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.

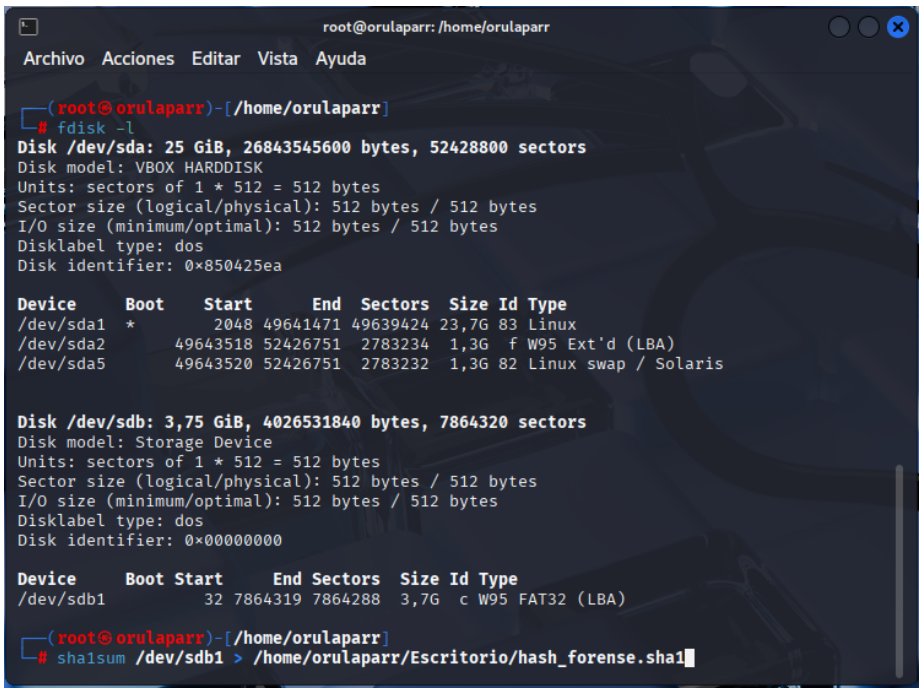
Iniciar la máquina virtual de Linux.

Ilustración 1 Linux.

COPIA E IMAGEN DE MEMORIA USB.

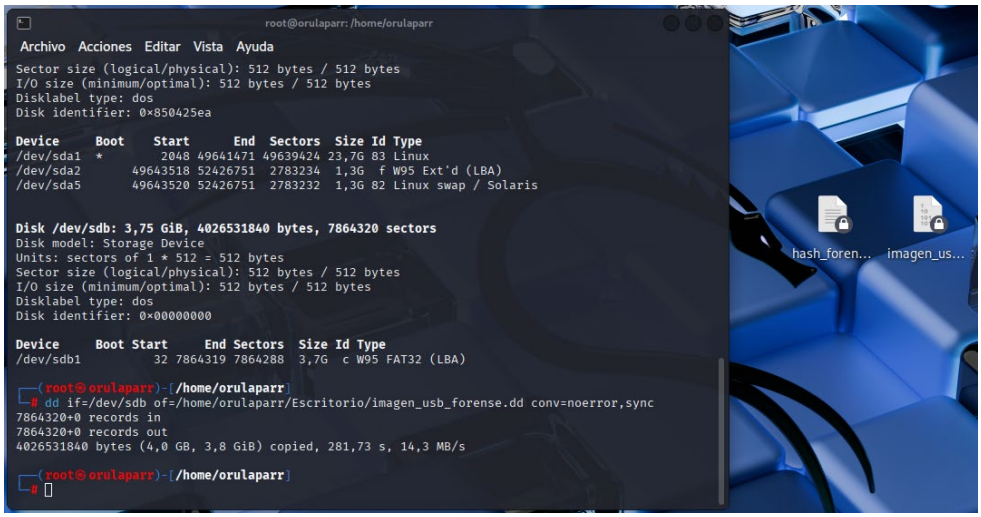
Para compartir hacer una copia e imagen de una memoria se debe hacer el siguiente procedimiento. Ingresar el comando `sha1sum /dev/sdb > /home/orulaparr/Escritorio/hash_forense.sha1`

Ilustración 2 Sha1sum.



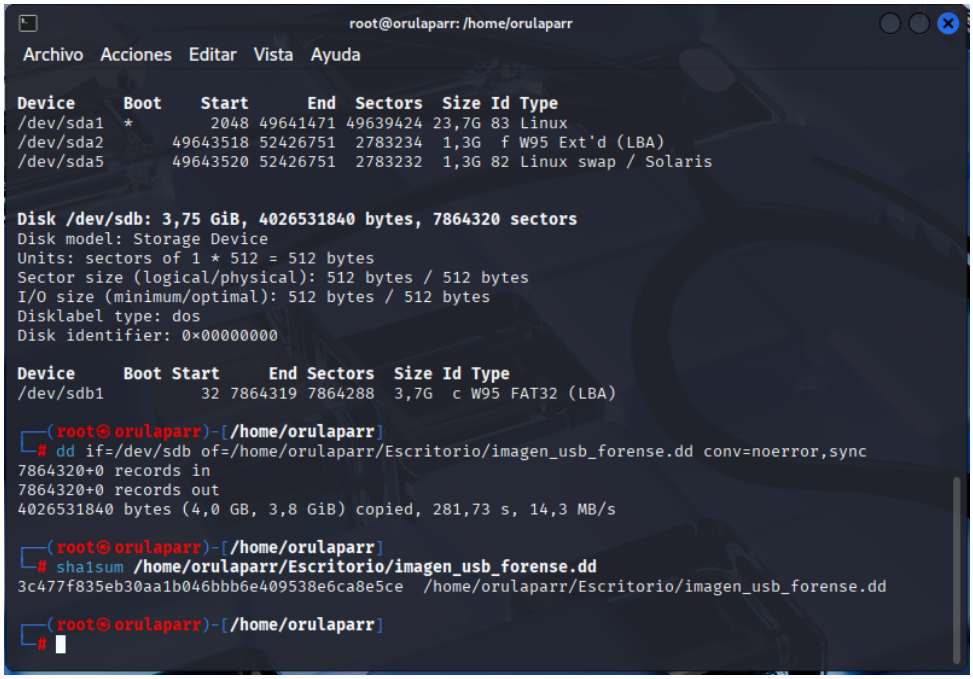
Para hacer la imagen se debe utilizar el siguiente comando **`dd if=/dev/sdb of=/home/orulaparr/Escritorio/imagen_usb_forense.dd conv=noerror,sync`**

Ilustración 3 Imagen dd.



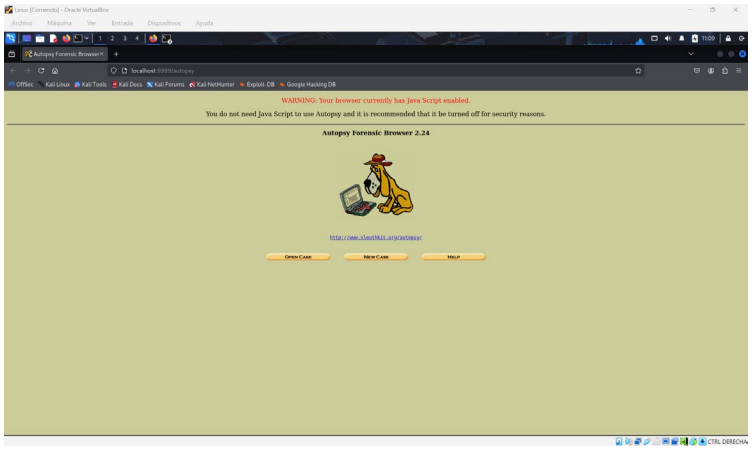
Al terminar lo más recomendable es reiniciar el sistema para que los cambios se hagan efectivos.

Ilustración 4 Finalización.



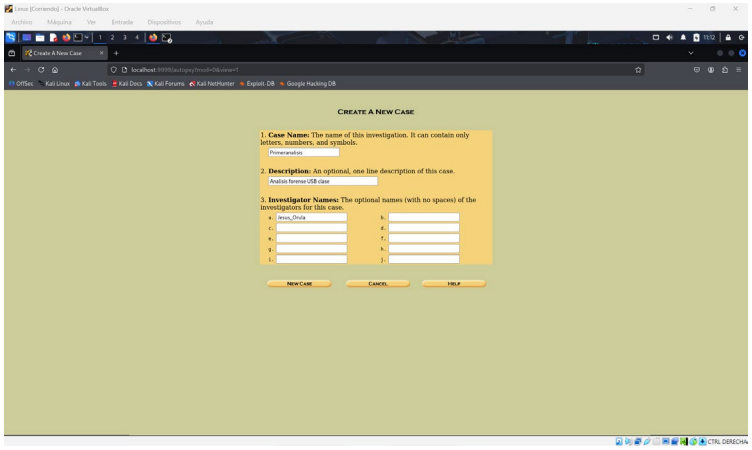
Abrir autopsy.

Ilustración 5 Autopsy.



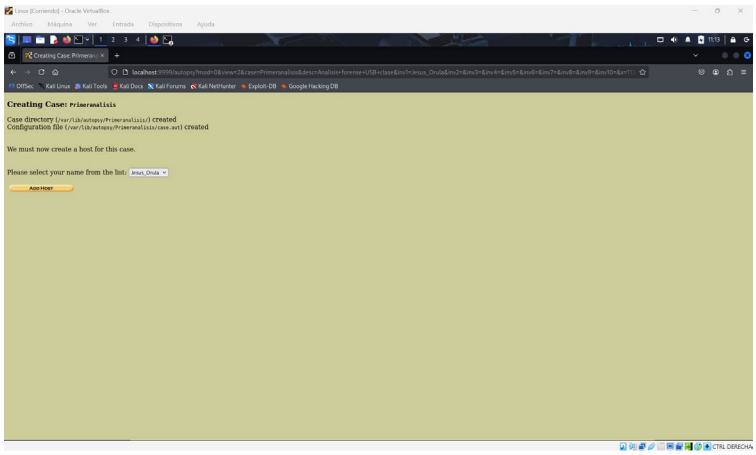
Crear caso, añadir una descripción y un nombre de investigador.

Ilustración 6 Crear caso en Linux.



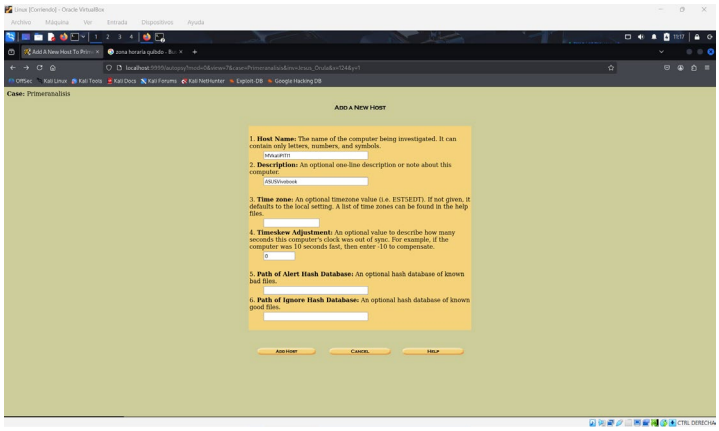
Caso creado con éxito.

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.

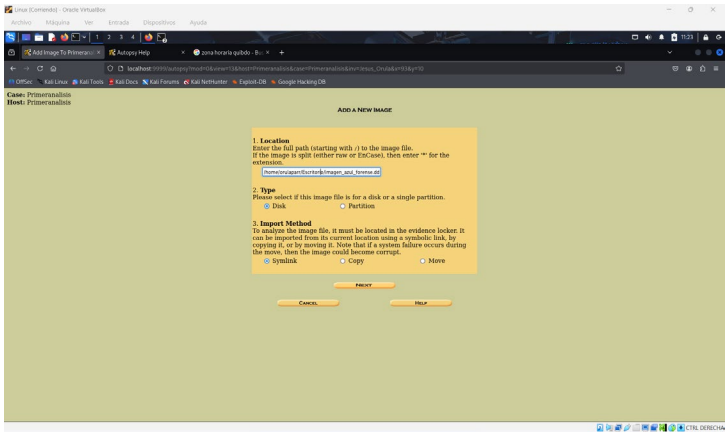
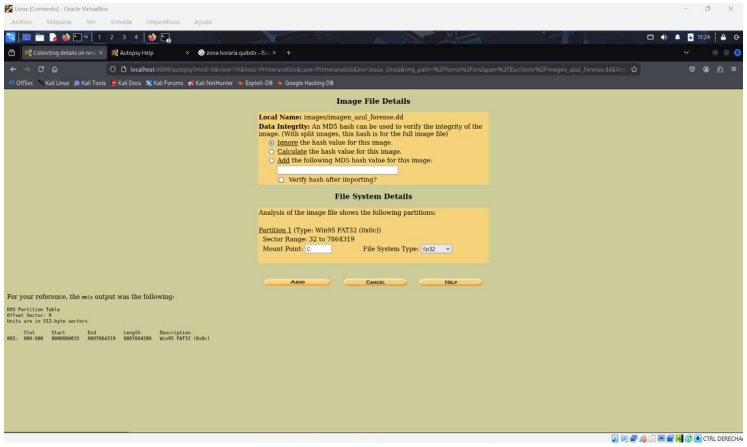
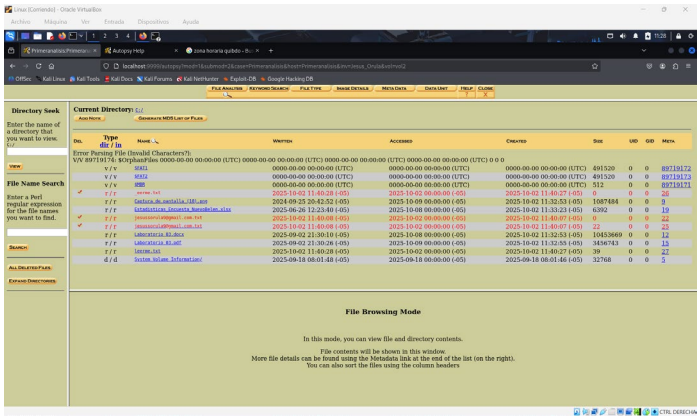


Ilustración 10 Detalles de la imagen.



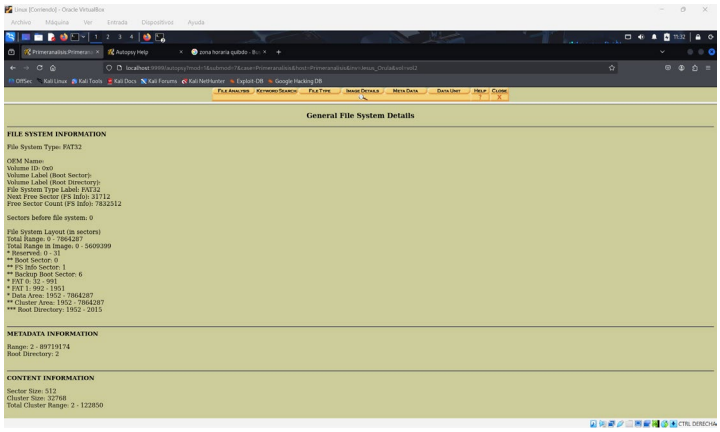
Aquí se pueden ver los archivos que contenía la imagen y los que contiene. Los azules son los que están presentes y los que aparecen en rojo son los que fueron eliminados alguna vez.

Ilustración 11 Archivos.



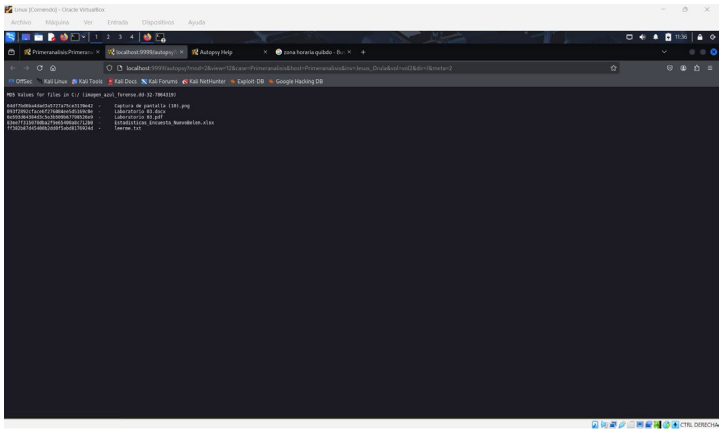
Información general del sistema de archivos.

Ilustración 12 Información general del sistema de archivos.



Cifrado de archivos en md5.

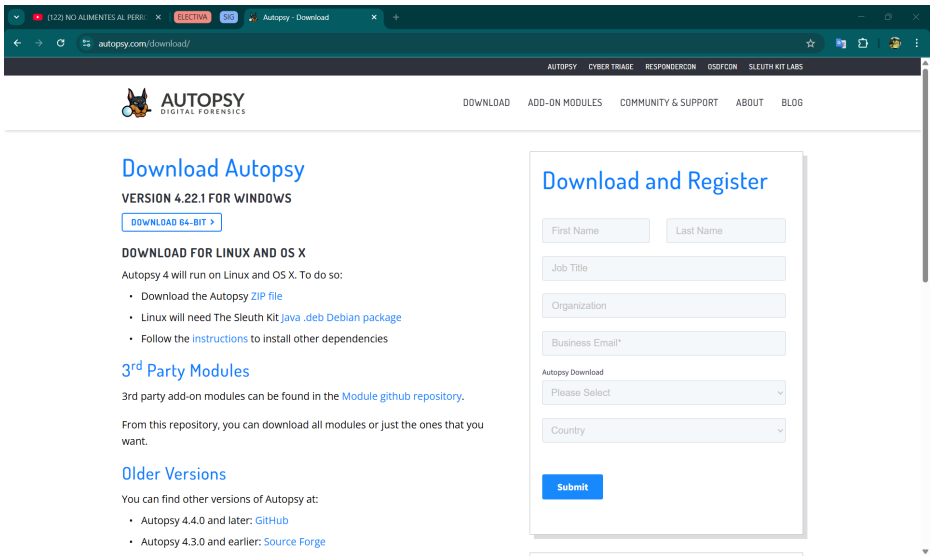
Ilustración 13 Cifrado md5.



ABRIR LINUX.

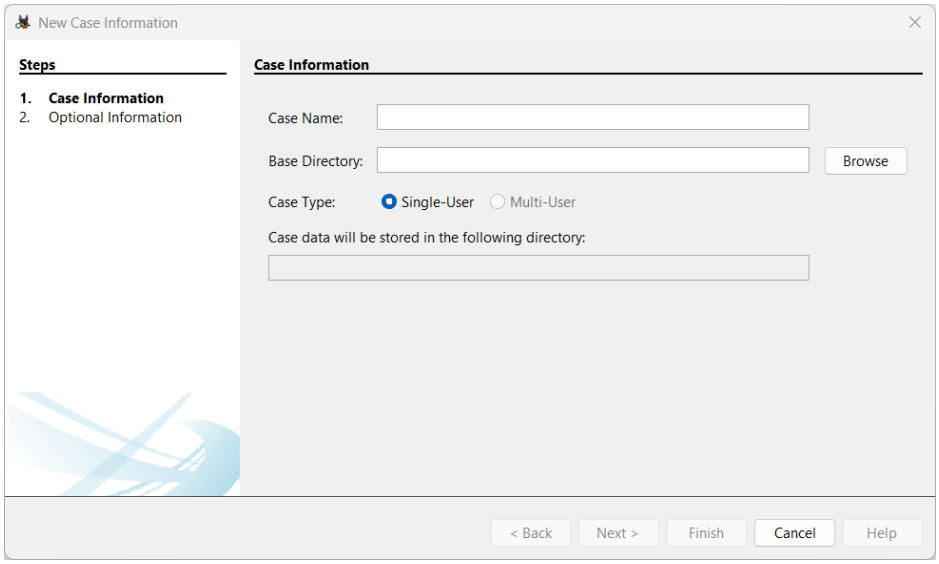
Descargar autopsy para windows desde su página principal.

Ilustración 14 Descargar autopsy.



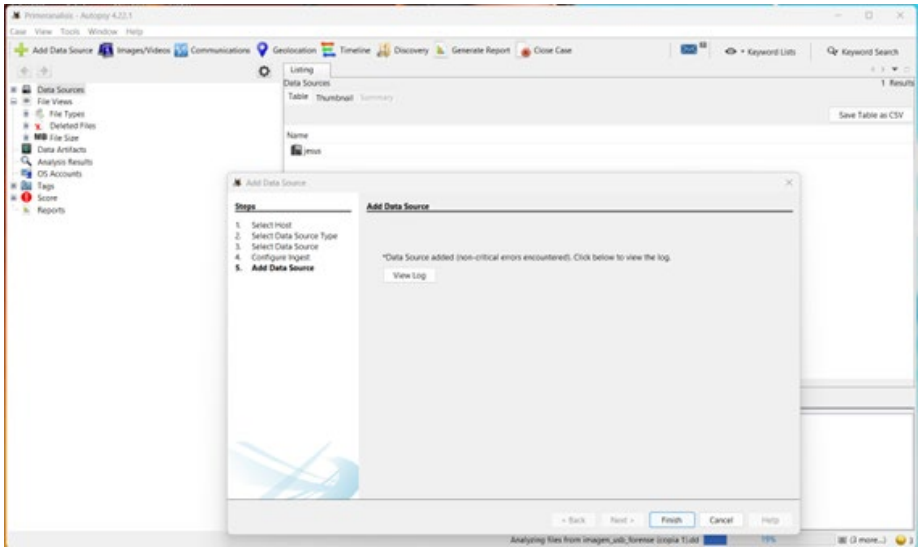
Luego de instalarlo, se procede a crear un caso.

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.