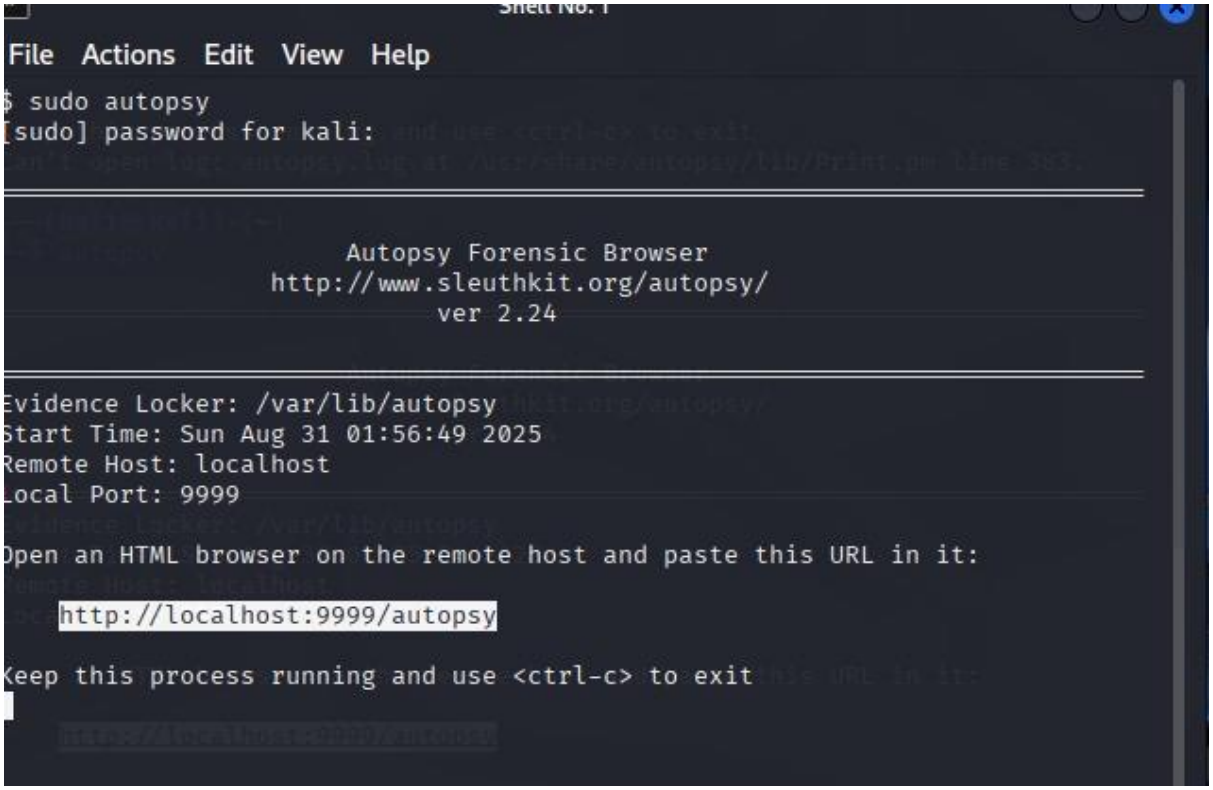
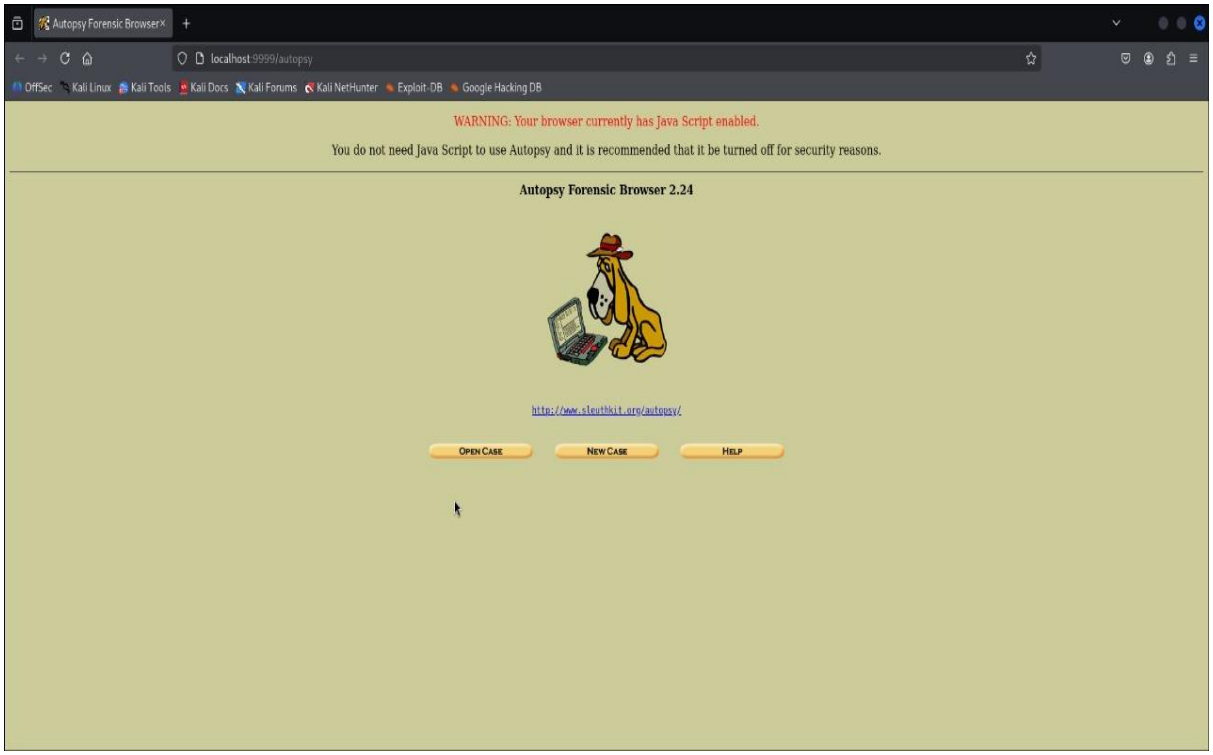
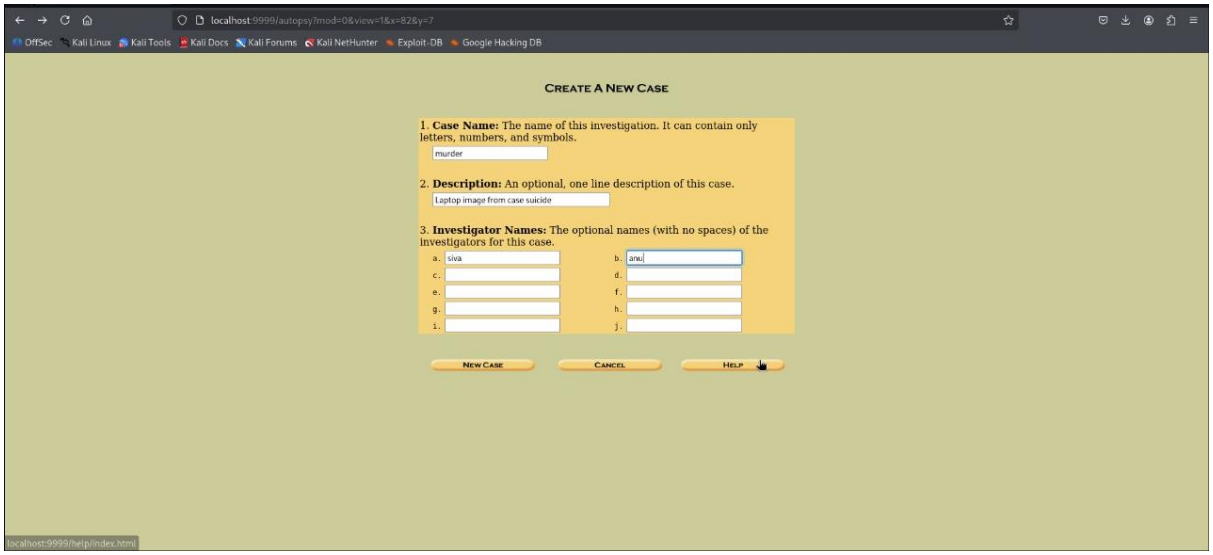
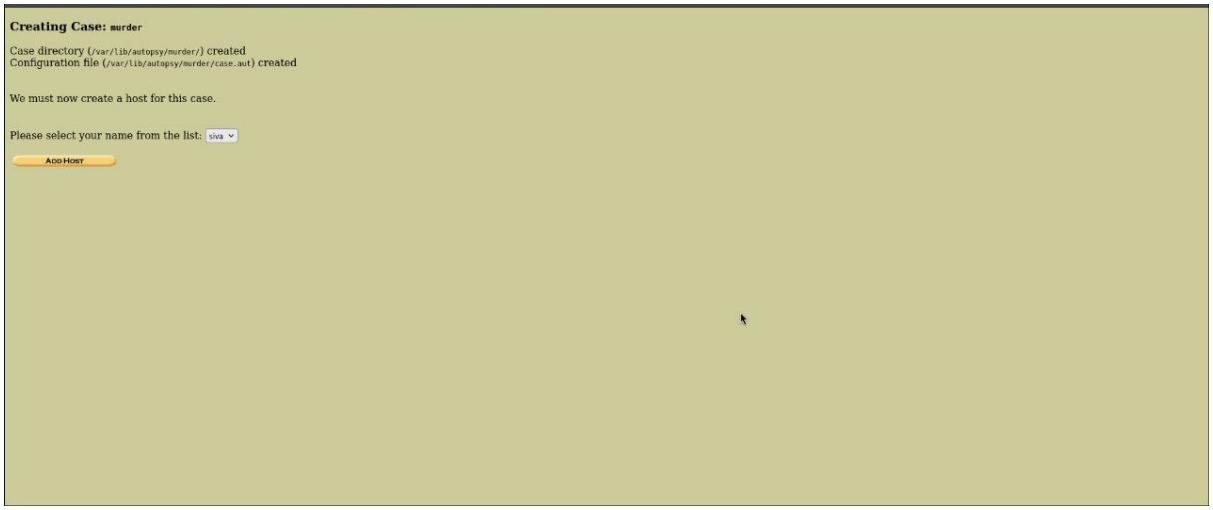
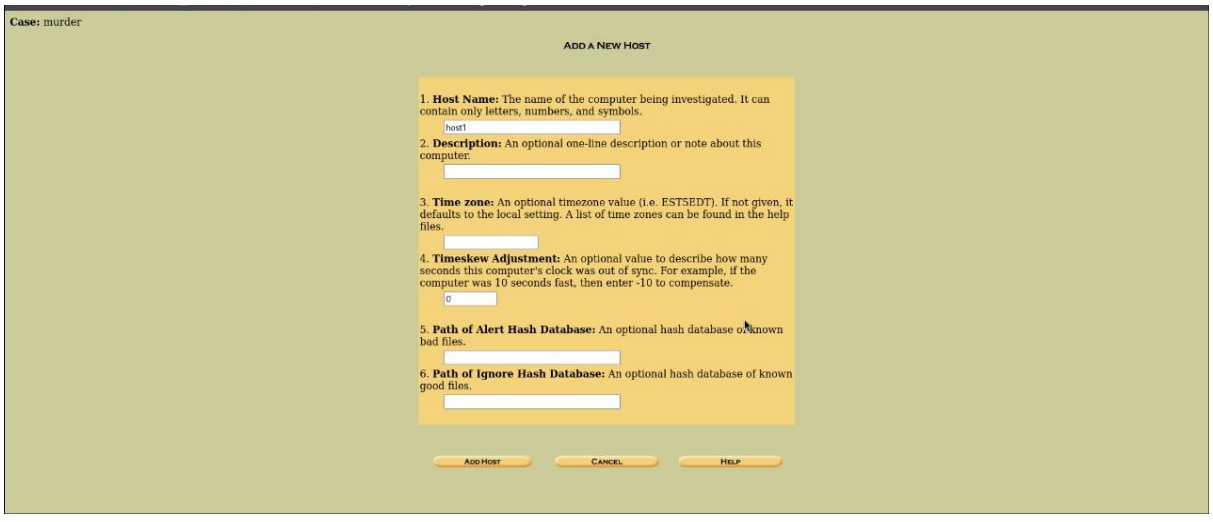
Use Autopsy to create a case and import evidence



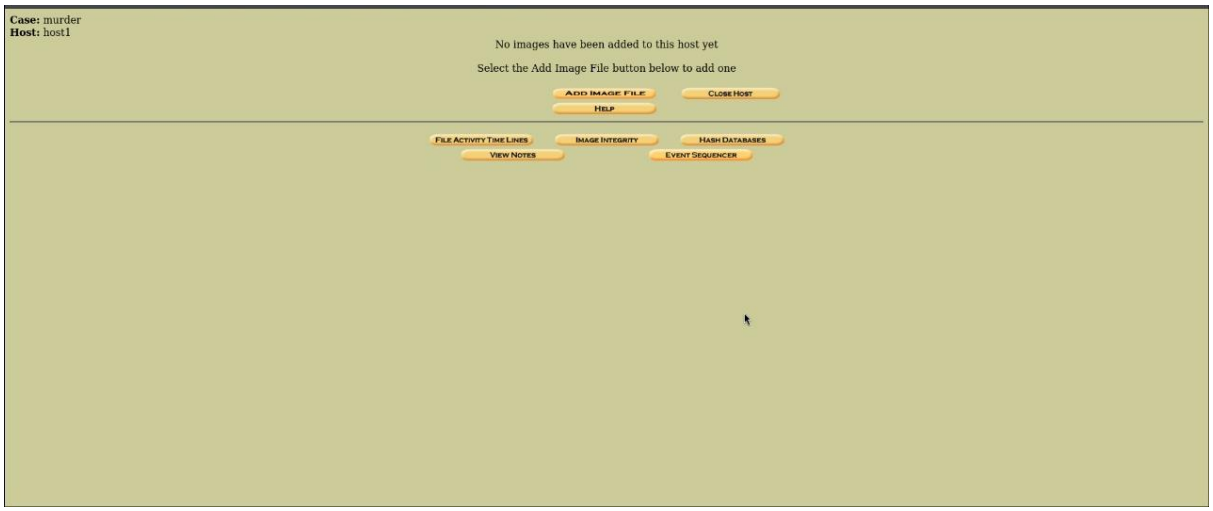


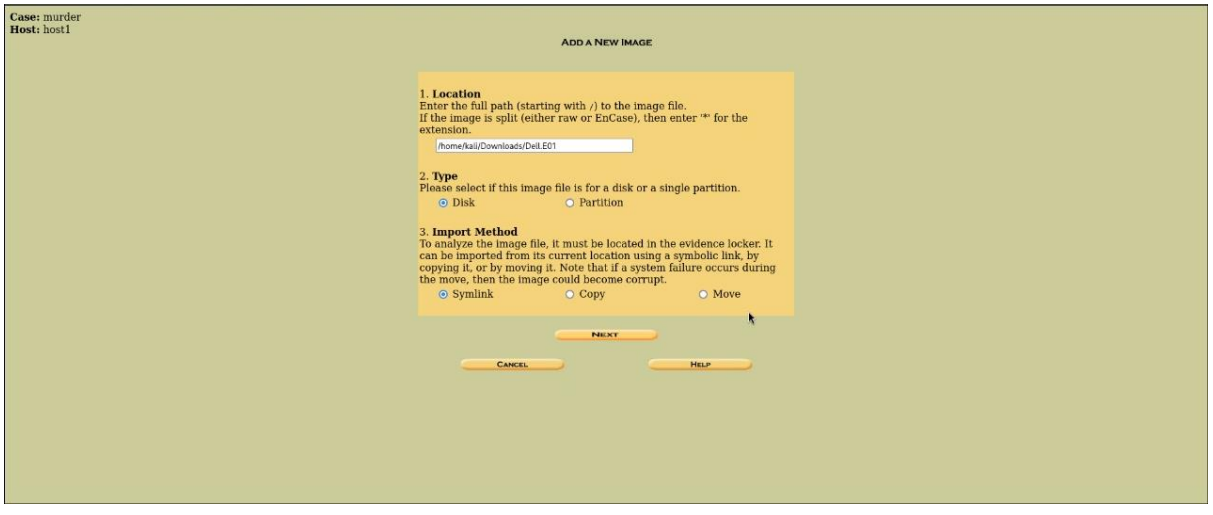

localhost:9999/autopsy?mod=0&view=1&x=82&y=7
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
murder
2. Description: An optional, one line description of this case.
Laptop image from case suicide
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. siva
b. anu
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
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


Adding host: host1 to case murder
Host Directory (/var/lib/autopsy/murder/host1/) created
Configuration file (/var/lib/autopsy/murder/host1/host.aut) created
We must now import an image file for this host
ADD IMAGE


Case: murder
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


Case: murder
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/Dell.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

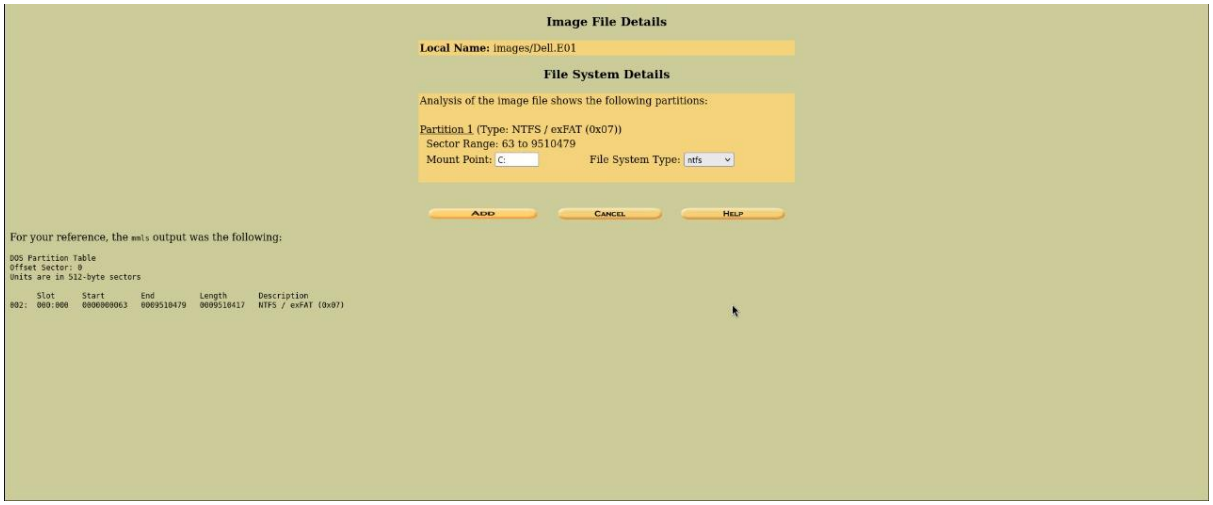
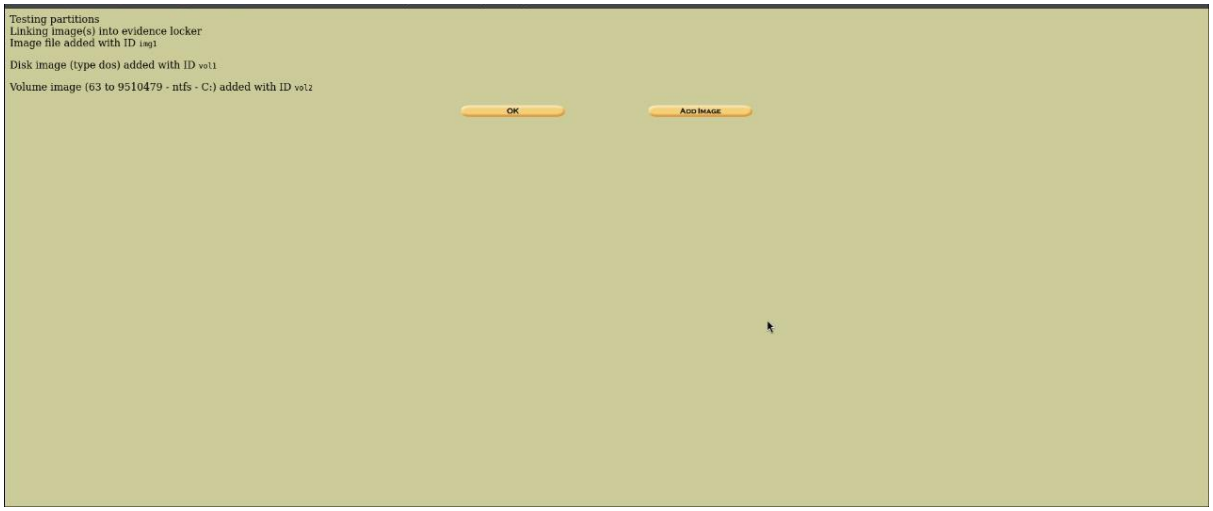
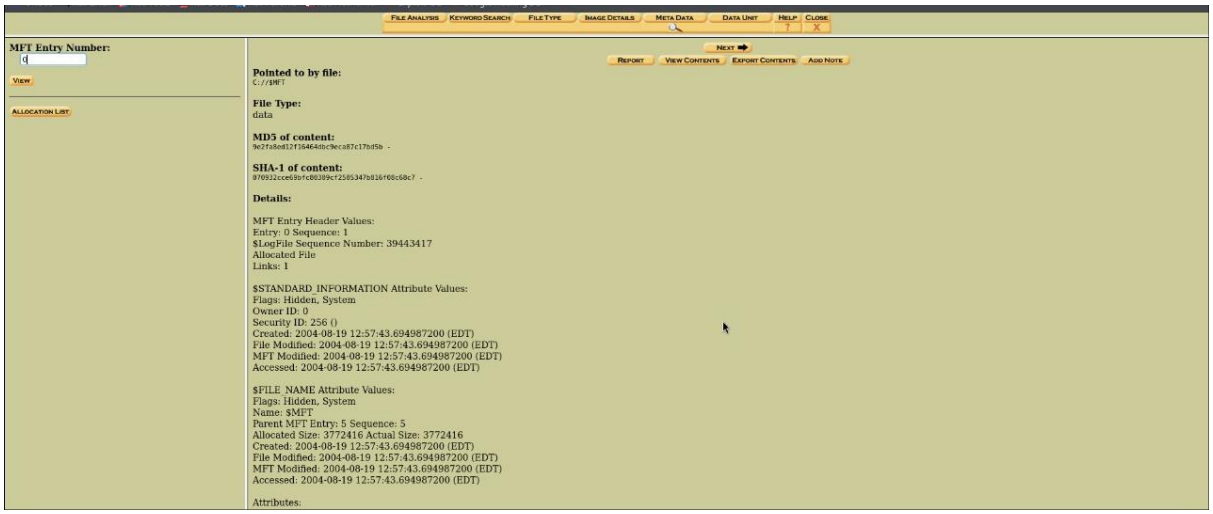
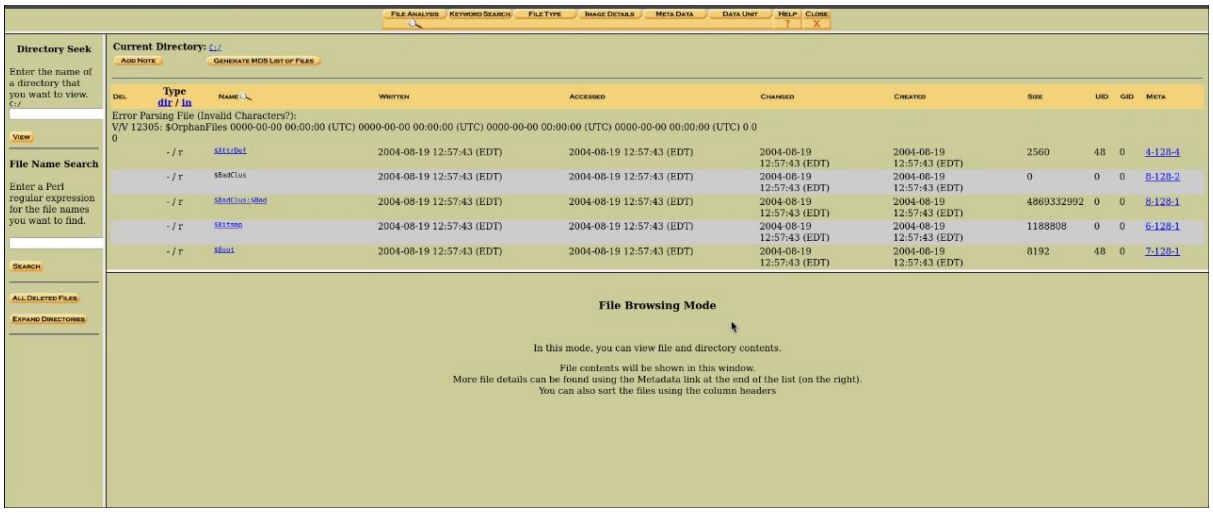


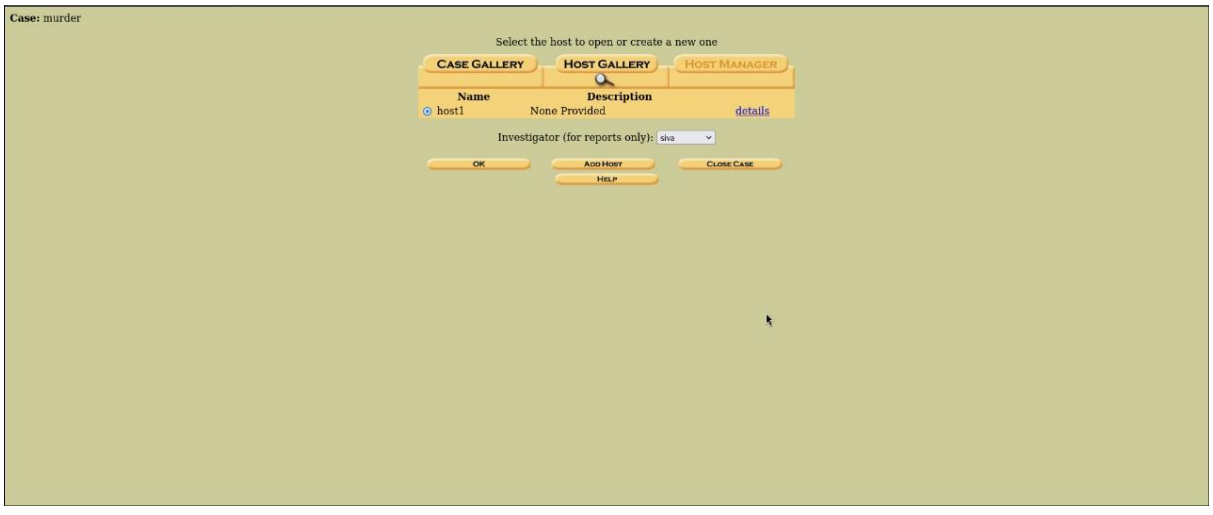
Image File Details
Local Name: images/Dell.E01
File System Details
Analysis of the image file shows the following partitions:
Partition 1 (Type: NTFS / exFAT (0x07))
Sector Range: 63 to 9510479
Mount Point: C:
File System Type: ntfs
ADD
CANCEL
HELP
For your reference, the mmls output was the following:
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
Slot Start End Length Description
002: 000:000 0000000063 0009510479 0009510417 NTFS / exFAT (0x07)


Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Disk image (type dos) added with ID vol1
Volume image (63 to 9510479 - ntfs - C:) added with ID vol2
OK
ADD IMAGE

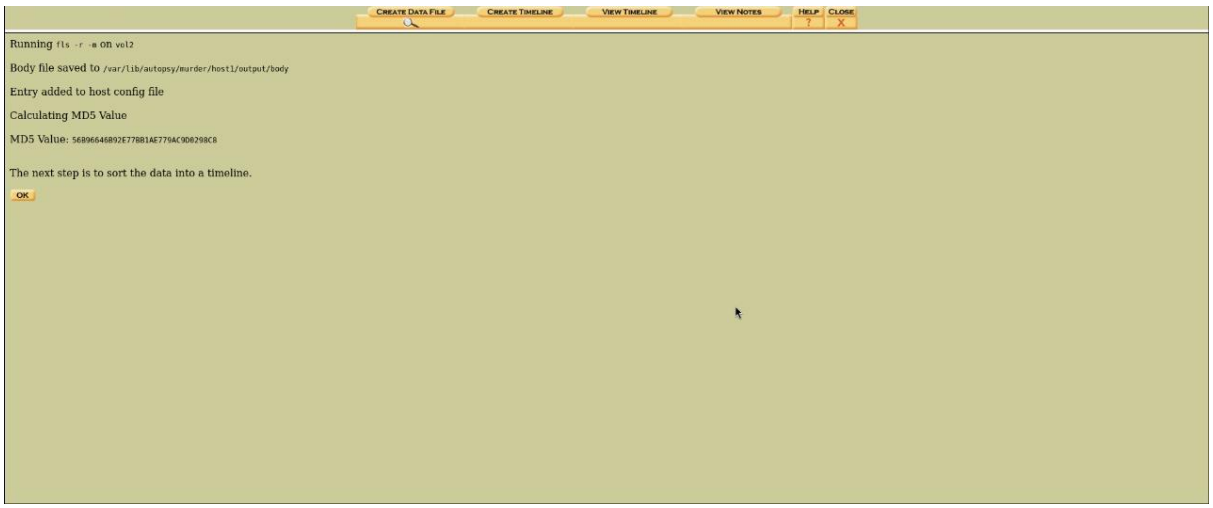

FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
General File System Details
FILE SYSTEM INFORMATION
File System Type: NTFS
Volume Serial Number: B26CB1CE6CB18D9B
OEM Name: NTFS
Version: Windows XP
METADATA INFORMATION
First Cluster of MFT: 2097152
First Cluster of 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
$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:
$INDEX_ROOT (144) Size: No Limit Flags: Resident

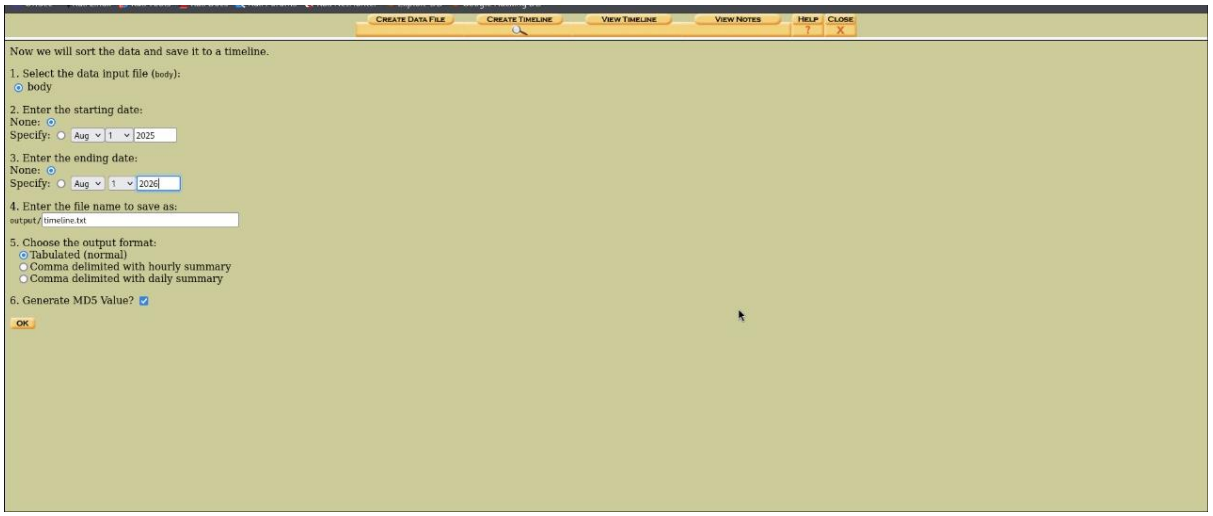

File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
MFT Entry Number:
0
View
Allocation List
Next
Report
View Contents
Export Contents
Add Note
Pointed to by file:
C://$MFT
File Type:
data
MD5 of content:
9e2fa8ed12f16464dbc9eca87c17bd5b -
SHA-1 of content:
070932cce69bfc80389cf2585347b016f68c68c7 -
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:

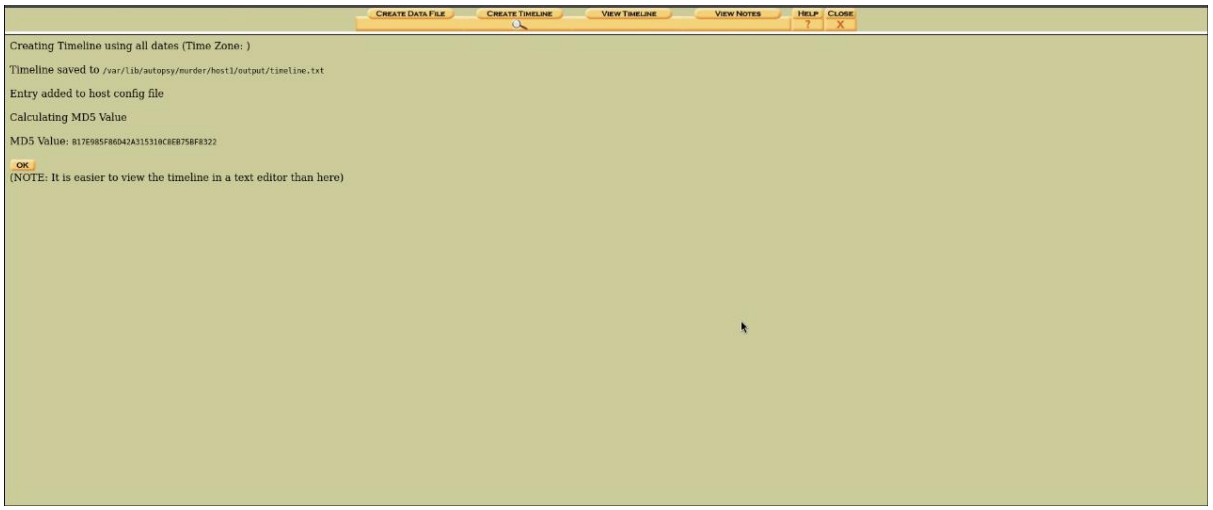

File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
Directory Seek
Enter the name of a directory that you want to view.
C:/
View
File Name Search
Enter a Perl regular expression for the file names you want to find.
Search
All Deleted Files
Expand Directories
Current Directory: C:/
Add Note
Generate MD5 List of Files
Del
Type
dir / in
Name
Written
Accessed
Changed
Created
Size
UID
GID
Meta
Error Parsing File (Invalid Characters?):
V/V 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
$AttrDef
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
$BadClus
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
$BadClus:$Bad
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
$Bitmap
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
$Boot
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

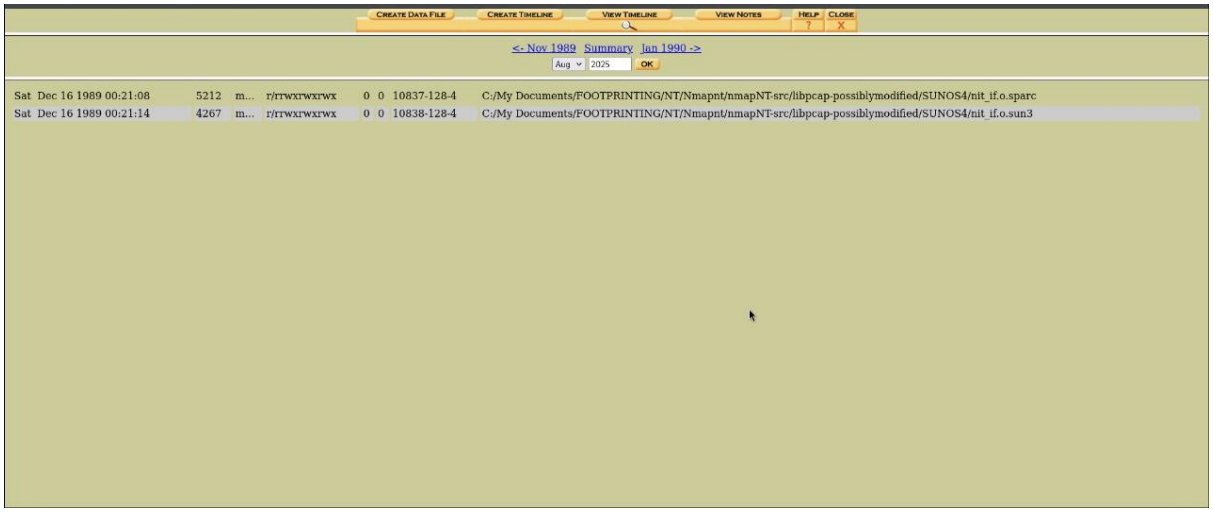

Case: murder
Select the host to open or create a new one
Case Gallery
Host Gallery
Host Manager
Name
Description
host1
None Provided
details
Investigator (for reports only):
siva
OK
Add Host
Close Case
Help


CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
CLOSE
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.E01-63-9510479 ntfs
2. Select the data types to gather:
Allocated Files
Unallocated Files
3. Enter name of output file (body):
output/ body
4. Generate MD5 Value?
OK


CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
CLOSE
Running fls -r -m on vol2
Body file saved to /var/lib/autopsy/murder/host1/output/body
Entry added to host config file
Calculating MD5 Value
MD5 Value: 568966468926778B1AE770AC9D0298C8
The next step is to sort the data into a timeline.
OK


CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
CLOSE
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: Aug 1 2025
3. Enter the ending date:
None:
Specify: Aug 1 2026
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 MD5 Value?
OK


CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
CLOSE
Creating Timeline using all dates (Time Zone:)
Timeline saved to /var/lib/autopsy/murder/host1/output/timeline.txt
Entry added to host config file
Calculating MD5 Value
MD5 Value: 817E985F86D42A315310C8EB75BF8322
OK
(NOTE: It is easier to view the timeline in a text editor than here)


CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
CLOSE
<- Nov 1989 Summary Jan 1990 ->
Aug
2025
OK
Sat Dec 16 1989 00:21:08 5212 m... r/rrwxrwxrwx 0 0 10837-128-4 C:/My Documents/FOOTPRINTING/NT/Nmapnt/nmapNT-src/libpcap-possiblymodified/SUNOS4/nit_if.o.sparc
Sat Dec 16 1989 00:21:14 4267 m... r/rrwxrwxrwx 0 0 10838-128-4 C:/My Documents/FOOTPRINTING/NT/Nmapnt/nmapNT-src/libpcap-possiblymodified/SUNOS4/nit_if.o.sun3


CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
CLOSE
File Activity Timelines
Here you can create a timeline of file activity.
This process requires two steps:
1. Create Data File from file system data -> 2. Create Timeline from the data file
Use the tabs above to start.