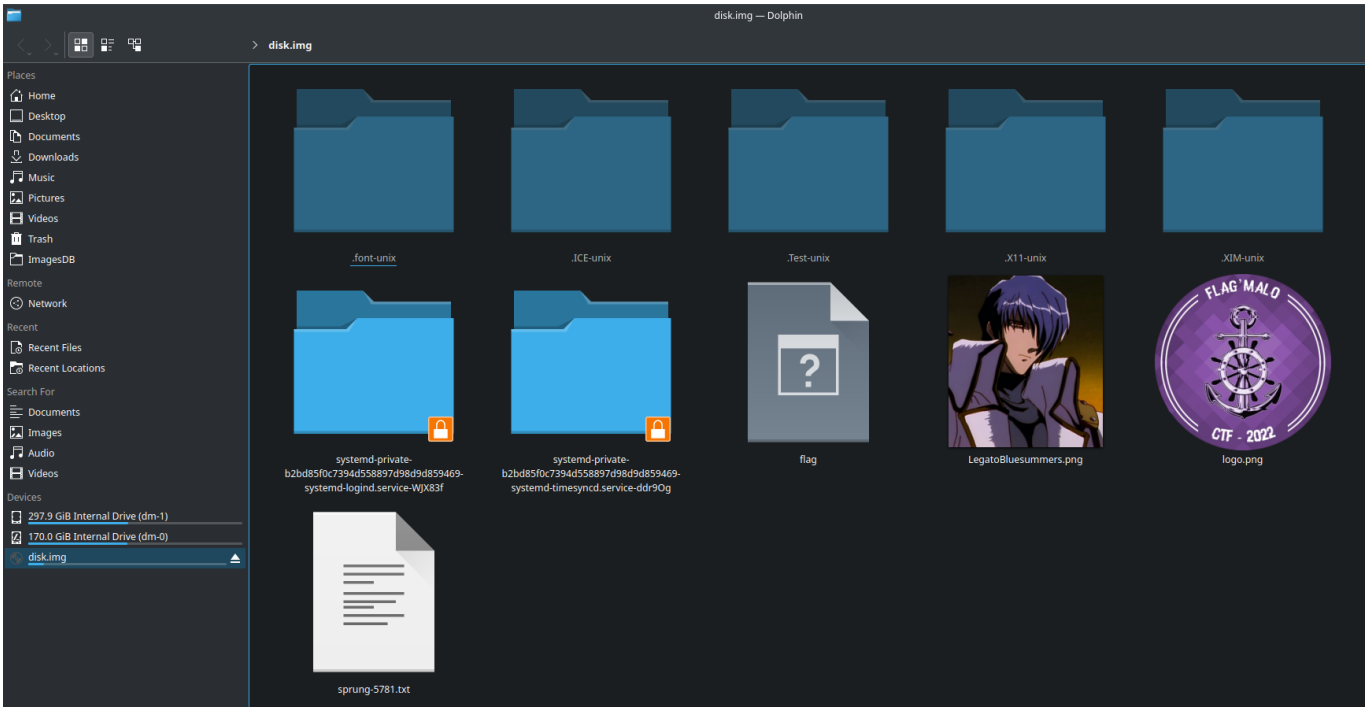
Del1337ed File

Auteur: bWlrYQ

1. Recon

On nous informe que notre flag a été supprimé mais qu'après la suppression une copie de la partition a été faite. Nous avons à notre diposition l'image disque de celle-ci.

On peut commencer par monter la partition avec `mkdir /home/mika/Desktop/deleted && sudo mount disk.img /home/mika/Desktop/deleted`. Cela va nous permettre d'en inspecter le contenu.



On ne remarque rien d'intéressant, le fichier flag ne contient que de la donnée illisible. Le fichier que l'on recherche a été supprimé, peut-on le récupérer ?

Ce qui est dit à l'utilisateur c'est qu'une fois supprimé le fichier n'est jamais récupérable, en réalité ça ne fonctionne pas comme ça. Un disque est un peu comme un compte rendu de TP, il y'a une table des matières et un numéro de page associé à la donnée que l'on cherche. Dans le cas d'un disque on a une sorte de table maîtresse qui contient le nom du fichier avec l'offset auquel on peut le trouver.

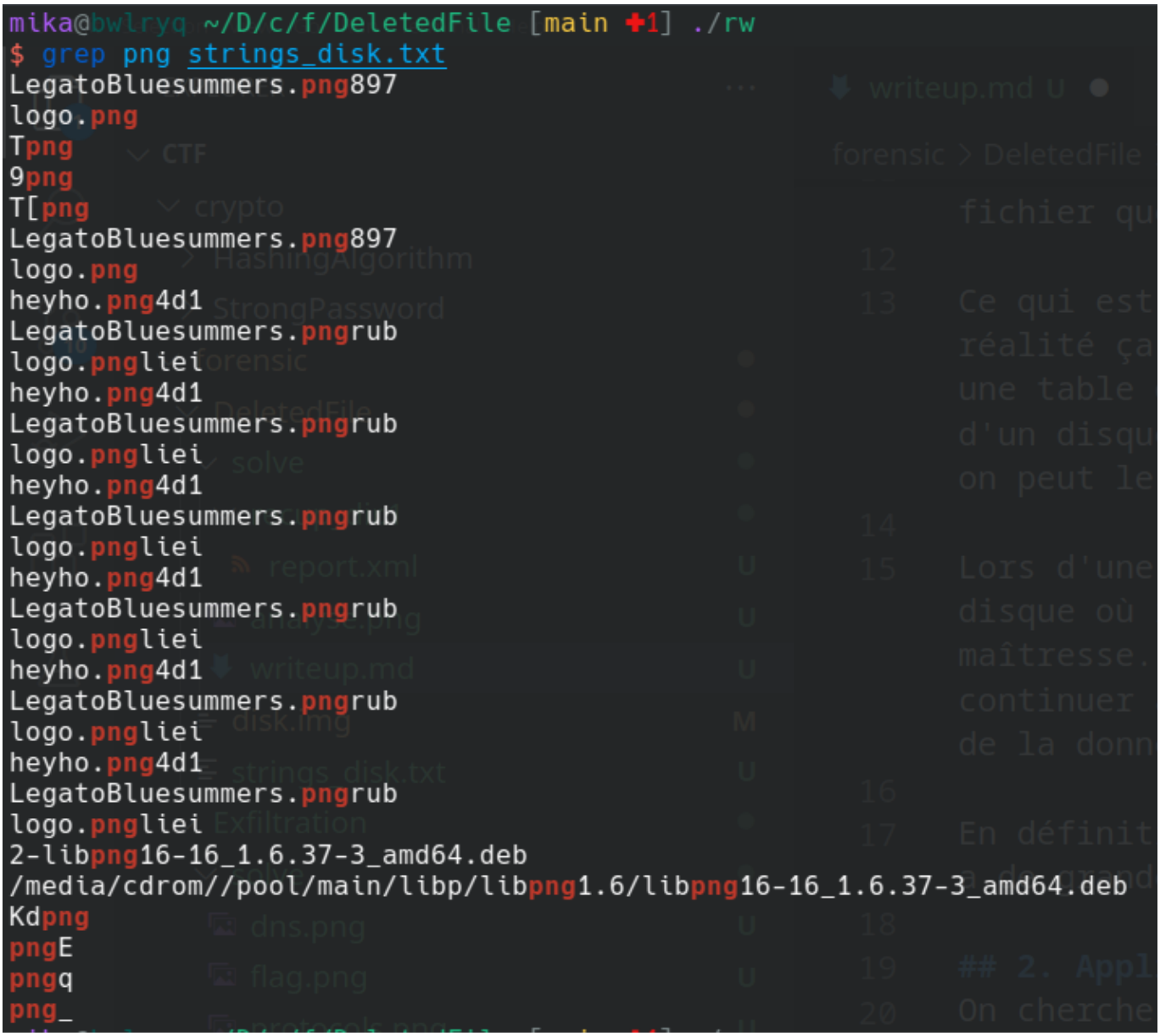
Lors d'une supression sur le disque, plutôt que d'effacer le fichier en réécrivant l'espace disque où il était avec des \x00 par exemple, on se contente d'effacer l'offset de la table maîtresse. Cela signifie que tant que le disque n'est pas plein le pointeur se contentera de continuer à écrire à la suite, en revanche une fois qu'il est plein il commmencera à écrire là où de la donnée a été supprimée par le passé.

En définitive, quand un fichier est supprimé par erreur, si on n'écrit plus rien sur le disqe, on a de grandes chances de pouvoir retrouver notre donnée perdue. On appelle cela le data carving.

2. Application à notre image disque

On cherche un fichier, pour confirmer la théorie vue plus haut, passons à la pratique. On peut d'abord extraire ce qui est "lisible" visuellement avec `strings disk.img > strings_disk.txt`.

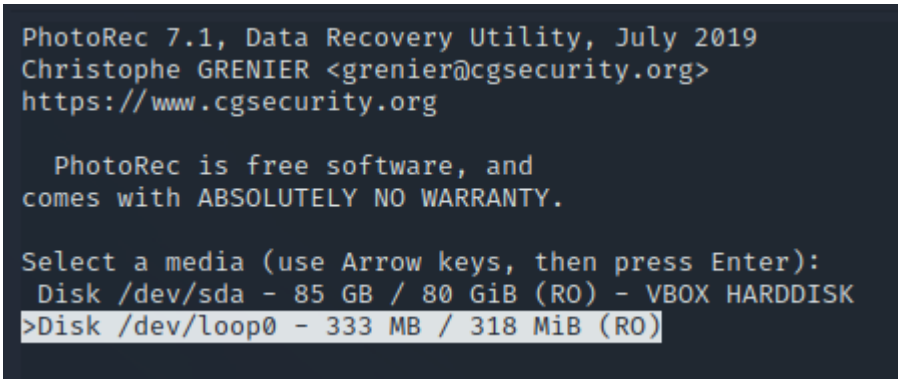
On peut ensuite utiliser grep sur des formats de fichiers connus (png, jpg, jpeg, txt, html, php...) Je vous épargne la liste mais quand on fait un `grep png strings_disk.txt` on obtient une sortie intéressante :



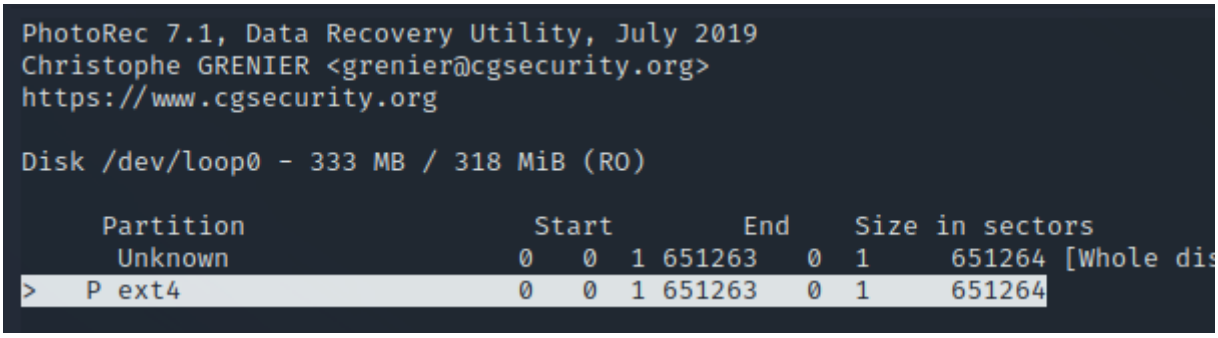
On voit un heyho.png, celui-ci n'est pas présent sur le disque monté. Cela signifie qu'il a été supprimé de la table maîtresse, mais qu'il est encore présent dans le disque. On va pouvoir essayer de le récupérer

Il existe de nombreux tools de data carving, dans notre cas le plus intéressant est photorec. Après installation on peut l'utiliser sur notre disque monté.

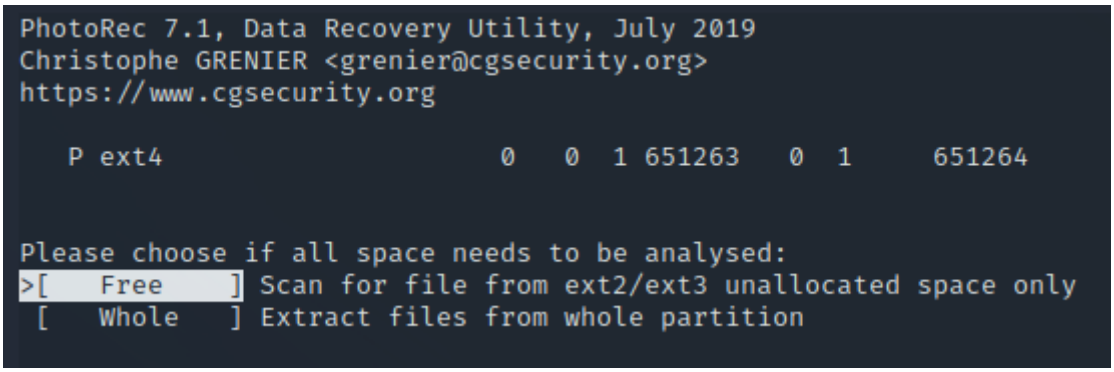
Dans un premier temps on sélectionne le disque monté qui nous intéresse



On choisit la partition du disque que l'on souhaite recouvrer



Puis uniquement l'espace libre car c'est ce qui nous intéresse



On valide la récupération de fichiers

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/loop0 - 333 MB / 318 MiB (RO)
     Partition                  Start        End    Size in sectors
   P ext4                     0   0  1 651263   0  1     651264


3 files saved in /home/kali/Desktop/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation

[ Quit ]
```

Enfin on profite de notre merveilleux flag !