



Gökhan Özeloğlu - 21627557

Burak Yılmaz - 21627868

BBM 453 Computer Networks Lab - IP Lab Assignment

Group ID: 1

**Note: We were using windows that's why we worked with ICMP protocol rather than UDP
as it is mentioned in lab assignment PDF.**

1. Select the first UDP segment message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

ANS: My ip address is 192.168.1.35

20	8.461253	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=2665/26890, ttl=255 (reply in 29)
21	8.499545	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=2666/27146, ttl=1 (no response found!)
22	8.509711	192.168.1.35	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
23	8.516469	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x0a46 PTR 1.1.168.192.in-addr.arpa
24	8.518379	192.168.1.1	192.168.1.35	DNS	112 Standard query response 0x0a46 PTR 1.1.168.192.in-addr.arpa PTR MitraStar.Home
25	8.539588	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=2667/27402, ttl=2 (no response found!)
26	8.557567	212.156.201.18	192.168.1.35	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
27	8.578497	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=2668/27658, ttl=3 (no response found!)
28	8.584677	81.212.78.245	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
29	8.601188	128.119.245.12	192.168.1.35	ICMP	70 Echo (ping) reply id=0x0001, seq=2665/26890, ttl=40 (request in 20)
30	8.618895	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=2669/27914, ttl=4 (no response found!)
31	8.628779	81.212.211.207	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
32	8.659276	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=2670/28170, ttl=5 (no response found!)
33	8.666859	212.156.108.248	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)

Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)	
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 56	
Identification: 0xec35 (60469)	
Flags: 0x0000	
0... .. = Reserved bit: Not set	
.0... .. = Don't fragment: Not set	
..0... .. = More fragments: Not set	
Fragment offset: 0	
Time to live: 255	
Protocol: ICMP (1)	
Header checksum: 0x983f [validation disabled]	
[Header checksum status: Unverified]	
Source: 192.168.1.35	
Destination: 128.119.245.12	
> Internet Control Message Protocol	

0000	08 26 97 35 a4 27 48 45 20 d6 b0 37 08 00 45 00	&S'HE --7--E:
0010	00 38 ec 35 00 00 ff 01 98 3f c0 a8 01 23 80 77	-8-S-...-?...#-W
0020	f5 0c 08 00 2b d4 00 01 0a 69 20 20 20 20 20 20	...-...-i
0030	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0040	20 20 20 20 20 20	

2. Within the IP packet header, what is the value in the upper layer protocol field?

ANS: As you can see from the above screenshot with the highlighted part the value in the upper layer protocol is ICMP(1)

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

ANS: Header bytes: 20 (as you can seen in screenshot with the highlighted parts)

Payload bytes: 36 (total length 56 minus the 20 header bytes = 36)

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

ANS: According to the screenshot above , under flags section, the more fragments bit = 0, so the data is not fragmented.

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

ANS: As you can see the screenshots(example of 3 screenshots) below the identification, Time to live and Header checksum fields are always changing.

298	17.178295	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2767/53002, ttl=24 (reply in 302)
297	17.128003	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2766/52746, ttl=23 (no response found!)
295	17.077223	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2765/52490, ttl=22 (no response found!)
292	17.039367	192.168.1.35	172.217.169.202	TCP	55 53179 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]	
291	17.027099	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2764/52234, ttl=21 (no response found!)
289	16.976329	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2763/51978, ttl=20 (no response found!)
287	16.926172	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2762/51722, ttl=19 (no response found!)
285	16.876092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2761/51466, ttl=18 (no response found!)
283	16.825443	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2760/51210, ttl=17 (no response found!)
282	16.774975	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2759/50954, ttl=16 (no response found!)
280	16.724736	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2758/50698, ttl=15 (no response found!)
278	16.673090	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2757/50442, ttl=14 (no response found!)
276	16.623092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2756/50186, ttl=13 (no response found!)
274	16.573143	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2755/49930, ttl=12 (no response found!)
> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)						
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 56						
Identification: 0xec9b (60571)						
Flags: 0x0000						
0... .. = Reserved bit: Not set						
.0... .. = Don't fragment: Not set						
..0... .. = More fragments: Not set						
Fragment offset: 0						
Time to live: 24						
Protocol: ICMP (1)						
Header checksum: 0x7eda [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.1.35						
Destination: 128.119.245.12						
> Internet Control Message Protocol						
298	17.178295	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2767/53002, ttl=24 (reply in 302)
297	17.128003	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2766/52746, ttl=23 (no response found!)
295	17.077223	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2765/52490, ttl=22 (no response found!)
292	17.039367	192.168.1.35	172.217.169.202	TCP	55 53179 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]	
291	17.027099	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2764/52234, ttl=21 (no response found!)
289	16.976329	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2763/51978, ttl=20 (no response found!)
287	16.926172	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2762/51722, ttl=19 (no response found!)
285	16.876092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2761/51466, ttl=18 (no response found!)
283	16.825443	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2760/51210, ttl=17 (no response found!)
282	16.774975	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2759/50954, ttl=16 (no response found!)
280	16.724736	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2758/50698, ttl=15 (no response found!)
278	16.673090	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2757/50442, ttl=14 (no response found!)
276	16.623092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2756/50186, ttl=13 (no response found!)
274	16.573143	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2755/49930, ttl=12 (no response found!)
> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)						
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 56						
Identification: 0xec9a (60570)						
Flags: 0x0000						
0... .. = Reserved bit: Not set						
.0... .. = Don't fragment: Not set						
..0... .. = More fragments: Not set						
Fragment offset: 0						
Time to live: 23						
Protocol: ICMP (1)						
Header checksum: 0x7fdb [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.1.35						
Destination: 128.119.245.12						
> Internet Control Message Protocol						
298	17.178295	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2767/53002, ttl=24 (reply in 302)
297	17.128003	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2766/52746, ttl=23 (no response found!)
295	17.077223	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2765/52490, ttl=22 (no response found!)
292	17.039367	192.168.1.35	172.217.169.202	TCP	55 53179 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]	
291	17.027099	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2764/52234, ttl=21 (no response found!)
289	16.976329	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2763/51978, ttl=20 (no response found!)
287	16.926172	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2762/51722, ttl=19 (no response found!)
285	16.876092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2761/51466, ttl=18 (no response found!)
283	16.825443	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2760/51210, ttl=17 (no response found!)
282	16.774975	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2759/50954, ttl=16 (no response found!)
280	16.724736	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2758/50698, ttl=15 (no response found!)
278	16.673090	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2757/50442, ttl=14 (no response found!)
276	16.623092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2756/50186, ttl=13 (no response found!)
274	16.573143	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2755/49930, ttl=12 (no response found!)
> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)						
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 56						
Identification: 0xec99 (60569)						
Flags: 0x0000						
0... .. = Reserved bit: Not set						
.0... .. = Don't fragment: Not set						
..0... .. = More fragments: Not set						
Fragment offset: 0						
Time to live: 22						
Protocol: ICMP (1)						
Header checksum: 0x000c [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.1.35						
Destination: 128.119.245.12						
> Internet Control Message Protocol						

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

ANS: Yellow ones are always changing, green ones always stay the same. You can compare two example screenshots.

298	17.178295	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2767/53002, ttl=24 (reply in 302)
297	17.128003	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2766/52746, ttl=23 (no response found!)
295	17.077223	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2765/52490, ttl=22 (no response found!)
292	17.039367	192.168.1.35	172.217.169.202	TCP	55 53179 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]	
291	17.027099	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2764/52234, ttl=21 (no response found!)
289	16.976329	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2763/51978, ttl=20 (no response found!)
287	16.926172	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2762/51722, ttl=19 (no response found!)
285	16.876092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2761/51466, ttl=18 (no response found!)
283	16.825443	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2760/51210, ttl=17 (no response found!)
282	16.774975	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2759/50954, ttl=16 (no response found!)
280	16.724736	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2758/50698, ttl=15 (no response found!)
278	16.673890	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2757/50442, ttl=14 (no response found!)
276	16.623092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2756/50186, ttl=13 (no response found!)
274	16.573143	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2755/49930, ttl=12 (no response found!)

Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)

Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 35

Identification: 0xec9b (60571)

Flags: 0x0000

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 24

Protocol: ICMP (1)

Header checksum: 0x7eda [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

Internet Control Message Protocol

298	17.178295	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2767/53002, ttl=24 (reply in 302)
297	17.128003	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2766/52746, ttl=23 (no response found!)
295	17.077223	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2765/52490, ttl=22 (no response found!)
292	17.039367	192.168.1.35	172.217.169.202	TCP	55 53179 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]	
291	17.027099	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2764/52234, ttl=21 (no response found!)
289	16.976329	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2763/51978, ttl=20 (no response found!)
287	16.926172	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2762/51722, ttl=19 (no response found!)
285	16.876092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2761/51466, ttl=18 (no response found!)
283	16.825443	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2760/51210, ttl=17 (no response found!)
282	16.774975	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2759/50954, ttl=16 (no response found!)
280	16.724736	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2758/50698, ttl=15 (no response found!)
278	16.673890	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2757/50442, ttl=14 (no response found!)
276	16.623092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2756/50186, ttl=13 (no response found!)
274	16.573143	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2755/49930, ttl=12 (no response found!)

Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)

Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 35

Identification: 0xec9a (60570)

Flags: 0x0000

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 23

Protocol: ICMP (1)

Header checksum: 0x7fdb [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

Internet Control Message Protocol

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)

The fields that must stay constant 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)

The fields that must change are:

- Identification(IP packets must have different ids)
- Time to live (traceroute increments each subsequent packet)
- Header checksum (since header changes, so must checksum)

7. Describe the pattern you see in the values in the Identification field of the IP datagram

ANS: The pattern is that the IP header Identification fields increment with each ICMP Echo (ping) request as you can see below screenshots.

298	17.178295	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2767/53002, ttl=24 (reply in 302)
297	17.128003	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2766/52746, ttl=23 (no response found!)
295	17.077223	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2765/52490, ttl=22 (no response found!)
292	17.039367	192.168.1.35	172.217.169.202	TCP	55 53179 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]	
291	17.027099	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2764/52234, ttl=21 (no response found!)
289	16.976329	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2763/51978, ttl=20 (no response found!)
287	16.926172	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2762/51722, ttl=19 (no response found!)
285	16.876092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2761/51466, ttl=18 (no response found!)
283	16.825443	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2760/51210, ttl=17 (no response found!)
282	16.774975	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2759/50954, ttl=16 (no response found!)
280	16.724736	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2758/50698, ttl=15 (no response found!)
278	16.673890	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2757/50442, ttl=14 (no response found!)
276	16.623092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2756/50186, ttl=13 (no response found!)
274	16.573143	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2755/49930, ttl=12 (no response found!)

<

>

> Frame 297: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACAD-E87503A65ADC}, id 0

> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxelCom_35:a4:27 (08:26:97:35:a4:27)

▼ Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0xec9a (60570)

> Flags: 0x0000

Fragment offset: 0

Time to live: 23

Protocol: ICMP (1)

Header checksum: 0x7fdb [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

> Internet Control Message Protocol

Identification number = 60570

298	17.178295	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2767/53002, ttl=24 (reply in 302)	
297	17.128003	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2766/52746, ttl=23 (no response found!)	
295	17.077223	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2765/52490, ttl=22 (no response found!)	
292	17.039367	192.168.1.35	172.217.169.202	TCP	55 53179 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]		
291	17.027099	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2764/52234, ttl=21 (no response found!)	
289	16.976329	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2763/51978, ttl=20 (no response found!)	
287	16.926172	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2762/51722, ttl=19 (no response found!)	
285	16.876092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2761/51466, ttl=18 (no response found!)	
283	16.825443	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2760/51210, ttl=17 (no response found!)	
282	16.774975	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2759/50954, ttl=16 (no response found!)	
280	16.724736	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2758/50698, ttl=15 (no response found!)	
278	16.673890	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2757/50442, ttl=14 (no response found!)	
276	16.623092	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2756/50186, ttl=13 (no response found!)	
274	16.573143	192.168.1.35	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=2755/49930, ttl=12 (no response found!)	

< >

> Frame 298: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACAD-E87503A65ADC}, id 0

> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

> 0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0xec9b (60571)

> Flags: 0x0000

Fragment offset: 0

Time to live: 24

Protocol: ICMP (1)

Header checksum: 0x7eda [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

> Internet Control Message Protocol

Identification number = 60571

8. What is the value in the Identification field and the TTL field?

Nearest router ip address is 192.168.1.1 as you can see below.

gaia.cs.umass.edu						Interval	2,5 seconds	Focus	
Hop	Count	IP	Name	Avg	Min	Cur	PL%		
1	5	192.168.1.1	MitraStar.Home	3,2	1,9	2,8			
2	5	212.156.201.18	212.156.201.18.static.turktelekom.com.tr	11,7	7,4	7,4			
3	5	81.212.78.245	81.212.78.245.static.turktelekom.com.tr	7,8	6,3	6,9			
4	5	81.212.211.207	06-balgat-t2-2---06-balgat-t3-3.statik.turktele	9,0	7,3	7,7			
5	5	212.156.108.248	06-ulus-xrs-t2-2---06-balgat-t2-2.statik.turkte	11,1	7,7	10,2			
6	4	81.212.217.121	06-ebgp-ulus-sr12e-k---06-ulus-xrs-t2-2.stat	7,7	7,7	*	75,0		
7	5	212.156.101.126	301-fra-col-1---06-ulus-xrs-t2-1.statik.turktele	51,0	49,8	52,5			
8	5	213.198.83.197	213.198.83.197	61,1	55,4	56,3			
9	5	129.250.4.76	ae-4.r20.frnkge13.de.bb.gin.ntt.net	59,9	56,1	59,3			
10	5	129.250.6.14	ae-3.r00.frnkge13.de.bb.gin.ntt.net	68,9	56,8	59,2			
11	5	130.117.14.129	be2914.agr41.fra03.atlas.cogentco.com	64,3	57,0	58,6			

ANS: Identification field = 22340 , TTL = 64

252	16.018783	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)		
197	13.516081	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)		
144	11.003591	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)		
135	9.680143	192.168.1.1	192.168.1.35	DNS	130 Standard query response 0xc128 PTR 113.83.80.192.in-addr.arpa PTR core2-rt-et-8-3-0.gw.umass.edu		
133	9.655997	192.168.1.1	192.168.1.35	DNS	124 Standard query response 0x9990 PTR 253.240.119.128.in-addr.arpa PTR nscs1bbs1.cs.umass.edu		
131	9.633375	192.168.1.1	192.168.1.35	DNS	128 Standard query response 0xbedd PTR 32.3.119.128.in-addr.arpa PTR cics-rt-xe-0-0-0.gw.umass.edu		
129	9.579835	192.168.1.1	192.168.1.35	DNS	131 Standard query response 0x2ab4 PTR 10.0.119.128.in-addr.arpa PTR n5-rt-1-1-et-10-0-0.gw.umass.edu		
108	9.360412	192.168.1.1	192.168.1.35	DNS	144 Standard query response 0x50e6 No such name PTR 14.218.104.38.in-addr.arpa SOA auth1.dns.cogentco.com		
99	9.298262	192.168.1.1	192.168.1.35	DNS	138 Standard query response 0xae00 PTR 26.6.54.154.in-addr.arpa PTR te0-3-1-5.pcr51.orh01.atlas.cogentco.com		
95	9.288586	192.168.1.1	192.168.1.35	DNS	136 Standard query response 0xa32a PTR 38.82.54.154.in-addr.arpa PTR be2101.ccr32.bos01.atlas.cogentco.com		
83	9.167713	192.168.1.1	192.168.1.35	DNS	138 Standard query response 0x5db6 PTR 41.51.117.130.in-addr.arpa PTR be12488.ccr42.lon13.atlas.cogentco.com		
81	9.151685	192.168.1.1	192.168.1.35	DNS	137 Standard query response 0x8c53 PTR 118.1.117.130.in-addr.arpa PTR be3187.ccr42.fra03.atlas.cogentco.com		
80	9.147758	192.168.1.1	192.168.1.35	DNS	137 Standard query response 0x81ac PTR 141.0.117.130.in-addr.arpa PTR be2814.ccr42.ams03.atlas.cogentco.com		
76	9.119218	192.168.1.1	224.0.0.1	IGMPv2	46 Membership Query, general		

< >

> Frame 252: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACAD-E87503A65ADC}, id 0

> Ethernet II, Src: ZyxeCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35

> 0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS6, ECN: Not-ECT)

Total Length: 84

Identification: 0x5744 (22340)

> Flags: 0x0000

Fragment offset: 0

Time to live: 64

Protocol: ICMP (1)

Header checksum: 0x9f30 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.1

Destination: 192.168.1.35

> Internet Control Message Protocol

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

ANS: The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

The TTL field remains unchanged because the TTL for the first hop router is always the same.

You can see the below with two screenshots.

252.16.0.18783	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
197.13.516081	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
144.11.003591	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
135.9.680143	192.168.1.1	192.168.1.35	DNS	130 Standard query response 0xc128 PTR 113.83.80.192.in-addr.arpa PTR core2-rt-et-8-3-0.gw.umass.edu
133.9.655997	192.168.1.1	192.168.1.35	DNS	124 Standard query response 0x9990 PTR 253.240.119.128.in-addr.arpa PTR nscs1bbs1.cs.umass.edu
131.9.633375	192.168.1.1	192.168.1.35	DNS	128 Standard query response 0xebbd PTR 32.3.119.128.in-addr.arpa PTR cics-rt-xe-0-0-0.gw.umass.edu
129.9.579835	192.168.1.1	192.168.1.35	DNS	131 Standard query response 0x2ab4 PTR 10.0.119.128.in-addr.arpa PTR n5-rt-1-1-et-10-0-0.gw.umass.edu
108.9.360412	192.168.1.1	192.168.1.35	DNS	144 Standard query response 0x50e6 No such name PTR 14.218.104.38.in-addr.arpa SOA auth1.dns.cogentco.com
99.9.298262	192.168.1.1	192.168.1.35	DNS	138 Standard query response 0x1ea0 PTR 26.6.54.154.in-addr.arpa PTR te0-3-1-5.rcr51.orth01.atlas.cogentco.com
95.9.280586	192.168.1.1	192.168.1.35	DNS	136 Standard query response 0xa32a PTR 38.82.54.154.in-addr.arpa PTR be2101.ccr32.bos01.atlas.cogentco.com
83.9.167713	192.168.1.1	192.168.1.35	DNS	138 Standard query response 0x5db6 PTR 41.51.117.130.in-addr.arpa PTR be12488.ccr42.lon13.atlas.cogentco.com
81.9.151685	192.168.1.1	192.168.1.35	DNS	137 Standard query response 0xbc53 PTR 118.1.117.130.in-addr.arpa PTR be3187.ccr42.fra03.atlas.cogentco.com
80.9.147758	192.168.1.1	192.168.1.35	DNS	137 Standard query response 0x81ac PTR 141.0.117.130.in-addr.arpa PTR be2814.ccr42.ams03.atlas.cogentco.com
76.9.119218	192.168.1.1	224.0.0.1	IGMPv2	46 Membership Query, general

< >

> Frame 197: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACAD-E87503A65ADC}, id 0

> Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 84

Identification: 0x5743 (22339)

> Flags: 0x0000

Fragment offset: 0

Time to live: 64

Protocol: ICMP (1)

Header checksum: 0x9f31 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.1

Destination: 192.168.1.35

> Internet Control Message Protocol

252.16.0.18783	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
197.13.516081	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
144.11.003591	192.168.1.1	192.168.1.35	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
135.9.680143	192.168.1.1	192.168.1.35	DNS	130 Standard query response 0xc128 PTR 113.83.80.192.in-addr.arpa PTR core2-rt-et-8-3-0.gw.umass.edu
133.9.655997	192.168.1.1	192.168.1.35	DNS	124 Standard query response 0x9990 PTR 253.240.119.128.in-addr.arpa PTR nscs1bbs1.cs.umass.edu
131.9.633375	192.168.1.1	192.168.1.35	DNS	128 Standard query response 0xebbd PTR 32.3.119.128.in-addr.arpa PTR cics-rt-xe-0-0-0.gw.umass.edu
129.9.579835	192.168.1.1	192.168.1.35	DNS	131 Standard query response 0x2ab4 PTR 10.0.119.128.in-addr.arpa PTR n5-rt-1-1-et-10-0-0.gw.umass.edu
108.9.360412	192.168.1.1	192.168.1.35	DNS	144 Standard query response 0x50e6 No such name PTR 14.218.104.38.in-addr.arpa SOA auth1.dns.cogentco.com
99.9.298262	192.168.1.1	192.168.1.35	DNS	138 Standard query response 0x1ea0 PTR 26.6.54.154.in-addr.arpa PTR te0-3-1-5.rcr51.orth01.atlas.cogentco.com
95.9.280586	192.168.1.1	192.168.1.35	DNS	136 Standard query response 0xa32a PTR 38.82.54.154.in-addr.arpa PTR be2101.ccr32.bos01.atlas.cogentco.com
83.9.167713	192.168.1.1	192.168.1.35	DNS	138 Standard query response 0x5db6 PTR 41.51.117.130.in-addr.arpa PTR be12488.ccr42.lon13.atlas.cogentco.com
81.9.151685	192.168.1.1	192.168.1.35	DNS	137 Standard query response 0xbc53 PTR 118.1.117.130.in-addr.arpa PTR be3187.ccr42.fra03.atlas.cogentco.com
80.9.147758	192.168.1.1	192.168.1.35	DNS	137 Standard query response 0x81ac PTR 141.0.117.130.in-addr.arpa PTR be2814.ccr42.ams03.atlas.cogentco.com
76.9.119218	192.168.1.1	224.0.0.1	IGMPv2	46 Membership Query, general

< >

> Frame 252: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACAD-E87503A65ADC}, id 0

> Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 84

Identification: 0x5744 (22340)

> Flags: 0x0000

Fragment offset: 0

Time to live: 64

Protocol: ICMP (1)

Header checksum: 0x9f30 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.1

Destination: 192.168.1.35

10. Find the first UDP segment message that was sent by your computer after you changed the Packet to be 12000. Has that message been fragmented across more than one IP datagram?

ANS: Yes, this packet has been fragmented across more than one IP datagram

281	16.578575	192.168.1.35	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ecdb) [Reassembled in #282]
280	16.539197	192.168.1.35	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=2836/5131, ttl=62 (no response found!)
279	16.539197	192.168.1.35	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ecda) [Reassembled in #280]
278	16.500283	192.168.1.35	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=2835/4875, ttl=61 (no response found!)
277	16.500283	192.168.1.35	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ecd9) [Reassembled in #278]
276	16.460679	192.168.1.35	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=2834/4619, ttl=60 (no response found!)
275	16.460679	192.168.1.35	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ecd8) [Reassembled in #276]
274	16.422604	192.168.1.35	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=2833/4363, ttl=59 (no response found!)
273	16.422604	192.168.1.35	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ecd7) [Reassembled in #274]
272	16.383580	192.168.1.35	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=2832/4107, ttl=58 (no response found!)
271	16.383580	192.168.1.35	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ecd6) [Reassembled in #272]
270	16.344281	192.168.1.35	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=2831/3851, ttl=57 (no response found!)
269	16.344281	192.168.1.35	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ecd5) [Reassembled in #270]
268	16.306082	192.168.1.35	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=2830/3595, ttl=56 (no response found!)

```

> Frame 281: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)
< Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xecdb (60635)
  < Flags: 0x2000, More fragments
    0... .. = Reserved bit: Not set
    .0... .. = Don't fragment: Not set
    ..1... .. = More fragments: Set
  Fragment offset: 0
  Time to live: 63
  Protocol: ICMP (1)
  Header checksum: 0x31f6 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.35
  Destination: 128.119.245.12

```

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

ANS: According to the screenshot below, The Flags bit for more fragments is set to 1 which means the datagram has been fragmented. The fragment offset is 0, we know this is the first fragment. The length of this first datagram is 1500 including the header

136	14.124347	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2774/54794, ttl=255 (no response found!)
138	14.162448	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2775/55050, ttl=1 (no response found!)
140	14.166171	192.168.1.1	192.168.1.35	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
143	14.202371	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2776/55306, ttl=2 (no response found!)
145	14.240604	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2777/55562, ttl=3 (no response found!)
147	14.279746	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2778/55818, ttl=4 (no response found!)
149	14.317937	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2779/56074, ttl=5 (no response found!)
151	14.357722	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2780/56330, ttl=6 (no response found!)
153	14.396380	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2781/56586, ttl=7 (no response found!)
155	14.436502	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2782/56842, ttl=8 (no response found!)
157	14.474798	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2783/57098, ttl=9 (no response found!)
159	14.514344	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2784/57354, ttl=10 (no response found!)
161	14.552973	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2785/57610, ttl=11 (no response found!)
163	14.592148	192.168.1.35	128.119.245.12	ICMP	1514	Echo (ping) request id=0x0001, seq=2786/57866, ttl=12 (no response found!)

```

> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)
< Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xec9c (60572)
  < Flags: 0x2000, More fragments
    0... .. = Reserved bit: Not set
    .0... .. = Don't fragment: Not set
    ..1... .. = More fragments: Set
  Fragment offset: 0
  Time to live: 255
  Protocol: ICMP (1)
  Header checksum: 0x7234 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.35
  Destination: 128.119.245.12

```


12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

ANS: According to the below screenshot, this is not the first fragment since the fragment offset is 1480 and this should be the last fragment, since the status of more fragments flag is not set.

136	14.124347	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9c) [Reassembled in #137]
137	14.124347	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2774/54784, ttl=255 (no response found!)
138	14.162440	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9c) [Reassembled in #139]
139	14.162440	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2775/55050, ttl=1 (no response found!)
140	14.166171	192.168.1.1	192.168.1.35	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)
141	14.195151	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6475 PTR 1.1.168.192.in-addr.arpa
142	14.197177	192.168.1.1	192.168.1.35	DNS	112 Standard query response 0x6475 PTR 1.1.168.192.in-addr.arpa PTR MitraStar.Home
143	14.202371	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9e) [Reassembled in #144]
144	14.202371	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2776/55306, ttl=2 (no response found!)
145	14.240604	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9f) [Reassembled in #146]
146	14.240604	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2777/55562, ttl=3 (no response found!)
147	14.279746	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=eca0) [Reassembled in #148]
148	14.279746	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2778/55818, ttl=4 (no response found!)

Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 520

Identification: 0xec9c (60572)

> Flags: 0x00b9

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0... .. = More fragments: Not set

Fragment offset: 1480

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x954f [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

> [2 IPv4 Fragments (1980 bytes): #136(1480), #137(500)]

> Internet Control Message Protocol

13. What fields change in the IP header between the first and second fragment?

ANS: Total length, the more fragments bit, fragment offset and header checksum. You can compare the results between first and second fragment considering the screenshots below.

First Fragment

136	14.124347	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2774/54794, ttl=255 (no response found!)
138	14.162448	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2775/55050, ttl=1 (no response found!)
140	14.166171	192.168.1.1	192.168.1.35	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)	
143	14.202371	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2776/55306, ttl=2 (no response found!)
145	14.240604	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2777/55562, ttl=3 (no response found!)
147	14.279746	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2778/55818, ttl=4 (no response found!)
149	14.317937	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2779/56074, ttl=5 (no response found!)
151	14.357722	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2780/56330, ttl=6 (no response found!)
153	14.396380	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2781/56586, ttl=7 (no response found!)
155	14.436502	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2782/56842, ttl=8 (no response found!)
157	14.474798	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2783/57098, ttl=9 (no response found!)
159	14.514344	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2784/57354, ttl=10 (no response found!)
161	14.552973	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2785/57610, ttl=11 (no response found!)
163	14.592148	192.168.1.35	128.119.245.12	ICMP	1514 Echo (ping) request	id=0x0001, seq=2786/57866, ttl=12 (no response found!)

Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxelCom_35:a4:27 (08:26:97:35:a4:27)	
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 1500	
Identification: 0xec9c (60572)	
Flags: 0x2000, More fragments	
0... .. = Reserved bit: Not set	
.0... .. = Don't fragment: Not set	
..1... .. = More fragments: Set	
Fragment offset: 0	
Time to live: 255	
Protocol: ICMP (1)	
Header checksum: 0x7234 [validation disabled]	
[Header checksum status: Unverified]	
Source: 192.168.1.35	
Destination: 128.119.245.12	

Second Fragment

136	14.124347	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9c) [Reassembled in #137]
137	14.124347	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2774/54794, ttl=255 (no response found!)
138	14.162448	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9c) [Reassembled in #139]
139	14.162448	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2775/55050, ttl=1 (no response found!)
140	14.166171	192.168.1.1	192.168.1.35	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)
141	14.195151	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6475 PTR 1.1.168.192.in-addr.arpa
142	14.197177	192.168.1.1	192.168.1.35	DNS	112 Standard query response 0x6475 PTR 1.1.168.192.in-addr.arpa PTR MitraStar.Home
143	14.202371	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9e) [Reassembled in #144]
144	14.202371	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2776/55306, ttl=2 (no response found!)
145	14.240604	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ec9f) [Reassembled in #146]
146	14.240604	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2777/55562, ttl=3 (no response found!)
147	14.279746	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=eca0) [Reassembled in #148]
148	14.279746	192.168.1.35	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=2778/55818, ttl=4 (no response found!)

Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 520	
Identification: 0xec9c (60572)	
Flags: 0x00b9	
0... .. = Reserved bit: Not set	
.0... .. = Don't fragment: Not set	
..0... .. = More fragments: Not set	
Fragment offset: 1480	
Time to live: 255	
Protocol: ICMP (1)	
Header checksum: 0x954f [validation disabled]	
[Header checksum status: Unverified]	
Source: 192.168.1.35	
Destination: 128.119.245.12	
> [2 IPv4 Fragments (1980 bytes): #136(1480), #137(500)]	
> Internet Control Message Protocol	

14. How many fragments were created from the original datagram?

ANS: As you can see from the below screenshot original datagram fragmented to 3 packets.

81	7.067584	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf4) [Reassembled in #83]
82	7.067584	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf4) [Reassembled in #83]
83	7.067584	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3138/16900, ttl=255 (no response found)
84	7.106694	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf5) [Reassembled in #86]
85	7.106694	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf5) [Reassembled in #86]
86	7.106694	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3139/17164, ttl=1 (no response found)
87	7.113532	192.168.1.1	192.168.1.35	ICMP	560 Time-to-live exceeded (time to live exceeded in transit)
88	7.124720	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.1.163.192.in-addr.arpa
89	7.146816	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf6) [Reassembled in #91]
90	7.146816	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf6) [Reassembled in #91]
91	7.146816	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3140/17420, ttl=2 (no response found)
92	7.149930	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.1.163.192.in-addr.arpa

> Frame 81: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0

> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxelCom_35:a4:27 (08:26:97:35:a4:27)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

> 0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1500

Identification: 0xedf4 (60916)

> Flags: 0x2000, More fragments

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

.1. = More fragments: Set

Fragment offset: 0

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x70dc [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

Reassembled IPv4 in frame: 83

15. What fields change in the IP header among the fragments?

ANS:

All fragments have different fragment offset and header checksum.

All fragments have the same TTL and identification number.

Fragment 1 and fragment 2 have the same total length and same More fragments bit.

So total length, fragment offset, header checksum and More fragments bit changed between these 3 fragments as you can see below screenshots.

Fragment 1

81 7.067504	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf4) [Reassembled in #83]
82 7.067504	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf4) [Reassembled in #83]
83 7.067504	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3138/16908, ttl=255 (no response found)
84 7.106094	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf5) [Reassembled in #86]
85 7.106094	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf5) [Reassembled in #86]
86 7.106094	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3139/17164, ttl=1 (no response found)
87 7.124720	192.168.1.1	192.168.1.1	ICMP	590 Time to live exceeded (time to live exceeded in transit)
88 7.124720	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa
89 7.146016	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf6) [Reassembled in #91]
90 7.146016	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf6) [Reassembled in #91]
91 7.146016	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3140/17420, ttl=2 (no response found)
92 7.149930	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa

< >

> Frame 81: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{B246CE7F-7719-4D09-ACAD-E87503A65ADC}, id 0

> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1500

Identification: 0xedf4 (60916)

> Flags: 0x2000, More fragments

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

.1.. .. = More fragments: Set

Fragment offset: 0

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x70d0 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

[Reassembled IPv4 in frame: 83]

Fragment 2

81 7.067504	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf4) [Reassembled in #83]
82 7.067504	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf4) [Reassembled in #83]
83 7.067504	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3138/16908, ttl=255 (no response found)
84 7.106094	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf5) [Reassembled in #86]
85 7.106094	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf5) [Reassembled in #86]
86 7.106094	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3139/17164, ttl=1 (no response found)
87 7.124720	192.168.1.1	192.168.1.1	ICMP	590 Time to live exceeded (time to live exceeded in transit)
88 7.124720	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa
89 7.146016	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf6) [Reassembled in #91]
90 7.146016	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf6) [Reassembled in #91]
91 7.146016	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3140/17420, ttl=2 (no response found)
92 7.149930	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa

< >

> Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{B246CE7F-7719-4D09-ACAD-E87503A65ADC}, id 0

> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxeCom_35:a4:27 (08:26:97:35:a4:27)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1500

Identification: 0xedf4 (60916)

> Flags: 0x2009, More fragments

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

.1.. .. = More fragments: Set

Fragment offset: 1480

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x7023 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.35

Destination: 128.119.245.12

[Reassembled IPv4 in frame: 83]

Fragment3

* 81 7.067504	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf4) [Reassembled in #83]
* 82 7.067504	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf4) [Reassembled in #83]
+ 83 7.067504	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3138/16908, ttl=255 (no response found!)
84 7.106094	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf5) [Reassembled in #86]
85 7.106094	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf5) [Reassembled in #86]
86 7.106094	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3139/17164, ttl=1 (no response found!)
87 7.113532	192.168.1.1	192.168.1.35	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)
88 7.124720	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa
89 7.146016	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf6) [Reassembled in #91]
90 7.146016	192.168.1.35	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf6) [Reassembled in #91]
91 7.146016	192.168.1.35	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3140/17420, ttl=2 (no response found!)
92 7.149930	192.168.1.35	192.168.1.1	DNS	84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa

< >

> Frame 83: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{B246CE7F-7719-4D09-AC40-E87503A65ADC}, id 0

> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxelCom_35:a4:27 (08:26:97:35:a4:27)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12

> 0100 = Version: 4

> 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

> Total Length: 540

> Identification: 0xedf4 (60916)

> Flags: 0x0172

> 0... .. = Reserved bit: Not set

> .0.. .. = Don't fragment: Not set

> ..0. = More fragments: Not set

> Fragment offset: 2960

> Time to live: 255

> Protocol: ICMP (1)

> Header checksum: 0x932a [validation disabled]

> [Header checksum status: Unverified]

> Source: 192.168.1.35

> Destination: 128.119.245.12

> 13 IPv4 Fragments (3480 bytes): #91(1480), #92(1480), #83(520)