ICMP protokol i primjeri njegove primjene

Markov, Petar

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:967193

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-17**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Stručni studij

ICMP PROTOKOL I PRIMJERI NJEGOVE PRIMJENE

Završni rad

Petar Markov

Osijek, 2019.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1S: Obrazac za imenovanje Povjerenstva za obranu završnog rada na preddiplomskom stručnom studiju

Osijek, 10.09.2019.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu završnog rada na preddiplomskom stručnom studiju

Ime i prezime studenta:	Petar Markov
Studij, smjer:	Preddiplomski stručni studij Elektrotehnika, smjer Informatika
Mat. br. studenta, godina upisa:	AI4483, 21.09.2018.
OIB studenta:	63900402378
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Doc. dr. sc. Višnja Križanović
Član Povjerenstva:	Mr.sc. Anđelko Lišnjić
Naslov završnog rada:	ICMP protokol i primjeri njegove primjene
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada	ICMP protokol (Internet Control Message Protocol) jedan je od najvažnijih internetskih protokola. Ne koristi se za transport podataka (poput TCP ili UDP protokola), već je riječ o kontrolnom protokolu (za razmjenu različitih kontrolnih poruka). Potrebno je analizirati ICMP protokol, te objasniti način njegove primjene. Analizirati način njegove primjene u naredbama "ping" i "traceroute" kroz nekoliko zadanih primjera, pri čemu je podatkovne tokove potrebno snimiti pomoću analizatora mrežnog prometa.
Prijedlog ocjene pismenog dijela ispita (završnog rada):	Vrlo dobar (4)
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: 2 razina
Datum prijedloga ocjene mentora:	10.09.2019.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

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

IZJAVA O ORIGINALNOSTI RADA

Osijek, 18.09.2019.

Ime i prezime studenta:	Petar Markov
Studij:	Preddiplomski stručni studij Elektrotehnika, smjer Informatika
Mat. br. studenta, godina upisa:	AI4483, 21.09.2018.
Ephorus podudaranje [%]:	4%

Ovom izjavom izjavljujem da je rad pod nazivom**: ICMP protokol i primjeri njegove primjene**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

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:

Sadržaj

1. UVOD 1

2. RAZVOJ I KARAKTERISTIKE ICMP PROTOKOLA 2

2.1. ICMP poruke 2

3. TIPOVI ICMP PORUKA 4

3.1. Odredište nedostupno (engl. *Destination Unreachable*) 5

3.2. Blokiranje Izvorišta (engl. *Source Quench*) 6

3.3. Istek vremena (engl. *Time Exceeded*) 6

3.4. Problem s parametrima (engl. *Parameter Problem*) 7

3.5. Preusmjeravanje (engl. *Redirection*) 8

3.6. Eho zahtjev/Eho odgovor (engl. *Echo request/Echo reply*) 9

3.7. Vremenska oznaka / Odgovor na vremensku oznaku (engl. *Timestamp/ Timestamp reply*) 10

3.8. Zahtjev za maskom mreže/ odgovor na zahtjev za maskom mreže (engl. *Address mask request/ Address mask reply*) 11

4. PRIMJENE ICMP PROTOKOLA 12

4.1.* Naredba *ping 12

4.2. Naredba *traceroute* 13

4.3. Wireshark program 13

4.4. Analiza *ping* naredbe pomoću programa Wireshark 14

4.5. Analiza *traceroute* naredbe pomoću programa Wireshark 21

5. ZAKLJUČAK 32

6. LITERATURA 33

1. UVOD

U ovom radu objašnjen je i analiziran ICMP protokol (*Internet Control Message Protocol*), te detaljnije objašnjena polja od kojih se sastoji, i poruke koje generira. Kako bi se prikazala primjena ICMP protokola, u praktičnom dijelu rada koristio se program Wireshark , koji nam olakšava praćenje paketa kroz našu mrežu. Uz pomoć Wireshark-a prikazali smo dvije primjene ICMP protokola, a to su *ping* i *traceroute*, s kojima provjeravamo povezanost dvaju računala, te ostalih računala koji su na putu od izvorišnog računala do odredišnog. ICMP protokol se nalazi na mrežnom sloju u OSI (*Open Systems Interconnection*) modelu. Zadatak mrežnog sloja je prijenos datagrama unutar mreže, uz što brži i efikasniji prijenos istih **[1]**. Uz ICMP protokol se na ovom sloju nalaze IP (*Internet Protocol*) protokol (a najvažnije verzije su IPv4 i IPv6) s kojim je usko vezan, te ARP (*Address Resolution Protocol*) i RIP (*Routing Information Protocol*) od važnijih**[2]**.Najvažnija uloga ICMP protokola je slanje poruka odredišnom računalu da je došlo do pogreške u prijenosu. U prvom, teorijskom, dijelu ovog rada objašnjen je razvoj ICMP protokola, njegove funkcije, strukturu, te poruke koje šalje. U drugom, praktičnom dijelu prikazane su njegove primjene uz pomoć programa Wireshark. Cilj ovog završnog rada je preko primjena ICMP protokola provjeriti dostupnost izabranog odredišta, te odrediti koliko „koraka“ ima do tog odredišta.

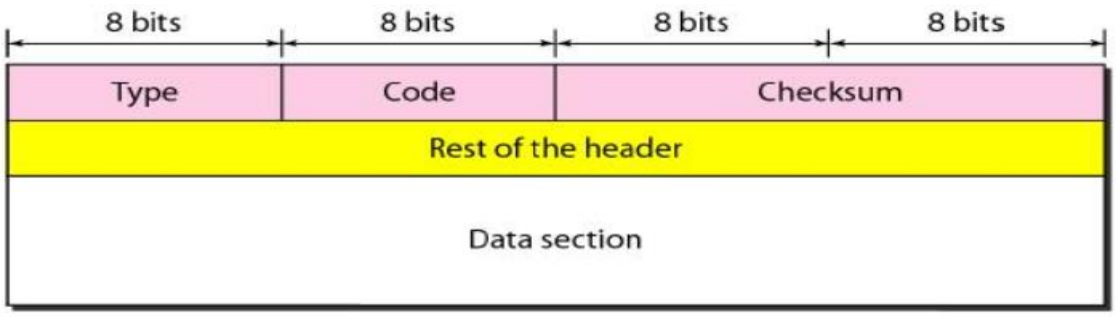
2. RAZVOJ I KARAKTERISTIKE ICMP PROTOKOLA

ICMP protokol je prvi put definiran u RFC 792 standardu 1981. godine. Nalazi se u mrežnom sloju OSI modela. On je integralni dio IP protokola, i mora biti implementiran u svaki IP modul. IP protokol se koristi za prijenos podataka i uspostavu komunikacije između izvorišnog i odredišnog računala. Datagram (paket) je podatak koji se šalje kroz mrežu. Glavna uloga ICMP protokola je slanje informacijskih poruka o pogreškama i kontrola prijenosa podataka do odredišta. Potrebno je provjeriti sadržaj ICMP poruke, te vratiti odredištu odgovarajuću poruku za grešku koja se dogodila. ICMP poruke se šalju u nekoliko situacija:

- Kada datagram ne može doći do odredišta
- Kada pristupnik (engl. *gateway*) nema dovoljno među memorijskog (engl. *buffering*) kapaciteta da proslijedi datagram
- Kada *gateway* može usmjeriti izvorište da šalje promet preko kraće rute

IP protokol nije napravljen da bude potpuno pouzdan, te nema mehanizam za prijavljivanje i ispravljanje grešaka . Namjena poruka koje ICMP protokol šalje su da pružaju povratnu informaciju o problemima u komunikacijskom okruženju, a ne da poboljšaju pouzdanost IP protokola. Uvođenjem ICMP protokola i dalje nije potpuno sigurno da će datagram biti dostavljen, ili da će se kontrolna poruka vratiti. Neki datagrami se neće dostaviti bez izvještaja o njihovim gubicima, što znači da ICMP protokol ne osigurava pouzdan prijenos. Protokoli većeg reda koji koriste IP protokol moraju implementirati sami svoja rješenja za pouzdanost prijenosa ako je potreba pouzdana komunikacija. ICMP poruke obično prijavljuju pogreške u procesiranju datagrama. Kako bi se izbjegla beskonačna petlja ne šalju se ICMP poruke o ICMP porukama.

2.1. ICMP poruke



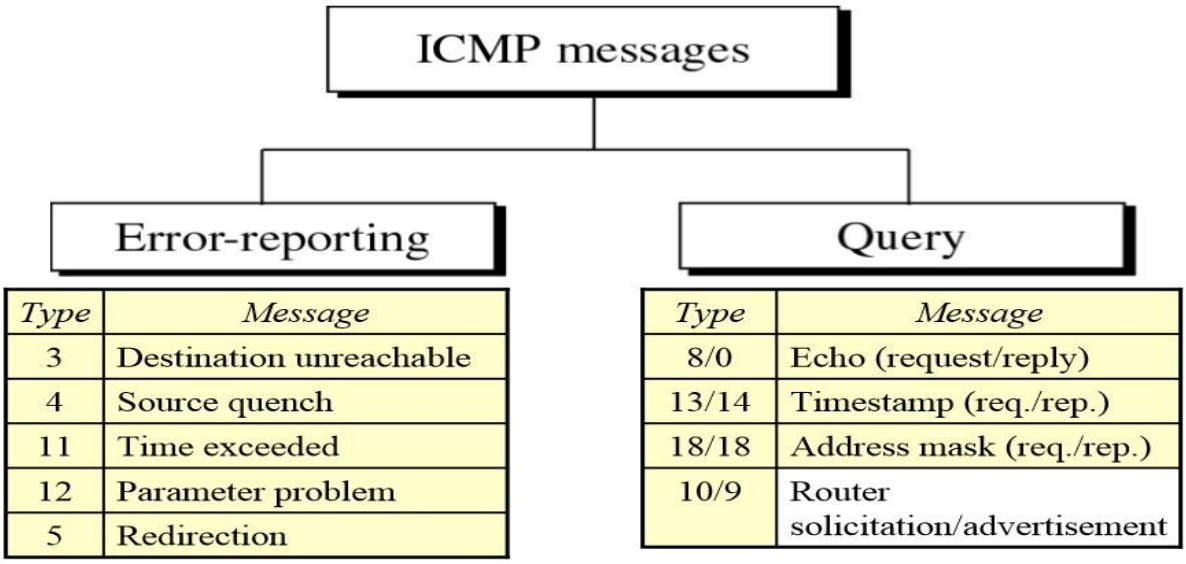
Slika 1. Format ICMP zaglavlja [9]

ICMP poruke se šalju koristeći osnovno IP zaglavlje. Sastoje se od zaglavlja (engl. *header*) i sekcija za podatke (engl. *Data section*). Prvi oktet (8 bitova) u zaglavlju se koristi za Tip (engl. *Type*) ICMP poruke. ICMP generira nekoliko tipova poruka koji će biti detaljnije objašnjeni u sljedećem poglavlju. Sljedeći oktet predstavlja Kod (engl. *Code*) poruke. Ti kodovi su posebno definirani za svaki tip poruke. Kontrolna suma (engl. *Checksum*) je 16-bitni komplement od komplementarne sume ICMP poruka počevši s poljem *Type* poruke. Polje *Checksum* bi trebalo biti nula zbog računanja te kontrolne sume. Ostatak zaglavlja (engl. *Rest of the header*) ima 4 okteta i njegov sadržaj varira ovisno o tipu i kodu poruke. *Data section* sadrži specifične podatke za vrstu poruke koji su naznačeni u poljima *Type* ICMP poruke i *Code* ICMP poruke. ICMP poruke su podijeljene u dvije osnovne kategorije:

- *Error-reporting poruke*
- *Query poruke*

Error-reporting poruke izvještavaju o problemu na koji usmjerivač (engl. *router*) ili odredišno računalo možda naiđu dok procesiraju IP datagram. *Query* poruke, koje su šalju u paru, pomažu host-u da dobije neku specifičnu informaciju od usmjerivača ili nekog drugog odredišta. One se najčešće koriste da bi se dobila informacija radi li odredište i dalje. ICMP uvijek šalje poruke o grešci nazad do izvornog izvora.

3. TIPOVI ICMP PORUKA



Type	*Message*
3	Destination unreachable
4	Source quench
11	Time exceeded
12	Parameter problem
5	Redirection

Type	*Message*
8/0	Echo (request/reply)
13/14	Timestamp (req./rep.)
18/18	Address mask (req./rep.)
10/9	Router solicitation/advertisement

Slika 2. Podjela ICMP poruka po kategorijama [10]

Prema slici 2. vidimo podjelu po kategorijama koje smo naveli u prošlom poglavlju. U *error-reporting* poruke svrstavaju se:

- Odredište nedostupno (engl. *Destination unreachable*)
- Blokiranje izvorišta (engl. *Source quench*)
- Istek vremena (engl. *Time exceeded*)
- Problem s parametrima (engl. *Parameter problem*)
- Preusmjeravanje (engl. *Redirection*)

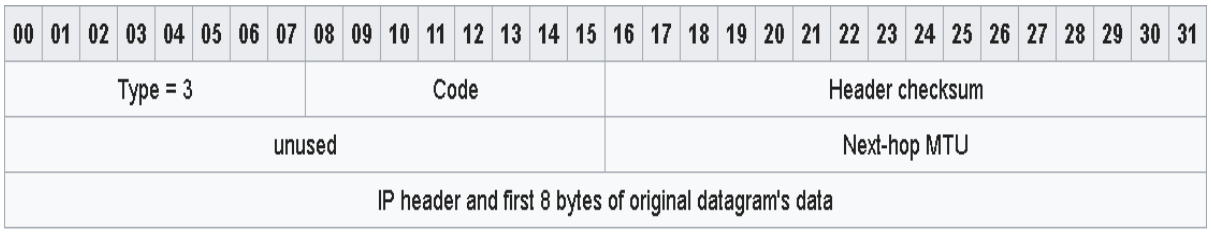
Za *error-reporting* poruke se ne zahtijeva odgovor. Kod *query* poruka se zahtijeva odgovor na poslanu poruku kako bi se doznala informacija koja se traži u zahtjevu. *Query* poruke su:

- Eho zahtjev/Eho odgovor (engl. *Echo request/ Echo reply*)
- Zahtjev za vremenskom oznakom / Odgovor na zahtjev za vremensku oznaku (engl. *Timestamp request/ Timestamp reply*)
- Zahtjev za maskom mreže/ Odgovor na zahtjev za maskom mreže (engl. *Address mask request/ Address mask reply*)

3.1. Odredište nedostupno (engl. *Destination Unreachable*)

ICMP poruka *Destination unreachable* šalje usmjerivač da informira izvorište da je *unicast* adresa odredišta nedostupna. *Unicast* adresa jedinstveno određuje sučelje po svojoj adresi. Pošiljaocu se vraćaju IP zaglavlje i prvih 8 bajtova originalnog datagrama. Ovi podaci se koriste od strane hosta da bi se napravio odgovarajući postupak. Neki od razloga za ovu poruku mogu biti:

- Fizička veza do hosta ne postoji (udaljenost je beskonačna)
- Navedeni protokol ili port nije aktivan
- Podaci moraju biti fragmentirani ali je *Don't fragment* zastavica podignuta



Slika 3. Izgled poruke *Destination unreachable* [7]

Polje *Type* je kod poruke *Destination unreachable* uvijek postavljeno na 3, dok se polje *Code* koristi da bi se specificirao tip pogreške. Postoji 15 kodova pogreška u poruci *Destination unreachable*, a neki od njih su :

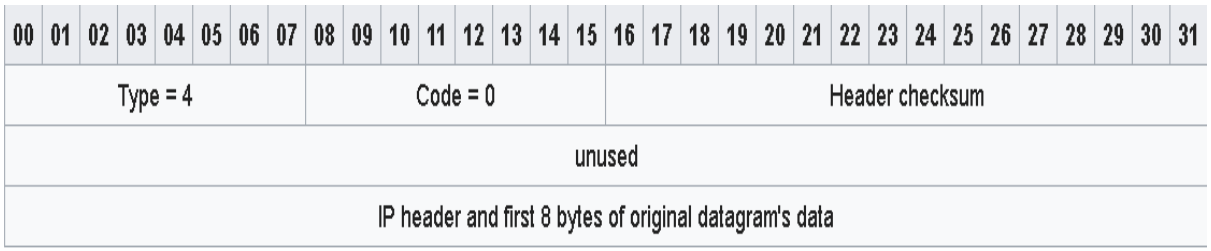
- *Code* 0: Mreža nedostupna (engl. *Network unreachable error*)
- *Code* 1: Host nedostupan (engl. *Host unreachable error*)
- *Code* 2: Protokol nedostupan (engl. *Protocol unreachable error*)
- *Code* 3: Port nedostupan (engl. *Port unreachable error*)
- *Code* 4: Datagram je prevelik i paket zahtijeva fragmentaciju, ali zastavica *Don't fragment* je podignuta (u ovome slučaju *gateway* mora odbaciti taj datagram i vratiti poruku *Destination unreachable*)
- Code 5: Ruta do izvora nije pronađena (engl. *Source route failed error*)

Kodovi 2 i 3 šalje samo odredišni host, dok sve ostale kodove šalje usmjerivač. Polje *Next-hop MTU* se koristi kad dođe do pogreške s kodom 4 (Datagram je prevelik). Ono sadrži MTU (*Maximum transmission unit*), što je veličina najvećeg PDU (*Protocol data unit*) koji

se može prenijeti u jednoj transakciji mrežnog sloja, sljedećeg najbližeg usmjerivača kroz kojeg paket može proći. PDU je jedna jedinica podataka koja se prenosi kroz mrežu.

3.2. Blokiranje Izvorišta (engl. *Source Quench*)

ICMP poruka *Source Quench* se šalje pošiljatelju da smanji broj poruka koje se šalju usmjerivaču ili hostu. Ova poruka se može generirati ako usmjerivač ili host nemaju dovoljno prostora u međuspremniku da se obradi poslani zahtjev, ili se taj prostor približava svome limitu. Kada se popuni red čekanja u usmjerivaču za primanje podataka, podaci koji dolaze se odbacuju sve dok se ne isprazni red čekanja. Zbog ovakvih situacija se uveo mehanizam blokiranja izvorišta. Kada usmjerivač vidi da je brzina ulaznih poruka veća nego brzina izlaznih poruka, on šalje ICMP poruku *Source Quench* klijentima da uspore sa slanjem ili da pričekaju određeno vrijeme prije pokušaja slanja novih podataka.



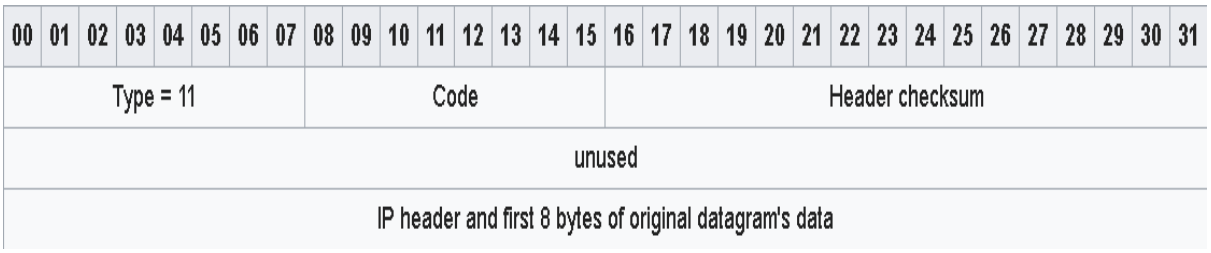
Slika 4. Izgled *Source Quench* poruke [7]

Polje *Type* poruke kod *Source Quench* poruke uvijek ima vrijednost 4, dok je vrijednost polja *Code* uvijek 0. Izvorištu se vraća IP zaglavlje te prvih 8 bajtova poruke kako bi se znalo na kojem paketu se greška pojavila. Jedna poruka *Source Quench* poslana je za svaki datagram koji se odbacio prilikom zakrčenosti prometa. *Code* 0 šalje samo *gateway* ili host.

3.3. Istek vremena (engl. *Time Exceeded*)

ICMP poruka *Time Exceeded* se generira od strane *gateway-a* kako bi se izvorište informiralo o odbačenom datagramu zbog toga što mu je polje TTL („*Time to live*“) smanjio na 0, ili od strane host-a kada ne uspije ponovno sastaviti fragmentirani datagram u vremenu u kojem je trebao. TTL je mehanizam uveden kako bi ograničio „život“ datagrama. Može biti implementiran kao brojač ili vremenska oznaka ugrađena u datagram. TTL polje je postavljeno na neki iznos od strane pošiljatelja datagrama, i smanjuje se nakon svakog usmjerivača kroz koji prođe tijekom puta do svojeg odredišta.

Ako se TTL polje smanji do 0 prije nego što datagram dođe do odredišta, taj datagram se odbacuje i ICMP poruka se šalje nazad pošiljatelju. Ovaj mehanizam je koristan zato što se tako sprječava da datagram beskonačno kruži mrežom. *Time Exceeded* poruke se koriste kod *traceroute* primjene da bi se identificirali *gateway-i* na putu između izvorišta i odredišta.

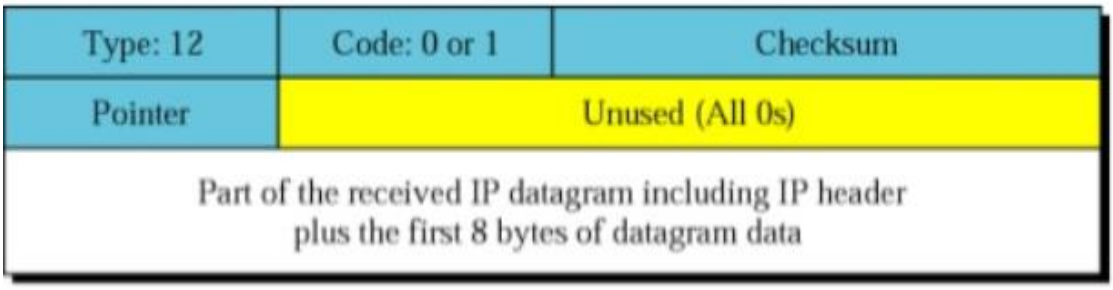


Slika 5. Izgled *Time Exceeded* poruke [7]

Polje *Type* kod *Time Exceeded* poruke uvijek ima 11 vrijednost. Polje *Code* može imati vrijednost 0 ili 1. Vrijednost 0 se dobiva kada se TTL prilikom prijenosa smanjio na vrijednost 0, i tu vrijednost izvorištu vraćaju samo usmjerivači. Vrijednost 1 vraća nazad odredište u slučaju da svi fragmenti nisu došli na vrijeme. Također se izvorištu šalje IP zaglavlje i prvih 8 bajtova poslanog datagrama kako bi se odredilo o kojem datagramu se radi.

3.4. Problem s parametrima (engl. *Parameter Problem*)

ICMP poruka *Parameter Problem* je generirana kao odgovor na bilo koju pogrešku koja nije pokrivena s drugom ICMP porukom. Prilikom obrade datagrama, ako *gateway* ili host naiđu na problem s parametrima zaglavlja tako da ne mogu završiti obradu datagrama, taj datagram se odbacuje.



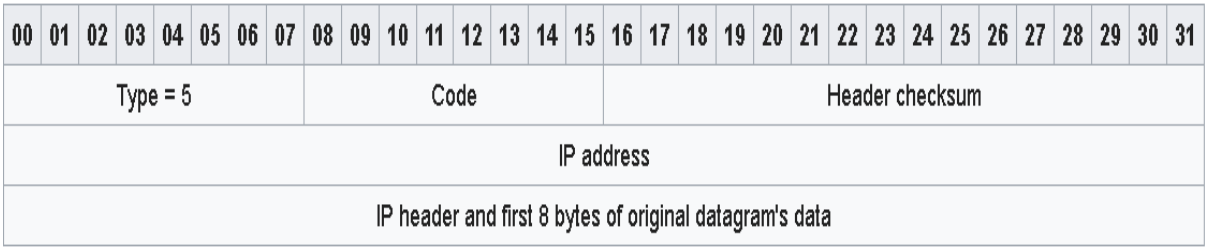
Slika 6. Izgled *Parameter Problem* poruke [9]

Polje *Type* kod ICMP poruke *Parameter Problem* je uvijek postavljen na 12. Polje *Code* može poprimiti vrijednosti 0 i 1. *Code* 0 se dobiva za nepostojeće IP zaglavlje, a *Code* 1 ako nedostaje obavezna opcija. *Code* 0 se dobiva od *gateway-a* ili host-a. Polje *Pointer* se

koristi samo ako se dobije *Code* 0, a on identificira *offset* bajta na kojem je došla pogreška u zaglavlju. Izvorištu se još šalje IP zaglavlje i prvih 8 bajtova originalnog datagrama kako bi se odredilo od kojem datagramu se radi.

3.5. Preusmjeravanje (engl. *Redirection*)

ICMP poruka *Redirection* se koristi kako bi se obavijestio udaljeni host da pakete šalje preko neke alternativne rute. Host ne bi trebao slati poruku *Redirection*, to bi trebali slati samo *gateway-i* (uvedeno u RFC 1122). Na primjer, ako jedan *gateway* G1 šalje neki podataka preko drugog *gateway-a* G2, a ima neki bliži *gateway* G3, koji se računa preko tablica za usmjeravanje, tada *gateway* G2 šalje ICMP poruku *Redirection gateway-u* G1 koji će osvježiti svoje tablice za usmjeravanje i ubuduće odmah slati preko *gateway-a* G3. Također *gateway* G2 šalje izvorni podatak do *gateway-a* G3.



Slika 7. Izgled *Redirection* poruke [7]

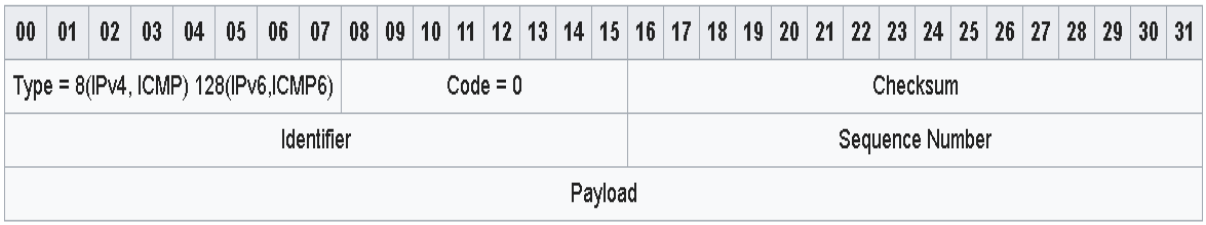
Polje *Type* kod ICMP poruke *Redirection* ima vrijednost 5. Polje *Code* može biti 0,1,2,3, a to su:

- *Code* 0: Preusmjeravanje datagrama za mrežu
- *Code* 1: Preusmjeravanje datagrama za host-a
- *Code* 2: Preusmjeravanje datagrama za ToS („*Type of Service*“) i mrežu
- *Code* 3: Preusmjeravanje datagrama za ToS i host-a

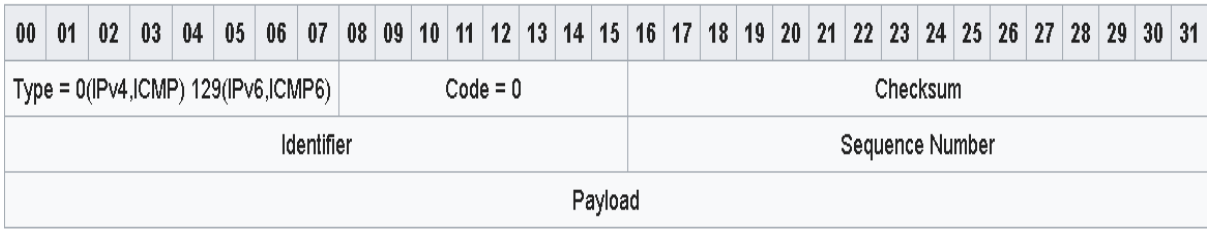
Type of Service je polje unutar IPv4 zaglavlja i ono specificira prioritet datagrama. Ovisno o vrijednostima ToS-a paket bi se smjestio u prioritetni odlazni red. Također se šalje IP adresa (32 bitna) *gateway-a* do kojeg bi se preusmjeravanje trebalo napraviti. Uz to se šalje i IP zaglavlje i prvih 8 bajtova originalnog datagrama.

3.6. Eho zahtjev/Eho odgovor (engl. *Echo request/Echo reply*)

ICMP *Echo request* poruka je prva od *Query* poruka koja će biti objašnjena u ovome radu. Ova poruka dolazi u paru s *Echo reply* porukom. Host ili usmjerivač šalje *Echo request,* a *Echo reply* šalje host ili usmjerivač koji je dobio *Echo request* poruku. Ovaj par poruka najčešće koristimo kako bi saznali je li odredište aktivno. *Echo request* i *Echo reply* mogu se još koristiti kako bi se provjerilo funkcioniranje IP protokola. Znači da ove dvije poruke imaju dvostruku zadaću, a to je provjeravanje aktivnosti odredišta i jesu li izvorište i odredište povezani. Ove poruke se koriste prilikom upotrebe *ping* naredbe, koju ćemo koristiti u praktičnom dijelu. Prilikom *Echo reply* adrese izvorišta i odredišta zamjene mjesta. Kako bi se napravila *Echo reply* poruka, izvorišna i odredišna adresa se zamjene, polje *Type* se promjeni na 0, a kontrolna suma se ponovo izračuna.



Slika 8. Izgled *Echo request* poruke [8]



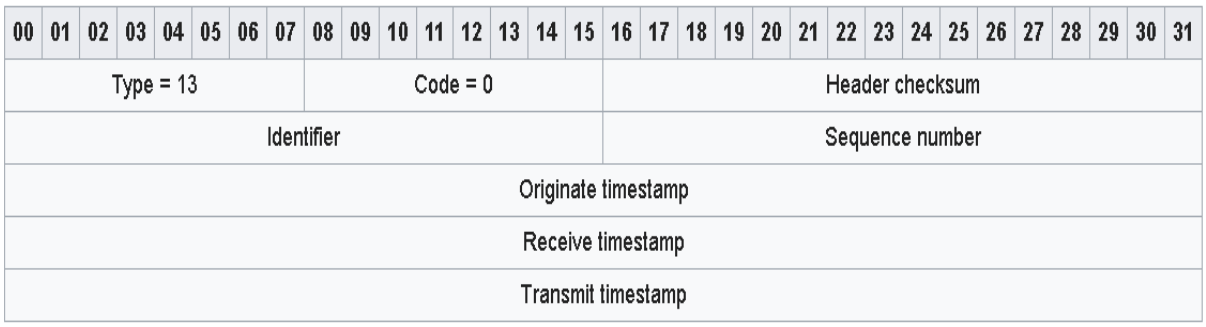
Slika 9. Izgled *Echo reply* poruke [8]

Kod *Echo request* poruke polje *Type* je postavljeno na 8, a kod *Echo reply* poruke je postavljeno na 0. Kod obje vrste poruka polje *Code* ima vrijednost 0. Polja Identifikator (engl. *Identifier*) i polje Redni Broj (engl. *Sequence Number*) se koriste kako bi se olakšalo spajanje zahtjeva s odgovarajućim odgovorom. Na primjer, *Identifier* se može koristiti kao port za TCP (*„Transmission Control Protocol“*) ili UDP (*„User Datagram Protocol“*) kako bi se identificirala sesija, a *Sequence Number* se povećava za svaki *Echo request* koji je poslan. Odredište mora vratiti te iste vrijednosti kada vraća *Echo reply*. U polju *Payload* se najčešće nalazi vremenska oznaka koja nam govori kada se dogodilo prijenos. Ovo je

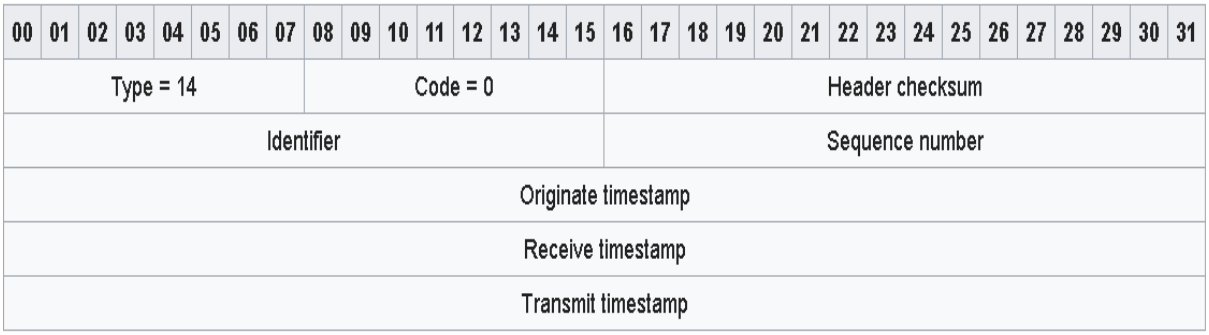
korisno za naredbu *ping* zato što preko toga može izračunati RTT (*„Round Trip Time“*). To je vrijeme (u milisekundama) potrebno da bi paket došao od izvora do odredišta i opet nazad do izvora.

3.7. Vremenska oznaka / Odgovor na vremensku oznaku (engl. *Timestamp/ Timestamp reply*)

U ICMP poruci *Timestamp* izvor šalje svoju vremensku oznaku, a odredište vraća dodatnu vremensku oznaku. U toj 32 bitnoj vremenskoj oznaci nalazi se vrijeme koje je prošlo od ponoći prema UTC (*„Coordinated Universal Time“*). Ove poruke se najčešće koriste kako bi se saznao RTT.



Slika 10. Izgled *Timestamp* poruke [7]



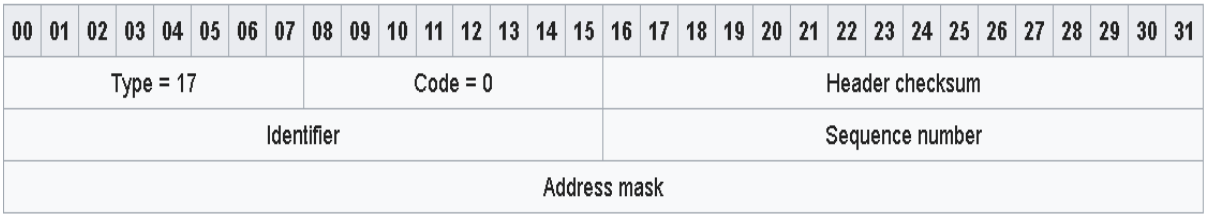
Slika 11. Izgled *Timestamp reply* poruke [7]

Polje *Type* kod poruke *Timestamp* je postavljeno na 13, a kod poruke *Timestamp reply* je postavljeno na 14. Polje *Code* je postavljeno na 0 kod obje poruke. Polja *Identifier* i *Sequence nubmer* se koriste kako bi olakšalo sparivanje zahtjeva i odgovora na vremensku oznaku. Izvorna vremenska oznaka (engl. *Originate timestamp*) je vrijeme kada je pošiljalac zadnji put „dodirnuo“ poruku prije slanja. Primljena vremenska oznaka (engl.

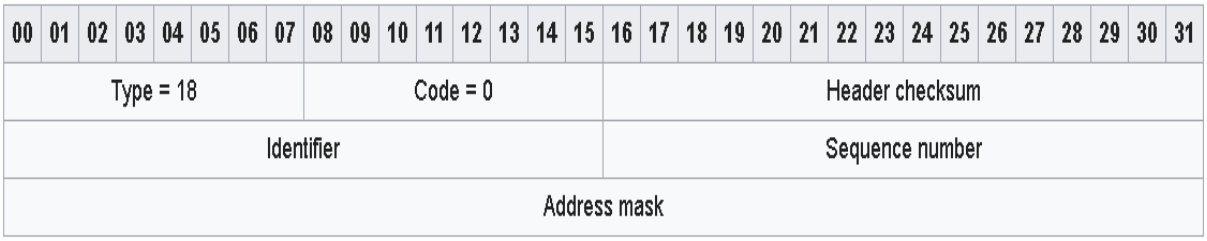
Receive timestamp) je vrijeme kada je primatelj „dotaknuo“ poruku, a Poslana vremenska oznaka (engl. *Transmit timestamp*) je vrijeme kada je primatelj zadnji put „dodirnuo“ poruku prije nego ju je vratio. Pomoću para ovih poruka može se izračunati RTT između izvora i odredišta iako njihovi satovi nisu sinkronizirani. Također možemo sinkronizirati dva sata u dva različita računala pomoću ovih poruka.

3.8. Zahtjev za maskom mreže/ odgovor na zahtjev za maskom mreže (engl. *Address mask request/ Address mask reply*)

Gateway koji dobije ICMP poruku *Address mask request* mreže trebao bi odgovoriti na taj zahtjev tako što vrati poruku *Address mask reply* gdje je polje Maska mreže (engl. *Address mask*) postavljeno na 32-bitnu masku koja identificira podmrežu i mrežu za traženu podmrežu.



Slika 12. Izgled *Address mask request* poruke [7]



Slika 13. Izgled *Address mask reply* poruke [7]

ICMP poruka *Address mask request* ima polje *Type* postavljeno na 17, dok je kod poruke *Address mask reply* postavljeno na 18. Kod obje poruke polje *Code* je postavljeno na 0. Polja *Identifier* i *Sequence number* se koriste kako bi olakšalo sparivanje zahtjeva i odgovora za maskom podmreže. Kod poruke *Address mask request* i kod poruke *Address mask reply* polje *Address mask* sadržava masku podmreže od host-a kojem šaljemo zahtjev.

4. PRIMJENE ICMP PROTOKOLA

U prijašnjem poglavlju navedene su dvije primjene ICMP protokola, a to su:

- Naredba *ping*
- Naredba *traceroute*

4.1. Naredba *ping*

Naredba *ping* je jedna od najpoznatijih primjena ICMP paketa kako bi se ocijenila povezanost dvaju računala. Ova naredba se može koristiti i za prikupljanje nekih statističkih podataka kao što su RTT (*„Round trip time"*) koji mjeri vrijeme potrebno da paket dođe od izvorišta do odredišta i nazad, te broj poslanih i vraćenih paketa i postotak izgubljenih paketa. Ova naredba funkcionira tako da šalje ICMP poruku *Echo request* do odredišnog računala i čeka ICMP poruku *Echo reply*.

```
C:\Users\Petar>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 13. Izgled *ping* naredbe

Prema slici 13 vidimo izgled *ping* naredbe i statističkih podataka koje dobijemo nazad. Da bi „pingali" neko računalo potrebno je znati ili IP adresu računala ili URL adresu nekog host-a. U ovome primjeru „pingali" smo sami svoje računalo. Šaljemo 4 paketa i dobivamo nazad 4 paketa. Također vidimo koliki je TTL. Podatak *time* označava RTT poslanog paketa. Ako nema odgovora od računala koje smo „pingali", ispisuju se obavijesti o isteku vremena i to računalo se smatra nedostupnim.

4.2. Naredba *traceroute*

Preko naredbe *traceroute* možemo saznati koliko „skokova“ je potrebno da se dođe od izvorišta do odredišta, tj. koliko usmjerivača ima od izvorišta do odredišta. *Traceroute* radi na principu da izvor pošalje poruku *Echo request* s TTL parametrom paketa postavljenog na 1. Kada dođe do prvog usmjerivača TTL se smanjuje na 0 i taj usmjerivač generira ICMP poruku *Time exceeded* koju šalje nazad na izvorište. Nakon toga TTL se poveća za 1. Kada dođe do prvog usmjerivača smanji na 1, te ide dalje do drugog usmjerivača gdje se TTL smanjuje na 0 i taj usmjerivač šalje ICMP poruku *Time exceeded* nazad na izvor. Ovaj postupak se ponavlja sve dok se ne dođe do odredišta. Prema tome znamo koliko usmjerivača ima na putu od izvora do odredišta.

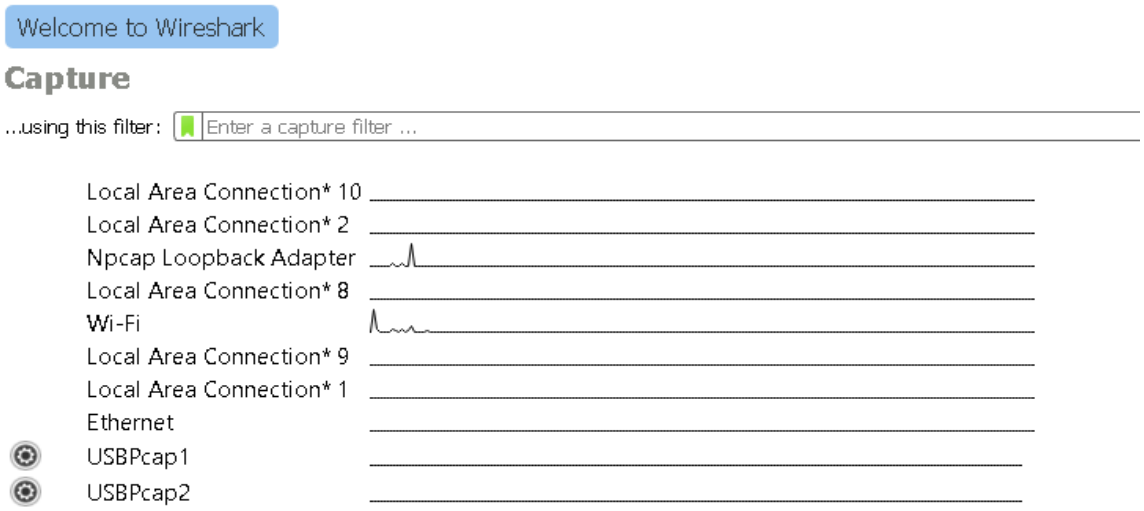
```
$traceroute wikipedia.org
traceroute to wikipedia.org (66.230.200.100), 64 hops max, 44 byte packets
 1  124.ae0.xr1.3d12.xs4all.net (194.109.21.1)  0.305 ms  0.360 ms  0.405 ms
 2  0.so-6-0-0.xr1.tc2.xs4all.net (194.109.5.10)  0.634 ms  0.716 ms  0.673 ms
 3  ams-ix-c00.wvfiber.net (195.69.145.58)  0.638 ms  0.601 ms  0.551 ms
 4  lon-c00-pos-4-0.OC48-ams-pos11-0.wvfiber.net (63.223.28.201)  7.512 ms  7.427 ms  7.494 ms
 5  nyc60-pos-1-0.OC48-lon-c00-pos-3-0.wvfiber.net (63.223.28.145)  84.108 ms  83.804 ms  83.995 ms
 6  66.216.1.181 (66.216.1.181)  83.435 ms  83.278 ms  83.348 ms
 7  ash-c01-tge-3-3.TG-nyc-c01-1-1.wvfiber.net (66.216.1.161)  89.563 ms  89.554 ms  89.551 ms
 8  atl-c01-tge-3-1.TG-ash-c01-3-1.wvfiber.net (66.216.1.157)  103.701 ms  103.606 ms  103.596 ms
 9  cpp-hostway.wvfiber.net (63.223.8.26)  103.678 ms  103.609 ms  103.630 ms
10  e1-12.co2.as30217.net (64.156.25.105)  113.014 ms  113.044 ms  113.084 ms
11  10ge5-1.csw5-pmtpa.wikimedia.org (84.40.25.102)  113.153 ms  113.251 ms  113.180 ms
12  rr.pmtpa.wikimedia.org (66.230.200.100)  113.069 ms  113.172 ms  113.003 ms
```

Slika 14. Izgled *traceroute* naredbe [11]

Ispis *traceroute* naredbe nam prikazuje sve usmjerivače i njihove IP adrese, te RTT između izvora i svakog usmjerivača. Na kraju dobijemo vrijeme potrebno za uspostavu konekcije između izvora i odredišta. Ako nam se ispiše „ * “, to znači da nema odgovora od traženog usmjerivača.

4.3. Wireshark program

Wireshark je besplatni program za analizu paketa koji prolaze kroz mrežu. Koristi se za rješavanje problema u mreži. Za razliku od ostalih sličnih programa Wireshark ima grafičko sučelje što olakšava snalaženje. Pomoću Wireshark-a i cmd-a (*„Command Prompt“*) ćemo prikazati i analizirati *ping* i *traceroute* naredbe, tj. koje pakete šalju te dvije naredbe. Prije svega u samom programu moramo odrediti koju mrežu hoćemo „osluškivati“.



Slika 15. Početna stranica Wireshark programa

Prema slici 15. vidimo ponuđene sučelja (engl. *Interface*) koje je moguće analizirati. Trenutno smo spojeni preko Wi-Fi, pa ćemo preko toga sučelja analizirati promet. Također moramo osigurati da nismo u promiskuitetnom načinu rada kako ne bi hvatali promet od ostalih uređaja koji su povezani na naš Wi-Fi.

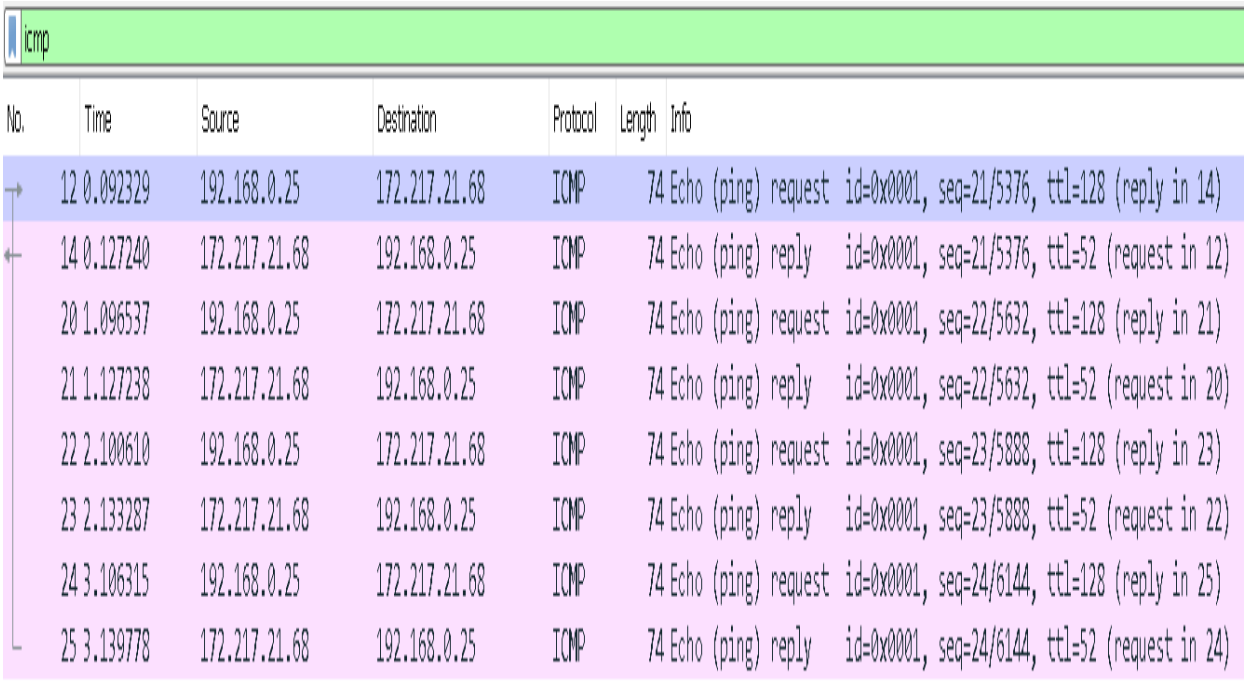
4.4. Analiza *ping* naredbe pomoću programa Wireshark

Za početak ćemo probati „pingati“ početnu stranicu Google-a. To radimo tako da u programu Wireshark pokrenemo „Način snimanja“ (engl. *Capture Mode*), te odaberemo naše sučelje. Nakon toga preko cmd-a pokrenemo „pinganje“ pomoću komande: ping www.google.com.

```
C:\Users\Petar>ping www.google.com

Pinging www.google.com [172.217.21.68] with 32 bytes of data:
Reply from 172.217.21.68: bytes=32 time=35ms TTL=52
Reply from 172.217.21.68: bytes=32 time=30ms TTL=52
Reply from 172.217.21.68: bytes=32 time=32ms TTL=52
Reply from 172.217.21.68: bytes=32 time=33ms TTL=52

Ping statistics for 172.217.21.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 35ms, Average = 32ms

C:\Users\Petar>
```

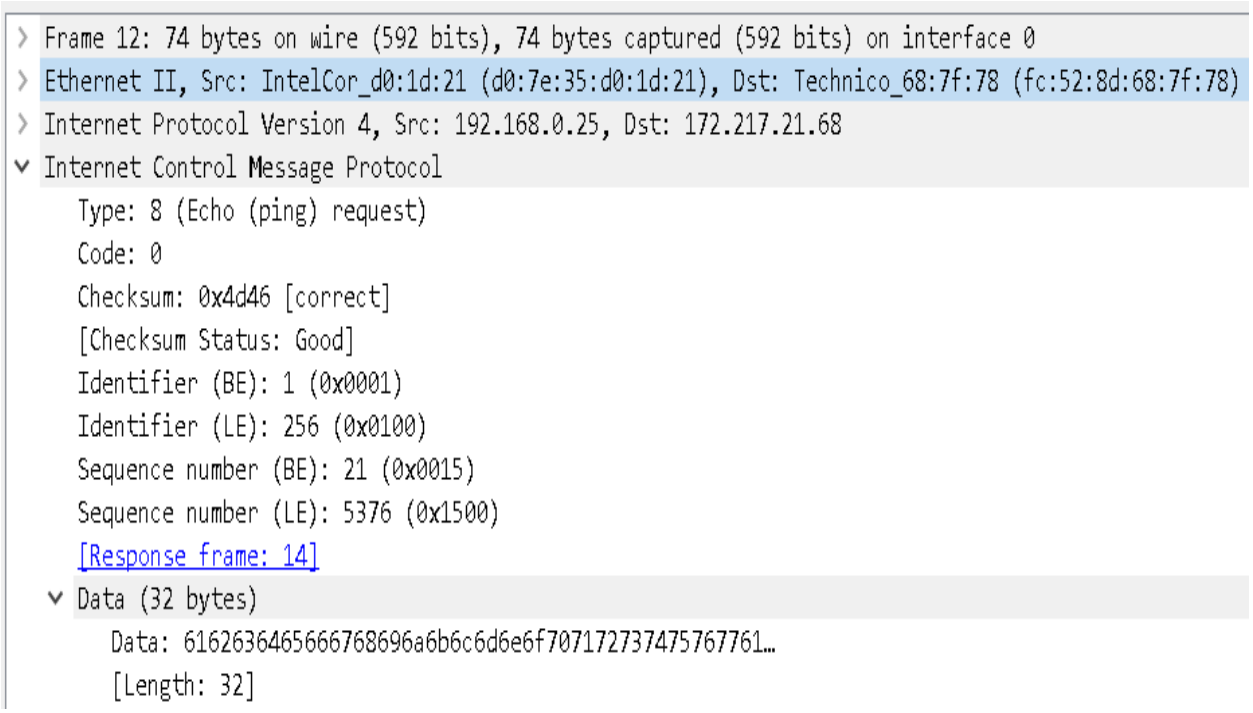
Slika 16. „Pinganje“ početne stranice Google-a

Nakon što dobijemo odgovore *ping* komande, zaustavljamo *Capture Mode*, te dobivamo u Wireshark-u analizu prometa. Wireshark ima mogućnosti filtriranja, te pomoću toga filtriramo ICMP pakete.



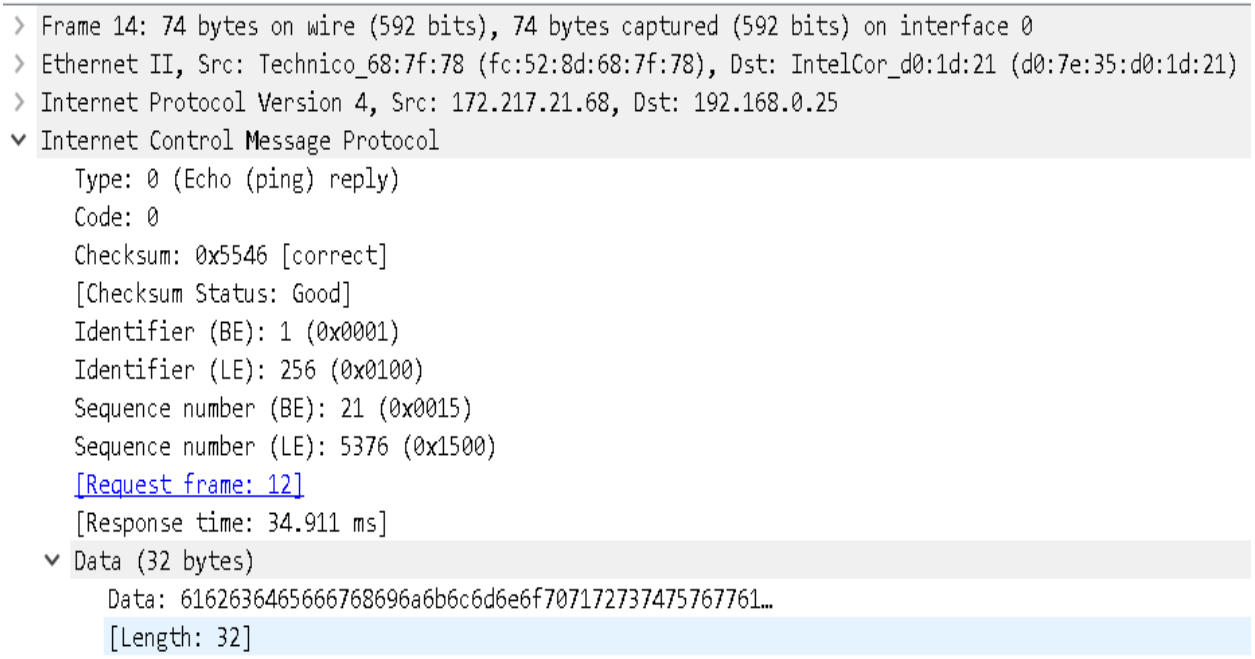
Slika 17. Filtrirani paketi u Wireshark-u

Na slici 17 vidimo sve pakete koje smo snimili i koji koriste ICMP protokol. Stupac Broj (No.) prikazuje koji je to paket koji smo snimili od početka snimanja. Stupac vrijeme (engl. *Time*) označava u kojoj sekundi od početka snimanja je paket snimljen. Stupci Izvor (engl. *Source*) i Odredište (engl. *Destination*) sadrže izvorišnu i odredišnu adresu paketa. Stupac Protokol (engl. *Protocol*) nam govori koji protokol koristi snimljeni paket, dok nam stupac veličina (engl. *Length*) govori kolika je ukupna veličina paketa. Stupac Info sadrži osnovne informacije o paketu kao što su ime ICMP poruke, *Identifier*, *Sequence number*, te TTL i u kojem je paketu poslan ili zahtjev ili odgovor na upit. Prvi paket koji je nama prikazan je paket *Echo request* koji je zapravo 12. uhvaćeni paket. Izvorišna adresa mu je naše računalo (192.168.0.25), a odredišna adresa u ovome slučaju adresa početne stranice Google-a kojega mu je dodijelio DNS (*„Domain Name System"*) server. U našem slučaju protokol je ICMP, a veličina paketa je 74 bajta. Također možemo detaljnije proučiti paket.



Slika 18. Detaljniji prikaz ICMP *Echo request* paketa

Na slici 18 vidimo osnova polja koja su navedena u poglavlju 2.1. gdje smo opisali izgled ICMP poruka . Polje *Type* poruke je 8 što odgovara ICMP poruci *Echo request*. Kod te poruke polje *Code* mora biti postavljeno na 0, što u našem slučaju je. Kontrolna suma je točna, a polje *Identifier* je 1 od mogućih 256. *Sequence number* je 21 od 5376. Odgovor na ovaj zahtjev smo dobili u 14 paketu.



Slika 19. Detaljniji prikaz ICMP *Echo reply* paketa

Prema slici 19 vidimo da su polja *Type* i *Code* postavljeni na 0, što odgovara izgledu ICMP poruke *Echo reply*. Polja *Identifier* i *Sequence number* su jednaka kao kod paketa za ICMP. Zbog ta dva polja *Echo request* je našao odgovarajući *Echo reply*. Zahtjev za ovaj odgovor smo dobili u paketu 12, a vrijeme odgovora, tj. RTT je 34.911 milisekunde, što možemo usporediti s vremenom koje nam je cmd ispisao na slici 16.

Za drugi primjer ćemo uzeti neko odredište koje je bliže nama. Također u ovome primjeru, kao i u svima na dalje smo spojeni preko LAN kabla, te preko toga sučelja pratimo promet. Za ovaj primjer uzeli smo početnu stranicu lokalnog portala Sbplus.

```
Pinging www.sbplus.hr [178.218.164.232] with 32 bytes of data:
Reply from 178.218.164.232: bytes=32 time=23ms TTL=120
Reply from 178.218.164.232: bytes=32 time=23ms TTL=120
Reply from 178.218.164.232: bytes=32 time=24ms TTL=120
Reply from 178.218.164.232: bytes=32 time=25ms TTL=120

Ping statistics for 178.218.164.232:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 25ms, Average = 23ms
```

Slika 20. „Pinganje“ početne stranice Sbplus portala

icmp

No.	Time	Source	Destination	Protocol	Length	Info
4	0.579241	192.168.1.3	178.218.164.232	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 5)
5	0.602720	178.218.164.232	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=120 (request in 4)
6	1.585279	192.168.1.3	178.218.164.232	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 7)
7	1.608554	178.218.164.232	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=120 (request in 6)
33	2.590208	192.168.1.3	178.218.164.232	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (reply in 34)
34	2.614533	178.218.164.232	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=42/10752, ttl=120 (request in 33)
35	3.596036	192.168.1.3	178.218.164.232	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 36)
36	3.621221	178.218.164.232	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=120 (request in 35)

Slika 21. Filtrirani paketi za stranicu Sbplus portala

Kao i u prošlom primjeru vidimo da imamo 4 zahtjeva i 4 odgovora, što znači da je odredište dostupno. U ovome primjeru RTT je manji, tj prosječno iznosi 23 milisekunde. To je zbog toga što smo uzeli odredište koje je bliže nama, pa je zbog toga i put koji pređe paket od nas do odredišta i nazad manji. To ćemo dodatno pokazati na sljedećem primjeru gdje ćemo „pingati“ početnu stranicu Fakulteta u Moskvi.

```
C:\Users\Petar>ping www.msu.ru

Pinging www.msu.ru [188.44.50.103] with 32 bytes of data:
Reply from 188.44.50.103: bytes=32 time=85ms TTL=50
Reply from 188.44.50.103: bytes=32 time=85ms TTL=50
Reply from 188.44.50.103: bytes=32 time=86ms TTL=50
Reply from 188.44.50.103: bytes=32 time=86ms TTL=50

Ping statistics for 188.44.50.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 85ms, Maximum = 86ms, Average = 85ms
```

Slika 22. „Pinganje“ početne stranice Fakulteta u Moskvi

icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	1.309495	192.168.1.3	188.44.50.103	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 3)
3	1.394673	188.44.50.103	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=50 (request in 2)
4	2.316165	192.168.1.3	188.44.50.103	ICMP	74	Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 5)
5	2.401464	188.44.50.103	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=65/16640, ttl=50 (request in 4)
6	3.321986	192.168.1.3	188.44.50.103	ICMP	74	Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (reply in 7)
7	3.408370	188.44.50.103	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=66/16896, ttl=50 (request in 6)
511	4.327018	192.168.1.3	188.44.50.103	ICMP	74	Echo (ping) request id=0x0001, seq=67/17152, ttl=128 (reply in 512)
512	4.413113	188.44.50.103	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=67/17152, ttl=50 (request in 511)

Slika 22. Filtrirani paketi za početnu stranicu Fakulteta u Moskvi

Prema slici 22. vidimo da je RTT skoro tri puta veći nego kada smo „pingali“ neko odredište u Hrvatskoj.

Za sljedeći primjer uzeli smo neku adresu da pokažemo šta se događa kada probamo pokušamo „pingati“ odredište koje nije dostupno.

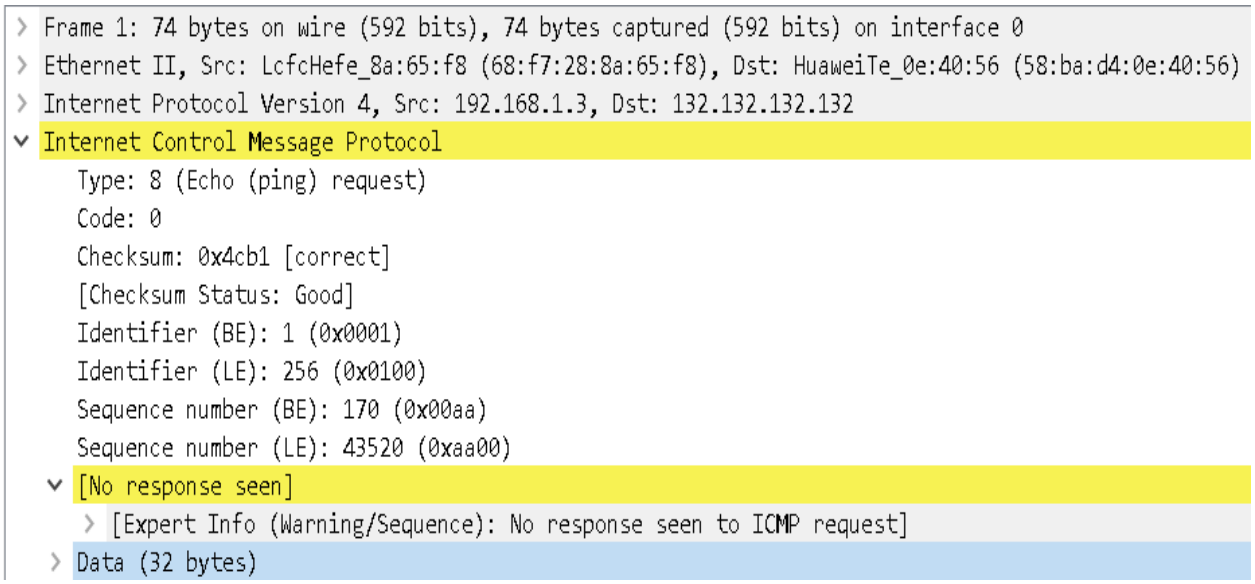
```
C:\Users\Petar>ping 132.132.132.132

Pinging 132.132.132.132 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 132.132.132.132:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Slika 23. „Pinganje“ nedostupnog odredišta

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	132.132.132.132	ICMP	74	Echo (ping) request id=0x0001, seq=170/43520, ttl=128 (no response found!)
9	4.796532	192.168.1.3	132.132.132.132	ICMP	74	Echo (ping) request id=0x0001, seq=171/43776, ttl=128 (no response found!)
10	9.796845	192.168.1.3	132.132.132.132	ICMP	74	Echo (ping) request id=0x0001, seq=172/44032, ttl=128 (no response found!)
18	14.797100	192.168.1.3	132.132.132.132	ICMP	74	Echo (ping) request id=0x0001, seq=173/44288, ttl=128 (no response found!)

Slika 24. Popis paketa kod nedostupnog odredišta



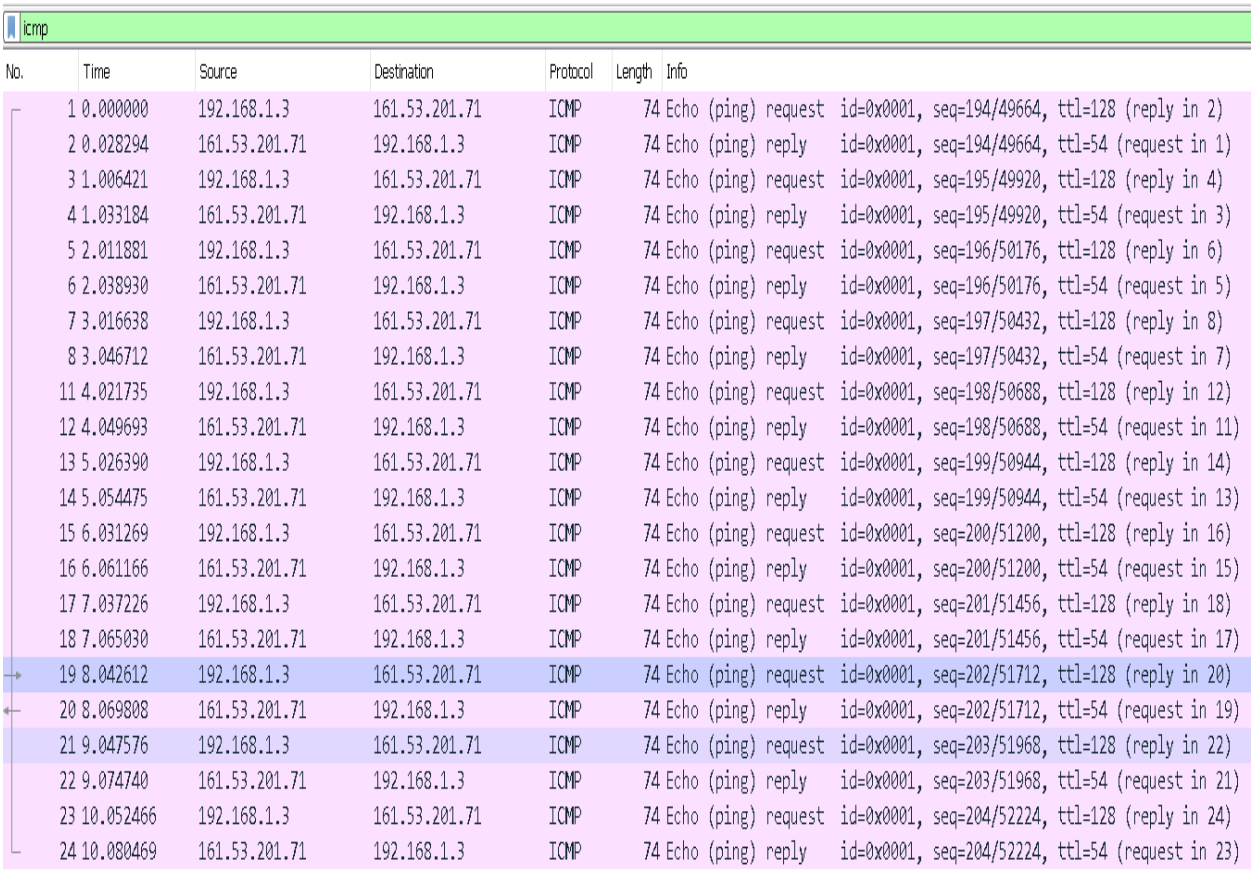
Slika 25. Detalji paketa

Prema slikama 23, 24 i 25 vidimo da smo poslali *Echo request* poruku, ali nismo dobili *Echo reply* poruku, te nam je ispisana poruka *„Request timed out.“*

Cmd nam nudi neke dodatne opcije uz naredbu *ping*. Jedna od opcija je „-t“ koji neprestano „pinga“ odredišno računalo dok mi, pomoću kombinacije tipki Ctrl i C ne zaustavimo „pinganje“. Također imamo opcije poput „[-n count]“ pomoću koje definiramo koliko puta želimo poslati *Echo request* poruku (zadani broj puta je 4), te [-w timeout] gdje definiramo, u milisekundama, koliki je istek vremena prije nego što se ispiše poruka *„Requested timed out“* (zadana vrijednost je 4000 milisekundi).

```
C:\Users\Petar>ping -t -w 2000 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=28ms TTL=54
Reply from 161.53.201.71: bytes=32 time=28ms TTL=54
Reply from 161.53.201.71: bytes=32 time=26ms TTL=54
Reply from 161.53.201.71: bytes=32 time=27ms TTL=54
Reply from 161.53.201.71: bytes=32 time=30ms TTL=54
Reply from 161.53.201.71: bytes=32 time=28ms TTL=54
Reply from 161.53.201.71: bytes=32 time=28ms TTL=54
Reply from 161.53.201.71: bytes=32 time=29ms TTL=54
Reply from 161.53.201.71: bytes=32 time=27ms TTL=54
Reply from 161.53.201.71: bytes=32 time=27ms TTL=54
Reply from 161.53.201.71: bytes=32 time=27ms TTL=54
Reply from 161.53.201.71: bytes=32 time=28ms TTL=54

Ping statistics for 161.53.201.71:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 30ms, Average = 27ms
Control-C
^C
```

Slika 26. „Pinganje“ pomoću dodatnih opcija



icmp

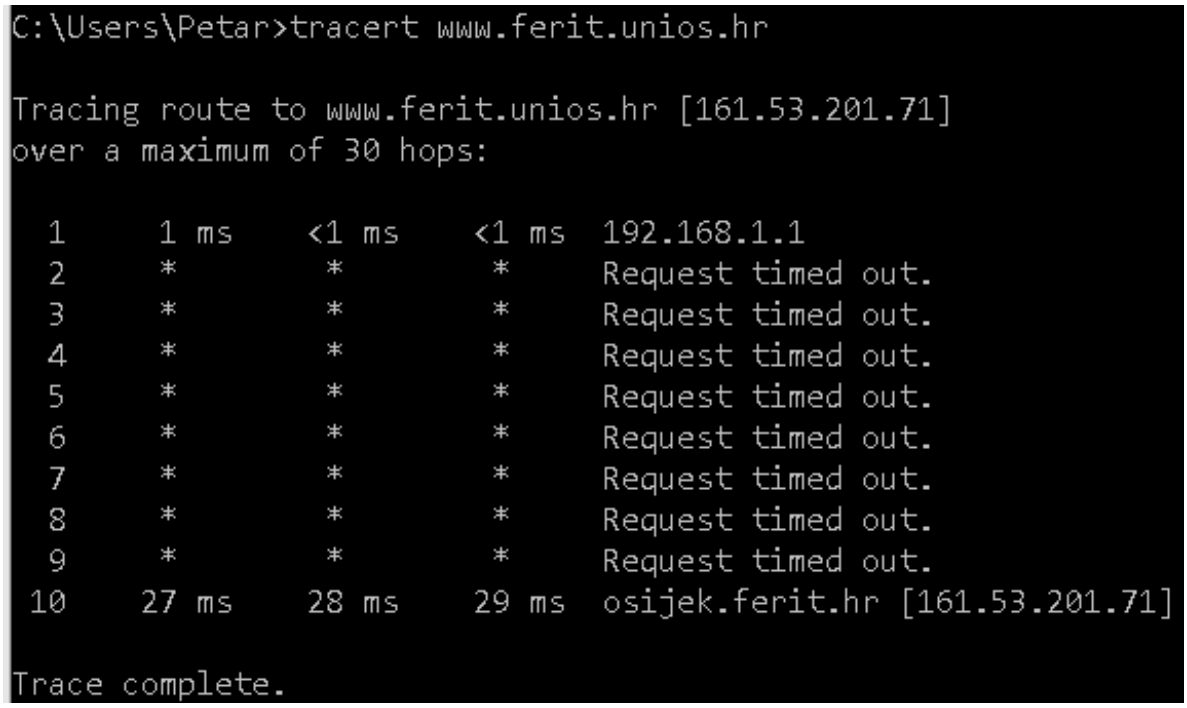
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=194/49664, ttl=128 (reply in 2)
2	0.028294	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=194/49664, ttl=54 (request in 1)
3	1.006421	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=195/49920, ttl=128 (reply in 4)
4	1.033184	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=195/49920, ttl=54 (request in 3)
5	2.011881	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=196/50176, ttl=128 (reply in 6)
6	2.038930	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=196/50176, ttl=54 (request in 5)
7	3.016638	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=197/50432, ttl=128 (reply in 8)
8	3.046712	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=197/50432, ttl=54 (request in 7)
11	4.021735	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=198/50688, ttl=128 (reply in 12)
12	4.049693	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=198/50688, ttl=54 (request in 11)
13	5.026390	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=199/50944, ttl=128 (reply in 14)
14	5.054475	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=199/50944, ttl=54 (request in 13)
15	6.031269	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=200/51200, ttl=128 (reply in 16)
16	6.061166	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=200/51200, ttl=54 (request in 15)
17	7.037226	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=201/51456, ttl=128 (reply in 18)
18	7.065030	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=201/51456, ttl=54 (request in 17)
19	8.042612	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=202/51712, ttl=128 (reply in 20)
20	8.069808	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=202/51712, ttl=54 (request in 19)
21	9.047576	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=203/51968, ttl=128 (reply in 22)
22	9.074740	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=203/51968, ttl=54 (request in 21)
23	10.052466	192.168.1.3	161.53.201.71	ICMP	74	Echo (ping) request id=0x0001, seq=204/52224, ttl=128 (reply in 24)
24	10.080469	161.53.201.71	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=204/52224, ttl=54 (request in 23)

Slika 27. Ispis svih ICMP paketa

U ovome primjeru smo uzeli dvije dodatne opcije, da „pingamo“ početnu stranicu FERIT-a dok ne zaustavimo to „pinganje“ i da istek vremena za odziv bude 2 sekunde. Ova opcija nam je korisna ako imamo neko udaljeno računalo koje kontroliramo od kuće i na njemu instaliramo neke zakrpe ili ažuriranja koja zahtijevaju ponovo pokretanje računala, pa pomoću naredbe *ping* možemo pratiti kada se računalo ponovo pokrene.

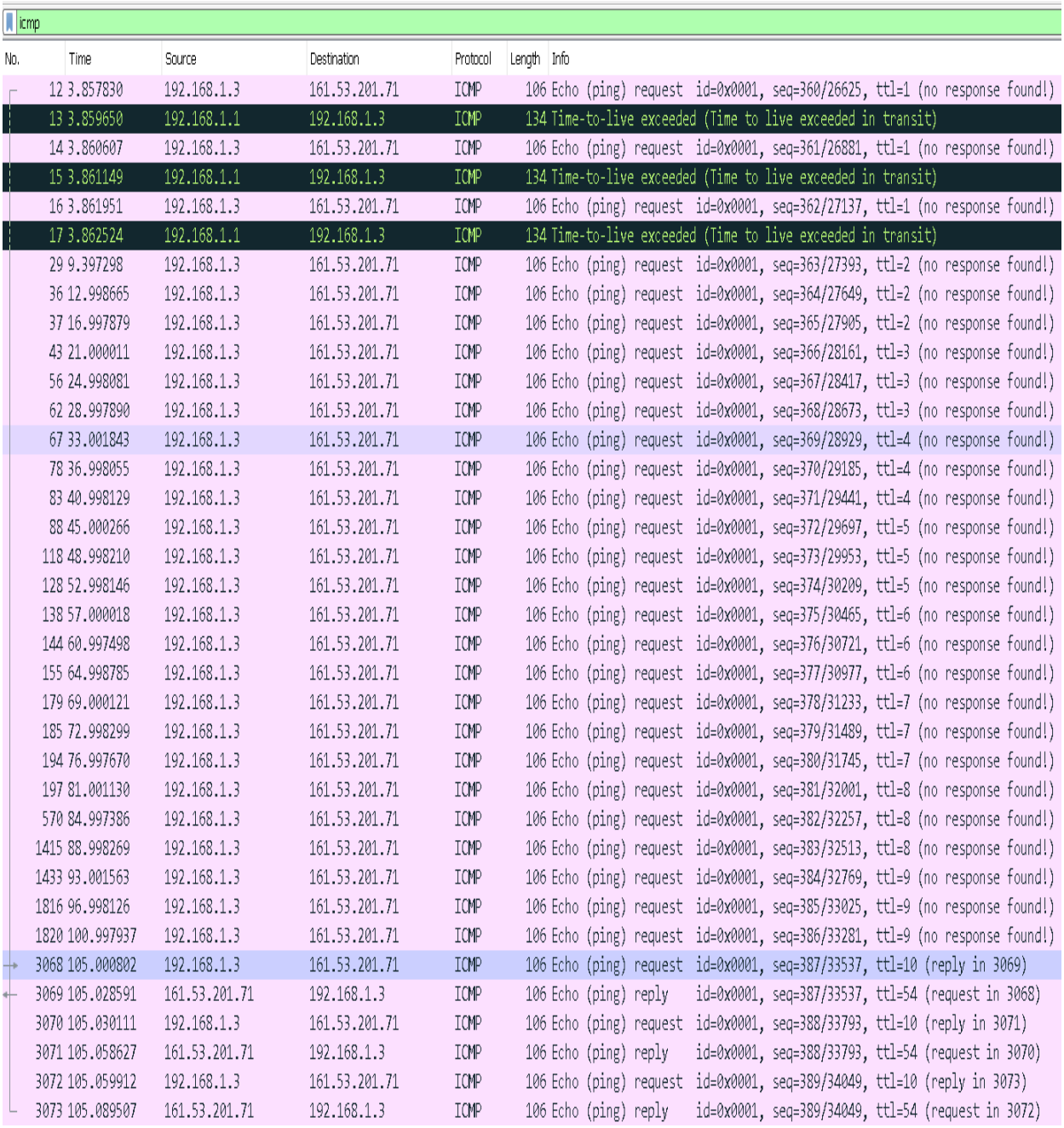
4.5. Analiza *traceroute* naredbe pomoću programa Wireshark

Traceroute, kao što smo naveli, nam omogućava da vidimo koliko usmjerivača ima između odredišta i izvorišta. U ovome primjeru ćemo pokušati to pokazati sa početnom stranicom FERIT-a. Naredba *traceroute* se koristi, isto kao i *ping* naredba, preko cmd-a na sljedeći način: tracert www.ferit.unios.hr



Slika 28. *Traceroute* početne stranice FERIT-a preko cmd-a

Prema slici 28 vidimo da ima od našeg računala do odredišnog računala ima 10 „skokova“. Prvi skok je naš usmjerivač. Ostali usmjerivači nisu odgovorili u određenom vremenu na poruku *Echo request*, pa je ispisana poruka *„Request timed out“*. Moguće je da su ti usmjerivači postavili vatrozid koji izbacuje ICMP pakete iz mreže zato što puno napada uskraćivanjem resursa dolazi baš preko ICMP paketa. Jedino možemo vidjeti završni usmjerivač, njegovu IP adresu (161.53.201.71), ime hosta (osijek.ferit.hr) i RTT (27 milisekundi, 28 milisekundi i 29 milisekundi) .

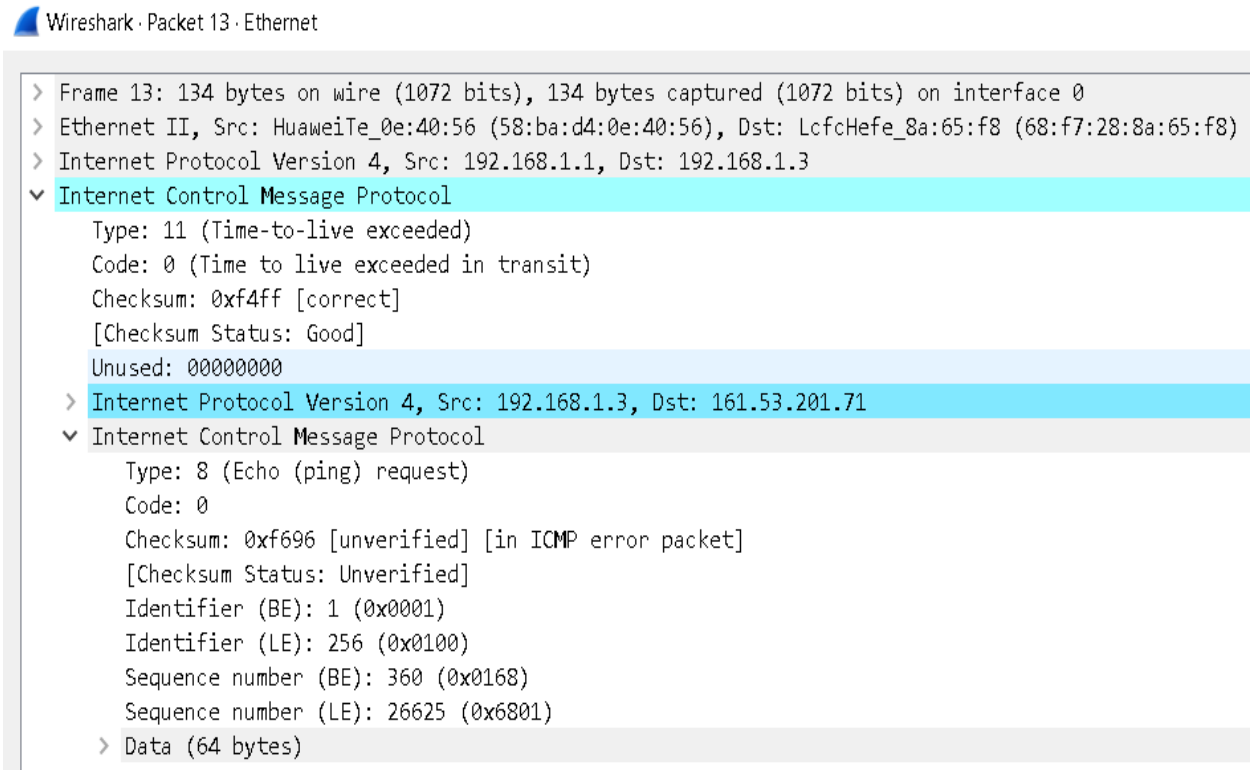


icmp

No.	Time	Source	Destination	Protocol	Length	Info
12	3.857830	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=360/26625, ttl=1 (no response found!)
13	3.859650	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
14	3.860607	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=361/26881, ttl=1 (no response found!)
15	3.861149	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
16	3.861951	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=362/27137, ttl=1 (no response found!)
17	3.862524	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
29	9.397298	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=363/27393, ttl=2 (no response found!)
36	12.998665	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=364/27649, ttl=2 (no response found!)
37	16.997879	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=365/27905, ttl=2 (no response found!)
43	21.000011	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=366/28161, ttl=3 (no response found!)
56	24.998081	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=367/28417, ttl=3 (no response found!)
62	28.997890	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=368/28673, ttl=3 (no response found!)
67	33.001843	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=369/28929, ttl=4 (no response found!)
78	36.998055	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=370/29185, ttl=4 (no response found!)
83	40.998129	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=371/29441, ttl=4 (no response found!)
88	45.000266	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=372/29697, ttl=5 (no response found!)
118	48.998210	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=373/29953, ttl=5 (no response found!)
128	52.998146	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=374/30209, ttl=5 (no response found!)
138	57.000018	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=375/30465, ttl=6 (no response found!)
144	60.997498	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=376/30721, ttl=6 (no response found!)
155	64.998785	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=377/30977, ttl=6 (no response found!)
179	69.000121	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=378/31233, ttl=7 (no response found!)
185	72.998299	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=379/31489, ttl=7 (no response found!)
194	76.997670	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=380/31745, ttl=7 (no response found!)
197	81.001130	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=381/32001, ttl=8 (no response found!)
570	84.997386	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=382/32257, ttl=8 (no response found!)
1415	88.998269	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=383/32513, ttl=8 (no response found!)
1433	93.001563	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=384/32769, ttl=9 (no response found!)
1816	96.998126	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=385/33025, ttl=9 (no response found!)
1820	100.997937	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=386/33281, ttl=9 (no response found!)
3068	105.000802	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=387/33537, ttl=10 (reply in 3069)
3069	105.028591	161.53.201.71	192.168.1.3	ICMP	106	Echo (ping) reply id=0x0001, seq=387/33537, ttl=54 (request in 3068)
3070	105.030111	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=388/33793, ttl=10 (reply in 3071)
3071	105.058627	161.53.201.71	192.168.1.3	ICMP	106	Echo (ping) reply id=0x0001, seq=388/33793, ttl=54 (request in 3070)
3072	105.059912	192.168.1.3	161.53.201.71	ICMP	106	Echo (ping) request id=0x0001, seq=389/34049, ttl=10 (reply in 3073)
3073	105.089507	161.53.201.71	192.168.1.3	ICMP	106	Echo (ping) reply id=0x0001, seq=389/34049, ttl=54 (request in 3072)

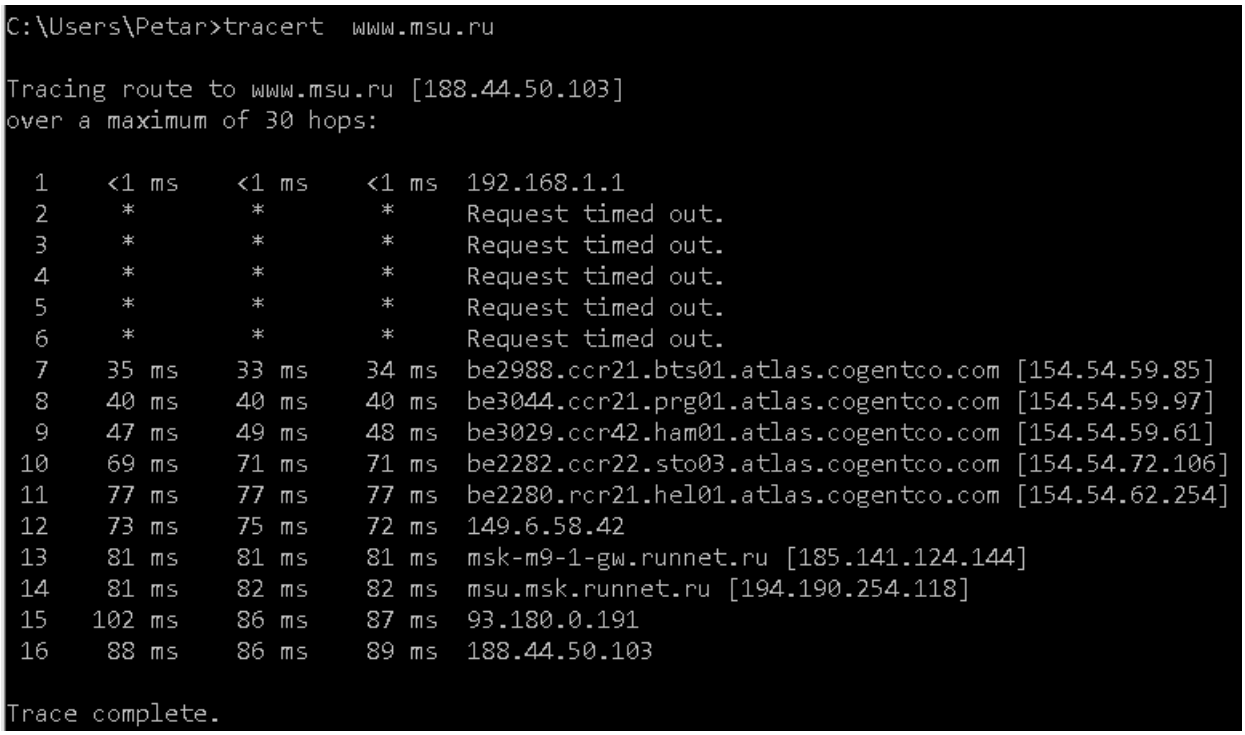
Slika 29. Popis svih ICMP paketa tijekom izvođenja *traceroute* naredbe do početne stranice FERIT-a

Na slici 29 vidimo sve ICMP pakete koje smo snimili tijekom izvođenja *traceroute* naredbe. Prvo se šalje paket s porukom *Echo request* s TTL = 1. Kada taj paket dođe do prvog usmjerivača, što je u ovome slučaju naš usmjerivač, TTL se smanji na 0, paket se izbacuje iz mreže i usmjerivač (192.168.1.1) šalje nazad na izvor (192.168.1.3) ICMP poruku *Time exceeded*. Preko ove poruke smo saznali koji je prvi usmjerivač na putu do odredišta i njegovu IP adresu. *Traceroute* uvijek šalje 3 *Echo request* poruke.



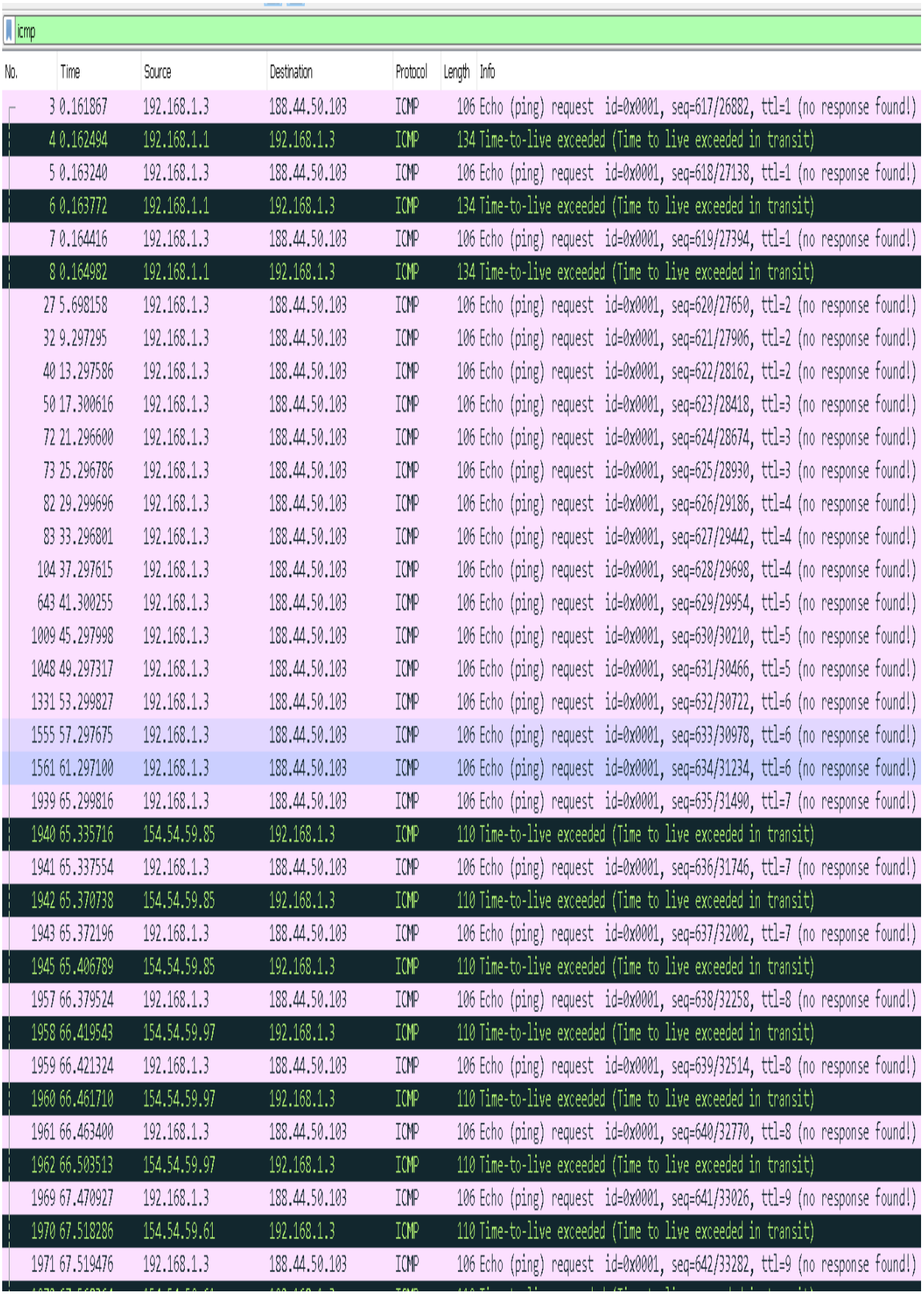
Slika 30. Izgled snimljene *Time Exceeded* poruke

Prema slici 30 vidimo da je polje *Type* postavljeno na 11, kao što smo naveli u poglavlju 3.3. Polje *Code* je postavljeno na 0 i to nam označava da se TTL smanjio na 0 tijekom prijenosa. Izvoru se šalje IP zaglavlje i prvih 8 bajtova originalnog datagrama.
Svaka sljedeća tri paketa imaju TTL uvećan za jedan, ali ne vidimo kroz koje usmjerivače su prošli, pa ne vidimo ni njihove IP adrese, niti dobivamo nazad ICMP poruku *Time exceeded*. Tek kod paketa kojem je TTL postavljen na 10 dolazimo do našeg odredišta, ali tada se taj paket ne izbacuje iz mreže, niti se šalje ICMP poruka *Time exceeded*, nego se šalje ICMP poruka *Echo reply*, zato što smo došli do našeg odredišta od kojeg smo zahtijevali odgovor.
U sljedećem primjeru ćemo uzeti početnu stranicu Fakulteta u Moskvi kao odredište.



Slika 31. Traceroute početne stranice Fakulteta u Moskvi preko cmd-a

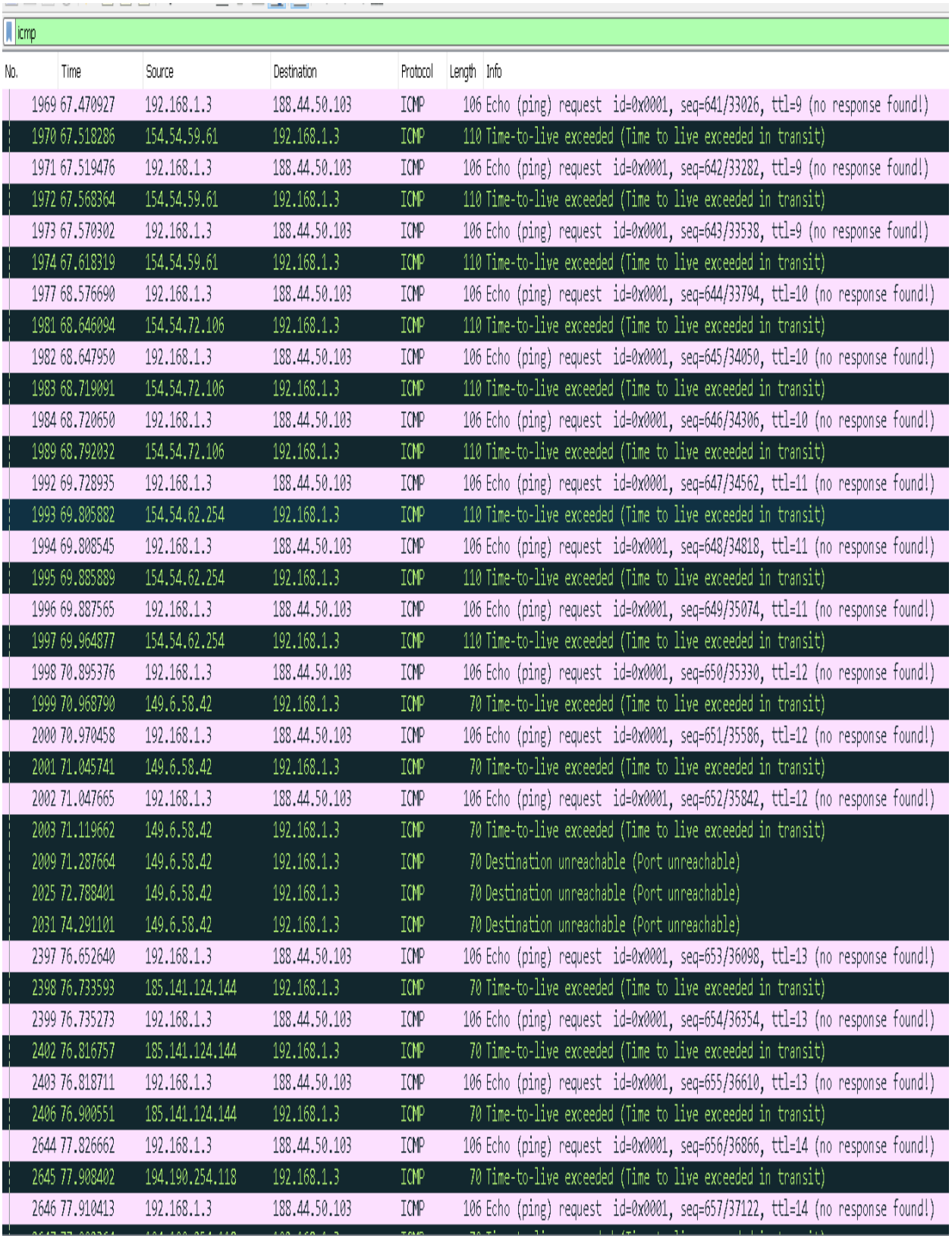
Prema slici 31 vidimo da do odredišta imamo 16 „skokova“. Prvi usmjerivač na putu je ,kao i u prošlom primjeru, naš usmjerivač. Sljedećih 5 usmjerivača su nedostupni. Nakon toga dolazimo do 5 sljedećih usmjerivača koji su pod vlasništvom Cogent Communications. Cogent Communications je jedan od najvećih ISP-ova (*„Internet Service Provider“*) u svijetu. To znači da je početna stranica Fakulteta u Moskvi koristi Cogent Communications kao svog davatelja internetskih usluga. Na 13. i 14. usmjerivaču dolazimo do ruske internetske domene. Također možemo vidjeti da se svakim daljnjim usmjerivačem povećava RTT., što znači da idemo sve dalje od izvora.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
3	0.161867	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=617/26882, ttl=1 (no response found!)
4	0.162494	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
5	0.163240	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=618/27138, ttl=1 (no response found!)
6	0.163772	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
7	0.164416	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=619/27394, ttl=1 (no response found!)
8	0.164982	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
27	5.698158	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=620/27650, ttl=2 (no response found!)
32	9.297295	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=621/27906, ttl=2 (no response found!)
40	13.297586	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=622/28162, ttl=2 (no response found!)
50	17.300616	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=623/28418, ttl=3 (no response found!)
72	21.296600	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=624/28674, ttl=3 (no response found!)
73	25.296786	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=625/28930, ttl=3 (no response found!)
82	29.299696	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=626/29186, ttl=4 (no response found!)
83	33.296801	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=627/29442, ttl=4 (no response found!)
104	37.297615	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=628/29698, ttl=4 (no response found!)
643	41.300255	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=629/29954, ttl=5 (no response found!)
1009	45.297998	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=630/30210, ttl=5 (no response found!)
1048	49.297317	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=631/30466, ttl=5 (no response found!)
1331	53.299827	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=632/30722, ttl=6 (no response found!)
1555	57.297675	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=633/30978, ttl=6 (no response found!)
1561	61.297100	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=634/31234, ttl=6 (no response found!)
1939	65.299816	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=635/31490, ttl=7 (no response found!)
1940	65.335716	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1941	65.337554	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=636/31746, ttl=7 (no response found!)
1942	65.370738	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1943	65.372196	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=637/32002, ttl=7 (no response found!)
1945	65.406789	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1957	66.379524	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=638/32258, ttl=8 (no response found!)
1958	66.419543	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1959	66.421324	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=639/32514, ttl=8 (no response found!)
1960	66.461710	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1961	66.463400	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=640/32770, ttl=8 (no response found!)
1962	66.503513	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1969	67.470927	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=641/33026, ttl=9 (no response found!)
1970	67.518286	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1971	67.519476	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=642/33282, ttl=9 (no response found!)

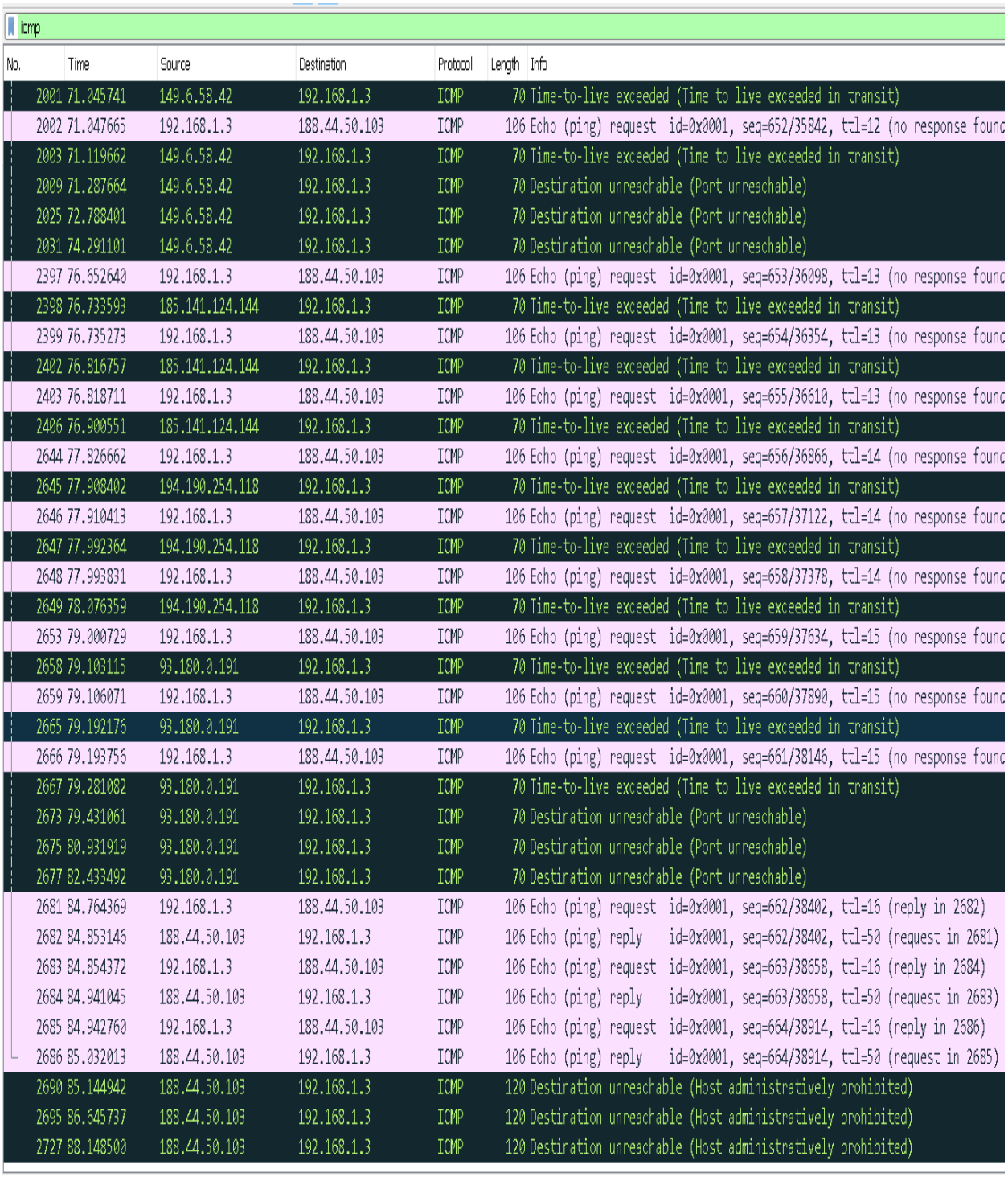
Slika 32. Popis svih ICMP paketa tijekom izvođenja *traceroute* naredbe do početne stranice Fakulteta u Moskvi



icmp

No.	Time	Source	Destination	Protocol	Length	Info
1969	67.470927	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=641/33026, ttl=9 (no response found!)
1970	67.518286	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1971	67.519476	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=642/33282, ttl=9 (no response found!)
1972	67.568364	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1973	67.570302	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=643/33538, ttl=9 (no response found!)
1974	67.618319	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1977	68.576690	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=644/33794, ttl=10 (no response found!)
1981	68.646094	154.54.72.106	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1982	68.647950	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=645/34050, ttl=10 (no response found!)
1983	68.719091	154.54.72.106	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1984	68.720650	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=646/34306, ttl=10 (no response found!)
1989	68.792032	154.54.72.106	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1992	69.728935	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=647/34562, ttl=11 (no response found!)
1993	69.805882	154.54.62.254	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1994	69.808545	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=648/34818, ttl=11 (no response found!)
1995	69.885889	154.54.62.254	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1996	69.887565	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=649/35074, ttl=11 (no response found!)
1997	69.964877	154.54.62.254	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1998	70.895376	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=650/35330, ttl=12 (no response found!)
1999	70.968790	149.6.58.42	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2000	70.970458	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=651/35586, ttl=12 (no response found!)
2001	71.045741	149.6.58.42	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2002	71.047665	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=652/35842, ttl=12 (no response found!)
2003	71.119662	149.6.58.42	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2009	71.287664	149.6.58.42	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2025	72.788401	149.6.58.42	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2031	74.291101	149.6.58.42	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2397	76.652640	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=653/36098, ttl=13 (no response found!)
2398	76.733593	185.141.124.144	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2399	76.735273	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=654/36354, ttl=13 (no response found!)
2402	76.816757	185.141.124.144	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2403	76.818711	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=655/36610, ttl=13 (no response found!)
2406	76.900551	185.141.124.144	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2644	77.826662	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=656/36866, ttl=14 (no response found!)
2645	77.908402	194.190.254.118	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2646	77.910413	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=657/37122, ttl=14 (no response found!)

Slika 33. Popis svih ICMP paketa tijekom izvođenja *traceroute* naredbe do početne stranice Fakulteta u Moskvi



icmp

No.	Time	Source	Destination	Protocol	Length	Info
2001	71.045741	149.6.58.42	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2002	71.047665	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=652/35842, ttl=12 (no response found
2003	71.119662	149.6.58.42	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2009	71.287664	149.6.58.42	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2025	72.788401	149.6.58.42	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2031	74.291101	149.6.58.42	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2397	76.652640	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=653/36098, ttl=13 (no response found
2398	76.733593	185.141.124.144	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2399	76.735273	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=654/36354, ttl=13 (no response found
2402	76.816757	185.141.124.144	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2403	76.818711	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=655/36610, ttl=13 (no response found
2406	76.900551	185.141.124.144	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2644	77.826662	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=656/36866, ttl=14 (no response found
2645	77.908402	194.190.254.118	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2646	77.910413	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=657/37122, ttl=14 (no response found
2647	77.992364	194.190.254.118	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2648	77.993831	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=658/37378, ttl=14 (no response found
2649	78.076359	194.190.254.118	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2653	79.000729	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=659/37634, ttl=15 (no response found
2658	79.103115	93.180.0.191	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2659	79.106071	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=660/37890, ttl=15 (no response found
2665	79.192176	93.180.0.191	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2666	79.193756	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=661/38146, ttl=15 (no response found
2667	79.281082	93.180.0.191	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2673	79.431061	93.180.0.191	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2675	80.931919	93.180.0.191	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2677	82.433492	93.180.0.191	192.168.1.3	ICMP	70	Destination unreachable (Port unreachable)
2681	84.764369	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=662/38402, ttl=16 (reply in 2682)
2682	84.853146	188.44.50.103	192.168.1.3	ICMP	106	Echo (ping) reply id=0x0001, seq=662/38402, ttl=50 (request in 2681)
2683	84.854372	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=663/38658, ttl=16 (reply in 2684)
2684	84.941045	188.44.50.103	192.168.1.3	ICMP	106	Echo (ping) reply id=0x0001, seq=663/38658, ttl=50 (request in 2683)
2685	84.942760	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=664/38914, ttl=16 (reply in 2686)
2686	85.032013	188.44.50.103	192.168.1.3	ICMP	106	Echo (ping) reply id=0x0001, seq=664/38914, ttl=50 (request in 2685)
2690	85.144942	188.44.50.103	192.168.1.3	ICMP	120	Destination unreachable (Host administratively prohibited)
2695	86.645737	188.44.50.103	192.168.1.3	ICMP	120	Destination unreachable (Host administratively prohibited)
2727	88.148500	188.44.50.103	192.168.1.3	ICMP	120	Destination unreachable (Host administratively prohibited)

Slika 34. Popis svih ICMP paketa tijekom izvođenja *traceroute* naredbe do početne stranice Fakulteta u Moskvi

Kao i prethodnom primjeru prvom ICMP paketu koji se poslao TTL polje je postavljeno na 1, i kada dođe do prvog usmjerivača paket se izbacuje iz mreže, te se šalje ICMP poruka *Time exceeded* nazad izvoru. Svaka 3 sljedeća zahtjeva TTL se poveća za 1. Od sljedećih 5 usmjerivača ne dobivamo ICMP poruku *Time exceeded*, pa zato nam na cmd-u ispisuje

poruku *„Request timed out“*. Na sljedećih 5 usmjerivača dobivamo ICMP poruku *Time exceeded*, a uz nju i IP adresu usmjerivača koji je poslao tu poruku, te njegov *„hostname“*. Na 12. „skoku“ također dobivamo od tog usmjerivača ICMP poruku *Destination unreachable* s poljem *Code* postavljeno na 3, što označava *Port unreachable*. Kada to usporedimo s ispisom na cmd-u vidimo da baš kod tog usmjerivača nismo dobili njegov *„hostname“*. To se isto dogodi na 15. i 16. „skoku“, gdje također nismo dobili *„hostname“* nego samo njegovu IP adresu. Završni, 16., usmjerivač, koji je naše odredište, šalje nazad izvoru *Echo reply* poruku i nakon toga naredba *traceroute* prestaje slati *Echo request* poruke i ispisuje nam da je pronašao put do traženog odredišta.

Kao i ping naredba, *traceroute* naredba dolazi s nekim dodatnim opcijama poput:

- -d : ispisuje samo IP adrese, bez imena računala
- [-m maximum_hops] : mi određujemo koliko „skokova“ ćemo napraviti prije nego što završimo (zadani broj skokova je 30)
- [-w timeout] : koliko milisekundi se čeka prije nego se pošalje sljedeći zahtjev

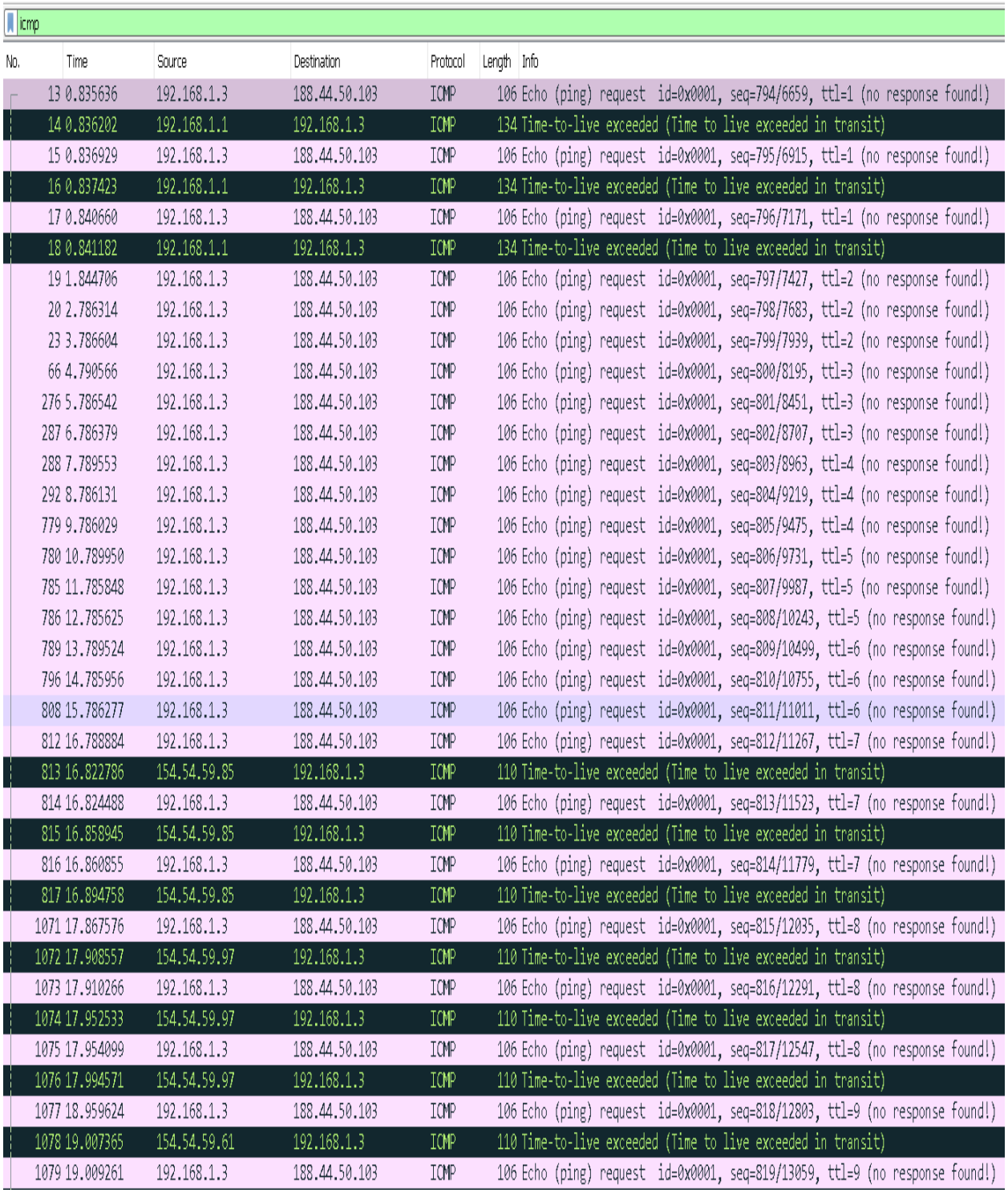
Pokazat ćemo, koristeći prošli primjer, kako se koriste navede opcije i koja je njihova uloga.

```
C:\Users\Petar>tracert -d -w 1000 -h 11 www.msu.ru

Tracing route to www.msu.ru [188.44.50.103]
over a maximum of 11 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    34 ms    34 ms    33 ms  154.54.59.85
  8    41 ms    42 ms    40 ms  154.54.59.97
  9    47 ms    48 ms    48 ms  154.54.59.61
 10    72 ms    70 ms    68 ms  154.54.72.106
 11    78 ms    76 ms    77 ms  154.54.62.254

Trace complete.
```

Slika 35. Dodatne opcije kod *traceroute* naredbe

Prema slici 35 vidimo da smo uključili 3 dodatne opcije. Ispisivat će se samo IP adrese, čeka se milisekunda prije sljedećeg zahtjeva i odradit će se 11 „skokova“. Ako usporedimo

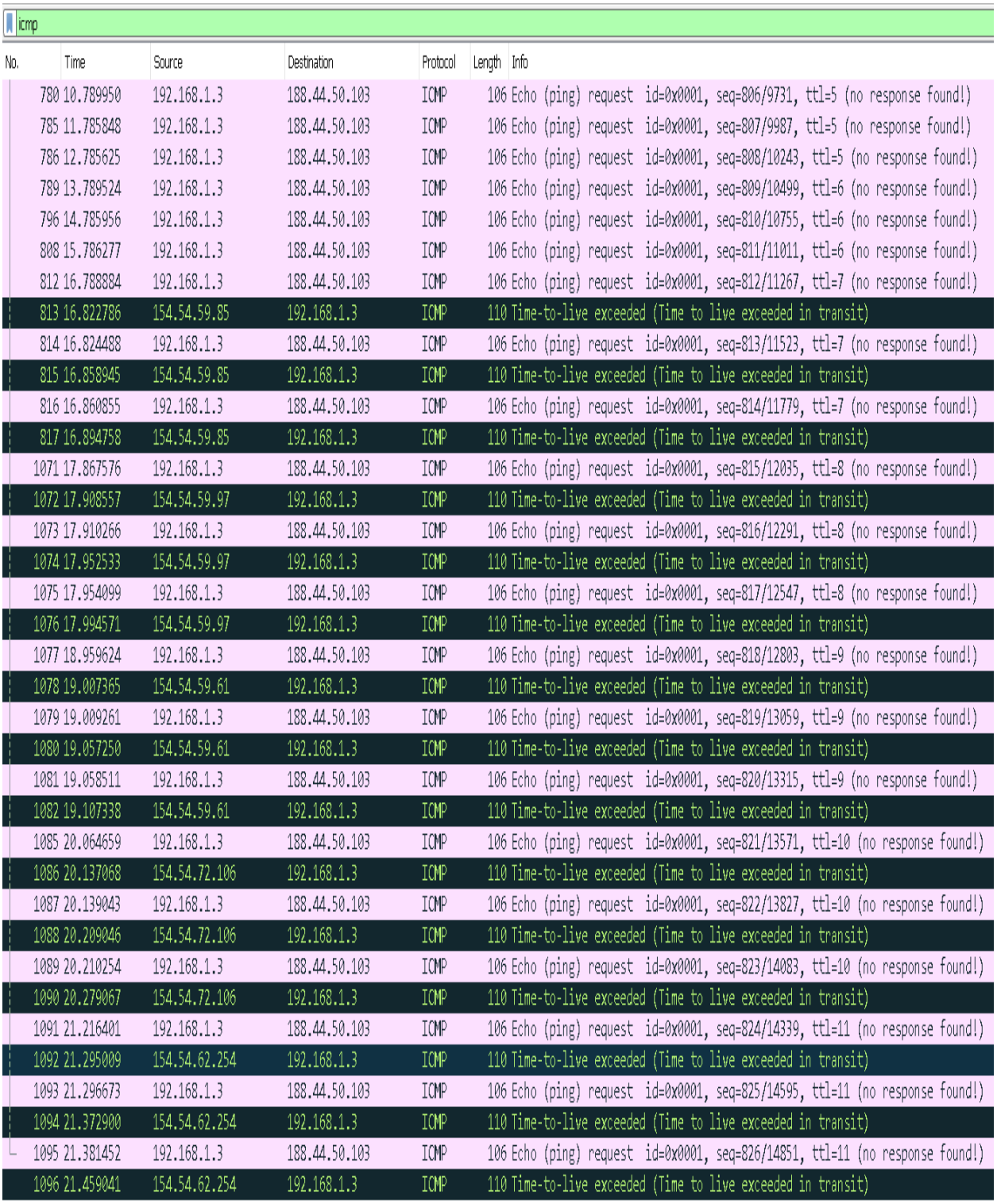
sliku 31 i 35 vidimo da nam nisu ispisana imena računala i da nakon 11 skoka završava praćenje.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
13	0.835636	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=794/6659, ttl=1 (no response found!)
14	0.836202	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
15	0.836929	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=795/6915, ttl=1 (no response found!)
16	0.837423	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
17	0.840660	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=796/7171, ttl=1 (no response found!)
18	0.841182	192.168.1.1	192.168.1.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19	1.844706	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=797/7427, ttl=2 (no response found!)
20	2.786314	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=798/7683, ttl=2 (no response found!)
23	3.786604	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=799/7939, ttl=2 (no response found!)
66	4.790566	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=800/8195, ttl=3 (no response found!)
276	5.786542	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=801/8451, ttl=3 (no response found!)
287	6.786379	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=802/8707, ttl=3 (no response found!)
288	7.789553	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=803/8963, ttl=4 (no response found!)
292	8.786131	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=804/9219, ttl=4 (no response found!)
779	9.786029	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=805/9475, ttl=4 (no response found!)
780	10.789950	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=806/9731, ttl=5 (no response found!)
785	11.785848	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=807/9987, ttl=5 (no response found!)
786	12.785625	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=808/10243, ttl=5 (no response found!)
789	13.789524	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=809/10499, ttl=6 (no response found!)
796	14.785956	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=810/10755, ttl=6 (no response found!)
808	15.786277	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=811/11011, ttl=6 (no response found!)
812	16.788884	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=812/11267, ttl=7 (no response found!)
813	16.822786	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
814	16.824488	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=813/11523, ttl=7 (no response found!)
815	16.858945	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
816	16.860855	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=814/11779, ttl=7 (no response found!)
817	16.894758	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1071	17.867576	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=815/12035, ttl=8 (no response found!)
1072	17.908557	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1073	17.910266	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=816/12291, ttl=8 (no response found!)
1074	17.952533	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1075	17.954099	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=817/12547, ttl=8 (no response found!)
1076	17.994571	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1077	18.959624	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=818/12803, ttl=9 (no response found!)
1078	19.007365	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1079	19.009261	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=819/13059, ttl=9 (no response found!)

Slika 36. ICMP paketi snimljeni tijekom izvršavanja *traceroute* naredbe s dodatnim opcijama



icmp

No.	Time	Source	Destination	Protocol	Length	Info
780	10.789950	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=806/9731, ttl=5 (no response found!)
785	11.785848	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=807/9987, ttl=5 (no response found!)
786	12.785625	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=808/10243, ttl=5 (no response found!)
789	13.789524	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=809/10499, ttl=6 (no response found!)
796	14.785956	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=810/10755, ttl=6 (no response found!)
808	15.786277	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=811/11011, ttl=6 (no response found!)
812	16.788884	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=812/11267, ttl=7 (no response found!)
813	16.822786	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
814	16.824488	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=813/11523, ttl=7 (no response found!)
815	16.858945	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
816	16.860855	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=814/11779, ttl=7 (no response found!)
817	16.894758	154.54.59.85	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1071	17.867576	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=815/12035, ttl=8 (no response found!)
1072	17.908557	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1073	17.910266	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=816/12291, ttl=8 (no response found!)
1074	17.952533	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1075	17.954099	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=817/12547, ttl=8 (no response found!)
1076	17.994571	154.54.59.97	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1077	18.959624	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=818/12803, ttl=9 (no response found!)
1078	19.007365	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1079	19.009261	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=819/13059, ttl=9 (no response found!)
1080	19.057250	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1081	19.058511	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=820/13315, ttl=9 (no response found!)
1082	19.107338	154.54.59.61	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1085	20.064659	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=821/13571, ttl=10 (no response found!)
1086	20.137068	154.54.72.106	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1087	20.139043	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=822/13827, ttl=10 (no response found!)
1088	20.209046	154.54.72.106	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1089	20.210254	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=823/14083, ttl=10 (no response found!)
1090	20.279067	154.54.72.106	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1091	21.216401	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=824/14339, ttl=11 (no response found!)
1092	21.295009	154.54.62.254	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1093	21.296673	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=825/14595, ttl=11 (no response found!)
1094	21.372900	154.54.62.254	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1095	21.381452	192.168.1.3	188.44.50.103	ICMP	106	Echo (ping) request id=0x0001, seq=826/14851, ttl=11 (no response found!)
1096	21.459041	154.54.62.254	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

Slika 37. ICMP paketi snimljeni tijekom izvršavanja *traceroute* naredbe s dodatnim opcijama

Ako usporedimo slike 36 i 37 sa slikama 31, 32 i 33 vidimo da je sve identično osim što slike 36 i 37 idu samo do 11 „skoka“ zbog opcija što smo napisali u cmd-u.

5. ZAKLJUČAK

Mrežni sloj se bavi prijenosom datagrama od jednog računala do drugog, a u tome mu uvelike pomaže ICMP protokol koji je implementiran u svaki IP modul. ICMP protokol šalje svoje poruke ukoliko je došlo do neke pogreške u prijenosu podataka, na primjer, ako nekom host-u ili usmjerivač-u nije moguće pristupiti, ili ako je neke datagrame moguće bližom rutom poslati do odredišta. Također, uz pomoć IP polja TTL koji se postavi na neku vrijednost, ICMP protokol pazi da neki datagram ne ostane beskonačno u nekoj petlji u mreži i ne troši mrežne resurse. ICMP protokol ne osigurava pouzdan prijenos kroz mrežu, nego samo šalje poruke ako dođe do greške. Uz navedeno, pomoću poruka koje šalje ICMP protokol, i naredbe *ping* moguće je saznati je li neko određeno računalo aktivno ili nije. Ako nas zanima put od našeg računala do nekog drugog, te svi usmjerivači na toj ruti, uz pomoć naredbe *traceroute* i ICMP poruka saznajemo te informacije.

6. LITERATURA

[1] **MREŽNI SLOJ, NETWORK LAYER**, http://spvp.zesoi.fer.hr/seminari/2000/internet/network_layer/routing_algoritmi/mrezni.htm

[2] List of network protocols (OSI model), Wikipedia, https://en.wikipedia.org/wiki/List_of_network_protocols_(OSI_model)

[3] J. Postel RFC 792, ISI, September 1981, https://tools.ietf.org/html/rfc792#ref-1

[4] ICMP protokol, http://mreze.layer-x.com/s030300-0.html

[5] RFC Sourcebook, IMCP, Internet Control Message Protocol http://www.networksorcery.com/enp/protocol/icmp.htm#Type

[6] Time to live, Wikipedia, https://en.wikipedia.org/wiki/Time_to_live

[7] Internet Control Message Protocol, Wikipedia, https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

[8] Ping, Wikipedia, https://en.wikipedia.org/wiki/Ping_(networking_utility)

[9] UNIT V Network Layer, http://www.eenadupratibha.net/pratibha/engineering/content_three_net_layer_u5.html

[10] TENET TECHNO, ICMP https://internettechnologyyooo.wordpress.com/icmp/

[11] Traceroute, Wikipedia, https://en.wikipedia.org/wiki/Traceroute

SAŽETAK: ICMP protokol i primjeri njegove primjene

Završni rad se bavi ICMP protokolom, njegovim primjenama i primjerima tih primjena. Na početku rada objašnjena je osnovna funkcija protokola te njegova pozicija u OSI referentom sustavu. Objašnjena je njegova povezanost s IP protokolom. Nakon toga su detaljnije proučene i opisane ICMP poruke. Napisana je njihova podjela, te nakon toga je svaka poruka pojedinačno opisana, te prikazan njezin izgled. Nakon toga su prikazane 2 primjene (*ping* i *traceroute*) koje su moguće uz pomoć ICMP protokola kroz par primjera za svaku primjenu.

Ključne riječi: ICMP, IP, ping, traceroute

Abstract: ICMP protocol and examples of its applications

This paper deals with ICMP protocol, his applications, and examples of its applications. The basic function of ICMP protocol and its position in the OSI reference system are explained in the beginning of the paper. Its connection to the IP protocol is explained. Then, the ICMP messages were studied and descibed in more detail. A subdivision is written, after which each message is individually described and its appearance is displayed. After that, 2 applications (ping and traceroute) that are possible using the ICMP protocol are shown through a couple of examples for each application.

Keywords: ICMP, IP, ping, traceroute

ŽIVOTOPIS

Petar Markov rođen je 28. listopada 1996. godine u Slavonskom Brodu. Završava Osnovnu školu Dragutin Tadijanović u Slavonskom Brodu, te se upisuje u Opću Gimnaziju Matija Mesić, opći smjer. Upisuje Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek 2015./2016. godine, stručni studij Informatika.