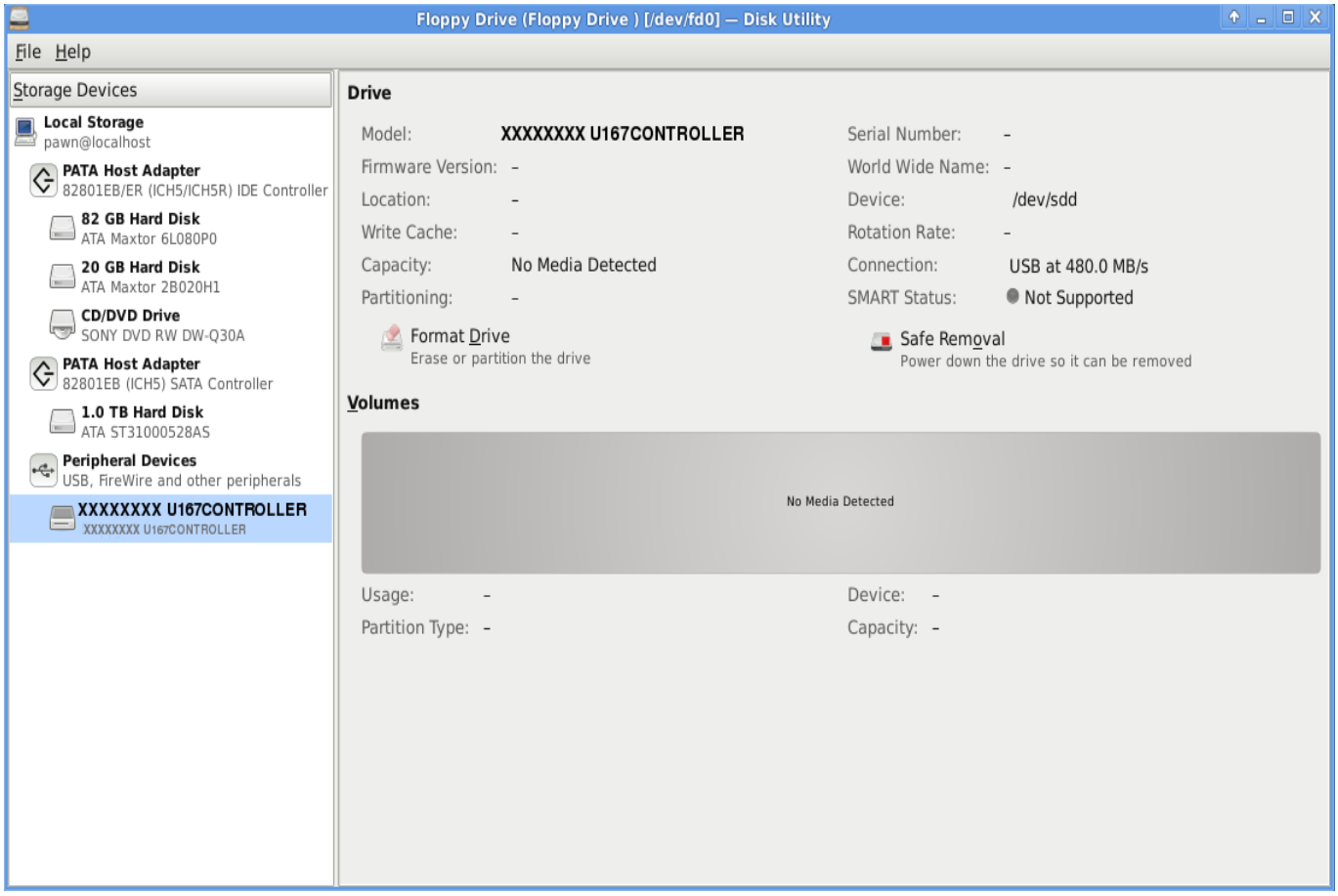
# Spašavanje USB sticka

Sinhronicitet sa nedavnom serijom članaka o spašavanju podataka pomoću alata *dd_rescue*, *testdisk*, *photorec* dogodio se kod mene na ustanovi. Kopiranje podataka na potpuno novi Diesel USB 2.0 Flash Drive kapaciteta 16 GB trajalo je predugo, pa je nestpljivi korisnik odustao i restartao cijeli posao. Nakon toga je USB stick jednostavno prestao komunicirati s vanjskim svijetom.

Korisnik mi je ga  donio sa molbom da mu probam "preko Linuxa otvoriti stick, jer ga Windowsi više ne prepoznaju".

Nakon spajanja na USB port stick je treptao LED lampicom kao što je uobičajeno pri inicijalizaciji uređaja, međutim treptanje nije prestajalo. Uobičajeno "mountanje" nije prolazilo. USB stick nisam pronalazio ni u svom File Manageru.

Prvo sam posegnuo za jednostavnom GUI Disk Utility metodom:




Disk manager je prepoznao uređaj pod sasvim čudnim imenom  XXXXXXXX U167CONTROLLER  bez većine uobičajenih podataka o uređaju.

Korisniku podaci nisu bili životno važni jer ima kopiju, ali želio bi i dalje koristiti svoj novi USB stick.

Pokušaj  formatiranja sa Gparted ne uspijeva jer on uopće ne pronalazi /dev/sdd kako je ga

prepoznao Disk Utility. Znači ne prikazuje se ni nealocirani prostor ni kao nepoznat ni poznat.

Posežemo za /var/log/syslog i pronalazimo:

```
Jan  7 13:16:19 savior kernel: [20603.040047] usb 1-8: new high speed USB device usin
g ehci_hcd and address 4
Jan  7 13:16:19 savior kernel: [20603.172407] usb 1-8: New USB device found, idVendor
=048d, idProduct=1167
Jan  7 13:16:19 savior kernel: [20603.172414] usb 1-8: New USB device strings: Mfr=0,
 Product=0, SerialNumber=0
Jan  7 13:16:19 savior kernel: [20603.172586] usb 1-8: configuration #1 chosen from 1
 choice
Jan  7 13:16:20 savior kernel: [20603.826433] Initializing USB Mass Storage driver...
Jan  7 13:16:20 savior kernel: [20603.826606] scsi4 : SCSI emulation for USB Mass Sto
rage devices
Jan  7 13:16:20 savior kernel: [20603.826761] usbcore: registered new interface drive
r usb-storage
Jan  7 13:16:20 savior kernel: [20603.826766] USB Mass Storage support registered.
Jan  7 13:16:20 savior kernel: [20603.827492] usb-storage: device found at 4
Jan  7 13:16:20 savior kernel: [20603.827497] usb-
storage: waiting for device to settle before scanning
Jan  7 13:16:25 savior kernel: [20608.824238] usb-storage: device scan complete
Jan  7 13:16:25 savior kernel: [20608.828747] scsi 4:0:0:0: Direct-
Access     XXXXXXXX U167CONTROLLER   0.00 PQ: 0 ANSI: 2
Jan  7 13:16:25 savior kernel: [20608.832264] sd 4:0:0:0: Attached scsi generic sg4 t
ype 0
Jan  7 13:16:25 savior kernel: [20608.839075] sd 4:0:0:0: [sdd] Attached SCSI removab
le disk
```

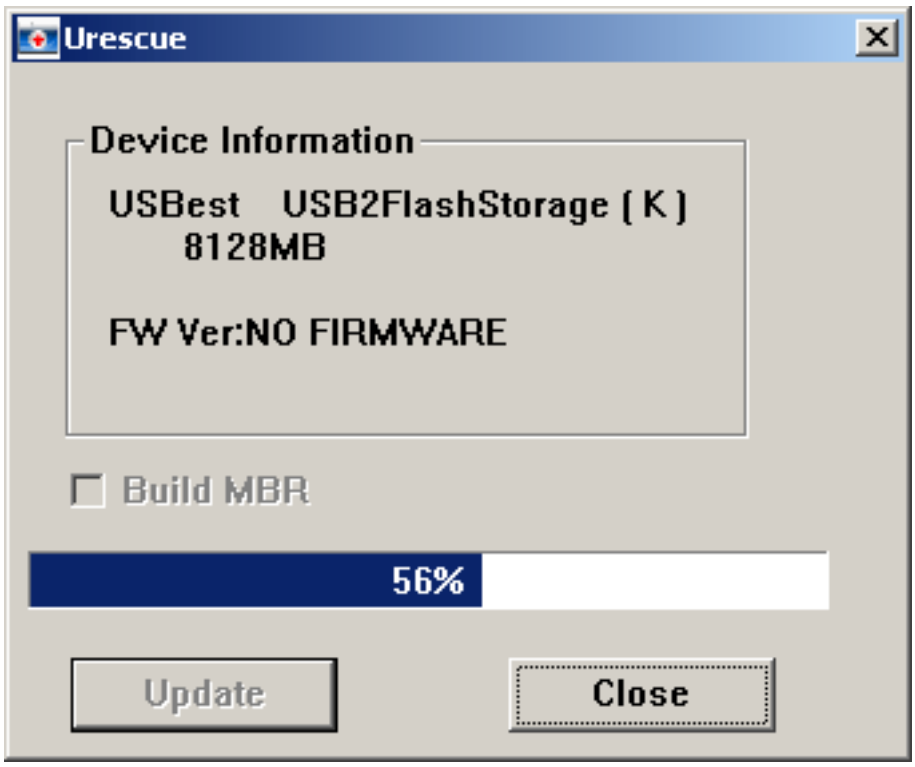
Pokušaji upotrebe alata *testdisk* i *dd_rescue* na /dev/sdd javljaju "nepoznat uređaj".

Nakon pretrage po Internetu javlja se sumnja na oštećen firmware, a nudi se i alat koji to može riješiti. Alat se zove Urescue v1.3.0.71, a nudi se na "sumnjivoj" stranici http://flashboot.ru.

Preuzimamo rizik, skidamo alat za "flash firmwarea". Po uputi s ruske stranice koristimo Windows XP. Prije pokretanja alata treba spojiti USB stick i ugasiti antivirusnu zaštitu koja bi blokirala "sumnjiv posao". Inače ikonica URescuea izgleda kao kutija "Prve pomoći" iz automobila i djeluje smirujuće :). No ipak sam bio oprezan. Pomogli su i komentari oduševljenih korisnika sa ruske stranice koji su spasili svoje USB ljubimce. Prije pokretanja alata i isključivanja antivirusa odskenirao sam ga antivirusom, nije pronađeno ništa sumnjivo.

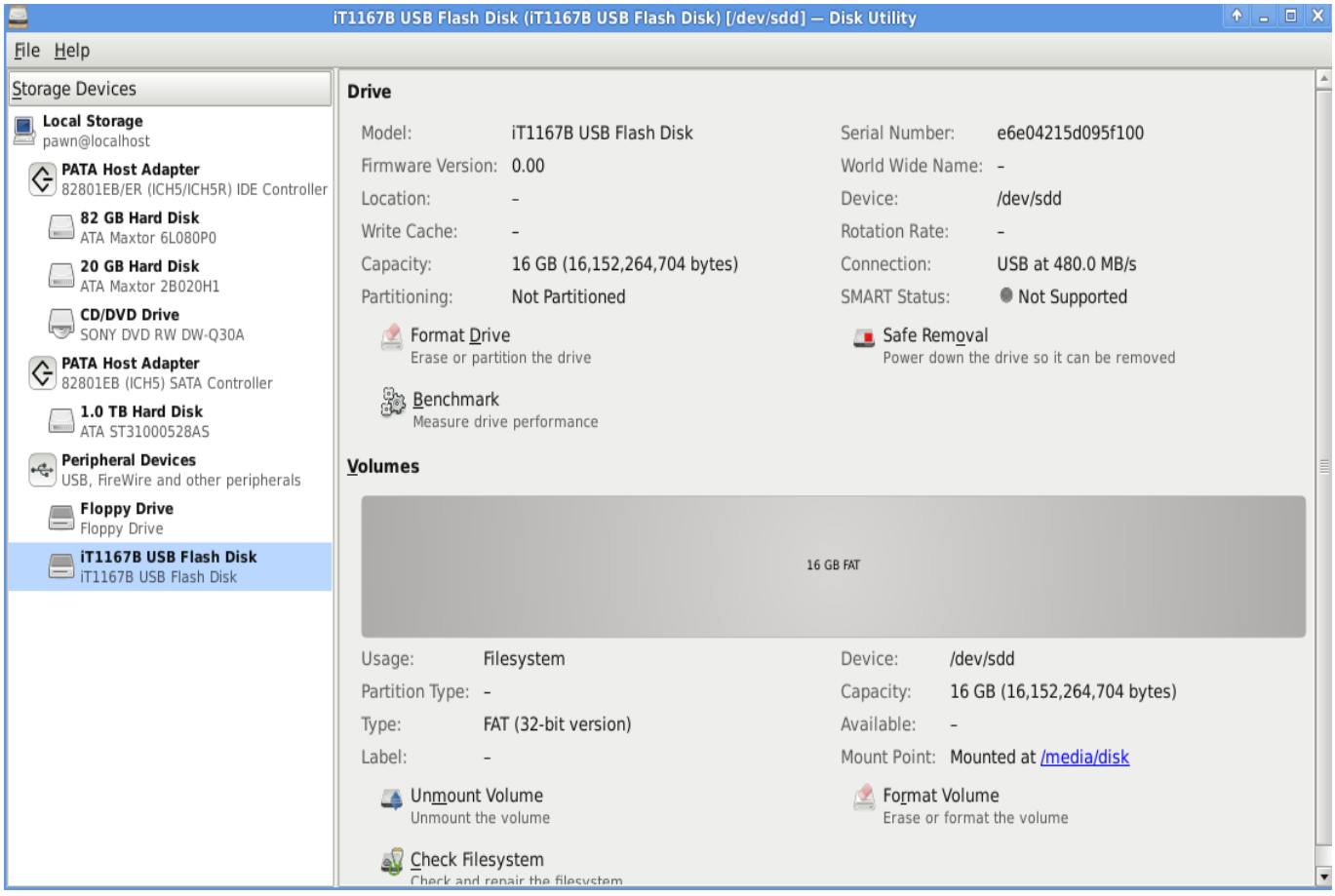
Pokretanjem alata pojavljuje se dijalog koji pita da li želimo pokrenuti nadogradnju firmwarea. Odaberemo "OK" bez označavanja opcije Build MBR.

Sam proces nadogradnje izgleda kao na slijedećoj slici:




Proces uspijeva, pacijent preživljava, ponovno se pojavljuje memorijski prostor i pokušaji pisanja prolaze. Svakako treba antivirusnim skenerom pretražiti stick da možda nema kakvog "slijepog putnika".

Premda je ime sticka promijenjeno USB stick se sada ispravno prikazuje na Linuxu.

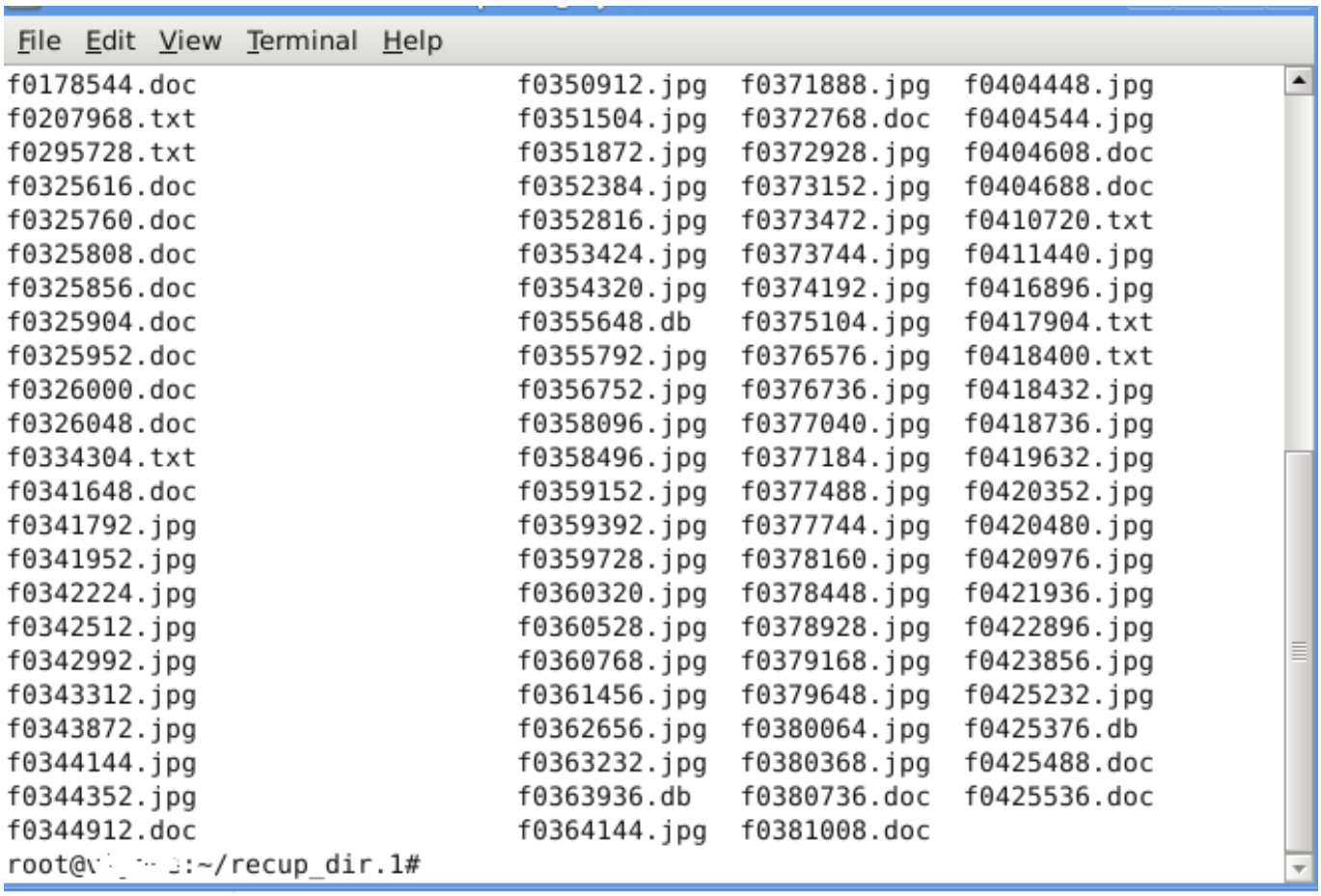


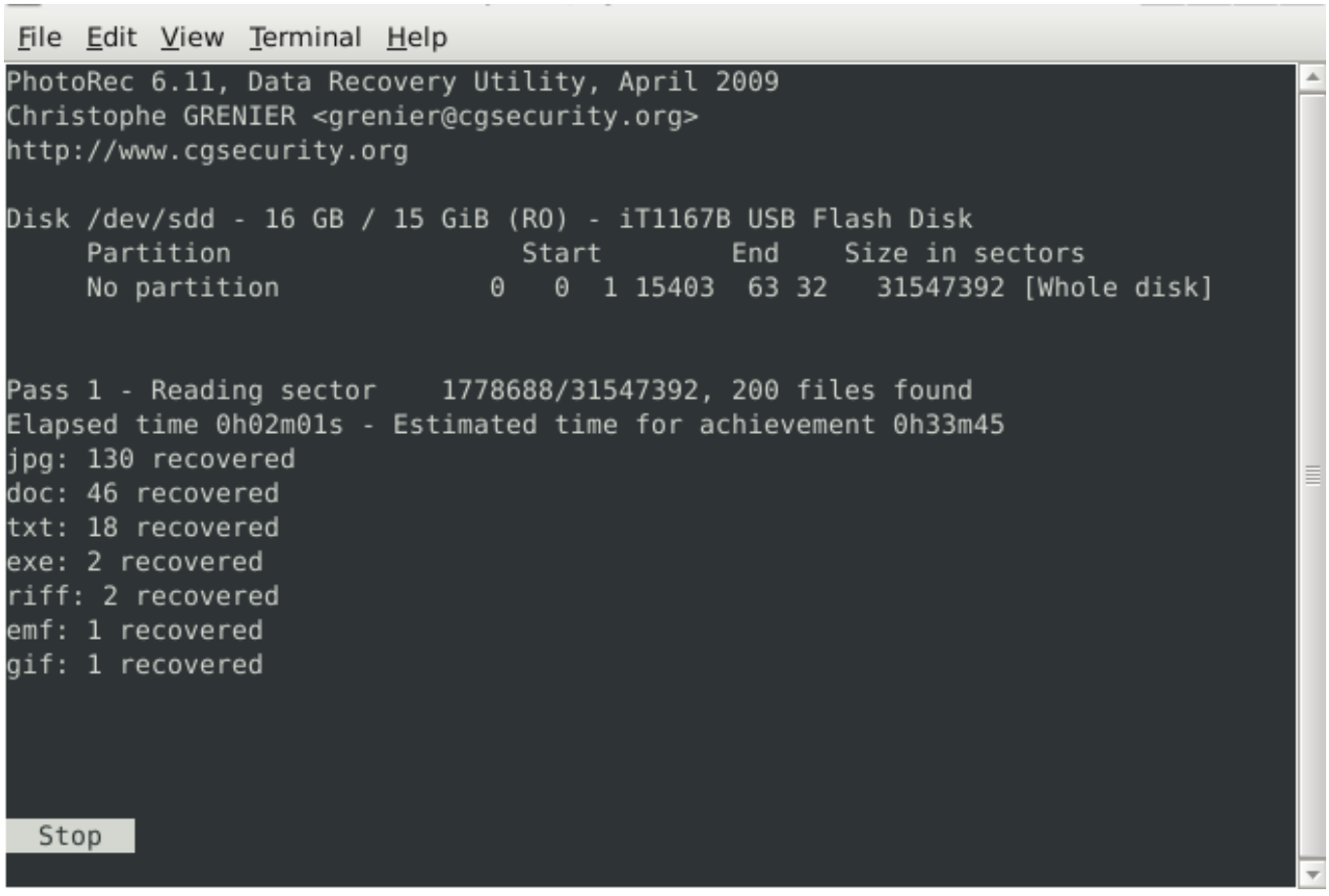

U /var/log/syslog se također ispravno vidi:

```
Jan  8 09:10:12 savior hald: unmounted /dev/sdd1 from '/media/disk' on behalf of uid
1000
Jan  8 09:10:17 savior kernel: [ 5352.907750] usb 1-8: USB disconnect, address 4
Jan  8 09:10:32 savior kernel: [ 5367.996037] usb 1-8: new high speed USB device usin
g ehci_hcd and address 5
Jan  8 09:10:32 savior kernel: [ 5368.130572] usb 1-8: New USB device found, idVendor
=048d, idProduct=1167
Jan  8 09:10:32 savior kernel: [ 5368.130579] usb 1-8: New USB device strings: Mfr=1,
 Product=2, SerialNumber=3
Jan  8 09:10:32 savior kernel: [ 5368.130584] usb 1-8: Product: USB Mass Storage Devi
ce
Jan  8 09:10:32 savior kernel: [ 5368.130588] usb 1-8: Manufacturer: iTE Tech
Jan  8 09:10:32 savior kernel: [ 5368.130591] usb 1-8: SerialNumber: e6e04215d095f100
Jan  8 09:10:32 savior kernel: [ 5368.130763] usb 1-8: configuration #1 chosen from 1
 choice
Jan  8 09:10:32 savior kernel: [ 5368.132976] scsi5 : SCSI emulation for USB Mass Sto
rage devices
Jan  8 09:10:32 savior kernel: [ 5368.133891] usb-storage: device found at 5
Jan  8 09:10:32 savior kernel: [ 5368.133895] usb-
storage: waiting for device to settle before scanning
Jan  8 09:10:37 savior kernel: [ 5373.132207] usb-storage: device scan complete
Jan  8 09:10:37 savior kernel: [ 5373.132818] scsi 5:0:0:0: Direct-
Access     iT1167B  USB Flash Disk   0.00 PQ: 0 ANSI: 2
Jan  8 09:10:37 savior kernel: [ 5373.135506] sd 5:0:0:0: Attached scsi generic sg4 t
ype 0
Jan  8 09:10:37 savior kernel: [ 5373.137004] sd 5:0:0:0: [sdd] 31547392 512-byte log
ical blocks: (16.1 GB/15.0 GiB)
Jan  8 09:10:37 savior kernel: [ 5373.137564] sd 5:0:0:0: [sdd] Write Protect is off
Jan  8 09:10:37 savior kernel: [ 5373.137570] sd 5:0:0:0: [sdd] Mode Sense: 00 00 00
00
Jan  8 09:10:37 savior kernel: [ 5373.137574] sd 5:0:0:0: [sdd] Assuming drive cache:
 write through
Jan  8 09:10:37 savior kernel: [ 5373.141308] sd 5:0:0:0: [sdd] Assuming drive cache:
 write through
Jan  8 09:10:37 savior kernel: [ 5373.141319]  sdd:
Jan  8 09:10:37 savior kernel: [ 5373.149783] sd 5:0:0:0: [sdd] Assuming drive cache:
 write through
Jan  8 09:10:37 savior kernel: [ 5373.149792] sd 5:0:0:0: [sdd] Attached SCSI removab
le disk
Jan  8 09:10:38 savior kernel: [ 5374.077172] FAT: utf8 is not a recommended IO chars
et for FAT filesystems, filesystem will be case sensitive!
Jan  8 09:10:38 savior hald: mounted /dev/sdd on behalf of uid 1000
```

Iako korisnika nije zanimalo spašavanje podataka, radoznali smo pa pokušavamo iskušati metode opisane u člancima na portalu.

Uzimamo photorec za probu, koji pronalazi dosta izgubljenih podataka koji bi se dali spasiti, kao što je ilustrirano na slijedećim slikama.




Ukratko. ponekad vrijedi riskirati s nekim alatima koji na prvi pogled mogu djelovati sumnjivo. Naravno prije toga treba malo istražiti po Internetu da se iza imena tog "rescue" alata ne krije neki

trojanac.

Sretno spašavanje!

Povezani članci:
Spašavanje podataka s oštećenih medija [1]
Testdisk [2]
Photorec [3]
Računalna forenzika [4]

čet, 2013-01-10 12:28 - Goran Šljivić**Kuharice:** OS [5]
**Kategorije:** Hardware [6]
**Vote:** 4

Vaša ocjena: Nema Average: 4 (4 votes)

**Source URL:** https://sysportal.carnet.hr./node/1179

**Links**
[1] https://sysportal.carnet.hr./node/1169
[2] https://sysportal.carnet.hr./node/1171
[3] https://sysportal.carnet.hr./node/1175
[4] https://sysportal.carnet.hr./node/1177
[5] https://sysportal.carnet.hr./taxonomy/term/16
[6] https://sysportal.carnet.hr./taxonomy/term/24