



BÁO CÁO THỰC HÀNH LAB 2

Môn học: Pháp chứng kỹ thuật số

Nhóm: Pha Pha

THÀNH VIÊN THỰC HIỆN:

STT	Họ và tên	MSSV
1	Nguyễn Đoàn Xuân Bình	19521265
2	Trần Hoàng Khang	19521671
3	Nguyễn Mỹ Quỳnh	19520241

BÁO CÁO CHI TIẾT

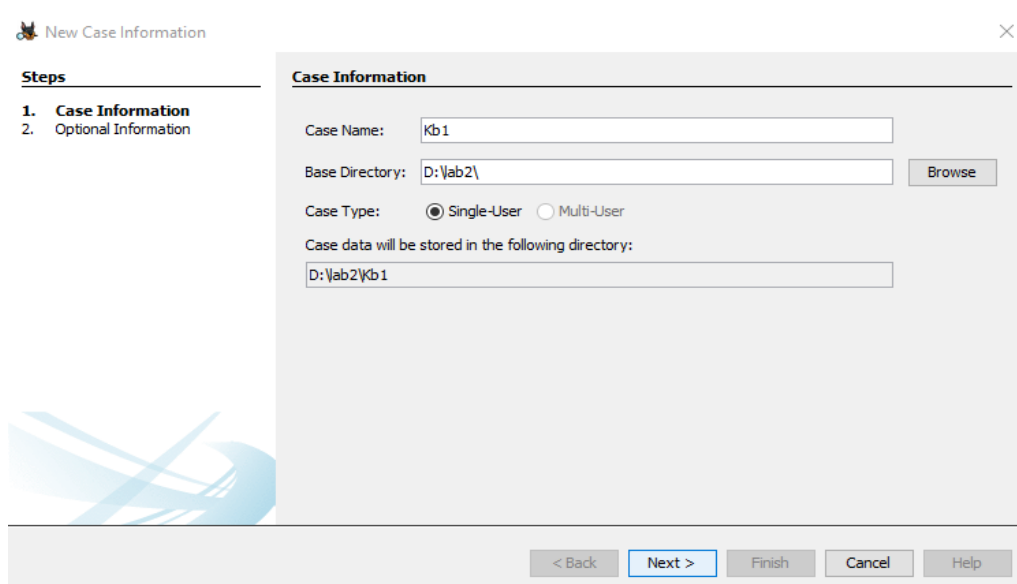
Kịch bản 01. Thực hiện phân tích dựa trên dữ liệu ổ đĩa (tự chọn)

- 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.

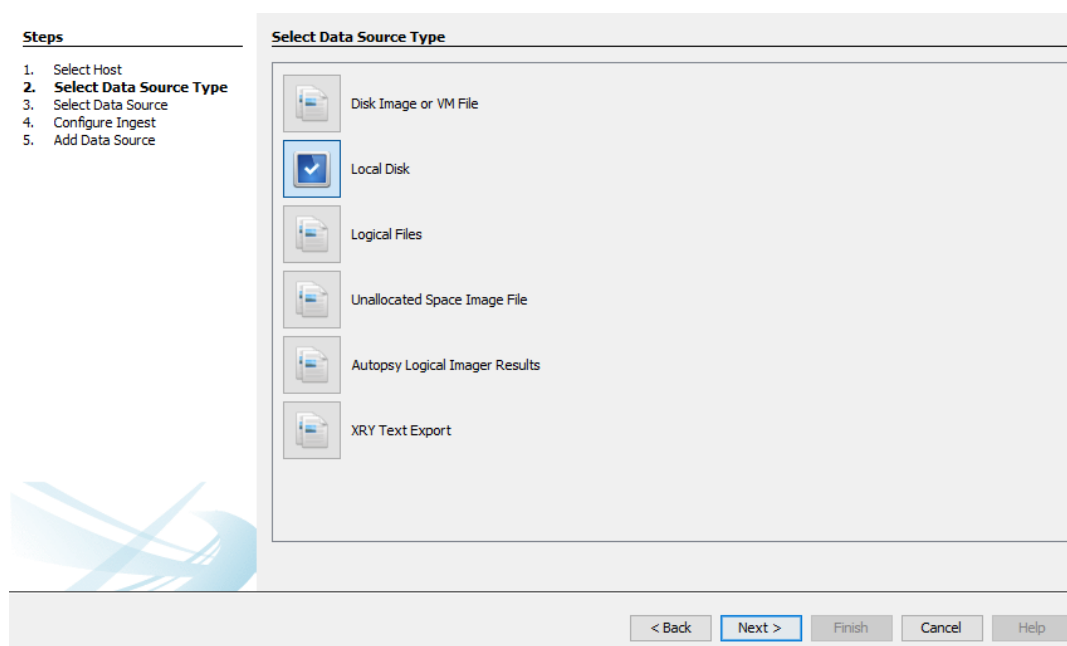
- Khởi động Autopsy và tạo một Case mới bằng option “Create New Case”



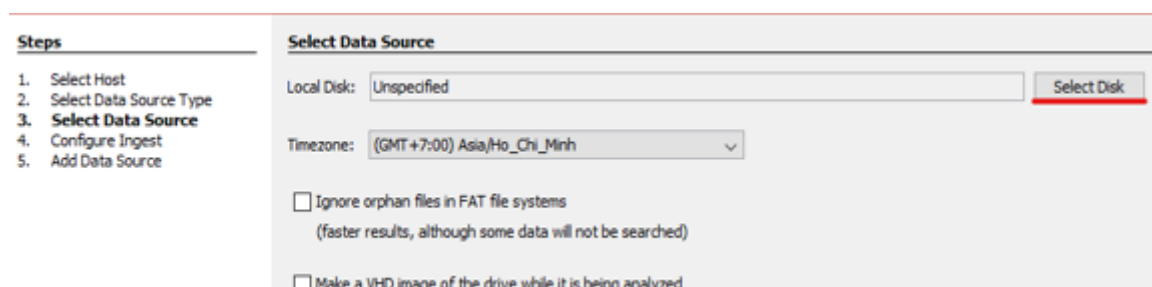
- Điền tên Case vào khung Case name



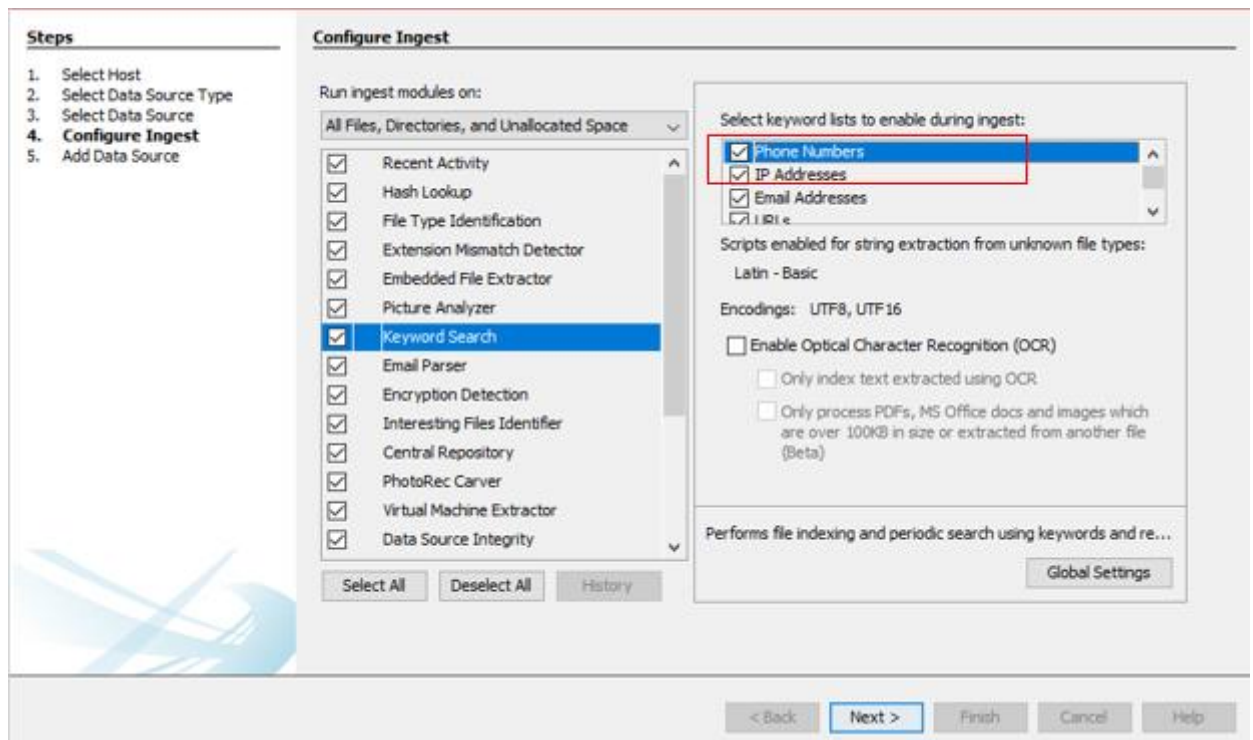
- Chọn Local Disk để phân tích các phân vùng trong máy



- Chọn Disk Name cần phân tích.



- Chọn ra các mô-đun để phân tích. Tại mô-đun Keyword Search tích chọn thêm tùy chọn IP Address và Phone Number.



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

Dump toàn bộ ổ đĩa C: (ổ hệ thống), tìm kiếm theo regex của số điện thoại: [\\.|-|?|,|;||\\.|:|[\\/\\^\\(\\)''!>|{}|(0-9){3}|][0-9]{3}([\\-|.])?[0-9]{3}([\\-|.])?[0-9]{4}[\\.|-|?|,|;||\\.|:|[\\/\\^\\(\\)''!>|{}]

☐ Exact Match ☐ Substring Match ☒ Regular Expression

☐ Restrict search to the selected data sources:

☒ Save search results

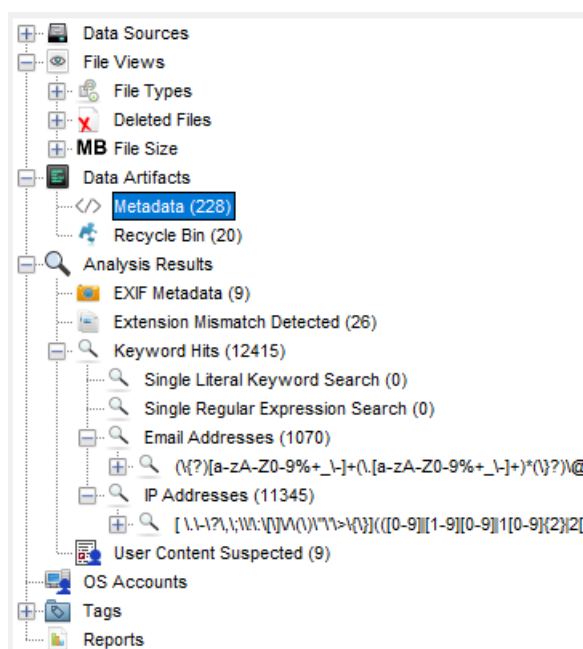
Files Indexed: 433,497 (ingest is ongoing)

Dữ liệu thu được:

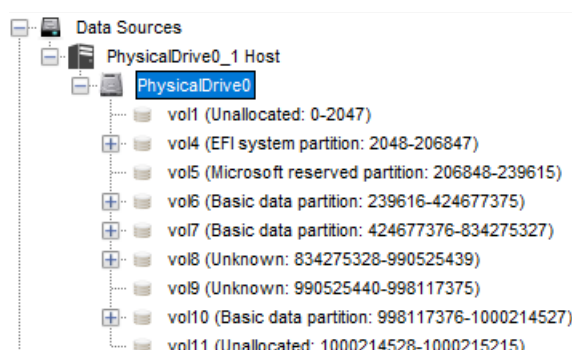
Tìm địa chỉ IP theo regex có sẵn (1 cách khác):

Danh sách có những content liên quan đến đúng định dạng địa chỉ IP được trả về :

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

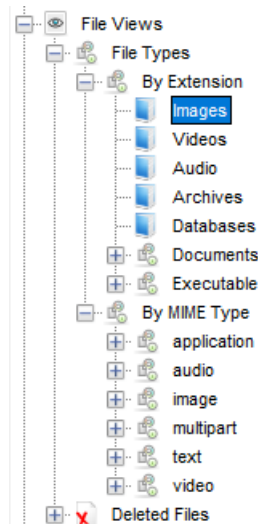


Data Source: là ổ đĩa được dump ra. Ở đây chứa các sector phân vùng của ổ đĩa.

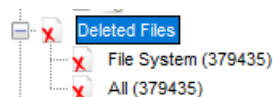


File View: Với 2 chức năng chính là :

+ **File Type:** AutoSpy có tính năng lọc file theo extension (đuôi file) hoặc topic để dễ dàng truy vết hơn. File ở đây chỉ đơn thuần được lọc theo extension mà không kiểm tra signature.



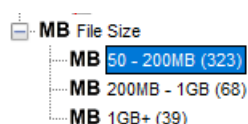
+ **Deleted files:** Lưu trữ những file đã bị xóa hoàn toàn khỏi máy PC, đa số đều không đọc được nội dung. Và có thể recover lại file nếu available.



Mình vừa mới xóa máy ảo Window 10_64bits và thấy có một số file liên quan:

File Name	File Size	File Type	File Location	File Date	File Owner	File Group	File Permissions	File Attributes	File Content
f_003fa9	464958	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/f_003fa9	2022-04-02 23:02:00 ICT	2022-04-03 08:31:57 L	2022-04-02 23:02:00 ICT	2022-04-02 23:02:00 ICT	Unknown
f_00377c	600878	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/f_00377c	2022-04-02 23:00:23 ICT	2022-04-03 08:31:57 L	2022-04-02 23:00:23 ICT	2022-04-02 23:00:23 ICT	Unknown
f_00377f	127583	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/f_00377f	2022-04-02 23:00:23 ICT	2022-04-03 08:31:57 L	2022-04-02 23:00:23 ICT	2022-04-02 23:00:23 ICT	Unknown
f_003f80	423901	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/f_003f80	2022-04-02 23:00:24 ICT	2022-04-03 08:31:57 L	2022-04-02 23:00:24 ICT	2022-04-02 23:00:24 ICT	Unknown
f_003f81	175859	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/f_003f81	2022-04-02 23:00:25 ICT	2022-04-03 08:31:57 L	2022-04-02 23:00:25 ICT	2022-04-02 23:00:25 ICT	Unknown
mksSandbox.log	51214	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/mksSandbox.log	2022-04-02 23:28:39 ICT	2022-04-03 08:31:57 L	2022-04-02 23:28:39 ICT	2022-04-02 23:28:39 ICT	Unknown
Windows 10 and later x64.nvram	270840	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/Windows 10 and later x64.nvram	2022-04-02 23:28:39 ICT	2022-04-03 08:31:57 L	2022-04-02 23:28:39 ICT	2022-04-02 23:28:39 ICT	Unknown
Windows 10 and later x64.vmx	3668	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/Windows 10 and later x64.vmx	2022-04-02 23:04:22 ICT	2022-04-03 08:31:57 L	2022-04-02 23:04:22 ICT	2022-04-02 23:04:22 ICT	Unknown
f_003f88	143007	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/f_003f88	2022-04-02 23:00:55 ICT	2022-04-03 08:31:57 L	2022-04-02 23:00:55 ICT	2022-04-02 23:00:55 ICT	Unknown
f_003f89	423177	Unallocated	Unknown	/img_PhysicalDrive0vol6/OrphanFiles/f_003f89	2022-04-02 23:00:55 ICT	2022-04-03 08:31:57 L	2022-04-02 23:00:55 ICT	2022-04-02 23:00:55 ICT	Unknown

File Size: Phân loại theo kích thước file



Data Artifact: Xem thông tin nội bộ

+ **Metadata:** List các metadata của file. Ví dụ đối với file **08_lecture-platf.pdf**

Source Name	S	C	O	Version	Date Modified	Date Created	Data Source
</> 02_lecture-basicREtool.pdf				1.5	2015-06-22 01:32:28 ICT	2015-02-03 22:59:33 ICT	PhysicalDrive0
</> 01_lecture-syllabus.pdf				1.7	2015-06-22 01:30:53 ICT	2015-01-28 01:53:38 ICT	PhysicalDrive0
</> 03_lecture-basic-RE.pdf				1.5	2015-06-22 01:59:02 ICT	2015-02-03 16:59:35 ICT	PhysicalDrive0
</> 05_lecture-shellcoding.pdf				1.5	2015-06-22 02:02:38 ICT	2015-02-21 00:39:50 ICT	PhysicalDrive0
</> 04_lecture-memory-corr.pdf				1.5	2015-06-22 02:00:10 ICT	2015-02-12 04:24:15 ICT	PhysicalDrive0
</> 07_lecture-DEP-ROP.pdf				1.7	2015-06-22 02:41:01 ICT	2015-03-11 21:41:38 ICT	PhysicalDrive0
</> 06_lecture-formatstrin.pdf				1.4	2015-06-22 02:10:36 ICT	2015-03-02 04:36:34 ICT	PhysicalDrive0
</> 08_lab.pdf				1.5	2015-02-27 19:17:45 ICT	2015-02-27 19:17:21 ICT	PhysicalDrive0
</> 09_lecture-ASLR.pdf				1.7	2015-06-22 02:19:14 ICT	2015-04-02 00:18:54 ICT	PhysicalDrive0
</> 10_lab.pdf				1.7	2015-03-11 23:06:45 ICT	2015-03-11 23:06:45 ICT	PhysicalDrive0
</> 08_lecture-platf.pdf				1.4	2015-06-22 01:23:24 ICT	2015-06-22 01:22:46 ICT	PhysicalDrive0
</> 10_lecture-heapExploit.pdf				1.7	2015-06-22 02:20:05 ICT	2015-04-08 03:28:29 ICT	PhysicalDrive0
</> 11_lecture-MiscConcept.pdf				1.7	2015-06-22 02:21:07 ICT	2015-04-17 18:16:56 ICT	PhysicalDrive0
</> 12_lab.pdf				1.7	2015-03-13 17:47:48 ICT	2015-03-13 17:47:48 ICT	PhysicalDrive0
</> 12_lecture.pdf				1.4	2015-06-22 02:21:48 ICT	2015-05-01 05:43:06 ICT	PhysicalDrive0
</> 13_lecture-Linux-kerne.pdf				1.4	2015-06-22 02:23:46 ICT	2015-05-01 05:52:45 ICT	PhysicalDrive0

Danh sách các Metadata hữu ích :

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences	Metadata
Result: 1	of 1	Result								
Type	Value									Source(s)
Version	1.4									org.sleuthkit.autopsy.keywordsearch.KeywordSearchin
Date Modified	2015-06-22 01:23:24 ICT									org.sleuthkit.autopsy.keywordsearch.KeywordSearchin
Date Created	2015-06-22 01:22:46 ICT									org.sleuthkit.autopsy.keywordsearch.KeywordSearchin
Source File Path	/img_PhysicalDrive0/vol0/home/virus/Documents/Safe_Coding/00_ModernBinaryExploitation - CSCI 4968/08_lecture-platf.pdf									
Artifact ID	-9223372038854775609									

+ **Recycle Bin:** Lưu các thư mục và file đang nằm trong “Thùng rác” (Recycle Bin) trên ổ đĩa

Source Name	S	C	O	Path	Time Deleted	Username	Data Source
SR6JZ49M.wav				C:\Users\ADMIN\Desktop\I0068424.wav	2022-04-07 23:30:57 ICT		PhysicalDrive0
SR6RM8H6.doc				C:\Users\ADMIN\Desktop\I402-8875837.doc	2022-04-08 14:22:45 ICT		PhysicalDrive0
SR6W96X.zip				C:\Users\ADMIN\Desktop\I789-2113038.zip	2022-04-07 23:32:18 ICT		PhysicalDrive0
SRHGQ5HS.jar				C:\Users\ADMIN\Desktop\I398-8821002.jar	2022-04-08 14:22:53 ICT		PhysicalDrive0
SRNZ6GOZ.cab				C:\Users\ADMIN\Desktop\I623-3485916.cab	2022-04-07 23:32:21 ICT		PhysicalDrive0
SRQK7QQU.wav				C:\Users\ADMIN\Desktop\I0061600.wav	2022-04-07 23:32:09 ICT		PhysicalDrive0
SRXOMULK.docx				C:\Users\ADMIN\Desktop\I856-secret.docx	2022-04-08 14:22:50 ICT		PhysicalDrive0
SRVMSUZE.txt				C:\Users\ADMIN\Desktop\I856-secret.docx_secret.txt	2022-04-07 23:33:08 ICT		PhysicalDrive0
SR8Q7QOS				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\wb5	2022-04-07 19:34:21 ICT		PhysicalDrive0
SR8E4M7C				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\wb6	2022-04-07 23:04:57 ICT		PhysicalDrive0
SR8P9JC				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\wb1	2022-04-08 15:02:03 ICT		PhysicalDrive0
SRDFEW08				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\wb5	2022-04-07 23:04:57 ICT		PhysicalDrive0
SRDKHOL				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\wb0	2022-04-07 21:10:57 ICT		PhysicalDrive0
SRQ96LY9.zip				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\wb0	2022-04-07 21:10:57 ICT		PhysicalDrive0
SRJ2N734.docx				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\NT...	2022-04-07 21:11:02 ICT		PhysicalDrive0
SR03E50H.raw				D:\HANG\Document\ForStudy\Digital forensic\Lab\Lab2\56...	2022-04-07 21:11:00 ICT		PhysicalDrive0

Analysis results: Đây là trường thông tin quan trọng phân tích kết quả thu thập được sau khi dump bộ nhớ, được thực hiện bởi các plug-in.

+ **Exif Metadata:** Thông tin metadata được trích xuất bởi công cụ Exif, cho nhiều thông tin hơn, thấy nó không khác gì metadata phân tích bình thường là mấy

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

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Extension	MIME Type	File Path
cschlosser.doxdocgen-1.3.2			3	File	Likely Notable			File has MIME type of application/x-ooxml	2	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
esbemp.prettier-vscode-9.3.0			3	File	Likely Notable			File has MIME type of application/x-ooxml	0	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
jeff-hykin.better-cpp-syntax-1.15.13			3	File	Likely Notable			File has MIME type of application/x-ooxml	13	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-edgesidebars.vscod-edge-devtools-1.4.5			3	File	Likely Notable			File has MIME type of application/x-ooxml	5	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-python.python-2022.0.1814523869			3	File	Likely Notable			File has MIME type of application/x-ooxml	1814523869	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-python.vscod-pylance-2022.2.3			3	File	Likely Notable			File has MIME type of application/x-ooxml	3	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-vscode.remote.remote-ssh-0.74.0			3	File	Likely Notable			File has MIME type of application/x-ooxml	0	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-toolsai.jupyter-2022.1.1301854968			3	File	Likely Notable			File has MIME type of application/x-ooxml	1301854968	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-vscode.remote.remote-ssh-edl-0.74.0			3	File	Likely Notable			File has MIME type of application/x-ooxml	0	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-vscode.remote.remote-wsl-0.64.2			3	File	Likely Notable			File has MIME type of application/x-ooxml	2	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-vscode.cmake-tools-1.9.2			3	File	Likely Notable			File has MIME type of application/x-ooxml	2	application/x-ooxml	Img_PhysicalDrive0\vol_vo8
ms-vscode.cpptools-extension-pack-1.1.0			3	File	Likely Notable			File has MIME type of application/x-ooxml	0	application/x-ooxml	Img_PhysicalDrive0\vol_vo8

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

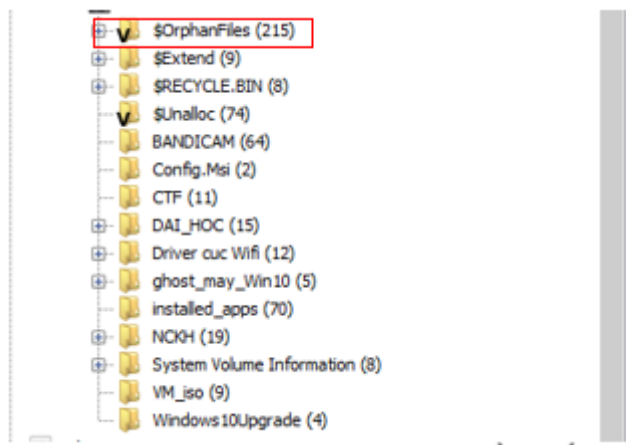
OS Account: Toàn bộ account trên hệ thống, bao gồm cả account của ứng dụng

Tags: Các tags được điều tra viên gắn nhãn

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

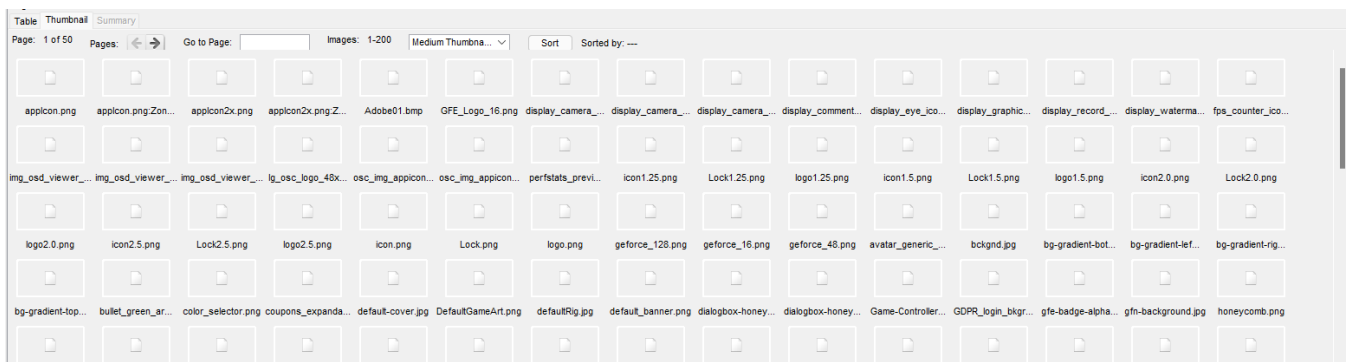
NOTE: Ngoài ra còn một số kết quả khác nếu để chạy Ingest Analysis đủ lâu thì sẽ có các phân tích khác trên nhiều module như Web Cookie, Web History, Cache , ...

- **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.**

Xem bằng thumbnail. Nếu chạy analyze đầy đủ thì nó sẽ đọc được thông tin ảnh, nhưng ở đây vì ổ đĩa gần hết nên mình để vậy.



Số lượng file **PDF** ta có thể xem bằng cách lọc file **.pdf**, **AutoSpy** đã giúp ta thực hiện việc này:

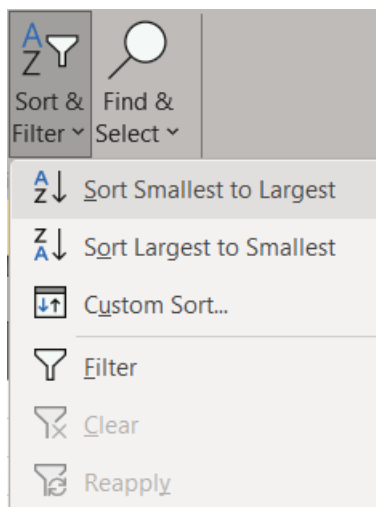
PDF														953 Results		
Table Thumbnail Summary																
Page: 1 of 1		Pages:  		Go to Page: <input type="text"/>												Save Table as CSV
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location				
 1.pdf				2022-02-05 11:14:06 ICT	2022-02-05 11:14:06 ICT	2022-03-05 20:08:09 ICT	2022-02-05 11:14:06 ICT	0	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...				
 Day02 Computer Forensics Investigation ProcessPost[7				2022-04-08 14:30:38 ICT	2022-04-08 14:30:38 ICT	2022-04-08 14:30:38 ICT	2022-04-08 14:30:38 ICT	2448894	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...				
 First Responder Procedures2-s[5].pdf				2022-04-08 14:30:57 ICT	2022-04-08 14:30:57 ICT	2022-04-08 14:30:57 ICT	2022-04-08 14:30:57 ICT	6344730	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...				
 lab01-forensic-withoutflag[4].pdf				2022-04-08 14:30:59 ICT	2022-04-08 14:30:59 ICT	2022-04-08 14:30:59 ICT	2022-04-08 14:30:59 ICT	1383697	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...				
 NT230.M21.ANTN-Lab3_Nhom_19521671-19521265-1				2022-04-08 14:31:02 ICT	2022-04-08 14:31:02 ICT	2022-04-08 14:31:02 ICT	2022-04-08 14:31:02 ICT	1800176	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...				
 Week03-Digital Evidence3-post[9].pdf				2022-04-08 14:30:47 ICT	2022-04-08 14:30:47 ICT	2022-04-08 14:30:47 ICT	2022-04-08 14:30:47 ICT	7360565	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...				
 40-TB Tiếp nhận Sinh viên vào ở KTX.pdf				2022-02-07 19:06:19 ICT	2022-02-07 19:06:19 ICT	2022-03-20 20:19:11 ICT	2022-02-07 19:06:19 ICT	2508805	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\Documents\Zab...				
 3253.pdf				2022-03-31 16:57:19 ICT	2022-03-31 16:57:20 ICT	2022-03-31 16:57:25 ICT	2022-03-31 16:57:18 ICT	453026	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\Downloads\Doc...				
 3_Attiques et ControleAccesBDR.pdf				2022-03-31 19:18:05 ICT	2022-03-31 19:18:06 ICT	2022-03-31 19:18:15 ICT	2022-03-31 19:18:04 ICT	651648	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\Downloads\Doc...				
 455-F005.pdf				2022-03-30 22:44:31 ICT	2022-03-30 22:44:32 ICT	2022-03-30 22:45:31 ICT	2022-03-30 22:44:30 ICT	677431	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\Downloads\Doc...				
 Carrier, Brian - File System Analysis.pdf				2022-03-29 09:30:32 ICT	2022-03-29 09:30:32 ICT	2022-03-29 11:21:22 ICT	2022-03-29 09:30:23 ICT	4220759	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\Downloads\Doc...				
 De-thi-mau-DHOG-HCM-2022.pdf				2022-02-09 14:37:13 ICT	2022-02-09 14:37:17 ICT	2022-02-10 14:25:34 ICT	2022-02-09 14:37:12 ICT	594509	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\Downloads\Doc...				
 EN - Time based blind SQL injection using heavy queriet				2022-04-01 23:28:18 ICT	2022-04-01 23:28:18 ICT	2022-04-01 23:28:20 ICT	2022-04-01 23:28:14 ICT	610316	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\Downloads\Doc...				
 90RXH4.pdf				2022-02-13 15:40:47 ICT	2022-02-13 15:40:47 ICT	2022-02-13 15:44:25 ICT	2022-02-13 15:40:47 ICT	118	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Recycle Bin\S-1-5-21-24185...				
 Acer Regulatory Information and Safety Guide.pdf				2020-04-24 08:52:20 ICT	2021-10-30 23:50:20 ICT	2021-10-31 01:06:09 ICT	2017-06-14 21:06:04 ICT	32940138	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\JCOMP\Preload\Autoun\GUI\ac...				

Số lượng file PDF là 953.

Số lượng file Word .doc phải kiểm bằng tay, không có sẵn bộ lọc, vì vậy mình phải có cách xử lý riêng. Vào File View → File Type → By extension → Document → Office

Page: 1 of 1 Pages: Go to Page: Save Table as CSV															
C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash	MIME Type	Extension	
		2021-05-15 14:10:18 ICT	2022-02-10 14:28:58 ICT	2022-02-10 14:28:58 ICT	2022-02-10 14:28:58 ICT	51260	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\ProgramData\NVIDIA Corporat...			docx		
		2022-03-01 20:59:30 ICT	2022-03-01 20:59:30 ICT	2022-03-01 20:59:30 ICT	2022-03-01 20:59:30 ICT	223800	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\vscode\extensi...			doc		
		2022-03-16 23:11:06 ICT	2022-03-16 23:11:06 ICT	2022-03-16 23:11:06 ICT	2022-03-16 23:11:06 ICT	0	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		
		2022-03-18 23:47:03 ICT	2022-03-18 23:47:03 ICT	2022-03-18 23:47:03 ICT	2022-03-18 23:47:03 ICT	10664	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			xlsx		
		2022-03-18 23:47:03 ICT	2022-03-18 23:47:03 ICT	2022-03-18 23:47:03 ICT	2022-03-18 23:47:03 ICT	188	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			xlsx		
		2022-04-01 09:29:22 ICT	2022-04-01 09:29:22 ICT	2022-04-01 09:29:22 ICT	2022-04-01 09:29:22 ICT	10829	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			xlsx		
		2022-04-01 09:29:22 ICT	2022-04-01 09:29:22 ICT	2022-04-01 09:29:22 ICT	2022-04-01 09:29:22 ICT	205	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			xlsx		
		2022-03-16 10:24:56 ICT	2022-03-16 10:24:56 ICT	2022-03-16 10:24:56 ICT	2022-03-16 10:24:56 ICT	62734	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		
		2022-03-16 10:24:56 ICT	2022-03-16 10:24:56 ICT	2022-03-16 10:24:56 ICT	2022-03-16 10:24:56 ICT	96	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		
		2022-03-16 10:28:35 ICT	2022-03-16 10:28:35 ICT	2022-03-16 10:28:35 ICT	2022-03-16 10:28:35 ICT	67430	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		
		2022-03-16 10:28:35 ICT	2022-03-16 10:28:35 ICT	2022-03-16 10:28:35 ICT	2022-03-16 10:28:35 ICT	96	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		
		2022-03-16 10:48:25 ICT	2022-03-16 10:48:25 ICT	2022-03-16 10:48:25 ICT	2022-03-16 10:48:25 ICT	63020	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		
		2022-03-16 10:48:25 ICT	2022-03-16 10:48:25 ICT	2022-03-16 10:48:25 ICT	2022-03-16 10:48:25 ICT	96	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		
		2022-03-16 10:44:35 ICT	2022-03-16 10:44:35 ICT	2022-03-16 10:44:35 ICT	2022-03-16 10:44:35 ICT	62797	Allocated	Allocated	unknown	\\mg_PhysicalDrive0\vol_vo6\Users\ADMIN\AppData\Local...			pptx		

Sau đó xuất file ra .csv để xử lý bên Excel cho dễ. Sort lại extension để gom các file .doc và .docx lại 1 nhóm :



Bảng được sort theo extension:

Name	Modified T	Change T	Access T	Created T	Size	Flags(Dir)	Flags(Met	Known	Location	MD5 Hash	SHA-256 H	MIME Typ	Extension
_I_Lucene	2022-03-0	2022-03-0	2022-03-0	2022-03-0	223800	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Users/ADMIN				doc
\$I6RM8H6	2022-04-0	2022-04-0	2022-04-0	2022-04-0	106	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin				doc
\$R6RM8H	2022-04-0	2022-04-0	2022-04-0	2022-04-0	1104	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin				doc
PROTTPLN	2022-01-2	2022-03-1	2022-01-2	2022-01-2	19968	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Program File				doc
PROTTPLV	2022-01-2	2022-03-1	2022-01-2	2022-01-2	19968	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Program File				doc
Canon Cop	2021-10-3	2021-10-3	2022-03-0	2021-10-3	22016	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Program File				doc
MsolrmPr	2021-06-0	2022-02-0	2022-02-1	2021-06-0	24064	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Windows/Sy				doc
MsolrmPr	2021-06-0	2022-02-0	2022-02-1	2021-06-0	24064	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Windows/Sy				doc
MsolrmPr	2021-06-0	2022-02-0	2022-02-1	2021-06-0	24064	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Windows/Wi				doc
MsolrmPr	2021-06-0	2022-02-0	2022-02-1	2021-06-0	24064	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Windows/Wi				doc
_0_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	5123221	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BI				doc
_0_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	2066753	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BI				doc
_0_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	36241	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BI				doc
_0_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	4672574	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BI				doc
_1_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	20722	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BI				doc
_2_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	1040651	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BI				doc
_0_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	3126996	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Docu				doc
_1_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	2255365	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Docu				doc
_2_Lucene	2022-04-0	2022-04-0	2022-04-0	2022-04-0	145118	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Docu				doc
_4_Lucene	2022-02-2	2022-02-2	2022-03-1	2022-02-2	346724	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Setu				doc
_1_Lucene	2022-02-2	2022-02-2	2022-02-2	2022-02-2	62217	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Setu				doc
_1_Lucene	2022-02-2	2022-02-2	2022-02-2	2022-02-2	112202	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Setu				doc
cs-fonts.d	1998-12-1	2022-03-1	1998-12-1	1998-12-1	7384	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Soft				doc
sympmi_re	2009-10-0	2022-03-1	2022-03-1	2009-10-0	101376	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Soft				doc
ThirdParty	2013-12-1	2022-01-2	2022-01-2	2022-01-2	25088	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol7/KHANG/Soft				doc

Dùng hàm **count()** và thực hiện lên các dòng có extension **.doc** và **.docx**

SUM													
=COUNT(A2:N132)													
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Modified T	Change T	Access T	Created T	Size	Flags(Dir)	Flags(Met	Known	Location	MD5 Hash	SHA-256 H	MIME Typ
2	_I_Lucene	2022-03-0	2022-03-0	2022-03-0	2022-03-0	223800	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Users/ADMIN			
3	\$I6RM8H6	2022-04-0	2022-04-0	2022-04-0	2022-04-0	106	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin			
4	\$R6RM8H	2022-04-0	2022-04-0	2022-04-0	2022-04-0	1104	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin			
5	PROTTPLN	2022-01-2	2022-03-1	2022-01-2	2022-01-2	19968	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Program File			
6	PROTTPLV	2022-01-2	2022-03-1	2022-01-2	2022-01-2	19968	Allocated	Allocated	unknown	/img_PhysicalDrive0/vol_vol6/Program File			

Kết quả là **131** dòng tương ứng với **131** file











- 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.

Chọn *Generate Report* → *HTML Report* → Báo cáo dạng HTML

Có một file report.html là file chính để hiển thị layout thông tin. Thư mục content chứa các file phụ trợ (ảnh, .html, ...) để đưa tài nguyên vào file HTML.

Nội dung báo cáo cô đọng, tập trung vào kết quả được xuất bởi các Analysis Modules và Search bởi người xem

Report Navigation

-  Case Summary
-  EXIF Metadata (9)
-  Extension Mismatch Detected (26)
-  Keyword Hits (12826)
-  Metadata (228)
-  Recycle Bin (20)
-  Tagged Files (0)
-  Tagged Images (0)
-  Tagged Results (0)
-  User Content Suspected (9)

Ví dụ kết quả của Keyword Hits. Các phần User search:

User Searches

.doc	Preview	S
71-19521265-19520241«.doc«x time deleted : 202	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BIN/S-1-5-21-2418528453-4143256655-726105812-1001/\$RJ2N734.docx	
\desktop\402-8875837«.doc«x time deleted : 2022	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin/S-1-5-21-2418528453-4143256655-726105812-1001/\$R6RM8H6.doc	
n\desktop\856-secret«.doc«x time deleted : 202	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin/S-1-5-21-2418528453-4143256655-726105812-1001/\$RXOMULK.docx	
n\desktop\858-secret«.doc«x_secret.txt time de	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin/S-1-5-21-2418528453-4143256655-726105812-1001/\$RYMSUZE.txt	
nt").listen(document«.doc«umentelement,a,f,c")	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/00A2BC8EEE9412D080C8876F1I	
y a)(t).innerwidth>t«.doc«umentelement.clientw	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/01214DDB8CB386FB2F5270A58;	
,b,c){var d=document«.doc«umentelement;d=dl=nu	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/02BCEBBFD8BA8F18058C49834	
rtant_software_phone«.doc«x.png" content-type:	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/033954C1CDFA28F5DE64176AD	
defaultview window)«.doc«ument,q=null==(n=p.	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/035F863E7E349D61376D738151I	
l==typeof n){var r=e«.doc«ument;"number"l==typ	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/03A3D2BFFAD0A39A9456A434F!	
a,b){return a==b a«.doc«umentelement&&a.docu	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/0422EAE02D8E76AAC83BB4A9B	
ancelable:IO});(g=da«.doc«ument.createevent("c	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/0655F188C0CE016B8FC41572F9	

Và phần search và parse của AutoSpy plugin, ví dụ thông tin email:

Email Addresses

%ssupport@hex-rays.com	Preview	Source File	Tags
2007-2022 hex-rays «%ssupport@hex-rays.com»%s</div> <d		/img_PhysicalDrive0/vol_vol8/home/virus/idafree-7.7/plugins/hexx64.so	
100320005b7d5e28@live.com	Preview	Source File	Tags
:"i:0h.f membership «100320005b7d5e28@live.com»","cachetoken":"0"} /img_PhysicalDrive0/vol_vol8/home/virus/.mozilla/firefox/ua9vydus.default-esr/webappsstore.sqlite			
1552xxxx@gm.uit.edu.vn	Preview	Source File	Tags
ân quyết 1552xxxx «1552xxxx@gm.uit.edu.vn» 2 nguyên hoàng h		/img_PhysicalDrive0/vol_vol8/home/virus/.local/share/Trash/files/SharingZone-NT521.zip/SharingZone-NT521/Exercises/tem	
1552yyyy@gm.uit.edu.vn	Preview	Source File	Tags
oàng hải 1552yyyy «1552yyyy@gm.uit.edu.vn» 2. nội dung thực		/img_PhysicalDrive0/vol_vol8/home/virus/.local/share/Trash/files/SharingZone-NT521.zip/SharingZone-NT521/Exercises/templ	
17520242@gm.uit.edu.vn	Preview	Source File	Tags
nhật anh 17520242 «17520242@gm.uit.edu.vn» 2. nội dung thực		/img_PhysicalDrive0/vol_vol8/home/virus/.local/share/Trash/files/SharingZone-NT521.zip/SharingZone-NT521/Seminar/ATCL	
17520642@gm.uit.edu.vn	Preview	Source File	Tags
iệt khoa 17520642 «17520642@gm.uit.edu.vn» 4 nguyên nhật an		/img_PhysicalDrive0/vol_vol8/home/virus/.local/share/Trash/files/SharingZone-NT521.zip/SharingZone-NT521/Seminar/ATCL	
18520085@ms.uit.edu.vn	Preview	Source File	Tags

Chọn *Generate Report* → *Excel Report* → *Báo cáo dạng Excel*

Excel thì cho lại giao diện “ít thiện cảm” hơn. Navigate không qua sub-link như HTML mà thông qua các sheet.

Summary	EXIF Metadata	Keyword Hits	Metadata	Recycle Bin	User Content Suspected	Extension Mismatch ...	+	:	◀
---------	---------------	--------------	----------	-------------	------------------------	------------------------	---	---	---

Kết quả cho lại thì hoàn toàn giống với been HTML

Ví dụ như been **Keyword Hits**, **User Search**:

User Searches	Source File
.doc	
Preview	
71-19521265-19520241«.doc»time deleted : 202	/img_PhysicalDrive0/vol_vol7/\$RECYCLE.BIN/S-1-5-21-2418528453-4143256655-726105812-1001/SR12N734.docx
\desktop\402-8875837«.doc»time deleted : 2022	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin/S-1-5-21-2418528453-4143256655-726105812-1001/SR6RM8H6.doc
n\desktop\856-secret«.doc»time deleted : 202	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin/S-1-5-21-2418528453-4143256655-726105812-1001/SRXOMULK.docx
n\desktop\858-secret«.doc»_secret.txttime de	/img_PhysicalDrive0/vol_vol6/\$Recycle.Bin/S-1-5-21-2418528453-4143256655-726105812-1001/SRYMSUZE.txt
nt").list(document«documentelement,a,f,c("	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/00A2BC8EE9
y.a).t).innerwidth««.documentelement.clientw	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/01214DDB8C
,b,c){var d=document«documentelement;d=d=nu	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/02BCEBFD8
rtant_software_phone«.doc».png»content-type:	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/033954C1CD
defaultview} window «.doc»ment,q=null==(n=p.	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/035F863E7E3
l==typeof n) var r=e«.doc»ment;"number"!==typ	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/03A3D2BFFA
a,b){return a==b} a«.doc»mentelement&&a.docu	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/0422EAE02D
ancelable: 0):lg=d«.doc»ment.createevent("c	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/0655F188C0
mutationobserver=a«.doc»ment,t=1,r=0,o=0cc	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/0697CF7C8B4
pe.foreach?document«.doc»mentelement.classli	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/0775B8DE637
on we(e){for(var t=«.doc».history.done,n=t.le	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/07E6C490CE5
rts?module.exports=«.doc»ment?{t(e, 0):functi	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/08A701C1BE
ancelable: 0):lg=«.doc»ment.createevent("c	/img_PhysicalDrive0/vol_vol8/home/virus/.cache/mozilla/firefox/ua9vydus.default-esr/cache2/entries/0901DEC5E6

Been **AutoSpy** phân tích và search:

Email Addresses	Source File
%ssupport@hex-rays.com	
Preview	
2007-2022 hex-rays «%ssupport@hex-rays.com»%s</div> <d	/img_PhysicalDrive0/vol_vol8/home/virus/idafree-7.7/plugins/hexx64.so
100320005b7d5e28@live.com	
Preview	
:"i:0h.f membership «100320005b7d5e28@live.com»","cachetoken":"0")	/img_PhysicalDrive0/vol_vol8/home/virus/.mozilla/firefox/ua9vydus.default-esr/webappsstore.sqlite
1552xxxx@gm.uit.edu.vn	
Preview	
ân quyết1552xxxx«1552xxxx@gm.uit.edu.vn»2 nguyên hoàng h	/img_PhysicalDrive0/vol_vol8/home/virus/.local/share/Trash/files/SharingZone-NT521.zip/SharingZone-NT521/Exerc
1552yyyy@gm.uit.edu.vn	
Preview	
oàng hải1552yyyy«1552yyyy@gm.uit.edu.vn»2. nội dung thực	/img_PhysicalDrive0/vol_vol8/home/virus/.local/share/Trash/files/SharingZone-NT521.zip/SharingZone-NT521/Exerc
17520242@gm.uit.edu.vn	
Preview	
nhật anh17520242«17520242@gm.uit.edu.vn»2. nội dung thực	/img_PhysicalDrive0/vol_vol8/home/virus/.local/share/Trash/files/SharingZone-NT521.zip/SharingZone-NT521/Semir

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

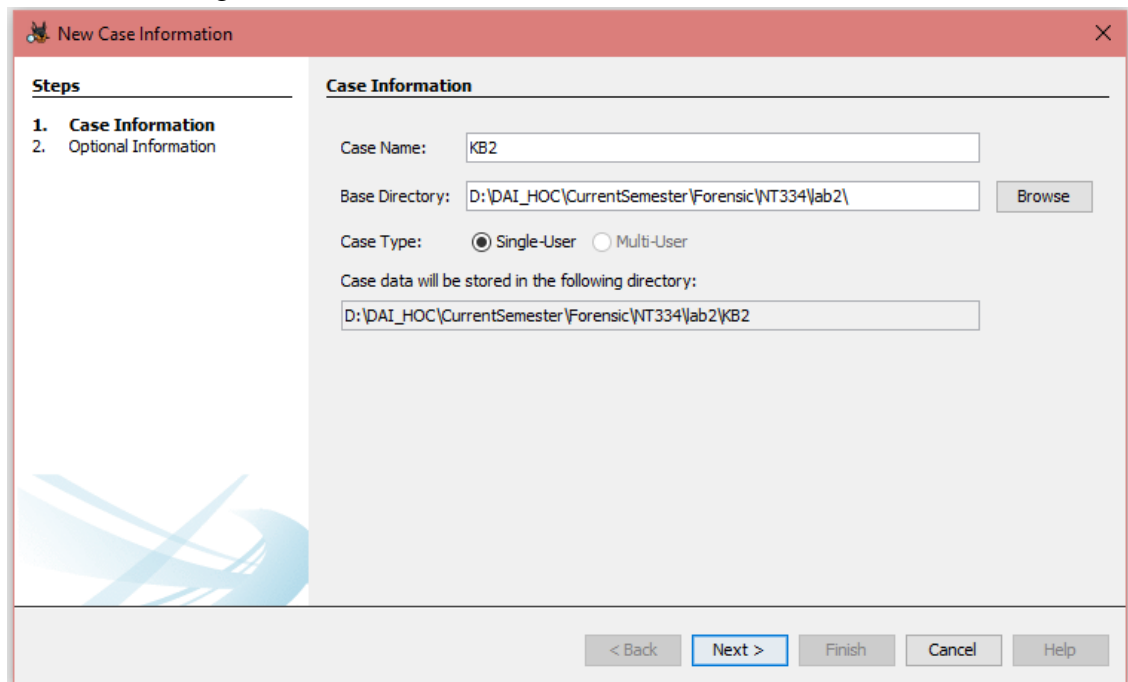
Tài nguyên: tải về theo link sau: <https://goo.gl/MRLtj4>

- 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 ...

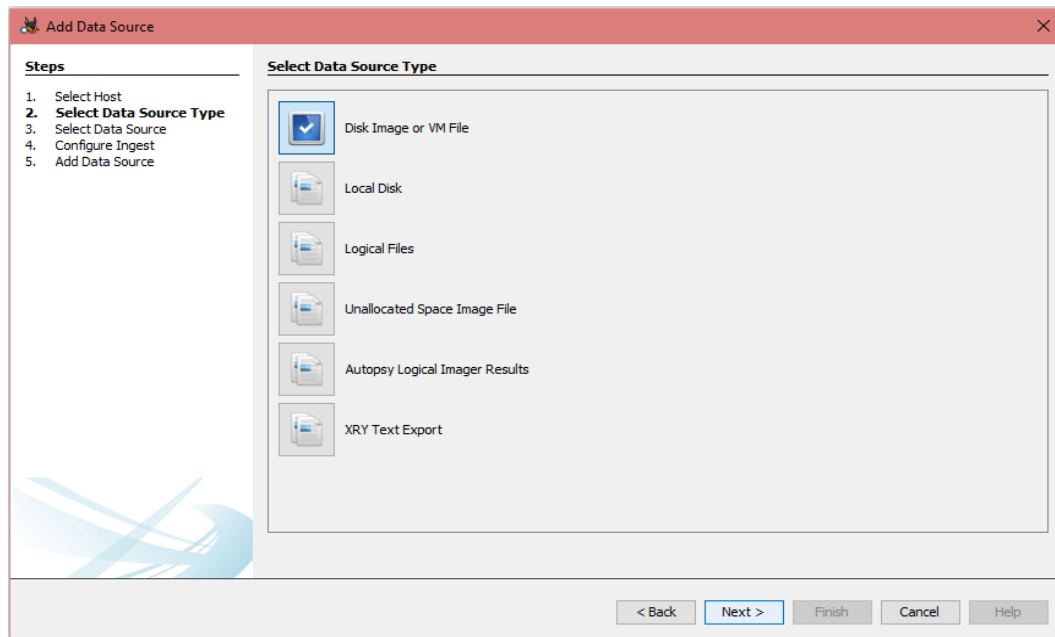
- Khởi động Autopsy và tạo một Case mới bằng option “Create New Case”



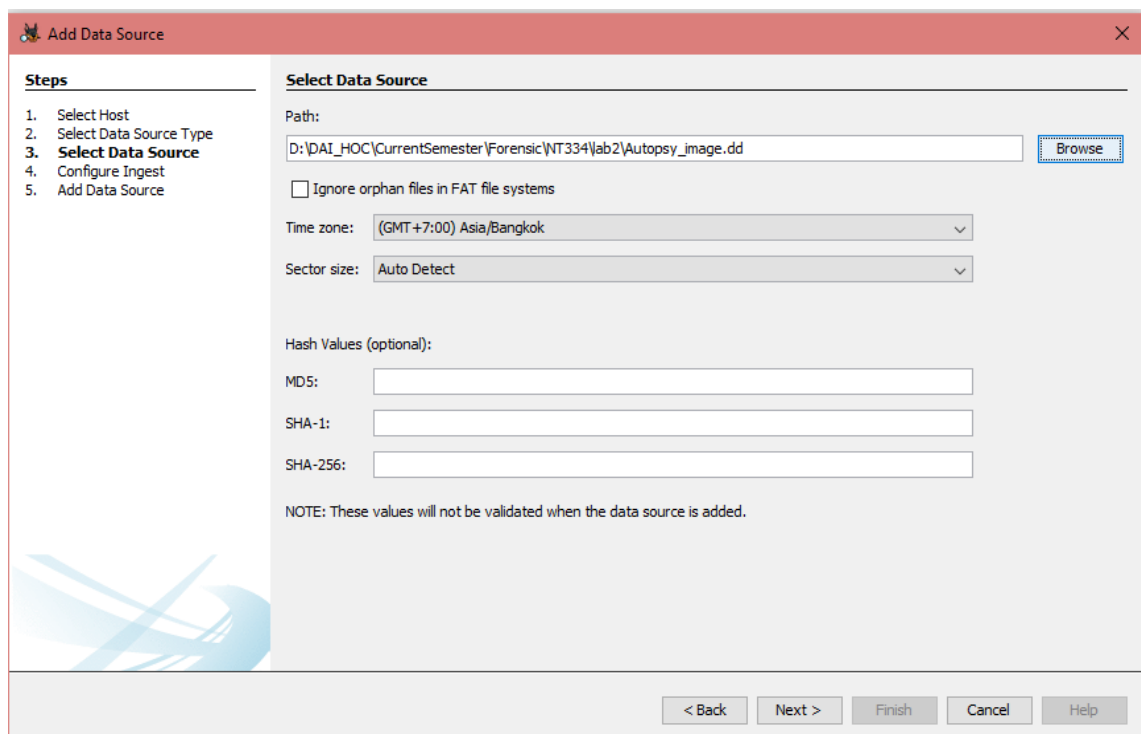
- Điền tên Case vào khung Case name



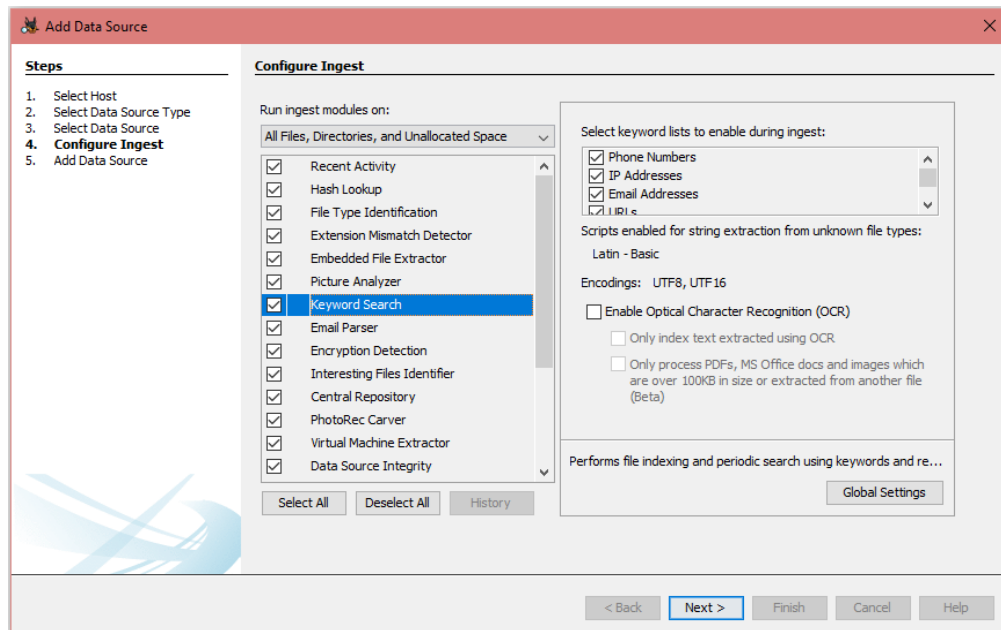
- Chọn *Disk Image or VM File* để phân tích file tài nguyên đã được cung cấp



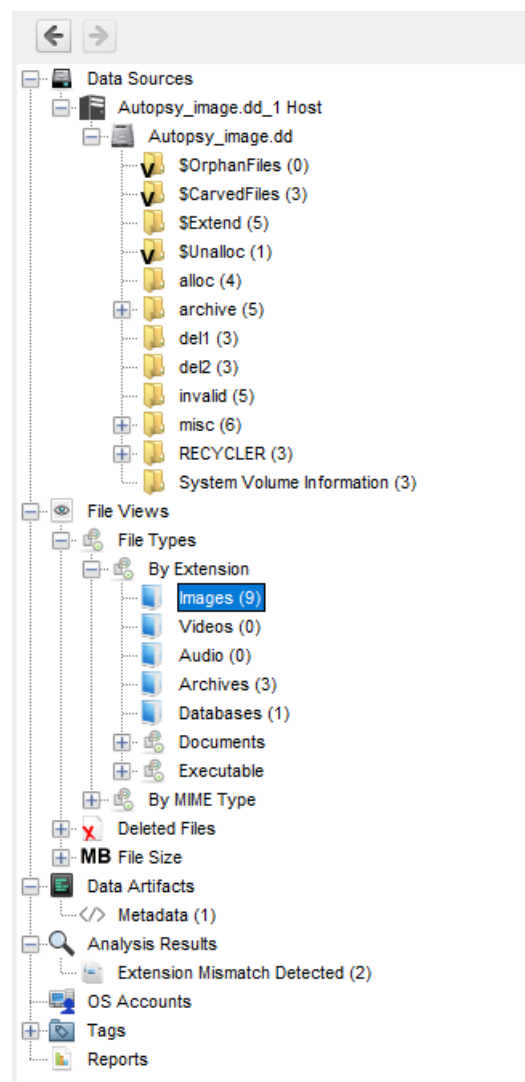
- Chọn File cần phân tích.



- Chọn ra các mô-đun để phân tích.



Sau khi tool chạy phân tích xong, để tìm được các hình ảnh có trong ổ đĩa đã cho, ta sẽ lọc theo Image vào: *File Views* → *File Types* → *By Extension* → *Image*



Phía bên tay phải sẽ hiển thị đầy đủ thông tin mỗi file hình ảnh tìm được: **tên file, loại file, size, thời gian tạo, xóa, sửa, MD5, kích thước hình ảnh ...**

Link video xem chi tiết các thông tin hình ảnh:

https://drive.google.com/file/d/1E8_VA7KGoBueN2a8JHPtsqe5Jq04g-Od/view?usp=sharing

Listing Images															
Table Thumbnail Summary															
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(U)	Known	Location	MD5 Hash	SHA-256 Hash	MIME Type
file4.jpg			1	2004-06-10 14:38:06 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:2...	2004-06-10 10:2...	189021	Allocated	Allocated	unknown	img_Autopsy_image.dd\invalid\file4.jpg	c8de721102617...	0da94b7a5d24...	application/octet-stream
file3.jpg			1	2004-06-10 14:27:02 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:2...	2004-06-10 10:2...	214228	Allocated	Allocated	unknown	img_Autopsy_image.dd\invalid\file3.jpg	1ba4e91591f05...	f1684e96895d...	text/plain
file1.jpg			1	2004-06-10 13:59:40 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:2...	2004-06-10 10:2...	274260	Allocated	Allocated	unknown	img_Autopsy_image.dd\alloc\file1.jpg	75b8d00568815...	2a082002a5d4...	image/jpeg
file10.jpg			1	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.dd\archive\file10.tar.gz\file10.1a...	c478a66ccdc27...	8115733ec0a6...	image/jpeg
file9.jpg			1	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.dd\archive\file9.boon\file9.jpg	c5a6917669c77...	522443d66dfd...	image/jpeg
file8.jpg			1	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.dd\archive\file8.zip\file8.jpg	f9956284a6915...	ca8c1910b7a7...	image/jpeg
r0000000.jpg			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	326859	Unallocated	Unallocated	unknown	img_Autopsy_image.dd\CarvedFiles\r0000000.jpg	0c452c5800fca...	e09242768c1f...	image/jpeg
r0000639.jpg			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	175630	Unallocated	Unallocated	unknown	img_Autopsy_image.dd\CarvedFiles\r0000639.jpg	afd55222024a4...	00ec3fab68b...	image/jpeg
image_0.jpg			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	110373	Allocated	Allocated	unknown	img_Autopsy_image.dd\misc\file12.doc\image_0.jpg	936d202bedec...	3a3f2e5011eef...	image/jpeg

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.

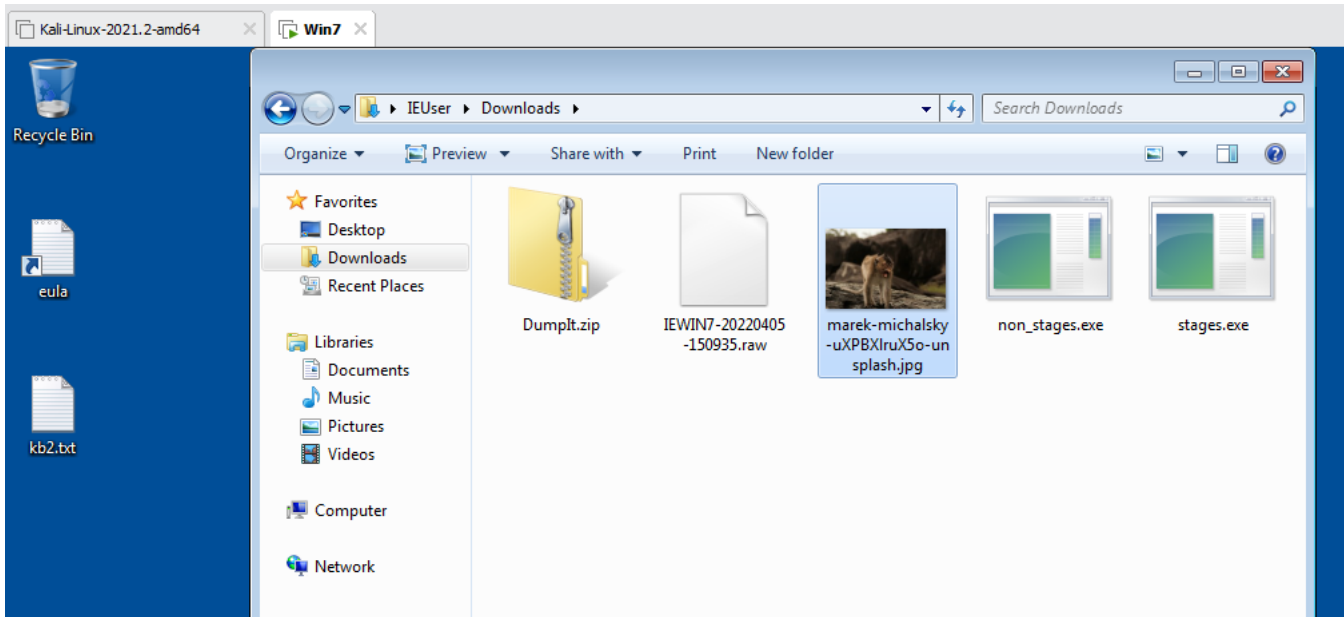
- Case Number: April_0001
- Evidence Number: 01
- Unique Description: Monkey Image
- Examiner: Your Name (tên của nhóm)

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

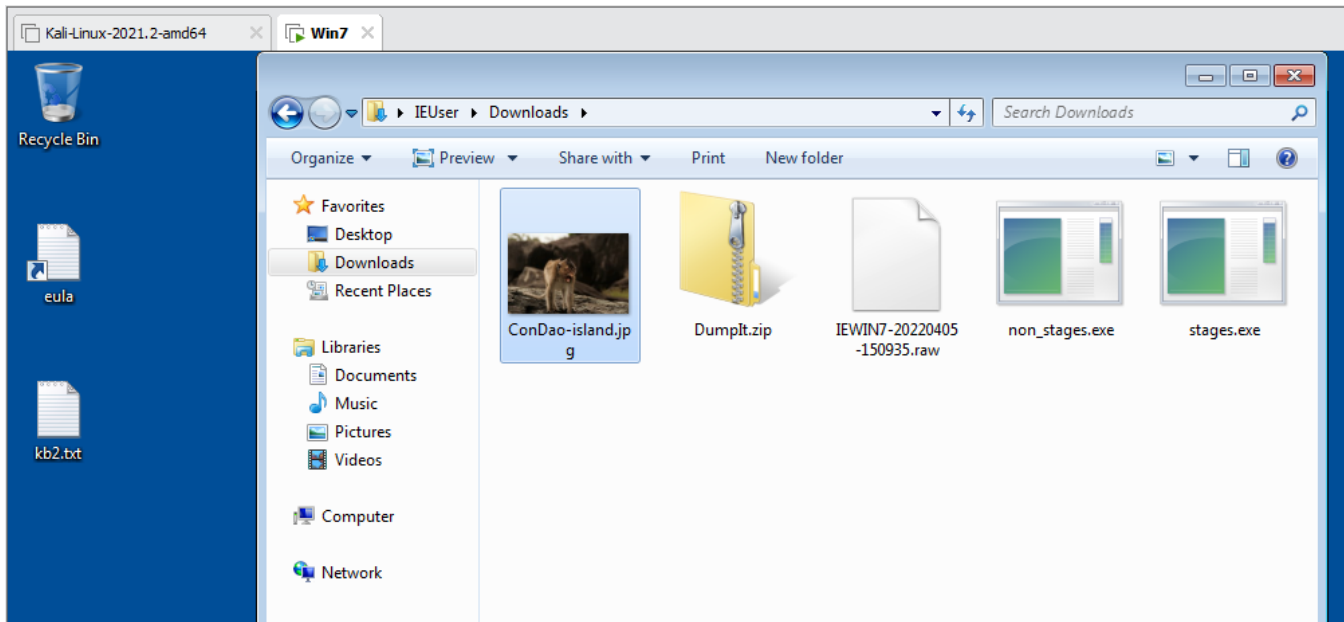
- Thực hiện điều tra, tìm ảnh đã bị xóa trên ổ đĩa bằng công cụ FTK Imager. Sử dụng tính năng phục hồi file ảnh đã bị xóa (tính năng Export Files), lưu trữ file này trong thư mục KB03\images.

- Kiểm tra giá trị hash MD5 của file ảnh vừa được phục hồi với file gốc ban đầu.

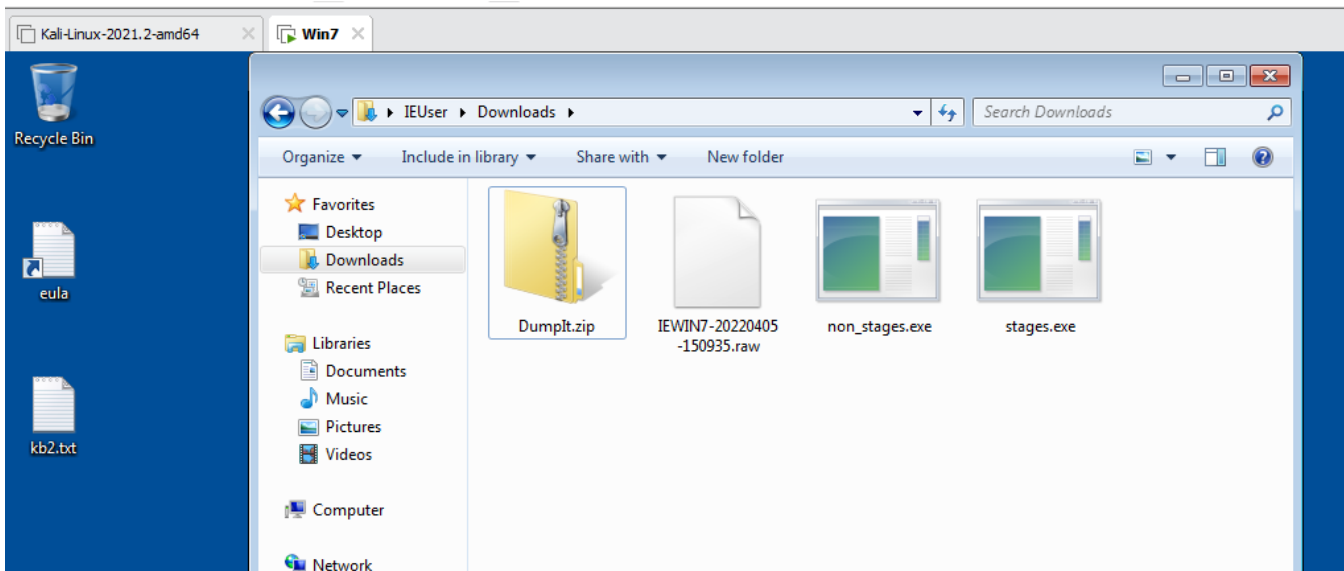
- Trên máy tính/máy ảo windows thực hiện tải về hình ảnh:



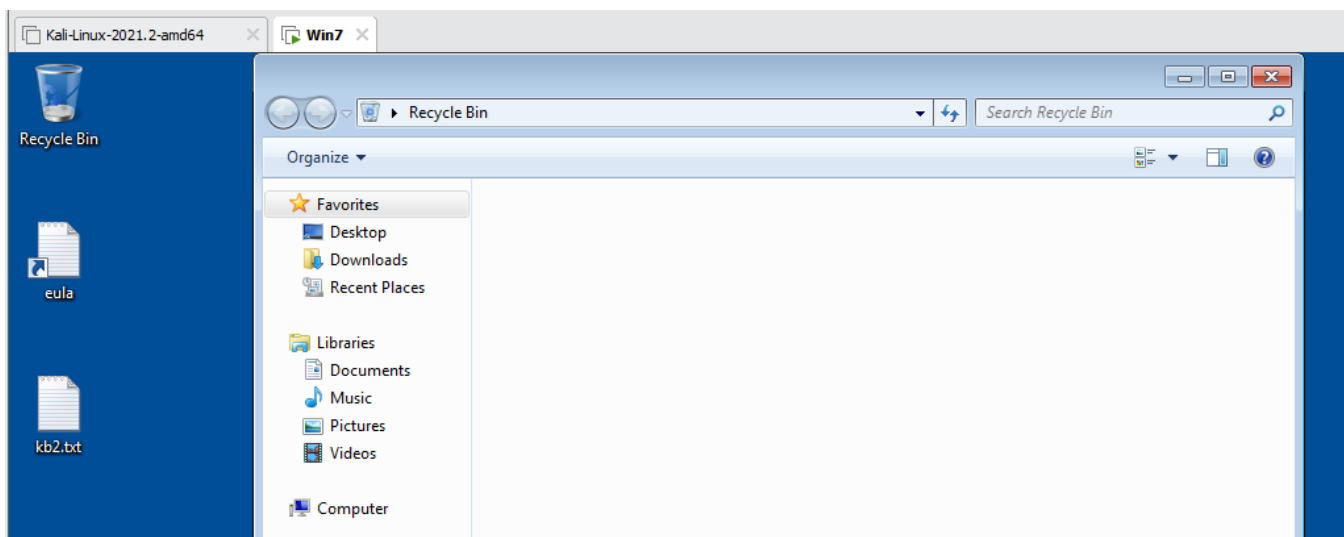
- Đặt tên ConDao-island:



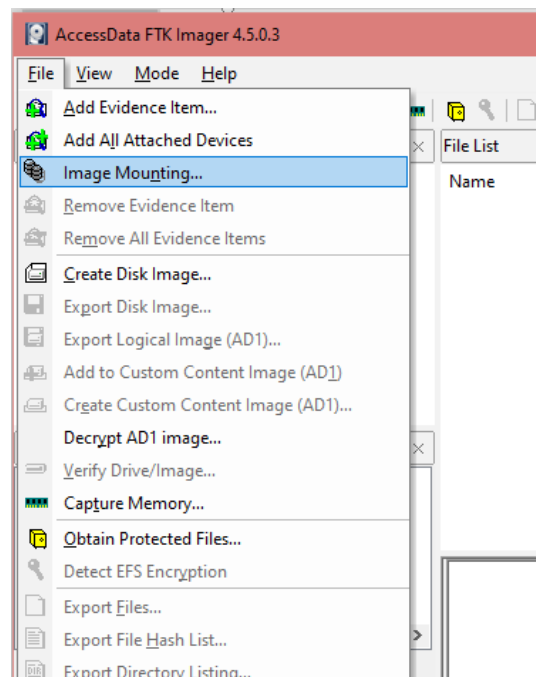
- Thực hiện xóa file ảnh vừa tạo:



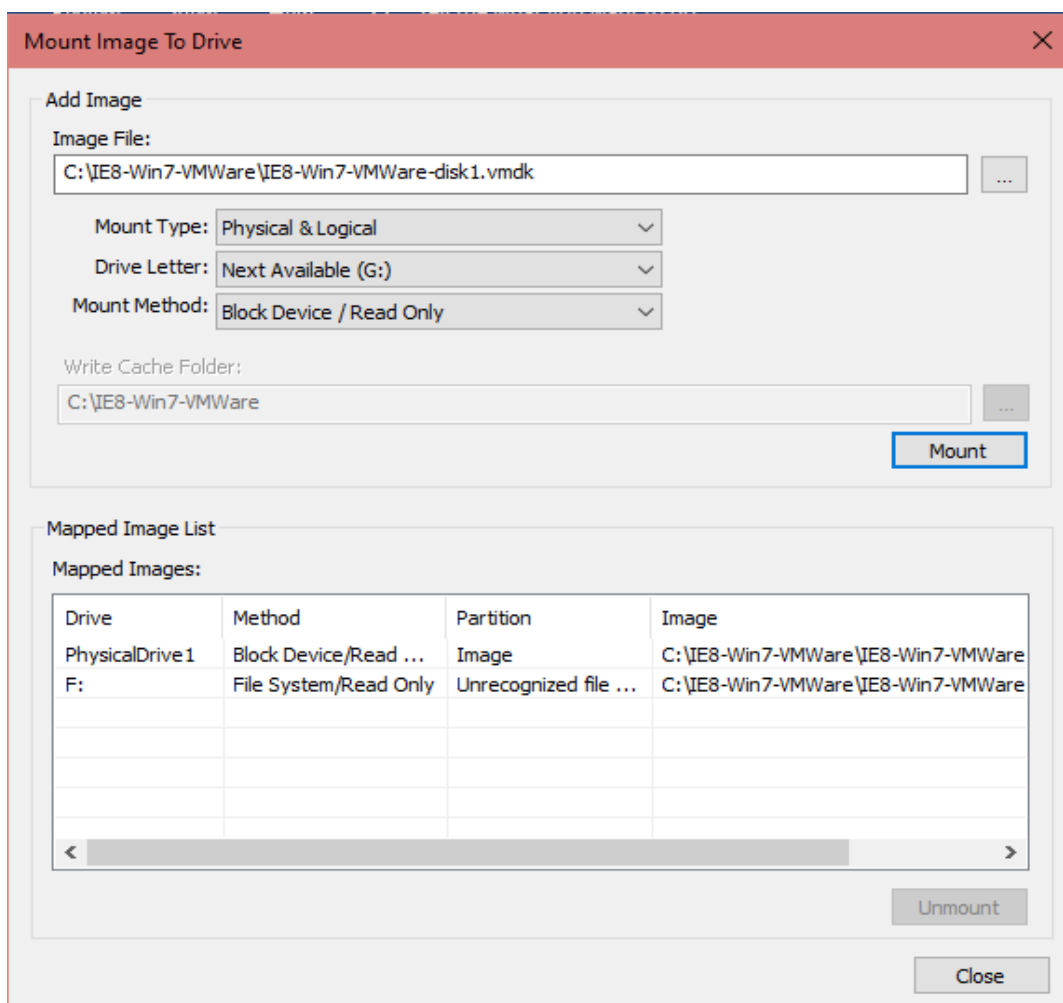
- Xóa trong Recycle Bin:



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



- Chọn ảnh đĩa (disk image) mục đích cần phân tích, ở đây là Win7, sau đó chọn Mount để gắn ổ đĩa:



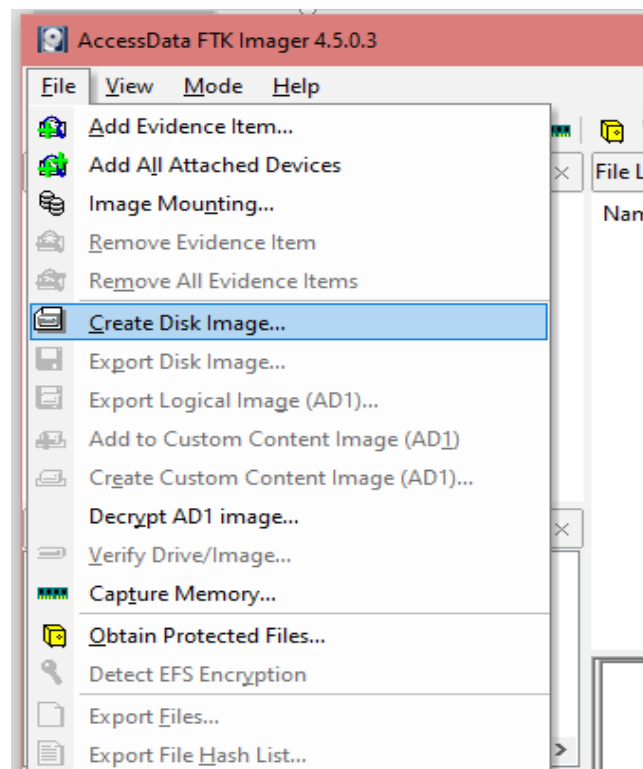
▼ Folders (7)



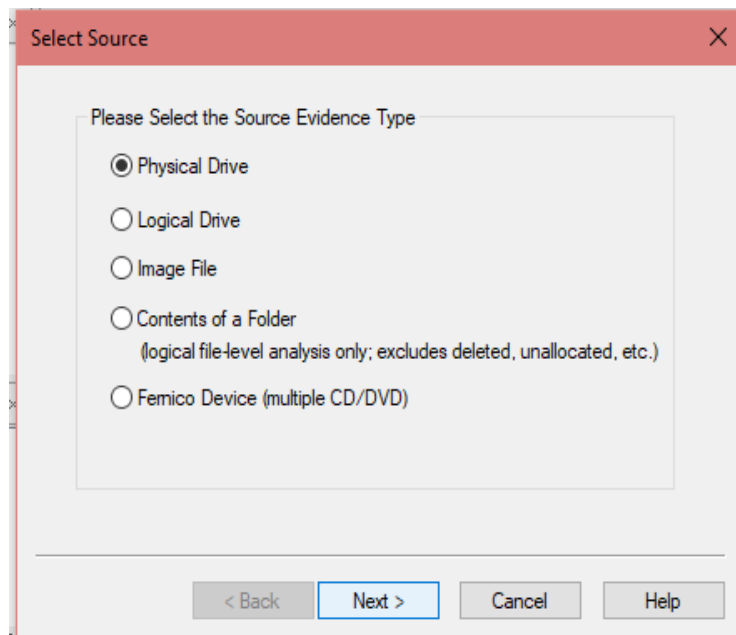
▼ Devices and drives (4)



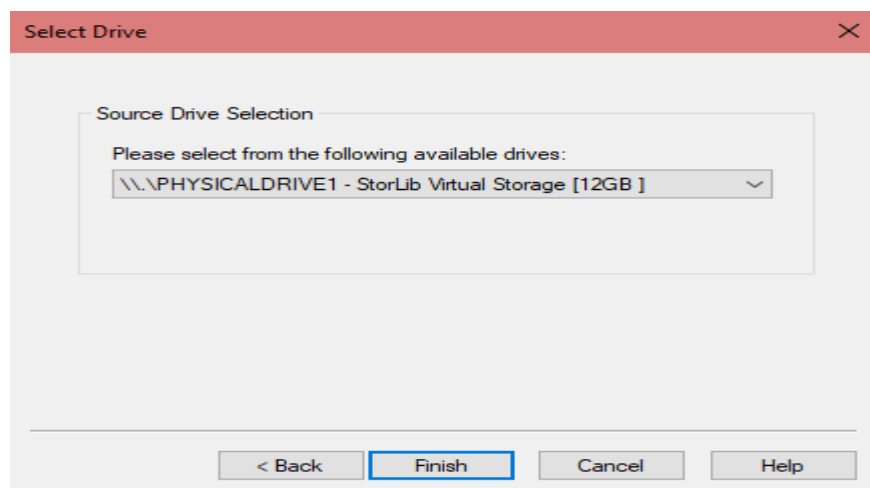
- Tạo một ảnh đĩa -định dạng Raw (dd). Chọn File => Create Disk Image



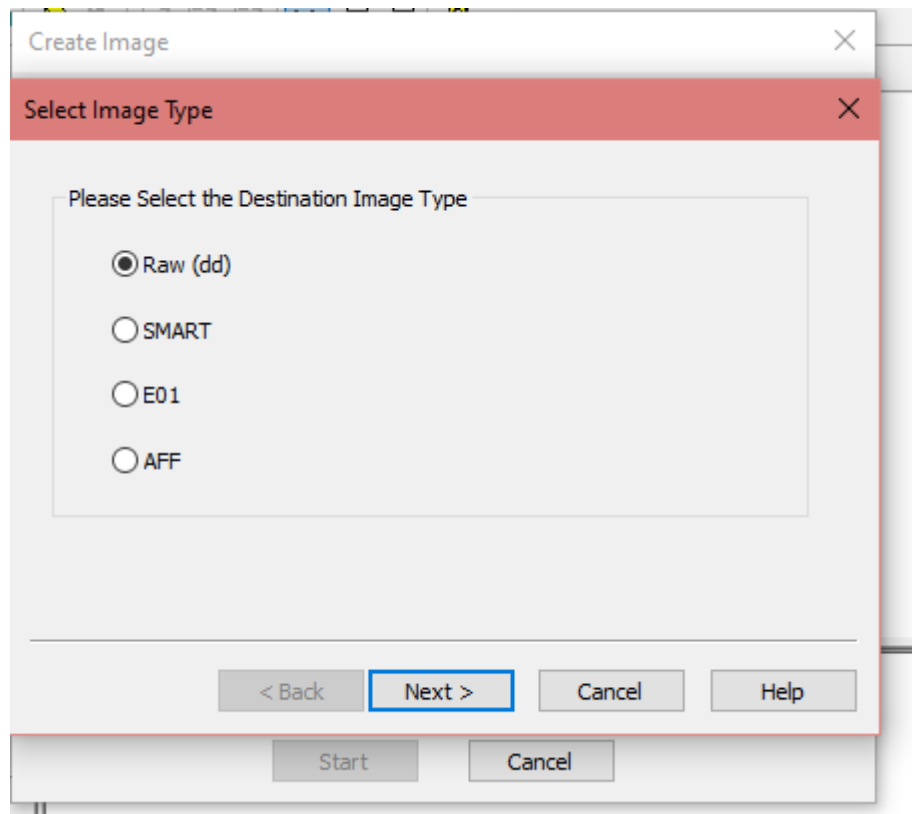
- Chọn loại ổ đĩa bằng chứng muốn tạo ra:



- Chọn Drive chứa win 7 vừa mount:

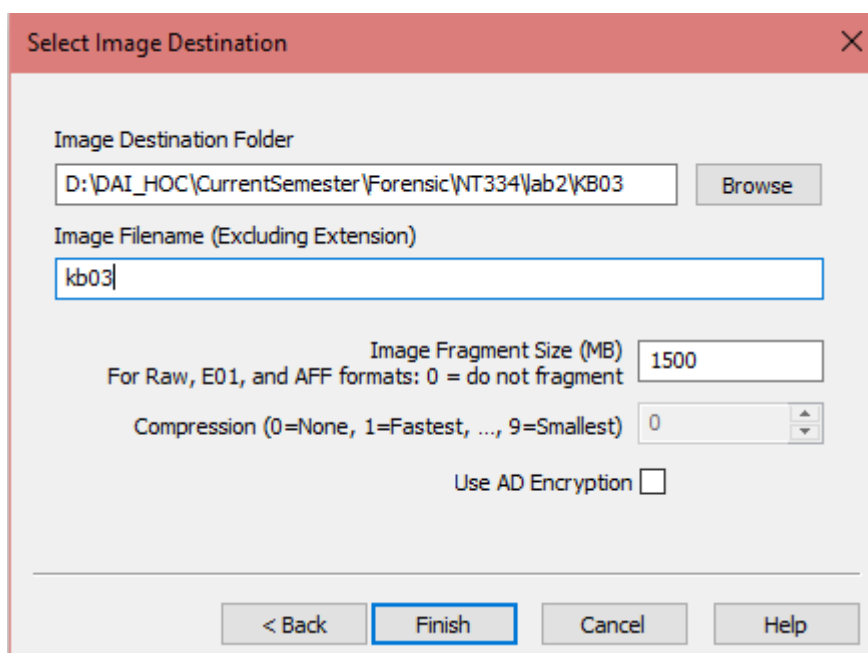


- Chọn loại ảnh đĩa là raw

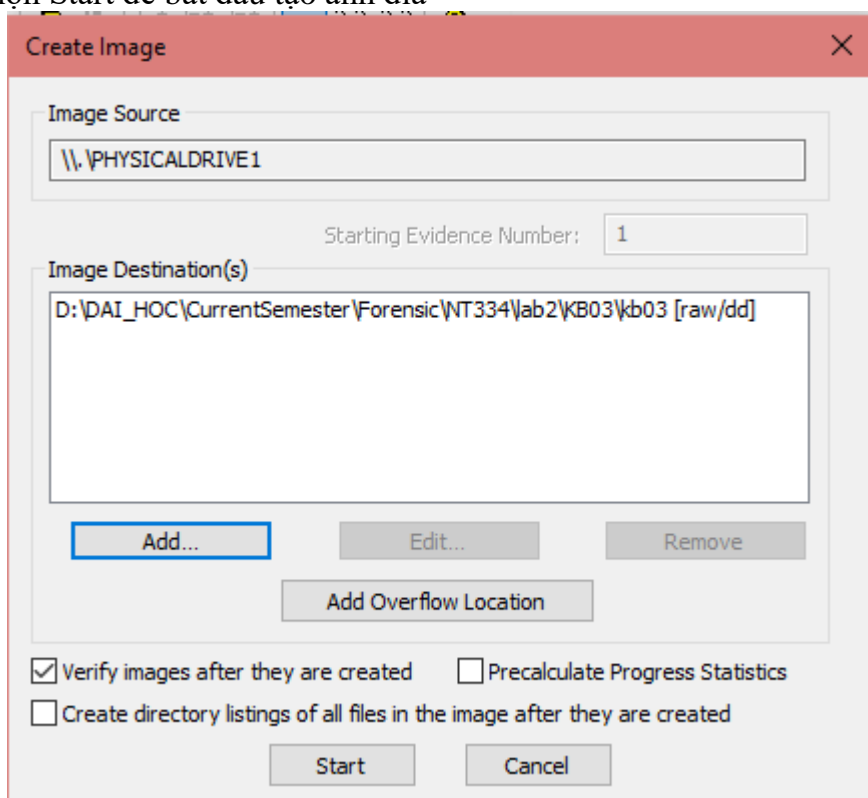


- Thực hiện điền thông tin của bằng chứng

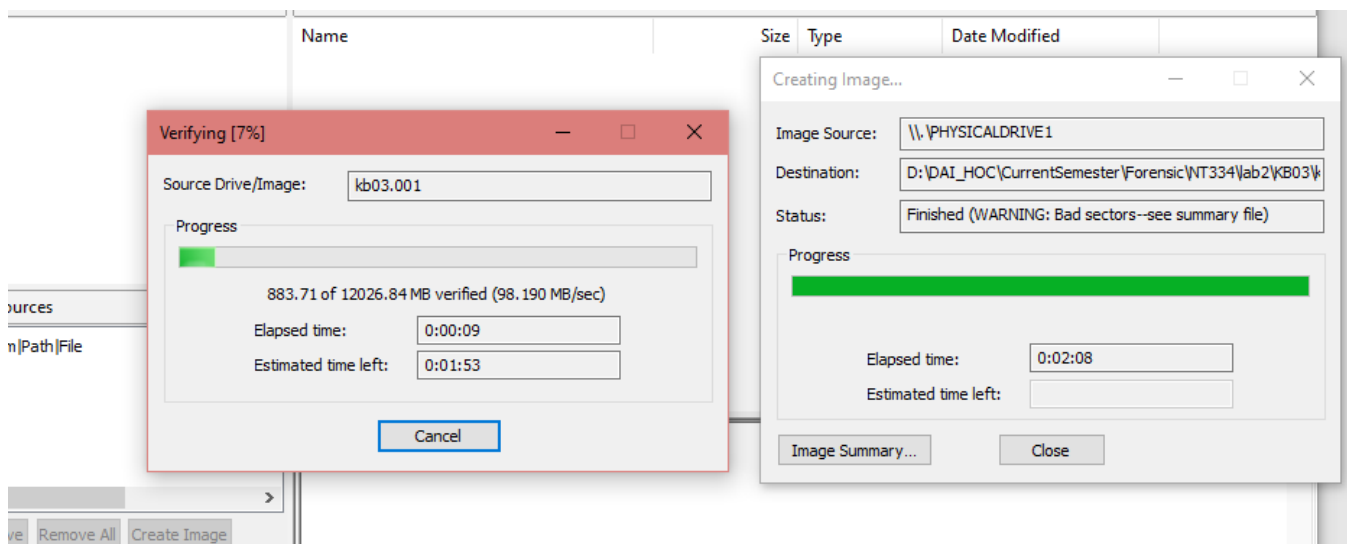
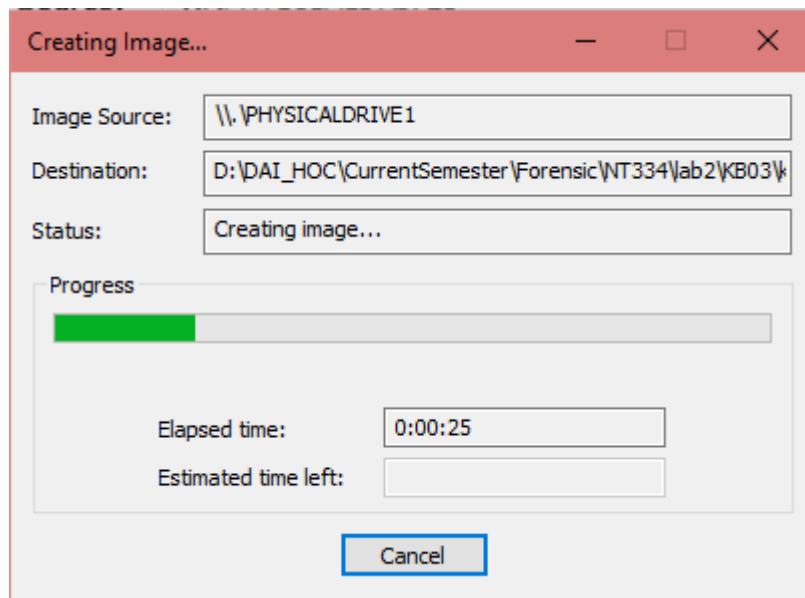
- Chọn nơi để lưu file ảnh đĩa.



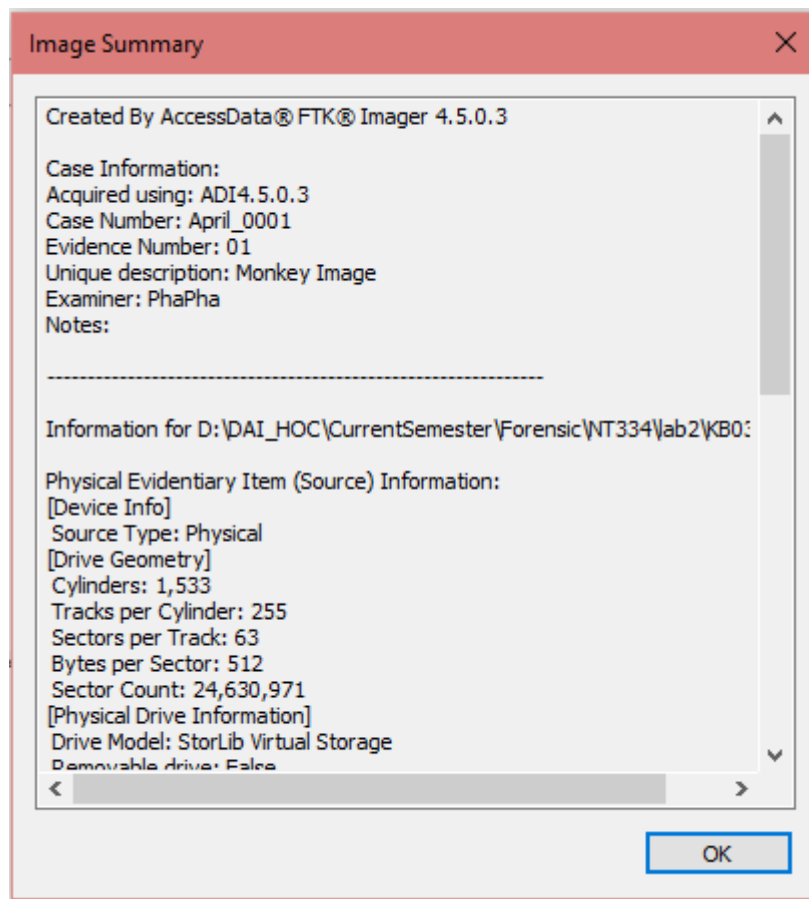
- Sau đó chọn Start để bắt đầu tạo ảnh đĩa



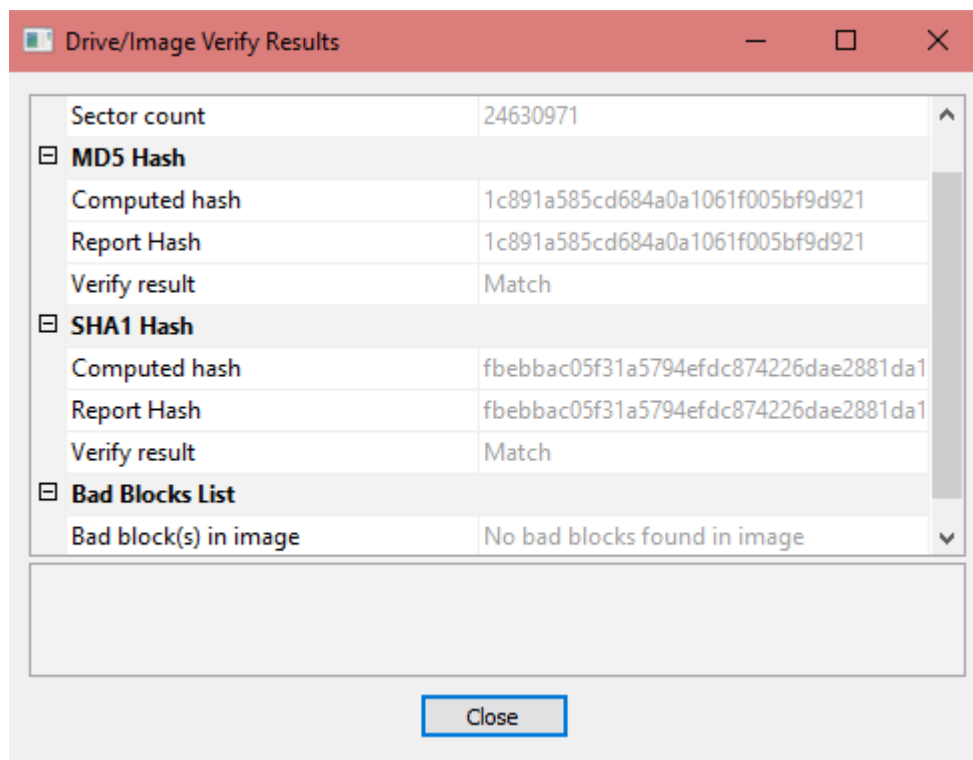
- Kiểm tra quá trình tạo:

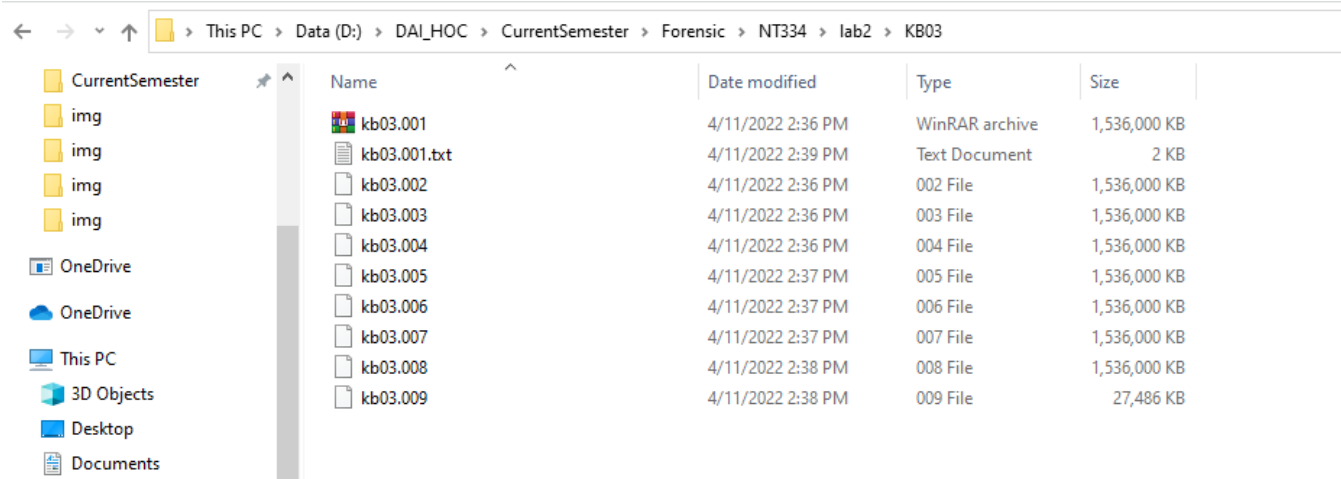


- Bảng tóm tắt của ảnh đĩa vừa được tạo xong như sau:

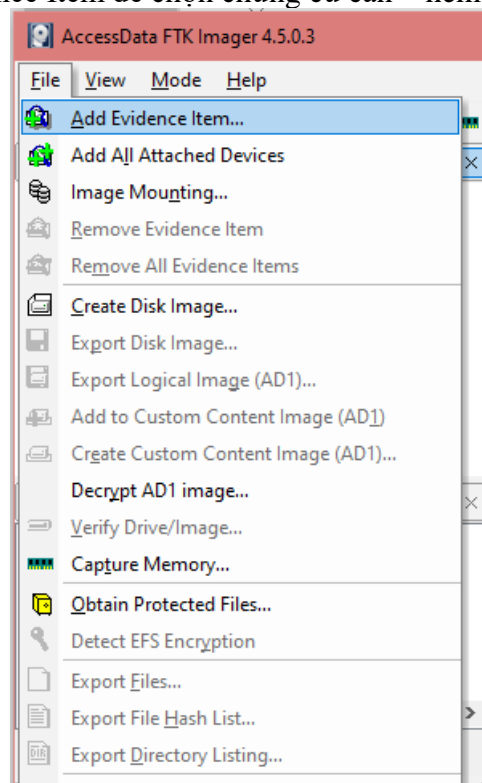


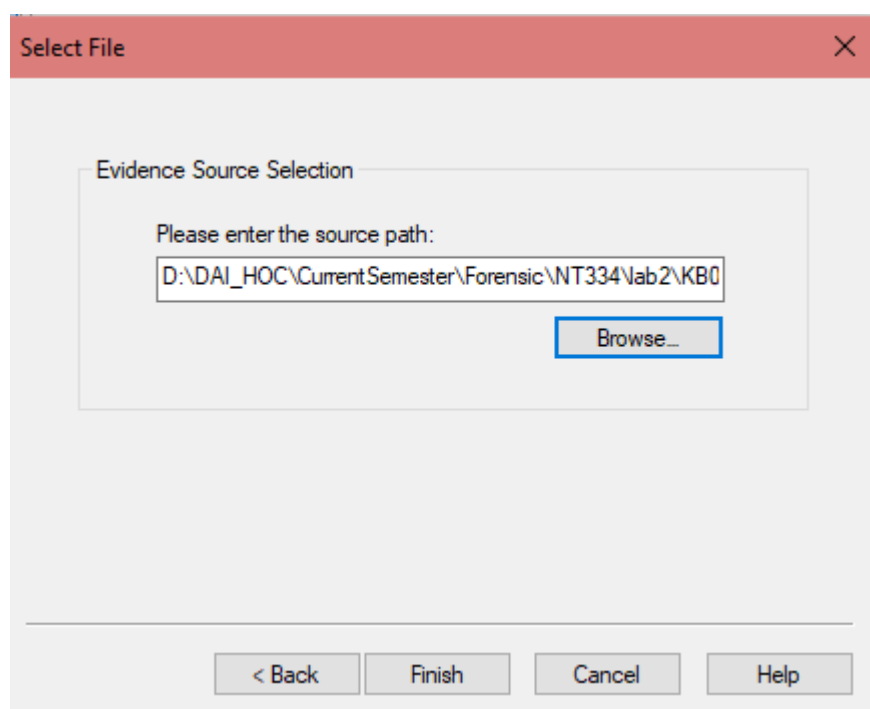
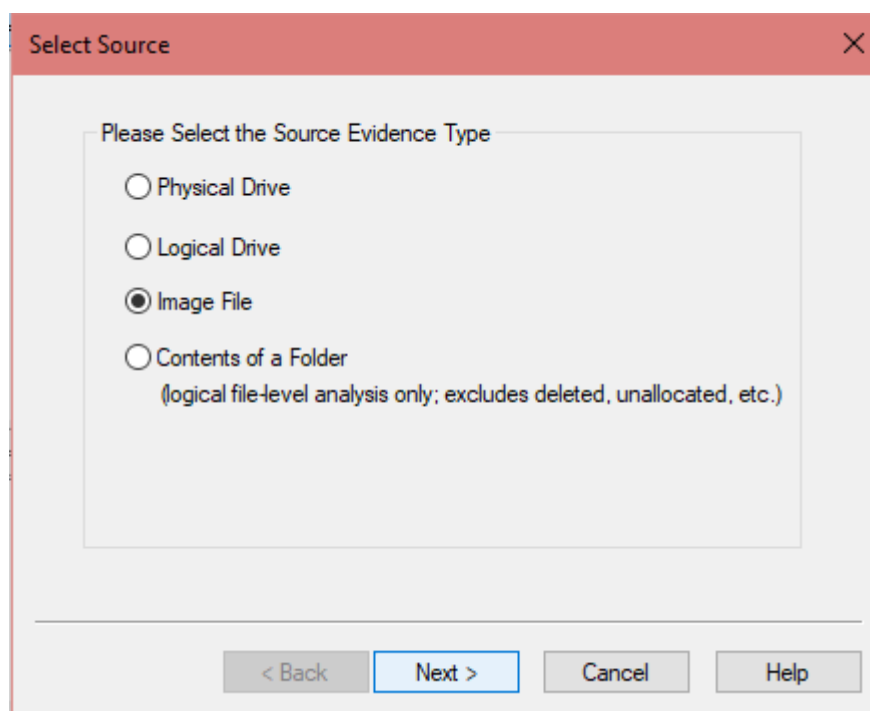
- Kết quả, thông tin của ảnh đĩa sau khi tạo như sau



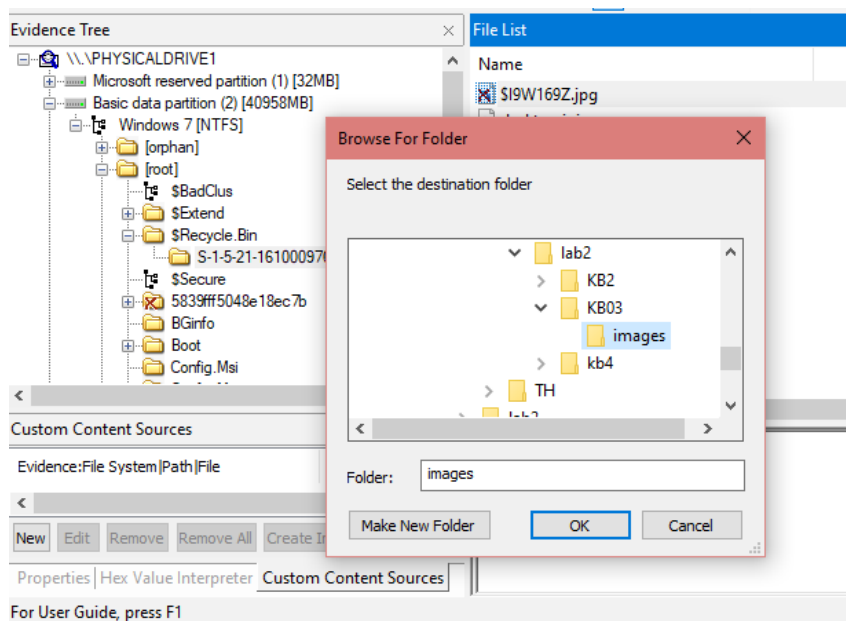


- Chọn File => Add Evidence Item để chọn chứng cứ cần thêm.





- 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.



Export Results



0 folder(s) and 1 file(s) exported successfully.
492865 bytes copied.

OK

- Kiểm tra giá trị hash MD5 của file ảnh vừa được phục hồi với file gốc ban đầu.

MD5 File Checksum

MD5 online hash file checksum function

ConDao-island.jpg

Hash ☒ Auto Update

b702d6f5ab256c910773324799e817b6

MD5 File Checksum

MD5 online hash file checksum function

\$I9W169Z.jpg

Hash

☒ Auto Update

b702d6f5ab256c910773324799e817b6

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

- Đầu tiên thực hiện extract:

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ gunzip kb04-session02.bin.gz

(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ ls
kb04-session02.bin
```

- Tiếp theo dùng lệnh file để xác định raw disk image:

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ file kb04-session02.bin
kb04-session02.bin: DOS/MBR boot sector; partition 1 : ID=0x7, start-CHS (0x1,0,1),
1), startsector 31, 31558 sectors, extended partition table (last)
```

- Fdisk hiển thị một phân vùng hợp lệ:

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ 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
```

- Dùng lệnh mmls - hiển thị bố cục phân vùng của một hệ thống ổ đĩa (bảng phân vùng)

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ mmls kb04-session02.bin
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Device:


|      | 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         |


```

- Theo các giá trị có được bởi mmls , chúng ta có thể trích xuất các phân vùng bằng dd

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ dd if=kb04-session02.bin of=kb04-session02_p0.bin bs=512 skip=0 count=1
1+0 records in
1+0 records out
512 bytes copied, 0.00126142 s, 406 kB/s
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ dd if=kb04-session02.bin of=kb04-session02_p1.bin bs=512 skip=0 count=31
31+0 records in
31+0 records out
15872 bytes (16 kB, 16 KiB) copied, 0.00109985 s, 14.4 MB/s
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ dd if=kb04-session02.bin of=kb04-session02_p2.bin bs=512 skip=31 count=31558
31558+0 records in
31558+0 records out
16157696 bytes (16 MB, 15 MiB) copied, 0.556059 s, 29.1 MB/s
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ dd if=kb04-session02.bin of=kb04-session02_p3.bin bs=512 skip=31589 count=27
27+0 records in
27+0 records out
13824 bytes (14 kB, 14 KiB) copied, 0.00164331 s, 8.4 MB/s
```


- Chạy lệnh strings trên phân vùng 3 chưa được phân bổ:

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ strings kb04-session02_p3.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
```

- Xem dạng hex dump:

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ hexdump -C kb04-session02_p3.bin
```

- Rõ ràng là ở đây không có key!

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ hexdump -C kb04-session02_p3.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 2d  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  .sometimesitreal
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 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 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 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 00  .e.r.e.....
```


- Theo hint đề bài dùng lệnh foremost khôi phục tệp đã xóa:

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ foremost kb04-session02.bin
Processing: kb04-session02.bin
[*]
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ ls -l
total 31628
-rwxrw-rw- 1 QuynhQuynh QuynhQuynh 16187392 Apr 11 05:34 kb04-session02.bin
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 512 Apr 11 05:51 kb04-session02_p0.bin
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 15872 Apr 11 05:52 kb04-session02_p1.bin
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 16157696 Apr 11 05:52 kb04-session02_p2.bin
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 13824 Apr 11 05:53 kb04-session02_p3.bin
drwxr-xr-- 4 QuynhQuynh QuynhQuynh 4096 Apr 11 06:03 output
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02]
$ cd output/
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02/output]
$ ls -l
total 12
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 1049 Apr 11 06:03 audit.txt
drwxr-xr-- 2 QuynhQuynh QuynhQuynh 4096 Apr 11 06:03 jpg
drwxr-xr-- 2 QuynhQuynh QuynhQuynh 4096 Apr 11 06:03 png
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02/output]
$ cd jpg/
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02/output/jpg]
$ ls
```

```
00000343.jpg 00000367.jpg 00000375.jpg 00001063.jpg 00001095.jpg 00001175.jpg 00001247.jpg
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02/output/jpg]
$ ls -l
```

```
total 120
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 11762 Apr 11 06:03 00000343.jpg
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 4096 Apr 11 06:03 00000367.jpg
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 1929 Apr 11 06:03 00000375.jpg
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 13862 Apr 11 06:03 00001063.jpg
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 36947 Apr 11 06:03 00001095.jpg
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 33383 Apr 11 06:03 00001175.jpg
-rw-r--r-- 1 QuynhQuynh QuynhQuynh 4378 Apr 11 06:03 00001247.jpg
```

- Dùng lệnh jhead phân tích và xem thông tin các file jpg:

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02/output/jpg]
$ jhead 00001095.jpg
File name      : 00001095.jpg
File size      : 36947 bytes
File date      : 2022:04:11 06:03:27
Resolution     : 500 x 625
JPEG Quality   : 80
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02/output/jpg]
$ jhead 00001175.jpg
File name      : 00001175.jpg
File size      : 33383 bytes
File date      : 2022:04:11 06:03:27
Resolution     : 480 x 341
JPEG Quality    : 78
```

```
(QuynhQuynh@kali)-[~/CurrentSemester/forensic/lab02/output/jpg]
$ jhead 00001247.jpg
File name      : 00001247.jpg
File size      : 4378 bytes
File date      : 2022:04:11 06:03:27
Resolution     : 116 x 102
GPS Latitude   : N 36d  8m  8.5s
GPS Longitude  : E 115d  9m 29s
JPEG Quality   : 65
Comment        : Who is the author?
===== IPTC data: =====
Credit         : libdisassemble
```

- Tuy nhiên không phát hiện gì hữu ích!
- Tiến hành phân tích với Autopsy :

Add Data Source

Steps

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

Select Data Source

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

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

- Phát hiện file key đã bị xóa:

Table Thumbnail Summary						
Name	S	C	O	Modified Time	Change Time	Access Time
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
furries.jpg				2010-05-19 07:32:45 ICT	2010-05-19 07:32:45 ICT	2010-05-19 06:38:20 ICT
furries.jpg:Zone.Identifier				2010-05-19 07:32:45 ICT	2010-05-19 07:32:45 ICT	2010-05-19 06:38:20 ICT
images.jpg				2010-05-19 07:33:08 ICT	2010-05-19 07:33:08 ICT	2010-05-19 07:21:00 ICT
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
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
whiteflag.jpg				2010-05-19 07:32:41 ICT	2010-05-19 07:32:41 ICT	2010-05-19 06:51:26 ICT
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

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 1 of 1 Result < >									
Type	Value								
Associated Artifact	-9223372036854775793								
Source File Path	/img_f100_6db079ca91c4860f.bin/vol_vol2/key								
Artifact ID	-9223372036854775792								

- Tuy nhiên, NTFS có một thành phần thú vị: Master File Table (MFT), được hiển thị trong hệ thống tệp NTFS dưới dạng \$ MFT . Tiến hành xem xét nó vì nó có thể vẫn chứa các phần của tệp đã xóa.

Timeline

Discovery

Generate Report

Close Case

16

Keyword Lists

Listing

img_f100_6db079ca91c4860f.bin/vol_vol2

TableThumbnailSummary

Name	S	C	O	Modified Time	Change Time	Access Time
\$Boot				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$LogFile				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$MFT				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$MFTMirr				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$Secure:\$SDS				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$UpCase				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$Volume				2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
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
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

<

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Page: 1 of 16

Page

Go to Page: 1

Jump to Offset

Launch in HxD

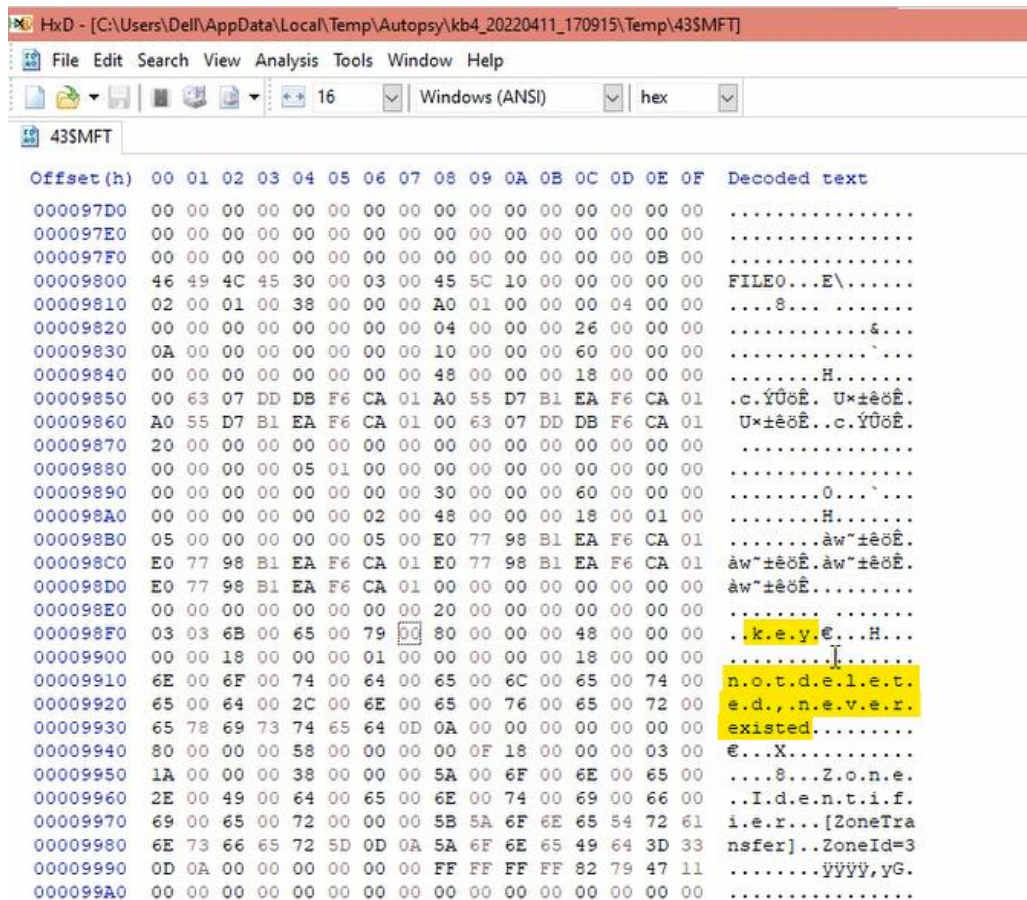
0x00000330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x00000340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x00000350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x00000360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- Sử dụng chức năng Launch in HxD, sau đó thực hiện tìm kiếm với từ khóa “key”. Và ta đã đọc tìm được nội dung của file key: “notdeleted, neverexisted”



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

Nhận được file **kb05-session02**. Check thì thấy nó là file **Zip**

```
(virus@kali)-[~/Desktop]
$ file kb05-session02
kb05-session02: Zip archive data, at least v2.0 to extract
```

Ban đầu tưởng bị troll nhưng mà file **kịch bản 06** nó là file PDF nên nó là ý người ra đề. Đổi đuôi file thành **.zip** cho hợp lý rồi giải nén.

```
(virus@kali)-[~/Desktop]
$ mv kb05-session02 kb05-session02.zip

(virus@kali)-[~/Desktop]
$ unzip kb05-session02.zip
Archive: kb05-session02.zip
  inflating: 56DACF1C6CF363F27501FFCA50CC0415.raw
```

Bây giờ ta đã có file **.raw**. Đưa file sang máy window và bỏ vào **AutoSpy** để testing. Dump hết bộ nhớ ra và search thử từ “kill” xem ông này có ý định tự sát không, search với tùy chọn **Substring**, không cần phải đúng chính xác từ, mà nó sẽ extract cái đoạn nào có chứa chuỗi “kill” thôi

Lược hết kết quả một hồi (24 result, cũng không nhiều). Thì có một file chứa thông tin khá thú vị:

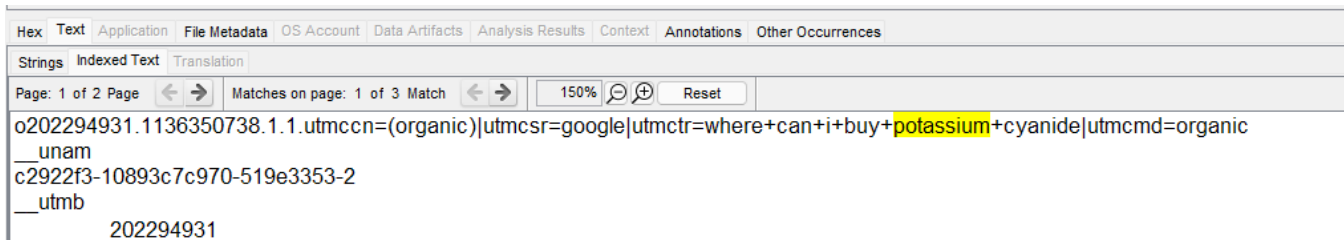
Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
0321240693[1]	words to learn new «skills» many people express	Img_56DACF1C6CF363F27501FFCA50CC0415.raw__TFA...	2006-01-04 18:30:30 ICT	0000-00-00 00:00:00	2006-01-04 00:00:00 ICT	2006-01-04 18:30:30 ICT	38110	Allocated	Allocated
sb[1].htm	the best technical «skills» for the best value.	Img_56DACF1C6CF363F27501FFCA50CC0415.raw__TFA...	2006-01-04 18:17:42 ICT	0000-00-00 00:00:00	2006-01-04 00:00:00 ICT	2006-01-04 18:17:42 ICT	12037	Allocated	Allocated
opr0028Y.js	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
OPR0028Y.JS	re, used mostly to «kill» successive calls to	Img_56DACF1C6CF363F27501FFCA50CC0415.raw\9Orph...	2006-01-06 12:09:18 ICT	0000-00-00 00:00:00	2006-01-06 00:00:00 ICT	2006-01-06 12:09:18 ICT	6152	Unallocated	Unallocated
opr001XG.png	«health»meds/kw=show_test_can_potassium_cyanide_ki...	Img_56DACF1C6CF363F27501FFCA50CC0415.raw__TFA...	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:32:06 ICT	113589	Unallocated	Unallocated
opr0020O.htm	three submissions: «skill» level: intermediate	Img_56DACF1C6CF363F27501FFCA50CC0415.raw__TFA...	2006-01-05 19:37:24 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:37:24 ICT	34757	Unallocated	Unallocated
CtrlLog.txt	dm_stop_replication «kill»e rapi timer2006-01-	Img_56DACF1C6CF363F27501FFCA50CC0415.raw__TFA...	2006-01-06 15:57:24 ICT	0000-00-00 00:00:00	2005-01-31 00:00:00 ICT	2005-01-31 12:00:36 ICT	37138	Allocated	Allocated

Nội dung file chứa từ khóa tìm kiếm cách để “ngủm” sớm:

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings Indexed Text Translation									
Page: 1 of 2 Page Matches on page: 1 of 1 Match 150% Reset									
http://ad.doubleclick.net/ad/wiki.health/meds/kw=How_fast_can_potassium_cyanide_kill_you;csrc=unanswered;pos=1;answ=ad;tile=1;dcopt=ist;sz=160x600;ord=69846684?									
text/html									
Tue, 09 Mar 2010 06:09:13 GMT									
text/html									
gzip									
opr001BT.htm									
Phttp://w.sharethiOPR001KHPNG									
\$4\$4									
Aopr00									
1K1.pn									
OPR001KIPNG									
\$4\$4									
Aopr00									
71KJ.pn									
OPR001KJPNG									
\$4\$4									
Aopr00									
1KK.pn									

Ông này search từ khóa **kw** với giá trị **How_fast_can_potassium_cyanide_kill_you** trên **doubleclick.net** Ai xem phim mấy phim trinh thám như Conan hay mấy bộ murder sẽ biết cyanide là chất độc giết người. Đến đây có thể kết luận là khả năng cao cách ông tự sát. Tìm thêm thử động cơ xem, search với **potassium**

Có một số thông tin như cách để mua potassium được chứa nhiều trong các **cookie**:



Ráng tìm **motivation** của ông này với các từ khóa như “love”, “study”, “robber”, “money”, ... Nhưng hoàn toàn không tìm ra manh mối nào. Tuy nhiên có thể kết luận đây là trường hợp tự sát. Xong !!!

Kịch bản 06. Thực hiện phân tích:

- Tài nguyên: kb06-session02.pdf

- Chúng tôi đảm nhiệm vai trò là đội ngũ điều tra viên pháp y trong vụ án tự tử của một thành 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 bà tăng 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 thân 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 mảnh mồi 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:

- 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 thấy file PDF chỉ có đúng nội dung như dưới:

Eden Sterling did not commit suicide. I have proof.

Vậy là file size tới **73.9MB**, có lẽ có file ẩn trong đây. Sử dụng **binwalk** để extract ra những file ẩn trong file **PDF** hiện tại:

```
(virus@kali)-[~/Desktop]
$ binwalk -e kb06-session02.pdf
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PDF document, version: "1.4"
147	0x93	Zlib compressed data, default compression
39724507	0x25E25DB	xz compressed data
39767781	0x25ECEE5	xz compressed data
39820771	0x25F9DE3	xz compressed data
39820951	0x25F9E97	xz compressed data
39899694	0x260D22E	xz compressed data
39935872	0x2615F80	xz compressed data
40009219	0x2627E03	xz compressed data
40013387	0x2628E4B	xz compressed data
40092191	0x263C21F	xz compressed data
40128120	0x2644E78	xz compressed data
40205040	0x2657AF0	xz compressed data
40209788	0x2658D7C	xz compressed data
40249502	0x266289E	xz compressed data
40329277	0x267603D	xz compressed data
40375259	0x26813DB	xz compressed data
40416593	0x268B551	xz compressed data
40503101	0x26A073D	xz compressed data
40518625	0x26A43E1	xz compressed data
40559387	0x26AE31B	xz compressed data

Ta thấy đa số các file giống nhau và đa số là file junk. Thấy có vài file **zlib** lạ lạ và một file **93** không rõ extension là gì

2B4B78D	30B29E1.xz	34EC12C	38AC24F.xz	3BD7BE7	3F33D80.xz	427D327	45FF58D.xz	49D3968
2B4B78D.xz	30BAD4A	34EC12C.xz	38B4451	3BD7BE7.xz	3F3C585	427D327.xz	460C87C	49D3968.xz
2B5015E	30BAD4A.xz	34F8D12	38B4451.xz	3BDBF87	3F3C585.xz	4283614	460C87C.xz	49D7BA1
2B5015E.xz	30BC40A	34F8D12.xz	38BA0B1	3BD8F87.xz	3F46C6F	4283614.xz	46163F5	49D7BA1.zlib
2B59D5F	30BC40A.xz	34FED0B	38BA0B1.xz	3BE8F62	3F46C6F.xz	428E181	46163F5.xz	49D7D7A
2B59D5F.xz	30C8694	34FED0B.xz	38C3CE0	3BE8F62.xz	3F4E6A1	428E181.xz	46165F9	49D7D7A.zlib
2B5E014	30C8694.xz	350C1A6	38C3CE0.xz	3BEB406	3F4E6A1.xz	429A725	46165F9.xz	49D7E06
2B5E014.xz	30D3D3B	350C1A6.xz	38CBE11	3BEB406.xz	3F5870A	429A725.xz	462391B	49D7E06.zlib
2B69914	30D3D3B.xz	350EB8E	38CBE11.xz	3BF31C4	3F5870A.xz	42A149E	462391B.xz	49DA0BD
2B69914.xz	30E1716	350EB8E.xz	38D53BE	3BF31C4.xz	3F6176F	42A149E.xz	46273B8	49DA0BD.zlib
2B77A43	30E1716.xz	3514CEB	38D53BE.xz	3BF94E5	3F6176F.xz	42ABA9C	46273B8.xz	93
2B77A43.xz	30E58DA	3514CEB.xz	38DCCFC	3BF94E5.xz	3F64A80	42ABA9C.xz	462F335	93.zlib
2B97865	30E58DA.xz	351EB09	38DCCFC.xz	3C00386	3F64A80.xz	42B5B8E	462F335.xz	
2B97865.xz	30EEBA0	351EB09.xz	38E7209	3C00386.xz	3F6E4A2	42B5B8E.xz	4639378	
2BB762D	30EEBA0.xz	352BF73	38E7209.xz	3C0CBE9	3F6E4A2.xz	42BEF17	4639378.xz	
2BB762D.xz	30EEF68	352BF73.xz	38F0717	3C0CBE9.xz	3F77DC0	42BEF17.xz	46469FB	
2BD73C3	30EEF68.xz	3534315	38F0717.xz	3C0EDC9	3F77DC0.xz	42C6060	46469FB.xz	

Thử extract file lạ nhất là 93 thì ta có file **Eden_Drive.dd**


```
(virus@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,2 CPUs 11th Gen Intel(R) Core(TM) i7-11800H
@ 2.30GHz (806D1),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

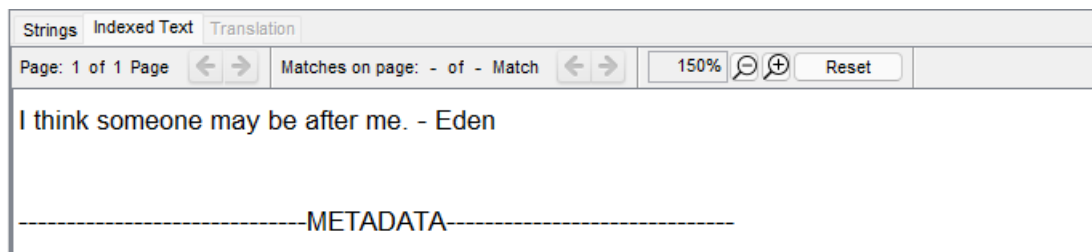
Size:      211812352
Compressed: 77422710
```

Ta có file **image** rồi. Giờ thì dump bộ nhớ với **AutoSpy**.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
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/vol4/secret.docx:secret.txt	93b0b2597238652bd76768645a
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/vol4/secret.docx	9580f981faa9e441562a555cd8e
10085384.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/vol2/CarvedFiles/10085384.docx	f97ea187d338cb30bc7a5b460b5
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_vrd2/Imy_stut1/8875837.doc	96b8569083644d8e0b7788818b

Ta thấy trong Document có một số file đáng ngờ:

secret.docx:secret.txt



Thanh niên này bị theo dõi chẳng, và kẻ này có thể ám sát Eden.