

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.

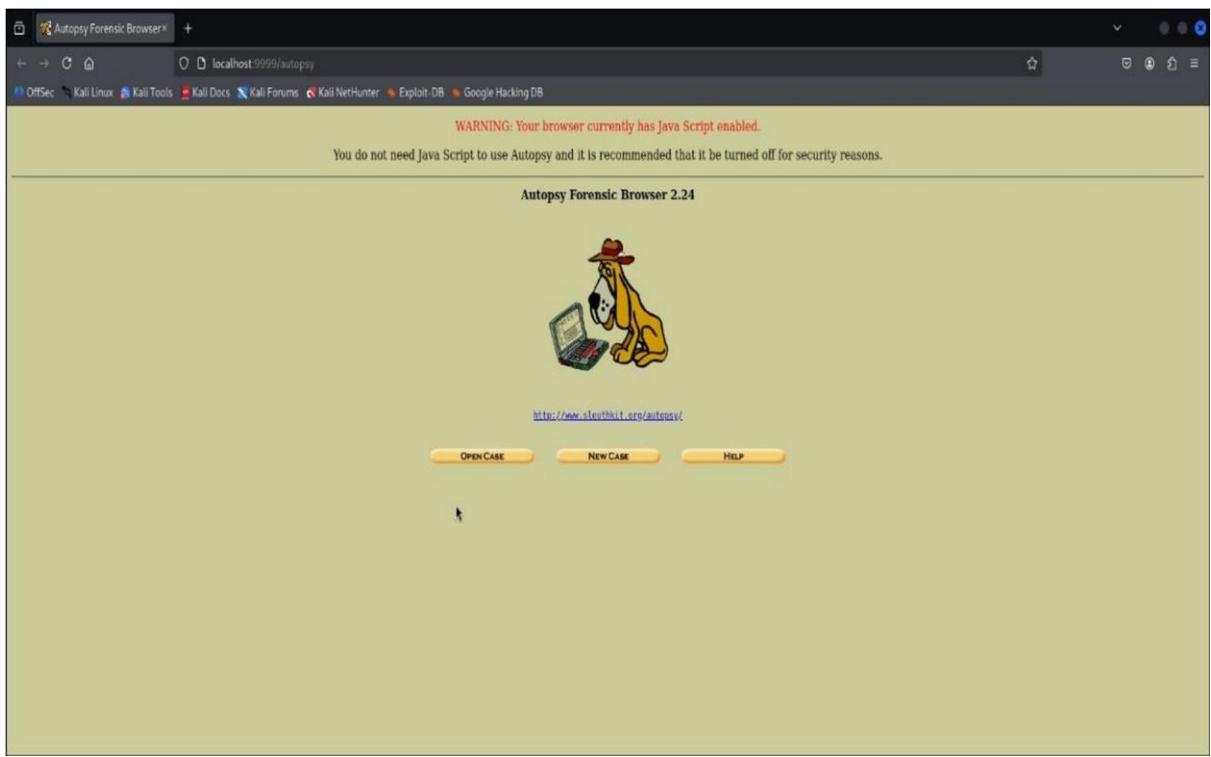
```
Shell No. 1
File Actions Edit View Help
$ sudo autopsy
[sudo] password for kali:
[Open log autopsy.log at /usr/share/autopsy/lib/autopsy.log line 383]

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

Evidence Locker: /var/lib/autopsy
Start Time: Sun Aug 31 01:56:49 2025
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
```



localhost:9999/autopsy?mod=0&view=1&a=82&y=7

CREATE A NEW CASE

- Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.
murder
- Description:** An optional, one line description of this case.
Laptop image from case suicide
- Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. siva	b. arun
c.	d.
e.	f.
g.	h.
i.	j.

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: siva

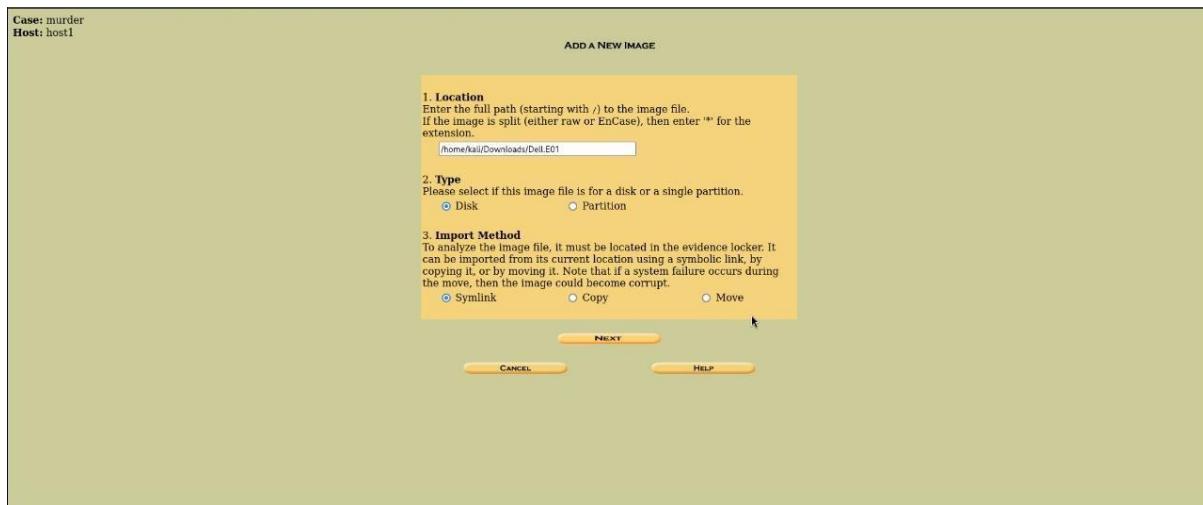
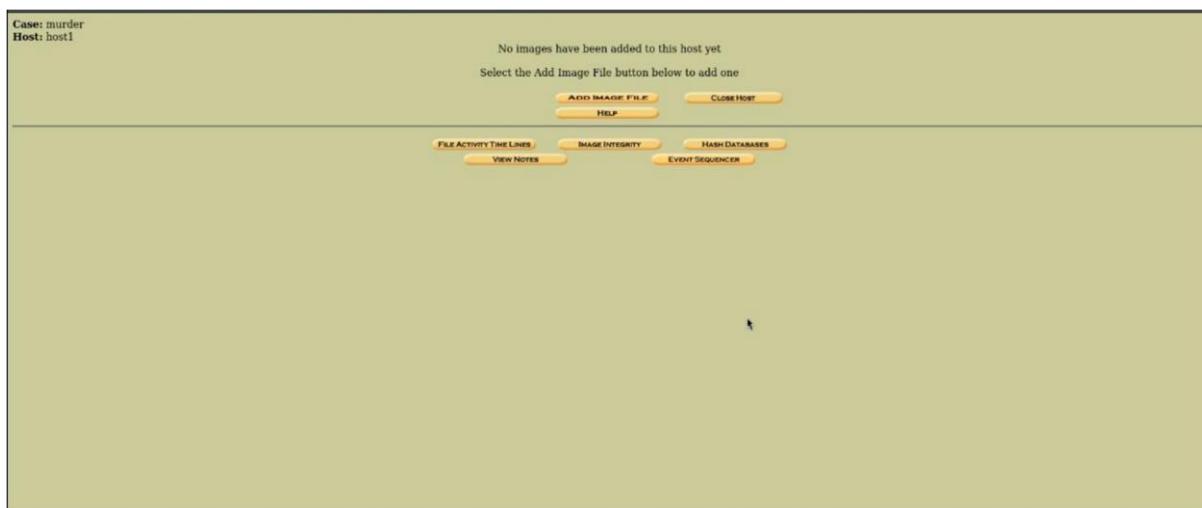
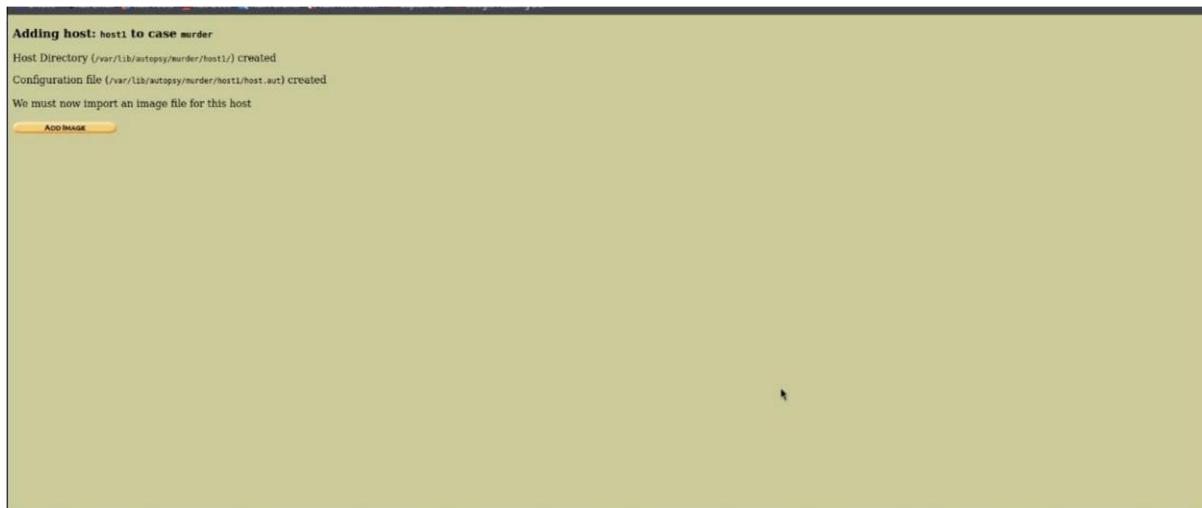
Add Host

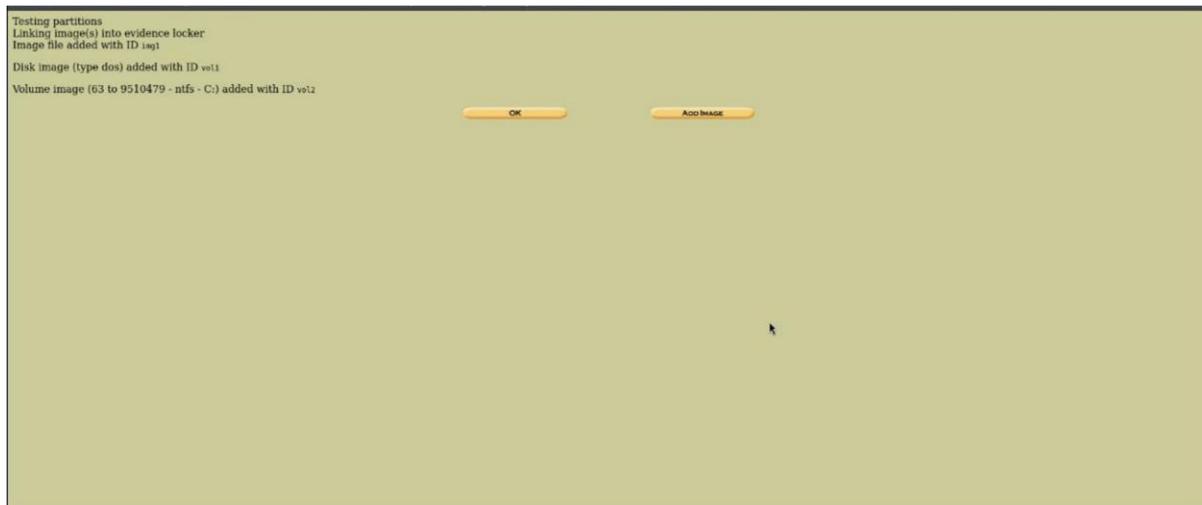
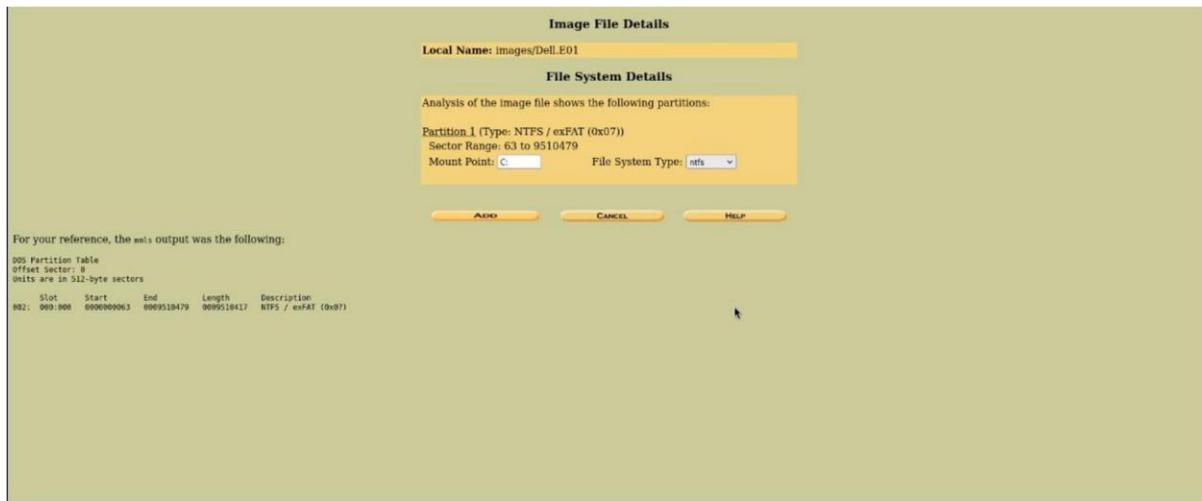
Case: murder

ADD A NEW HOST

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
host
- Description:** An optional one-line description or note about this computer:
- Time zone:** An optional timezone value (i.e. EST5EDT). If not given, defaults to the local setting. A list of time zones can be found in the help files.
- 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
- Path of Alert Hash Database:** An optional hash database of known bad files.
- Path of Ignore Hash Database:** An optional hash database of known good files.

Add Host **CANCEL** **HELP**





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: B26CB1CE6CB18D9B
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION

First Cluster of MFT: 2097152
First Cluster of MFT Mirror: 4755208
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 12305
Root Directory: 5

CONTENT INFORMATION

Sector Size: 512
Cluster Size: 512
Total Cluster Range: 0 - 9510415
Total Sector Range: 0 - 9510415

\$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
\$COMPRESSION_DESCRIPTOR (16) Size: No Limit Flags: Non-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:
\$INDEX_ROOT (144) Size: No Limit Flags: Resident

MFT Entry Number:

Pointed to by file: C:\198T

File Type: data

MD5 of content: 9c7f87c1760a -

SHA-1 of content: 8709121ce09fb02d409c2105347b816700c69c7 -

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
Allocation 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:

Directory Seek
Enter the name of a directory that you want to view.

View

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

SEARCH

Current Directory: [C:\](#) [Add Note](#) [GENERATE MD5 LIST OF FILES](#)

DIR.	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
Error Parsing File (Invalid Characters?): VN\12305: \$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	Attribute	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	FileClass	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	MinIcon-Util	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	SE11000	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)	1188808	0	0	6-128-1
	- / r	Shax1	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

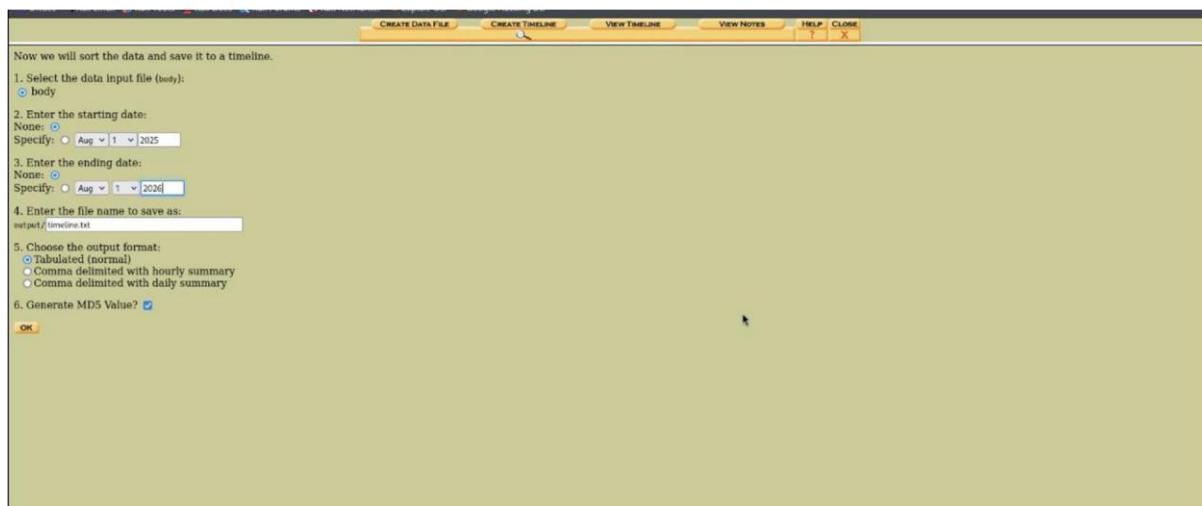
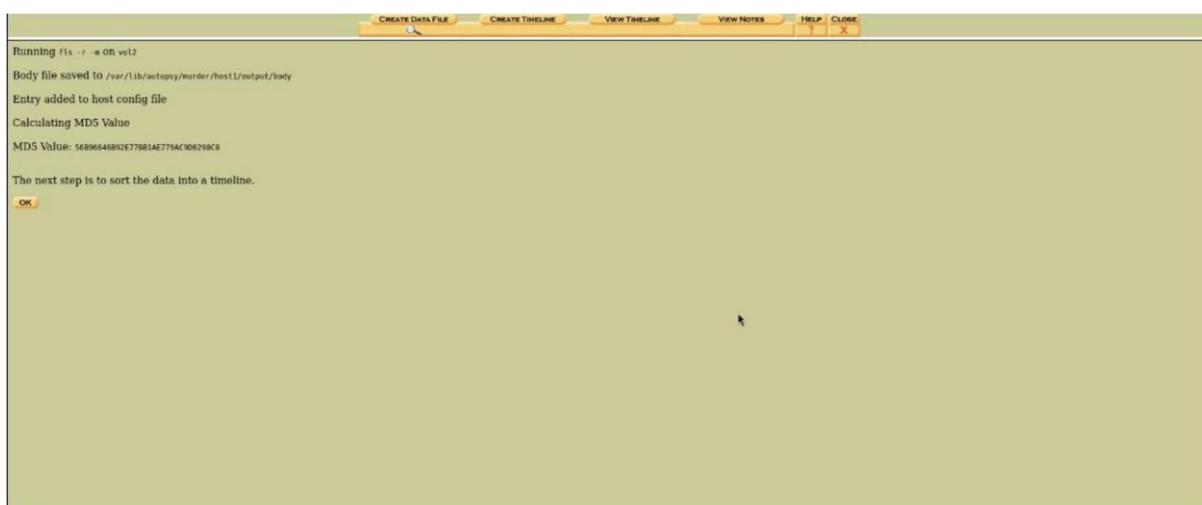
In this mode, you can view file and directory contents.

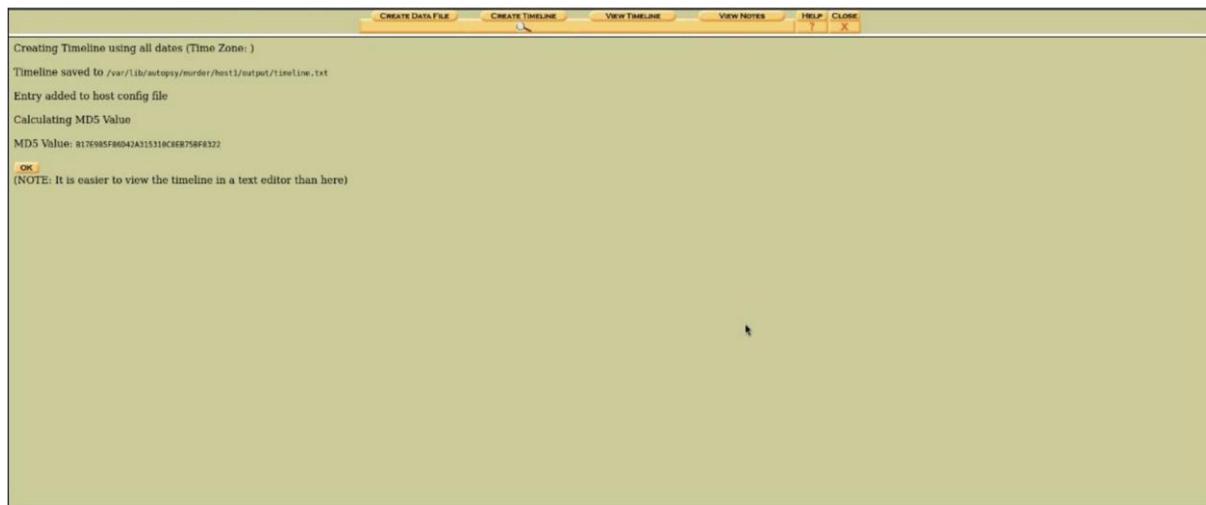
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers.

Case: murder

Select the host to open or create a new one

CASE GALLERY	HOST GALLERY	HOST MANAGER
<input checked="" type="radio"/> host1	Name: None Provided	Description: details
Investigator (for reports only): siva		
OK	ADD HOST	CLOSE CASE
HELP		





RESULT:

