

Lsof - vraćanje obrisane datoteke



Naredba **ls** ima toliko primjena (vidi <http://sistemac.carnet.hr/node/562> [1], <http://sistemac.carnet.hr/node/1229> [2]) da ponekad i zaboravimo koje su joj sve mogućnosti.

Sigurno vam se barem jednom dogodilo da ste greškom obrisali neku datoteku (backup naravno niste napravili), pa se potom "lupali po glavi" radi vlastite brzopletosti. Ukoliko se radi o nekoj bitnoj datoteci, moguće je da vas uhvati lagana panika, no ne brinite. Ukoliko su ispunjeni neki uvjeti, možda je moguće vratiti tu datoteku.

Poznato je da Linux svakoj datoteci dodjeljuje broj "inode" (index node - predstavlja "adresu" gdje je pohranjen na disku i sve njegove atribute, primjerice owner, group, read, write itd). Kad koristimo naredbu **rm** u stvari brišemo poveznicu (link) prema inode-u, ali ne i sam inode. Sve dok postoji inode u mogućnosti smo vratiti obrisanu datoteku (moguće je da ga proces i dalje drži otvorenim).

Ako **proces i dalje drži otvorenu datoteku**, tada smo u mogućnosti vratiti obrisano, bez obzira što nam naredba **ls** ne može izlistati traženu datoteku. Naredba **ls** nam pomaže da vidimo koje su datoteke otvorene (list open files), proces koji ga drži otvorenim i **fd** (file descriptor) koji čuva poveznice prema procesu.

Inače to su svi potrebni elementi koji nam trebaju da bi vratili obrisanu datoteku (što je otvoreno, broj procesa i fd). Još jednom treba napomenuti da pomoću naredbe *ls* možemo vratiti samo datoteke koje su otvorene, dakle ako je proces drži otvorenom. U protivnom, vraćanje nije moguće.

Ovaj se postupak najčešće primjenjuje kod slučajno obrisanih datoteka koje se nalaze u direktoriju /tmp.

Kao i uvijek, najbolje je pokazati kako to izgleda u praksi.

Napravili smo jednu tekstualnu datoteku u kojoj će se nalaziti izlistanje direktorija:

```
~/RASPORED$ ls -lah > popis_rasporeda.
```

Naredbom *ls* pogledat ćemo je li datoteka kreirana:

```
~/RASPORED$ ls -lah
-rw-r--r-- 1 pero  pero  660 Mar 10 11:04 popis_rasporeda.txt
```

Pogledat ćemo sadržaj datoteke pomoću naredbe **less**, samo što ćemo naredbu *less* prekinuti sa **CTRL+Z** (ne napuštamo proces):

```
~/RASPORED$ less popis_rasporeda.txt
total 284K
drwxr-xr-x  3 pero  pero  4.0K Mar 10 11:04 .
drwxr-xr-x 73 pero  users  4.0K Mar 19 12:48 ..
-rw-r--r--  1 pero  pero   40K Oct 10 17:16 I_godina_Redoviti_2013.pdf
-rw-r--r--  1 pero  pero   48K Nov  5 12:35 Izvanredni_II_godina_2013.pdf
-rw-r--r--  1 pero  pero   58K Nov  6 14:34 kandidacijska-lista.pdf
popis_rasporeda.txt (END)
```

```
[2]+ Stopped less popis_rasporeda.txt
```

Zapamtimo da naredbu **less** nismo prekinuli, već smo ju pomoću CTRL+Z stavili u pozadinu. Ovo možemo provjeriti ako u shellu pokrenemo naredbu **lsof**:

```
~/RASPORED$ lsof | grep less
less      19072    pero  cwd      DIR     8,7    4096  196640 /home/pero/RASPORED
less      19072    pero  4r      REG     8,7     660  196649 /home/pero/RASPORED/p
opis_rasporeda.
```

Slijedi brisanje datoteke popis_rasporeda.txt:

```
~/RASPORED$ rm popis_rasporeda.
```

Pokušajmo izlistati file popis_rasporeda.txt:

```
~/RASPORED$ ls -lah popis_rasporeda.txt
ls: cannot access popis_rasporeda.txt: No such file or
```

Datoteka je obrisana, no nakon ovoga ne smijemo nikako napustiti naš shell, kao ni ugasiti proces kojim smo otvorili datoteku. Naredba less i dalje drži otvorenu datoteku, jer smo ju prekinuli sa ctrl+z.

Sad slijedi vraćanje obrisane datoteke. Pomoću naredbe **lsof** prvo potražimo potrebne parametre o obrisanoj datoteci:

```
~/RASPORED$ lsof | grep popis_rasporeda.txt
less      19072    pero  4r      REG     8,7     660  196649 /RASPORED/popis_rasporeda.txt (deleted)
```

U prvom stupcu se nalazi naredba koja drži datoteku otvorenom, drugi stupac je ID procesa, zatim slijedi vlasnik, a četvrti stupac je stupac file descriptor. Slovo "r" ovdje znači regularnu datoteku. Svi potrebni parametri su tu, datoteka, broj procesa i fd.

Što dalje napraviti, sada kada imamo sve parametre?. Ono što moramo dokučiti je gdje linux pohranjuje privremeno otvorene datoteke. To je poddirektorij **/proc/[pid]/fd**.

Pogledajmo pomoću ls kako to izgleda, naredba lsof dala je sljedeće parametre: proces 19072, fd 4:

```
~/RASPORED$ ls -l /proc/19072/fd/4
lr-x----- 1 pero pero 64 Mar 10 11:49 /proc/19072/fd/4 -> /RASPORED/popis_rasporeda.txt (deleted)
```

Vidimo da je datoteka u /proc i pripremljena za brisanje, na našu sreću još nije obrisana. Vraćanje ovakvih datoteka je vrlo jednostavno, potrebna je samo naredba cp bez dodatnih parametara. Prilikom vraćanja datoteke, ona se vraća na točno mjesto gdje se i nalazila, zajedno sa svim atributima.

```
~/RASPORED$ cp /proc/19072/fd/4 popis_rasporeda.txt
```

```
~/RASPORED$ ls -lah
-rw-r--r-- 1 pero pero 660 Mar 10 11:56 popis_rasporeda.txt
```

Zdravko Rašić

sri, 2013-03-27 16:36 - Zdravko Rašić **Kuharice:** [Linux](#) [3]

Kategorije: [Operacijski sustavi](#) [4]

Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: <https://sysportal.carnet.hr./node/1237>

Links

[1] <https://sysportal.carnet.hr./node/562>

[2] <https://sysportal.carnet.hr./node/777>

[3] <https://sysportal.carnet.hr./taxonomy/term/17>

[4] <https://sysportal.carnet.hr./taxonomy/term/26>