

450 - CIBERSEGURIDAD

Primeros pasos en análisis forense

Aprende a crear una imagen exacta de un disco de prueba para investigar un incidente sin tocar el original.



NIVEL
Avanzado

TIEMPO
45 min

CATEGORÍA
Ciberseguridad

WEB
soporteinformatico360.com

Cuando un equipo se ve comprometido, lo primero es no alterar las pruebas. El análisis forense empieza por hacer una copia exacta del disco y trabajar siempre sobre la copia. Aquí lo practicas en tu laboratorio.

■ Qué necesitas

- ✓ Ubuntu de laboratorio o una máquina virtual
- ✓ Un disco o USB de prueba, solo tuyo
- ✓ Permiso: equipos y datos propios únicamente

■ Paso a paso

01

Monta tu laboratorio

Trabaja en una máquina virtual aislada con un USB o disco de prueba que puedas sacrificar.



02

Identifica el disco

Lista los discos del sistema para saber cuál es el de prueba. Confúndete aquí y borrarás lo que no debes.

Terminal

```
$ lsblk
$ sudo fdisk -l
$
```

03

Crea la imagen exacta

Copia todo el disco de prueba a un archivo imagen, bloque a bloque, sin modificar el original.

Terminal

```
$ sudo dd if=/dev/sdX of=prueba.img
bs=4M status=progress
$
```

04

Calcula su huella

Genera una suma de comprobación para demostrar que la copia es idéntica y no se ha tocado.

```
Terminal
$ sha256sum prueba.img
$
```

05

Trabaja solo sobre la copia

Monta la imagen en modo solo lectura para explorar los archivos sin alterar las pruebas.

```
Terminal
$ sudo mount -o ro,loop prueba.img /mnt/caso
$
```

06

Documenta cada paso

Anota qué hiciste, cuándo y con qué comandos. En forense, el orden y las notas son tan importantes como los datos.



■ Consejos

CONSEJO 1

La regla de oro: nunca trabajes sobre el original, siempre sobre una copia verificada con su huella.

CONSEJO 2

Herramientas como Autopsy te ayudan a explorar la imagen de forma visual y ordenada.

CONSEJO 3

Si una empresa sufre un incidente real, que no apague ni formatee: avísanos antes de tocar nada.



Importante: Analiza solo equipos y datos tuyos o con permiso por escrito. Acceder a información de dispositivos ajenos sin autorización es un delito.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. En taller, a domicilio en Madrid o por asistencia remota.

910 117 112
sosporte@soporteinformatico360.com
soporteinformatico360.com