

Assignment – 2 (ICMP)

PART – 1

1. What is the IP address of your host? What is the IP address of the destination host?

A. IP address of my host is 2401:4900:1cde:8a74:d9b0:e926:c54e:1427

IP address of the destination host is 2404:6800:4007:811::2004

No.	Time	Source	Destination	Protocol	Length	Info
28	1.835912122	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=1, hop limit=64 (reply in 30)
30	1.861409382	2404:6800:4007:8...	2401:4900:1cde:8...	ICMPv6	118	Echo (ping) reply id=0x0005, seq=1, hop limit=118 (request in 28)
46	2.837895970	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=2, hop limit=64 (reply in 48)
48	2.862969118	2404:6800:4007:8...	2401:4900:1cde:8...	ICMPv6	118	Echo (ping) reply id=0x0005, seq=2, hop limit=118 (request in 46)
51	3.840057056	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=3, hop limit=64 (reply in 52)

Frame 28: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface wlp8s0, id 0	0000	b4 a7 c6 19 98 f0 b8 9a 2a 71 fa
Ethernet II, Src: IntelCor_71:fa:4d (b8:9a:2a:71:fa:4d), Dst: Serverco_19:98:f0 (b4:a7:c6:19:98:f0)	0010	5c ed 00 40 3a 40 24 01 49 00 1c
Internet Protocol Version 6, Src: 2401:4900:1cde:8a74:d9b0:e926:c54e:1427, Dst: 2404:6800:4007:811::2004	0020	e9 26 c5 4e 14 27 24 04 68 00 40
0110 = Version: 6	0030	00 00 00 00 20 04 80 00 13 60 00
.... 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)	0040	0e 66 00 00 00 00 04 95 0b 00 00
.... 0100 0101 1100 1101 = Flow Label: 0x45ced	0050	12 13 14 15 16 17 18 19 1a 1b 1c
Payload Length: 64	0060	22 23 24 25 26 27 28 29 2a 2b 2c
Next Header: ICMPv6 (58)	0070	32 33 34 35 36 37
Hop Limit: 64		
Source Address: 2401:4900:1cde:8a74:d9b0:e926:c54e:1427		
Destination Address: 2404:6800:4007:811::2004		
[Source GeoIP: IN]		
[Destination GeoIP: AU]		
Internet Control Message Protocol v6		
Type: Echo (ping) request (128)		
Code: 0		
Checksum: 0x1360 [correct]		
[Checksum Status: Good]		
Identifier: 0x0005		
Sequence: 1		
[Response In: 30]		
Data (56 bytes)		

2. Why is it that an ICMP packet does not have source and destination port numbers?

A. ICMP packet is a network layer protocol.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

A. ICMP Type is 128 and Code number is 0

Other fields are checksum, sequence number, identifier and data field

Checksum is 2 bytes

Identifier is 2 bytes

Sequence number is 2 bytes

No.	Time	Source	Destination	Protocol	Length	Info
28	1.835912122	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=1, hop limit=64 (reply in 30)
30	1.861409382	2404:6800:4007:8...	2401:4900:1cde:8...	ICMPv6	118	Echo (ping) reply id=0x0005, seq=1, hop limit=118 (request in 28)
46	2.837895970	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=2, hop limit=64 (reply in 48)
48	2.862969118	2404:6800:4007:8...	2401:4900:1cde:8...	ICMPv6	118	Echo (ping) reply id=0x0005, seq=2, hop limit=118 (request in 46)
51	3.840057056	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=3, hop limit=64 (reply in 52)

Frame 28: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface wlp8s0, id 0	0000	b4 a7 c6 19 98 f0 b8 9a 2a 71 fa
Ethernet II, Src: IntelCor_71:fa:4d (b8:9a:2a:71:fa:4d), Dst: Serverco_19:98:f0 (b4:a7:c6:19:98:f0)	0010	5c ed 00 40 3a 40 24 01 49 00 1c
Internet Protocol Version 6, Src: 2401:4900:1cde:8a74:d9b0:e926:c54e:1427, Dst: 2404:6800:4007:811::2004	0020	e9 26 c5 4e 14 27 24 04 68 00 40
0110 = Version: 6	0030	00 00 00 00 20 04 80 00 13 60 00
.... 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)	0040	0e 66 00 00 00 00 04 95 0b 00 00
.... 0100 0101 1100 1101 = Flow Label: 0x45ced	0050	12 13 14 15 16 17 18 19 1a 1b 1c
Payload Length: 64	0060	22 23 24 25 26 27 28 29 2a 2b 2c
Next Header: ICMPv6 (58)	0070	32 33 34 35 36 37
Hop Limit: 64		
Source Address: 2401:4900:1cde:8a74:d9b0:e926:c54e:1427		
Destination Address: 2404:6800:4007:811::2004		
[Source GeoIP: IN]		
[Destination GeoIP: AU]		
Internet Control Message Protocol v6		
Type: Echo (ping) request (128)		
Code: 0		
Checksum: 0x1360 [correct]		
[Checksum Status: Good]		
Identifier: 0x0005		
Sequence: 1		
[Response In: 30]		
Data (56 bytes)		

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

A. ICMP Type is 129 and Code number is 0

Other fields are checksum, sequence number, identifier and data field

Checksum is 2 bytes

Identifier is 2 bytes

Sequence number is 2 bytes

No.	Time	Source	Destination	Protocol	Length	Info
28	1.835912122	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=1, hop limit=64 (reply in 30)
30	1.861409382	2404:6800:4007:8...	2401:4900:1cde:8...	ICMPv6	118	Echo (ping) reply id=0x0005, seq=1, hop limit=118 (request in 28)
46	2.837895970	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=2, hop limit=64 (reply in 48)
48	2.862969118	2404:6800:4007:8...	2401:4900:1cde:8...	ICMPv6	118	Echo (ping) reply id=0x0005, seq=2, hop limit=118 (request in 46)
51	3.840057056	2401:4900:1cde:8...	2404:6800:4007:8...	ICMPv6	118	Echo (ping) request id=0x0005, seq=3, hop limit=64 (reply in 52)

Frame 30: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface wlp8s0, id 0	0000	b8 9a 2a 71 fa 4d b4 a7 c6 19 98
Ethernet II, Src: Serverco_19:98:f0 (b4:a7:c6:19:98:f0), Dst: IntelCor_71:fa:4d (b8:9a:2a:71:fa:4d)	0010	5c ed 00 40 3a 76 24 04 68 00 40
Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:1cde:8a74:d9b0:e926:c54e:1427	0020	00 00 00 00 20 04 24 01 49 00 1c
0110 = Version: 6	0030	e9 26 c5 4e 14 27 81 00 12 60 00
.... 1011 1000 = Traffic Class: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)	0040	0e 66 00 00 00 00 04 95 0b 00 00
.... 0100 0101 1100 1101 = Flow Label: 0x45ced	0050	12 13 14 15 16 17 18 19 1a 1b 1c
Payload Length: 64	0060	22 23 24 25 26 27 28 29 2a 2b 2c
Next Header: ICMPv6 (58)	0070	32 33 34 35 36 37
Hop Limit: 118		
Source Address: 2404:6800:4007:811::2004		
Destination Address: 2401:4900:1cde:8a74:d9b0:e926:c54e:1427		
[Source GeoIP: AU]		
[Destination GeoIP: IN]		
Internet Control Message Protocol v6		
Type: Echo (ping) reply (129)		
Code: 0		
Checksum: 0x1260 [correct]		
[Checksum Status: Good]		
Identifier: 0x0005		
Sequence: 1		
[Response To: 28]		
[Response Time: 25.497 ms]		
Data (56 bytes)		

PART – II

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

A.

The image shows a Wireshark packet capture interface. The top pane displays a list of network packets. The bottom pane shows the detailed view of the selected packet (No. 235).

No.	Time	Source	Destination	Protocol	Length	Info
235	1.292967128	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=1/256, ttl=1 (no response found!)
236	1.293005782	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=2/512, ttl=1 (no response found!)
237	1.293015492	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=3/768, ttl=1 (no response found!)
238	1.293027029	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=4/1024, ttl=2 (no response found!)
239	1.293036071	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=5/1280, ttl=2 (no response found!)
240	1.293044427	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=6/1536, ttl=2 (no response found!)
241	1.293053799	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=7/1792, ttl=3 (no response found!)
242	1.293062347	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=8/2048, ttl=3 (no response found!)
243	1.293070462	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=9/2304, ttl=3 (no response found!)
244	1.293081480	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=10/2560, ttl=4 (no response found!)
245	1.293090746	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=11/2816, ttl=4 (no response found!)
246	1.293100424	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=12/3072, ttl=4 (no response found!)
247	1.293110823	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=13/3328, ttl=5 (no response found!)
248	1.293119263	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=14/3584, ttl=5 (no response found!)
249	1.293127404	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=15/3840, ttl=5 (no response found!)
250	1.293138027	192.168.1.15	142.250.195.174	ICMP	78	Echo (ping) request id=0x0013, seq=16/4096, ttl=6 (no response found!)
251	1.301419557	192.168.1.1	192.168.1.15	ICMP	106	Time-to-live exceeded (Time to live exceeded in transit)
252	1.301562730	192.168.1.1	192.168.1.15	ICMP	106	Time-to-live exceeded (Time to live exceeded in transit)

Frame 235: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface Ethernet II, Src: IntelCor_71:fa:4d (b8:9a:2a:71:fa:4d), Dst: Serverco_19:98:f0

Internet Protocol Version 4, Src: 192.168.1.15, Dst: 142.250.195.174

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 00.. = Differentiated Services Codepoint: Default (0)
-00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 64
- Identification: 0x1a5d (6749)
- 000. = Flags: 0x0
- 0... = Reserved bit: Not set
- .0.. = Don't fragment: Not set
- ..0. = More fragments: Not set
- ...0 0000 0000 0000 = Fragment Offset: 0
- ▼ Time to Live: 1
- ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
- ["Time To Live" only 1]
- [Severity level: Note]
- [Group: Sequence]
- Protocol: ICMP (1)
- Header Checksum: 0x8b00 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.15
- Destination Address: 142.250.195.174
- [Destination GeoIP: US]
- Internet Control Message Protocol

2. Which of the IP datagrams are fragmented?

A. Whenever data exceeds 1500 bytes, IP datagrams are fragmented.

No.	Time	Source	Destination	Protocol	Length	Info
1016	24.264793583	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=80/20480, ttl=27 (no response found!)
1019	24.264819714	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=81/20736, ttl=27 (no response found!)
1022	24.264847598	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=82/20992, ttl=28 (no response found!)
1025	24.264872974	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=83/21248, ttl=28 (no response found!)
1028	24.264897604	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=84/21504, ttl=28 (no response found!)
1031	24.264922551	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=85/21760, ttl=29 (no response found!)
1034	24.264949006	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=86/22016, ttl=29 (no response found!)
1037	24.264974768	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=87/22272, ttl=29 (no response found!)
1040	24.265000507	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=88/22528, ttl=30 (no response found!)
1043	24.265024678	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=89/22784, ttl=30 (no response found!)
1046	24.265047995	192.168.1.15	142.250.195.174	ICMP	54	Echo (ping) request id=0x0014, seq=90/23040, ttl=30 (no response found!)
<p>Frame 1040: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface wlp8s0, id 0</p> <p>Ethernet II, Src: IntelCor_71:fa:4d (b8:9a:2a:71:fa:4d), Dst: Serverco_19:98:f0 (b4:a7:c6:19:98:f0)</p> <p>Internet Protocol Version 4, Src: 192.168.1.15, Dst: 142.250.195.174</p> <p>0100 = Version: 4</p> <p>.... 0101 = Header Length: 20 bytes (5)</p> <p>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</p> <p>Total Length: 40</p> <p>Identification: 0x4b79 (19321)</p> <p>0000 = Flags: 0x0</p> <p>...0 0001 0111 0010 = Fragment Offset: 2960</p> <p>Time to Live: 30</p> <p>Protocol: ICMP (1)</p> <p>Header Checksum: 0x3b8a [validation disabled]</p> <p>[Header checksum status: Unverified]</p> <p>Source Address: 192.168.1.15</p> <p>Destination Address: 142.250.195.174</p> <p>[Destination GeoIP: US]</p> <p>[3 IPv4 Fragments (2980 bytes): #1038(1480), #1039(1480), #1040(20)]</p> <p>[Frame: 1038, payload: 0-1479 (1480 bytes)]</p> <p>[Frame: 1039, payload: 1480-2959 (1480 bytes)]</p> <p>[Frame: 1040, payload: 2960-2979 (20 bytes)]</p> <p>[Fragment count: 3]</p> <p>[Reassembled IPv4 length: 2980]</p> <p>[Reassembled IPv4 data: 0800e2b60014005848494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f60616263...]</p> <p>Internet Control Message Protocol</p>						

3. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

A. Identification, Time to live and Header checksum fields always change.

4. Which fields stay constant? Why?

A. The fields that stay constant across the IP datagrams are:

- Version (since we are using IPv4 for all packets)
- Header length (since these are ICMP packets)
- Source IP (since we are sending from the same source)
- Destination IP (since we are sending to the same dest)
- Differentiated Services (since all packets are ICMP they use the same Type of Service class)
- Upper Layer Protocol (since these are ICMP packets)

These fields are essential for routing and processing the IP datagram across the network and remain constant to ensure proper delivery and handling of the packet by intermediate routers and the final destination.