

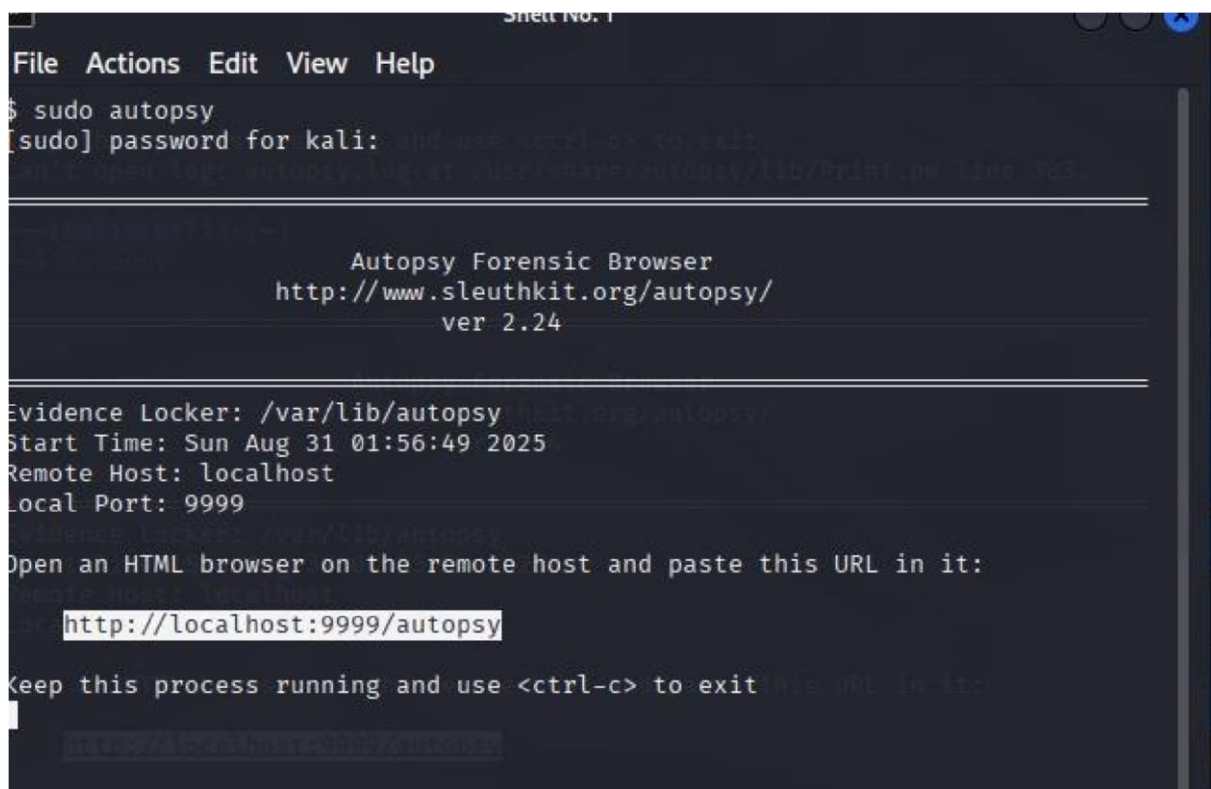
EXP NO 5: Use Autopsy to create a case and import evidence

Aim:

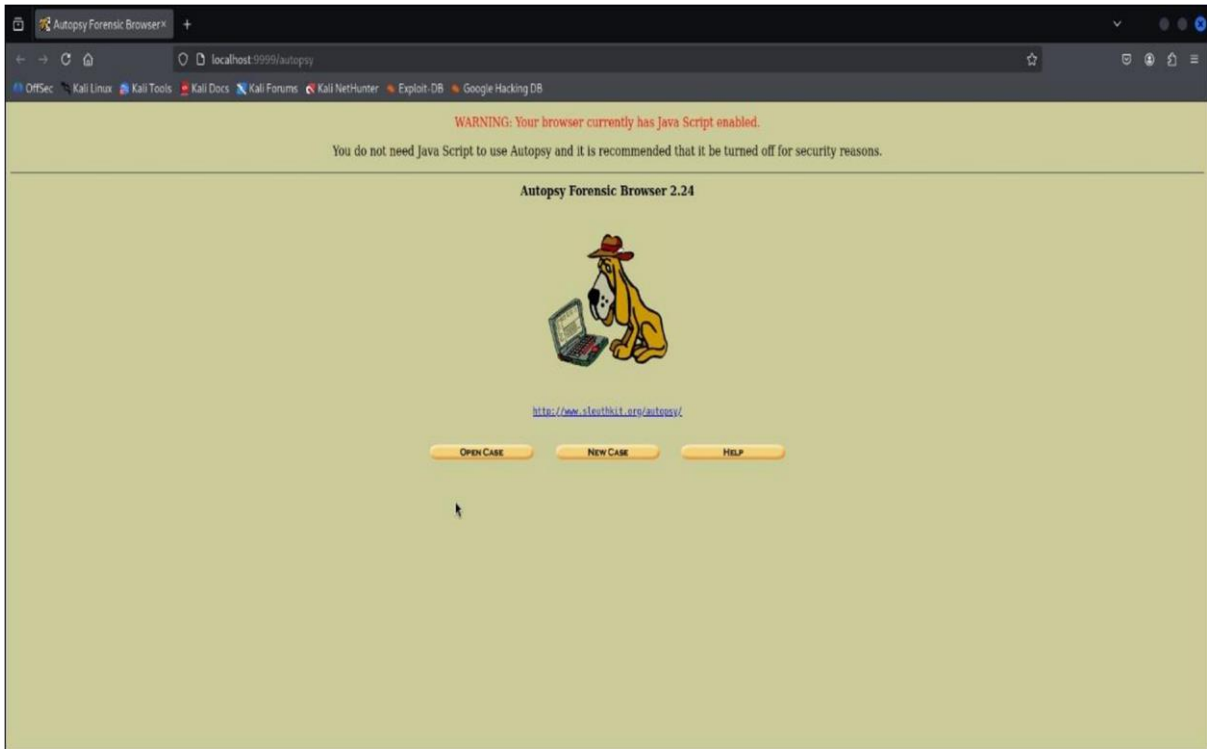
To create a forensic case in Autopsy, import digital evidence such as disk images or local drives, and analyze the data using built-in modules to extract and document relevant artifacts for investigation.

Procedure:

Autopsy is an open-source digital forensics platform used to analyze and extract data from digital devices, including disk images and local drives. It allows creation of cases, importing evidence, running analysis modules like keyword search, file type identification, and hash comparisons. The results can be explored, exported, and reported for forensic investigation and documentation.



```
Shell No. 1
File Actions Edit View Help
$ sudo autopsy
[sudo] password for kali: and use <ctrl-c> to exit
and use <ctrl-c> to exit
and use <ctrl-c> to exit
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy http://www.sleuthkit.org/autopsy/
Start Time: Sun Aug 31 01:56:49 2025
Remote Host: localhost
Local Port: 9999
Evidence Locker: /var/lib/autopsy
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 this URL in it:
http://localhost:9999/autopsy
```



localhost:9999/autopsy/mod=0&view=1&n=82&p=7

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

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

murder

2. **Description:** An optional, one line description of this case.

Laptop image from case suicide

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

NEW CASE CANCEL HELP

localhost:9999/help/index.html

Creating Case: murder

Case directory (/var/lib/autopsy/murder/) created
Configuration file (/var/lib/autopsy/murder/case.aut) created

We must now create a host for this case.

Please select your name from the list:

ADD HOST

Case: murder

ADD A NEW HOST

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.

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.

0

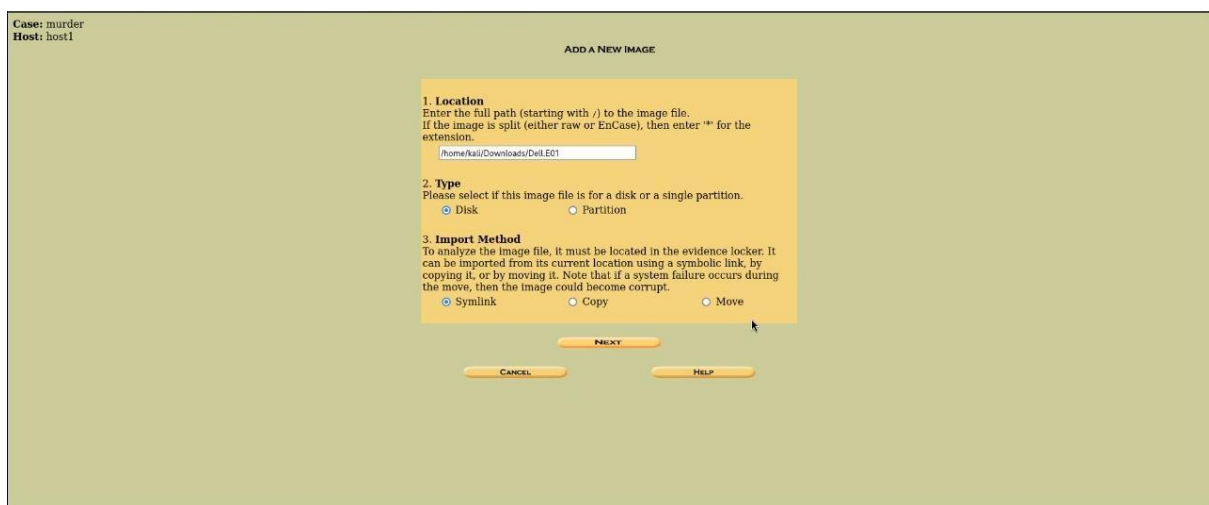
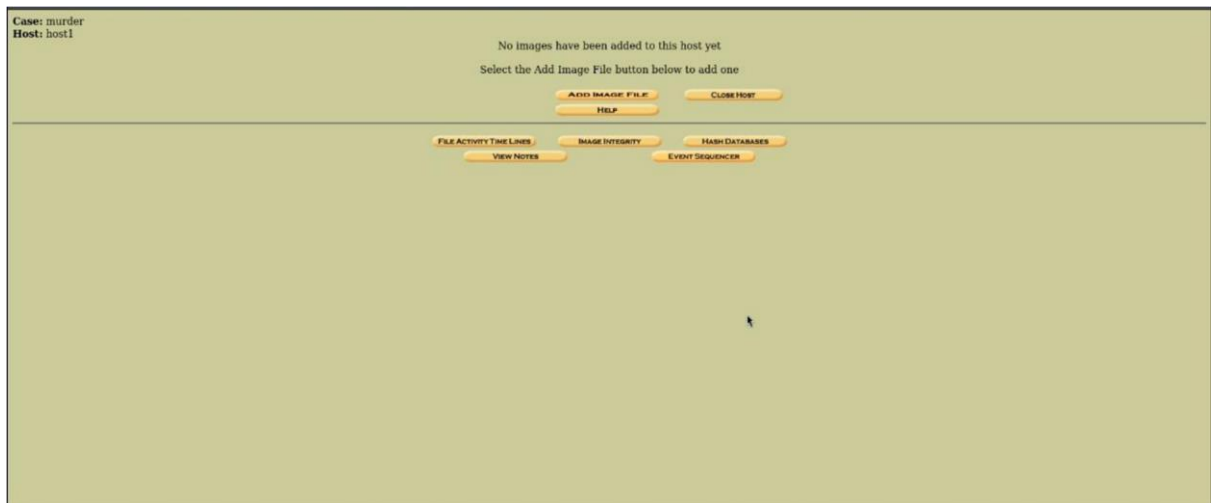
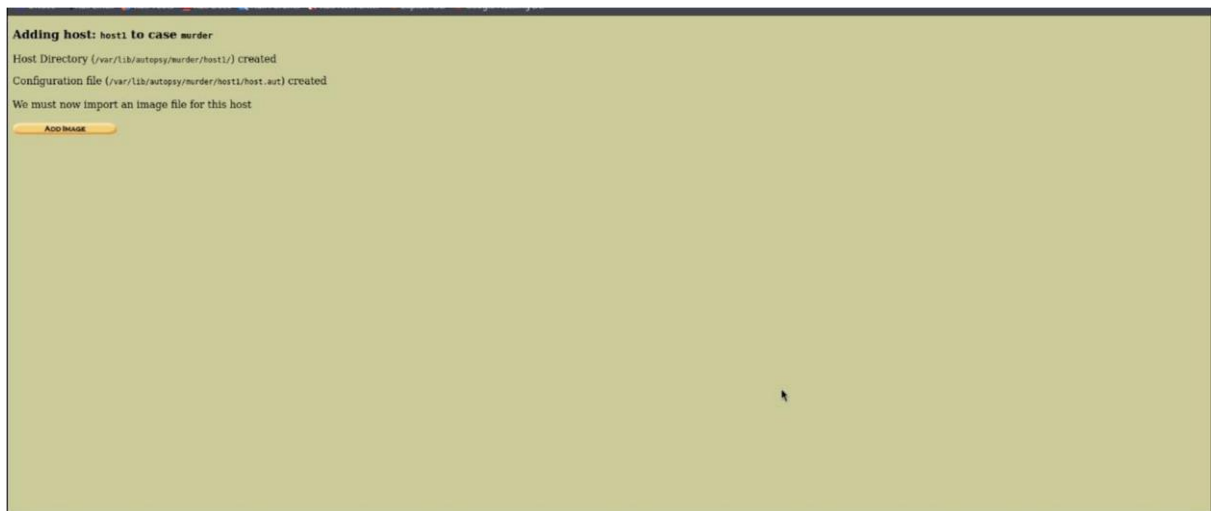
5. **Path of Alert Hash Database:** An optional hash database of known bad files.

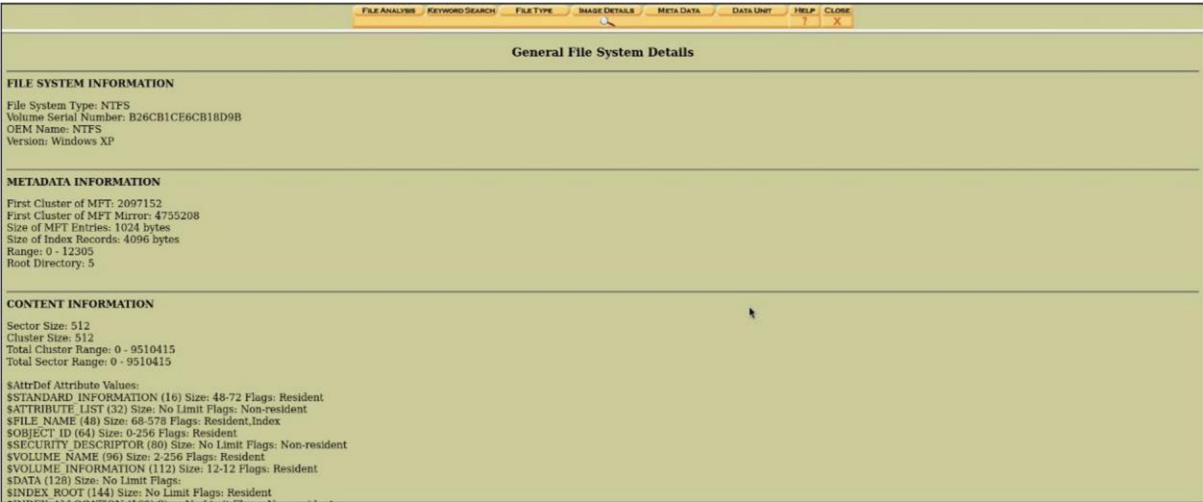
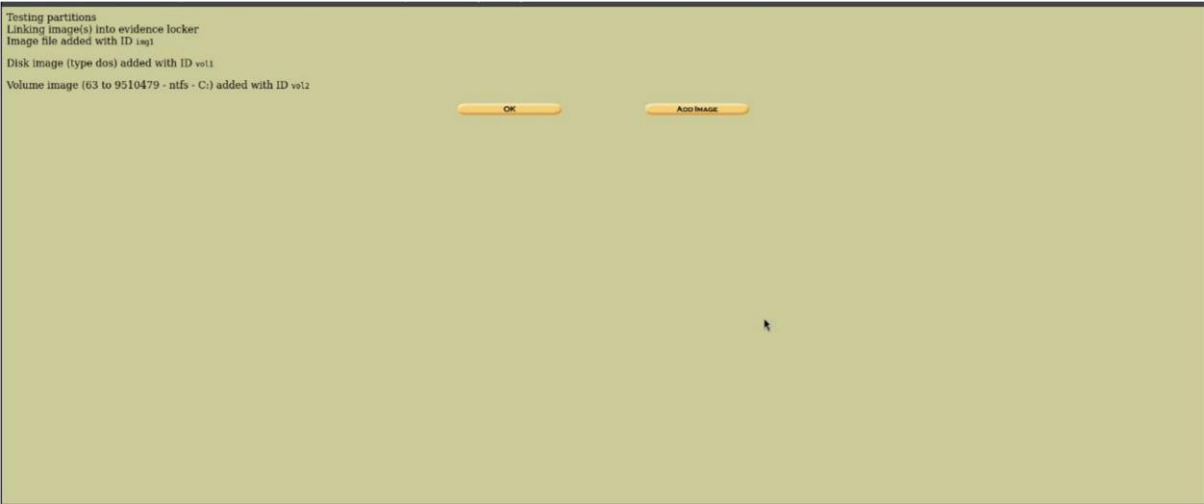
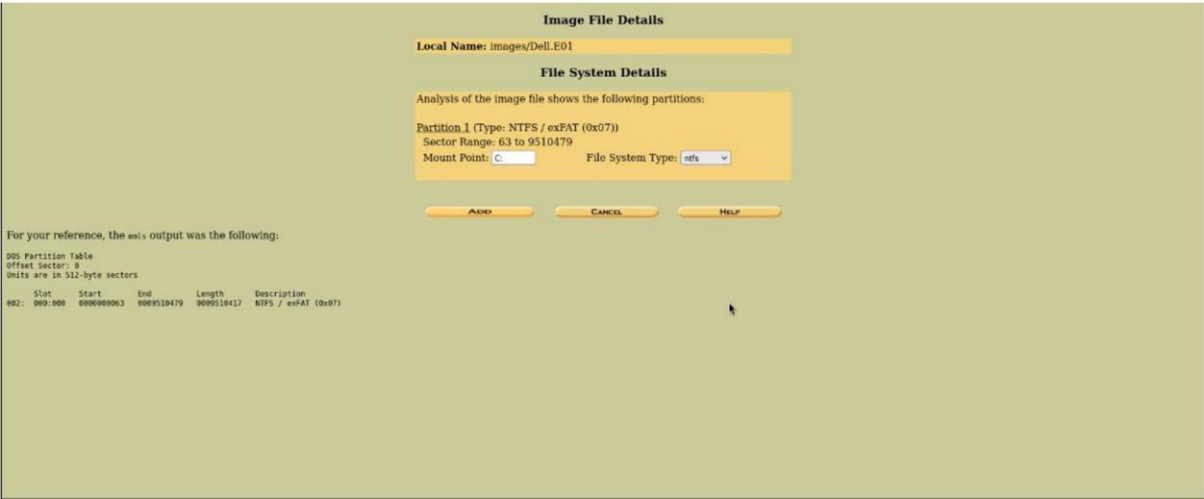
6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST

CANCEL

HELP





File Analysis / Keyword Search / File Type / Basic Details / Meta Data / Data Unit / Help / Close

MFT Entry Number:
4
[View](#)

[Allocation List](#)

Pointed to by file:
C:\PWT

File Type:
data

MD5 of content:
bc7fa8d3f16646b36c487c17b5b0 -

SHA-1 of content:
970922c0d89fcd8299c728b347626f6b5dc7 -

Details:
MFT Entry Header Values:
Entry: 0 Sequence: 1
\$LogFile Sequence Number: 39443417
Allocated File
Links: 1

\$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 ()
Created: 2004-08-19 12:57:43.694987200 (EDT)
File Modified: 2004-08-19 12:57:43.694987200 (EDT)
MFT Modified: 2004-08-19 12:57:43.694987200 (EDT)
Accessed: 2004-08-19 12:57:43.694987200 (EDT)

\$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: \$MFT
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 3772416 Actual Size: 3772416
Created: 2004-08-19 12:57:43.694987200 (EDT)
File Modified: 2004-08-19 12:57:43.694987200 (EDT)
MFT Modified: 2004-08-19 12:57:43.694987200 (EDT)
Accessed: 2004-08-19 12:57:43.694987200 (EDT)

Attributes:

Report / View Contents / Export Contents / Add Note

File Analysis / Keyword Search / File Type / Basic Details / Meta Data / Data Unit / Help / Close

Directory Seek
Enter the name of a directory that you want to view.
C:\r
[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:\r
[Add Note](#) [Generate MD5 List of Files](#)

DEL	Type	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
	dir / ln									
Error Parsing File (Invalid Characters?): V\W 12305: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0										
	- / r	Mittdat	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2560	48	0	4-128-4
	- / r	WinCtun	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	0	0	0	8-128-2
	- / r	ModCtun.vbs	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	4869332992	0	0	8-128-1
	- / r	Mittdat	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	118808	0	0	8-128-1
	- / r	Mittdat	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	2004-08-19 12:57:43 (EDT)	8192	48	0	7-128-1

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.

Case: murder

Select the host to open or create a new one

CASE GALLERY

HOST GALLERY

HOST MANAGER

Name	Description
host1	None Provided details

Investigator (for reports only): sha

OK

ADD HOST

CLOSE CASE

HELP

CREATE DATA FILECREATE TIMELINEVIEW TIMELINEVIEW NOTESHELPCLOSE

Here we will process the file system images, collect the temporal data, and save the data to a single file.

1. Select one or more of the following images to collect data from:

☒ C:/ dell.E01-63-9516479 hifs

2. Select the data types to gather:

☒ Allocated Files☒ Unallocated Files

3. Enter name of output file (body):

output/body

4. Generate MDS Value? ☒

OK

CREATE DATA FILECREATE TIMELINEVIEW TIMELINEVIEW NOTESHELPCLOSE

Running fls -r -w ON vol2

Body file saved to /var/lib/autopsy/murder/host1/output/body

Entry added to host config file

Calculating MDS Value

MDS Value: 56B96648B2E778B1AE779AC90E298C8

The next step is to sort the data into a timeline.

OK

CREATE DATA FILECREATE TIMELINEVIEW TIMELINEVIEW NOTESHELPCLOSE

Now we will sort the data and save it to a timeline.

1. Select the data input file (body):

☒ body

2. Enter the starting date:

None: ☒

Specify:

3. Enter the ending date:

None: ☒

Specify:

4. Enter the file name to save as:

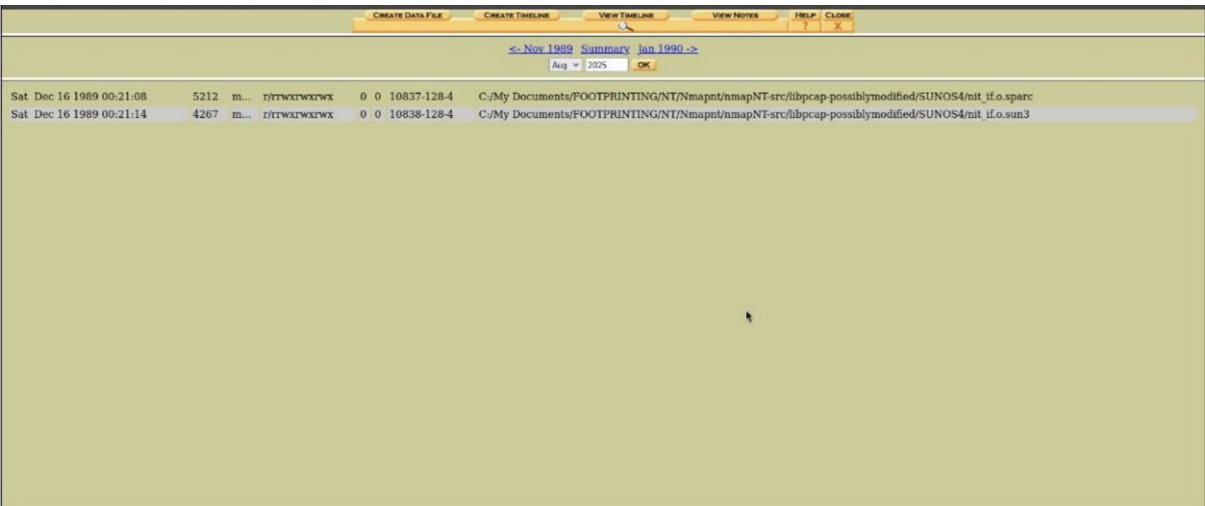
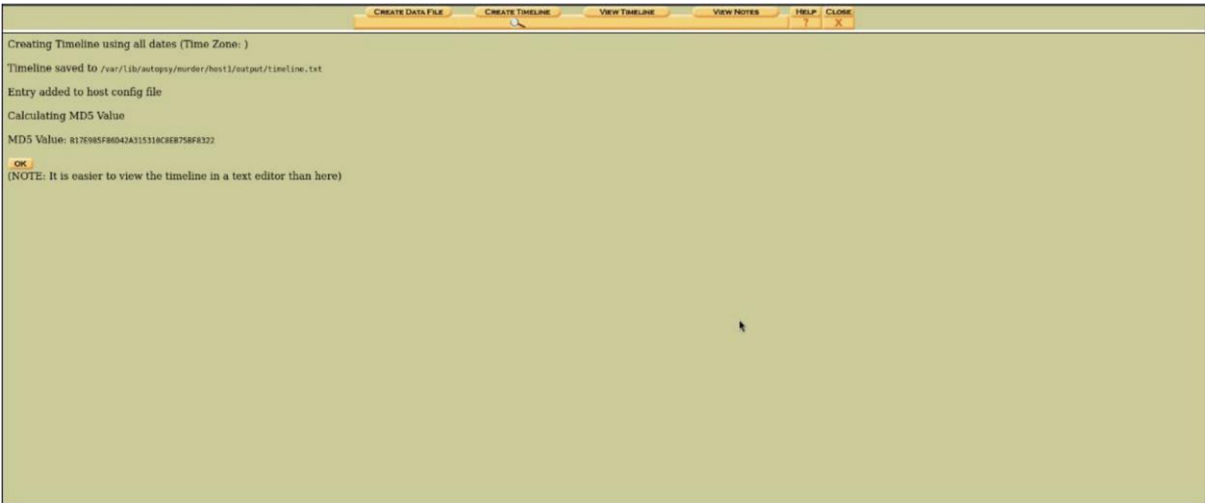
output/timeline.txt

5. Choose the output format:

☒ Tabulated (normal)
☐ Comma delimited with hourly summary
☐ Comma delimited with daily summary

6. Generate MDS Value? ☒

OK



RESULT:

