# Spašavanje podataka s oštećenih medija


Korisniku se pokvario disk, OS se više ne podiže, podaci su nedostupni. Drugi se korisnik žali da su mu propale fotografije, jer je memorijska kartica u digitalnom fotoaparatu nečitljiva. Od sistemca se očekuje da priskoči upomoć.

Možda je disk fizički mrtav, ali možda mu je samo oštećena tablica particija (virus?), ili su pojedini sektori nečitljivi? Disk se možda i može spasiti, ali time ćemo se baviti kasnije, najprije treba spasiti podatke.

Prvi test obavit ćemo spajanjem kvarnog diska preko USB sučelja na svoje računalo s Linuxom (pravi sistemci koriste Linux :). Za to se može lijepo iskoristiti USB dok za SATA diskove. Takav bi dok trebao biti dio standardne opreme za preživljavanje marljivog sistemca. Ako vam ga uprava ne želi kupiti, kupite ga sami, kao što sam ja uradio. Trošak od tristotinjak kuna za dok s USB 3.0 sučeljem neće previše opteretiti kućni budžet, a poslužit će mnogo puta, za kloniranje diskova, za privremeno sklanjanje korisničkih podataka pri prelasku na novi/drugačiji OS itd. Neki modeli imaju dodatno e-SATA sučelje, a poneki i utore za memorijske kartice - sve će to dobro doći.

Kad disk priključite preko USB porta, kernel bi ga trebao prepoznati. To se provjeri slijedećom naredbom:

```
# dmesg
...
[17640.997540] usb 1-1.4.2: new high-speed USB device number 19 using ehci_hcd
[17641.095033] usb 1-1.4.2: New USB device found, idVendor=18a5, idProduct=022a
[17641.095040] usb 1-1.4.2: New USB device strings: Mfr=10, Product=11, SerialNumber=
3
[17641.095044] usb 1-1.4.2: Product: Desktop USB3.0 Drive
[17641.095048] usb 1-1.4.2: Manufacturer: Verbatim
[17641.095051] usb 1-1.4.2: SerialNumber: 18A5022A0001A689
[17641.096012] scsi8 : usb-storage 1-1.4.2:1.0
[17642.091894] scsi 8:0:0:0: Direct-
Access     SAMSUNG  HD103SI          0010 PQ: 0 ANSI: 2 CCS
[17642.092888] sd 8:0:0:0: Attached scsi generic sg2 type 0
[17642.093635] sd 8:0:0:0: [sdb] 1953525168 512-byte logical blocks: (1.00 TB/931 GiB
)
[17642.095084] sd 8:0:0:0: [sdb] Write Protect is off
[17642.095088] sd 8:0:0:0: [sdb] Mode Sense: 28 00 00 00
[17642.095875] sd 8:0:0:0: [sdb] No Caching mode page present
[17642.095883] sd 8:0:0:0: [sdb] Assuming drive cache: write through
[17642.098512] sd 8:0:0:0: [sdb] No Caching mode page present
[17642.098520] sd 8:0:0:0: [sdb] Assuming drive cache: write through
[17642.482460]  sdb: sdb1
```

Potražite gdje se spominju USB uređaji, pa ćete vidjeti da je disk prijavljen kao /dev/sdb. Obratite pažnju na činjenicu da je /dev/sdb cijeli disk, dok bi pojedine particije bile /dev/sdb1, /dev/sdb2 itd. U gornjem slučaju tablica particija je čitljiva i vidi se da disk ima jednu ispravnu particiju.

U slučaju da spašavate podatke sa SD kartice, zapis će izgledati malo drugačije:

```
# dmesg
...
[25547.449691] mmc0: new SD card at address b368
[25547.464639] mmcblk0: mmc0:b368 SD    1.88 GiB
[25547.467353]  mmcblk0: p1
```

Ako su particije ispravne, sistem će ih nakon prepoznavanja uređaja montirati, što će se vidjeti naredbom mount:

```
# mount
...
/dev/sdb1 on /media/sistemac/VERBATIM HD type vfat (rw,nosuid,nodev,uid=1000,gid=1000
,shortname=mixed,dmask=0077,utf8=1,showexec,flush,uhelper=udisks2)
/dev/mmcblk0p1 on /media/sistemac/FC30-3DA9 type vfat (rw,nosuid,nodev,uid=1000,gid=1
000,shortname=mixed,dmask=0077,utf8=1,showexec,flush,uhelper=udisks2)
```

Ako disk nije prepoznat, onda mu se ne može pristupiti na fizičkoj razini, pa podatke (možda) mogu izvući samo specijalizirane tvrtke, kad bi vaš korisnik bio spreman platiti takvu uslugu. Ako se uređaj odaziva, ali je oštećena tablica particija, onda nije moguće montirati particije, ali se podaci još uvijek mogu spasiti, samo treba prekopirati cijeli sadržaj diska.

Unixoidi dolaze s naredbom koja se naprosto nudi za takav posao: ***dd***. Njeno je ime pomalo zagonetno. Neki smatraju da je to asocijacija na *Data Description* iz IBM-ovog *Job Control Languagea*. Drugi kažu da se naredba trebala zapravo zvati *cc*, od *Copy and Convert*, ali je to ime već zauzeo C compiler, pa su naprosto uzeli slijedeće slobodno slovo. Kako bilo da bilo, *dd* obavlja funkcije kopiranja blokova podataka, datoteka, particija ili cijelog uređaja, a usput može obaviti različite konverzije, na primjer velikih slova u mala, ili EBDIC kodiranja u ASCII, što danas rijetko kome još treba.

No naredba *dd* za spašavanje nije posve pogodna, jer nije napravljena za korumpirane filesysteme i oštećene diskove. Ako naleti na loš sektor, *dd* može prekinuti kopiranje, ili naprosto preskočiti nečitke podatke. Time će se poremetiti razmaci među blokovima podataka, takozvani offset. Zato je za spašavanje bolje koristiti modificiranu naredbu ***dd_rescue***, čiji je autor Kurt Garloff [1].

*dd_rescue* će obaviti posao od početka do kraja, a mjesto koje zauzimaju nečitki podaci bit će popunjeno ba bi se sačuvala "geometriju" datotečnog sustava. Osim toga, *dd_rescue* može čitati disk od početka prema kraju, ili obrnuto, ako nešto zapne. Na taj način se može spasiti bar dio podataka.

Na Debianu je dostupan paket *ddrescue*, koji je jednostavno instalirati:

```
# apt-get install ddrescue
```

Na Ubuntuu se paket zove *gddrescue*, a sama naredba *ddrescue*.

Odmah instalirajte i drugi alat koji će vam trebati za spašavanje podataka:

```
# apt-get install testdisk
```

Kad kopiramo cijeli disk, što je preporučen način spašavanja podataka, tada ne koristimo naredbu za montiranje datotečnih sustava. Naredbi *dd_rescue* kažemo da iskopira cijeli disk u jednu datoteku:

```
# dd_rescue /dev/sdb korisnikov-disk.img
```

Ili, za kopiranje SD kartice:

```
# dd_rescue /dev/mmcblk0 SDcard
GNU ddrescue 1.16
Press Ctrl-C to interrupt

rescued:     2028 MB,  errsize:       0 B,  current rate:    7208 kB
   ipos:     2028 MB,   errors:       0,    average rate:    9180 kB/s
   opos:     2028 MB,     time since last successful read:       0 s
Finished
```

Sada imate presliku cijelog oštećenog tvrdog diska, ili SD kartice. Originalne medije možete spremiti, o njima ćete misliti kasnije, sada treba brzo i efikasno spasiti podatke.

Za spašavanje datoteka poslužit će naredba ***photorec***, koja je dio paketa *testdisk*. Naziv je vjerojatno dobila radi spašavanja podataka s memorijskih kartica fotoaparata. Kada je baterija u kameri pri kraju, upisivanje novih snimaka postaje rizično, pa se povremeno zna dogoditi gubitak podataka.

Photorec radi ispod razine datotečnog sustava, može izvući datoteke iz korumpiranih particija. Prt tome ne dira izvornu sliku diska, nastojati će iz nje izvući datoteke i prepisati ih na ispravan filesystem.

```
# photorec /log /d spaseno korisnikov-disk.img
```

Uključili smo logiranje, ulazna datoteka je korisnikov-disk.img, koju nam je pripremo dd_rescue, a spašene datoteke idu u u direktorij spaseno.

Kad se radi o većem disku, najbolje vam je naredbu pokrenuti navečer i ostaviti računalo da radi preko noći. Ili, ako ste na poslu, pokrenite photorec na kraju radnog vremena.

U narednom članku [2] pozabavit ćemo se oporavkom oštećenog medija.

Povezani članci:
[3]Testdisk [2]
Photorec [4]
Računalna forenzika [5]
Spašavanje USB sticka [3]

pon, 2012-12-24 08:30 - Aco Dmitrović**Vote:** 4

Vaša ocjena: Nema Average: 4 (2 votes)

**Source URL:** https://sysportal.carnet.hr/node/1169?page=0

**Links**
[1] http://www.garloff.de/kurt/linux/ddrescue/
[2] https://sysportal.carnet.hr/node/1171
[3] https://sysportal.carnet.hr/node/1179
[4] https://sysportal.carnet.hr/node/1175
[5] https://sysportal.carnet.hr/node/1177