

PhotoRec passo-a-passo

From CGSecurity

 English  Deutsch  Español  Français  Italiano  Português  Română  Русский

Este *Exemplo de recuperação* orienta-o passo-a-passo através do PhotoRec, para arquivos deletados, dados perdidos de uma partição reformatada ou um sistema de arquivos corrompido. Para partições deletadas/perdidas ou arquivos deletados de um sistema de arquivos FAT ou NTFS, tente TestDisk primeiro - ele é geralmente mais rápido, e TestDisk pode restabelecer os nomes originais dos arquivos. Traduções para este manual do PhotoRec para outros idiomas são bem vindos.






Contents

- 1 Abra o executável do PhotoRec
- 2 Seleção do Disco
- 3 Seleção da partição de origem
- 4 Opções do PhotoRec
- 5 Seleção dos arquivos para recuperar
- 6 Tipo do sistema de arquivos
- 7 Grave a partição ou só o espaço não alocado
- 8 Selecione onde os arquivos recuperados podem ser gravados
- 9 Recuperação em progresso
- 10 A recuperação está completa

Abra o executável do PhotoRec

Se o PhotoRec não estiver instalado ainda, ele pode ser baixado de TestDisk Download. Extraia os arquivos do zip incluindo os sub-diretórios.

Para recuperar arquivos de um disco rígido, pen drive, Smart Card(Cartão com chip), CD-ROM, DVD, etc., você precisa de privilégios necessários para acessar o dispositivo físico.

-  Sobre o DOS, execute `photorec.exe`
-  Sobre o Windows, inicie PhotoRec (ex.: `testdisk-6.13/photorec_win.exe`) a partir de uma conta no grupo Administrador. Sobre Windows Vista ou posterior, clique com o botão direito em `photorec_win.exe` e então clique em executar como administrador para abrir o PhotoRec.
-  Sobre Unix/Linux/BSD, você precisa ser superusuário (root) para executar o PhotoRec (ex.: `sudo testdisk-6.13/photorec_static`)
-  Sobre Mac OS X, inicie PhotoRec (ex.: `testdisk-6.13/photorec`). Se você não é superusuário, o PhotoRec irá iniciar-se usando `sudo` depois de uma confirmação de sua parte. O `sudo` irá perguntar por uma senha - insira sua Mac OS X senha de usuário.
-  Sobre OS/2, o PhotoRec não manipula dispositivos físicos, só imagens de discos. Desculpe.

Para recuperar arquivos de uma mídia de imagem, execute

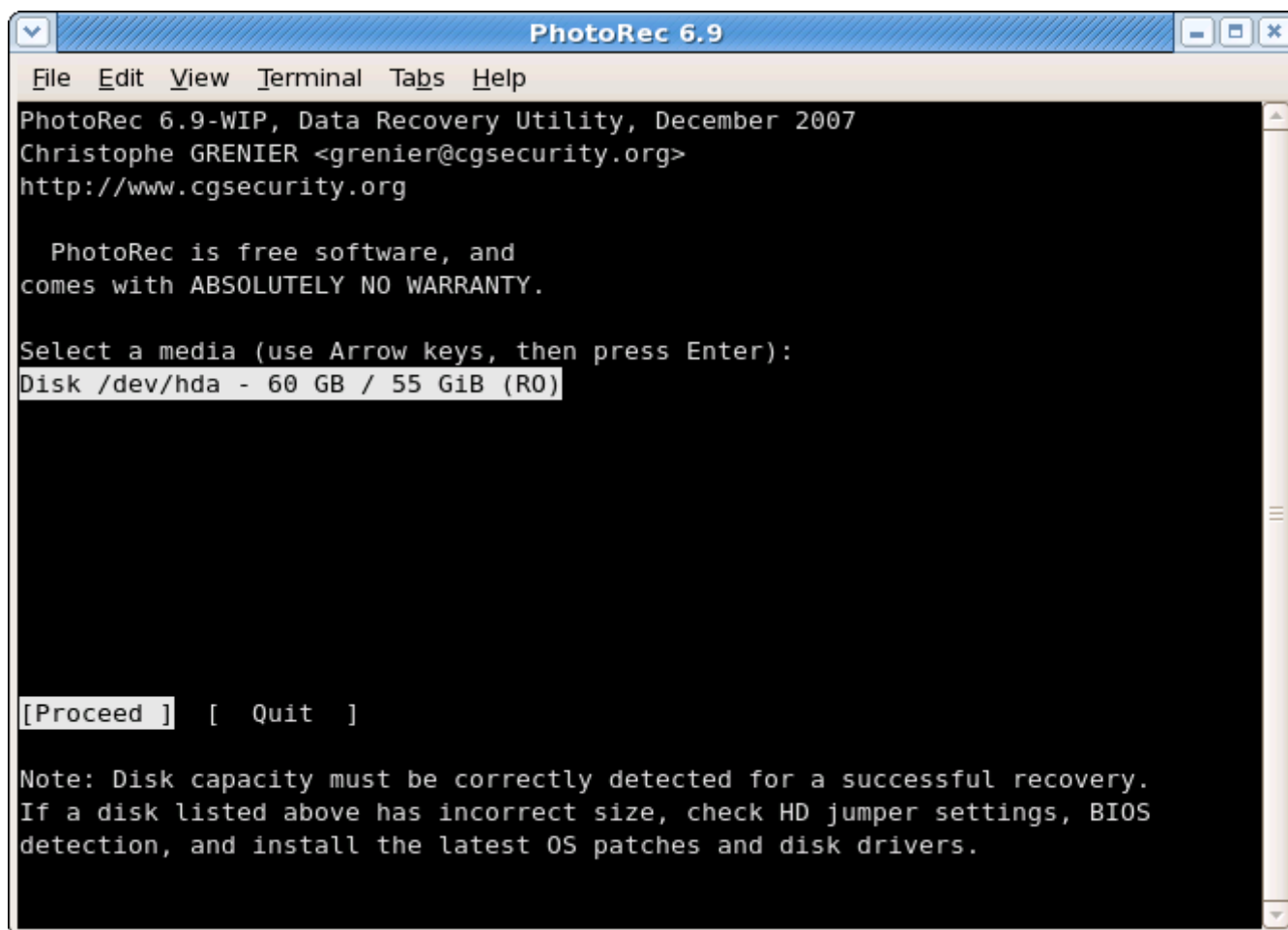
- `photorec image.dd` para entalhar(gravar) uma imagem de disco
- `photorec image.E01` para recuperar arquivos de uma imagem Encase EWF
- `photorec 'image.???'` Se a imagem Encase estiver dividida em vários arquivos.

- `photorec '/cygdrive/d/evidence/image.???'` Se a imagem Encase estiver dividida em vários arquivos no diretório `d:\evidence`

X A maioria dos dispositivos podem ser detectados inclusive software Linux RAID (isto é, `/dev/md0`) e arquivos de sistema encriptados com `cryptsetup`, `dm-crypt`, `LUKS` ou `TrueCrypt` (ex.: `/dev/mapper/truecrypt0`). Para recuperar arquivos a partir de outro dispositivo, execute `photorec device`.

Usuários forenses podem usar o parâmetro `/log` para criar um arquivo de log chamado `photorec.log`; ele grava a localização dos arquivos recuperados pelo PhotoRec.

Seleção do Disco



As mídias disponíveis são listadas. Use as teclas cima/baixo para selecionar os discos que contêm os arquivos perdidos.

Pressione Enter para prosseguir.

X Se disponível, use dispositivo raw, `/dev/rdisk*` ao invés de `/dev/disk*` para uma recuperação dos dados mais rápida.

Seleção da partição de origem

```

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

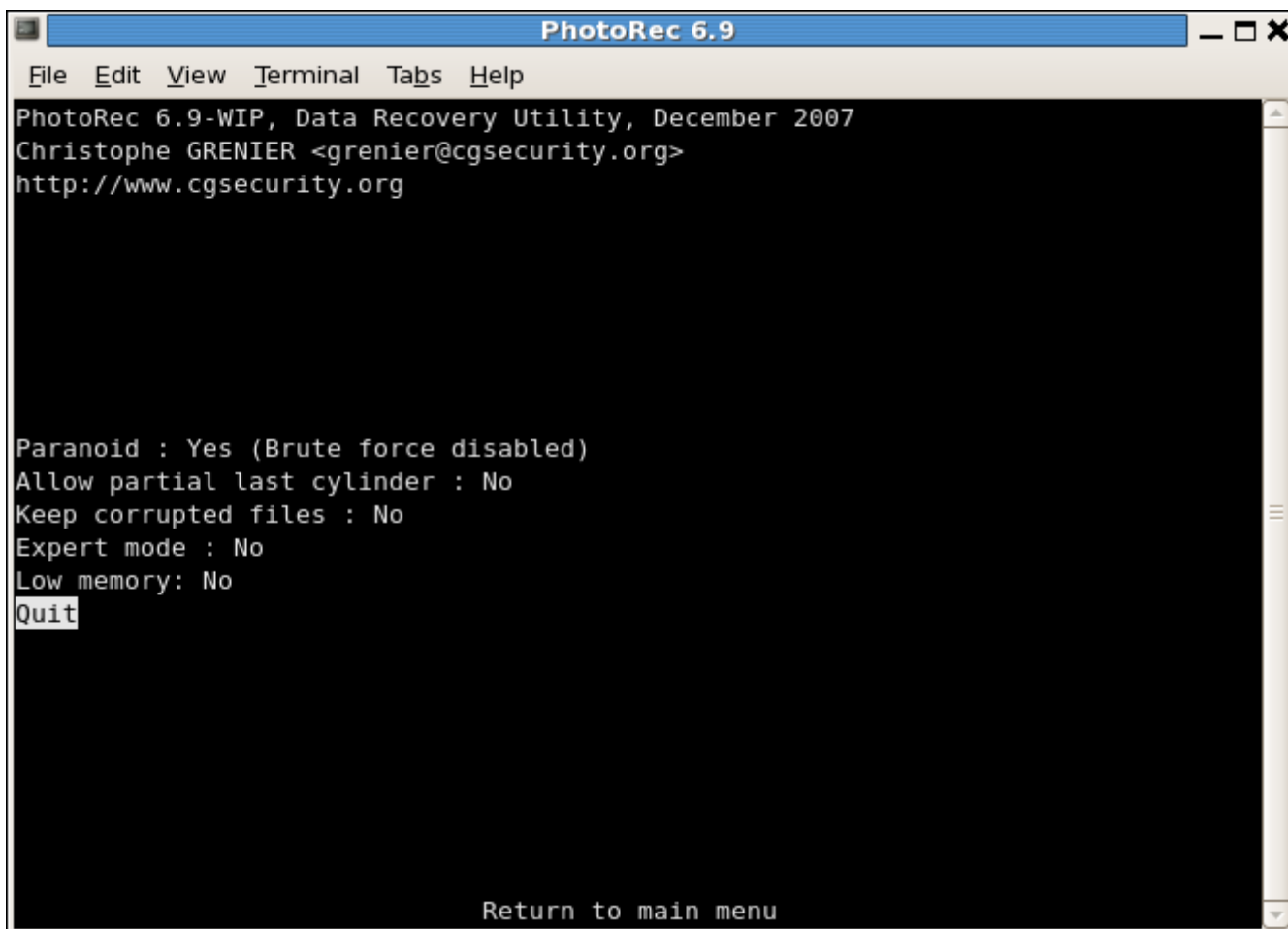
[ Search ] [ Options ] [ File Opt ] [ Quit ]
Start file recovery

```

Escolha

- Procurar depois de seleccionar a partição que contem os arquivos perdidos para iniciar a recuperação,
- Opções para modificar as opções,
- Opções de arq para modificar a lista de tipos de arquivos recuperados pelo PhotoRec.

Opções do PhotoRec



```
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

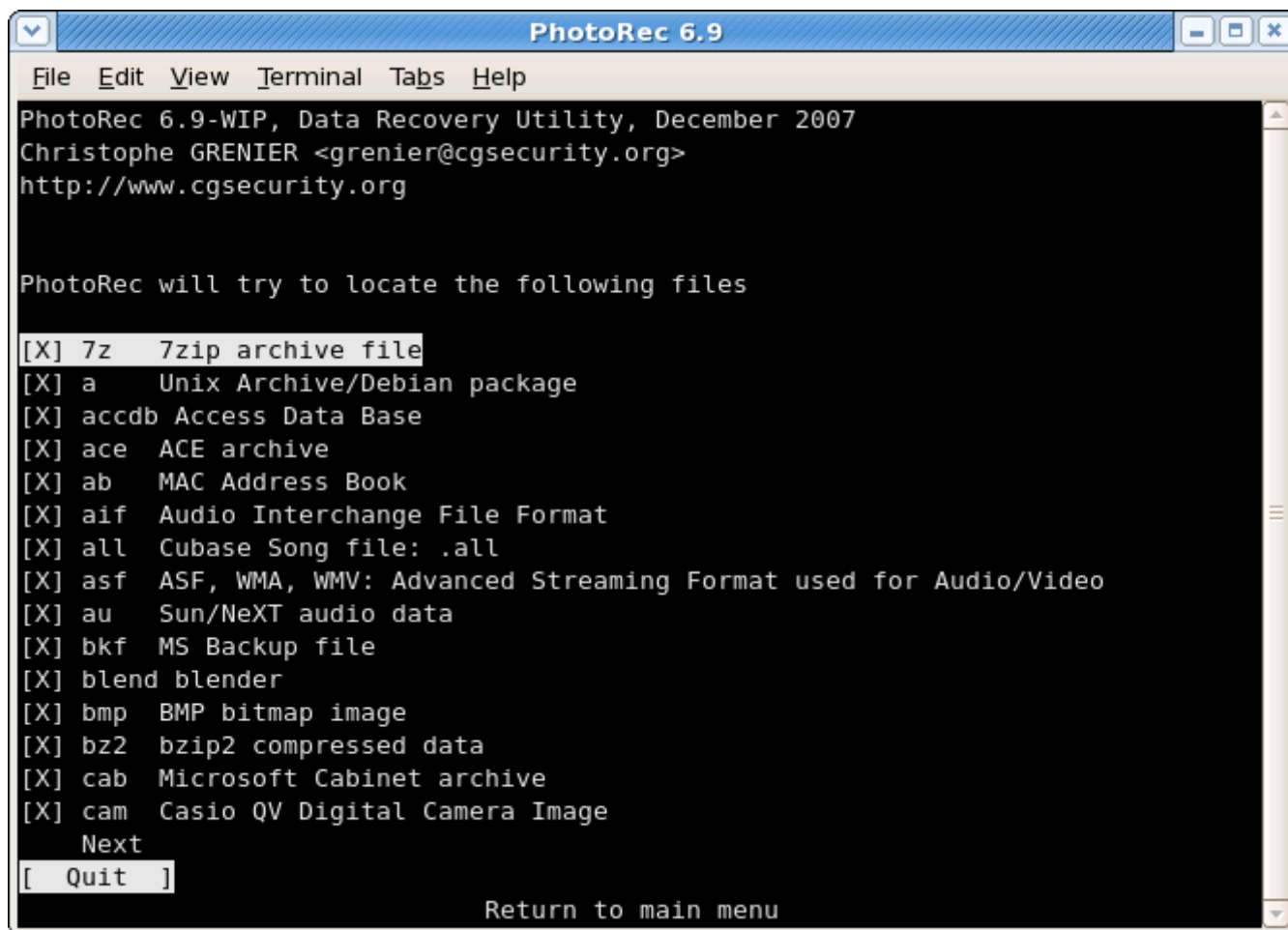
Return to main menu
```

- Paranóia Por padrão, arquivos recuperados não verificados e arquivos inválidos rejeitados.

Habilite forçabruta se você quer recuperar arquivos JPEG fragmentados, observe que isso requer uma operação intensa do CPU.

- Permitir último cilindro parcial modifica como a geometria dos disco é modificada - só mídias não particionadas podem ser afetadas.
- A opção modo expert permite o usuário forçar o tamanho do bloco do sistema de arquivos e o offset. Cada sistema de arquivos tem seu próprio tamanho de bloco (um múltiplo do tamanho do setor) e o offset (0 para NTFS, exFAT, ext2/3/4), esses valores são fixos quando o sistema de arquivos foi criado/formatado. Quando se trabalha com o disco inteiro(ex.: partições originais são perdidas) ou uma partição reformatada, se o PhotoRec encontrar muito poucos arquivos, você pode tentar o mínimo valor que o PhotoRec deixa você selecionar(ele é o tamanho do setor) para o tamanho do bloco (0 será usado para o offset).
- Habilite Mantenha arquivos corrompidos para guardar arquivos mesmo que eles sejam inválidos na esperança que os dados ainda possam ser salvos de um arquivo inválido usando outras ferramentas.
- Habilite Memória baixa se seu sistema não tem memória suficiente e ele falha durante a recuperação. Pode ser necessário para grandes sistemas de arquivos que estejam gravemente fragmentados. Não use esta opção a menos que seja absolutamente necessário.

Seleção dos arquivos para recuperar

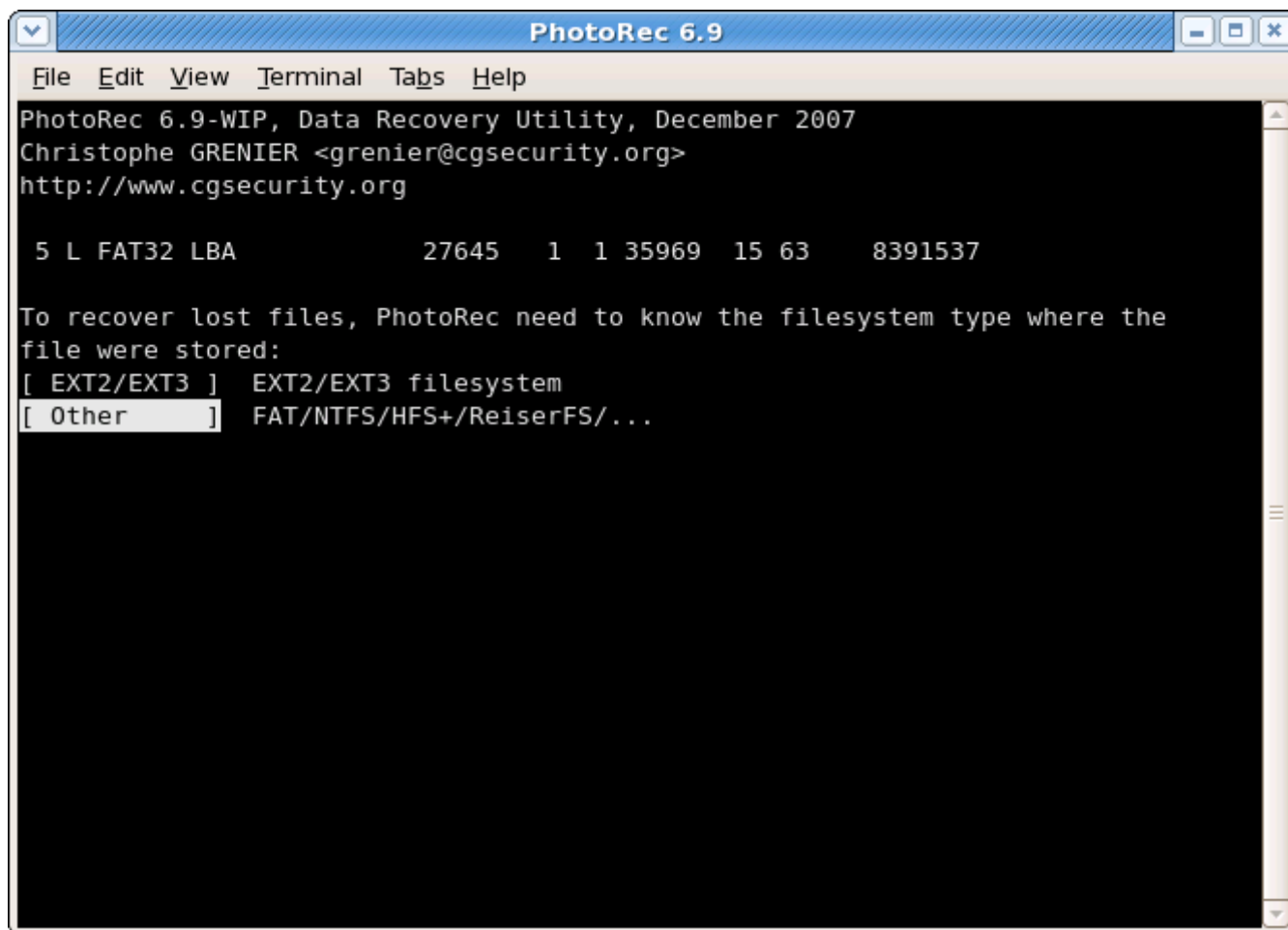


Em Opções de Arquivo, habilite ou desabilite a recuperação de certos tipos de arquivos, por exemplo,

```
[X] riff RIFF audio/video: wav, cdr, avi
...
[X] tif marque Image File Format e alguns formatos de arquivo em raw (pef/nef/dcr/sr2/cr2)
...
[X] zip arquivo zip inclusive OpenOffice e MSOffice 2007
```

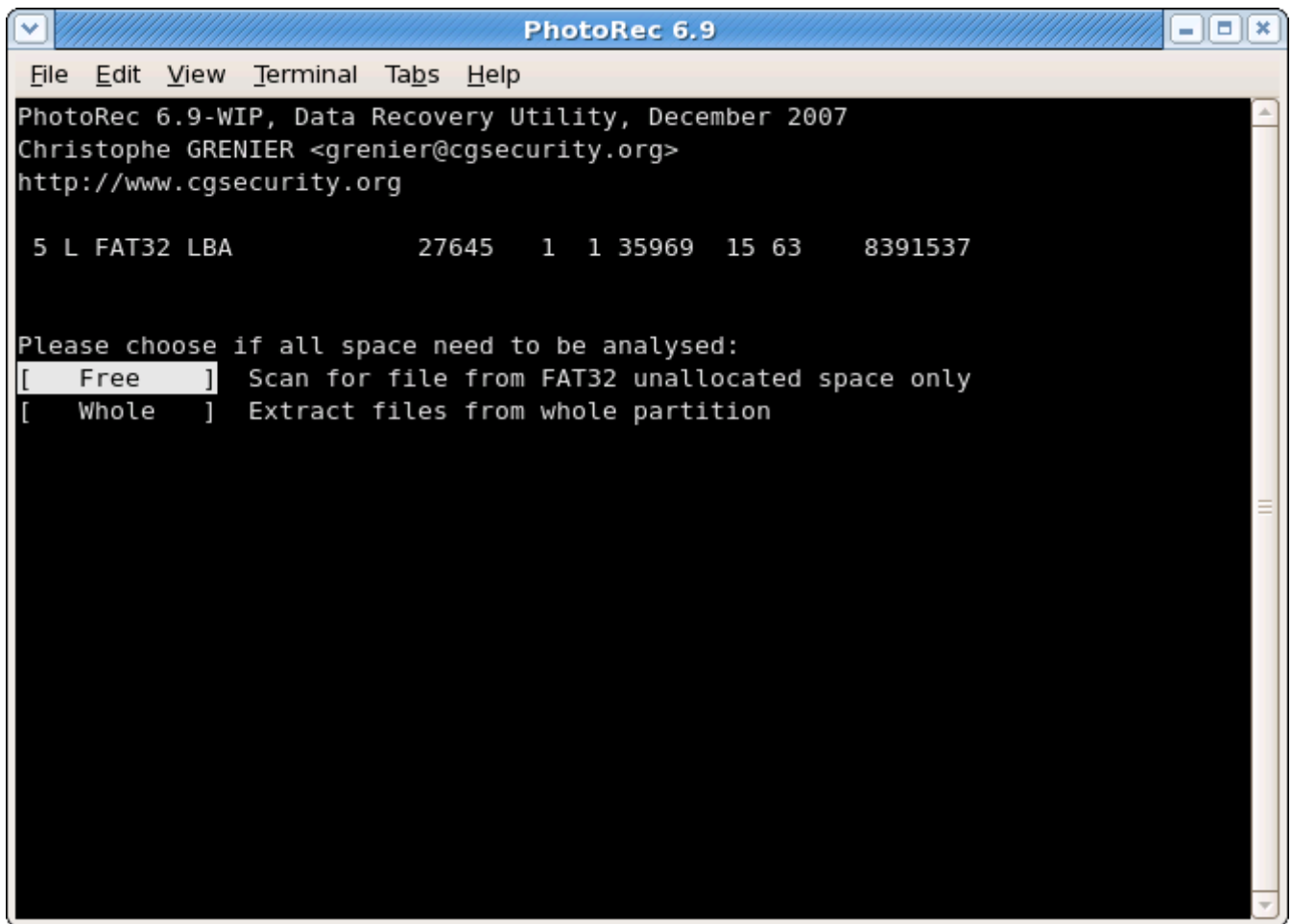
A lista completa de formato de arquivos recuperados pelo PhotoRec contém mais de 320 famílias de arquivos representando mais de 200 extensões de arquivos.

Tipo do sistema de arquivos



Uma vez que a partição foi selecionada validada com Porcurar, O PhotoRec precisa saber como os dados dos blocos são alocados. A menos que ele seja uma sistema de arquivos ext2/ext3/ext4 , escolha outro.

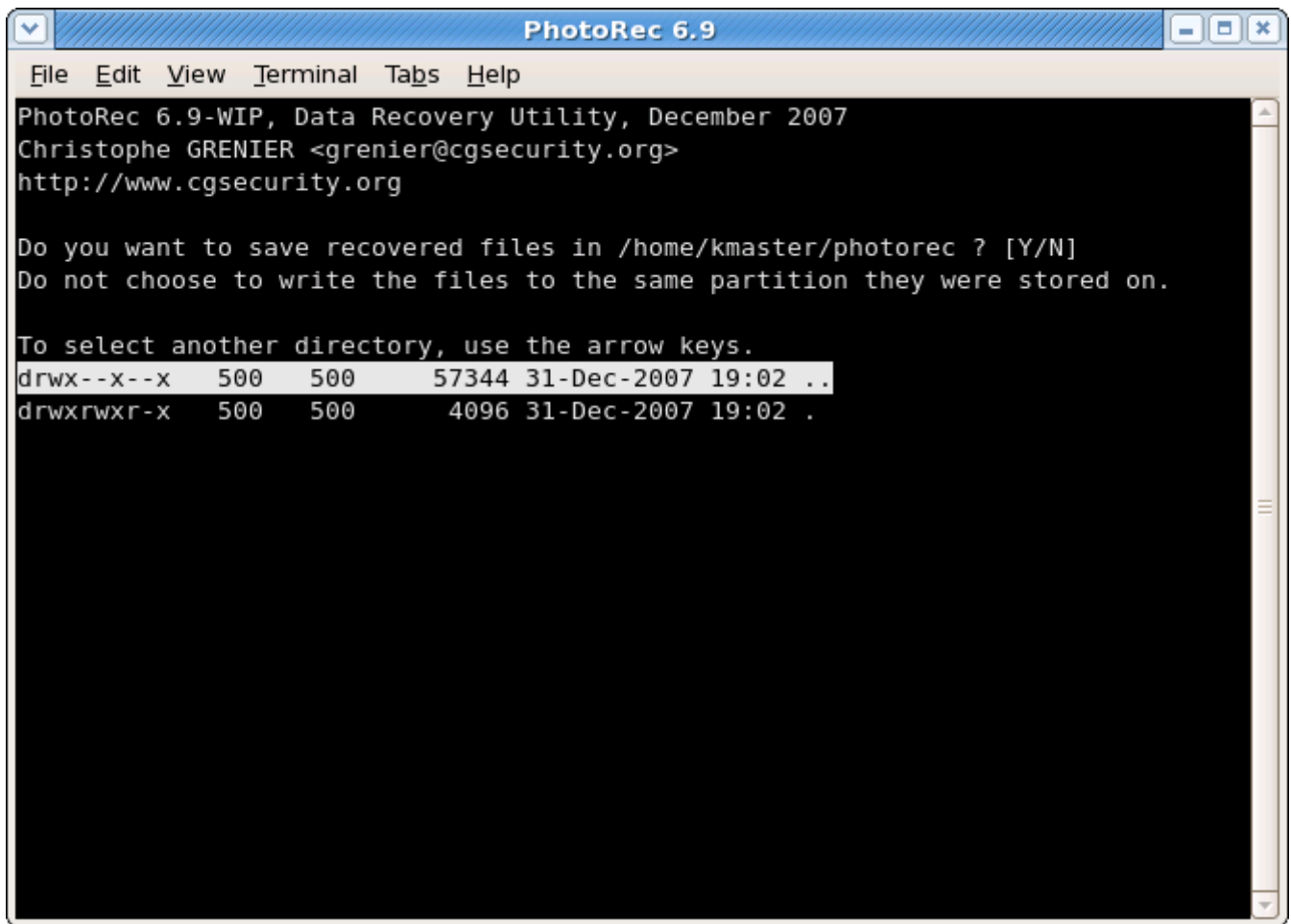
Grave a partição ou só o espaço não alocado



O PhotoRec pode procurar arquivos de:

- de uma partição inteira (útil quando o sistema de arquivos está corrompido) ou
- somente de um espaço não alocado (disponível para ext2/ext3/ext4, FAT12/FAT16/FAT32 e NTFS). Com esta opção, só os arquivos deletados são recuperados.

Selecione onde os arquivos recuperados podem ser gravados






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

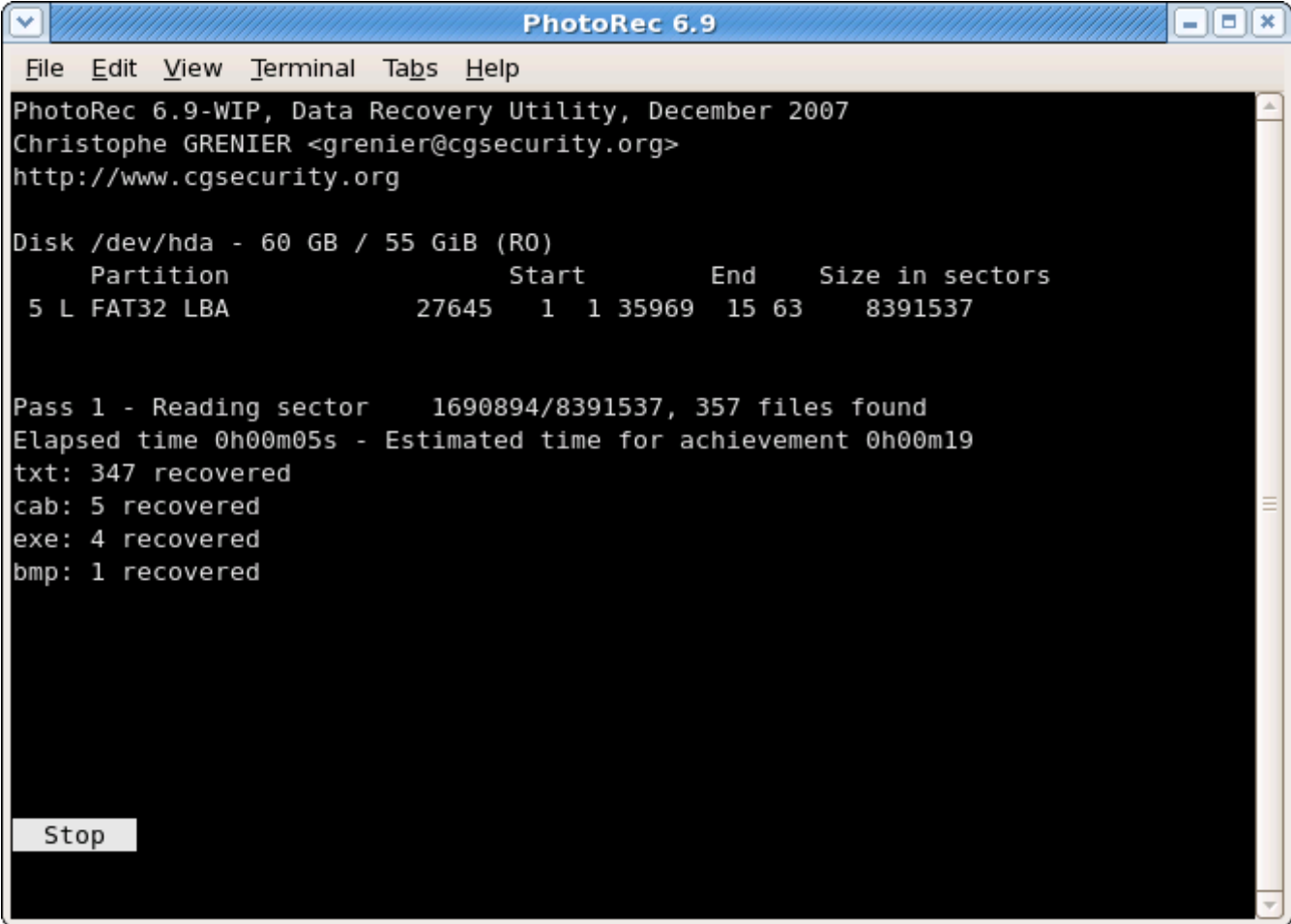
Do you want to save recovered files in /home/kmaster/photorec ? [Y/N]
Do not choose to write the files to the same partition they were stored on.

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 .
```

Escolha o diretório onde os arquivos recuperados podem ser gravados.

-  Para obter a lista de drives de disco (C:, D:, E:, etc.), use as teclas de seta para selecionar .., pressione a tecla Enter - repita até você selecionar o drive de disco de sua escolha. Valide com sim quando você chegar ao destino esperado.
-  Um sistema de arquivos de um disco externo pode estar disponível em /media, /mnt ou /run/mediasub-directório.
-  As partições de um disco externo são geralmente montadas em /Volumes.

Recuperação em progresso



```
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

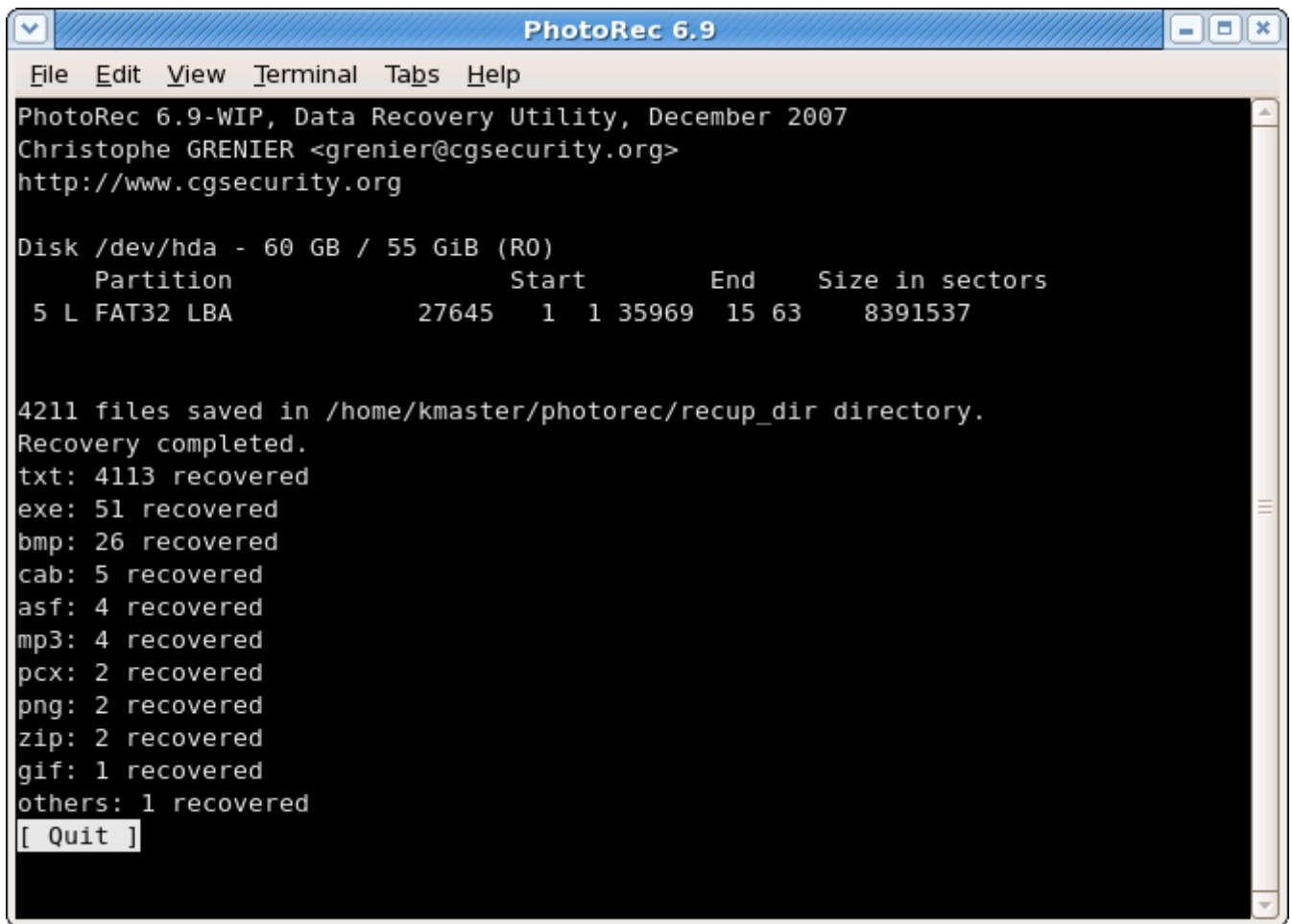
Stop
```

O número de arquivos recuperados é atualizado em tempo real.

- Durante pass 0, O PhotoRec procura os 10 primeiros arquivos para determinar o tamanho do bloco.
- Durante pass 1 e depois, arquivos são recuperados, inclusive alguns arquivos fragmentados.

Os arquivos recuperados são gravados nos sub-diretórios `recup_dir.1`, `recup_dir.2`, etc. É possível acessar os arquivos mesmo se o processo de recuperação não estiver terminado.

A recuperação está completa




```
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 ]
```

Quando a recuperação está completa, um relatório é mostrado. Note que se você interromper a recuperação, da próxima vez que o PhotoRec for reiniciado você será perguntado se quer retomar a recuperação.

- Miniaturas encontradas dentro das fotos são salvas como `t*.jpg`
- Se você escolheu arquivos corrompidos/fragmentos de arquivos, seus nomes de arquivos iniciarão pela letra `q`(uebrado).
- Depois de usar o PhotoRec: Algumas ideias para ordenar arquivos recuperados ou reparar os quebrados.
-  Pode ser que você tenha desabilitados sua proteção anti-vírus durante a recuperação para acelerar o processo, mas é recomendado scanear os arquivos recuperados a procura de vírus antes de abri-los - O PhotoRec pode ter recuperado um documento infectado ou um cavalo de tróia.



Porfavor mantenha o projeto com suas doações.

Retrieved from "http://www.cgsecurity.org/mw/index.php?title=PhotoRec_passo-a-passo&oldid=8206"

Category: Data Recovery

- This page was last modified on 18 January 2016, at 19:43.
- Content is available under GNU Free Documentation License 1.2 unless otherwise noted.