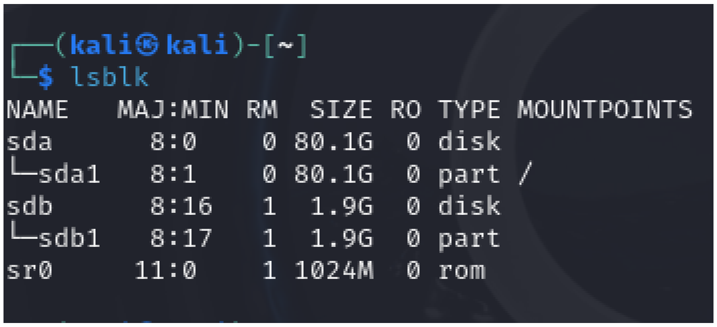
Step-by-Step Guide: Using Autopsy on Kali Linux (v2.24) on Raspberry Pi

1. Starting Autopsy from the Kali Terminal

1. Open Kali Linux.
2. Open a terminal and type the following command lsblk to list all connected drives. This will display all storage devices available on the system. The main drive will be labeled as sda, and any connected USB devices will typically be labeled as sdb, sdc, etc.

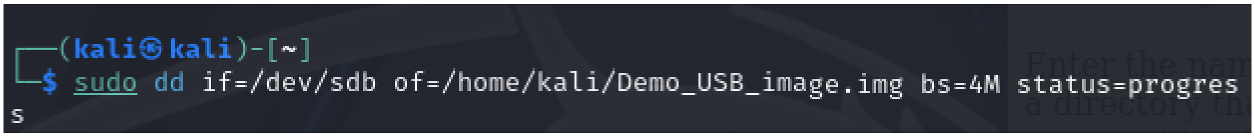


```
┌──(kali㉿kali)-[~]
└─$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 80.1G  0 disk
└─sda1   8:1    0 80.1G  0 part /
sdb      8:16   1  1.9G  0 disk
└─sdb1   8:17   1  1.9G  0 part
sr0     11:0    1 1024M  0 rom
```

3. Confirm the correct USB device by checking its size. If your USB drive is 2GB, you should see an entry for sdb that is around **1.9GB** in size.

Creating an Image of the USB Drive

4. Now that you have identified the drive you want to make the image of use the command sudo dd if=/dev/sdX of=/home/kali/usb_image.image bs=4M status=progress

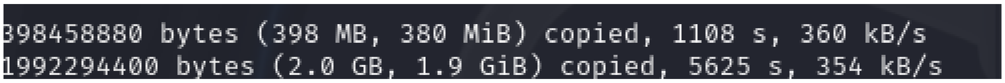


```
┌──(kali㉿kali)-[~]
└─$ sudo dd if=/dev/sdb of=/home/kali/Demo_USB_image.img bs=4M status=progres
s
```

- Replace /dev/sdX with the actual USB device name (e.g., /dev/sdb).
- of=/home/kali/ tells kali where to save the file to so in this case is will be saved to home
- The usb_image.image is the output files name so that will be of=Demo_SUB_image.image

- bs=4M sets the block size for copying.
- status=progress shows the progress of the process.

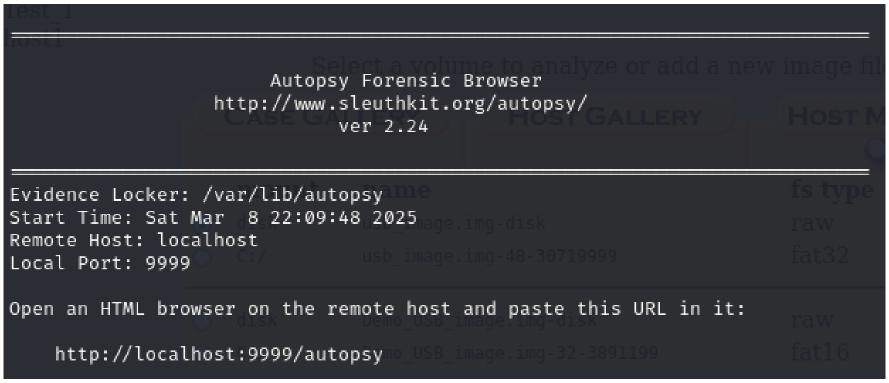
After typing in the command kali will prompt for the sudo password when the command is running it will look something like this:



```
398458880 bytes (398 MB, 380 MiB) copied, 1108 s, 360 kB/s
1992294400 bytes (2.0 GB, 1.9 GiB) copied, 5625 s, 354 kB/s
```

Launching Autopsy

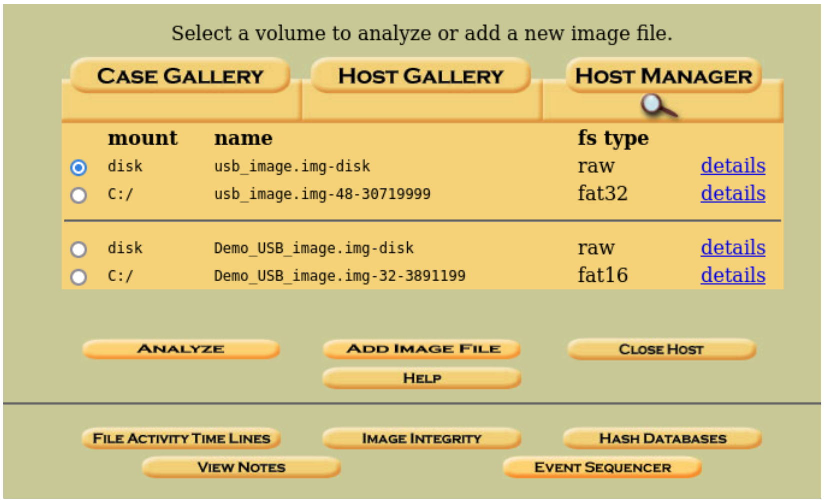
5. The command to launch Autopsy type autopsy into the terminal will redecet you to copy a link into your browser of choice. This will bring up Autopsy’s interface.



```
============================================================================

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

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Sat Mar  8 22:09:48 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
```

2. Loading an Image in Autopsy

Now that you are in Autopys, you would be greeted by this home page.



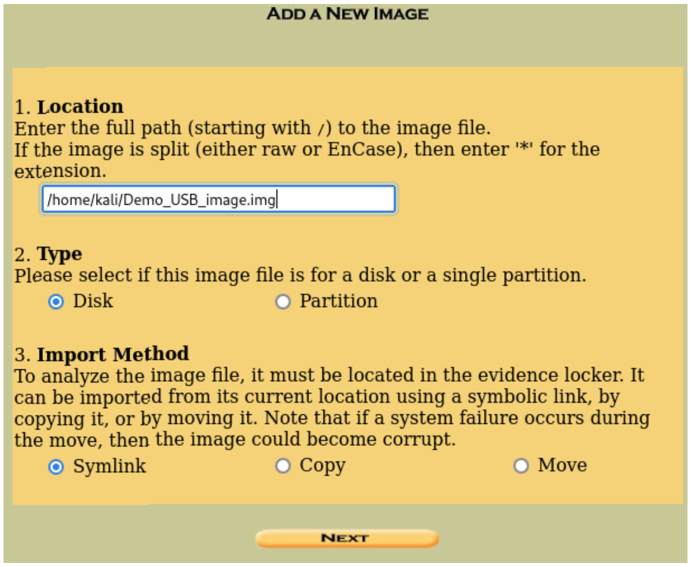
Select a volume to analyze or add a new image file.

	mount	name	fs type	
●	disk	usb_image.img-disk	raw	details
○	C:/	usb_image.img-48-30719999	fat32	details
○	disk	Demo_USB_image.img-disk	raw	details
○	C:/	Demo_USB_image.img-32-3891199	fat16	details

1. To add a new image, click Add Image Fil.e

2. In the Location field, enter the exact file path for the forensic image created earlier.

   That path would be /hime/kali/Demo_USB_image.img click next



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/Demo_USB_image.img

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

3. For the image details have it set up as

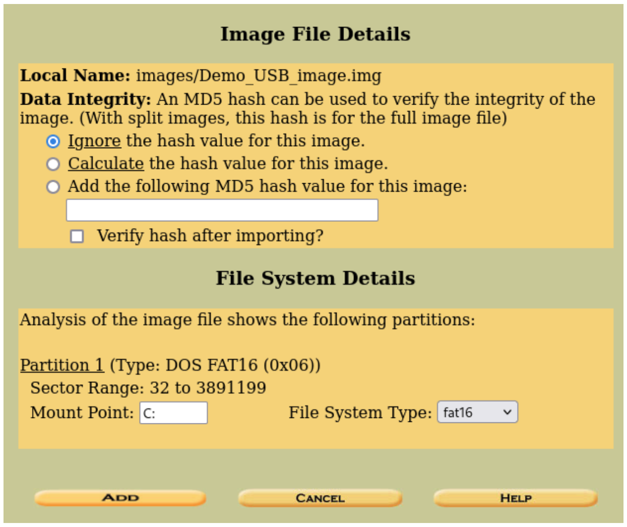


Image File Details

Local Name: images/Demo_USB_image.img
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

● Ignore the hash value for this image.
○ Calculate the hash value for this image.
○ Add the following MD5 hash value for this image:

□ Verify hash after importing?

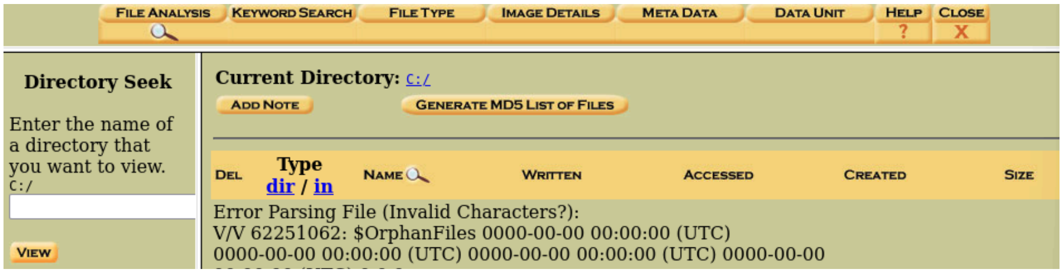
File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: DOS FAT16 (0x06))
Sector Range: 32 to 3891199
Mount Point: C: File System Type: fat16

3. Understanding the Autopsy Interface

Overview of the Main Window Layout



Directory Seek

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

Current Directory: C:/

Error Parsing File (Invalid Characters?):
V/V 62251062: $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

Once the image is loaded, the main Autopsy interface will appear. The top menu bar provides access to several tools:

- File Analysis Tab : Displays all files within the image.
- Keyword Search Tab: Allows searching for specific terms within the image.
- File Type Sorting Tab: Organizes files by type to simplify browsing.
- Image Details Tab: Provides metadata, file system information, and other technical details.
- Metadata Tab: Displays metadata for selected files.

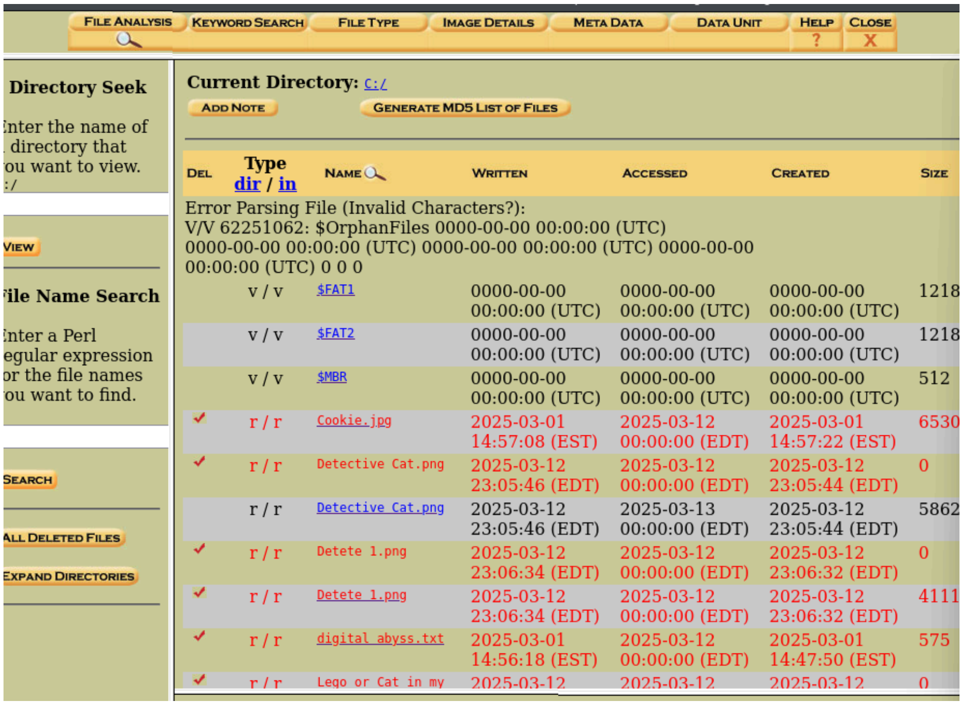
Understanding File Types in Autopsy

- Meta File on the USB are marked as v/v
- Directories are marked as d/d.
- Files are marked as r/r.
- Blue file names indicate existing files.
- Red file names indicate deleted files that may be recoverable.

4. Accessing the Image Contents

- Walk through the prompts to reach the file system view.
  1. You are going to click in the mount, C:/ type, fat16 type for the Demo image
  2. Then click analyze
  3. Then File analyze

Now you should be looking at a window if the different files.



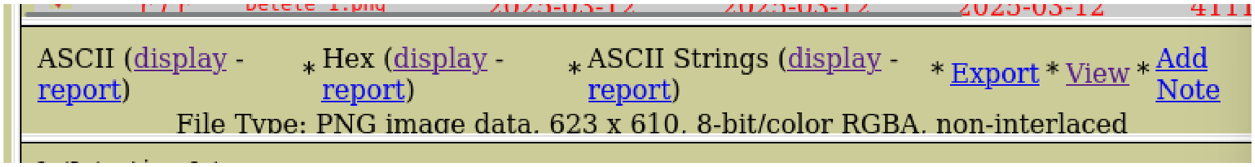
Current Directory: C:/

Del	Type dir / in	Name	Written	Accessed	Created	Size

Error Parsing File (Invalid Characters?):
V/V 62251062: $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

Del	Type dir / in	Name	Written	Accessed	Created	Size
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	1218
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	1218
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512
✓	r / r	Cookie.jpg	2025-03-01 14:57:08 (EST)	2025-03-12 00:00:00 (EDT)	2025-03-01 14:57:22 (EST)	6530
✓	r / r	Detective Cat.png	2025-03-12 23:05:46 (EDT)	2025-03-12 00:00:00 (EDT)	2025-03-12 23:05:44 (EDT)	0
	r / r	Detective Cat.png	2025-03-12 23:05:46 (EDT)	2025-03-13 00:00:00 (EDT)	2025-03-12 23:05:44 (EDT)	5862
✓	r / r	Detete 1.png	2025-03-12 23:06:34 (EDT)	2025-03-12 00:00:00 (EDT)	2025-03-12 23:06:32 (EDT)	0
✓	r / r	Detete 1.png	2025-03-12 23:06:34 (EDT)	2025-03-12 00:00:00 (EDT)	2025-03-12 23:06:32 (EDT)	4111
✓	r / r	digital abyss.txt	2025-03-01 14:56:18 (EST)	2025-03-12 00:00:00 (EDT)	2025-03-01 14:47:50 (EST)	575
✓	r / r	Lego or Cat in my	2025-03-12	2025-03-12	2025-03-12	0

4. Browse through the files listed in the image. Look for r/r file types with non-zero file sizes.
5. Click on the first blue file name this should be Detective cat.png
6. The there will be a few options on how to view this file



r / r Detete 1.png 2025-03-12 2025-03-12 2025-03-12 4111

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note

File Type: PNG image data, 623 x 610, 8-bit/color RGBA, non-interlaced

- ASCII or Hex: Displays the raw file data.
- ASCII Strings: Extracts readable text from the file.
- View: Displays the file as it appears (e.g., images, documents).

7. Click on Add Note this will bring you to a new tab, where you can add a note about this file. Which can be view later. To get back to the Demo image click back to the previous tab.

8. Click on digital abyss.txt. The file contents will appear, allowing you to review the deleted data. As this file was deleted off the USB but was still in the USB memory and so was captured by the the image.
9. Now click view notes. This will bring you to a page with all the notes on this cast. You will be able to see the file, the meta tag number for the file, and the data the note was made.
10. Now click close this will bring you back to the case home page.
11. If you want to export a file form the Demo USB to do stuff with the click the Export and that will down load that file to your drive. To see the exported file will can be found in the downloads.