

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.N21.ATCL

STT	Họ và tên	MSSV	Email
1	Lê Viết Tài Mẫn	20521593	20521593@gm.uit.edu.vn
2	Hoàng Thanh Lâm	20521513	20521513@gm.uit.edu.vn
3	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 1	100%
2	Kịch bản 2	100%
3	Kịch bản 3	100%
4	Kịch bản 4	100%
5	Kịch bản 5	100%
6	Kịch bản 6	100%

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

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

BÁO CÁO CHI TIẾT

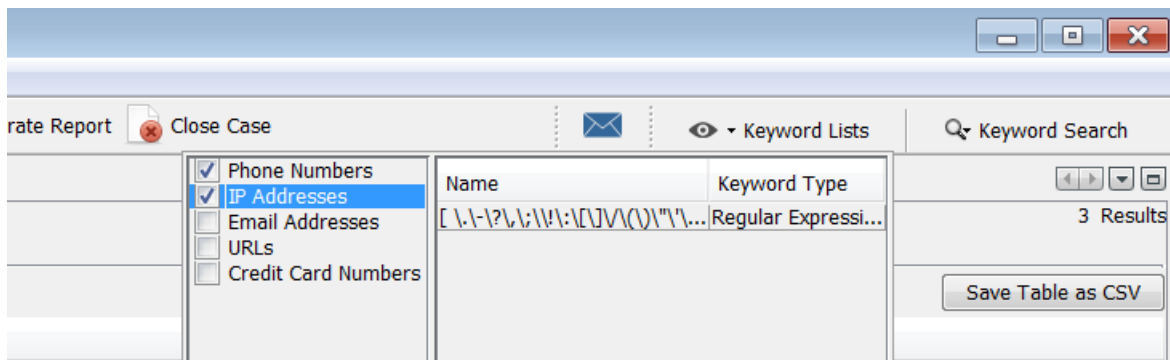
1. Kịch bản 1 - Thực hiện phân tích dựa trên dữ liệu ổ đĩa (tự chọn)

Kịch bản 01. Thực hiện phân tích dựa trên dữ liệu ổ đĩa (tự chọn)

- Chọn tìm các số điện thoại và địa chỉ IP có trong Filesystem.
- Thực hiện việc xem xét toàn bộ Filesystem, xem xét các lựa chọn nằm ở phía bên trái của màn hình.
- Tìm thư mục có nhiều File nhất trong Filesystem.
- Xem các file hình ảnh chứa trong Filesystem bằng chế độ view Thumbnail. Xác định số lượng các files dạng doc và pdf chứa trong Filesystem.
- Sử dụng nút "Generate Report" để tạo ra báo cáo dạng HTML và Excel, xem nội dung báo cáo trong mục Report. Nêu nhận xét, kết luận về nội dung của báo cáo.

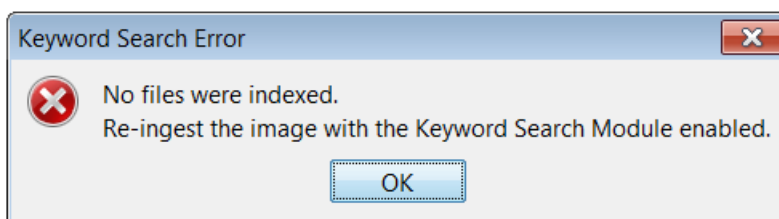
Đáp án:

- Ổ đĩa lựa chọn là ổ D trong máy ảo Win 7
- **Chọn tìm các số điện thoại và địa chỉ IP có trong Filesystem.**

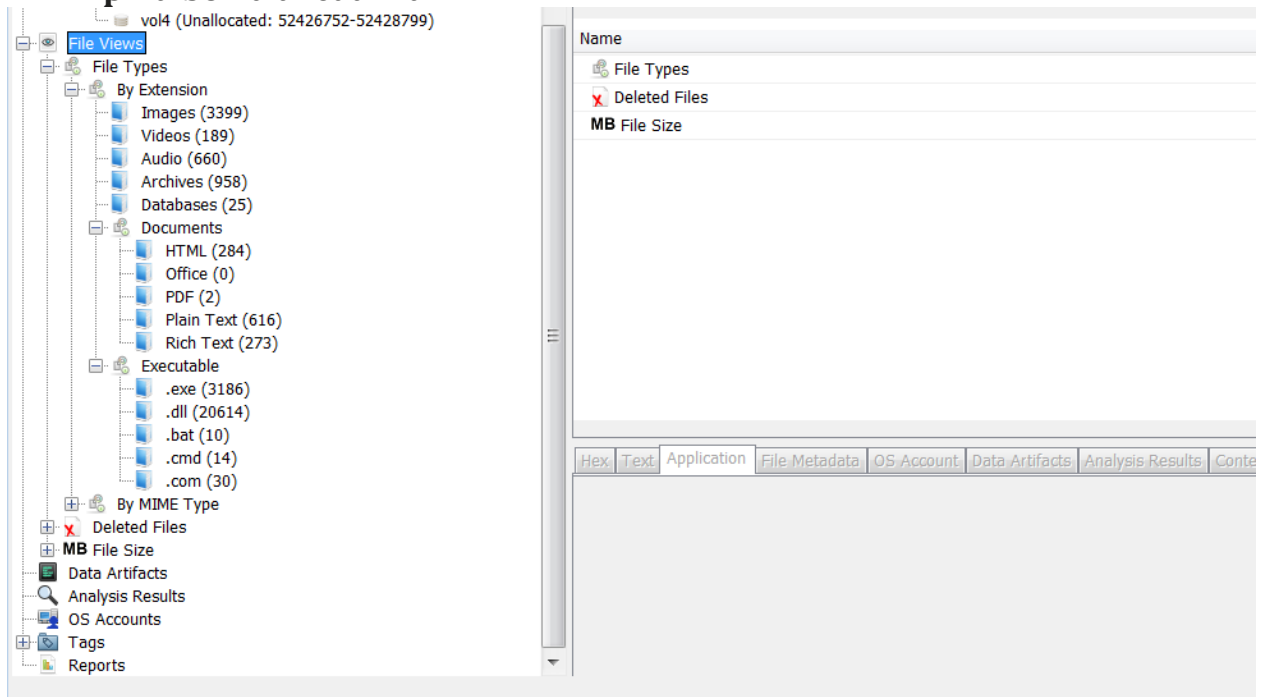


- Kết quả: Không tìm kiếm được gì

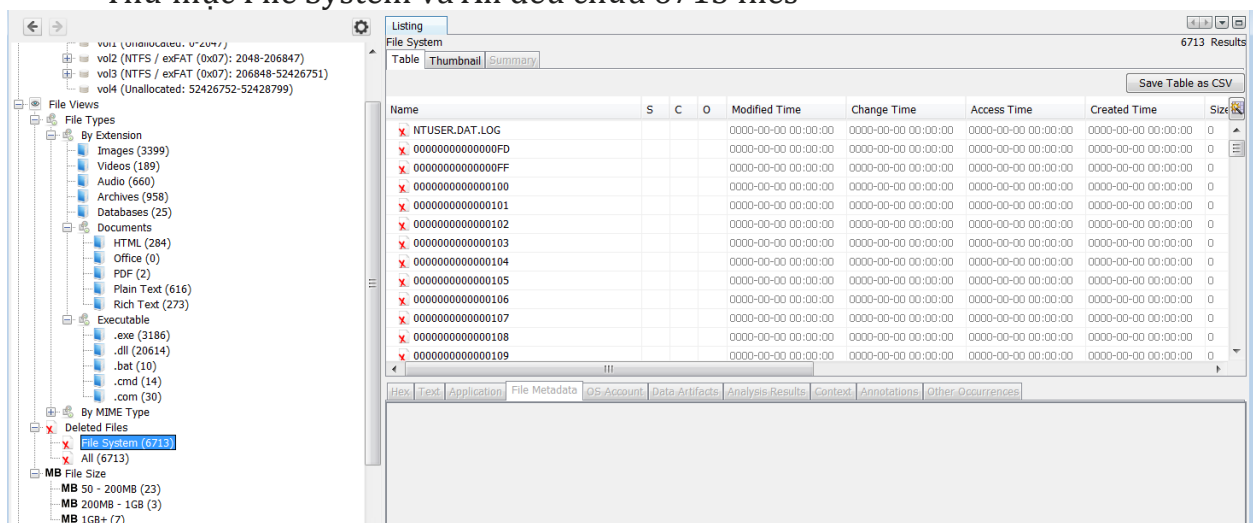
THE SIZE



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

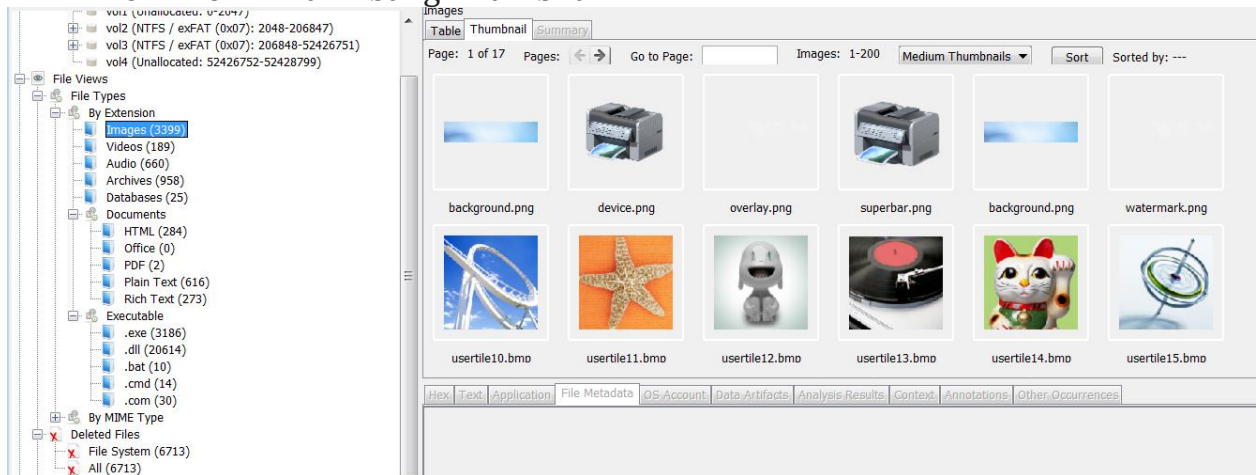


- Tìm thư mục có nhiều File nhất trong Filesystem.
Thư mục File System và All đều chứa 6713 files

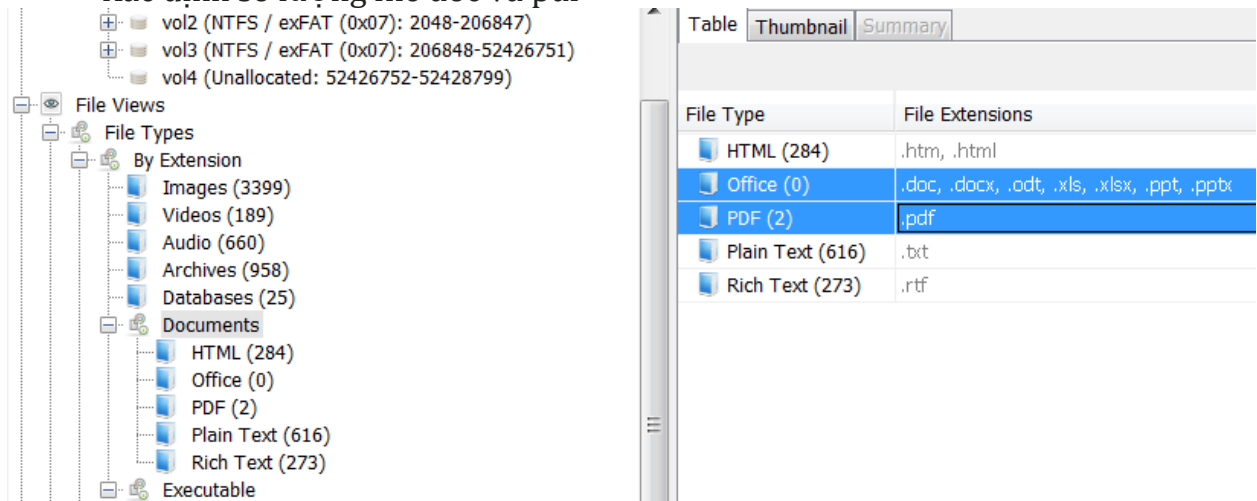


- Xem các file hình ảnh chứa trong Filesystem bằng chế độ view Thumbnail. Xác định số lượng các files dạng doc và pdf chứa trong Filesystem.

Xem file hình ảnh bằng Thumbnail



Xác định số lượng file doc và pdf



Doc: 0

Pdf: 2

- Sử dụng nút "Generate Report" để tạo ra báo cáo dạng HTML và Excel, xem nội dung báo cáo trong mục Report. Nêu nhận xét, kết luận về nội dung của báo cáo.
 - o HTML Report: Bản tóm tắt các thông tin chính bao gồm các thông tin về case name, số lượng data source, thông tin hình ảnh, múi giờ, đường dẫn tới ổ cứng khai thác, phiên bản ứng dụng và ingest history (theo tìm hiểu thì đây là lịch sử truy cập dữ liệu để phân tích hoạt động của người dùng)

Report Navigation

- Case Summary
- ★ Tagged Files (0)
- ★ Tagged Images (0)
- ★ Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2023/04/19 15:01:13

Case: kb01
Number of data sources in case: 1

Image Information:

PhysicalDrive0

Timezone: Asia/Bangkok
Path: \\.\PhysicalDrive0

Software Information:

Autopsy Version: 4.20.0

Ingest History:

- Exel Report: Chỉ gồm 2 thông tin là Casename và số lượng data sources trong case này

	A	B	C	D
1	Summary			
2				
3	Case Name:	kb01		
4	Number of data sources in case:	1		
5				
6				
7				

2. Kịch bản 2 - Thực hiện phân tích dựa trên tài nguyên được cung cấp.

- Hãy tìm tất cả những hình ảnh có trong ổ đĩa đã cho.
- 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, xóa, sửa, MD5, kích thước hình ảnh ...

Đáp án:

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

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: kb02

Base Directory: C:\Users\Admin\Desktop\HKII 2022-2023\Pháp chứng kỹ thuật số\Thực hành\Lab2\Lab2\ Browse

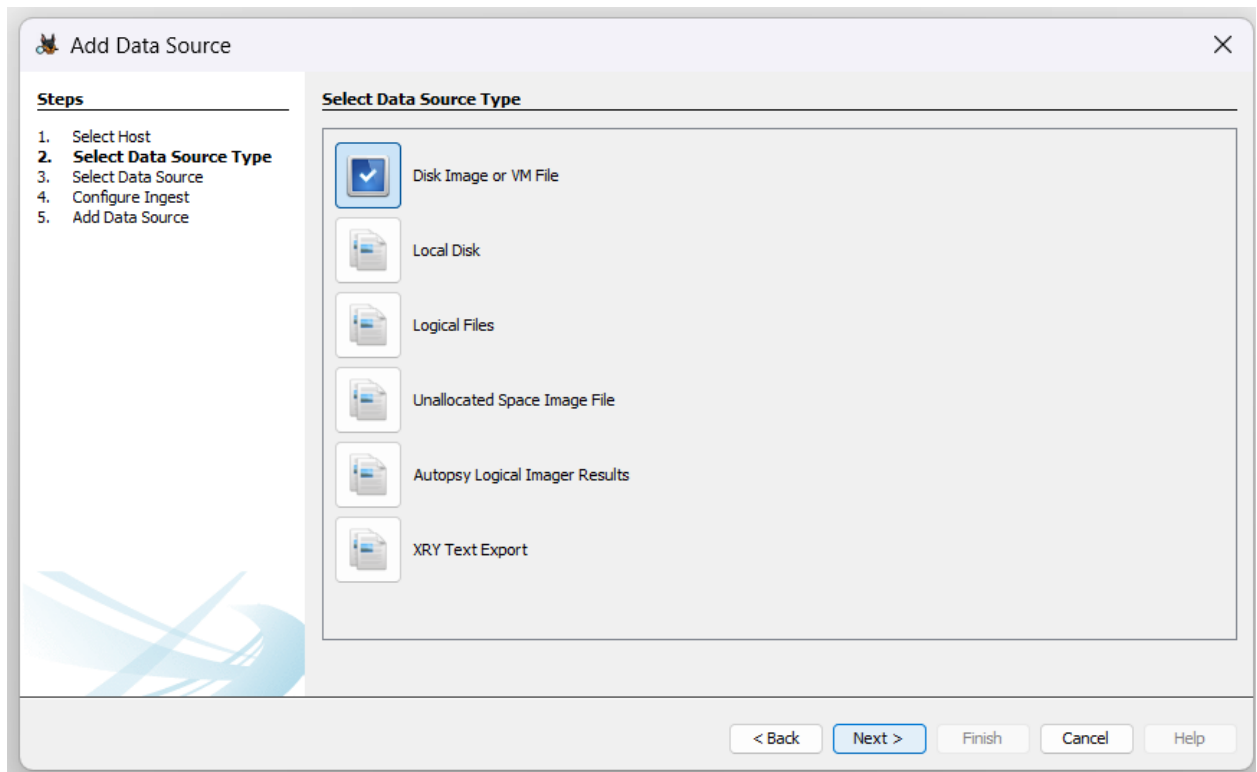
Case Type: ☒ Single-User ☐ Multi-User

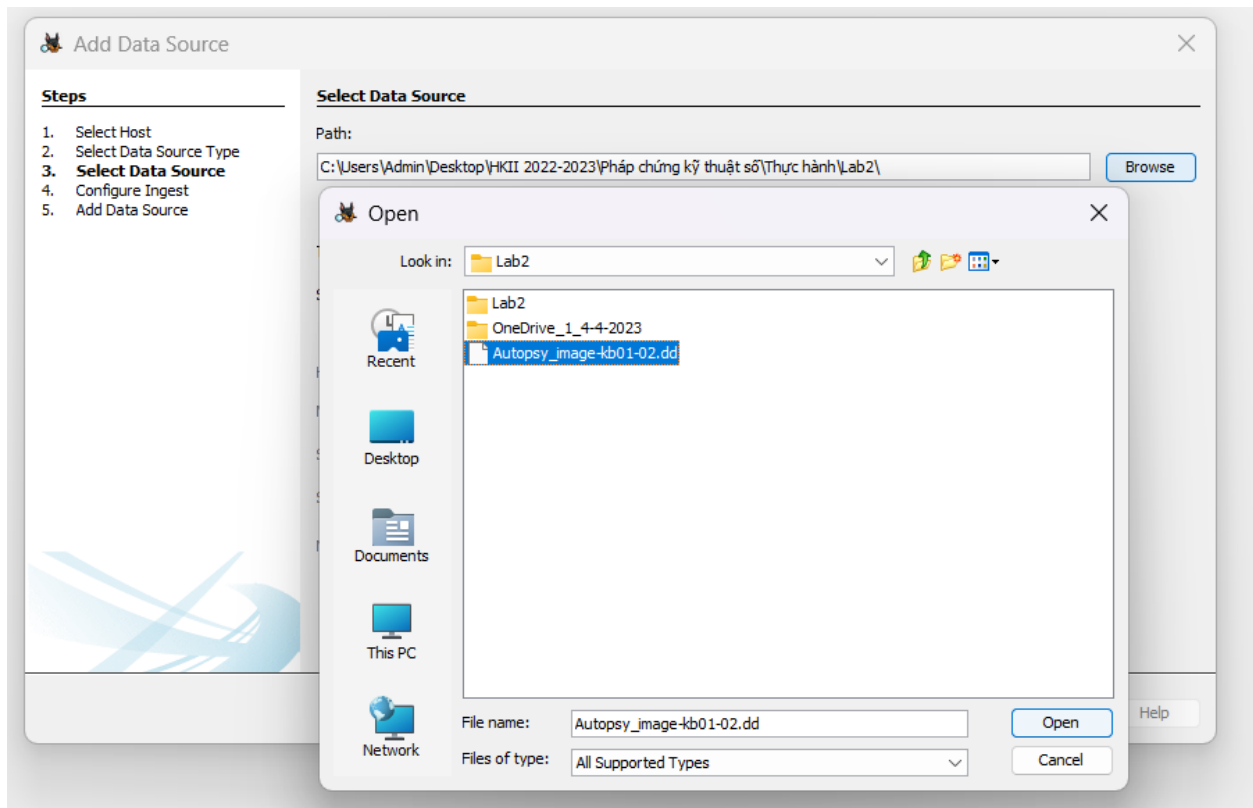
Case data will be stored in the following directory:

C:\Users\Admin\Desktop\HKII 2022-2023\Pháp chứng kỹ thuật số\Thực hành\Lab2\Lab2\kb02

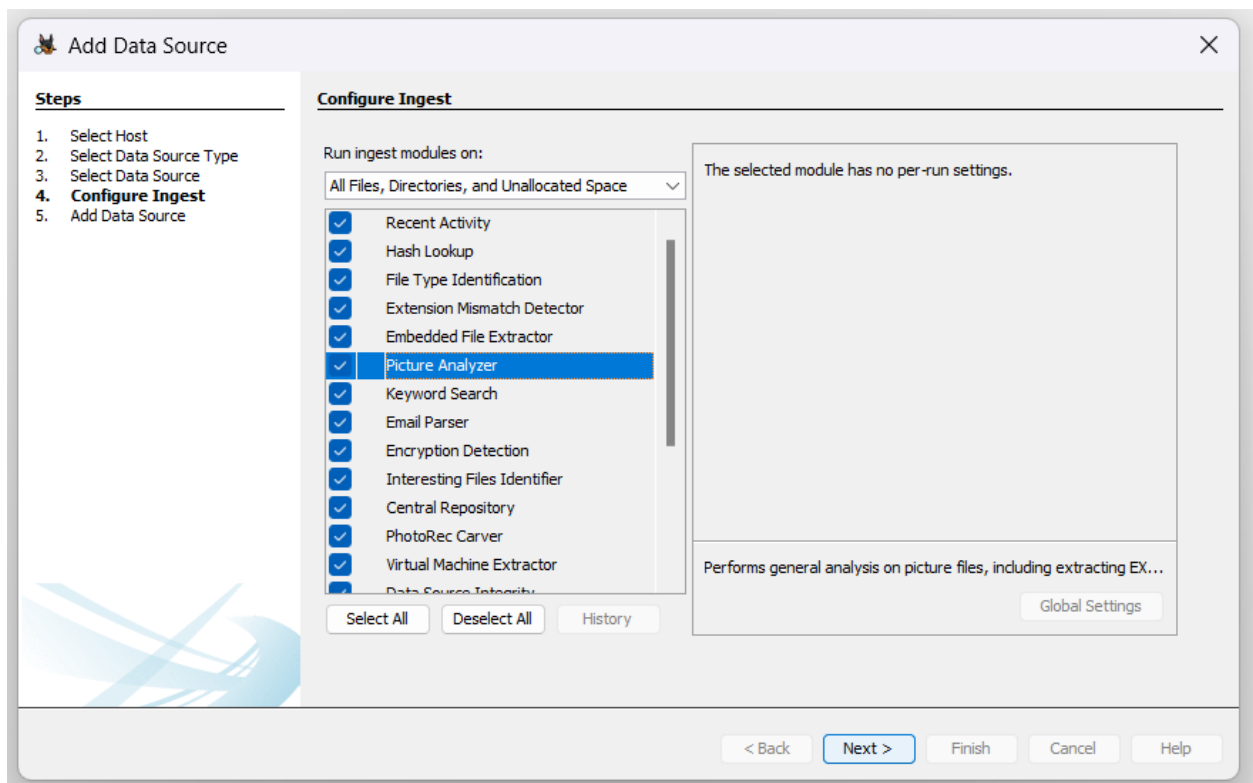
< Back Next > Finish Cancel Help

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



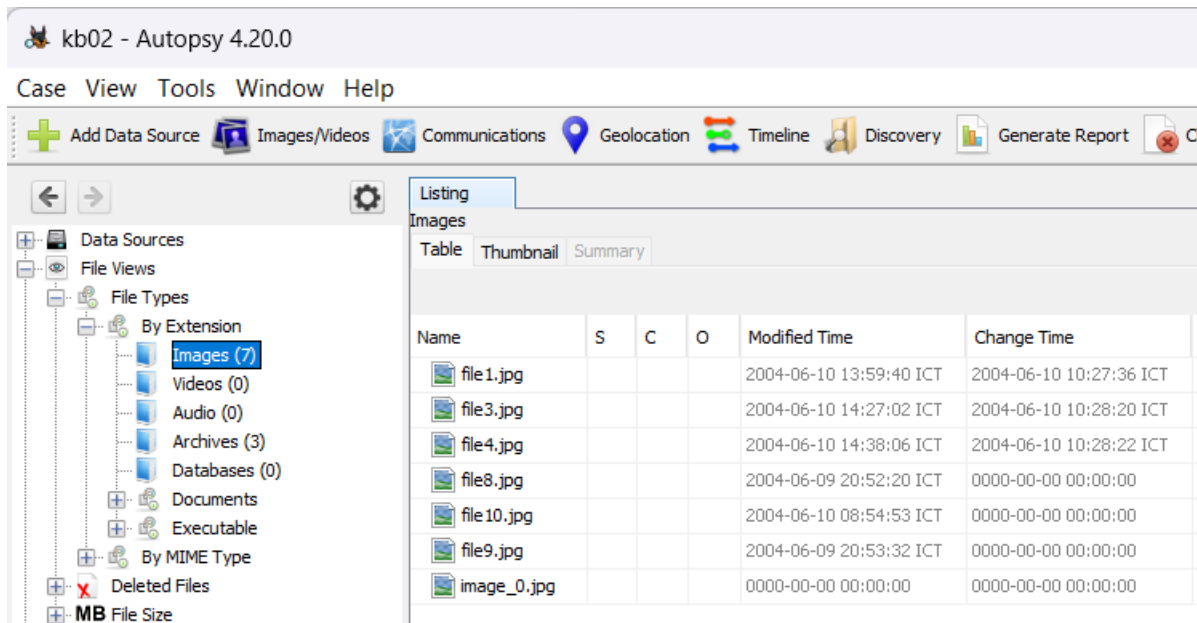


- Chọn các module cần phân tích










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

- **Tìm tất cả các hình ảnh**
File Views -> File Types -> By Extension



- **Liệt kê thông tin liên quan tới các file ảnh tìm được**

Listing																7 Results	
Images																	
Table Thumbnail Summary																	
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash	MIME Type	Extension	
 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-Hb01-02-dd/invalidfile1.jpg				jpg	
 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-Hb01-02-dd/invalidfile3.jpg				jpg	
 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-Hb01-02-dd/allocfile1.jpg				jpg	
 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-Hb01-02-dd/archivefile8.zip/file8.jpg				jpg	
 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-Hb01-02-dd/archivefile10.tar.gz/file...				jpg	
 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-Hb01-02-dd/archivefile9.boof/boof.jpg				jpg	
 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-Hb01-02-dd/misc/file12.doc/image_0...				jpg	

3. Kịch bản 3 - Thực hiện phân tích theo kịch bản mô tả

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

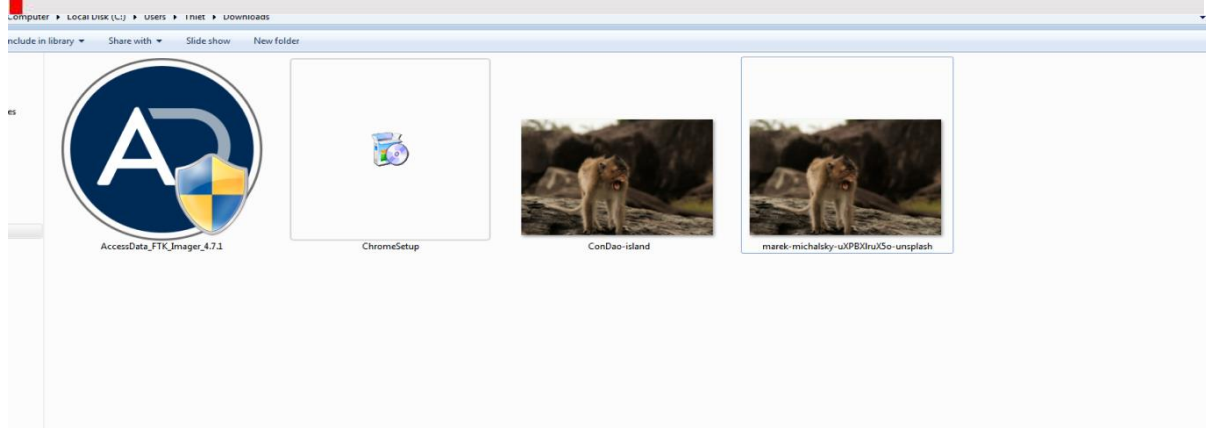
- Trên máy tính/máy ảo windows thực hiện tải về hình ảnh và đặt tên ConDao-island.
- Liên kết tải: <https://unsplash.com/photos/uXPBXlruX5o>
- Thực hiện xóa file ảnh vừa tạo, xóa trong Recycle Bin.
- Tạo một ảnh đĩa -định dạng Raw (dd) sau khi xóa file ảnh trên.
 - Case Number: April_0001
 - Evidence 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:

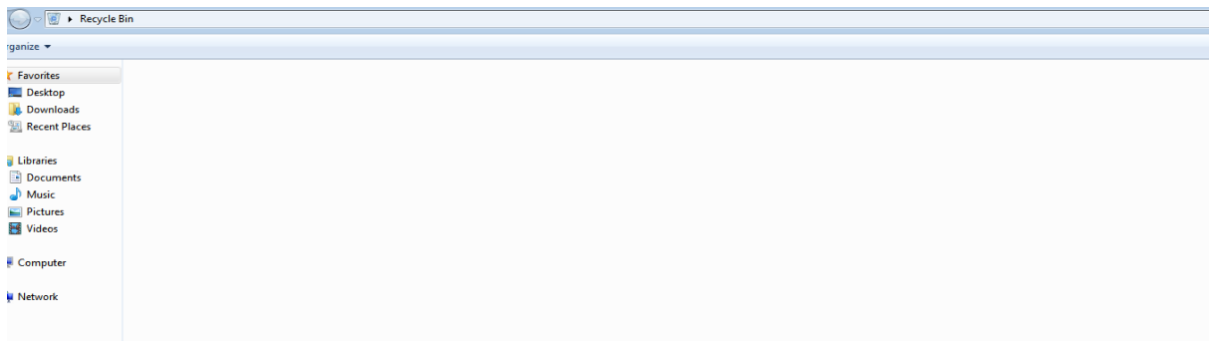
```
dir D:\KB03 | findstr "ConDao-island"
```

```
date /t
```

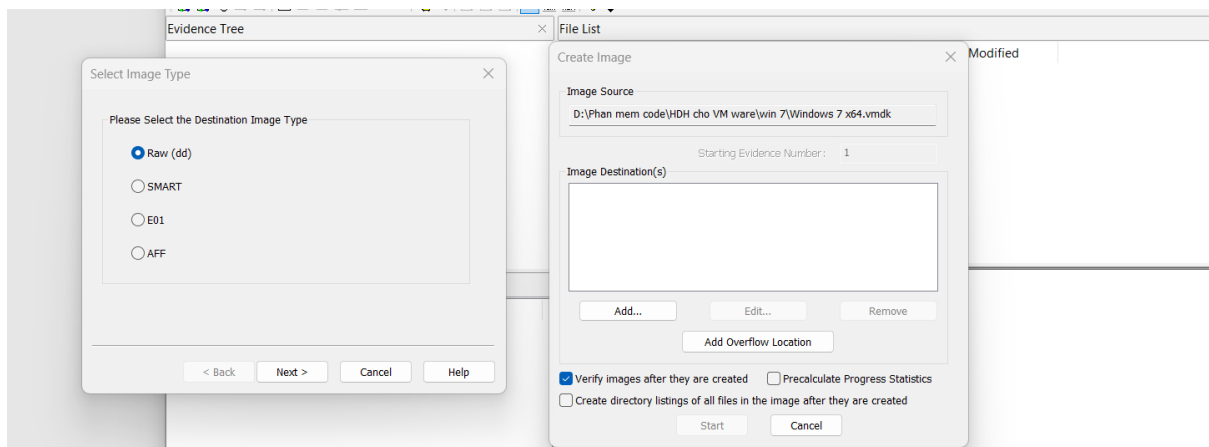
```
echo "Tên nhóm"
```



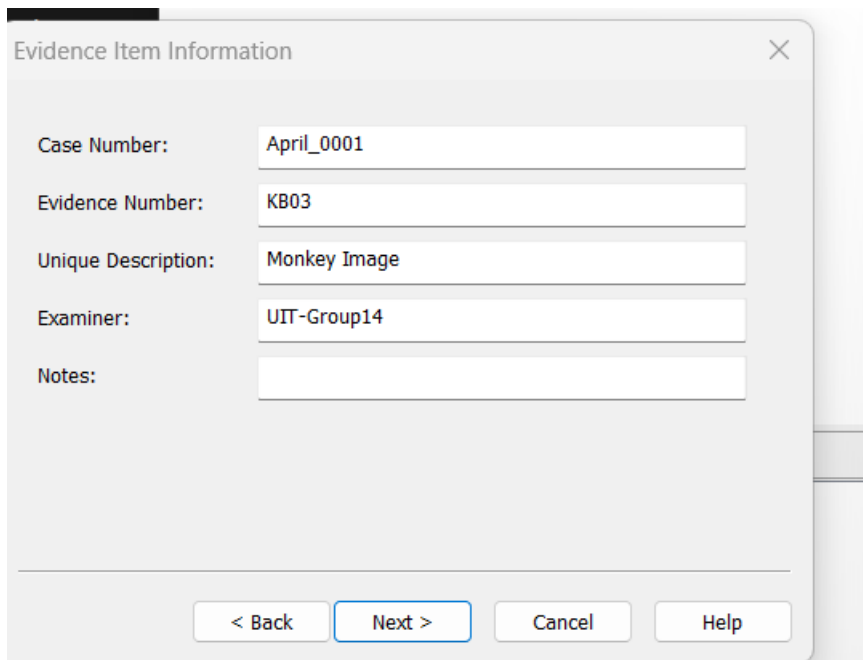
- Trên máy ảo win 7 ta tải file ảnh về sau đó đổi tên “ConDao-island”



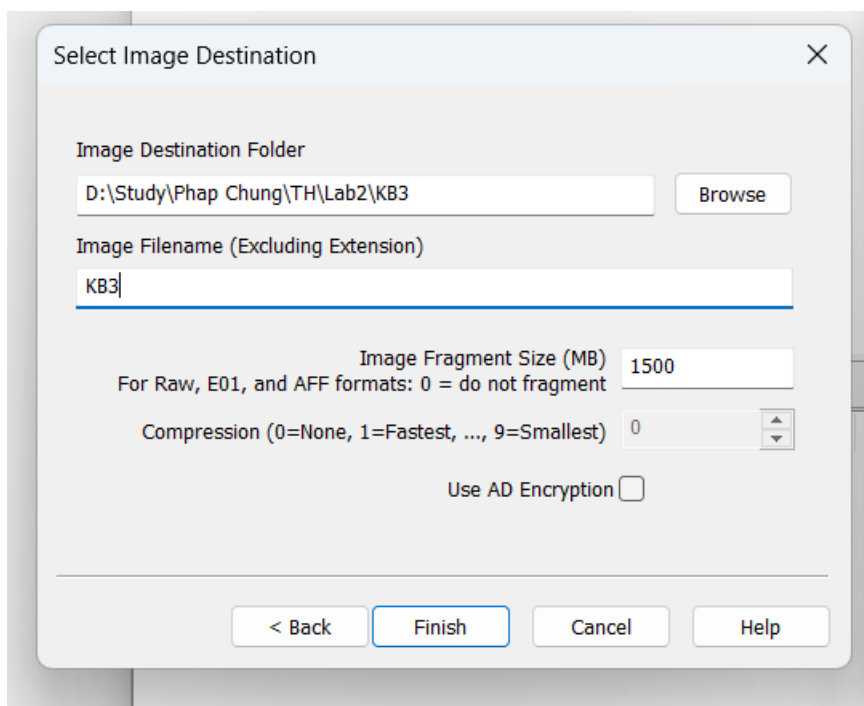
- Ta thực hiện xóa ảnh, Xóa luôn trong recycle bin



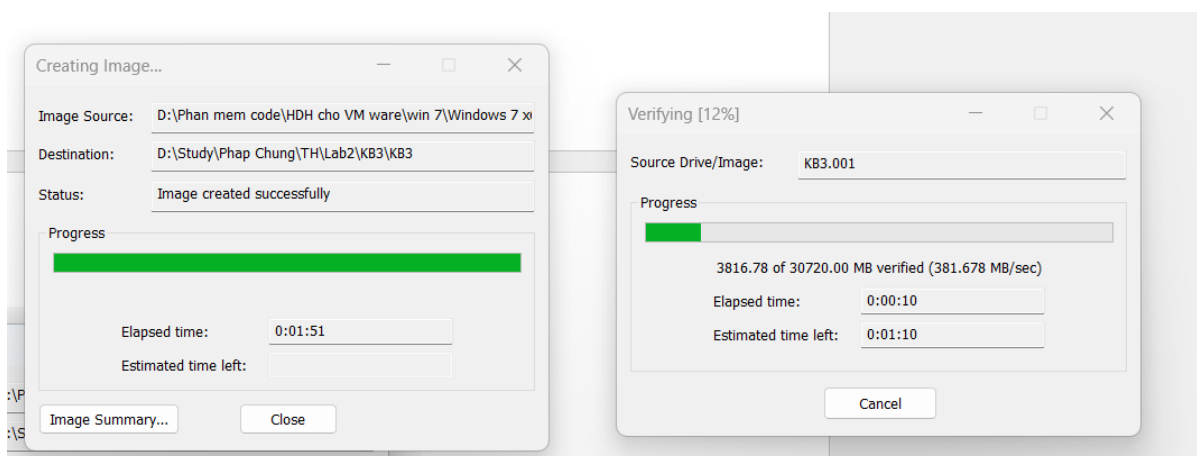
- Tạo một ảnh đĩa -định dạng Raw (dd) sau khi xóa file ảnh trên



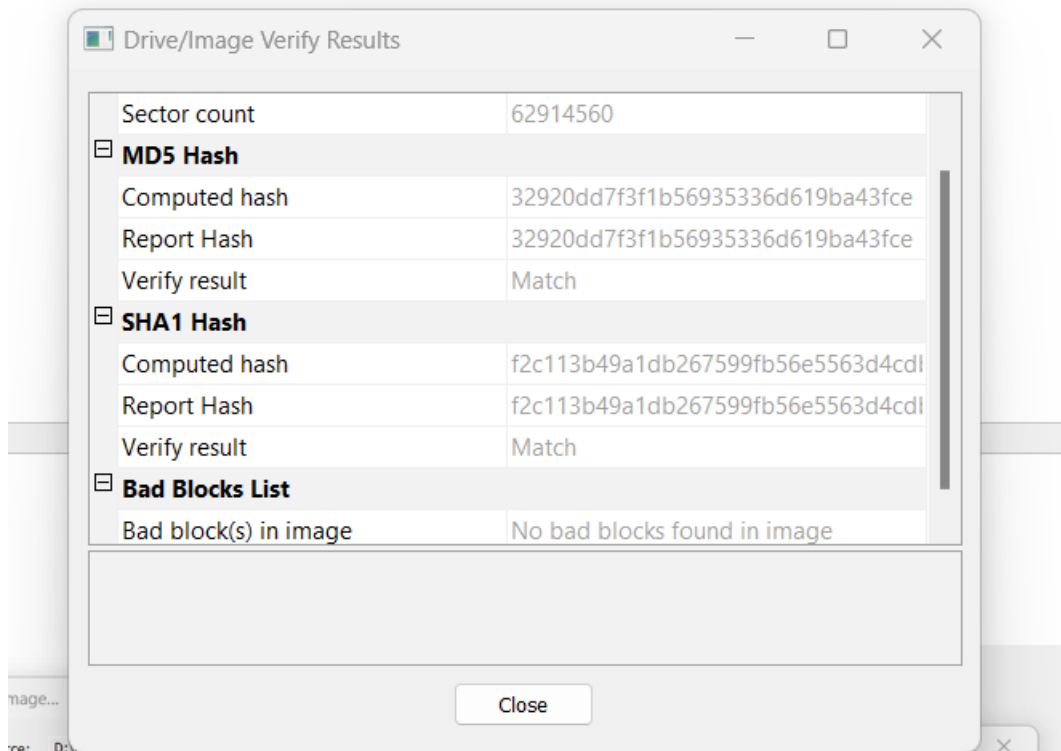
- Đặt tên theo yêu cầu



- Ta lưu vào 1 folder và đặt tên là KB3



- Đợi quá trình tạo disk image hoàn tất

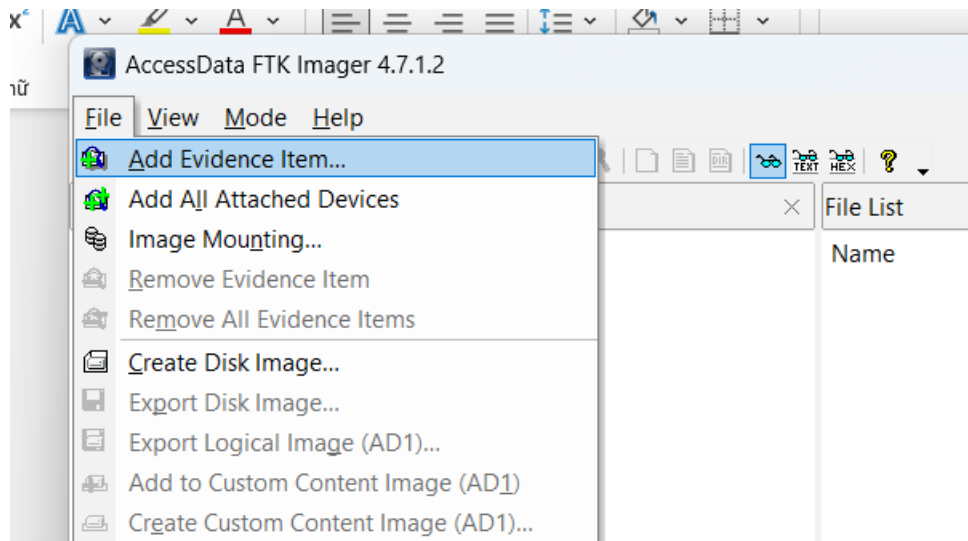


- Sau khi hoàn tất thì ta có bảng tóm tắt disk image vừa tạo

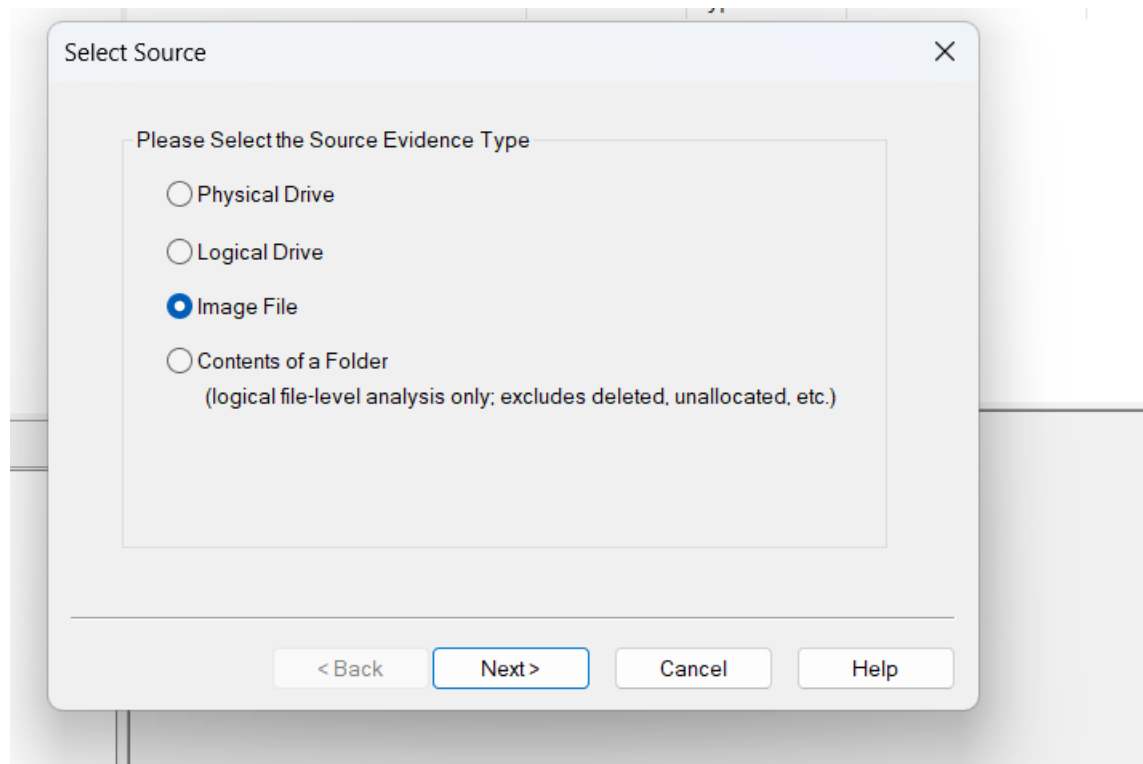
File Explorer view showing the contents of the 'KB3' folder:

Name	Date modified	Type	Size
KB3.001	4/19/2023 1:52 PM	WinRAR archive	1,536,000 ...
KB3.001.txt	4/19/2023 1:55 PM	Tài liệu văn bản	3 KB
KB3.002	4/19/2023 1:52 PM	002 File	1,536,000 ...
KB3.003	4/19/2023 1:52 PM	003 File	1,536,000 ...
KB3.004	4/19/2023 1:53 PM	004 File	1,536,000 ...
KB3.005	4/19/2023 1:53 PM	005 File	1,536,000 ...
KB3.006	4/19/2023 1:53 PM	006 File	1,536,000 ...
KB3.007	4/19/2023 1:53 PM	007 File	1,536,000 ...
KB3.008	4/19/2023 1:53 PM	008 File	1,536,000 ...
KB3.009	4/19/2023 1:53 PM	009 File	1,536,000 ...
KB3.010	4/19/2023 1:53 PM	010 File	1,536,000 ...
KB3.011	4/19/2023 1:53 PM	011 File	1,536,000 ...
KB3.012	4/19/2023 1:53 PM	012 File	1,536,000 ...

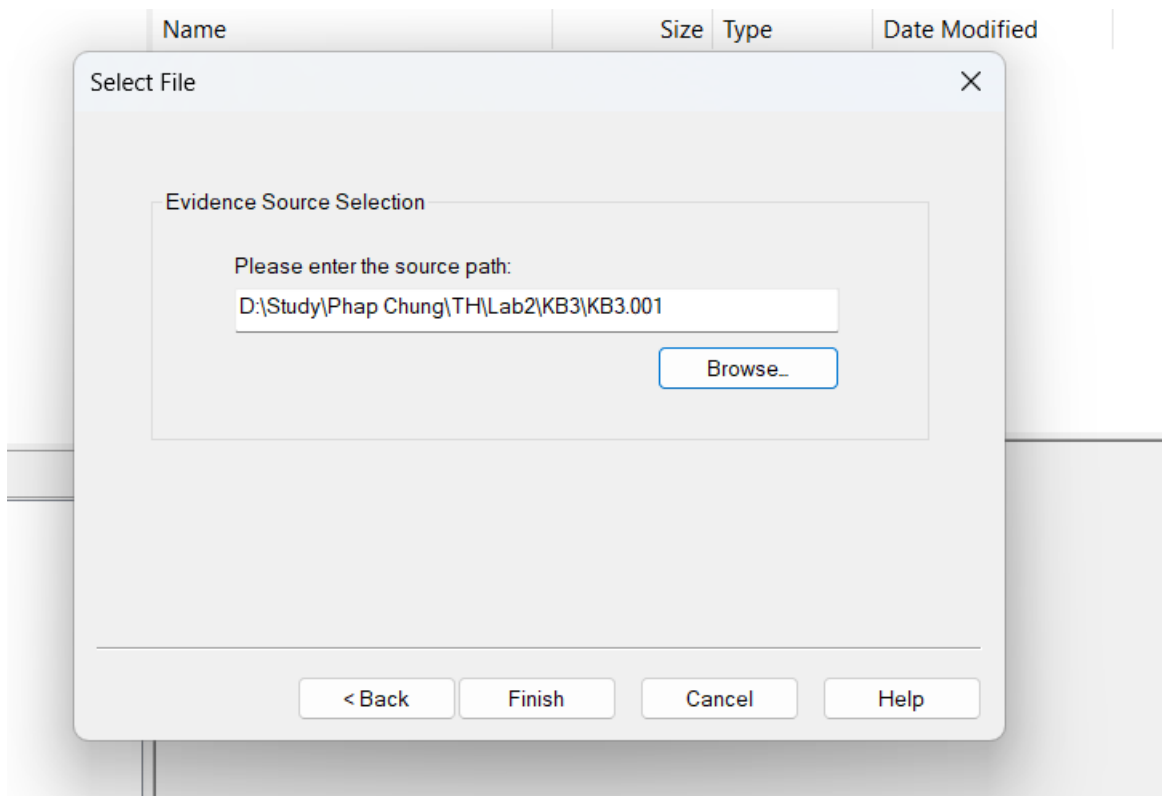
- Trong thư mục KB3 vừa tạo chứa disk image ta vừa tạo



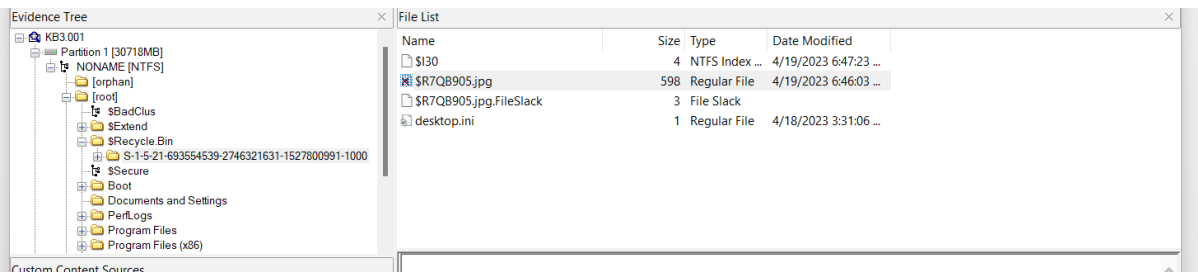
- Để thêm bằng chứng ta chọn file -> add evidence item



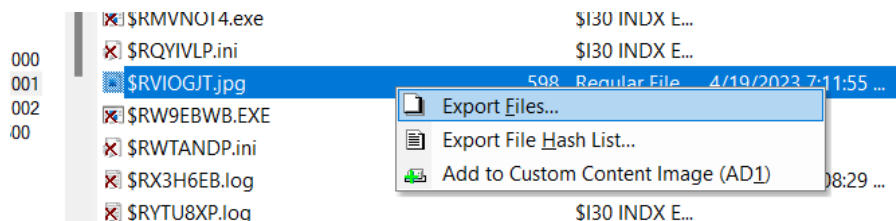
- Chọn image file



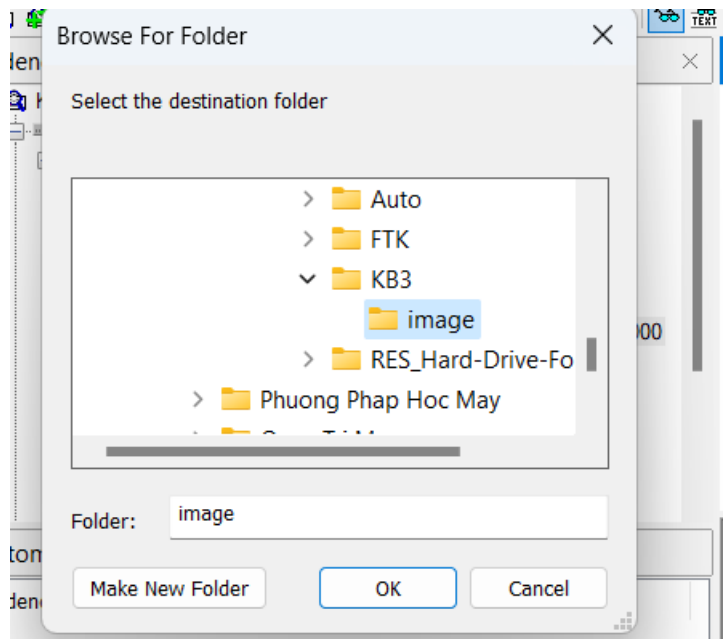
- Ta chọn disk image vừa tạo trong folder KB03



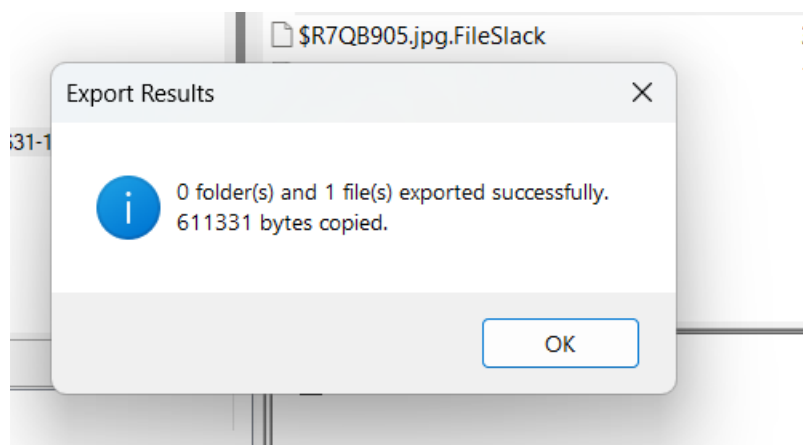
- Sử dụng tính năng phục hồi file ảnh đã bị xóa (tính năng Export Files), lưu trữ file này trong thư mục KB03\images.
- Ta để ý file ảnh của ta có kích thước 598kb trùng với kích thước file ảnh ta tải về



- Sử dụng tính năng export file để phục hồi



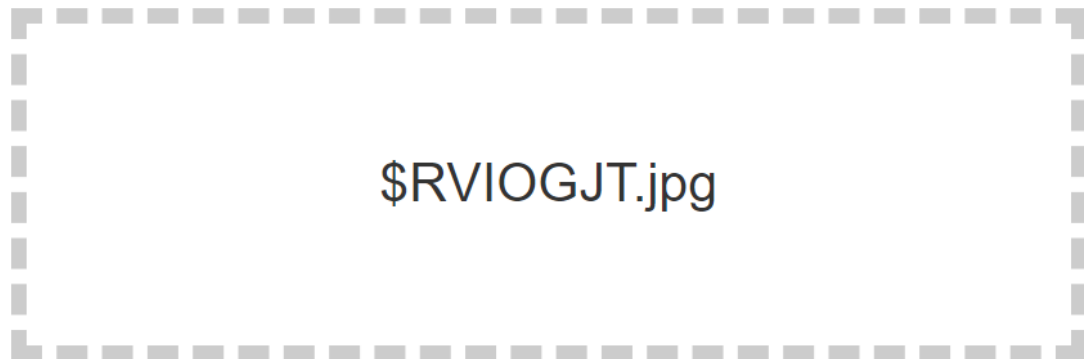
- Lưu vào thư mục KB3/image



- Ta phục hồi thành công

MD5 File Checksum

MD5 online hash file checksum function



Hash

☒ Auto Update

9ee18830b6c7d85abcc9c570686463e6

MD5 File Checksum

MD5 online hash file checksum function

ConDao-island.jpg

Hash ☒ Auto Update

9ee18830b6c7d85abcc9c570686463e6

- Mã MD5 hash giống nhau vậy là cùng 1 file

```
C:\Users\Thiet>dir "D:\Study\Phap Chung\TH\Lab2\KB3\image" | findstr "ConDao-island"
04/19/2023  02:06 PM                611,331 ConDao-island.jpg

C:\Users\Thiet>date /t
Wed 04/19/2023

C:\Users\Thiet>echo "Group14-UIT"
"Group14-UIT"

C:\Users\Thiet>
```

4. Kịch bản 4 – Phân tích tài nguyên có sẵn

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:

- Phân tích bằng kali với các gợi ý được cung cấp
- Giải nén bằng gunzip và xác định raw disk image bằng lệnh file

```
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ ls
bb1s_rel6_student.pdf kb04-session02.bin.gz
(kali@kali)-[~/Downloads]
$ gunzip kb04-session02.bin.gz
(kali@kali)-[~/Downloads]
$ ls
bb1s_rel6_student.pdf kb04-session02.bin
(kali@kali)-[~/Downloads]
$ file kb04-session02.bin
kb04-session02.bin: DOS/MBR boot sector; partition 1 : ID=0x7, start-CHS (0x1,0,1), end-CHS (0x3fa,0,31), startsector 31, 31558 sectors, extended partition table (last)
(kali@kali)-[~/Downloads]
$
```

- Hiển thị phân vùng hợp lệ bằng lệnh **fdisk -lu kb04-session02.bin**

```
(kali@kali)-[~/Downloads]
$ fdisk -lu kb04-session02.bin
Disk kb04-session02.bin: 15.44 MiB, 16187392 bytes, 31616 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device                Boot Start    End Sectors  Size Id Type
kb04-session02.bin1    31 31588   31558 15.4M  7 HPFS/NTFS/exFAT

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

- Dựa vào gợi ý và tìm hiểu, ta biết được cách sử dụng lệnh **mmls** để hiển thị thông tin về các phân vùng trong một hệ thống tệp đĩa

```
(kali㉿kali)-[~/Downloads]
$ mmls kb04-session02.bin
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot      Start      End      Length    Description
000:  Meta      0000000000  0000000000  0000000001  Primary Table (#0)
001:  _____ 0000000000  0000000030  0000000031  Unallocated
002:  000:000  0000000031  0000031588  0000031558  NTFS / exFAT (0x07)
003:  _____ 0000031589  0000031615  0000000027  Unallocated

(kali㉿kali)-[~/Downloads]
$ ss
```

- Tiếp theo ta tiến hành trích xuất từng phân vùng để tránh tác động lên dữ liệu gốc, ở đây ta sử dụng lệnh dd, kết hợp các thông tin về các phân vùng đã có được ở bước 3
 - o Tiến hành phân tích sử dụng kali với các gợi ý
 - Phân vùng 0

```
(kali@kali)-[~/Downloads]
$ dd if=kb04-session02.bin of=kb04-session02_cau4_pv0.bin bs=512 count=1 skip=0
1+0 records in
1+0 records out
512 bytes copied, 0.000240301 s, 2.1 MB/s

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

- Phân vùng 1

```
(kali@kali)-[~/Downloads]
$ dd if=kb04-session02.bin of=kb04-session02_cau4_pv1.bin bs=512 count=31 skip=0
31+0 records in
31+0 records out
15872 bytes (16 kB, 16 KiB) copied, 0.001182 s, 13.4 MB/s

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

- Phân vùng 2

```
(kali@kali)-[~/Downloads]
$ dd if=kb04-session02.bin of=kb04-session02_cau4_pv2.bin bs=512 count=31 skip=31558
31+0 records in
31+0 records out
15872 bytes (16 kB, 16 KiB) copied, 0.000679702 s, 23.4 MB/s

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

- Phân vùng 3

```
(kali@kali)-[~/Downloads]
$ dd if=kb04-session02.bin of=kb04-session02_cau4_pv3.bin bs=512 count=27 skip=31589
27+0 records in
27+0 records out
13824 bytes (14 kB, 14 KiB) copied, 0.000642702 s, 21.5 MB/s

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

Trong đó:

- If: tên và đường dẫn tới tệp tin ta cần sao chép/trích xuất
- Of: tên và đường dẫn của tệp tin đầu ra mong muốn
- Bs: Kích thước khối đọc và ghi, ở đây là 512 byte
- Count: số lượng khối sẽ được đọc và ghi, ở đây là 1

Skip: số lượng block trong tệp gốc sẽ bị bỏ qua

- Tiếp theo ta tiến hành trích xuất từng phân vùng để tránh tác động lên dữ liệu gốc, ở đây ta sử dụng lệnh dd, kết hợp các thông tin về các phân vùng đã có được ở bước 3

```
(kali㉿kali)-[~/Downloads]
$ strings kb04-session02_cau4_pv3.bin
Mustapha Laden          972-3-5197575
Hank Huessein           00-1-703-343-7604
Samir Nagheenanajar     9661-4883800
Pete Mitchell           843-234-2342
Tom Kazanski            343-343-2343
Pete Gibbons            234-324-2342
Hans Gruber             49-89-2888-0
Wah Sing Ku             011-81-3-3224-5000
sf8D
aN3jl:
ajid
sometimesisitreal
24jssj.
sometimes it is not real
strings suck
where0where15thek3y?
keyfile.dat

(kali㉿kali)-[~/Downloads]
$ strings kb04-session02_cau4_pv2.bin
NTFS
NTFSu
TCPAu$
fSfSfU
fY[ZfYfY
A disk read error occurred
BOOTMGR is missing
BOOTMGR is compressed
Press Ctrl+Alt+Del to restart

(kali㉿kali)-[~/Downloads]
$ strings kb04-session02_cau4_pv1.bin

(kali㉿kali)-[~/Downloads]
$ strings kb04-session02_cau4_pv0.bin

(kali㉿kali)-[~/Downloads]
$
```

- Kết quả: Không tìm được gì hữu ích

- Ta sử thử xem ở dạng hex-dump
 - o Phân vùng 3

```
(kali@kali)~[~/Downloads]
$ hexdump -C kb04-session02_cau4_pv3.bin
00000000 4d 75 73 74 61 70 68 61 20 4c 61 64 65 6e 09 09 |Mustapha Laden..|
00000010 39 37 32 2d 33 2d 35 31 39 37 35 37 35 0d 0a 48 |972-3-5197575...H|
00000020 61 6e 6b 20 48 75 65 73 73 65 69 6e 09 09 30 30 |ank Huessein..00|
00000030 2d 31 2d 37 30 33 2d 33 34 33 2d 37 36 30 34 0d |-1-703-343-7604.|
00000040 0a 53 61 6d 69 72 20 4e 61 67 68 65 65 6e 61 6e |.Samir Nagheenan|
00000050 61 6a 61 72 09 39 36 36 31 2d 34 38 38 33 38 30 |ajar.9661-488380|
00000060 30 0d 0a 50 65 74 65 20 4d 69 74 63 68 65 6c 6c |0..Pete Mitchell|
00000070 09 09 38 34 33 2d 32 33 34 2d 32 33 34 32 0d 0a |..843-234-2342..|
00000080 54 6f 6d 20 4b 61 7a 61 6e 73 6b 69 09 09 33 34 |Tom Kazanski..34|
00000090 33 2d 33 34 33 2d 32 33 34 33 0d 0a 50 65 74 65 |3-343-2343..Pete|
000000a0 20 47 69 62 62 6f 6e 73 09 09 32 33 34 2d 33 32 | Gibbons..234-32|
000000b0 34 2d 32 33 34 32 0d 0a 48 61 6e 73 20 47 72 75 |4-2342..Hans Gru|
000000c0 62 65 72 09 09 34 39 2d 38 39 2d 32 38 38 38 2d |ber..49-89-2888-|
000000d0 30 0d 0a 57 61 68 20 53 69 6e 67 20 4b 75 20 20 |0..Wah Sing Ku |
000000e0 20 20 09 09 30 31 31 2d 38 31 2d 33 2d 33 32 32 | ..011-81-3-322|
000000f0 34 2d 35 30 30 30 00 00 00 00 00 00 00 00 00 |4-5000.....|
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000400 73 66 38 44 00 61 4e 33 6a 6c 3a 00 61 6a 69 64 |sf8D.aN3jl:ajid|
00000410 00 73 6f 6d 65 74 69 6d 65 73 69 73 69 74 72 65 |.sometimesisitrel|
00000420 61 6c 00 32 34 6a 73 73 6a 2e 00 73 6f 6d 65 74 |al.24jssj..somet|
00000430 69 6d 65 73 20 69 74 20 69 73 20 6e 6f 74 20 72 |imes it is not r|
00000440 65 61 6c 00 00 00 00 00 00 00 00 00 00 00 00 |eal.....|
00000450 00 00 73 74 72 69 6e 67 73 20 73 75 63 6b 00 00 |..strings suck..|
00000460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000470 00 00 00 00 00 e0 00 00 77 68 65 72 65 30 77 68 |.....where0wh|
00000480 65 72 65 31 35 74 68 65 6b 33 79 3f 00 00 00 00 |ere15thek3y?....|
00000490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
000004a0 00 69 00 74 00 69 00 73 00 6e 00 6f 00 74 00 68 |.i.t.i.s.n.o.t.h|
000004b0 00 65 00 72 00 65 00 00 00 00 00 00 00 00 00 |.e.r.e.....|
000004c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
000004d0 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 50 |.....P|
000004e0 4b 00 31 38 00 0d 00 00 00 04 00 20 00 03 10 00 |K.18.....|
000004f0 22 01 01 00 42 00 00 00 00 00 00 00 00 00 00 |"...B.....|
00000500 00 00 00 00 00 e0 00 ee 00 6b 65 79 66 69 6c 65 |.....keyfile|
00000510 2e 64 61 74 00 00 00 00 00 00 00 00 00 00 00 |.dat.....|
00000520 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
```

- o Phân vùng 2

```
(kali@kali)~[~/Downloads]
$ hexdump -C kb04-session02_cau4_pv2.bin
00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00003c00 eb 52 90 4e 54 46 53 20 20 20 20 02 08 00 00 |.R.NTFS .....|
00003c10 00 00 00 00 00 f8 00 00 3f 00 ff 00 1f 00 00 00 |.....?.....|
00003c20 00 00 00 00 80 00 00 00 45 7b 00 00 00 00 00 00 |.....E{.....|
00003c30 22 05 00 00 00 00 00 00 02 00 00 00 00 00 00 |".....|
00003c40 f6 00 00 00 01 00 00 00 63 1f 85 d4 48 85 d4 22 |.....c...H.."|
00003c50 00 00 00 00 fa 33 c0 8e d0 bc 00 7c fb 68 c0 07 |.....3....|.h..|
00003c60 1f 1e 68 66 00 cb 88 16 0e 00 66 81 3e 03 00 4e |..hf.....f.>..N|
00003c70 54 46 53 75 15 b4 41 bb aa 55 cd 13 72 0c 81 fb |TFSu...A..U..r...|
00003c80 55 aa 75 06 f7 c1 01 00 75 03 e9 dd 00 1e 83 ec |U.u....u.....|
00003c90 18 68 1a 00 b4 48 8a 16 0e 00 8b f4 16 1f cd 13 |.h...H.....|
00003ca0 9f 83 c4 18 9e 58 1f 72 e1 3b 06 0b 00 75 db a3 |.....X.r.;...u..|
00003cb0 0f 00 c1 2e 0f 00 04 1e 5a 33 db b9 00 20 2b c8 |.....Z3... +..|
00003cc0 66 ff 06 11 00 03 16 0f 00 8e c2 ff 06 16 00 e8 |f.....|
00003cd0 4b 00 2b c8 77 ef b8 00 bb cd 1a 66 23 c0 75 2d |K.+..w.....f#.u-|
00003ce0 66 81 fb 54 43 50 41 75 24 81 f9 02 01 72 1e 16 |f..TCPAu$....r..|
00003cf0 68 07 bb 16 68 70 0e 16 68 09 00 66 53 66 53 66 |h...hp..h..fsfSf|
00003d00 55 16 16 16 68 b8 01 66 61 0e 07 cd 1a 33 c0 bf |U...h..fa....3..|
00003d10 28 10 b9 d8 0f fc f3 aa e9 5f 01 90 90 66 60 1e |(....._...f`.|
00003d20 06 66 a1 11 00 66 03 06 1c 00 1e 66 68 00 00 00 |.f...f.....fh...|
00003d30 00 60 50 06 53 68 01 00 68 10 00 b4 42 8a 16 0e |.fP.Sh..h...B...|
00003d40 00 16 1f 8b f4 cd 13 66 59 5b 5a 66 59 66 59 1f |.....fY[ZfYfY..|
00003d50 0f 82 16 00 66 ff 06 11 00 03 16 0f 00 8e c2 ff |.....f.....|
00003d60 0e 16 00 75 bc 07 1f 66 61 c3 a0 f8 01 e8 09 00 |...u...fa.....|
00003d70 a0 fb 01 e8 03 00 f4 eb fd b4 01 8b f0 ac 3c 00 |.....<..|
00003d80 74 09 b4 0e bb 07 00 cd 10 eb f2 c3 0d 0a 41 20 |t.....A...|
00003d90 64 69 73 6b 20 72 65 61 64 20 65 72 72 6f 72 20 |disk read error |
00003da0 6f 63 63 75 72 72 65 64 00 0d 0a 42 4f 4f 54 4d |occurred ... BOOTM|
00003db0 47 52 20 69 73 20 6d 69 73 73 69 6e 67 00 0d 0a |GR is missing...|
00003dc0 42 4f 4f 54 4d 47 52 69 69 73 20 63 6f 6d 70 72 |BOOTMGR is compr|
00003dd0 65 73 73 65 64 00 0d 0a 50 72 65 73 73 20 43 74 |essed... Press Ct|
00003de0 72 6c 2b 41 6c 74 2b 44 65 6c 20 74 6f 20 72 65 |rl+Alt+Del to rel|
00003df0 73 74 61 72 74 0d 0a 00 8c a9 be d6 00 00 55 aa |start.....U..|
00003e00
```

- Kết quả: Không tìm thấy gì hữu ích
- Ta còn một gợi ý nữa là foremost để khôi phục tệp đã xóa

```
(kali@kali)-[~/Downloads]
$ foremost kb04-session02.bin
Processing: kb04-session02.bin
[*]

(kali@kali)-[~/Downloads]
$ ls
bbls_rel6_student.pdf kb04-session02.bin kb04-session02_cau4_pv0.bin kb04-session02_cau4_pv1.bin kb04-session02_cau4_pv2.bin kb04-session02_cau4_pv3.bin output

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

- Kiểm tra thư mục output

```
(kali@kali)-[~/Downloads]
$ cd output

(kali@kali)-[~/Downloads/output]
$ ls
audit.txt jpg png

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

- Sau khi tìm tòi thì ta biết file audit chứa nội dung thông tin về các file hình ảnh trong 2 thư mục jpg và png

```
(kali@kali)-[~/Downloads/output]
$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Apr 26 15:29:23 2023
Invocation: foremost kb04-session02.bin
Output directory: /home/kali/Downloads/output
Configuration file: /etc/foremost.conf

File: kb04-session02.bin
Start: Wed Apr 26 15:29:23 2023
Length: 15 MB (16187392 bytes)



| Num | Work Name (bs=512) | Size  | File Offset | Comment     |
|-----|--------------------|-------|-------------|-------------|
| 0:  | 00000343.jpg       | 11 KB | 175616      |             |
| 1:  | 00000367.jpg       | 4 KB  | 187904      |             |
| 2:  | 00000375.jpg       | 1 KB  | 192000      |             |
| 3:  | 00001063.jpg       | 13 KB | 544256      |             |
| 4:  | 00001095.jpg       | 36 KB | 560640      |             |
| 5:  | 00001175.jpg       | 32 KB | 601600      |             |
| 6:  | 00001247.jpg       | 4 KB  | 638464      |             |
| 7:  | 00000319.png       | 9 KB  | 163328      | (634 x 278) |

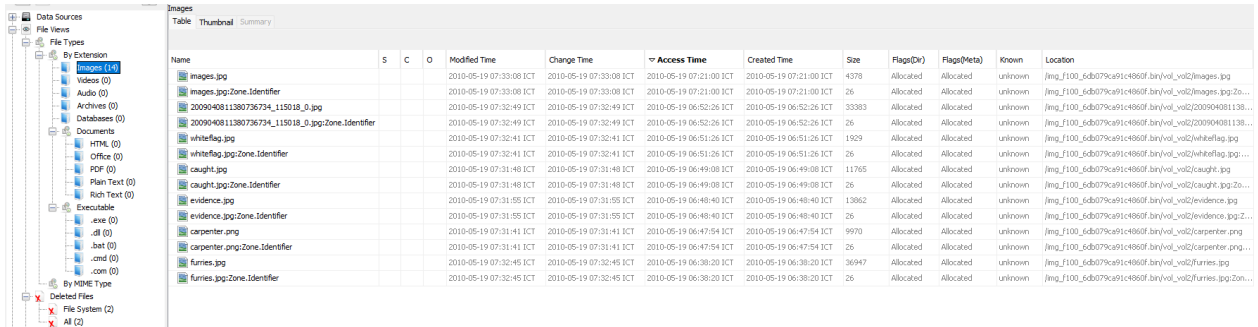

Finish: Wed Apr 26 15:29:24 2023

8 FILES EXTRACTED

jpg:= 7
png:= 1

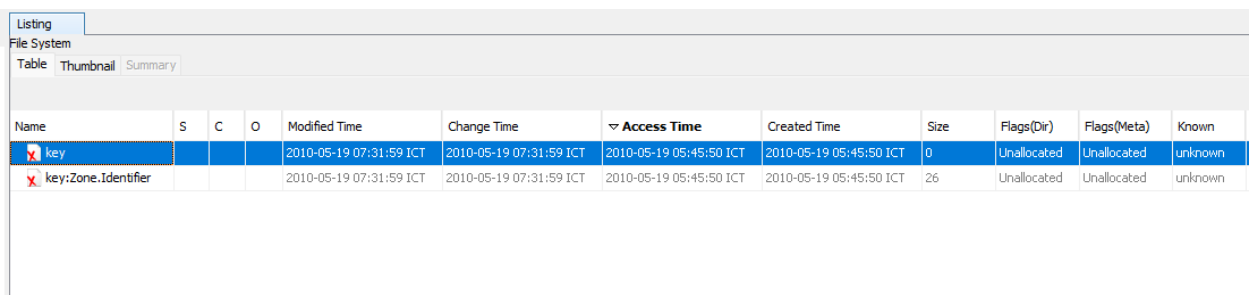
Foremost finished at Wed Apr 26 15:29:24 2023
```


- Kết quả: Không tìm được thông tin hữu ích
- **Tiến hành phân tích sử dụng Autopsy**
 - Tìm kiếm ở phần Image: không có thông tin gì



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Images.jpg				2010-05-19 07:33:08 ICT	2010-05-19 07:33:08 ICT	2010-05-19 07:21:00 ICT	2010-05-19 07:21:00 ICT	4378	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/Images.jpg
Images.jpg:Zone.Identifier				2010-05-19 07:33:08 ICT	2010-05-19 07:33:08 ICT	2010-05-19 07:21:00 ICT	2010-05-19 07:21:00 ICT	26	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/Images.jpg:Zone.Identifier
2009040811380736734_115018_0.jpg				2010-05-19 07:32:49 ICT	2010-05-19 07:32:49 ICT	2010-05-19 06:52:26 ICT	2010-05-19 06:52:26 ICT	33383	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/200904081138...
2009040811380736734_115018_0.jpg:Zone.Identifier				2010-05-19 07:32:49 ICT	2010-05-19 07:32:49 ICT	2010-05-19 06:52:26 ICT	2010-05-19 06:52:26 ICT	26	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/200904081138...
whiteflag.jpg				2010-05-19 07:32:41 ICT	2010-05-19 07:32:41 ICT	2010-05-19 06:51:26 ICT	2010-05-19 06:51:26 ICT	1929	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/whiteflag.jpg
whiteflag.jpg:Zone.Identifier				2010-05-19 07:32:41 ICT	2010-05-19 07:32:41 ICT	2010-05-19 06:51:26 ICT	2010-05-19 06:51:26 ICT	26	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/whiteflag.jpg:Zone.Identifier
caught.jpg				2010-05-19 07:31:48 ICT	2010-05-19 07:31:48 ICT	2010-05-19 06:49:08 ICT	2010-05-19 06:49:08 ICT	11765	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/caught.jpg
caught.jpg:Zone.Identifier				2010-05-19 07:31:48 ICT	2010-05-19 07:31:48 ICT	2010-05-19 06:49:08 ICT	2010-05-19 06:49:08 ICT	26	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/caught.jpg:Zone.Identifier
evidence.jpg				2010-05-19 07:31:55 ICT	2010-05-19 07:31:55 ICT	2010-05-19 06:48:40 ICT	2010-05-19 06:48:40 ICT	13862	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/evidence.jpg
evidence.jpg:Zone.Identifier				2010-05-19 07:31:55 ICT	2010-05-19 07:31:55 ICT	2010-05-19 06:48:40 ICT	2010-05-19 06:48:40 ICT	26	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/evidence.jpg:Zone.Identifier
carpenter.png				2010-05-19 07:31:41 ICT	2010-05-19 07:31:41 ICT	2010-05-19 06:47:54 ICT	2010-05-19 06:47:54 ICT	9970	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/carpenter.png
carpenter.png:Zone.Identifier				2010-05-19 07:31:41 ICT	2010-05-19 07:31:41 ICT	2010-05-19 06:47:54 ICT	2010-05-19 06:47:54 ICT	26	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/carpenter.png:Zone.Identifier
furnies.jpg				2010-05-19 07:32:45 ICT	2010-05-19 07:32:45 ICT	2010-05-19 06:38:20 ICT	2010-05-19 06:38:20 ICT	36947	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/furnies.jpg
furnies.jpg:Zone.Identifier				2010-05-19 07:32:45 ICT	2010-05-19 07:32:45 ICT	2010-05-19 06:38:20 ICT	2010-05-19 06:38:20 ICT	26	Allocated	Allocated	unknown	/img_f100_6db079ca91c4869f.bin/vol_02/furnies.jpg:Zone.Identifier

- Tuy nhiên khi tìm kiếm ở phần Delete File ta đã tìm được file key



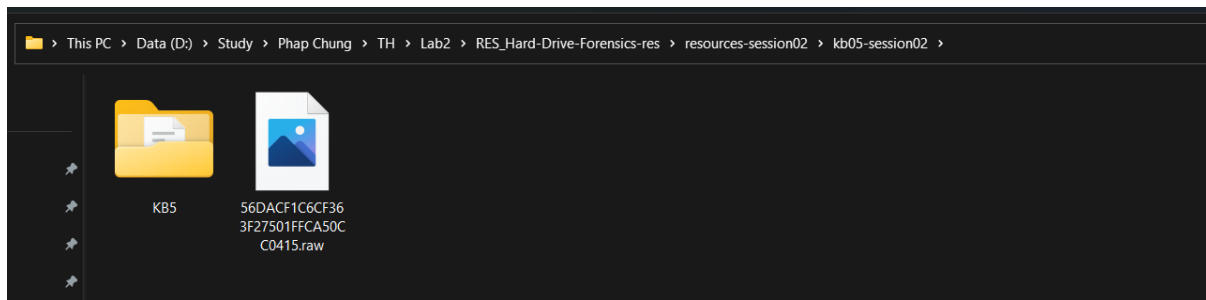
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
key				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45:50 ICT	2010-05-19 05:45:50 ICT	0	Unallocated	Unallocated	unknown
key:Zone.Identifier				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45:50 ICT	2010-05-19 05:45:50 ICT	26	Unallocated	Unallocated	unknown

5. Kịch bản 5 - Thực hiện phân tích theo yêu cầu

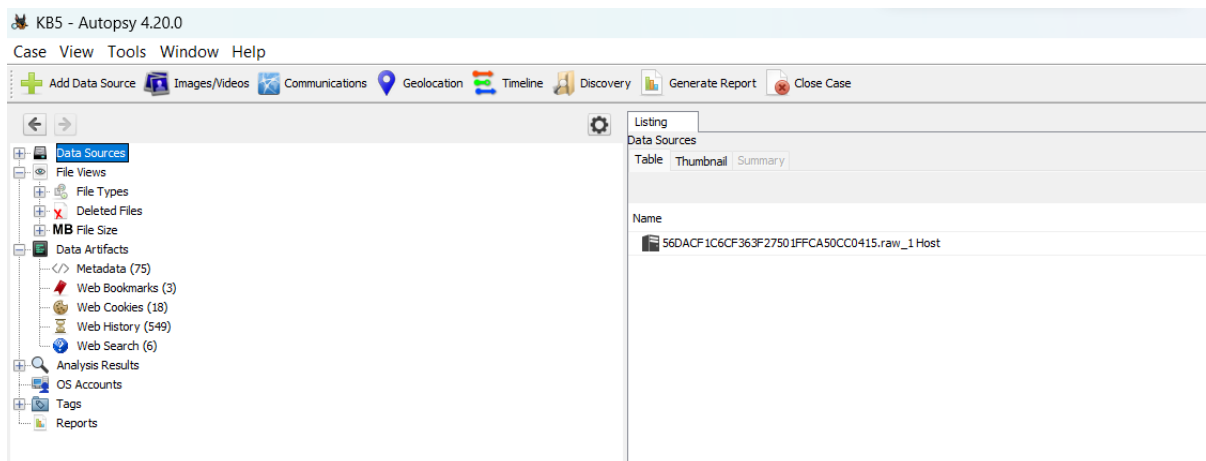
Kịch bản 05. Thực hiện phân tích:

- 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.

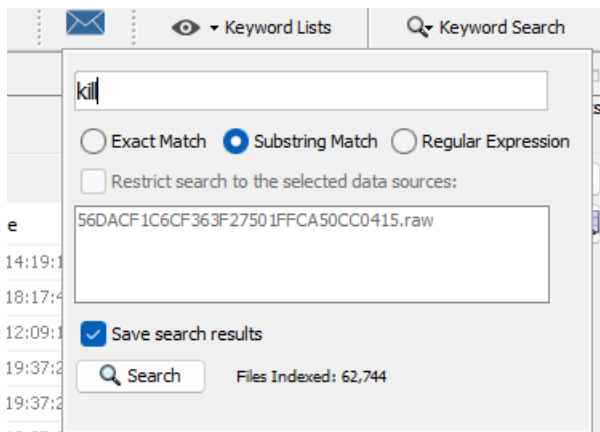
Đáp án:



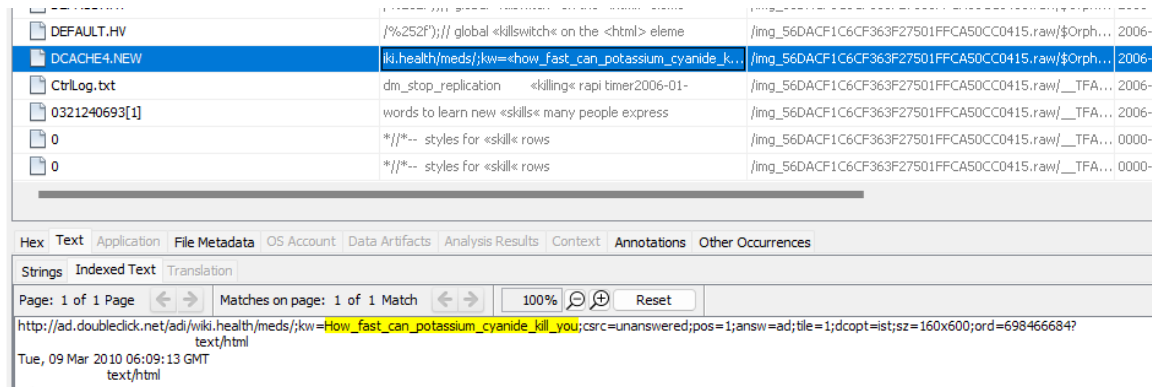
- Thực hiện giải nén file kb5 và ta được 1 file .raw
- Mở bằng autopsy



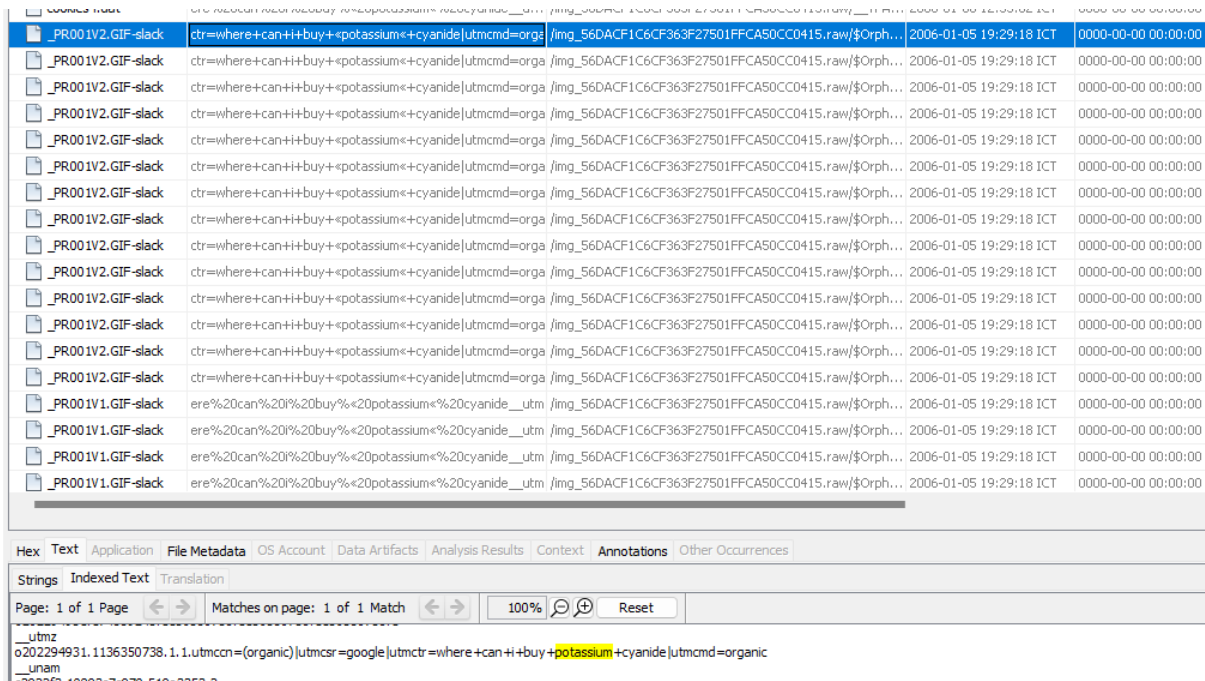
- Đặt tên là KB5 để phân tích



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



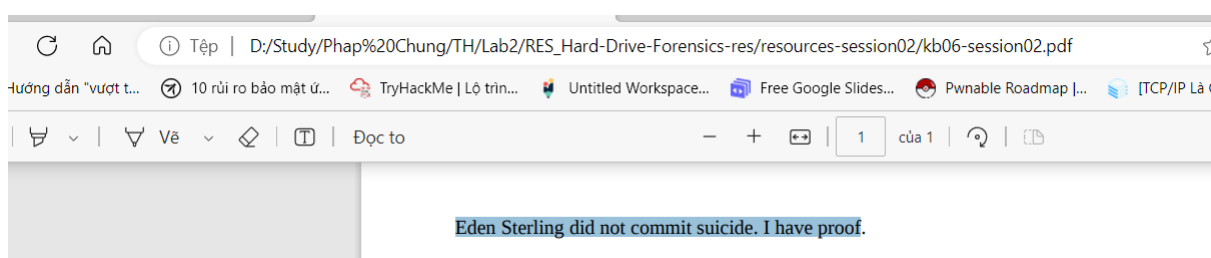
- Ta thấy người đàn ông có tìm kiếm 1 thông tin đại khái là cách chất độc cyanide có thể giết ta trong bao lâu (How fast can potassium cyanide kill you) ở 1 trang tìm kiếm tên là "doubleclick.net"



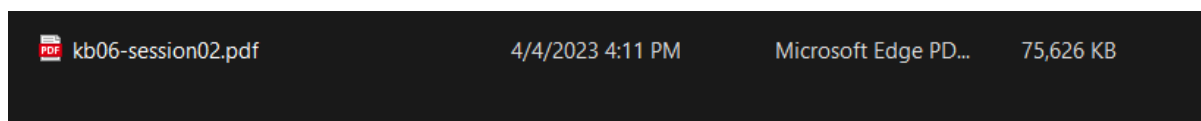
- Ta thấy ông ta có tìm kiếm nơi để mua potassium cyanide nên có thể chắc đây là tự tử
- Thử kiểm các lí do để ông ta có thể tự tử như là : "love", "money", "stress", ... nhưng không có gì mấy
- Nhưng từ đây ta có thể kết luận là ông ta tự tử

6. Kịch bản 6 – Thực hiện phân tích

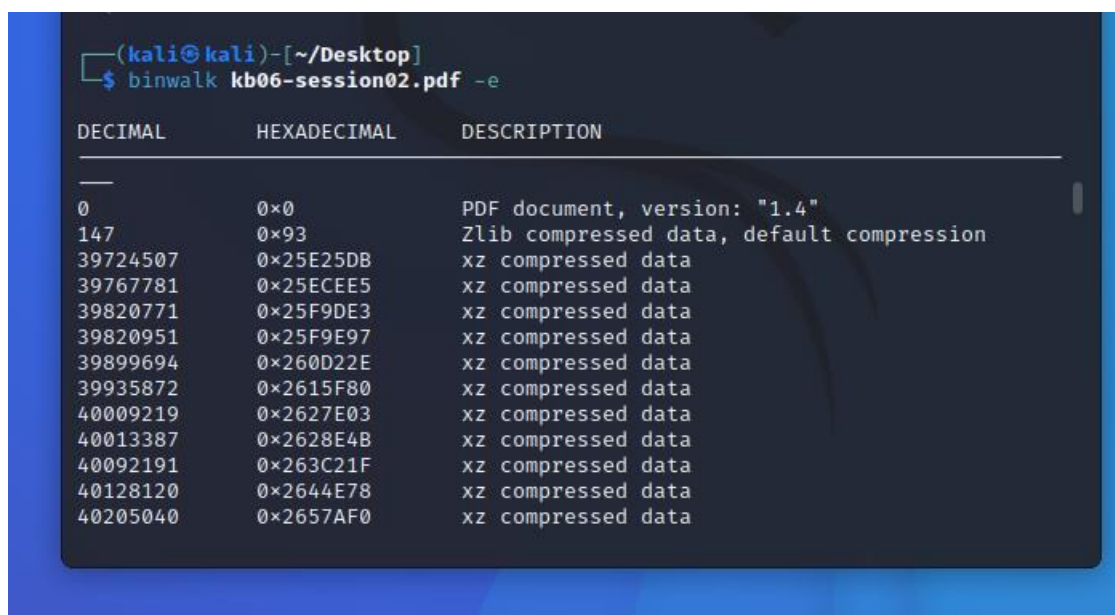
- Tên trưởng nhóm nhân viên điều tra pháp y là gì?
- Ai đã gửi thông tin nặc danh tới đội điều tra pháp y?
- Thông tin đăng nhập của tài khoản truyền thông xã hội của Eden là gì?
- Mật khẩu cho máy tính xách tay của Alice là gì?
- Mật khẩu của Bruce là gì?
- Các thông tin đăng nhập/ bảo mật của trang web NO. CO.?



- Ta mở file pdf thì nó chỉ có 1 dòng này



- Nhưng mà file lại nặng tới 75MB nên có thể sẽ có file ẩn



- Sử dụng binwalk để xuất ra các file ẩn

```

2E111DE.xz 34CAE2E 3A42FE8.xz 3F231D9 4423775.xz 49AC74D
2E15846 34CAE2E.xz 3A44599 3F231D9.xz 442D297 49AC74D.xz
2E15846.xz 34D8A60 3A44599.xz 3F26A19 442D297.xz 49B5022
2E1FAB0 34D8A60.xz 3A4FD3E 3F26A19.xz 44378F1 49B5022.xz
2E1FAB0.xz 34E5A32 3A4FD3E.xz 3F32194 44378F1.xz 49BAF3C
2E23B18 34E5A32.xz 3A514EF 3F32194.xz 444008F 49BAF3C.xz
2E23B18.xz 34EC12C 3A514EF.xz 3F33DB0 444008F.xz 49C96D6
2E2E1AB 34EC12C.xz 3A589A8 3F33DB0.xz 4446188 49C96D6.xz
2E2E1AB.xz 34F8D12 3A589A8.xz 3F3C585 4446188.xz 49D3968
2E4038A 34F8D12.xz 3A62DCE 3F3C585.xz 444AD3C 49D3968.xz
2E4038A.xz 34FED0B 3A62DCE.xz 3F46C6F 444AD3C.xz 49D7BA1
2E4E46C 34FED0B.xz 3A66B72 3F46C6F.xz 4452102 49D7BA1.zlib
2E4E46C.xz 350C1A6 3A66B72.xz 3F4E6A1 4452102.xz 49D7D7A
2E5B746 350C1A6.xz 3A6E394 3F4E6A1.xz 445959B 49D7D7A.zlib
2E5B746.xz 350EB8E 3A6E394.xz 3F5870A 445959B.xz 49D7E06
2E5F7F3 350EB8E.xz 3A745ED 3F5870A.xz 4460289 49D7E06.zlib
2E5F7F3.xz 3514CEB 3A745ED.xz 3F6176F 4460289.xz 49DA0BD
2E6D622 3514CEB.xz 3A80ADC 3F6176F.xz 4467239 49DA0BD.zlib
2E6D622.xz 351EB09 3A80ADC.xz 3F64A80 4467239.xz 93
2E7AFB4 351EB09.xz 3A83F3B 3F64A80.xz 446D9DF 93.zlib
2E7AFB4.xz 352BF73 3A83F3B.xz 3F6E4A2 446D9DF.xz
2E866FA 352BF73.xz 3A8CC8A 3F6E4A2.xz 4475910
(kali@kali)-[~/Desktop/_kb06-session02.pdf.extracted]
$

```

- Ta thấy các file giống nhau và toàn là các file rác
- Ta có một số file lạ như là zlib và file 93 khá là lạ

```

(kali@kali)-[~/Desktop/_kb06-session02.pdf.extracted]
$ 7z e 93

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,32 CPUs
AMD Ryzen 5 4600H with Radeon Graphics (860F01),ASM,AES-NI)

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

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

Everything is Ok

Size:      211812352
Compressed: 77422710

(kali@kali)-[~/Desktop/_kb06-session02.pdf.extracted]
$

```

- Giải nén file lạ nhất là file 93

```

2E6D622 3514CEB.xz 3A80ADC 3F6176F.xz 4467239 49DA0BD.zlib
2E6D622.xz 351EB09 3A80ADC.xz 3F64A80 4467239.xz 93
2E7AFB4 351EB09.xz 3A83F3B 3F64A80.xz 446D9DF 93.zlib
2E7AFB4.xz 352BF73 3A83F3B.xz 3F6E4A2 446D9DF.xz Eden_Drive.dd
2E866FA 352BF73.xz 3A8CC8A 3F6E4A2.xz 4475910
(kali@kali)-[~/Desktop/_kb06-session02.pdf.extracted]
$

```

- Ta có được file tên là Eden_Drive.dd
- Bỏ nó vào autopsy để tiến hành phân tích

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
8875837.doc			0	2014-12-04 13:33:57 ICT	2014-12-04 13:33:57 ICT	2014-12-04 13:33:57 ICT	2014-12-04 13:33:57 ICT	1104	Allocated	Allocated	unknown	/img_Eden_Drive.dd/vol_vol2/my_stuff/8875837.doc
secret.docx			0	2014-12-04 13:40:32 ICT	2014-12-04 13:40:32 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	11433	Allocated	Allocated	unknown	/img_Eden_Drive.dd/vol_vol4/secret.docx
f0085384.docx			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	11632	Unallocated	Unallocated	unknown	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0085384.docx
secret.docx:secret.txt			0	2014-12-04 13:40:32 ICT	2014-12-04 13:40:32 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT	41	Allocated	Allocated	unknown	/img_Eden_Drive.dd/vol_vol4/secret.docx:secret.txt

- Trong File views ở Document ta thấy có file khá lạ tên là “secret.docx:secret.txt” đọc thử thì thấy là có vẻ như anh ta bị người theo dõi
- Và có thể kẻ theo dõi này là người ám sát anh ta
- Em có thể tìm các IP cũng như email thì không có gì bất thường
- Em cũng thử tìm các tên “name”, “Alice”, “Bruce”, ... nhưng không thấy

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, trộm, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT