



Systeme d'exploitation

Chapitre 1. Introduction

Dans un ordinateur, le système d'exploitation assure l'interface avec les différents éléments matériels et en mesure le pilotage. Sans système d'exploitation, l'utilisation d'un ordinateur et de ses capacités est impossible.

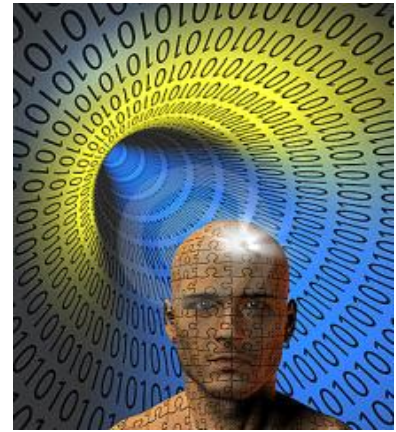
Pour aborder le chapitre sur les systèmes d'exploitation, voici un petit rappel concernant l'informatique, l'ordinateur, ses composants et périphériques.

1) Le codage de l'information numérique

Les informations utilisées dans tous les systèmes informatiques sont d'un seul type : **numérique**.

Toutes les données échangées ou tous les programmes exécutés sur une machine sont codés sous forme de **valeurs numériques**, que ce soit du texte, du son, de l'image, des vidéos, etc.

La base de ces valeurs numériques est le codage de l'information avec des 0 et des 1, appelés aussi **BIT**, et la réunion de huit de ces éléments s'appelle un **OCTET** ou un **BYTE**.



Cet Octet ou Byte peut en fait correspondre à une valeur entre 0 et 255.

Le **bit** est la plus petite unité de mesure en informatique. Un **octet** comporte 8 bits.

Le terme "**Byte**" est le mot anglais pour octet, afin de ne pas le confondre avec les **bits**, il est toujours noté avec un **B** majuscule.

Exemple : **11111111 = 255**

- La valeur **11111111** est la représentation en **binaire**.
- la valeur 255 est la représentation **décimale**.

Tableau de conversion du binaire (8 bits) en décimal								
Binaire	1	1	1	1	1	1	1	1
Décimal	(2 ⁷ =) 128	(2 ⁶ =) 64	(2 ⁵ =) 32	(2 ⁴ =) 16	(2 ³ =) 8	(2 ² =) 4	(2 ¹ =) 2	(2 ⁰ =) 1
Exemple avec la valeur décimale de 25 = 16 + 8 + 1								
Binaire	0	0	0	1	1	0	0	1
Décimal				(2 ⁴ =) 16	(2 ³ =) 8			(2 ⁰ =) 1

C'est pour cette raison que les représentations de l'informatique utilisent souvent des valeurs avec des 0 et des 1, et que l'on emploie parfois des mots comme « *fracture numérique* », pour représenter la frontière entre les personnes qui utilisent l'informatique et ceux qui ne l'utilisent pas.

C'est aussi pour cette raison que les chiffres employés pour des vitesses de transfert ou du stockage de données en informatique sont toujours des multiples de 8 (1 Octet / 1 Byte = 8 bits).

En informatique, si on simplifie, on peut dire qu'un **Octet (Byte) = un caractère**.

- bit = unité de base 0 ou 1
- Byte(octet) = un caractère (huit bits)

2) Unités de mesure

Unité	S'écrit	Valeur simplifiée	En octet	Équivalence
Octet	o	8 bits	1	Un caractère
Kilo-octet Kilobyte	Ko KB	1 000 octets	1 000 (exactement 1024)	+ -1000 caractères ou un fichier texte
Méga-octet Megabyte	Mo MB	1 000 Ko	1 000 000 (exactement 1024 ²)	+ - 1 million de car. ou un fichier image
Giga-octet Gigabyte	Go GB	1 000 Mo	1 000 000 000 (exactement 1024 ³)	+ - 1 milliard de car.
Téra-octet Terabyte	To TB	1 000 Go	1 000 000 000 000	+ - mille milliards de car.

Exemple :

Mémoire, clé USB Capacité 16 GB :

(+ - 16 milliards de caractères)



Chapitre 2. Les composants de l'ordinateur

Il s'agit principalement de composants électroniques dont les logiciels se servent pour accomplir leur tâche. Tous les composants de l'ordinateur participent aux performances. On peut en distinguer 2 catégories:

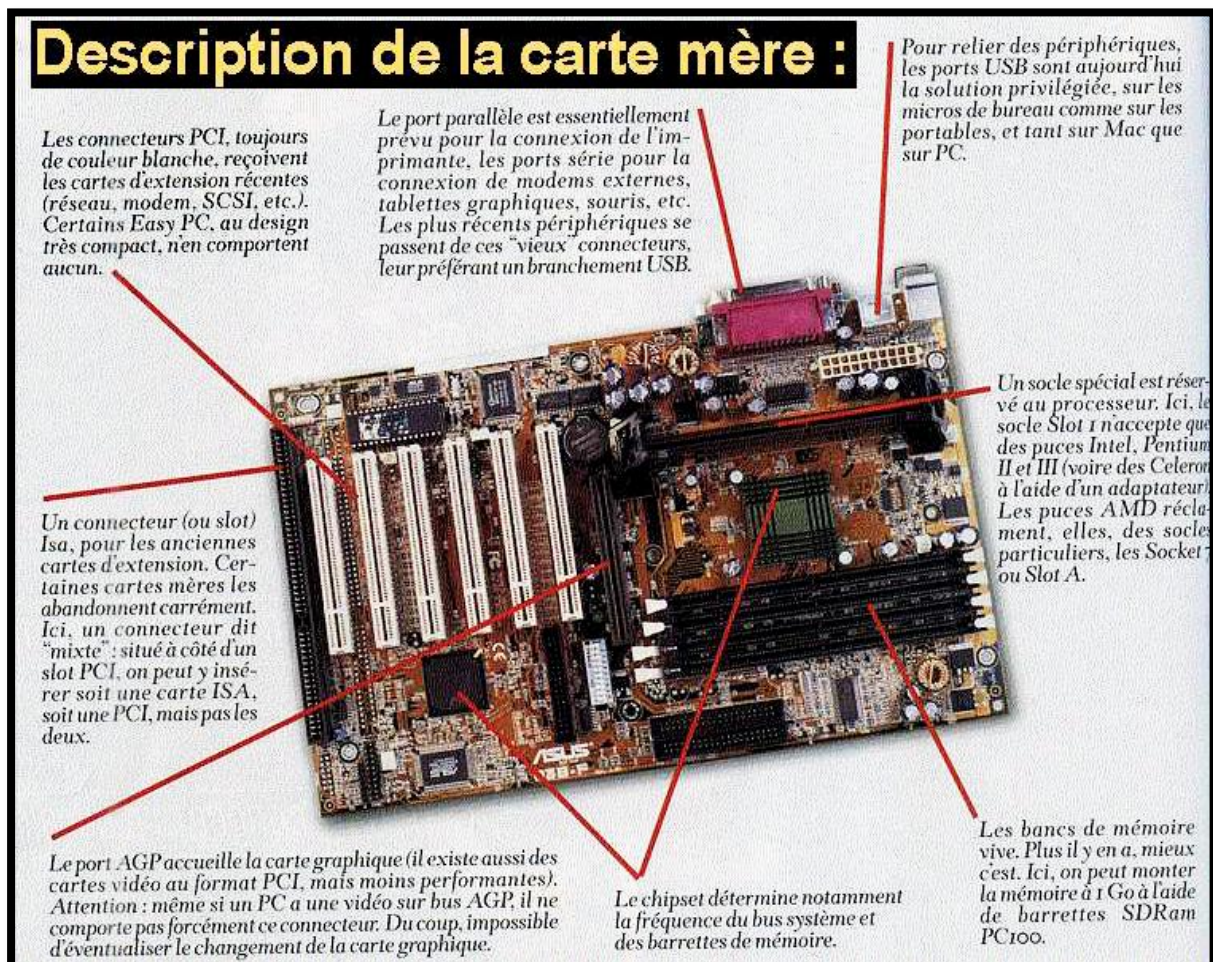
- Les composants internes de l'ordinateur.
- Les périphériques informatiques.

1) Les composants internes de l'ordinateur.

Se sont les éléments qui se trouvent à l'intérieur du boîtier du PC :

- Microprocesseur
- Mémoire vive
- Carte mère
- Bloc alimentation
- Câbles de connexion
- Différentes cartes (son, réseau, vidéo, ...)
- Radiateur et ventilateur

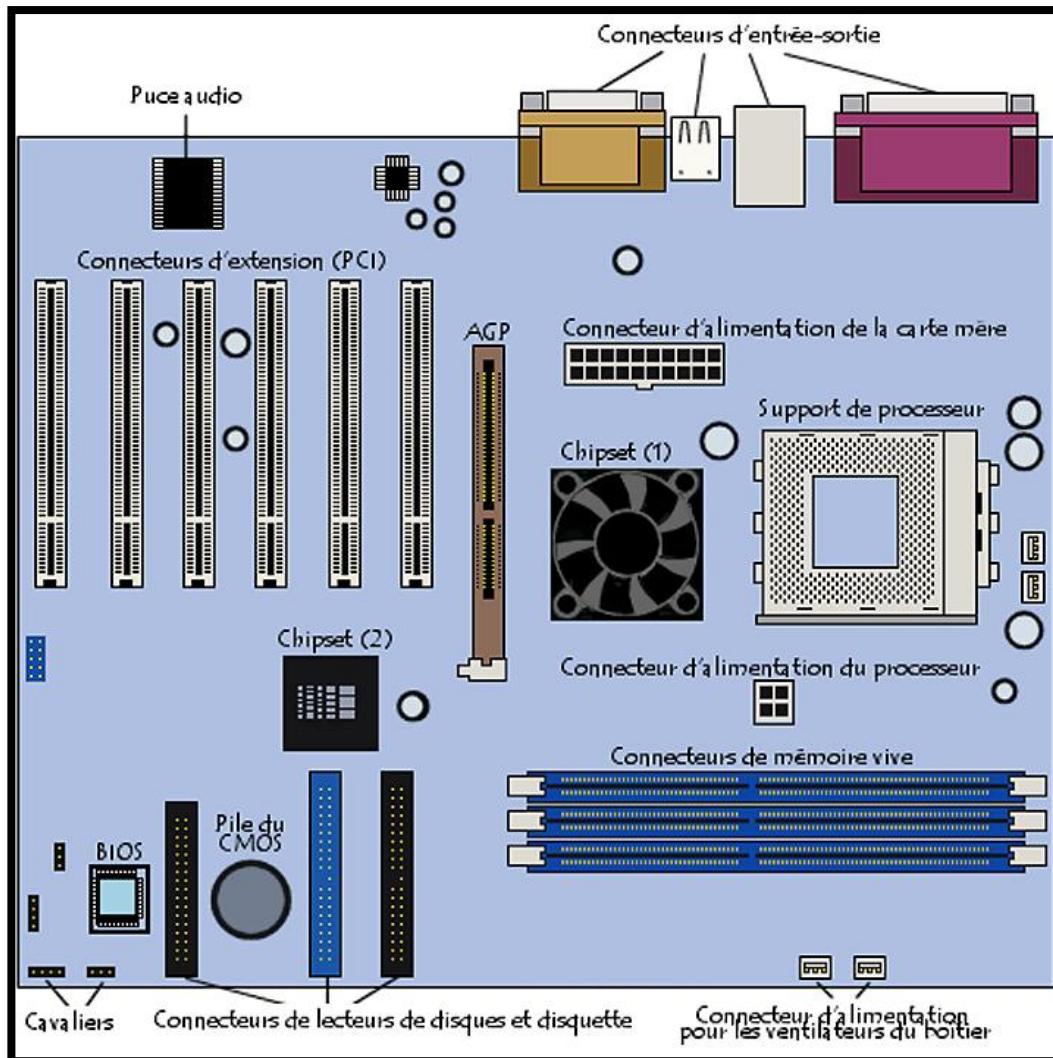
1.1. La carte mère :



Elle assure la connexion de tous les autres composants. Elle est la pièce maîtresse des circuits internes de l'ordinateur et, en ce sens, elle permet l'échange d'informations entre les différents composants par l'intermédiaire d'un canal appelé bus de communication. C'est sur elle que sont greffés les éléments les plus importants du PC (on y connecte aussi bien le processeur que la mémoire, le disque dur, la carte graphique, etc).

C'est le cœur et le système nerveux de l'ordinateur.

Le cœur de la carte mère est un composant dénommé "chipset" : le type de chipset va déterminer si votre carte mère accepte les différents processeurs, les nouveaux formats de mémoire ainsi que les dernières innovations technologiques. Globalement chaque nouvelle génération de chipset amène son lot d'améliorations technologiques et de petites performances en plus (à même configuration machine pour les autres composants).



Que trouve-t-on sur la carte mère ?

➤ Chipset

Il y en a la plupart du temps 2: le northbridge (abrégé NB) et le southbridge (abrégé SB).

Le NB est le plus important, c'est lui qui gère les échanges entre processeur, RAM et carte graphique.

Le SB gère les ports supplémentaires, le stockage et la connectique externe (PCI, EIDE, COM, LPT, Clavier, souris, USB, BIOS, et toutes les autres E/S (entrée/sorties)).

Le mieux refroidi et le plus proche du processeur est le NB, il est donc facilement reconnaissable.

➤ Ports destinés à connecter différents périphériques:

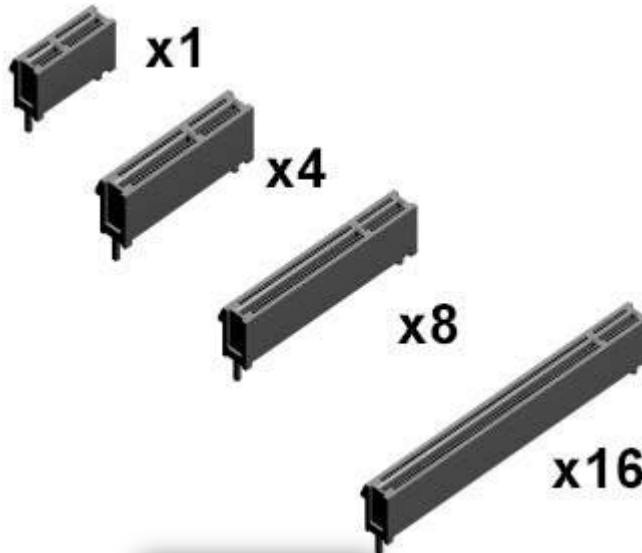
Le port PCI : Cadencé à 33 MHz et pouvant transporter 32 bit de données par cycle d'horloge (64 sur les systèmes 64 bit), le port PCI est encore utilisé mais est trop lent pour certaines cartes graphiques, lesquelles utilisent un port AGP ou PCI Express (encore plus rapide).



Le port AGP : Il a un bus plus rapide que le bus PCI (allant jusqu'à 64 bit et 66 MHz).



Le port PCI Express : allant de 250 Mo/s pour le PCI Express 1X, les débits de ce bus peuvent monter à 4 Go/s en mode 16X. C'est le remplaçant des bus PCI et AGP.



➤ Le socket :

Destiné à recevoir le processeur



➤ Quelques bus :

Un bus est un circuit intégré à la carte-mère qui assure la circulation des données entre les différents éléments du PC (mémoire vive, carte graphique, USB, etc...). On caractérise un bus par sa fréquence (cadence de transmission des bits) et sa largeur (nombre de bits pouvant être transmis simultanément).

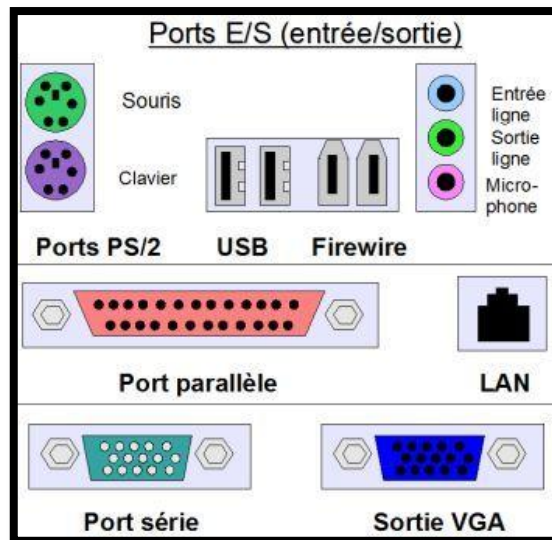
- Le bus système : appelé aussi FSB pour Front Side Bus, c'est le bus qui assure le transport de données entre le processeur et la mémoire vive.
- Le bus série : c'est le bus que tous les PC possèdent, celui qui débouche sur le port servant à brancher une souris ou un modem, ou encore certains périphériques de jeux. Son défaut est sa lenteur extrême car les données ne sont envoyées que bit par bit (0 ou 1).
- Le bus parallèle : c'est le bus qui communique avec le port parallèle, qui sert à brancher l'imprimante, le scanner, des graveurs externes, etc... Il est 8 fois plus rapide que le port série (les informations sont transmises par tranche de 8 bit en parallèle, soit 1 octet à la fois), mais toujours lent si on le compare aux bus USB et FIREWIRE.

- Le bus USB (Universal Serial Bus) : il est largement plus rapide que le bus parallèle et peut aller à la vitesse de 1.5 Mo par seconde pour l'USB 1.1. L'USB 2.0 peut quant à lui monter à 60 Mo par seconde ! Il est relié au port USB qui sert à brancher presque tous les périphériques du marché : webcams, modems, imprimantes, scanners, manettes de jeu...
- Le bus FIREWIRE : il permet de brancher 63 périphériques et offre des caractéristiques semblables à l'USB, en beaucoup plus performant : le bus FIREWIRE permet d'atteindre de 25 à 100 Mo par seconde ! Défaut : les périphériques qui se branchent sur ce type de port sont rares (et chers).
- Le bus ISA (industry standard architecture) : c'est le bus archaïque du PC avec le port série ! il fonctionne en 8 bit (1 octet) pour les ordinateurs anciens, ou 16 bit pour les ordinateurs récents disposant encore de ce type de bus. Son taux de transfert est d'environ 8 Mo par seconde pour le 8 bit et 16 Mo par seconde pour le 16 bit.
- Le bus PCI (peripheral component interconnect) : c'est le bus qui tend à être remplacé avec l'AGP par le bus PCI Express.
- Le bus AGP (accelerated graphic port) : Il est apparu avec le pentium II en 1997. Il permet de traiter 32 bit à la fois et a une fréquence de bus de 66 MHz. Sa qualité : sa rapidité (500 Mo par seconde pour le 2 X et 1 Go pour le 4 X, et maintenant 2 Go par seconde pour le 8x). Il communique avec le port AGP.
- Le bus PCI Express : allant de 250 Mo/s à 4 Go/s via ses nombreuses déclinaisons (1X, 2X, 4X, 8X, 16X) il va remplacer à terme les bus PCI et AGP.

➤ Les connecteurs IDE :

Ils servent à brancher les disques durs, lecteurs et graveurs de CDROM / DVDROM, systèmes de sauvegardes internes et autres périphériques à cette norme. Ils sont soit au nombre de 2, soit au nombre de 4 sur la carte mère. Chaque connecteur IDE permet d'accueillir 2 périphériques à la norme IDE sur la même nappe. Il en résulte qu'avec 2 connecteurs IDE vous pouvez brancher 4 périphériques à cette norme ce qui est suffisant dans la plupart des cas.

➤ Connecteurs E/S :



➤ Pile du CMOS :

C'est la pile qui permet de conserver les données dans la ROM (mémoire morte) après l'arrêt de l'ordinateur.

Lorsque vous éteignez l'ordinateur, il conserve l'heure et tous les paramètres qui lui permettent de démarrer correctement. Cela vient d'une pile plate au format pile bouton. Le CMOS est une mémoire lente mais qui consomme peu d'énergie, voilà pourquoi on

l'utilise dans nos PC alimentés par des piles à l'arrêt. Si l'heure de votre PC commence à retarder ou si elle change brutalement, changez la pile. Enlever la pile permet aussi de restaurer les paramètres par défaut du BIOS. Si vous avez touché au BIOS et que par malchance votre PC ne démarre plus, enlevez puis remettez la pile peu de temps après.

➤ BIOS :

Le BIOS (Basic Input/Output System) est un petit logiciel essentiel, il contrôle les éléments matériels, gère les périphériques et fait fonctionner les applications. En effet il permet au PC de booter (démarrer) et d'initialiser les périphériques avant de passer le relais au système d'exploitation (Windows, Linux...).

➤ Processeur :

Le processeur (CPU, soit Central Processing Unit, qui veut dire en français « Unité Centrale de Traitement ») est un composant essentiel d'un ordinateur. Le processeur sert à interpréter les ordres transmis par les programmes. Chaque tâche effectuée sur un ordinateur est due au processeur qui interprète chaque information numérique (sous forme binaire) qui lui est transmise. Il s'occupe aussi de transmettre des données à la carte graphique (et à d'autres composants tel que la carte son, etc.) qui permet à cette dernière d'interpréter et d'afficher sur le moniteur l'image correspondante. Le processeur est donc, en quelque sorte le cerveau de l'ordinateur.

Les performances du CPU sont jugées sur deux éléments :

- La puissance de calcul : elle se mesure au nombre de bits que le processeur est capable de traiter (32 ou 64). On peut comparer le nombre de bits aux couloirs d'une autoroute : plus ils sont nombreux, plus le trafic peut être fluide
- Leur cadence ou fréquence, improprement appelée « vitesse ».

La fréquence du processeur est définie en Hertz (Hz), 1 Hz correspond à 1 impulsion et, à chaque impulsion, le processeur exécute une instruction ou partie d'instruction.

Actuellement, la montée en puissance des processeurs s'évalue en gigahertz, c'est à dire en milliards de cycles par seconde. De nos jours, les PC sont cadencés à plus de 4 GHz. La fréquence d'horloge est généralement un multiple de la fréquence du système (FSB : Front-side Bus) à savoir un multiple de la fréquence de la carte mère.

Unités de mesure : MHz : mégahertz : million de HZ
 GHz : gigahertz : milliard de HZ

Ex : CPU cadencé à **3,6 GHz** est capable d'exécuter **3 milliard 600 millions d'instructions par seconde**.

Il est important de connaître la cadence ou fréquence (vitesse) de son processeur lorsqu'on veut utiliser certains logiciels comme des jeux. Pour certains il est indiqué la **fréquence minimum** du processeur pour un bon fonctionnement, **si la vitesse est moindre le programme ne fonctionnera pas, ou pas bien** (ex pour les jeux : image qui se fige ou le jeu ne répond pas aux commandes du joueur).

Le premier microprocesseur date de 1971. Il était cadencé à 108 KHz.

Fin 2007, la fréquence atteignant vraisemblablement ses limites, notamment au niveau de la surchauffe, il n'y a plus de processeur simple core (un seul cœur), c'est la génération des « double cœur » actuellement déjà dépassée.



Un processeur multi-core ou multi-cœur est un processeur ayant deux ou plusieurs noyaux indépendants. Ces noyaux ou cœurs sont les unités de calculs, situées au sein de tout processeur. C'est en 2005 que sont arrivés les premiers processeurs double cœur (« dual

core » en anglais) conçus par AMD et Intel. Les processeurs multi-core ont été mis au point pour augmenter la puissance d'un PC, sans accroître la fréquence de l'horloge du processeur. En outre, la nouvelle technologie permet de diminuer la quantité de chaleur. Actuellement, la technologie des processeurs se base sur la multiplication des cœurs.

Exemple chez Intel : Intel Core i7 : Processeur à 4 cœurs réels mais 8 cœurs virtuels grâce à une technologie appelée hyper-threading (HT) qui divise tous les processeurs en 2.



➤ Connecteur d'alimentation :

C'est le connecteur qui relie la carte mère à l'alimentation.

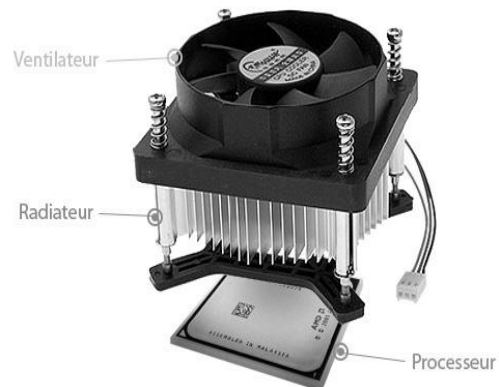
➤ Ventilateurs et radiateurs

Généralement, il y a un ventilateur à l'avant de l'unité centrale, chargé de capter l'air frais extérieur. A l'arrière, un autre ventilateur va expulser de l'air chaud, créant de ce fait un courant d'air.

Astuce : placez votre unité centrale de manière à ce que le ventilateur arrière ne soit pas contre une paroi ou un mur, afin qu'il puisse expulser l'air chaud correctement.

Le ventilateur est une pièce d'usure, c'est pour cette raison que votre ordinateur devient bruyant au fil du temps.

Le radiateur est une pièce métallique composée de fines lamelles espacées afin de capter la chaleur et la diffuser rapidement. Le processeur, qui chauffe beaucoup, possède un radiateur juste au dessus, surmonté lui-même d'un ventilateur.



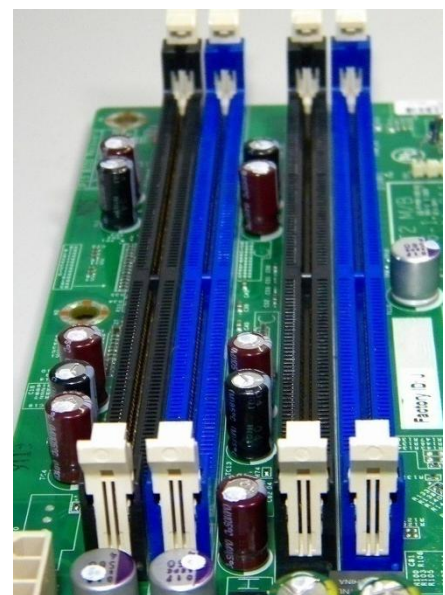
➤ Les connecteurs pour la RAM (Random Access Memory)

1.2. Les mémoires

a) La mémoire vive, aussi appelée RAM

Random Access Memory, ce qui veut dire mémoire à accès aléatoire c'est la **mémoire centrale** de l'ordinateur, elle permet de stocker les données lors de l'exécution d'un programme. Ce stockage est temporaire, contrairement à une mémoire de masse comme le disque dur, car elle ne permet de stocker des données que tant qu'elle est alimentée électriquement. A chaque fois que l'ordinateur est éteint, toutes les données présentes en mémoire vive sont complètement effacées. Il faut faire attention à ne pas la confondre avec le disque dur !

Les barrettes de RAM s'enfichent sur la carte mère dans des emplacements spéciaux (grands connecteurs généralement noirs ou bleus, terminés par une languette en plastique blanche à chaque extrémité):



On distingue généralement deux grandes catégories de mémoires vives :

- Les **mémoires dynamiques (DRAM, Dynamic Random Access Module)**, peu coûteuses. Elles sont principalement utilisées pour la mémoire centrale de l'ordinateur ;
- Les **mémoires statiques (SRAM, Static Random Access Module)**, rapides et onéreuses. Les SRAM sont notamment utilisées pour les mémoires cache du processeur.

La **fréquence de fonctionnement** est mesurée en Mégahertz. Elle permet de calculer la vitesse de la *bande passante* qui mesure le nombre d'octets transmis en une seconde :

Vitesse de la bande passante = Fréquence de la mémoire (en MHz) x nombre d'octets de la mémoire.

Exemple : sachant que les mémoires SDRAM et DDR-SDRAM fonctionnent avec des données de 64 bits (soit 8 octets), quelle est la vitesse de la bande passante d'une SDRAM et d'une DDR-SDRAM à 133 MHz ?

----> La mémoire SDRAM aura une bande passante de $133 \times 8 = 1050$ Mo/seconde ou 1Go/s.

----> La mémoire DDR-SDRAM aura une bande passante de $2 \times 133 \times 8 = 2100$ Mo/seconde ou 2,1 Go/s (le coefficient 2 étant dû au fait qu'elle est en DDR-SDRAM). Une demi-page contient à peu près 1000 octets.

Une barrette contient 1, 2, 4 et maintenant 8 et bientôt 16 Go (GB).

Types de RAM :

- **DRAM EDO**

Ce type de mémoire est apparu en 1995, il disparu au profit de la mémoire SDRAM

- **SDRAM**

Ce type de mémoire est apparu en 1997 pour remplacer la mémoire EDO. Génération des processeurs Pentium 1, 2 et 3.

- **RDRAM**

C'est une technique de mémoire vive développée par la société Rambus. Elle a eu une forte publicité autour de l'an 2000 lors de la sortie des premiers processeurs Pentium 4. Ce type de mémoire étant très cher, Intel l'a abandonné rapidement au profit de la DDR- SDRAM (et ses versions suivantes).

- **DDR-SDRAM**

Ce type de mémoire existe dans différentes fréquences (266, 333 et 400 MHz). Il est utilisé avec les processeurs Intel Pentium 4 et les processeurs AMD Athlon.

- **DDR2-SDRAM , DDR3-SDRAM**

La DDR2 a eu son heure de gloire pendant plusieurs années. Actuellement, la DDR3 s'est généralisée. Deux fois plus "rapide" (en terme de débit de données) que de la mémoire DDR2-SDRAM classique de même fréquence interne, elle est la mémoire la plus recommandée actuellement pour une plate forme neuve.

Remarque : Physiquement, les différents types de RAM se distinguent par une encoche les empêchant de se monter sur une carte mère qui ne les supporte pas.

- La **XDR DRAM**

C'est l'évolution la plus récente de la RDRAM.

Elle est basée sur la technique Rambus, concurrente des techniques DDR3 SDRAM, mais

elle est actuellement plus onéreuse.

Comment connaître la quantité de mémoire dont on dispose ?

En effet il est important de connaître la quantité de mémoire disponible pour le système, mais aussi pour l'utilisation de logiciels comme par exemple certains jeux ou applications de traitements d'images.

- o Sous XP : allez dans le menu «*Démarrer*» et sélectionnez «*Panneau de configuration*», ouvrez vos informations système en double cliquant sur l'icône "Système".
- o Sous Vista : «*Démarrer*», cliquez sur «*Panneau de configuration*». Dans la fenêtre du panneau de configuration, cliquez sur «*Système et maintenance*», cliquez sur «*Afficher la quantité de mémoire RAM et la vitesse du processeur*»
- o Sous Win 7 : Cliquez sur «*Démarrer*» puis sur «*Panneau de configuration*». Dans la fenêtre du panneau de configuration, cliquez sur «*Système et sécurité*» puis cliquez sur «*Système*».

Quelle est la quantité de Ram nécessaire au bon fonctionnement de votre PC ?

Tout dépend du système d'exploitation et de l'utilisation du PC. Plus la quantité de mémoire est importante, plus le gain en performances sera significatif.

Exemples : Les valeurs suivantes sont des minimas donnés à titre indicatif. Ces valeurs peuvent varier en fonction du processeur et des périphériques installés.

- o OS : Windows XP
Utilisation : Bureautique + surf Internet
RAM : 256 Mo mini, 512 Mo pour l'utilisation simultanée de plusieurs applications.
- o OS : Windows XP
Utilisation : Jeux 3D moyennement gourmands, traitement d'images courant (photo).
RAM : 512 Mo mini.
- o OS : Windows XP
Utilisation : Jeux 3D récents, édition vidéo.
RAM : 1024 Mo mini.
- o OS : Windows Vista (sans interface Aero)
Utilisation : Bureautique + surf Internet
RAM : 512 Mo mini.
- o OS : Windows Vista (avec interface Aero)
Utilisation : Bureautique + surf Internet
RAM : 1 Go mini (avec une carte graphique puissante).
- o OS : Windows Vista (avec interface Aero)
Utilisation : Jeux 3D récents + édition vidéo
RAM : 1,5 à 2 Go suivant le jeu (avec une carte graphique puissante).
- o OS: Windows Seven (sans Interface Aero)
Utilisation: Bureautique, Internet
RAM: 1Go, 512 mo mini.
- o OS: Windows Seven (avec Interface Aero)
Utilisation: Bureautique. Internet
RAM: 1Go mini, 2Go recommandés.
- o OS: Windows Seven (avec Interface Aero)
Utilisation: Jeux 3D
RAM: 1,5 à 2Go mini.

Lorsqu'il n'y a plus suffisamment de mémoire, le système utilise le disque dur comme mémoire de secours, c'est ce que l'on appelle la **mémoire virtuelle**. Cette mémoire physique est alors divisée en unités appelées « pages ».

Différents noms désignent cette technique : fichier pagefile.sys, fichier d'échange, fichier SWAP. Mais l'accès disque peut être jusqu'à 100 fois moins rapide que l'accès à des mémoires RAM, d'où un ralentissement des calculs.

Idéalement, on réglerait la taille de la mémoire virtuelle à 1,5 fois la quantité de RAM installée. Pour régler la taille de la mémoire virtuelle, allez à :

- Démarrer > Panneau de configuration > Système
 - Sous Vista : Paramètres système avancés
 - Sous les autres Windows : Avancé
- Sous "Performances", cliquez sur "Paramètres"
- Allez sous l'onglet "Avancé"
- Sous "Mémoire virtuelle", cliquez sur "Modifier"
- Définir la quantité de mémoire vive sur un disque vélocité et disposant de suffisamment d'espace libre, en fonction des critères suivants :
 - Taille initiale = 1,5 fois la quantité de RAM installée.
 - Taille maximale = 2 fois la taille initiale.

b) La mémoire de masse

Appelée également *mémoire physique* ou *mémoire externe* permettant de stocker des informations à long terme, y compris lors de l'arrêt de l'ordinateur. La mémoire de masse correspond aux dispositifs de stockage magnétiques, tels que le disque dur, aux dispositifs de stockage optique, correspondant par exemple aux CD-ROM ou aux DVD-ROM, ainsi qu'aux mémoires mortes.

La **mémoire morte**, appelée **ROM** pour *Read Only Memory* (traduisez *mémoire en lecture seule*) est un type de mémoire permettant de conserver les informations qui y sont contenues même lorsque la mémoire n'est plus alimentée électriquement. A la base ce type de mémoire ne peut être accédé qu'en lecture. Toutefois il est désormais possible d'enregistrer des informations dans certaines mémoires de type ROM.

Ce type de mémoire permet notamment de conserver les données nécessaires au démarrage de l'ordinateur. En effet, ces informations ne peuvent être stockées sur le disque dur étant donné que les paramètres du disque (essentiels à son initialisation) font partie de ces données vitales à l'amorçage.

Différentes mémoires de type ROM contiennent des données indispensables au démarrage, c'est-à-dire :

- Le BIOS est un programme permettant de piloter les interfaces d'entrée-sortie principales du système, d'où le nom de *BIOS ROM* donné parfois à la puce de mémoire morte de la carte-mère qui l'héberge.
- Le **chargeur d'amorce**: un programme permettant de charger le système d'exploitation en mémoire (vive) et de le lancer. Celui-ci cherche généralement le système d'exploitation sur le lecteur de disquette, puis sur le disque dur, ce qui permet de pouvoir lancer le système d'exploitation à partir d'une disquette système en cas de dysfonctionnement du système installé sur le disque dur.
- Le **Setup CMOS**, c'est l'écran disponible à l'allumage de l'ordinateur permettant de modifier les paramètres du système (souvent appelé *BIOS* à tort...).

- Le **Power-On Self Test (POST)**, programme exécuté automatiquement à l'amorçage du système permettant de faire un test du système (c'est pour cela par exemple que vous voyez le système "compter" la RAM au démarrage).

c) La mémoire cache

La mémoire cache a fait son apparition vers les années 80, elle est placée près du processeur, voire greffée sur ce dernier. Étant encore plus rapide que la RAM, **le processeur s'en sert pour stocker les données auxquelles il accède particulièrement souvent**, réduisant d'autant le temps de latence entre deux requêtes. La mémoire fait office de tampon entre le processeur et la mémoire vive.

Si cette mémoire est jusqu'à 10 fois plus rapide que la RAM, elle a cependant une capacité beaucoup plus limitée, notamment pour une question de prix. Pour disposer d'un système équilibré, il faut donc combiner différents types de mémoires plus ou moins rapides et onéreuses (en prenant également en compte les temps d'accès et tant de cycle).

Il peut y avoir de nombreux caches pour un seul processeur, chacun pouvant se spécialiser dans un jeu d'instruction particulier. Un cache peut même être placé entre le processeur et un autre cache, si cela peut servir les performances. Ainsi, plus le processeur est rapide, plus il profitera d'un grand nombre de mémoires caches (sans quoi ses capacités ne pourront être exploitées au mieux).

La hiérarchie mémoire : Si on classe les mémoires selon les critères *prix* et *temps d'accès*, en commençant par le niveau de hiérarchie le plus haut, on aurait :

- la mémoire cache de Niveau 1 (la plus chère, la plus rapide et se trouvant à l'intérieur du processeur)
- la mémoire cache de Niveau 2 (SRAM = RAM statique)
- la RAM classique (DRAM = RAM dynamique)
- le disque dur

1.3. Le disque dur

Le **disque dur** est l'organe de l'ordinateur servant à conserver les données de manière permanente, contrairement à la mémoire vive, qui s'efface à chaque redémarrage de l'ordinateur, c'est la raison pour laquelle on parle parfois de mémoire de masse pour désigner les disques durs.

Le disque dur est relié à la carte-mère par l'intermédiaire d'un **contrôleur de disque dur** faisant l'interface entre le processeur et le disque dur. Le contrôleur de disque dur gère les disques qui lui sont reliés, interprète les commandes envoyées par le processeur et les achemine au disque concerné. On distingue généralement les interfaces suivantes :

- IDE (PATA), le + ancien. Sa nappe est encombrante et difficile à déclipser. Cette technologie lente est limitée à 133Mo/s
- Serial ATA (SATA) : le débit maximal théorique du SATA I (Serial ATA) se situe à 150 Mo/s et le SATA II à 300 Mo/s. Plus performant il est aussi plus facile à clipser. Moins encombrant,



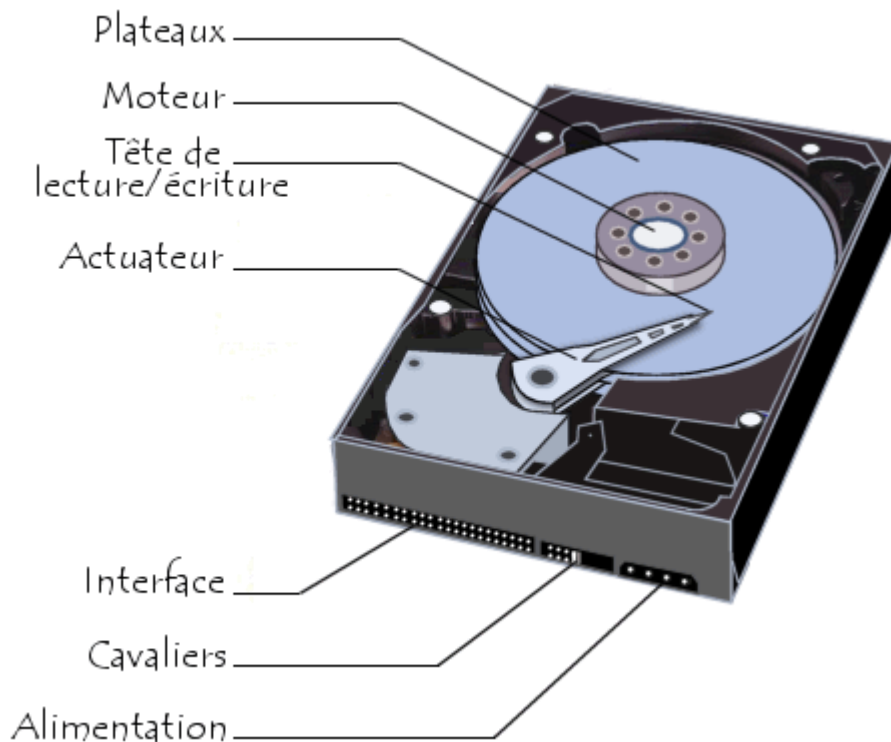
il permet une meilleure ventilation dans le boîtier. Contrairement à l'IDE qui supporte deux périphériques, le SATA profite pleinement de toute la bande passante du contrôleur. Plus performant en terme de vitesse de transfert, il est également *hot plug* et peut être débranché à chaud. Fini également le positionnement du *jumper* en maître/esclave.

- SCSI : pour les serveurs, très rapide et surtout très cher.

Avec l'apparition de la norme USB, des boîtiers externes permettant de connecter un disque dur sur un port USB ont fait leur apparition, rendant le disque dur facile à installer et permettant de rajouter de la capacité de stockage pour faire des sauvegardes. On parle ainsi de **disque dur externe** par opposition aux disques durs internes branchés directement sur la carte mère.

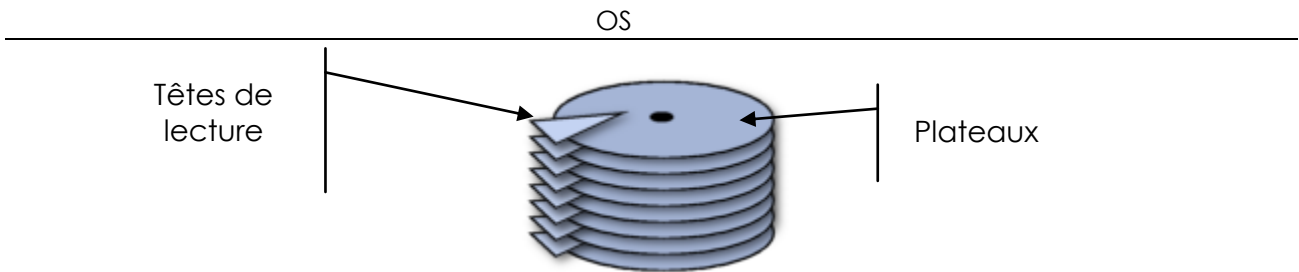
a) Structure

Un **disque** dur est constitué non pas d'un seul disque, mais de plusieurs disques rigides (en anglais *hard disk* signifie *disque dur*) en métal, en verre ou en céramique, empilés à une très faible distance les uns des autres et appelés **plateaux** (en anglais *platters*).



Ces disques tournent très rapidement autour d'un axe.

La lecture et l'écriture se font grâce à des **têtes de lecture** situées de part et d'autre de chacun des **plateaux**, elles survolent à quelques microns les plateaux. Si une tête touche un plateau, il devient inutilisable. De plus ces têtes sont mobiles latéralement afin de pouvoir balayer l'ensemble de la surface du disque.



Cependant, les têtes sont liées entre elles et une tête seulement peut lire ou écrire à un moment donné. On parle donc de **cylindre** pour désigner l'ensemble des données stockées verticalement sur la totalité des disques.

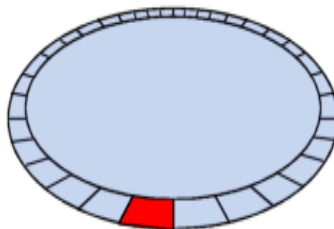
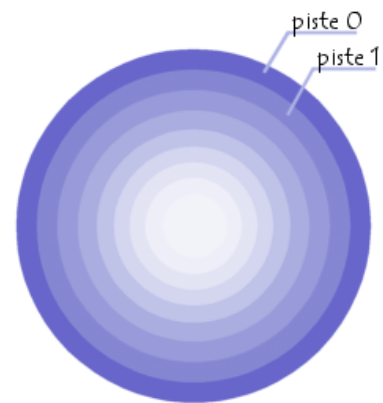
L'ensemble de cette mécanique de précision est contenu dans un boîtier totalement hermétique, car la moindre particule peut détériorer la surface du disque.

b) Fonctionnement

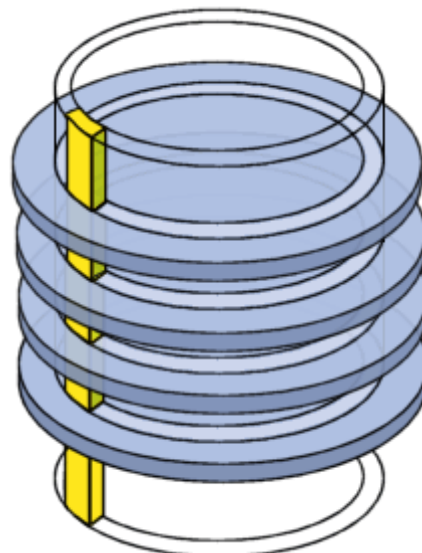
Les têtes commencent à inscrire des données à la périphérie du disque (piste 0), puis avancent vers le centre.

Les données sont organisées en cercles concentriques appelés «**pistes**», elles sont créées par le formatage de bas niveau.

Les pistes sont découpées en **secteurs** (de taille fixe) contenant les données (au minimum 512 octets par secteur en général).



On appelle **cylindre** l'ensemble des données situées sur une même piste sur des plateaux différents (c'est-à-dire à la verticale les unes des autres) car cela forme dans l'espace un "cylindre" de données :



Le formatage de haut niveau va alors créer les **clusters** (ou en français **unité d'allocation**), c'est la zone minimale que peut occuper un fichier sur le disque. Ces **blocs** sont composés de plusieurs **secteurs** (entre 1 et 16 secteurs). Un fichier minuscule devra donc occuper plusieurs secteurs (un cluster).

2) Les périphériques informatiques

Les termes « périphériques informatiques » désignent des composants de matériel informatique assurant les communications entre l'ordinateur et le monde extérieur.

Suivant le flux de communication on distingue trois types de périphériques :



Les périphériques d'entrée :

Pour entrer de l'info dans le PC

- Clavier
- Lecteur DVD-ROM
- Dispositifs de pointage
 - Souris
 - Tablette graphique
- Acquisition numérique
 - Scanner
 - Caméscope numérique
 - Appareil photo numérique
 - Lecteur de carte d'identité
 - Webcam
- Acquisition sonore
 - Microphone

Les périphériques d'entrée-sortie:

Pour faire entrer ou sortir de l'info.

- Lecteur de disquettes.
- Disque dur
- Lecteur graveur.
- Ecran tactile
- Lecteur de bandes magnétiques, notamment les bandes DAT utilisées pour sauvegarder les données sur les réseaux.
- Modem.
- Clé USB (mémoire flash amovible).

Les périphériques de sortie :

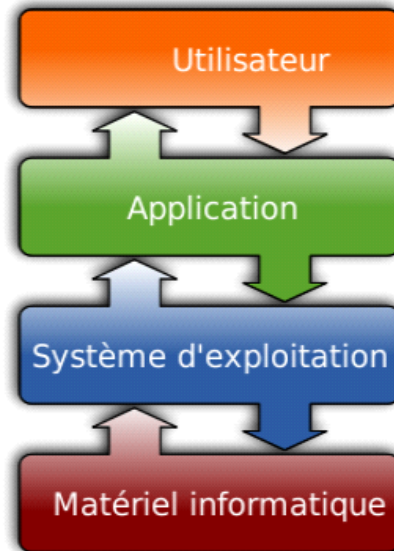
Pour sortir l'info du PC.

- Moniteur
- Imprimante
- Enceinte acoustique

Chapitre 3. Le système d'exploitation

Au démarrage, l'ordinateur a besoin d'un programme lui indiquant comment gérer tous ses périphériques et lui indiquant aussi comment communiquer avec l'utilisateur.

Ce programme s'appelle le **système d'exploitation** (noté SE ou OS, abréviation du terme anglais *Operating System*). Il est chargé d'assurer la liaison entre les ressources matérielles, l'utilisateur et les applications (traitement de texte, jeu vidéo, ...)



Il joue un grand rôle dans le transfert des données entre le lecteur de disque dur, la mémoire vive, le microprocesseur et les autres périphériques. Le système d'exploitation retient l'emplacement de l'information sur les disques durs à partir d'un système de répertoires, tel que le **FAT32 (File Allocation System de 32 bits)**, ou encore le système de fichier **NTFS (New Technology File System)**, et peut ainsi retrouver l'information rapidement ou encore indiquer au lecteur de disque dur à quel endroit enregistrer les nouvelles données.

Par exemple, lorsqu'un texte est tapé dans un traitement de texte puis enregistré, l'information est transmise de la mémoire vive (qui contient l'information du logiciel de traitement de texte) vers le microprocesseur (guidé par le système d'exploitation) qui transfère les données dans le câble IDE ou SCSI qui se rendent jusqu'à la mémoire cache, de capacité 512 Ko à 8 Mo, située sur la carte de circuit du lecteur de disque dur qui transmet les données à la tête de lecture/écriture qui enregistre l'information sur le disque dur à l'emplacement précisé par le système d'exploitation.

1) Principales tâches

Gestion des entrées/sorties : le système d'exploitation permet d'unifier et de contrôler l'accès des programmes aux ressources matérielles par l'intermédiaire des pilotes.



Gestion du processeur : la principale tâche du système d'exploitation concerne l'allocation du processeur aux processus. Il s'agit de décider quel processus s'exécute à un moment donné, à quel moment interrompre le processus, quel sera le suivant, et de quoi il a besoin comme ressources pour son exécution.

Gestion de la mémoire centrale (mémoire vive) : il s'agit ici de gérer l'allocation de cette mémoire aux programmes (attribution, libération de mémoire). En cas d'insuffisance de mémoire physique, le système d'exploitation peut créer une zone mémoire sur le disque dur, appelée «**mémoire virtuelle**» qui permet de faire fonctionner des applications.


Gestion des fichiers : le système est chargé de l'organisation des données enregistrées sur les volumes.

2) Les systèmes d'exploitation les plus connus

2.1. Microsoft Windows

<p>Basé sur DOS (de Microsoft Disk Operating System)</p> <p>Il s'agit d'un système fonctionnant en mode réel, mono-tâche et mono-utilisateur, et équipé par défaut d'une interface en ligne de commande. Des années 1980 au début des années 1990, il a été le système le plus utilisé sur compatible PC, avant d'être progressivement remplacé par des systèmes d'exploitation plus évolués, notamment Windows. Son développement est maintenant arrêté.</p>	<p>MS-DOS ·3.x ·95 ·98 ·Me</p> 
<p>Branche NT (New Technology nouvelle technologie)</p> <p>Il désigne la série de systèmes d'exploitation multitâche préemptif, multi-utilisateur, multiprocesseur, créés par Microsoft et ne reposant pas sur le système historique MS-DOS</p>	<p>NT ·2000 ·XP ·2003 ·Vista ·2008 ·Win7</p> 

2.2. Apple

<p>Mac OS Classic (Macintosh Operating System)</p> <p>Nom du système d'exploitation d'Apple pour ses ordinateurs Macintosh</p> <p>Dérivés de NeXTSTEP</p> <p>Suite au rachat de NeXT par Apple en 1996, NeXTSTEP devint le noyau de base de Mac OS pour donner naissance à Mac OS X.</p>	 <p>Système 5, Système 6, Système 7 Mac OS 8 · Mac OS 9</p> <p>NeXTSTEP ·Rhapsody ·Darwin ·Mac OS X (MacBook Pro et iMac) ·iOS</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


2.3. IBM

<p>(International Business Machines)</p> <p>Dès 1934, la filiale allemande d'IBM fournit au régime nazi des machines mécanographiques de poinçonnage de cartes perforées destinées aux recensements de la population. Ces cartes permirent aux nazis de se saisir rapidement et presque totalement des populations de Juifs et de Roms en Allemagne et, avec une efficacité plus variable, dans les autres pays sous domination allemande.</p> <p>Dès 1993, après avoir créé des ordinateurs de grande puissance de traitement destinés aux grandes entreprises, IBM se centre sur les services. Depuis 2002, IBM est devenu la 1ère entité de conseil dans le monde entier.</p>	<p>AIX · MVS · OS/2 · OS/360 · OS/390 · z/OS · OS/400</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------

2.4. UNIX

C'est un système d'exploitation multitâche et multiutilisateur créé en 1969.

Il a donné naissance à une famille de systèmes dont un ensemble de standards réunis sous la norme POSIX vise à unifier certains aspects de leur fonctionnement.

 <p>GNU/Linux(souvent appelé <i>Linux</i>) C'est un système d'exploitation libre s'appuyant sur les outils GNU fonctionnant avec le noyau Linux.</p>	Debian GNU/Hurd · Arch Hurd · Arch Linux · Debian Frugalware Fedora Funtoo · Gentoo · Mandriva Red Hat · Slackware · SUSE · Ubuntu, ETC.
<p>BSD désigne en informatique une famille de systèmes d'exploitation Unix, développés à l'Université de Californie (Berkeley) entre 1977 et 1995</p>	FreeBSD · NetBSD · OpenBSD · DragonFly BSD · PC-BSD Darwin sur lequel est construit le noyau de Mac OS X
<p>Autres dérivés</p>	AIX · HP-UX · IRIX · LynxOS · Minix · QNX · Solaris · SystemV · Tru64 · UnixWare · ChorusOS

2.5. Système d'exploitation mobile

 <p>système d'exploitation conçu pour fonctionner sur un appareil mobile (smartphones, tablettes numériques,...)</p>	Android · Bada · BlackBerry OS · Cisco IOS · iOS · Palm OS · webOS · Symbian OS · Windows CE · Windows Mobile, Etc.
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------

3) Caractéristiques d'un système d'exploitation

○ **Multi-utilisateurs :**

Possibilité de travailler à plusieurs sur la même machine. Chaque utilisateur peut configurer son espace de travail, a ses propres fichiers, etc...

○ **Monotâche (DOS) :**

À tout instant, un seul programme est exécuté; un autre programme ne démarrera que lorsque le premier sera fermé.

○ **Monosession (Windows 95-98) :**

Au maximum un utilisateur à la fois sur une machine. Les systèmes réseaux permettent de différencier plusieurs utilisateurs, mais chacun d'eux utilise de manière exclusive la machine (multi-utilisateur, monosession)

○ **Multisession (Windows XP et les suivants, Linux, Mac) :**

Plusieurs utilisateurs peuvent travailler simultanément. Le système d'exploitation est capable de partager ses ressources entre plusieurs sessions d'utilisateurs connectés en même temps et de créer un espace distinct de traitement entre chaque session.

○ **Multitâche (Windows, Linux, Mac) :**

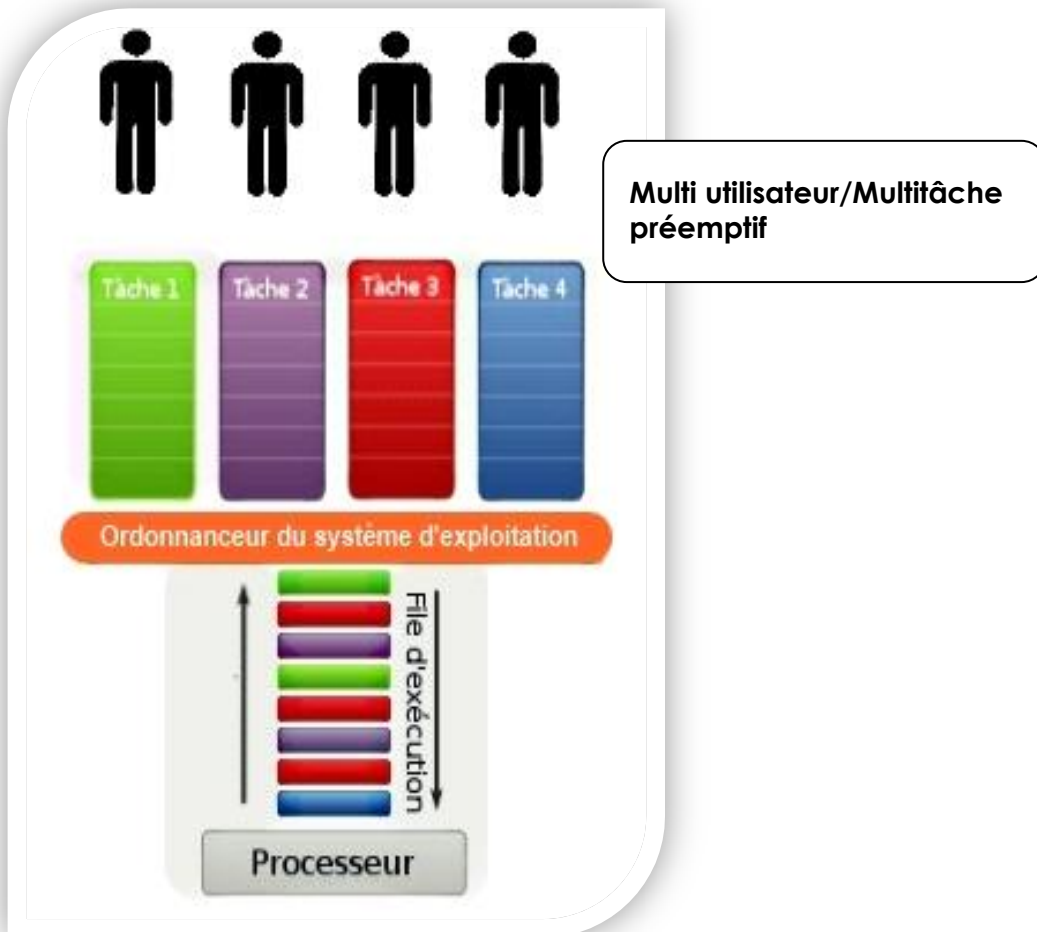
Le système d'exploitation est capable d'exécuter simultanément plusieurs tâches, d'exécuter plusieurs programmes et processus en partageant les ressources.

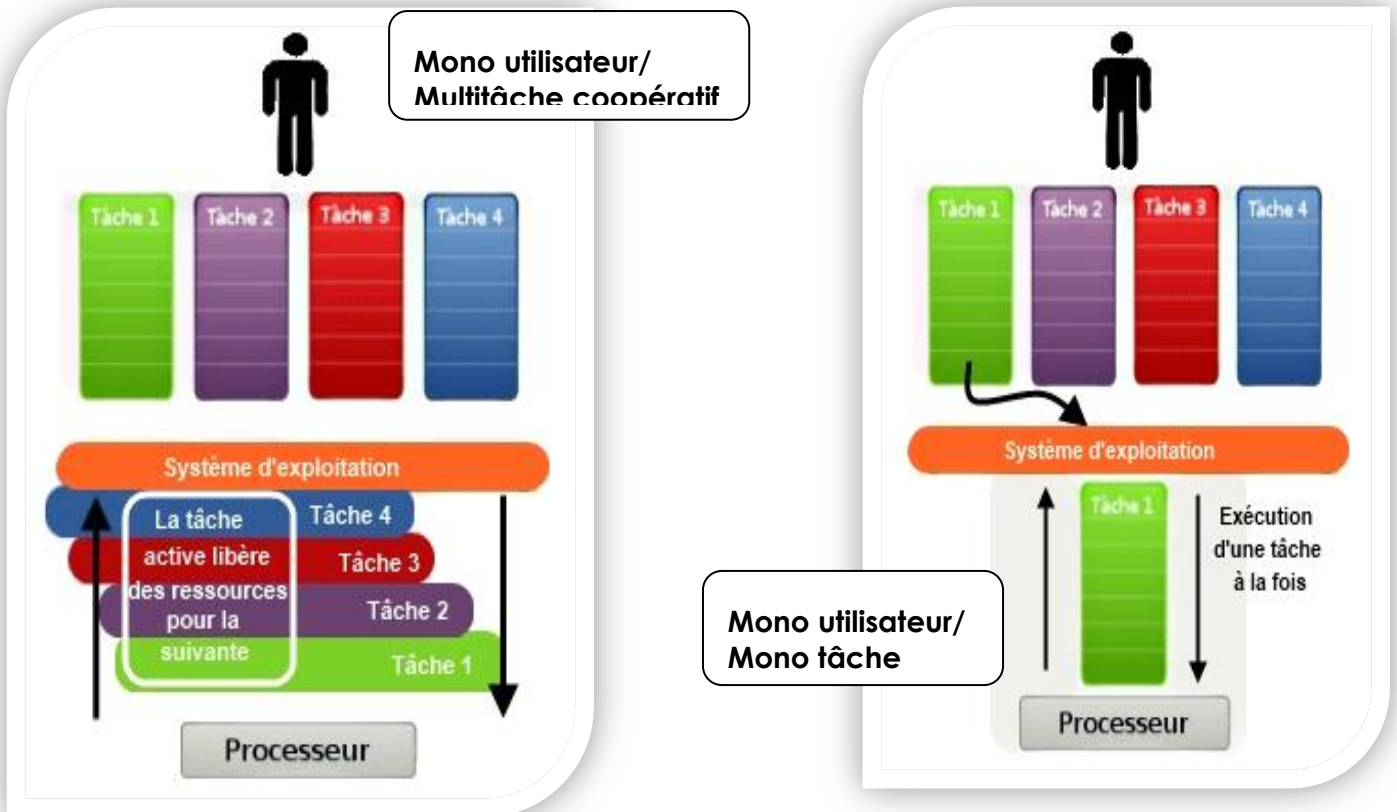
Il existe deux types de fonctionnement multitâches :

- **Le multitâche coopératif** (ex. Windows 95, 98, Millenium) : il revient aux applications actives de se répartir elles-mêmes le temps de calcul. Il n'existe alors aucune hiérarchie entre les différentes applications.

- **Le multitâche préemptif** (Linux, Windows 2000 et les suivants) : un module du système d'exploitation se charge de partager de façon équilibrée le temps de calcul entre les différents programmes actifs. Une notion de priorité lui permet de hiérarchiser les programmes. Cette priorité est appelée l'ordonnancement et est gérée par un **Ordonnanceur**.

Quelques représentations de systèmes d'exploitation :





3.1. Liste des systèmes les plus courants et de leurs caractéristiques.

Système	Codage	Mono-utilisateur	Multi-utilisateur	Mono tâche	Multitâche
DOS	16 bits	X		X	
Windows3.1	16/32 bits	X			non préemptif
Windows95/98/Me	32 bits	X			coopératif
WindowsNT/2000	32 bits		X		préemptif
WindowsXP	32/64 bits		X		préemptif
Windows7	32/64 bits		X		préemptif
Unix / Linux	32/64 bits		X		préemptif
MAC/OS X	32 bits		X		préemptif
(Open)VMS, employé au sein des institutions bancaires, militaires, industrielles	32 bits		X		préemptif

Quelques autres caractéristiques :

Les processeurs multi-cœurs favorisent un véritable fonctionnement multitâche.

Sur les systèmes mono-cœurs, le fonctionnement multitâche peut dépasser les capacités du processeur, entraînant une baisse des performances liée à la mise en attente des opérations à traiter. Sur les systèmes multi-cœurs, dans la mesure où chaque cœur dispose

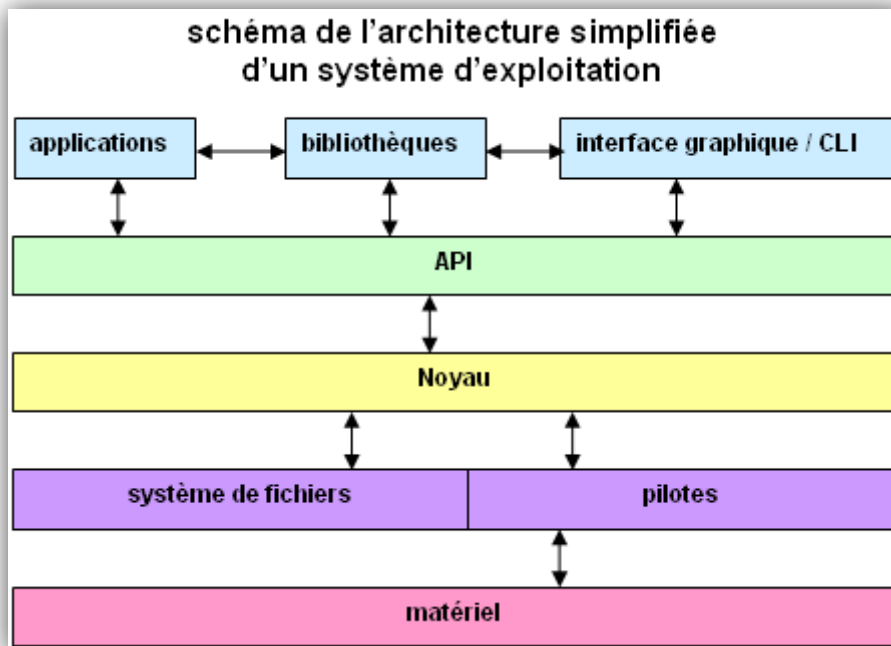
de sa propre mémoire cache, le système d'exploitation dispose de suffisamment de ressources pour traiter en parallèle les tâches les plus exigeantes en calculs.

Les **systèmes embarqués** sont des systèmes d'exploitation prévus pour fonctionner sur des machines de petite taille, telles que des PDA (*personal digital assistants* ou en français *assistants numériques personnels*) ou des appareils électroniques autonomes (sondes spatiales, robot, ordinateur de bord de véhicule, etc.), possédant une autonomie réduite. Ainsi, une caractéristique essentielle des systèmes embarqués est leur gestion avancée de l'énergie et leur capacité à fonctionner avec des ressources limitées.

Les systèmes informatiques temps réel se différencient des autres systèmes informatiques par la prise en compte de contraintes temporelles dont le respect est aussi important que l'exactitude du résultat, autrement dit le système ne doit pas simplement délivrer des résultats exacts, il doit les délivrer dans des délais imposés. Les systèmes informatiques temps réel sont aujourd'hui présents dans de nombreux secteurs d'activités (systèmes de contrôle de procédé dans les usines, les centrales nucléaires, traitement des données boursières en « temps réel », etc...).

N.B. Un programme peut engendrer plusieurs processus simultanés et indépendants sans bloquer grâce à une technique de conception de logiciel (*multi-threading*) où l'utilisateur peut continuer d'interagir avec le programme même lorsque celui-ci est en train d'exécuter une tâche. Une application pratique se retrouve dans les traitements de texte où la correction orthographique est exécutée tout en permettant à l'utilisateur de continuer à entrer son texte.

4) Organisation d'un système d'exploitation



4.1. Les bibliothèques

Les bibliothèques mettent à disposition du système d'exploitation et des programmes applicatifs des morceaux de programmes tout prêts, dont le but est de faciliter l'accès à certaines fonctions. Grâce aux bibliothèques (.dll, .OCX, ...), les développeurs peuvent facilement et rapidement réutiliser des fonctions utiles, sans avoir à les reprogrammer eux-mêmes.

4.2. L'interface homme machine

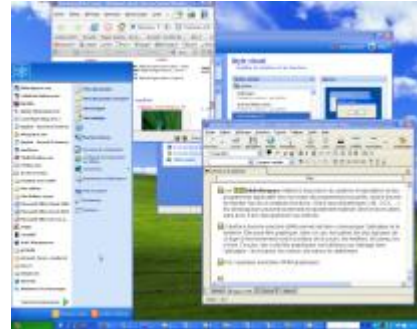
L'interface homme machine permet de faire communiquer l'utilisateur et le système. C'est d'ailleurs le shell ou DOS qui est un logiciel fournissant une interface pour un utilisateur qui se charge de cela. Elle peut être graphique (GUI, pour Graphical User Interface), dans ce cas les parties les plus typiques de ce type d'environnement sont le pointeur de la souris, les fenêtres, le bureau, les icônes. De plus, des contrôles graphiques sont utilisés pour interagir avec l'utilisateur : les boutons, les menus, les barres de défilement.

Voici quelques exemples d'IHM graphiques :

Windows Vista



Windows XP



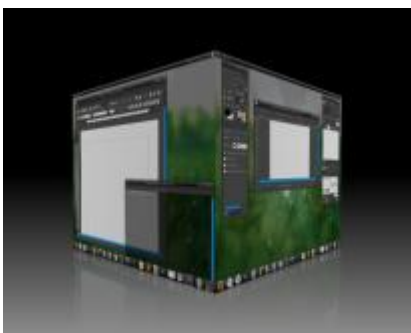
Ubuntu



Mac



Compiz fusion (3D) sous Ubuntu



Aero (3D) sous Windows Vista



Si l'interface de type graphique est la plus répandue, l'interface en ligne de commande (en anglais CLI pour Command Line Interface) reste très utilisée, notamment sur les machines ayant une configuration matérielle qui nécessite de faire des économies sur la mémoire utilisée (qui est très sollicitée par une interface graphique) ou bien souvent sur les serveurs. Une interface en ligne de commande propose une invite de commande qui a pour rôle le traitement des commandes tapées au clavier par l'utilisateur. Ces

commandes, une fois interprétées, auront pour effet de réaliser telle ou telle tâche d'administration, ou bien de lancer l'exécution d'un logiciel.

L'invite de commande sous MS-DOS (DOS de microsoft) débute par une lettre  et par le nom de l'utilisateur.

Le système d'exploitation est également pourvu d'un interpréteur de commande pour permettre à l'utilisateur de communiquer avec l'ordinateur et ses périphériques. Cet interpréteur de commande se nommait *Shell* sous les anciennes versions de Windows mais, depuis Windows7, il s'agit de *PowerShell*.

4.3. L'API (interface de programmation)

L'API est une interface de programmation (Application Programming Interface) qui permet de définir la manière dont un composant informatique peut communiquer avec un autre. Une API a pour objet de faciliter le travail d'un programmeur en lui fournissant les outils de base nécessaires à tout travail à l'aide d'un langage donné. Elle constitue une interface servant de fondement à un travail de programmation plus poussé.

Une API pour la programmation dans un langage x est ainsi composée d'un ensemble de fonctions, routines et méthodes, écrites dans ce langage. Ces fonctions de bas niveau (ouvrir un fichier, le fermer, ...) ont la propriété d'être d'un usage courant dans toutes les applications dérivées de x. D'où l'idée de les programmer une fois pour toutes puis de les mettre à disposition de la communauté des programmeurs. Ces derniers n'ont plus alors qu'à choisir et appeler les fonctions pertinentes selon les objectifs de leur code. Les API permettent d'assurer une certaine interopérabilité entre les applications et le système d'exploitation.

Pour exemple, l'API de windows XP est l'API System32.

4.4. Le noyau

Le programme principal gérant l'OS est appelé « noyau » ou *kernel* (de l'anglais). Il gère les ressources de l'ordinateur et permet aux différents composants (matériels et logiciels) de communiquer entre eux. C'est une véritable machine virtuelle. Le noyau est la partie la plus critique d'un système d'exploitation et rend sa conception et sa programmation particulièrement délicates.

Pour résumer, le noyau est le centre d'un système d'exploitation. C'est par lui que passent toutes les informations logicielles et matérielles; de plus, c'est lui qui valide toutes les actions.

Exemple: Quand vous faites un *scan* de dossier avec votre antivirus, celui-ci ne va pas chercher les virus directement dans votre dossier, mais il demande au noyau d'aller chercher l'information et c'est le noyau qui lui répond.

Le noyau d'un système d'exploitation assure :

- o la communication entre les logiciels et le matériel ;
- o la gestion des divers logiciels (tâches) d'une machine (lancement des programmes, organisation du travail suivant des critères de priorité. ...)
- o la gestion du matériel (mémoire, processeur, périphérique, stockage...).

4.5. Les pilotes :

Le système d'exploitation utilise des **pilotes de périphériques** souvent abrégés en **pilotes** ("*drivers*") pour interagir avec un périphérique. En général, chaque périphérique a son propre pilote. Sans pilote, l'imprimante ou la carte graphique par exemple ne pourraient pas être utilisées. Certains systèmes d'exploitation comme Windows proposent leurs propres pilotes génériques censés fonctionner de manière satisfaisante avec la plupart

des périphériques pour une utilisation courante. Si ces pilotes gèrent les grandes fonctions communes à tous les matériels, ils n'ont pas toujours toutes les capacités des pilotes de constructeurs, qui seuls connaissent parfaitement et en détail les spécifications du matériel piloté. Un pilote est programmé et compilé (*code machine*) pour un système d'exploitation bien précis ou, dans certains cas, une famille de système d'exploitation (Windows, Linux, MacOS ...). Il est toujours important de se renseigner sur l'existence ou non de pilote pour un nouveau périphérique compatible avec son système d'exploitation

4.6. Le système de fichiers

Chaque système d'exploitation dispose de son propre système de fichiers permettant, sur des périphériques de stockage (disque dur), d'enregistrer les fichiers, de créer de arborescences (dossiers) et de gérer, selon les cas, les droits d'accès à ceux-ci.

4.7. Les applications ou logiciels

Traduction du terme anglais Software, le logiciel constitue l'ensemble des programmes et des procédures nécessaires au fonctionnement d'un système informatique.

Il existe différents types de logiciels :

- le BIOS est le logiciel de bas niveau qui permet de faire fonctionner la carte mère d'un ordinateur personnel,
- Le système d'exploitation sert d'interface entre le matériel et les logiciels applicatifs.
- Un logiciel applicatif, le type de logiciel le plus courant, aussi appelé application informatique est destiné à assister un utilisateur dans une de ses activités.

Un logiciel est composé d'un ou plusieurs fichiers tels que :

- des programmes (extension « .exe ou .com »)
- des scripts : on peut distinguer 2 niveaux :
 - Un **langage de script** est un langage de programmation (ex : PHP pour le web, Python, ...).
 - Les langages *shell / bash* servent principalement à lancer et coordonner l'exécution de programmes (ex : .bat de Win ou .sh de linux).
- des bibliothèques logicielles ou librairies (sous Win .dll ou .ocx, sous Linux .so)
- des fichiers de configuration,
- des fichiers de données,
- des documents électroniques ou du code source.

4.8. Les fichiers de données des applications

Beaucoup de logiciels ont besoin de données externes au programme pour fonctionner.

Par exemple: Un jeu a besoin d'images, de représentations 3D, de sons, etc...
 Un traitement de texte nécessite de sauvegarder le travail en cours dans un fichier indépendant.
 Un lecteur MP3 lit les données dans un fichier externe au programme.

Les fichiers ont une **extension** qui les relie à une application installée sur l'ordinateur. Si plusieurs applications peuvent lire un même type de fichier, vous pouvez choisir l'une d'entre-elles comme application par défaut. L'extension d'un fichier indique l'origine (où le logiciel qui a permis la création du fichier) et la nature (ou le format) du document. Elle est placée après le nom de chaque fichier. Elle est composée d'un point et d'une série

de caractères (trois, en général). Suivant le mode d'affichage de vos fichiers, une icône est également associée à chaque fichier. Elle correspond au programme en lui-même

Voici une liste non exhaustive pour les extensions de fichiers les plus courantes :

➤ Pour des données essentiellement de type texte:

- **.DOC** : format propriétaire des fichiers texte du logiciel Word 2003 et versions antérieures
- **.DOCX** : idem pour Microsoft Word 2007 et 2010
- **.ODT** (format libre) : fichier texte du logiciel Writer, suites bureautiques OpenOffice et LibreOffice.



- **.TXT** (format libre) : texte brut universel (lisible par un grand nombre de logiciels) mais sans mise en forme.
- **.RTF** : fichier de traitement de texte au format standard Rich Text Format avec mise en forme.

L'intérêt du format RTF est de pouvoir être lu par la quasi-totalité des applications de bureautique et sur tous les systèmes d'exploitation (Windows, Mac, Linux, Unix, etc.).

Remarque : Writer d'OpenOffice ou Libreoffice permet d'ouvrir et travailler tous ces types de fichiers.

➤ Pour des données de type images, graphiques:

- **.BMP**: fichier image de base non compressé, fichier lourd, le plus simple des fichiers graphiques.



- **.JPEG** ou **.JPG** : fichier image compressé (16 millions de couleurs), la compression engendre une perte de données irréversible, mais le poids d'1 image jpg est beaucoup petit que celui d'1 .Raw ou .Tiff.
- **.GIF**: fichier image compressé avec transparence (256 couleurs).
- **.GIF ANIMÉ**: idem, mais permet des séquences d'images, animation.
- **.AI** : Adobe Illustrator - Fichier vectoriel avec textes, images, formes, multicalque, transparence, dégradés.
- **.ICO** : icône - Petite image que l'on associe à un programme ou une extension.
- **.PNG** : créé pour remplacer le GIF, 16 millions ou 256 couleurs.



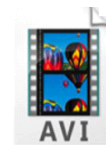
- **.PSD** : fichier Photoshop (Adobe) avec plusieurs couches, transparence.
- **.PSP** : fichier Paint Shop Pro (Jasc software) avec plusieurs couches, transparence.
- **.RAW** : créé pour les appareils photo numériques (APN), aucune perte.
- **.SVG** : Scalable Vector Graphics - Format de dessin vectoriel (logiciels d'édition : Inkscape, Skencil).
- **.TIFF/TIF** : compression sans perte.




➤ Pour les données de type audio :

- **.WAV** : format de base Microsoft non compressé.
- **.CDA** : *CD audio* - Pointeur vers une piste sur le CD. Ce n'est pas un fichier exploitable en tant que tel.
- **.MID** : fichier qui ne contient que les notes de musique.
- **.MP3** : format audio compressé, permettant de réduire la taille du fichier jusqu'à 10 fois par rapport à l'original de type WAV, CDA ...
- **.OGG** : *Ogg Vorbis* - Compressé mieux que le MP3. Sans brevet, ouvert et libre.
- **.RM, .RAM** : format propriétaire Real Player, utilisé sur Internet.
- **.WMA** : format compressé propriétaire Microsoft.
- **.M3U** : format développé pour stocker une liste de fichiers audio.
- **.AIF ou .AIFF** : format de fichier audionumérique développé par Apple pour stocker les sons sur les ordinateurs de la marque. Ce format n'est pas sans rappeler le format WAV de Microsoft.
- **.MP4** : format conteneur qui peut stocker l'audio numérique. Il est utilisé par MPEG-4, pour lire de la vidéo sur Internet
- **.FLAC** : format libre de compression audio sans perte. À l'inverse des MP3 ou Vorbis, il n'enlève aucune information du flux audio. Cette qualité maximale a pour conséquence un poids plus élevé, qui se trouve en moyenne être de l'ordre de 50% de la taille du même fichier au format WAV.


➤ Pour des données de type vidéo :



- **.AVI** : format de base non compressé spécifié par Microsoft.
- **.VOB** : fichiers utilisés sur les DVD vidéo.
- **.MPG, .MPEG** : format vidéo compressé MPEG1, MPEG2 (DVD), MPEG 4 (utilisé pour la compression des DivX et XVID).
- **.DIVX** : compression très forte des fichiers vidéo. 
- **.XVID** : similaire à DIVX mais c'est un logiciel libre (code source disponible et librement modifiable). DivX est distribué comme gratuit.
- **.DVD** : complet sur un CD.
- **.MOV** : format propriétaire (Quick Time d'Apple).
- **.WMV** : format propriétaire de vidéo compressée (Microsoft).
- **.FLV** : format de fichier utilisé sur Internet pour diffuser des vidéos.

➤ Pour des données compressées

Permet de compresser les données d'un fichier pour réduire sa taille ; pour certains fichiers textes, on peut diviser la taille de 10 à 50 fois ; notez qu'une image déjà compressée de type JPG gardera sa taille d'origine.

- **BZ2** : surtout utilisé dans le monde Unix, Linux.
- **TGZ** : surtout utilisé dans le monde Unix, Linux pour la compression des archives d'installation d'un programme.
- **CAB** : fichiers archives compressés de Microsoft. On les retrouve par exemple sur les cédéroms. d'installation de Microsoft Windows, ou de Microsoft Office.
- **RAR** : utilisé sous Linux, Windows (format propriétaire). 
- **ZIP** : utilisé sous Linux, Windows.

- **GZ** : surtout utilisé dans le monde Unix, Linux.

➤ Autres:



- **PDF** : fichier document de Adobe Acrobat Reader - format de document portable (mise en page « figée »).
- **XLS** : fichier du tableur Microsoft Excel avant 2007.
- **XLSX** : fichier du tableur Microsoft Excel sans macros à partir de 2007.
- **ODS** : fichier du tableur OpenOffice ou LibreOffice.
- **PPS, PPT** : fichier d'animation et de présentation de Microsoft PowerPoint avant 2007.
- **PPTX** : présentation PowerPoint à partir de 2007.
- **ODP** : fichier d'animation et de présentation OpenOffice ou LibreOffice.
- **CSV** : fichier de formatage des données, en les séparant par une virgule ou un point virgule (lisible avec Excel, Open Office).
- **HTML** : fichier de présentation de texte pour les pages Web.
- **XML** : fichier de formatage de données en mode texte (en quelque sorte un langage HTML amélioré permettant de définir de nouvelles balises).
- **MDB** : fichier Base de données de Microsoft Access avant 2007.
- **ACCDB** : fichier Base de données de Microsoft Access à partir de 2007.
- **ODF** : fichier Base de données OpenOffice ou LibreOffice.

N.B. OpenOffice et LibreOffice permettent de lire la plupart des formats du Pack Office.

5) Gestion d'un système d'exploitation

5.1. Arborescence du système et des fichiers

À la base d'une arborescence se trouve un répertoire appelé la racine (c:\). Ce répertoire peut contenir des fichiers et des répertoires, qui eux-mêmes peuvent en contenir.

En général, Windows 7 comporte une structure de dossiers similaire à Windows Vista. Cependant, vous remarquerez certaines différences. Par exemple, vous accéderez à la plupart de vos fichiers en utilisant les bibliothèques plutôt que les dossiers. Les bibliothèques rassemblent les fichiers provenant de différents emplacements et les affichent dans un emplacement unique.

Toutefois, la structure de dossiers dans Windows XP est assez différente de celle de Windows Vista ou Windows 7. Utilisez le tableau suivant pour comparer les chemins et les noms de dossiers de ces trois versions de Windows.

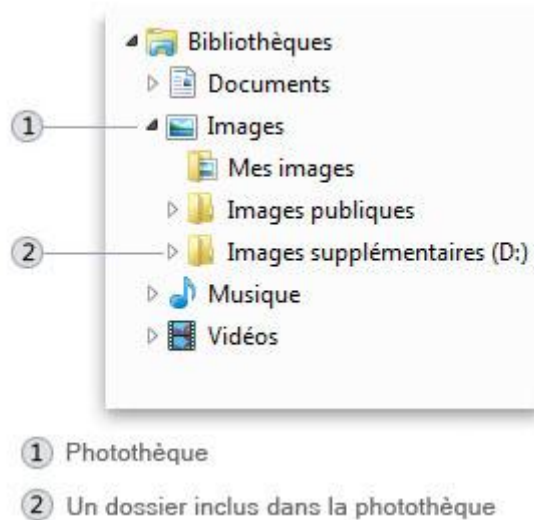
Nom de dossier (et chemin) dans Windows XP	Nom de dossier (et chemin) dans Windows Vista	Nom de dossier (et chemin) dans Windows 7
<i>Documents and Settings</i> C:\Documents and Settings	<i>Utilisateurs :</i> C:\Utilisateurs	<i>Utilisateurs :</i> C:\Utilisateurs
<i>Mes documents :</i> C:\Documents and Settings\nom_utilisateur\Mes documents	<i>Documents :</i> C:\Utilisateurs\nom_utilisateur\Documents	<i>Mes documents :</i> C:\Utilisateurs\nom_utilisateur\Documents
<i>Mes images :</i> C:\Documents and Settings\nom_utilisateur\Mes documents\Mes images	<i>Images :</i> C:\Utilisateurs\nom_utilisateur\Images	<i>Mes images :</i> C:\Utilisateurs\nom_utilisateur\Images
<i>Ma musique :</i> C:\Documents and Settings\nom_utilisateur\Mes documents\Ma musique	<i>Musique :</i> C:\Utilisateurs\nom_utilisateur\Musique	<i>Ma musique :</i> C:\Utilisateurs\nom_utilisateur\Musique
<i>Mes vidéos :</i> C:\Documents and Settings\nom_utilisateur\Mes documents\Mes vidéos	<i>Vidéos :</i> C:\Utilisateurs\nom_utilisateur\Vidéos	<i>Mes vidéos :</i> C:\Utilisateurs\nom_utilisateur\Vidéos
<i>Bureau :</i> C:\Documents and Settings\nom_utilisateur\Bureau	<i>Bureau :</i> C:\Utilisateurs\nom_utilisateur\Bureau	<i>Bureau :</i> C:\Utilisateurs\nom_utilisateur\Bureau
<i>Local Settings :</i> C:\Documents and Settings\nom_utilisateur\Local Settings	<i>Local :</i> C:\Utilisateurs\nom_utilisateur\AppData\Local	<i>Local :</i> C:\Utilisateurs\nom_utilisateur\AppData\Local

Bureau contient les raccourcis que vous avez placés sur le bureau. Vous pouvez donc en ajouter soit directement par le bureau, soit par l'intermédiaire de ce répertoire (inutile mais pratique à savoir).

C:\Programmes (sous XP « program Files) est le dossier privilégié d'installation des programmes. La plupart d'entre eux s'installent à l'intérieur de ce dossier dans un nouveau dossier ayant d'habitude comme dénomination le nom du programme.

C:\WINDOWS\system32\ est l'emplacement des librairies et extensions de programmes et d'applications du système d'exploitation.

Dans les versions précédentes de Windows, la gestion de vos fichiers signifiait les organiser dans différents dossiers et sous-dossiers. Dans les dernières versions vous pouvez également utiliser des bibliothèques pour organiser et accéder aux fichiers, quel que soit l'endroit où ils sont stockés :



Une bibliothèque rassemble des fichiers provenant de différents emplacements et les affiche sous la forme d'une même collection, sans les déplacer depuis l'endroit où ils sont stockés. Il existe 4 bibliothèques par défaut (Documents, Musique, Images et Vidéos), mais vous pouvez créer de nouvelles bibliothèques pour d'autres collections.

5.2. Attributs des fichiers

Sous Windows chaque fichier et dossier possède des attributs spécifiques (pour y accéder, cliquez droit dans l'explorateur de fichiers-Propriétés) :

- Lecture seule (R read only) : interdit la modification et suppression du fichier.
- Archive (A archive) : marque les fichiers créés ou modifiés depuis la dernière sauvegarde.
- Fichier caché (H hidden) : dans l'explorateur Windows, pour activer l'affichage des fichiers cachés il faut ouvrir « Option Des Dossiers » et dans l'Onglet Affichage cocher « Afficher les fichiers cachés ».
- Fichier système (S system) : indique un fichier utilisé par le système d'exploitation. (non visible dans l'explorateur, pour ajouter ou supprimer cet attribut utilisez la commande dos `attrib+S NomFichier` ou `attrib-S NomFichier`). Pour vérifier l'intégrité des fichiers systèmes en commande dos : **sfc /scannow**.

5.3. Gestion des droits des utilisateurs

Comme avec Vista, vous pouvez avec Windows 7 bénéficier d'un environnement de travail bien à vous, tel que vous l'avez défini et personnalisé. Ce travail de configuration

et de réglage passe par l'utilisation des comptes utilisateurs. Leur fonction première est de permettre à différents utilisateurs de se partager l'usage d'un même ordinateur. C'est idéal notamment dans le cadre d'une utilisation familiale du PC. Mais les comptes utilisateurs ne servent pas qu'à ça puisqu'ils permettent d'optimiser la sécurité de l'ordinateur en définissant les droits dont chacun dispose, par exemple pour installer un nouveau logiciel ou modifier certains fichiers sensibles.

Ces réglages de sécurité, ainsi que ceux permettant à Windows de fonctionner de façon optimale, sont regroupés au sein de Centre de maintenance, qui remplace le Centre de sécurité de Windows XP et de Windows Vista. Il donne un accès rapide à tous les outils de surveillance permettant de garantir du mieux possible l'intégrité des données et d'éviter les plantages.

- L'**Administrateur** dispose de tous les droits sur l'ordinateur et peut donc accéder à ses propres fichiers ainsi qu'à ceux des autres utilisateurs, il peut modifier les privilèges (attribution du statut Administrateur aux utilisateurs), les mots de passe, les paramètres appliqués sur l'ensemble du système, installer des logiciels, des pilotes et des périphériques.
- L'**Utilisateur standard** ne peut pas installer ni ouvrir certains programmes, mais il peut changer l'image associée à son compte et créer, modifier ou supprimer le mot de passe de son compte. Il lui est impossible de modifier (voire même de consulter) les fichiers des autres utilisateurs. Il ne peut pas installer de logiciel. Ce dernier point, lié à la sécurité, en fait le compte le mieux protégé des virus et autres programmes malicieux.
- Le compte **Invité** a un accès limité (comme un compte Standard) aux ressources de l'ordinateur et peut exécuter certains programmes installés par d'autres utilisateurs. Il ne peut pas accéder à des fichiers personnels ou protégés par mot de passe.

6) Le registre Windows

Apparu pour la première fois dans Windows 3.1, sous le nom de **base de registre**, il sert à faciliter l'administration et la centralisation des paramètres du système d'exploitation.

Depuis, le registre a connu quelques modifications comme le changement de forme de stockage sur le disque dur, ou le changement de nom : la base de registre est devenue le **registre Windows**.

Pour y accéder tapez Regedit dans la barre de recherche du menu Démarrer.

Attention aux risques de perte ou d'altération du Registre : Etant le seul support de configuration Windows, si le registre est trop endommagé et ne peut être récupéré cela entraîne une réparation par la réinstallation du registre avec le DVD Windows voire la réinstallation complète du système d'exploitation. Sa protection est donc cruciale.

Sous Windows 95-98-ME il est en fait constitué de deux fichiers qui se trouvent dans votre répertoire Windows : USER.DAT et SYSTEM.DAT. Ces fichiers sont construits à chaque démarrage par Windows. Windows ME utilise un fichier supplémentaire pour la base de registre : CLASSES.DAT

A chaque démarrage réussi, Windows crée une copie de sauvegarde de ces deux fichiers qu'il appelle USER.DA0 et SYSTEM.DA0.

Si vous utilisez des profils utilisateurs, le fichier USER.DAT est situé dans le dossier Profiles\"nom du profil\"USER.DAT. En effet le fichier USER.DAT contient les données de personnalisation d'un utilisateur. Donc si vous utilisez plusieurs profils utilisateur il est normal que chaque utilisateur possède son fichier USER.DAT afin qu'il ait ses propres personnalisations.

Structure de la Base de Registre :

Le contenu du registre est très variable selon votre utilisation (programmes, jeux, navigateurs...), mais il demeure un ensemble hiérarchisé avec 6 grandes "clés" principales ("dossiers") et des tas de ramifications (les sous-clés).

Les données du registre sont donc organisées dans ce que l'on appelle des HKEY (« handle key » ou « poignée de clé »). Ces poignées de clés sont comparables aux dossiers racines du registre.

Il existe six poignées de clés nommées HKEY_{nom} :

1. HKEY_LOCAL_MACHINE : votre équipement

Cette branche du registre reçoit les paramètres de l'ordinateur : profils utilisateurs, composants matériels, configuration réseau, paramètres de sécurité et système. Ces paramètres se définissent à l'installation du système et sont modifiés lors de changement dans la configuration. Ne les changez pas manuellement, car l'ordinateur peut devenir instable ou même se bloquer. Certaines interventions peuvent également avoir de mauvaises conséquences : fonctionnement incorrect de certaines sections du système (par exemple les fonctions réseau ou certains périphériques), impossibilité de lancer Windows...L'examen du contenu de la clé HKEY_LOCAL_MACHINE livre de nombreuses informations intéressantes sur votre configuration : périphériques, paramétrage du matériel, etc.

2. HKEY_CURRENT_USER : les paramètres de l'utilisateur

Ce niveau assure le paramétrage propre à l'utilisateur : événements système, aide à la saisie, apparence, curseur actuel de la souris. La plupart de ces paramètres se modifient aisément sous Windows. Les modifications sont sans véritable danger lorsque vous avez défini plusieurs profils utilisateurs. Elles ne s'appliquent en effet qu'à l'utilisateur actuel. Si vous rencontrez des problèmes après avoir effectué quelques modifications, changez de profil au démarrage suivant.

3. HKEY_CLASSES_ROOT : les classes et les objets

La branche HKEY_CLASSES_ROOT contient les paramètres les plus importants des programmes. Y sont gérés les extensions de nom de fichier, les liaisons avec les logiciels ainsi que les serveurs ActiveX (les composants utilisés en commun). Cette branche permet d'attribuer à une application une extension spécifique. La sélection de l'un de ces fichiers dans l'explorateur lancera l'application qui chargera ce fichier.

La clé gère en outre des composants communs de Windows et les objets COM (Component Object Model), c'est à dire les DLL ActiveX, les EXE ActiveX, les contrôles complémentaires, etc. Ces composants s'enregistrent eux mêmes, c'est à dire qu'ils inscrivent les informations nécessaires à l'installation ou à l'exécution : identificateurs de classe, numéro de version... Evitez de modifier manuellement les inscriptions de ces éléments. D'une part, les programmes d'installation risquent de ne plus pouvoir identifier correctement les versions, d'autre part le composant peut devenir introuvable.

4. HKEY_USERS : aperçu de tous les utilisateurs

La branche HKEY_USERS décrit un environnement de système d'exploitation par défaut et contient une clé pour chaque utilisateur ayant ouvert une session locale ou via une connexion réseau. Il contient tous les profils utilisateurs chargés activement, y compris HKEY_CURRENT_USER, déjà désigné comme enfant de HKEY_USERS et profil par défaut.

NB: des utilisateurs qui accèdent à un serveur distant n'ont pas de profil sous cette clé sur le serveur, leurs profils sont chargés dans le registre de leur propre ordinateur.

5. HKEY_CURRENT_CONFIG : la configuration actuelle

La branche HKEY_CURRENT_CONFIG contient des informations sur le profil matériel utilisé par l'ordinateur local au démarrage. Ces informations sont utilisées pour configurer des paramètres tels que les pilotes de périphérique à charger et la résolution d'écran à adopter. N'y modifiez rien sous peine de devoir tout réinstaller ou risquer des dysfonctionnements graves.

6. HKEY_PERFORMANCE_DATA : clé invisible

Elle contient les informations des performances du noyau NT et de ses services. Ces données, bien qu'invisibles dans l'éditeur de registre sont visibles dans le moniteur de performances.

Chapitre 4. Linux : Gestion du système d'exploitation

Présenté comme l'alternative à Windows, Linux est un système d'exploitation gratuit basé sur un autre système d'exploitation plus ancien Unix.



Linux et ses logiciels sont distribués sur le principe de la licence GPL (General Public Licence issu du projet GNU) qui a pour philosophie la liberté de système d'exploitation et des logiciels. Un logiciel GPL peut être copié, redistribué ou modifié car ses codes sources sont toujours accessibles à tous. On utilise aussi le terme de « logiciel Open Source ». Linux représente le noyau du système d'exploitation. On distingue le noyau des distributions. En effet les distributions utilisent toutes le même noyau, mais peuvent parfois proposer des applications et logiciels différents.

1) Les distributions Linux

Les différentes distributions Linux centralisent et rassemblent les différents composants logiciels dans un environnement stable avec un outil d'installation du système et différents outils de configuration (formatage, chargeur de démarrage, gestion des paquets logiciels, outils de configuration de services, etc....).

Certaines de ces distributions sont conçues pour des tâches bien précises (bureau, serveur, pare-feu, routeur, etc....). Le système d'exploitation Linux est gratuit, cependant certaines distributions sont payantes en échange de services d'aide et de documentation.



2) Caractéristiques

Le système **Linux** est un système **multi-utilisateurs** et **multi-tâches**. En tant que système d'exploitation, son rôle principal est donc d'assurer aux différentes tâches et aux différents utilisateurs une bonne répartition des ressources de l'ordinateur (mémoire, processeur(s), espace disque, imprimante(s), programmes utilitaires...) et cela sans intervention des utilisateurs; il prend totalement en charge ces utilisateurs et lorsque les demandes sont trop importantes pour être satisfaites rapidement, l'utilisateur le ressent par un certain ralentissement (qui peut être effectivement important, voire insupportable...), mais le système (en principe) ne se bloque pas.

Linux est par ailleurs un système de développement et les utilisateurs y ont à leur disposition un très grand nombre d'outils, pour la plupart assez simples à utiliser, leur permettant d'écrire, de mettre au point et de documenter leurs programmes (éditeurs, compilateurs, débogueurs, système de traitement de textes...). Les utilisateurs ont ainsi à leur disposition une boîte à outils bien garnie, le principal problème qui se pose à eux étant de savoir ce qu'elle contient exactement et à quoi sert chacun de ces outils !

En résumé, on peut dire que le système est composé de :

- un noyau assurant la gestion de la mémoire et des entrées-sorties de bas niveau et l'enchaînement des différentes tâches ;

- un (ou plusieurs) interpréteur(s) de langage de commandes; il existe en effet différents langages de commandes nommés **Shell**, le plus connu étant le **Bourne Shell** (du nom de son auteur), un autre étant le **C-Shell** développé à l'université de **Berkeley** et le plus répandu actuellement étant le **Bash**. Nous verrons dans ce tutoriel un cours de **Bourne Shell** et de **Bash**. Il est important de noter que, quelle que soit la version du langage de commandes utilisée, il s'agit d'un véritable langage de programmation possédant des instructions et surtout des structures de contrôle de très grande puissance ;
- un système de messagerie assez complet (courrier, conversation en temps réel, journal de bord) ;
- un grand nombre de programmes utilitaires dont évidemment un compilateur de **langage C**, des éditeurs, des outils de traitement de textes, des logiciels de communication avec d'autres systèmes **Linux** (ou autres), des générateurs d'analyseurs lexicaux et syntaxiques...

a) Linux est fiable

L'écran bleu de Windows n'existe pas sous Linux. Les systèmes Linux et Unix peuvent fonctionner pendant des années sans échec (Windows aussi mais tout dépend de l'utilisation que vous en faites !). L'équivalent de l'écran bleu sur Linux se nomme **Kernel Panic**, il est extrêmement rare et est dans 99% des cas dus à une fausse manipulation de l'utilisateur.

Cette fiabilité est due à son noyau qui, d'après plusieurs études, contient bien moins de bogues que ses concurrents propriétaires. Mais attention extrêmement fiable ne veut pas dire 100%, des bogues existent toujours et vous ne serez jamais à l'abri, un jour peut-être, d'une mauvaise surprise.

Petit conseil : avant de toucher un quelconque fichier de configuration sous Linux il est **IMPERATIF** de sauvegarder le fichier d'origine et surtout avant de procéder à n'importe quel changement, soyez sûr et certain de ce que vous modifiez, sinon de graves conséquences sur le système seront inévitables et c'est donc ainsi que le système devient non fiable car vous avez créé une faille de sécurité, un bogue qui ne vous permettra plus de faire certaines choses, un plantage complet de la machine, un arrêt brutal de l'affichage, etc.

Il faut aussi savoir que les virus sont vraiment très rares sous Linux contrairement à Windows. Mais attention il existe malgré tout beaucoup de menaces sous Linux. Ceci est dû au fait que les exécutables tels que vous les connaissez sous Windows n'existent pas sous Linux.

b) Linux fonctionne partout

L'efficacité de Linux et de tous les Unix-oïdes peut être utilisée sur pratiquement tous les ordinateurs même les plus vieux. Il en va de même pour beaucoup d'applications. Par contre, certaines applications peuvent recommander un certain taux de performance.

Il existe maintenant ce que l'on appelle les **live-CD** qui sont intégrés à toutes (ou du moins quasiment toutes) les distributions Linux. Ceci vous permet d'avoir sur un CD à la fois le programme d'installation du système d'exploitation, mais surtout (et c'est là l'intérêt du live-CD !!) d'utiliser Linux sans rien installer du tout sur votre disque dur.

Mais attention il y a des limites à cette possibilité, il faut savoir que l'utilisation d'un live-CD n'est pas faite pour une utilisation intensive de Linux (serveur, développement, etc.) vous ne pourrez d'ailleurs rien installer et les performances ne seront pas géniales vu que tout se passe non pas sur le disque dur mais dans la RAM. Le live-CD est donc fait pour une simple découverte du monde Linux c'est-à-dire se familiariser avec l'environnement de Bureau et

comment on l'utilise par exemple. Une autre utilisation des live-CD est la possibilité d'effectuer des réparations ou des récupérations de données sur les disques durs qui, par exemple, ont un problème de boot.

c) Linux est gratuit

Vous pouvez télécharger Linux sur Internet et l'installer sur autant de machines que vous le voulez, ainsi que les applications. Il est possible aussi, pour beaucoup de distributions de commander le CD/DVD de la distribution. A noter aussi qu'il y a des distributions payantes, mais se sont des distributions réservées aux professionnels et entreprises.

Il faut savoir que ceci est dû au fait que le développement des distributions Linux est fait en open source.

Il y a principalement 4 moyens d'acquérir une distribution Linux :

- en la téléchargeant, ceci est totalement gratuit
- en achetant un magazine spécialisé sur Linux (ces magazines contiennent toujours une distribution sur le CD qui est fourni avec) et ainsi vous payez le prix du magazine
- en achetant la distribution dans un magasin spécialisé et dans ce cas, vous payerez le prix proposé par le magasin en question
- en commandant un CD/DVD à l'éditeur de la distribution, ici par contre cela peut être gratuit ou bien alors payant suivant l'éditeur et la manière dont vous faites votre commande.

d) Le support de Linux

Linux regroupe aujourd'hui une grande communauté. Tout ça grâce à Internet. Vous pouvez obtenir de l'aide de plusieurs dizaines de milliers d'utilisateurs Linux et programmeurs bénévoles sur Internet. Le support est gratuit (pour les distributions non professionnelles).

Par contre pour ce qui concerne les distributions professionnelles en général, c'est dans un forfait mais il se peut aussi que le support soit offert si vous êtes partenaire de l'entreprise qui développe la distribution.

e) Linux n'a pas de registre

Lorsque Microsoft a introduit le registre dans Windows 95 il a été applaudi pour ce mécanisme qui a vocation d'éliminer la gestion d'un système avec les fichiers **.ini** de Windows 3.x. Linux, lui, est géré par de simples fichiers de texte brut pour sa configuration.

C'est beaucoup plus pratique mais aussi plus dangereux car on est moins à l'abri d'une fausse manipulation. Par contre, le fait d'instaurer un fichier de configuration pour chaque partie ou programme permet de savoir exactement ce que l'on essaie de modifier et on n'a pas cette hiérarchie catastrophique du registre Windows où on ne sait jamais où se trouve ce que l'on cherche.

De plus il existe pour beaucoup de programmes, ainsi que pour le système d'exploitation lui-même, des outils permettant d'automatiser ou de fortement simplifier la configuration de ceux-ci.

f) Redémarrage du système

La plupart des changements de configurations de Windows requièrent un redémarrage (mise à jour comprise), cela peut être vite embêtant lorsque la machine est un serveur.

Sous Linux rares sont les changements qui requièrent un redémarrage, ceci permet d'effectuer des changements sur votre serveur sans affecter leurs utilisateurs. Quand je parle de mise à jour je parle bien évidemment de mises à jour proposées par votre distribution.

Il faut savoir que ceci est dû à la non-utilisation de registre et que sous Linux se sont seulement des fichiers qui sont modifiés et donc un simple redémarrage des services suffit. Alors que sous Windows, les mises à jour consistent les trois quarts du temps à modifier le registre et comme la prise en compte n'est pas dynamique, il faut le redémarrage du système pour que les nouveaux paramètres soient pris en compte. En général sous Linux seules les mises à jour du noyau requièrent un redémarrage du système.

2.2. L'interface graphique

Windows a toujours été fourni avec une interface graphique. Pourtant certains serveurs (Web, fichiers, BDD,...) n'ont aucunement besoin d'une interface graphique et de cette façon des ressources sont occupées pour rien. L'interface graphique Linux (X Window) est un sous-système facultatif que vous pouvez choisir d'utiliser ou non. En outre, vous pouvez démarrer et arrêter l'interface graphique quand vous le souhaitez sans avoir à redémarrer le système et sans avoir un quelconque effet sur les programmes en cours d'exécution.

Il faut savoir que sous Windows il n'existe qu'un seul environnement de bureau possible par défaut. Alors que sous Linux, il en existe plusieurs (KDE, GNOME, XFCE, etc.). On peut les combiner, c'est-à-dire choisir à l'ouverture de sa session le type d'environnement que l'on souhaite.

2.3. La défragmentation

Toutes les versions de Windows souffrent du même problème : la fragmentation du disque. Ceci réduit considérablement les performances. Linux, lui, ne fragmente pas les données sur le disque et est ainsi plus apte à être un serveur de fichiers que Windows.

Il est vrai que les systèmes de fichiers Linux font un usage optimisé de l'espace, mais il n'est malheureusement pas en mesure de savoir aujourd'hui quelle sera l'organisation optimale de votre disque après une ou deux années d'usage intensif. Pour résumer, si vos disques durs ont une durée de vie supérieure à environ deux ans, que vous travaillez régulièrement dessus, que vous manipulez quotidiennement de gros fichiers (vidéos, morceaux de musique, etc.), que vous vous livrez au P2P ou encore qu'il vous arrive d'exhumer de vieux (et gros !) fichiers pour retravailler dessus, vous ressentirez vite, comme tout le monde, le besoin de défragmenter votre disque Linux !

2.4. A quoi ressemblent les commandes Linux ?

Sous Linux, l'utilisateur dispose de nombreuses commandes. Une commande se compose du nom proprement dit de cette commande (un simple mot), suivi éventuellement d'un ou plusieurs arguments (fournissant des informations supplémentaires : options ou paramètres), les différents éléments de la commande étant séparés par des espaces ou des caractères de tabulation; la commande complète est elle-même terminée par l'appui sur la touche **ENTRÉE**. Il faut en effet savoir que chaque ligne entrée au clavier est mémorisée et n'est effectivement interprétée que lorsqu'elle est complète, c'est-à-dire à la réception du caractère de fin de ligne; ce mode de fonctionnement est appelé **canonique**. Il offre en particulier l'avantage de permettre l'annulation de caractères de la ligne en cours de frappe avant son interprétation. Une possibilité offerte est de modifier ce mode de fonctionnement afin par exemple que chaque caractère tapé soit interprété immédiatement.

Au cours de la procédure d'identification ("login") en mode console ou au cours d'une

session de travail, si le mode de fonctionnement est canonique, un certain nombre de caractères jouent un rôle particulier en ce sens qu'ils permettent d'annuler tout ou partie de la ligne en cours de frappe :

- la touche **BACKSPACE** ou la combinaison **CTRL+H** annule le dernier caractère tapé
- la combinaison **CTRL+U** annule tout ce qui précède sur la ligne.

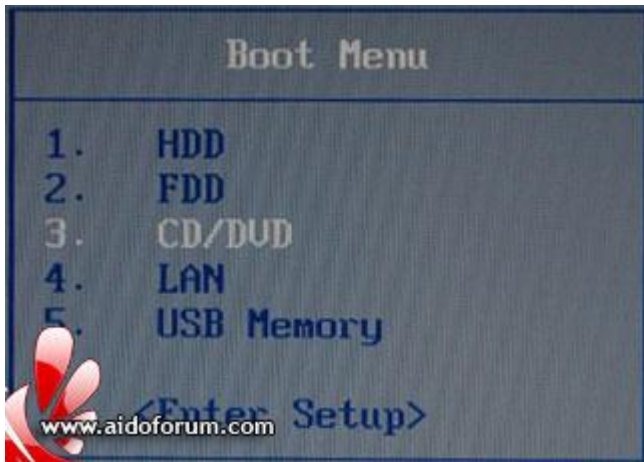
Exemple : La commande echo

Elle affiche la liste des paramètres sur la sortie standard, c'est-à-dire la chaîne de caractères qui suit echo :

```
>>echo coucou tout le monde !  
coucou tout le monde !
```

Chapitre 5. Installation d'un OS

Pour installer ou ajouter un système d'exploitation sur un disque dur vous devez d'abord vous procurer le programme d'installation (actuellement la plupart des systèmes d'exploitation s'installent directement à partir du Cdrom ou DVD rom), ensuite il vous faut entrer dans le BIOS pour préciser de lancer le boot sur le CD et non sur le disque dur.



NB : Cette étape peut différer quelque peu selon les PC.

Redémarrez et suivez les instructions d'installation.

1) Etapes

Les grandes étapes d'une installation peuvent se résumer comme suit :

- Choix du périphérique de stockage de destination pour l'installation
- Choix du type d'installation :
Soit une *installation complète* (en effaçant et formatant le support)
Soit une *réparation*
Soit une *mise à jour* (si l'ancien système est compatible)
- Choix sur la création de partitions¹ supplémentaires ou pas (sous linux il est nécessaire de créer 1 partition SWAP servant de mémoire virtuelle, +- le double de la mémoire physique RAM ; sous Windows cette mémoire virtuelle est enregistrée dans un fichier système)
- Choix du système de fichiers² pour la ou les partitions (ex : FAT32 ou NTFS pour Windows, EXT2 ou EXT3 pour Linux)
- Formatage du support (disque dur)³
- Copie des fichiers d'installation (pour les distributions Linux, vous avez également le choix du type d'applications supplémentaires à installer)
- Configuration clavier, date/heure, fuseaux horaires,....
- Configuration des paramètres.
- Encodage du mot de passe administrateur (Os multi utilisateurs)
- Création d'au moins un utilisateur et encodage de son mot de passe (pour éviter la connexion comme administrateur global ayant tous les droits)
- Installation du système d'exploitation (pour les distributions Linux l'installation

¹ Voir point 3 de ce chapitre

² Voir point 4 de ce chapitre

³ Voir point 2 de ce chapitre

s'effectue souvent avec plusieurs CDs, vu l'installation supplémentaire d'applications diverses comme les navigateurs Internet, les applications bureautiques, etc....)

- Fin de l'installation et redémarrage du PC.

Les systèmes d'exploitation payants comme Windows demandent également l'enregistrement et l'encodage d'une clé de validation fournie avec le CD pour l'installation du système. Vous avez alors 30 jours pour activer Windows en validant votre clé via internet.

Linux est un système d'exploitation gratuit et librement diffusable, créé par Linus Torvalds, étudiant finlandais dès 1991. Diverses distributions existent comme **Debian, RedHat/Fedora, Gentoo, Mandriva Linux (ex-MandrakeSoft), Slackware, SuSE, Ubuntu, etc...** Toutes ces distributions utilisent le même noyau et rassemblent chacune une compilation de programmes stables s'installant en même temps que le système d'exploitation.

2) Le formatage du disque dur

Si vous décidez de faire une nouvelle installation complète de l'OS (donc pas une mise à jour) il vous faudra alors préparer le disque dur de façon à ce qu'il puisse être utilisé par l'OS.

La préparation du support par un formatage est une étape importante lors de l'installation d'un nouveau système d'exploitation. Outre le formatage, il est également utile de créer des partitions différentes (voir plus bas) permettant par exemple de séparer les fichiers systèmes des fichiers de travail.

Attention, avant de commencer :

- Sauvegardez (par ex sur un disque dur externe) toutes les données qui doivent impérativement être sauvées : textes, images, photos ...
- Il peut aussi être utile de sauvegarder son carnet d'adresses Outlook avec toutes les coordonnées de ses correspondants
- Pensez qu'il vous faudra réinstaller tous vos logiciels.
- Assurez-vous que vous disposez bien de tous vos drivers (pilotes) de périphériques (carte son, carte vidéo, modem, imprimante, scanner, etc.).

En effet ce qui n'a pas été sauvegardé sera irrémédiablement perdu après le formatage

Il existe deux niveaux de formatage pour un disque dur :

- Le formatage de bas niveau ou formatage physique
- Le formatage de haut niveau ou formatage logique

Lorsque vous formatez une disquette à l'aide de la commande FORMAT de DOS, cette commande effectue ces deux types de formatage simultanément. Pour formater un disque dur, en revanche, vous devez effectuer chaque formatage séparément.

Vous devrez de surcroît procéder à une troisième manœuvre entre chaque formatage, durant laquelle les informations sur le partitionnement seront écrites sur le disque.

Remarque : Vous devez partitionner le disque dur lorsque vous souhaitez l'utiliser avec plusieurs systèmes d'exploitation. En séparant les formats physiques d'une manière identique à chaque fois, indépendamment du système d'exploitation utilisé et du formatage de haut niveau (qui serait différent pour chaque système d'exploitation), vous pourrez utiliser plusieurs systèmes d'exploitation sur un seul et même disque dur.

Le partitionnement permet en effet à plusieurs types de systèmes d'exploitation d'utiliser le même disque dur ou à un seul et même OS d'utiliser ce disque sous forme de plusieurs

volumes ou lecteurs logiques. Un volume ou lecteur logique est un élément auquel DOS attribue une lettre.

Le formatage s'effectue en trois étapes:

- Formatage de **bas niveau** - Fait en usine par le fabricant.
- Partitionnement - Fait par l'utilisateur
- Formatage de **haut niveau** - Fait par l'utilisateur

2.1. Formatage de bas niveau

Contrairement au formatage logique (qui efface uniquement les données du disque dur), le formatage bas niveau reconstruit les "clusters" du disque. C'est ainsi que l'on peut résoudre les problèmes de clusters défectueux.

Le principe d'un formatage bas niveau est simple et lorsque vous achetez un disque neuf, celui-ci est TOUJOURS formaté bas niveau : cela consiste à préparer le support physique du disque dur en organisant la surface de chaque plateau en pistes et secteurs.

Attention : ce type de formatage n'est à utiliser que dans des cas extrêmes (dysfonctionnement grave) car il s'applique à la totalité du disque dur physique. Reformater en bas niveau n'exclut pas des erreurs plus graves.

Quand utiliser le formatage de bas-niveau ?

- Un virus de boot s'auto-réplique en permanence sur votre HD, et un formatage normal n'en est pas venu à bout.
- Votre disque dur vous pose quelques inquiétudes: bruits bizarres, pertes de clusters incongrues...
- Vous croyez votre disque dur "fichu" : essayez ! Le jeu en vaut parfois la chandelle.
- Vous voulez simplement formater votre disque dur: n'hésitez pas à procéder à un formatage de bas-niveau pour le remettre à neuf...

Cela permet :

1. de vérifier l'état d'un disque au moindre doute de fiabilité
2. de le reparer pour un usage 100% sûr (au moins pour ce qui est des secteurs) en remettant au propre la table d'allocation de référence du disque (de secours) pour un formatage haut niveau propre
3. d'optimiser le meilleur rapport cylindre/têtes/secteurs en fonction du disque, du mode d'accès choisi et de l'OS qu'il va accueillir. En effet, il faut savoir que la capacité physique d'un disque est fixe, mais que son exploitation est le fruit d'un découpage en cylindres, têtes et secteurs et qu'il est donc possible de paramétrer

2.2. Formatage de haut niveau

Les disques durs, aussi petits soient-ils, contiennent des millions de bits, il faut donc organiser les données afin de pouvoir localiser les informations, c'est le but du système de fichiers. Un disque dur est, rappelons-le, constitué de plusieurs plateaux circulaires tournant autour d'un axe. Les pistes (zones concentriques écrites de part et d'autre d'un plateau) sont divisées en quartiers appelés secteurs (d'une taille de 512 octets). Le formatage logique d'un disque permet de créer un système de fichiers (FAT, NTFS,...) sur le disque, qui va permettre à un système d'exploitation (DOS, Windows, UNIX, ...) d'utiliser l'espace disque pour stocker et utiliser des fichiers.

Si le système d'exploitation est capable d'utiliser plusieurs systèmes de fichiers, le choix dépendra des caractéristiques que l'on désire utiliser, par exemple sous Windows le formatage en NTFS permet de définir une politique de gestion des droits d'accès aux fichiers et dossiers qui est impossible avec un système FAT.

Vous pouvez choisir entre "formatage rapide" et "formatage normal" :

Le formatage rapide remet simplement la table d'allocation (table de matières vers les fichiers) à zéro, celle-ci est donc réinitialisée mais les données enregistrées sur le disque dur ne sont en réalité pas effacées, il est alors toujours possible de récupérer les fichiers avec des logiciels spécialisés.

Le formatage normal ou complet va remplacer toutes les données par des données vides afin d'empêcher toute récupération ultérieure des données initiales. Donc si vous ne souhaitez pas que les informations précédemment présentes sur la partition à formater soient récupérables par des logiciels spécialisés, choisissez "Formatage complet".

3) Partitionner un disque dur

3.1. Définition et intérêt

Par défaut quand vous installez votre OS votre disque dur contient une seule partition. Partitionner un disque dur physique sert à le diviser en deux ou plusieurs parties.

Les partitions une fois créées et formatées sont considérées par le système comme étant des disques durs indépendants.

exemple: 1^{ère} partition -> disque C:
 2^{ème} partition -> disque D:

ATTENTION: Si vous voulez partitionner votre disque dur alors que vous avez déjà installé votre OS, vous devrez formater votre unique partition et vous perdrez toutes vos données...

Après avoir créé vos partitions vous devrez redémarrer votre ordinateur pour que vos partitions soit prises en compte et ensuite vous devrez formater chaque partition afin qu'elle soit utilisable.

Pourquoi séparer un disque dur en 2 partitions ? :

- L'installation de deux ou plusieurs systèmes d'exploitation (multiboot), pour les séparer au niveau environnement (ex : installation de deux systèmes Windows) et/ou pour séparer deux systèmes de fichiers (ex : installation de Windows et Linux).
- Partitionnez votre disque dur avant d'installer votre OS et créez au moins 2 partitions, sur la 1^{ère} vous installerez votre système d'exploitation et vos logiciels et sur la 2^{ème} vous enregistrerez vos données, ce qui vous donnera la possibilité de reformater votre première partition, de réinstaller votre système et vos logiciels sans perdre vos données...
- Permet de réduire le temps de défragmentation d'un disque.

3.2. Types de partition

En raison de limitations dues au BIOS et à la table de partitions, le nombre de partitions est limité à 4 partitions primaires maximum. Pour palier à cette limitation, on peut utiliser une partition étendue dans laquelle on peut créer plusieurs lecteurs logiques.

Il existe trois types de partitions :

Partition primaire : une minimum et quatre maximum par disque dur physique.

Partition étendue : partition de même niveau qu'une partition primaire sauf qu'elle peut contenir plusieurs lecteurs logiques. Une partition étendue utilise sa propre table de partitions permettant d'accéder à ses lecteurs logiques.

Lecteur logique : nombre non limité mais obligatoirement situé dans une partition

étendue.

3.3. Méthodes

Il existe de nombreuses applications permettant de formater un disque dur en mode console (invite de commande en mode texte) ou en mode graphique.

Quelques références :

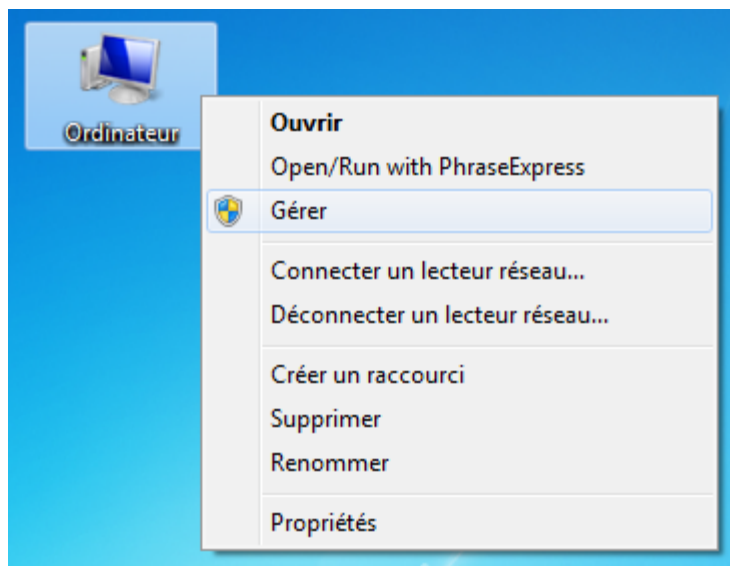
- En DOS c'est la commande FORMAT : petit programme dos pour le formatage de disquettes et de disques au format FAT
ex : **format a:/s** formate une disquette sur le lecteur A en y incluant les fichiers systèmes DOS
- FDisk est l'utilitaire de formatage et de partitions en mode console sous Linux et Windows
- PartitionMagic est un des logiciels de référence dans ce domaine de par sa facilité d'utilisation, mais il est payant.
- DiskDruid est l'équivalent de PartitionMagic mais gratuit.

Mais il est aussi possible de partitionner son disque dur sous Windows 7 sans passer par un utilitaire externe (qu'il soit gratuit ou payant).

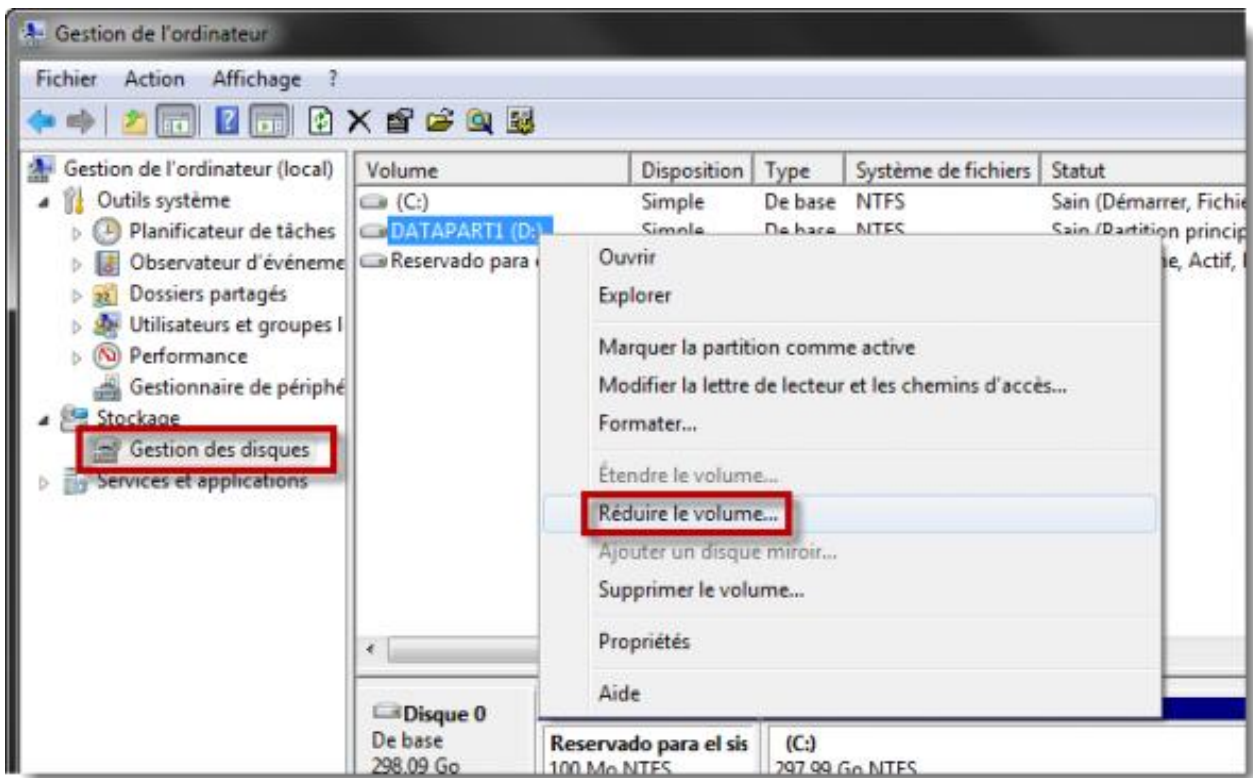
Note importante: Vous devez avoir un espace disque libre suffisant pour réaliser la procédure.

a) Réduire une partition existante

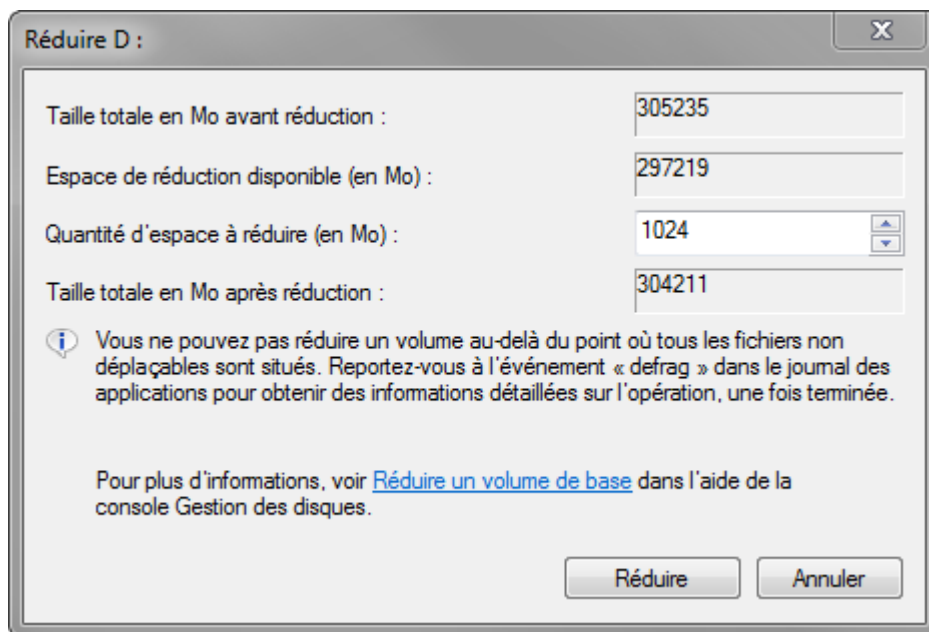
Sur le bureau, faites un clic droit sur **Ordinateur** et cliquez sur **Gérer** :



Dans l'outil de gestion de l'ordinateur, dans le menu à gauche, cliquez sur **Gestion des disques**. Ensuite, effectuez un clic droit sur le volume à partitionner et cliquez sur **Réduire le volume**.



L'outil évalue l'espace disponible sur votre disque dur. A la fin de l'analyse, une fenêtre apparaît vous permettant de **choisir la quantité d'espace à réduire**. Entrez le nombre voulu. Dans notre exemple, nous réduisons une partition de 1Go.

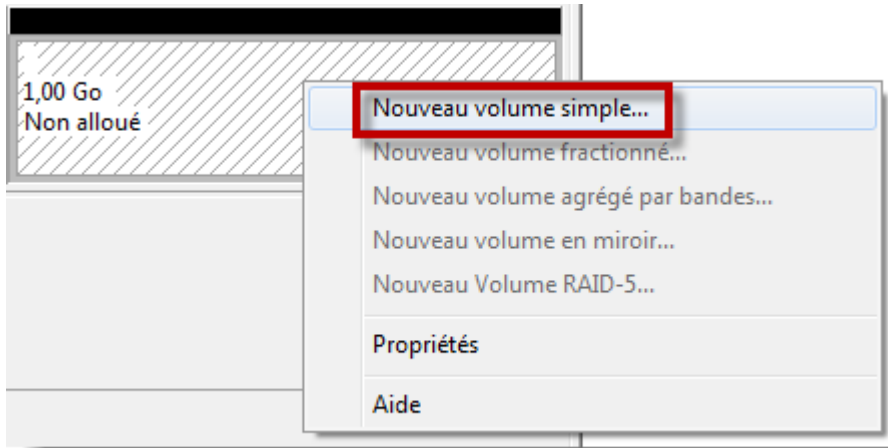


Lorsque l'opération est terminée, votre nouvelle partition est créée :

Disque 1	Volume	Statut
De base 298,09 Go En ligne	DATAPART1 (D:) 297,08 Go NTFS Sain (Partition principale)	1,00 Go Non alloué

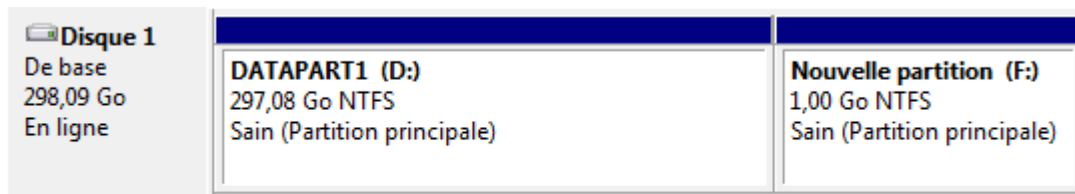
b) Formater la nouvelle partition

Après avoir créé la nouvelle partition, il faut la **formater** afin de pouvoir l'exploiter. Pour cela, effectuez un clic droit sur la nouvelle partition et cliquez sur **Nouveau volume simple**:



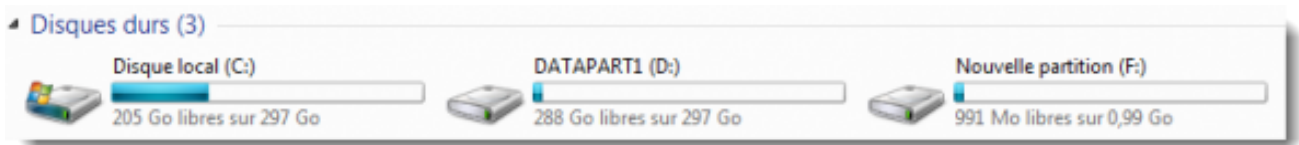
Suivez l'assistant de création de volumes qui s'affiche. Celui-ci vous permettra notamment de renommer la nouvelle partition, de choisir le système de fichier à utiliser...

Patiencez lors du formatage de la partition par Windows. Une fois l'opération terminée, votre nouvelle partition s'affiche avec sa description comme dans l'image ci-dessous :



c) Votre nouveau disque est prêt

Depuis le menu Démarrer ou le bureau, rendez-vous dans **Ordinateur**. Le nouveau disque apparaît prêt à être utilisé et vous pouvez y copier vos fichiers depuis les autres disques.



4) Le système de fichiers

4.1. Introduction

Les disques durs, aussi petits soient-ils, contiennent des millions de bits, il faut donc organiser les données afin de pouvoir localiser les informations, c'est le but du **système de fichiers**. Un disque dur est, rappelons-le, constitué de plusieurs plateaux circulaires tournant autour d'un axe. Les pistes (zones concentriques écrites de part et d'autre d'un plateau) sont divisées en quartiers appelés secteurs (d'une taille de 512 octets). Le formatage logique d'un disque permet de créer un système de fichiers sur le disque, qui va permettre à un système d'exploitation (DOS, Windows, UNIX, ...) d'utiliser l'espace disque pour stocker et utiliser des fichiers. Le système de fichiers est basé sur la gestion des clusters (en français « unité d'allocation »), c'est-à-dire la plus petite unité de disque que le système d'exploitation est capable de gérer.

Les tables d'allocation de fichiers (FAT et MFT) ont trois fonctions principales :

- le suivi de l'espace alloué et libre,
- la gestion des répertoires et noms de fichiers
- le suivi de l'emplacement dans lequel les différentes parties de chaque fichier sont physiquement stockées sur le disque.

C'est donc une façon de stocker les informations et de les organiser sur des périphériques de stockage (disque dur, CD-ROM, clé USB, etc.).

Attention, le système de fichiers ne dépend ni du type d'ordinateur, ni du disque dur, il est lié à l'OS uniquement.

4.2. Quelques définitions

FAT = File Allocation Table

MFT = Master File Table (table allocation du système NTFS)

Le chemin d'accès est une formule qui sert à indiquer l'emplacement où se trouve un fichier dans l'arborescence du système de fichiers. La syntaxe de la formule diffère d'un système d'exploitation à l'autre.

La taille du fichier indique la quantité d'informations conservée, exprimée en octets.

La taille physique indique la place réservée dans la mémoire - en octets - pour conserver le fichier ainsi que ses caractéristiques. La taille physique est légèrement supérieure à la taille du fichier.

L'extension est un suffixe ajouté au nom du fichier pour indiquer la nature de son contenu.

La journalisation d'un système de fichiers enregistre les opérations d'écriture tant qu'elles ne sont pas terminées et cela en vue de garantir l'intégrité des données en cas d'arrêt brutal.

Sans un tel fichier journal, un outil de récupération de données après un arrêt brutal doit parcourir l'intégralité du système de fichier pour vérifier sa cohérence. Lorsque la taille du système de fichiers est importante, cela peut durer très longtemps (jusqu'à plusieurs heures) pour un résultat parfois moins efficace (possibilité de perte de données). **Un système de fichiers journalisé** travaille de façon à prévenir une corruption. Lors de la sauvegarde d'un fichier, au lieu d'écrire immédiatement sur le disque dur les données à l'endroit exact où elles devraient être enregistrées, le système de fichiers écrit les données dans une autre partie du disque dur et note les changements nécessaires dans un journal, et ensuite, en arrière-plan, il repasse chacune des entrées du journal et termine le travail commencé ; lorsque la tâche est accomplie, il raye la tâche de la liste.

La gestion des droits d'accès aux fichiers et répertoires permet d'associer des droits d'écriture, de lecture et d'exécution pour des fichiers et/ou dossiers à des utilisateurs ou à des groupes d'utilisateurs du système.

5) Quel système de fichiers choisir ?

En réalité le choix du système de fichiers se fait en premier lieu suivant le système d'exploitation que vous utilisez. D'une manière générale, plus le système d'exploitation est récent plus le nombre de systèmes de fichiers supporté sera important. Ainsi, sous DOS et sur les premières versions de Windows la FAT16 était de rigueur.

A partir de Windows 95 OSR2 vous avez le choix entre les systèmes de fichiers FAT16 et FAT32. Si jamais la taille de la partition est supérieure à 2Go, le système de fichier FAT16 est exclu, vous devez donc utiliser le système FAT32 (ou modifier la taille de la partition).

En dessous de cette limite, la FAT16 est recommandée pour des partitions d'une capacité

inférieure à 500Mo, dans l'autre cas l'utilisation de FAT32 est préférable.

Dans le cas de Windows NT (jusqu'à la version 4) vous avez le choix entre le système FAT16 et NTFS, par contre celui-ci ne supporte pas la FAT32. D'une manière générale le système NTFS est conseillé car il procure une sécurité plus grande ainsi que des performances accrues par rapport à la FAT. Microsoft recommande en fait d'utiliser une petite partition (comprise entre 250 et 500Mo) de type FAT pour le système d'exploitation, afin de pouvoir démarrer à partir d'une disquette DOS bootable en cas de malheur, et de conserver les données sur une seconde partition pour stocker vos données.

Sous Windows NT5 l'éventail s'agrandit puisqu'il accepte des partitions de type FAT16, FAT32 et NTFS. Une fois de plus, le système de fichiers le plus récent (NTFS 5) est conseillé, puisqu'il offre de plus nombreuses fonctionnalités. Pour les mêmes raisons que précédemment vous pouvez toutefois opter pour une partition de type FAT.

Systeme d'exploitation	Types de systeme de fichiers supportés	Journalisation	Gestion des droits
DOS	FAT16		
Windows 95 OSR2	FAT16 FAT32		
Windows 98	FAT16, FAT32		
Windows 2000/XP/ Vista/ Win 7	FAT, FAT16, FAT32, NTFS(4),NTFS(5)	NTFS(5)	NTFS(4),NTFS(5)
Linux	Ext2, Ext3, Ext4,ReiserFS, FAT16, FAT32, NTFS	Ext3, Ext4, ReiserFS,NTFS	Ext2, Ext3, Ext4, ReiserFS,
MacOS	HFS (Hierarchical File System), HFS+ (version étendue)	HFS+	HFS+
FreeBSD, OpenBSD Solaris dorénavant Oracle Solaris depuis le rachat de Sun par Oracle en janv 2010.	UFS (Unix File System)	UFS	UFS

Lorsque plusieurs systèmes d'exploitation cohabitent sur une même machine, le problème du choix du système de fichiers se pose. En effet, le système de fichiers est étroitement lié au système d'exploitation, ainsi lorsqu'il y a plusieurs systèmes d'exploitations, il faut choisir pour chacun d'entre eux le système de fichiers en prenant en compte le fait qu'il est possible que l'on ait à accéder à des données de l'un à partir de l'autre. Une première solution consiste à utiliser des partitions FAT pour tous les systèmes, en faisant attention à n'utiliser que des partitions d'une taille inférieure à 2Go. La solution la plus adaptée est d'utiliser pour chacun des systèmes une partition dont le système de fichiers est le plus adapté, et de dédier une partition en FAT16 aux données vouées à être partagées par les différents systèmes d'exploitation.

6) FAT et NTFS

6.1. FAT

La FAT (File Allocation Table) est une structure contenant la liste des clusters utilisés et non utilisés. Chaque partition comporte, en plus de la FAT originale, une copie de sauvegarde située juste après la FAT originale en début de partition (juste après le secteur de boot), afin que le système puisse récupérer celle-ci si la FAT originale s'avérait corrompue. Chaque FAT occupe plusieurs milliers de clusters sur la partition.

Lorsque l'on crée un fichier ou un sous-répertoire, les informations correspondantes sont

stockées dans la FAT sous la forme de données hexadécimales détaillant le nom et la taille du fichier, la date et l'heure de sa dernière modification, le numéro de cluster de départ et l'attribut (Archive, Caché, Système...). C'est une liste de valeurs numériques permettant de décrire l'allocation des clusters d'une partition, c'est-à-dire l'état de chaque cluster de la partition dont elle fait partie. La table d'allocation est en fait un tableau dont chaque cellule contient un chiffre qui permet de savoir si le cluster qu'elle représente est utilisé par un fichier, et, le cas échéant, indique l'emplacement du prochain cluster que le fichier occupe. On obtient donc une chaîne FAT, c'est-à-dire une liste chaînée de références pointant vers les différents clusters successifs jusqu'au cluster de fin de fichier. Chaque entrée de la FAT a une longueur de 16 ou 32 bits (selon qu'il s'agit d'une FAT16 ou d'une FAT32). Les deux premières entrées permettent de stocker des informations sur la table elle-même, tandis que les entrées suivantes permettent de référencer les clusters. Certaines entrées peuvent contenir des valeurs indiquant un état du cluster spécifique. Ainsi la valeur 0000 indique que le cluster n'est pas utilisé, FFF7 permet de marquer le cluster comme défectueux pour éviter de l'utiliser, et les valeurs comprises entre FFF8 et FFFF spécifient que le cluster contient la fin d'un fichier.

6.2. NTFS (New Technology File System)

La MFT (Master File Table) constitue la structure centrale du système de fichiers NTFS et, comme pour la FAT, il existe une copie de sauvegarde sur la partition (MFT Mirror) permettant de se protéger d'une perte éventuelle des données. Là encore la MFT occupe plusieurs milliers de clusters et par défaut NTFS lui réserve 12,5 % de l'espace disponible sur la partition (les données ne pouvant pas être écrites sur cette zone réservée), ce qui évite la fragmentation de la MFT.

On peut définir dans la base de registre la taille de la MFT en fonction du type de fichiers que l'on a l'habitude d'enregistrer : si l'on enregistre beaucoup de petits fichiers (de nombreux documents textes par exemple) il vaut mieux avoir une grande MFT (car il y aura beaucoup d'entrées), mais si on enregistre des fichiers peu nombreux mais volumineux (des films par exemple), il vaut mieux avoir une petite MFT pour laisser le plus possible de place sur la partition pour ces gros fichiers :

En d'autres termes, on peut augmenter la MFT (et ça peut améliorer les performances) tant qu'il reste suffisamment d'espace libre sur la partition. Par contre s'il reste peu d'espace libre sur la partition, augmenter la MFT risque de favoriser sa fragmentation (car des fichiers ne trouvant pas de place sur la partition viendront s'y loger) et on aura l'effet inverse de celui attendu... seuls certains logiciels permettent de défragmenter la MFT en faisant une défragmentation au démarrage de l'ordinateur.

Pour le réglage de la taille de la MFT dans la base de registre, il faut sauvegarder au préalable son registre puis chercher la clé suivante :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem >
```

clic droit sur la valeur NtfsMftZoneReservation et lui attribuer une valeur entre 1 et 4 selon l'espace que l'on veut réserver pour la MFT (12.5 %, 25 %, 37.5 %, 50 % de l'espace partitionné). Puis quitter le registre et redémarrer le PC...

6.3. Avantages NTFS/FAT

a) Sécurité, gestion des droits d'accès

Sur le plan des caractéristiques techniques, le système NTFS offre :

- la compression (Compresser le lecteur pour augmenter l'espace disque disponible),

- le cryptage (**Cryptage des fichiers (EFS)** améliore la sécurité en particulier pour les entreprises en cryptant certains fichiers ou dossiers pour en restreindre l'accès à certains utilisateurs),
- les autorisations d'accès et les niveaux de permissions (**Autorisations** : elles peuvent être définies avec précision pour chaque utilisateur, sur les fichiers ou dossiers. En **FAT32** tous les utilisateurs auront accès à tous les fichiers de votre disque dur, quel que soit leur type de compte : administrateur, limité ou standard),
- la gestion des quotas de disque (permet d'analyser et de contrôler la quantité d'espace disque utilisée par chaque personne),
- l'utilisation des fonctionnalités importantes comme Active Directory (nécessaire pour les domaines, les comptes d'utilisateurs et d'autres fonctionnalités de sécurité importantes) et la sécurité basée sur les domaines
- les points de montage, le stockage étendu, etc.

Le seul réel inconvénient intervient en cas de multiboot avec des systèmes d'exploitation qui ne gèrent pas le NTFS (Win 9x jusqu'à ME) sans l'aide d'utilitaires spécifiques.

b) Taille des clusters

Vient ensuite un problème lié à la taille des clusters. On sait qu'un cluster est la plus petite unité d'allocation décidée par l'OS pour le stockage des données. Un cluster a une taille fixe qui dépend de la taille totale de la partition et du système de partitionnement. On ne trouvera jamais plus d'un fichier dans un cluster. En conséquence, si un fichier est plus petit que la taille minimale d'un cluster, il existe de l'espace perdu.

Taille de la partition	Taille des clusters		
	FAT 16	FAT 32	NTFS
7 Mo – 16 Mo	2 Ko	Pas supporté	512 octets
17 Mo – 32 Mo	512 octets	Pas supporté	512 octets
33 Mo – 64 Mo	1 Ko	512 octets	512 octets
65 Mo – 128 Mo	2 Ko	1 Ko	512 octets
129 Mo – 256 Mo	4 Ko	2 Ko	512 octets
257 Mo – 512 Mo	8 Ko	4 Ko	512 octets
513 Mo – 1.024 Mo	16 Ko	4 Ko	1 Ko
1.025 Mo – 2 Go	32 Ko	4 Ko	2 Ko
2 Go – 4 Go	64 Ko	4 Ko	4 Ko
4 Go – 8 Go	Pas supporté	4 Ko	4 Ko
8 Go – 16 Go	Pas supporté	8 Ko	4 Ko
16 Go – 32 Go	Pas supporté	16 Ko	4 Ko
32 Go – 2 To	Pas supporté	Pas supporté	4 Ko

Donc pour 1 disque dur de plus de 10 Go, on peut considérer que la FAT 32 va gâcher 2 à 8 fois plus d'espace que le NTFS.

c) Performances

Un autre avantage du système NTFS tient à sa plus grande **rapidité d'accès aux disques durs** (sauf, à la rigueur, sur ceux de petite capacité).

La recherche d'un fichier prendra plus de temps sur un disque partitionné en FAT (16 ou 32) que sur le même disque partitionné en NTFS, le système sous FAT devant parcourir obligatoirement toute la structure d'un dossier contrairement au système NTFS en dépit du

fait que ce système doit en outre vérifier les permissions sur le fichier recherché. Les accès sont plus rapides, mais aussi moins nombreux. Pour être plus précis, on peut estimer que le système NTFS est au moins aussi performant sur des disques de petite taille que le système FAT, et **bien plus performant que le système FAT sur des disques de grande capacité**.

S'agissant du temps de démarrage de la machine, le système FAT on le sait requiert la lecture complète de la structure de la FAT. Les performances en écriture et en lecture sont également affectées par le système FAT32 qui, pour les mêmes raisons citées, doit analyser toute la FAT afin de déterminer l'espace libre sur le disque.

d) Taille max fichier, partition

Autre avantage, destiné en particulier aux amateurs d'édition vidéo ou musicale, NTFS ne connaît pas la limite de taille de fichier de 4 Go. En FAT il est en effet impossible de créer un fichier d'une taille supérieure à 4 Go. Sous NTFS, la taille limite d'un fichier correspond à celle du disque dur (de la partition plus exactement).

Question taille des dossiers (répertoires), la FAT peut adresser jusqu'à 65.534 entrées (et moins sur la racine), la FAT 32 également tandis que NTFS ne connaît pas de limite à cet égard. On peut résumer les aptitudes des différents systèmes de partitionnement à l'aide du tableau suivant :

Description	FAT16	FAT32	NTFS
Taille maximale d'1 fichier	4 Go	4 Go	Non limitée (la limite est l'espace disponible sur la partition !)
Nbre max de fichiers par volume	65.535	4.194.303	4.294.967.295
Taille maximale d'une partition	2 Go à 4 Go	8 Go, en théorie 8 To	Théorique: 16 Eo (exaoctets) 2 To Actuellement 128 Go
Nbre max d'entrées (fichier ou dossier) à la racine du disque	512 entrées	Limité par la taille du disque	Pas de limite

Remarque : Sous Windows 2000 / XP / Vista / 7 le formatage en FAT32 est limité à 32 Go (si vous choisissez une valeur supérieure, seul le NTFS vous sera proposé).

6.4. Convertir FAT32 en NTFS avec Win7

La **conversion** d'une partition en NTFS est simple à réaliser et ne prend que quelques instants. Il ne faut pas confondre cette opération avec le **formatage** lui-même qui est une opération destructrice de données. Seulement, on dit parfois que l'intérêt du formatage en NTFS sur la simple conversion est un meilleur alignement des clusters avec ce type de partition, alors que la conversion n'opère aucune modification de ce côté là.

Nous allons voir comment convertir un système de fichiers FAT 32 en NTFS, sans perdre les données qui y sont liées. Il est néanmoins fortement conseillé d'effectuer une sauvegarde des données converties, même si le risque de corruption des données est minimal.

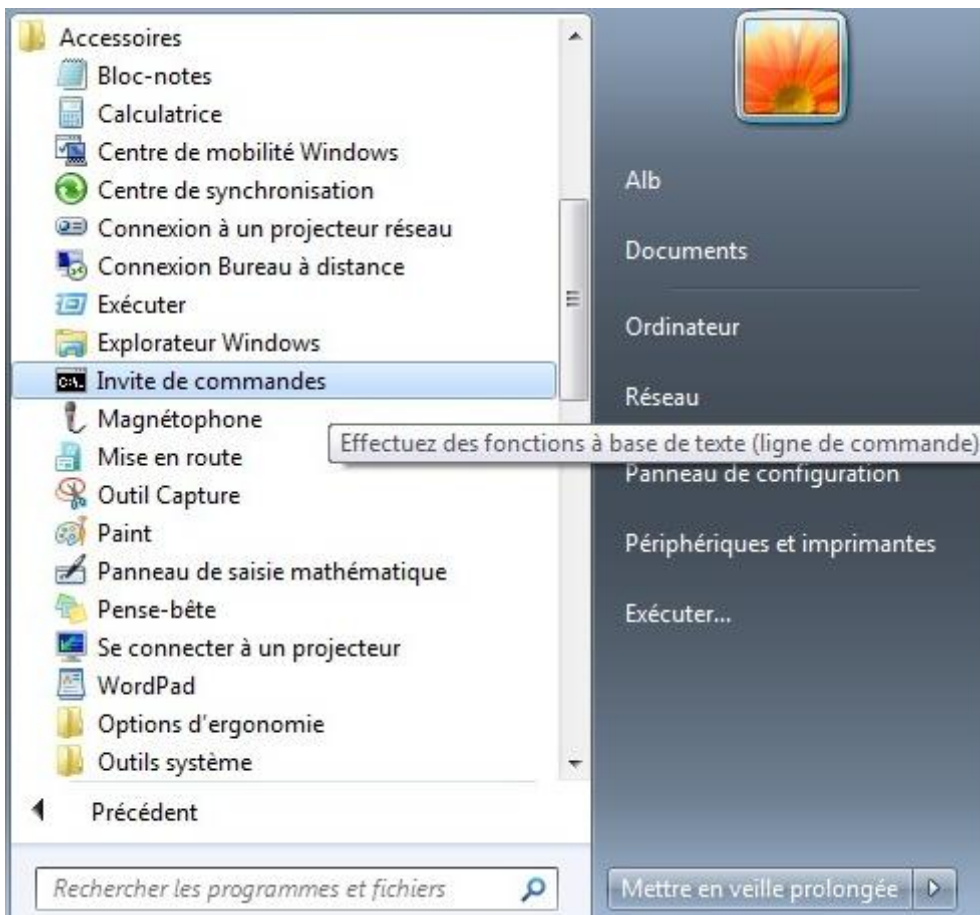
Attention, la conversion sans perte de données ne peut se faire que de FAT32 vers NTFS, et pas inversement.

Si vous avez la possibilité de supprimer les données ou les stocker temporairement sur un autre support, il vaut mieux le faire pour pouvoir formater le support en NTFS plutôt que de le convertir, et repartir avec un support bien propre comme il faut

a) Invite de commandes

Tout d'abord, ouvrez une invite de commande en mode administrateur. Pour ce faire, allez dans :

Démarrer => Accessoires => Effectuez un clic droit sur "Invite de commandes" puis sélectionnez "Exécuter en tant qu'administrateur"



b) Lettre du lecteur

Il faut maintenant repérer la lettre du lecteur que vous souhaitez convertir. Il vous suffit pour cela de vous rendre sur le poste de travail, et de regarder quelle lettre a été attribuée au lecteur en question :



Dans cet exemple, nous allons convertir une clé USB de 16Go à laquelle la lettre G: a été attribuée.

c) Commande « convert »

Utilisez la commande **convert** pour lancer la conversion, elle se présente comme suit :

```
convert LETTRE: /fs:ntfs
```

Donc dans l'exemple :



```

CA. Administrateur : Invite de commandes - convert G: /fs:ntfs
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Alb>convert G: /fs:ntfs
Le type du système de fichiers est FAT32.

```

Validez en appuyant sur **Enter**, et le prompt vous donne alors le type de système de fichiers sur le lecteur en cours de conversion. On voit bien sur l'image ci-dessus que la clé était formatée en **FAT32**.

d) Fin !

Voilà, il vous suffit d'attendre un peu, la conversion des 16Go de la clé n'a pris que quelques secondes... (Si vous convertissez un système de quelques TeraOctets, ça prendra un peu plus de temps !)



```

CA. Administrateur : Invite de commandes
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Alb>convert G: /fs:ntfs
Le type du système de fichiers est FAT32.
Volume ALB' a créé 03/03/2010 22:51
Le numéro de série du volume est D5F1-E281
Windows vérifie les fichiers et les dossiers...
Vérification des fichiers et des dossiers terminée.
Windows a vérifié le système de fichiers sans trouver de problème.
 15 647 784 Ko d'espace disque au total.
      368 Ko dans 42 dossiers.
  5 324 248 Ko dans 815 fichiers.
 10 323 160 Ko sont disponibles.

      8 192 octets dans chaque unité d'allocation.
  1 955 973 unités d'allocation au total sur le disque.
  1 290 395 unités d'allocation disponibles sur le disque.

Détermination de l'espace disque requis pour la conversion du systè
de fichiers...
Espace disque total :          15663084 Ko
Espace libre sur le volume :    10323160 Ko
Espace requis pour la conversion : 86286 Ko
Conversion du système de fichiers
La conversion est terminée

C:\Users\Alb>_

```

On voit maintenant sur le poste de travail que la clé est bien en NTFS, et pourra donc accueillir des fichiers de plus de 4Go sans souci



Chapitre 6. Le démarrage et le BIOS

Lorsque l'utilisateur met sa machine sous tension l'OS n'est pas directement chargé, le démarrage du PC se déroule suivant les étapes suivantes :

- Un 1^{er} programme de base, le **BIOS** (Basic Input/Output System), se trouvant sur la carte mère est activé.

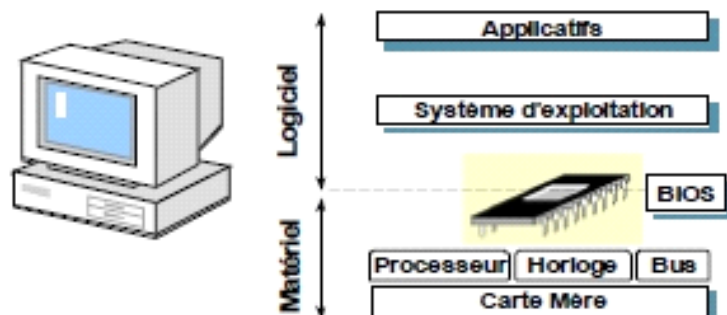
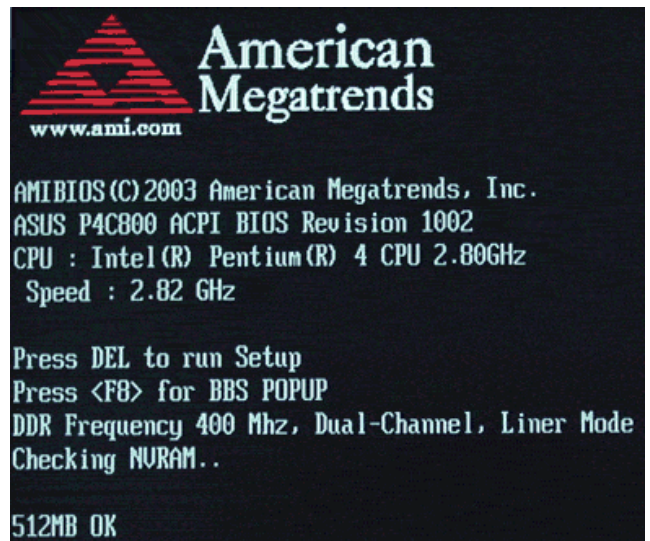
Il sert d'interface entre la partie matérielle (la carte mère et ses périphériques) et le Système d'Exploitation.

En effet il va localiser et vérifier l'intégrité des principaux composants du PC (disque dur, mémoire, clavier, ports...). Ensuite il recherchera un OS sur le disque dur ou le lecteur CD.

Il est contenu dans une mémoire morte située sur la carte mère.

Un autre élément important est associé au BIOS : la mémoire **CMOS** qui stocke tous les paramètres du BIOS. Cette mémoire est sauvegardée à l'aide d'une pile se trouvant sur la carte mère.

- Lorsque le système d'exploitation est trouvé, il est alors chargé dans la mémoire centrale et active la communication entre l'utilisateur et l'ordinateur.



1) Test POST et BIOS

Lorsque le système est mis sous-tension ou réamorcé (Reset), le BIOS fait l'inventaire du matériel présent dans l'ordinateur et effectue un test (appelé **POST**, pour "Power-On Self Test") afin de vérifier son bon fonctionnement.

Si le POST rencontre une erreur le BIOS va arrêter le système et :

- afficher un message à l'écran si possible (le matériel d'affichage n'étant pas forcément encore initialisée ou bien pouvant être défaillant),
- émettre un signal sonore, sous forme d'une séquence de bips (beeps en anglais) permettant de diagnostiquer l'origine de la panne,
- envoyer un code (appelé code POST) sur le port série de l'ordinateur, pouvant être récupéré à l'aide d'un matériel spécifique de diagnostic.

Le POST (séquence de vérification du BIOS) effectue des tests concernant :

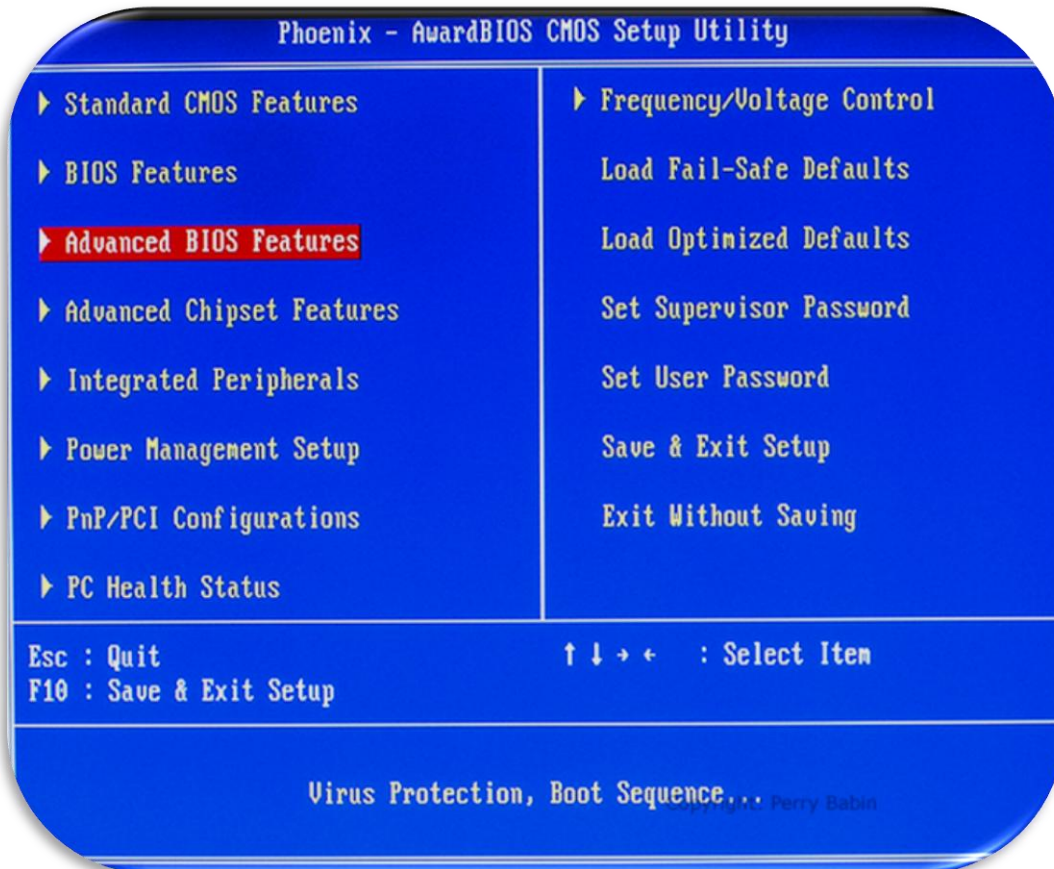
- Le processeur (CPU)

- Le BIOS
- La configuration du CMOS
- L'initialisation de l'horloge interne
- L'initialisation du contrôleur DMA (*Direct Memory Access*, canal qui permet l'accès direct à la mémoire vive)
- La vérification de la mémoire vive et la mémoire cache
- L'installation de toutes les fonctions du BIOS
- La vérification de toutes les configurations (clavier, disques durs ...)

1.1. Messages d'erreurs possibles au démarrage du BIOS

- **CMOS CHECKSUM FAILURE** : problème avec la pile, remplacez-la.
- **BIOS ROM CHECKSUM ERROR-SYSTEM HALTED** : **erreur BIOS**. Remplacez la puce du BIOS.
- **KB/INTERFACE ERROR** : le clavier est endommagé ou mal branché.
- **FDD CONTROLLER FAILURE** : erreur du contrôleur du lecteur de disquettes. Vérifiez si la nappe floppy est branchée correctement. Si le problème persiste, changez le contrôleur.
- **HDD CONTROLLER FAILURE** : vérifiez si la nappe IDE est bien connectée. Si le problème persiste, changez de nappe puis de contrôleur.
- **MEMORY ERROR DURING MEMORY TEST** : vérifiez si les barrettes mémoire sont enfoncées correctement.
- **CMOS SYSTEM OPTIONS NOT SET RUN SETUP UTILITY** : aucun paramètre n'est défini dans le Setup du BIOS. Lancez le BIOS et configurez les paramètres.
- **CMOS MEMORY SIZE MISMATCH** : la mémoire déclarée n'est pas physiquement installée.
- **UNABLE TO INITIALIZE HARD DRIVE (DRIVE TYPE 1)** : l'unité du disque dur a été mal définie. Passez les paramètres en "AUTO" dans la configuration des disques durs.
- **KEYBOARD IS LOCKED** : le clavier est verrouillé. Déverrouillez-le en mettant la clé dans la serrure présente sur la façade de certains PC et tournez-la. Redémarrez ensuite le PC ou appuyez sur une touche. Pour certaines cartes mères, il vous faut enlever (ou déplacer) un cavalier qui empêche l'utilisation du clavier.
- **Cache memory bad, do not enable cache** : défaillance de la mémoire cache. Désactivez le cache L 1 (et L2) du processeur.
- **Address line short** : problème logique dans le décodage d'une adresse mémoire. Le problème peut venir d'une perturbation magnétique. Éteignez et rallumez le PC une minute après.
- **On board parity error** : erreur de parité dans la mémoire de la carte mère. Faites une vérification antivirale du BIOS.
- **DMA bus time out** : un périphérique a monopolisé les signaux du bus pendant une durée supérieure à la durée allouée (7,8 microsecondes). Généralement, le périphérique incriminé est défectueux. Remplacez ce périphérique.
- **No ROM Basic** : aucune unité de boot n'est définie dans le Setup du Bios. Définissez un lecteur sur lequel booter.

1.2. Configuration du Bios



Suivant les cartes mères, les BIOS peuvent présenter des options un peu différentes. Pour accéder à l'interface du Bios (**Setup du BIOS**), il faut faire une combinaison de touches qui s'affiche au bas de l'écran lors du démarrage du PC. Par exemple: « Press F1 to continue », « DEL to enter SETUP »

Voici les plus connues : [DEL] ; [ESC] ; [F1] ; [F2] ; [F10] ; (ALT) + [Entrée] ; ETC.

La configuration et la modification du BIOS d'une carte mère permettent entre autre de:

- Déterminer l'ordre de démarrage (Boot sequence):

Ces commandes sont généralement présentes dans les menus *Bios Features Setup* ou *Advanced CMOS Setup* ou *Boot*. Quand votre système démarre, il cherche un système d'exploitation à partir d'un ordre prédéfini de lecteurs. (Exemple : sur le lecteur DVD lors de la réinstallation d'un système d'exploitation)

- Paramétrer les périphériques intégrés :

Exemples : désactiver la carte son, changer l'ordre d'initialisation des cartes graphiques s'il y en a deux.

- Paramétrer la carte graphique :

Un nouveau paramètre est intéressant à tester si votre carte mère est récente. Dans le menu *Bios Features Setup* ou *Advanced CMOS Setup*, vous allez trouver une commande ressemblant à *Video Memory Cache Mode* ou *Video RAM Cache Methode/Write Combining*. Placez l'option UC sur *Enable* ou *USWC*. C'est une technologie permettant d'accélérer les échanges entre votre processeur et le cache de votre carte graphique.

- Paramétrer le port USB :

Exemple : paramétrer USB 3.0, USB 2.0 (les ports USB2.0 doivent être paramétrés en *full speed* et non en *high speed*).

- Sécuriser l'accès au BIOS :

Ces commandes sont généralement présentes dans le menu *Password Settings*. La commande *System Password* permet de définir un mot de passe dès l'ouverture de votre ordinateur. La commande *Setup Password* ne bloque que l'accès au BIOS. Il faudra choisir entre ces deux options : *System* ou *Setup*.

- Restaurer les réglages par défaut :

Il y a sur tous les BIOS deux options : régler le BIOS sur les paramètres servant au dépannage (*Load Bios Default*), ou régler le BIOS sur les paramètres optimisés (*Load Setup Default*). Dans les deux cas, le BIOS sera réinitialisé sur un certain nombre de réglages définis par le constructeur.

- Paramétrer la gestion de la mémoire :

Il existe une multitude de réglages permettant une gestion plus fine de la RAM.

- Protéger le PC en empêchant la modification du secteur de boot d'un disque (boot virus detection), en empêchant la modification du bios (bios update).

Le BIOS est indépendant du système d'exploitation, si vous installez deux systèmes, le BIOS sera le même.

2) Le MBR

Le **MBR (Master Boot Record)** aussi appelé secteur principal de démarrage (secteur de boot) ou zone amorce, est le nom donné au 1^{er} secteur de chaque disque dur (1^{er} secteur de la 1^{ère} piste du 1^{er} cylindre). Il y en a donc 1 par disque dur et sa taille est toujours de 512 octets (logique puisqu'il est égal à 1 secteur et qu'1 secteur fait toujours 512 octets !).

Ces 512 octets sont divisés en plusieurs parties, chacune de ces parties est nécessaire au démarrage de l'ordinateur : les 446 du début correspondent au boot et les suivants indiquent la structure de partitions du disque.

Le MBR contient en effet :

- **La table de partitions du disque dur** (64 octets), indiquant l'emplacement de ou des partitions présentes sur le disque, 4 partitions primaires ou étendues maximum.
- **Une routine d'amorçage** (446 octets) pour charger sur une partition (partition système) le système d'exploitation ou un « Boot Loader » (logiciel permettant de lancer un ou plusieurs systèmes)
- **Les messages d'erreur du POST**

Le rôle du MBR est de passer la main au chargeur d'amorçage. Ce chargeur d'amorçage indique quel système d'exploitation il faut lancer. Chaque système d'exploitation qu'on installe propose son propre chargeur d'amorçage :

- Pour Windows NT 3.0, NT 4.0, 2000, XP et Serveur 2003, le chargeur d'amorçage s'appelle NTLDR (NT Loader) qui lit le fichier c:\boot.ini.
- Windows Vista utilise un nouveau chargeur d'amorçage qui se compose de 2 fichiers : c:\bootmgr en plus de c:\boot.ini.
- Le chargeur d'amorçage de Linux peut être GRUB (GRand Unified Bootloader) ou LILO (Linux LOader).

Chacun de ces chargeurs d'amorçage est capable de gérer le multiboot (lancement de plusieurs OS). Selon les chargeurs, cela se fait plus ou moins facilement.

Il est possible d'installer et de faire cohabiter sur un même disque plusieurs systèmes d'exploitations (ex : Win XP et Linux). Dans ce cas chaque système d'exploitation et son système de fichiers seront installés sur une partition différente.

Le MBR est donc essentiel pendant la phase de démarrage d'un système d'exploitation sur un disque dur. Si la table de partitions indiquant la structure du disque dur et/ou la routine d'amorçage sont défectueuses, votre ordinateur sera bloqué et inutilisable.

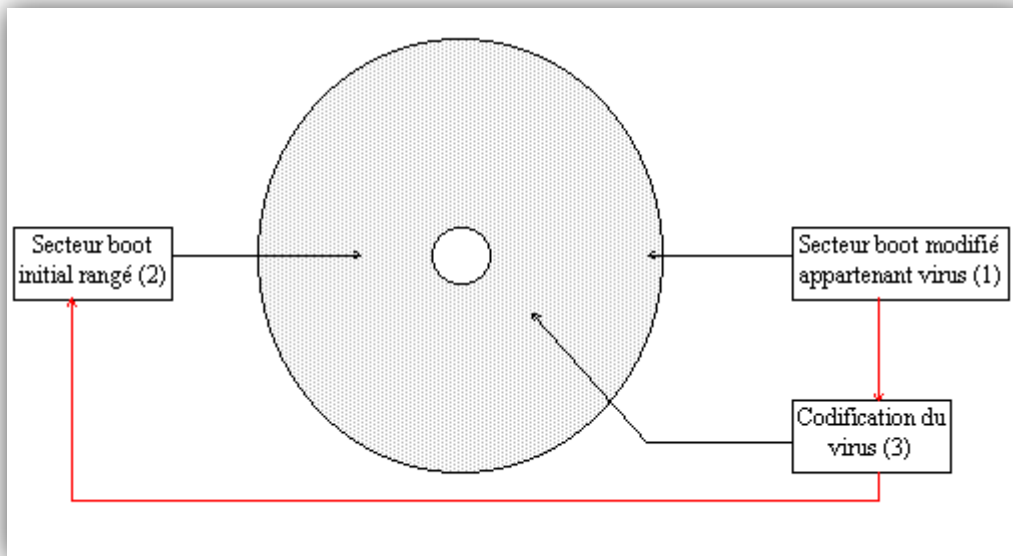
2.1. Virus de boot

Même chose si le PC est infecté par un virus de boot : Il s'installe dans le MBR. Il remplace un chargeur d'amorçage existant mais ne modifie pas un programme comme un virus normal.

a) Fonctionnement :

Les virus de boot modifient le contenu du secteur de démarrage (MBR) du disque en remplaçant son contenu initial par leur propre version. La version d'origine est normalement "rangée" ailleurs sur le disque ce qui fait que lorsqu'il y a exécution des instructions contenues dans le secteur démarrage du disque (démarrage de l'ordinateur sur le disque dur), c'est le virus qui s'exécute en premier. Le mécanisme d'infection de ce virus s'opère sur trois points clefs :

1. Le secteur de démarrage est remplacé par une version altérée, c'est la voie d'accès du virus.
2. Un secteur libre est utilisé pour stocker le secteur de démarrage initial.
3. Un certain nombre de secteurs libres servent à stocker l'ensemble de la codification du virus.



b) Que faire ?

- Protéger le MBR :

Vous avez, dans les BIOS de vos machines, un paramètre appelé "Antivirus". Ce n'est pas réellement un antivirus mais une surveillance de toute tentative de modification du MBR. Cet "antivirus" devrait toujours être activé afin de verrouiller la zone MBR. C'est une interdiction d'écrire dans ces zones que vous devez positionner sur "on" ou "actif" dès

après l'installation du système d'exploitation. Aucun autre programme ne devra, par la suite, vous demander l'autorisation de modifier ce 1^{er} secteur.

- Restaurer le MBR :

Voici quelques procédures de récupération ou de sauvegarde possibles. **Attention** certaines manipulations sont à effectuer avec attention et si possible en consultant la documentation associée à la ou aux commandes:

2.2. Sous windows

a) MS DOS

Sous MS-DOS et les versions de Windows jusqu'à Windows Millenium, il est possible à partir d'une disquette de démarrage de recréer la routine de boot du MBR à l'aide de la commande **FDISK /MBR**. Le Master Boot Record est ainsi réécrit. Cela permet d'éliminer certains virus de boot, de restaurer un MBR endommagé (le PC ne démarre plus), ou de supprimer un chargeur de démarrage installé dans le MBR (ex: lilo, GRUB, si une distribution Linux a été installée parallèlement à Windows).

b) XP

Sous Windows XP, la commande à utiliser pour restaurer le MBR est **fixmbr**. Elle est accessible depuis la console de récupération. ! il faut le CD d'installation.

Différence entre Fixboot et fixmbr : - FIXBOOT [FIXBOOT nom_du_lecteur] écrit un nouveau code de secteur de démarrage de Windows dans la partition de démarrage. Ceci résout le problème à l'endroit où le secteur de démarrage de WindowsXP est endommagé.

- FIXMBR [FIXMBR (nom_du_périphérique)] répare le secteur de démarrage principal de la partition système. Cette méthode s'applique lorsqu'un virus a endommagé le secteur de démarrage principal et que Windows ne peut démarrer. Attention: Cette commande peut endommager vos tables de partition et les rendre inaccessibles! Utilisez donc cette commande prudemment...

Comment faire ?

Redémarrez votre PC avec le CD de Windows XP (fonctionne aussi avec VISTA) et choisissez l'option Réparer, puis dans l'invite de commande tapez fixboot c: puis appuyez sur la touche Entrée. Tapez O pour oui.

Si rien n'a changé au démarrage suivant, retournez dans la console (via l'option Réparer) et tapez cette fois fixmbr, ce qui aura pour effet d'écraser le secteur de boot (attention si vous êtes en multiboot, donc si vous avez plus d'un système d'exploitation sur votre PC). Redémarrez ensuite votre ordinateur.

c) Vista - 7

Sous Windows Vista et Windows 7, la commande à utiliser pour restaurer le MBR est **bootrec /FixMbr**. Elle est accessible depuis la console de récupération.

Exemple avec Win 7 :

- Démarrez le système sur le **DVD d'installation de Windows 7**

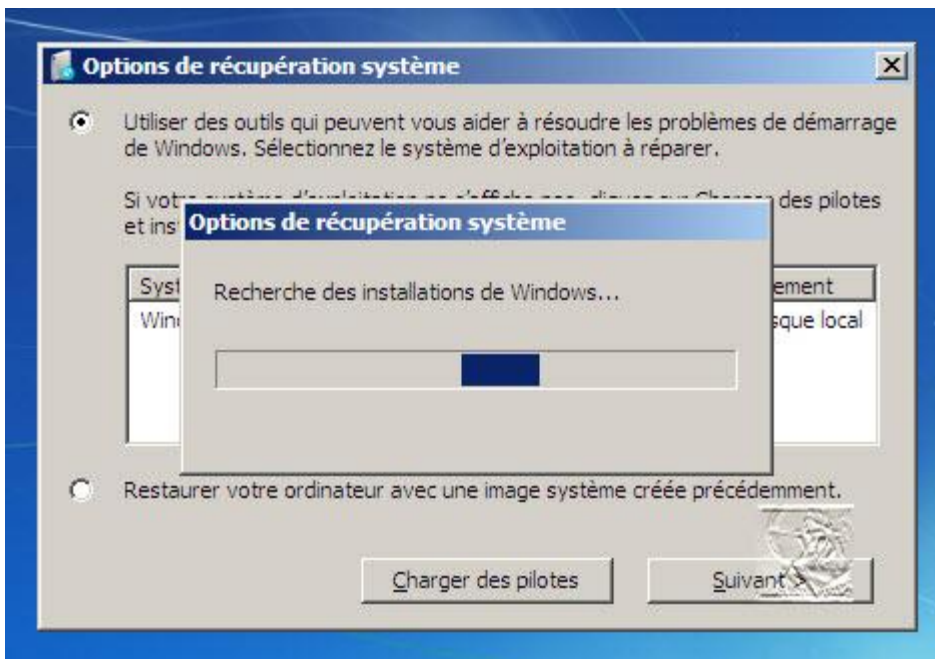
Windows charge les fichiers, puis la fenêtre du **choix de langue** apparaît. Cliquez sur **Suivant** :



- Cliquez sur **Réparer l'ordinateur** (en bas à gauche)

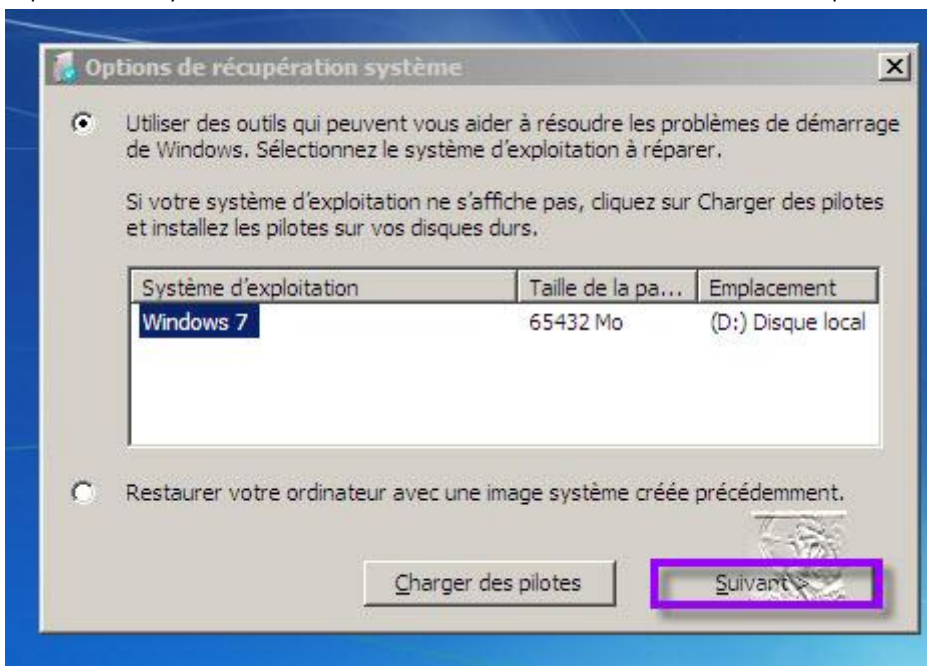


Une recherche des installations Windows se lance :

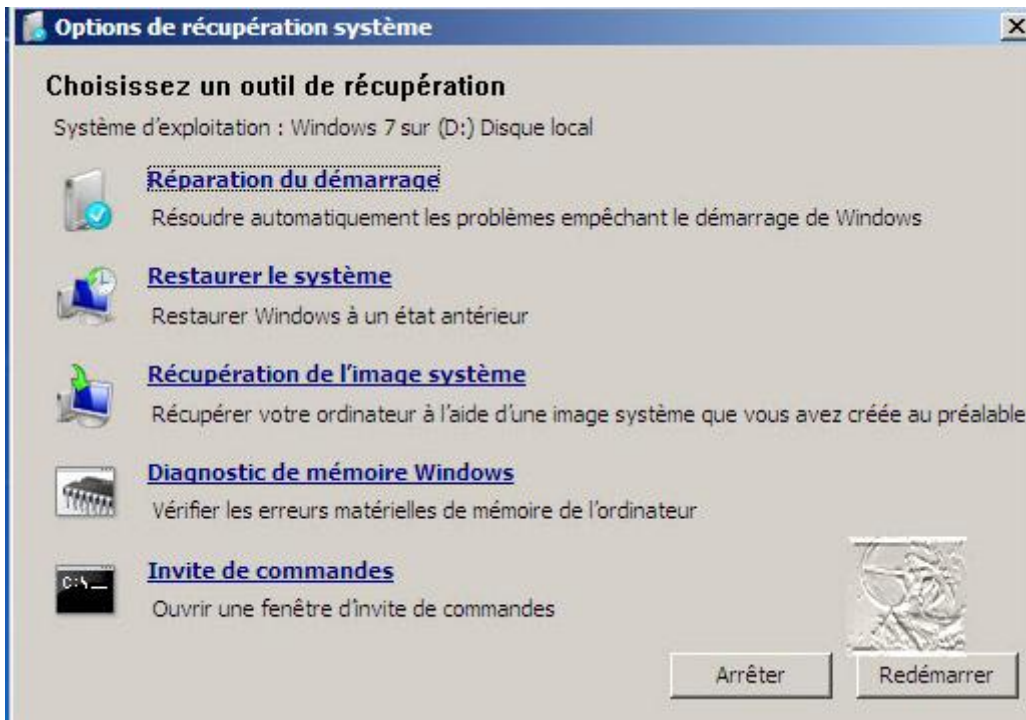


Le système d'exploitation Windows 7 est trouvé.

Si plusieurs systèmes sont installés, sélectionnez **Windows 7**, puis cliquez sur **Suivant**.



- La fenêtre des **options de récupération** s'affiche :



- Lancez l'Invite de commandes :

Cliquez sur **Invite de commandes** et tapez les commandes suivantes en validant par **Enter** entre chacune d'elle :

diskpart

select disk 0

list volume

Relevez la lettre attribuée au lecteur DVD :

```

Microsoft Windows [version 6.1.7600]

X:\Sources>diskpart

Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
Sur l'ordinateur : MININT-J7MEGJ0

DISKPART> select disk 0

Le disque 0 est maintenant le disque sélectionné.

DISKPART> list volume

   N° volume   Ltr   Nom                Fs           Type           Taille  Statut  Info
-----
Volume 0      E     GRMCHPFRER_        UDF          DVD-ROM       2335 M   Sain
Volume 1      C     Réservé au         NTFS         Partition     100 M   Sain
Volume 2      D                                NTFS         Partition     63 G   Sain

DISKPART>
  
```

Admettons que ce soit la lettre **E**, tapez **exit** et validez par Enter pour refermer **diskpart**

- On va d'abord vérifier que **bootsect.exe** est bien présent sur **E** :

Tapez les commandes suivantes en validant par **Enter** entre chacune d'elles :

E: (ou la lettre du lecteur DVD)\>**cd boot**

E:\>**dir**

Le contenu du dossier E:\boot est listé, assurez-vous que **bootsect.exe** est bien présent :

```

C:\> Administrateur : X:\windows\system32\cmd.exe
X:\Sources>E:
E:\>cd boot
E:\boot>dir
Le volume dans le lecteur E s'appelle GRMCHPFRER_FR_DVD
Le numéro de série du volume est CEB9-E41F

Répertoire de E:\boot

14/07/2009  12:05    <REP>          .
14/07/2009  12:05    <REP>          ..
14/07/2009  12:05                262 144 bcd
14/07/2009  12:05                3 170 304 boot.sdi
14/07/2009  12:05                1  24 bootfix.bin
14/07/2009  12:05               97 280 bootsect.exe
14/07/2009  12:05                4 096 etfsboot.com
14/07/2009  12:05    <REP>          fonts
14/07/2009  12:05    <REP>          fr-fr
14/07/2009  12:05           485 440 mentest.exe
                6 fichier(s)          4 021 752 octets
                4 Rép(s)             0 octets libres

E:\boot>
  
```

- Pour restaurer le MBR, tapez cette commande et validez par **Enter** :

E:\>**bootsect /nt60 SYS /mbr**

Un message de réussite doit apparaître :

```

C:\> Administrateur : X:\windows\system32\cmd.exe
E:\boot>bootsect /nt60 SYS /mbr
Target volumes will be updated with BOOTMGR compatible bootcode.
C: <\\?\Volume{64213cc7-eb38-11df-9cd8-806e6f6e6963}>
    Successfully updated NTFS filesystem bootcode.
\Device\Harddisk0\DR0
    Successfully updated disk bootcode.
Bootcode was successfully updated on all targeted volumes.
E:\boot>
  
```

- Tapez **exit** et validez par **Enter** pour refermer l'**invite de commandes**. Puis retentez un démarrage du PC en mode normal en cliquant sur **Redémarrer**.

2.3. Sous Linux:

Sous un système GNU/Linux, on sauve le MBR du disque à l'aide de la commande dd :

dd if=source of=destination count=nombre_de_blocs bs=taille_de_bloc

Explications :

- if = input file : fichier source qui sera copié
- of = output file : fichier de destination où sera copié la source
- count = nombre de blocs à copier
- bs = taille en octets de chaque bloc devant être copié

Un exemple tel que « `dd if=toto of=titi count=5 bs=100` » va donc lire les 5 premiers blocs de 100 octets du répertoire courant et les copier dans un nouveau fichier « titi » qui sera créé dans le répertoire courant.

Et comme sous Linux tout est fichier, on va pouvoir utiliser cette commande pour le MBR.

Quelle syntaxe utiliser pour notre sauvegarde de MBR ?

- Il faut d'abord trouver le nom du disque où est installé votre OS. Pour cela utilisez la commande **fdisk -l**

```
# fdisk -l
Disk /dev/sda: 320.1 GB, 320072933376 bytes
255 heads, 63 sectors/track, 38913 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x24e124e0
Device Boot          Start      End          Blocks      Id  System
/dev/sda1  *           1        6079         48827392    83  Linux
/dev/sda2                6079     15076         72265728    83  Linux
/dev/sda3            15076     15298          1786880    82  Linux swap / Solaris
/dev/sda5            15299     38914         189687808    7  HPFS/NTFS
```

Dans cet exemple c'est "sda1".

- Ensuite utilisez la commande **dd** pour sauvegarder le mbr dans un fichier qu'on va nommer "boot.mbr":

```
# dd if=/dev/sda1 of=boot.mbr bs=512 count=1
```

- Si tous se passe bien, vous devriez voir ce message:

```
1+0 enregistrements lus
1+0 enregistrements écrits
512 octets (512 B) copiés, 3,3479e-05 s, 15,3 MB/s
```

- Pour restaurer ce même fichier:

```
# dd if=boot.mbr of=/dev/sda1 bs=512 count=1
```

- Si tous se passe bien, vous devriez voir ce message:

```
1+0 enregistrements lus
1+0 enregistrements écrits
512 octets (512 B) copiés, 0,000759254 s, 674 kB/s
```

On voit donc dans cet exemple que la commande de restauration est quasi identique à celle de sauvegarde : on inverse simplement IF et OF.

Attention cette commande va lire le fichier sauvegardé et l'écrire sur le MBR actuel, en conséquence l'ancien MBR sera totalement effacé : toute erreur sera sanctionnée par un disque inutilisable ! Il faut donc être certain d'utiliser le bon fichier de sauvegarde (lui donner un nom clair est souvent utile).

Le MBR contenant les infos qui permettent le boot, mais aussi la table des partitions, si entre la sauvegarde et la casse du MBR vous avez changé vos partitions, la commande précédente n'est plus utilisable : Elle redonnerait théoriquement à l'OS la possibilité de démarrer mais avec une table de partition fausse donc un disque inutilisable !

Que faire ? : Une restauration partielle :

Il suffira de ne pas réécrire sur la partie du MBR qui concerne la table de partition (c'est-à-dire les octets de 447 à 512, en effet les 446 premiers octets contiennent les infos de boot).

```
dd if= boot.mbr of=/dev/sda1 bs=446 count=1
```

2.4. Utilitaires

a) TestDisk

TestDisk est un logiciel gratuit permettant de récupérer des partitions perdues, et de refaire fonctionner un disque dur non bootable. TestDisk reconnaît de nombreux types de partitions, cela va des classiques FAT 12, FAT 16, FAT 32 et NTFS aux LVM, LVM 2, UFS ou encore UFS 2 les partitions MAC et Linux RAID sont elles aussi reconnues. Les fonctionnalités se lancent depuis une fenêtre DOS mais il reste simple, puisqu'il suffit de suivre les instructions qui s'affichent à l'écran et de valider ses choix. Une documentation en français, est là pour aider ceux qui auraient du mal à s'en sortir.

b) MBRtool

MBRtool est un outil DOS de réparation du MBR. Il peut sauvegarder, appliquer un MBR fonctionnel, réparer un MBR corrompu...

Il permet aussi de nombreuses manipulations: édition du MBR (pour Linux par exemple), écriture et manipulation des signatures, modification de la table des partitions...

c) MBRWizard

Le MBR ne doit pas tomber en panne sous peine de ne plus pouvoir utiliser son disque dur. Heureusement des solutions existent et, plutôt que de rester devant le fait accompli, le logiciel MBRWizard se charge de prévoir la catastrophe. En effet, cette application vous permet de sauvegarder préventivement les informations de votre MBR afin de les restituer aisément au moment propice, à savoir quand votre disque dur ne retrouve pas ses informations de démarrage. Il vous autorisera aussi quelques manipulations sur vos partitions voire même de créer une partition de démarrage indépendante sur laquelle est stocké un MBR sécurisé.

2.5. Le multiboot

Le "multi boot" est envisagé lorsque l'on souhaite pouvoir faire démarrer une même machine avec des OS différents. Par exemple, nous pourrions souhaiter pouvoir installer sur la même machine Windows XP et GNU/Linux, et pouvoir choisir au moment du démarrage le système à faire monter.

Comme expliqué précédemment, le BIOS se chargera de lancer la routine ou gestionnaire d'amorçage présent au niveau du MBR. Si vous désirez avoir plusieurs OS sur la même machine il est conseillé d'installer un gestionnaire d'amorçage qui permettra de choisir la partition et le système d'exploitation souhaité, sinon l'utilisation d'une disquette d'amorçage pointant sur la bonne partition sera nécessaire.

Un **chargeur d'amorçage** (ou Boot loader) est un logiciel permettant de lancer un ou plusieurs systèmes d'exploitation (multiboot), c'est-à-dire qu'il permet d'utiliser plusieurs systèmes, à des moments différents, sur la même machine.

Attention, si vous installez ou réinstallez un système Windows quel qu'il soit sur un système possédant Linux vous aurez des soucis de démarrage. En effet Windows a la mauvaise habitude d'écraser le MBR lors de son installation et de remplacer et supprimer les données du secteur d'amorçage par son propre gestionnaire d'amorçage : En résumé, le bootloader du nouveau système Windows installé va écraser celui de Linux et il vous sera donc impossible de démarrer Linux. Il est donc conseillé d'installer Windows avant les autres systèmes d'exploitation.

Dans le cas le plus simple : il y a une seule partition du disque de boot : le BIOS lit les 512 premiers octets de ce disque pour charger le MBR. À partir des informations du MBR, il détermine l'emplacement de la routine d'amorçage.

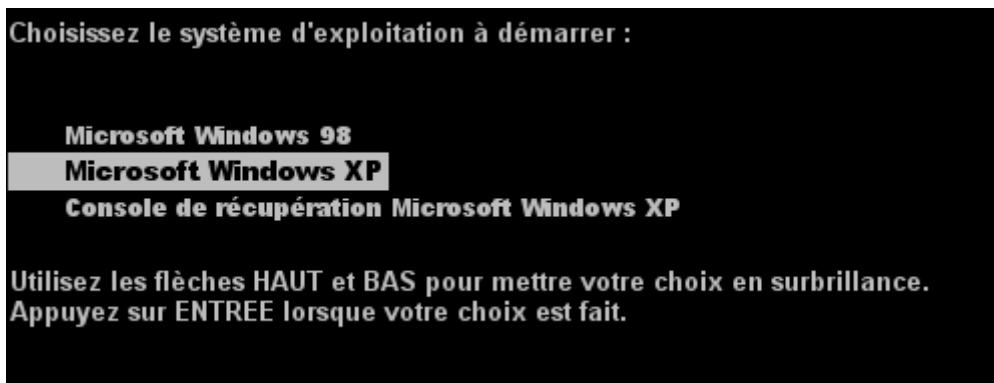
Si le disque de boot a plusieurs partitions, le BIOS lit le MBR du disque, puis il lit le VBR de la partition (Volume Boot Record, chaque partition possède le sien). À partir de ces informations, il peut déterminer l'emplacement du chargeur d'amorçage et le lancer.

Le choix du BootLoader dépend de votre configuration (OS installés) et surtout de vos goûts personnels. Parmi les plus connus et utilisés se trouvent NTLDR, winload.exe, EasyBCD, LILO, GRUB et GAG.

a) NTLDR (NT LoadER)

Il permet de gérer seulement les OS Windows NT antérieurs à XP (XP compris) et est installé par défaut sur tous ces OS.

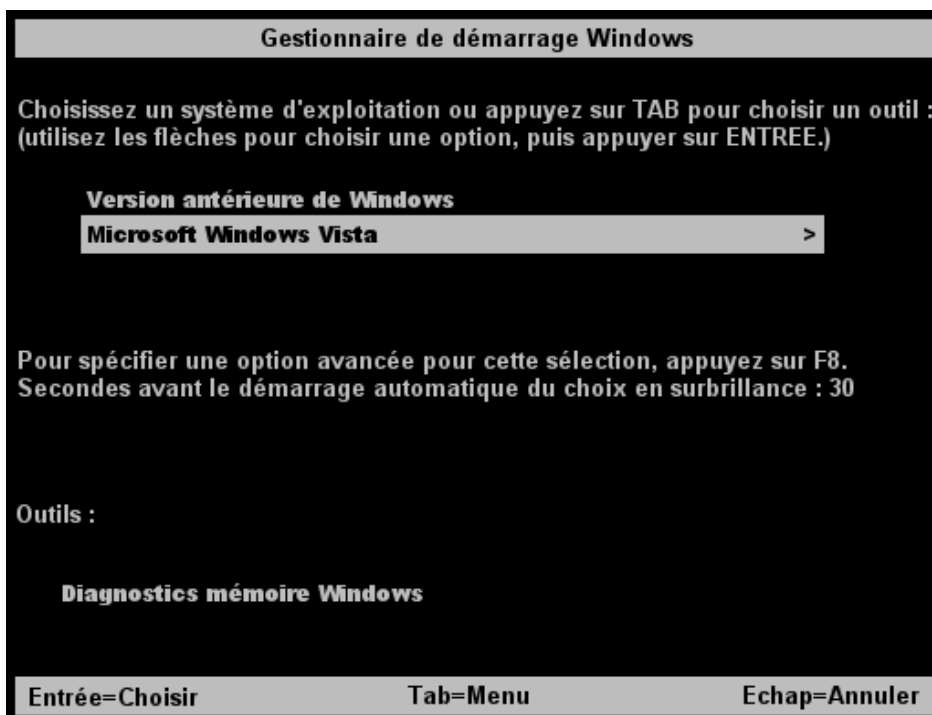
Il a pour fichier de configuration **BOOT.INI** qui se trouve à la racine de la partition système (le plus souvent C:\).



b) winload.exe

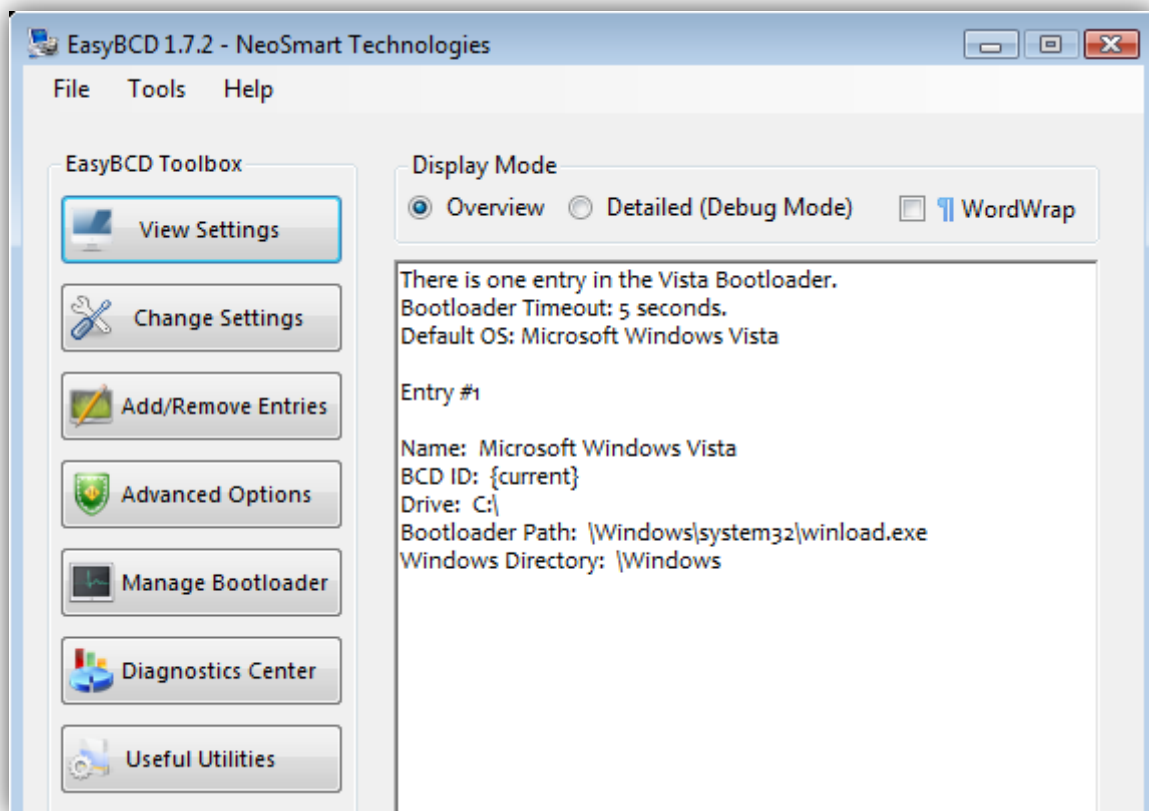
Il permet de gérer seulement les OS Windows NT antérieurs à Vista (Vista compris) et est installé par défaut sur tous ces OS.

Il a pour fichier de configuration **BCD** qui se trouve dans le répertoire caché **\Boot** de la partition système.

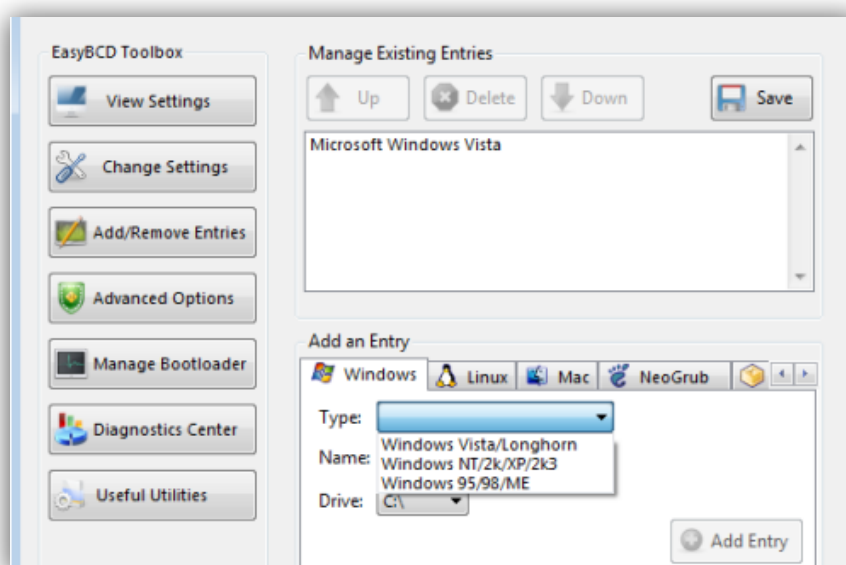


c) EasyBCD

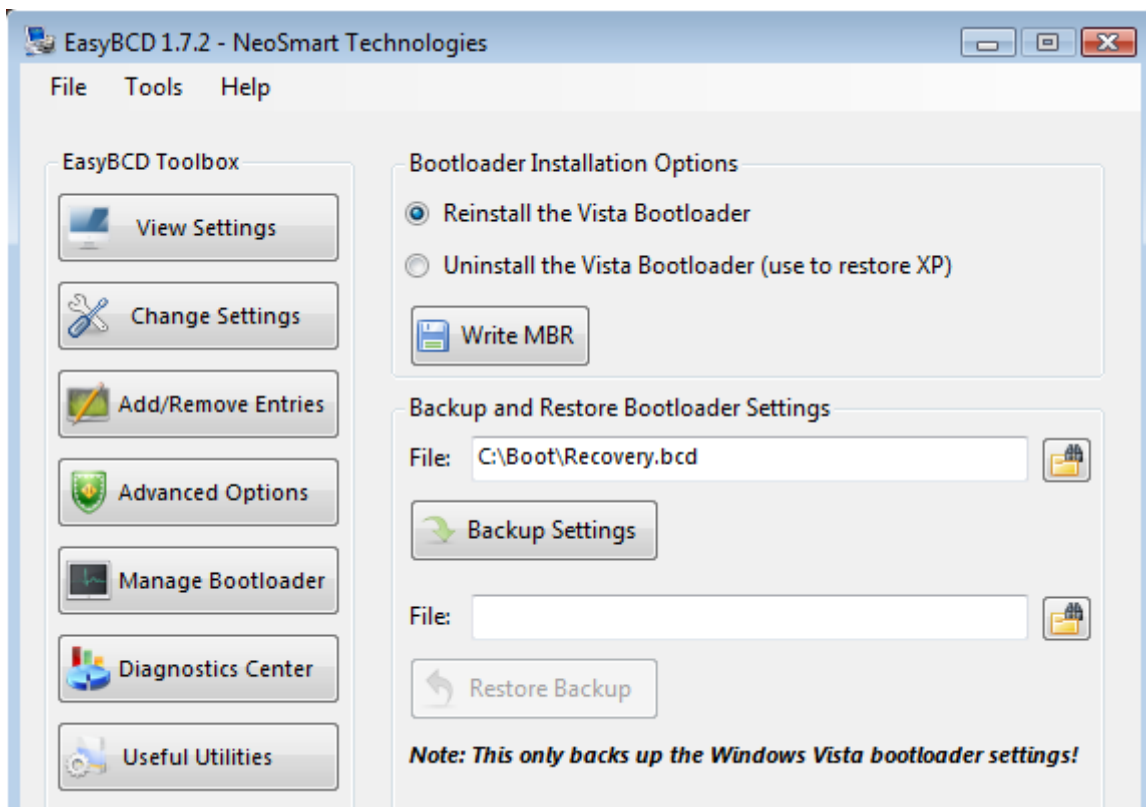
Il s'agit plus d'un outil que d'un BootLoader. Il permet de gérer les systèmes Windows, Linux et Mac OS X et s'installe depuis Windows Vista. Il facilite grandement l'utilisation de *winload.exe*, qui est difficilement configurable sans cet outil.



Ajout et suppression d'entrées dans le menu du choix de l'OS : L'interface est très intuitive, il vous suffit de choisir le type de système à ajouter (Windows, Linux, Mac, NeoGrub et WinPE), puis dans certains cas, de lui donner un nom explicite.



Changer le Bootloader : Vous pouvez choisir votre Bootloader : **NTLDR** (Bootloader de Windows XP) ou **winload.exe** (Bootloader de Windows Vista). Si vous possédez Windows Vista, un seul choix s'offre à vous : **winload.exe**.

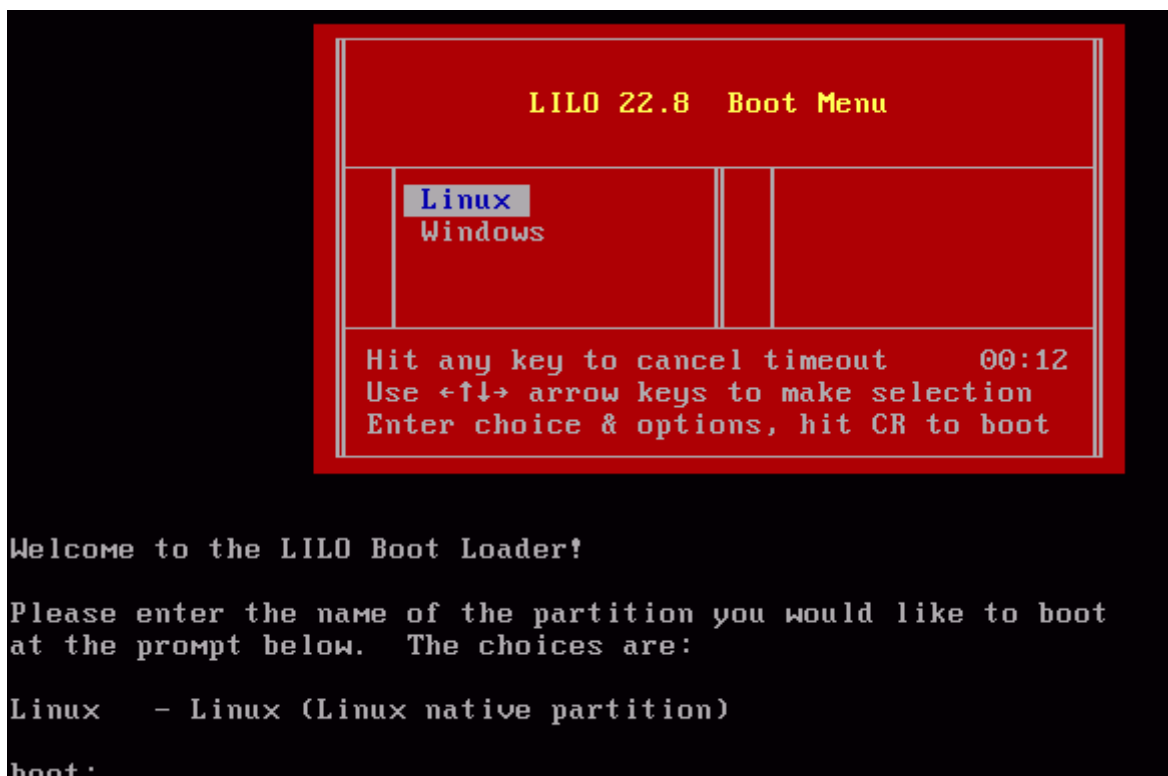


Vous pouvez choisir l'OS qui sera démarré par défaut, ainsi que le temps en secondes avant qu'il soit lancé automatiquement.

d) LILO (Linux LOader)

Il permet de gérer les systèmes Windows et UNIX et est installé par défaut sur certains systèmes Linux.

Il a pour fichier de configuration `/etc/lilo.conf`. Après toute modification, il est nécessaire de réinstaller LILO dans le secteur de boot en tapant **lilo** dans un shell.



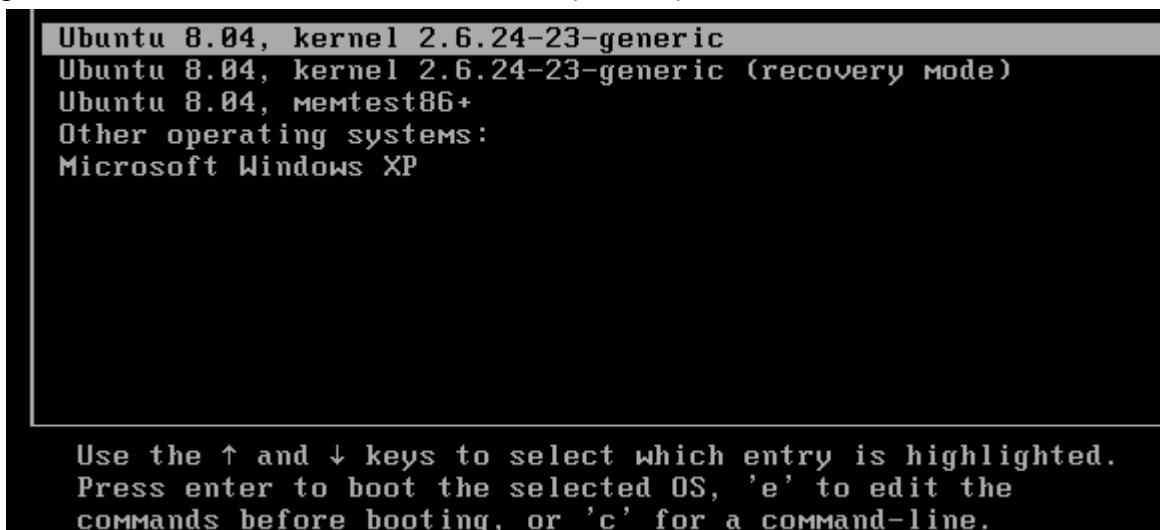
e) GRUB (GRand Unified Bootloader)

Il permet de gérer les systèmes Windows et UNIX (plus que LILO) et est installé par défaut sur certains systèmes UNIX. Il a pour fichier de configuration **/boot/grub/menu.lst**

Contrairement à LILO, GRUB n'a pas besoin d'être réinstallé dans le secteur de boot pour mettre à jour sa configuration, il prend en compte les modifications de son fichier de configuration automatiquement.

Dans le cas où le fichier de configuration serait incorrect, GRUB peut fournir un interpréteur de commandes pour permettre à l'utilisateur de charger un système d'exploitation manuellement.

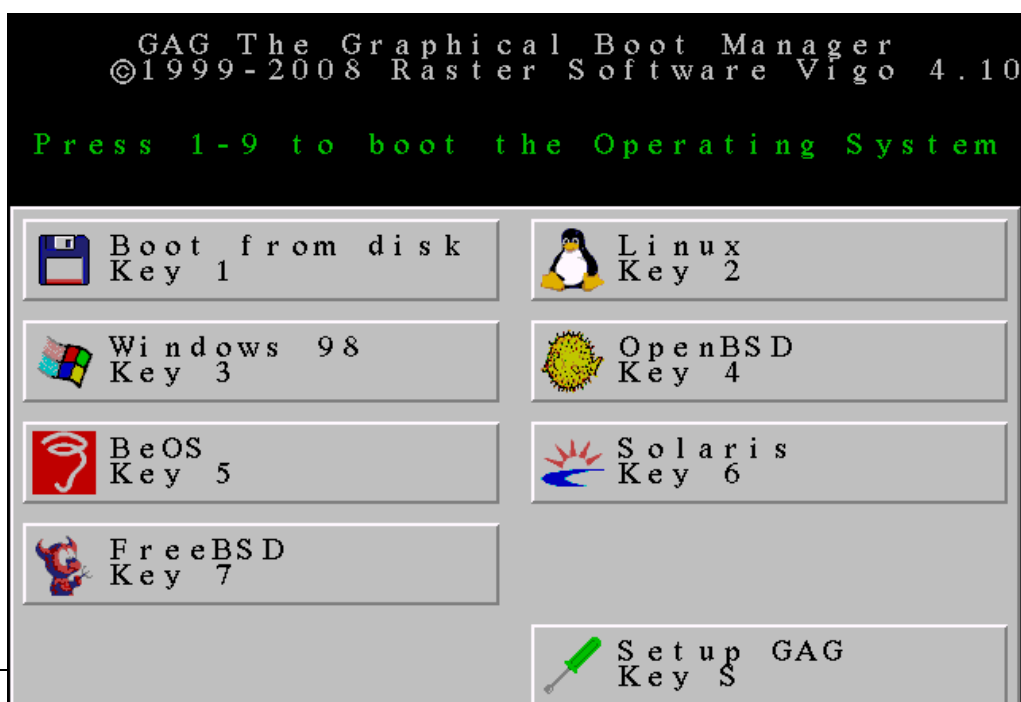
GRUB peut être utilisé avec différentes interfaces : certaines distributions de Linux utilisent l'interface graphique pour afficher au démarrage de l'ordinateur un menu avec une image de fond, et l'utilisation de la souris est parfois possible.



f) GAG (Gestor de Arranque Grafico)

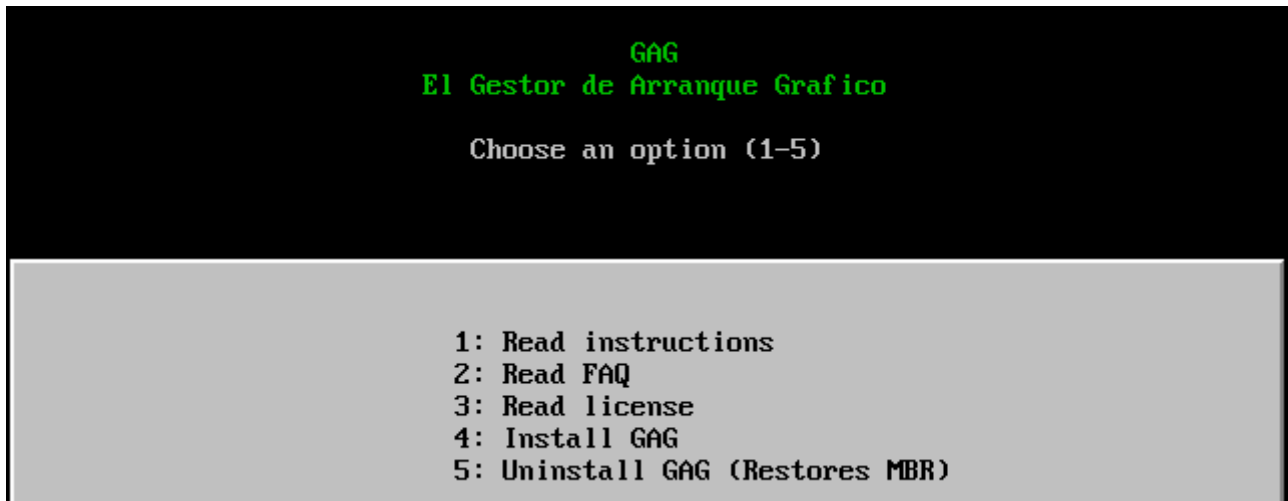
Il permet de gérer les systèmes Windows et UNIX.

Interface graphique originale, configuration protégée par mot de passe, GAG s'installe directement dans le MBR, par conséquent, contrairement à la plupart des BootLoader, le formatage ou la réinstallation d'un OS ne nécessite pas la réinstallation de GAG. Il permet ainsi d'éviter tous les problèmes rencontrés lors d'un Multiboot, ce qui le différencie de



beaucoup des autres BootLoader.

Installation via un CD bootable : Cette installation nécessite la gravure de l'image **cdrom.iso** présente dans l'archive téléchargée. Une fois la gravure terminée, laissez le CD dans le lecteur et redémarrez. Si votre BIOS est configuré de façon à booter en premier sur le lecteur CD, le menu d'installation de GAG s'affiche :



Le second menu qui s'affiche vous propose de choisir le type de clavier. La dernière étape vous demande de choisir votre langue. L'installation terminée, il ne vous reste plus qu'à configurer GAG.

Chapitre 7. La protection de votre ordinateur

Il existe différents types de menaces pouvant endommager votre PC. Les moyens de protection dépendent du type d'attaque. On utilise souvent et abusivement le mot virus pour désigner toute forme de programme malveillant (malware). Les virus informatiques ne constituent qu'une des nombreuses attaques dont peuvent être victimes les systèmes informatiques. Il est donc important de les distinguer du cheval de Troie, du ver ou de la bombe logique, par exemple le virus ne doit pas être confondu avec les vers qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans avoir besoin de contaminer de programme hôte.

1) Virus

Un **virus** est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé. La définition d'un virus pourrait être la suivante :

« Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire. »

Le véritable nom donné au virus est CPA soit *Code Auto-Propageable*, mais par analogie avec le domaine médical, le nom de "virus" est communément utilisé. En effet, il se reproduit, investi les clés USB, les systèmes informatiques et/ou les réseaux. Comme tout virus qui se respecte, il n'est pas seulement constitué d'une codification autoreproductrice, mais il contient également une « charge » qui, dans la plupart des cas, est malveillante et ses effets peuvent être dévastateurs. Le virus comporte généralement les fonctions suivantes:

- Il modifie des logiciels extérieurs par inclusion de ses propres structures.
- Les modifications qu'il apporte ne se limitent pas à 1 seul logiciel, mais touchent au moins un groupe de logiciels
- Il sait reconnaître si un logiciel a déjà été infecté.
- S'il reconnaît un logiciel déjà modifié il s'interdit de procéder à une nouvelle modification.
- Le logiciel infecté présente désormais les propriétés 1. à 4.

Les **virus résidents** (appelés **TSR** en anglais pour *Terminate and stay resident*) se chargent dans la mémoire vive de l'ordinateur afin d'infecter les fichiers exécutables lancés par l'utilisateur. Les **virus non résidents** infectent les programmes présents sur le disque dur dès leur exécution.

Ils ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection :

- Le virus classique : C'est un morceau de programme qui s'intègre dans un programme normal. Dès que l'utilisateur exécute ce programme « infecté », il active le virus qui en profite pour aller s'intégrer dans d'autres programmes exécutables. Le résultat peut être d'envoyer un simple message anodin, mais peut aller jusqu'à destruction complète de toutes les données de l'ordinateur.
- Le virus de boot : Il s'installe dans un des secteurs de boot du disque de démarrage. Il remplace un chargeur d'amorçage existant mais ne modifie pas un programme comme un virus normal.

Le virus de type Batch : C'est un virus "primitif" apparu à l'époque du MS-DOS. Ils sont lents et ont un pouvoir infectant très faible. Certains programmeurs ont été jusqu'à créer des virus Batch cryptés et polymorphes. Ce qui relève d'une vraie prouesse technique tant le langage Batch est simple et primitif.

2) Types de virus

2.1. Les virus mutants

En réalité, la plupart des virus sont des clones, ou plus exactement des «**virus mutants**», c'est-à-dire des virus ayant été réécrits par d'autres utilisateurs afin d'en modifier leur comportement ou leur signature.

Le fait qu'il existe plusieurs versions (on parle de **variantes**) d'un même virus le rend d'autant plus difficile à repérer dans la mesure où les éditeurs d'antivirus doivent ajouter ces nouvelles signatures à leurs bases de données.

2.2. Les virus polymorphes

Dans la mesure où les antivirus détectent notamment les virus grâce à leur signature (la succession de bits qui les identifie), certains créateurs de virus ont pensé à leur donner la possibilité de modifier automatiquement leur apparence, tel un caméléon, en dotant les virus de fonction de chiffrement et de déchiffrement de leur signature, de façon à ce que seuls ces virus soient capables de reconnaître leur propre signature. Ce type de virus est appelé «**virus polymorphe**» (mot provenant du grec signifiant «*qui peut prendre plusieurs formes*»).

2.3. Les rétrovirus

On appelle «**rétrovirus**» ou «virus flibustier» (en anglais *bounty hunter*) un virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants.

2.4. Les virus de secteur d'amorçage

On appelle «**virus de secteur d'amorçage**» (ou *virus de boot*), un virus capable d'infecter le secteur de démarrage d'un disque dur (*MBR*, soit *master boot record*), c'est-à-dire un secteur du disque copié dans la mémoire au démarrage de l'ordinateur, puis exécuté afin d'amorcer le démarrage du système d'exploitation.

2.5. Les virus trans-applicatifs (virus macros)

Avec la multiplication des programmes utilisant des macros, Microsoft a mis au point un langage de script commun pouvant être inséré dans la plupart des documents pouvant contenir des macros, il s'agit de VBScript, un sous-ensemble de Visual Basic. Ces virus arrivent actuellement à infecter les macros des documents Microsoft Office, c'est-à-dire qu'un tel virus peut être situé à l'intérieur d'un banal document Word ou Excel, et exécuter une portion de code à l'ouverture de celui-ci lui permettant d'une part de se propager dans les fichiers, mais aussi d'accéder au système d'exploitation (généralement Windows).

Or, de plus en plus d'applications supportent Visual Basic, ces virus peuvent donc être imaginables sur de nombreuses autres applications supportant le VBScript. Le début du troisième millénaire a été marqué par l'apparition à grande fréquence de scripts Visual Basic diffusés par mail en fichier attaché (repérables grâce à leur extension *.VBS*) avec un titre de mail poussant à ouvrir le cadeau empoisonné.

Celui-ci a la possibilité, lorsqu'il est ouvert sur un client de messagerie Microsoft, d'accéder à l'ensemble du carnet d'adresse et de s'auto diffuser par le réseau. Ce type de virus est appelé **ver** (ou worm en anglais).

3) Les vers

Les vers (en anglais *worm*) sont des programmes informatiques qui, au même titre que les virus, possèdent une fonction de réplication. La différence essentielle entre un ver et un virus réside dans le fait que les vers n'ont pas besoin de programme hôte pour se reproduire et se propager. Il se déplace en mémoire vive, un ver est donc **un virus réseau**.

3.1. Le fonctionnement d'un ver dans les années 80

La plus célèbre anecdote à propos des vers date de 1988. Un étudiant (Robert T. Morris, de Cornell University) avait fabriqué un programme capable de se propager sur un réseau, il le lança et, 8 heures après l'avoir lâché, celui-ci avait déjà infecté plusieurs milliers d'ordinateurs. C'est ainsi que de nombreux ordinateurs sont tombés en panne en quelques heures car le « ver » (car c'est bien d'un ver dont il s'agissait) se reproduisait trop vite pour qu'il puisse être effacé sur le réseau. De plus, tous ces vers ont créé une saturation au niveau de la bande passante, ce qui a obligé la NSA à arrêter les connexions pendant une journée.

Voici la manière dont le ver de Morris se propageait sur le réseau :

- Le ver s'introduisait sur une machine de type UNIX
- il dressait une liste des machines connectées à celle-ci
- il forçait les mots de passe à partir d'une liste de mots
- il se faisait passer pour un utilisateur auprès des autres machines
- il créait un petit programme sur la machine pour pouvoir se reproduire
- il se dissimulait sur la machine infectée et ainsi de suite

3.2. Les vers actuels

Les vers actuels se propagent principalement grâce à la messagerie (et notamment par le client de messagerie *Outlook*) grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-mêmes à tous ces destinataires.

Ces vers sont la plupart du temps des scripts (généralement VBScript) ou des fichiers exécutables envoyés en pièce jointe et se déclenchant lorsque l'utilisateur destinataire clique sur le fichier attaché.

3.3. Comment se protéger des vers ?

Il est simple de se protéger d'une infection par ver. La meilleure méthode consiste à ne pas ouvrir "à l'aveugle" les fichiers qui vous sont envoyés en fichier attachés.

Ainsi, tous les fichiers exécutables ou interprétables par le système d'exploitation peuvent potentiellement infecter votre ordinateur. Les fichiers comportant notamment les extensions suivantes sont potentiellement susceptibles d'être infectés : *exe, com, bat, pif, vbs, scr, doc, xls, msi, eml*

Sous Windows, il est conseillé de désactiver la fonction "masquer les extensions", car cette fonction peut tromper l'utilisateur sur la véritable extension d'un fichier. Ainsi un fichier dont l'extension est *.jpg.vbs* apparaîtra comme un fichier d'extension *.jpg* !

Les fichiers comportant les extensions suivantes ne sont pas interprétés par le système et possèdent donc un risque d'infection minime : *txt, jpg, gif, bmp, avi, mpg, asf, dat, mp3, wav, mid, ram, rm*

Tous les fichiers peuvent contenir un morceau de code informatique véhiculant un virus; mais le système devra préalablement avoir été modifié par un autre virus pour être capable d'interpréter le code contenu dans ces fichiers ! Il est donc nécessaire d'installer un antivirus et de scanner systématiquement les fichiers attachés avant de les ouvrir.

4) Le cheval de Troie

Il permet de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle).

On appelle « **Cheval de Troie** » (en anglais *trojan horse*) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur. C'est un programme

entièrement conçu pour provoquer des dommages, mais en empruntant le nom et l'apparence d'un programme ayant une autre fonction.

Un cheval de Troie donne généralement accès à l'ordinateur sur lequel il est exécuté en ouvrant une **porte dérobée** (en anglais *backdoor*). En effet en ouvrant des ports de la machine il permet à son concepteur de s'introduire sur votre machine par le réseau.

Les backdoors : ce terme peut être traduit par « porte dérobée ». C'est un moyen pour contourner la manière normale d'entrer dans un programme.

Divers virus, vers ou chevaux de Troie peuvent installer des backdoors sur un ordinateur, ce qui permet à un pirate de prendre le contrôle de la machine, en général avec des privilèges d'administrateur. A partir de là il est possible de faire n'importe quoi : pirater le contenu de l'ordinateur, récupérer le mot de passe vers un compte bancaire, et surtout se servir de cet ordinateur pour lancer, de façon masquée, une attaque vers d'autres ordinateurs bien plus intéressants du point de vue du pirate.

Chevaux de Troie et backdoors sont souvent introduits subrepticement par des vers ou la visite de pages Web piégées.

Mais ce n'est pas nécessairement un virus, dans la mesure où son but n'est pas de se reproduire pour infecter d'autres machines. Par contre certains virus peuvent également être des chevaux de Troie, c'est-à-dire se propager comme un virus et ouvrir un port sur les machines infectées ! Détecter un tel programme est difficile car il faut arriver à détecter si l'action du programme (le cheval de Troie) est voulue ou non par l'utilisateur.

4.1. Les symptômes d'une infection

Une infection par un cheval de Troie fait généralement suite à l'ouverture d'un fichier contaminé contenant le troyen et se traduit par les symptômes suivants :

- activité anormale du modem, de la carte réseau ou du disque: des données sont chargées en l'absence d'activité de la part de l'utilisateur ;
- des réactions curieuses de la souris ;
- des ouvertures impromptues de programmes ;
- des plantages à répétition ;

4.2. Principe du cheval de Troie

Le principe des chevaux de Troie étant généralement (et de plus en plus) d'ouvrir un port de votre machine pour permettre à un pirate d'en prendre le contrôle (par exemple voler des données personnelles stockées sur le disque), le but du pirate est dans un premier temps d'infecter votre machine en vous faisant ouvrir un fichier infecté contenant le troyen et dans un second temps d'accéder à votre machine par le port qu'il a ouvert.

Toutefois pour pouvoir s'infiltrer sur votre machine, le pirate doit généralement en connaître l'adresse IP. Ainsi :

- soit vous avez une adresse IP fixe (cas d'une entreprise ou bien parfois de particuliers connecté par câble) auquel cas l'adresse IP peut être facilement récupérée
- soit votre adresse IP est dynamique (affectée à chaque connexion), c'est le cas pour les connexions par modem ; auquel cas le pirate doit scanner des adresses IP au hasard afin de déceler les adresses IP correspondant à des machines infectées.

4.3. Se protéger contre les troyens

Pour se protéger il suffit d'installer un firewall, c'est-à-dire un programme filtrant les communications entrantes et sortantes de votre machine. Un firewall (*pare-feu*) permet ainsi d'une part de voir les communications sortantes de votre machine (donc



normalement initiées par des programmes que vous utilisez) ou bien les communications entrantes. Toutefois, il n'est pas exclu que le firewall détecte des connexions provenant de l'extérieur sans pour autant que vous ne soyez la victime choisie d'un hacker. En effet, il peut s'agir de tests effectués par votre fournisseur d'accès ou bien un hacker scannant au hasard une plage d'adresses IP.

Exemple de firewall gratuit : [ZoneAlarm](#)

4.4. En cas d'infection

Si un programme dont l'origine vous est inconnue essaye d'ouvrir une connexion, le firewall vous demandera une confirmation pour initier la connexion. Il est essentiel de ne pas autoriser la connexion aux programmes que vous ne connaissez pas, car il peut très bien s'agir d'un cheval de Troie. En cas de récurrence, il peut être utile de vérifier que votre ordinateur n'est pas infecté par un troyen en utilisant un programme permettant de les détecter et de les éliminer (appelé *bouffe-troyen*). C'est le cas de *The Cleaner*.

5) La bombe logique

Une bombe logique est un programme qui provoque des dégâts lorsqu'il est déclenché par une condition quelconque : heure donnée, présence ou non d'une donnée, ce qui rend sa détection difficile.

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise !

Par exemple la bombe logique Tchernobyl s'est activée le 26 avril 1999, jour du 13ème anniversaire de la catastrophe nucléaire

6) Hoax

Depuis quelques années un autre phénomène est apparu, il s'agit des canulars (en anglais *hoax*), c'est-à-dire des annonces reçues par mail (par exemple l'annonce de l'apparition d'un nouveau virus destructeur ou bien la possibilité de gagner un téléphone portable gratuitement) accompagnées d'une note précisant de faire suivre la nouvelle à tous ses proches. Ce procédé a pour but l'engorgement des réseaux ainsi que la désinformation.

Ainsi, de plus en plus de personnes font suivre (anglicisé en *forwardent*) des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus.

Les conséquences de ces canulars sont multiples :

- L'**engorgement des réseaux** en provoquant une masse de données superflues circulant dans les infrastructures réseaux ;
- Une **désinformation**, c'est-à-dire faire admettre à de nombreuses personnes de faux concepts ou véhiculer de fausses rumeurs (on parle de *légendes urbaines*) ;
- L'**engorgement des boîtes aux lettres électroniques** déjà chargées ;
- La **perte de temps**, tant pour ceux qui lisent l'information, que pour ceux qui la relayent ;
- La **dégradation de l'image** d'une personne ou bien d'une entreprise ;
- L'**incrédulité** : à force de recevoir de fausses alertes les usagers du réseau risquent de ne plus croire aux vraies.

Ainsi, il est essentiel de suivre certains principes avant de faire circuler une information sur Internet.

6.1. Comment lutter contre la désinformation ?

Afin de lutter efficacement contre la propagation de fausses informations par courrier électronique, il suffit de retenir un seul concept :

Toute information reçue par courriel non accompagnée d'un lien hypertexte vers un site précisant sa véracité doit être considérée comme non valable !

Ainsi tout courrier contenant une information non accompagnée d'un pointeur vers un site d'information ne doit pas être transmis à d'autres personnes. Lorsque vous transmettez une information à des destinataires, cherchez un site prouvant votre propos.

6.2. Comment vérifier s'il s'agit d'un canular ?

Lorsque vous recevez un courriel insistant sur le fait qu'il est essentiel de propager l'information (et ne contenant pas de lien prouvant son intégrité), vous pouvez vérifier sur le site [hoaxbuster](#) (site en français) s'il s'agit effectivement d'un hoax (canular). Si l'information que vous avez reçue ne s'y trouve pas, recherchez l'information sur les principaux sites d'actualités ou bien par l'intermédiaire d'un [moteur de recherche](#).

7) Les espioniciels

Un **espioniciel** (en anglais **spyware**) est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on l'appelle donc parfois *mouchard*) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (on parle de *profilage*).

Les récoltes d'informations peuvent ainsi être :

- la traçabilité des URL des sites visités,
- le traquage des mots-clés saisis dans les moteurs de recherche,
- l'analyse des achats réalisés via internet,
- voire les informations de paiement bancaire (numéro de carte bleue / VISA)
- ou bien des informations personnelles.

Les spywares s'installent généralement en même temps que d'autres logiciels (la plupart du temps des freewares ou sharewares). En effet, cela permet aux auteurs des dits logiciels de rentabiliser leur programme, par de la vente d'informations statistiques, et ainsi permettre de distribuer leur logiciel gratuitement. Il s'agit donc d'un modèle économique dans lequel la gratuité est obtenue contre la cession de données à caractère personnel.

Les spywares ne sont pas forcément illégaux car la licence d'utilisation du logiciel qu'ils accompagnent précise que ce programme tiers va être installé ! En revanche étant donné que la longue licence d'utilisation est rarement lue en entier par les utilisateurs, ceux-ci savent très rarement qu'un tel logiciel effectue ce profilage dans leur dos.

Par ailleurs, outre le préjudice causé par la divulgation d'informations à caractère personnel, les spywares peuvent également être une source de nuisances diverses :

- consommation de mémoire vive,
- utilisation d'espace disque,
- mobilisation des ressources du processeur,
- plantages d'autres applications,
- gêne ergonomique (par exemple l'ouverture d'écrans publicitaires ciblés en fonction des données collectées).

7.1. Les types de spywares

On distingue généralement deux types de spywares :

- Les **spywares internes** (ou *spywares intégrés*) comportant directement des lignes de codes dédiées aux fonctions de collecte de données.
- Les **spywares externes** (non intégrés) qui sont des programmes de collectes autonomes installés.

7.2. Se protéger

La principale difficulté avec les spywares est de les détecter. La meilleure façon de se protéger est encore de ne pas installer de logiciels dont on n'est pas sûr à 100% de la provenance et de la fiabilité (notamment les freewares, les sharewares et plus particulièrement les logiciels d'échange de fichiers en peer-to-peer). Voici quelques exemples de logiciels connus pour embarquer un ou plusieurs spywares : Babylon Translator, GetRight, Go!Zilla, Download Accelerator, Cute FTP, PKZip. Qui plus est, la désinstallation de ce type de logiciels ne supprime que rarement les spywares qui l'accompagnent. Pire, elle peut entraîner des dysfonctionnements sur d'autres applications !

Dans la pratique il est quasiment impossible de ne pas installer de logiciels. Ainsi la présence de processus d'arrière plans suspects, de fichiers étranges ou d'entrées inquiétantes dans la base de registre peuvent parfois trahir la présence de spywares dans le système.

Si vous ne parcourez pas la base de registre à la loupe tous les jours rassurez-vous, il existe des logiciels, nommés **anti-spywares** permettant de détecter et de supprimer les fichiers, processus et entrées de la base de registre créés par des spywares.

De plus l'installation d'un pare-feu personnel peut permettre d'une part de détecter la présence d'espioniciels, d'autre part de les empêcher d'accéder à Internet (donc de transmettre les informations collectées).

7.3. Quelques anti-spywares

Parmi les anti-spywares les plus connus citons notamment : Ad-Aware de Lavasoft et Spybot Search&Destroy

8) Les keyloggers

Un **keylogger** (littéralement *enregistreur de touches*) est un dispositif chargé d'enregistrer à l'insu de l'utilisateur les frappes de touches du clavier. Il s'agit donc d'un dispositif d'espionnage.

Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur !

Dans la mesure où les keyloggers enregistrent toutes les frappes de clavier, ils peuvent servir à des personnes mal intentionnées pour récupérer les mots de passe des utilisateurs du poste de travail ! Cela signifie donc qu'il faut être particulièrement vigilant lorsque vous utilisez un ordinateur en lequel vous ne pouvez pas avoir confiance (poste en libre accès dans une entreprise, une école ou un lieu public tel qu'un cybercafé).

8.1. Keyloggers : logiciel ou matériel

Les keyloggers peuvent être soit logiciels soit matériels. Dans le premier cas il s'agit d'un processus furtif (ou bien portant un nom ressemblant fortement au nom d'un processus système), écrivant les informations captées dans un fichier caché !

Les keyloggers peuvent également être matériel : il s'agit alors d'un dispositif (câble ou dongle) intercalé entre la prise clavier de l'ordinateur et le clavier.

8.2. Se protéger des keyloggers

La meilleure façon de se protéger est la vigilance :

- N'installez pas de logiciels dont la provenance est douteuse,
- Soyez prudent lorsque vous vous connectez sur un ordinateur qui ne vous appartient pas. S'il s'agit d'un ordinateur en accès libre, examinez rapidement la configuration, avant de vous connecter à des sites demandant votre mot de passe, pour voir si des utilisateurs sont passés avant vous et s'il est possible ou non pour un utilisateur lambda d'installer un logiciel. En cas de doute ne vous connectez pas à des sites sécurisés pour lesquels un enjeu existe (banque en ligne, ...)

Si vous en avez la possibilité, inspectez l'ordinateur à l'aide d'un anti-spyware.

9) Les protections

Nous pouvons d'ores et déjà assurer qu'il n'existe pas de moyen 100% fiable contre les virus. Les virus font partie du monde informatique et de ses risques, il faut donc apprendre à vivre avec. Lorsqu'une attaque est détectée, il ne faut surtout pas céder à la panique! Il ne faut surtout pas détruire un programme ou formater son disque dur, juste parce que l'on croit être infecté. Un des moyens de protection est l'antivirus.

9.1. Antivirus

Un **antivirus** est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier. On parle ainsi d'**éradication** de virus pour désigner la procédure de nettoyage de l'ordinateur.

Il existe plusieurs méthodes d'éradication :

- La suppression du code correspondant au virus dans le fichier infecté ;
- La suppression du fichier infecté ;
- La mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement où il ne pourra pas être exécuté.

9.2. Détection des virus

Les virus se reproduisent en infectant des « *applications hôtes* », c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant. Or, afin de ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois un même fichier. Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la **signature virale**.

Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de **recherche de signature** (*scanning*), la plus ancienne méthode utilisée par les antivirus. Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indétectable : il s'agit de "**virus polymorphes**".

Certains antivirus utilisent un **contrôleur d'intégrité** pour vérifier si les fichiers ont été modifiés. Ainsi le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille et éventuellement une somme de contrôle). Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.

La **méthode heuristique** consiste à analyser le comportement des applications afin de

détecter une activité proche de celle d'un virus connu. Ce type d'antivirus peut ainsi détecter des virus même lorsque la base antivirale n'a pas été mise à jour. En contrepartie, ils sont susceptibles de déclencher de fausses alertes.

Si l'antivirus est paralysé par un virus ou ver on peut avoir recours à un antivirus en ligne, tels ceux qui sont disponibles sur les sites suivants :

[http://fr.trendmicroeurope.](http://fr.trendmicroeurope.com/consumer/products/housecall_pre.php)

[com/consumer/products/housecall_pre.php](http://fr.trendmicroeurope.com/consumer/products/housecall_pre.php)

<http://www.mcafee.com/myapps/mfs/default.asp>

http://www.pandasoftware.com/activescan/fr/activescan_principal.htm

<http://www.bitdefender.com/scan/licence.php>

<http://www.secuser.com/antivirus/index.htm>

Ces antivirus en ligne nécessitent généralement l'utilisation d'Internet Explorer

Table des matières

Chapitre 1. Introduction	2
1) Le codage de l'information numérique	2
2) Unités de mesure	3
Chapitre 2. Les composants de l'ordinateur	4
1) Les composants internes de l'ordinateur.	4
1.1. La carte mère :	4
1.2. Les mémoires	9
1.3. Le disque dur	13
2) Les périphériques informatiques	16
Chapitre 3. Le système d'exploitation	17
1) Principales tâches.....	17
2) Les systèmes d'exploitation les plus connus.....	18
2.1. Microsoft Windows.....	18
2.2. Apple.....	18
2.3. IBM.....	18
2.4. UNIX.....	18
2.5. Système d'exploitation mobile.....	19
3) Caractéristiques d'un système d'exploitation	19
3.1. Liste des systèmes les plus courants et de leurs caractéristiques.	21
4) Organisation d'un système d'exploitation	22
4.1. Les bibliothèques.....	22
4.2. L'interface homme machine	23
4.3. L'API (interface de programmation)	24
4.4. Le noyau.....	24
4.5. Les pilotes :.....	24
4.6. Le système de fichiers	25
4.7. Les applications ou logiciels	25
4.8. Les fichiers de données des applications	25
5) Gestion d'un système d'exploitation	28
5.1. Arborescence du système et des fichiers	28
5.2. Attributs des fichiers	30
5.3. Gestion des droits des utilisateurs	30
6) Le registre Windows	31
Chapitre 4. Linux : Gestion du système d'exploitation	34
1) Les distributions Linux	34

2) Caractéristiques.....	34
2.2. L'interface graphique	37
2.3. La défragmentation.....	37
2.4. A quoi ressemblent les commandes Linux ?.....	37
Chapitre 5. Installation d'un OS.....	39
1) Etapes	39
2) Le formatage du disque dur	40
2.1. Formatage de bas niveau	41
2.2. Formatage de haut niveau.....	41
3) Partitionner un disque dur.....	42
3.1. Définition et intérêt	42
3.2. Types de partition	42
3.3. Méthodes	43
4) Le système de fichiers.....	45
4.1. Introduction.....	45
4.2. Quelques définitions.....	46
5) Quel système de fichiers choisir ?	46
6) FAT et NTFS.....	47
6.1. FAT	47
6.2. NTFS (New Technology File System).....	48
6.3. Avantages NTFS/FAT.....	48
6.4. Convertir FAT32 en NTFS avec Win7	50
Chapitre 6. Le démarrage et le BIOS.....	53
1) Test POST et BIOS.....	53
1.1. Messages d'erreurs possibles au démarrage du BIOS	54
1.2. Configuration du Bios	55
2) Le MBR.....	56
2.1. Virus de boot.....	57
2.2. Sous windows.....	58
2.3. Sous Linux:.....	62
2.4. Utilitaires	64
2.5. Le multiboot	64
Chapitre 7. La protection de votre ordinateur.....	70
1) Virus.....	70
2) Types de virus.....	71
2.1. Les virus mutants.....	71

2.2.	Les virus polymorphes	71
2.3.	Les rétrovirus	71
2.4.	Les virus de secteur d'amorçage	71
2.5.	Les virus trans-applicatifs (virus macros)	71
3)	<i>Les vers</i>	71
3.1.	Le fonctionnement d'un ver dans les années 80	72
3.2.	Les vers actuels	72
3.3.	Comment se protéger des vers ?	72
4)	<i>Le cheval de Troie</i>	72
4.1.	Les symptômes d'une infection	73
4.2.	Principe du cheval de Troie	73
4.3.	Se protéger contre les troyens	73
4.4.	En cas d'infection	74
5)	<i>La bombe logique</i>	74
6)	<i>Hoax</i>	74
6.1.	Comment lutter contre la désinformation ?	75
6.2.	Comment vérifier s'il s'agit d'un canular ?	75
7)	<i>Les espioniciels</i>	75
7.1.	Les types de spywares	75
7.2.	Se protéger	76
7.3.	Quelques anti-spywares	76
8)	<i>Les keyloggers</i>	76
8.1.	Keyloggers : logiciel ou matériel	76
8.2.	Se protéger des keyloggers	77
9)	<i>Les protections</i>	77
9.1.	Antivirus	77
9.2.	Détection des virus	77