

Vežba 6 - Mrežni dijagnostički alati

1. Prikaz mrežne konfiguracije – ipconfig

Komanda *ipconfig* je najčešće korišćen alat za uvid u informacije o mrežnoj konfiguraciji lokalnog računara i na koji način je konfigurisana mreža kojoj računar pripada.

```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : rayda-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : charter.com

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : charter.com
    Description . . . . . : Realtek RTL8102E/RTL8103E Family PCI-E Fa
    st Ethernet NIC (NDIS 6.20)
    Physical Address. . . . . : 00-21-97-AD-29-A5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::993a:600b:8ca1:a121%11(Preferred)
    IPv4 Address. . . . . : 192.168.1.103(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, January 14, 2012 9:52:10 PM
    Lease Expires . . . . . : Sunday, January 15, 2012 9:52:09 PM
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 234889623
    DHCPv6 Client DUID. . . . . : 00-01-00-01-15-4F-E7-7B-00-21-97-AD-29-A5

    DNS Servers . . . . . : 71.9.127.107
                           68.190.192.35
                           24.205.224.36
    NetBIOS over Tcpip. . . . . : Enabled
```

Slika 1 – Primer korišćenja ipconfig /all naredbe

Ova komanda se obično koristi sa opcijom *-all*, kako bi se prikazale sve dostupne informacije o konfiguraciji. Pored IP adrese i MAC adrese lokalnog računara, ova komanda pruža informacije o IP adresi gateway-a, subnet maski, adresi DHCP servera i adresi DNS servera. Na slici 1 dat je prikaz poziva *ipconfig /all* komande.

Prikaz svih keširanih DNS zapisa moguće je korišćenjem *ipconfig /displaydns* komande.

```
Record Name . . . . . : plus.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 1
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 173.194.36.7

Record Name . . . . . : plus.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 1
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 173.194.36.8
```

Slika 2 – Prikaz DNS zapisa

2. Provera funkcionisanja IP protokola - ping

Postoji uobičajena procedura za proveru funkcionisanja IP protokola na računaru i otkrivanje problema. Procedura se oslanja na jednostavnu komandu – ping. Ovaj dijagnostički alat, dostupan na svim operativnim sistemima omogućava da se na proizvoljnu adresu pošalju posebne poruke “Echo Request”. Računar koji primi ovakvu poruku odgovara sa “Echo Replay” porukom. Ukoliko računar dobije odgovor na svoju “Echo” poruku može se zaključiti da između dva računara mreža funkcioniše na 1., 2., i 3. sloju OSI modela. Za slanje poruka se koristi protokol pod nazivom ICMP (engl. Internet Control Message Protocol) koji funkcioniše na 3. (mrežnom) sloju OSI modela.

Ping komanda pokreće se iz *Command Prompt*-a, koji se može otvoriti ako se u pretrazi startnog menija upiše ključna reč *cmd*. Za prekid izvršavanja komande pod Windows operativnim sistemom pritisnuti istovremeno *Ctrl+C*.

U nastavku je dat redosled komandi kojim bi se moglo detektovati gde je nastala greška u komunikaciji. Obratiti pažnju i na odgovore na Ping. Prikazano je povratno vreme RTT (engl. Round Trip Time) i TTL (engl. Time To Live) vrednost koja je poslata u paketima. Posle četiri odgovora prikazano je i minimalno, maksimalno i prosečno povratno vreme kao i procenat izgubljenih paketa.

Uputstvo za korišćenje ove komande (pod Windows operativnim sistemom) dobićete ako ukucate ping/?

Provera ispravnosti lokalne petlje

Adresa lokalne petlje (engl. *Loopback address*) je specijalna adresa (127.0.0.1) namenjena softverski implementiranom interfejsu koji služi kao povratna sprega za komunikaciju unutar jednog računara.

- **ping 127.0.0.1**

Ukoliko se ne dobiju nikakvi ECHO odgovori to znači da IP protokol nije valjano instaliran na računaru. Uspešan prijem odgovora ne sugerise nikakve informacije o tome da li IP adresa, subnet maska ili adresa gateway protokola valjano konfigurisana

Primena računarskih mreža u IS

```
C:\Windows\system32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

Slika 3 - Ping loopback adrese

Provera ispravnosti mrežnog adaptera ping *ip_adresa_lokalnog_racunara*

odnosno ping na sopstvenu IP adresu. Ukoliko se ne dobiju ECHO odgovori, to bi moglo da sugeriše da IP protokol nije vezan za mrežni adapter, zbog pogrešne konfiguracije ili fizičkog kvara adaptera.

```
C:\Windows\system32>ping 192.168.1.111

Pinging 192.168.1.111 with 32 bytes of data:
Reply from 192.168.1.111: bytes=32 time<1ms TTL=128
Reply from 192.168.1.111: bytes=32 time<1ms TTL=128
Reply from 192.168.1.111: bytes=32 time<1ms TTL=128
Reply from 192.168.1.111: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

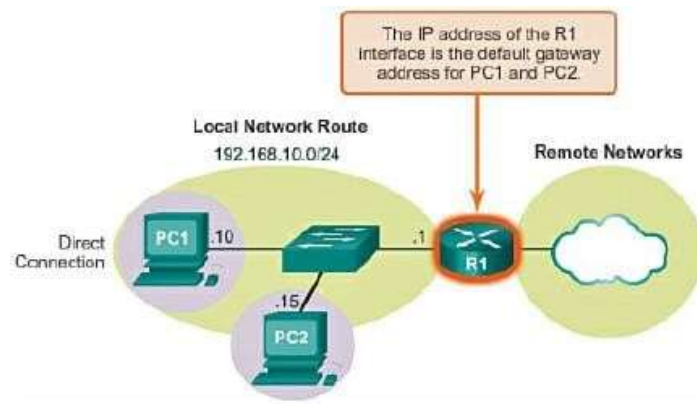
C:\Windows\system32>
```

Slika 4 - Ping lokalnog računara

Primena računarskih mreža u IS

Provera mogućnosti komunikacije unutar lokalne mreže

Mogućnost komunikacije unutar lokalne mreže testira se slanjem ping poruke krajnjem ruteru mreže (engl. *Gateway router*). Prethodno je potrebno pomoću *ipconfig* komande saznati adresu gateway-a.



Slika 5 - Uloga gateway-a u lokalnoj mreži

Ukoliko ruter vrati odgovor, to znači da je lokalna mreža dobro konfigurisana i da ruter obavlja svoj posao valjano. U suprotnom, trebalo bi posumnjati na

Ping mogućnosti komunikacije sa drugim računarom

- **ping ip_adresa_udaljenog_racunara**

U datom primeru korišćena je adresa računara koji se nalazi u drugoj mreži (u konkretnom slučaju numerička IP adresa Narodnog muzeja u Beogradu). Ukoliko se dobiju ECHO odgovori možemo znati da je konfigurisani podrazumevani mrežni prolaz ispravan. U našem slučaju ne možemo tačno znati iz kog razloga udaljeni računar nije dostupan.

```
Pinging 94.127.2.226 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 94.127.2.226:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>
```

Slika 6 - Ping drugog računara

Primena računarskih mreža u IS

Provera dostupnosti drugog računara korišćenjem njegovog imena

U komandnoj liniji uneti: **ping *www.google.com***

ukoliko se u ping komandi referišemo na ime računara i dobijemo ECHO odgovor, posredno znamo i da razrešavanje imena uz konfigurisani DNS server funkcioniše.

```
C:\Windows\system32>ping google.rs

Pinging google.rs [173.194.116.111] with 32 bytes of data:
Reply from 173.194.116.111: bytes=32 time=28ms TTL=50
Reply from 173.194.116.111: bytes=32 time=25ms TTL=50
Reply from 173.194.116.111: bytes=32 time=34ms TTL=50
Reply from 173.194.116.111: bytes=32 time=24ms TTL=50

Ping statistics for 173.194.116.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 34ms, Average = 27ms

C:\Windows\system32>
```

Slika 7 – Ping drugog računara korišćenjem njegovog imena

Dodatne opcije

Ping komanda omogućava promenu podrazumevanih parametara kroz opcije. U tabeli su dateneke od najbitnijih opcija.

Opcija	Značenje opcije	Podrazumevana vrednost opcije
<i>-n</i>	Ukupan broj puta pozivanja ping komande (odnosno koliki broj puta se šalje <i>Echo Request</i> poruka).	4 poruke
<i>-l</i>	Količina korisničkih podataka (van zaglavlja).	32 bajta
<i>-i</i>	Maksimalni dozvoljen broj skokova (TTL)	64
<i>-w timeout</i>	Vremensko ograničenja za čekanje odgovora na upućeni zahtev.	4 sekunde

U komandnoj liniji uneti: **ping -n 2 *www.google.com***

```
Pinging google.rs [173.194.116.111] with 32 bytes of data:
Reply from 173.194.116.111: bytes=32 time=38ms TTL=50
Reply from 173.194.116.111: bytes=32 time=45ms TTL=50

Ping statistics for 173.194.116.111:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 38ms, Maximum = 45ms, Average = 41ms

C:\Windows\system32>
```

Slika 8 – Korišćenjem dodatnih opcija za ping komandu

Primena računarskih mreža u IS

Pingovanje udaljenog računara – poruke o grešci

Ukoliko Ping prema računaru na nekoj bližoj ili daljoj mreži ne uspe, moguće su četiri poruke o greškama:

Greška	Objašnjenje greške
<i>TTL Expired in Transit</i>	Broj potrebnih skokova (čvorova) da bi se stiglo do odredišta veći je od vrednosti TTL koju je računar pošiljalac postavio za slanje paketa. Potrebno je povećati TTL koristeći opciju ping – i (max. do 255)
<i>Destination Host Unreachable</i>	Lokalni ili udaljeni računar nema put do željenog odredišta. <div> <div> Destination Host Unreachable Ne postoji putanja od lokalnog računara i da paketi koje treba poslati nisu ni postavljeni na prenosni medijum. </div> <div> Replay from <IP adresa>: Destination Host Unreachable Došlo je do problema u preusmeravanju paketa kroz mrežu došlo na ruteru čija je IP adresa navedena u poruci. </div> </div>
<i>Request Timed Out</i>	U podrazumevanom vremenskom intervalu od 1 sekunde nije primljen ICMP odgovor Echo Replay. Razloga ima više: zagušenje mreže, neuspeh ARP zahteva, filtriranje paketa, greška u rutiranju itd. Najčešće ova poruka znači da odredišni računar ili neki od rutera (moguće i defaultni gateway odredišnog računara) “ne zna” put nazad ka računaru koji je inicirao ping. Zagušenje mreže može se prepoznati ako jednostavno produžimo vreme čekanja koristeći opciju ping – w timeout (timeout u milisekundama).
<i>Unknown host</i>	Zahtevano ime računara ne može se prevesti u IP adresu. Potrebno je proveriti da li je ime mrežnog čvora pravilno napisano i da li su dostupni DNS serveri.

3. Tracert (Traceroute)

Tracert (za Windows) / Traceroute (za Linux) predstavlja pomoćni program za proveravanje putanje kojom paket putuje na svom putu od izvorišnog računara do odredišta. Rezultat programa je lista interfejsa svih rutera kroz koje je paket prošao na svom putu ka odredištu. Koristeći TTL polje u ICMP poruci “*Echo Request*” i ICMP poruku “*Time Exceeded*”, Tracert je u mogućnosti da odredi putanju od izvora do odredišta kroz međusobno povezane IP mreže. Neki ruteri ne vraćaju “*Time Exceeded*” poruku za pakete sa nultim TTL vrednostima pa su kao takvi “nevidljivi” za Tracert. U tom slučaju, red zvezdica (*) se prikazuje za taj čvor. Slanje paketa iz jednog sistema u drugi Tracert označava kroz skokove (engl. *hops*), gde svaki mrežni čvor kroz koji paket prolazi predstavlja jedan skok. Svaki red tabele predstavlja informacije dobijene od čvora na putanji između izvorišnog čvora i odredišta.

```
C:\Windows\system32\cmd.exe
C:\>tracert www.rt-rk.uns.ac.rs
Tracing route to webserv.domain.local [192.168.231.112] over a maximum of 30 hops:
  0  1 ms  <1 ms  <1 ms  192.168.2.1
  1  <1 ms  1 ms  1 ms  192.168.255.2
  2  <1 ms  <1 ms  1 ms  webserv.domain.local [192.168.231.112]
Trace complete.
C:\>
```

Slika 9- Tracert program daje tabelarni prikaz mrežnih čvorova na putanji do odredišta

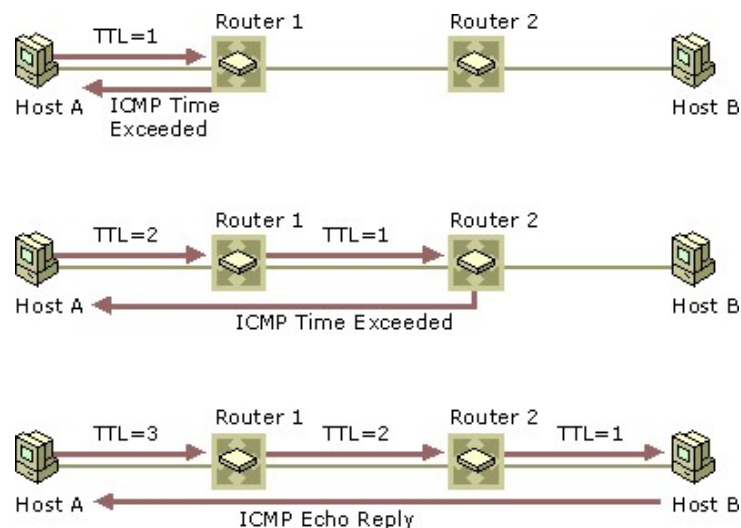
Prva kolona u izlaznoj tabeli (broj 2 na slici 9) prikazuje potreban broj skokova (čvorova) do odredišnog računara. Druga, treća i četvrta kolona (broj 3 na slici 9) prikazuje RTT parametar u milisekundama za svaki ICMP paket u setu. Ovaj parametar govori koliko vremena je potrebno paketu da od izvorišta dođe do određenog čvora i nazad. Tracert uvek šalje tri paketa ka odredištu kako bi se dobilo što realnije RTT vreme. Svaka RTT vrednost za pojedini čvor do 500milisekundi smatra se prihvatljivom. Peta kolona (broj 4 na slici 9) daje pregled IP adresa (a po mogućnosti i domenskih adresa) za svaki čvor na putanji do odredišta.

Princip rada alata Tracert

Kao što smo videli Ping softver šalje ICMP zahtev “*Echo Request*” na određenu IP adresu i čeka ICMP odgovor “*Echo Replay*” sa te IP adrese. Na osnovu broja primljenih odgovora i vremenskog perioda od slanja zahteva do dobijanja odgovora, Ping pravi izveštaj o stanju IP konekcije prema nekom računaru unutar TCP/IP mreže.

Da bi razumeli način na koji Tracert program radi, neophodno je razumeti značaj TTL polja unutar zaglavlja svakog IP paketa. Vrednost ovog polja predstavlja u stvari maksimalno vreme trajanja IP paketa na mreži. Njegovu vrednost postavlja pošiljalac IP paketa (pre slanja paketa) da bi ga svaki čvor (ruter ili host) na putu ka odredištu smanjio za određeni iznos. Ukoliko vrednost TTL polja padne na nulu pre nego što paket stigne na svoje odredište, paket se odbacuje a ICMP poruka o grešci (“*Time Exceeded*”) šalje se nazad pošiljaocu paketa. Svrha ovog polja je izbegavanje situacija u kojima paket koji je nemoguće dostaviti odredištu beskonačno kruži mrežom, sprečavajući time mogućnost zagušenja mreže ovim “besmrtnim” paketima. Svaki čvor kroz koji paket prolazi na svom putu ka odredištu umanjuje vrednost TTL-a za jedan. Na slici 9 prikazan je princip rada programa Tracert koji se izvršava na računaru A, a prati putanju do računara B. Program radi tako što vrednost TTL-a za svaki sledeći ICMP paket “*Echo Request*” povećava za jedan i čeka na ICMP poruku “*Time Exceeded*”. Vrednost TTL-a u Tracert paketu počinje od jedan i svaki put se povećava za jedan. Paket koji Tracert pošalje putuje svaki put jedan skok (čvor) dalje.

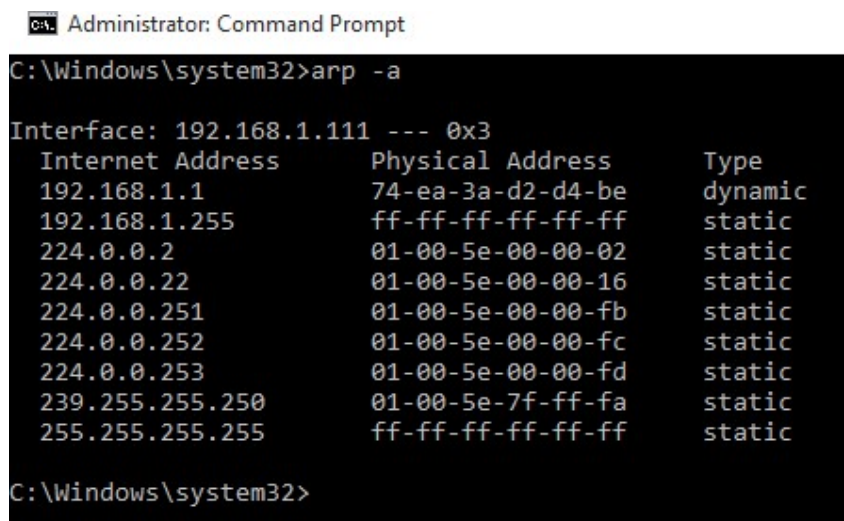
Na ruterima 1 i 2 TTL se smanjuje na nulu, što dovodi do slanja ICMP poruke “*Time Exceeded*”. Kad ICMP paket “*Echo Request*” stigne do računara B, on vraća ICMP paket “*Echo Replay*”.



Slika 10 - Princip rada Tracert programa

4. Prikaz sadržaja arp tabele

Address Resolution Protocol (ARP) tabela omogućava mapiranje mrežnih adresa na fizičke adrese. Prikaz sadržaja ove tabele omogućen je pomoću **arp -a** naredbe.



```
C:\Windows\system32>arp -a

Interface: 192.168.1.111 --- 0x3
    Internet Address      Physical Address      Type
    192.168.1.1           74-ea-3a-d2-d4-be    dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff    static
    224.0.0.2             01-00-5e-00-00-02    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    224.0.0.253           01-00-5e-00-00-fd    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Windows\system32>
```

Slika 11 – Sadržaj ARP tabele lokalnog računara

5. Pregled utičnica na lokalnom računaru

Netstat dijagnostički program prikazuje statistike protokola i trenutne TCP/IP konekcije sa i prema drugim mrežnim uređajima. Na komandnoj liniji potrebno je upisati **netstat -a** da bi se prikazale sve konekcije i portovi na kojima se te konekcije uspostavljaju. Opcija **-n** upućuje Netstat da ne prevodi adrese i brojeve portova u imena, čime se ubrzava izvršavanje. Moguće je kombinovati različite opcije unutar jedne komande. Na slici 9 prikazan je primer komande **netstat -a -n**.

```

C:\Windows\system32\cmd.exe

C:\Users\milosp>netstat -a -n

Active Connections

Proto Local Address          Foreign Address        State
TCP    0.0.0.0:80               0.0.0.0:0              LISTENING
TCP    0.0.0.0:135              0.0.0.0:0              LISTENING
TCP    0.0.0.0:443              0.0.0.0:0              LISTENING
TCP    0.0.0.0:445              0.0.0.0:0              LISTENING
TCP    0.0.0.0:902              0.0.0.0:0              LISTENING
TCP    0.0.0.0:912              0.0.0.0:0              LISTENING
TCP    0.0.0.0:2343             0.0.0.0:0              LISTENING
TCP    0.0.0.0:3389             0.0.0.0:0              LISTENING
TCP    0.0.0.0:3580             0.0.0.0:0              LISTENING
TCP    0.0.0.0:3582             0.0.0.0:0              LISTENING
TCP    0.0.0.0:8080             0.0.0.0:0              LISTENING
TCP    0.0.0.0:12793            0.0.0.0:0              LISTENING
TCP    0.0.0.0:26143            0.0.0.0:0              LISTENING
TCP    0.0.0.0:48080            0.0.0.0:0              LISTENING
TCP    0.0.0.0:49152            0.0.0.0:0              LISTENING
TCP    0.0.0.0:49153            0.0.0.0:0              LISTENING
TCP    0.0.0.0:49154            0.0.0.0:0              LISTENING
TCP    0.0.0.0:49155            0.0.0.0:0              LISTENING
TCP    0.0.0.0:49286            0.0.0.0:0              LISTENING
TCP    0.0.0.0:52582            0.0.0.0:0              LISTENING
TCP    0.0.0.0:57000            0.0.0.0:0              LISTENING
TCP    0.0.0.0:59110            0.0.0.0:0              LISTENING
TCP    0.0.0.0:59111            0.0.0.0:0              LISTENING
TCP    0.0.0.0:59112            0.0.0.0:0              LISTENING
TCP    127.0.0.1:898            0.0.0.0:0              LISTENING
TCP    127.0.0.1:899            0.0.0.0:0              LISTENING
TCP    127.0.0.1:49156          127.0.0.1:49157        ESTABLISHED
TCP    127.0.0.1:49157          127.0.0.1:49156        ESTABLISHED
TCP    127.0.0.1:49158          127.0.0.1:49159        ESTABLISHED
TCP    127.0.0.1:49159          127.0.0.1:49158        ESTABLISHED
TCP    127.0.0.1:49163          127.0.0.1:49164        ESTABLISHED
TCP    127.0.0.1:49164          127.0.0.1:49163        ESTABLISHED
TCP    127.0.0.1:49173          127.0.0.1:49174        ESTABLISHED
TCP    127.0.0.1:49174          127.0.0.1:49173        ESTABLISHED
TCP    127.0.0.1:49175          127.0.0.1:49176        ESTABLISHED
TCP    127.0.0.1:49176          127.0.0.1:49175        ESTABLISHED
TCP    127.0.0.1:49179          0.0.0.0:0              LISTENING
TCP    127.0.0.1:49179          127.0.0.1:49196        ESTABLISHED
TCP    127.0.0.1:49179          127.0.0.1:49225        ESTABLISHED
TCP    127.0.0.1:49179          127.0.0.1:49226        ESTABLISHED
TCP    127.0.0.1:49179          127.0.0.1:49227        ESTABLISHED
TCP    127.0.0.1:49179          127.0.0.1:49228        ESTABLISHED
TCP    127.0.0.1:49179          127.0.0.1:49231        ESTABLISHED
TCP    127.0.0.1:49179          127.0.0.1:49381        ESTABLISHED
TCP    127.0.0.1:49182          0.0.0.0:0              LISTENING
TCP    127.0.0.1:49183          127.0.0.1:49184        ESTABLISHED
TCP    127.0.0.1:49184          127.0.0.1:49183        ESTABLISHED
TCP    127.0.0.1:49192          127.0.0.1:49193        ESTABLISHED
TCP    127.0.0.1:49193          127.0.0.1:49192        ESTABLISHED

```

Slika 12 - Primer netstat naredbe

Broj iza dvotačke je broj porta koji konekcija koristi, dok kolona *State* predstavlja trenutno stanjekonekcije po pojedinoj adresi i portu (tj. utičnici).

Postoji veći broj (tačnije 10) mogućih stanja konekcije od kojih ćemo izdvojiti samo neke:

- LISTENING – Server je spreman za prihvatanje konekcije
- ESTABLISHED – Uspostavljena konekcija sa udaljenim hostom
- CLOSED – Zatvorena konekcija prema udaljenom hostu
- CLOSE_WAIT – Server je u procesu raskida konekcije prema klijentu
- TIME_WAIT – Klijent je u procesu raskida konekcije prema serveru.

6. Pregled IP tabele rutiranja

IP tabelu rutiranja koja se nalazi na lokalnom računaru moguće je prikazati korišćenjem komande *netstat -r*.

- *Network Destination* - izlistane su sve dostupne mreže na koje je moguće poslati poruku;
- *Netmask* - data je lista subnet maski koje definišu koji deo adrese pripada mreži a kojiračunaru
- *Gateway* – lista adresa koju lokalni računr koristi da bi mogao poslati poruku na njenoodredište. “On-link” vrednost u koloni označava da je odredište direktno dostupno.
- *Interface* – Logička adresa mrežne kartice koja se koristi da bi se poslao paket kagateway-u.
- *Metric* – koliko „košta” korišćenje date putanje. Veća vrednost metrike ukazuje na lošijuputanju za slanje poruka (sporiju brzinu slanja, nebezbednost, ...)

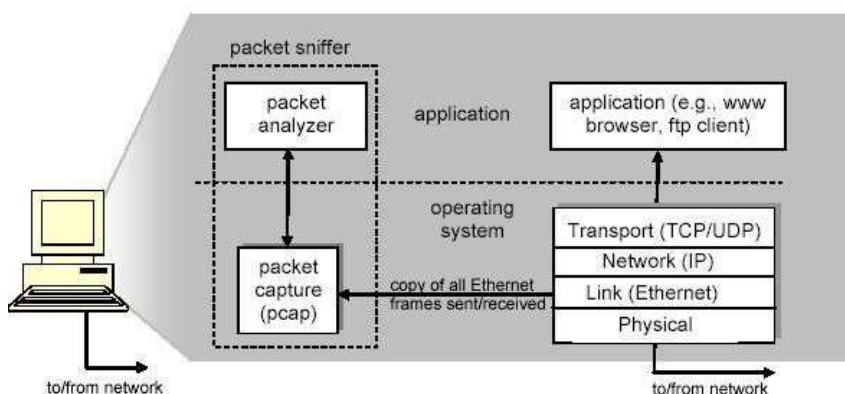
```
C:\Windows\system32>netstat -r
=====
Interface List
 5...1e 65 9d f3 5d 3a .....Microsoft Wi-Fi Direct Virtual Adapter
 3...1c 65 9d f3 5d 3a .....Broadcom 802.11n Network Adapter
 1.....Software Loopback Interface 1
 6...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
 23...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.111    30
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
192.168.1.0                255.255.255.0    On-link          192.168.1.111    286
192.168.1.111              255.255.255.255  On-link          192.168.1.111    286
192.168.1.255              255.255.255.255  On-link          192.168.1.111    286
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.1.111    286
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          192.168.1.111    286
=====
Persistent Routes:
None
```

Slika 13 – Lokalna IP tabela rutiranja

Wireshark

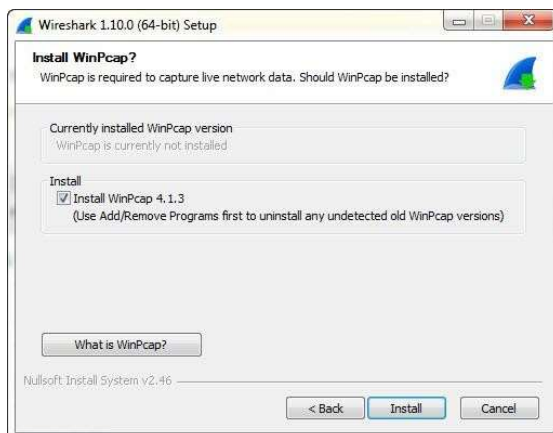
Wireshark je besplatan i open-source program za analizu paketa koji se koristi za otklanjanje grešaka (engl. *Troubleshooting*), analizu mrežnog saobraćaja, podršku programiranju mrežnih aplikacija i u edukaciji. Ovaj program je *packet sniffer* tj. omogućava presretanje i kopiranje u memoriju paketa koji prođu kroz mrežnu karticu računara. Pored presretanja, wireshark pruža grafički uvid u sadržaj uhvaćenih paketa, kao i vođenje raznih statistika koje bi pružile dublji uvid u saobraćaj mrežne kartice koja se prati. Analiza paketa omogućena je po pojedinačnim slojevima (PDU) na osnovu odgovarajuće RFC specifikacije. Pokriveni su svi nivoi od nivoa veze do aplikativnog nivoa, izuzev fizičkog nivoa, koji odstranjuje sama kartica prilikom prijema poruke.



Slika 1 – Struktura packet sniffer-a

Wireshark pripada grupi pasivnih programa, jer ne učestvuje u kreiranju i slanju paketa, već samo njihovom hvatanju, analizi i prikazivanju. U savremenom svetu postoji podeljenost u mišljenju da li je ispravno koristiti *packet sniffer*-e, zbog mogućnosti prisluškivanja saobraćaja koji ne pripada samom korisniku.

Wireshark 2.0.2 se može besplatno preuzeti sa stranice www.wireshark.org. Prilikom instalacije programa treba izabrati opciju da se instalira i WinPcap biblioteka, jer bez nje nije moguće hvatati saobraćaj uživo sa mreže.

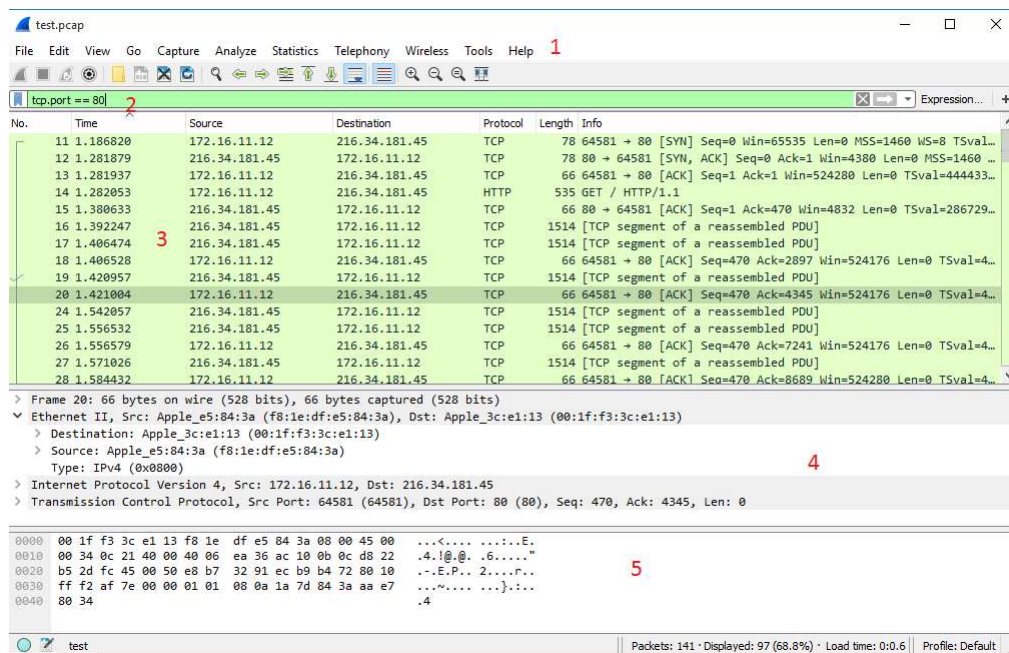


Slika 2. Izbor instaliranja WinPcap biblioteke

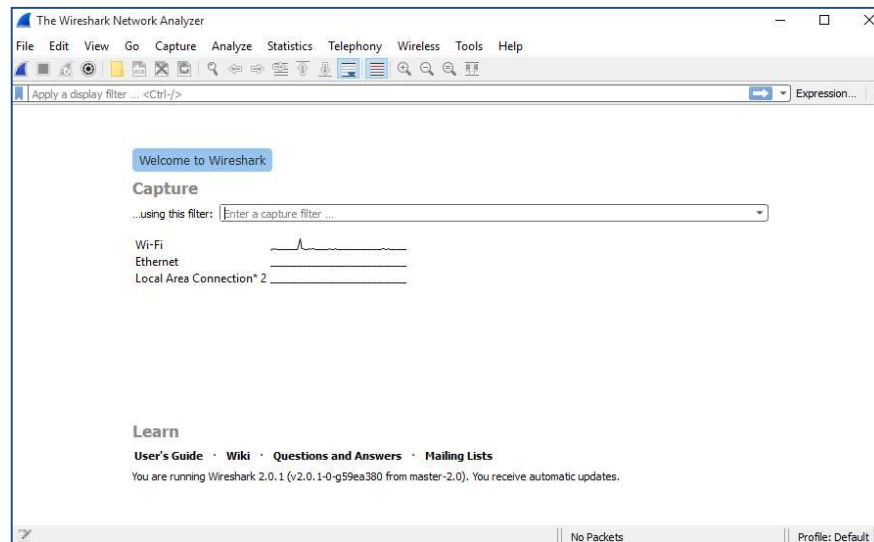
Wireshark interfejs ima pet osnovnih komponenti:

1. **Komandni meni** – standardni padajući meni koji se nalaze na vrhu prozora. U njemu se nalaze sve moguće komande koje su implementirane u aplikaciji. Najznačajnije stavke menija:
 - *File* - omogućava čuvanje “uhvaćenih” paketa ili otvaranje fajla koji sadrži prethodno uhvaćene pakete.
 - *Capture* - omogućava početak “hvatanja” paketa i odabir mrežne kartice koja će se koristiti.
 - *Statistics* – mogućnost analize saobraćaja mrežne kartice praćenjem statistike zasnovane na korišćenim protokolima, adresama, portovima...
2. **Polje za filtriranje** – u koje se mogu uneti ime protokola ili druge informacije, kako bi se u prikazu uhvaćenih paketa) izdvojili samo paketi koji su od interesa korisniku.
3. **Prikaz uhvaćenih paketa** – prikazuje podatke za svaki “uhvaćeni” paket, uključujući broj paketa (koji mu dodeljuje Wireshark; ovo nije broj paketa koji se nalazi u zaglavlju bilo kog protokola), trenutak u kojem je paket uhvaćen, adresu izvora i destinacije paketa, tip protokola i specifičnu informaciju o protokolu koja se nalazi u svakom paketu. Lista paketa može biti sortirana po bilo kojoj od ovih kategorija klikom na ime kolone.
4. **Prikaz detalja paketa** – obezbeđuje detalje o paketu koji je selektovan u listi uhvaćenih paketa
5. **Prikaz sirovog paketa** – prikazuje sadržaj selektovanog paketa u heksadecimalnom i ASCII zapisu.

Dve heksadecimalne cifre prikazuju po 1 bajt paketa ($16 \times 16 = 2^8 = 256$)

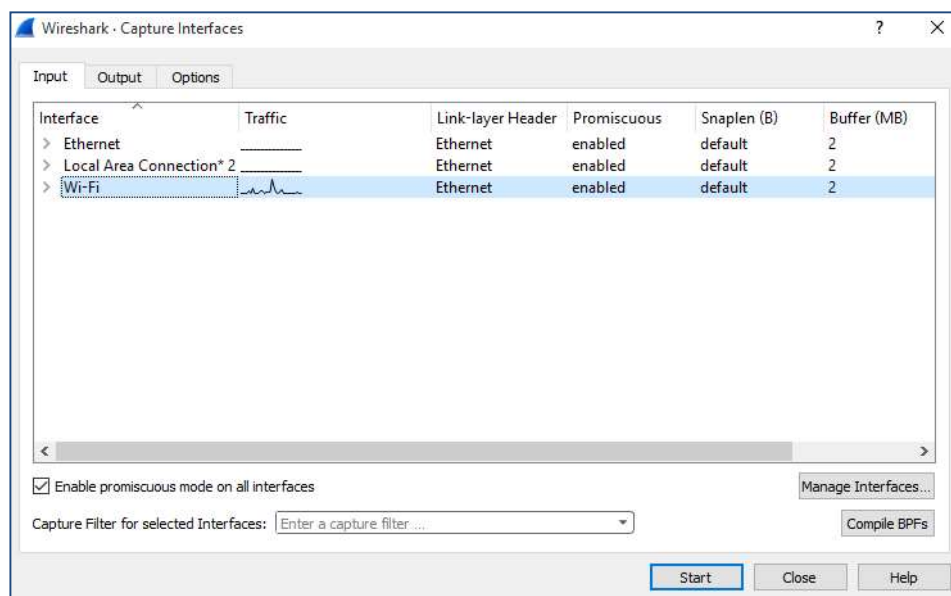


Slika 4 – Prikaz osnovnih komponenti Wireshark aplikacije



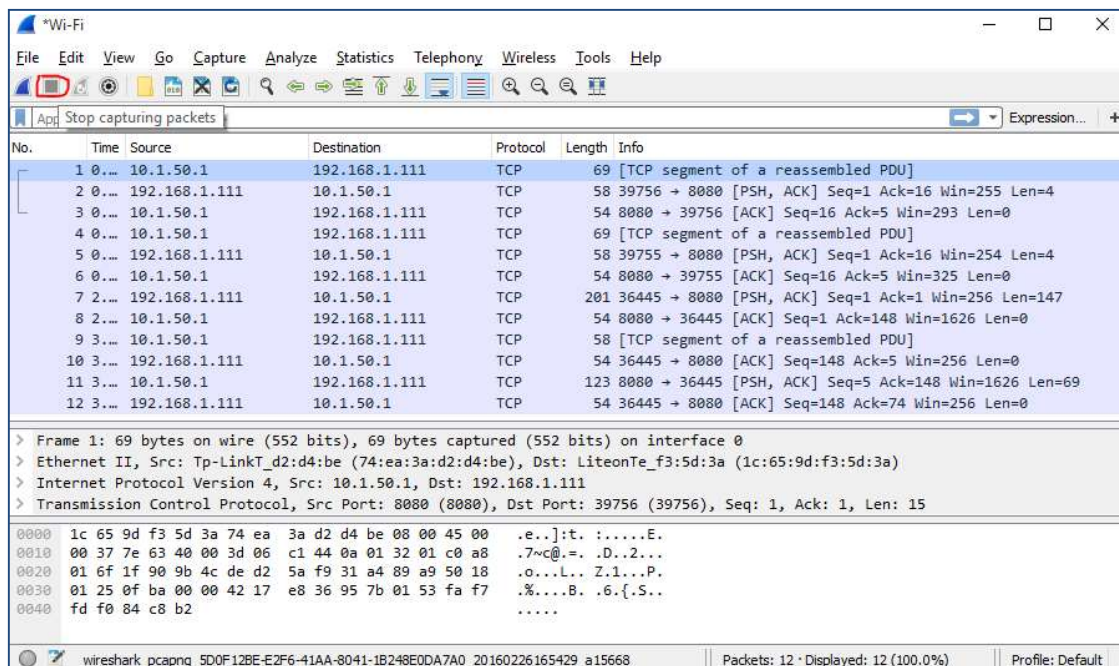
Slika 3 – Početna stranica Wireshark-a

Na početku programa potrebno je otvoriti meni *Capture* → *Options*, kako bi se izabrala mrežna kartica na kojoj želimo hvatati pakete. Obratiti pažnju da računar može imati više mrežnih kartica i da je potrebno izabrati onu karticu na kojoj želimo analizirati saobraćaj. Nakon što je odabrana odgovarajuća kartica, pokretanjem programa vrši se pomoću dugmeta *Start*.



Slika 5 – Prozor za odabir mrežne kartice

Nakon pokretanja programa možemo uočiti da je program počeo da ispisuje u redove pakete koji su prošli kroz mrežnu karticu. Kada se prikupi dovoljan broj paketa za analizu, process prikupljanja paketa se može prekinuti komandom *Stop* koja se nalazi u meniju sa alatima.



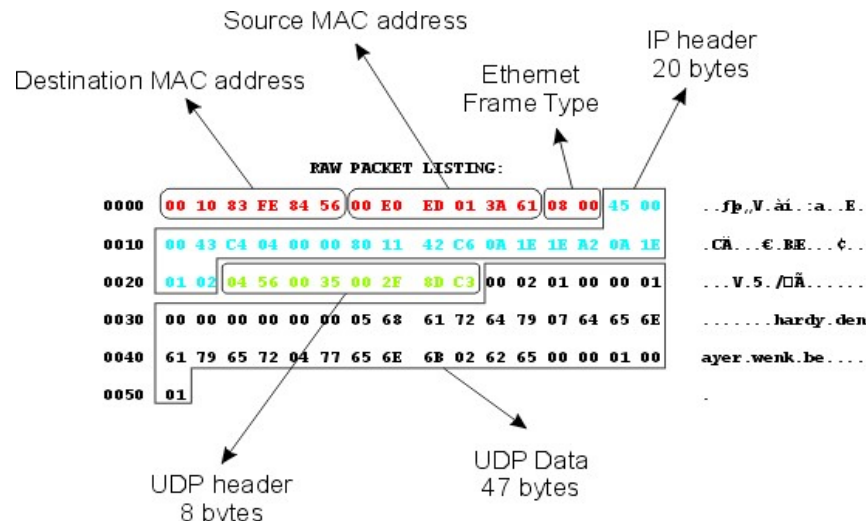
Slika 6 - Izgled prozora sa uhvaćenim paketima

U tabelu su upisani svi paketi koji su prošli kroz mrežnu karticu u periodu kada je bio uključen režim za analizu saobraćaja određene mrežne kartice. Svakom paketu dodeljen je jedan red u čijim poljima se nalaze sledeće informacije:

1. Redni broj koji je Wireshark aplikacija dodelila paketu
2. IP adresa pošiljaoca poruke
3. IP adresa primaoca poruke
4. Protokol najvišeg nivoa koji je korišćen pri slanju poruke
5. Ukupna dužina poruke
6. Neke od važnih informacija koje se nalaze u samoj poruci

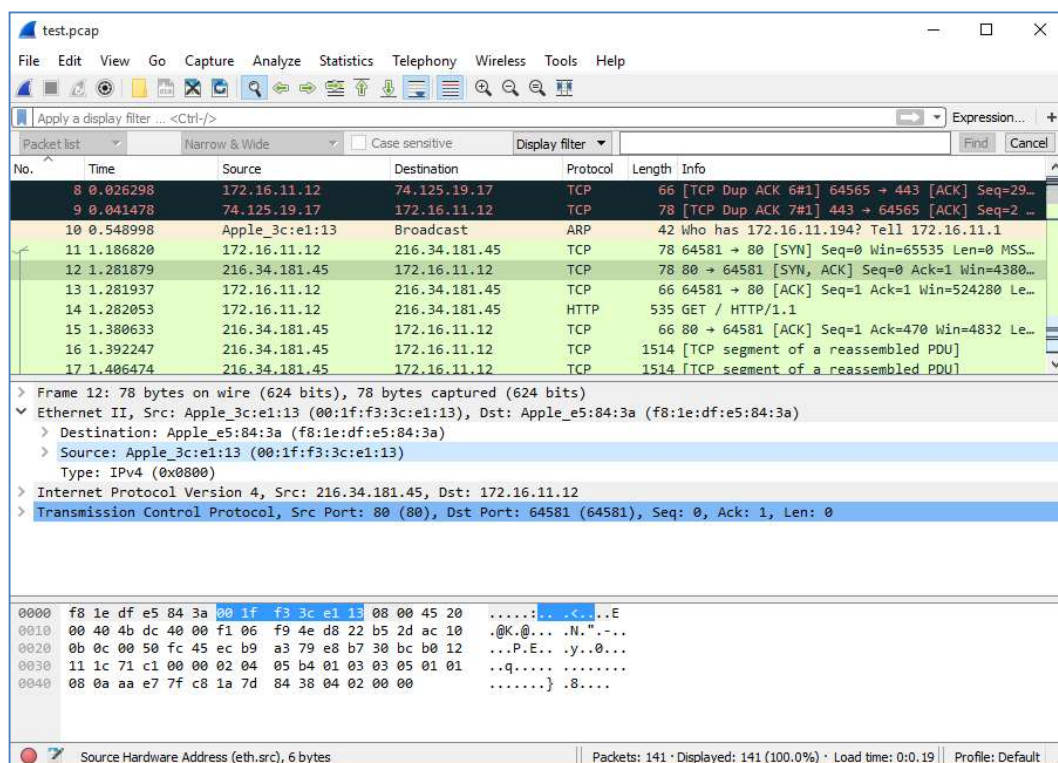
Ukoliko je potrebno doznati nešto više informacija o samom paketu, potrebno je selektovati paket kako bi se prikazala struktura protokola iz kojih je izgrađen paket po slojevima OSI modela. Data je mogućnost pristupa svakom polju određenog sloja. Pored toga, u dnu aplikacije nalazi se prikaz sadržaja označenog paketa po bajtima.

Kao primer analize paketa na slici 7 je prikazan jedan UDP segment. Prilikom formiranja paketa vršena je enkapsulacija podataka tako što je protokol na svakom sloju preuzimao podatke sa višeg sloja i dodavao mu svoje zaglavlje. Zadnji sloj koji dodaje svoje zaglavlje je sloj za pristup mreži (2. OSI nivo) i tada se dobija Ethernet okvir. Zato je Ethernet zaglavlje na vrhu paketa (sa odredišnom i izvorišnom MAC (fizičkom) adresom i oznakom tipa okvira). Iza njega sledi zaglavlje IP protokola (3. OSI nivo), a potom ide UDP zaglavlje (4. OSI nivo) i UDP podaci.



Slika 7 – Analiza uhvaćenog paketa na primeru UDP segmenta

Na slici 8 prikazana je fizička adresa pošiljaoca paketa u hijerarhiji protokola. Može se sa slike uočiti da je u prikazu sirovih podataka uokvireno 6 bajta, što odgovara veličini fizičke adrese.

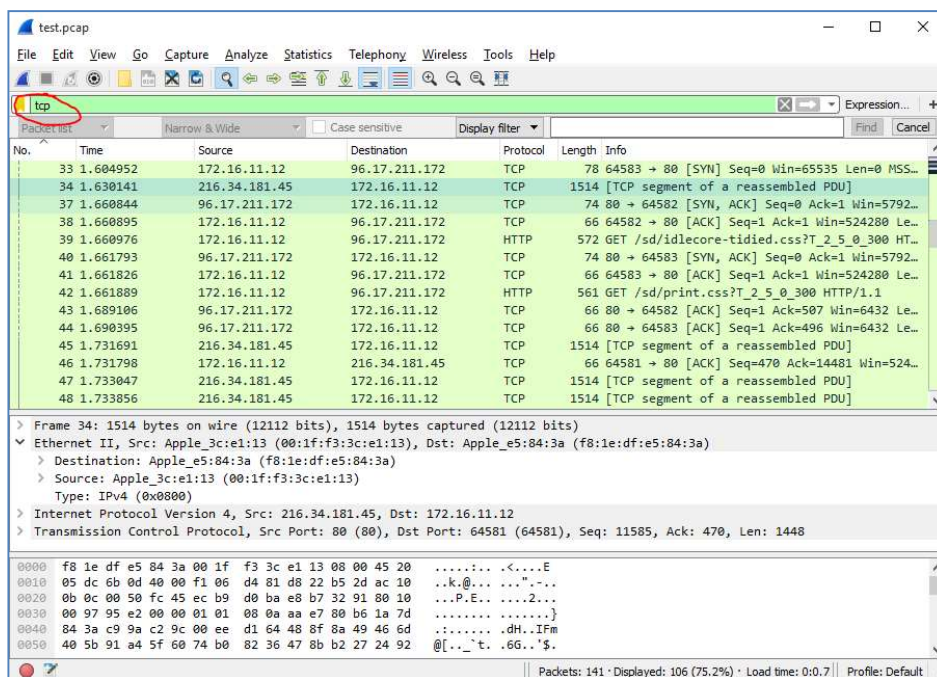


Slika 8 – Detaljan prikaz pojedinačnog paketa

Paketi se mogu markirati ako se u listi paketa odabere opcija desnog klika na odgovarajući paket i izabere *Mark Packet* stavka iz popup menija.

Filtiranje paketa

Često veliki broj uhvaćenih paketa može otežati analizu saobraćaja. Opcija filtriranja omogućava da se prikaže samo deo paketa koji zadovoljava uslov koji je dat u izrazu filtera. Ukoliko, na primer, želimo na ekranu prikazati samo pakete koji koriste TCP protokol, potrebno je u polje za filtriranje uneti *tcp* (malim slovima – imena svih protokola se pišu malim slovima u Wireshark-u) i zatim kliknuti dugme *Apply*.



Slika 9 - Filtriranje liste paketa

U nastavku su navedeni još neki primeri koji pokazuju na koje sve načine je moguće formirati izraz za filtriranje:

Izraz	Značenje
<i>arp</i>	Prikaz svih paketa koji koriste ARP protokol
<i>tcp.port == 80</i>	Prikaz svih paketa koji koriste TCP protokol i port 80
<i>ip.addr == 10.0.0.1</i>	Prikaz svih paketa koji koriste ip adresu 10.0.0.1
<i>ip.src == 192.168.1.100 and ip.dst == 192.168.1.101</i>	Prikaz svih paketa čiji pošiljaoc koristi ip adresu 192.168.1.100, a primao ip adresu 192.168.1.101
<i>http or dns</i>	Prikaz svih paketa koji koriste http ili dns protokol

Rad sa datotekom

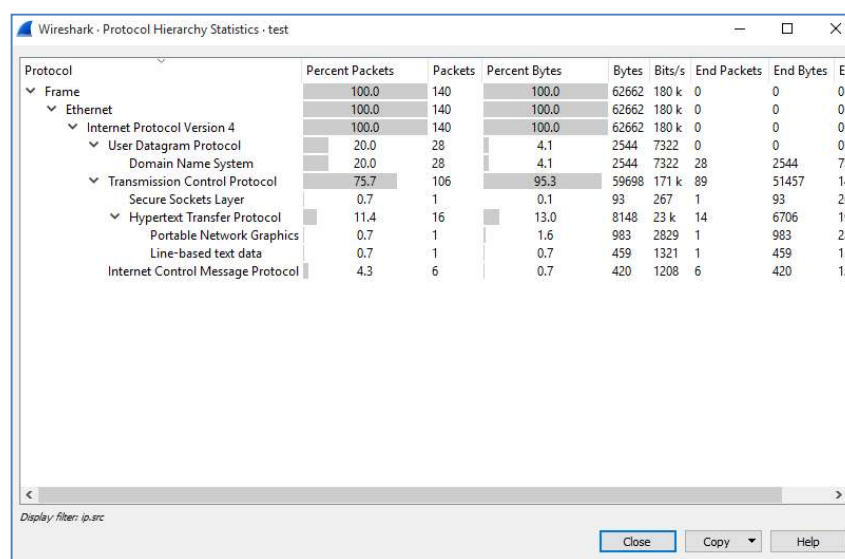
Otvaranje uhvaćenih paketa iz datoteke moguć je korišćenjem dvoklika miša na datoteku ili pomoću menija *File → Open*.

Ukoliko je potrebno snimiti uhvaćene pakete u datoteku, potrebno je izabrati opciju menija *File* → *Save As*.

Ukoliko želimo snimiti samo pojedine pakete potrebno je izabrati opciju *File* → *Export Specified Packets* i izabrati da je potrebno snimiti samo pakete koji su markirani i prikazani.

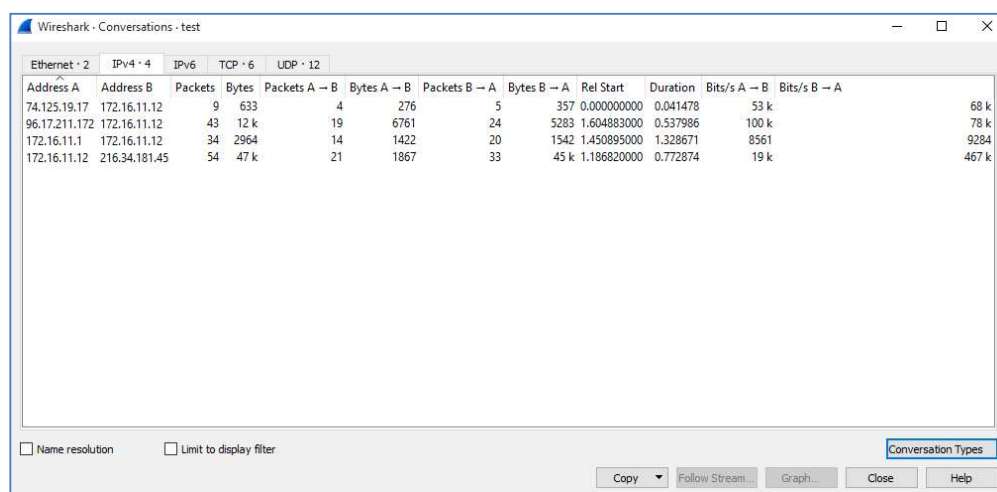
Statistika mrežnog saobraćaja

Statistika u kojoj je prikazano koliko je koji od protokola bio zastupljen u procentima u odnosu na ukupan broj analiziranih paketa omogućena je odabirom stavke iz menija: *Statistics* → *Protocol Hierarchy*.



Slika 10 - Statistika zastupljenosti protokola

Analiza statistike pojedinačnih konverzacija, omogućena je odabirom *Statistics* → *Conversations*



Slika 11 – Statistika pojedinačnih konverzacija

ZADATAK VEŽBE

1. Koristeći *ipconfig* komandu potrebno je otkriti:
 - a) logičku adresu računara
_____.
 - b) fizičku adresu računara
_____.
2. Nakon toga otvoriti sa Wireshark aplikacijom *example.pcap* datoteku koja je data u materijalima vežbe i odgovoriti na sledeća pitanja:
 - a) Koja je fizička adresa pošiljaoca prvog paketa iz liste?
_____.
 - b) Koliko DNS paketa je uhvaćeno?
_____.
 - c) Koji protokol koristi 10-ti paket iz liste i kolika je ukupna dužina tog paketa?
_____.
 - d) Koja je logička adresa primaoca poslednjeg paketa iz liste i kolika je dužina zaglavlja mrežnog sloja u tom paketu?
_____.
 - e) Koji aplikativni protokol je za transport koristio UDP?
_____.
 - f) Koji transportni protokol su koristili HTTP paketi?
_____.
 - g) Na koji port odredišta je bio poslat prvi zahtev za uspostavom veze?
_____.
 - h) Koliku količinu podataka je poslao računar sa ip adresom 96.17.211.172?
_____.
 - i) Koji je najveći broj porta koji je korišćen za komunikaciju?
_____.