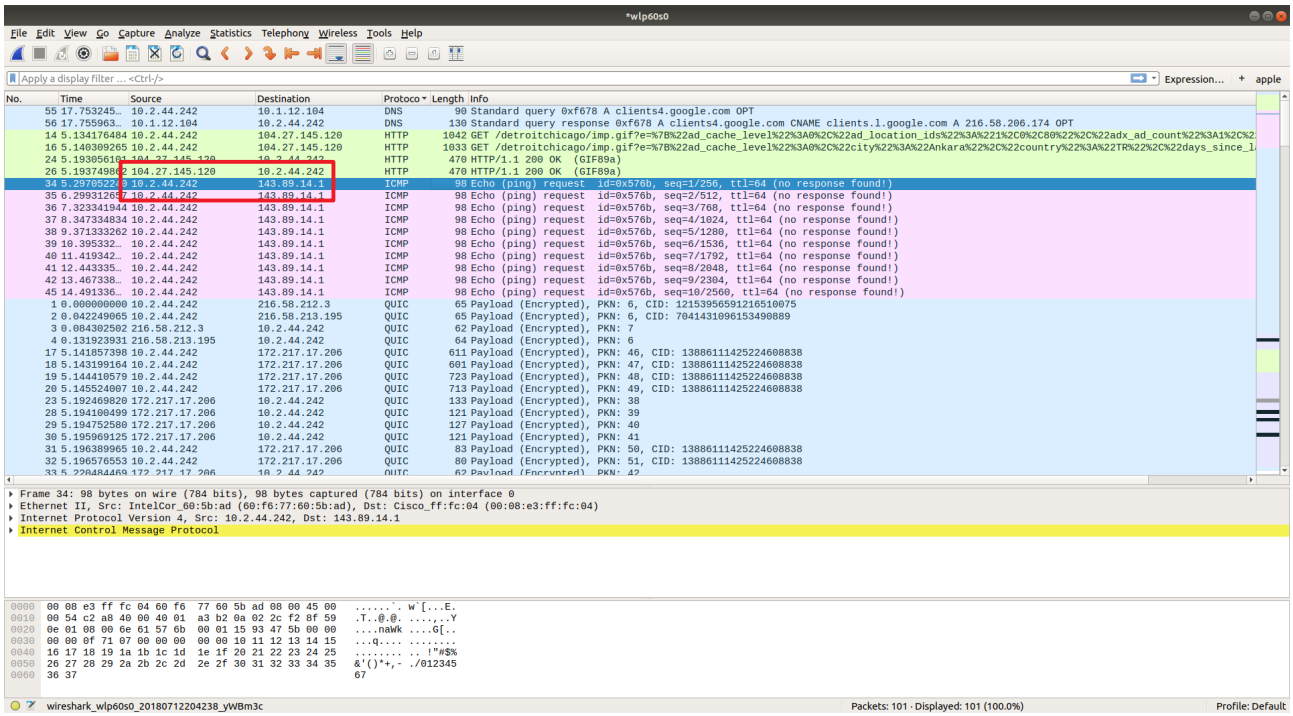
Bil 452 Ödev 6 -ICMP

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
```

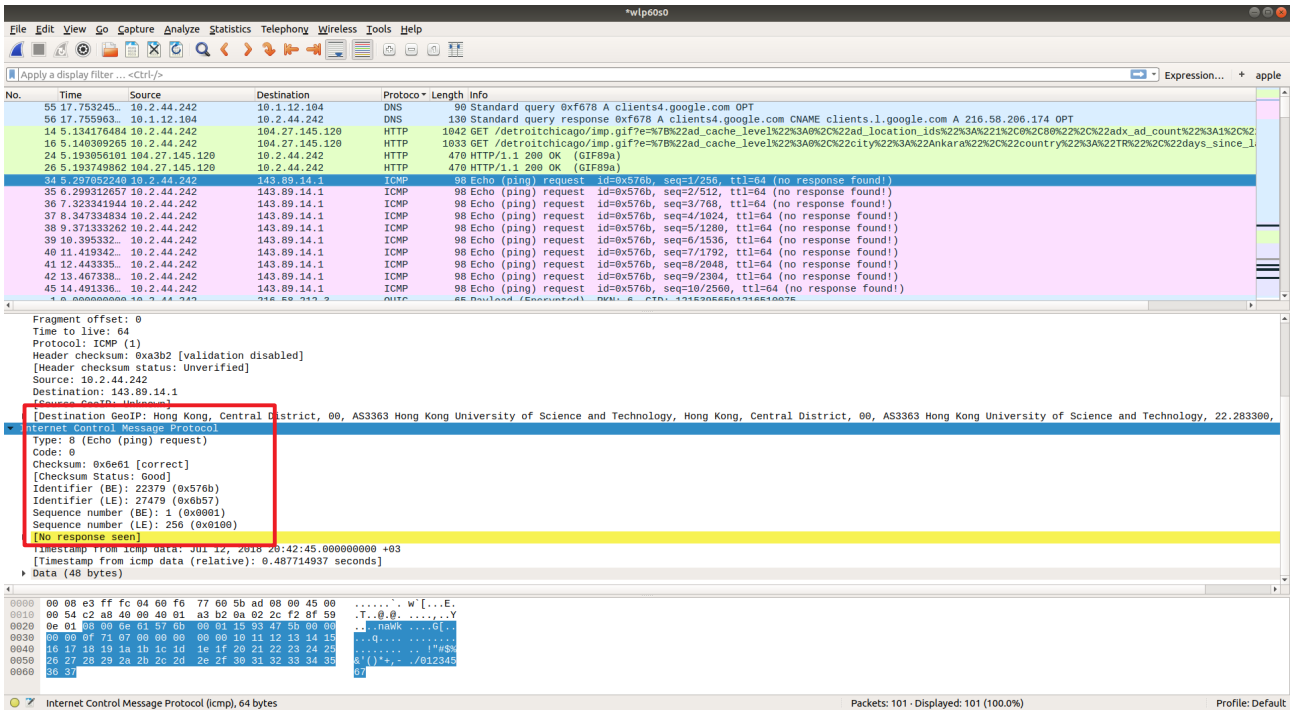


Source: 10.2.44.242
Destination: 143.89.14.1

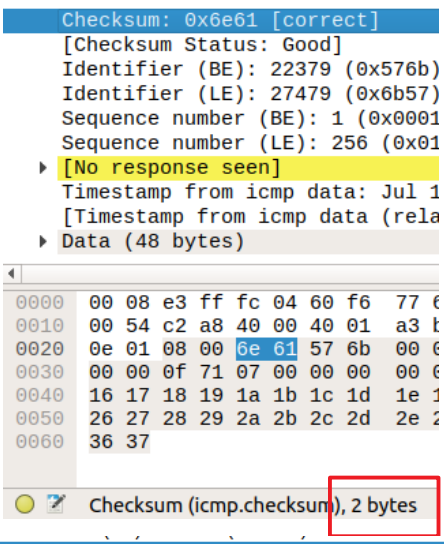
2-)

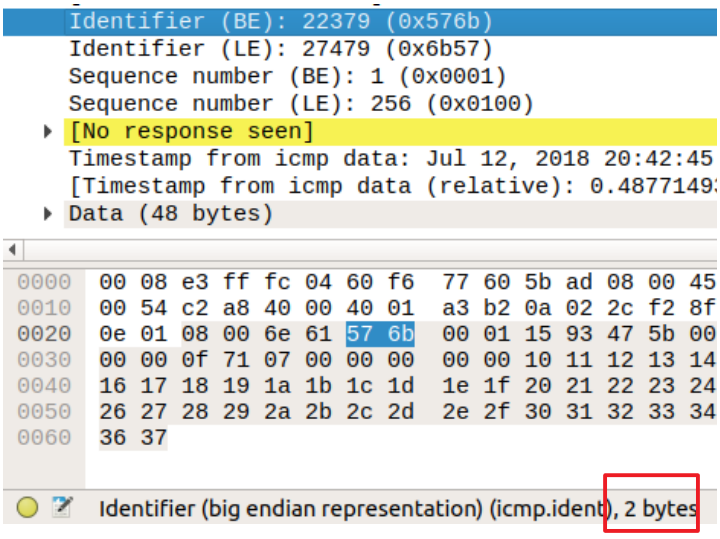
ICMP protokolü network layerda çalıştığı için protokole ihtiyaç duymaz.

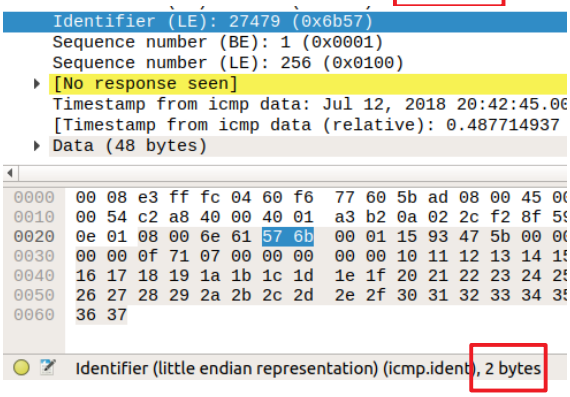
3-)

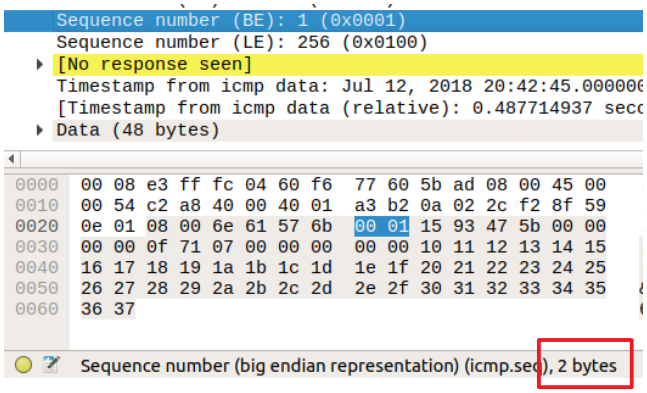


Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x6e61 [correct] ----------> 2 bytes
Identifier (BE): 22379 (0x576b) ----------> 2 bytes
Identifier (LE): 27479 (0x6b57) ----------> 2 bytes
Sequence number (BE): 1 (0x0001) ----------> 2 bytes
Sequence number (LE): 256 (0x0100) ----------> 2 bytes

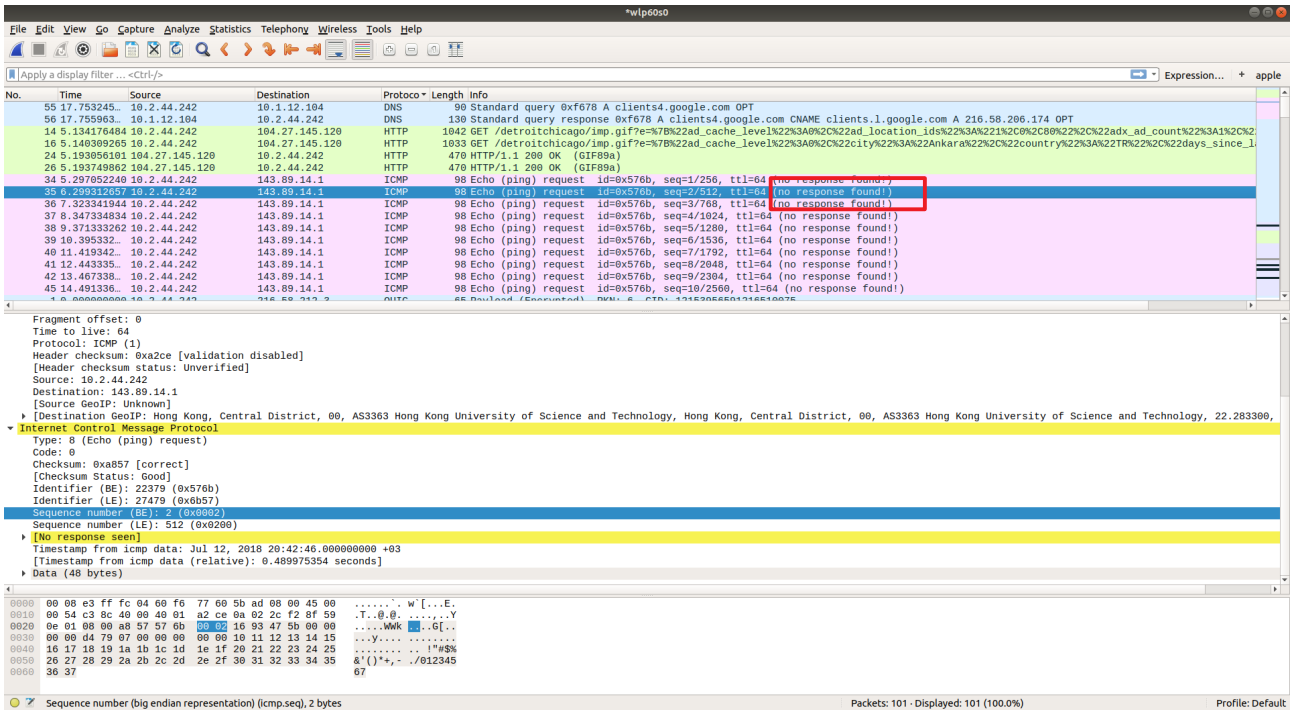








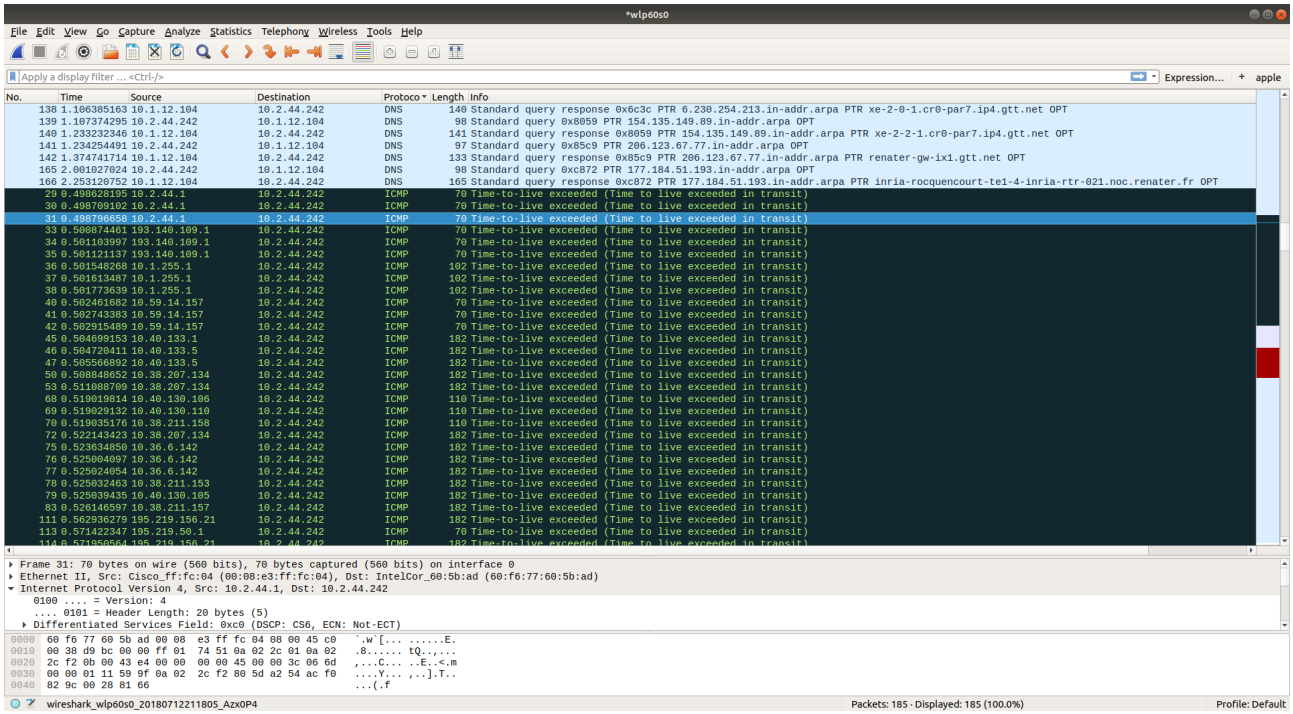
4-)



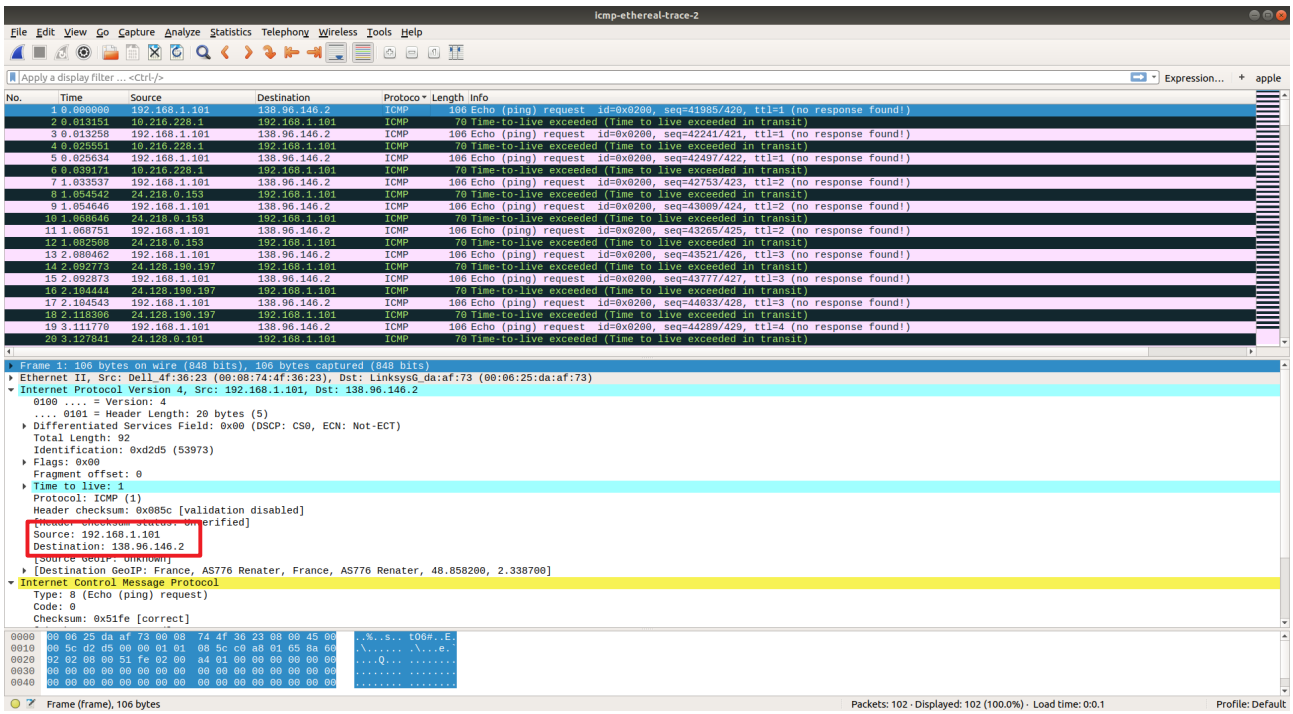
Yukaridaki ekran görüntüsünde görüldüğü üzere response olmadığı için bu soruyu cevaplayamadım. Ancak eğer olsaydı bir önceki soru ile yaklaşık olarak aynı field'ların olacağı tahmin edebiliriz.

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  10.40.133.1 (10.40.133.1)  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)  11.548 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  * * *
```



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

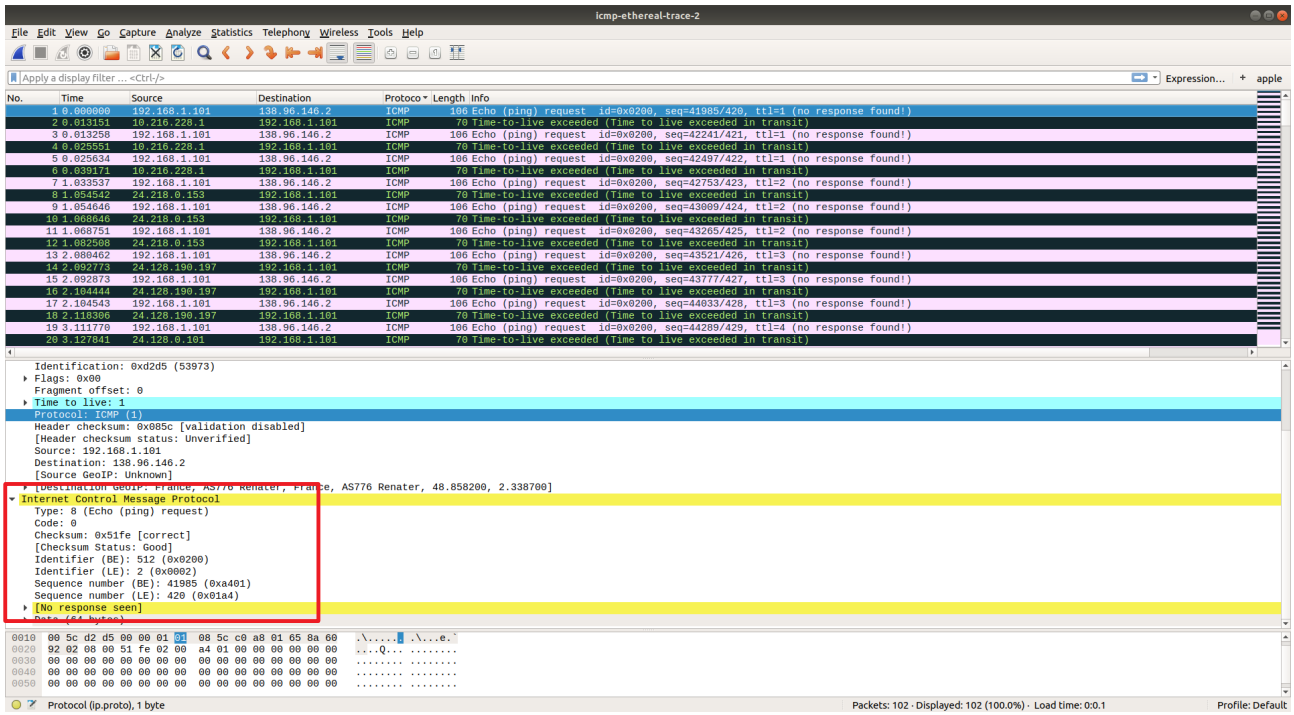


Source: 192.168.1.101
Destination: 138.96.146.2

6-)

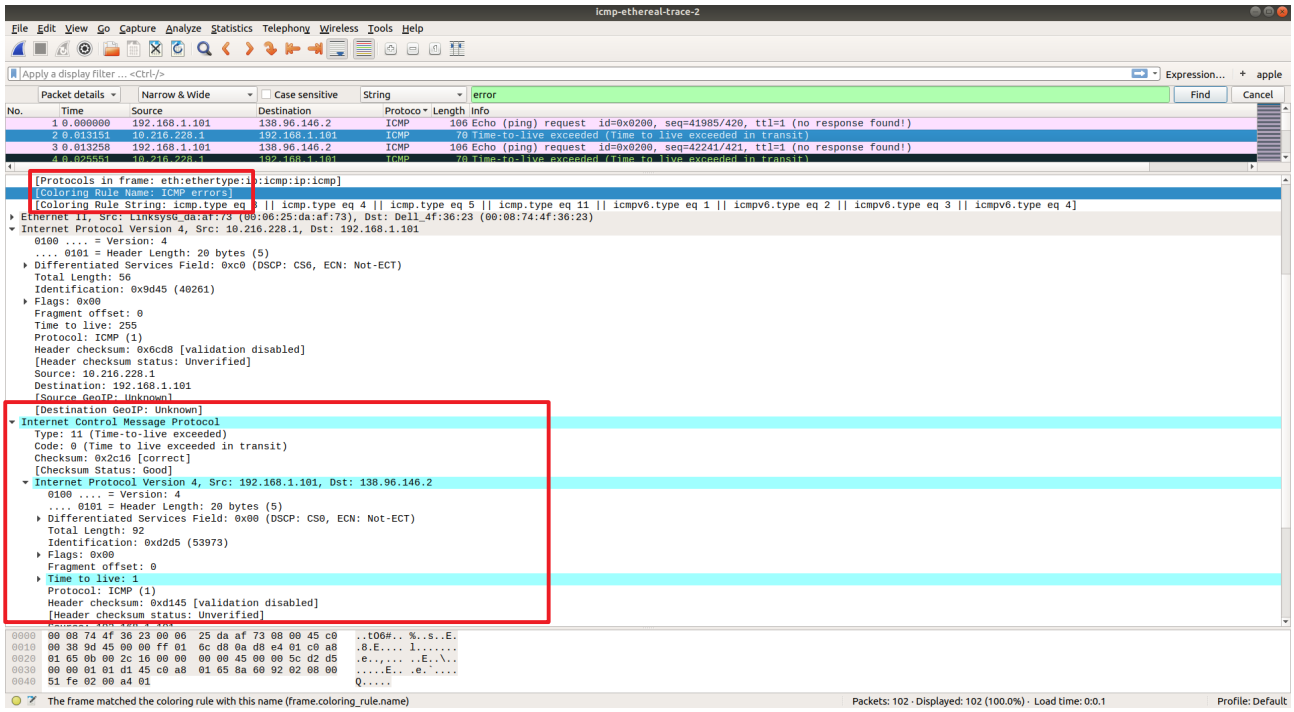
Eğer Linuxta'ki gibi UDP olarak gönderilirse 5. sorunun başında gösterdiğim çıktılara bakarsak (ben Linux kullanmaktayım) UDP kullanılsaydı 17 numarasını alırdı. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml buradan da görebiliriz.

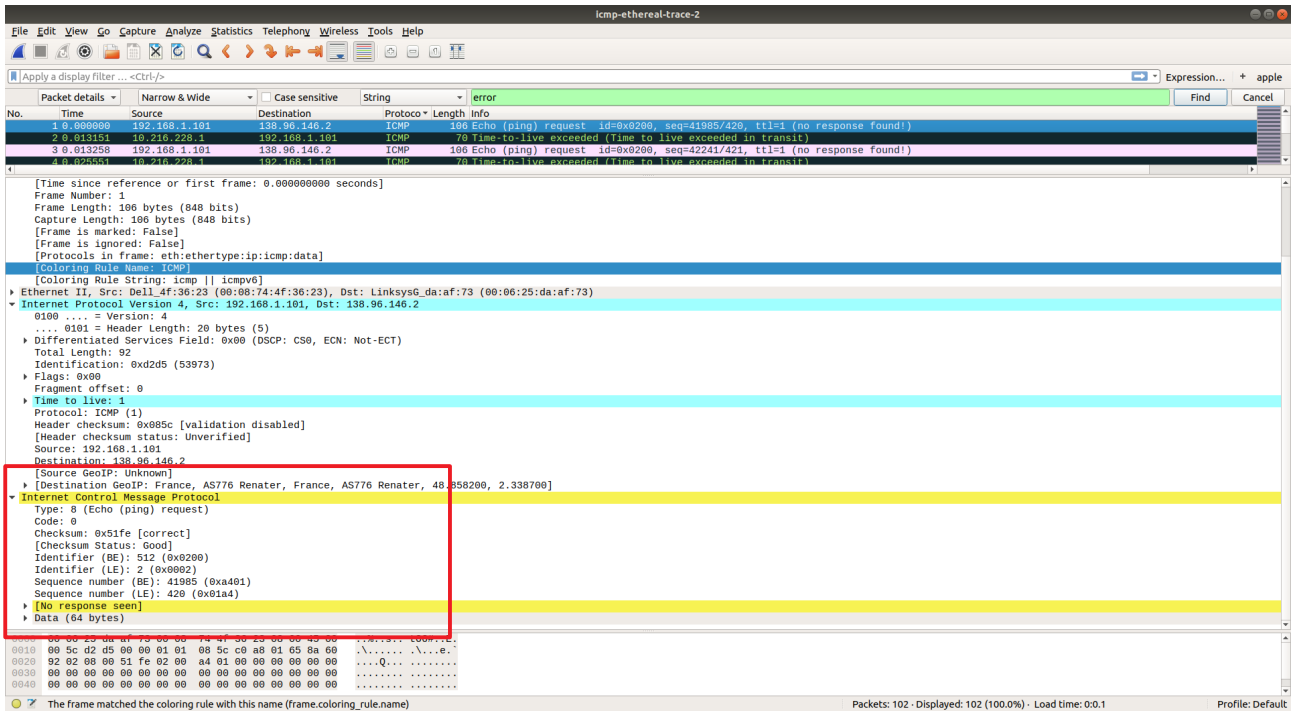
7-)



Field'lar ilk bölümdeki değerler ile aynıdır.

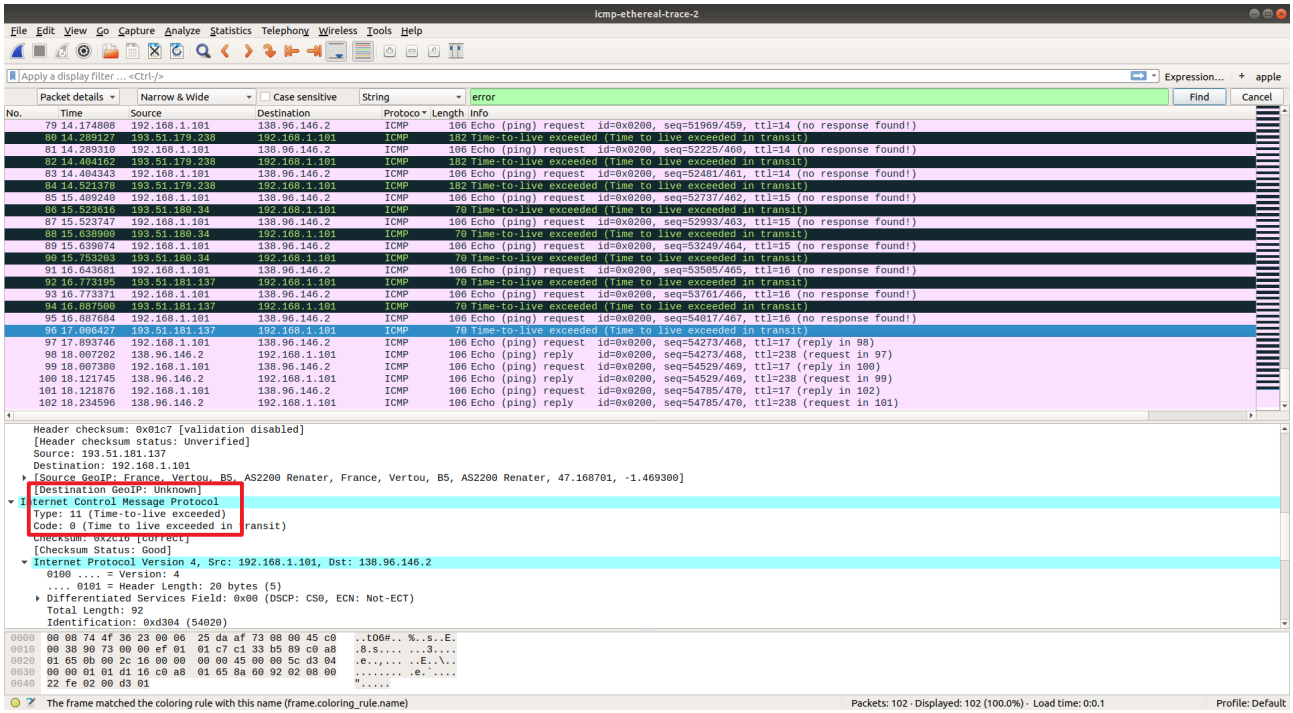
8-)

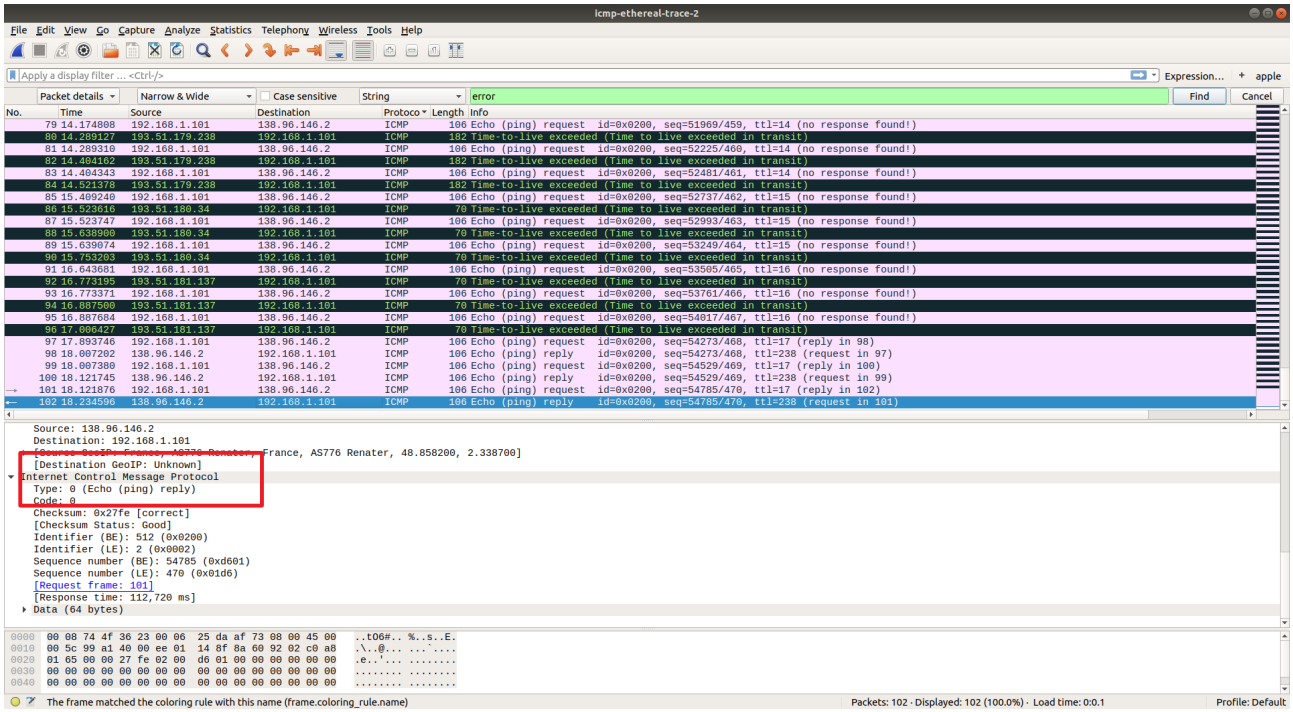




Görüldüğü gibi farklı bilgiler taşımaktadırlar üstteki ekran görüntüsü “error” için olandır.

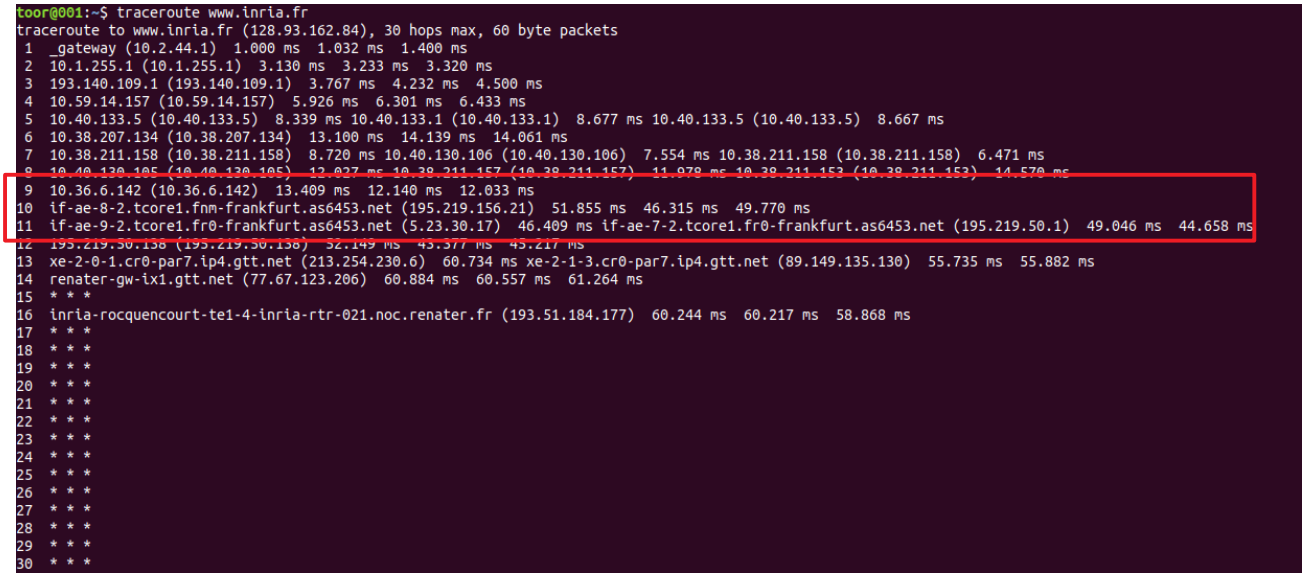
9-)





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

10-)



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