

Tutorial PhotoRec

1. Apresentação

Quem nunca perdeu um arquivo importante ou apagou sem querer ? Eu cai um dia em um problema desses. Um cliente meu perdeu vários arquivos por que o sistema de arquivos do hd se corrompeu . Existem varias soluções comerciais que resolvem o problema, porém não encontrei nenhuma que eu pudesse comprar no brasil, e não tenho cartão de credito internacional. Como eu não iria crackear um programa para funcionar, então procurei uma solução em software livre e gratuita, por sorte achei essa excelente ferramenta o PhotoRec que me surpreendeu sendo melhor em alguns pontos que os softwares comerciais. Lembre-se que soluções como esta não fazem milagres, só vão recuperar dados caso não hajam defeitos físicos nas mídias. Em caso de defeito físico, procure uma empresa especializada no assunto caso os dados sejam imprescindíveis . Caso você não entenda como funciona o esquema de discos e partições no linux aconselho que leia o guia foca linux:

<http://focalinux.cipsga.org.br/guia/intermediario/ch-disc.htm#s-disc-id>

O Photorec funciona nos seguintes sistemas operacionais:

- DOS/Win9x
- Windows NT 4/2000/XP/2003
- Linux
- FreeBSD, NetBSD, OpenBSD
- Sun Solaris
- Mac OS X

Recupera arquivos nos seguintes tipos de dispositivos:

- hd's
- Pendrive
- cdroms
- Memory stick
- Câmeras

Funciona com os seguintes sistemas de arquivo:

- FAT
- NTFS
- EXT2/EXT3
- HFS+

No site oficial consta o Reiserfs como não suportado.

2. Como é possível?

Quando apagamos um arquivo , na verdade não apagamos o arquivo. Primeiramente vamos entender oque é um arquivo. Um arquivo é uma unidade aonde alocamos um tipo de dado. Ele é formado , como todos os dados por uma sequência de 1 e 0, Todo arquivo, tem um nome e um tamanho, um ponto aonde começa e aonde termina na mídia aonde esta armazenado. Cada sistema de arquivos tem um jeito de tratar os arquivos, mas no básico todos trabalham da seguinte forma: Existem uma tabela que contem as informações do arquivo, seu nome e como localiza-lo. Depois de verificar essas

informações o aplicativo pode ler os seus dados. Quando um arquivo é apagado , não é escrito uma sequência de zeros na posição aonde ficam os dados do arquivo, apenas a referência do arquivo é apagado, seu conteúdo fica intacto no momento em que você o apaga, porém sua área fica disponível para que outros arquivos sejam criados, ou que cresçam sobre a área aonde ele ocupava. Ou seja, assim que tiver perdido um arquivo, não faça mais nada com a mídia, pra não correr o risco de escrever em cima da área aonde estão os dados. Use o programa de recuperação logo após perder o arquivo, pois isso vai aumentar consideravelmente a chance de recuperar os arquivos perdidos.








3. Download e instalação

Como conseguir essa ferramenta tão útil para manutenção? Ela pode ser baixada no seguinte site:

http://www.cgsecurity.org/wiki/TestDisk_Download

A ferramenta vem junto da ferramenta TestDisk que é uma ferramenta para recuperação de partições perdidas ou danificadas.

Nas opções de download temos:

-  [Dos/Win9x](#), zip
-  [Windows](#) NT/XP/2000/2003/Vista, zip
-  [Linux](#), tar.bz2 (/tmp must allow execution of program)
-  [Mac OS X](#), tar.bz2
-  Linux [RPM](#)
-  Linux [SRPM](#)
-  Non official version of [PhotoRec for OS2](#)
- [Source](#), tar.bz2.

A minha documentação será feita a partir do arquivo apenas compactado. Não existe pacote oficial para debian na pagina do PhotoRec, porém o pacote é disponibilizado pela distribuição junto ao software Testdisk. Pode ser instalado pelo comando:

```
#apt-get install testdisk
```

Após baixarmos o arquivo, nos temos que descompacta-lo. Então no terminal vá no diretório aonde salvou o arquivo e vamos descompacta-lo:

```
# tar -xjvf testdisk-6.6.linuxstatic.tar.bz2
```

4. Utilização

será criado uma pasta aonde se encontra o programa, vamos entrar nela para executar o photorec:

```
#cd testdisk-6.6
```

Nesta pasta encontram-se alguma documentação e uma pasta linux aonde realmente esta o programa photorec e o programa testdisk.

```
# cd linux
```

Para ter acesso irrestrito aos dispositivos você deve ser usuário root . Devemos lembrar que **nunca você pode recuperar um hd, ou pendrive e apontar para escrever os arquivos recuperados na mesma mídia**. Se você fizer isso, pode gravar em cima dos dados do arquivo que esta tentando recuperar e além de perder definitivamente o arquivo pode corromper o seu sistema de arquivos, perdendo o restante dos seus dados. Para se tornar root você pode usar o comando su:

```
#su
```

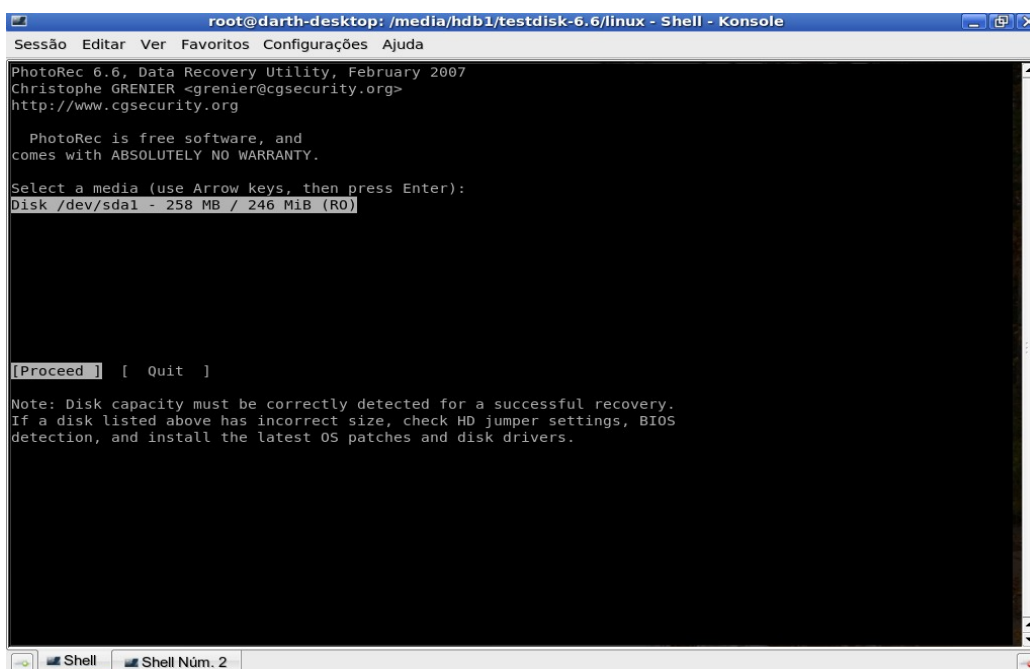
Logo após sera necessário inserir a senha de root. Para sair do modo root, digite “exit”

Para executar o photorec você deve na linha de comando especificar qual dispositivo vai ser recuperado e pasta para onde vai os arquivos recuperados:

```
#!/photorec_static /d /media/hdb1/backup /dev/sda1
```

/d /media/hdb1/backup ---> pasta aonde vai ser salvo os arquivos recuperados.

/dev/sda1 ---> o dispositivo aonde sera feito a recuperação



```
root@darth-desktop: /media/hdb1/testdisk-6.6/linux - Shell - Konsole
Sessão Editar Ver Favoritos Configurações Ajuda
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

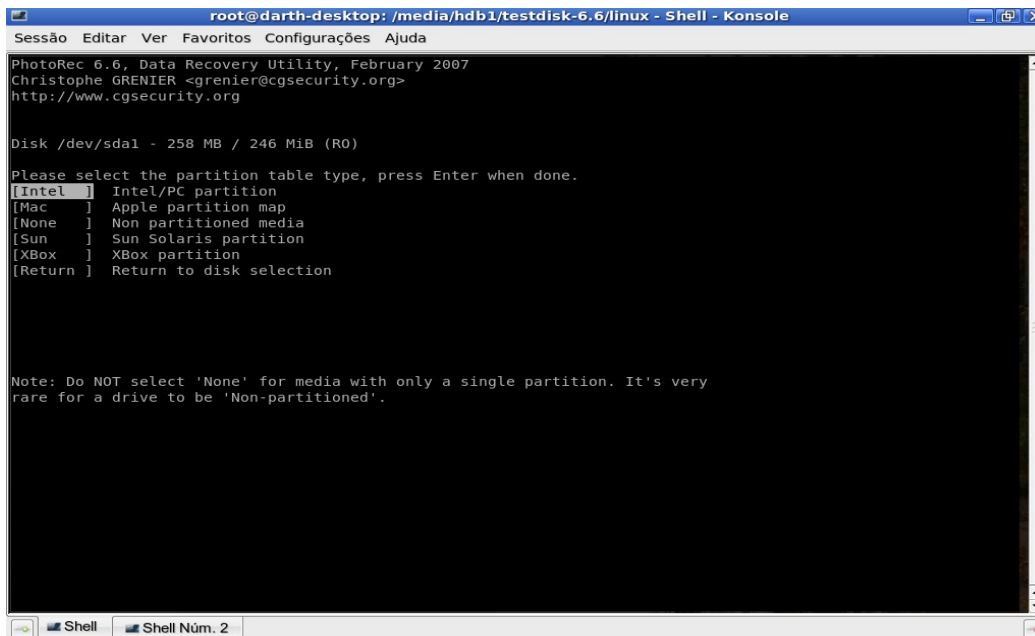
PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda1 - 258 MB / 246 MiB (R0)

[Proceed] [Quit]

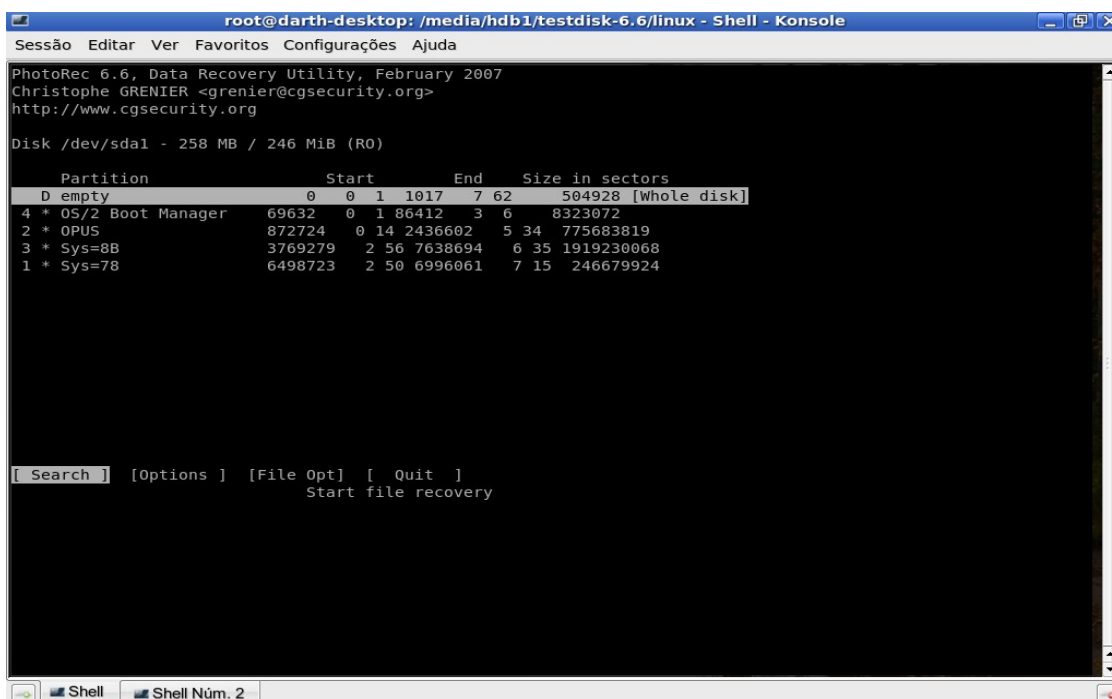
Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

Se você tiver feito tudo corretamente ele vai aparecer esta tela com as informações básicas do hd que você apontou para a recuperação(no caso o meu pendrive 256MB). Você vai ter duas opções, proceed, para prosseguir ou quit para sair do programa. Você pode navegar pelas opções com as setas do teclado. Aperte enter com o proceed destacado.

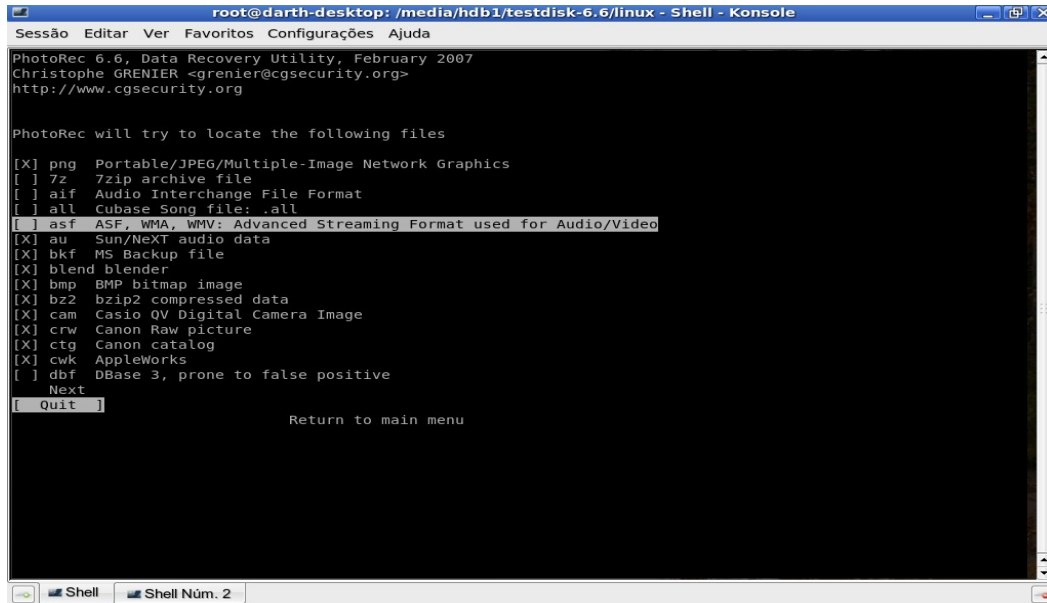


Depois você vai escolher a plataforma de hardware da sua maquina. Um computador pessoal que a maioria das pessoas tem é o Intel ou baseado na arquitetura i386(maquinas com processador Pentium, Athlon, Duron, Sempron,Celeron) da qual se refere a primeira opção. Exceto que você tenha um MAC, ou servidor da SUN ou esteja rodando Linux em um Xbox, use a primeira opção.

Agora vamos para a próxima tela do photorec:



Com as teclas para cima e para baixo você escolhe entre as partições do disco. Que no caso são quatro e a primeira opção é verificar o disco inteiro. As opções embaixo são acessadas com as setas do teclado horizontais (esquerda e direita). A primeira opção já ira fazer o serviço, a opção options tem algumas opções como recuperar arquivos corrompidos, porém as opções default são as mais recomendadas. Na opção “File Opt” você pode escolher quais tipos de arquivo serão recuperados. Ao invés de recuperar todos arquivos, você pode escolher apenas arquivos .doc, por exemplo, arquivos de imagem, etc.



```
root@darth-desktop: /media/hdb1/testdisk-6.6/linux - Shell - Konsole
Sessão Editar Ver Favoritos Configurações Ajuda
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

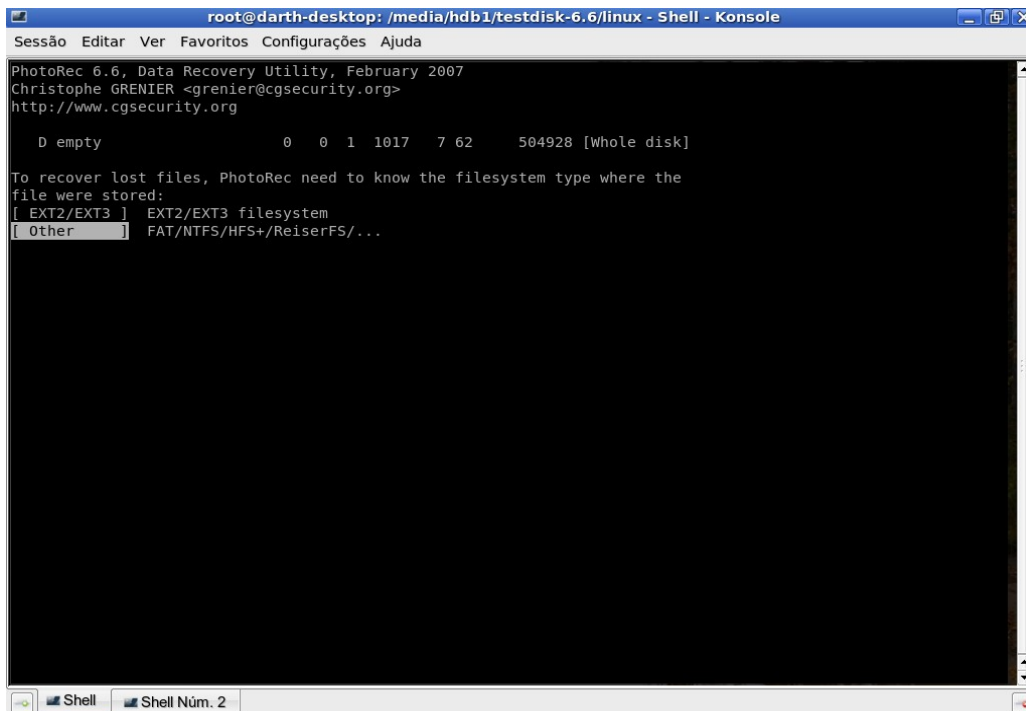
PhotoRec will try to locate the following files

[X] png Portable/JPEG/Multiple-Image Network Graphics
[ ] 7z 7zip archive file
[ ] aif Audio Interchange File Format
[ ] all Cubase Song file: .all
[ ] asf ASF, WMA, WMV: Advanced Streaming Format used for Audio/Video
[X] au Sun/NeXT audio data
[X] bkf MS Backup file
[X] blend blender
[X] bmp BMP bitmap image
[X] bz2 bzip2 compressed data
[X] cam Casio QV Digital Camera Image
[X] crw Canon Raw picture
[X] ctg Canon catalog
[X] cwk AppleWorks
[ ] dbf DBase 3, prone to false positive
[ ] Next
[ Quit ]

Return to main menu
```

Você vai com as teclas para cima e para baixo e barra de espaço para desmarcar uma extensão de arquivo. Depois de enter para voltar a tela anterior. Volte na opção search e pressione enter.

Escolha o tipo de sistema de arquivos, a primeira opção é ext2/ext3 a segunda para os outros sistemas de arquivos. No caso do nosso disco (um pendrive) ele esta em FAT e vamos escolher a segunda opção.



```
root@darth-desktop: /media/hdb1/testdisk-6.6/linux - Shell - Konsole
Sessão Editar Ver Favoritos Configurações Ajuda
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

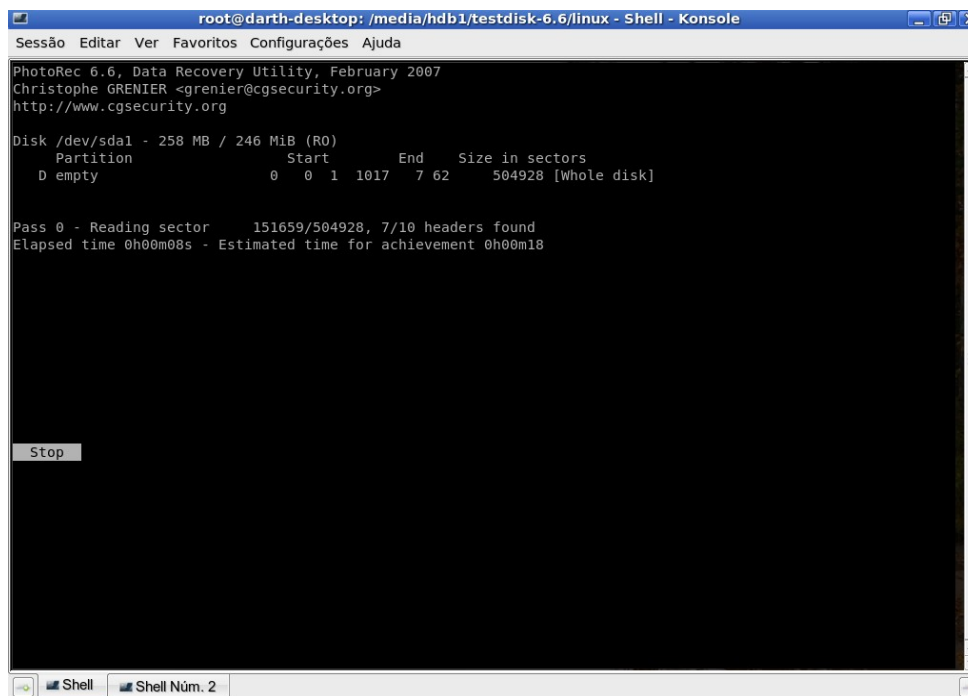
D empty          0  0  1  1017  7  62  504928 [Whole disk]

To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
[ EXT2/EXT3 ] EXT2/EXT3 filesystem
[ Other ] FAT/NTFS/HFS+/ReiserFS/...
```

Caso não saiba qual sistema de arquivos esta na mídia, abra outro terminal, se torne root e de o comando:

fdisk -l /dev/sda (você pode trocar por hda, hdb, de acordo com a mídia), então sera listado as partições e os sistemas de arquivos que eles estão formatados.

Agora é esperar o final do processo



```
root@darth-desktop: /media/hdb1/testdisk-6.6/linux - Shell - Konsole
Sessão Editar Ver Favoritos Configurações Ajuda

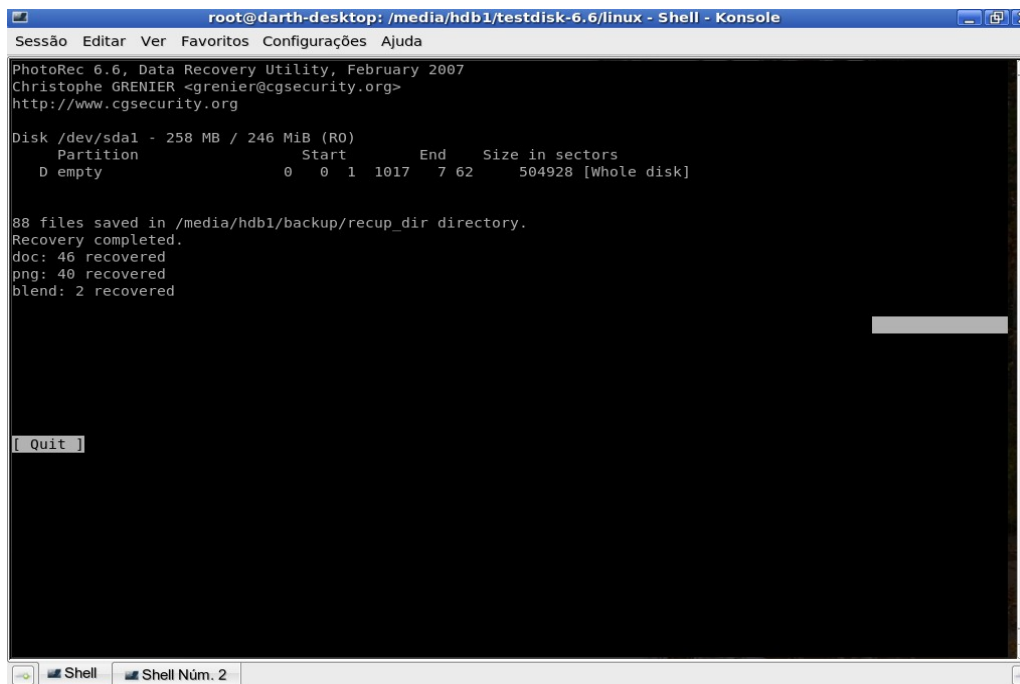
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda1 - 258 MB / 246 MiB (R0)
Partition      Start      End      Size in sectors
D empty        0 0 1 1017 7 62 504928 [Whole disk]

Pass 0 - Reading sector 151659/504928, 7/10 headers found
Elapsed time 0h00m08s - Estimated time for achievement 0h00m18

[ Stop ]
```

No final do processo temos uma estatística dos arquivos recuperados:



```
root@darth-desktop: /media/hdb1/testdisk-6.6/linux - Shell - Konsole
Sessão Editar Ver Favoritos Configurações Ajuda

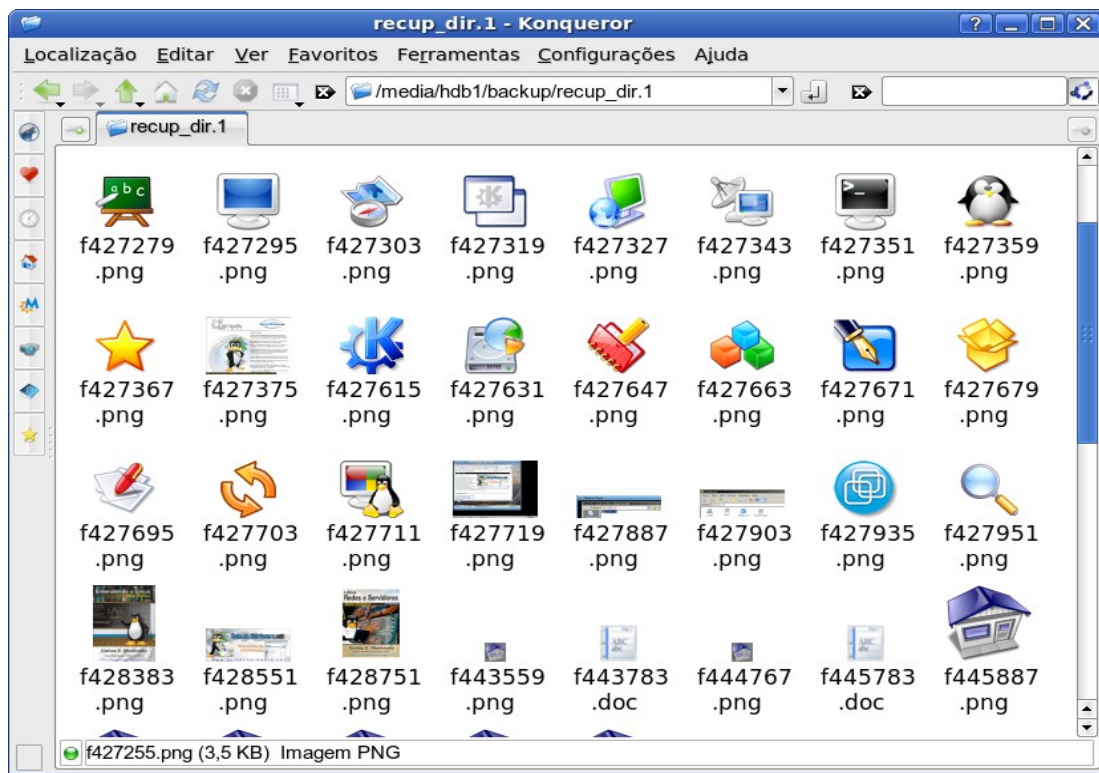
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda1 - 258 MB / 246 MiB (R0)
Partition      Start      End      Size in sectors
D empty        0 0 1 1017 7 62 504928 [Whole disk]

88 files saved in /media/hdb1/backup/recup_dir directory.
Recovery completed.
doc: 46 recovered
png: 40 recovered
blend: 2 recovered

[ Quit ]
```

Como resultado o diretório com os arquivos, verifique que ele não conseguiu recuperar os nomes dos arquivos, mas por outro lado todos abriram com seu conteúdo intacto, repare que ele criou uma pasta recup_dir dentro do diretório backup aonde apontamos que deveria ser recuperados os arquivos:



O PhotoRec vai voltar a tela anterior, vá até a opção quit. Como a recuperação dos arquivos é feita pelo usuário root, os arquivos pertencem a ele. Antes de deixar de ser root você deve mudar o dono para que você não tenha que ser root para acessar os arquivos:

```
#cd /media/hdb1/backup -->entrando no diretório
```

```
#chown -Rf user.user recup_dir.1 --> este comando muda o dono e o grupo do diretório recup_dir.1 para o usuário "user" do qual você deve mudar para seu usuário.
```

5. Conclusão

O programa apesar de não ter conseguido recuperar os nomes dos arquivos, conseguiu recuperar o mais importante, o conteúdo. Ele também tem um numero limitado de tipos de arquivos que ele reconhece, porém pode recuperar a maioria dos arquivos conhecidos, 80 extensões, o que engloba a maioria dos tipos de documento e arquivos multimídia. Resumindo, resolveu o meu problema a custo zero :).

6. Bibliografia :

PhotoRec Wiki

<http://www.cgsecurity.org/wiki/PhotoRec>

Guia Foca Linux

<http://focalinux.cipsga.org.br/guia/intermediario/index.htm>

Sobre o autor

Alexandre da Silva Costa - Técnico em Informática e Profissional em Linux, aluno do curso de Tecnologia da Informação do Centro Universitário de Belo Horizonte - UNI-BH

Sugestões e críticas podem ser enviadas para

anakinpendragon@gmail.com