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

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 necessarios para acessar o dispositivo físico.

- Sobre o DOS, execute `photorec.exe`
- Sobre o Windows, inicie PhotoRec (ex.: `testdisk-6.13/photorec_win.exe`) apartir 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

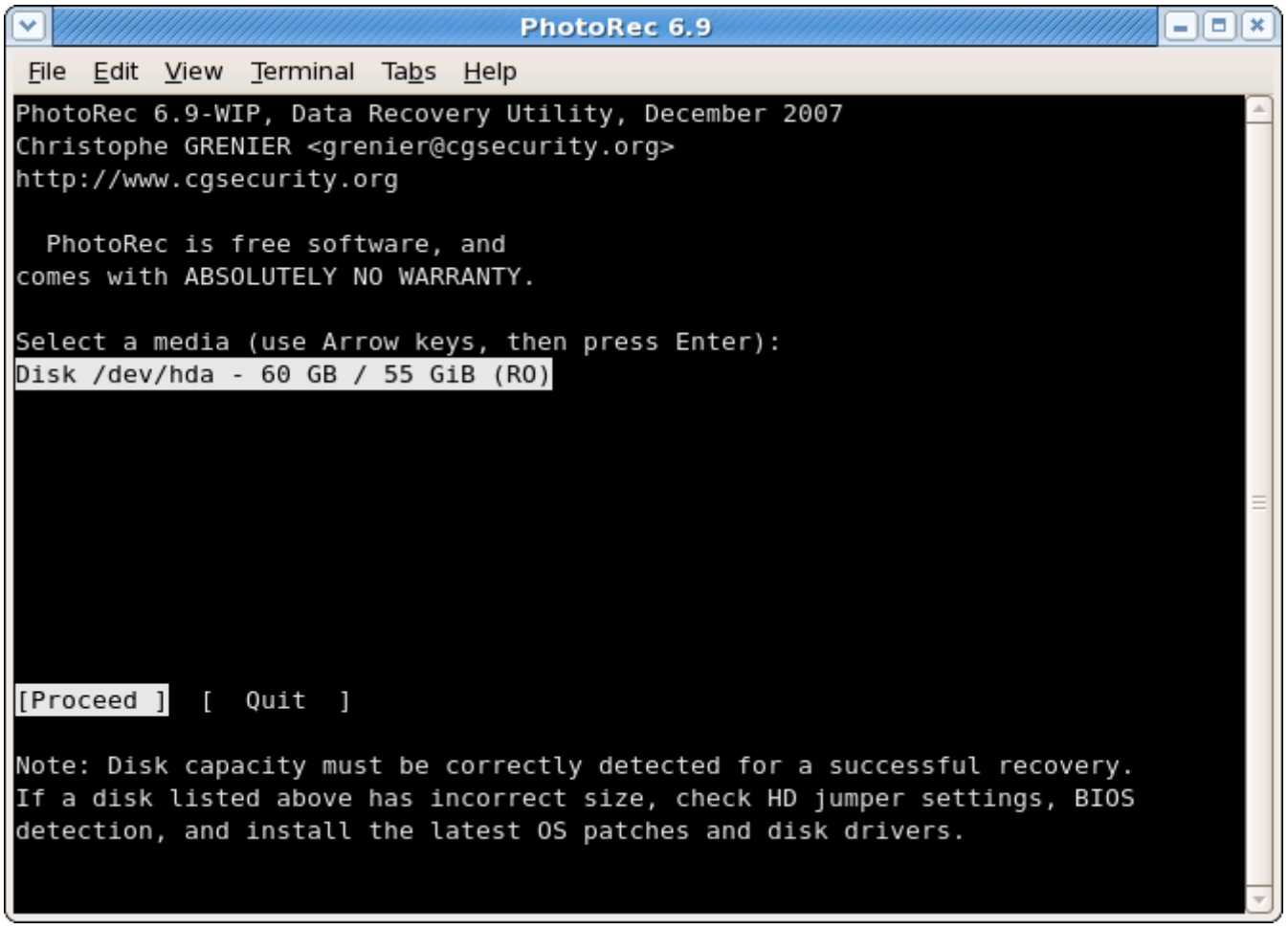
- `photorec image.dd` para entalhar(gravar) uma imgem de disco
- `photorec image.E01` para recuperar arquivos de uma imagem Encase EWF
- `photorec 'image.???'` Se a imagem Encase estiver dividida em vários arquivos.

- `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 sitema encriptados com cryptsetup, dm-crypt, LUKS ou TrueCrypt (ex.:. `/dev/mapper/truecrypt0`). Para recuperar arquivos apartir 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

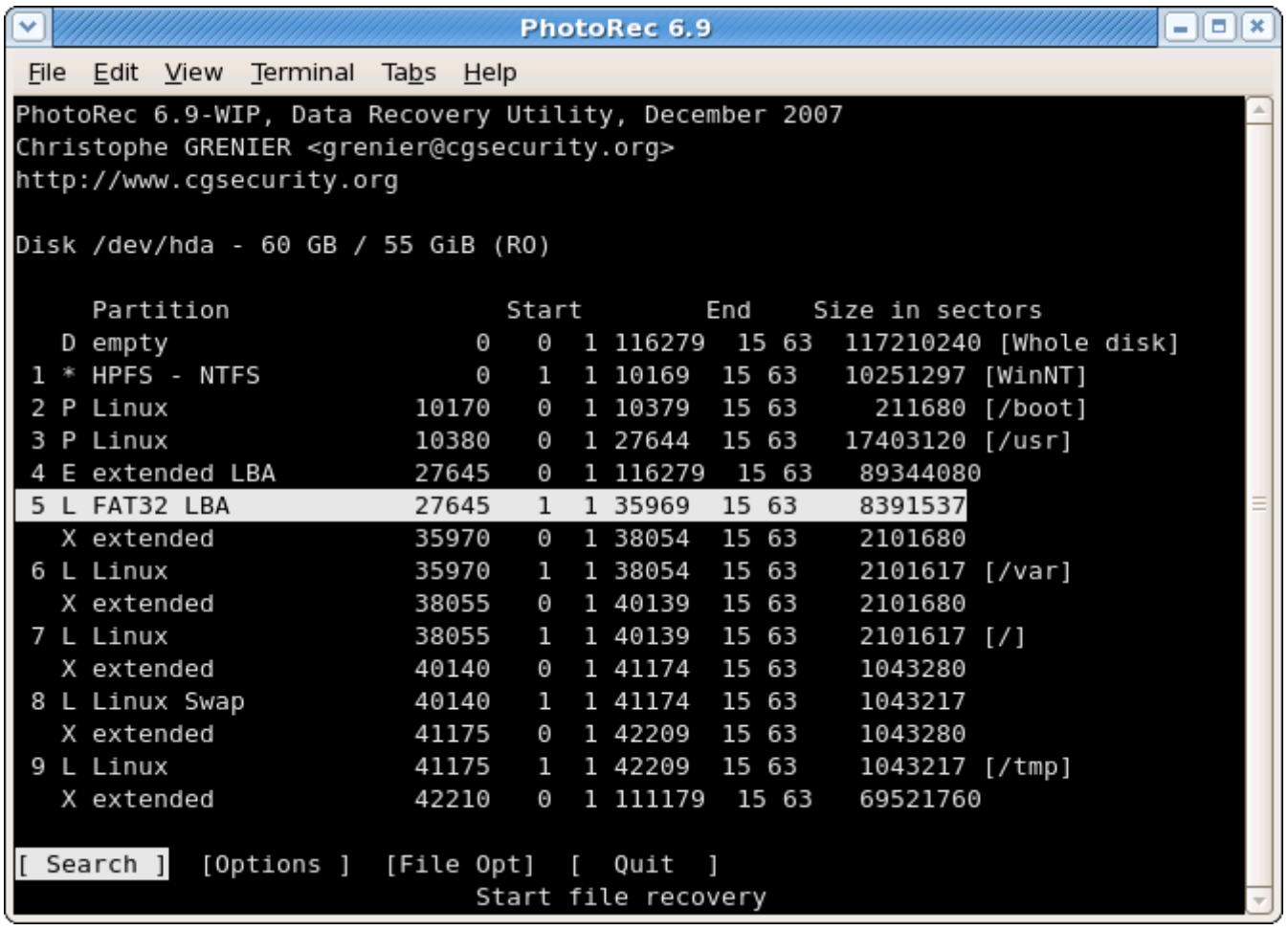


As mídias disponíveis são listadas. Use as teclas cima/baixo para celecionar os discos que contém os arquivos perdidos.

Pressione `Enter` para prosseguir.

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

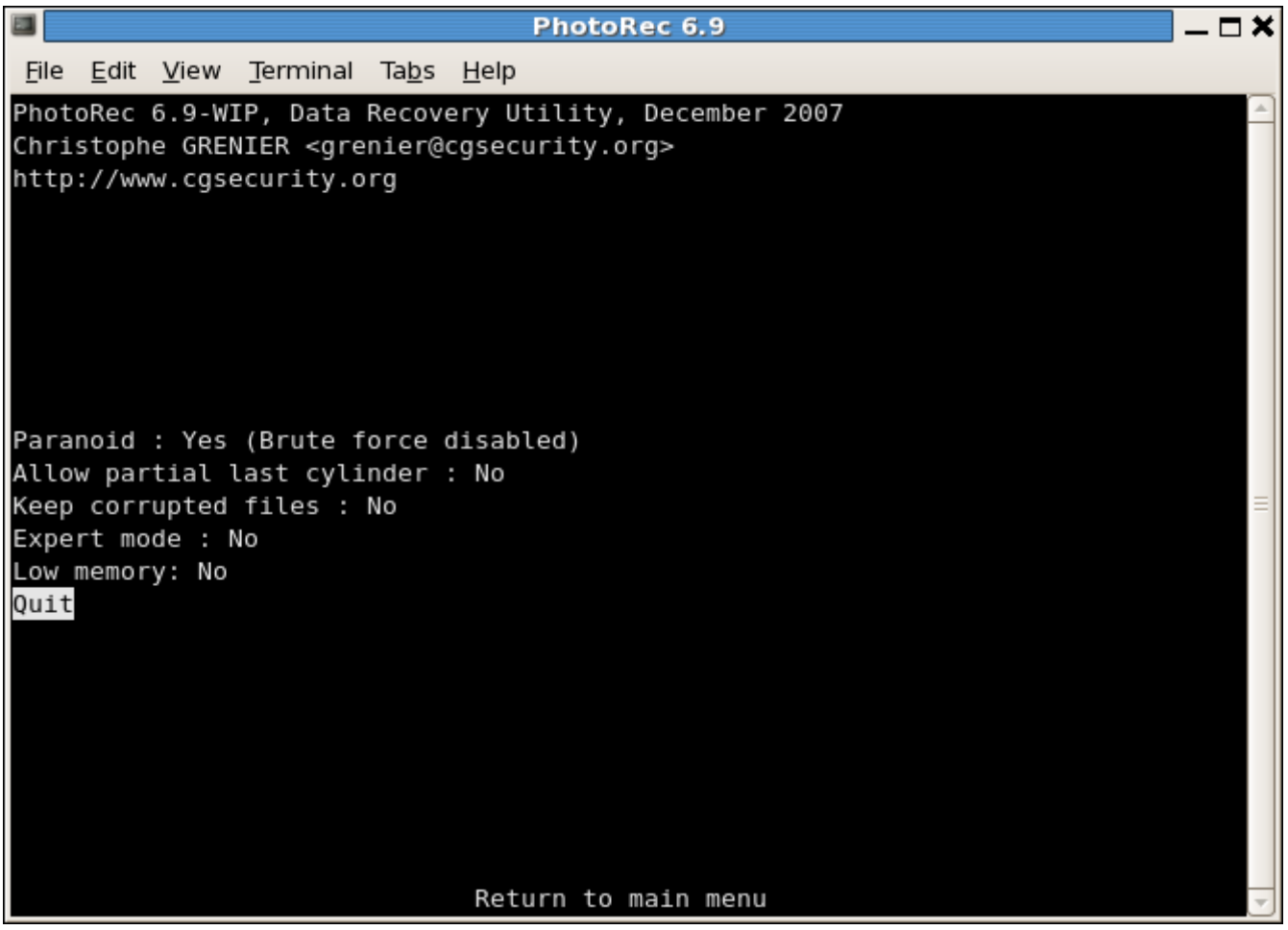
Seleção da partição de origem



Escolha

- `Procurar` depois de selecionar 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



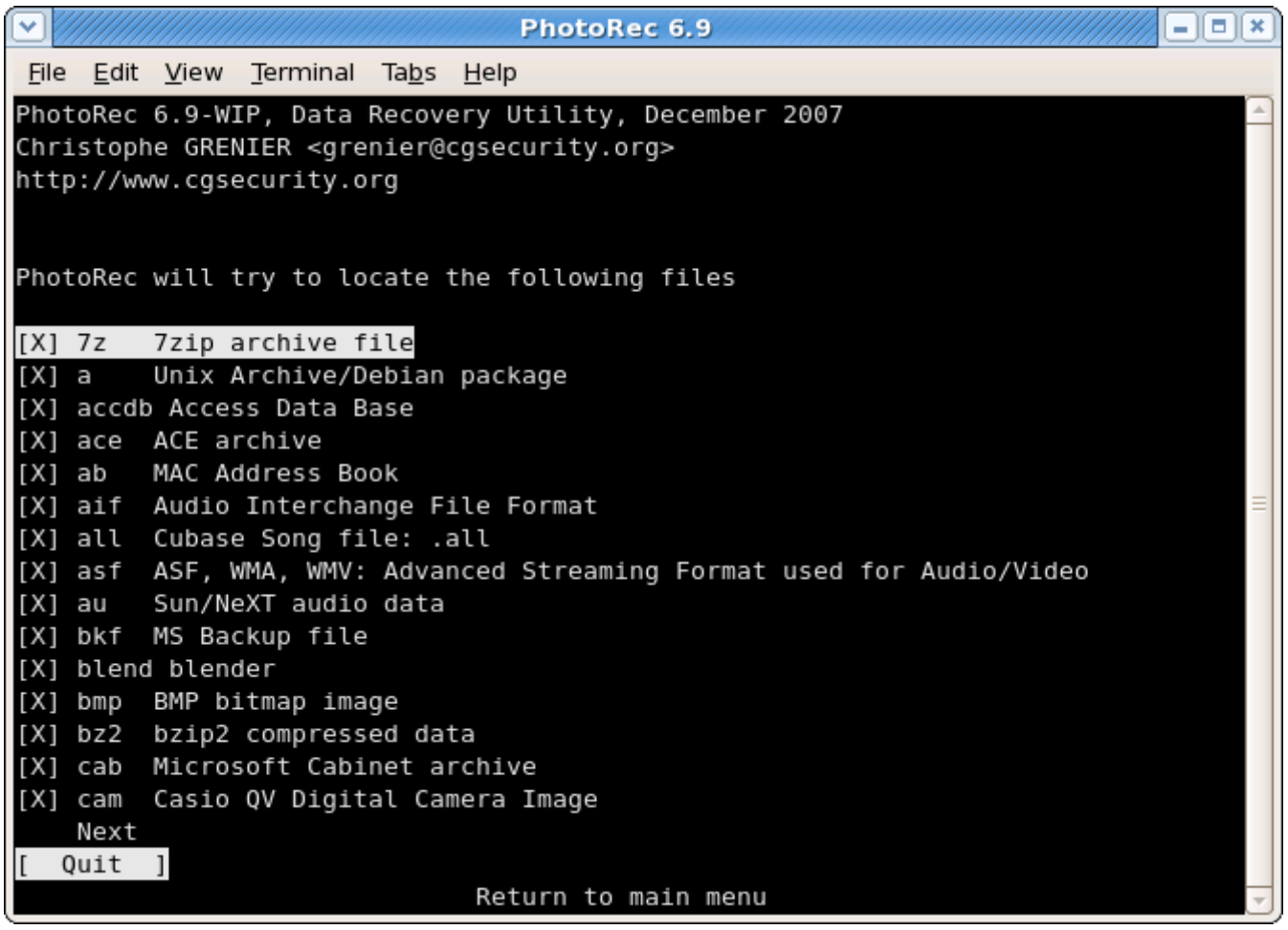
- `Paranória` Por padrão, arquivos recuperados não verificados e arquivos inválidos rejeitados.

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

- `Permitir último cilíndro 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

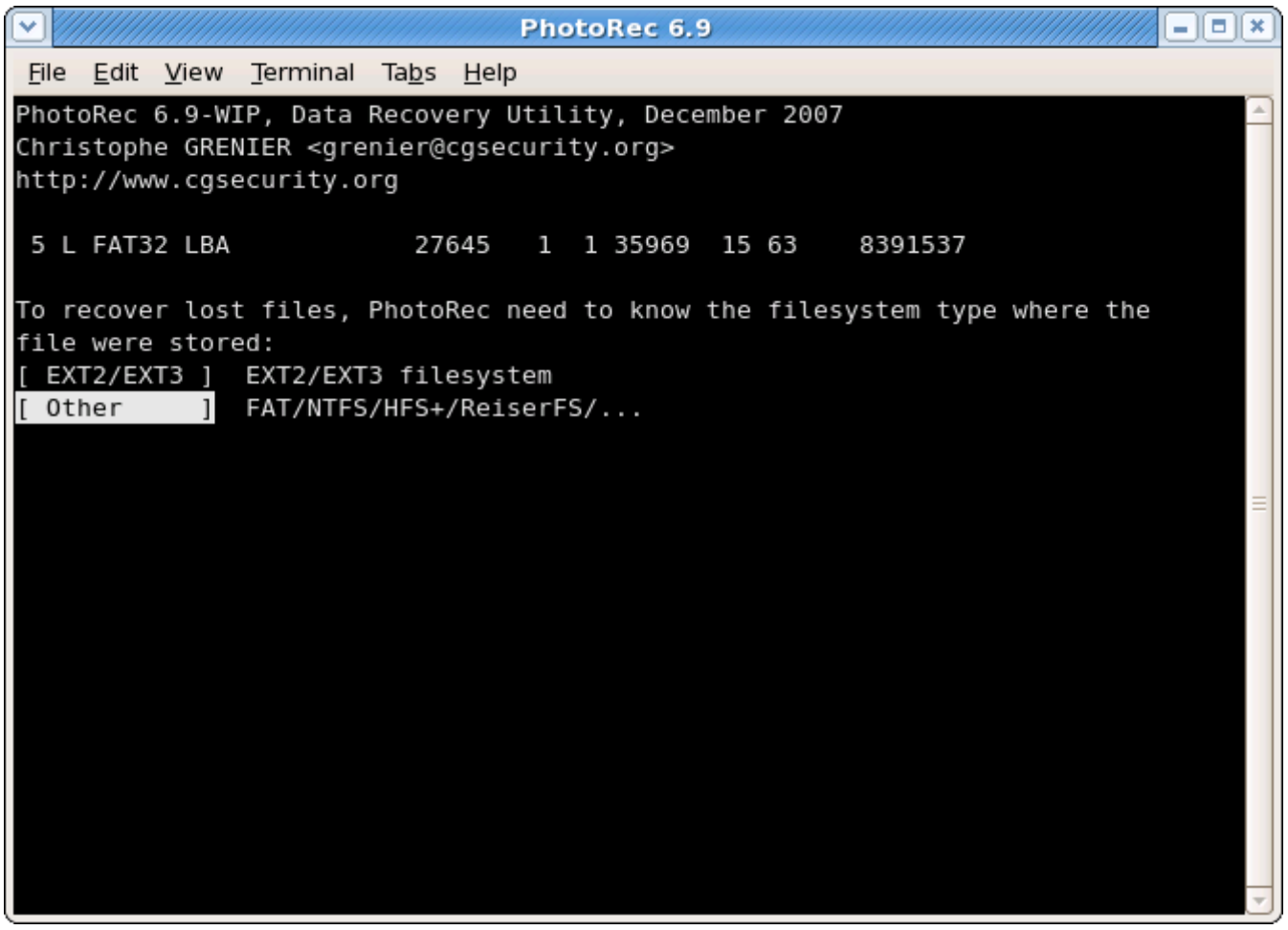


Em `Opções de Arquivo`, habilite ou desbilite a recuperação de certos tipos de arquivos, por exemplo,

```
[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
```

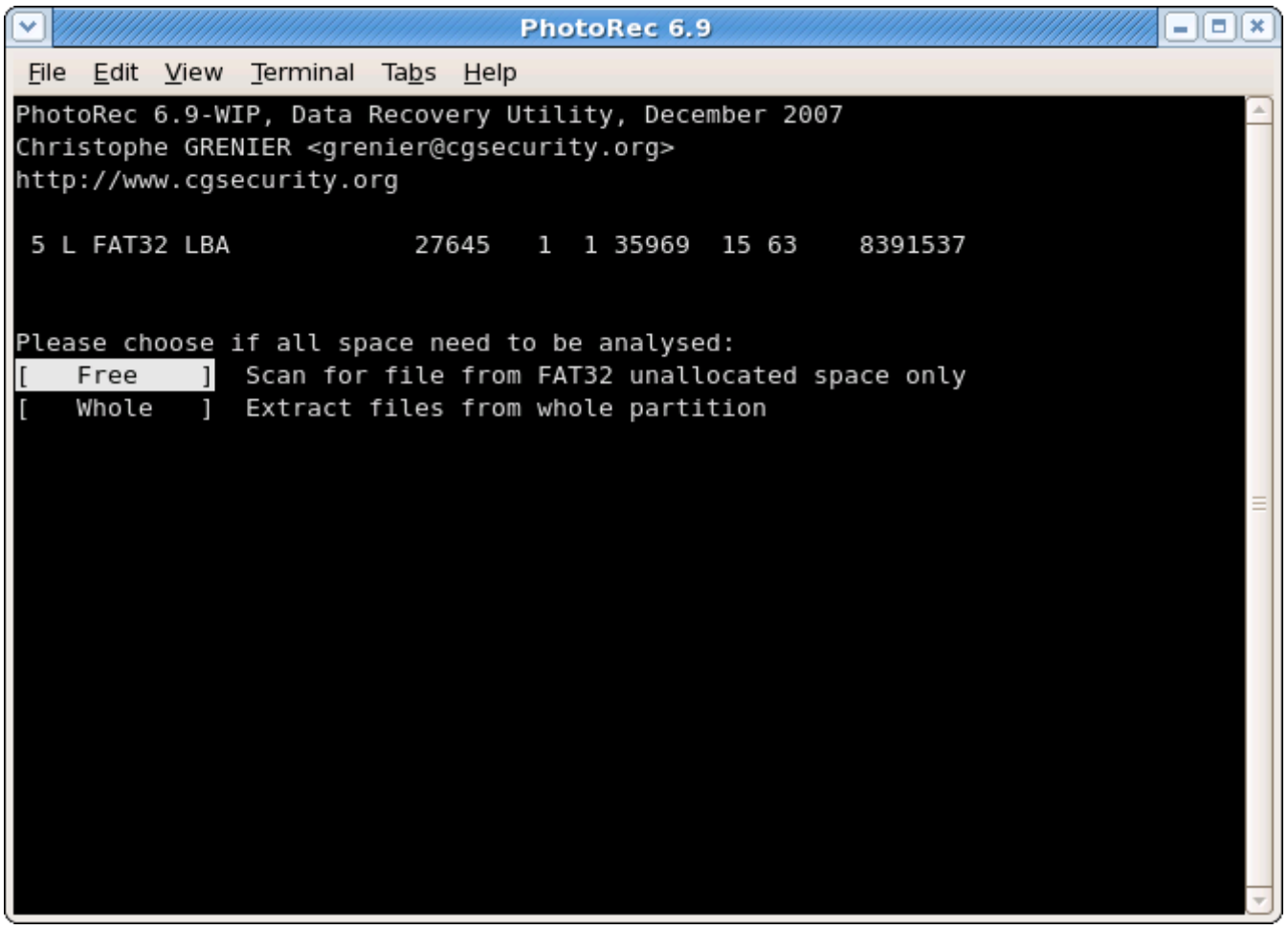
A lista completa de formato de arquivos recuperados pelo PhotoRec contém mais de 320 famílias de arquvios representando mais de 200 extensões de arquivos.

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`.

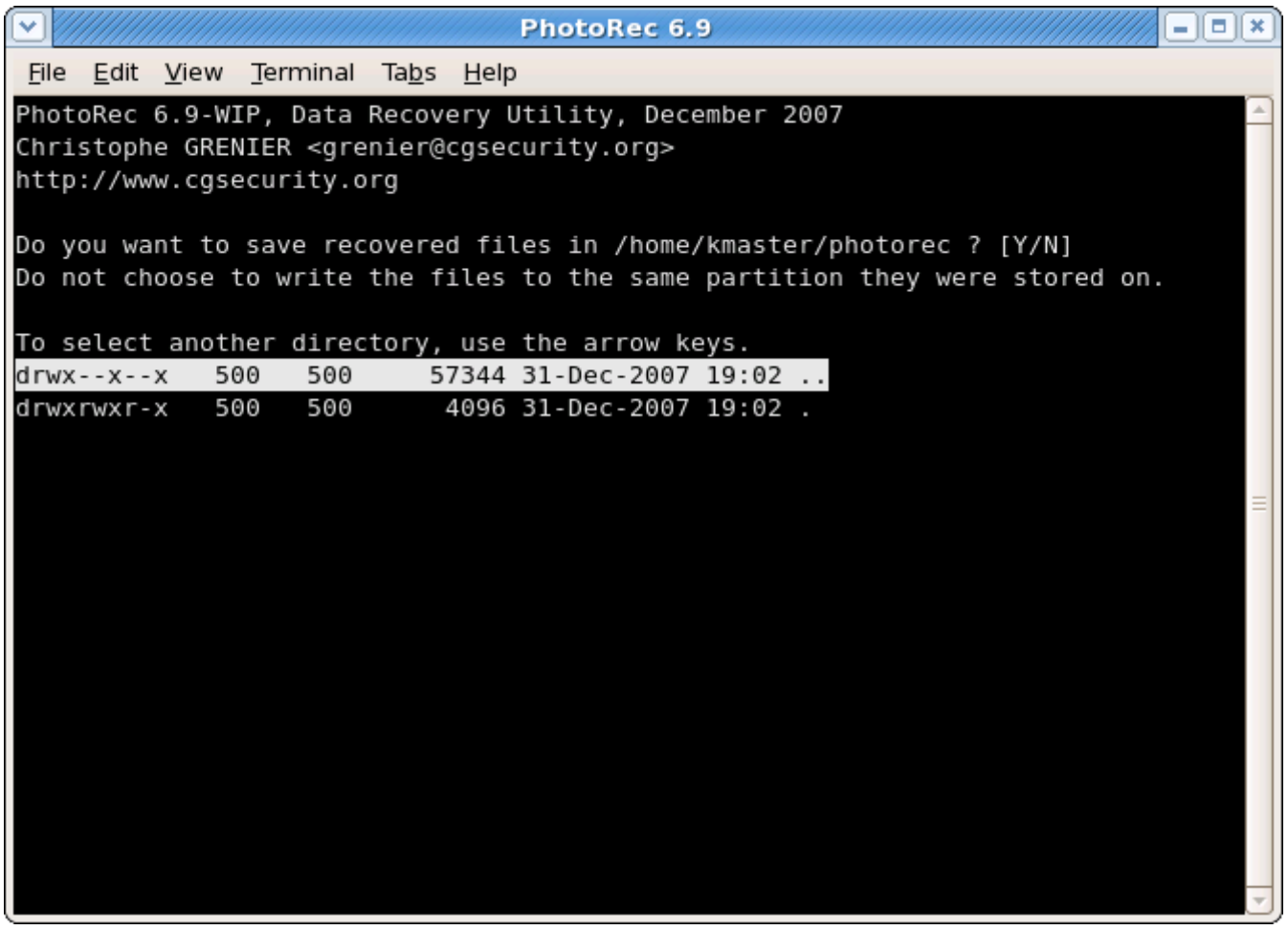
Grave a partição ou só o espaço não alocado



O PhotoRec pode procurar arquivos de:

- de uma partição inteira (últil quando o sitema 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.

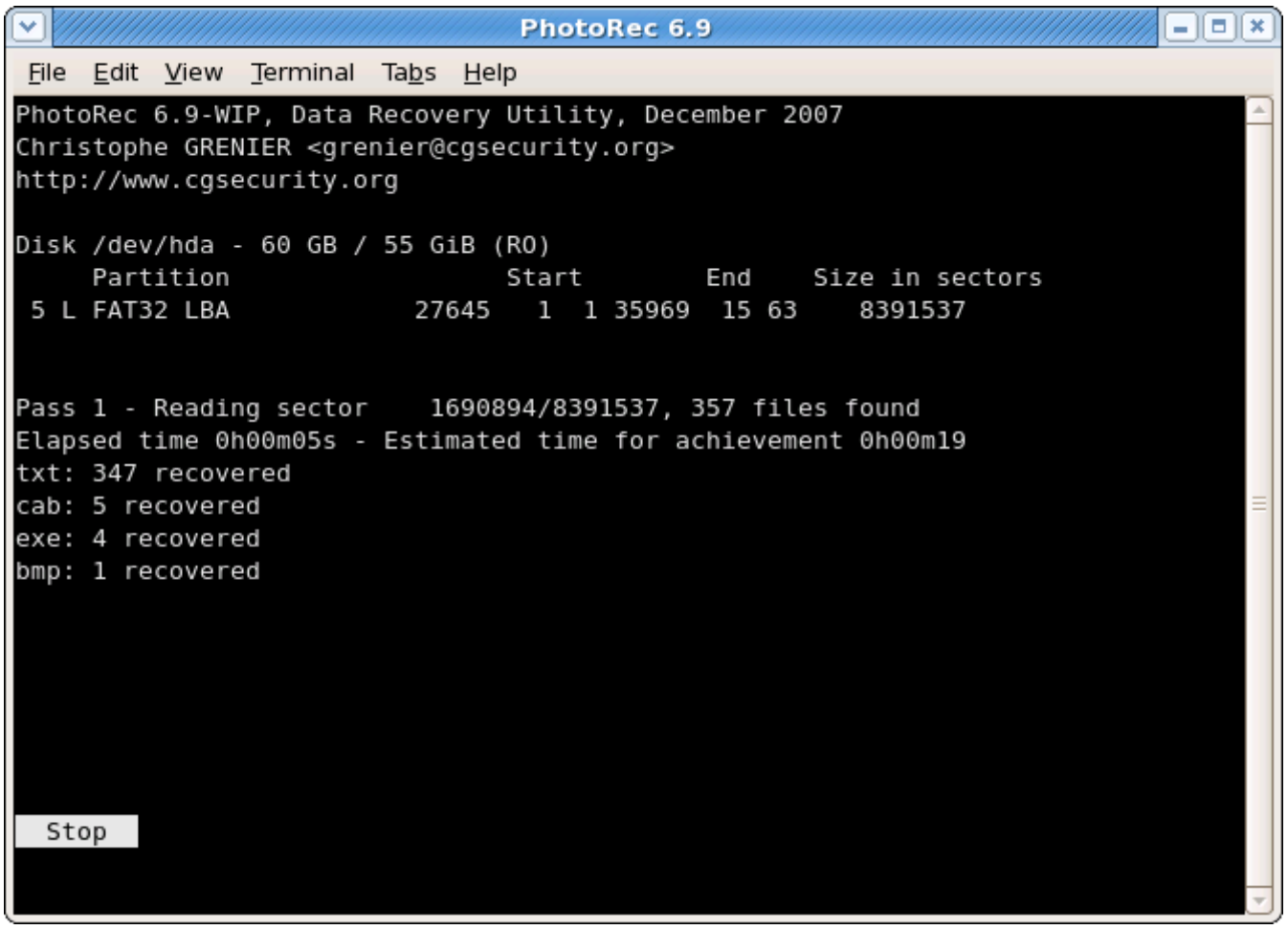
Selecione onde os arquivos recuperados podem ser gravados



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/media`sub-directório.
- As partições de um dico externo são geralmente montadas em `/Volumes`.

Recuperação em progresso

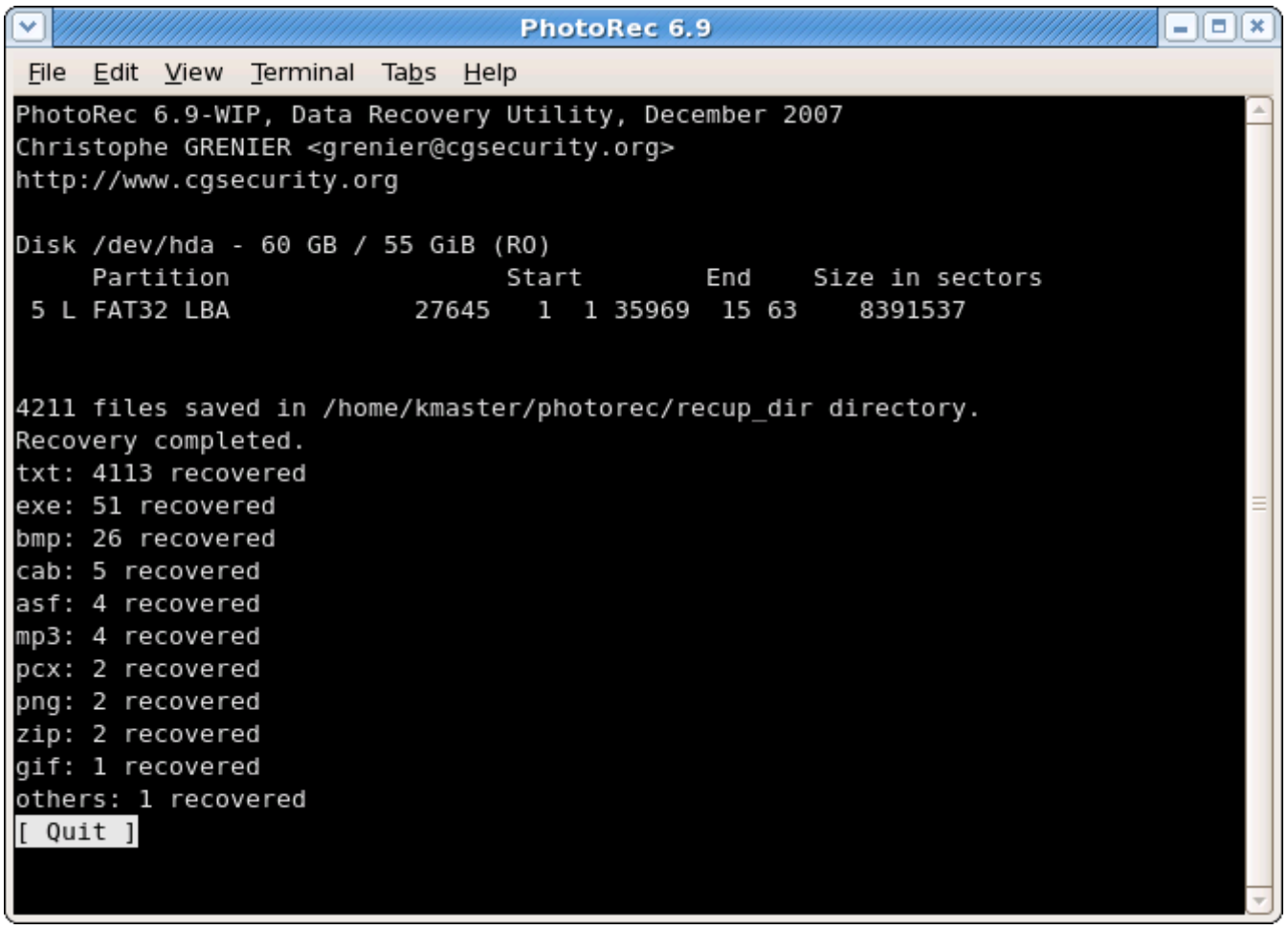


O número de arquivos recuperados é atualizado em tempo real.

- 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



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-virus durante a recuperação para acelerar o processo, mas é recomendado scanear os arquivos recuperados a procura de vírus antes de abrí-los - O PhotoRec pode ter recuperado um documento infectado ou um cavalo de tróia.
