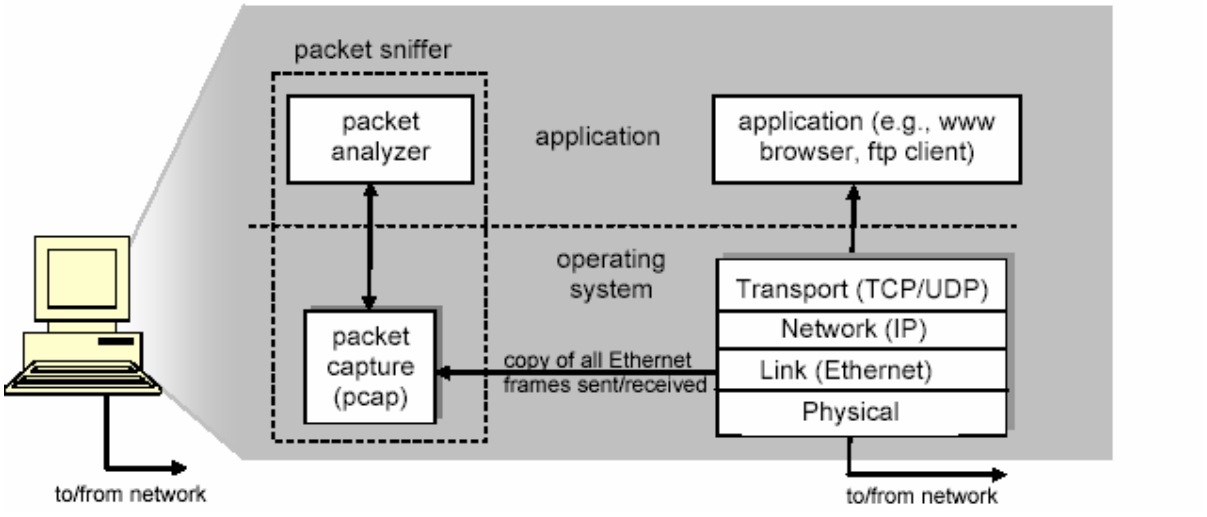
Vežba 7 – Wireshark

Za bolje razumevanje mrežnih protokola, najbolje je posmatrati „protokol u akciji“, odnosno posmatrati sekvence poruka koje se razmenjuju između dva entiteta.

Osnovni alat za posmatranje poruka koje se razmenjuju između izvršnih protokol entiteta naziva se ***packet sniffer***. Ovaj alat „hvata“ poruke koje se šalju ili primaju na računaru i prikazuje polja različitih protokola.

Packet sniffer je sam po sebi pasivan program. On posmatra poruke koje su poslate ili primljene od strane aplikacija i protokola na računar, ali nikad ne šalje pakete sam.
Takođe, primljeni paketi nikada nisu eksplicitno adresirani na *packet sniffer*. *Packet sniffer* prima kopije paketa koje su poslate/primljene na aplikacije i protokole koji se izvršavaju na računaru.

Na slici 1. prikazana je struktura *packet sniffer*-a. Na desnoj strani nalaze se protokoli (u ovom slučaju Internet protokoli) i aplikacije (kao što su web browser-i ili ftp klijent) koji se nalaze na računaru.



Slika 1. Struktura *packet sniffer-a*

Packet sniffer, označen isprekidanim pravougaonikom na slici 1. je dodatak uobičajenom softveru na računaru i sastoji se od dva dela:

- ***packet capture library*** - prima kopiju svakog okvira nivoa linka (*link-layer frejma*) koji je primljen na računaru, ili se šalje sa računara. Inače, poruke se razmenjuju

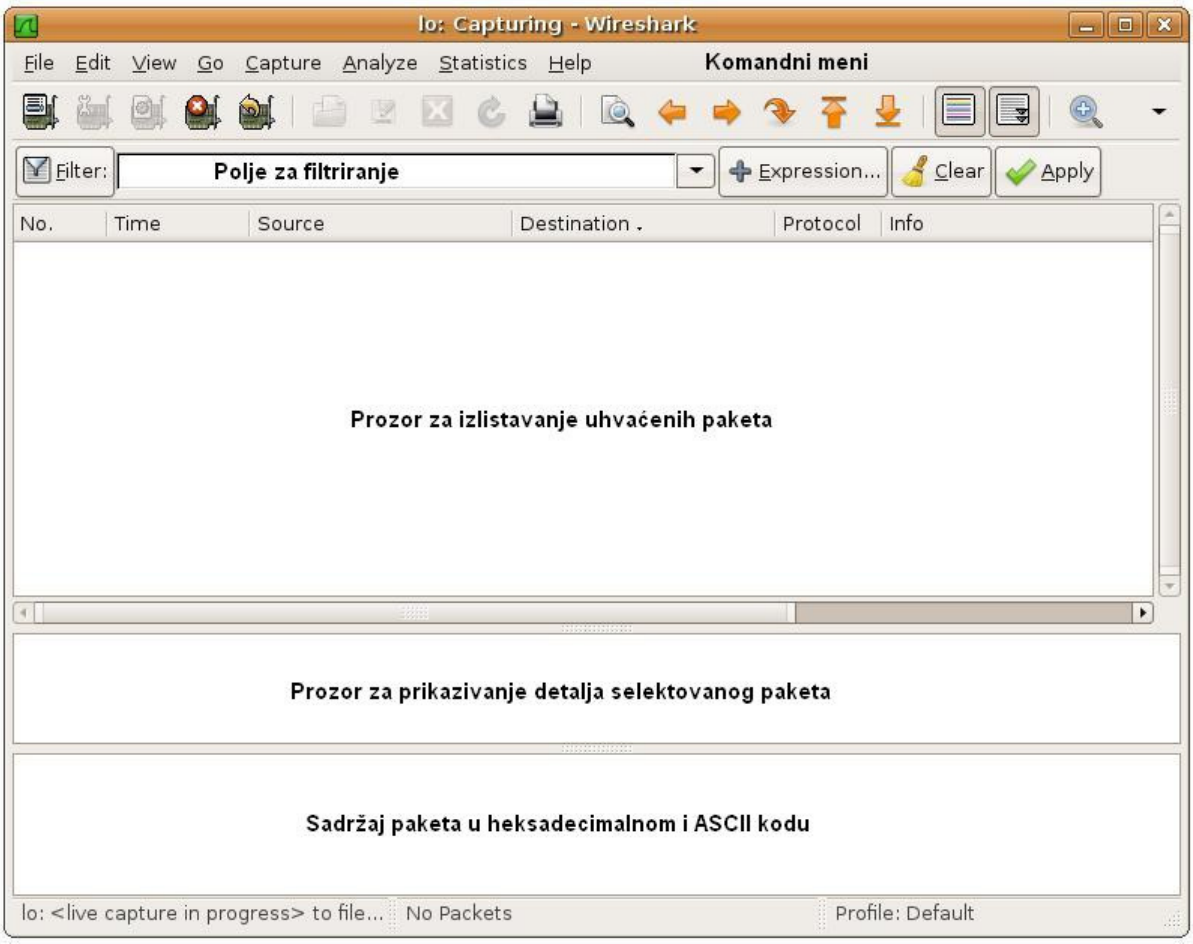
pomoću protokola viših nivoa kao što su HTTP (*Hyper-Text Transfer Protocol*), FTP (*File Transfer Protocol*), TCP (*Transmission Control Protocol*), UDP (*Internet Protocol*), DNS (*Domain Name System*) ili IP (*Internet Protocol*). Svi oni su sadržani u okviru nivoa linka. Na slici 1. pretpostavljeno je da je nivo linka Ethernet i svi protokoli viših nivoa su obuhvaćeni u okviru Ethernet okvira. Prema tome, "hvatajući" sve okvire nivoa linka dobijaju se sve poruke koje su poslate ili primljene od protokola i aplikacija koje se izvršavaju na računaru.

- ***packet analyzer*** - prikazuje sadržaj svih polja u okviru poruke.

1. Korišćenje Wireshark aplikacije

Instalacija Wireshark-a u Raspbian OS-u (u terminalu uneti): **sudo apt-get install wireshark**

Wireshark je besplatan mrežni *protocol analyzer* koji radi pod Windows, Linux/Unix i Mac operativnim sistemom. Kada se pokrene Wireshark program, pojavljuje se grafički korisnički interfejs prikazan na slici 2.



Slika 2. Wireshark grafički korisnički interfejs

Wireshark interfejs ima pet osnovnih komponenti:

- ***Command menus*** (komandni meni) **-** standardni padajući menii koji se nalaze na vrhu prozora. Najznačajni su:
  - *File* - omogućava čuvanje "uhvaćenih" paketa ili otvaranje fajla koji sadrži prethodno uhvaćene pakete.
  - *Capture* - omogućava početak "hvatanja" paketa.

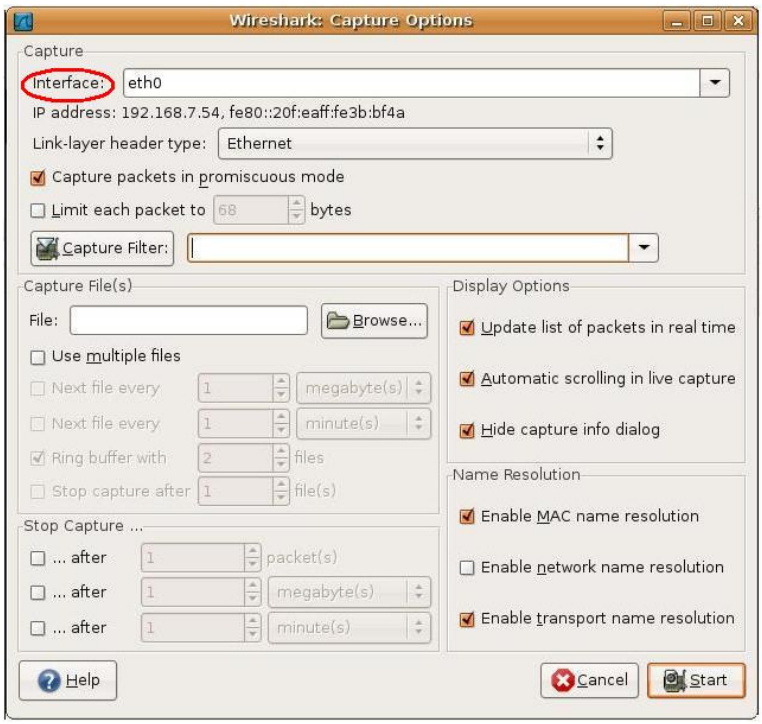
- ***Packet-listing window*** (prozor za prikazivanje uhvaćenih paketa) – prikazuje podatke za svaki "uhvaćeni" paket, uključujući broj paketa (koji mu dodeljuje Wireshark; ovo nije broj paketa koji se nalazi u zaglavlju bilo kog protokola), trenutak u kojem je paket uhvaćen, adresu izvora i destinacije 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.

- ***Packet - header details window*** (prozor za prikazivanje detalja selektovanog paketa) - obezbeđuje detalje o paketu odabranom u *packet listing* prozoru.

- ***Packet - contents window* -** prikazuje ukupan sadržaj uhvaćenog paketa u ASCII i heksadecimalnom zapisu.

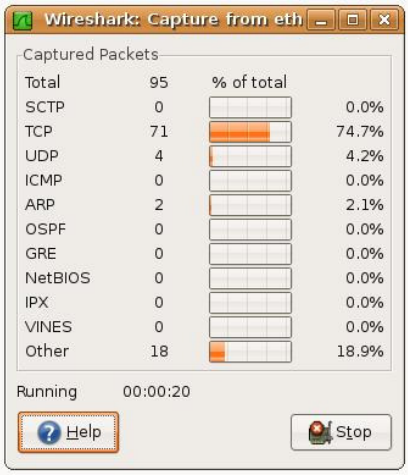
- ***Filter*** (polje za filtriranje) u koje se mogu uneti ime protokola ili druge informacije, kako bi se u packet-listing prozoru (kao i packet–header i packet–contents prozorima) izdvojile samo one informacije koje nas zanimaju.

Kako bi se započelo hvatanje paketa, potrebno izabrati ***Capture*** padajući meni i izabrati ***Options***.
Pojaviće se prozor kao na slici 3.



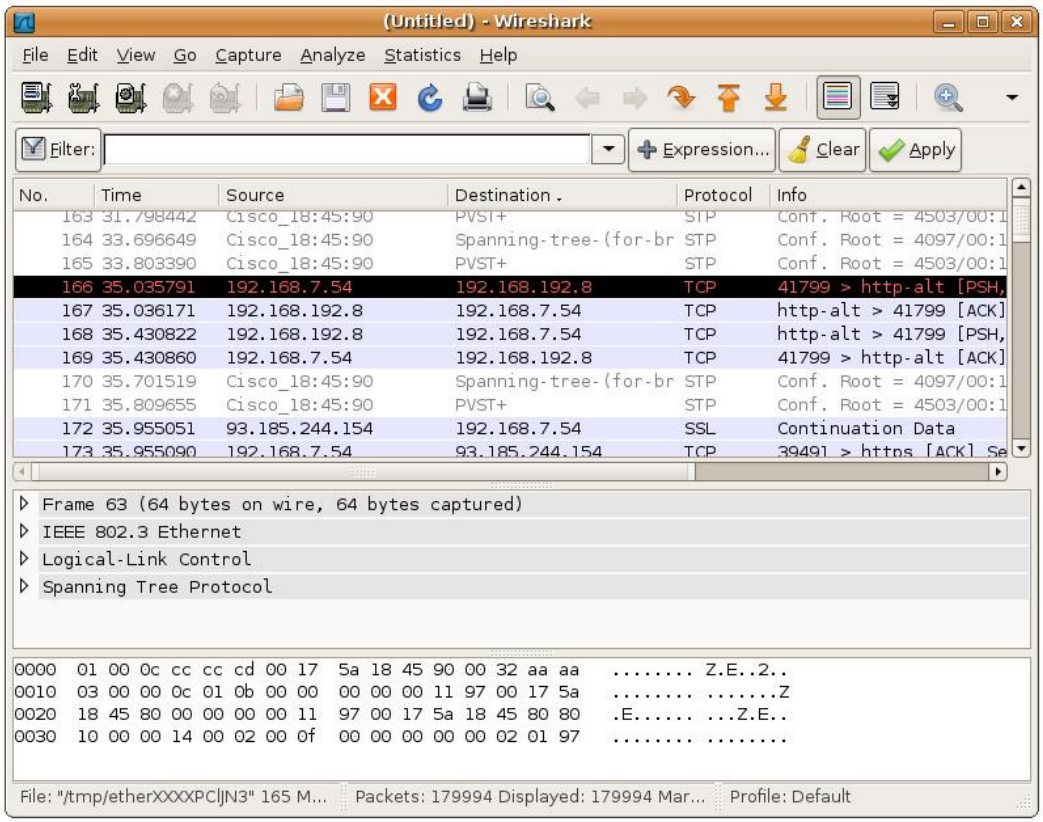
Slika 3. Wireshark *Capture Options* prozor

U *Capture options* prozoru potrebno je odabrati jednu od mrežnih kartica koje se nalaze u računaru (npr. wireless ili wired Ethernet, u našem slučaju je to *eth0*)., a zatim kliknuti **Start**, nakon čega počinje hvatanje paketa.
Ukoliko je deselektovana opcija u *Capture Options – Display options – Hide capture info dialog*, pojaviće se ***packet capture summary*** prozor, kao na slici 4. Ovaj prozor prikazuje broj paketa različitih tipova protokola koji su uhvaćeni.



Slika 4. Wireshark *Packet Capture summary* prozor

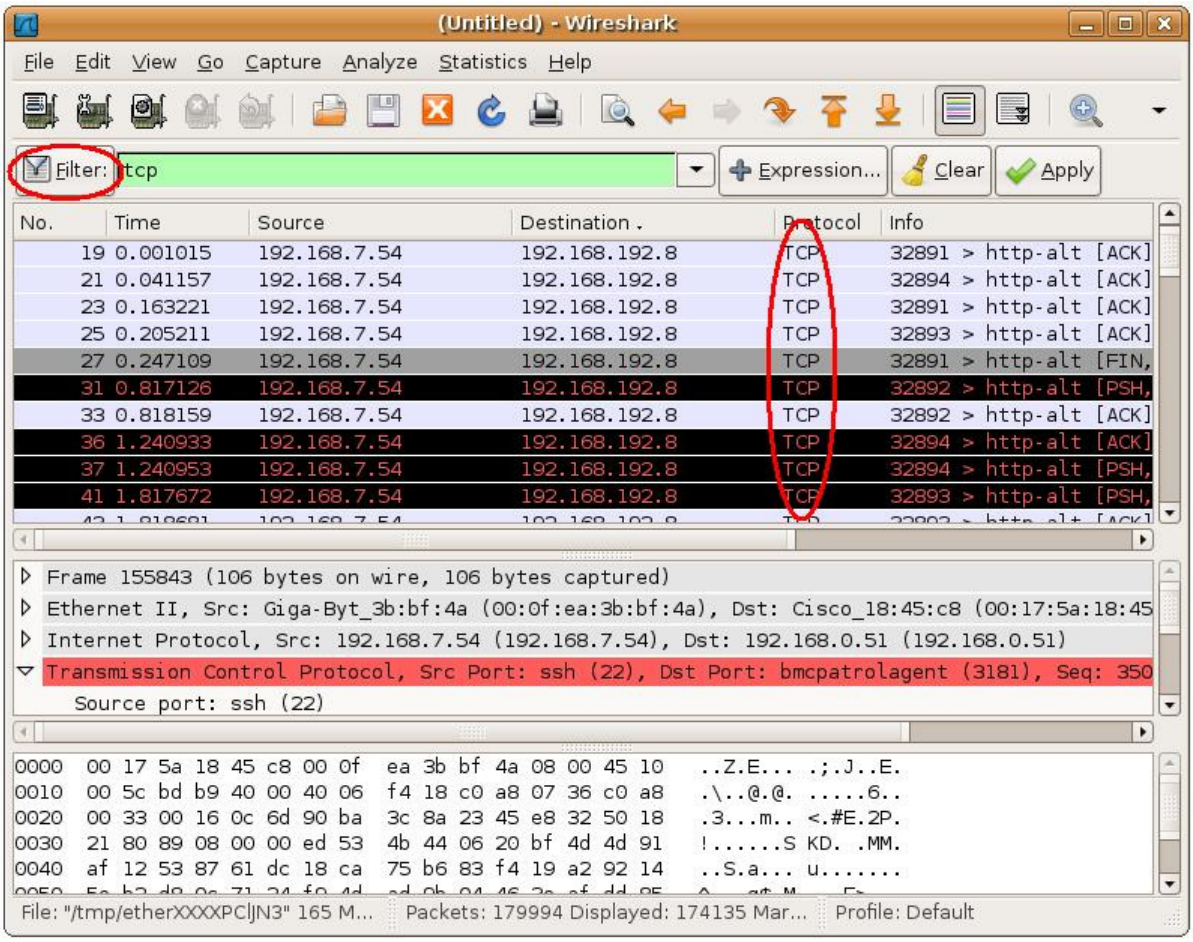
Ukoliko želimo da vidimo uhvaćene pakete, potrebno je pritisnuti dugme ***Stop*** u *Packet Capture summary* prozoru. Nakon toga dobije se prozor kao na slici 5. sa prikazom svih uhvaćenih paketa.



Slika 5. Prikaz svih uhvaćenih paketa

Pored paketa koje možemo odmah prepoznati (pristup nekoj adresi na internetu, slanje paketa između dva računara itd.), evidentno je da postoji još mnogo drugih protokola koji obavljaju određene radnje na računaru, a koje korisnik ne vidi.

Kako bi videli samo pakete koji npr. koriste TCP protokol, u polje za filtriranje uneti ***tcp*** (malim slovima – imena svih protokola se pišu malim slovima u Wireshark-u) i zatim kliknuti ***Apply***. Sada će jedino TCP poruke biti prikazane u packet-listing prozoru, kao što je prikazano na slici 6.



Slika 6. Prikaz samo TCP razmenjenih poruka

2. TCP/IP model

TCP/IP je razvijen kao otvoren standard, što znači da ga svako može slobodno koristiti. Ovaj model sadrži četiri sloja:

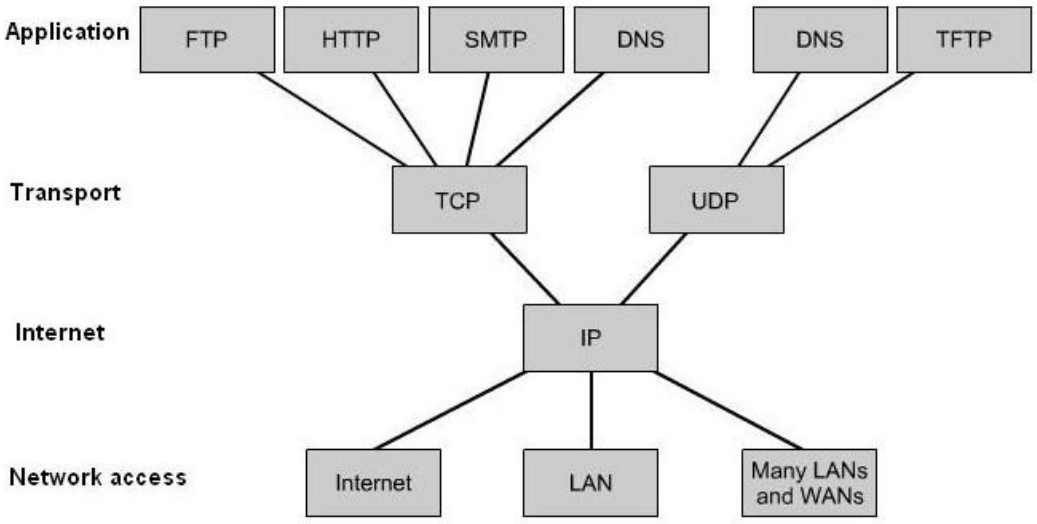
- Aplikativni (*Application layer*)
- Transportni (*Transport layer*)
- Internet (*Internet layer*)
- Mrežni (*Network access layer*)

Aplikacija sa ***aplikativnog*** sloja, koja interpretira podatke i prikazuje informacije u razumljivom obliku, koristi protokole za slanje i primanje podataka kroz mrežu. Kako bi se podaci poslali na odredišnu adresu, nižem sloju (***transportnom***) je potrebno poslati broj port-a koji će osigurati da će podaci stići do odgovarajućeg servisa koji će ih dalje obrađivati.
Kada su podaci prosleđeni transportnom sloju, TCP i UDP protokoli razbijaju podatke u manje delove – ***segmente***. Pošto nije sigurno na koji način će segmenti stizati do odredišta, koristi se mehanizam numerisanja segmenata (Sequence number). Segmenti koji stižu ne moraju biti vezani za istu aplikaciju, potrebno je imati i broj porta, tako da se u izvoru određuje i odredišni (aplikativni) i izvorni port (od pošaljioca). Mehanizam numerisanja (SEQ) i potvrde prijema (ACK) koristi TCP protokol, tako da se za njega kaže da je pouzdan, dok UDP spada u nepouzdane protokole. U poglavljima 3. i 4. je detaljno opisana struktura zaglavlja koje TCP i UDP dodaju segmentu.

Segmenti se dalje isporučuju sledećem nižem sloju (***internet***), koji pomoću IP protokola segmentu dodaje svoje zaglavlje u kojem se nalazi izvorna IP adresa računara i odredišna IP adresa dobijena od aplikacije. Stvara se jedinstvena celina koja se naziva ***paket*** ili ***datagram***. Zaglavlje koje IP protokol dodaje paketu, detaljno je objašnjeno u poglavlju 5.

Kada paket stigne na niži nivo (***mrežni***), dodaje se zaglavlje koje se sastoji od izvorne i odredišne MAC adrese, dužine, podataka i kontrolne sume koja se dodaje na kraju. Ovaj skup podataka naziva se ***okvir*** (frame). Detaljan opis okvira je dat u poglavlju 6.

Na slici 7. je prikazano na koji način protokoli koriste TCP/IP model tj. odnos slojeva i protokola.



Slika 7. TCP/IP model i protokoli

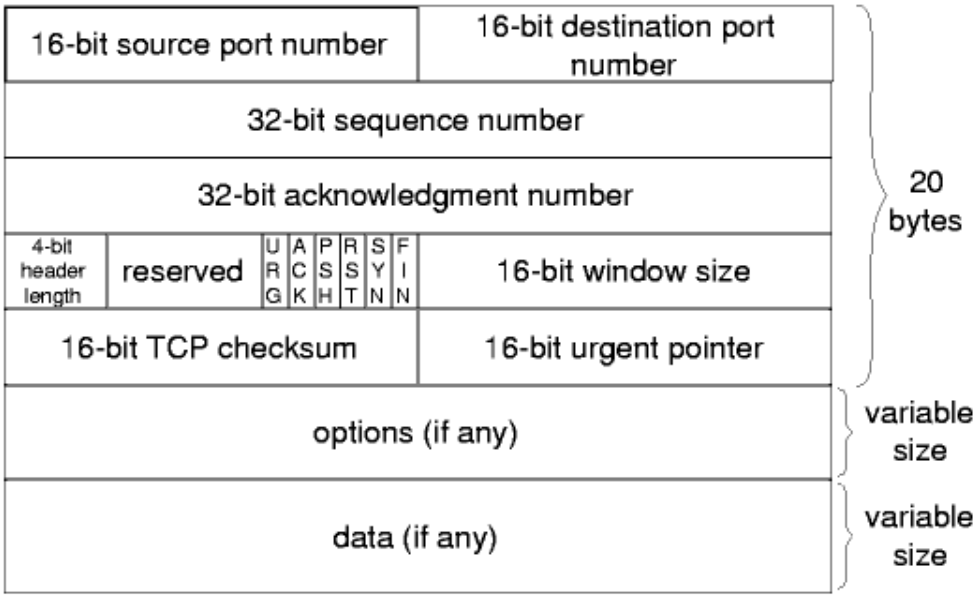
3. Opis TCP paketa

TCP protokol definiše uslugu pouzdane isporuke toka (engl. stream) korisničkih podataka. Osobine TCP-a su:

- Obavlja kontrolu toka podataka i obezbeđuje komunikaciju sistema različitih brzina.
- Osnovna jedinica prenosa TCP-a je segment podataka. Segmenti se koriste za prenos upravljačke informacije (npr. poruke za uspostavu i raskid veze), ili za prenos podataka.
- Kontrola toka realizovana tako što prijemnik oglašava količinu podataka koju je spreman da primi.
- TCP takođe podržava poruke van opsega (engl "out of band"), koje služe za slanje urgentnih podataka i za forsiranje isporuke korišćenjem (engl "push") podataka.

TCP vrši transfer podataka kao nestruktuiran niz bajtova koji se identifikuju sekvencom. Bajtovi se grupišu u segmente i dodeljuje se broj sekvence, dok se aplikacijama dodeli broj porta i prosleđuje se IP protokolu.

Strana koja prima podatke šalje broj sekvence bajta koji je primio i u slučaju da destinacija ne pošalje ACK da je primio određenu sekvencu bajtova u određenom vremenskom intervalu ona će biti naknadno ponovo poslata.



Slika 8. Izgled TCP segmenta

Na slici 8. je dat prikaz TCP segmenta, koji se sastoji iz zaglavlja i dela u kome se nalaze podaci.

Zaglavlje se sastoji iz:

- ***Source port*** – prolaz koji identifikuje aplikaciju na izvorištu.
- ***Destination port*** – prolaz koji identifikuje aplikaciju na odredištu.
- ***Sequence number*** – Broj sekvence prvog okteta podataka u segmentu (osim ukoliko je SYN postavljen). Kada je SYN prisutan, broj sekvence koji sledi je početni broj sekvence (ISN – Initial Sequence Number) i prvi oktet podataka ima vrednost ISN+1.

- ***Acknowledgment number*** – ACK je upravljački bit. Ukoliko je postavljen ovaj bit, ovo polje sadrži vrednost sledećeg broja sekvence kojeg pošaljioc segmenta očekuje da primi.
- ***Header length*** – dužina zaglavlja (4 bita). Pokazuje gde počinju podaci.
- ***Reserved*** – rezervisana polja za buduću upotrebu.
- ***URG, ACK, PSH, RST, SYN, FIN*** – kontrolni biti.
- ***Window*** – Broj okteta koje prijemna strana još može primiti. Ovo polje govori predajnoj strani da može slati segmente sve dok ukupni broj okteta koje treba poslati ne bude veće od broja okteta upisanih u polju prozor. Kada je veličina prozora jednaka 0, predajna strana treba prekinuti slanje podataka dok ne dobije segment u kojem je veličina prozora veća od nule.
- ***Checksum*** – kontrolna suma za proveru bitskih grešaka.
- ***Urgent pointer*** – pokazivač prioriteta – važnost poruke koja se šalje. Ukazuje na broj sekvence okteta u kojem su hitni podaci. Može se interpretirati samo u segmentima za koje je URG upravljački bit postavljen.
- ***Options*** – opciona informacija.

Data – Podaci koji se šalju (ako postoji opciona informacija, podaci počinju na 192. bitu, inače od 160. bita).

Značenje određenih bita u ***CODE BITS*** polju :

- ***URG*** - polje urgentnog pokazivača je važeće.
- ***ACK*** - polje potvrde je važeće.
- ***PSH*** - ovaj segment zahteva operaciju potiskivanja «push».
- ***RST*** - resetuj vezu.
- ***SYN*** - sinhronizuj brojeve sekvenci.
- ***FIN*** - pošiljaoc je došao do kraja toka podataka.

Neki rezervisani portovi koje koristi TCP:

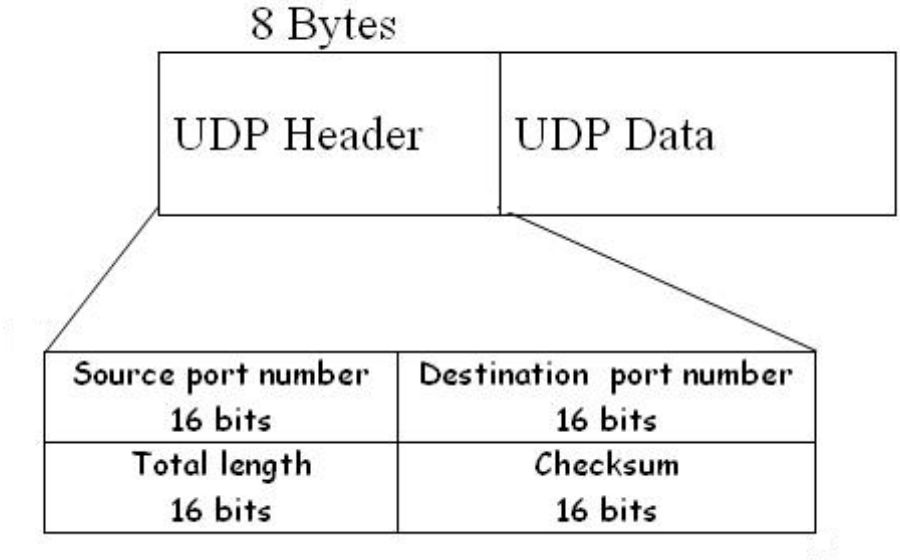
- FTP – 21
- SSH – 22
- Telnet – 23
- SMTP – 25
- HTTP – 80

4. Opis UDP paketa

UDP protokol definiše uslugu nepouzdane isporuke korisničkih podataka (datagrama). UDP razlikuje više procesa na jednoj mašini i omogućava predajniku (engl. Sender) i prijemniku (engl. Receiver) da svakoj UDP poruci dodaju dva 16-bitna broja, koji identifikuju prolaze izvora i odredišta.

Osobine UDP-a:

- Nepouzdana isporuka podataka.
- Nije obavezna uspostava konekcije pre slanja podataka.
- Ne koristi *sequence number, acknowledgment number*, niti obavlja kontrolu toka podataka.



Slika 9. Izgled UDP segmenta

Zaglavlje se sastoji iz:

- ***Source port*** – prolaz koji identifikuje aplikaciju na izvorištu.
- ***Destination port*** – prolaz koji identifikuje aplikaciju na odredištu.
- ***Total length*** – ukupna veličina korisničkog datagrama (zaglavlje i podaci).
- ***Checksum*** – opciono polje. Koristi se za detekciju greške

UDP Data – podaci koji se šalju

UDP port se realizuje kao red čekanja (queue). OS stvara ovaj red na zahtev aplikacije. Aplikacija može da zada ili promeni veličinu reda čekanja. Nakon prijema UDP datagrama, UDP provera broj prolaza sa brojevima koji su trenutno u upotrebi. Ako se zadati prolaz ne koristi, šalje se ICMP poruka "port unreachable" i UDP datagram se odbacuje. U suprotnom, UDP ulančava UDP datagram u red čekanja, osim ako je on pun, kad dolazi do greške i odbacivanja primljenog UDP datagrama.

Postoji nekoliko slučajeva kada je bolje koristiti UDP umesto TCP protokola:

- Kada je blok podataka koji treba poslati mali, veličine jednog paketa – jednostavnije je, brže i efikasnije prenositi samo podatke (uz zaglavlje UDP-a), pa u slučaju pogrešno primljene poruke ponoviti slanje, nego uspostavljati vezu i proveravati pouzdanost prenosa.
- UDP koriste poruke tipa upita koje jedan računar šalje drugom, pri čemu se ako odgovor ne stigne u nekom određenom vremenu, zahtev ponovi ili se od njega odustane.
- Neke aplikacije imaju sopstvene tehnike za pouzdani prenos podataka i ne zahtevaju korišćenje TCP protokola, tako da je tada bolje koristiti UDP.

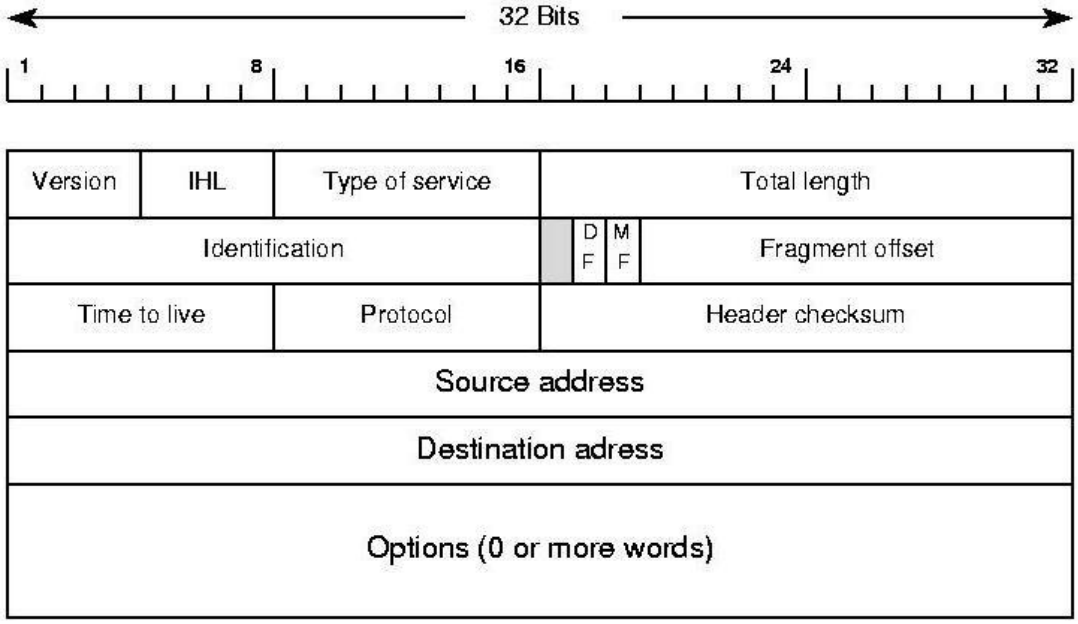
Neki rezervisani portovi koje koristi UDP:

- Echo – 7
- Daytime – 13

- Nameserver – 53
- Bootpc – 68
- RPC – 111
- NTP – 123

5. Opis IP paketa

Internet protokol (IP) je usmeravajući protokol za prenos datagrama.IP zaglavlje koje se dodaje kreiranom segmentu sadrži informacije potrebne da se novonastali paketi – datagrami usmere prema odredištu. Struktura IP zaglavlja prikazana je na slici 10.



Slika 10. Zaglavlje IP paketa

Zaglavlje IP paketa se sastoji iz:

- ***Version*** – Verzija internet zaglavlja.
- ***IHL*** – Internet header length – dužina internet zaglavlja tj. određuje gde počinju podaci.
- ***Type of service*** – Ukazuje na željeni kvalitet usluge – vrstu prometa. Podešavanje bita:
  - ***Biti 0-2 – prioritet***
    111 – Kontrola od strane mreže
    110 – Kontrola unutar mreže
    101 – CRITIC/ECP
    100 – Kratkotrajno opterećenje
    011 – Brzo
    010 – Direktno
    001 – Prioritet
    000 – Uobičajen postupak
  - ***Bit 3- kašnjenje***
    0 – Normalno kašnjenje
    1 – Malo kašnjenje
  - ***Bit 4 – propusna moć***
    0 – Normalna propusnost
    1 – Velika propusnost

- ***Bit 5 – pouzdanost***
  0 – Normalna pouzdanost
  1 – Velika pouzdanost
- ***Biti 6-7 – za buduću upotrebu***

- ***Total length –*** Dužina datagrama – uključuje internet zaglavlje i podatke.
- ***Identification*** – Identifikacijska vrednost datagrama koja služi odredištu da lakše sastavlja fragmente datagrama.
- ***Flags*** – DF, MF. Bit 0 je rezervisan, Bit 1 opisuje da li ima ili nema fragmentacije (0 – dopuštena fragmentacija, 1 – nije dopuštena). Bit 2 opisuje status pristiglog fragmenta (0 – poslednji fragment, 1 – ima još fragmenata).
- ***Fragment offset*** – Pokazuje mesto gde fragment pripada u datagramu.
- ***Time to live*** – Dužina trajanja datagrama. Pokazuje maksimalno vreme trajanja opstanka datagrama u mreži. Vreme je u sekundama. Po isteku TTL vremena datagram se odbacuje.
- ***Protocol*** – Ukazuje na sledeći protokol koji se koristi u delu sa podacima koji su sadržani u datagramu.
- ***Header checksum*** – Kontrolna suma zaglavlja.
- ***Source address*** – Izvorna adresa objekta
- ***Destination address*** – Odredišna adresa objekta
- ***Options*** – Opciono polje datagrama.

Data – podaci koji se šalju.

6. Opis mrežnog okvira

Nivo mreže dodaje zaglavlje datagramu i dobija se okvir. Struktura okvira data je da slici 11.

7 bytes	*1 byte*	*2 or 6 bytes*	*2 or 6 bytes*	*2 bytes*	*4-1500 bytes*				*4 bytes*
Preamble	Start Frame Delimiter	Dest. MAC address	Source MAC address	Length	(Data / Pad)				FCS
					DSAP	SSAP	CTRL	NLI	

Slika 11. Struktura Ethernet okvira

Ethernet okvir se sastoji iz:

- ***Preamble*** – Niz bita koji služi predajniku i prijemniku da sinhronizuju komunikaciju.
- ***Start frame delimiter*** – Uvek je postavljeno na 10101011 i koristi se kao početak okvira.
- ***Destination MAC address*** – MAC adresa računara koji prima podatke.
- ***Source MAC address*** – MAC adresa računara koji šalje podatke.
- ***Length*** – Dužina Ethernet okvira u bajtima.
- ***Data/Pading*** – Podaci. Ovde se nalazi IP zaglavlje i četiri specifična polja:
  - DSAP – Destination Service Access Point
  - SSAP – Source Service Access Point
  - CTRL – Control bits for Ethernet communication
  - NLI – Network Layer Interface
- **FCS** – Frame Check Sequence – računa se pomoću CRC i koristi se za detekciju grešaka u Ethernet okviru.

ZADATAK VEŽBE

- Posmatrati razmenu paketa između klijenta i servera preko TCP i UDP porta u Wireshark-u.