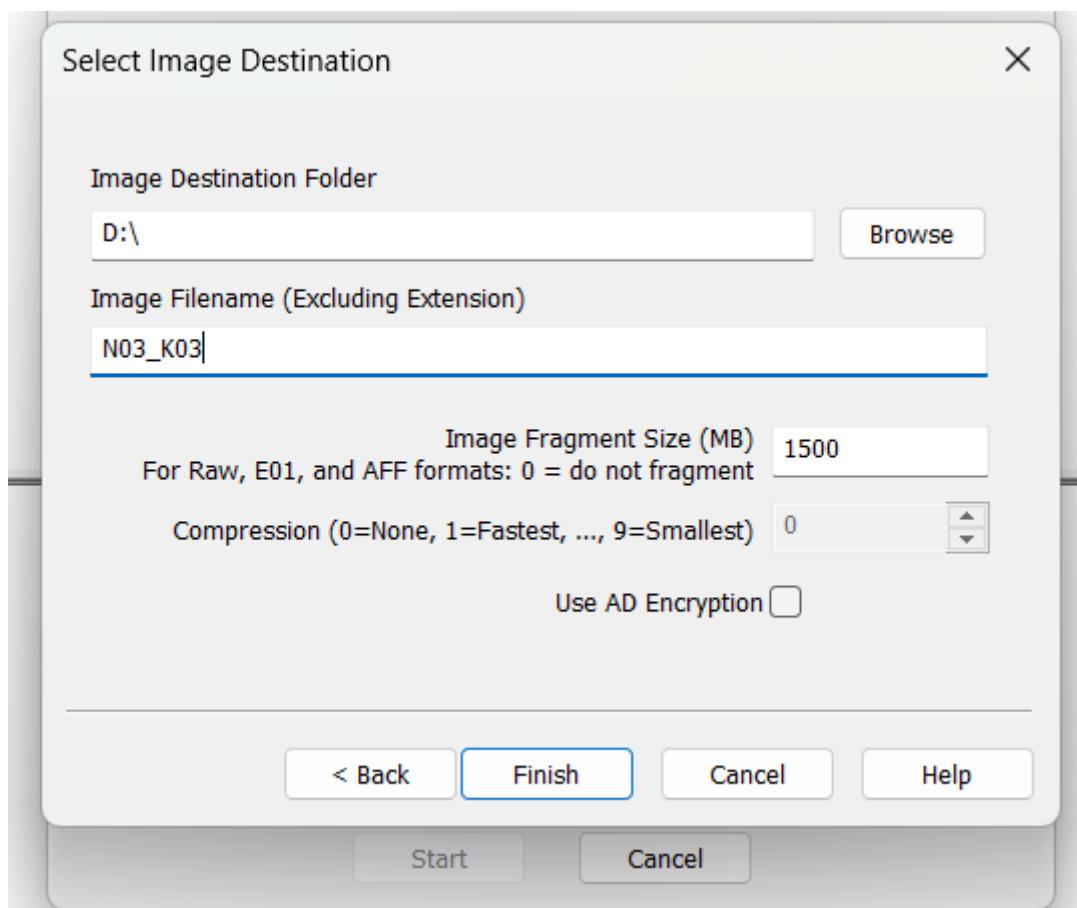
[< Back](#) [Next >](#) [Cancel](#) [Help](#)

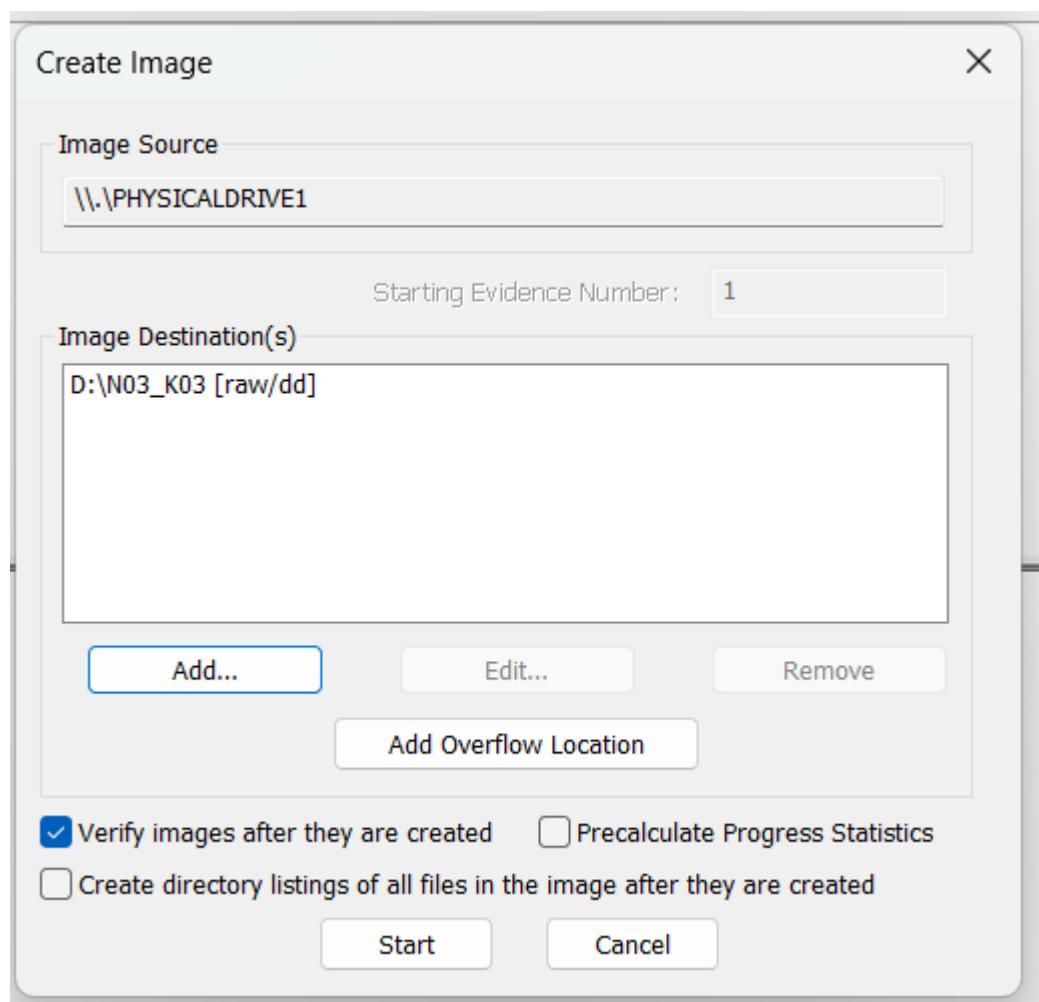
[Start](#) [Cancel](#)

Chọn đích để lưu image:

## Lab 2: Hard Drive Forensics

12 |

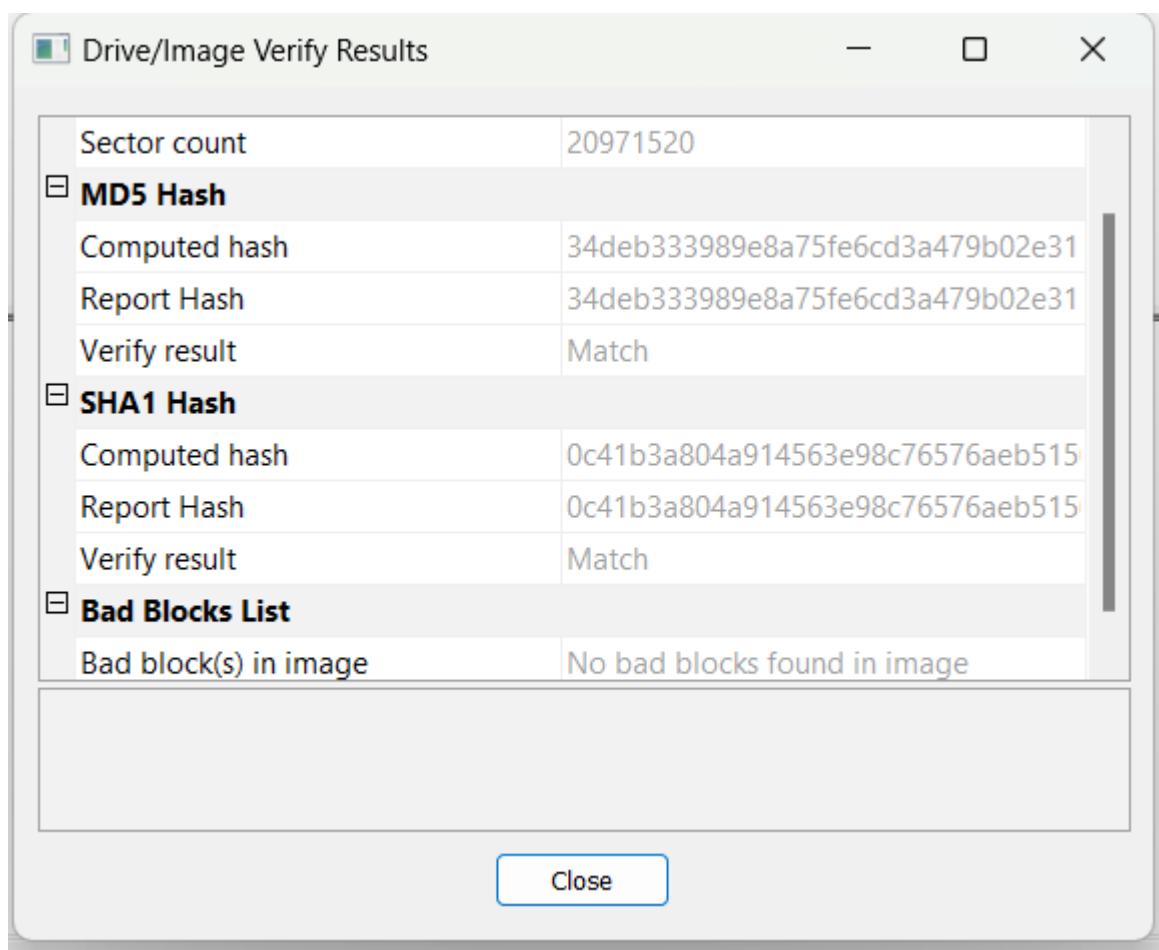




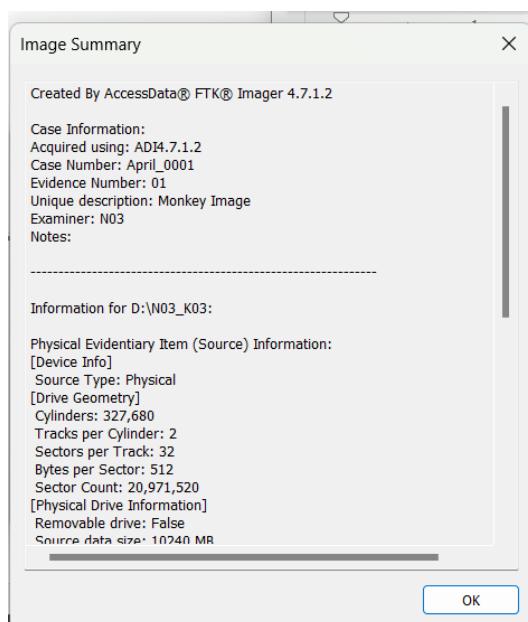
Sau khi tạo xong:

## Lab 2: Hard Drive Forensics

14



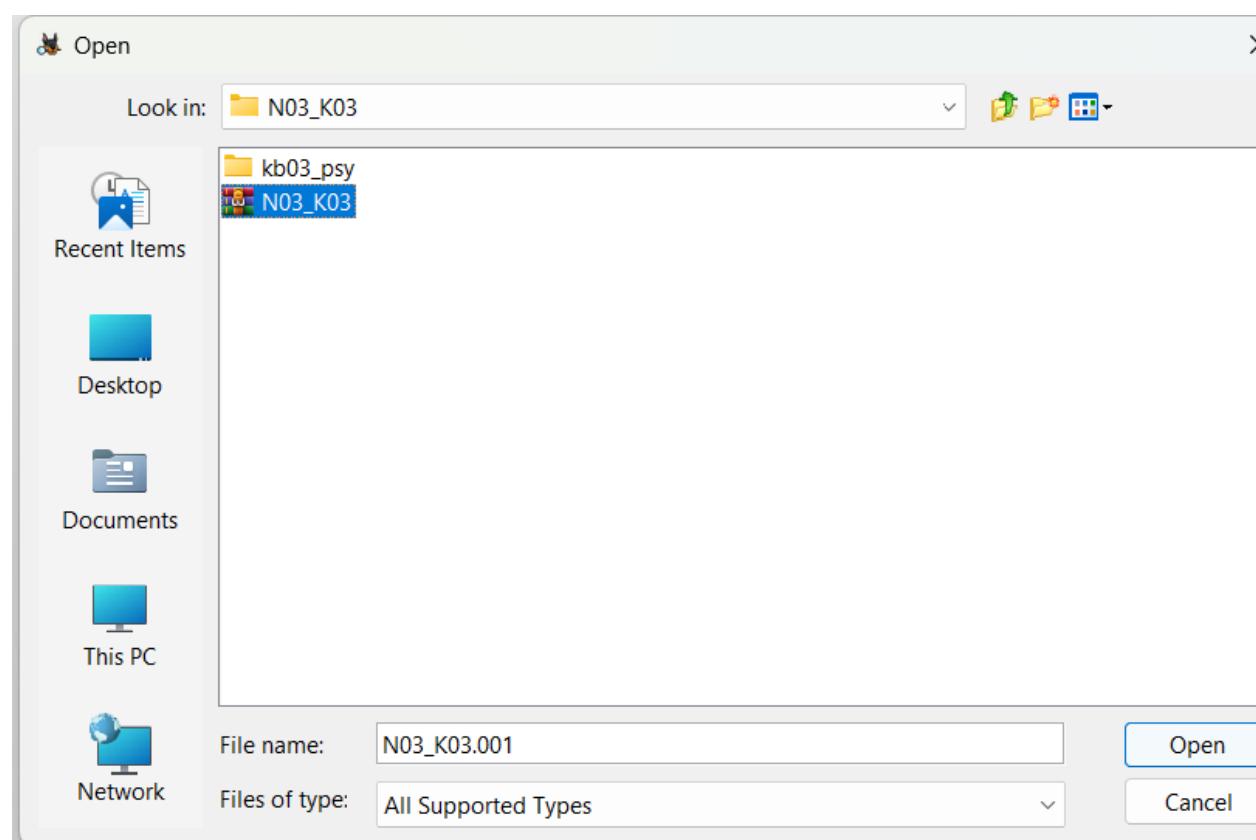
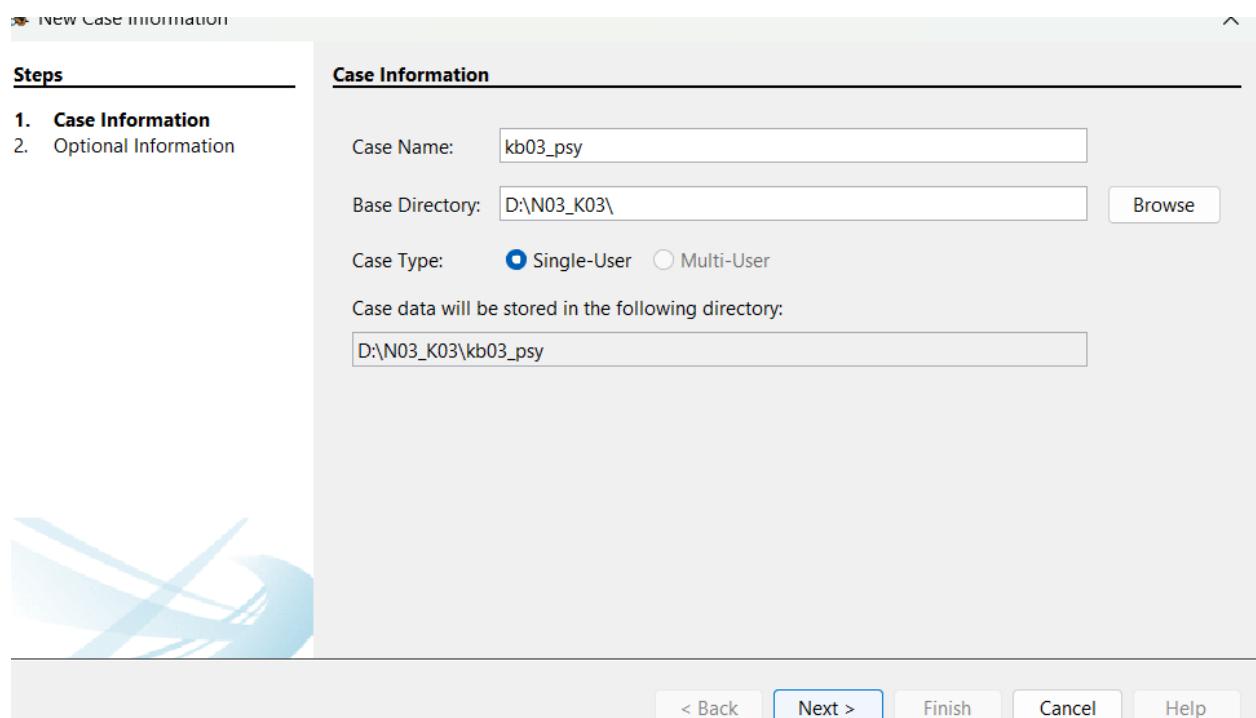
Thông tin Image:



Giờ thì vô Autopsy để phân tích image này thôi:

## Lab 2: Hard Drive Forensics

15



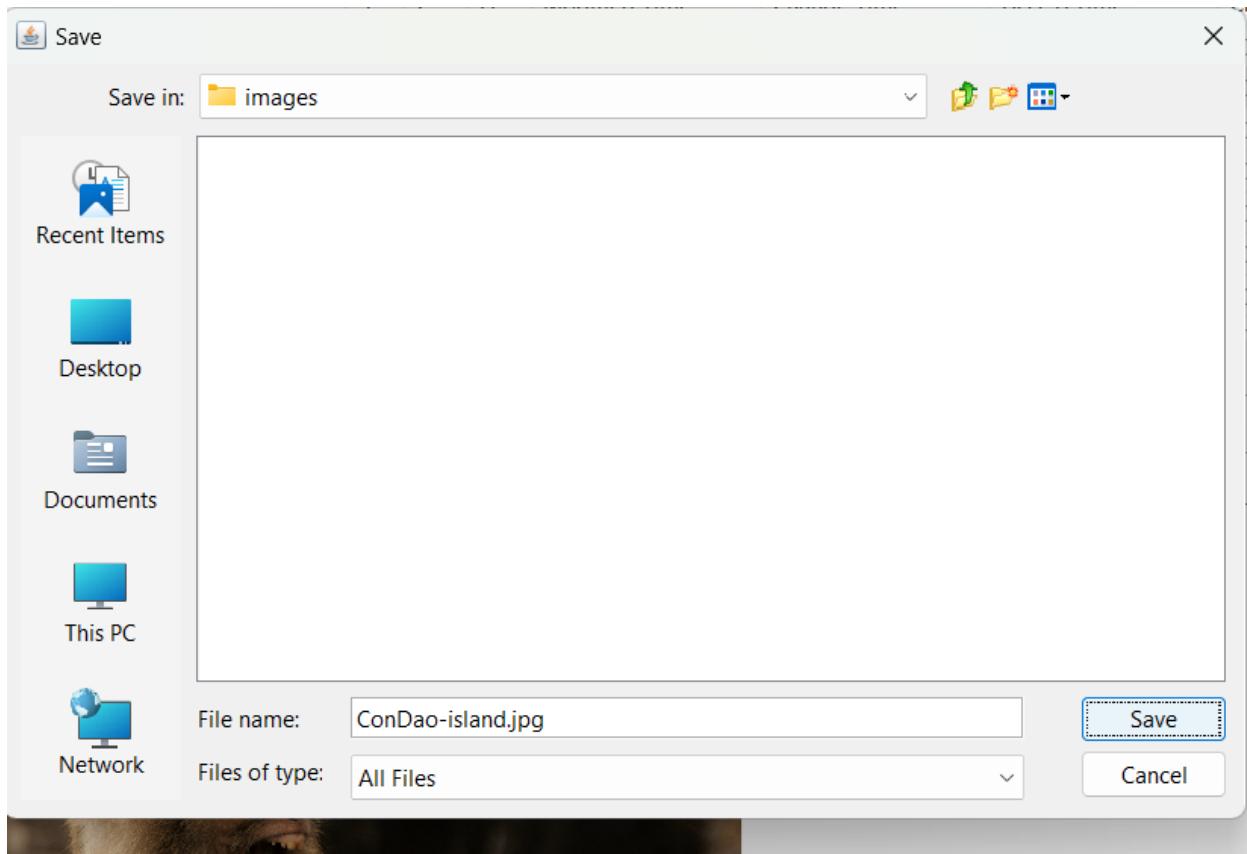
Xem Deleted files thì đã tìm thấy file mình đã xóa:

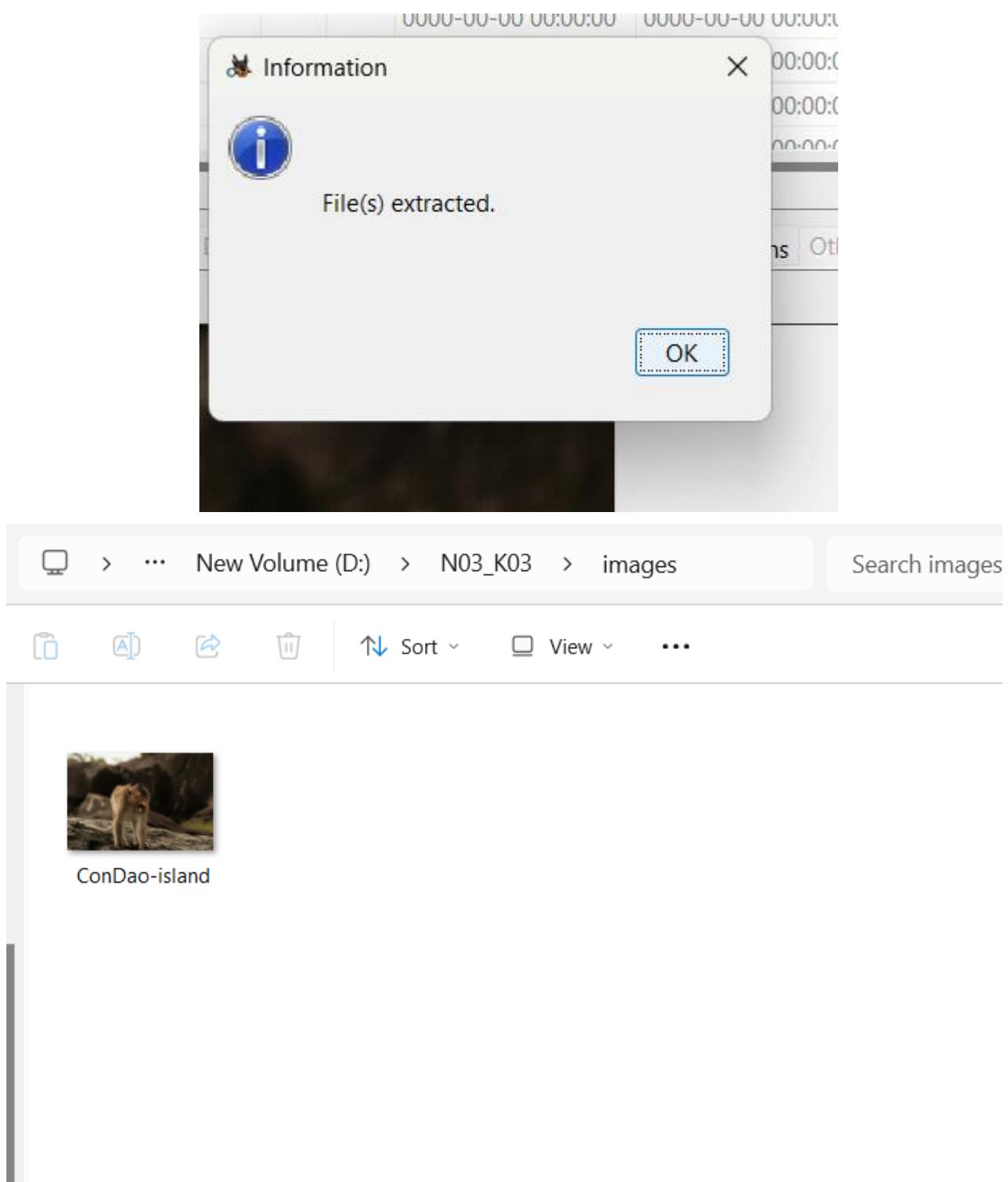
## Lab 2: Hard Drive Forensics

The screenshot shows a forensic analysis interface with a sidebar containing navigation links like Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts, Analysis Results, and Reports. The main area displays a table of files with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and a preview icon. One file, 'ConDao-island.jpg', is selected and shown in a preview window below the table. The preview shows a baboon standing on a rock, barking.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
Contents0.dir				2024-10-17 12:00:36 L	2024-10-17 11:02:21 L	2024-10-17 12:00:36 L	2024-10-17 12:00:36 L	68	Unallocated	Unallocated	unknown /
ConDao-island.jpg				2024-10-16 21:06:40 L	2024-10-16 21:06:40 L	2024-10-16 21:04:39 L	2024-10-16 21:04:39 L	619289	Unallocated	Unallocated	unknown /
CertEnvLibCrt.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	unknown /
Candaria.ttf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	unknown /
CJS202.DLL				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	unknown /
C_865.NLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	unknown /
C_852.NLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	unknown /
ConDao-NIC				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	unknown /

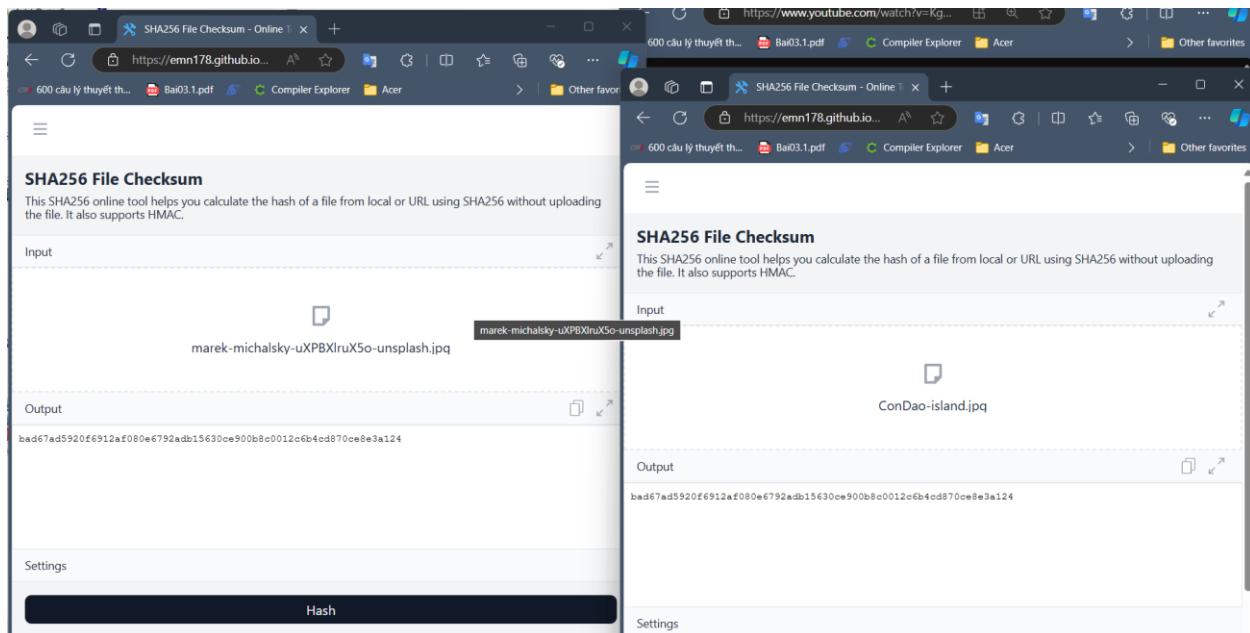
Khôi phục lại vào thư mục images





Tải lại file cũ về, băm và so sánh:

## Lab 2: Hard Drive Forensics



Hai mã băm là giống nhau

- Thực hiện chụp màn hình terminal sau khi hoàn thành điều tra bằng cách gõ các câu lệnh sau:

```
C:\> Command Prompt
C:\Users\Admin>dir D:\N03_K03
Volume in drive D is New Volume
Volume Serial Number is 2EF5-901C

Directory of D:\N03_K03

10/16/2024  09:39 PM    <DIR>          .
10/16/2024  09:39 PM    <DIR>          images
10/16/2024  09:43 PM    <DIR>          kb03_psy
10/16/2024  09:17 PM      1,572,864,000 N03_K03.001
10/16/2024  09:18 PM          1,305 N03_K03.001.txt
10/16/2024  09:17 PM      1,572,864,000 N03_K03.002
10/16/2024  09:18 PM      1,572,864,000 N03_K03.003
10/16/2024  09:18 PM      1,572,864,000 N03_K03.004
10/16/2024  09:18 PM      1,572,864,000 N03_K03.005
10/16/2024  09:18 PM      1,572,864,000 N03_K03.006
10/16/2024  09:18 PM      1,300,234,240 N03_K03.007
               8 File(s) 10,737,419,545 bytes
               3 Dir(s) 16,603,992,064 bytes free

C:\Users\Admin>dir D:\N03_K03\images | findstr "ConDao-island"
10/16/2024  09:39 PM           619,289 ConDao-island.jpg

C:\Users\Admin>date /t
Wed 10/16/2024

C:\Users\Admin>echo "N03"
"N03"

C:\Users\Admin>
```

Kịch bản 04:

## Lab 2: Hard Drive Forensics

### 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:

Sử dụng Autopsy để phân tích file, tìm thấy 2 file có từ khóa “key”:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
_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	/img_f100_6db079ca91c4860f.bin
_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	/img_f100_6db079ca91c4860f.bin

Tiếp tục phân tích thêm file MFT (Master File Table), đây là bảng chính lưu trữ thông tin về tất cả các tệp và thư mục trên phân vùng đĩa được định dạng NTFS.

MFT chứa các bản ghi cho mỗi tệp và thư mục, bao gồm:

- Tên tệp.
- Kích thước tệp.
- Vị trí lưu trữ trên ổ đĩa.
- Dữ liệu quyền truy cập (permissions).
- Các thuộc tính tệp khác (ngày tạo, ngày chỉnh sửa,...).

## Lab 2: Hard Drive Forensics

The screenshot shows a digital forensics tool's main interface. On the left, there's a sidebar with various data sources like 'Data Sources', 'File Views', 'Deleted Files', 'File System (2)', 'MB File Size', 'Data Artifacts', 'Web Downloads (8)', 'Analysis Results', 'EXIF Metadata (1)', 'Keyword Hits (12)', 'User Content Suspected (1)', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main area has tabs for 'Listing', 'Keyword search 1 - MFT', 'Timeline', 'Discovery', 'Generate Report', and 'Close Case'. A 'Keyword Search' bar at the top right contains 'MFT' with a count of '2 Results'. Below it is a table with columns: Name, Keyword Preview, Location, Modified Time, Change Time, Access Time, Created Time, and Size. Two entries are listed: '\$MFT' and '\$MFTMirr'. At the bottom, there's a hex dump view with columns for Address, Value, and ASCII representation.

Tìm trong file MFT này, chúng ta thấy từ khóa “key” với nội dung “notdeleted, neverexisted”.

### Kịch bản 05

#### 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:*

Điều tra trên kali linux, ta thấy được file kb05 là file zip.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[kali㉿kali] ~[~/Desktop/RES_Hard-Drive-Forensics-res/resources-session02]
$ file kb05-session02
kb05-session02: Zip archive data, at least v2.0 to extract, compression method=deflate
```

Tiến hành đổi đuôi file thành .zip rồi tiến hành giải nén.

Tìm kiếm các từ khóa có liên quan đến việc tự tử. Khi tìm kiếm đến từ khóa “kill”, chúng ta thấy lịch sử tìm kiếm có liên quan là How\_fast\_can\_potassium\_cyanide\_kill\_you.

## Lab 2: Hard Drive Forensics

kb05 - Autopsy 4.21.0

Case View Tools Window Help

Listing Keyword search 1 - kill x

Keyword search

Name Keyword Preview Location Modified Time Change Time Access Time

OPR00200.HTM hree submissions-<skill> level: intermediate /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR00200.HTM hree submissions-<skill> level: intermediate /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR00200.HTM hree submissions-<skill> level: intermediate /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR00200.HTM hree submissions-<skill> level: intermediate /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR001XK.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 2006-01-05 00:00:00

dcache4new .\$.\$.\$.x3/45\$ii=+killid<+hvv6uuuy4%>>w^ /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\_TF.. 2006-01-04 18:06:00 ICT 0000-00-00 00:00:00 2006-01-04 00:00:00

OPR001ZXJS e&&e\_widgetmanager?i=&e\_widgetmanager\_killpopup /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:35:02 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR001ZXJS e&&e\_widgetmanager?i=&e\_widgetmanager\_killpopup /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:35:02 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR001ZXJS e&&e\_widgetmanager?i=&e\_widgetmanager\_killpopup /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\_TF.. 2006-01-05 19:35:02 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR0020KJS 52?); }; // global +killswitch on the element if ( /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

OPR0020KJS 52?); }; // global +killswitch on the element if ( /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:37:24 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

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 2006-01-06 00:00:00

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 2006-01-06 00:00:00

0 /\*\*/- styles for <skill> rows /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\_TF.. 0000-00-00 00:00:00 0000-00-00 00:00:00

OPR001ZXJS e&&e\_widgetmanager?i=&e\_widgetmanager\_killpopup /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:35:02 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00

Tìm kiếm thêm về potassium cyanide ta thấy được một đường link có liên quan: where+can+i+buy+potassium+cyanide. Có thể thấy được việc chủ máy tính có ý định tự tử với potassium cyanide.

kb05 - Autopsy 4.21.0

Case View Tools Window Help

Listing Keyword search 1 - kill x Keyword search 2 - cyanide x

Keyword search

Name Keyword Preview Location Modified Time Change Time Access Time Created Time

COOKIES4.NEW can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 12:05:32 ICT 0000-00-00 00:00:00 2006-01-06 00:00:00 ICT 2006-01-06 12:05:

OPR001XG.PNG can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:32:06 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00 ICT 2006-01-05 19:32:

OPR001XG-PNG %2b%buy%2bpotassium%20cyanide%+ image /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:32:06 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00 ICT 2006-01-05 19:32:

P0001L.GIF-slack %2b%buy%20potassium%20cyanide%\_utm /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-04 18:54:54 ICT 0000-00-00 00:00:00 2006-01-04 00:00:00 ICT 2006-01-04 18:54:

P0001V1.GIF-slack %2b%buy%20potassium%20cyanide%\_utm /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:29:18 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00 ICT 2006-01-05 19:29:

P0001V2.GIF-slack can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:29:18 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00 ICT 2006-01-05 19:29:

COOKIES4.DAT can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:47:32 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00 ICT 2006-01-05 19:47:

COOKIES4.DAT can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-06 12:53:02 ICT 0000-00-00 00:00:00 2006-01-06 00:00:00 ICT 2006-01-06 12:53:

DCACHE4URL can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-06 12:04:32 ICT 0000-00-00 00:00:00 2006-01-06 00:00:00 ICT 2006-01-06 12:04:

cookie4.dat can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\_TF.. 2006-01-06 12:53:02 ICT 0000-00-00 00:00:00 2006-01-06 00:00:00 ICT 2006-01-06 12:53:

\_OOKEY4.NEW can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:47:32 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00 ICT 2006-01-05 19:47:

VLINK4.DAT can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-06 12:04:32 ICT 0000-00-00 00:00:00 2006-01-06 00:00:00 ICT 2006-01-06 12:04:

\_OOKEY4OLD can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-05 19:46:30 ICT 0000-00-00 00:00:00 2006-01-05 00:00:00 ICT 2006-01-05 19:46:

COOKIES4.DAT can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-06 12:05:32 ICT 0000-00-00 00:00:00 2006-01-06 00:00:00 ICT 2006-01-06 12:05:

COOKIES4.DAT can+i+buy+potassium+<cyanide>/utmcmd=organic\_.. /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-04 19:05:50 ICT 0000-00-00 00:00:00 2006-01-04 00:00:00 ICT 2006-01-04 19:05:

P0001L.GIF-slack %2b%buy%20potassium%20cyanide%\_utm /img\_56DACP1C6CF363F27501FFCA50CC0415.raw/\$Orp. 2006-01-04 18:52:54 ICT 0000-00-00 00:00:00 2006-01-04 00:00:00 ICT 2006-01-04 18:52:

## Kịch bản 06

Thực hiện phân tích:

- Tài nguyên: kb06-session02.pdf

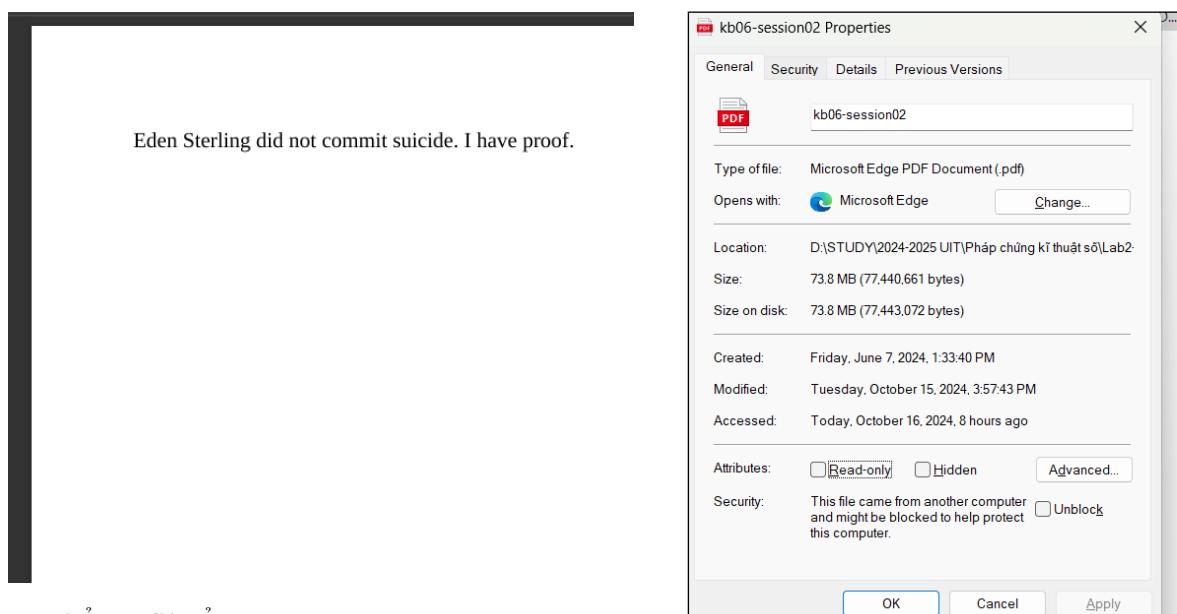
## Lab 2: Hard Drive Forensics

- 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 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:

1. Thông tin đăng nhập của tài khoản truyền thông xã hội của Eden là gì?
2. Bỏ tất cả các câu có Alice và Bruce, thay vào đó là tìm tập tin có nội dung liên quan đến nơi Eden làm việc và học tập? Ai là người viết nội dung trong đó? (Gợi ý: Nancy)
3. Giao dịch (transaction) cũ nhất được ghi lại vào ngày nào? - Tìm trong mục Credit Card, ghi thông tin ngày tháng gần nhất là được (Gợi ý: vào năm 2014)
4. Tìm tài khoản ngân hàng?
5. Tìm file secret.txt và đọc nội dung mà Eden để lại.
6. Tìm được tấm hình Nobias.

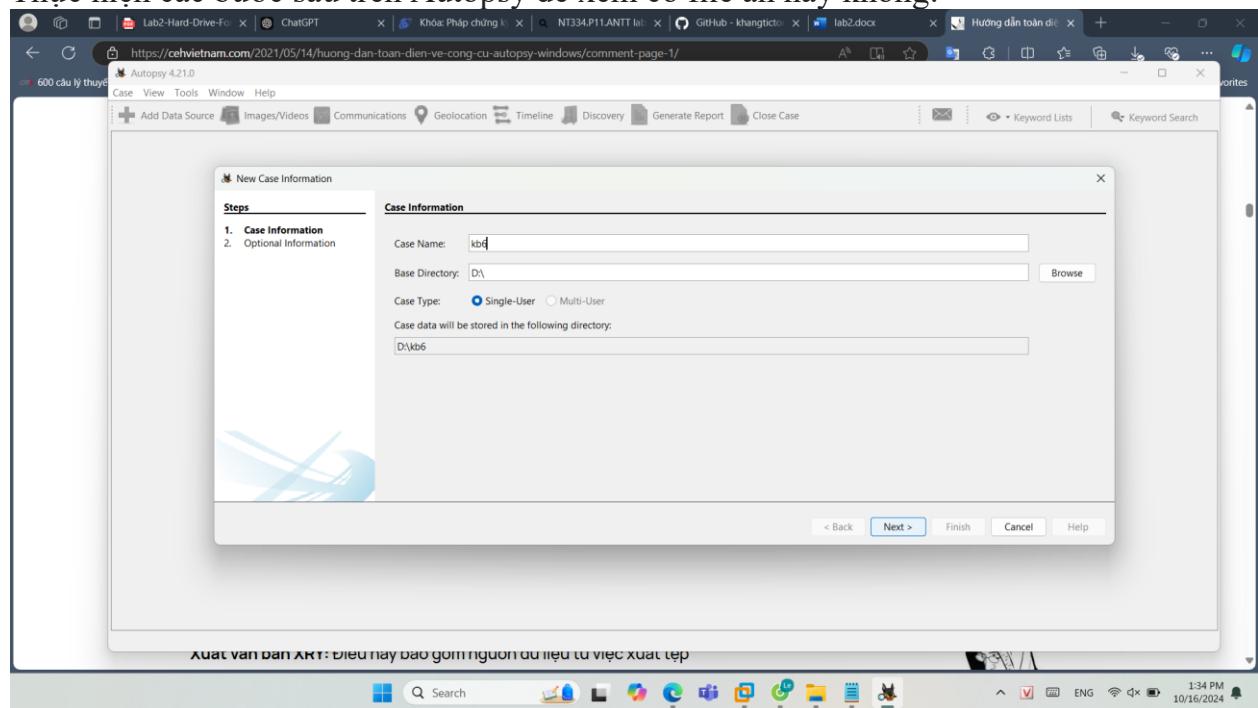
Mở file PDF bôi đen hết chỉ thấy có 1 dòng duy nhất như bên dưới và file này nặng bất thường so với 1 file PDF thông thường

## Lab 2: Hard Drive Forensics

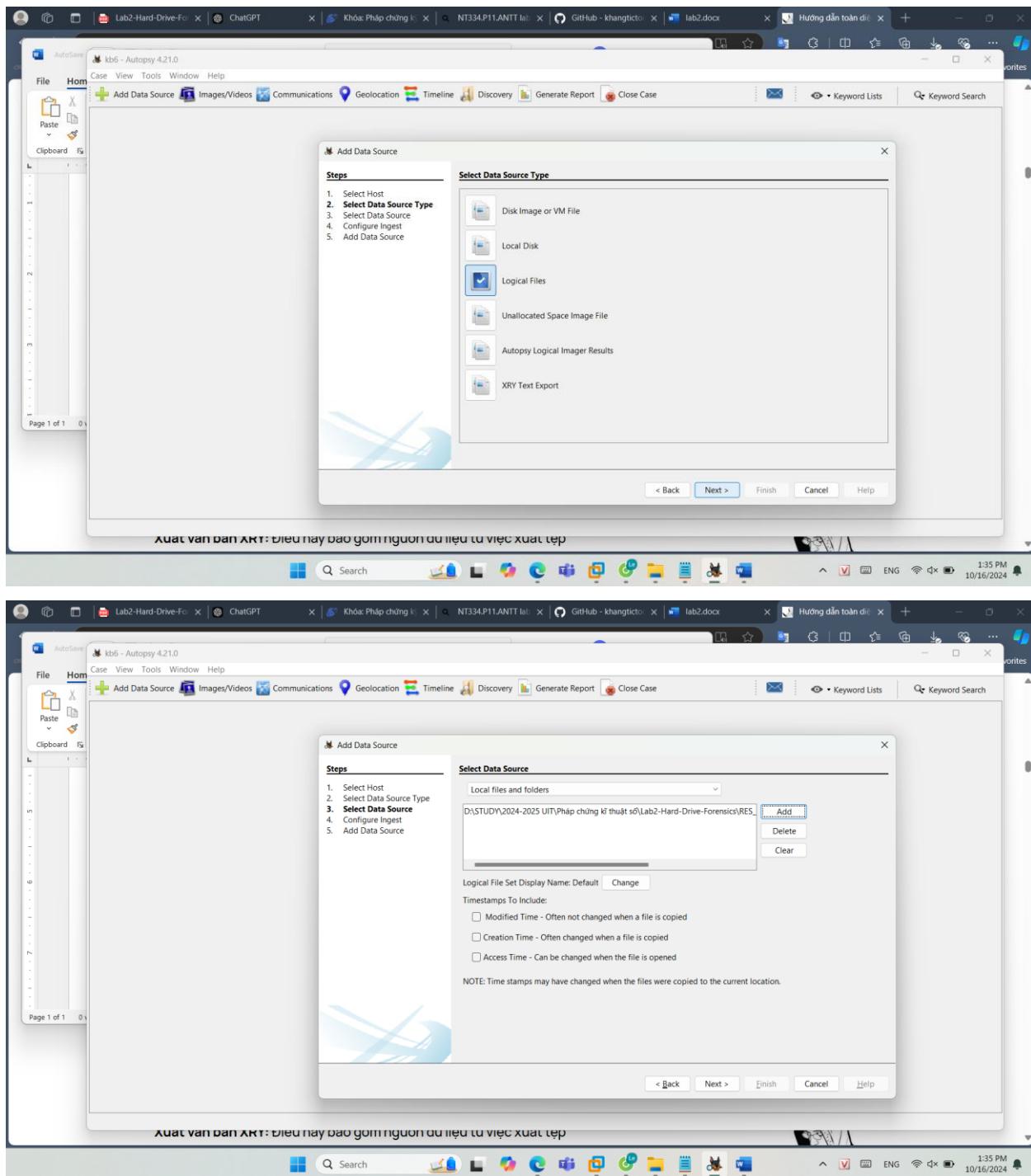


Có thể có file ẩn

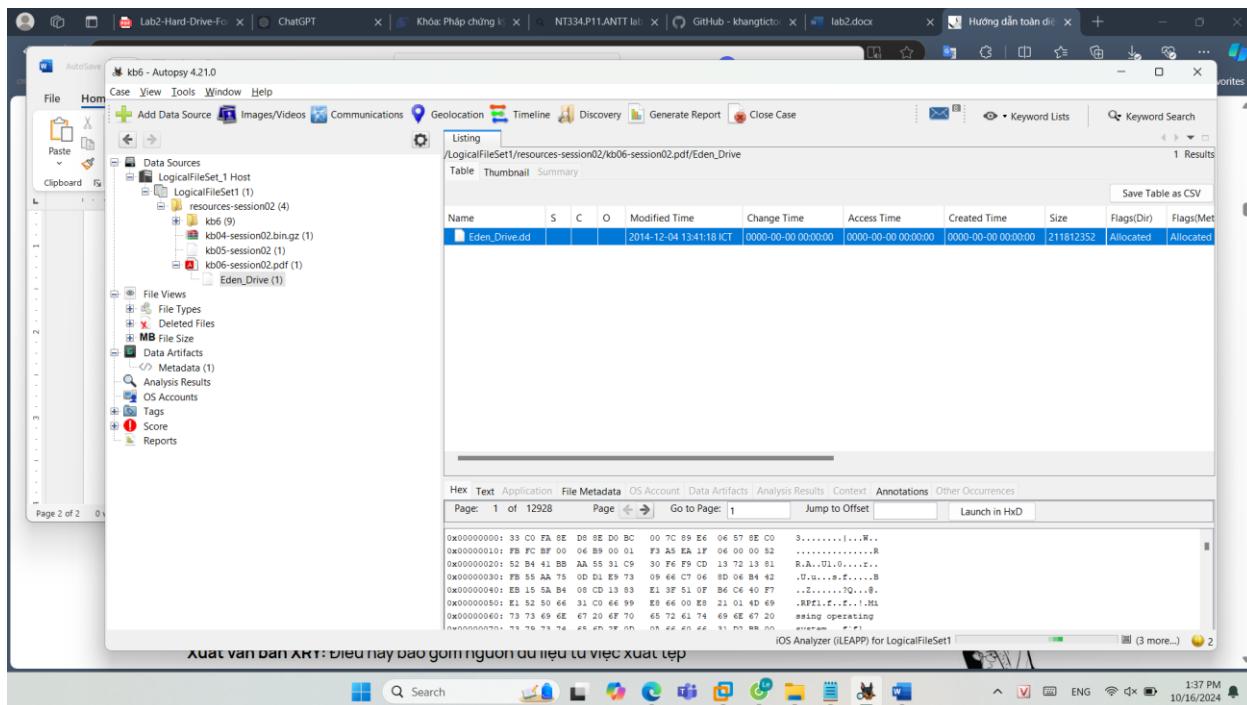
Thực hiện các bước sau trên Autopsy để xem có file ẩn hay không:



## Lab 2: Hard Drive Forensics

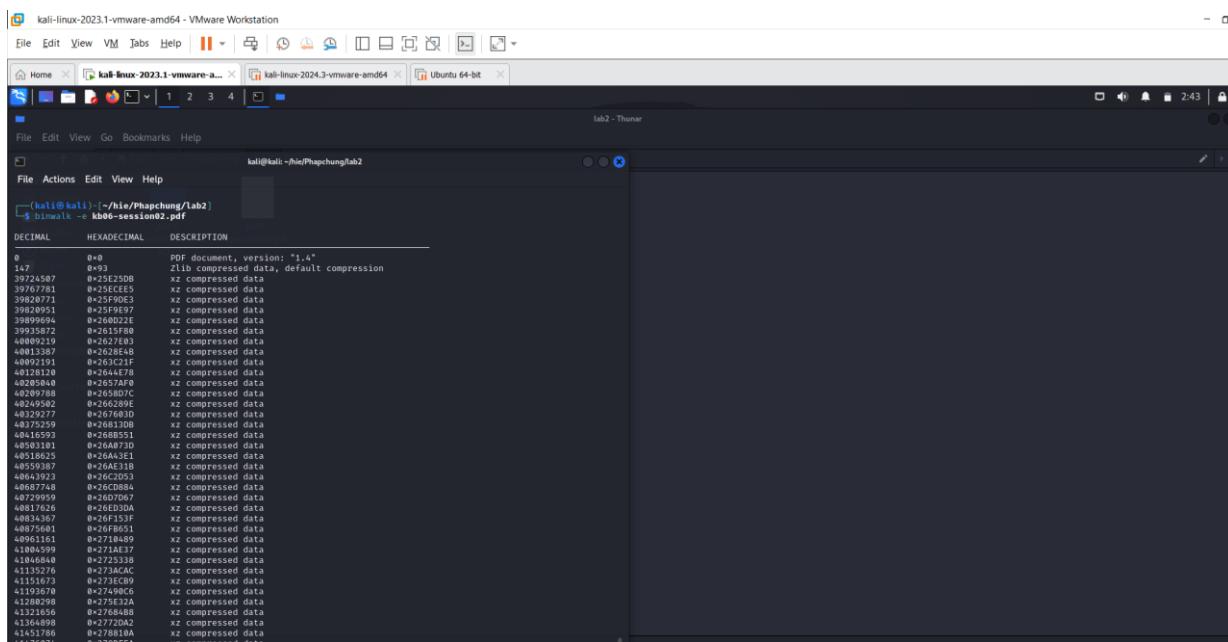


## Lab 2: Hard Drive Forensics



Thấy có 1 file ảnh nằm trong file pdf có tên là Eden\_Drive.dd đây là 1 file ảnh đĩa có thể sử dụng nó để phân tích luôn.

Trường hợp khác có thể dùng linux để xem file ảnh:

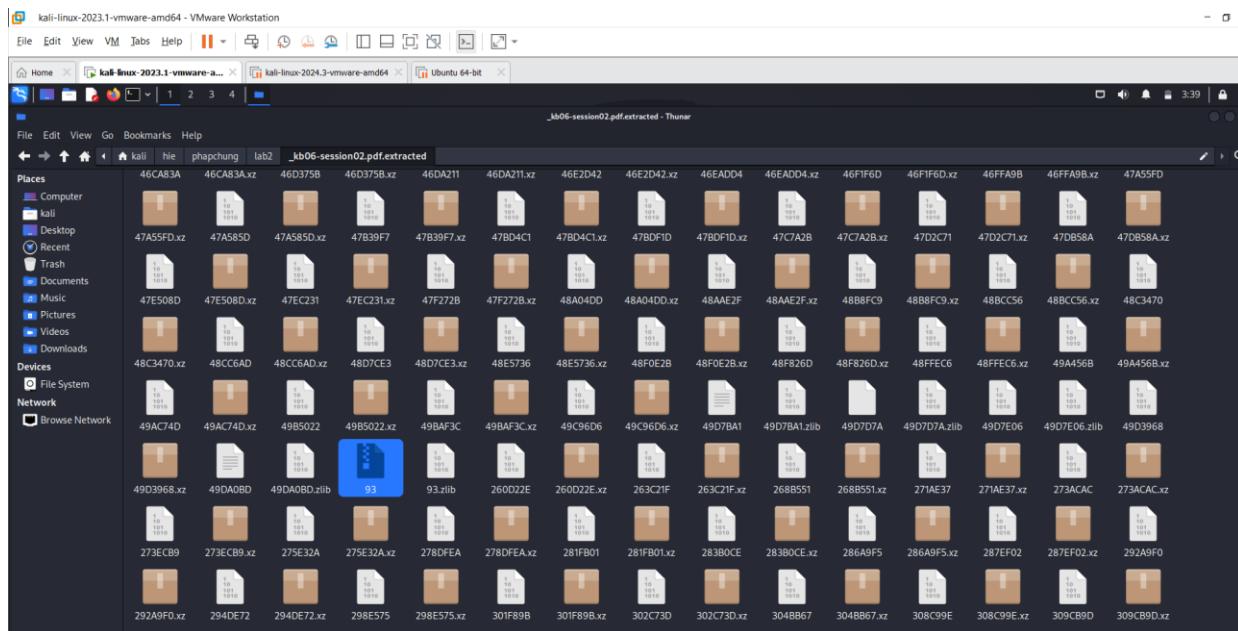


**Binwalk** là một công cụ phân tích tệp nhị phân, được thiết kế chủ yếu để trích xuất và phân tích nội dung trong các tệp nhị phân.

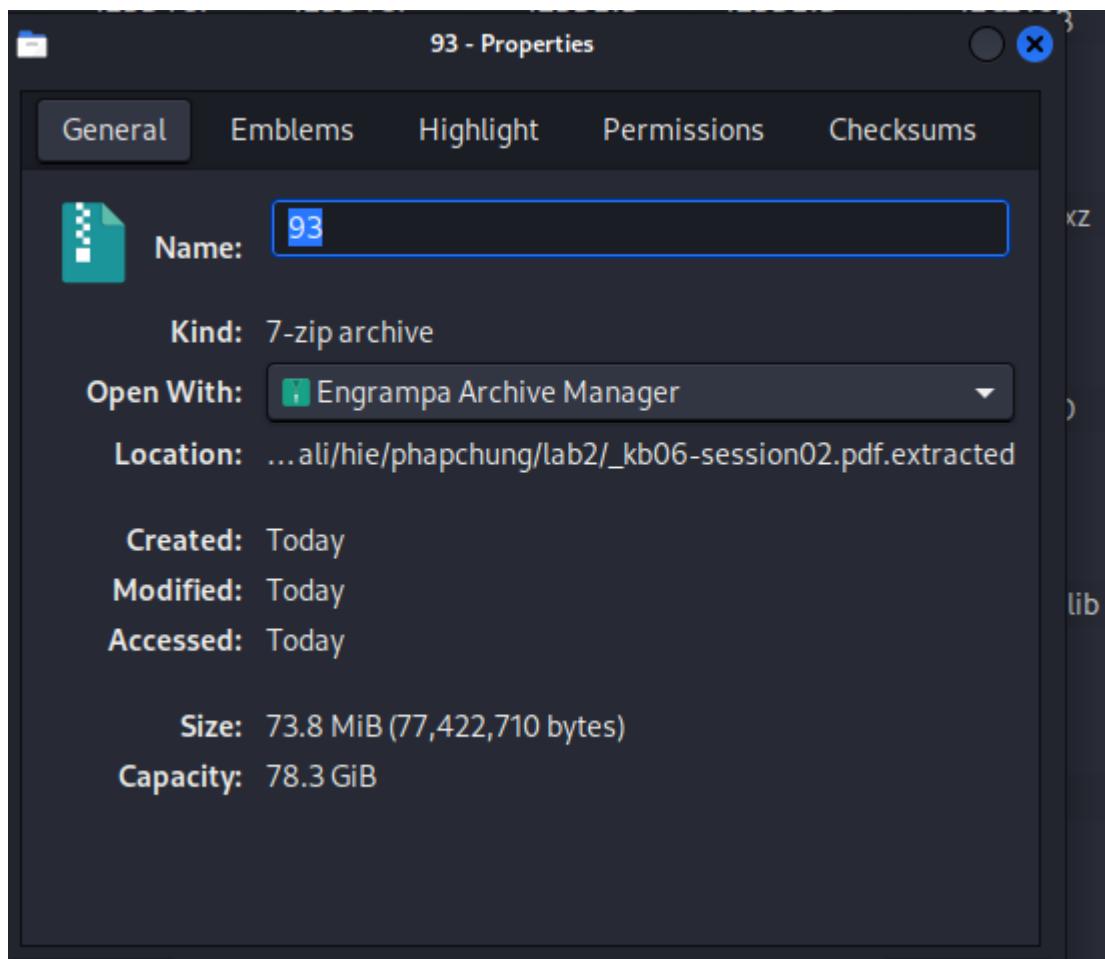
Sử dụng tùy chọn -e để trích xuất các tệp thành phần từ tệp nhị phân

Kết quả:

## Lab 2: Hard Drive Forensics



Có 1 file nén duy nhất khả nghi. Thông tin của file này



Thực hiện giải nén:

## Lab 2: Hard Drive Forensics

```
(kali㉿kali)-[~/hie/phapchung/lab2/_kb06-session02.pdf.extracted]
$ 7z x 93

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20 A14.xz 2A005F2.xz 2A
64-bit locale=en_US.UTF-8 Threads:32 OPEN_MAX:1024

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

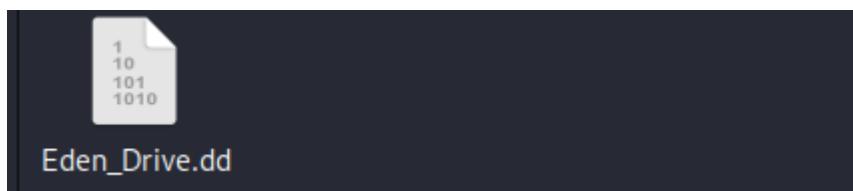
Extracting archive: 93 2A9631C.xz 2A81051 2A81051.xz 2AAA808 2AAA808.xz 2A
-- 2 AE479F.xz 2AE479F 2AF2C01 2AF2C01.xz 2AFDC77 2AF
Path = 93
Type = 7z
Physical Size = 77422710
Headers Size = 122
Method = LZMA2:26
Solid = -
Blocks = 1

Everything is Ok

Size: 211812352 2B5E014.xz 2B25A16 2B25A16.xz 2B59D5F 2B59D5F.xz 2B
Compressed: 77422710

(kali㉿kali)-[~/hie/phapchung/lab2/_kb06-session02.pdf.extracted]
```

Được file disk image có thể đưa vào Autopsy để thực hiện phân tích



### 1. Thông tin đăng nhập của tài khoản truyền thông xã hội của Eden là gì?

File PDF này dường như chứa gì đó khi em vô tình kéo chuột vào nó lại được bôi xanh

Copy and paste thì nó ra như này:

Thì nó ra như này

**Username:** stringsinCsharp  
WĂΞΕΙŽdĚ EłdšŶŐ ĐĂΞEИŽdĚ c□ūGħwĠsŶħtie'

Mói có username

Em qua mục text thì thấy được nhiều thông tin hơn

## Viết ngang lại

## Username: strings in Csharp

**Password:** string password = "letmein321!";

## Lab 2: Hard Drive Forensics

2. Tìm tập tin có nội dung liên quan đến nơi Eden làm việc và học tập? Ai là người viết nội dung trong đó?

Nội dung liên quan đến nơi Eden làm việc và học tập: Dường như đây là một mẫu báo cáo

**Lab Title:**  
Unknown Letter or Number \_\_\_\_\_ (if applicable)  
**Class and Section:**  
**Date Lab was Performed:**  
**Student Name:**  
**Lab Partner's Name (if applicable):**

Qua mục Data Artifacts thì thấy tác giả là Nancy

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	K
f0075416_CHE_112 LABORATORY_NOTEBOOKS.pdf	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	96863	Unallocated	Unallocated	un
f0025304.pdf	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	72671	Unallocated	Unallocated	un
6590629.pdf	0	2014-12-04 13:33:57 ICT	45289	Allocated	Allocated	ur					
6105002.pdf	0	2014-12-04 13:33:57 ICT	17920	Allocated	Allocated	ur					
4723306.pdf	0	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	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	5371	Allocated	Allocated	ur

**Metadata:**

Type	Value	Source(s)
Version	1.4	org.sleuthkit.autopsy.keyword
Date Created	2014-06-16 22:50:53 ICT	org.sleuthkit.autopsy.keyword
Owner	Nancy	org.sleuthkit.autopsy.keyword
Date Modified	2014-06-16 22:50:55 ICT	org.sleuthkit.autopsy.keyword
Source File Path	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0075416_CHE_112 LABORATORY_NOTEBOOKS.pdf	
Artifact ID	-9223372036854775766	

3. Giao dịch (transaction) cũ nhất được ghi lại vào ngày nào? - Tìm trong mục Credit Card, ghi thông tin ngày tháng gần nhất là được (Gợi ý: vào năm 2014)

Dùng Keyword List để lọc credit card number

## Lab 2: Hard Drive Forensics

The screenshot shows a digital forensics tool interface. On the left, there is a list of files found during a search across four transactions. The columns include Name, Keyword Preview, and Location. Some preview text is visible for each file. On the right, a panel displays a definition for 'Credit Card Numbers' with regular expression patterns: '(%?)(B7)([0-9][\ \ ]\*)?(12,19)...'. Below this are sections for 'Restrict search to the selected data sources' and 'Save search results'. At the bottom, there are buttons for 'Search', 'Manage Lists', and 'Files Indexed: 0'.

Sau đó qua phần thumbnail để xem tổng quan:

The screenshot shows a digital forensics tool interface with a thumbnail view of found files. A single thumbnail for '1073084.jpg' is displayed, labeled '\$UpCase'. Below the thumbnails, there is a table of search results for 'Accounts'. The columns include Type, Value, and Source(s). The results show details for a Credit Card account, including ID, Card Number, Keyword, Set Name, Keyword Preview, Keyword Search Type, Source File Path, and Artifact ID.

Type	Value	Source(s)
Account Type	CREDIT_CARD	Keyword Search
ID	2021222324252627282	Keyword Search
Card Number	2021222324252627282	KeywordSearch
Keyword	2021222324252627282	KeywordSearch
Set Name	Credit Card Numbers	Keyword Search
Keyword Preview	28'2'(2)2*2+2,2-2.2/*2021222324252627282*92;2<2=2>2?@2a2b2	Keyword Search
Keyword Search Type	2	Keyword Search
Source File Path	/img_Eden_Drive.dd/vol_vo14/\$UpCase	
Artifact ID	-922337203685475230	

## **Lab 2: Hard Drive Forensics**

Metadata	
Name:	/img_Eden_Drive.dd/vol_vol4/\$UpCase
Type:	File System
MIME Type:	image/vnd.microsoft.icon
Size:	131072
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2014-11-28 03:51:26 ICT
Accessed:	2014-11-28 03:51:26 ICT
Created:	2014-11-28 03:51:26 ICT
Changed:	2014-11-28 03:51:26 ICT
MD5:	2f03b5a69d486ff3864cecb0d7f24440
SHA-256:	d82e679f23b7988b320807e81b72f6d965b42068e8aa7f2e0932f07cf349a146
Hash Lookup Results:	UNKNOWN
Internal ID:	491

So sánh với các mục khác trong phần table

Giao dịch cũ nhất được ghi lại vào ngày: 28/11/2014

#### 4. Tìm tài khoản ngân hàng?

5. Tìm file secret.txt và đọc nội dung mà Eden để lại.

## Lab 2: Hard Drive Forensics

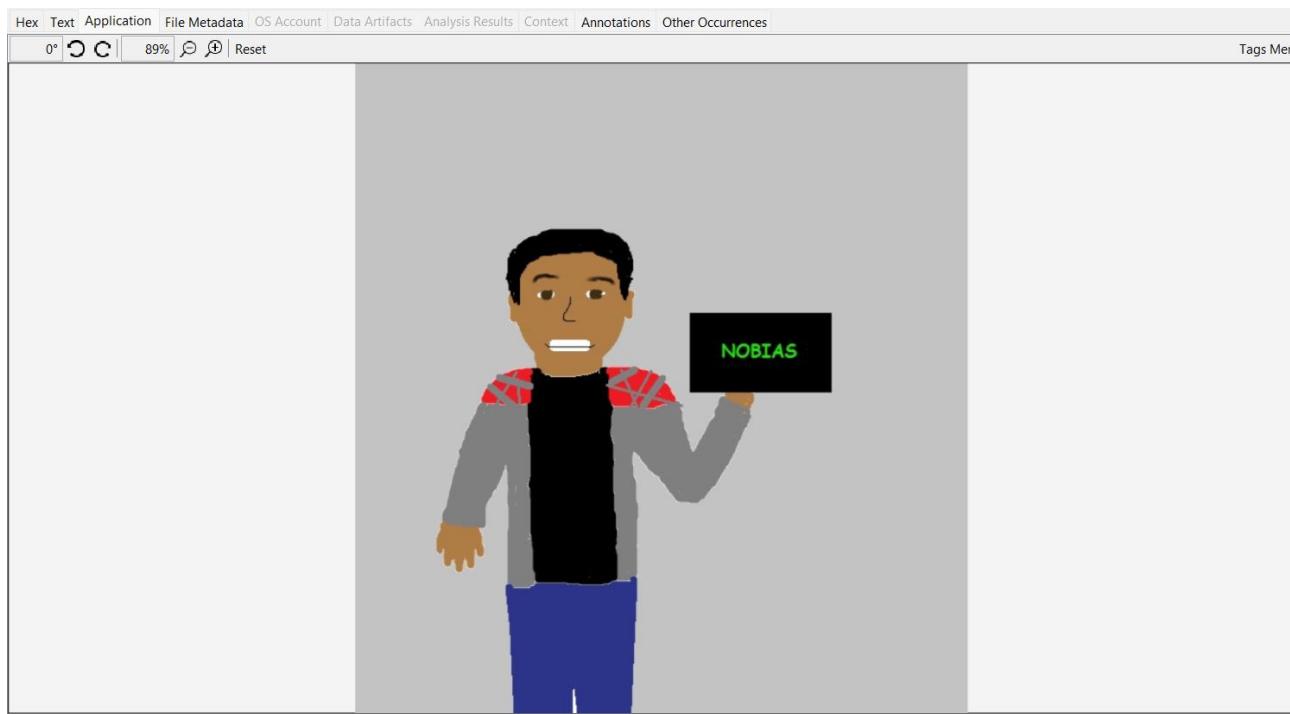
The screenshot shows a forensic analysis interface with two main panes. The left pane displays a file tree for a logical file set named 'LogicalFileSet\_1 Host'. The right pane has a 'Table' view with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. It lists several files including 'secret.docxsecret.txt', 'secret.docx', 'f0085384.docx', and '8875837.doc'. Below the table is a 'Text' view showing the content of 'secret.docx' which includes the text 'I think someone may be after me. - Eden'. A section labeled 'METADATA' follows.

Nội dung mà Eden để lại: “I think someone may be after me. – Eden”

### 6. Tìm được tấm hình Nobias

Thumbnail image thì tìm được tấm hình nobias

This screenshot shows the same forensic tool interface as above, but with a focus on images. The left pane shows the file tree. The right pane has a 'Thumbnail' view with a grid of image thumbnails. One thumbnail is selected, showing a person holding a phone with the word 'NOBIAS' on its screen. Below the thumbnails is a detailed view of the selected image, showing its hex dump and file metadata.



## Challenge

Encrypted Disk:

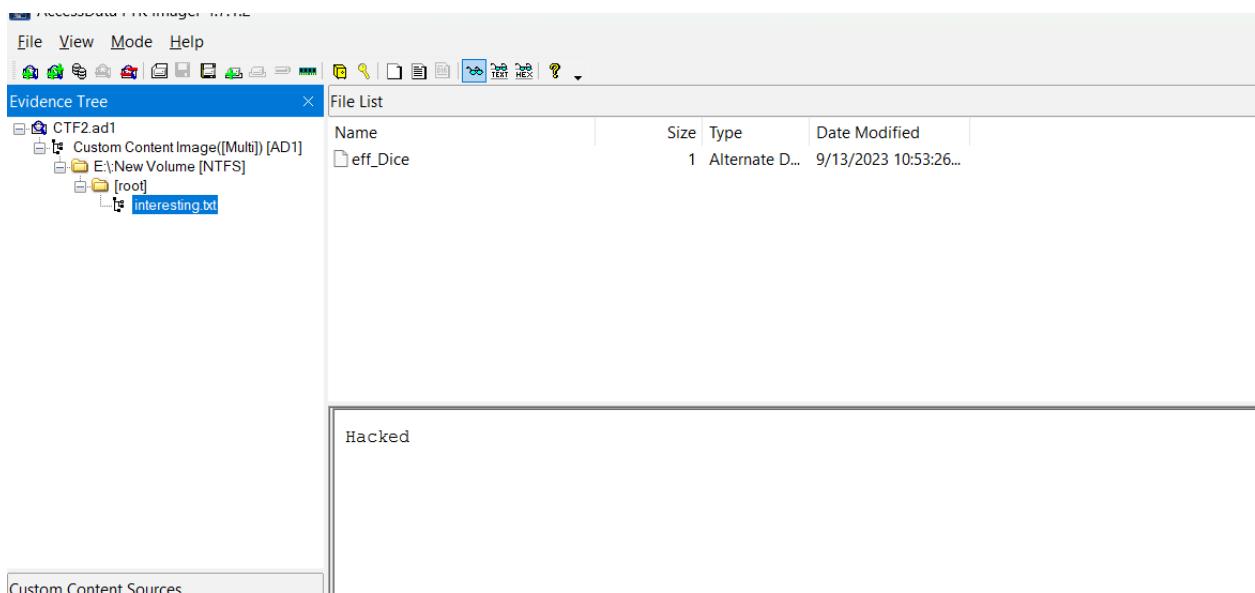
Link tài nguyên: [https://drive.google.com/file/d/1yRM10QeH3KI7-xVhZffOLrK6QKqncYj/view?usp=drive\\_link](https://drive.google.com/file/d/1yRM10QeH3KI7-xVhZffOLrK6QKqncYj/view?usp=drive_link)

My PC was Hacked, Can you help me know what happened?

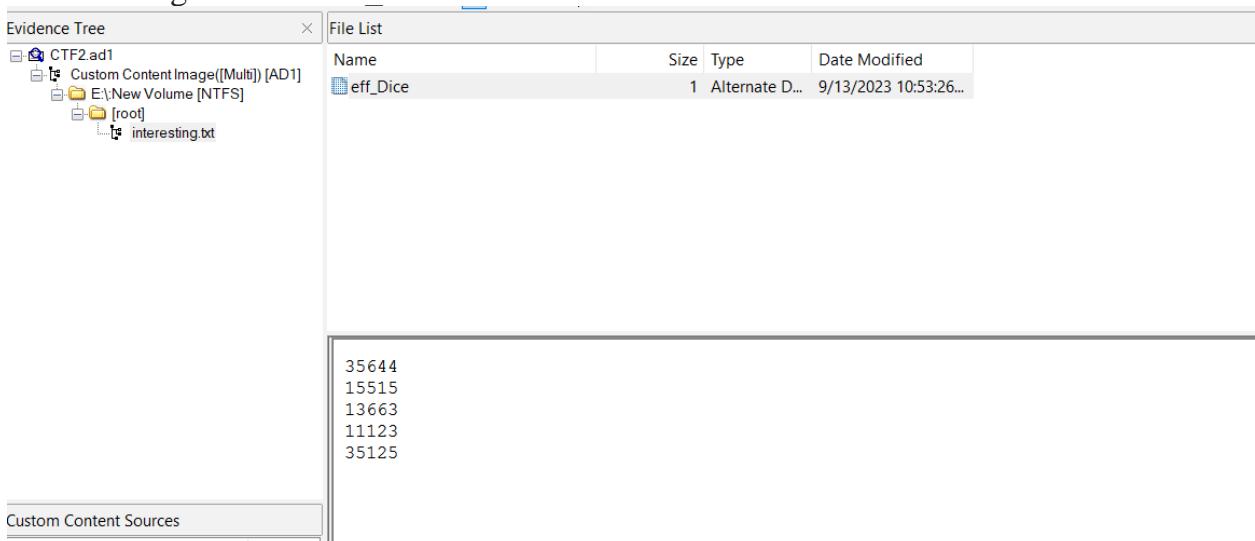
Đây là tệp có đuôi .ad1 đây là một tệp Image sử dụng bởi bộ công cụ pháp y FTK. Mở nó lên.

Thấy bên trong chứa tệp interesting.txt có nội dung “Hacker”

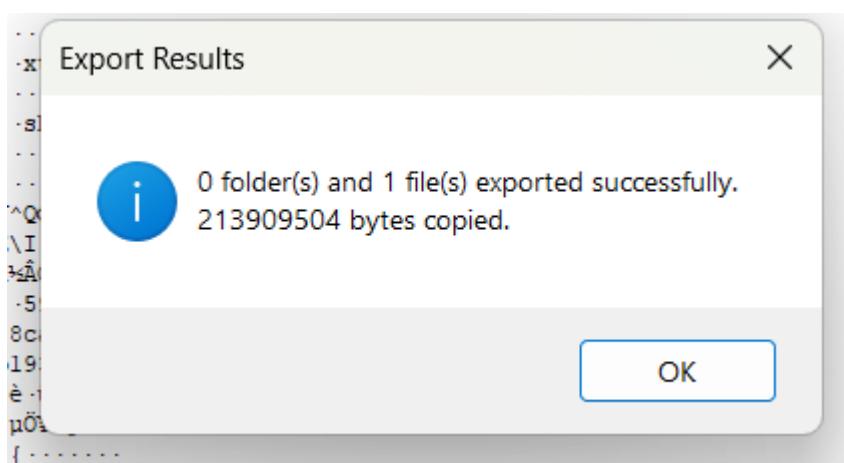
## Lab 2: Hard Drive Forensics



Và bên trong chứa file eff\_Dice chứa các chuỗi số:



Trích xuất file challenge1.img ra:



## Lab 2: Hard Drive Forensics

Sử dụng công cụ **cryptsetup** đây là 1 công cụ mã hóa theo tiêu chuẩn **LUKS (Linux Unified Key Setup-on-disk-format)** dành cho linux.

Xem thông tin thủ thông tin

```
Sudo: 1 incorrect password attempt

[(kali㉿kali)-[~/.../phapchung/Lab3/challenge/Encrypted Disk]]
$ sudo cryptsetup luksDump challenge1.img
[sudo] password for kali:
LUKS header information for challenge1.img

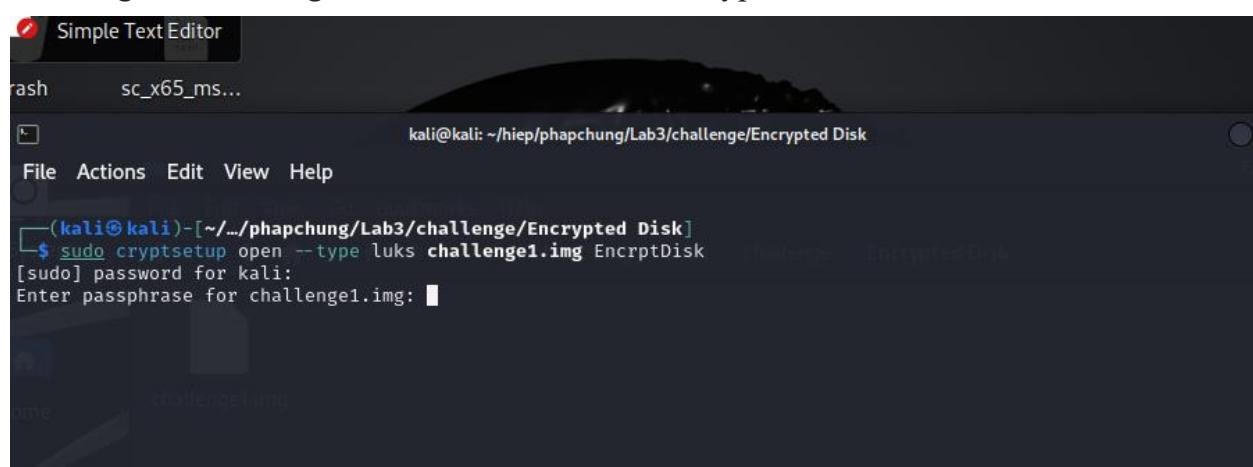
Version:      1
Cipher name:  aes
Cipher mode:  xts-plain64
Hash spec:    sha256
Payload offset: 4096
MK bits:     256
MK digest:   fe b0 66 62 08 c9 4a 5e 51 ae 03 55 4a 4d 96 e5 1d c8 62 5e
MK salt:     03 01 cb 5c 49 95 02 b5 c7 c2 d7 87 05 74 32 70
              d0 32 e4 bd c2 4f 1f 4d 8a 8a 4f af 15 79 31 63
MK iterations: 112798
UUID:        596ea45e-0b33-48ca-9257-0769f7b193fb

Key Slot 0: ENABLED
  Iterations:      1804776
  Salt:           80 fb 96 8b 6e 95 2c 68 e7 cf 77 1b 44 11 1d b5
                  d6 a5 d8 67 1c 2a f6 7a e4 2b e9 2e 72 cb 49 7b
  Key material offset: 8
  AF stripes:     4000

Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED

[(kali㉿kali)-[~/.../phapchung/Lab3/challenge/Encrypted Disk]]
$ ss
```

Sử dụng lệnh mở và giải mã file, đặt tên file là Ecrypt Disk



The screenshot shows a terminal window titled "Simple Text Editor". The command entered is:

```
(kali㉿kali)-[~/.../phapchung/Lab3/challenge/Encrypted Disk]
$ sudo cryptsetup open --type luks challenge1.img EncrptDisk
[sudo] password for kali:
Enter passphrase for challenge1.img: [REDACTED]
```

Cần mật khẩu để giải mã file. Nhớ lại file eff\_Dice thử các dãy số với trường hợp viết liền và viết cách nhau đều sai

Tìm được Worklist cũng có tên là eff



### Deep Dive: EFF's New Wordlists for Random Passphrases

BY JOSEPH BONNEAU | JULY 19, 2016

*Note: Just looking for the word lists?*

- [Click here for EFF's long word list \(for use with five dice\) \[.txt\]](#),
- [Click here for EFF's general short word list \(for use with four dice\) \[.txt\]](#), and
- [Click here for EFF's short word list \(with words that have unique three-character prefixes\) \[.txt\]](#).

#### Discover more.

Email updates on news, actions, events in your area, and more.

Email Address

Digital Code (optional)

Tìm được các cụm:

35644 legacy

15515 childhood

13663 bottom

11123 abnormal

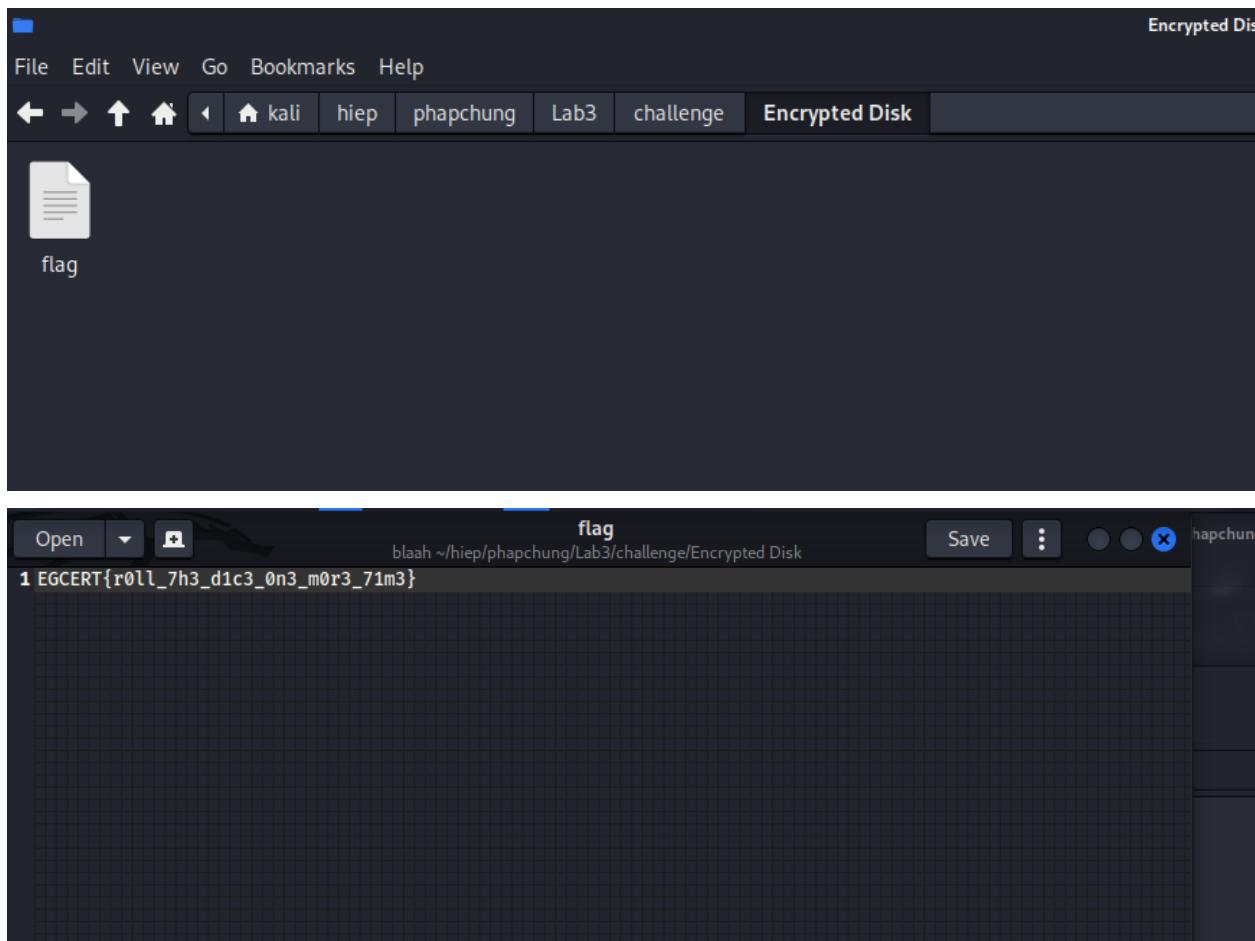
35125 jazz

Mật khẩu là: “legacy legacy bottom abnormal jazz”

Gắn mout vào thư mục hiện tại để giải mã:

```
test.cpp
└──(kali㉿kali)-[~/.../phapchung/Lab3/challenge/Encrypted Disk]
    $ sudo mount /dev/mapper/EncrptDisk ./
    
└──(kali㉿kali)-[~/.../phapchung/Lab3/challenge/Encrypted Disk]
    $ ls
    sc_x65_ms...
```

Kết quả:



Flag là: **EGCERT{r0ll\_7h3\_d1c3\_0n3\_m0r3\_71m3}**

Timestomp

### Timestomp

500

The attacker dropped malware that stomped the timestamp of malicious files according to the timestamps of the files in the same directory.

Can you retrieve the logfile sequence number of the timestamped file?

**EGCERT{decimal\_logfile\_sequence\_number}**

**Kẻ tấn công đã thả phần mềm độc hại và thay đổi dấu thời gian của các tệp tin độc hại sao cho trùng khớp với dấu thời gian của các tệp tin khác trong cùng thư mục.**

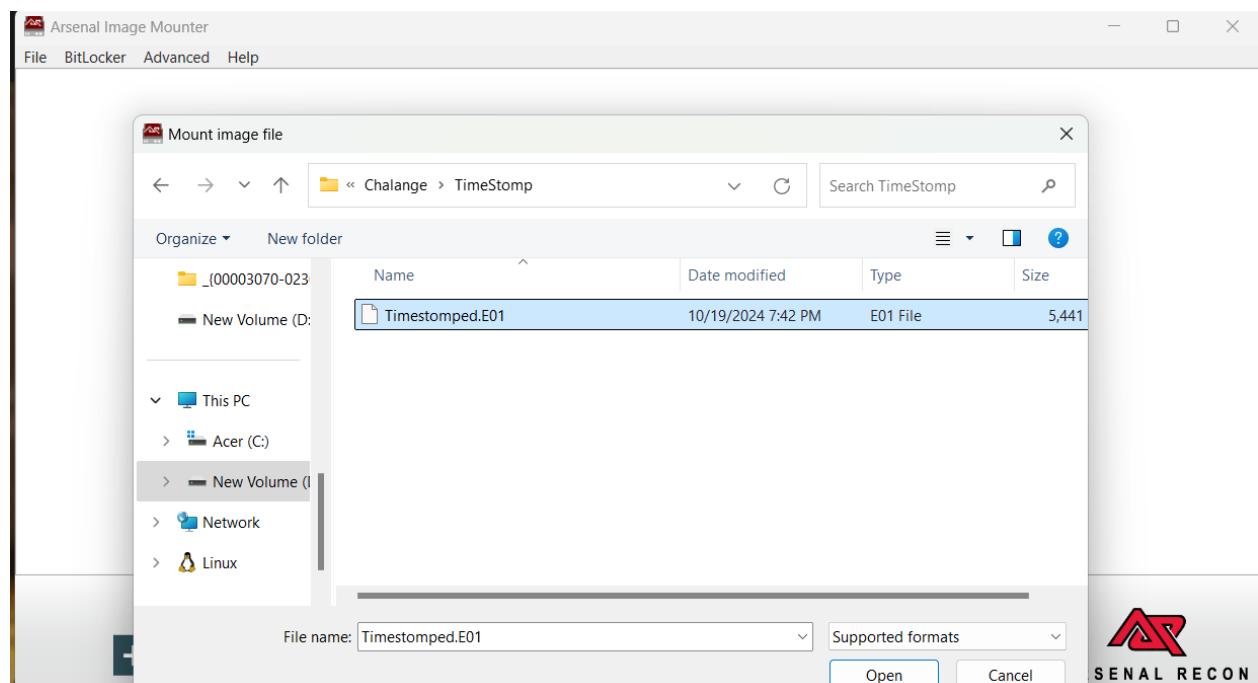
## **Lab 2: Hard Drive Forensics**

Bạn có thể truy xuất số thứ tự của file log đã bị thay đổi dấu thời gian không?

Link tải tài nguyên: [TimeStomp-20230919T073502Z-001.zip - Google Drive](#)

Name	Date modified	Type	Size
Details	10/19/2024 7:42 PM	Text Document	1 KB
Timestomped.E01	10/19/2024 7:42 PM	E01 File	5,441 KB
Walkthrough	10/19/2024 7:42 PM	GIF File	2,254 KB

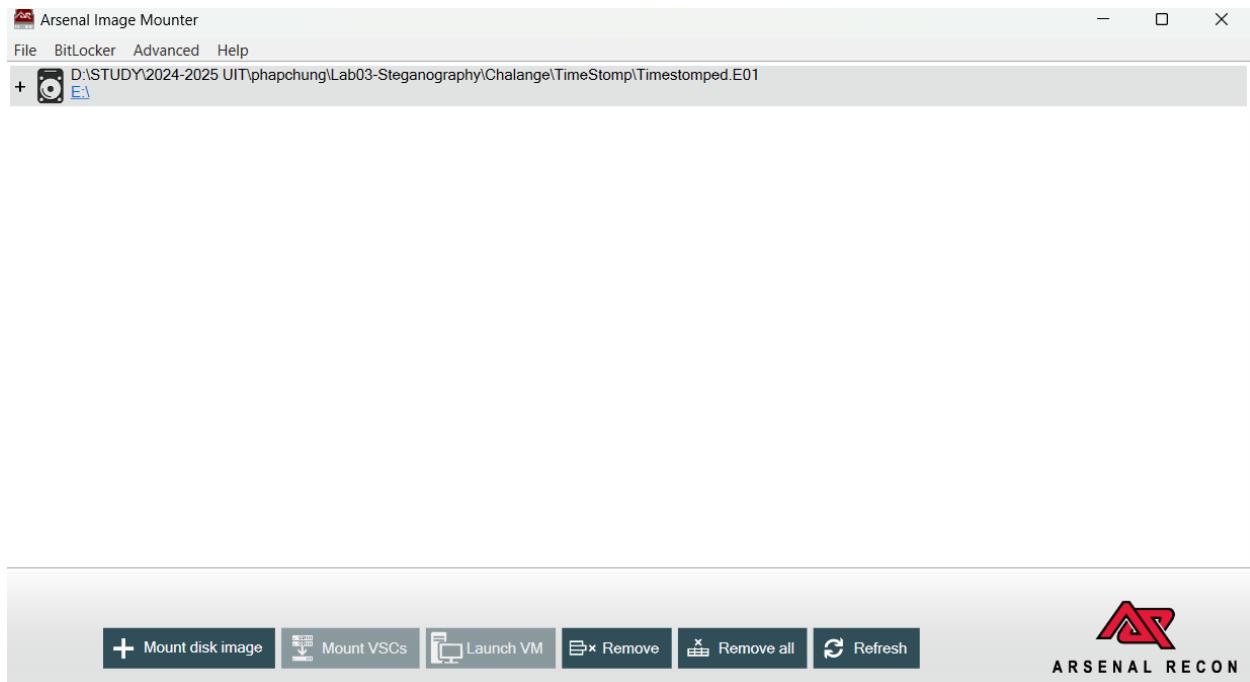
File có đuôi .E01 là một định dạng tệp được sử dụng để lưu trữ ảnh đĩa (disk image). Định dạng này thuộc về **EnCase Forensic Image**, được phát triển bởi Guidance Software. Chứa cấu trúc file system, dấu thời gian, và các dữ liệu khác.



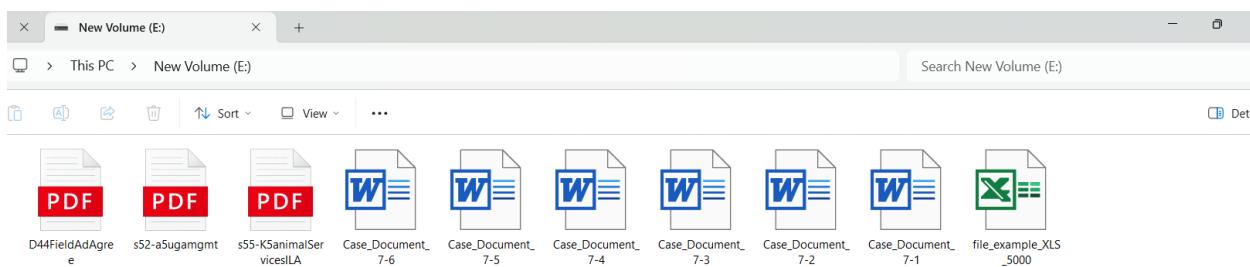
Gắn mount vào máy tính bằng công cụ Arsenal Image Mounter

## Lab 2: Hard Drive Forensics

39

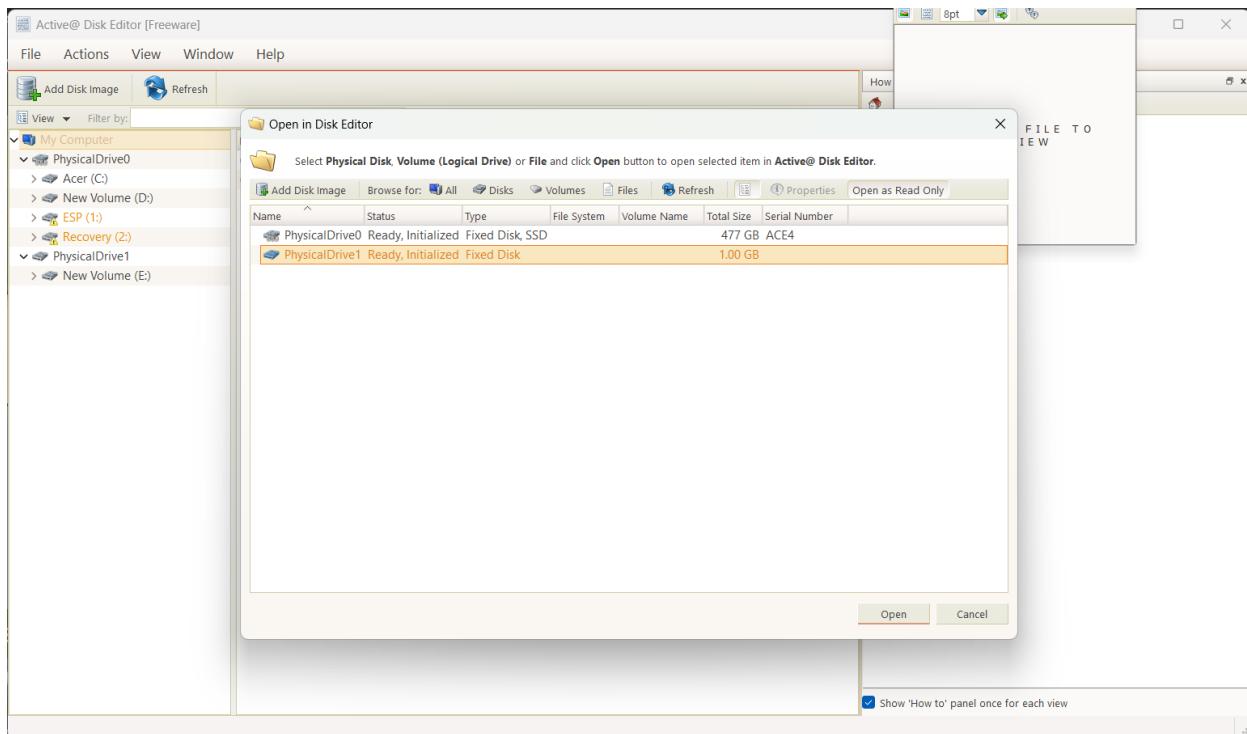


Lúc này ổ đĩa mới:

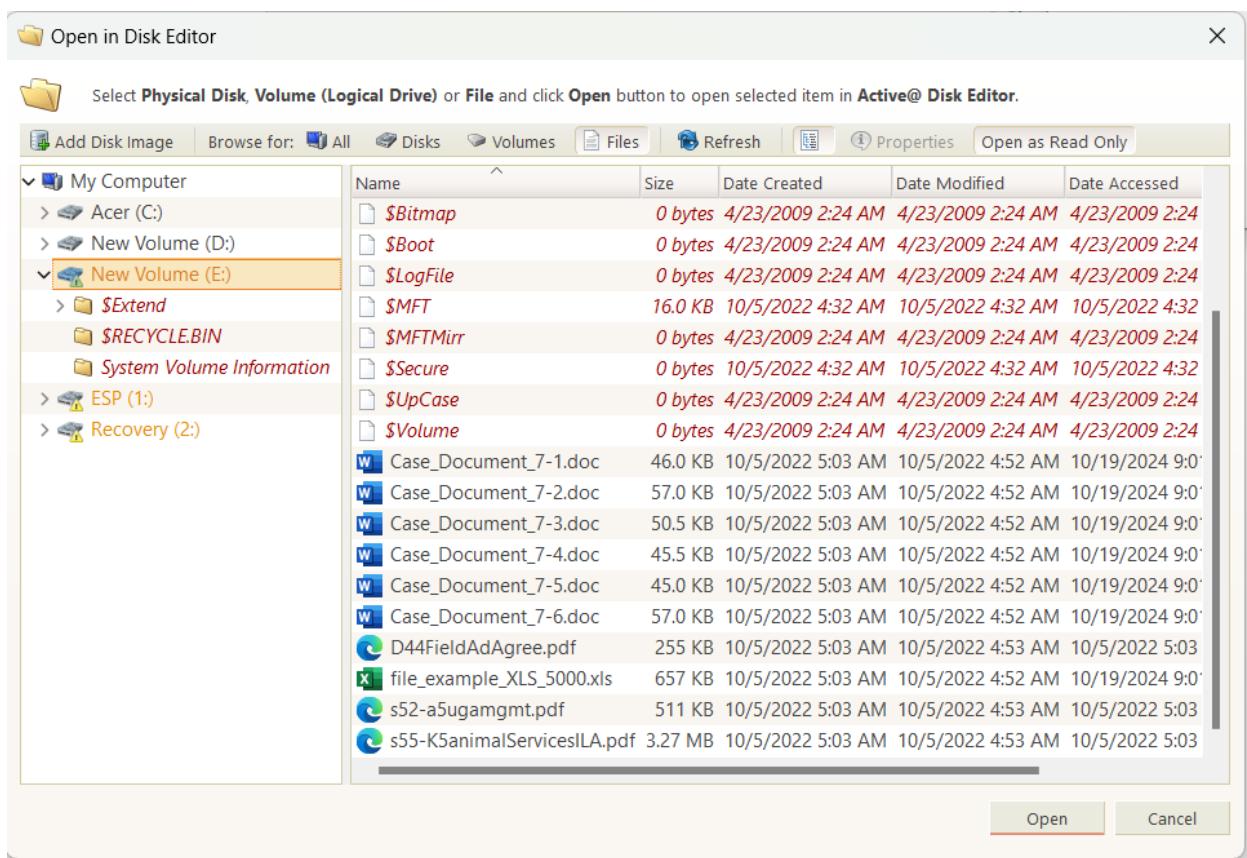


Sử dụng công cụ Active Disk Editor, đây là một công cụ phân tích ổ đĩa:

## Lab 2: Hard Drive Forensics



Mở ở đĩa mà chúng ta đã mount



## Lab 2: Hard Drive Forensics

<b>\$STANDARD_INF...</b>	<b>080</b>	
File created (UTC)	080	10/4/2022 10:03 PM
File modified (...)	088	10/4/2022 9:52 PM
Record change...	096	10/4/2022 9:52 PM
Last access tim...	104	10/19/2024 2:01 PM
> File Permissions	112	21 00 00 00
Maximum num...	116	0
Version number	120	0
Class Id	124	0
Owner Id	128	0
Security Id	132	264
Quota Charged	136	0
Update Sequen...	144	0

Thấy dấu thời gian ở \$STANDARD INFORMATION và \$FILENAME là không nhất quán

## Lab 2: Hard Drive Forensics

<b>\$FILE_NAME</b>	<b>176</b>	
Parent directory...	176	5
Parent directory...	182	5
File created (UTC)	184	10/4/2022 10:22 PM
File modified (...)	192	10/4/2022 10:22 PM
Record change...	200	10/4/2022 10:22 PM
Last access tim...	208	10/4/2022 10:22 PM
Allocated size	216	675,840
Real size	224	0
> File attributes	232	21 00 00 00
(used by EAs an...	236	0
File name length	240	25
File name name...	241	0
File name	242	file_example_XLS_5000.xls
<b>Attribute \$80</b>	<b>296</b>	
Attribute type	296	0x80

Active@ Disk Editor [Freeware]

File Edit Navigate View Window Help

Templates

NTFS MFT File Rec

Name	Offset	Value
Signature (must be 'FILE')	000	FILE
Offset to the update sequence	004	0x30
Update sequence size in words	006	3
<b>\$LogFile Sequence Number (LSN)</b>	<b>008</b>	<b>31,480,189</b>
Sequence number	016	2
Hard link count	018	1
Offset to the first attribute	020	0x38
> Flags	022	01 00
Real size of the FILE record	024	376

Flag: EGCERT{32480189}

*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](http://courses.uit.edu.vn).

### Đánh giá:

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

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

HẾT