Slučaj ultratankog notebooka

Sistemac je još jednom u prilici da pomogne korisniku u nevolji. Na stolu mu je moderan, super tanak notebook, lagan, "damski". Kupljen prije godinu dana, s dvogodišnjom garancijom (nećemo spominjati ime proizvođača - Nomina sunt odiosa [1]!). Notebook je isporučen s Windowsima 8, ali korisnik kaže da mu se Desetka "sama instalirala", radila do nedavno, a sad se odjednom ne želi više pokrenuti.

Nakon uključivanja na ekranu je obavijest o grešci 0x000021a. Slijedi reboot u *recovery* način rada. MSDN ima stranicu o toj grešci, ***Bug Check 0xC000021A: STATUS_SYSTEM_PROCESS_TERMINATED***, dostupnu ovdje https://msdn.microsoft.com/en-us/library/windows/hardware/ff560177(v=vs.85).aspx [2]. Tu se spominje nekoliko mogućih uzroka:

- Oštećen/kompromitiran *user-mode subsystem*, na primjer *WinLogon* ili *Client Server Run-Time Subsystem* (CSRSS). OS se prebacuje u kernel mode.
- Nepodudarne sistemske datoteke, što se obično događa nakon *restorea* s pričuvne kopije. Programi za backup ponekad ne naprave kopiju sistemskih datoteka ako ih tog časa neki program drži otvorenima/zaključanima.
- Kao najvjerojatniji potencijalni krivac navode se loše napisane aplikacije treće strane i virusi. Dakle, nije kriv MS, nego netko treći. :)

Pokušavamo od korisnika saznati što više informacija, ali on samo sliježe ramenima. Sjeća se da je nakon kupovine računala napravio particiju na koju je instalirao Linux, ali se Linux nije htio pokrenuti, pa je iz Windowsa preformatirao tu particiju u NTFS i koristio je za podatke. Ne sjeća se da je u zadnje vrijeme instalirao neki novi program "treće strane".

Windowsi 10 nude brojne načine oporavka. Sve smo ih isprobali, uključujući *restore* sa skrivene particije, dakle vraćanje na stanje koje je bilo kad je računalo kupljeno. Nude se dva načina, s gubitkom korisničkih podataka, ili s njihovim očuvanjem. Korisnik se prisjetio da je i sam probao oba načina prije nego je zatražio pomoć, ni jedan nije uspio. Te su procedure dobro objašnjene na brojnim siteovima, pa se neću njima baviti.

Korisnik bi svakako želio sačuvati podatke. Godinu dana marljivog rada nije za bacanje. Nema *backup*, naravno. Što drugo preostaje nego dići neku *rescue* distribuciju Linuxa s USB sticka ili CD-a. U BIOS-u smo podesili *boot* poredak, USB stick/CD na prvom mjestu. Ubacimo stick s Linuxom - uzalud. Umjesto sticka priključimo vanjski USB DVD - isto. Uključivanje u druge USB portove ne pomaže. Kad spojimo stick ili USB CD na neko drugo računalo, Linux se normalno pokreće. Vjerojatno bi trebalo omogućiti *boot* sa non-efi uređaja, možda još isključiti *Safe boot*, jer Linux nema Microsoftov certifikat. No sistemca kopka kako ultra tanki, "damski" notebook izgleda iznutra! U napadu radoznalosti odlučuje otvoriti kućište, izvaditi HD, staviti ga u USB dock i spasiti podatke.

Otvaranje notebooka pretvorilo se u noćnu moru. Kao prvo, sistemac stare škole očekuje s donje strane kućišta poklopac koji prekriva tvdi disk, da se zamjena može obaviti bez otvaranja kućišta. Nekad su prijenosnici imali poklopce za RAM i za tvrdi disk. Ništa od toga na ovoj "modernoj" igrački. S donje strane su samo križni vijci, minijaturni, za koje trebaju urarski odvijači. Nakon pažljivog odvrtanja i vađenja vijaka sistemac uviđa da su svi različite dužine. Ako se pri sastavljanu računala u neki utor uvrne predugačak vijak, može se oštetiti matična ploča. Zato izvađen vijak odmah selotejpom pričvršćuje uz njegovo mjesto s donje strane kućišta. Kad su svi vijci izvađeni, kućište se

ne da otvoriti! Na rubovima su plastične kuke, a njihovo razdvajanje je pipav posao jer je lako potrgati kuke od mekane plastike.

U ljutnji, sistemac donosi zaključak: **notebook nije rađen za servisiranje, nego za bacanje**. Dok radi, radi, kad se pokvari, baci ga i kupi novi. Kad je kućište nakon sat vremena otvoreno bez lomova, slijede nova iznenađenja. Tvrdi disk nije pričvršćen vijcima, nego ljepilom! Nakon pažljivog odijepljvanja, u rukama je tanka, krhka igračka, tanja od standardnog 2,5 inčnog diska. Sistemac se suzdržava od kihanja, da ne uništi podatke!

Stavljanje diska u USB dock ne polučuje rezultat. Disk je toliko tanak da je trebalo s obje strane ugurati smotane antistatičke vrećice da drže disk u okomitom položaju. Nakon nekoliko pokušaja, konktakt je uspostavljen, Linux na sistemčevom notebooku prepoznao je i montirao disk. Iz mape Users spašavamo korisničke podatke.

Prije nego se pokuša popravak, bilo bi poželjno napraviti *bitcopy* cijelog diska, da se u slučaju neuspjeha može vratiti početno stanje. Pozivamo u pomoć *ddrescue*, proširenu naredbu *dd*. Originalni *dd* preskočio bi dijelove diska koje ne može pročitati, pa se više ne bi slagali *offseti*.

```
$ sudo ddrescue /dev/sdc disk.img
GNU ddrescue 1.19
Press Ctrl-C to interrupt
rescued:   500107 MB,  errsize:       0 B,  current rate:   20470 kB/s
   ipos:   500107 MB,   errors:       0,    average rate:   43228 kB/s
   opos:   500107 MB, run time:    3.21 h,  successful read:       0 s ago
Finished
```

Hajdemo sad pogledati što se dogodilo s diskom. Umjesto zastarjelog *fdiska*, koristimo *gdisk*.

```
$ sudo gdisk /dev/sdc
[sudo] lozinka:
GPT fdisk (gdisk) version 1.0.1

Warning! Disk size is smaller than the main header indicates! Loading
secondary header from the last sector of the disk! You should use 'v' to
verify disk integrity, and perhaps options on the experts' menu to repair
the disk.
Caution: invalid backup GPT header, but valid main header; regenerating
backup header from main header.

Warning! Error 0 reading partition table for CRC check!
Warning! One or more CRCs don't match. You should repair the disk!

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: damaged

****************************************************************************
Caution: Found protective or hybrid MBR and corrupt GPT. Using GPT, but disk
verification and recovery are STRONGLY recommended.
****************************************************************************
```

Sad je jasnije što se dogodilo. Na disku su GPT particije, a glavna tablica i njezina kopija na kraju diska nisu sinkronizirane. U tablicama su spremljeni CRC kontrolni kodovi, koji ukazuju da je sadržaj tablice mijenjan, nakon čega nije generiran novi CRC kod. Je li to neki virus petljao po podacima? Ili loše napisana aplikacija? Ili Windows restore? Ne znamo.

Pogledajmo particije:

```
Command (? for help): p
Disk /dev/sdc: 976773165 sectors, 465.8 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 9C27FD54-ADD5-4B9F-BEE4-289BBD29F584
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 976773134
Partitions will be aligned on 2048-sector boundaries
Total free space is 4077 sectors (2.0 MiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048         1230847   600.0 MiB   2700  Basic data partition
   2         1230848         1845247   300.0 MiB   EF00  EFI system partition
   3         1845248         2107391   128.0 MiB   0C01  Microsoft reserved ...
   4         2107392       533413887   253.3 GiB   0700  Basic data partition
   5       533413888       934780927   191.4 GiB   0700  Basic data partition
   6       934782976       943013887   3.9 GiB     8200
   7       943013888       976773119   16.1 GiB    2700  Basic data partition
```

Korisniku su na raspolaganju dvije particije, jedna od 253 GiB, s Windowsima, druga od 191 GiB, na kojoj je nekada bio instaliran Linux. Na kraju liste je "izgubljen" prostor od 3.9 GiB, vjerojatno je instalacija Linuxa napravila swap particiju, te mala particija od 16.1 GiB, pretpostavljamo da je na njoj recovery.

Sad možemo prekontrolirati stanje diska.

gdisk ima naredbu za verifikaciju, pritisnemo tipku v.

```
Command (? for help): v

Caution: The CRC for the backup partition table is invalid. This table may
be corrupt. This program will automatically create a new backup partition
table when you save your partitions.

Problem: The secondary header's self-pointer indicates that it doesn't reside
at the end of the disk. If you've added a disk to a RAID array, use the 'e'
option on the experts' menu to adjust the secondary header's and partition
table's locations.

Problem: Disk is too small to hold all the data!
(Disk size is 976773165 sectors, needs to be 976773168 sectors.)
The 'e' option on the experts' menu may fix this problem.

Partition(s) in the protective MBR are too big for the disk! Creating a
fresh protective or hybrid MBR is recommended.

Identified 4 problems!
```

Dakle gdisk je dijagnosticirao četiri problema i sugerirao kako ih popraviti. Idemo u ekspertni način rada:

```
Command (? for help):x

Expert command (? for help): ?
```

```
a    set attributes
c    change partition GUID
d    display the sector alignment value
e    relocate backup data structures to the end of the disk
g    change disk GUID
h    recompute CHS values in protective/hybrid MBR
i    show detailed information on a partition
l    set the sector alignment value
m    return to main menu
n    create a new protective MBR
o    print protective MBR data
p    print the partition table
q    quit without saving changes
r    recovery and transformation options (experts only)
s    resize partition table
t    transpose two partition table entries
u    replicate partition table on new device
v    verify disk
w    write table to disk and exit
z    zap (destroy) GPT data structures and exit
?    print this menu
```

Tablicu particija ćemo kopirati na kraj diska, jer nam je *gdisk* javio da je rezervna tablica oštećena i na pogrešnom mjestu.

```
Expert command (? for help): e
Relocating backup data structures to the end of the disk
```

Pokušajmo još ponovo izračunati CHS vrijednosti (Cilinder, Head, Sector), jer gdisk kaže da veličina diska ne odgovara zapisanim podacima.

```
Expert command (? for help): h
```

Nakon ovih zahvata, mogli bi ponoviti verifikaciju.

```
Expert command (? for help): v

Caution: The CRC for the backup partition table is invalid. This table may
be corrupt. This program will automatically create a new backup partition
table when you save your partitions.

Identified 1 problems!
```

Dakle tri problema su riješena, ostao je pogrešan CRC. Hajdemo zapisati izmjene na disk, očekujući da ćemo time riješiti pogrešan CRC.

```
Expert command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/sdc.
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
```

```
run partprobe(8) or kpartx(8)
The operation has completed successfully.
```

Za svaki slučaj reboot, pa sad možemo ponoviti verifikaciju.

```
Command (? for help): v

No problems found. 4074 free sectors (2.0 MiB) available in 3
segments, the largest of which is 2048 (1024.0 KiB) in size.
```

Odlično, kontrolne sume obnovljene su prilikom snimanja izmjena.

Pokreške u konfiguraciji diskovnog prostora su popravljene, *gdisk* je uspješno odradio svoj posao. Za svaki slučaj pokrenuli smo još *chkdsk* koji je našao i popravo nekoliko grešaka. Puni nade krećemo u podizanje Windowsa, ali Desetka se i dalje odbija pokrenuti. Očigledno da je napravljena šteta bila prevelika. Korisnik je nestrpljiv, računalo mu treba za rad, pa je odlučio odnijeti ga u servis. Neka disk vrate u originalno stanje, s Windowsima 8. Nakon toga možemo vratiti korisničke podatke.

Sistemac je iz ovog iskustva izvukao nekoliko pouka. Prije svega, ne treba kupovati notebook koji s donje strane kućišta nema poklopce za vađenje/zamjenu diska i RAM-a. Drugo, ako želite zadržati staru verziju Windowsa treba isključiti automatski *upgrade* i sami birati update koje želite instalirati - definitivno previše posla za običnog korisnika. Treće, ako vam se već naseli Desetka, instalirajte sve ponuđene zakrpe pa nanovo napravite *rescue* image. Četvrto, ako započnete instalaciju Linuxa uz Windowse, onda je i završite. Vjerojatno je korisnik trebao samo promijeniti neke postavke BIOS-a, da bi se OS mogao bootati i s Linux particije. Obično pomogne isključivanje UEFI-ja, Legacy mode, isključivanje Safe boota, a u jednom bizarnom slučaju pomogla je zamjena AHCI standarda komunikacije s diskom starijim IDE standardom. Ne pitajte me zašto.

Pa čemu onda sav trud, kad je notebook ionako završio u servisu? Spasili smo korisničke podatke, koje bi servis pregazio (ili dodatno naplatio njihovo spašavanje). Ponešto smo i naučili, *gdisk* se pokazao kao korisna alatka. A i otvaranje notebooka nije bilo puka gnjavaža. Korisno je zaviriti u utrobu omiljene igračke. Spoznaja da se tvrdi disk može učvrstiti ljepilom, ajme meni, pokazuje što su sve proizvođači sposobni uraditi da bi uštedjeli. I kakvo smeće mi naivni kupci i ne sluteći kupujemo, u nastojanju da dobijemo "kvalitetu" za što manje novca.

Na kraju je sistemac ostao zbunjen. Kakav je niz koincidencija doveo Desetku u takvo rastrojeno stanje? Je li problem u tome što je korisnik pokušao instalirati Linux, pa je instalacija petljala po tablicama particija koje su napravili Windowsi? Zatim je iz Windowsa ponovo prisvojio Linux particiju, dakle Windowsi su pisali po tablicama koje je već modificirao Linux. Možda je "kriv" pokušaj *restorea* Desetke nazad u Osmicu? Ili je za sve kriv nekakav virus kojeg je korisnik usput pokupio? Sistemac je zadržao *bitcopy* tvrdog diska kako bi na miru obavio forenziku. Ali već se javio drugi korisnik kojem treba pomoći, pa je bio prisiljen pobrisati presliku diska. Ionako bi forenzika samo zadovoljila sistemčevu radoznalost, to nije djelatnost koju poslodavac cijeni, priznaje, nagrađuje. Sistemac bi to morao odraditi u slobodno vrijeme, "hobistički". Zar nije bolje prošetati parkom, maknuti se od računala na par sati?

No saga još nije gotova. Kad je preuzeo računalo sa servisa, korisnik je vratio podatke s vanjskog diska. Nakon toga zove sistemca, žaleći se da ne može otvoriti neke od tih datoteka! Većinu je kreirao s Desetkom, a Osmica ih sada ne može otvoriti! Sistemac mu savjetuje da ručno pokrene upgrade Osmice, ali da ne prihvati instalaciju Desetke. Drugi dan korisnik zove i zahvaljuje: zakrpe za Osmicu odradile su posao, sada može normalno raditi. Problem je riješen, ali sistemac je još jednom zbunjen: kakve veze imaju zakrpe za Osmicu s otvaranjem standarnih tipova datoteka? Umjesto da razbija glavu Microsoftovim misterijama, sistemac odlazi šetati u Maksimir. Treba iskoristiti lijep dan! Ne mora se sve znati i razumjeti, zar ne?

pon, 2016-10-31 17:49 - Aco Dmitrović**Kategorije:** Operacijski sustavi [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (3 votes)

Source URL: https://sysportal.carnet.hr/node/1697

Links
[1] http://www.hrleksikon.info/definicija/nomina-sunt-odiosa.htm
[2] https://msdn.microsoft.com/en-us/library/windows/hardware/ff560177(v=vs.85).aspx
[3] https://sysportal.carnet.hr/taxonomy/term/26