CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-10
Wireshark Lab: ICMP
March 24, 2025

Chidurala Tejaswini
(220010012/CS22BT012)

Introduction

In this lab, we'll explore several aspects of the ICMP protocol:

- ICMP messages generated by the Ping program;
- ICMP messages generated by the Traceroute program;

Part 0: Paste a screenshot of your system IP address, using ipconfig (on Windows) or ifconfig (on Mac and Linux), and fill out this Google form to submit the details of your system. The same system must be used to attempt all exercises of this lab.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.240.118.97  netmask 255.255.248.0  broadcast 10.240.119.255
        inet6 fe80::1d6b:1bfb:2bd6:ef0d  prefixlen 64  scopeid 0x20<link>
        ether e0:73:e7:0a:99:9a  txqueuelen 1000  (Ethernet)
        RX packets 42435  bytes 50116506 (50.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17089  bytes 3877647 (3.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x80900000-80920000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 980  bytes 90486 (90.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 980  bytes 90486 (90.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Part-1: ICMP and Ping

Let's begin our ICMP adventure by capturing the packets generated by the Ping program. You may recall that the Ping program is a simple tool that allows anyone (for example, a network administrator) to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. As you might have guessed (given that this lab is about ICMP), both of these Ping packets are ICMP packets

Do the following:

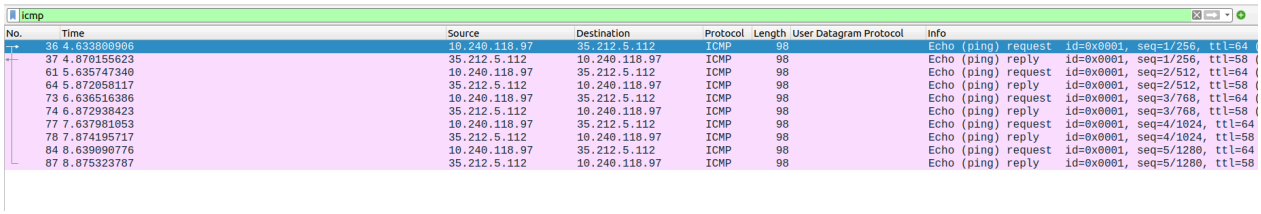
`For ubuntu: ping -c 5 wireshark.com`

`For Windows: ping -n 5 wireshark.com`

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ping -c 5 wireshark.com
PING wireshark.com (35.212.5.112) 56(84) bytes of data.
64 bytes from 112.5.212.35.bc.googleusercontent.com (35.212.5.112): icmp_seq=1 ttl=58 time=236 ms
64 bytes from 112.5.212.35.bc.googleusercontent.com (35.212.5.112): icmp_seq=2 ttl=58 time=236 ms
64 bytes from 112.5.212.35.bc.googleusercontent.com (35.212.5.112): icmp_seq=3 ttl=58 time=236 ms
64 bytes from 112.5.212.35.bc.googleusercontent.com (35.212.5.112): icmp_seq=4 ttl=58 time=236 ms
64 bytes from 112.5.212.35.bc.googleusercontent.com (35.212.5.112): icmp_seq=5 ttl=58 time=236 ms

--- wireshark.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 236.250/236.337/236.457/0.075 ms
```

1. **How many ping requests and replies do you observe for the ping command?**

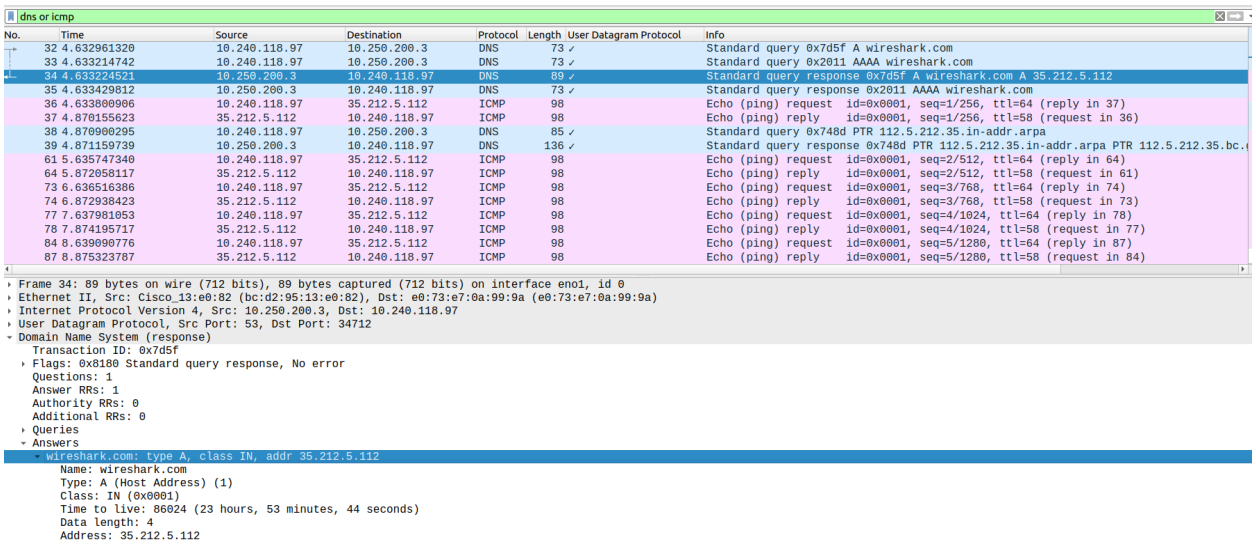


icmp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
36	4.633800906	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=1/256, ttl=64
37	4.870155623	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=1/256, ttl=58
61	5.635747340	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=2/512, ttl=64
64	5.872058117	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=2/512, ttl=58
73	6.636516386	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=3/768, ttl=64
74	6.872938423	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=3/768, ttl=58
77	7.637981053	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=4/1024, ttl=64
78	7.874195717	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=4/1024, ttl=58
84	8.639090776	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=5/1280, ttl=64
87	8.875323787	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=5/1280, ttl=58

- **Ping requests:** 5 (Frame numbers: 36, 61, 73, 77,84)
- **Ping replies:** 5 (Frame numbers: 37, 64, 74, 78, 87)

2. **What is the destination IP address in the ping request packets, specify the domain name associated with this IP address.**



dns or icmp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
32	4.632961320	10.240.118.97	10.250.200.3	DNS	73	✓	Standard query 0x7d5f A wireshark.com
33	4.633214742	10.240.118.97	10.250.200.3	DNS	73	✓	Standard query 0x2011 AAAA wireshark.com
34	4.633224521	10.250.200.3	10.240.118.97	DNS	89	✓	Standard query response 0x7d5f A wireshark.com A 35.212.5.112
35	4.633429812	10.250.200.3	10.240.118.97	DNS	73	✓	Standard query response 0x2011 AAAA wireshark.com
36	4.633800906	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 37)
37	4.870155623	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=1/256, ttl=58 (request in 36)
38	4.870900295	10.240.118.97	10.250.200.3	DNS	85	✓	Standard query 0x748d PTR 112.5.212.35.in-addr.arpa
39	4.871159739	10.250.200.3	10.240.118.97	DNS	136	✓	Standard query response 0x748d PTR 112.5.212.35.in-addr.arpa PTR 112.5.212.35.bc.
61	5.635747340	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 64)
64	5.872058117	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=2/512, ttl=58 (request in 61)
73	6.636516386	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 74)
74	6.872938423	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=3/768, ttl=58 (request in 73)
77	7.637981053	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 78)
78	7.874195717	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=4/1024, ttl=58 (request in 77)
84	8.639090776	10.240.118.97	35.212.5.112	ICMP	98		Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 87)
87	8.875323787	35.212.5.112	10.240.118.97	ICMP	98		Echo (ping) reply id=0x0001, seq=5/1280, ttl=58 (request in 84)

```
▸ Frame 34: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface eno1, id 0
▸ Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: e0:73:e7:0a:99:9a (e0:73:e7:0a:99:9a)
▸ Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.118.97
▸ User Datagram Protocol, Src Port: 53, Dst Port: 34712
▾ Domain Name System (response)
    Transaction ID: 0x7d5f
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▾ wireshark.com: type A, class IN, addr 35.212.5.112
        Name: wireshark.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 86024 (23 hours, 53 minutes, 44 seconds)
        Data length: 4
        Address: 35.212.5.112
```

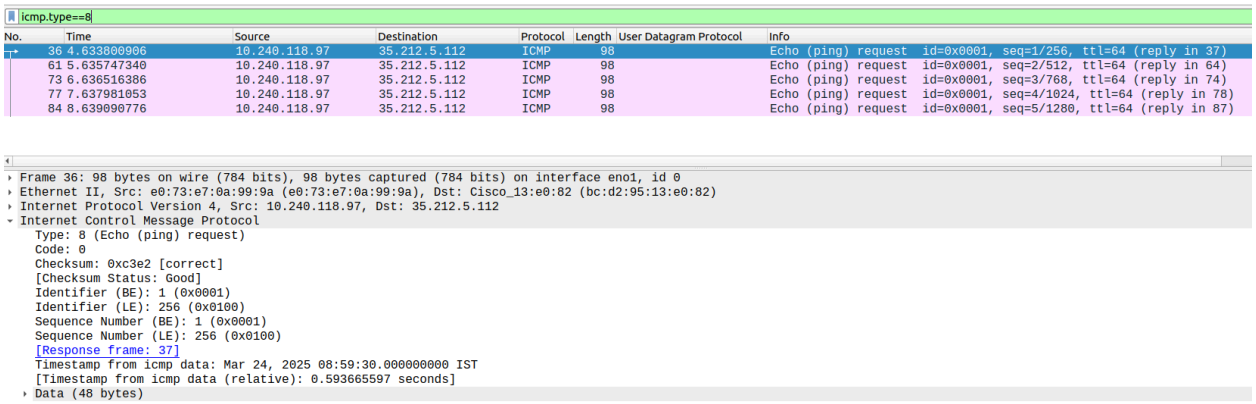
- **Destination IP address:** `35.212.5.112`
- **Domain name associated with this IP :** `wireshark.com`

3. **Examine the sequence number field in the ICMP Echo Request packets. How does it change for each packet?**

We can see in the image that the sequence number in ICMP Echo Request packets follows a pattern where 1 (BE) corresponds to 256 (LE), 2 (BE) corresponds to 512 (LE), and so on. This happens due to the difference in Big Endian (BE) and Little Endian (LE) representations of the sequence number field.We can observe seq=1/256 for example where 1 corresponds to BE and 256 corresponds to LE.

Explanation of BE and LE Representation:

1. Big Endian (BE) stores the most significant byte first, following a natural increasing order (1, 2, 3, 4,...).
2. Little Endian (LE) stores the least significant byte first, causing the value to appear differently (256, 512, 768, 1024,...).



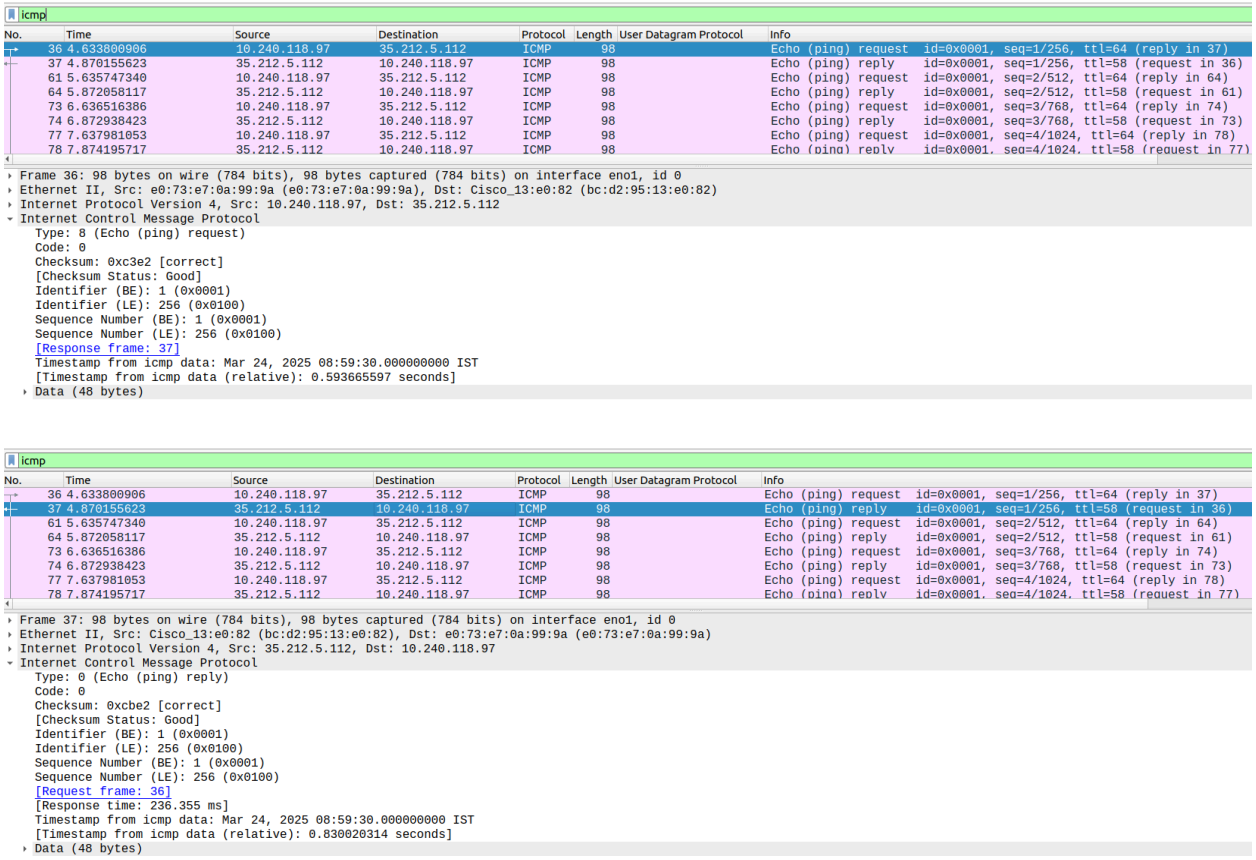
Frame No	Type	Sequence Number (BE) in decimal	Sequence Number (Hex)	Sequence Number (LE) in decimal	Sequence Number(Hex)
36	Echo (ping) request	**1**	0x0001	**256**	0x0100
61	Echo (ping) request	**2**	0x0002	**512**	0x0200
73	Echo (ping) request	**3**	0x0003	**768**	0x0300
77	Echo (ping) request	**4**	0x0004	**1024**	0x0400
84	Echo (ping) request	**5**	0x0005	**1280**	0x0500

The BE sequence number increases by 1 for each ICMP Echo Request. The LE sequence number increases in steps of 256 due to the byte-swapping effect.

4. **How many different types of echo ping do you observe in the trace?**
   In an ICMP echo trace, there are **two types of ICMP messages**:

   - ICMP Echo (ping) Request (Type = 8)
   - ICMP Echo (ping) Reply (Type = 0)

5. **Provide the field name(s) and the value that remains unchanged in the ICMP ping request and replies.**



- Code:0
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256(0x0100)
- Sequence Number(BE): 1(0x0001)
- Sequence Number(LE): 256(0x0100)
- Data(48 bytes)
- [CheckSum Status: Good]

Part-2: Traceroute on `ambergroupindia.com`

```
traceroute -m 15 ambergroupindia.com
```

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ traceroute -m 15 ambergroupindia.com
traceroute to ambergroupindia.com (220.158.165.21), 15 hops max, 60 byte packets
 1  10.240.118.1 (10.240.118.1)  0.425 ms  0.389 ms  0.373 ms
 2  internet.iitdh.ac.in (10.240.240.1)  0.699 ms  0.680 ms  0.665 ms
 3  117.205.73.161 (117.205.73.161)  2.179 ms  2.101 ms  2.283 ms
 4  117.216.207.216 (117.216.207.216)  8.376 ms  8.452 ms  8.346 ms
 5  * * *
 6  49.44.218.92 (49.44.218.92)  31.245 ms  31.439 ms  31.205 ms
 7  * * *
 8  * * *
 9  49.44.220.189 (49.44.220.189)  43.495 ms  43.817 ms  43.769 ms
10  182.79.134.249 (182.79.134.249)  45.354 ms  47.878 ms  45.901 ms
11  aes-static-146.133.22.125.airtel.in (125.22.133.146)  47.828 ms  49.156 ms  45.856 ms
12  103.43.33.2 (103.43.33.2)  52.180 ms  51.418 ms  51.402 ms
13  103.221.208.18 (103.221.208.18)  49.082 ms  49.065 ms  46.366 ms
14  cp165021.spectraidc.net (220.158.165.21)  52.086 ms  52.071 ms  49.268 ms
```

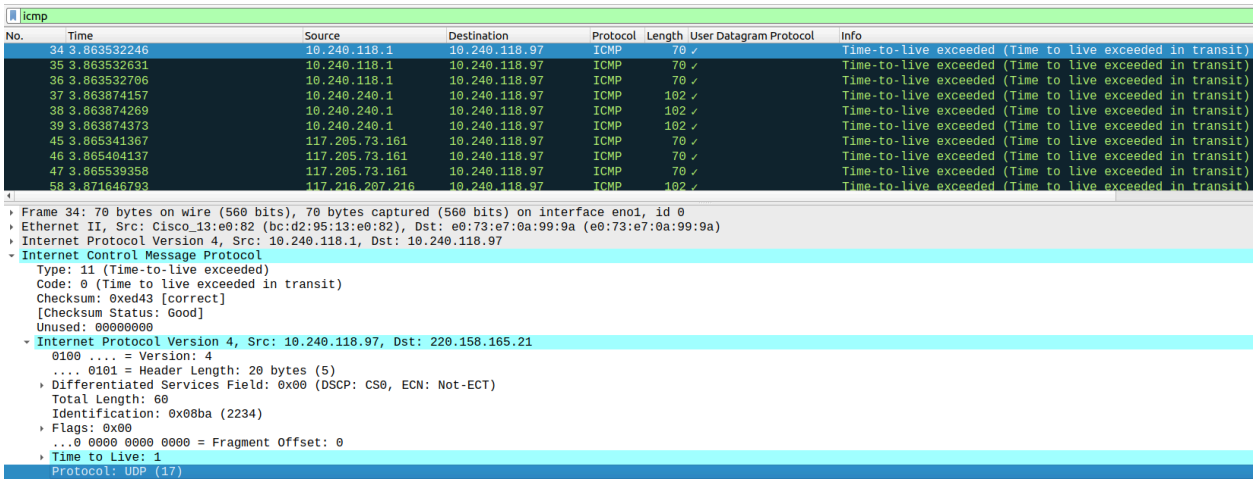
icmp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
34	3.863532246	10.240.118.1	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
35	3.863532631	10.240.118.1	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
36	3.863532706	10.240.118.1	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
37	3.863874157	10.240.240.1	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
38	3.863874269	10.240.240.1	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
39	3.863874373	10.240.240.1	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
45	3.865341367	117.205.73.161	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
46	3.865404137	117.205.73.161	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
47	3.865539358	117.205.73.161	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
58	3.871646793	117.216.207.216	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
59	3.871646987	117.216.207.216	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
60	3.871738061	117.216.207.216	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
62	3.894610466	49.44.218.92	10.240.118.97	ICMP	110	✓	Time-to-live exceeded (Time to live exceeded in transit)
63	3.896158667	49.44.218.92	10.240.118.97	ICMP	110	✓	Time-to-live exceeded (Time to live exceeded in transit)
64	3.896355810	49.44.218.92	10.240.118.97	ICMP	110	✓	Time-to-live exceeded (Time to live exceeded in transit)
65	3.911412687	49.44.220.189	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
174	13.925389149	49.44.220.189	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
175	13.925389610	49.44.220.189	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
178	13.926993022	182.79.134.249	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
180	13.930601984	125.22.133.146	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
181	13.930602296	182.79.134.249	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
182	13.931204054	103.221.208.18	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
183	13.932543593	182.79.134.249	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
184	13.932543941	125.22.133.146	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
185	13.933887151	125.22.133.146	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
186	13.933887579	103.221.208.18	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
187	13.933887649	103.221.208.18	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
188	13.936192615	103.43.33.2	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
189	13.936193040	103.43.33.2	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
190	13.936941044	103.43.33.2	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
191	13.936941507	220.158.165.21	10.240.118.97	ICMP	102	✓	Destination unreachable (Port unreachable)
192	13.936941626	220.158.165.21	10.240.118.97	ICMP	102	✓	Destination unreachable (Port unreachable)
193	13.974906406	220.158.165.21	10.240.118.97	ICMP	102	✓	Destination unreachable (Port unreachable)
194	13.978121070	220.158.165.21	10.240.118.97	ICMP	102	✓	Destination unreachable (Port unreachable)
217	16.996905156	220.158.165.21	10.240.118.97	ICMP	102	✓	Destination unreachable (Port unreachable)

1. **List all the unique IP addresses you observe for the traceroute on ambergroupindia.com.**
   Unique IP addresses observed for traceroute to ambergroupindia.com:

   - 10.240.118.1
   - 10.240.240.1
   - 117.205.73.161
   - 117.216.207.216
   - 49.44.218.92
   - 49.44.220.189
   - 182.79.134.249
   - 125.22.133.146
   - 103.43.33.2
   - 103.221.208.18
   - 220.158.165.21 (ambergroupindia.com)

2. **For the command traceroute -m 15 ambergroupindia.com, what does the -m 15 flag do, and how does it affect the captured packets?**
    - The `-m` flag sets the maximum TTL (Time-to-Live) value.
    - Here, `-m 15` limits the traceroute to a maximum of **15 hops**.
    - **Effect on captured packets:**
      The packets will have TTL values incrementing from 1 up to 15. After 15 hops, it stops probing further hops.
3. **Which transport layer protocol is used in the ICMP packets?**



UDP is used in the ICMP packets. ICMP does not use a transport layer protocol like TCP or UDP. It operates directly over IP at the network layer. However, in Traceroute, UDP packets trigger ICMP "Time Exceeded" responses, but ICMP itself does not rely on UDP.

4. **What happens when a router does not respond to a traceroute probe? How is this represented in the captured packets?**
   When a router does not respond to a traceroute probe, it means that the router is either configured to drop or ignore those ICMP Time-to-Live (TTL) exceeded messages or UDP probe responses. This lack of response is typically represented in the traceroute output by an asterisk (`*`) instead of an IP address and response time.

   ### In the traceroute output:

   We can see `* * *` in some hops (lines 5,7 and 8), indicating that those routers did not respond.

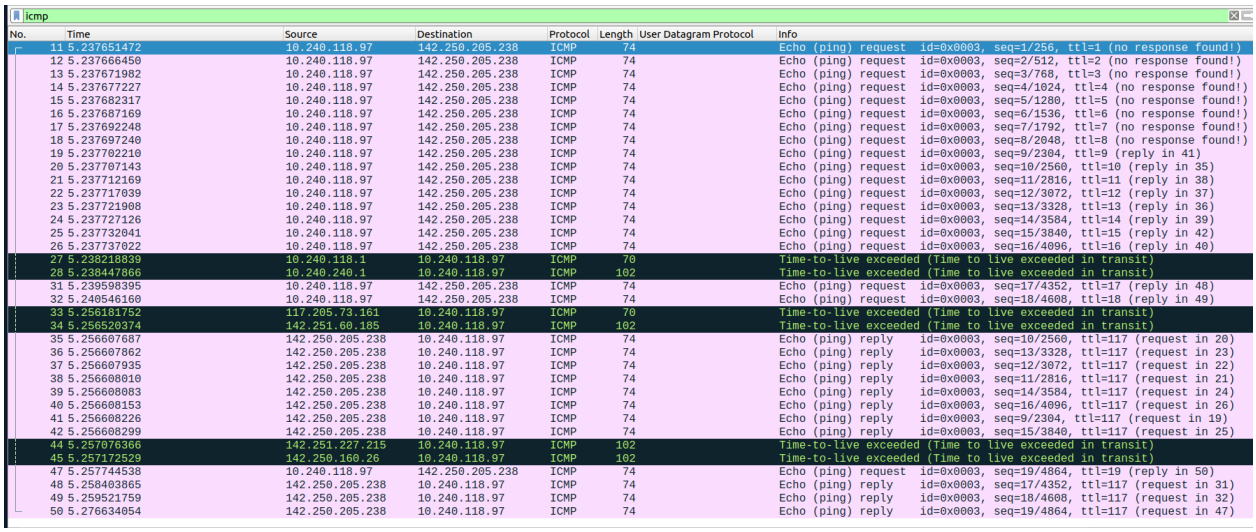
   ### In the captured packets (Wireshark capture):

- When a router does not respond, you will **not see any ICMP Time Exceeded response** from that router.
- Instead, the probe either:
    - Expires without a reply, or
    - Gets dropped silently by the router (not visible in packet capture as it never returns).
- The traceroute tool will just move on to the next TTL value and try again.

Part-3: Traceroute on `drive.google.com`

```
traceroute -I -q 1 drive.google.com
```

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ traceroute -I -q 1 drive.google.com
traceroute to drive.google.com (142.250.205.238), 30 hops max, 60 byte packets
 1  10.240.118.1 (10.240.118.1)  0.581 ms
 2  internet.iitdh.ac.in (10.240.240.1)  0.784 ms
 3  117.205.73.161 (117.205.73.161)  18.512 ms
 4  *
 5  *
 6  142.250.160.26 (142.250.160.26)  19.488 ms
 7  142.251.227.215 (142.251.227.215)  19.387 ms
 8  142.251.60.185 (142.251.60.185)  18.826 ms
 9  maa05s28-in-f14.1e100.net (142.250.205.238)  18.909 ms
```



icmp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
11	5.237651472	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=1/256, ttl=1 (no response found!)
12	5.237666450	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=2/512, ttl=2 (no response found!)
13	5.237671982	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=3/768, ttl=3 (no response found!)
14	5.237677227	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=4/1024, ttl=4 (no response found!)
15	5.237682317	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=5/1280, ttl=5 (no response found!)
16	5.237687169	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=6/1536, ttl=6 (no response found!)
17	5.237692248	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=7/1792, ttl=7 (no response found!)
18	5.237697240	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=8/2048, ttl=8 (no response found!)
19	5.237702210	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=9/2304, ttl=9 (reply in 41)
20	5.237707143	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=10/2560, ttl=10 (reply in 35)
21	5.237712169	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=11/2816, ttl=11 (reply in 38)
22	5.237717039	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=12/3072, ttl=12 (reply in 37)
23	5.237721908	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=13/3328, ttl=13 (reply in 36)
24	5.237727126	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=14/3584, ttl=14 (reply in 39)
25	5.237732041	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=15/3840, ttl=15 (reply in 42)
26	5.237737022	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=16/4096, ttl=16 (reply in 40)
27	5.238218839	10.240.118.1	10.240.118.97	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
28	5.238447866	10.240.240.1	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
31	5.239598395	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=17/4352, ttl=17 (reply in 48)
32	5.240546160	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=18/4608, ttl=18 (reply in 49)
33	5.256181752	117.205.73.161	10.240.118.97	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
34	5.256520374	142.251.60.185	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
35	5.256607687	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=10/2560, ttl=117 (request in 20)
36	5.256607862	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=13/3328, ttl=117 (request in 23)
37	5.256607935	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=12/3072, ttl=117 (request in 22)
38	5.256608010	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=11/2816, ttl=117 (request in 21)
39	5.256608083	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=14/3584, ttl=117 (request in 24)
40	5.256608153	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=16/4096, ttl=117 (request in 26)
41	5.256608226	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=9/2304, ttl=117 (request in 19)
42	5.256608299	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=15/3840, ttl=117 (request in 25)
44	5.257076366	142.251.227.215	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
45	5.257172529	142.250.160.26	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
47	5.257744538	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=19/4864, ttl=19 (reply in 50)
48	5.258403865	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=17/4352, ttl=117 (request in 31)
49	5.259521759	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=18/4608, ttl=117 (request in 32)
50	5.276634054	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=19/4864, ttl=117 (request in 47)

1. **How does the '-q 1' option in the traceroute command to drive.google.com affect the captured packets?**

   The `-q 1` option in the `traceroute` command specifies that only one probe (packet) is sent per hop instead of the default three.

Effect on captured packets:

1. **Reduced number of ICMP packets per hop:**
   In your Wireshark capture, you will notice that for each TTL (Time-to-Live) value, only one ICMP Echo Request and its corresponding ICMP Time Exceeded (if not the final destination) or Echo Reply (if destination reached) is observed.
2. **Less congestion and faster completion:**
   With `-q 1`, traceroute finishes more quickly and sends fewer packets, making the output less verbose and the capture more compact.The accuracy of latency measurements per hop might be lower due to fewer samples.

3. **Observation in your capture:**
   - You can see each increment in TTL results in a single `Time-to-live exceeded` message from intermediate hops.
   - When the destination is reached, only one Echo Reply is captured for each hop attempt.
   - This clean pattern of single probe attempts per hop is a direct result of the `-q 1` option

2. **What is the significance of the -I option in the traceroute command? How does it affect the type of packets sent compared to the default traceroute behaviour?**

   Significance of the `-I` option in the `traceroute` command:

   The `-I` option tells `traceroute` to use **ICMP Echo Requests** instead of the default **UDP packets**.

   How it affects the type of packets sent:

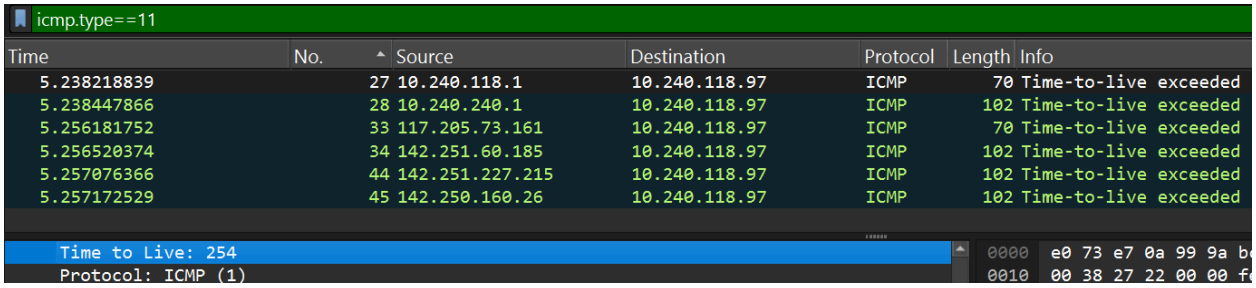
Without `-I` (default)	With `-I`
Sends **UDP** packets to high-numbered ports (typically 33434 and above) with incrementing TTL.	Sends **ICMP Echo Request** packets with incrementing TTL.
The destination responds with an **ICMP Port Unreachable** message when reached.	The destination responds with an **ICMP Echo Reply(Type 0)**.
Intermediate hops send back **ICMP Time Exceeded** messages when TTL expires.	Intermediate hops also send **ICMP Time Exceeded** messages when TTL expires.
Sometimes blocked by firewalls that filter UDP traffic.	Often more successful across restrictive networks, since ICMP Echo Requests are usually allowed (similar to ping).

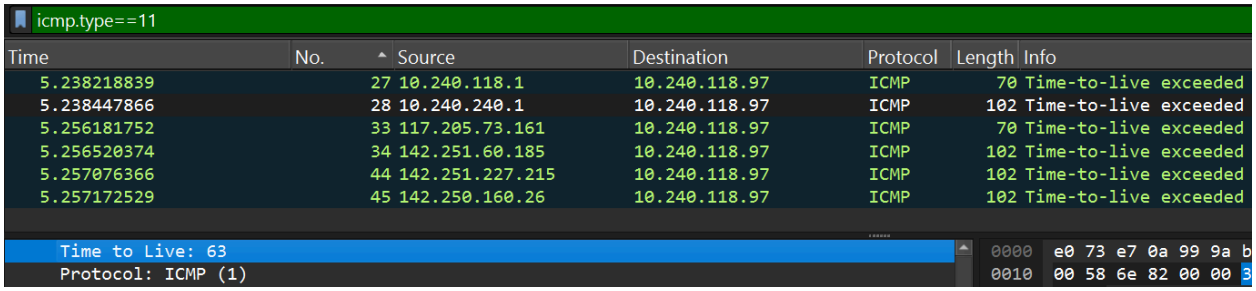
What you see in your Wireshark capture:

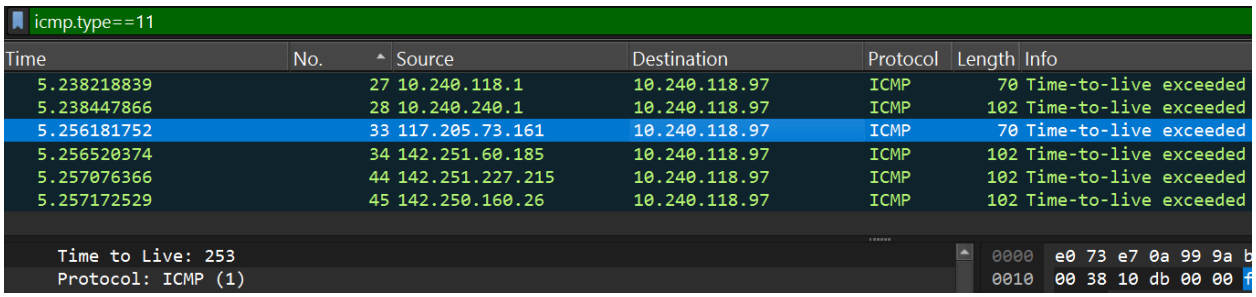
1. The packets are **ICMP Echo Requests** (`Protocol: ICMP` with "Echo request" in Info column).
2. The responses are either **Time-to-live exceeded** messages or **Echo replies**.
3. This confirms that `-I` made `traceroute` behave similarly to `ping` but with incrementing TTL values.

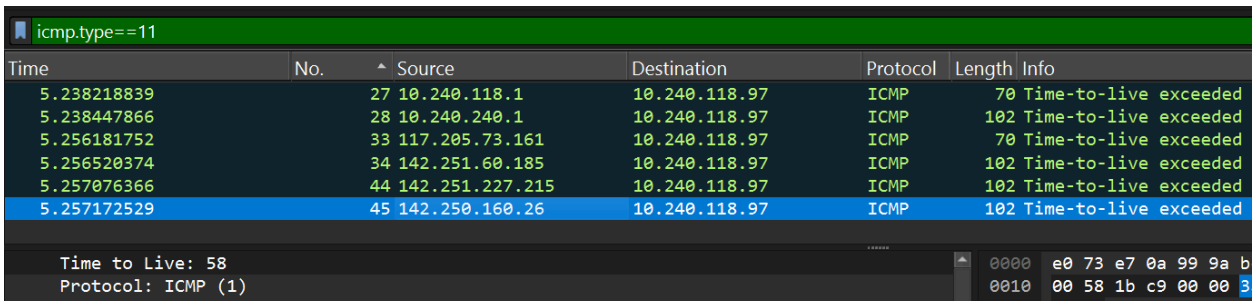
3. **Compare the TTL values in ICMP Time Exceeded messages from different routers in the traceroute output. What pattern do you observe?**

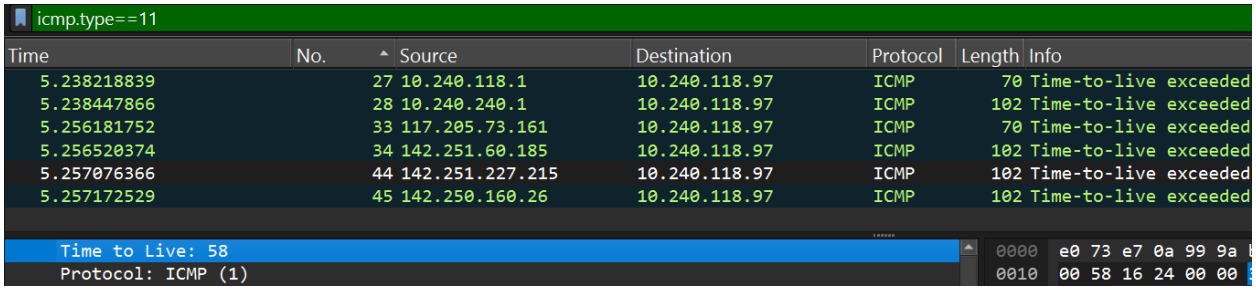
```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ traceroute -I -q 1 drive.google.com
traceroute to drive.google.com (142.250.205.238), 30 hops max, 60 byte packets
 1  10.240.118.1 (10.240.118.1)  0.581 ms
 2  internet.iitdh.ac.in (10.240.240.1)  0.784 ms
 3  117.205.73.161 (117.205.73.161)  18.512 ms
 4  *
 5  *
 6  142.250.160.26 (142.250.160.26)  19.488 ms
 7  142.251.227.215 (142.251.227.215)  19.387 ms
 8  142.251.60.185 (142.251.60.185)  18.826 ms
 9  maa05s28-in-f14.1e100.net (142.250.205.238)  18.909 ms
```

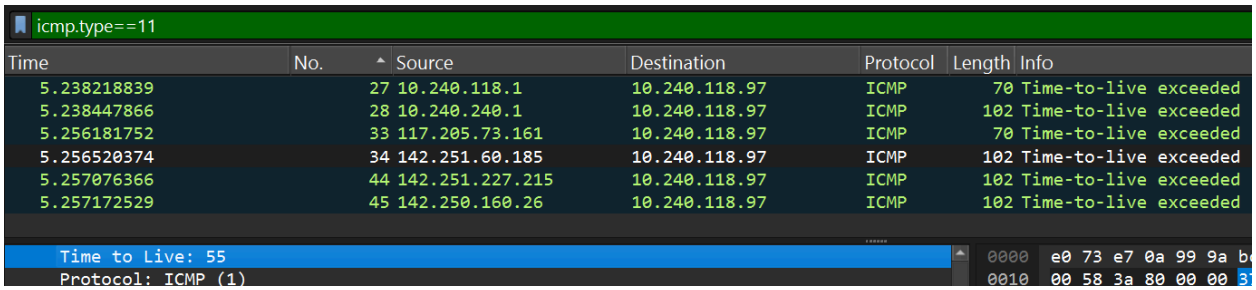












From the traceroute output in your Wireshark captures, the Time-to-Live (TTL) values in the ICMP Time Exceeded messages show a consistent decrement pattern. Here's the observed trend:

Router IP	**Initial TTL**	**Observed TTL**	**Hops Traversed(TTL decrements)**
10.240.118.1	255	254	1
10.240.240.1	64	63	1
117.205.73.161	255	253	2
142.250.160.26	64	58	6
142.251.227.215	64	58	6
142.251.60.185	64	55	9

Pattern Observed:

1. **TTL Values Indicate Operating Systems & Router Types:**
   - **Cisco/Enterprise routers** typically start with **255** (TTL around 254-253).
   - **Linux/Unix-based routers** generally start with **64** (TTL around 63-58).
   - **Destination servers** often start with **128** (common for Windows-based systems).

2. **TTL Decrement Reveals Network Distance & Routing Path:**
   - **Local/Internal routers (10.x.x.x)** show **minimal TTL decrement (1 hop)**, suggesting proximity

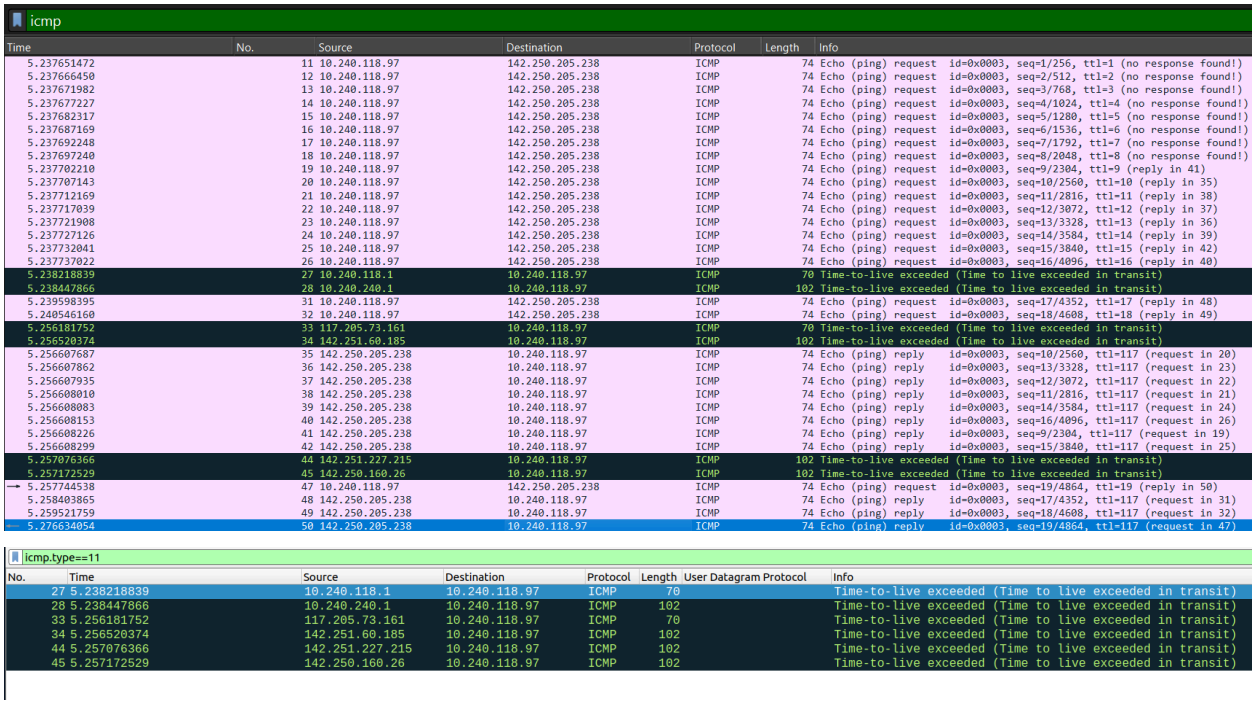
- **ISP/Transit routers** experience moderate TTL decrements **(~2-3 hops)**.
- **Google Backbone Routers** exhibit **higher TTL decrements (6+ hops)**, indicating longer network paths.

3. **Asymmetric Routing is Evident:**
   - Return paths often differ from the outbound paths (e.g., some routers show higher TTL decrements).
   - Google's infrastructure uses **load balancing**, leading to varied TTL values in different backbone routers.

4. **Network Boundaries Are Visible:**
   - **Local ISP network** shows small TTL losses.
   - **Google's network (142.x.x.x)** exhibits significant TTL decrements due to multiple intermediate routers.

Conclusion: This analysis demonstrates how **TTL values in ICMP Time Exceeded messages** reveal key insights into **network topology, router types, and routing behaviors**. By observing TTL decrement patterns, one can infer **network boundaries, asymmetric routing paths, and infrastructure diversity** across the internet.

4. **For the traceroute to drive.google.com, how many different unique IP addresses do you observe in the captured packets?**



icmp

Time	No.	Source	Destination	Protocol	Length	Info
5.237651472	11	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=1/256, ttl=1 (no response found!)
5.237666450	12	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=2/512, ttl=2 (no response found!)
5.237671982	13	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=3/768, ttl=3 (no response found!)
5.237677227	14	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=4/1024, ttl=4 (no response found!)
5.237682317	15	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=5/1280, ttl=5 (no response found!)
5.237687169	16	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=6/1536, ttl=6 (no response found!)
5.237692248	17	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=7/1792, ttl=7 (no response found!)
5.237697240	18	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=8/2048, ttl=8 (no response found!)
5.237702210	19	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=9/2304, ttl=9 (reply in 41)
5.237707143	20	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=10/2560, ttl=10 (reply in 35)
5.237712169	21	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=11/2816, ttl=11 (reply in 38)
5.237717039	22	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=12/3072, ttl=12 (reply in 37)
5.237721908	23	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=13/3328, ttl=13 (reply in 36)
5.237727126	24	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=14/3584, ttl=14 (reply in 39)
5.237732041	25	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=15/3840, ttl=15 (reply in 42)
5.237737022	26	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=16/4096, ttl=16 (reply in 40)
5.238218839	27	10.240.118.1	10.240.118.97	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5.238447866	28	10.240.240.1	10.240.118.97	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
5.239598395	31	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=17/4352, ttl=17 (reply in 48)
5.240546160	32	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=18/4608, ttl=18 (reply in 49)
5.256181752	33	117.205.73.161	10.240.118.97	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5.256520374	34	142.251.60.185	10.240.118.97	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
5.256607687	35	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=10/2560, ttl=117 (request in 20)
5.256607862	36	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=13/3328, ttl=117 (request in 23)
5.256607935	37	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=12/3072, ttl=117 (request in 22)
5.256608010	38	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=11/2816, ttl=117 (request in 21)
5.256608083	39	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=14/3584, ttl=117 (request in 24)
5.256608153	40	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=16/4096, ttl=117 (request in 26)
5.256608226	41	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=9/2304, ttl=117 (request in 19)
5.256608299	42	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=15/3840, ttl=117 (request in 25)
5.257076366	44	142.251.227.215	10.240.118.97	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
5.257172529	45	142.250.160.26	10.240.118.97	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
5.257744538	47	10.240.118.97	142.250.205.238	ICMP	74	Echo (ping) request id=0x0003, seq=19/4864, ttl=19 (reply in 50)
5.258403865	48	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=17/4352, ttl=117 (request in 31)
5.259521759	49	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=18/4608, ttl=117 (request in 32)
5.276634054	50	142.250.205.238	10.240.118.97	ICMP	74	Echo (ping) reply id=0x0003, seq=19/4864, ttl=117 (request in 47)

icmp.type==11

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
27	5.238218839	10.240.118.1	10.240.118.97	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
28	5.238447866	10.240.240.1	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
33	5.256181752	117.205.73.161	10.240.118.97	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
34	5.256520374	142.251.60.185	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
44	5.257076366	142.251.227.215	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
45	5.257172529	142.250.160.26	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)

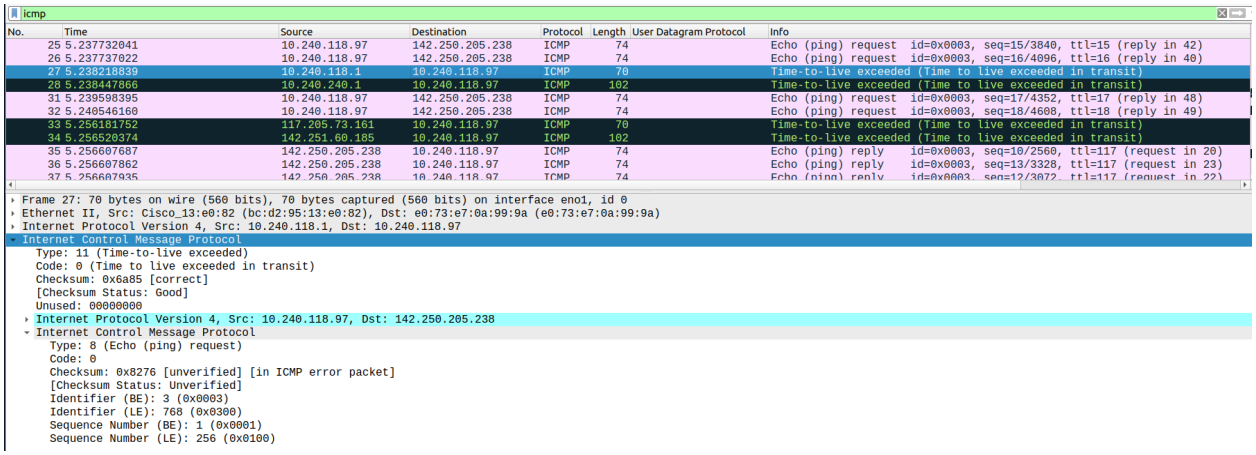
<u>Unique IP addresses observed in captured packets:</u>

- 10.240.118.1
- 10.240.240.1
- 117.205.73.161

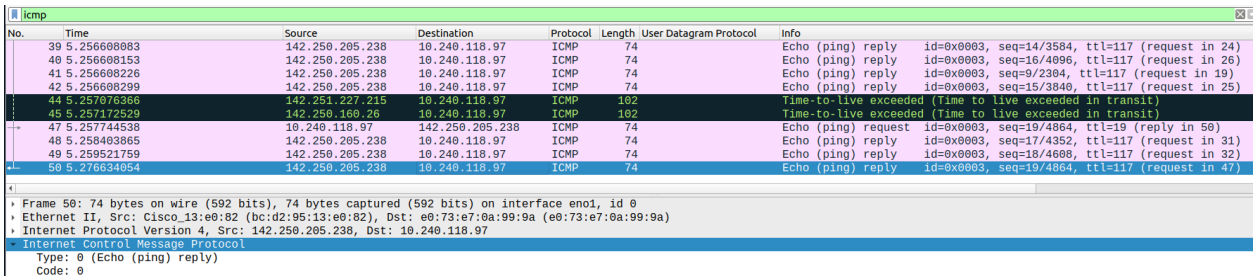
- 142.250.160.26
- 142.251.227.215
- 142.251.60.185

  → 1 Final Destination IP Address: 142.250.205.238

5. **In the captured Wireshark packets, what type of ICMP messages do you observe for intermediate hops, and what type of response do you receive from the final destination?**

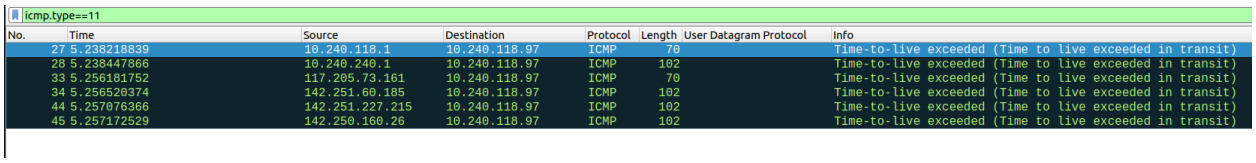


- **Intermediate hops** send **ICMP Time Exceeded** messages (Type 11, Code 0) indicating TTL expiration at that hop.



- **Final destination** responds with **ICMP Echo Reply** (Type 0, Code 0) in response to the ping request.

6. **What is the source IP address of the ICMP Time Exceeded messages, and what does it indicate about the network path?**



The source IP address of the ICMP Time Exceeded messages is the IP address of the router or hop where the packet's TTL reaches zero.

- At hop 1: source IP = **10.240.118.1**
- At hop 2: source IP = **10.240.240.1**
- At hop 3: source IP = **117.205.73.161**

- At hop 4: source IP = **142.251.60.185**
- At hop 5: source IP = **142.251.227.215**
- At hop 6: source IP = **142.250.160.26**

This indicates the exact routers the traceroute packet traverses, showing the **sequential path** of packets through the network.

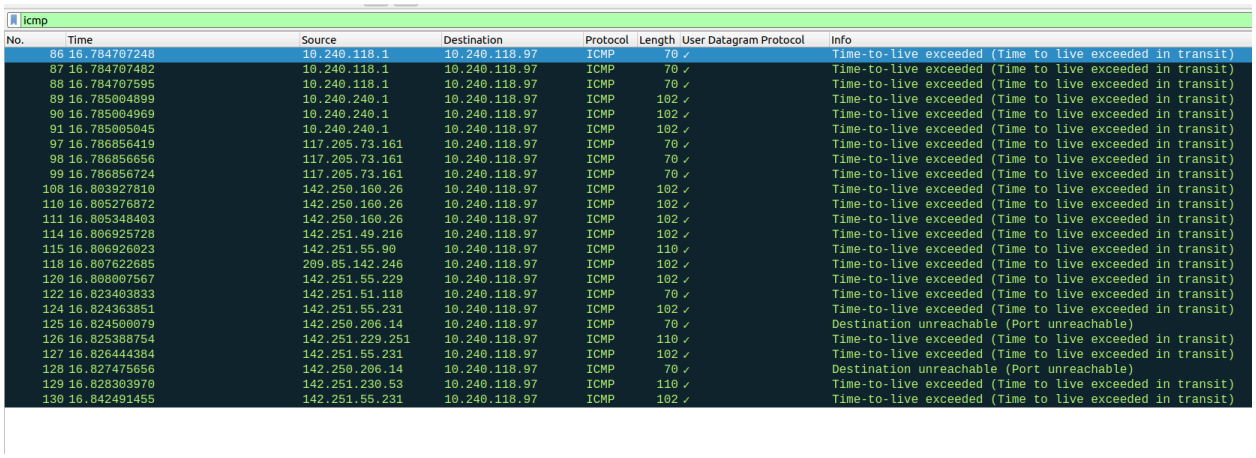
7. **If you compare the results of traceroute -I -q 1 drive.google.com and traceroute drive.google.com, what key differences would you expect in the captured packets?**

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ traceroute -I -q 1 drive.google.com
traceroute to drive.google.com (142.250.205.238), 30 hops max, 60 byte packets
 1  10.240.118.1 (10.240.118.1)  0.581 ms
 2  internet.iitdh.ac.in (10.240.240.1)  0.784 ms
 3  117.205.73.161 (117.205.73.161)  18.512 ms
 4  *
 5  *
 6  142.250.160.26 (142.250.160.26)  19.488 ms
 7  142.251.227.215 (142.251.227.215)  19.387 ms
 8  142.251.60.185 (142.251.60.185)  18.826 ms
 9  maa05s28-in-f14.1e100.net (142.250.205.238)  18.909 ms
```

icmp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
11	5.237651472	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=1/256, ttl=1 (no response found!)
12	5.237666450	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=2/512, ttl=2 (no response found!)
13	5.237671982	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=3/768, ttl=3 (no response found!)
14	5.237677227	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=4/1024, ttl=4 (no response found!)
15	5.237682317	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=5/1280, ttl=5 (no response found!)
16	5.237687169	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=6/1536, ttl=6 (no response found!)
17	5.237692248	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=7/1792, ttl=7 (no response found!)
18	5.237697240	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=8/2048, ttl=8 (no response found!)
19	5.237702210	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=9/2304, ttl=9 (reply in 41)
20	5.237707143	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=10/2560, ttl=10 (reply in 35)
21	5.237712169	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=11/2816, ttl=11 (reply in 38)
22	5.237717039	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=12/3072, ttl=12 (reply in 37)
23	5.237721908	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=13/3328, ttl=13 (reply in 36)
24	5.237727126	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=14/3584, ttl=14 (reply in 39)
25	5.237732041	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=15/3840, ttl=15 (reply in 42)
26	5.237737022	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=16/4096, ttl=16 (reply in 40)
27	5.238218839	10.240.118.1	10.240.118.97	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
28	5.238447866	10.240.240.1	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
31	5.239598395	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=17/4352, ttl=17 (reply in 48)
32	5.240546160	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=18/4608, ttl=18 (reply in 49)
33	5.256181752	117.205.73.161	10.240.118.97	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
34	5.256520374	142.251.60.185	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
35	5.256607687	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=10/2560, ttl=117 (request in 20)
36	5.256607862	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=13/3328, ttl=117 (request in 23)
37	5.256607935	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=12/3072, ttl=117 (request in 22)
38	5.256608010	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=11/2816, ttl=117 (request in 21)
39	5.256608083	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=14/3584, ttl=117 (request in 24)
40	5.256608153	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=16/4096, ttl=117 (request in 26)
41	5.256608226	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=9/2304, ttl=117 (request in 19)
42	5.256608299	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=15/3840, ttl=117 (request in 25)
44	5.257076366	142.251.227.215	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
45	5.257172529	142.250.160.26	10.240.118.97	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
47	5.257744538	10.240.118.97	142.250.205.238	ICMP	74		Echo (ping) request id=0x0003, seq=19/4864, ttl=19 (reply in 50)
48	5.258403865	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=17/4352, ttl=117 (request in 31)
49	5.259521759	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=18/4608, ttl=117 (request in 32)
50	5.276634054	142.250.205.238	10.240.118.97	ICMP	74		Echo (ping) reply id=0x0003, seq=19/4864, ttl=117 (request in 47)

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ traceroute drive.google.com
traceroute to drive.google.com (142.250.206.14), 30 hops max, 60 byte packets
 1  10.240.118.1 (10.240.118.1)  0.405 ms  0.373 ms  0.356 ms
 2  internet.iitdh.ac.in (10.240.240.1)  0.639 ms  0.623 ms  0.608 ms
 3  117.205.73.161 (117.205.73.161)  2.444 ms  2.397 ms  2.381 ms
 4  * * *
 5  * * *
 6  142.250.160.26 (142.250.160.26)  19.316 ms  19.230 ms  19.127 ms
 7  * * *
 8  142.251.55.90 (142.251.55.90)  19.602 ms 142.251.49.216 (142.251.49.216)  18.163 ms 209.85.142.246 (209.85.142.246)  18.825 ms
 9  142.251.55.229 (142.251.55.229)  19.191 ms 142.251.51.118 (142.251.51.118)  19.293 ms 142.251.55.231 (142.251.55.231)  18.839 ms
10  pnmaaa-ax-in-f14.1e100.net (142.250.206.14)  18.947 ms 142.251.230.53 (142.251.230.53)  21.224 ms 142.251.229.251 (142.251.229.251)  18.276 ms
```



icmp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
86	16.784707248	10.240.118.1	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
87	16.784707482	10.240.118.1	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
88	16.784707595	10.240.118.1	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
89	16.785004899	10.240.240.1	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
90	16.785004969	10.240.240.1	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
91	16.785005045	10.240.240.1	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
97	16.786856419	117.205.73.161	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
98	16.786856656	117.205.73.161	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
99	16.786856724	117.205.73.161	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
108	16.803927810	142.250.160.26	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
110	16.805276872	142.250.160.26	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
111	16.805348403	142.250.160.26	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
114	16.806925728	142.251.49.216	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
115	16.806926023	142.251.55.90	10.240.118.97	ICMP	110	✓	Time-to-live exceeded (Time to live exceeded in transit)
118	16.807622685	209.85.142.246	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
120	16.808007567	142.251.55.229	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
122	16.823403833	142.251.51.118	10.240.118.97	ICMP	70	✓	Time-to-live exceeded (Time to live exceeded in transit)
124	16.824363851	142.251.55.231	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
125	16.824500079	142.250.206.14	10.240.118.97	ICMP	70	✓	Destination unreachable (Port unreachable)
126	16.825388754	142.251.229.251	10.240.118.97	ICMP	110	✓	Time-to-live exceeded (Time to live exceeded in transit)
127	16.826444384	142.251.55.231	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)
128	16.827475656	142.250.206.14	10.240.118.97	ICMP	70	✓	Destination unreachable (Port unreachable)
129	16.828303970	142.251.230.53	10.240.118.97	ICMP	110	✓	Time-to-live exceeded (Time to live exceeded in transit)
130	16.842491455	142.251.55.231	10.240.118.97	ICMP	102	✓	Time-to-live exceeded (Time to live exceeded in transit)

Feature	`traceroute drive.google.com` (default)	`traceroute -I -q 1 drive.google.com`
Protocol used	UDP packets with increasing TTL	ICMP Echo Requests with increasing TTL
Destination responses	ICMP "Port Unreachable" messages from the final destination	ICMP Echo Replies from the final destination
Number of probes per hop	By default, 3 probes per hop,providing more statistical accuracy but increasing the number of captured packets.	Only 1 probe per hop (due to `-q 1`) is sent, reducing network traffic and making the trace faster.

Part-4: Controlling Packet Size `using ping`

`For ubuntu: ping -s 1570 -c 5` www.godaddy.com

`For Windows: ping -l 1570 -n 5` www.godaddy.com

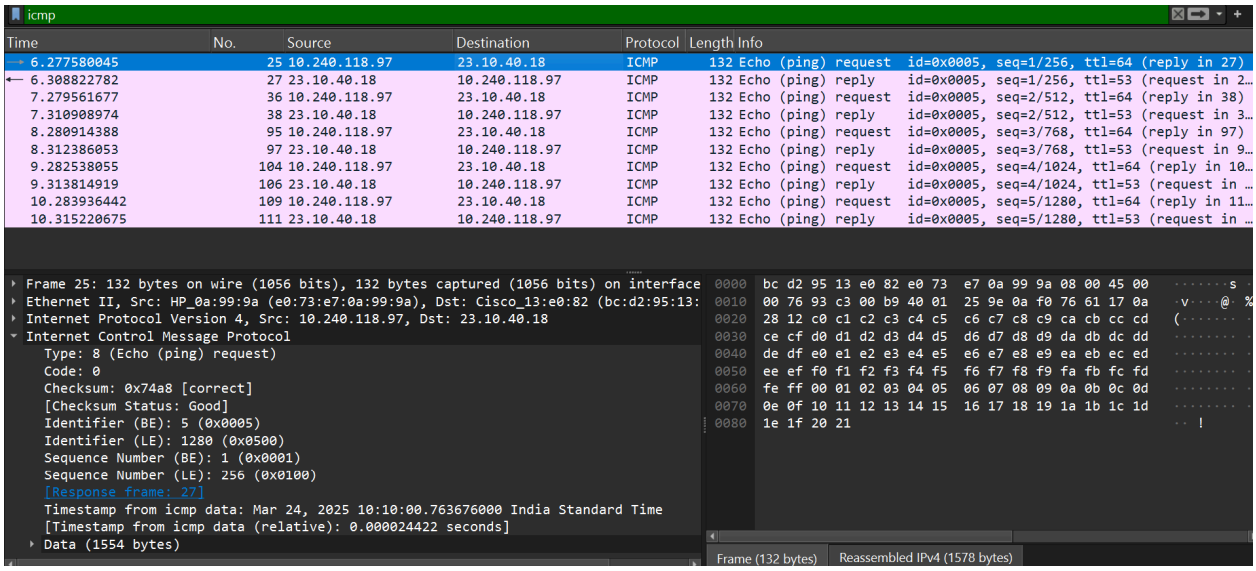
```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ping -s 1570 -c 5 www.godaddy.com
PING e6001.dscx.akamaiedge.net (23.10.40.18) 1570(1598) bytes of data.
1578 bytes from a23-10-40-18.deploy.static.akamaitechnologies.com (23.10.40.18): icmp_seq=1 ttl=53 time=31.3 ms
1578 bytes from a23-10-40-18.deploy.static.akamaitechnologies.com (23.10.40.18): icmp_seq=2 ttl=53 time=31.4 ms
1578 bytes from a23-10-40-18.deploy.static.akamaitechnologies.com (23.10.40.18): icmp_seq=3 ttl=53 time=31.5 ms
1578 bytes from a23-10-40-18.deploy.static.akamaitechnologies.com (23.10.40.18): icmp_seq=4 ttl=53 time=31.3 ms
1578 bytes from a23-10-40-18.deploy.static.akamaitechnologies.com (23.10.40.18): icmp_seq=5 ttl=53 time=31.3 ms

--- e6001.dscx.akamaiedge.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 31.267/31.367/31.519/0.086 ms
```

1. **What is the significance of the '-s 1570' option in the ping command? Calculate the total size of each ping request packet sent to the specified domain, including all protocol headers.**

   Significance of `-s 1570`:

   The `-s 1570` option in the `ping` command specifies the size of the ICMP payload (data) in bytes.So, `ping -s 1570` means each ICMP Echo Request packet will carry **1570 bytes** of data (excluding headers).



Wireshark Breakdown:

1. **16 bytes** → Timestamp
2. **1554 bytes** → ICMP Data

Now, adding these together:ICMP payload= 16+1554= 1570 bytes

Total Size of Each Ping Request Packet Each ICMP packet consists of:

- **IP Header:** 20 bytes (IPv4 standard)
- **ICMP Header:** 8 bytes (fixed)
- **ICMP Payload:** 1570 bytes (as specified above)

Total Packet Size=20+8+1570=1598 bytes

2. **State the number of fields in the ICMP header along with its size.**

ICMP Header Structure

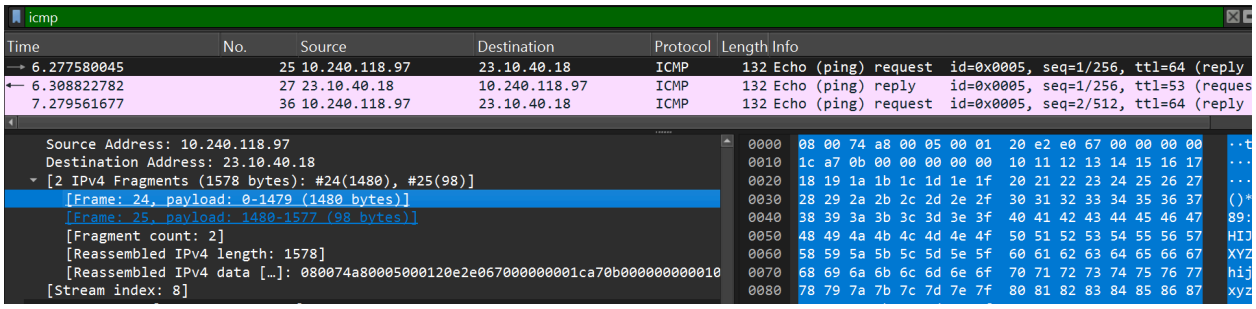
The **ICMP (Internet Control Message Protocol) header** consists of **5 main fields**, totaling **8 bytes** in size.**Total ICMP Header Size: 8 bytes**

Field Name	Size (bytes)	Description
Type	1 byte	Specifies the ICMP message type (e.g., 8 for Echo Request, 0 for Echo Reply).
Code	1 byte	Further classifies the message type (e.g., for Echo Request/Reply, this is 0).
Checksum	2 bytes	Error-checking field to verify header integrity.
Identifier	2 bytes	Used to match requests with replies (helps track multiple pings).
Sequence Number	2 bytes	Helps identify and order packets in a series of pings.

Additionally, some ICMP messages (like Echo Request/Reply) include **data** (payload), which varies in size.

3. **What is the maximum ICMP packet size that can be transmitted without fragmentation, considering standard MTU constraints?**
   The maximum ICMP **payload** that can be transmitted without fragmentation over a standard **Ethernet MTU (1500 bytes)** is **1472 bytes**.Any ICMP payload greater than 1472 bytes will require fragmentation.

   - **Total MTU:** 1500 bytes
   - **IP Header:** 20 bytes
   - **ICMP Header:** 8 bytes
   - **Max ICMP Payload:** 1500 - (20 + 8) = **1472 bytes**
4. **Does the captured packet trace indicate fragmentation for the ICMP echo request sent to the specified domain? If so, determine the total number of fragmented packets and analyze their fragment offset in the IP header.**



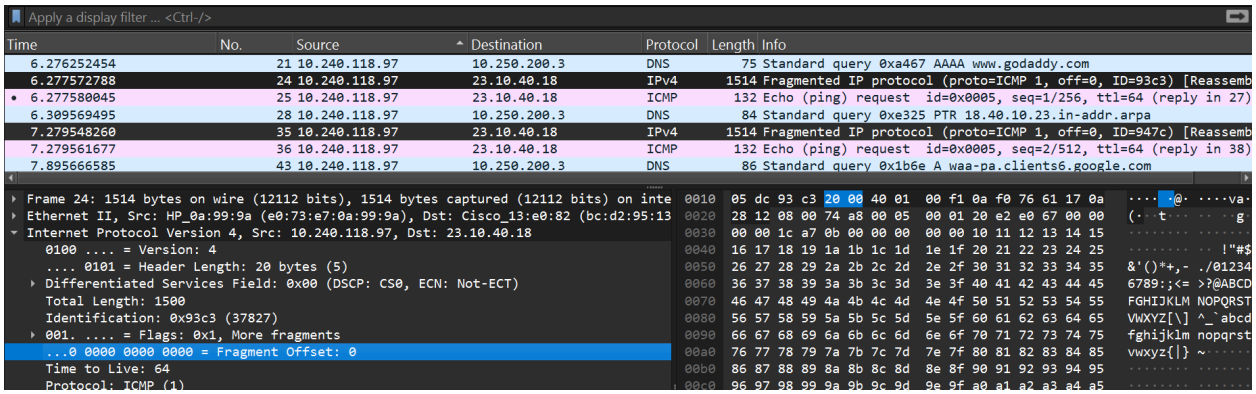
Yes, the captured packet trace **does indicate fragmentation** for the ICMP Echo Request due to the payload size exceeding the standard MTU of 1500 bytes.The Wireshark capture shows two IPv4 fragments for the ICMP echo request.

Evidence of Fragmentation:

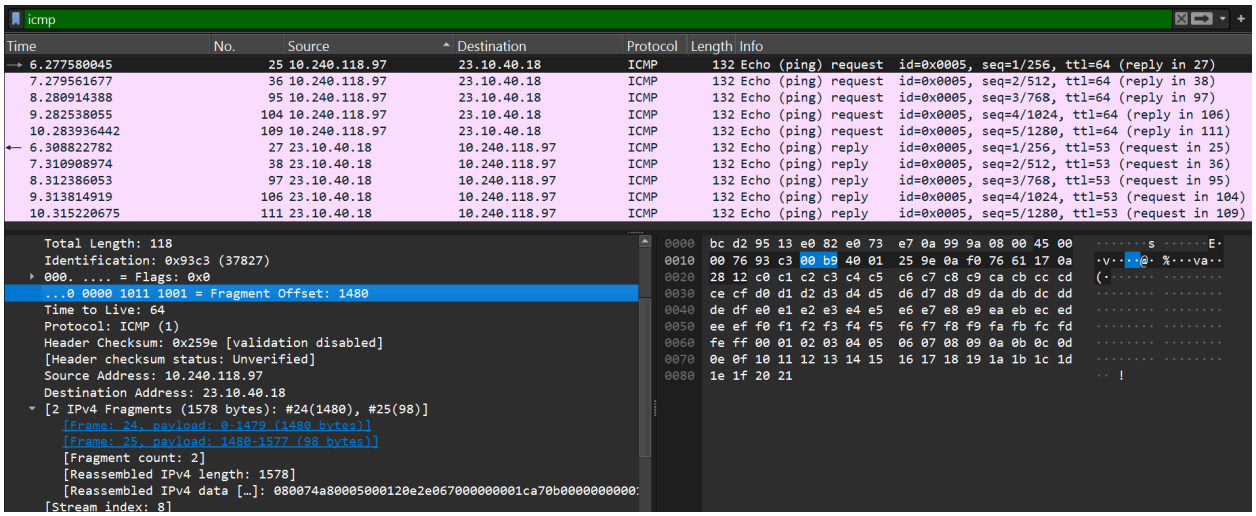
- The ICMP Echo Request has a **total reassembled length of 1578 bytes**.
- The **IPv4 MTU is typically 1500 bytes**, so any packet larger than this requires fragmentation.
- The trace shows **two IPv4 fragments**:
    - **Frame 24**: **1480 bytes** (Payload: 0-1479)
    - **Frame 25**: **98 bytes** (Payload: 1480-1577)
- This confirms that the original ICMP packet was split into **two fragments**.

Fragment Offset Analysis:

The **IP header contains a fragment offset field**, which indicates the position of a fragment in the original packet.



- **Frame 24 (First fragment)**:
    - **Offset:** 0 (Indicates this is the first fragment)
    - **MF (More Fragments) flag: Set** (Indicates more fragments follow)
    - **Payload:** 1480 bytes



- **Frame 25 (Second fragment)**:
    - **Offset:** 1480 (Indicates this fragment starts at byte 1480 in the original packet)
    - **MF flag: Not Set** (Indicates this is the last fragment)
    - **Payload:** 98 bytes

Final Conclusion:

Yes, the ICMP Echo Request was **fragmented into two packets**:

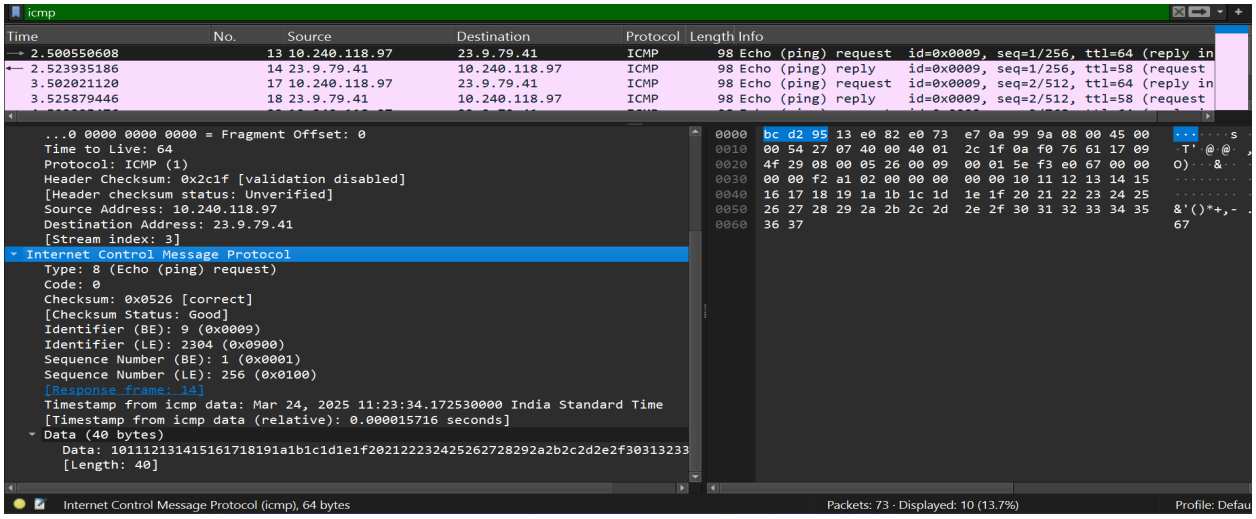
1. **First fragment**: 1480 bytes (Offset: 0)
2. **Second fragment**: 98 bytes (Offset: 1480)

This fragmentation likely occurred because the ICMP payload exceeded the **Maximum Transmission Unit (MTU) limit of 1500 bytes**, requiring it to be split into multiple packets for transmission.

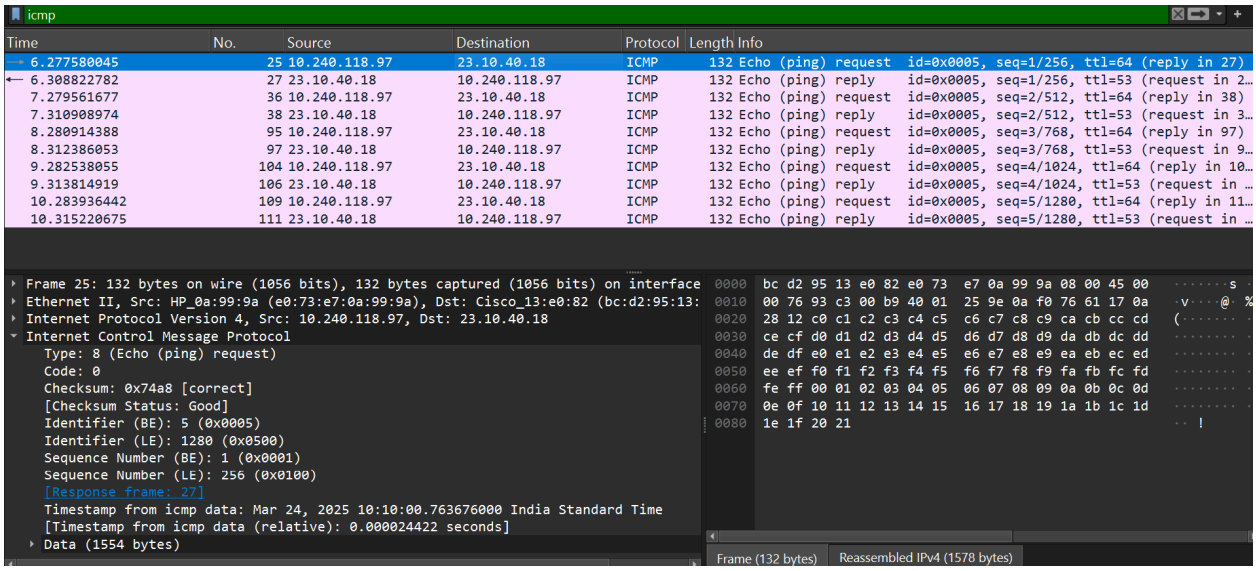
5. **What is the default ICMP payload size observed in the standard ping request to the specified domain using this command `ping -c 5 www.godaddy.com`? Additionally, analyze the difference in payload size between the default ping request and the custom-sized `ping -s 1570 -c 5` www.godaddy.com.**

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ping -c 5 www.godaddy.com
PING e6001.dscx.akamaiedge.net (23.9.79.41) 56(84) bytes of data.
64 bytes from a23-9-79-41.deploy.static.akamaitechnologies.com (23.9.79.41): icmp_seq=1 ttl=58 time=23.4 ms
64 bytes from a23-9-79-41.deploy.static.akamaitechnologies.com (23.9.79.41): icmp_seq=2 ttl=58 time=23.9 ms
64 bytes from a23-9-79-41.deploy.static.akamaitechnologies.com (23.9.79.41): icmp_seq=3 ttl=58 time=21.9 ms
64 bytes from a23-9-79-41.deploy.static.akamaitechnologies.com (23.9.79.41): icmp_seq=4 ttl=58 time=24.9 ms
64 bytes from a23-9-79-41.deploy.static.akamaitechnologies.com (23.9.79.41): icmp_seq=5 ttl=58 time=23.9 ms

--- e6001.dscx.akamaiedge.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 21.873/23.594/24.906/0.990 ms
```



1. **Default ICMP Payload Size:**
    - The `ping -c 5 www.godaddy.com` command captures packets with **64 bytes of data**, as shown in the Wireshark capture and terminal output.
    - The total packet size in this case would be:
        - **ICMP header**: 8 bytes
        - **ICMP payload (default data)**: 56 bytes
        - **Total ICMP packet size**: **64 bytes**
2. **Comparison with Custom-sized Ping (`ping -s 1570 -c 5 www.godaddy.com`):**



    - The `-s 1570` flag sets the payload size to **1570 bytes**.
    - The total packet size in this case would be:
        - **ICMP header**: 8 bytes
        - **ICMP payload**: 1570 bytes
        - **Total ICMP packet size**: **1578 bytes**
    - Since the maximum transmission unit (MTU) for Ethernet is typically **1500 bytes**, this larger packet size would lead to **fragmentation** at the IP layer.

Ping Command	ICMP Payload	ICMP Header	Total ICMP Size	Fragmentation
`ping -c 5 www.godaddy.com`	56 bytes	8 bytes	64 bytes	No
`ping -s 1570 -c 5 www.godaddy.com`	1570 bytes	8 bytes	1578 bytes	Yes (due to exceeding MTU of 1500 bytes)

Thus, using `ping -s 1570`, the packet would be **fragmented** into multiple IP packets to fit within the MTU constraints.

Submission Details

- Write your ICMP answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).