Les disques durs

Fonctionnement général et analyse forensique

HackademINT

- Composant essentiel
- mémoire *persistante* ($\neq$ volatile)
- 2 types de disques : HDD et SSD

Figure – Un HDD.

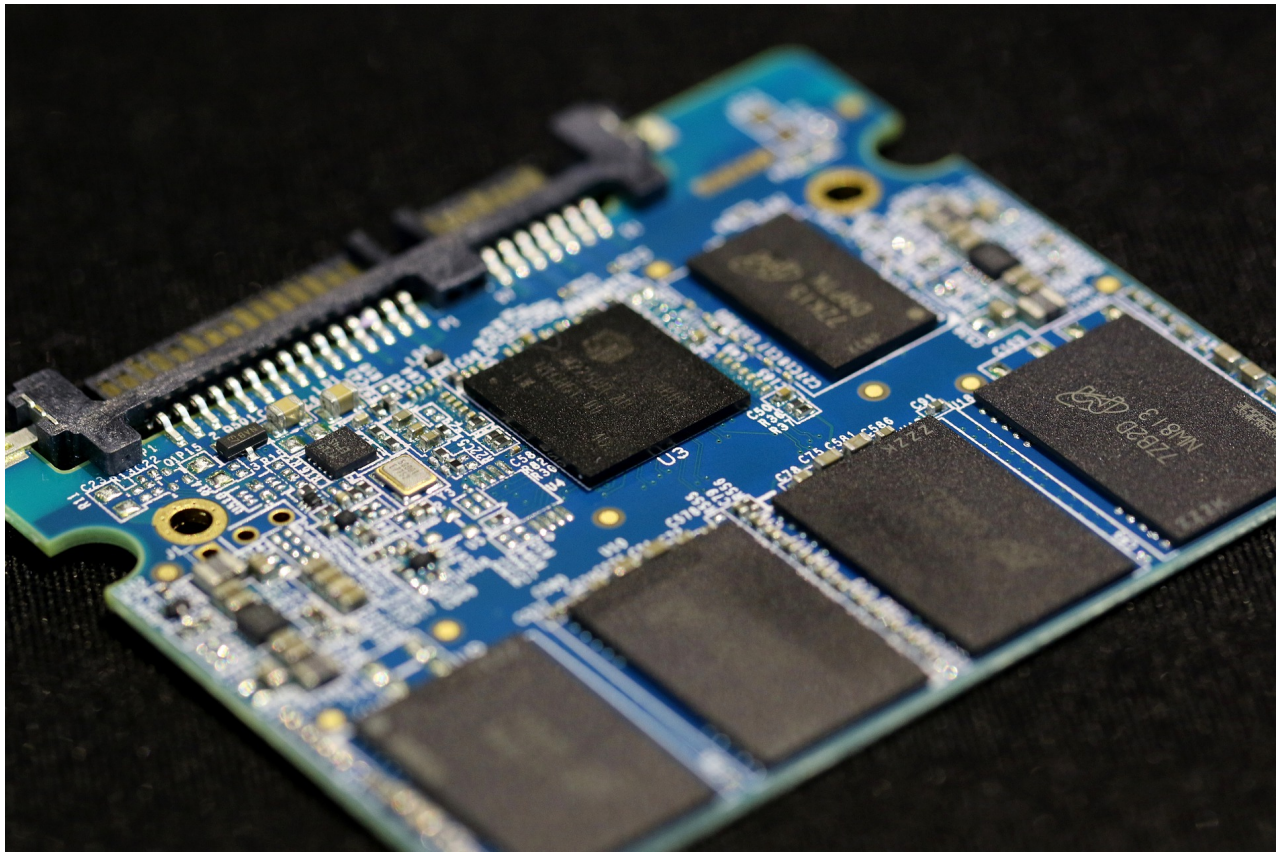

Figure – Un SSD.

Même pas grave !

Quel que soit le type de disque utilisé, le fonctionnement du stockage des informations est strictement identique.

- l'USB (Universal Serial Bus)
- l'IDE (Integrated Drive Electronics)

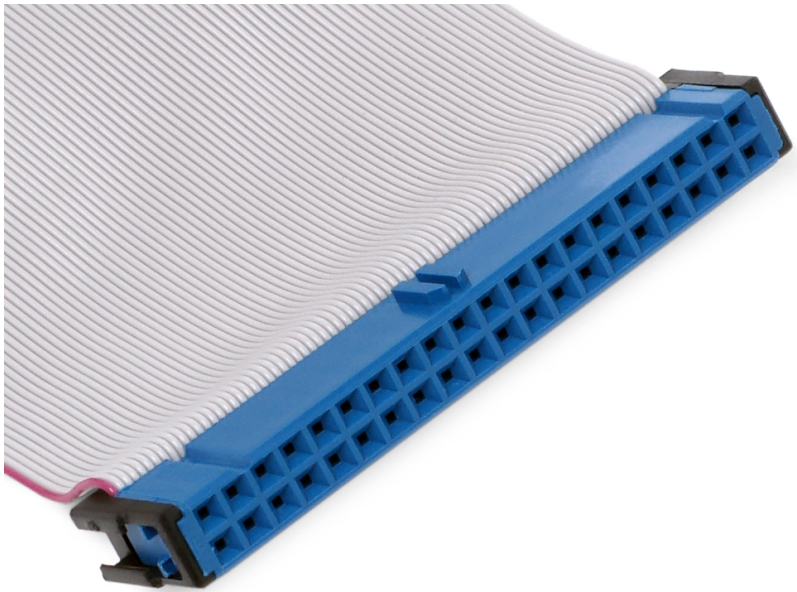

Figure – Une nappe IDE et son connecteur.

- Le SATA (Serial Advanced Technology Attachment)

Figure – Un connecteur SATA.

- Des partitions de données
- La swap
- La partition de boot
- Les partitions de crash Windows

- FAT (File Allocation Table) : 3 versions majeures, FAT12, FAT16 et FAT32. Ce système n'est quasiment plus utilisé aujourd'hui (par exemple, le maximum de données pouvant être stocké sur un FAT16 est de 4Go...), et est connu pour énormément se fragmenter.
- l'exFAT (Extensible File Allocation Table), appelé improprement FAT64 : cartes SD.
- le format ext (Extended File System) a été créé spécifiquement pour le noyau Linux.
- NTFS (New Technology File System) est un système propriétaire, développé par Microsoft pour Windows.

- Structure de données (présentes sur ext)
- Numéro d'identifiant unique
- Informations vitales sur le fichier
- Gestion de la mémoire et de la suppression !


QUAND TU PENSAIS
AVOIR SUPPRIMÉ LES PREUVES
ET QU'EN FAIT ELLES SONT
JUSTE DANS LA CORBEILLE...
imgflip.com

Sous Linux, comme vous le savez sûrement déjà, "tout est fichier". La plupart des éléments de votre ordinateur sont en fait regroupés dans le dossier /dev (pour devices) : cpu, souris, clavier, entrées USB... et votre disque.

- Les deux premières lettres (fd, hd, sd) correspondent à la connectique. fd = "floppy disk" ou disquette, hd = IDE, sd = SATA (et éventuellement d'autres).
- La lettre suivante correspond au numéro du disque.
- Le numéro qui suit correspond aux partitions. sda3 représente donc la troisième partition de votre premier disque SATA. Simple, non ?

C'est pas tout !

Il est possible de retrouver d'autres nommages, notamment pour les connecteurs. Ainsi, ceux qui possède un PC avec un SSD récent ont peut-être un disque du genre nvme0n1 : cela correspond à une connectique récente, qui apparaît de plus en plus sur les SSD car elle est plus rapide et permet de mieux exploiter les possibilités d'un gros SSD (notamment en termes de parallélisme).

- L'opération qui consiste à choisir une partition sur un disque et à l'associer à un endroit dans votre arborescence de fichiers afin de pouvoir y accéder s'appelle *le montage*. **Nécessite par défaut les droits root.**
- Partitions montées par défaut sur / et /boot au démarrage
- Fichier important : /etc/fstab

Sécurité des clés USB

Attention : même si la plupart des systèmes d'exploitation le font automatiquement, cela reste une assez mauvaise idée en termes de cybersécurité de monter une clé USB externe automatiquement : s'il s'agit d'une clé malicieuse, elle a ainsi accès directement au PC de la victime, et ce parfois alors que le PC est en veille avec l'écran verrouillé ! Monter les clés USB à la main et taper son mot de passe à chaque fois peut paraître long et fastidieux, mais cela vous assure que seules les clés USB que vous avez explicitement autorisées ont accès à votre PC.

- mount : **mount <partition> <dossier cible>**
- umount : **umount <partition>**
- lsblk : il s'agit du ls des disques et partitions. Son avantage (énorme dans certains cas) est qu'il ne nécessite pas les droits root.
- fdisk : il fait partie d'un groupe plus étendu d'outils (fdisk, cfdisk, sfdisk...) qui permettent de faire beaucoup de choses sur les disques / partitions, de les déplacer, redimensionner... **fdisk -l** équivaut à lsblk.
- parted
- gparted
- dd **dd if=<entrée> of=<sortie> [bs=<taille des blocs>]**
- shred : **shred <fichier>**

- Récupérer des données corrompues ou effacées
- Obtenir de nouvelles informations sur un fichier
- Retrouver un rootkit
- ...

Divers problèmes possibles, surtout la taille ! ! !

- fls
- fcat (avec les inodes)
- plein d'autres (voir lien sur le pdf)
- autopsy

- Différents formats (métadonnées, compression...) : souvent EWF ou AFF
- file est votre ami, Google aussi
- Autopsy lit quand même beaucoup de formats !

- Redundant Array of Independent Disks
- permet la redondance et la performance
- plusieurs versions n'utilisant pas les mêmes technologies (RAID1, RAID2, RAID4, RAID5...)
- outils spécifiques disponibles

- disque chiffré : z'êtes en galère
- LUKS (Linux Unified Key Setup)
- high entropy detected
- pensez aux hash !

Merci de votre attention

Des questions ?