

Bil 452 – Ödev 5 – IP
Fatih Furkan Has
141101024

1-)

```
traceroute@001:~$ traceroute gala.cs.umass.edu 56
traceroute to gala.cs.umass.edu (128.119.245.12), 30 hops max, 56 byte packets
 1 _gateway (10.2.42.1)  1.019 ms  1.098 ms  1.875 ms
 2 10.1.255.1 (10.1.255.1)  3.606 ms  4.694 ms  8.542 ms
 3 193.140.109.1 (193.140.109.1)  8.608 ms  8.961 ms  9.395 ms
 4 10.59.14.157 (10.59.14.157)  11.128 ms  11.372 ms  11.366 ms
 5 10.40.133.5 (10.40.133.5)  13.935 ms  10.40.133.1 (10.40.133.1)  13.927 ms  10.38.210.145 (10.38.210.145)  13.906 ms
 6 10.38.207.134 (10.38.207.134)  18.771 ms  9.536 ms  9.482 ms
 7 10.38.211.150 (10.38.211.150)  7.335 ms  7.340 ms  10.40.130.106 (10.40.130.106)  7.316 ms
 8 10.38.211.161 (10.38.211.161)  11.870 ms  10.38.211.153 (10.38.211.153)  11.859 ms  10.38.211.149 (10.38.211.149)  11.841 ms
 9 10.36.6.142 (10.36.6.142)  11.824 ms  14.559 ms  9.772 ms
10 if-ae-8-2.tcore1.frm-frankfurt.as6453.net (195.219.156.21)  97.230 ms  97.258 ms  97.240 ms
11 if-ae-9-2.tcore1.fr0-frankfurt.as6453.net (5.23.30.17)  97.239 ms  if-ae-7-2.tcore1.fr0-frankfurt.as6453.net (195.219.50.1)  97.220 ms  96.392 ms^[[A
12 * * *
13 * * *
14 UNIVERSITY.ear3.NewYork1.Level3.net (4.71.230.234)  237.490 ms  235.840 ms  235.918 ms
15 core1-rt-et-8-3-0.gw.umass.edu (192.80.83.109)  233.687 ms  core2-rt-et-8-3-0.gw.umass.edu (192.80.83.113)  239.095 ms  234.985 ms
16 n5-rt-1-1-et-7-0-0.gw.umass.edu (128.119.0.10)  238.757 ms  n5-rt-1-1-et-5-0-0.gw.umass.edu (128.119.0.8)  242.148 ms  n5-rt-1-1-et-7-0-0.gw.umass.edu (128.119.0.10)  240.732 ms
17 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  239.623 ms  226.299 ms  228.402 ms
18 nscc1bs1.cs.umass.edu (128.119.240.253)  234.239 ms  233.311 ms  228.678 ms
19 gala.cs.umass.edu (128.119.245.12)  228.057 ms IX 229.543 ms IX 228.491 ms IX
traceroute@001:~$ traceroute gala.cs.umass.edu 2000
traceroute to gala.cs.umass.edu (128.119.245.12), 30 hops max, 2000 byte packets
 1 _gateway (10.2.42.1)  2.243 ms  2.206 ms  2.305 ms
 2 10.1.255.1 (10.1.255.1)  2.410 ms  2.440 ms  2.630 ms
 3 193.140.109.1 (193.140.109.1)  4.647 ms  4.805 ms  9.631 ms
 4 10.59.14.157 (10.59.14.157)  10.562 ms  11.224 ms  11.197 ms
 5 10.40.133.1 (10.40.133.1)  11.137 ms  12.029 ms  12.005 ms
 6 10.38.207.134 (10.38.207.134)  17.178 ms  9.837 ms  11.567 ms
 7 10.38.211.150 (10.38.211.158)  6.836 ms  6.761 ms  6.731 ms
 8 10.38.211.149 (10.38.211.149)  13.372 ms  13.361 ms  13.963 ms
 9 10.36.6.142 (10.36.6.142)  9.260 ms  10.118 ms  10.799 ms
10 if-ae-8-2.tcore1.frm-frankfurt.as6453.net (195.219.156.21)  52.584 ms  52.590 ms  52.570 ms
11 if-ae-9-2.tcore1.fr0-frankfurt.as6453.net (5.23.30.17)  50.807 ms  50.918 ms  51.074 ms
12 * * *
13 ae-1-3501.ear3.NewYork1.Level3.net (4.69.150.202)  135.970 ms  135.108 ms  135.199 ms
14 UNIVERSITY.ear3.NewYork1.Level3.net (4.71.230.234)  226.477 ms  224.652 ms  224.849 ms
15 core1-rt-et-8-3-0.gw.umass.edu (192.80.83.109)  223.374 ms  224.334 ms  224.313 ms
16 * n5-rt-1-1-et-5-0-0.gw.umass.edu (128.119.0.8)  224.400 ms  224.464 ms
17 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  222.935 ms  215.918 ms  216.337 ms
18 gala.cs.umass.edu (128.119.245.12)  237.440 ms IX 237.209 ms IX 243.085 ms IX
traceroute@001:~$ traceroute gala.cs.umass.edu 3500
traceroute to gala.cs.umass.edu (128.119.245.12), 30 hops max, 3500 byte packets
 1 _gateway (10.2.42.1)  2.769 ms  2.746 ms  2.868 ms
 2 10.1.255.1 (10.1.255.1)  2.893 ms  3.837 ms  4.018 ms
 3 193.140.109.1 (193.140.109.1)  4.108 ms  4.279 ms  4.255 ms
 4 10.59.14.157 (10.59.14.157)  5.398 ms  16.440 ms  16.387 ms
 5 10.40.133.1 (10.40.133.1)  16.270 ms  16.269 ms  16.234 ms
 6 10.38.207.134 (10.38.207.134)  21.678 ms  18.778 ms  18.723 ms
 7 10.38.211.158 (10.38.211.158)  11.755 ms  11.659 ms  12.218 ms
 8 10.38.211.149 (10.38.211.149)  17.378 ms  17.362 ms  17.334 ms
 9 10.36.6.142 (10.36.6.142)  16.201 ms  15.467 ms  9.916 ms
10 if-ae-8-2.tcore1.frm-frankfurt.as6453.net (195.219.156.21)  51.574 ms  51.562 ms  51.534 ms
11 if-ae-9-2.tcore1.fr0-frankfurt.as6453.net (5.23.30.17)  49.726 ms  49.701 ms  49.478 ms
12 * * *
13 * * *
14 UNIVERSITY.ear3.NewYork1.Level3.net (4.71.230.234)  244.994 ms  245.003 ms  245.258 ms
15 core1-rt-et-8-3-0.gw.umass.edu (192.80.83.109)  243.424 ms  235.588 ms  235.613 ms
16 n5-rt-1-1-et-5-0-0.gw.umass.edu (128.119.0.8)  235.563 ms  239.879 ms  239.898 ms
```

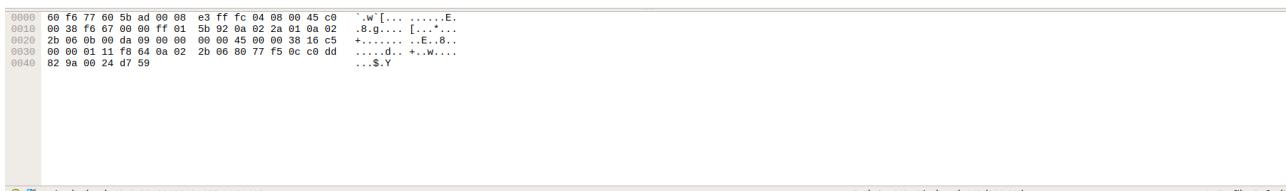
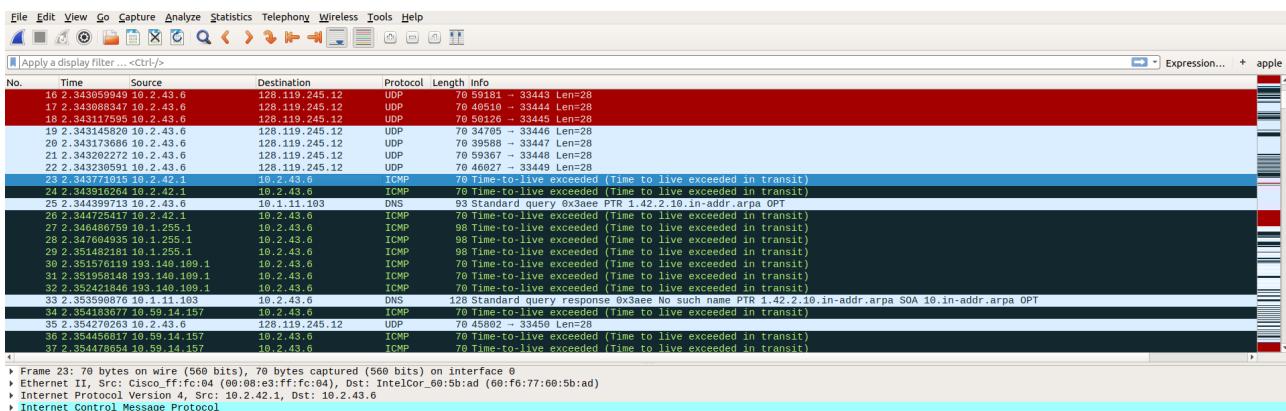
İlk soruda istenildiği gibi:

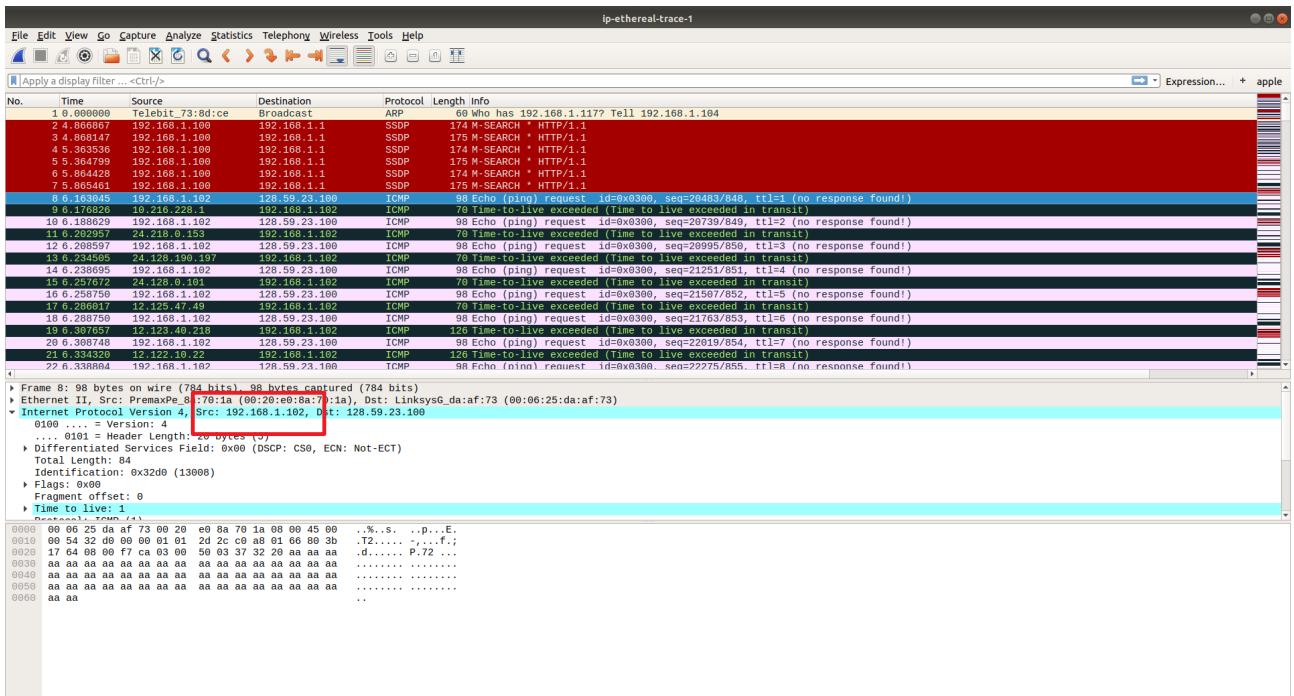
traceroute gaia.cs.umass.edu 56

traceroute gaia.cs.umass.edu 2000

traceroute gaia.cs.umass.edu 3500

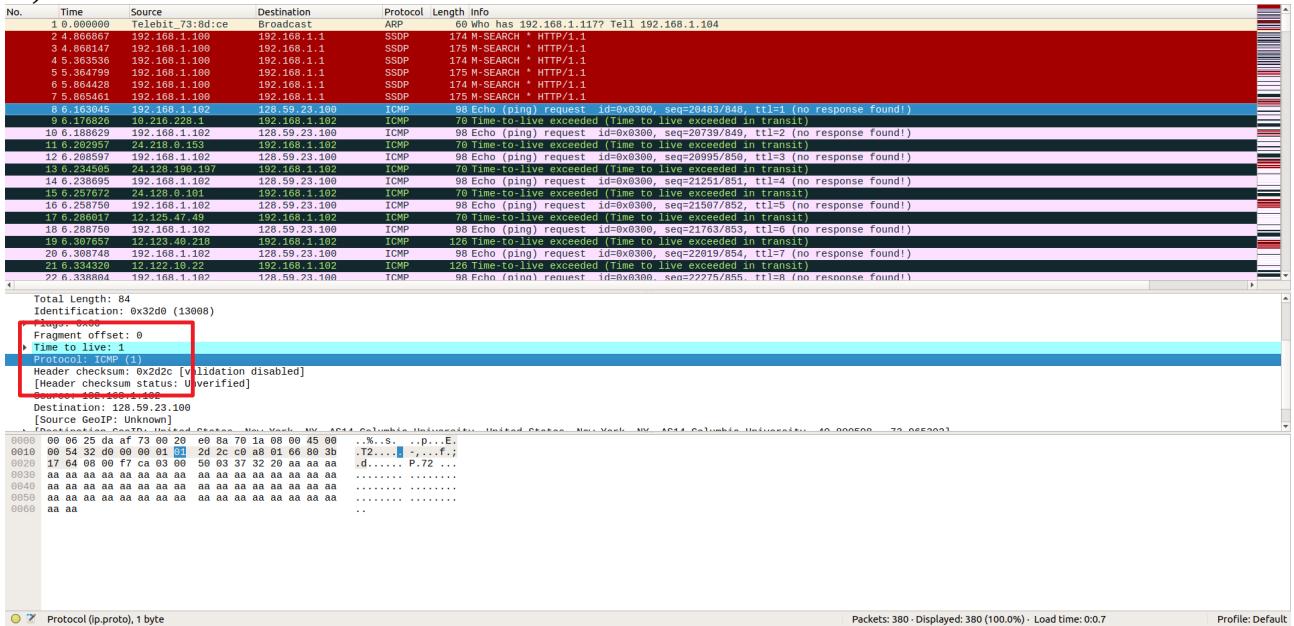
komutlarını çalıştırıldım ancak Wireshark üzerinden Echo (request) isteklerini göremedim bu yüzden pdf'de verilen ip-ethernal-trace-1 dosyasını kullanarak inceleme yapmaya devam ediyorum. Echo isteklerini göremediğim Wireshark çıktısını da aşağıya ekliyorum.





IP adresimiz: 192.168.1.102

2-)



Protocol: ICMP (1)

3-)

Frame	Number	Source	Destination	Protocol	Description
7	6.865461	192.168.1.100	192.168.1.1	SSDP	179 M-SEARCH HTTP/1.1
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	6.286017	12.125.47.49	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19	6.307657	12.123.40.218	192.168.1.102	ICMP	126 Time-to-live exceeded (Time to live exceeded in transit)
20	6.308748	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126 Time-to-live exceeded (Time to live exceeded in transit)
22	6.338864	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)

Length: 20

Payload: 56 – 20 = 36

Frame	Number	Source	Destination	Protocol	Description
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	6.286017	12.125.47.49	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19	6.307657	12.123.40.218	192.168.1.102	ICMP	126 Time-to-live exceeded (Time to live exceeded in transit)
20	6.308748	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126 Time-to-live exceeded (Time to live exceeded in transit)
22	6.338864	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)

Protocol: ICMP (1)
Header checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[Source GeoIP: Unknown]
► [Destination GeoIP: United States, New York, NY, AS14 Columbia University, United States, New York, NY, AS14 Columbia University, 40.800598, -73.965302]
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ca [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 20483 (0x5003)
Sequence number (LE): 848 (0x0350)
► [No response seen]
Data (56 bytes)

4-)

Fragment offset: 0 olarak görülebiliyor. Yani fragmented olmadığını anlayabiliriz.

5-)

```
 8 6.163845 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
 9 6.168626 192.168.1.102 192.168.1.102 ICMP 79 Time-to-live exceeded (Time to live exceeded in transit)
10 6.178829 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11 6.202957 24.218.0.153 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
12 6.268597 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20995/856, ttl=3 (no response found!)
13 6.345207 24.218.0.153 192.168.1.102 ICMP 98 Echo (ping) request id=0x0300, seq=21251/857, ttl=4 (no response found!)
14 6.423095 192.168.1.102 128.59.23.100 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
15 6.457672 24.218.0.153 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
16 6.258750 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17 6.286617 12.125.47.49 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
18 6.288709 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19 6.307657 12.123.40.218 192.168.1.102 ICMP 126 Time-to-live exceeded (Time to live exceeded in transit)
20 6.308148 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
21 6.334520 192.168.1.102 192.168.1.102 ICMP 126 Time-to-live exceeded (Time to live exceeded in transit)
22 6.338854 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)

Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Srv-Box-E8-Ba:70:1a (00:0e:08:0a:70:1a), Dst: LinkSysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    Version: 4
    IHL: 5
    Identification: 0x32d1 (13609)
    Flags: 0x00
    FragOffset: 0
    TTL: 1
    Time to live: 2
    Header checksum: 0x2c2b [validation disabled]
    Header length: 84 [Header verified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeolP: Unknown]
    [Destination GeolP: United States, New York, NY, AS14 Columbia University, United States, New York, NY, AS14 Columbia University, 40.800598, -73.965302]
Internet Control Message Protocol
    00 00 00 25 da 07 33 20 e8 8a 7a 01 00 45 00 ..%.s ..p..E.
0010 00 54 32 d1 00 00 02 01 26 2b c9 a8 01 66 80 3b .t2. ....,....f;
0020 00 00 00 00 00 00 00 00 51 03 00 29 aa aa aa aa aa .....Q.72...
0030 aa .....Q.72...
0040 aa .....Q.72...
0050 aa .....Q.72...
0060 aa .....Q.72...
0070 aa .....
```

Frame, Indetification, Header checksum ve Time to live değerlerimiz değişmiştir. Yukarıda art arda gönderilen iki farklı paketin çıkışlarından anlayabiliyoruz. Diğer paketler de incelediğinde aynı sonucu görebiliriz.

6-)

5. sorudaki ekran görüntülerini incelediğimizde Version, Header Length, Source, Destination, Service field, Protocol alanları değişmemiştir. 5. soruda belirtilen alanlar ise gönderilen paketler farklı olduğu için değişmiştir.

7-)

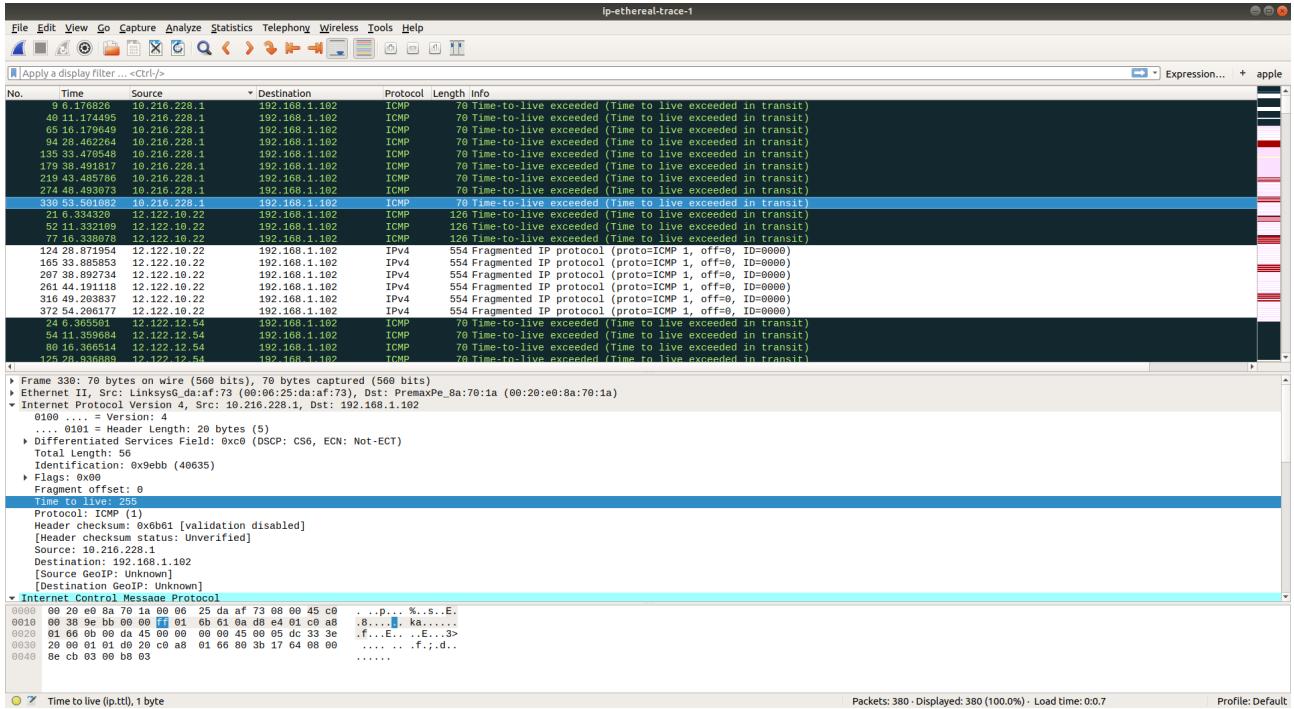
5. sorudaki ekran görüntülerine tekrar bakarsak Frame, Identification, Time to live değerlerinin +1 olacak şekilde ilerlediğini görebiliriz.

8-)

ip-ethereal-trace-1									
No.	Time	Source	Destination	Protocol	Length	Info			
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
40	11.174495	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
65	16.179649	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
179	38.491841	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
210	43.500566	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
274	44.483073	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
330	53.561082	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
21	6.334329	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)			
52	11.332109	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)			
77	16.338078	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)			
124	28.871954	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)			
165	33.872056	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)			
209	38.892734	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)			
261	44.191118	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)			
316	49.208387	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)			
372	54.206177	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)			
24	6.365501	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
54	11.359664	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
80	16.366514	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
125	28.936089	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)			
► Frame 9: 78 bytes on wire (606 bits), 78 bytes captured (566 bits) ► Ethernet II, Src: Linksys0_d:af:73 (00:06:25:d:a:f7:3), Dst: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a) ► Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102 0100 .. 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ... 0101 = Header Length: 20 bytes (5) ► Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT) Total Length: 90 Identification: 0x9d7c (40316) Flags: 0x00 Fragment Offset: 0 Protocol: ICMP Header checksum: 0x6ca0 [validation disabled] [Header checksum status: Unverified] Source: 10.216.228.1 Destination: 192.168.1.102 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] ► Internet Protocol Version 4 0000 00 20 e0 8a 70 1a 00 00 25 da af 73 00 45 c9 .P..K..S..E. 0019 00 38 9d 7c 00 00 ff 01 6c a0 0a d8 e4 01 c9 a8 .8. .J..1..... 0020 01 66 00 d9 40 00 00 00 45 00 00 54 32 d8 .f..F.. .E..T2. 0030 00 00 01 01 f6 16 c0 a8 01 66 80 3b 17 64 08 00f.;.d.. 0040 f7 ca 03 00 50 03P. Time to live (ip.ttl), 1 byte	Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.7			Profile: Default					

Identification: 0x9d7c (40316)
Time to live: 255

9-)



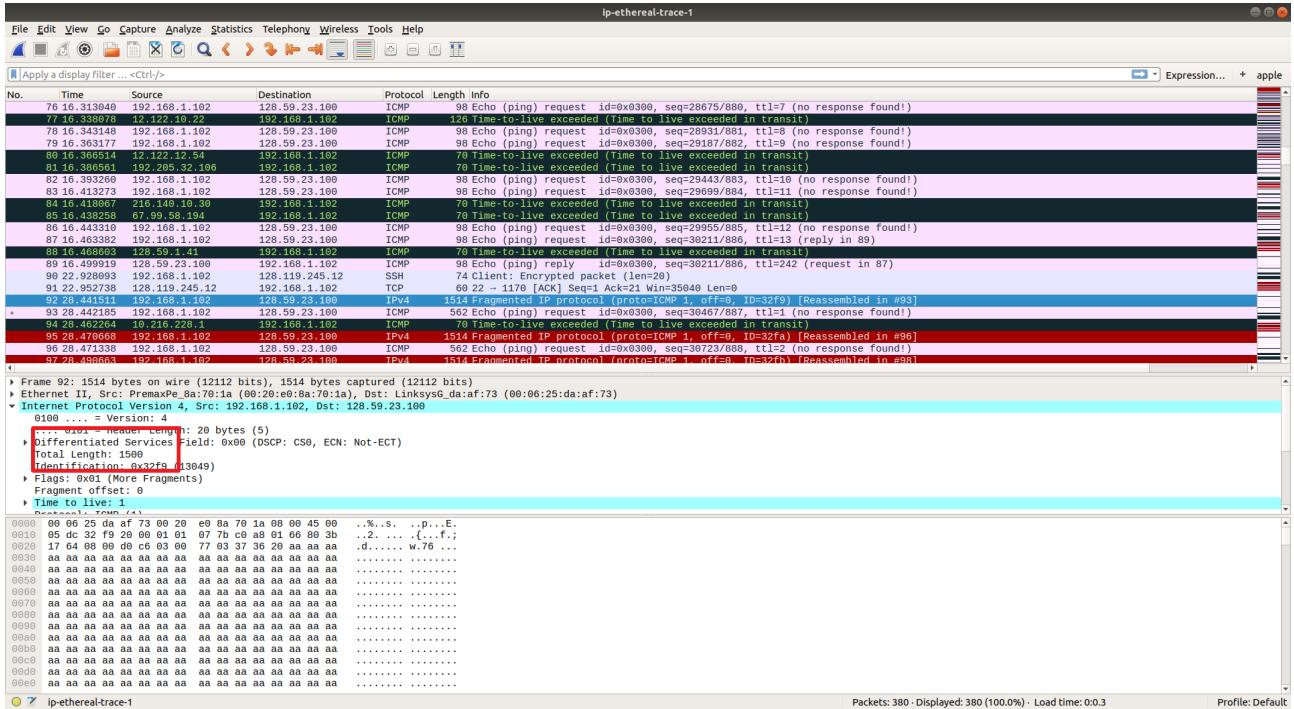
8. sorudaki ekran görüntüsü en yakın routerden gelen ilk cevap üstteki ekran görüntüsü ise son cevaba aittir. Bu iki ekran görüntüsünü karşılaştırdığımızda TTL değerinin değişmediğini ancak Identification değerinin değiştiğini görüyoruz. Identification unique bir değer olduğu için değişimmemiştir. TTL ise aynı routerden geldiği için aynı kalmıştır.

10-)

The screenshots show two instances of Wireshark capturing network traffic. Both instances display a list of network frames, primarily ICMP echo requests and responses, between two hosts. A specific ICMP frame is highlighted in red in both instances. The red-highlighted frame is a fragmented IP protocol (proto:ICMP) packet with source 192.168.1.102 and destination 128.59.23.100. It has an offset of 0, ID=32ff, and TTL=1. The payload contains the string "aaaaaaa...". The bottom screenshot also includes a yellow-highlighted section containing information about the captured traffic, such as the number of fragments and the reassembled IPv4 data.

İki ekran görüntüsünde görüldüğü gibi fragmented olmuştur.

11-)

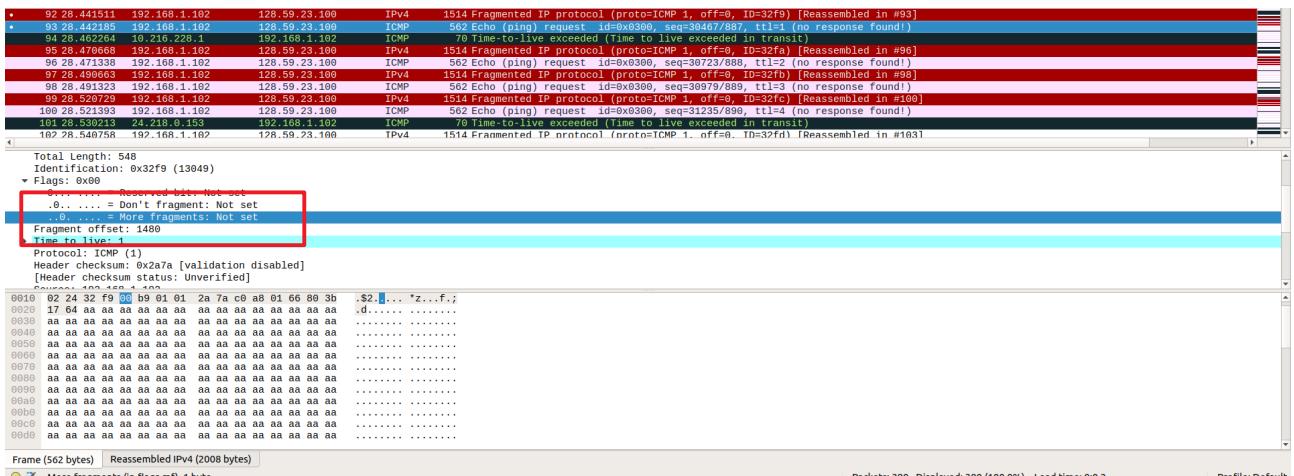


Fragment offset: 0'dır. Bu sebeple bunun ilk fragment olduğunu söyleyebiliriz. Length'imiz de 1500 olarak görülebilir.

▼ Flags: 0x01 (More Fragments)
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.1. = More fragments: Set

More fragment 1 olarak set edildiği için de fragmented diyebiliriz.

12-)

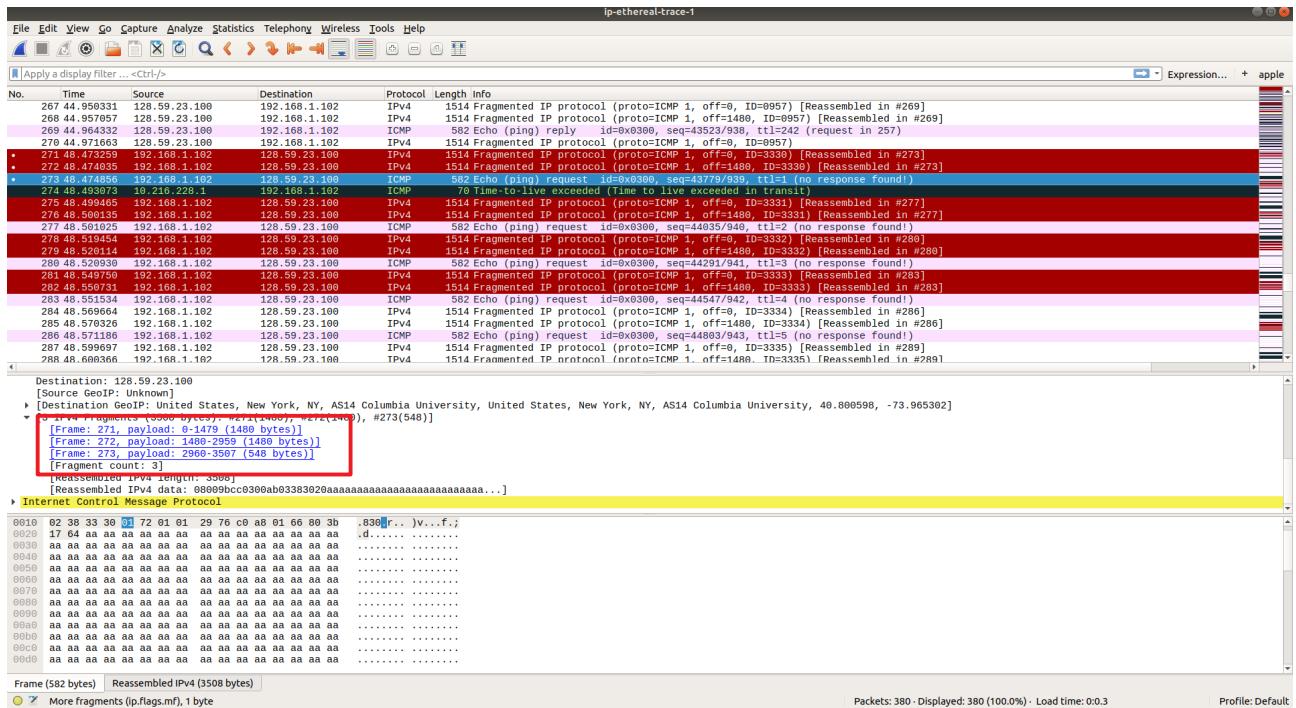


Fragment offset: 1480 olarak görülebilir. Bu sebeple bunun ilk fragment olmadığını söyleyebiliriz. Flagleri incelediğimizde ise More Fragments 0 olarak set edilmiş bundan dolayı da son fragment olduğunu söyleyebiliriz.

13-)

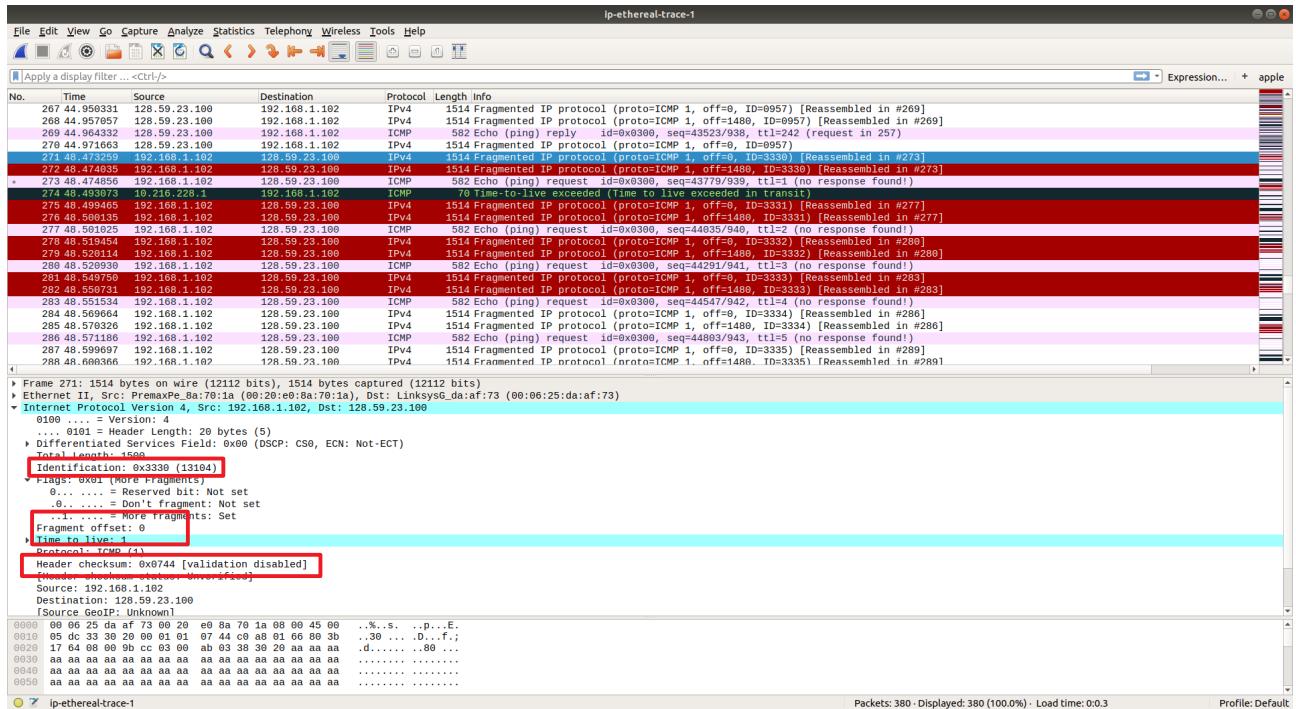
Total length, Flags, checksum ve fragment offset değerleri değişmiştir.

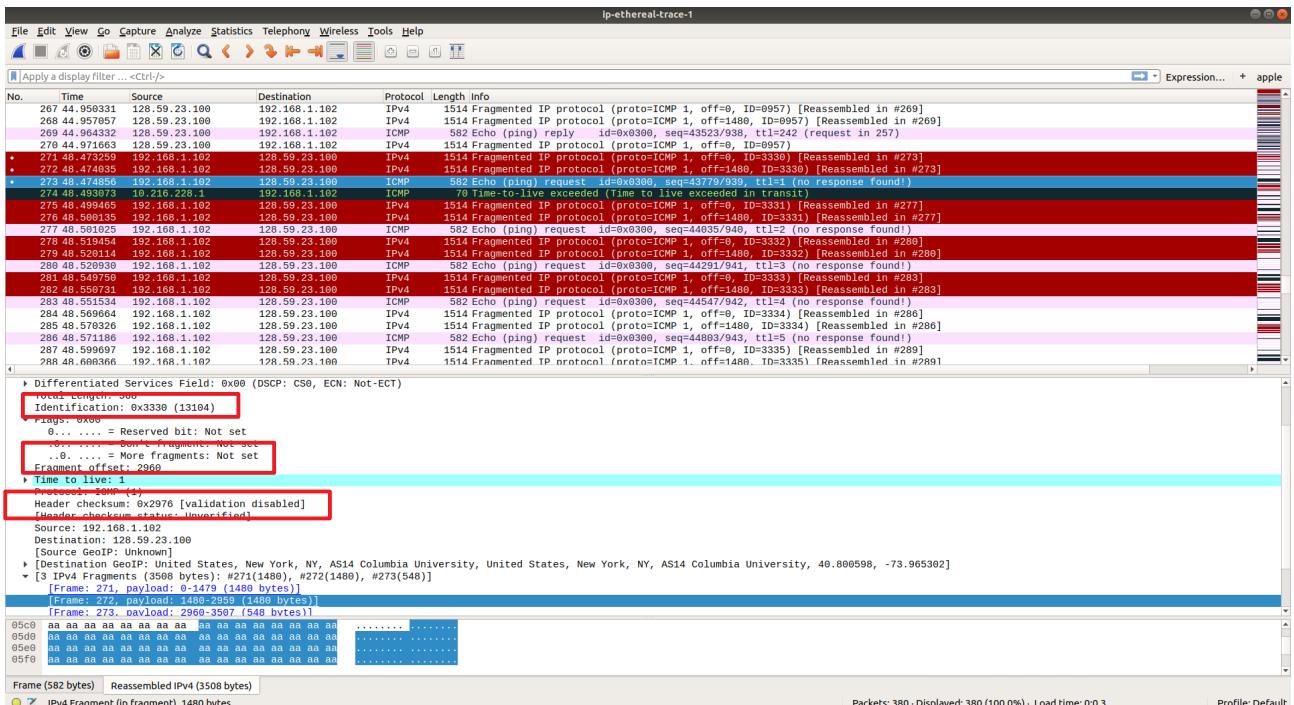
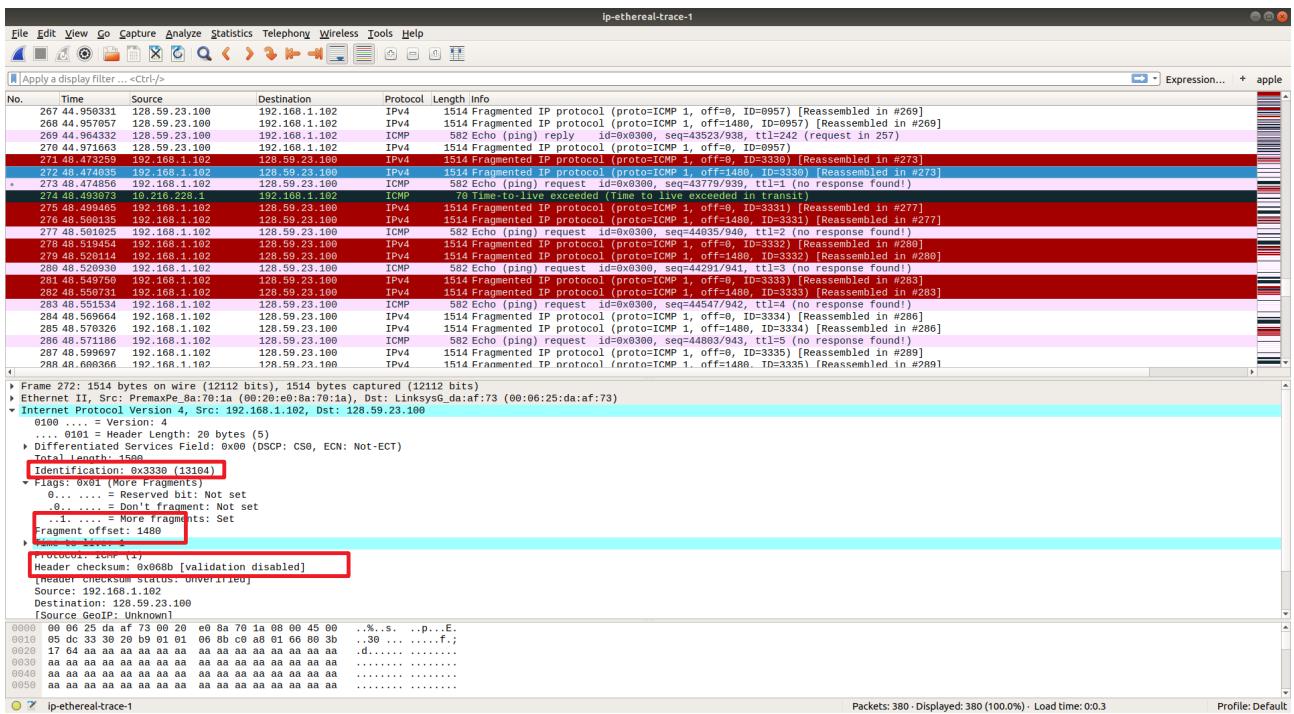
14-)



Fragment count'u 3 olarak görüyoruz.

15-)





Checksum, Identification, fragment offset ve Flags içerisindeki More fragments değişmiştir.