

CS 315 : Computer Networks Lab
Assignment - 10
Wireshark Lab: ICMP

Ayush Mallick
CS22BT008

Part-0

```
cs101@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.240.118.81 netmask 255.255.248.0 broadcast 10.240.119.255
    inet6 fe80::caaa:5c87:96bd:271f prefixlen 64 scopeid 0x20<link>
    ether 7c:57:58:d1:f3:dc txqueuelen 1000 (Ethernet)
    RX packets 68091 bytes 78312796 (78.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17889 bytes 5535475 (5.5 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 1680 bytes 179182 (179.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1680 bytes 179182 (179.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp0s20f3: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether b0:dc:ef:bf:4c:fd txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Part-1

1.1

Number of ping requests : 5

Number of ping replies : 5

icmp							
No.	Time	Source	Destination	Protocol	Length	Text item	Info
38	3.6936741..	10.240.118.81	35.212.5.112	ICMP	98	Echo (ping) request	id=0x0001, seq=1/256, ttl=64 (reply in 39)
39	3.9300016..	35.212.5.112	10.240.118.81	ICMP	98	Echo (ping) reply	id=0x0001, seq=1/256, ttl=58 (request in 38)
43	4.6946790..	10.240.118.81	35.212.5.112	ICMP	98	Echo (ping) request	id=0x0001, seq=2/512, ttl=64 (reply in 44)
44	4.9309351..	35.212.5.112	10.240.118.81	ICMP	98	Echo (ping) reply	id=0x0001, seq=2/512, ttl=58 (request in 43)
76	5.6948503..	10.240.118.81	35.212.5.112	ICMP	98	Echo (ping) request	id=0x0001, seq=3/768, ttl=64 (reply in 87)
87	5.9311231..	35.212.5.112	10.240.118.81	ICMP	98	Echo (ping) reply	id=0x0001, seq=3/768, ttl=58 (request in 76)
128	6.6949318..	10.240.118.81	35.212.5.112	ICMP	98	Echo (ping) request	id=0x0001, seq=4/1024, ttl=64 (reply in 140)
140	6.9314662..	35.212.5.112	10.240.118.81	ICMP	98	Echo (ping) reply	id=0x0001, seq=4/1024, ttl=58 (request in 128)
175	7.6954923..	10.240.118.81	35.212.5.112	ICMP	98	Echo (ping) request	id=0x0001, seq=5/1280, ttl=64 (reply in 188)
188	7.9319001..	35.212.5.112	10.240.118.81	ICMP	98	Echo (ping) reply	id=0x0001, seq=5/1280, ttl=58 (request in 175)

1.2

Destination IP address : 35.212.5.112

Domain name : *wireshark.com*

Header checksum status: Unverified	▼ wireshark.com: type A, class IN, addr 35.212.5.112
Source Address: 10.240.118.81	Name: wireshark.com
Destination Address: 35.212.5.112	Type: A (Host Address) (1)
▼ Internet Control Message Protocol	Class: IN (0x0001)
Type: 8 (Echo (ping) request)	Time to live: 86013 (23 hours, 53 minutes, 33 seconds)
Code: 0	Data length: 4
	Address: 35.212.5.112

1.3

The Sequence Number (BE) field starts with 1 and increments by 1 for each packet, and the Sequence Number (LE) field starts with 256 and increments by 256 for each packet.

Identifier (LE): 256 (0x0100)	Identifier (LE): 256 (0x0100)
Sequence Number (BE): 1 (0x0001)	Sequence Number (BE): 2 (0x0002)
Sequence Number (LE): 256 (0x0100)	Sequence Number (LE): 512 (0x0200)
[Response frame: 201]	[Response frame: 441]
Identifier (LE): 256 (0x0100)	Identifier (LE): 256 (0x0100)
Sequence Number (BE): 3 (0x0003)	Sequence Number (BE): 4 (0x0004)
Sequence Number (LE): 768 (0x0300)	Sequence Number (LE): 1024 (0x0400)
[Response frame: 871]	[Response frame: 1401]
Identifier (LE): 256 (0x0100)	Identifier (LE): 256 (0x0100)
Sequence Number (BE): 5 (0x0005)	Sequence Number (BE): 5 (0x0005)
Sequence Number (LE): 1280 (0x0500)	Sequence Number (LE): 1280 (0x0500)
[Response frame: 1891]	[Response frame: 1891]

1.4

There are 2 types of echo pings in the trace :

Type 8 (Echo (ping) request)

Type 0 (Echo (ping) reply)

▼ Internet Control Message Protocol	▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)	Type: 0 (Echo (ping) reply)
Code: 0	Code: 0

1.5

Fields unchanged between ping request and reply packets :

Code : 0

Identifier (BE) : 1 (0x0001)

Identifier (LE) : 256 (0x0100)

Sequence Number (BE) : 1 (0x0001)

Sequence Number (LE) : 256 (0x0100)

Timestamp from icmp data: Mar 24, 2025 08:59:42.000000000 IST

Data

```

- Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x7d63 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Response frame: 39]
  Timestamp from icmp data: Mar 24, 2025 08:59:42.000000000 IST
  [Timestamp from icmp data (relative): 0.560700583 seconds]
- Data (48 bytes)
  Data: 2c8e080000000000101112131415161718191a1b1c1d1e1f20212
  [Length: 48]

```

```

- Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x8563 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Request frame: 38]
  [Response time: 236.327 ms]
  Timestamp from icmp data: Mar 24, 2025 08:59:42.000000000 IST
  [Timestamp from icmp data (relative): 0.797028045 seconds]
- Data (48 bytes)
  Data: 2c8e080000000000101112131415161718191a1b1c1d1e1f20212
  [Length: 48]

```

Part-2

2.1

Unique IPs observed :

10.240.118.2
 10.240.0.1
 10.240.240.1
 117.205.73.161
 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

icmp							
No.	Time	Source	Destination	Protocol	Length	Text item	Info
23	1.0900458...	10.240.0.1	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
24	1.0900460...	10.240.0.1	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
25	1.0900461...	10.240.0.1	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
29	1.0903232...	10.240.118.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
30	1.0903234...	10.240.118.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
31	1.0903235...	10.240.118.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
32	1.0903236...	10.240.240.1	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
33	1.0903236...	10.240.240.1	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
34	1.0903237...	10.240.240.1	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
37	1.0920998...	117.205.73.161	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
38	1.0920999...	117.205.73.161	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
39	1.0920999...	117.205.73.161	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
55	1.1213833...	49.44.218.92	10.240.118.81	ICMP	110	Time-to-live exceeded	(Time to live exceeded in transit)
57	1.1258055...	49.44.218.92	10.240.118.81	ICMP	110	Time-to-live exceeded	(Time to live exceeded in transit)
59	1.1260737...	49.44.218.92	10.240.118.81	ICMP	110	Time-to-live exceeded	(Time to live exceeded in transit)
61	1.1405111...	49.44.220.189	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
63	1.1662577...	49.44.220.189	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
65	1.1701780...	49.44.220.189	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
67	1.1754194...	182.79.134.249	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
69	1.1892931...	182.79.134.249	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
71	1.2147113...	182.79.134.249	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
73	1.2193029...	125.22.133.146	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
75	1.2255813...	125.22.133.146	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
77	1.2381724...	125.22.133.146	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
79	1.2668432...	103.43.33.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
81	1.2709389...	103.43.33.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
83	1.2770473...	103.43.33.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
85	1.2887371...	103.221.208.18	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
87	1.3197275...	103.221.208.18	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
89	1.3211221...	103.221.208.18	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
90	1.3292373...	220.158.165.21	10.240.118.81	ICMP	102	Destination unreachable	(Port unreachable)
91	1.3402736...	220.158.165.21	10.240.118.81	ICMP	102	Destination unreachable	(Port unreachable)
92	1.3717961...	220.158.165.21	10.240.118.81	ICMP	102	Destination unreachable	(Port unreachable)

2.2

The '-m' flag in traceroute sets the maximum number of hops (TTL) that the probe will attempt to reach the destination. In this case, '-m 15' limits the traceroute to a maximum of 15 hops. The TTL (Time-To-Live) field in the IP header is set to 1 for the first probe, and if the destination is not reached within 15 hops, the traceroute will stop automatically. Since we have 4 hidden responses and 3 packets for each response, the total number of packets observed is $(15 - 4) * 3 = 33$.

Packets: 181 · Displayed: 33 (18.2%) · Dropped: 0 (0.0%)

2.3

Transport layer protocol used : *UDP (User Datagram Protocol)*

▶ User Datagram Protocol, Src Port: 37864, Dst Port: 33437

2.4

If a router does not respond to a probe, traceroute will display an asterisk (*) instead of an IP address or hostname, because the router drops the packet silently without sending back an ICMP response. In the captured packets in Wireshark, it is observed that the UDP packet is being sent with incremented TTL values, and no 'ICMP Time Exceeded' message from the router that did not respond. The next packet will be sent with a higher TTL value, continuing the probing process.

Part-3

3.1

The '-q' option in traceroute specifies the number of probe packets sent per hop. '-q 1' means that only one probe packet will be sent to each hop. In the captured packets in Wireshark, it is observed that the number of probe packets per hop reduces from the default (3) to 1.

3.2

The '-I' option tells traceroute to use ICMP Echo Requests instead of UDP probes. By default, traceroute on Linux uses UDP packets to random high-numbered ports (typically 33434 and above). With the '-I' option, traceroute uses ICMP Echo Requests (similar to ping), and generates ICMP Time Exceeded responses from intermediate routers.

3.3

The TTL value increases by 1 as the packet traverses each router. The first hop starts with TTL = 1, second hop with TTL = 2, and so on.

3.4

Unique IPs observed :

10.240.118.2
10.240.0.1
10.240.240.1
117.205.73.161
142.250.160.26
216.239.43.135
142.251.55.69
142.250.195.110

icmp							
No.	Time	Source	Destination	Protocol	Length	Text item	Info
59	4.703120860	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=1/256, ttl=1 (no response found!)
60	4.703133629	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=2/512, ttl=2 (no response found!)
61	4.703139313	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=3/768, ttl=3 (no response found!)
62	4.703144123	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=4/1024, ttl=4 (no response found!)
63	4.703148700	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=5/1280, ttl=5 (no response found!)
64	4.703153432	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=6/1536, ttl=6 (no response found!)
65	4.703158030	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=7/1792, ttl=7 (no response found!)
66	4.703162701	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=8/2048, ttl=8 (no response found!)
67	4.703167301	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=9/2304, ttl=9 (no response found!)
68	4.703171946	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=10/2560, ttl=10 (reply in 93)
69	4.703176444	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=11/2816, ttl=11 (reply in 95)
70	4.703180913	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=12/3072, ttl=12 (reply in 96)
71	4.703185575	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=13/3328, ttl=13 (reply in 99)
72	4.703190131	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=14/3584, ttl=14 (reply in 98)
73	4.703194654	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=15/3840, ttl=15 (reply in 97)
74	4.703199318	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=16/4096, ttl=16 (reply in 100)
75	4.703693841	10.240.118.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
76	4.703694088	10.240.0.1	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
77	4.703751310	10.240.240.1	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
80	4.705442972	117.205.73.161	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
85	4.708436425	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=17/4352, ttl=17 (reply in 104)
86	4.708453326	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=18/4608, ttl=18 (reply in 102)
87	4.708460628	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=19/4864, ttl=19 (reply in 103)
90	4.709777888	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=20/5120, ttl=20 (reply in 105)
91	4.721345931	216.239.43.135	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
92	4.721474414	10.240.118.81	142.250.195.110	ICMP	74	Echo (ping) request	id=0x0002, seq=21/5376, ttl=21 (reply in 106)
93	4.722078937	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=10/2560, ttl=58 (request in 68)
94	4.722079041	142.251.55.69	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
95	4.722079114	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=11/2816, ttl=58 (request in 69)
96	4.722079186	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=12/3072, ttl=58 (request in 70)
97	4.722079259	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=15/3840, ttl=58 (request in 73)
98	4.722079333	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=14/3584, ttl=58 (request in 72)
99	4.722079406	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=13/3328, ttl=58 (request in 71)
100	4.722079479	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=16/4096, ttl=58 (request in 74)
101	4.722518495	142.250.160.26	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
102	4.727633600	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=18/4608, ttl=58 (request in 86)
103	4.727633924	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=19/4864, ttl=58 (request in 87)
104	4.727633996	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=17/4352, ttl=58 (request in 85)
105	4.728775951	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=20/5120, ttl=58 (request in 90)
106	4.740364733	142.250.195.110	10.240.118.81	ICMP	74	Echo (ping) reply	id=0x0002, seq=21/5376, ttl=58 (request in 92)

3.5

In the captured packets in wireshark, it is observed that the intermediate routers send 'ICMP Type : 11 (Time-to-live exceeded)' packets, and the final destination sends 'ICMP Type : 0 (Echo (ping) reply)' packets.

Internet Control Message Protocol	Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)	Type: 0 (Echo (ping) reply)
Code: 0 (Time to live exceeded in	Code: 0

3.6

Each ICMP Time Exceeded message has a Source IP address that belongs to the router at that specific hop. These IP addresses represent the network nodes (routers) through which the packet is traversing. It provides the sequence of routers that the packet is traversing to reach the final destination.

icmp.type==11							
No.	Time	Source	Destination	Protocol	Length	Text item	Info
75	4.703693841	10.240.118.2	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
76	4.703694088	10.240.0.1	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
77	4.703751310	10.240.240.1	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
80	4.705442972	117.205.73.161	10.240.118.81	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
91	4.721345931	216.239.43.135	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
94	4.722079041	142.251.55.69	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)
101	4.722518495	142.250.160.26	10.240.118.81	ICMP	102	Time-to-live exceeded	(Time to live exceeded in transit)

3.7

When comparing the results of 'traceroute -I -q 1 drive.google.com' and 'traceroute drive.google.com', the key difference lies in the type of packets used and the corresponding responses received. The '-I' option instructs traceroute to use ICMP Echo Request packets, similar to the ping command, while the default traceroute uses UDP packets to high-numbered ports (typically 33434 and above). Consequently, intermediate routers in the ICMP-based traceroute respond with '*ICMP Type : 11 (Time-to-live exceeded)*' messages, and the destination responds with an '*ICMP Type : 0 (Echo (ping) reply)*'. In contrast, the default UDP-based traceroute receives '*ICMP Type : 11 (Time-to-live exceeded)*' from intermediate routers and '*ICMP Type : 3 (Port Unreachable)*' messages from the final destination. Additionally, the '-q 1' option ensures that only one probe is sent per hop, resulting in fewer captured packets in Wireshark compared to the default behavior, which typically sends three probes per hop.

Part-4

4.1

The '-s' option in the ping command specifies the size of the ICMP payload in bytes. In this case, '-s 1570' sets the ICMP payload size to 1570 bytes.

Total size of the ping request packet = ICMP Data size + ICMP Header size + IP Header size = 1562 + 8 + 20 = 1590 bytes.

4.2

Fields in ICMP Header :

- Type (1 byte)
- Code (1 byte)
- Checksum (2 bytes)
- Identifier (2 bytes)
- Sequence Number (2 bytes)

There are 6 fields in the ICMP header, with a total size of 64 bits, or 8 bytes.

```

▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x0b1f [correct]
  [Checksum Status: Good]
  Identifier (BE): 3 (0x0003)
  Identifier (LE): 768 (0x0300)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Response frame: 9]
  Timestamp from icmp data: Mar 24, 2025 10:45:02.000000000 IST
  [Timestamp from icmp data (relative): 0.469615748 seconds]
▼ Data (1562 bytes)

```

4.3

Considering standard MTU constraints, the maximum size of the packet can be 1500 bytes, including the protocol headers. Hence the maximum size of the ICMP data = maximum size of the packet - IP Header size - ICMP Header size = $1500 - 20 - 8 = 1472$ bytes.

4.4

Yes, the captured packet trace includes fragmentation for the ICMP echo request packets, as indicated by the More Fragments bit in the IP headers of the fragments. There are 2 fragments for each ICMP echo request packet, totalling to 10 fragments for all 5 ICMP echo request packets, with fragment offset values 0 (for the first fragment), and 1480 (for the last fragment).

6	0.121648317	10.240.118.81	23.10.40.18	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=41dc) [Reassembled in #7]
7	0.121658284	10.240.118.81	23.10.40.18	ICMP	132	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply in 9)

▼ Flags: 0x20, More fragments	▼ Flags: 0x00
0... = Reserved bit: Not set	0... = Reserved bit: Not set
.0.. = Don't fragment: Not set	.0.. = Don't fragment: Not set
..1. = More fragments: Set	..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0	...0 0101 1100 1000 = Fragment Offset: 1480

4.5

\$ ping -c 5 www.godaddy.com

ICMP payload size = ICMP Header size + ICMP Data size
 $= 8 + 48 = 56$ bytes

\$ ping -s 1570 -c 5 www.godaddy.com

ICMP payload size = ICMP Header size + ICMP Data size
 $= 8 + 1562 = 1570$ bytes

```

▼ Data (1562 bytes)
  Data: 542a070000
  [Length: 1562]

```

```

▼ Data (48 bytes)
  Data: 20570a00
  [Length: 48]

```