CLONACIÓN DE DISCOS Y CADENA DE CUSTODIA

¿Qué es una clonación?

La clonación de discos es el proceso de copiar perfectamente cada bit de información de un disco duro de un equipo o dispositivo electrónico a otro disco.

¿Qué es una imagen de disco?

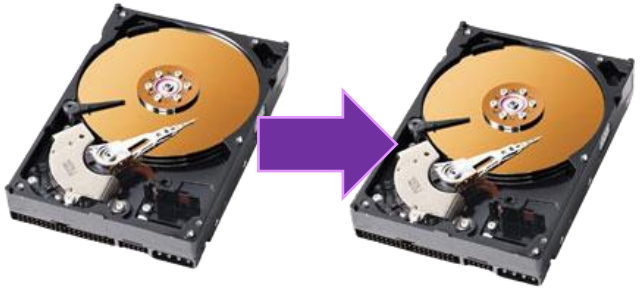
La creación de imágenes de disco es el proceso de realizar una copia de respaldo o de archivo de todo el contenido de un disco duro. Es un archivo de almacenamiento que contiene todos los datos almacenados en el disco duro de origen y la información necesaria para iniciar el sistema operativo. Sin embargo, la imagen del disco debe volcarse mediante software al disco duro para que funcione (útil para transferir).

¿Qué necesito para hacer una clonación?

Dependerá del tipo de clonación que vayamos a realizar de los tipos principales que existen, estos son:

- Clonación mediante **hardware**
- Clonación mediante **software**

Cuentan con diferencias pero el resultado será una **copia exacta** de los datos disponibles en la fuente de datos usada como origen de datos.



Clonación mediante **HARDWARE**

Ventajas:

- Multiples clonación paralelas
- Velocidades de clonación elevadas en equipos profesionales
- Cifrado del disco destino
- Cálculo de hash veloz
- Duplicación 1:2
- Etc

USBDUPE17

1:7 Standalone USB Duplicator and Eraser - for USB Flash Drives

Duplicate or erase up to seven USB flash drives, without connecting to a computer

Your price

$865.99USD

In stock

US: 49 | CA: 1

Add to ca

TABLEAU T3IU FORENSIC SATA IMAGING BAY

$319.99

Add to Cart

Add to Quote

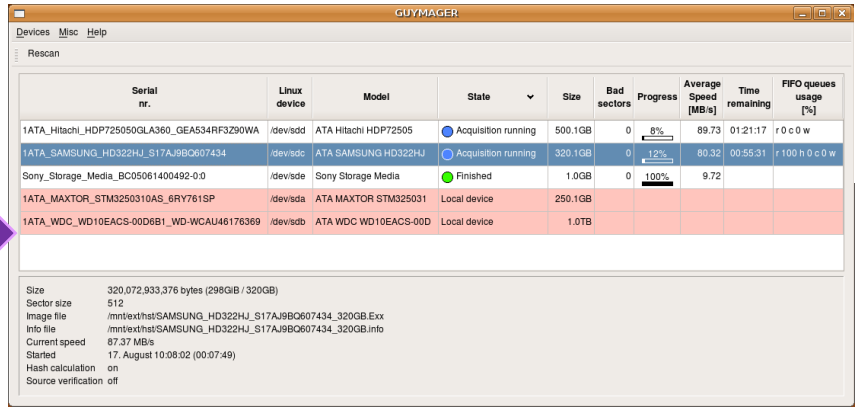
Duplicadora Ditto DX Forensic

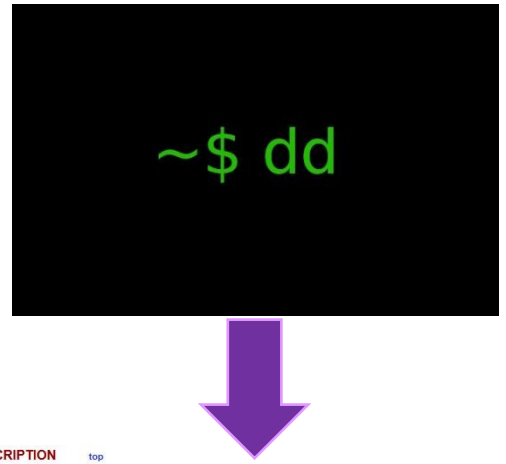
Duplicadora Forensic Talon Ultimate

Clonación mediante **SOFTWARE**

Ventajas:

- Versatilidad
- Precio
- Fuentes de información públicas
- Personalización
- Etc





DESCRIPTION top

Copy a file, converting and formatting according to the operands.

bs=BYTES
read and write up to BYTES bytes at a time (default: 512); overrides ibs and obs

cbs=BYTES
convert BYTES bytes at a time

conv=CONVS
convert the file as per the comma separated symbol list

count=N
copy only N input blocks

ibs=BYTES
read up to BYTES bytes at a time (default: 512)

if=FILE
read from FILE instead of stdin

CADENA DE **CUSTODIA**

¿Qué es?

La cadena de custodia es el procedimiento, oportunamente documentado, que **permite constatar el origen, autenticidad e integridad de una prueba digital**, indiciaria o demostrativa, de un hecho relevante para el proceso judicial, desde que es encontrada e intervenida hasta que se aportan al proceso adquiriendo capacidad probatoria.

CLAVE: CONSTATAR INTEGRIDAD DE LOS DATOS

ELEMENTO CENTRAL DE CUMPLIMIENTO:

Un ***hash*** o **función *hash*** es cualquier función matemática utilizada para mapear datos de tamaño arbitrario a un conjunto de datos de tamaño fijo.

Aplicada una función ***hash*** a un disco, una imagen o un archivo nos devolverá un conjunto de caracteres de tamaño fijo y dependiente del tipo de función elegida que identifican inequívocamente a dicho archivo.

¿Qué elementos llevamos hasta ahora?

- Clonadoras hardware
- Clonadoras software
- Imagen de disco
- Hash

Agreguemos 2 elementos para apuntalar la cadena de custodia

Elemento **hardware**:

- Bloqueadores de escritura

Elemento **humano**:

- Notarios

CONTINUAMOS EN EL SIGUIENTE CAPÍTULO

Ejemplo de proceso de clonación

Clonación por **software**:

Existen multitud de distribuciones específicas para tareas de peritaje forense, e incluso “dd” una de las principales herramientas de clonación es estandar en los sistemas Unix-like.

Usaremos **dd** como ejemplo

```
ubuntu@ubuntu:~$ sudo dd if=/dev/sdb bs=2048 count=11224576 conv=noerror|pv -s 21G|sudo dd of=/dev/sda
11224576+0 records inMiB/s] [=============================================================>] 101% ETA 0:00:00
11224576+0 records out
22987931648 bytes (23 GB, 21 GiB) copied, 1238.43 s, 18.6 MB/s
21.4GiB 0:20:38 [17.7MiB/s] [=============================================================>] 101%
44898304+0 records in
44898304+0 records out
22987931648 bytes (23 GB, 21 GiB) copied, 1238.7 s, 18.6 MB/s
ubuntu@ubuntu:~$ sudo fdisk -l /dev/sdb
Disk /dev/sdb: 30 GiB, 32212254720 bytes, 62914560 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
Disklabel type: dos
Disk identifier: 0xfca79835

Device     Boot   Start      End  Sectors  Size Id Type
/dev/sdb1  *       2048  1026047  1024000  500M  7 HPFS/NTFS/exFAT
/dev/sdb2       1026048 44898303 43872256 20.9G  7 HPFS/NTFS/exFAT
ubuntu@ubuntu:~$ sudo fdisk -l /dev/sda
Disk /dev/sda: 60 GiB, 64424509440 bytes, 125829120 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
Disklabel type: dos
Disk identifier: 0xfca79835

Device     Boot   Start      End  Sectors  Size Id Type
/dev/sda1  *       2048  1026047  1024000  500M  7 HPFS/NTFS/exFAT
/dev/sda2       1026048 44898303 43872256 20.9G  7 HPFS/NTFS/exFAT
ubuntu@ubuntu:~$
```