

Photorec



Nakon što smo se pozabavili alatima za spašavanje podataka [dd_rescue](#) [1] i [testdisk](#) [2], vrijeme je da se поближе upoznamo i s trećim iz ovog trolista, programom **photorec**. Korisnik nam je donio USB stick s kojeg mu je dijete obrisalo cijeli sadržaj, uglavnom fotografije, da bi snimilo glazbu koju voli slušati. Naš je zadatak pronaći pobrisane fotografije.

U prethodnim smo ga primjerima koristili neinteraktivno, zadavši na komandnoj liniji sve potrebne parametre. Ovog ćemo ga puta koristiti malo drugačije:

```
# photorec
```

Kao što pokazuje prva ilustracija, photorec će nam ponuditi listu dostupnih medija s podacima. Tu su tvrdi disk i USB stick s kojeg nastojimo spasiti podatke, pa ćemo odabrati njega.

```
PhotoRec 6.13, Data Recovery Utility, November 2011
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 - 160 GB / 149 GiB (RO) - INTEL SSDSA1M160G2HP
>Disk /dev/sdb - 511 MB / 487 MiB (RO) - USBDisk RunDisk

>[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.
```

Photorec je na USB-u pronašao ispravnu FAT particiju.

```

PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 511 MB / 487 MiB (RO) - USBDisk RunDisk

    Partition              Start          End      Size in sectors
    No partition          0  0  1  1023  5  47      998800 [Whole disk]
> 1 P FAT16 >32M         0  0  33  1023  0  48      998464 [NO NAME]

[ Search ] [Options ] >[File Opt] [ Quit ]
                          Modify file options
    
```

No prije nego pokrenemo traženje datoteka, izaberimo ponudu **File options**. Pojavit će se dugačak popis vrsta datoteka koje je *photorec* u stanju prepoznati i rekonstruirati.

```

PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec will try to locate the following files

>[X] Own custom signatures
[X] 1cd Russian Finance 1C:Enterprise 8
[X] 7z 7zip archive file
[X] DB
[X] a Unix Archive/Debian package
[X] abcdp Apple binary property list
[X] accdb Access Data Base
[X] ace ACE archive
[X] ab MAC Address Book
[X] ahn Ahnenblatt
[X] aif Audio Interchange File Format
[X] all Cubase Song file: .all
[X] als Ableton Live Sets
[X] amd AlphaCAM (amd/amt/atd/att)
    Next
Press s to disable all file families, b to save the settings
>[ Quit ]

                          Return to main menu
    
```

Spuštajte se kursorom prema dolje, pa ćete ustanoviti da je tu navedeno pravo bogatstvo različitih vrsta datoteka i datotečnih sustava. Ako znate što tražite i ako želite ubrzati pretragu, možete neke od njih isključiti. No za tim nema stvarne potrebe, jer će *photorec* brzo obaviti svoj posao na ne tako velikom USB sticku.

Pod **Options** će nam ponuditi neke naprednije mogućnosti koje u većini slučajeva možemo zanemariti.

```
PhotoRec 6.13, Data Recovery Utility, November 2011
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
```

Vratimo se na ekran s odabranom particijom i odaberimo **Search**. *Photorec* će nas najprije, za svaki slučaj, pitati za vrstu datotečnog sustava, iako je već prepoznao da se radi FAT16 particiji.

```
PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
1 P FAT16 >32M          0  0 33 1023  0 48      998464 [NO NAME]
```

```
To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
```

```
[ ext2/ext3 ] ext2/ext3/ext4 filesystem
> [ Other   ] FAT/NTFS/HFS+/ReiserFS/...
```

Potvrdimo da se radi o Microsoftovom datotečnom sustavu. Nakon toga pita da li želimo pretražiti cijeli prostor diska, ili samo nealociran prostor, a upravo se tu nalaze obrisane dateke. To ćete odabrati ako vas zanimaju samo obrisane datoteke. U protivnom, odaberite sigurniju mogućnost, a to je pretraživanje cijelog diska.

```
PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

 1 P FAT16 >32M          0  0 33 1023  0 48      998464 [NO NAME]

Please choose if all space need to be analysed:
>[  Free  ] Scan for files from FAT16 unallocated space only
 [  Whole ] Extract files from whole partition
```

Zatim nas pita kamo želimo smjestiti spašene datoteke, nakon čega konačno počinje pravi posao. *Photorec* će nas cijelo vrijeme dok radi obavještavati o broju rekonstruiranih datoteka.

```
PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 511 MB / 487 MiB (RO) - USBDisk RunDisk
  Partition          Start      End      Size in sectors
 1 P FAT16 >32M      0  0 33 1023  0 48      998464 [NO NAME]

Pass 1 - Reading sector      513456/998464, 107 files found
Elapsed time 0h00m26s - Estimated time to completion 0h00m24
jpg: 98 recovered
doc: 4 recovered
txt: 2 recovered
exe: 1 recovered
mpg: 1 recovered
riff: 1 recovered
```

Stop

Kada završi, dobit ćemo sumarni izvještaj.

```
PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 511 MB / 487 MiB (RO) - USBDisk RunDisk
  Partition          Start      End      Size in sectors
  1 P FAT16 >32M      0  0 33 1023  0 48      998464 [NO NAME]

111 files saved in /home/hombre/recup_dir directory.
Recovery completed.

You are welcome to donate to support further development and encouragement
http://www.cgsecurity.org/wiki/Donation

[ Quit ]
```

Spašeno je 111 datoteka, uglavnom slike u jpeg formatu i poneki dokument. Sve je to uredno smješteno u direktoriju recup_dir. Pri tome je sva glazba snimljena na stick i dalje dostupna! Photorec je sadržaj sticka ostavio nedirnutim, samo je pronašao obrisani sadržaj.

I eto prilike da sistemac bar na trenutak bude omiljen na svojoj ustanovi!

Povezani članci:

[Spašavanje podataka s oštećenih medija](#) [1]

[Testdisk](#) [2]

[Računalna forenzika](#) [3]

[Spašavanje USB sticka](#) [4]

uto, 2013-01-01 21:01 - Aco Dmitrović **Kuharice:** [Linux](#) [5]

Kategorije: [Sigurnost](#) [6]

Vote: 4.142855

Vaša ocjena: Nema Average: 4.1 (7 votes)

Source URL: <https://sysportal.carnet.hr/node/1175>

Links

- [1] <https://sysportal.carnet.hr/node/1169>
- [2] <https://sysportal.carnet.hr/node/1171>
- [3] <https://sysportal.carnet.hr/node/1177>
- [4] <https://sysportal.carnet.hr/node/1179>
- [5] <https://sysportal.carnet.hr/taxonomy/term/17>
- [6] <https://sysportal.carnet.hr/taxonomy/term/30>