https://commons.wikimedia.org/wiki/File:BouleTesch.jpg

Hey, vous êtes perdus ?

Un cas classique que l'on traite souvent en investigation numérique sont les images disques.

Il s'agit de l'image disque en brut. Pour comprendre comment le stockage de mémoire marche, je vous redirige vers Wikipedia. Ce sera utile ici sûrement :)

Regarder l'état des partitions :

```
$ fdisk -l [image-disque]
```

```
$ mmls <image-disque>
(sleuthkit)
```

Un bon réflexe quand on fait face à une image disque est de la monter. Comment ?

Sans arguments fdisk -l renvoie l'état des partions des devices dans `/proc/partitions.` Ce sont celles utilisées actuellement par l'ordinateur.

La commande losetup si il y a plusieurs partitions :

```
$ losetup -fP <image-disque>
```

(crée des loop devices correspondant à chaque partition)

La commande mount :

Permet de monter un système de fichier.

```
$ mount <source> <destination>

EX :
$ mount /path/to/partition /mnt
```