<09introduction.htm>

Initiation à l'Utilisation de l'Informatique 2009-2010
Windows, le téléchargement, la sécurité, les antivirus, le compactage, la gravure, le scannage, ...

En 2009, l'essentiel des éléments de ce chapitre seront vus à travers l'utilisation de la Framakey. Les logiciels de la Framakey possèdent des tutoriels que vous pouvez retrouver sur la Framakey, ainsi que sur notre site (rubrique "Tutoriels" du menu "Framakey"). Ces tutoriels vous seront très utiles, en support au cours oral, pour l'utilisation de la plupart des logiciels utilitaires ou autres qui seront étudiés durant les séances.

Ci-dessous figurent d'autres informations, dont toutes ne seront pas développées au cours.

Contenu de ce document

Remarque générale: On utilise systématiquement les deux langues français/anglais pour favoriser les transitions d'une version à l'autre. Les logiciels Office 2003 installés dans les salles Renaissance sont en Anglais. Les mots du jargon informatique se retrouvent en italique dans ce document.

1. Introduction à l'Informatique

1.1. Matériel et Logiciels

On travaille sur PC (*Personnal Computer*). Le PC est constitué de *l'unité centrale* et des *périphériques* d'entrée et de sortie (*l'écran*, la *souris*, le *clavier*, *l'imprimante*). En salle Renaissance, les machines sont reliées par *réseau*. *L'imprimante* est partagée par chaque machine grâce à ce *réseau*. Les *logiciels* figurant sur les machines sont installés sur chaque machine, mais les données (nos *fichiers*) sont envoyées et partagées depuis le *serveur*, installé en salle Renaissance1.

Pour accéder aux données du *serveur*, il faut lancer les machines (et éventuellement les écrans) grâce au bouton *Power* et introduire un *login* (ou *UserName*) et un *password*. Vérifiez à cet effet que la touche *Num Lock* est bien activée, sinon les chiffres du *pavé numérique* ne seront pas pris en compte. Ces informations permettent à la machine de reconnaître la configuration à utiliser pour le cours. La configuration est variable selon le cours, en fonction des *applications* utilisées, des droits et des restrictions choisies. Le cours se termine par un *logoff* (et un *Shut Down*) pour laisser place à une autre configuration pour le cours suivant. Ces contraintes sont les premières des contraintes nécessaires à l'utilisation optimale d'un réseau informatique pour étudiants. D'autres contraintes suivront comme l'impossibilité *d'écrire sur* certains *disques*, l'impossibilité de conserver les *fichiers* dans la *corbeille*, …

Deux machines différentes du réseau, démarrées à l'aide du même login, affichent donc les dossiers et fichiers du même compte. Nous vous déconseillons de travailler sur deux machines différentes sur le même fichier du même compte. Si les modifications que vous faites sur le fichier sont différentes d'une machine à l'autre, la sauvegarde risque de donner un résultat inattendu, et risque même de "planter" les machines ou de rendre le fichier illisible. Ne travaillez donc jamais avec deux machines différentes sur le même fichier !

Le *logiciel* OS (Operating System) installé sur les machines est Windows 2000 Professional. D'autres versions de Windows sont Windows 95, Windows 98, Windows Millenium (plus anciennes), Windows XP, Windows Vista (plus récentes). Il existe d'autres OS que Windows. Un très populaire actuellement est Linux.

Les *applications* principales qu'on utilise cette année sont le traitement de texte Word, le tableur Excel, le gestionnaire de bases de données Access, le logiciel de présentations PowerPoint, un explorateur d'Internet,... La *version* de ces logiciels est celle d'Office 2003 Professional (Professionnel). On côtoiera des *logiciels* de dessins, de mise en page, de messagerie, des *accessoires*, un *compacteur*, un *antivirus* … Certains logiciels se lancent automatiquement au démarrage de Windows. En particulier l'antivirus sur lequel nous reviendrons dans nos cours.

1.2. Concepts de base

Nous allons rencontrer dans ce cours les notions de *fichiers, dossiers* (section du disque dur identifiée par un nom et qui contient des fichiers; Pour ordonner les fichiers sur un disque dur, classez-les dans des dossiers et des sous-dossiers; les fichiers et dossiers sont visualisés à l'aide de l'Explorateur)*, nom* et *extension d'un fichier* (la partie terminale d'un nom de fichier; elle suit le dernier point; elle détermine le logiciel associé au fichier), *enregistrer* ou *sauver (*copier des données sur un support de stockage: disque, disquette, mini-disque Zip, bande magnétique, clé USB,...)*, copier, déplacer, ouvrir, imprimer,...* N'employez pas des termes à tort comme "*back up*" pour une simple *copie de sauvegarde* !

La structure de classement des *fichiers* et *dossiers* est appelée *arborescence*. L'arborescence sera aussi visualisée grâce à l'Explorateur dans la suite du cours. Le *desktop (bureau)* y est le "tronc commun", du moins du point de vue de l'interprétation que les concepteurs veulent lui donner. Il ne s'agit du point de vue logique que d'un dossier situé sur le disque d'installation de Windows. Les *dossiers* sont représentés par les "branches", se divisant en d'autres "branches" ou se terminant par des "feuilles" symbolisant les *fichiers*.

2. Windows

2.1. Windows et ses objets

Windows est un système de *fenêtres* (grands rectangles de travail) dimensionnables, déplaçables et superposables les unes sur les autres. Ces *fenêtres* contiennent des *applications*, des *fichiers*, ... Une seule *fenêtre* est *active* à la fois. C'est usuellement celle qui a sa *barre de titre* (son nom dans la partie supérieure) de couleur plus vive que les autres. Chacune des *fenêtres* peut être fermée, réduite en un *bouton* de la *barre de tâches*, ou représentée par une icône de raccourci sur le bureau. L'icône de raccourci est un simple dessin symbolisant *l'application*, le *fichier*, ... Toute *application*, qu'elle soit ouverte ou réduite, est rappelée par un *bouton* sur la *barre de tâches*.

Il est possible d'ouvrir plusieurs *fenêtres* en même temps (tant que le permet la *mémoire vive* de la machine), mais pas de travailler sur ces différentes *fenêtres* simultanément. L'intérêt d'ouvrir deux *fenêtres* est par exemple de voir le contenu de deux *disques* différents pour comparer ou assurer le transfert de données de l'un à l'autre.

Chaque fenêtre comporte un bouton Fermer dans son coin supérieur droit, sur lequel vous pouvez cliquer pour fermer la fenêtre et arrêter le programme. Pour réduire la fenêtre, on utilise le boutons Réduire. Le bouton Agrandir/Restaurer représente successivement une fenêtre couvrant l'écran et deux fenêtres se superposant. Le bouton Aide, parfois présent, permet d'obtenir de l'aide sur le contenu de la fenêtre, ou sur une zone particulière de celle-ci.

Fermer	Réduire	Agrandir	Restaurer
			

Le Bureau (Desktop)

Lorsque Windows est lancé, la zone qui apparaît est appelée le *bureau*. Le bureau peut-être personnalisé en y ajoutant des *icônes de raccourcis* vers les logiciels, les documents, les dossiers et fichiers, et en modifiant son aspect général via la couleur, le *papier-peint*,... Placer des raccourcis sur le bureau constitue un moyen rapide d'accéder à des éléments souvent utilisés. On crée le *raccourci* d'un fichier grâce au *clic droit*, et en choisisant la commande Créer un raccourci (Create Shortcut). On peut ensuite le déplacer sur le *bureau*. Dans les salles Renaissance, ne déposez rien sur le *bureau* !

Manipulation de la souris

Le déplacement de la *souris* sur son *tapis* permet le déplacement à l'écran d'un *pointeur* de forme variable: flèche, grand " I ", carré, double flèche, sablier, ... On distingue:

- **Clic**: appuyer une fois sur le *bouton gauche* de la *souris*. Cela permet de *sélectionner* un *fichier*, ouvrir un *menu*, choisir une *commande*, placer le *pointeur* dans le texte, ...
- **Double-clic**: appuyer deux fois rapidement sur le *bouton gauche*. Cela permet d'ouvrir un *fichier*, lancer un *logiciel* par son *icône*, ...
- **Clic droit**: appuyer une fois sur le *bouton droit* de la *souris*. Cela permet d'appeler le *menu contextuel*. Ce menu contient des *commandes* courantes que l'on applique à l'élément désigné. Par exemple, en *cliquant* sur un *fichier* avec le *bouton droit* de la *souris*, on peut choisir de *l'ouvrir*, de le *copier*, de le *supprimer*, de l'envoyer sur la disquette, ...
- **Cliquer-glisser** (ou "*draguer*"): appuyer sur le *bouton gauche* de la *souris* et ne le lâcher qu'après avoir déplacé la *souris* à l'endroit voulu. Cela permet de *sélectionner* des *fichiers*, *sélectionner* du *texte*, *déplacer* un objet, dessiner des *formes*, ...

La Corbeille (Recycle Bin)  

Windows place les fichiers supprimés dans la *Corbeille* située sur le *bureau*. On peut ainsi ouvrir la *Corbeille* pour récupérer des *fichiers supprimés* par erreur (exception faite pour des fichiers qui se trouvaient sur disquette, ou supprimés au moyen de programmes particuliers), ou la *vider* pour créer davantage *d'espace* sur le *disque*. Attention: pour des raisons de gestion des machines, il est possible que tout élément envoyé à la *corbeille* lors de nos cours soit définitivement perdu ! ! ! Evitez d'utiliser cet outil pour la réalisation de votre travail dans les salles Renaissance.

Poste de travail (My Computer)  

Le *Poste de travail* permet d'afficher rapidement et facilement une vue d'ensemble du contenu de l'ordinateur. Pour avoir une vue plus précise du contenu, on emploie un outil plus pratique; *l'Explorateur Windows*.

Bouton Démarrer et barre des tâches (Start Button & Task Bar)

Au bas de l'écran se trouve la *barre des tâches*. Elle présente le *bouton Démarrer (Start)*, employé pour lancer rapidement un programme. Il constitue aussi un moyen rapide pour accéder à *l'aide*.

Pour démarrer un logiciel, on clique sur le *bouton Démarrer (Start)*, puis on pointe sur *Programmes (Programs).* Si le *logiciel* désiré n'apparaît pas sur le *menu*, on pointe sur le *dossier* dans lequel il devrait se trouver, portant souvent le nom de l'éditeur du logiciel. Lorsque l'on ouvre un logiciel, un document ou une fenêtre, un *bouton* s'affiche sur la *barre des tâches*. Il suffit de *cliquer* sur ce bouton pour basculer rapidement entre les fenêtres qui sont ouvertes. La fenêtre active est représentée par le *bouton* enfoncé.

Attention : le *bouton Démarrer* n'a pas pour fonction d'explorer tout l'ordinateur. On ne trouvera pas dans ses *menus* le *fichier* précis que l'on cherche (ceci est le rôle de *l'Explorateur*). Le *bouton Démarrer* est un outil qui permet d'organiser facilement et logiquement les *raccourcis*.

Les différents *logiciels* utilisés cette année sont ceux d'Office 2003 Professional, *installés* en version anglaise. On les obtient en suivant successivement Démarrer/Programmes (Start/Programs) puis en pointant vers le sous-menu consacré à Microsoft Office 2003. Les *logiciels* utilisés sur un ordinateur personnel peuvent se révéler incompatibles. La meilleure compatibilité avec les logiciels des salles Renaissance est assurée pour des *fichiers* créés sur Office 2003 (version anglaise) pour Windows 2000. Un *fichier* créé sur une ancienne version d'Office pourra être *converti*, automatiquement lors de l'ouverture, pour être lisible sous Office 2003. Méfiez-vous des langues: des problèmes de compatibilités existent par exemple entre Access en version anglaise et en version française.

2.2. L'Explorateur Windows (Windows Explorer)

On lance *l'Explorateur Windows* (Windows Explorer) à partir du *bouton Démarrer* en suivant Programmes/Accessoires (Programs/Accessories). On ne s'occupe pas de l'entreposage physique des données. Il est géré par la machine. La machine copie les informations sous forme de caractères spéciaux (octets, bytes) sur des "clusters" sur support magnétique. Il est parfois nécessaire de vérifier ce type de rangement et d'y mettre un peu d'ordre (défragmentation; voir un peu plus loin dans ce document).

L'Explorateur nous propose de nous occuper de l'entreposage logique des données: Comment nommer tel *fichier* ? Dans quel *dossier* le ranger ? Dans quel *dossier* ranger ce *dossier* ? …

- **Les unités de stockage:**
  - **Disque (Disk):**

les disques sont les supports physiques sur lesquels on travaille. On y accède par un lecteur. Exemples: *disquette et lecteur de disquette*, *disque dur*, *disque de travail*, *CD-Rom*, *DVD-Rom, clé USB, appareil photo numérique, lecteur MP3, lecteur de cartes, ...*

Dans le cadre de nos cours, vous rencontrerez les disques suivants:
A - 3 1/2 Floppy - *lecteur de disquettes*
D - Compact Disc - *lecteur* et *graveur* de *CD-Rom*
F - exam128 - *disque* de l'enseignant sur lequel se trouvent les fichiers de cours
H - exam128n01 par exemple - *disque* de travail individuel, différent pour chaque *compte*.

- **Les éléments de l'Explorateur:**
  - **Fichiers (Files):**

Les entités d'informations utilisées, créées, ou celles déjà créées et placées sur la machine. Il y a toutes sortes de *fichiers*: des *programmes exécutables* (scan.exe), des *documents* de texte (lettre.doc), des *feuilles de calcul* (impôts.xls), des images (chat.jpg), et beaucoup d'autres encore! Pour identifier les *fichiers*, on leur donne un nom suivi d'un point et d'une *extension* reflétant le plus souvent le *logiciel* de création du *fichier* (revoir les exemples ci-dessus). Le *nom* et *l'extension* ne peuvent contenir de *caractères spéciaux* (\ / : ? " < > |).

- **Dossiers (Folders):** 
  Ils permettent de regrouper et classer les fichiers. Les dossiers peuvent contenir des sous-dossiers et/ou des fichiers.

- **La structure de l'Explorateur:**

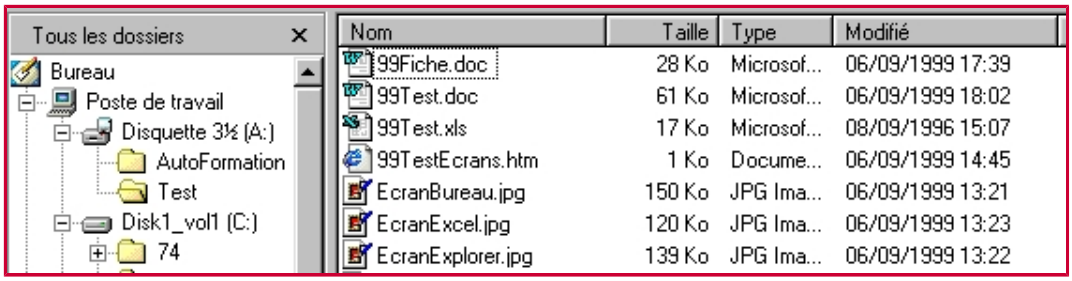
  La structure présentant les *fichiers* et *dossiers* dans *l'Explorateur* est appelée *arborescence*. Le *bureau (desktop)* y est le "tronc commun", les *dossiers* sont représentés par les "branches", se divisant en d'autres "branches" ou se terminant par des "feuilles" symbolisant les *fichiers*.

  Pour voir le contenu d'un *dossier*, *cliquer* sur son nom dans la *fenêtre* de gauche, ou *double-cliquer* dessus dans la *fenêtre* de droite. Un dossier précédé du symbole + indique qu'il contient des sous-dossiers. Un dossier précédé du signe - indique que le dossier est ouvert; ses sous-dossiers sont visibles à l'écran. Un dossier sans symbole ne contient que des fichiers, à moins qu'il soit vide.

  Les disques sont visibles dans le *Poste de Travail* (*My Computer*).

  Une grande majorité de *fichiers* peuvent être ouverts à partir de *l'Explorateur* en *double-cliquant* sur leur nom.

  Concernant les *fichiers* et *dossiers* dans la partie droite de *l'Explorateur*, il est possible de les faire apparaître sous forme de *grandes icônes*, de *petites icônes*, en *liste*, ou avec leur *détail* au moyen du *menu* Affichage (View). Le *détail* est composé, selon les options choisies à l'aide d'un clic droit dans l'en-tête des colonnes, du *nom*, de la *taille*, du *type de fichier*, et de la *date de dernière modification*.



  Un *clic* sur l'en-tête d'une colonne permet un tri sur cette colonne. On peut ainsi classer les *fichiers* par ordre alphabétique, du plus petit au plus grand, par *type* de *fichier*, par date de modification.

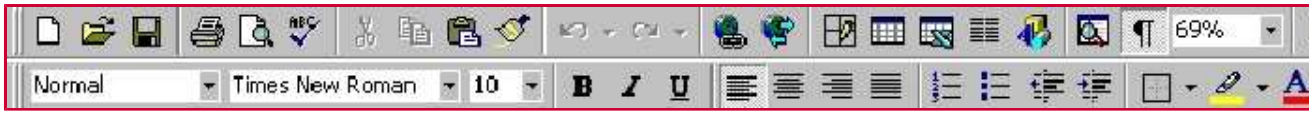
  Un fichier peut être en "*lecture seule*" ("*read-only*"). Il s'agit d'un mode de protection. Cela signifie que ce fichier peut être ouvert et copié, mais qu'il ne peut être modifié et en principe supprimé. Les fichiers que l'on copie d'un CD-Rom sur un disque dur sont souvent copiés en *lecture seule*. La suppression de cet attribut est cependant assez simple. Il faut appeler les propriétés (properties) du fichier dans le menu Fichier (File), et dans la boite qui apparaît, enlever la coche au niveau de l'attribut "*lecture seule*" ("*read only*").

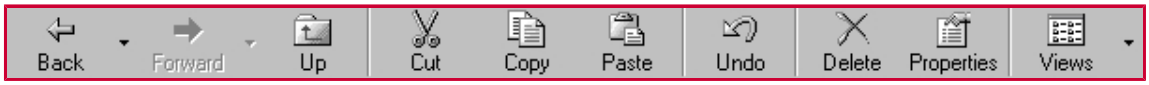
Objets de bases: barre de titre, de menu, d'outils, d'état

- **Barre de titre:**
  

  Elle affiche en général le nom de *l'application* et du document actifs dans le coin supérieur gauche de la fenêtre. Si plusieurs *fenêtres* se côtoient, la *fenêtre active* aura généralement sa *barre de titre* de couleur plus vive que les autres. Les *boutons Rétrécir, Agrandir et Fermer* figurent en haut à droite.
- **Barre de menus:**
  

  Elle affiche toutes les *commandes* du *logiciel* Windows utilisé. Une *commande* est une instruction qui indique à Windows qu'il doit exécuter une action. La plupart des *commandes* de Windows peuvent être choisies en *cliquant* dans les *barres d'outils* à l'aide de la *souris*. Les *commandes* d'un même type sont groupées dans un même *menu*. Certaines *commandes* exécutent immédiatement une action, d'autres affichent une *boîte de dialogue* pour permettre de sélectionner des options ou d'entrer des *paramètres.* Ces *commandes* sont rencontrées en Anglais ou en Français selon l'origine du *logiciel*. Une commande en gris clair est une commande non disponible (dans la plupart des cas parce que le contexte ne s'y prête pas).
  Les menus ont une cohérence conceptuelle. Par exemple, les actions qui concernent les fichiers, comme la sauvegarde, la mise en page, l'impression, ... se trouvent dans le menu Fichier (File). Ne cherchez par exemple pas à sauvegarder votre travail à l'aide du menu Affichage (View).
- **Barres d'outils:**





Les *barres d'outils* comprennent des *outils* qui permettent d'accéder rapidement à de nombreuses *commandes* du *logiciel*. Les dessins figurant sur ces *outils* symbolisent le plus fidèlement possible l'effet de la *commande*.

Visite des disques Q et H

- **h** est le *disque de travail*. Il convient de le nettoyer à chaque fin de séance. Lors des séances d'applications, ce disque H vous permet d'entreposer vos données. Ne déposez rien ni sur le bureau, ni dans les dossiers MyPictures ou MyDocuments ! ! ! Le bureau et ces dossiers sont situés sur le disque C, et un entreposage sur ce disque signifie un ralentissement de la machine, un ralentissement du lancement de votre profil, et le cas échéant l'impossibilité de lancer votre compte et de récupérer vos données.
- **q** est le *disque* des enseignants, réservé (pour les étudiants) à la *lecture* et à la "pêche" de fichiers.

Copies et déplacements

Les items qui suivent constituent les premières manipulations de *copie* et de *déplacement* de *fichiers* ou de *dossiers* effectuées au cours:

1ère méthode (les menus):

- Si ce n'est pas encore fait, faites appel à *l'Explorateur* à partir du *bouton Démarrer/Programmes/Accessoires (Start/Programs/Accessories).* Vérifiez que sa *barre d'outils* soit présente, sinon, faites-la apparaître au moyen du *menu* Affichage (View).
  Apparition du contenu du *disque* désiré en *cliquant* sur le *disque* adéquat (disque a, h ou q).
- Sur le *disque* h, nettoyez éventuellement des anciens *fichiers* au moyen de la *commande* Fichier/Supprimer (File/Delete) ou par la méthode du *dragage* vers la *Corbeille*. Rappel: Sur toute autre machine, il est possible de récupérer des *fichiers* envoyés à la *corbeille*. Pour des raison de gestion, cette option n'est pas disponible en salle Renaissance; tout *fichier* envoyé à la *corbeille* est définitivement perdu!
  Il existe sur le clavier une touche Supprimer (Delete) évitant de passer par les *menus*.
- *Copiez* sur h le *dossier* de cours Windows *sélectionné* sur le *disque* f au moyen des *commandes* Edition/Copier (Edit/Copy) et Edition/Coller (Edit/Paste).
- Sur le disque a (Il faut insérer une *disquette vierge* dans le *lecteur.* Attention au sens de la disquette !!! Etiquette vers le haut ou vers la droite, selon l'orientation du lecteur !), créez un *dossier* personnalisé au moyen du *menu* Fichier/Nouveau/Dossier (File/New/Folder). Remarquez la lenteur relative du travail avec la *disquette*.
- *Copiez* sur a (sur la *racine*) les *fichiers* du *dossier* de cours Windows au moyen des *commandes* Edition/Copier (Edit/Copy) et Edition/Coller (Edit/Paste).
- *Déplacez* dans le dossier créé les *fichiers* sur le *disque* a au moyen des *commandes* Edition/Couper (Edit/Cut) et Edition/Coller (Edit/Paste).
- L'écran montre la "*copie*" ou le "*déplacement*" des *fichier*s:

2ème méthode (cliquer-glisser):

Il est possible de *copier* et de *déplacer* des *fichiers* et *dossiers* sans passer par les *menus*, uniquement à l'aide de la souris.

- Ouvrir le *dossier* dans lequel doivent être *copiés* les *fichiers*.
- Ouvrir le *dossier* dans lequel figurent les *fichiers* à *copier* et *sélectionner* ces *fichiers*.
- Eventuellement, si les deux dossiers sont éloignés, repérer dans la partie gauche de la fenêtre (sans aucun clic, uniquement à l'aide de *l'ascenseur*) le *dossier* de destination (cela accélère énormément la procédure).
- *Cliquer-glisser* sur les *fichiers* (*volet* de droite), du *dossier* de départ au *dossier* d'arrivée (*volet* de gauche).

Remarque sur la sélection des objets:
Si plusieurs fichiers adjacents sont à copier, on les sélectionne en cliquant sur le premier, puis sur le dernier en maintenant enfoncée la touche MAJ / SHIFT (grosse flêche pointant vers le haut). Si plusieurs fichiers non adjacents sont à copier, on les sélectionne en cliquant sur chacun d'eux en maintenant la touche CTRL enfoncée.

Remarque sur la copie et le déplacement:
Si le *dragage* se fait sur un même *disque*, il y a *déplacement* des *fichiers*; pour obtenir une *copie*, il faut appuyer en même temps sur la touche CTRL (un petit + accompagne le pointeur).

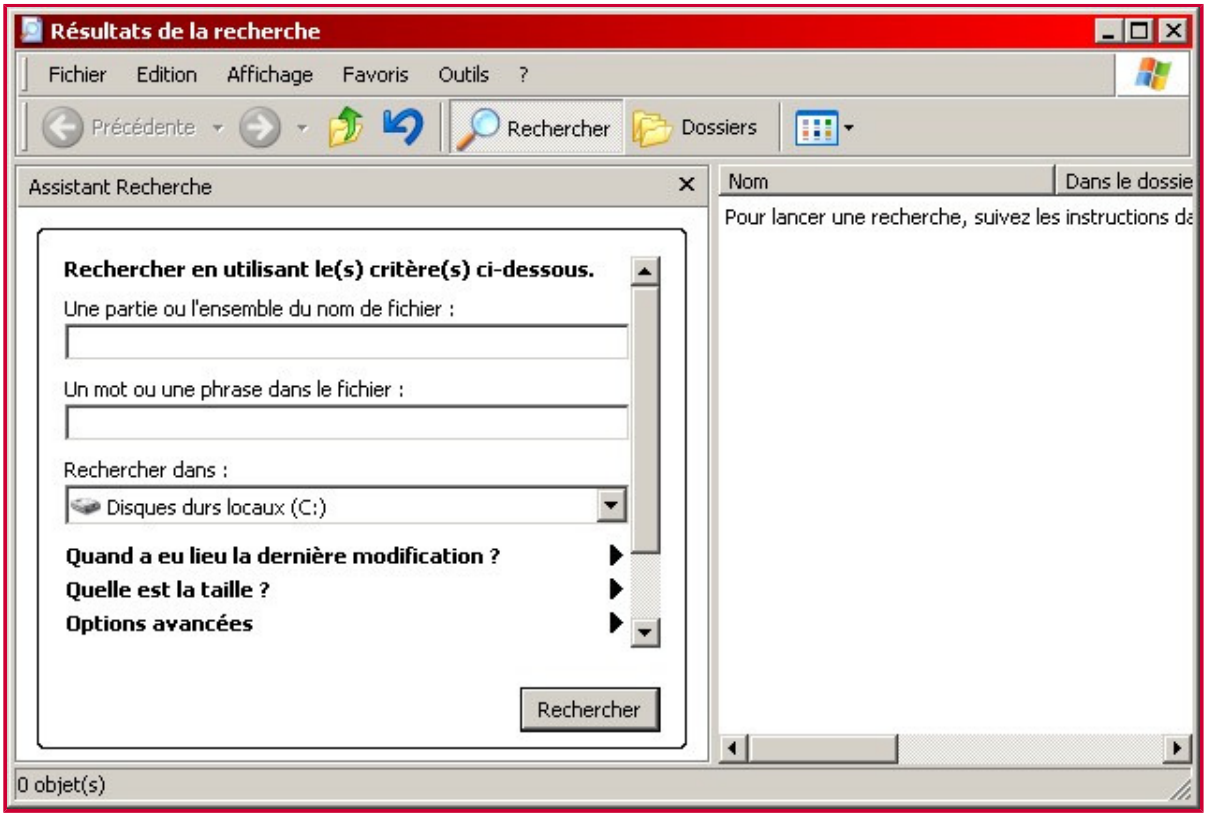
Si le *dragage* se fait d'un *disque* à un autre, il y a *copie* des *fichiers*; pour obtenir un *déplacement*, il faut appuyer sur la touche SHIFT (le petit + disparaît).

Lors de la *copie* ou du *déplacement* des *fichiers*, il importe de lâcher le *bouton* de *souris* au bon moment sous peine de voir les *fichiers* ou *dossiers* parachutés n'importe où, et ainsi mettre le désordre sur le *disque*. Attendez donc que le défilement des *dossiers* se soit stoppé avant de lacher le bouton.

2.3. Autres outils de Windows

L'outil de recherche (Find ou Search selon les versions) 

Le *bouton Rechercher (Search)* de l'explorateur est très utile lorsqu'il s'agit de retrouver un *fichier* dont on a oublié *l'emplacement*, dont on ne connaît plus qu'une partie du *nom*, dont on ne connaît que certains mots de son contenu, dont on ne peut qu'approximer la *taille*,... Cet outil de recherche est aussi accessible à partir de Démarrer/Rechercher/Des Fichiers ou Dossier (Start/Search/For Files or Folders)



Dans la première zone (Search for Files Named), on tape une partie des lettres ou toutes les lettres du nom du *fichier*. Les astérisques remplacent éventuellement des parties inconnues du *nom* (on parle parfois de caractère "Joker"). Par exemple, pour retrouver le *fichier* <explorer.exe>, on peut essayer [*explo*.*] (tous les *fichiers* contenant "explo" dans leur *nom*), [explo*.*] ou même [explo*] (tous les *fichiers* dont le nom commence par "explo"). On entre un mot ou une phrase dans la zone *Contenant le texte (Containing text)* si on ne connaît pas le *nom* d'un *fichier* mais bien un mot ou une phrase spécifique qu'il contient (pour des fichiers de *type texte*, bien sûr). Si on souhaite spécifier l'endroit à partir duquel la recherche doit commencer, on *clique* sur *Parcourir (Browse)* dans la zone Rechercher Dans (Look In), sinon on choisit un disque.

Les options supplémentaires de recherche permettent de retrouver des fichiers et des dossiers sur critères de date, type, taille. L'option Date permet de trouver des fichiers et dossiers *créés*, *modifiés* ou *accédés* entre deux dates, ou lors des derniers jours (à nous de préciser le nombre de jours). L'option Type permet de choisir un *type* de *fichier. L'option Taille permet de spécifier* le minimum ou maximum de *taille* du *fichier* recherché

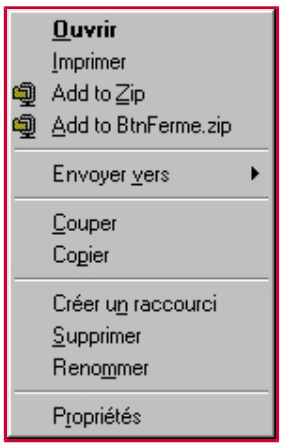
Lorsqu'on *clique* sur *Rechercher (Search)*, l'ordinateur parcourt tous ses *dossiers* et *sous-dossiers* à la recherche des *fichiers* et *dossiers* satisfaisant les critères choisis. Ces *fichiers* et *dossiers* sont alors classés en liste dans la partie droite de la *fenêtre*. Il est possible, depuis cette *fenêtre*, de reproduire les mêmes opérations sur *fichiers* et *dossiers* que dans *l'Explorateur* (*ouverture*, *copie*, *déplacement*,...).

Les menus contextuels

Si on *clique* avec le bouton droit sur un *fichier* ou un *dossier* dans l'Explorateur, le *menu* qui apparaît affiche les *commandes* les plus fréquemment utilisées pour ce *fichier* ou ce *dossier*. On peut aussi *cliquer* avec le bouton droit sur un espace vide de la *barre des tâches* ou du *bureau*. Le *menu* sera différent car le contexte aura changé.

Le *menu contextuel* d'un *fichier* permet d'accélérer la première méthode de *copie* et de *déplacement* décrite ci-dessus. Les *commandes Couper*, *Copier* et *Coller* y sont accessibles beaucoup plus rapidement.

Le *menu contextuel* permet aussi *d'ouvrir* rapidement le *fichier sélectionné* à l'aide du *logiciel associé* à *l'extension* du *fichier*. On peut aussi *l'imprimer*, éventuellement l'ajouter à une *archive*. La *commande* "Envoyer vers" (Send To) permet d'en faire une *sauvegarde* sur disquette, d'en faire un *raccourci* sur le *bureau*, de le joindre comme "*attache*" à un *message électronique*, ...



Les *propriétés* du *fichier* sont constituées de son *nom*, son *type*, son *emplacement* sur le *disque*, sa *taille*, ses dates de création, de dernière modification, de dernier accès,.. Parfois un *aperçu* (sans l'ouvrir) est même possible.

Un *clic droit* sur une partie vide de l'Explorateur permet en outre de créer un *nouveau dossier* ou un *nouveau fichier*. Plusieurs *types* de *fichiers* sont proposés *par défaut*.

L'impression de fichiers

Avant d'imprimer à partir d'un ordinateur, il faut qu'une imprimante y soit installée physiquement et logiciellement.

Pour installer (logiciellement) une imprimante réseau sur les ordinateurs des salles Renaissance, vous devez suivre Démarrer/Paramètres/Imprimantes et Télécopieurs/Ajouter une imprimante (Start/Setup/Printers.../Add Printer). Un assistant vous aider ensuite à l'installation. Si l'assistant varie d'une machine à l'autre ou d'un Windows à l'autre, les informations qu'il récolte sont les mêmes. L'assistant demande si l'imprimante est "locale" ou "réseau". L'imprimante des salles Renaissance est en réseau. L'assistant vous demande ensuite son chemin réseau et son nom. Il faut lui indiquer "\\lis-dc2000\renaissance1" pour ainsi installer l'imprimante de Renaissance1.

Pour imprimer dans les salles Renaissance, à partir de Windows ou de toute application, nous vous déconseillons d'utiliser le bouton représentant une imprimante. Ce bouton lance une impression sur l'imprimante par défaut avec les paramètres par défaut, et vous risquez de ne pas voir votre travail correctement imprimé, ou de ne pas le voir du tout. Utilisez plutôt la commande Fichier/Imprimer... (File/Print...). Dans la boite de dialogue qui apparaît, choisissez la bonne imprimante (Printer) et changez les propriétés de l'imprimante ou les paramètres d'impression selon vos besoins. Les options sont variables selon les logiciels et les imprimantes: orientation des pages, objets à imprimer, qualité d'impression,...

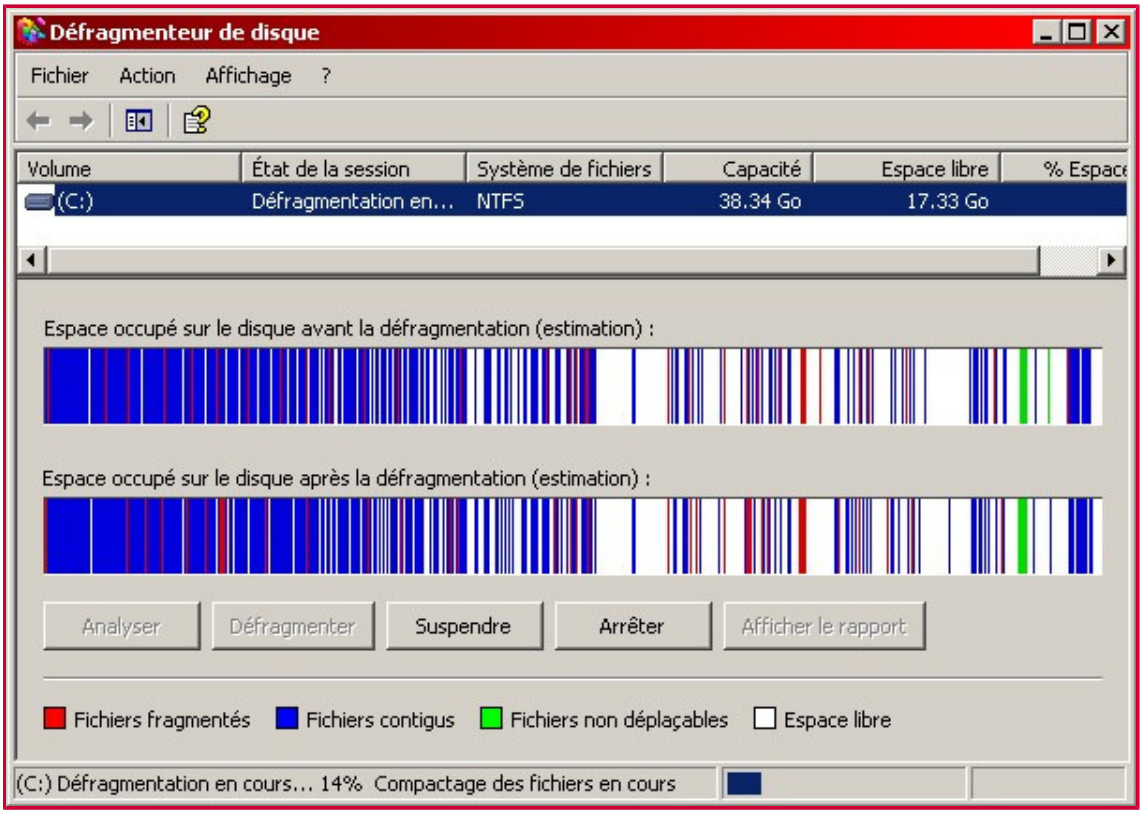
Le défragmenteur de disque

(Les paragraphes sur la défragmentation sont en grande partie extraits du site www.commentcamarche.net.)

Lorsque vous enregistrez un fichier sur le disque (celui-ci étant vide à la base), toutes les informations concernant ce fichier sont écrites les unes à la suite des autres. Lorsque vous enregistrez un deuxième fichier, celui-ci va s'enregistrer à la suite du premier et ainsi de suite. Cependant, lorsque un fichier est effacé, ceci génère un espace vide sur le disque. Or, les fichiers suivants vont combler les "trous", et vont donc être éparpillés en portions de fichiers sur le disque. Cela est d'autant plus vrai que le disque dur a une grosse capacité et possède une grande quantité de fichiers. Ainsi, lorsque le système accède à un fichier, la tête du disque va devoir parcourir l'ensemble des endroits où les morceaux du fichier sont enregistrés pour pouvoir lire celui-ci. Cela se traduit donc par une baisse de performances...

La copie, le déplacement et la suppression des fichiers est inévitable, car le système écrit constamment des fichiers temporaires. Il est donc indispensable de recourir à un outil de défragmentation, c'est-à-dire un logiciel capable de réorganiser les fichiers sur le disque dur de telle façon que les "parcelles" de fichiers soient stockées de manière

contiguë afin de former des fichiers plus "compacts". Il est ainsi recommandé d'utiliser régulièrement (une fois par mois environ) un utilitaire de défragmentation, qui va réorganiser les données stockées sur le disque.



Windows propose un outil de défragmentation. Vous y accédez à partir de l'Explorateur Windows, en ouvrant les propriétés du disque que vous désirez défragmenter. Sur l'onglet Outils (Tools) des propriétés se trouvent un outil de vérification des erreurs de disque, et l'outil de défragmentation. D'autres logiciels permettent la défragmentation. Ils sont parfois plus puissants que l'outil de Windows, mais parfois également payants.

L'outil de défragmentation utilise des algorithmes afin de réordonner au mieux les fichiers sur le disque. Les morceaux de fichiers éparpillés sur le disque sont déplacés tour à tour dans l'espace disque disponible (non utilisé par des fichiers) de manière temporaire, puis replacés à un endroit adéquat. Cette défragmentation se fait ainsi d'autant plus facilement que l'espace disque disponible est important.

D'autre part, si les données sont changées lors de la défragmentation, l'outil doit recalculer la manière de déplacer les fichiers afin de tenir compte de ces nouveaux changements. Il est donc indispensable de fermer toutes les applications ouvertes avant de commencer la défragmentation. Or le système d'exploitation possède des processus fonctionnant en arrière-plan et accédant au disque dur (notamment lorsque la quantité de mémoire vive présente sur le système n'est pas suffisante, car le système crée des fichiers d'échange). Ainsi, il est fortement recommandé pour les ordinateurs fonctionnant sous Windows, de le redémarrer en *mode sans échec*, c'est-à-dire un mode dans lequel les éléments de configuration minimaux sont chargés. Pour redémarrer l'ordinateur en mode sans échec, il suffit d'appuyer sur la touche *F8* juste après l'écran de démarrage de l'ordinateur (comptage de la mémoire vive et détection des disques) et juste avant le message *Démarrage de Windows*.

L'aide

L'aide Windows est une première source d'informations pour apprendre à utiliser Windows et pour devenir autonome. La plupart des logiciels qui tournent sous Windows sont équipés d'une rubrique d'aide, assez semblable à celle de Windows (surtout pour les logiciels Office). Toujours disponible depuis le menu Aide (Help) du logiciel utilisé, l'aide décrit comment effectuer un grand nombre de tâches comme (pour Windows par exemple) l'installation d'une imprimante, ou la connexion à Internet. L'aide contient aussi un glossaire, des aides au dépannage, des liens aux ressources Web,...

Pour ouvrir l'aide Windows, cliquez le bouton Démarrer (Start) puis Aide (Help). Vous trouverez les différents thèmes dans l'onglet Contenu (Contents), les mots-clés dans l'onglet Index (index), et pourrez faire une recherche dans l'onglet Recherche (Search). Vous pouvez aussi obtenir des informations concernant une boîte de dialogue en cliquant sur le bouton point d'interrogation situé dans la barre de titre puis en cliquant sur la zone de la boîte de dialogue qui vous intéresse.

D'autres outils d'aide sont disponibles sous la forme de tutoriaux sur Internet, de sites de vulgarisation informatique (par exemple www.commentcamarche.net ou www.hotline-pc.org), ou encore à l'aide des moteurs de recherche.

Par exemple, face à un message d'erreur obscur, saisissez le message ou le code d'erreur avec la même syntaxe dans Google. Les moteurs vous renvoient souvent vers des forums où les problèmes sont déchiffrés et où des solutions sont parfois proposées.

2.4. Tableau d'équivalence entre Windows en Français et en Anglais

Voici un tableau donnant l'équivalent français / anglais des mots de vocabulaire rencontrés dans Windows.

Français	Anglais
Fichier	File
Dossier	Folder
Disque	Disk
Logiciel	Software
Matériel	Hardware
Fenêtre	Window
Bureau	Desktop
Barre de Tâches	Task Bar
Bouton Démarrer	Start Button
Explorateur	Explorer
Poubelle	Recycle Bin
Enregistrer	Save
Copier un fichier	Copy
Couper un fichier	Cut
Coller un fichier	Paste
Supprimer	Delete

3. Téléchargement et installation de logiciels utilitaires

3.1. Téléchargement de logiciels utilitaires

Le terme de téléchargement est utilisé en français pour décrire deux opérations inverses, que les anglophones définissent avec deux mots différents: upload et download. L'upload est l'envoi de fichiers de son ordinateur vers un serveur. Le download est l'import d'un fichier depuis un serveur sur son ordinateur. Le terme téléchargement utilisé dans ce document ne concerne que la deuxième opération, le download. Le téléchargement, dans le cadre de ce cours, ne concernera d'ailleurs que le download de logiciels utilitaires.

Il existe de nombreux logiciels utilitaires sur Internet. Ceux-ci facilitent vos taches usuelles, qu'il s'agisse d'écrire, de calculer, de dessiner, de compresser, de télécharger, de gérer,... Dans le cadre de ce cours, on peut par exemple télécharger et installer un antivirus (AntiVir Personnal Edition), un compacteur (WinZip), un lecteur et imprimeur de fichiers PDF (Adobe Reader), un logiciel de multimedia (QuickTime). Les références détaillées de ces logiciels (nom, site de l'éditeur, licence,...) se trouvent sur notre site www.ulb.ac.be/soco/matsch/info-d-203 , dans la partie téléchargement.

Parmi les logiciels que vous téléchargerez, tous ne seront pas gratuits. A côté des freeware, on trouve des demoware ou des logiciels en shareware, souvent sous forme de trialware.

- Un freeware est un logiciel totalement gratuit et dont les fonctions ne sont pas limitées. On parle aussi de graticiel.
- Un demoware est un logiciel gratuit qui correspond à une version de démonstration limitée. Par exemple, la démo d'un jeu qui ne contient que quelques niveaux.
- Un shareware, ou partagiciel, est un logiciel en mode de distribution directe. Ces logiciels sont souvent libres d'utilisation, à charge de l'utilisateur d'envoyer une somme d'argent à l'auteur si le logiciel lui plaît et s'il veut l'utiliser de manière continue. D'autres shareware sont plutôt des trialware.
- Un trialware est une version d'évaluation gratuite qui cesse de fonctionner après un certain temps. Il est alors

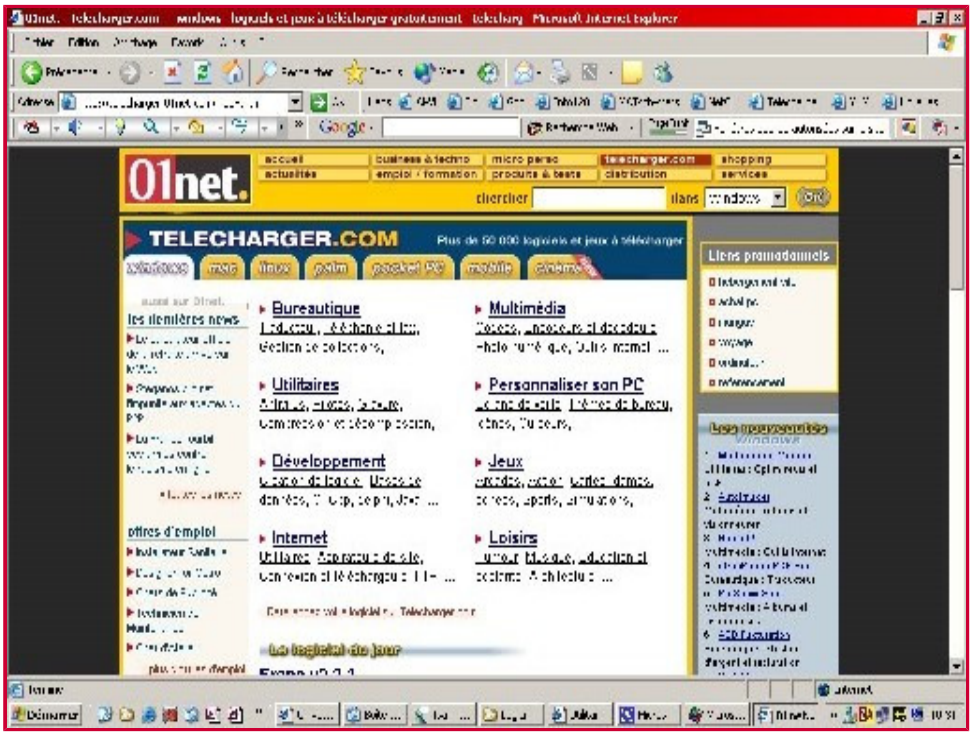
recommandé de payer la licence pour continuer à l'utiliser.

3.1.1. Téléchargement à l'aide d'un site de téléchargement

Il existe de nombreux sites de téléchargement.

- Download.com (www.download.com) : sans doute le plus connu. Malheureusement, en anglais, et ne propose aucun logiciel en français.
- Telecharger (www.telecharger.com) : de très nombreux logiciels au catalogue (le plus complet); un affichage permettant de trouver immédiatement les logiciels en français; logiciels pour Windows, MacIntosh, Linux, Palm, PocketPC.
- Clubic (www.clubic.com) : très belle logithèque, complète et très bien ordonnée.
- ZDNet (www.zdnet.fr/telecharger) : pendant francophone de Download.com; complet et ordonné; logiciels destinés aux professionnels; certains logiciels peuvent être directement achetés en ligne.
- Framasoft (www.framasoft.net) : pour les spécialistes; logiciels gratuits et "libres" uniquement; liens pour accéder aux modes d'emploi ou explications.
- ...

Dans le cadre de ce cours, nous utiliserons le site www.telecharger.com pour ses nombreux avantages. Les procédures ci-dessous sont assez générales, et vous n'aurez pas de difficultés à les appliquer sur d'autres sites.



3.1.1.1. Recherche par rubriques (par exemple pour AntiVir)

Le premier moyen d'atteindre un logiciel est d'utiliser les rubriques proposées. Pour télécharger l'antivirus AntiVir par exemple, nous choisirons la rubrique "Utilitaires", et la sous-rubrique "Antivirus".

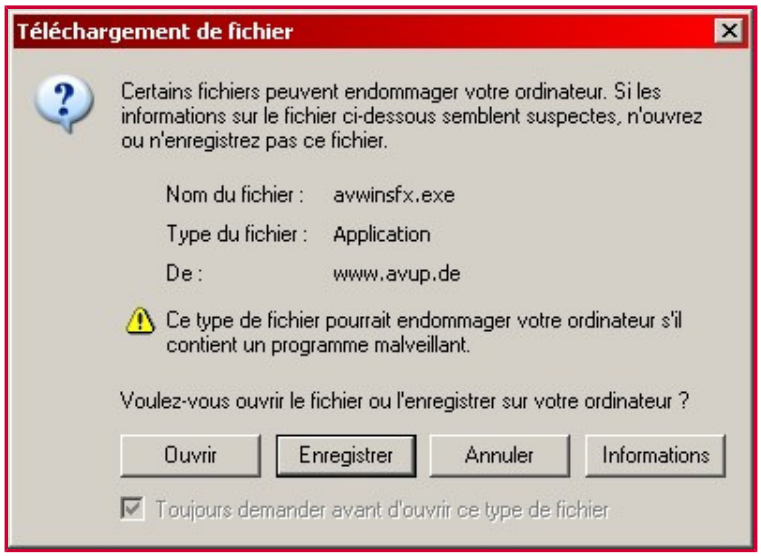
Une liste de logiciels antivirus, ou assimilés, nous est proposée. Une commande permet de n'afficher que les logiciels gratuits. Pour trouver le(s) plus populaire(s), il est possible d'afficher le listing "par nombre de téléchargements". Attention, il vaut peut-être mieux passer au-delà des premiers liens sponsorisés pour lesquels trop peu d'informations nous sont données.

Nous parcourons les quelques premières pages à la recherche de "AntiVir Personnal Edition". Lorsqu'il est trouvé, cliquez sur son titre afin de lancer sa page d'informations. On y découvre son descriptif, sa langue, sa licence, sa taille, la configuration minimale pour l'installation. Lisez bien ce qui est écrit sur chaque page ou site de téléchargement. Chaque logiciel ne fonctionne par sur n'importe quel ordinateur, mais sur une configuration précise avec une mémoire vive particulière et un système d'exploitation particulier.

INFORMATIONS SUR CE LOGICIEL	
Taille :	3.97168 Mo
Version :	6.25.00.94
Configuration minimale :	Windows NT/95/98/2000/ME/XP,
Temps du téléchargement en 56 K :	9 min et 27.6 s.
->(adsl et cable) 512 K :	1 min et 1.8 s.
Licence :	gratuit
Rubrique :	Utilitaires
Sous rubrique :	Antivirus
Langue:	Anglais
Auteur / Editeur :	H+BEDV Datentechnik GmbH
Téléchargé la semaine dernière:	5718 fois
Date de sortie :	14 Juin 2004

Cliquez sur le bouton "Télécharger", et attendez que la fenêtre d'enregistrement apparaisse. Le cas échéant, choisissez l'option "Si rien ne se passe, vous pouvez choisir l'un de ces liens: lien N°1'". Des fenêtres Pop-up peuvent apparaître durant votre visite des sites de téléchargement. Il s'agit de fenêtres de navigation qui s'ouvrent au-dessus de la fenêtre principale. De nombreux sites affichent des publicités dans de telles fenêtres. Nous vous conseillons de les fermer sans cliquer sur leur contenu.

Lorsque la fenêtre d'enregistrement est apparue, choisissez le bouton "Enregistrer", sélectionnez un disque, un dossier (classiquement C:/Program Files hors des salles Renaissance), et créez-y un sous-dossier (de type "NomDuLogiciel", par exemple ici "AntiVir"). Il peut être intéressant de créer un sous-dossier, que l'on appelle par exemple "Téléchargement" ou "Archive" afin de bien distinguer le fichier téléchargé des fichiers d'installation qui vont bientôt apparaître. Téléchargez le fichier dans ce dossier.



Confirmez le message de fin d'enregistrement. Si l'option vous est proposée, ouvrez directement le dossier contenant le fichier à l'aide du bouton adéquat.

Archivez soigneusement aussi sur disquettes ou sur CD-Rom les fichiers compressés que vous avez téléchargés. En cas de problème avec votre ordinateur, vous pourrez ainsi réinstaller les logiciels à partir de leurs fichiers d'origine, sans avoir à les télécharger à nouveau.

3.1.1.2. Recherche par mot-clé (par exemple pour WinZip)

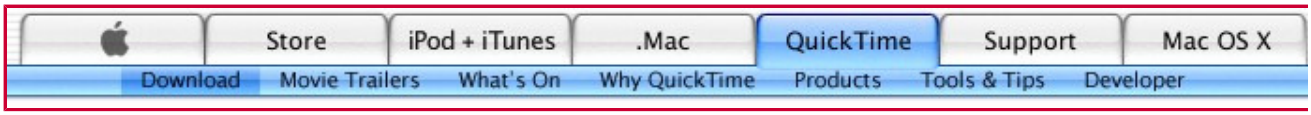
Dans la zone de recherche du site de téléchargement, entrez Zip afin de sortir le listing de tous les logiciels liés à ce format. Cette zone permet de rechercher des logiciels à utiliser ailleurs que sur Windows: Mac, Palm, Linux,...

Les résultats peuvent à nouveau être triés par nombre de téléchargements. Le listing fournit par exemple WinZip 8 en version française, et WinZip 9 en version anglaise. A nouveau, on découvre la fiche du logiciel avec son descriptif, sa langue, sa licence, sa taille, la configuration minimale pour son installation. La suite du téléchargement se passe exactement comme au point 3.1.1.1.

3.1.2. Téléchargement sur le site de l'éditeur (par exemple pour QuickTime)

Si l'adresse de l'éditeur du logiciel est connue, il suffit de l'encoder dans la barre d'adresses de votre navigateur Internet. Sinon, on ne risque rien à essayer des adresses du type www.[NomDuLogiciel].com ou www.[NomDuLogiciel].fr .. Mais attention aux sites qui ne sont pas ceux attendus. Par exemple, le site www.quicktime.fr n'a rien à voir avec le logiciel multimedia dont nous traitons ici! Sinon, entrer le lom du logiciel dans un moteur de recherche donne parfois un bon résultat en fournissant d'emblée un lien vers le site de l'éditeur. C'est le cas avec le mot "quicktime" dans Google.

Lorsque vous êtes sur le site de l'éditeur, il faut parfois naviguer afin de découvrir la page des logiciels de l'éditeur, ou la page de téléchargements. Par exemple si vous avez atteint le site www.apple.com , commencez par lire la page d'accueil, puis cherchez les liens dans les menus du site vers la page de téléchargement de QuickTime. Vous aurez à cliquer sur l'onglet "QuickTime", puis à y choisir le menu "Download" (Il y a différents moyens d'y arriver sur ce site, et cette procédure varie bien sûr d'un site à l'autre).



Certains sites demandent des informations sur votre plateforme afin de vous permettre de télécharger la version adéquate du logiciel. D'autres informations parfois demandées sont votre langue ou d'autres informations plus personnelles. Certains sites proposent de vous inscrire à une "newsletter" de sorte à vous avertir de mises à jour de logiciels, ou à vous envoyer des informations promotionnelles. Sur le site de QuickTime, lorsque vous avez répondu aux quelques questions, appuyez sur le bouton "Download".

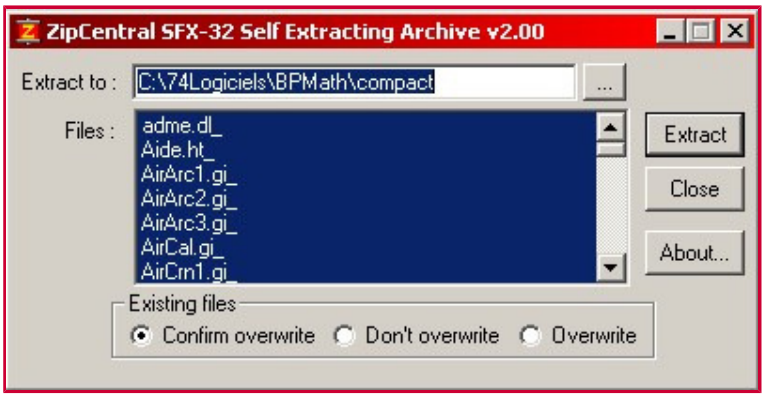
Dans la plupart des cas, la fin de l'installation se passera comme au point 3.1.1.1. (Choisir un disque, un dossier, ...). Parfois, pour de "gros" logiciels comme QuickTime, ou lors d'installations comme pour les mises à jour de produits Microsoft, l'installation se fera en ligne. Aucun fichier n'est téléchargé sur le disque dur, et un assistant aide à l'installation directement à partir d'Internet (voir ci-dessous pour l'installation à l'aide d'un assistant).

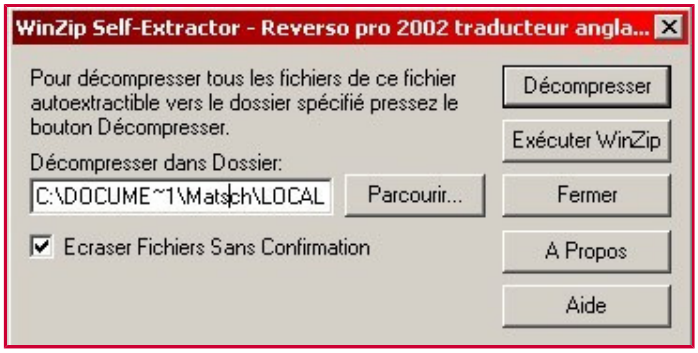
3.2. Installation de logiciels utilitaires

Si ce n'est déjà fait, ouvrez le dossier contenant le fichier téléchargé. Soit il s'agit d'une archive (zip, exe,...), soit il s'agit d'un fichier d'installation (exe). On ne sait généralement pas dans quel cas on se trouve, car le fichier est souvent un fichier de type "exe". On note alors la différence en fonction du comportement du fichier lorsque l'on double-clique dessus. Si le fichier est une archive, la suite de la procédure est indiquée au point 3.2.1. S'il s'agit d'un fichier d'installation, vous pouvez passer directement au 3.2.2.

3.2.1. Décompression d'une archive

Cette procédure est à suivre si le fait de double-cliquer sur le fichier téléchargé lance une fenêtre de décompression. Décompressez l'archive dans le dossier de téléchargement, si possible dans un nouveau dossier, par exemple le dossier "Installation" que vous créez. Le chemin vers le fichier d'installation devrait donc être du type C:\ProgramFiles\[NomDuLogiciel]\Installation\. Certaines de ces fenêtres vous proposent d'exécuter WinZip. Les détails de procédure de décompression, en particulier avec le logiciel WinZip, sont décrites plus loin dans ce document.





Après décompression, ouvrez le dossier Installation et trouvez-y le fichier d'installation. Ce sera souvent un fichier de type "exe", qui s'appellera d'ailleurs souvent "setup.exe".

3.2.2. Installation du logiciel (par exemple pour AntiVir)

Double-cliquez sur le fichier d'installation, qui aura directement été téléchargé comme au point 3.1., ou qui aura été décompressé comme au point 3.2.1. Dans le cadre du logiciel AntiVir, le fichier téléchargé s'appelle "avwinsfx.exe". Le double-clic lance très souvent un assistant d'installation, qui pose souvent le même genre de questions: quel est le chemin d'installation, quelles sont les options logicielles d'installation, quels sont les paramètres personnels (nom, adresse e-mail, ...), ...

L'assistant varie bien sûr selon le logiciel à installer. Il est donc difficile de présenter toutes les installations. Mais la procédure qui suit devrait vous aider à vous familiariser avec l'installation de n'importe quel logiciel. Les copies d'écrans suivantes montrent l'assistant d'installation de AntiVir.

Remarquez que avwinsfx.exe est une archive auto-extractible qui décompresse sans laisser de choix d'options (le chemin par exemple) et qui lance directement après décompression le fichier d'installation.

Vous rencontrerez des fenêtres d'informations. Lisez ces informations, et appuyez sur le bouton Next. Vous rencontrerez des fenêtres de licence. Lisez ces licences, et si vous êtes d'accord, cochez la case de type "I accept all the terms of the preceeding license agreement", et appuyez sur le bouton Next. Vous rencontrerez des fenêtres d'options. Choisissez celles qui vous intéressent. Laissez finalement le logiciel s'installer. C'est parfois assez long, même sur des machines récentes.

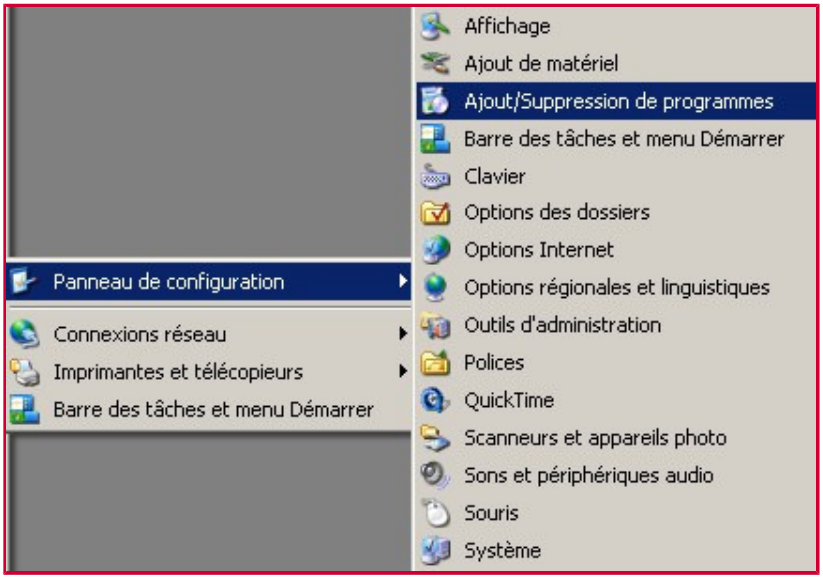
Il est parfois nécessaire de redémarrer la machine, de sorte que des informations supplémentaires puissent s'inscrire dans des fichiers système ou dans la base de registres. Même si on ne vous le propose pas, ou si on vous propose de le faire plus tard, redémarrez l'ordinateur après l'installation. Vous éviterez ainsi de nombreux plantages.

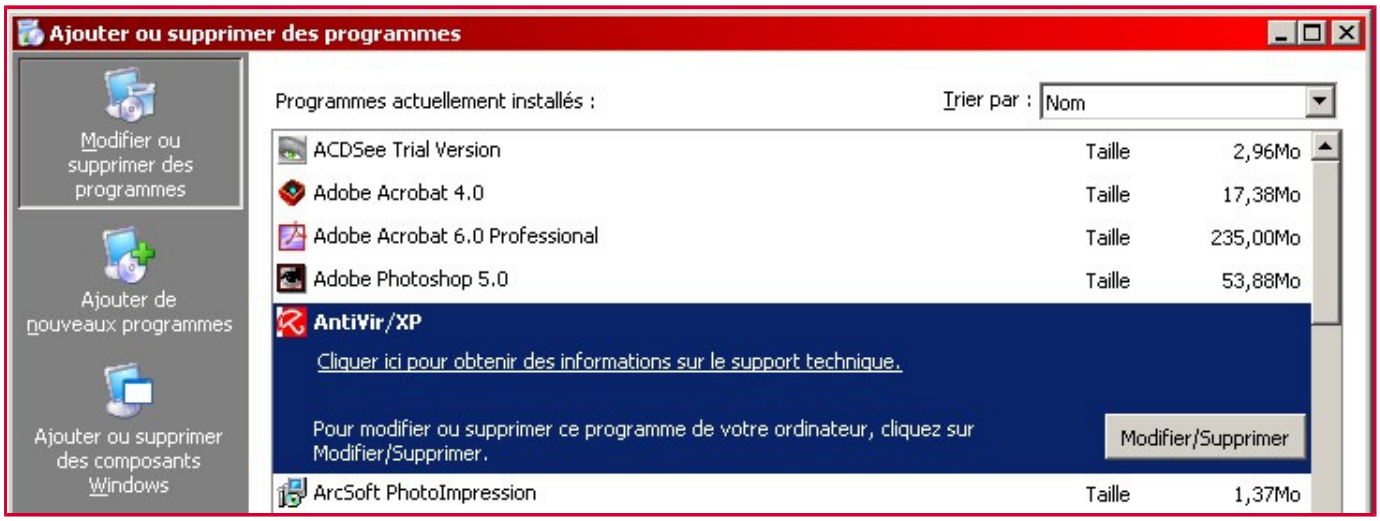
Après installation, et après redémarrage, testez les fonctionnalités de votre logiciel.

3.3. Désinstallation de logiciels.

Par manque de place sur votre machine, ou en cas de mauvais fonctionnement, vous devrez peut-être désinstaller votre logiciel (pour le réinstaller "proprement s'il s'agit de mauvais fonctionnement). La première méthode de désinstallation consiste à chercher la commande de désinstallation du logiciel. Le logiciel utilitaire aura créé un "groupe" dans le menu démarrer (souvent Démarrer/Programmes/[NomDuLogiciel] (Start/Programs/[NomDuLogiciel])) contenant les commandes qui lancent le logiciel, qui ouvre la page d'aide ou le manuel, qui lance des options,... Ce groupe contient parfois une commande de type "uninstall" qui devrait vous permettre de désinstaller proprement le logiciel.

La seconde méthode, si la première n'est pas pratiquable, est de désinstaller à l'aide de Windows. Cette option n'est pas disponible dans les salles Renaissance, pour raison de sécurité. Ouvrez le panneau de configuration: Démarrer/Paramètres/Panneau de Configuration (Start/Setup/Setup Panel). Choisissez-y "Ajout/suppression de programmes" ou "Installation/désinstallation" (selon les versions de Windows). Vous trouverez une liste de nombreux logiciels installés sur votre machine (pas tous). Sélectionnez celui à désinstaller, et choisissez le bouton ou la commande de désinstallation.





Lorsque vous avez désinstallé un logiciel, si vous n'avez plus à l'utiliser, vous pouvez supprimer le dossier d'installation afin d'alléger votre disque dur. Ne désinstallez jamais un logiciel en supprimant simplement son dossier d'installation ! ! ! Vous ne supprimerez ainsi pas les informations stockées dans les fichiers système ou dans la base de registre. Avec cette méthode, vous vous assurez de nombreux plantages à chaque prochaine utilisation de votre machine.

Après la désinstallation, redémarrez votre machine.

4. La sécurité informatique

(paragraphes essentiellement repris de l'encyclopédie informatique libre CommentCaMarche, page http://www.commentcamarche.net/secu/secuintro.php3 et suivantes)

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation ou d'un poste seul sont uniquement utilisées dans le cadre prévu. La sécurité informatique consiste généralement en quatre principaux objectifs :

- L'intégrité, c'est-à-dire garantir que les données sont bien celles qu'on croit être
- La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources
- La disponibilité, permettant de maintenir le bon fonctionnement du système informatique
- La non répudiation, permettant de garantir qu'une transaction ne peut être niée

4.1. Les virus et les codes cachés

4.1.1. Les 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. Le véritable nom donné aux virus est CPA soit Code Auto-Propageable, mais par analogie avec le domaine médical, le nom de "virus" leur a été donné.

Le champ d'application des virus va de la simple balle de ping-pong qui traverse l'écran au virus destructeur de données, ce dernier étant la forme de virus la plus dangereuse. Ainsi, étant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées, les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection. On distingue ainsi différents types de virus :

- les vers sont des virus capables de se propager à travers un réseau
- les troyens (chevaux de Troie) sont des virus permettant 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)
- les bombes logiques sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...)

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.

4.1.2. Concept d'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.

4.1.3. Les vers

Un ver est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager; un ver est donc un virus réseau. 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. Ils se déclenchent lorsque l'utilisateur destinataire clique sur le fichier attaché.

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 susceptible d'être infectés : exe, com, bat, pif, vbs, scr, doc, xls, msi, eml. Pour tous les fichiers dont l'extension peut supposer que le fichier soit infecté (ou pour les extensions que vous ne connaissez pas) n'hésitez pas à installer un antivirus et à scanner systématiquement le fichier attaché avant de l'ouvrir.

4.1.4. Les chevaux de Troie

On appelle "Cheval de Troie" (en anglais trojan horse) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur. Le nom "Cheval de Troie" provient de la légende narrée dans l'Iliade (de l'écrivain Homère) à propos du siège de la ville de Troie par les Grecs. Un cheval de Troie (informatique) est donc un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (en anglais backdoor), par extension il est parfois nommé troyen par analogie avec les habitants de la ville de Troie.

A la façon du virus, le cheval de Troie est un code (programme) nuisible placé dans un programme sain (imaginez une fausse commande de listage des fichiers, qui détruit les fichiers au lieu d'en afficher la liste). Un cheval de Troie peut par exemple

- voler des mots de passe ;
- copier des données sensibles ;
- exécuter tout autre action nuisible ;
- …

Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur.

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

- activité anormale du modem ou de la carte réseau : 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 ;

Pour se protéger de ce genre d'intrusion, il suffit d'installer un firewall, c'est-à-dire un programme filtrant les communications entrant et sortant de votre machine. Un firewall (littéralement pare-feu) permet ainsi d'une part de voir les communications sortant de votre machines (donc normalement initiées par des programmes que vous utilisez) ou bien les communications entrant. 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 pirate. En effet il peut s'agir de tests effectués par votre fournisseur d'accès ou bien un pirate scannant au hasard une plage d'adresses IP.

Pour les systèmes de type Windows, il existe des firewalls non payants très performants :

- ZoneAlarm en version non professionnelle
- Tiny personal firewall

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 récidive, 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, téléchargeable sur http://www.moosoft.com.

4.1.5. Les hoaxes

On appelle hoax (en français canular) un courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues. Ainsi, de plus en plus de personnes font suivre des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus. Le but des hoax est simple : provoquer la satisfaction de son concepteur d'avoir berné un grand nombre de personnes.

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'encombrement des boîtes aux lettres électroniques déjà chargées,
- La perte de temps, tant pour ceux qui lisent l'information, que pour ceux qui la relaye ;
- 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.

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.

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 (Google étant un des plus fiables).

4.1.6. Les espiogiciels

Un espiogiciel (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).

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 (e liste non exhaustive) de logiciels connus pour embarquer un ou plusieurs spywares : Babylon Translator, GetRight, Go!Zilla, Download Accelerator, Cute FTP, PKZip, KaZaA ou encore iMesh.

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 registres créés par des spywares. Parmi les anti-spywares les plus connus ou efficaces citons notamment :

- Ad-Aware de Lavasoft.de
- Spybot Search&Destroy

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

4.1.7. Les keyloggers

Un keylogger (littéralement enregistreur de touches) est un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. 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 malintentionnées 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).

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.

4.1.8. Les kits de désinfection

Un kit de désinfection est un petit exécutable dont le but est de nettoyer une machine infectée par un virus particulier. Chaque kit de désinfection est donc uniquement capable d'éradiquer un type de virus particulier voire une version particulière d'un virus. Les utilitaires de désinfection ne remplacent en rien l'action d'un logiciel antivirus. En effet l'antivirus a un rôle préventif, afin d'intercepter le virus avant l'infection de la machine. Toutefois en cas d'infection, les kits de désinfection vous permettront de prendre des mesures correctives pour éradiquer le virus !

Pour éradiquer un virus présent sur votre machine, pourvu que vous sachiez quel virus a infecté votre système, la meilleure méthode consiste tout d'abord à déconnecter la machine infectée du réseau, puis à

récupérer le kit de désinfection adhoc. Puis il s'agit de redémarrer l'ordinateur en mode sans échec (hormis pour WindowsNT) et de lancer l'utilitaire de désinfection.

D'autre part, certains vers se propagent par l'intermédiaire d'une faille de sécurité de Microsoft Internet Explorer, ce qui signifie que vous pouvez être contaminé par le virus en naviguant sur un site infecté. Pour y remédier il est nécessaire de télécharger le patch (correctif logiciel) pour Microsoft Internet Explorer 5.01 et supérieur. Ainsi, veuillez vérifier la version de votre navigateur et télécharger le correctif si nécessaire : http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

Pour télécharger les utilitaires: www.commentcamarche.net/virus/desinfection.php3 ou www.secuser.com

4.2. Autres problèmes de sécurité : les attaques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont en réalité généralement lancées automatiquement à partir de machines infectées (virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire et plus rarement par des pirates informatiques. C'est la raison pour laquelle il est absolument impératif d'installer un pare-feu afin de faire barrière entre l'ordinateur et le réseau.

On appelle «attaque réseau» l'exploitation d'une faille (du système d'exploitation, d'un logiciel communiquant par le réseau ou bien même de l'utilisateur) à des fins non connues par la victime et généralement préjudiciables. Le but peut être de différentes sortes :

- obtenir un accès au système
- obtenir des informations personnelles sur l'utilisateur
- récupérer des données bancaires
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- faire dysfonctionner un service
- utiliser le système de l'utilisateur comme «rebond» pour une attaque
- utiliser le système de l'utilisateur comme serveur FTP, lorsque le réseau sur lequel il est situé possède une bande passante élevée

4.2.1. Types d'attaques

Les attaques réseau consistent généralement à exploiter une vulnérabilité du système d'exploitation ou de l'une de ses applications en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à l'accès au système tout entier.

Pour autant les erreurs de programmation contenues dans les programmes sont habituellement corrigées assez rapidement par leur concepteur dès lors que la vulnérabilité a été publiée. Il appartient alors aux administrateurs (ou utilisateurs personnels avertis) de se tenir informé des mises à jour des programmes qu'ils utilisent afin de limiter les risques d'attaques.

D'autre part il existe un certain nombre de dispositifs (pare-feu, systèmes de détection d'intrusions, antivirus) permettant d'ajouter un niveau de sécurisation supplémentaire.

Enfin dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! En effet c'est souvent lui, par méconnaissance ou dupé par un interlocuteur malicieux, qui va exécuter un fichier vérolé, donner des informations personnelles ou bancaires, etc. Ainsi, aucun dispositif de protection ne peut protéger l'utilisateur contre les arnaques, seuls bon sens, raison et un peu d'information sur les différentes pratiques peuvent lui éviter de tomber dans le piège !

4.2.2. Le hacking

Le terme «hacker» est souvent utilisé pour désigner un pirate informatique. Les hackers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des failles, c'est-à-dire des vulnérabilités nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation ! Les termes de vulnérabilité, de brèche ou en langage plus familier de trou de sécurité (en anglais security hole) sont également utilisés pour désigner les failles de sécurité.

Pour pouvoir mettre en oeuvre un exploit (il s'agit du terme technique signifiant exploiter une vulnérabilité), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci.

Une fois que le hacker a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui

permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.

La dernière étape du hacker consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

4.2.3. Attaques par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer l'adresse IP réelle du pirate et d'utiliser les ressources de la machine servant de rebond. Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, car celui-ci se retrouve «complice» contre son gré de l'attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.

Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car si le réseau sans fils est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

4.2.4. Ingénierie sociale

Le terme d'«ingénierie sociale» (en anglais «social engineering») désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct. L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de la maison, un technicien, un administrateur, etc.

La meilleure façon de se protéger des techniques d'ingénierie sociale est d'utiliser son bon sens pour ne pas divulguer à n'importe qui des informations pouvant nuire à la sécurité de vos biens ou de votre entreprise.

4.2.5. Le scam

Le «scam» («ruse» en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est issue du Nigéria, ce qui lui vaut également l'appellation «419» en référence à l'article du code pénal nigérian réprimant ce type de pratique.

L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.

En répondant à un message de type scam, l'internaute s'enferme dans un cercle vicieux pouvant lui coûter plusieurs centaines d'euro s'il mord à l'hameçon.

4.2.6. Introduction au phishing

Le phishing (contraction des mots anglais «fishing», en français pêche, et «phreaking», désignant le piratage de lignes téléphoniques), traduit parfois en «hameçonnage», est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.

La technique du phishing est une technique d'«ingénierie sociale» c'est-à-dire consistant à exploiter non pas une faille informatique mais la «faille humaine» en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce. Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

4.2.7. Loterie internationale

Vous recevez un courrier électronique indiquant que vous êtes l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs (centaines de) milliers d'euro. Pour empocher le pactole il suffit de répondre à ce courrier. Après une mise en confiance et quelques échanges de courriers, éventuellement

avec des pièces jointes représentant des papiers attestant que vous êtes bien le vainqueur, votre interlocuteur vous expliquera que pour pouvoir toucher la dite somme, il faut s'affranchir de frais administratifs, puis viennent des frais de douane, des taxes diverses et variées,… C'est de cette façon que ces cybertruands arrivent à extorquer des milliers d'euros à des internautes dupes de cette supercherie.

4.2.8. Le spam

Depuis que le World Wide Web existe, les ressources se sont démocratisées et le flux d'informations circulant sur le réseau des réseaux n'a cessé d'augmenter. Cependant le contenu de ces informations n'a pas toujours évolué dans le bon sens et de nombreuses personnes ont vite compris comment se servir abusivement de ces ressources... On appelle «spam» (le terme de pourriel est parfois également utilisé) l'envoi massif de courrier électronique à des destinataires ne l'ayant pas sollicité.

Le spam consiste à envoyer des e-mails en grand nombre (souvent de type publicitaire) à des destinataires dont les adresses ont été récupérées au hasard sur Internet. Le mot "spam" provient du nom d'une marque de jambonneau commercialisée par la compagnie L'association de ce mot au postage excessif provient d'une pièce des Monty Python (Monty Python's famous spam-loving vikings) qui se déroule dans un restaurant viking dont la spécialité est le jambonneau "spam". Dans ce sketch, alors qu'un client commande un plat différent, les autres client se mettent à chanter en choeur "spam spam spam spam spam ..." si bien que l'on n'entend plus le pauvre client ! Les personnes pratiquant l'envoi massif de courrier publicitaire sont appelées "spammers", (en français spammeurs), un mot qui a désormais une connotation péjorative !

Le but premier du spam est de faire de la publicité à moindre prix par "envoi massif de courrier électronique non sollicité" (junk mail) ou par "multi-postage abusif" (EMP). Les spammeurs prétendent parfois, pour leur défense, que le courrier est facile à supprimer et qu'il est par conséquent un moyen écologique de faire de la publicité.

Les spammeurs collectent des adresses électroniques sur Internet (dans les forums, sur les sites Internet, dans les groupes de discussion, etc.) grâce à des logiciels (appelés robots) parcourant les différentes pages et stockant au passage dans une base de données toutes les adresses email y figurant. Il ne reste ensuite au spammeur qu'à lancer une application envoyant successivement à chaque adresse le message publicitaire.

Le principal inconvénient du spam est l'espace qu'il occupe dans les boîtes aux lettres des victimes et la bande passante qu'il gaspille sur le réseau Internet, le rendant moins rapide. Cela induit également des coûts de gestion supplémentaires pour les fournisseurs d'accès à Internet (FAI):

- mise en place des systèmes antispam,
- sensibilisation des utilisateurs,
- formation du personnel,
- ressources supplémentaires (serveurs de filtrage, etc.)

Du coup ces frais supplémentaires se répercutent sur les abonnés, de par le prix supplémentaire de l'abonnement, et du temps perdu inutilement...

La chose la plus importante est de ne pas répondre à ces abus, cela ne ferait qu'empirer les choses, et rentrer dans le même jeu que les spammers. Il ne faut donc pas:

- Menacer les spammers (cela ne ferait que les énerver)
- Bombarder les spammers de courrier électronique
- Pirater le site des spammers
- Utiliser le spamming contre les spammers (dépourvu de bon sens...)
- Utiliser toute attaque

4.2.9. Le Mail Bombing

Le mail bombing consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres électroniques afin de la saturer. En effet les mails sont stockés sur un serveur de messagerie, jusqu'à ce qu'ils soient relevés par le propriétaire du compte de messagerie. Ainsi lorsque celui-ci relèvera le courrier, ce dernier mettra beaucoup trop de temps et la boîte aux lettres deviendra alors inutilisable...

Les solutions au mail bombing sont les suivantes :

- Posséder plusieurs boîte aux lettres : une principale que vous ne divulguez qu'aux personnes dignes de confiance, et une à laquelle vous tenez moins, utilisée par exemple pour s'inscrire à des services en ligne sur Internet ;
- Installer un logiciel anti-spam qui interdira la réception de plusieurs messages identiques à un intervalle de temps trop court.

4.2.10. Les exploits

Un «exploit» est un programme qui «exploite» une vulnérabilité dans un logiciel spécifique. Chaque exploit est spécifique à une version d'une application car il permet d'en exploiter les failles.

4.2.11. Le Denial Of Service

Les attaques par «Denial Of service» (souvent abrégé en DoS, en français "Déni de service") consistent à paralyser temporairement (rendre indisponible pendant un temps donné) des serveurs afin qu'ils ne puissent être utilisés et consultés. Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à Internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur Internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information en l'empêchant de fonctionner.

4.3. Autres points concernant la sécurité informatique

4.3.1. Introduction aux cookies

Quels sont ces étranges gâteaux qu'un site Internet vous a sûrement déjà proposé? La plupart du temps un serveur vous propose de placer un cookie, vous ignorez ce terme et cliquez sur "OK" sans vous préoccuper de son devenir. Ce cookie est en fait un fichier qui est stocké sur votre disque et qui permettra que le serveur vous reconnaisse la prochaine fois que vous revenez sur le site de telle façon à connaître vos préférence (par exemple les options que vous aurez coché) pour vous éviter de les ressaisir.

Le problème de ces cookies est qu'ils contiennent des informations vous concernant. En effet, lorsque vous vous connectez à un site personnalisable, celui-ci va vous poser quelques questions afin de dresser votre profil, puis stocker ces données dans un cookie. Selon le site sur lequel vous vous connectez cela peut être à votre avantage ou non...

En effet, si vous vous connectez sur le site d'un magasin permettant d'acheter en ligne, il pourra, par le biais d'un questionnaire, connaître vos goûts et vous proposer des articles pouvant vous intéresser. Par exemple, en sachant si vous êtes un homme ou une femme il pourra vous aiguiller directement au rayon approprié pour vous faire économiser du temps (et surtout pour mieux vendre), et s'il sait que vous êtes amateur de tennis il vous proposera les derniers articles en la matière. En revanche, refusez de céder des informations sur vous à un site ne vous inspirant pas confiance... il n'a aucune raison de collecter des informations vous concernant.

En réalité un cookie n'a rien de dangereux en soi car c'est le navigateur qui le gère en écrivant des valeurs dans un fichier de type texte.

D'autre part, les données stockées dans un cookie sont envoyées par le serveur, ce qui signifie qu'il ne peut en aucun cas contenir des informations sur l'utilisateur que celui-ci n'a pas donné, ou en d'autres termes: le cookie ne peut pas collecter des informations sur le système de l'utilisateur.

Ces cookies sont généralement stockés dans un fichier cookies.txt. Vous pouvez par exemple le mettre en lecture seule pour ne plus être ennuyé par les serveurs vous les proposant.

4.3.2. Introduction aux processus

Dans un souci de modularité, Windows est architecturé en services (processus) fonctionnant en arrière-plan. Il est possible d'afficher la liste des processus en cours dans le gestionnaire des tâches en appuyant simultanément sur CTRL+ALT+Suppr, puis en cliquant sur l'onglet Processus. La fenêtre affiche alors la liste des processus en cours d'exécution et les ressources qui leur sont allouées.

Parmi ces processus un grand nombre sont des processus système faisant partie intégrante de Windows et certains correspondent à des applications tierces. Ainsi lorsque le système d'exploitation semble "ramer" il peut être intéressant de déterminer quel est le processus consommant le plus de ressources.

D'autre part la présence de vers, virus, chevaux de Troie, spywares, et AdWares sur le système est

généralement trahie par la présence de processus suspects, c'est la raison pour laquelle ils prennent souvent un nom proche d'un processus système réel afin de passer inaperçu (par exemple system32.exe au lieu de system32.dll, isass.exe au lieu de lsass.exe).

4.4. Derniers conseils

A l'heure actuelle, un antivirus n'est plus suffisant pour gérer les problèmes d'insécurité relatifs à Internet et l'informatique. Tout utilisateur qui veut naviguer avec un bon niveau de sécurité devra installer sur sa machine :

- Un antivirus ! (nous conseillons Antivir, gratuit)
- Un firewall ! (nous conseillons ZoneAlarm)
- Un logiciel antispam ou un logiciel de messagerie qui gère le spam, ou activer les options antispam du fournisseur de messagerie
- Un logiciel antispyware (nous conseillons Spybot Search&Destroy)

Microsoft a longtemps été critiqué pour la sécurité de ses produits. Avec Windoxs XP, Microsoft vous propose des solutions de sécurité de base sous forme de firewall et de mises à jour automatiques:

- Si vous ne possédez pas de firewall, vous pouvez utiliser celui de Windows XP. Il est toutefois extrêmement moins moins performant qu'un firewall professionnel, ou même moins que le firewall ZoneAlarm dans sa version non professionnelle (non payante).
- Tous les *x* jours, les mises à jour automatiques de Windows vous proposent des correctifs pour réparer les failles de sécurité de vos logiciels, des "Service Pack" pour mettre à jour certains logiciels, des outil de suppression de virus (qui ne remplacent pas un bon antivirus).

Il est utile de se tenir au courant des stratégies de sécurité proposées par Windows. Il est toutefois préférable de les renforcer par des solutions personnelles adaptées.

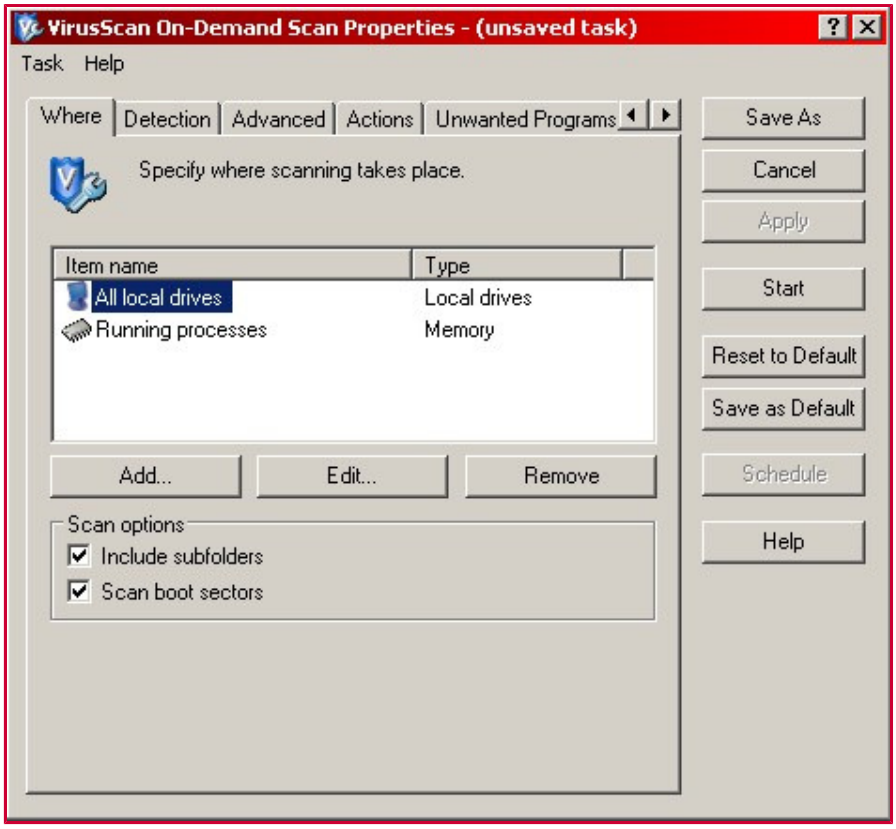
5. Virus et Antivirus.

Il est recommandé de *protéger la disquette en écriture* au moyen du taquet sur la *disquette* (cf les cassettes audio et vidéo). Si le taquet est ouvert, la machine n'enregistrera rien sur la *disquette* et n'y modifiera rien.

Il est possible de protéger la machine contre les *virus*. *l'Antivirus* installé en salle Renaissance est le VirusScan de McAfee.On lance VirusScan à partir du *bouton Démarrer*: En général il faut suivre Démarrer / Programmes / Network Associates / VirusScan - Analyse à la demande (*Start / Programs / Network Associates / VirusScan On-Demand Scan)*. La version de VirusScan que vous utilisez est déterminée par la commande A Propos De... (About...) du menu Aide (Help).

5.1. Utilisation de l'antivirus VirusScan 7.1.0. et 8.0.0.

Dans ce point 5.1., les commandes en anglais sont relatives à la version 7.1.0 et les commandes en français relatives à la version 8.0.0.

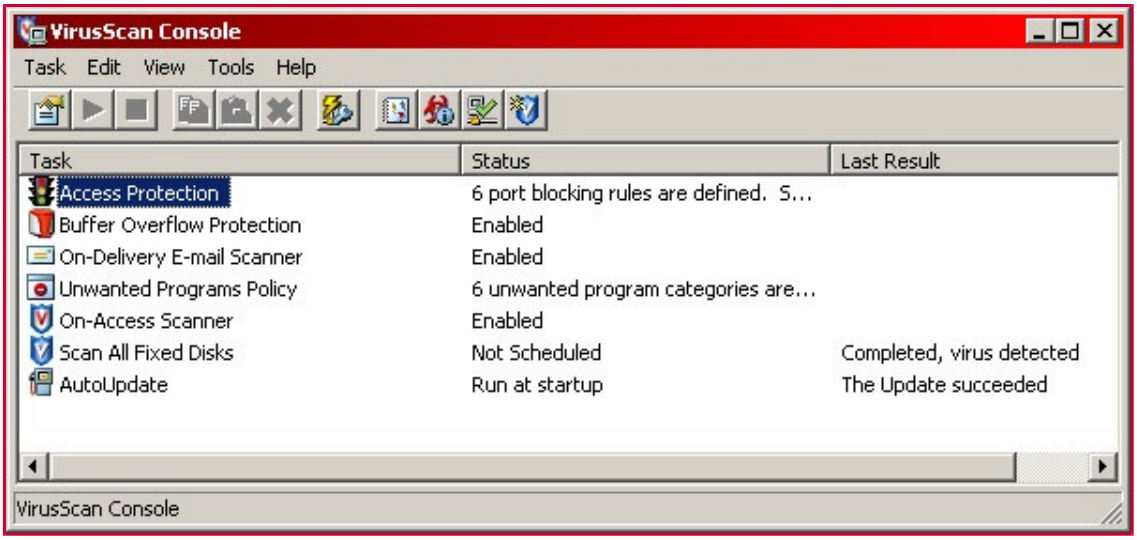


La fenêtre d'analyse à la demande propose les onglet décrits ci-dessous. Si vous avez lancé la VirusScan Console, vous pouvez obtenir la même fenêtre d'analyse en demandant une nouvelle tâche (Create New Task Scan), et en choisissant de scanner un disque ou un dossier particulier.

- L'onglet Emplacement (Where) spécifie ce qui est à scanner (Ajouter (Add)) et permet d'inclure les sous-dossiers. Pour cela on utilise la commande Ajouter (Add/Add Scan Item) et on choisit Lecteur ou Dossier (Drive Or Folder), puis on navigue (Parcourir (Browse)) jusqu'à la disquette (Floppy A:/) ou jusqu'à notre dossier. On peut supprimer (Remove) la tâche de scan des disques locaux (Tous les Disques Locaux (All Local Drives)) afin de gagner un peu de temps.
- L'onglet Détection (Detection) spécifie quels types de fichiers sont à scanner. Il est conseillé de scanner Tous Les Fichiers (All Files). Il existe une liste d'exclusions.
- L'onglet Avancé (Advanced) propose quelques options avancées.
- L'onglet Actions (Action) propose les actions réalisables lorsqu'un virus est trouvé. On conseille de Nettoyer Les Fichiers (Clean Infected File), ou alors de choisir d'Interroger l'Utilisateur (Prompt [User] For Action) qui permet de demander l'action à l'utilisateur au moment de sa découverte. Ces actions sont alors de nettoyer le fichier, ou de le déplacer ou le supprimer. Attention, si l'action par défaut est le déplacement (Move To), le dossier de destination est sans doute par défaut un dossier de quarantaine sur le disque C, et n'est donc pas accessible dans les salles informatiques. Choisissez un dossier de quarantaine sur le disque H, ou changez d'action.
- L'onglet Rapports (Report) propose la création d'un rapport (Consigner Dans Le Fichier (Log To File)) du scan et de la désinfection. Nous demandons de créer ce rapport dans notre dossier personnel (pas sur le disque c!), et de l'appeler <rapport_de_scan.txt>. Pour rappel, en salles Renaissance, le rapport ne peut être créé sur le disque C.
- Dans la version 8.0.0. du logiciel, il existe encore un onglet pour les Programmes Indésirables (Unwanted Programs), qui permet d'agir contre les logiciels espions, les logiciels publicitaires, les outils d'administration à distance, les numéroteurs, les crackers, les canulars, et les autres programmes potentiellement indésirables. Il est possible de rajouter soi-même des programmes à la liste.

Lorsque les options sont choisies, on lance le scan à partir du bouton Démarrer (Scan Now). Il faut attendre, parfois longtemps selon les options et le nombre de fichiers. Lorsque le scan est terminé, nous sommes informés du résultat dans une petite fenêtre, ou par le rapport inscrit dans le dossier sélectionné. On peut ensuite fermer le logiciel et le rapport.

La Console de VirusScan propose encore quelques options importantes (Start/Programs/Network Associates/Console VirusScan):



- Analyseur à l'Accès (On Access Scanner), le scan "transparent" de tous nos fichiers pendant que l'on travaille, accessible aussi à partir du bouclier dans le coin inférieur droit de l'écran.
- Mise à Jour Automatique (AutoUpdate), qui permet de mettre à jour la base de données des virus. A mettre à jour le plus souvent possible, car de nouveaux virus sont créés tous les jours.
- Analyser les Messages Electroniques à la Réception (On Delivery Email Scanner), pour scanner vos messages électroniques
- Analyser Tous les Disques Fixes (Scan All Fixed Disks), qui scanne tout les disques.
- Protections d'Accès (Access Protection), qui permet de bloquer le traffic réseau sur certains ports (fonction de type pare-feu).
- Le Buffer Overflow, qui empêche les applications d'exécuter du code arbitraire sur l'ordinateur.
- La Politique d'Action concernant les Programmes Indésirables (Unwanted Programs Policy), qui détermine la politique d'action concernant les éventuels logiciels espions, logiciels publicitaires, outils d'administration à distance, numéroteurs, crackers, et autres programmes indésirables.

D'habitude on peut ajouter d'autres tâches, comme scanner les dossiers particuliers de downloads, ou le lecteur de CD-Roms. En salle Informatique il est possible de créer une tâche sur demande (Analyse à la Demande (New On-Demand Scan Task)), mais celle-ci ne sera pas mémorisable pour une prochaine session (pour préserver les protections du réseau des salles Renaissance).

Il y a encore le bouton "rouge" qui ouvre la liste des virus traités par VirusScan. Liste assez intéressante pour se tenir au courant des ravages ou des protections contre les virus "à la mode".

5.2. Autres antivirus

VirusScan est un antivirus puissant, mais payant. L'Université en possède une licence pour son utilisation sur le domaine de l'ULB. D'autres antivirus existent, parfois en Français, parfois gratuits. La première partie de ce document vous indique en particulier comment télécharger AntiVir Personal Edition (gratuit) et comment l'installer.

S'il vous est impossible d'installer ou d'utiliser un logiciel antivirus sur une machine, il vous reste la possibilité d'utiliser un antivirus en ligne. Le site Secuser.com (www.secuser.com) est un site sur la sécurité sur Internet. Il vous donnera de nombreuses informations sur les virus, sur les hoax (canulars), sur les spywares (logiciels espions),... Dans le menu de ce site, vous trouverez un antivirus en ligne, et gratuit. Celui-ci ne demande pas d'installation, sinon celle d'un contrôle ActiveX qui devrait s'installer sans que vous ne le remarquiez.

Comme le précise le site, "cet antivirus en ligne ne remplace pas un antivirus installé en permanence sur votre ordinateur. Il constitue une aide d'appoint, mais n'est pas conçu pour protéger en temps réel votre système et empêcher notamment l'ouverture accidentelle d'un fichier contaminé".

6. Les archives et le compactage

En 2009, le compactage se fera à l'aide de la Framakey et du logiciel 7Zip. Vous trouverez un tutoriel de ce logiciel sur la Framakey, ainsi qu'en ligne sur le site www.campusb.fr/communaute/spipb873.html et une copie sur notre site de cours (rubrique "Tutoriels" dans le menu "Framakey").

7. Gravure

En 2009, la gravure se fera à l'aide de la Framakey et du logiciel InfraRecorder. Vous trouverez un tutoriel de ce logiciel sur la Framakey, ainsi qu'en ligne sur le site www.campusb.fr/communaute/spip429b.html et une copie sur notre site de cours (rubrique "Tutoriels" dans le menu "Framakey").

8. Les F.A.Q. relatives à Windows

1. question: Où peut-on trouver la matière d'examen? Y-a-t'il un syllabus? Sur quoi interroge-t-on à l'examen?

   problème: A l'examen, de nombreux étudiants ne parviennent pas à répondre à de nombreuses questions dont les solutions se trouvent dans nos "notes de cours".

   solution:
   - Un syllabus est disponible au Bespo pour en faire des photocopies. Attention, il y a un syllabus pour la filière gestion et un syllabus pour la filière communication. En outre, tous les documents de cours se trouvent sur le serveur des salles informatiques. Le disque Q (Data-Info128 ou un nom équivalent) vous est donc accessible pour copier sur disquettes ou clé. Chaque logiciel vu au cours y est représenté par un dossier. N'oubliez pas de copier les fichiers images (Jpeg, Gif, ...) pour la bonne lisibilité de ces notes. Ces notes contiennent le minimum à connaître à l'examen. Ces informations sont aussi sur notre site Web à l'adresse www.ulb.ac.be/soco/matsch/info-d-203 .

2. question: J'ai travaillé sur mon sujet à la maison. En revenant travailler à l'université, pourquoi le logiciel ne veut-il pas ouvrir le fichier?

   problème: Ayant été partiellement faits à domicile, de nombreux travaux se retrouvent "illisibles" lorsqu'ils sont continués en salles informatiques. Il s'agit d'un problème de compatibilité de versions entre logiciels. Ceci ne devrait pas se produire avec les travaux de la filière communication réalisés avec Etomite.

   solution: Il existe de nombreuses versions de Windows (Windows 95, 98, NT, Millennium, 2000, XP,...). Chaque logiciel se retrouve aussi sous différentes versions (par exemple PowerPoint 97, PowerPoint 2000, PowerPoint 2003) Et il y a encore une différence dans la langue (version française ou version anglaise, ou autre). La seule solution qui assure qu'il n'y aura pas de problème de compatibilité est de faire le travail sous une unique version: Access 2003 ou PowerPoint 2003 sur Windows 2000 Professionnal en version anglaise.

3. question: Mon ordinateur s'est planté, et j'ai dû le redémarrer. Comment récupérer les données sur lesquelles je travaillais?

   problème: Lorsque l'ordinateur redémarre, la mémoire vive se vide, et perd les données du travail qui était en cours.

   solution: Si aucune copie de sauvegarde n'a été faite, il n'y a pas de solution. Les "plantages" sont imprévisibles. Il est impératif de sauvegarder l'objet sur lequel on travaille aussi souvent que possible. Grâce à la sauvegarde régulière, on minimisera le nombre de données perdues.

4. question: Pourquoi l'ordinateur me refuse-t-il l'accès aux données qui étaient sur ma disquette?

   problème: La disquette est un support fragile dont la destruction peut-être due à divers facteurs:

   - On a travaillé sur la disquette, ce qui nécéssite de nombreux transferts de données entre le disque dur et le disque volatil. La disquette ne supporte pas l'effort et s'abîme;
   - On a sorti la disquette alors que le voyant vert du lecteur était encore allumé, ce qui interrompt le transfert de données de manière très brutale. La disquette ne supporte pas le coup et s'abîme;
   - On a laissé la disquette au chaud, au froid, près du téléphone portable ou d'un baffle, elle a été mouillée, elle a traîné dans un endroit poussiéreux, on a joué avec son mécanisme de ressort, ...

   solution: Certains logiciels (Scandisk, Norton, ... non-disponibles en salle informatique) permettent de réparer, en partie et occasionnellement, des disquettes abîmées. Si on parvient à récupérer des données, il est conseillé de se débarrasser très vite de la disquette qui risque de voir le problème se reproduire très vite.

- La disquette n'est qu'un moyen de transport de données. On ne travaille pas dessus.
- Attendez toujours que les opérations avec la disquette soient terminées, c'est-à-dire que le voyant vert s'éteigne.
- Rangez la disquette loin du radiateur, de liquides, du téléphone, ... Ne jouez pas avec le ressort de la protection plastique.

Aujourd'hui, on trouve facilement des clés USB de grande capacité pour de faible prix. A condition de bien "éjecter" votre clé USB, les problèmes rencontrés avec les disquettes ne devraient pas vous arriver avec une clé.

5. question: Comment faire lorsque rien ne sort de l'imprimante?

   problème: Vous avez envoyé un document à l'imprimante, et rien ne se passe...

   solution:

   - La bonne réponse est de chercher pourquoi rien ne s'est passé et résoudre le problème. La mauvaise réponse est de relancer l'impression en espérant que cela marche. Certains utilisateurs continuent d'envoyer leur travaux en espérant qu'ils seront finalement imprimés. Le résulat est plutôt gênant quand quelqu'un résout finalement le problème (imprimante éteinte, bourrage papier, cable débranché, ...) et regarde 20 versions du même travail s'imprimer.

   - En salle Renaissance, il est possible aussi que votre travail soit imprimé sur une imprimante d'une autre salle. Pour contrôler votre impression, ne cliquez pas sur le bouton représentant l'imprimante, mais passer par les menus: Fichier/Imprimer (File/Print), et choissisez l'imprimante de votre salle.