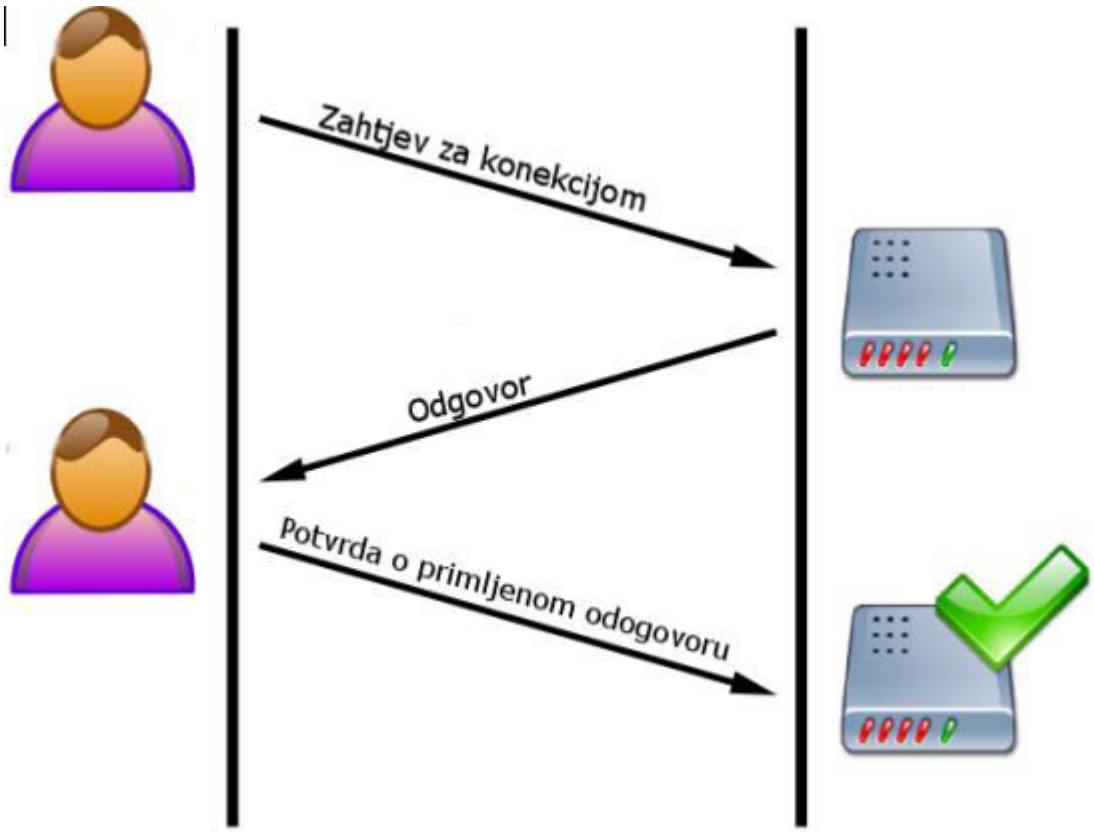
TEHNIČKA ŠKOLA
RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Nastavni predmet:	**RAČUNALNE MREŽE**
Vježba:	Protokoli transportnog sloja (TCP i UDP)
Cilj vježbe:	Naučiti pratiti i analizirati TCP i UDP segemente

Maja Markovac i Sven Grgić

PRIPREMA ZA VJEŽBU

1. Koje su prednosti i nedostaci protokola TCP?
   PREDNOSTI: retransmisija u slučaju oštećenja ili gubitka, prijenos cijeli poruke u izvornom obliku uz kontrolu kvarova i protoka.
   NEDOSTATCI: sporiji protocol od UDP-a.
2. Koje su prednosti i nedostaci protokola UDP?
   PREDNOSTI: ne zahtijeva obavijest o primitku i ne brine se je li svaki paket ispravno zaprimljen, veća brzina prijenosa.
   NEDOSTATCI: ne sadržava funkcije pouzdanosti, kontrole protoka ili oporavka od pogreške.
3. Skiciraj i objasni postupak uspostave TCP veze između klijenta i poslužitelja.



IZVOĐENJE VJEŽBE

- Pokrenuti program za praćenje mrežnog prometa Wireshark
- Odabrati mrežni adapter na kojem će se pratiti promet
- Pokrenuti praćenje prometa
- Pomoću preglednika učitati web stranicu po želji
- Zaustaviti praćenje prometa

1. Analizirati zaglavlje odlaznih i dolaznih TCP segmenata

```
Transmission Control Protocol, Src Port: 52707, Dst Port: 443, Seq: 1, Ack: 1, Len: 80
    Source Port: 52707
    Destination Port: 443
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 80]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 841070968
    [Next Sequence Number: 81    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2298858395
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1020
    [Calculated window size: 1020]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x086b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (80 bytes)
```

   a. Pronaći segmente pomoću kojih se uspostavila veza između klijenta i poslužitelja (SYN, SYN-ACK, ACK)

```
Data
[ACK] Seq=81 Ack=1 Win=1020 Len=1440 [TCP segment of a reassembled PDU]
[ACK] Seq=1521 Ack=1 Win=1020 Len=1440 [TCP segment of a reassembled PDU]
Data
Data
[ACK] Seq=1 Ack=81 Win=16382 Len=0
[ACK] Seq=1 Ack=1521 Win=16386 Len=0
[ACK] Seq=1 Ack=2961 Win=16380 Len=0
[ACK] Seq=1 Ack=3478 Win=16386 Len=0
[ACK] Seq=1 Ack=3516 Win=16385 Len=0
Data
[ACK] Seq=3516 Ack=147 Win=1019 Len=0
```

```
Flags: 0x018 (PSH, ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Accurate ECN: Not set
   .... 0... .... = Congestion Window Reduced: Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...1 .... = Acknowledgment: Set
   .... .... 1... = Push: Set
   .... .... .0.. = Reset: Not set
   .... .... ..0. = Syn: Not set
   .... .... ...0 = Fin: Not set
   [TCP Flags: ·····AP···]
Window: 516
```

b. Pronađene segmente usporedite sa skicom iz pripreme, zadatak 3.
POŠILJATELJ pošalje FIN i ACK, PRIMATELJ ih primi i šalje nazad, POŠILJATELJ primi i šalje nazad ACK, PRIMATELJ prima ACK.
POŠILJATELJ pošalje SYN, PRIMATELJ prima i šalje nazad SZN i ACK, POŠILJATELJ prima i šalje nazad ACK, PRIMATELJ prima ACK.

c. Koji je broj ishodišnog priključka (engl.port)?
52707

d. Koji je broj odredišnog priključka (engl.port)?
443

e. Pronađite brojeve koji označavaju redni broj segmenata (SEQ) i komentirajte!

```
ata
ACK] Seq=81 Ac
ACK] Seq=1521
ata
ata
ACK] Seq=1 Ack
ACK] Seq=1 Ack
ACK] Seq=1 Ack
ACK] Seq=1 Ack
ACK] Seq=1 Ack
ata
```

Broj dodijeljen prvom bajtu podataka u trenutačnoj poruci, stalno se mijenja.

f. Čemu služi oznaka Win?
Služi za označavanje prozora, što je oznaka za definiranje veličine pošiljateljevoga prostora mešuspremnika dostupnog za dolazne poruke.

g. Pronađite brojeve koji označavaju potvrdu primljenog segmenta (ACK) i komentirajte.

```
66 [ACK] Seq=122 Ack=109 Win=8 Len=0
 → 443 [ACK] Seq=109 Ack=123 Win=515 Len=0
ck=1 Win=507 Len=1
ck=2 Win=265 Len=0 SLE=1 SRE=2
68 [ACK] Seq=37 Ack=75 Win=8 Len=0
 → 443 [ACK] Seq=75 Ack=38 Win=515 Len=0
```

ACK: 109, 123, 1, 2, 75, 38
Vrijednost sljedećeg sekvencijskog broja koji pošiljatelj segmenta očekuje da će primiti ako je postavljen kontrolni bit; ACK označava da je taj broj valjan.

h. Koja su ostala polja TCP zaglavlja? Istražite i zapišite čemu služe!

+	Bitovi 0 - 3	4 - 9	10 - 15	16 - 31
0	Izvorišni port			Odredišni port
32	Broj sekvence			
64	Broj potvrde			
96	Podatkovni ofset	Rezervirano	Zastavice	Prozor
128	Checksum			Hitni pokazivač
160	Opcionalno			
192	Opcije (nastavak)			*Padding* (do 32)
224	Korisnički podaci			

- **izvorišni port (16 bitova) i odredišni port (16 bitova) – krajnje točke veze**
- **broj sekvencije (32 bita) – broj dodjeljen prvom bajtu podataka u trenutačnoj poruci**
- **broj potvrde (32 bita) – sadržava vrijednost sljedećeg sekvencijskog broja koji pošiljatelj segmenta očekuje da će primiti ako je postavljen kontrolni bit**
- **polje odstupanja podataka (duljina zaglavlja, promjenjive duljine) – Koliko je 32-bitnih riječi unutar TCP zaglavlja**
- **rezervirano polje (6 bitova) – uvijek nula, služi za buduću uporabu**
- **zastavice (6 bitova) – sadržava TCP zastavice,; URG, ACK, PSH, RST, SYN, FIN**
- **prozor (16 bitova) – definira veličinu međuspremnika dostupnog za dolazak podataka**
- **kontrolni zbroj (checksum, 16 bitova) – je li zaglavlje oštećeno tijekom transporta**
- **hitni pokazivač (16 bitova) – prvi hitni bajt podataka u paketu**
- **opcije (promjenjive duljine) – različite TCP opcije**
- **podatci (promjenjive duljine) – informacije gornjeg sloja, segment**

2. Analizirati zaglavlje odlaznih i dolaznih UDP segmenata
   a. Pronaći UDP segmente
      filtre - udp
   b. Koje protokole enkapsulira UDP?
      NFS, SNMP, DNS, TFTP, QUIC itd.
   c. Koji je broj ishodišnog priključka (engl.port)?
      443
   d. Koji je broj odredišnog priključka (engl.port)?
      59359
   e. Koja su ostala polja UDP zaglavlja? Istražite i zapišite čemu služe!

+	Bitovi 0 - 15	16 - 31
0	Polazni port	Ciljni/odredišni port
32	Duljina paketa	*Kontrolni zbroj*
64	Podatci	

- **duljina podataka (duljina paketa, 16 bitova) – duljina zaglavlja i podataka**
- **kontrolni zbroj (16 bitova) – je li zaglavlje oštećeno tijekom transporta**

3. Koja je uloga priključka u TCP i UDP segmentima?
   Uloga je identificiranje krajnjih točaka veze, to su logičke adrese procesa te omogućuju komunikaciju većeg broja aplikacija putem zajedničkog mrežnog sloja istovremeno, jer je svaki port jedinstven.
4. Za poznate protokole koje ste „ulovili“ navedite predefinirane brojeve priključaka (za TCP ili UDP)

Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer