

CGSecurity



Mode d'emploi
étape par étape
du logiciel de récupération
de données, d'images,
de vidéos



Photorec

Est un programme de récupération de données conçu pour récupérer des images perdues provenant de carte mémoire d'appareil photo, d'où le nom de PhotoRec provenant de l'anglais Photo Recovery. Il peut aussi récupérer de nombreux fichiers perdus, tels que de la vidéo, des documents et des archives stockés sur un disque dur ou sur un CD-ROM.

PhotoRec ignore le système de fichiers et va directement aux données fondamentales, il devrait donc fonctionner même si le système de fichiers est sévèrement endommagé ou formaté. PhotoRec est sûr d'utilisation, il n'essayera jamais d'écrire sur votre disque dur ou autre support mémoire que vous voulez récupérer. Les fichiers récupérés seront écrits sur le disque dur où vous exécutez PhotoRec.

PhotoRec est un logiciel multiplateforme totalement gratuit distribué sous la [licence générale publique GNU](#) (GPLV v2+). PhotoRec est un prolongement de l'application [TestDisk](#), qui permet de récupérer des partitions perdues sur une grande variété de systèmes de fichiers et de rendre des disques non-montés montables. Vous pouvez le télécharger à partir de ce [lien](#).

Important: Sitôt que manque à l'appel une photo ou un fichier ou que vous les avez détruits par erreur, cessez d'enregistrer toute autre photo ou fichier sur le disque dur ou la carte mémoire concerné; autrement vous risqueriez d'écraser les données perdues. En particulier lors de l'utilisation de Photorec, vous ne devez **surtout pas** choisir de stocker les fichiers récupérés sur la partition d'où vous les extrayez.

Systemes d'exploitation

PhotoRec fonctionne sous:

- DOS/Win9x
- Windows NT 4/2000/XP/2003/Vista
- Linux
- FreeBSD, NetBSD, OpenBSD
- Sun Solaris

- Mac OS X

et peut être compilé sur la plupart des systèmes UNIX.



[Télécharger TestDisk & PhotoRec](#)

Systemes de fichiers

Photorec ignore le système de fichiers, ainsi il fonctionne même si le système de fichiers est sévèrement endommagé.

Il peut récupérer des fichiers perdus à partir de:

- FAT,
- NTFS,
- ext2/ext3 (système de fichiers)
- HFS+

ReiserFS inclut quelques optimisations spéciales concentrées sur des queues, un nom pour des fichiers et des portions de fin de fichiers qui sont plus petits qu'un bloc de systèmes de fichiers. Afin d'augmenter l'exécution, ReiserFS peut stocker des fichiers à l'intérieur des noeuds de feuille de b*tree eux-mêmes, plutôt que de stocker les données autre part sur le disque et en pointant sur lui. Malheureusement, PhotoRec ne peut pas traiter ceci, c'est pourquoi il ne fonctionne pas bien avec ReiserFS.

Média

PhotoRec fonctionne avec des disques durs, CD-ROM, CompactFlash, Memory Stick, SecureDigital, SmartMedia, Microdrive, MMC, USB Memory Drives...

PhotoRec a été testé avec les [appareils photo numériques](#) suivants:

- Canon EOS300D, 10D
- HP PhotoSmart 620, 850, 935
- Nikon CoolPix 775, 950, 5700
- Olympus C350N, C860L, Mju 400 Digital, Stylus 300
- Sony DSC-P9
- Praktica DCZ-3.4
- Casio Exilim EX-Z 750

Il a été capable de récupérer avec succès des photos effacées. La technique utilisée par PhotoRec fonctionne en principe quelle que soit la marque ou le modèle

Formats de fichier connus

PhotoRec cherche des en-têtes de fichiers connus et, parce que fréquemment les données ne sont pas fragmentées, il peut ainsi récupérer le fichier en entier. PhotoRec reconnaît de nombreux formats de fichiers dont les archives ZIP, les documents Office, les PDF, HTML, JPEG ainsi que de nombreux autres formats. La liste des [formats récupérés par PhotoRec](#) couvre plus de 180 extensions de fichiers (une centaine de formats de fichier).

Fonctionnement sur : CD-R / CR-RW / DVD

Organisation d'un CD

Un CD est composé de plusieurs zones distinctes.

- PCA (Power Calibration Area)
- PMA (Program Memory Area)
- Une ou plusieurs sessions

Le SUA (System User Area) est composé du PCA et du PMA.

Chaque session est composée de :

- Une zone de Lead-In, contenant "the session's Table of Contents" (TOC), la "table des matières de la session".
- La zone du programme, dans laquelle les pistes individuelles sont présentes.
- Et la zone de Lead-Out.

Une piste est composée de :

- Une zone d'intervalle (pre-gap zone)
- Une zone de données
- Une zone tampon (pad zone)

Chaque bloc ou secteur a un entête contenant diverses informations dont la position du secteur ou son numéro.

Récupération de CD-R/CR-RW/DVD rayés

Photorec fonctionne bien, mais les secteurs corrompus sont susceptibles de ralentir la récupération.

Récupération d'un CD-RW effacé

Il est possible de récupérer les données d'un CD-RW qui a été effacé à condition de ne pas l'avoir réinscrit. Lorsqu'un CD-RW est effacé, le PMA, le TOC, le pre-gap, et le premier secteur sont effacés. Du fait que le TOC est effacé, le CD-RW apparaît comme vierge. Et du fait que le premier secteur a été effacé et également les headers; les secteurs 0, 1, 2... ne peuvent plus être localisés, mais les secteurs suivants peuvent encore être trouvés.

Malheureusement, tous les systèmes d'exploitation ne permettent pas ce genre de manipulation. Linux, lui, le fait parfaitement. Pour récupérer vos données perdues, lancer la version Linux de Photorec, puis lancer la récupération. Elle se déroulera très lentement, car le premier secteur est illisible, mais, généralement après le secteur 300, les données sont facilement récupérables. Soyez donc patient !

Lecture de la session précédente d'un CD-ROM

Avec les CD-ROM multi-sessions, il est possible de supprimer des fichiers de sessions précédentes. Par le fait que ces fichiers ne sont pas réellement "supprimés", il est possible de les récupérer.

Pour lire les fichiers de la première session, lancez sous Linux:

```
mount /dev/cdrom /mnt/cdrom -t iso9660 -o session=0
```






PhotoRec Etape par Etape

Ce manuel 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.

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-6.9/win/photorec_win.exe) depuis un compte dans le groupe Administrateur. Sous Vista, 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-6.9/linux/photorec_static)
-  Sous MacOSX, si vous n'êtes pas root, PhotoRec (par exemple, testdisk-6.9/darwin/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.

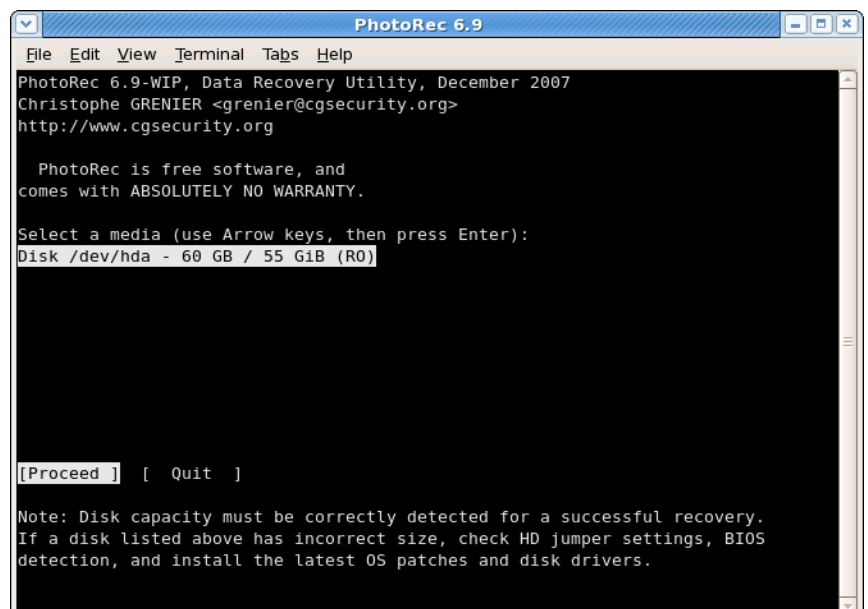
 **X** Pour récupérer des fichiers d'autres périphériques, exécuter photorec périphérique, par exemple:

- 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.



```
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

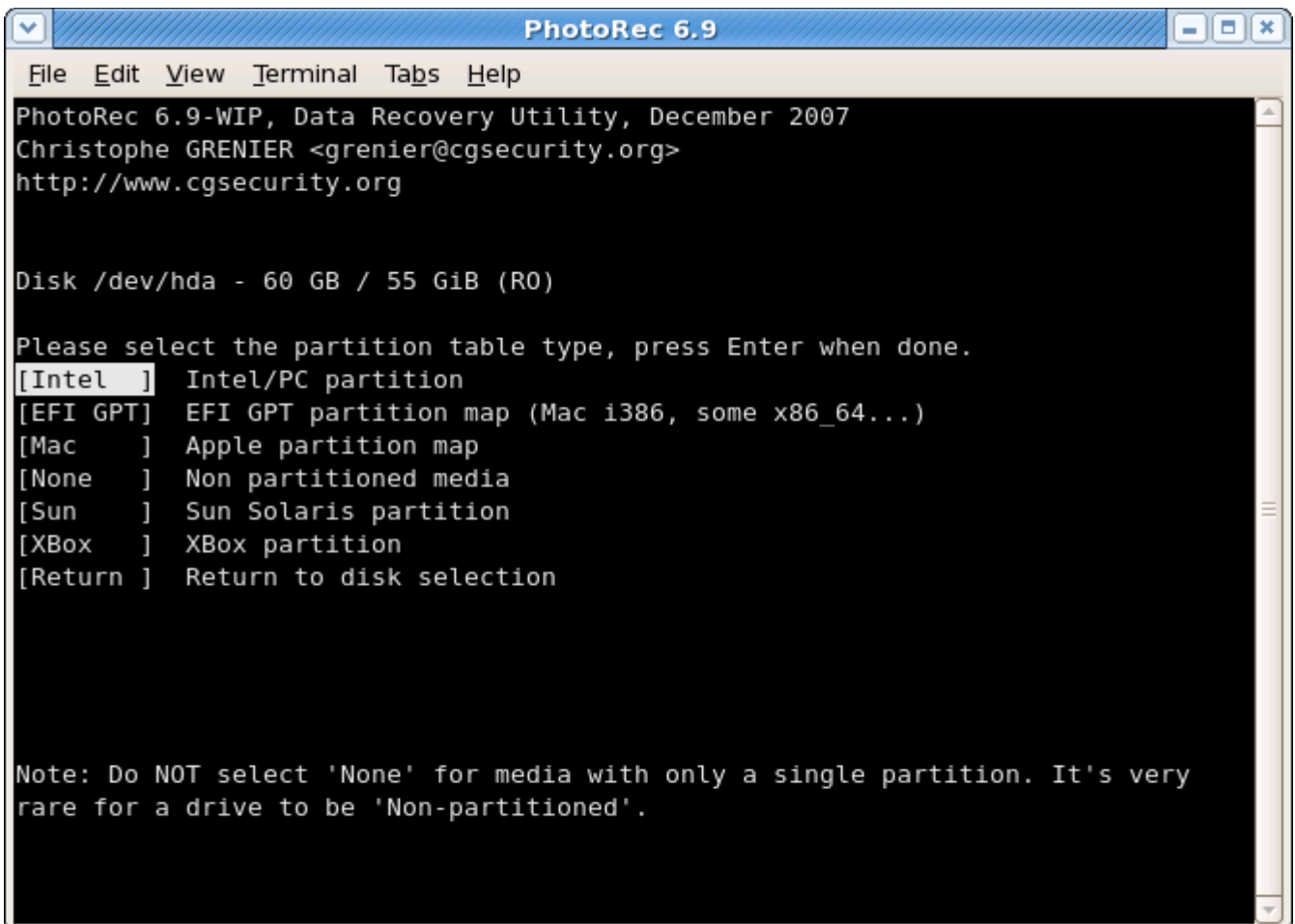
PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/hda - 60 GB / 55 GiB (R0)

[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.
```

Sélection du type de la table des partitions



```
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

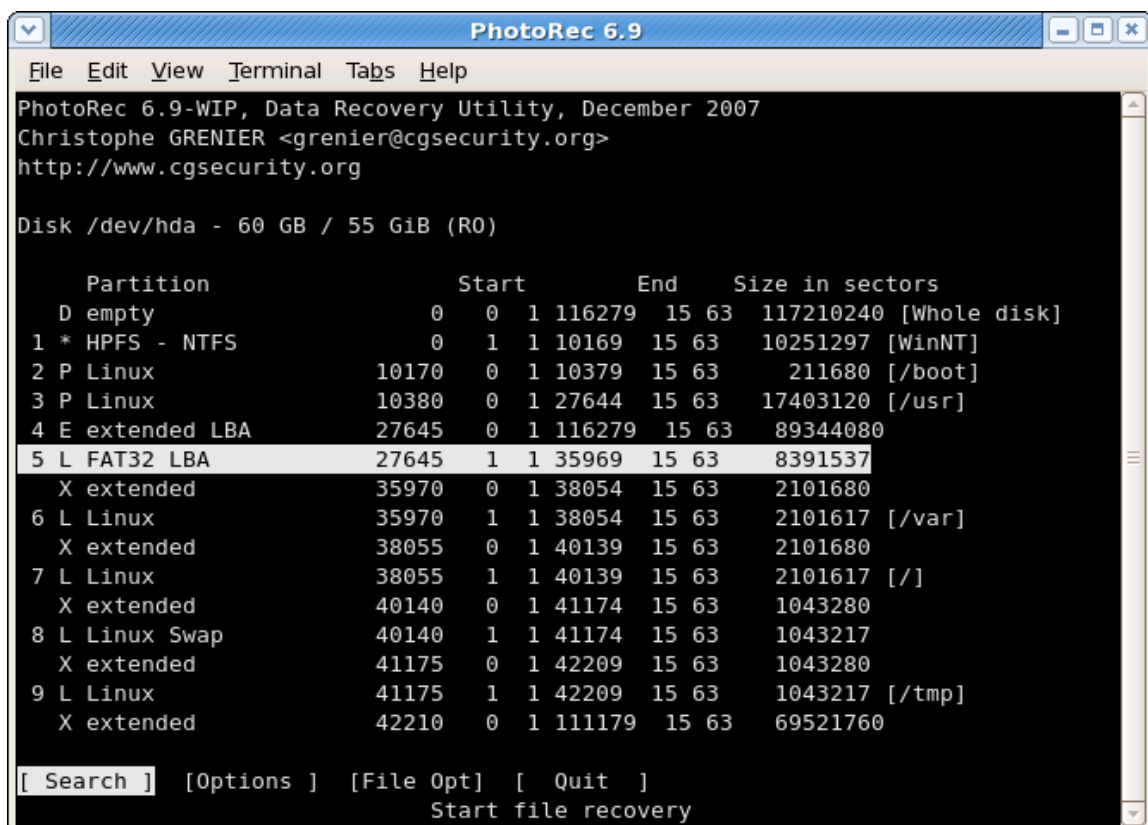
Disk /dev/hda - 60 GB / 55 GiB (R0)

Please select the partition table type, press Enter when done.
[Intel ] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Mac ] Apple partition map
[None ] Non partitioned media
[Sun ] Sun Solaris partition
[XBox ] Xbox partition
[Return ] Return to disk selection

Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.
```

Sélectionner le type de la table des partitions, en principe la valeur par défaut est la bonne, car PhotoRec effectue une auto détection.

Sélection de la partition source



```
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)

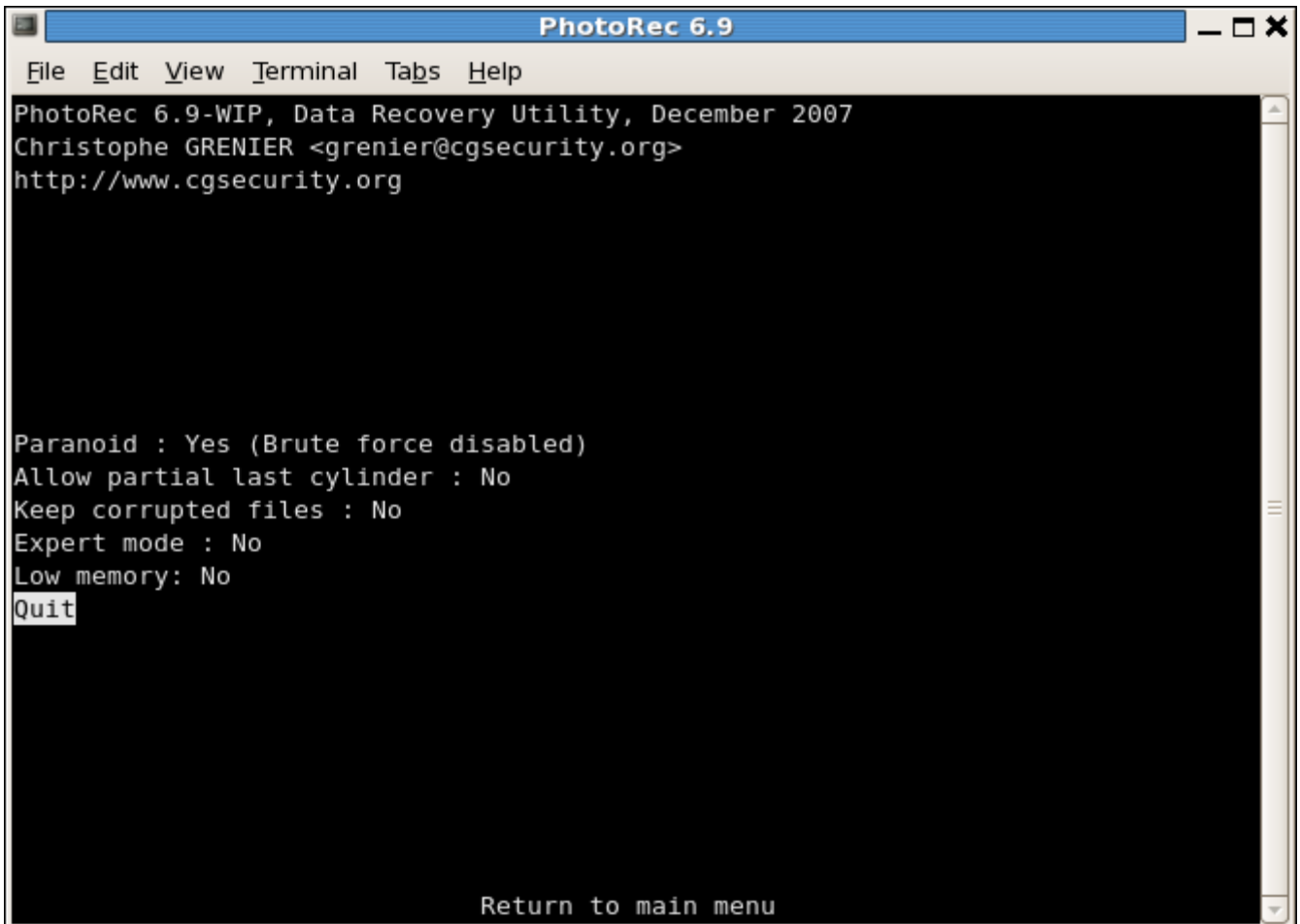
Partition          Start      End      Size in sectors
D empty            0 0 1 116279 15 63 117210240 [Whole disk]
1 * HPFS - NTFS    0 1 1 10169 15 63 10251297 [WinNT]
2 P Linux          10170 0 1 10379 15 63 211680 [/boot]
3 P Linux          10380 0 1 27644 15 63 17403120 [/usr]
4 E extended LBA   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

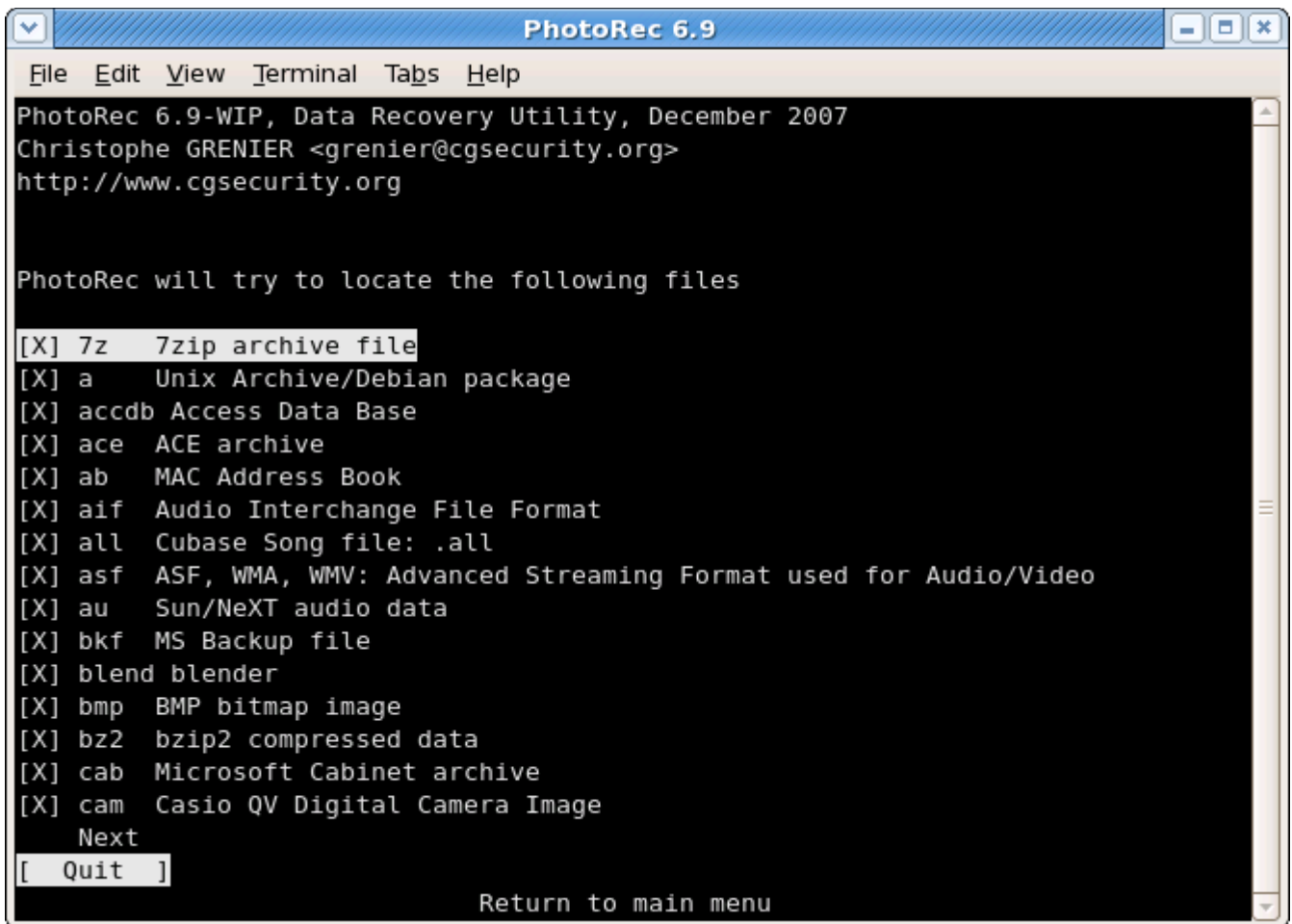


- Paranoid Par défaut, les fichiers récupérés sont vérifiés et les fichiers invalides rejetés.

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.
- 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

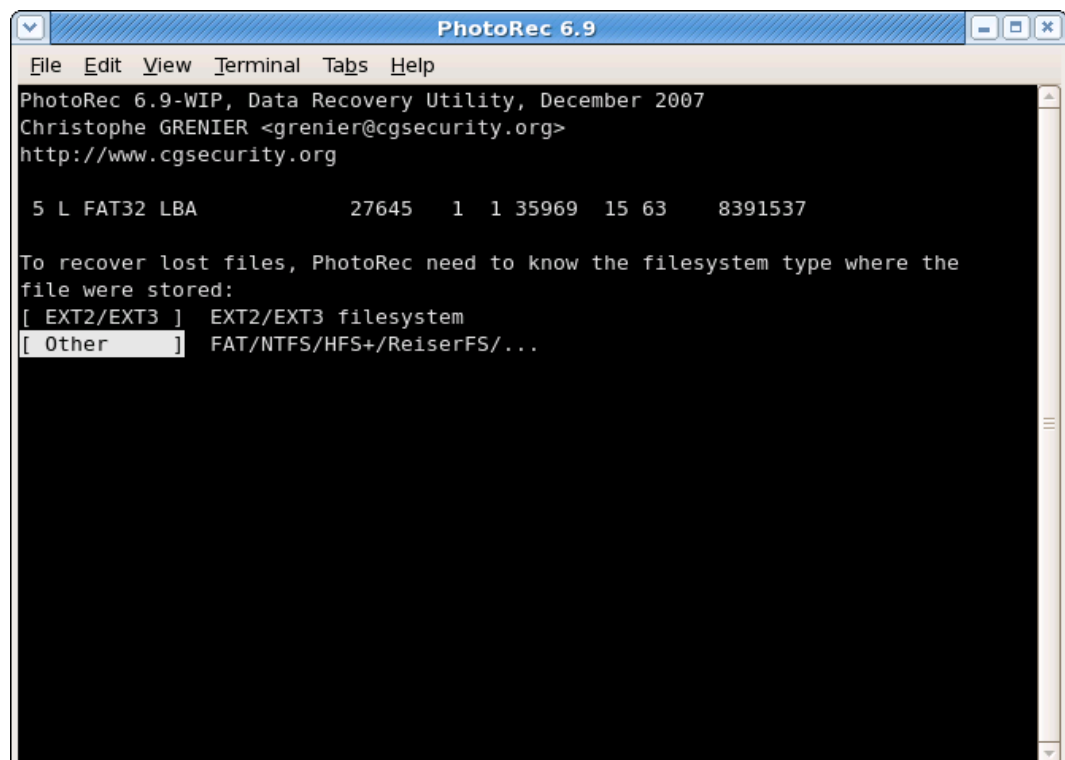
Sélection des formats de fichiers à récupérer



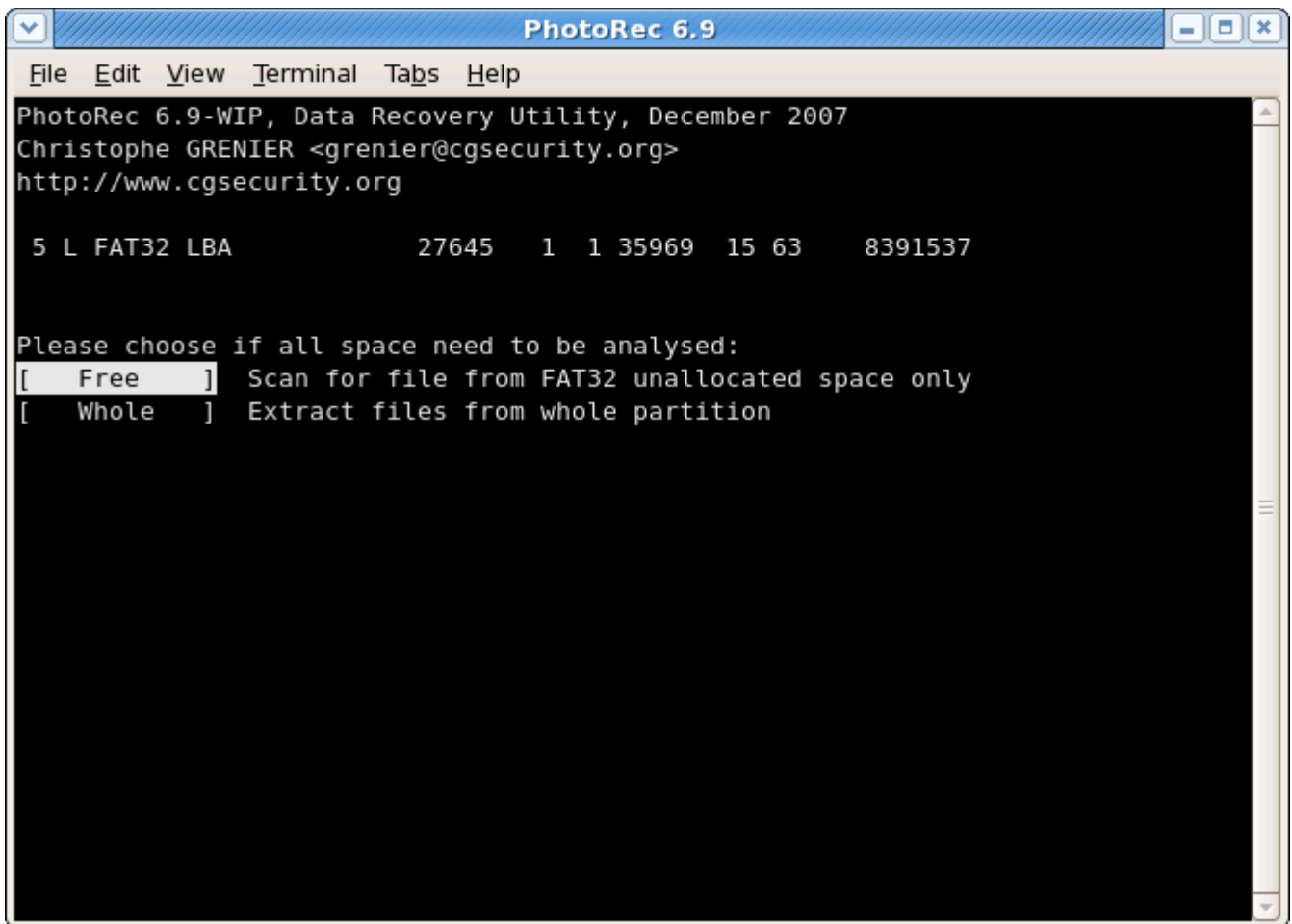
- Activer ou désactiver la récupération de certains types de fichier, par exemple
- [X] tif Tag Image File Format and some raw file formats (pef/nef/dcr/sr2/cr2)
- ... [X] zip zip archive including OpenOffice and MSOffice 2007 </pre> La famille `tif` permet aussi la récupération des images raws `pef/nef/dcr/sr2/cr2`, 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`.



Extraire les données de la partition ou de son espace libre






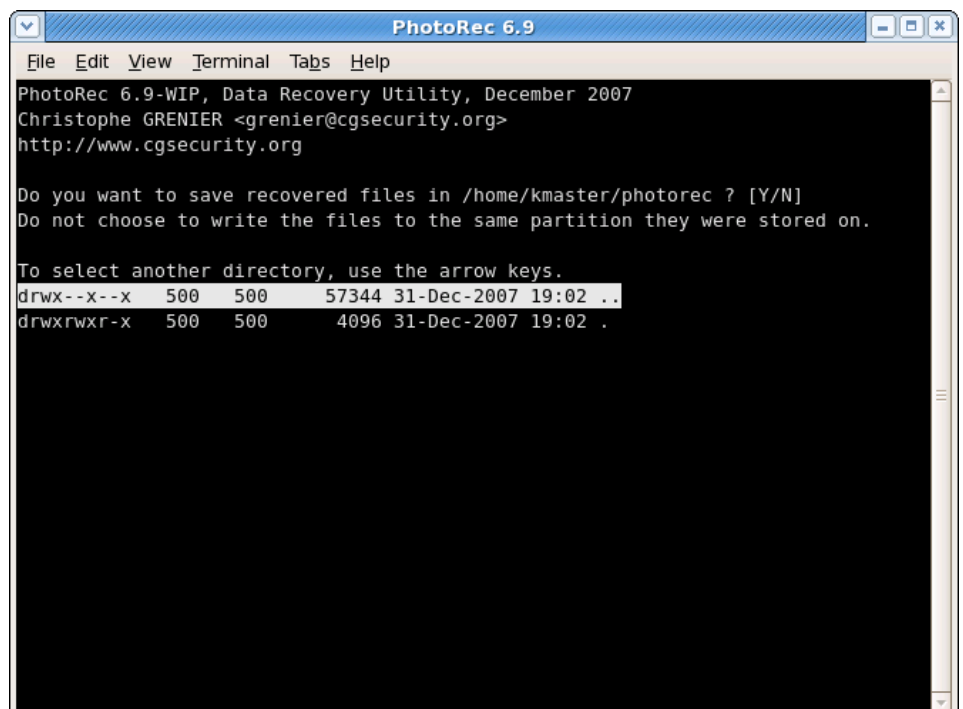
PhotoRec peut rechercher les fichiers

- 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.

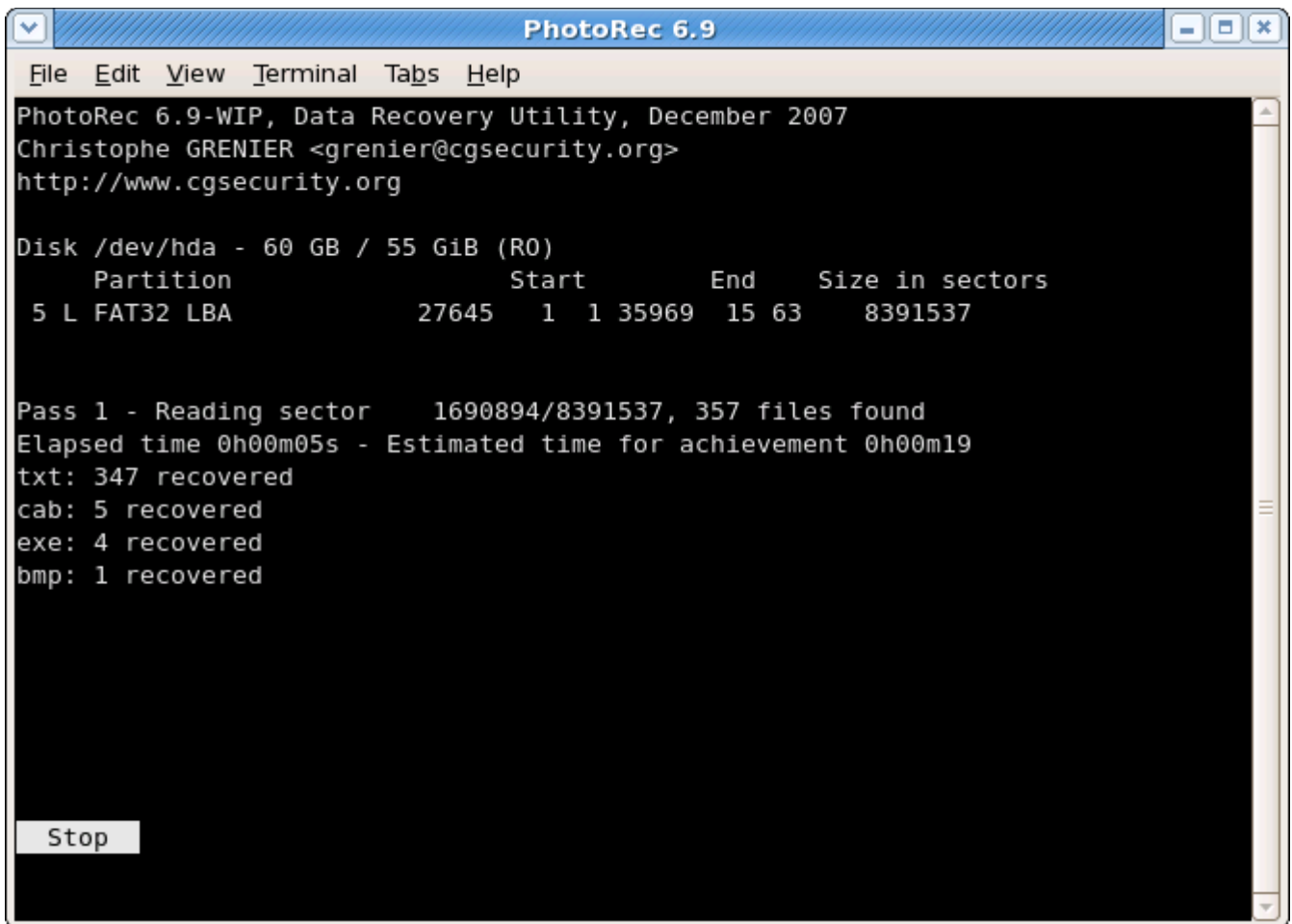
Sélection de la destination des fichiers récupérés

Sélectionner le répertoire où les fichiers récupérés doivent être créés.

-  Choisir .. plusieurs fois pour obtenir la liste des disques (C:, D:, E:..).
-  Les systèmes de fichiers des disques externes sont généralement disponibles dans un sous-répertoire de /media ou /mnt.
-  Les partitions des disques externes sont généralement montées dans le répertoire /Volumes.



Récupération en cours



```
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

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
```

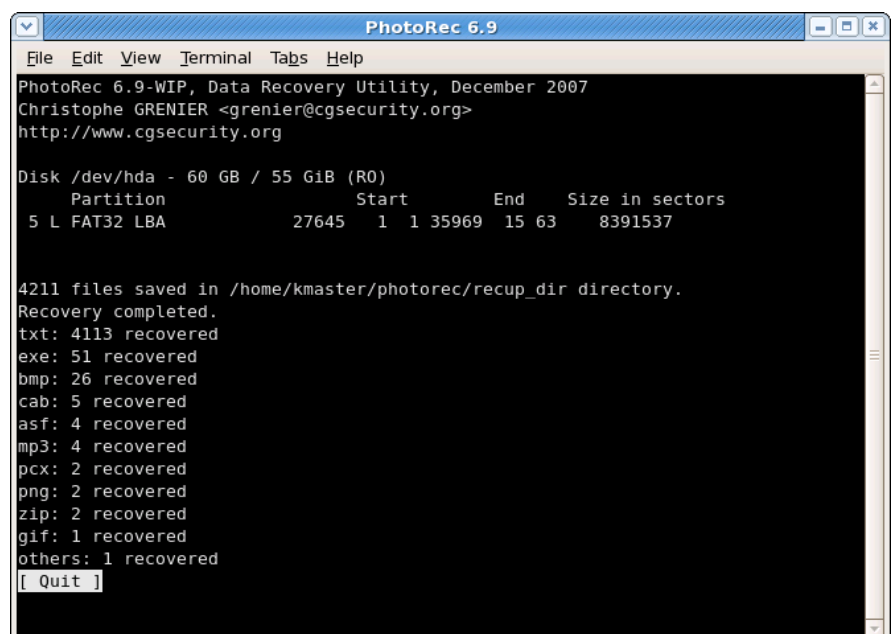
Le nombre de fichiers récupérés est mis à jour en temps réel.

- 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

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.



```
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 ]
```