



# Note technique

## Fichiers cachés

Sous un système d'exploitation Linux il est possible de créer des dossiers et des fichiers cachés c'est-à-dire qui n'est pas visible ni via l'interface graphique de notre environ. Pour créer un fichier caché il suffit que son nom commence par un point et le système d'exploitation comprendra qu'il s'agit d'un fichier caché.

Pour pouvoir afficher un fichier caché il faut utiliser la commande **ls -a** pour lister tous les dossiers et fichiers y compris ceux qui sont cachés. Pour afficher seulement les fichiers/dossiers cachés la commande **ls -d .\*** est recommandée.

## Foremost

Foremost est une application donnant la possibilité de récupérer des fichiers qui ont été effacé ou des fichiers disparus suite à un formatage de disque.

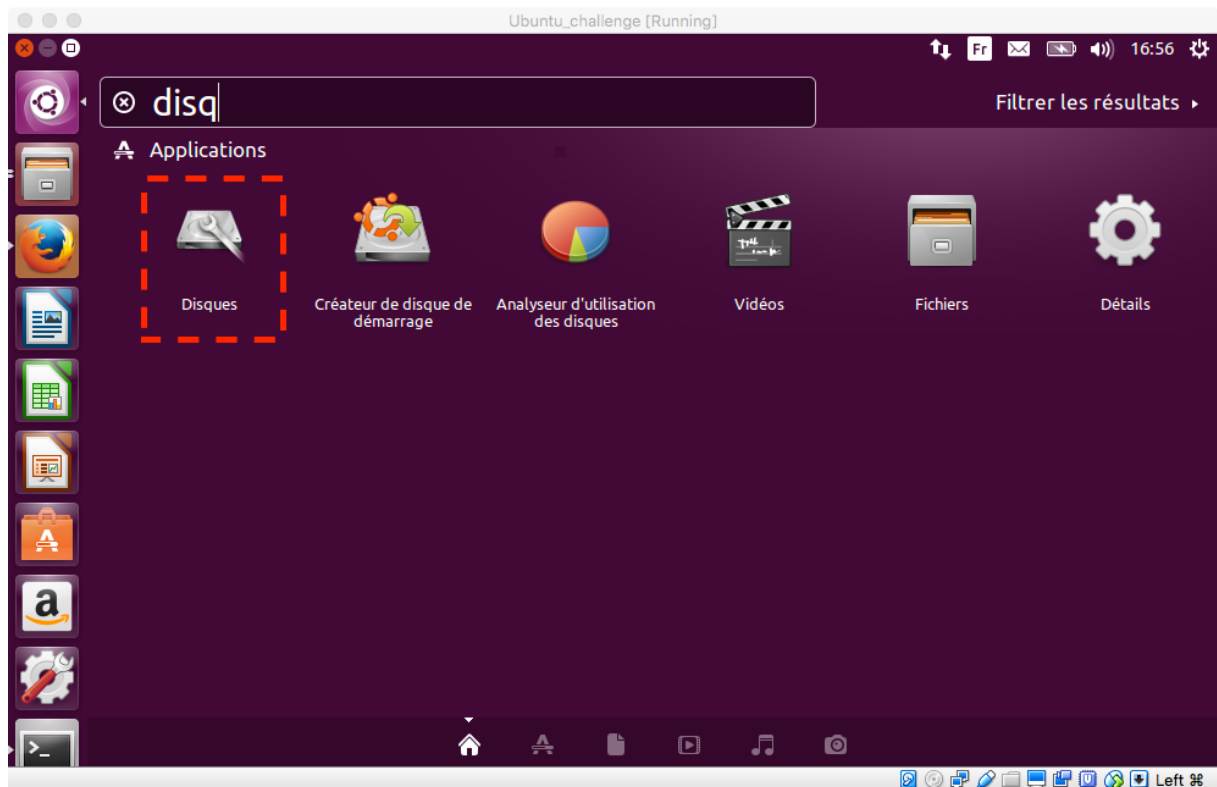
Il est possible de faire récupérer un fichier effacé car en vérité quand on supprime un document ce n'est pas l'objet lui même qui est supprimé mais seulement le lien qui mène à cet objet. Ce document sera effacé seulement quand il sera écrasé par d'autres données.

### Utilisation

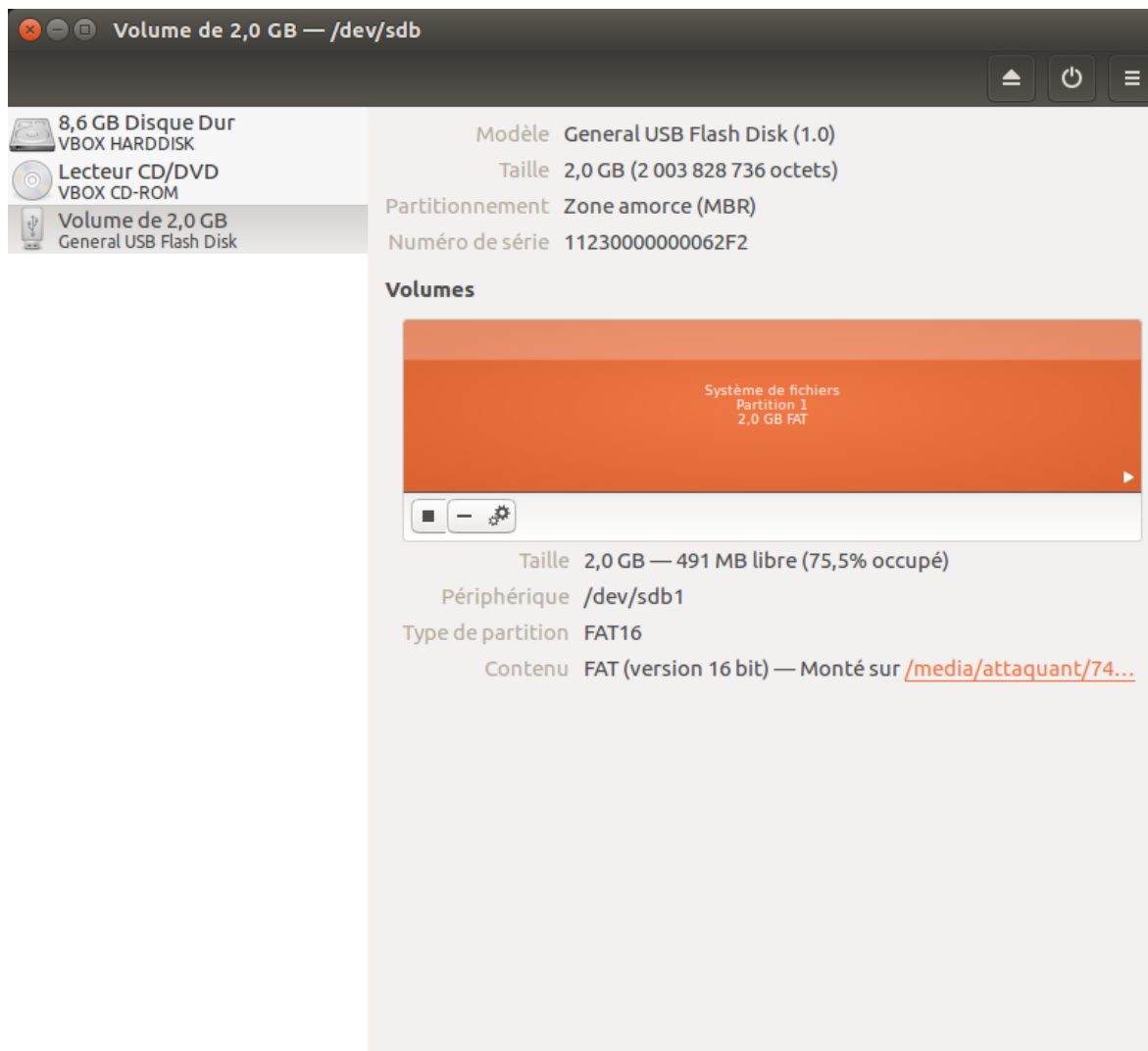
Pour connaître les types de fichiers que foremost peut récupérer sur votre clé USB par exemple il faut taper dans un terminal la commande :

**sudo foremost -w *chemin vers la clé USB***

Pour trouver le chemin vers votre appareil, dans notre exemple la clé USB, il faut ouvrir le gestionnaire de disque en tapant disque dans la barre de recherche d'Ubuntu.



Une fois l'application ouverte sélectionnez dans le menu de gauche votre appareil : toutes les informations lui étant relative s'affiche sur la droite dont son chemin dans le champ **Périphérique**.



Si vous voulez récupérer un type de fichier particulier, utilisez la commande suivante :

**`sudo foremost -t type de fichier -i chemin vers la clé USB`**

Par exemple : si je peux récupérer les images de ma clé USB je taperais la commande **`sudo foremost -t jpg -i /dev/sdb1`**

## ***Récupération des fichiers***

Une fois l'analyse de foremost fini, il mettra les documents qu'il a trouvé dans le dossier **output** dans votre home (chemin /output), attention si vous essayez de récupérer des éléments deux fois de suite grâce à foremost il faut supprimer le dossier output créé pour que foremost puisse réaliser une nouvelle fois l'opération.

/ ! \ Attention pour pouvoir y accéder il faut vous donner les droits avec la commande

**sudo chown -R attaquant output**

## **Le script stegano.py**

Le script stegano.py permet de faire cacher une image dans une image en modifiant les bits de poids faible de l'image 1 pour mettre les bits de poids forts de l'image 2.

Pour cacher l'image2.jpg dans l'image1.jpg il suffit de lancer le script avec la commande suivante :

***./stegano.py image1.jpg image2.jpg***

Pour récupérer une image il faut lancer la commande suivante, l'image qui était cachée sera alors nommée reveal.png :

***./stegano.py image\_modifié.jpg***