

# Lab Report

Karthikeyan G

Roll Number: CB.SC.P2CYS24008

December 25, 2024

## *Lab1: Recovering Deleted Files from Hard Disks Using WinHex*

### **Lab Scenario**

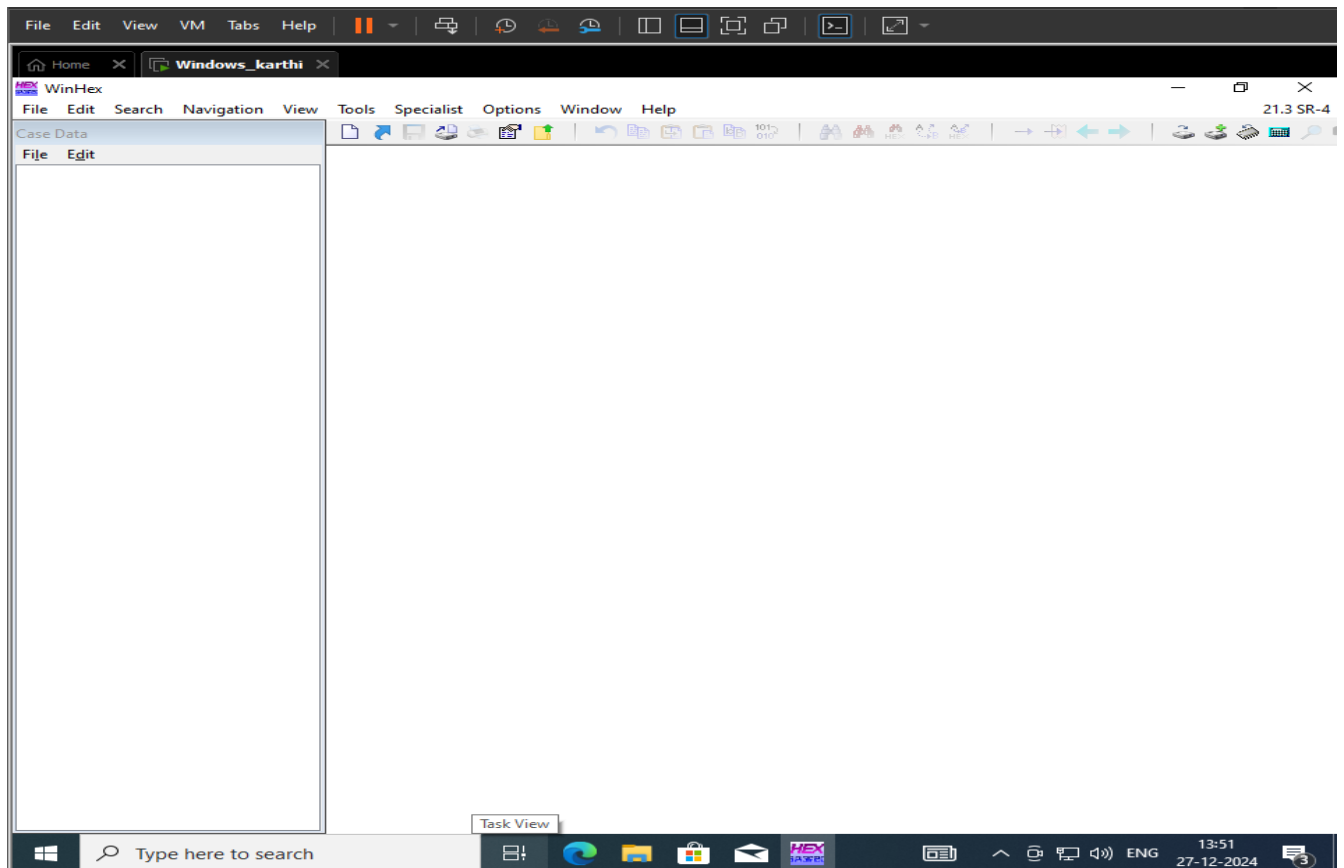
Forensic investigators are scanning computers for deleted data to catch a perpetrator who has been collecting a company's private data for harmful purposes. The perpetrator deleted the data to avoid identification.

### **Lab Objectives**

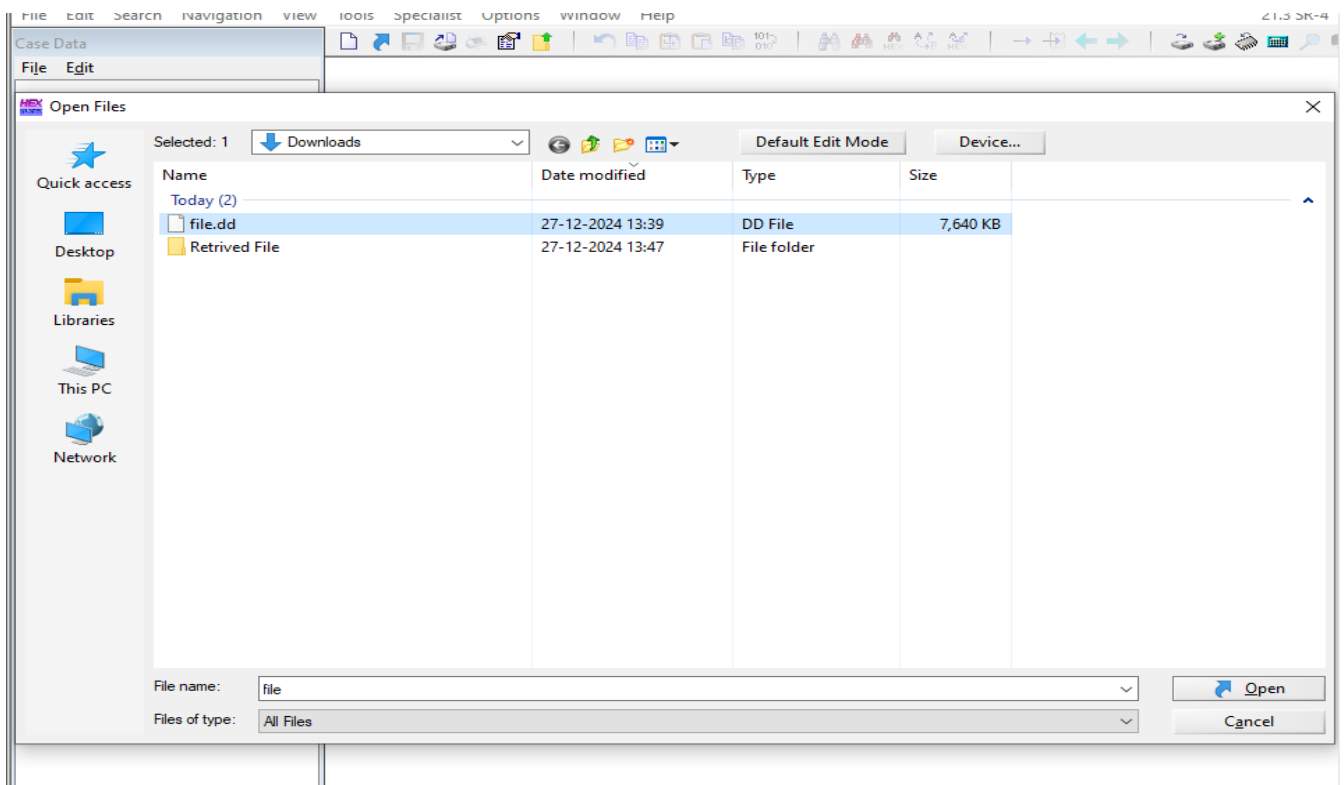
Understand how to recover files that have been permanently deleted using the WinHex tool.

### **Lab Tasks**

1. Install WinHex



2. Open Evidence File



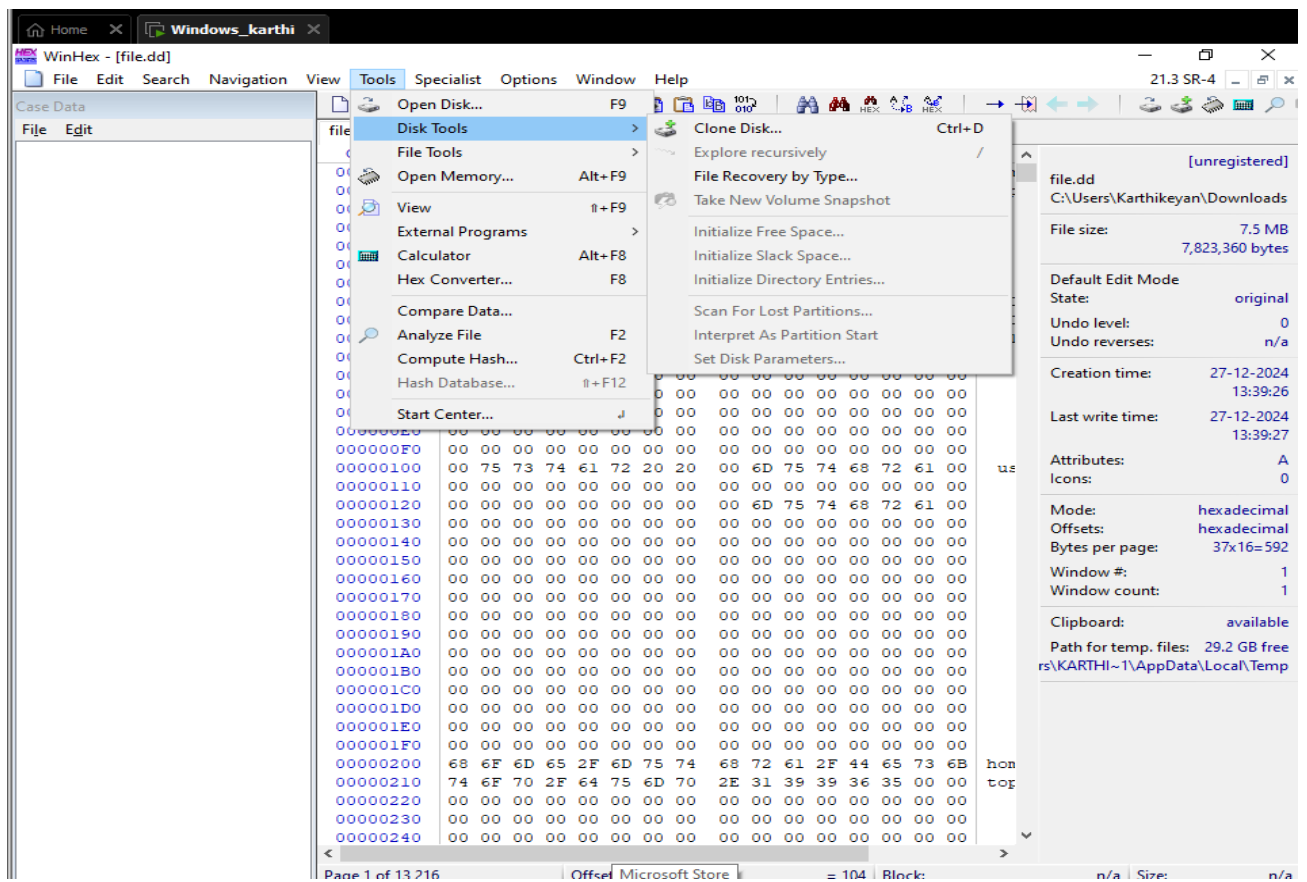
### 3. Analyse Target DD Image

The screenshot shows the 'file.dd' image analysis window. The main pane displays a hex dump of the file data. The right pane shows file metadata:

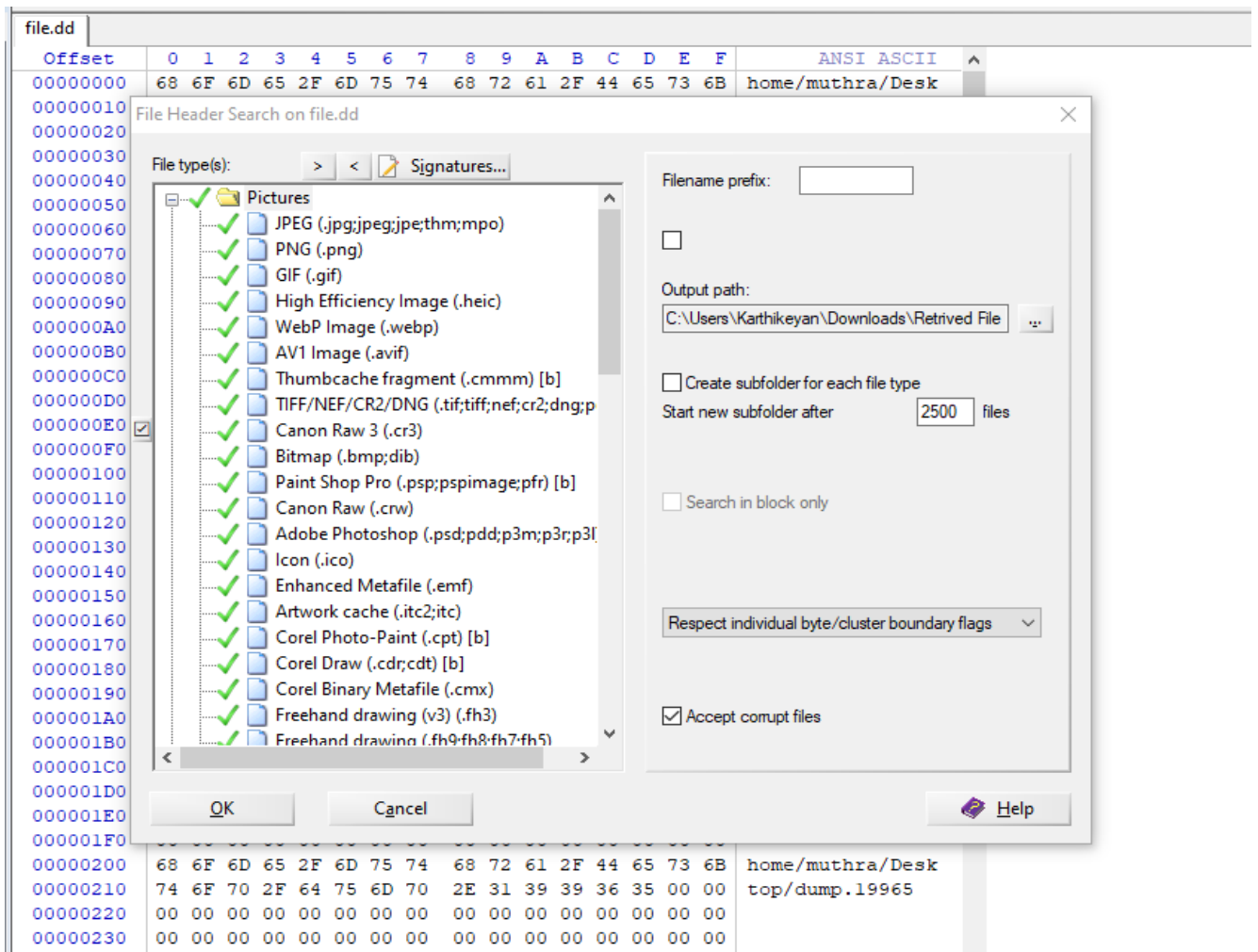
- file.dd [unregistered]
- C:\Users\Karthikeyan\Downloads
- File size: 7.5 MB (7,823,360 bytes)
- Default Edit Mode: original
- State: original
- Undo level: 0
- Undo reverses: n/a
- Creation time: 27-12-2024 13:39:26
- Last write time: 27-12-2024 13:39:27
- Attributes: A
- Icons: 0
- Mode: hexadecimal
- Offsets: hexadecimal
- Bytes per page: 37x16=592
- Window #: 1
- Window count: 1
- Clipboard: available
- Path for temp. files: 29.2 GB free rs\KARTHI~1\AppData\Local\Temp

The bottom status bar shows: Page 1 of 13,216 | Offset: Mail = 104 Block: n/a Size: n/a

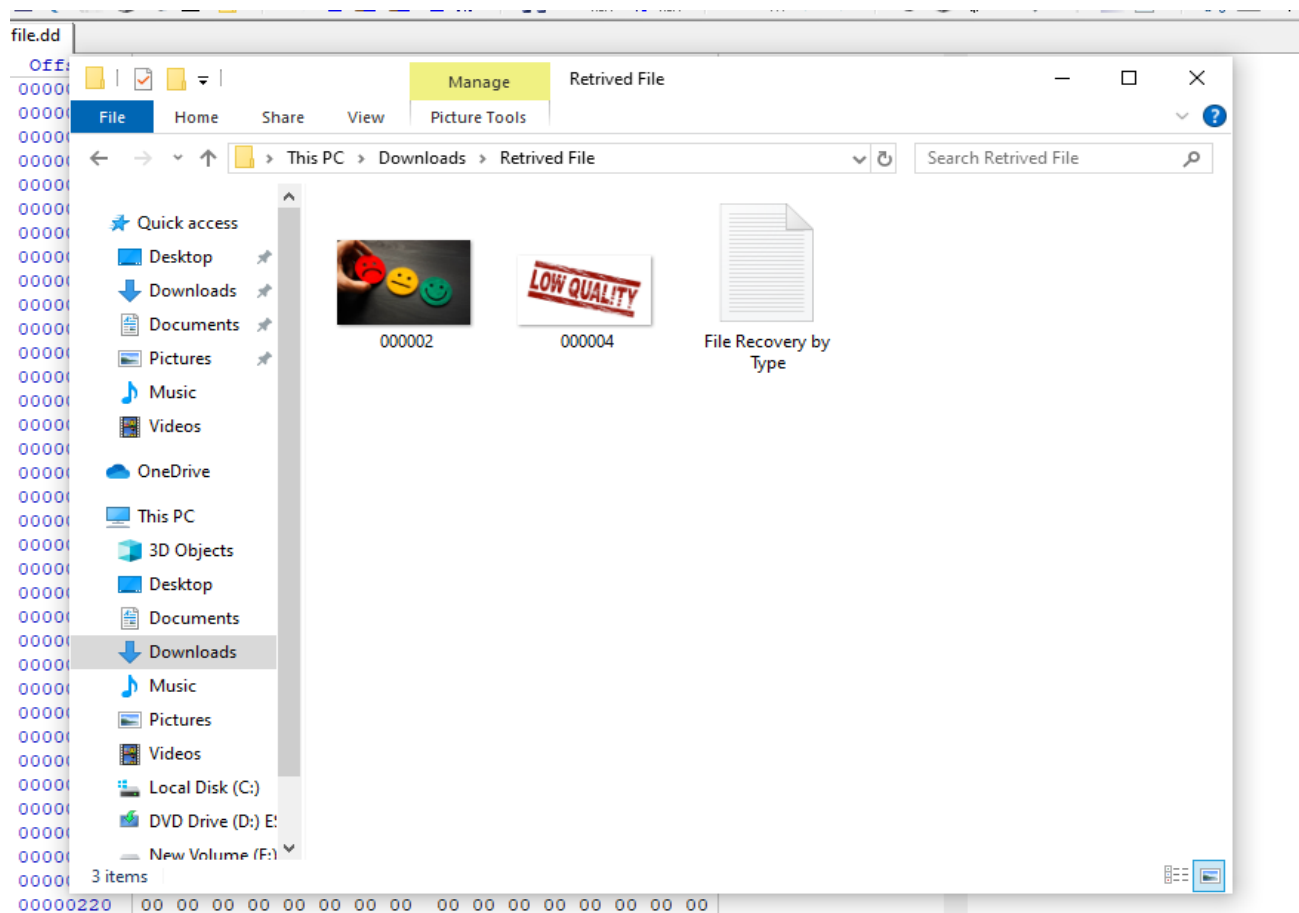
### 4. File Recovery by Type



## 5. Select File Types



## 6. View Retrieved Files



### ***Lab2: Analysing File System Types Using The Sleuth Kit (TSK)***

#### **Lab Scenario**

Investigators are scanning a large number of systems to identify a culprit leaking a company's secret information. They use The Sleuth Kit (TSK) to determine the volume and file system data, simplifying their search.

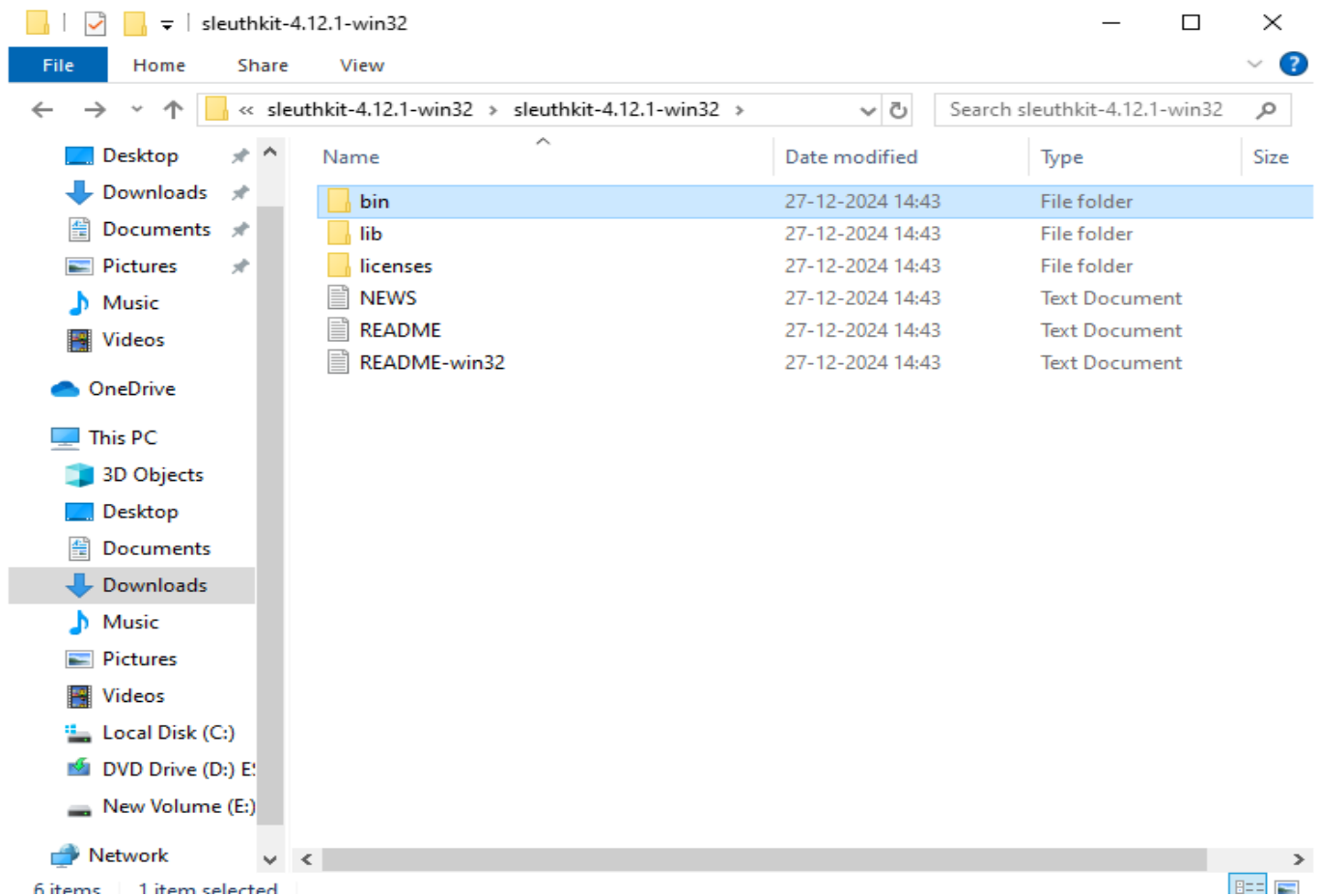
#### **Lab Objectives**

Learn and perform file system analysis using The Sleuth Kit (TSK) to obtain:

- File system type
- Metadata information
- Content information

#### **Lab Tasks**

1. Navigate to The Sleuth Kit (TSK)



## 2. View File System Details

```
C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>bin\fsstat -f ntfs "C:\Users\Karthikeyan\Documents\3-kwsrch-ntfs\ntfs-img-kw-1.dd"
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: BA50ED9250ED5623
OEM Name: NTFS
Volume Name: KW-SRCH-1
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 5355
First Cluster of MFT Mirror: 8032
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 39
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 0 - 16063
Total Sector Range: 0 - 16063

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
$FILE_NAME (48) Size: 68-578 Flags: Resident,Index
$OBJECT_ID (64) Size: 0-256 Flags: Resident
$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident
$VOLUME_NAME (96) Size: 2-256 Flags: Resident
$VOLUME_INFORMATION (112) Size: 12-12 Flags: Resident
$DATA (128) Size: No Limit Flags:
```

## 3. istat

```

C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>bin\istat "C:\Users\Karthikeyan\Documents\3-kwsrch-ntfs\ntfs-img-kw-1.dd" 0
MFT Entry Header Values:
Entry: 0      Sequence: 1
$LogFile Sequence Number: 1075381
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-21-1757981266-484763869-1060284298-1003)
Created:      2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified: 2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:      2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5      Sequence: 5
Allocated Size: 16384      Actual Size: 16384
Created:      2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified: 2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:      2003-10-23 22:42:59.693550400 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 74
Type: $DATA (128-1) Name: N/A Non-Resident size: 39936 init_size: 39936
5355 5356 5357 5358 5359 5360 5361 5362
5363 5364 5365 5366 5367 5368 5369 5370
5371 5372 5373 5374 5375 5376 5377 5378
5379 5380 5381 5382 5383 5384 5385 5386
5387 5388 5389 5390 5391 5392 5393 5394
5395 5396 5397 5398 5399 5400 5401 5402
5403 5404 5405 5406 5407 5408 5409 5410
5411 5412 5413 5414 5415 5416 5417 5418
5419 5420 5421 5422 5423 5424 5425 5426
5427 5428 5429 5430 5431 5432 5433 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
Type: $BITMAP (176-5) Name: N/A Non-Resident size: 8 init_size: 8
5354

```

Task View

```

C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>bin\istat "C:\Users\Karthikeyan\Documents\3-kwsrch-ntfs\ntfs-img-kw-1.dd" 8
MFT Entry Header Values:
Entry: 8      Sequence: 8
$LogFile Sequence Number: 1053084
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-21-1757981266-484763869-1060284298-1003)
Created:      2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified: 2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:      2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $BadClus
Parent MFT Entry: 5      Sequence: 5
Allocated Size: 0      Actual Size: 0
Created:      2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified: 2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:      2003-10-23 22:42:59.693550400 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 82
Type: $DATA (128-2) Name: N/A Resident size: 0
Type: $DATA (128-1) Name: $Bad Non-Resident size: 8224768 init_size: 0

```

#### 4. fls.exe

```
C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>bin\fls.exe -f ntfs "C:\Users\Karthikeyan\Documents\3-kwsrch-ntfs\ntfs-img-kw-1.dd"
r/r 4-128-4: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-1: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
r/r 2-128-1: $LogFile
r/r 0-128-1: $MFT
r/r 1-128-1: $MFTMirr
r/r 9-128-8: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 3-128-3: $Volume
d/r 38-128-4: dir-n-6:there
d/d 38-144-1: dir-n-6
d/r 30-128-3: dir-r-4:there
d/d 30-144-1: dir-r-4
r/r 33-128-3: file-n-1.dat
r/r 35-128-3: file-n-3.dat
r/r 36-128-3: file-n-4.dat
r/r 37-128-3: file-n-5.dat
r/r 37-128-5: file-n-5.dat:here
r/r 27-128-1: file-r-1.dat
r/r 29-128-1: file-r-3.dat
r/r 29-128-3: file-r-3.dat:here
d/d 31-144-1: System Volume Information
-/r * 34-128-1: file-r-2.dat
V/V 39: $OrphanFiles

C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>
C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>_
```

#### 5. List Files and Directory Names

```
C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>
C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>bin\fls -d ntfs "C:\Users\Karthikeyan\Documents\3-kwsrch-ntfs\ntfs-img-kw-1.dd"
Error stat(ing) image file (raw_open: image "ntfs" - No such file or directory)

C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>bin\fls -d "C:\Users\Karthikeyan\Documents\3-kwsrch-ntfs\ntfs-img-kw-1.dd"
-/r * 34-128-1: file-r-2.dat

C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>
```

#### 6. Image file information

```
C:\Users\Karthikeyan\Downloads\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32>bin\img_stat "C:\Users\Karthikeyan\Documents\3-kwsrch-ntfs\ntfs-img-kw-1.dd"
IMAGE FILE INFORMATION
-----
Image Type: raw

Size in bytes: 8224768
Sector size: 512
```



### Lab 3: Analysing Raw Image Using Autopsy

#### Lab Scenario

An inspector finds a dead system at a crime scene and suspects it is related to a murder incident. The forensic investigator uses Autopsy to replicate the hard disk and analyze the file systems, finding obscene videos and pictures that could have been the cause of the murder.

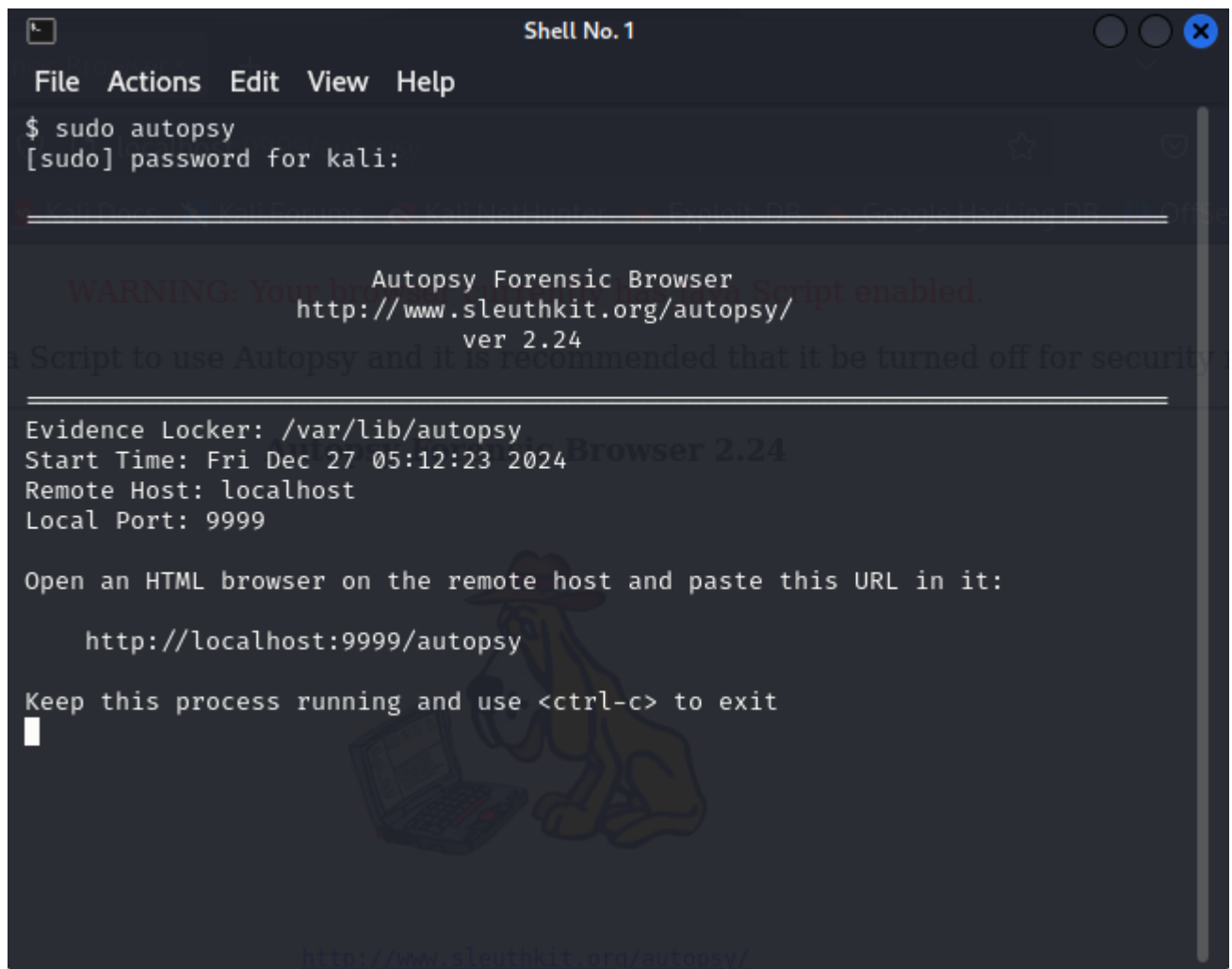
#### Lab Objectives

Learn and perform file system analysis using Autopsy to obtain:

- File system type
- Metadata information
- Content information

#### Lab Tasks

1. Launch Autopsy



```
Shell No. 1
File Actions Edit View Help
$ sudo autopsy
[sudo] password for kali:

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

WARNING: Your browser has JavaScript enabled.
Script to use Autopsy and it is recommended that it be turned off for security.

Evidence Locker: /var/lib/autopsy
Start Time: Fri Dec 27 05:12:23 2024
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

2. Open Autopsy in Browser

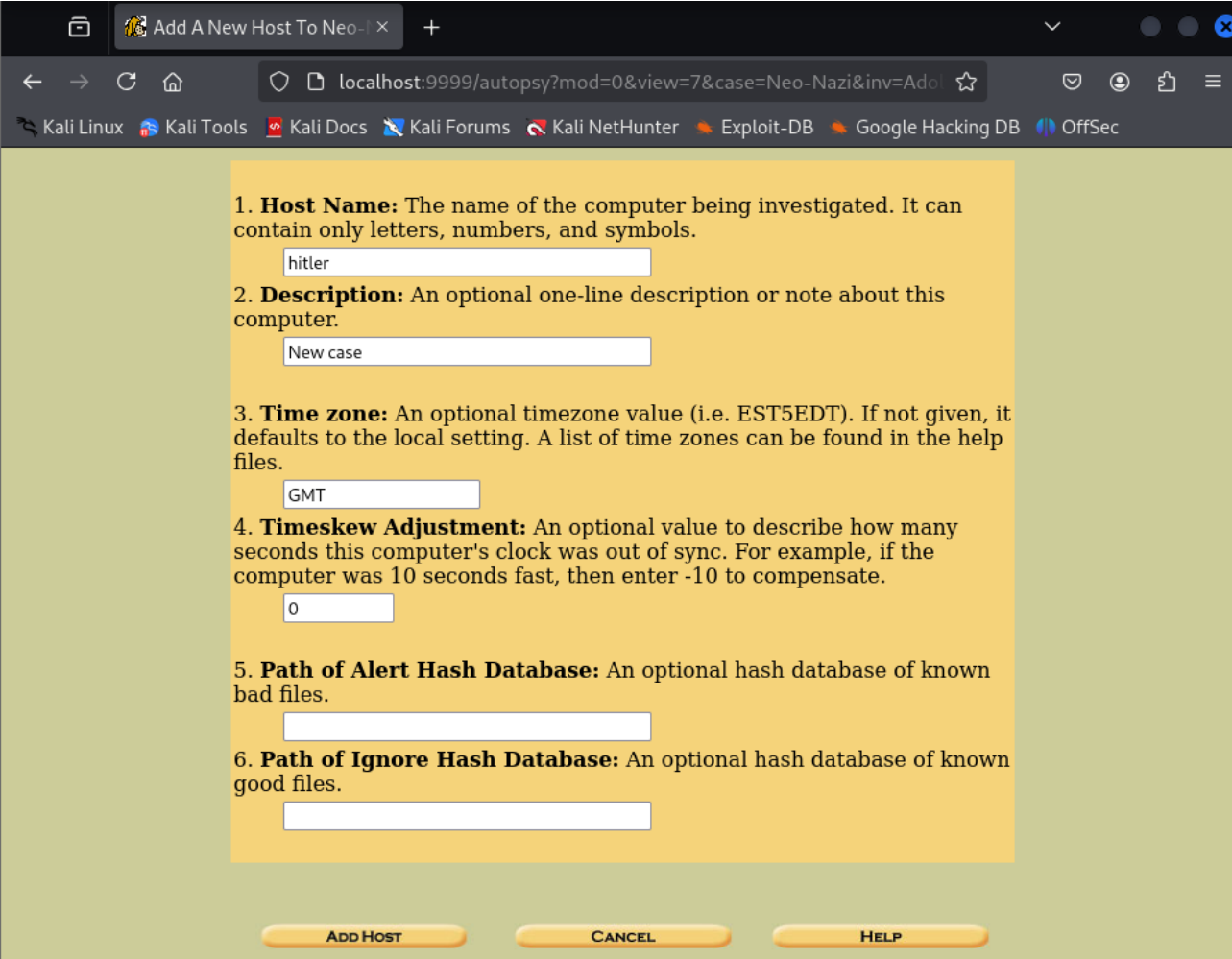




### 3. Create New Case

The screenshot shows the "Create A New Case" form within the Autopsy Forensic Browser. The browser's address bar shows "localhost:9999/autopsy?mod=0&view=1". The form has a yellow background and is titled "CREATE A NEW CASE". It contains three main sections: 1. "Case Name": A text box with the value "Neo-Nazi". 2. "Description": A text box with the value "fun". 3. "Investigator Names": A grid of ten text boxes labeled a. through j. The first box (a.) contains the value "Adolf". At the bottom of the form are three yellow buttons: "NEW CASE", "CANCEL", and "HELP".

#### 4. Add Host



1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

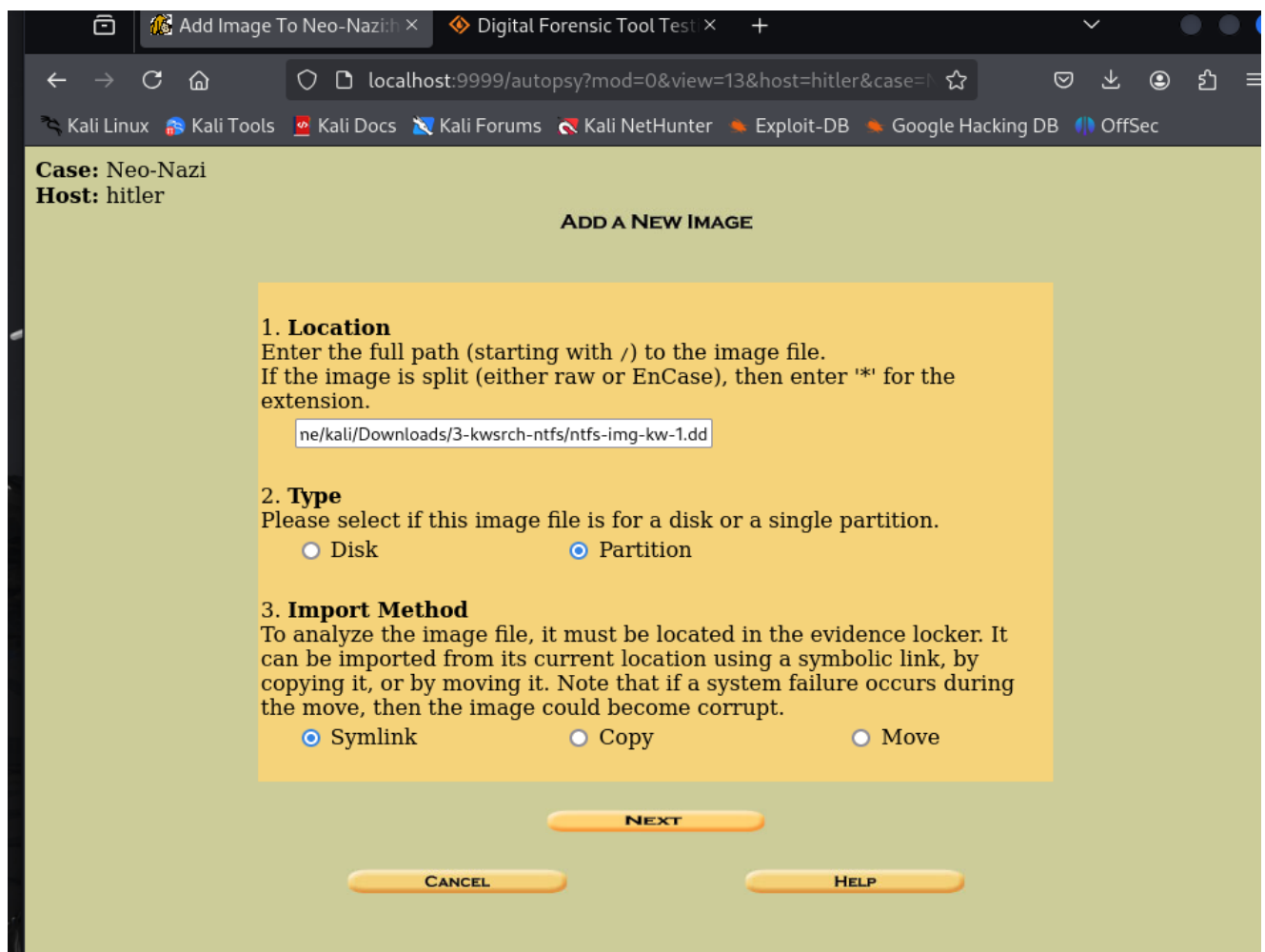
3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

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.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

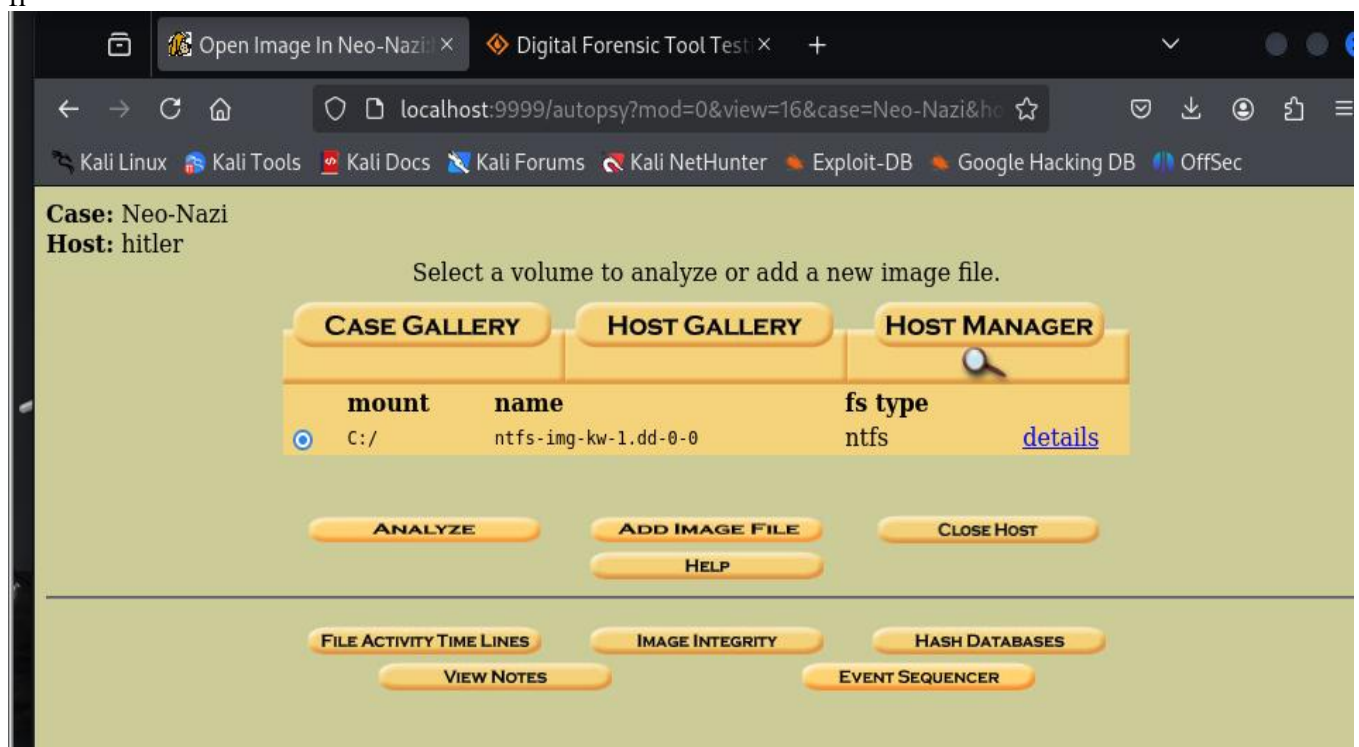
6. **Path of Ignore Hash Database:** An optional hash database of known good files.

#### 5. Add Image



## 6. Analyze Image

fi



## 7. File Analyze

Neo-Nazi:hitler:vol1

Digital Forensic Tool Test

localhost:9999/autopsy?mod=1&submod=2&case=Neo-Nazi&host=hitler&inv=Adolf&vol=vol1

Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE

Directory Seek

Enter the name of a directory that you want to view.  
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Current Directory: C:/

ADD NOTE

GENERATE MD5 LIST OF FILES

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	dir / in									
Error Parsing File (Invalid Characters?): V/V 39: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0										
	r / r	\$AttrDef	2003-10-23 17:12:59 (GMT)	2003-10-23 17:12:59 (GMT)	2003-10-23 17:12:59 (GMT)	2003-10-23 17:12:59 (GMT)	2560	48	0	<a href="#">4-128-4</a>
	r / r	\$BadClus	2003-10-23 17:12:59 (GMT)	2003-10-23 17:12:59 (GMT)	2003-10-23 17:12:59 (GMT)	2003-10-23 17:12:59 (GMT)	0	0	0	<a href="#">8-128-2</a>
	r / r	\$BadClus:\$Bad	2003-10-23	2003-10-23	2003-10-23	2003-10-23	8224768	0	0	<a href="#">8-128-1</a>

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.

More file details can be found using the Metadata link at the end of the list (on the right).

You can also sort the files using the column headers

## 8. Generate MD5 list of file

Neo-Nazi:hitler:vol1

localhost:9999/autopsy?r

Digital Forensic Tool Test

localhost:9999/autopsy?mod=2&view=12&case=Neo-Nazi&host=hitler&inv=Adolf&vol=vol1

Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

MD5 Values for files in C:/ (ntfs-img-kw-1.dd-0-0)

ad617ac3906958de35eacc3d90d31043 - \$AttrDef  
d41d8cd98f00b204e9800998ecf8427e - \$BadClus  
d41d8cd98f00b204e9800998ecf8427e - \$BadClus:\$Bad  
7810ad2a077259a0c749b35c5d2b68e2 - \$Bitmap  
085c7e7f76ecce7093e7009e64a12805 - \$Boot  
982d5b0b8273638af199ef42f2ad2618 - \$LogFile  
697a7d36f41249be73121e6a74ae8b20 - \$MFT  
5fe3f6772286df48378a08b15556bfdd - \$MFTMirr  
153746ff480b662c5a95193082ed404c - \$Secure:\$SDS  
ea040d3151178184bb523d6bf3c3eab8 - \$Secure:\$SDH  
17f25ce4ac91855edf1e7f3108ee8adc - \$Secure:\$SII  
6fa3db2468275286210751e869d36373 - \$UpCase  
d41d8cd98f00b204e9800998ecf8427e - \$Volume  
049109e97e7dfe3213cf21a95d713cdc - file-n-1.dat  
03f92745c1c3dfc078cc0a192bb9d2cf - file-n-3.dat  
ecf3d88d78f6b05ef57fd93b591902f5 - file-n-4.dat  
2b21e56e1eee66419cdb36b3abf72029 - file-n-5.dat  
759681c75ae452d8abfb57760f665a36 - file-n-5.dat:here  
544fdd2d47f570b912807d1c871f81e0 - file-r-1.dat  
d201f17f7447fa75362bd61ac3aa7706 - file-r-3.dat  
0d9332a3532a8adaf34bcb79e1442c0b - file-r-3.dat:here

## 9. General File system detail

localhost:9999/autopsy?mod=1&submod=7&case=Neo-Nazi&host=hitler&inv=Adolf&vol=vol1

80%

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

General File System Details

FILE SYSTEM INFORMATION

File System Type: NTFS  
Volume Serial Number: BA50ED9250ED5623  
OEM Name: NTFS  
Volume Name: KW-SRCH-1  
Version: Windows XP

METADATA INFORMATION

First Cluster of MFT: 5355  
First Cluster of MFT Mirror: 8032  
Size of MFT Entries: 1024 bytes  
Size of Index Records: 4096 bytes  
Range: 0 - 39  
Root Directory: 5

CONTENT INFORMATION

Sector Size: 512  
Cluster Size: 512  
Total Cluster Range: 0 - 16063  
Total Sector Range: 0 - 16063  
  
\$AttrDef Attribute Values:  
\$STANDARD\_INFORMATION (16) Size: 48-72 Flags: Resident  
\$ATTRIBUTE\_LIST (32) Size: No Limit Flags: Non-resident  
\$FILE\_NAME (48) Size: 68-578 Flags: Resident, Index  
\$OBJECT\_ID (64) Size: 0-256 Flags: Resident  
\$SECURITY\_DESCRIPTOR (80) Size: No Limit Flags: Non-resident  
\$VOLUME\_NAME (96) Size: 2-256 Flags: Resident  
\$VOLUME\_INFORMATION (112) Size: 12-12 Flags: Resident  
\$DATA (128) Size: No Limit Flags: Resident