Table des matières

Effacement sécurisé de données

Les « disques durs » utilisaient des plateaux magnétiques. Ces derniers sont très capacitifs, mais lourds, assez lents et bruyants. Désormais, on rencontre plus souvent des disques à cellules flash (SSD, NVMe, clefs USB…). Ces derniers sont beaucoup plus légers et permettent des accès très rapides aux données.

Pour effacer définitivement des données sur des disques magnétiques, il est d'usage de réécrire (plusieurs fois) des données aléatoires avant de supprimer les fichiers pour s'assurer qu'ils ne seront pas récupérables.

Les disques flash fonctionnent avec des cellules dont le nombre d'écritures est limité. Pour augmenter la durée de vie de ces stockages, une même cellule n'est jamais immédiatement réécrite, rendant caduque la méthode précédente. Il faut alors remplir tout l'espace disponible pour détruire les données.  Attention : **ça n'est pas complètement efficace**, le système n'a pas accès à tous les secteurs du disque ; la seule solution efficace consiste en un **reformatage spécifique** du disque.

Linux, macOS

Sur les dérivés d'Unix (Linux, macOS…), utiliser `shred(1)` (fournit avec les GNU coreutils) ou `srm(1)` (srm) pour détruire des fichiers sur des disques magnétiques :

```
$ shred -fuz fichier-a-effacer.txt
```

Pour les mémoires flash, réécrire des données aléatoires sur l'espace libre dans un fichier sur le volume considéré et supprimer ce dernier à la fin :

```
$ dd if=/dev/random of=/path/to/shredder-file ; rm -f /path/to/shredder-file
```

Windows

Sous Windows, utiliser sdelete par exemple (il existe SDelete-GUI pour avoir une version graphique) pour effacer des fichiers sur des disques magnétiques.

```
C:\temp> sdelete64.exe C:\temp\a_effacer.txt

SDelete v2.05 - Secure file delete
Copyright (C) 1999-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
C:\temp\a_effacer.txt...deleted.

Files deleted: 1
```

Pour les disques SSD et autres mémoires flash comme les clefs USB, ouvrir un terminal et utiliser la commande `cipher.exe` :

```
C:\Windows\system32> cipher.exe /w:E
```

ici, les données du disque `E:` ont été détruites.