Photorec

Nakon što smo se pozabavili alatima za spašavnje podataka ***dd_rescue*** [1] i ***testdisk*** [2], vrijeme je da se pobliže 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.

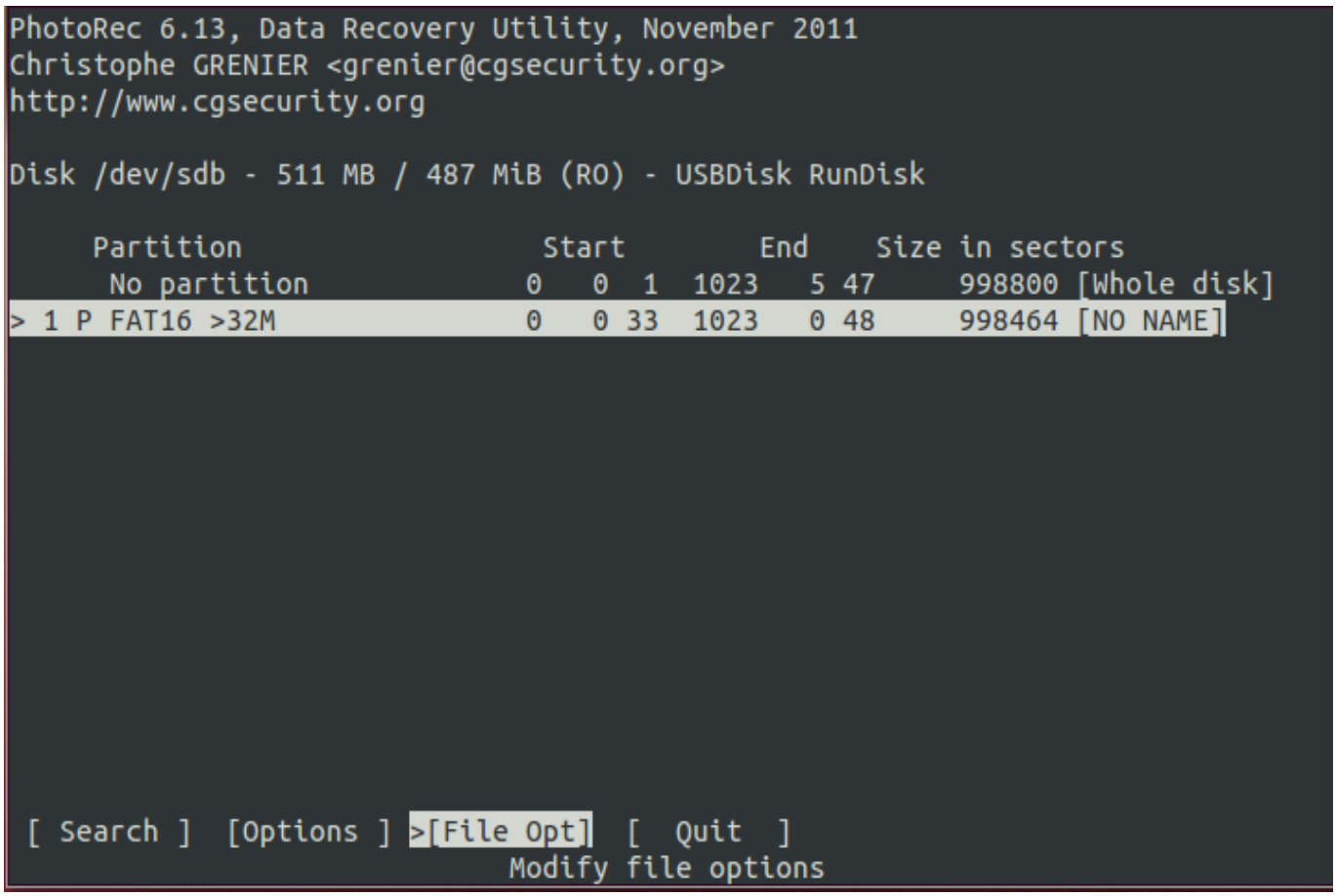
U prethodnim smo ga primjerima koristili neinteraktivno, zadavši na komandnoj liniji sve potrebne parametre. Ovog ćemo ga puta koristiti malo drugačije:

```
# photorec
```

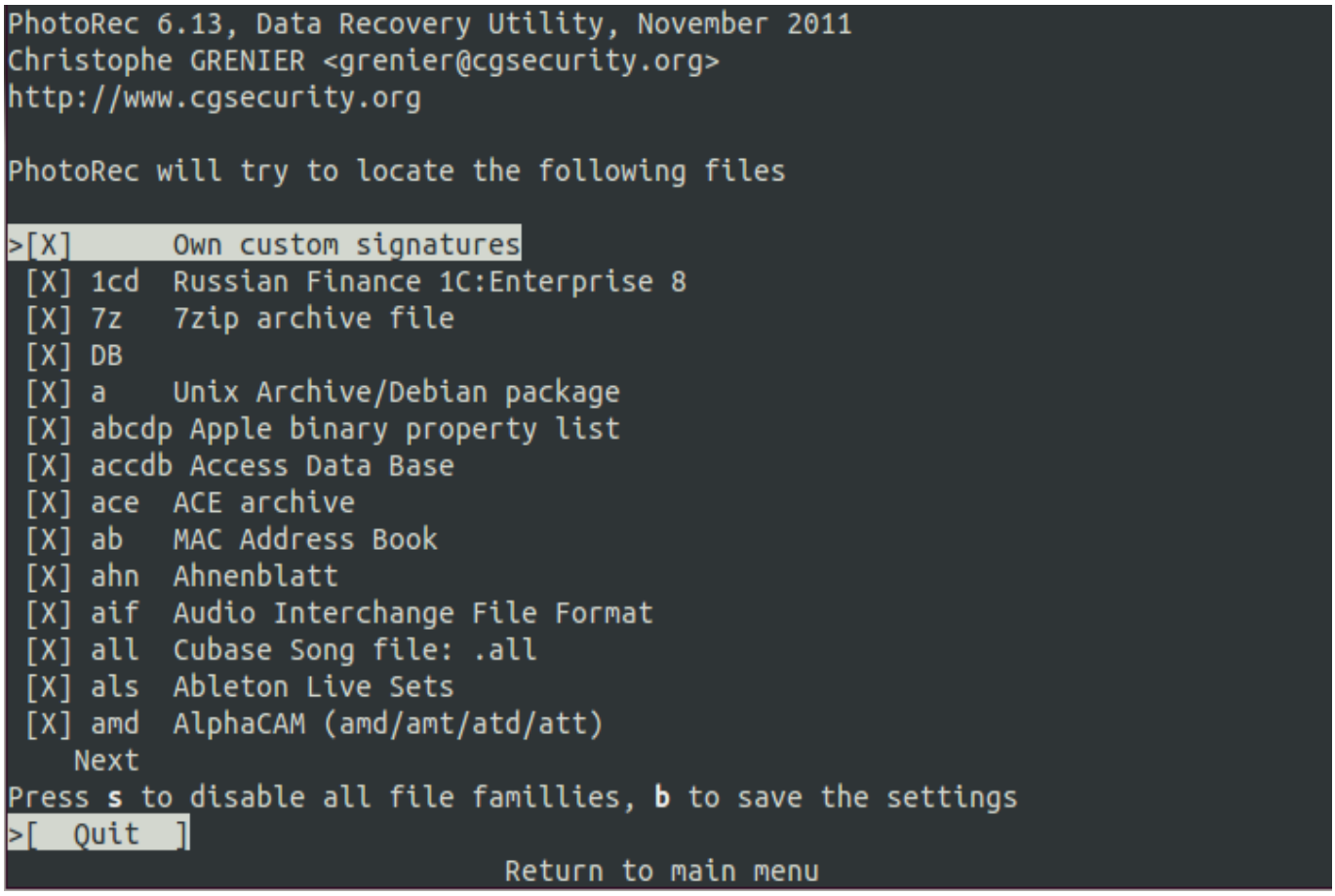
Kao što pokazuje prva ilustracija, photorec će nam ponuditi listu dostupnih medija s podacima. Tu su tvrdi disk i USB stick s kojeg nastojimo spasiti podatke, pa ćemo odabrati njega.

```
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.

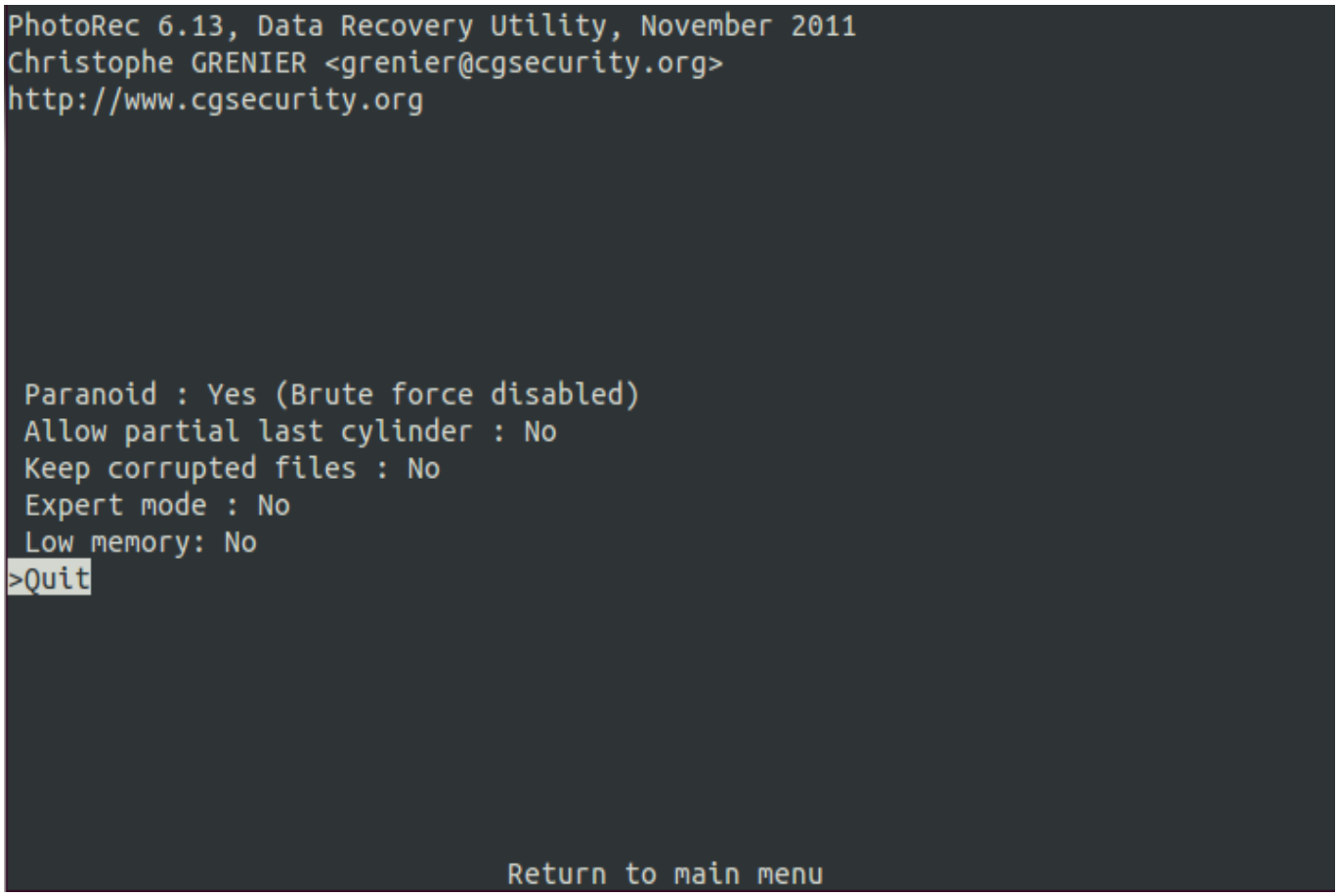


No prije nego pokrenemo traženje datoteka, izaberimo ponudu ***File options***. Pojavit će se dugačak popis vrsta datoteka koje je *photorec* u stanju prepoznati i rekonstruirati.

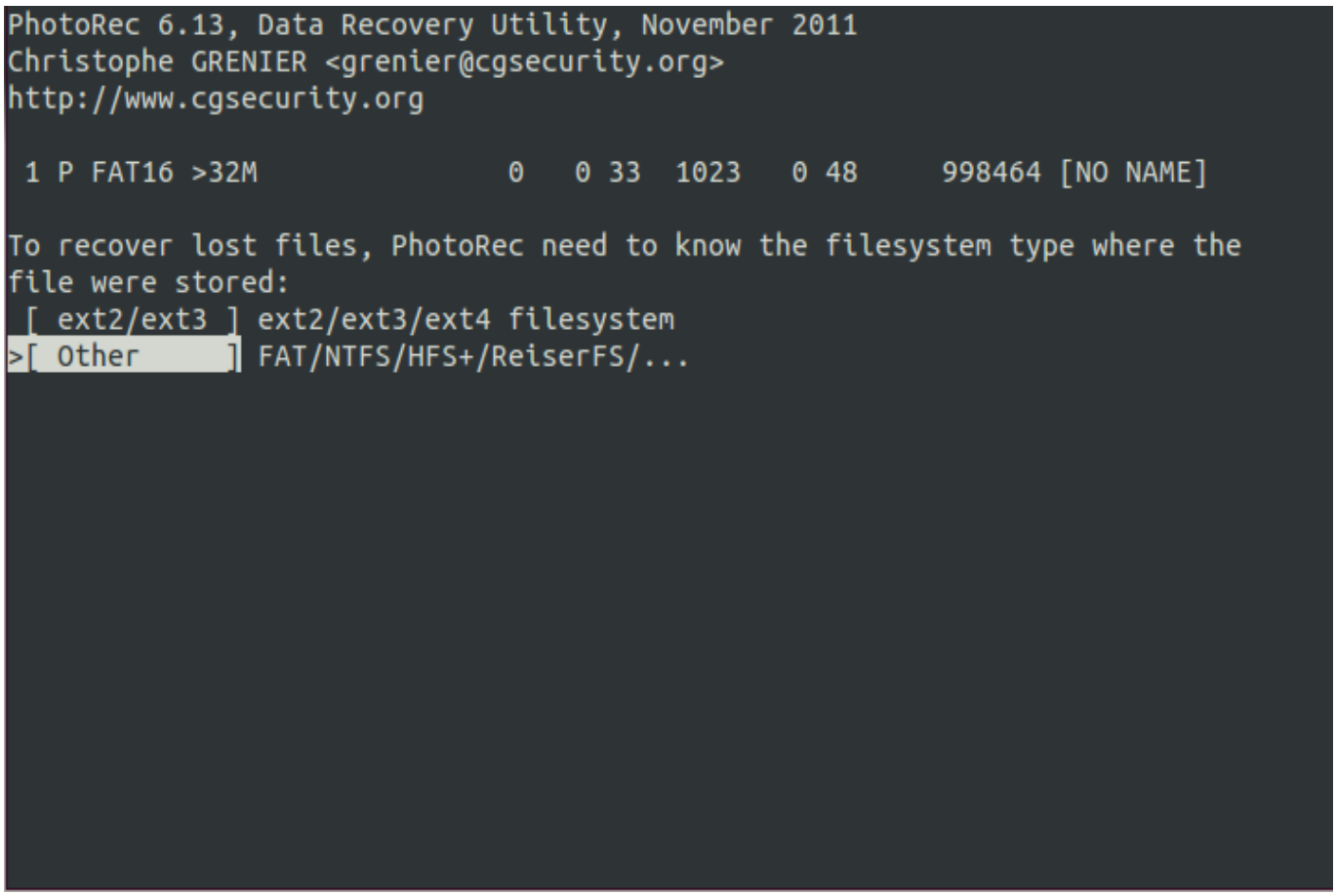


Spuštajte se kursorom prema dolje, pa ćete ustanoviti da je tu navedeno pravo bogatstvo različitih vrsta datoteka i datotečnih sustava. Ako znate što tražite i ako želite ubrzati pretragu, možete neke od njih isključiti. No za tim nema stvarne potrebe, jer će *photorec* brzo obaviti svoj posao na ne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

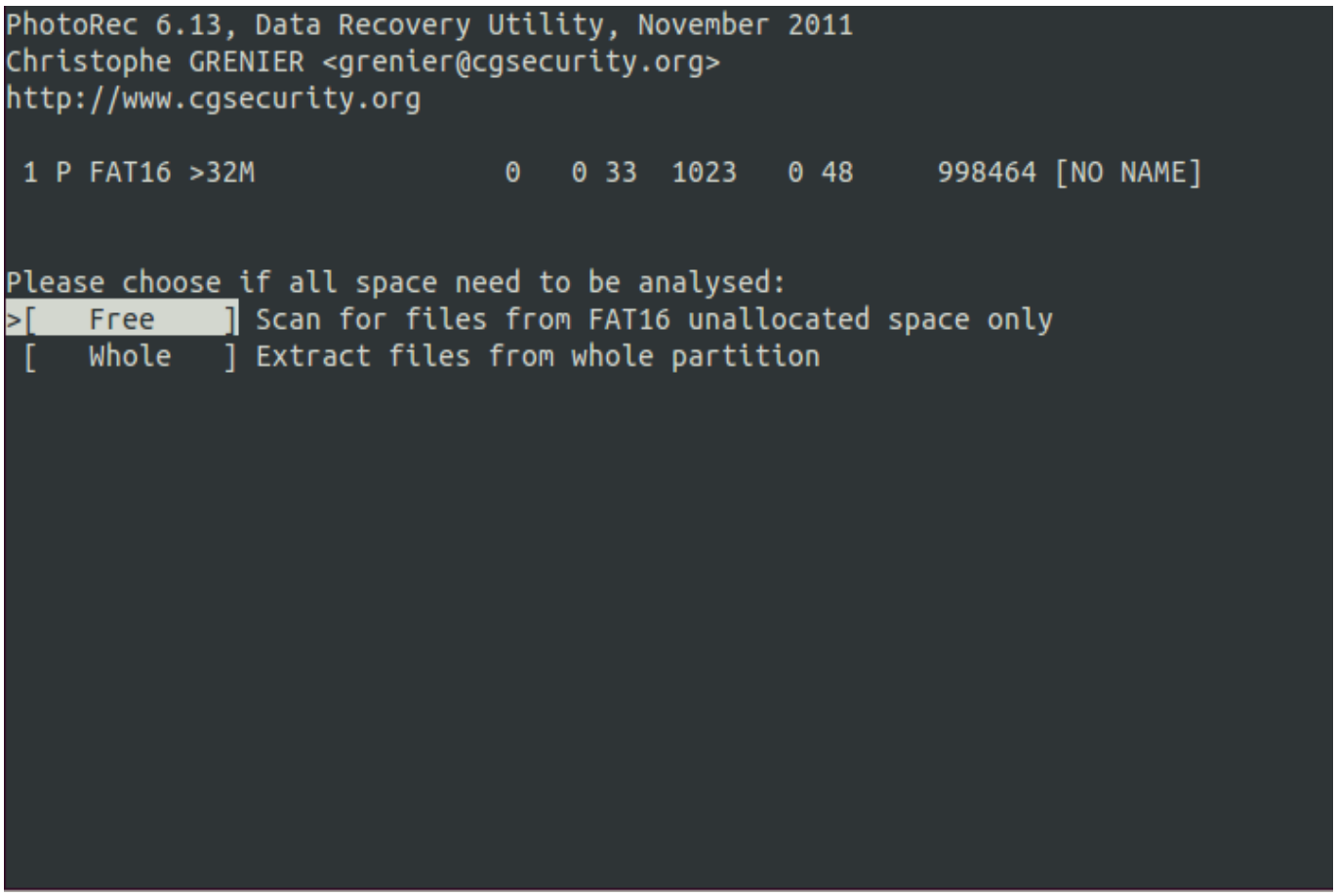
Pod ***Options*** će nam ponuditi neke naprednije mogućnosti koje u većini slučajeva možemo zanemariti.



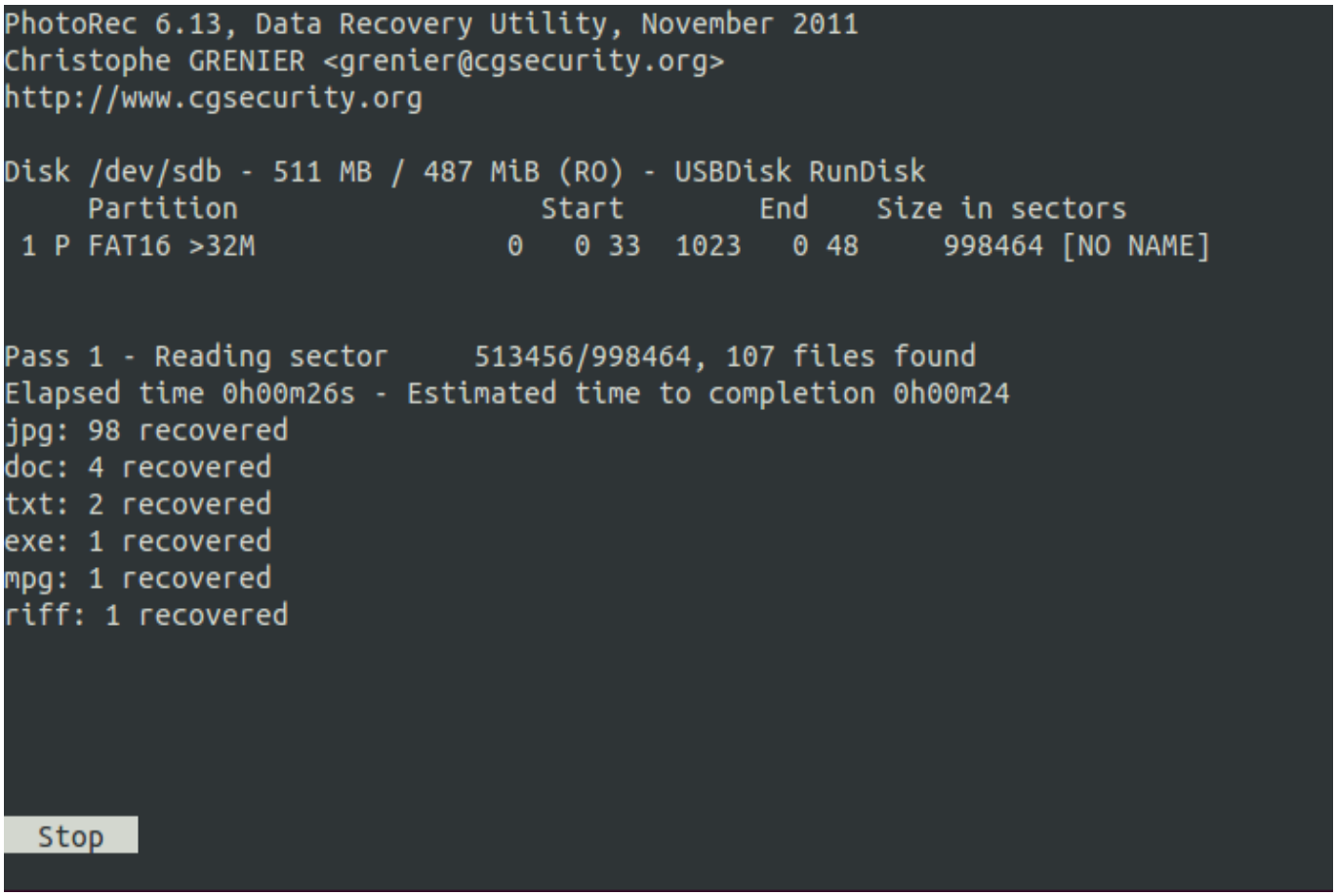
Vratimo se na ekran s odabranom particijom i odaberimo ***Search***. *Photorec* će nas najprije, za svaki slučaj, pitati za vrstu datotečnog sustava, iako je već prepoznao da se radi FAT16 particiji.



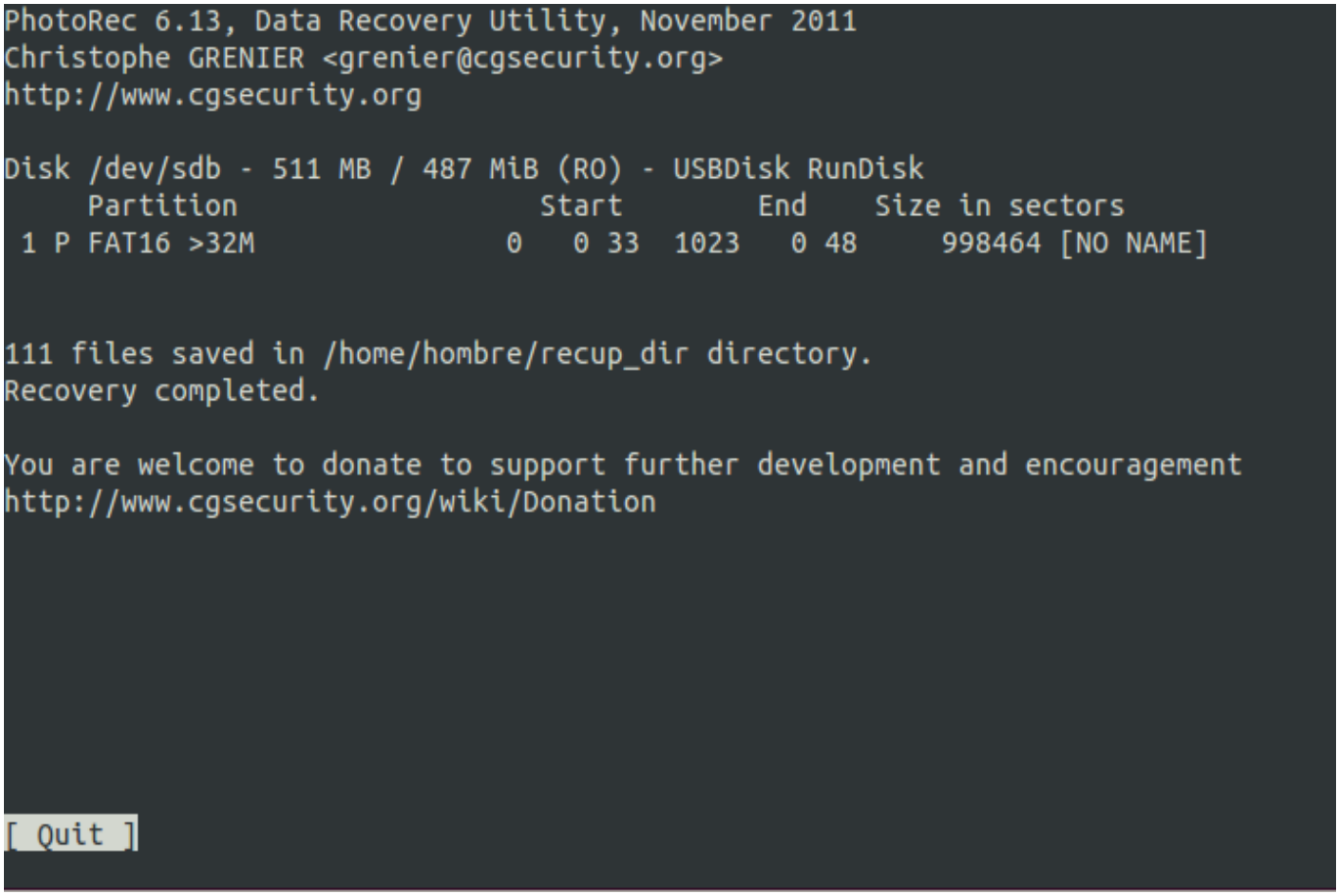
Potvrdimo da se radi o Microsoftovom datotečnom sustavu. Nakon toga pita da li želimo pretražiti cijeli prostor diska, ili samo nealociran prostor, a upravo se tu nalaze obrisane dateke. To ćete odabrati ako vas zanimaju samo obrisane datoteke. U protivnom, odaberite sigurniju mogućnost, a to je pretraživanje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



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.



Kada završi, dobit ćemo sumarni izvještaj.



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