Practica 2

# Adquisición de evidencia, sistema apagado (Cold-Clone)

1. ¿Qué requisitos debemos de cumplir para que la evidencia digital no se vea comprometida?

Para garantizar la integridad y validez de la evidencia digital, es esencial cumplir con los siguientes requisitos:

- Establecer una cadena de custodia sólida
- Preservar la integridad de la evidencia, evitando modificaciones
- Autenticar la evidencia, demostrando su origen y conservación
- Aplicar medidas de seguridad física y lógica
- Utilizar herramientas y métodos forenses reconocidos
- Registrar detalladamente todas las acciones realizadas
- Capacitar al personal en prácticas forenses digitales
- Documentar de manera completa la evidencia y el proceso
- Conservar los metadatos asociados con la evidencia
- Cumplir con las leyes y regulaciones aplicables

2. ¿Qué materiales/software necesitas?

Para la clonación de un disco, podemos necesitar los siguientes materiales y software:

- **Materiales:**
  - Un dispositivo de almacenamiento de origen (disco que se va a clonar).
  - Un dispositivo de almacenamiento de destino (disco donde se copiarán los datos).
  - Un USB con Kali Live Boot.
- **Software:**
  - Kali Live Boot: Proporciona un entorno Linux desde una unidad USB o DVD sin instalar en el sistema principal.
  - dd: Herramienta de línea de comandos para copiar y convertir archivos.
  - Terminal de Linux: Para ejecutar comandos, como el comando dd.

Partimos de una máquina virtual que tiene un VHD vacío y un Kali Linux Live Boot, añadiremos el disco duro donde obtendremos las evidencias.


Después de agregar el disco a la máquina virtual, podemos verificar su estado utilizando el comando **'lsblk'**.

```
┌──(kali㉿kali)-[~]
└─$ lsblk
NAME                    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0                     7:0    0  3.6G  1 loop /usr/lib/live/mount/rootfs/filesystem.squashfs
                                                  /run/live/rootfs/filesystem.squashfs
sda                       8:0    0    5G  0 disk
sdb                       8:16   0    5G  0 disk
├─sdb1                    8:17   0  487M  0 part
├─sdb2                    8:18   0    1K  0 part
└─sdb5                    8:21   0  4.5G  0 part
  ├─debian--vg-root     254:0    0  1.8G  0 lvm
  ├─debian--vg-swap_1   254:1    0  976M  0 lvm
  └─debian--vg-home     254:2    0  1.8G  0 lvm
sr0                      11:0    1  4.2G  0 rom  /usr/lib/live/mount/medium
                                                  /run/live/medium
```

La clonación de discos en sistemas Linux puede llevarse a cabo utilizando el comando "**dd**". Este comando es potente, aunque debe usarse con precaución, ya que opera a nivel de bajo nivel y puede sobrescribir datos de manera irreversible si se utiliza incorrectamente.

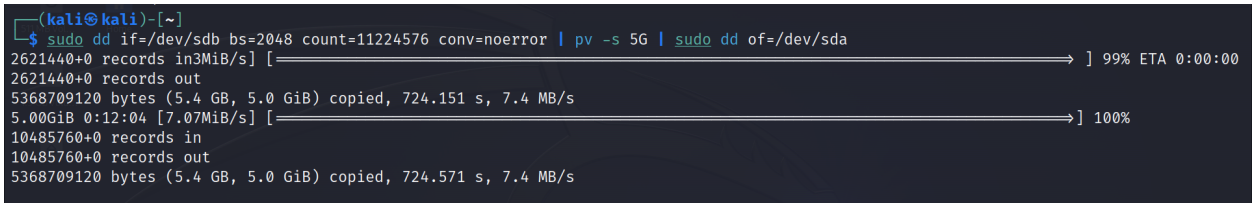
***sudo dd if=/dev/sdb bs=2048 count=11224576 conv=noerror | pv -s 5G | sudo dd of=/dev/sda***

En este caso hemos dividido el comando en tres secciones con el carácter "|".

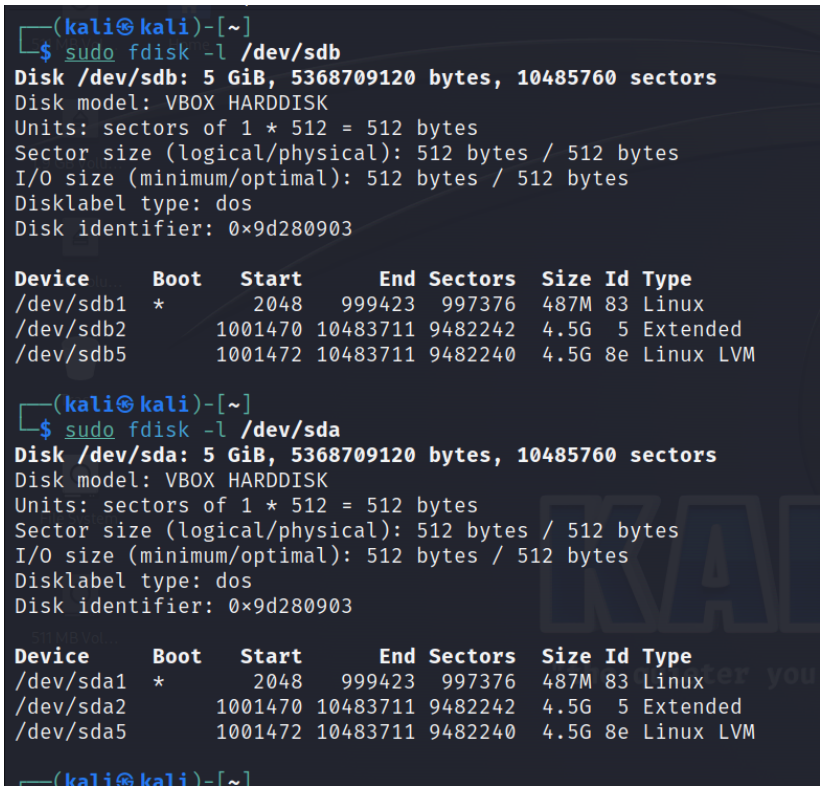
- **dd if=/dev/sdb bs=2048 count=11224576 conv=noerror**: Esta primera parte del comando realiza la lectura desde el dispositivo de origen (/dev/sdb) con un tamaño de bloque (bs) de 2048 bytes. La opción count limita la cantidad de bloques que se copiarán, en este caso, se están copiando 11224576 bloques. La opción conv=noerror permite que la operación continúe incluso si se encuentran errores de lectura en el dispositivo de origen.

- **pv -s 5G**: Aquí se utiliza el comando pv (Pipe Viewer) para mostrar el progreso de la operación. pv -s 5G indica que el tamaño total de la operación es de 5 gigabytes

- **dd of=/dev/sda**: La segunda parte del comando realiza la escritura en el dispositivo de destino (/dev/sda). Este comando copia los datos del dispositivo de origen al dispositivo de destino



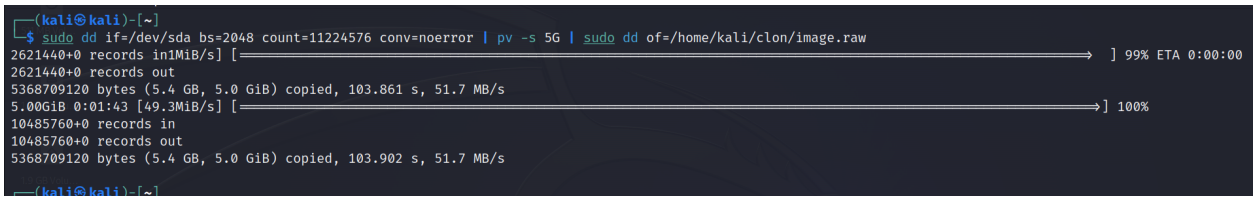
Podemos verificar que la clonación se ha realizado correctamente utilizando los comandos '**fdisk -l /dev/sdb**' y '**fdisk -l /dev/sda**', asegurándonos de que ambos dispositivos presentan la misma información



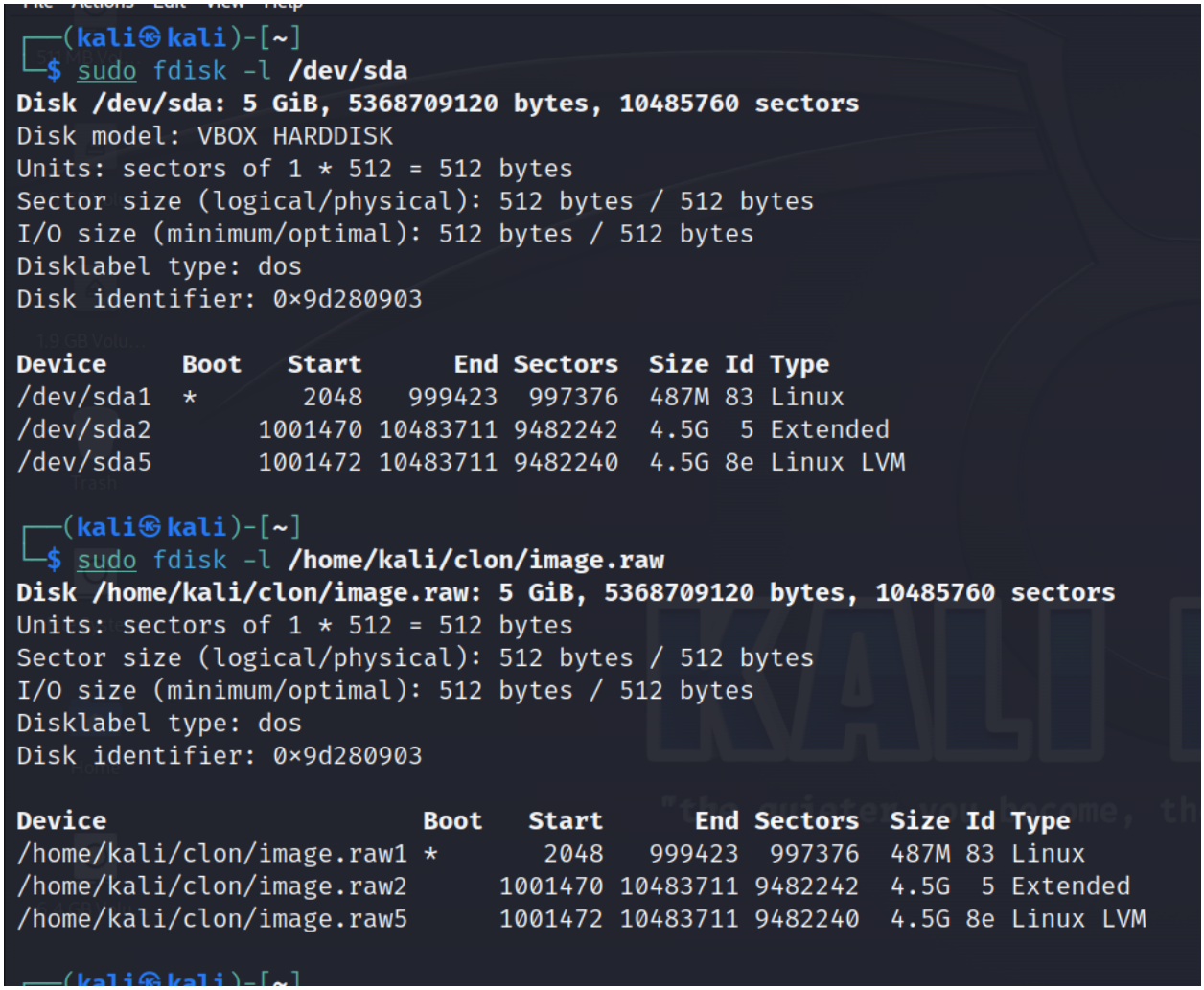

Finalmente, podemos confirmar que ambos discos, tanto el original como la copia, tienen el mismo hash utilizando el comando '**sha512sum**'


Como estoy trabajando con un Kali Live muestro la salida del comando history

Una vez completada la clonación del disco, podemos generar una imagen de disco a partir de la clonación realizada utilizando el mismo comando que se empleó previamente.




Podemos verificar que la clonación se ha realizado correctamente utilizando los comandos '**fdisk -l /dev/sda**' y '**fdisk -l /home/kali/clon/image.raw**', asegurándonos de que ambos dispositivos presentan la misma información



Finalmente, podemos confirmar que ambos discos, tanto el original como la copia, tienen el mismo hash utilizando el comando '**sha512sum**'

```
┌──(kali㉿kali)-[~]
└─$ sudo sha512sum /dev/sda
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae  /dev/sda

┌──(kali㉿kali)-[~]
└─$ sudo sha512sum /home/kali/clon/image.raw
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae  /home/kali/clon/image.raw

┌──(kali㉿kali)-[~]
```

Salida del comando history

```
┌──(kali㉿kali)-[~]
└─$ history
    1  setxkbmap es
    2  sudo mkfs.ext4 /dev/sdb
    3  mkdir clon
    4  sudo mount /home/kali/clon
    5  sudo mount /dev/sdb /home/kali/clon
    6  sudo dd if=/dev/sda bs=2048 count=11224576 conv=noerror | pv -s 5G | sudo dd of=/home/kali/clon/image.raw
    7  sudo fdisk -l /dev/sda
    8  sudo fdisk -l /home/kali/clon/image.raw
    9  sudo sha512sum /dev/sda
   10  sudo sha512sum /home/kali/clon/image.raw

┌──(kali㉿kali)-[~]
```