OPCIÓN 1: Instalar Autopsy en Ubuntu o Debian (recomendado)

🔧 **Requisitos previos**

Instalar Java, SleuthKit y dependencias necesarias:

```
sudo apt update

sudo apt install sleuthkit openjdk-11-jdk unzip wget -y
```

📥 1. Descargar Autopsy

```
cd /opt

sudo wget https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.21.0/
autopsy-4.21.0.zip

sudo unzip autopsy-4.21.0.zip

sudo chmod -R +x autopsy-4.21.0
```

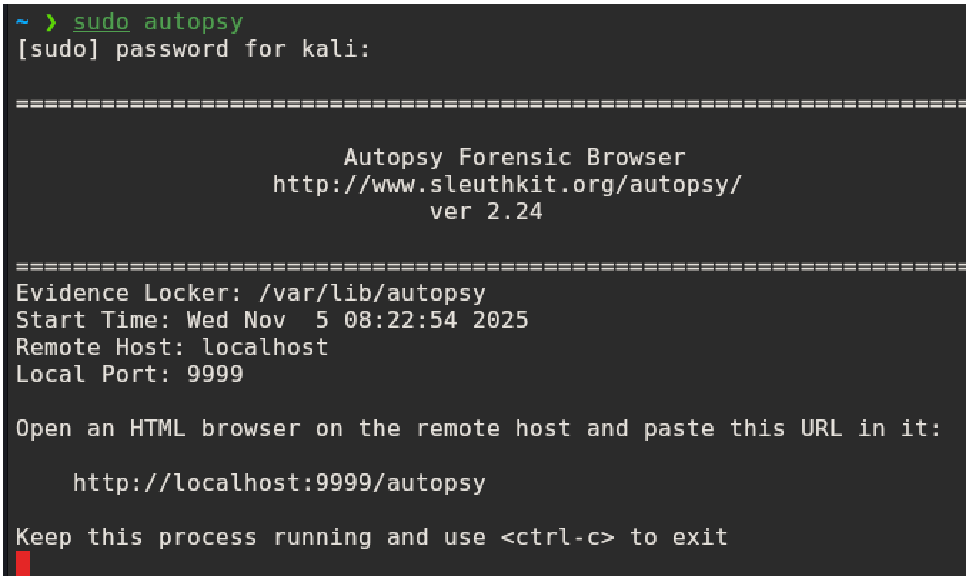
📌 Puedes consultar la última versión en GitHub

▶️ 2. Ejecutar Autopsy

```
cd /opt/autopsy-4.21.0/bin

./autopsy
```

🔗 Se abrirá un servidor local y te mostrará una URL como:

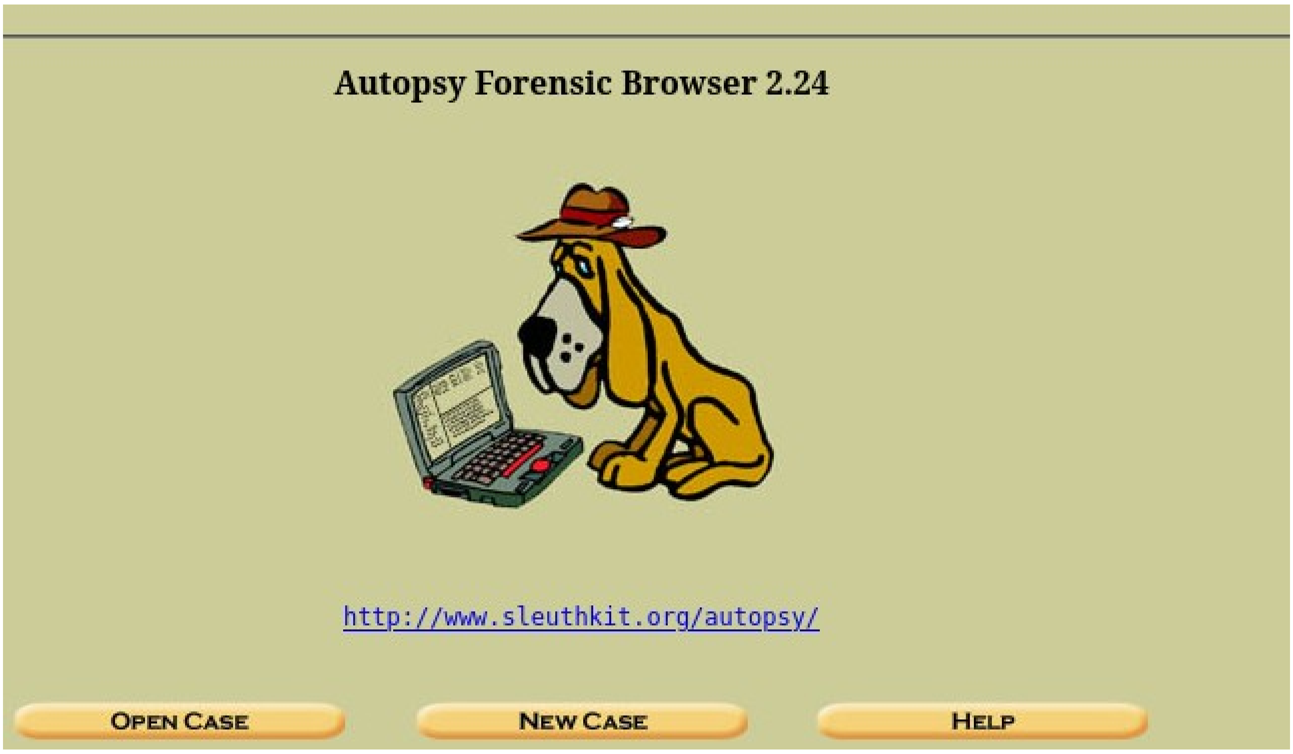
Starting Autopsy...



```
~ ❯ sudo autopsy
[sudo] password for kali:

==================================================================

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

==================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Wed Nov  5 08:22:54 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
```

Open your browser to http://localhost:9999/autopsy

📎 Abre esa URL en tu navegador y ¡listo!



Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

🖥️ ¿Quieres un acceso directo en el escritorio?

Crea un lanzador .desktop:

```
nano ~/.local/share/applications/autopsy.desktop
```

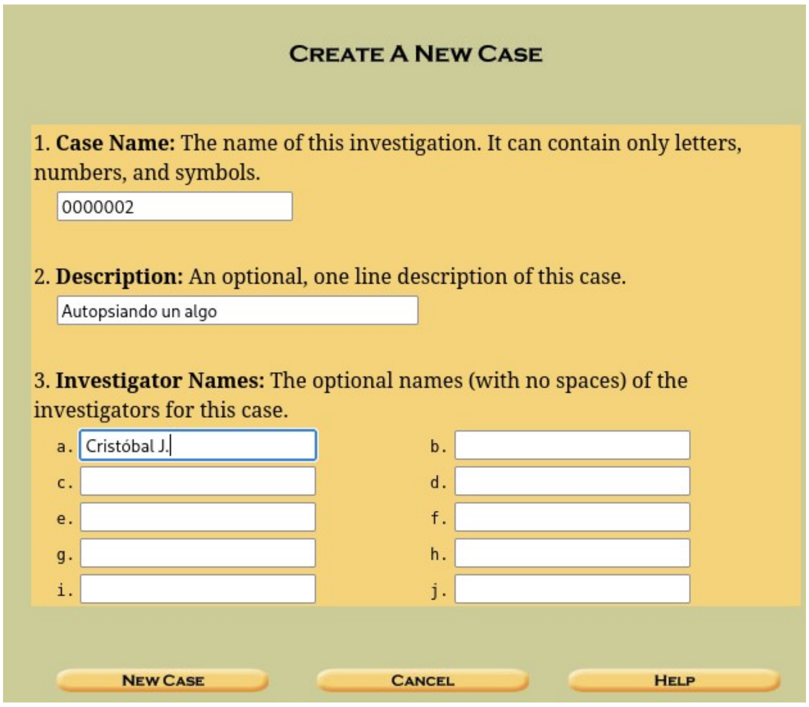
Y pega:

```
[Desktop Entry]

Name=Autopsy

Exec=/opt/autopsy-4.21.0/bin/autopsy

Icon=utilities-terminal

Terminal=true

Type=Application

Categories=Utility;

Guarda con CTRL+O y sal con CTRL+X.
```

✅ OPCIÓN 2 (alternativa): Ejecutar con Docker

Si no quieres instalar nada en el sistema:

```
docker pull rmoriz/autopsy

docker run -it -p 9999:9999 rmoriz/autopsy

Luego abre en navegador: http://localhost:9999/autopsy
```



CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

0000002

2. **Description:** An optional, one line description of this case.

Autopsiando un algo

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Cristóbal J.

b.

c.

d.

e.

f.

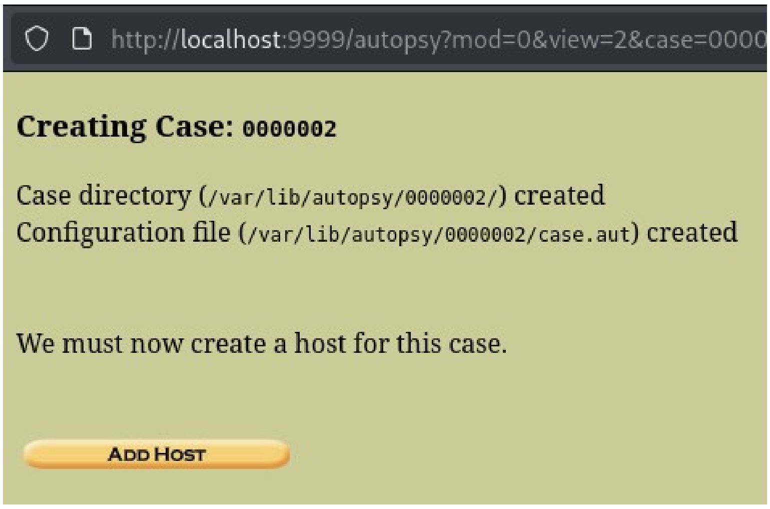
g.

h.

i.

j.

UNA VEZ CREADO EL CASO



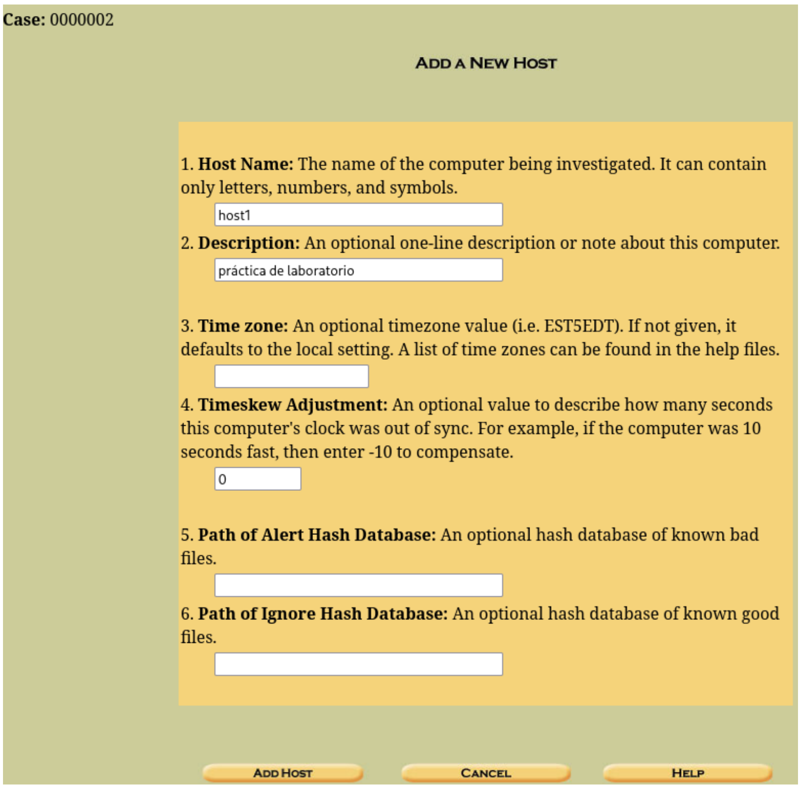
http://localhost:9999/autopsy?mod=0&view=2&case=0000

Creating Case: 0000002

Case directory (/var/lib/autopsy/0000002/) created
Configuration file (/var/lib/autopsy/0000002/case.aut) created

We must now create a host for this case.

EL SIGUIENTE PASO



Case: 0000002

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.
práctica de laboratorio

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.

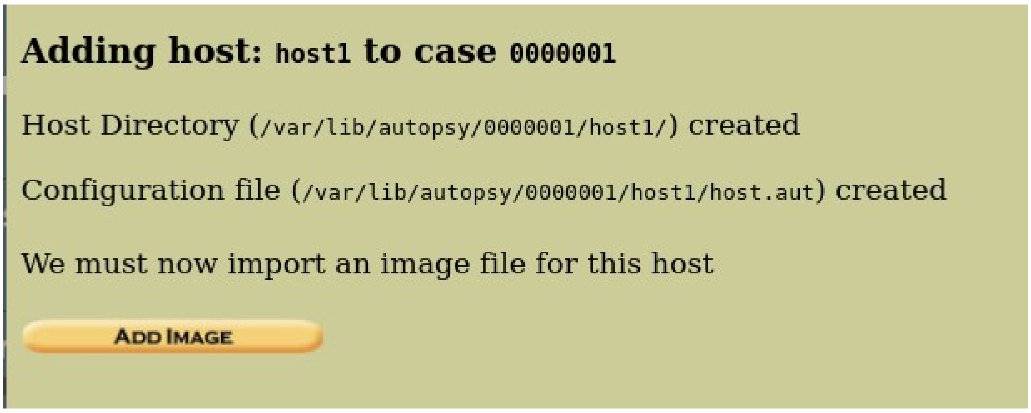
6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Rellenamos con estos datos

Relleno rápido recomendado (para empezar ya)

- **Host Name:** host1
- **Description:** práctica de laboratorio
- **Time zone:** *(vacío)* o UTC
- **Timeskew:** 0
- **Alert Hash DB:** *(vacío)*
- **Ignore Hash DB:** *(vacío)*

Luego **Create Host** → y en el siguiente paso añades la **imagen forense** (Add Image), eliges el **tipo** (raw/dd/E01), marcas **verify** si quieres, y continúas con el análisis (File Analysis, Keyword Search, Timeline, etc.). Ahora añadimos una imagen



Adding host: host1 to case 0000001

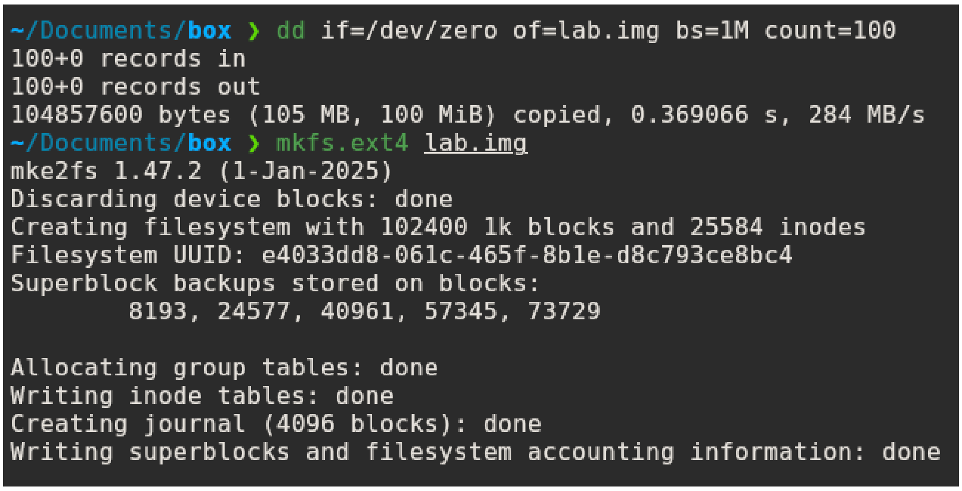
Host Directory (/var/lib/autopsy/0000001/host1/) created

Configuration file (/var/lib/autopsy/0000001/host1/host.aut) created

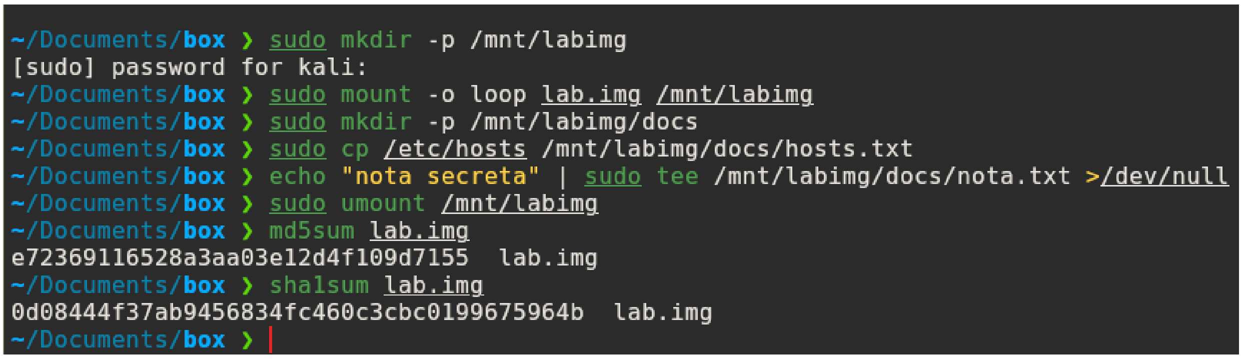
We must now import an image file for this host

Puedes descargar imágenes de disco o crear una, por ejemplo:

```
# 1) Crear un "disco" vacío de 100 MB

dd if=/dev/zero of=lab.img bs=1M count=100

# 2) Formatearlo (ext4; vale cualquier FS que quieras probar)

mkfs.ext4 lab.img

# 3) Montarlo en loop y meter "evidencias"

sudo mkdir -p /mnt/labimg

sudo mount -o loop lab.img /mnt/labimg

sudo mkdir -p /mnt/labimg/docs

sudo cp /etc/hosts /mnt/labimg/docs/hosts.txt

echo "nota secreta" | sudo tee /mnt/labimg/docs/nota.txt >/dev/null

# 4) Desmontar

sudo umount /mnt/labimg

# (Opcional) Calcular hashes para la cadena de custodia

md5sum lab.img

sha1sum lab.img
```



```
~/Documents/box ❯ dd if=/dev/zero of=lab.img bs=1M count=100
100+0 records in
100+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 0.369066 s, 284 MB/s
~/Documents/box ❯ mkfs.ext4 lab.img
mke2fs 1.47.2 (1-Jan-2025)
Discarding device blocks: done
Creating filesystem with 102400 1k blocks and 25584 inodes
Filesystem UUID: e4033dd8-061c-465f-8b1e-d8c793ce8bc4
Superblock backups stored on blocks:
        8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
```



```
~/Documents/box ❯ sudo mkdir -p /mnt/labimg
[sudo] password for kali:
~/Documents/box ❯ sudo mount -o loop lab.img /mnt/labimg
~/Documents/box ❯ sudo mkdir -p /mnt/labimg/docs
~/Documents/box ❯ sudo cp /etc/hosts /mnt/labimg/docs/hosts.txt
~/Documents/box ❯ echo "nota secreta" | sudo tee /mnt/labimg/docs/nota.txt >/dev/null
~/Documents/box ❯ sudo umount /mnt/labimg
~/Documents/box ❯ md5sum lab.img
e72369116528a3aa03e12d4f109d7155  lab.img
~/Documents/box ❯ sha1sum lab.img
0d08444f37ab9456834fc460c3cbc0199675964b  lab.img
~/Documents/box ❯
```

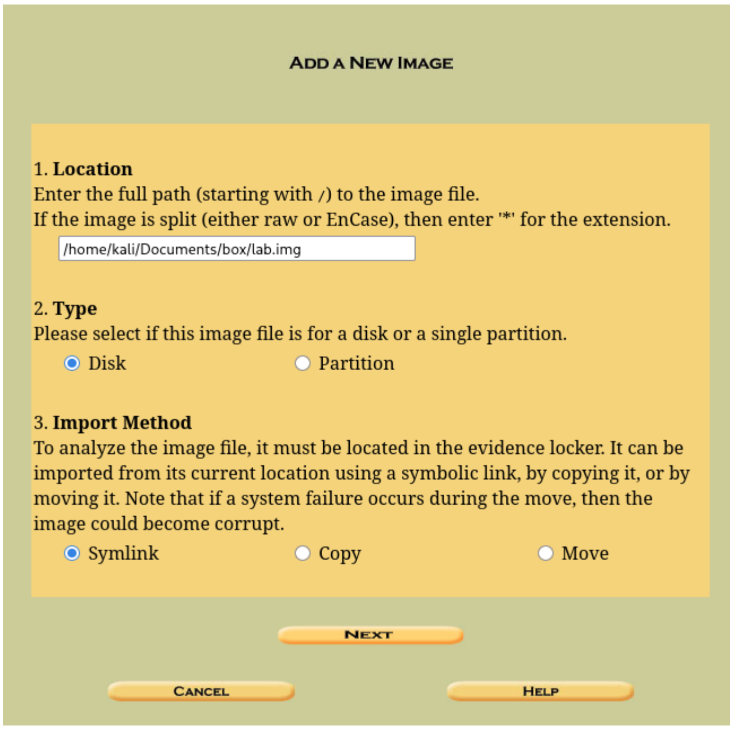
y ahora

□ Haz clic en el botón **“Add Image File”**
(justo en el centro de la pantalla que muestras).

□ En la nueva ventana que aparece:

- **Image Type:** selecciona
  👉 Single, raw (dd)
  (porque creaste una imagen con dd, que es formato raw)
- **Image File Path:**
  pulsa el botón **Browse** y selecciona tu archivo lab.img.
  📁 Si lo hiciste en tu carpeta personal, estará en:
- /home/tu_usuario/lab.img

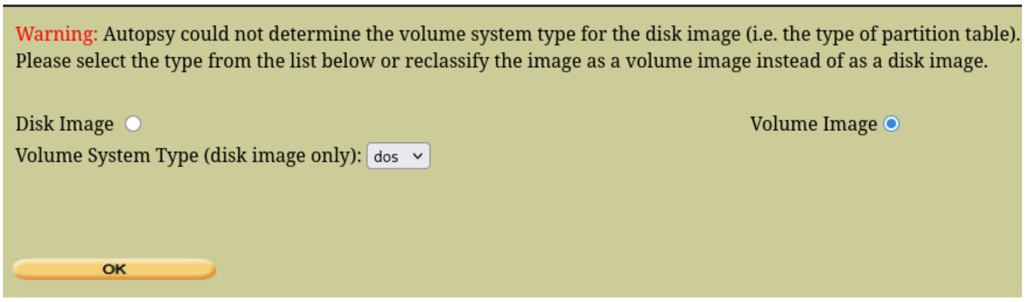
(ajusta el nombre del usuario según corresponda).



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/Documents/box/lab.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



Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table).
Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image ○ Volume Image ●
Volume System Type (disk image only): dos

Pulsamos en volumen image

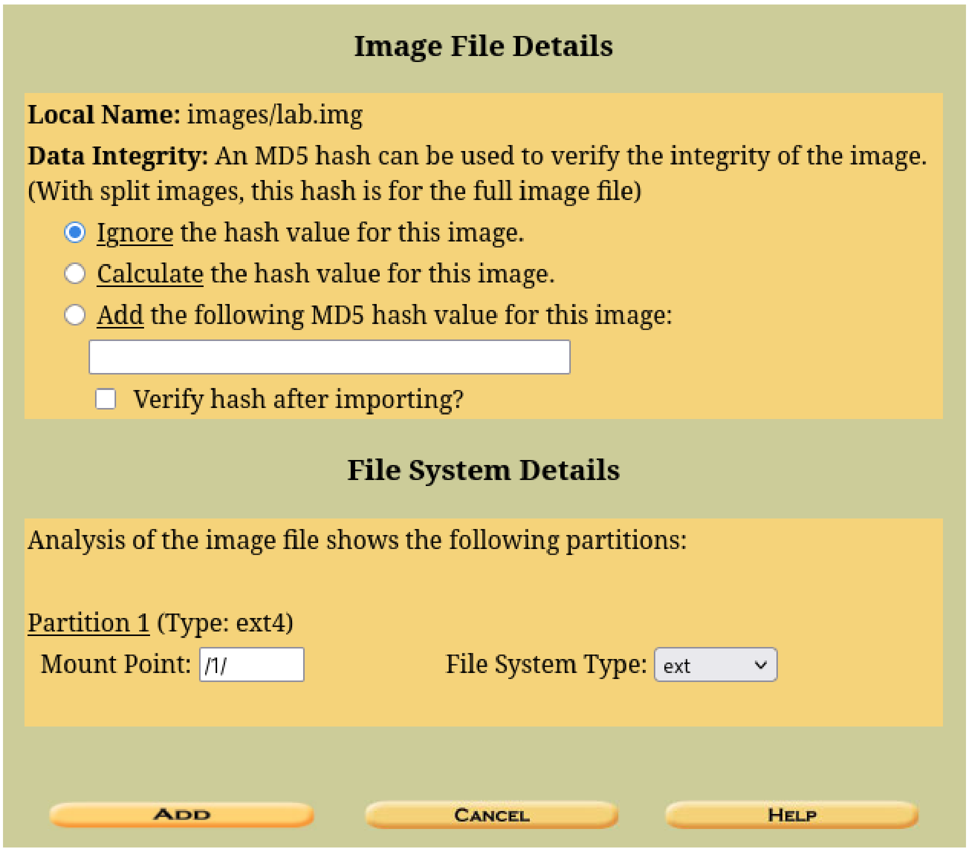


Image File Details

Local Name: images/lab.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:

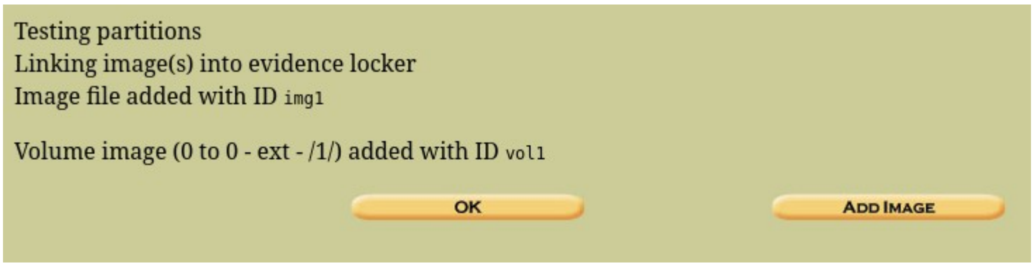
□ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ext4)

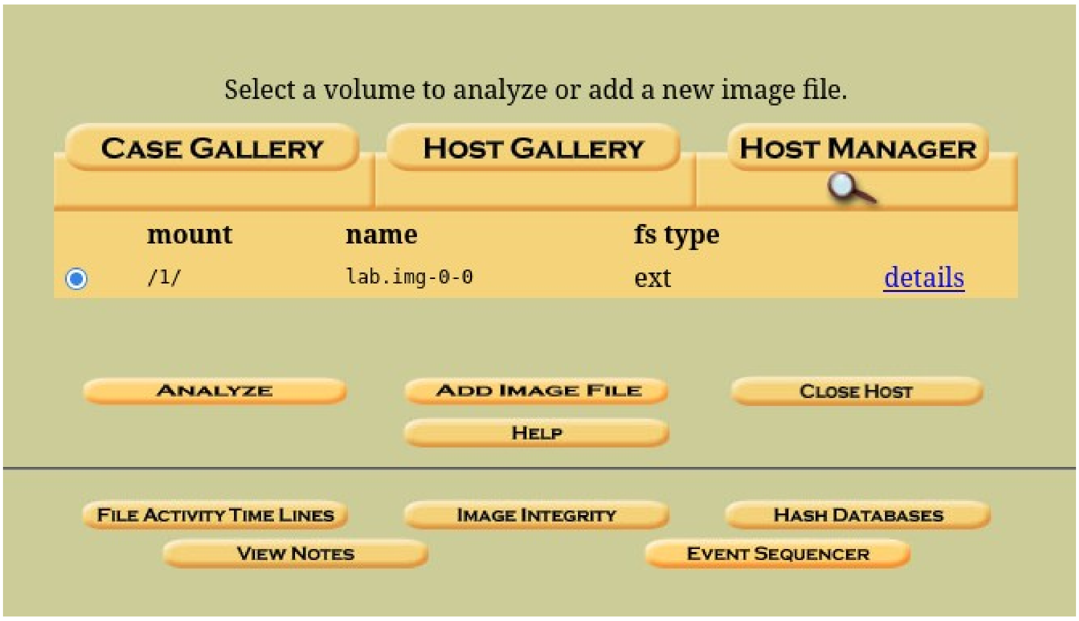
Mount Point: /1/ File System Type: ext



Testing partitions
Linking image(s) into evidence locker
Image file added with ID `img1`

Volume image (0 to 0 - ext - /1/) added with ID `vol1`

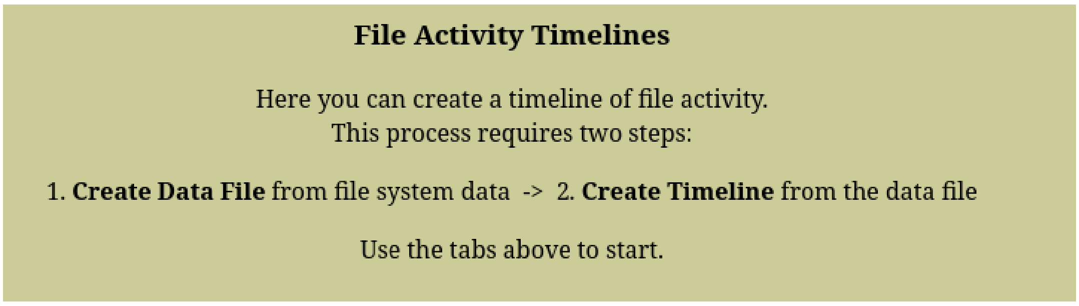
Pulsa en add



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

	mount	name	fs type	
●	`/1/`	`lab.img-0-0`	ext	details

Elegimos el tipo de análisis

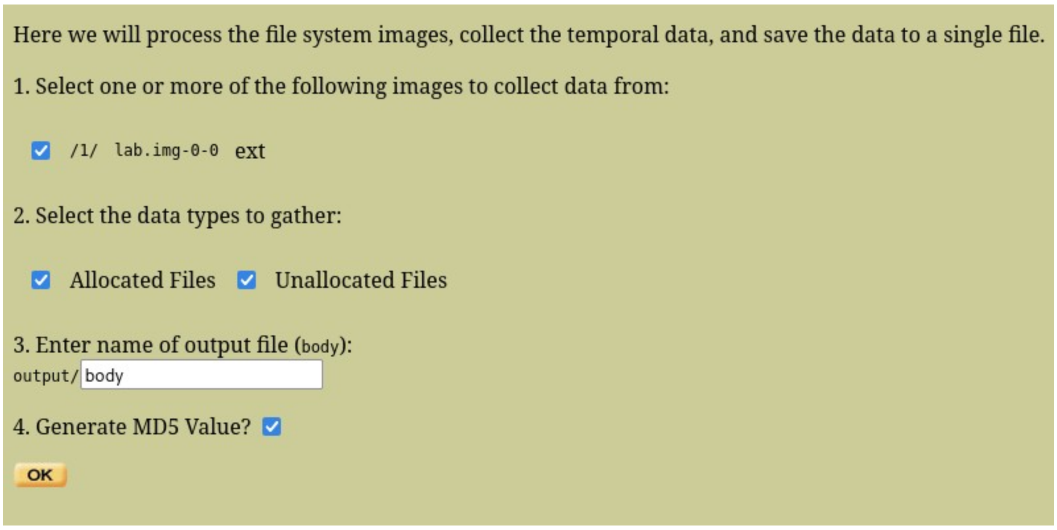


File Activity Timelines

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.



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:

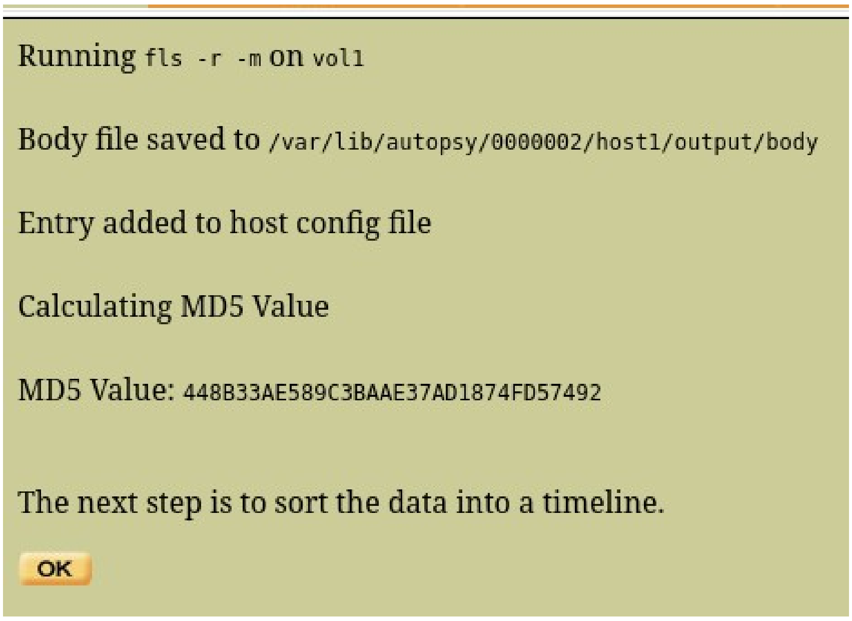
☑ `/1/ lab.img-0-0` ext

2. Select the data types to gather:

☑ Allocated Files ☑ Unallocated Files

3. Enter name of output file (`body`):
`output/` body

4. Generate MD5 Value? ☑



Running `fls -r -m` on `vol1`

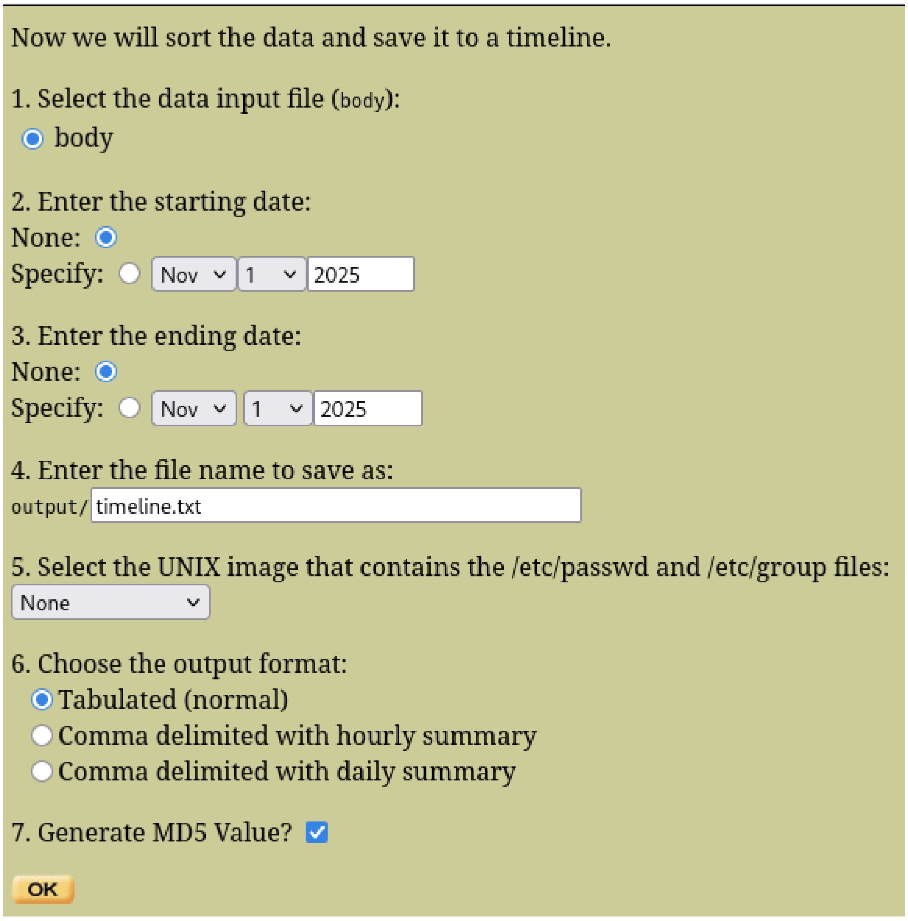
Body file saved to `/var/lib/autopsy/0000002/host1/output/body`

Entry added to host config file

Calculating MD5 Value

MD5 Value: `448B33AE589C3BAAE37AD1874FD57492`

The next step is to sort the data into a timeline.



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: ○ Nov 1 2025

3. Enter the ending date:

None: ●

Specify: ○ Nov 1 2025

4. Enter the file name to save as:

`output/` timeline.txt

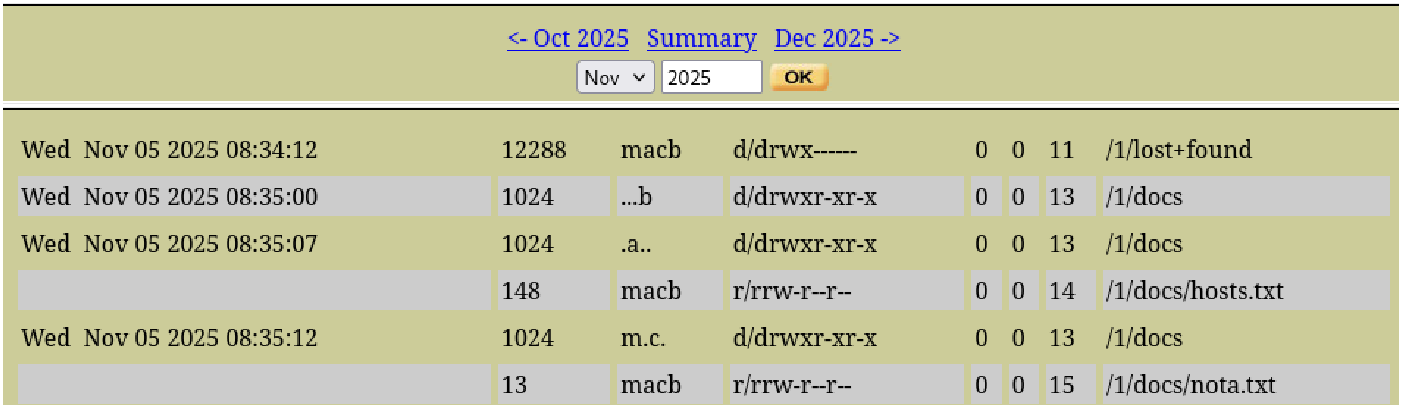
5. Select the UNIX image that contains the /etc/passwd and /etc/group files:

None

6. Choose the output format:

● Tabulated (normal)
○ Comma delimited with hourly summary
○ Comma delimited with daily summary

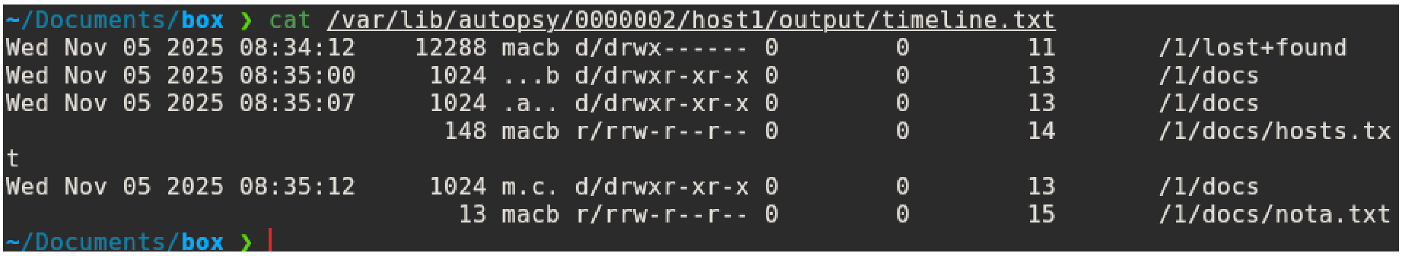
7. Generate MD5 Value? ☑



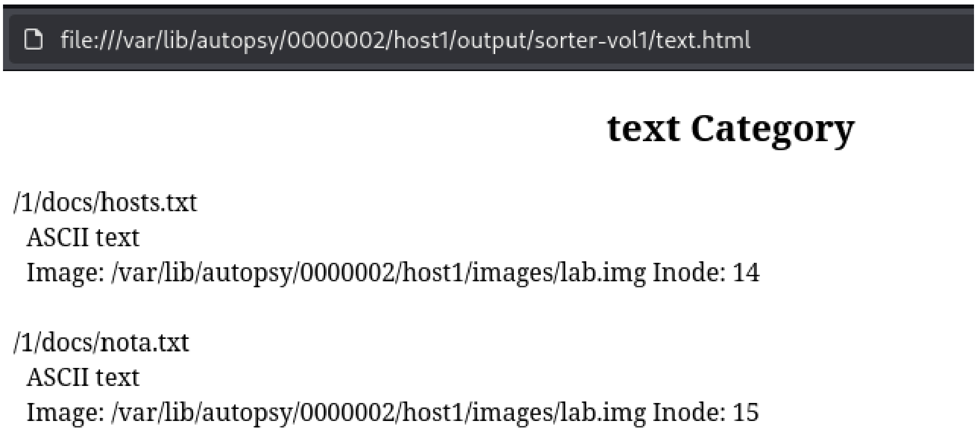
<- Oct 2025 Summary Dec 2025 ->

Nov 2025

Wed Nov 05 2025 08:34:12	12288	macb	d/drwx------	0	0	11	/1/lost+found
Wed Nov 05 2025 08:35:00	1024	...b	d/drwxr-xr-x	0	0	13	/1/docs
Wed Nov 05 2025 08:35:07	1024	.a..	d/drwxr-xr-x	0	0	13	/1/docs
	148	macb	r/rrw-r--r--	0	0	14	/1/docs/hosts.txt
Wed Nov 05 2025 08:35:12	1024	m.c.	d/drwxr-xr-x	0	0	13	/1/docs
	13	macb	r/rrw-r--r--	0	0	15	/1/docs/nota.txt



```
~/Documents/box ❯ cat /var/lib/autopsy/0000002/host1/output/timeline.txt
Wed Nov 05 2025 08:34:12    12288 macb d/drwx------ 0        0        11       /1/lost+found
Wed Nov 05 2025 08:35:00     1024 ...b d/drwxr-xr-x 0        0        13       /1/docs
Wed Nov 05 2025 08:35:07     1024 .a.. d/drwxr-xr-x 0        0        13       /1/docs
                              148 macb r/rrw-r--r-- 0        0        14       /1/docs/hosts.tx
t
Wed Nov 05 2025 08:35:12     1024 m.c. d/drwxr-xr-x 0        0        13       /1/docs
                               13 macb r/rrw-r--r-- 0        0        15       /1/docs/nota.txt
~/Documents/box ❯
```

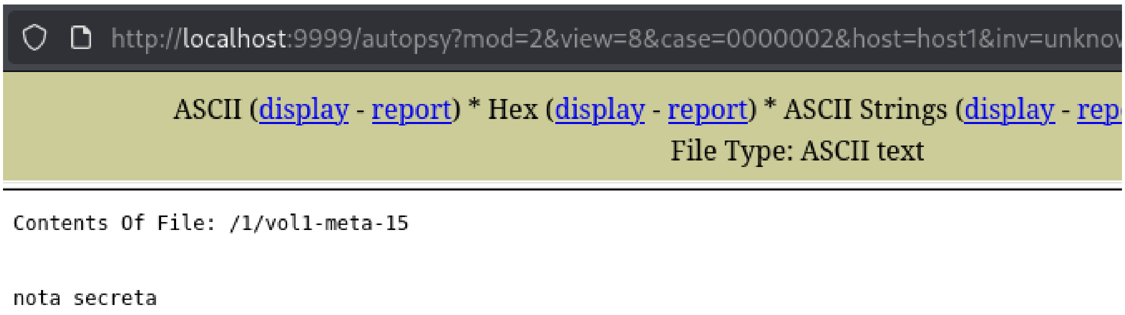


file:///var/lib/autopsy/0000002/host1/output/sorter-vol1/text.html

text Category

/1/docs/hosts.txt
ASCII text
Image: /var/lib/autopsy/0000002/host1/images/lab.img Inode: 14

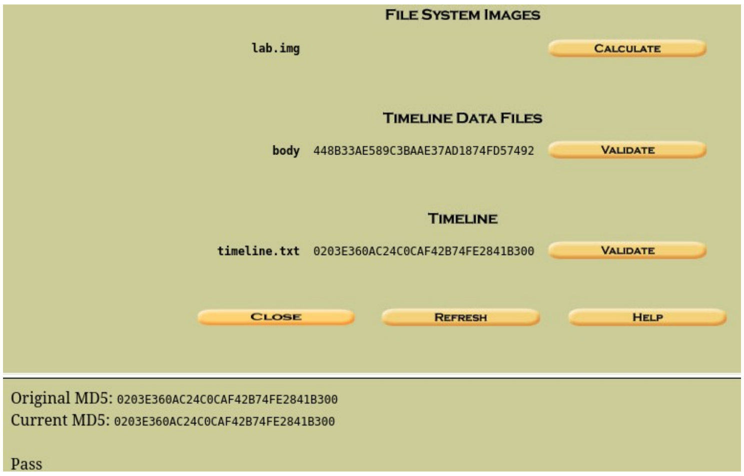
/1/docs/nota.txt
ASCII text
Image: /var/lib/autopsy/0000002/host1/images/lab.img Inode: 15



http://localhost:9999/autopsy?mod=2&view=8&case=0000002&host=host1&inv=unknov

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - rep
File Type: ASCII text

```
Contents Of File: /1/vol1-meta-15


nota secreta
```



File System Images

lab.img

Timeline Data Files

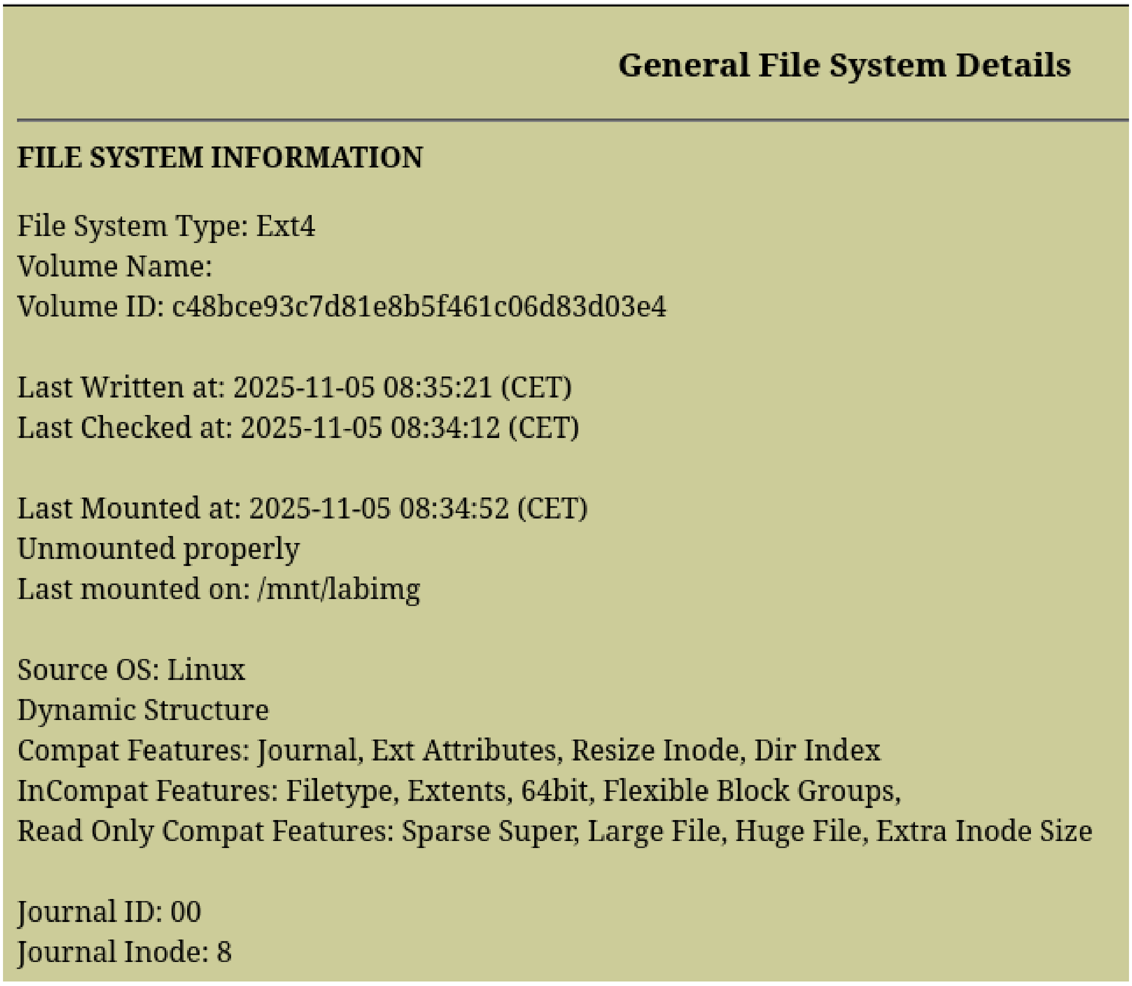
body 448B33AE589C3BAAE37AD1874FD57492

Timeline

timeline.txt 0203E360AC24C0CAF42B74FE2841B300

Original MD5: 0203E360AC24C0CAF42B74FE2841B300
Current MD5: 0203E360AC24C0CAF42B74FE2841B300

Pass



General File System Details

FILE SYSTEM INFORMATION

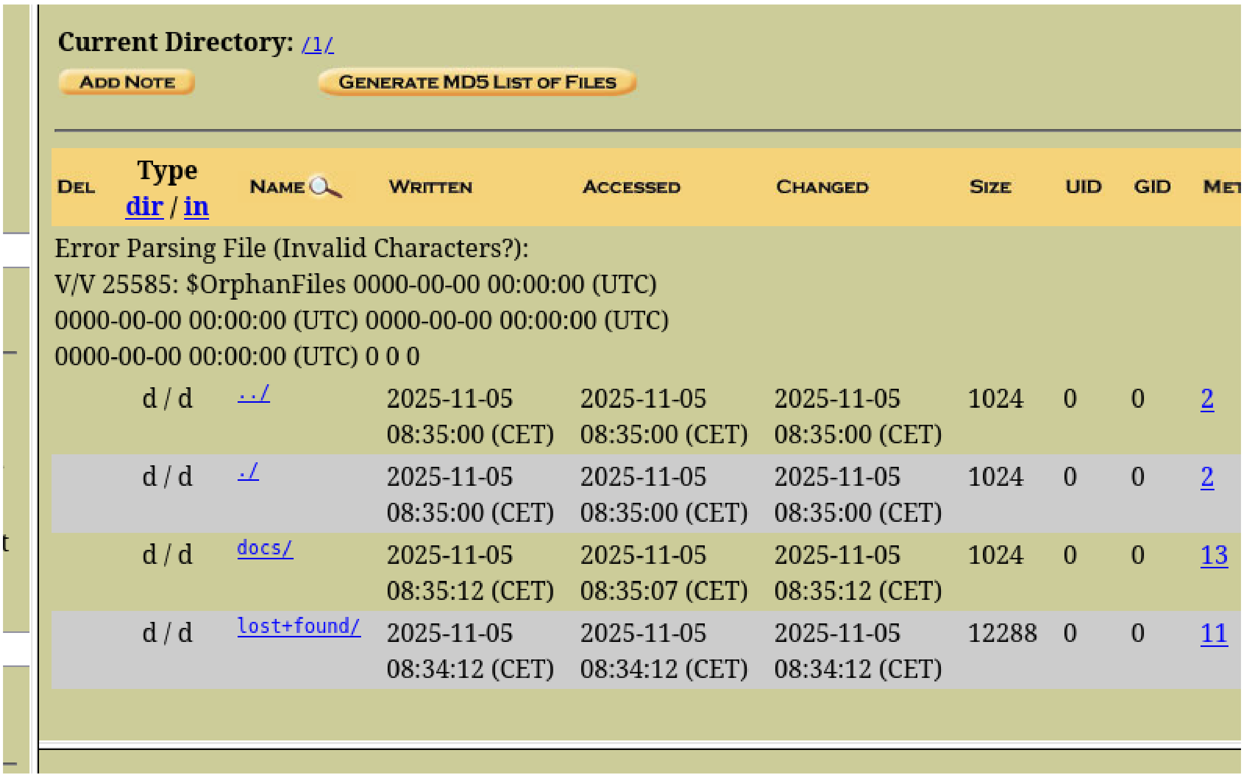
File System Type: Ext4
Volume Name:
Volume ID: c48bce93c7d81e8b5f461c06d83d03e4

Last Written at: 2025-11-05 08:35:21 (CET)
Last Checked at: 2025-11-05 08:34:12 (CET)

Last Mounted at: 2025-11-05 08:34:52 (CET)
Unmounted properly
Last mounted on: /mnt/labimg

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Extents, 64bit, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size

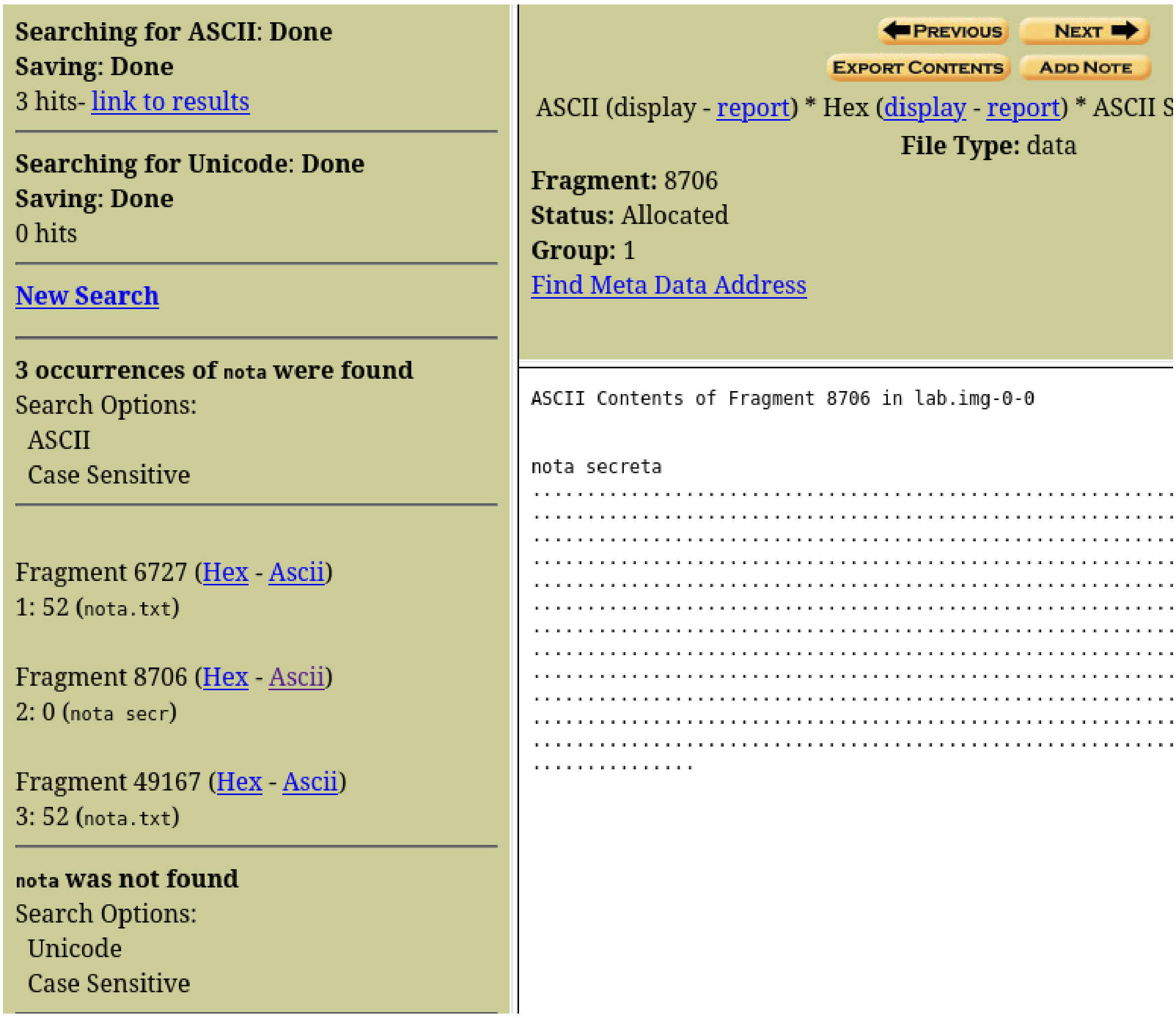
Journal ID: 00
Journal Inode: 8



Current Directory: /1/

Error Parsing File (Invalid Characters?):
V/V 25585: $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	Changed	Size	UID	GID	Met
	d / d	../	2025-11-05 08:35:00 (CET)	2025-11-05 08:35:00 (CET)	2025-11-05 08:35:00 (CET)	1024	0	0	2
	d / d	./	2025-11-05 08:35:00 (CET)	2025-11-05 08:35:00 (CET)	2025-11-05 08:35:00 (CET)	1024	0	0	2
	d / d	docs/	2025-11-05 08:35:12 (CET)	2025-11-05 08:35:07 (CET)	2025-11-05 08:35:12 (CET)	1024	0	0	13
	d / d	lost+found/	2025-11-05 08:34:12 (CET)	2025-11-05 08:34:12 (CET)	2025-11-05 08:34:12 (CET)	12288	0	0	11



Searching for ASCII: Done
Saving: Done
3 hits- link to results

Searching for Unicode: Done
Saving: Done
0 hits

New Search

3 occurrences of `nota` were found
Search Options:
ASCII
Case Sensitive

Fragment 6727 (Hex - Ascii)
1: 52 (`nota.txt`)

Fragment 8706 (Hex - Ascii)
2: 0 (`nota secr`)

Fragment 49167 (Hex - Ascii)
3: 52 (`nota.txt`)

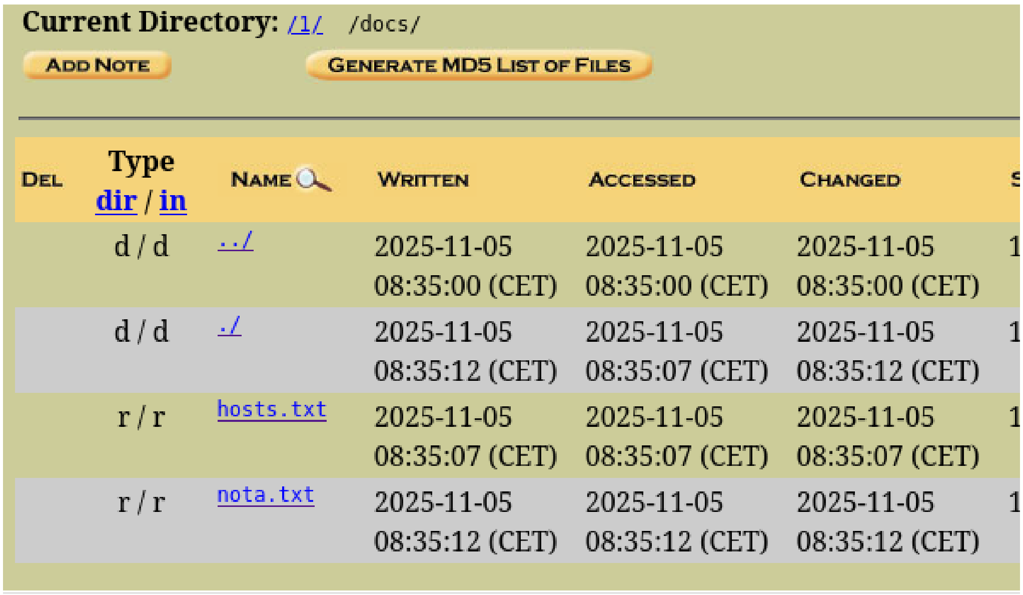
`nota` was not found
Search Options:
Unicode
Case Sensitive

ASCII (display - report) * Hex (display - report) * ASCII S

File Type: data

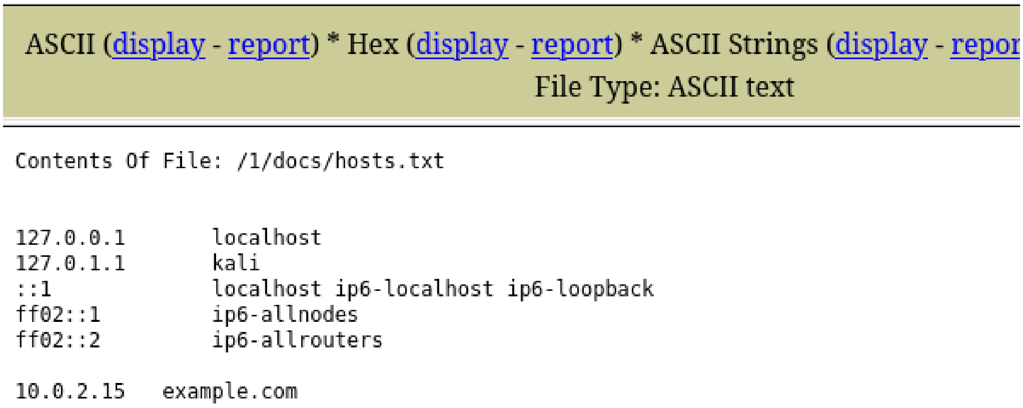
Fragment: 8706
Status: Allocated
Group: 1
Find Meta Data Address

```
ASCII Contents of Fragment 8706 in lab.img-0-0


nota secreta
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...............
```



Current Directory: /1/ `/docs/`

Del	Type dir / in	Name	Written	Accessed	Changed	S
	d / d	../	2025-11-05 08:35:00 (CET)	2025-11-05 08:35:00 (CET)	2025-11-05 08:35:00 (CET)	1
	d / d	./	2025-11-05 08:35:12 (CET)	2025-11-05 08:35:07 (CET)	2025-11-05 08:35:12 (CET)	1
	r / r	hosts.txt	2025-11-05 08:35:07 (CET)	2025-11-05 08:35:07 (CET)	2025-11-05 08:35:07 (CET)	1
	r / r	nota.txt	2025-11-05 08:35:12 (CET)	2025-11-05 08:35:12 (CET)	2025-11-05 08:35:12 (CET)	1



ASCII (display - report) * Hex (display - report) * ASCII Strings (display - repor

File Type: ASCII text

```
Contents Of File: /1/docs/hosts.txt


127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.15    example.com
```

SOLUCIONES SI DA PROBLEMAS EL LOG

1) Diagnóstico rápido (ejecuta en la misma terminal donde lanzaste Autopsy)

```
# ¿Dónde estás ejecutando Autopsy?

pwd

# ¿qué usuario eres?

whoami

# listar permisos del directorio donde está el binario/los scripts

ls -ld /usr/share/autopsy

ls -l /usr/share/autopsy/autopsy.log 2>/dev/null

# comprobar permisos del Evidence Locker (ya lo muestra el arranque)

ls -ld /var/lib/autopsy
```

Si ls -l /usr/share/autopsy/autopsy.log muestra “No such file or directory” o el directorio /usr/share/autopsy no es escribible por tu usuario, ahí está el problema.

---

2) Solución 1 — Crear el fichero de log y dar permisos (rápido y seguro)

Si quieres que el log exista en /usr/share/autopsy (donde parece buscarlo):

```
sudo touch /usr/share/autopsy/autopsy.log

sudo chown $(whoami):$(whoami) /usr/share/autopsy/autopsy.log

sudo chmod 644 /usr/share/autopsy/autopsy.log
```

Después reinicia Autopsy (o vuelve a lanzar el comando que usaste). Si el proceso corre como root, podrías en su lugar asignarlo al usuario que ejecute Autopsy.

---

3) Solución 2 — Ejecutar Autopsy con privilegios (si estás en entorno de pruebas)

Si no te importa ejecutar como root (solo en laboratorio):

```
sudo autopsy

# o si lo lanzaste con java:

sudo java -jar /usr/share/autopsy/bin/autopsy.jar
```