PRACTICAL: 2

Using Forensic Tool: Autopsy.

Aim

To demonstrate the recovery of deleted files using the Autopsy Digital Forensics Tool by creating a forensic image with FTK Imager, deleting selected files, and analyzing the image in Autopsy.

System Prerequisites

- Computer system with Windows Operating System
- FTK Imager installed on the system
- Autopsy installed on the system
- Minimum 4 GB RAM (8 GB recommended)
- Sufficient free disk space to store image and case files
- Administrator privileges on the system

Tools Required

- FTK Imager
- Autopsy Digital Forensics Tool
- External storage device or test folder
- Sample test files (documents, images, text files, etc.)

About Autopsy

Autopsy is an open-source digital forensics platform used for analyzing disk images and recovering digital evidence. It provides a graphical interface for The Sleuth Kit and allows investigators to examine file systems, recover deleted files, analyze metadata, and generate forensic reports. Autopsy is widely used in academic laboratories and professional investigations for post-acquisition forensic analysis.

Procedure (Attach Screenshots for Each Step)

Step 1: Create Test Files

1. Create a folder on the system (e.g., Test_Evidence).
2. Add five test files of different types (e.g., .txt, .pdf, .jpg, .docx, .png).

Step 2: Create Forensic Image Using FTK Imager

3. Open FTK Imager with administrator privileges.
4. Click File → Create Disk Image.
5. Select Contents of a Folder and choose the *Test_Evidence* folder.

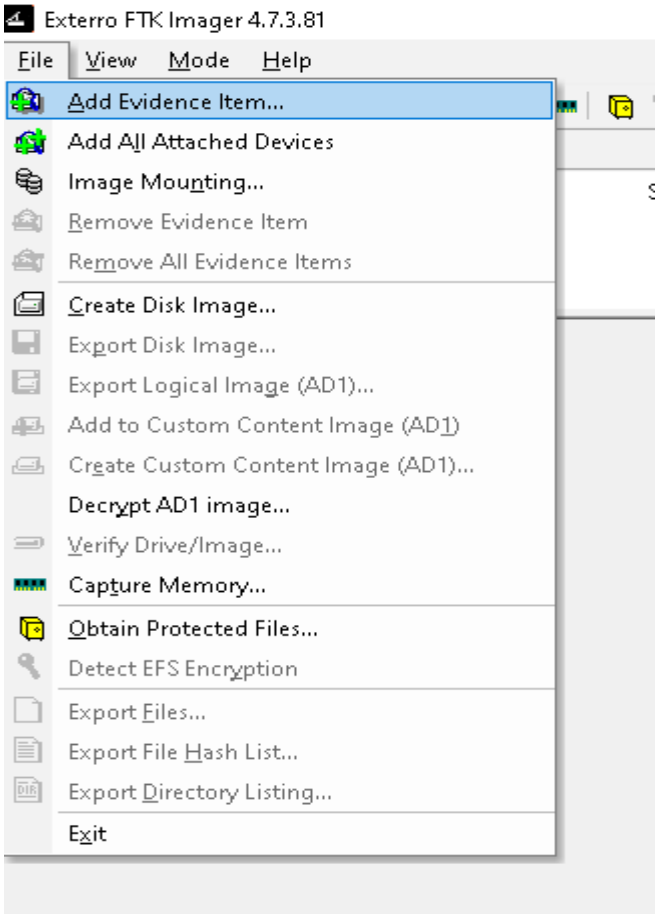
6. Select the image format (RAW or E01).
7. Enter case details and choose a destination path.
8. Enable hash calculation and start imaging.
9. Wait for the image creation to complete and verify hash values.

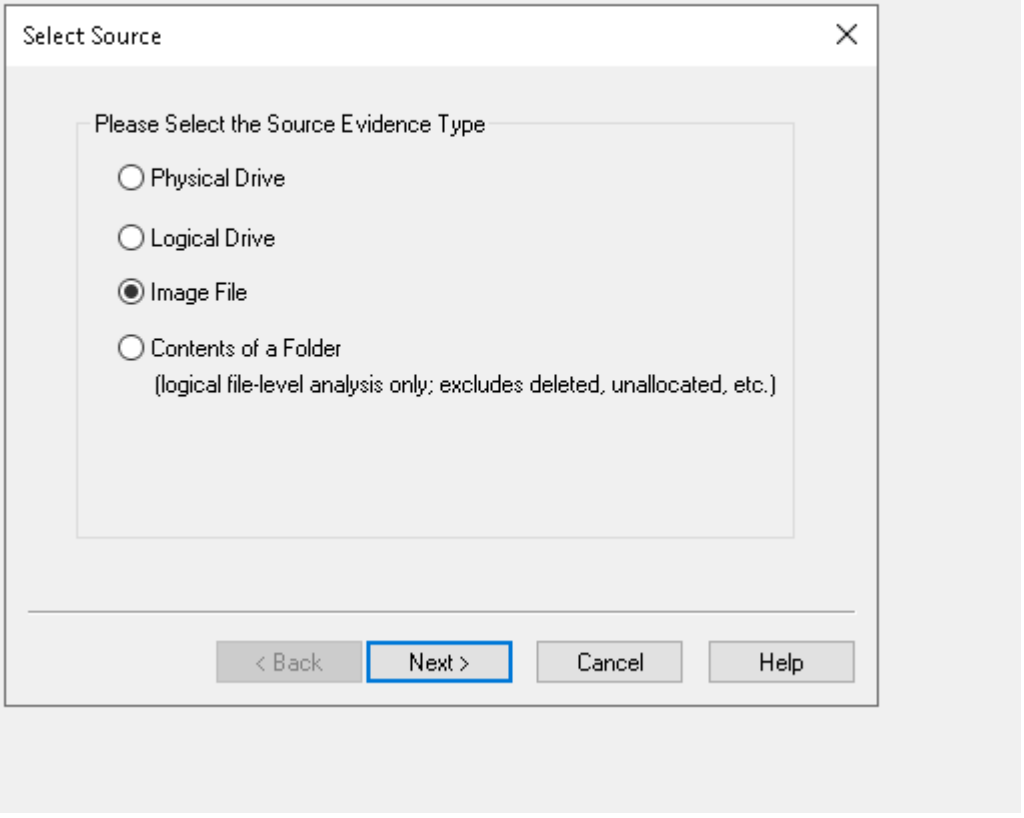
Step 3: Delete Test Files

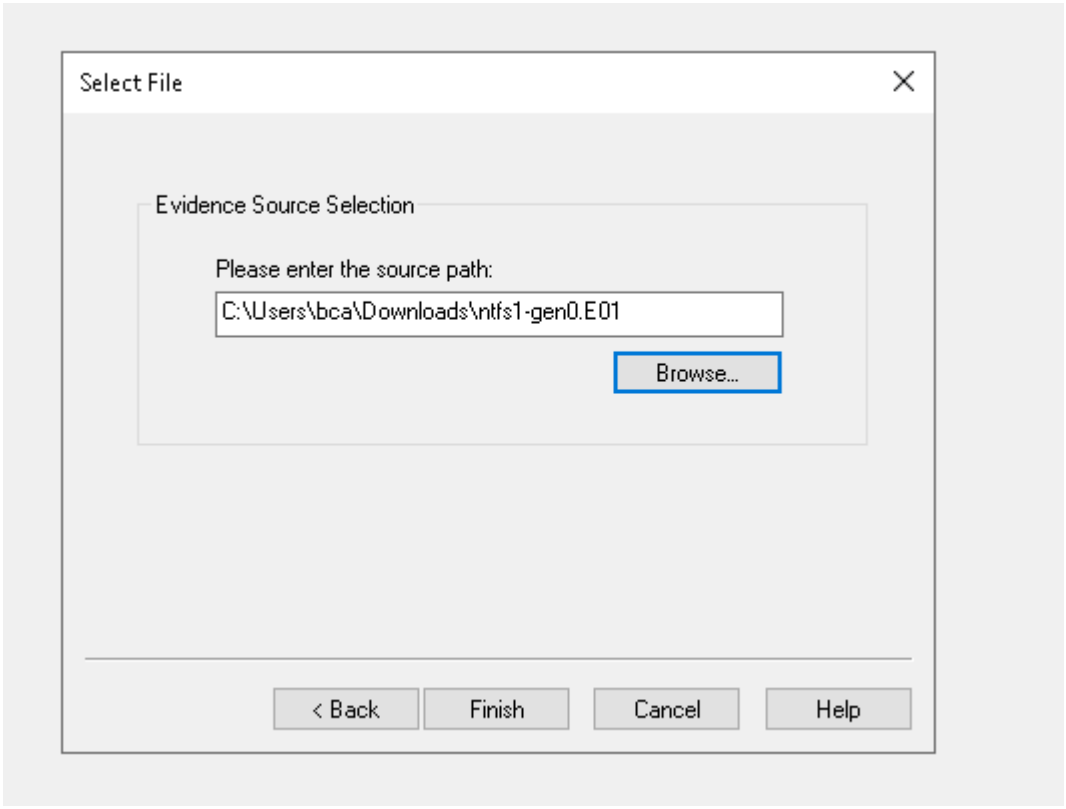
10. Go to the original *Test_Evidence* folder.
11. Delete all five test files.
12. Empty the Recycle Bin to ensure permanent deletion.

Step 4: Analyze and Recover Files Using Autopsy

13. Launch Autopsy and create a New Case.
14. Enter case name, examiner details, and select case directory.
15. Add data source → Disk Image or VM File.
16. Browse and select the forensic image created using FTK Imager.
17. Configure ingest modules (file system, deleted file recovery, hash lookup).
18. Start the analysis process.
19. Navigate to Deleted Files section.
20. Identify and recover the deleted test files.
21. Export recovered files if required.


Exterro FTK Imager 4.7.3.81
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit


Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help



Exterro FTK Imager 4.7.3.81

File View Mode Help

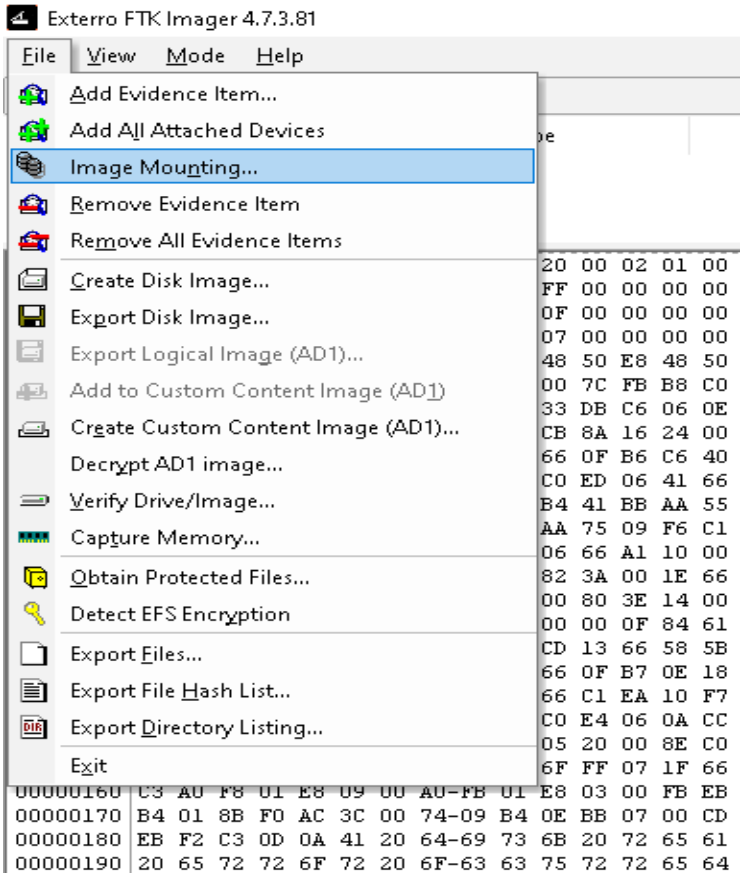
File List

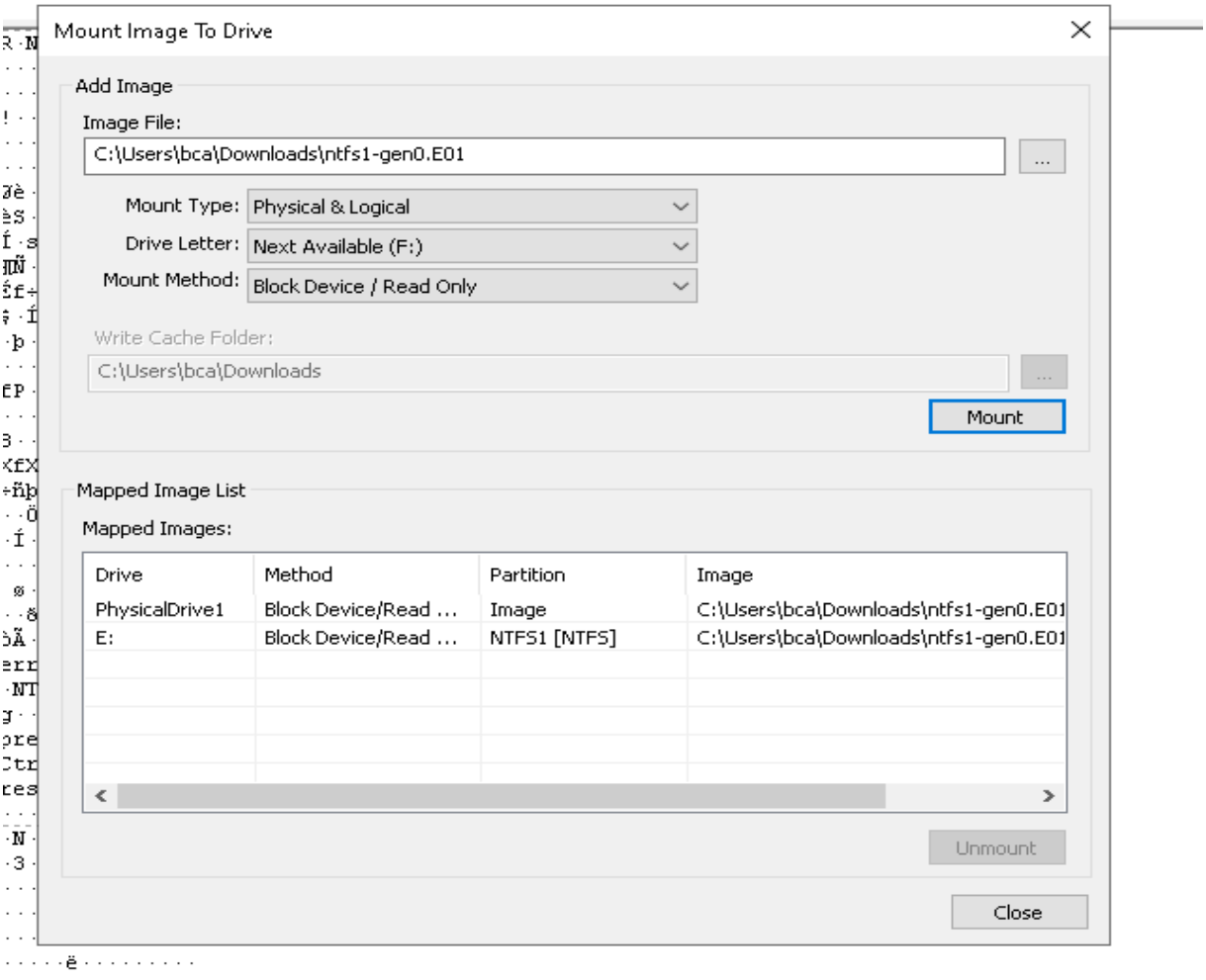
Name	Type	Size	Date Modified

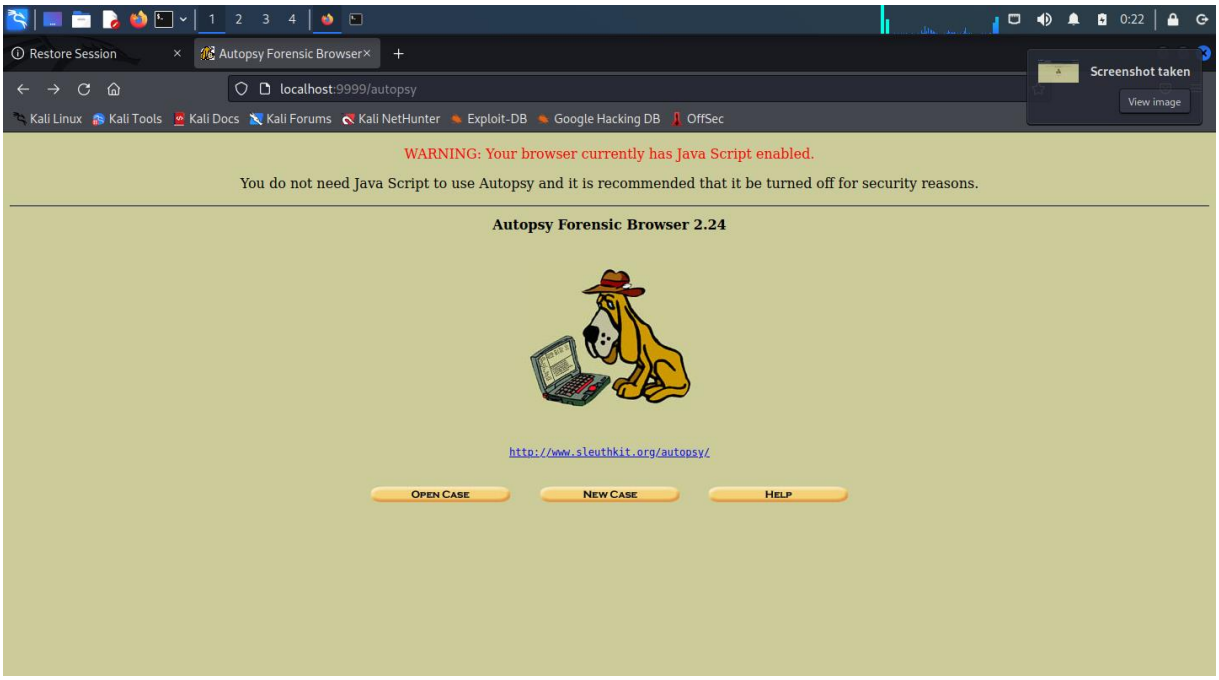
```
00000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 01 00 00  ëR·NTFS   ····
00000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 00 00 00  ·····ø··?·ÿ·····
00000020 00 00 00 00 80 00 00 00-FF 64 0F 00 00 00 00 00  ·····ÿd·····
00000030 AA 21 05 00 00 00 00 00-7F B2 07 00 00 00 00 00  ª!·····²·····
00000040 02 00 00 00 08 00 00 00-C7 CC 48 50 E8 48 50 DA  ·····ÇÌHPèHPÚ
00000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB B8 C0 07  ····ú3À·Ð¼·|û¸À·
00000060 8E D8 E8 16 00 B8 00 0D-8E C0 33 DB C6 06 0E 00  ·Øè··¸···À3ÛÆ···
00000070 10 E8 53 00 68 00 0D 68-6A 02 CB 8A 16 24 00 B4  ·èS·h··hj·Ë··$·´
00000080 08 CD 13 73 05 B9 FF FF-8A F1 66 0F B6 C6 40 66  ·Í·s·¹ÿÿ·ñf·¶Æ@f
00000090 0F B6 D1 80 E2 3F F7 E2-86 CD C0 ED 06 41 66 0F  ·¶Ñ·â?÷â·ÍÀí·Af·
000000a0 B7 C9 66 F7 E1 66 A3 20-00 C3 B4 41 BB AA 55 8A  ·Éf÷áf£ ·Ã´A»ªU·
000000b0 16 24 00 CD 13 72 0F 81-FB 55 AA 75 09 F6 C1 01  ·$·Í·r··ûUªu·öÁ·
000000c0 74 04 FE 06 14 00 C3 66-60 1E 06 66 A1 10 00 66  t·þ···Ãf`··f¡··f
000000d0 03 06 1C 00 66 3B 06 20-00 0F 82 3A 00 1E 66 6A  ····f;· ···:··fj
000000e0 00 66 50 06 53 66 68 10-00 01 00 80 3E 14 00 00  ·fP·Sfh·····>···
000000f0 0F 85 0C 00 E8 B3 FF 80-3E 14 00 00 0F 84 61 00  ····è³ÿ·>·····a·
00000100 B4 42 8A 16 24 00 16 1F-8B F4 CD 13 66 58 5B 07  ´B··$····ôÍ·fX[·
00000110 66 58 66 58 1F EB 2D 66-33 D2 66 0F B7 0E 18 00  fXfX·ë-f3Òf·····
00000120 66 F7 F1 FE C2 8A CA 66-8B D0 66 C1 EA 10 F7 36  f÷ñþÂ·Êf·ÐfÁê·÷6
00000130 1A 00 86 D6 8A 16 24 00-8A E8 C0 E4 06 0A CC B8  ···Ö··$··ÈÀä···Ì¸
00000140 01 02 CD 13 0F 82 19 00-8C C0 05 20 00 8E C0 66  ··Í·····À· ··Àf
00000150 FF 06 10 00 FF 0E 0E 00-0F 85 6F FF 07 1F 66 61  ÿ···ÿ·····oÿ··fa
00000160 C3 A0 F8 01 E8 09 00 A0-FB 01 E8 03 00 FB EB FE  Ã ø·è·· û·è··ûëþ
00000170 B4 01 8B F0 AC 3C 00 74-09 B4 0E BB 07 00 CD 10  ´·ð¬<·t·´·»··Í·
00000180 EB F2 C3 0D 0A 41 20 64-69 73 6B 20 72 65 61 64  ëòÃ··A disk read
00000190 20 65 72 72 6F 72 20 6F-63 63 75 72 72 65 64 00   error occurred·
000001a0 0D 0A 4E 54 4C 44 52 20-69 73 20 6D 69 73 73 69  ··NTLDR is missi
000001b0 6E 67 00 0D 0A 4E 54 4C-44 52 20 69 73 20 63 6F  ng···NTLDR is co
000001c0 6D 70 72 65 73 73 65 64-00 0D 0A 50 72 65 73 73  mpressed···Press
000001d0 20 43 74 72 6C 2B 41 6C-74 2B 44 65 6C 20 74 6F   Ctrl+Alt+Del to
000001e0 20 72 65 73 74 61 72 74-0D 0A 00 00 00 00 00 00   restart·····
000001f0 00 00 00 00 00 00 00 00-83 A0 B3 C9 00 00 55 AA  ·········³É··Uª
00000200 05 00 4E 00 54 00 4C 00-44 00 52 00 04 00 24 00  ··N·T·L·D·R···$·
00000210 49 00 33 00 30 00 00 E0-00 00 00 30 00 00 00 00  I·3·0··à···0····
00000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ····************
00000230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ····************
00000240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ····************
00000250 00 00 00 00 00 00 EB 12-90 90 00 00 00 00 00 00  ·····ë·········
00000260 00 00 00 00 00 00 00 00-00 00 8C C8 8E D8 C1 E0  ··········È·ØÁà
00000270 04 FA 8B E0 FB E8 03 FE-66 0F B7 06 0B 00 66 0F  ·ú·àûè·þf·····f·
00000280 B6 1E 0D 00 66 F7 E3 66-A3 4E 02 66 8B 0E 40 00  ¶···f÷ãf£N·f··@·
00000290 80 F9 00 0F 8F 0E 00 F6-D9 66 B8 01 00 00 00 66  ·ù·····öÙf¸····f
000002a0 D3 E0 EB 08 90 66 A1 4E-02 66 F7 E1 66 A3 52 02  Óàë··f¡N·f÷áf£R·
000002b0 66 0F B7 1E 0B 00 66 33-D2 66 F7 F3 66 A3 56 02  f·····f3Òf÷óf£V·
```

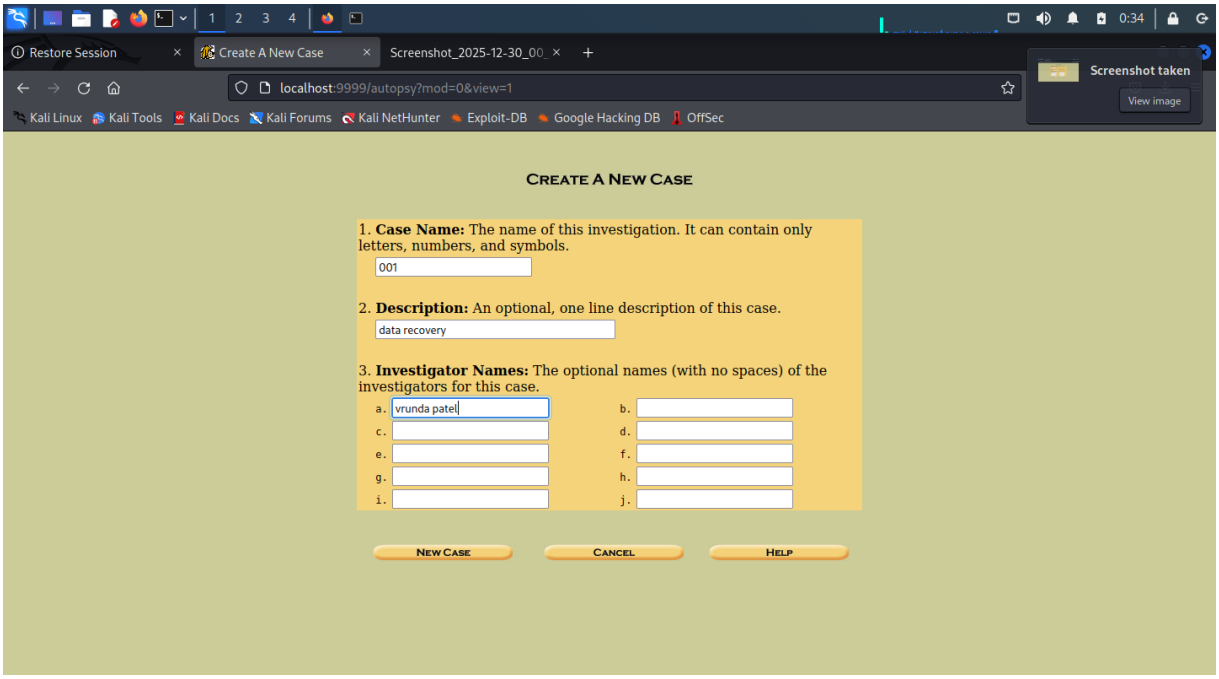
Cursor pos = 336; log sec = 0

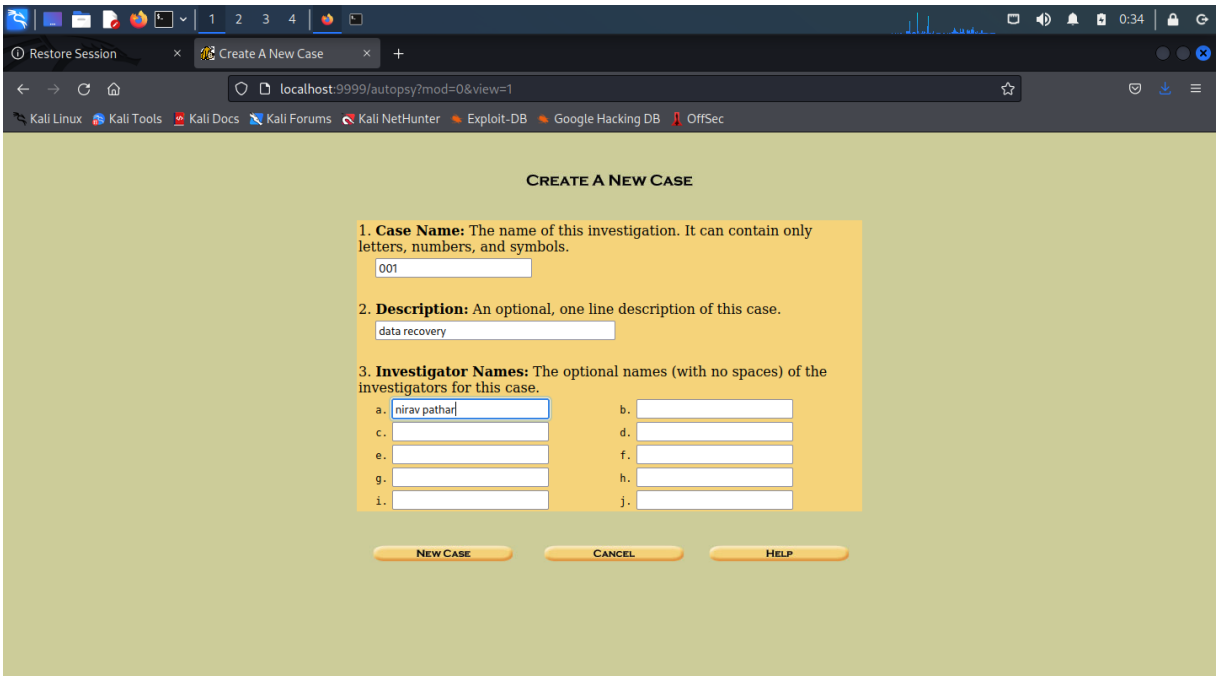
For User Guide, press F1

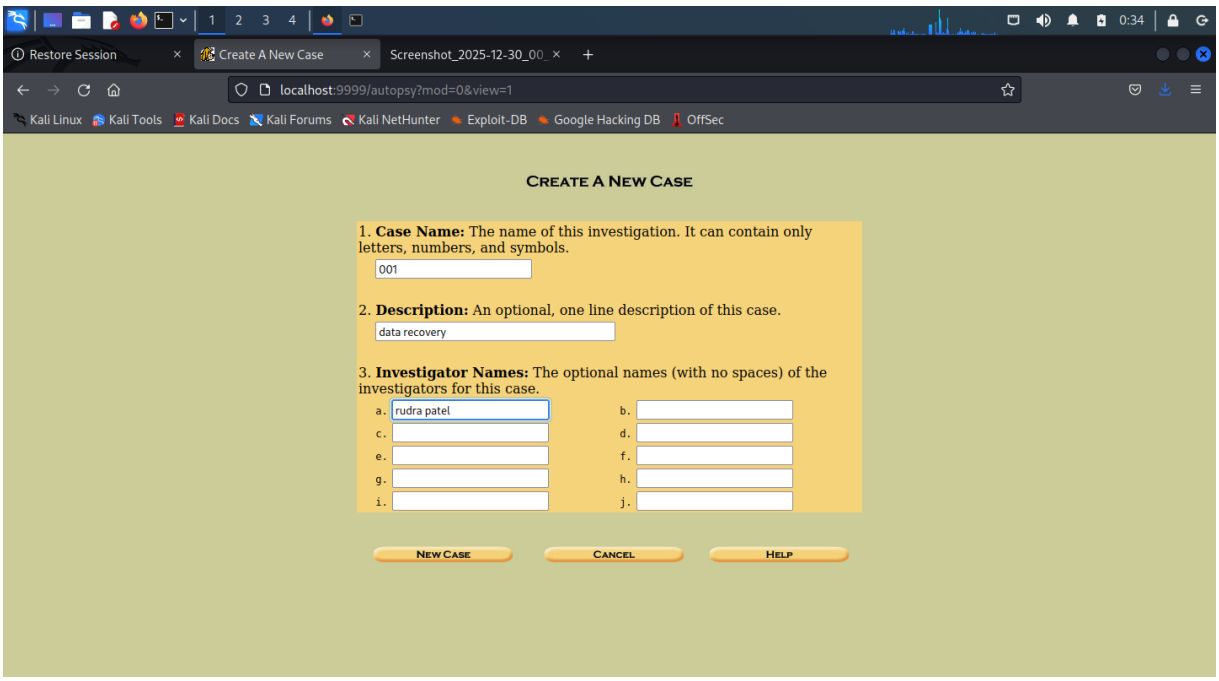

Exterro FTK Imager 4.7.3.81
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit

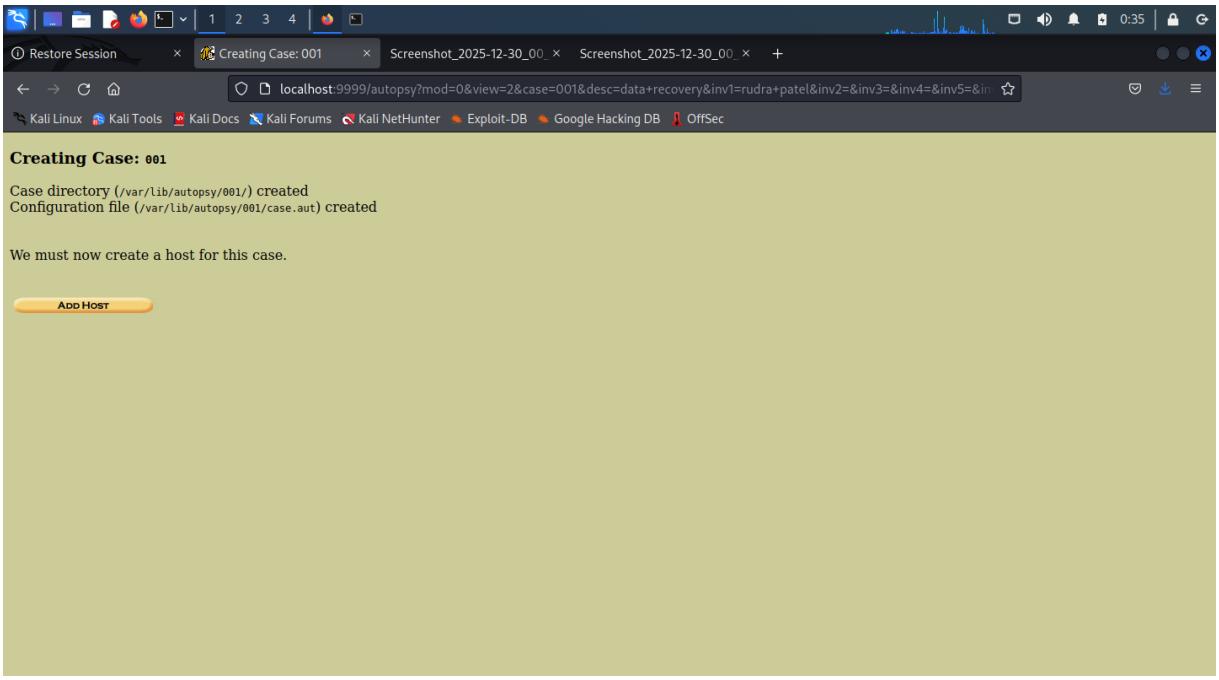

Mount Image To Drive
Add Image
Image File:
C:\Users\bca\Downloads\ntfs1-gen0.E01
Mount Type:
Physical & Logical
Drive Letter:
Next Available (F:)
Mount Method:
Block Device / Read Only
Write Cache Folder:
C:\Users\bca\Downloads
Mount
Mapped Image List
Mapped Images:
Drive
Method
Partition
Image
PhysicalDrive1
Block Device/Read ...
Image
C:\Users\bca\Downloads\ntfs1-gen0.E01
E:
Block Device/Read ...
NTFS1 [NTFS]
C:\Users\bca\Downloads\ntfs1-gen0.E01
Unmount
Close

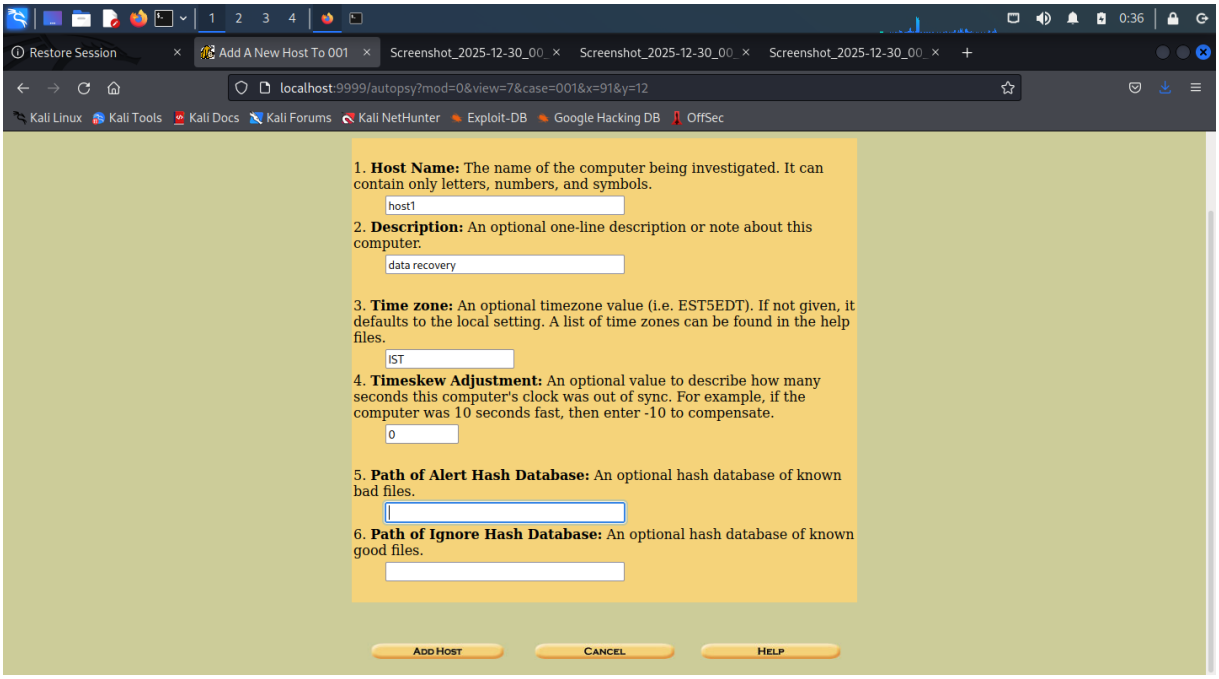

Restore Session
Autopsy Forensic Browser
localhost:9999/autopsy
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Screenshot taken
View image
WARNING: Your browser currently has Java Script enabled.
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.
Autopsy Forensic Browser 2.24
http://www.sleuthkit.org/autopsy/
OPEN CASE
NEW CASE
HELP

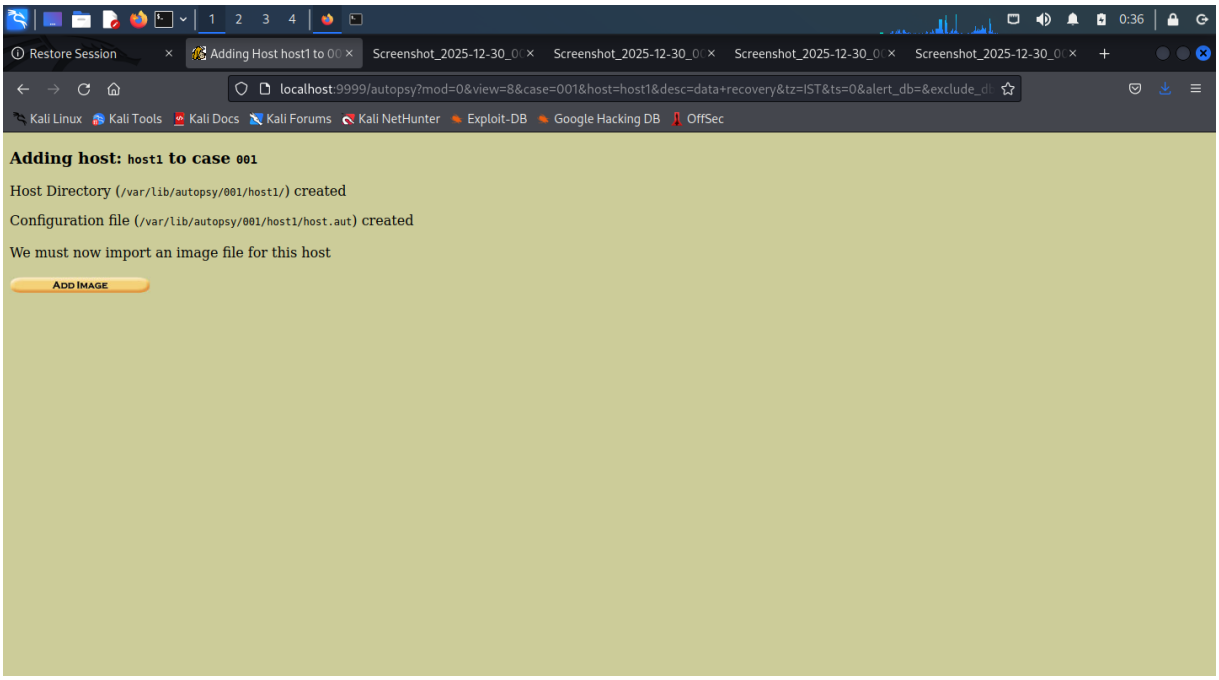

Restore Session
Create A New Case
localhost:9999/autopsy?mod=0&view=1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Screenshot taken
View image
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
001
2. Description: An optional, one line description of this case.
data recovery
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. vrunda patel
b.
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP

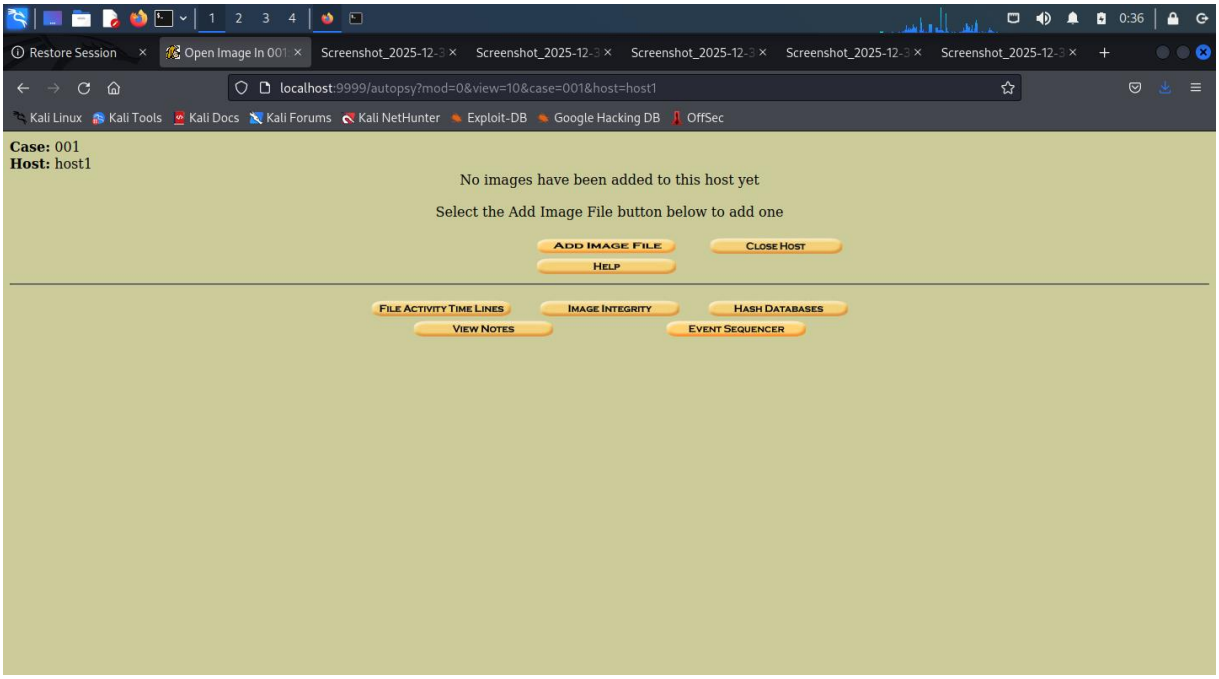

Restore Session
Create A New Case
localhost:9999/autopsy?mod=0&view=1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
001
2. Description: An optional, one line description of this case.
data recovery
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. nirav pathar
b.
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP

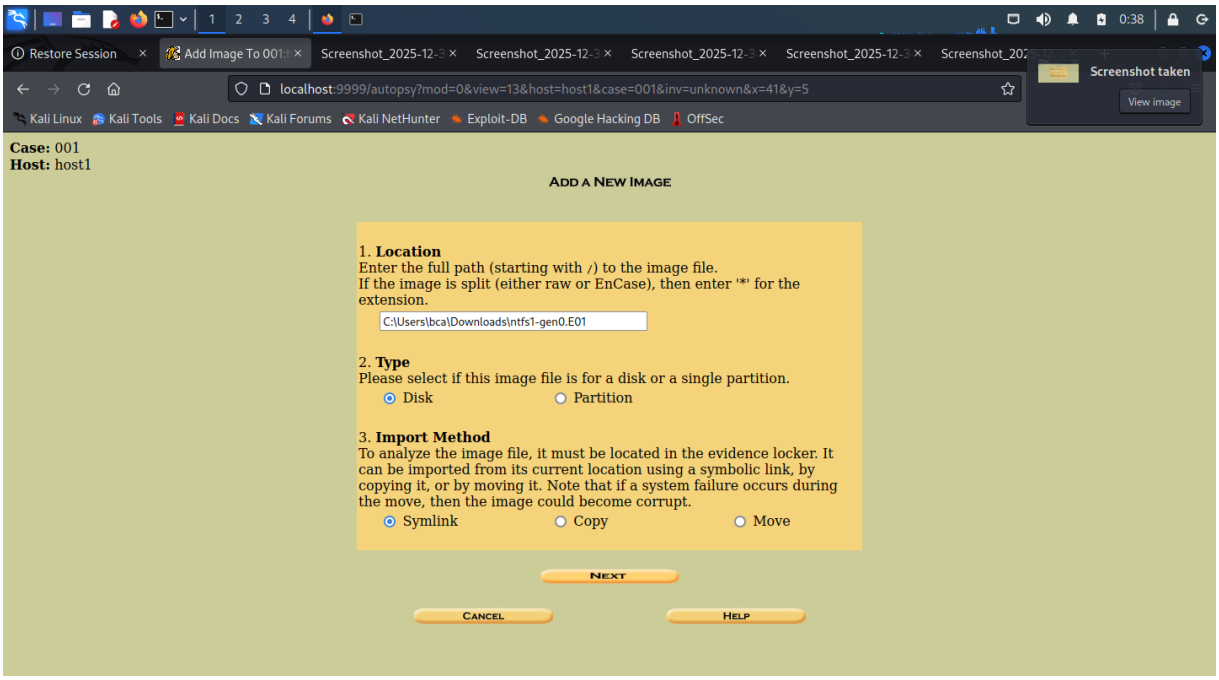

Restore Session
Create A New Case
Screenshot_2025-12-30_00
localhost:9999/autopsy?mod=0&view=1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
001
2. Description: An optional, one line description of this case.
data recovery
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. rudra patel
b.
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP

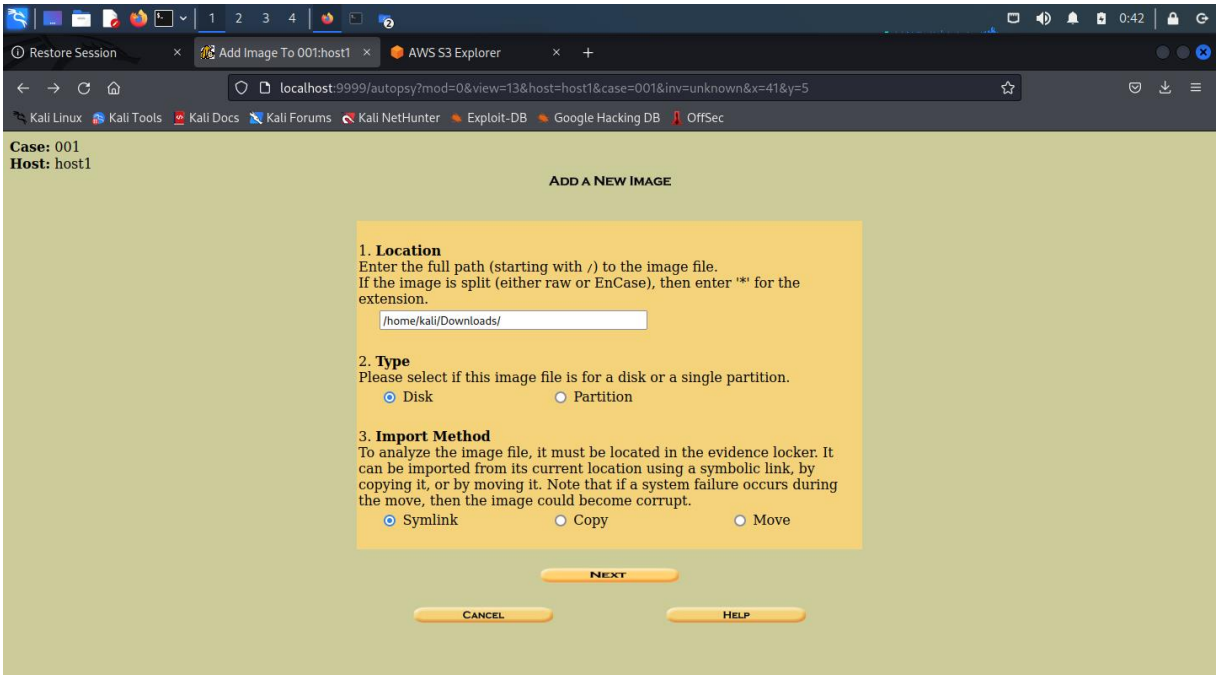

Restore Session
Creating Case: 001
Screenshot_2025-12-30_00_
Screenshot_2025-12-30_00_
localhost:9999/autopsy?mod=0&view=2&case=001&desc=data+recovery&inv1=rudra+patel&inv2=&inv3=&inv4=&inv5=&in
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Creating Case: 001
Case directory (/var/lib/autopsy/001/) created
Configuration file (/var/lib/autopsy/001/case.aut) created
We must now create a host for this case.
ADD HOST

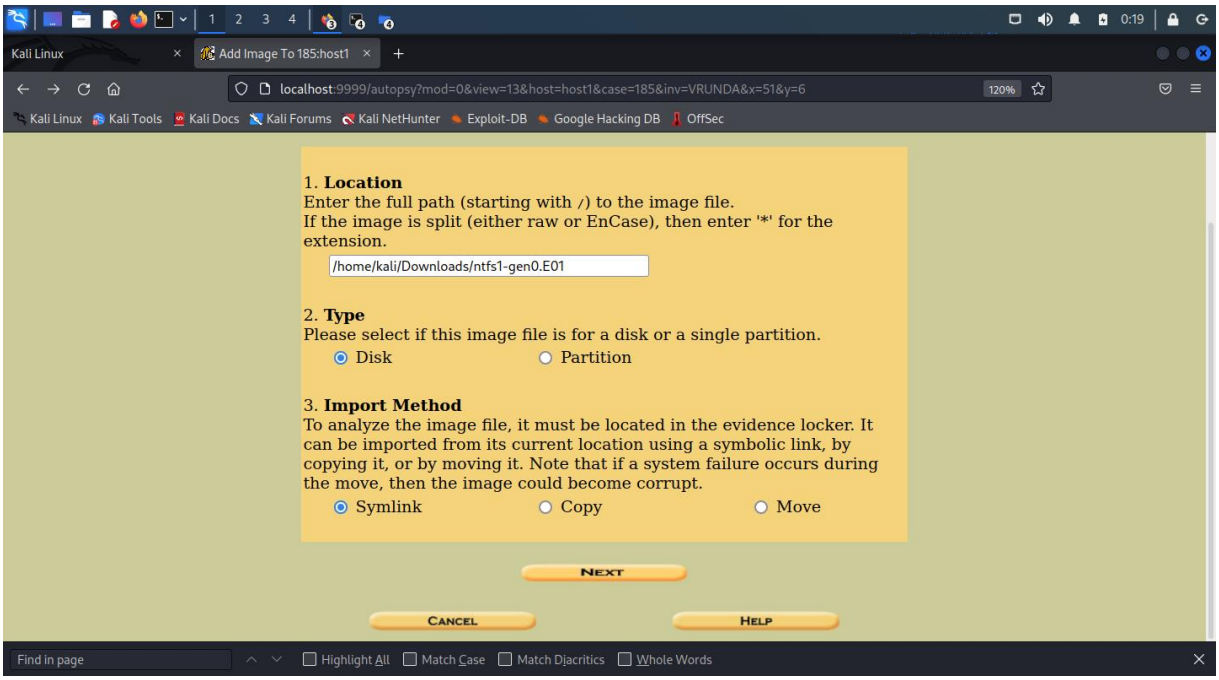

Restore Session
Add A New Host To 001
Screenshot_2025-12-30_00_
Screenshot_2025-12-30_00_
Screenshot_2025-12-30_00_
localhost:9999/autopsy?mod=0&view=7&case=001&x=91&y=12
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
host1
2. Description: An optional one-line description or note about this computer.
data recovery
3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
IST
4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0
5. Path of Alert Hash Database: An optional hash database of known bad files.
6. Path of Ignore Hash Database: An optional hash database of known good files.
ADD HOST
CANCEL
HELP

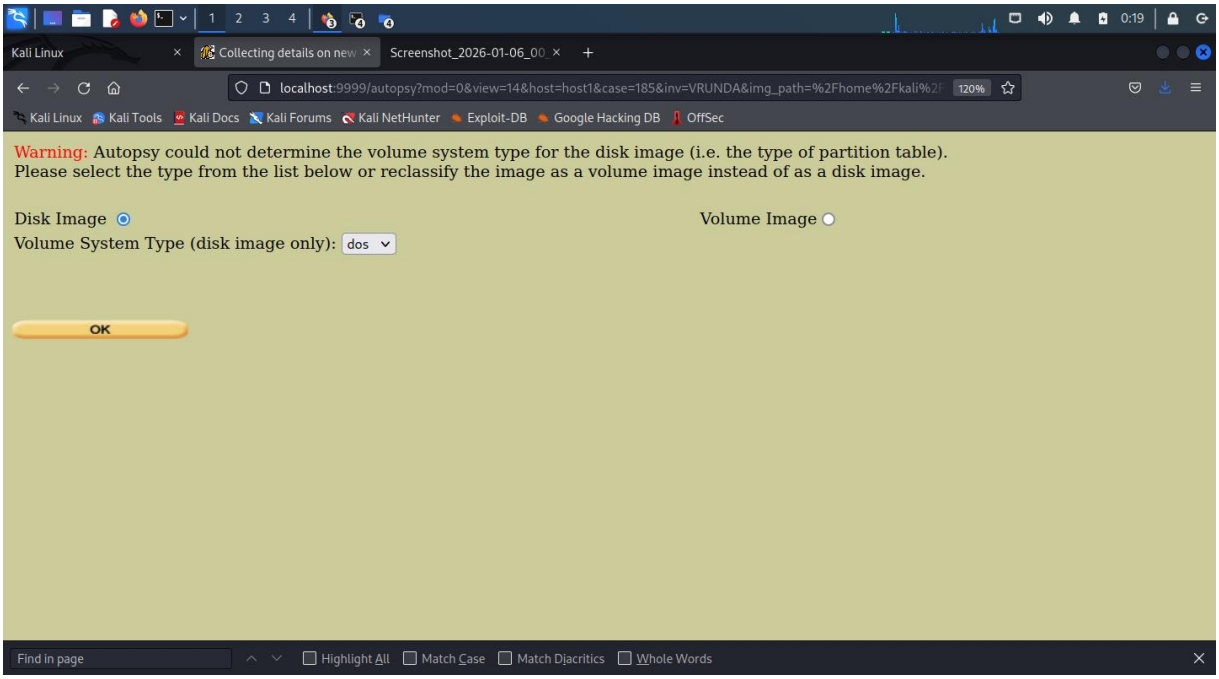

Restore Session
Adding Host host1 to 00
Screenshot_2025-12-30_0
localhost:9999/autopsy?mod=0&view=8&case=001&host=host1&desc=data+recovery&tz=IST&ts=0&alert_db=&exclude_d
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Adding host: host1 to case 001
Host Directory (/var/lib/autopsy/001/host1/) created
Configuration file (/var/lib/autopsy/001/host1/host.aut) created
We must now import an image file for this host
ADD IMAGE

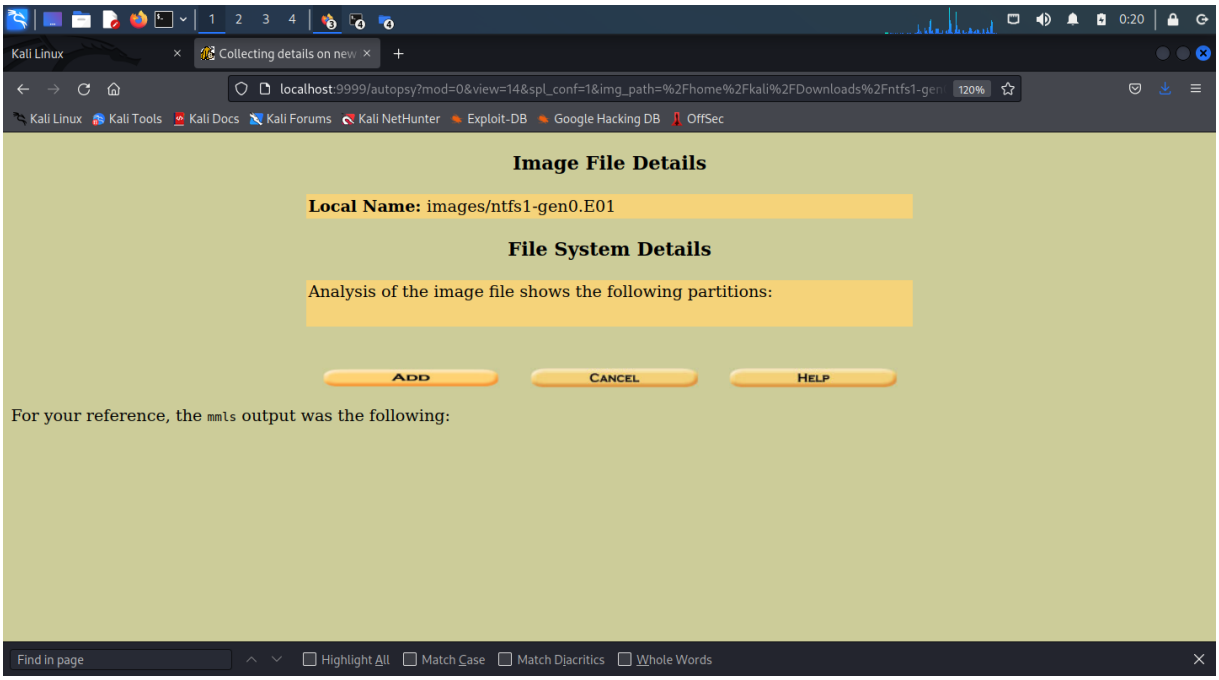

Restore Session
Open Image In 001
Screenshot_2025-12-3
localhost:9999/autopsy?mod=0&view=10&case=001&host=host1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Case: 001
Host: host1
No images have been added to this host yet
Select the Add Image File button below to add one
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER

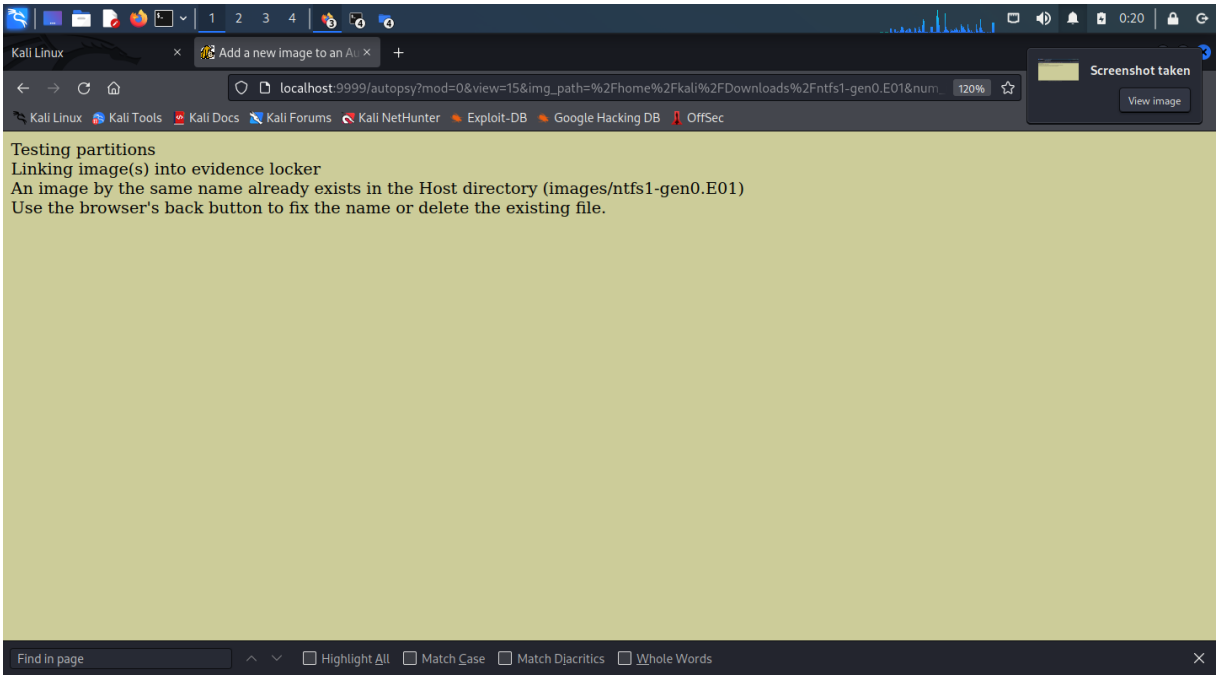

Restore Session
Add Image To 001:
Screenshot_2025-12-
Screenshot taken
View image
localhost:9999/autopsy?mod=0&view=13&host=host1&case=001&inv=unknown&x=41&y=5
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Case: 001
Host: host1
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
C:\Users\bca\Downloads\ntfs1-gen0.E01
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink
Copy
Move
NEXT
CANCEL
HELP

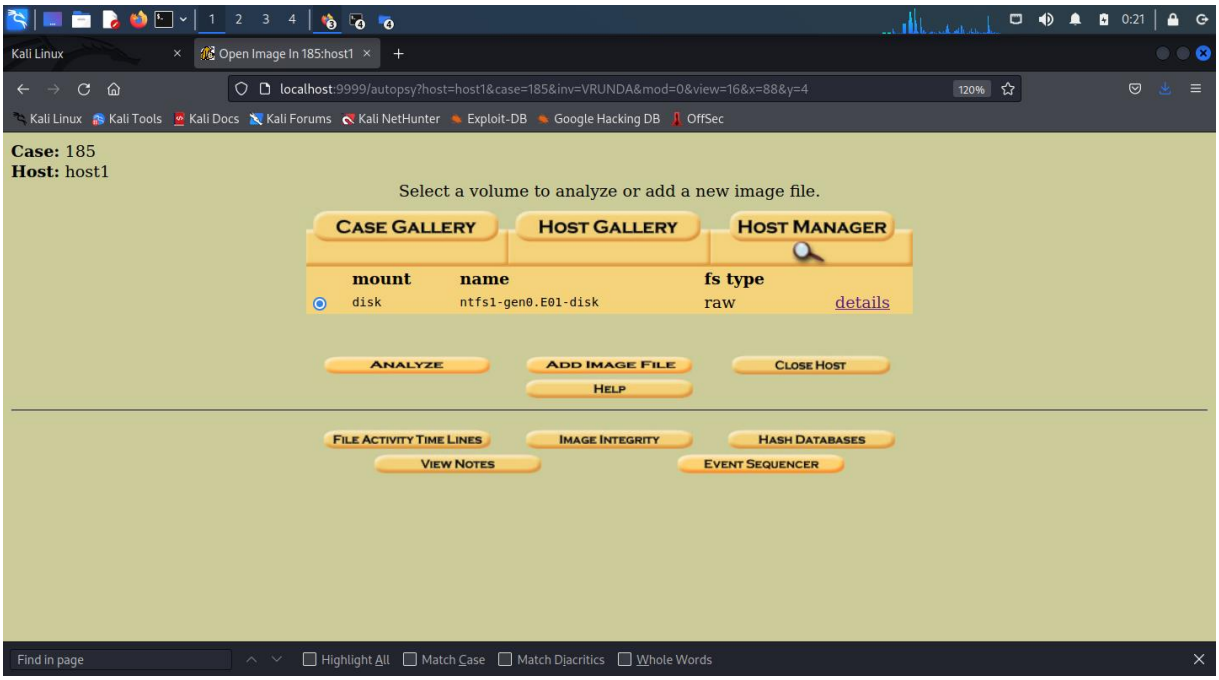

Restore Session
Add Image To 001:host1
AWS S3 Explorer
localhost:9999/autopsy?mod=0&view=13&host=host1&case=001&inv=unknown&x=41&y=5
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Case: 001
Host: host1
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/kali/Downloads/
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink
Copy
Move
NEXT
CANCEL
HELP

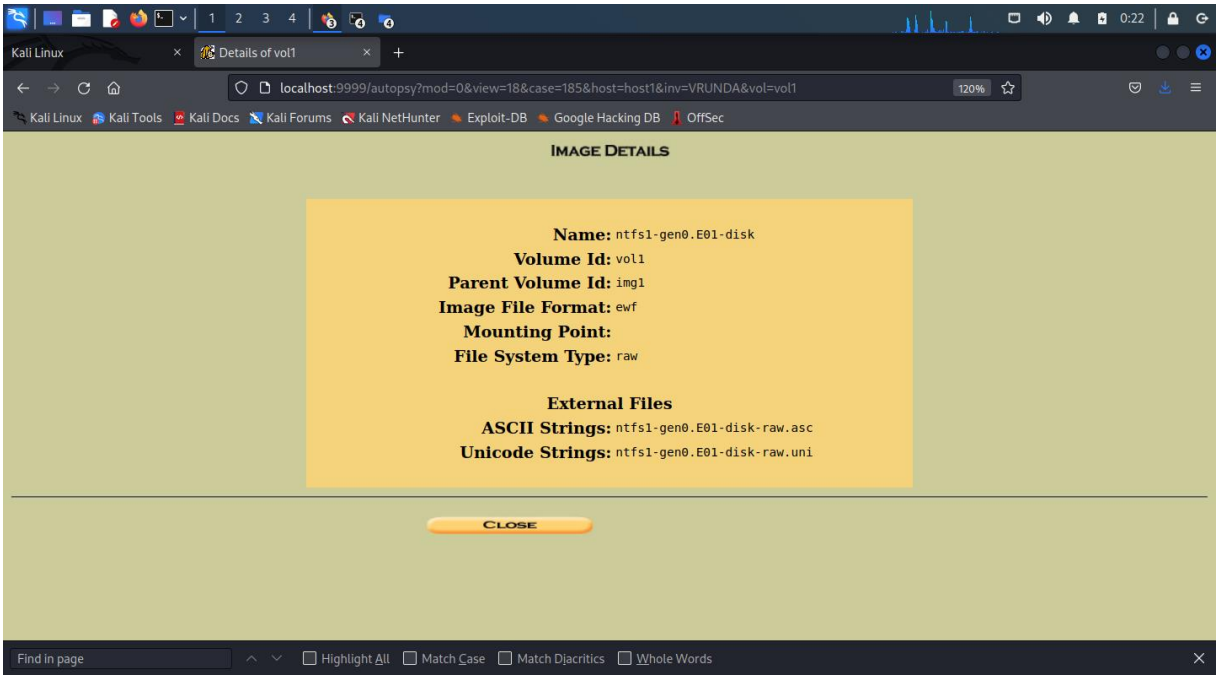

Kali Linux
Add Image To 185:host1
localhost:9999/autopsy?mod=0&view=13&host=host1&case=185&inv=VRUNDA&x=51&y=6
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/kali/Downloads/ntfs1-gen0.E01
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink
Copy
Move
NEXT
CANCEL
HELP
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words


Kali Linux
Collecting details on new
Screenshot_2026-01-06_00
localhost:9999/autopsy?mod=0&view=14&host=host1&case=185&inv=VRUNDA&img_path=%2Fhome%2Fkali%2F
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table).
Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.
Disk Image
Volume Image
Volume System Type (disk image only):
dos
OK
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words


Kali Linux
Collecting details on new
localhost:9999/autopsy?mod=0&view=14&spl_conf=1&img_path=%2Fhome%2Fkali%2FDownloads%2Fntfs1-gen
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Image File Details
Local Name: images/ntfs1-gen0.E01
File System Details
Analysis of the image file shows the following partitions:
ADD
CANCEL
HELP
For your reference, the mmls output was the following:
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words


Kali Linux
Add a new image to an Au
localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fkali%2FDownloads%2Fntfs1-gen0.E01&num
120%
Screenshot taken
View image
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Testing partitions
Linking image(s) into evidence locker
An image by the same name already exists in the Host directory (images/ntfs1-gen0.E01)
Use the browser's back button to fix the name or delete the existing file.
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words


Kali Linux
Open Image In 185:host1
localhost:9999/autopsy?host=host1&case=185&inv=VRUNDA&mod=0&view=16&x=88&y=4
120%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Case: 185
Host: host1
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
disk
ntfs1-gen0.E01-disk
raw
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words


Kali Linux
Details of vol1
localhost:9999/autopsy?mod=0&view=18&case=185&host=host1&inv=VRUNDA&vol=vol1
120%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
IMAGE DETAILS
Name: ntfs1-gen0.E01-disk
Volume Id: vol1
Parent Volume Id: img1
Image File Format: ewf
Mounting Point:
File System Type: raw
External Files
ASCII Strings: ntfs1-gen0.E01-disk-raw.asc
Unicode Strings: ntfs1-gen0.E01-disk-raw.uni
CLOSE
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words

Observation

- Forensic image successfully loaded into Autopsy
- Deleted files were identified and recovered
- File metadata and timestamps were visible

Conclusion

The experiment successfully demonstrated the recovery of deleted files using Autopsy. By creating a forensic image with FTK Imager before deletion, evidence integrity was preserved. Autopsy effectively analyzed the image and recovered deleted files, proving its usefulness in digital forensic investigations.