

Spašavanje USB sticka

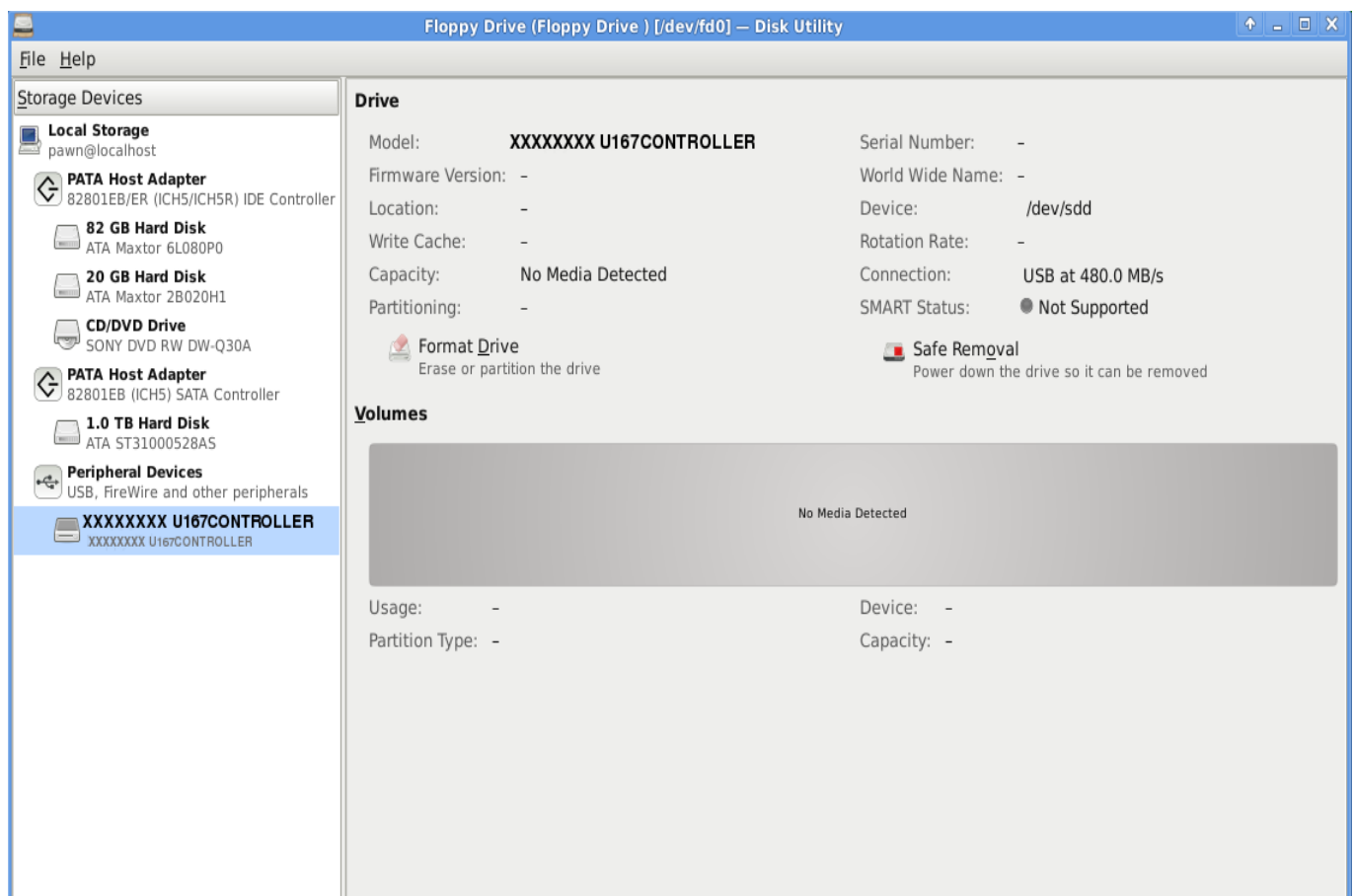


Sinhronicitet sa nedavnom serijom članaka o spašavanju podataka pomoću alata *dd_rescue*, *testdisk*, *photorec* dogodio se kod mene na ustanovi. Kopiranje podataka na potpuno novi Diesel USB 2.0 Flash Drive kapaciteta 16 GB trajalo je predugo, pa je nestpljivi korisnik odustao i restartao cijeli posao. 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 using 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 Storage devices
Jan  7 13:16:20 savior kernel: [20603.826761] usbcore: registered new interface driver 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 type 0
Jan  7 13:16:25 savior kernel: [20608.839075] sd 4:0:0:0: [sdd] Attached SCSI removable disk
```

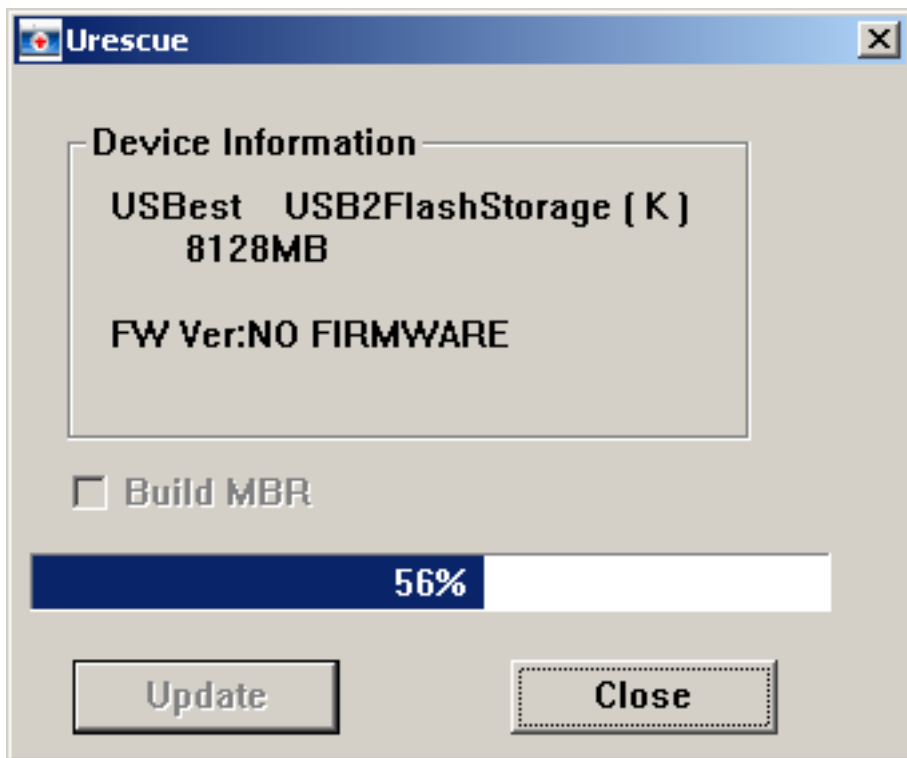
Pokušaji upotrebe alata `testdisk` i `dd_rescue` na `/dev/sdd` javljaju "nepoznat uređaj".

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 ugaziti 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.

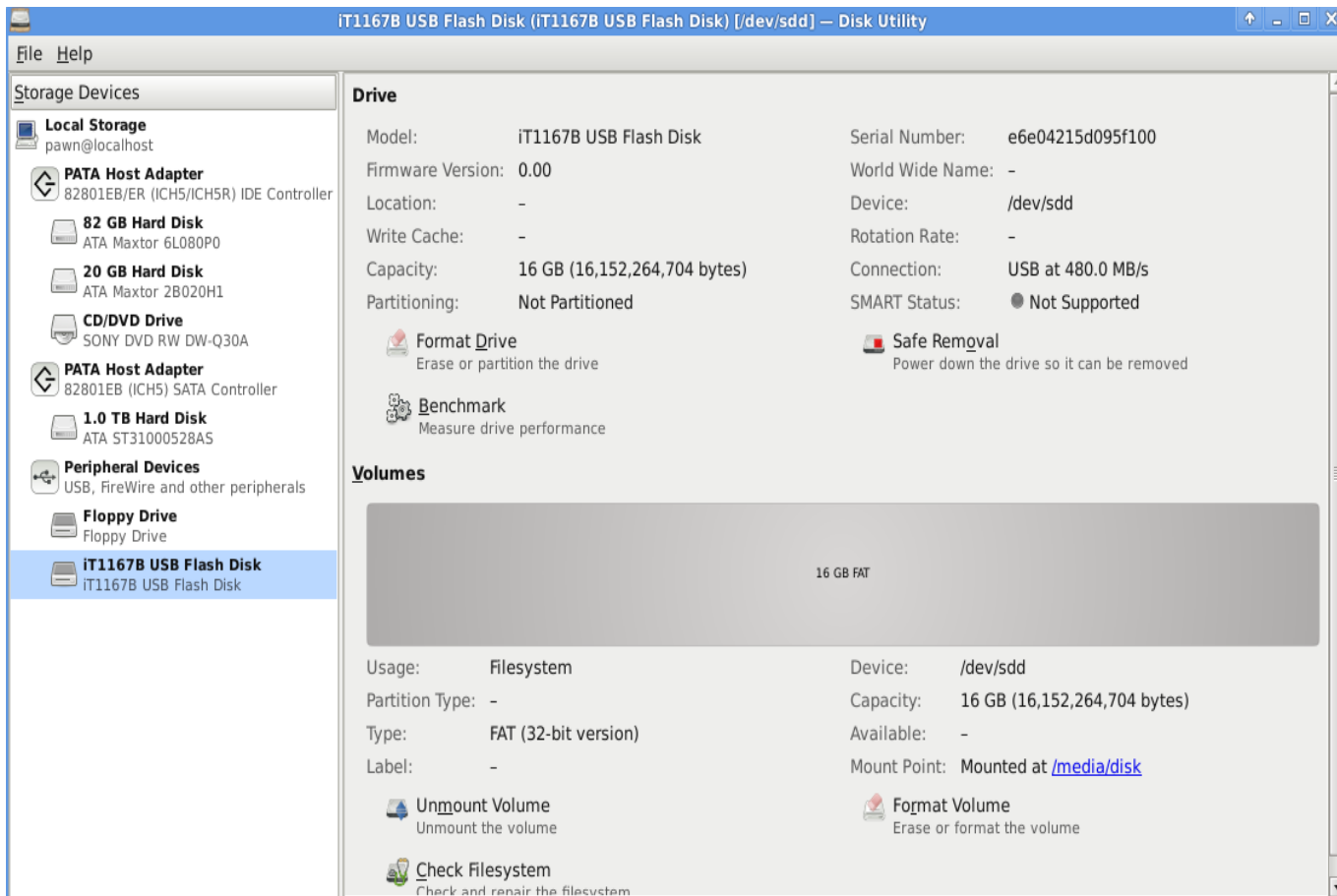
Pokretanjem alata pojavljuje se dijalog koji pita da li želimo pokrenuti nadogradnju firmwarea. Odaberemo "OK" bez označavanja opcije Build MBR.

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

```
File Edit View Terminal Help
f0178544.doc      f0350912.jpg    f0371888.jpg    f0404448.jpg
f0207968.txt      f0351504.jpg    f0372768.doc    f0404544.jpg
f0295728.txt      f0351872.jpg    f0372928.jpg    f0404608.doc
f0325616.doc      f0352384.jpg    f0373152.jpg    f0404688.doc
f0325760.doc      f0352816.jpg    f0373472.jpg    f0410720.txt
f0325808.doc      f0353424.jpg    f0373744.jpg    f0411440.jpg
f0325856.doc      f0354320.jpg    f0374192.jpg    f0416896.jpg
f0325904.doc      f0355648.db     f0375104.jpg    f0417904.txt
f0325952.doc      f0355792.jpg    f0376576.jpg    f0418400.txt
f0326000.doc      f0356752.jpg    f0376736.jpg    f0418432.jpg
f0326048.doc      f0358096.jpg    f0377040.jpg    f0418736.jpg
f0334304.txt      f0358496.jpg    f0377184.jpg    f0419632.jpg
f0341648.doc      f0359152.jpg    f0377488.jpg    f0420352.jpg
f0341792.jpg      f0359392.jpg    f0377744.jpg    f0420480.jpg
f0341952.jpg      f0359728.jpg    f0378160.jpg    f0420976.jpg
f0342224.jpg      f0360320.jpg    f0378448.jpg    f0421936.jpg
f0342512.jpg      f0360528.jpg    f0378928.jpg    f0422896.jpg
f0342992.jpg      f0360768.jpg    f0379168.jpg    f0423856.jpg
f0343312.jpg      f0361456.jpg    f0379648.jpg    f0425232.jpg
f0343872.jpg      f0362656.jpg    f0380064.jpg    f0425376.db
f0344144.jpg      f0363232.jpg    f0380368.jpg    f0425488.doc
f0344352.jpg      f0363936.db     f0380736.doc    f0425536.doc
f0344912.doc      f0364144.jpg    f0381008.doc
root@v...:~/recup_dir.1#
```

```
File Edit View Terminal Help
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 16 GB / 15 GiB (R0) - iT1167B USB Flash Disk
Partition          Start          End          Size in sectors
No partition       0 0 1 15403 63 32 31547392 [Whole disk]

Pass 1 - Reading sector 1778688/31547392, 200 files found
Elapsed time 0h02m01s - Estimated time for achievement 0h33m45
jpg: 130 recovered
doc: 46 recovered
txt: 18 recovered
exe: 2 recovered
riff: 2 recovered
emf: 1 recovered
gif: 1 recovered

Stop
```

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?page=0>

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>