

## Digital Forensics Task

### What is Digital Forensics?

Investigating digital devices in order to gather, examine, and preserve evidence for legal reasons is known as digital forensics.

### Important Ideas:

- An HDD, SSD, or USB disk image is a bit-by-bit replica of the whole storage device.
- Evidence Integrity: Using hashing (SHA-256, MD5) to make sure the evidence is not altered.
- Data Volatility: If the power is turned off, the data in RAM is lost, but the data on the drive is left.
- Chain of Custody: Recording the methods used to gather, preserve, and examine evidence.

### Autopsy

Autopsy is an open-source digital forensics application that may be used to examine disk images, retrieve erased data, and look into online fraud.

### Installation

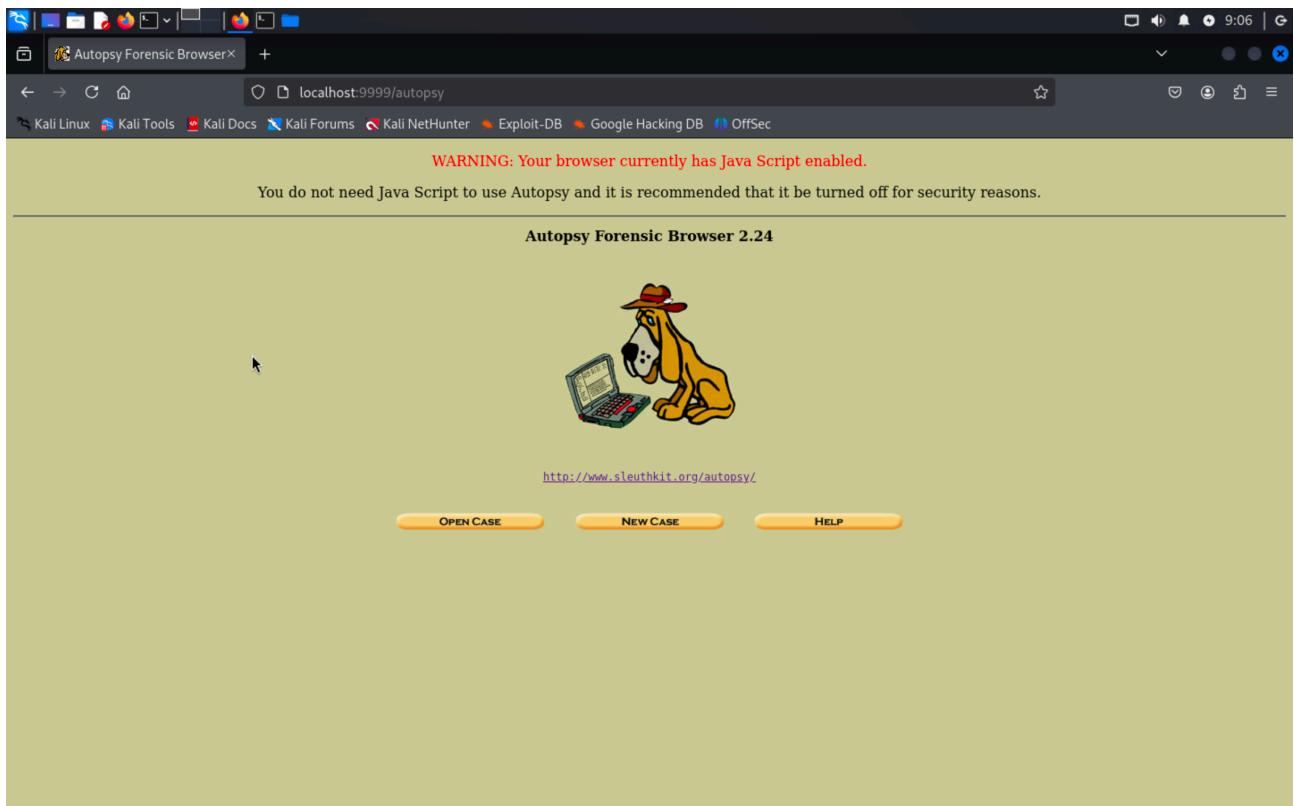
```
(kali㉿kali)-[~] You do not need Java Script to use Autopsy and it is rec
$ autopsy
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

Evidence Locker: /var/lib/autopsy
Start Time: Sat Feb 8 09:04:38 2025
Remote Host: localhost
Local Port: 9999

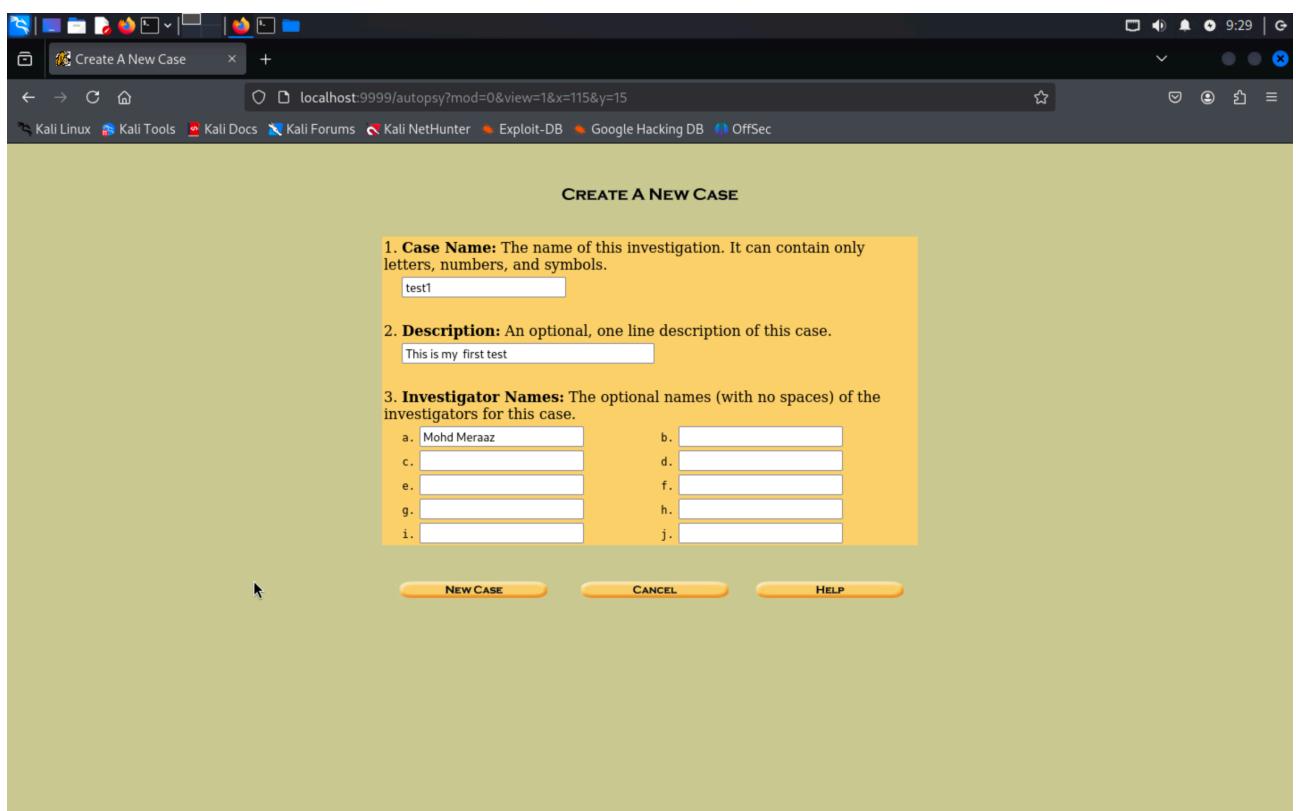
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
[ http://www.sleuthki
[ OPEN CASE ] [ NEW C
]
```

**After the installation we open the given link in the browser**



**Then goto new case**



## Create host

### Creating Case: test1

Case directory (/var/lib/autopsy/test1/) created  
Configuration file (/var/lib/autopsy/test1/case.aut) created

We must now create a host for this case.

**ADD HOST**

### After click on add host

The screenshot shows a web browser window titled "Add A New Host To test1". The URL is "localhost:9999/autopsy?mod=0&view=7&case=test1&x=102&y=9". The page displays a form for adding a new host to the "test1" case. The form consists of six numbered steps:

- 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.  
[empty input field]
- 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.  
[empty input field]
- 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.  
[empty input field]
- 6. Path of Ignore Hash Database:** An optional hash database of known good files.  
[empty input field]

At the bottom of the form are three buttons: "ADD HOST", "CANCEL", and "HELP".

Then click on add host again

We get this page , click on add image

## Adding host: host1 to case test1

Host Directory (/var/lib/autopsy/test1/host1/) created

Configuration file (/var/lib/autopsy/test1/host1/host.aut) created

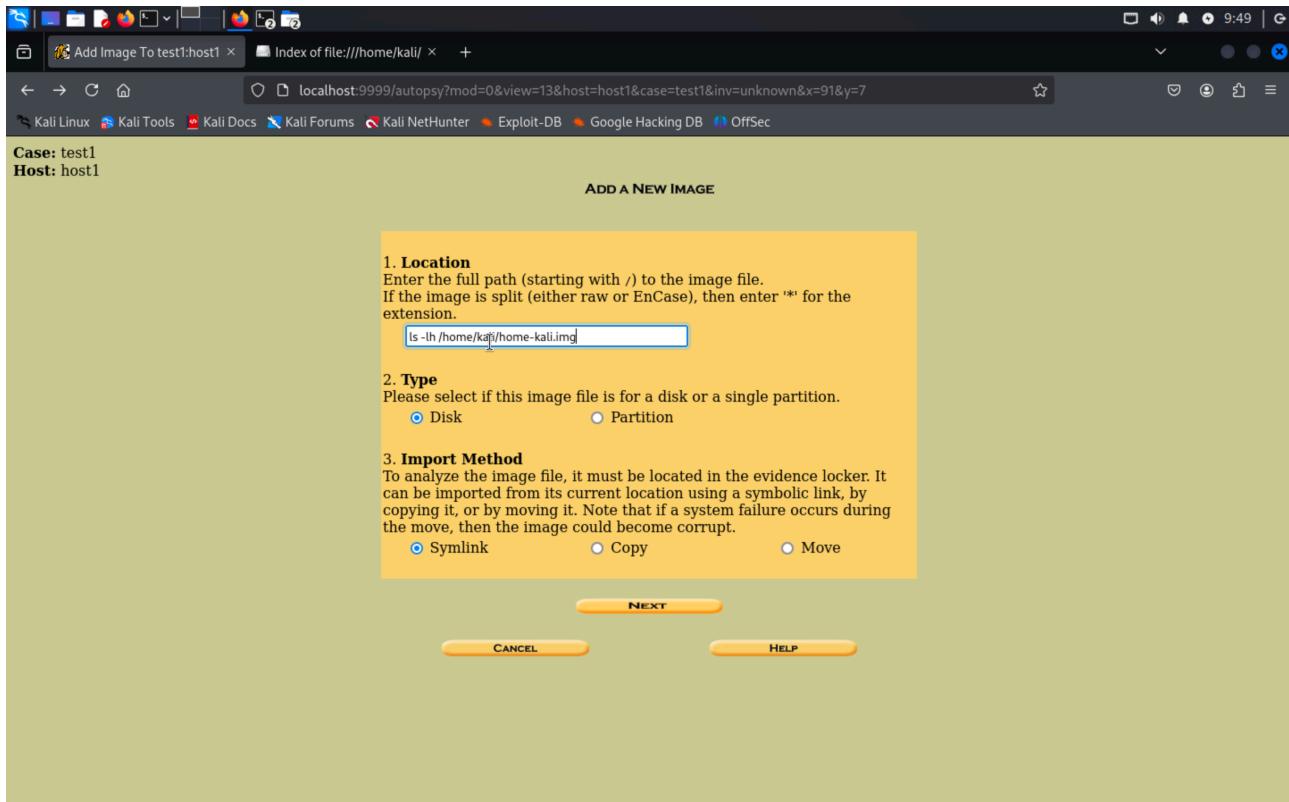
We must now import an image file for this host

**ADD IMAGE**

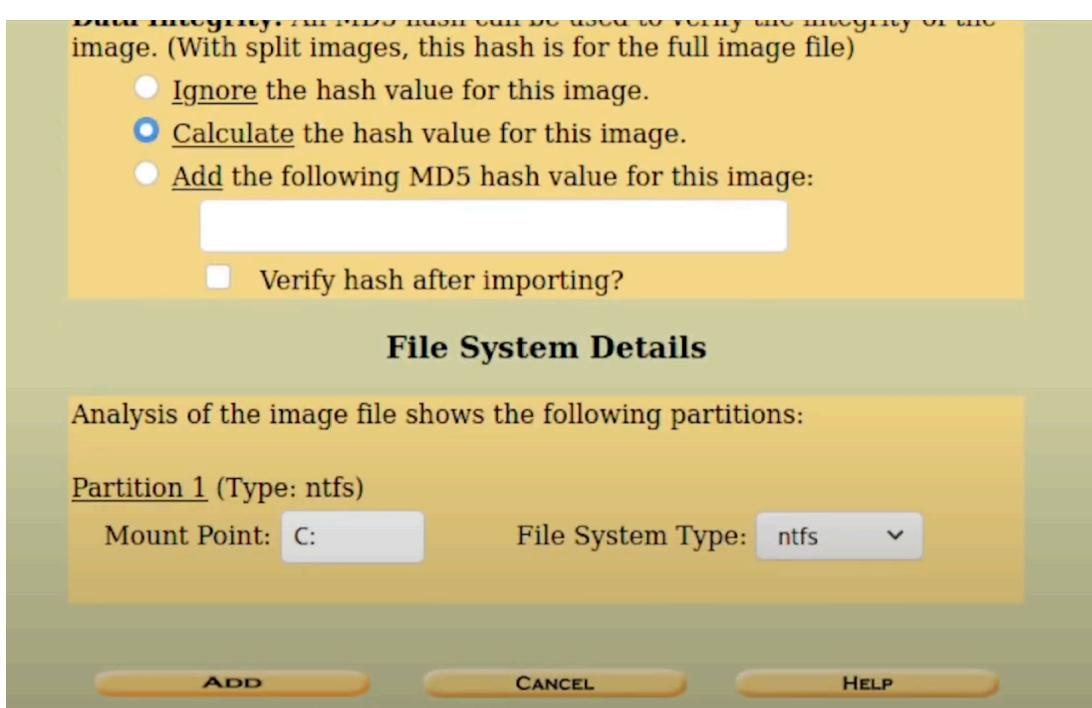
Then add image file

The screenshot shows a web browser window for the Autopsy Forensic Browser. The URL in the address bar is `localhost:9999/autopsy?mod=0&view=10&case=test1&host=host1`. The page title is "Open Image In test1:host1". The main content area displays the message "No images have been added to this host yet" and "Select the Add Image File button below to add one". Below this text are two orange buttons: "ADD IMAGE FILE" and "CLOSE HOST". Underneath these buttons is a horizontal menu bar with several items: FILE ACTIVITY TIME LINES, IMAGE INTEGRITY, HASH DATABASES, VIEW NOTES, and EVENT SEQUENCER. At the bottom of the page, there is a footer bar with the URL `localhost:9999/autopsy?case=test1&host=host1&mod=10&view=6`.

**After that , click next**



**then click on add button then click ok**



Thereafter we analyze → click on analyze

Case: Case1  
Host: host1

Select a volume to analyze or add a new image file.

CASE GALLERY		HOST GALLERY		HOST MANAGER	
mount	name			fs type	details
C:/	samplepartition.img-0-0			ntfs	<a href="#">details</a>

[ANALYZE](#)

[ADD IMAGE FILE](#)

[CLOSE HOST](#)

[HELP](#)

[FILE ACTIVITY TIME LINES](#)

[IMAGE INTEGRITY](#)

[HASH DATABASES](#)

[VIEW NOTES](#)

[EVENT SEQUENCER](#)

Then we goto → file analysis>then del1/ folder

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

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

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

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

**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

d / d	<a href="#">alloc/</a>	23:59:10 (EDT)	23:59:10 (EDT)
d / d	<a href="#">archive/</a>	2004-06-09 23:27:36 (EDT)	2004-06-09 23:27:36 (EDT)
d / d	<a href="#">del1/</a>	2004-06-09 23:28:51 (EDT)	2004-06-09 23:28:52 (EDT)
d / d	<a href="#">del2/</a>	2004-06-09 23:59:15 (EDT)	2004-06-09 23:59:15 (EDT)

**Here we get our deleted file as it is**

The screenshot shows a file analysis interface with the following details:

**Top Navigation:** Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security.

**Toolbar:** FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, CLOSE.

**Left Panel - Directory Seek:** Enter the name of a directory that you want to view. C:/

**Left Panel - File Name Search:** Enter a Perl regular expression for the file names you want to find.

**Main Table:** Shows a list of files with the following columns: DEL, Type, NAME, WRITTEN, ACCESSED.

DEL	Type	NAME	WRITTEN	ACCESSED
	dir / in	..	2004-06-09 23:59:10 (EDT)	2004-06-09 23:59:10 (EDT)
	d / d	..	2004-06-09 23:59:15 (EDT)	2004-06-09 23:59:15 (EDT)
✓	- / r	file6.jpg	2004-06-10 02:48:08 (EDT)	2004-06-09 23:28:00 (EDT)

**Bottom Panel:** ASCII (display - report), \* Hex (display - report), \* ASCII Strings (display - report), \* Export, \* View, \* Add Note.

**Preview Area:** I AM PICTURE #3

**Thank you**

