Primjena ICMP protokola

Hardi, Mario

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija

Sveučilišni preddiplomski studij

PRIMJENA ICMP PROTOKOLA

Završni rad

Mario Hardi

Osijek, 2022.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 20.09.2022.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime Pristupnika:	Mario Hardi
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R4348, 22.07.2019.
OIB Pristupnika:	60176870143
Mentor:	Doc. dr. sc. Višnja Križanović
Sumentor:	,
Sumentor iz tvrtke:	
Naslov završnog rada:	Primjena ICMP protokola
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rad:	U radu je potrebno opisati način rada ICMP protokola. U praktičnim primjerima unutar uspostavljene računalne mreže potrebno je demonstrirati i analizirati primjenu osnovnih alata navedenog protokola.
Prijedlog ocjene završnog rada:	Dobar (3)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 1 razina
Datum prijedloga ocjene od strane mentora:	20.09.2022.
Datum potvrde ocjene od strane Odbora:	21.09.2022.

Potvrda mentora o predaji konačne verzije rada:	*Mentor elektronički potpisao predaju konačne verzije.*
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 22.09.2022.

Ime i prezime studenta:	Mario Hardi
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R4348, 22.07.2019.
Turnitin podudaranje [%]:	10

Ovom izjavom izjavljujem da je rad pod nazivom**: Primjena ICMP protokola**

izrađen pod vodstvom mentora Doc. dr. sc. Višnja Križanović

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

IZJAVA

o odobrenju za pohranu i objavu ocjenskog rada

kojom ja __Mario Hardi_____, OIB: __60176870143_____, student/ica Fakulteta elektrotehnike, računarstva i informacijskih tehnologija Osijek na studiju _Preddiplomski sveučilišni studij Računarstvo_, kao autor/ica ocjenskog rada pod naslovom: _Primjena ICMP protokola**,**

dajem odobrenje da se, bez naknade, trajno pohrani moj ocjenski rad u javno dostupnom digitalnom repozitoriju ustanove Fakulteta elektrotehnike, računarstva i informacijskih tehnologija Osijek i Sveučilišta te u javnoj internetskoj bazi radova Nacionalne i sveučilišne knjižnice u Zagrebu, sukladno obvezi iz odredbe članka 83. stavka 11. *Zakona o znanstvenoj djelatnosti i visokom obrazovanju* (NN 123/03, 198/03, 105/04, 174/04, 02/07, 46/07, 45/09, 63/11, 94/13, 139/13, 101/14, 60/15).

Potvrđujem da je za pohranu dostavljena završna verzija obranjenog i dovršenog ocjenskog rada. Ovom izjavom, kao autor/ica ocjenskog rada dajem odobrenje i da se moj ocjenski rad, bez naknade, trajno javno objavi i besplatno učini dostupnim:

a) široj javnosti

b) studentima/icama i djelatnicima/ama ustanove

c) široj javnosti, ali nakon proteka 6 / 12 / 24 mjeseci (zaokružite odgovarajući broj mjeseci).

**U slučaju potrebe dodatnog ograničavanja pristupa Vašem ocjenskom radu, podnosi se obrazloženi zahtjev nadležnom tijelu Ustanove.*

__Osijek, 22.09.2022._____ _____

(mjesto i datum) (vlastoručni potpis studenta/ice)

Sadržaj

1. UVOD 1

1.1 Zadatak završnog rada 1

2. OSNOVNO O ICMP PROTOKOLU 2

2.1 Struktura ICMP paketa 2

3. PODJELA ICMP PORUKA 4

3.1 Istek vremena 4

3.2 Blokiranje izvorišta 5

3.3 Odredište nedostupno 6

3.4 Preusmjeravanje 7

3.5 Problem s parametrima 8

3.6 Vremenska oznaka/Odgovor na vremensku oznaku 9

3.7. Zahtjev za maskom mreže/odgovor na zahtjev za masku mreže 10

3.8 Eho zahtjev/Eho odgovor 10

4. PROGRAM WIRESHARK 12

4.1 Značajke 13

5. NAREDBA PING 14

5.1 Primjena naredbe ping 14

6. NAREDBA TRACEROUTE 21

6.1 Primjena naredbe traceroute 21

ZAKLJUČAK 28

LITERATURA 29

SAŽETAK 30

ABSTRACT 30

ŽIVOTOPIS 31

PRILOZI 32

1. UVOD

U ovom završnom radu je objašnjen i primijenjen *Internet Control Message Protocol*, skraćeno ICMP. Za primjenu ICMP protokola korišteni su programi *Wireshark* i *Command Prompt*. ICMP protokol koristi usmjerivače i krajnje uređaje kako bi slali informacije za kontrolu mreže. U programima su primijenjene dvije naredbe, a to su *ping* i *traceroute* naredbe. *Traceroute* je naredba koja se koristi za prikaz rute kojom prelaze podatkovni paketi dok putuju preko interneta do svog odredišta. Najvažnija uloga ICMP protokola je slanje poruka nekom odredišnom računalu da je došlo do pogreške u prijenosu. Objašnjene su različite vrste ICMP poruka i njihove strukture. Svaka poruka sadrži različitu strukturu.

1.1 Zadatak završnog rada

U teorijskom dijelu završnog rada potrebno je bilo proučiti opisati različite poruke ICMP protokola i način kako ICMP protokol radi. Uz to je bilo potrebno opisati naredbe koje se primjenjuju kod primjene ICMP. U praktičnom dijelu je prikazana primjena i analiza ICMP protokola Također, trebalo je primijeniti i analizirati slanje ICMP paketa u programu Wireshark i Command Prompt.

2. OSNOVNO O ICMP PROTOKOLU

ICMP protokol je protokol za izvještavanje o pogreškama koje usmjerivači i drugi mrežni uređaji koriste za komuniciranje informacija o pogreškama. Definiran je u RFC-792. Primarno se koristi za analizu mrežnog prometa. ICMP poruke se šalju kada dođe do pogreške prilikom slanja paketa. Jedan od scenarija je da ako jedan uređaj pošalje poruku koja je prevelika da bi je primatelj mogao obraditi, primatelj će u tom slučaju odbaciti izvornu poruku i poslati ICMP poruku natrag izvoru. Drugi slučaj je kad mrežni *gateway* pronađe kraću rutu kojom poruka može putovati. Kada se to dogodi, *gateway* šalje ICMP poruku i paket se preusmjerava na kraću rutu. ICMP se obično povezuje s *tracerout* i *ping* naredbom prema uobičajenim mrežnim dijagnostičkim alatima koji koriste ICMP poruke. *Traceroute* naredba pomaže administratorima da lociraju izvor kašnjenja mreže dok je *ping* naredba korisna za prikupljanje informacija o kašnjenju. Međutim, ICMP se također može iskoristiti u obranu od hakerskih napada. Napadači preplavljuju cilj neželjenim prometom tako da cilj ne može pružiti uslugu svojim korisnicima. Postoji više načina kako hakeri mogu koristiti ICMP za napade[1][2]. Neke od njih su *ping sweep*, *ping flood* i *smurf attack*[3]. Zbog mogućih napada koje omogućuje ICMP, mrežni administratori ponekad onemogućuju ICMP radi brže sigurnosne mjere dok TCP/IP još uvijek može raditi s blokiranim ICMP prometom.

2.1 Struktura ICMP paketa

Nakon IPv4 zaglavlja počinje ICMP zaglavlje i prikazuje se protokolnim brojem 1. Svaki ICMP paket ima svoje zaglavlje veličine 8 bajta i sekciju s podacima koje mogu biti različite veličine. Vrste ICMP-a prikazujemo na prvom bajtu. Drugi se bajt koristi za ICMP kod, a treći i četvrti se koristi za kontrolnu sumu[1][2].

Bitovi	0-7	8-15	16-23	24-31
0	Tip	Kod	Kontrolna suma	
32	Ostatak zaglavlja			

Tablica 2.1. Prikaz strukture ICMP paketa

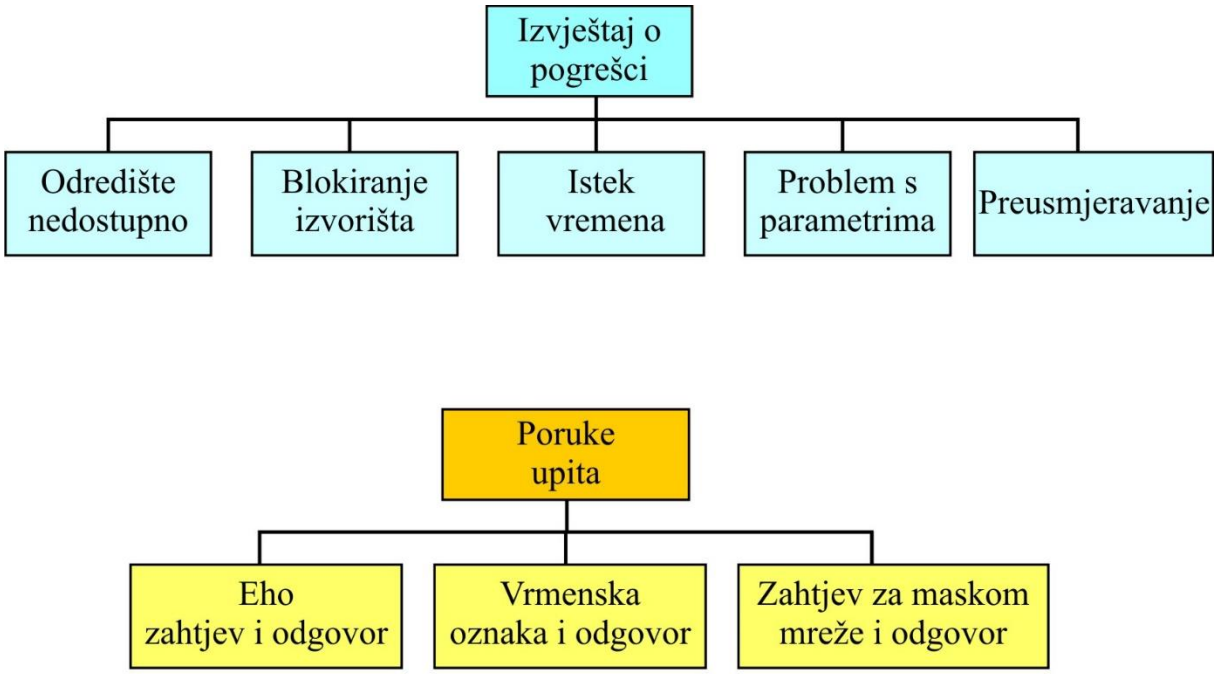
Na tablici 1. razlikujemo:

TIP-8-bitno polje koje definira tip ICMP-a. Postoje različite kontrolne poruke.

KOD-8 bitno polje definira kontrolnu poruku. Daje nam više informacija o poruci koja je odabrana.

KONTROLNA SUMA-16 bitno polje se koristi za provjeravanje poruka.

3. PODJELA ICMP PORUKA



Slika 3.1. Prikaz poruke o izvješćivanju o pogrešci i poruke upita

Na slici 3.1. vidimo dvije podjele ICMP poruka, a to su izvješćivanju o pogrešci i poruke upita. Razlika između ove dvije vrste poruka je što poruke upita, za razliku od izvješćivanja o pogrešci, očekuje odgovor na poslanu poruku kako bi saznala više informacija.

3.1 Istek vremena

ICMP poruka *Istek vremena* obavještava računalo kada je paket, koji je poslao, „ostao bez vremena“. TTL je oblikovan kako bi ograničio postojanje dijagrama s podacima. Ako se dijagramu s podacima polje TTL ("Time to live") smanji na 0, on biva odbačen, a izvorište se o tome informira putem generirane ICMP poruke istek vremena od *gateway-a*. Ista poruka se generira od strane računala kada se ne uspije iznova sastaviti fragmentirani dijagram s podacima u vremenskom intervalu u kojem se trebao sastaviti. TTL mehanizam može funkcionirati kao brojač ili kao vremenska oznaka ugrađena u dijagram s podacima[4]. Pošiljatelj dijagrama s podacima postavlja TTL polje na određeni iznos, a onda se on smanjuje

nakon svakog usmjerivača kroz koji prođe putem do odredišta. ICMP poruka se vraća pošiljatelju ako se TTL polje smanji do nule prije nego što dijagram podataka stigne do svog odredišta. Na taj način se sprječava da dijagram podataka neprestano kruži mrežom. *Istek vremena* poruke se koristi da bi se identificiralo pristupnika na putu od izvorišta do odredišta.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=11								Kod								Kontrolna suma															
Neiskorišteno																															
IP zaglavlje i prvih 8 podataka dijagrama																															

Tablica 2. Prikaz ICMP poruke *Istek vremena*

Prema tablici 3. polje Tip iznosi 11. Polje Kod navodi dva razloga isteka vremena koje možemo vidjeti u tablici 3.

Kod	Opis
0	Vrijeme života prekoračeno u prijenosu
1	Vrijeme ponovnog slaganja fragmenta

Tablica 3. Razlozi isteka vremena.

3.2 Blokiranje izvorišta

Pošiljatelj šalje podatke primatelju i on ih obradi. No ponekad se može dogoditi da pošiljatelj pošalje podatke velikom brzinom i onda naš primatelj ne može sve podatke obraditi. U tom slučaju paketi će se akumulirati na jednom mjestu i stvorit će zagušenje u mreži. Usmjerivač će obavijestit pošiljatelja slanjem ICMP paketa govoreći da postoji zagušenje u našoj mreži jer šaljemo pakete prevelikom brzinom. Ako usmjerivač želi odbaciti paket, on će uzet izvornu IP adresu iz IPv4 zaglavlja i obavijestiti izvor slanjem poruke o gašenju izvora. Izvor će smanjiti brzinu prijenosa tako da će usmjerivač osloboditi zagušenje. Ponekad se može dogoditi da je usmjerivač, na kojem je zagušenje, jako udaljen od izvora[4]. ICMP će tada poslati poruku jednom po jednom usmjerivaču tako da će svi usmjerivači smanjiti brzinu.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=4								Kod=0								Kontrolna suma															
Neiskorišteno																															
IP zaglavlje i prvih 8 podataka dijagrama																															

Tablica 4. Prikaz ICMP poruke *Blokiranje izvorišta*

U tablici 4. polja Tip i Kod će uvijek imati istu vrijednost, a to je 4 kod polja Tip i 0 kod polja Kod. Kako bi se znalo na kojem točno paketu imamo grešku, izvorištu se vraća 8 bajta poruke i zaglavlje.

3.3 Odredište nedostupno

ICMP poruka *Odredište nedstupno* generira krajnji uređaj kako bi informirao izvorište da je odredište nedostupno iz nekoliko razloga. Razlozi mogu biti: udaljenost je beskonačna što znači da fizička veza ne postoji ili port nije aktivan.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=3								Kod								Kontrolna suma															
Neiskorišteno																Sljedeći skok MTU														
IP zaglavlje i prvih 8 podataka dijagrama																															

Tablica 5. Prikaz ICMP poruke *Odredište nedostupno*

U tablici 65 polje Tip uvijek ima istu vrijednost, a to je vrijednost 3. Polje Kod se koristi za određivanje vrste pogreške.

Imamo 15 različitih kodova pogrešaka u poruci *Odredište nedostupno* (engl.Destination unreachable), kao što se vidi u tablici 6.

Kod	Opis
0	Pogreška nedostupnosti mreže
1	Pogreška nedostupnosti krajnjeg uređaja
2	Pogreška nedostupnosti protokola (određeni transportni protokol nije podržan
3	Pogreška nedostupnosti krajnjeg uređaja (određeni protokol ne može obavijestit krajnji uređaj o dolaznoj poruci
4	Dijagram podataka je prevelik potrebna je fragmentacija paketa, ali je uključena zastavica nemoj fragmentirat
5	Greška izvorne rute
6	Greška odredišne mreže
7	Nepoznata greška odredišnog računala
8	Izolirana pogreška izvornog računala
9	Odredišna mreža je zabranjena od administracije
10	Odredišno računalo je zabranjeno od administracije
11	Mreža je nedostupna za vrstu usluge
12	Računalo je nedostupan za vrstu usluge
13	Komunikacija je zabranjena od administracije
14	Kršenje prednosti poslužitelja
15	Prekid prednosti u djelovanju

Tablica 6. Prikaz 15 različitih kodova pogrešaka u poruci *Odredište nedostupno*

3.4 Preusmjeravanje

ICMP poruka *Preusmjeravanje* (engl. *Redirect*) je poruka koja informira računalo o boljoj ruti kroz mrežu. Ukoliko imamo dva *gateway-a* koji si međusobno šalju podatke, a postoji bliži *gateway,* tada će *gateway* koji prima podatke poslati ICMP poruku preusmjeravanja gateway-a koji šalje podatke. *Gateway* koji je u ovom primjeru slao podatke, sljedeći puta će poslati podatke na bliži *gateway* i tako skratiti rutu putovanja podataka[4][10].

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=5								Kod								Kontrolna suma															
IP adresa																															
IP zaglavlje i prvih 8 podataka dijagrama																															

Tablica 7. Prikaz ICMP poruke *Preusmjeravanje*

U tablici 7. polje Tip uvijek mora imati vrijednost 5, a polje Kod može imati vrijednost od 0 do 3.

Kod	Opis
0	Preusmjeravanje za mrežu
1	Preusmjeravanje za krajnji uređaj
2	Preusmjeravanje za mrežu i vrstu usluge
3	Preusmjeravanje za vrstu usluge i krajnji uređaj

Tablica 8. Prikaz 4 različite vrste preusmjeravanja

3.5 Problem s parametrima

Poruka *Problem s parametrima* može kreirati usmjerivač ili odredišno računalo. Poruka problem s parametrom pokazuje da postoji problem s IP dijagramom podataka i da se on odbija. Također može pokazati da usmjerivač i računalo ne mogu interpretirati parametar koji nije valjan u zaglavlju IPv4 dijagrama podataka. Kada računalo ili usmjerivač pronađu parametar koji nije valjan, odbacit će paket i poslat ICMP poruku problem s parametrima nazad izvoru.[10]

Tip 12	Kod: 0 ili 1	Kontrolna suma
Pokazivač	Neiskorišteno	
Dio primljenog IP dijagrama podataka uključujući IP zaglavlje plus prvih 8 bajtova dijagrama podataka		

Tablica 9. Prikaz ICMP poruke *Problem s parametrima*

U tablici 9. vidimo da je polje Tip na 12 i da polje Kod može biti 1 ili 0.

3.6 Vremenska oznaka/Odgovor na vremensku oznaku

Vremenska oznaka i *Odgovor na vremensku oznaku* su poruke upita koje sikroniziraju sustav za vrijeme i datum. ICMP poruka vremenska oznaka se danas ne koristi jer postoji standarni protokol koji se koristi za vremensku sinkronizaciju a to je *Network Time Protocol* (NTP). Ako je potrebno da usmjerivač sinkronizira svoje sistemsko vrijeme, on će poslati poruku drugom usmjerivaču kao ICMP zahtjev za vremensku oznaku. Kada drugi usmjerivač primi poruku ICMP *Vremenska oznaka*, on odgovara ICMP porukom *Odgovor na vremensku oznaku*[4]. Takva poruka s vremenskom oznakom sadrži datum i vrijeme usmjerivača.

00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Tip=13	Kod=0	Kontrolna suma
Identifikator		Redni broj
Izvorna vremenska oznaka		
Primljena vremenska oznaka		
Prijenosna vremenska oznaka		

Tablica 10. Prikaz ICMP poruke *Vremenska oznaka*

00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Tip=14	Kod=0	Kontrolna suma
Identifikator		Redni broj
Izvorna vremenska oznaka		
Primljena vremenska oznaka		
Prijenosna vremenska oznaka		

Tablica 11. Prikaz ICMP poruke *Odgovor na vremensku oznaku*

3.7. Zahtjev za maskom mreže/odgovor na zahtjev za masku mreže

Da bi se dobila maska podmreže, računalo šalje usmjerivaču zahtjev za masku adrese. Na ovu poruku primatelji odgovaraju porukom odgovora maske adrese. Ova poruka se koristi za odgovor na poruku zahtjeva za maskom adrese s odgovarajućom maskom podmreže. Zahtjev za masku adrese i poruke odgovora rade u paru. Ipak, danas rijetko koristimo ovu poruku, ali njezin dizajn podržava funkciju dinamičkog dobivanja maske podmreže. Tijekom pokretanja s udaljenog krajnjeg uređaja, oni mogu koristiti ICMP zahtjev za maskom adrese za preuzimanje maski podmreže[4][10]. Korištenje ICMP za primanje maske može uzrokovati probleme ako krajnji uređaj daje netočnu masku iz vanjskog izvora. Ukoliko vanjski izvor ne da odgovor, izvorni krajnji uređaj mora preuzeti masku klase.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=17								Kod=0								Kontrolna suma															
Identifikator																Redni broj															
Maska adrese																															

Tablica 12. Prikaz ICMP poruke *Zahtjev za maskom mreže*

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=18								Kod=0								Kontrolna suma															
Identifikator																Redni broj															
Maska adrese																															

Tablica 13.. Prikaz ICMP poruke *Odgovor na zahtjev za masku mreže*

3.8 Eho zahtjev/Eho odgovor

ICMP koristi ove poruke u paru pa govorimo o ICMP tipu *Eho zahtjeva* 8 i tipu *Eho odgovora* 0. Ove dvije vrste poruka koriste udaljeni domaćini za testiranje povezanosti. Korisnik izvršava uslužni program *ping* tako da pokreće generiranje ICMP eho zahtjeva kako bi odredišni krajnji uređaj poslao odgovarajući eho sadržaj[4].

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=8(IPv4,ICMP) 128(IPv6,ICMP6)								Kod=0								Kontrolna suma															
Identifikator																Redni broj															
Podatak																															

Tablica 14. Prikaz ICMP poruke *Eho zahtjev*

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tip=0(IPv4,ICMP) 129(IPv6,ICMP6)								Kod=0								Kontrolna suma															
Identifikator																Redni broj															
Podatak																															

Tablica 15. Prikaz ICMP poruke *Eho odgovor*

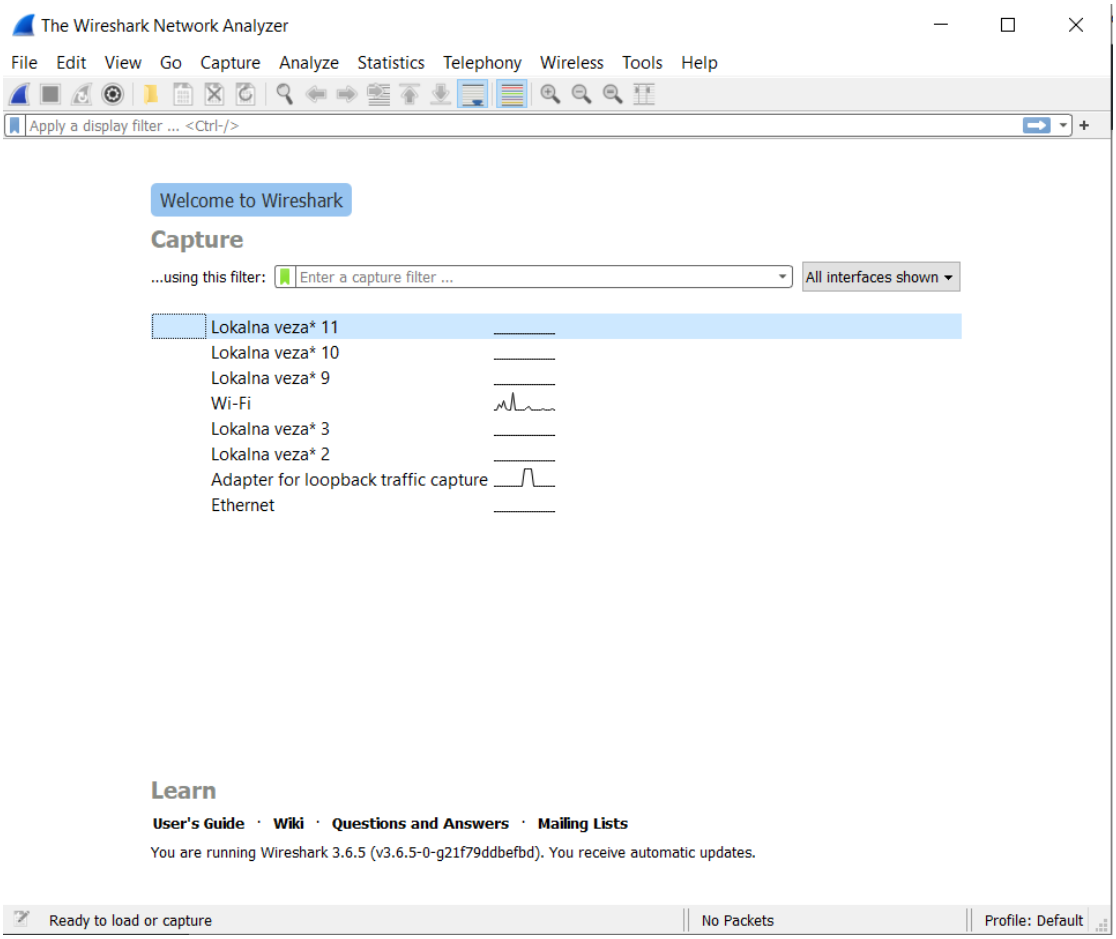
U tablicama 14. i 15. možemo vidjeti da polje Kod imaju vrijednost 0 dok im se polje Tip razlikuje. *Eho zahtjev* ima vrijednost 8 na polju Tip dok *Eho odgovor* ima vrijednost 0 na polju Tip. Polje podataka nam govori kada se dogodio prijenos.

4. PROGRAM WIRESHARK

Wireshark je program otvorenog koda koji prati podatkovne pakete prilikom prijenosa preko mreže. U samom početku projekta prvo je nazvan *Ethereal*, ali 2006. godine mu je ime promijenjeno u Wireshark. Wireshark program radi na *Linuxu, MacOS*-u, BSD-u, *Solarisu* itd. Postoji i druga verzija koja je bazirana na terminalu (ne-GUI) koja se zove TShark. Koristi se za analizu mrežnih paketa, ali primarno se koristi za rješavanje problema s mrežom. Također se može koristit kao zaštita od hakiranja[5][6].

Razlozi zašto koristiti Wireshark program:

- koristimo ga kada imamo problema s mrežom
- zbog sigurnosnih razloga
- za provjeru mrežnih aplikacija
- lakše rukovanje unutarnjim dijelovima mrežnog protokola

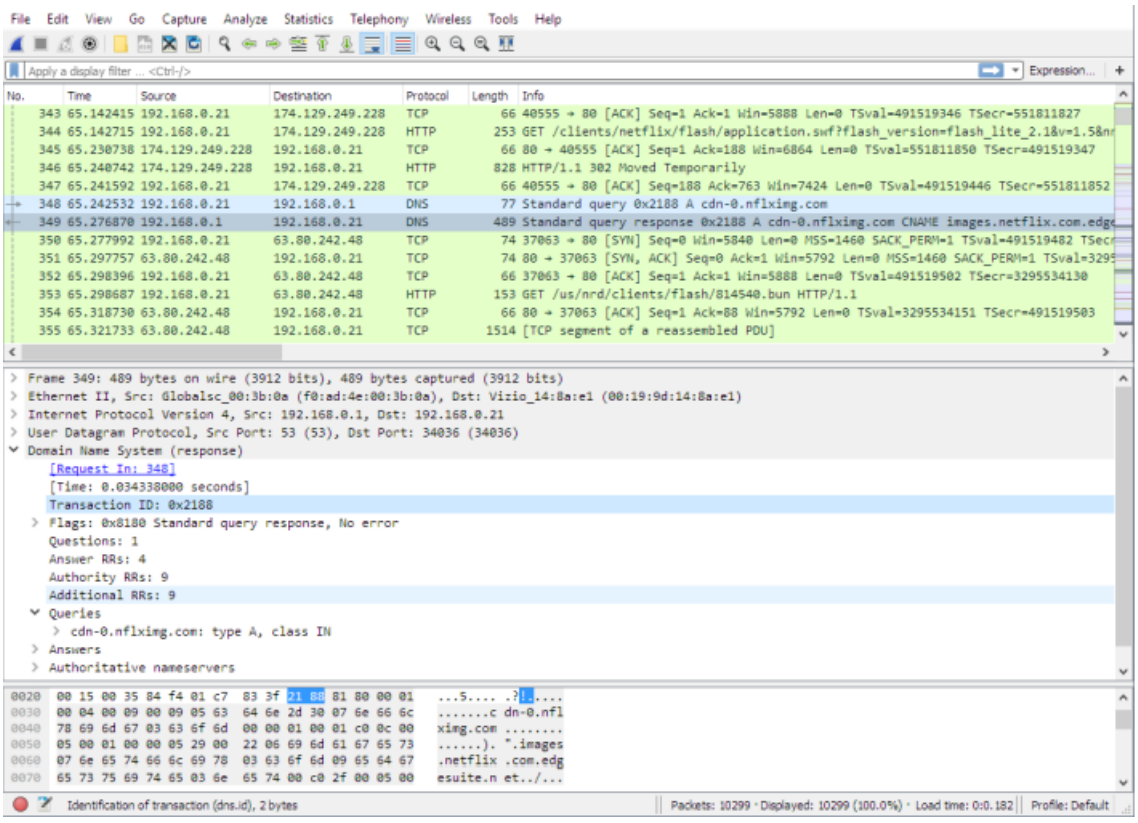


Slika 2. Prikaz početnog zaslona Wireshark-a.

4.1 Značajke

Različite su značajke koje nam pruža Wireshark program, a neke od njih su:

- može se koristit na *Windowsu* i na UNIX-u
- detaljno prikazuje informacije o protokolu
- sprema sve pakete koje je uhvatio
- pravi različite statistike
- možemo tražiti pakete po različitim kriterijima



Slika 3. Prikaz detalja jednog paketa.

5. NAREDBA PING

Naredba *ping* je alat koji se koristi za rješavanje problema s mrežom kao što je mrežna povezanost. Može se još koristit za testiranje jesmo li povezani s lokalnom mrežom ili jesmo li povezani s internetom. Kada se provjera IP adresa računala uz primjenu *ping* naredbe, taj uređaj bi mogao biti bilo koji mrežni uređaj kao što je računalo, poslužitelj ili usmjerivač. Ukoliko se prilikom provjere konekcije uz primjenu *ping* naredbe dobije odgovor, to znači da između nas i poslužitelja postoji mrežna povezanost. *Ping* naredba šalje ICMP poruku *Eho zahtjev* nekom računalu i čeka ICMP poruku *Eho odgovor*[7].

5.1 Primjena naredbe ping

U prvom primjeru se primijenjuje naredba *ping* na stranicu *youtube*. U programu Wireshark u gornjem lijevom kutu pritisnemo mišem naredbu „Start capturing packets“. Nakon toga se u programu Command Prompt primijeni naredba ping *www.youtube.com*. Kada se u Command Promptu dobije odgovor o *ping* naredbi, zaustavi se „Capture mode“ u programu Wireshark i dobije se analiza prometa[8].

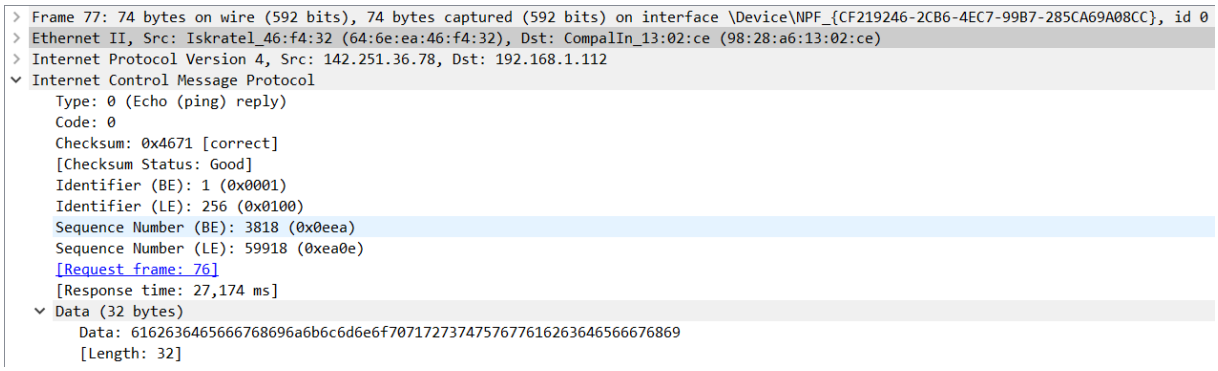
```
C:\Program Files\Microsoft Visual Studio\2022\Community>ping www.youtube.com

Pinging youtube-ui.l.google.com [142.251.36.78] with 32 bytes of data:
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116

Ping statistics for 142.251.36.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 25ms, Average = 25ms
```

Slika 4. Prikaz primjene naredbe *ping* na stranicu *youtube-a*

No.	Time	Source	Destination	Protocol	Length	Info
191	15.862437	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=3821/60686, ttl=116 (request in 190)
185	14.842694	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=3820/60430, ttl=116 (request in 184)
182	13.824777	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=3819/60174, ttl=116 (request in 181)
77	12.805960	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=3818/59918, ttl=116 (request in 76)
190	15.836970	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=3821/60686, ttl=128 (reply in 191)
184	14.817220	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=3820/60430, ttl=128 (reply in 185)
181	13.795456	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=3819/60174, ttl=128 (reply in 182)
76	12.778786	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=3818/59918, ttl=128 (reply in 77)

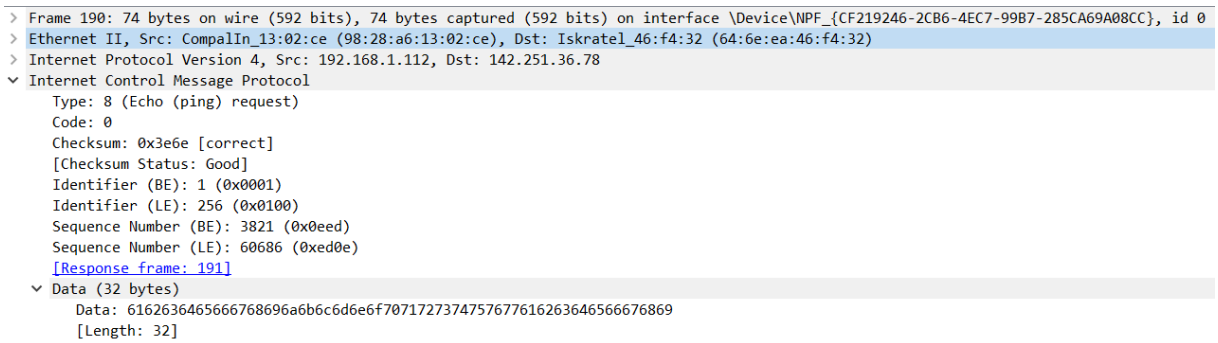
Slika 5. Prikaz paketa dobivenih primjenom naredbe *ping* na stranicu *youtube-a*

Na slici 5. se vide filtrirani paketi koji koriste ICMP protokol. Prvi stupac (NO.) pokazuje koji je to paket koji je snimljen od početka snimanja. Drugi stupac (engl.*Time*) prikazuje vrijeme u kojoj sekundi je paket snimljen od početka snimanja. Stupac (engl.*Source*) prikazuje izvorišnu adresu paketa. Stupac (engl.*Destination*) prikazuje odredišnu adresu paketa. Stupac protokol prikazuje i koji protokol koristimo, a u ovome slučaju to je ICMP. Stupac (engl.*Length*) predstavlja veličinu paketa. Stupac (engl.*Info)* sadrži najosnovnije informacije o paketu koji smo dobili kao što su ime ICMP poruke, identifikator, redni broj te TTL. Prvi paket u danom primjeru je *Eho odgovor* koji je 191. uhvaćeni paket. Njegova veličina iznosi 74 bajta i koristi protokol ICMP.



Slika 6. Prikaz detalja Eho odgovor paketa

Slika 6. prikazuje detaljniji prikaz *Eho odgovor* paketa. Kod *Eho odgovor* poruke polja Tip i Kod su na 0 što i je u navedenom slučaju. Kontrolna suma(engl. *Checksum*) je točna. Redni broj(*engl.Sequence Number*) je 3821. od 60686, a polje Identifikator(engl.*Identifier*) je 1. od 256. Vrijeme reagiranja(engl.*Response time*) ili RTT iznosi 27.174 ms.



Slika 7. Prikaz detalja *Eho zahtjev* paketa

Na slici 7. se vidi detaljni prikaz *Eho zahtjev* paketa. Polje *Type* se razlikuje od eho odgovora polja *Type* i ono je sada na 8 dok je polje *Code* ostalo na 0. Kontrolna suma(engl. *Checksum*) je točna. Identifikator(engl.*Identifier)* i redni broj(*engl.Sequence Number*) su ostali isti.

U sljedećem primjeru se primjenjuje naredba *ping* na vlastitom računalu. U programu Command Prompt se upiše IP adresa našeg računala.

```
C:\Program Files\Microsoft Visual Studio\2022\Community>ping 95.178.175.197

Pinging 95.178.175.197 with 32 bytes of data:
Reply from 95.178.175.197: bytes=32 time=1ms TTL=64
Reply from 95.178.175.197: bytes=32 time<1ms TTL=64
Reply from 95.178.175.197: bytes=32 time<1ms TTL=64
Reply from 95.178.175.197: bytes=32 time<1ms TTL=64

Ping statistics for 95.178.175.197:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8. Prikaz primjene naredbe *ping* na vlastito računalo

Na slici 8. se može vidjeti da je TTL=64 što je gotovo duplo manje nego kad se primijeni naredba *ping* na stranicu *youtube-a*. Sva 4 paketa, koja su poslana, su se isporučila. Može se uočiti da prosječan RTT iznosi 0 ms.

No.	Time	Source	Destination	Protocol	Length	Info
78	8.792390	192.168.1.112	95.178.175.197	ICMP	74	Echo (ping) request id=0x0001, seq=2889/18699, ttl=128 (reply in 79)
79	8.793046	95.178.175.197	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=2889/18699, ttl=64 (request in 78)
84	9.805532	192.168.1.112	95.178.175.197	ICMP	74	Echo (ping) request id=0x0001, seq=2890/18955, ttl=128 (reply in 85)
85	9.806036	95.178.175.197	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=2890/18955, ttl=64 (request in 84)
108	10.812895	192.168.1.112	95.178.175.197	ICMP	74	Echo (ping) request id=0x0001, seq=2891/19211, ttl=128 (reply in 109)
109	10.813649	95.178.175.197	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=2891/19211, ttl=64 (request in 108)
114	11.818493	192.168.1.112	95.178.175.197	ICMP	74	Echo (ping) request id=0x0001, seq=2892/19467, ttl=128 (reply in 115)
115	11.819019	95.178.175.197	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=2892/19467, ttl=64 (request in 114)

Slika 9. Prikaz analize primjene naredbe *ping* na vlastitom računalo.

Sljedeći primjer pokazuje što se dogodi kada se provjerava konekcija uz primjenu naredbe *ping* na odredište koje ne postoji.

```
C:\Program Files\Microsoft Visual Studio\2022\Community>ping 92.98.123.25

Pinging 92.98.123.25 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 92.98.123.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Slika 10. Prikaz provjere konekcije uz primjenu naredbe *ping -Odredište nedostupno*

Na slici 10. se vidi da su sva 4 paketa izgubljena. U ovome slučaju je poslana *Eho zahtjev* poruka no nije dobivena nikakva *Eho odgovor* poruka nazad. Zato je ispisana poruka „*Request timed out*“

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4078 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 3299 (0x0ce3)
    Sequence Number (LE): 58124 (0xe30c)
  > [No response seen]
  > Data (32 bytes)
```

Slika 11. Prikaz detalja paketa odredište nedostupno

U detaljima paketa se vidi da nema odgovora.

145	18.553514	192.168.1.112	92.98.123.25	ICMP	74 Echo (ping) request id=0x0001, seq=3299/58124, ttl=128 (no response found!)
152	23.422457	192.168.1.112	92.98.123.25	ICMP	74 Echo (ping) request id=0x0001, seq=3300/58380, ttl=128 (no response found!)
207	28.420256	192.168.1.112	92.98.123.25	ICMP	74 Echo (ping) request id=0x0001, seq=3301/58636, ttl=128 (no response found!)
220	33.418635	192.168.1.112	92.98.123.25	ICMP	74 Echo (ping) request id=0x0001, seq=3302/58892, ttl=128 (no response found!)

Slika 12. Prikaz filtriranih paketa primjenom naredbe *ping* neodređenog odredišta

U sljedećem primjeru koristimo naredbu *ping* na stranici Stanford fakulteta u Sjedinjenim Američkim Državama.

```
C:\Program Files\Microsoft Visual Studio\2022\Community>ping stanford.edu

Pinging stanford.edu [171.67.215.200] with 32 bytes of data:
Reply from 171.67.215.200: bytes=32 time=168ms TTL=241
Reply from 171.67.215.200: bytes=32 time=168ms TTL=241
Reply from 171.67.215.200: bytes=32 time=169ms TTL=241
Reply from 171.67.215.200: bytes=32 time=168ms TTL=241

Ping statistics for 171.67.215.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 168ms, Maximum = 169ms, Average = 168ms
```

Slika 13. Prikaz primjene naredbe *ping* na stranicu Stanford fakulteta

Na slici 13. se uočava da TTL iznosi 241 ms. TTL je puno veći nego u dosadašnjim primjerima. Također RTT je puno veći zato što se primijenila naredba *ping* na stranicu koja je izvan Hrvatske.

52471	106.807464	192.168.1.112	171.67.215.200	ICMP	74	Echo (ping) request id=0x0001, seq=4141/11536, ttl=128 (reply in 52473)
52473	106.976237	171.67.215.200	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4141/11536, ttl=241 (request in 52471)
52474	107.812944	192.168.1.112	171.67.215.200	ICMP	74	Echo (ping) request id=0x0001, seq=4142/11792, ttl=128 (reply in 52475)
52475	107.981108	171.67.215.200	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4142/11792, ttl=241 (request in 52474)
52484	108.824220	192.168.1.112	171.67.215.200	ICMP	74	Echo (ping) request id=0x0001, seq=4143/12048, ttl=128 (reply in 52486)
52486	108.993209	171.67.215.200	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4143/12048, ttl=241 (request in 52484)
52487	109.829337	192.168.1.112	171.67.215.200	ICMP	74	Echo (ping) request id=0x0001, seq=4144/12304, ttl=128 (reply in 52488)
52488	109.998007	171.67.215.200	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4144/12304, ttl=241 (request in 52487)

Slika 14. Prikaz filtriranih paketa

```
> Frame 1322: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CF219246-2CB6-4EC7-99B7-285CA69A08CC}, id 0
> Ethernet II, Src: CompalIn_13:02:ce (98:28:a6:13:02:ce), Dst: Iskratel_46:f4:32 (64:6e:ea:46:f4:32)
> Internet Protocol Version 4, Src: 192.168.1.112, Dst: 161.53.72.120
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x3d32 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 4137 (0x1029)
    Sequence Number (LE): 10512 (0x2910)
  > [No response seen]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
      [Length: 32]
```

Slika 15. Prikaz detalja paketa „pinganja“ stranice Stanford fakulteta

Command Prompt program omogućuje da se doda nastavak –t na *ping* naredbu. Ova opcija omogućuje slanje poruka neograničeno. Omogućuje također da se u određenom vremenskom razdoblju vidi jesu li paketi ispušteni na IP adresu. Da bi se zaustavila ova opcija, potrebno je pritisnuti CTRL+C na tipkovnici u command prompt programu.

```
C:\Program Files\Microsoft Visual Studio\2022\Community>ping -t www.youtube.com

Pinging youtube-ui.l.google.com [142.251.36.78] with 32 bytes of data:
Reply from 142.251.36.78: bytes=32 time=26ms TTL=116
Reply from 142.251.36.78: bytes=32 time=26ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116
Reply from 142.251.36.78: bytes=32 time=26ms TTL=116
Reply from 142.251.36.78: bytes=32 time=26ms TTL=116
Reply from 142.251.36.78: bytes=32 time=26ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116
Reply from 142.251.36.78: bytes=32 time=25ms TTL=116

Ping statistics for 142.251.36.78:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 26ms, Average = 25ms
Control-C
```

Slika 16. Prikaz slanja neograničeno poruka

No.	Time	Source	Destination	Protocol	Length	Info
30	10.535822	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4282/47632, ttl=128 (reply in 31)
31	10.562008	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4282/47632, ttl=116 (request in 30)
34	11.547619	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4283/47888, ttl=128 (reply in 35)
35	11.573738	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4283/47888, ttl=116 (request in 34)
47	12.565812	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4284/48144, ttl=128 (reply in 48)
48	12.591463	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4284/48144, ttl=116 (request in 47)
54	13.581240	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4285/48400, ttl=128 (reply in 55)
55	13.607002	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4285/48400, ttl=116 (request in 54)
59	14.596794	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4286/48656, ttl=128 (reply in 60)
60	14.623251	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4286/48656, ttl=116 (request in 59)
66	15.615512	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4287/48912, ttl=128 (reply in 67)
67	15.641589	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4287/48912, ttl=116 (request in 66)
78	16.630879	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4288/49168, ttl=128 (reply in 79)
79	16.656763	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4288/49168, ttl=116 (request in 78)
80	17.644699	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4289/49424, ttl=128 (reply in 81)
81	17.670496	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4289/49424, ttl=116 (request in 80)
83	18.660102	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4290/49680, ttl=128 (reply in 84)
84	18.685929	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4290/49680, ttl=116 (request in 83)
86	19.677676	192.168.1.112	142.251.36.78	ICMP	74	Echo (ping) request id=0x0001, seq=4291/49936, ttl=128 (reply in 87)
87	19.703439	142.251.36.78	192.168.1.112	ICMP	74	Echo (ping) reply id=0x0001, seq=4291/49936, ttl=116 (request in 86)

Slika 17. Prikaz filtriranih paketa

U sljedećem primjeru će biti analizirano primjena ping naredbe na neku bližu lokaciju,a to je Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek.

```
C:\Program Files\Microsoft Visual Studio\2022\Community>ping -t www.ferit.unios.hr

Pinging www.ferit.unios.hr [161.53.201.71] with 32 bytes of data:
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=18ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=15ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56
Reply from 161.53.201.71: bytes=32 time=16ms TTL=56

Ping statistics for 161.53.201.71:
    Packets: Sent = 13, Received = 13, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 18ms, Average = 16ms
Control-C
```

Slika 18. Primjena naredbe *ping* uz dodatne opcije na Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek.

No.	Time	Source	Destination	Protocol	Length	Info
87	2.013857	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3874/8719, ttl=128 (reply in 88)
88	2.030064	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3874/8719, ttl=56 (request in 87)
97	3.025043	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3875/8975, ttl=128 (reply in 98)
98	3.041184	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3875/8975, ttl=56 (request in 97)
100	4.038134	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3876/9231, ttl=128 (reply in 101)
101	4.056534	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3876/9231, ttl=56 (request in 100)
102	5.046496	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3877/9487, ttl=128 (reply in 103)
103	5.063100	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3877/9487, ttl=56 (request in 102)
107	6.056600	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3878/9743, ttl=128 (reply in 108)
108	6.072981	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3878/9743, ttl=56 (request in 107)
113	7.066625	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3879/9999, ttl=128 (reply in 114)
114	7.082956	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3879/9999, ttl=56 (request in 113)
116	8.075518	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3880/10255, ttl=128 (reply in 117)
117	8.091323	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3880/10255, ttl=56 (request in 116)
137	9.085715	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3881/10511, ttl=128 (reply in 138)
138	9.101622	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3881/10511, ttl=56 (request in 137)
153	10.094708	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3882/10767, ttl=128 (reply in 154)
154	10.110632	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3882/10767, ttl=56 (request in 153)
160	11.113591	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3883/11023, ttl=128 (reply in 161)
161	11.129850	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3883/11023, ttl=56 (request in 160)
173	12.121943	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3884/11279, ttl=128 (reply in 174)
174	12.138278	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3884/11279, ttl=56 (request in 173)
181	13.132574	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3885/11535, ttl=128 (reply in 182)
182	13.148999	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3885/11535, ttl=56 (request in 181)
186	14.144610	192.168.1.109	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=3886/11791, ttl=128 (reply in 187)
187	14.160802	161.53.201.71	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=3886/11791, ttl=56 (request in 186)

Slika 19. Prikaz filtriranih paketa

Na slici 18. je upotrebljena dodatna opcija –t koja nam omogućuje slanje beskonačno paketa sve dok na tipkovnici ne stisnemo CTRL+C. IP adresa od fakulteta iznosi [161.53.201.71]. *Round trip times:* Minimalno=15ms,maksimalno =8ms i prosječno=16ms.

6. NAREDBA TRACEROUTE

Traceroute je naredba koja se koristi za prikaz rute kojom prelaze podatkovni paketi dok putuju preko interneta do svog odredišta. Internet je globalna mreža usmjerivača koja omogućuje računalima i poslužiteljima mogućnost međusobne komunikacije iz cijelog svijeta. Usmjerivači međusobno komuniciraju kako bi mogli usmjeravati podatkovne podatke do željenog odredišta. Naredba *traceroute* je alat koji se koristi za otkrivanje točne putanje do koje podatkovni paket prešao od pošiljatelja do odredišta. *Traceroute* može pomoći u pronalaženju problema kao što je "bottlenecks". *Traceroute* naredba se malo razlikuje od *ping* naredbe. Kada se primjenjuje naredba *ping* na poslužitelj kao što je *facebook.com*, naše računalo će poslati 4 podatkovna paketa na odredište, a kad stigne na odredište, vratit će ih natrag na naše računalo. *Traceroute* daje više informacija nego *ping*. *Traceroute* ne samo da „pinguje“ konačno odredište, već „pinga“ svaki usmjerivač koji se nađe na putu do odredišta. Mjeri vrijeme povratnog puta koje su paketi podataka uzeli od svakog usmjerivača i odredišta[9].

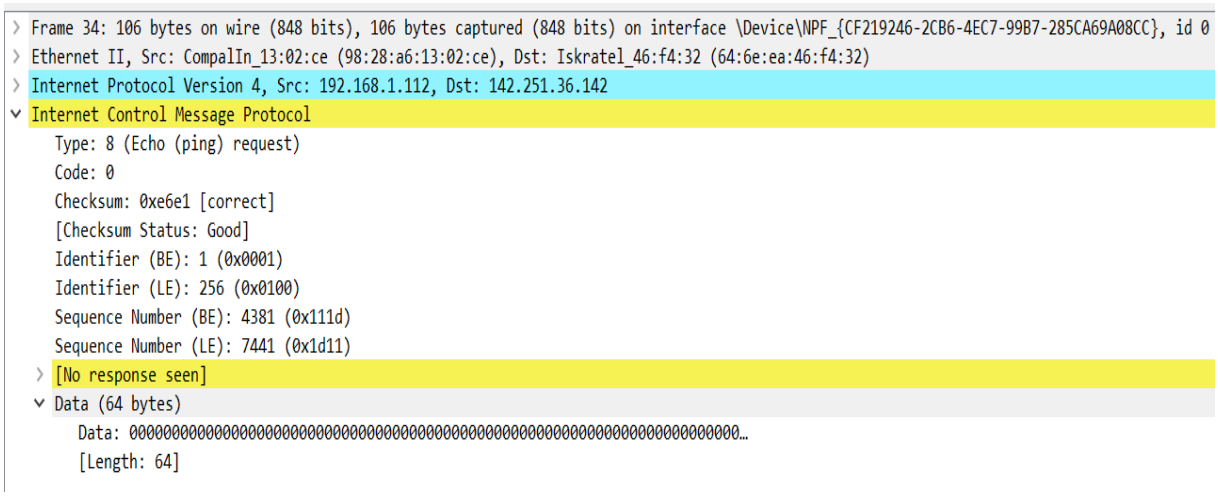
6.1 Primjena naredbe traceroute

Naredba *traceroute* se koristi u Command Promptu gotovo isto kao i naredba *ping*. U programu Command Prompt se upiše tracert i onda IP adresa odredišta. U sljedećem primjeru primjenjuje se naredba *traceroute* upisivanjem „tracert www.youtube.com“.

```
C:\Program Files\Microsoft Visual Studio\2022\Community>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.251.37.110]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  Gateway.Home [192.168.1.1]
  2    13 ms    42 ms    13 ms  85.114.32.145
  3    13 ms    13 ms    13 ms  85.114.32.146
  4    14 ms    14 ms    14 ms  e0-30.core2.zag1.he.net [216.66.93.61]
  5    20 ms     *        *     100ge0-71.core2.vie1.he.net [184.104.193.113]
  6    19 ms    19 ms    19 ms  100ge16-2.core1.vie1.he.net [184.104.197.137]
  7    20 ms    20 ms    20 ms  100ge5-1.core1.bts1.he.net [72.52.92.206]
  8    25 ms    25 ms    25 ms  nixsk1.google.com [194.30.187.211]
  9    26 ms    25 ms    26 ms  108.170.245.49
 10    25 ms    25 ms    25 ms  142.251.224.229
 11    25 ms    25 ms    25 ms  prg03s13-in-f14.1e100.net [142.251.37.110]

Trace complete.
```

Slika 20. *Traceroute* stranice *youtube-a* u Command Prompt-u

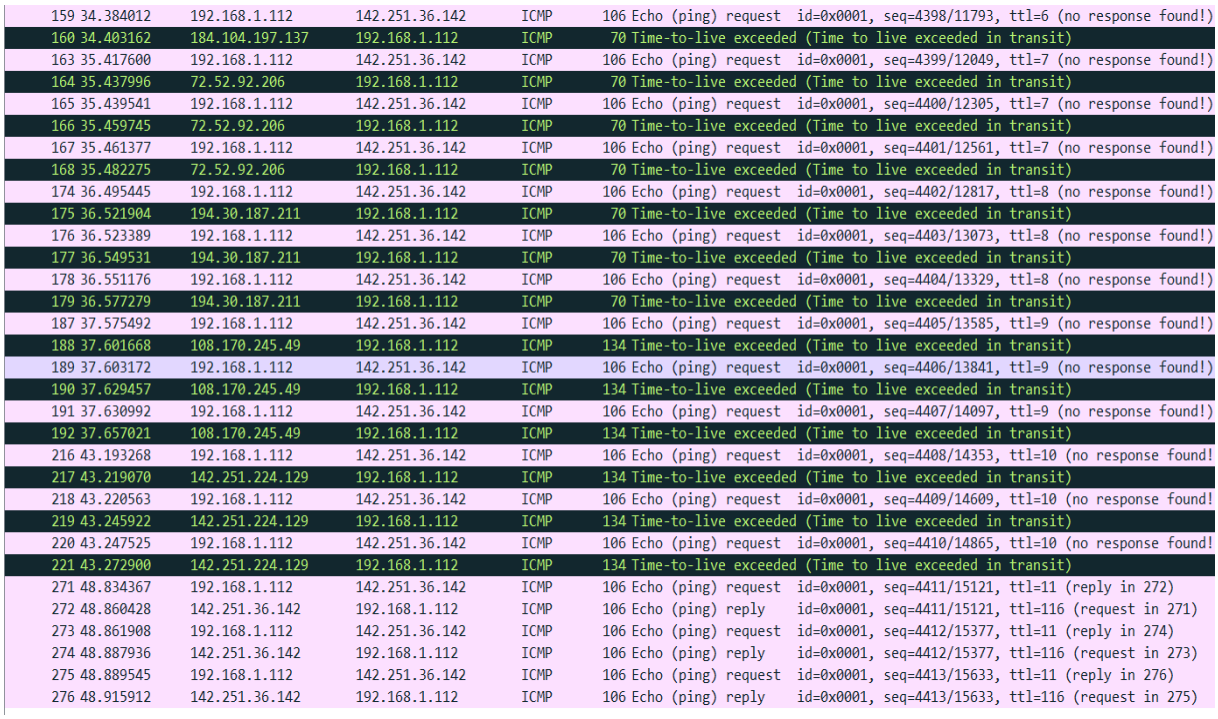
Na slici 20. se vidi da ima 11 skokova od našeg računala do odredišta. Naš usmjerivač je prvi skok. Vidimo da su nam svi usmjerivači odgovorili. Na 11. skoku se može iščitati RTT (25 ms) i IP adresa (142.251.37.110) našeg odredišta.



Slika 21. Detalji paketa traceroute

No.	Time	Source	Destination	Protocol	Length	Info
34	9.293679	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4381/7441, ttl=1 (no response found!)
35	9.294296	192.168.1.1	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
36	9.294948	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4382/7697, ttl=1 (no response found!)
37	9.295413	192.168.1.1	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
38	9.296003	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4383/7953, ttl=1 (no response found!)
39	9.296436	192.168.1.1	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
41	10.306064	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4384/8209, ttl=2 (no response found!)
42	10.320105	85.114.32.145	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
43	10.321936	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4385/8465, ttl=2 (no response found!)
44	10.335551	85.114.32.145	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
45	10.337267	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4386/8721, ttl=2 (no response found!)
46	10.401163	85.114.32.145	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
50	10.431072	85.114.32.145	192.168.1.112	ICMP	70	Destination unreachable (Port unreachable)
54	11.943005	85.114.32.145	192.168.1.112	ICMP	70	Destination unreachable (Port unreachable)
67	13.458385	85.114.32.145	192.168.1.112	ICMP	70	Destination unreachable (Port unreachable)
76	15.894308	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4387/8977, ttl=3 (no response found!)
77	15.907837	85.114.32.146	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
78	15.909580	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4388/9233, ttl=3 (no response found!)
79	15.923153	85.114.32.146	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
80	15.924899	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4389/9489, ttl=3 (no response found!)
81	15.938002	85.114.32.146	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
85	15.968200	85.114.32.146	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
98	17.461464	85.114.32.146	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
102	18.962792	85.114.32.146	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
105	21.454003	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4390/9745, ttl=4 (no response found!)
106	21.467827	216.66.93.61	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
107	21.469551	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4391/10001, ttl=4 (no response found!)
108	21.483002	216.66.93.61	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
109	21.484675	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4392/10257, ttl=4 (no response found!)
110	21.498723	216.66.93.61	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
115	22.500642	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4393/10513, ttl=5 (no response found!)
135	26.340600	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4394/10769, ttl=5 (no response found!)
142	30.342638	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4395/11025, ttl=5 (no response found!)
155	34.341921	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4396/11281, ttl=6 (no response found!)
156	34.361477	184.104.197.137	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
157	34.363158	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4397/11537, ttl=6 (no response found!)
158	34.382484	184.104.197.137	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Slika 22. *Traceroute* filtriranih paketa stranice *youtube-a*



159	34.384012	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4398/11793, ttl=6 (no response found!)
160	34.403162	184.104.197.137	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
163	35.417600	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4399/12049, ttl=7 (no response found!)
164	35.437996	72.52.92.206	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
165	35.439541	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4400/12305, ttl=7 (no response found!)
166	35.459745	72.52.92.206	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
167	35.461377	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4401/12561, ttl=7 (no response found!)
168	35.482275	72.52.92.206	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
174	36.495445	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4402/12817, ttl=8 (no response found!)
175	36.521904	194.30.187.211	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
176	36.523389	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4403/13073, ttl=8 (no response found!)
177	36.549531	194.30.187.211	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
178	36.551176	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4404/13329, ttl=8 (no response found!)
179	36.577279	194.30.187.211	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
187	37.575492	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4405/13585, ttl=9 (no response found!)
188	37.601668	108.170.245.49	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
189	37.603172	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4406/13841, ttl=9 (no response found!)
190	37.629457	108.170.245.49	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
191	37.630992	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4407/14097, ttl=9 (no response found!)
192	37.657021	108.170.245.49	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
216	43.193268	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4408/14353, ttl=10 (no response found!
217	43.219070	142.251.224.129	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
218	43.220563	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4409/14609, ttl=10 (no response found!
219	43.245922	142.251.224.129	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
220	43.247525	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4410/14865, ttl=10 (no response found!
221	43.272900	142.251.224.129	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
271	48.834367	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4411/15121, ttl=11 (reply in 272)
272	48.860428	142.251.36.142	192.168.1.112	ICMP	106	Echo (ping) reply id=0x0001, seq=4411/15121, ttl=116 (request in 271)
273	48.861908	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4412/15377, ttl=11 (reply in 274)
274	48.887936	142.251.36.142	192.168.1.112	ICMP	106	Echo (ping) reply id=0x0001, seq=4412/15377, ttl=116 (request in 273)
275	48.889545	192.168.1.112	142.251.36.142	ICMP	106	Echo (ping) request id=0x0001, seq=4413/15633, ttl=11 (reply in 276)
276	48.915912	142.251.36.142	192.168.1.112	ICMP	106	Echo (ping) reply id=0x0001, seq=4413/15633, ttl=116 (request in 275)

Slika 23. *Traceroute* filtriranih paketa stranice youtube-a

Na slikama 22. i 23 na 6 mjesta smo dobili poruku da je *Odredište nedostupno*.

```
C:\Program Files\Microsoft Visual Studio\2022\Community>tracert stanford.edu

Tracing route to stanford.edu [171.67.215.200]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  Gateway.Home [192.168.1.1]
  2    13 ms    13 ms    13 ms  85.114.32.145
  3    13 ms    13 ms    13 ms  85.114.32.146
  4    13 ms    12 ms    13 ms  85.114.32.102
  5    13 ms    13 ms    13 ms  e0-30.core2.zag1.he.net [216.66.93.61]
  6     *        *       19 ms  100ge0-71.core2.vie1.he.net [184.104.193.113]
  7    19 ms    19 ms    20 ms  100ge16-2.core1.vie1.he.net [184.104.197.137]
  8    43 ms    39 ms     *     100ge0-63.core2.par2.he.net [184.105.65.5]
  9   105 ms   104 ms   104 ms  100ge11-2.core1.nyc4.he.net [72.52.92.113]
 10   167 ms   166 ms   167 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
 11   167 ms   166 ms   168 ms  100ge1-1.core1.pao1.he.net [72.52.92.158]
 12   168 ms   168 ms   167 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 13   170 ms   169 ms   171 ms  woa-west-rtr-vl2.SUNet [171.64.255.132]
 14     *        *        *     Request timed out.
 15   168 ms   168 ms   168 ms  web.stanford.edu [171.67.215.200]

Trace complete.
```

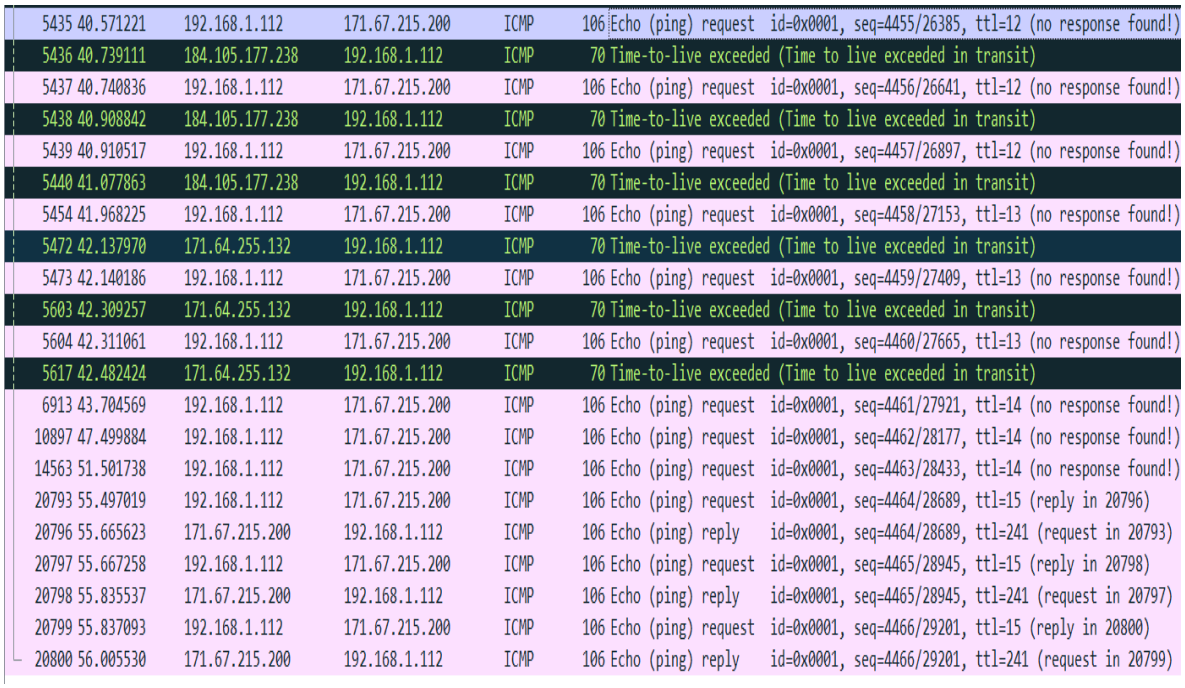
Slika 24. Traceroute početne stranice Stanford fakulteta

No.	Time	Source	Destination	Protocol	Length	Info
27	4.035525	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4422/17937, ttl=1 (no response found!)
28	4.036156	192.168.1.1	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
29	4.037131	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4423/18193, ttl=1 (no response found!)
30	4.037570	192.168.1.1	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
31	4.038058	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4424/18449, ttl=1 (no response found!)
32	4.038429	192.168.1.1	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
34	5.043534	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4425/18705, ttl=2 (no response found!)
35	5.057178	85.114.32.145	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
36	5.058828	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4426/18961, ttl=2 (no response found!)
37	5.072251	85.114.32.145	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
38	5.073766	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4427/19217, ttl=2 (no response found!)
39	5.086917	85.114.32.145	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
43	5.118278	85.114.32.145	192.168.1.112	ICMP	70	Destination unreachable (Port unreachable)
46	6.627528	85.114.32.145	192.168.1.112	ICMP	70	Destination unreachable (Port unreachable)
48	8.138431	85.114.32.145	192.168.1.112	ICMP	70	Destination unreachable (Port unreachable)
53	10.629746	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4428/19473, ttl=3 (no response found!)
54	10.642600	85.114.32.146	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
55	10.644218	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4429/19729, ttl=3 (no response found!)
56	10.657428	85.114.32.146	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
57	10.658931	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4430/19985, ttl=3 (no response found!)
58	10.671852	85.114.32.146	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
62	10.702531	85.114.32.146	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
74	12.211689	85.114.32.146	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
77	13.718759	85.114.32.146	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
87	16.210394	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4431/20241, ttl=4 (no response found!)
88	16.223584	85.114.32.102	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
90	16.225536	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4432/20497, ttl=4 (no response found!)
91	16.238392	85.114.32.102	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
92	16.239840	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4433/20753, ttl=4 (no response found!)
93	16.253019	85.114.32.102	192.168.1.112	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
98	16.284146	85.114.32.102	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
108	17.795383	85.114.32.102	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
121	19.304121	85.114.32.102	192.168.1.112	ICMP	110	Destination unreachable (Port unreachable)
153	21.799305	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4434/21009, ttl=5 (no response found!)
154	21.812871	216.66.93.61	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
155	21.814560	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4435/21265, ttl=5 (no response found!)
156	21.828220	216.66.93.61	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)

Slika 25. Prikaz filtriranih paketa početne stranice Stanford fakulteta

No.	Time	Source	Destination	Protocol	Length	Info
157	21.829981	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4436/21521, ttl=5 (no response found!)
158	21.843564	216.66.93.61	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
172	22.855431	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4437/21777, ttl=6 (no response found!)
623	26.506681	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4438/22033, ttl=6 (no response found!)
974	30.504513	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4439/22289, ttl=6 (no response found!)
975	30.523833	184.104.193.113	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
978	31.530002	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4440/22545, ttl=7 (no response found!)
979	31.549104	184.104.197.137	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
980	31.550136	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4441/22801, ttl=7 (no response found!)
981	31.569038	184.104.197.137	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
982	31.570302	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4442/23057, ttl=7 (no response found!)
983	31.590391	184.104.197.137	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1719	32.598651	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4443/23313, ttl=8 (no response found!)
1898	32.642113	184.105.65.5	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1901	32.643515	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4444/23569, ttl=8 (no response found!)
2073	32.682148	184.105.65.5	192.168.1.112	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2098	32.687228	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4445/23825, ttl=8 (no response found!)
5105	36.518804	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4446/24081, ttl=9 (no response found!)
5106	36.624074	72.52.92.113	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5107	36.625751	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4447/24337, ttl=9 (no response found!)
5110	36.730299	72.52.92.113	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5111	36.731609	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4448/24593, ttl=9 (no response found!)
5112	36.836169	72.52.92.113	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5382	37.801129	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4449/24849, ttl=10 (no response found!)
5383	37.968078	184.105.81.218	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5384	37.969623	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4450/25105, ttl=10 (no response found!)
5385	38.136311	184.105.81.218	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5386	38.137322	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4451/25361, ttl=10 (no response found!)
5387	38.304270	184.105.81.218	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5415	39.171766	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4452/25617, ttl=11 (no response found!)
5416	39.339623	72.52.92.158	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5417	39.341266	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4453/25873, ttl=11 (no response found!)
5426	39.508134	72.52.92.158	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5427	39.509856	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4454/26129, ttl=11 (no response found!)
5428	39.677812	72.52.92.158	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5435	40.571221	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4455/26385, ttl=12 (no response found!)
5436	40.739111	184.105.177.238	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Slika 26. Prikaz filtriranih paketa početne stranice Stanford fakulteta



5435 40.571221	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4455/26385, ttl=12 (no response found!)
5436 40.739111	184.105.177.238	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5437 40.740836	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4456/26641, ttl=12 (no response found!)
5438 40.908842	184.105.177.238	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5439 40.910517	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4457/26897, ttl=12 (no response found!)
5440 41.077863	184.105.177.238	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5454 41.968225	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4458/27153, ttl=13 (no response found!)
5472 42.137970	171.64.255.132	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5473 42.140186	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4459/27409, ttl=13 (no response found!)
5603 42.309257	171.64.255.132	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5604 42.311061	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4460/27665, ttl=13 (no response found!)
5617 42.482424	171.64.255.132	192.168.1.112	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
6913 43.704569	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4461/27921, ttl=14 (no response found!)
10897 47.499884	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4462/28177, ttl=14 (no response found!)
14563 51.501738	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4463/28433, ttl=14 (no response found!)
20793 55.497019	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4464/28689, ttl=15 (reply in 20796)
20796 55.665623	171.67.215.200	192.168.1.112	ICMP	106	Echo (ping) reply id=0x0001, seq=4464/28689, ttl=241 (request in 20793)
20797 55.667258	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4465/28945, ttl=15 (reply in 20798)
20798 55.835537	171.67.215.200	192.168.1.112	ICMP	106	Echo (ping) reply id=0x0001, seq=4465/28945, ttl=241 (request in 20797)
20799 55.837093	192.168.1.112	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=4466/29201, ttl=15 (reply in 20800)
20800 56.005530	171.67.215.200	192.168.1.112	ICMP	106	Echo (ping) reply id=0x0001, seq=4466/29201, ttl=241 (request in 20799)

Slika 27. Prikaz filtriranih paketa početne stranice Stanford fakulteta

Na slikama 24. 25. 26. 27. vidimo da imamo 15 skokova što je zapravo samo 4 skoka više nego kad smo primijenili naredbu *traceroute* za *youtube.com* no također vidimo smo naišli na puno više adresa sa nedostupnim odredištem.

Traceroute i *ping* naredbe imaju dodatne opcije poput:

• -d: ova dodatna opcija ne ispisuje imena računala nego samo njegovu IP adresu

• [-m maximum_hops]: naredba pokazuje koliko će „skokova napraviti prije nego što se završi (zadani broj skokova je 30

• [-w timeout]: ova naredba pokazuje koliko milisekundi se čeka prije nego se pošalje sljedeći zahtjev

Koristeći prošli primjer, pokazat ćemo kako se koriste dodatne opcije i koja je njihova uloga.

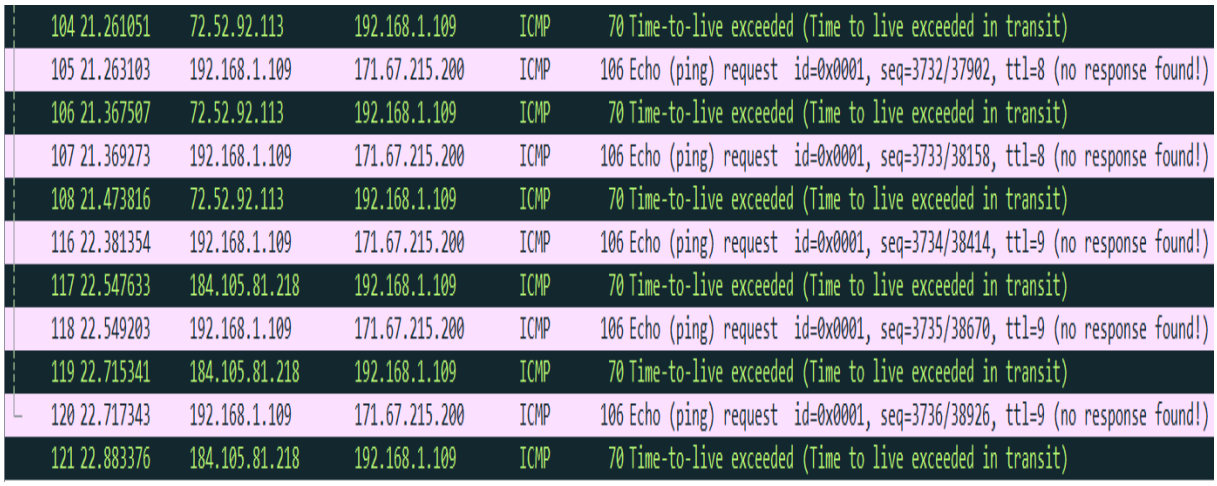
```
C:\Program Files\Microsoft Visual Studio\2022\Community>tracert -d -w 2000 -h 9 stanford.edu

Tracing route to stanford.edu [171.67.215.200]
over a maximum of 9 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    14 ms    14 ms    14 ms  85.114.32.145
  3    12 ms    12 ms    12 ms  85.114.32.146
  4    13 ms    13 ms    13 ms  85.114.32.102
  5    14 ms    13 ms    13 ms  216.66.93.61
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8   104 ms   104 ms   104 ms  72.52.92.113
  9   166 ms   166 ms   166 ms  184.105.81.218

Trace complete.
```

Slika 28. Primjena *traceroute* naredbe pomoću dodatnih opcija

Na slici 26. se vidi da su korištene dodatne opcije. Ispisivat će se samo IP adrese, čeka se 2000 ms prije sljedećeg zahtjeva i odradit će se 9 „skokova“. Uspoređivanjem slike 22. i slike 26. vidi se da se pomoću opcije –d ispisuje samo IP adresu bez imena i da nakon 9. skokova završava praćenje.

14	4.313866	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3710/32270, ttl=1 (no response found!)
15	4.314568	192.168.1.1	192.168.1.109	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
16	4.315583	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3711/32526, ttl=1 (no response found!)
17	4.315972	192.168.1.1	192.168.1.109	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
18	4.316456	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3712/32782, ttl=1 (no response found!)
19	4.316869	192.168.1.1	192.168.1.109	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
26	5.326866	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3713/33038, ttl=2 (no response found!)
27	5.341245	85.114.32.145	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	5.343448	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3714/33294, ttl=2 (no response found!)
29	5.357599	85.114.32.145	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
30	5.359793	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3715/33550, ttl=2 (no response found!)
31	5.373644	85.114.32.145	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
37	6.370127	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3716/33806, ttl=3 (no response found!)
38	6.382921	85.114.32.146	192.168.1.109	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
39	6.383532	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3717/34062, ttl=3 (no response found!)
40	6.396325	85.114.32.146	192.168.1.109	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
41	6.397903	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3718/34318, ttl=3 (no response found!)
42	6.410690	85.114.32.146	192.168.1.109	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
43	7.414676	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3719/34574, ttl=4 (no response found!)
44	7.428133	85.114.32.102	192.168.1.109	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
45	7.429949	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3720/34830, ttl=4 (no response found!)
46	7.443109	85.114.32.102	192.168.1.109	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
47	7.444914	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3721/35086, ttl=4 (no response found!)
48	7.457945	85.114.32.102	192.168.1.109	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
50	8.455754	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3722/35342, ttl=5 (no response found!)
51	8.469717	216.66.93.61	192.168.1.109	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
52	8.471527	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3723/35598, ttl=5 (no response found!)
53	8.485372	216.66.93.61	192.168.1.109	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
54	8.487066	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3724/35854, ttl=5 (no response found!)
55	8.500540	216.66.93.61	192.168.1.109	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
61	9.497782	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3725/36110, ttl=6 (no response found!)
72	11.162073	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3726/36366, ttl=6 (no response found!)
78	13.167684	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3727/36622, ttl=6 (no response found!)
81	15.164784	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3728/36878, ttl=7 (no response found!)
89	17.166871	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3729/37134, ttl=7 (no response found!)
98	19.167397	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3730/37390, ttl=7 (no response found!)
103	21.156758	192.168.1.109	171.67.215.200	ICMP	106	Echo (ping) request id=0x0001, seq=3731/37646, ttl=8 (no response found!)

Slika 29. Prikaz ICMP paketa koji su uhvaćeni prilikom korištenja *traceroute* naredbe s dodatnim opcijama.



Slika 30. Prikaz ICMP paketa koji su uhvaćeni prilikom korištenja *traceroute* naredbe s dodatnim opcijama.

Na slikama 29. i 30. vidimo da idu do 9. „skoka“.

ZAKLJUČAK

Najbitnija zadaća ICMP je obavijestiti porukom ukoliko poslana poruka nije stigla na odredište zbog različitih smetnji. ICMP promet je neophodan za rješavanje problema TCP/IP-a i za upravljanje njegovim protokom i ispravnom funkcijom. Primjenom naredbe ping dobili smo različite podatke za vrijednosti kao što je TTL, redni broj, indentifikator. Primjenom naredbe ping na neko neodređeno odredište će se ispustit svi paketi. ICMP šalje odgovarajuće poruke ukoliko dođe do greške, dakle on ne osigurava prijenos paketa kroz mrežu. Ukoliko nas zanima putanja paketa od nekog računala do odredišta koristimo naredbu *traceroute.* Programom Wireshark mogli smo napraviti najbolju primjenu ovih dviju naredbi.

LITERATURA

[1] ICMP,Wikipedia

https://hr.wikipedia.org/wiki/ICMP

(Datum pristupa web sadržaju: 15.5.2022.)

[2] Internet Control Message Protocol,Wikipedia

https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

(Datum pristupa web sadržaju: 15.5.2022.)

[3] CloudFlare-What is Internet Control Message Protocol?

https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/

(Datum pristupa web sadržaju: 15.5.2022.)

[4] GeeksforGeek-Type of messages

https://www.geeksforgeeks.org/types-of-icmp-internet-control-message-protocol-messages/

(Datum pristupa web sadržaju: 15.5.2022.)

[5] Wireshark,Wikipedia

https://en.wikipedia.org/wiki/Wireshark

(Datum pristupa web sadržaju: 12.6.2022.)

[6] Wireshark

https://wiki.wireshark.org/Home

(Datum pristupa sadržaju:12.6.2022.)

[7] Ping,Wikipedia

https://hr.wikipedia.org/wiki/Ping

(Datum pristupa web sadržaju: 15.5.2022.)

[8]N4L

https://support.n4l.co.nz/s/article/How-to-use-Ping

(Datum pristupa web sadržaju: 12.6.2022.)

[9] Traceroute,Wikipedia

https://en.wikipedia.org/wiki/Traceroute

(Datum pristupa web sadržaju: 15.5.2022.)

[10]Pearson

https://www.informit.com/articles/article.aspx?p=26557&seqNum=5

(Datum pristupa web sadržaju: 12.6.2022.)

SAŽETAK

U teorijskom dijelu završnog rada opisana je struktura ICMP i njegovih poruka. Nakon toga je svaka poruka detaljno objašnjena i prikazan je njen izgled. U praktičnom dijelu su opisane i prikazane različitim primjerima dvije naredbe koje smo koristili u programu Wireshark, a to su *ping* i *traceroute*. Svakim primjerom je prikazana različita mogućnost ovih naredbi. Na kraju smo koristili dodatne opcije koje nam nude naredbe. U radu je korišten program Wireshark i sučelje Command Prompt.

Ključne riječi: ICMP, Wireshark, ping, traceroute

ABSTRACT

The structure of ICMP and it's messages are described in the theoretical part of the undergraduate thesis. After that, each message is explained in detail and it's layout is depicted. In the practical part, two commands used in the Wireshark program are elaborated by using different examples. The two commands are ping and trace route. Each example illustrates the different capabilities of these commands. Furthermore, additional options which are offered by the commands are used. Wireshark program and the Command Prompt interface are used in the thessis.

Key words: ICMP, Wireshark, ping, traceroute

ŽIVOTOPIS

Mario Hardi je rođen 15. lipnja 1999. godine u Osijeku. Pohađao je Osnovnu školu Vladimira Nazora u Đakovu. Sudjelovao je u različitim natjecanjima iz informatike. Opću gimnaziju završio je u Gimnazija A. G. Matoša u Đakovu. Nakon završetka srednjoškolskog obrazovanja upisuje Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, preddiplomski studij računarstva.

PRILOZI

Prilog 1. Završni rad u datoteci docx

Prilog 2. Završni radu u datoteci pdf