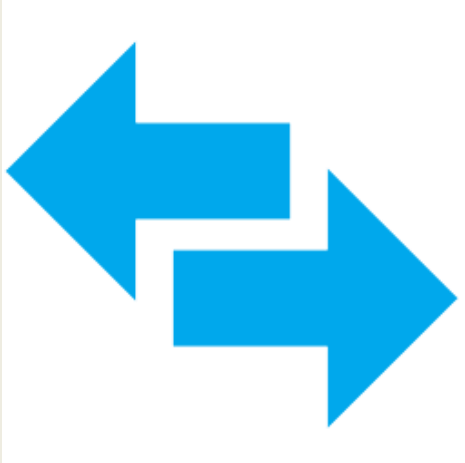
Analizator mrežnih protokola

Predmet: Mrežni servisi

Prof. dr Dušan Stefanović



Poglavlje 1

Šta je Wireshark?

- ✓ **Wireshark predstavlja analizator mrežnih protokola**
  - Open-Source (GNU javna licenca),
  - Radi na različitim platformama (Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, itd.),
  - Lako se nadograđuje,
  - U svakodnevnom razvoju.
- ✓ **Ranije se zvao “Ethereal”**

✓ Karakteristike:

- Inspekcija na hiljadu mrežnih protokola
- Online praćenje i offline analiza saobraćaja.
- Standardni *three-pane* (3 okna) pretraživač paketa.
- Markiran saobraćaj se može pretraživati uz pomoć GUI, ili preko TShark servisa.
- Široki spektar filtera.
- VoIP analiza.
- Podrška za Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI itd standarde.
- Pravila "kolorizacije" za lakše snalaženje.
- Saobraćaj može biti eksportovan u XML, PostScript®, CSV, ili plain text.

✓Sistemski zahtevi:

- Wireshark predstavlja jednu od prosečno zahtevnih aplikacija po pitanju resursa.
- Minimalna zahtevana brzina procesora je 400Mhz, dok je minimalna količina memorije 128 MB.
- Zahtev za prostorom na disku iznosi 100-200 MB, zahtev za memorijom može biti drastično povećan, u zavisnosti od uhvaćenih paketa u jedinici vremena
- Hvatanje paketa na potpuno zaštićenoj ethernet mreži brzine 100 Mb/s zahteva 750 MB/minut).

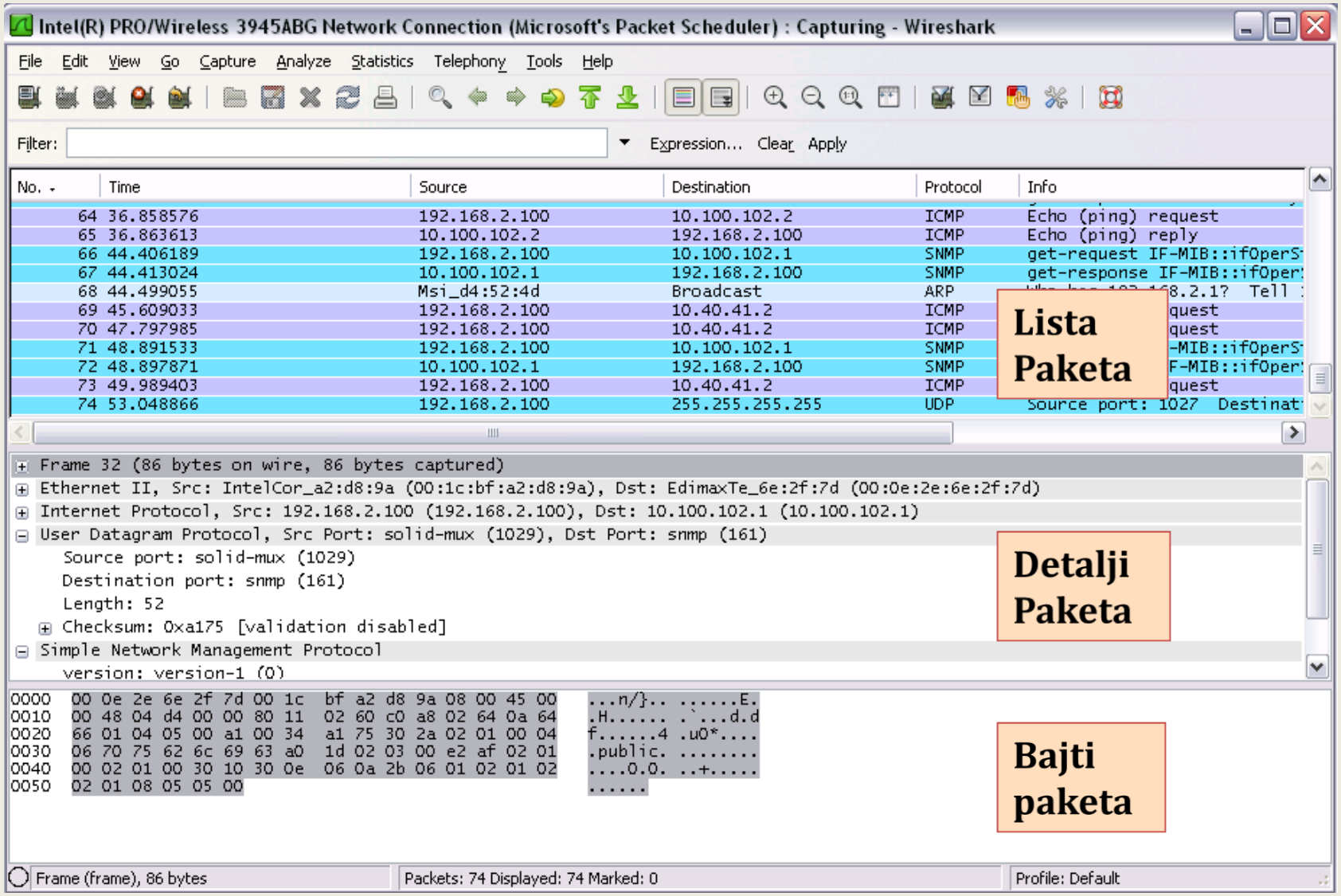
✓ Šta možemo uraditi:

- Snimanje mrežnog saobraćaja,
- Dekodiranje paketa i protokola,
- Definisanje filtera – beleženje i prikazivanje,
- Pametne statistike,
- Problemi prilikom analize i njihovo rešavanje,
- Interaktivno pretraživanje saobraćaja.

✓ Neki primeri korišćenja Wiresharka:

- *Mrežni administratori:*
  - **rešavanje problema na mreži,**
- *Inženjeri sigurnosti na mreži*:
  - **proučavanje sigurnosnih problema,**
- *Developeri*:
  - **debugiranje, implementacija protokola,**
- *Studenti*:
  - **učenje osnova iz računarskih mreža.**

Wireshark Interfejs



Main Toolbar

1. **List the available capture interfaces**

   lista dostupnih interfejsa za hvatanje

2. **Show the capture options**

   opcije hvatanja podataka (selektovanjem ove opcije određujemo interfejs kartici na šta će se asocirati prilikom hvatanja paketa u saobraćaju. Takođe mogu se koristiti više fajlova npr: ako fajl pređe 1MB automatski se kreira drugi, može se kreirati automatsko stopiranje snimanja podataka posle npr. 1000 paketa) itd.

3. **Start new live capture**

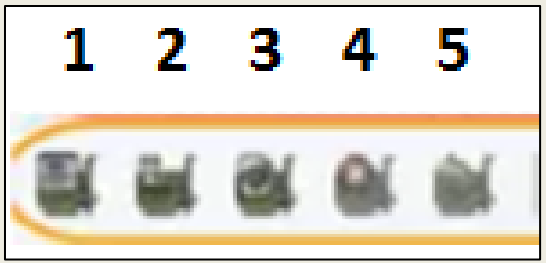
   start novog hvatanja.

4. **Stop the running capture**

   stopiranje trenutnog hvatanja.

5. **Restart the running live capture**

   restart trenutnog hvatanja.



Main Toolbar

6. Open a capture file

otvori uhvaćen fajl.

7. Save this capture file

sačuvaj uhvaćen fajl.

8. Close this capture file

zatvori uhvaćen fajl.

9. Reload this capture file

ponovo otvori uhvaćen fajl.

10. Print

Main Toolbar

Find packet pronadji paket (ako želimo da nađemo određeni paket npr: ARP, neće biti predstavljen u Display Filtru već nas vodi na prvi ARP paket u Packet list panel-u i Packet detail panel-u ,i pokazuje detalje o njemu.

11.Go back in packet history

pamti sve selektovane pakete (opcija vraćanja ne neki od prethodno selektovanih paketa npr: 50, 25, 10,1)

12.Go forward in packet history

idi napred u istoriji paketa (veoma korisna opcija ako imamo više hiljada paketa a želimo da se vratimo na par njih)

13.Go to the packet with number

idi na paket sa brojem (unosi se željeni broj paketa, i automatski se prikazuju detalji o paketu u Packet list panel-u i Packet details panel-u).

14.Go to the first packet

idi na prvi paket.

15.Go to the last packet

idi na zadnji paket.

Main Toolbar

16. **Colorize packet list**

    kolorizuj paket listu (ako ne želimo da vidimo ništa sem crne i bele boje, vršimo selektovanje ove opcije)

17. **Auto scroll packet list in live capture**

    automatsko skrolovanje liste paketa u trenutku hvatanja (pomaze pri određenom pregledu željenog podatka).

18. **Zoom in**

    povećanje veličine podataka

19. **Zoom out**

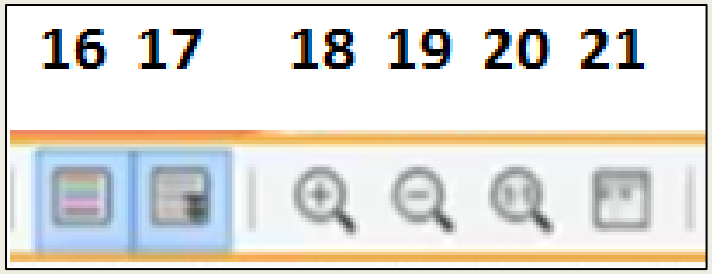
    umanjenje veličine podataka

20. **Zoom 100 %**

    stoprocentualno zumiranje

21. **Resize All Columns**

    (opcija poboljšava pregled kolona i detalja: Time, Source, Destination, Protocol, Length, Info)



Main Toolbar

22. Edit capture filter

uređivanje filtera hvatanja - (opcija hvatanja podataka po želji, npr: samo ARP protokol, i njegov kasniji prikaz i analiza u Display Filter-u)

23. Edit/apply display filter

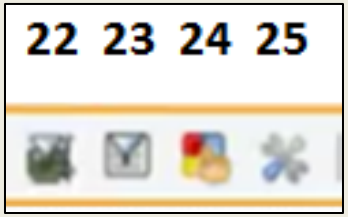
dodavanje display filtra

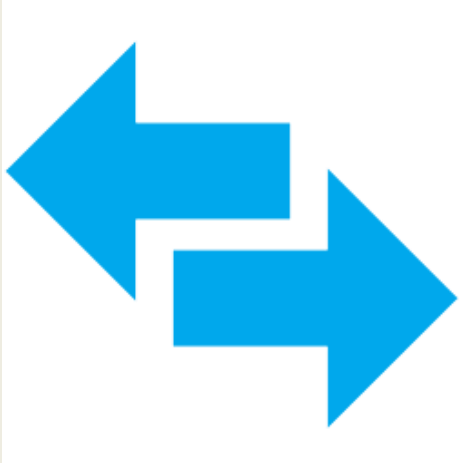
24. Edit coloring rules

uređivanje pravila boja (opcija biranja raznih vrsta boja za različitu vrstu paketa)

25. Edit preferences

uređivanje preferenca (opcija služi za otklanjanje grešaka u uhvaćenim paketima, npr: isključivanje signalizacije greške kod ipv4 protokola)

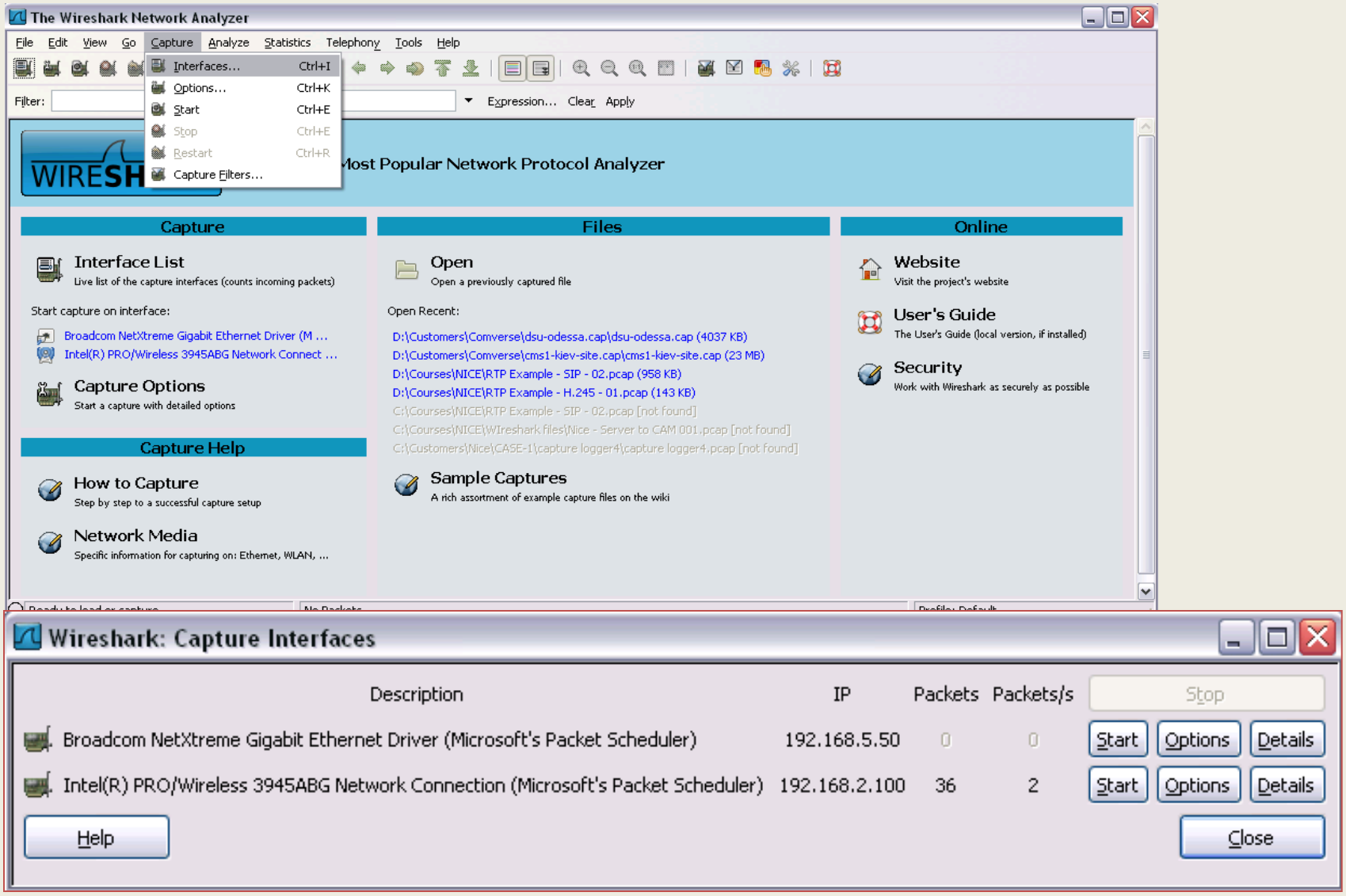


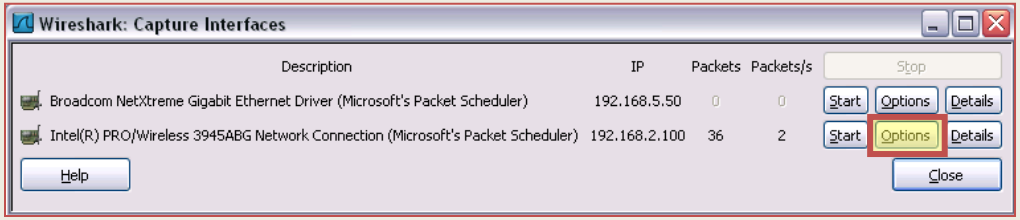


Poglavlje 2

Beleženje paketa

Lista interfejsa





Beleženje svih paketa na mreži

Buffer size da ne bi došlo do preopterećenja memorije

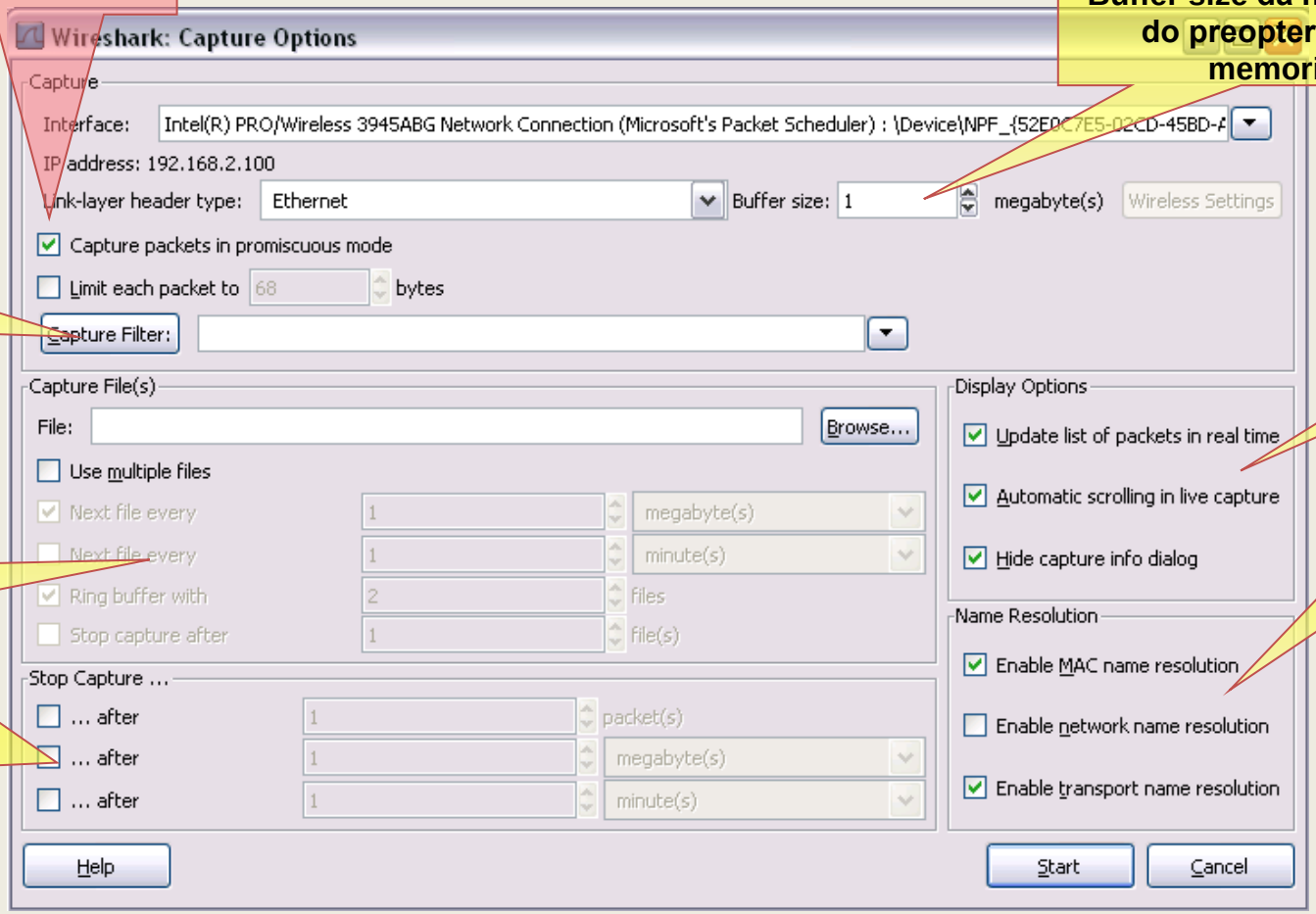
Filter beleženja

Opcije prikaza

Beleženje višestrukih fajlova

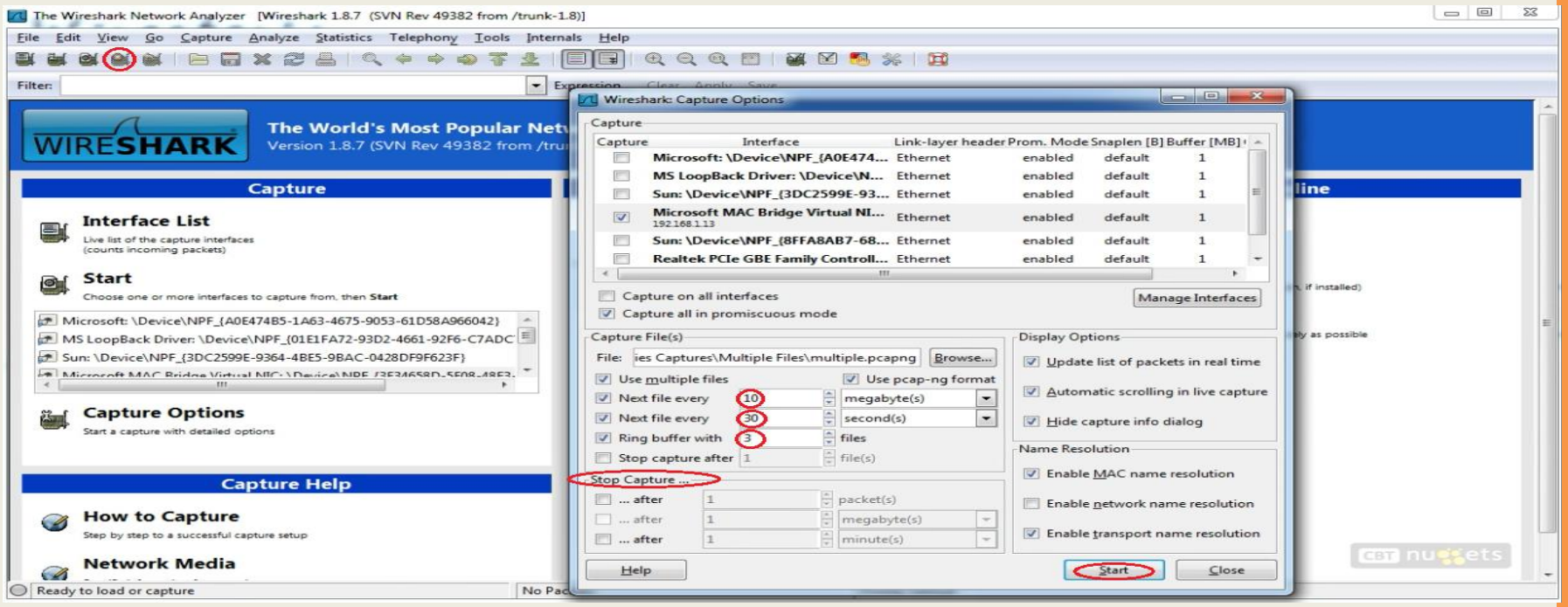
Opcije razrešavanja imena

U kome trenutku automatski prestati sa beleženjem

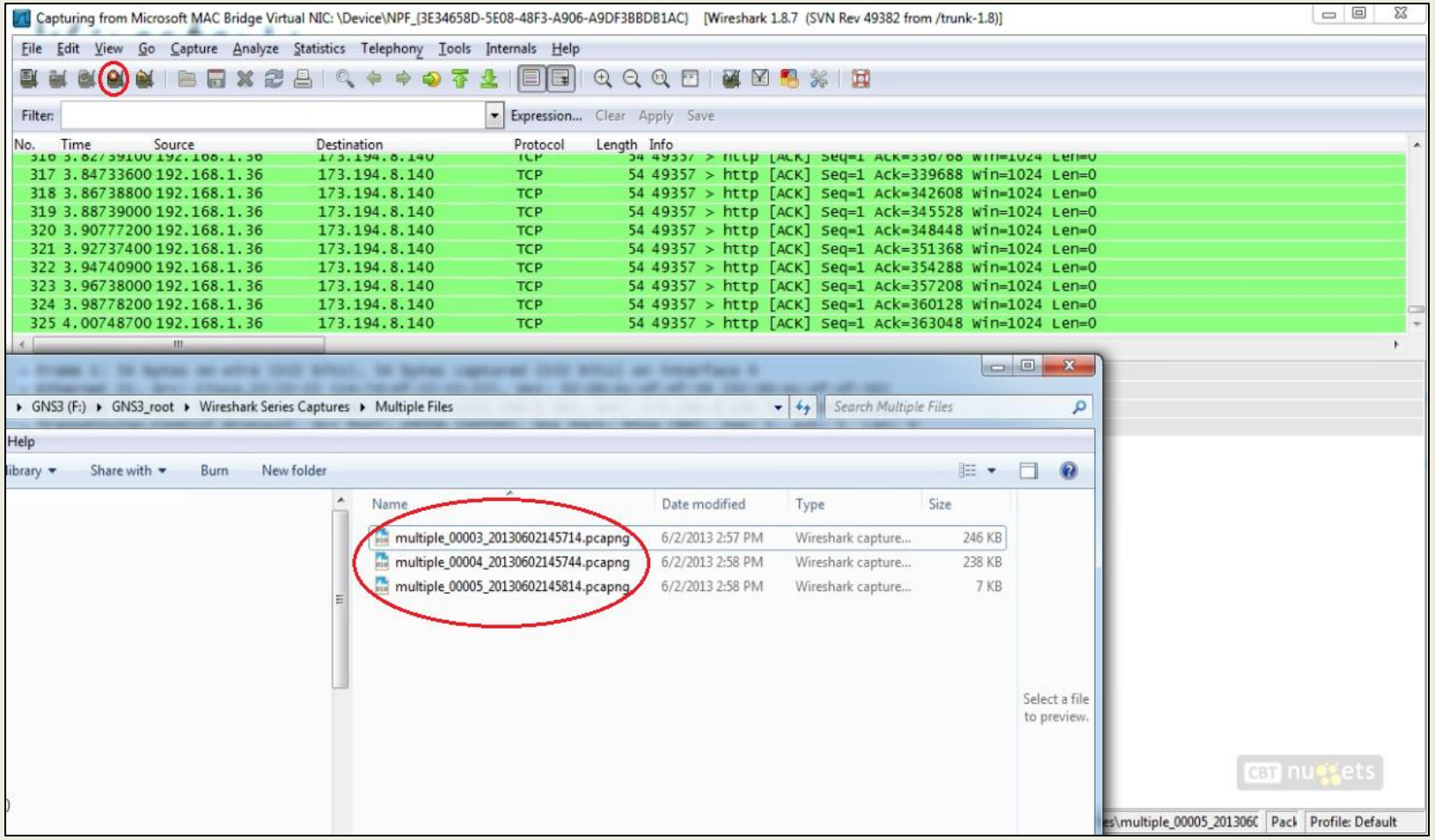


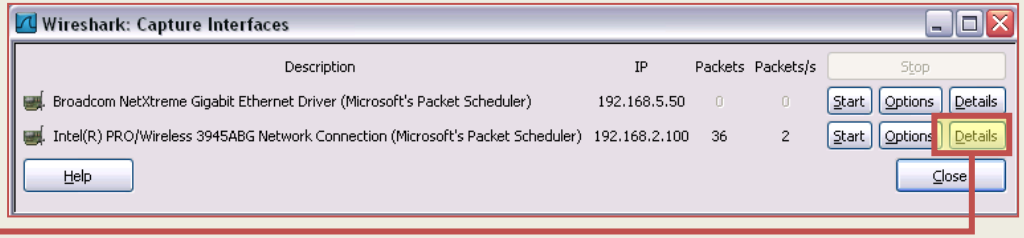
Use multiple files - Definisanje veličine fajlu:

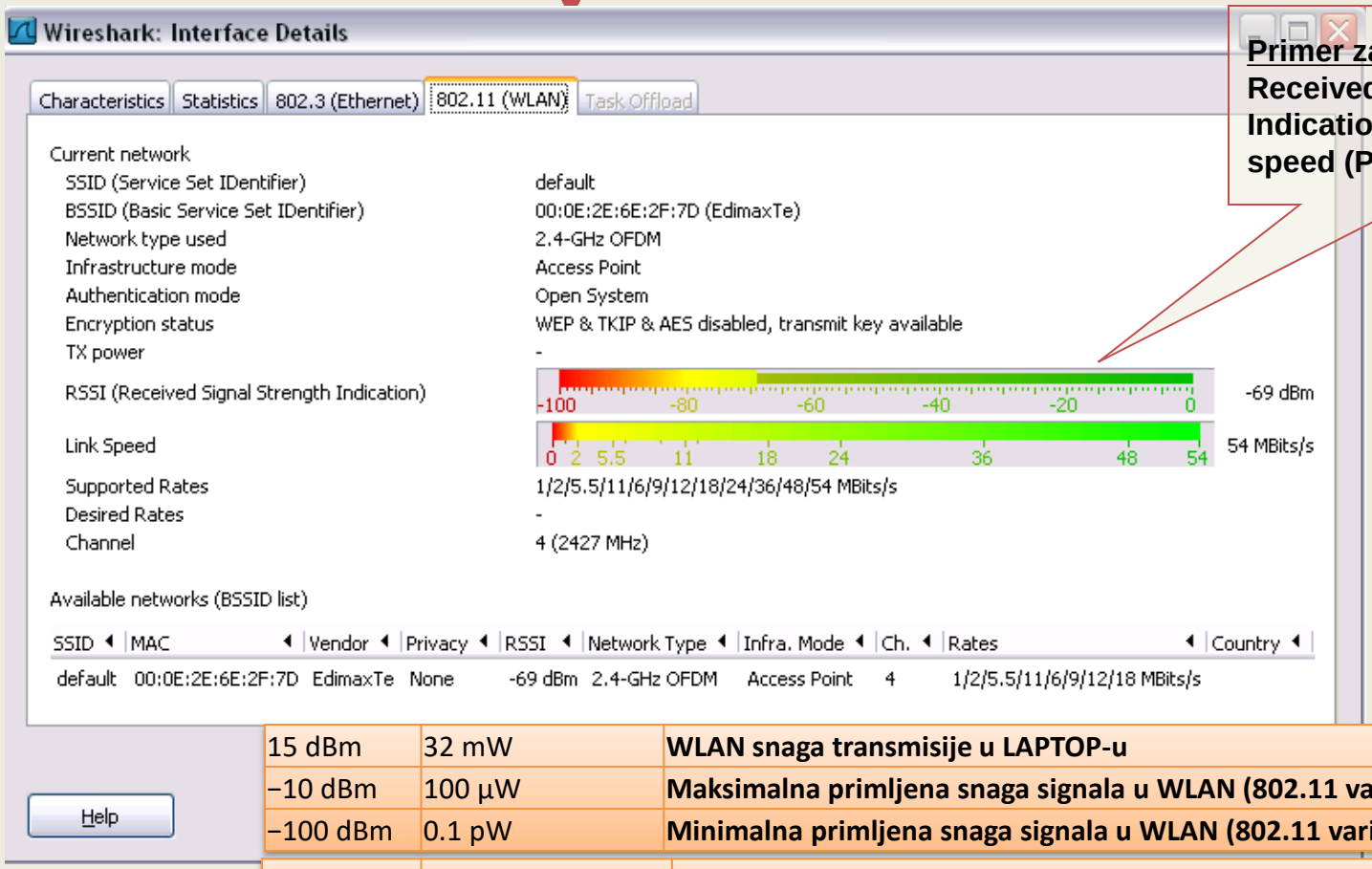
- **Kreiranje novog fajla**
  - kada fajl predje 10 MB vrši se automatsko kreiranje novog (prvi će biti multiple 1, drugi - multiple 2, treći - multiple 3 itd, dok mi ne zaustavimo hvatanje podataka.
- **Vremensko kreiranje fajla**
  - kreiranje fajla svakih 30s uključujući i veličinu fajla do 10 MB.
- **Ring buffer with**
  - opcija npr. u ovom slučaju čuvanja zadnja 3 fajla.
- **Stop Capture after**
  - opcija koja nam omogućava stopiranje hvatanja (Capture) podataka nakon željenog broja paketa, veličine paketa u MB, određenog broja minuta (sekundi)…



- Nakon stopiranja hvatanja podataka - *Stop the running capture* (4 ikonica 2 red) , na slici su prikazani multiple_00003, multiple_00004 i multiple_00005.
- Sačuvana su samo tri zadnja fajla podataka po naredbi u programu, što znači da su multiple _00001 i multiple _00002 fajlovi odbačeni aktivacijom opcije *Ring buffer with (3 files).*



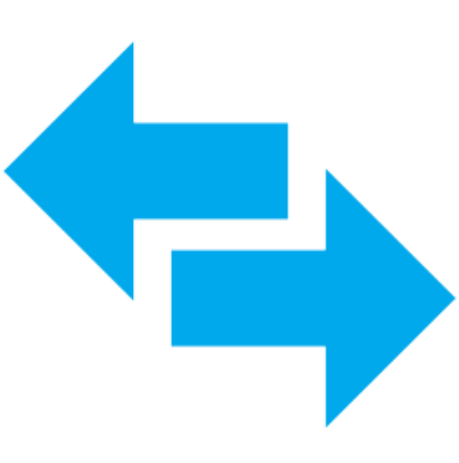




Primer za (W-LAN):
Received Signal Strength Indication (RSSI) i Link speed (Propusni opseg)

15 dBm	32 mW	**WLAN snaga transmisije u LAPTOP-u**
−10 dBm	100 µW	**Maksimalna primljena snaga signala u WLAN (802.11 variants)**
−100 dBm	0.1 pW	**Minimalna primljena snaga signala u WLAN (802.11 variants)**

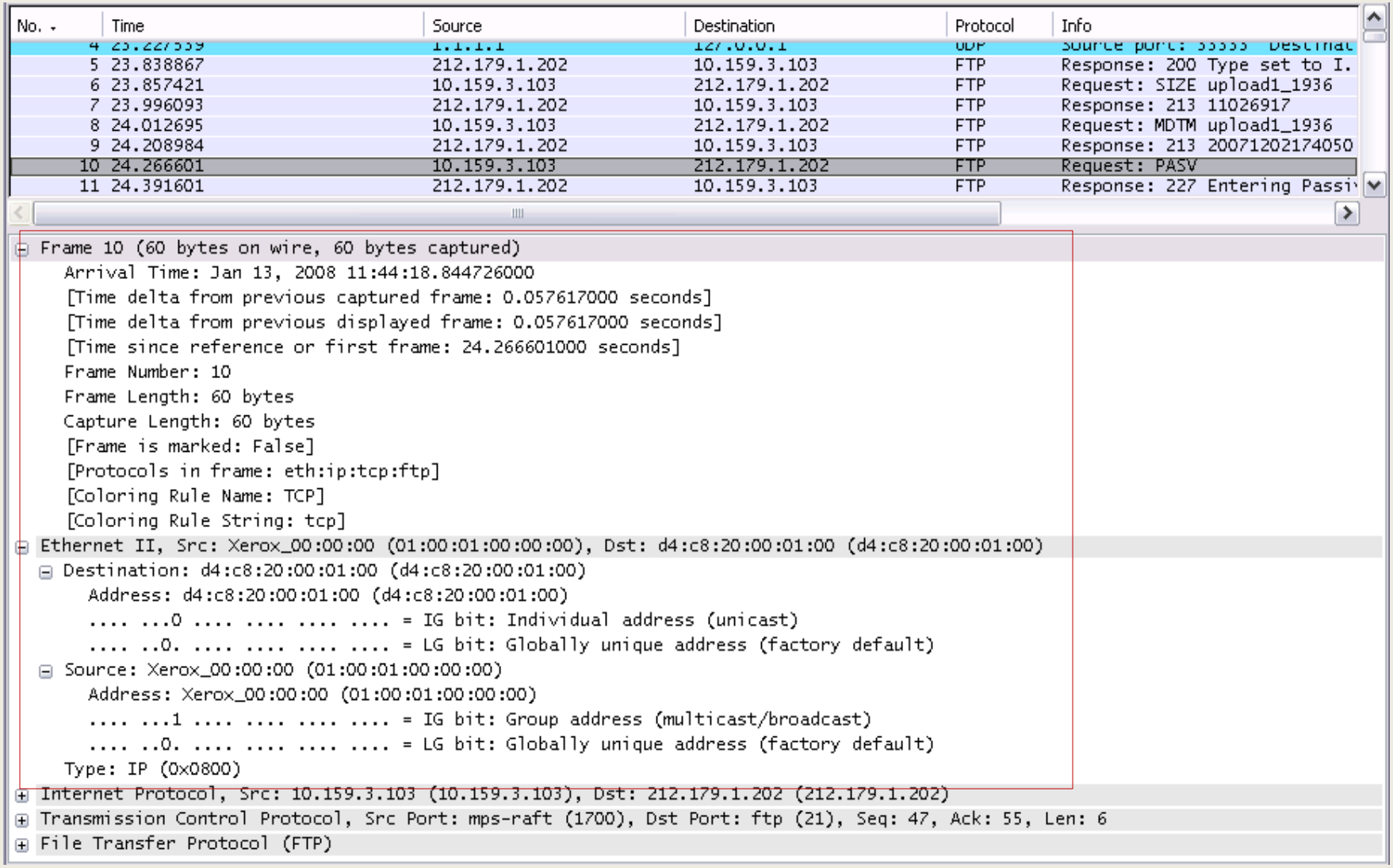
20 dBm	100 mW	**EIRP za IEEE 802.11b/g Wireless LAN 20 MHz-kanale na 2.4 GHz**



Poglavlje 3

Analiza paketa

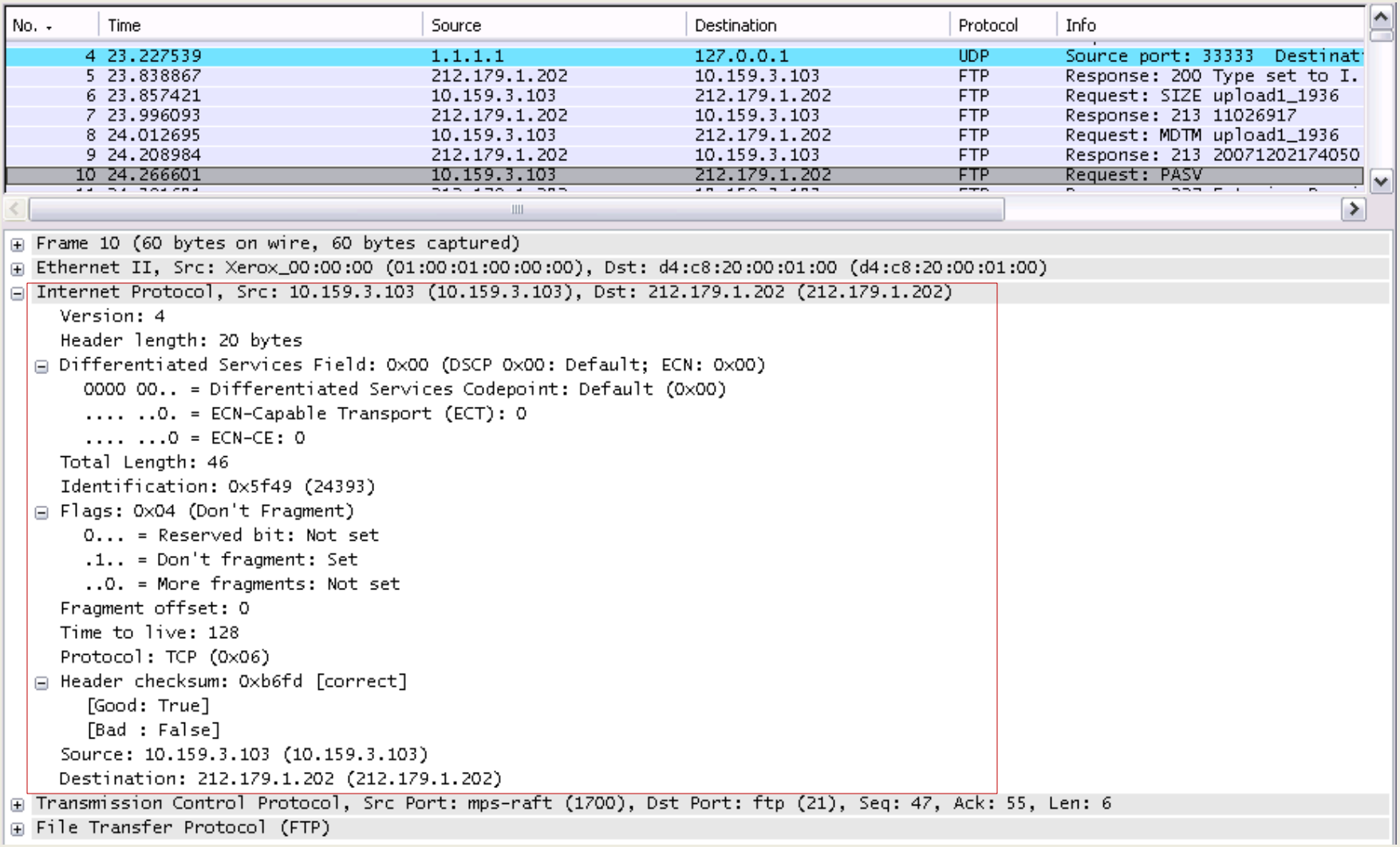
Primer ethernet frejma



No.	Time	Source	Destination	Protocol	Info
4	23.227339	1.1.1.1	127.0.0.1	UDP	Source port: 33333 Destinat
5	23.838867	212.179.1.202	10.159.3.103	FTP	Response: 200 Type set to I.
6	23.857421	10.159.3.103	212.179.1.202	FTP	Request: SIZE upload1_1936
7	23.996093	212.179.1.202	10.159.3.103	FTP	Response: 213 11026917
8	24.012695	10.159.3.103	212.179.1.202	FTP	Request: MDTM upload1_1936
9	24.208984	212.179.1.202	10.159.3.103	FTP	Response: 213 20071202174050
10	24.266601	10.159.3.103	212.179.1.202	FTP	Request: PASV
11	24.391601	212.179.1.202	10.159.3.103	FTP	Response: 227 Entering Passi

```
Frame 10 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Jan 13, 2008 11:44:18.844726000
    [Time delta from previous captured frame: 0.057617000 seconds]
    [Time delta from previous displayed frame: 0.057617000 seconds]
    [Time since reference or first frame: 24.266601000 seconds]
    Frame Number: 10
    Frame Length: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp:ftp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Xerox_00:00:00 (01:00:01:00:00:00), Dst: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)
  Destination: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)
      Address: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Source: Xerox_00:00:00 (01:00:01:00:00:00)
      Address: Xerox_00:00:00 (01:00:01:00:00:00)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 10.159.3.103 (10.159.3.103), Dst: 212.179.1.202 (212.179.1.202)
Transmission Control Protocol, Src Port: mps-raft (1700), Dst Port: ftp (21), Seq: 47, Ack: 55, Len: 6
File Transfer Protocol (FTP)
```

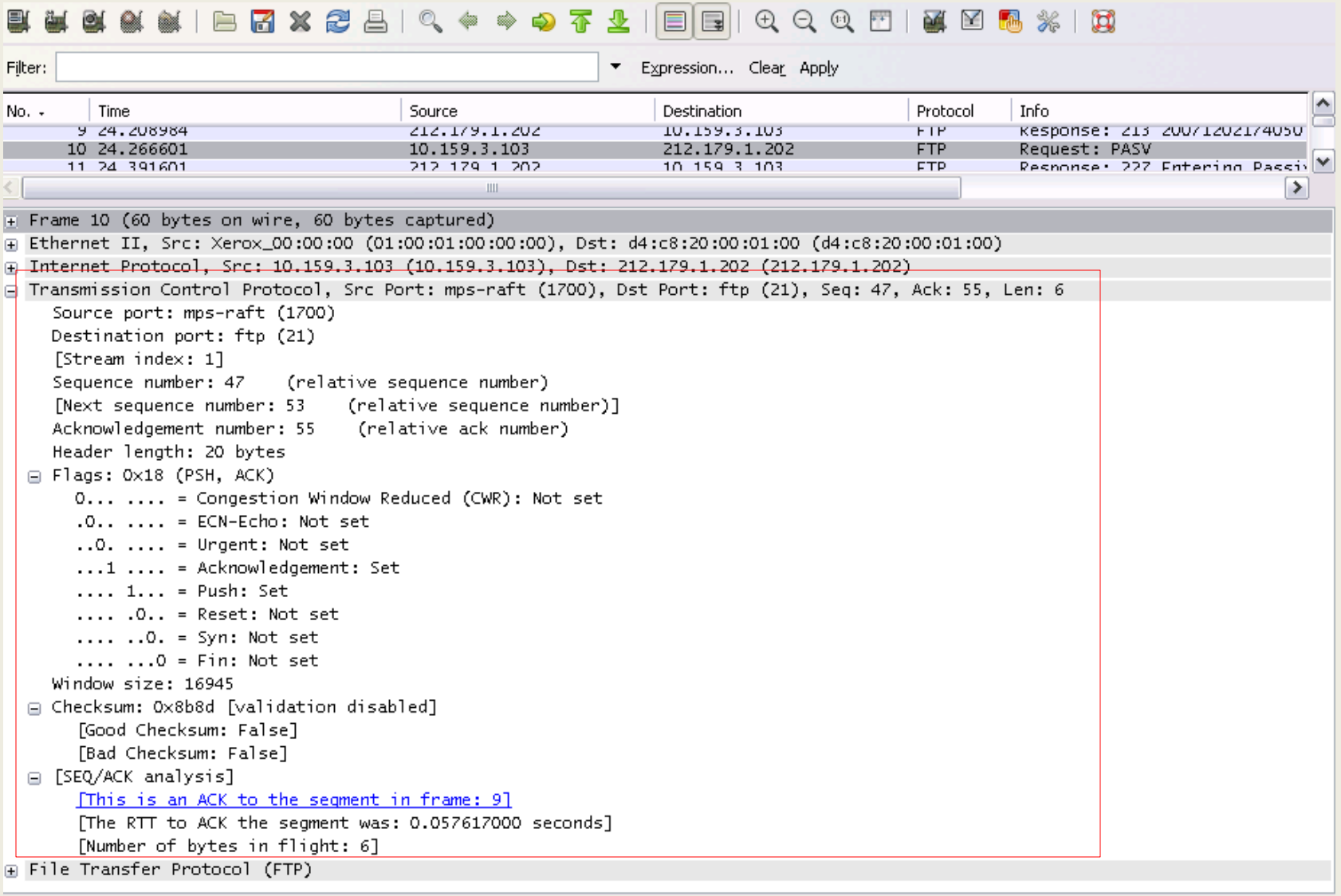
Primer IPv4 paketa



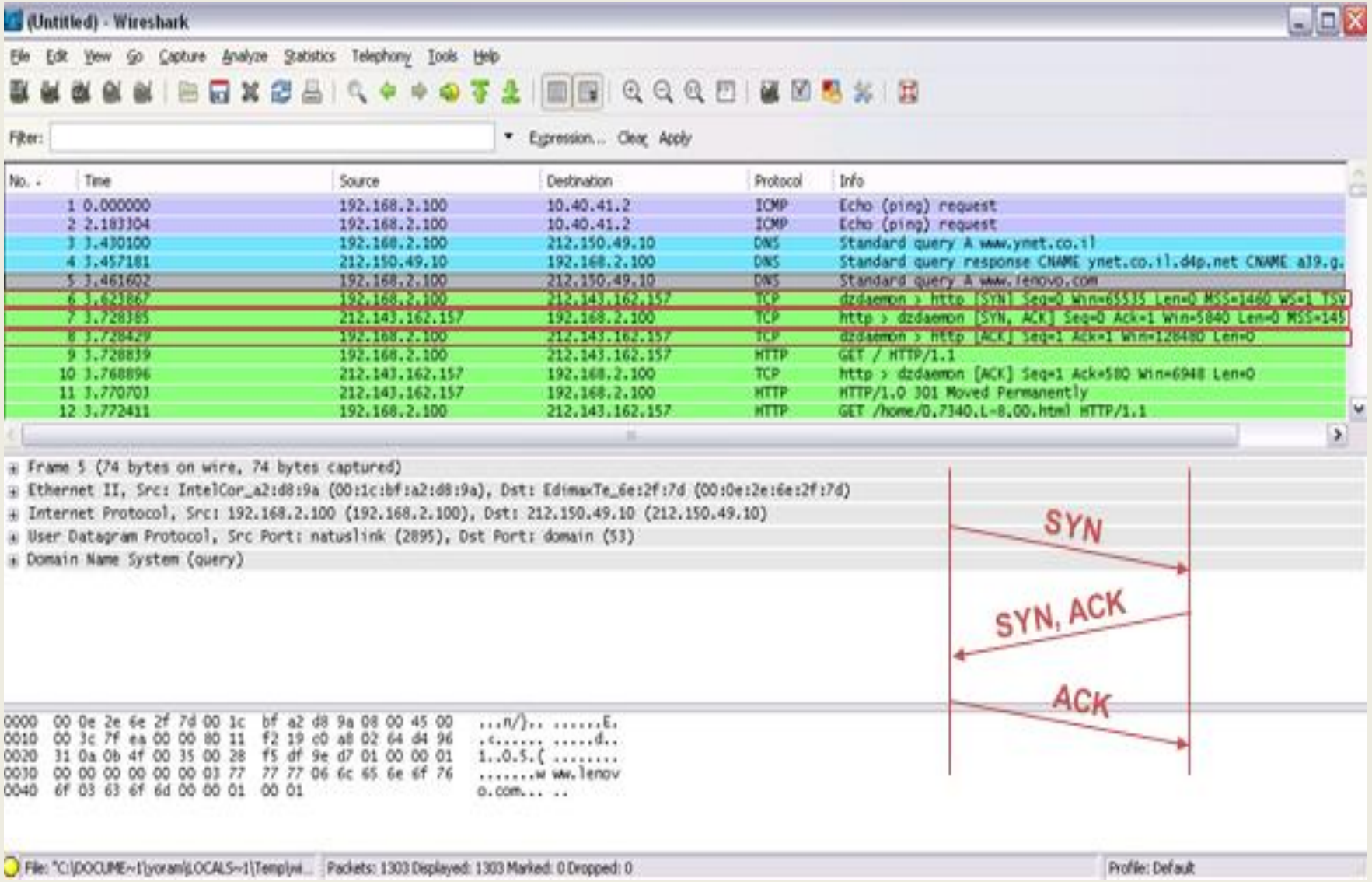
No.	Time	Source	Destination	Protocol	Info
4	23.227539	1.1.1.1	127.0.0.1	UDP	Source port: 33333 Destinat
5	23.838867	212.179.1.202	10.159.3.103	FTP	Response: 200 Type set to I.
6	23.857421	10.159.3.103	212.179.1.202	FTP	Request: SIZE upload1_1936
7	23.996093	212.179.1.202	10.159.3.103	FTP	Response: 213 11026917
8	24.012695	10.159.3.103	212.179.1.202	FTP	Request: MDTM upload1_1936
9	24.208984	212.179.1.202	10.159.3.103	FTP	Response: 213 20071202174050
10	24.266601	10.159.3.103	212.179.1.202	FTP	Request: PASV

```
⊞ Frame 10 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Xerox_00:00:00 (01:00:01:00:00:00), Dst: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)
⊟ Internet Protocol, Src: 10.159.3.103 (10.159.3.103), Dst: 212.179.1.202 (212.179.1.202)
    Version: 4
    Header length: 20 bytes
  ⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..0. = ECN-Capable Transport (ECT): 0
      .... ...0 = ECN-CE: 0
    Total Length: 46
    Identification: 0x5f49 (24393)
  ⊟ Flags: 0x04 (Don't Fragment)
      0... = Reserved bit: Not set
      .1.. = Don't fragment: Set
      ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
  ⊟ Header checksum: 0xb6fd [correct]
      [Good: True]
      [Bad : False]
    Source: 10.159.3.103 (10.159.3.103)
    Destination: 212.179.1.202 (212.179.1.202)
⊞ Transmission Control Protocol, Src Port: mps-raft (1700), Dst Port: ftp (21), Seq: 47, Ack: 55, Len: 6
⊞ File Transfer Protocol (FTP)
```

Primer TCP paketa

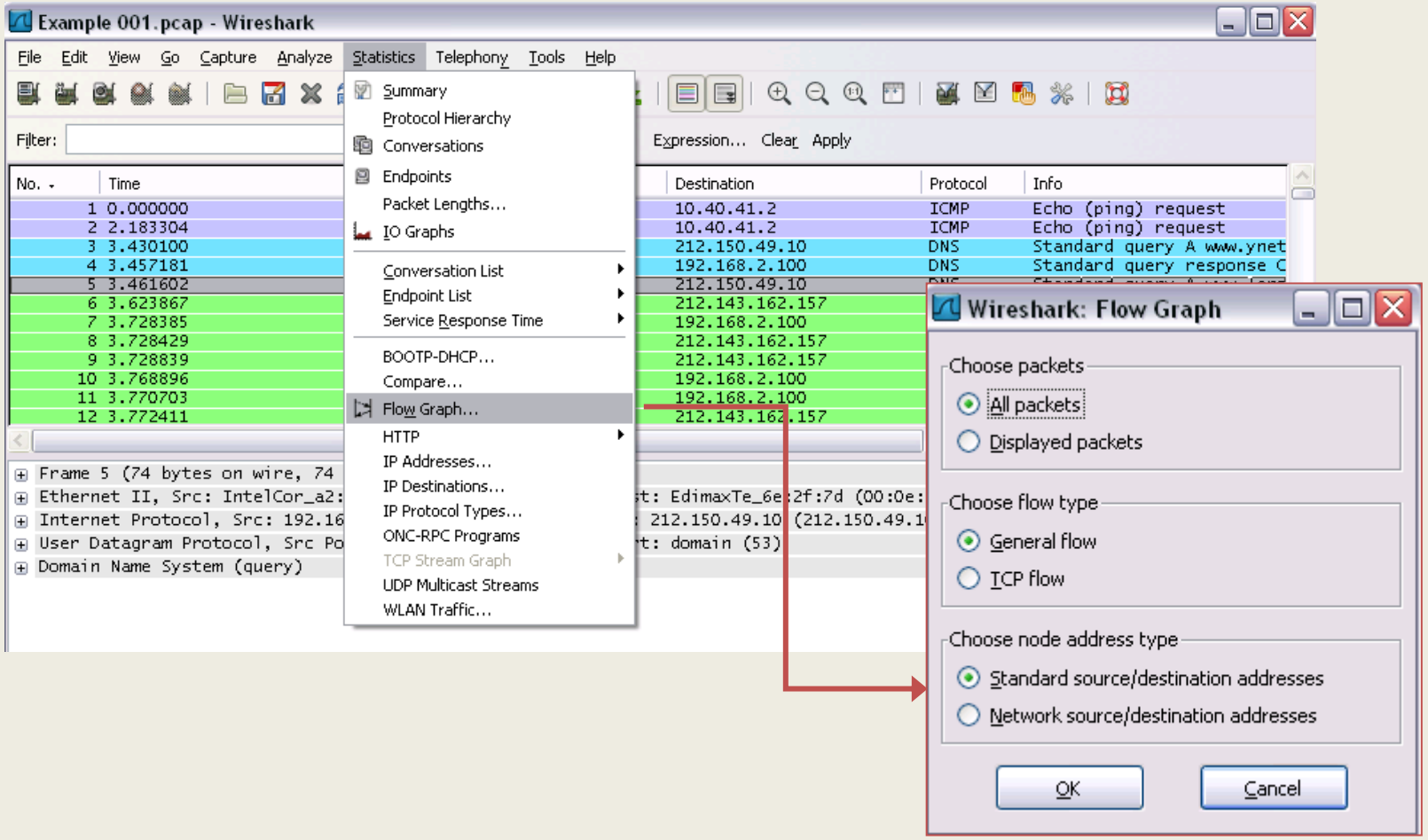


Primer TCP “Trostrukog rukovanja” (3-Way handshake)



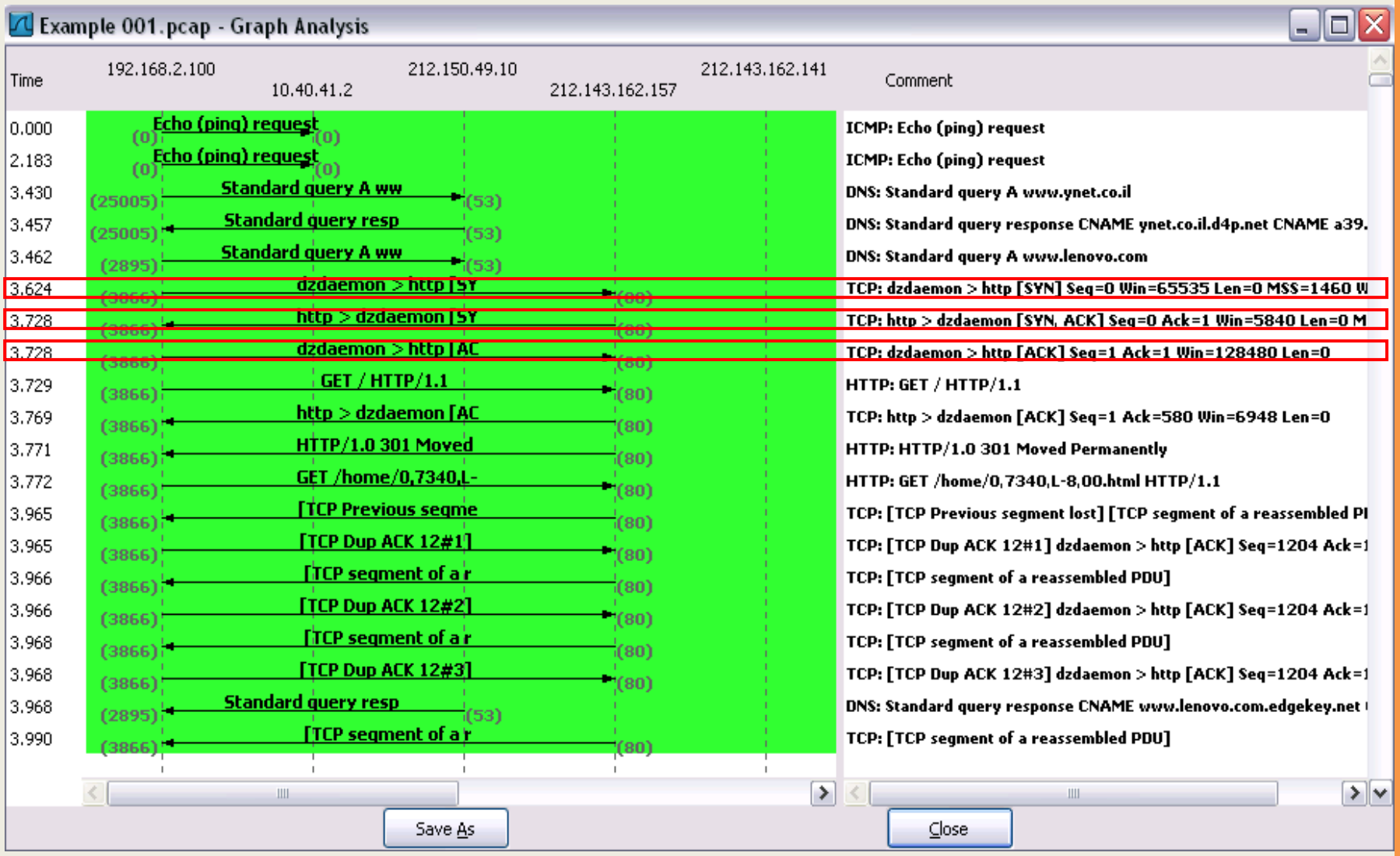
Grafik toka podataka

- Grafički prikaz toka podataka, za bolje razumevanje onoga što vidimo
- Flow Graph predstavlja sekvencijalnu analizu TCP konekcije.
- Može se odnositi na sve pakete ili samo na prikazane pakete.



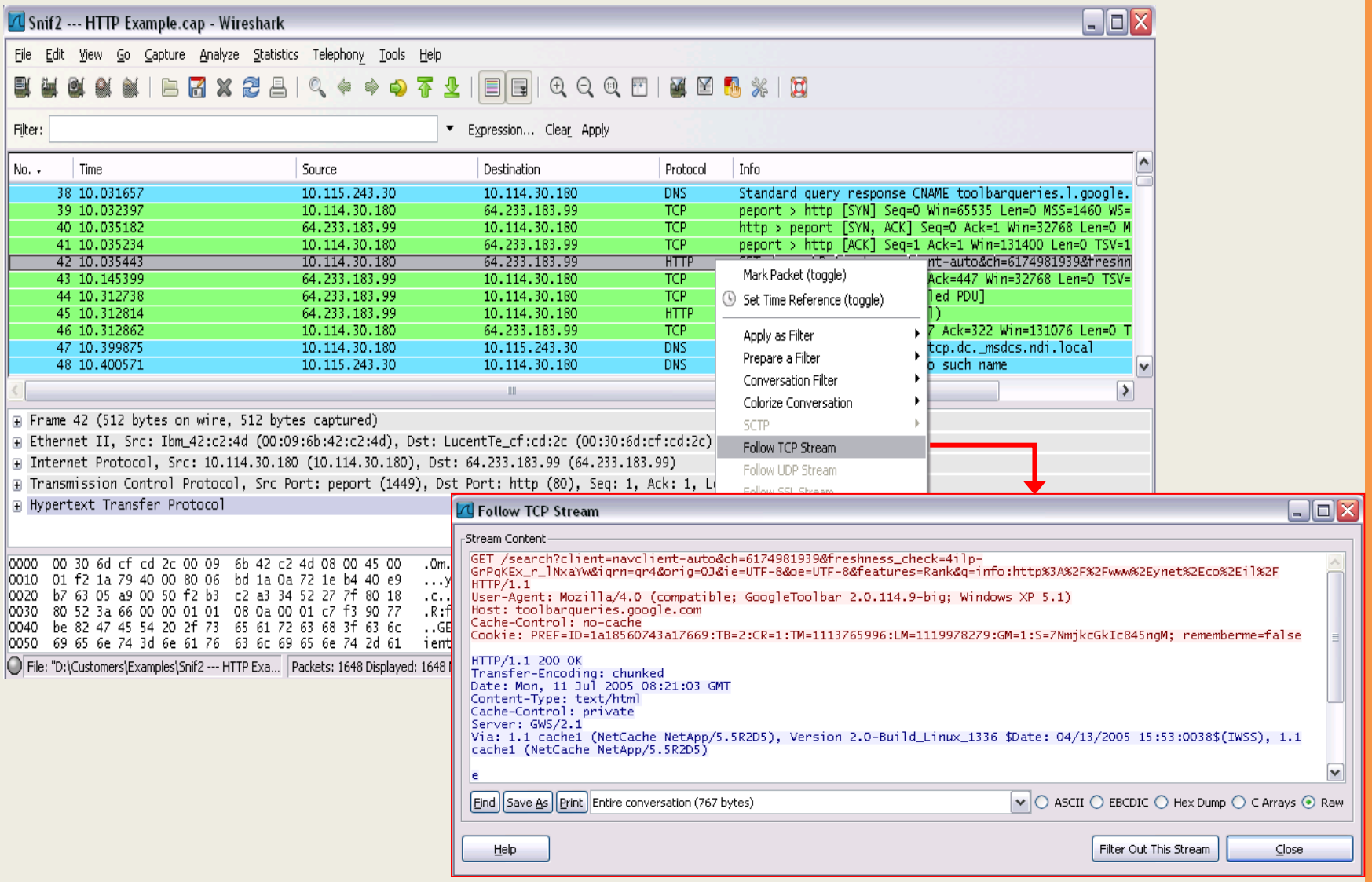
Grafik toka podataka

3-Way Handshake konekcija, grafički prikaz toka podataka.



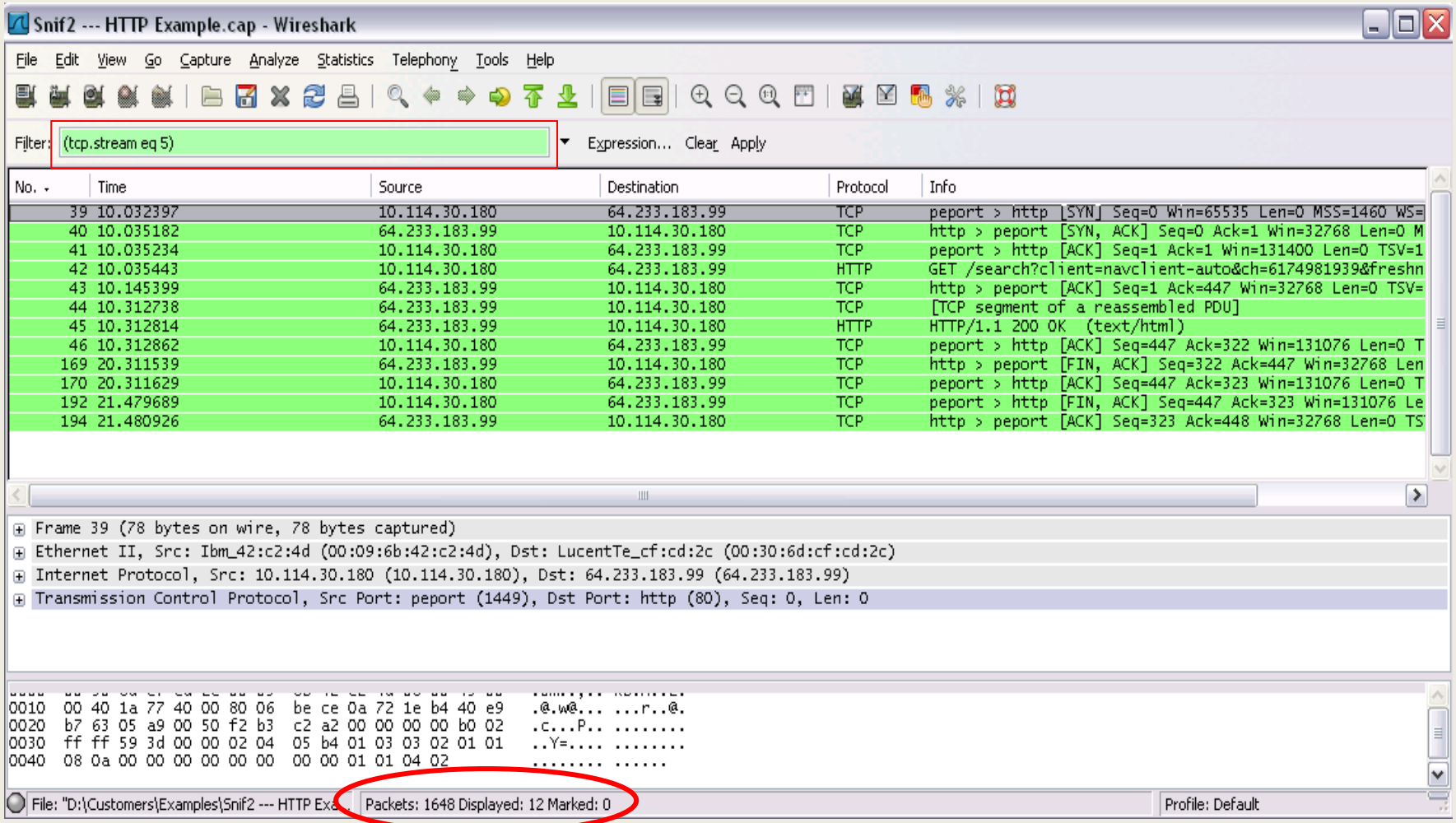
Prikaz TCP Stream-a

U realnom vremenu možemo tražiti od Wireshark-a da prikaže kompletan TCP prenos podataka između izvora i odredišta za željeni protokol na aplikativnom nivou



Prikaz TCP Stream-a

Filter ***tcp.strem eq 5*** označava peti zabeleženi stream od početka komunikacije.

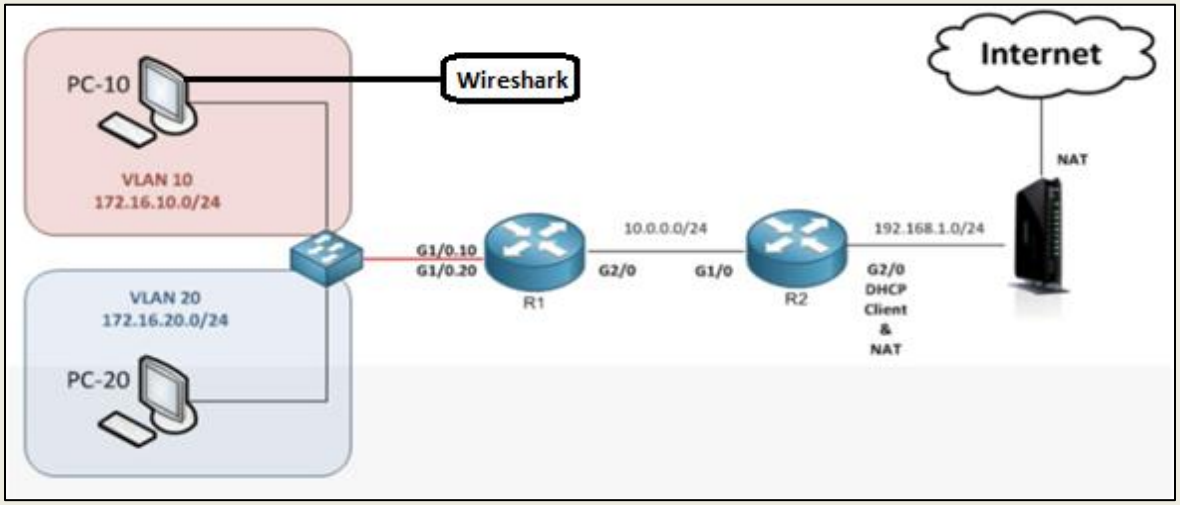


Poglavlje 4

Lokacija analizatora paketa

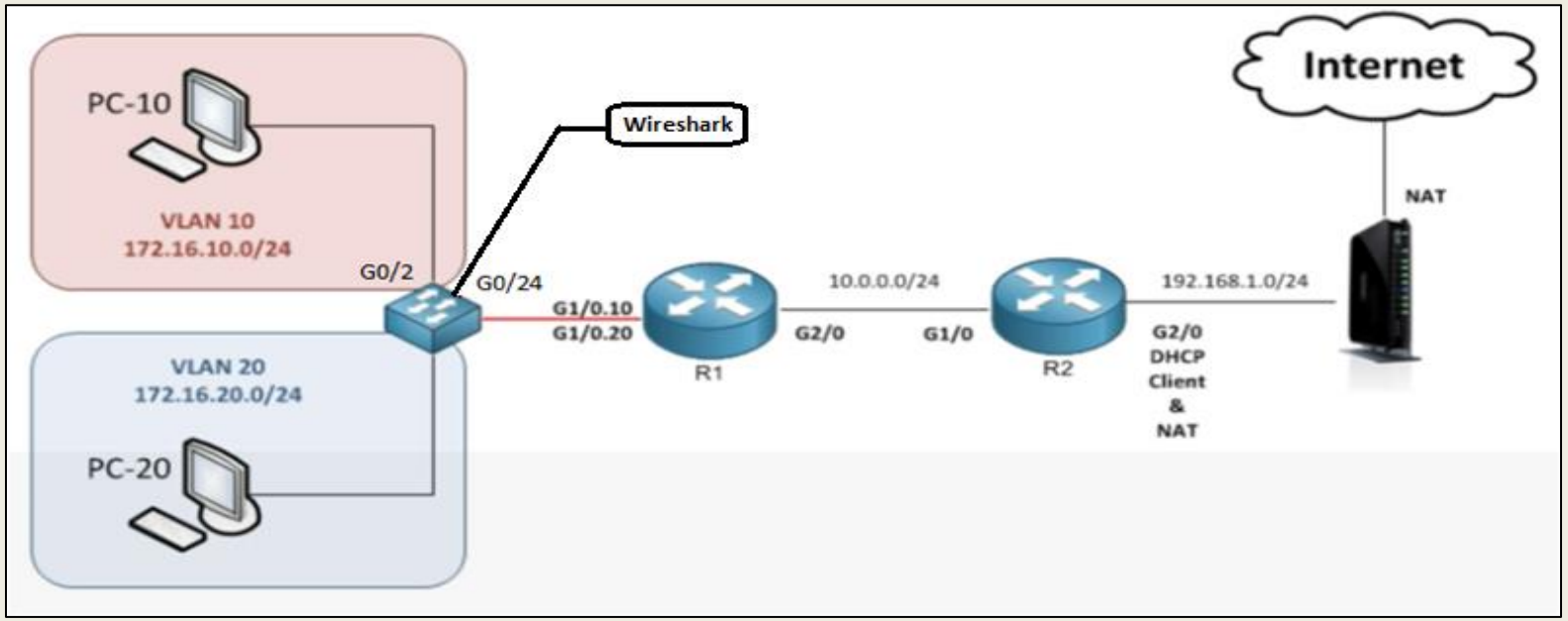
Controling The Capture - Kontrola uhvaćenih podataka

- Scenario 2 personalna računara PC-10, PC-20 ,Switch, R1 i R2 (rutere) i internet.
- Ako korisnik računara PC-10 želi da se konektuje na mrežu (Internet) i ima značajno veliko kašnjenje ili neki drugi problem, verovatno je da nećemo startovati hvatanje (Capture) podataka na segmentu PC-20, jer neće doći do hvatanja podataka.
- Moramo da znamo dostupne pozicije (lokacije) na kojima možemo da izvršimo kontrolu i hvatanje podataka:
- Ako pokušavamo da otkrijemo šta se događa sa korisnikom PC-10, možemo instalirati Wireshark na računaru PC-10 (istom računaru) i startovati hvatanje.



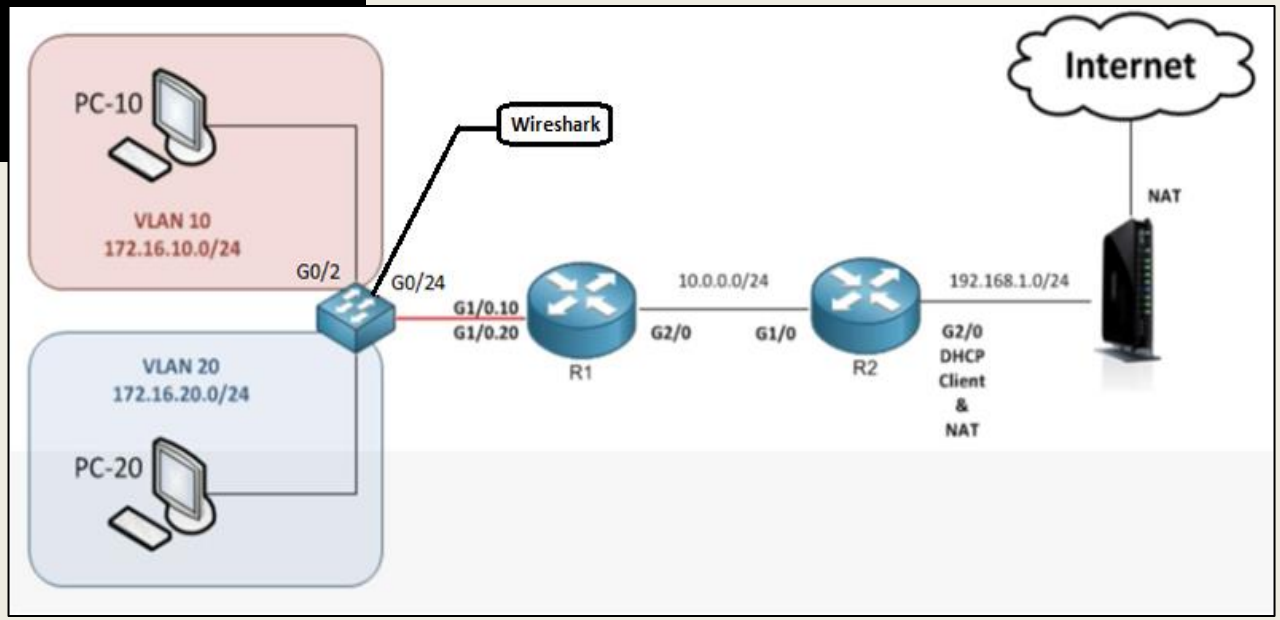
Port Mirroring

- Prethodna opcija nije jedina opcija za prihvatanje podataka na PC-10. Može se takođe izvršiti opcija Port Mirroring (koristi se na Switch-u da pošalje kopiju mrežnih paketa koje vidi sa jednog na drugi port), naravno ako Switch podržava ovu opciju.
- Ako imamo port G0/2 na koji je korisnik konektovan, i Wireshark kompjuter (Macintosh, Linux, Vindows) sa kojim je izvršena konekcija na port G0/24.
- Switch konfigurišemo da nam pošalje kopiju svih Frame-ova, podataka koji odlaze ili ulaze sa porta G0/2 na port G0/24.



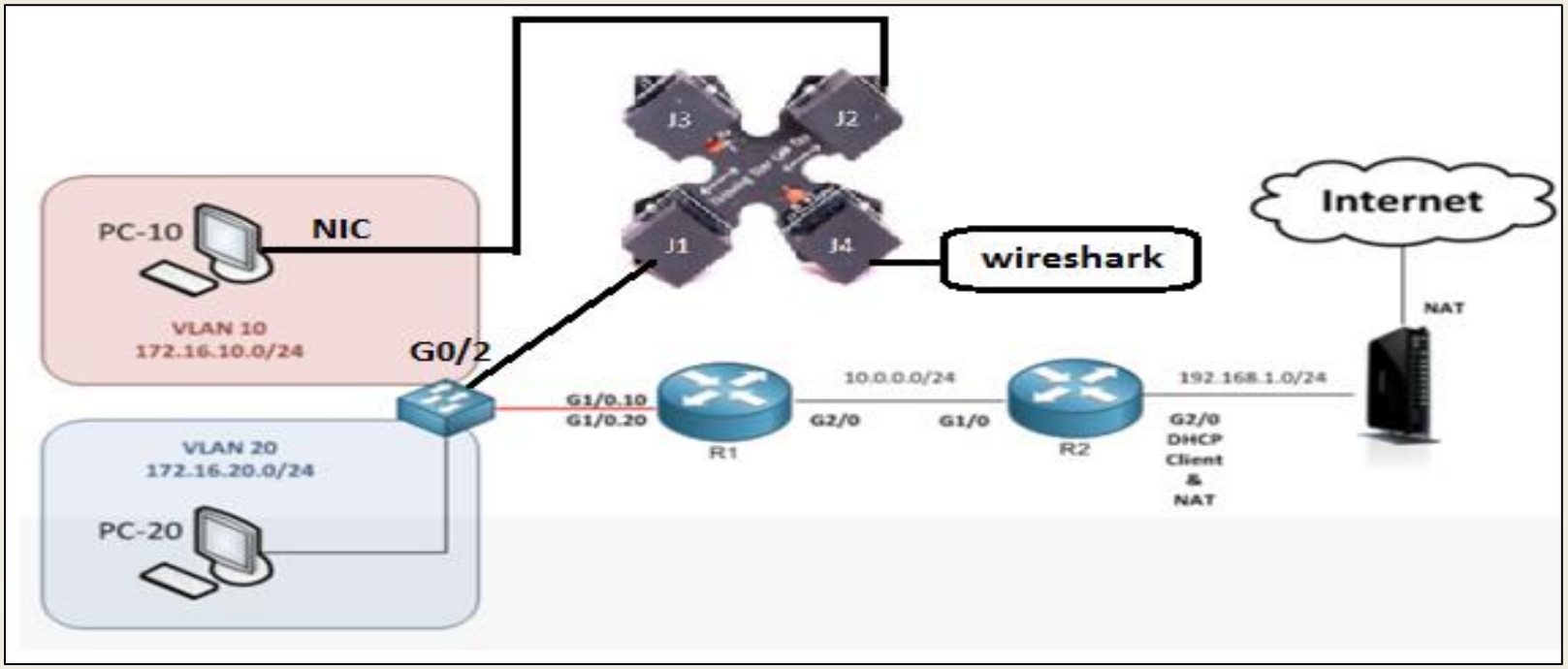
- U sledećem primeru prikazan je postupak podešavanja Port Mirroring-a na L3 Switch-u (3560 -Cisco Switch):
  - Monitor session 1 Source int g0/2 both
  - Monitor session 1 destination int g0/24

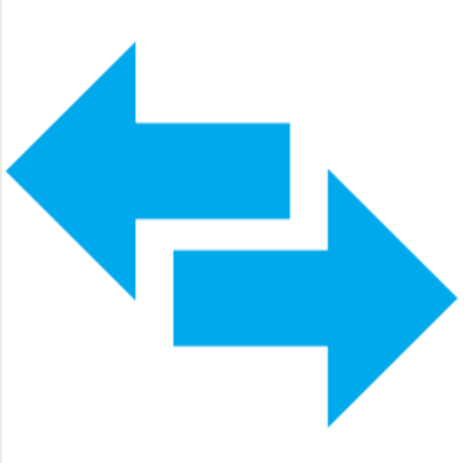
```
3560_Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
3560_Switch(config)#
3560_Switch(config)#monitor session 1 source int g0/2 both
3560_Switch(config)#
3560_Switch(config)#monitor session 1 destination int g0/24
3560_Switch(config)#
3560_Switch(config)#
3560_Switch(config)#do show monitor
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Gi0/2
Destination Ports      : Gi0/24
    Encapsulation      : Native
          Ingress      : Disabled


3560_Switch(config)#
```



Tap (internet TAP) :

- Ako Switch ne podržava Port Mirroring funkciju postoji i opcija Tap (Internet TAP). Prikazan je TAP sa 4 konektora :
- Vrši se konekcija kabla iz NIC (Network Interface Card) mrežne kartice na port npr J2, a iz Switch-a (G0/2) vrši se konekcija na port (ulaz) J1, što znači da će TAP biti u sredini između PC-10 i Switch-a.
- Celokupni saobraćaj između PC-a i Switch-a koji prolazi kroz TAP može da se vidi sa bilo kog drugog uređaja priključenog npr. na port J4 (Wireshark).





Poglavlje 4

Filtriranje paketa

Osobine Display Filtra

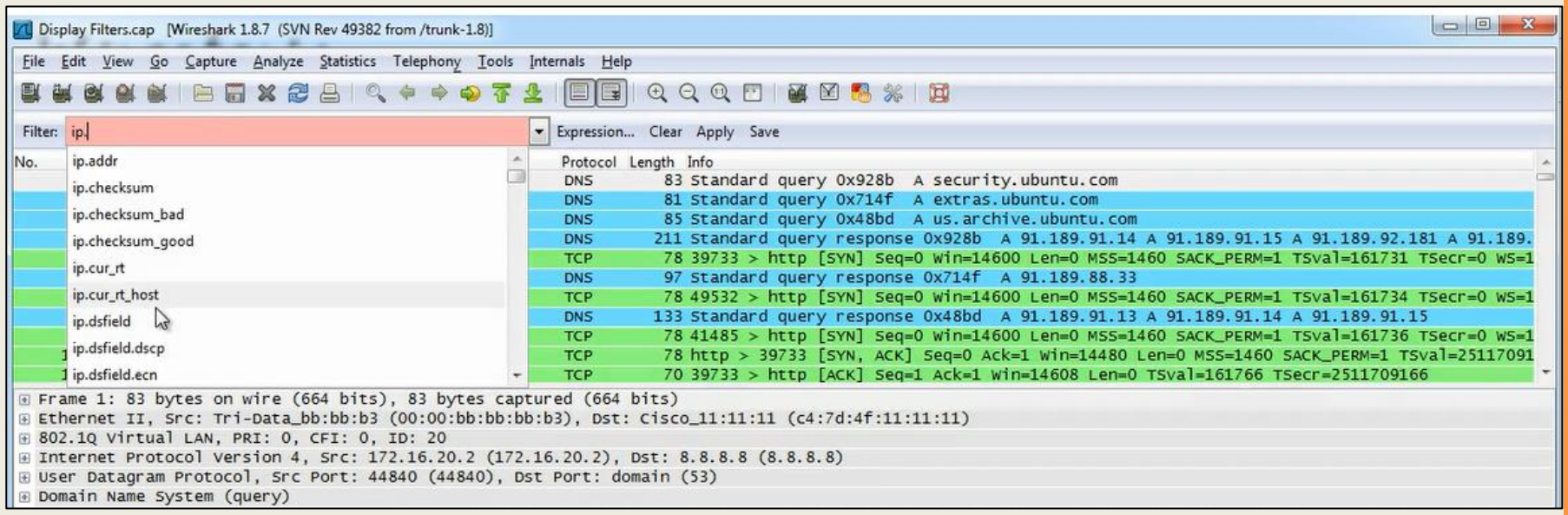
- Snimanje fajlova može biti velike sadržine i imati na hiljade razgovora u mreži
- Koristeći **Display Filter** u **WireShark** možemo da odredimo koji paket da se prikaže, što nam pomaže da se fokusiramo na određeni prenos (saobraćaj).
- Mogu se filtrirati protokoli, aplikacije, adrese itd.
- Koristimo operator (sa različitim komandama) kojim određujemo na koji način radimo filtriranje.

	Komanda	Komanda	Primer
Jednako	eq	==	ip.dst==a.b.c.d
Ne jednako	ne	!=	udp.dstport !=53
Manje od	lt	<	ip.ttl < 45
Veće ili jednako	ge	>=	tcp.analysis.bytes_in_flight >= 1000
Sadržaj	contains		dns.resp.name contains google

Primena Display filtra

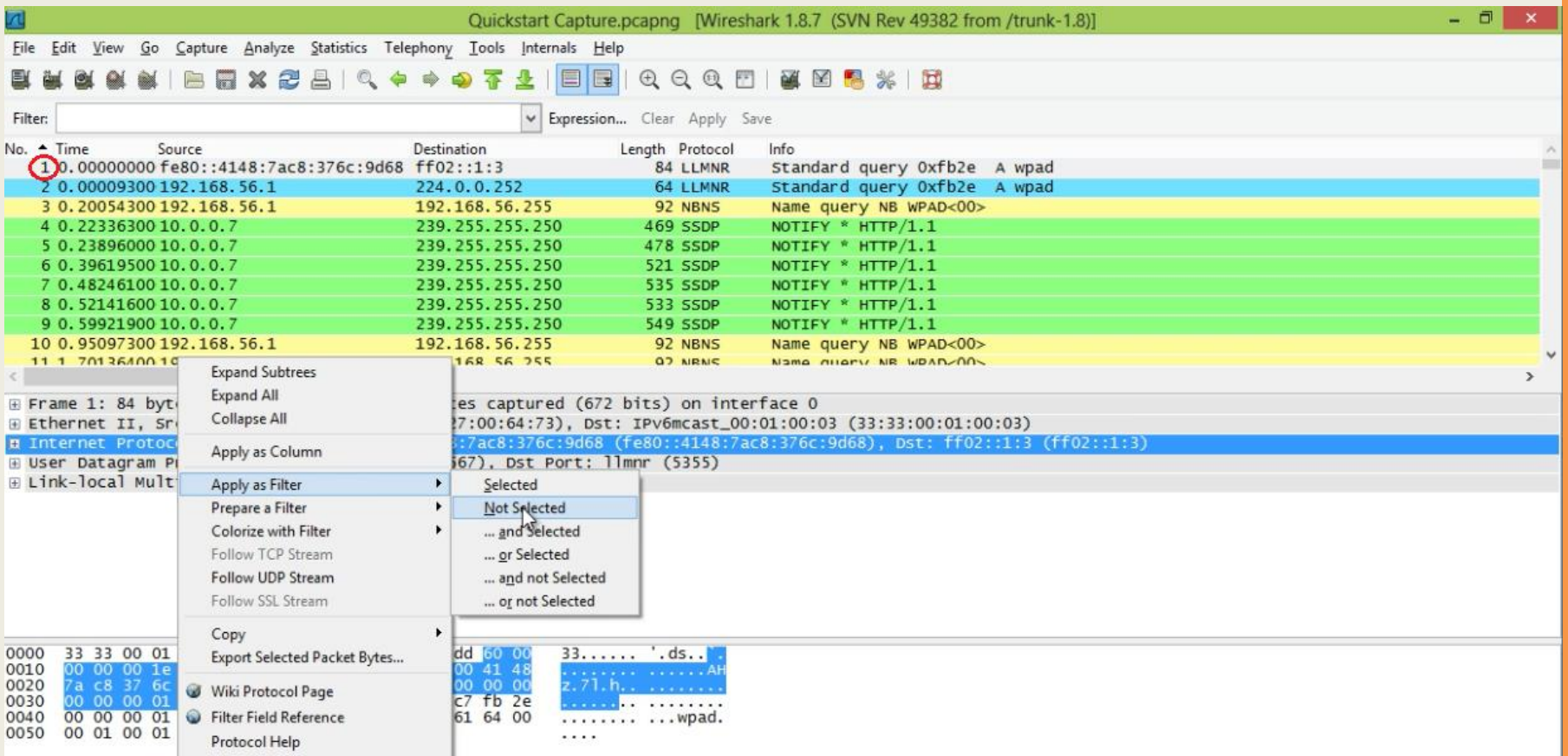
- U zavisnosti da li tražimo neku ip adresu ili bilo koji drugi parametar po kom želimo da radimo filtriranje, u zaglavlju za filtriranje se kuca, i može se pojaviti više opcija u zavisnosti od potrebe filtriranja.
- Kucanjem > **ip.**< filter je pronašao više mogućnosti, kao što su:

  >**ip.addr**<,>**ip.checksum**<,>**ip.cur_rt**< …

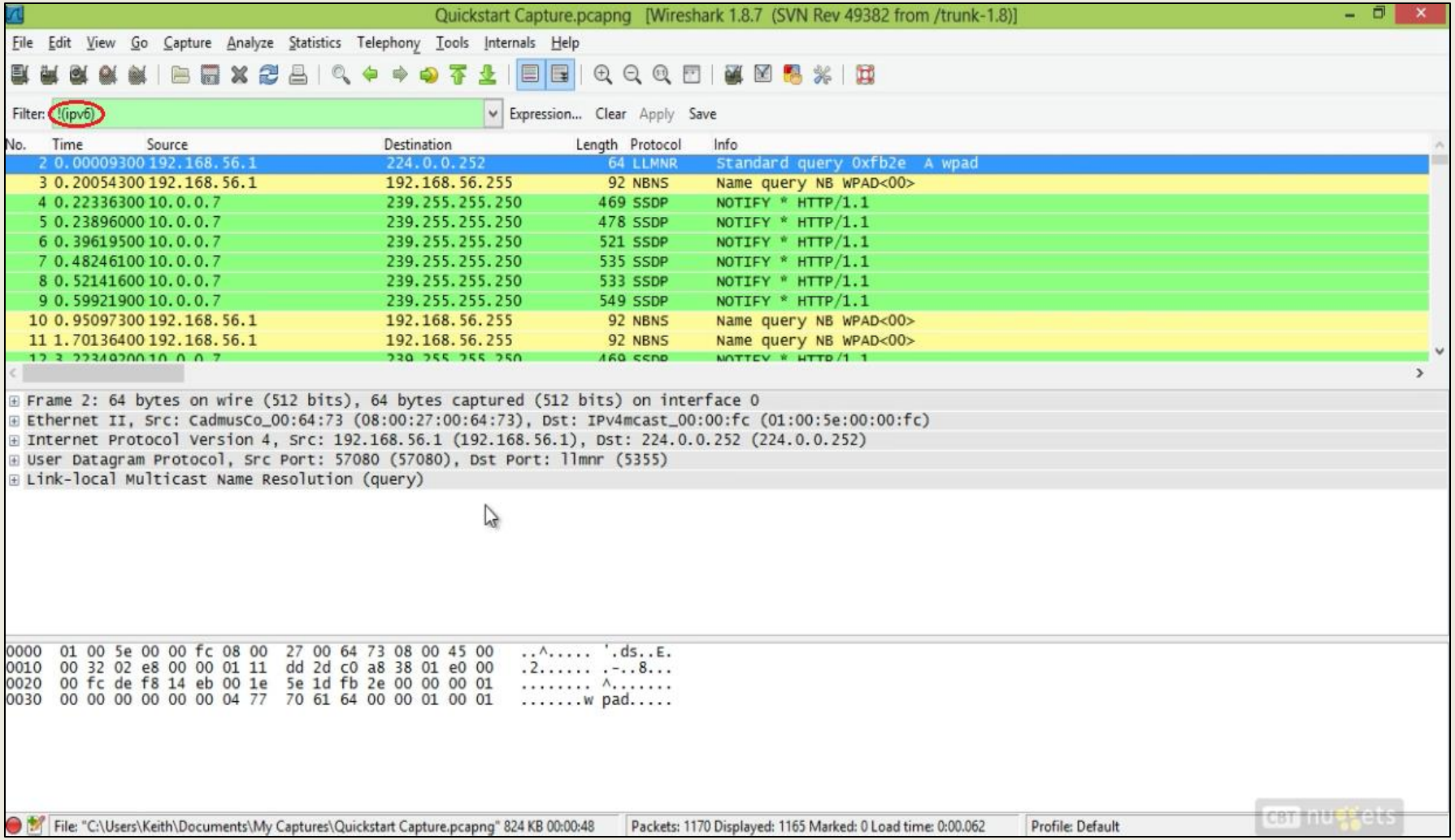


Add Display Filter – kreiranje Display Filtra

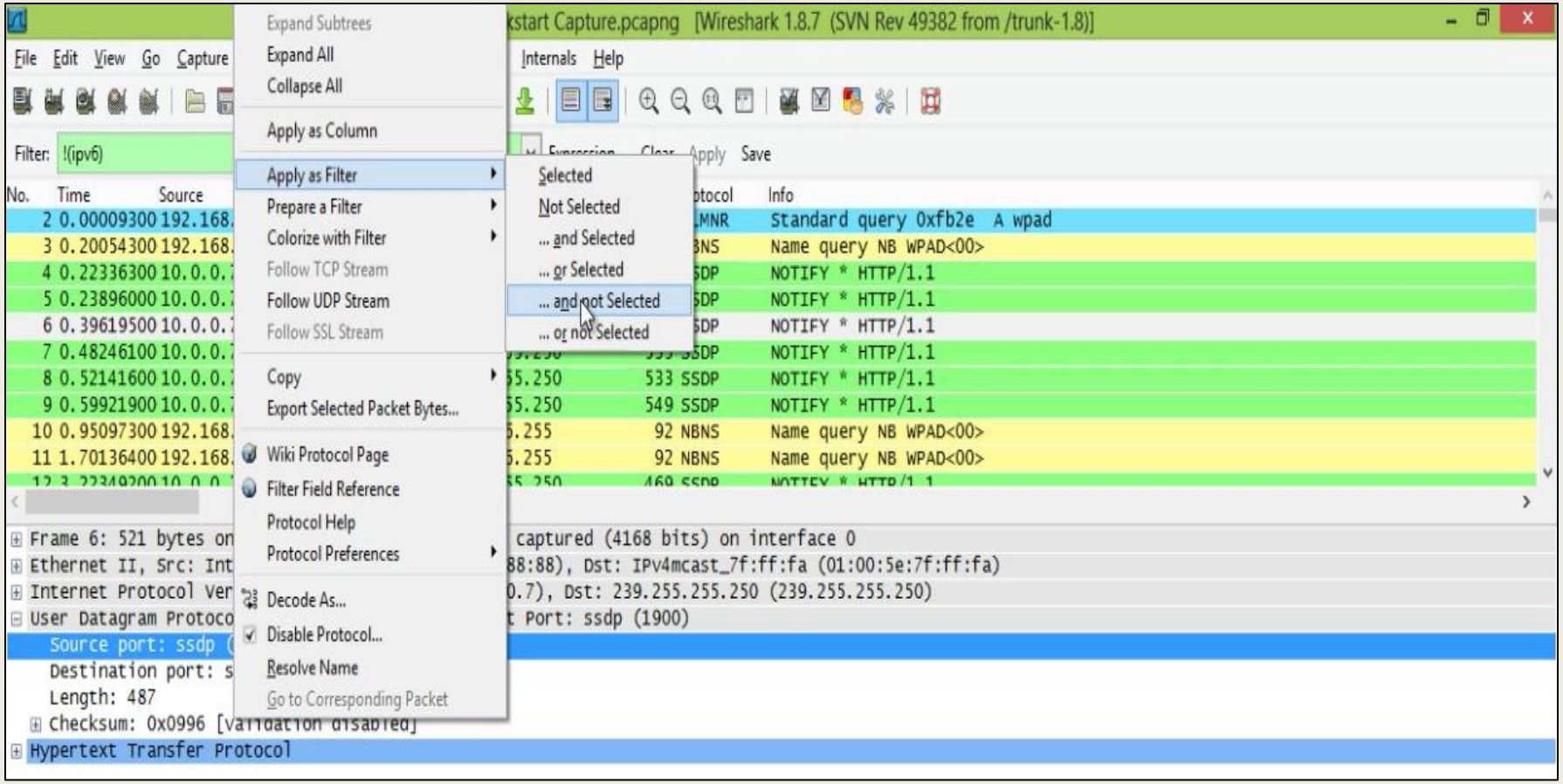
- Prikazuje pakete na osnovu unetog kriterijuma ali ne odbacuje pakete
- Prvi paket je ipv6 (Internet Version Protocol 6) koga ne želimo da uzmemo u obzir za analizu.
- Izaberemo ipv6 u Packet Details Pane-u (desni klik) zatim na opciju Apply as filter - **Not selected**.



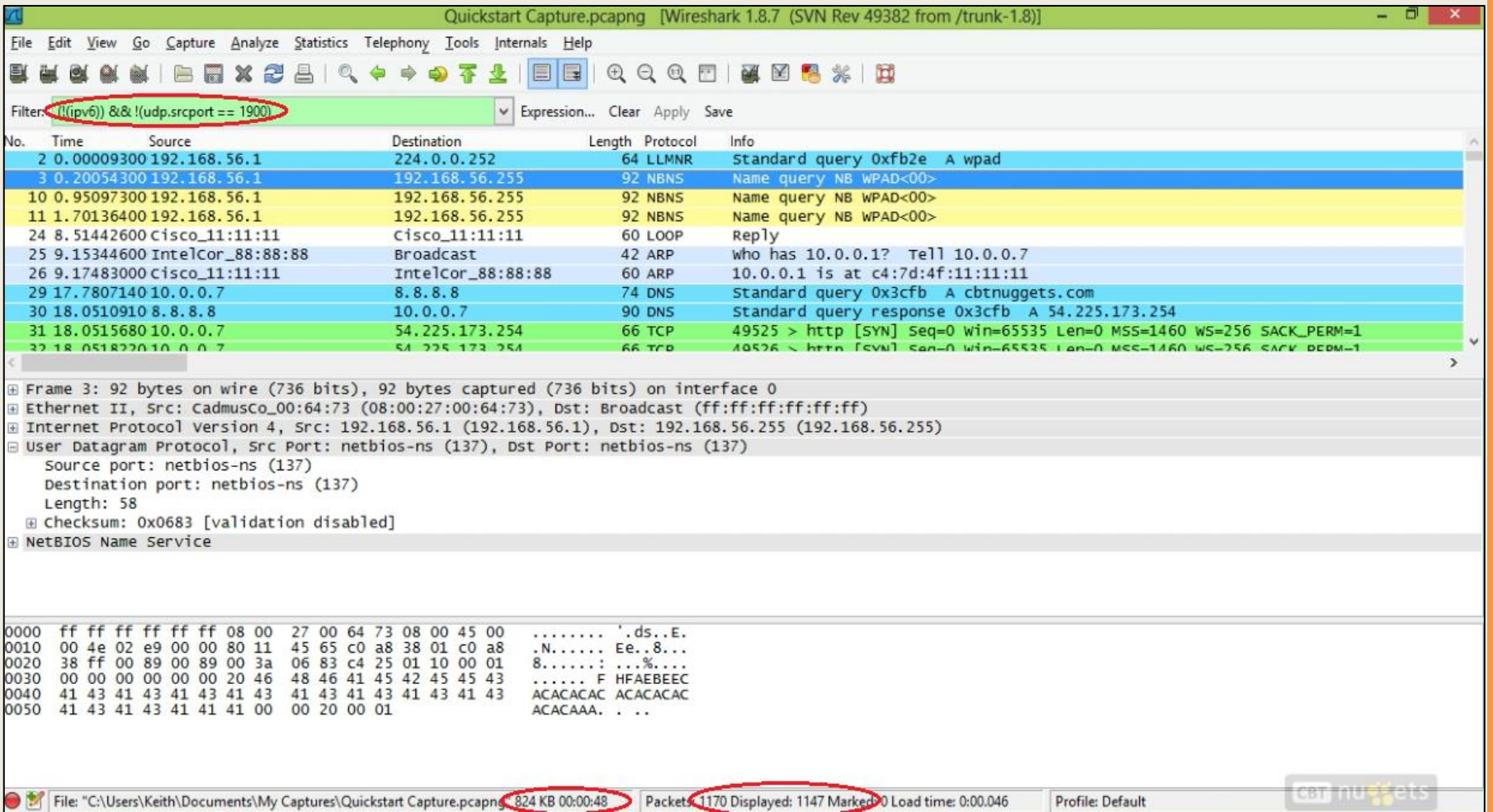
- Nakon selektovanja opcije **Apply as filter - Not selected**, uočava se izostanak 1 paketa u Packet List Pane-u, odnosno u Display Filter-u izostavlja se prikaz ipv6 protokola (sve osim ipv6 protokola biće prikazano).
- Ovo je jedan od najlakših načina za kreiranje filtra.



- Pored paketa vezanih za ipv6 protokol želimo da izostavimo analiziranje i ssdp paketa.
- Proširenjem User Datagram Protocol-a i odabiranjem izvršnog porta source port : ssdp (1900), kao i odabiranjem opcije (desni klik) - and not selected.

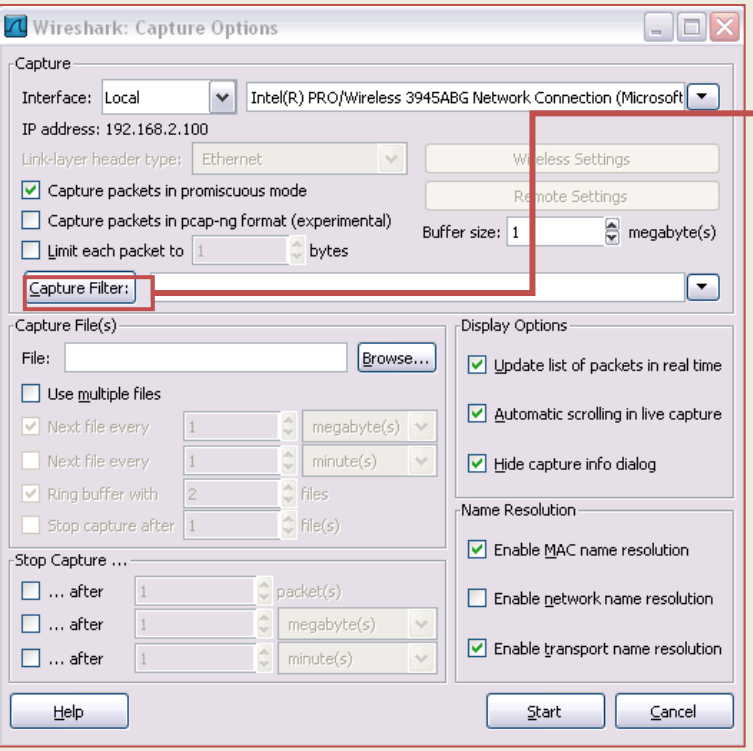


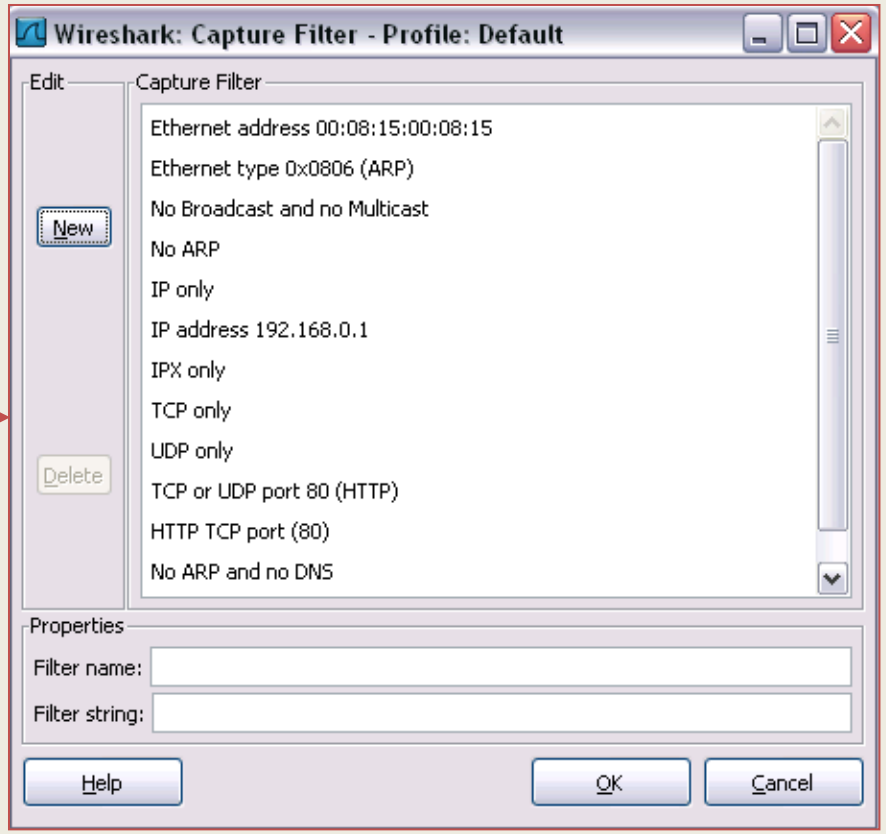
- U polju filter imamo izostavljene pakete vezane za ipv6 i ssdp protokole.
- Selektovanjem paketa npr, broj 3 može se baciti pogled na Status bar.
- Status Bar daje informacije o paketu sa kojim se radi trenutno, kao što su veličina paketa od 824 KB, 1170 paketa uhvaćenih podataka, trenutno prikazanih 1147 paketa



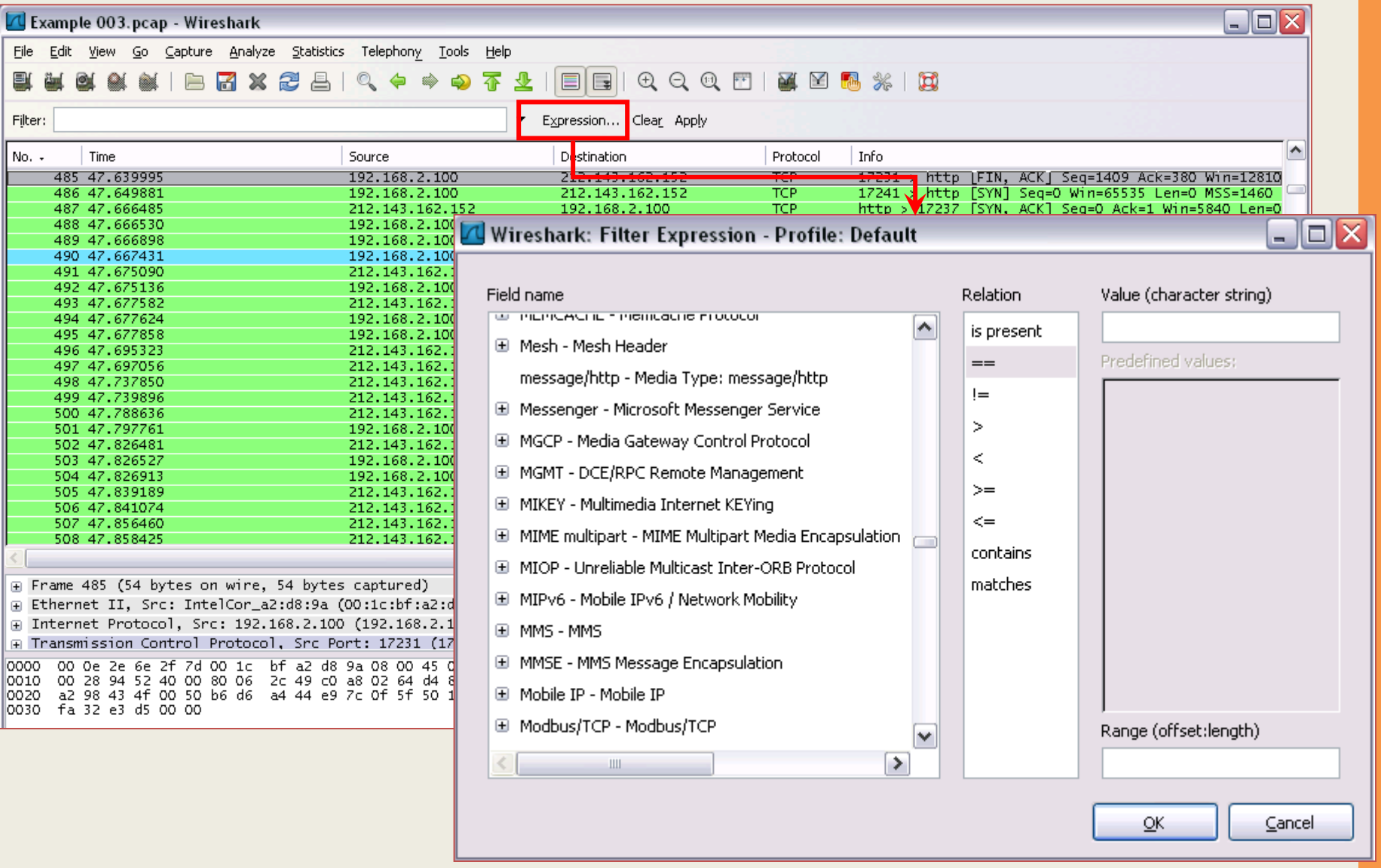
Izbor dostupnih filtera

Capture → Interfaces → Options:





Primena filtera (ekspresija)



Primeri :

- ✓ Snimanje saobraćaja iskuljučivo sa adrese 172.18.5.4
  - host 172.18.5.4
- ✓ Snimanje saobraćaja iskuljučivo iz konkretnog opsega IP adresa
  - net 192.168.0.0/24
  - net 192.168.0.0 mask 255.255.255.0
- ✓ Snimanje saobraćaja source opsega IP adresa
  - src net 192.168.0.0/24
  - src net 192.168.0.0 mask 255.255.255.0
- ✓ Snimanje saobraćaja destination opsega IP adresa
  - dst net 192.168.0.0/24
  - dst net 192.168.0.0 mask 255.255.255.0
- ✓ Snimanje isključivo DNS (port 53) saobraćaja
  - port 53
- ✓ Snimanje non-HTTP i non-SMTP saobraćaja na serveru
  - host www.vtsnis.edu.rs and not port 80 or port 25
  - host www.vtsnis.edu.rs and not port 80 and not port 25

Primeri :

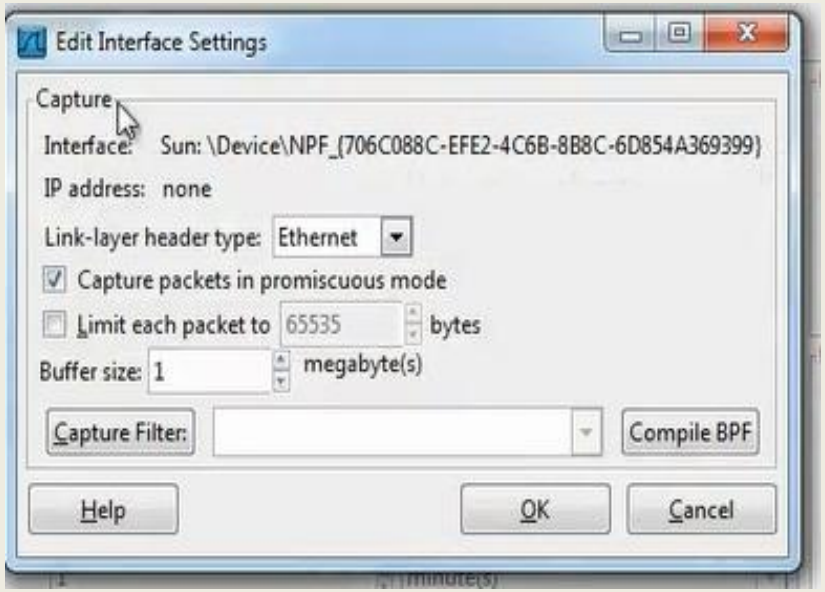
- ✓ **Snimanje svega osim ARP i DNS saobraćaja**
  - **port not 53 and not arp**
- ✓ **Snimanje saobraćaja u opsegu određenih portova**
  - **(tcp[2:2] > 1500 and tcp[2:2] < 1550) or (tcp[4:2] > 1500 and tcp[4:2] < 1550)**
  - **tcp portrange 1501-1549**
- ✓ **Snimanje isključivo IP saobraćaja**
  - **(najkraći filter ali veoma koristan kada nam nije neophodan prikaz ARP i STP protokola) - IP**
- ✓ **Snimanje isključivo unicast saobraćaja**
  - **not broadcast and not multicast**

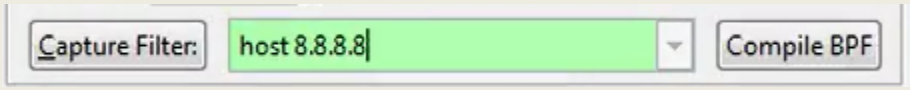
Capture Filter

- Kada postoje podaci u gigabajtima koji prolaze kroz mrežu, i potrebno nam je poslednjih 24h u zavisnosti od vremena snimanja, memorija (disk) će biti puna, čak i ako se snimanje podeli u više fajlova.
- *Capture Filters* omogućava WireShark-u da prikazuje i snima samo saobraćaj koji smo definisali.
- Capture Filter može filtrirati npr:
  - host, src,
  - dst, net,
  - ether(mac adress),
  - port itd u zavisnosti šta želimo da snimimo

Capture Filter

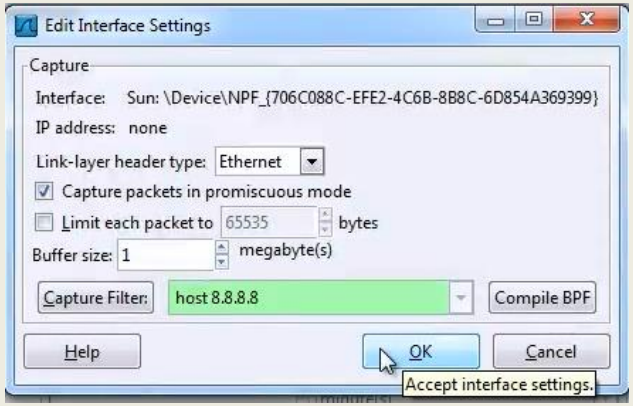
- Otvara se prozor *Edit Interface Settings*.
- Za filtriranje je potrebno upisati način filtriranja.
- Ukoliko prozor za upisivanje dobije crvenu boju, pretraživač nema određenu destinaciju filtriranja, tj. nema dovoljno informacija.

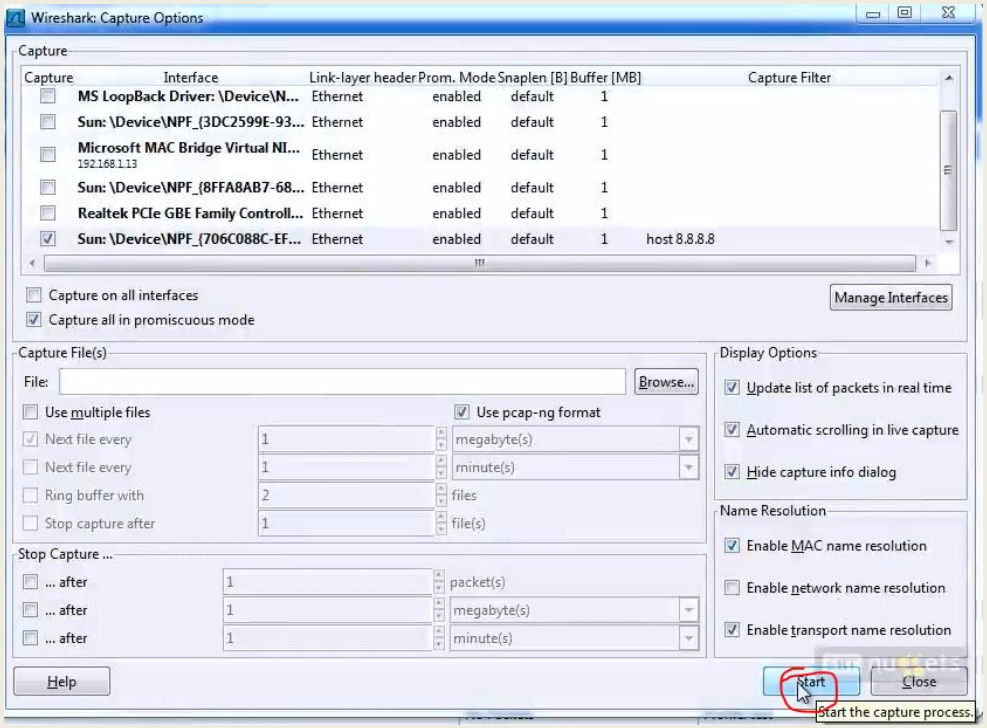




Capture Filter - Primer

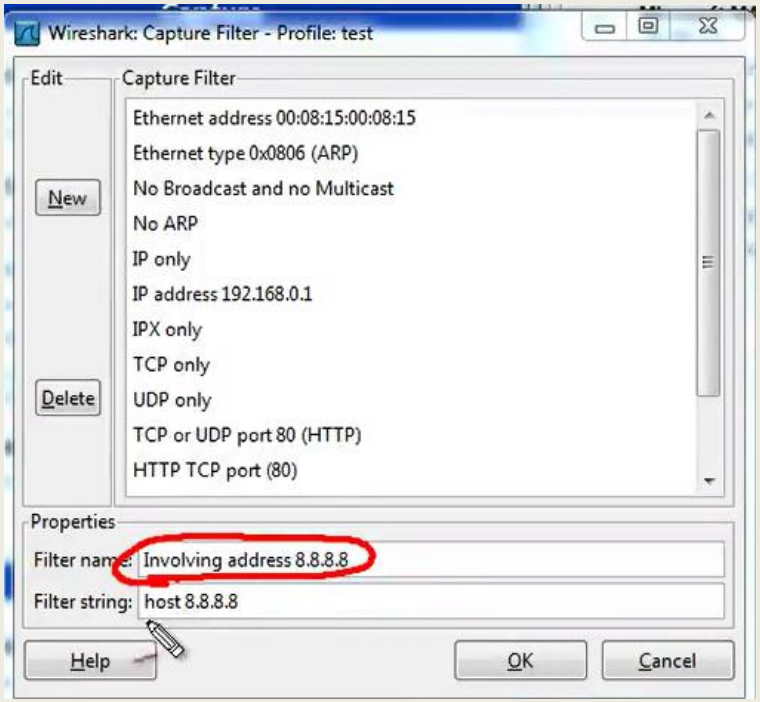
- Koristimo adresu Google-a koju unosimo u polje Capture filter koristeći sintaksu host 8.8.8.8.

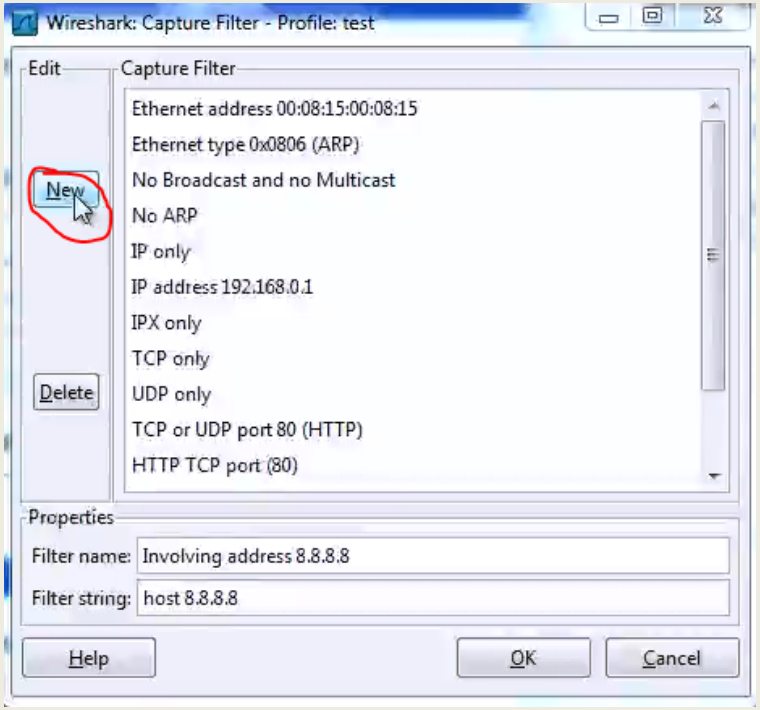


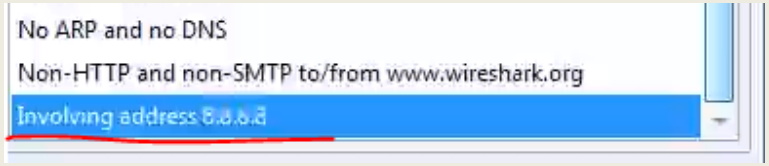


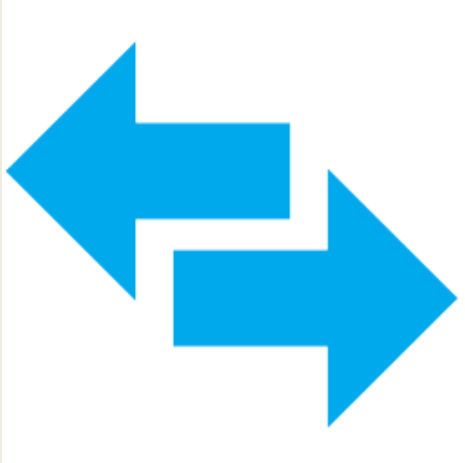
Capture Filter – Snimanje filtra

- Kako bi, po želji, ovu vrstu filtriranja zapamtili, za naredni put kada želimo upotrebiti istu vrstu filtriranja, potrebno je u prozoru Capture Filter zapamtiti željenu opciju, tako što imenujemo filter i izaberemo New.





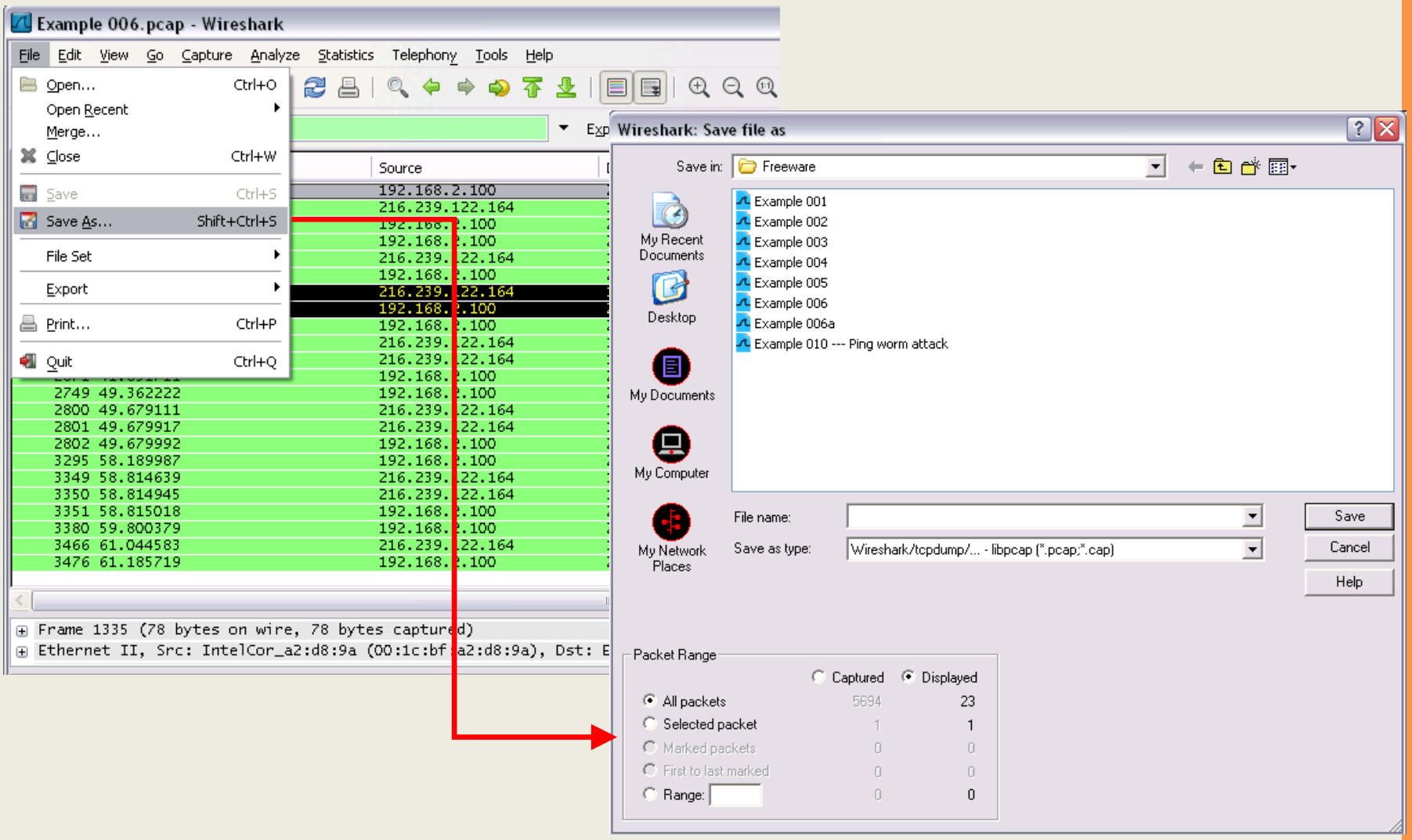




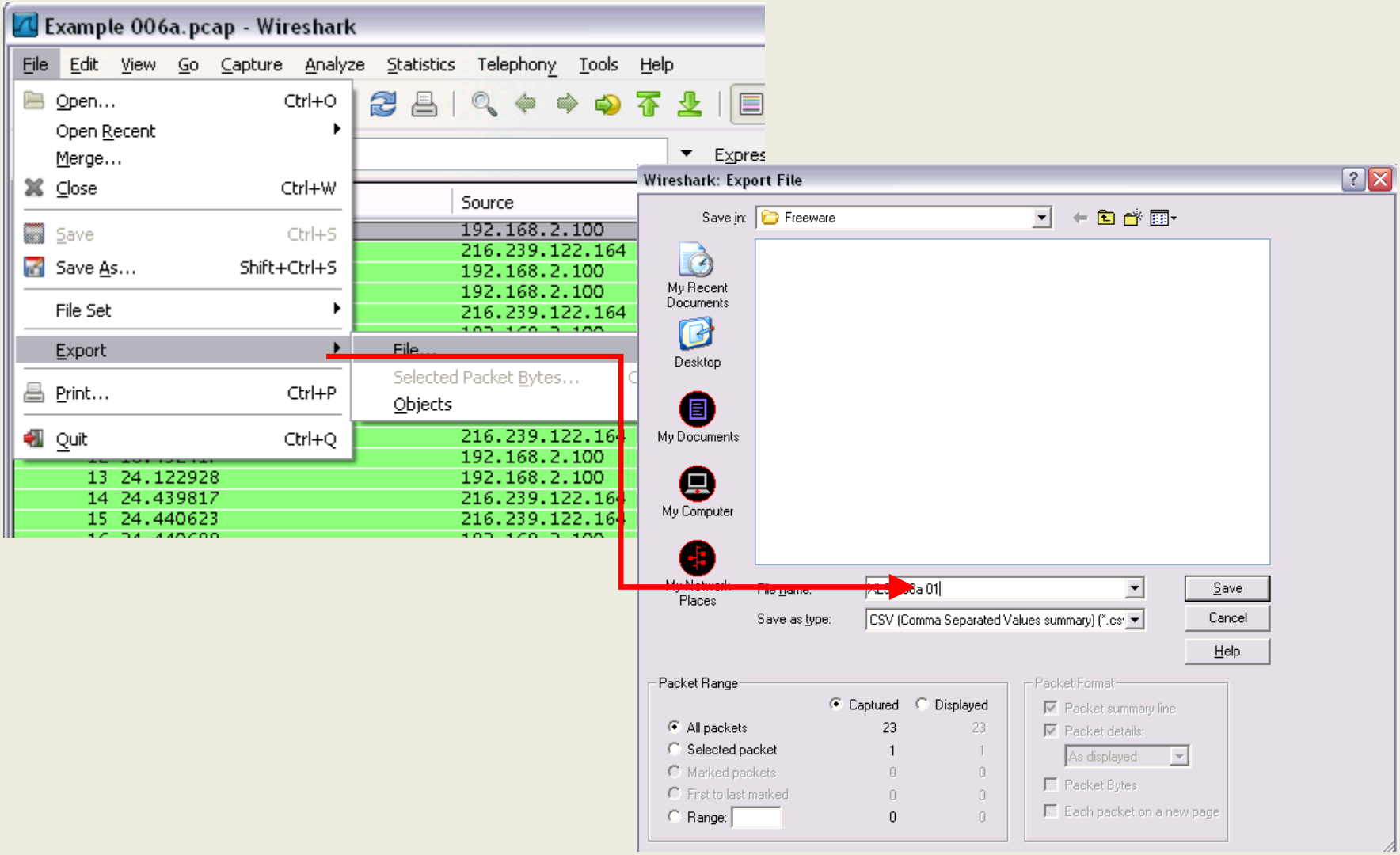
Poglavlje 5

Čuvanje podataka i manipulacija paketa

Čuvanje odabranih paketa

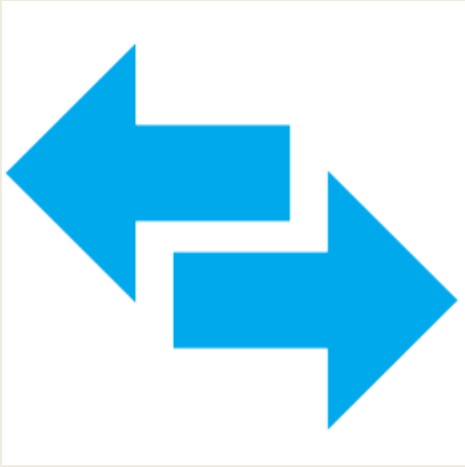


Izvoženje u CSV datoteku



Prikaz izvezene CSV datoteke

No.	Time	Time Variation	Source	Destination	Protocol	Info
1	0	0	192.168.2.100	216.239.122.164	TCP	27837 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 TSV=0 TSER=0
2	0.226724	0.226724	216.239.122.164	192.168.2.100	TCP	http > 27837 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1380
3	0.226772	4.8E-05	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.227146	0.227098	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
5	0.700674	0.473576	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
6	0.883533	0.409957	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=649 Ack=767 Win=64769 Len=0
7	1.161312	0.751355	216.239.122.164	192.168.2.100	HTTP	[TCP Retransmission] HTTP/1.1 200 OK (JPEG JFIF image)
8	1.161361	0.410006	192.168.2.100	216.239.122.164	TCP	[TCP Dup ACK 6#1] 27837 > http [ACK] Seq=649 Ack=767 Win=64769 Len=0
9	16.211468	15.801462	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
10	16.452024	0.650562	216.239.122.164	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
11	16.452343	15.801781	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
12	16.452417	0.650636	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=1539 Ack=1533 Win=65535 Len=0
13	24.122928	23.472292	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
14	24.439817	0.967525	216.239.122.164	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
15	24.440623	23.473098	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
16	24.440698	0.9676	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=2384 Ack=2299 Win=64769 Len=0
17	32.950693	31.983093	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
18	33.575345	1.592252	216.239.122.164	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
19	33.575651	31.983399	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
20	33.575724	1.592325	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=3269 Ack=3065 Win=65535 Len=0
21	34.561085	32.96876	192.168.2.100	216.239.122.164	HTTP	GET /b.gif HTTP/1.1
22	35.805289	2.836529	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (GIF89a)
23	35.946425	33.109896	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=4080 Ack=3567 Win=65033 Len=0

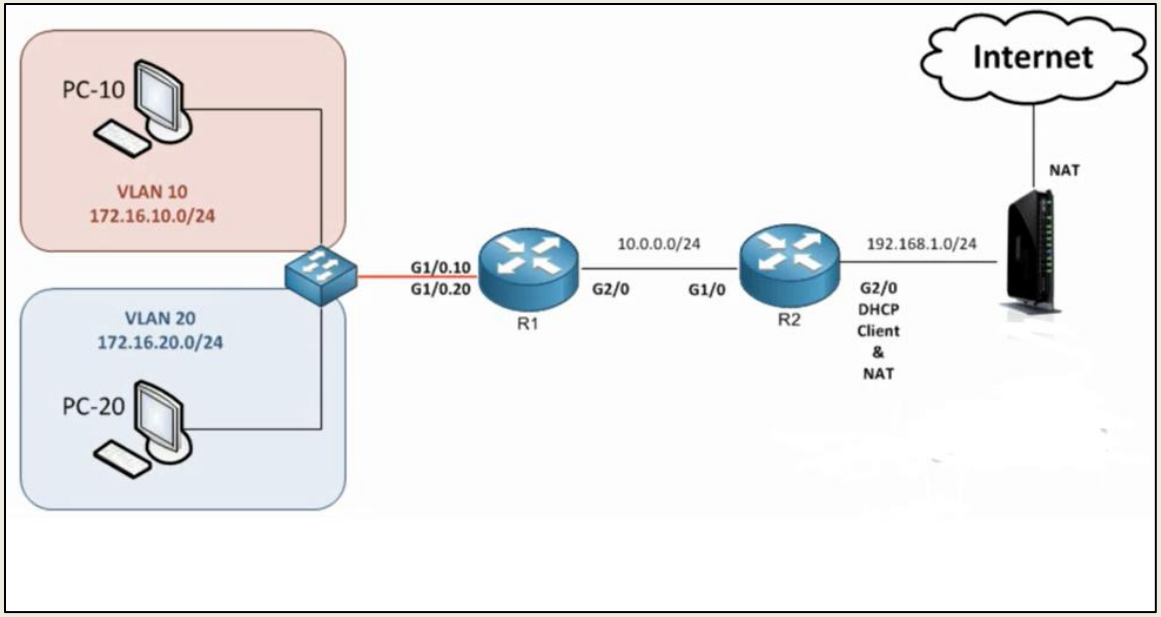


Poglavlje 6

Snalaženje u moru paketa

Praćenjne željene konverzacije

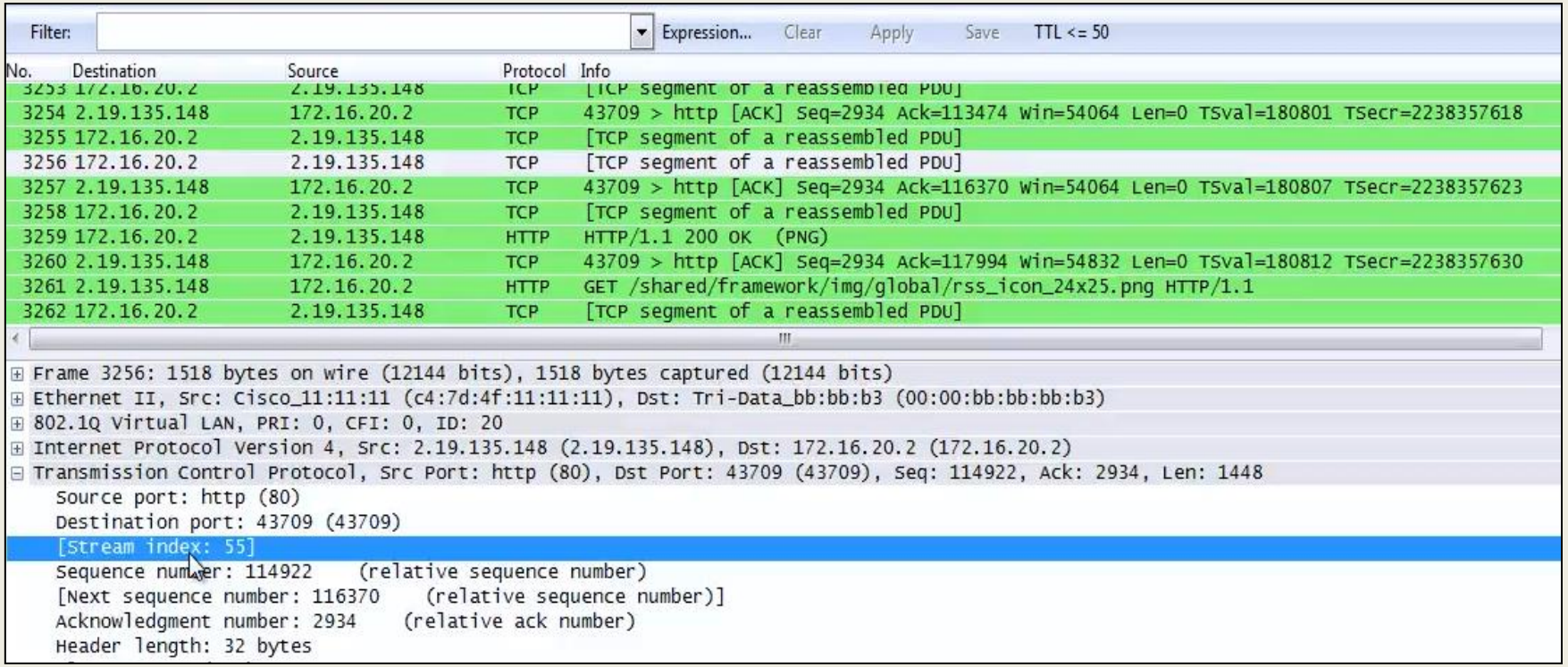
- Fokusiranje na jedan razgovor među hiljadama koji mogu biti deo snimanja datoteke, može biti kao traženje igle u plastu sena.
- Primer: dva računara **PC-10(VLAN 10)** i **PC-20(VLAN 20).**
- Kako znati koji je računar više zauzet, koji ima veći saobraćaj podataka i koje aplikacije i protokole ovi računari koriste?



- Analizira se protokol na mreži **G1/0.10** i **G1/0.20**, na koju su povezana 2 računara, **PC-10** i **PC-20**.

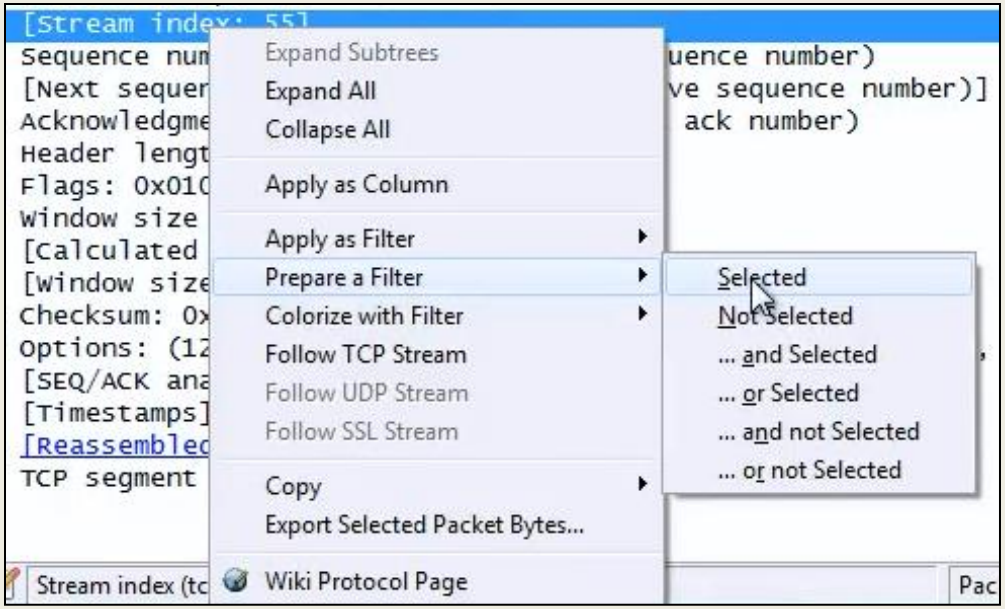
Praćenjne željene konverzacije

- ***tcp.stream Index Number***
  - izabere se bilo koj TCP paket, (npr. 3256, kao sa slike) i u detaljima o tom paketu "**Transmission Control Protocol**" se vidi da je Stream index: 55.



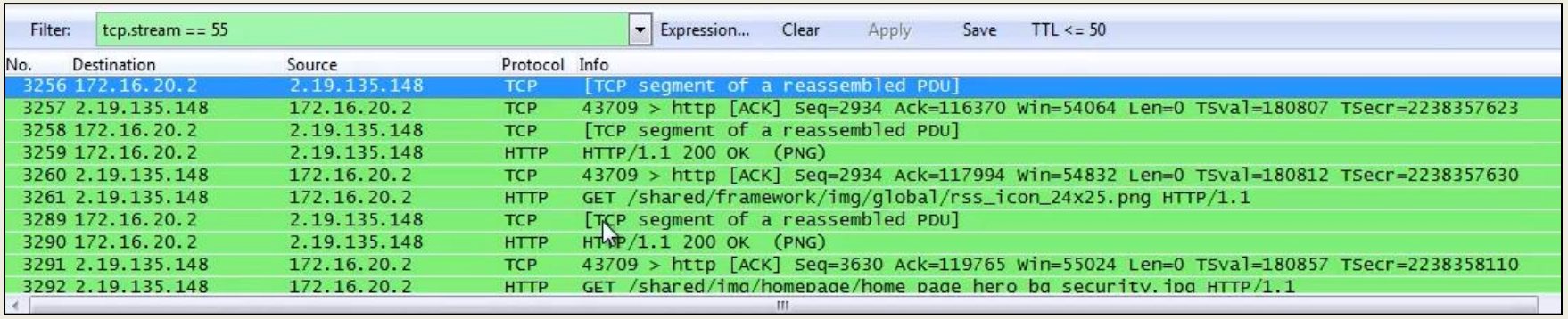
Praćenjne željene konverzacije

- Ukoliko želimo da filtriramo pakete koji imaju vrednost ***Stream index: 55***, onda moramo ići desnim klikom na taj detalj, pa izabrati **“Prepare a Filter”**, pa zatim izabrati **“Selected”**.
- Ovim smo definisali filter u filter polju, a proces filtriranja pokrećemo klikom na **“Apply”.**



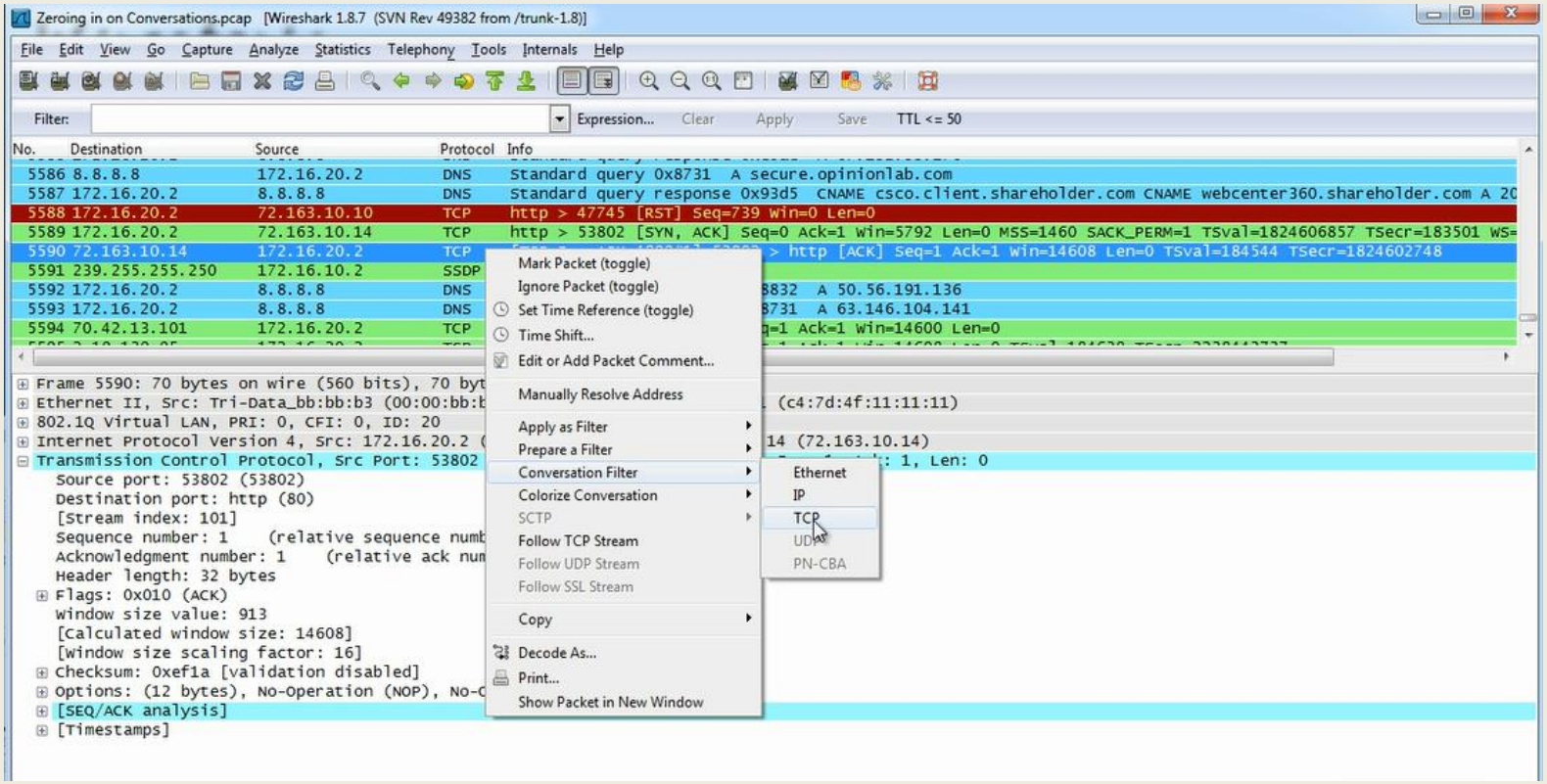
Praćenjne željene konverzacije

- Nakon primene filtriranja, prikazaće nam se paketi koji uključuju **“Stream index: 55”**



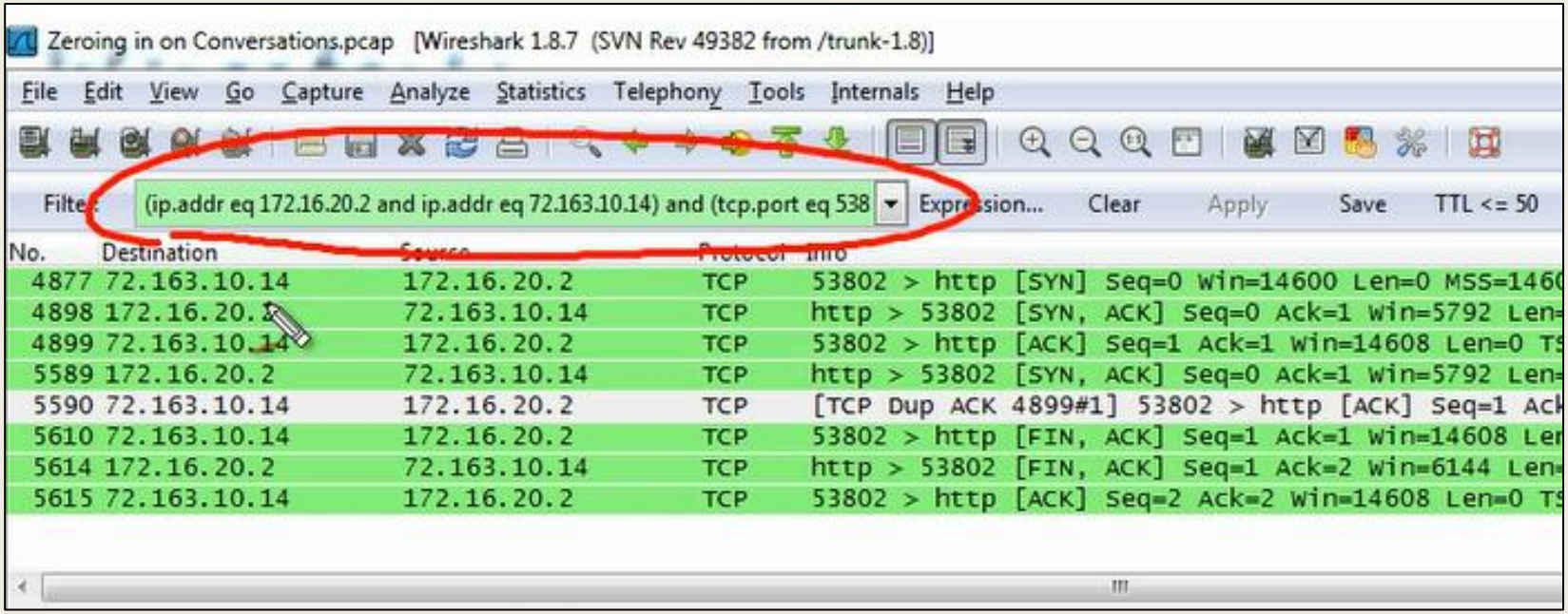
Conversation Filter

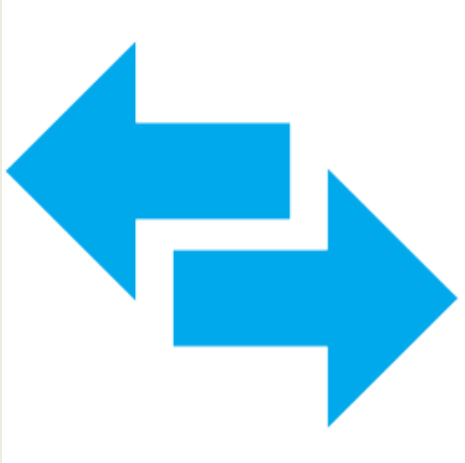
- Kao primer uzimamo bilo koji paket iz grupe.
- Trenutno ih u “**WireShark**-u” imamo 5647.
- Kako ne bi uzimali prvi ili poslednji paket za proveru saobraćaja, tj. razgovor sa računarom, uzećemo paket br.5590.
- Desnim klikom na određeni paket bira se opcija ***Conversation Filter > TCP***.



Conversation Filter

- Ovim postupkom se filtrira **TCP** i pojavljuju se **IP** adrese i portovi u obrascu "**Filter**".

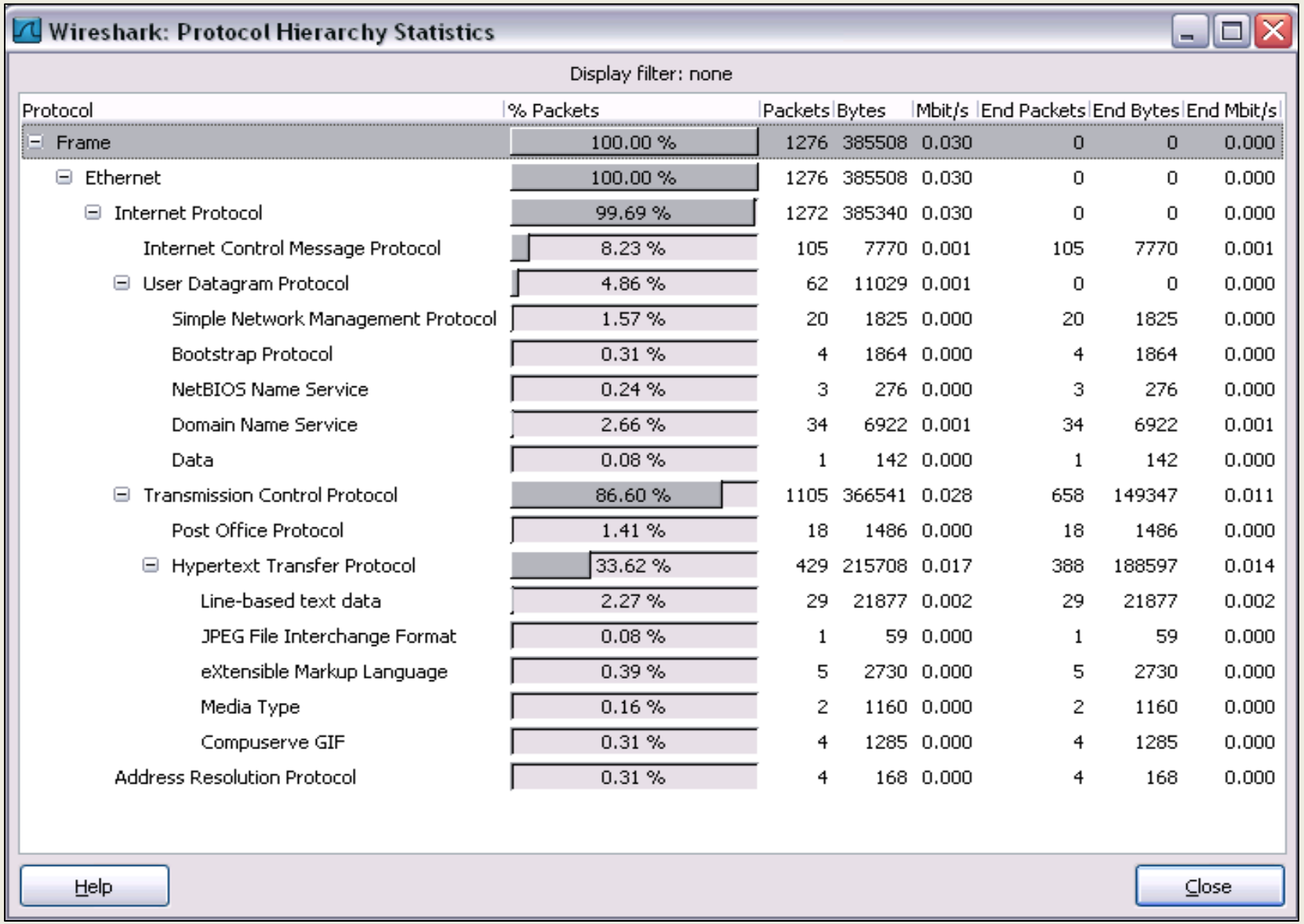




Poglavlje 6

Statistika paketa

Hijerarhija protokola



Wireshark: Protocol Hierarchy Statistics

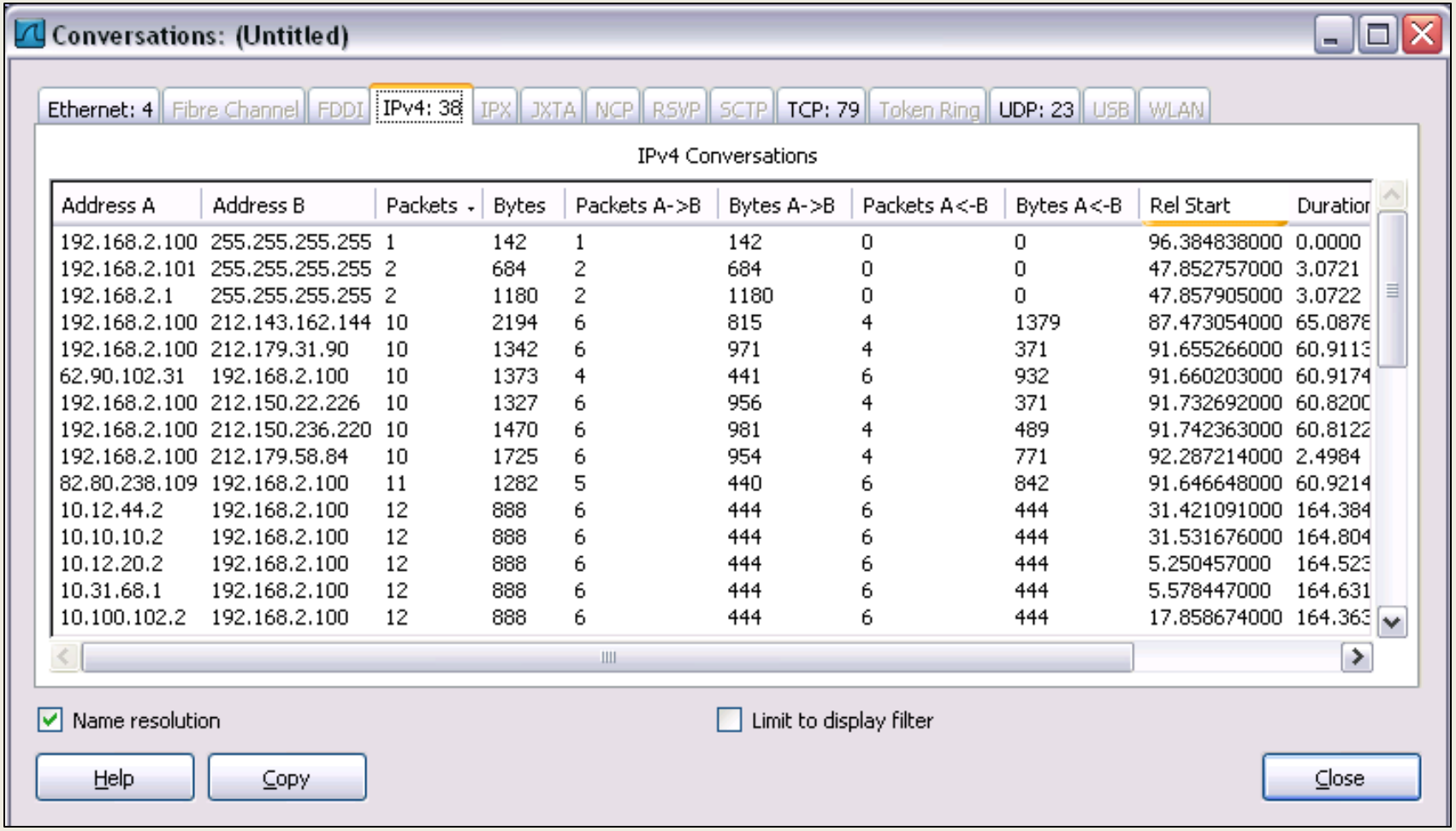
Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	1276	385508	0.030	0	0	0.000
Ethernet	100.00 %	1276	385508	0.030	0	0	0.000
Internet Protocol	99.69 %	1272	385340	0.030	0	0	0.000
Internet Control Message Protocol	8.23 %	105	7770	0.001	105	7770	0.001
User Datagram Protocol	4.86 %	62	11029	0.001	0	0	0.000
Simple Network Management Protocol	1.57 %	20	1825	0.000	20	1825	0.000
Bootstrap Protocol	0.31 %	4	1864	0.000	4	1864	0.000
NetBIOS Name Service	0.24 %	3	276	0.000	3	276	0.000
Domain Name Service	2.66 %	34	6922	0.001	34	6922	0.001
Data	0.08 %	1	142	0.000	1	142	0.000
Transmission Control Protocol	86.60 %	1105	366541	0.028	658	149347	0.011
Post Office Protocol	1.41 %	18	1486	0.000	18	1486	0.000
Hypertext Transfer Protocol	33.62 %	429	215708	0.017	388	188597	0.014
Line-based text data	2.27 %	29	21877	0.002	29	21877	0.002
JPEG File Interchange Format	0.08 %	1	59	0.000	1	59	0.000
eXtensible Markup Language	0.39 %	5	2730	0.000	5	2730	0.000
Media Type	0.16 %	2	1160	0.000	2	1160	0.000
Compuserve GIF	0.31 %	4	1285	0.000	4	1285	0.000
Address Resolution Protocol	0.31 %	4	168	0.000	4	168	0.000

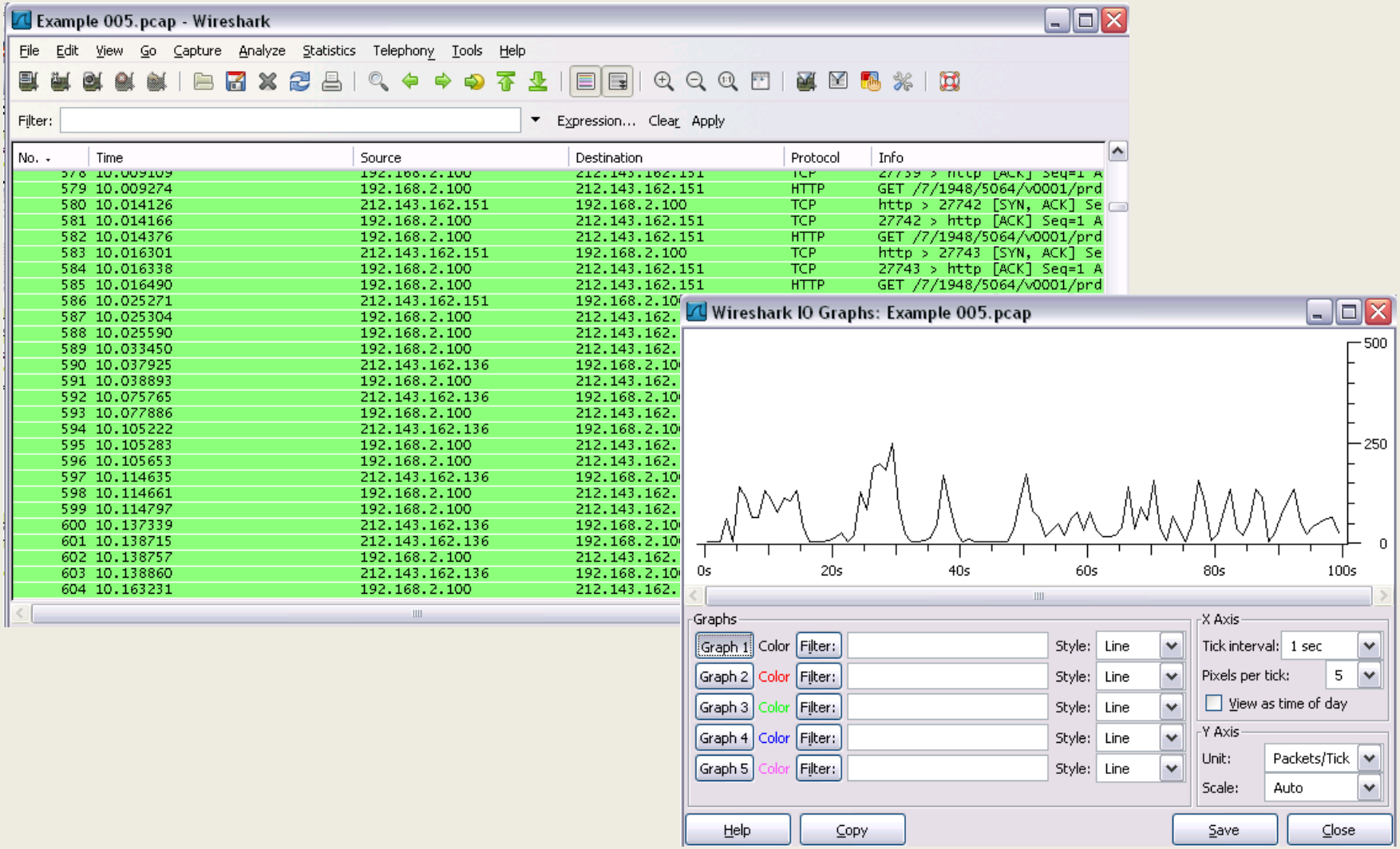
Help

Close

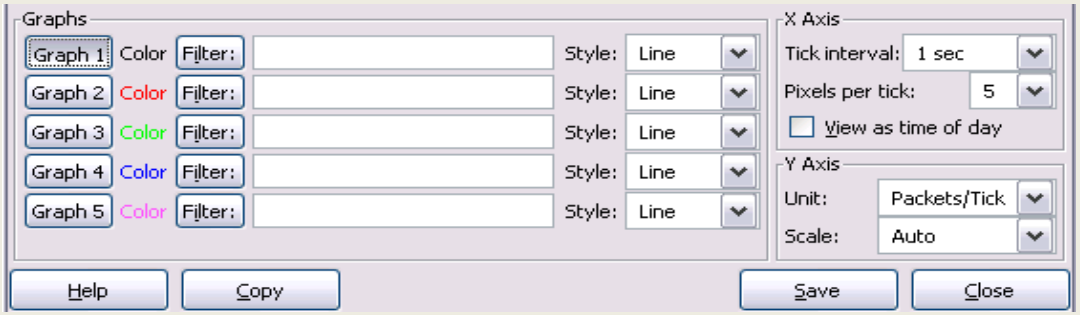
Konverzacija između dve krajnje tačke (end-pointa)



I/O Grafik


Example 005.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
579 10.009274 192.168.2.100 212.143.162.151 HTTP GET /7/1948/5064/v0001/prd
580 10.014126 212.143.162.151 192.168.2.100 TCP http > 27742 [SYN, ACK] Se
581 10.014166 192.168.2.100 212.143.162.151 TCP 27742 > http [ACK] Seq=1 A
582 10.014376 192.168.2.100 212.143.162.151 HTTP GET /7/1948/5064/v0001/prd
583 10.016301 212.143.162.151 192.168.2.100 TCP http > 27743 [SYN, ACK] Se
584 10.016338 192.168.2.100 212.143.162.151 TCP 27743 > http [ACK] Seq=1 A
585 10.016490 192.168.2.100 212.143.162.151 HTTP GET /7/1948/5064/v0001/prd
586 10.025271 212.143.162.151
587 10.025304 192.168.2.100
588 10.025590 192.168.2.100
589 10.033450 192.168.2.100
590 10.037925 212.143.162.136
591 10.038893 192.168.2.100
592 10.075765 212.143.162.136
593 10.077886 192.168.2.100
594 10.105222 212.143.162.136
595 10.105283 192.168.2.100
596 10.105653 192.168.2.100
597 10.114635 212.143.162.136
598 10.114661 192.168.2.100
599 10.114797 192.168.2.100
600 10.137339 212.143.162.136
601 10.138715 212.143.162.136
602 10.138757 192.168.2.100
603 10.138860 212.143.162.136
604 10.163231 192.168.2.100
Wireshark IO Graphs: Example 005.pcap
500
250
0
0s
20s
40s
60s
80s
100s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

Opcije konfigurisanja



I/O Grafici

Grafik 1-5: Grafik 1 je podrazumevano(default) izabran .
Filter: displej filter za izabrani grafik
Style: stil grafika(Line/Impulse/FBar/Dot)

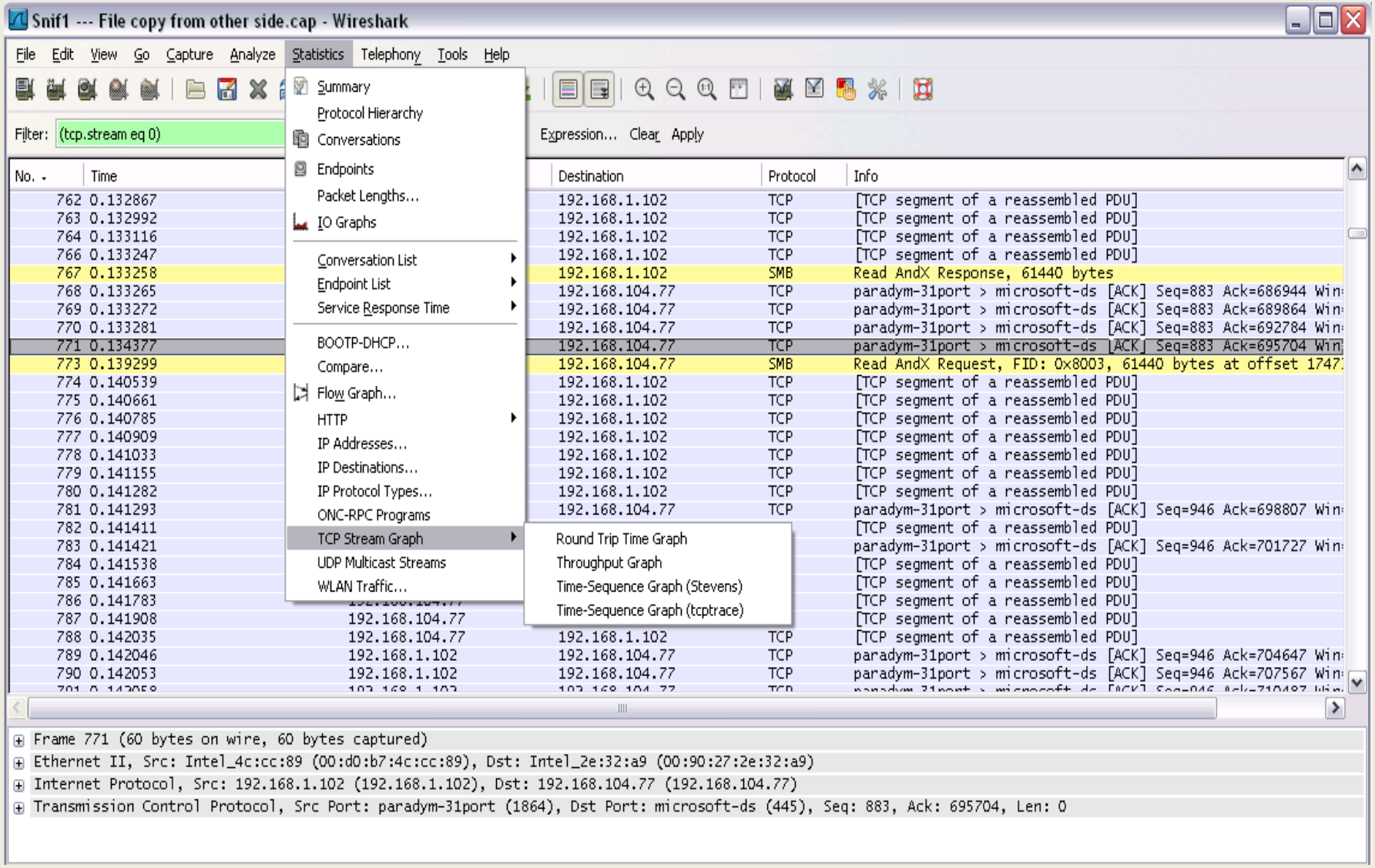
X Osa

Tick interval: interval trajanja
(10/1 minuta ili 10/1/0.1/0.01/0.001 sekundi)
Pixels per tick: koristi 10/5/2/1 *pixela per tick* interval vremena
View as time of day: mogućnost prikaza doba dana od početka snimanja umesto minuta/sekundi.

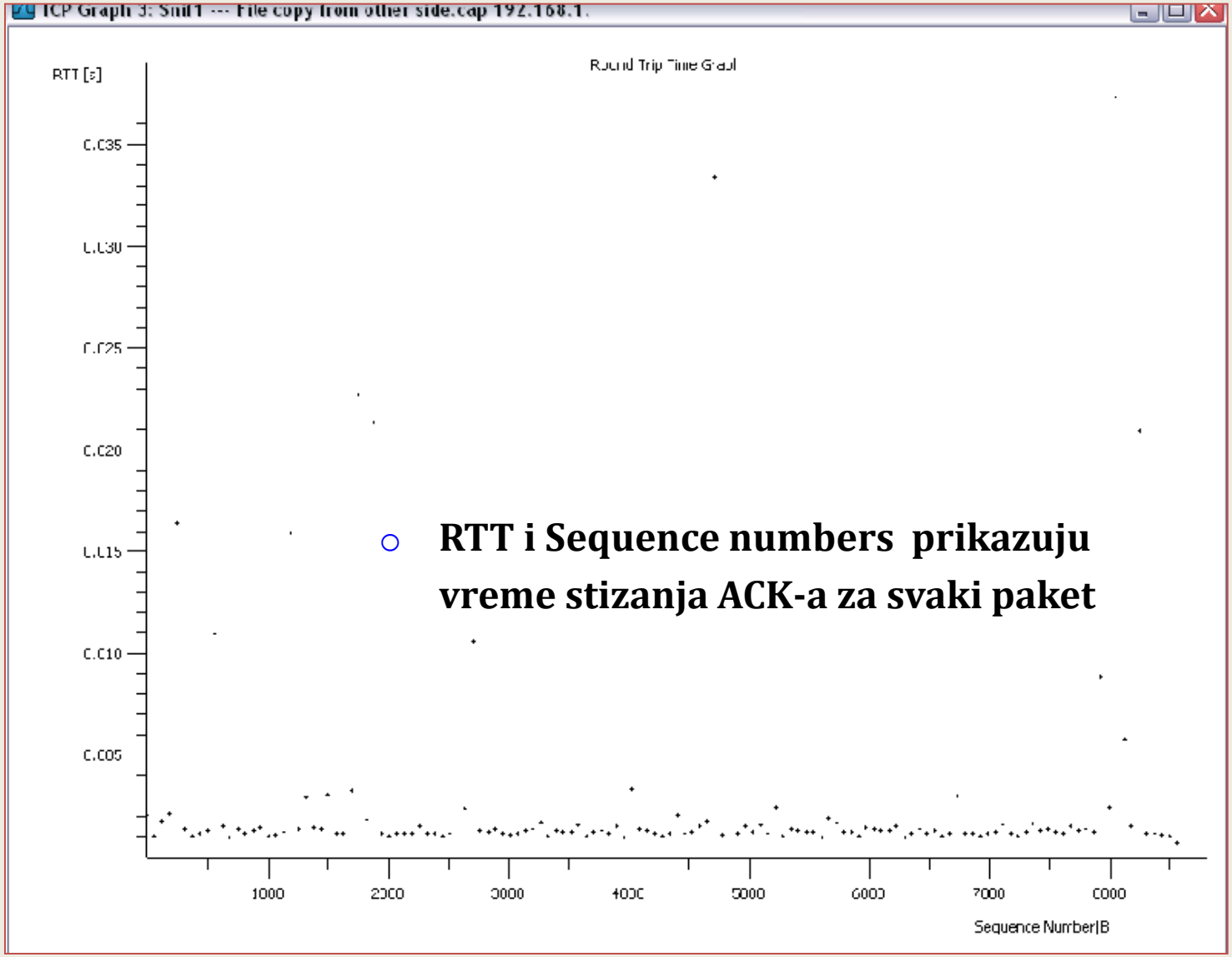
Y osa

Unit: jedinica prikaza za y osu
(Packets/Tick, Bytes/Tick, Bits/Tick, Advanced...)
Skala: skala y ose (Logaritamska, Auto, 10, 20, 50, 100, 200,...)

TCP Stream Grafik

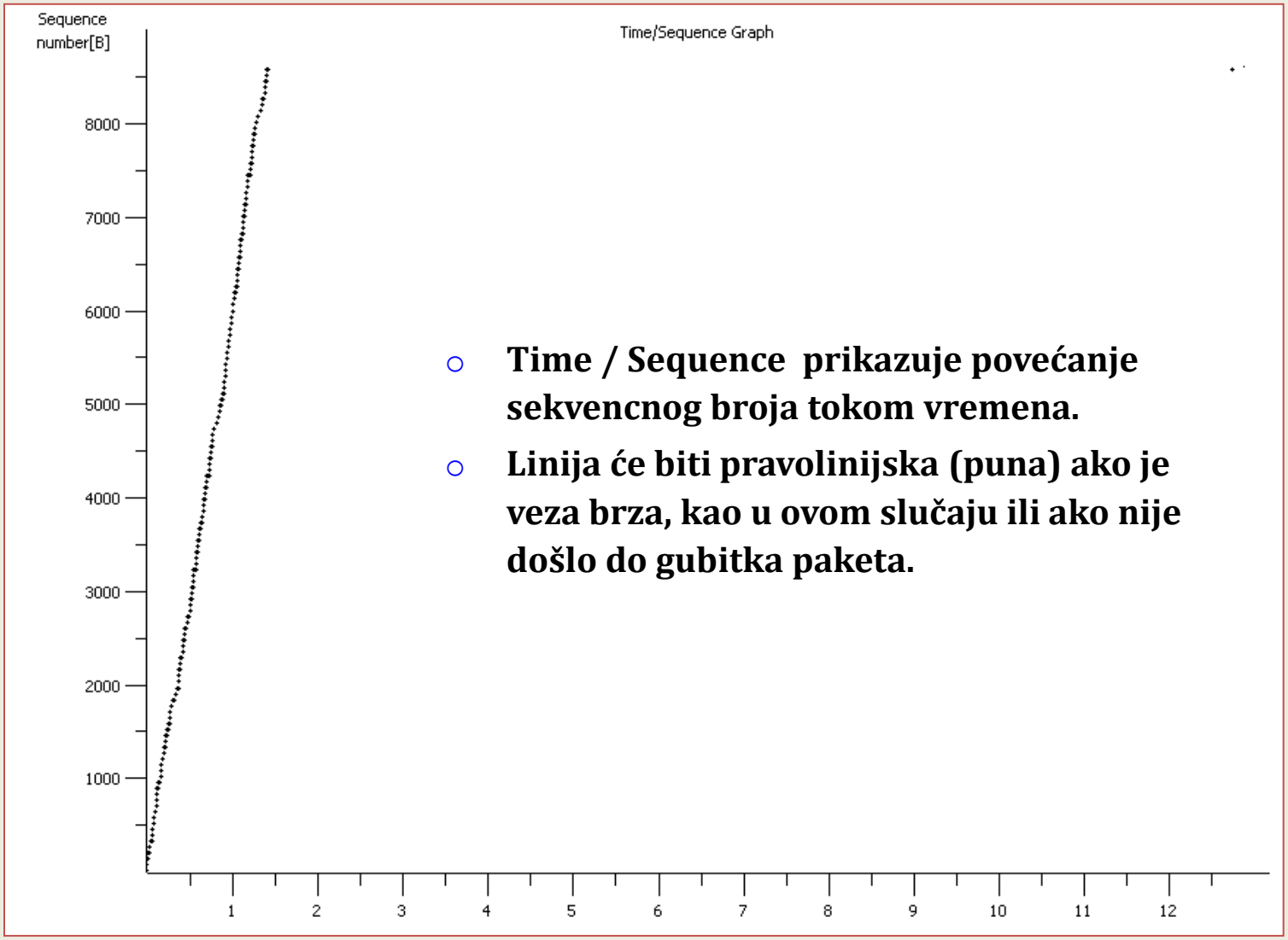


Round-Trip Time Grafik



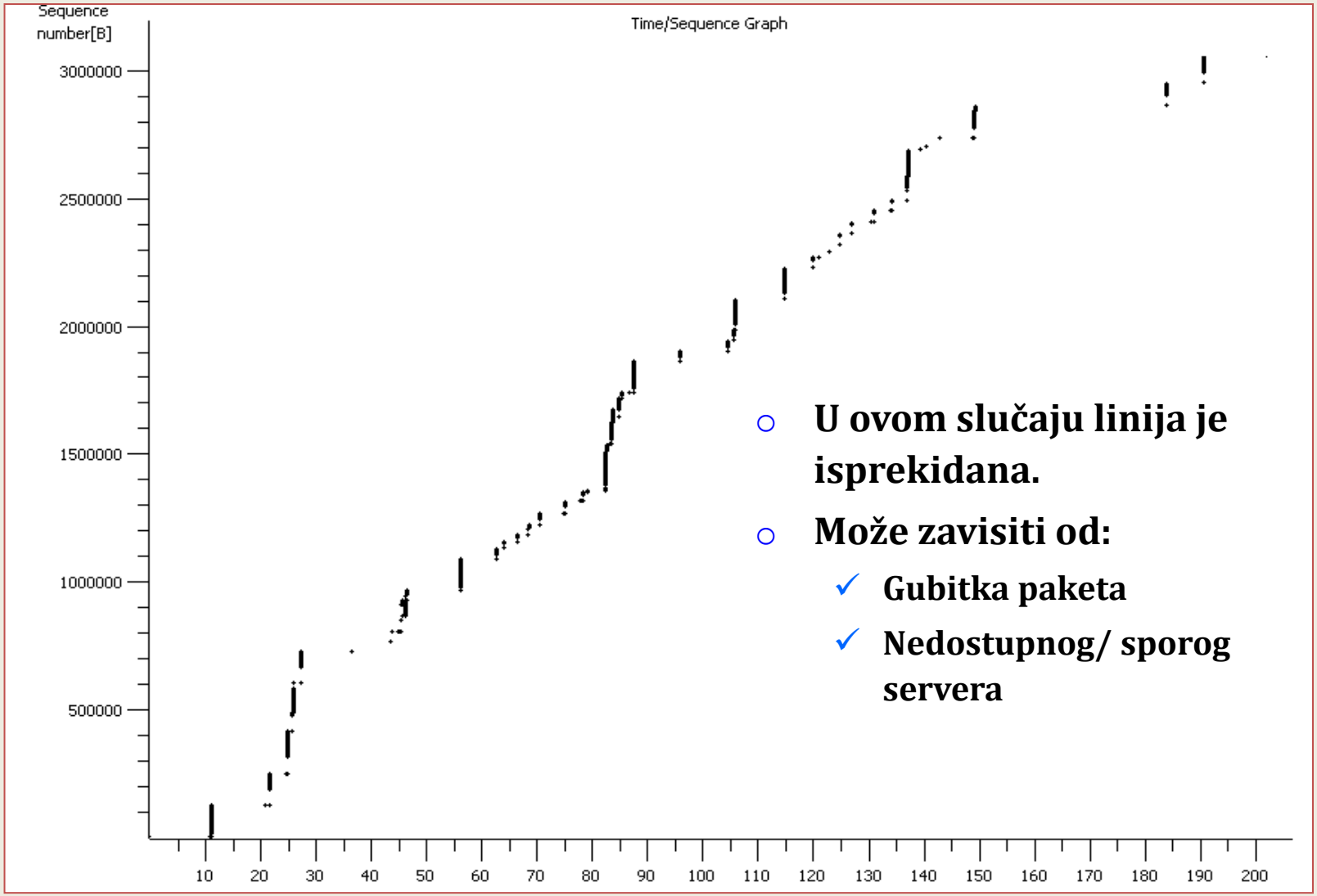
- **RTT i Sequence numbers prikazuju vreme stizanja ACK-a za svaki paket**

Time / Sequence Grafik

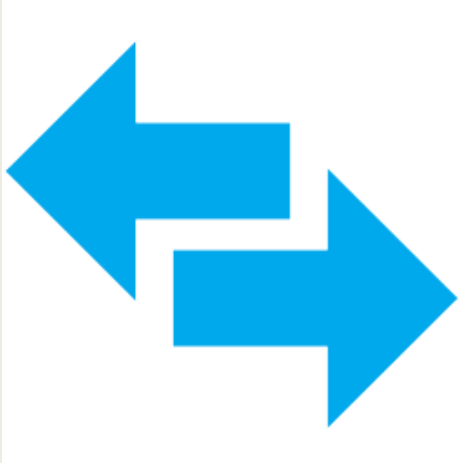


- **Time / Sequence prikazuje povećanje sekvencnog broja tokom vremena.**
- **Linija će biti pravolinijska (puna) ako je veza brza, kao u ovom slučaju ili ako nije došlo do gubitka paketa.**

Time / Sequence Grafik



- **U ovom slučaju linija je isprekidana.**
- **Može zavisiti od:**
  - ✓ **Gubitka paketa**
  - ✓ **Nedostupnog/ sporog servera**

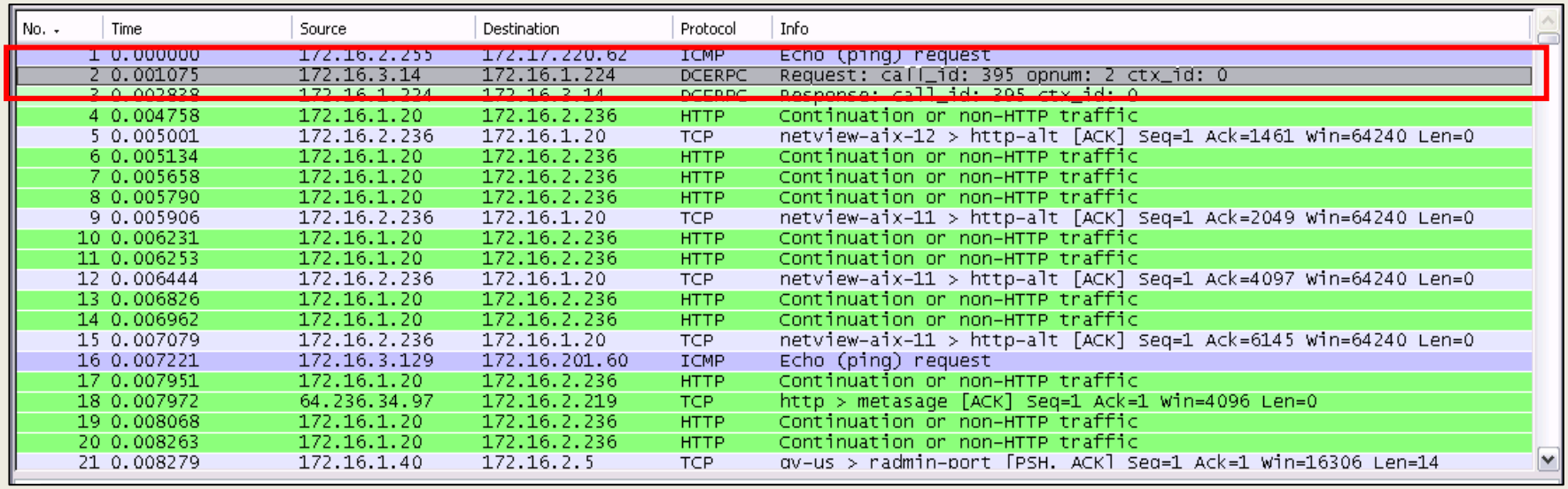


Poglavlje 7

Kolorizacija paketa

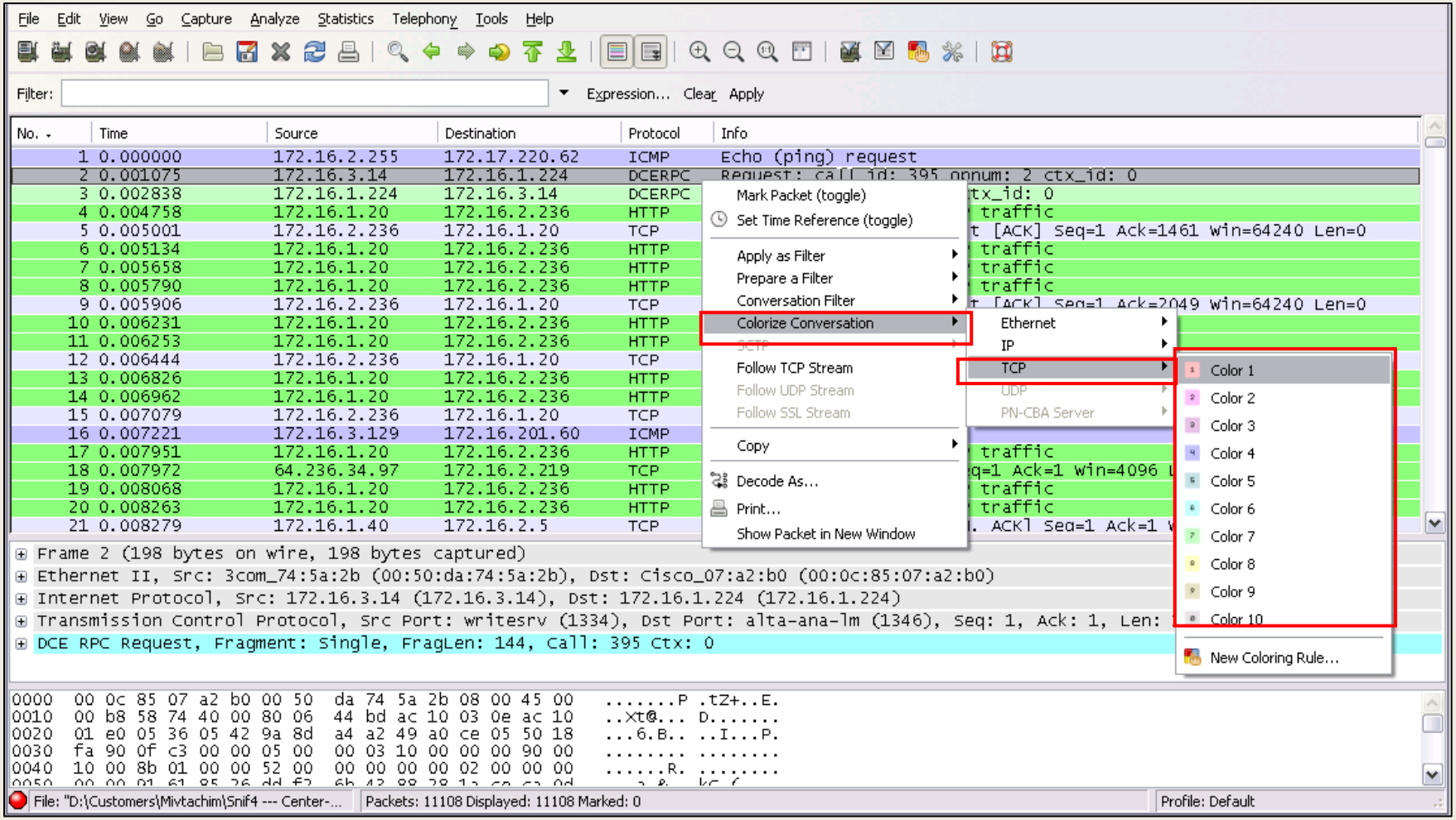
Kolorizacija:

- Kolorizacija u odnosu na filter
- Kolorizacija samo određenih paketa, po izboru
- Mnogo primera je dato na Wireshark Wiki stranici http://wiki.wireshark.org/ColoringRules



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.2.255	172.17.220.62	ICMP	Echo (ping) request
2	0.001075	172.16.3.14	172.16.1.224	DCERPC	Request: call_id: 395 opnum: 2 ctx_id: 0
3	0.002838	172.16.1.224	172.16.3.14	DCERPC	Response: call_id: 395 ctx_id: 0
4	0.004758	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
5	0.005001	172.16.2.236	172.16.1.20	TCP	netview-aix-12 > http-alt [ACK] Seq=1 Ack=1461 Win=64240 Len=0
6	0.005134	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
7	0.005658	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
8	0.005790	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
9	0.005906	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=2049 Win=64240 Len=0
10	0.006231	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
11	0.006253	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
12	0.006444	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=4097 Win=64240 Len=0
13	0.006826	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
14	0.006962	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
15	0.007079	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=6145 Win=64240 Len=0
16	0.007221	172.16.3.129	172.16.201.60	ICMP	Echo (ping) request
17	0.007951	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
18	0.007972	64.236.34.97	172.16.2.219	TCP	http > metasage [ACK] Seq=1 Ack=1 Win=4096 Len=0
19	0.008068	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
20	0.008263	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
21	0.008279	172.16.1.40	172.16.2.5	TCP	av-us > radmin-port [PSH, ACK] Seq=1 Ack=1 Win=16306 Len=14

Primer kolorizacije



Primer kolorizacije