

Bil 452 Ödev 6 -ICMP  
Fatih Furkan Has  
141101024

1-)

```
toor@001:~$ ping -c 10 www.ust.hk
PING www.ust.hk (143.89.14.1) 56(84) bytes of data.

--- www.ust.hk ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9194ms
```

Wireshark packet capture showing ICMP Echo (ping) requests from 10.2.44.242 to 143.89.14.1. The packet list shows 10 ping requests, all with 'no response found!'. The packet details show the ICMP Echo request structure. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
55	17.753245	10.2.44.242	10.1.12.104	DNS	90	Standard query 0xf678 A clients4.google.com OPT
56	17.755963	10.1.12.104	10.2.44.242	DNS	130	Standard query response 0xf678 A clients4.google.com CNAME clients.l.google.com A 216.58.286.174 OPT
14	5.134176484	10.2.44.242	104.27.145.120	HTTP	1042	GET /detroitchicago/imp.gif?e=%7B%22ad_cache_level%22%3A0%2C%22ad_location_ids%22%3A%221%2C0%2C80%22%2C%22adx_ad_count%22%3A1%2C%22
16	5.140389265	10.2.44.242	104.27.145.120	HTTP	1033	GET /detroitchicago/imp.gif?e=%7B%22ad_cache_level%22%3A0%2C%22city%22%3A%22Ankara%22%2C%22country%22%3A%22TR%22%2C%22days_since_l
24	5.19395619	10.2.44.242	10.2.44.242	HTTP	470	HTTP/1.1 200 OK (GIF89a)
26	5.19374966	104.27.145.120	10.2.44.242	HTTP	470	HTTP/1.1 200 OK (GIF89a)
34	5.29705223	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=1/256, ttl=64 (no response found!)
35	6.29931267	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=2/512, ttl=64 (no response found!)
36	7.323341944	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=3/768, ttl=64 (no response found!)
37	8.347334034	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=4/1024, ttl=64 (no response found!)
38	9.371333262	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=5/1280, ttl=64 (no response found!)
39	10.395332	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=6/1536, ttl=64 (no response found!)
40	11.419342	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=7/1792, ttl=64 (no response found!)
41	12.443335	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=8/2048, ttl=64 (no response found!)
42	13.467338	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=9/2304, ttl=64 (no response found!)
45	14.491336	10.2.44.242	143.89.14.1	ICMP	98	Echo (ping) request id=0x576b, seq=10/2560, ttl=64 (no response found!)
1	0.009090909	10.2.44.242	216.58.212.3	QUIC	65	Payload (Encrypted), PKN: 6, CID: 12153956591216519075
2	0.042249065	10.2.44.242	216.58.213.195	QUIC	65	Payload (Encrypted), PKN: 6, CID: 7041431096153490869
3	0.084302562	216.58.212.3	10.2.44.242	QUIC	62	Payload (Encrypted), PKN: 7
4	0.131923931	216.58.213.195	10.2.44.242	QUIC	64	Payload (Encrypted), PKN: 6
17	5.141857398	10.2.44.242	172.217.17.206	QUIC	611	Payload (Encrypted), PKN: 46, CID: 13886111425224608838
18	5.143199164	10.2.44.242	172.217.17.206	QUIC	601	Payload (Encrypted), PKN: 47, CID: 13886111425224608838
19	5.14410579	10.2.44.242	172.217.17.206	QUIC	723	Payload (Encrypted), PKN: 48, CID: 13886111425224608838
20	5.145524087	10.2.44.242	172.217.17.206	QUIC	713	Payload (Encrypted), PKN: 49, CID: 13886111425224608838
23	5.192409829	172.217.17.206	10.2.44.242	QUIC	133	Payload (Encrypted), PKN: 38
29	5.194109499	172.217.17.206	10.2.44.242	QUIC	121	Payload (Encrypted), PKN: 39
29	5.194752580	172.217.17.206	10.2.44.242	QUIC	127	Payload (Encrypted), PKN: 40
30	5.195909125	172.217.17.206	10.2.44.242	QUIC	121	Payload (Encrypted), PKN: 41
31	5.196389965	10.2.44.242	172.217.17.206	QUIC	83	Payload (Encrypted), PKN: 50, CID: 13886111425224608838
32	5.196576553	10.2.44.242	172.217.17.206	QUIC	80	Payload (Encrypted), PKN: 51, CID: 13886111425224608838
33	5.220484468	172.217.17.206	10.2.44.242	QUIC	62	Payload (Encrypted), PKN: 42

Frame 34: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: IntelCor\_08:0b:ad (08:0b:ad:08:0b:ad), Dst: Cisco\_ff:fc:04 (08:0b:e3:ff:fc:04)  
Internet Protocol Version 4, Src: 10.2.44.242, Dst: 143.89.14.1  
Internet Control Message Protocol

0000 00 00 e3 ff fc 04 00 f6 77 00 5b ad 00 00 45 00 ..... w[...]E.  
0010 00 54 c2 a8 40 00 40 01 a3 b2 0a 02 2c f2 8f 59 .T..@.. ....Y  
0020 0e 01 00 00 0e 61 57 6b 00 01 15 93 47 5b 00 00 ....naWk....G[..  
0030 00 00 0f 71 07 00 00 00 00 00 10 11 12 13 14 15 ...q.....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !\*%\$%  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()\*+,-./012345  
0060 36 37 67

Source: 10.2.44.242  
Destination: 143.89.14.1

2-)

ICMP protokolü network layerda çalıştığı için protokole ihtiyaç duymaz.

3-)

Wireshark packet capture showing an ICMP Echo (ping) request. The packet list shows a ping request from 10.2.44.242 to 143.89.14.1. The packet details pane shows the ICMP header with fields: Type: 8 (Echo (ping) request), Code: 0, Checksum: 0x6e61, Identifier (BE): 22379, Identifier (LE): 27479, Sequence number (BE): 1, and Sequence number (LE): 256. The packet bytes pane shows the raw data of the ICMP packet.

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x6e61 [correct]

-----> 2 bytes

Identifier (BE): 22379 (0x576b)

-----> 2 bytes

Identifier (LE): 27479 (0x6b57)

-----> 2 bytes

Sequence number (BE): 1 (0x0001)

-----> 2 bytes

Sequence number (LE): 256 (0x0100)

-----> 2 bytes

Checksum: 0x6e61 [correct]  
[Checksum Status: Good]  
Identifier (BE): 22379 (0x576b)  
Identifier (LE): 27479 (0x6b57)  
Sequence number (BE): 1 (0x0001)  
Sequence number (LE): 256 (0x0100)  
▶ [No response seen]  
Timestamp from icmp data: Jul 12, 2018 20:42:45.000000000 +03  
[Timestamp from icmp data (relative): 0.487714937 seconds]  
▶ Data (48 bytes)

0000 00 08 e3 ff fc 04 60 f6 77 60 5b ad 08 00 45 00  
0010 00 54 c2 a8 40 00 40 01 a3 b2 0a 02 2c f2 8f 59  
0020 0e 01 08 00 6e 61 57 6b 00 01 15 93 47 5b 00 00  
0030 00 00 0f 71 07 00 00 00 00 00 11 12 13 14 15  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  
0060 36 37

Checksum (icmp.checksum), 2 bytes

Identifier (LE): 27479 (0x6b57)  
Sequence number (BE): 1 (0x0001)  
Sequence number (LE): 256 (0x0100)  
▶ [No response seen]  
Timestamp from icmp data: Jul 12, 2018 20:42:45.000000000 +03  
[Timestamp from icmp data (relative): 0.487714937 seconds]  
▶ Data (48 bytes)

0000 00 08 e3 ff fc 04 60 f6 77 60 5b ad 08 00 45 00  
0010 00 54 c2 a8 40 00 40 01 a3 b2 0a 02 2c f2 8f 59  
0020 0e 01 08 00 6e 61 57 6b 00 01 15 93 47 5b 00 00  
0030 00 00 0f 71 07 00 00 00 00 00 11 12 13 14 15  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  
0060 36 37

Identifier (little endian representation) (icmp.ident), 2 bytes

Identifier (BE): 22379 (0x576b)  
Identifier (LE): 27479 (0x6b57)  
Sequence number (BE): 1 (0x0001)  
Sequence number (LE): 256 (0x0100)  
▶ [No response seen]  
Timestamp from icmp data: Jul 12, 2018 20:42:45.000000000 +03  
[Timestamp from icmp data (relative): 0.487714937 seconds]  
▶ Data (48 bytes)

0000 00 08 e3 ff fc 04 60 f6 77 60 5b ad 08 00 45 00  
0010 00 54 c2 a8 40 00 40 01 a3 b2 0a 02 2c f2 8f 59  
0020 0e 01 08 00 6e 61 57 6b 00 01 15 93 47 5b 00 00  
0030 00 00 0f 71 07 00 00 00 00 00 11 12 13 14 15  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  
0060 36 37

Identifier (big endian representation) (icmp.ident), 2 bytes

Sequence number (BE): 1 (0x0001)  
Sequence number (LE): 256 (0x0100)  
▶ [No response seen]  
Timestamp from icmp data: Jul 12, 2018 20:42:45.000000000 +03  
[Timestamp from icmp data (relative): 0.487714937 seconds]  
▶ Data (48 bytes)

0000 00 08 e3 ff fc 04 60 f6 77 60 5b ad 08 00 45 00  
0010 00 54 c2 a8 40 00 40 01 a3 b2 0a 02 2c f2 8f 59  
0020 0e 01 08 00 6e 61 57 6b 00 01 15 93 47 5b 00 00  
0030 00 00 0f 71 07 00 00 00 00 00 11 12 13 14 15  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  
0060 36 37

Sequence number (big endian representation) (icmp.seq), 2 bytes

4-)

The image shows a Wireshark packet capture of an ICMP Echo (ping) request. The packet list shows a series of ping requests from 10.2.44.242 to 143.89.14.1. The packet details pane shows the structure of an ICMP Echo (ping) request, including the sequence number (512) and the data field. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Fragment offset: 0  
Time to live: 64  
Protocol: ICMP (1)  
Header checksum: 0xa2ce [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.2.44.242  
Destination: 143.89.14.1  
[Source GeoIP: Unknown]  
[Destination GeoIP: Hong Kong, Central District, 00, AS3363 Hong Kong University of Science and Technology, Hong Kong, Central District, 00, AS3363 Hong Kong University of Science and Technology, 22.283300,  
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0xa857 [correct]  
[Checksum Status: Good]  
Identifier (BE): 22379 (0x576b)  
Identifier (LE): 27479 (0x6b57)  
Sequence number (BE): 512 (0x0200)  
Sequence number (LE): 512 (0x0200)  
[No response seen]  
Timestamp from icmp data: Jul 12, 2018 20:42:46.000000000 +03  
[Timestamp from icmp data (relative): 0.489975354 seconds]  
Data (48 bytes)

0000 00 00 e3 ff fc 04 60 f6 77 60 5b ad 00 00 45 00 ..... w' [...E.  
0010 00 54 c3 8c 40 00 40 01 a2 ce 0a 02 2c f2 8f 59 .T..@.. ....Y  
0020 0e 01 00 00 a8 57 57 6b 00 00 16 93 47 5b 00 00 ....mwk ..G[..  
0030 00 00 d4 79 07 00 00 00 00 00 19 11 12 13 14 15 ....Y....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !\*K\$  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()\*+,-./012345  
0060 36 37 67

Sequence number (big endian representation) (icmp.seq), 2 bytes

Packets: 101 - Displayed: 101 (100.0%)

Profile: Default

Yukarıdaki ekran görüntüsünde görüldüğü üzere response olmadığı için bu soruyu cevaplayamadım. Ancak eğer olsaydı bir önceki soru ile yaklaşık olarak aynı field'ların olacağı tahmin edebiliriz.

5-)

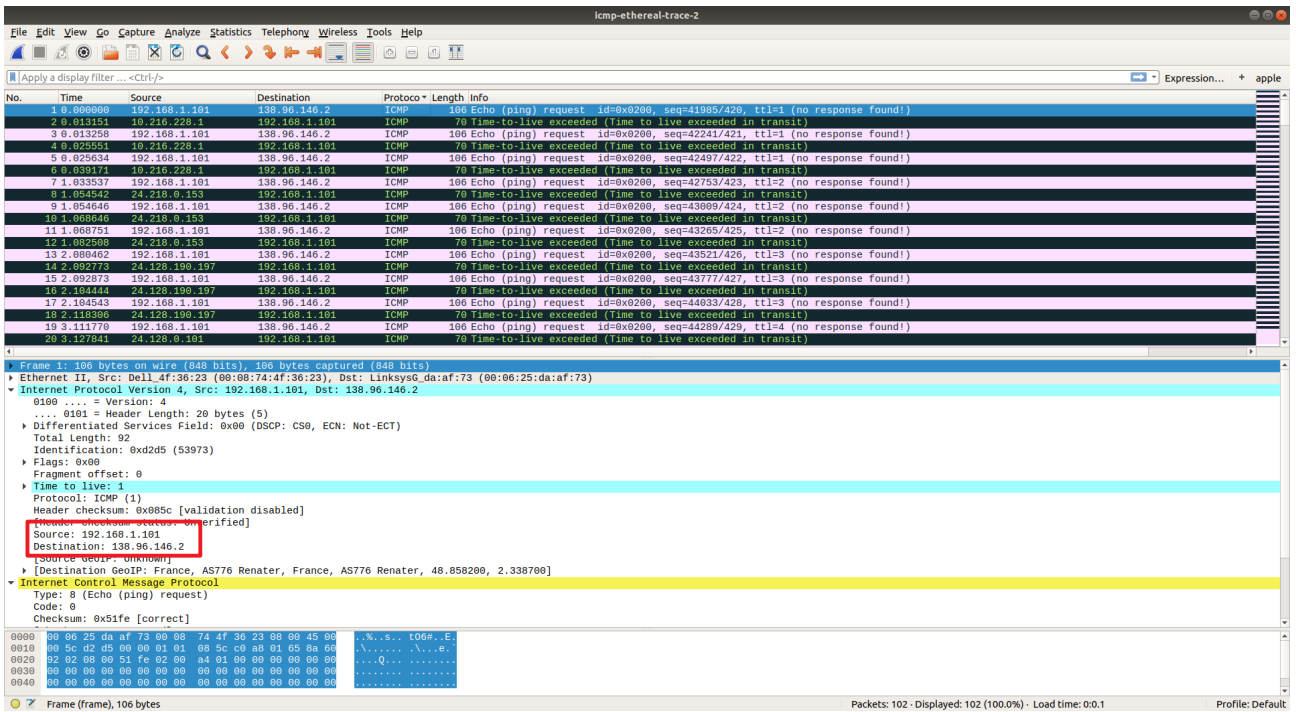
```
toor@001:~$ traceroute www.inria.fr
traceroute to www.inria.fr (128.93.162.84), 30 hops max, 60 byte packets
 1 _gateway (10.2.44.1) 1.233 ms 1.245 ms 1.299 ms
 2 10.1.255.1 (10.1.255.1) 4.022 ms 4.059 ms 4.190 ms
 3 193.140.109.1 (193.140.109.1) 3.263 ms 3.464 ms 3.453 ms
 4 10.59.14.157 (10.59.14.157) 4.765 ms 5.014 ms 5.144 ms
 5 10.40.133.5 (10.40.133.5) 6.891 ms 10.40.133.5 (10.40.133.5) 6.882 ms 7.701 ms
 6 10.38.207.134 (10.38.207.134) 10.954 ms 8.015 ms 8.805 ms
 7 10.40.130.106 (10.40.130.106) 5.624 ms 10.40.130.110 (10.40.130.110) 5.604 ms 10.38.211.158 (10.38.211.158) 5.581 ms
 8 10.38.211.153 (10.38.211.153) 11.546 ms 10.40.130.105 (10.40.130.105) 11.527 ms 10.38.211.157 (10.38.211.157) 12.607 ms
 9 10.36.6.142 (10.36.6.142) 11.436 ms 11.427 ms 10.008 ms
10 if-ae-8-2.tcore1.fnm-frankfurt.as6453.net (195.219.156.21) 49.283 ms 45.914 ms 47.047 ms
11 if-ae-7-2.tcore1.fr0-frankfurt.as6453.net (195.219.50.1) 45.265 ms if-ae-9-2.tcore1.fr0-frankfurt.as6453.net (5.23.30.17) 48.531 ms 46.890 ms
12 195.219.50.138 (195.219.50.138) 45.889 ms 47.103 ms 47.216 ms
13 xe-2-1-3.cr0-par7.ip4.gtt.net (89.149.135.130) 53.327 ms xe-2-0-1.cr0-par7.ip4.gtt.net (213.254.230.6) 60.700 ms xe-2-2-1.cr0-par7.ip4.gtt.net (89.149.135.154) 56.117 ms
14 renater-gw-ix1.gtt.net (77.67.123.206) 63.139 ms 61.057 ms 62.078 ms
15 * * *
16 inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177) 61.436 ms 60.351 ms 60.044 ms
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

The image shows a Wireshark packet capture analysis of a traceroute to www.inria.fr. The packet list pane displays 30 hops, each represented by an ICMP Echo (ping) request and response. The packet details pane shows the Internet Protocol Version 4 header and the ICMP Echo (ping) section. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	1.233	10.2.44.1	10.1.255.1	DNS	140	Standard query response 0x0c3c PTR 6.238.254.213.in-addr.arpa PTR xe-2-0-1.cr0-par7.ip4.gtt.net OPT
2	4.022	10.1.255.1	10.2.44.242	DNS	141	Standard query response 0x8059 PTR 154.135.149.89.in-addr.arpa PTR xe-2-2-1.cr0-par7.ip4.gtt.net OPT
3	3.263	193.140.109.1	10.1.255.1	DNS	97	Standard query response 0x85c9 PTR 206.123.67.77.in-addr.arpa OPT
4	4.765	10.59.14.157	10.2.44.242	DNS	133	Standard query response 0x85c9 PTR 206.123.67.77.in-addr.arpa PTR renater-gw-ix1.gtt.net OPT
5	6.891	10.40.133.5	10.2.44.242	DNS	165	Standard query response 0xc872 PTR 177.184.51.193.in-addr.arpa PTR inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr OPT
6	10.954	10.38.207.134	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
7	5.604	10.40.130.110	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
8	11.546	10.38.211.158	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
9	11.436	10.38.211.157	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
10	49.283	195.219.156.21	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
11	45.265	195.219.50.1	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
12	48.531	5.23.30.17	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
13	45.889	195.219.50.138	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
14	53.327	89.149.135.130	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
15	60.700	213.254.230.6	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
16	61.436	89.149.135.154	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
17	60.351	77.67.123.206	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
18	60.044	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
19	61.436	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
20	60.351	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
21	60.044	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
22	61.436	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
23	60.351	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
24	60.044	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
25	61.436	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
26	60.351	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
27	60.044	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
28	61.436	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
29	60.351	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)
30	60.044	193.51.184.177	10.2.44.242	DNS	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 31: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0  
Ethernet II, Src: Cisco\_ff:fc:04 (00:08:e3:ff:fc:04), Dst: IntelCor\_60:5b:ad (60:f6:77:60:5b:ad)  
Internet Protocol Version 4, Src: 10.2.44.1, Dst: 10.2.44.242  
8180 ... = Version: 4  
... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  
0000 60 f6 77 60 5b ad 00 00 e3 ff fc 04 08 00 45 c0 .w[... ..E.  
0010 00 38 d9 0c 00 00 ff 01 74 51 0a 02 2c 01 0a 02 .8.....tQ...  
0020 2c f2 0b 00 43 e4 00 00 00 00 45 00 00 3c 06 6d ...C...E..m  
0030 00 00 01 11 59 9f 0a 02 2c f2 00 5d a2 54 ac f0 ...Y...].T..  
0040 82 9c 00 28 81 66 ...(.f

Yukarıdaki çıktılarda görebileceğiniz üzere ilk ekran görüntüsüne baktığımızda traceroute ile attığımız istekte 17 ile 30 arasındaki routerları bulamadık ve wireshark çıktısında da ping requestleri görememekteyim bu sebeple bu soruları lab dosyalarında mevcut olan wireshark çıktıları ile cevaplayacağım.

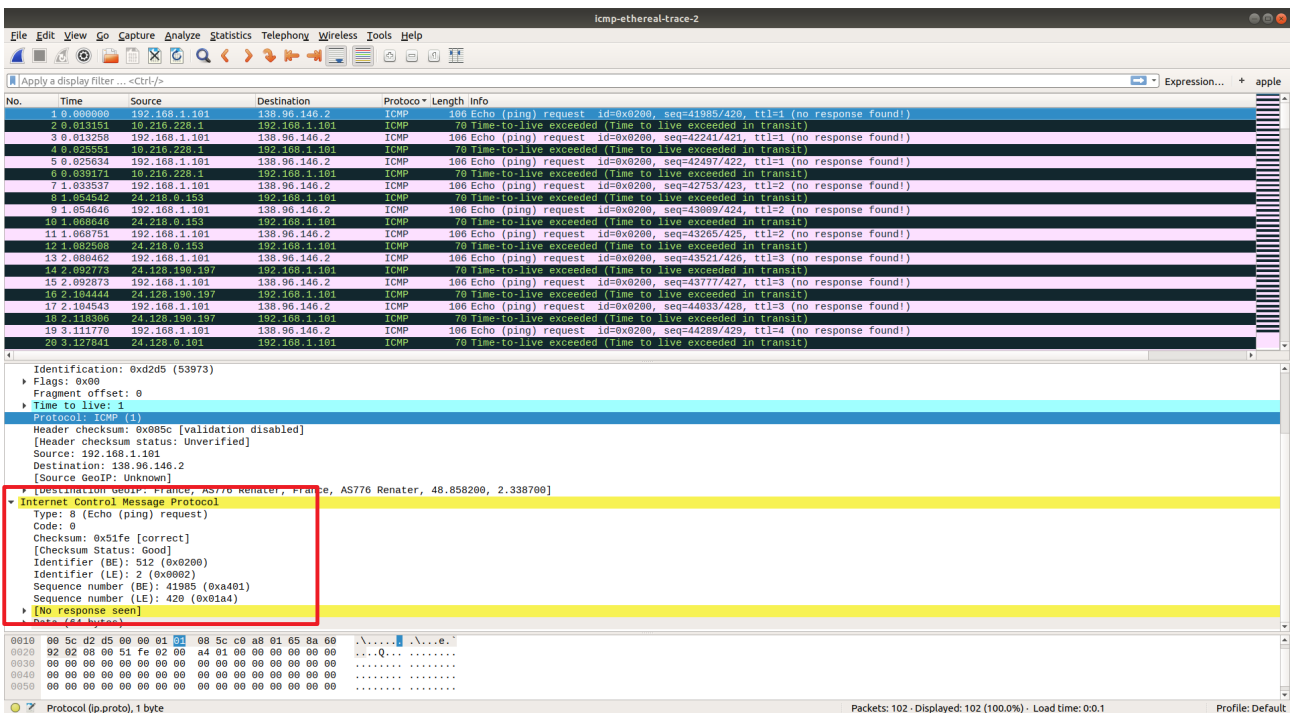


Source: 192.168.1.101  
Destination: 138.96.146.2

6-)

Eğer Linuxta'ki gibi UDP olarak gönderilirse 5. sorunun başında gösterdiğim çıktıları bakarsak (ben Linux kullanmaktayım) UDP kullanılırdı 17 numarasını alırdı.  
<https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml> buradan da görebiliriz.

7-)



Field'lar ilk bölümdeki değerler ile aynıdır.



8-)

The screenshot shows the Wireshark interface with a packet capture of ICMP errors. The packet list shows several ICMP Echo (ping) requests and responses. The packet details pane for the selected packet (No. 4) shows the following structure:

- Protocols in frame: eth:ethertype:ip:icmp:ip:icmp
- Coloring Rule Names: ICMP errors
- Coloring Rule String: icmp.type eq 11 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4
- Ethernet II, Src: Linksys6\_da:af:73 (08:00:25:da:af:73), Dst: Dell\_4f:36:23 (08:00:74:4f:36:23)
- Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101
- 0100 .... = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
- Total Length: 56
- Identification: 0x9d45 (40261)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 255
- Protocol: ICMP (1)
- Header checksum: 0x0d0 [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.216.228.1
- Destination: 192.168.1.101
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Internet Control Message Protocol
- Type: 11 (Time-to-live exceeded)
- Code: 0 (Time to live exceeded in transit)
- Checksum: 0x2c16 [correct]
- [Checksum Status: Good]
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
- 0100 .... = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 92
- Identification: 0xd2d5 (53973)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0xd145 [validation disabled]
- [Header checksum status: Unverified]

The screenshot shows the Wireshark interface with a packet capture of ICMP Echo (ping) requests and responses. The packet list shows several ICMP Echo (ping) requests and responses. The packet details pane for the selected packet (No. 4) shows the following structure:

- [Time since reference or first frame: 0.000000000 seconds]
- Frame Number: 1
- Frame Length: 100 bytes (848 bits)
- Capture Length: 100 bytes (848 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- Protocols in frame: eth:ethertype:ip:icmp:data
- Coloring Rule Names: ICMP
- Coloring Rule String: icmp || icmpv6
- Ethernet II, Src: Dell\_4f:36:23 (08:00:74:4f:36:23), Dst: Linksys6\_da:af:73 (08:00:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
- 0100 .... = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 92
- Identification: 0xd2d5 (53973)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x085c [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.101
- Destination: 138.96.146.2
- [Source GeoIP: Unknown]
- [Destination GeoIP: France, AS776 Renater, France, AS776 Renater, 48.858200, 2.338700]
- Internet Control Message Protocol
- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x51fe [correct]
- [Checksum Status: Good]
- Identifier (BE): 512 (0x0200)
- Identifier (LE): 2 (0x0002)
- Sequence number (BE): 41985 (0xa401)
- Sequence number (LE): 420 (0x01a4)
- [No response seen]
- Data (64 bytes)

Görüldüğü gibi farklı bilgiler taşımaktadırlar üstteki ekran görüntüsü “error” için olandır.

9-)

Wireshark packet capture of ICMP Echo (ping) requests and replies. The packet list shows multiple requests and replies, with some marked as 'Time-to-live exceeded'. The packet details pane shows the structure of an ICMP Echo (ping) request, including the IP header, ICMP header, and the data field.

Header checksum: 0x01c7 [validation disabled]  
[Header checksum status: Unverified]  
Source: 193.51.181.137  
Destination: 192.168.1.101  
[Destination GeoIP: Unknown]  
Internet Control Message Protocol  
Type: 11 (Time-to-live exceeded)  
Code: 0 (Time to live exceeded in transit)  
Checksum: 0x0000 [correct]  
[Checksum Status: Good]  
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2  
0100 .... = Version: 4  
... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 92  
Identification: 0xd394 (54820)  
00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 c0 ..t06#..%.s..E..  
00 38 99 73 00 00 ef 01 61 c7 c1 33 b5 08 c0 a8 \.s.......3...  
01 05 00 00 2c 16 00 00 00 00 45 08 00 5c d3 04 .e.....E.\..  
00 00 01 01 d1 16 c0 a8 01 65 8a 08 92 02 08 00 .....e.....  
22 fe 02 00 d3 01 .....

Wireshark packet capture of ICMP Echo (ping) requests and replies. The packet list shows multiple requests and replies, with some marked as 'Time-to-live exceeded'. The packet details pane shows the structure of an ICMP Echo (ping) reply, including the IP header, ICMP header, and the data field.

Source: 138.96.146.2  
Destination: 192.168.1.101  
[Destination GeoIP: Unknown]  
Internet Control Message Protocol  
Type: 0 (Echo (ping) reply)  
Code: 0  
Checksum: 0x27fe [correct]  
[Checksum Status: Good]  
Identifier (BE): 512 (0x0200)  
Identifier (LE): 2 (0x0002)  
Sequence number (BE): 54785 (0xd601)  
Sequence number (LE): 470 (0x01d6)  
[Request frame: 101]  
[Response time: 112,720 ms]  
Data (64 bytes)  
00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ..t06#..%.s..E..  
00 5c 99 a1 40 00 ee 01 14 df 8a 08 92 02 c0 a8 \.s.......3...  
01 05 00 00 27 fe 02 00 d6 01 00 00 00 00 00 00 .e.'.....  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Görüldüğü gibi type ve code farklıdır. Burada farklı olmasının sebebi TTL 0'lanmadan önce hedefe ulaşmış olmalarıdır.



10-)

```
toor@001:~$ traceroute www.inria.fr
traceroute to www.inria.fr (128.93.162.84), 30 hops max, 60 byte packets
 0  gateway (10.2.44.1)  1.000 ms  1.032 ms  1.400 ms
 1  10.1.255.1 (10.1.255.1)  3.130 ms  3.233 ms  3.320 ms
 2  193.140.109.1 (193.140.109.1)  3.767 ms  4.232 ms  4.500 ms
 3  10.59.14.157 (10.59.14.157)  5.926 ms  6.301 ms  6.433 ms
 4  10.40.133.5 (10.40.133.5)  8.339 ms  10.40.133.1 (10.40.133.1)  8.677 ms  10.40.133.5 (10.40.133.5)  8.667 ms
 5  10.38.207.134 (10.38.207.134)  13.100 ms  14.139 ms  14.061 ms
 6  10.38.211.158 (10.38.211.158)  8.720 ms  10.40.130.106 (10.40.130.106)  7.554 ms  10.38.211.158 (10.38.211.158)  6.471 ms
 7  10.40.130.106 (10.40.130.106)  12.027 ms  10.38.211.157 (10.38.211.157)  11.070 ms  10.38.211.153 (10.38.211.153)  14.570 ms
 8  10.36.6.142 (10.36.6.142)  13.409 ms  12.140 ms  12.033 ms
 9  if-ae-8-2.tcore1.fnm-frankfurt.as6453.net (195.219.156.21)  51.855 ms  46.315 ms  49.770 ms
10  if-ae-9-2.tcore1.fr0-frankfurt.as6453.net (5.23.30.17)  46.409 ms  if-ae-7-2.tcore1.fr0-frankfurt.as6453.net (195.219.50.1)  49.046 ms  44.658 ms
11  195.219.50.138 (195.219.50.138)  52.149 ms  45.377 ms  45.217 ms
12  xe-2-0-1.cr0-par7.ip4.gtt.net (213.254.230.6)  60.734 ms  xe-2-1-3.cr0-par7.ip4.gtt.net (89.149.135.130)  55.735 ms  55.882 ms
13  renater-gw-ix1.gtt.net (77.67.123.206)  60.884 ms  60.557 ms  61.264 ms
14  * * *
15  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177)  60.244 ms  60.217 ms  58.868 ms
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

9 ile 10 arasında çok büyük süre farkı vardır bunun sebebi iki router arasındaki mesafenin çok uzak olmasıdır. Ancak konumlarını bulamadım.