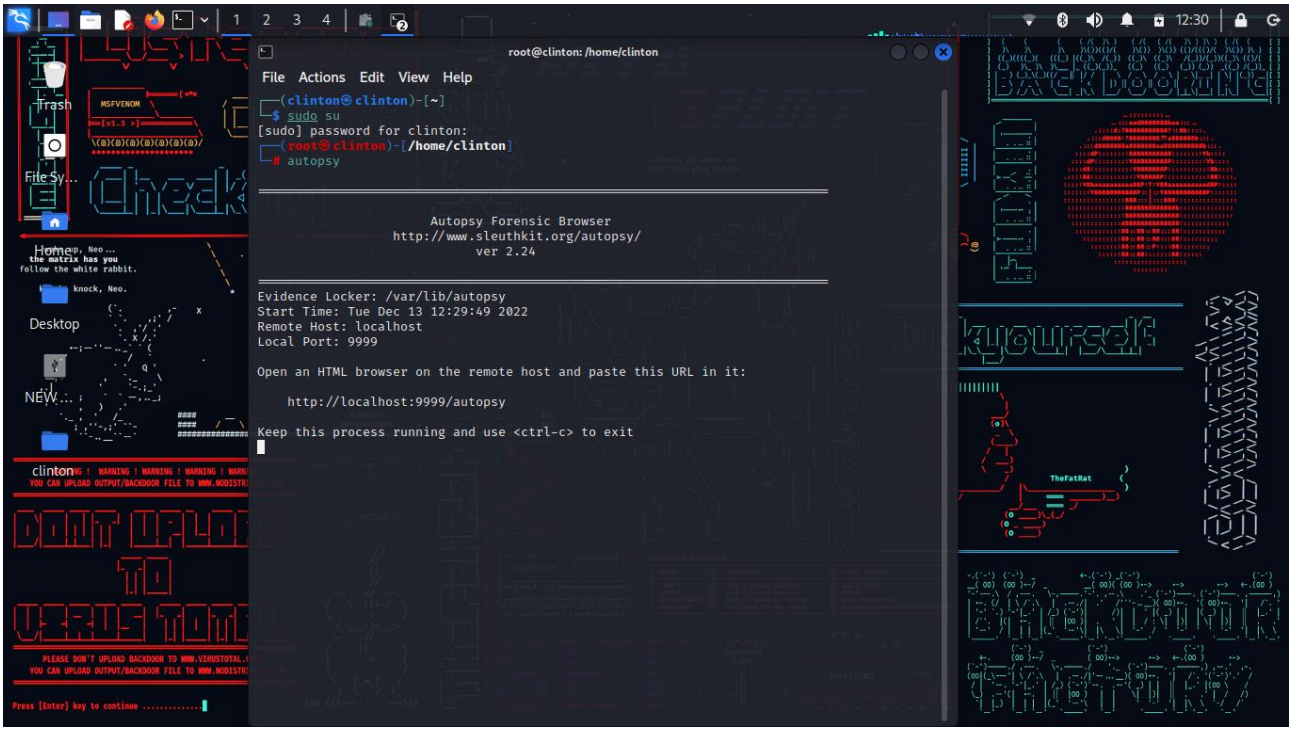
2} **AUTOSPY**

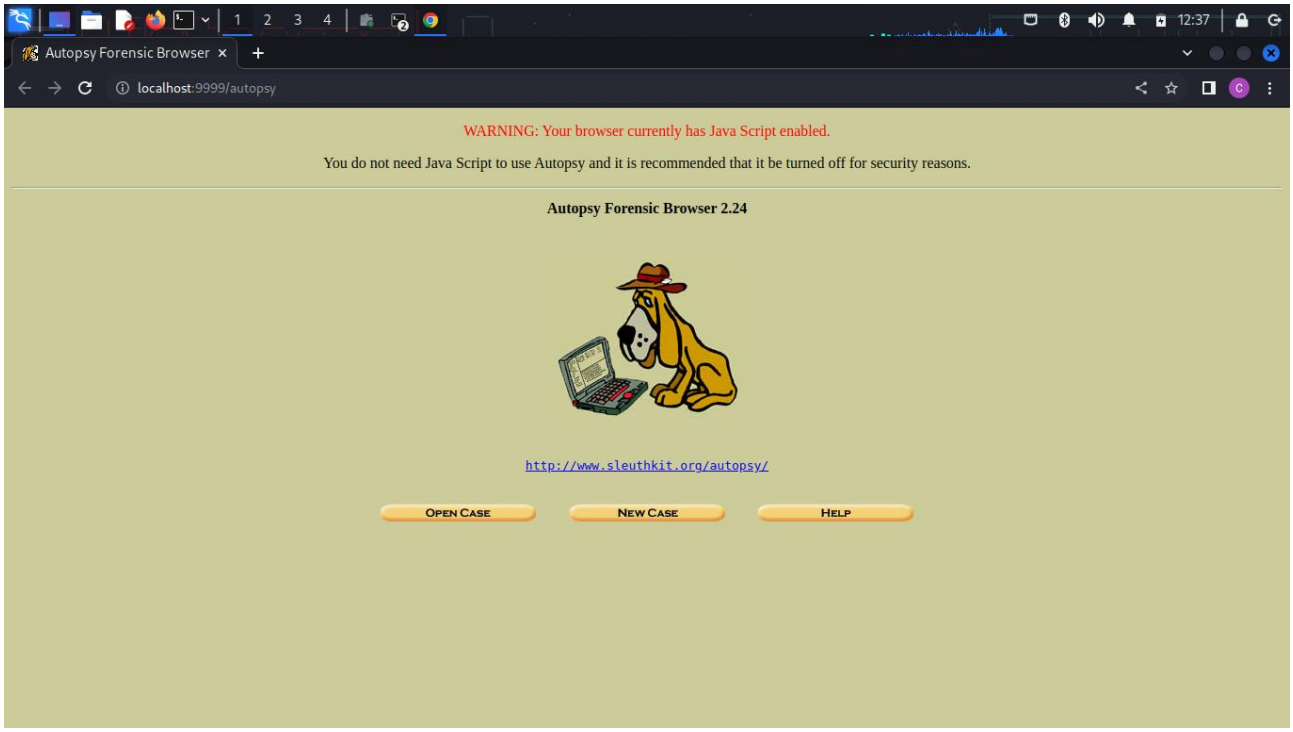
Autopsy is like a special magnifying glass for computers. When someone wants to see what's hidden on a computer or phone, like finding lost pictures or figuring out why something broke, they use Autopsy. It helps people like detectives, police, or computer doctors look at the insides of a computer without messing it up.

Autopsy provides a GUI to perform cyber forensic investigations like file hashing, deleted file recovery, file

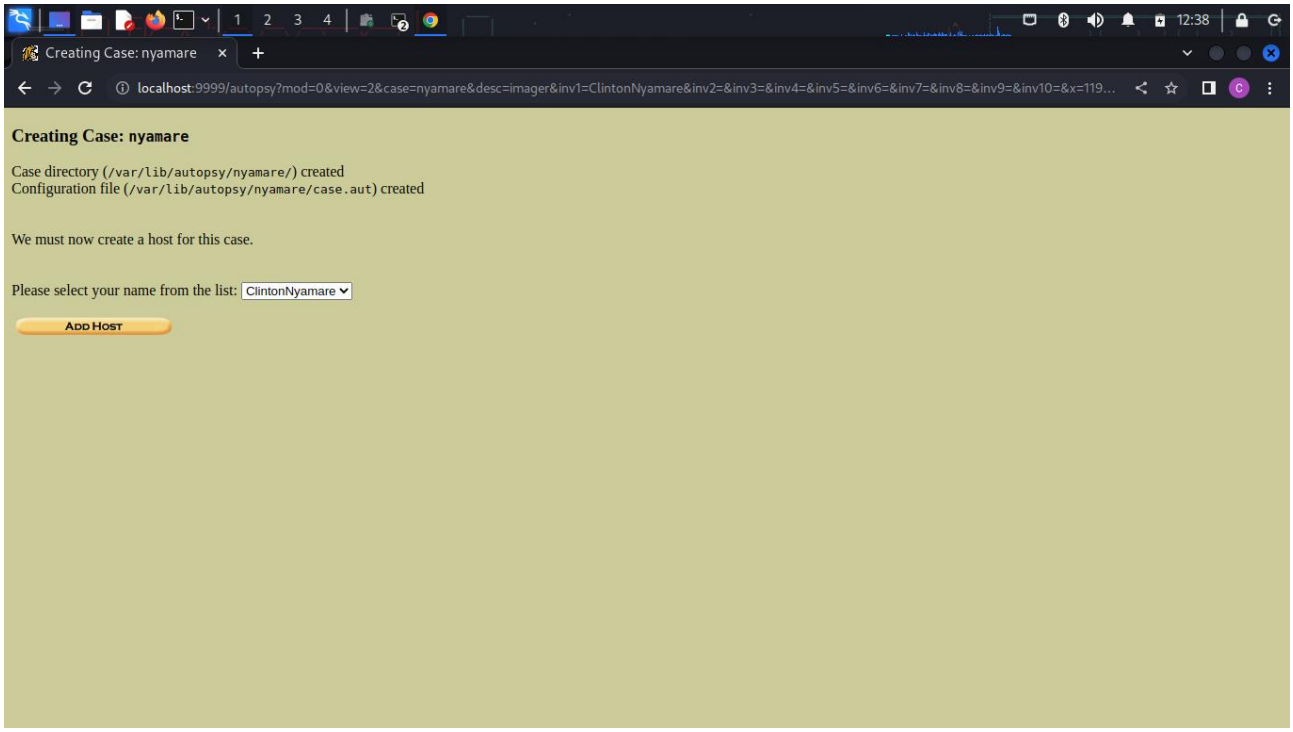


Start autopsy from the command line. It automatically opens the default browser as it runs as a web application.

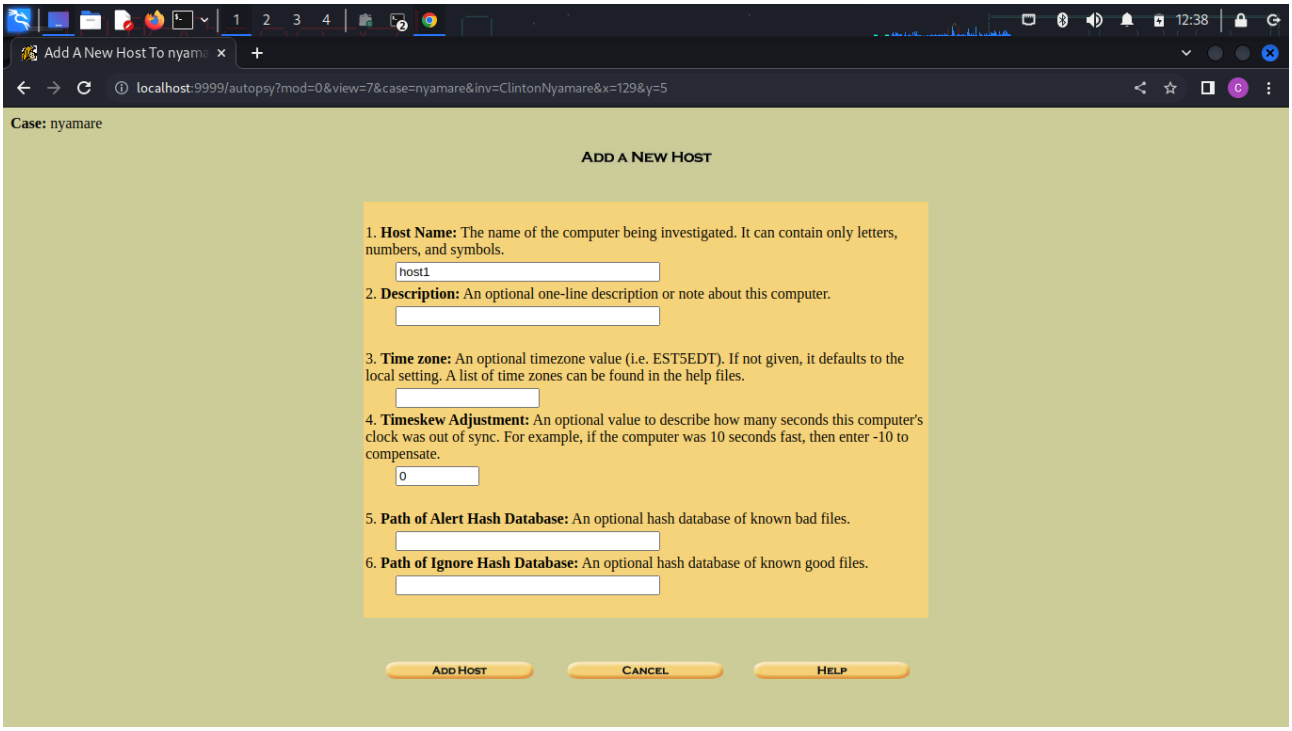
Step 2: Start a New Case



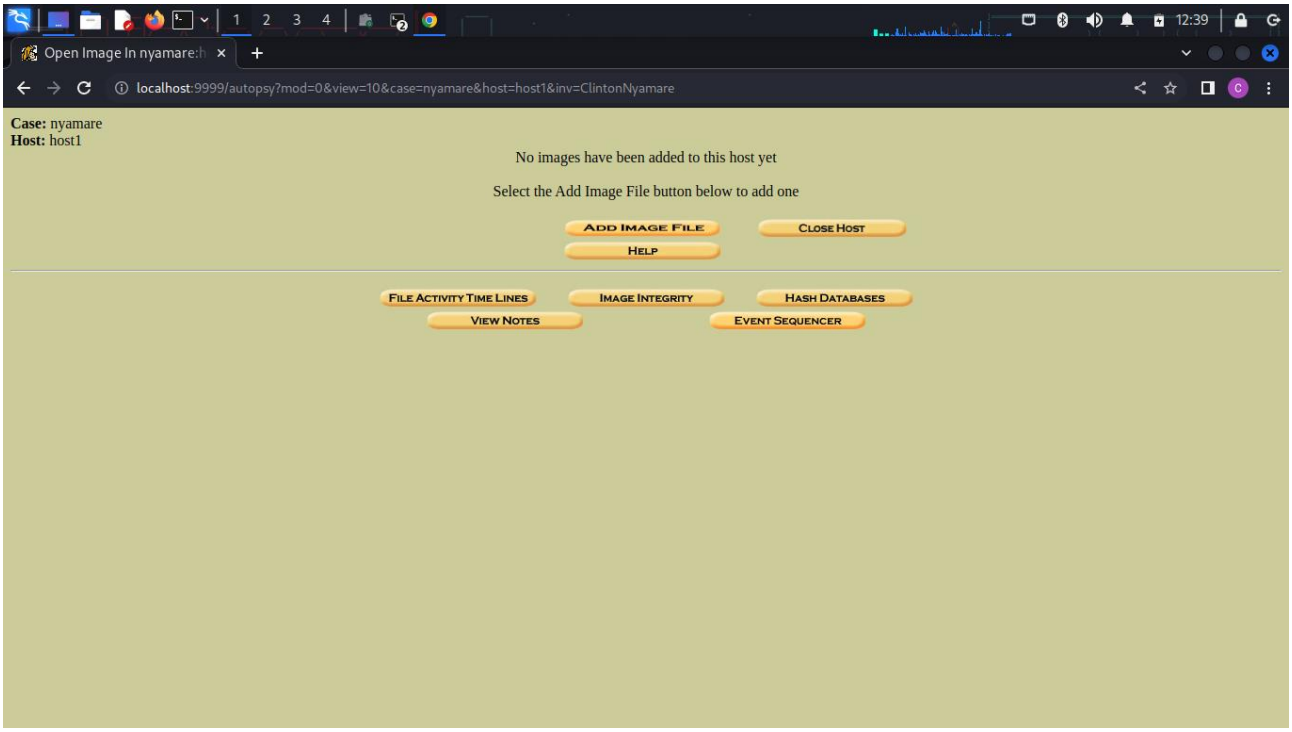
1. In the browser, click "Create New Case."
2. Fill in the case name, description, and examiner information.
3. Choose the location to store your case files



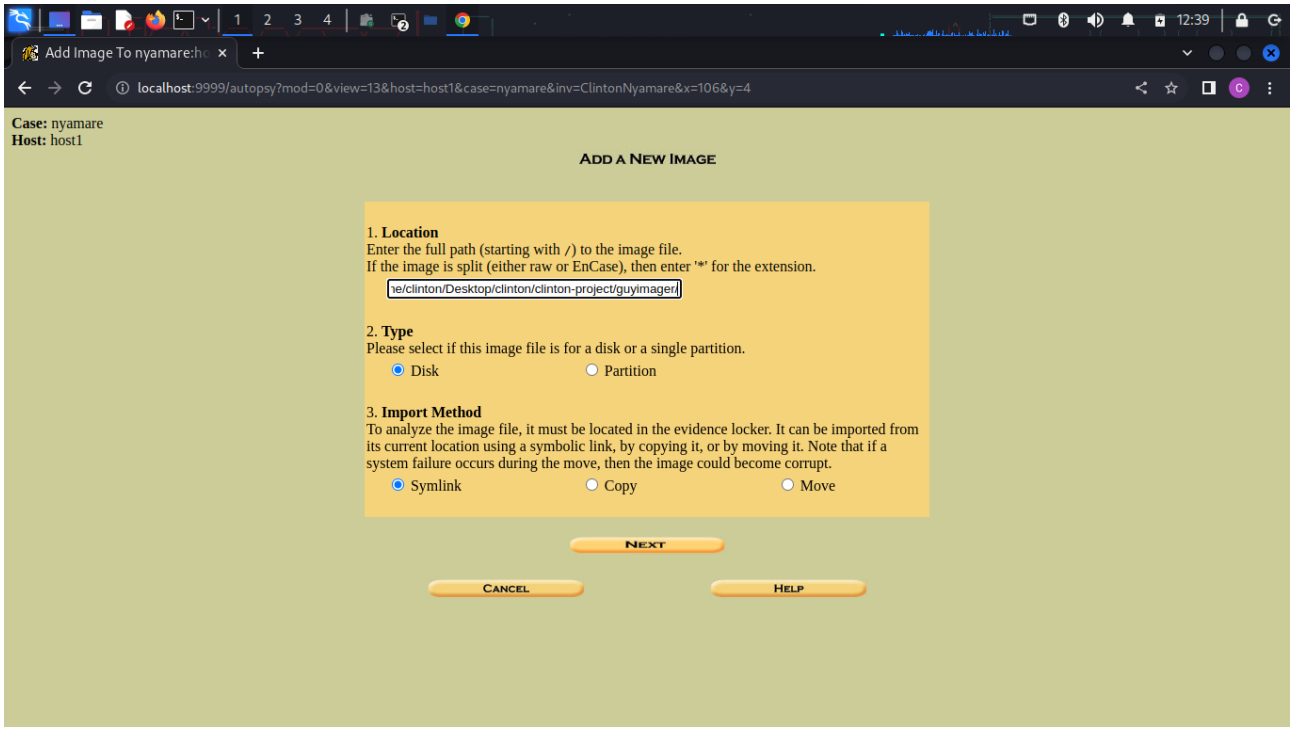
choose also the host name of the computer being investigated.



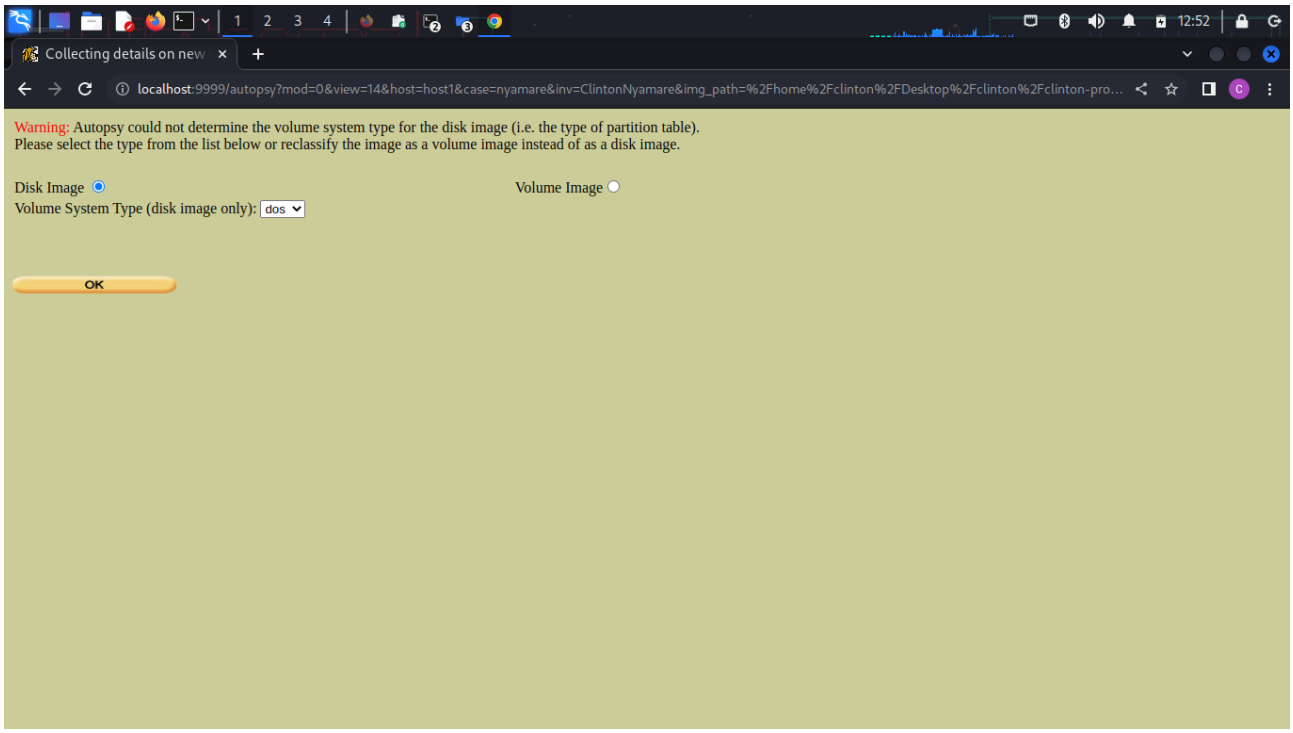
Click on add a new image file to incorporate a disk image or similar file for forensic analysis

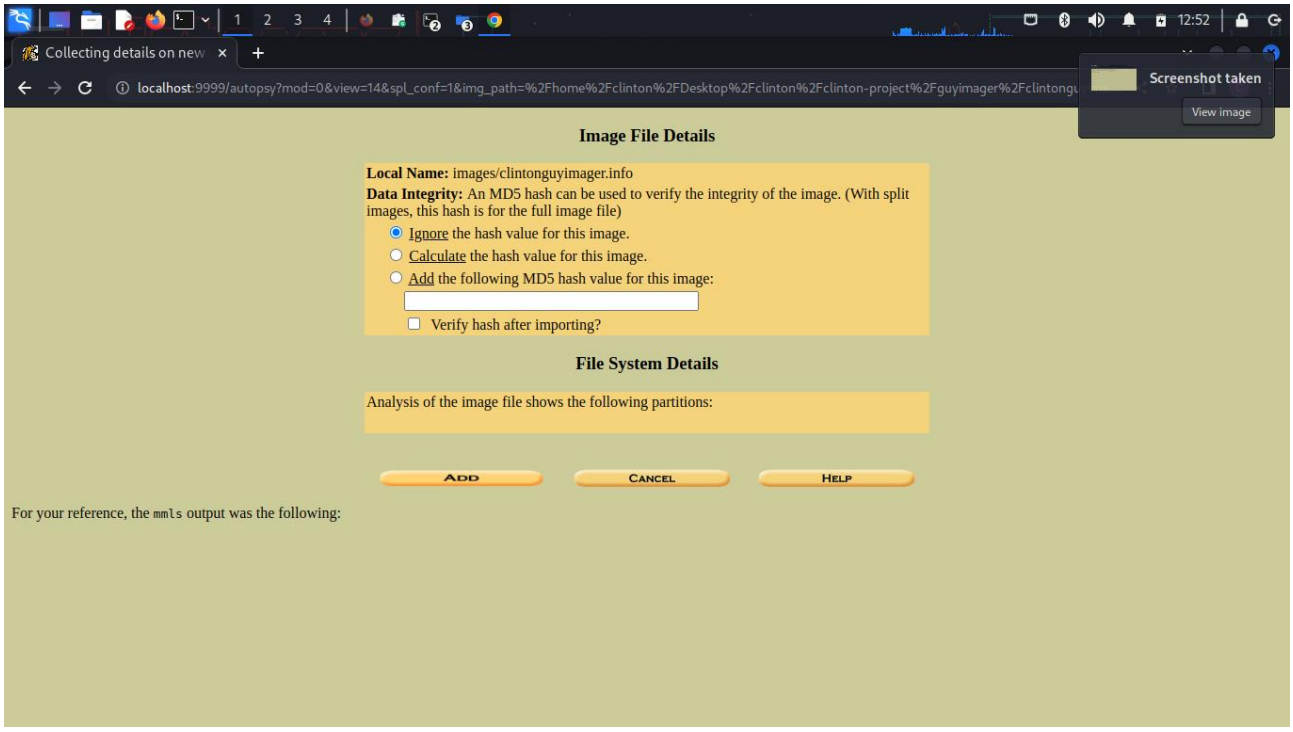


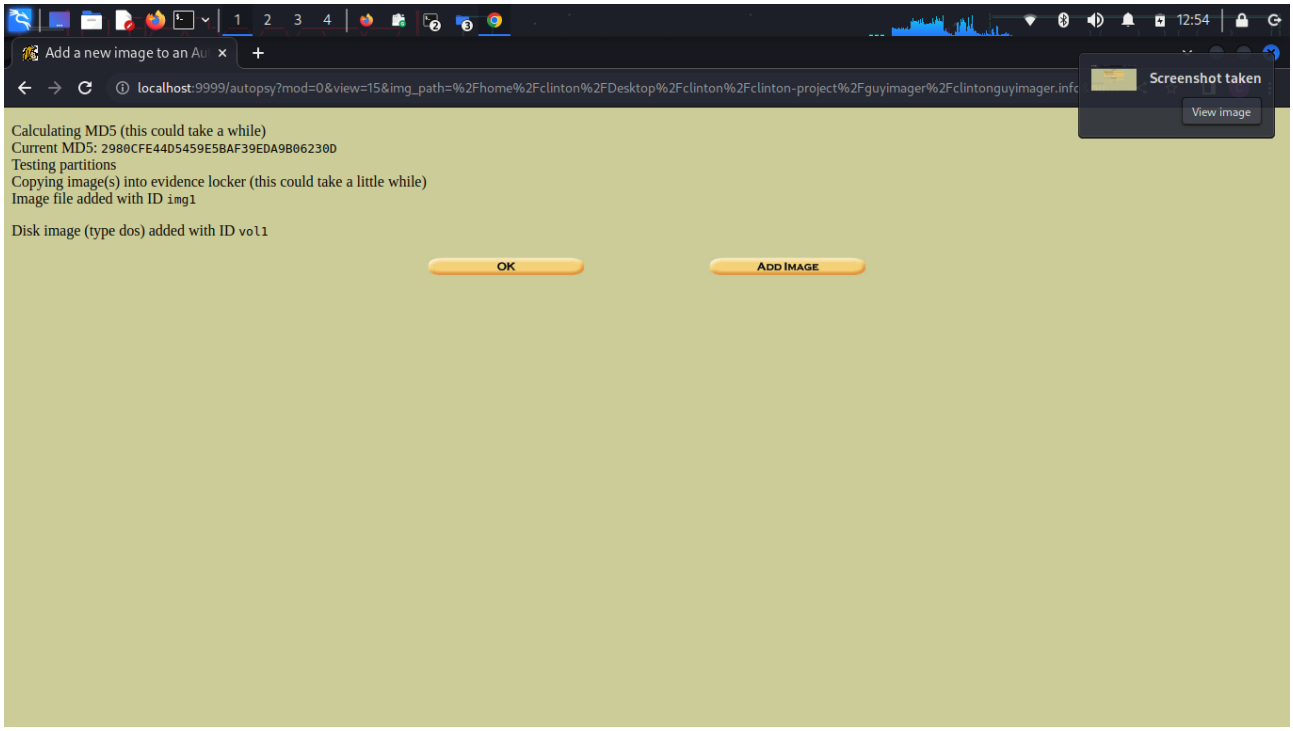
Choose the location of the image, its image is a disk or a single partion and choose the import method.

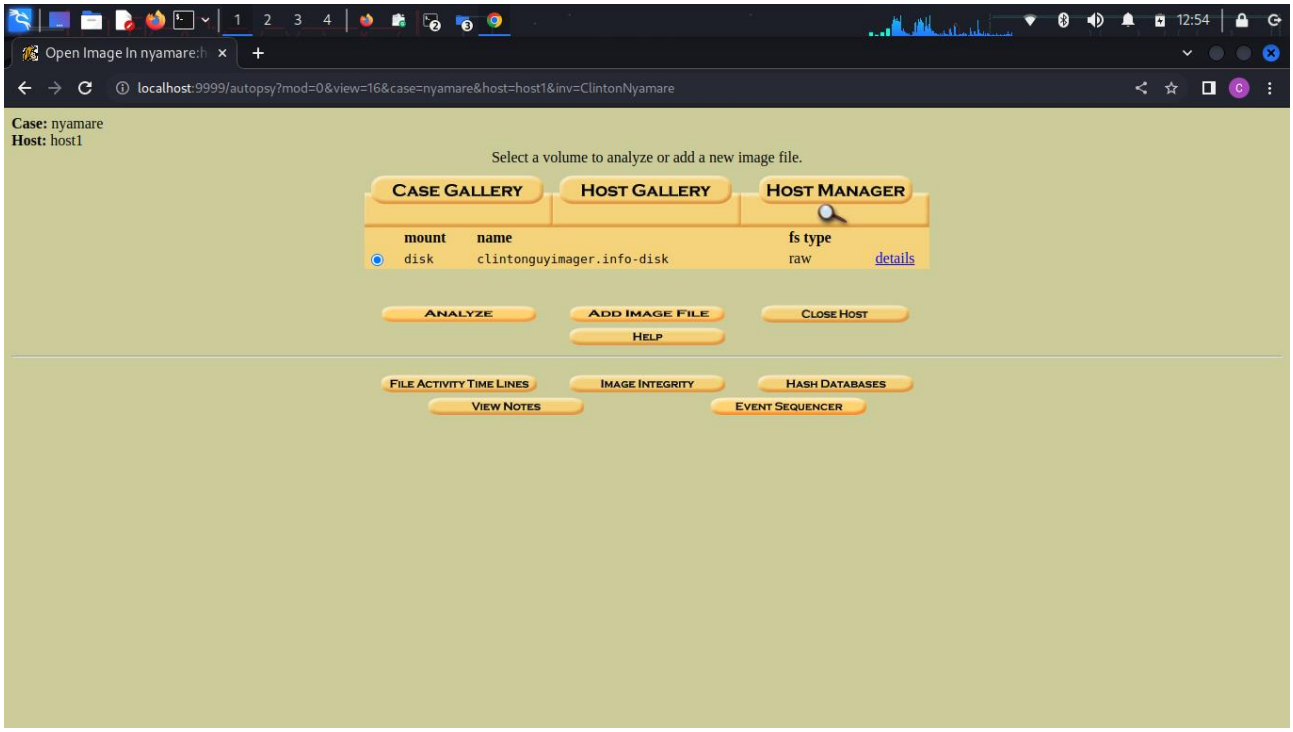


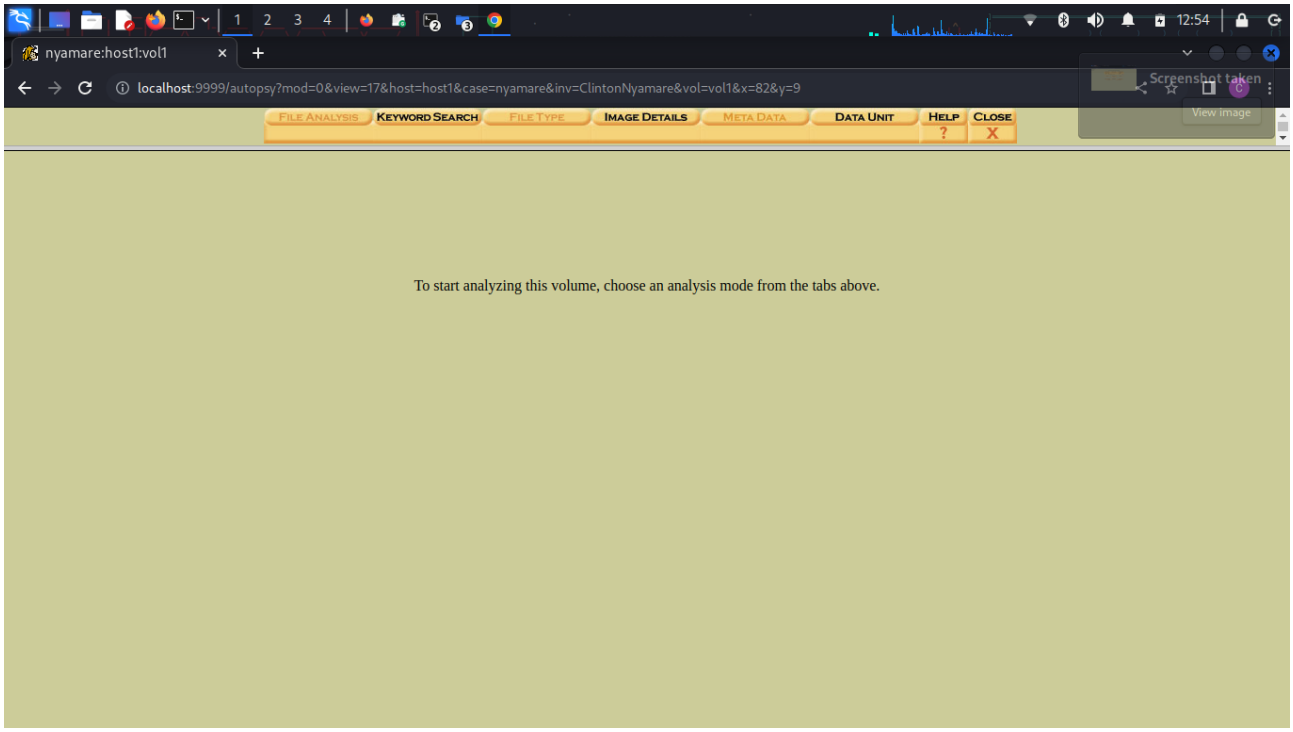
In case of an error re- clarify your options and press ok

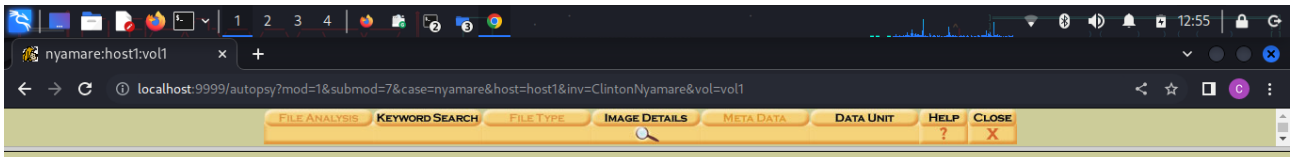





1 2 3 4
12:54
Add a new image to an Au
localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fclinton%2FDesktop%2Fclinton%2Fclinton-project%2Fguyimager%2Fclintonguyimager.inf
Screenshot taken
View image
Calculating MD5 (this could take a while)
Current MD5: 2980CFE44D5459E5BAF39EDA9B06230D
Testing partitions
Copying image(s) into evidence locker (this could take a little while)
Image file added with ID img1
Disk image (type dos) added with ID vol1
OK
ADD IMAGE

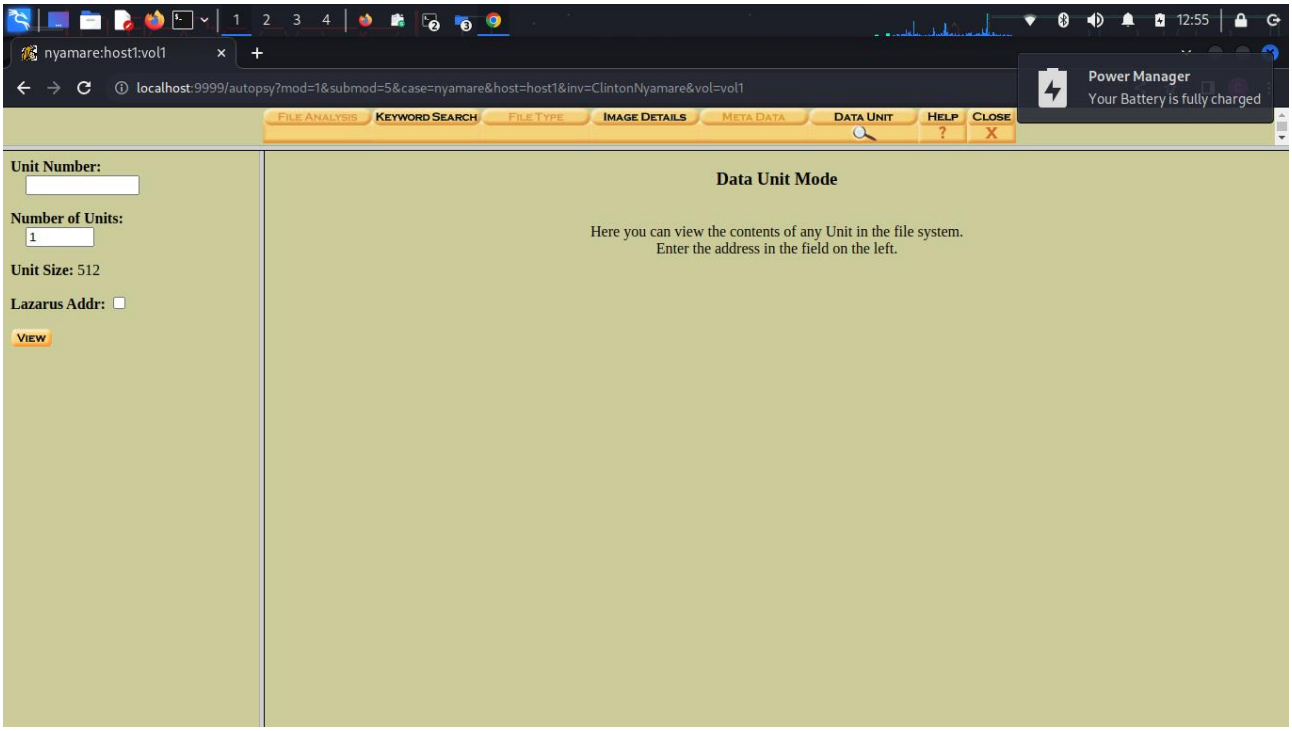

Open Image In nyamare:h
localhost:9999/autopsy?mod=0&view=16&case=nyamare&host=host1&inv=ClintonNyamare
Case: nyamare
Host: host1
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
disk
clintonguyimager.info-disk
raw
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER


nyamare:host1:vol1
localhost:9999/autopsy?mod=0&view=17&host=host1&case=nyamare&inv=ClintonNyamare&vol=vol1&x=82&y=9
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Screenshot taken
View image
To start analyzing this volume, choose an analysis mode from the tabs above.



Disk Image Details

PARTITION INFORMATION


nyamare:host1:vol1
localhost:9999/autopsy?mod=1&submod=5&case=nyamare&host=host1&inv=ClintonNyamare&vol=vol1
Power Manager
Your Battery is fully charged
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Unit Number:
Number of Units:
1
Unit Size: 512
Lazarus Addr:
VIEW
Data Unit Mode
Here you can view the contents of any Unit in the file system.
Enter the address in the field on the left.

Advantages of Autopsy

Easy to Use: It’s like having a treasure map that shows exactly where to look. You don’t need to be super smart to use it.

Finds Hidden Stuff: If something is deleted or lost, it can help bring it back, like finding a toy under your bed.

Free: You don’t need to pay to use it, like free candy!

Shows a Lot of Information: It can find pictures, videos, messages, or even secrets someone tried to hide.

Disadvantages of Autopsy

Needs a Good Computer: If your computer is slow, Autopsy will also be slow, like walking through sticky mud.

Lots of Information: Sometimes it shows too much, and it’s hard to know what’s important, like too many toys in one box.

Not Perfect: It can miss some stuff, especially if the bad guys are very smart at hiding things.