# Protéger son ordinateur

Par jean jacques Pellé


# Sommaire

# 1. Introduction

Protéger son ordinateur est absolument indispensable.
Il ne faut pas le protéger uniquement contre les virus. D'autres dangers le guettent.

- La fragmentation des fichiers, qui en quelque temps vont faire ralentir énormément la vitesse d'exécution de votre machine
- Les fichiers temporaires qui ne s'effacent pas et finissent par saturer votre disque.
- Les cookies qui s'accumulent.
- Les messages non effacés des messageries internes.
- Les espions qui s'installent au fur et à mesure que vous naviguez sur internet.

Il faut tout mettre en œuvre pour protéger votre machine. Un ordinateur non nettoyé est un ordinateur mort ....à brève échéance ! Sans compter les désagréments d'une machine qui rame et qu'on a envie de passer par la fenêtre.
En suivant les conseils qui vont suivre, vous avez toutes les chances de limiter au maximum un gros problème. J'ai une machine qui date de 2002. Elle pédale aussi rapidement qu'un ordinateur moderne car il est nettoyé en permanence.
Je reconnais qu'on n'a pas toujours le temps de se mettre sur son ordinateur, mais en prenant un peu de temps toutes les semaines on gagnera du temps et de l'argent (pas besoin de ramener la machine chez le marchand pour dépannage).
On peut lancer les anti- espions et antivirus pendant le repas ou pendant la nuit !

# 2. Les Malwares

## *2.1- Définition du Malware :*

***Malware : Nom désignant de manière générale les programmes non sollicités tels que les virus, les vers, les chevaux de Troie.**

### 2.1.1 Les virus

***Programme généralement de petite ou très petite taille possédant la propriété d'infecter, de se multiplier, possédant une fonction nocive.***

La fonction d'infection permet au virus de s'introduire dans des fichiers de programme, dans des fichiers de données utilisant un langage de script, ou dans une partie de la disquette ou du disque dur contenant un petit programme (secteur de démarrage). Lors de l'accès à ces programmes ou secteur, le code du virus s'exécutera de façon d'abord silencieuse (phase de multiplication pendant laquelle il infectera d'autres fichiers) puis visible (activation de la fonction nocive).

La fonction nocive pourra être déclenchée par des facteurs très variables selon le virus (au bout de n réplications, à une date fixe, lors de l'exécution de certaines tâches précises...). Elle peut se limiter à l'affichage d'un message agaçant ou, plus généralement, conduire à des perturbations graves de l'ordinateur (ralentissement du fonctionnement, effacement ou corruption de fichiers, formatage du disque dur...). Les virus sont donc des programmes parasites qui doivent être hébergés dans d'autres fichiers (ou secteur exécutable du disque). On emploie souvent de façon impropre le mot virus pour désigner d'autres programmes nocifs (malwares), en particulier les vers.

### 2.1.2 Les vers

***En informatique un ver est un programme nocif qui diffère des virus par plusieurs points.***

Tout d'abord le ver est un programme autonome qu'on peut retrouver sur le disque dur, contrairement aux virus qui se dissimulent comme des parasites dans des fichiers ou dans le code exécutable contenu dans le secteur de démarrage du disque. Toutefois quelques très rares vers ne s'enregistrent pas sur le disque et subsistent uniquement en mémoire).
Un ver peut arriver directement par le réseau en profitant d'un port ouvert, **mais la méthode la plus classique consiste à s'introduire sous la forme d'une pièce jointe attachée à un mail.**

- Certains s'exécutent alors directement à la simple lecture du mail (en particulier si le système de l'ordinateur n'a pas été mis à jour).
- La plupart du temps il faut cliquer sur la pièce jointe pour que le ver s'exécute.

Un ver ne se multiplie pas localement, contrairement aux virus mais sa méthode la plus habituelle de propagation consiste à s'envoyer dans des mails générés automatiquement.
Ces mails sont expédiés à l'insu de l'utilisateur vers diverses adresses.

Ces adresses sont généralement prélevées par le ver dans les fichiers présents sur le disque (en particulier le carnet d'adresse), ou bien il s'agit d'adresses construites de façon semi aléatoires.
**Les vers installent généralement sur l'ordinateur d'autres programmes nocifs : spywares, keyloggers, backdoors (portes dérobées), chevaux de Troie**.
**Ces programmes peuvent être exploités pour espionner votre activité, capturer des mots de passe ou numéros de carte bancaire, ou prendre le contrôle de l'ordinateur à distance pour le transformer en PC zombie**.

Un tel PC peut être utilisé comme relais pour des attaques par déni de service ou pour l'envoi en masse de **spams**. De façon erronée le public, et même certains articles spécialisés, utilisent le terme de virus pour désigner ces malwares.

### 2.1.3 Les spywares

#### *2.1.3.1 Définition*

**Le terme *logiciel espion* est tiré de l'anglais *spyware : Spy (espion) et Software (logiciel).* .**
**On parle également de mouchard ou, plus rarement, d'espiogiciel équivalent français de Spyware.**

Les logiciels espions sont souvent inclus dans des logiciels gratuits et s'installent généralement à l'insu de l'utilisateur.
Les logiciels espions ne sont généralement actifs qu'après redémarrage de l'ordinateur.
Certains, comme Gator, sont furtifs et ne se retrouvent donc pas dans la table des processus (accès : « Ctrl+alt+suppr »).
Un logiciel anti-espion performant peut toutefois les détecter et envoie une alerte avant leur installation.

Le logiciel espion peut afficher des offres publicitaires, télécharger un virus, installer un cheval de Troie (ce que fait *WhenU.SaveNow*, par exemple), capturer des mots de passe en enregistrant les touches pressées au clavier (*keyloggers*), espionner les programmes exécutés à telle ou telle heure, ou encore espionner les sites Internet visités.

#### *2.1.3.2 Les principaux vecteurs d'infections*

**- les logiciels de cassage de protection type cracks et keygens ;**
**- les faux codecs ;**
**- les logiciels gratuits ;**
**- les faux logiciels de sécurité ;**
**- la navigation sur des sites à haut risque d'infections ;**
**- les pièces jointes et les vers par messagerie instantanée.**

#### *2.1.3.3 Prévention*

Avant d'installer un logiciel téléchargé, soyez sûr d'avoir installé un programme anti-virus et anti-espiogiciel. Pour plus de sécurité, prenez quelques renseignements complémentaires en faisant une recherche d'avis d'utilisateurs qui signalent parfois les menaces cachées de certains programmes.

**L'utilisation des logiciels libres est un bon moyen de lutter contre les logiciels espions, car les sources de ces logiciels sont disponibles, vérifiables et modifiables, ce qui permet la détection et l'élimination de logiciels espions de ces programmes. Dans les logiciels non libres, comme les sources ne sont pas disponibles, il est plus difficile de détecter la présence de ce genre de menace et impossible de l'éliminer.**

Enfin, attention aux pièges. Dans le passé, certains programmes soi-disant destinés à lutter contre les logiciels espions contenaient eux-mêmes ce type de menace ou bien se révélaient totalement inefficaces avec pour seul but de facturer une licence d'utilisation (**cas de Spyware Assassin par exemple**)

## 2.1.4 Les chevaux de Troie

### *2.1.4.1 Définition*

Un **cheval de Troie** est un logiciel d'apparence légitime conçu pour exécuter subrepticement (de façon cachée) des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

### *2.1.4.2 Fonctionnement*

Un cheval de Troie n'est pas un virus informatique, en ce sens qu'il ne se reproduit pas par lui-même, fonction essentielle pour qu'un logiciel puisse être considéré comme un virus. Un cheval de Troie est conçu pour être reproduit lors de téléchargements ou de copies par des utilisateurs, attirés par les fonctionnalités du programme.

Les chevaux de Troie servent très fréquemment à introduire une porte dérobée sur un ordinateur. L'action nuisible à l'utilisateur est alors le fait qu'un pirate informatique peut à tout moment prendre à distance (par Internet) le contrôle de l'ordinateur.

Un cheval de Troie se compose de deux parties distinctes : la partie "client" et la partie "serveur". La partie serveur est le composant envoyé à la victime tandis que la partie client reste sur l'ordinateur du pirate. La partie serveur est envoyée par courriel et se présente sous la forme d'une amélioration d'un logiciel (ex : MSN, Adobe Photoshop, Safari ...). Il peut aussi se présenter sous la forme d'un test de QI ou d'un jeu à but lucratif. Bref, les formes sont multiples. Attention, dites-vous bien que jamais une entreprise de micro-informatique ne proposera des améliorations par courriel. Le cheval de Troie se glisse donc dans l'ordinateur et s'installe dans l'éditeur de registre (pour aller le voir tapez "Regedit" dans *Exécuter* du menu Démarrer, vous comprendrez mieux pourquoi). Le fichier peut également s'infiltrer et s'installer dans l'autoexec de démarrage, afin d'être opérationnel dès le lancement de la machine. Là, il ouvre une porte dérobée (backdoor en anglais), sur le port choisi par le pirate de l'ordinateur et établit une connexion avec l'ordinateur pirate. La partie serveur, elle, s'occupe d'envoyer les instructions à la partie client logée dans l'ordinateur de la victime. Le pirate peut alors contrôler la totalité du PC (il peut contrôler la souris, le clavier mais aussi imprimer, initialiser le disque dur, activer une webcam, etc.).

**Il existe deux types de chevaux de Troie :**

- ceux en connexion directe, de moins en moins utilisés, où c'est le pirate qui se connecte à la victime, mais où il faut que le pirate dispose de l'adresse IP de sa victime.

- ceux en *remote connection* où c'est l'ordinateur victime qui se connecte au pirate. Le pirate, lui, possède une liste où chacune de ses victimes connectées est affichée. Il peut ainsi diffuser son cheval de Troie à grande échelle.

## *2.2. Les logiciels antimalwares*

### 2.2.1 Quelques antivirus gratuits.

Il existe un très grand nombre d'antivirus sur le marché. Parmi ceux-ci, on en trouve des gratuits de très bonne qualité.
Il existe souvent deux versions. La version payante et la gratuite qui malgré tout protège bien notre machine.
Parmi ceux-ci :

**AVAST** de la société AVAST Software (anciennement *Alwil Software*) située à Prague en République tchèque
**ANTIVIR** de la société AVIRA société allemande spécialisée dans la sécurité informatique
**AVG** développé par la société tchèque Grisoft
**BIT DEFENDER** de l'éditeur SOFTWIN, basé en Roumanie
F SECURE de **F-Secure** Corporation est une société finlandaise spécialisée dans la sécurité informatique.
**KASPERSKY** (anciennement AntiViral Toolkit Pro ou AVP) est un antivirus créé par la société russe Kaspersky Lab

**Je privilégie AVAST qui est parmi les plus réputés.**
**Ce qu'il faut savoir, c'est le seul antivirus gratuit qui scan le secteur d'amorçage (démarrage de l'ordinateur)**

#### *2.2.1.1 Utilisation d'un antivirus.*

Les antivirus scannent ce qui rentre dans votre ordinateur. Vos téléchargements, les messages… mais ils ne voient pas forcément passer un virus caché dans un programme et qui ne s'est pas encore développé.

**C'est pourquoi il faut régulièrement effectuer un scan à la demande autrement dit, il faut lancer votre antivirus de temps en temps Afin qu'il scanne l'ensemble de vos fichiers et programmes.**

**Je dirais :**

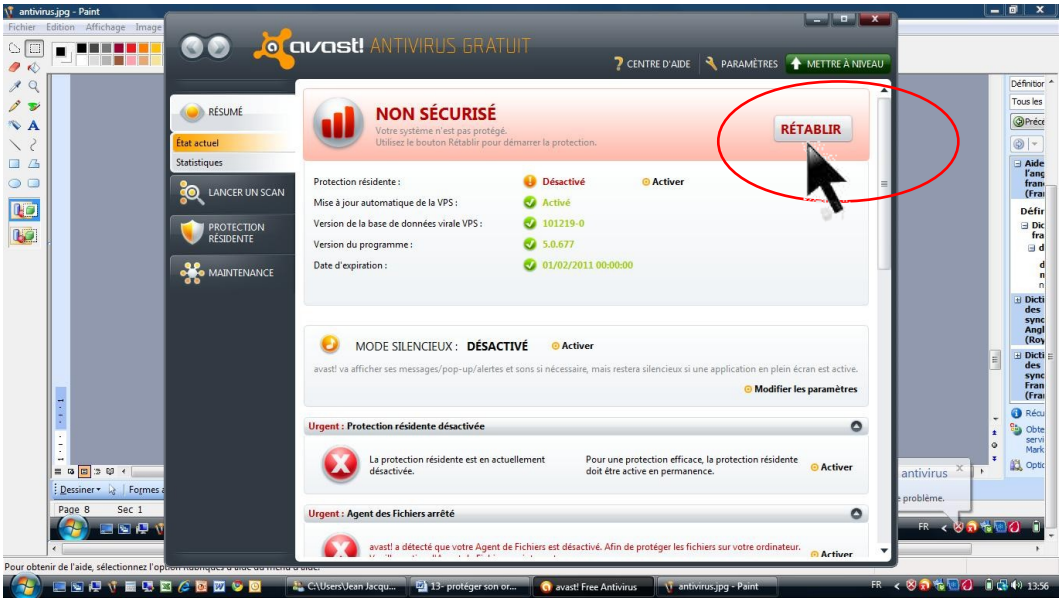
**- Environ tous les mois**
**- Si je détecte un comportement suspect de mon ordinateur (fonctionnement inhabituel)**

### *2.2.1.2 Etat de l'antivirus*

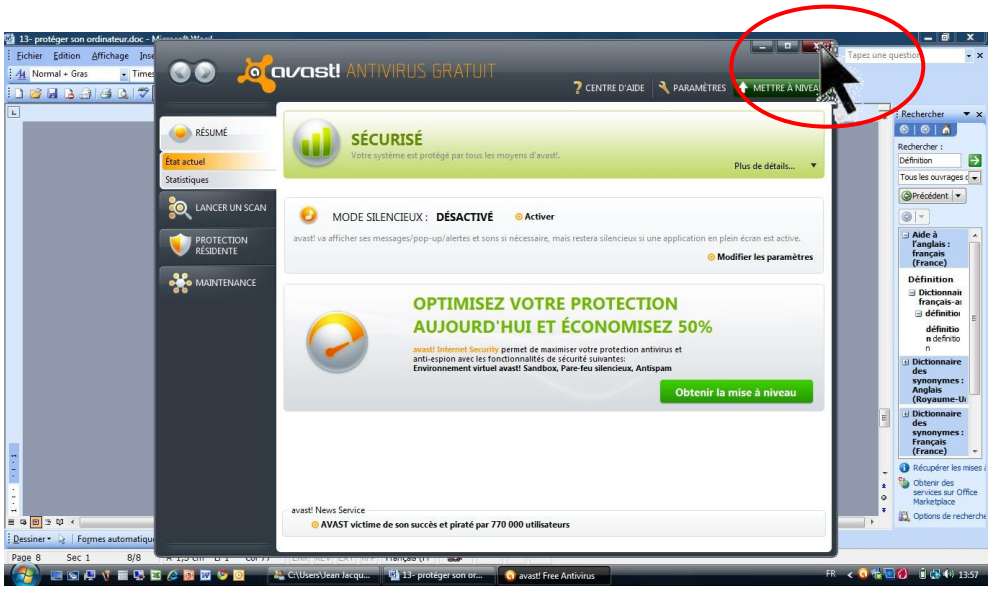
On sait qu'un antivirus est actif par son icone dans la barre de notification (partie droite de la barre des tâches).
Si celui-ci est désactivé, il est indiqué par une croix pour Avast, par le parapluie fermé dans l'icône pour **Antivir** par exemple.


On peut être obligé de le désactiver quelques fois pour installer certains programmes.

Pour le désactiver ou le réactiver, cliquer sur l'icône de la barre de notification afin d'ouvrir la fenêtre suivante.




Pour l'exemple d'Avast, cliquer sur le bouton « **RETABLIR** »



La fenêtre ci-dessus c'est affichée. Ne pas cliquer sur le bouton vert obtenir la mise à jour, il n'a pour but que de vous faire acheter la version payante.
Fermez tout simplement la fenêtre en cliquant sur la croix en haut à droite de celle-ci .

### *2.2.1.3 Précaution lors de l'installation d'un nouvel anti virus*

Avant d'installer un nouvel antivirus, prenez bien la précaution de supprimer l'ancien avant.
**L'activation simultanée de deux antivirus peut générer le blocage de l'ordinateur.**

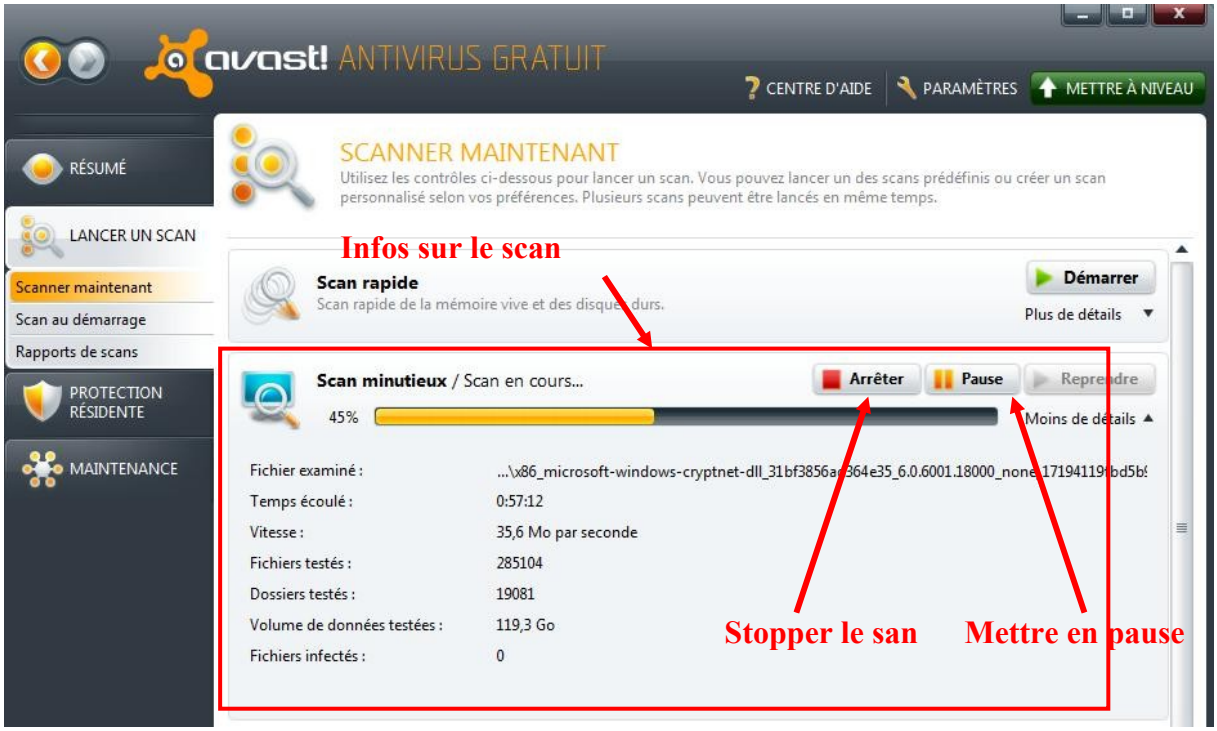
### *2.2.1.4 Mise en route d'un scan à la demande*

Je vous conseille de le faire au moins une fois par mois cela vous évitera bien des déboires.
Nous allons lancer la nouvelle version de AVAST par exemple (l'ancienne version se présente sous forme d'une face avant d'un autoradio).
Au cas ou vous possédiez cette ancienne version, je vous conseille de vous mettre à jour et installer la nouvelle.

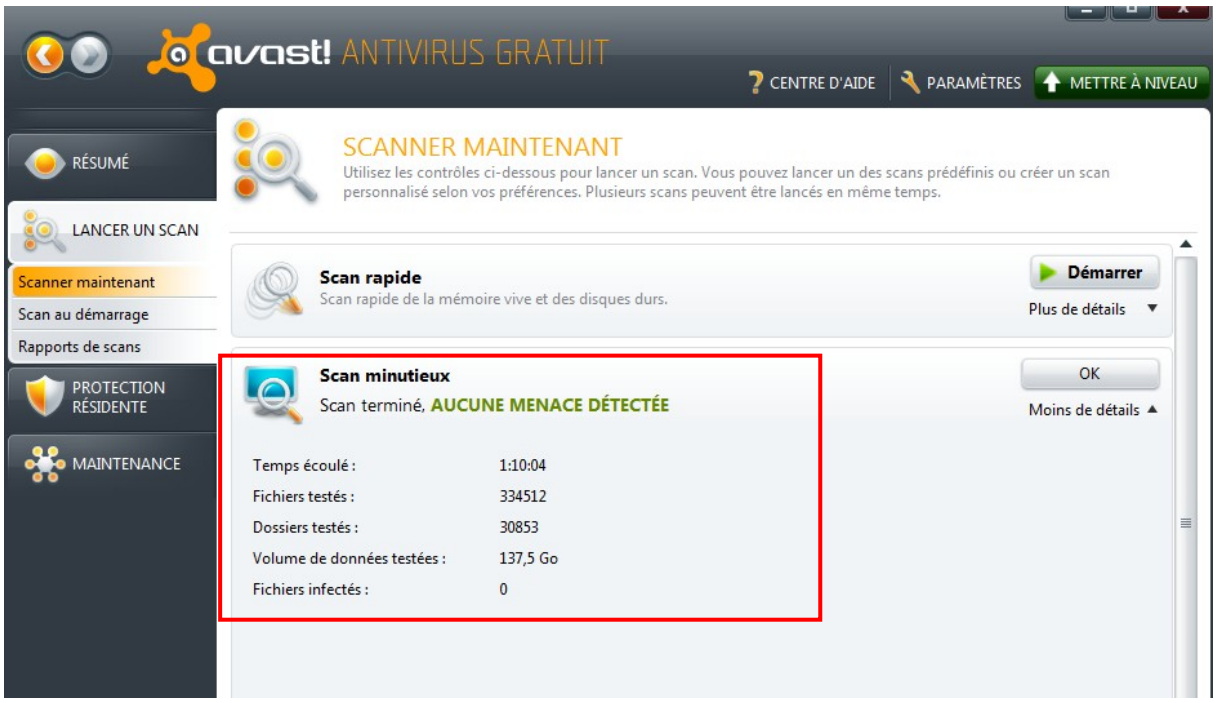
1- Cliquer sur l'**icône** se trouvant dans votre barre de notification ou celle se trouvant sur votre bureau pour l'ouvrir puis cliquer sur « **Lancer un scan** » à droite de la fenêtre.


Cliquer sur le bouton « **Démarrer** » du **scan minutieux**

Un scan minutieux va demander plusieurs heures, mais il est nécessaire. Vous pouvez le lancer pendant que vous faites autre chose. Un petit inconvénient d'Avast, il faut être présent car en cas de détection d'un virus, il alarme et on doit valider immédiatement sa suppression pour qu'il continue son scan.
On peut l'arrêter à tout moment ou le mettre en pause.




**Une heure et dix minutes plus tard :**
Aucune menace détectée, grâce à des scans souvent répétés.
A savoir que je télécharge énormément, testant toutes sortes de programmes gratuits ou en shareware*.



### 2.2.2 Quelques logiciels  anti-espions gratuits

- **Ad-Aware** :

  **Gratuiciel*** développé par la société suédoise Lavasoft spécialisé dans la suppression des adware. Il existe une version payante plus sophistiquée.

**J'émets des réserves sur ce logiciel qui nous a apporté des soucis. Il empêchait régulièrement l'antivirus de scanner et nous laissait passer des espions.**

- **Spybot - Search & Destroy** :
  Un logiciel gratuit qui permet également de supprimer les autres traceurs d'activité sur le système (fichiers journaux)

- **HijackThis :**
  Ce logiciel permet de détecter et de détruire tous les processus en cours de fonctionnement sur votre ordinateur.C'est un logiciel anti-espion pour les systèmes d'exploitation Microsoft Windows dont les droits appartiennent à Trend Micro

- **Spyware Terminator** :
  Détecte les **espiogiciels***, mais aussi des chevaux de Troie et d'autres maliciels. Il permet aussi une surveillance des services Windows, pour empêcher les modifications que vous ne voulez pas autoriser, contre les **rootkits*** par exemple.

- **Malwarebytes' Anti-Malware**

  C'est un logiciel antivirus pour la famille de systèmes d'exploitation Windows de Microsoft.Il permet de détecter et supprimer différents types de logiciels malveillants sur un ordinateur.

**Je vous conseille d'installer Malwarebytes et Spyware Terminator qui sont complémentaires excellents**

**Nota : description  de nouveau mots qui apparaissent avec l'évolution de l'informatique et qui ont pour but de franciser les termes anglais.**

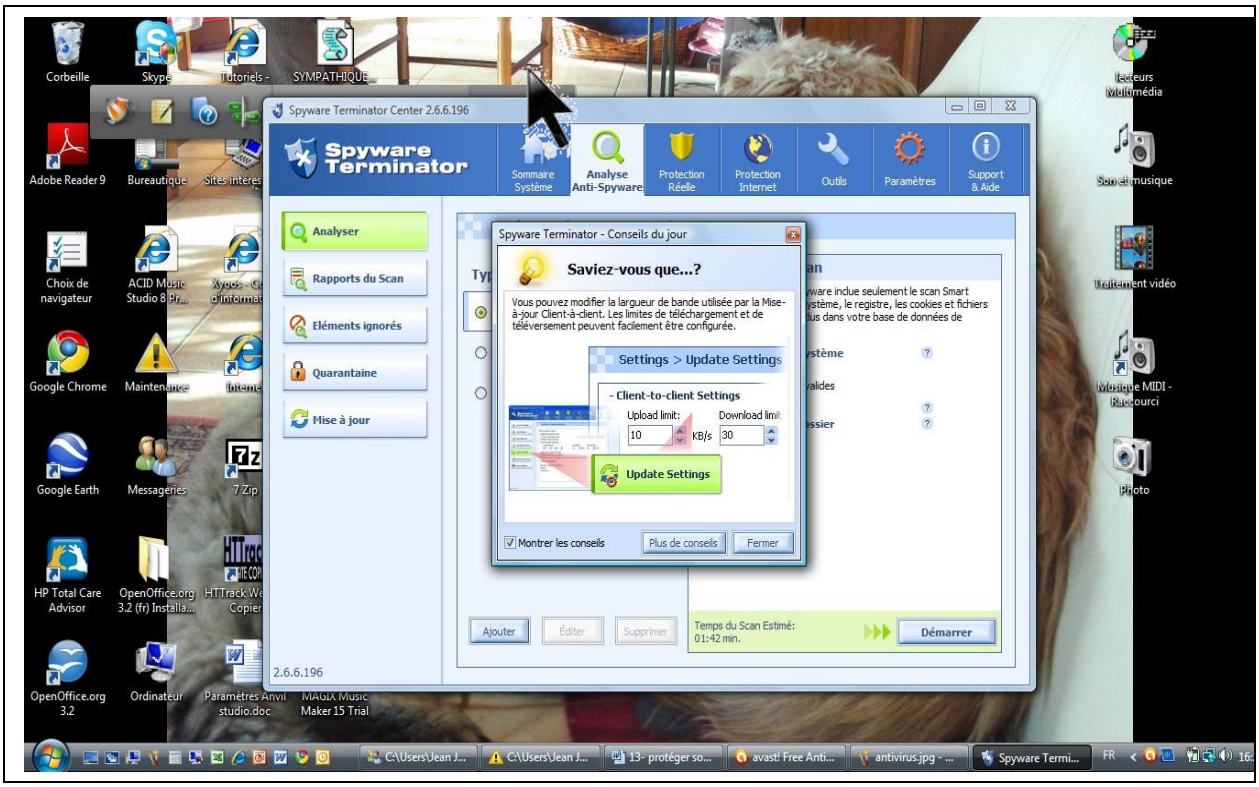
**Espiogiciels :** (spyware en anglais) ou logiciel espion.
**Gratuiciel :** (**freeware** en anglais), ou **logiciel gratuit** est un logiciel mis gratuitement à disposition par son créateur

**Partagiciel :** (shareware en anglais), logiciel propriétaire, subordonné au droit d'auteur, qui peut être utilisé gratuitement généralement durant une certaine période ou avec des fonctionnalités limitées. Après cette période de gratuité, l'utilisateur peut rétribuer l'auteur s'il veut continuer à utiliser le logiciel ou avoir accès à la version complète.

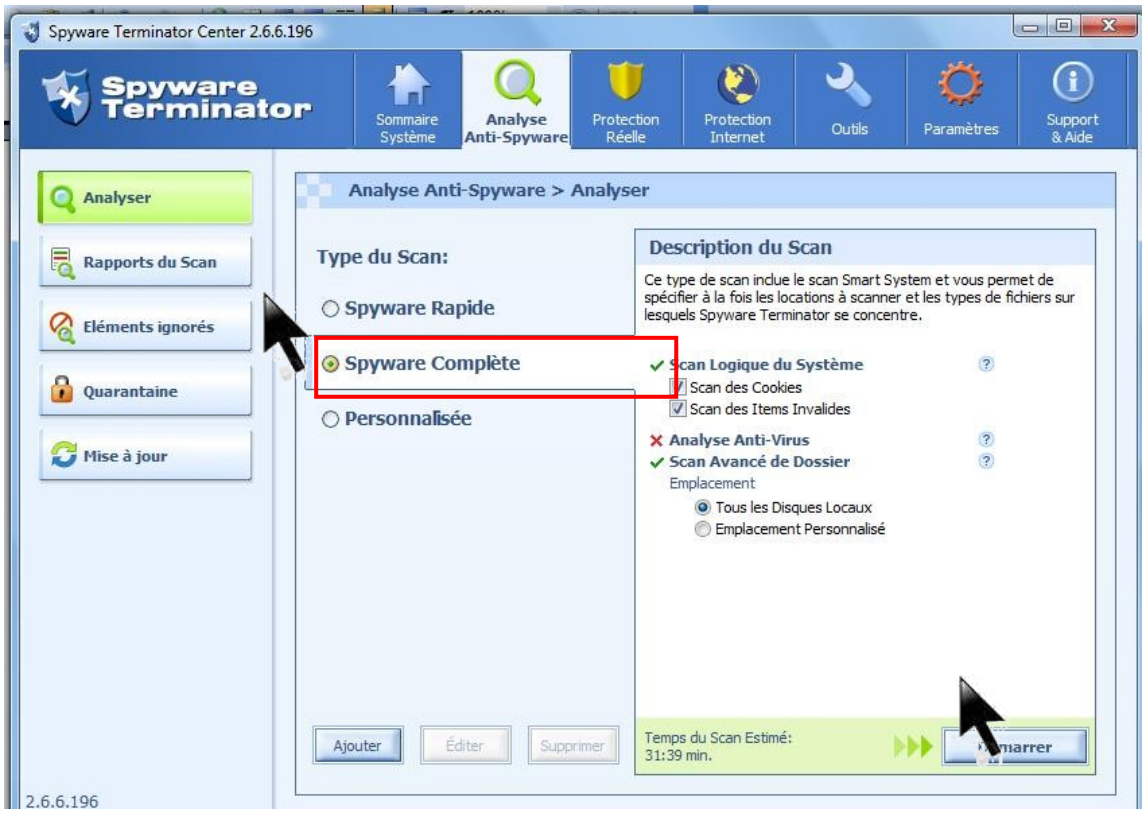
**Rootkit :** (en français : « outil de dissimulation d'activité »), parfois simplement « kit », est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible, à la différence des autres logiciels malveillants.
Le terme peut désigner la technique de dissimulation ou, par métonymie, un ensemble particulier d'objets informatiques mettant en œuvre cette technique.

### *2.2.2.1 Utilisation de Spyware Terminator.*

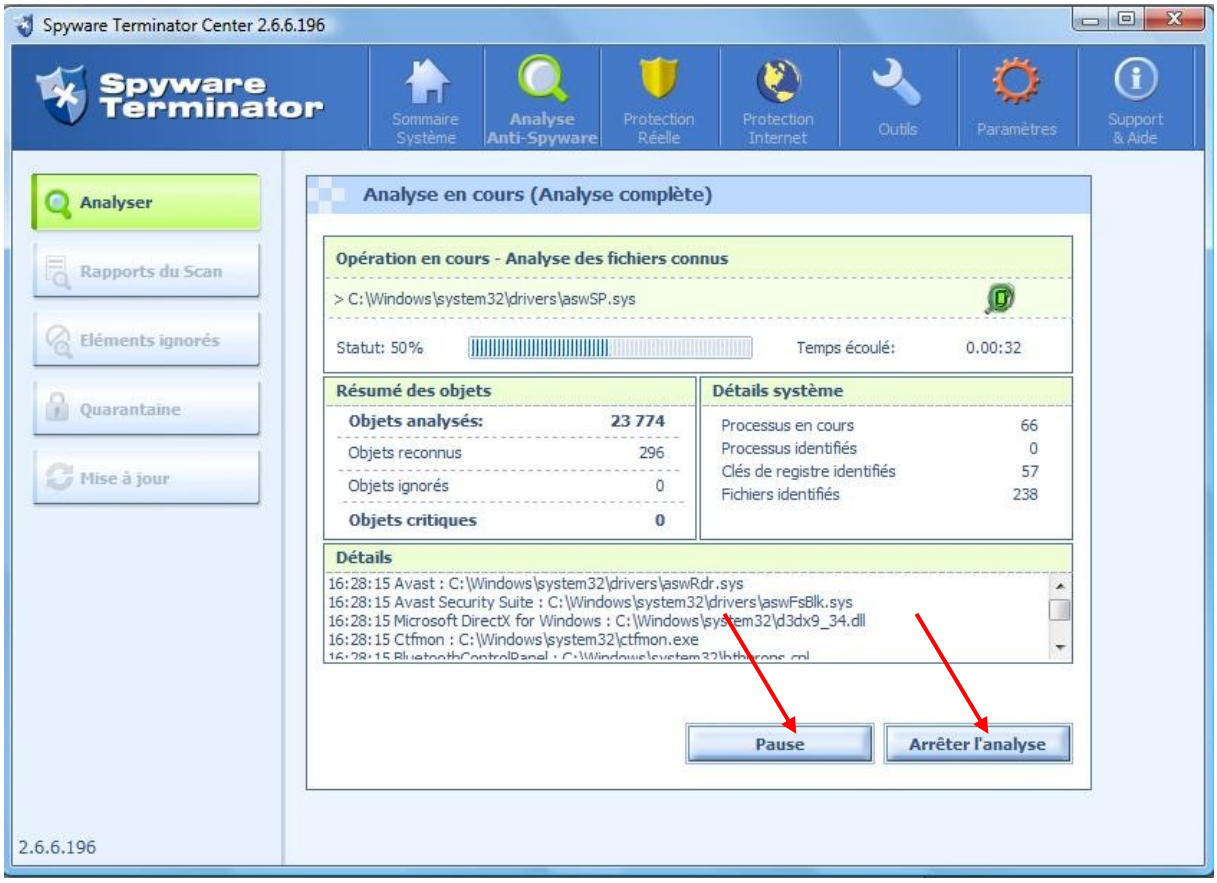
Cliquer sur l'icône du programme pour l'ouvrir (après l'avoir installé bien entendu).
Cliquer sur l'option « **Analyse Anti Spyware** »
Un écran conseil du jour s'affiche, on a le choix entre le lire ou fermer la fenêtre en cliquant sur la petite croix en haut à droite



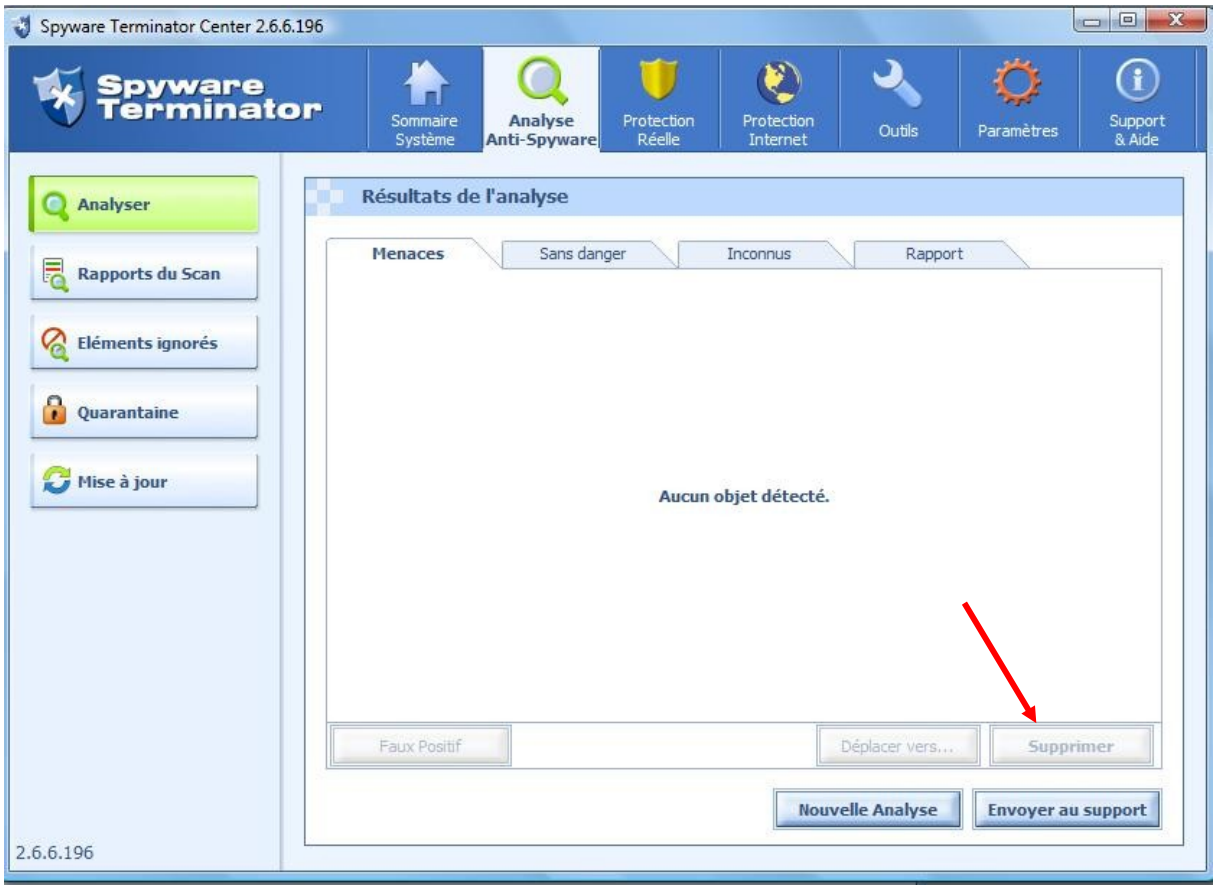

Cliquer sur Spyware complète afin de faire une analyse totale (conseillé) puis sur le bouton démarrer



L'analyse démarre, vous pouvez suivre son évolution grâce à l'écran suivant qui reste affiché
On peut mettre en pause le programme ou l'arrêter à tout moment

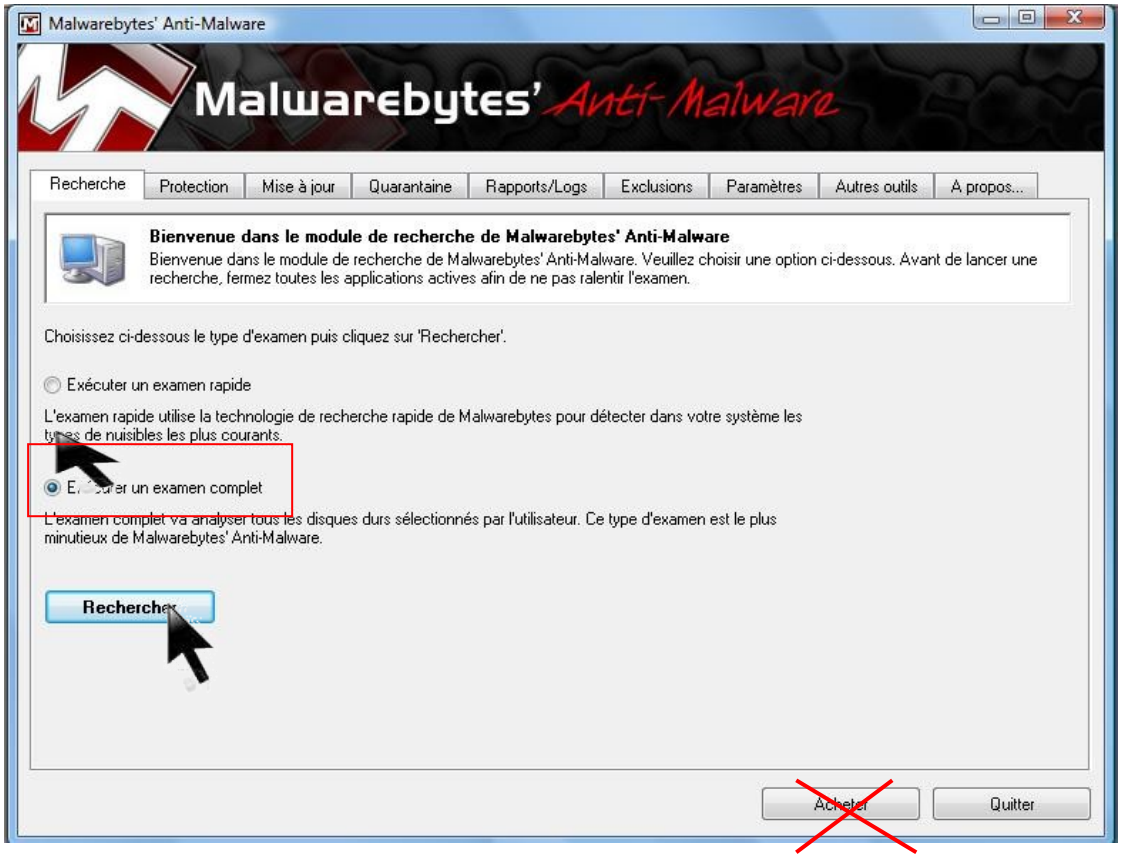



Résultat à la fin de l'analyse. En cas de spyware trouvé, cliquer sur le bouton supprimer
La durée à été d'environ 12 mn

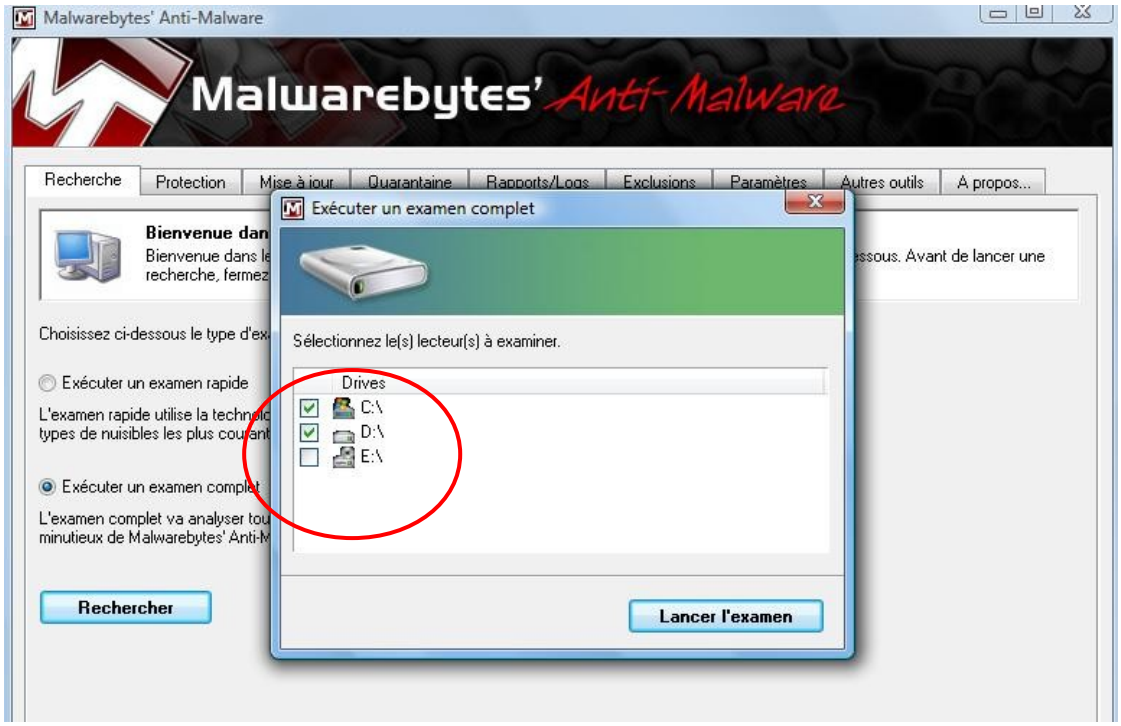


### *2.2.2.2 Utilisation de Malwarebytes*

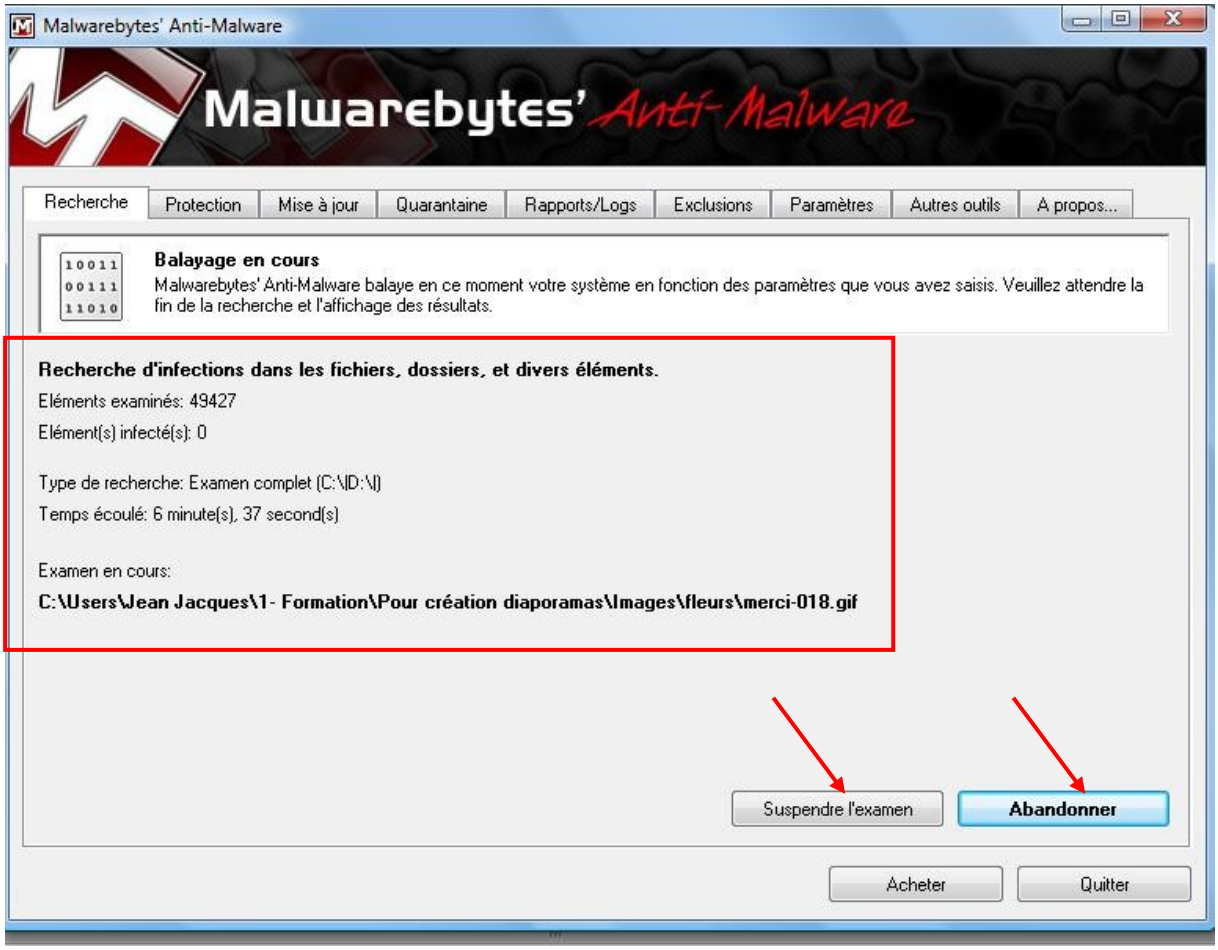
Cliquer sur l'icône du programme (après l'avoir installé bien entendu).
Ne pas tenir compte du bouton « Acheter », c'est uniquement si vous désirez acheter la version payante, mais la version gratuite est très suffisante surtout lorsqu'elle est complètée de spyware Terminator.
Cliquer sur « **Exécuter un examen complet** » puis sur le bouton « **Rechercher** »



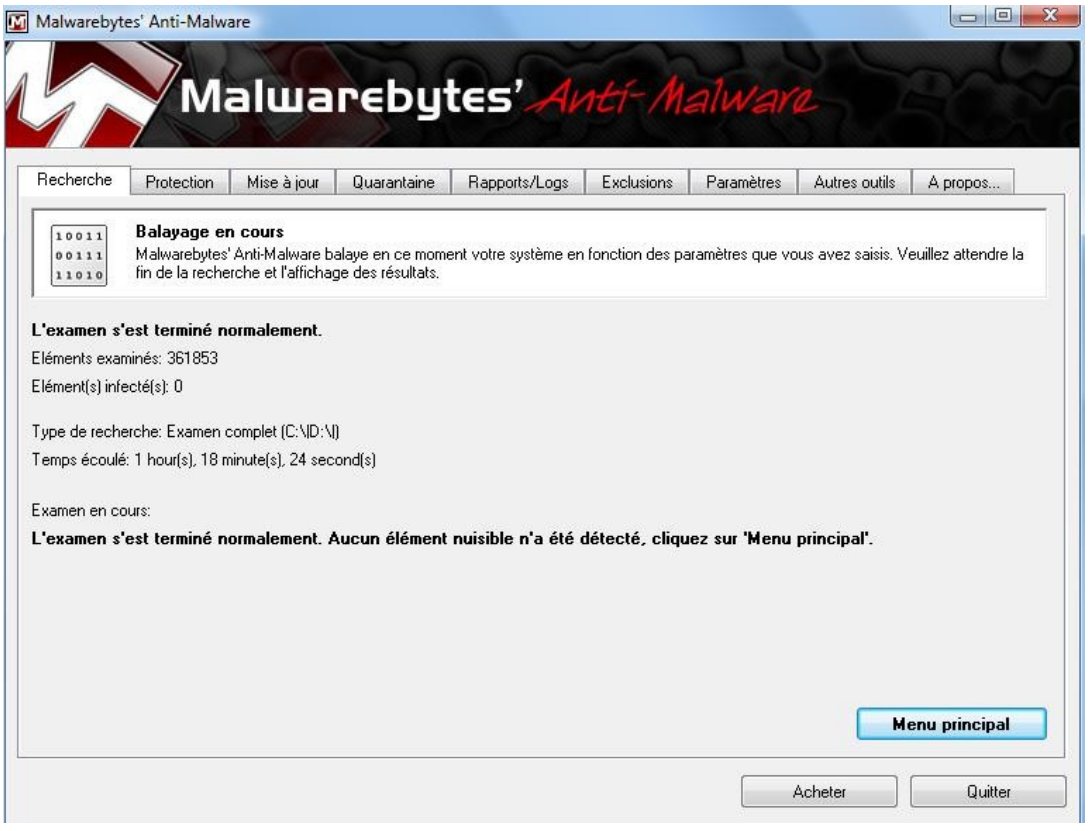

Une fenêtre s'affiche permettant de choisir les disques à scanner



Je choisis mes deux disques dures « C et D »  puis je clique sur « **Lancer l'examen** » et le scan démarre. Comme pour les autres programmes anti Malwares, vous pouvez suivre l'évolution du scan, Le stopper ou le suspendre




**Analyse terminée, le mois dernier il m'a trouvé trois spywares.**



# 3. CCleaner, un programme de nettoyage efficace

## *3.1. Introduction*

**CCleaner** (abréviation de *Crap Cleaner*) est un graticiel (*freeware*) permettant d'optimiser le fonctionnement d'un ordinateur muni du système d'exploitation Windows et de protéger la vie privée des utilisateurs de l'ordinateur. Il supprime les fichiers et les enregistrements inutiles, ce qui permet à l'ordinateur de fonctionner plus rapidement et libère de l'espace sur le disque dur. Il efface aussi les traces de navigation sur Internet et certaines traces d'accès aux fichiers de l'ordinateur, ce qui protège la vie privée des utilisateurs de l'ordinateur.

**CCleaner** supprime les fichiers temporaires, les Cookies, les historiques des navigations dans internet, les adresses internet tapées récemment ; les fichiers temporaire de windows, les vieux fichiers du préfecht, il vide la corbeille…….

### 3.1.1Les fichiers temporaires internet

Les **fichiers Internet temporaires** sont les fichiers contenus dans le dossier **Temporary Internet Files** du système d'exploitation Windows. Ce dossier est utilisé par Internet Explorer comme mémoire cache pour les pages web visitées par l'utilisateur. Cette mémoire cache permet à Internet Explorer d'afficher plus rapidement des pages déjà visitées lorsque l'utilisateur désire les consulter de nouveau. Les pages sont alors lues de la mémoire cache plutôt que du site Internet qui les contenait originalement.

En dépit du mot *temporaire* contenu dans l'expression *fichiers Internet temporaires*, les fichiers Internet temporaires demeurent stockés sur le disque dur jusqu'à ce que l'utilisateur les efface manuellement ou jusqu'à ce qu'ils soient effacés automatiquement par le navigateur internet parce qu'il manque de place pour emmagasiner de nouvelles pages web. Comme les fichiers Internet temporaires peuvent contenir des centaines et même des milliers de pages web, les pages web peuvent demeurer dans la mémoire cache durant des jours ou même des semaines avant d'être écrasées par de nouvelles pages. Ceci est souvent considéré comme une atteinte à la vie privée, parce que n'importe qui ayant accès à l'ordinateur peut lire la mémoire cache et connaître les pages web qui ont été visitées par l'utilisateur.

***Les avantages des fichiers Internet temporaires***

Les principaux avantages des fichiers Internet temporaires sont :

- Ils accélèrent la navigation sur le Web. Cela est particulièrement vrai pour les gens utilisant des connexions à faible débit (moins de 250 000 bits par seconde).

- Ils réduisent le trafic sur Internet, ce qui bénéficie à tous les utilisateurs.

- Ils permettent de consulter les pages web enregistrées sur le disque dur même lorsqu'une connexion à Internet n'est pas disponible (voir les options de travail hors connexion de votre navigateur).

- Ils permettent aux enquêteurs d'obtenir des preuves pour faire condamner des criminels…

***Les Inconvénients des fichiers temporaires***

- Certaines informations confidentielles peuvent demeurer dans les fichiers Internet temporaires après la visite de sites avec lesquels vous avez échangé de telles informations, par exemple des sites bancaires. Pour éviter de laisser de telles informations dans les fichiers Internet temporaires, terminez toujours vos sessions de navigation sur une site bancaire de la façon standard, c'est-à-dire en cliquant sur le bouton *Fin de la session* du site et non en fermant votre navigateur en cliquant sur le X en haut à droite de la fenêtre du navigateur. Le site bancaire effacera alors vos fichiers Internet temporaires avant de terminer la session.

- Certaines personnes considèrent que les fichiers Internet temporaires constituent une violation de la vie privée en révélant les sites qui ont été visités par un utilisateur.

- La place qu'occupe de tels fichiers n'est pas négligeable (valeur maximale par défaut fixé à 10 % de la taille du volume). Ceci peut s'avérer d'autant plus problématique que ce dossier se trouve par défaut dans le profil des utilisateurs itinérant (*roaming*) ralentissant ainsi l'enregistrement et le chargement du profil à l'ouverture et fermeture de session dans un environnement réseaux

## 3.1.2 Les Cookies

En informatique, un **cookie** (aussi appelé plus rarement **témoin**) est défini comme étant une suite d'informations envoyée par un serveur à un client, que ce dernier retourne lors de chaque interrogation du même serveur sous certaines conditions.
Il est envoyé en tant qu'en-tête par le serveur web au navigateur web qui le renvoie inchangé à chaque fois qu'il accède au serveur.

Un **cookie** peut être utilisé pour une authentification, une session (maintenance d'état), et pour stocker une information spécifique sur l'utilisateur, comme les préférences d'un site ou le contenu d'un panier d'achat électronique. Le terme **cookie** est dérivé de *magic cookie*, un concept bien connu dans l'informatique d'UNIX qui a inspiré l'idée et le nom des cookies de navigation. Quelques alternatives aux cookies existent; chacune a ses propres utilisations, avantages et inconvénients. Étant de simples fichiers de texte, les cookies ne sont pas exécutables. Ils ne sont ni des logiciels espions ni des virus, bien que des cookies provenant de certains sites soient détectés par plusieurs logiciels antivirus parce qu'ils permettent aux utilisateurs d'être suivis quand ils ont visité plusieurs sites.

La plupart des navigateurs récents permettent aux utilisateurs de décider s'ils acceptent ou rejettent les cookies. Les utilisateurs peuvent aussi choisir la durée de stockage des cookies. Toutefois, le rejet complet des cookies rend certains sites inutilisables. Par exemple, les paniers d'achat de magasins ou les sites qui exigent une connexion à l'aide d'identifiants (utilisateur et mot de passes).

## 3.1.3. Le dossier prefetch

Dans l'architecture des ordinateurs, **prefetch instruction** est une technique utilisée dans les microprocesseurs pour accélérer l'exécution d'un programme en réduisant les états d'attente.

Il faut bien comprendre à quoi sert le dossier prefetch (C:\WINDOWS\Prefetch):

Lorsque vous lancez un programme, il fait un traitement, le charge sur le disque, refait un traitement, le charge sur le disque etc…

Au premier lancement du programme, Windows va analyser (pendant 10 secondes) quels sont les fichiers auxquels le programme accède et il les note dans un fichier dans le dossier prefetch.
La mémoire est 1000 000  fois plus rapide que le disque (quelques nanosecondes pour quelques millisecondes)
Lors des lancements suivants, lors des phases de traitement du programme, Windows en profitera pour aller chercher à l'avance les fichiers dont le programme va avoir besoin pour les placer dans une mémoire cache..
Résultat: Un lancement plus rapide des programmes.

En plus de cela, le système prefetch est également actif lors du démarrage de Windows, afin de tracer les chargements de fichiers au démarrage (et optimiser le démarrage de Windows).

Enfin, le défragmenteur de Windows peut également utiliser les informations du dossier prefetch, afin de placer les fichiers les plus utilisés lors du démarrage, en début de disque, pour améliorer encore les performances.

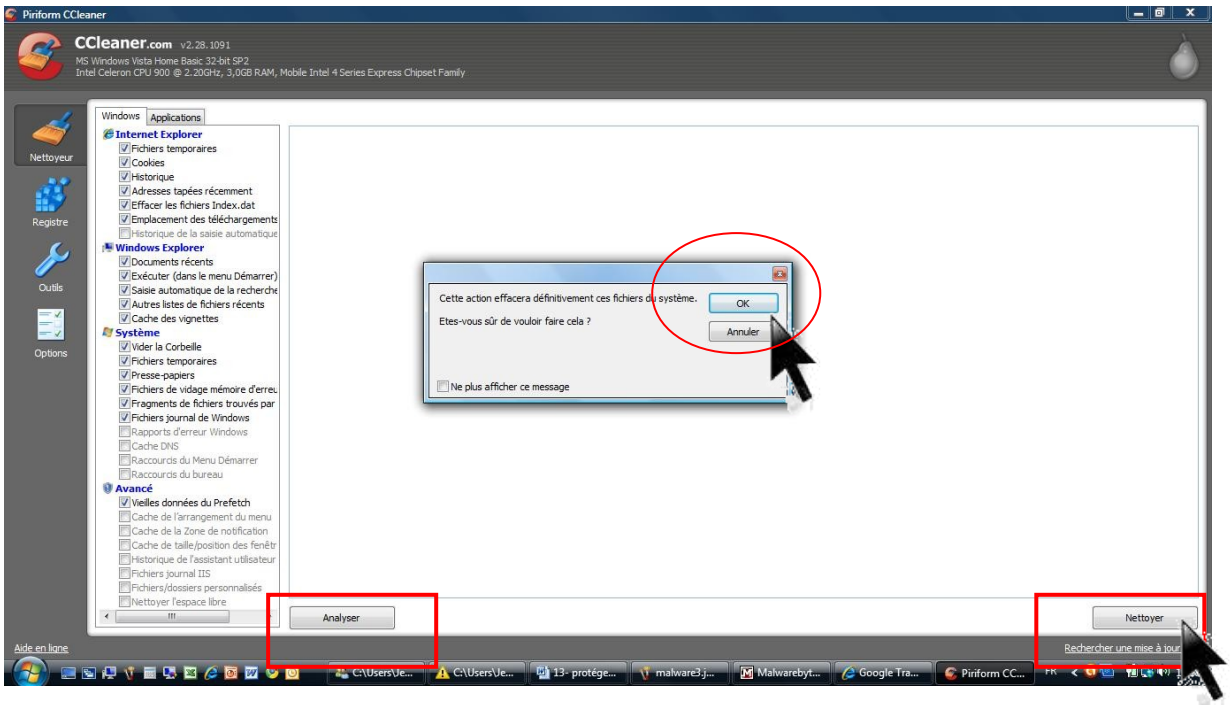
On dit qu'il est inutile de purger ce dossier, car Windows le limite à 128 fichiers de toute manière. Supprimer le contenu de ce dossier ne ferait que réduire les performances de Windows. Désactiver la fonction prefetch vous privera également des améliorations de performances apport.
Par contre, Ccleaner élimine les anciens fichiers du prefetch qui ne sont plus utilisé et ceci peut accélérer le démarrage des programmes actuels.

## *3.2.Utilisation de Ccleaner*

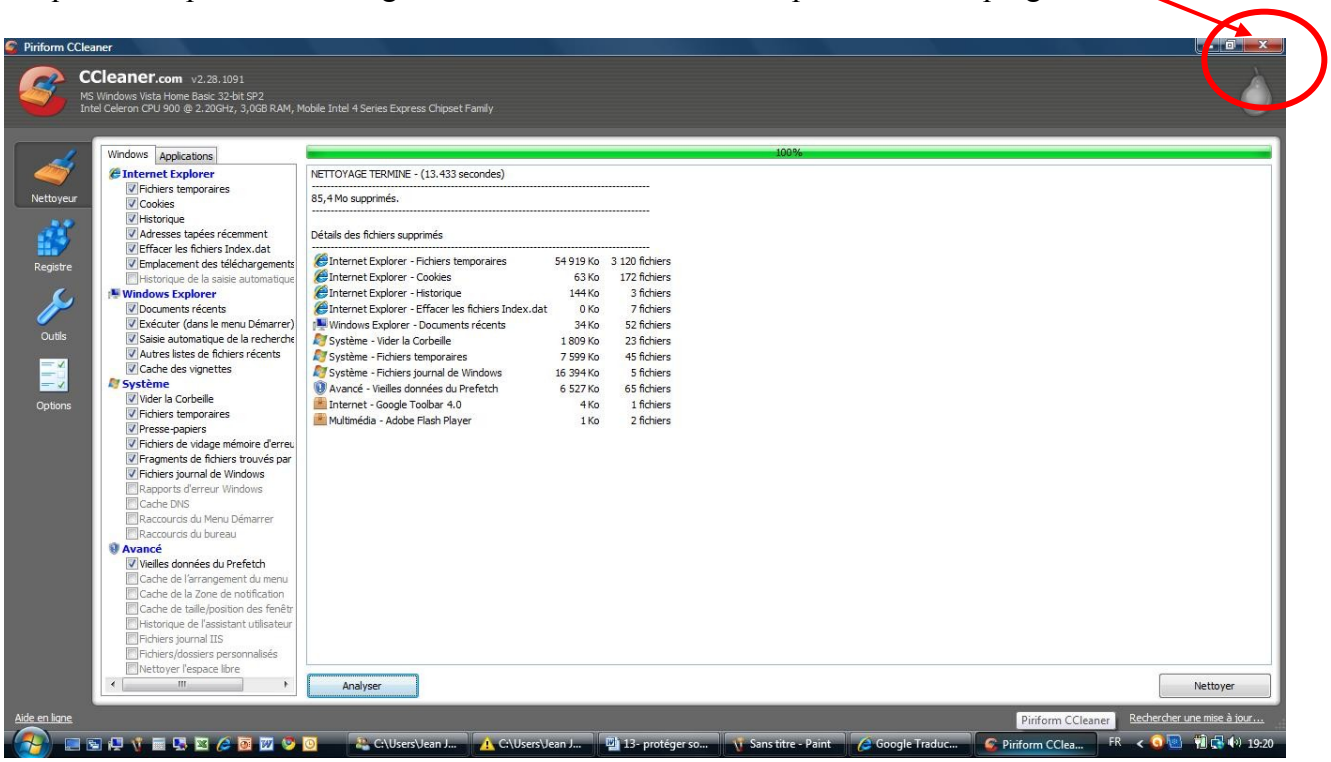
C'est un programme très simple à utiliser.

Cliquer sur l'icône de Ccleaner  pour ouvrir le programme, la fenêtre suivante s'ouvre.
Cliquer sur analyser pour avoir un aperçu de ce que va vous éliminer Ccleaner ou directement sur Nettoyer

Une petite fenêtre s'ouvre au centre vous demandant de confirmer l'effacement des fichiers, répondre OK



Une barre verte déroulante permet de voir l'évolution du pourcentage du nettoyage.
A la fin, le résultat est affiché sur l'écran. Ici, 85Mo ont été libérés.
Cliquer sur la petite croix rouge en haut à droite de la fenêtre pour fermer le programme.




# 4. Défragmentation du disque

## *4.1 Qu'est-ce que la fragmentation d'un disque ?*

Le mot fragmentation, signifie découpé en un grand nombre de petits morceaux
Assimilons le disque dur à une grande armoire à tiroirs, tous de même taille, dans laquelle on rangerait des dossiers.
Au départ, tous les tiroirs sont vides, et la secrétaire peut remplir les premiers tiroirs sans problème. Des dossiers sont retirés, ce qui amène des trous dans la rangée des tiroirs. Un problème se pose alors lorsqu'un dossier est trop grand pour rentrer intégralement dans un des emplacements vides. Le dossier est alors séparé en plusieurs morceaux puis réparti dans des cases vides.

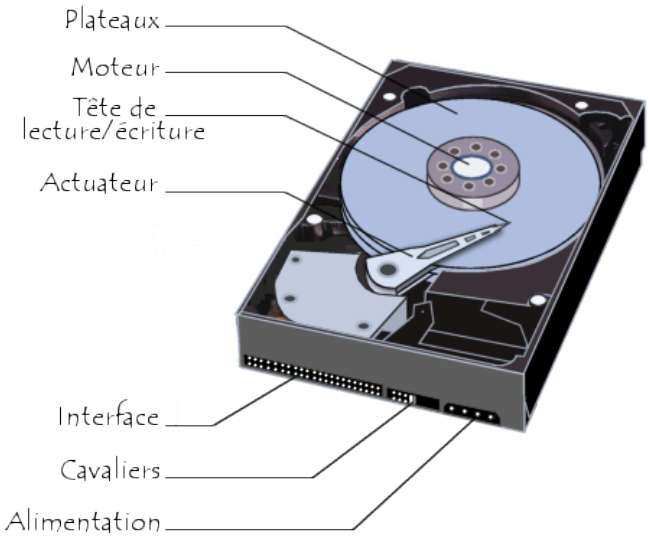
**C'est l'équivalent de ce qu'on appelle la fragmentation en informatique.**

Maintenant, si la secrétaire doit aller chercher ce dossier, elle doit aller chercher les différentes parties du dossier à des endroits différents, ce qui prend plus de temps que si l'intégralité du dossier était stockée au même endroit. Pour y remédier, il suffit que, régulièrement, quelqu'un s'occupe de réorganiser toute l'armoire en rassemblant les éléments de chaque dossier,

**C'est l'équivalent de ce qu'on appelle la défragmentation en informatique.**

Au début, lorsque le disque est vide, les données des fichiers sont contigus lorsqu'elles s'installent sur le disque.

Au fil de l'eau, on efface des fichiers. Lorsqu'on enregistre un gros fichier, celui-ci peut prendre l'emplacement de plusieurs petits, car Windows essaie de combler les trous . On dit qu'il est fragmenté.
Lorsque ceci se répète de nombreuses fois, on dit que le disque est fragmenté puis, arrivé à un certain niveau de la fragmentation, on commence à rencontrer des problèmes.




**Conséquences d'un disque fortement fragmenté :**

Lorsqu'un fichier n'est pas fragmenté, la tête de lecture du disque dur se déplace très peu car le fichier est en un seul morceau.

Par contre, lorsqu'un fichier est fortement fragmenté, la tête de lecture va faire de multiples aller-retours pour lire chacun des groupes du fichier : Le temps d'accès des tête est mécanique donc prend un temps énorme par rapport à une lecture mémoire 3 à 10 ms suivant les disques. Ce qui est énorme comparé au temps d'accès de la mémoire vive (10 nano secondes) qui travaille environ 1000 000 de fois plus rapidement.
On comprend dès lors que lorsqu'on multiplie les accès disques, l'ordinateur perd beaucoup de temps.

**Un disque fortement fragmenté entraine un ralentissement important du fonctionnement de l'ordinateur. Il existe des outils permettant de défragmenter le disque**

## *4.2 Précautions pendant la défragmentation*

**Eviter d'arrêter brutalement l'ordinateur pendant une défragmentation. S'il est en train de replacer un fichier système à ce moment sur le disque, cela peut causer des problèmes à votre machine**

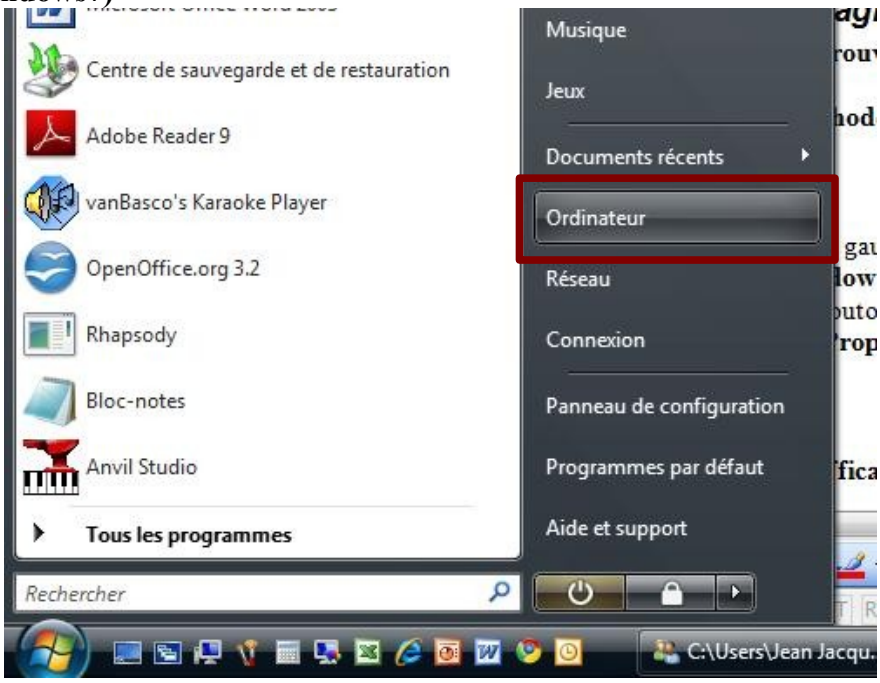
## *4.3 Le défragmenteur de Windows*

### *Comment le trouver ?*

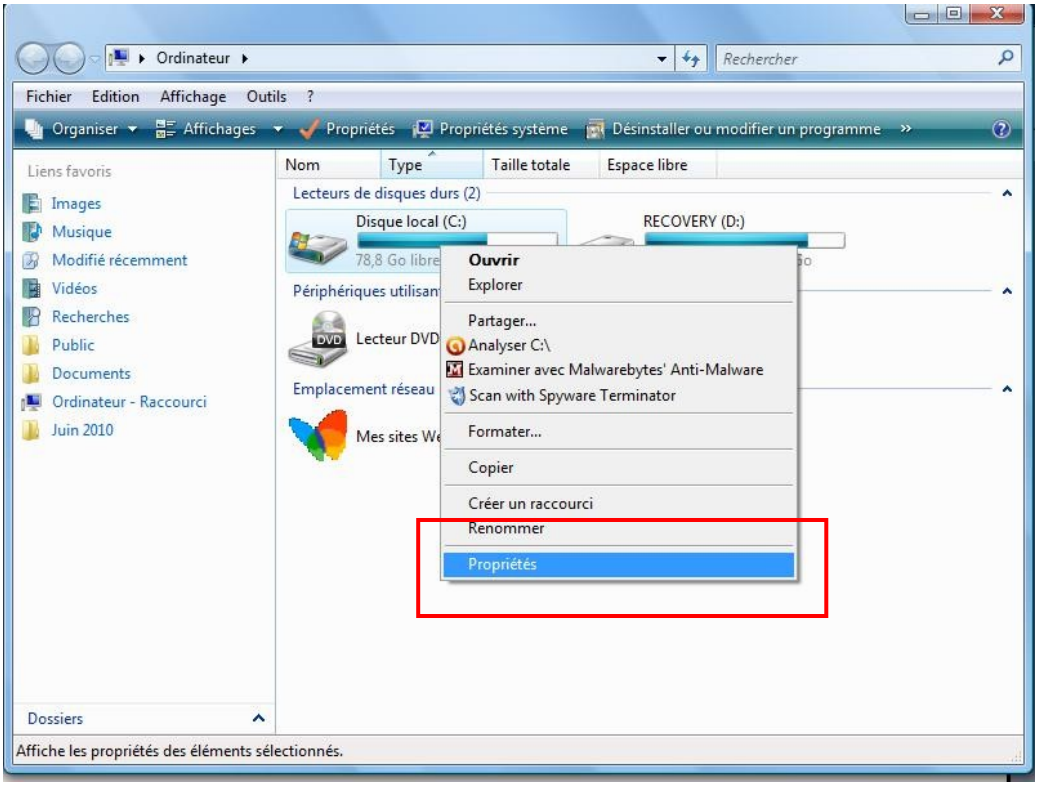
**Plusieurs méthodes**

### 4.3.1La première méthode :

Cliquer bouton gauche sur **« Démarrer »,** puis **« Poste de travail » (XP)** ou **« Ordinateur » (Vista ou windows7)**

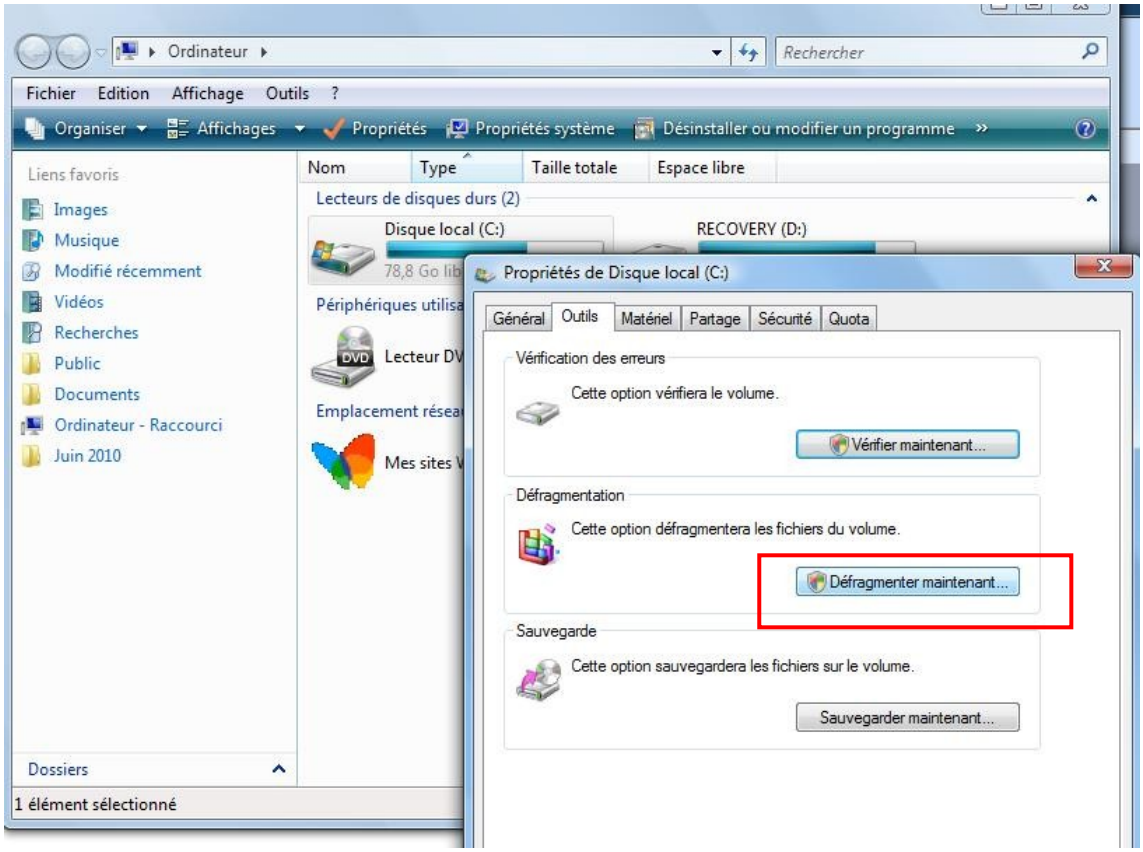



Faire un clic bouton droit sur le disque que vous désirez défragmenter (en général le disque C) puis option **« Propriété** » puis **« Outils».**

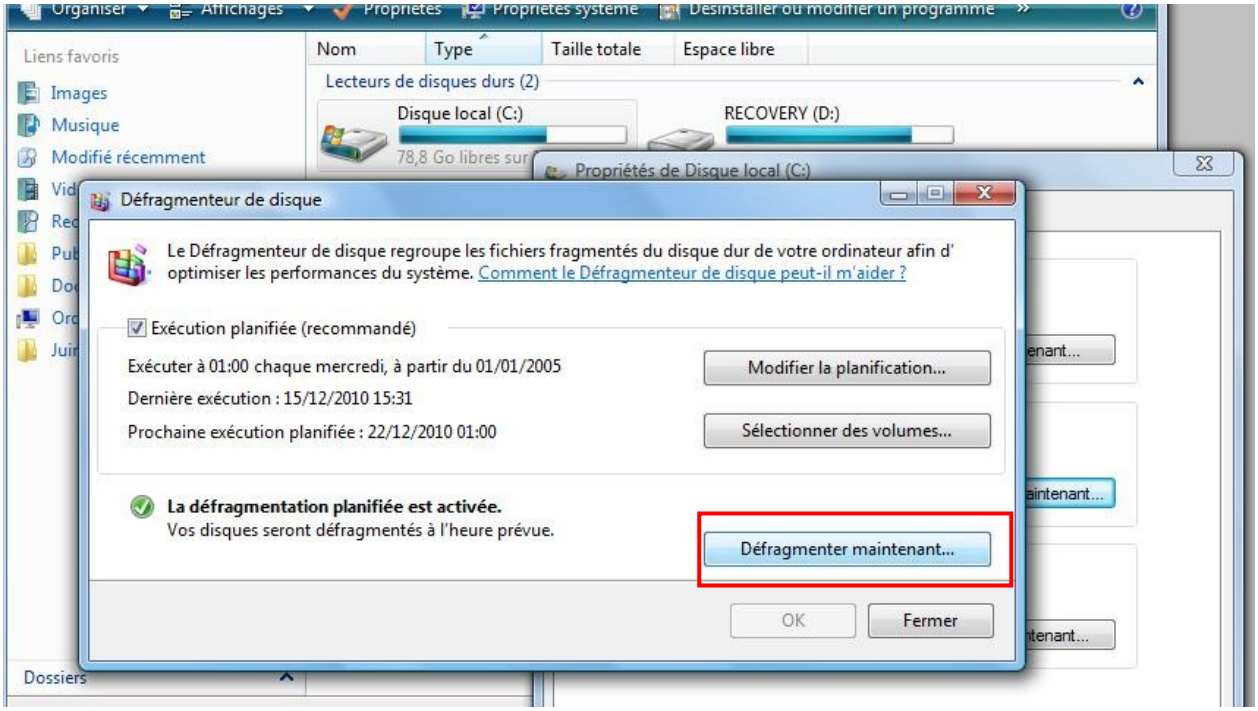



**Ensuite, cliquer sur « défragmenter maintenant »**

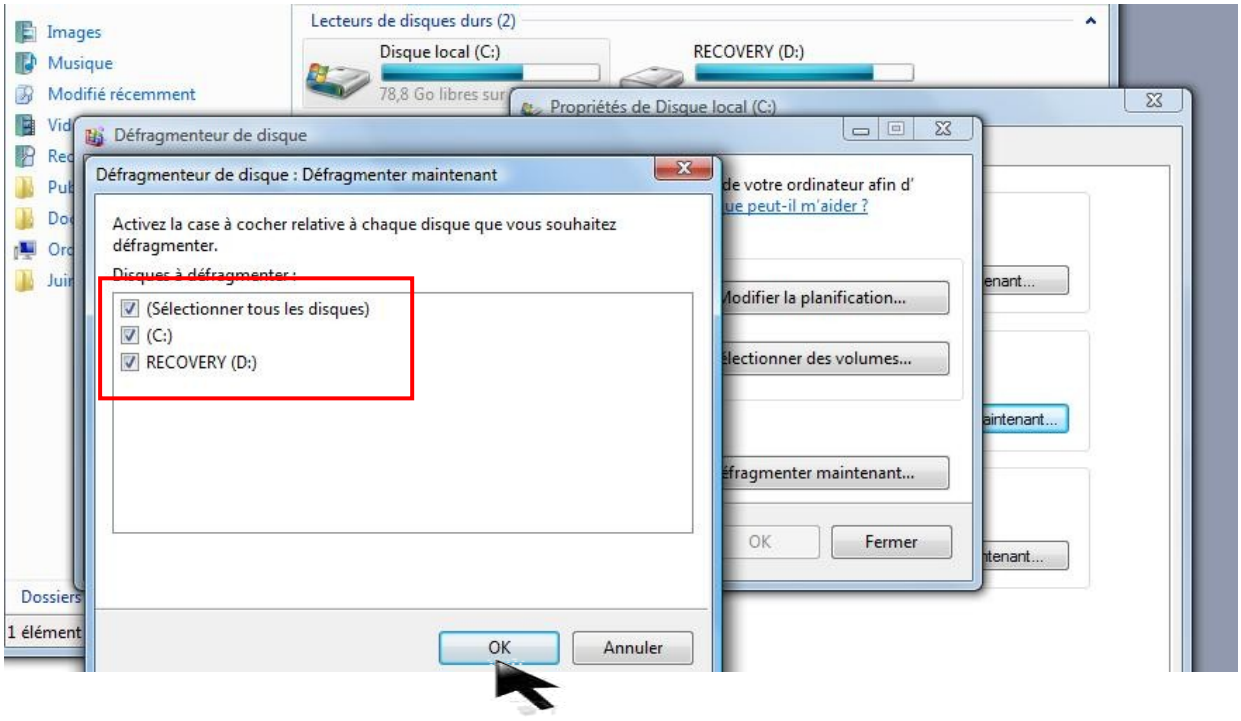
**NOTA : les écrans peuvent être différents suivant votre version de Windows, mais le principe reste le même**



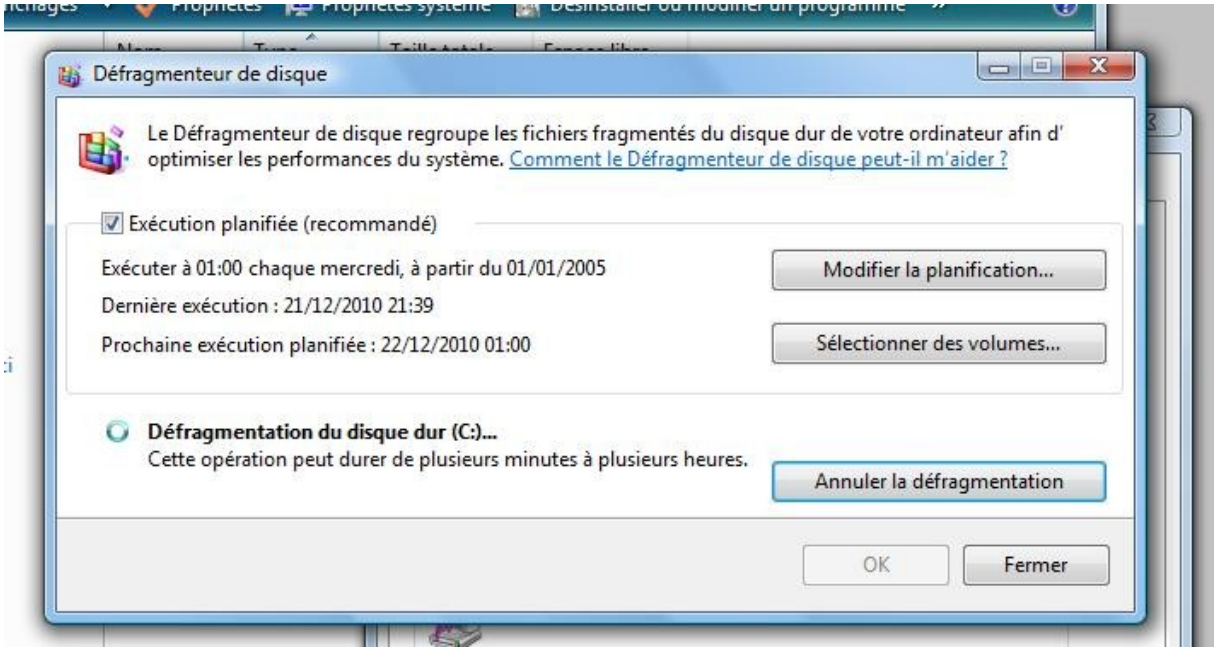
**Puis de nouveau sur défragmenter maintenant**




**Les disques apparaissent sélectionnés, reconfigurer selon ses besoins, puis OK**

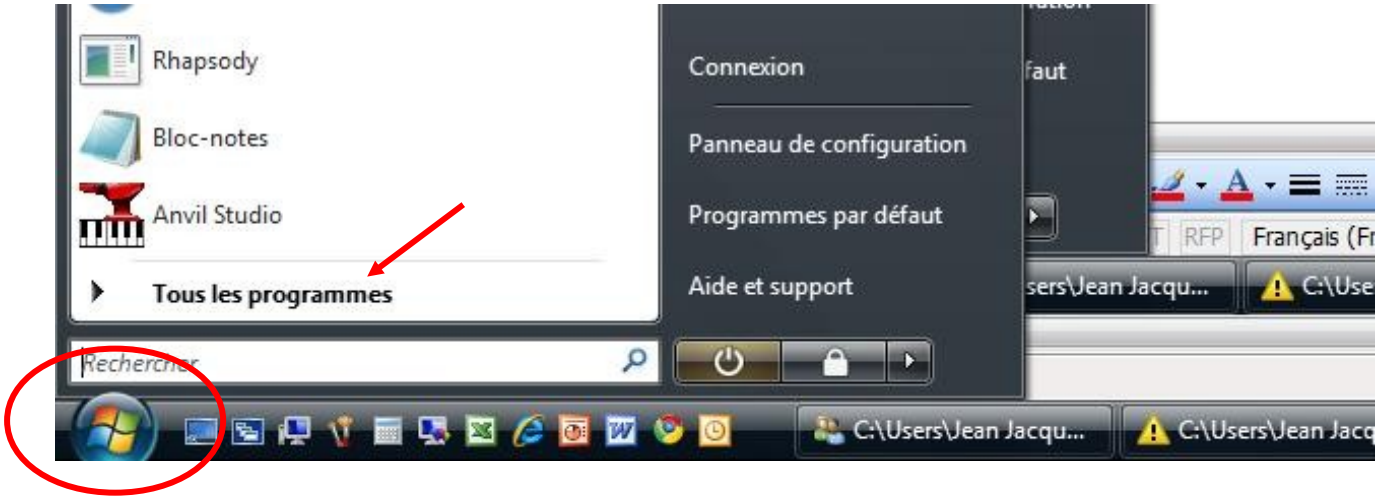


**La défragmentation démarre**

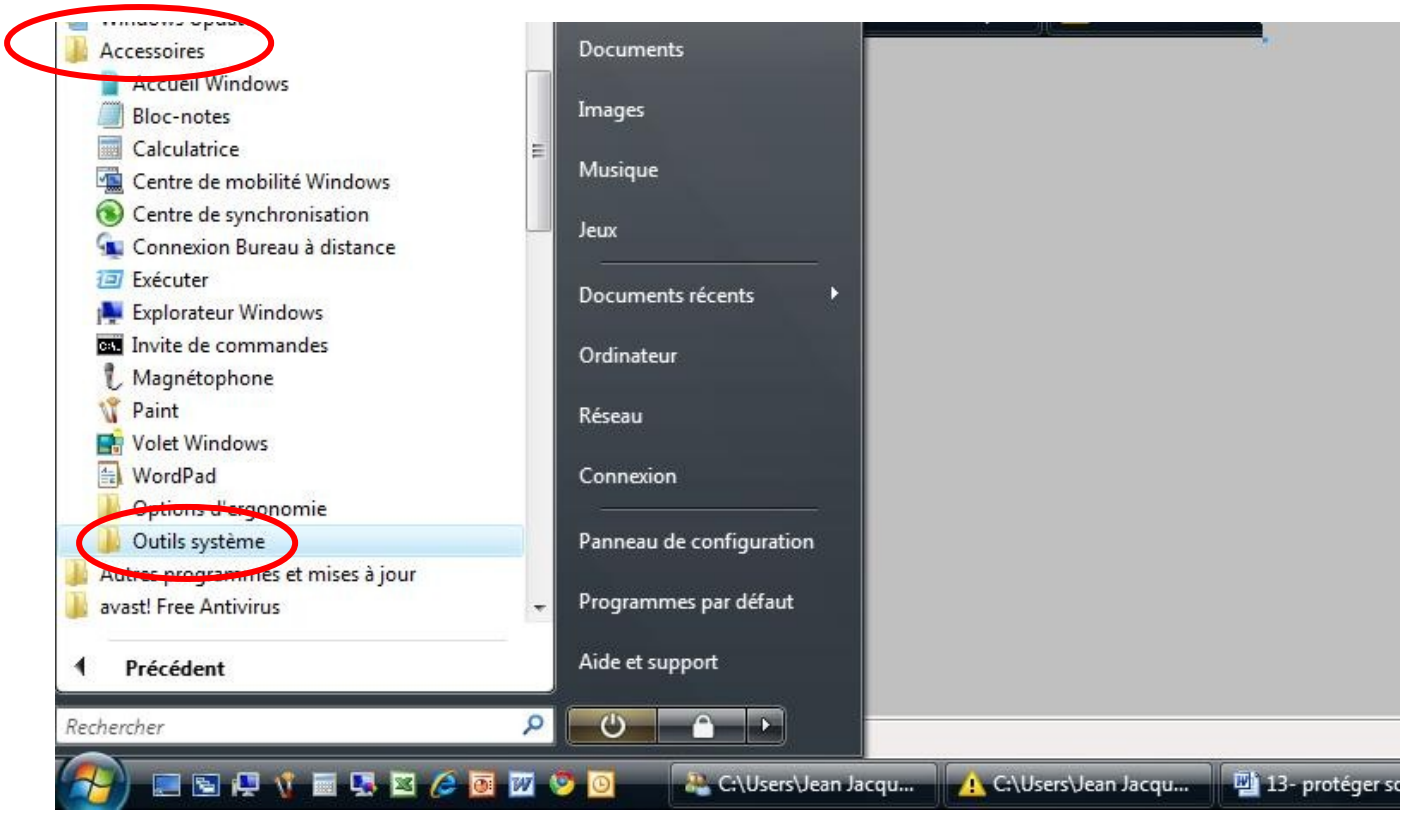



## 4.3.2 Seconde méthode

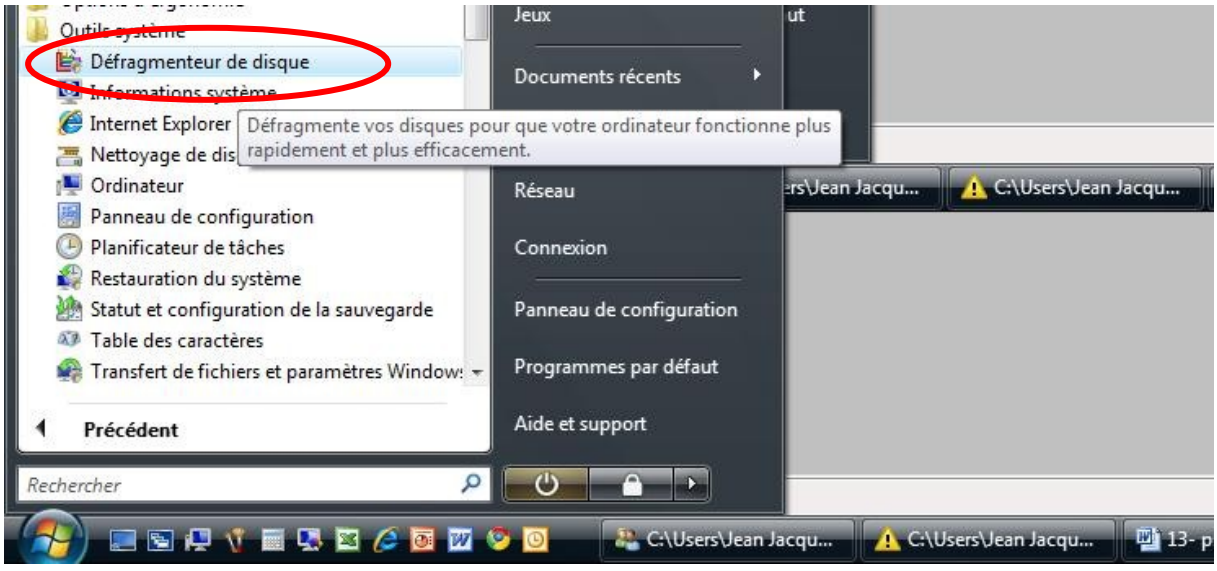
**Cliquer sur le bouton démarrer puis sur tous les programmes**



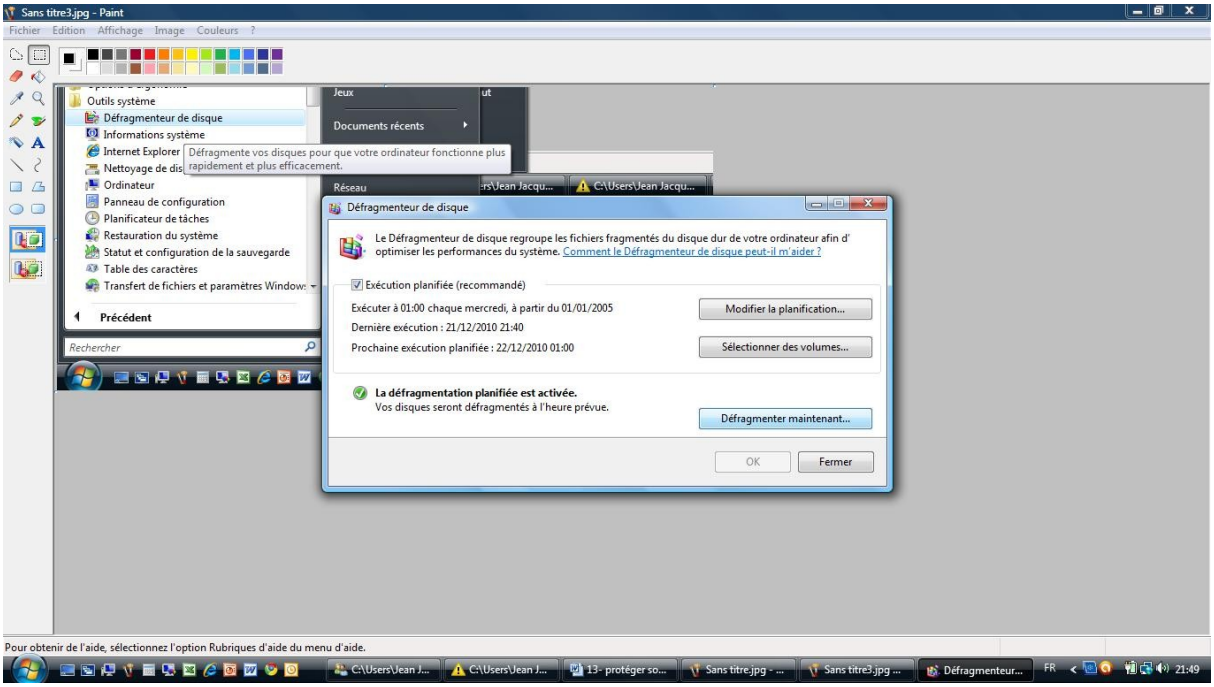
**Ensuite, cliquer sur le dossier « Accessoires » puis le dossier « Outils système »**




**Puis cliquer sur l'option « Défragmenteur de disque »**

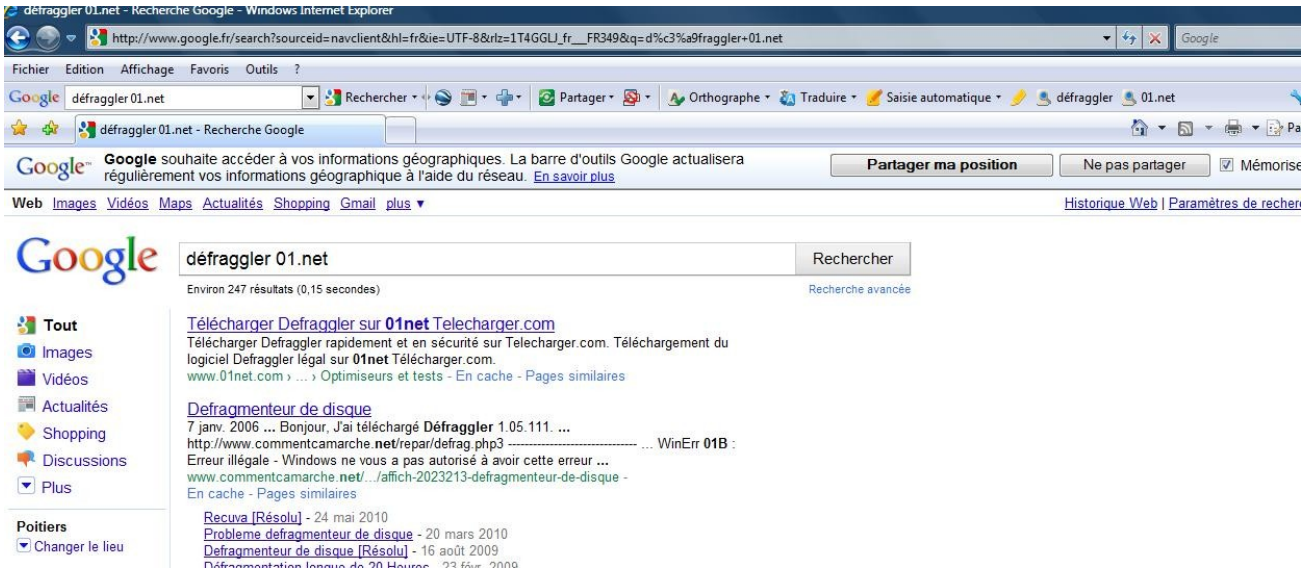


**On se retrouve sur l'écran du défragmenteur vu dans la première méthode.**




## 4.4. Un outil efficace et plus intéressant Déffragler

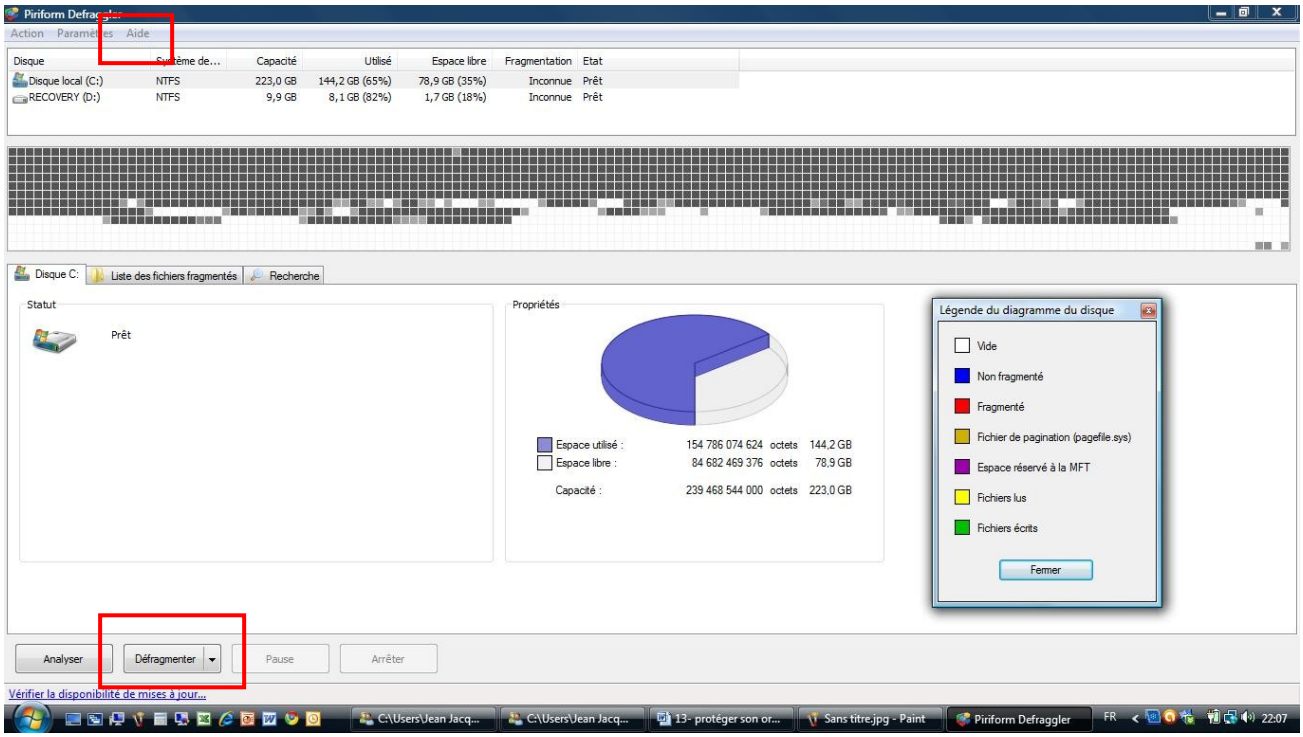
Il existe un programme gratuit vraiment très performant que l'on peut télécharger gratuitement sur internet et installer sur son ordinateur, « **DEFRAGGLER** »
Je tape « **défraggler 01.net** » dans Google (car je sais que « 01.net » est un site sérieux)



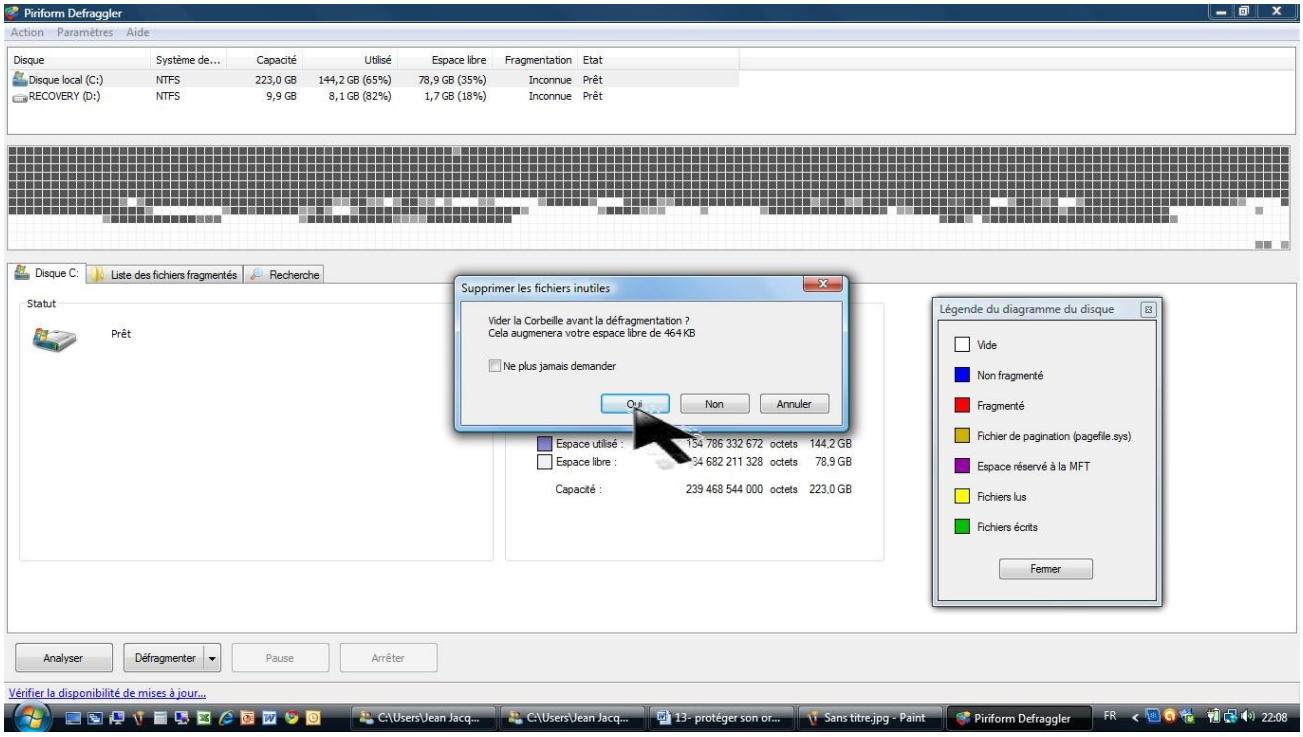
## *Une fois installé, voici comment il fonctionne.*

**Clic gauche sur son icône se trouvant sur le bureau**

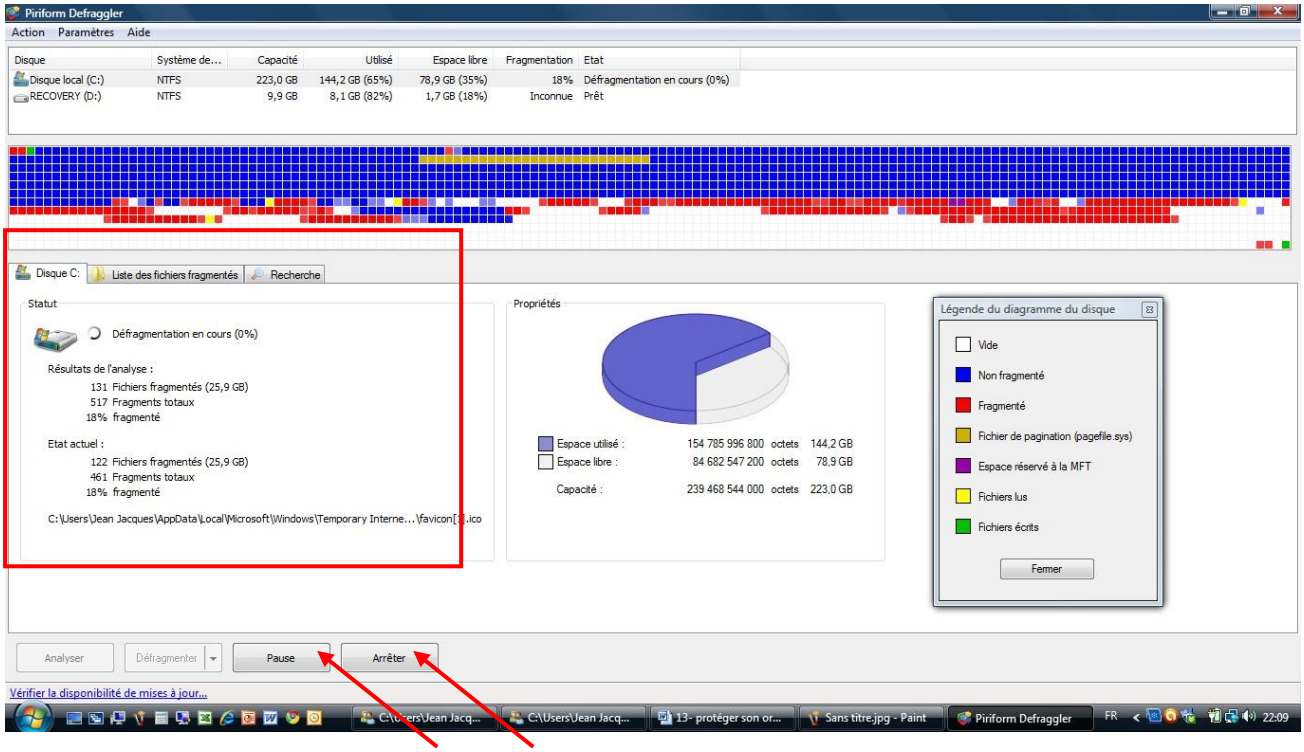

**On peut afficher la légende en cliquant sur « Aide » dans le menu**
**Cliquer sur le bouton « Défragmenter » pour démarrer**



**On peut vider la corbeille (conseillé) en cliquant sur « Oui »**

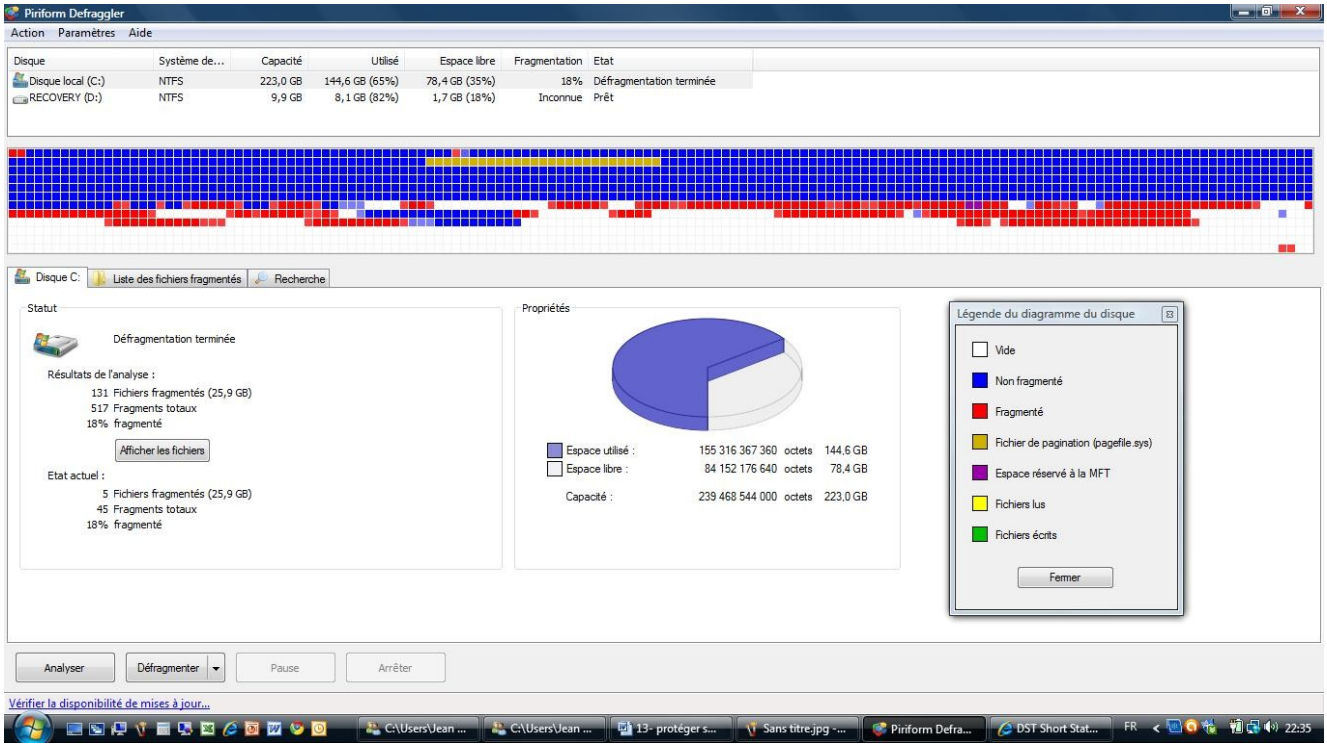



**La défragmentation commence, les fragments de fichiers sont en rouge.**
**Le détail de la situation initiale et de l'évolution de la défrag sont indiqués à gauche**




**On peut la stopper en cliquant sur « Arrêter » ou la mettre en pause**

**La défragmentation est terminée. Il peut rester des fichiers fragmentés.**
**Dans l'exemple, il reste 5 fichiers fragmentés.**




# 5. Conclusion

**Je vous conseille d'effectuer régulièrement ces opérations sur votre ordinateur.**

- Ccleaner toutes les semaines
- Une défragmentation tous les mois
- L'antivirus au moins tous les mois sauf si comportement suspect de l'ordinateur (faire de suite).
- Les anti espion au moins une fois par mois sauf si comportement suspect de l'ordinateur (faire de suite).

En faisant une maintenance régulière sur votre machine, vous limiterez les problèmes (perte de données, plantage, destruction totale du disque…) et éviterez d'avoir à amener votre machine chez le réparateur ce qui n'est pas gratuit !