MODULO 2

Instructor: John H. Pérez C.

Análisis práctico de los fundamentos y las posibles dificultades de un análisis informático forense

INFORMÁTICA FORENSE

- **Análisis practico**

INFORMÁTICA FORENSE

- **Dificultades de un análisis**

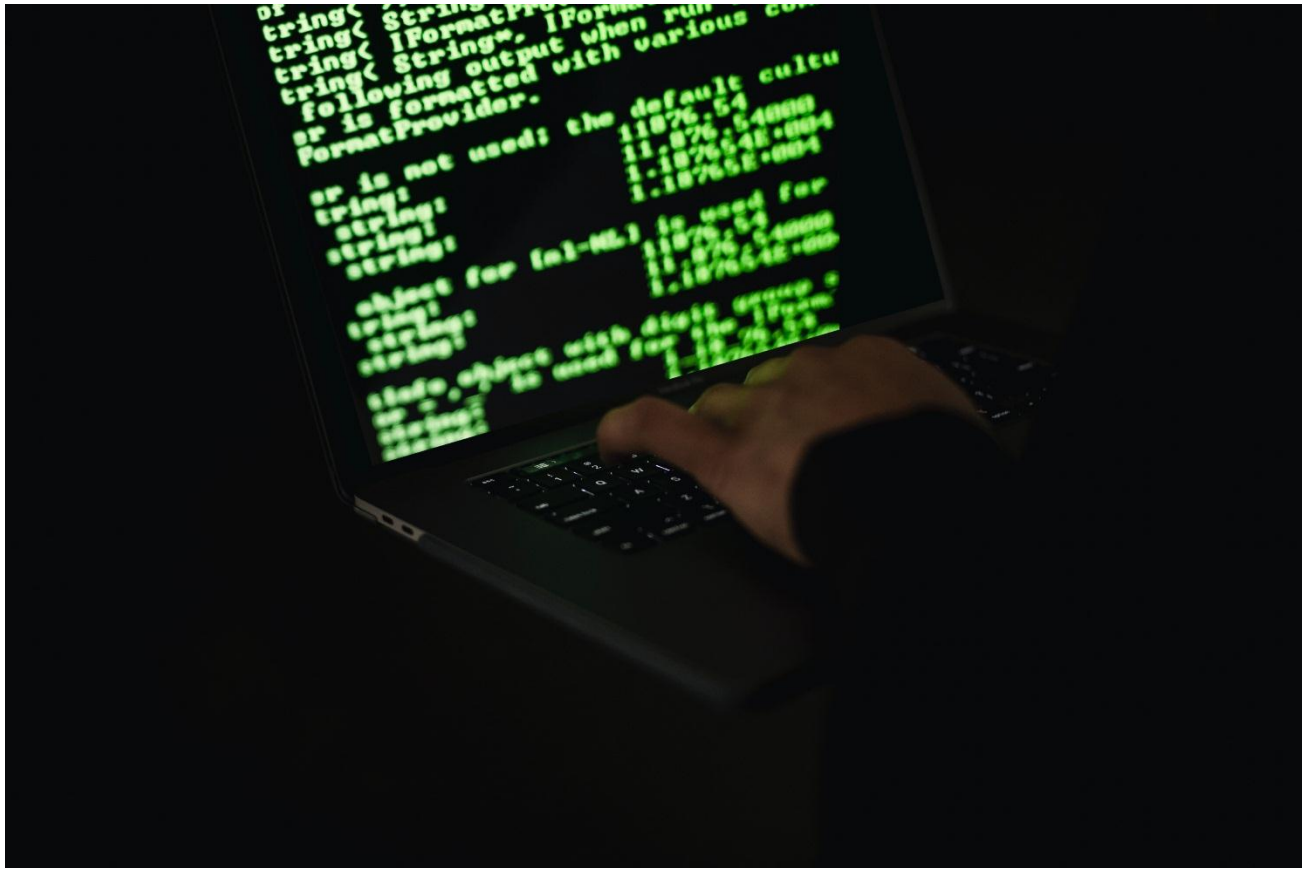
INFORMÁTICA FORENSE

- **Análisis practico**
- **Dificultades de un análisis**

2.1
Analizando los fundamentos forenses.

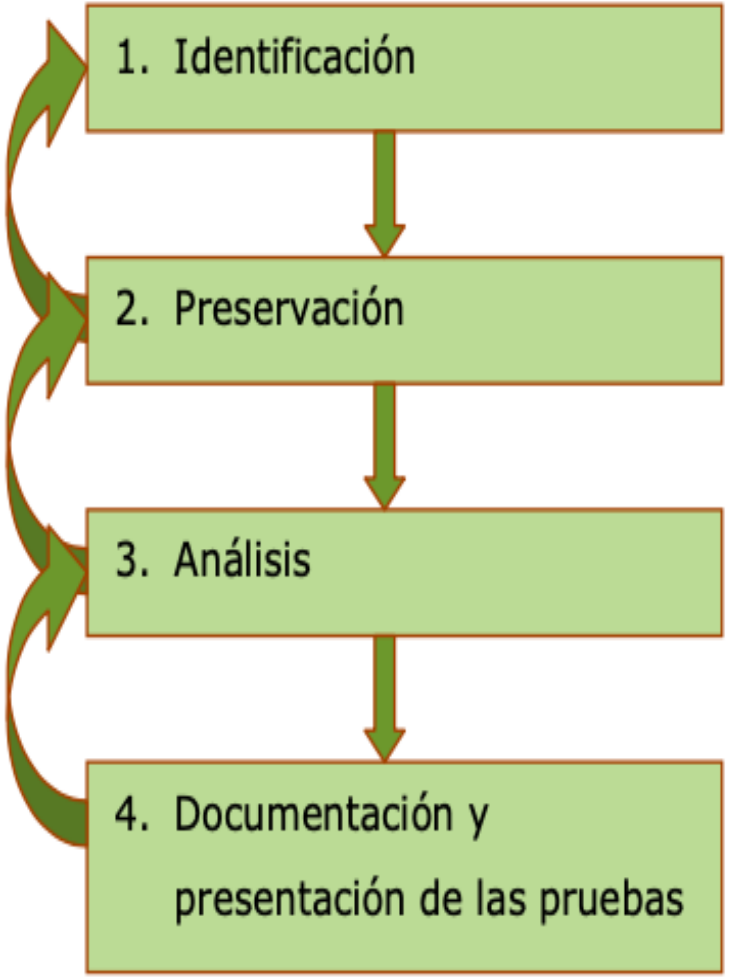
INFORMÁTICA FORENSE

INFORMÁTICA FORENSE

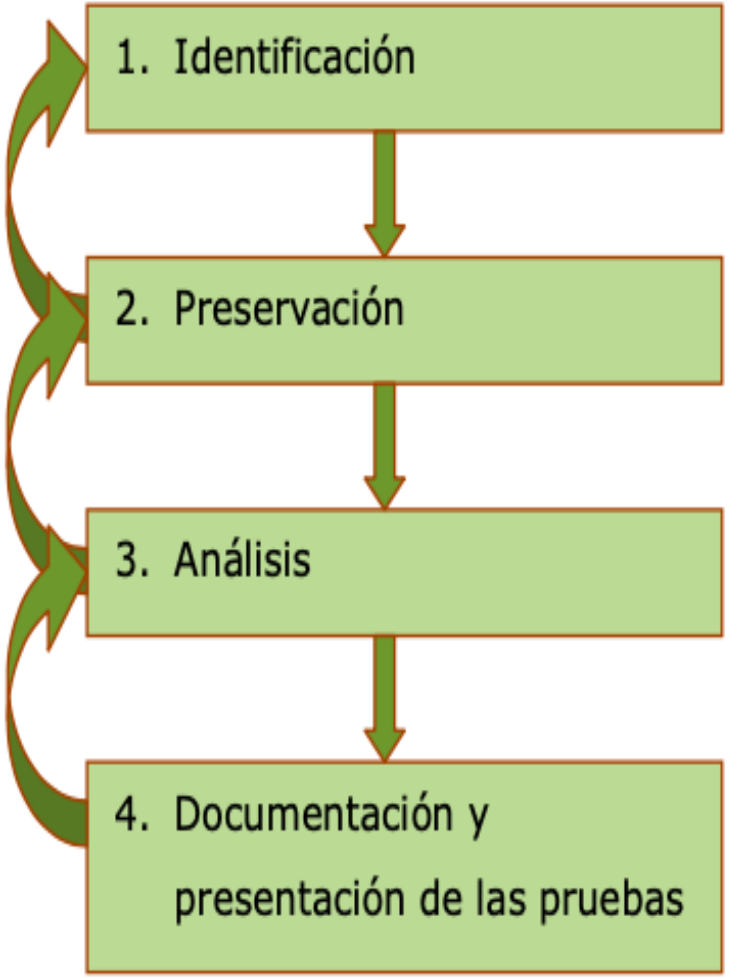


INFORMÁTICA FORENSE

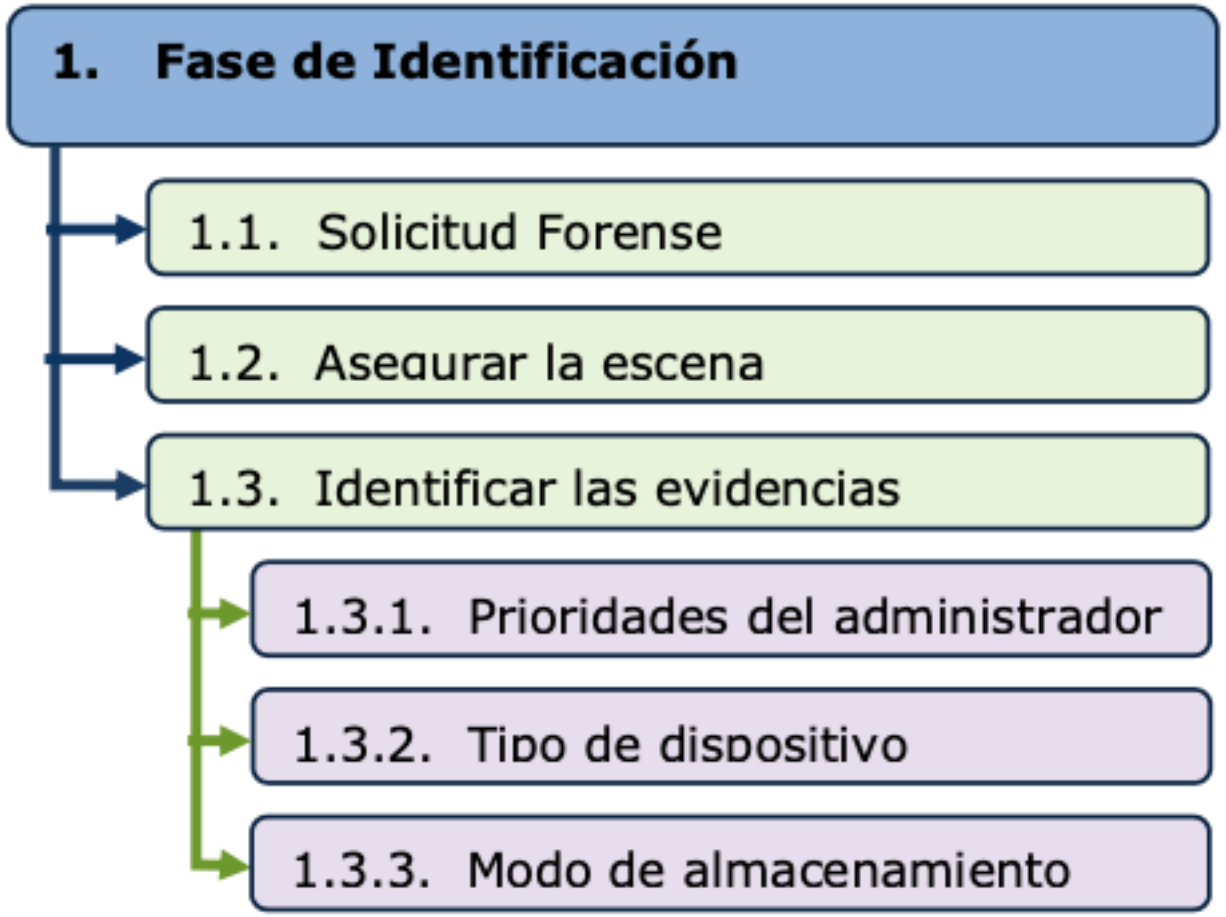
INFORMÁTICA FORENSE



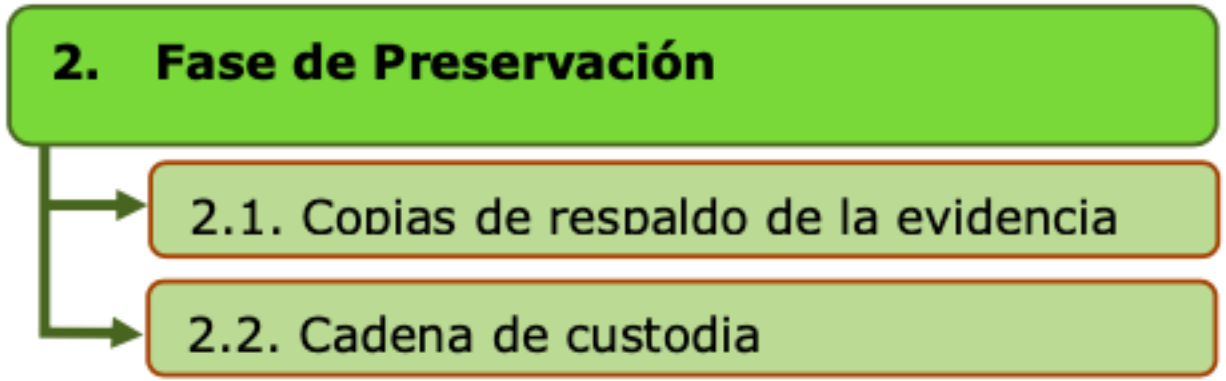
INFORMÁTICA FORENSE



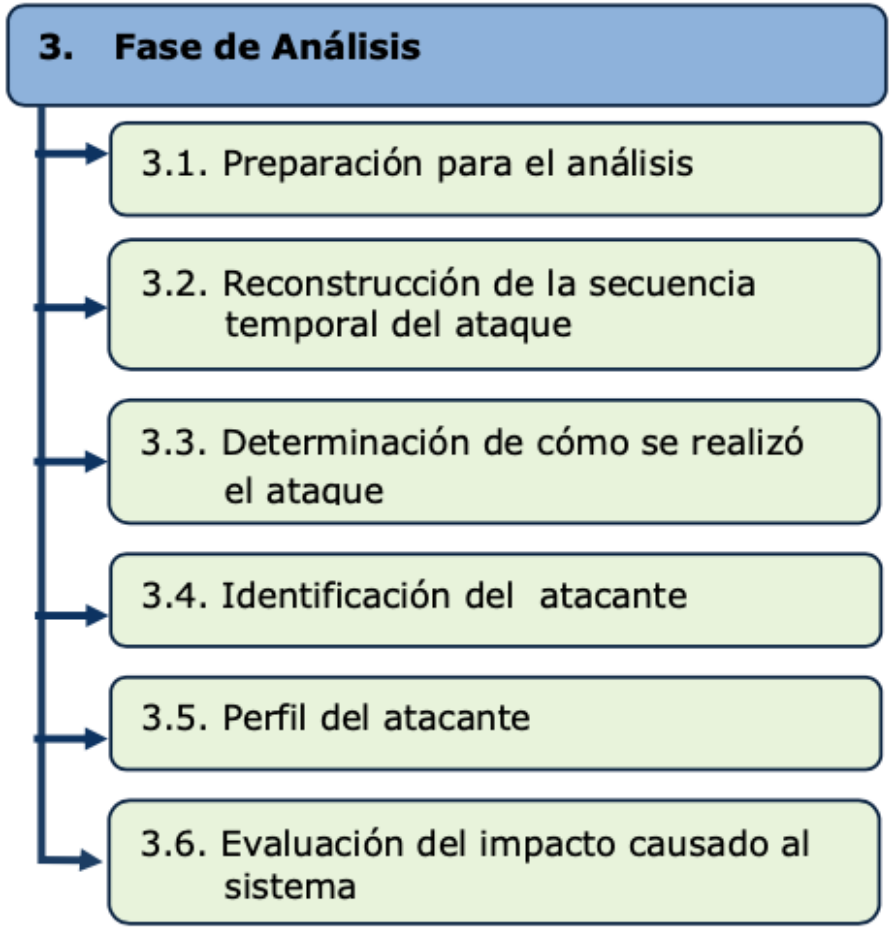
INFORMÁTICA FORENSE



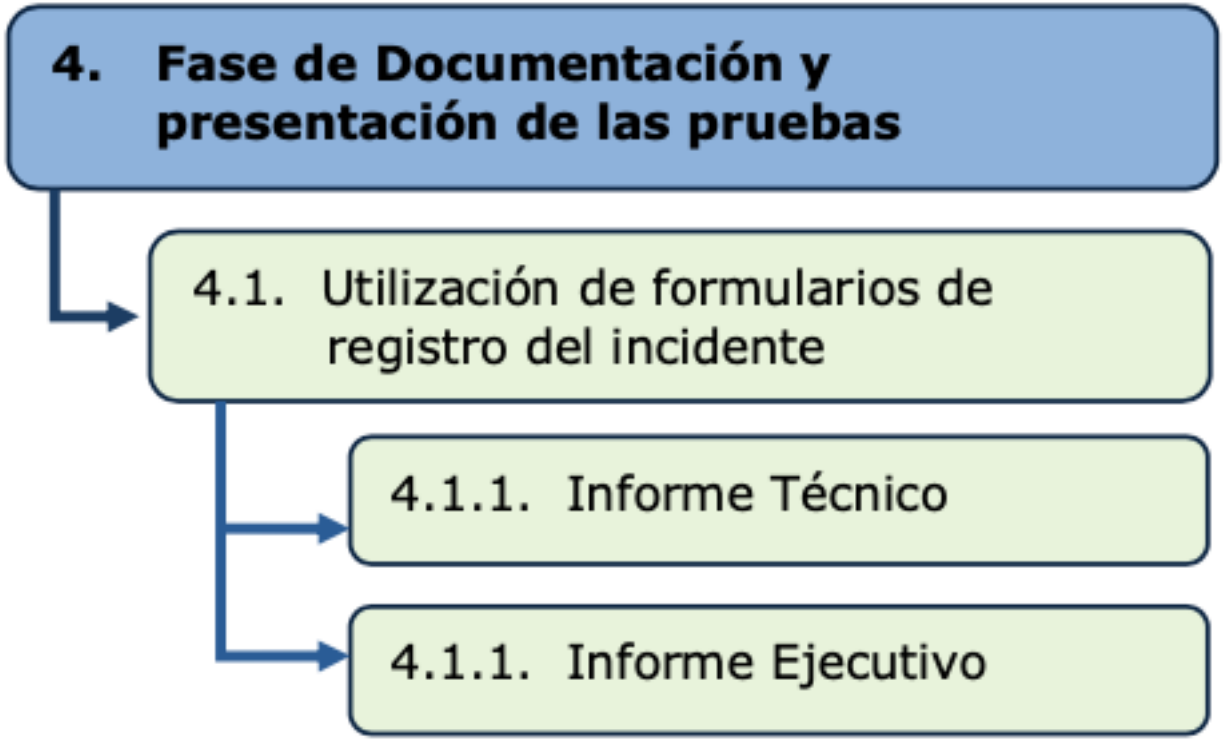
INFORMÁTICA FORENSE



INFORMÁTICA FORENSE



INFORMÁTICA FORENSE



INFORMÁTICA FORENSE

- **MODULO 2**

INFORMÁTICA FORENSE

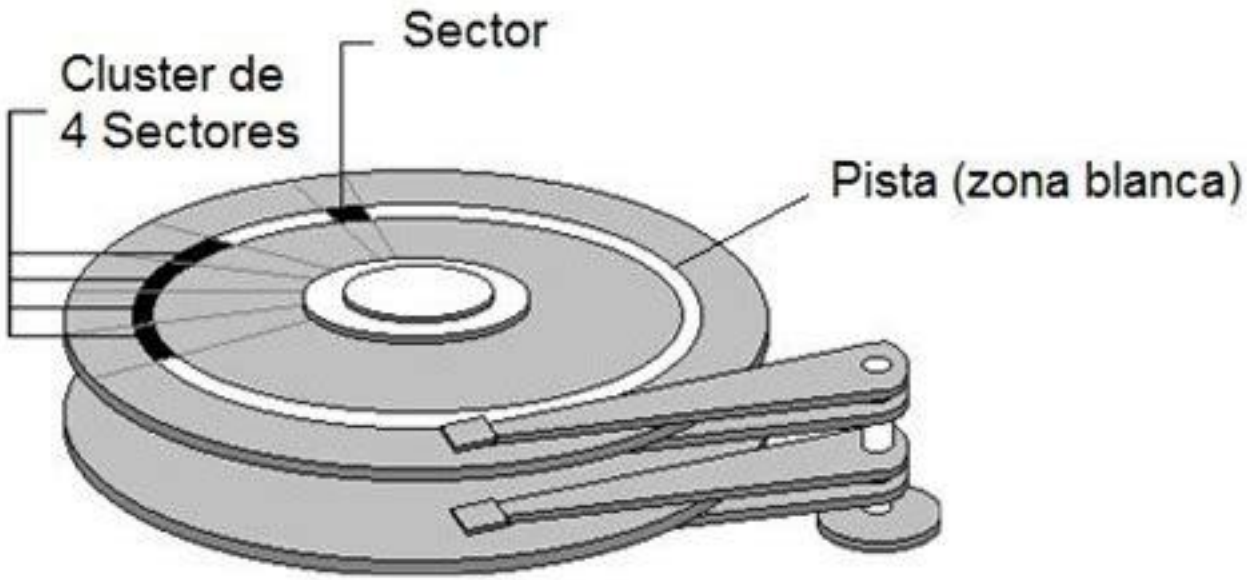
- **Estructura física de un disco duro**

INFORMÁTICA FORENSE

INFORMÁTICA FORENSE

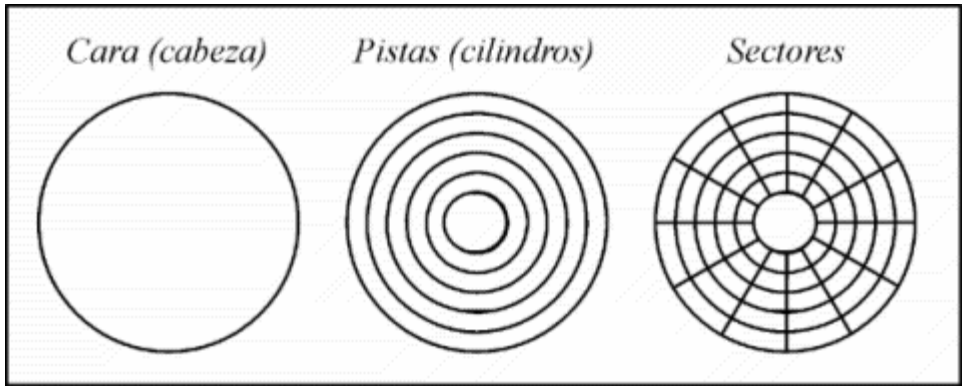
- **Estructura lógica de un disco duro**

INFORMÁTICA FORENSE

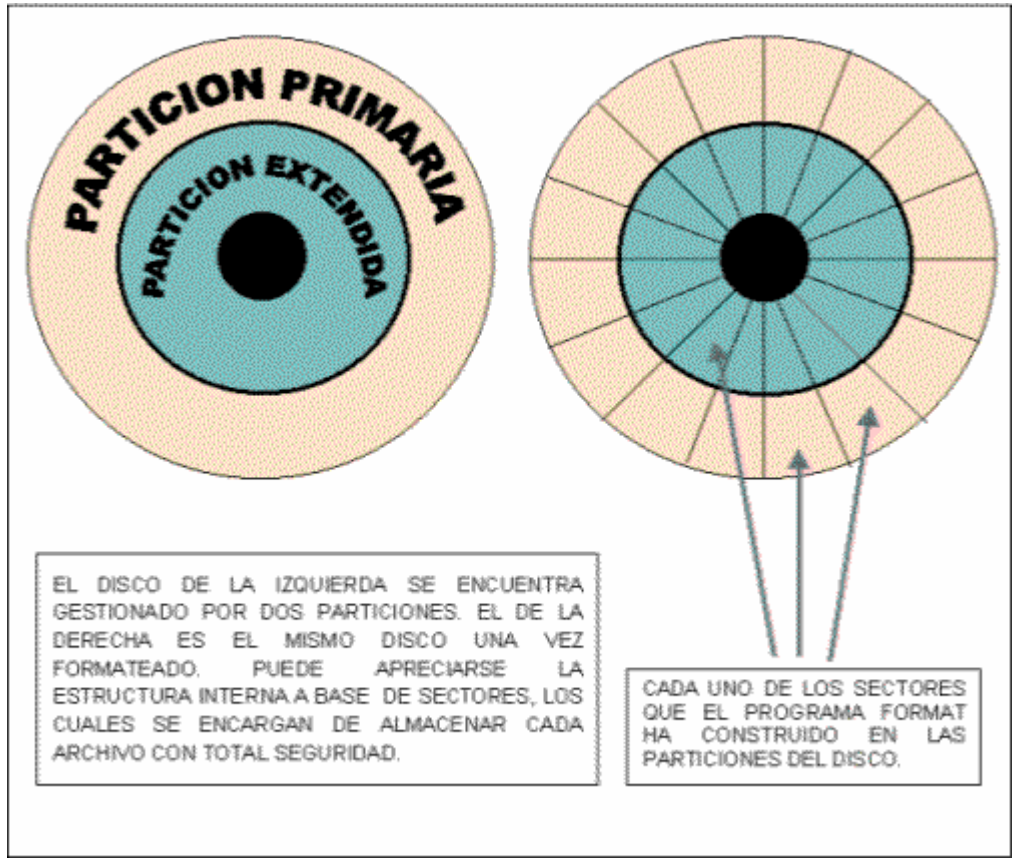


INFORMÁTICA FORENSE

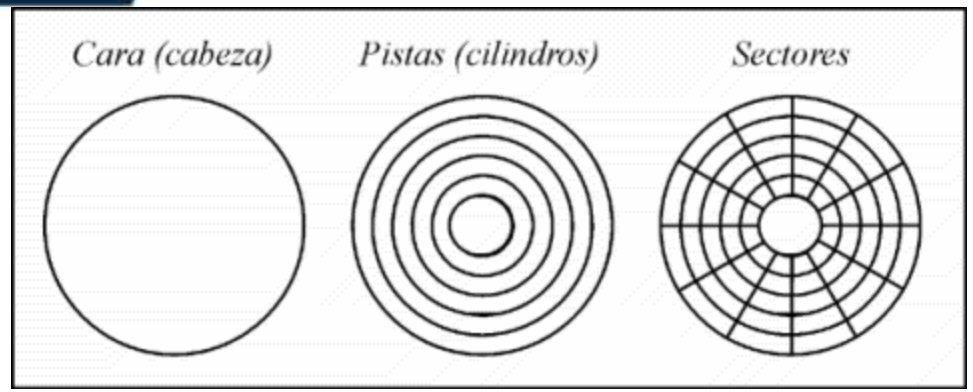
- **Estructura lógica de un disco duro**



ESTRUCTURA DE UN DD

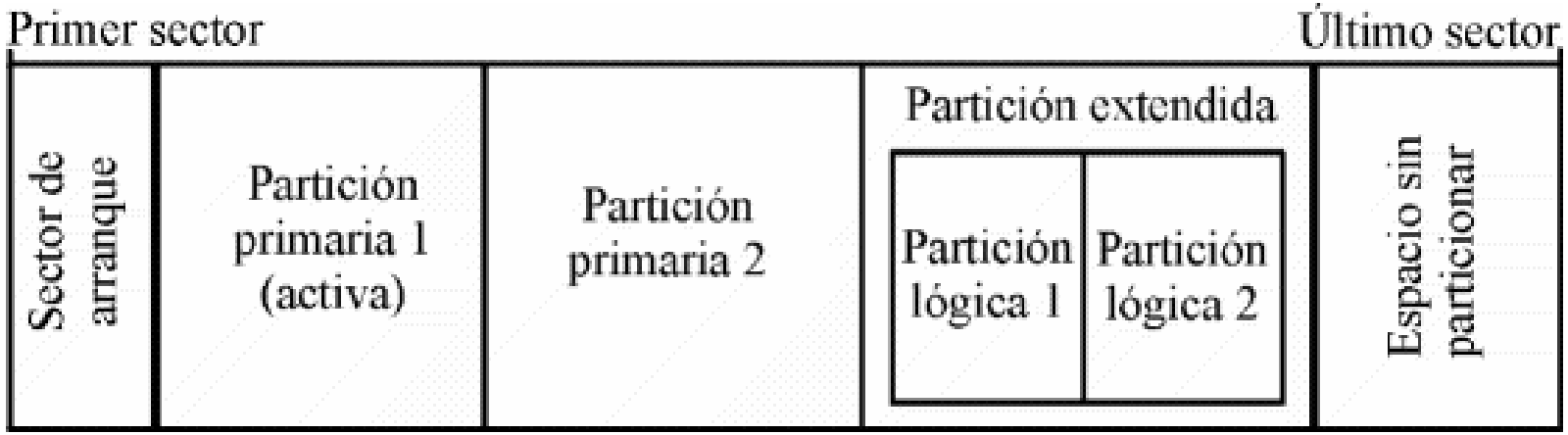


INFORMÁTICA FORENSE



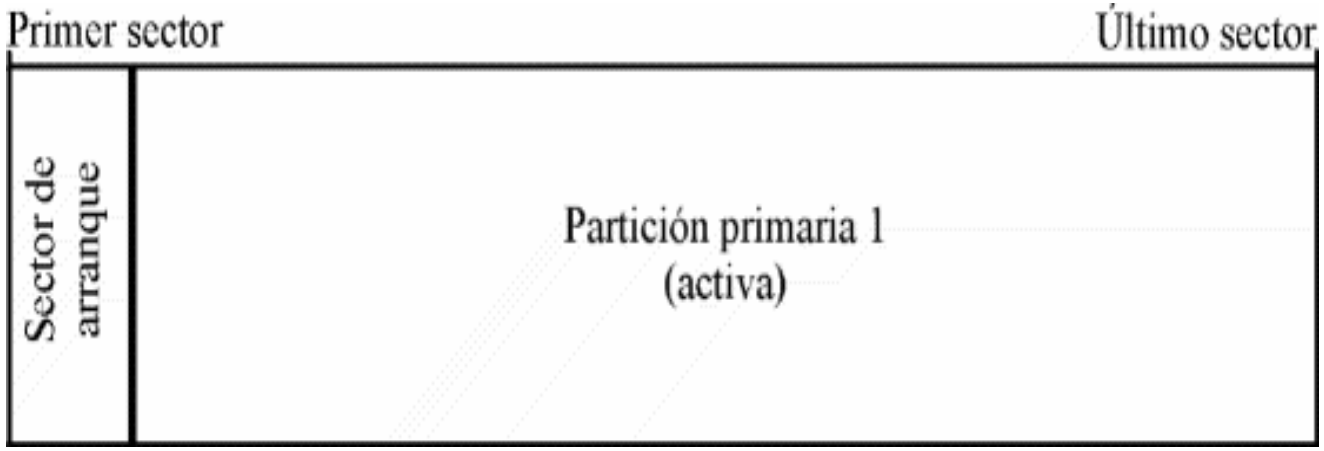
Por ejemplo, el disco duro *ST33221A* de *Seagate* tiene las siguientes especificaciones: *cilindros* = 6.253, *cabezas* = 16 y *sectores* = 63. El número total de sectores direccionables es, por tanto, 6.253*16*63 = 6.303.024 sectores. Si cada sector almacena 512 bytes de información, la capacidad máxima de este disco duro será de 6.303.024 sectores * 512 bytes/sector = 3.227.148.228 bytes ~ 3 GB.

INFORMÁTICA FORENSE

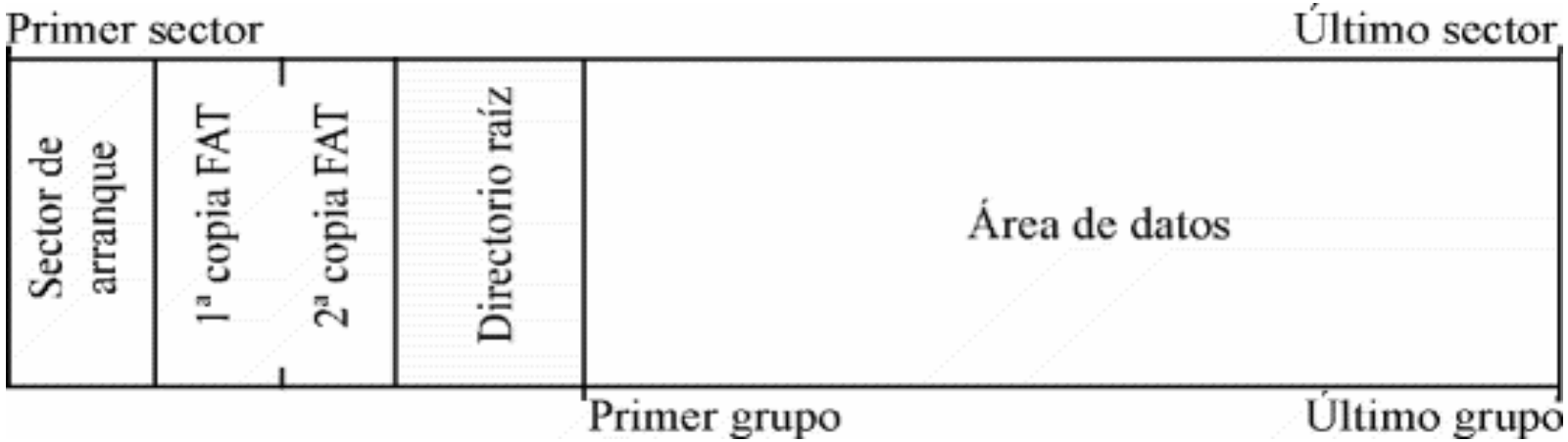


Primer sector

INFORMÁTICA FORENSE

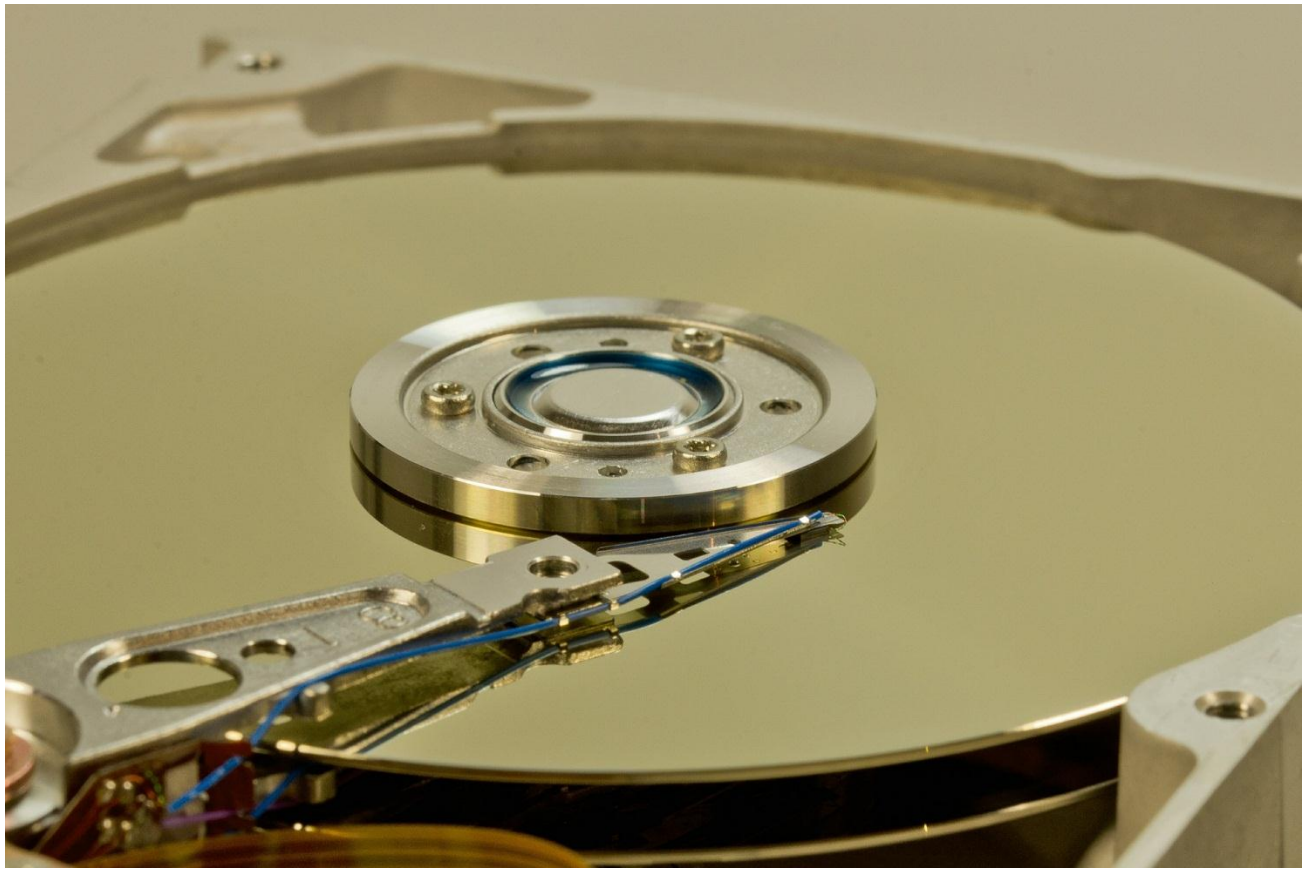


INFORMÁTICA FORENSE



Primer sector

INFORMÁTICA FORENSE



- **FAT**

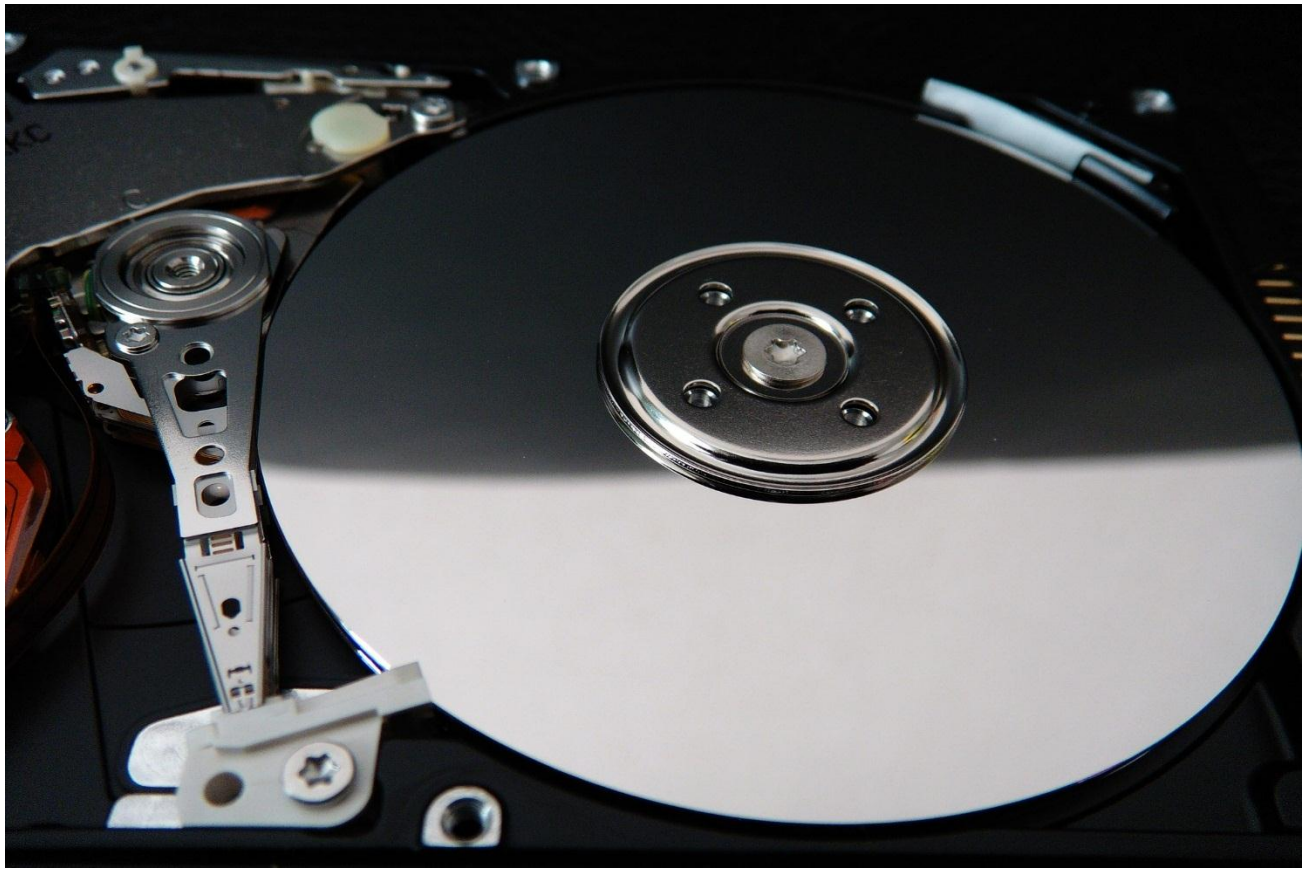
INFORMÁTICA FORENSE

- **NTFS**

INFORMÁTICA FORENSE

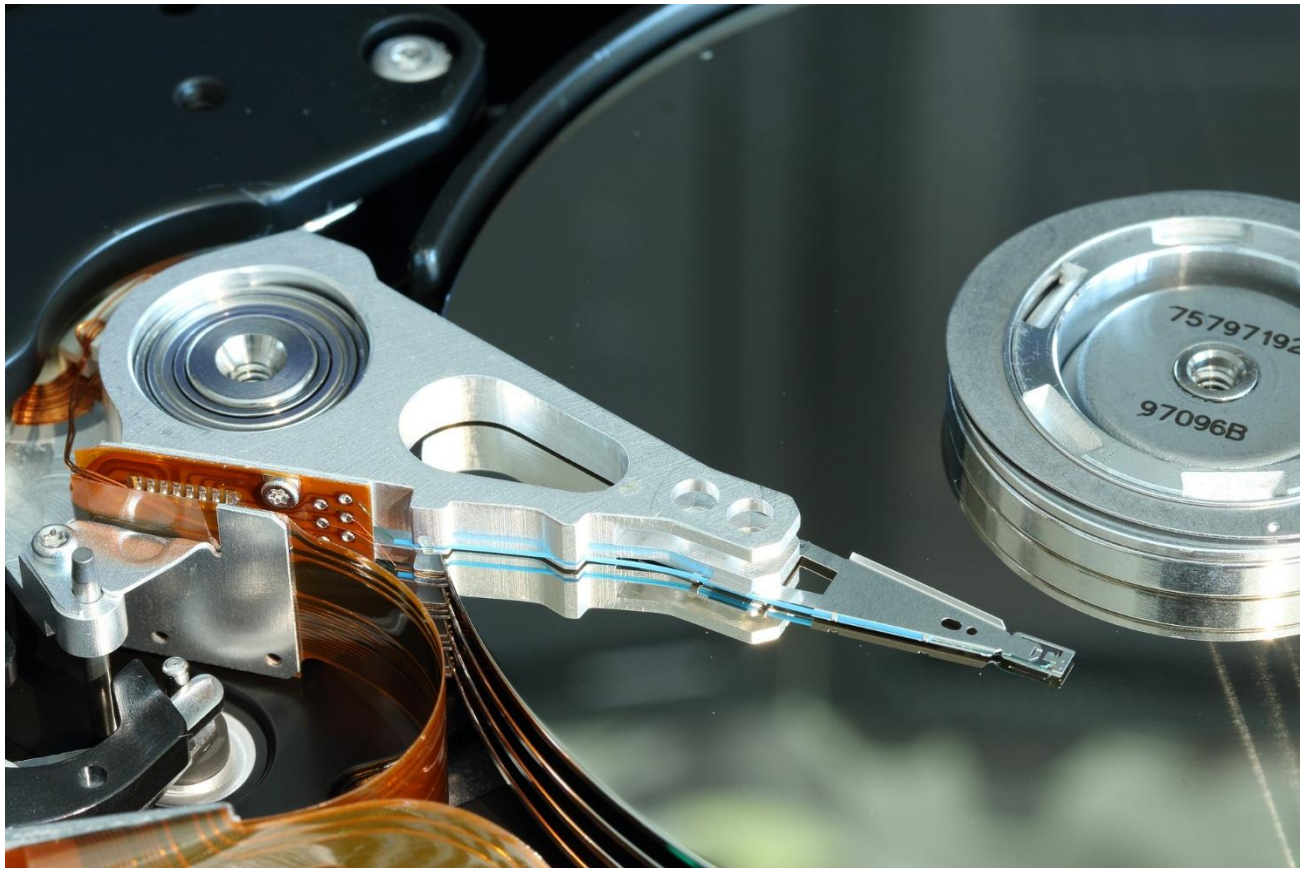
- **EXT2,EXT3,EXT4**

INFORMÁTICA FORENSE



- **HFS+**

INFORMÁTICA FORENSE



- **APFS**

INFORMÁTICA FORENSE

- **Práctica, como formatear un disco duro en Linux.**

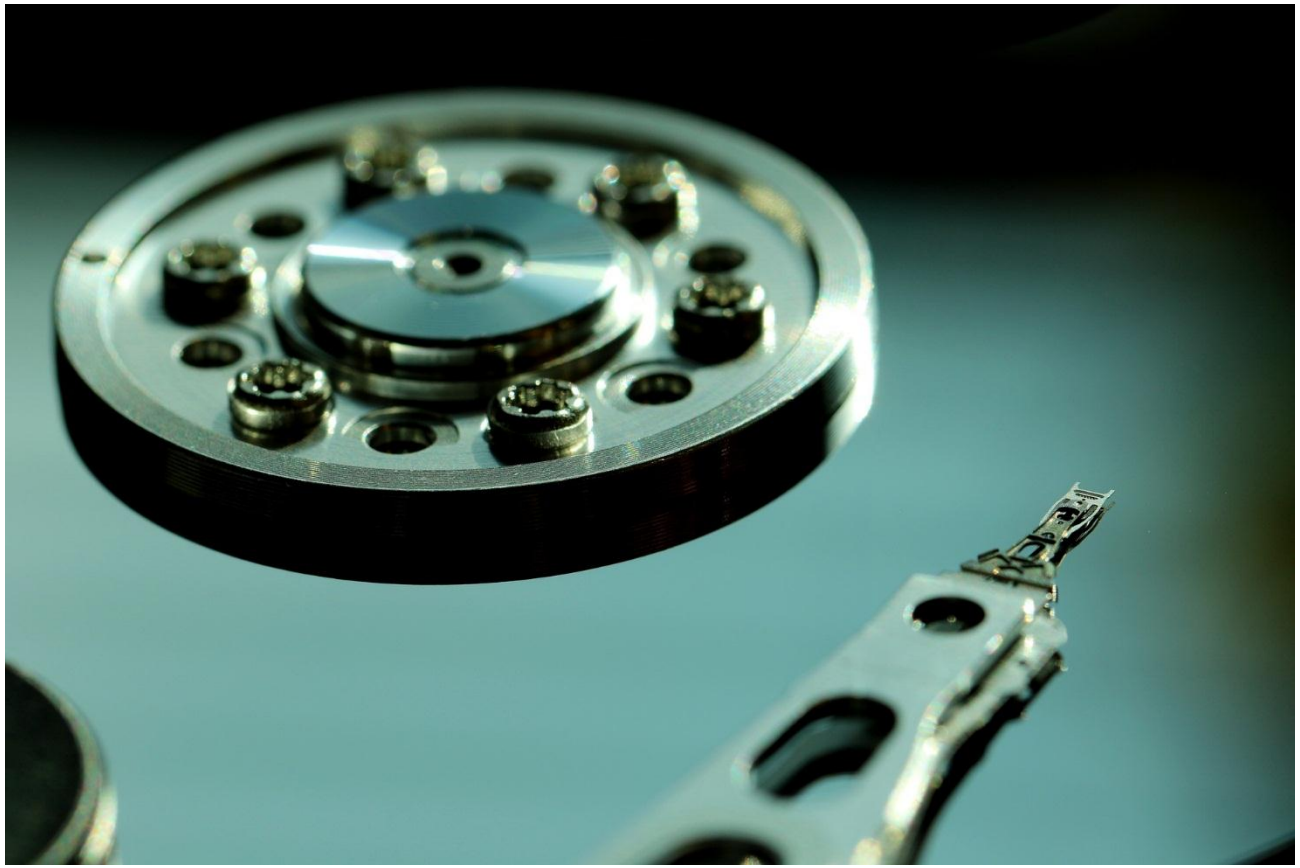
INFORMÁTICA FORENSE

$ su (o "sudo su" en algunas ediciones)

INFORMÁTICA FORENSE

Disk /dev/sda: 16.1 GB, 16139354112
bytes /dev/sda1 * 1 1874 15052873+ 83
Linux
/dev/sda2 1875 1962 706860 5 Extended
/dev/sda5 1875 1962 706828+ 82 Linux
swap / Solaris
Tu nuevo disco duro no tendrá
particiones, por lo que todo lo que verás
será una línea parecida a:
Disk /dev/sdb: 16.1 GB, 16139354112
bytes

INFORMÁTICA FORENSE



df

INFORMÁTICA FORENSE

umount /dev/sdb

INFORMÁTICA FORENSE

fdisk /dev/sdb

INFORMÁTICA FORENSE

- La entrada "fdisk" se abrirá. Presiona "n" para crear la nueva partición, y después presiona "Enter".

INFORMÁTICA FORENSE

- Presiona "1" para crear la primera partición, seguido de "Enter

INFORMÁTICA FORENSE

Introduzca el valor predeterminado para el primer y último cilindros cuando el equipo te solicite esta información. Esto hará que la partición abarque el disco entero y no sólo una parte de él.

INFORMÁTICA FORENSE

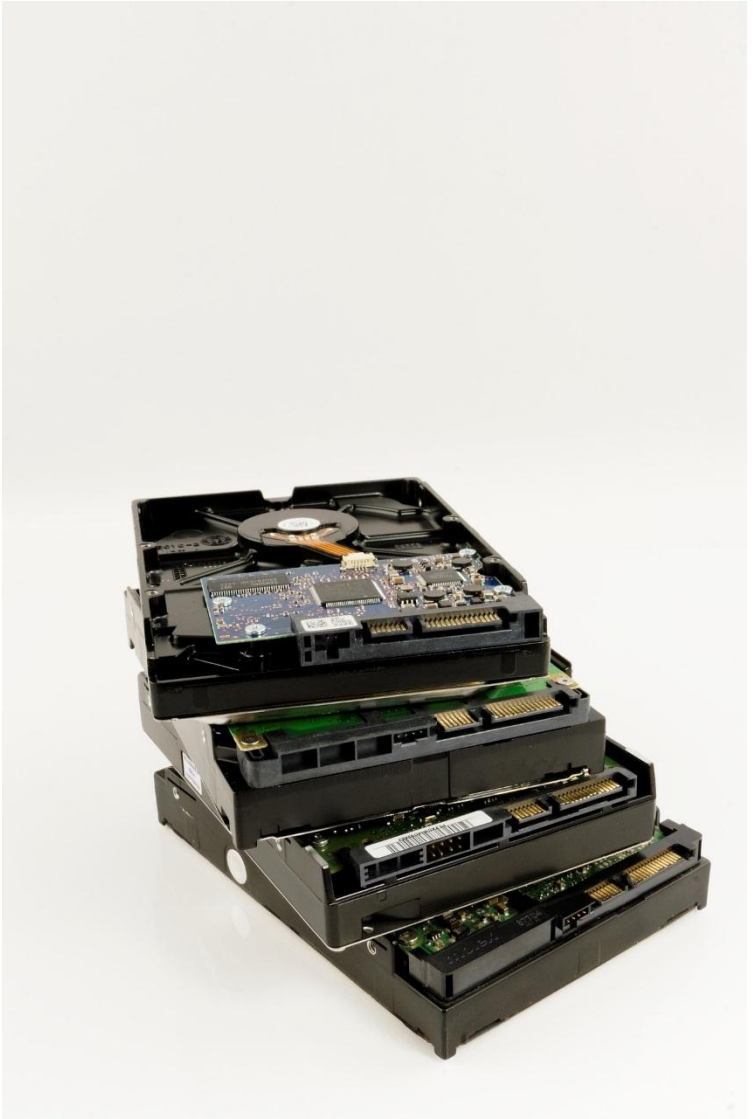
Pulsa el botón "t" para cambiar el tipo del sistema de archivos, seguido de "Enter".

INFORMÁTICA FORENSE

Escribe "L" para ver una lista de los tipos conocidos, seguido de "Enter".

INFORMÁTICA FORENSE

- **XXX**

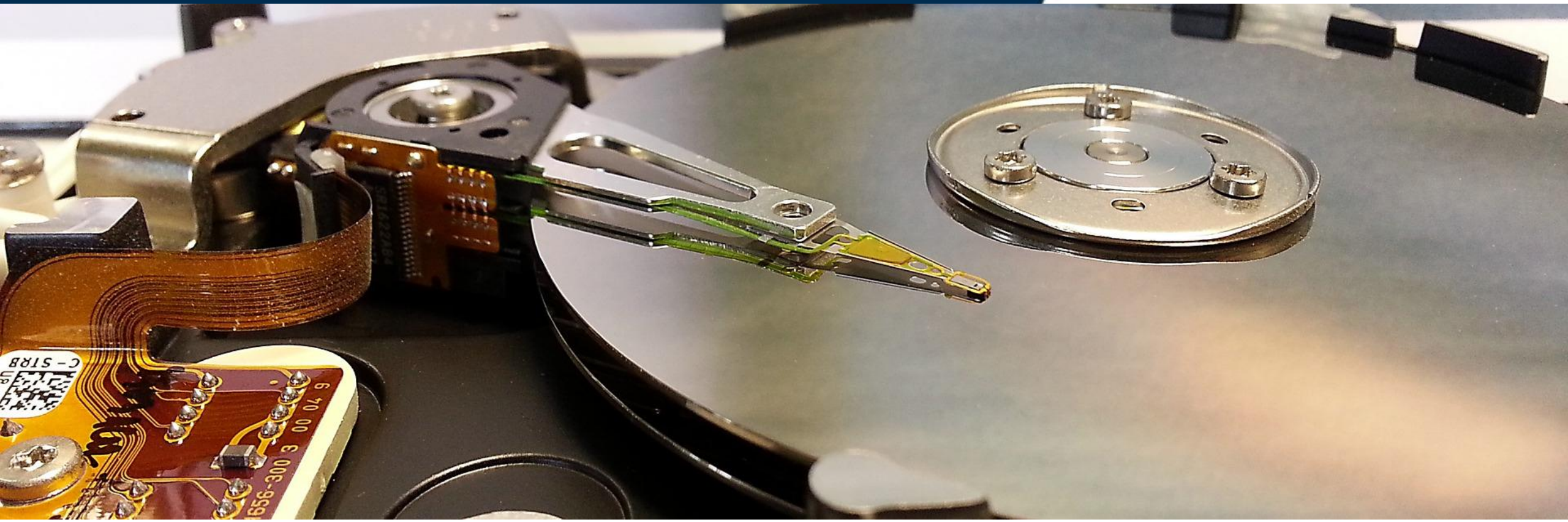


INFORMÁTICA FORENSE

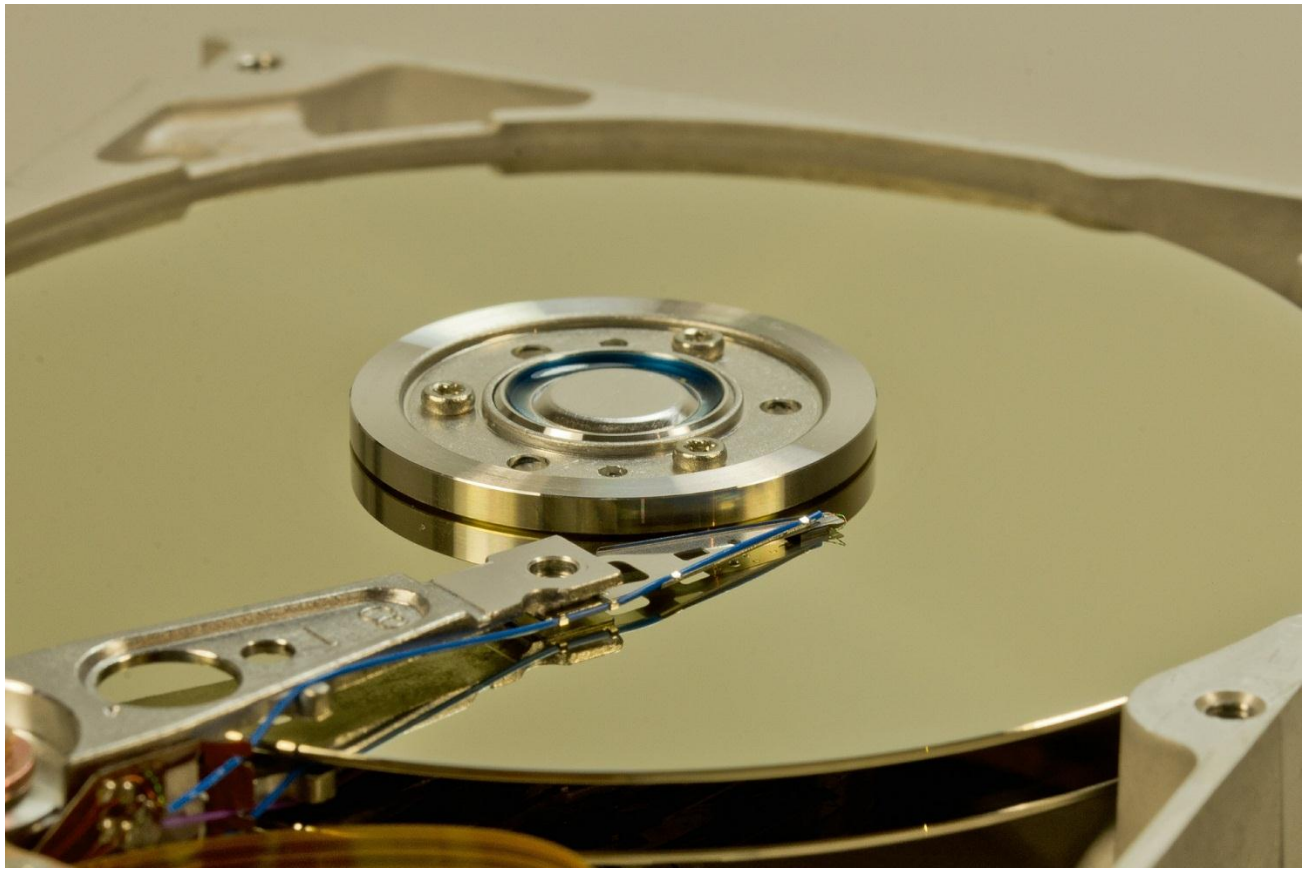
Presiona "w" para escribir la partición en el disco (esto no se puede deshacer), y luego presiona "Enter".

Formatea la nueva partición

INFORMÁTICA FORENSE



INFORMÁTICA FORENSE



- **FAT**

INFORMÁTICA FORENSE

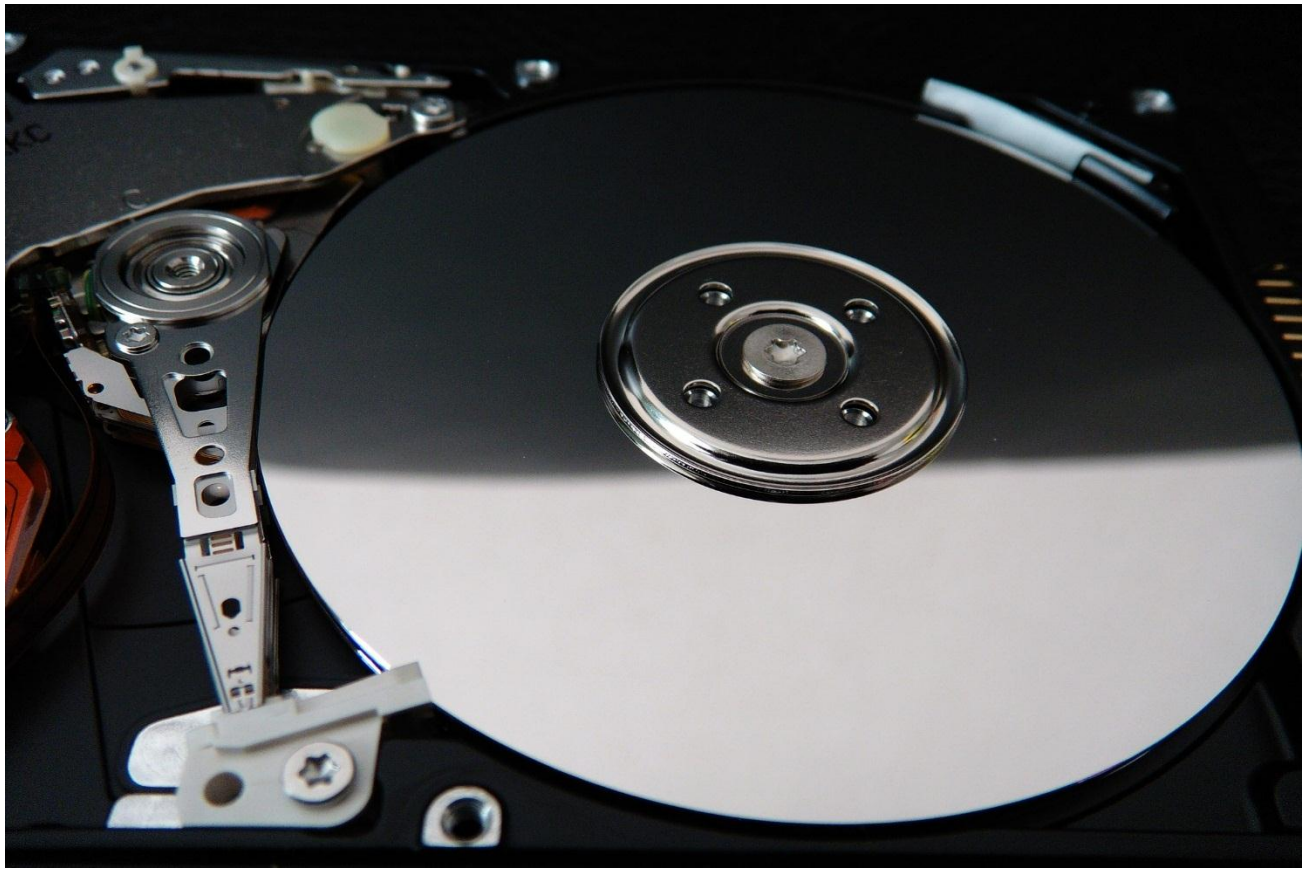
Una nueva partición

mkfs.ext4 /dev/sdb1

INFORMÁTICA FORENSE

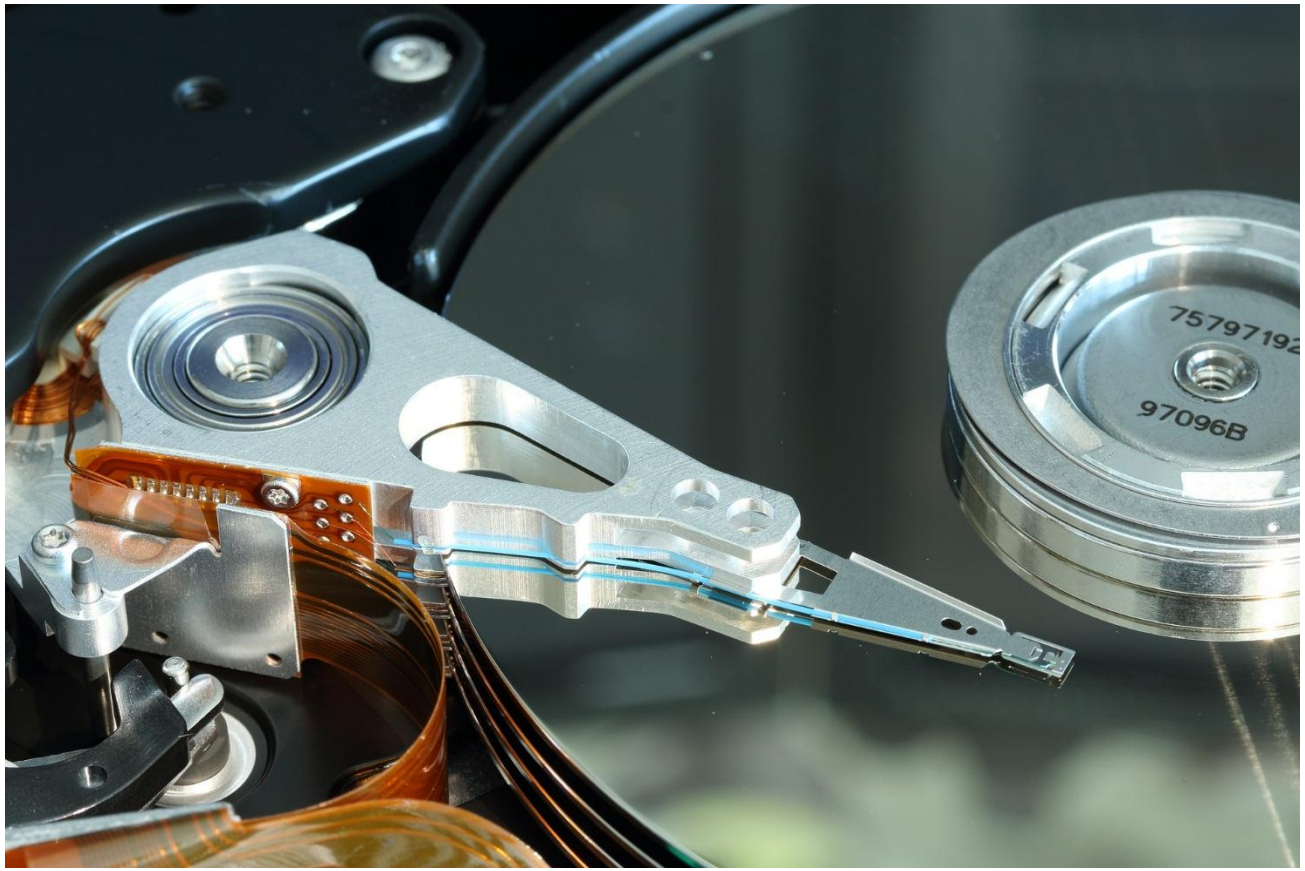
mkdir /media/newdrive (o cualquier nombre que prefieras)
mount /dev/sdb1 /media/newdrive

INFORMÁTICA FORENSE



nano /etc/fstab or # vi /etc/fstab

INFORMÁTICA FORENSE



/dev/sdb1 /media/newdrive
ext4 defaults 1 2

INFORMÁTICA FORENSE

- **Práctica, como formatear un disco duro en Linux.**