

Récupération de données



S
S
T
I
C

2
0
1
3

Christophe GRENIER - grenier@cgsecurity.org



PhotoRec

Récupération de fichiers

Logiciel OpenSource (GPL)

Fonctionne sous

DOS,

Windows,

Linux,

Mac OS X

FreeBSD, NetBSD, OpenBSD,

SunOS

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/ext4

HFS+

Effectue plusieurs passes pour tenter de récupérer les fichiers fragmentés

File Edit View Terminal Tabs Help

PhotoRec 6.10-WIP, Data Recovery Utility, May 2008
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/sda - 60 GB / 55 GiB (R0) - ATA FUJITSU MHT2060A

Disk /dev/mapper/drivecrypt - 104 MB / 99 MiB (R0)

Disk /dev/dm-0 - 104 MB / 99 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.



File Edit View Terminal Tabs Help

PhotoRec 6.10-WIP, Data Recovery Utility, May 2008

Christophe GRENIER <grenier@cgsecurity.org>

<http://www.cgsecurity.org>

Disk /dev/mapper/drivecrypt - 104 MB / 99 MiB (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'.

File Edit View Terminal Tabs Help

PhotoRec 6.10-WIP, Data Recovery Utility, May 2008

Christophe GRENIER <grenier@cgsecurity.org>

<http://www.cgsecurity.org>

Disk /dev/mapper/drivecrypt - 104 MB / 99 MiB (R0)

Partition	Start	End	Size in sectors
D Unknown	0	203767	203768 [Whole disk]
P ext3	0	203767	203768 [SecureVolume]

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



File Edit View Terminal Tabs Help

PhotoRec 6.10-WIP, Data Recovery Utility, May 2008

Christophe GRENIER <grenier@cgsecurity.org>

<http://www.cgsecurity.org>

P ext3 0 203767 203768 [SecureVolume]

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/...


```
kmaster@christophe:~/perso/testdisk-6.10-WIP/src
File Edit View Terminal Tabs Help
PhotoRec 6.10-WIP, Data Recovery Utility, May 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

P ext3          0      203767      203768 [SecureVolume]

Please choose if all space need to be analysed:
[ Free ] Scan for file from ext2/ext3 unallocated space only
[ Whole ] Extract files from whole partition
```



File Edit View Terminal Tabs Help

PhotoRec 6.10-WIP, Data Recovery Utility, May 2008

Christophe GRENIER <grenier@cgsecurity.org>

<http://www.cgsecurity.org>

Do you want to save recovered files in /home/kmaster/perso/testdisk-6.10-WIP/
/src ? [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	20480	3-Jun-2008	22:52	.
drwxrwxr-x	500	500	4096	3-Jun-2008	16:19	..
drwxr-xr-x	0	0	4096	3-Jun-2008	21:26	recup_dir.1
-rw-rw-r--	500	500	32549	3-Jun-2008	16:19	Makefile
-rw-r--r--	500	500	3341	29-May-2008	09:06	Makefile.am
-rw-r--r--	500	500	39191	31-May-2008	12:21	Makefile.in
-rw-r--r--	500	500	37350	18-May-2008	23:48	adv.c
-rw-r--r--	500	500	1615	12-Sep-2007	16:55	adv.h
-rw-rw-r--	500	500	54708	3-Jun-2008	16:19	adv.o
-rw-r--r--	500	500	3546	9-Apr-2008	20:37	alignio.h
-rw-r--r--	500	500	14983	5-Dec-2007	00:32	analyse.c
-rw-r--r--	500	500	2202	14-Oct-2007	20:57	analyse.h
-rw-rw-r--	500	500	50244	3-Jun-2008	16:19	analyse.o
-rw-r--r--	500	500	3178	14-Oct-2007	11:34	bfs.c
-rw-r--r--	500	500	3288	12-Sep-2007	17:01	bfs.h
-rw-rw-r--	500	500	11652	3-Jun-2008	16:19	bfs.o

Next

File Edit View Terminal Tabs Help

PhotoRec 6.10-WIP, Data Recovery Utility, May 2008

Christophe GRENIER <grenier@cgsecurity.org>

<http://www.cgsecurity.org>

Disk /dev/mapper/drivecrypt - 104 MB / 99 MiB (R0)

Partition	Start	End	Size in sectors
P ext3	0	203767	203768 [SecureVolume]

2 files saved in /home/kmaster/perso/testdisk-6.10-WIP/src/recup_dir directory.

Recovery completed.

gpg: 2 recovered

[Quit]



PhotoRec

Une démo !

<http://www.cgsecurity.org>