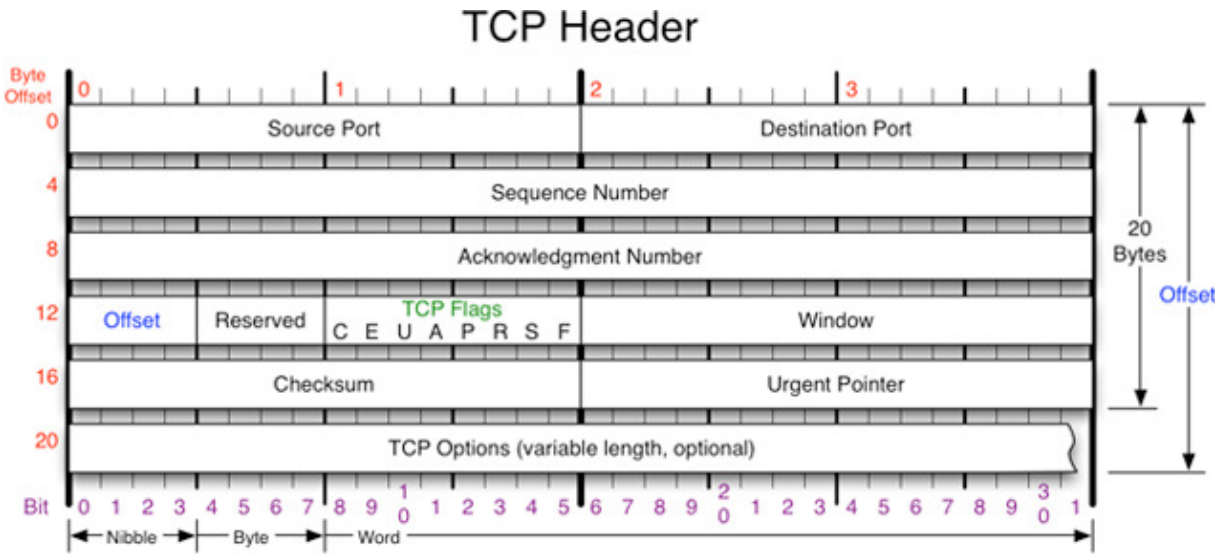
Vežba 7 – Interpretacija sadržaja mrežnih paketa upotrebom Libpcap (Raspbian) –WinPcap (Windows) programske biblioteke - nastavak

1. TCP zaglavlje protokola

TCP segment se sastoji iz TCP zaglavlja i podataka koji su dobijeni od nekog aplikacionog protokola (npr. HTTP, SMTP ili FTP). Izgled TCP zaglavlja je dat na slici 1.



Slika 1. TCP zaglavlje

TCP 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*** – Redni broj narednog bajta koji jedna strana u ostvarenoj TCP vezi očekuje da primi od druge. Ovim mehanizmom se drugoj strani potvrđuje ispravan prijem svih prethodno poslatih bajtova do rednog broja ACK-1.
- ***Header length*** – Dužina zaglavlja TCP segmenta izražena u umnošcima 32-bitnih reči. Zbog polja "Options" dužina zaglavlja je promenljiva, pa nam ovaj podatak ukazuje kolika je stvarna dužina TCP zaglavlja.
- ***Reserved*** – rezervisana polja za buduću upotrebu (4 bita).
- ***URG, ACK, PSH, RST, SYN, FIN*** – kontrolni biti (8 bita).
- ***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.

U nastavku je dat izgled strukture koja omogućava pristup poljima zaglavlja TCP protokola. Pošto veličina opcionih informacija varira, TCP zaglavlje nema konstantnu veličinu. Iz tog razloga do mesta u memoriji gde su smešteni aplikativni podaci se može doći korišćenjem veličine TCP zaglavlja koja je zapisana u okviru polja header_length. Vrednost upisanu u polje header_length treba pomnožiti sa 4 da bi dobili dužinu TCP zaglavlja izraženu u bajtima.

```
// TCP header
typedef struct tcp_header {
	unsigned short src_port;		// Source port
	unsigned short dest_port;		// Destination port
	unsigned int sequence_num;		// Sequence Number
	unsigned int ack_num;			// Acknowledgement number
	unsigned char reserved :4;		// Reserved for future use (4 bits)
	unsigned char header_length :4;	// Header length (4 bits)
	unsigned char flags;			// Packet flags
	unsigned short windows_size;		// Window size
	unsigned short checksum;		// Header Checksum
	unsigned short urgent_pointer;	// Urgent pointer
	// + Option bytes
} tcp_header;
```

ZADATAK

1. Omogućiti ispis instaliranih mrežnih kartica i odabir mrežne kartice na kojoj korisnik želi vršiti hvatanje paketa. **(0.2)**
2. Omogućiti hvatanje paketa otvaranjem mrežne kartice koja je odabrana. **(0.4)**
    - Za hvatanje je potrebno koristiti normalni režim rada mrežne kartice.
    - Iščitavanje paketa sa adaptera podesiti na vremenski period od 2 sekunde.
3. Proveriti da li odabrana mrežna kartica koristi Ethernet protokol na nivou veze. **(0.1)**
4. Omogućiti hvatanje 5 paketa korišćenjem callback funkcije. **(0.2)**
5. Podesiti filter na drajveru da se korisničkoj aplikaciji prosleđuju samo paketi koji zadovoljavaju sledeće uslove: **(0.4)**
    - Na nivou veze paketa koristi se Ethernet, a na mrežnom nivou IPv4 protokol
    - Za transport paketa se mogu koristiti UDP i TCP protokol.
    - Paket je poslat sa fizičke adrese računara koji student koristi.
6. Izračunati na kojoj memorijskoj lokaciji počinje Ethernet zaglavlje i ispisati na ekranu fizičku adresu primaoca paketa. **(0.4)**
7. Izračunati na kojoj memorijskoj lokaciji počinje IP zaglavlje i ispisati na ekranu logičku adresu primaoca paketa. **(0.4)**
8. Pomoću Wireshark aplikacije otkriti ime polja iz IP zaglavlja koje nosi informaciju koji od protokola je korišćen kao transportni protokol. Koja vrednost definiše da se radi o UDP protokolu, a koja o TCP protokolu? **(0.2)**
9. Ukoliko je na transportnom sloju korišćen TCP protokol, izračunati na kojoj memorijskoj lokaciji počinje TCP zaglavlje i ispisati na ekranu port primaoca paketa. **(0.2)**
10. Ukoliko je na transportnom sloju korišćen UDP protokol, izračunati na kojoj memorijskoj lokaciji počinje UDP zaglavlje i ispisati na ekranu port primaoca paketa. **(0.1)**
11. Omogućiti ispis aplikativnih podataka po bajtima korišćenjem heksadecimalnog zapisa za slučaj da je za transport korišćen TCP ili UDP protokol. **(0.4)**
    - Izračunati lokaciju u memoriji na kojoj se nalazi početak sadržaja koji pripada aplikativnom sloju.
    - Izračunati kolika je veličina podataka koji pripada aplikativnom sloju.