UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI

Information and Communication Technology Department

Lab Work Day 4

Digital Forensic

Name - ID: Đào Ngọc Tùng BA12-185

Trần Đức Trung BA12-179

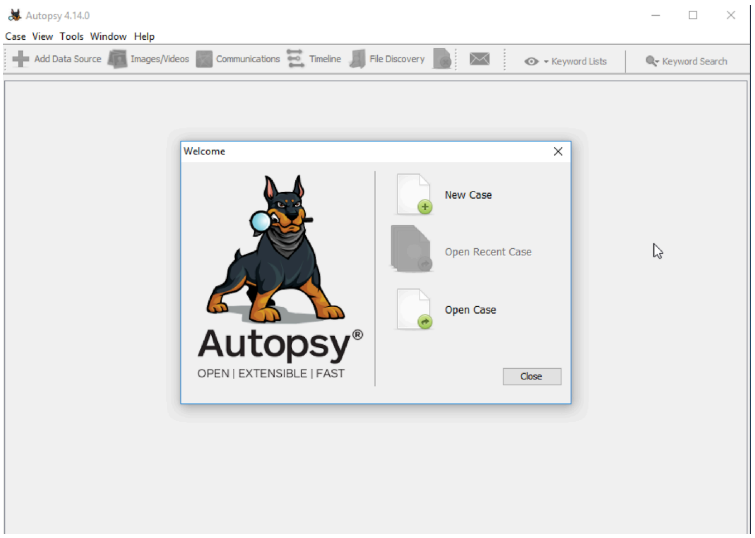
Phạm Phú Hưng BA12-081

Nguyễn Tiến Ngọc BA12-140

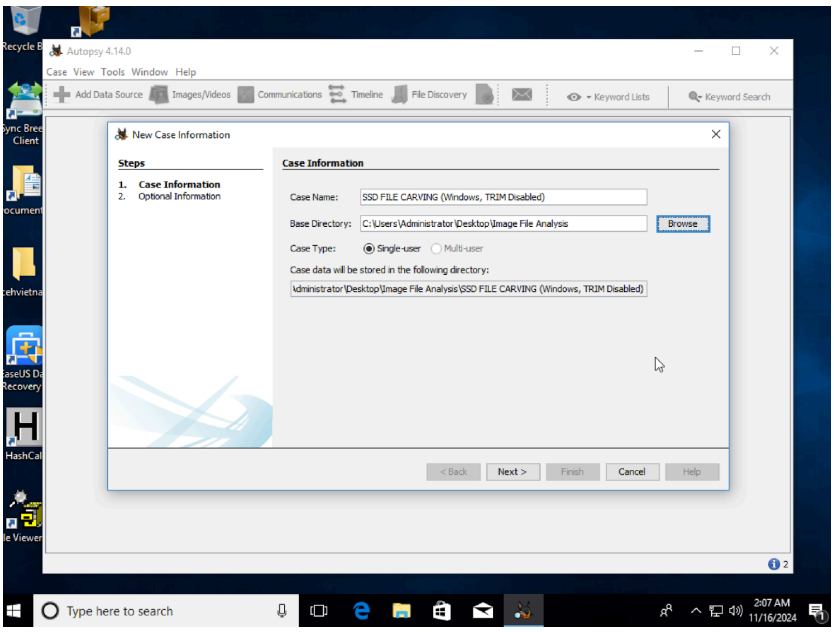
Ha Noi, 06 November 2024

Lab 1:

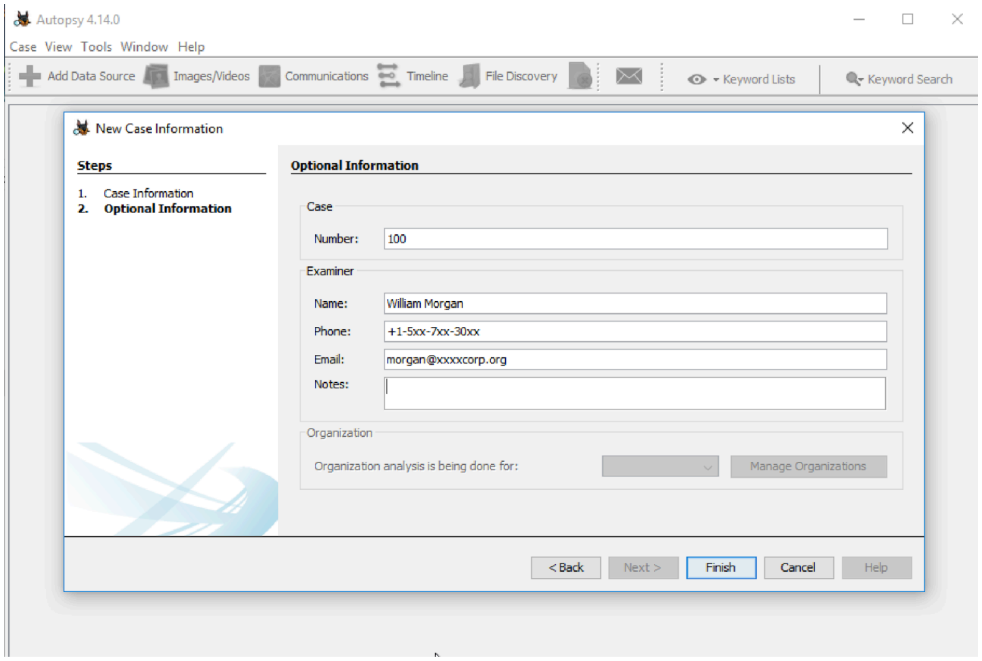
Step 1: Open Psy



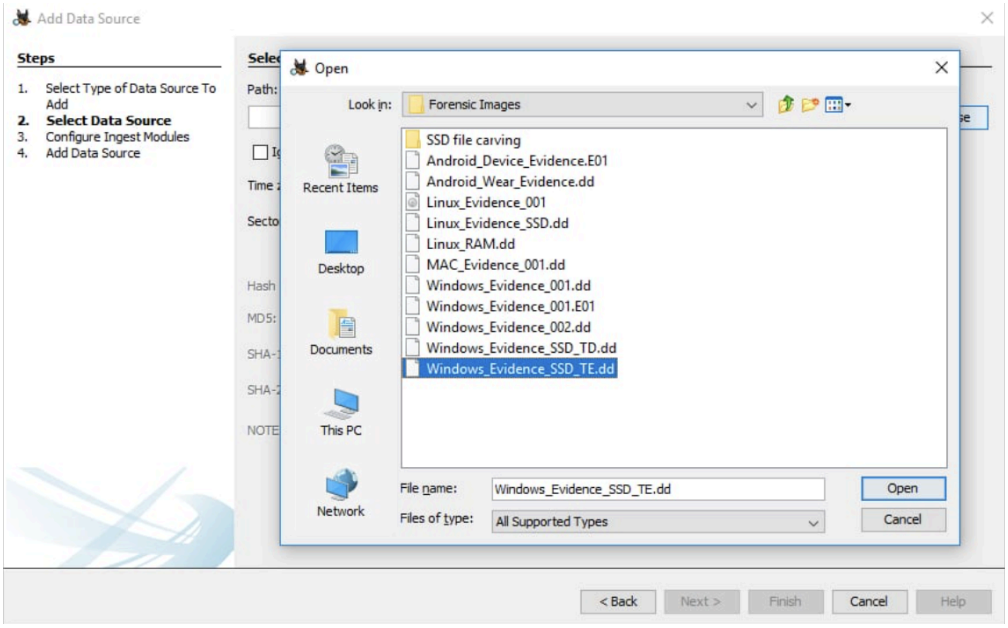
Step 2: Create a new case whose case name is SSD FILE CARVING (Windows, TRIM Disabled). After that, we will save the case data in the image file analysis folder located on Desktop.



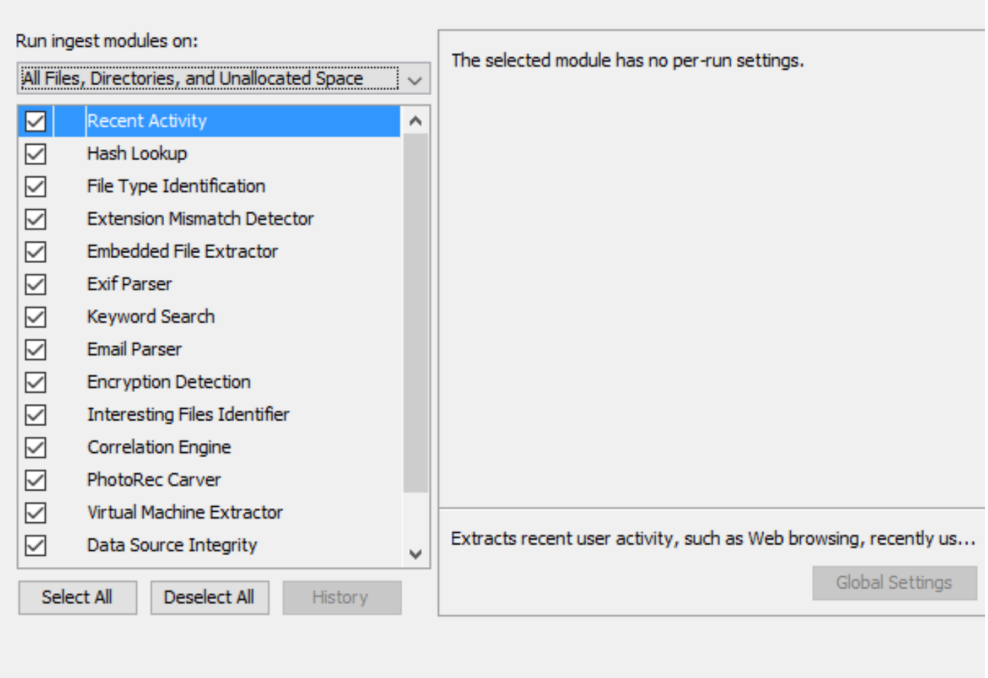
Step 3: Setup optional information



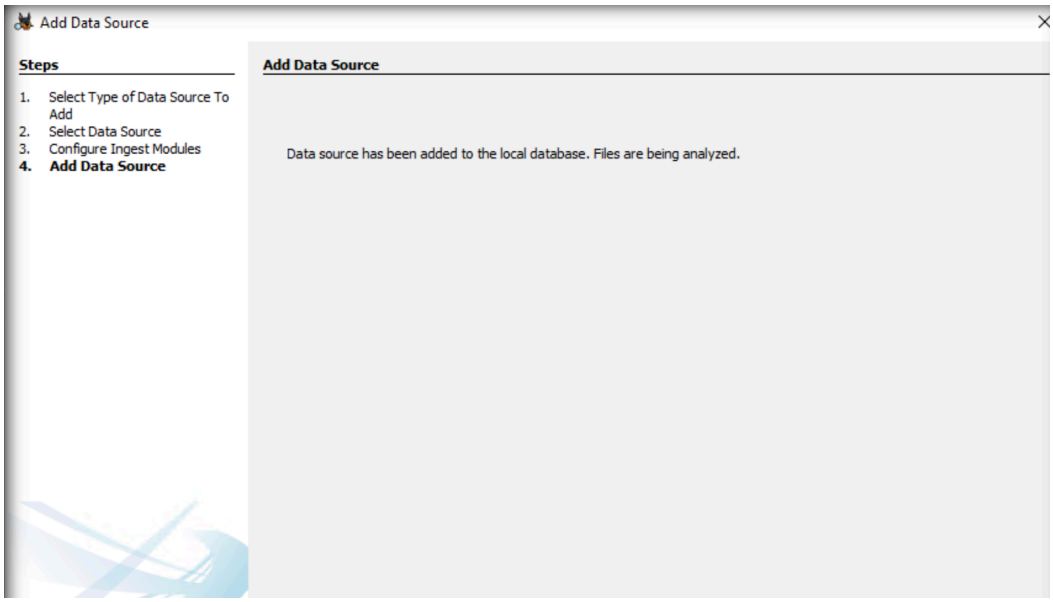
Step 4: Open folder C:\CHFI-Tools\Evidence Files\Forensics Images. We choose the file Windows_Evidence_SSD_TD.dd



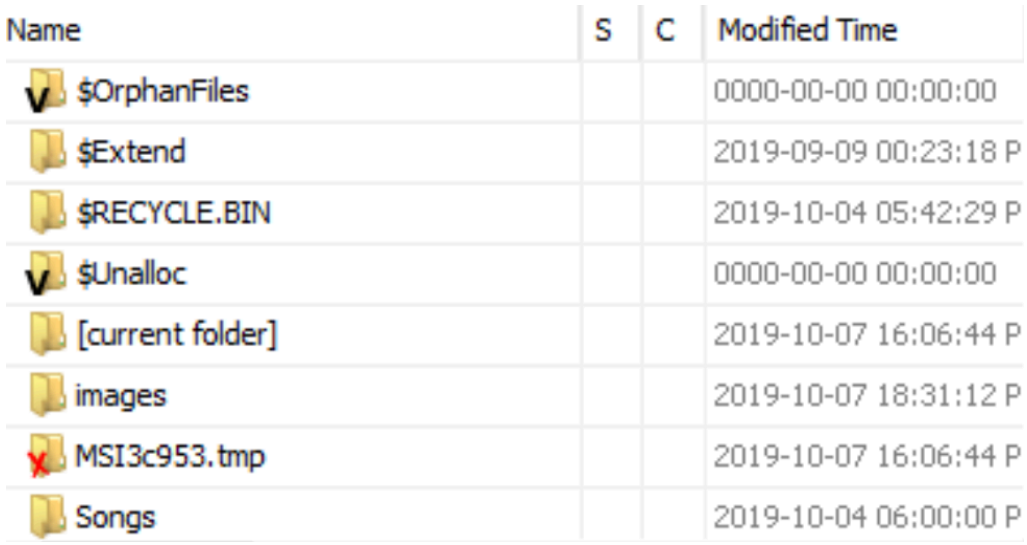
Step 5: Configure ingest module



Step 6: Add data source

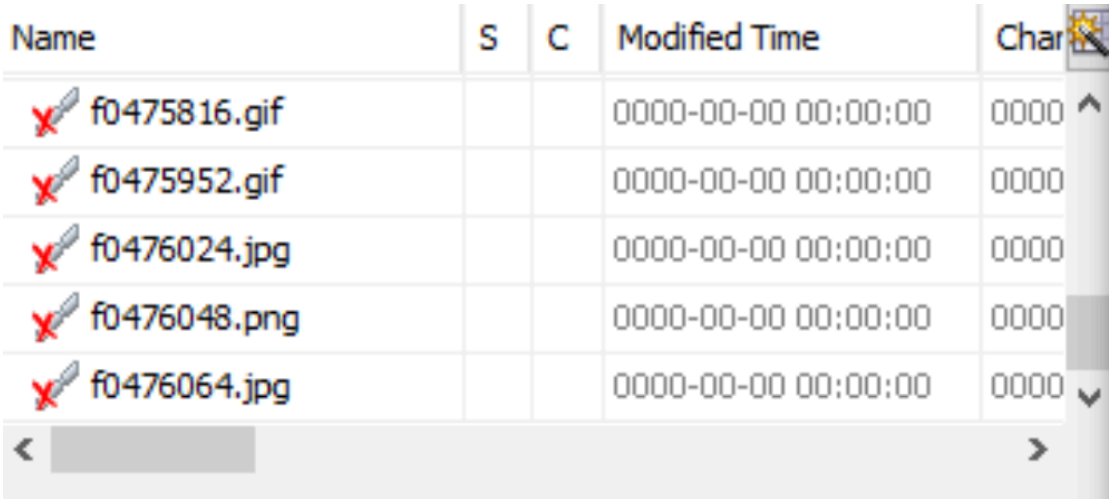


Step 7: Click the image Windows_Evidence_SSD_TD.dd to view the folders that store data related to files, processes, services, tools,...



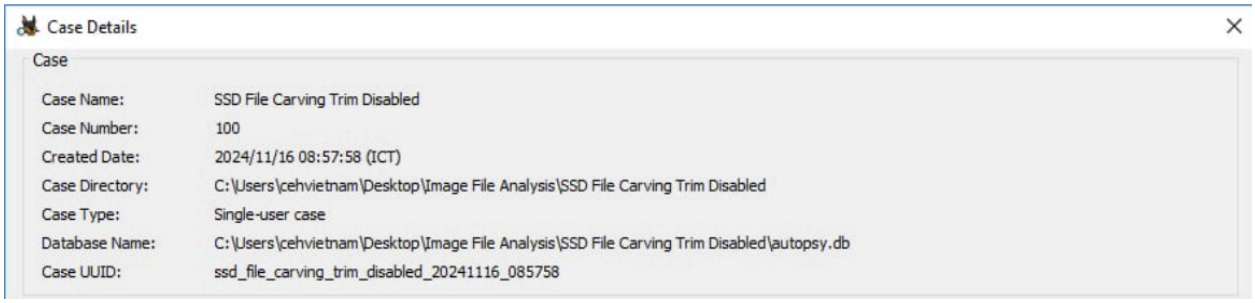
Name	S	C	Modified Time
$OrphanFiles			0000-00-00 00:00:00
$Extend			2019-09-09 00:23:18 P
$RECYCLE.BIN			2019-10-04 05:42:29 P
$Unalloc			0000-00-00 00:00:00
[current folder]			2019-10-07 16:06:44 P
images			2019-10-07 18:31:12 P
MSI3c953.tmp			2019-10-07 16:06:44 P
Songs			2019-10-04 06:00:00 P

Step 8: Choose CarvedFiles and select f0475952.gif and extract file and save Export folder. This folder is the sub-folder that exists within the case folder created in the Image File Analysis folder on the Desktop



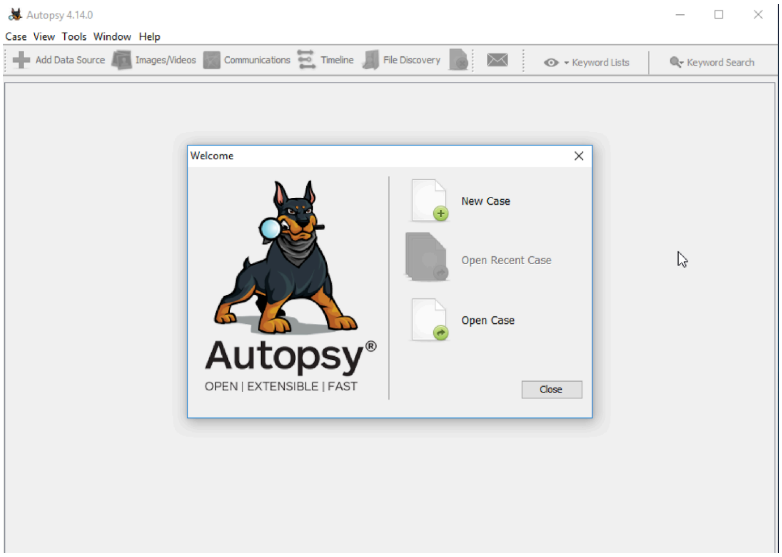
Name	S	C	Modified Time	Char
f0475816.gif			0000-00-00 00:00:00	0000
f0475952.gif			0000-00-00 00:00:00	0000
f0476024.jpg			0000-00-00 00:00:00	0000
f0476048.png			0000-00-00 00:00:00	0000
f0476064.jpg			0000-00-00 00:00:00	0000

Step 9: Navigation to the location where the carved image file has been saved. We can retrieve and view the file's content because it was taken from the disk when TRIM was disabled on it.

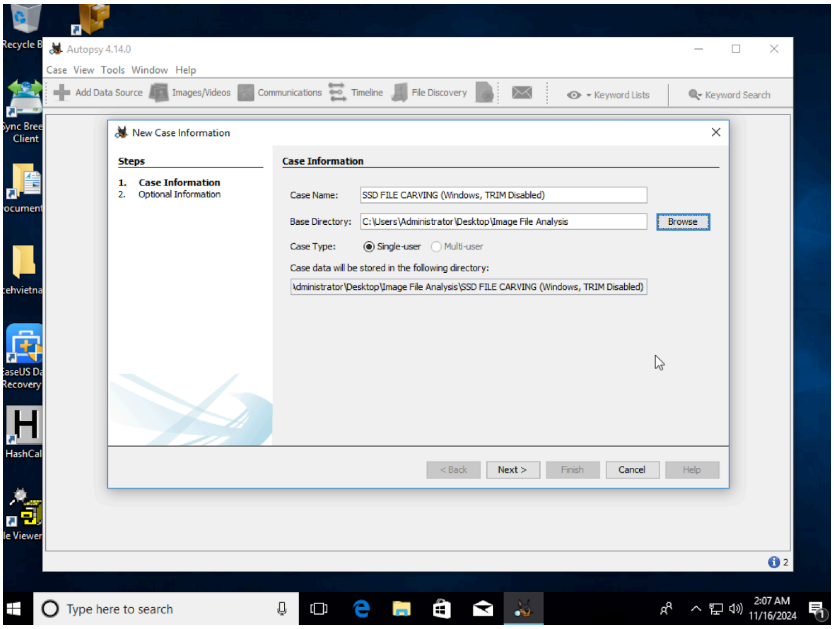


Lab 2:

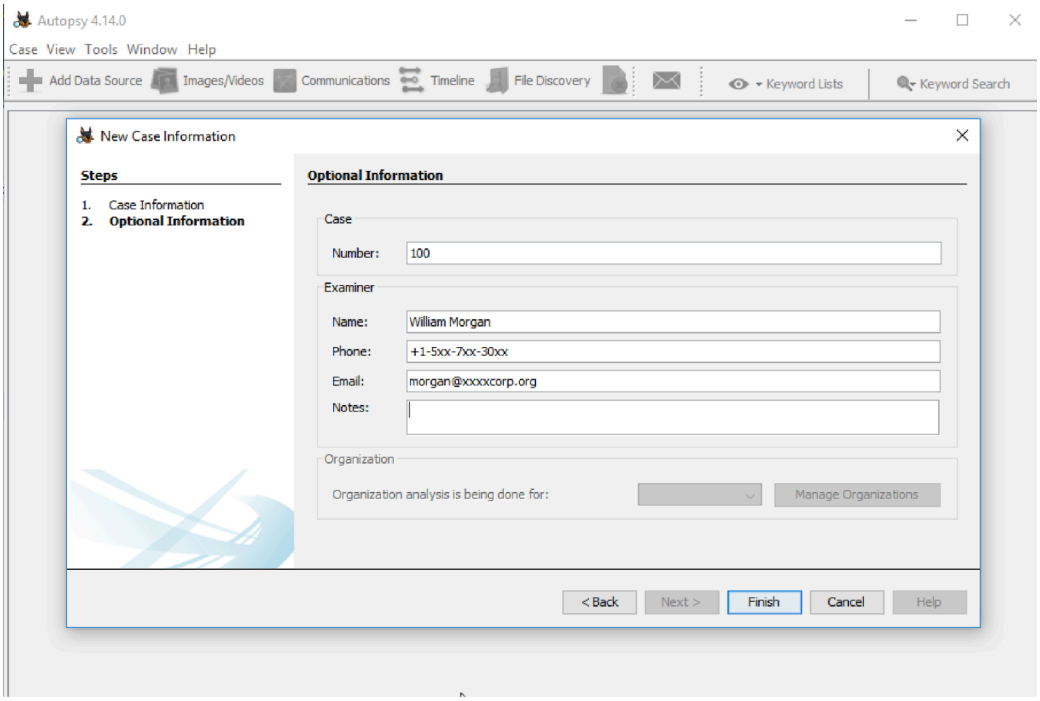
Step 1: Open Psy



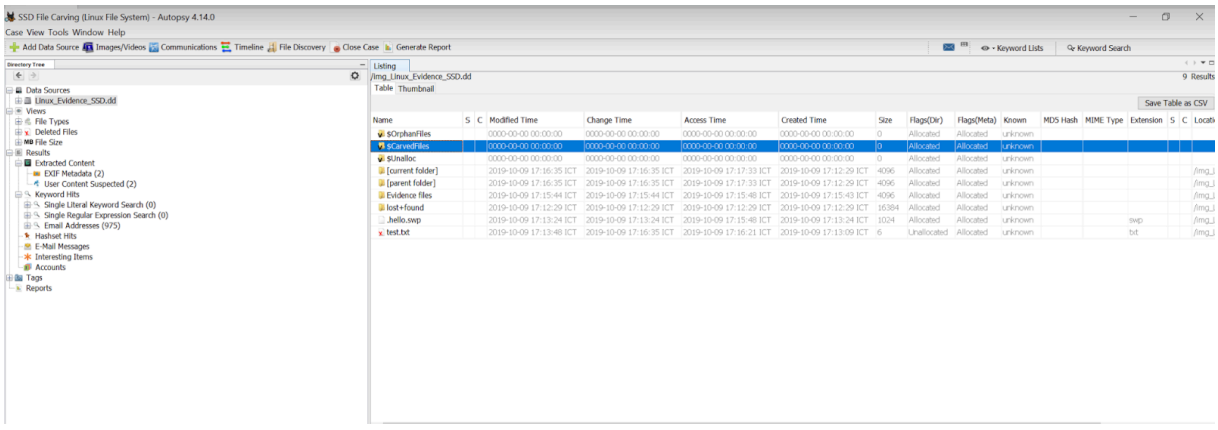
Step 2: Create a new case whose case name is SSD FILE CARVING (Windows, TRIM Disabled). After that, we will save the case data in the image file analysis folder located on Desktop



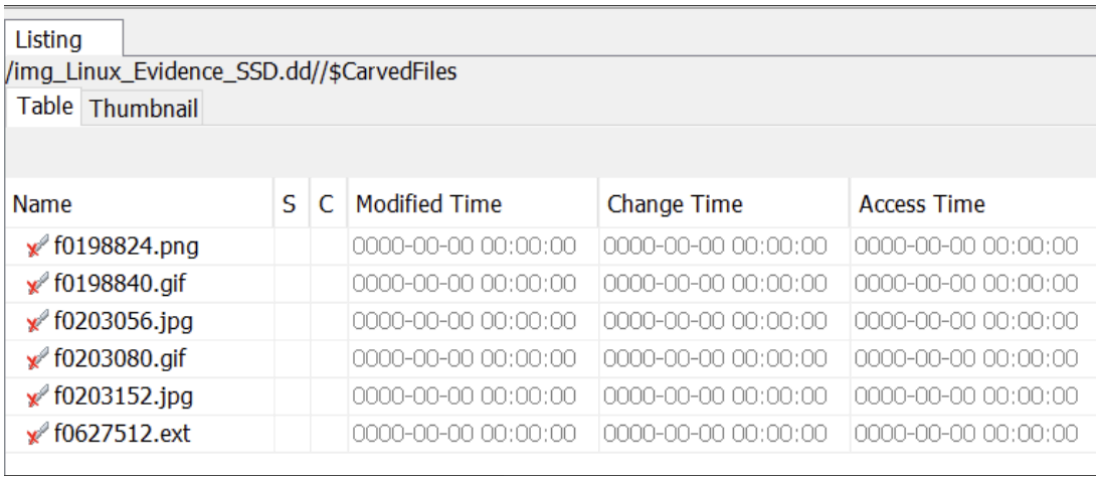
Step 3: Setup optional information



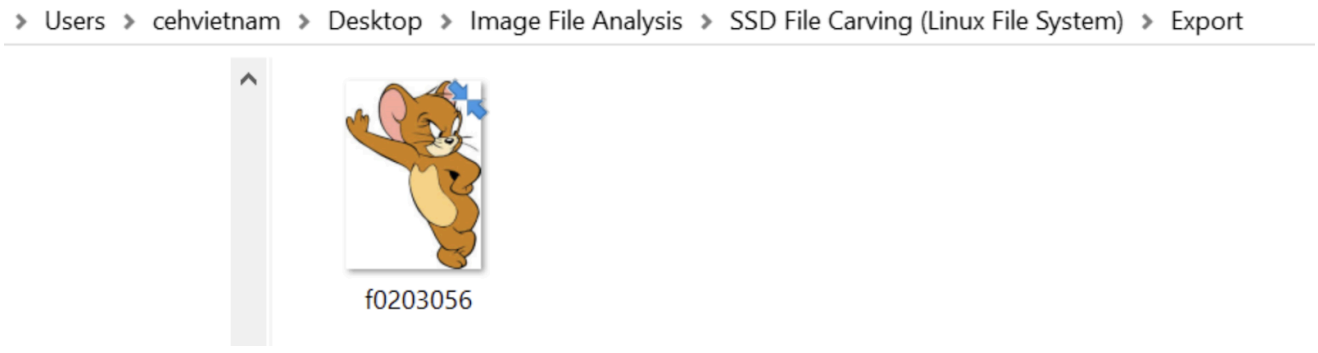
Step 4: Click the image Linux_Evidence_SSD_TD.dd to view the folders that store data related to files, processes, services, tools,...



Step 5: Choose CarvedFiles and select f0203056.gpg and extract file and save Export folder. This folder is the sub-folder that exists within the case folder created in the Image File Analysis folder on the Desktop

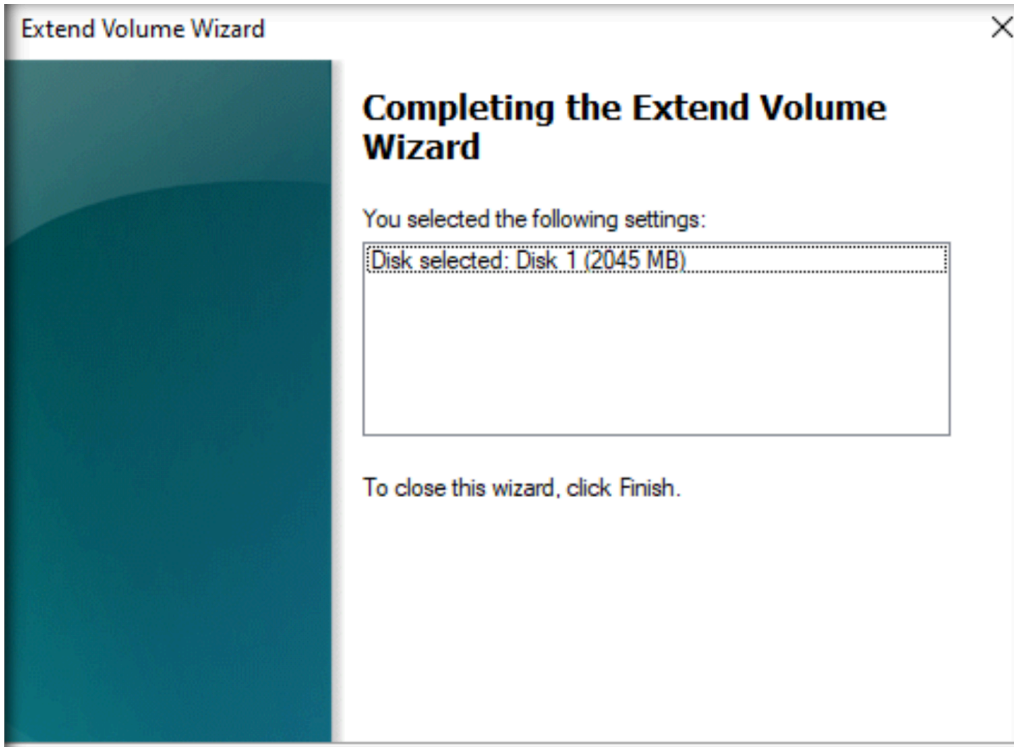


Step 6: Navigation to the location where the carved image file has been saved. We can retrieve and view the file's content because it was taken from the disk when TRIM was disabled on it.

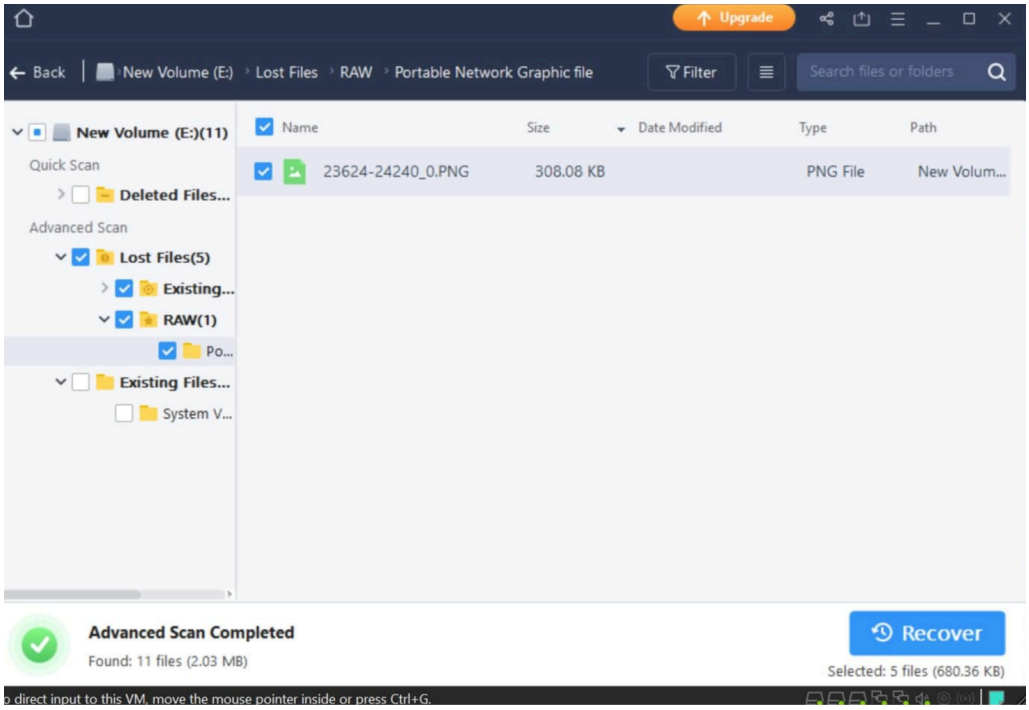


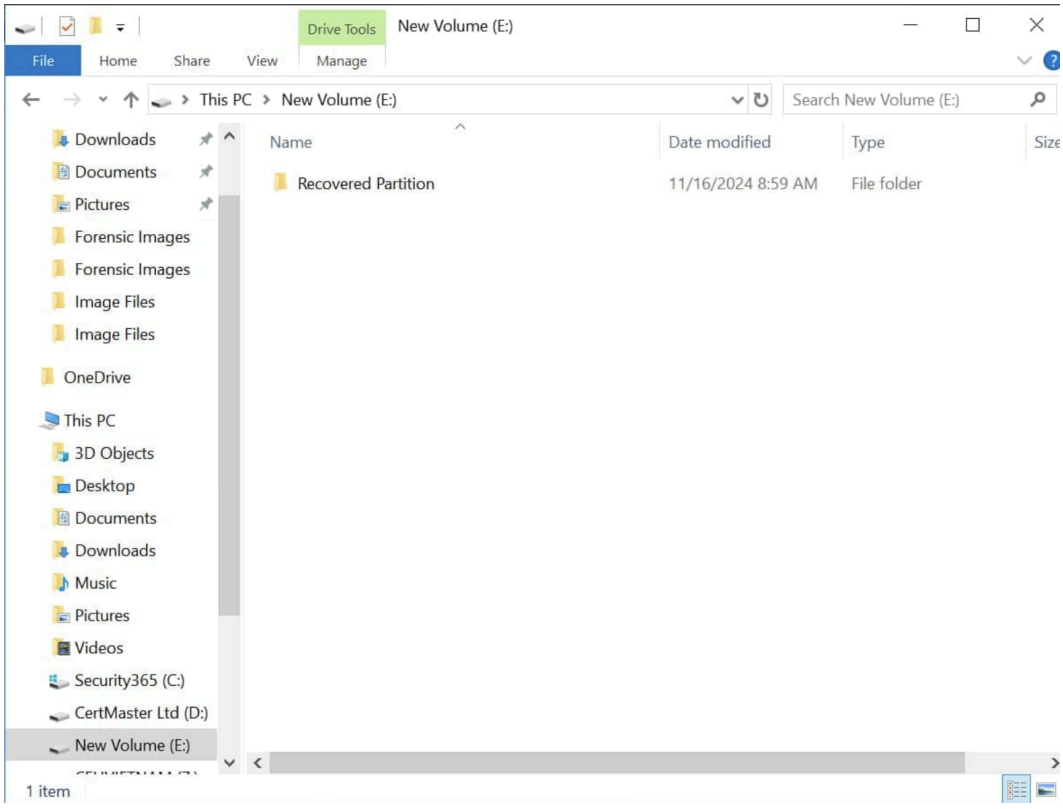
Lab 3:

Step 1: Create Volume Wizard



Step 2: Click recover and choose the folder that we want to export partition

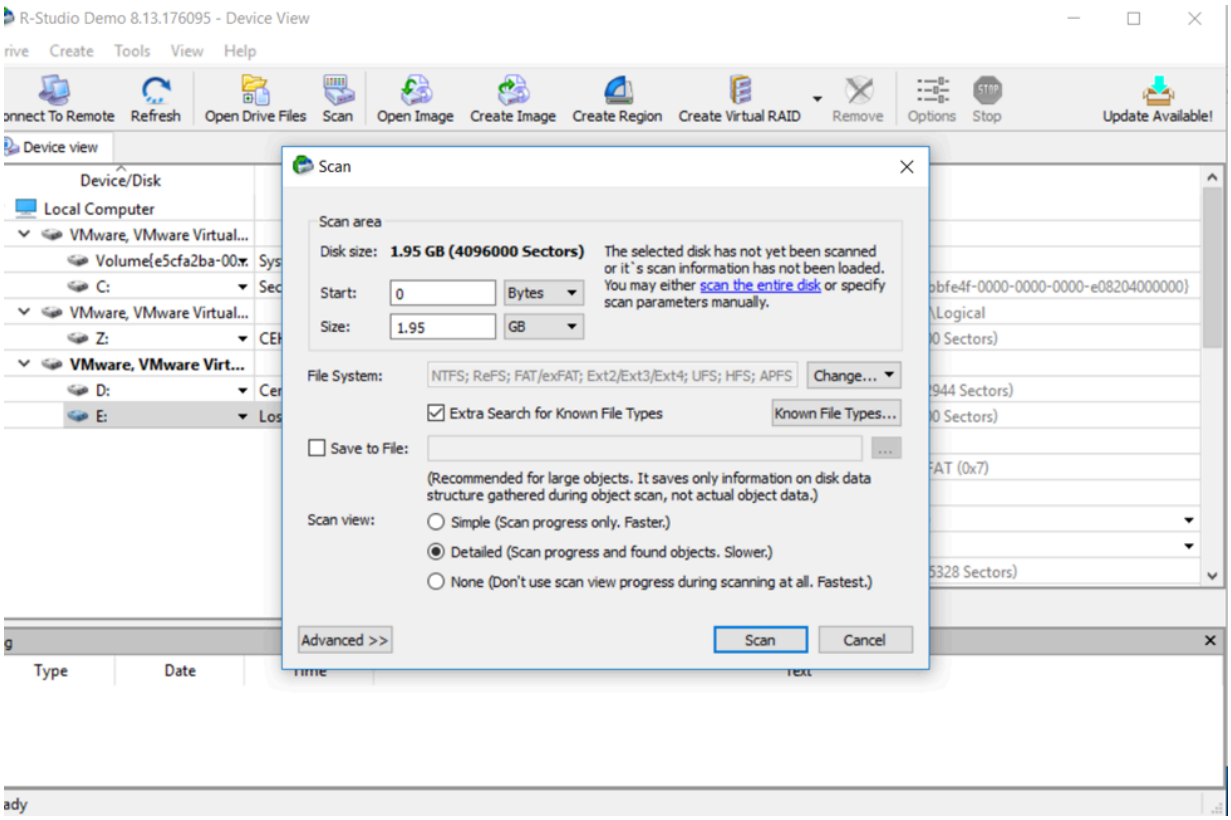


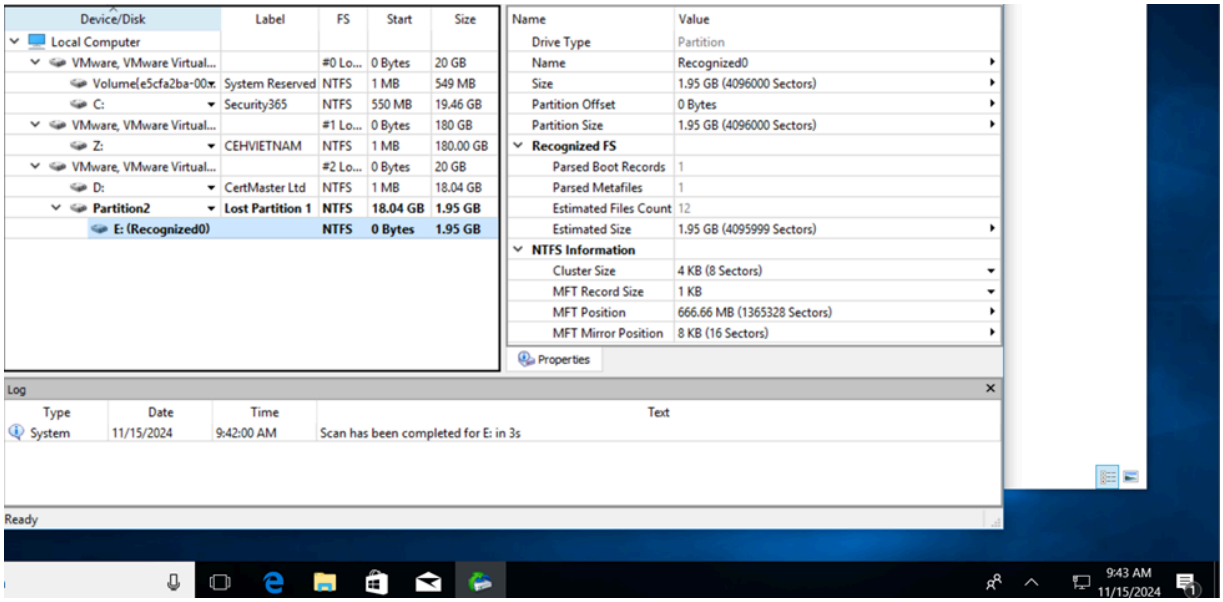


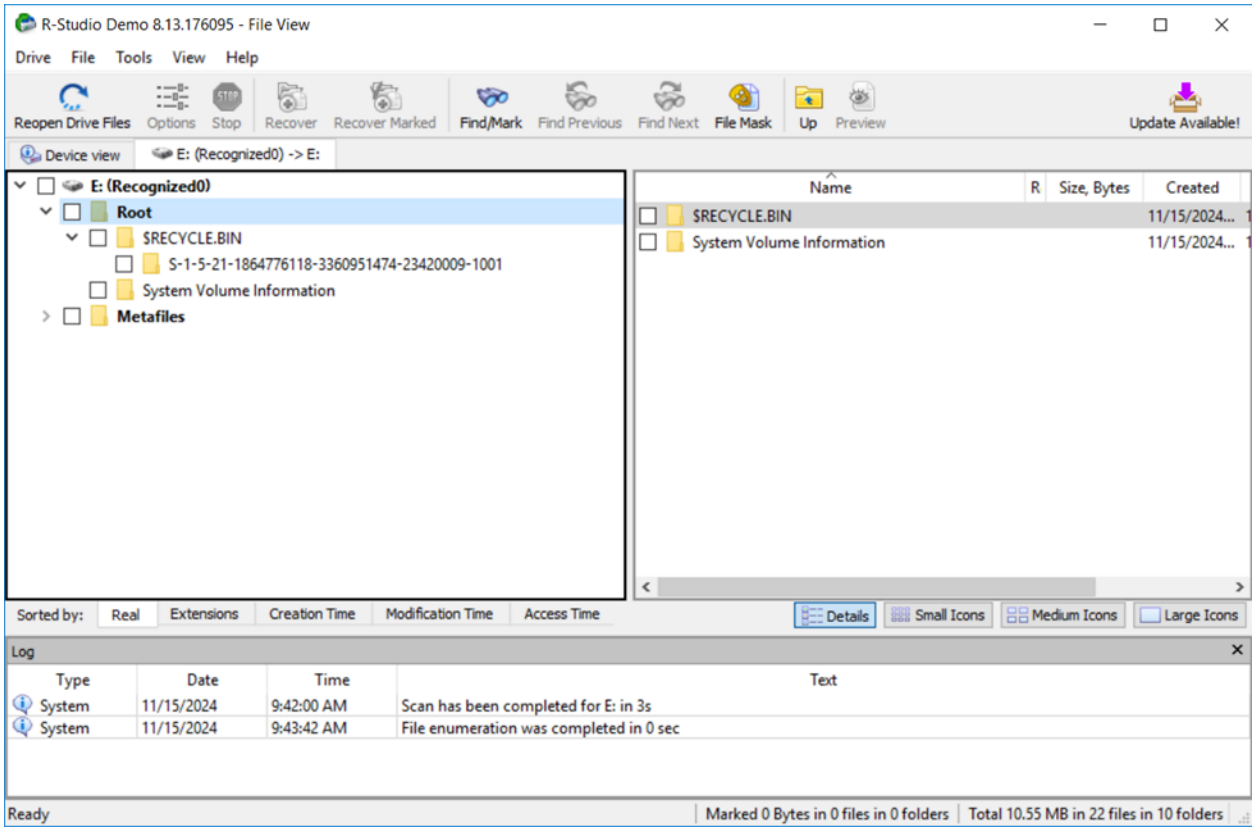
Lab 4:

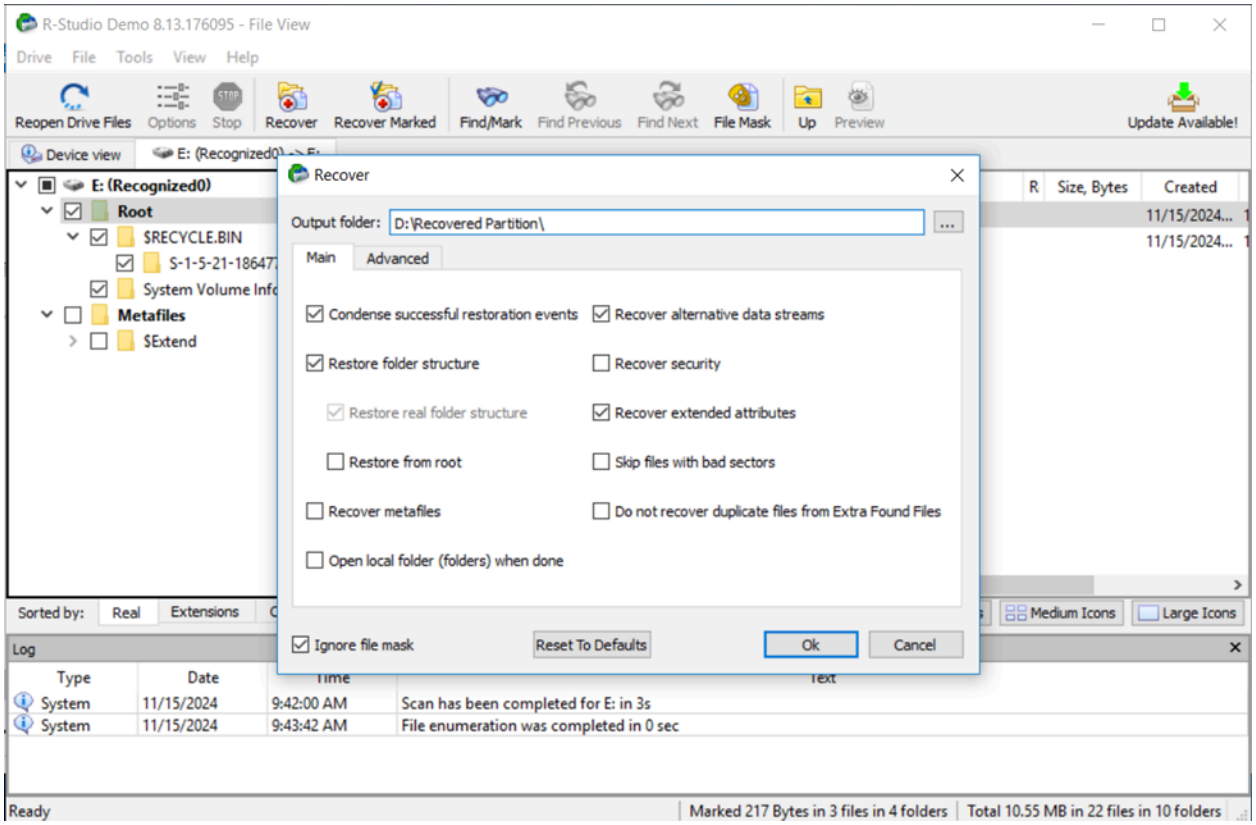
Recovering Data from a Partition that is Deleted and Merged into another Partition.

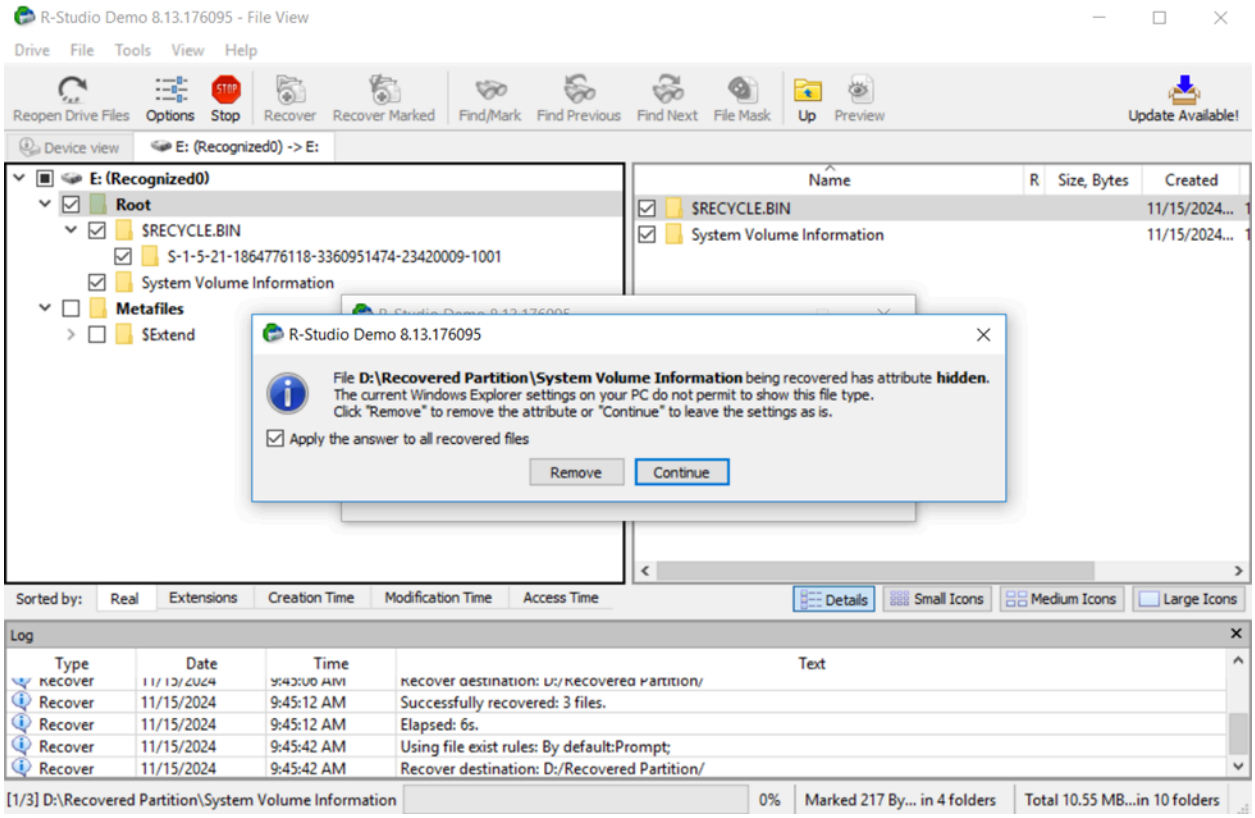
The attacker merged this partition into another. The victim discovered that one of the disk partitions on their system was missing, and the size of another partition has increased by the size of the deleted partition.

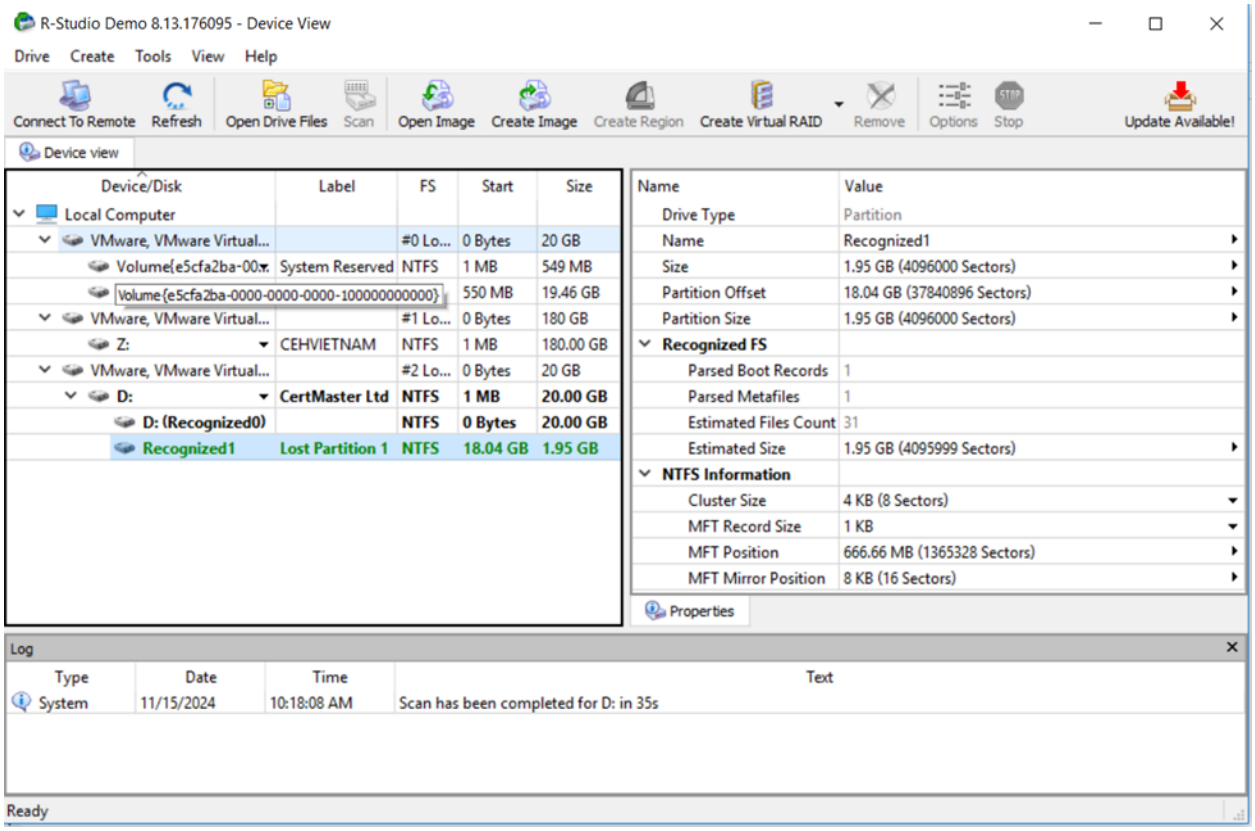



Device/Disk
Label
FS
Start
Size
Local Computer
VMware, VMware Virtual...
#0 Lo...
0 Bytes
20 GB
Volume{e5cfa2ba-00...
System Reserved
NTFS
1 MB
549 MB
C:
Security365
NTFS
550 MB
19.46 GB
VMware, VMware Virtual...
#1 Lo...
0 Bytes
180 GB
Z:
CEHVIETNAM
NTFS
1 MB
180.00 GB
VMware, VMware Virtual...
#2 Lo...
0 Bytes
20 GB
D:
CertMaster Ltd
NTFS
1 MB
18.04 GB
Partition2
Lost Partition 1
NTFS
18.04 GB
1.95 GB
E: (Recognized0)
NTFS
0 Bytes
1.95 GB
Name
Value
Drive Type
Partition
Name
Recognized0
Size
1.95 GB (4096000 Sectors)
Partition Offset
0 Bytes
Partition Size
1.95 GB (4096000 Sectors)
Recognized FS
Parsed Boot Records
1
Parsed Metafiles
1
Estimated Files Count
12
Estimated Size
1.95 GB (4095999 Sectors)
NTFS Information
Cluster Size
4 KB (8 Sectors)
MFT Record Size
1 KB
MFT Position
666.66 MB (1365328 Sectors)
MFT Mirror Position
8 KB (16 Sectors)
Properties
Log
Type
Date
Time
Text
System
11/15/2024
9:42:00 AM
Scan has been completed for E: in 3s
Ready
9:43 AM
11/15/2024


R-Studio Demo 8.13.176095 - File View
Drive
File
Tools
View
Help
Reopen Drive Files
Options
Stop
Recover
Recover Marked
Find/Mark
Find Previous
Find Next
File Mask
Up
Preview
Update Available!
Device view
E: (Recognized0) -> E:
E: (Recognized0)
Root
$RECYCLE.BIN
S-1-5-21-1864776118-3360951474-23420009-1001
System Volume Information
Metafiles
Name
R
Size, Bytes
Created
$RECYCLE.BIN
11/15/2024...
System Volume Information
11/15/2024...
Sorted by:
Real
Extensions
Creation Time
Modification Time
Access Time
Details
Small Icons
Medium Icons
Large Icons
Log
Type
Date
Time
Text
System
11/15/2024
9:42:00 AM
Scan has been completed for E: in 3s
System
11/15/2024
9:43:42 AM
File enumeration was completed in 0 sec
Ready
Marked 0 Bytes in 0 files in 0 folders
Total 10.55 MB in 22 files in 10 folders


R-Studio Demo 8.13.176095 - File View
Drive File Tools View Help
Reopen Drive Files
Options
Stop
Recover
Recover Marked
Find/Mark
Find Previous
Find Next
File Mask
Up
Preview
Update Available!
Device view
E: (Recognized0)
Root
$RECYCLE.BIN
System Volume Info
Metafiles
$Extend
Size, Bytes
Created
11/15/2024...
11/15/2024...
Recover
Output folder:
D:\Recovered Partition\
Main
Advanced
Condense successful restoration events
Recover alternative data streams
Restore folder structure
Recover security
Restore real folder structure
Recover extended attributes
Restore from root
Skip files with bad sectors
Recover metafiles
Do not recover duplicate files from Extra Found Files
Open local folder (folders) when done
Ignore file mask
Reset To Defaults
Ok
Cancel
Sorted by:
Real
Extensions
Medium Icons
Large Icons
Log
Type
Date
Time
Text
System
11/15/2024
9:42:00 AM
Scan has been completed for E: in 3s
System
11/15/2024
9:43:42 AM
File enumeration was completed in 0 sec
Ready
Marked 217 Bytes in 3 files in 4 folders
Total 10.55 MB in 22 files in 10 folders


R-Studio Demo 8.13.176095 - File View
Drive File Tools View Help
Reopen Drive Files Options Stop Recover Recover Marked Find/Mark Find Previous Find Next File Mask Up Preview Update Available!
Device view E: (Recognized0) -> E:
E: (Recognized0)
Root
$RECYCLE.BIN
S-1-5-21-1864776118-3360951474-23420009-1001
System Volume Information
Metafiles
$Extend
Name R Size, Bytes Created
$RECYCLE.BIN 11/15/2024...
System Volume Information 11/15/2024...
R-Studio Demo 8.13.176095
File D:\Recovered Partition\System Volume Information being recovered has attribute hidden.
The current Windows Explorer settings on your PC do not permit to show this file type.
Click "Remove" to remove the attribute or "Continue" to leave the settings as is.
Apply the answer to all recovered files
Remove Continue
Sorted by: Real Extensions Creation Time Modification Time Access Time
Details Small Icons Medium Icons Large Icons
Log
Type Date Time Text
Recover 11/15/2024 9:45:12 AM Successfully recovered: 3 files.
Recover 11/15/2024 9:45:12 AM Elapsed: 6s.
Recover 11/15/2024 9:45:42 AM Using file exist rules: By default:Prompt;
Recover 11/15/2024 9:45:42 AM Recover destination: D:/Recovered Partition/
[1/3] D:\Recovered Partition\System Volume Information 0% Marked 217 By... in 4 folders Total 10.55 MB...in 10 folders


R-Studio Demo 8.13.176095 - Device View
Drive Create Tools View Help
Connect To Remote Refresh Open Drive Files Scan Open Image Create Image Create Region Create Virtual RAID Remove Options Stop Update Available!
Device view
Device/Disk Label FS Start Size
Local Computer
VMware, VMware Virtual... #0 Lo... 0 Bytes 20 GB
Volume{e5cfa2ba-00... System Reserved NTFS 1 MB 549 MB
Volume{e5cfa2ba-0000-0000-0000-100000000000} 550 MB 19.46 GB
VMware, VMware Virtual... #1 Lo... 0 Bytes 180 GB
Z: CEHVIETNAM NTFS 1 MB 180.00 GB
VMware, VMware Virtual... #2 Lo... 0 Bytes 20 GB
D: CertMaster Ltd NTFS 1 MB 20.00 GB
D: (Recognized0) NTFS 0 Bytes 20.00 GB
Recognized1 Lost Partition 1 NTFS 18.04 GB 1.95 GB
Name Value
Drive Type Partition
Name Recognized1
Size 1.95 GB (4096000 Sectors)
Partition Offset 18.04 GB (37840896 Sectors)
Partition Size 1.95 GB (4096000 Sectors)
Recognized FS
Parsed Boot Records 1
Parsed Metafiles 1
Estimated Files Count 31
Estimated Size 1.95 GB (4095999 Sectors)
NTFS Information
Cluster Size 4 KB (8 Sectors)
MFT Record Size 1 KB
MFT Position 666.66 MB (1365328 Sectors)
MFT Mirror Position 8 KB (16 Sectors)
Properties
Log
Type Date Time Text
System 11/15/2024 10:18:08 AM Scan has been completed for D: in 35s
Ready

Lab 5: Cracking Application Passwords:

Run Passware Kit Forensic Demo option is checked.

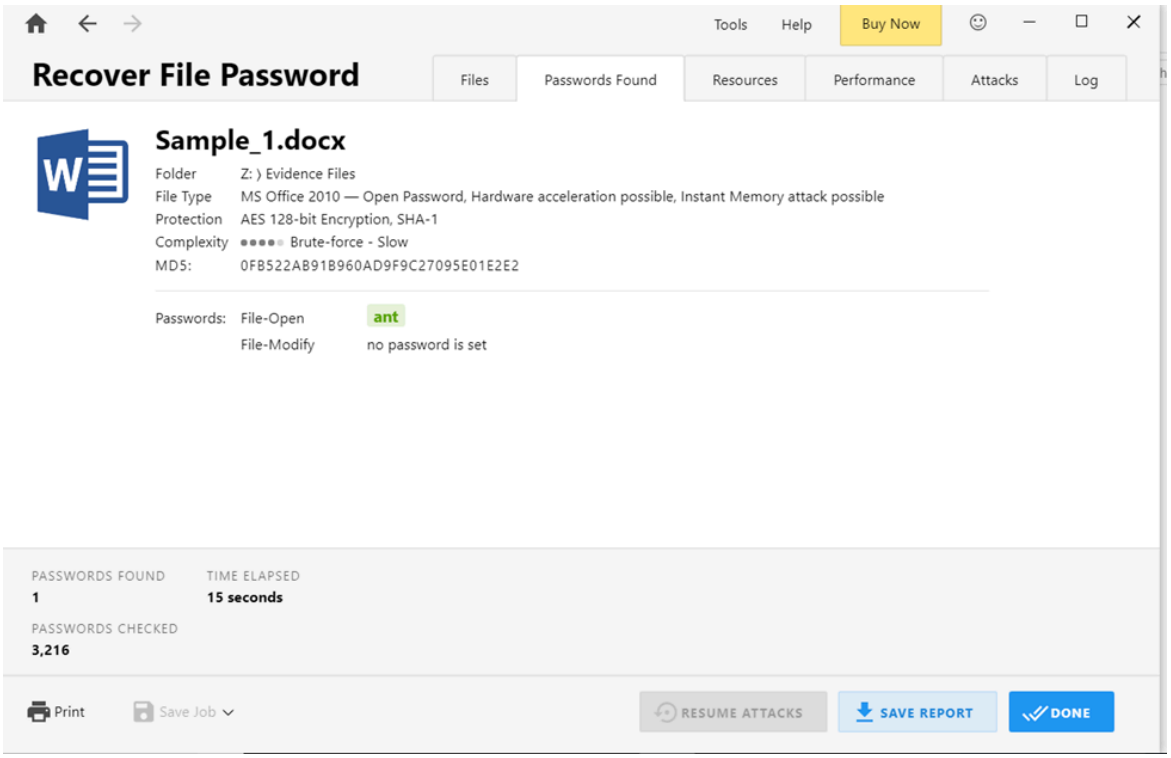
Click the Recover File Password option from the main window of the tool.

Navigate to the location Z:\Evidence Files, select the file Sample_1.docx, and click Open.

The Recover File Password window wizard appears, where you need to select the Use Predefined Settings option.

The tool will take some time to crack the password. The time required is proportional to the number and types of characters used in the password.

The tool displays the cracked password.

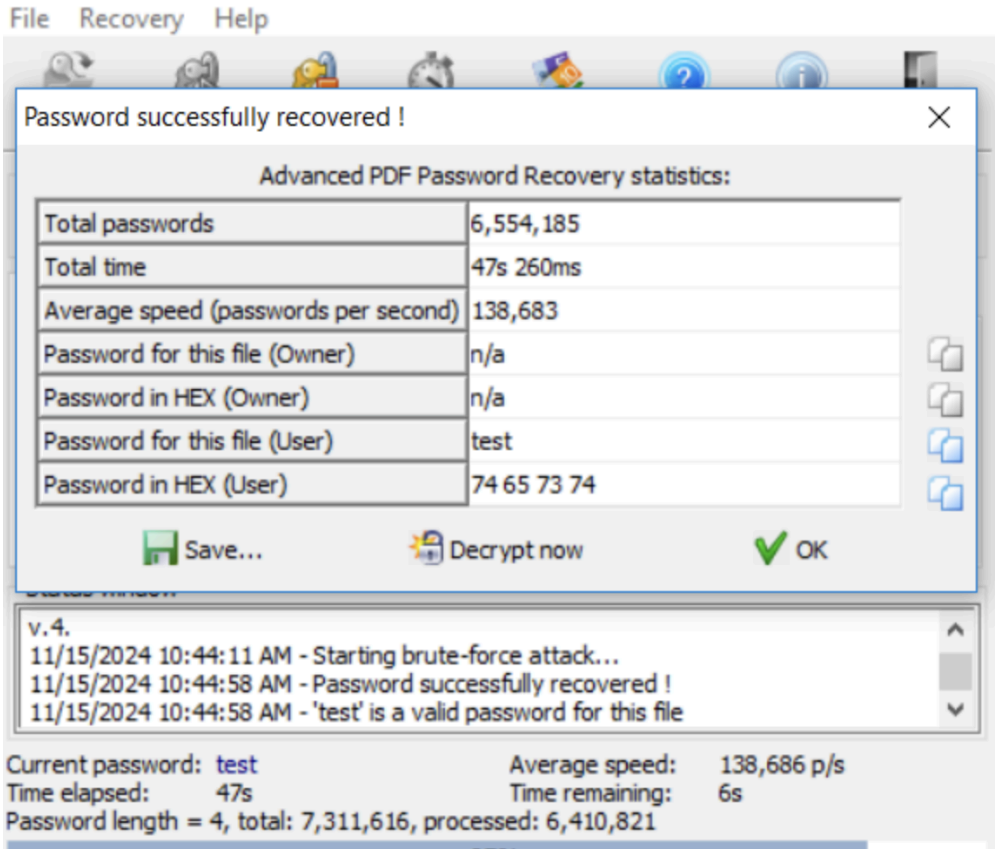


Run Advanced Archive Password Recovery is checked.

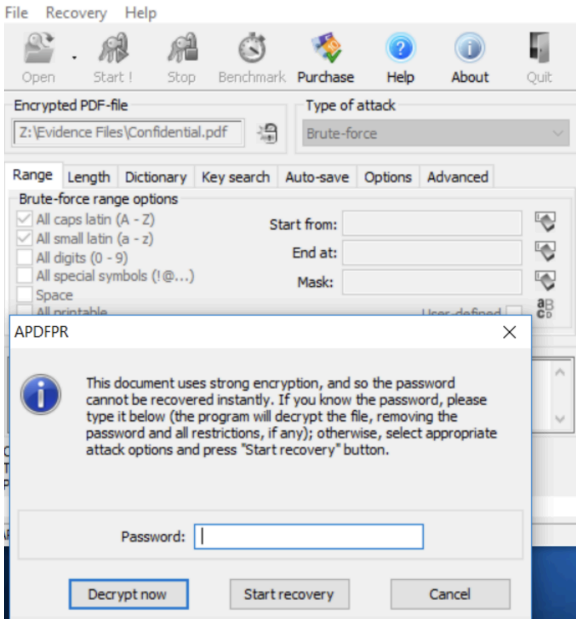
Advanced Archive Password Recovery GUI appears, as shown in the following scrchecked.

Checking the All digits (0-9) option while leaving all the other options unchecked.

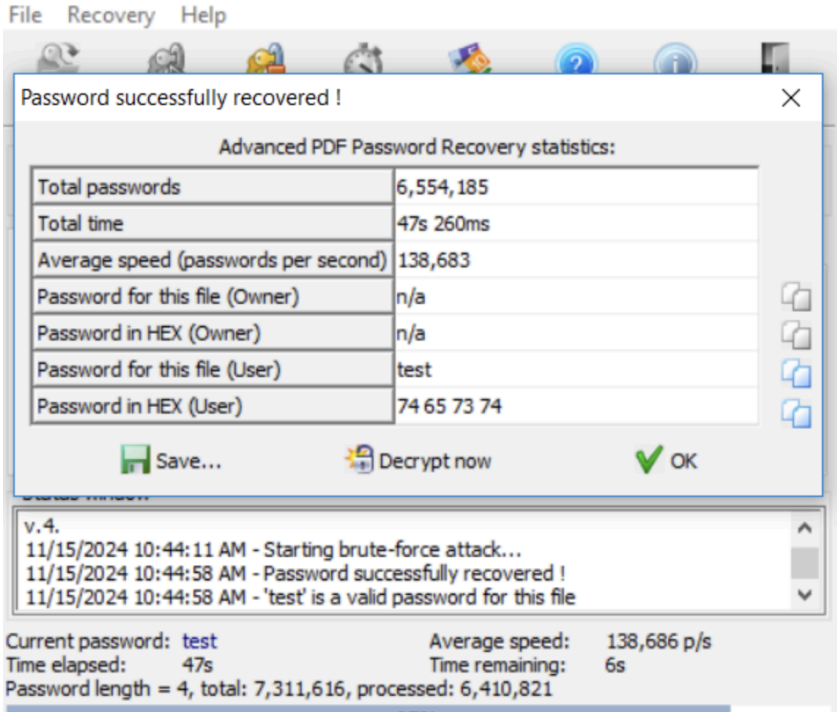
The tool cracks the password and displays it along with other details, as shown in the screenshot:



After performing the analysis, the tool will display a window with the password for the Confidential.pdf file, as shown in the following screenshot:



Therefore, the tool takes a large amount of time for cracking a password, if it is complex in nature.

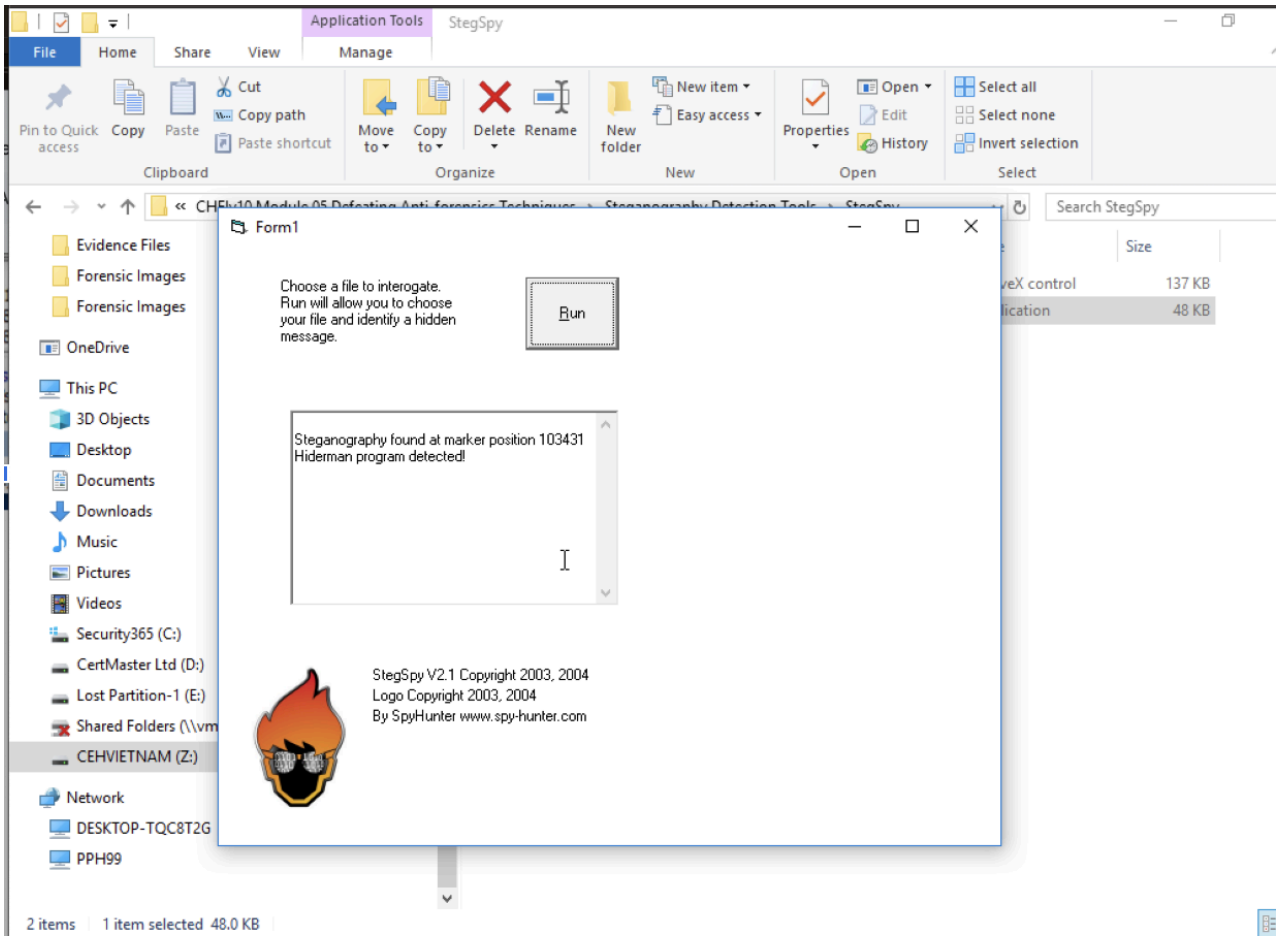


Lab 6:

Open window appears. Navigate to the location of the suspicious file, C:\CHFI-Tools\Evidence Files\Image Files. Select the file Model.png and click the Open button.

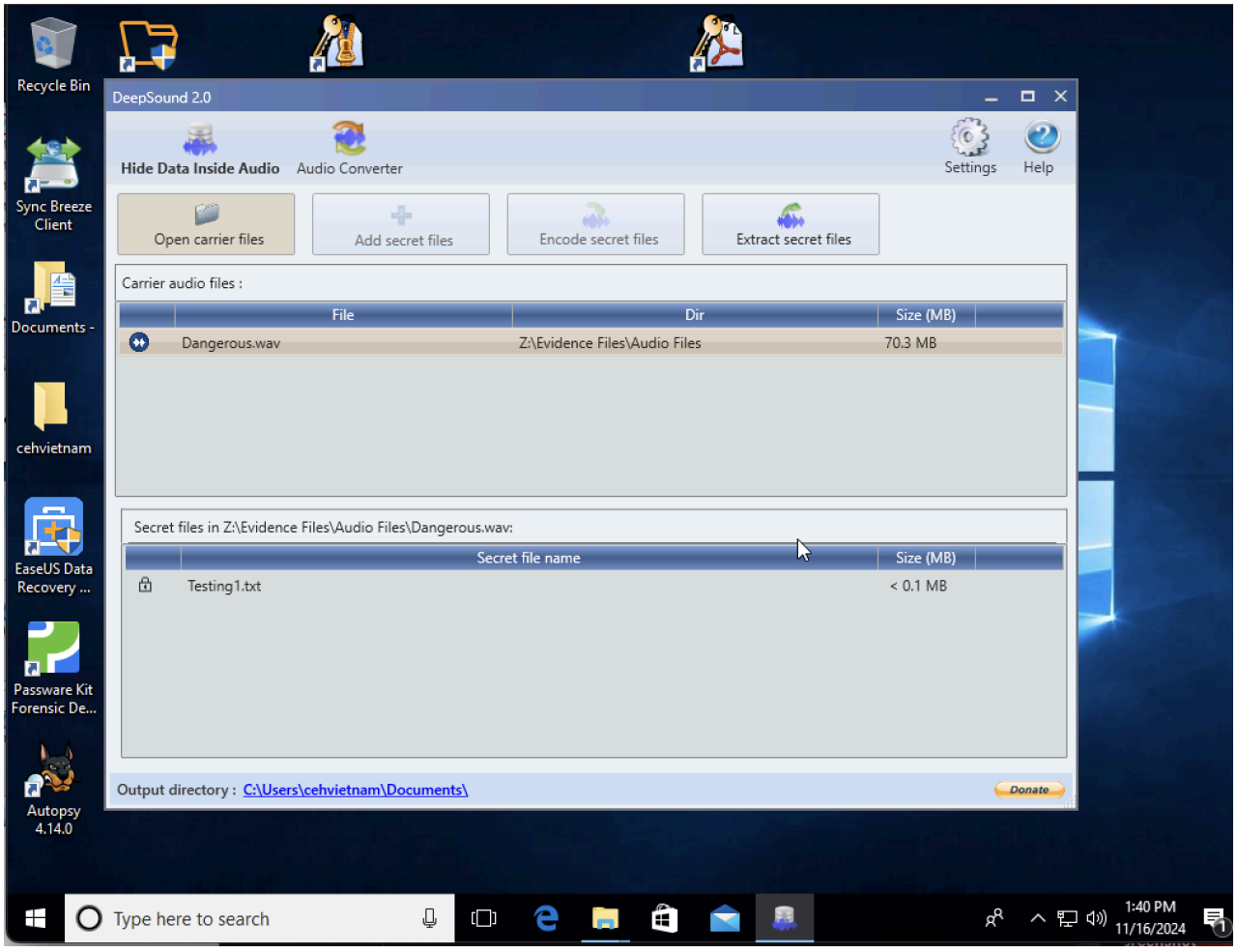
The tool will scan the file and display the type of steganography technique used to hide another file in it.

Open OpenStego to extract hidden message

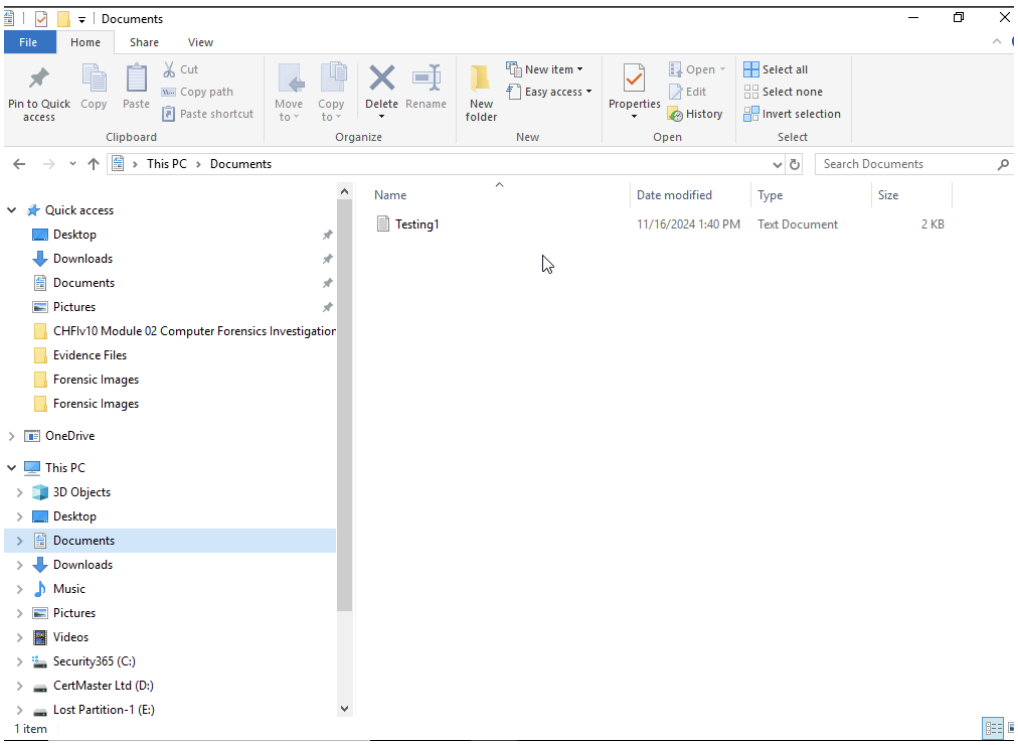


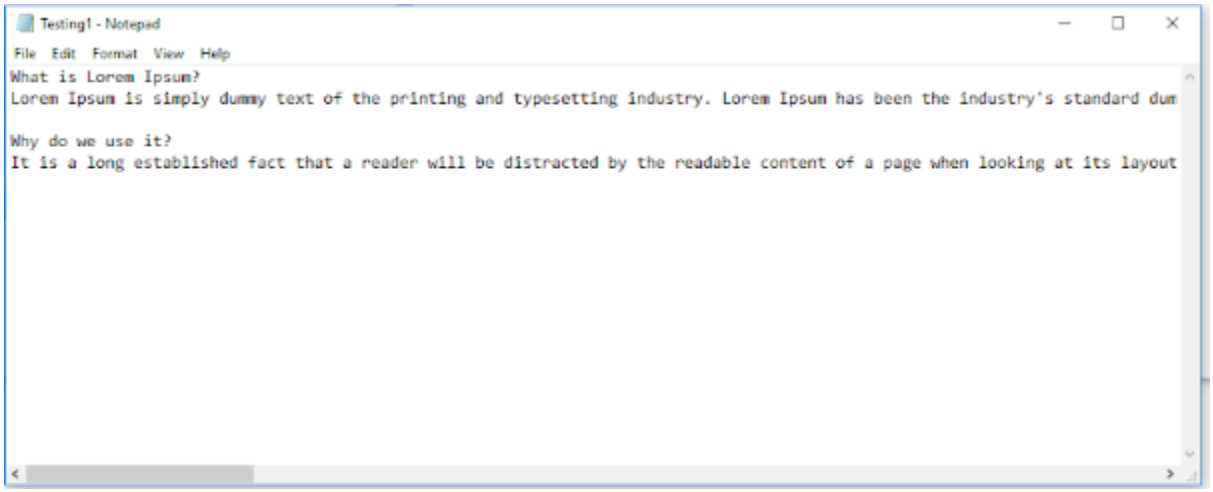
The DeepSound GUI appears as shown in the following screenshot:

Navigate to the location C:\CHFI-Tools\Evidence Files\Audio Files; select the file containing steganography, Dangerous.wav, and click the Open button.



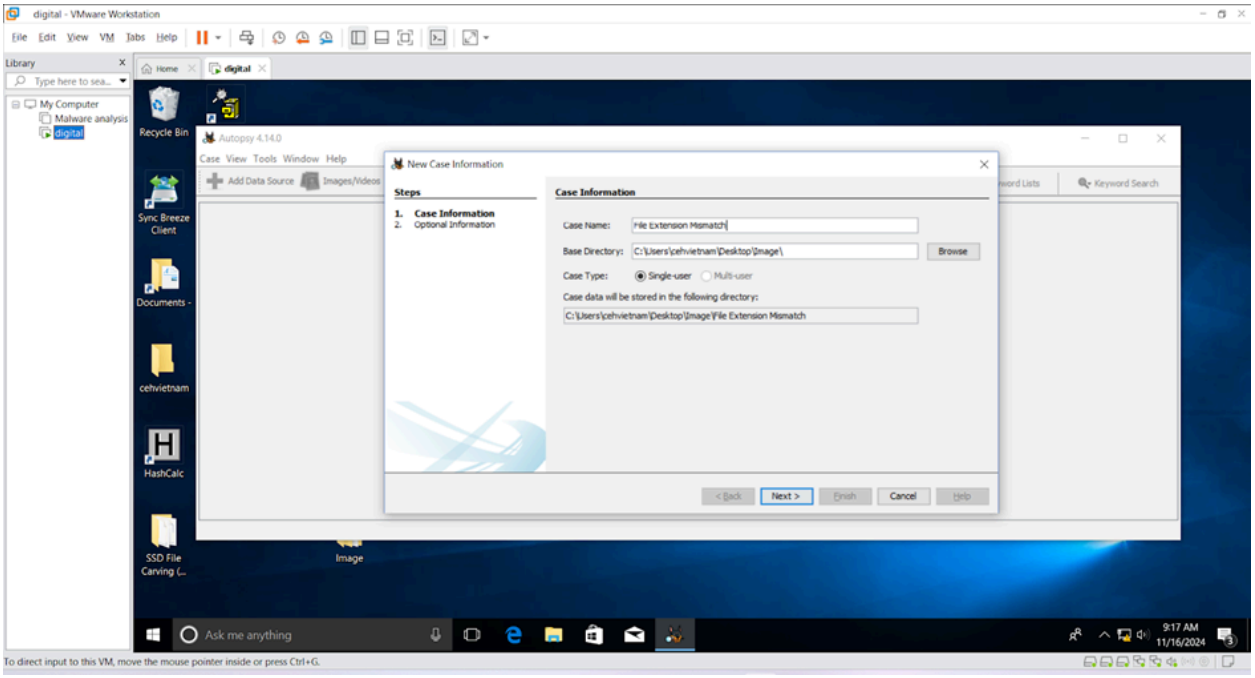
To view the hidden file that was extracted in the previous step, navigate to the location displayed in the screenshot above, i.e., C:\Users\Administrator\Documents.

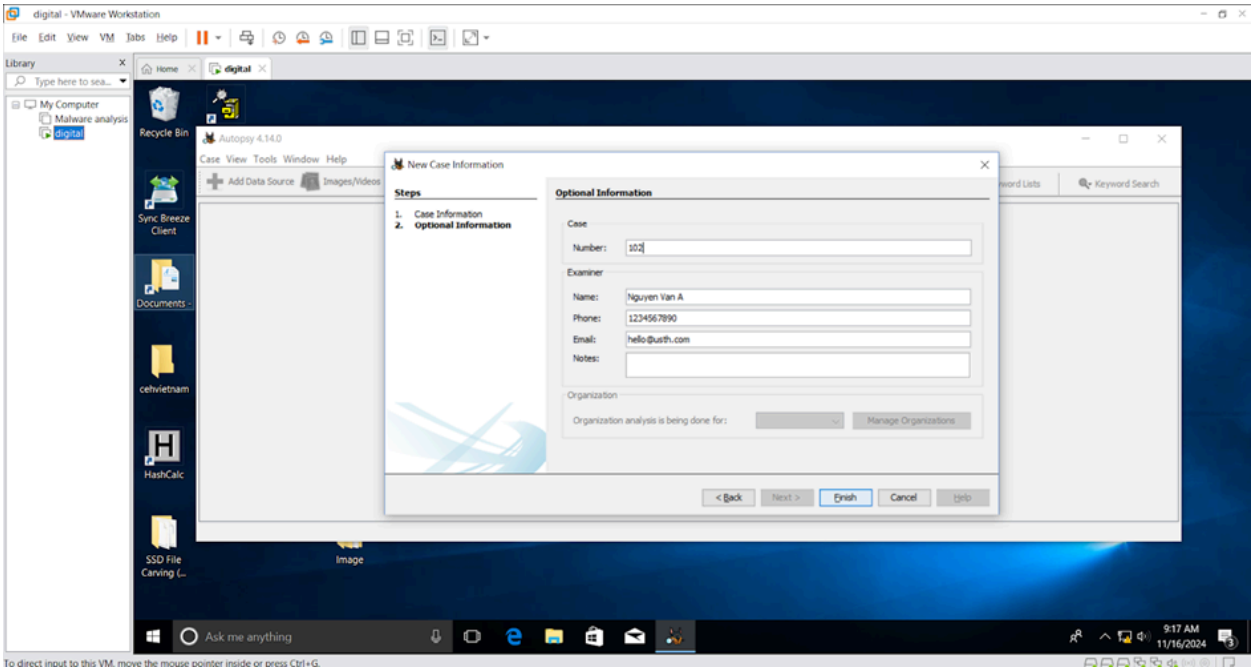




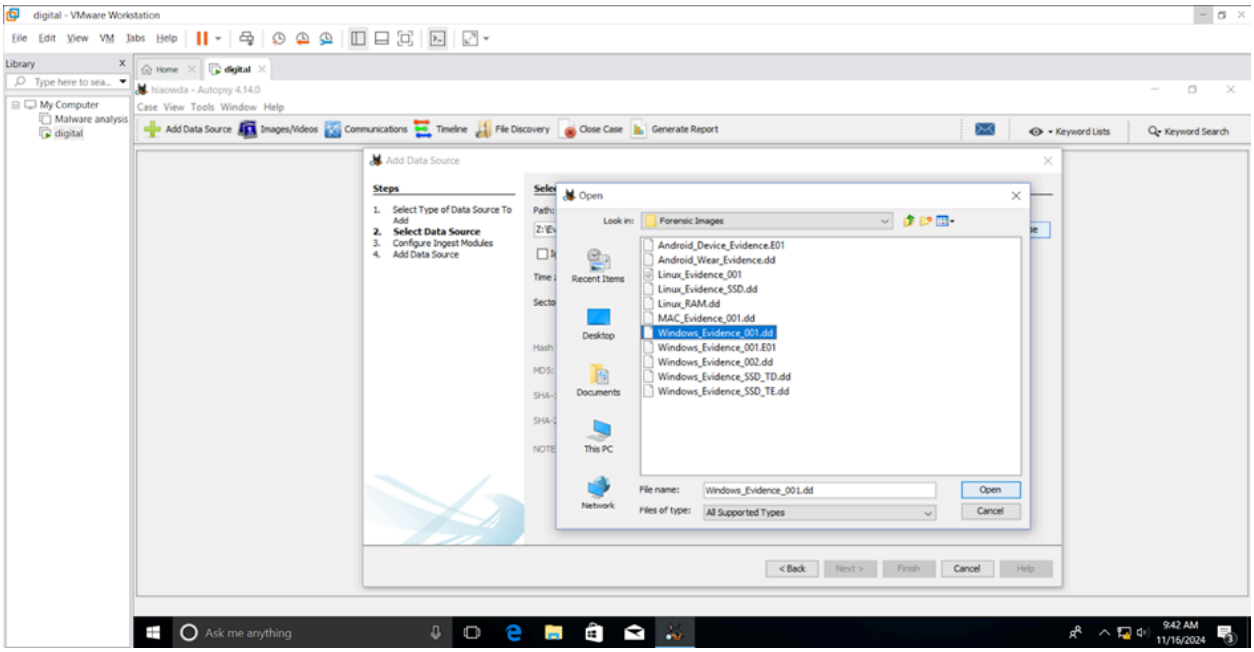
Lab 8: Detecting File Extension Mismatch

In this task, we using AutoPsy tool again. Create new case:

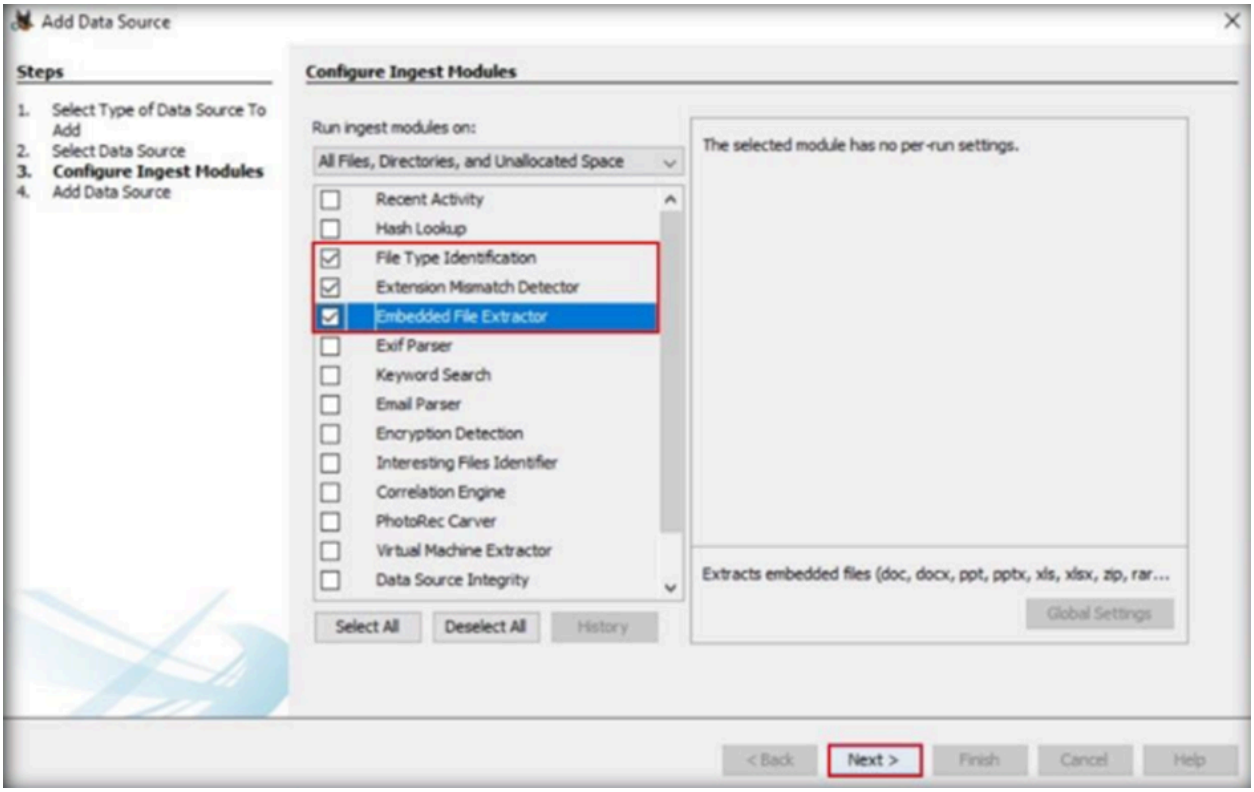




Click on “browse” and select the file **Windows_Evidence_001.dd**, then open it.

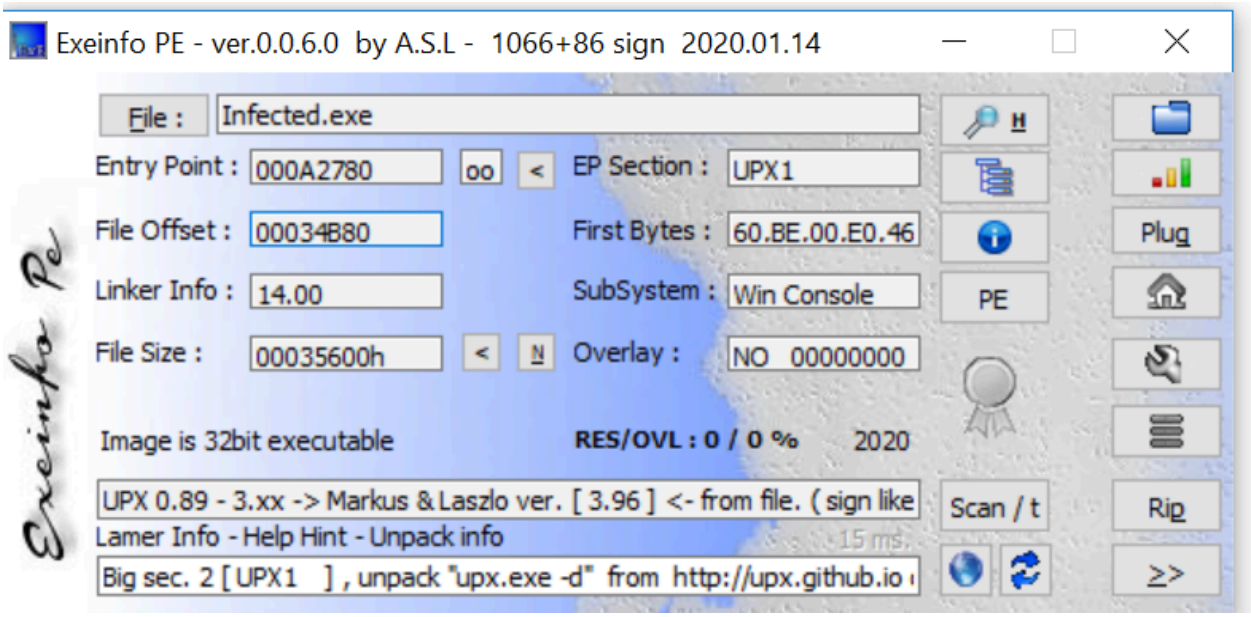


When the **Configure Ingest Modules** section appears, we deselect all and check **File Type Identification**, **Extension Mismatch Detector** and **Embedded File Extractor** options.



Click the **Windows_Evidence_001.dd** to view its contents in the right pane of the tool window.

Lab 9:



Analyzing the Packed File:

- Exeinfo PE displayed details about the file, such as the entry point, file offset, linker information, and overlay data.
- The tool also identified that `Infected.exe` is packed with UPX (Ultimate Packer for eXecutables) 3.x, a popular packing software used to compress executable files.

- The unpacking hint from Exeinfo PE suggested using the command `upx.exe -d`.

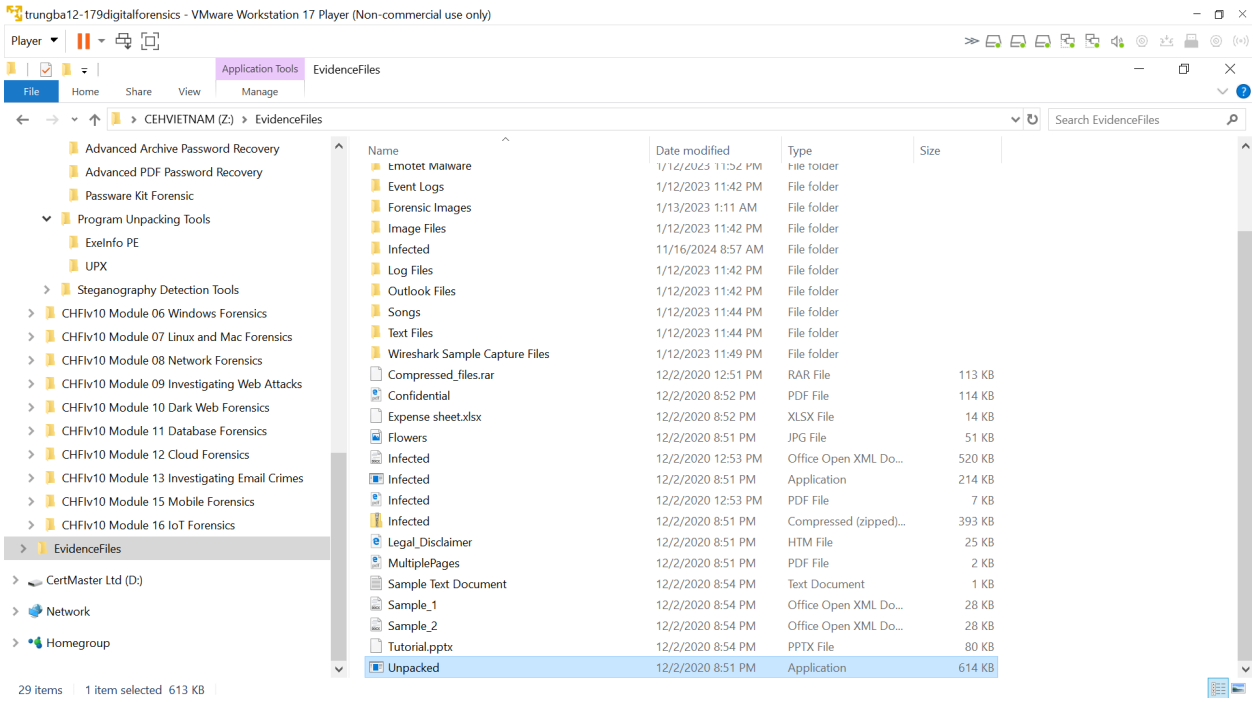
```
Z:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Program Unpacking Tools\UPX>upx -d "Z:\EvidenceFil
es\Infected.exe" -o "Z:\EvidenceFiles\Unpacked.exe"
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    628224 <-    218624   34.80%    win32/pe     Unpacked.exe

Unpacked 1 file.

Z:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Program Unpacking Tools\UPX>
```

UPX successfully unpacked the file, reducing its compression ratio from 34.8% to its full size.



THANK!