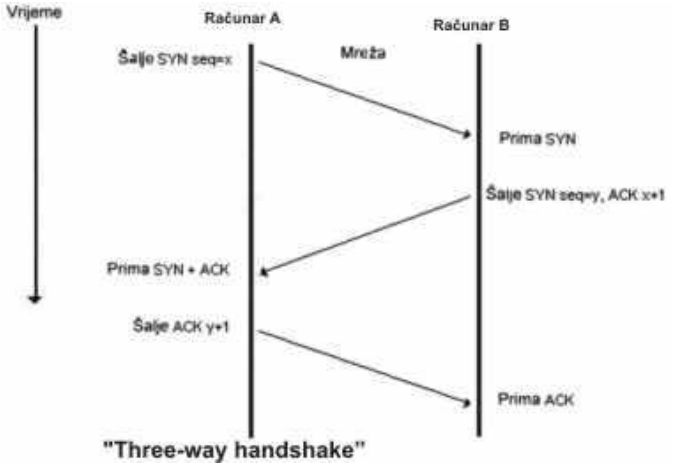
Nastavni predmet:	**RAČUNALNE MREŽE**
Vježba:	Protokoli transportnog sloja (TCP i UDP) **Ana Baćak i Ella Spivak 3.F**
Cilj vježbe:	Naučiti pratiti i analizirati TCP i UDP segemente

PRIPREMA ZA VJEŽBU

1. **Koje su prednosti i nedostaci protokola TCP?**
   Prednosti TCP protokola uključuju pouzdanu i redoslijednu dostavu podataka, kontrolu zagušenja radi održavanja performansi mreže te potvrde o primitku (ACK) za svaki poslani paket. *Međutim*, TCP je povezan protokol što može uzrokovati dodatan overhead i kašnjenje, te je složeniji u implementaciji i održavanju u usporedbi s drugim protokolima kao što je UDP, što može negativno utjecati na performanse mreže.

2. **Koje su prednosti i nedostaci protokola UDP?**
   Prednosti UDP protokola uključuju jednostavnost i nisku latenciju, što ga čini pogodnim za aplikacije poput streaminga i igara u stvarnom vremenu. Također, UDP ima manji overhead u usporedbi s TCP-om. Međutim, *nedostaci* UDP-a uključuju nedostatak pouzdanosti, nedostatak kontrole zagušenja i nedostatak potvrda o primitku, što može rezultirati gubicima podataka i neuređenom dostavom.

3. **Skiciraj i objasni postupak uspostave TCP veze između klijenta i poslužitelja.**
   Postupak uspostave TCP veze između klijenta i poslužitelja započinje kada klijent šalje SYN paket poslužitelju, koji sadrži inicijalni broj sekvence. Nakon primanja SYN paketa, poslužitelj odgovara s SYN-ACK paketom, potvrđujući primitak SYN paketa i specificirajući svoj inicijalni broj sekvence. Konačno, klijent potvrđuje primanje SYN-ACK paketa slanjem ACK paketa poslužitelju, koji potvrđuje broj sekvence poslužitelja. Ovaj trostruki rukovanje omogućuje uspostavu sinkronizirane TCP veze između klijenta i poslužitelja, pripremajući ih za komunikaciju i prijenos podataka.



IZVOĐENJE VJEŽBE

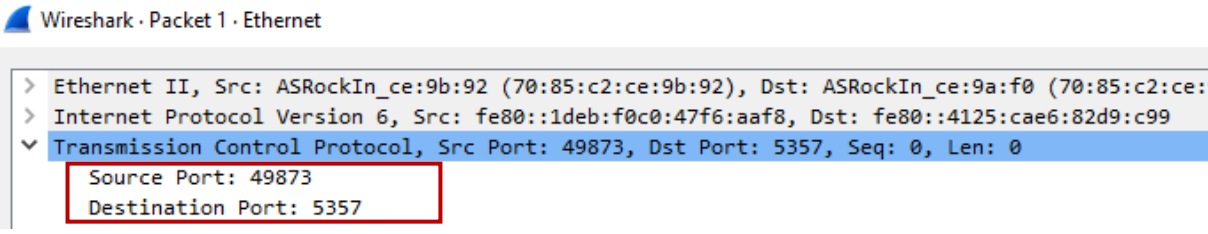
- Pokrenuti program za praćenje mrežnog prometa Wireshark
- Odabrati mrežni adapter na kojem će se pratiti promet
- Pokrenuti praćenje prometa
- Pomoću preglednika učitati web stranicu po želji
- Zaustaviti praćenje prometa

1. **Analizirati zaglavlje odlaznih i dolaznih TCP segmenata**
   a. **Pronaći segmente pomoću kojih se uspostavila veza između klijenta i poslužitelja (SYN, SYN-ACK, ACK)**

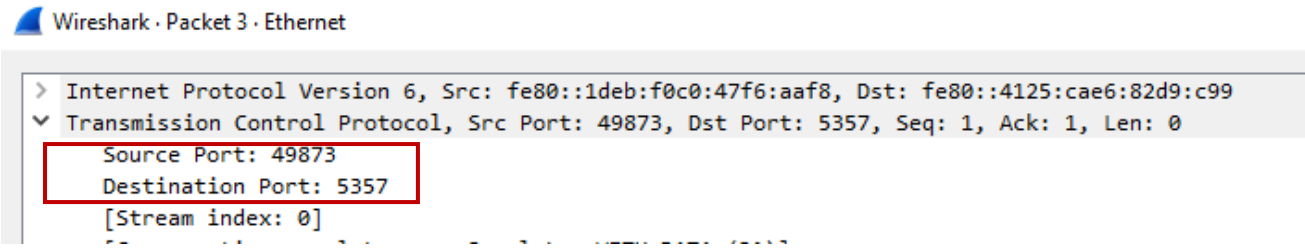
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::1deb:f0c0:47f…	fe80::4125:cae6:82d…	TCP	86	49873 → 5357 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
2	0.000054	fe80::4125:cae6:82d…	fe80::1deb:f0c0:47f…	TCP	86	5357 → 49873 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256
3	0.000359	fe80::1deb:f0c0:47f…	fe80::4125:cae6:82d…	TCP	74	49873 → 5357 [ACK] Seq=1 Ack=1 Win=2108160 Len=0

b. **Koji je broj ishodišnog priključka (engl.port) i odredišnog priključka (engl.port)?**

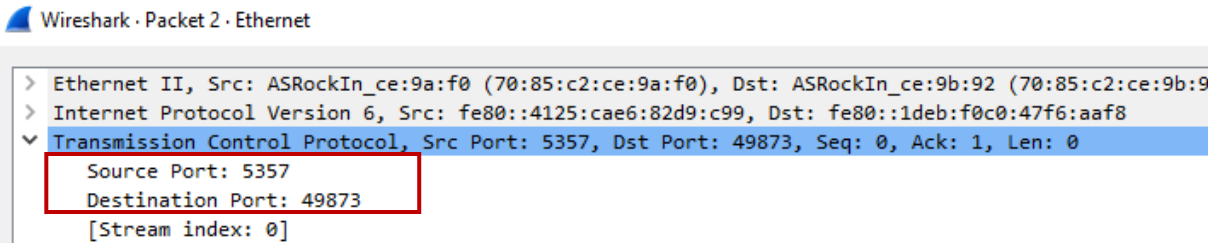
SYN



ACK

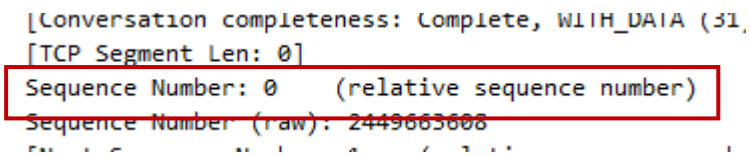


SYN,ACK

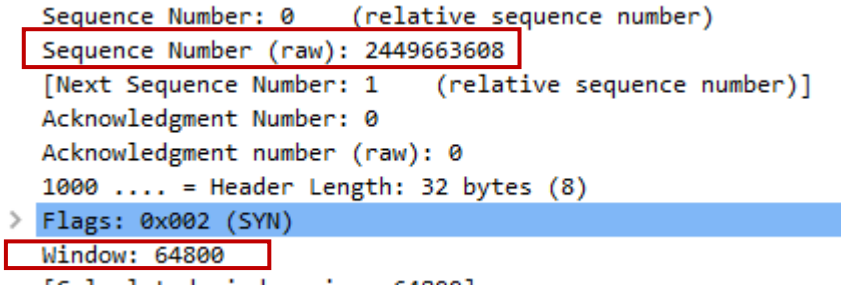


Segmenti su identični kao skica u 3. zadatku pripreme.
Prije nego što klijent i poslužitelj mogu razmjenjivati podatke, klijent i poslužitelj moraju uspostaviti TCP vezu. To se radi putem TCP trosmjernog rukovanja.
SYN - Klijent šalje SYN (Synchronize) paket poslužitelju
SYN ACK - Poslužitelj klijentu šalje paket SYN ACK (Synchronize Acknowledge)
ACK - Klijent šalje ACK (Acknowledge) paket poslužitelju
Trosmjerno rukovanje može se vidjeti u Wiresharku. U ovom primjeru, klijent šalje SYN (sinkroniziraj) paket poslužitelju , poslužitelj šalje SYN ACK (sinkroniziraj potvrda) paket klijentu, a klijent šalje ACK (potvrda) paket poslužitelju.

c. **Pronađite brojeve koji označavaju Koji je broj odredišnog priključka (engl.port)?** Broj sekvence (32 bita) specifira broj dodijeljen prvom bajtu podataka u trenutačnoj poruci



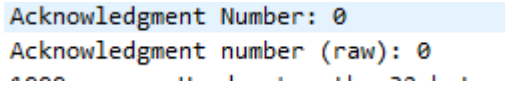
d. **redni broj segmenata (SEQ) i komentirajte! Čemu služi oznaka Win?**



Redni broj segmenata (SEQ) je polje u TCP zaglavlju koje označava broj sekvence podataka u trenutnom TCP segmentu. SEQ broj se koristi za numeriranje podataka kako bi se osiguralo da su oni ispravno raspoređeni i da se mogu rekonstruirati u ispravnom redoslijedu prilikom primitka na odredištu. Svakom segmentu podataka dodjeljuje se jedinstveni redni broj sekvence kako bi se omogućila rekonstrukcija podataka i održavanje redoslijeda.

Oznaka Win, ili Window, je polje u TCP zaglavlju koje definira veličinu pošiljateljevog prozora (odnosno prostor međuspremnika dostupan za dolazne podatke)

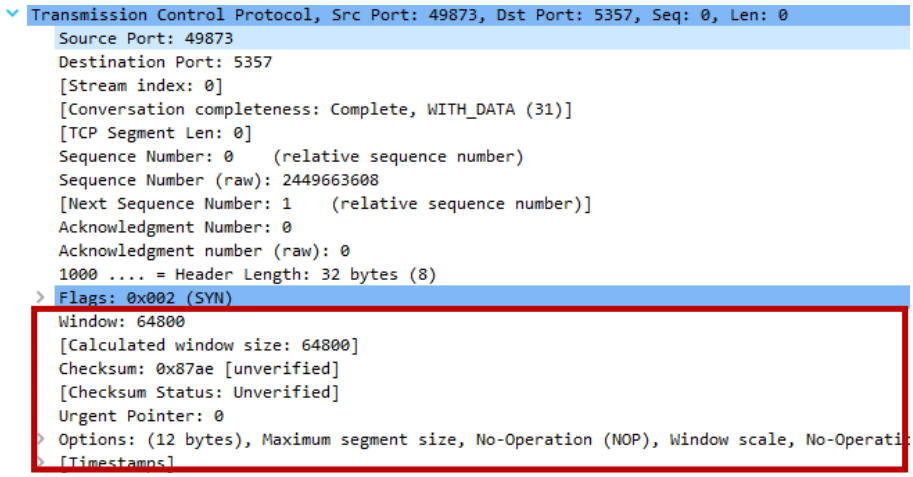
g. **Pronađite brojeve koji označavaju potvrdu primljenog segmenta (ACK) i komentirajte.**



ACK=0, **Broj potvrde** sadržava vrijednost sljedećeg sekvencijskog broja koji pošiljatelj segmenta očekuje da će primiti ako je postavljen kontrolni bit ACK. Broj sekvence odnosi se na tok koji teče u istom smjeru kao segment, dok se broj potvrde odnosi na tok koji teče u suprotnom smjeru od segmenta.

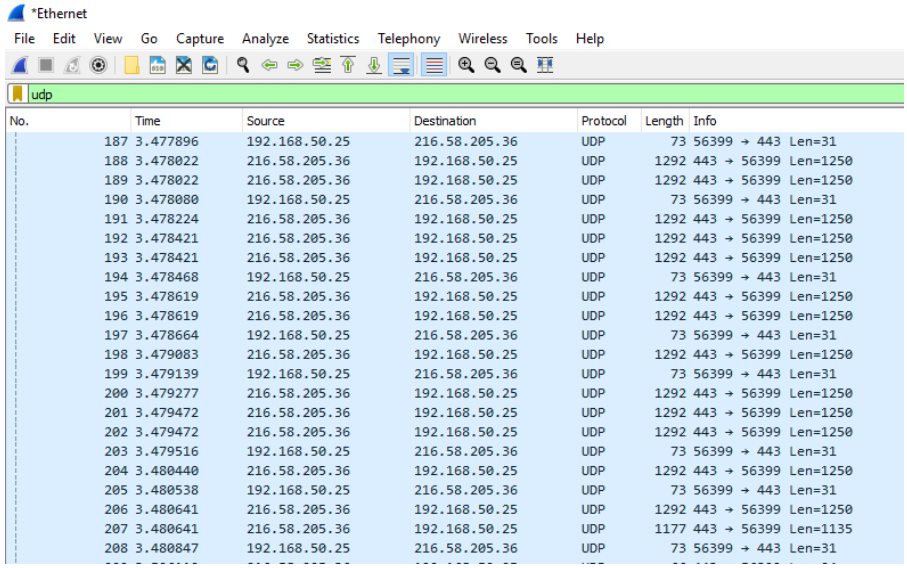
h. **Koja su ostala polja TCP zaglavlja? Istražite i zapišite čemu služe!**

Window size: Označava broj bajtova koje primatelj može primiti u jednom trenutku. To je važno za kontrolu protoka i izbjegavanje preopterećenja mreže.
Checksum(unvertified): Polje koje se koristi za provjeru integriteta podataka koji se prenose. Izračunava se uz pomoć matematičkog algoritma koji uzima u obzir sadržaj segmenta.
Urgent pointer: Koristi se za označavanje važnih podataka unutar segmenta. Označavanje se koristi za označavanje hitnih podataka koji zahtijevaju brzu obradu.
Options: Ova polja su opcionalna i koriste se za prilagođavanje TCP performansi i mogućnostima. Primjerice, mogu se koristiti za aktiviranje opcija poput selektivne potvrde, koja omogućuje primatelju da potvrdi samo određene dijelove podataka koje je primio



2. **Analizirati zaglavlje odlaznih i dolaznih UDP segmenata**

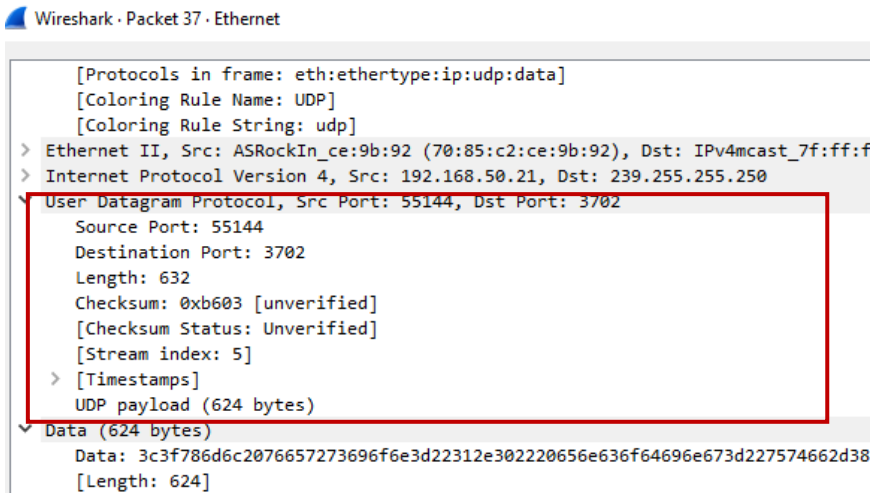
   a. **Pronaći UDP segmente**



   b. **Koje protokole enkapsulira UDP?** Enkapsulira DNS,DHCP,TFTP,SNMP,NTP

   c. **Koji je broj ishodišnog priključka (engl.port)?** 55144

   d. **Koji je broj odredišnog priključka (engl.port)?** 3702



e. **Koja su ostala polja UDP zaglavlja? Istražite i zapišite čemu služe!**

Length: Ukupna duljina datagrama, uključujući zaglavlje i podatke. Ovo polje koristi se za segmentiranje podataka u manje datagrame ako je potrebno.

Checksum: Polje koje se koristi za provjeru integriteta podataka koji se prenose. UDP koristi jednostavniji algoritam za izračun checksuma od TCP-a, ali i dalje pruža osnovnu razinu zaštite.

3. **Koja je uloga priključka u TCP i UDP segmentima?**
   Priključak (engl. Port) je polje unutar zaglavlja TCP i UDP segmenta koje se koristi za identifikaciju aplikacije koja šalje ili prima podatke preko mreže. Svaki TCP i UDP segment sadrži polje za izvor i odredišni priključak. U TCP protokolu, priključak služi kao identifikator aplikacije koja šalje ili prima podatke preko mreže. TCP koristi tzv. "well-known" priključke za poznate usluge poput HTTP (80), FTP (21), SSH (22), itd., ali aplikacije mogu koristiti i proizvoljne priključke izvan ovog raspona za svoju komunikaciju. Kada klijent šalje zahtjev prema poslužitelju, on će specificirati odredišni priključak na poslužitelju koji služi za identifikaciju aplikacije koja se koristi na tom priključku. Slično kao i u TCP-u, priključak u UDP-u služi za identifikaciju aplikacije koja šalje ili prima podatke preko mreže. UDP nema dobro definiran skup "well-known" priključaka, pa se aplikacije obično oslanjaju na registraciju svojih priključaka i usklađivanje s drugim aplikacijama kako bi se izbjegli konflikti u korištenju istih priključaka. U oba protokola, korištenje priključaka omogućava višestruku komunikaciju između različitih aplikacija na istom računalu, pruža mogućnost uspostave višestrukih veza prema različitim poslužiteljima ili klijentima te olakšava rutiranje podataka preko mreže

4. **Za poznate protokole koje ste „ulovili“ navedite predefinirane brojeve priključaka**
   HTTP: TCP port 80
   HTTPS: TCP port 443
   FTP: TCP port 21
   SSH: TCP port 22
   Telnet: TCP port 23
   SMTP: TCP port 25
   DNS: UDP port 53
   DHCP: UDP ports 67 and 68
   SNMP: UDP ports 161 and 162
   NTP: UDP port 123
   TFTP: UDP port 69
   RTP: UDP ports 5004-5005
   SIP: UDP port 5060 (or TCP port 5060)
   RTSP: TCP port 554