



# Comment nettoyer son PC avant de s'en défaire?

Pour plus de sécurité, adoptez les réflexes CASES !

## Introduction

Les données qui vous appartiennent et que vous manipulez ont différents niveaux de confidentialité. Vous ne traitez probablement pas de la même manière les données que vous mettez sur un réseau social et celles que vous gardez exclusivement sur votre disque local.

Photos, vidéos, textes, lettres ou mails sont la partie visible de l'iceberg, il existe aussi quantité de données qui sont le produit secondaire de l'utilisation que vous faites de votre ordinateur : fichiers temporaires, historiques de navigation, profils d'utilisateurs, mots de passe sauvegardés en sont quelques exemples. Sur votre ordinateur vous laissez sur votre passage, tel un escargot, une traînée visible de tout ce que vous faites.

Si vous souhaitez mettre au rebut ou léguer votre ordinateur, il est important d'effacer vos traces car un simple effacement de fichiers ou reformatage du disque ne suffisent pas. Ce document vous y aidera.

## Méthode 1 - L'annihilation totale de vos données

### Objectif

Vous voulez revendre ou mettre au rebut votre PC. Les disques qui contiennent vos données vont tomber dans des mains inconnues. Il vous faut tout effacer.

### Démarche à suivre

#### Matériel et méthodes

Pour effacer efficacement toutes les données précédemment citées, il est important d'utiliser un système indépendant de celui dont vous souhaitez vous débarrasser. Vous pourrez par exemple démonter les disques et les brancher à un autre ordinateur. La manière la plus simple consiste cependant à utiliser un système dit « live » qui peut démarrer votre ordinateur sans utiliser ses disques durs internes.

Le système Live « Darik's Boot And Nuke » est gratuitement mis à disposition sur le site suivant : <http://www.dban.org/>

Veillez télécharger le fichier avec l'extension « iso ». Ce fichier est une image de disque compact prête à être gravée. Pour l'utiliser, il suffit de se servir d'un logiciel de gravure. Prenez bien garde de ne pas graver votre CD comme disque de données conventionnel avec le fichier image comme contenu, mais cherchez plutôt l'option « graver une image » ou « burn image » en anglais.

Une fois le CD gravé il faudra redémarrer votre ordinateur avec le CD dans votre lecteur. Sur la plupart des ordinateurs le disque sera lancé au démarrage au lieu du système d'exploitation. Si votre système d'exploitation habituel se charge au lieu de « Darik's Boot And Nuke » il faudra définir dans votre BIOS le lecteur CD comme premier lecteur de démarrage. Nous vous conseillons de faire une recherche sur Internet pour vous aider à faire cette configuration.

## Destruction des données

Une fois ce live CD démarré vous aurez ceci à l'écran :

```
Darik's Boot and Nuke
-----

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied
warranty of merchantability or fitness for a particular purpose. In no event
shall the software authors or contributors be liable for any damages arising
from the use of this software. This software is provided "as is".

http://www.dban.org/

* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key to read the RAID disclaimer.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

Tapez alors autonuke[entrée] pour effacer tous les disques sur votre ordinateur. Attention cela effacera aussi les mémoires de masse attachées à l'ordinateur par usb (comme les appareils photo, ou disques externes). Vous pourrez alors retourner à vos activités habituelles car cette opération peut-être très longue, prévoyez de laisser l'ordinateur allumé pendant au moins une journée.

Si vous voulez plus de contrôle appuyez simplement sur [entrée] pour accéder au menu principal :

```
Darik's Boot and Nuke 2.2.6 (beta)
-----
Options                               Statistics
-----
Entropy: Linux Kernel (urandom)        Runtime:
PRNG: Mersenne Twister (mt19937ar-cok)  Remaining:
Method: DoD Short                       Load Averages:
Verify: Last Pass                       Throughput:
Rounds: 1                               Errors:

-----
Disks and Partitions
-----
▶ [  ] ATA Disk UBOX HARDDISK 1.0 16GB UBb03261be-9ba0141a

P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

Sur cet écran vous pourrez sélectionner les disques à effacer en appuyant sur [espace].

Si vous appuyez sur la touche [M] vous pourrez aussi choisir la méthode d'effacement.

```

Darik's Boot and Nuke 2.2.6 (beta)
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Merseenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Wipe Method -----
▶ Quick Erase          syslinux.cfg: nuke="dwipe --method zero"
RCMP TSSIT OPS-II    Security Level: Low (1 pass)
DoD Short
DoD 5220.22-M
Gutmann Wipe
PRNG Stream

This method fills the device with zeros. Note that the rounds option does
not apply to this method. This method always runs one round.

Use this method to blank disks before internal redeployment, or before
reinstalling Microsoft Windows to remove the data areas that the format
utility preserves.

J=Up K=Down Space=Select

```

Vous pourrez ici choisir la méthode qui vous convient le mieux.

Précisons ici que la seule méthode que vous devriez utiliser pour la mémoire flash (et donc pour des disques SSD) est la méthode « Quick Erase ». Les autres méthodes risqueraient d'endommager ce type de disques et ne seraient pas plus efficaces, car adaptées à des supports magnétiques.

En général, pour des supports magnétiques (disques durs conventionnels) la méthode « Quick Erase » suffit, elle a aussi l'avantage d'être la plus rapide.

### *Après la destruction*

Selon vos aspirations, vous pouvez maintenant réinstaller votre système d'exploitation favori ou vous défaire en toute quiétude de votre ordinateur.

### *Avantages*

Opération efficace et qui demande peu d'interactions.

### *Désavantages*

Opération longue à effectuer. Pour une entreprise désirant détruire beaucoup de disques, une destruction physique sera plus rapide (et peut-être moins chère).

## **Méthode 2 – Relativement rapide, mais moins efficace**

### **Objectif**

Vous voulez céder votre PC à une personne de confiance, peut-être à l'un de vos enfants. Cette méthode est particulièrement valable si vous avez égaré le disque de réinstallation de votre PC et que vous souhaitez céder un ordinateur fonctionnel.

Le but est d'effacer les données confidentielles tout en laissant le système d'exploitation intact.

Elle présente néanmoins de gros problèmes car non seulement il restera toujours quelques traces de vos données, mais en cas de présence de logiciels malveillants vous léguerez un ordinateur infecté à l'un de vos proches.

## Démarche à suivre

### Matériel et méthodes

Nous allons, en plus des outils déjà présents sur votre ordinateur, utiliser le logiciel suivant :

- ccleaner – téléchargeable sur <http://www.piriform.com/ccleaner>

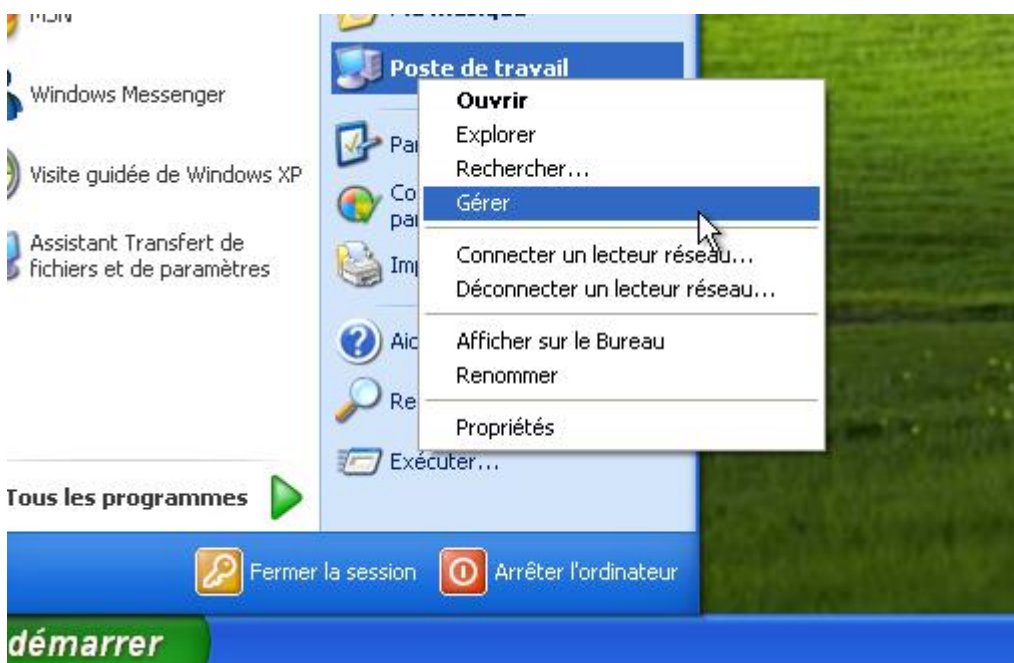
### Destruction des données

Il existe par défaut un compte « Administrateur » dans tout système Windows. Fermez votre session actuelle (démarrer->Fermer la session). Vous vous retrouverez devant un écran d'authentification Windows. L'utilisateur « Administrateur » est malheureusement caché il faut donc appuyer sur [ctrl][alt][delete] pour faire apparaître la fenêtre d'authentification classique :

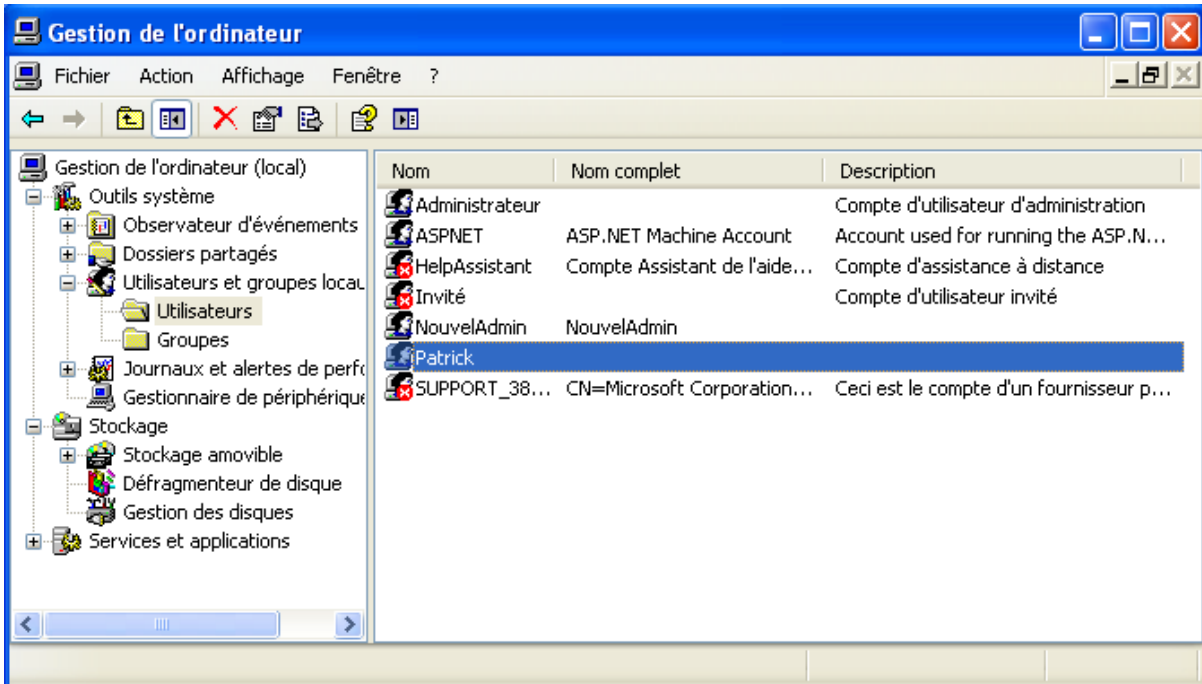


Cet utilisateur spécial s'appelle « Administrateur » dans la version française de Windows mais « Administrator » en anglais ou allemand. Si vous ne vous souvenez plus du mot de passe « Administrateur » nous vous conseillons de créer un nouvel utilisateur ayant les droits d'administration et d'utiliser celui-ci. Ce qui est important est que vous ne soyez pas authentifié avec votre utilisateur habituel.

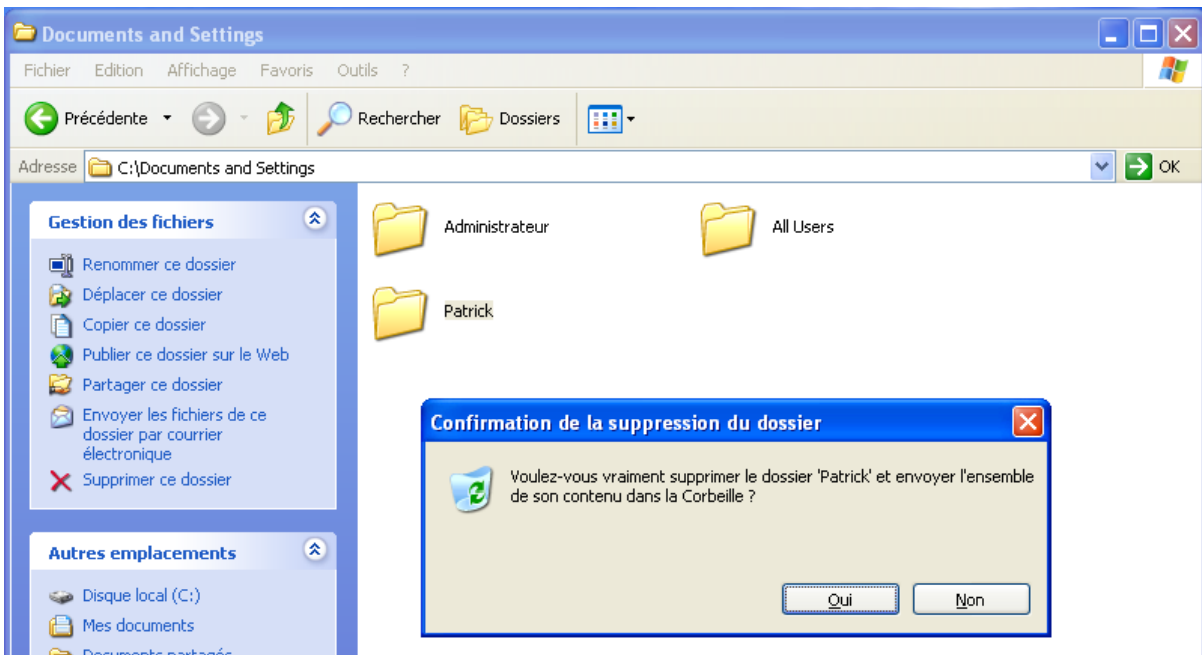
Faites alors un click droit sur votre Poste de travail et sélectionnez « Gérer » :



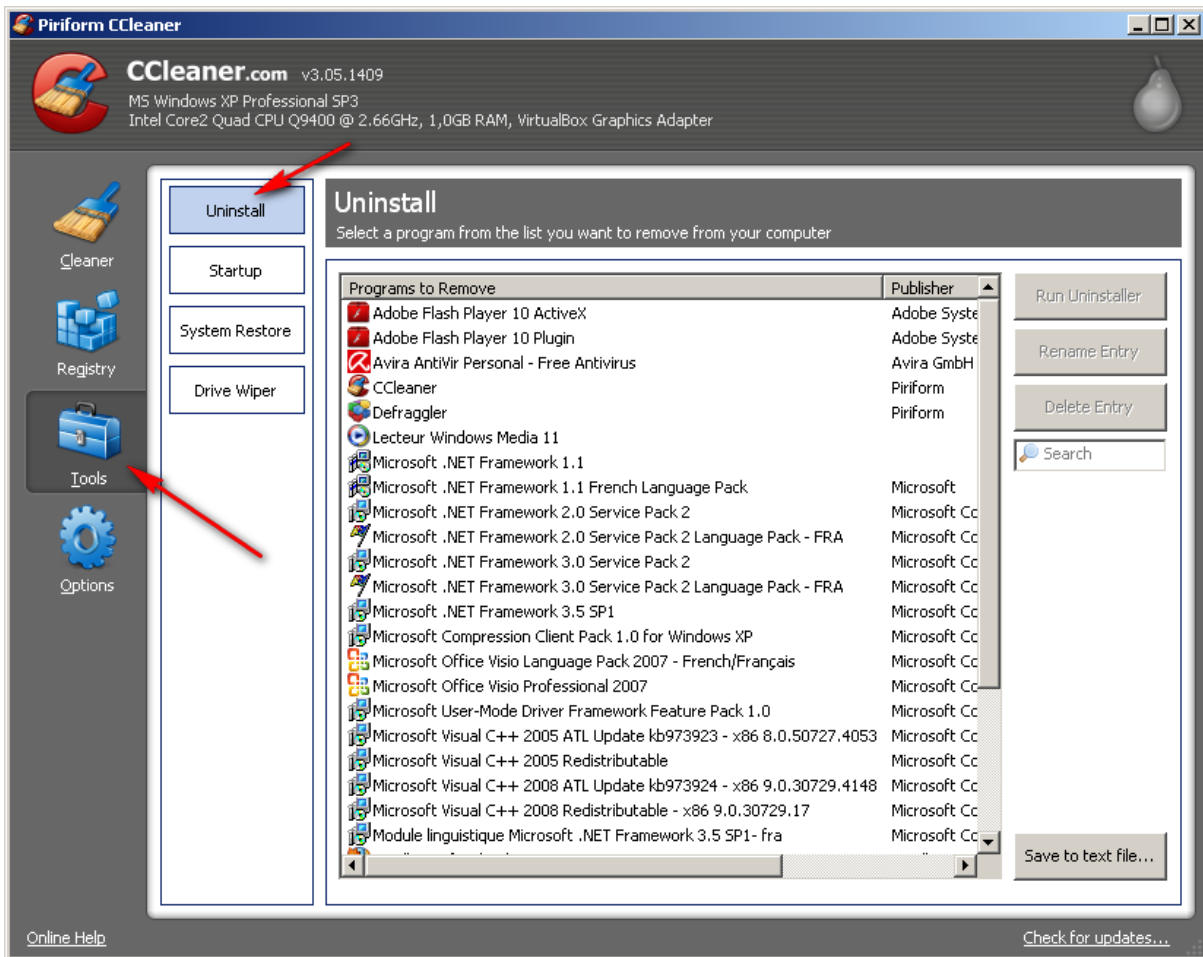
Sélectionnez maintenant vos comptes habituels et effacez-les en appuyant sur la touche [Delete] :



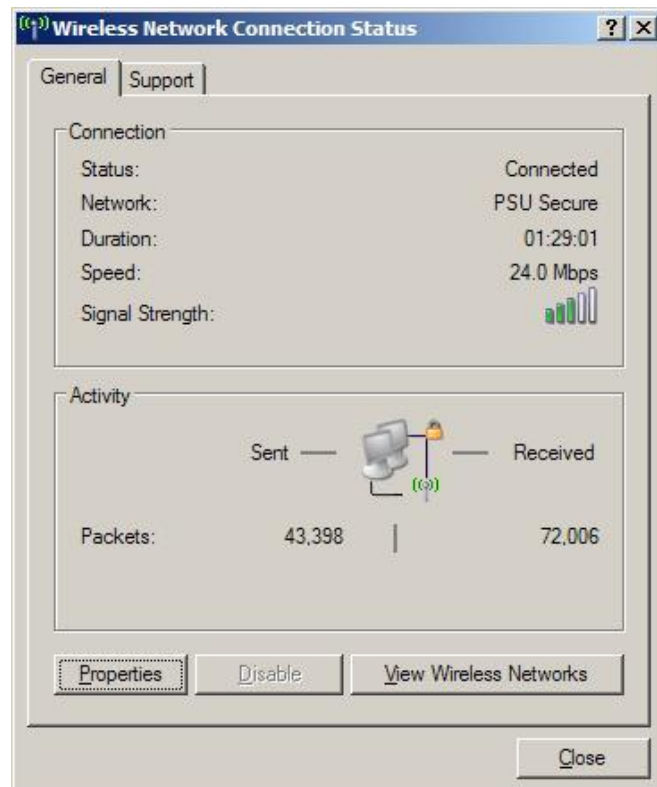
Puis effacez le répertoire personnel des comptes effacés qui se trouve sur 'C://Documents and Settings/' ou 'C://Users' pour des versions de Windows plus récentes :



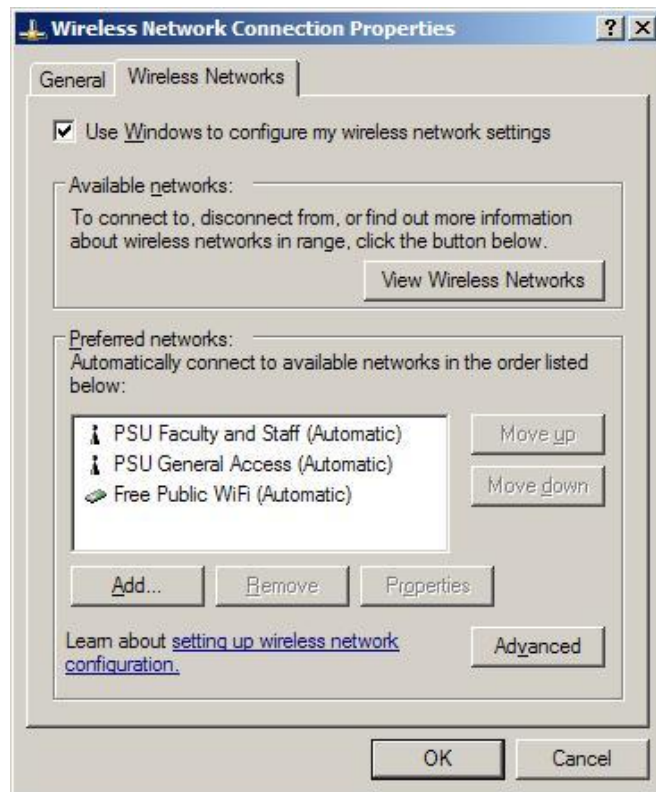
Ensuite il est important de désinstaller les logiciels que l'on ne veut pas céder, par exemple pour des raisons de licences. Il est possible d'utiliser les fonctionnalités de désinstallations intégrées à Windows, mais ccleaner est sensiblement plus rapide. Lancez donc ccleaner :



Pensez aussi à effacer les mots de passe wifi éventuels en allant dans le panneau de configuration cherchez l'icône « Connexions réseau ». Sélectionnez votre connexion réseau et faites un click droit :



Choisissez « Propriétés » puis l'onglet « réseaux sans fil »

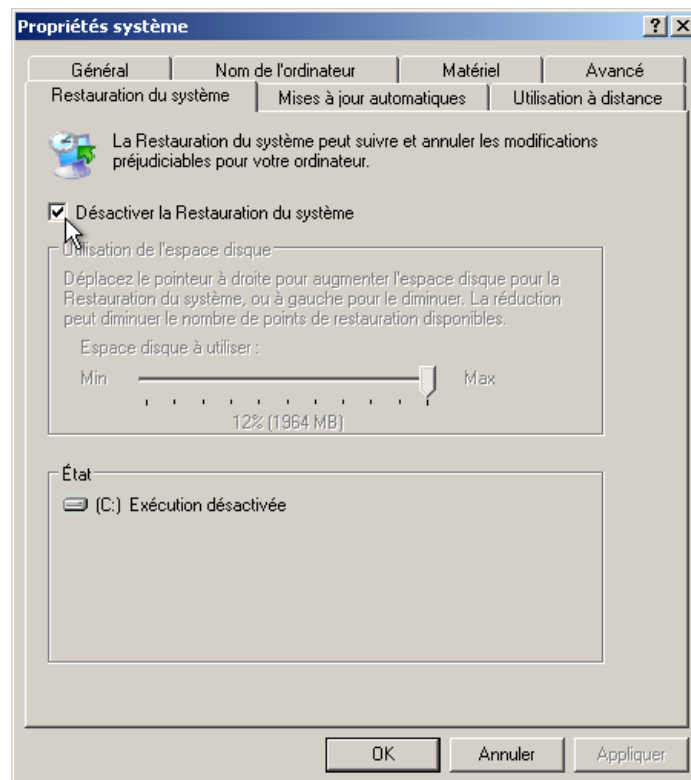


Sous Windows 7 et Vista cherchez dans le panneau de configuration le gestionnaire de réseaux sans fil, dans lequel vous pourrez sélectionner des réseaux et les effacer.

Pensez maintenant à effacer vos points de restauration. Faites un click droit sur votre poste de travail et sélectionnez « Propriétés » :



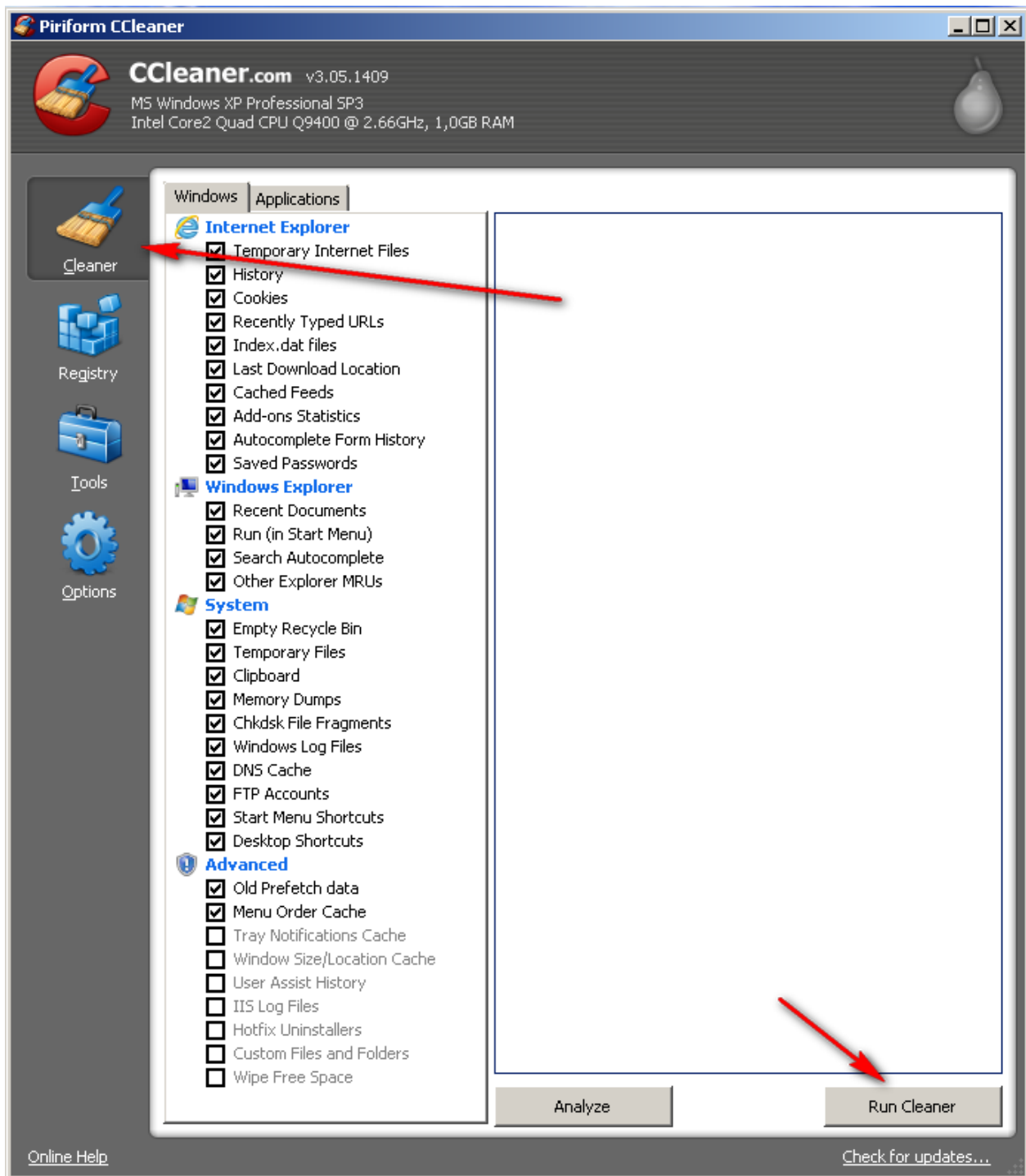
Choisissez alors l'onglet « Restauration du système » et désactivez-la. Après avoir cliqué sur « Ok » vos points de restauration seront effacés.



Si tout ce processus n'a pas assouvi votre saine paranoïa, vous pouvez aussi, tant que vous y êtes, éliminer le fichier de mémoire virtuelle, qui pourrait contenir des bribes de mémoire compromettantes, en allant sur l'onglet « Avancé », le bouton « Paramètres » de « Performances », onglet « Avancées », mémoire virtuelle. Cette dernière étape n'est pas aussi importante et peut être ignorée.

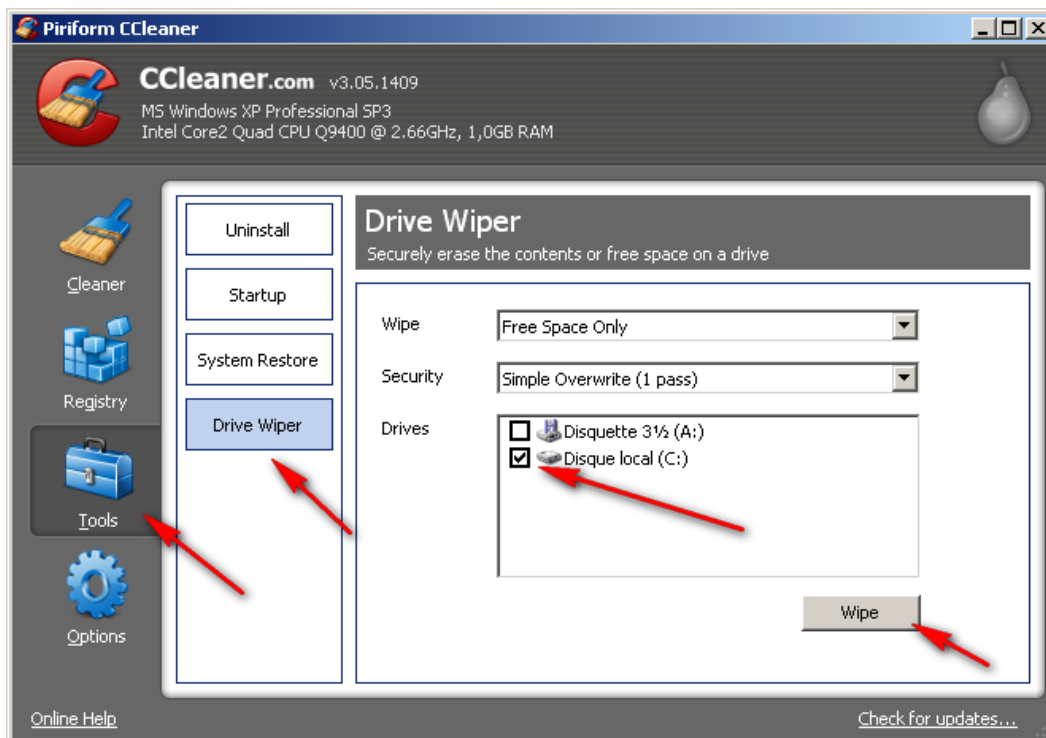
Si vous avez encore des données à d'autres endroits il est à présent important de les effacer. Sélectionnez les dossiers ou fichiers à effacer et appuyez sur les touches [shift]+[delete] pour les effacer sans les envoyer par la corbeille. Si vous avez effacé les fichiers de manière conventionnelle pensez juste à vider la corbeille juste après.

Effacez alors les données cachées en utilisant ccleaner :



Les configurations par défaut suffisent vu que vous avez effacé le profil de l'utilisateur principal.

Toutes les données effacées sont en théorie récupérables dans l'espace libre du disque. Utilisez ccleaner pour effacer l'espace libre :



### *Après la destruction*

Vous pouvez maintenant créer le compte du nouvel utilisateur.

### *Avantages*

Opération qui ne demande pas une réinstallation du système.

### *Désavantages*

Opération qui ne garantit pas la destruction totale des données. De plus, en cas d'infection antérieure par un logiciel malveillant, le système reste infecté.

### **Conclusion**

Deux méthodes ont été présentées pour effacer les données d'un PC. Il est vivement conseillé d'utiliser la première méthode, qui permet de garantir :

1. l'effacement total des données ;
2. après une réinstallation, un système exempt de logiciels malveillants.

L'effacement y est plus facile à effectuer mais plus long que pour la deuxième méthode. En revanche, si vous désirez léguer un ordinateur fonctionnel, il vous faudra réinstaller le système d'exploitation.

Un autre moyen très efficace est évidemment de procéder à une destruction par broyage, si ce n'est de votre ordinateur, du moins de vos disques durs. C'est une solution parfaite pour les grands volumes et donc pour les entreprises. Certaines entreprises sont spécialisées dans la destruction des données, et il vaudra toujours mieux, payer pour détruire ses données que se les faire voler.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)