

Análisis Forense

ADQUISICIÓN DE EVIDENCIAS. SISTEMA APAGADO (COLD-CLONE)

Jennifer Galván Bejarano

Índice

Introducción	3
Preparación del entorno	4
Técnica Clonación	7
Calculando el hash	8
Técnica Imagen	10
Calculando el hash	11
Respuesta de las preguntas.	12

Introducción

En este documento vamos a aprender a realizar la adquisición de evidencias digitales en un entorno forense con el sistema apagado (Cold-Clone). Se explican paso a paso los procedimientos para preparar el entorno virtual, clonar discos, crear imágenes forenses y verificar la integridad de los datos mediante el uso de hashes.

Requisitos para realizar la práctica

Software de virtualización:

- VirtualBox (u otro gestor de máquinas virtuales compatible).

- Archivos necesarios:

- Disco virtual debian10.vdi (sistema que se va a analizar/clonar).

- Imagen ISO de Kali Linux Live (para arrancar el sistema sin iniciar Debian).

Configuración de la máquina virtual:

- Crear nueva VM en VirtualBox.

- Asignar el disco debian10.vdi como disco principal.

- Añadir un segundo disco duro para clonar.

- Montar la ISO de Kali como sistema de arranque (Live).

Conocimientos básicos y comandos utilizados:

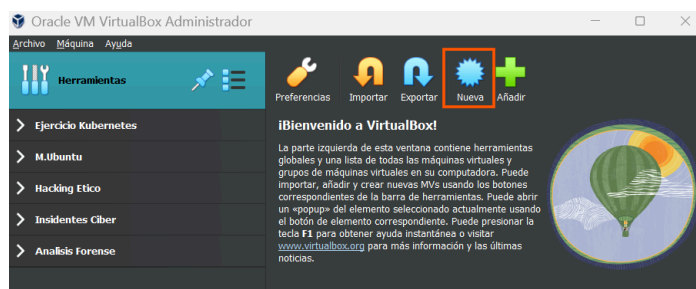
- Uso de terminal en Linux.

- Comandos como dd, fdisk, sha512sum, mkfs.ext4, mount, etc.

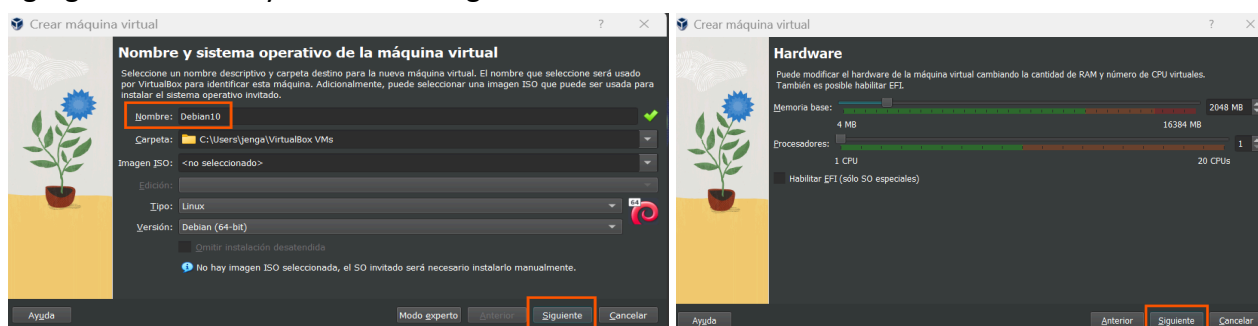
Preparación del entorno

Descargue el disco debian10.vdi

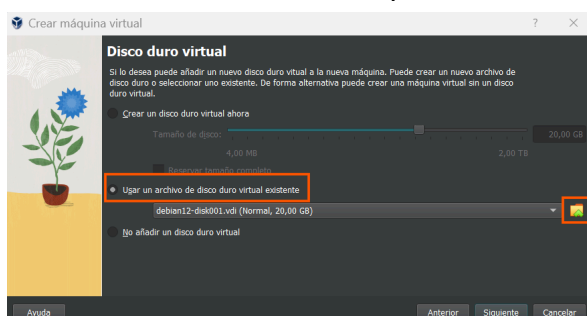
En Virtual box en el área de herramientas seleccionar Nueva



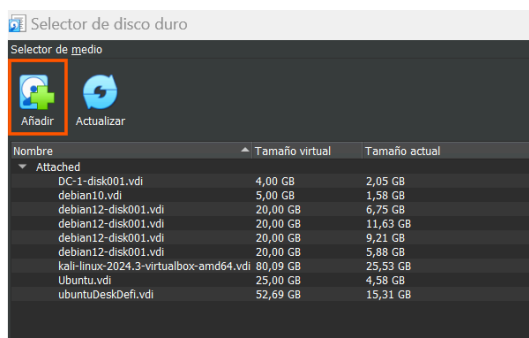
Agregar un nombre y seleccionar siguiente



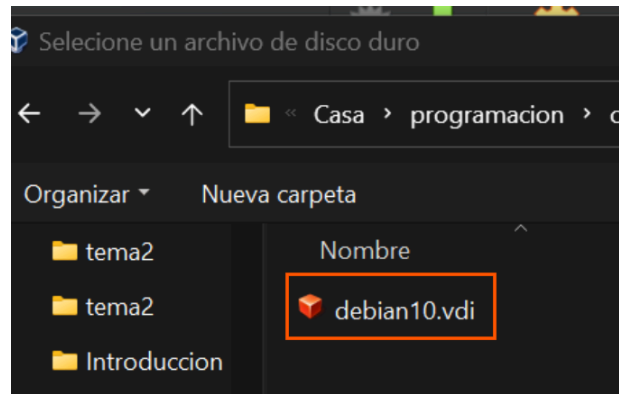
Seleccionar Usar un archivo de disco duro virtual existente y seleccionar la símbolo de la carpeta



Se abre una ventana, seleccionar Añadir



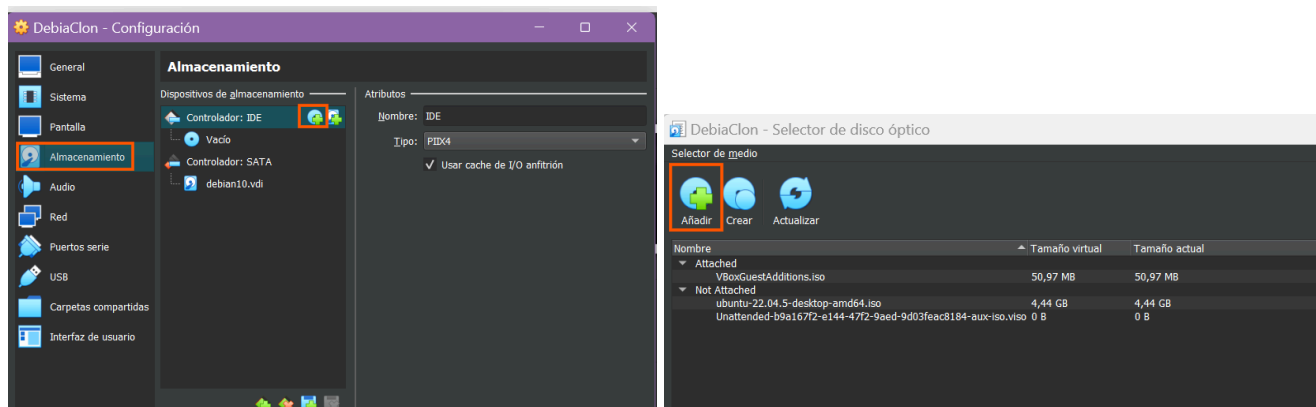
Seleccionar el disco que se pide en las indicaciones

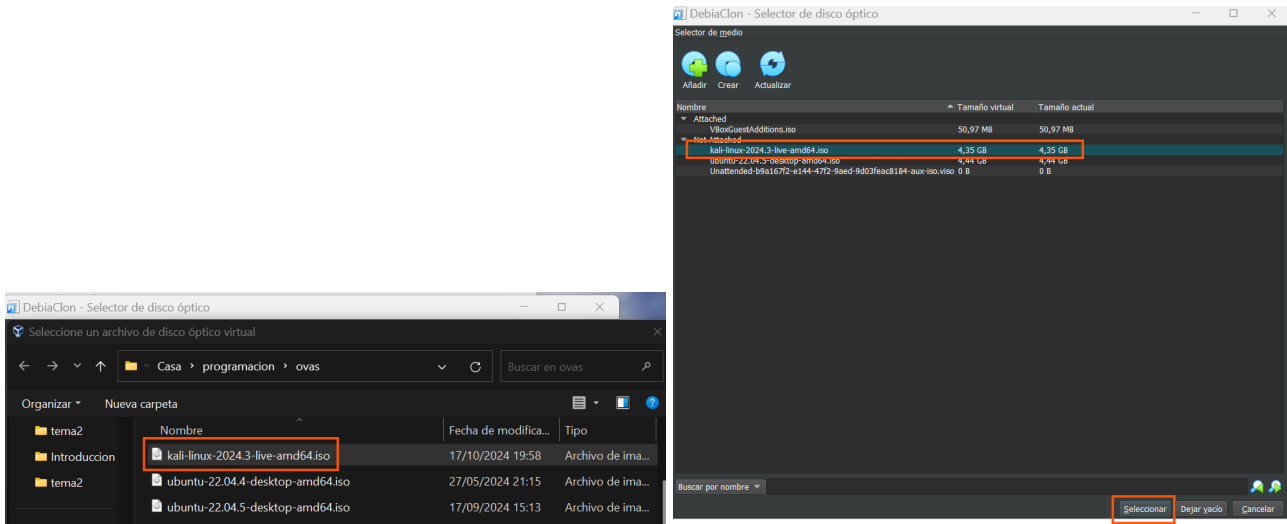


Seleccionar el disco que vamos a clonar y seleccionamos configuración

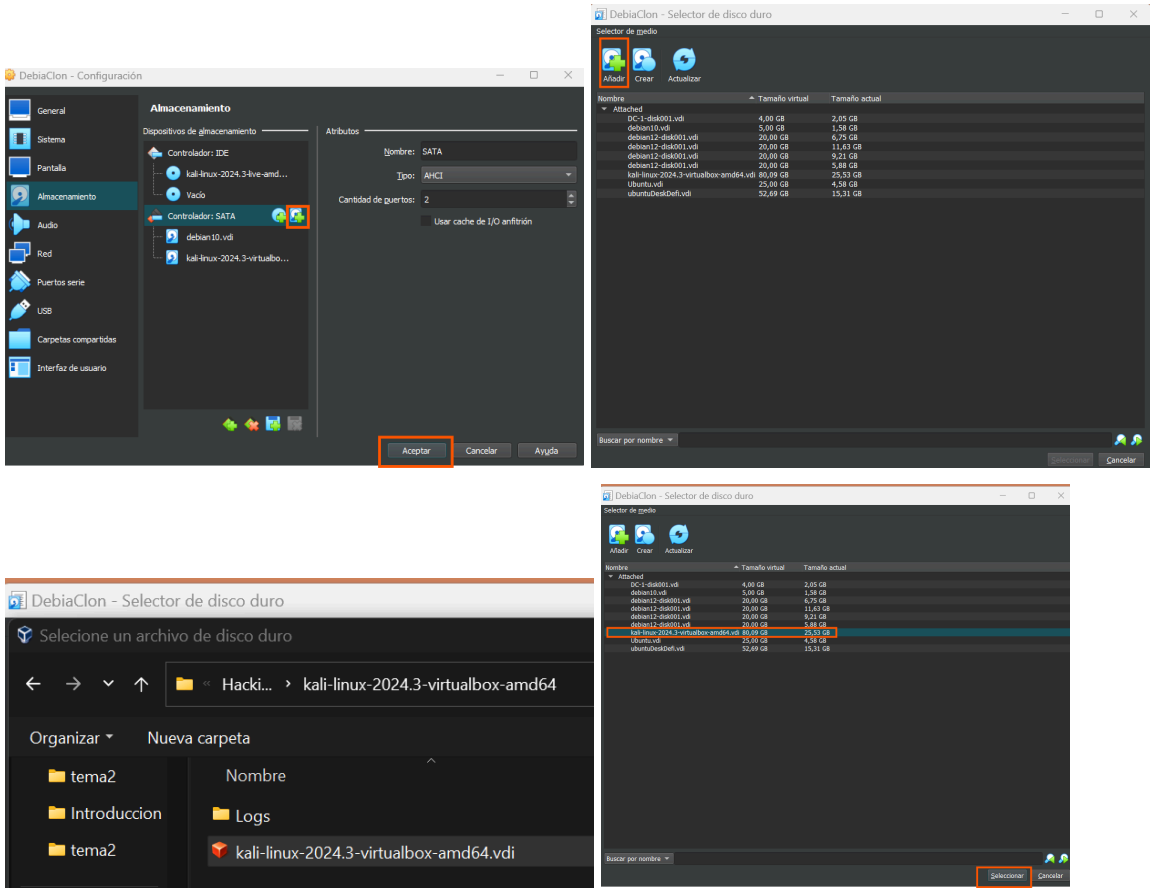


Se abrirá una ventana seleccionar Almacenamiento y en el área de Controlador: IDE seleccionamos el símbolo de cd, agregar un sistema Kali live que se usará como arranque y no inicialice el debian.

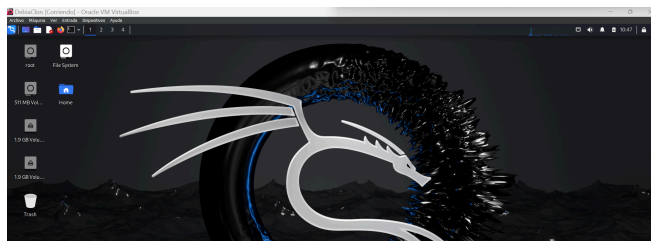
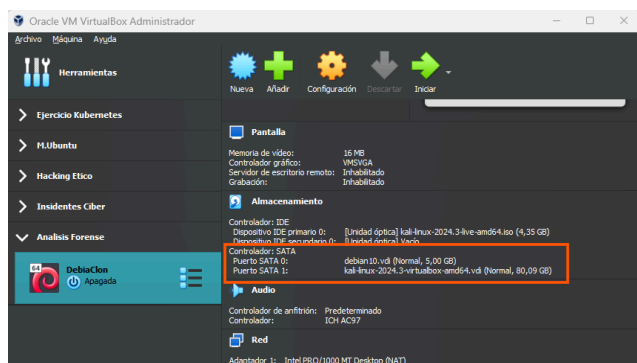




Agregamos un disco duro para la clonación se usará un kali; En el área de Controlador:SATA seleccionar Añadir disco duro



Ya estamos listos para comenzar con lo que nos pide.



índice

Técnica Clonación

Para esta técnica vamos a ver los discos que tiene la máquina, como es clonación es necesario que tenga un espacio de 5 o más Gb.

Para ello entramos como super usuario:

\$ sudo su

```

DebianClon [Corriendo] - Oracle VM VirtualBox
File Actions Edit View Help
(kali@kali)~$ sudo su
(root@kali)~/home/kali# fdisk -l

Disk /dev/sda: 5 GiB, 5368709120 bytes, 10485760 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: 0x9d280903

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 999423 997376 487M 83 Linux
/dev/sda2 1001470 10483711 9482242 4.5G 5 Extended
/dev/sda5 1001472 10483711 9482240 4.5G 8e Linux LVM

Disk /dev/sdb: 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

```

Visualizamos los discos que hay:

fdisk -l

Iniciamos la clonación con el siguiente comando:

dd if=/dev/sda of=/dev/sdb bs=1M conv=sync,noerror status=progress

Este comando se utiliza para clonar un disco (o partición) de un origen a un destino utilizando el programa dd.

- **if=/dev/sda:** Disco o partición de origen /dev/sda.
- **of=/dev/sdb:** Disco donde se va a clonar la información.

- **bs=1M:** Define el tamaño del bloque que dd va a leer/escribir a la vez. 1M significa que se leerán/escribirán bloques de 1 MiB (megabyte).
- **conv=sync,noerror:** Especifican el comportamiento de dd en caso de errores:
 - **sync:** Asegura que los bloques se llenen con ceros si hay errores de lectura, para mantener la alineación del bloque en el disco de destino.
 - **noerror:** Le indica a dd que continúe el proceso de clonación incluso si **encuentra errores de lectura en el disco de origen.**
- **status=progress:** Muestra el progreso de la clonación en tiempo real.

```
(root@kali)-[/home/kali]
# dd if=/dev/sda of=/dev/sdb bs=1M conv=sync,noerror status=progress
4933550080 bytes (4.9 GB, 4.6 GiB) copied, 10 s, 493 MB/s
5120+0 records in
5120+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 11.215 s, 479 MB/s
```

Calculando el hash

Verificamos que la clonación es efectiva tenemos que fijarnos en el tamaño del dispositivo o partición, este valor es la capacidad total en bytes del disco.

vamos a ver que tamaño tiene el disco que vamos a clonar.

fdisk -l

```
(root@kali)-[/home/kali]
# dd if=/dev/sda of=/dev/sdb bs=1M conv=sync,noerror status=progress
4933550080 bytes (4.9 GB, 4.6 GiB) copied, 10 s, 493 MB/s
5120+0 records in
5120+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 11.215 s, 479 MB/s

(root@kali)-[/home/kali]
# fdisk -l
Disk /dev/sda: 5 GiB, 5368709120 bytes, 10485760 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: 0x9d280903
```

Para comprobar la clonación y el disco que clonamos debe que tener la misma capacidad total de bytes para que el hash sea el mismo.

Para ello usaremos el siguiente comando

sha512sum /dev/sda

dd if=/dev/sdb count=10485760 bs=512 | sha512sum

Este comando se utiliza para verificar la integridad de los datos copiados.

- **dd if=/dev/sdb:** if es el archivo de entrada, que es el disco o partición de destino (/dev/sdb). Aquí lees el disco que se ha clonado.
- **count=1023410176 bs=512:** Esto le dice a dd que lea 1048576 bloques de tamaño 512 bytes cada uno (equivalente a 512 MiB).

- | **sha512sum**: La tubería | toma la salida de dd y la pasa al comando sha512sum, que calcula el hash SHA-512 del contenido leído.

```
(root@kali)-[/home/kali]
# sha512sum /dev/sda
b26c0b5944797be179aecf69dce998bc711ee33c566b9a82ee6ddc9ed0a1a2939741b468ed4d0253ecdd3c19f714385d069ea8d08
e9e9984e758f7e5e0c32f4d /dev/sda

(root@kali)-[/home/kali]
# dd if=/dev/sdb count=10485760 bs=512 | sha512sum
10485760+0 records in
10485760+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 21.9407 s, 245 MB/s
b26c0b5944797be179aecf69dce998bc711ee33c566b9a82ee6ddc9ed0a1a2939741b468ed4d0253ecdd3c19f714385d069ea8d08
e9e9984e758f7e5e0c32f4d -
```

Podemos ver que tiene el mismo hash.

Este comando es importante usar ya que el disco que usamos para la clonación es mucho mayor que el original y si usamos el siguiente comando

```
# sha512sum /dev/sda
```

```
# sha512sum /dev/sdb
```

Nos dará un hash diferente ya que estará comando los bytes del disco no usado:

```
(root@kali)-[/home/kali]
# sha512sum /dev/sda
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f
5134aaabaca5c30ae /dev/sda

(root@kali)-[/home/kali]
# sha512sum /dev/sdb
f1cd35212112fa357e255bdc911bfdd32e747d106ad0af3d4ea98338796bec1ecff072d93b7665cf9e904d78dcf7655aa294a1e5dcbc75b
66e16924feb586e15 /dev/sdb
```

índice

Técnica Imagen

Para esta técnica voy a crear una tabla de particiones en el disco donde guardaré las imágenes con el objetivo de tener más organización y se pueda acceder a él de la mejor manera. Este comando abre la utilidad fdisk para gestionar particiones en el disco

fdisk /dev/sdb

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

Welcome to fdisk (util-linux 2.40.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help):

Command (m for help): g

Created a new GPT disklabel (GUID: E57C3687-3A61-42C6-994D-33767868E07D).
The device contains 'dos' signature and it will be removed by a write command. See fdisk(8) man page and --wipe
option for more details.

Command (m for help): n
Partition number (1-128, default 1):
First sector (2048-167968716, default 2048):
Last sector, +/-sectors or +/-size[K,M,G,T,P] (2048-167968716, default 167966719): w
Last sector, +/-sectors or +/-size[K,M,G,T,P] (2048-167968716, default 167966719):

Created a new partition 1 of type 'Linux filesystem' and of size 80.1 GiB.
Partition #1 contains a ext2 signature.
Do you want to remove the signature? [Y]es/[N]o: y
The signature will be removed by a write command.

Command (m for help): w
```

Formateamos S

mkfs.ext4 /dev/sdb1

```
(root@kali)-[/home/kali]
# mkfs.ext4 /dev/sdb1
mke2fs 1.47.1 (20-May-2024)
Creating filesystem with 20995584 4k blocks and 5251072 inodes
Filesystem UUID: 183ee188-821c-48bd-be12-dae3b4d41170
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done

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

Montamos la partición en el directorio /mnt

```
(root@kali)-[/home/kali]
# mount /dev/sdb1 /mnt

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

Creó la imagen

dd if=/dev/sda of=/mnt/imagen-5g.dd bs=1M status=progress

```
(root@kali)-[/home/kali]
# dd if=/dev/sda of=/mnt/imagen-5g.dd bs=1M status=progress
4800380928 bytes (4.8 GB, 4.5 GiB) copied, 8 s, 600 MB/s
5120+0 records in
5120+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 8.77627 s, 612 MB/s
```

Veo los ficheros

```
# cd /mnt
```

```
# ls -lh
```

```
(root@kali)-[/mnt]
# ls -lh
total 5.1G
-rw-r--r-- 1 root root 5.0G Oct 20 12:04 imagen-5g.dd
drwx----- 2 root root 16K Oct 20 11:58 lost+found
```

Calculando el hash

Para calcular que la imagen y el disco tengan el mismo hash vamos a usar los siguientes comandos

```
# sha512sum imagen-5g.dd
```

```
# sha512sum /dev/sda
```

```
(root@kali)-[/mnt]
# sha512sum /dev/sda
b26c0b5944797be179aecf69dce998bc711ee33c566b9a82ee6ddc9ed0a1a2939741b468ed4d0253ecdd3c19f714385d069ea8d08
e9e9984e758f7e5e0c32f4d /dev/sda

(root@kali)-[/mnt]
# sha512sum imagen-5g.dd
b26c0b5944797be179aecf69dce998bc711ee33c566b9a82ee6ddc9ed0a1a2939741b468ed4d0253ecdd3c19f714385d069ea8d08
e9e9984e758f7e5e0c32f4d imagen-5g.dd
```

[índice](#)