

LABORATORIO 08

JESUS ORULA BARCOS PADILLA

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E
INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

LABORATORIO 08

JESUS ORULA BARCOS PADILLA

INFORME DE EXPLOTACIÓN

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E
INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES	4
ABRIR LINUX.	5
COPIA E IMAGEN DE MEMORIA USB.	5
ABRIR LINUX.	10

TABLA DE ILUSTRACIONES

Ilustración 1 Linux.	5
Ilustración 2 Sha1sum.	5
Ilustración 3 Imagen dd.	6
Ilustración 4 Finalización.	6
Ilustración 5 Autopsy.	7
Ilustración 6 Crear caso en Linux.	7
Ilustración 7 Caso creado con éxito.	7
Ilustración 8 Crear host.	8
Ilustración 9 Seleccionar imagen forense.	8
Ilustración 10 Detalles de la imagen.	8
Ilustración 11 Archivos.	9
Ilustración 12 Información general del sistema de archivos.	9
Ilustración 13 Cifrado md5.	9
Ilustración 14 Descargar autopsy.	10
Ilustración 15 Crear caso.	10
Ilustración 16 Caso creado.	11
Ilustración 17 Archivos de la imagen.	11

ABRIR LINUX.

Iniciar la máquina virtual de Linux.

Ilustración 1 Linux.



COPIA E IMAGEN DE MEMORIA USB.

Para compartir hacer una copia e imagen de una memoria se debe hacer el siguiente procedimiento. Ingresar el comando `sha1sum /dev/sdb > /home/orulaparr/Escritorio/hash_forense.sha1`

Ilustración 2 Sha1sum.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda

(root@orulaparr)-[/home/orulaparr]
# fdisk -l
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x850425ea

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 49641471 49639424 23,7G 83 Linux
/dev/sda2 49643518 52426751 2783234 1,3G f W95 Ext'd (LBA)
/dev/sda5 49643520 52426751 2783232 1,3G 82 Linux swap / Solaris

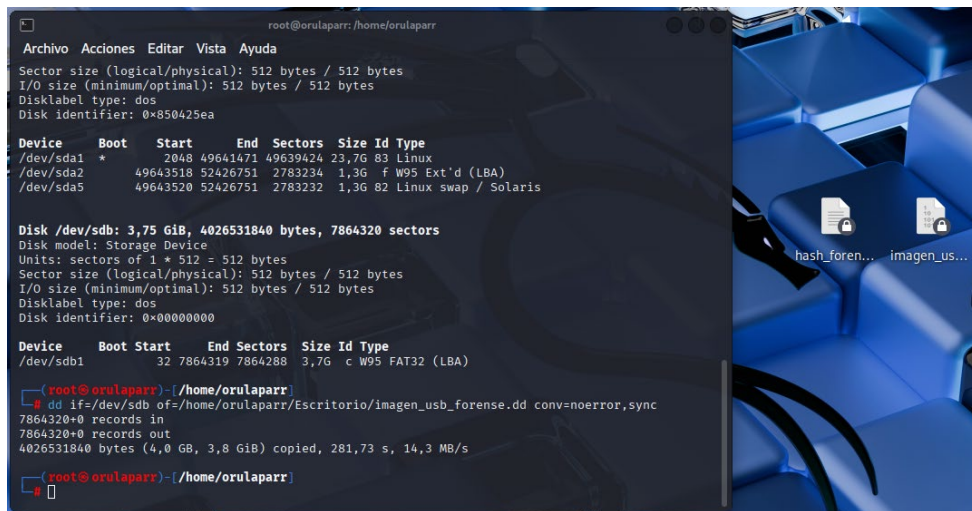
Disk /dev/sdb: 3,75 GiB, 4026531840 bytes, 7864320 sectors
Disk model: Storage Device
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device Boot Start End Sectors Size Id Type
/dev/sdb1 32 7864319 7864288 3,7G c W95 FAT32 (LBA)

(root@orulaparr)-[/home/orulaparr]
# sha1sum /dev/sdb1 > /home/orulaparr/Escritorio/hash_forense.sha1
```

Para hacer la imagen se debe utilizar el siguiente comando **dd if=/dev/sdb of=/home/orulaparr/Escritorio/imagen_usb_forense.dd conv=noerror,sync**

Ilustración 3 Imagen dd.



```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x850425ea

Device      Boot   Start    End  Sectors  Size Id Type
/dev/sda1   *         2048 49641471 49639424 23,7G 83 Linux
/dev/sda2         49643518 52426751 2783234   1,3G  f W95 Ext'd (LBA)
/dev/sda5         49643520 52426751 2783232   1,3G 82 Linux swap / Solaris

Disk /dev/sdb: 3,75 GiB, 4026531840 bytes, 7864320 sectors
Disk model: Storage Device
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

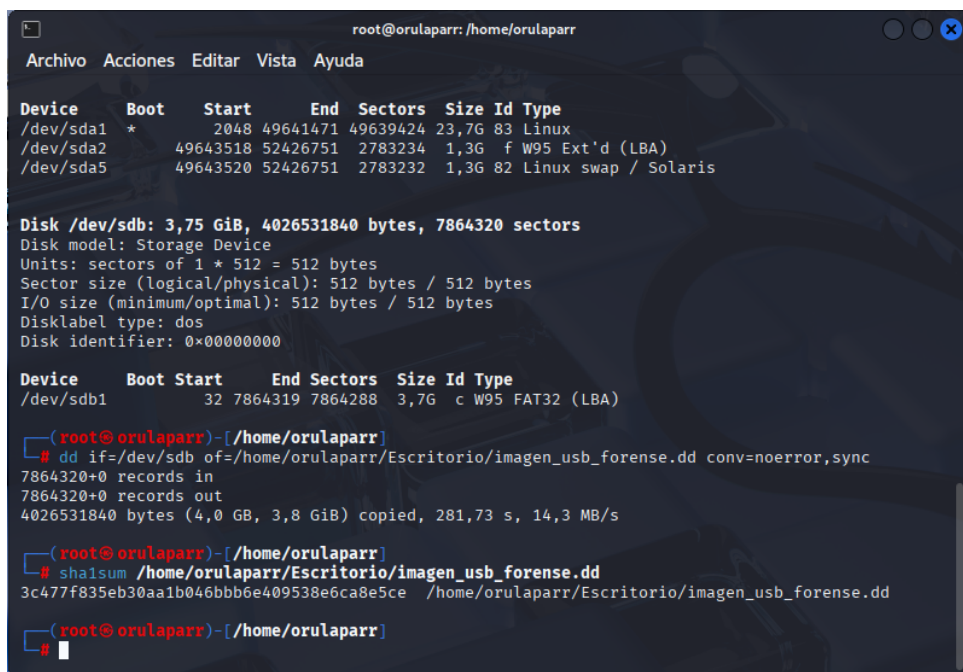
Device      Boot   Start    End  Sectors  Size Id Type
/dev/sdb1         32 7864319 7864288   3,7G  c W95 FAT32 (LBA)

(root@orulaparr)-[/home/orulaparr]
# dd if=/dev/sdb of=/home/orulaparr/Escritorio/imagen_usb_forense.dd conv=noerror,sync
7864320+0 records in
7864320+0 records out
4026531840 bytes (4,0 GB, 3,8 GiB) copied, 281,73 s, 14,3 MB/s

(root@orulaparr)-[/home/orulaparr]
#
```

Al terminar lo más recomendable es reiniciar el sistema para que los cambios se hagan efectivos.

Ilustración 4 Finalización.



```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda

Device      Boot   Start    End  Sectors  Size Id Type
/dev/sda1   *         2048 49641471 49639424 23,7G 83 Linux
/dev/sda2         49643518 52426751 2783234   1,3G  f W95 Ext'd (LBA)
/dev/sda5         49643520 52426751 2783232   1,3G 82 Linux swap / Solaris

Disk /dev/sdb: 3,75 GiB, 4026531840 bytes, 7864320 sectors
Disk model: Storage Device
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device      Boot   Start    End  Sectors  Size Id Type
/dev/sdb1         32 7864319 7864288   3,7G  c W95 FAT32 (LBA)

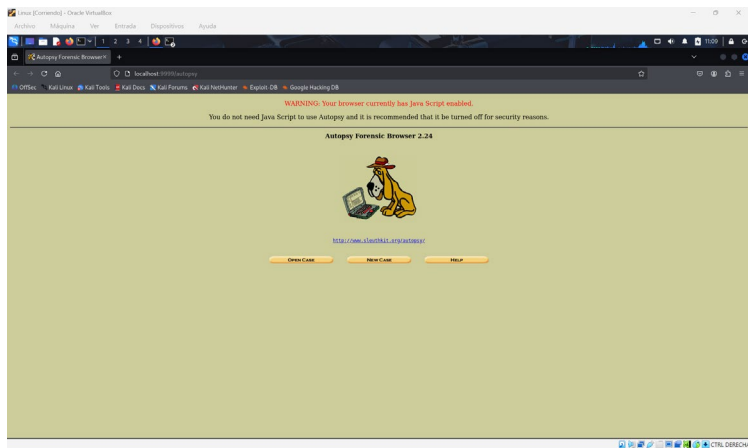
(root@orulaparr)-[/home/orulaparr]
# dd if=/dev/sdb of=/home/orulaparr/Escritorio/imagen_usb_forense.dd conv=noerror,sync
7864320+0 records in
7864320+0 records out
4026531840 bytes (4,0 GB, 3,8 GiB) copied, 281,73 s, 14,3 MB/s

(root@orulaparr)-[/home/orulaparr]
# sha1sum /home/orulaparr/Escritorio/imagen_usb_forense.dd
3c477f835eb30aa1b046bbb6e409538e6ca8e5ce /home/orulaparr/Escritorio/imagen_usb_forense.dd

(root@orulaparr)-[/home/orulaparr]
#
```

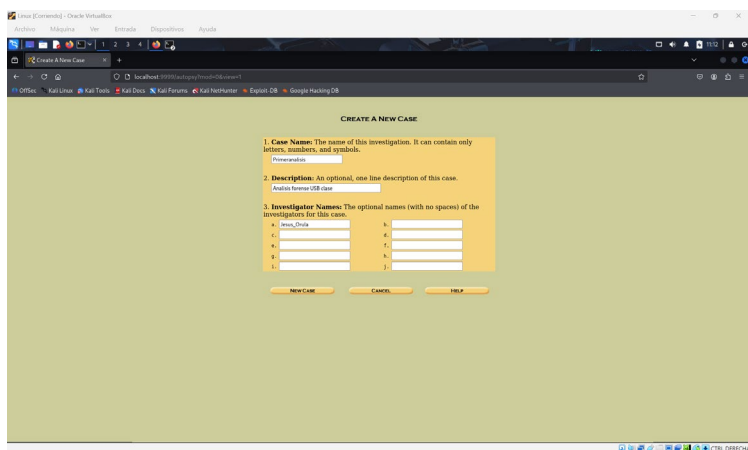
Abrir autopsy.

Ilustración 5 Autopsy.



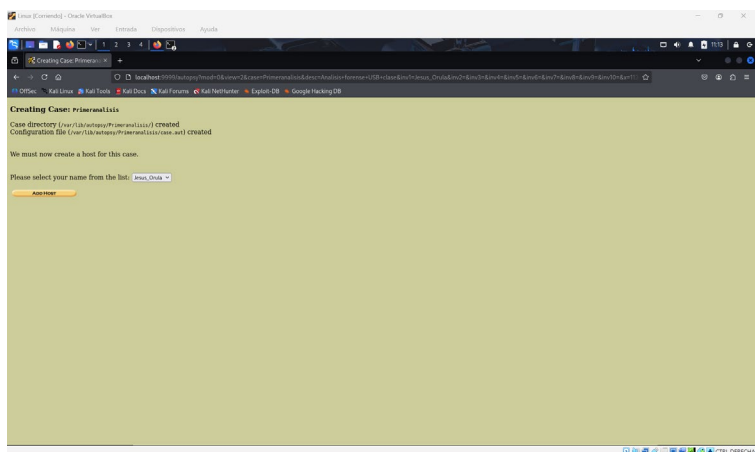
Crear caso, añadir una descripción y un nombre de investigador.

Ilustración 6 Crear caso en Linux.



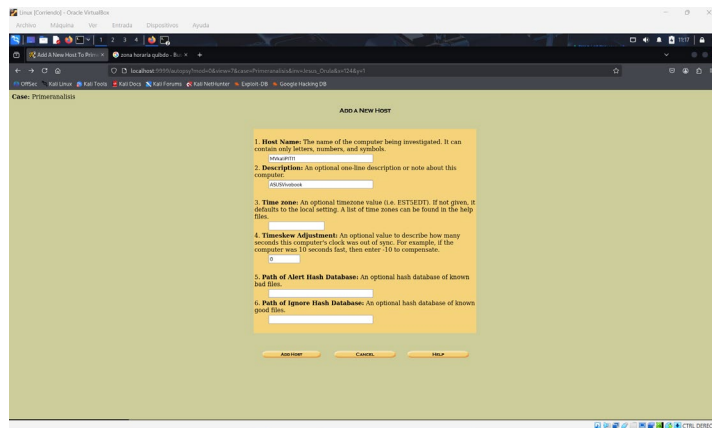
Caso creado con éxito.

Ilustración 7 Caso creado con éxito.



Crear un host y añadir una descripción.

Ilustración 8 Crear host.



Seleccionar la dirección de la ubicación de la imagen forense.

Ilustración 9 Seleccionar imagen forense.

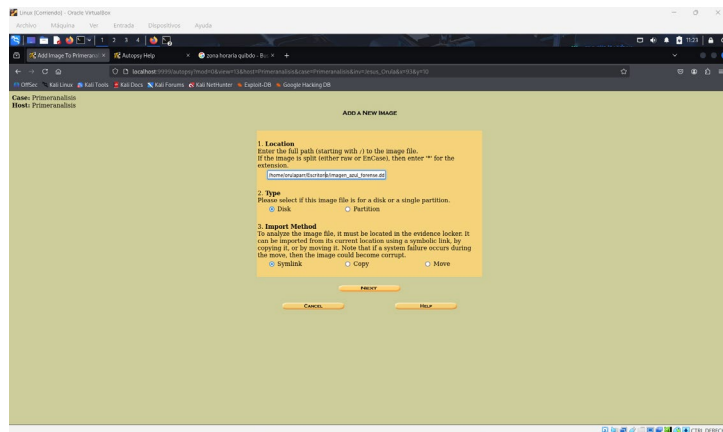


Ilustración 10 Detalles de la imagen.

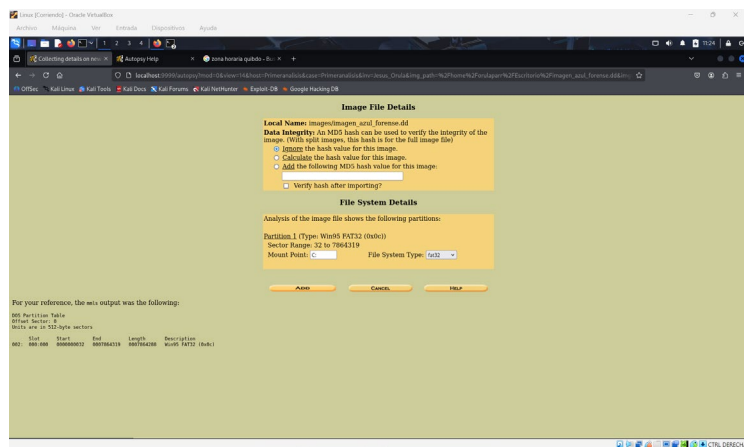


Ilustración 11 Archivos.

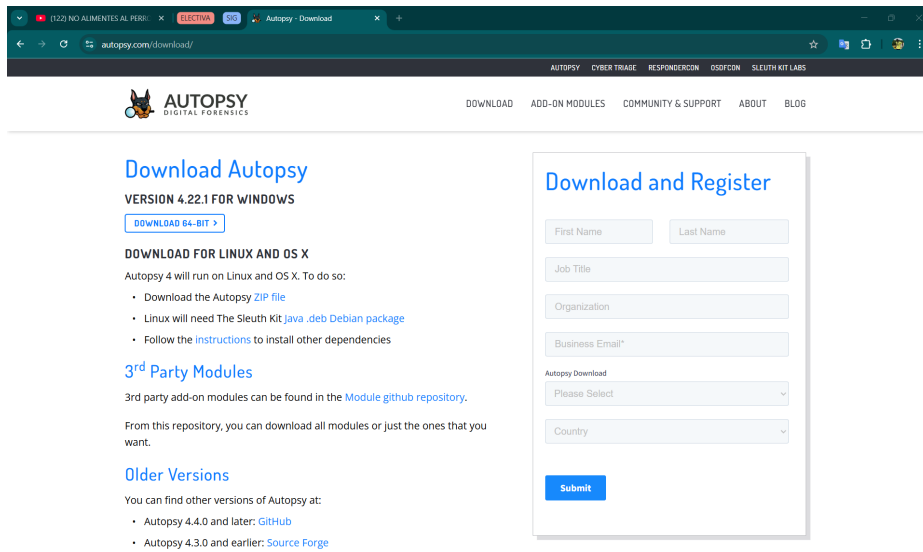
Ilustración 12 Información general del sistema de archivos.

Ilustración 13 Cifrado md5.

ABRIR LINUX.

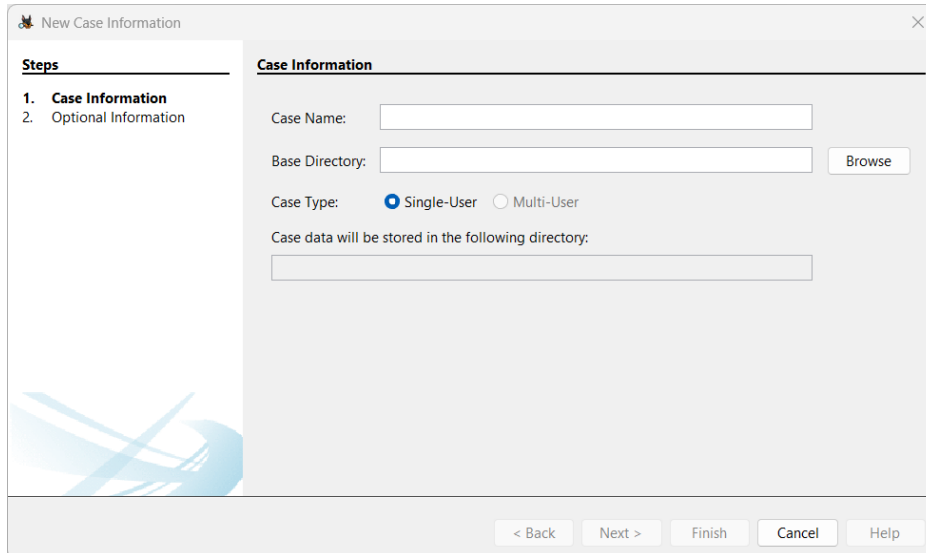
Descargar autopsy para windows desde su página principal.

Ilustración 14 Descargar autopsy.



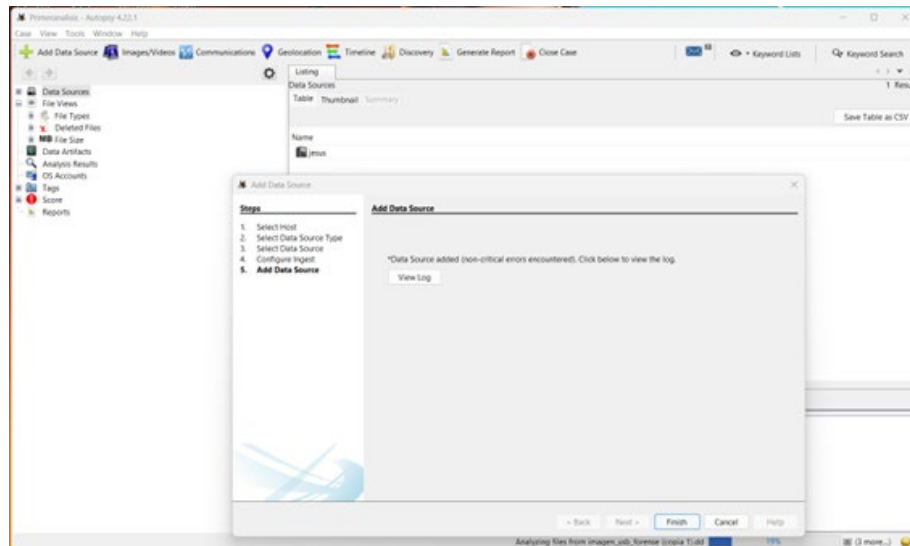
Luego de instalarlo, se procede a crear un caso.

Ilustración 15 Crear caso.



Como Autopsy es un programa para el análisis forense digital, no permite tomarle captura al paso a paso que hay que seguir para crear el caso. Pero una vez creado el caso, aparecerá así.

Ilustración 16 Caso creado.



Y aquí se puede ver los documentos de la imagen hecha en el Linux.

Ilustración 17 Archivos de la imagen.

