

Práctica 5

Adquisición de Evidencias por la Red

Índice

Índice.....	2
Pasos Previos:.....	3
1. Creación de Máquinas Virtuales (VM):.....	3
a. Debian:.....	3
b. Kali Linux:.....	4
2. Configuración del Pendrive:.....	5
Clonado por Red (netcat):.....	6
1. Estación forense.....	6
2. Máquina con las evidencias.....	6
3. Estación forense.....	8
Clonado por Red (ssh):.....	9
1. Estación forense.....	9
2. Máquina con las evidencias.....	10
3. Estación forense.....	10
Evidencias Obtenidas:.....	11
1. Práctica 2 - Tema 2:.....	11
2. Práctica 5 - Tema 2:.....	12

Pasos Previos:

1. Creación de Máquinas Virtuales (VM):

a. Debian:

Configuramos la máquina virtual para que tenga 2GB de memoria Ram, 20 GB de disco duro, y una unidad óptica con un Kali Lite.

Usamos una ISO de Debian x64.

The screenshot displays the configuration window for a new virtual machine, divided into four main sections: General, Sistema, Almacenamiento, and Audio.

- General:** The 'Básico' tab is active. The name is 'forense_practica_2'. The type is 'Linux', subtype is 'Debian', and version is 'Debian (64-bit)'. A red arrow points to the version dropdown.
- Sistema:** The 'Aceleración' tab is active. The 'Memoria base' (base memory) is set to 2048 MB, indicated by a slider and a red arrow. The 'Orden de arranque' (boot order) shows 'Disquete' and 'Óptica' as bootable devices.
- Almacenamiento:** The 'Dispositivos' list shows three items: 'Controlador: IDE', 'Controlador: SATA', and 'Controlador: SCSI'. The 'SATA' controller is selected, and its attributes are shown on the right: 'Nombre: SATA', 'Tipo: AHCI', and 'Cantidad de puertos: 1'. The 'Usar cache de I/O anfitrión' checkbox is unchecked.
- Audio:** The 'Habilitar audio' checkbox is checked.

At the bottom of each section are buttons for 'Aceptar' (Accept), 'Cancelar' (Cancel), and 'Ayuda' (Help).

b. Kali Linux:

Configuramos la máquina virtual para que tenga 2GB de memoria Ram y 80 GB de disco duro.

Usamos una ISO de Kali Linux 2024.3 x64.

General

Básico Avanzado Descripción Cifrado de disco

Nombre: kali-linux-2024.2-virtualbox-amd64

Tipo: Linux

Subtype: Debian

Versión: Debian (64-bit)

Sistema

Placa base Procesador Aceleración

Memoria base: 2048 MB

Orden de arranque: ☒ Disco duro ☒ Óptica

Almacenamiento

Dispositivos

Controlador: IDE

Vacío

Controlador: SATA

kali-linux-2024.2-virtualbox-amd64.v...

Atributos

Disco duro: Puerto SATA 0

☐ Unidad de estado sólido

☐ Conectable en caliente

Información

Tipo (formato): Normal (vdi)

Virtual size: 80,09 GB

Actual size: 14,71 GB

Detalles de almacenamiento: Almacenamiento diferen..

Ubicación: C:\Users\Fortuna_457\D...

Conectado a: kali-linux-2024.2-virtual...

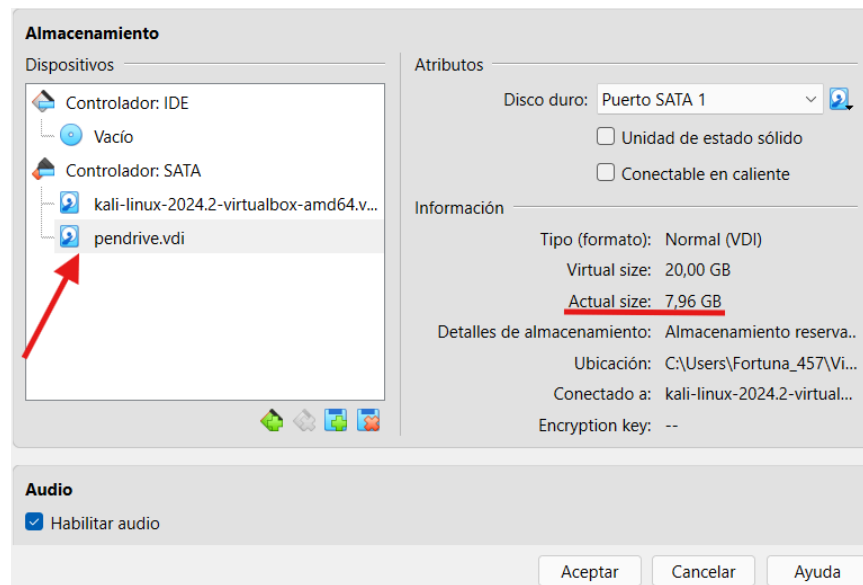
Encryption key: --

Audio

☒ Habilitar audio

2. Configuración del Pendrive:

Utilizaremos el mismo “pendrive” de la práctica 3 del tema 2.



Clonado por Red (netcat):

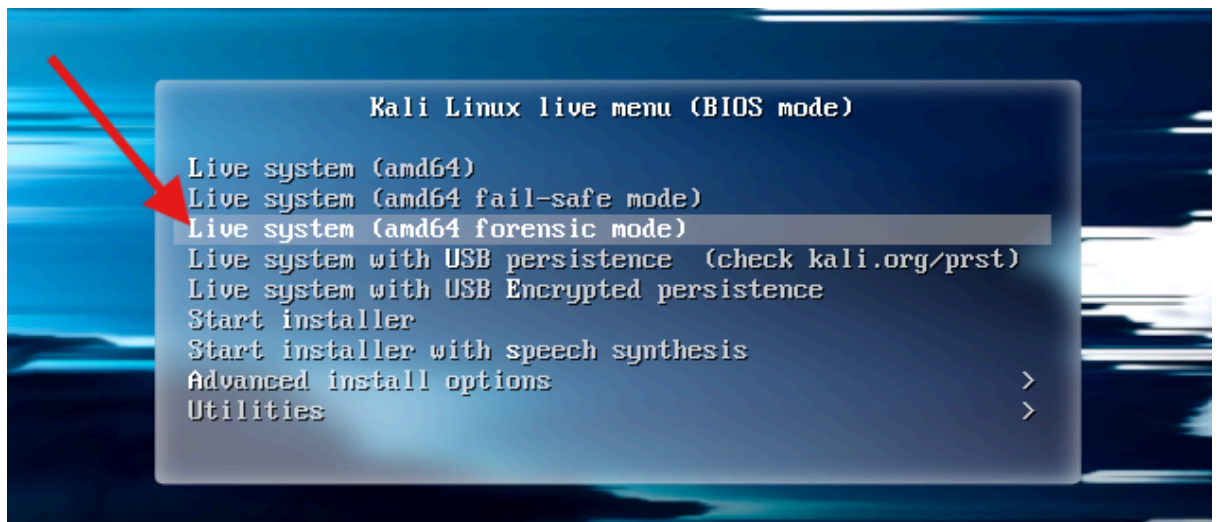
1. Estación forense.

Abrimos el puerto 5000 de nuestra estación forense con el comando nc, para que esté en escucha ante cualquier comunicación.

```
File Actions Edit View Help
(kali@kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$ sudo nc -l -p 5000 > imagen.dd
[sudo] password for kali:
```

2. Máquina con las evidencias.

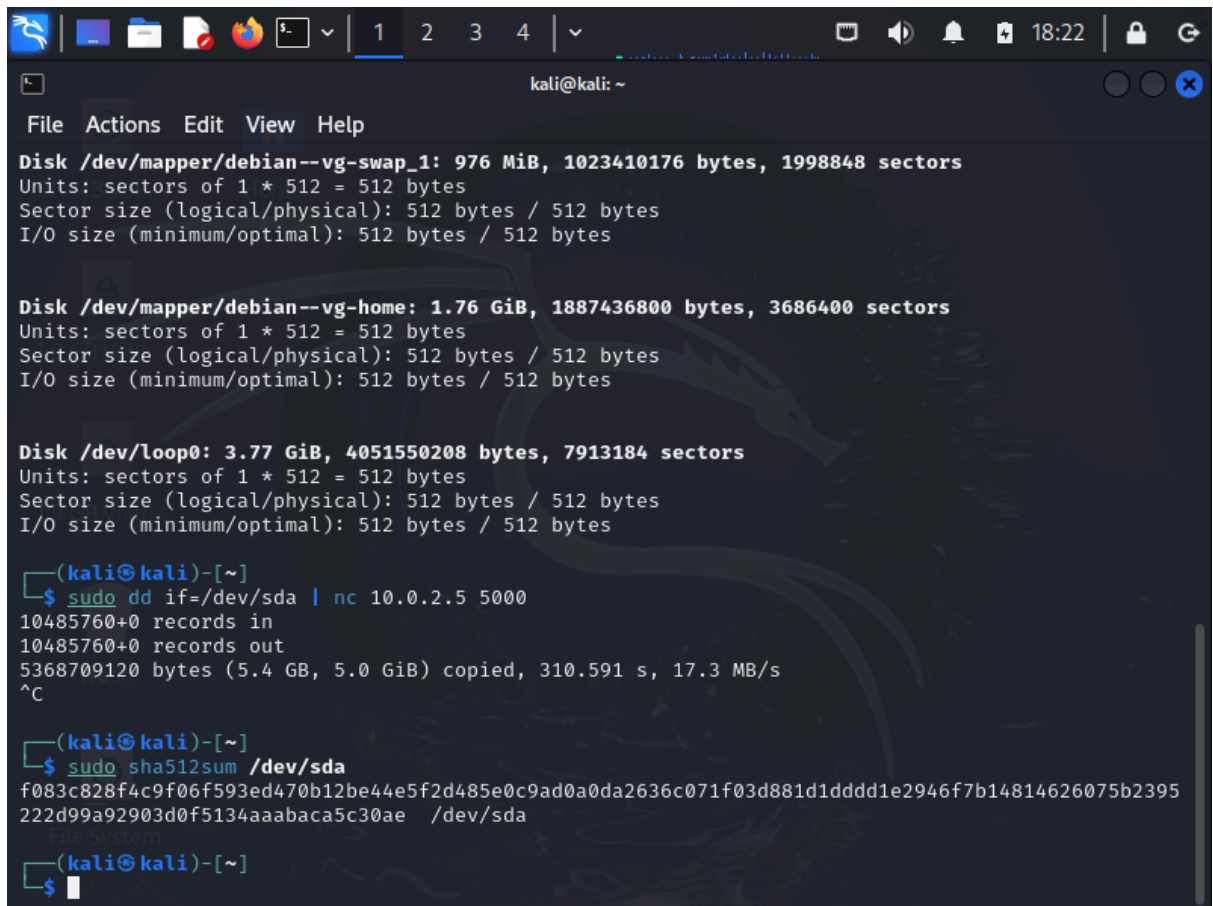
Una vez arrancamos la máquina con las evidencias, nos preguntará con qué modo queremos hacerlo. Seleccionamos el **Live system (amd64 forensic mode)**. Para así no contaminar las evidencias del disco.



Una vez dentro, hacemos un **fdisk -l** para ver la estructura de los discos y sus particiones.

Y hacemos una imagen de disco en **/dev/sda**, y el resultado lo enviamos a través de netcat con el comando **nc** a la IP de nuestra estación forense.

Por último, calculamos el hash del disco.



```
kali@kali: ~  
File Actions Edit View Help  
Disk /dev/mapper/debian--vg-swap_1: 976 MiB, 1023410176 bytes, 1998848 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
  
Disk /dev/mapper/debian--vg-home: 1.76 GiB, 1887436800 bytes, 3686400 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
  
Disk /dev/loop0: 3.77 GiB, 4051550208 bytes, 7913184 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
  
(kali@kali)-[~]  
$ sudo dd if=/dev/sda | nc 10.0.2.5 5000  
10485760+0 records in  
10485760+0 records out  
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 310.591 s, 17.3 MB/s  
^C  
  
(kali@kali)-[~]  
$ sudo sha512sum /dev/sda  
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395  
222d99a92903d0f5134aaabaca5c30ae /dev/sda  
  
(kali@kali)-[~]  
$
```

Hash:

```
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881  
d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae  
/dev/sda
```

3. Estación forense.

Una vez recibida la imagen del disco a través del puerto 5000, cerramos la conexión haciendo **ctrl+C**.

Y calculamos el hash de la evidencia obtenida, para así compararlo con el hash obtenido en la máquina con las evidencias.

```
(kali㉿kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$ sudo sha512sum imagen.dd
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1ddd1e2946f7b14814626075b2395222d99a92903d0f5134a
aabaca5c30ae  imagen.dd
(kali㉿kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$
```

Hash:

**f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881
d1ddd1e2946f7b14814626075b2395222d99a92903d0f5134aabaca5c30ae
imagen.dd**

Clonado por Red (ssh):

1. Estación forense.

En el archivo de configuración:

```
sudo nano /etc/ssh/sshd_config
```

Descomentamos la opción:

```
PermitRootLogin yes
```

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

Reiniciamos el servicio de ssh.

```
(kali㉿kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$ sudo systemctl status ssh.service
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Thu 2024-11-07 14:02:57 EST; 5s ago
     Invocation: e534da77104c4cc682a92557de747bd9
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 48937 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 48938 (sshd)
      Tasks: 1 (limit: 2272)
     Memory: 1.3M (peak: 1.6M)
        CPU: 27ms
    CGroup: /system.slice/ssh.service
            └─48938 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 07 14:02:57 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Nov 07 14:02:57 kali sshd[48938]: Server listening on 0.0.0.0 port 22.
Nov 07 14:02:57 kali sshd[48938]: Server listening on :: port 22.
Nov 07 14:02:57 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(kali㉿kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$
```

2. Máquina con las evidencias.

En la máquina con las evidencias, hacemos un imagen del disco, cuyo resultado mandamos por ssh a la estación forense.

Y sacamos el hash del disco de la máquina con las evidencias.

```
(kali@kali)-[~]
$ sudo dd if=/dev/sda | ssh kali@10.0.2.5 "dd of=/media/kali/Nuevo\ vol/practica_5-tema_2/imagen2.dd"
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
ED25519 key fingerprint is SHA256:dbCxZGONhKUZPBPySX0s+0R4Wi69YBv2la9+LORWQOg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.5' (ED25519) to the list of known hosts.
kali@10.0.2.5's password:
10485760+0 records in
10485760+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 413.905 s, 13.0 MB/s
10485760+0 records in
10485760+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 405.427 s, 13.2 MB/s

(kali@kali)-[~]
$ sudo sha512sum /dev/sda
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134a
aabaca5c30ae /dev/sda

(kali@kali)-[~]
$
```

Hash:

```
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881
d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aabaca5c30ae
/dev/sda
```

3. Estación forense.

De vuelta en nuestra estación forense. Una vez hayamos recibido la imagen del disco, calculamos el hash y lo comparamos con el conseguido en la máquina con las evidencias.

```
(kali@kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$ ls
imagen2.dd imagen.dd

(kali@kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$ sudo sha512sum imagen2.dd
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134
aabaca5c30ae imagen2.dd

(kali@kali)-[/media/kali/Nuevo vol/practica_5-tema_2]
$
```

Hash:

```
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881
d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aabaca5c30ae
imagen2.dd
```

Evidencias Obtenidas:

1. Práctica 2 - Tema 2:

Clonado de disco:

```

kali@kali: ~
File Actions Edit View Help

Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/debian--vg-swap_1: 976 MiB, 1023410176 bytes, 1998848 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/debian--vg-home: 1.76 GiB, 1887436800 bytes, 3686400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop0: 3.77 GiB, 4051550208 bytes, 7913184 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

(kali@kali)-[~]
$ dd if=/dev/sda of=/dev/sdb bs=1M conv=sync,noerror status=progress
dd: failed to open '/dev/sda': Permission denied

(kali@kali)-[~]
$ sudo dd if=/dev/sda of=/dev/sdb bs=1M conv=sync,noerror status=progress
5162139648 bytes (5.2 GB, 4.8 GiB) copied, 10 s, 516 MB/s
5120+0 records in
5120+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 10.4931 s, 512 MB/s

(kali@kali)-[~]
$ dd if=/dev/sdb count=10485760 bs=512 | sha512sum
dd: failed to open '/dev/sdb': Permission denied
cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a53
8327af927da3e -

(kali@kali)-[~]
$ sudo 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, 26.8028 s, 200 MB/s
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae -

(kali@kali)-[~]
$

```

Hash:

f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae

Imagen de disco:

```

File Actions Edit View Help
(kali@kali)~$ sudo dd if=/dev/sda of=/mnt/imagen.dd
10485760+0 records in
10485760+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 21.0984 s, 254 MB/s

(kali@kali)~$ sha512sum /mnt/imagen.dd
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae /mnt/imagen.dd

(kali@kali)~$ sha512sum /dev/sda
sha512sum: /dev/sda: Permission denied

(kali@kali)~$ sudo sha512sum /dev/sda
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae /dev/sda

(kali@kali)~$

```

Hash:

f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae /mnt/imagen.dd

2. Práctica 5 - Tema 2:

netcat:

```

(kali@kali)~/media/kali/Nuevo vol/practica_5-tema_2$ sudo sha512sum imagen.dd
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae imagen.dd

(kali@kali)~/media/kali/Nuevo vol/practica_5-tema_2$

```

Hash:

f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae imagen.dd

ssh:

```

(kali@kali)~/media/kali/Nuevo vol/practica_5-tema_2$ ls
imagen2.dd imagen.dd

(kali@kali)~/media/kali/Nuevo vol/practica_5-tema_2$ sudo sha512sum imagen2.dd
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae imagen2.dd

(kali@kali)~/media/kali/Nuevo vol/practica_5-tema_2$

```

Hash:

f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1dddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae imagen2.dd