

PhotoRec Etape par Etape - CGSecurity

Ce manuel de PhotoRec vous guide à travers PhotoRec étape par étape pour récupérer des fichiers effacés ou les fichiers d'une partition dont le système de fichiers est corrompu ou a été reformaté. Les traductions de ce manuel d'utilisation de PhotoRec vers d'autres langues sont les bienvenues.

Exécuter PhotoRec

Si PhotoRec n'est pas encore installé, téléchargez-le depuis Télécharger TestDisk. Extraire les fichiers de l'archive, y compris les sous répertoires.

Pour récupérer des fichiers de disques durs, clés USB, Smart Card, cdrom, dvd..., vous devez avoir suffisamment de droits pour accéder directement aux périphériques.

-



Sous Dos, exécuter `photorec.exe`

-



Sous Windows, exécuter PhotoRec (par exemple, `testdisk-6.13/photorec_win.exe`) depuis un compte dans le groupe Administrateur. Sous Windows Vista et suivant, utiliser le clic droit `run as administrator` pour lancer PhotoRec.

-



Sous Unix/Linux/BSD, vous avez besoin d'être root pour exécuter PhotoRec (par exemple, `sudo testdisk-6.13/photorec_static`)

-

X

Sous MacOSX, si vous n'êtes pas root, PhotoRec (par exemple, `testdisk-6.13/photorec`) va se redémarrer lui-même en utilisant `sudo` après confirmation de votre part. `sudo` vous demande votre mot de passe utilisateur.

-



Sous OS/2, PhotoRec ne gère pas les périphériques physiques, uniquement les images disques, désolé.

Pour récupérer des fichiers depuis une image disque, utiliser

- `photorec image.dd` pour analyser une image brute d'un disque (raw image)
- `photorec image.E01` pour récupérer des fichiers depuis une image Encase EWF
- `photorec 'image.E*'` si l'image Encase est découpée en plusieurs fichiers.



X

Pour récupérer des fichiers d'autres périphériques, exécuter `photorec périphérique`, par exemple:

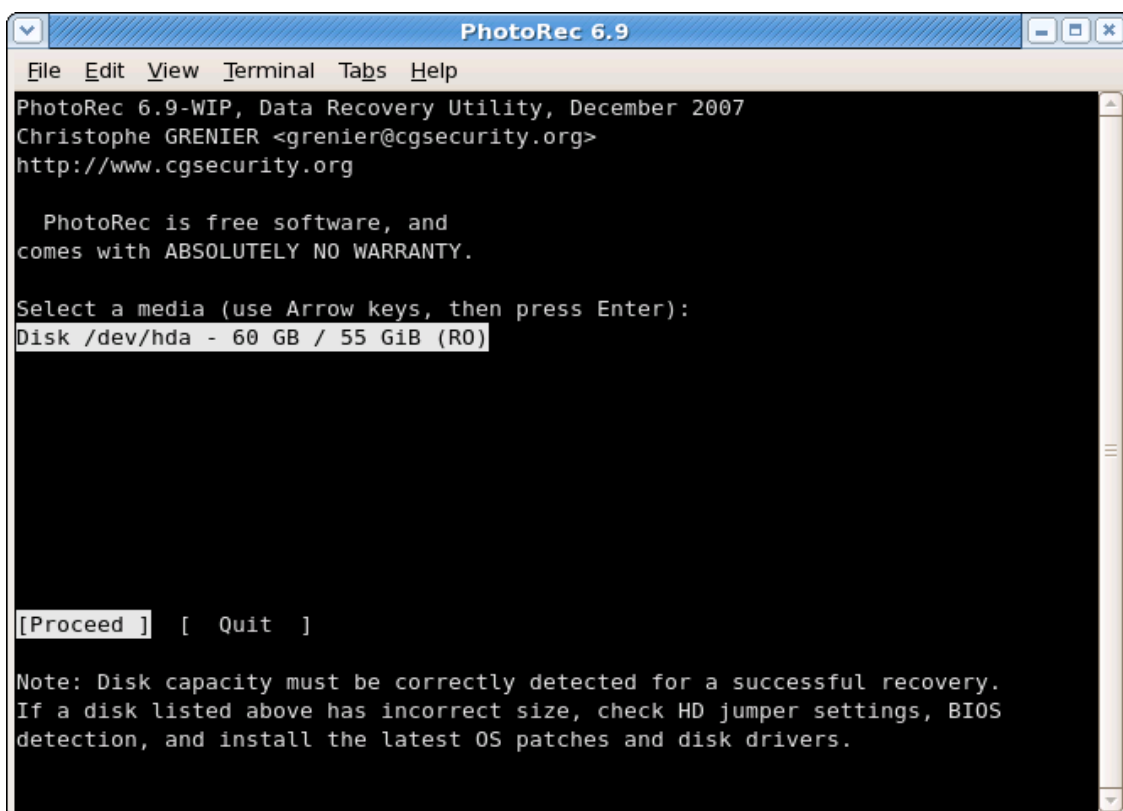
- `photorec /dev/mapper/truecrypt0` pour récupérer des fichiers depuis une partition TrueCrypt. La même méthode

s'applique aussi aux systèmes de fichiers chiffrés par cryptsetup/dm-crypt/LUKS.

- `photorec /dev/md0` pour récupérer des fichiers depuis un RAID logiciel sous Linux.

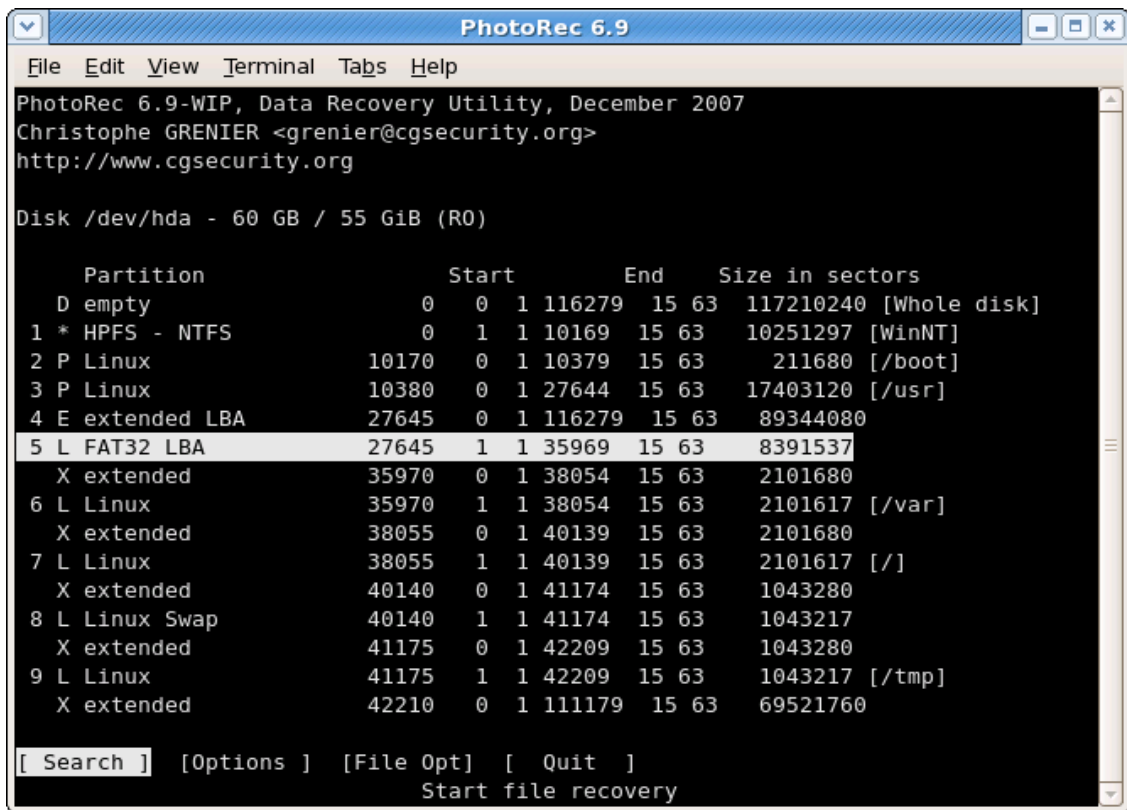
Pour des investigations numériques, utiliser le paramètre `/log` pour créer un fichier de log nommé `photorec.log`; il contient l'emplacement des fichiers récupérés par PhotoRec.

Sélection du disque



Les médias (disque dur, cdrom...) sont listés. Utiliser les touches fléchées haut/bas pour sélectionner le disque contenant les fichiers perdus. Appuyer sur la touche `Entrée` pour continuer.

Sélection de la partition source



PhotoRec 6.9-WIP, Data Recovery Utility, December 2007
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

Disk /dev/hda - 60 GB / 55 GiB (R0)

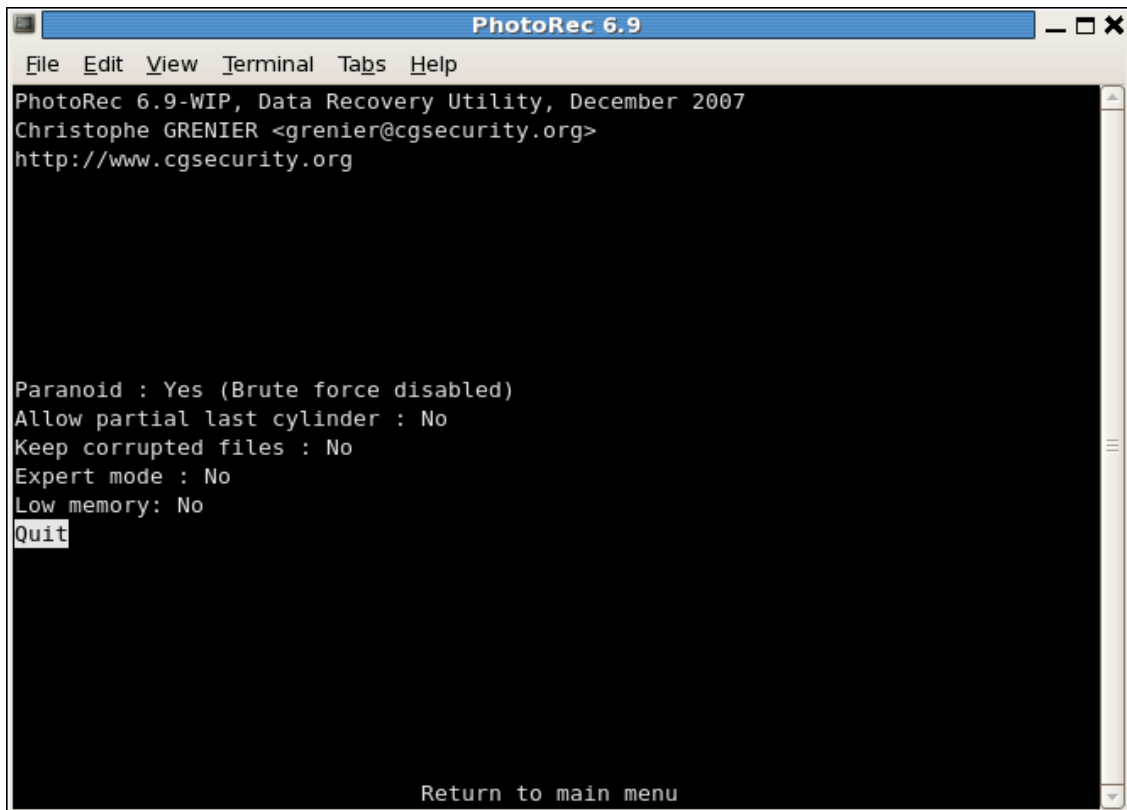
Partition	Start	End	Size in sectors
D empty	0 0 1 116279	15 63	117210240 [Whole disk]
1 * HPFS - NTFS	0 1 1 10169	15 63	10251297 [WinNT]
2 P Linux	10170 0 1 10379	15 63	211680 [/boot]
3 P Linux	10380 0 1 27644	15 63	17403120 [/usr]
4 E extended LBA	27645 0 1 116279	15 63	89344080
5 L FAT32 LBA	27645 1 1 35969	15 63	8391537
X extended	35970 0 1 38054	15 63	2101680
6 L Linux	35970 1 1 38054	15 63	2101617 [/var]
X extended	38055 0 1 40139	15 63	2101680
7 L Linux	38055 1 1 40139	15 63	2101617 [/]
X extended	40140 0 1 41174	15 63	1043280
8 L Linux Swap	40140 1 1 41174	15 63	1043217
X extended	41175 0 1 42209	15 63	1043280
9 L Linux	41175 1 1 42209	15 63	1043217 [/tmp]
X extended	42210 0 1 111179	15 63	69521760

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

Choisir

- Search après avoir sélectionné la partition contenant les fichiers perdus pour commencer la recherche.
- Options pour modifier les options.
- File Opt pour modifier la liste des types de fichiers récupérés par PhotoRec.

Les options de PhotoRec

A screenshot of the PhotoRec 6.9 terminal window. The window title is "PhotoRec 6.9". The menu bar includes "File", "Edit", "View", "Terminal", "Tabs", and "Help". The main content area shows the following text:

```
PhotoRec 6.9-WIP, Data Recovery Utility, December 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Paranoid : Yes (Brute force disabled)
Allow partial last cylinder : No
Keep corrupted files : No
Expert mode : No
Low memory: No
Quit
```

At the bottom of the terminal, there is a prompt "Return to main menu".

- `Paranoid` Par défaut, les fichiers récupérés sont vérifiés et les fichiers invalides rejetés.

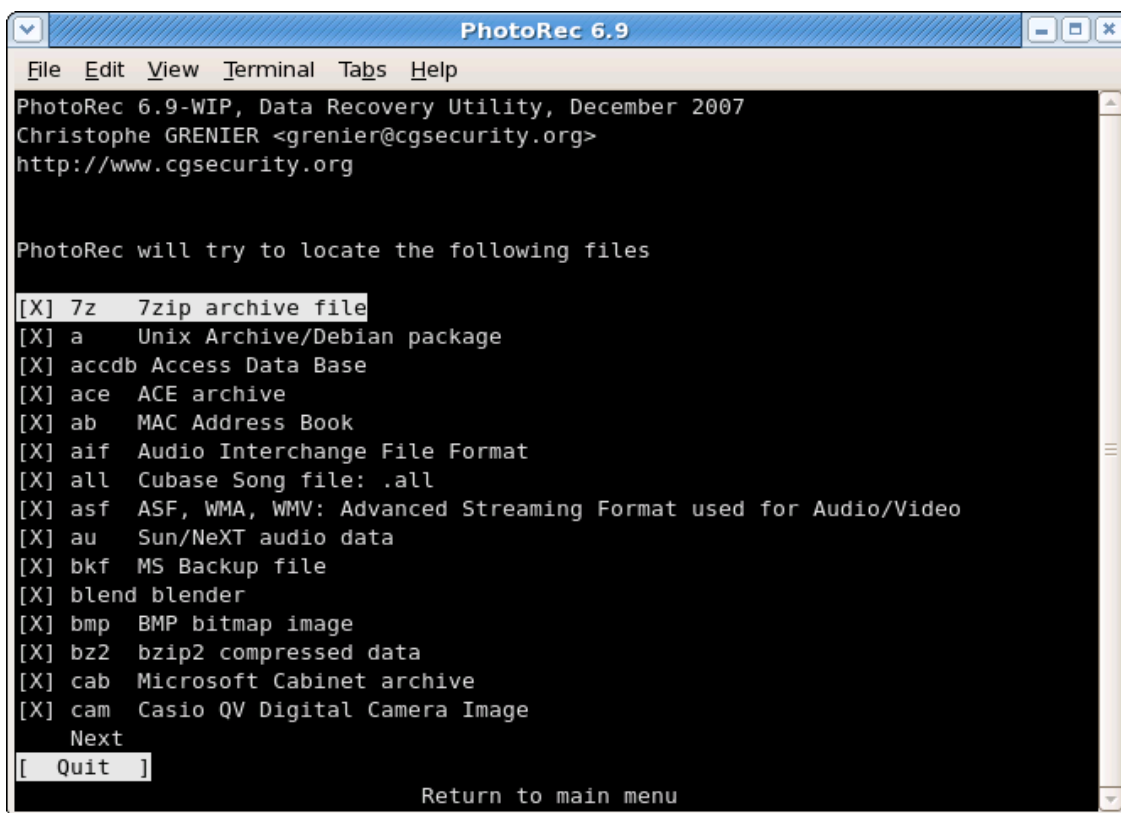
Activer le `bruteforce` si vous souhaitez récupérer plus de fichiers JPEG fragmentés, attention, cela nécessite beaucoup de ressource processeur.

- `Allow partial last cylinder` modifie la façon dont la géométrie du disque est déterminée, cela n'affecte que les volumes non partitionnés.
- L'option `expert mode` permet à l'utilisateur de forcer la taille de bloc utilisé (en principe, taille des clusters ou équivalent) et l'offset. Chaque système de fichier a ses propres valeurs par la taille des blocs (un multiple de la taille des secteurs) et pour l'offset (0 pour les systèmes de fichiers NTFS, exFAT, ext2/3/4), ces valeurs sont définies lors du formatage, lors de la création du système de fichier. Quand on travaille sur le disque entier (par exemple, si les partitions sont perdues) ou une partition reformaté, si PhotoRec retrouve peu de fichiers,

on peut essayer comme taille de bloc la valeur minimale que PhotoRec propose (il s'agit de la taille d'un secteur (0 sera alors utilisé pour l'offset).

- Activer l'option `Keep corrupted files` pour garder les fichiers récupérés même s'ils sont endommagés dans l'espoir qu'ils puissent être réparés par d'autres outils.
- Utiliser `Low memory` si votre système n'a pas assez de mémoire et plante durant la récupération de données. Cela ne devrait être nécessaire que pour des systèmes de fichiers très volumineux et très fragmentés. N'utiliser cette option que si cela est absolument nécessaire.

Sélection des formats de fichiers à récupérer

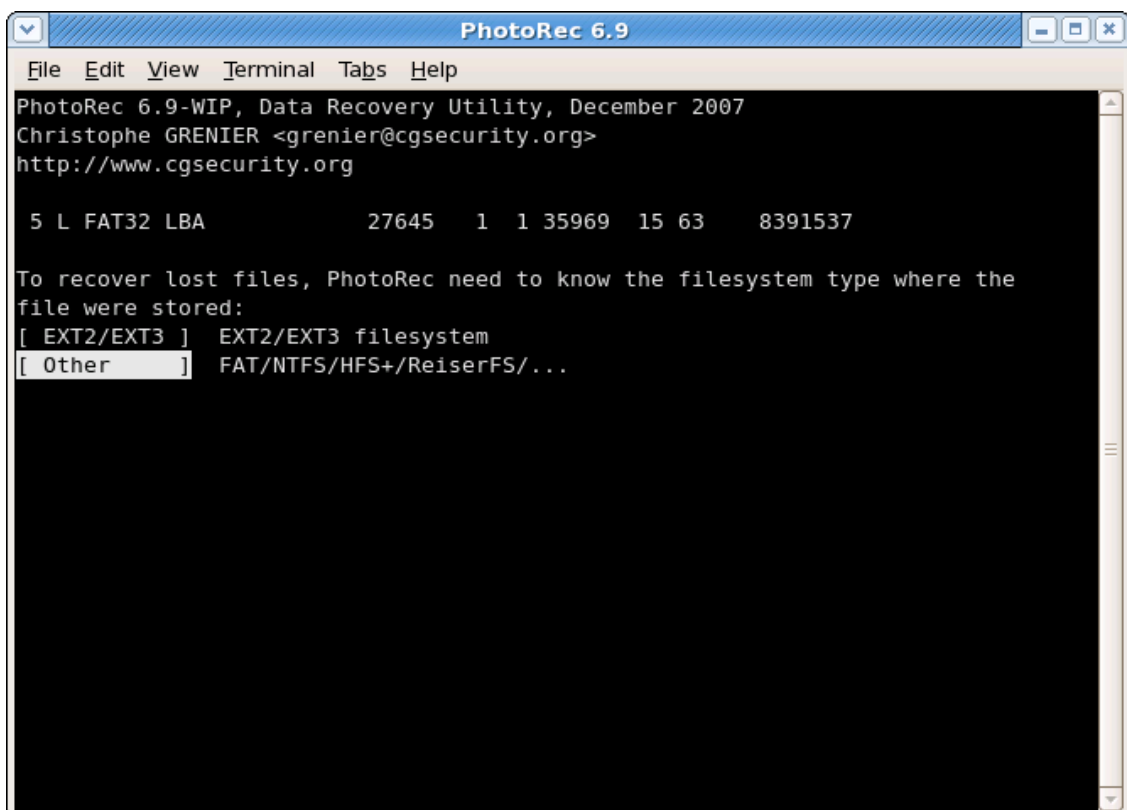


Activer ou désactiver la récupération de certains types de fichier, par exemple

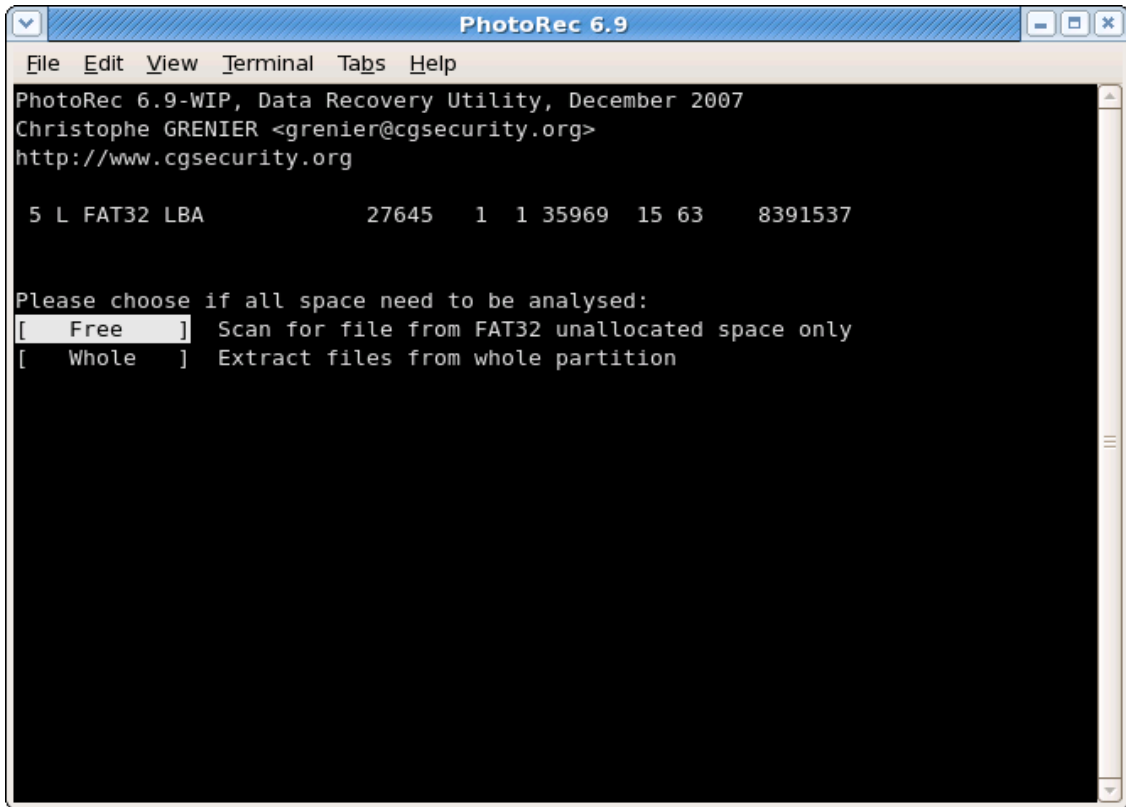
```
[X] tif Tag Image File Format and some raw file formats (pef/nef/dcr/sr2/cr2)
```

... [X] zip zip archive including OpenOffice and MSOffice 2007
</pre> La famille `tif` permet aussi la récupération des images raws `pef/nef/dcr/sr2/cr2`, la famille des archives `zip` inclus aussi les fichiers OpenOffice et Microsoft Office 2007. La liste complète des formats de fichier récupérés par PhotoRec comporte plus de 100 familles de fichiers représentant plus de 180 extensions de fichiers.

Type de système de fichier



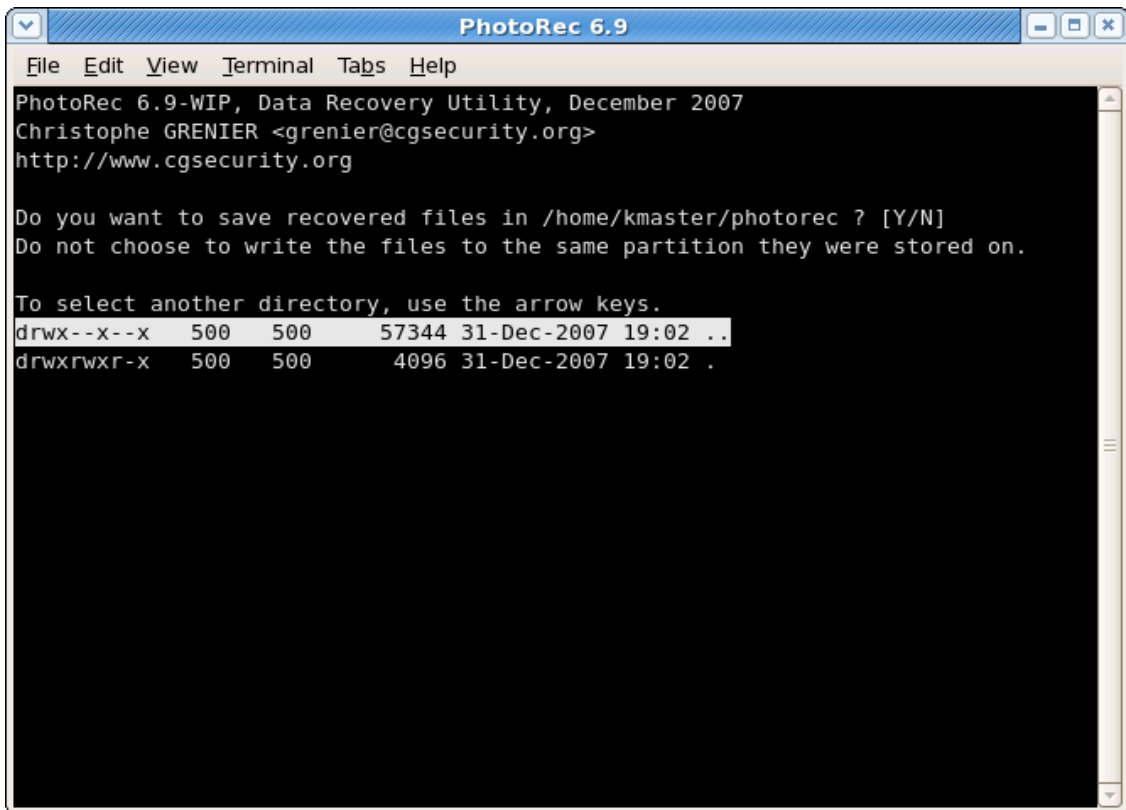
Une fois la partition sélectionnée, auto détection a besoin de connaître comment les blocs de données sont alloués. A moins qu'un système de fichier `ext2/ext3` soit utilisé, choisissez `Other`.



PhotoRec peut rechercher les fichiers

- sur l'intégralité de la partition (utile si le système de fichier est particulièrement corrompu) ou bien
- uniquement depuis l'espace non alloué (Disponible pour les systèmes de fichiers ext2/ext3, FAT12/FAT6/FAT32 et NTFS). Avec cette option, seuls les fichiers effacés seront récupérés.

Sélection de la destination des fichiers récupérés



```
PhotoRec 6.9-WIP, Data Recovery Utility, December 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

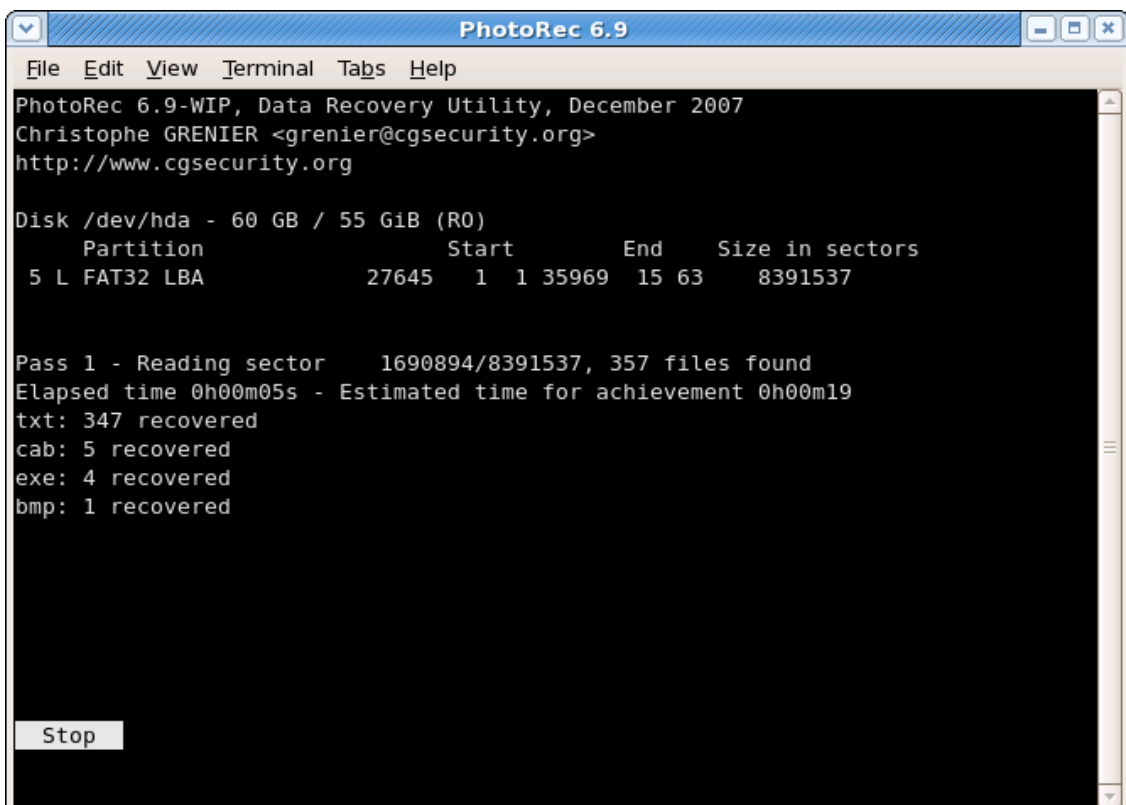
Do you want to save recovered files in /home/kmaster/photorec ? [Y/N]
Do not choose to write the files to the same partition they were stored on.

To select another directory, use the arrow keys.
drwx--x--x  500  500  57344 31-Dec-2007 19:02 ..
drwxrwxr-x  500  500   4096 31-Dec-2007 19:02 .
```

Sélectionner le répertoire où les fichiers récupérés doivent être créés.

Appuyer sur la touche 'Y' pour valider la destination.

Récupération en cours



```
PhotoRec 6.9-WIP, Data Recovery Utility, December 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/hda - 60 GB / 55 GiB (R0)
  Partition      Start      End      Size in sectors
 5 L FAT32 LBA   27645     1 1 35969 15 63   8391537

Pass 1 - Reading sector 1690894/8391537, 357 files found
Elapsed time 0h00m05s - Estimated time for achievement 0h00m19
txt: 347 recovered
cab: 5 recovered
exe: 4 recovered
bmp: 1 recovered

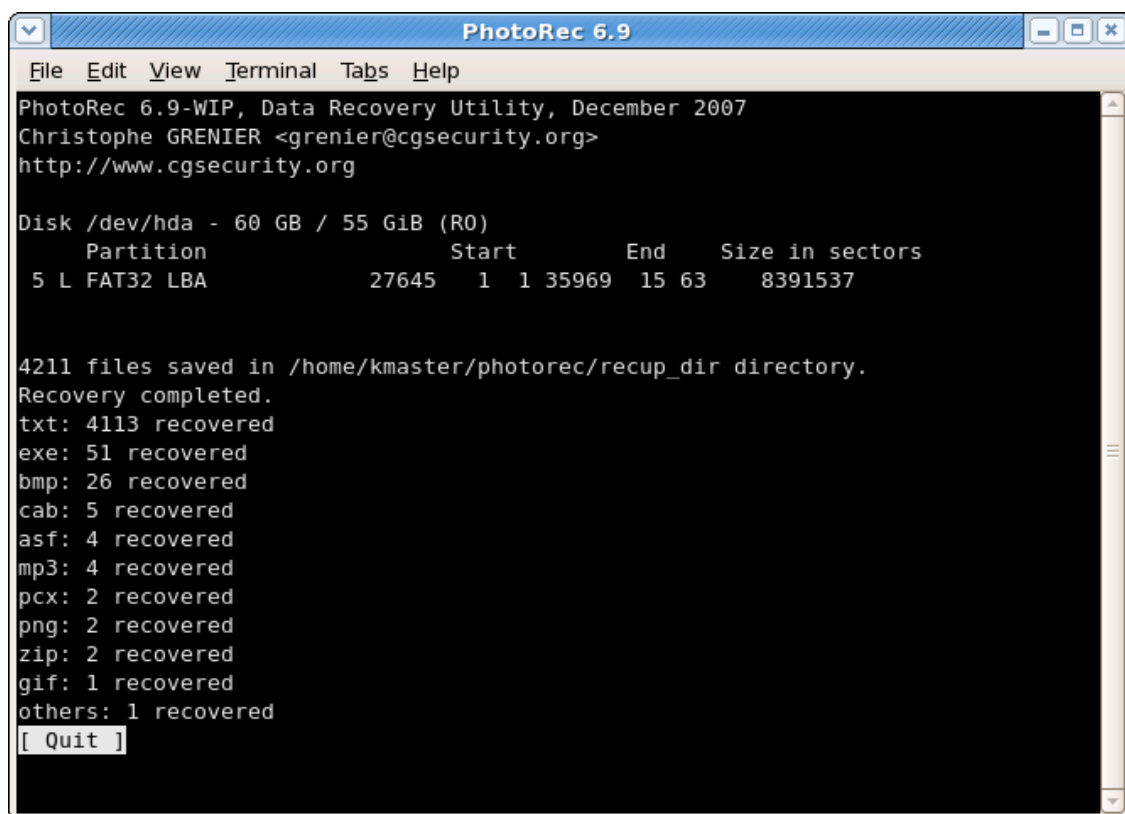
Stop
```

Le nombre de fichiers récupérés est mis à jour en temps réel.

- Durant la passe 0, PhotoRec cherche les 10 premiers fichiers pour déterminer la taille des blocs de données.
- Lors des passes suivantes, les fichiers sont récupérés y compris certains fichiers fragmentés.

Les fichiers récupérés sont créés dans des sous répertoires `recup_dir.1`, `recup_dir.2`... Il est possible d'accéder à ces fichiers même si la récupération n'est pas terminée.

Récupération terminée



```
PhotoRec 6.9
File Edit View Terminal Tabs Help
PhotoRec 6.9-WIP, Data Recovery Utility, December 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/hda - 60 GB / 55 GiB (R0)
  Partition          Start      End      Size in sectors
  5 L FAT32 LBA      27645     1 1 35969 15 63     8391537

4211 files saved in /home/kmaster/photorec/recup_dir directory.
Recovery completed.
txt: 4113 recovered
exe: 51 recovered
bmp: 26 recovered
cab: 5 recovered
asf: 4 recovered
mp3: 4 recovered
pcx: 2 recovered
png: 2 recovered
zip: 2 recovered
gif: 1 recovered
others: 1 recovered
[ Quit ]
```

Quand la récupération est terminée, un résumé est affiché. Si jamais PhotoRec a été interrompu, lors de son prochain démarrage, il demandera si vous souhaitez reprendre la récupération de donnée.

