

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 02 (Session 01)

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

GVHD: Đoàn Minh Trung

Nhóm: 03 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: ATCL2020

STT	Họ và tên	MSSV	Email
1	Phan Văn Quyết	15520711	15520711@gm.uit.edu.vn
2	Nguyễn Hoàng Hải	15520186	15520186@gm.uit.edu.vn

1. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Thực hiện	Kết quả tự đánh giá
1	Kịch bản 01	Thực hiện phân tích dựa trên dữ liệu ổ đĩa (tự chọn)	100%
2	Kịch bản 02	Thực hiện phân tích dựa trên tài nguyên được cung cấp.	100%
3	Kịch bản 03	Thực hiện phân tích theo kịch bản mô tả	100%

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

BÁO CÁO CHI TIẾT

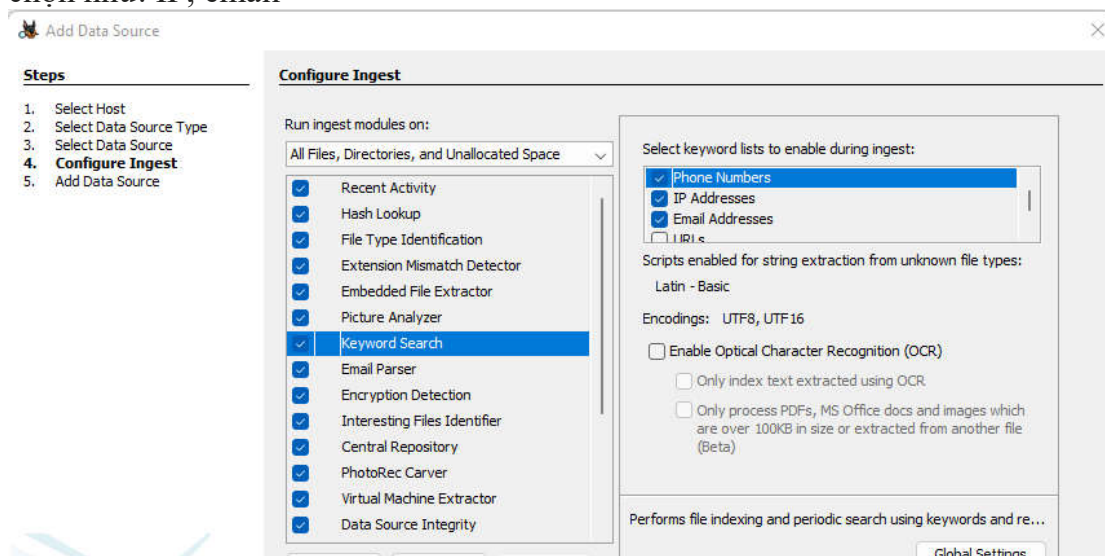
Kịch bản 01. Thực hiện phân tích dựa trên dữ liệu ổ đĩa (tự chọn)

- 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.

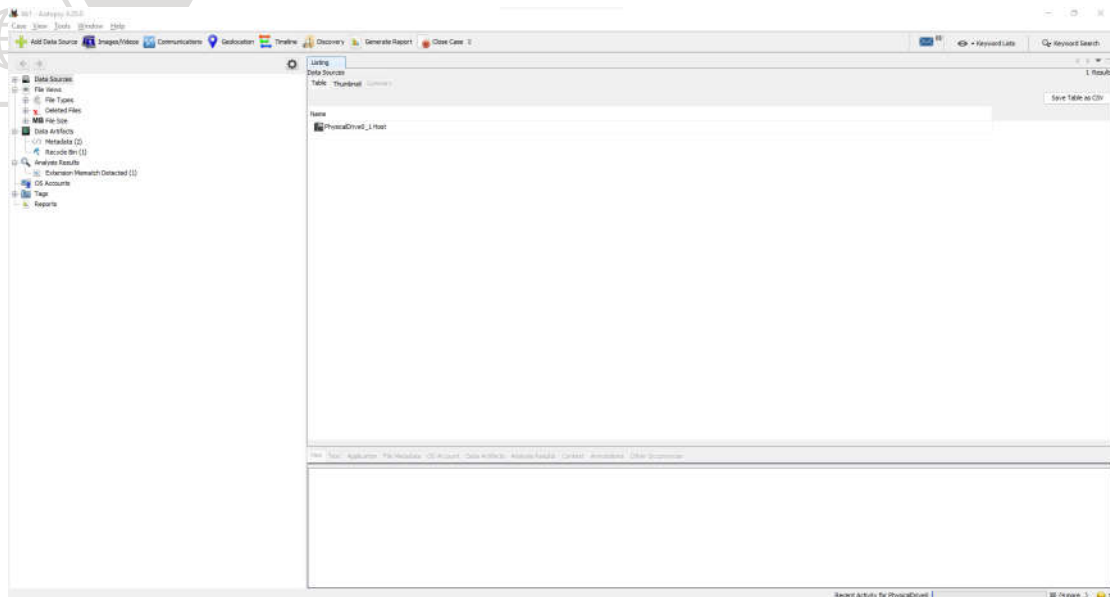
Đáp án:

*Dump

Chọn ra mô-đun để phân tích, mô-đun Keyword Search sẽ có thêm một số tùy chọn như: IP, email

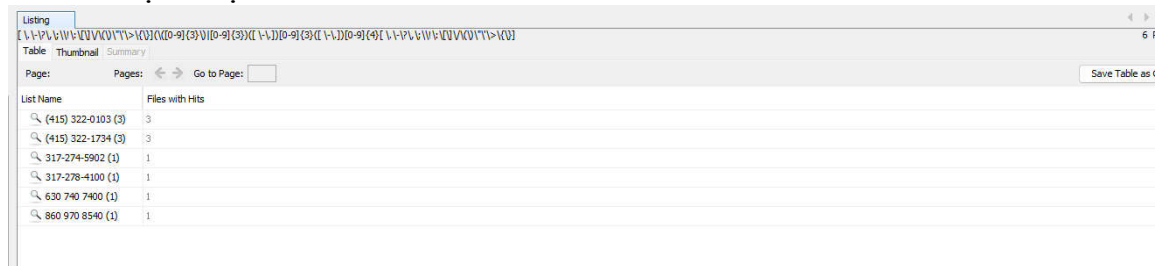


Giao diện của Autopsy sau khi dump thành công

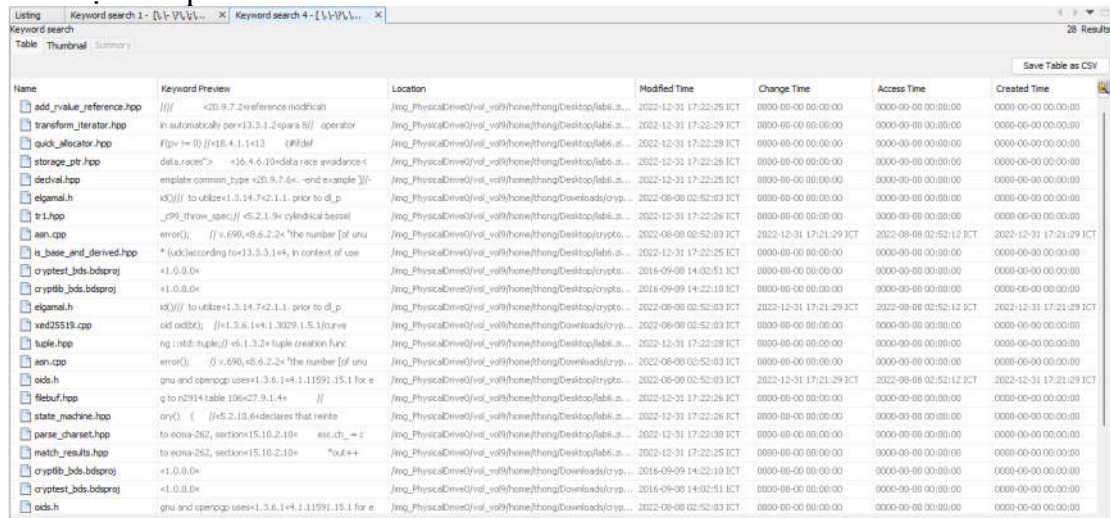


Chọn tìm các số điện thoại và địa chỉ IP có trong Filesystem

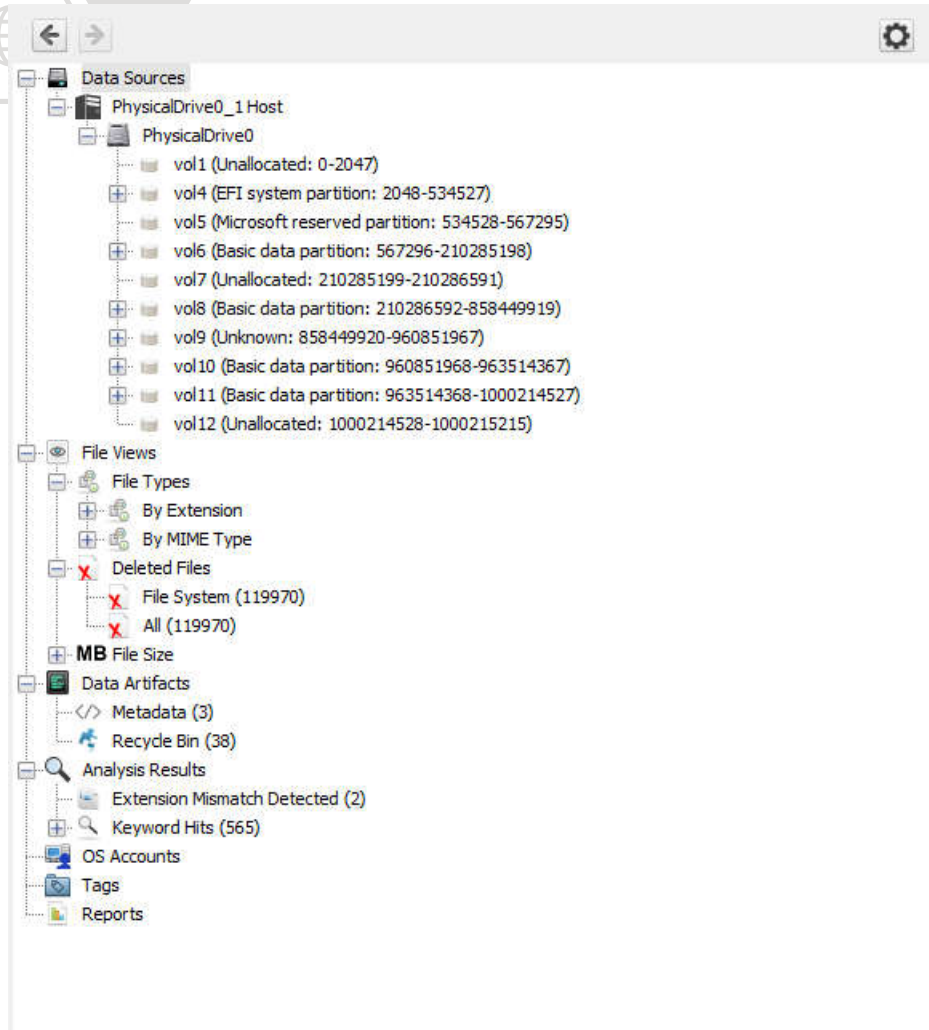
Tìm số điện thoại



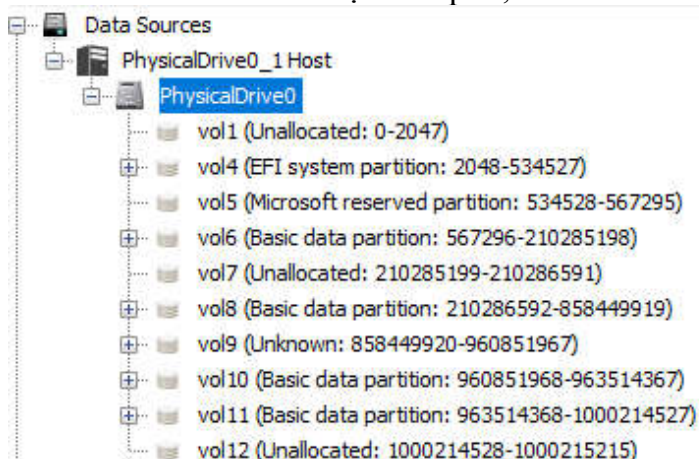
Tìm địa chỉ ip



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

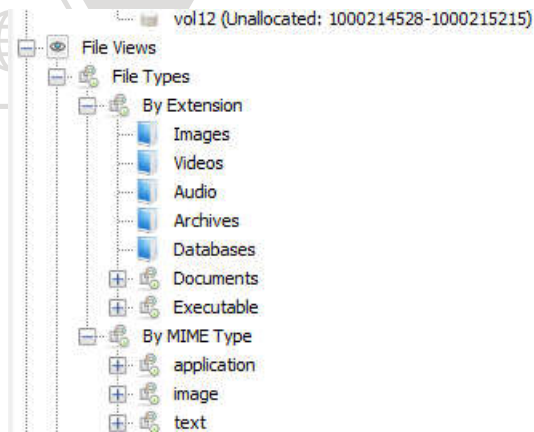


Data Source là ổ đĩa được dump ra, chứa các sector phân vùng của ổ đĩa

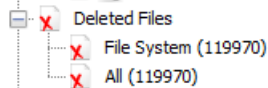


File Views: với 3 phần là

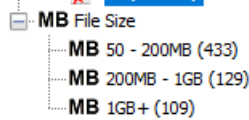
+ **File Types:** Phân loại file theo extension hoặc các topic khác để dễ quản lý và tìm kiếm



+ **Delete File:** lưu trữ các file đã xóa



+ **File Size:** Phân loại file theo kích thước



Data Artifacts: Xem thông tin nội bộ, bao gồm



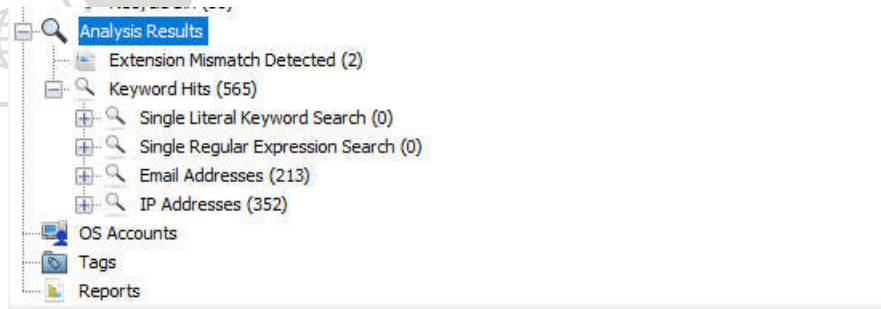
Metadata: chứa các metadata của file

Source Name	S	C	O	Date Modified	Date Created	Data Source	Program Name	Last Printed Date	User ID	Owner
\\> lab6.doc				2023-01-01 13:44:59 ICT	2023-01-01 12:45:37 ICT	PhysicalDrive0				
\\> 20520605_YoAnhKet_lab5.6.docx				2022-09-09 10:18:00 ICT	2022-09-29 06:11:00 ICT	PhysicalDrive0	Microsoft Office Word	2022-09-30 16:07:00 ICT	Vũ Anh Kiệt	Vũ Anh Kiệt
\\> lab6.doc				2023-01-01 13:44:59 ICT	2023-01-01 12:45:37 ICT	PhysicalDrive0				

Recycle Bin: Chứa các thư mục và files nằm trong thùng rác

Source Name	S	C	O	Path	Time Deleted	Username	Data Source
SR108MLB				C:\Program Files (x86)\Mozilla Firefox	2023-04-04 20:17:11 ICT		PhysicalDrive0
SRBU3RF				C:\Program Files (x86)\TouchWIN	2023-04-04 20:17:30 ICT		PhysicalDrive0
SR10ATYJ				C:\Program Files\Microsoft Update Health Tools	2023-04-04 20:16:33 ICT		PhysicalDrive0
SR60FRK				D:\Nam 3\France\lab 2\lab1	2023-04-04 20:25:37 ICT		PhysicalDrive0
SRHUE753.ge				D:\Crypto\lab5-6\lab5\ask\out1_bin.ge	2023-01-01 07:57:59 ICT		PhysicalDrive0
SRIL0THQ				D:\Nam 3\Crypto\Project\CLOUD\Server0\830316D48E27B...	2023-01-06 23:03:54 ICT		PhysicalDrive0
SR091QJ3				D:\Nam 3\Crypto\Project\CLOUD\Server0\CF9348B9E93C...	2023-01-06 23:03:54 ICT		PhysicalDrive0
SRRLTBKR				D:\Nam 3\Crypto\Project\CLOUD\Server1\3E9984F97F3E5...	2023-01-06 23:04:02 ICT		PhysicalDrive0
SRPF3LJ				D:\Nam 3\Crypto\Project\CLOUD\Server1\3E9984F97F3E5...	2023-01-06 23:04:02 ICT		PhysicalDrive0
SRLL74YI				D:\Nam 3\Crypto\Project\CLOUD\Server1\26C9384A5000...	2023-01-06 23:04:02 ICT		PhysicalDrive0
SR9239W1				D:\Nam 3\Crypto\Project\CLOUD\Server1\51C08E54C196...	2023-01-06 23:04:02 ICT		PhysicalDrive0
SRH4CRUY				D:\Nam 3\Crypto\Project\CLOUD\Server1\30D98C3225A...	2023-01-06 23:04:02 ICT		PhysicalDrive0
SRPFP2R3				D:\Nam 3\Crypto\Project\CLOUD\Server1\6284E2A71C380...	2023-01-06 23:04:02 ICT		PhysicalDrive0
SR557LB7				D:\Nam 3\Crypto\Project\CLOUD\Server1\B1AC7909485E...	2023-01-06 23:04:02 ICT		PhysicalDrive0
SR0505T2				D:\Nam 3\Crypto\Project\CLOUD\Server1\07A86C879F81...	2023-01-06 23:04:03 ICT		PhysicalDrive0
SR04F52V				D:\Nam 3\Crypto\Project\CLOUD\Server1\E5F34167FF1F...	2023-01-06 23:04:03 ICT		PhysicalDrive0
SRIC7XFG				D:\Nam 3\Crypto\Project\CLOUD\Server2\48D6F016CC9...	2023-01-06 23:04:05 ICT		PhysicalDrive0
SR8CE3N4				D:\Nam 3\Crypto\Project\CLOUD\Server2\7580ED6F0A93...	2023-01-06 23:04:05 ICT		PhysicalDrive0
SRH2Q3E1				D:\Nam 3\Crypto\Project\CLOUD\Server2\2084F6E759258...	2023-01-06 23:04:05 ICT		PhysicalDrive0
SR7VGS3				D:\Nam 3\Crypto\Project\CLOUD\Server2\650CD4A463D...	2023-01-06 23:04:05 ICT		PhysicalDrive0
SR0PGRP				D:\Nam 3\Crypto\Project\CLOUD\Server2\48065CA912647...	2023-01-06 23:04:06 ICT		PhysicalDrive0

Analysis Result: Chứa các thông tin về kết quả thu thập được sau khi dump bộ nhớ, gồm có



+ **Extension Mismatch Detected:** Những file có extension và signature khác nhau, thường là những file bất thường hoặc không có signature hợp lệ.

Page: 1 of 1		Pages: Go to Page: <input type="text"/>		Save Table as CSV							
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Extension	MIME Type	File Path
lab6.doc			1	File	Likely Notable			File has MIME type of application/vnd.ms-excel.openxmlformats-officedocument.wordprocessingml.document	.doc	application/vnd.ms-excel.openxmlformats-officedocument.wordprocessingml.document	\\mq.physicaldrive\vol_vols\home\thong\De
lab6.doc			1	File	Likely Notable			File has MIME type of application/vnd.ms-excel.openxmlformats-officedocument.wordprocessingml.document	.doc	application/vnd.ms-excel.openxmlformats-officedocument.wordprocessingml.document	\\mq.physicaldrive\vol_vols\home\thong\De

+ **Keyword hints:** Danh sách các mẫu tìm kiếm theo một format nào đó (mail, IP, ...)

OS Account: Toàn bộ account trên hệ thống, bao gồm cả account của ứng dụng

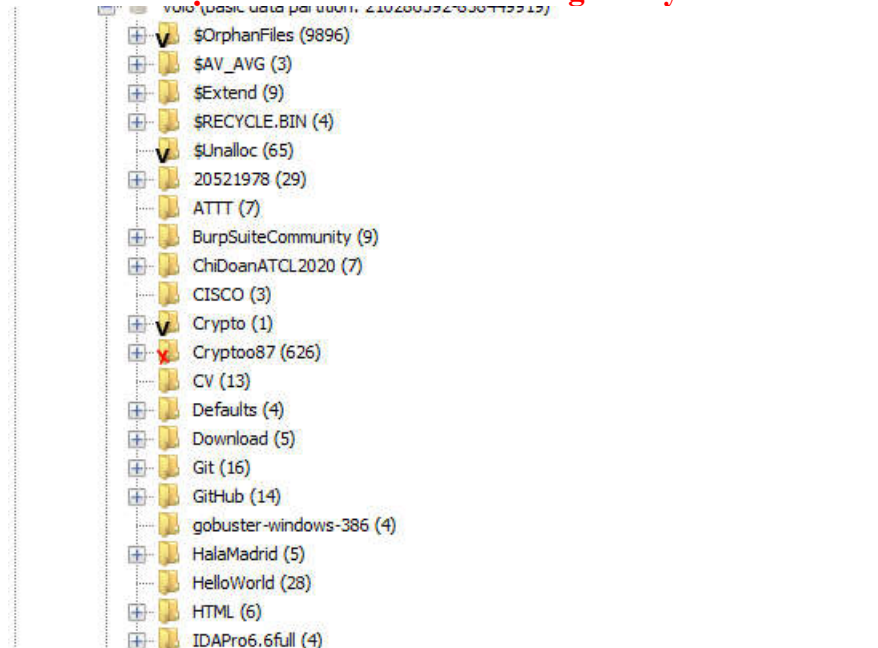
Tags: Các tags được điều tra viên gắn nhãn

Reports: Những bản báo cáo được điều tra viên lưu lại

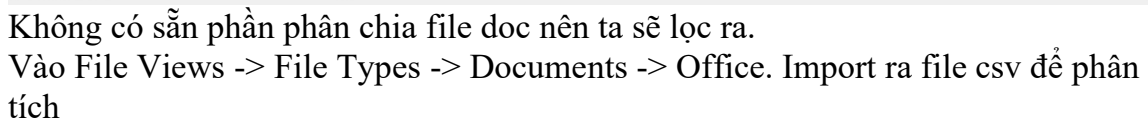
NOTE: Ngoài ra còn một số kết quả khác nếu để chạy Ingest Analysis đủ lâu thì sẽ có các phân tích

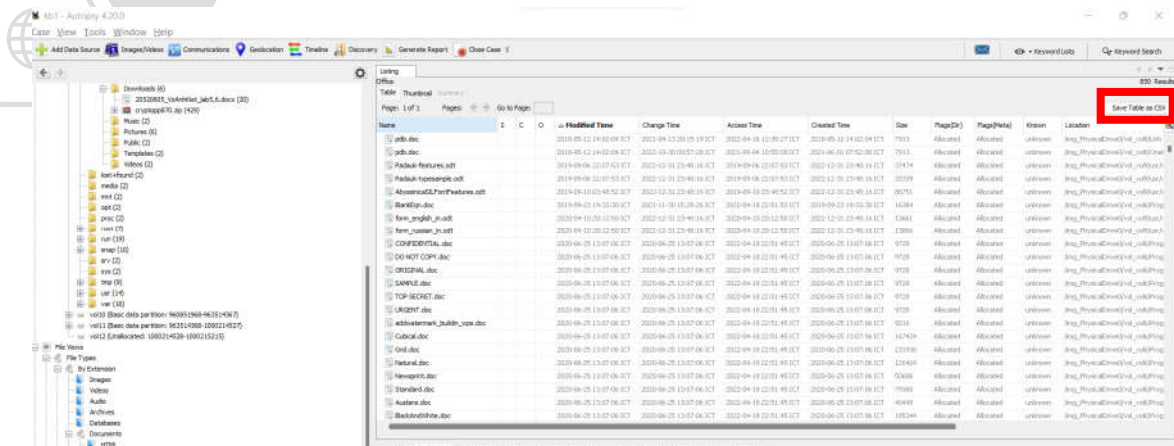
khác trên nhiều module như Web Cookie, Web History, Cache , ...

- **Tìm thư mục có nhiều File nhất trong Filesystem.**

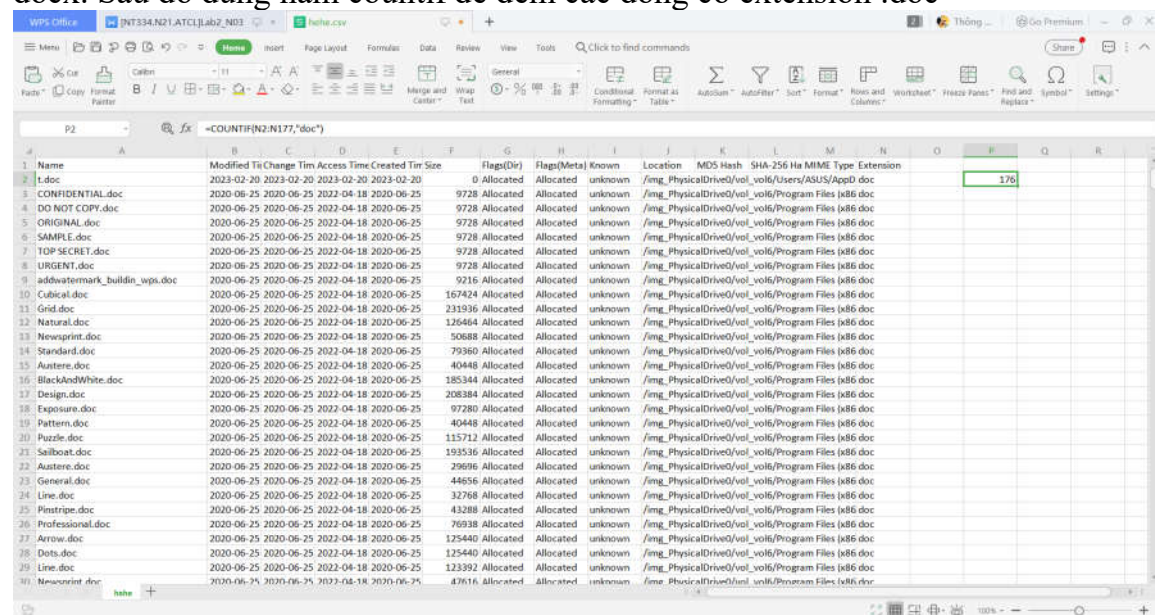


- **Xem các file hình ảnh chứa trong Filesystem bằng chế độ view Thumbnail. Xác định số lượng các files dạng doc và pdf chứa trong Filesystem**





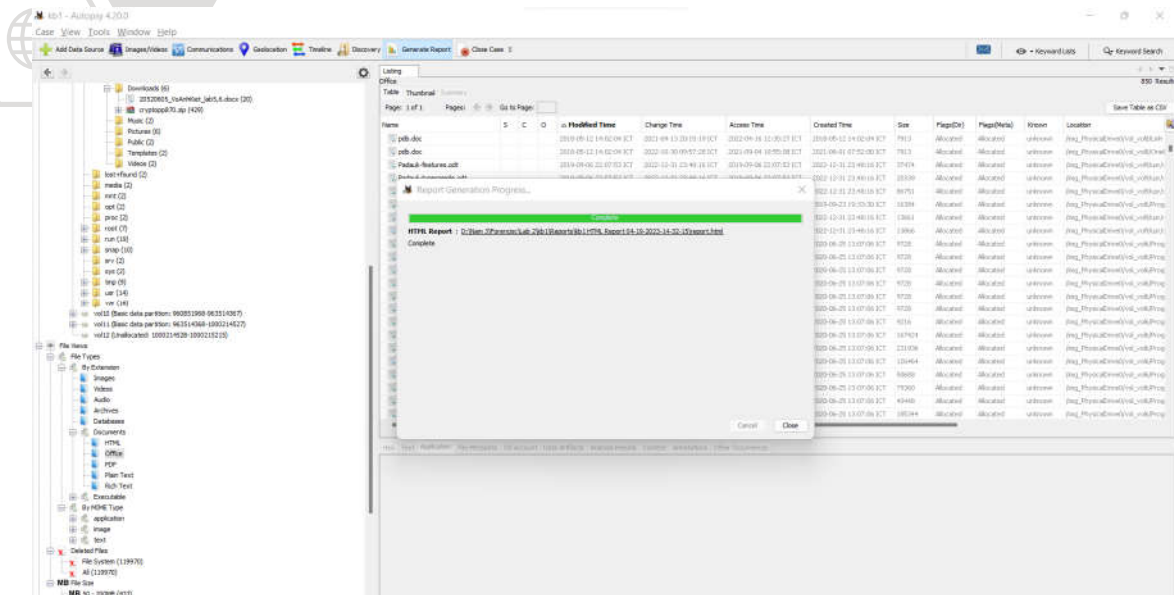
Xử lý bên csv, dùng sort để sắp xếp lại hàng extension thành 2 phần là doc và docx. Sau đó dùng hàm countif để đếm các dòng có extension .doc



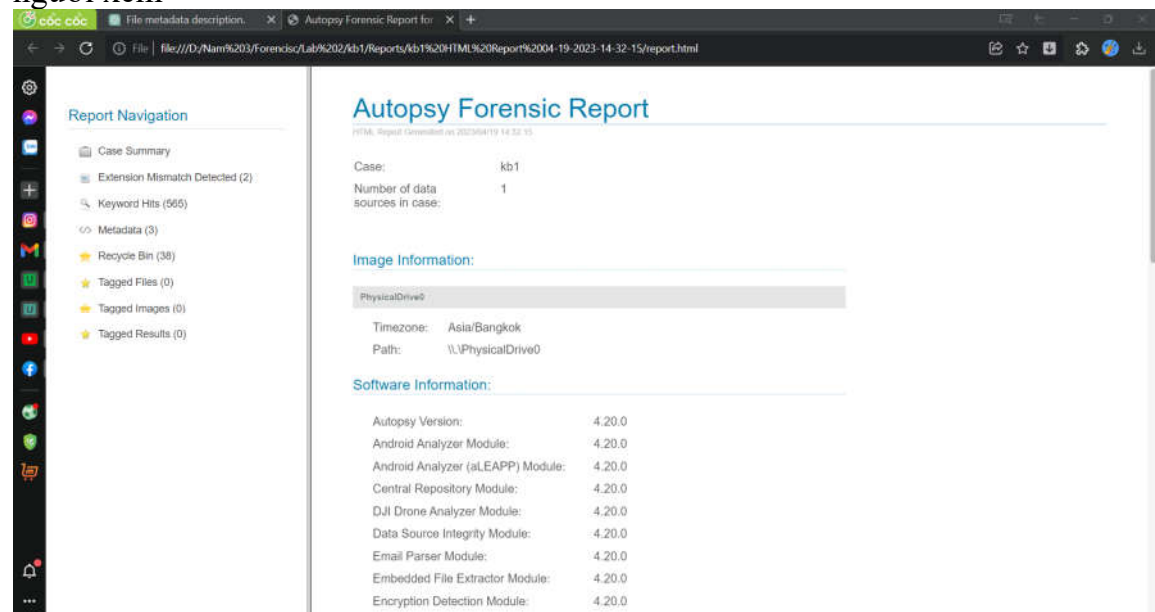
Kết quả có 176 dòng tương ứng 176 file doc

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

Export báo cáo dạng HTML



File báo cáo gồm 2 phần, phần chính hiển thị thông tin, phần content chứa các file phụ như keyword hints, metadata,... để hiển thị ra phần chính của html
File báo cáo chính xác, dễ nhìn tập trung vào kết quả được xuất bởi các Analysis Modules và Search bởi người xem



Phần IP Address trong Keyword hints

The screenshot displays a forensic analysis tool interface. On the left, a 'Report Navigation' sidebar lists various report sections: Case Summary, Extension Mismatch Detected (2), Keyword Hits (565), Metadata (3), Recycle Bin (38), Tagged Files (0), Tagged Images (0), and Tagged Results (0). The main window is titled 'IP Addresses' and shows three sections of data:

- 1.0.0.0**: A table with columns 'Preview', 'Source File', and 'Tags'. It lists multiple instances of IP addresses and file paths, such as `/img_PhysicalDrive0/vol1/home/thong/Desktop/cryptopp870/bds10.zip/cryptest_bds.bdsproj`.
- 1.3.14.7**: A table with columns 'Preview', 'Source File', and 'Tags'. It lists file paths and timestamps, such as `id() // to utilize=1.3.14.7+2.1.1. prior to d1_p /img_PhysicalDrive0/vol1/home/thong/cache/tracker/meta.db`.
- 1.3.6.1**: A table with columns 'Preview', 'Source File', and 'Tags'. It lists file paths and timestamps, such as `id() // to utilize=1.3.14.7+2.1.1. prior to d1_p /img_PhysicalDrive0/vol1/home/thong/Desktop/cryptopp870/elgamal.h`.

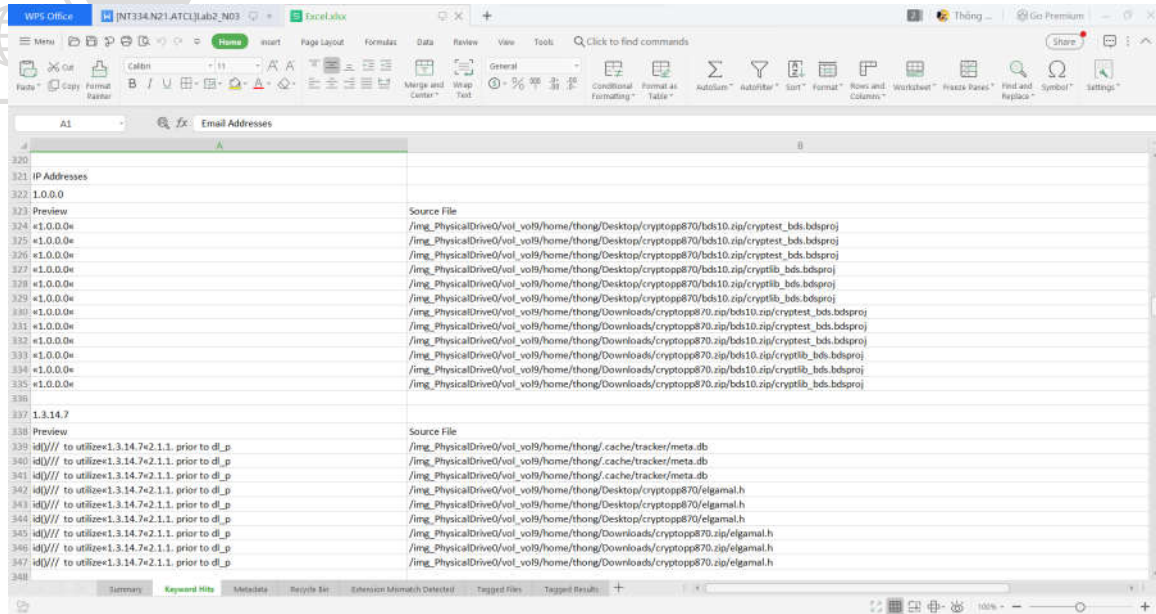
Export báo cáo qua excel. Báo cáo gồm các sheet chứa nội dung

The screenshot shows an Excel spreadsheet titled 'WPS Office' with the file name '[N7334.N21.ATCLJLab2_ND3]'. The spreadsheet has a 'Summary' sheet selected, which contains the following data:

Case Name:	kb1
Number of data sources in case:	1

The bottom of the spreadsheet shows a tab bar with the following sheets: Summary, Keyword Hits, Metadata, Recycle Bin, Extension Mismatch Detected, Tagged Files, and Tagged Results. The 'Summary' sheet is highlighted with a red box.

Phần IP Address trong Keyword Hints



The screenshot shows a WPS Office Excel spreadsheet with a table titled "Email Addresses". The table has two columns: A1 and B. The data is organized into sections separated by row numbers. The first section (rows 320-336) lists IP addresses and their corresponding source files. The second section (rows 337-347) lists email addresses and their corresponding source files. The third section (rows 348-357) lists email addresses and their corresponding source files. The table is displayed in a grid format with alternating row colors.

A1	B
320	
321 IP Addresses	
322 1.0.0.0	
323 Preview	Source File
324 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/bds10.zip/cryptest_bds.bdsproj
325 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/bds10.zip/cryptest_bds.bdsproj
326 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/bds10.zip/cryptest_bds.bdsproj
327 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/bds10.zip/cryptlib_bds.bdsproj
328 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/bds10.zip/cryptlib_bds.bdsproj
329 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/bds10.zip/cryptlib_bds.bdsproj
330 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/bds10.zip/cryptest_bds.bdsproj
331 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/bds10.zip/cryptest_bds.bdsproj
332 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/bds10.zip/cryptest_bds.bdsproj
333 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/bds10.zip/cryptlib_bds.bdsproj
334 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/bds10.zip/cryptlib_bds.bdsproj
335 *1.0.0.0*	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/bds10.zip/cryptlib_bds.bdsproj
336	
337 1.3.14.7	
338 Preview	Source File
339 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/.cache/tracker/meta.db
340 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/.cache/tracker/meta.db
341 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/.cache/tracker/meta.db
342 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/egamal.h
343 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/Desktop/cryptopp870/egamal.h
344 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/egamal.h
345 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/egamal.h
346 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/egamal.h
347 id0/// to utilize=1.3.14.7x2.1.1. prior to dl_p	/img_PhysicalDrive0/vol_vol9/home/thong/Downloads/cryptopp870.zip/egamal.h
348	

Kết quả tương tự như báo cáo HTML

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

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

- 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:

Khởi động Autopsy để tạo một Case mới, sử dụng lựa chọn "Create New Case". Sau đó điền tên case.

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: KB2

Base Directory: F:\Hoctap\TH_Forensic\Lab2\ Browse

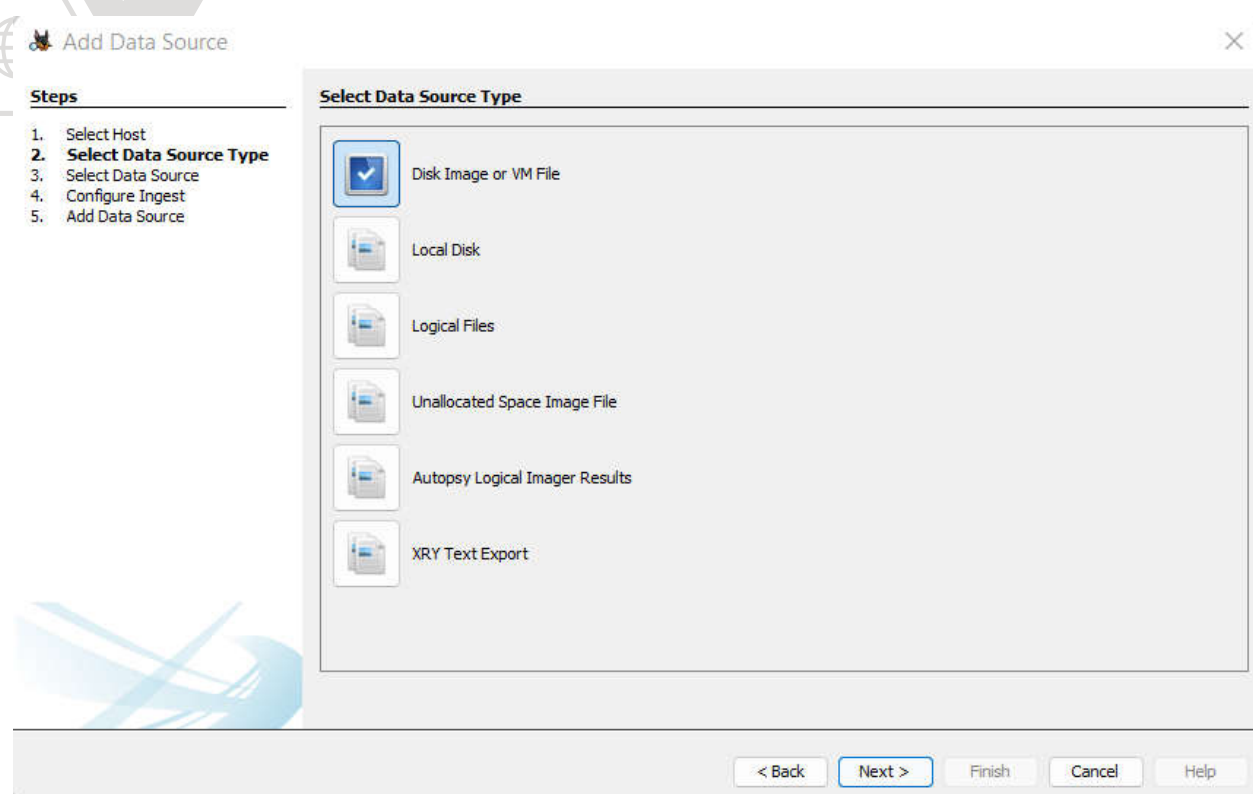
Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

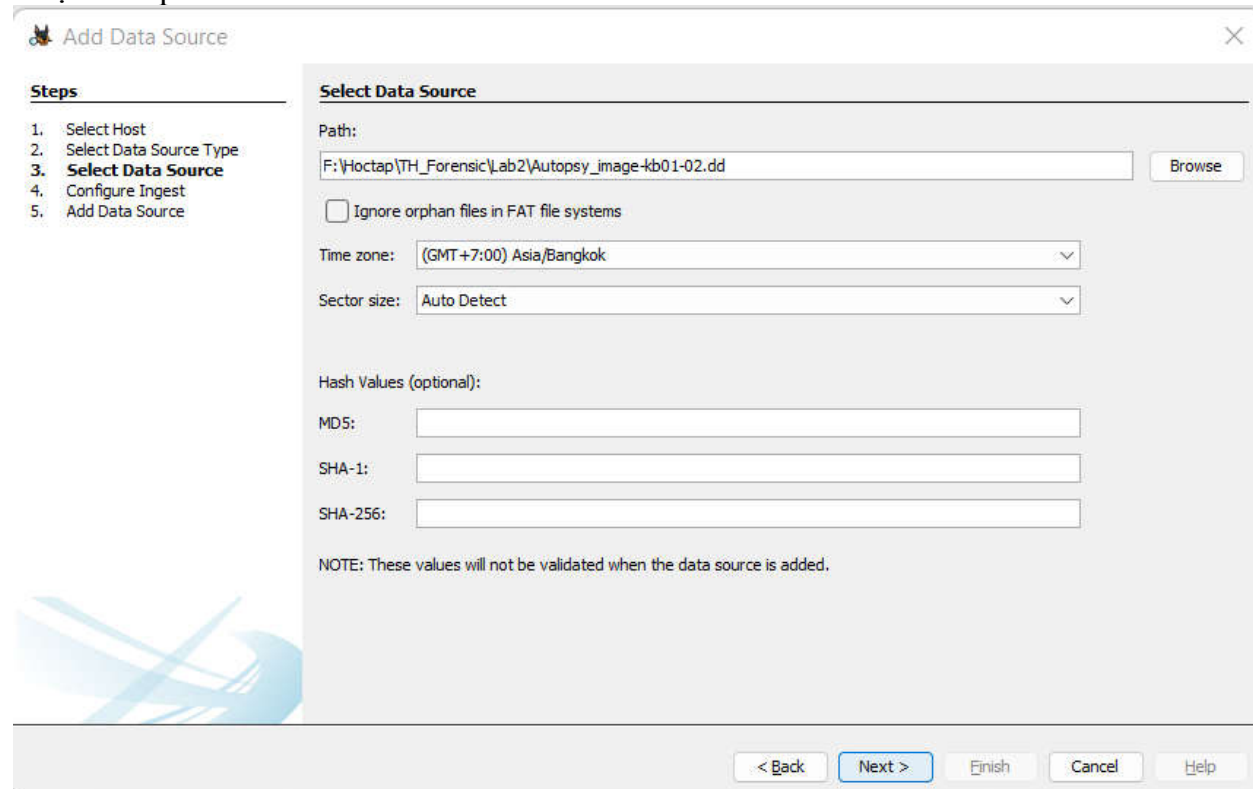
F:\Hoctap\TH_Forensic\Lab2\KB2

< Back Next > Finish Cancel Help

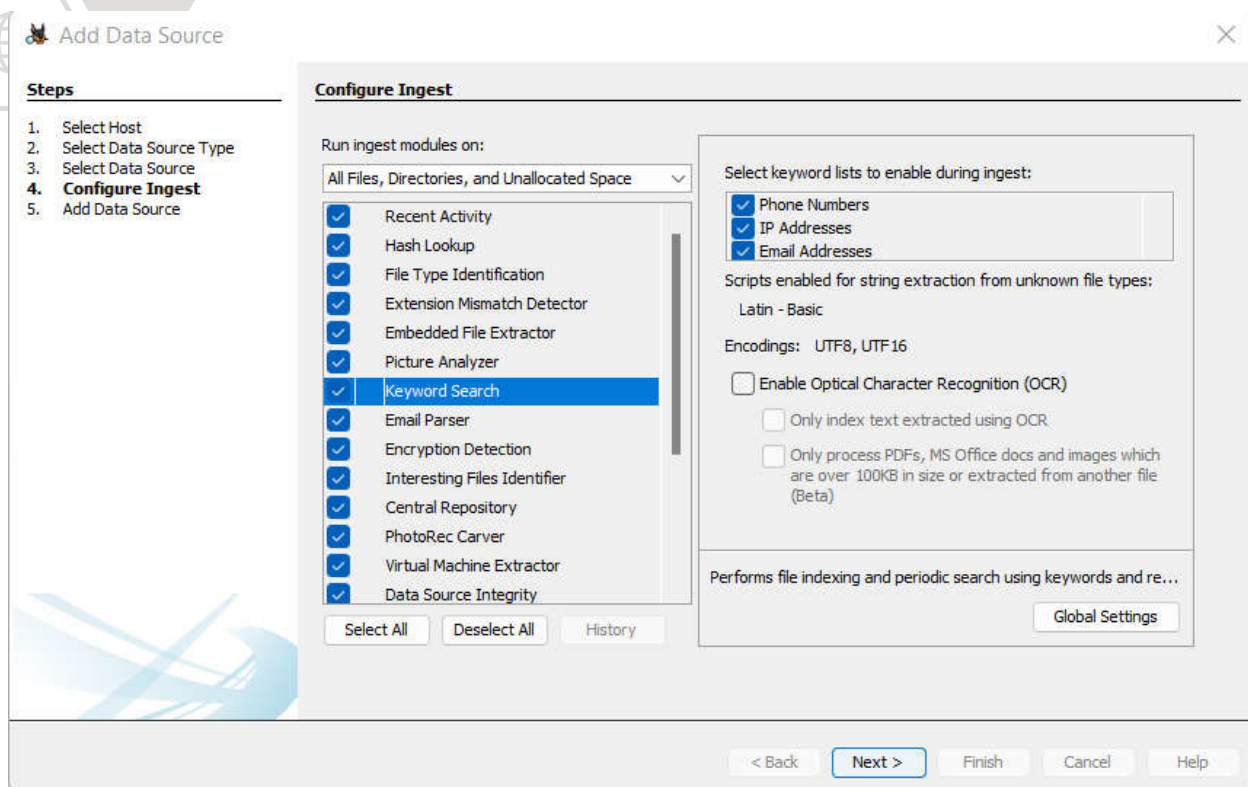
Chọn *Disk Image or VM File* để phân tích file tài nguyên đã được cung cấp



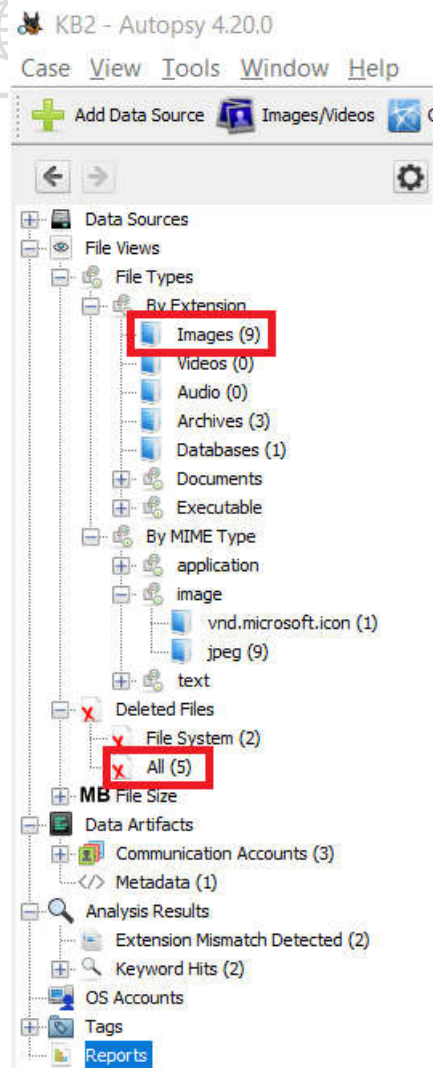
Chọn File phân tích



Chọn ra các mô-đun



Sau khi phân tích xong, tìm tất cả những hình ảnh có trong ổ đĩa đã cho bằng cách lọc theo image: *File Views* → *File Types* → *By Extension* → *Image* và *File Views* → *Deleted Files* → *All*



- Có được thông tin liên quan đến các file đó

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
✓ f0000000.jpg			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	326859	Unallocated	Unallocated	unknown
✓ f0000639.jpg			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	175630	Unallocated	Unallocated	unknown
file1.jpg			0	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
file10.jpg			0	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
file3.jpg			0	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
file4.jpg			0	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
file8.jpg			0	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
file9.jpg			0	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
image_0.jpg			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	110373	Allocated	Allocated	unknown

- Ở góc phải có tính năng save table as csv

Save Table as CSV

- Chi tiết trong các file csv. Link:
https://drive.google.com/drive/folders/1dW-SFpojIxxGgU_CZgaKQZb_nnX1U9dO?usp=sharing



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.

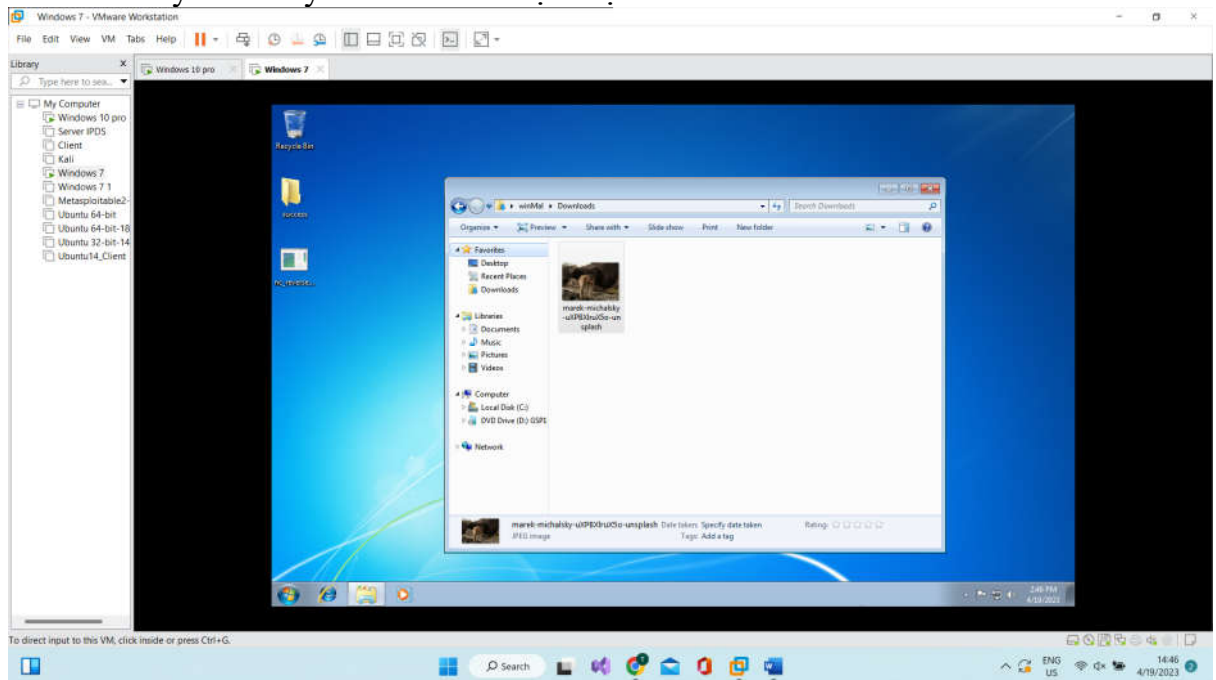
Yêu cầu: Các nhóm thực hiện chụp màn hình terminal sau khi hoàn thành điều tra bằng cách gõ các câu lệnh sau:

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

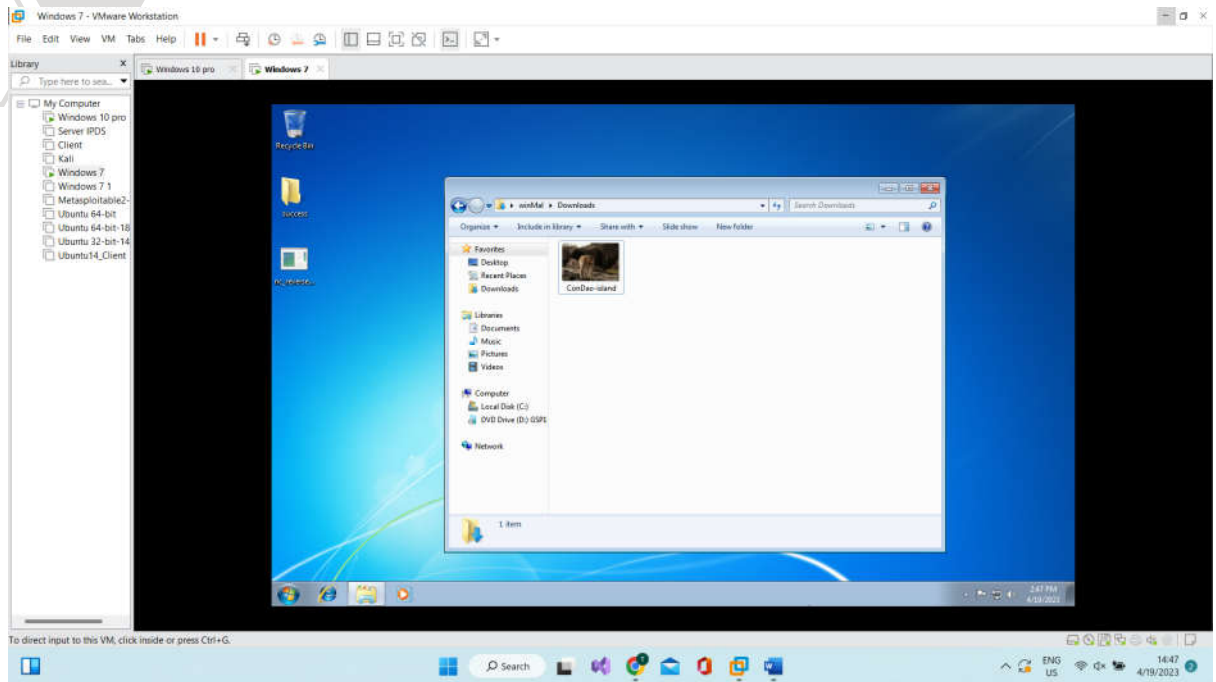
```
date /t
```

```
echo "Tên nhóm"
```

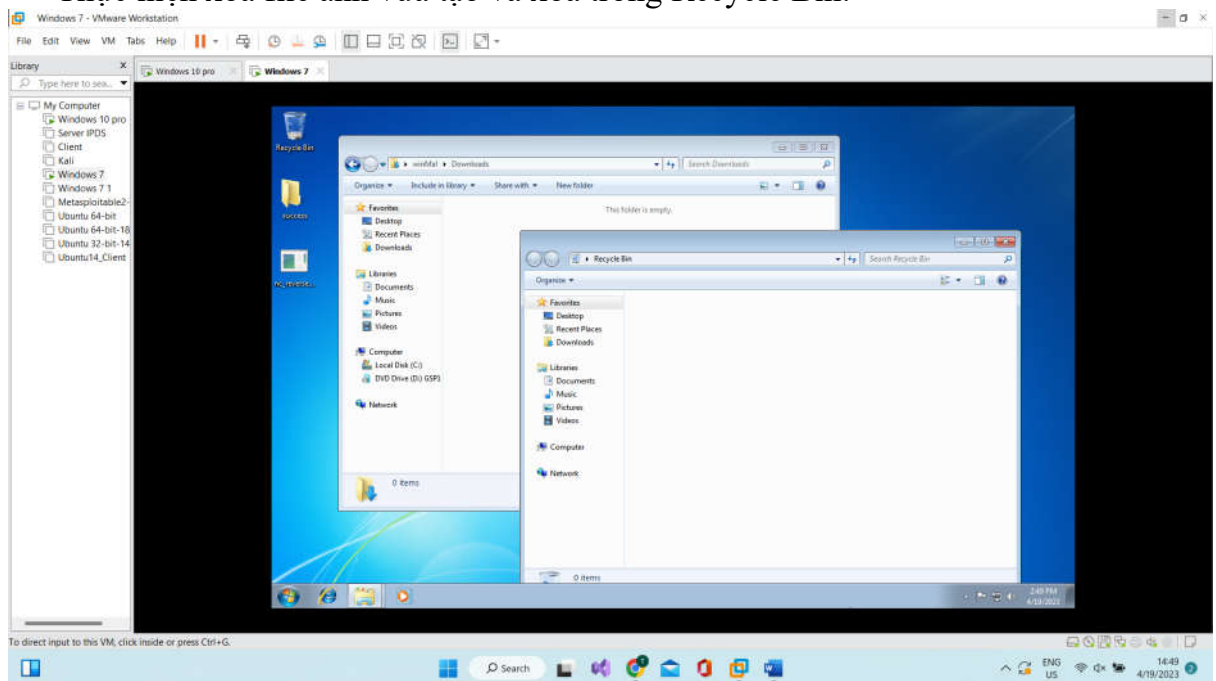
- Trên máy tính/máy ảo windows thực hiện tải về hình ảnh:



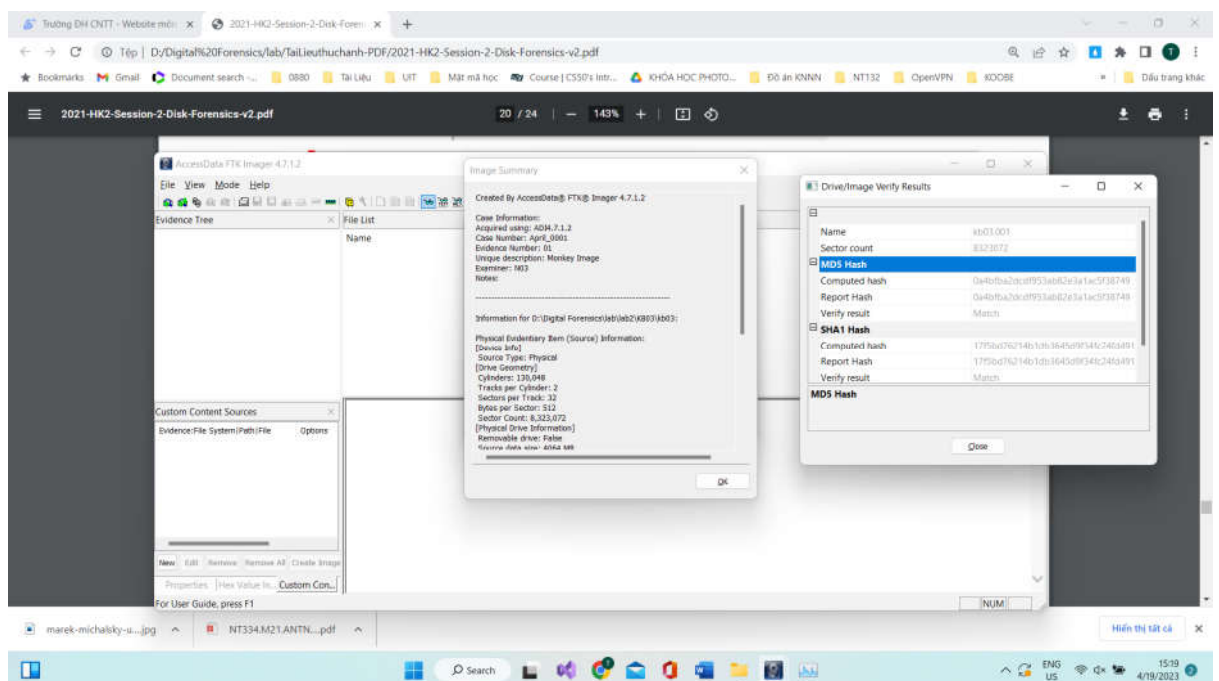
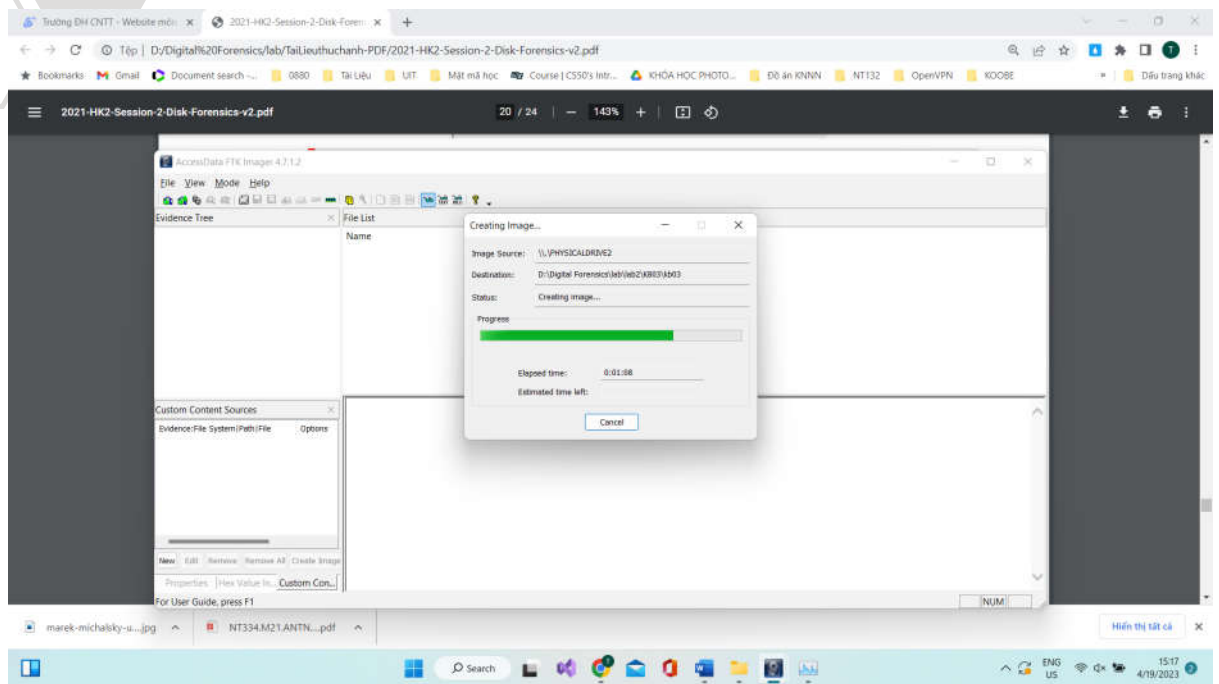
- Đặt tên ConDao-island:







- Thực hiện xóa file ảnh vừa tạo và xóa trong Recycle Bin:



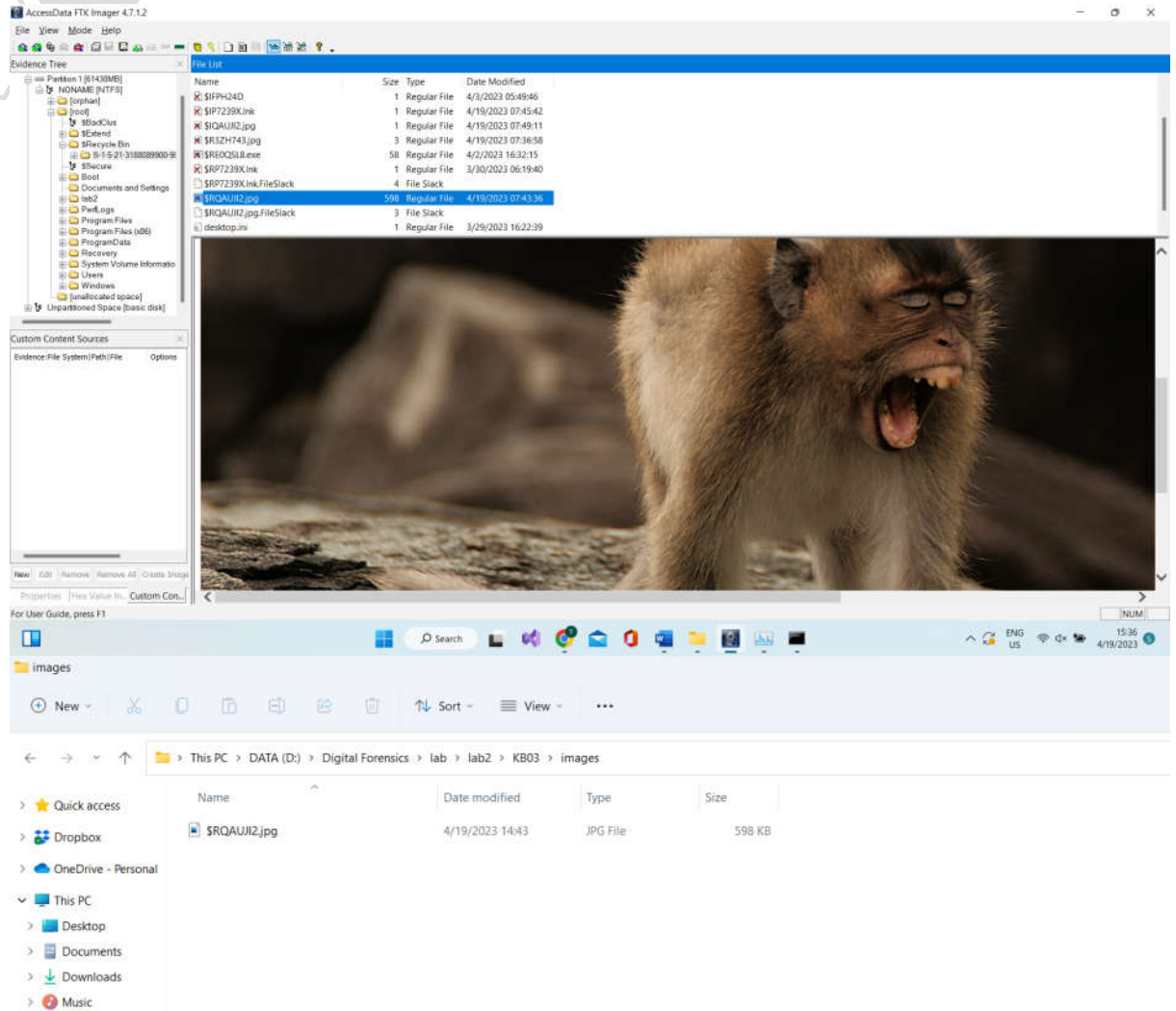
- Gắn (mounting) file ảnh của ổ đĩa (disk images) vào máy tính phân tích.
- Sau đó bắt đầu tạo ổ đĩa.



Chọn File => Add Evidence Item để chọn chứng cứ cần thêm:
Chọn file kb03.001

 kb03.001	4/19/2023 15:16	WinRAR archive	1,536,000 ...
 kb03.001.txt	4/19/2023 15:17	Text Document	2 KB
 kb03.002	4/19/2023 15:17	002 File	1,536,000 ...
 kb03.003	4/19/2023 15:17	003 File	1,089,536 ...

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

The screenshot displays the 'MD5 File Checksum' online tool interface. The tool is used to generate various hash values for a given file. The interface includes a text input field for the file name, a 'Hash' button, and an 'Auto Update' checkbox. Below the input field, the generated hash values are displayed in a table format.

MD5 File Checksum
MD5 online hash file checksum function

File name: \$RQAUJI2.jpg

Hash: ☒ Auto Update

9ee18830b6c7d85abcc9c570686463e6

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384

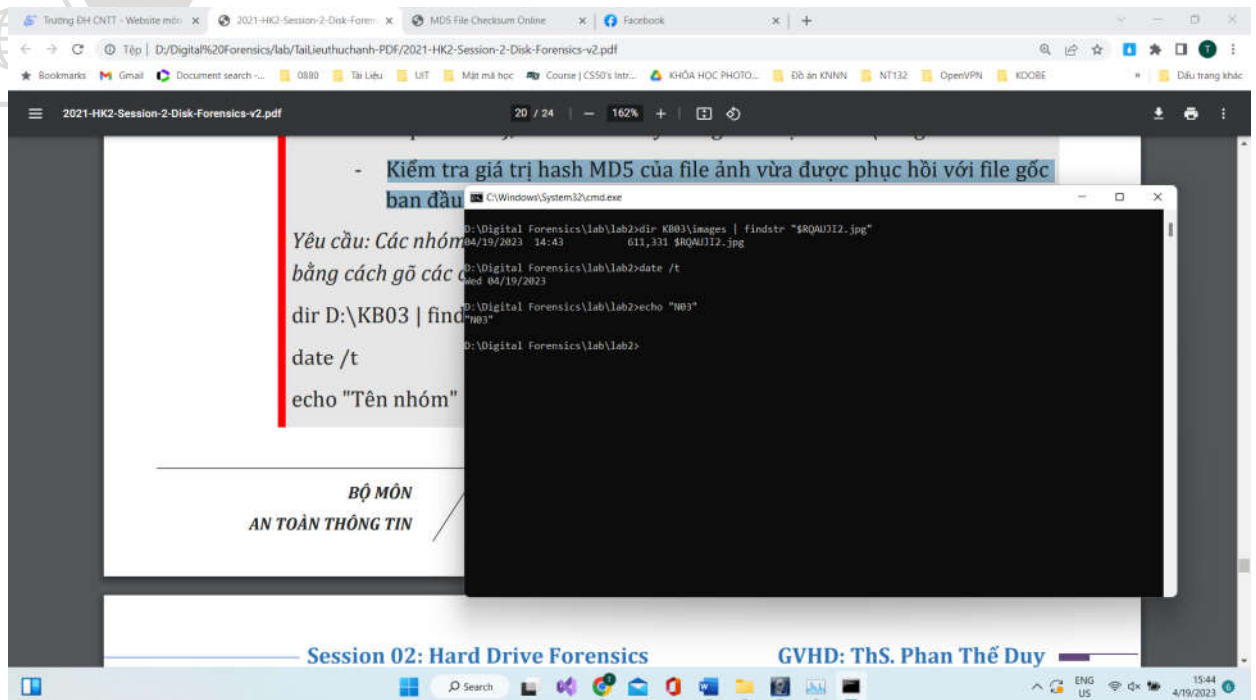
File name: ConDao-island.jpg

Hash: ☒ Auto Update

9ee18830b6c7d85abcc9c570686463e6

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384

Thêm tên nhóm sau khi hoàn thành điều tra



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

- Khởi động Autopsy để tạo một Case mới, sử dụng lựa chọn "Create New Case". Sau đó điền tên case và chọn file phân tích

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: F:\Hoctap\TH_Forensic\Lab2\F100_6db079ca91c4860f.bin Browse

☐ Ignore orphan files in FAT file systems

Time zone: (GMT+7:00) Asia/Bangkok

Sector size: Auto Detect

Hash Values (optional):

MD5:

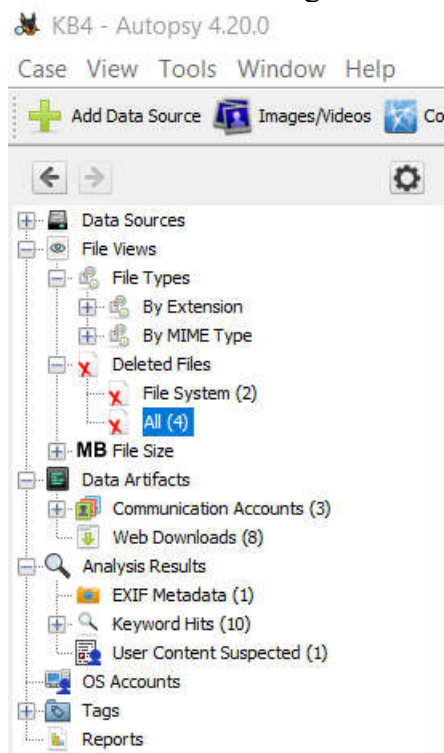
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back **Next >** Finish Cancel Help

- Tìm kiếm trong *File Views* → *Deleted Files* → *All*



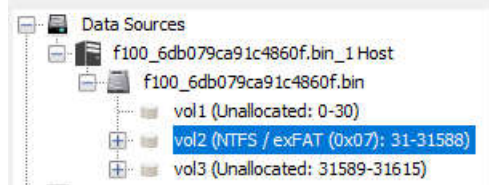
- Thấy có file key

Name	S	C	O	Modified Time	Change Time	Access Time
f0000000.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000000.txt		▼	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
key				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45:50 ICT
key:Zone.Identifier				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45:50 ICT

- Và thông tin Source File Path là
`/img_f100_6db079ca91c4860f.bin/vol_vol2/key`

Result: 1 of 1 Result < >	
Type	Value
Associated Artifact	-9223372036854775793
Source File Path	/img_f100_6db079ca91c4860f.bin/vol_vol2/key
Artifact ID	-9223372036854775792



- Vào Data Source thấy có vol2 là hệ thống tệp NTFS



- Theo gợi ý, tìm thông tin của Master File Table (MFT). Nó được hiển thị dưới dạng \$MFT

Name	S	C	O	Modified Time	Change Time	Access Time
\$AttrDef			1	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$BadClus				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$BadClus:\$Bad				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$Bitmap			0	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$Boot			0	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$CarvedFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$Extend				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$LogFile			0	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$MFT			0	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$MFTMirr			0	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$Secure:\$SDS				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT

- Xem xét nó ở dạng Hex và tìm kiếm với từ khóa “key”, tìm thấy nội dung: “notdeleted, neverexisted”

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Page: 3 of 16		Page			Go to Page: 3	Jump to Offset		Launch in HxD	
0x0000098c0:	E0 77 98 B1 EA F6 CA 01	E0 77 98 B1 EA F6 CA 01	E0 77 98 B1 EA F6 CA 01	.W.....W.....					
0x0000098d0:	E0 77 98 B1 EA F6 CA 01	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.W.....					
0x0000098e0:	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x0000098f0:	03 03 EB 00 65 00 79 00	80 00 00 00 00 00 00 00	48 00 00 00 00 00 00 00	..k.e.y.....H...					
0x000009900:	00 00 18 00 00 00 01 00	00 00 00 00 18 00 00 00						
0x000009910:	6E 00 6F 00 74 00 64 00	65 00 6C 00 65 00 74 00	n.o.t.d.e.l.e.t.						
0x000009920:	65 00 64 00 2C 00 6E 00	65 00 76 00 65 00 72 00	e.d.,n.e.v.e.r.						
0x000009930:	65 78 69 73 74 65 64 0D	0A 00 00 00 00 00 00 00	existed						
0x000009940:	80 00 00 00 58 00 00 00	00 0F 18 00 00 00 03 00	...X.....						
0x000009950:	1A 00 00 00 38 00 00 00	5A 00 6F 00 6E 00 65 00	...8...Z.o.n.e.						
0x000009960:	2E 00 49 00 64 00 65 00	6E 00 74 00 69 00 66 00	..I.d.e.n.t.i.f.						
0x000009970:	69 00 65 00 72 00 00 00	5B 5A 6F 6E 65 54 72 61	i.e.r...[ZoneTra						
0x000009980:	6E 73 66 65 72 5D 0D 0A	5A 6F 6E 65 49 64 3D 33	nsfer]..ZoneId=3						
0x000009990:	0D 0A 00 00 00 00 00 00	FF FF FF FF 82 79 47 11yG.						
0x0000099a0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						
0x0000099b0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						
0x0000099c0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						
0x0000099d0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						