

--	--

--	--

Tabla de contenido

1.	OBJETIVO	3
2.	ALCANCE	3
3.	ENTRADAS	3
4.	SALIDAS	3
5.	FUENTES EXTERNAS	3
6.	DESARROLLO DEL LABORATORIO	4

--	--

1. OBJETIVO

El objetivo de este laboratorio es realizar la adquisición forense de una unidad USB siguiendo los procedimientos adecuados para garantizar la integridad de la evidencia. Para ello, se utilizarán herramientas como dd, fdisk, mmls, y sha1sum en Kali Linux, además de FTK Imager en Windows. Este laboratorio se ejecuta en un entorno virtualizado utilizando VirtualBox, donde tengo una máquina virtual con Kali Linux.

2. ALCANCE

Este procedimiento cubre la identificación de dispositivos, clonación de una unidad USB, extracción del MBR (Master Boot Record), validación de la integridad mediante hashes y análisis de la imagen en FTK Imager.

3. ENTRADAS

- a. Máquina virtual con Kali Linux en VirtualBox
- b. Unidad USB como dispositivo de almacenamiento a analizar
- c. Terminal de Kali Linux
- d. Comandos forenses (dd, fdisk, mmls, sha1sum)
- e. FTK Imager instalado en Windows

4. SALIDAS

- a. Imagen forense de la unidad USB (sdb.dd)
- b. Copia del Master Boot Record (mbr)
- c. Hashes SHA1 de la evidencia original y la imagen generada
- d. Reporte de análisis con capturas de pantalla

5. FUENTES EXTERNAS

Este laboratorio se desarrolla siguiendo la **guía proporcionada por el profesor, Ingeniero Manuel Pérez**, la cual detalla los procedimientos de adquisición de evidencia digital mediante herramientas como dd en Linux y **FTK Imager** en Windows.

La información presentada se basa en los pasos y comandos definidos en la guía, asegurando el cumplimiento del procedimiento indicado en el taller.

6. DESARROLLO DEL LABORATORIO

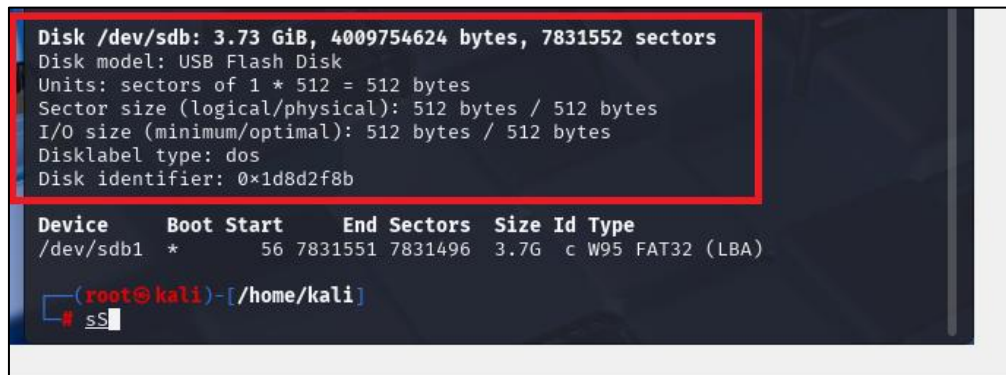
Paso 1: Inicio del entorno de trabajo

Inicié mi máquina virtual en **VirtualBox**, cargando el sistema operativo **Kali Linux**. Me aseguré de que la unidad USB estuviera conectada y reconocida por la máquina virtual.

Para garantizar que el sistema estuviera actualizado, ejecuté en la terminal: **sudo update-grub**. Luego, reinicié **Kali Linux** para aplicar los cambios.

Paso 2: Identificación del dispositivo USB

Para visualizar las unidades de almacenamiento conectadas, utilicé los siguientes comandos: **fdisk -l**



```
Disk /dev/sdb: 3.73 GiB, 4009754624 bytes, 7831552 sectors
Disk model: USB Flash Disk
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: 0x1d8d2f8b

Device      Boot  Start    End Sectors  Size Id Type
/dev/sdb1   *      56 7831551 7831496   3.7G  c W95 FAT32 (LBA)

(root@kali)~[/home/kali]
# ss
```

Imagen 1: Listado de dispositivos extraíbles, incluyendo la memoria USB de 4GB.

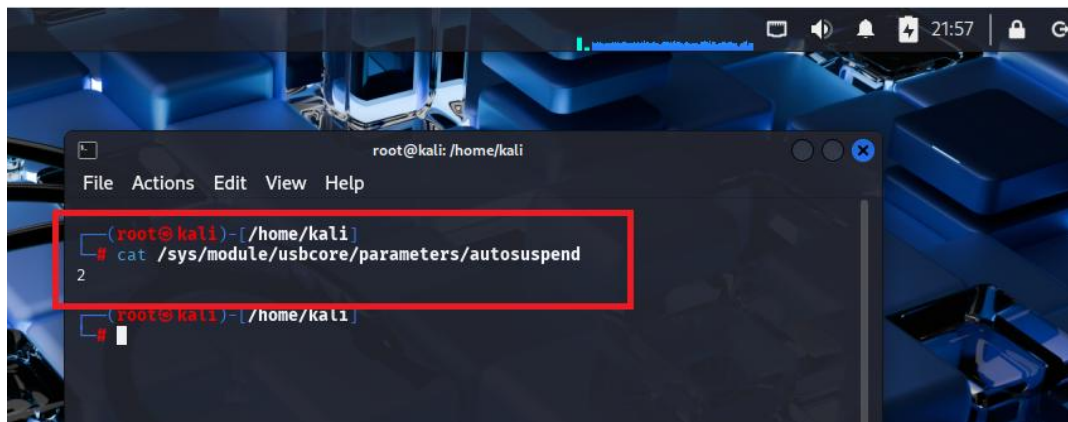


Imagen 2: Para evitar que la suspensión automática afecté mis dispositivos USB durante el laboratorio, procedí a modificar el archivo de configuración de GRUB en mi máquina virtual Kali Linux.

Primero, verifiqué el estado actual del parámetro autosuspend ejecutando el siguiente comando en la terminal: **cat /sys/module/usbcore/parameters/autosuspend**

Como resultado arrojo **2** lo que indica que la suspensión automática está activada. Para deshabilitar esta opción, edité el archivo de configuración de GRUB ubicado en **/etc/default/grub**

Abrí el archivo con privilegios de root usando el siguiente comando: **sudo nano /etc/default/grub** Dentro del archivo, ubiqué la línea: Y la modifiqué agregando el parámetro **usbcore.autosuspend=-1**, dejándola así: **GRUB_CMDLINE_LINUX_DEFAULT="quiet splash usbcore.autosuspend=-1"**

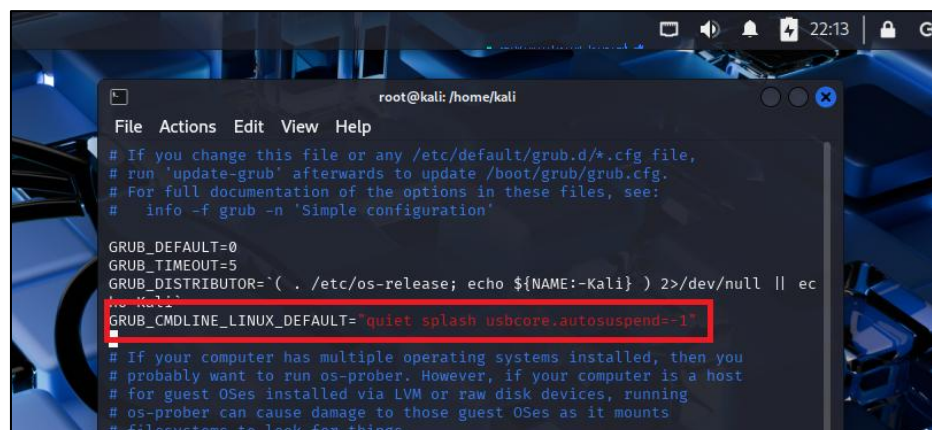
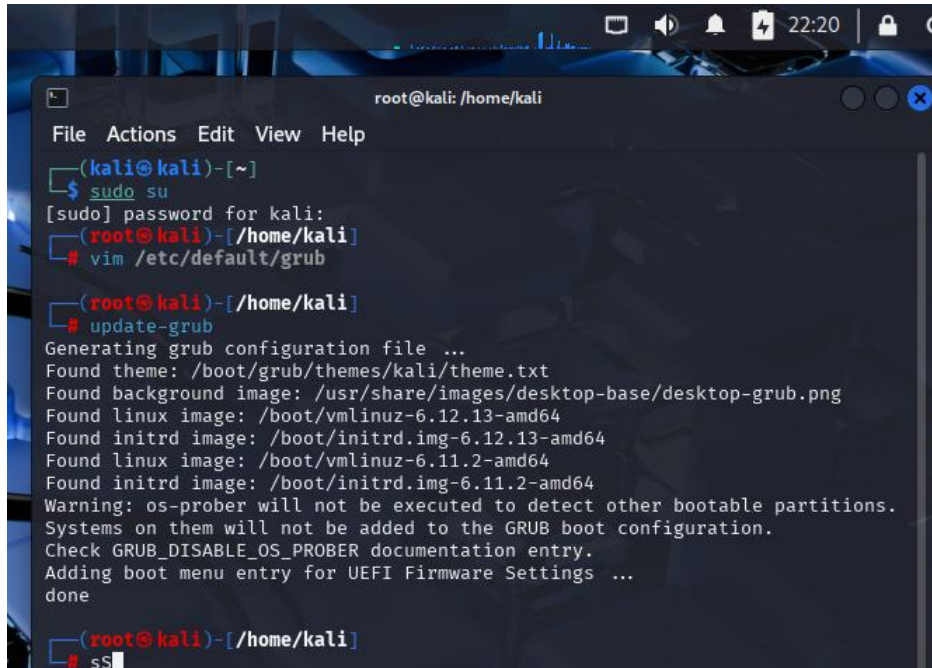


Imagen 3: modificación del archivo **/etc/default/grub**

Después de realizar la modificación, guardé los cambios (Ctrl + X, luego Y y Enter) y apliqué la configuración actualizando GRUB con el siguiente comando: **update-grub**

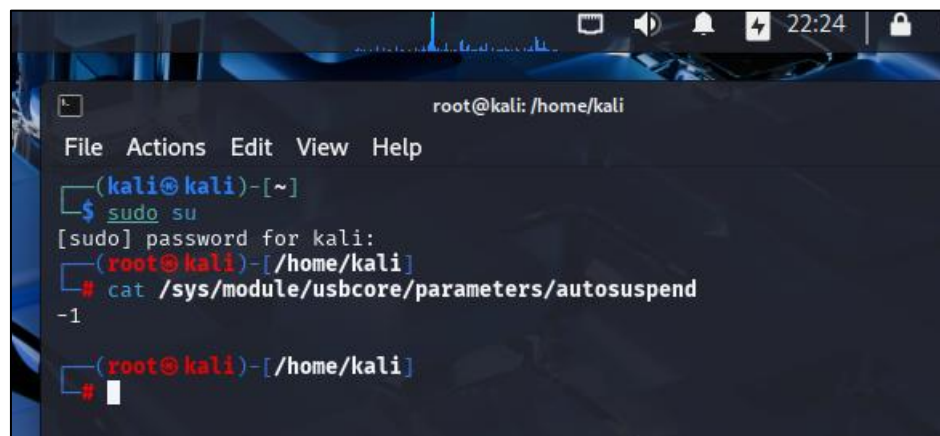
A terminal window titled 'root@kali: /home/kali' showing the execution of the 'update-grub' command. The user starts as 'kali' and uses 'sudo su' to become root. Then, they run 'vim /etc/default/grub' to edit the GRUB configuration. After saving and exiting vim, they run 'update-grub'. The command outputs the following: 'Generating grub configuration file ...', 'Found theme: /boot/grub/themes/kali/theme.txt', 'Found background image: /usr/share/images/desktop-base/desktop-grub.png', 'Found linux image: /boot/vmlinuz-6.12.13-amd64', 'Found initrd image: /boot/initrd.img-6.12.13-amd64', 'Found linux image: /boot/vmlinuz-6.11.2-amd64', 'Found initrd image: /boot/initrd.img-6.11.2-amd64', 'Warning: os-prober will not be executed to detect other bootable partitions. Systems on them will not be added to the GRUB boot configuration. Check GRUB_DISABLE_OS_PROBER documentation entry.', 'Adding boot menu entry for UEFI Firmware Settings ...', and 'done'. The prompt returns to root@kali: /home/kali.

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~$ vim /etc/default/grub
# update-grub
Generating grub configuration file ...
Found theme: /boot/grub/themes/kali/theme.txt
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.12.13-amd64
Found initrd image: /boot/initrd.img-6.12.13-amd64
Found linux image: /boot/vmlinuz-6.11.2-amd64
Found initrd image: /boot/initrd.img-6.11.2-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
(root@kali)~$ ss
```

Imagen 4: ejecuto comando update-grub para guardar los cambios modificados en el archivo grub

Finalmente, reinicié la máquina para que los cambios surtieran efecto: reboot

Una vez reiniciada la máquina, volví a ejecutar el comando de verificación: el por la modificacion anterior debe ser resultado -1

A terminal window titled 'root@kali: /home/kali' showing the execution of the 'cat' command to verify the status of USB autosuspend. The user is already root. They run 'cat /sys/module/usbcore/parameters/autosuspend'. The output is '-1'.

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~$ cat /sys/module/usbcore/parameters/autosuspend
-1
(root@kali)~$
```

Imagen 4: confirmando que la suspensión automática de dispositivos USB había sido deshabilitada correctamente el resultado fue -1

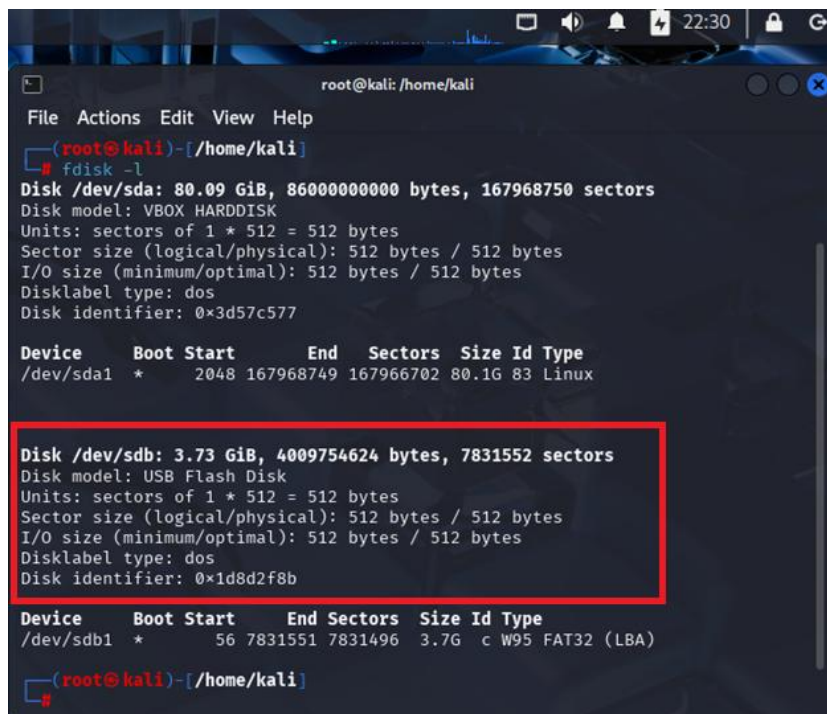
Toma de Imagen (Adquisición) de la Unidad USB

En este paso del laboratorio, procedí con la adquisición forense de la memoria USB conectada a mi máquina virtual Kali Linux en VirtualBox. La adquisición forense implica la creación de una copia exacta del dispositivo para su análisis sin alterar la evidencia original.

Visualización de la Unidad USB

Antes de proceder con la adquisición de la imagen, verifiqué que el sistema detectara correctamente la unidad USB ejecutando el siguiente comando: **fdisk -l**

Este comando listó todas las unidades de almacenamiento conectadas al sistema, incluyendo la memoria USB. Identifiqué que el dispositivo estaba asignado como **/dev/sdb**.



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# fdisk -l
Disk /dev/sda: 80.09 GiB, 86000000000 bytes, 167968750 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: 0x3d57c577

Device      Boot Start      End  Sectors  Size Id Type
/dev/sda1   *      2048 167968749 167966702 80.1G 83 Linux

Disk /dev/sdb: 3.73 GiB, 4009754624 bytes, 7831552 sectors
Disk model: USB Flash Disk
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: 0x1d8d2f8b

Device      Boot Start      End  Sectors  Size Id Type
/dev/sdb1   *         56 7831551 7831496   3.7G  c W95 FAT32 (LBA)

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

Imagen 5: reconocimiento unida extraíbles en este caso reconoció la USB de 4GB como **/dev/sdb**

Para visualizar la estructura de particiones de la unidad USB, utilicé el comando: **mmls /dev/sdb**

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)~[/home/kali]
# mmls /dev/sdb
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Slot      Start      End      Length    Description
000: Meta  0000000000 0000000000 0000000001 Primary Table (#0)
001:      0000000000 0000000055 0000000056 Unallocated
002: 000:000 0000000056 0007831551 0007831496 Win95 FAT32 (0x0c)

(root@kali)~[/home/kali]
#
```

Imagen 6: evidencia de la ejecución del comando **mmls /dev/sdb**

Este comando permitió ver los sectores donde inician y terminan las particiones dentro del dispositivo, información útil para decidir qué imagen forense generar.

Explicación de los Parámetros en el Comando DD

Antes de realizar la clonación, comprendí los parámetros principales del comando **dd**, que es una herramienta utilizada en la adquisición de imágenes forenses:

- a. **if= (input file):** Especifica la ubicación de origen de la imagen (en este caso, la unidad USB).
- b. **of= (output file):** Define el nombre y la ubicación del archivo donde se almacenará la imagen clonada.

Adquisición Forense de la Unidad USB

Para capturar la imagen completa de la unidad, ejecuté el siguiente comando: **dd if=/dev/sdb of=/home/kali/sdb.dd**

Con este comando, generé una copia bit a bit de toda la unidad USB en un archivo de imagen (sdb.dd).

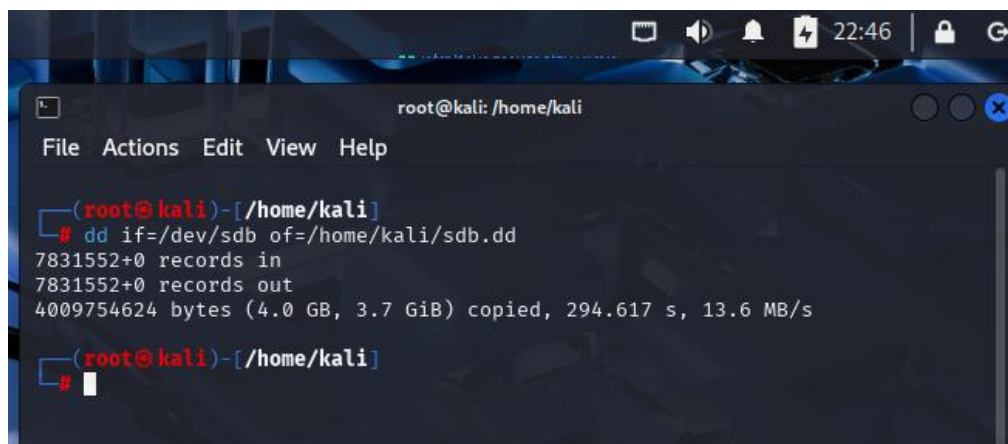
A screenshot of a terminal window titled 'root@kali: /home/kali'. The window shows the execution of the command 'dd if=/dev/sdb of=/home/kali/sdb.dd'. The output indicates that 7831552+0 records were read and written, totaling 4009754624 bytes (4.0 GB, 3.7 GiB) copied in 294.617 seconds at a speed of 13.6 MB/s. The prompt is now '# '.

Imagen 7: evidencia copia bit a bit de toda la unidad USB

Copia del Master Boot Record (MBR)

Para capturar exclusivamente el MBR, que contiene la tabla de particiones y el código de arranque, utilicé: **dd if=/dev/sdb of=/home/kali/mbr bs=512 count=1**

Con este comando copió los primeros 512 bytes del disco, que corresponden al MBR.

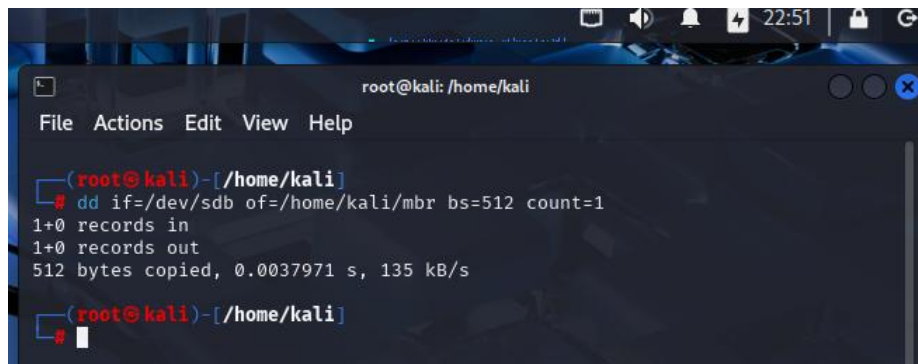
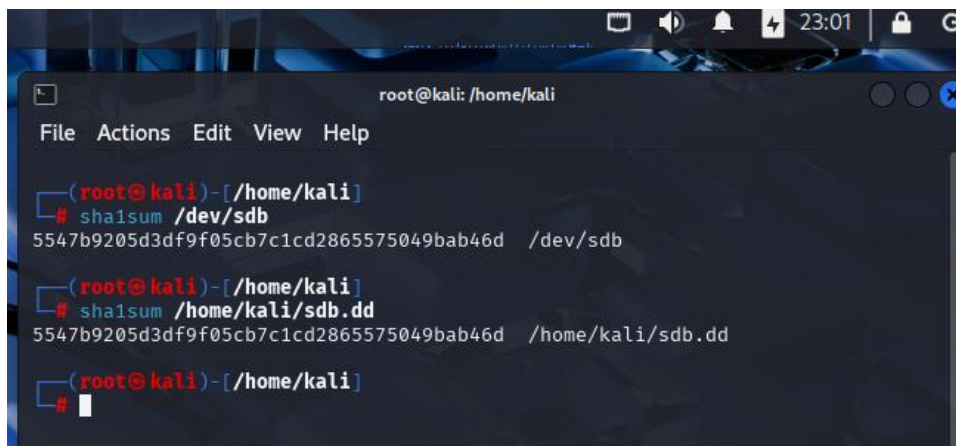
A screenshot of a terminal window titled 'root@kali: /home/kali'. The window shows the execution of the command 'dd if=/dev/sdb of=/home/kali/mbr bs=512 count=1'. The output indicates that 1+0 records were read and written, totaling 512 bytes copied in 0.0037971 seconds at a speed of 135 kB/s. The prompt is now '# '.

Imagen 8: evidencia copia de los primeros 512 bytes del disco, que correspondiente al MBR.

Validación de la Integridad de la Imagen

Para garantizar que la copia forense no sufrió alteraciones, generé y comparé los hashes de la unidad original y de la imagen adquirida. Primero, obtuve el hash SHA-1 de la unidad USB ejecutando el comando: `sha1sum /dev/sdb`

Luego, generé el hash de la imagen obtenida con el comando: `sha1sum /home/kali/sdb.dd`

A screenshot of a terminal window on a Kali Linux system. The window title is 'root@kali: /home/kali'. The terminal shows three commands and their outputs. The first command is 'sha1sum /dev/sdb', which outputs '5547b9205d3df9f05cb7c1cd2865575049bab46d /dev/sdb'. The second command is 'sha1sum /home/kali/sdb.dd', which outputs '5547b9205d3df9f05cb7c1cd2865575049bab46d /home/kali/sdb.dd'. The third command is a prompt for another command, with a cursor visible. The terminal has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The background of the terminal is dark with a blue and white pattern.

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# sha1sum /dev/sdb
5547b9205d3df9f05cb7c1cd2865575049bab46d /dev/sdb

(root@kali)-[/home/kali]
# sha1sum /home/kali/sdb.dd
5547b9205d3df9f05cb7c1cd2865575049bab46d /home/kali/sdb.dd

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

Imagen 9: evidencia de la generación hash SHA-1 de la USB

Dado que ambos valores hash coinciden, puedo confirmar que la imagen forense (sdb.dd) es una copia exacta de la unidad USB original (/dev/sdb). Esto garantiza la integridad de la evidencia digital y permite continuar con su análisis sin riesgo de alteración.

FTK IMAGER sobre Windows

Seguí los pasos de instalación de **FTK Imager** AccessData_FTK_Imager_4.7.1 según la guía del profesor, descargando la herramienta desde el sitio oficial y ejecutando la instalación con privilegios de administrador.

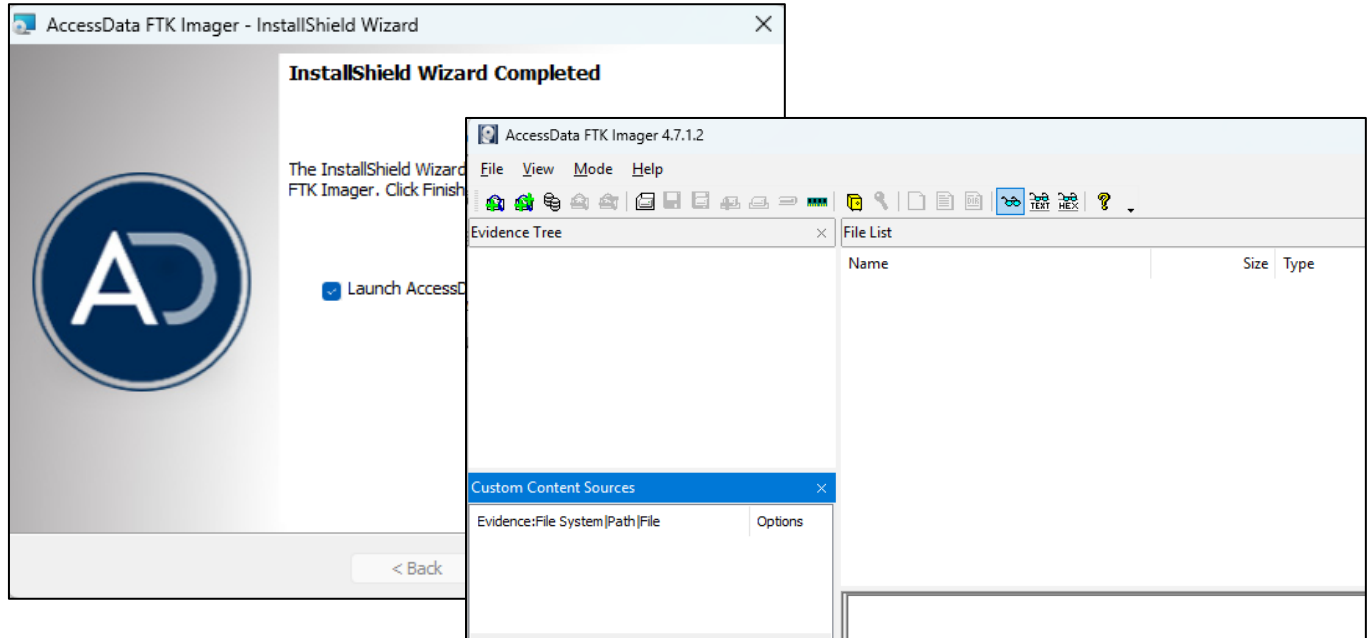


Imagen 9: instalación de imagen descarga de la herramienta desde el sitio web oficial de Exterro y descargué el instalador de FTK Imager en mi sistema.

Inicie FTK y cree una imagen digital forense

Inicié **FTK Imager** y procedí a crear una imagen digital forense siguiendo las instrucciones proporcionadas en la guía del profesor.

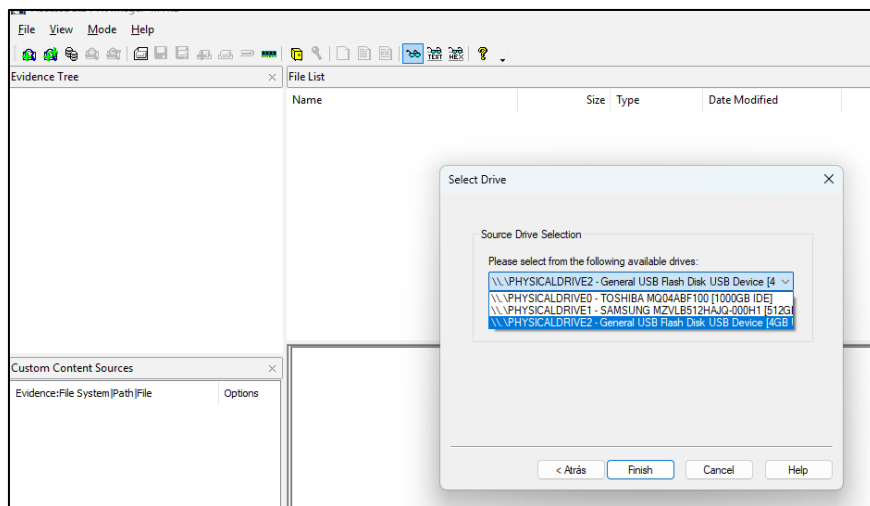


Imagen 10: configuración para la creación de la imagen digital forense

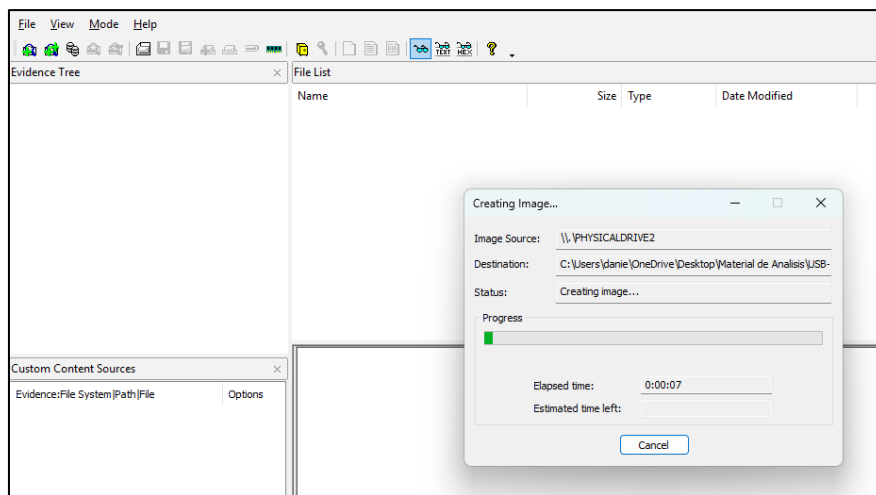


Imagen 11: Inicio de la creación de la imagen digital forense

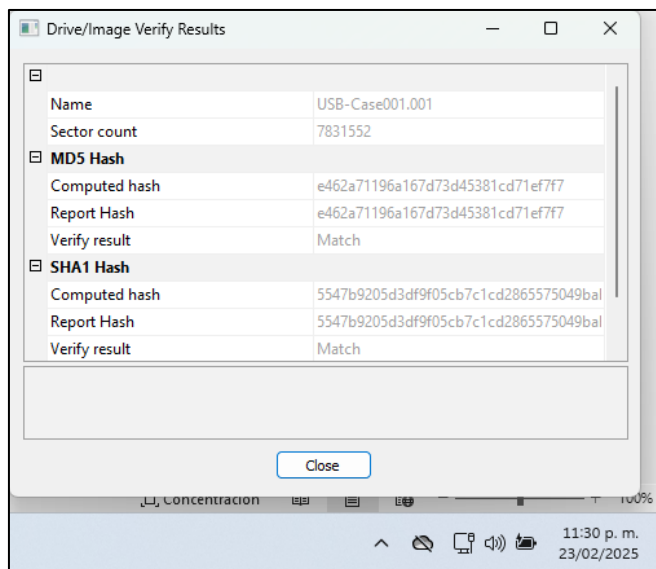


Imagen 12: Finalización de la creación de la imagen digital forense

Ordenar Ver ...				
Nombre	Fecha de modificación	Tipo	Tamaño	
USB-Case001	23/02/2025 11:27 p. m.	Archivo WinRAR	1.536.000 KB	
USB-Case001.001	23/02/2025 11:30 p. m.	Documento de tex...	2 KB	
USB-Case001.002	23/02/2025 11:29 p. m.	Archivo 002	1.536.000 KB	
USB-Case001.003	23/02/2025 11:30 p. m.	Archivo 003	843.776 KB	

Imagen 13: Archivos generados por la creación de la imagen forense con la herramienta AccessData_FTK

Resumen de la adquisición: Copy -& Paste

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: EF-EMP-Case001

Evidence Number: 001

--	--

Unique description: Eliminación de archivos

Examiner: Daniel Rojas

Notes: Recuperación de datos eliminados

Information for C:\Users\danie\OneDrive\Desktop\Material de Analisis\USB-Case001:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 487

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 7.831.552

[Physical Drive Information]

Drive Model: General USB Flash Disk USB Device

Drive Serial Number: AA00000000000489

Drive Interface Type: USB

Removable drive: True

Source data size: 3824 MB

Sector count: 7831552

[Computed Hashes]

MD5 checksum: e462a71196a167d73d45381cd71ef7f7

SHA1 checksum: 5547b9205d3df9f05cb7c1cd2865575049bab46d

Image Information:

Acquisition started: Sun Feb 23 23:25:36 2025

Acquisition finished: Sun Feb 23 23:30:11 2025

Segment list:

C:\Users\danie\OneDrive\Desktop\Material de Analisis\USB-Case001.001

C:\Users\danie\OneDrive\Desktop\Material de Analisis\USB-Case001.002

C:\Users\danie\OneDrive\Desktop\Material de Analisis\USB-Case001.003

Image Verification Results:

Verification started: Sun Feb 23 23:30:11 2025

Verification finished: Sun Feb 23 23:30:23 2025

MD5 checksum: e462a71196a167d73d45381cd71ef7f7 : verified

SHA1 checksum: 5547b9205d3df9f05cb7c1cd2865575049bab46d : verified

Finalicé la creación de la imagen forense con **FTK Imager**, asegurando la integridad de los datos mediante la generación y verificación de los valores hash **MD5** y **SHA1**. La imagen digital se generó correctamente con la información del caso y se almacenó en segmentos en la carpeta designada. La verificación confirmó que la adquisición se realizó sin alteraciones, garantizando la autenticidad de la evidencia.

Cargar imagen digital en FTK

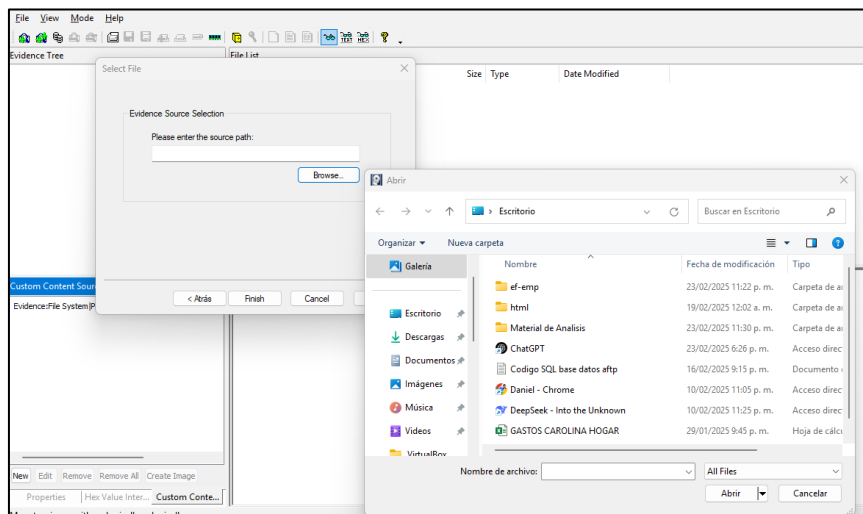


Imagen 14: proceso de carga de la imagen forense generada con la herramienta AccessData_FTK

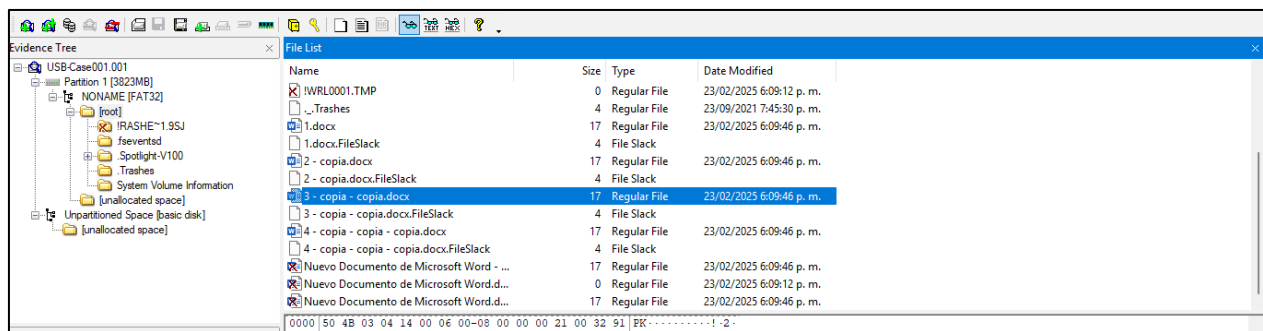


Imagen 15: evidencia de archivo borrado

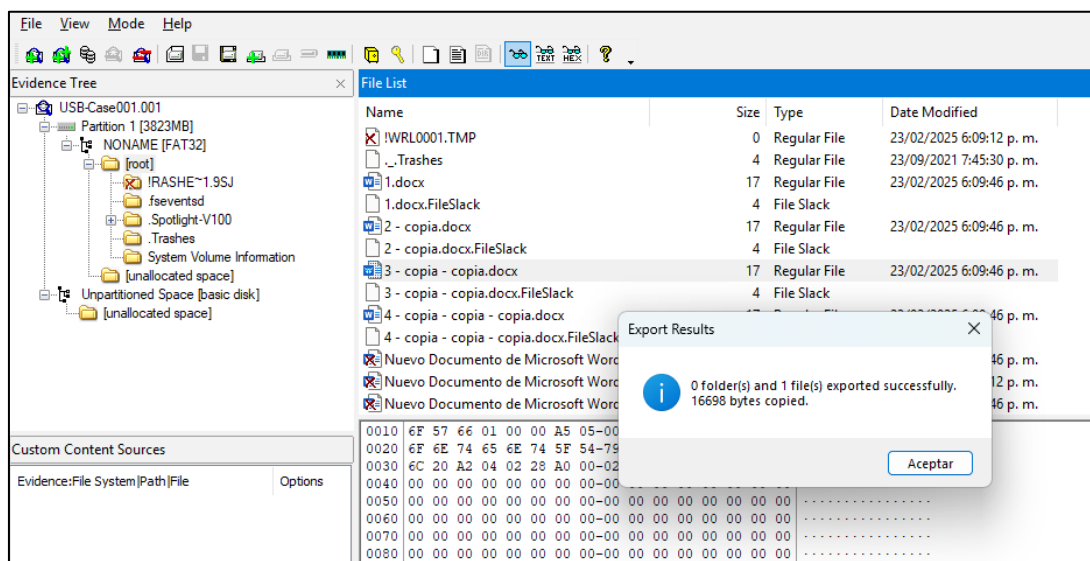


Imagen 16: Extracción de archivo al equipo local

Lectura visible de la Extracción

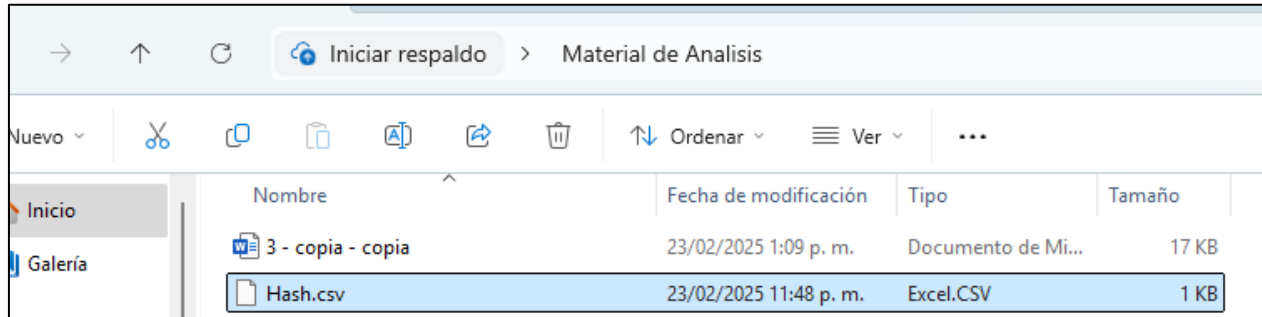


Imagen 17: evidencia de archivos hash generado.

Validación del hash de extracción.

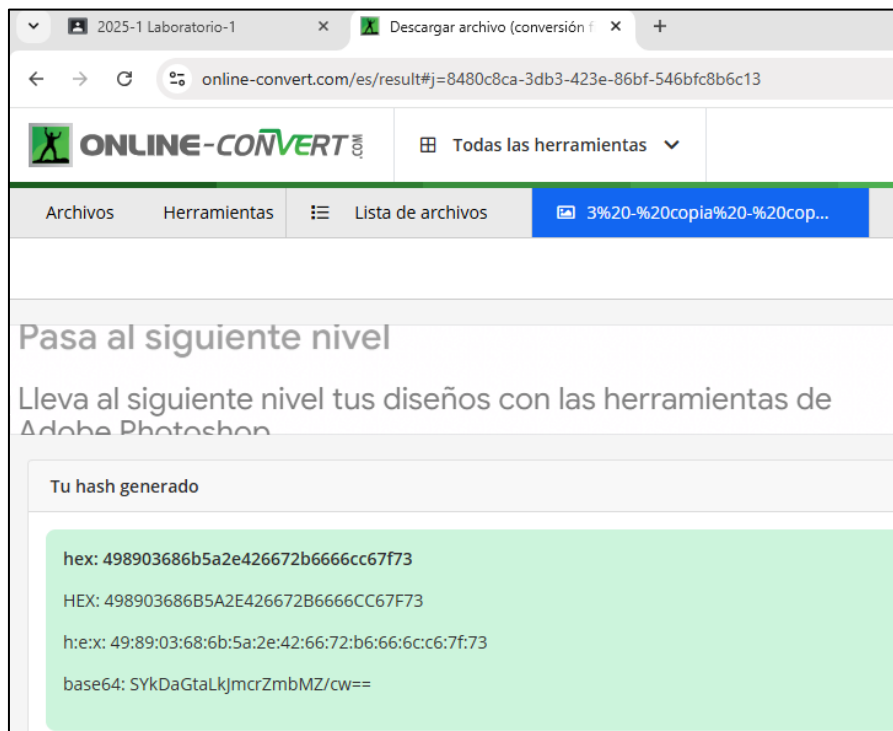


Imagen 18: se genera hash del archivo

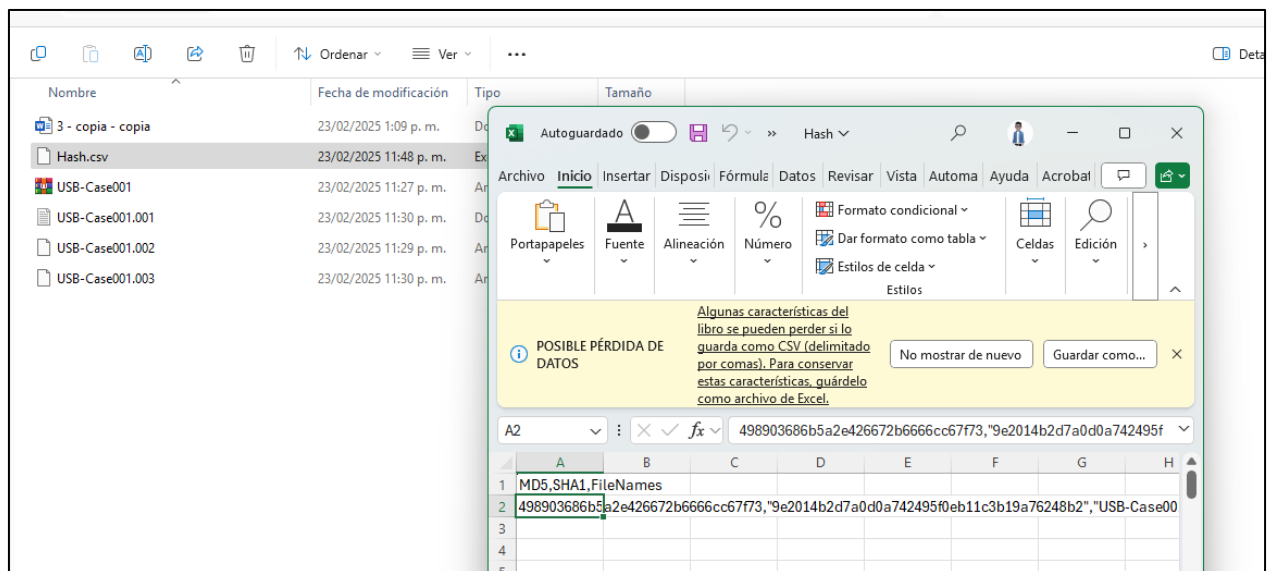


Imagen 19: se valida las claves y son correctas.

Realicé el proceso de carga de la imagen forense en **FTK Imager**, donde pude visualizar la estructura de los archivos, incluyendo aquellos eliminados. Extraje archivos al equipo local para su análisis y generé los valores hash correspondientes para validar su autenticidad. Finalmente, verifiqué la integridad de los datos comparando los hashes obtenidos, confirmando que la extracción se realizó sin alteraciones.

--	--

7. Conclusión

En este laboratorio, seguí detalladamente la guía proporcionada por el **Ingeniero Manuel Pérez** para realizar la adquisición y análisis de una imagen forense de una memoria USB. Utilicé herramientas como **dd** en **Kali Linux** para generar imágenes forenses y **FTK Imager** para su análisis. Aseguré la integridad de los datos mediante la verificación de hashes y logré recuperar archivos eliminados con éxito. Este proceso permitió comprender la importancia de la adquisición forense de evidencia digital y la validación de su autenticidad, garantizando la confiabilidad de los datos en un análisis forense.