

Effacer ses données

Difficulté ★ ★ ★ ★ ★ Temps requis ⌚ 10min

Objectif

Supprimer aussi complètement que possible les données d'un disque, y compris quand il est chiffré



Étapes

[keyboard_arrow_right](#) Supprimer numériquement les données

[keyboard_arrow_right](#) Supprimer physiquement les données

✓ Prérequis

[task](#) [Effacer ses métadonnées](#)

🧰 Matériel requis

[sell](#) Ordinateur avec Linux (Tails si possible)

[sell](#) Marteau

[sell](#) Disqueuse

[sell](#) Cheminée ou barbecue

🔗 Intérêts de la mesure

[thumb_up](#) Ralentir au maximum les enquêtes

🚫 Inconvénients

[thumb_down](#) Nécessite de ne pas avoir une phobie du terminal

[thumb_down](#) La partie physique demande du matériel "spécifique"

⚠ Menaces concernées

[🏠 Perquisition](#)

— Introduction et parti pris

💡 Conseil

La donnée la plus sécurisée est celle qui n'a jamais existée !

⚠ Attention

Il est impossible de garantir à 100% qu'une donnée numérique a été supprimée, même si le support de stockage a été détruit (par exemple [des données ont été récupérées suite au crash de la navette Colombia](#))

Si tu veux garder ton fichier mais supprimer les méta-données associées, va sur ce tutoriel :

[Effacer ses métadonnées](#)

Principes physiques

Il est impossible de s'assurer à 100 % qu'une donnée numérique soit complètement supprimée, mais il existe divers moyens pour réduire les chances de pouvoir la retrouver.

Sur un [disque dur à disques tournants](#), les données sont stockées par changement de magnétisme sur ces dits disques. Sur les [SSD](#) et la plupart des clés [USB](#), les données sont stockées dans des microtransistors.

Pour s'assurer de la suppression des données, je dois réécrire plusieurs fois sur les endroits où les données ont été écrites avec de nouvelles données insignifiantes : on ajoute des couches et des couches de données pour empêcher les archéologues numériques de pouvoir descendre suffisamment loin jusqu'aux données recherchées.

Une donnée stockée dans la RAM a très peu de chance d'être récupérée une fois l'ordinateur éteint. Il existe des attaques permettant de récupérer le contenu de la RAM d'un ordinateur allumé, non déverrouillé. L'attaquant va "congeler" physiquement la RAM puis redémarrer l'ordinateur sur un autre système d'exploitation afin de lire les données toujours présentes. L'usage de cette technique par des flics en France n'a jamais été documenté.

Suppression numérique

Pour l'application Signal

- Si le délai d'autosuppression n'était pas activé ou pas suffisamment court par rapport à l'urgence de la situation, fais en sorte que les messages soient effacés de tous les appareils avec deux opérations suivant le cas de figure :
 -  : appui long sur le message >  Supprimer > Supprimer pour tout le monde .
Tu peux aussi  Sélectionner plusieurs messages d'un coup
 -  : appui long sur le message >  Supprimer > Supprimer pour moi

Auteur-ice des messages	Messages récents < 24h	Vieux messages > 24h
J'ai écrit les messages	Fais l'opération 	Chaque membre du groupe fait l'opération 
J'ai le contact de l'auteur-ice	Demande à l'auteur-ice de faire l'opération 	Chaque membre du groupe fait l'opération 
Je ne peux pas contacter l'auteur-ice	Chaque membre du groupe fait l'opération 	Chaque membre du groupe fait l'opération 

- Supprime la description du groupe et la photo de profil si elle est personnalisée
- Renomme le groupe
- Poste un message avec un délai éphémère de 5 minutes demandant à chaque personne de quitter puis supprimer le groupe de son côté
- Quitte le groupe
- Supprime le groupe (sans le bloquer : le groupe serait toujours lié à ton compte. S'il se fait récupérer, il pourrait être croisé avec les données d'autres comptes)



Cas des groupes et des conversations avec délai de suppression

Le déclenchement du délai de disparition d'un message commence uniquement à sa lecture effective. Par exemple, si une personne reçoit un message, mais qu'elle ne l'ouvre qu'une semaine après, le délai de disparition pour ce message ne commencera qu'à ce moment-là.

<https://signal.org/blog/disappearing-messages/>

Pour les métadonnées

Voir [Effacer ses métadonnées](#).

Pour les fichiers

Les mémoires flash (SSD, clef USB, mémoire de téléphone) ont un mécanisme interne qui rend compliqué de réécrire précisément sur le fichier que tu veux effacer :

<https://peterbabic.com/blog/how-not-to-securely-erase-nvme-drive/>.

Les meilleures options sont en prévention de chiffrer ton disque ([Chiffrer son ordinateur](#), [Avoir un téléphone chiffré et mis à jour](#)), ou de supprimer le fichier puis de remplir ta mémoire de données inutiles pour forcer le disque à écrire sur tout l'espace disponible (dont la place laissée par la suppression de ton fichier).

Supprimer définitivement un fichier est plus simple sur un disque dur magnétique (HDD).

Tu peux utiliser la commande suivante dans un terminal pour les supprimer de manière ciblée :

Bash

```
1 # Supprimer un fichier unique, change le chemin par ce que tu veux  
vraiment supprimer  
2 shred -vfuz -n 25 $HOME/Documents/fichier_a_supprimer  
3 # Supprimer tous les fichiers dans un dossier  
4 find $HOME/Documents/dossier_a_supprimer -depth -type f -exec shred -vfuz  
-n 25 {} \;  
5 find $HOME/Documents/dossier_a_supprimer -type d -empty -print -delete
```

[illegible]

! Pas de retour en arrière

Ces commandes suppriment définitivement les fichiers sans demander de confirmation !

Vérifie que ce sont bien les bons fichiers que tu veux supprimer !

Pour les dossiers

Pour supprimer les dossiers, utilise la commande suivante :

Bash

```
1 # Change le chemin par ce que tu veux vraiment supprimer
2 rm -rf /home/user/Documents/dossier_a_supprimer
```

```
[~ /Documents]% ls /home/user/Documents
dossier_a_supprimer
[~ /Documents]% rm -rf /home/user/Documents/dossier_a_supprimer
[~ /Documents]% ls /home/user/Documents
[~ /Documents]%
```

Cette commande permet de supprimer tout le contenu du dossier mais sans réécrire par-dessus les fichiers, ils sont donc potentiellement toujours retrouvables par une analyse forensique.

! Pas de retour en arrière

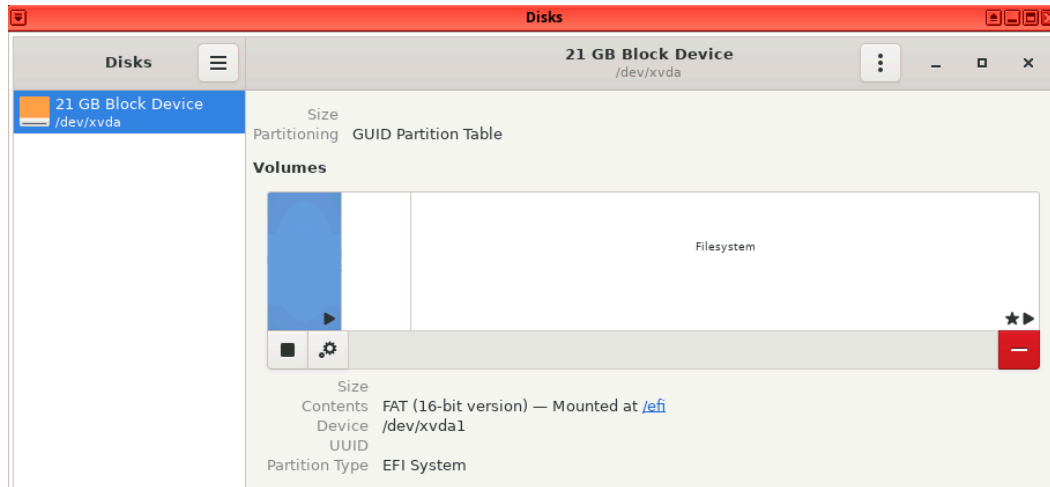
Ces commandes suppriment définitivement les dossiers sans demander de confirmation !

Vérifie que ce sont bien les bons dossiers que tu veux supprimer !

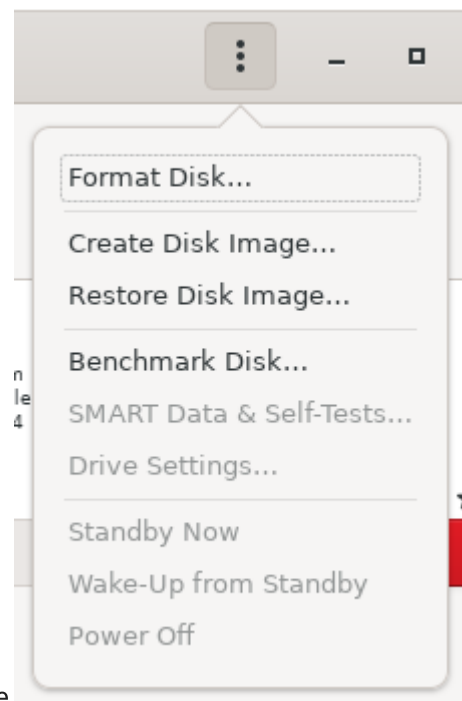
Pour les disques durs

Si tu peux te le permettre, il vaut mieux effacer complètement le disque dur. Il faut, dans l'ordre :

- Utilise GNOME Disks (<https://apps.gnome.org/DiskUtility/>, déjà disponible sur Tails)
- sélectionne le disque dur à effacer



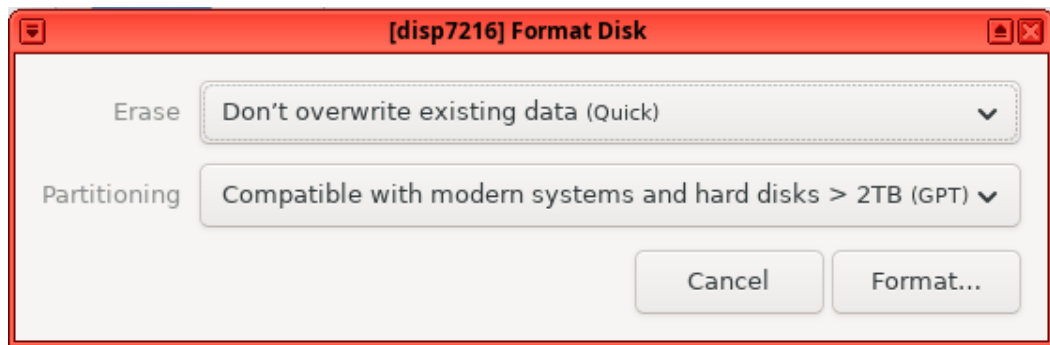
- Supprime le disque dur en activant l'option `Erase: Overwriting existing data with zeroes (Slow)`



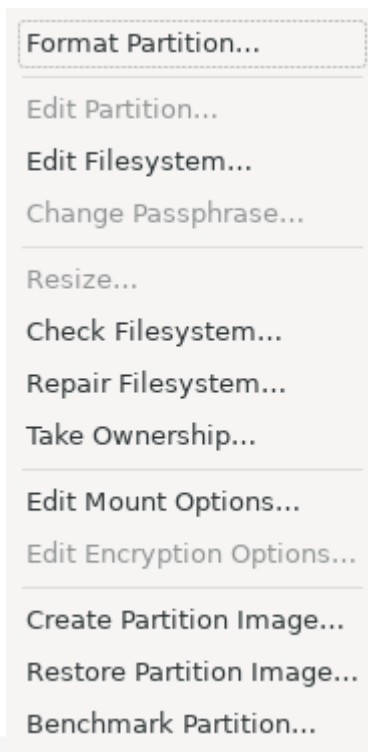
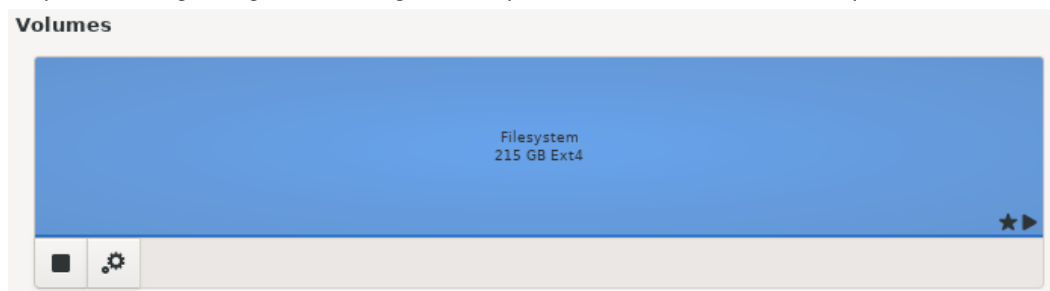
- clique sur les trois petits points en haut à droite

- clique sur `Format Disk`

- change l'option `Don't overwrite existing data (Quick)` en `Overwriting existing data with zeroes (Slow)`

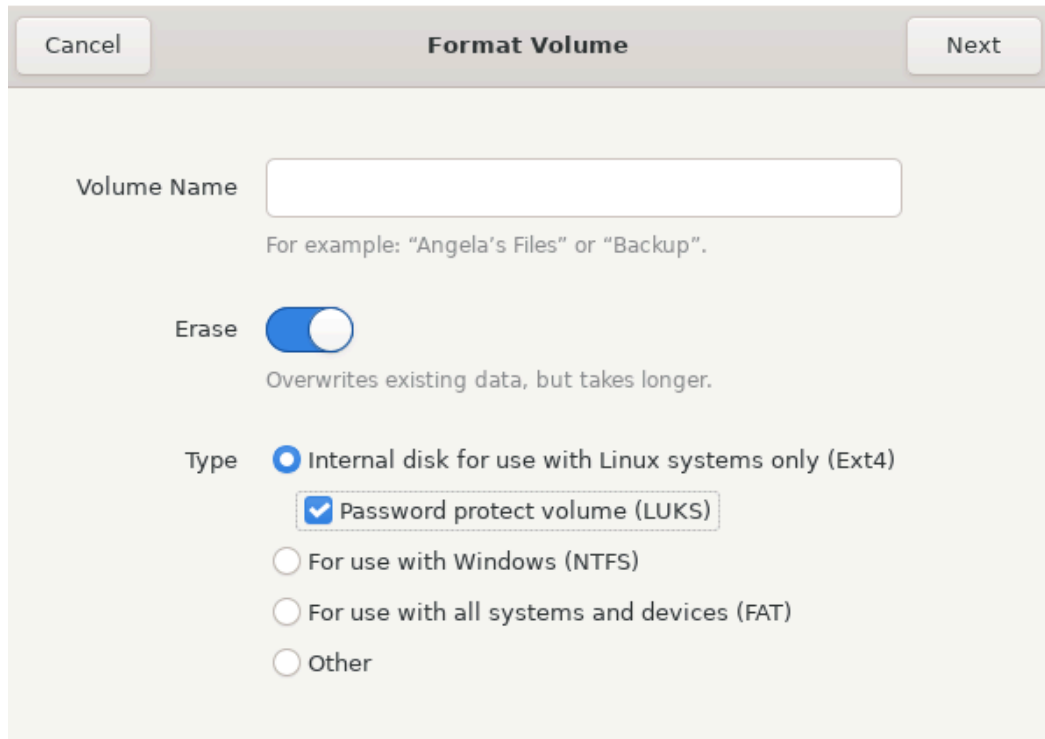


- clique sur `Format...`
- Crée une nouvelle partition chiffrée en activant l'option `Erase: Overwrites existing data, but takes longer`.
- clique sur l'engrenage en bas à gauche après avoir sélectionné le disque dur formaté



- clique sur `Format Partition...`

- active l'option **Erase**

A screenshot of the 'Format Volume' dialog box. It has a title bar with 'Cancel' and 'Next' buttons. The main area contains a 'Volume Name' text field with a hint 'For example: "Angela's Files" or "Backup"'. Below this is an 'Erase' toggle switch, which is turned on, with the text 'Overwrites existing data, but takes longer.' underneath. The 'Type' section has four radio button options: 'Internal disk for use with Linux systems only (Ext4)' (selected), 'Password protect volume (LUKS)' (checked with a checkbox), 'For use with Windows (NTFS)', 'For use with all systems and devices (FAT)', and 'Other'.

- lance le formatage du volume en cliquant sur **Next**

Suppression physique

Si tu peux et veux aller plus loin, après avoir supprimé numériquement les données, détruis physiquement les supports numériques compromettants, que ce soit avec un marteau, une scie à disque ou dans une source de chaleur très élevée 🔥, ou une combinaison de tout cela.

Un HDD semble plus fragile et "facile à détruire" ; un SSD semble plus compliqué de le faire avec certitude.

Information

Pour détruire des données sensibles, la NSA exige la destruction d'un SSD en parties de moins de 2mm, ce qui se fait bien avec un blender domestique.

<https://commons.erau.edu/jdfsl/vol16/iss2/1/>

— Pour aller plus loin

Quiz

Question 1

Sur un disque dur à plateaux (HDD), les données sont stockées

- ☐ dans des microtransistors
- ☐ dans la RAM
- ☐ par changement de magnétisme

Question 2

Pour supprimer un fichier en réécrivant 25 fois par-dessus, on utilise

- ☐ `dd`
- ☐ `rm -rf`
- ☐ `shred`

Question 3

La commande `rm -rf dossier` permet de

- ☐ réécrire le contenu du dossier avant de le supprimer
- ☐ chiffrer le dossier avant de le supprimer
- ☐ oublier le dossier sans réécrire par-dessus les fichiers

Question 4

Le délai de disparition d'un message Signal commence

- ☐ à la réception sur le serveur
- ☐ à la lecture effective du message
- ☐ à l'envoi du message

Question 5

Avant de supprimer un groupe Signal, il est recommandé de

- ☐ renommer le groupe, supprimer sa description et sa photo personnalisée
- ☐ supprimer le groupe **sans** le bloquer
- ☐ bloquer le groupe pour couper tout lien
- ☐ demander à chacun de quitter puis supprimer le groupe de son côté

Soumettre

Progression du quiz

0 / 5 questions répondues (0%)

0 correctes

2026-06-162026-10-17

Page citée par

-  [Effacer ses métadonnées](#) — Supprimer les métadonnées d'un fichier avant de le partager