

PhotoRec Step By Step

Downloaded from www.filerecoverycentral.com
Click here for more free tools, advice and tutorials

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. Translation of this PhotoRec manual to other languages are welcome.






Contents

- 1 Run PhotoRec executable
- 2 Disk selection
- 3 Partition table type selection
- 4 Source partition selection
- 5 PhotoRec options
- 6 Selection of files to recover
- 7 File system type
- 8 Carve the partition or unallocated space only
- 9 Select where recovered files should be written
- 10 Recovery in progress
- 11 Recovery is completed

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.

-  Under DOS, run photorec.exe
-  Under Windows, start PhotoRec (ie testdisk-6.9/win/photorec_win.exe) from an account in the Administrator group. Under Vista, right click photorec_win.exe and then click Run as administrator to launch PhotoRec.
-  Under Unix/Linux/BSD, you need to be root to run PhotoRec (ie. `sudo testdisk-6.9/linux/photorec_static`)
-  Under MacOSX, start PhotoRec (ie testdisk-6.9/darwin/photorec). If you are not root, PhotoRec will restart itself using sudo after a confirmation on your part. Sudo will ask for a password - enter your Mac OS X user password.
-  Under OS/2, PhotoRec doesn't handle physical device, only disk images. Sorry.

To recover files from a media image, run

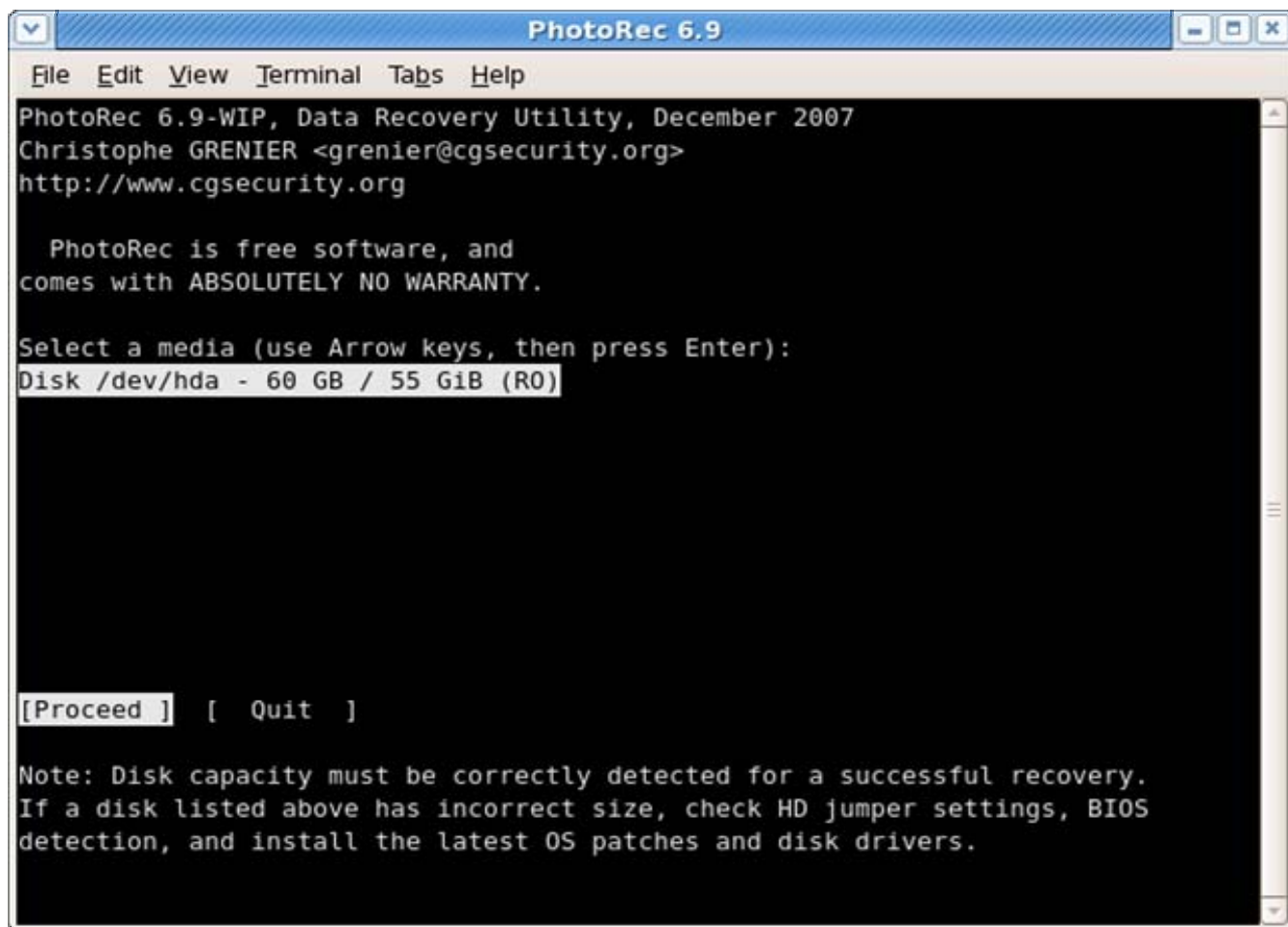
- `photorec image.dd` to carve a raw disk image
- `photorec image.E01` to recover files from an Encase EWF image
- `photorec 'image.???'` if the Encase image is split into several files.
- `photorec '/cygdrive/d/evidence/image.???'` if the Encase image is split into several files in the directory `d:\evidence`

  Most devices should be autodetected including Linux software RAID (ie. `/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



```
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)

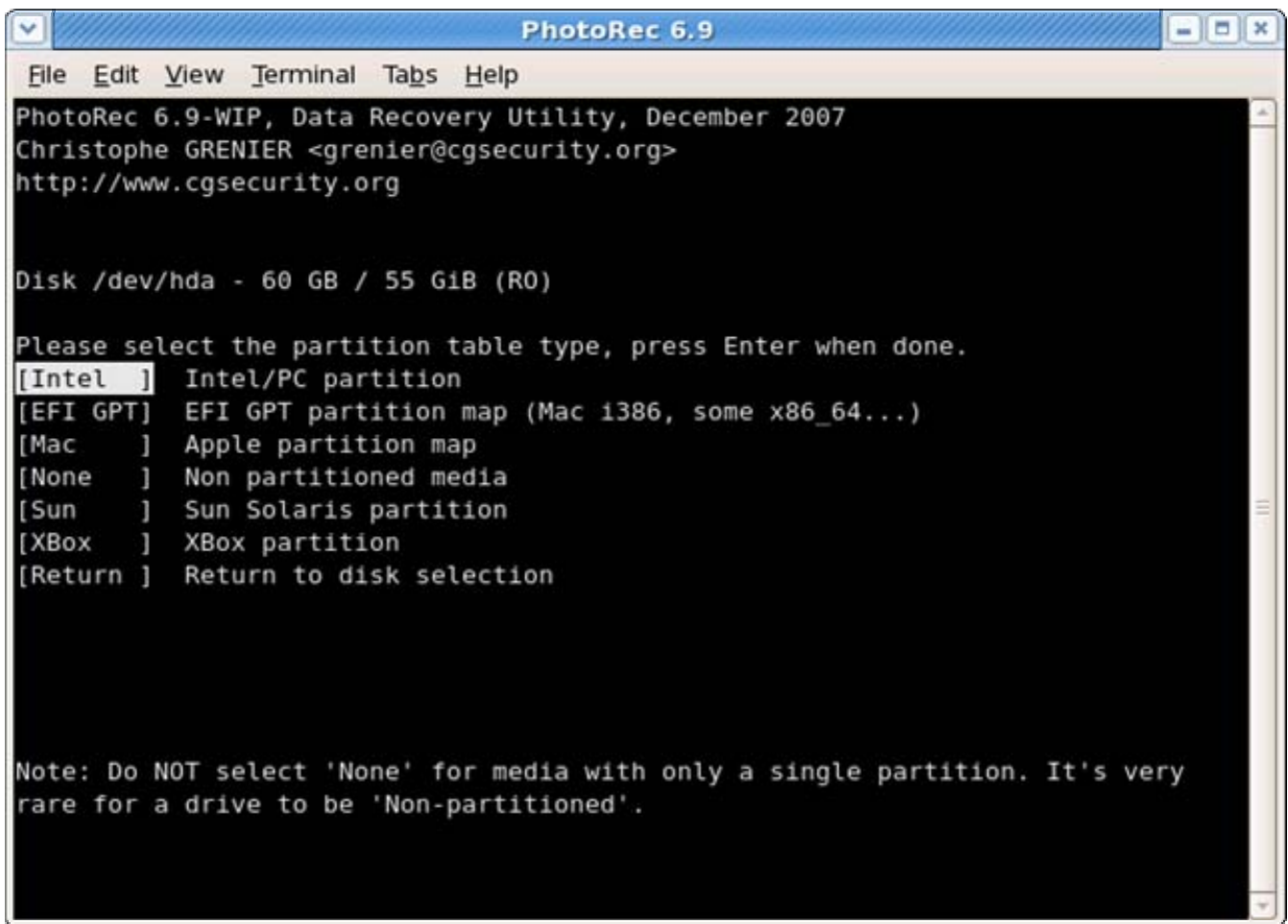
[Proceed] [Quit]

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.

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

Partition table type 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

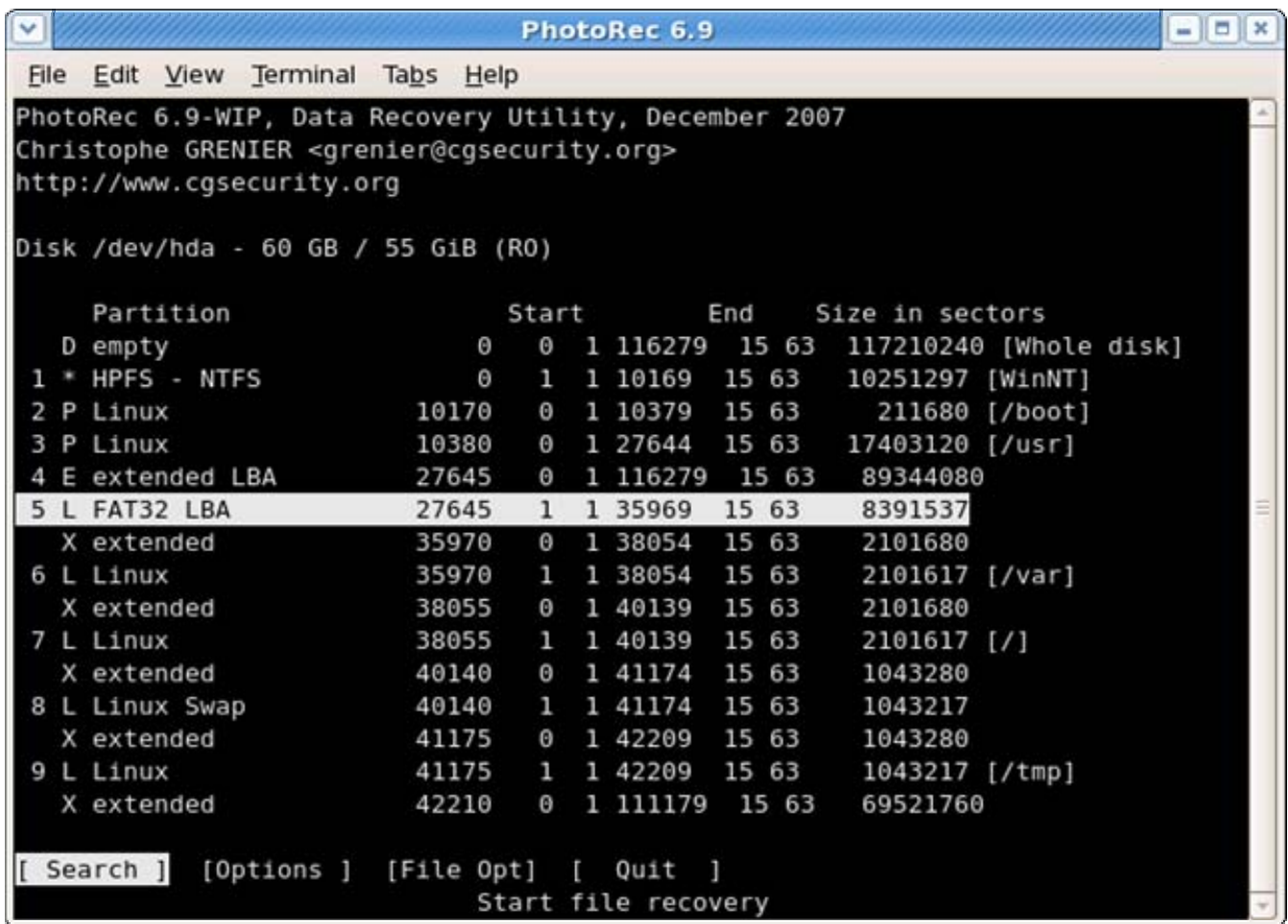
Disk /dev/hda - 60 GB / 55 GiB (R0)

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'.
```

Select the partition table type - usually the default value is the correct one as PhotoRec auto-detects the partition table type.

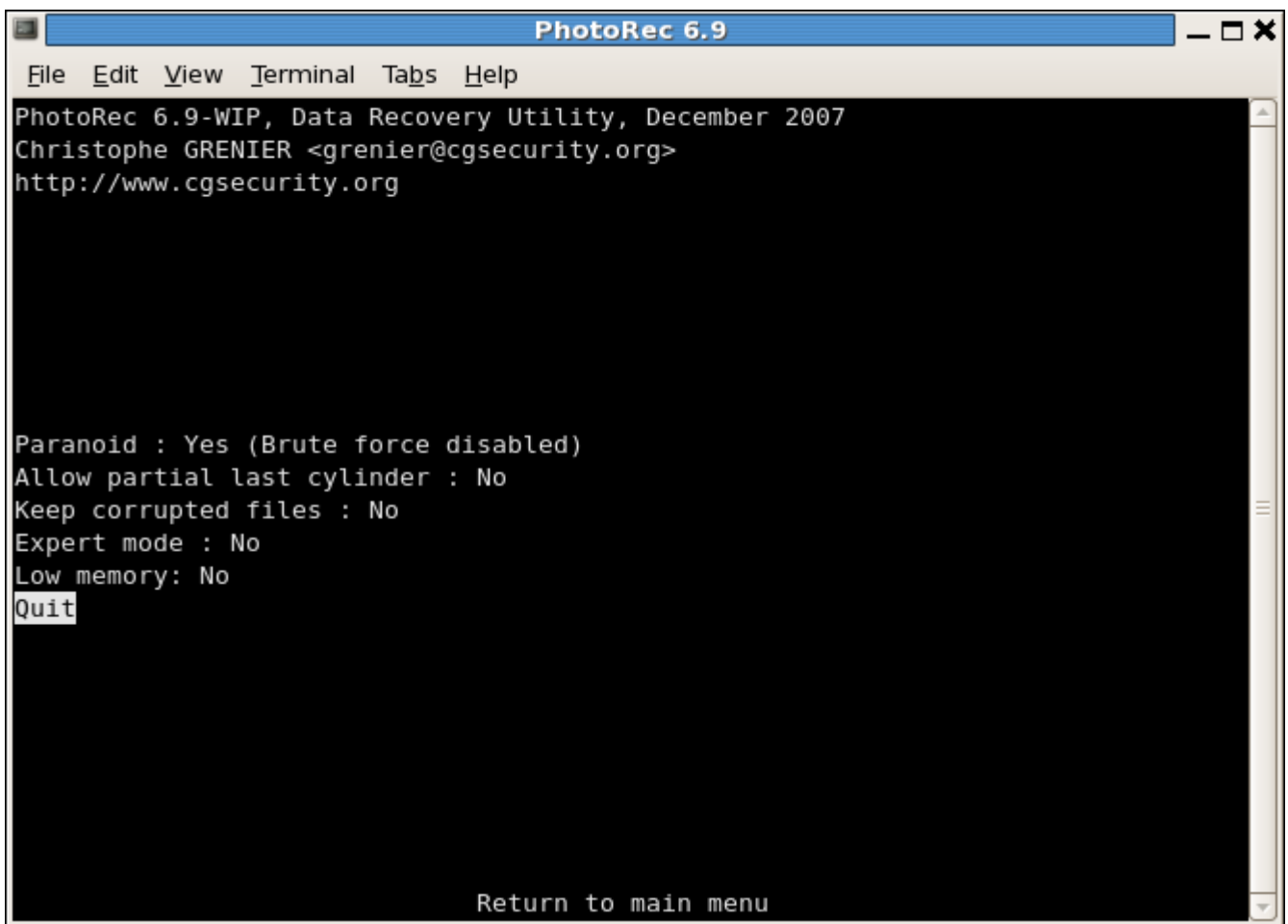
Source partition selection



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

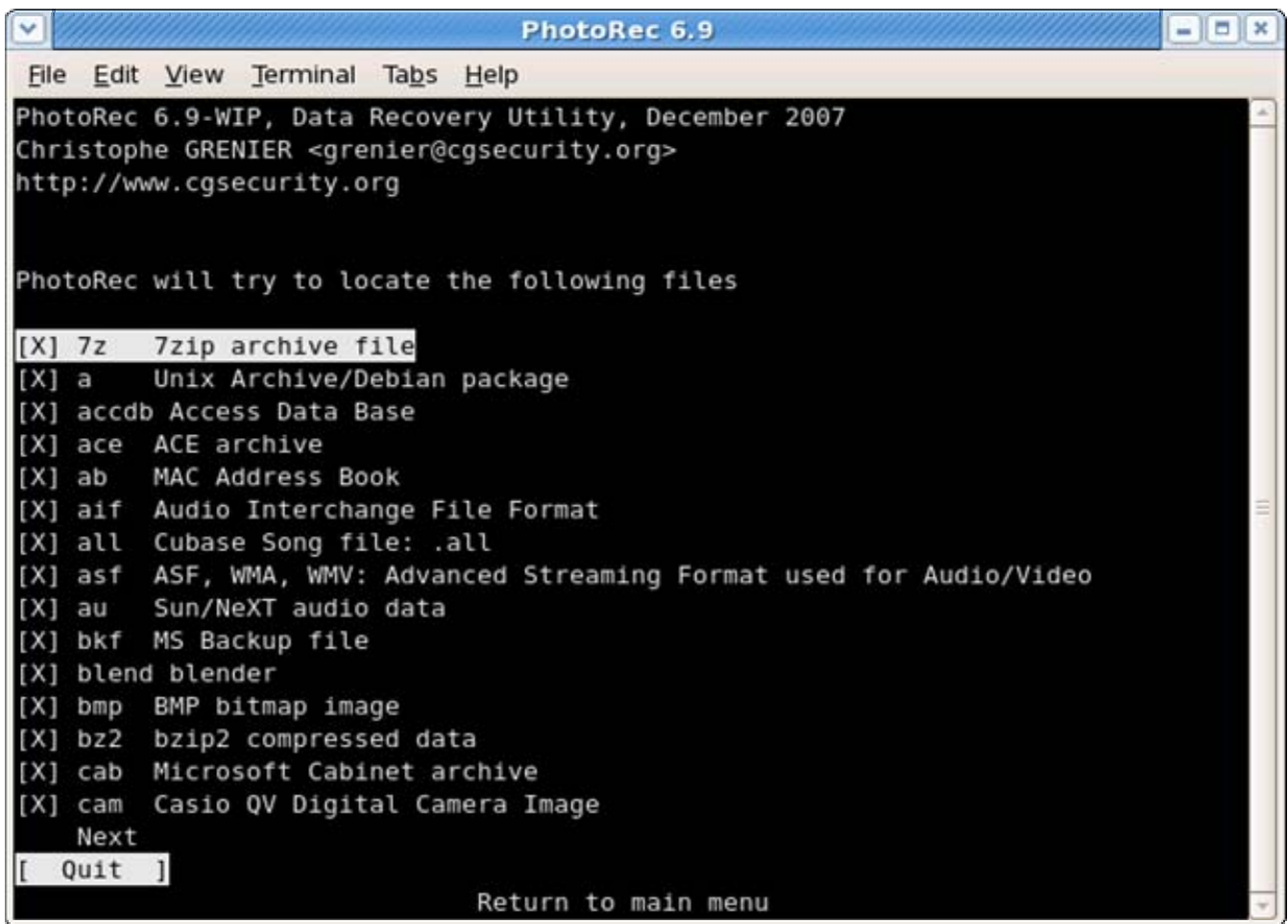


- Paranoid By default, recovered files are verified and invalid files rejected.

Enable `bruteforce` if you want to recover more fragmented JPEG files, note it's 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.
- 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 doesn't have enough memory and crashes during recovery. It may be needed for large file systems that are heavily fragmented. Don't use this option unless absolutely necessary.

Selection of files to recover

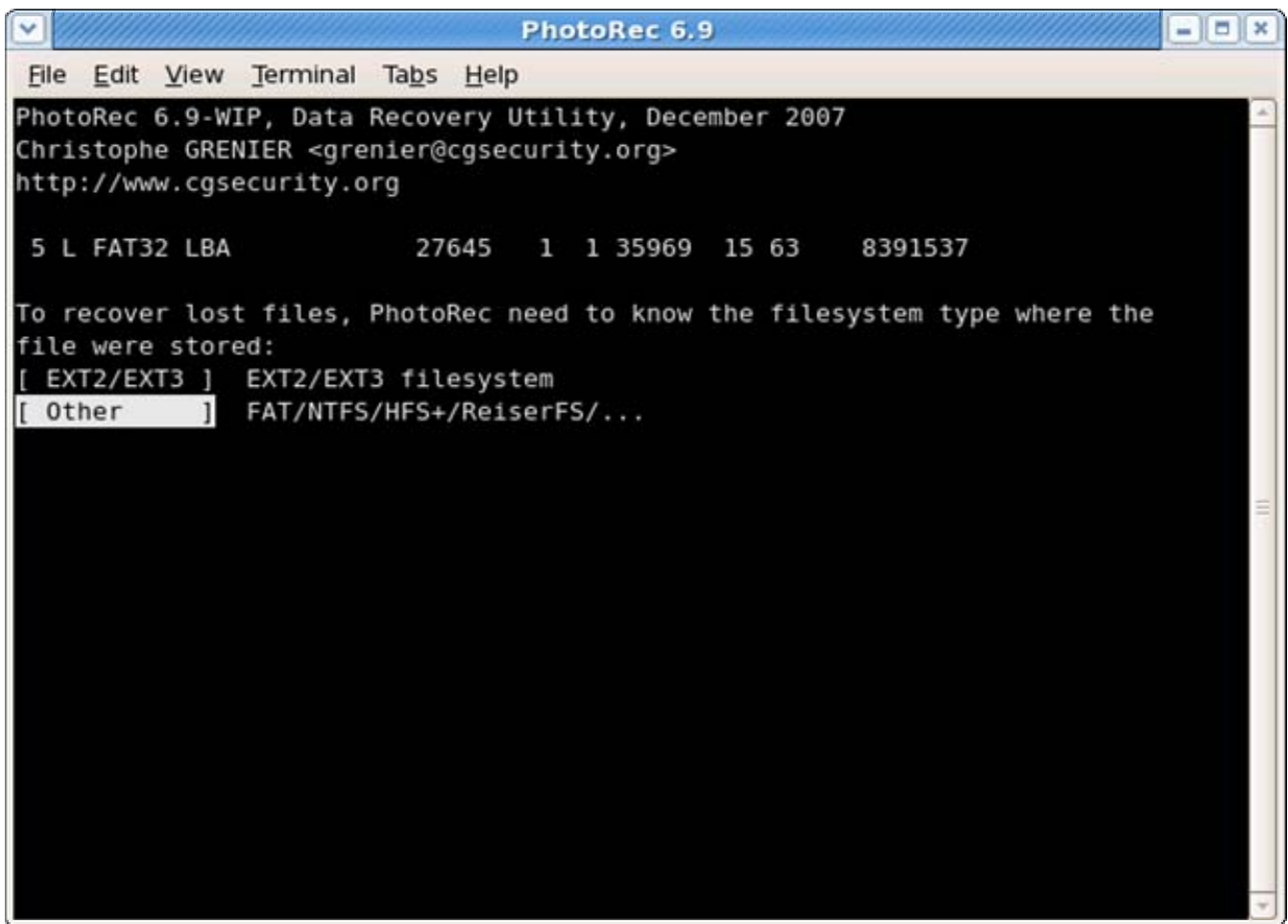


In FileOpts, enable or disable the recovery of certain file types, e.g.

```
[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
```

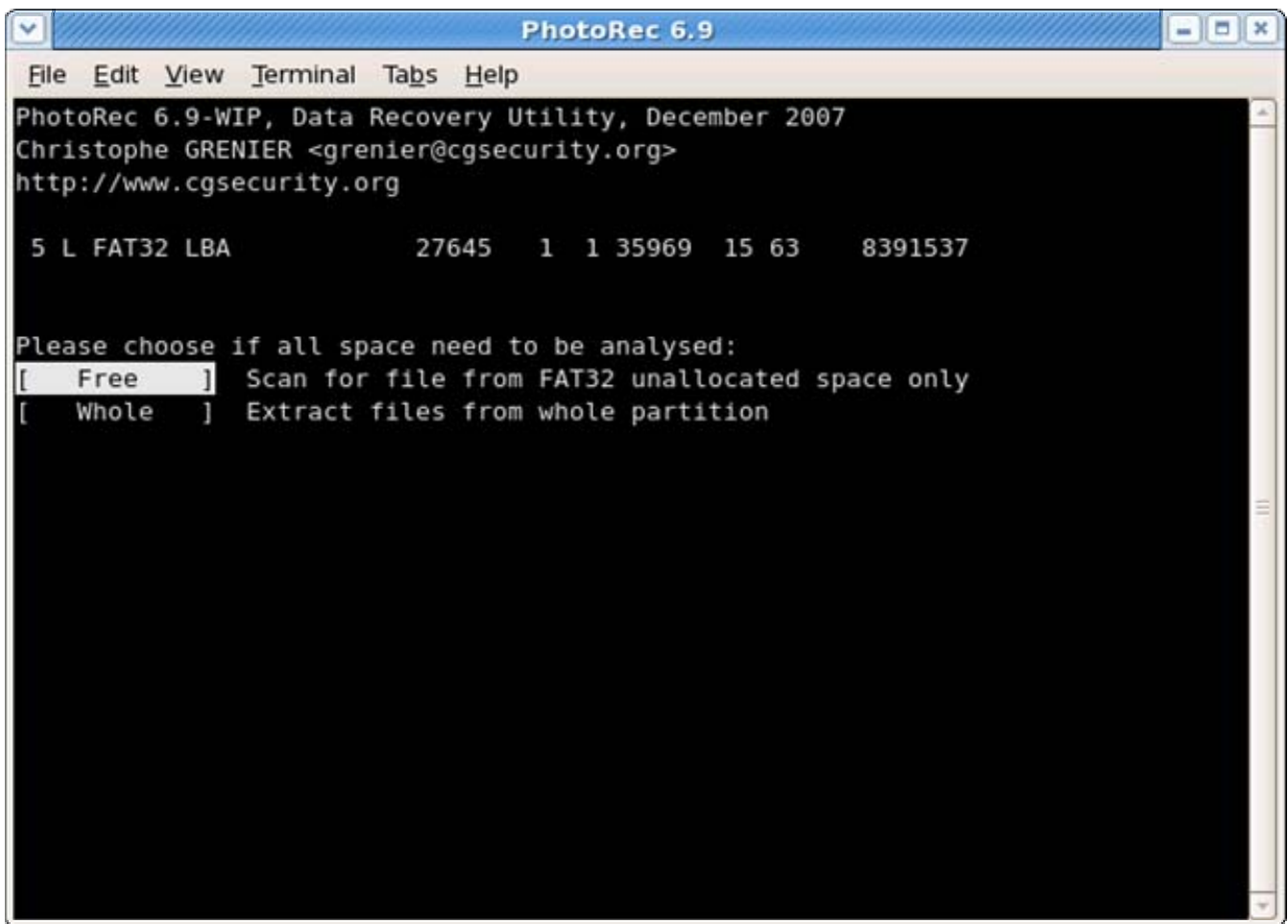
The whole list of file formats recovered by PhotoRec contains more than 320 file families representing more than 200 file extensions.

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's ext2/ext3 filesystem, choose `Other`.

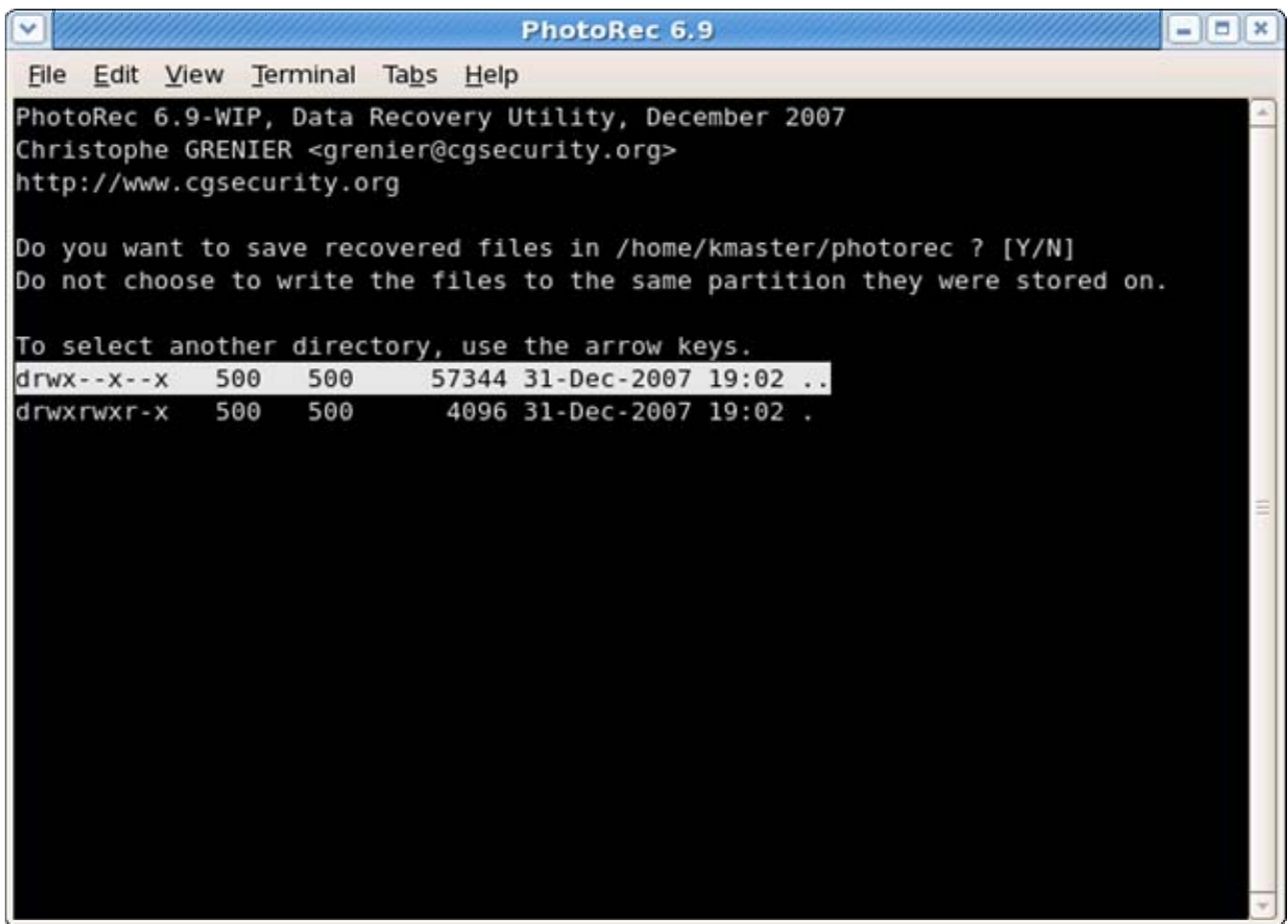
Carve the partition or unallocated space only



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.

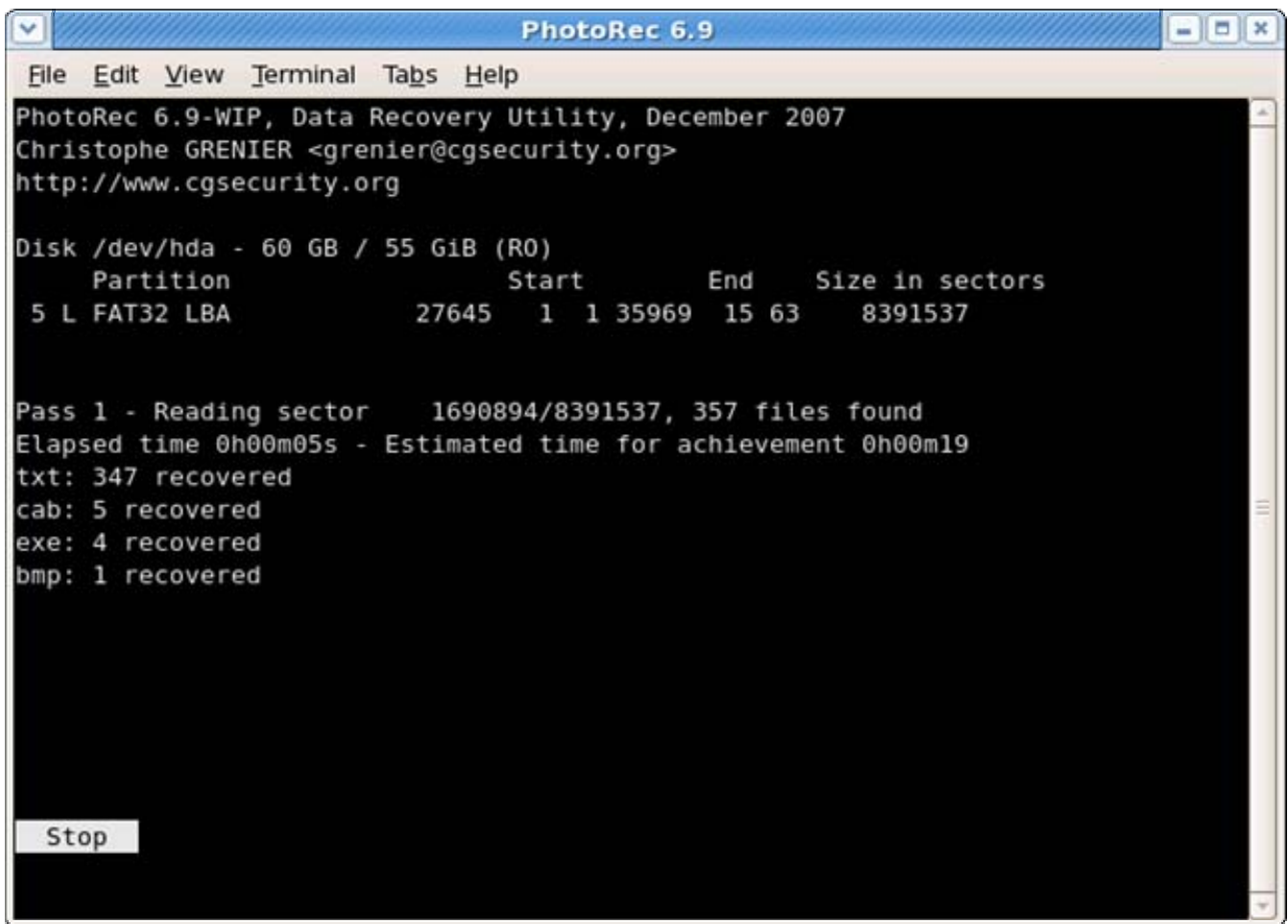
Select where recovered files should be written



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` or `/mnt` sub-directory.
- **X** Partitions from external disk are usually mounted in `/Volumes`.

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

```
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.

- 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.

Category: Data Recovery

- This page was last modified on 9 April 2010, at 07:19.
- Content is available under GNU Free Documentation License 1.2.