

PhotoRec Step By Step - CGSecurity

CGSecurity : 5-7 minutes : 1/18/2016

This **Recovery example** guides you through [PhotoRec](#) step by step to recover deleted files or lost data from a reformatted partition or corrupted file system. For lost/deleted partitions or deleted files from a [FAT](#) or [NTFS](#) file system, try [TestDisk](#) first - it's usually faster and TestDisk can retrieve the original file names. [Translations of this PhotoRec manual](#) to other languages are welcome.


Run PhotoRec executable

If PhotoRec is not yet installed, it can be downloaded from [TestDisk Download](#). Extract the files from the archive including the sub-directories.

To recover files from hard disk, USB key, Smart Card, CD-ROM, DVD, etc., you need enough rights to access the physical device.

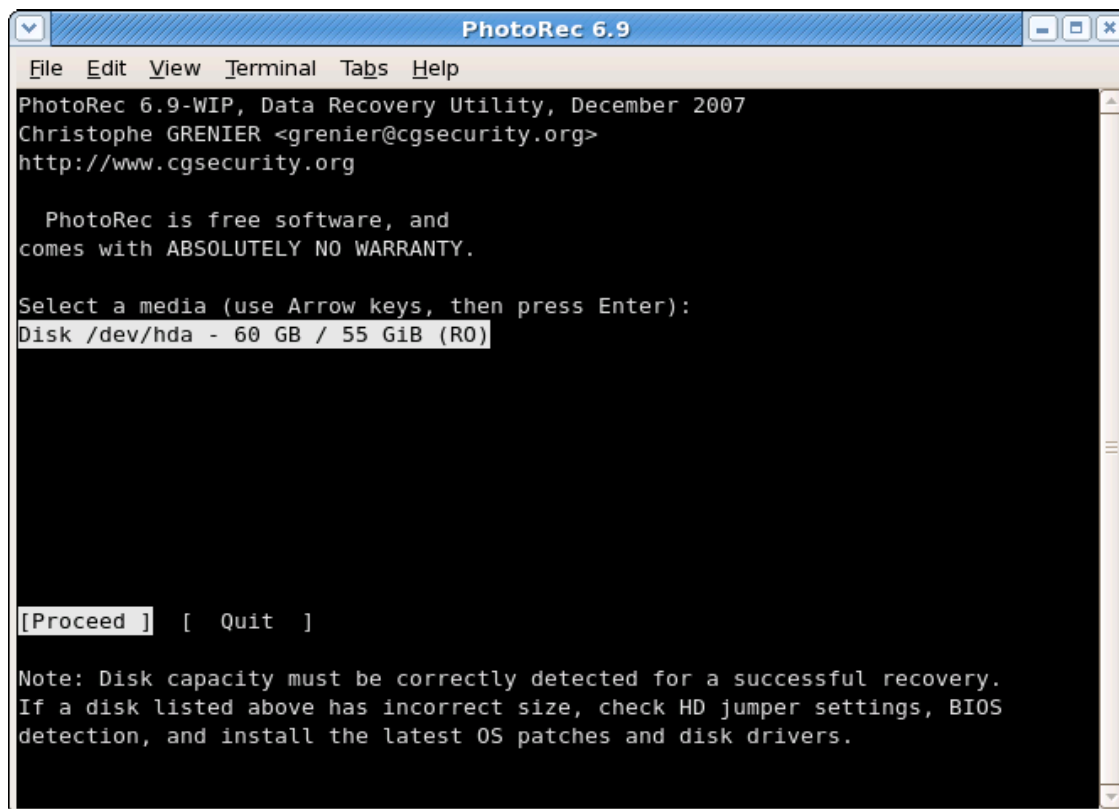
To recover files from a media image, run

- `photorec image.dd` to carve a raw disk image
- `photorec image.E01` to recover files from an Encase EWF image
- `photorec 'image.???'` if the Encase image is split into several files.
- `photorec '/cygdrive/d/evidence/image.???'` if the Encase image is split into several files in the directory `d:\evidence`

 **X** Most devices should be autodetected including Linux software RAID (that is, `/dev/md0`) and file system encrypted with cryptsetup, dm-crypt, LUKS or TrueCrypt (ie. `/dev/mapper/truecrypt0`). To recover files from other devices, run `photorec device`.

Forensics users can use the parameter `/log` to create a log file named `photorec.log`; it records the location of the files recovered by PhotoRec.

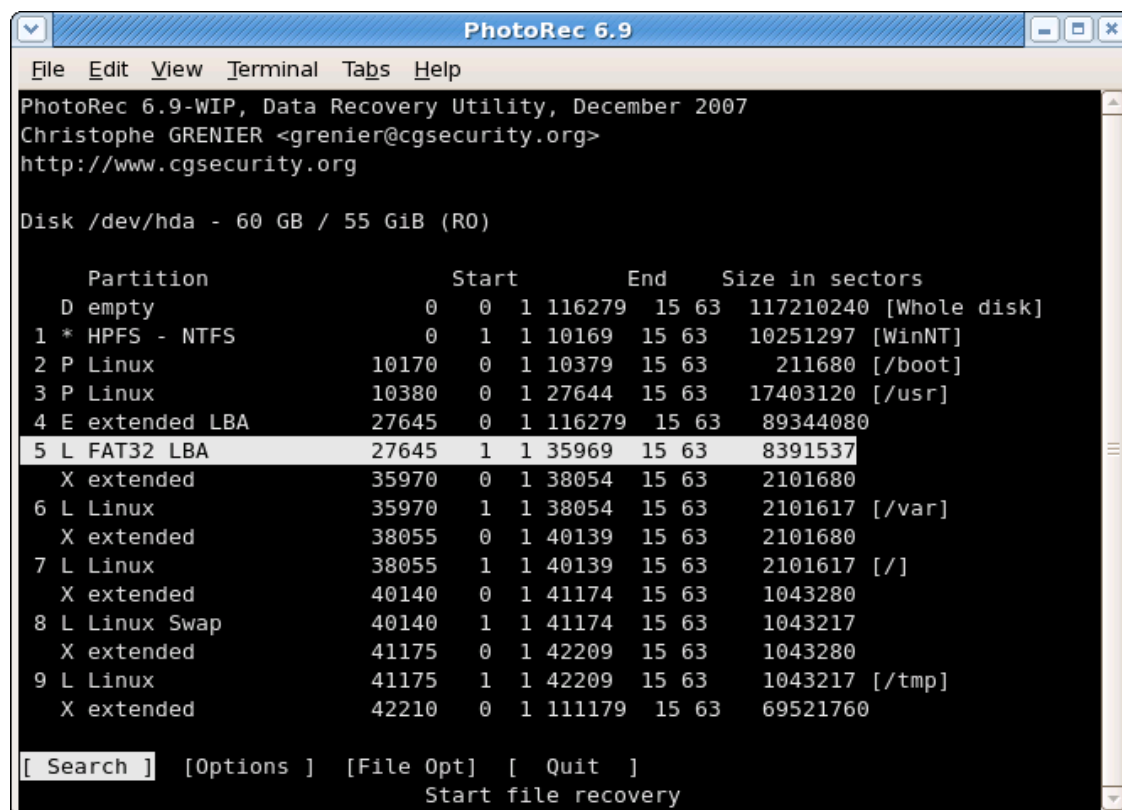
Disk selection



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

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

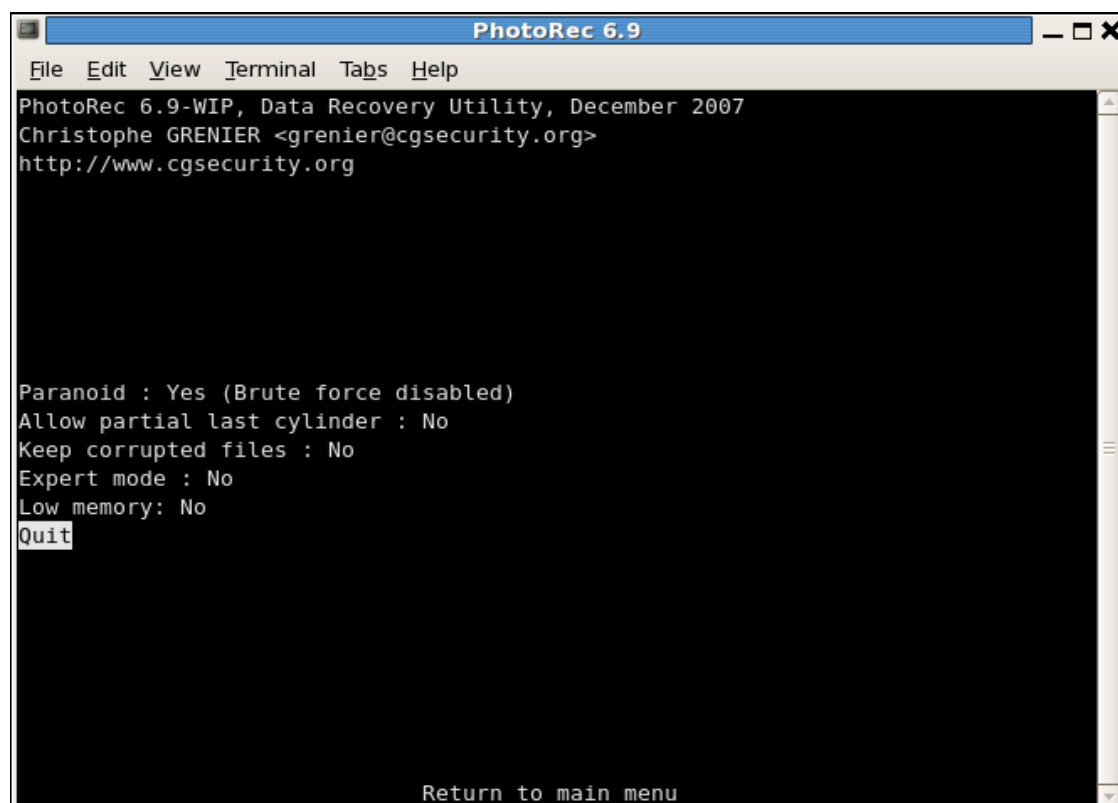
Source partition selection



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

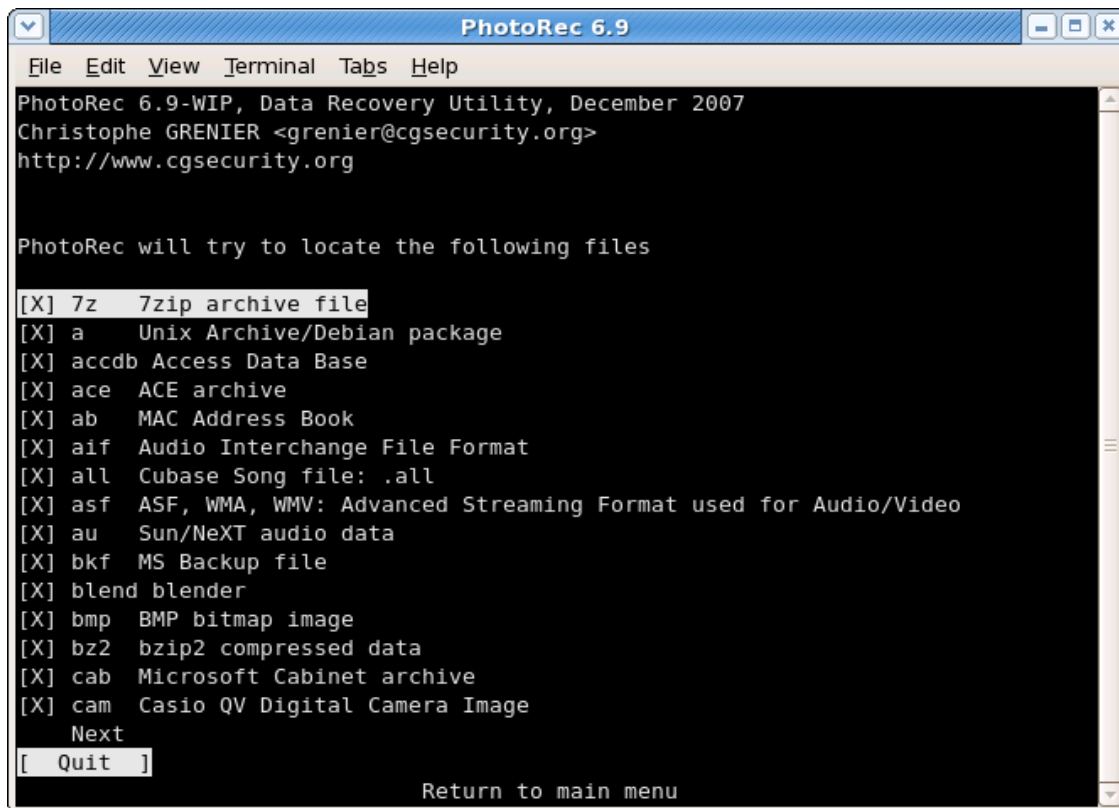


- Paranoid By default, recovered files are verified and invalid files rejected.

Enable brute force 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 its own block size (a multiple of the sector size) and offset (0 for NTFS, exFAT, ext2/3/4), these values are fixed when the filesystem has been created/formatted. 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

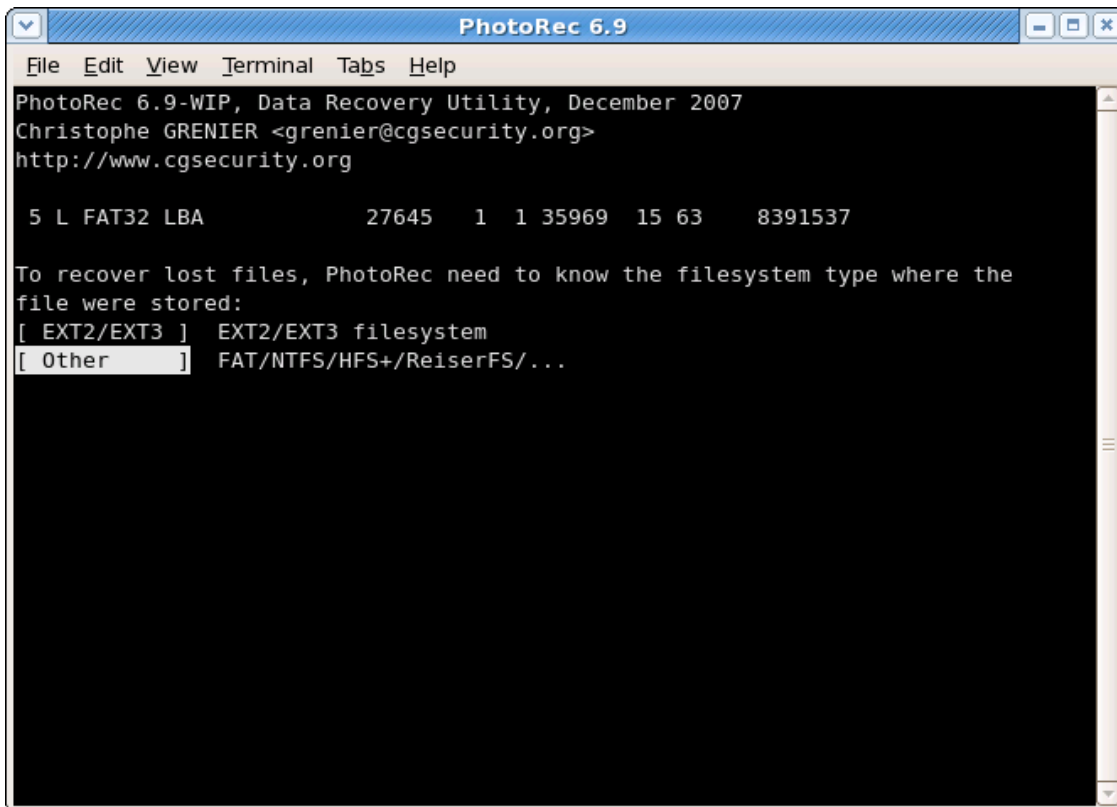


In FileOpts, enable or disable the recovery of certain file types, for example,

```
[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
```

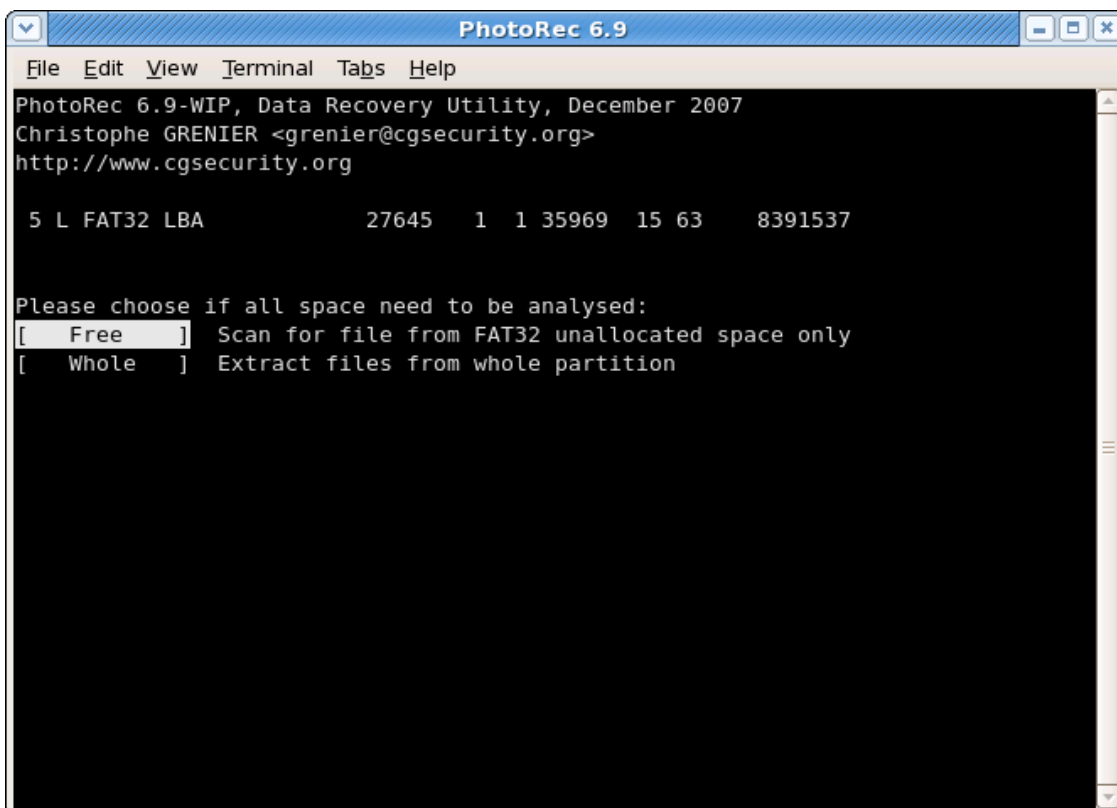
The whole list of [file formats recovered by PhotoRec](#) contains more than 300 file families representing more than 480 file extensions.

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.

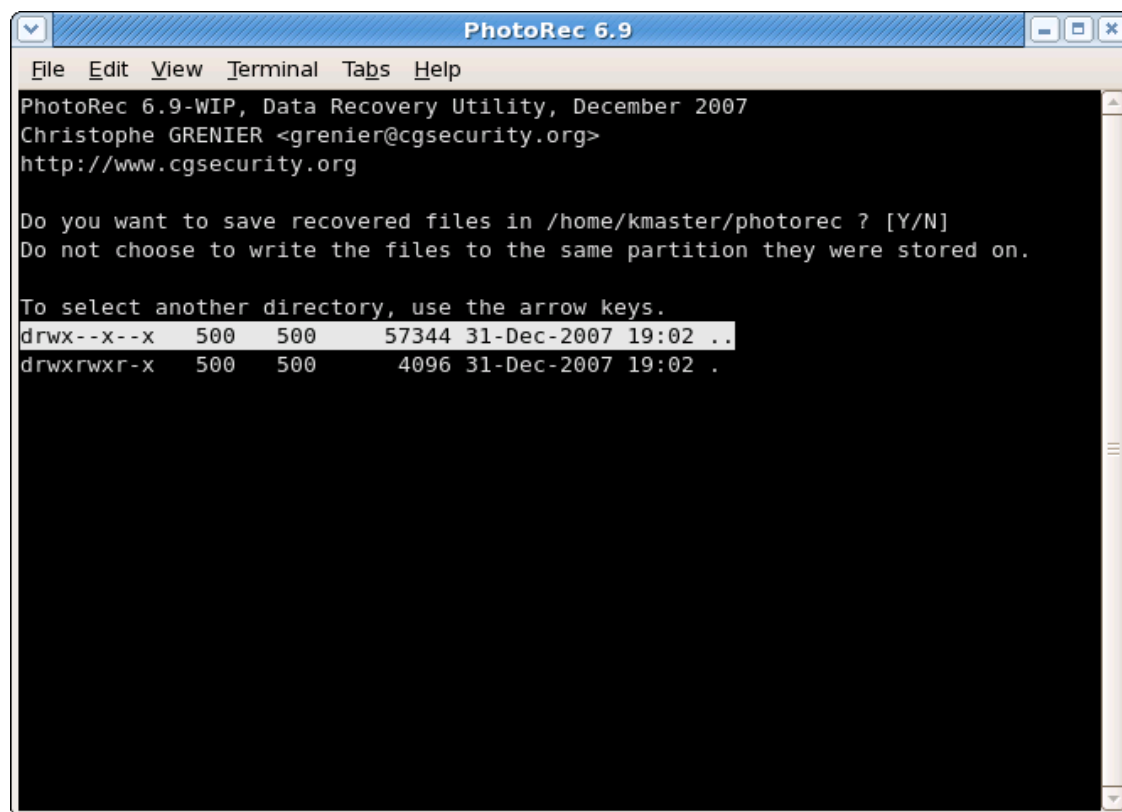
Carve the partition or unallocated space only



PhotoRec can search files from

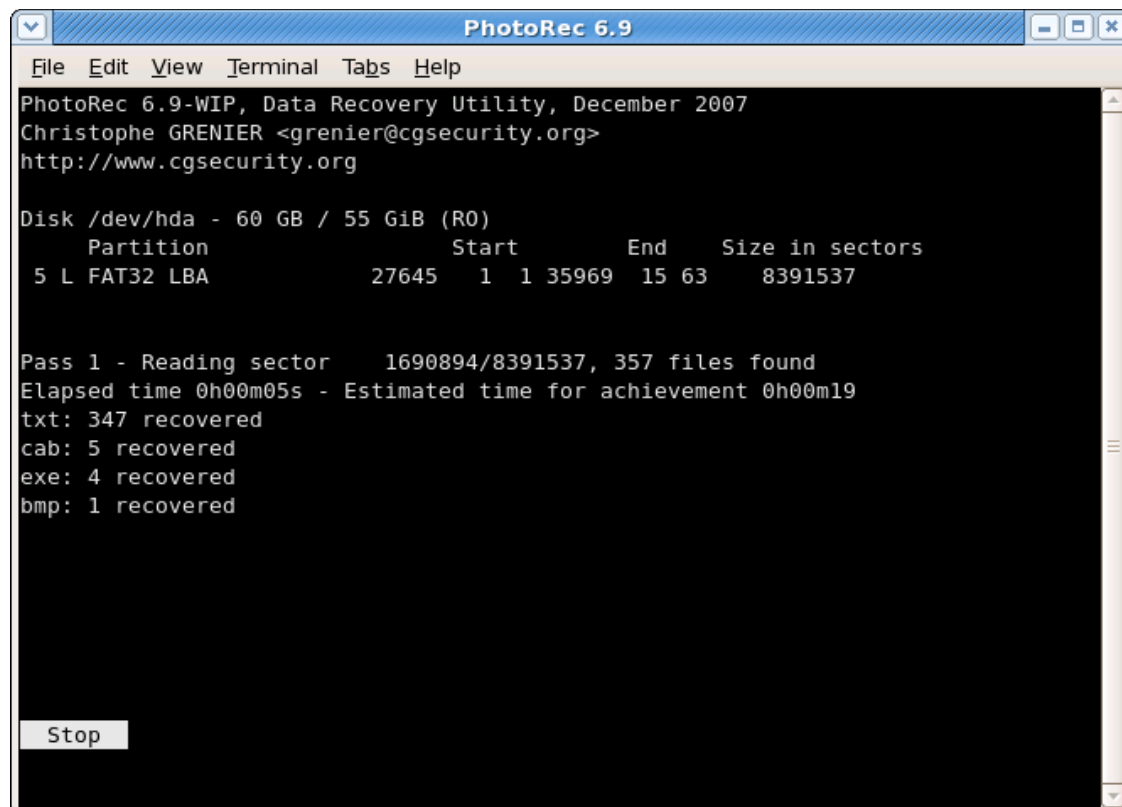
- from the whole partition (useful if the filesystem is corrupted) or
- from the unallocated space only (available for ext2/ext3/ext4, FAT12/FAT16/FAT32 and NTFS). With this option only deleted files are recovered.

Select where recovered files should be written



Choose the directory where the recovered files should be written.

Recovery in progress

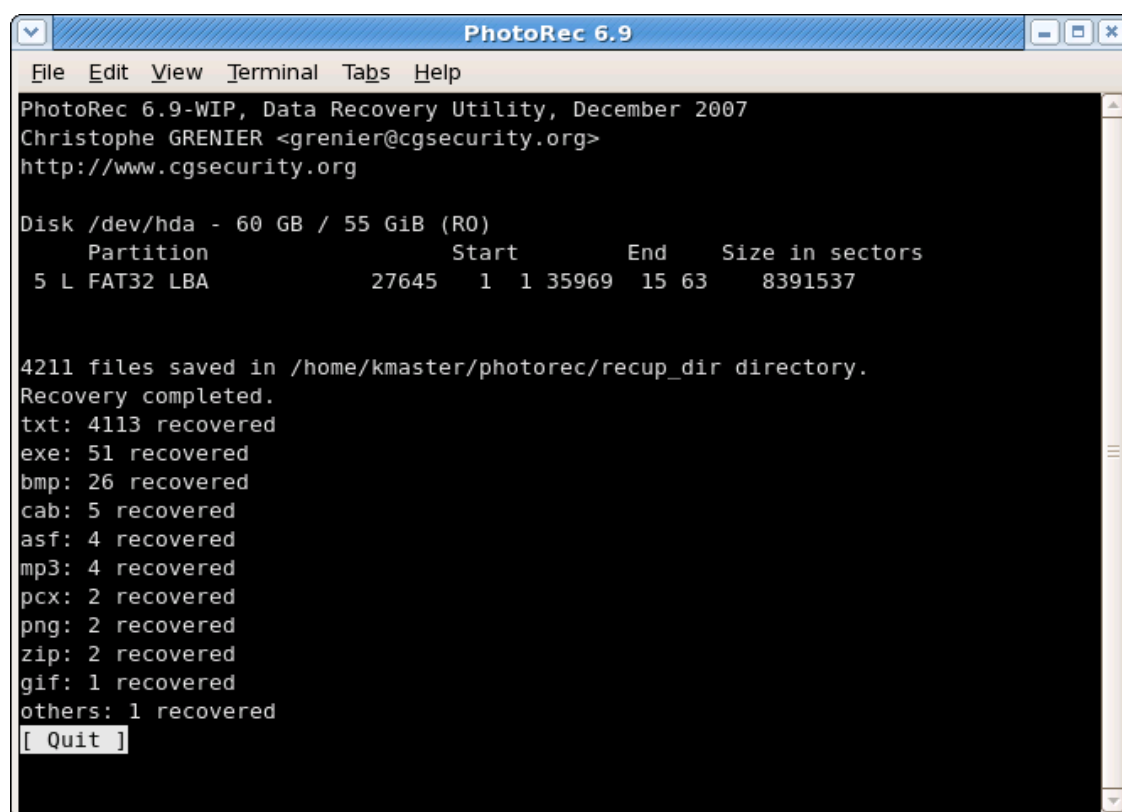


Number of recovered files is updated in real time.

- 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

A screenshot of the PhotoRec 6.9 terminal window. The window has a title bar "PhotoRec 6.9" and a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal text shows the version "PhotoRec 6.9-WIP, Data Recovery Utility, December 2007", the author "Christophe GRENIER <grenier@cgsecurity.org>", and the website "http://www.cgsecurity.org". It then displays disk information for "/dev/hda - 60 GB / 55 GiB (R0)" and a table of partitions. The table has columns "Partition", "Start", "End", and "Size in sectors". The first partition is "5 L FAT32 LBA" starting at "27645" and ending at "1 1 35969 15 63" with a size of "8391537". Below the table, it states "4211 files saved in /home/kmaster/photorec/recup_dir directory." and "Recovery completed." followed by a list of recovered file types: "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", and "others: 1 recovered". At the bottom, there is a "[Quit]" prompt.

```
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 by 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.

[Donate](#)



Please support the project with your [donations](#).