Logiciel

Photorec : récupérer des données effacées ou perdues sur un disque défectueux

Introduction

Le logiciel en ligne de commande **Photorec** permet de récupérer tous types de fichiers sur un support endommagé (disque dur, SSD, clé USB, carte mémoire, etc.).

Ces problèmes sont le plus souvent liés à une mauvaise table d'allocation du disque ou à un mbr (master boot record) endommagé.

Photorec analyse la partition octet par octet pour récupérer les données.

Pré-requis

Installation

On installe le paquetage **Testdisk** qui contient le logiciel **Photorec**.

Installez le paquet **testdisk** ou en ligne de commande :

```
$ sudo apt install testdisk
```

Configuration

Utilisation

Photorec peut récupérer des fichiers sur une image de partition d'un disque faite par exemple avec la commande **dd**.

> Il est vivement conseillé de faire une image du disque défectueux et d'utiliser **Photorec** sur cette image pour éviter de perdre des données si le disque rend l'âme en cours de scan.

Syntaxe:

```
$ sudo photorec [image_disque]
```

exemple :

```
$ sudo photorec ~/image.dd
```

Donc lancez **Photorec** dans le terminal :

```
$ sudo photorec
```

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk /dev/sda - 1000 GB / 931 GiB (RO) - HGST HTS541010A9E680
 Disk /dev/sdb - 1000 GB / 931 GiB (RO) - ST1000LM024 HN-M101MBB
 Disk /dev/sdc - 1000 GB / 931 GiB (RO) - HGST HTS541010A9E680
 Disk /dev/sdd - 1000 GB / 931 GiB (RO) - HGST HTS541010A9E680
 Disk /dev/sde - 1000 GB / 931 GiB (RO) - HGST HTS541010A9E680
 Disk /dev/sdf - 2000 GB / 1862 GiB (RO) - H/W RAID 10




>[Proceed ]  [  Quit  ]

Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

Déplacez-vous avec les flèches :

- ↑ et ↓ pour choisir le disque où il y a des données à récupérer.
- ← et → pour choisir dans le menu en bas de l'écran (ici, Proceed / Quit).

Choisissez **Proceed** et appuyer sur la touche ↵ Entrée.

Choisissez le type de la table de partition (Photorec sélection automatiquement le bon type). Dans notre exemple ce sera de type “Intel”.

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 1000 GB / 931 GiB (RO) - HGST HTS541010A9E680
```

```
     Partition                  Start        End    Size in sectors
      No partition             0   0  1 121601  80 63 1953525168 [Whole
disk]
> 1 * Linux                    0  32 33  6450 185 50  103628907
  2 P Linux Swap            6450 216 39  6973   4  7    8388608
  3 P Linux                 9583 216 42 95492 194 62 1380126720 [home]
  4 E extended             95493   4 62 98103 217 34   41943042
  5 L Linux                95493   5  1 98103 217 34   41943040

>[ Search ]  [Options ]  [File Opt]  [  Quit  ]
                                Start file recovery
```

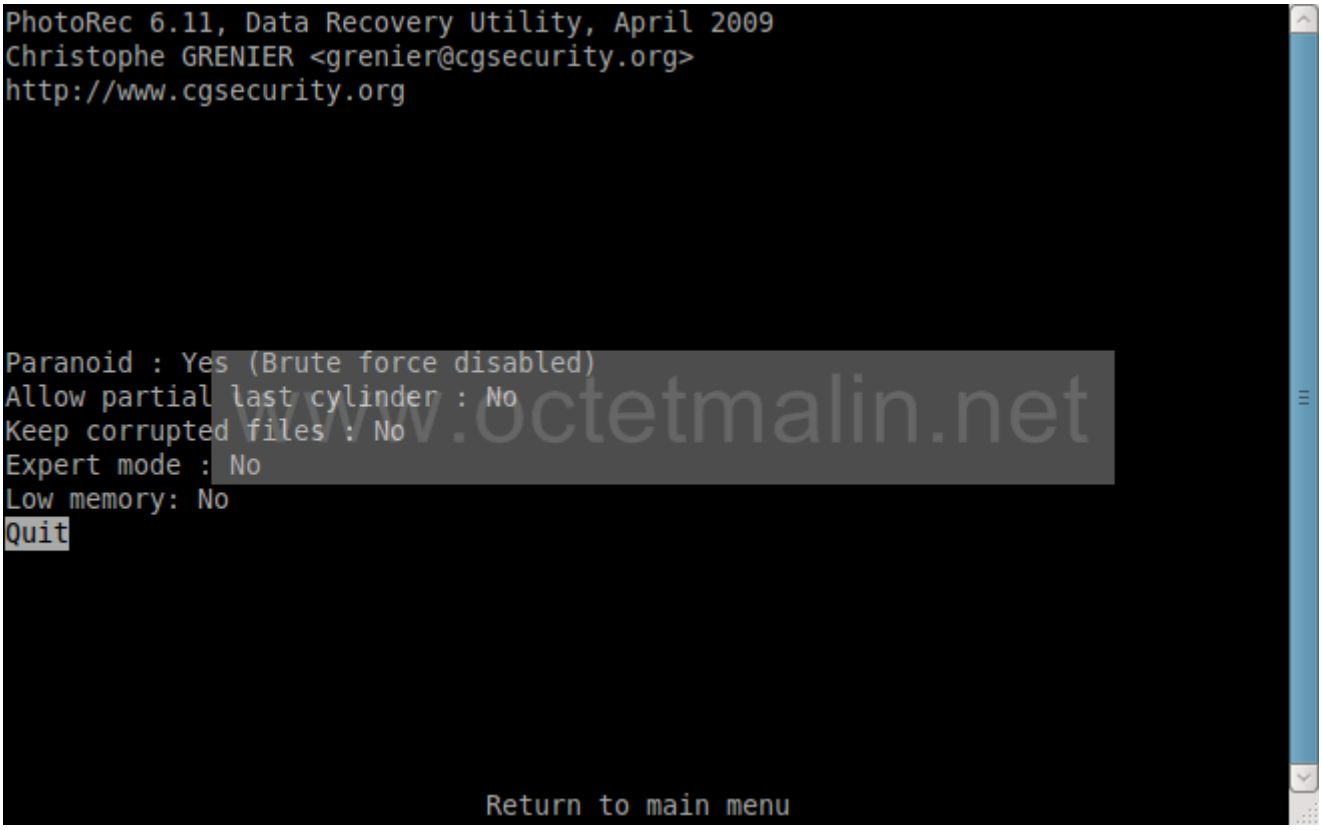
```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

 1 * Linux                    0  32 33  6450 185 50  103628907

To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
>[ ext2/ext3 ] ext2/ext3/ext4 filesystem
 [ Other     ] FAT/NTFS/HFS+/ReiserFS/...
```

Maintenant la table de partition s'affiche, il faut choisir la partition où il y a les données à récupérer. Dans cette exemple ce sera la partition numéro 7 au format NTFS. Mais avant de passer a la suite en choisissant “Search” dans le menu en bas, nous allons voir les “Options”.

```
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 80 GB / 74 GiB (RO) - ATA SAMSUNG HM080HC

     Partition                  Start        End    Size in sectors
     No partition             0   0  1  9729  80 63  156301488 [Whole disk]
 1 P Linux                    0  32 33  4255  57 26   68358144
 2 P Linux Swap            4255  57 27  4407  46 55    2441216
 3 * Linux                 4407  46 56  6230 207 57   29296640
 4 E extended              6230 241 23  6413  61 48    2928581
 5 L Linux                 6230 241 25  6249 254 63     306093
   X extended              6250   0  1  6319 254 63    1124550
 6 L Linux                 6250   1  1  6319 254 63    1124487
   X extended              6320   0  1  6413  61 48    1497936
 7 L HPFS - NTFS           6320  45 62  6413  61 48    1495040 [toto]

[ Search ]  [Options ]  [File Opt]  [  Quit  ]
                                Start file recovery
```

Voici le détail des options disponibles: Paranoid ⇒ Par défaut sur “Yes”, mettre sur “No” pour activer le mode brute force pour récupérer plus de fichier (beaucoup plus long). Allow partial last cylinder ⇒

Par défault sur “No”, permet de modifier la façon de lire le disque, mais cette option n'est utile que pour les disques non partitionnés. Keep corrupted files ⇒ Par défault sur “No”, cette option mit sur “Yes” permet de récupérer les fichiers même si ils sont endommagés. Expert mode ⇒ Par défault sur “No” cette option permet de forcer la taille des blocs (clusters). Low memory ⇒ Par défault sur “No”, cette option permet d'utiliser moins de mémoire dans le cas où votre système planterait durant son utilisation.



La section “File Opt” permet de choisir les types de formats de fichiers que vous voulez récupérer. Pour sélectionner ou désélectionner un format utilisez la touche “Espace”, vous pouvez aussi sélectionner ou désélectionner d'un coup tous les types avec la touche “s”, et après appuyer sur la touche “b” pour sauvegarder les nouveaux paramètres.

```
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec will try to locate the following files

[X] 7z   7zip archive file
[X] DB
[X] a    Unix Archive/Debian package
[X] abcdp Apple binary property list
[X] accdb Access Data Base
[X] ace  ACE archive
[X] ab   MAC Address Book
[X] ahn  Ahnenblatt
[X] aif  Audio Interchange File Format
[X] all  Cubase Song file: .all
[X] als  Ableton Live Sets
[X] amd  AlphaCAM (amd/amt/atd/att)
[X] amr  Adaptive Multi-Rate
[X] apa  APA Style Helper
    Next
Press s to disable all file famillies, b to save the settings
[  Quit  ]
                              Return to main menu
```

www.octetmalin.net

Ici il faut choisir le type de formatage de la partition, soit “ext2, ext3 et ext4” ou bien tous les autres types de formats comme le FAT16, FAT32, NTFS, HFS+, ReiserFS … Photorec choisi automatiquement le bon type de formatage, ici on choisira “Other” pour notre partition en NTFS.

```
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

 7 L HPFS - NTFS          6320  45 62  6413  61 48    1495040 [toto]

To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
[ ext2/ext3 ]  ext2/ext3/ext4 filesystem
[ Other     ]  FAT/NTFS/HFS+/ReiserFS/...
```

www.octetmalin.net

On peut choisir l'étendu à analyser, soit “Free” pour analyser que l'espace disque de libre ou bien “Whole” pour extraire des données sur toute la partition, c'est à dire l'espace libre et l'espace utilisé.

```
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

 7 L HPFS - NTFS          6320  45 62  6413  61 48    1495040 [toto]


Please choose if all space need to be analysed:
[   Free    ]  Scan for file from NTFS unallocated space only
[   Whole   ]  Extract files from whole partition
```

www.octetmalin.net

Maintenant il faut choisir l'emplacement ou sera sauvegardé tous les fichiers qui seront récupérés. PS: Attention ne surtout pas sauvegarder sur la partition que vous allez analyser au risque d'écrire sur les données que vous voulez récupérer. Utilisez la flèche de gauche et de droite pour remonter ou entrez dans un répertoire puis appuyez sur la touche “Y” pour enregistrer le répertoire de sauvegarde.

```
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Do you want to save recovered files in /home/cedric/recuperation ? [Y/N]
Do not choose to write the files to the same partition they were stored on.

To select another directory, use the arrow keys.
drwxrwxr-x  1000  1000      4096 17-Feb-2012 20:22 .
drwxr-xr-x  1000  1000      4096 17-Feb-2012 20:22 ..
```

www.octetmalin.net

Photorec est maintenant en train de récupérer les fichiers sur le disque. Il affiche au fur et à mesure le nombre de fichiers qui son récupérés, il affiche aussi le nombre d'octets actuellement scanné et

affiche une estimation du temps restant pour finir la tâche.

```
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 80 GB / 74 GiB (RO) - ATA SAMSUNG HM080HC
     Partition                  Start        End    Size in sectors
 7 L HPFS - NTFS           6320  45 62  6413  61 48    1495040 [toto]


Pass 1 - Reading sector     618880/1495040, 1479 files found
Elapsed time 0h00m23s - Estimated time for achievement 0h00m32
png: 877 recovered
txt: 262 recovered
tx?: 116 recovered
gz: 110 recovered
gif: 38 recovered
jpg: 30 recovered
sqlite: 23 recovered
MYI: 9 recovered
zip: 7 recovered
a: 4 recovered
others: 3 recovered
  Stop
```

www.octetmalin.net

Voici une fois le scan fini, il affiche le nombre total de fichiers récupérés ainsi que l'emplacement de sauvegarde.

```
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 80 GB / 74 GiB (RO) - ATA SAMSUNG HM080HC
     Partition                  Start        End    Size in sectors
 7 L HPFS - NTFS           6320  45 62  6413  61 48    1495040 [toto]


4957 files saved in /home/cedric/recuperation/recup_dir directory.
Recovery completed.
png: 1795 recovered
txt: 1529 recovered
tx?: 477 recovered
gz: 461 recovered
gif: 208 recovered
MYI: 109 recovered
jpg: 101 recovered
elf: 80 recovered
sqlite: 46 recovered
a: 36 recovered
others: 115 recovered
[ Quit ]
```

www.octetmalin.net

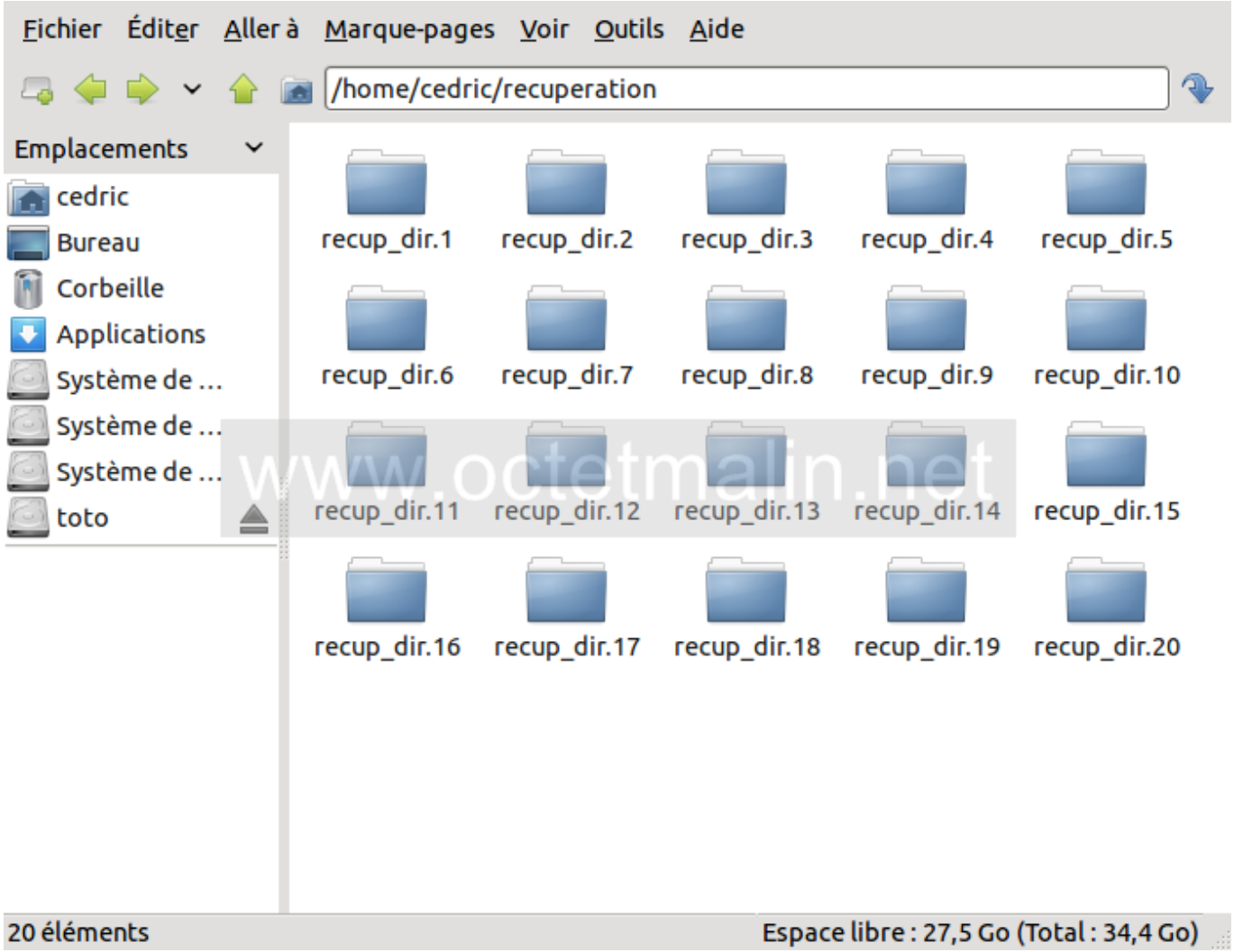
Pour accéder a vos fichiers depuis un compte utilisateur normal, vous devrez changer les droits en changeant le propriètaire du répertoire ainsi que sont contenu avec la commande chown. Dans notre

exemple se sera :

```
...@...:~ $ chown -R cedric:cedric /home/cedric/recuperation
```

Voir ce tutoriel pour utiliser la commande “chown”: chown - Changer le propriétaire et le groupe d'un fichier ou dossier en ligne de commande

Maintenant vous remarquerez que des sous-dossiers se sont crée dans votre répertoire de sauvegarde nommé “recup_dir.1, recup_dir.2 ...” chacun d'eux contient 500 fichiers qui ont été récupéré.



Désinstallation

Voir aussi

- **(fr)** http://www.octetmalin.net/linux/tutoriels/photorec.php

---

Basé sur « Article » par Auteur.

From:
https://nfrappe.fr/doc-0/ - **Documentation du Dr Nicolas Frappé**

Permanent link:
https://nfrappe.fr/doc-0/doku.php?id=logiciel:systeme:photorec:start

Last update: **2022/08/13 21:57**