

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 3

Tên chủ đề: Hard Drive Forensics

GVHD: Lê Đức Thịnh

Ngày báo cáo: 17/4/2023

Nhóm: 7

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
2	Nguyễn Bình Thực Trâm	20520815	20520815@gm.uit.edu.vn
3	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Thực hiện	Thành viên thực hiện	Kết quả tự đánh giá
1	Kịch bản 01	Đã hoàn thành tại lớp	Trâm	100%
2	Kịch bản 02	Đã hoàn thành tại lớp	Ngân	100%
3	Kịch bản 03	Đã hoàn thành tại lớp	Kiệt	100%
4	Kịch bản 04	- Phân tích tài nguyên kb04-session02.bin.gz: hoàn thành - Tìm thông tin có liên quan đến từ khóa “key”: hoàn thành	Trâm	100%
5	Kịch bản 05	- Phân tích tài nguyên: kb05-session02: hoàn thành - Xác định tình nghi một người đàn ông chết do tự tử: hoàn thành	Kiệt	100%

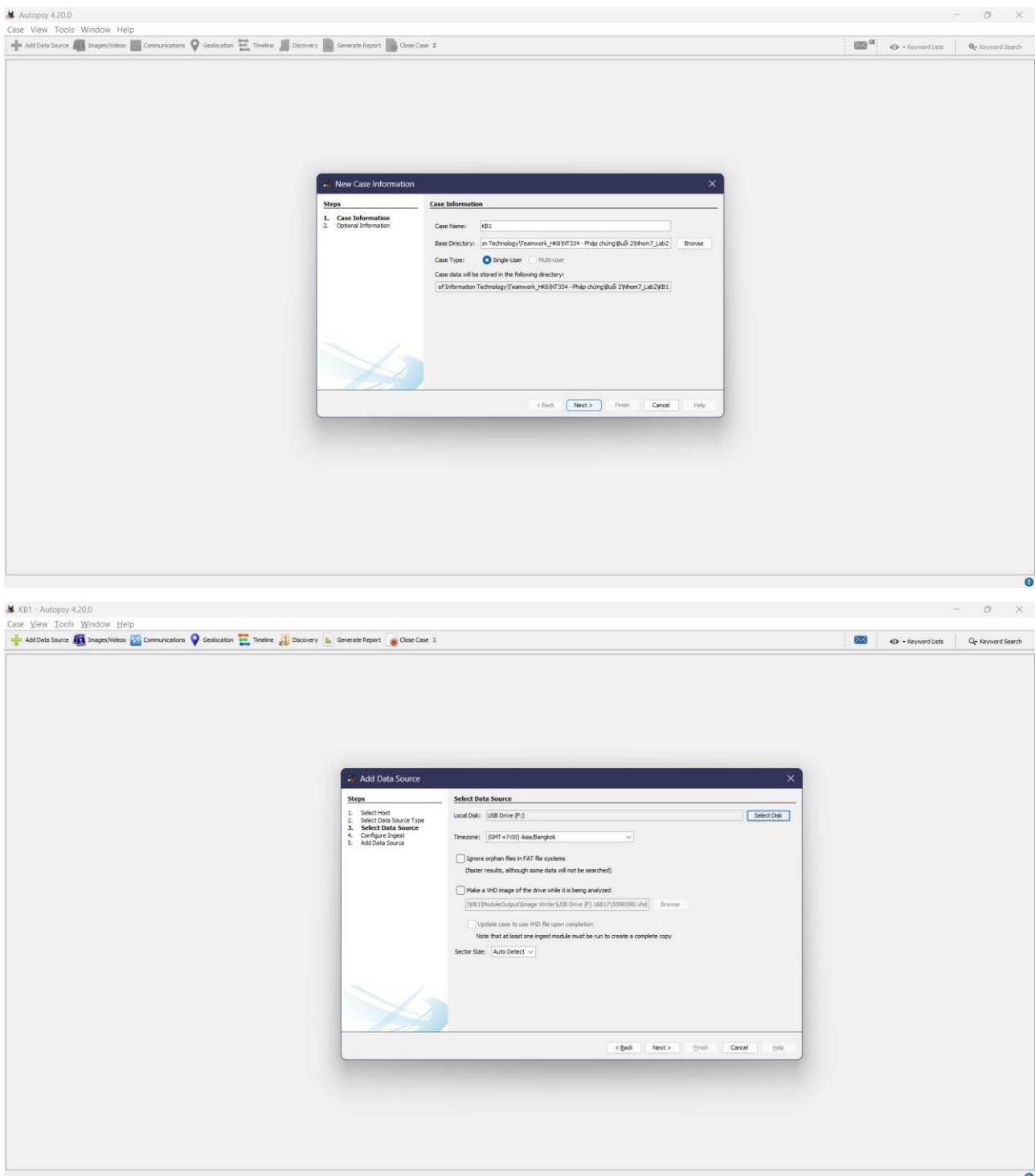
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành,

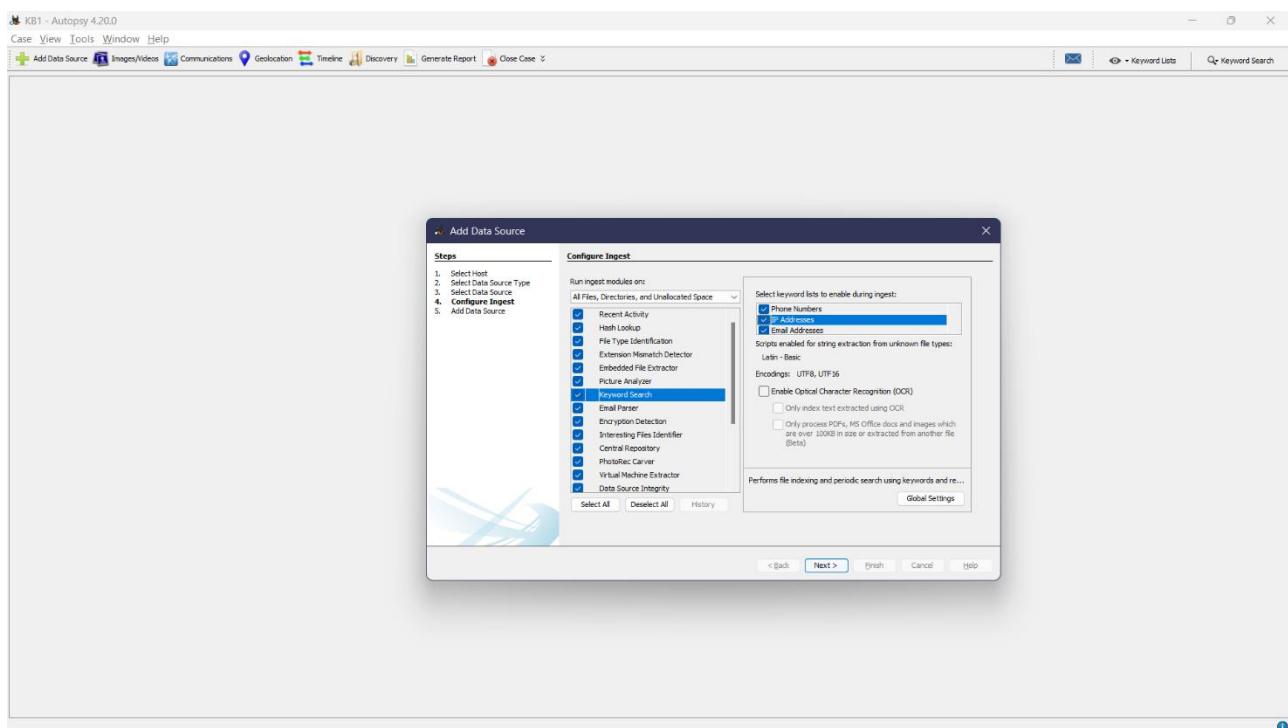
6	Kịch bản 06	- Phân tích tài nguyên kb06-session02.pdf: hoàn thành - Điều tra các thông tin liên quan đến vụ án	Kiệt, Trâm, Ngân	30%
---	-------------	---	------------------------	-----

BÁO CÁO CHI TIẾT

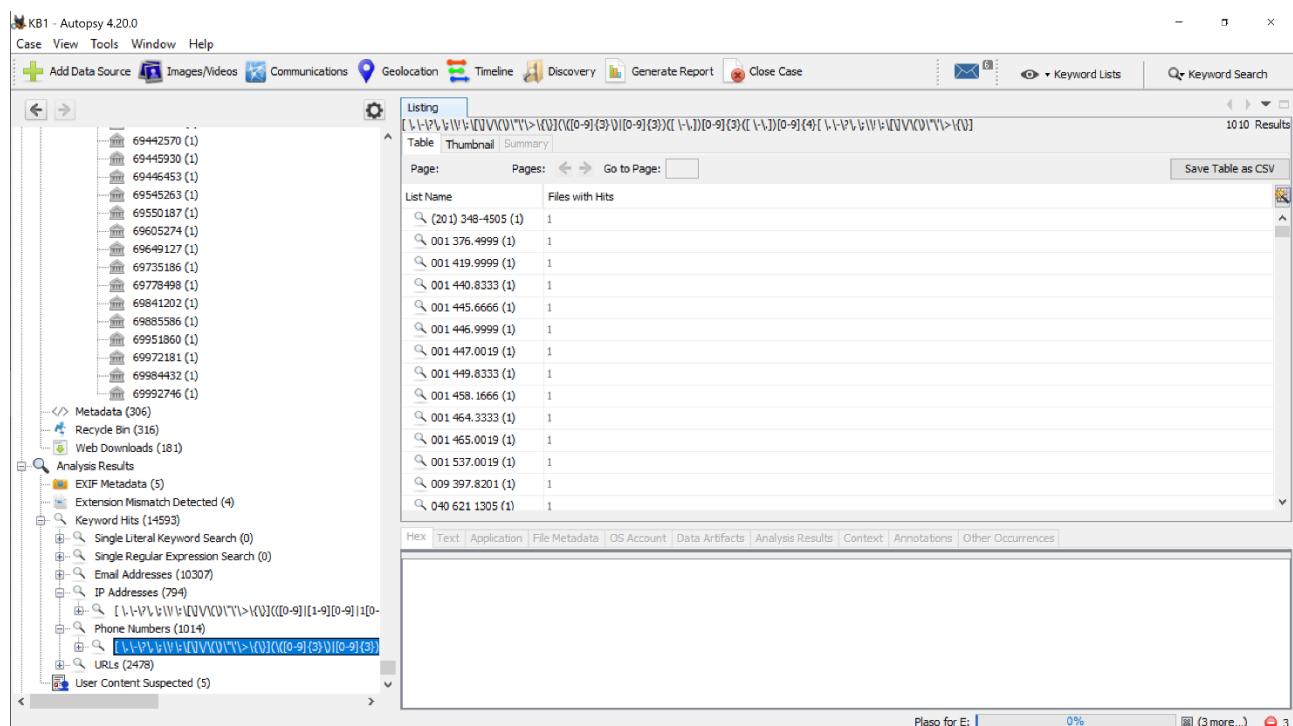
1. Kích bản 1:

Set up các config scan và chọn ổ đĩa để scan (USB):

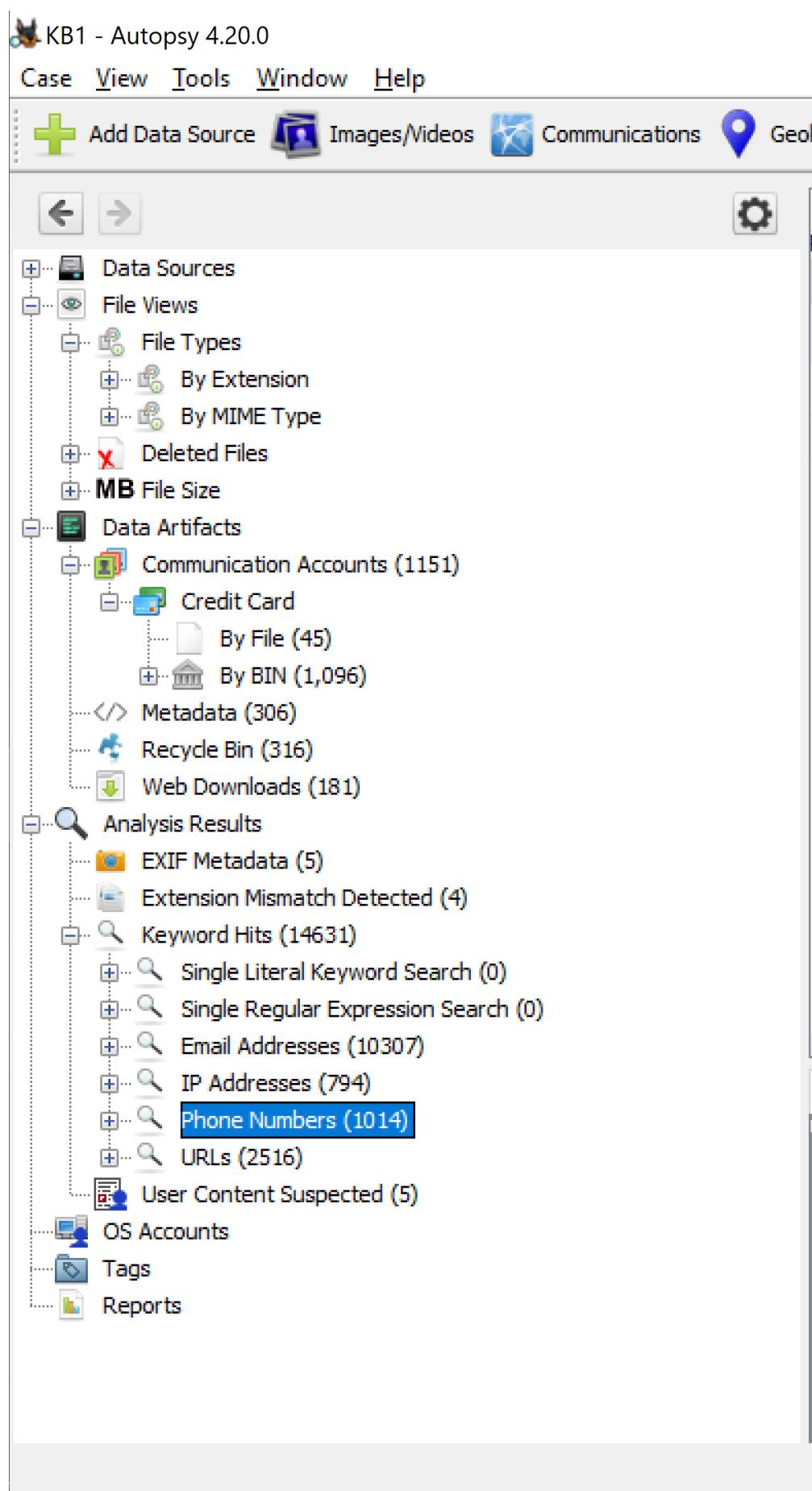




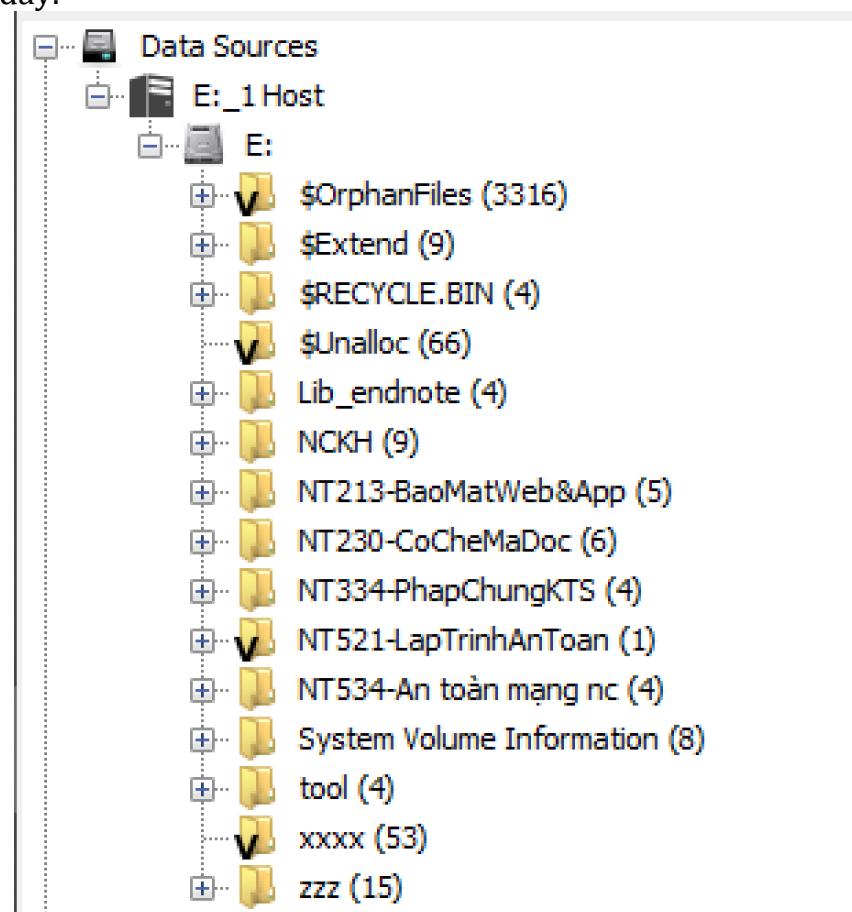
Chọn tìm các số điện thoại và địa chỉ IP có trong Filesystem.



Thực hiện việc xem xét toàn bộ file system, xem các options bên cây thư mục bên trái:

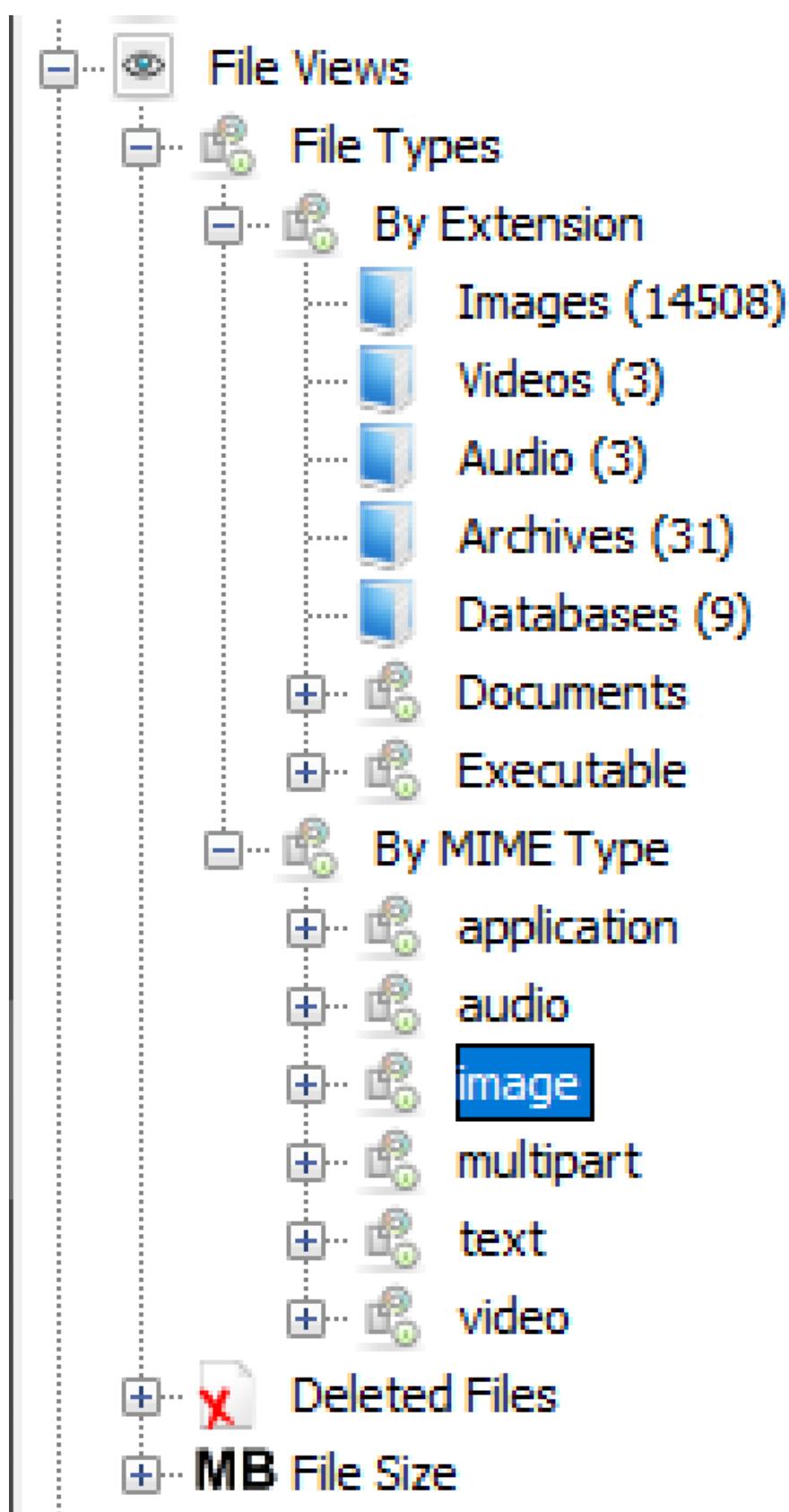


Data Sources: Là chỗ lưu ổ đĩa được dump ra, ta có thể coi các cây thư mục trong ổ đĩa ở đây.

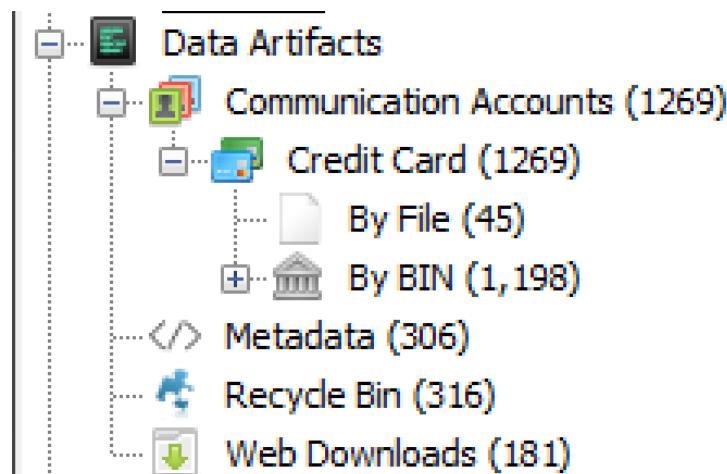


File view: Là nơi để coi cụ thể các file có trong ổ đĩa.

- File Type: Phân loại file dựa trên đuôi file và không có kiểm tra signature.
- By MIME Type: Phân loại file dựa trên signature.
- Delete Files: Xem các files đã bị xóa.
- File Size: Phân loại theo kích thước file.



Data Artifact: Xem các thông tin ở local.



- Communication Accounts: Xem một số thông tin được xác định liên quan đến tài khoản cá nhân như credit card, mã BIN...

Type	Value	Source(s)
Account Type	CREDIT_CARD	Keyword Search
ID	44442212345567	Keyword Search
Card Number	44442212345567	KeywordSearch
Keyword	44442212345567	KeywordSearch

Metadata: List các metadata của file.

Data Artifacts - Recycle Bin (316)

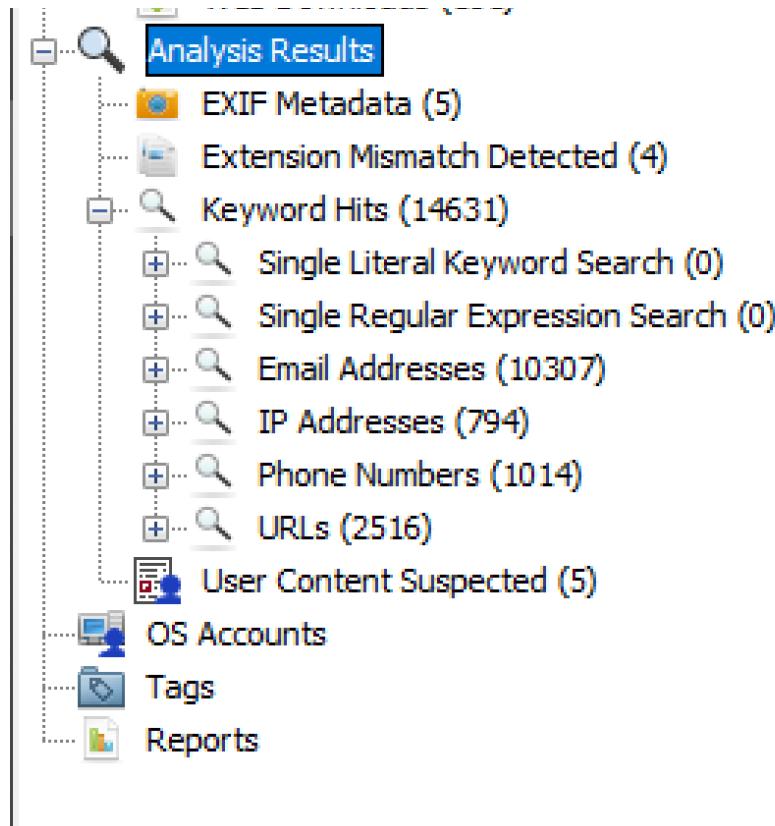
Source Name	S	C	O	Version	Date Modified	Date Created	Owner
Project-topics-and-Guides.pdf				1.7	2022-02-23 11:30:24 ICT	2022-02-23 11:30:24 ICT	Nguyễn Ngọc Tú
b-Tree1.pdf				1.7	2020-05-24 13:45:12 ICT	2020-05-24 13:45:12 ICT	Nguyễn Thành Sơn
b_tree.docx				1.5	2021-06-09 14:30:00 ICT	2021-06-08 15:58:00 ICT	NGAN
Algorithm Paradigms.pdf				1.5	2019-03-03 04:25:28 ICT	2019-03-03 04:25:28 ICT	Son Nguyễn Thành
CSE680-16ShortestPaths.pptx				1.5	2011-11-28 15:23:40 ICT	2009-08-20 22:13:58 ICT	Roger Crewfis
Chapter 1 - Overview.pdf				1.5	2019-02-22 06:30:11 ICT	2019-02-22 06:30:11 ICT	Son Nguyễn Thành
hashtable.pdf				1.7	2019-05-13 13:55:49 ICT	2019-05-13 13:55:49 ICT	Nguyễn Thành Sơn
Danh-sach-lienket-blockchain.pdf				1.5	2021-04-27 12:52:23 ICT	2021-04-27 12:52:23 ICT	Son Nguyễn Thành
IT003.Decuong.ATTN.2020.pdf				1.5	2021-03-02 08:36:57 ICT	2021-03-02 08:36:57 ICT	Admin
LinkedList.pptx				1.7	2021-05-28 11:07:41 ICT	2018-03-23 14:04:26 ICT	Son Nguyễn Thành
linkedlist_prev.pdf				1.7	2020-04-11 12:29:53 ICT	2020-04-11 12:29:53 ICT	Nguyễn Thành Sơn
Searching.pdf				1.7	2021-03-09 14:55:53 ICT	2021-03-09 14:55:53 ICT	Nguyễn Thành Sơn
Sorting.pdf				1.7	2021-03-09 14:56:26 ICT	2021-03-09 14:56:26 ICT	Nguyễn Thành Sơn

Recycle Bin: Xem các thư mục có trong thùng rác của máy.
Web Downloads: Xem các file được download từ internet.

Data Artifacts - Web Downloads (181)

Source Name	S	C	O	Path	URL
SRJ61D9T.csv:Zone.Identifier				/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	about:internet
RRH52YE.rar:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://raw.githubusercontent.com
NVD.7z:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://raw.githubusercontent.com
SRW96NQS.zip:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://raw.githubusercontent.com
Tài liệu thực hành-20221223.zip:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://courses.uit.edu.vn/mod/folk
Bai tap chuong 1.pdf:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://courses.uit.edu.vn/pluginfile
Bai tap chuong 2.pdf:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://courses.uit.edu.vn/pluginfile
Bai tap chuong 3.pdf:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://courses.uit.edu.vn/pluginfile
Bai tap chuong 4.pdf:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://courses.uit.edu.vn/pluginfile
Bai tap chuong 5.pdf:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://courses.uit.edu.vn/pluginfile
Bai tap chuong 6.pdf:Zone.Identifier	1			/\$RECYCLE.BIN/S-1-5-21-3907455383-3182094125-13507...	https://courses.uit.edu.vn/pluginfile
Bai-tap-BMW.rar:Zone.Identifier	1			/Bai-tap-BMW.rar	https://cdn.fbsbx.com/v/t59.2708-
A-Voting-Based-Blockchain-Interoperability-Ora.pdf:Zon	1			/Lib_endnote/My EndNote Library.Data/PDF/2804036524/...	https://arxiv.org/pdf/2111.10091 v

Analysis Result: Lưu kết quả phân tích từ các plug-in có trong tool liên quan đến thông tin được dump.



- Exif Metadata: Thông tin metadata được trích xuất bởi công cụ Exif, cho nhiều thông tin hơn.
- Extension Mismatch Detected: Những file có extension và signature khác nhau, là những file bất thường hoặc có signature không hợp lệ.
- Keyword Hints: Lọc các thông tin dựa trên những keywords có sẵn để dễ dàng xem thông tin hơn.

Vd xem email address:

The screenshot shows the main Autopsy 4.20.0 interface with the 'Analysis Results' pane open. The pane lists 'Email Addresses (10307)' with the following entries:

List Name	Files with Hits
15-213-staff@cs.cmu.edu (1)	1
1652010@gm.uit.edu.vn (2)	2
1smalmukadi@nu.edu.sa (1)	1
20520648@gm.uit.edu.vn (8)	8
20520815@gm.uit.edu.vn (6)	6
33duyn@uit.edu.vn (1)	1
69rc@3.hr (1)	1
a2e3a@pigeon.hereway.com (1)	1
aabbieqt@pinterest.com (1)	1
aabercromby@ssoup.io (1)	1
acorybu@berkeley.edu (1)	1
aaddingv@wired.com (1)	1
aadneyp3@unblog.fr (1)	1
addiran53@webo.com (1)	1

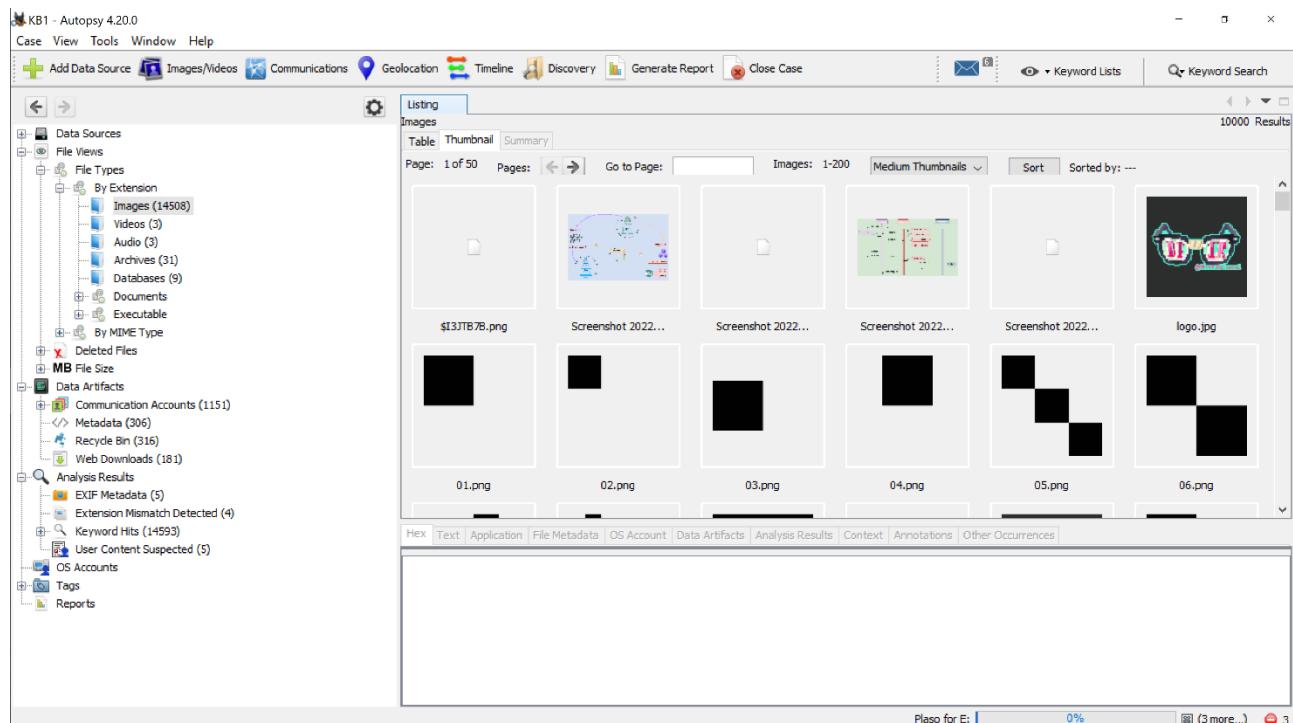
- User Content Suspected: Đưa ra một số file bị nghi ngờ làm lộ thông tin user.
- OS Account: Các accounts tồn tại trong hệ điều hành:

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	E:_1 Host	Local	NT AUTHORITY	
S-1-5-21-3907455383-3182094125-1350755033-1003	0				E:_1 Host	Domain		
S-1-5-21-3907455383-3182094125-1350755033-500	0				E:_1 Host	Domain		

- Tags: Các tags được điều tra viên gắn nhãn từ trước đó.
 - Reports: Các bản báo cáo được điều tra viên lưu lại trước đó.
- Tìm thư mục có nhiều File nhất trong Filesystem.*

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
063				2022-12-27 20:02:00 ICT	2022-12-27 20:02:00 ICT	2022-12-13 13:30:32 ICT	2022-12-13 13:30:32 ICT	48
064				2022-12-27 20:02:00 ICT	2022-12-27 20:02:00 ICT	2022-12-13 13:30:32 ICT	2022-12-13 13:30:32 ICT	48
065				2022-12-27 20:02:02 ICT	2022-12-27 20:02:02 ICT	2022-12-13 13:30:32 ICT	2022-12-13 13:30:32 ICT	48
066				2022-12-27 20:02:03 ICT	2022-12-27 20:02:03 ICT	2022-12-13 13:30:32 ICT	2022-12-13 13:30:32 ICT	48
067				2022-12-27 20:02:04 ICT	2022-12-27 20:02:04 ICT	2022-12-13 13:30:32 ICT	2022-12-13 13:30:32 ICT	48
068				2022-12-27 20:02:05 ICT	2022-12-27 20:02:05 ICT	2022-12-13 13:30:32 ICT	2022-12-13 13:30:32 ICT	48
069				2022-12-27 20:02:06 ICT	All changes have been saved	2022-12-13 13:30:32 ICT	2022-12-13 13:30:32 ICT	48
070				2022-12-27 20:02:07 ICT	2022-12-27 20:02:07 ICT	2022-12-13 13:30:33 ICT	2022-12-13 13:30:33 ICT	48
071				2022-12-27 20:02:08 ICT	2022-12-27 20:02:08 ICT	2022-12-13 13:30:33 ICT	2022-12-13 13:30:33 ICT	48

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



File .pdf

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
whitepaper-v2.pdf:Zone.Identifier	▼			2023-04-08 13:35:22 ICT	2023-04-08 13:35:24 ICT	2023-04-08 13:35:22 ICT	2023-04-08 13:35:22 ICT
whitepaper-v2.pdf				2023-04-08 13:35:22 ICT	2023-04-08 13:35:24 ICT	2023-04-08 13:35:22 ICT	2023-04-08 13:35:22 ICT
tree.pdf	0			2021-05-19 10:01:22 ICT	2021-05-19 10:04:44 ICT	2021-06-02 12:37:24 ICT	2021-05-19 10:04:44 ICT
template-NT521.N11.ANTN.pdf	▼	0		2022-11-21 21:32:41 ICT	2022-11-29 09:09:31 ICT	2022-11-29 12:47:51 ICT	2022-11-29 12:47:51 ICT
stackqueue.pdf	0			2021-05-12 07:29:11 ICT	2021-05-12 07:32:18 ICT	2021-05-19 10:04:45 ICT	2021-05-12 07:29:11 ICT
seedlab-lab 12-instruction-return-to-lbc.pdf	0			2022-11-18 13:36:31 ICT	2022-11-18 13:38:12 ICT	2022-11-21 16:58:05 ICT	2022-11-18 13:36:31 ICT
report_lab5.pdf	0			2022-05-25 09:01:19 ICT	2022-05-25 09:05:07 ICT	2023-03-27 22:16:51 ICT	2022-05-25 09:01:19 ICT
report_Lab6.pdf	0			2022-06-01 15:50:13 ICT	2022-07-23 15:37:47 ICT	2023-03-27 22:18:58 ICT	2022-06-01 15:50:13 ICT
report.pdf	1			2022-06-14 22:52:01 ICT	2022-06-14 22:52:45 ICT	2022-06-16 15:48:38 ICT	2022-06-14 22:52:01 ICT

Ở đây trong phần lọc extension thì tool cũng đã lọc cho chúng ta các file office, ta có thể vào table office, chọn sort theo extention và bôi đen tất cả file doc cho vào 1 tag để xem số lượng:

Hard Drive Forensics

KB1 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

Listing Office

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created
0_Lucene84_0.doc	▼			2023-04-17 14:18:02 ICT	2023-04-17 14:18:02 ICT	2023-04-17 14:33:57 ICT	2023-04-
Microsoft_Word_97_-2004_Document4.doc	▼	0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document12.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document3.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document11.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document6.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document2.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document5.doc	▼	0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document1.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of Page Go to Page: Script: Latin - Basic

Plaso for E: 0% (4 more...) 3

KB1 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

Listing Office

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created
0_Lucene84_0.doc	▼			2023-04-17 14:18:02 ICT	2023-04-17 14:18:02 ICT	2023-04-17 14:33:57 ICT	2023-04-
Microsoft_Word_97_-2004_Document4.doc	▼	0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document12.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document3.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document11.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document6.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document2.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document5.doc	▼	0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-
Microsoft_Word_97_-2004_Document1.doc		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-

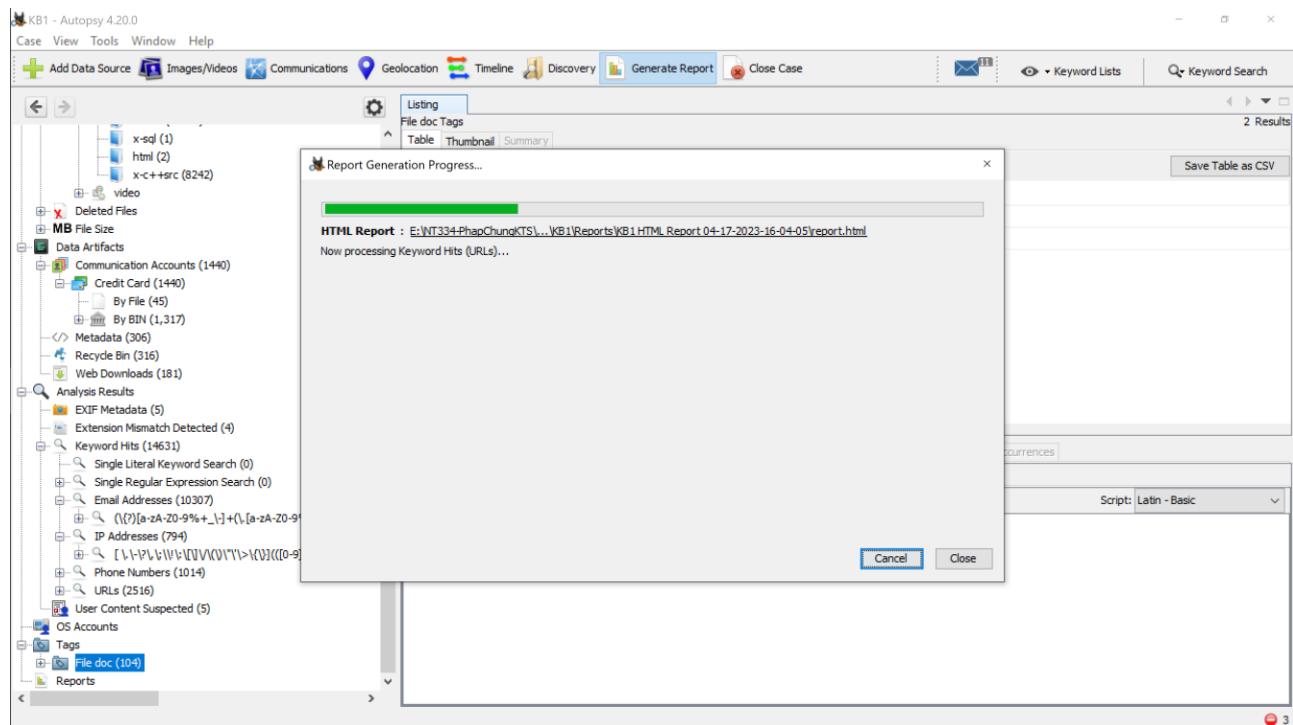
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

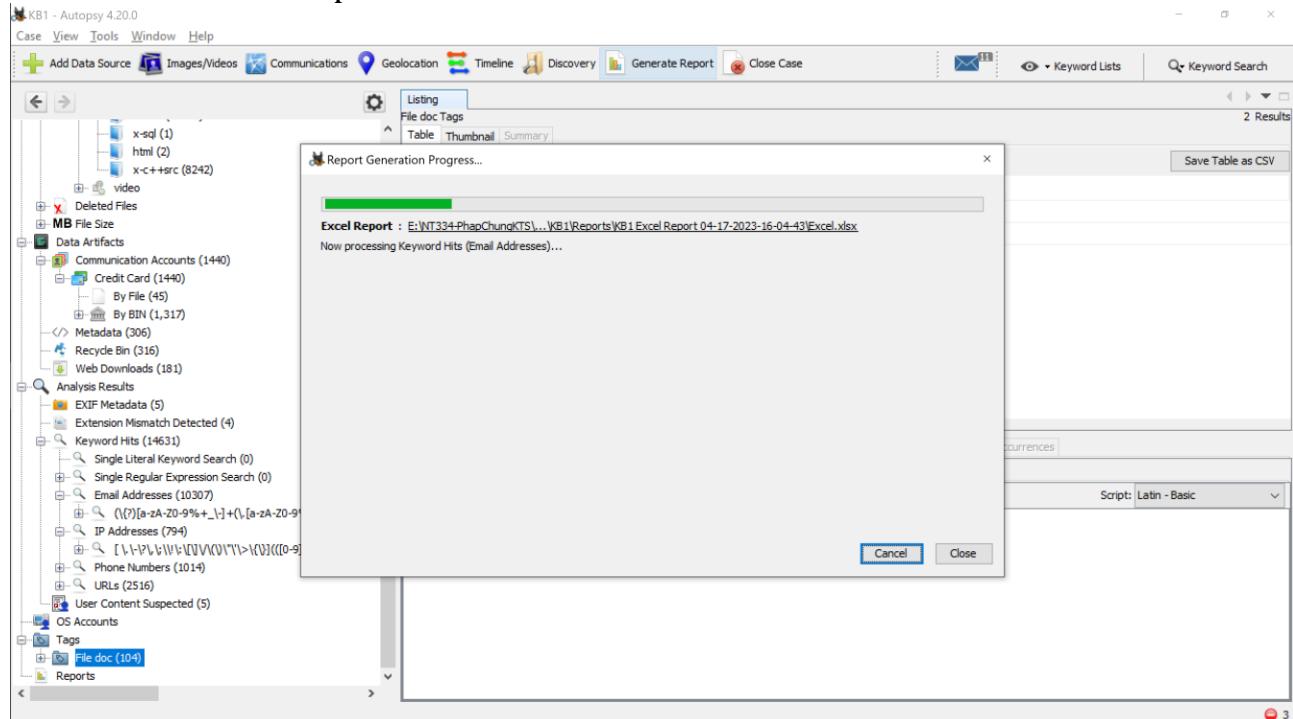
Page: 1 of Page Go to Page: Script: Latin - Basic

Plaso for E: 0% (4 more...) 3

Generate file report HTML:



Generate file report Excel:



File report HTML:

Report Navigation

- Case Summary
- Accounts: Credit Card (1440)
- EXIF Metadata (5)
- Extension Mismatch Detected (4)
- Keyword Hits (16057)
- Metadata (306)
- Recycle Bin (316)
- Tagged Files (104)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (5)
- Web Downloads (181)

Keyword Hits

- Email Addresses
- IP Addresses
- Phone Numbers
- URLs

Email Addresses

Email Address	Preview	Source File	Tags
15-213-staff@cs.cmu.edu	staff mailing list: «15-213-staff@cs.cmu.edu» use this for all co /img_E:/zzz/l_hethong/slide_vn/01-overview.pptx		
16520010@gm.uit.edu.vn	ười nhận 7 ví dụ: «16520010@gm.uit.edu.vn», tranvana@gmail.com /img_E:/zzz/Network/slide/TL7-all.pdf • mailto:«16520010@gm.uit.edu.vn» mailto:tranvana@gma /img_E:/zzz/Network/vfsvàd/Lab5/HDT5 - Lab 5 - Sending Receiving Email ir		
1smalmukadi@nu.edu.sa	bpanda@uark.edu «1smalmukadi@nu.edu.sa» abstract. databases /img_E:/zzz/Cryptography/DoAn/Design.pdf		
20520648@gm.uit.edu.vn	i kim ngân 20520648 «20520648@gm.uit.edu.vn» 2 nguyên bình thư /img_E:/zzz/NT101 - net sec/ThucHanh/Lab2/NT101.N11.ANTN-Lab2.1_Gi		

Đánh giá, nhận xét: Thông qua file report này, ta có thể xem được hầu hết các trường dữ liệu có thể xem trong AutoSpy với giao diện trực quan hơn so với trong app.

Ngoài ra trong file report cũng bao gồm cả phiên bản cụ thể của các tool, plugin được dùng trong quá trình thực hiện điều tra.

Report Navigation

- Case Summary
- Accounts: Credit Card (1440)
- EXIF Metadata (5)
- Extension Mismatch Detected (4)
- Keyword Hits (16057)
- Metadata (306)
- Recycle Bin (316)
- Tagged Files (104)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (5)
- Web Downloads (181)

Autopsy Version:	4.20.0
Android Analyzer Module:	4.20.0
Central Repository Module:	4.20.0
Data Source Integrity Module:	4.20.0
Email Parser Module:	4.20.0
Embedded File Extractor Module:	4.20.0
Encryption Detection Module:	4.20.0
Extension Mismatch Detector Module:	4.20.0
File Type Identification Module:	4.20.0
GPX Parser Module:	1.2
Hash Lookup Module:	4.20.0
Interesting Files Identifier Module:	4.20.0
Keyword Search Module:	4.20.0
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.20.0
Plaso Module:	4.20.0
Recent Activity Module:	4.20.0
YARA Analyzer Module:	4.20.0

Ingest History:

File report Excel:

Hard Drive Forensics

Nhóm 7

4

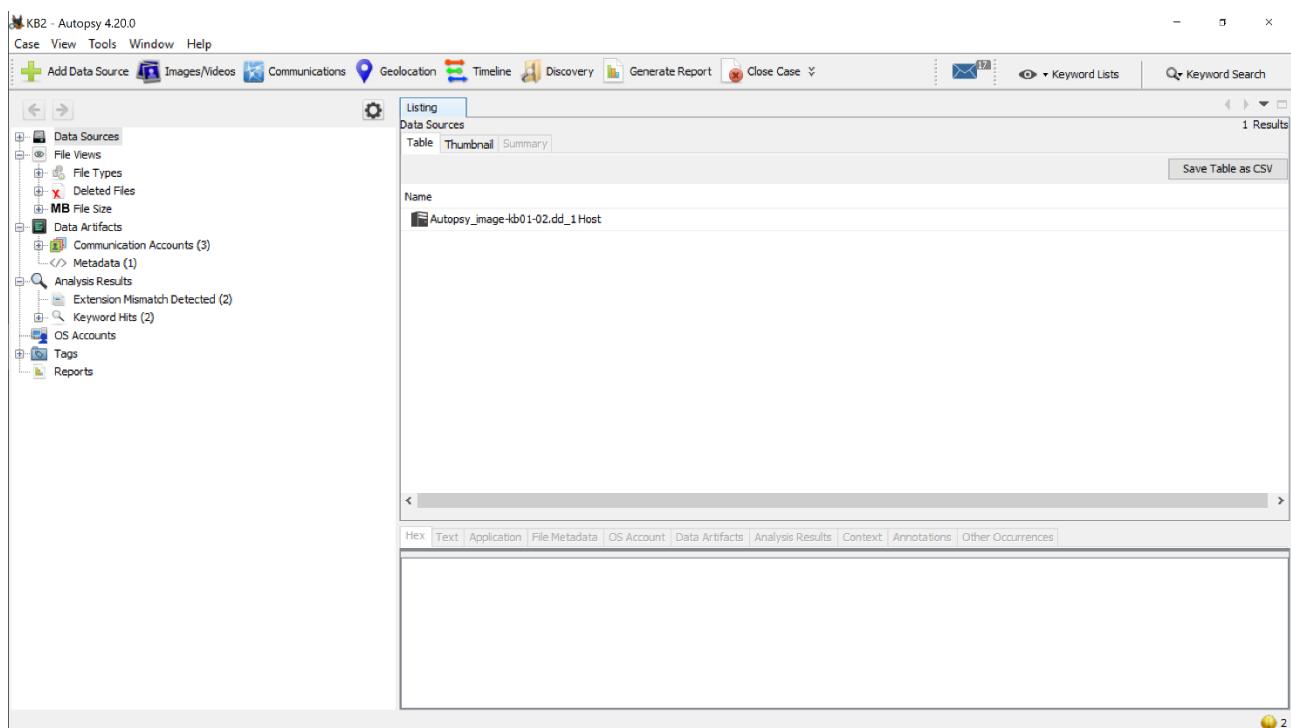
The screenshot shows a Microsoft Excel spreadsheet titled "Excel.xlsx". The ribbon menu is visible at the top, with tabs for Home, Insert, Draw, Page Layout, Formulas, Data, Review, View, Automate, and Help. The Home tab is selected. The main area contains a table with 12 columns and approximately 30 rows of data. The columns are labeled A through L. Column A is titled "Review Status", B is "Bank Name", C is "Card Number", D is "Card Scheme", E is "Card Type", F is "Country", G is "ID", H is "Keyword", and I is "Keyword Preview". The data includes various bank names like "Undecided", "Bank of America", "Wells Fargo", etc., card numbers, and IDs. The "Keyword Preview" column contains long strings of characters representing the keywords found in the data.

Nhận xét, đánh giá: File report dạng Excel được chia thành nhiều sheet tương ứng với nhiều trường dữ liệu. Theo em thì file report dạng này có phần hơi khó nhìn và thiếu trực quan.

Về nội dung, phần sumary các version tool, plugin có phần ít và không đầy đủ bằng trong file report HTML.

The screenshot shows a Microsoft Excel spreadsheet titled "Excel.xlsx". The "Home" tab is selected. The first row contains the header "Summary". Row 3 contains the text "Case Name:" followed by "KB1". Row 4 contains the text "Number of data sources in case:" followed by "1". Rows 5 through 21 are empty. The ribbon menu includes "File", "Home", "Insert", "Draw", "Page Layout", "Formulas", "Data", "Review", "View", "Automate", and "Help". The "Home" tab has sections for "Clipboard", "Font", "Alignment", "Number", "Styles", "Cells", and "Editing". The "Cells" section includes "Insert", "Delete", "Sort & Find & Filter", and "Format". The "Editing" section includes "Conditional Formatting", "Format as Table", "Cell Styles", and "Format". The status bar at the bottom shows tabs for "Summary", "EXIF Metadata", "Web Downloads", "Keyword Hits", "Accounts_Credit Card", and "Accounts_Credit Card".

2. Kịch bản 2:



Tìm các images có trong ảnh:
File Views → File Types → By Extension → Image

The screenshot shows the Autopsy 4.20.0 interface. The left sidebar is identical to the previous screenshot. The main pane now displays a table titled 'Listing' under the 'Images' tab. It shows 9 results. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags. The results include:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
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	2004-06-10 10:28:20 ICT	189021	Alloc
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	2004-06-10 10:27:36 ICT	274260	Alloc
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	0000-00-00 00:00:00	0000-00-00 00:00:00	326859	Unalloc
f00000639.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	0000-00-00 00:00:00	0000-00-00 00:00:00	175630	Unalloc
file6.jpg	0	2004-06-09 20:52:20 ICT	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	337653	2000-00-00 00:00:00	337653	Alloc
file10.jpg	0	2004-06-10 08:54:53 ICT	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	208919	2000-00-00 00:00:00	208919	Alloc
file9.jpg	0	2004-06-09 20:53:32 ICT	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	292813	2000-00-00 00:00:00	292813	Alloc
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	0000-00-00 00:00:00	0000-00-00 00:00:00	110373	Alloc
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	2004-06-10 10:28:20 ICT	214228	Alloc

Với mỗi file hình ảnh tìm được, liệt kê tất cả các thông tin liên quan đến file đó: tên file, loại file, size, thời gian tạo, xoá, sửa, MD5, kích thước hình ảnh:

KB2 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

Listing

file4.jpg - Properties

Name	Value
Name	file4.jpg
Size	(No Property Editor)
Comments	NO_COMMENT
Modified Time	2004-06-10 10:28:22 ICT
Change Time	2004-06-10 10:28:06 ICT
Access Time	2004-06-10 10:28:22 ICT
Created Time	2004-06-10 10:28:20 ICT
Size	189021
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/Img_Autopsy_image-kb01-02.dd/invalid/file4.jpg
MDS Hash	c8de721102617158e8492121bdad3711
SHA-256 Hash	0da94b7a5d24698f7dca510255493c4e5ae...
MIME Type	application/octet-stream
Extension	jpg

Annotations Other Occurrences

file1.jpg - Properties

Name	Value
Name	file1.jpg
Size	(No Property Editor)
Comments	NO_COMMENT
Modified Time	2004-06-10 13:59:40 ICT
Change Time	2004-06-10 10:27:36 ICT
Access Time	2004-06-10 10:27:36 ICT
Created Time	2004-06-10 10:27:36 ICT
Size	274260
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/Img_Autopsy_image-kb01-02.dd/alloc/file1.jpg
MDS Hash	75b6d0056615a36c3809b46fc64ba6d
SHA-256 Hash	2a082002a5d42b71b67934a23371cel0bae9...
MIME Type	image/jpeg
Extension	jpg

Annotations Other Occurrences

Tags Menu

KB2 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Data Sources File Views File Types By Extension Images (9) Videos (0) Audio (0) Archives (3) Databases (1) Documents Executable By MIME Type Deleted Files File System (2) All (5) MB File Size Data Artifacts Communication Accounts (3) Metadata (1) Analysis Results Extension Mismatch Detected (2) Keyword Hits (2) OS Accounts Tags Reports

f0000000.jpg - Properties

Name	f0000000.jpg
(No Property Editor)	NO_COMMENT
Na	O
Modified Time	0000-00-00 00:00:00
Change Time	0000-00-00 00:00:00
Access Time	0000-00-00 00:00:00
Created Time	0000-00-00 00:00:00
Size	326859
Flags(Dir)	Unallocated
Flags(Meta)	Unallocated
Known	unknown
Location	/Img_Autopsy_image-kb01-02.dd\$CarvedFil...
MDS Hash	0c452c58001cfaf7c66027ae89c41068a
SHA-256 Hash	e09242768c1f897197b499042511b105c2...
MIME Type	image/jpeg
Extension	jpg

f00000639.jpg - Properties

Name	f0000639.jpg
(No Property Editor)	NO_COMMENT
Na	O
Modified Time	0000-00-00 00:00:00
Change Time	0000-00-00 00:00:00
Access Time	0000-00-00 00:00:00
Created Time	0000-00-00 00:00:00
Size	175630
Flags(Dir)	Unallocated
Flags(Meta)	Unallocated
Known	unknown
Location	/Img_Autopsy_image-kb01-02.dd\$CarvedFil...
MDS Hash	a0f55222024a4e221715a3a665320763
SHA-256 Hash	00ee3fab68b24f98f8f758fa8f25b360550ba...
MIME Type	image/jpeg
Extension	jpg

Annotations Other Occurrences Tags Menu

Save Table as CSV

Access Time Created Time Size Flags

2004-06-10 10:28:22 ICT 2004-06-10 10:28:20 ICT 189021 Alloc
 2004-06-10 10:27:36 ICT 2004-06-10 10:27:36 ICT 274260 Alloc
 0000-00-00 00:00:00 0000-00-00 00:00:00 326859 Unalloc
 0000-00-00 00:00:00 0000-00-00 00:00:00 175630 Unalloc
 0000-00-00 00:00:00 0000-00-00 00:00:00 337653 Alloc
 0000-00-00 00:00:00 0000-00-00 00:00:00 208919 Alloc
 0000-00-00 00:00:00 0000-00-00 00:00:00 292813 Alloc
 0000-00-00 00:00:00 0000-00-00 00:00:00 110373 Alloc
 2004-06-10 10:28:20 ICT 2004-06-10 10:28:20 ICT 214228 Alloc

I AM PICTURE #4

I AM PICTURE #3

The screenshot displays two side-by-side instances of the Autopsy 4.20.0 forensic analysis tool. Both instances show the same analysis results for two different files: file8.jpg and file10.jpg.

File8 Properties:

Name	Value
Name	file8.jpg
S	(No Property Editor)
C	NO_COMMENT
O	0
Modified Time	2004-06-09 20:52:20 ICT
Change Time	0000-00-00 00:00:00
Access Time	0000-00-00 00:00:00
Created Time	0000-00-00 00:00:00
Size	337653
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.ddf/archive/file...
MDS Hash	f9956234a8915eeff6957b049eced9d1b1
SHA-256 Hash	ca8c1910b7a759b63da9d146a62c3af26337...
MIME Type	image/jpeg
Extension	jpg

File10 Properties:

Name	Value
Name	file10.jpg
S	(No Property Editor)
C	NO_COMMENT
O	0
Modified Time	2004-06-10 08:54:53 ICT
Change Time	0000-00-00 00:00:00
Access Time	0000-00-00 00:00:00
Created Time	0000-00-00 00:00:00
Size	208919
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.ddf/archive/file...
MDS Hash	c476a66ccdc2795b4f6f8e27273dd788
SHA-256 Hash	81f5733ec0e6053e100351503e82645501485...
MIME Type	image/jpeg
Extension	jpg

Analysis Results: Both instances show identical analysis results for both files, including Extension Mismatch Detected (2) and Keyword Hits (2).

Timeline: Both instances show a single entry in the Timeline: "2004-06-10 10:28:20 ICT".

Discovery: Both instances show a single entry in the Discovery table: "2004-06-10 10:28:20 ICT".

Generate Report: Both instances have a "Save Table as CSV" button in the top right corner of their respective property windows.

Hard Drive Forensics

The screenshot shows two separate forensic analysis sessions in the Autopsy tool. Both sessions are titled "KB2 - Autopsy 4.20.0".

Session 1 (Top): The left pane shows a tree view of data sources, including "File Types" (By Extension: Images, Videos, Audio, Archives, Databases), "Deleted Files", and "MB File Size". The right pane displays the properties of a file named "file9.jpg". The properties table includes fields like Name, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, Location, MD5 Hash, SHA-256 Hash, MIME Type, and Extension. The "Known" field is set to "unknown". The "Location" field shows the path "Img_Autopsy_image-kb01-02.dd/archive/file...". The "SHA-256 Hash" field contains a long string of characters. The "MIME Type" is listed as "image/jpeg". A yellow circular watermark "I AM PICTURE #8" is overlaid on the bottom right of the properties window.

Session 2 (Bottom): Similar to Session 1, it shows a tree view of data sources and the properties of a file named "image_0.jpg". The properties table is identical, with the "Known" field set to "unknown" and the "Location" field showing the same path as the first session. A purple arrow-shaped watermark "I AM PICTURE #9" is overlaid on the bottom right of the properties window.

KB2 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Data Sources File Views File Types By Extension Images (9) Videos (0) Audio (0) Archives (3) Databases (1) Documents Executable Deleted Files File System (2) All (5) MB File Size Data Artifacts Communication Accounts (3) Metadata (1) Analysis Results Extension Mismatch Detected (2) Keyword Hits (2) OS Accounts Tags Reports

file3.jpg - Properties

Name	file3.jpg
S	(No Property Editor)
C	NO_COMMENT
Na	0
D	2004-06-10 10:14:27:02 ICT
M	2004-06-10 10:26:20 ICT
G	2004-06-10 10:26:20 ICT
A	2004-06-10 10:26:20 ICT
R	214228
F(Dir)	Allocated
F(Meta)	Allocated
K	unknown
L	/img_Autopsy_image-kb01-02.dd/invalid/file3...
MDS Hash	1ba4e915910541eda255ee2617533bc
SHA-256 Hash	f1684e96895d2970dbda0f95786fb41109c7...
MIME Type	text/plain
E	jpg

file3.jpg

Annotations Other Occurrences

Access Time Created Time Size Flags

2004-06-10 10:28:22 ICT 2004-06-10 10:28:20 ICT 189021 Alloc

2004-06-10 10:27:36 ICT 2004-06-10 10:27:36 ICT 274260 Alloc

0000-00-00 00:00:00 0000-00-00 00:00:00 326859 Unalloc

0000-00-00 00:00:00 0000-00-00 00:00:00 175630 Unalloc

0000-00-00 00:00:00 0000-00-00 00:00:00 337653 Alloc

0000-00-00 00:00:00 0000-00-00 00:00:00 208911 Alloc

0000-00-00 00:00:00 0000-00-00 00:00:00 292813 Alloc

0000-00-00 00:00:00 0000-00-00 00:00:00 110373 Alloc

2004-06-10 10:28:20 ICT 2004-06-10 10:28:20 ICT 214228 Alloc

Annotations Other Occurrences

Reset Text Source: File Text

Ngoài ra, tụi em còn tìm được 1 file ảnh bị giấu đi bằng cách chèn thêm bytes vào trong file.

Dấu hiệu để biết được file này là file ảnh là vì trong file có bytes JEFIF (Trong các file ảnh kia cũng có các bytes tương tự)

KB2 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Data Sources Autopsy_image-kb01-02.dd_1 Host Autopsy_image-kb01-02.dd \$OrphanFiles (0) \$CarvedFiles (1) \$Extend (5) \$Unalloc (1) alloc (4) archive (5) del1 (3) del2 (3) invalid (5) misc (6) RECYCLER (3) System Volume Information (3)

File Views File Types By Extension By MIME Type Deleted Files File System (2) All (5) MB File Size MB 50 - 200MB (0) MB 200MB - 1GB (0) MB 1GB+ (0) Data Artifacts Communication Accounts (3) Credit Card By File (1) By BIN (3) Metadata (1)

Listing /img_Autopsy_image-kb01-02.dd/misc

Table Thumbnail Summary

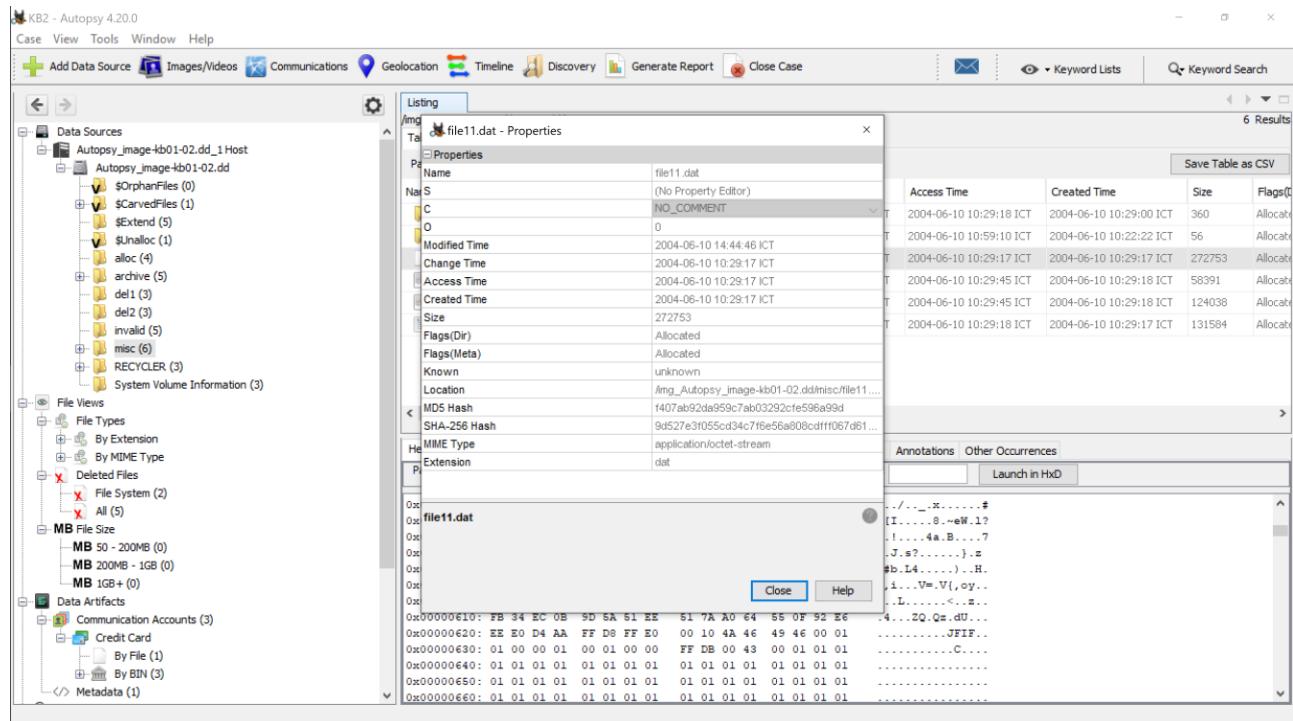
Page: 1 of 1 Pages: < > Go to Page: []

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
[current folder]				2004-06-10 10:29:18 ICT	2004-06-10 10:29:18 ICT	2004-06-10 10:29:00 ICT	2004-06-10 10:29:00 ICT	360	Alloc
[parent folder]				2004-06-10 10:59:10 ICT	2004-06-10 10:59:10 ICT	2004-06-10 10:22:22 ICT	2004-06-10 10:22:22 ICT	56	Alloc
file11.dat				0	2004-06-10 14:44:46 ICT	2004-06-10 10:29:17 ICT	2004-06-10 10:29:17 ICT	272753	Alloc
file13.dll				0	2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	58391	Alloc
file13.dll:here				0	2004-06-10 10:29:45 ICT	2004-06-10 10:29:45 ICT	2004-06-10 10:29:18 ICT	124038	Alloc
file12.doc				0	2004-06-10 14:20:58 ICT	2004-06-10 10:29:18 ICT	2004-06-10 10:29:17 ICT	131584	Alloc

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

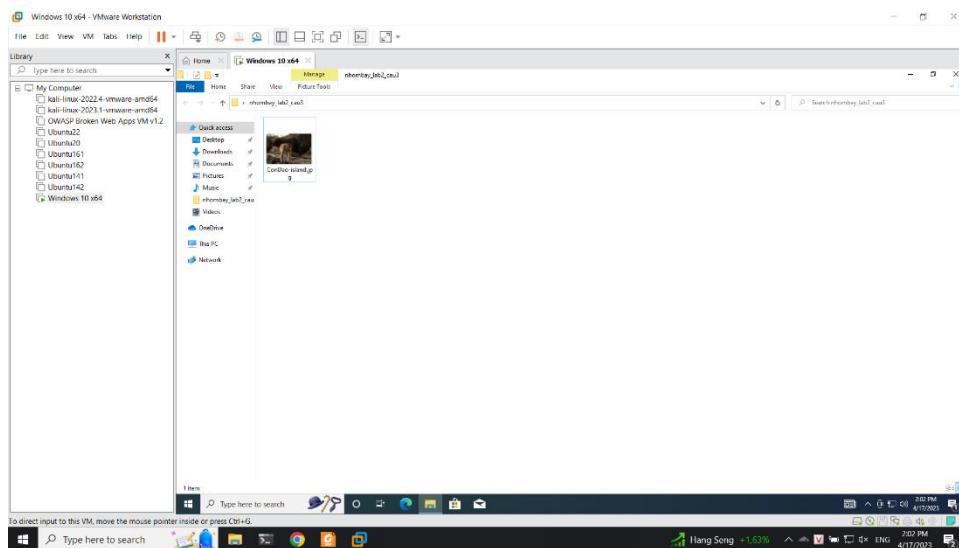
Page: 1 of 17 Page < > Go to Page: 1 Jump to Offset Launch in HxD

0x000005a0: 62 1B B2 2F FA C6 5F 0C 78 82 01 B3 C4 EF 8C 23 b.../...x...#
0x000005b0: B2 5B 49 B0 0F C8 10 F4 38 9B 7E 65 57 94 6C 3F .[I.....8-eW.1?
0x000005c0: 30 D7 21 B1 AB F4 F2 34 E1 C7 42 1D F3 04 03 37 01....4a.B...?7
0x000005d0: EC OD 4A EC 73 3F 10 00 CB FF 04 86 7D BF 7A 20 ...J.s?....}z
0x000005e0: 23 23 D2 7F 4C 34 E3 C5 B8 86 E3 29 D6 F0 48 83 *#b.I4....).H.
0x000005f0: BD 2C 69 01 17 0F 56 3D DC 56 7B 2C 6F 79 E0 BC ,.i....V!.oy..
0x00000600: 8C EF 90 4C E3 CF 03 A3 C3 9C 3C 16 98 7A 17 07 ...L....<..z..
0x00000610: FB 34 E0 OB 9D 5A 51 EE 51 7A A0 64 55 OF 98 E6 .4...ZQ.Qs.dU...
0x00000620: EE EO D4 AA FF DE FF EO 00 10 4X 46 49 46 00 01JF11.
0x00000630: 01 00 00 01 00 01 00 00 FF DE 00 43 00 01 01 01C...
0x00000640: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01C...
0x00000650: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01C...
0x00000660: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01



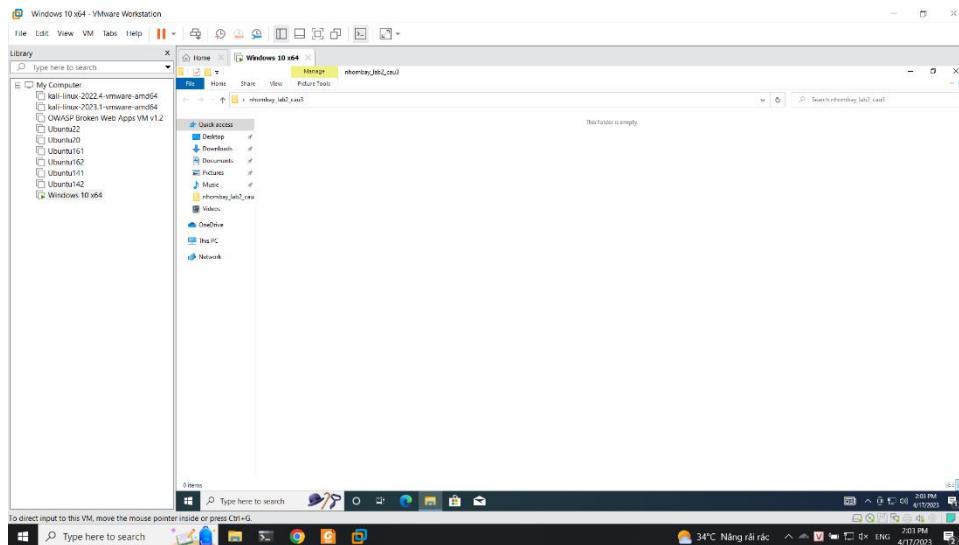
3. Kịch bản 3:

Đầu tiên tải file ảnh về và đổi tên thành ConDao-island

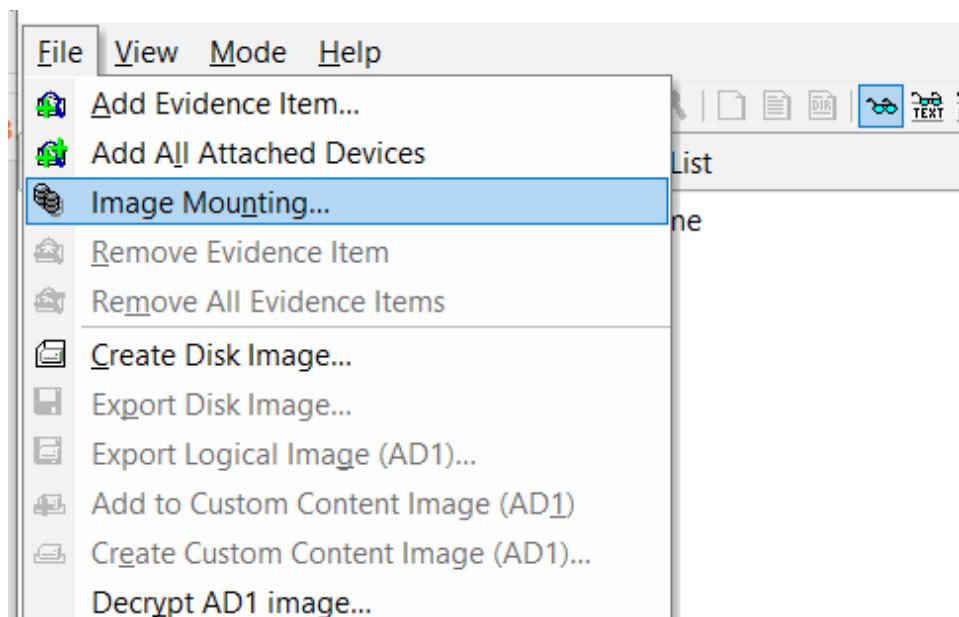


Xoá dữ file khỏi máy tính và xoá hẳn khỏi thùng rác

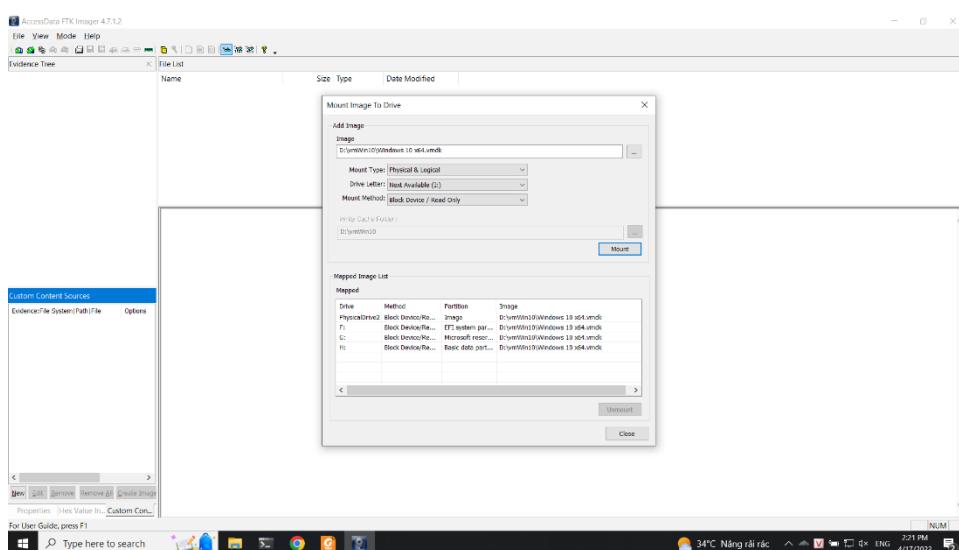
Hard Drive Forensics



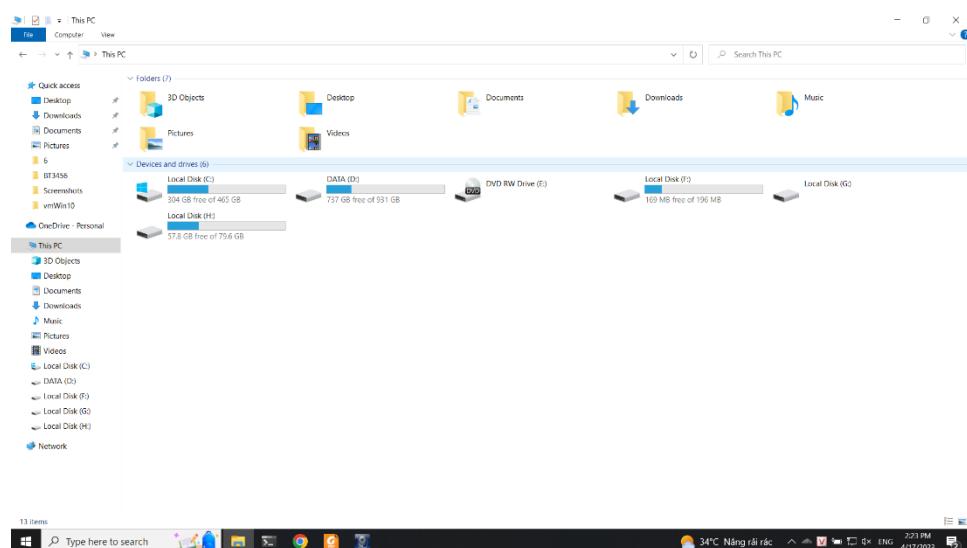
Chọn image mounting



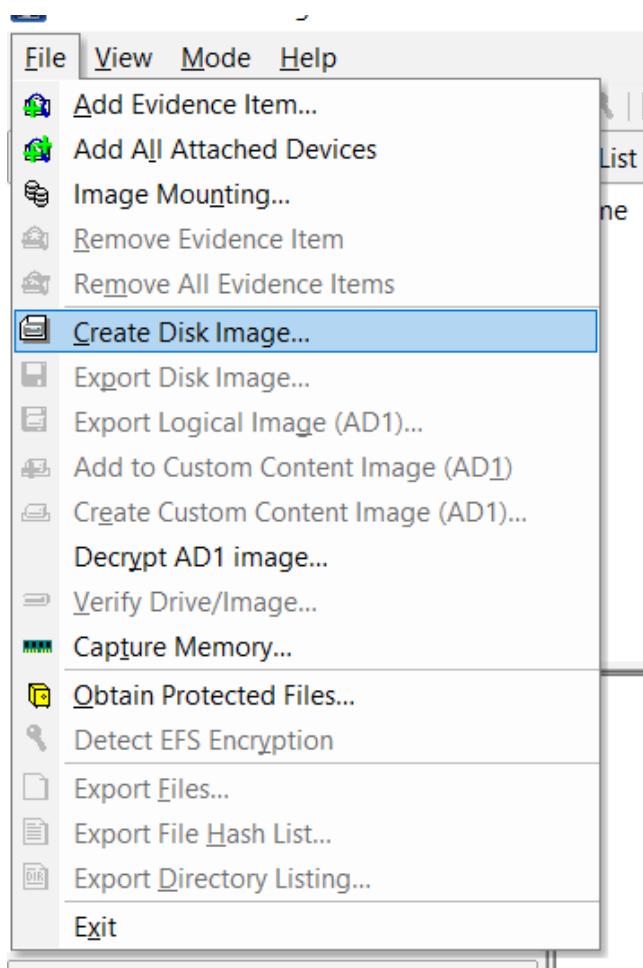
Thực hiện mouting



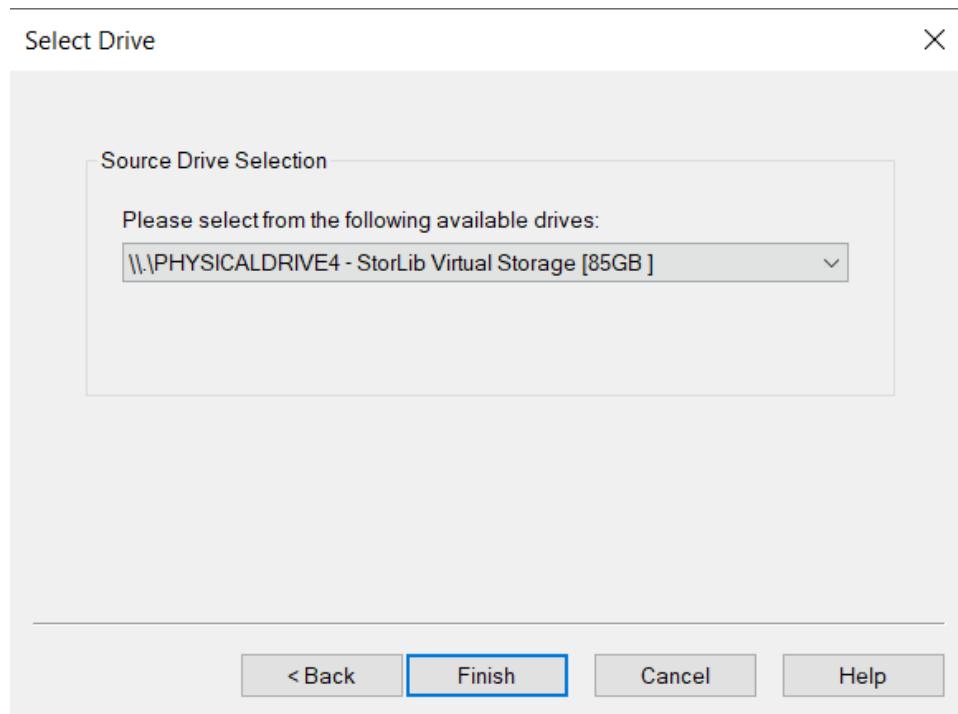
Máy sau khi được tạo ảnh đĩa thành công



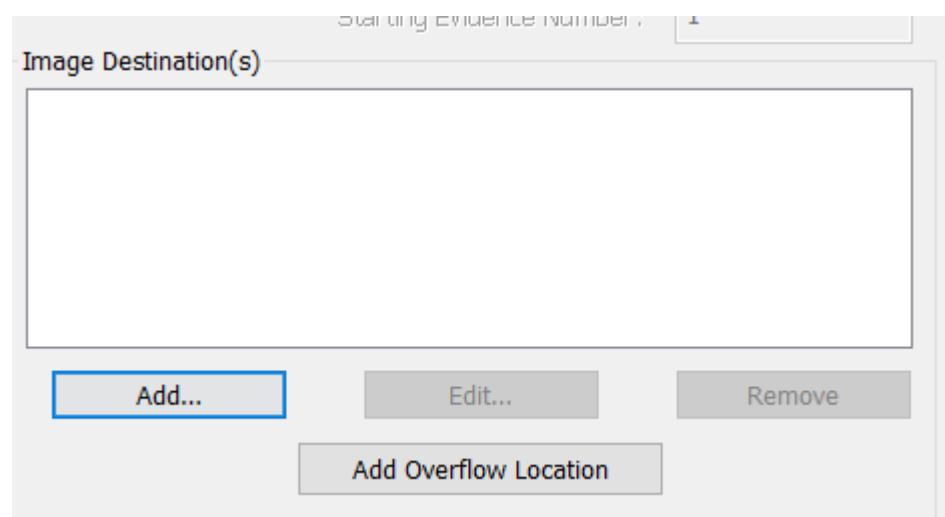
Thực hiện tạo ảnh đĩa



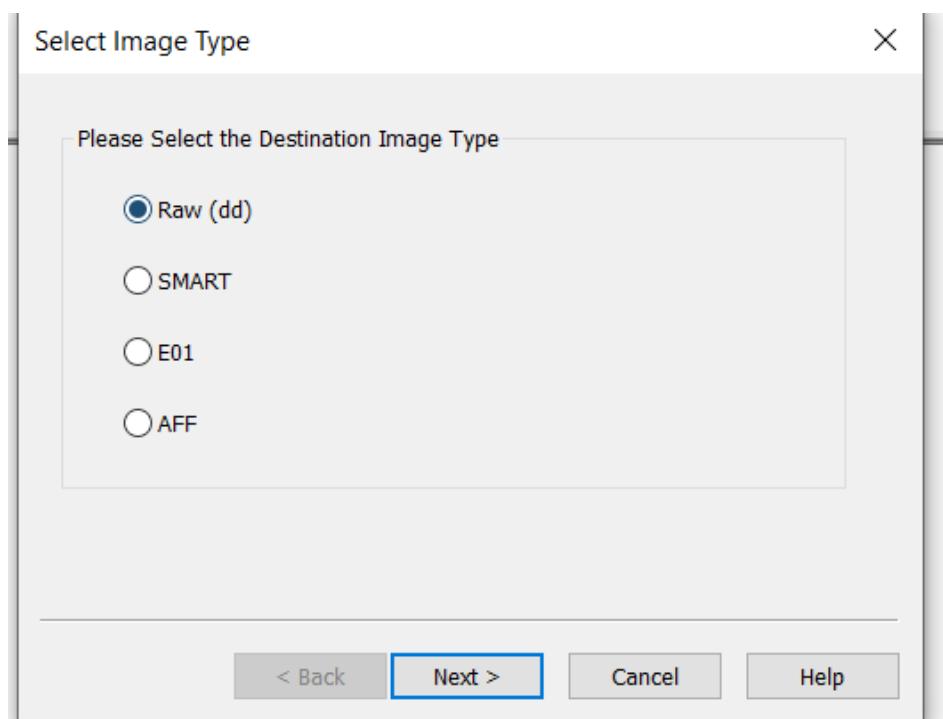
Chọn ổ đĩa cần dump



Chọn add và thêm các trường thông tin



Chọn dd Raw để dump

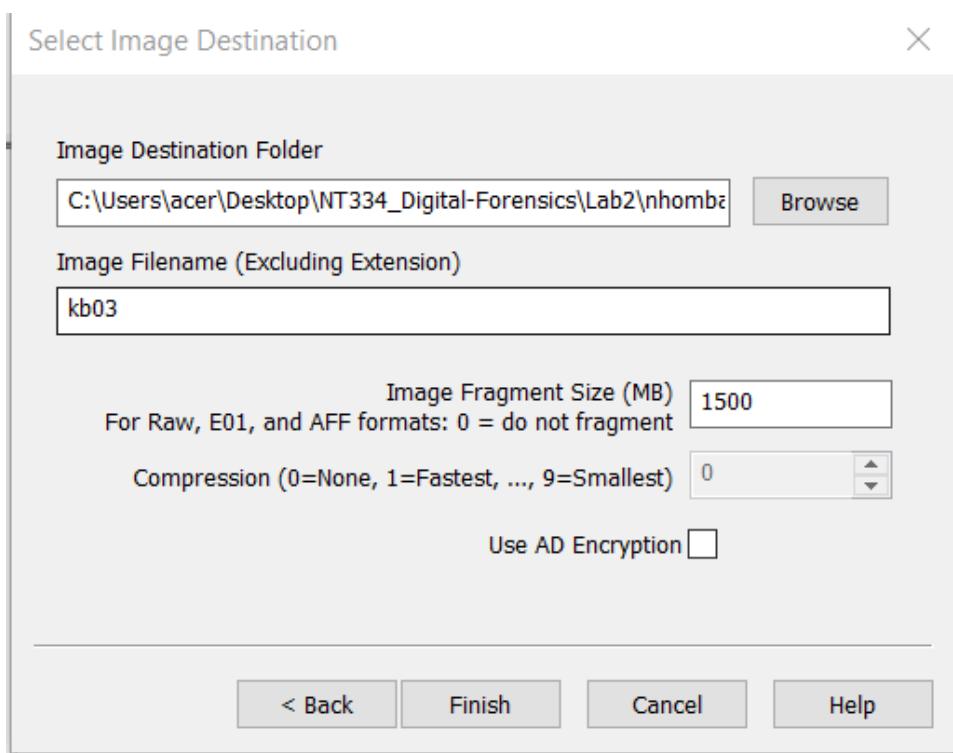


Thực hiện thêm các thông tin evidence

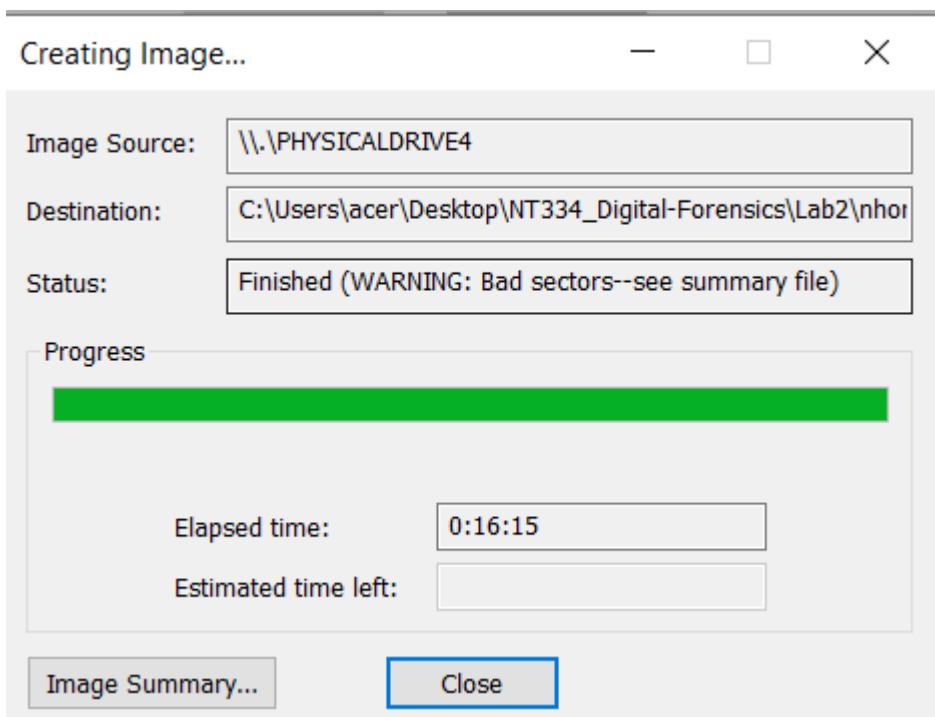
The dialog box is titled "Evidence Item Information" and contains fields for Case Number (April_0001), Evidence Number (01), Unique Description (Monkey Image), Examiner (nhombay), and Notes. The "Examiner" field has a blue border, indicating it is the active or selected field. At the bottom are buttons for "< Back", "Next >" (highlighted in blue), "Cancel", and "Help".

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

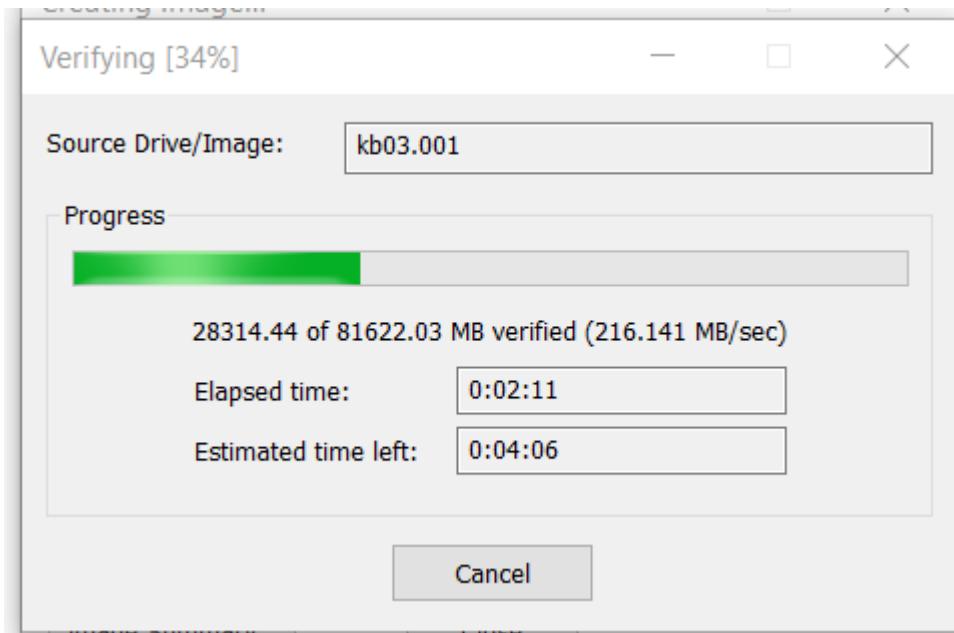
Chọn nơi lưu trữ



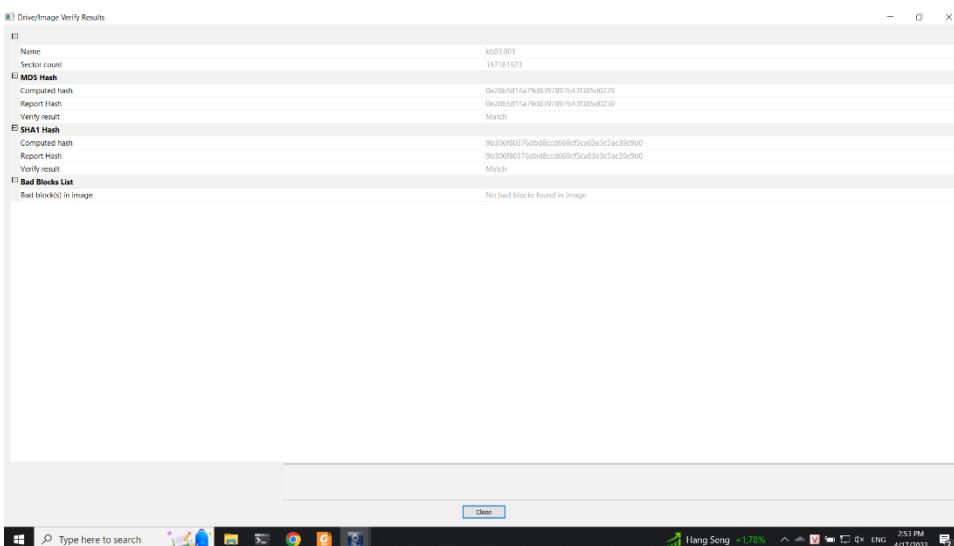
Thực hiện tạo image



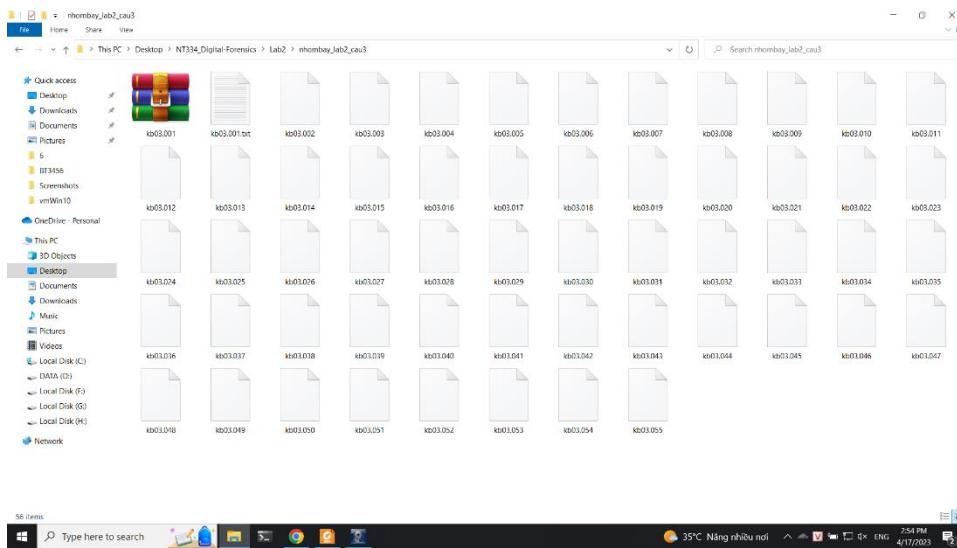
Thực hiện quá trình verify



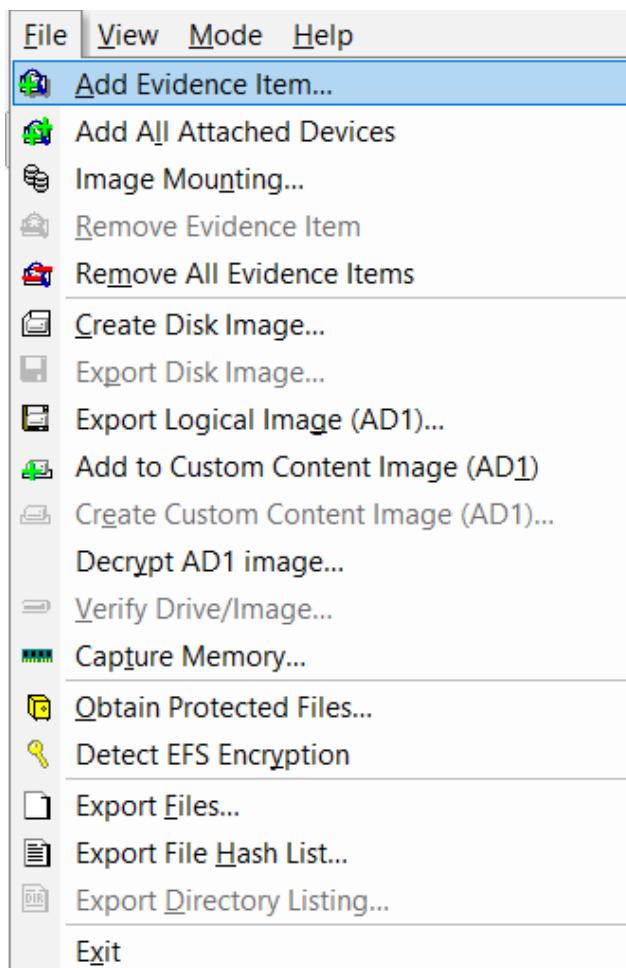
Thông báo hoàn thành quá trình



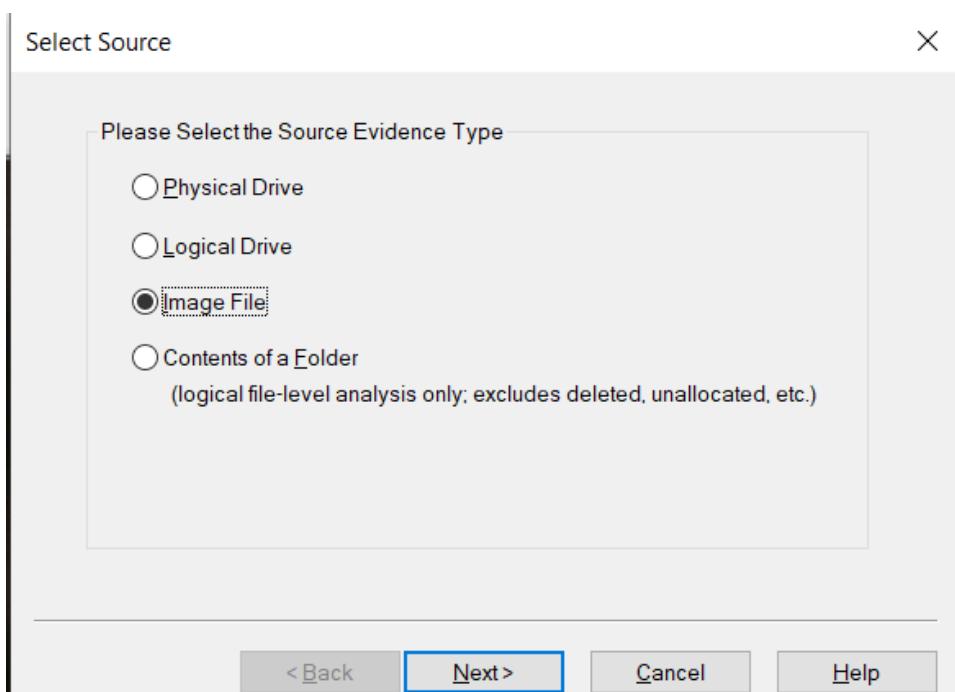
Thực hiện kiểm tra các evidence sau khi được dump



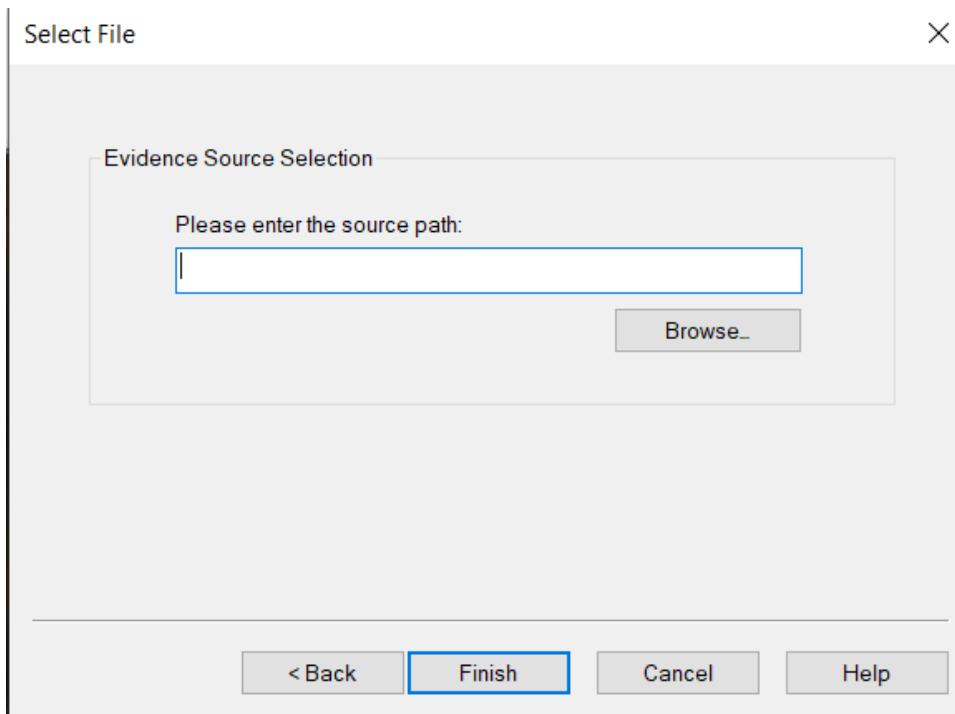
Tiếp tục thực hiện việc add evidence



Chọn image file

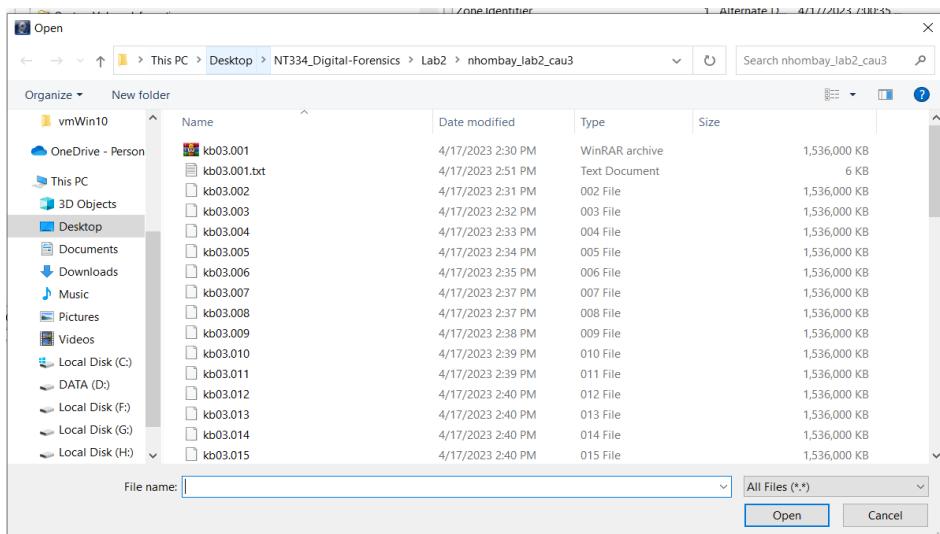


Chọn nơi lưu các evidence khi nãy

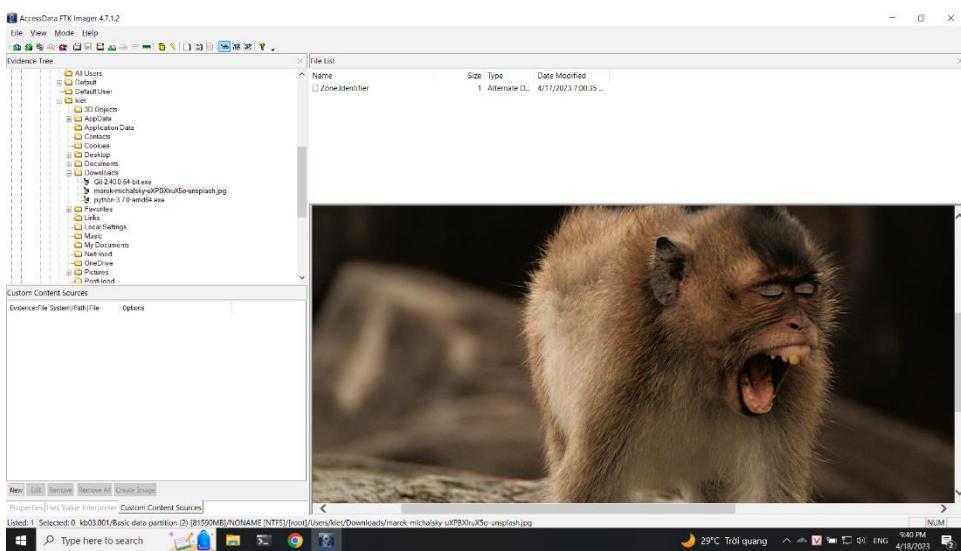


Thực hiện việc chọn kb03.001

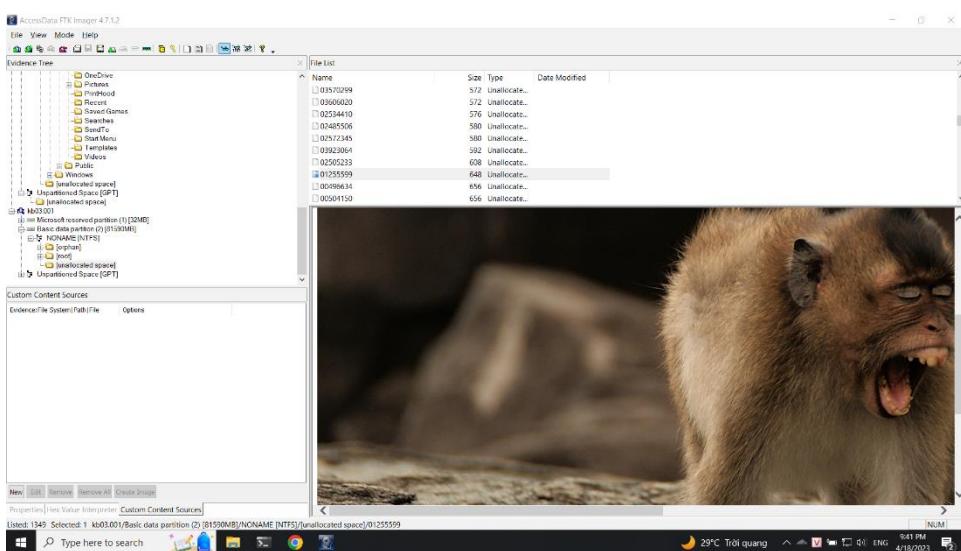
Hard Drive Forensics



Dump file từ located

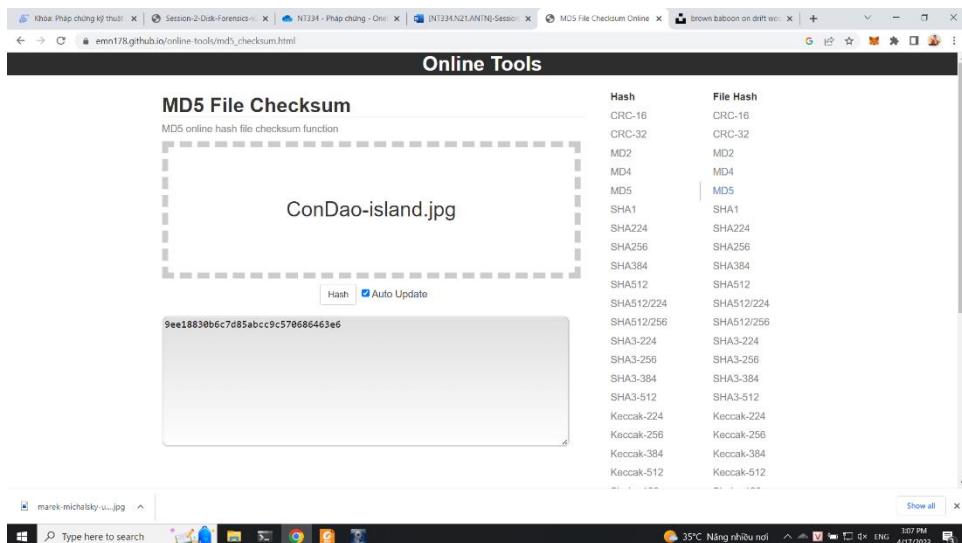


Dump file từ unlocated

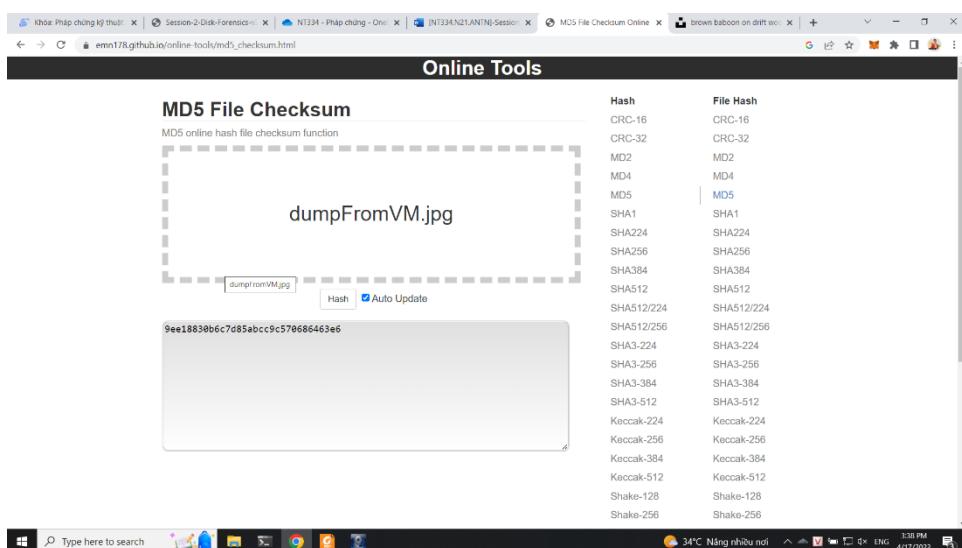


Thực hiện kiểm tra md5 hash

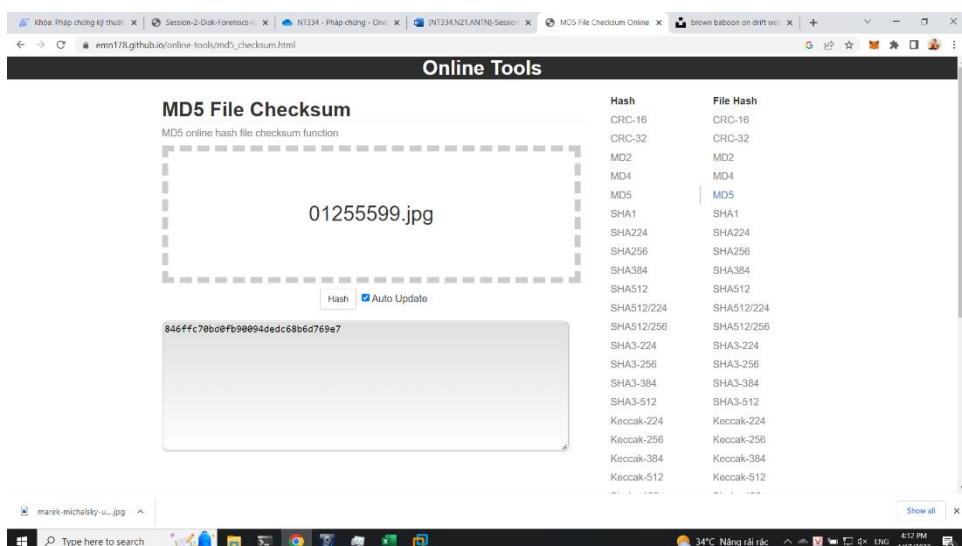
Hard Drive Forensics



Trích xuất từ vùng nhớ located



Trích xuất từ vùng nhớ unlocated

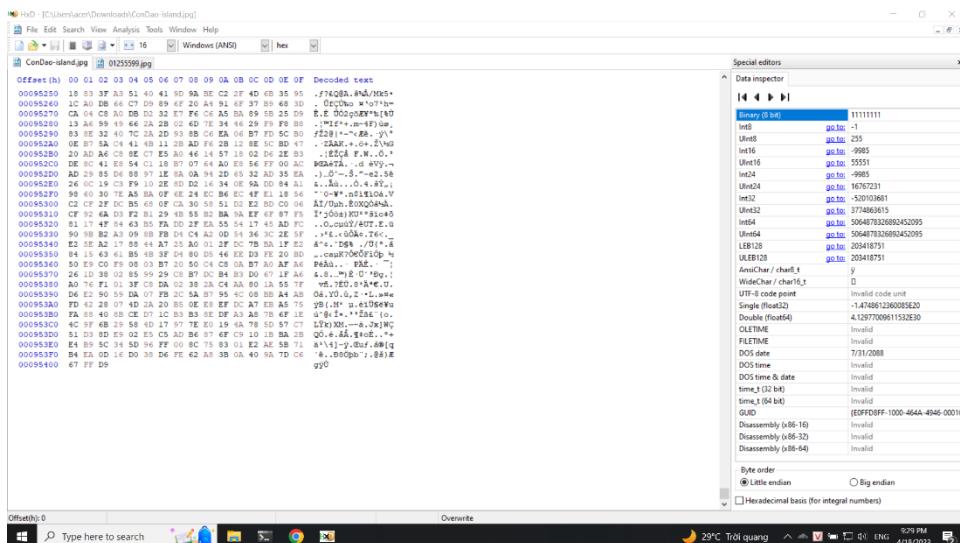


Xác nhận làm trong ngày

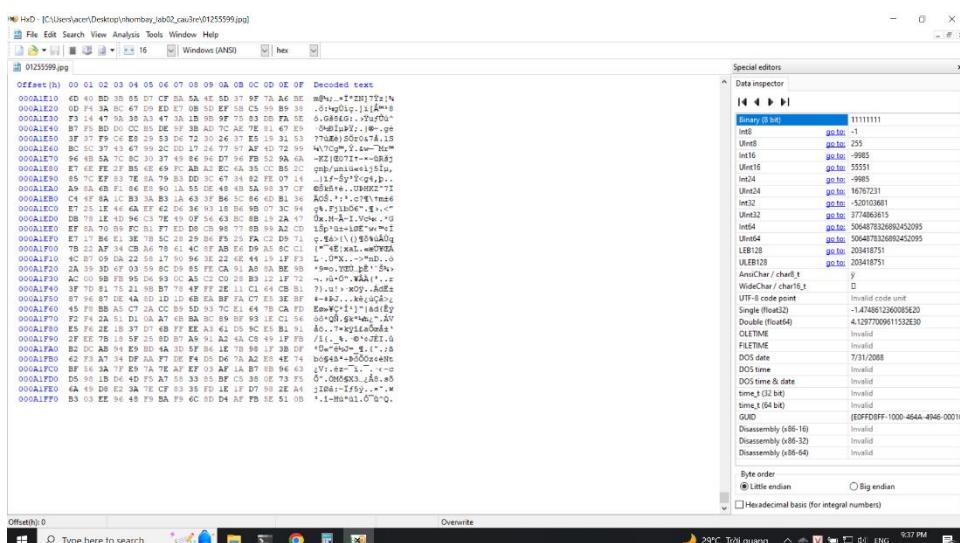
```
A new PowerShell stable release is available: v7.3.4
Upgrade now, or check out the release page at:
https://aka.ms/PowerShell-Release?tag=v7.3.4

PS C:\Users\acer\Desktop\nhombay_lab02_cau3re> dir | findstr "01255599.jpg"
-a--- 4/17/2023 3:59 PM 663552 01255599.jpg
PS C:\Users\acer\Desktop\nhombay_lab02_cau3re> date /t
Get-Date: Cannot bind parameter 'Date'. Cannot convert value "/t" to type "System.DateTime". Error: "String '/t' was not recognized as a valid DateTime."
PS C:\Users\acer\Desktop\nhombay_lab02_cau3re> echo nhombay
nhombay
PS C:\Users\acer\Desktop\nhombay_lab02_cau3re> |
```

Thực hiện kiểm tra file dump từ located



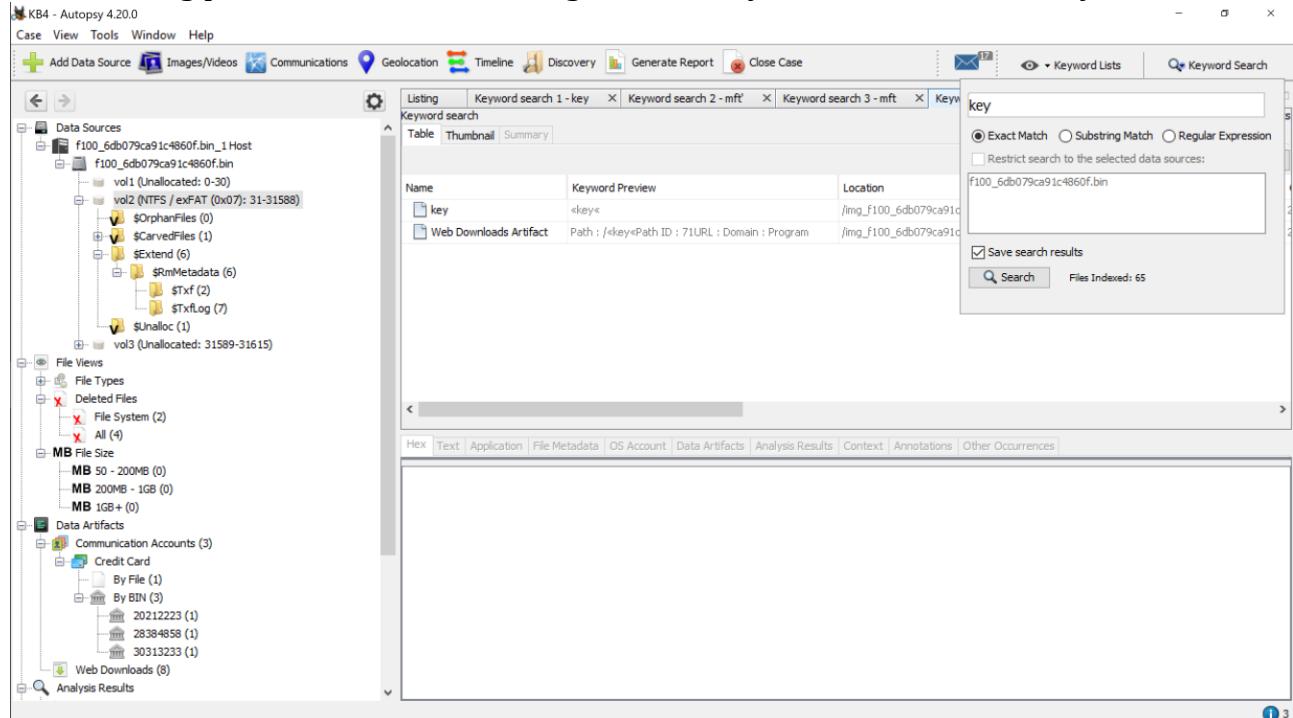
Thực hiện kiểm tra file dump từ unlocated thì ta thấy được có thêm padding lên đến 52208 byte trong đó có 49152 byte padding và 3056 byte null (\x00)



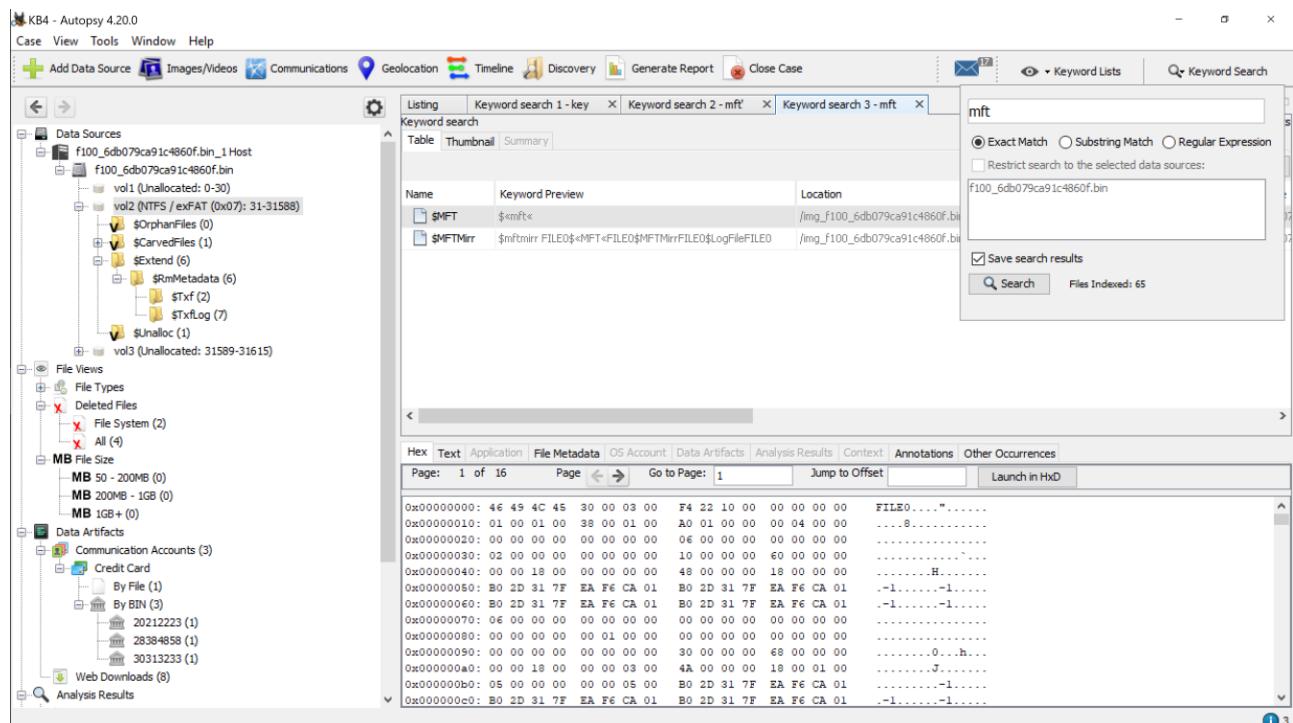
4. Kịch bản 4:

Sử dụng AutoSpy để kiểm tra file đ\Queue.

Trong phần Deleted Files, chúng em tìm thấy 2 files có từ khóa “key”:



Ngoài ra thì trong đề bài và khi thầy giảng cũng có nhắc đến file MFT, vậy nên em cũng thử tìm trong đây có file MFT không để kiểm tra thì tìm được 2 file bên dưới.



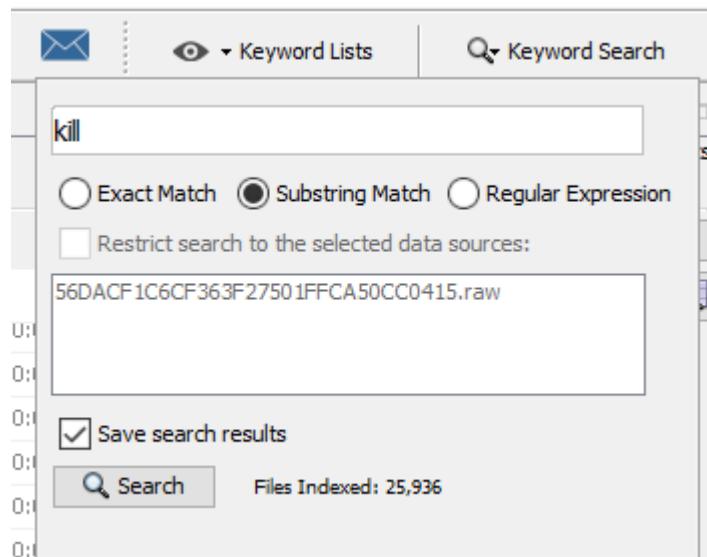
Trong file MFT có tìm được key:

Name	Keyword Preview	Location	Modified Time	Change Time
\$MFT	\$MFT	/img_f100_6db079ca91c4860f.bin/vol_vol2/\$MFT	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT
\$MFTMirr	\$MFTMirr	/img_f100_6db079ca91c4860f.bin/vol_vol2/\$MFTMirr	2010-05-19 07:30:35 ICT	2010-05-19 07:30:35 ICT

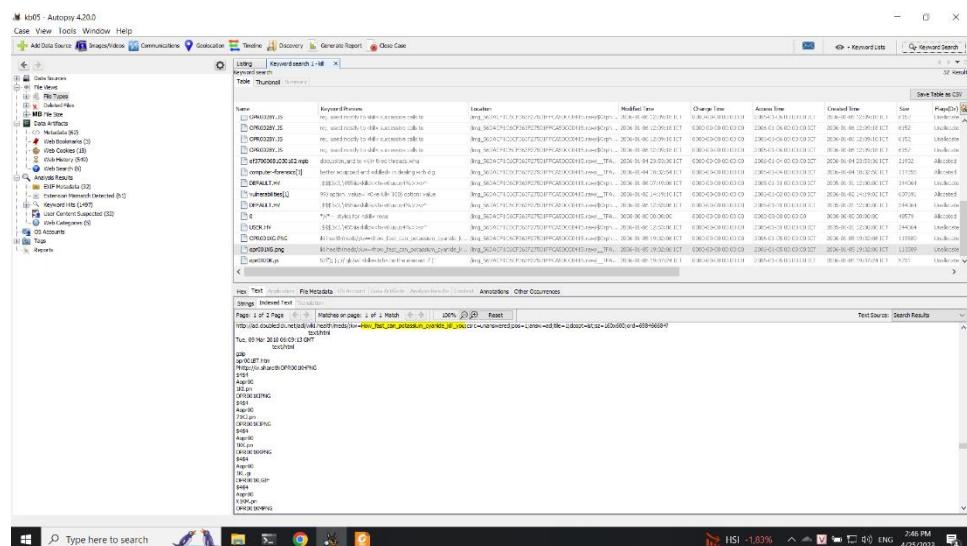
5. Kịch bản 5:

Đầu tiên ta sẽ giải nén file và có được file dump, mở bằng auto spy

Tiếp tục tìm kiếm với từ khoá kill

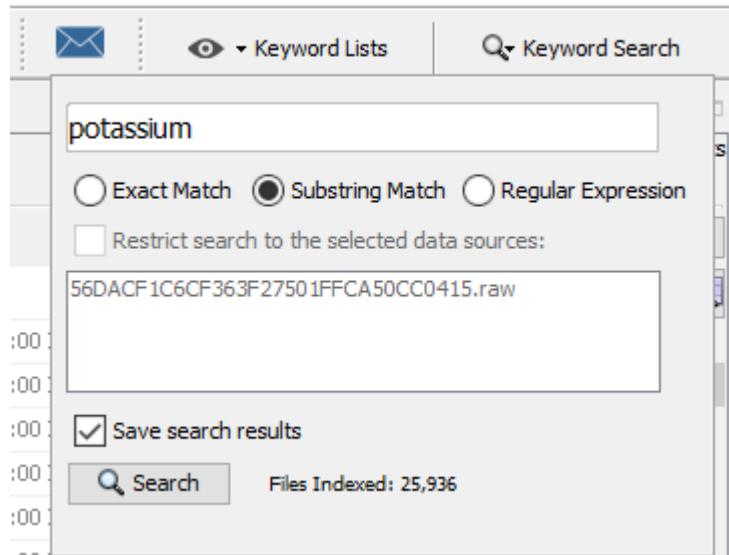


Ta thấy được thông tin là [How_fast_can_potassium_cyanide_kill_you](#)

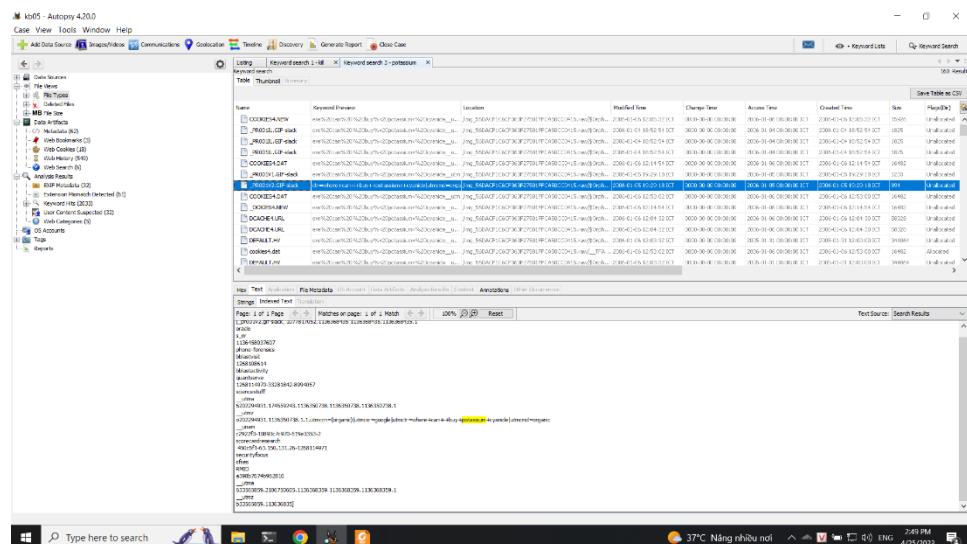


Có lẽ như người dùng này dự kiến kết liễu bản thân bằng potassium cyanide (Kali cyanide)

Tiếp tục tìm kiếm thông tin với potassium



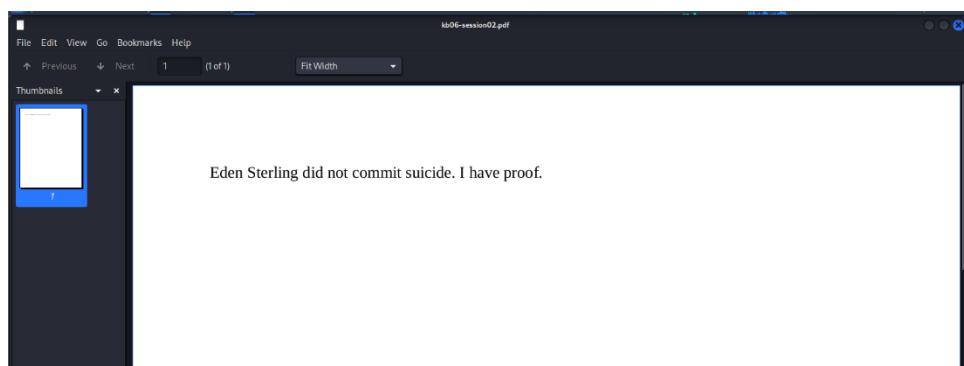
Ta thấy được thông tin người này đang tìm mua potassium cyanide với thông tin
where+can+i+buy+potassium+cyanide



Vậy có thể thấy ông này muốn tư tử bằng potassium cyanide

6. Kích bản 6:

Vào file pdf để xem thông tin thì ta chỉ thấy có thông tin như vậy



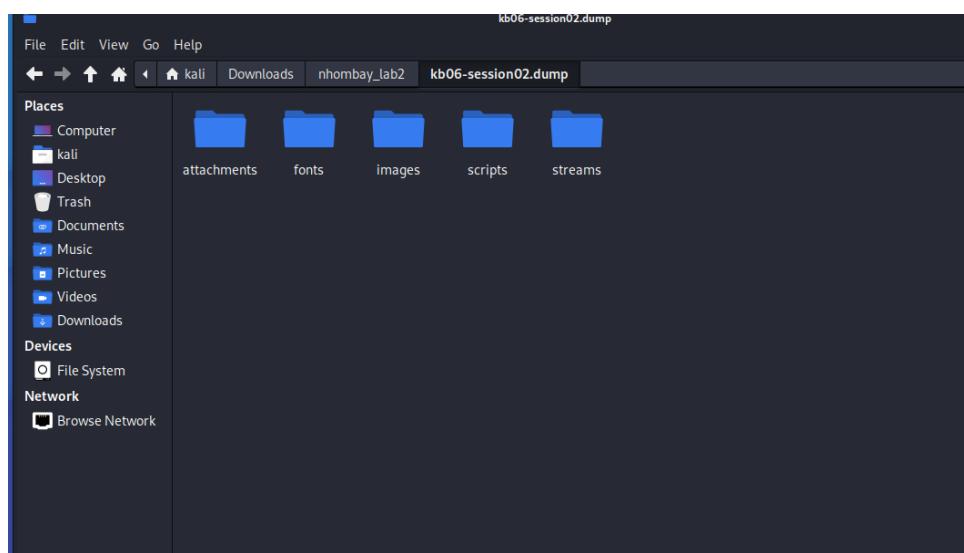
Sử dụng tool binwalk để xem thông tin bên trong

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	0x265807C	xz compressed data
40249502	0x266289E	xz compressed data
40329277	0x267603D	xz compressed data
40375259	0x26813DB	xz compressed data
40416593	0x268B551	xz compressed data
40503101	0x26A073D	xz compressed data
40518625	0x26A43E1	xz compressed data
40559387	0x26AE31B	xz compressed data
40643923	0x26C2D53	xz compressed data
40687748	0x26CD884	xz compressed data
40729959	0x26D7D67	xz compressed data
40817626	0x26ED3DA	xz compressed data
40834367	0x26F153F	xz compressed data
40875601	0x26FB651	xz compressed data

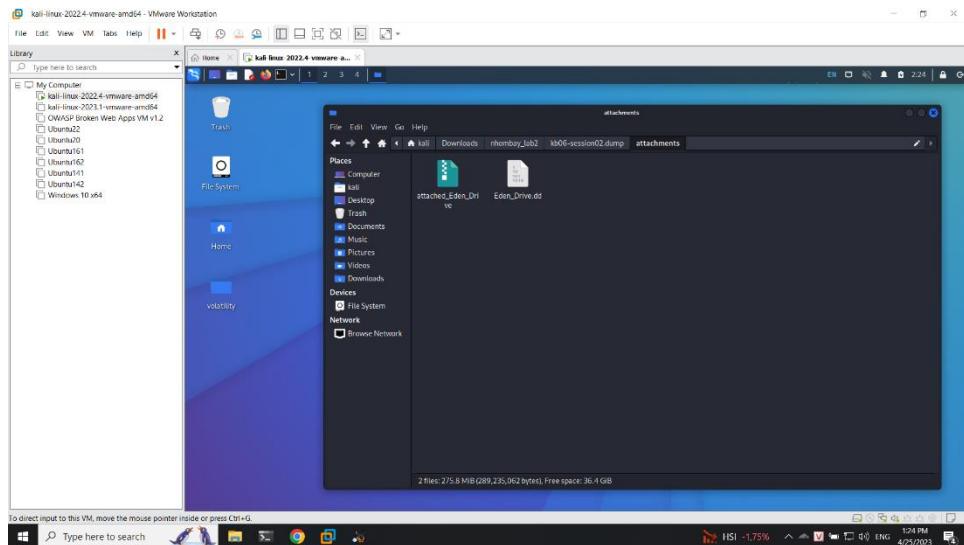
Sau khi thấy được có file nén ta sẽ sử dụng extractpdf để xem thông tin

Sử dụng lệnh

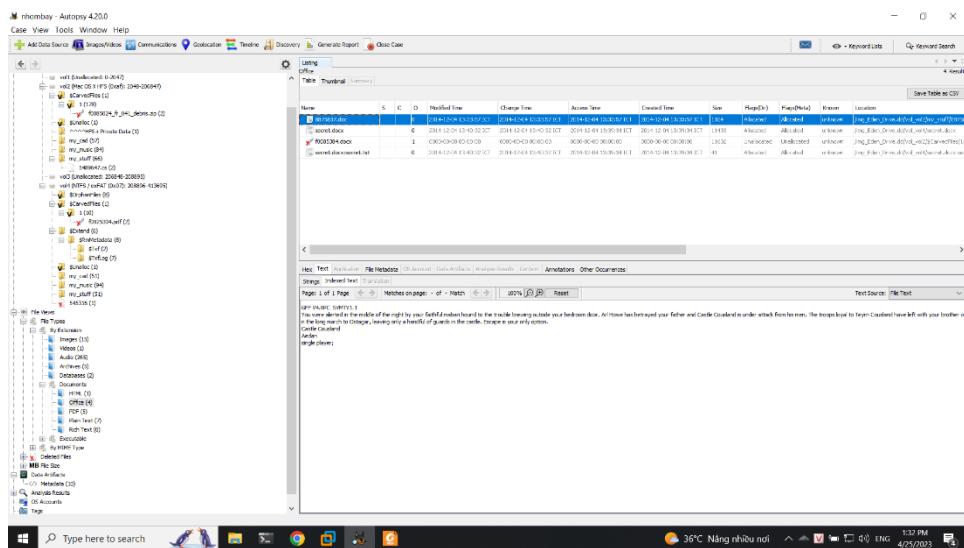
\$ extractpdf kb06-session02.pdf



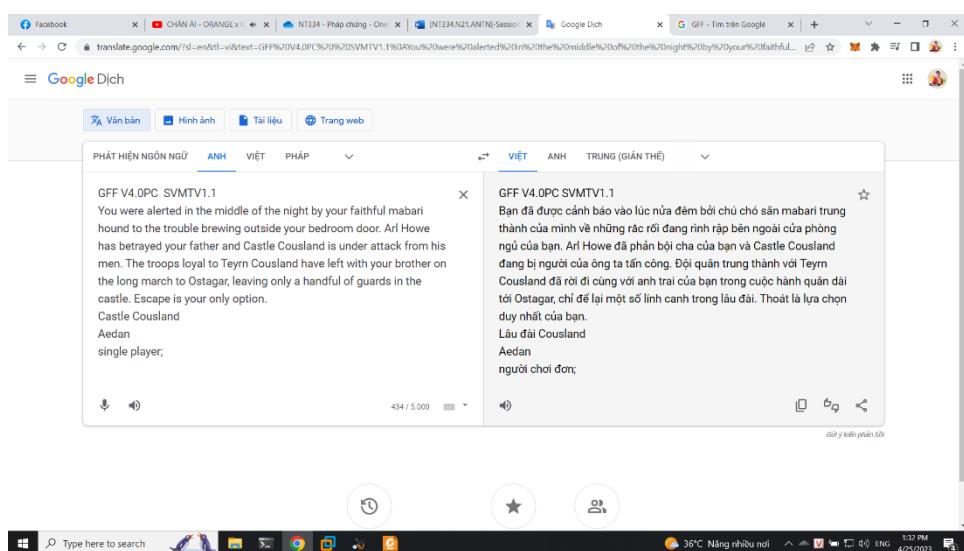
Tiếp tục giải nén file nén trong attachment thì ta có được file dd



Tiếp tục mở và phân tích bằng auto spy ta có được các file chứa thông tin

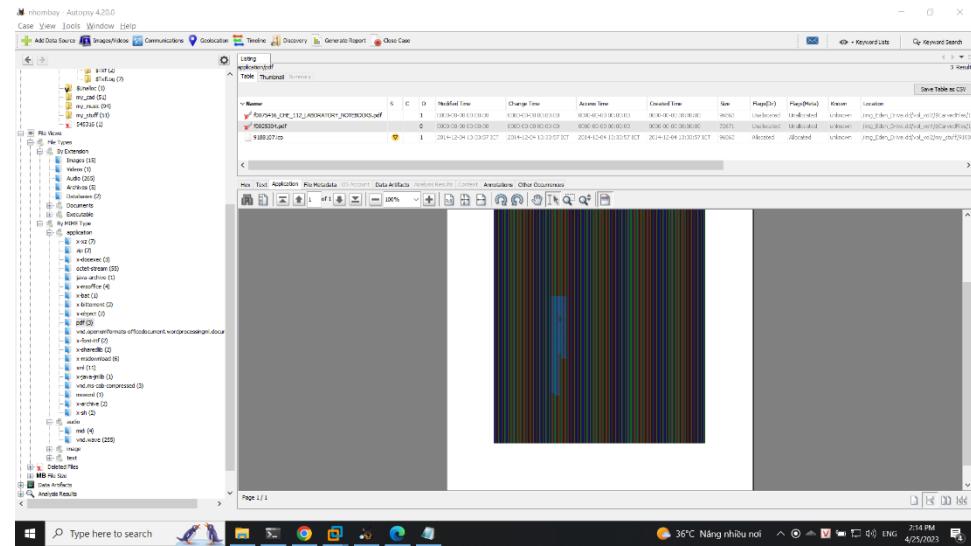


Trong đó có một mail khá lạ



Có thể thấy được thông tin người gửi nặc danh với cái tên Aedan, tên Teyrn Cousland có thể là trưởng điều tra pháp y

Ngoài ra trong hình này



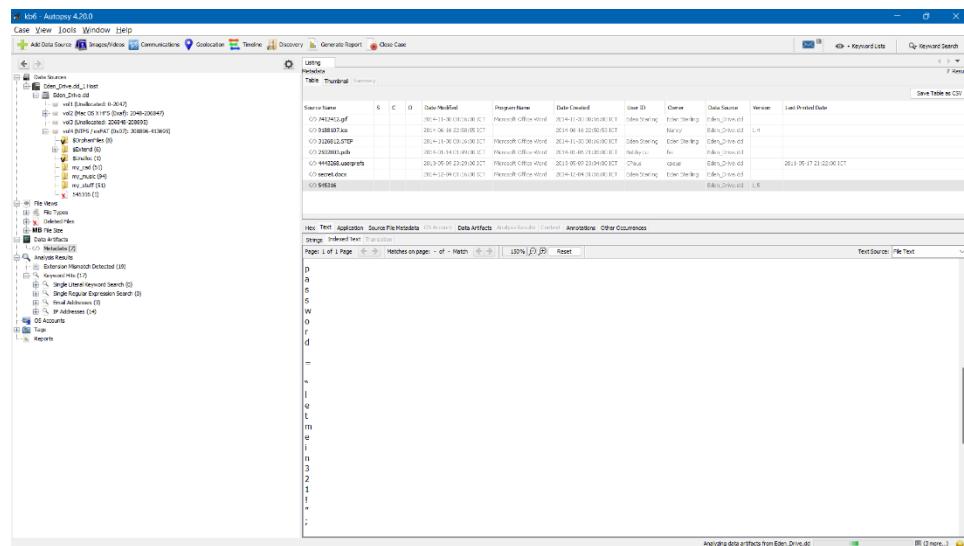
Ta trích lục được thông tin

Username:stringsinCsharp

WĂEE||ŽaĚĘĘdšŶŐĘĐĂEE||ŽaĚĘĘcĘūGłwŶtřę

Có thể đây là thông tin username và password, nhưng phần password ta giải mã được một phần

<char>s-r---<char>-password<char>-<char>-----



Ngoài ra ở một file khác ta có được password là letmein321!

Hard Drive Forensics

The screenshots show the Autopsy 4.20.0 forensic tool interface. Both windows have the title 'Autopsy 4.20.0' and are set to 'Case' mode.

Screenshot 1 (Top): This window shows the analysis results for the drive 'E:\'. The left sidebar lists various data sources such as 'Data Sources', 'File Types', 'Keywords', 'Reports', and 'Logs'. The main pane displays a table of files found on the drive, including their name, size, type, modified time, change time, access time, creation time, owner, file path, file media, known status, and location. A search bar at the top right allows for keyword searching. Below the table, there are tabs for 'Hex', 'Text', 'File Metadata', 'File Hashes', 'Data Analysis', 'Analysis Results', and 'Annotations'. A message in the text area says: 'I think someone may be after me. -Edwin'.

Screenshot 2 (Bottom): This window shows the analysis results for the drive 'F:\'. The left sidebar is similar to the first. The main pane displays a table of files found on the drive, with a single entry: 'Notes.txt'. The file details are: Name: Notes.txt, Size: 0, Type: Text, Modified Time: 2014-12-04 10:00:00, Change Time: 2014-12-04 10:00:00, Access Time: 2014-12-04 10:00:00, Creation Time: 2014-12-04 10:00:00, Owner: NT AUTHORITY\SYSTEM, File Path: F:\Notes.txt, File Media: Allocated, Known: Unknown, Location: F:\Notes.txt. Below the table, there are tabs for 'Hex', 'Text', 'File Metadata', 'File Hashes', 'Data Analysis', 'Analysis Results', and 'Annotations'. A message in the text area says: 'Password is in the other partition in case I forget.'

Lưu ý: Chỉ ghi Kịch bản thực hành được GVTH chỉ định phải làm báo cáo

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

(Xem trang kế tiếp)

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13**. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

Ví dụ: [NT101.H11.1]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

HẾT