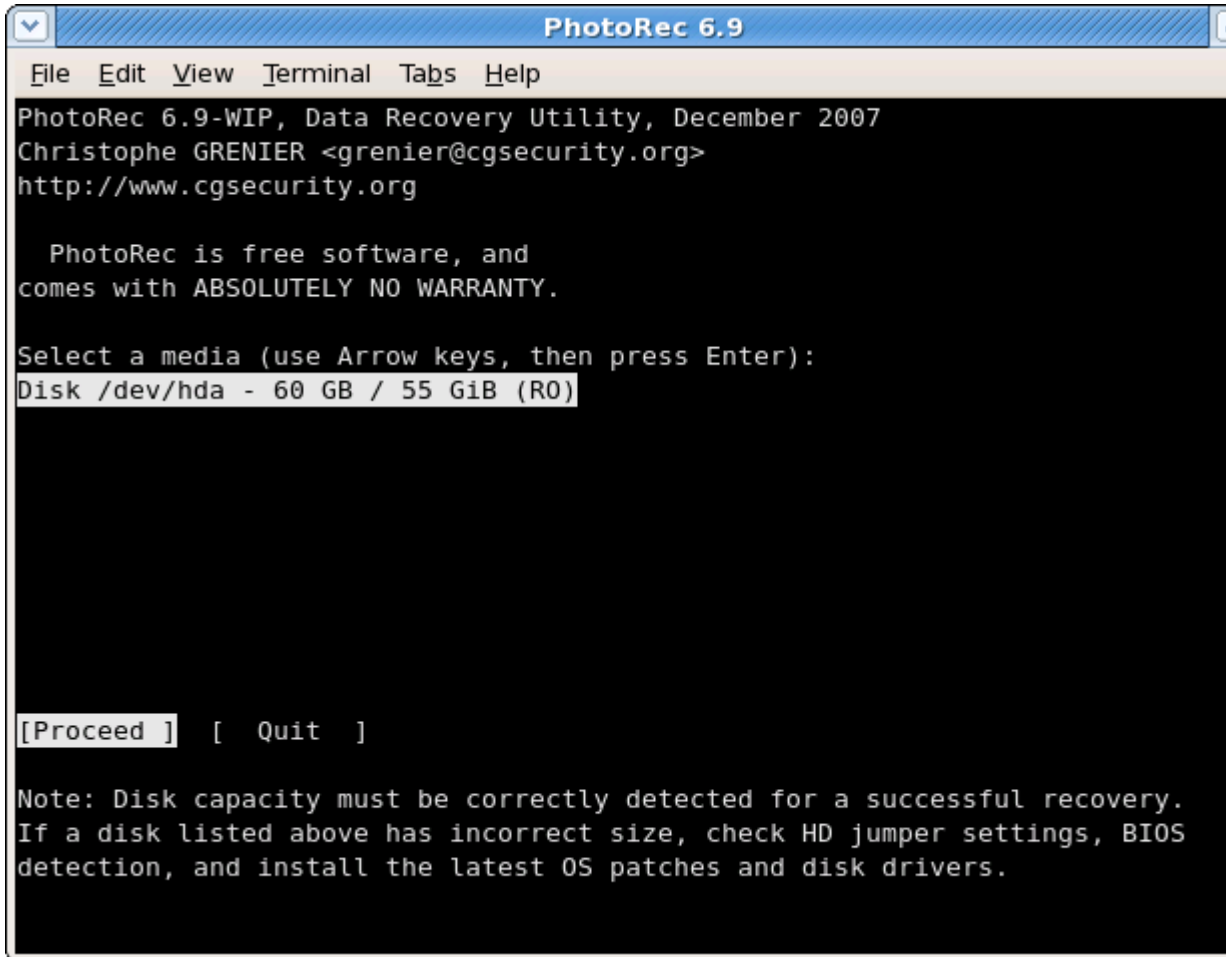




Anleitung zu PhotoRec

Disk selection



```
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.
```

Available media are listed. Use up/down arrow keys to select the disk that holds the lost files. Press `Enter` to proceed.

XIf available, use the raw device, `/dev/rdisk*` instead of `/dev/disk*` for faster data transfer.



Source partition selection

```
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

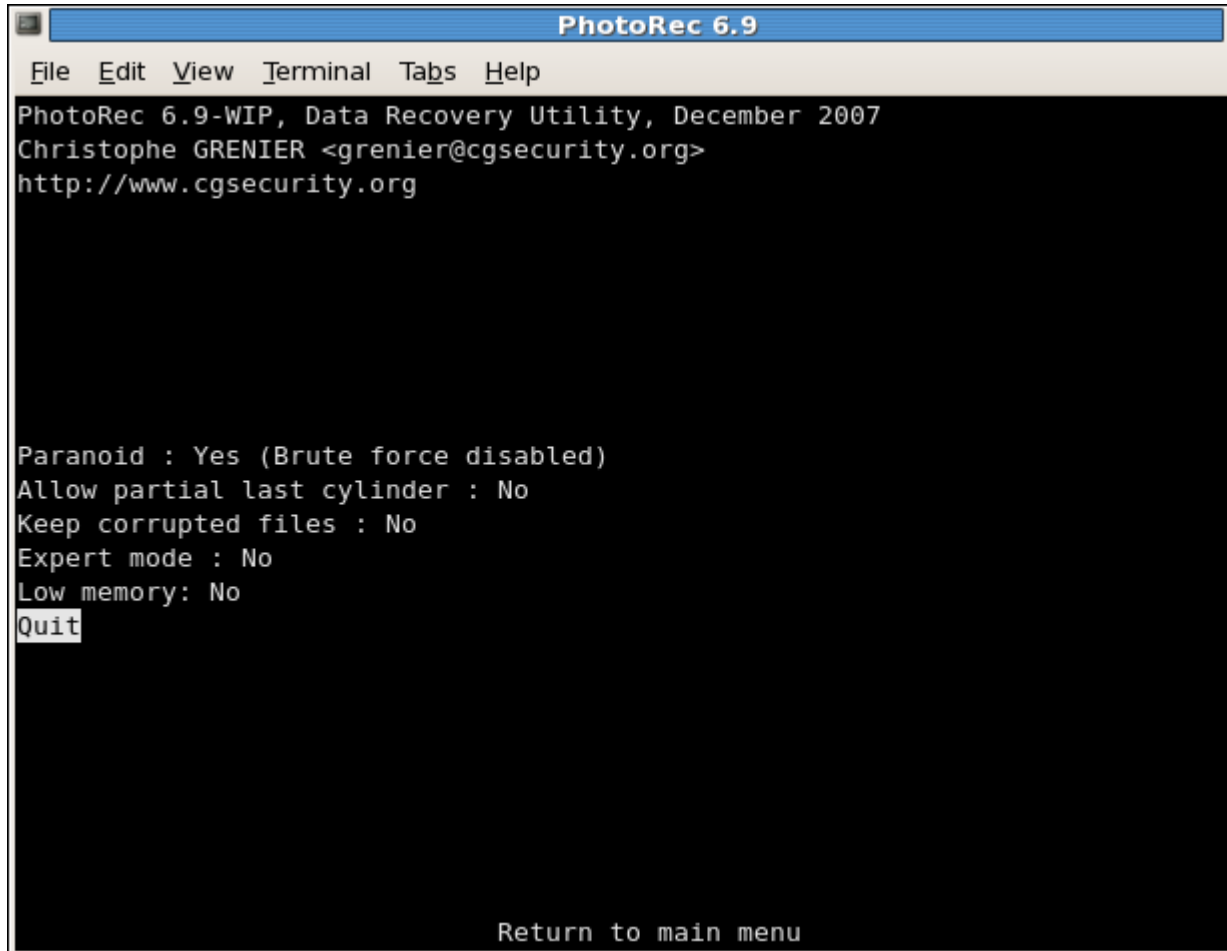
[ Search ] [Options ] [File Opt] [ Quit ]
Start file recovery
```

Choose

- Search after selecting the partition that holds the lost files to start the recovery,
- Options to modify the options,
- File Opt to modify the list of file types recovered by PhotoRec.



PhotoRec options



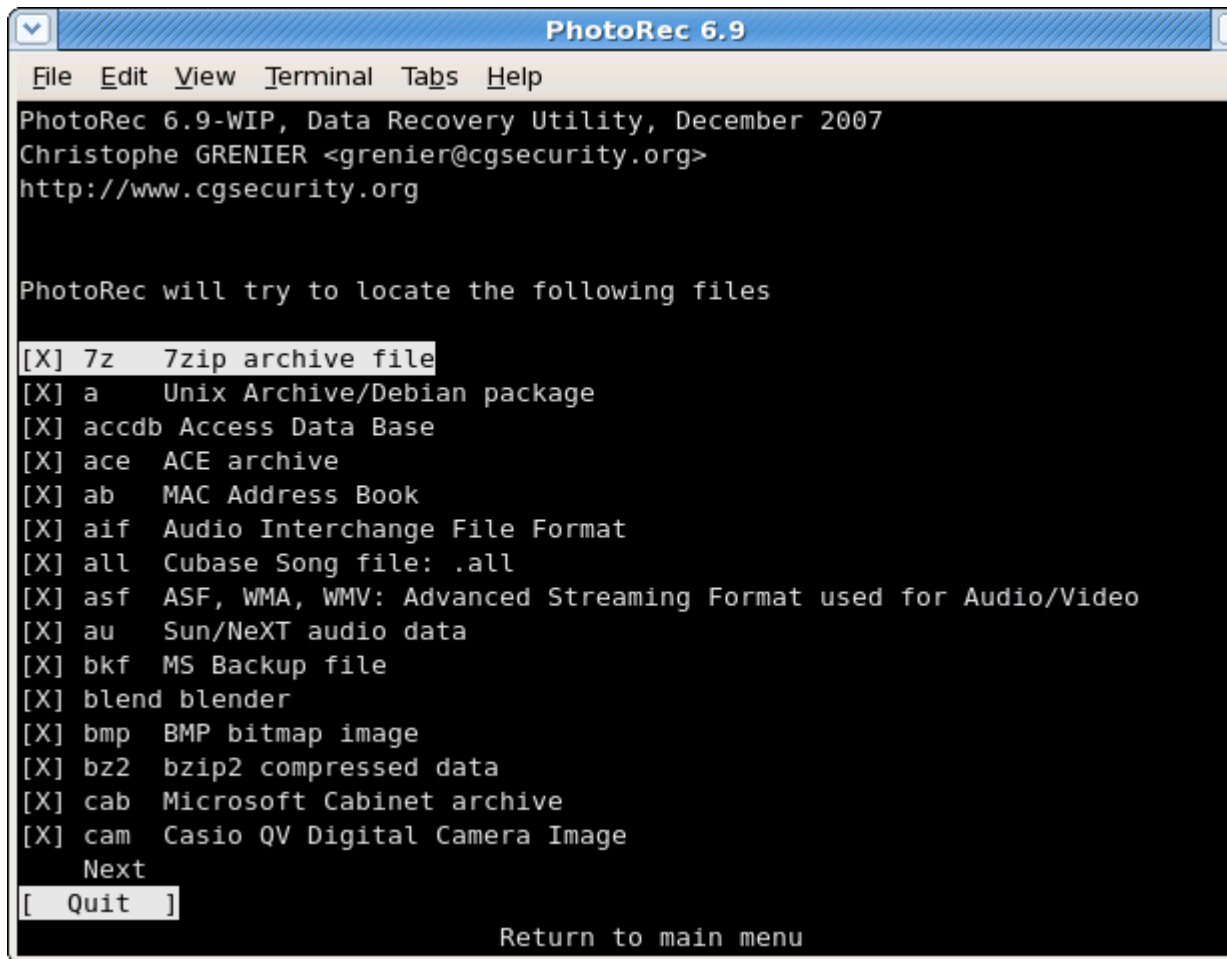
- **Paranoid** By default, recovered files are verified and invalid files rejected.

Enable `bruteforce` if you want to recover more fragmented JPEG files, note it is a very CPU intensive operation.

- `Allow partial last cylinder` modifies how the disk geometry is determined - only non-partitioned media should be affected.
- The `expert mode` option allows the user to force the file system block size and the offset. Each filesystem has his own block size (a multiple of the sector size) and offset (0 for NTFS, exFAT, ext2/3/4), these value are fixed when the filesystem has been created/formated. When working on the whole disk (ie. original partitions are lost) or a reformatted partition, if PhotoRec has found very few files, you may want to try the minimal value that PhotoRec let you select (it's the sector size) for the block size (0 will be used for the offset).
- Enable `Keep corrupted files` to keep files even if they are invalid in the hope that data may still be salvaged from an invalid file using other tools.
- Enable `Low memory` if your system does not have enough memory and crashes during recovery. It may be needed for large file systems that are heavily fragmented. Do not use this option unless absolutely necessary.



Selection of files to recover



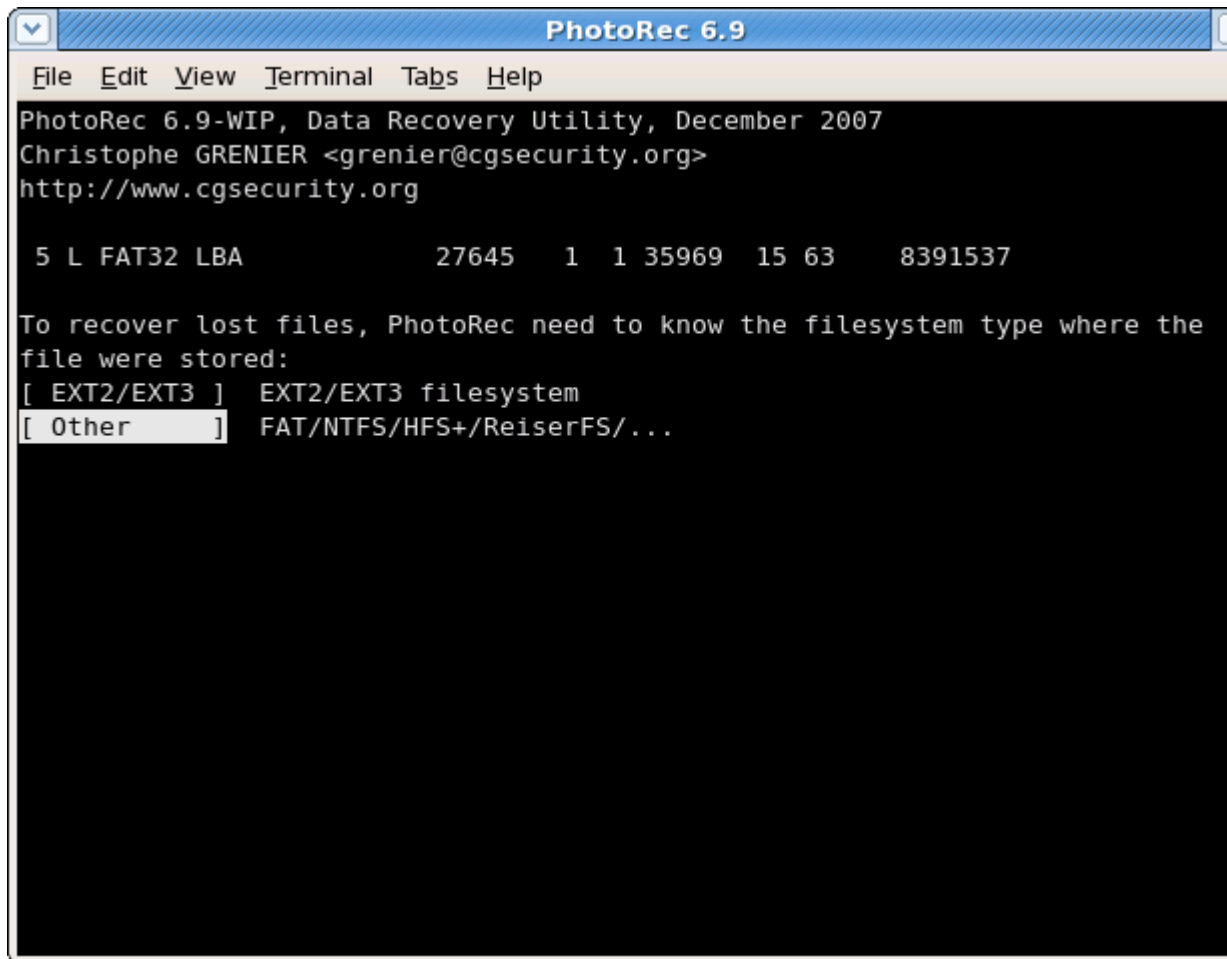
In FileOpts, enable or disable the recovery of certain file types, for example,

```
[X] riff RIFF audio/video: wav, cdr, avi
...
[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
```

The whole list of [file formats recovered by PhotoRec](#) contains more than 320 file families representing more than 200 file extensions.



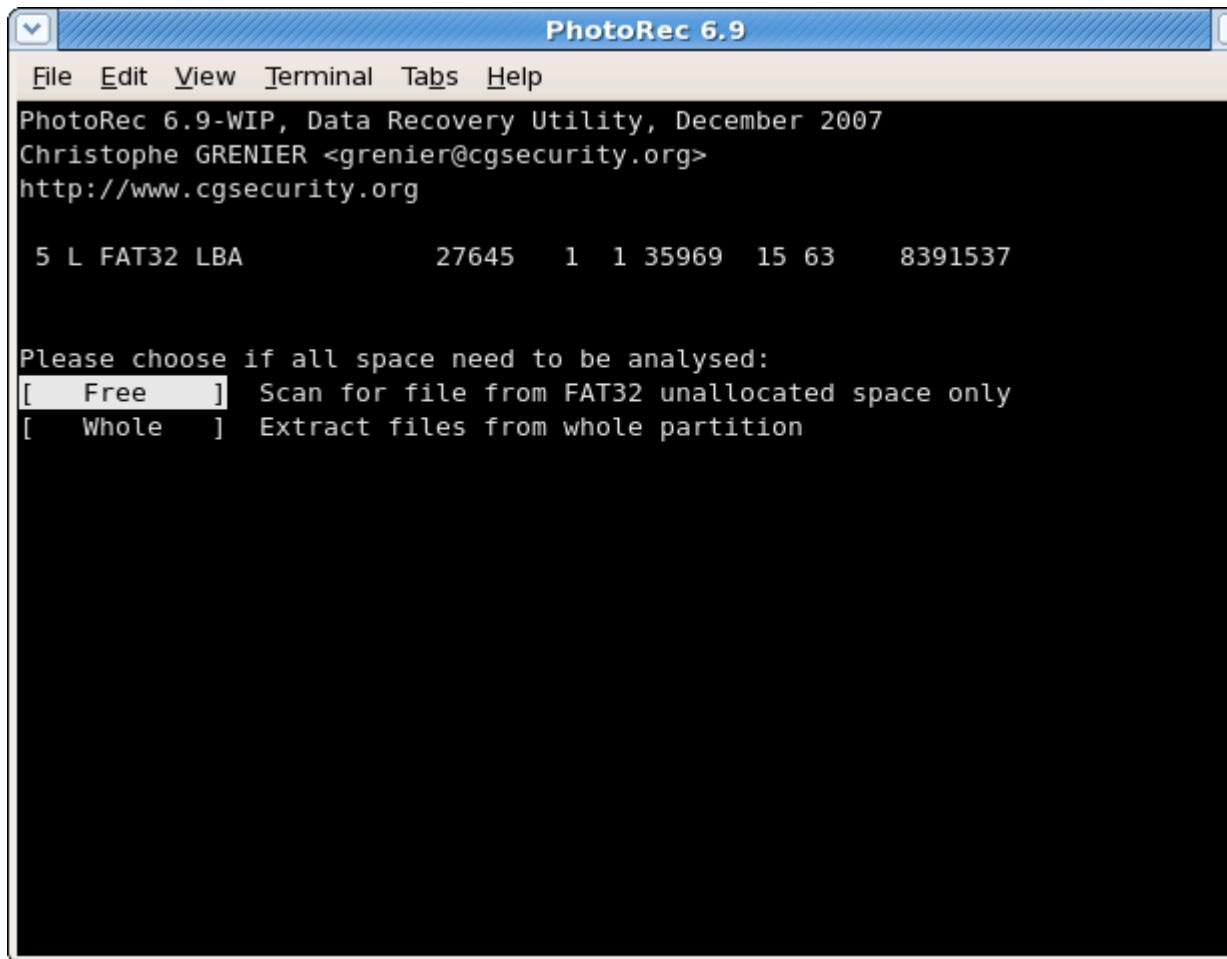
File system type



Once a partition has been selected and validated with `Search`, PhotoRec needs to know how the data blocks are allocated. Unless it is an ext2/ext3/ext4 filesystem, choose `Other`.



Carve the partition or unallocated space only

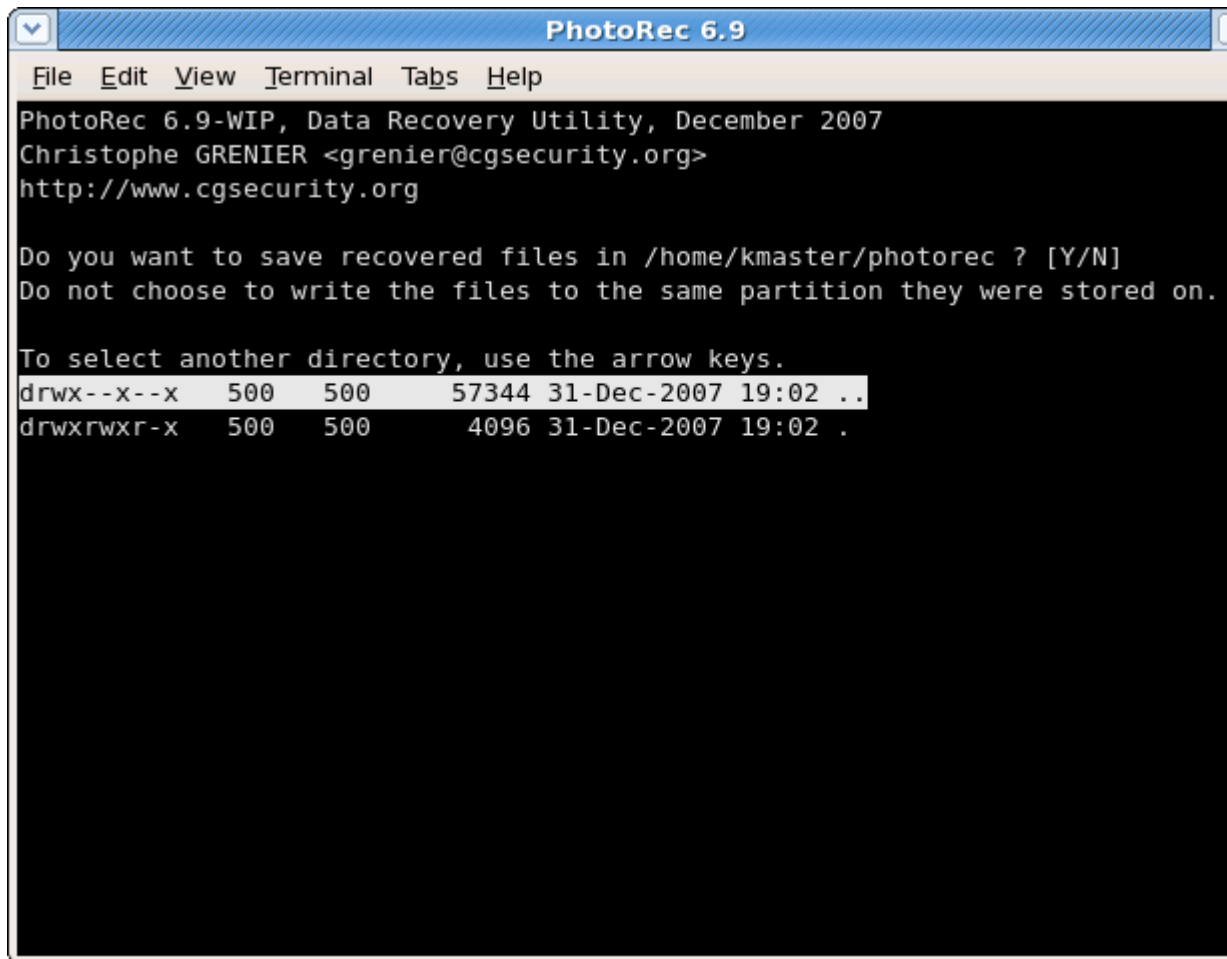


PhotoRec can search files from

- from the whole partition (useful if the filesystem is corrupted) or
- from the unallocated space only (available for ext2/ext3/ext4, FAT12/FAT16/FAT32 and NTFS). With this option only deleted files are recovered.



Select where recovered files should be written



Choose the directory where the recovered files should be written.

- 🖥️ To get the drive list (C:, D:, E:, etc.), use the arrow keys to select .., press the **Enter** key - repeat until you can select the drive of your choice. Validate with **yes** when you get the expected destination.
- 🗂️ File system from external disk may be available in a /media, /mnt or /run/media sub-directory. Mount your destination drive if necessary.
- 📁 Partitions from external disk are usually mounted in /Volumes.



Recovery in progress

```
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
```

Number of recovered files is updated in real time.

- During pass 0, PhotoRec searches the first 10 files to determine the blocksize.
- During pass 1 and later, files are recovered including some fragmented files.

Recovered files are written in recup_dir.1, recup_dir.2... sub-directories. It's possible to access the files even if the recovery is not finished.



Recovery is completed

```
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 ]
```

When the recovery is complete, a summary is displayed. Note that if you interrupt the recovery, the next time PhotoRec is restarted you will be asked to resume the recovery.

- Thumbnails found inside pictures are saved as `t*.jpg`
- If you have chosen to keep corrupted files/file fragments, their filenames will begin with the letter `b`(roken).
- Hint: When looking for a specific file. Sort your recovered files by extension and/or date/time. PhotoRec uses time information (metadata) when available in the file header to set the file modification time
- [After Using PhotoRec](#): Some ideas to sort recovered files or repair broken ones.
-  You may have disabled your live antivirus protection during the recovery to speed up the process, but it's recommended to scan the recovered files for viruses before opening them - PhotoRec may have undeleted an infected document or a trojan.

Quelle: http://www.cgsecurity.org/wiki/PhotoRec_Step_By_Step