Récupération de données

SSTIC 2007

Christophe GRENIER - grenier@cgsecurity.org

PhotoRec
Récupération de fichiers

- Logiciel OpenSource (GPL)
- Fonctionne sous
  - DOS,
  - Windows,
  - Linux,
  - FreeBSD, NetBSD, OpenBSD,
  - SunOS
  - MacOS
- Disponible sur http://www.cgsecurity.org

PhotoRec
Récupération de fichiers

- Reconnaît les entêtes des formats de fichiers les plus courants
  - Archives: 7z, bz2, gz, rar, tar, zip
  - Multimedia: asf, au, avi, wav, bmp, cdr, cr2, crw, ctg, dcr, dsc, fla, gif, jng, jpg, mng, mov, mp3, mp4, mpg, mrw, nef, ogg, orf, pcx, pef, png, psd, qxd, qxp, raf, raw, rdc, sit, sr2, tif, x3f, xcf
  - Office: doc, mdb, odd, odp, ods, odt, pap, ppt, rtf, sda, sdc, sdd, sdw, slk, sxc, sxd, sxi, sxw, txt, vis, xls
  - Divers: asp, bat, c, dbf, dbx, eps, exe, frm, h, html, jsp, myi, pdf, php, pl, prc, ps, pst, py, qdf, sh, wab

PhotoRec
Récupération de fichiers

- Capable de récupérer des données, y compris si le système de fichier est irréparable.
- Utilise la notion de bloc de taille fixe
  - FAT
  - NTFS
  - EXT2/EXT3
  - HFS+
- Effectue plusieurs passes pour tenter de récupérer les fichiers fragmentés

PhotoRec
Récupération de fichiers sur CD

- Certains essayent de cacher des données sur des cdroms !
- Récupérons ces fichiers!

Deux images bien innocentes

- [kmaster@christophe cdrecorder]$ ls -al
  total 229
  dr-xr-xr-x 2 root root   2048 May 31 11:12 .
  drwxr-xr-x 3 root root   4096 Jun 4 10:33 ..
  -r--r--r-- 1 root root 102316 May 30 23:28 img-1.jpg
  -r--r--r-- 1 root root 121228 May 30 23:29 img-26.jpg

A priori que deux fichiers

- [kmaster@christophe sstic2007]$ isoinfo -l -i sstic2006.iso
  Directory listing of /
  d--------- 0 0 0 2048 May 31 2007 [28 02] .
  d--------- 0 0 0 2048 May 31 2007 [28 02] ..
  ---------- 0 0 0 102316 May 30 2007 [31 00] IMG_1.JPG;1
  ---------- 0 0 0 121228 May 30 2007 [81 00] IMG_26.JPG;1

  [kmaster@christophe sstic2007]$ isoinfo -J -l -i sstic2006.iso
  Directory listing of /
  d--------- 0 0 0 2048 May 31 2007 [29 02] .
  d--------- 0 0 0 2048 May 31 2007 [29 02] ..
  ---------- 0 0 0 102316 May 30 2007 [31 00] img-1.jpg
  ---------- 0 0 0 121228 May 30 2007 [81 00] img-26.jpg
  [kmaster@christophe sstic2007]$ isoinfo -R -l -i sstic2006.iso
  Directory listing of /
  dr-xr-xr-x 2 0 0 2048 May 31 2007 [28 02] .
  ?--------- 0 0 0 2048 May 31 2007 [28 02] ..
  -r--r--r-- 1 0 0 102316 May 30 2007 [31 00] img-1.jpg
  -r--r--r-- 1 0 0 121228 May 30 2007 [81 00] img-26.jpg

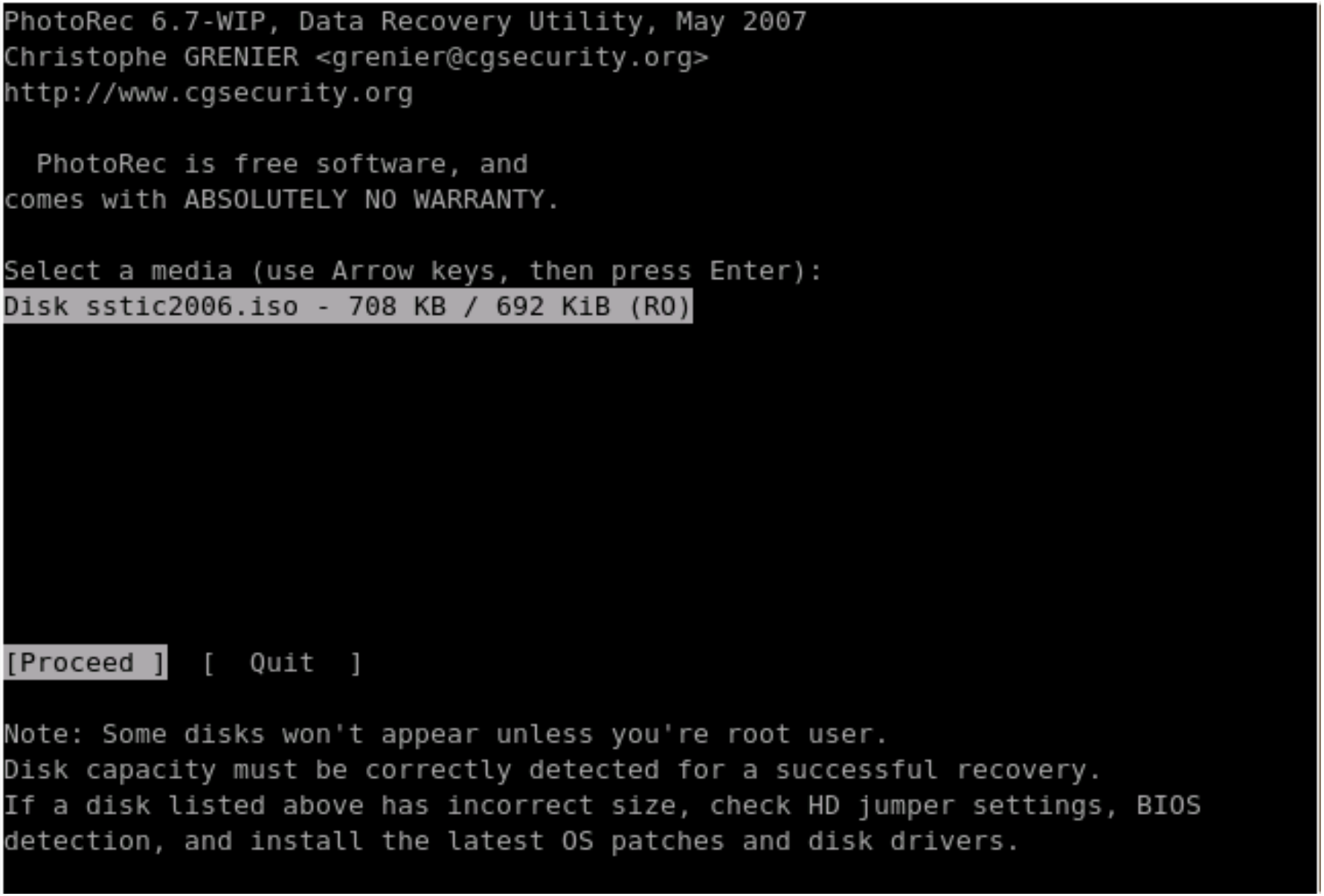
Bon, toujours deux fichiers

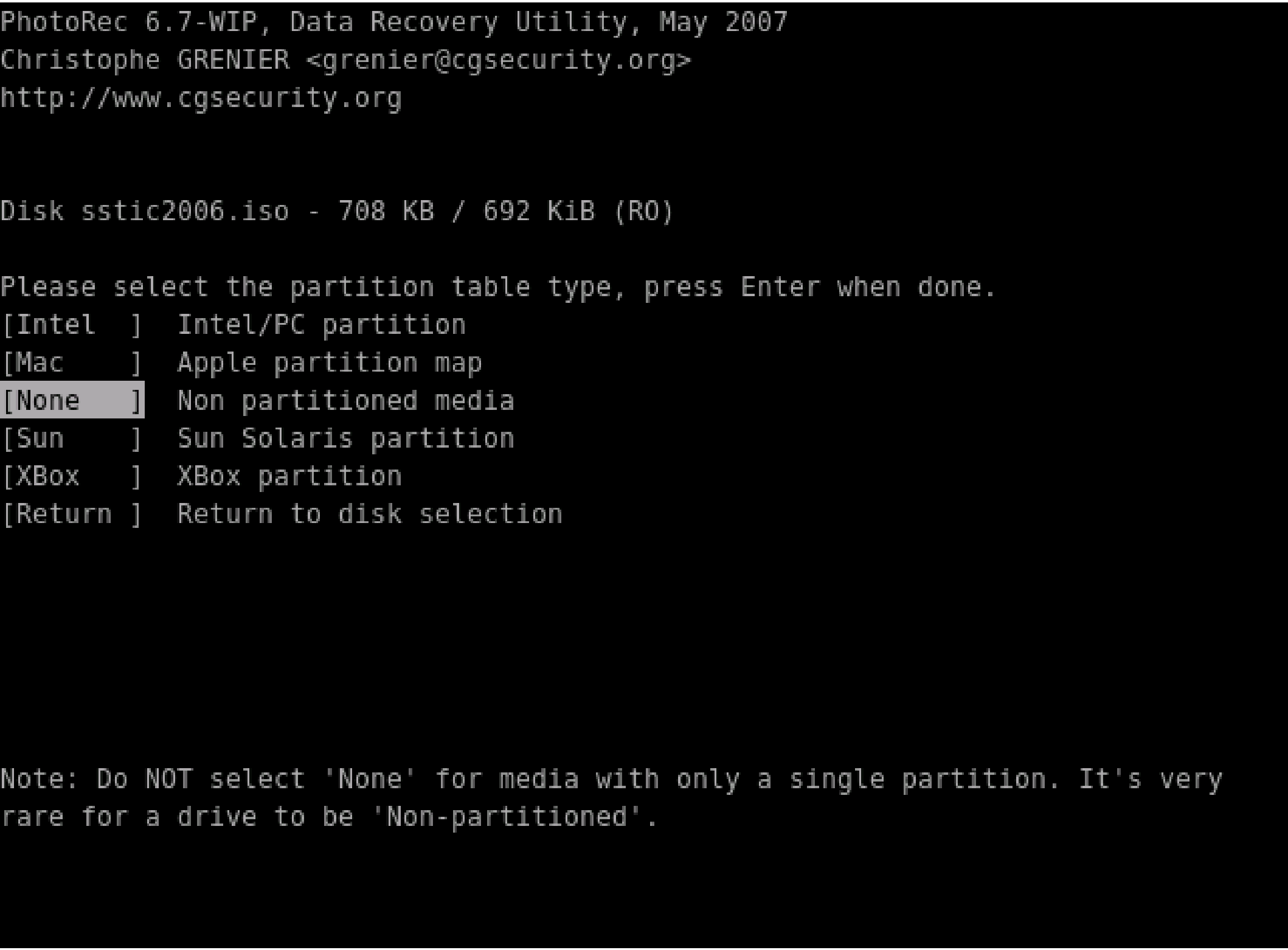
- [kmaster@christophe sstic2007]$ iso-info -l -i sstic2006.iso
  iso-info version 0.77 i686-redhat-linux-gnu
  Copyright (c) 2003, 2004, 2005 R. Bernstein
  This is free software; see the source for copying conditions.
  There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
  PARTICULAR PURPOSE.

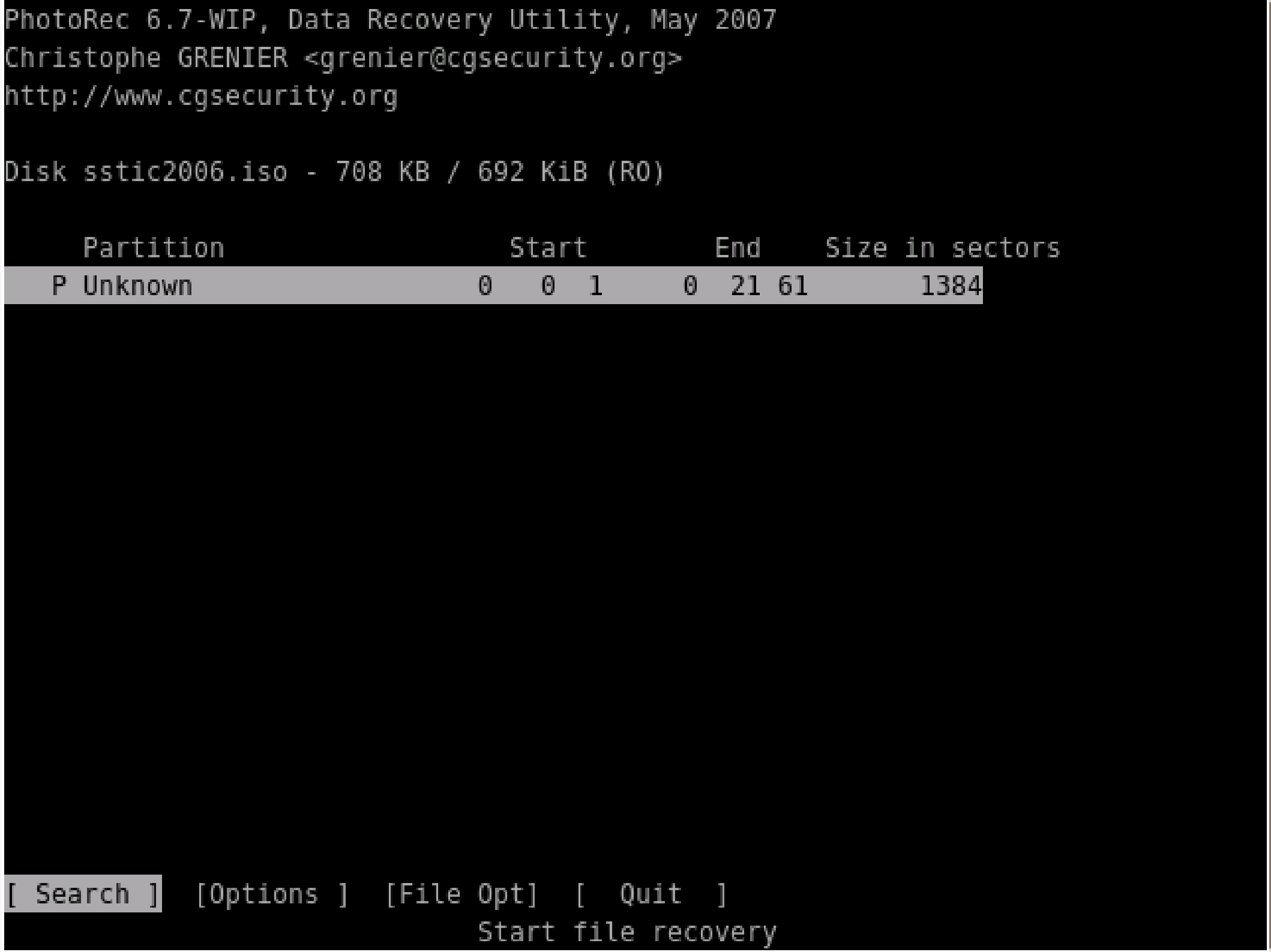
  ISO 9660 image: sstic2006.iso
  Application: K3B THE CD KREATOR (C) 1998-2005 SEBASTIAN TRUEG AND THE K3B TEAM
  System : LINUX
  Volume : SSTIC

  ISO-9660 Information
  /:
  d [LSN 29] 2048 May 31 2007 10:12:27 .
  d [LSN 29] 2048 May 31 2007 10:12:27 ..
  - [LSN 31] 102316 May 30 2007 22:28:48 img-1.jpg
  - [LSN 81] 121228 May 30 2007 22:29:09 img-26.jpg

Et avec PhotoRec ?




PhotoRec 6.7-WIP, Data Recovery Utility, May 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Disk sstic2006.iso - 708 KB / 692 KiB (RO)
Please select the partition table type, press Enter when done.
[Intel] Intel/PC partition
[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'.


PhotoRec 6.7-WIP, Data Recovery Utility, May 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Disk sstic2006.iso - 708 KB / 692 KiB (RO)
Partition Start End Size in sectors
P Unknown 0 0 1 0 21 61 1384
[Search] [Options] [File Opt] [Quit]
Start file recovery

```
PhotoRec 6.7-WIP, Data Recovery Utility, May 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

   P Unknown                  0   0  1     0  21 61       1384

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/...
```

```
PhotoRec 6.7-WIP, Data Recovery Utility, May 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Do you want to save recovered files in /home/kmaster/sstic2007 ? [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.
drwxrwxr-x   500   500      4096 31-May-2007 00:14 prep
drwx--x--x   500   500     57344  4-Jun-2007 18:58 ..
drwxrwxr-x   500   500      4096  4-Jun-2007 19:21 .
```

Bingo: trois fichiers!

```
PhotoRec 6.7-WIP, Data Recovery Utility, May 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk sstic2006.iso - 708 KB / 692 KiB (RO)
     Partition                  Start        End    Size in sectors
   P Unknown                  0   0  1     0  21 61       1384


3 files saved in /home/kmaster/sstic2007/recup_dir directory.
Recovery completed.
jpg: 3 recovered

[ Quit ]
```

Voici la photo dissimulée!