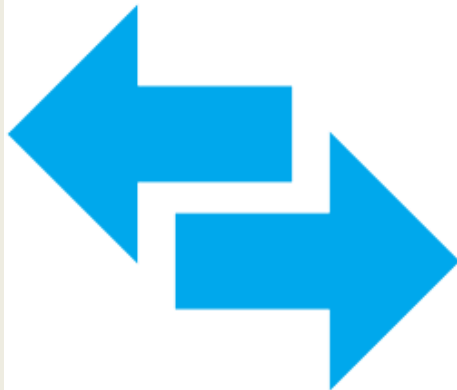




# Analizator mrežnih protokola

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.

## ✓ **Sistemske zahteve:**

- 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,
- Definisane 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

The screenshot displays the Wireshark interface with the following components:

- Filter:** Expression... Clear Apply
- Packet List:** A table showing 74 captured packets. The selected packet (No. 32) is highlighted in blue.
- Packet Details:** A tree view showing the structure of the selected packet: Ethernet II, Internet Protocol, User Datagram Protocol, and Simple Network Management Protocol.
- Packet Bytes:** A hex-to-ASCII conversion of the selected packet's raw data.

No.	Time	Source	Destination	Protocol	Info
64	36.858576	192.168.2.100	10.100.102.2	ICMP	Echo (ping) request
65	36.863613	10.100.102.2	192.168.2.100	ICMP	Echo (ping) reply
66	44.406189	192.168.2.100	10.100.102.1	SNMP	get-request IF-MIB::ifOperS
67	44.413024	10.100.102.1	192.168.2.100	SNMP	get-response IF-MIB::ifOperS
68	44.499055	Msi_d4:52:4d	Broadcast	ARP	who-has 192.168.2.1? Tell
69	45.609033	192.168.2.100	10.40.41.2	ICMP	quest
70	47.797985	192.168.2.100	10.40.41.2	ICMP	quest
71	48.891533	192.168.2.100	10.100.102.1	SNMP	-MIB::ifOperS
72	48.897871	10.100.102.1	192.168.2.100	SNMP	F-MIB::ifOperS
73	49.989403	192.168.2.100	10.40.41.2	ICMP	quest
74	53.048866	192.168.2.100	255.255.255.255	UDP	Source port: 1027 Destinat

**Lista Paketa**

**Detalji Paketa**

```
0000 00 0e 2e 6e 2f 7d 00 1c bf a2 d8 9a 08 00 45 00  ...n/}. . . . .E.
0010 00 48 04 d4 00 00 80 11 02 60 c0 a8 02 64 0a 64  .H. . . . .d.d
0020 66 01 04 05 00 a1 00 34 a1 75 30 2a 02 01 00 04  f. . . . .4 .u0*. . . .
0030 06 70 75 62 6c 69 63 a0 1d 02 03 00 e2 af 02 01  .public. . . . .
0040 00 02 01 00 30 10 30 0e 06 0a 2b 06 01 02 01 02  ....0.0. .+. . . .
0050 02 01 08 05 05 00  . . . . .
```

**Bajti paketa**

Frame (frame), 86 bytes      Packets: 74 Displayed: 74 Marked: 0      Profile: Default

# 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

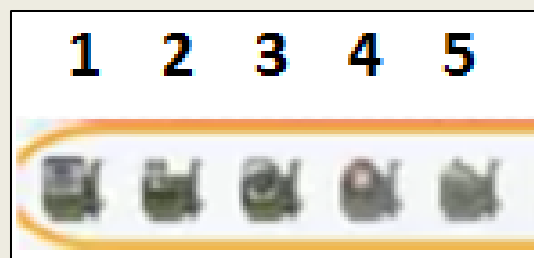
start novog hvatanja.

## 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.

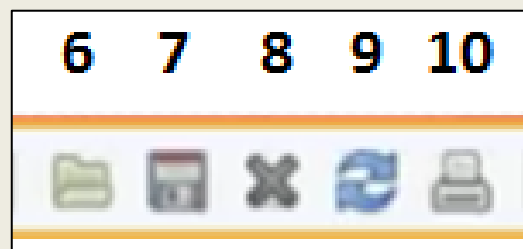
## 8. Close this capture file

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

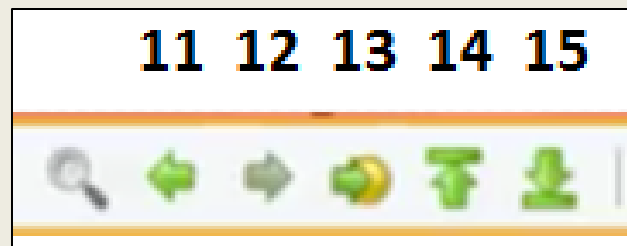
idi na paket sa brojem (unositi se željeni broj paketa, i automatski se prikazuju detalji o paketu u Packet list panel-u i Packet details panel-u).

## 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

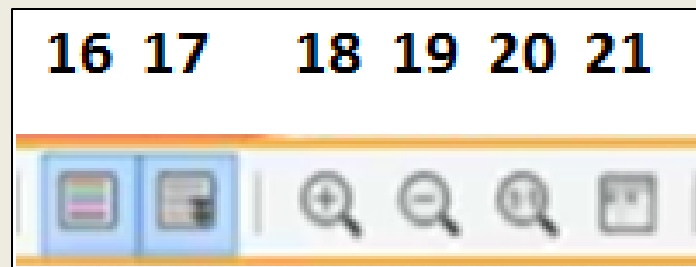
umanjenje veličine podataka

## 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

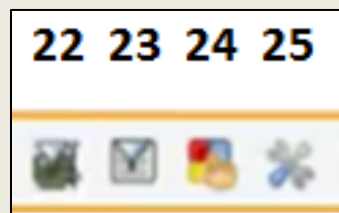
dodavanje display filtra

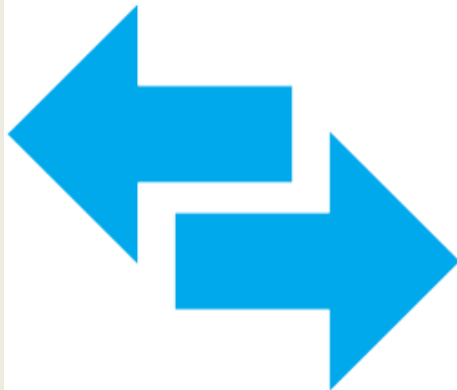
## 24. Edit coloring rules

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)

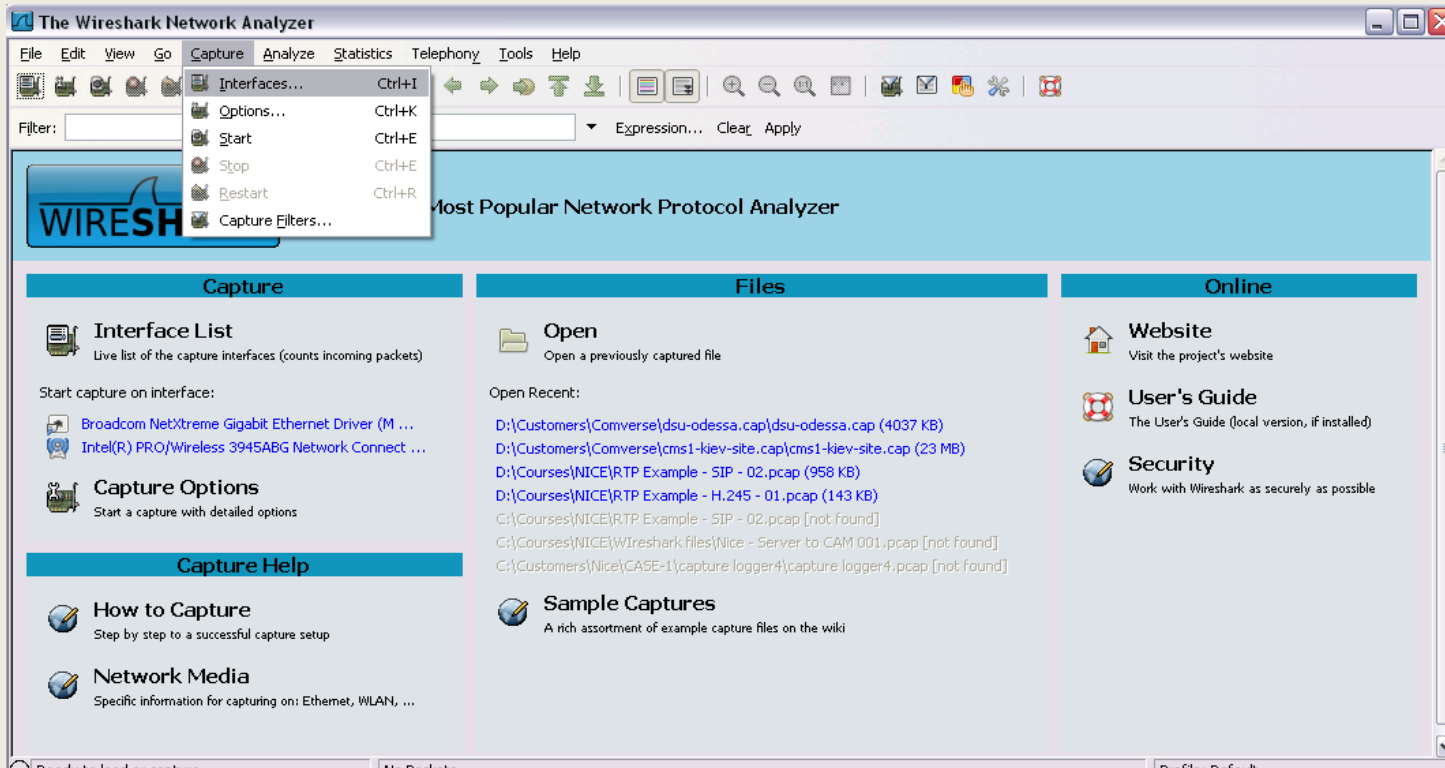




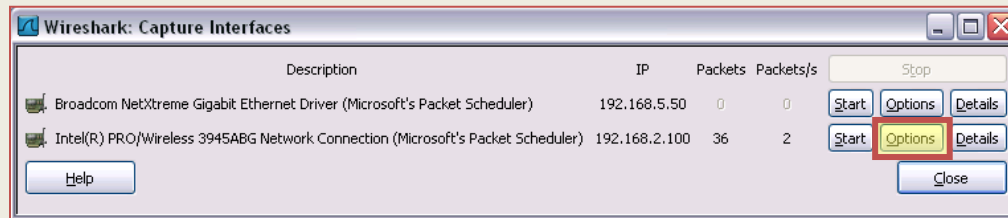
*Poglavlje 2*

***Beleženje paketa***

# Lista interfejsa

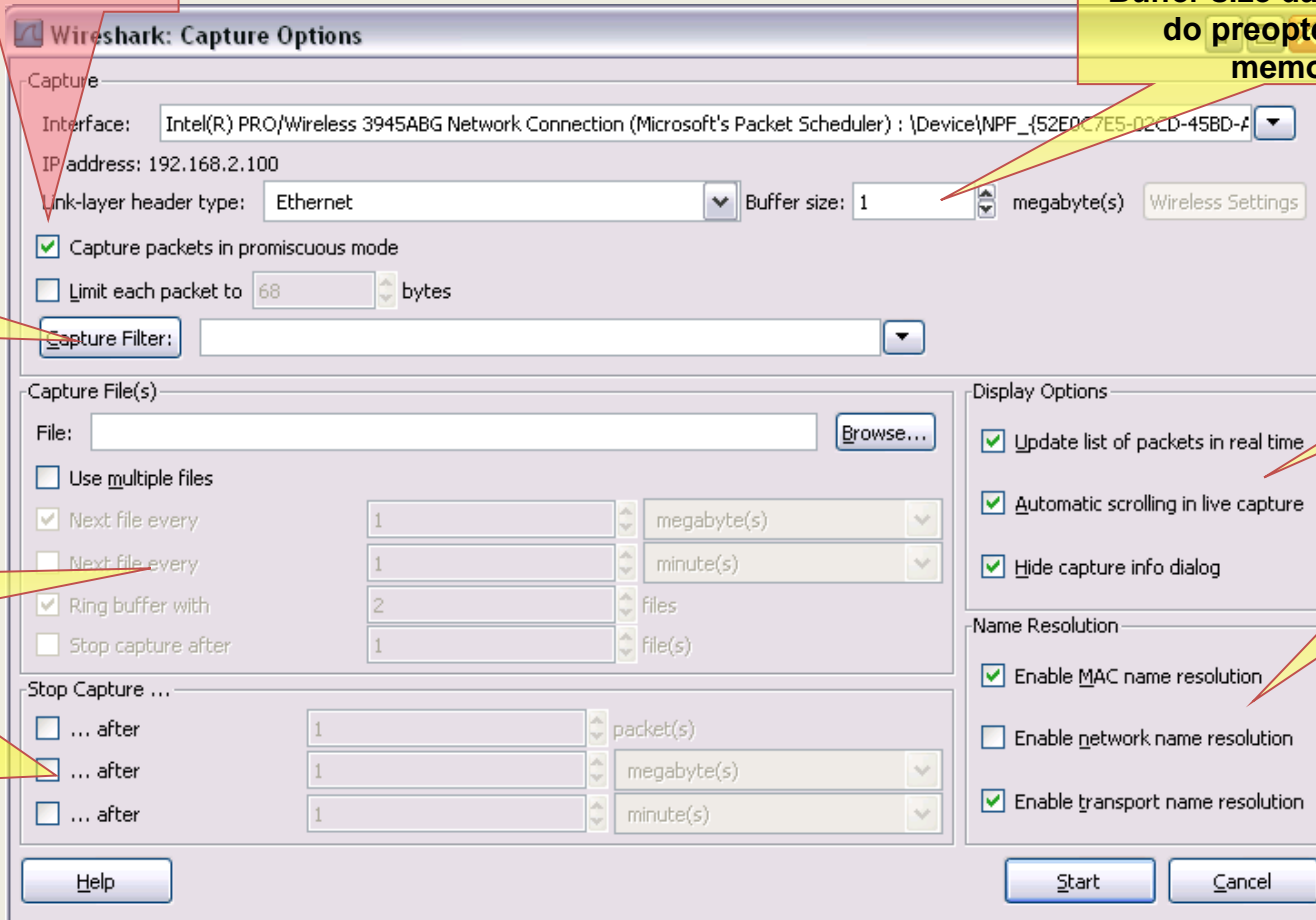


Description	IP	Packets	Packets/s	Stop
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	192.168.5.50	0	0	<input type="button" value="Start"/> <input type="button" value="Options"/> <input type="button" value="Details"/>
Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler)	192.168.2.100	36	2	<input type="button" value="Start"/> <input type="button" value="Options"/> <input type="button" value="Details"/>



Beleženje svih paketa na mreži

Buffer size da ne bi došlo do preopterećenja memorije



Filter beleženja

Opcije prikaza

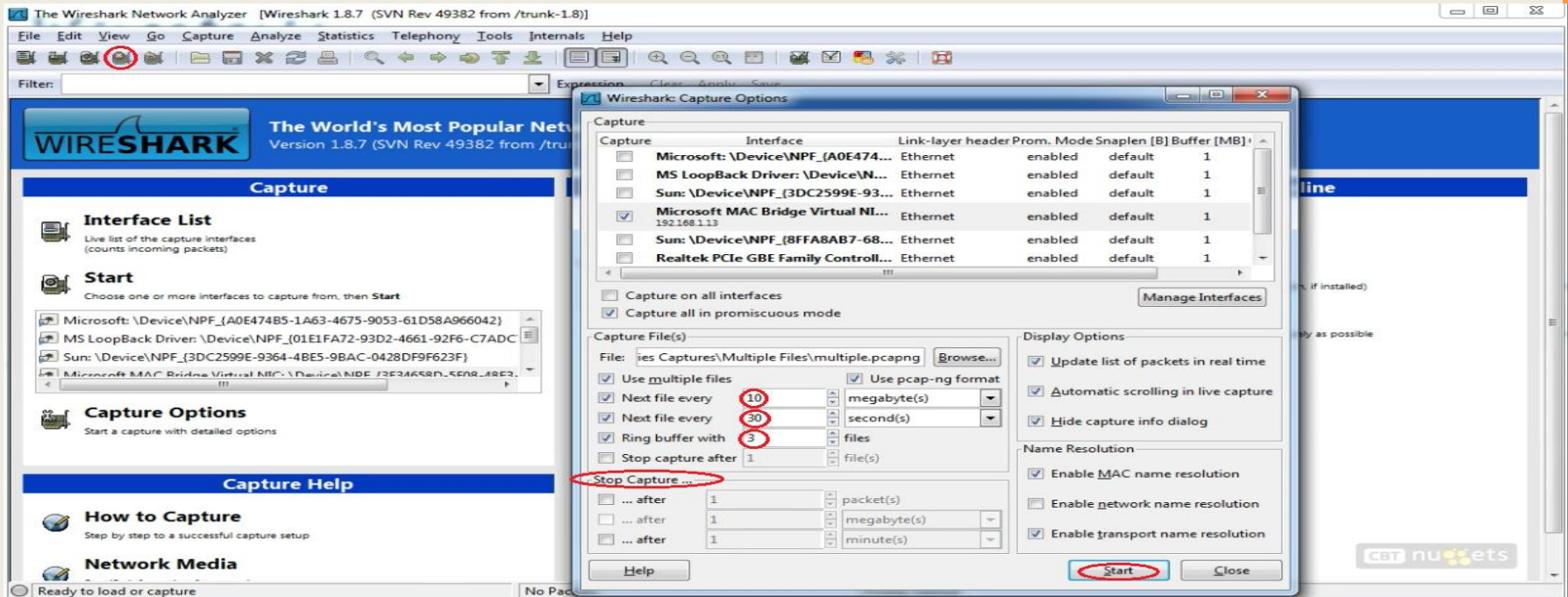
Beleženje višestrukih fajlova

Opcije razrešavanja imena

U kome trenutku automatski prestati sa beleženjem

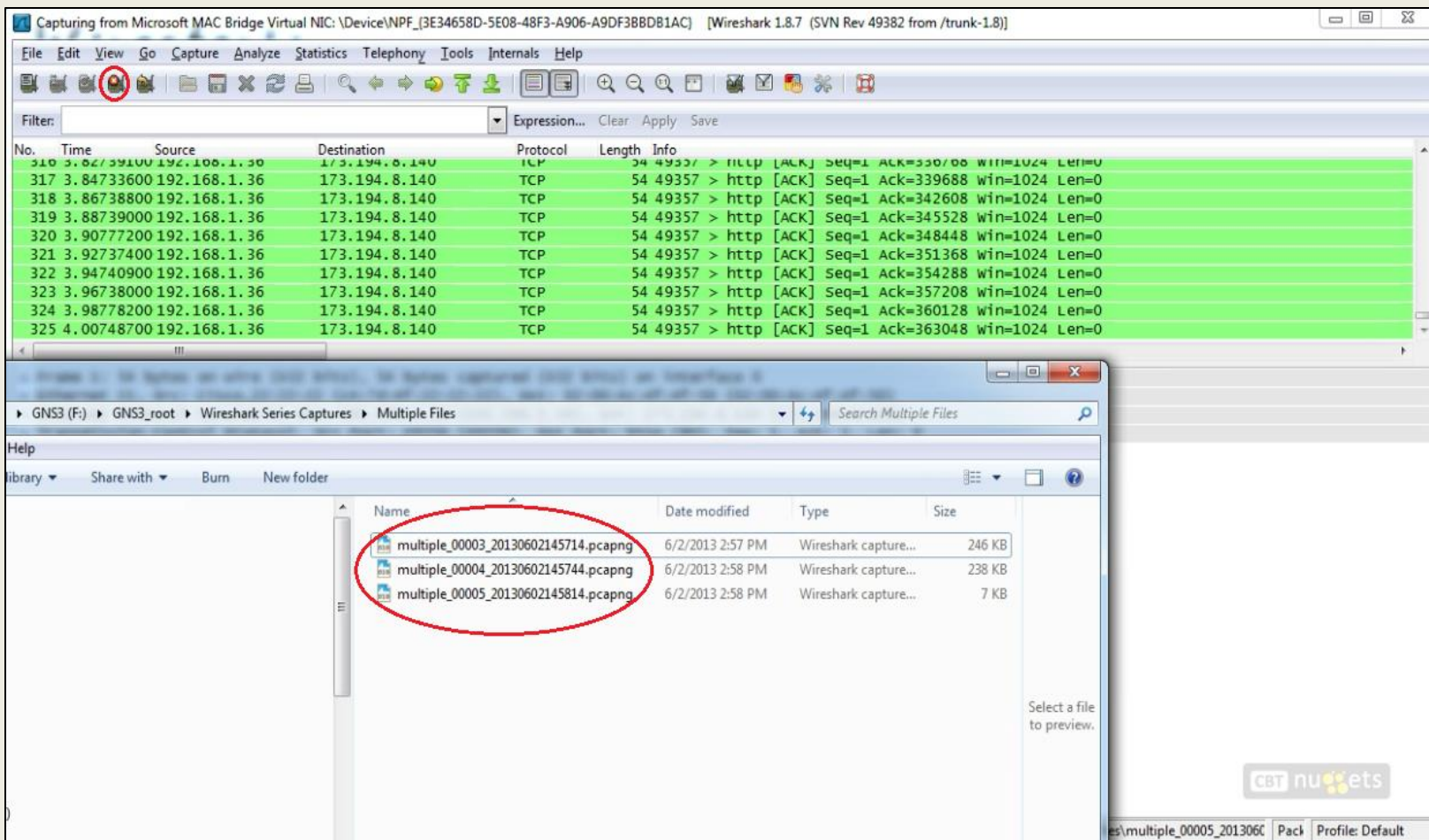
# Use multiple files - Definisiranje veličine fajlu:

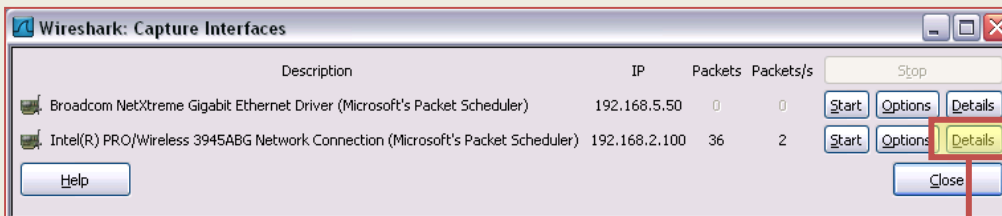
- **Kreiranje novog fajla**
  - kada fajl predje 10 MB vrši se automatsko kreiranje novog (prvi će biti multiple 1, drugi - multiple 2, treći - multiple 3 itd, dok mi ne zaustavimo hvatanje podataka).
- **Vremensko kreiranje fajla**
  - kreiranje fajla svakih 30s uključujući i veličinu fajla do 10 MB.
- **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 )*.





**Wireshark: Interface Details**

Characteristics | Statistics | 802.3 (Ethernet) | **802.11 (WLAN)** | Task Offload

Current network

SSID (Service Set Identifier) default

BSSID (Basic Service Set Identifier) 00:0E:2E:6E:2F:7D (EdimaxTe)

Network type used 2.4-GHz OFDM

Infrastructure mode Access Point

Authentication mode Open System

Encryption status WEP & TKIP & AES disabled, transmit key available

TX power -

RSSI (Received Signal Strength Indication) -69 dBm

Link Speed 54 Mbits/s

Supported Rates 1/2/5.5/11/6/9/12/18/24/36/48/54 Mbits/s

Desired Rates -

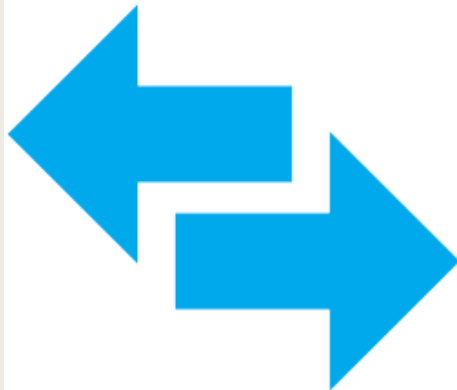
Channel 4 (2427 MHz)

Available networks (BSSID list)

SSID	MAC	Vendor	Privacy	RSSI	Network Type	Infra. Mode	Ch.	Rates	Country
default	00:0E:2E:6E:2F:7D	EdimaxTe	None	-69 dBm	2.4-GHz OFDM	Access Point	4	1/2/5.5/11/6/9/12/18 Mbits/s	

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

15 dBm	32 mW	<b>WLAN snaga transmisije u LAPTOP-u</b>
-10 dBm	100 $\mu$ W	<b>Maksimalna primljena snaga signala u WLAN (802.11 variants)</b>
-100 dBm	0.1 pW	<b>Minimalna primljena snaga signala u WLAN (802.11 variants)</b>
20 dBm	100 mW	<b>EIRP za IEEE 802.11b/g Wireless LAN 20 MHz-kanale na 2.4 GHz</b>



*Poglavlje 3*

*Analiza paketa*

# Primer ethernet frejma

No. -	Time	Source	Destination	Protocol	Info
4	23.227559	1.1.1.1	127.0.0.1	UDP	source port: 55555 destination
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

The screenshot displays the Wireshark interface with a packet list and packet details pane. The packet list shows three packets: packet 9 (FTP Response), packet 10 (FTP Request), and packet 11 (FTP Response). Packet 11 is selected, and its details are shown in the packet details pane. The details pane shows the following information:

- 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)
- Transmission Control Protocol, Src Port: mps-raft (1700), Dst Port: ftp (21), Seq: 47, Ack: 55, Len: 6
  - Source port: mps-raft (1700)
  - Destination port: ftp (21)
  - [Stream index: 1]
  - Sequence number: 47 (relative sequence number)
  - [Next sequence number: 53 (relative sequence number)]
  - Acknowledgement number: 55 (relative ack number)
  - Header length: 20 bytes
  - Flags: 0x18 (PSH, ACK)
    - 0... .... = Congestion Window Reduced (CWR): Not set
    - .0.. .... = ECN-Echo: Not set
    - ..0. .... = Urgent: Not set
    - ...1 .... = Acknowledgement: Set
    - .... 1... = Push: Set
    - .... .0.. = Reset: Not set
    - .... ..0. = Syn: Not set
    - .... ...0 = Fin: Not set
  - Window size: 16945
  - Checksum: 0x8b8d [validation disabled]
    - [Good Checksum: False]
    - [Bad Checksum: False]
  - [SEQ/ACK analysis]
    - [\[This is an ACK to the segment in frame: 9\]](#)
    - [The RTT to ACK the segment was: 0.057617000 seconds]
    - [Number of bytes in flight: 6]
- File Transfer Protocol (FTP)

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

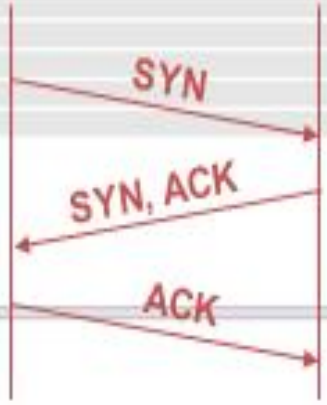
(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.100	10.40.41.2	ICMP	Echo (ping) request
2	2.183304	192.168.2.100	10.40.41.2	ICMP	Echo (ping) request
3	3.430100	192.168.2.100	212.150.49.10	DNS	Standard query A ww.ynet.co.il
4	3.457181	212.150.49.10	192.168.2.100	DNS	Standard query response CNAME ynet.co.il.d4p.net CNAME a39.g.
5	3.461602	192.168.2.100	212.150.49.10	DNS	Standard query A ww.lenovo.com
6	3.621867	192.168.2.100	212.143.162.157	TCP	dzdaemon > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 TSV
7	3.728385	212.143.162.157	192.168.2.100	TCP	http > dzdaemon [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=145
8	3.728429	192.168.2.100	212.143.162.157	TCP	dzdaemon > http [ACK] Seq=1 Ack=1 Win=128480 Len=0
9	3.728839	192.168.2.100	212.143.162.157	HTTP	GET / HTTP/1.1
10	3.768896	212.143.162.157	192.168.2.100	TCP	http > dzdaemon [ACK] Seq=1 Ack=580 Win=6948 Len=0
11	3.770703	212.143.162.157	192.168.2.100	HTTP	HTTP/1.0 301 Moved Permanently
12	3.772411	192.168.2.100	212.143.162.157	HTTP	GET /home/D.7340.L=8.00.html HTTP/1.1

- # Frame 5 (74 bytes on wire, 74 bytes captured)
- # Ethernet II, Src: IntelCor\_a2:d8:9a (00:1c:bf:a2:d8:9a), Dst: EdimaxTe\_6e:2f:7d (00:0e:2e:6e:2f:7d)
- # Internet Protocol, Src: 192.168.2.100 (192.168.2.100), Dst: 212.150.49.10 (212.150.49.10)
- # User Datagram Protocol, Src Port: natuslink (2895), Dst Port: domain (53)
- # Domain Name System (query)



```

0000  00 0e 2e 6e 2f 7d 00 1c bf a2 d8 9a 08 00 45 00  ...n/)... ..E.
0010  00 3c 7f ea 00 00 80 11 f2 19 c0 a8 02 64 d4 96  .c.....d..
0020  31 0a 0b 4f 00 35 00 28 f5 df 9e d7 01 00 00 01  1..0.S.{ .....
0030  00 00 00 00 00 00 03 77 77 77 06 6c 65 6e 6f 76  ....ww ww.lenov
0040  6f 03 63 6f 6d 00 00 01 00 01                   o.com... ..
  
```

# 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.

The screenshot shows the Wireshark interface with the 'Flow Graph' dialog box open. The dialog box has three sections: 'Choose packets', 'Choose flow type', and 'Choose node address type'. The 'All packets' radio button is selected under 'Choose packets'. Under 'Choose flow type', the 'General flow' radio button is selected. Under 'Choose node address type', the 'Standard source/destination addresses' radio button is selected. The 'OK' and 'Cancel' buttons are at the bottom of the dialog box. A red arrow points from the 'Flow Graph...' menu item in the Statistics menu to the dialog box.

Example 001.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Summary  
Protocol Hierarchy  
Conversations  
Endpoints  
Packet Lengths...  
IO Graphs  
Conversation List  
Endpoint List  
Service Response Time  
BOOTP-DHCP...  
Compare...  
Flow Graph...  
HTTP  
IP Addresses...  
IP Destinations...  
IP Protocol Types...  
ONC-RPC Programs  
TCP Stream Graph  
UDP Multicast Streams  
WLAN Traffic...

Filter:

No. -	Time
1	0.000000
2	2.183304
3	3.430100
4	3.457181
5	3.461602
6	3.623867
7	3.728385
8	3.728429
9	3.728839
10	3.768896
11	3.770703
12	3.772411

Destination Protocol Info

Destination	Protocol	Info
10.40.41.2	ICMP	Echo (ping) request
10.40.41.2	ICMP	Echo (ping) request
212.150.49.10	DNS	Standard query A www.y.net
192.168.2.100	DNS	Standard query response C
212.150.49.10	DNS	Standard query response C
212.143.162.157	DNS	Standard query response C
192.168.2.100	DNS	Standard query response C
212.143.162.157	DNS	Standard query response C
212.143.162.157	DNS	Standard query response C
192.168.2.100	DNS	Standard query response C
192.168.2.100	DNS	Standard query response C
212.143.162.157	DNS	Standard query response C

Expression... Clear Apply

Wireshark: Flow Graph

Choose packets

All packets  
 Displayed packets

Choose flow type

General flow  
 TCP flow

Choose node address type

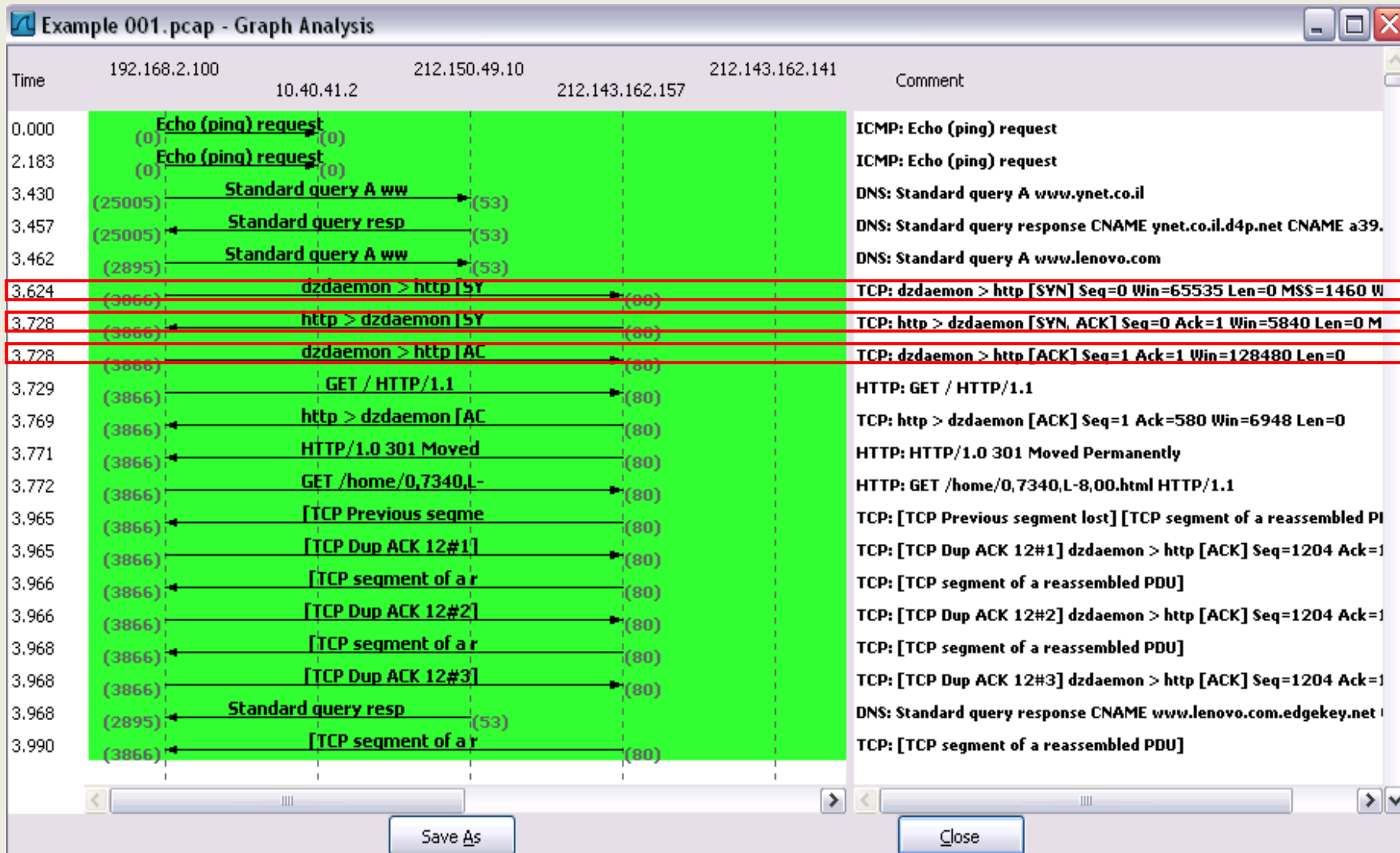
Standard source/destination addresses  
 Network source/destination addresses

OK Cancel



# 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

The image shows a screenshot of the Wireshark network protocol analyzer. The main window displays a packet capture titled "Snif2 --- HTTP Example.cap". The packet list pane shows several packets, with packet 42 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. A context menu is open over packet 42, with the "Follow TCP Stream" option highlighted. A red arrow points from this menu item to the "Follow TCP Stream" dialog box in the foreground.

The "Follow TCP Stream" dialog box shows the stream content, which is an HTTP response. The stream content is displayed in hexadecimal and ASCII format. The ASCII format shows the following text:

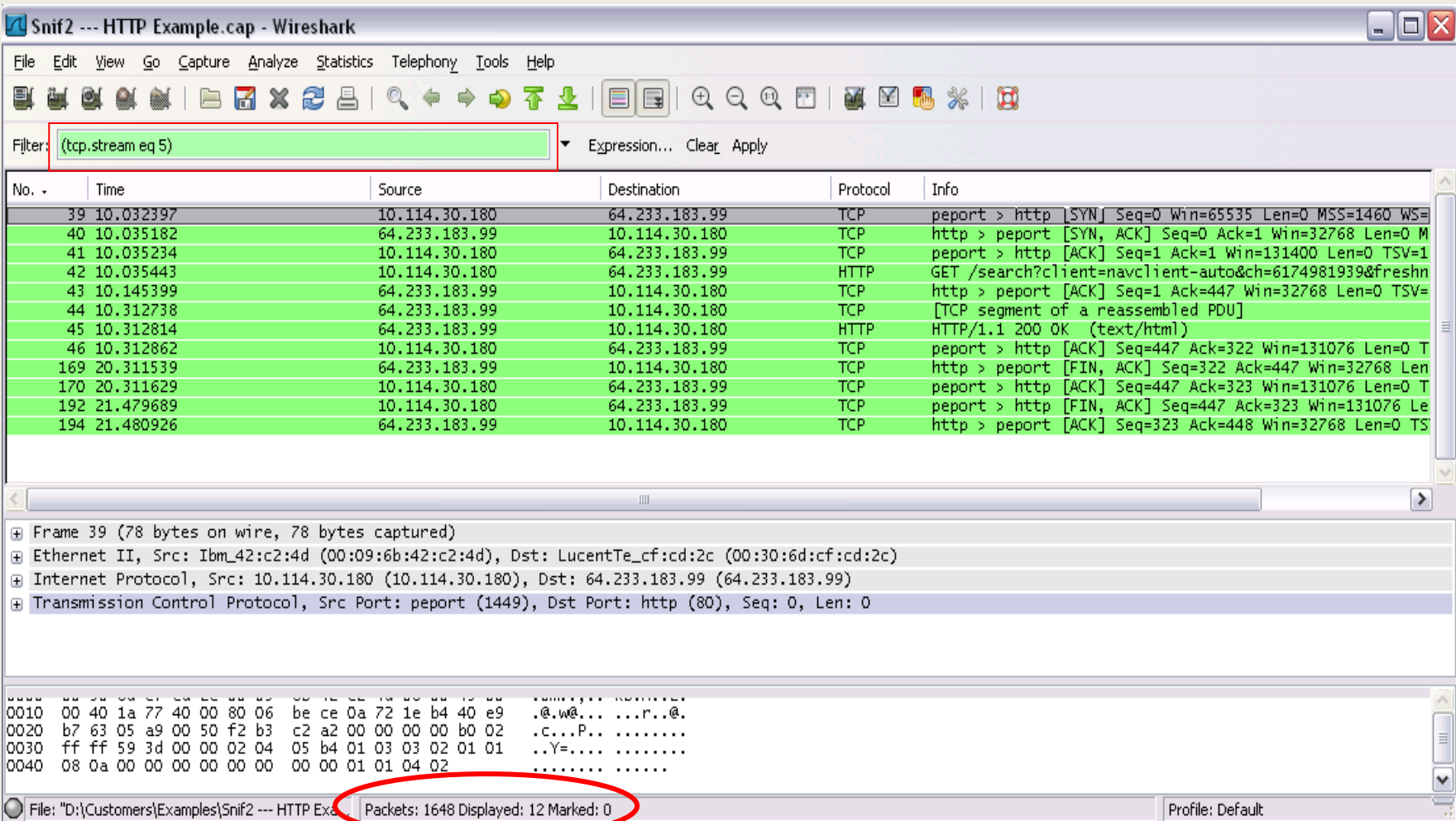
```
GET /search?client=navclient-auto&ch=6174981939&freshness_check=4ilp-GrPqKEX_r_lNxaYw&iqrn=qr4&orig=0J&ie=UTF-8&oe=UTF-8&features=Rank&q=info:http%3A%2F%2Fwww%2Eynet%2Eco%2Eil%2F HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; GoogleToolbar 2.0.114.9-big; Windows XP 5.1)
Host: toolbarqueries.google.com
Cache-Control: no-cache
Cookie: PREF-ID=1a18560743a17669;TB=2;CR=1;TM=1113765996;LM=1119978279;GM=1;S=7NmjkCGkIc845ngM; rememberme=false

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Date: Mon, 11 Jul 2005 08:21:03 GMT
Content-Type: text/html
Cache-Control: private
Server: GWS/2.1
Via: 1.1 cache1 (NetCache NetApp/5.5R2D5), Version 2.0-Build_Linux_1336 $Date: 04/13/2005 15:53:0038$(IWSS), 1.1 cache1 (NetCache NetApp/5.5R2D5)
```

The dialog box also includes a search bar, a "Find" button, and radio buttons for selecting the output format: ASCII, EBCDIC, Hex Dump, C Arrays, and Raw. The "Raw" format is currently selected. The dialog box also has a "Filter Out This Stream" button and a "Close" button.

# Prikaz TCP Stream-a

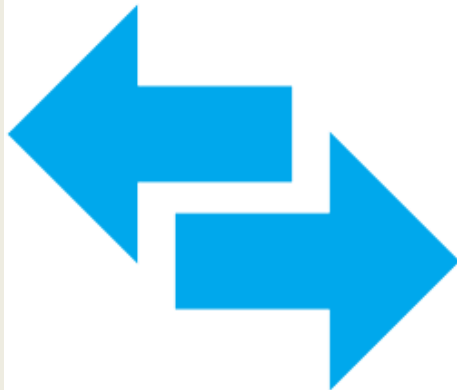
Filter *tcp.strem eq 5* označava peti zabeleženi stream od početka komunikacije.



The screenshot displays the Wireshark interface for a capture file named 'Snif2 --- HTTP Example.cap'. The 'Filter' field is set to '(tcp.strem eq 5)'. The packet list pane shows several packets, with packet 39 highlighted in green. The details pane for packet 39 shows the following layers:

- Frame 39 (78 bytes on wire, 78 bytes captured)
- Ethernet II, Src: IbmL42:c2:4d (00:09:6b:42:c2:4d), Dst: LucentTe\_cf:cd:2c (00:30:6d:cf:cd:2c)
- Internet Protocol, Src: 10.114.30.180 (10.114.30.180), Dst: 64.233.183.99 (64.233.183.99)
- Transmission Control Protocol, Src Port: peport (1449), Dst Port: http (80), Seq: 0, Len: 0

The packet bytes pane shows the raw data for the selected packet, with the first four bytes (0010 0040 1a77 4000) circled in red. The status bar at the bottom indicates 'Packets: 1648 Displayed: 12 Marked: 0'.

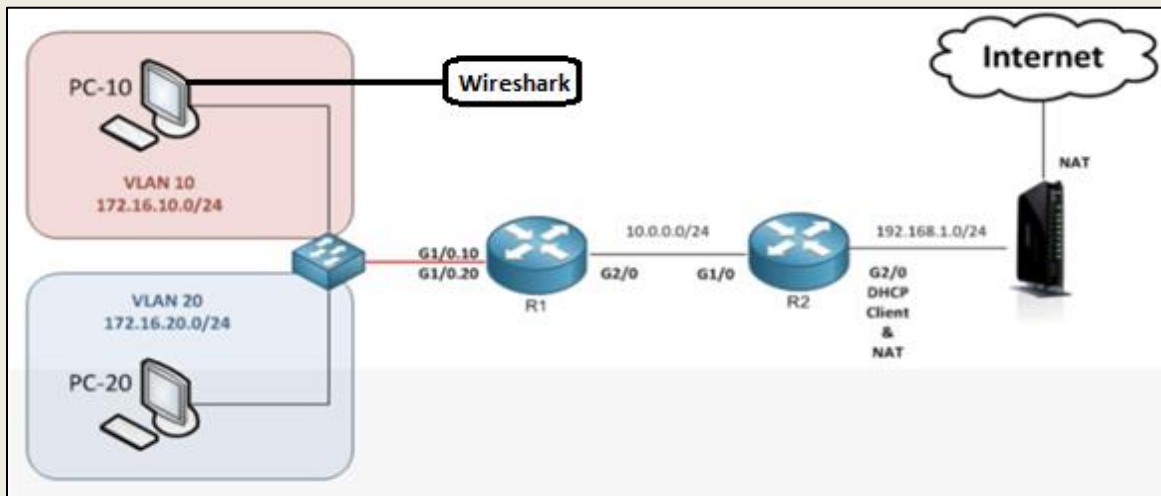


*Poglavlje 4*

***Lokacija analizatora paketa***

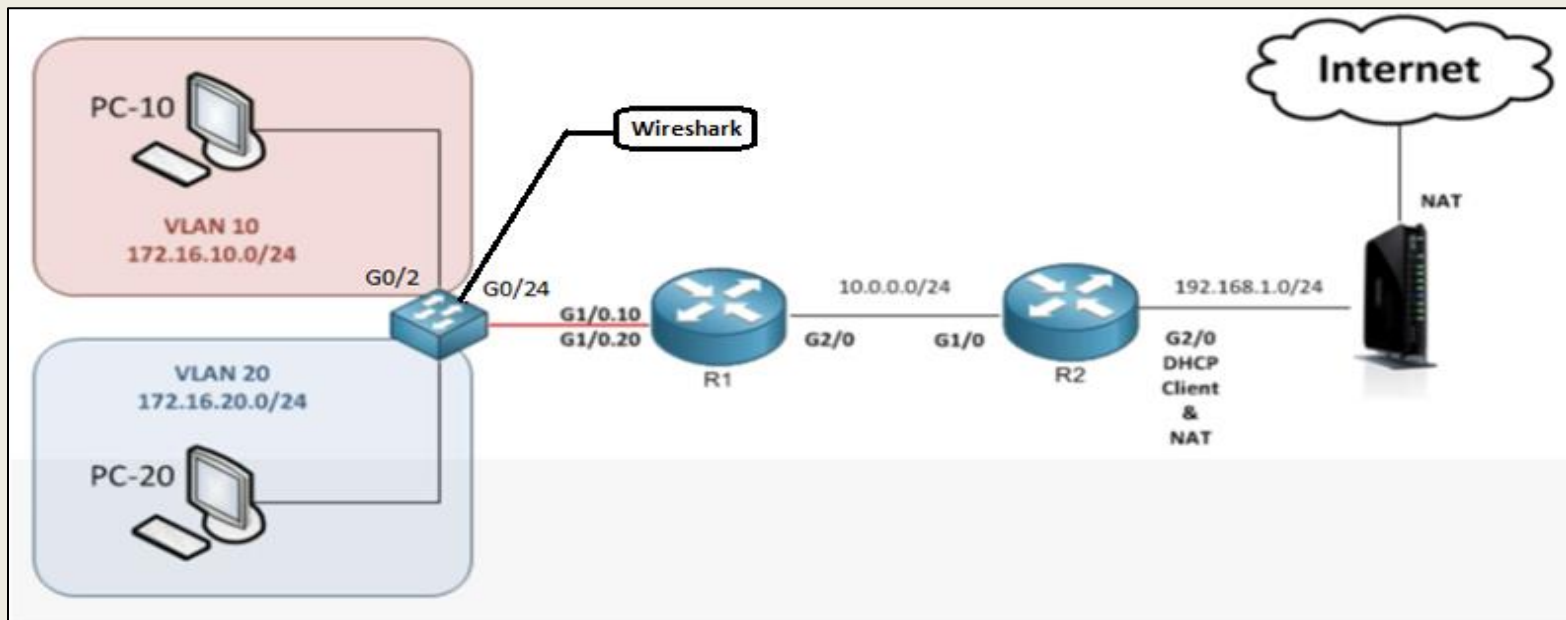
# Controlling The Capture - Kontrola uhvaćenih podataka

- 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

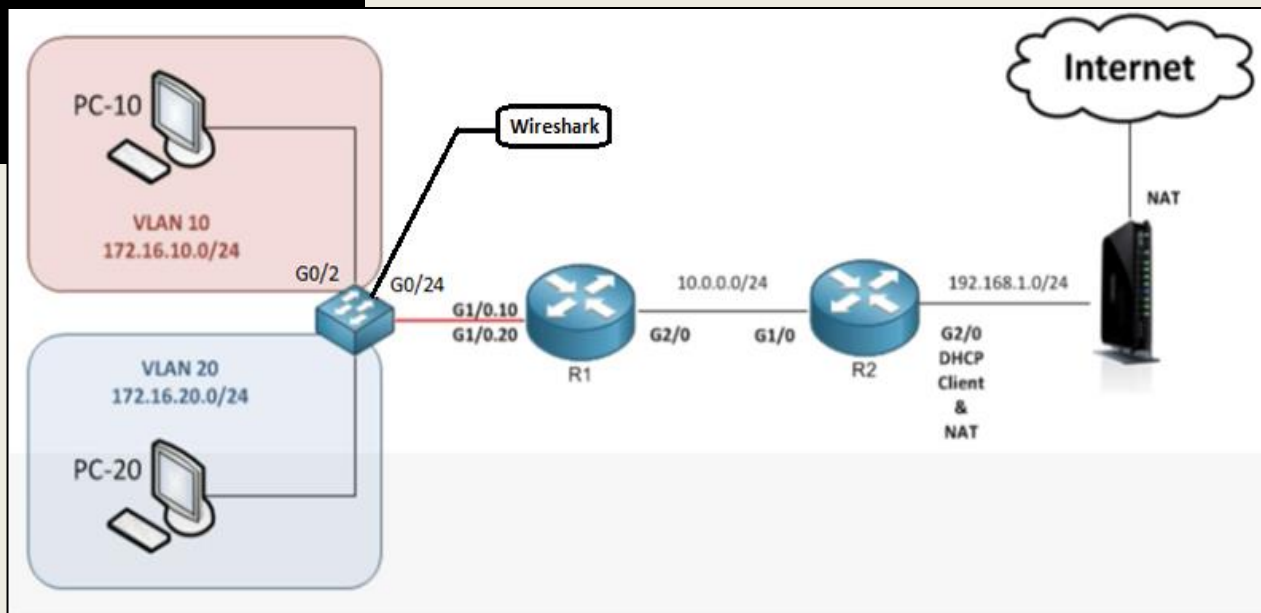
- Prethodna opcija nije jedina opcija za prihvatanje podataka na PC-10. Može se takođe izvršiti opcija Port Mirroring (koristi se na Switch-u da pošalje kopiju mrežnih paketa koje vidi sa jednog na drugi port ), naravno ako Switch podržava ovu opciju.
- Ako imamo port G0/2 na koji je korisnik konektovan,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

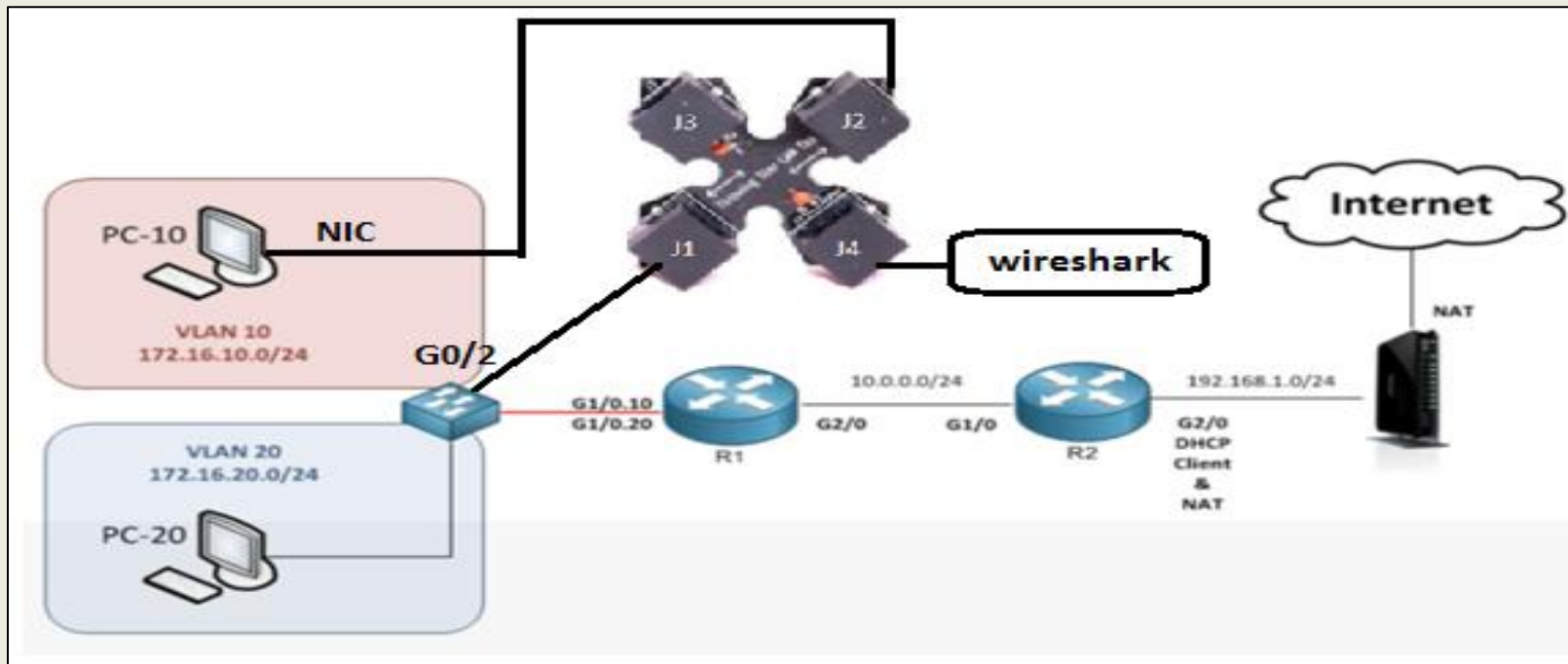
```
3560_Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
3560_Switch(config)#
3560_Switch(config)#monitor session 1 source int g0/2 both
3560_Switch(config)#
3560_Switch(config)#monitor session 1 destination int g0/24
3560_Switch(config)#
3560_Switch(config)#
3560_Switch(config)#do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

3560_Switch(config)#
```

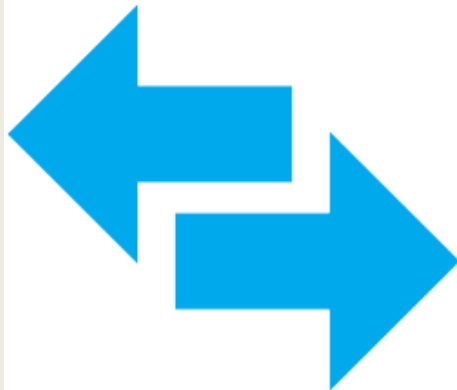


# Tap (internet TAP) :

- Ako Switch ne podržava Port Mirroring funkciju postoji i opcija Tap (Internet TAP). Prikazan je TAP sa 4 konektora :
- Vršiti 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

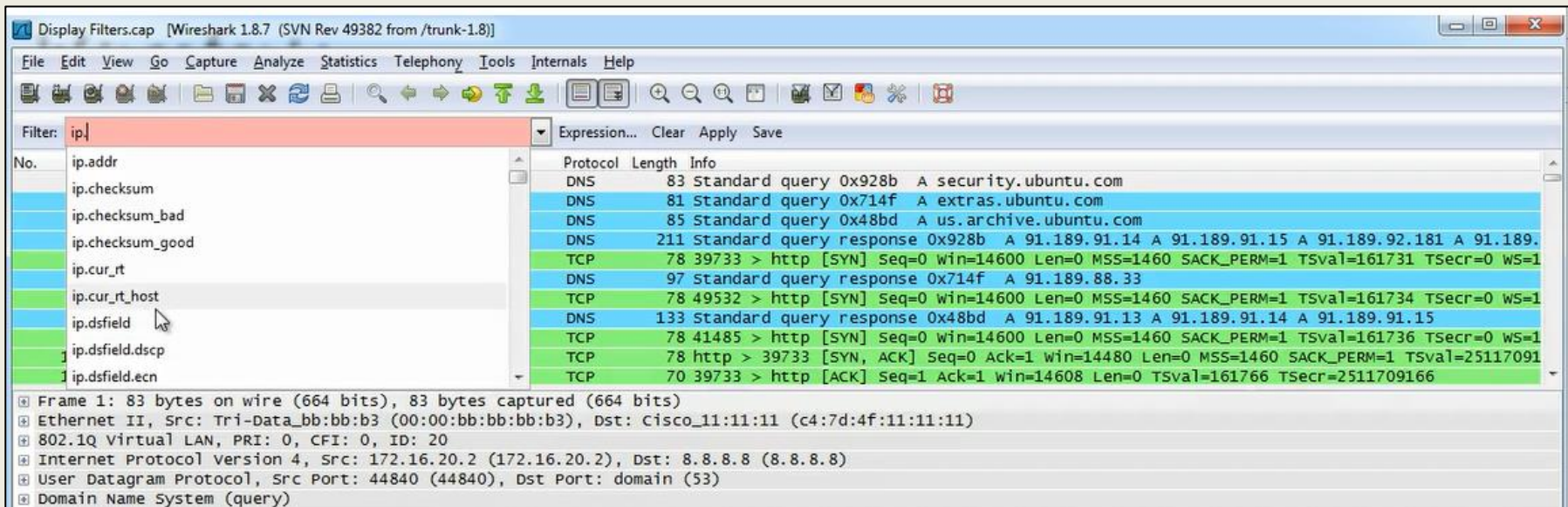
- Snimanje fajlova može biti velike sadržine i imati na hiljade razgovora u mreži
- Koristeći **Display Filter** u **WireShark** možemo da odredimo koji paket da se prikaže, što nam pomaže da se fokusiramo na određeni prenos (saobraćaj).
- Mogu se filtrirati protokoli, aplikacije, adrese itd.
- Koristimo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



Display Filters.cap [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip| Expression... Clear Apply Save

No.	Filterable Field	Protocol	Length	Info
	ip.addr			
	ip.checksum	DNS	83	Standard query 0x928b A security.ubuntu.com
	ip.checksum_bad	DNS	81	Standard query 0x714f A extras.ubuntu.com
	ip.checksum_good	DNS	85	Standard query 0x48bd A us.archive.ubuntu.com
	ip.cur_rt	DNS	211	Standard query response 0x928b A 91.189.91.14 A 91.189.91.15 A 91.189.92.181 A 91.189.92.182
	ip.cur_rt_host	TCP	78	39733 > http [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=161731 TSecr=0 WS=1
	ip.dsfield	DNS	97	Standard query response 0x714f A 91.189.88.33
	ip.dsfield.dscp	TCP	78	49532 > http [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=161734 TSecr=0 WS=1
	ip.dsfield.ecn	DNS	133	Standard query response 0x48bd A 91.189.91.13 A 91.189.91.14 A 91.189.91.15
		TCP	78	41485 > http [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=161736 TSecr=0 WS=1
		TCP	78	http > 39733 [SYN, ACK] Seq=0 Ack=1 win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=25117091
		TCP	70	39733 > http [ACK] Seq=1 Ack=1 win=14608 Len=0 TSval=161766 TSecr=2511709166

Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)  
Ethernet II, Src: Tri-Data\_bb:bb:b3 (00:00:bb:bb:b3), Dst: Cisco\_11:11:11 (c4:7d:4f:11:11:11)  
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20  
Internet Protocol Version 4, Src: 172.16.20.2 (172.16.20.2), Dst: 8.8.8.8 (8.8.8.8)  
User Datagram Protocol, Src Port: 44840 (44840), Dst Port: domain (53)  
Domain Name System (query)

# 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**.

The screenshot shows the Wireshark interface with a packet capture of an IPv6 multicast group announcement. The packet list pane shows several packets, with the first one (No. 1) circled in red. The packet details pane for the selected packet shows the following information:

Frame 1: 84 bytes on interface (672 bits) captured (672 bits) on interface 0
Ethernet II, Src: Intel E80000000000, Dst: Intel 701364001000
Internet Protocol Version 6, Src: fe80::4148:7ac8:376c:9d68, Dst: ff02::1:3
User Datagram Protocol, Src Port: 5355, Dst Port: 11mnr (5355)
LLMNR
Standard query 0xfb2e A wpad

The packet bytes pane shows the following data:

```
dd 60 00 33 ..... .ds..
00 41 48 ..... AH
00 00 00 z.71.h.....
c7 fb 2e .....
61 64 00 ..... wpad.
....
```

The 'Apply as Filter' menu is open, and the 'Not Selected' option is highlighted. The 'Filter' field at the top of the interface is empty.

- 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.

Quickstart Capture.pcapng [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **!ipv6** Expression... Clear Apply Save

No.	Time	Source	Destination	Length	Protocol	Info
2	0.00009300	192.168.56.1	224.0.0.252	64	LLMNR	Standard query 0xfb2e A wpad
3	0.20054300	192.168.56.1	192.168.56.255	92	NBNS	Name query NB WPAD<00>
4	0.22336300	10.0.0.7	239.255.255.250	469	SSDP	NOTIFY * HTTP/1.1
5	0.23896000	10.0.0.7	239.255.255.250	478	SSDP	NOTIFY * HTTP/1.1
6	0.39619500	10.0.0.7	239.255.255.250	521	SSDP	NOTIFY * HTTP/1.1
7	0.48246100	10.0.0.7	239.255.255.250	535	SSDP	NOTIFY * HTTP/1.1
8	0.52141600	10.0.0.7	239.255.255.250	533	SSDP	NOTIFY * HTTP/1.1
9	0.59921900	10.0.0.7	239.255.255.250	549	SSDP	NOTIFY * HTTP/1.1
10	0.95097300	192.168.56.1	192.168.56.255	92	NBNS	Name query NB WPAD<00>
11	1.70136400	192.168.56.1	192.168.56.255	92	NBNS	Name query NB WPAD<00>
12	2.22340300	10.0.0.7	239.255.255.250	469	SSDP	NOTIFY * HTTP/1.1

Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0

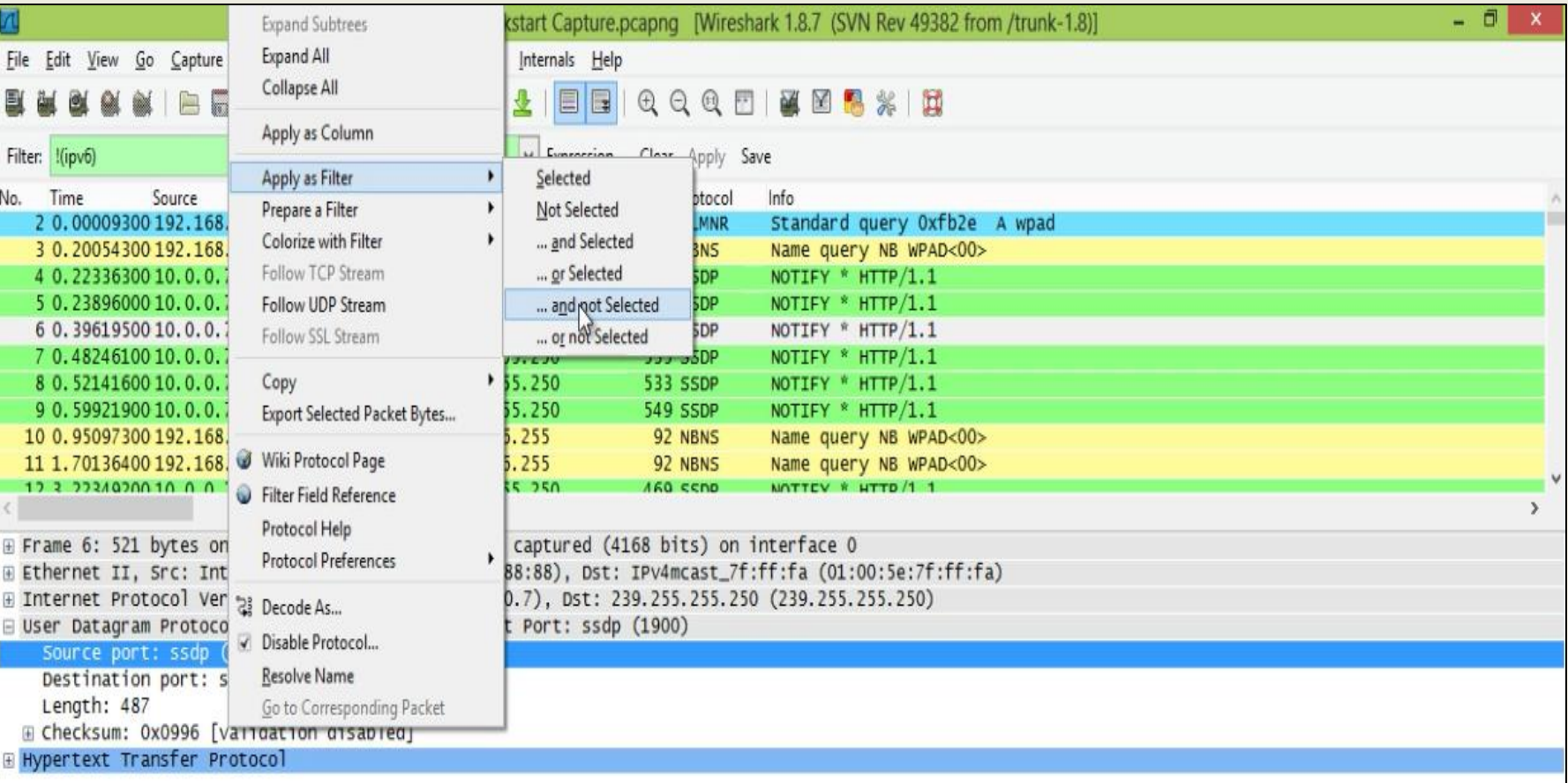
- Ethernet II, Src: cadmusCo\_00:64:73 (08:00:27:00:64:73), Dst: IPv4mcast\_00:00:fc (01:00:5e:00:00:fc)
- Internet Protocol Version 4, Src: 192.168.56.1 (192.168.56.1), Dst: 224.0.0.252 (224.0.0.252)
- User Datagram Protocol, Src Port: 57080 (57080), Dst Port: llmnr (5355)
- Link-local Multicast Name Resolution (query)

```

0000  01 00 5e 00 00 fc 08 00 27 00 64 73 08 00 45 00  ..^.....'.ds..E.
0010  00 32 02 e8 00 00 01 11 dd 2d c0 a8 38 01 e0 00  .2.....-.8...
0020  00 fc de f8 14 eb 00 1e 5e 1d fb 2e 00 00 00 01  .....^.....
0030  00 00 00 00 00 00 04 77 70 61 64 00 00 01 00 01  .....w pad.....
  
```

File: "C:\Users\Keith\Documents\My Captures\Quickstart Capture.pcapng" 824 KB 00:00:48 Packets: 1170 Displayed: 1165 Marked: 0 Load time: 0:00:062 Profile: Default

- Pored paketa vezanih za ipv6 protokol želimo da izostavimo analiziranje i sdp paketa.
- Proširenjem User Datagram Protocol-a i odabiranjem izvršnog porta source port : sdp ( 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

Quickstart Capture.pcapng [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **!(ipv6) && !(udp.srcport == 1900)** Expression... Clear Apply Save

No.	Time	Source	Destination	Length	Protocol	Info
2	0.00009300	192.168.56.1	224.0.0.252	64	LLMNR	Standard query 0xfb2e A wpad
3	0.20054300	192.168.56.1	192.168.56.255	92	NBNS	Name query NB WPAD<00>
10	0.95097300	192.168.56.1	192.168.56.255	92	NBNS	Name query NB WPAD<00>
11	1.70136400	192.168.56.1	192.168.56.255	92	NBNS	Name query NB WPAD<00>
24	8.51442600	Cisco_11:11:11	Cisco_11:11:11	60	LOOP	Reply
25	9.15344600	IntelCor_88:88:88	Broadcast	42	ARP	who has 10.0.0.1? Tell 10.0.0.7
26	9.17483000	Cisco_11:11:11	IntelCor_88:88:88	60	ARP	10.0.0.1 is at c4:7d:4f:11:11:11
29	17.78071400	10.0.0.7	8.8.8.8	74	DNS	Standard query 0x3cfb A cbtnuggets.com
30	18.05109100	8.8.8.8	10.0.0.7	90	DNS	Standard query response 0x3cfb A 54.225.173.254
31	18.05156800	10.0.0.7	54.225.173.254	66	TCP	49525 > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
32	18.05182200	10.0.0.7	54.225.173.254	66	TCP	49526 > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 3: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

- Ethernet II, Src: CadmusCo\_00:64:73 (08:00:27:00:64:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.56.1 (192.168.56.1), Dst: 192.168.56.255 (192.168.56.255)
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
  - Source port: netbios-ns (137)
  - Destination port: netbios-ns (137)
  - Length: 58
  - Checksum: 0x0683 [validation disabled]
- NetBIOS Name Service

```

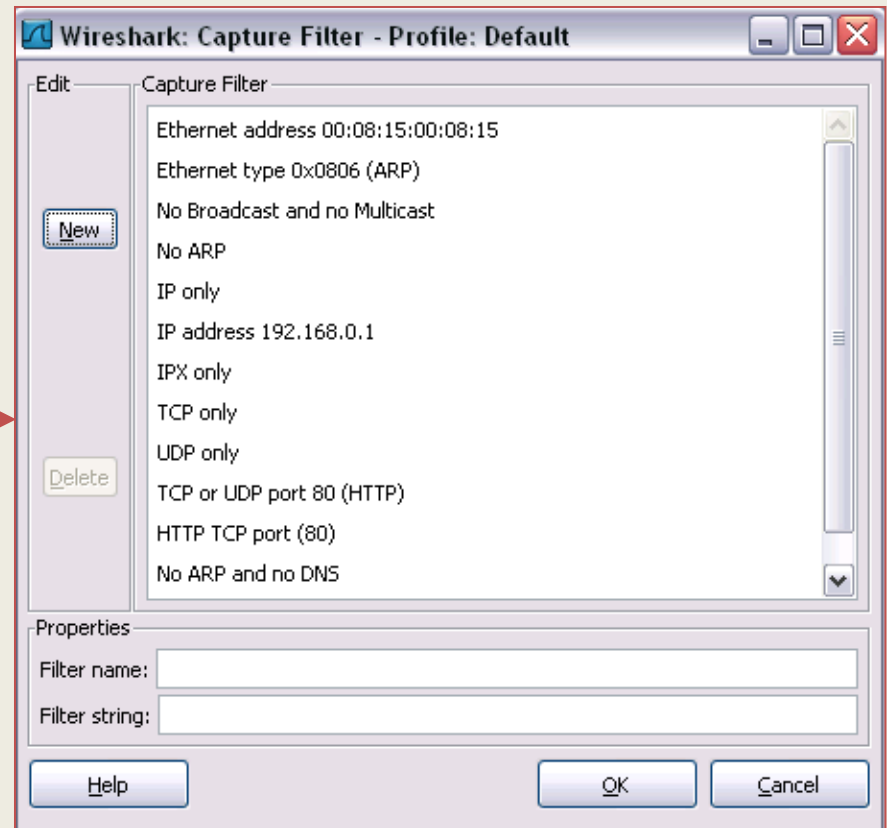
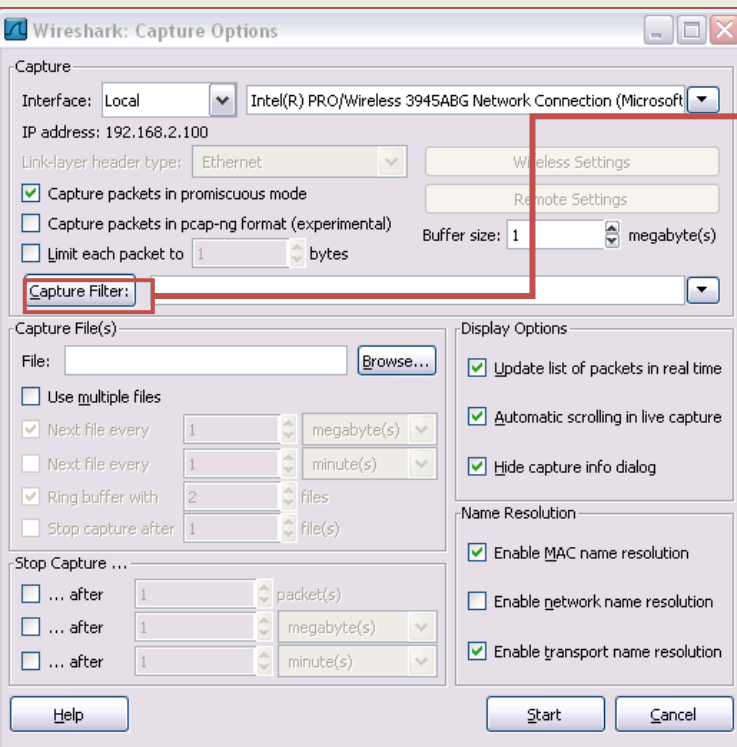
0000  ff ff ff ff ff ff 08 00 27 00 64 73 08 00 45 00  .....'.ds..E.
0010  00 4e 02 e9 00 00 80 11 45 65 c0 a8 38 01 c0 a8  .N.....Ee..8...
0020  38 ff 00 89 00 89 00 3a 06 83 c4 25 01 10 00 01  8.....:..%....
0030  00 00 00 00 00 00 20 46 48 46 41 45 42 45 45 43  .....F HFAEBEEC
0040  41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43  ACACACAC ACACACAC
0050  41 43 41 43 41 41 41 00 00 20 00 01             ACACAAA. ...

```

File: "C:\Users\Keith\Documents\My Captures\Quickstart Capture.pcapng" 824 KB 00:00:48 Packets: 1170 Displayed: 1147 Marked: 0 Load time: 0:00:046 Profile: Default

# Izbor dostupnih filtera

Capture → Interfaces → Options:





# Primena filtera (ekspresija)

The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture for 'Example 003.pcap'. The packet list pane shows several packets, with packet 485 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol, and Transmission Control Protocol. A red box highlights the 'Expression...' button in the filter bar. A second dialog box, 'Wireshark: Filter Expression - Profile: Default', is open, showing a list of field names, a relation dropdown set to 'is present', and a value input field. The field name 'message/http - Media Type: message/http' is selected. The dialog also includes a 'Predefined values' section and an 'OK' button.

Example 003.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:  Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
485	47.639995	192.168.2.100	212.143.162.152	TCP	17231 http [FIN, ACK] Seq=1409 Ack=380 Win=12810
486	47.649881	192.168.2.100	212.143.162.152	TCP	17241 http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
487	47.666485	212.143.162.152	192.168.2.100	TCP	17237 http > [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
488	47.666530	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
489	47.666898	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
490	47.667431	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
491	47.675090	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
492	47.675136	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
493	47.677582	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
494	47.677624	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
495	47.677858	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
496	47.695323	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
497	47.697056	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
498	47.737850	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
499	47.739896	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
500	47.788636	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
501	47.797761	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
502	47.826481	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
503	47.826527	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
504	47.826913	192.168.2.100	212.143.162.152	TCP	17237 http > [ACK] Seq=1409 Ack=1 Win=0 Len=0
505	47.839189	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
506	47.841074	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
507	47.856460	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0
508	47.858425	212.143.162.152	192.168.2.100	TCP	17237 http > [ACK] Seq=0 Ack=1 Win=0 Len=0

Wireshark: Filter Expression - Profile: Default

Field name

- Mesh - Mesh Header
- message/http - Media Type: message/http
- Messenger - Microsoft Messenger Service
- MGCP - Media Gateway Control Protocol
- MGMT - DCE/RPC Remote Management
- MIKEY - Multimedia Internet KEYing
- MIME multipart - MIME Multipart Media Encapsulation
- MIOP - Unreliable Multicast Inter-ORB Protocol
- MIPv6 - Mobile IPv6 / Network Mobility
- MMS - MMS
- MMSE - MMS Message Encapsulation
- Mobile IP - Mobile IP
- Modbus/TCP - Modbus/TCP

Relation

- is present
- ==
- !=
- >
- <
- >=
- <=
- contains
- matches

Value (character string)

Predefined values:

Range (offset:length)

OK Cancel

# Primeri :

- ✓ Snimanje saobraćaja isključivo sa adrese 172.18.5.4
  - **host 172.18.5.4**
- ✓ Snimanje saobraćaja isključivo 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 :

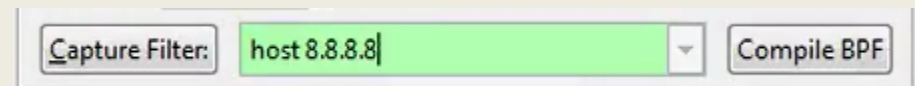
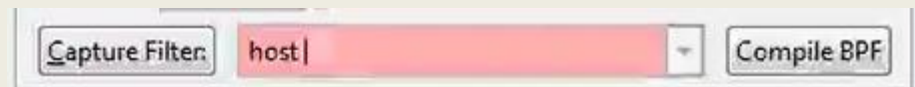
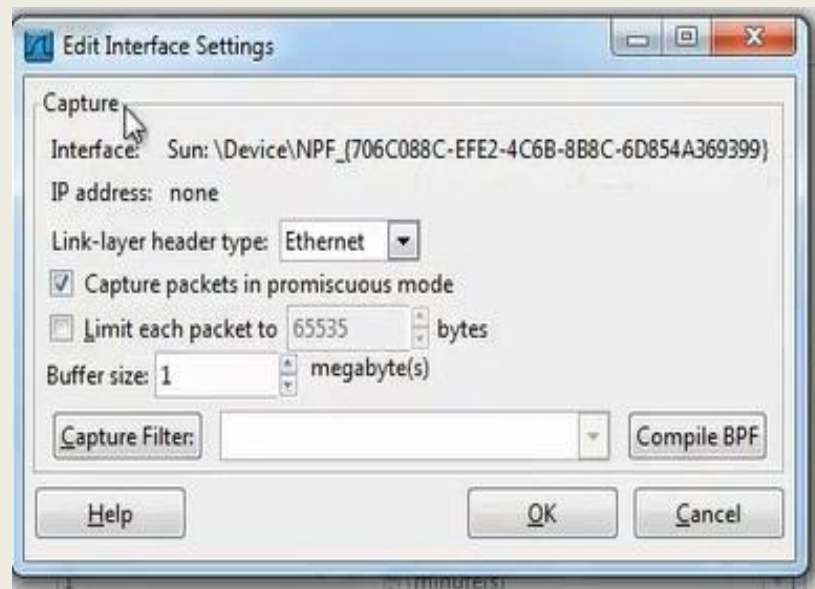
- ✓ **Snimanje svega osim ARP i DNS saobraćaja**
  - port not 53 and not arp
- ✓ **Snimanje saobraćaja u opsegu određenih portova**
  - (tcp[2:2] > 1500 and tcp[2:2] < 1550) or (tcp[4:2] > 1500 and tcp[4:2] < 1550)
  - tcp portrange 1501-1549
- ✓ **Snimanje isključivo IP saobraćaja**
  - (najkraći filter 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 adres),
  - port itd u zavisnosti šta želimo da snimimo

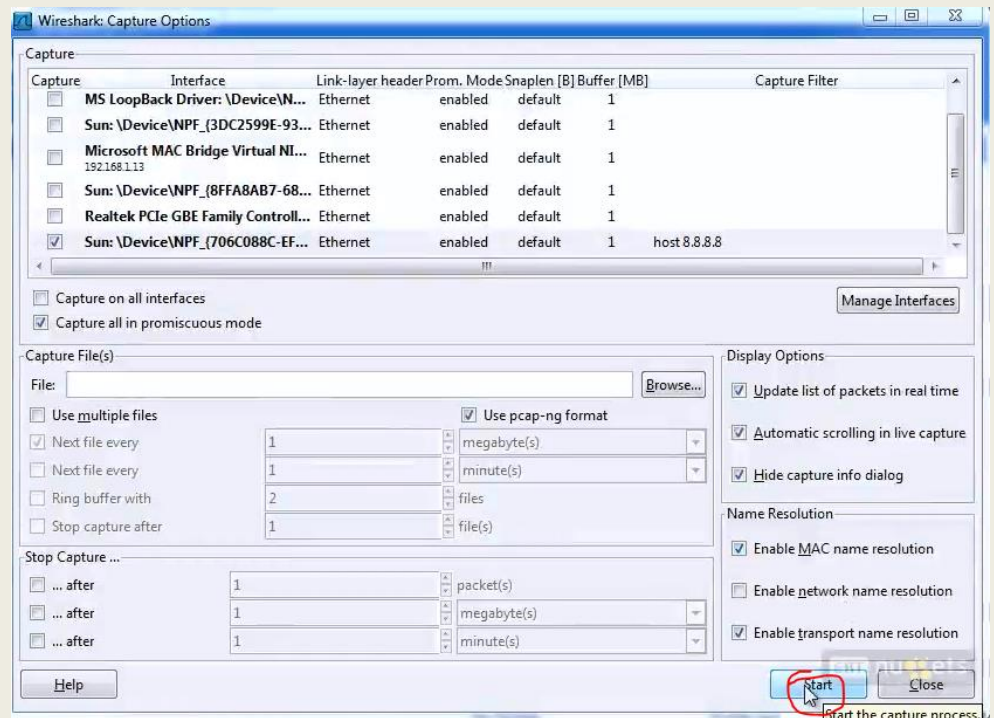
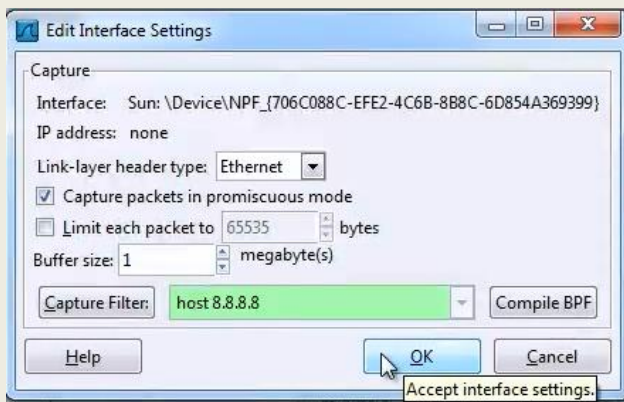
# Capture Filter

- Otvora 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.



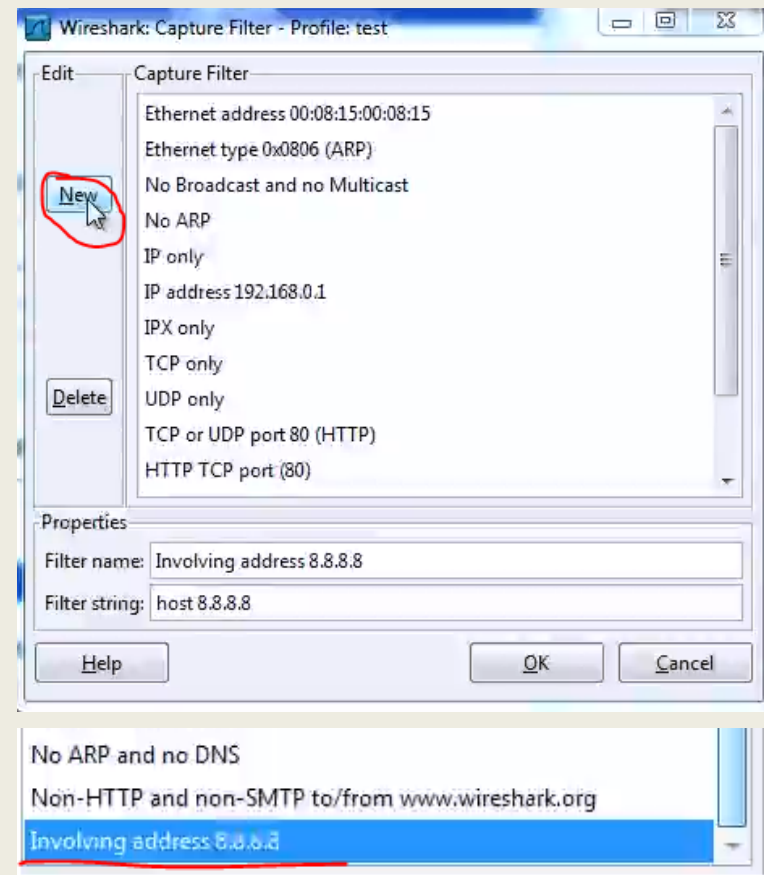
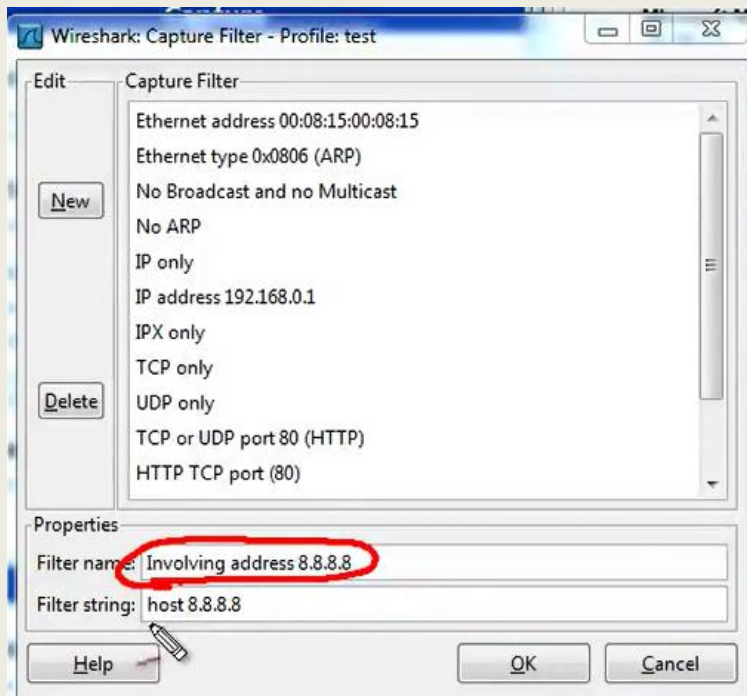
# Capture Filter - Primer

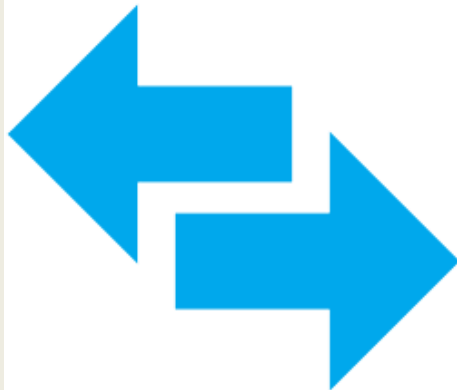
- Koristimo adresu Google-a koju unosimo u polje Capture filter koristeći sintaksu host 8.8.8.8.



# 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

The screenshot shows the Wireshark interface with the 'File' menu open and the 'Save As...' option selected. The packet list shows several packets, with the one at frame 1335 selected. The 'Wireshark: Save file as' dialog box is open, showing the file name 'Wireshark/tcpdump/... - libpcap (\*.pcap;\*.cap)' and the 'Packet Range' section.

**Packet Range**

	<input type="radio"/> Captured	<input checked="" type="radio"/> Displayed
<input checked="" type="radio"/> All packets	5694	23
<input type="radio"/> Selected packet	1	1
<input type="radio"/> Marked packets	0	0
<input type="radio"/> First to last marked	0	0
<input type="radio"/> Range: <input type="text"/>	0	0

# Izvoženje u CSV datoteku

The image shows the Wireshark interface with the 'File' menu open and the 'Export' option selected. A red box highlights the 'Export' menu item, and a red arrow points from it to the 'Wireshark: Export File' dialog box. The dialog box shows the file name 'Example 006a 01' and the save type 'CSV (Comma Separated Values summary) (\*.csv)'. The 'Packet Range' section is set to 'All packets' (23 captured, 23 displayed). The 'Packet Format' section has 'Packet summary line' and 'Packet details' checked, and 'As displayed' selected in the dropdown.

**Wireshark: Export File**

Save in: Freeware

File name: Example 006a 01

Save as type: CSV (Comma Separated Values summary) (\*.csv)

Packet Range:

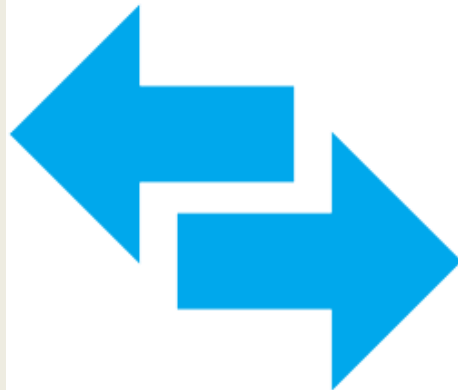
	Captured	Displayed
<input checked="" type="radio"/> All packets	23	23
<input type="radio"/> Selected packet	1	1
<input type="radio"/> Marked packets	0	0
<input type="radio"/> First to last marked	0	0
<input type="radio"/> Range: <input type="text"/>	0	0

Packet Format:

- Packet summary line
- Packet details: As displayed
- Packet Bytes
- Each packet on a new page

# Prikaz izvezena 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

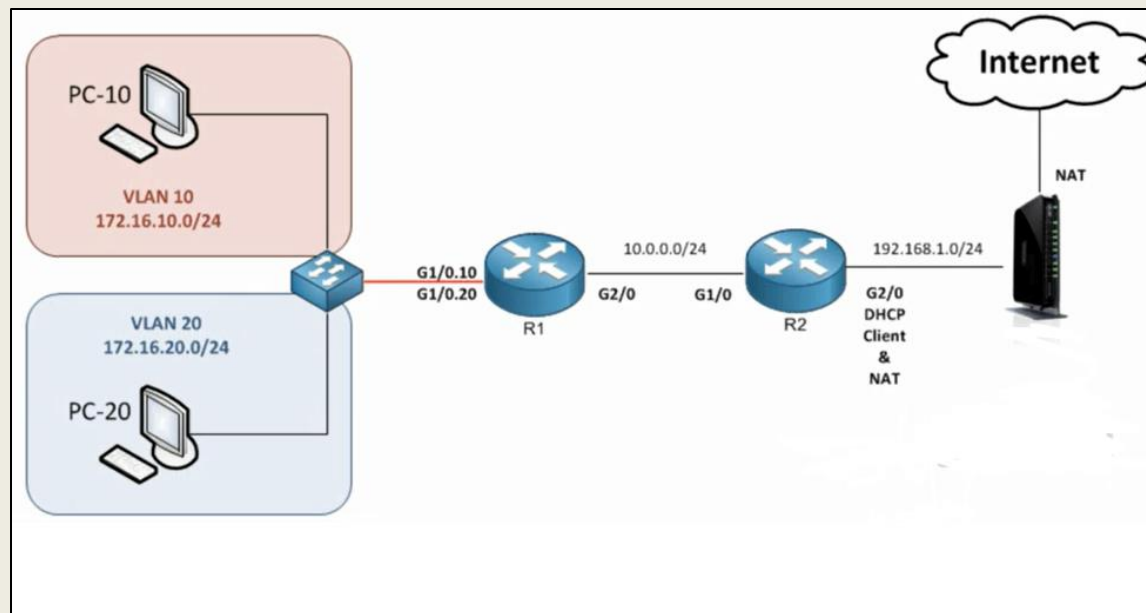


*Poglavlje 6*

***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.

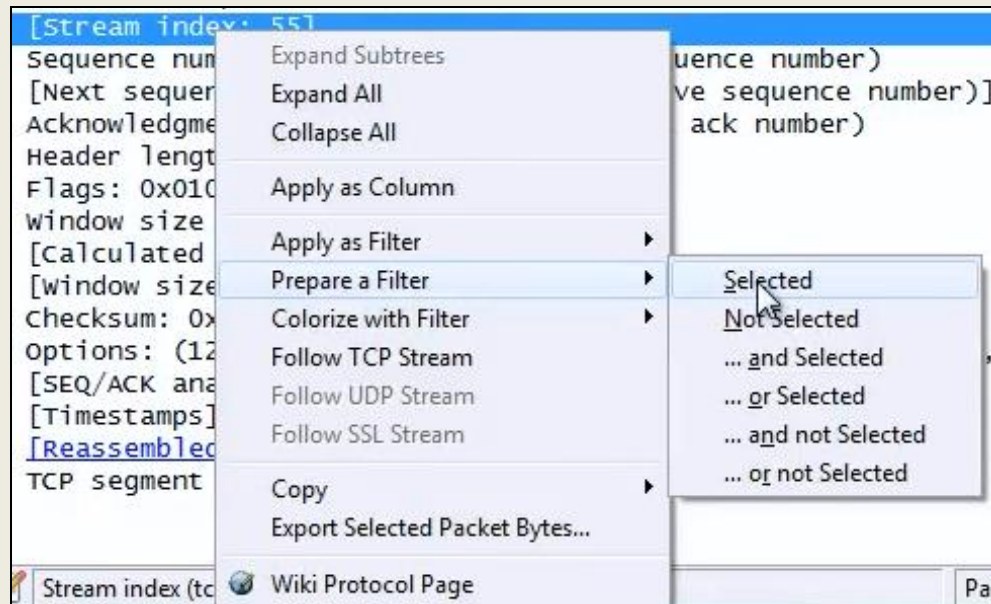
No.	Destination	Source	Protocol	Info
3253	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]
3254	2.19.135.148	172.16.20.2	TCP	43709 > http [ACK] Seq=2934 Ack=113474 win=54064 Len=0 TSval=180801 TSecr=2238357618
3255	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]
3256	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]
3257	2.19.135.148	172.16.20.2	TCP	43709 > http [ACK] Seq=2934 Ack=116370 win=54064 Len=0 TSval=180807 TSecr=2238357623
3258	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]
3259	172.16.20.2	2.19.135.148	HTTP	HTTP/1.1 200 OK (PNG)
3260	2.19.135.148	172.16.20.2	TCP	43709 > http [ACK] Seq=2934 Ack=117994 win=54832 Len=0 TSval=180812 TSecr=2238357630
3261	2.19.135.148	172.16.20.2	HTTP	GET /shared/framework/img/global/rss_icon_24x25.png HTTP/1.1
3262	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]

Frame 3256: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)
Ethernet II, Src: Cisco_11:11:11 (c4:7d:4f:11:11:11), Dst: Tri-Data_bb:bb:b3 (00:00:bb:bb:bb:b3)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20
Internet Protocol Version 4, Src: 2.19.135.148 (2.19.135.148), Dst: 172.16.20.2 (172.16.20.2)
Transmission Control Protocol, Src Port: http (80), Dst Port: 43709 (43709), Seq: 114922, Ack: 2934, Len: 1448
Source port: http (80)
Destination port: 43709 (43709)
[Stream index: 55]
Sequence number: 114922 (relative sequence number)
[Next sequence number: 116370 (relative sequence number)]
Acknowledgment number: 2934 (relative ack number)
Header length: 32 bytes

# 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

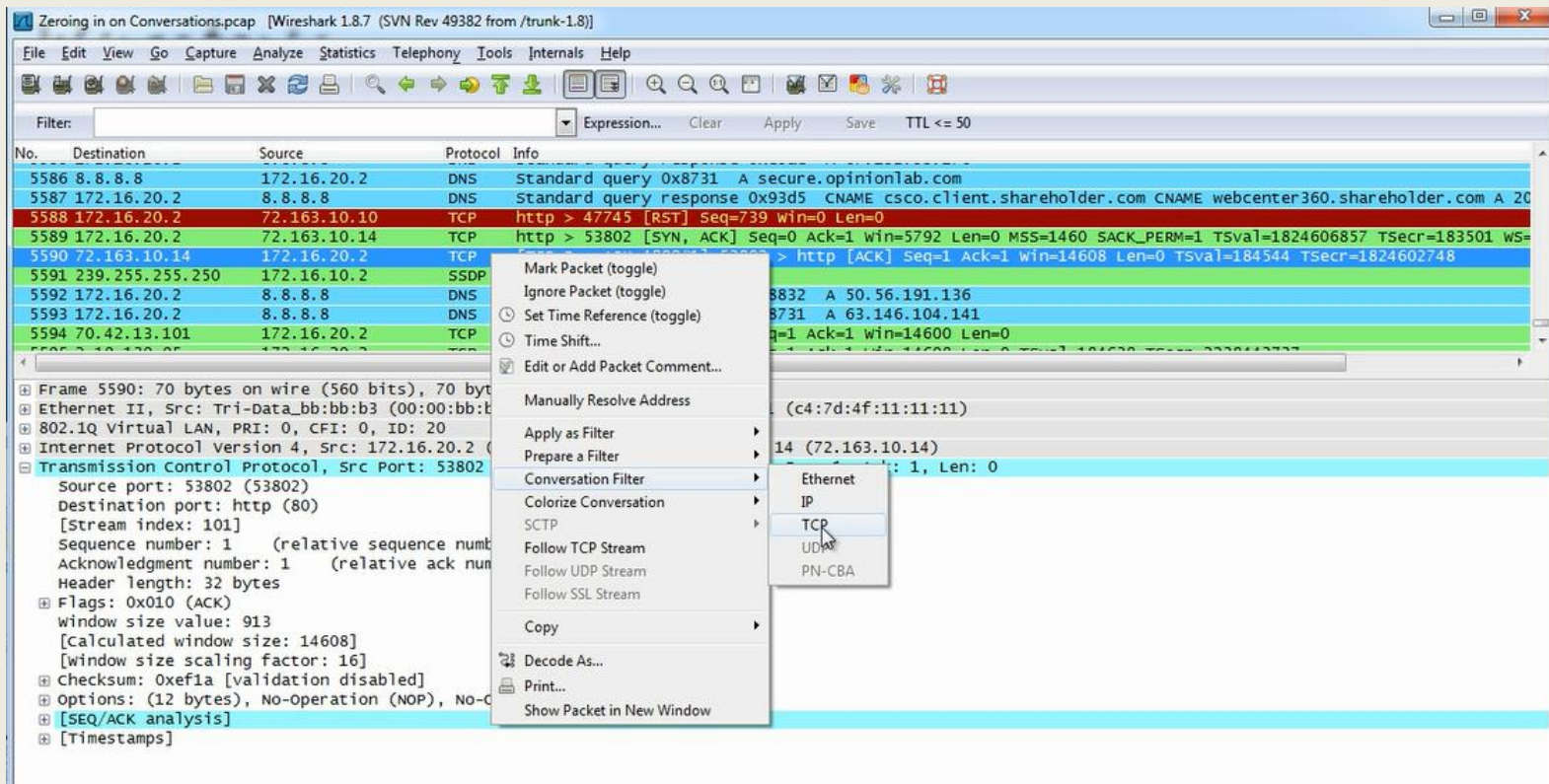
- Nakon primene filtriranja, prikazaće nam se paketi koji uključuju **“Stream index: 55”**

No.	Destination	Source	Protocol	Info
3256	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]
3257	2.19.135.148	172.16.20.2	TCP	43709 > http [ACK] Seq=2934 Ack=116370 win=54064 Len=0 Tsval=180807 TSecr=2238357623
3258	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]
3259	172.16.20.2	2.19.135.148	HTTP	HTTP/1.1 200 OK (PNG)
3260	2.19.135.148	172.16.20.2	TCP	43709 > http [ACK] Seq=2934 Ack=117994 win=54832 Len=0 Tsval=180812 TSecr=2238357630
3261	2.19.135.148	172.16.20.2	HTTP	GET /shared/framework/img/global/rss_icon_24x25.png HTTP/1.1
3289	172.16.20.2	2.19.135.148	TCP	[TCP segment of a reassembled PDU]
3290	172.16.20.2	2.19.135.148	HTTP	HTTP/1.1 200 OK (PNG)
3291	2.19.135.148	172.16.20.2	TCP	43709 > http [ACK] Seq=3630 Ack=119765 win=55024 Len=0 Tsval=180857 TSecr=2238358110
3292	2.19.135.148	172.16.20.2	HTTP	GET /shared/img/homepage/home_page_hero_banner_security.jpg HTTP/1.1



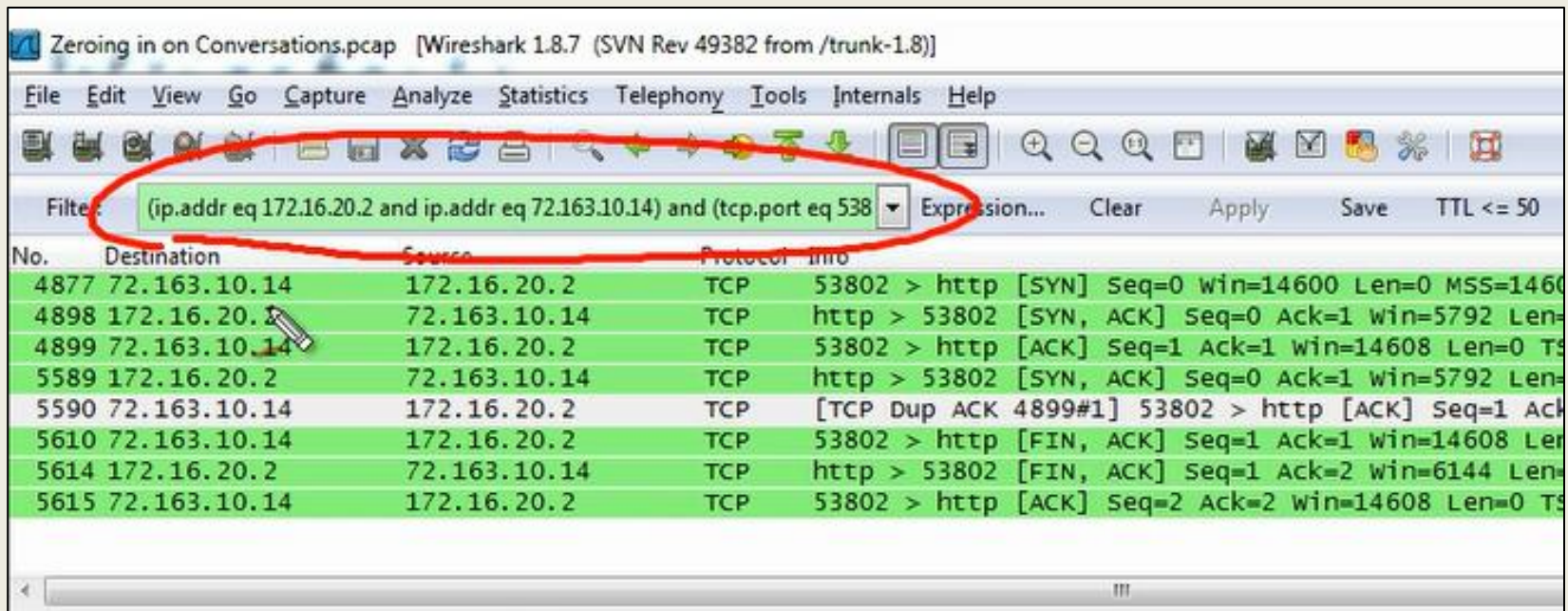
# Conversation Filter

- 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**".

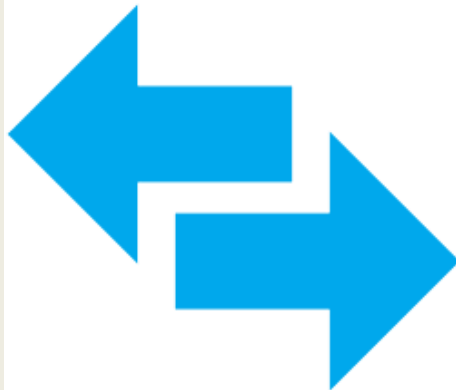


Zeroing in on Conversations.pcap [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 172.16.20.2 and ip.addr eq 72.163.10.14) and (tcp.port eq 538) Expression... Clear Apply Save TTL <= 50

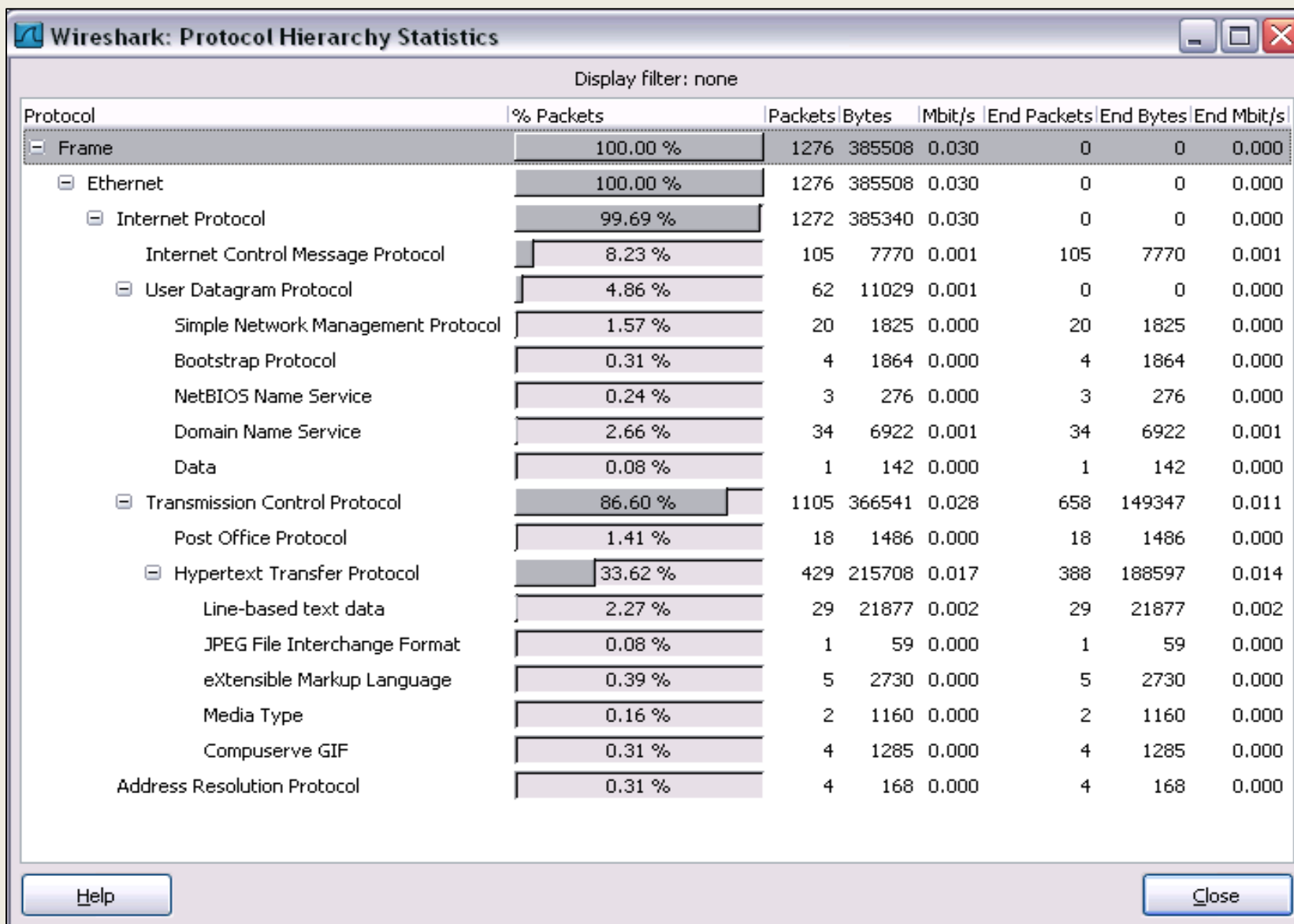
No.	Destination	Source	Protocol	Info
4877	72.163.10.14	172.16.20.2	TCP	53802 > http [SYN] Seq=0 win=14600 Len=0 MSS=1460
4898	172.16.20.2	72.163.10.14	TCP	http > 53802 [SYN, ACK] Seq=0 Ack=1 win=5792 Len=
4899	72.163.10.14	172.16.20.2	TCP	53802 > http [ACK] Seq=1 Ack=1 win=14608 Len=0 TS
5589	172.16.20.2	72.163.10.14	TCP	http > 53802 [SYN, ACK] Seq=0 Ack=1 win=5792 Len=
5590	72.163.10.14	172.16.20.2	TCP	[TCP Dup ACK 4899#1] 53802 > http [ACK] Seq=1 Ack
5610	72.163.10.14	172.16.20.2	TCP	53802 > http [FIN, ACK] Seq=1 Ack=1 win=14608 Len
5614	172.16.20.2	72.163.10.14	TCP	http > 53802 [FIN, ACK] Seq=1 Ack=2 win=6144 Len=
5615	72.163.10.14	172.16.20.2	TCP	53802 > http [ACK] Seq=2 Ack=2 win=14608 Len=0 TS



*Poglavlje 6*

*Statistika paketa*

# Hijerarhija protokola

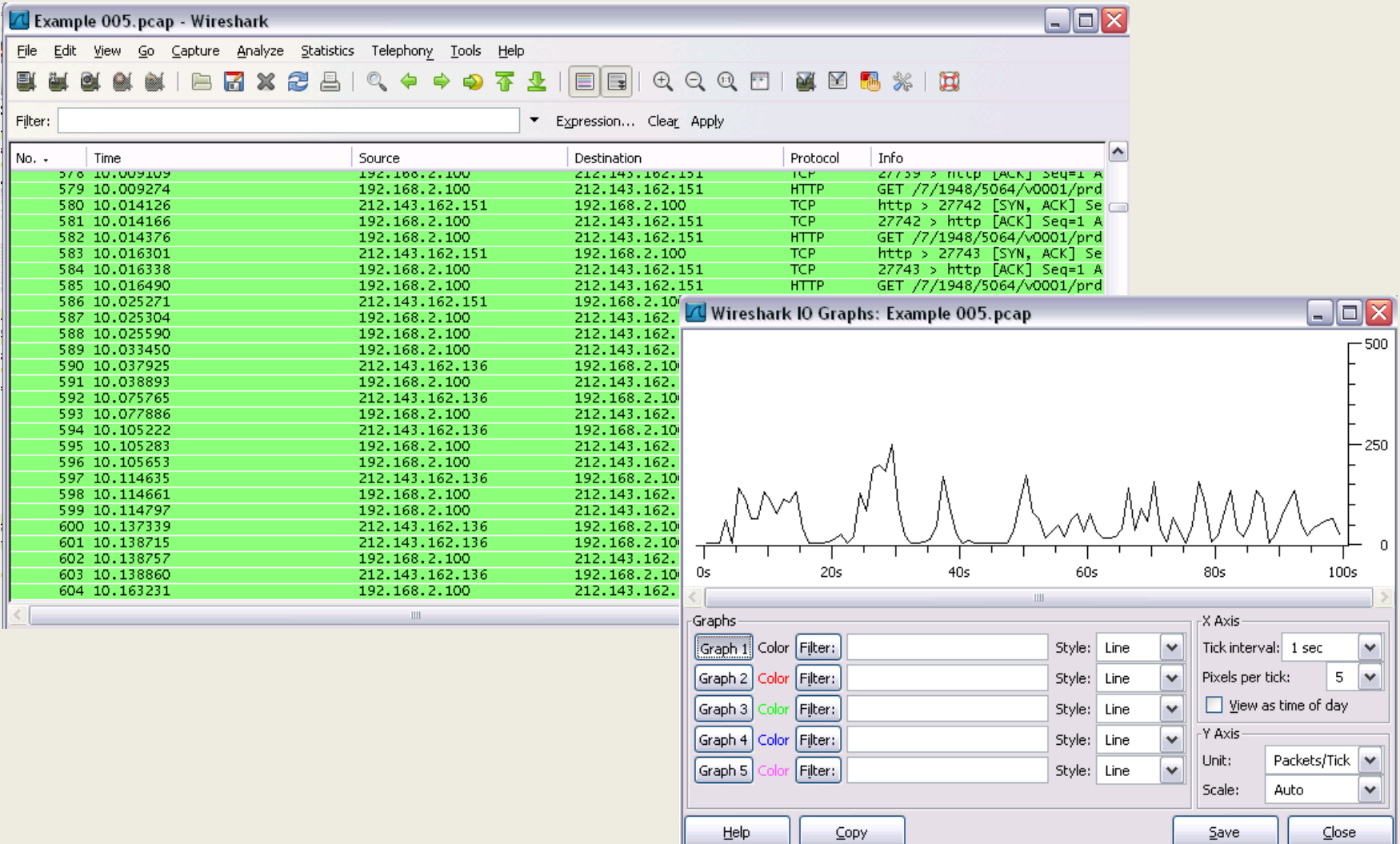


# Konverzacija između dve krajnje tačke (end-pointa)

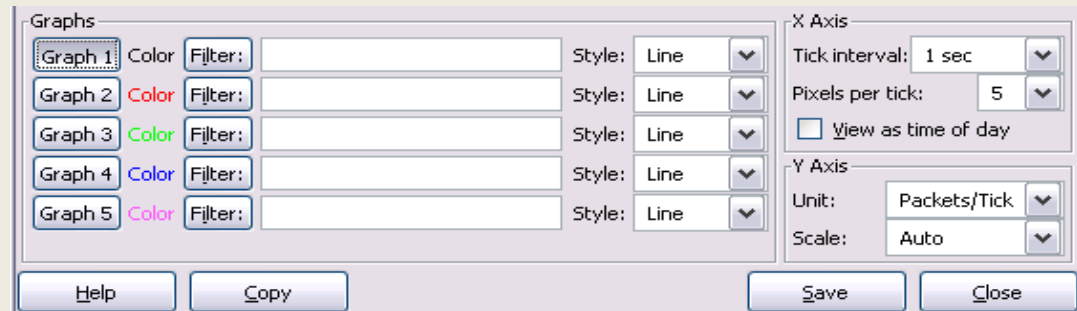
The screenshot shows a window titled "Conversations: (Untitled)" with a toolbar containing various protocol tabs. The "IPv4: 38" tab is selected. Below the toolbar is a table titled "IPv4 Conversations" with the following columns: Address A, Address B, Packets, Bytes, Packets A->B, Bytes A->B, Packets A<-B, Bytes A<-B, Rel Start, and Duration. The table contains 15 rows of data. At the bottom of the window, there are checkboxes for "Name resolution" (checked) and "Limit to display filter" (unchecked), along with "Help", "Copy", and "Close" buttons.

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration
192.168.2.100	255.255.255.255	1	142	1	142	0	0	96.384838000	0.0000
192.168.2.101	255.255.255.255	2	684	2	684	0	0	47.852757000	3.0721
192.168.2.1	255.255.255.255	2	1180	2	1180	0	0	47.857905000	3.0722
192.168.2.100	212.143.162.144	10	2194	6	815	4	1379	87.473054000	65.0878
192.168.2.100	212.179.31.90	10	1342	6	971	4	371	91.655266000	60.9113
62.90.102.31	192.168.2.100	10	1373	4	441	6	932	91.660203000	60.9174
192.168.2.100	212.150.22.226	10	1327	6	956	4	371	91.732692000	60.8200
192.168.2.100	212.150.236.220	10	1470	6	981	4	489	91.742363000	60.8122
192.168.2.100	212.179.58.84	10	1725	6	954	4	771	92.287214000	2.4984
82.80.238.109	192.168.2.100	11	1282	5	440	6	842	91.646648000	60.9214
10.12.44.2	192.168.2.100	12	888	6	444	6	444	31.421091000	164.384
10.10.10.2	192.168.2.100	12	888	6	444	6	444	31.531676000	164.804
10.12.20.2	192.168.2.100	12	888	6	444	6	444	5.250457000	164.523
10.31.68.1	192.168.2.100	12	888	6	444	6	444	5.578447000	164.631
10.100.102.2	192.168.2.100	12	888	6	444	6	444	17.858674000	164.363

# I/O Grafik



# 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

Sniff1 --- File copy from other side.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: (tcp.stream eq 0)

Summary  
Protocol Hierarchy  
Conversations  
Endpoints  
Packet Lengths...  
IO Graphs  
Conversation List  
Endpoint List  
Service Response Time  
BOOTP-DHCP...  
Compare...  
Flow Graph...  
HTTP  
IP Addresses...  
IP Destinations...  
IP Protocol Types...  
ONC-RPC Programs  
TCP Stream Graph  
UDP Multicast Streams  
WLAN Traffic...

Expression... Clear Apply

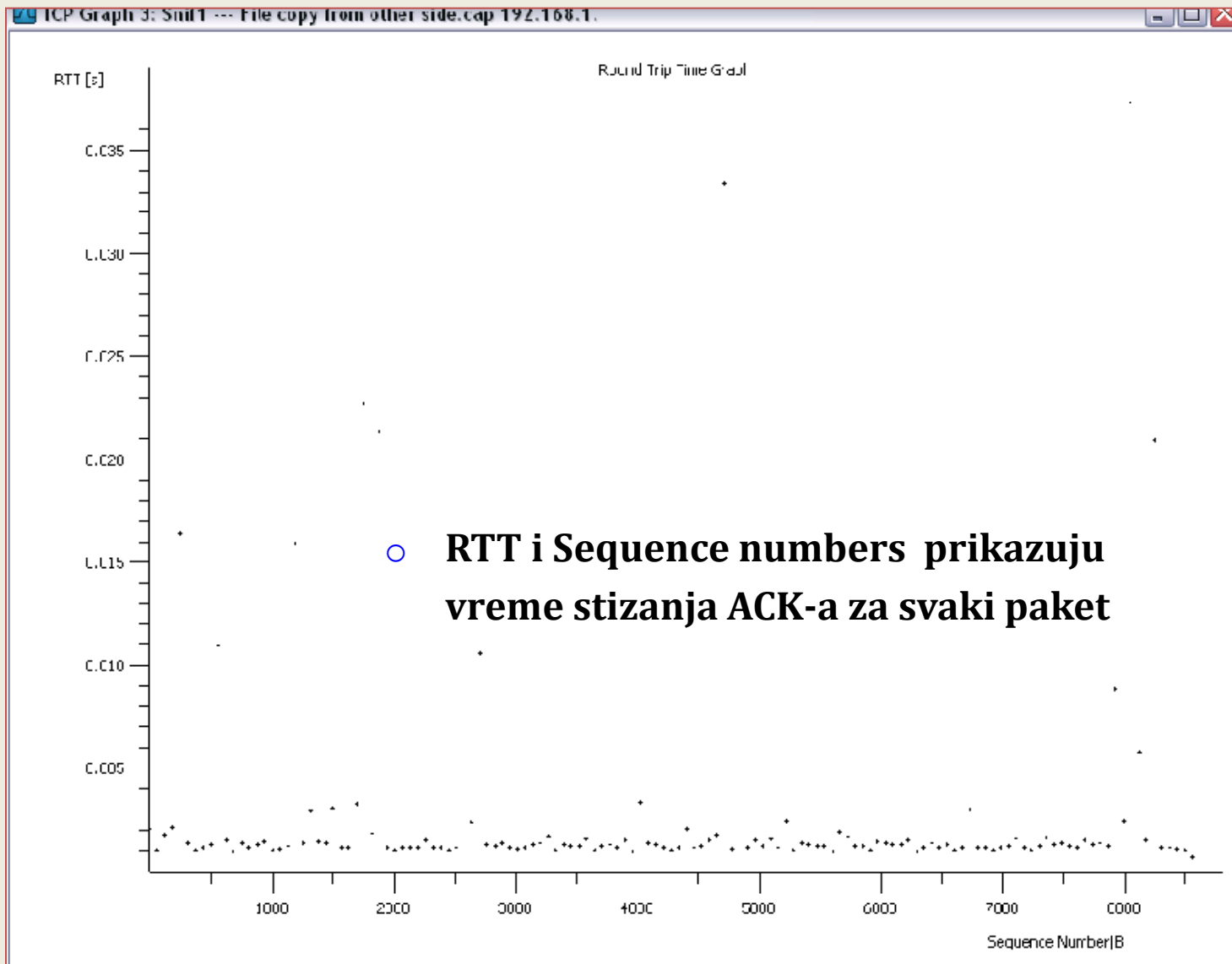
No.	Time	Destination	Protocol	Info
762	0.132867	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
763	0.132992	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
764	0.133116	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
766	0.133247	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
767	0.133258	192.168.1.102	SMB	Read AndX Response, 61440 bytes
768	0.133265	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=686944 Win:
769	0.133272	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=689864 Win:
770	0.133281	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=692784 Win:
771	0.134377	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=695704 Win:
773	0.139299	192.168.104.77	SMB	Read AndX Request, FID: 0x8003, 61440 bytes at offset 1747.
774	0.140539	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
775	0.140661	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
776	0.140785	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
777	0.140909	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
778	0.141033	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
779	0.141155	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
780	0.141282	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
781	0.141293	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=698807 Win:
782	0.141411	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
783	0.141421	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=701727 Win:
784	0.141538	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
785	0.141663	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
786	0.141783	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
787	0.141908	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
788	0.142035	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
789	0.142046	192.168.1.102	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=704647 Win:
790	0.142053	192.168.1.102	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=707567 Win:
791	0.142058	192.168.1.102	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=710487 Win:

Round Trip Time Graph  
Throughput Graph  
Time-Sequence Graph (Stevens)  
Time-Sequence Graph (tcptrace)

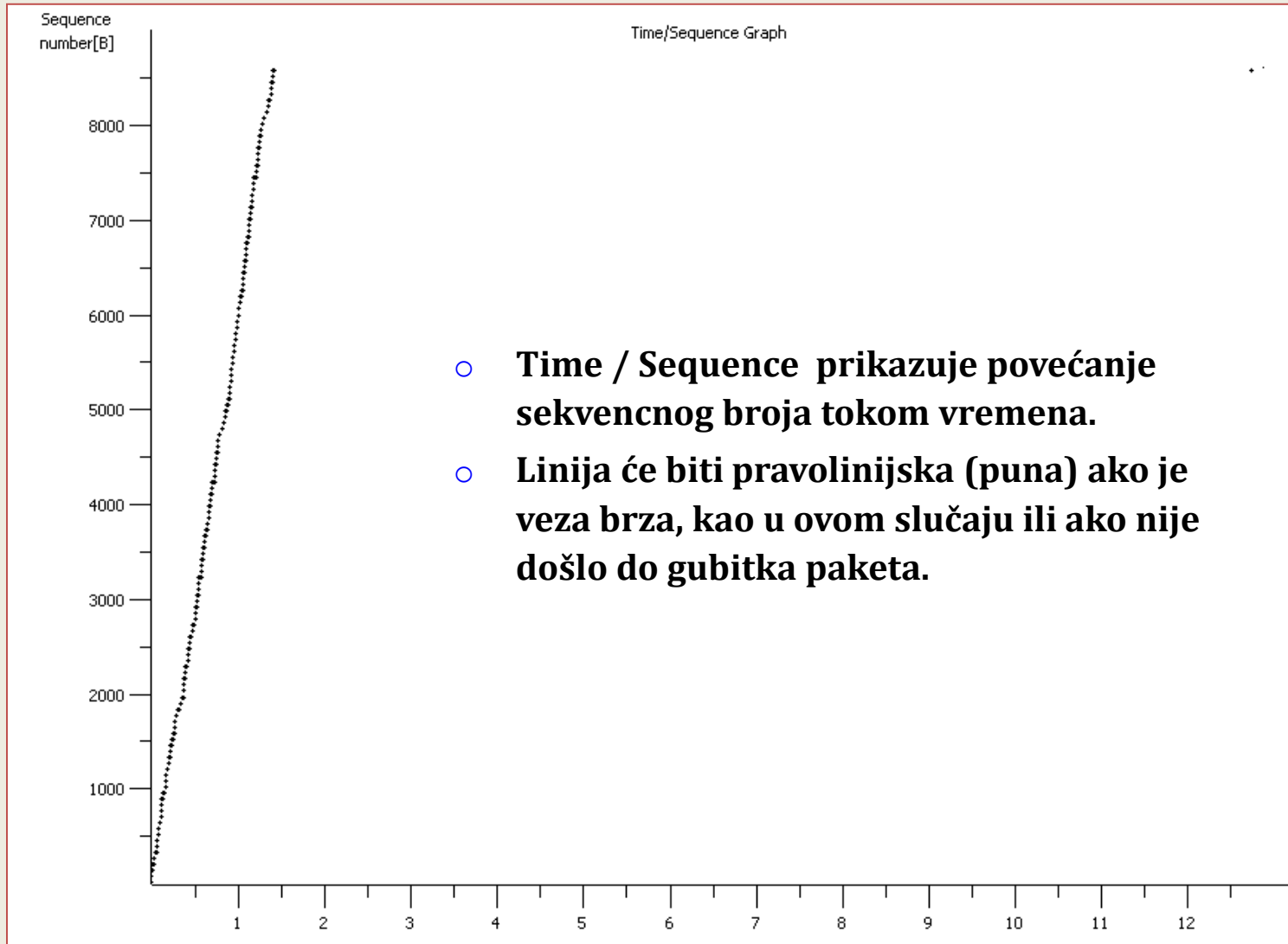
Frame 771 (60 bytes on wire, 60 bytes captured)  
Ethernet II, Src: Intel\_4c:cc:89 (00:d0:b7:4c:cc:89), Dst: Intel\_2e:32:a9 (00:90:27:2e:32:a9)  
Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.104.77 (192.168.104.77)  
Transmission Control Protocol, Src Port: paradym-31port (1864), Dst Port: microsoft-ds (445), Seq: 883, Ack: 695704, Len: 0



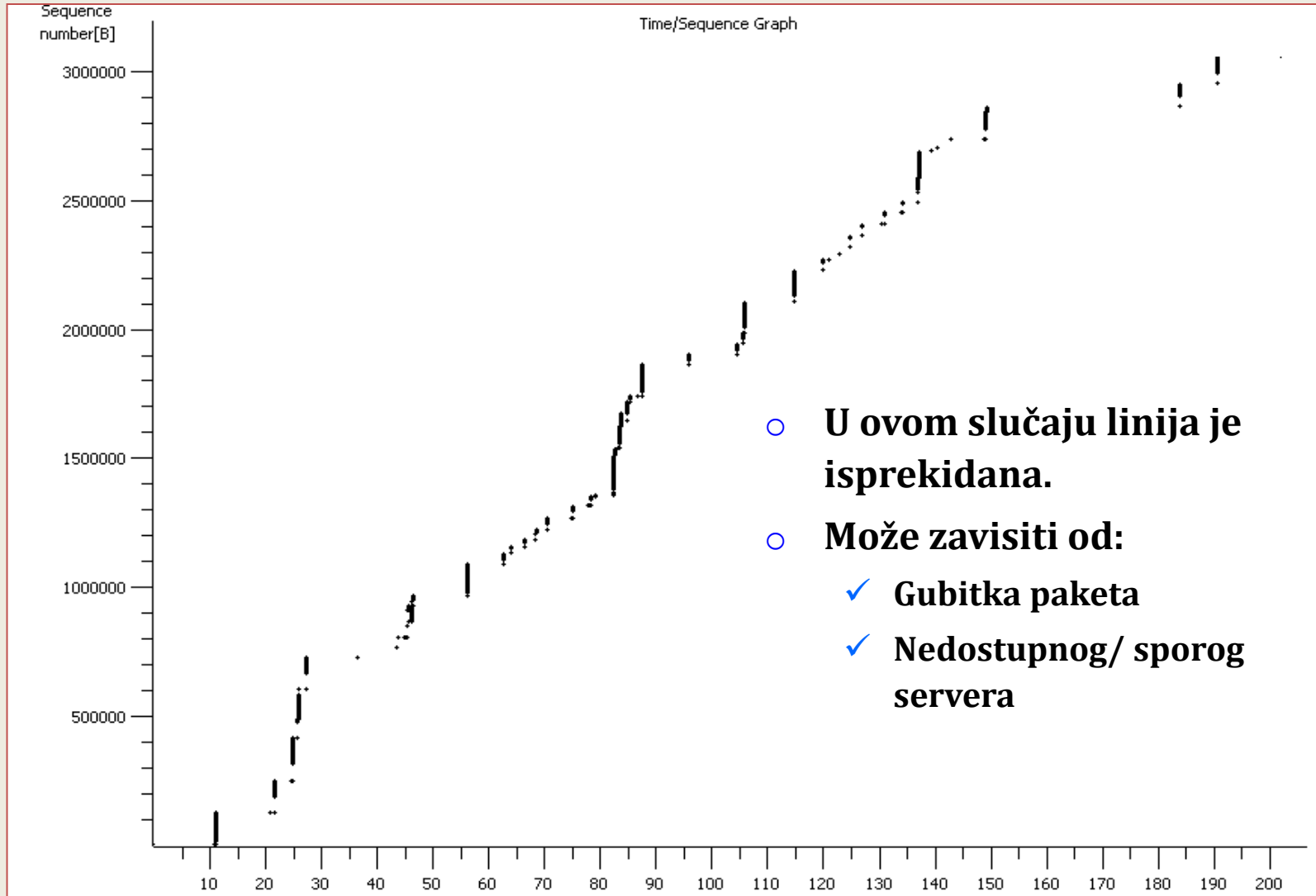
# Round-Trip Time Grafik

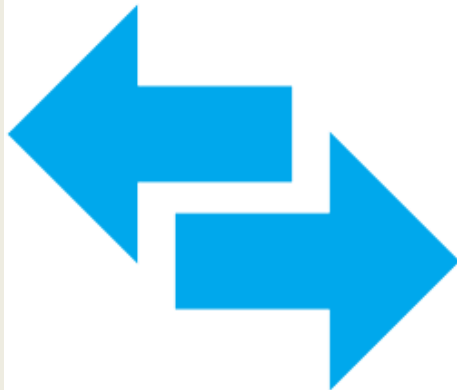


# Time / Sequence Grafik



# Time / Sequence Grafik





*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	0.002828	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

The screenshot displays the Wireshark network protocol analyzer interface. The main pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packets are color-coded by conversation. A context menu is open over packet 10, with the 'Colorize Conversation' option selected. This opens a sub-menu where 'Color 1' is chosen. The bottom pane shows the packet details for the selected packet, including Ethernet II, Internet Protocol, and DCE RPC Request fields. The status bar at the bottom indicates the file path and the number of packets displayed and marked.

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 num: 2 ctx_id: 0
3	0.002838	172.16.1.224	172.16.3.14	DCERPC	Response: call id: 395 num: 2 ctx_id: 0
4	0.004758	172.16.1.20	172.16.2.236	HTTP	GET / HTTP/1.1
5	0.005001	172.16.2.236	172.16.1.20	TCP	64.236.34.97 [ACK] Seq=1 Ack=1461 win=64240 Len=0
6	0.005134	172.16.1.20	172.16.2.236	HTTP	200 OK
7	0.005658	172.16.1.20	172.16.2.236	HTTP	200 OK
8	0.005790	172.16.1.20	172.16.2.236	HTTP	200 OK
9	0.005906	172.16.2.236	172.16.1.20	TCP	64.236.34.97 [ACK] Seq=1 Ack=2049 win=64240 Len=0
10	0.006231	172.16.1.20	172.16.2.236	HTTP	200 OK
11	0.006253	172.16.1.20	172.16.2.236	HTTP	200 OK
12	0.006444	172.16.2.236	172.16.1.20	TCP	64.236.34.97 [ACK] Seq=1 Ack=2049 win=64240 Len=0
13	0.006826	172.16.1.20	172.16.2.236	HTTP	200 OK
14	0.006962	172.16.1.20	172.16.2.236	HTTP	200 OK
15	0.007079	172.16.2.236	172.16.1.20	TCP	64.236.34.97 [ACK] Seq=1 Ack=2049 win=64240 Len=0
16	0.007221	172.16.3.129	172.16.201.60	ICMP	Destination unreachable: protocol (8)
17	0.007951	172.16.1.20	172.16.2.236	HTTP	200 OK
18	0.007972	64.236.34.97	172.16.2.219	TCP	64.236.34.97 [ACK] Seq=1 Ack=1 win=4096 Len=0
19	0.008068	172.16.1.20	172.16.2.236	HTTP	200 OK
20	0.008263	172.16.1.20	172.16.2.236	HTTP	200 OK
21	0.008279	172.16.1.40	172.16.2.5	TCP	172.16.1.40 [ACK] Seq=1 Ack=1 Win=0 Len=0

⊕ Frame 2 (198 bytes on wire, 198 bytes captured)  
⊕ Ethernet II, Src: 3com\_74:5a:2b (00:50:da:74:5a:2b), Dst: Cisco\_07:a2:b0 (00:0c:85:07:a2:b0)  
⊕ Internet Protocol, Src: 172.16.3.14 (172.16.3.14), Dst: 172.16.1.224 (172.16.1.224)  
⊕ Transmission Control Protocol, Src Port: writesrv (1334), Dst Port: alta-ana-lm (1346), Seq: 1, Ack: 1, Len: 1  
⊕ DCE RPC Request, Fragment: Single, FragLen: 144, Call: 395 Ctx: 0

0000 00 0c 85 07 a2 b0 00 50 da 74 5a 2b 08 00 45 00 .....P .tZ+..E.  
0010 00 b8 58 74 40 00 80 06 44 bd ac 10 03 0e ac 10 ..xt@... D.....  
0020 01 e0 05 36 05 42 9a 8d a4 a2 49 a0 ce 05 50 18 ...6.B... ..I...P.  
0030 fa 90 0f c3 00 00 05 00 00 03 10 00 00 00 90 00 .....  
0040 10 00 8b 01 00 00 52 00 00 00 00 00 02 00 00 00 .....R.....  
0050 00 00 01 61 85 26 dd f7 6b 42 88 28 12 00 00 0d .....&..kC/

File: "D:\Customers\Mivtachim\Snif4 --- Center-... Packets: 11108 Displayed: 11108 Marked: 0 Profile: Default

# Primer kolorizacije

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:  Expression... Clear Apply

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

⊕ Frame 7 (1514 bytes on wire, 1514 bytes captured)

⊕ Ethernet II, Src: Cisco\_07:a2:b0 (00:0c:85:07:a2:b0), Dst: 3Com\_21:5a:ee (00:04:76:21:5a:ee)

⊕ Internet Protocol, Src: 172.16.1.20 (172.16.1.20), Dst: 172.16.2.236 (172.16.2.236)

⊕ Transmission Control Protocol, Src Port: http-alt (8080), Dst Port: netview-aix-11 (1671), Seq: 1, Ack: 1, Len: 1460

⊕ Hypertext Transfer Protocol

```
0000  00 04 76 21 5a ee 00 0c 85 07 a2 b0 08 00 45 00  ..v!Z... ..E.
0010  05 dc da 91 40 00 7e 06 c0 69 ac 10 01 14 ac 10  ....@.~. .i.....
0020  02 ec 1f 90 06 87 63 1c 76 33 75 66 1b 04 50 10  ....c. v3uf..P.
0030  ff ff c8 c0 00 00 09 09 09 09 09 09 3c 74 72 3e  ....<tr>
0040  3c 74 64 20 68 65 69 67 68 74 3d 22 33 22 3e 3c  <td heig ht="3"><
0050  2f 74 64 20 2c 2c 2f 74 72 20 0d 03 00 00 00 00  (td><tr>
```

File: "D:\Courses\Freeware\Example 016.cap" 4... Packets: 11108 Displayed: 11108 Marked: 0 Profile: Default