PRÁCTICA 5: ADQUISICIÓN DE EVIDENCIAS POR LA RED.

En caso de no disponer del hardware adecuado se plantea la posibilidad de realizar la extracción de evidencias a través de la red.

En principio contamos con dos equipos, el equipo implicado y la estación forense.

Primero se procederá a preparar la estación forense, lo único necesario es un servidor ssh y un usuario.

En la **máquina con las evidencias** se cargará una distribución live como puede ser caine, kali, clonezilla,... y se ejecutará el siguiente comando:

```
dd if=/dev/sdaX  | ssh usuario@estacion_forense "dd of=/ruta/imagen.raw"
dd if=/dev/sdaX | gzip -1 - | ssh usuario@estacion_forense "dd of=/ruta/imagen.gz"
```

Otra posibilidad si no podemos disponer de un servidor ssh es utilizar la herramienta netcat, aunque es menos aconsejable. En la estación forense se debe ejecutar el siguiente comando:

```
nc -l -p 5000 > /ruta/imagen_sda1.dd
```

El comando anterior ejecuta la herramienta netcat, se prepara para recibir conexiones (-l) en el puerto 5000 (-p 5000) y redirige la salida a un fichero llamado imagen.dd (> imagen.dd). es posible establecer multiples ficheros de salida con el comando *tee:*

En la máquina a analizar se ejecuta la siguiente línea:

```
dd if=/dev/sda1 | nc estacion_forense 5000
```

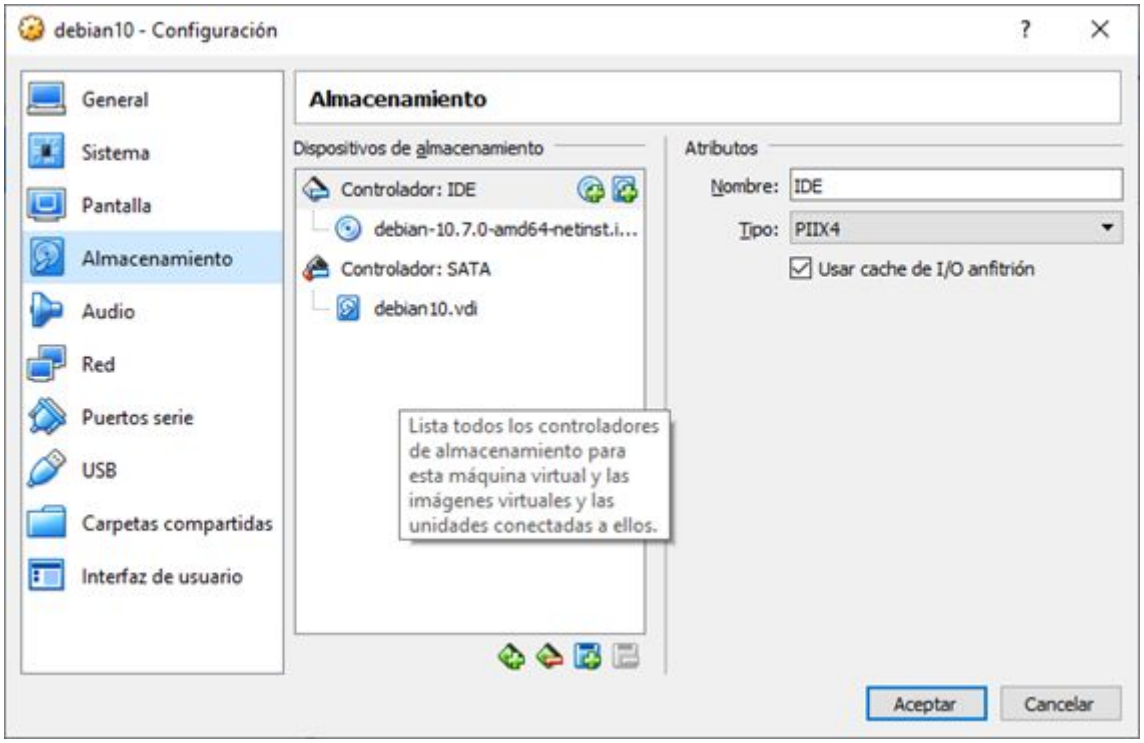
Objetivos principales de la práctica:

- **Recopilación de pruebas cuando no contamos con acceso físico a los discos de la máquina y/o con el cableado adecuado.**

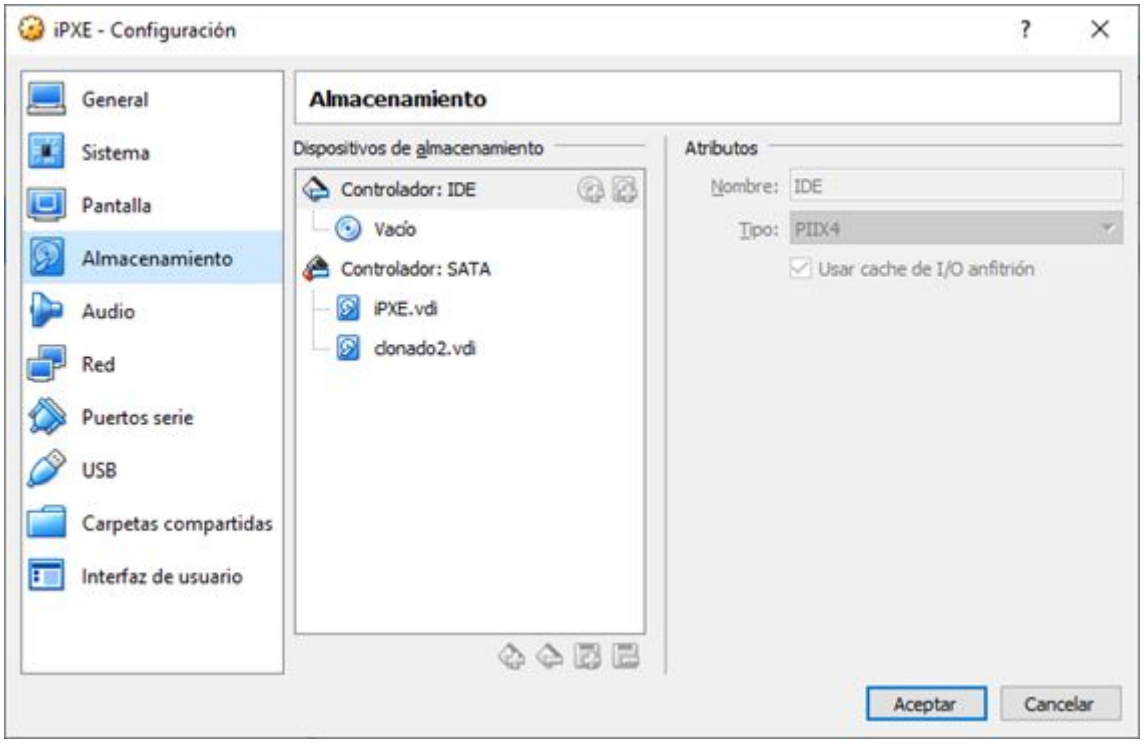
Se pide:

- Crear dos máquinas virtuales: la máquina de la práctica 2 (debian) hará las veces de equipo con evidencias y una nueva máquina linux que actuará como estación de trabajo forense.
- Conecta a la estación de trabajo forense un disco duro virtual que hará las veces de flash drive.
    - Arranca el SO y prepara el disco para ser utilizado (particionado, formateo y montado)
- Realizar la extracción de las evidencias digitales volátiles (particiones) mediante SSH y mediante NETCAT
    - Calcula los HASH de las evidencias extraídas (comando sha512sum) y comprueba que coinciden los HASHES de sda1 y sda5 con los obtenidos en la práctica 2.
- Documenta todo el proceso anterior.

Máquina con evidencias



Estación de trabajo forense (linux)



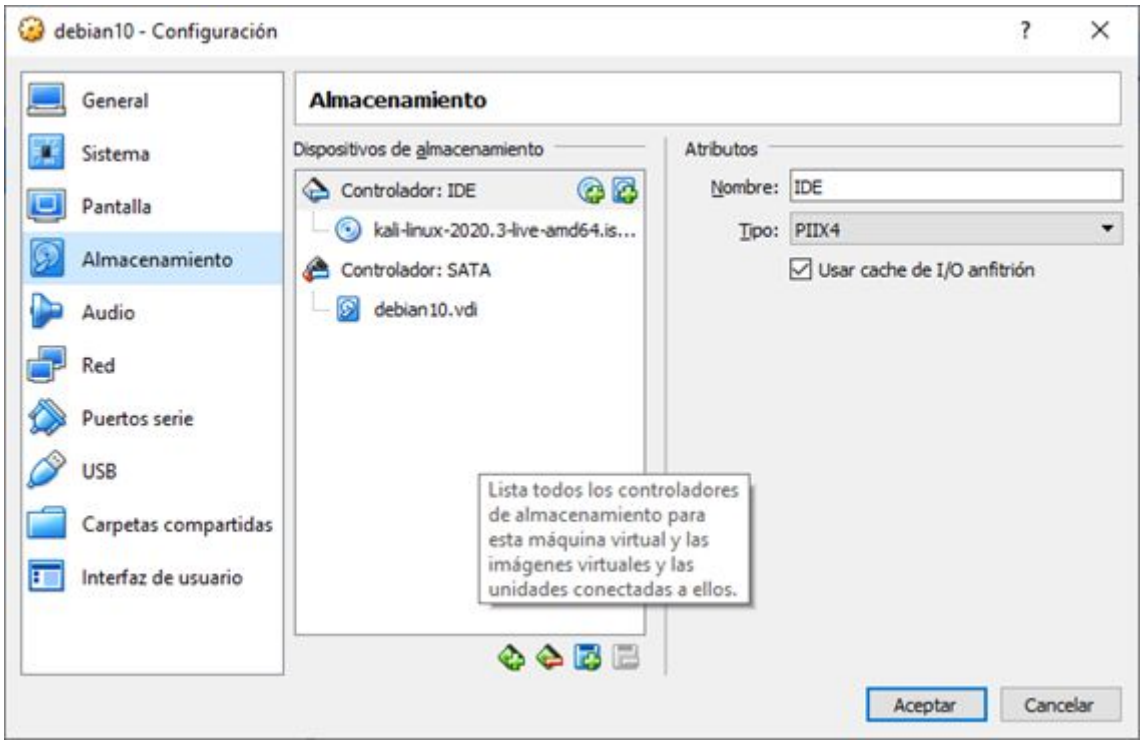
Preparación del disco, apertura del puerto NETCAT y recepción de las evidencias por la red

```
   p   primaria (0 primaria(s), 0 extendida(s), 4 libre(s))
   e   extendida (contenedor para particiones lógicas)
Seleccionar (valor predeterminado p): p
Número de partición (1-4, valor predeterminado 1):
Primer sector (2048-16777215, valor predeterminado 2048):
Último sector, +/-sectores o +/-tamaño{K,M,G,T,P} (2048-16777215, valor predeterminado 16777215):

Crea una nueva partición 1 de tipo 'Linux' y de tamaño 8 GiB.

Orden (m para obtener ayuda): w
Se ha modificado la tabla de particiones.
Llamando a ioctl() para volver a leer la tabla de particiones.
Se están sincronizando los discos.

root@debian:~# mkfs.
mkfs.bfs     mkfs.cramfs  mkfs.ext2    mkfs.ext3    mkfs.ext4    mkfs.minix
root@debian:~# mkfs.ext4 /dev/sdb1
mke2fs 1.44.5 (15-Dec-2018)
Creating filesystem with 2096896 4k blocks and 524288 inodes
Filesystem UUID: b88f813b-7130-4d23-ba80-45140dd5640a
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

root@debian:~#
root@debian:~#
root@debian:~# mount /dev/sdb1 /mnt
root@debian:~# nc -l -p 5000 > /mnt/imagen.dd
root@debian:~# cd /mnt/
root@debian:/mnt# sha512sum imagen.dd
c8cdd58e34a5f7fe26d1a84e00db61fb7b33a70f94b536e4ebdc9bdf54e2b23add83a6a2d0e653055515186b6024318726ee
4cb2c39a97b9b7ffbb738b1226ce  imagen.dd
root@debian:/mnt# _
```

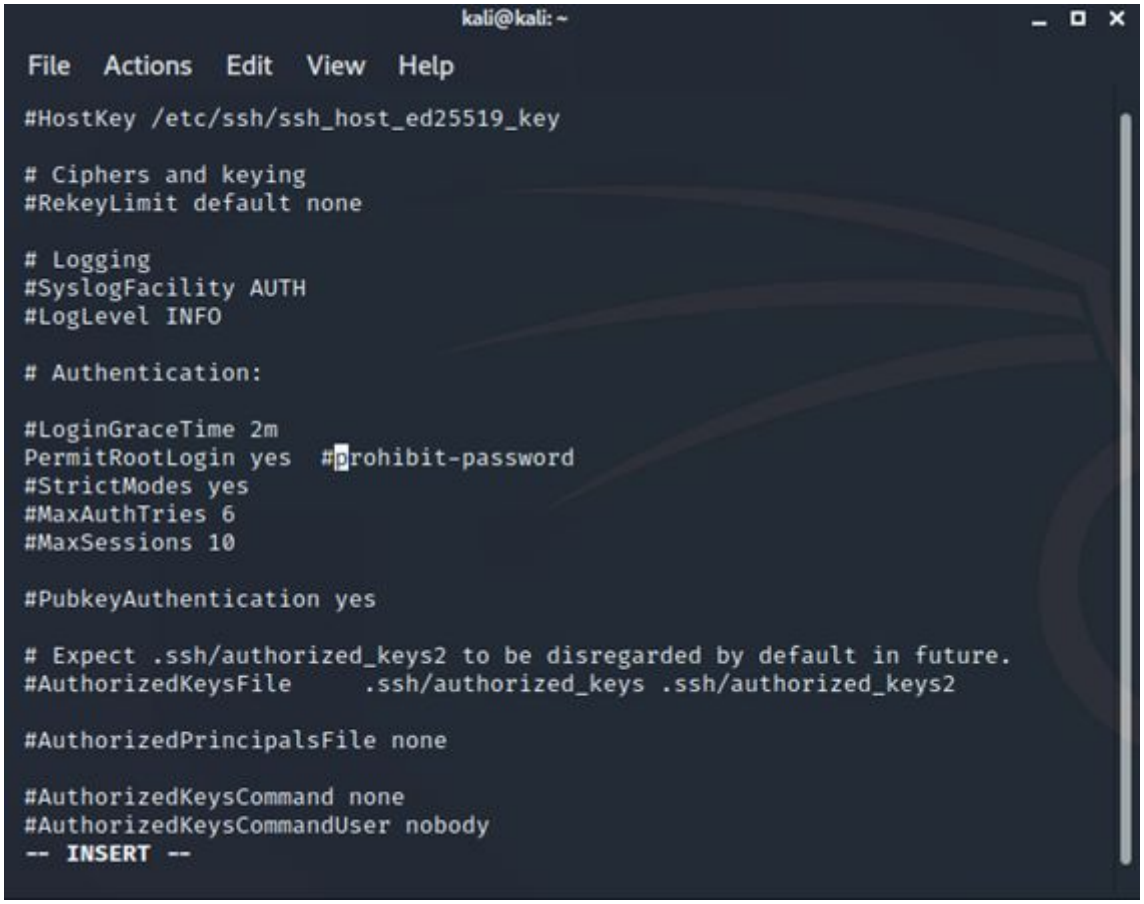
Envío de la evidencias desde el equipo implicado

```
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/mapper/debian--vg-root: 1.8 GiB, 1941962752 bytes, 3792896 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-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: 1.8 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
~ # dd if=/dev/sda1 | nc 192.168.11.141 5000
997376+0 records in
997376+0 records out
~ # sha512sum /dev/sda1
c8cdd58e34a5f7fe26d1a84e00db61fb7b33a70f94b536e4ebdc9bdf54e2b23add83a6a2d0e653055515186b6024318726ee
4cb2c39a97b9b7ffbb738b1226ce  /dev/sda1
~ #
```

Máquina con evidencias



Configuración de SSH en equipo implicado para permitir acceso como ROOT



Clonado mediante comando SSH