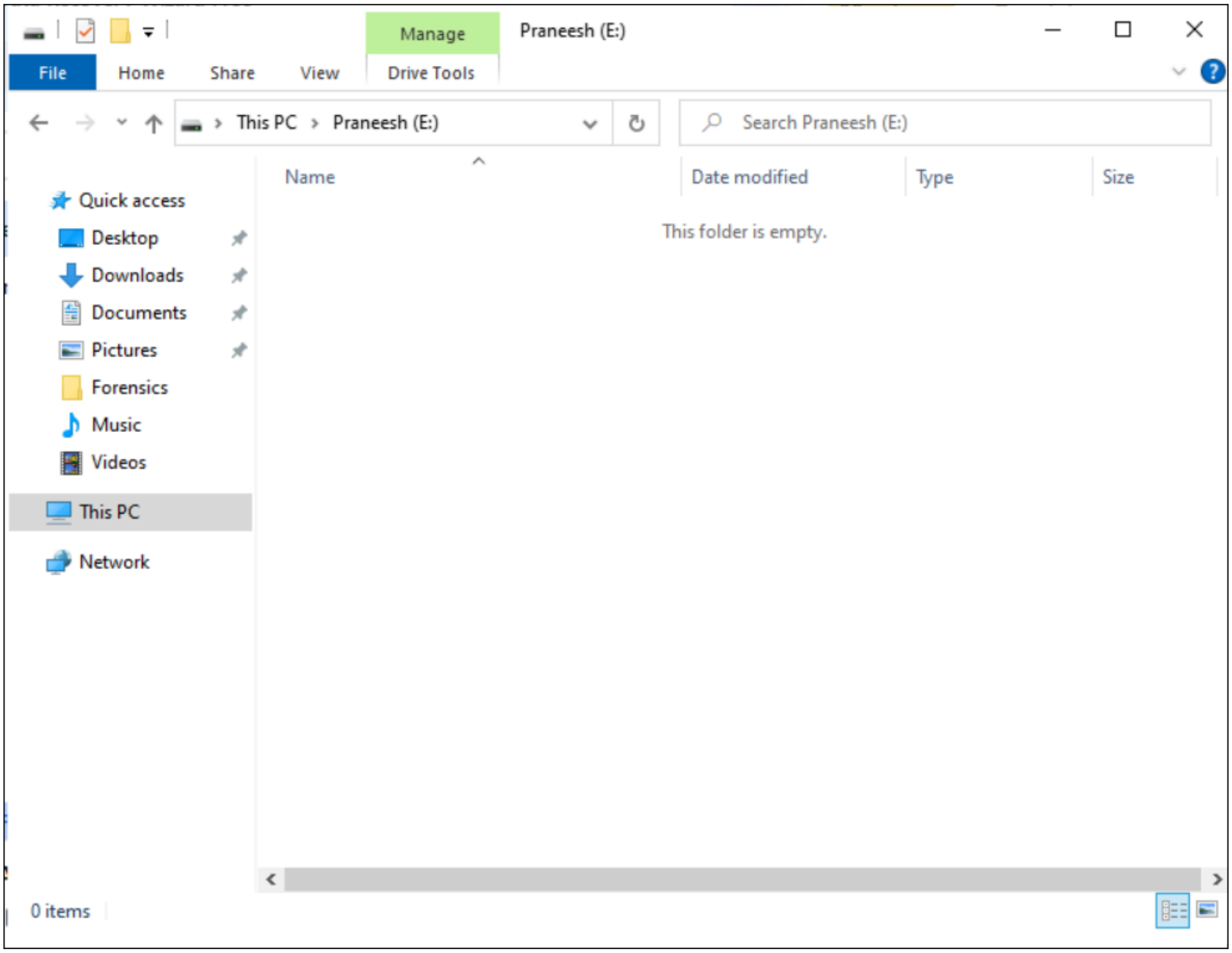
Praneesh R V
CB.SC.U4CYS23036

Cybersecurity Forensics - Lab 1

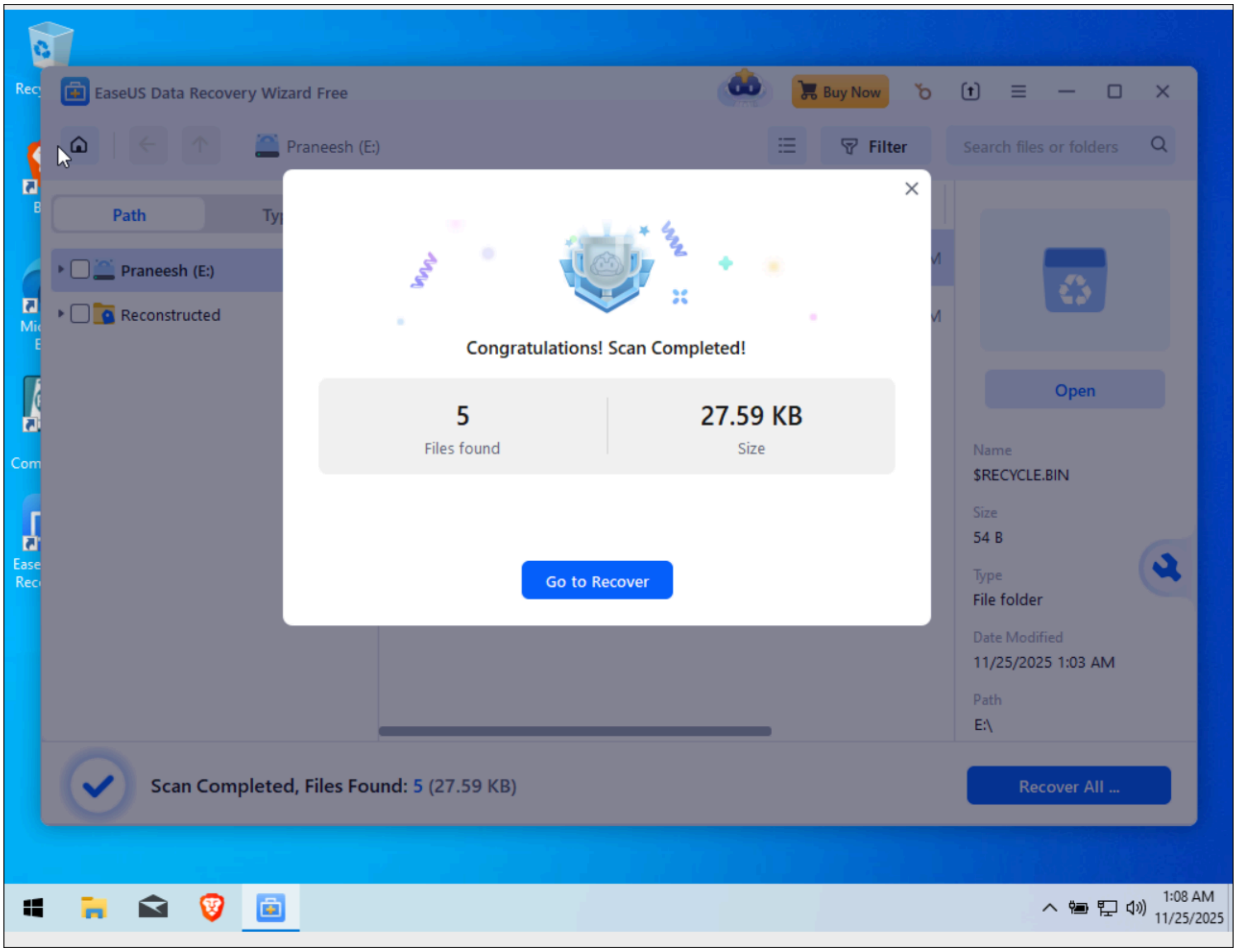
Task 1 - Recovering deleted data using EaseUS Data Recovery tool



This folder is empty.

I deleted the files from my E Drive, and emptied the recycle bin

Then I scanned my E Drive using EaseUS data recovery tool



Congratulations! Scan Completed!

5 Files found

27.59 KB Size

Name: $RECYCLE.BIN

Size: 54 B

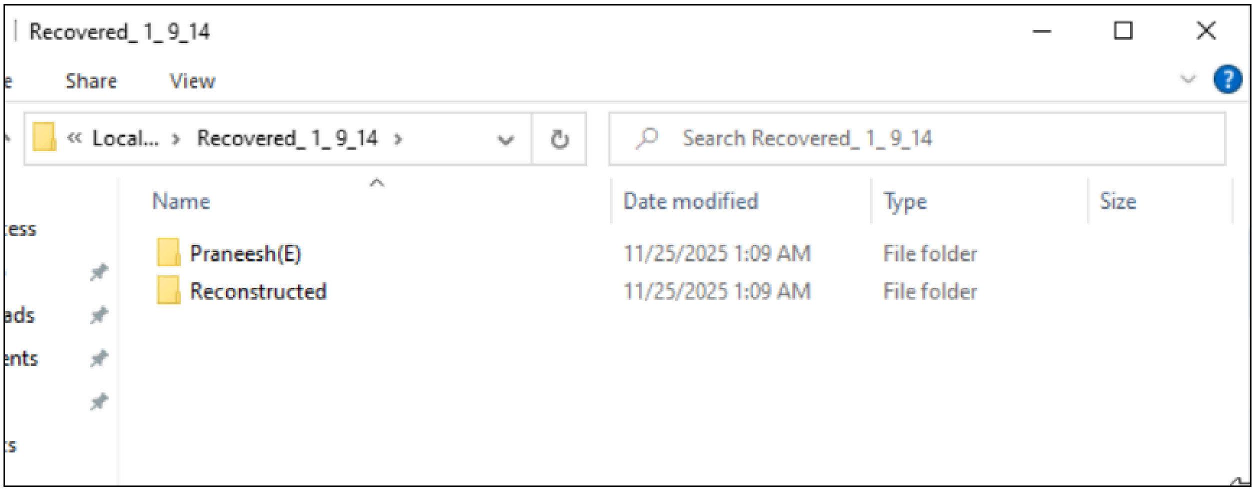
Type: File folder

Date Modified: 11/25/2025 1:03 AM

Path: E:\

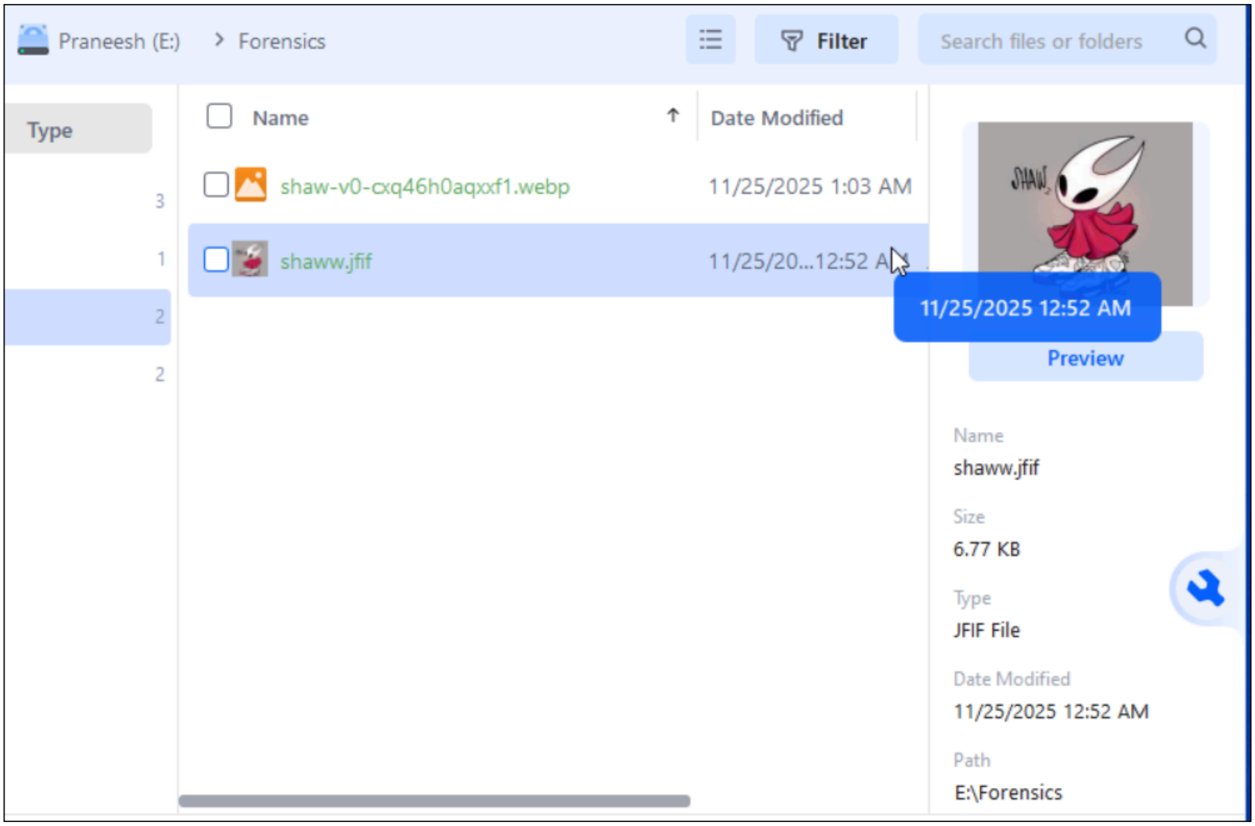
Scan Completed, Files Found: 5 (27.59 KB)

I clicked recover and the recoverdd files are saved in a different path



Name	Date modified	Type	Size
Praneesh(E)	11/25/2025 1:09 AM	File folder	
Reconstructed	11/25/2025 1:09 AM	File folder	

And I got the image that i deleted earlier



Name	Date Modified
shaw-v0-cxq46h0aqxxf1.webp	11/25/2025 1:03 AM
shaww.jfif	11/25/20...12:52 AM

11/25/2025 12:52 AM

Name
shaww.jfif

Size
6.77 KB

Type
JFIF File

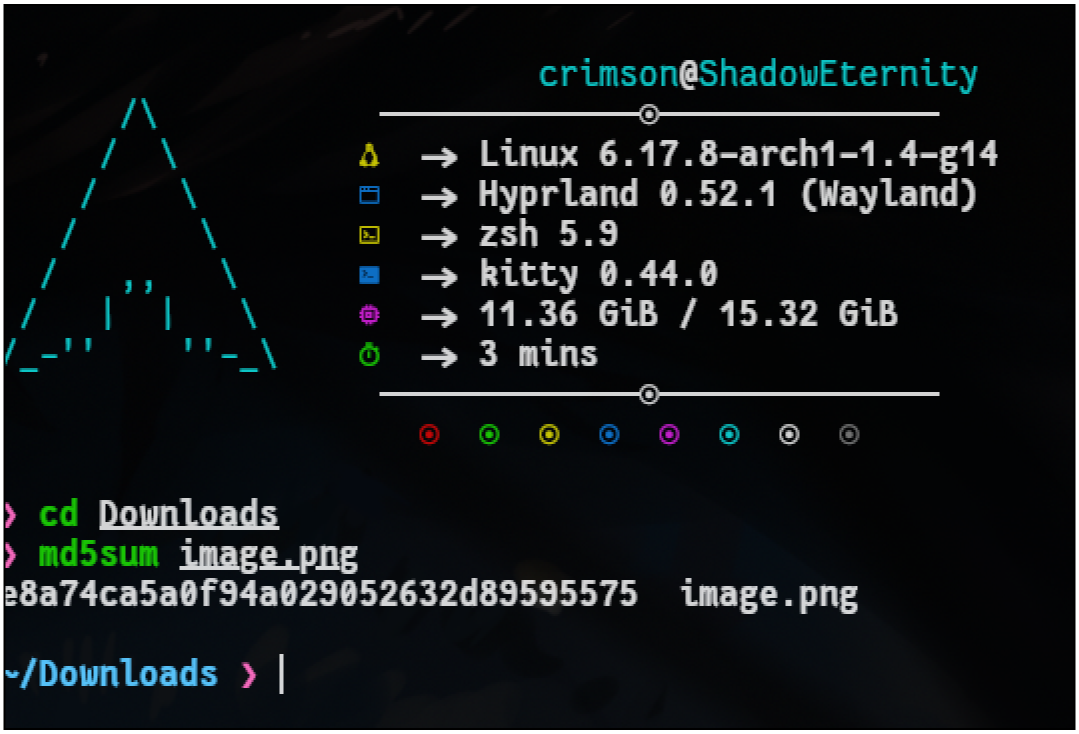
Date Modified
11/25/2025 12:52 AM

Path
E:\Forensics

Task - 2 - Performing Hash, Checksum or HMAC Calculations using the HashCalc

This is the image that i am going to calculate the md5 hash of

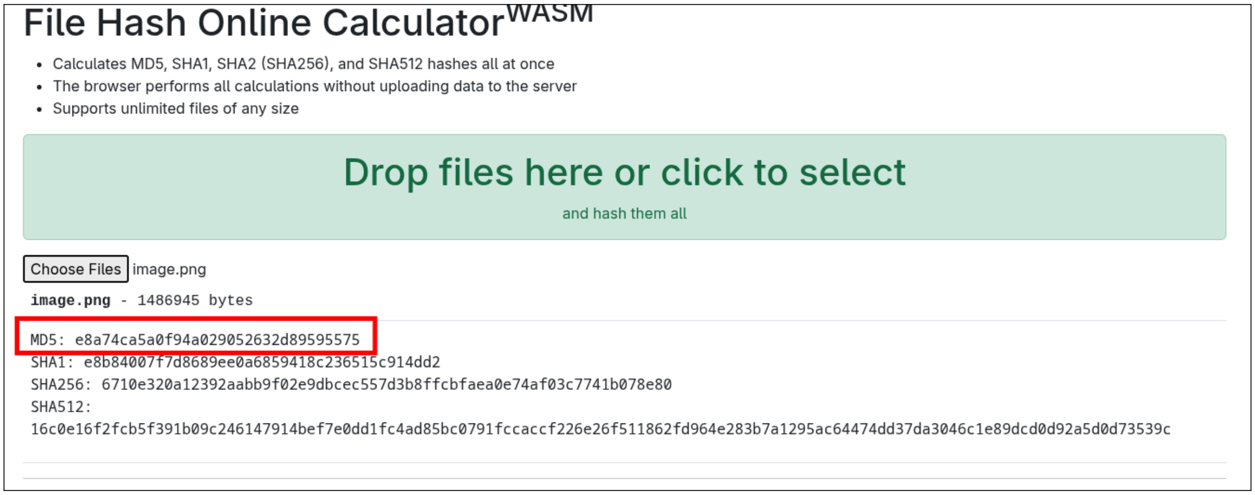
First I calculated the hash from my arch linux terminal



```
                         crimson@ShadowEternity
      /\             ──────────────⊙──────────────
     /  \          ⚠  → Linux 6.17.8-arch1-1.4-g14
    /    \         ▭  → Hyprland 0.52.1 (Wayland)
   /      \        ▭  → zsh 5.9
  /   ,,   \       ▭  → kitty 0.44.0
 /   |  |   \      ▣  → 11.36 GiB / 15.32 GiB
/_-''    ''-_\     ⏱  → 3 mins
                     ──────────────⊙──────────────
                        ●  ●  ●  ●  ●  ●  ●  ●

❯ cd Downloads
❯ md5sum image.png
e8a74ca5a0f94a029052632d89595575  image.png

~/Downloads ❯ |
```

Then I went to http://hash-file.online
Uploaded the file and calculated the md5 hash,
And got the same hash as the md5sum command
I even did it in https://md5file.com/calculator

As you can see the hash is the same in all 3 calculators



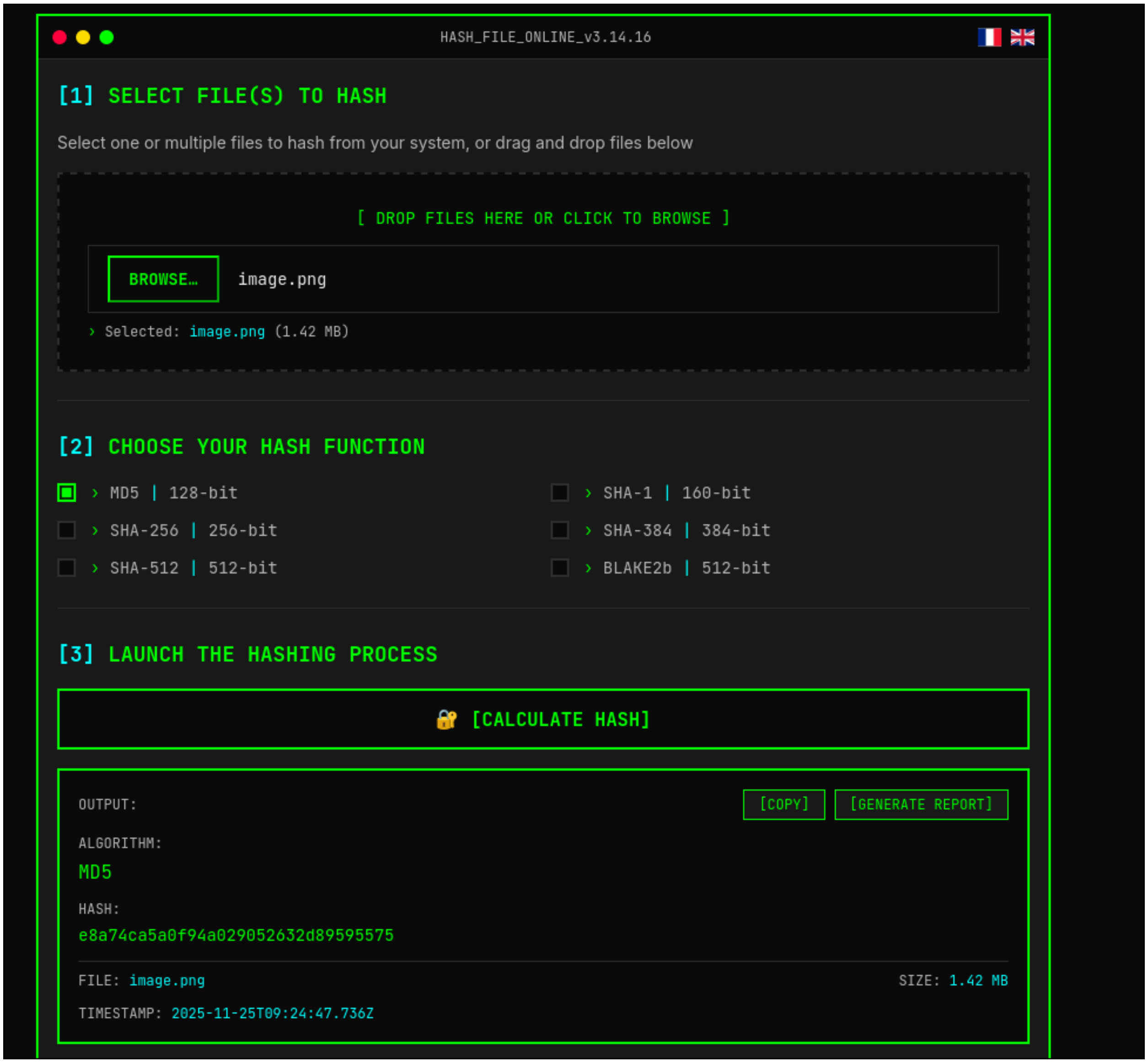
File Hash Online Calculator WASM

- Calculates MD5, SHA1, SHA2 (SHA256), and SHA512 hashes all at once
- The browser performs all calculations without uploading data to the server
- Supports unlimited files of any size

image.png

```
image.png - 1486945 bytes

MD5: e8a74ca5a0f94a029052632d89595575
SHA1: e8b84007f7d8689ee0a6859418c236515c914dd2
SHA256: 6710e320a12392aabb9f02e9dbcec557d3b8ffcbfaea0e74af03c7741b078e80
SHA512:
16c0e16f2fcb5f391b09c246147914bef7e0dd1fc4ad85bc0791fccaccf226e26f511862fd964e283b7a1295ac64474dd37da3046c1e89dcd0d92a5d0d73539c
```

The hash was e8a74ca5a0f94a029052632d89595575



HASH_FILE_ONLINE_v3.14.16

[1] SELECT FILE(S) TO HASH

Select one or multiple files to hash from your system, or drag and drop files below

[DROP FILES HERE OR CLICK TO BROWSE]
BROWSE…

image.png

› Selected: image.png (1.42 MB)

[2] CHOOSE YOUR HASH FUNCTION

☑ › MD5 | 128-bit
☐ › SHA-1 | 160-bit
☐ › SHA-256 | 256-bit
☐ › SHA-384 | 384-bit
☐ › SHA-512 | 512-bit
☐ › BLAKE2b | 512-bit

[3] LAUNCH THE HASHING PROCESS

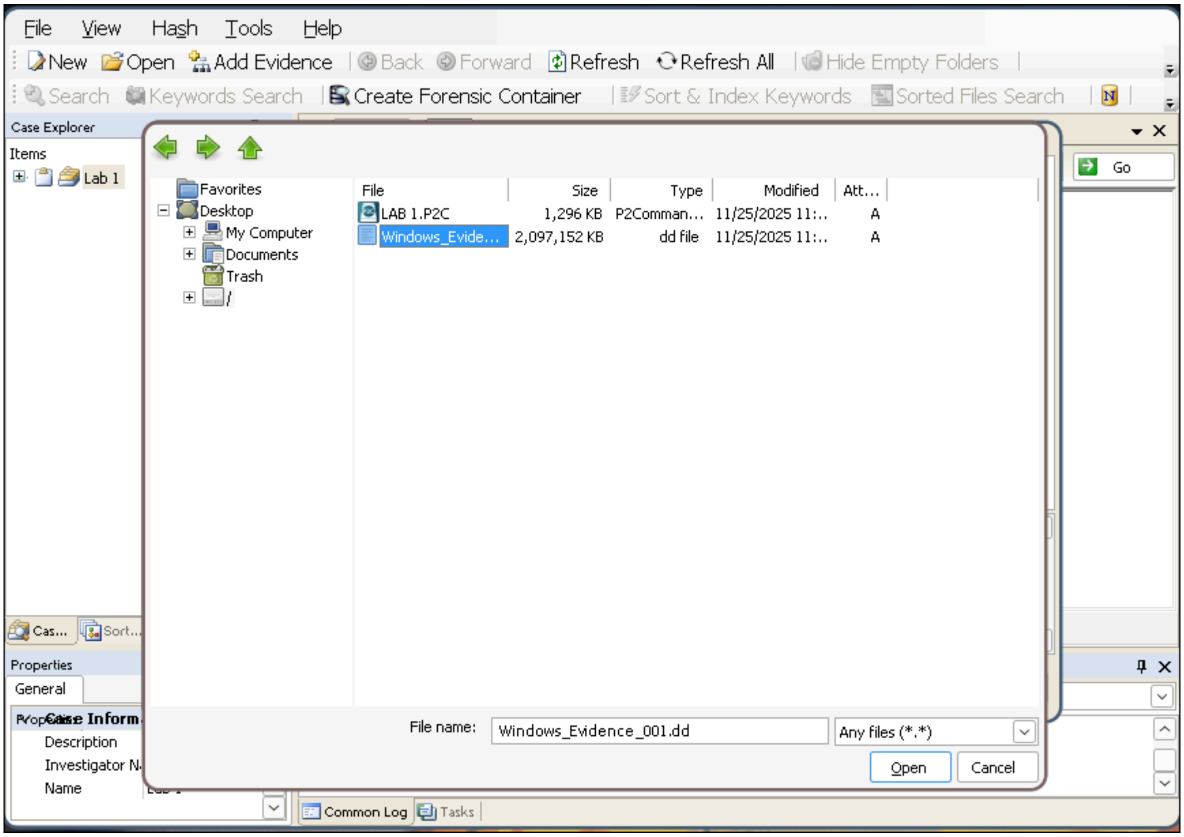
🔐 [CALCULATE HASH]
[COPY]
[GENERATE REPORT]

```
OUTPUT:

ALGORITHM:
MD5

HASH:
e8a74ca5a0f94a029052632d89595575

FILE: image.png                                              SIZE: 1.42 MB
TIMESTAMP: 2025-11-25T09:24:47.736Z
```

Task -5 Handling Evidence Data using P2 Commander

I downloaded P2 Commander in my Arch linux using wine emulator as P2 Commander did not run in my windows vm

I created a new case called Lab 1, gave the investigator name as Praneesh, I chose the Windows_Evidence001.dd file to add a new evidence


File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders
Search Keywords Search Create Forensic Container Sort & Index Keywords Sorted Files Search
Case Explorer
Items
Lab 1
Favorites
Desktop
My Computer
Documents
Trash
/
Go
Cas... Sort...
Properties
General
Common Log Tasks

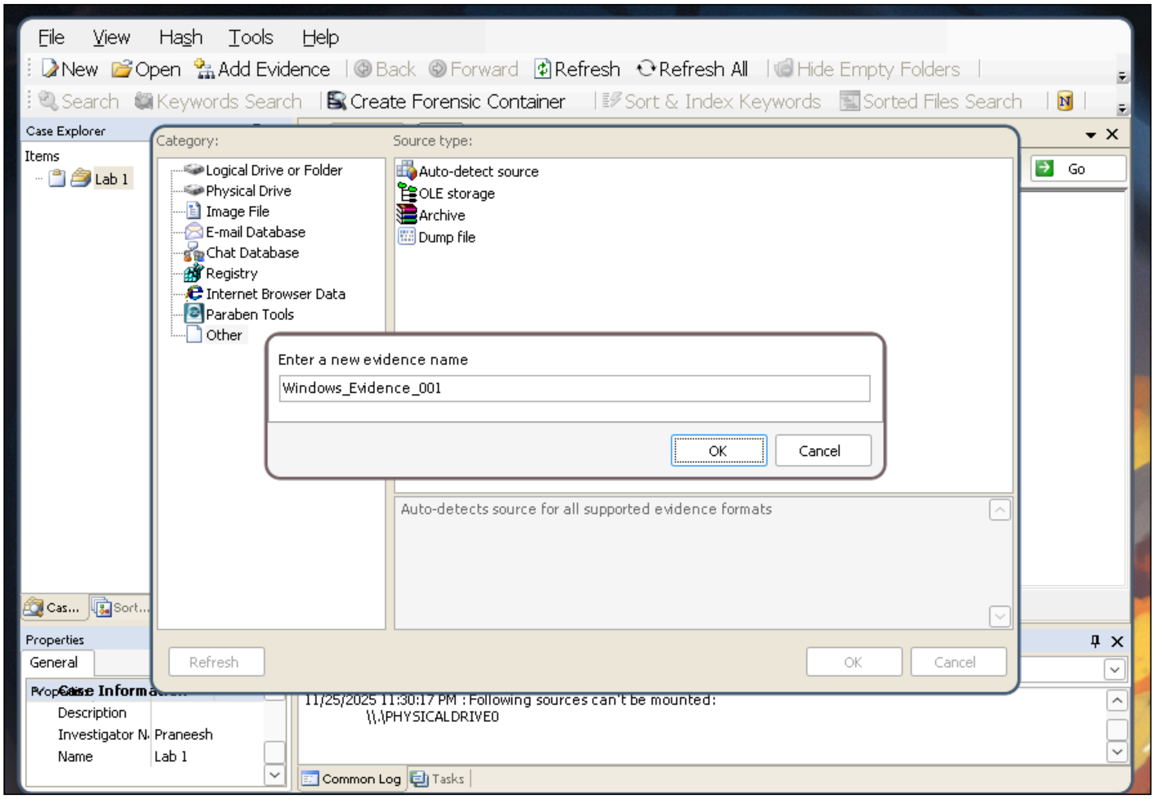
File	Size	Type	Modified	Att...
LAB 1.P2C	1,296 KB	P2Comman...	11/25/2025 11:...	A
Windows_Evide...	2,097,152 KB	dd file	11/25/2025 11:...	A

File name: Windows_Evidence_001.dd

Any files (*.*)

Open Cancel

Case Information
Description
Investigator N
Name


File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders
Search Keywords Search Create Forensic Container Sort & Index Keywords Sorted Files Search
Case Explorer
Items
Lab 1
Go
Cas... Sort...
Properties
General
Refresh
OK
Cancel
Common Log Tasks

Category:
- Logical Drive or Folder
- Physical Drive
- Image File
- E-mail Database
- Chat Database
- Registry
- Internet Browser Data
- Paraben Tools
- Other

Source type:
- Auto-detect source
- OLE storage
- Archive
- Dump file

Enter a new evidence name

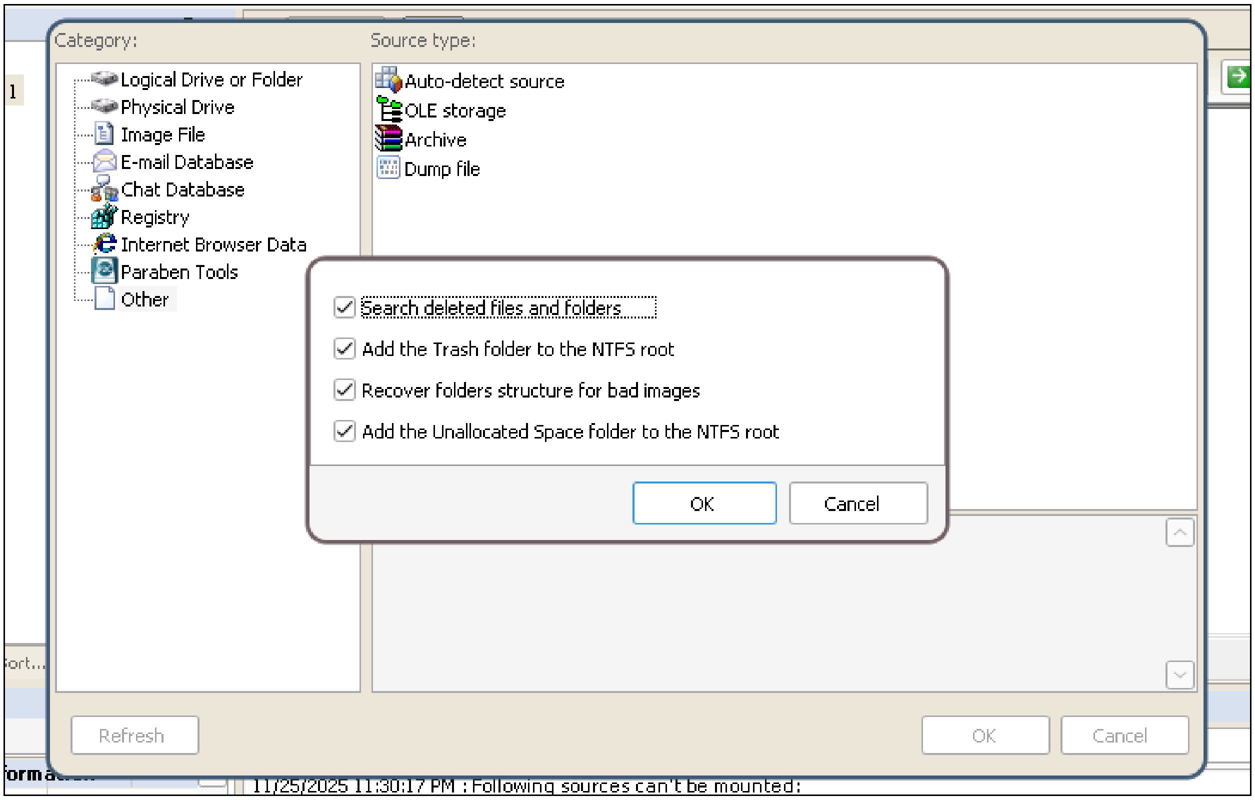
Windows_Evidence_001

OK Cancel

Auto-detects source for all supported evidence formats

Case Information
Description
Investigator N Praneesh
Name Lab 1

```
11/25/2025 11:30:17 PM : Following sources can't be mounted:
        \\.\PHYSICALDRIVE0
```



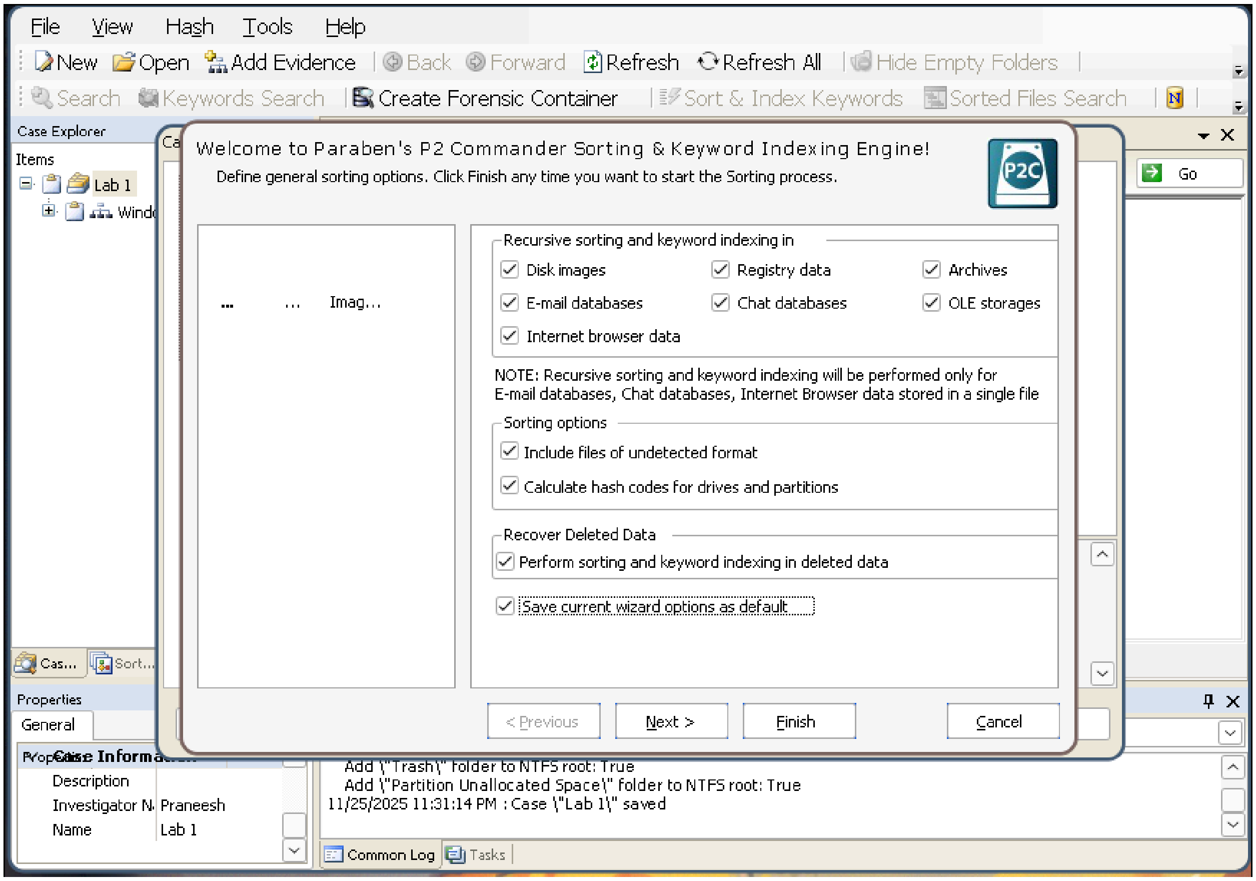
☑ Search deleted files and folders

☑ Add the Trash folder to the NTFS root

☑ Recover folders structure for bad images

☑ Add the Unallocated Space folder to the NTFS root

```
11/25/2025 11:30:17 PM : Following sources can't be mounted:
```



Welcome to Paraben's P2 Commander Sorting & Keyword Indexing Engine!

Define general sorting options. Click Finish any time you want to start the Sorting process.

Recursive sorting and keyword indexing in

☑ Disk images ☑ Registry data ☑ Archives

☑ E-mail databases ☑ Chat databases ☑ OLE storages

☑ Internet browser data

NOTE: Recursive sorting and keyword indexing will be performed only for E-mail databases, Chat databases, Internet Browser data stored in a single file

Sorting options

☑ Include files of undetected format

☑ Calculate hash codes for drives and partitions

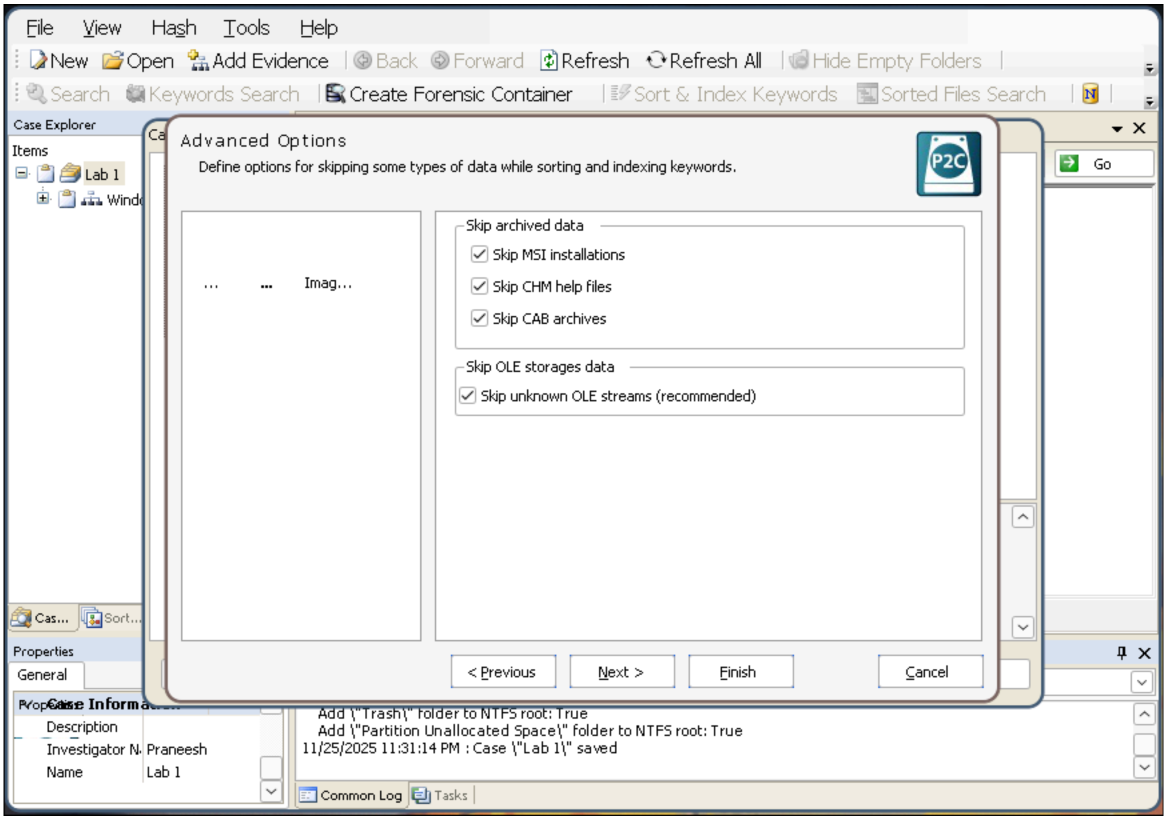
Recover Deleted Data

☑ Perform sorting and keyword indexing in deleted data

☑ Save current wizard options as default

Properties	
General	
Case Information	
Description	
Investigator N	Praneesh
Name	Lab 1

```
Add \"Trash\" folder to NTFS root: True
Add \"Partition Unallocated Space\" folder to NTFS root: True
11/25/2025 11:31:14 PM : Case \"Lab 1\" saved
```


File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders
Search Keywords Search Create Forensic Container Sort & Index Keywords Sorted Files Search
Case Explorer
Items
Lab 1
Wind
Go
Cas... Sort...
Properties
General
Common Log Tasks
< Previous Next > Finish Cancel
P2C

Advanced Options

Define options for skipping some types of data while sorting and indexing keywords.

Skip archived data

☑ Skip MSI installations

☑ Skip CHM help files

☑ Skip CAB archives

Skip OLE storages data

☑ Skip unknown OLE streams (recommended)

Description	
Investigator N.	Praneesh
Name	Lab 1

```
Add \"Trash\" folder to NTFS root: True
Add \"Partition Unallocated Space\" folder to NTFS root: True
11/25/2025 11:31:14 PM : Case \"Lab 1\" saved
```

Keep image size as 65 x 65

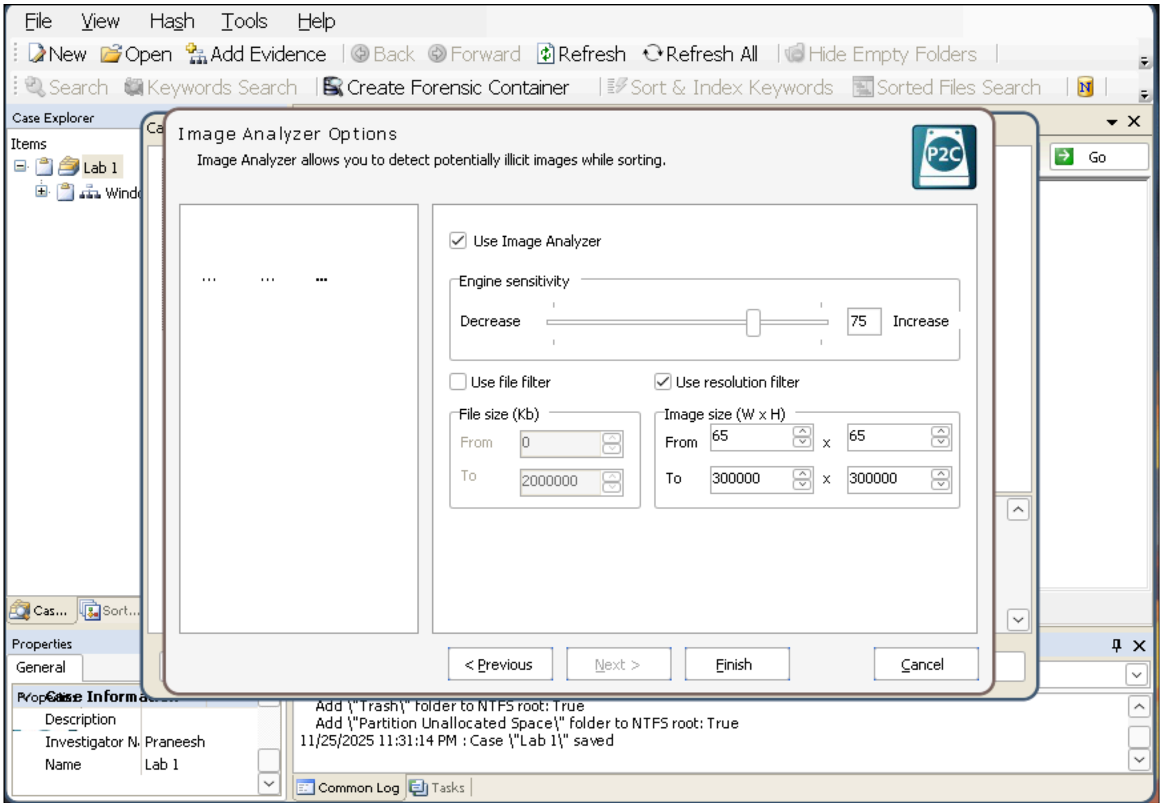

File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders
Search Keywords Search Create Forensic Container Sort & Index Keywords Sorted Files Search
Case Explorer
Items
Lab 1
Wind
Go
Cas... Sort...
Properties
General
Common Log Tasks
< Previous Next > Finish Cancel
P2C

Image Analyzer Options

Image Analyzer allows you to detect potentially illicit images while sorting.

☑ Use Image Analyzer

Engine sensitivity

Decrease 75 Increase

□ Use file filter

☑ Use resolution filter

File size (Kb)

From 0

To 2000000

Image size (W x H)

From 65 x 65

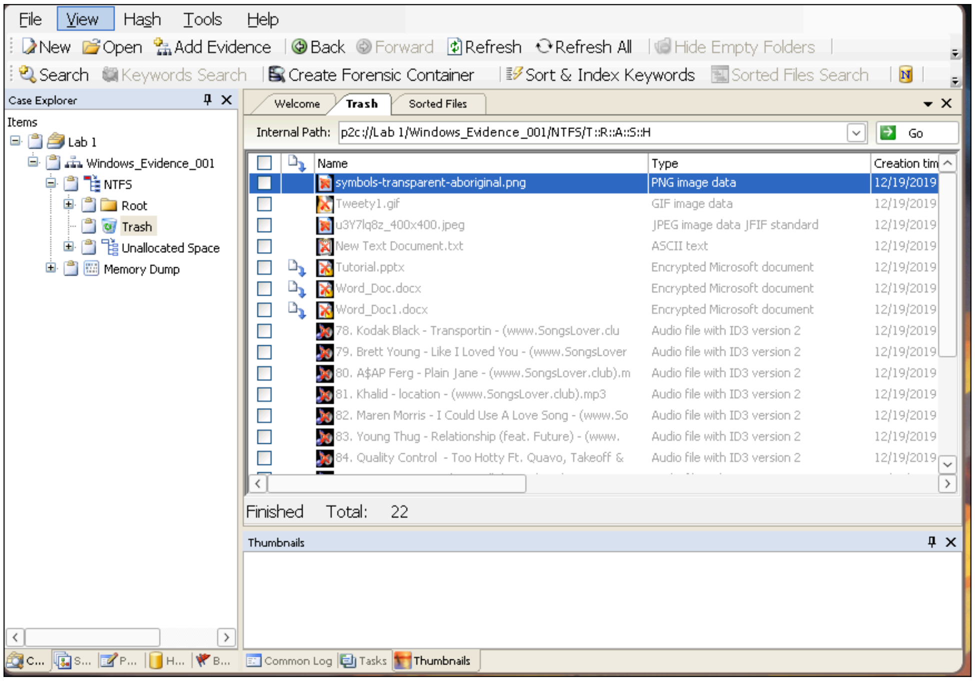
To 300000 x 300000

Description	
Investigator N.	Praneesh
Name	Lab 1

```
Add \"Trash\" folder to NTFS root: True
Add \"Partition Unallocated Space\" folder to NTFS root: True
11/25/2025 11:31:14 PM : Case \"Lab 1\" saved
```

The .dd file has been successfully added

In the trash folder, we can see all the deleted files

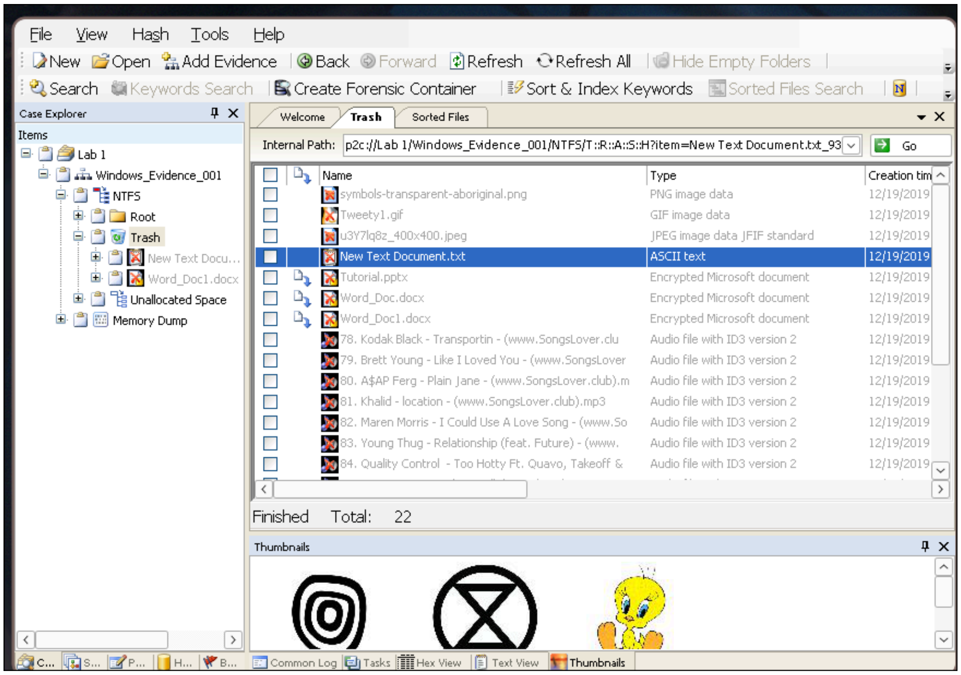


Internal Path: p2c://Lab 1/Windows_Evidence_001/NTFS/T::R::A::S::H

Name	Type	Creation tim
symbols-transparent-aboriginal.png	PNG image data	12/19/2019
Tweety1.gif	GIF image data	12/19/2019
u3Y7lq8z_400x400.jpeg	JPEG image data JFIF standard	12/19/2019
New Text Document.txt	ASCII text	12/19/2019
Tutorial.pptx	Encrypted Microsoft document	12/19/2019
Word_Doc.docx	Encrypted Microsoft document	12/19/2019
Word_Doc1.docx	Encrypted Microsoft document	12/19/2019
78. Kodak Black - Transportin - (www.SongsLover.clu	Audio file with ID3 version 2	12/19/2019
79. Brett Young - Like I Loved You - (www.SongsLover	Audio file with ID3 version 2	12/19/2019
80. A$AP Ferg - Plain Jane - (www.SongsLover.club).m	Audio file with ID3 version 2	12/19/2019
81. Khalid - location - (www.SongsLover.club).mp3	Audio file with ID3 version 2	12/19/2019
82. Maren Morris - I Could Use A Love Song - (www.So	Audio file with ID3 version 2	12/19/2019
83. Young Thug - Relationship (feat. Future) - (www.	Audio file with ID3 version 2	12/19/2019
84. Quality Control - Too Hotty Ft. Quavo, Takeoff &	Audio file with ID3 version 2	12/19/2019

Finished Total: 22

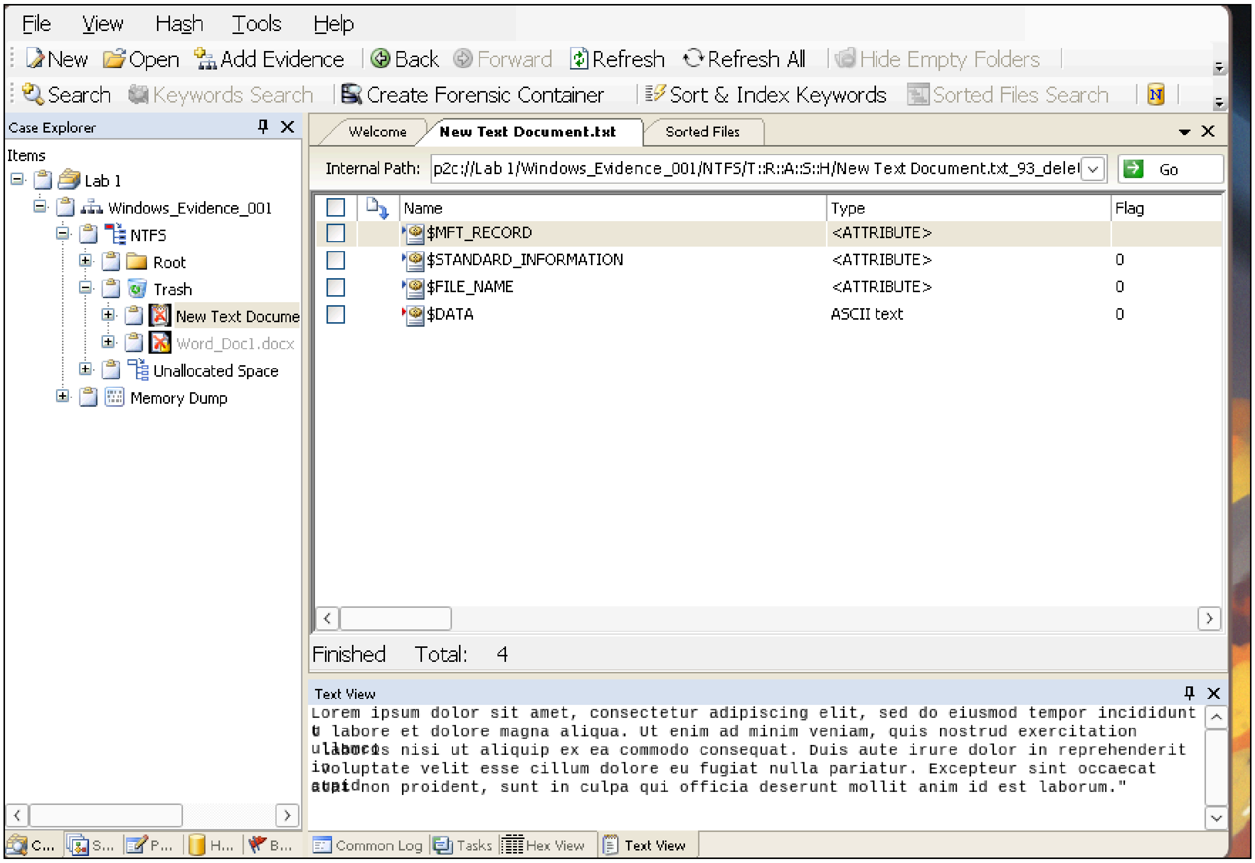
I selected this new text document.txt to see details



Internal Path: p2c://Lab 1/Windows_Evidence_001/NTFS/T::R::A::S::H?item=New Text Document.txt_93

Name	Type	Creation tim
symbols-transparent-aboriginal.png	PNG image data	12/19/2019
Tweety1.gif	GIF image data	12/19/2019
u3Y7lq8z_400x400.jpeg	JPEG image data JFIF standard	12/19/2019
New Text Document.txt	ASCII text	12/19/2019
Tutorial.pptx	Encrypted Microsoft document	12/19/2019
Word_Doc.docx	Encrypted Microsoft document	12/19/2019
Word_Doc1.docx	Encrypted Microsoft document	12/19/2019
78. Kodak Black - Transportin - (www.SongsLover.clu	Audio file with ID3 version 2	12/19/2019
79. Brett Young - Like I Loved You - (www.SongsLover	Audio file with ID3 version 2	12/19/2019
80. A$AP Ferg - Plain Jane - (www.SongsLover.club).m	Audio file with ID3 version 2	12/19/2019
81. Khalid - location - (www.SongsLover.club).mp3	Audio file with ID3 version 2	12/19/2019
82. Maren Morris - I Could Use A Love Song - (www.So	Audio file with ID3 version 2	12/19/2019
83. Young Thug - Relationship (feat. Future) - (www.	Audio file with ID3 version 2	12/19/2019
84. Quality Control - Too Hotty Ft. Quavo, Takeoff &	Audio file with ID3 version 2	12/19/2019

Finished Total: 22



Internal Path: p2c://Lab 1/Windows_Evidence_001/NTFS/T::R::A::S::H/New Text Document.txt_93_delel

□	Name	Type	Flag
□	$MFT_RECORD	<ATTRIBUTE>	
□	$STANDARD_INFORMATION	<ATTRIBUTE>	0
□	$FILE_NAME	<ATTRIBUTE>	0
□	$DATA	ASCII text	0

Finished Total: 4

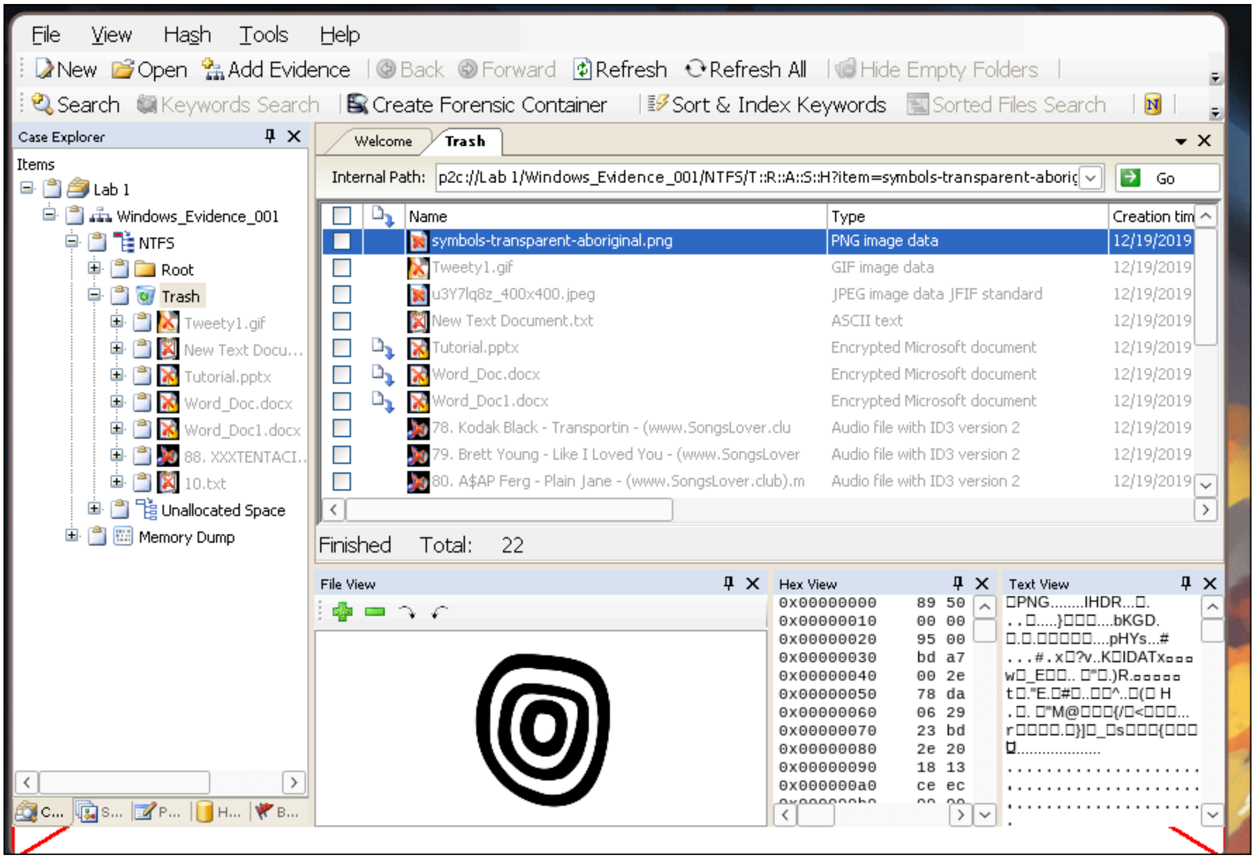
Text View

```
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt
t labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation
ullaboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit
ivoluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat
cupidnon proident, sunt in culpa qui officia deserunt mollit anim id est laborum."
```

Can see the data stored in the file

“Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.”

Selecting this file, i can see the symbol, and it’s data



Internal Path: p2c://Lab 1/Windows_Evidence_001/NTFS/T::R::A::S::H?item=symbols-transparent-aborig

□		Name	Type	Creation tim
□		symbols-transparent-aboriginal.png	PNG image data	12/19/2019
□		Tweety1.gif	GIF image data	12/19/2019
□		u3Y7lq8z_400x400.jpeg	JPEG image data JFIF standard	12/19/2019
□		New Text Document.txt	ASCII text	12/19/2019
□		Tutorial.pptx	Encrypted Microsoft document	12/19/2019
□		Word_Doc.docx	Encrypted Microsoft document	12/19/2019
□		Word_Doc1.docx	Encrypted Microsoft document	12/19/2019
□		78. Kodak Black - Transportin - (www.SongsLover.clu	Audio file with ID3 version 2	12/19/2019
□		79. Brett Young - Like I Loved You - (www.SongsLover	Audio file with ID3 version 2	12/19/2019
□		80. A$AP Ferg - Plain Jane - (www.SongsLover.club).m	Audio file with ID3 version 2	12/19/2019

Finished Total: 22

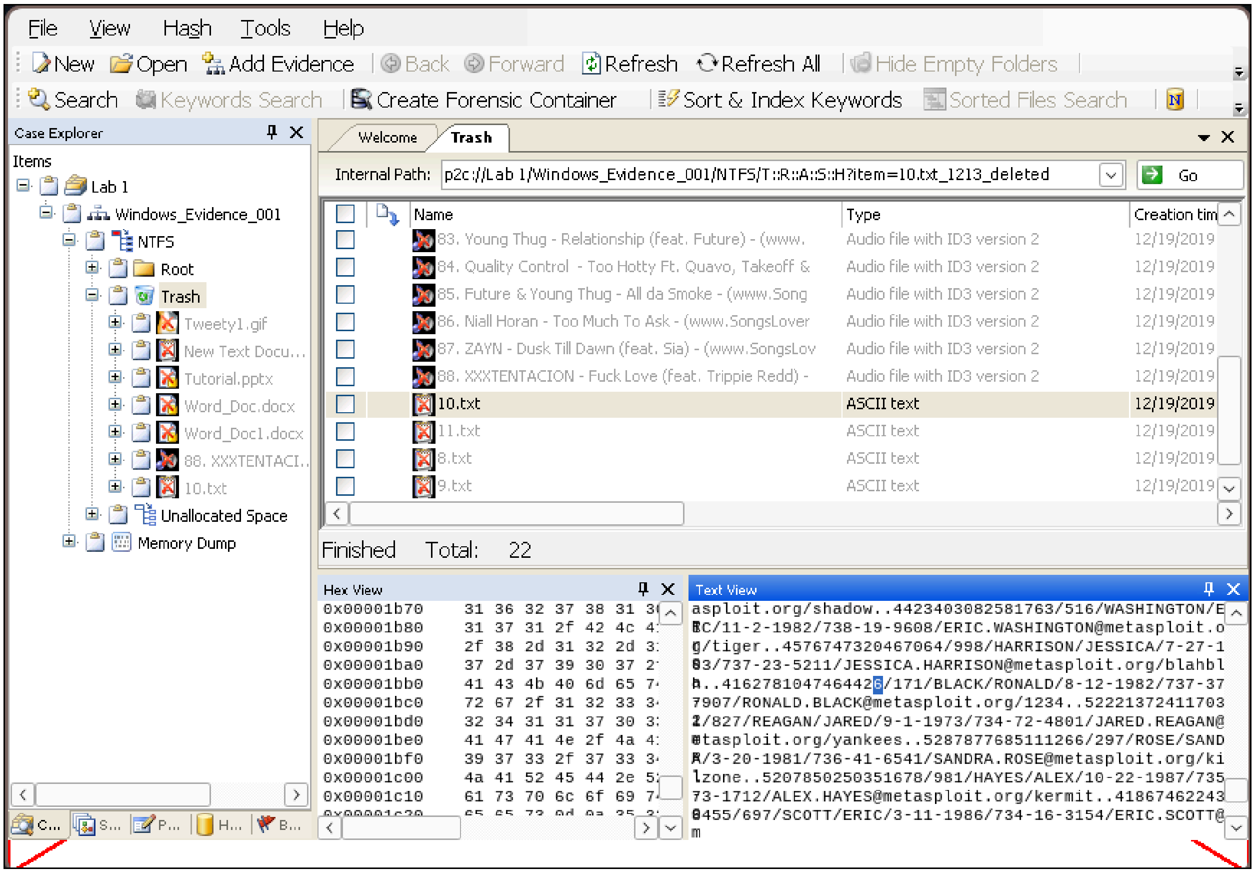
```
0x00000000   89 50
0x00000010   00 00
0x00000020   95 00
0x00000030   bd a7
0x00000040   00 2e
0x00000050   78 da
0x00000060   06 29
0x00000070   23 bd
0x00000080   2e 20
0x00000090   18 13
0x000000a0   ce ec
```

```
□PNG........IHDR...□.
..□.....}□□□....bKGD.
□.□.□□□□□....pHYs...#
...#.x□?v..K□IDATx□□□
w□_E□□.. □"□.)R.□□□□□
t□."E.□#□..□□^..□(□ H
.□. □"M@□□□{/□<□□□...
r□□□□.□}]□_□s□□□{□□□
□...................
.....................
.....................
.....................
.
```

10.txt and it’s text content, having some interesting mentions of metasploit

5211668811752783/479/BROWN/ALLEN/8-20-1979/735-75-5023/ALLEN.BROWN@metasploit.org/orioles..4571128145633021/978/MOORE/JESSICA/5-22-1972/737-89-6174/JESSICA.MOORE@metasploit.org/money..5212844336323774/185/KILBURN/JACOB/7-10-1967/736-78-3939/JACOB.KILBURN@metasploit.org/sandbox..4220463278341180/534/STOTT/ALEX/7-27-1967/737-15-2403/ALEX.STOTT@metasploit.org/sandbox...

Looks like an Info DUMP



Internal Path: p2c://Lab 1/Windows_Evidence_001/NTFS/T::R::A::S::H?item=10.txt_1213_deleted

		Name	Type	Creation tim
□		83. Young Thug - Relationship (feat. Future) - (www.	Audio file with ID3 version 2	12/19/2019
□		84. Quality Control - Too Hotty Ft. Quavo, Takeoff &	Audio file with ID3 version 2	12/19/2019
□		85. Future & Young Thug - All da Smoke - (www.Song	Audio file with ID3 version 2	12/19/2019
□		86. Niall Horan - Too Much To Ask - (www.SongsLover	Audio file with ID3 version 2	12/19/2019
□		87. ZAYN - Dusk Till Dawn (feat. Sia) - (www.SongsLov	Audio file with ID3 version 2	12/19/2019
□		88. XXXTENTACION - Fuck Love (feat. Trippie Redd) -	Audio file with ID3 version 2	12/19/2019
□		10.txt	ASCII text	12/19/2019
□		11.txt	ASCII text	12/19/2019
□		8.txt	ASCII text	12/19/2019
□		9.txt	ASCII text	12/19/2019

Finished Total: 22

```
0x00001b70     31 36 32 37 38 31 30
0x00001b80     31 37 31 2f 42 4c 4
0x00001b90     2f 38 2d 31 32 2d 3
0x00001ba0     37 2d 37 39 30 37 2
0x00001bb0     41 43 4b 40 6d 65 7
0x00001bc0     72 67 2f 31 32 33 3
0x00001bd0     32 34 31 31 37 30 3
0x00001be0     41 47 41 4e 2f 4a 4
0x00001bf0     39 37 33 2f 37 33 3
0x00001c00     4a 41 52 45 44 2e 5
0x00001c10     61 73 70 6c 6f 69 7
```

```
asploit.org/shadow..4423403082581763/516/WASHINGTON/E
RC/11-2-1982/738-19-9608/ERIC.WASHINGTON@metasploit.o
g/tiger..4576747320467064/998/HARRISON/JESSICA/7-27-1
83/737-23-5211/JESSICA.HARRISON@metasploit.org/blahbl
a..4162781047464426/171/BLACK/RONALD/8-12-1982/737-37
7907/RONALD.BLACK@metasploit.org/1234..52221372411703
2/827/REAGAN/JARED/9-1-1973/734-72-4801/JARED.REAGAN@
etasploit.org/yankees..5287877685111266/297/ROSE/SAND
A/3-20-1981/736-41-6541/SANDRA.ROSE@metasploit.org/ki
lzone..5207850250351678/981/HAYES/ALEX/10-22-1987/735
73-1712/ALEX.HAYES@metasploit.org/kermit..41867462243
0455/697/SCOTT/ERIC/3-11-1986/734-16-3154/ERIC.SCOTT@
m
```