T2 P1 - Effacer nos traces

Cette partie du guide pratique sert à vous montrer comment effacer vos traces d'activité militante, en rendant impossible leur récupération

Nous ne supprimons pas réellement nos fichiers

Sachez que même lorsque vous pensez avoir réellement effacé des données, ces dernières laissent toujours des traces.

Dans le cas d'un ou plusieurs fichiers/dossiers supprimés sur votre PC, même en fois la corbeille vidée, ces derniers restent physiquement présents sur votre disque dur. En effet, lorsque nous supprimons un fichier, ce dernier n'est pas réellement « supprimé », mais marqué comme « à supprimer », il reste cependant physiquement sur le disque dur, jusqu'à ce que d'autres données ne l'écrasent.
Il existe, sur les différents systèmes d'exploitation (Windows, Linux, Mac OS) des logiciels ou des commandes, pour vous permettre de réellement supprimer le fichiers/dossiers qui vous intéressent , en écrasant leurs données sur le disque dur, pour qu'on ne puisse pas les récupérer

Comment « réellement » supprimer vos données ?

Je vais vous présenter ici quelques logiciels/commandes qui peuvent vous permettre de réellement supprimer vos données.

(Attention, soyez extrêmement vigilant.e sur les fichiers que vous supprimez, il ne pourront pas être récupérés !)

Vous n'êtes bien entendue pas obligé.e de le faire pour le moindre fichier personnel, mais je le recommande fortement si ce sont des fichiers sensibles, et que vous ne voulez pas qu'on puisse les

récupérer

Je vous montrerais également comment effacer toutes traces de fichiers supprimés par le passé sur votre ordinateur. Cela peut être utile si vous voulez vous assurer qu'il ne reste plus aucune traces de fichiers sensibles sur l'espace libre de votre disque dur

Sur Windows :

Nous pouvons trouver sur Windows les 2 logiciels/commandes suivantes pour écraser des fichiers :

- Le logiciel **Eraser**
  - Télécharger ici
  - Tutoriel ici

Si vous souhaitez télécharger **Eraser**, attention à ne pas vous faire avoir par les faux liens de téléchargement pouvant apparaître sur la page, il s'agit potentiellement de liens frauduleux ou pointant vers des publicités.

Vous devez cliquer sur une des versions listées en dessous du paragraphe, de préférence la première (qui est la plus récente)

Build Name	Version	Release Date	Downloads
Eraser 6.2.0.2993	6.2.0.2993	2021-10-05	674636
Eraser 6.2.0.2992	6.2.0.2992	2021-02-26	485367
Eraser 6.2.0.2991	6.2.0.2991	2020-10-11	221552
Eraser 6.2.0.2990	6.2.0.2990	2020-07-14	158230
Eraser 6.2.0.2989	6.2.0.2989	2020-06-07	73214
Eraser 6.2.0.2988	6.2.0.2988	2020-06-05	12249
Eraser 6.2.0.2986	6.2.0.2986	2019-08-18	416132
Eraser 6.2.0.2983	6.2.0.2983	2019-07-02	80324

Attention : Dans son utilisation, Eraser se base sur une liste de « tasks », correspondants aux fichiers/dossiers que l'on souhaite écraser, et pouvant être lancés manuellement ou automatiquement. Cette liste de « tasks » n'est pas supprimée automatiquement après avoir été lancée, je vous recommande donc de faire clique droit > Delete task après l'avoir lancé si vous ne voulez pas qu'on puisse savoir que vous avez écrasé tel fichier ou dossier

- La commande **sdelete** (Cliquer ici pour savoir comment ouvrir l'invite de commande)
  - Télécharger ici
  - Tutoriel ici

Purger l’espace libre du disque dur

(Cliquer ici pour savoir comment ouvrir l’invite de commande)

Vous pouvez également vous assurez qu’il ne reste plus aucune trace d’anciennes données supprimées sur votre disque dur, en exécutant des commandes ou des logiciels qui vont automatiquement purger/écraser l’espace libre.

La **défragmentation** du disque dur permet de purger les données marquées comme supprimées.

Cliquez ici pour savoir comment défragmenter un disque dur sur Windows 10

La commande **sdelete** permet aussi d’écraser l’espace libre de votre disque dur, avec la commande suivante :
sdelete.exe -c C:

Vous pouvez faire la même chose sans avoir à installer **sdelete** avec la commande suivante :
cipher /wC:

« **cipher** » étant déjà installé de base sur Windows

Je vous conseille fortement de fermer un maximum de logiciel sur votre ordinateur avant l’ exécution de cette commande

Une fois la commande lancée, soyez patient.e, cela va prendre un certain temps

Sur Mac OS :

Note1 : De OS 10.4 à 10.10 il existe une fonction de "**vider la corbeille en mode sécurisé** ". Cette fonction ayant pour but d'effacer les documents de manière fiables (information que l'on retrouve sur de nombreux sites) est en réalité limitée. Elle a d'ailleurs été supprimée depuis OS 10.11 car elle n'est pas réellement efficace en fonction du matériel (disque) utilisé. Donc si vous ne maîtrisez pas quel type de matériel votre Mac est équipé, ou ne maîtrisez pas les limitations de cette fonction, **ne la considérez pas comme fiable.**

La commande **rm -P** permet d'écraser un fichier en écrivant plusieurs fois. La encore, en fonction du matériel utilisé elle peut avoir des limitations sur son efficacité. Cependant elle reste la fonction native la plus simple installée par défaut.

Point d'attention : Apple aime bien sécuriser vos données. Ceci implique donc de nombreuses copies réalisées un peu partout. Par exemple dans iCloud ou TimeMachine. Effacer vos données de votre ordi n'implique donc pas que la donnée en question ne reste pas accessible sur d'autres

supports.

Pour de plus amples informations sur MAC : https://ssd.eff.org/fr/module/guide-pratique-supprimer-vos-donn%C3%A9es-en-toute-s%C3%A9curit%C3%A9-sous-macos

Sur Linux :

(Cliquer ici pour savoir comment ouvrir l'invite de commande)

Il existe sur Linux la commande **shred** pour écraser des fichiers, déjà installée de base, dont voici une documentation plus complète ici

Pour simplement supprimer (définitivement) un fichier, vous pouvez faire :
`sudo shred -uvz <fichier>`

Pour écraser tout un dossier, vous pouvez taper les commandes suivantes :
`IFS=$'\n'` (Nécessaire si certains noms de fichiers contiennent des espaces)
`sudo shred -uvz $(find <dossier> -type f)`
`rm -rf <dossier>`

Purger l'espace libre du disque dur

(Cliquer ici pour savoir comment ouvrir l'invite de commande)

La **défragmentation** du disque dur permet de purger les données marquées comme supprimées.
Cliquez ici pour savoir comment défragmenter un disque dur sur Linux

Il existe aussi sur Linux la commande **sfill** permettant de purger tout l'espace libre du disque dur, vous devez cependant installer le paquet **secure-delete** pour avoir accès à cette commande.

Si vous êtes sur une distribution Debian de linux (Ubuntu, Tails, Linux mint, Pure OS) :
`sudo apt-get install secure-delete`

Si vous êtes sur une distribution basée sur Red Hat (Fedora, CentOS) :
`sudo yum install secure-delete`

Une fois la commande **sfill** installée, voici des exemples de syntaxes de la commande **sfill** :

Purger tout l'espace libre du disque dur :
`sudo sfill -v /`

Purger l'espace libre un peu plus rapidement, en réécrivant moins de fois les données
`sudo sfill -vl /`

Purger l’espace libre encore plus rapidement, en réécrivant encore moins de fois les données
`sudo sfill -vll /`

Purger l’espace libre encore plus rapidement, encore moins sécurisé :
`sudo sfill -vfll /`

Ces commandes prennent un temps conséquent pour purger/écraser tout l’espace libre du disque dur, je vous conseille de trouver une occupation en attendant.

Comment « réellement » désinstaller nos logiciels

En plus des fichiers eux mêmes, vous pouvez également vouloir désinstaller des logiciels sensibles, dont vous ne souhaitez pas laisser de traces sur votre ordinateur, et vous n’allez bien entendu pas utiliser un logiciel comme **Eraser**, ou **shred** sur chaque fichier relatif au logiciel pour cela, ce serait beaucoup trop long.

Je vais vous proposer à la place quelques logiciels ou commandes qui vont supprimer automatiquement toutes les traces qu’ils trouveront de ce que vous souhaitez désinstaller

Après ces « purge » faites, vous aurez la possibilité d’écraser l’espace libre de votre disque, pour vous assurez qu’on ne puisse pas, même en récupérant les fichiers supprimés, savoir que vous avez utilisé tel logiciel.

Bien entendu, le risque 0 de retrouver des traces des logiciels supprimés sur l’ordinateur n’existe pas, mais utiliser ces techniques le diminue drastiquement

Sur Windows :

Il existe sur Windows le logiciel **Revo Uninstaller**, ce dernier va supprimer toutes les traces qu’il peut trouver d’un logiciel donné.

Vous pouvez le télécharger ici
Le site propose des versions payantes de ce logiciel, mais la version gratuite est suffisante.

Voici un petit tutoriel ici

Point de restauration système : Il est parlé dans le tuto ci-dessus de créer un point de restauration système. Cela offre une sécurité au cas où la désinstallation du logiciel nuit au fonctionnement de Windows.
Cependant, si vous voulez vraiment effacer les traces de votre logiciel, je vous conseille soit de

décocher la case, soit de bien veiller à supprimer le point de restauration système une fois le logiciel désinstallé.

Après Revo Uninstaller :

Après votre ou vos logiciels supprimés par **Revo Uninstaller**, pensez à vider la corbeille.
En effet, **Revo Uninstaller** risque de mettre dans la corbeille certains fichiers liés au logiciel, ainsi, en plus de laisser des traces, ces derniers ne seront pas écrasés si vous utilisez une commande pour écraser l'espace libre de votre disque dur.

Une fois **Revo Uninstaller** utilisé, et votre corbeille vidée, vous pouvez, en plus, écraser l'espace libre de votre disque dur, pour être sûre que même le fichiers supprimés associés au logiciel désinstallé ne pourront pas être récupérés

Pour se faire, vous pouvez vous rendre à cette section, qui vous montre comment faire.

Cette action peut prendre un certain temps pour s'exécuter

Sur Linux :

(Cliquez ici pour savoir comment ouvrir l'invite de commande)

Vous pouvez d'abord lister tout les paquets installés avec la commande :
`sudo apt list –installed`

Ou bien lister les paquets qui vous intéressent, en filtrant par nom, avec cette commande :
`sudo apt list –installed | grep <filtre>`
Remplacez <filtre> par ce que vous voulez.

Vous pouvez ensuite purger le logiciel souhaité, avec la commande :
`sudo apt-get purge <logiciel>`
Remplacer <logiciel> pour le nom de logiciel à purger

Après la purge

Une fois votre ou vos logiciels purgés, vous pouvez, si vous le souhaitez, purger/écraser l'espace libre du disque dur, pour vous assurer qu'on ne pourra pas trouver de trace des logiciels désinstallés, à partir des fichiers supprimés.

Pour cela, rendez vous dans cette section

L'écrasement/purge de l'espace libre du disque dur peut prendre un temps assez conséquent

Effacer les méta-données

Parmi les différents types de traces que vous pourriez avoir besoin d'effacer sur votre ordinateur, il y a aussi les méta-données.

Les méta-données sont toutes les données qui tournent autour de la donnée « principale » d'un fichier.
Pour donner un exemple plus clair, une photo peut avoir comme méta-donnés, l'appareil qui a servit à prendre la photo, la localisation correspondante au lieu d'où a été prise la photo, etc …

Ainsi, dans un fichier, en plus des données « principales » (par exemple, l'image en elle même dans le cas d'une photo), peuvent également êtres stockées d'autres données relatives à cette donnée « principale ».

Ces méta-données peuvent contenir des informations auxquelles vous n'avez pas envie que d'autres personnes n'aient accès.

Si vous avez par exemple pris des photos d'une action, il peut être pertinent d'y effacer les méta-données, avant de les publier sur internet

Je vais donc vous montrer comment effacer ces méta-données.

Vous pouvez également consulter ce guide, pour effacer les métadonnées d'une image, avec Gimp 4

Signal

Signal, l'application de communication chiffrée que nous utilisons souvent au sein d'XR a la faculté de supprimer automatiquement les méta-données des photos/vidéos qu'on envoie.

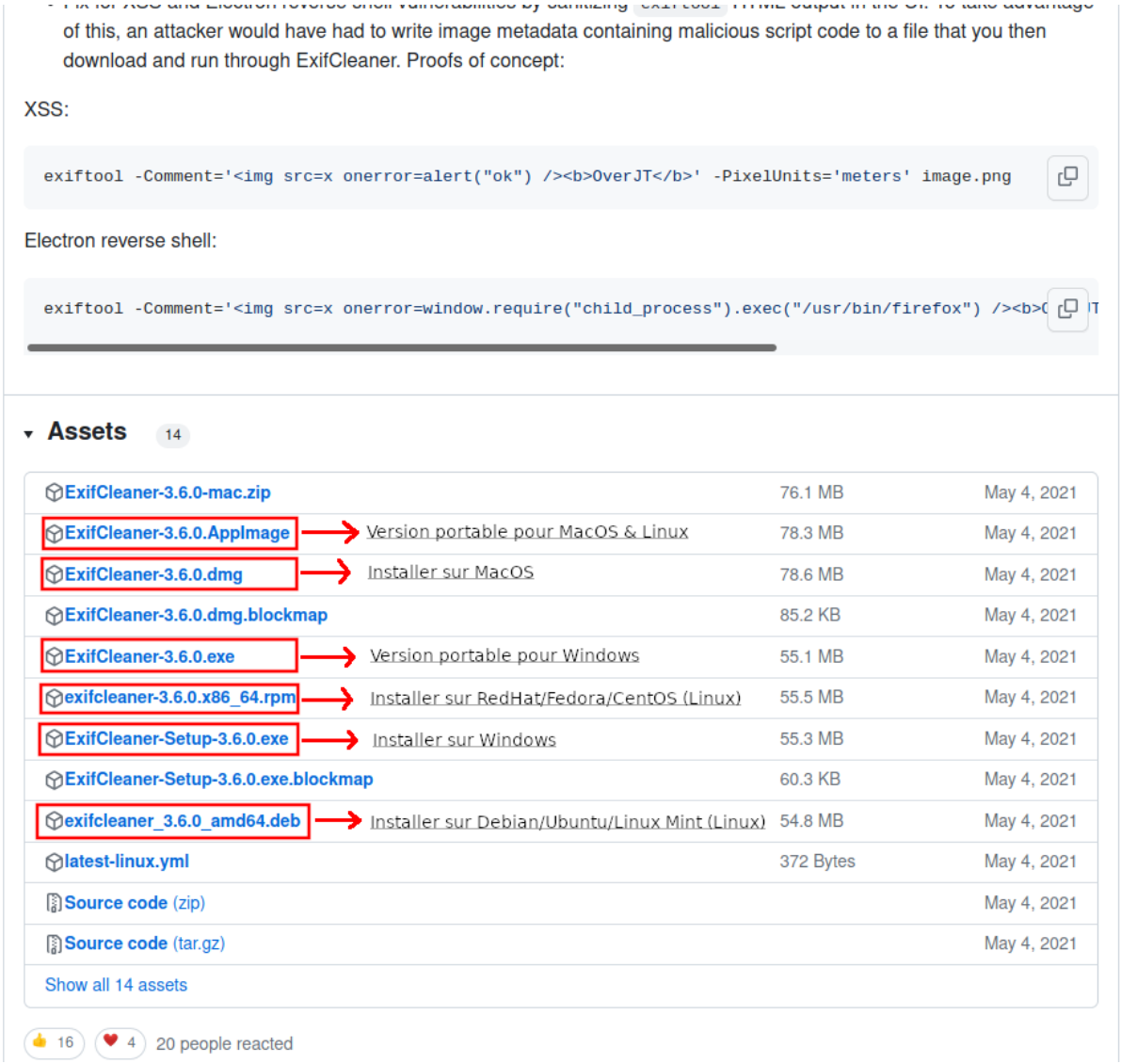
Si vous envoyez par **Signal**, à quelqu'un, des photos ou vidéos que vous avez prises, leurs méta-données seront automatiquement supprimées

Exifcleaner

ExifCleaner est un outil simple d'utilisation, disponible à la fois sur Windows, Linux et MacOS, qui va automatiquement retirer les méta-données de tout les fichiers glissé-déposé dans sa fenêtre.

Pour l'installer rendez vous sur cette page.

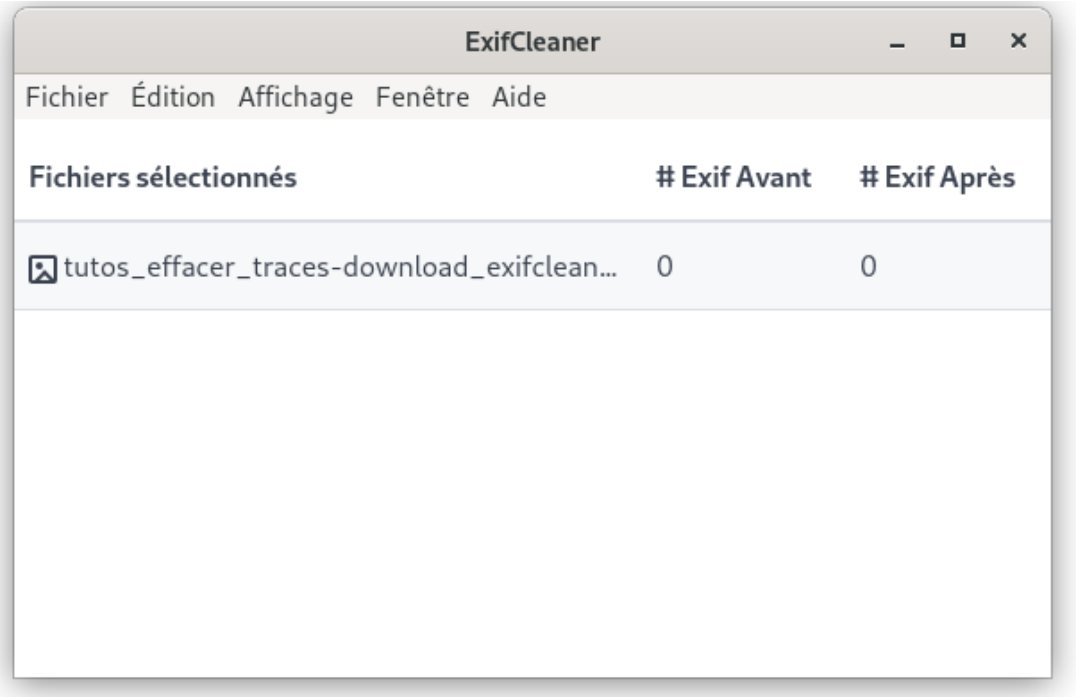
Vous pouvez choisir le fichier à télécharger, en fonction de votre système d'exploitation, et de si vous voulez l'installer ou utiliser la version portable :



(Pour savoir ce qu'est un système d'exploitation, cliquez ici)

La version portable signifie qu'il suffit simplement de lancer le fichier, pour lancer le logiciel, là où la version « installation » installe le logiciel sur votre ordinateur avant de pouvoir le lancer.

Une fois lancé, vous avez une fenêtre qui s'ouvre, et vous avez simplement à glisser/déposer le/les fichiers dans la fenêtre pour effacer automatiquement leurs méta-données.



Exiftool

(Cliquez ici pour savoir comment ouvrir l'invite de commande)

Il existe également un outil en ligne de commande, assez efficace, qui s'appelle « exiftool ».
Cet outil est déjà installé de base sur le système Tails, cependant, si vous avez besoin de l'installer, vous pouvez faire une des choses suivantes :

Si vous êtes sur Ubuntu :
Exécuter cette commande
`sudo apt install libimage-exiftool-perl`

Si vous êtes sur un autre système d'exploitation :
Suivre les instructions de ce lien dans la section correspondante à votre système d'exploitation :

https://exiftool.org/install.html

Voici quelques exemples de commandes.

Voir les méta-données d'un fichier :
`exiftool "<nom-du-fichier>"`

Effacer toutes les méta-données d'un fichier :
`exiftool -all= "<nom-du-fichier>"` (l'espace entre le « all= » et le nom du fichier est à garder)

Effacer toutes les méta-données de tout les fichiers d'un dossier :
`IFS=$'\n'` (Nécessaire si certains noms de fichiers contiennent des espaces)
`exiftool -all= $(find <dossier> -type f)`

Autre solution tout-en-un pour effacer toutes les méta-données des jpg et des mp4 dans un dossier :

```
exiftool -overwrite_original -all= -ext jpg -ext mp4 .
```

Et pour inclure les sous-dossiers :

```
exiftool -r -overwrite_original -all= -ext jpg -ext mp4 .
```

Vous pouvez également voir ce tutoriel en ligne pour plus de détails

---

Créé 2023-12-31 18:26:27 CET par mollusque
Mis à jour 2026-08-23 14:16:02 CEST par pico_