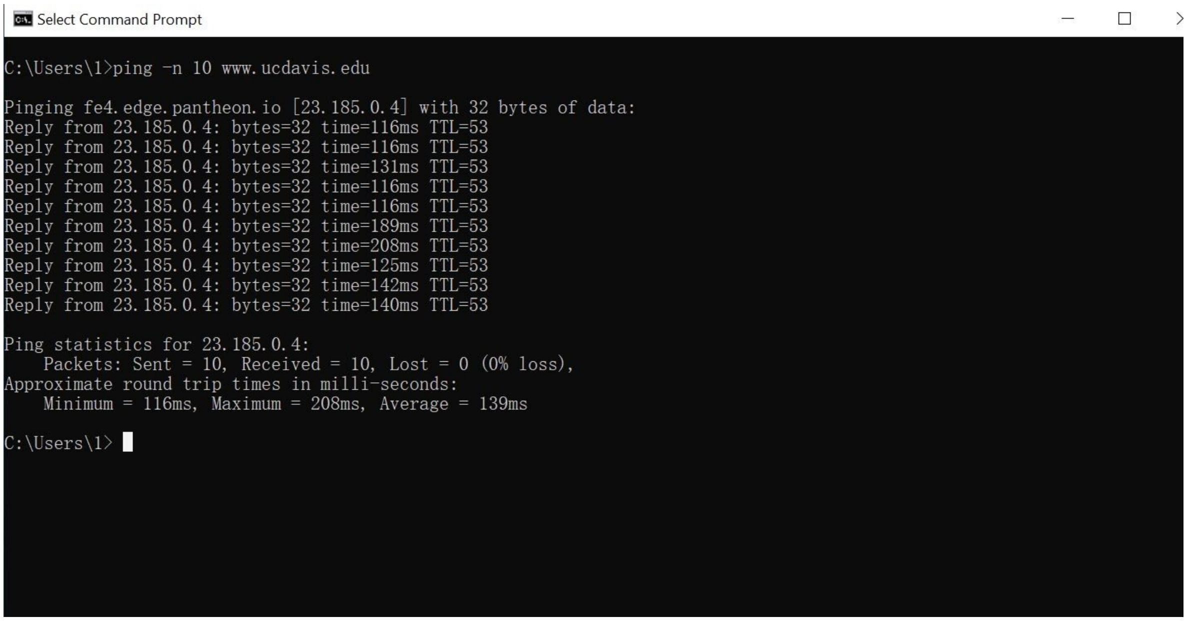
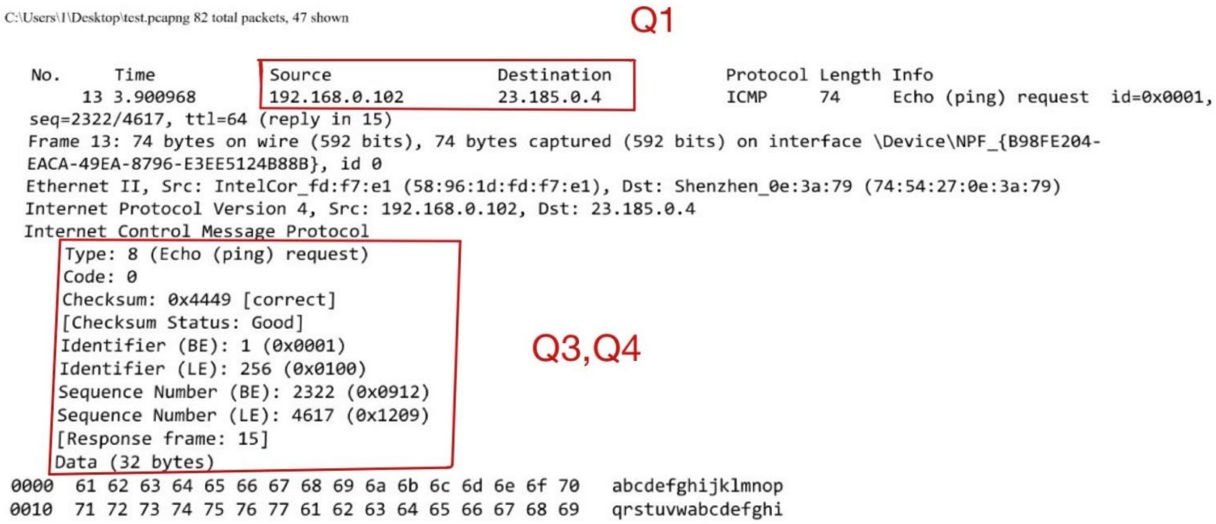
P1_Wireshark_ICMP

Programming 1



```
C:\Users\1>ping -n 10 www.ucdavis.edu

Pinging fe4.edge.pantheon.io [23.185.0.4] with 32 bytes of data:
Reply from 23.185.0.4: bytes=32 time=116ms TTL=53
Reply from 23.185.0.4: bytes=32 time=116ms TTL=53
Reply from 23.185.0.4: bytes=32 time=131ms TTL=53
Reply from 23.185.0.4: bytes=32 time=116ms TTL=53
Reply from 23.185.0.4: bytes=32 time=116ms TTL=53
Reply from 23.185.0.4: bytes=32 time=189ms TTL=53
Reply from 23.185.0.4: bytes=32 time=208ms TTL=53
Reply from 23.185.0.4: bytes=32 time=125ms TTL=53
Reply from 23.185.0.4: bytes=32 time=142ms TTL=53
Reply from 23.185.0.4: bytes=32 time=140ms TTL=53

Ping statistics for 23.185.0.4:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 116ms, Maximum = 208ms, Average = 139ms

C:\Users\1>
```

Figure 1 My screen shot of the Command Prompt window [I choose www.ucdavis.edu since I am now in China.]



```
C:\Users\1\Desktop\test.pcapng 82 total packets, 47 shown

No.     Time           Source                Destination          Protocol Length Info
     13 3.900968       192.168.0.102         23.185.0.4           ICMP     74     Echo (ping) request  id=0x0001,
seq=2322/4617, ttl=64 (reply in 15)
Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B98FE204-
EACA-49EA-8796-E3EE5124B88B}, id 0
Ethernet II, Src: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1), Dst: Shenzhen_0e:3a:79 (74:54:27:0e:3a:79)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 23.185.0.4
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4449 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 2322 (0x0912)
    Sequence Number (LE): 4617 (0x1209)
    [Response frame: 15]
    Data (32 bytes)
0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

Figure 2 The packet information for Q1, Q3, Q4

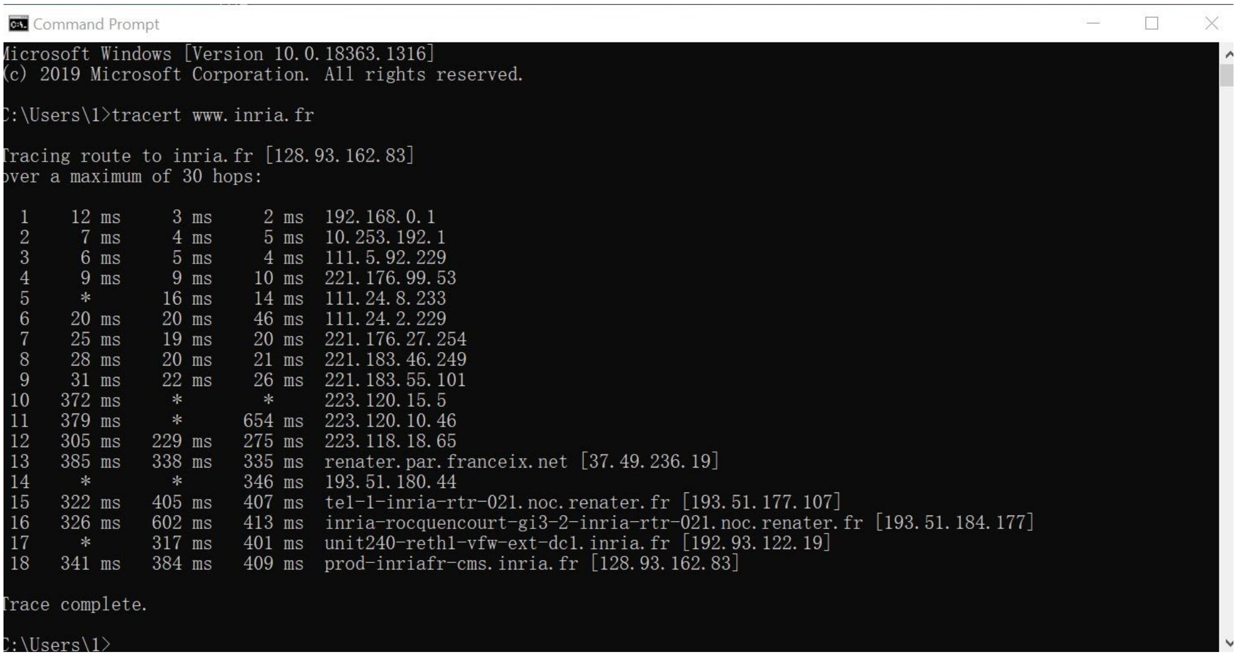
1. From the packet information above, it is clear to see that the IP address of my host is **192.168.0.102,** the IP address of the destination host is **23.185.0.4.**

2. **The Reason: ICMP packet does not have source and port number because it is specified as the upper-layer protocol and it only uses a type and a code field for ping.**[1]

3. From the packet information above, the ICMP type is **8 (Echo (ping request))** and code number is **0.** This ICMP packet also has other fields, such as **Checksum, Identifier (BE/LE), Sequence Number (BE/LE), and Data**.

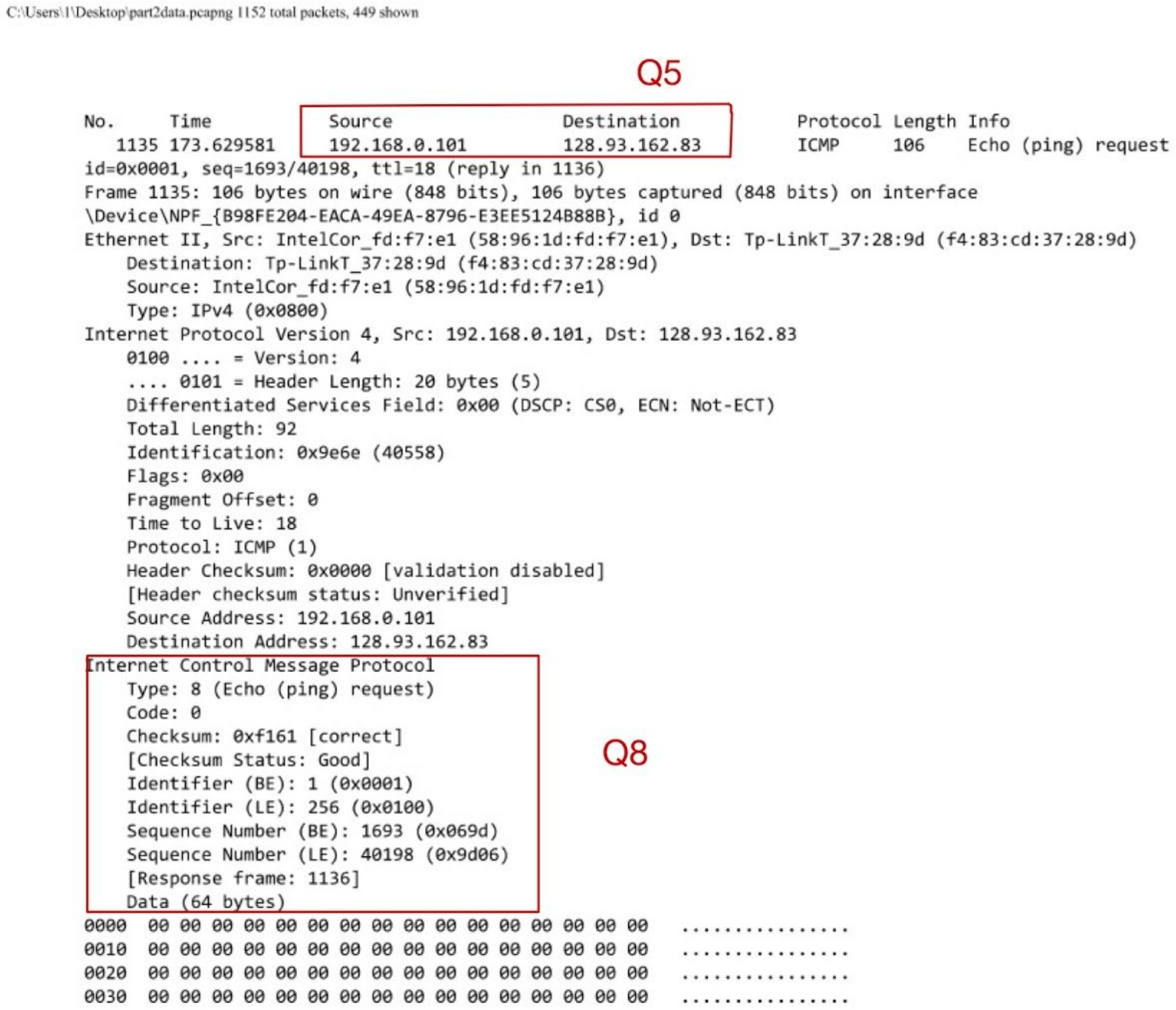
4. From the packet information above, we can know that Checksum, Identifier (BE/LE), and Sequence Number (BE/LE), are represented in **four hexadecimal digits (For example, 0x4449 for Checksum)**. Since we know that each hexadecimal digit represents 4 bits and 8 bits equal to 1 byte, in this case, Checksum, Identifier (BE/LE), and Sequence Number (BE/LE) are **4*4/8 = 2 bytes.**

[1] Refer to Textbook 5.6 ICMP: The Internet Control Message Protocol



```
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\1>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:

  1    12 ms     3 ms     2 ms  192.168.0.1
  2     7 ms     4 ms     5 ms  10.253.192.1
  3     6 ms     5 ms     4 ms  111.5.92.229
  4     9 ms     9 ms    10 ms  221.176.99.53
  5     *       16 ms    14 ms  111.24.8.233
  6    20 ms    20 ms    46 ms  111.24.2.229
  7    25 ms    19 ms    20 ms  221.176.27.254
  8    28 ms    20 ms    21 ms  221.183.46.249
  9    31 ms    22 ms    26 ms  221.183.55.101
 10   372 ms     *        *     223.120.15.5
 11   379 ms     *      654 ms  223.120.10.46
 12   305 ms   229 ms   275 ms  223.118.18.65
 13   385 ms   338 ms   335 ms  renater.par.franceix.net [37.49.236.19]
 14     *        *      346 ms  193.51.180.44
 15   322 ms   405 ms   407 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 16   326 ms   602 ms   413 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 17     *      317 ms   401 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 18   341 ms   384 ms   409 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Users\1>
```

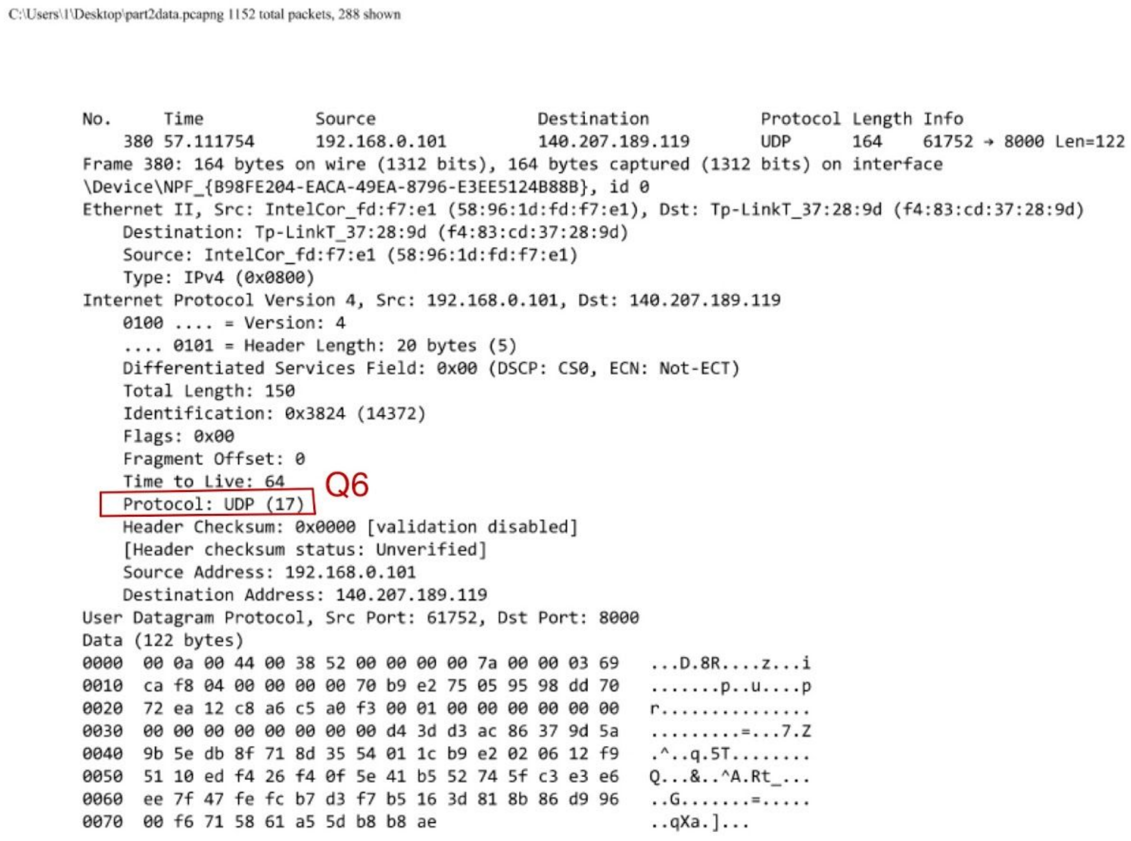
Figure 3 My screen shot of the Command Prompt window



```
C:\Users\1\Desktop\part2data.pcapng 1152 total packets, 449 shown

No.     Time          Source              Destination         Protocol Length Info
   1135 173.629581    192.168.0.101       128.93.162.83       ICMP     106    Echo (ping) request
id=0x0001, seq=1693/40198, ttl=18 (reply in 1136)
Frame 1135: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface
\Device\NPF_{B98FE204-EACA-49EA-8796-E3EE5124B88B}, id 0
Ethernet II, Src: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1), Dst: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
    Destination: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
    Source: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.93.162.83
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x9e6e (40558)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 18
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.101
    Destination Address: 128.93.162.83
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf161 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1693 (0x069d)
    Sequence Number (LE): 40198 (0x9d06)
    [Response frame: 1136]
    Data (64 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Figure 4 ICMP packets for Q5 and Q8

5. From the packet information above, we can see that the IP address of my host is **192.168.0.101** and the IP address of the target destination host is **128.93.162.83**.



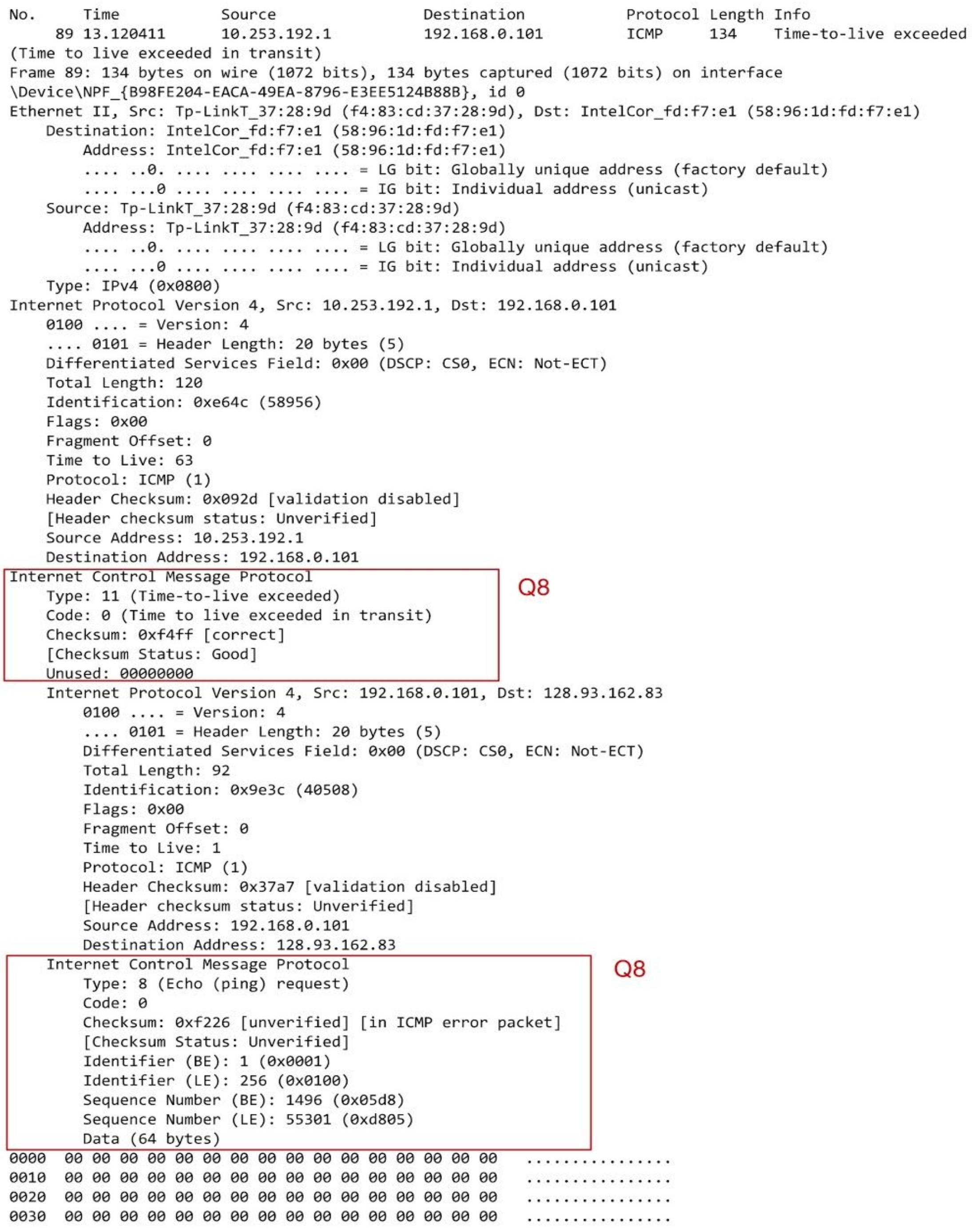
C:\Users\1\Desktop\part2data.pcapng 1152 total packets, 288 shown

```
No.     Time           Source                Destination           Protocol Length Info
    380 57.111754      192.168.0.101         140.207.189.119       UDP      164    61752 → 8000 Len=122
Frame 380: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface
\Device\NPF_{B98FE204-EACA-49EA-8796-E3EE5124B88B}, id 0
Ethernet II, Src: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1), Dst: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
    Destination: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
    Source: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 140.207.189.119
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 150
    Identification: 0x3824 (14372)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.101
    Destination Address: 140.207.189.119
User Datagram Protocol, Src Port: 61752, Dst Port: 8000
Data (122 bytes)
0000  00 0a 00 44 00 38 52 00 00 00 00 7a 00 00 03 69   ...D.8R....z...i
0010  ca f8 04 00 00 00 00 70 b9 e2 75 05 95 98 dd 70   .......p..u....p
0020  72 ea 12 c8 a6 c5 a0 f3 00 01 00 00 00 00 00 00   r...............
0030  00 00 00 00 00 00 00 00 d4 3d d3 ac 86 37 9d 5a   .........=...7.Z
0040  9b 5e db 8f 71 8d 35 54 01 1c b9 e2 02 06 12 f9   .^..q.5T........
0050  51 10 ed f4 26 f4 0f 5e 41 b5 52 74 5f c3 e3 e6   Q...&..^A.Rt_...
0060  ee 7f 47 fe fc b7 d3 f7 b5 16 3d 81 8b 86 d9 96   ..G.......=.....
0070  00 f6 71 58 61 a5 5d b8 b8 ae                     ..qXa.]...
```

Figure 5 about UDP packets [Q6]

6. No, by randomly picking up a UDP packet in my data, we can see that the IP protocol number for the probe packets is **17**.
7. No, they are the same.

C:\Users\1\Desktop\part2data.pcapng 1152 total packets, 449 shown



```
No.     Time           Source                Destination           Protocol Length Info
     89 13.120411      10.253.192.1          192.168.0.101         ICMP     134    Time-to-live exceeded
(Time to live exceeded in transit)
Frame 89: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface
\Device\NPF_{B98FE204-EACA-49EA-8796-E3EE5124B88B}, id 0
Ethernet II, Src: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d), Dst: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
    Destination: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        Address: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        Address: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.253.192.1, Dst: 192.168.0.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 120
    Identification: 0xe64c (58956)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0x092d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.253.192.1
    Destination Address: 192.168.0.101
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
    Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.93.162.83
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 92
        Identification: 0x9e3c (40508)
        Flags: 0x00
        Fragment Offset: 0
        Time to Live: 1
        Protocol: ICMP (1)
        Header Checksum: 0x37a7 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.101
        Destination Address: 128.93.162.83
    Internet Control Message Protocol
        Type: 8 (Echo (ping) request)
        Code: 0
        Checksum: 0xf226 [unverified] [in ICMP error packet]
        [Checksum Status: Unverified]
        Identifier (BE): 1 (0x0001)
        Identifier (LE): 256 (0x0100)
        Sequence Number (BE): 1496 (0x05d8)
        Sequence Number (LE): 55301 (0xd805)
        Data (64 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Q8

Q8

Figure 6: ICMP error packet about Q8 [need to compare with Figure 4]

8. By comparing the ICMP error packet and the normal ICMP echo packet above, we can see that the ICMP error packet has **two parts of Internet Control Message Protocol. The first part belongs to itself, having Type 11 for Time-to-live exceeded and a field called “unused”, which only has “00000000”. The second part of Internet Control Message Protocol is much similar to the normal ICMP echo packet.**

```
No.     Time           Source                Destination           Protocol Length Info
   1150 175.418140     211.20.171.198        192.168.0.101         ICMP     58     Echo (ping) reply
id=0x0001, seq=1695/40710, ttl=46 (request in 1149)
Frame 1150: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{B98FE204-
EACA-49EA-8796-E3EE5124B88B}, id 0
Ethernet II, Src: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d), Dst: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
    Destination: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        Address: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        Address: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 211.20.171.198, Dst: 192.168.0.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x04 (DSCP: LE, ECN: Not-ECT)
    Total Length: 44
    Identification: 0x1b68 (7016)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 46
    Protocol: ICMP (1)
    Header Checksum: 0x317d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 211.20.171.198
    Destination Address: 192.168.0.101
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)       Q9
    Code: 0
    Checksum: 0x628e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1695 (0x069f)
    Sequence Number (LE): 40710 (0x9f06)
    [Request frame: 1149]
    [Response time: 96.091 ms]
    Data (16 bytes)
0000  44 72 61 67 6f 6e 20 49 43 4d 50 20 65 63 68 6f   Dragon ICMP echo
No.     Time           Source                Destination           Protocol Length Info
   1151 176.420153     192.168.0.101         211.20.171.198        ICMP     58     Echo (ping) request
id=0x0001, seq=1696/40966, ttl=255 (reply in 1152)
Frame 1151: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{B98FE204-
EACA-49EA-8796-E3EE5124B88B}, id 0
Ethernet II, Src: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1), Dst: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
    Destination: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        Address: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        Address: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 211.20.171.198
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0xc9c4 (51652)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.101
    Destination Address: 211.20.171.198
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)         Q9
    Code: 0
    Checksum: 0x5a8d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1696 (0x06a0)
    Sequence Number (LE): 40966 (0xa006)
    [Response frame: 1152]
    Data (16 bytes)
0000  44 72 61 67 6f 6e 20 49 43 4d 50 20 65 63 68 6f   Dragon ICMP echo
No.     Time           Source                Destination           Protocol Length Info
   1152 176.503414     211.20.171.198        192.168.0.101         ICMP     58     Echo (ping) reply
id=0x0001, seq=1696/40966, ttl=46 (request in 1151)
Frame 1152: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{B98FE204-
EACA-49EA-8796-E3EE5124B88B}, id 0
Ethernet II, Src: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d), Dst: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
    Destination: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        Address: IntelCor_fd:f7:e1 (58:96:1d:fd:f7:e1)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        Address: Tp-LinkT_37:28:9d (f4:83:cd:37:28:9d)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 211.20.171.198, Dst: 192.168.0.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x04 (DSCP: LE, ECN: Not-ECT)
    Total Length: 44
    Identification: 0x1e49 (7753)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 46
    Protocol: ICMP (1)
    Header Checksum: 0x2e9c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 211.20.171.198
    Destination Address: 192.168.0.101
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)         Q9
    Code: 0
    Checksum: 0x628d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1696 (0x06a0)
    Sequence Number (LE): 40966 (0xa006)
    [Request frame: 1151]
    [Response time: 83.261 ms]
    Data (16 bytes)
0000  44 72 61 67 6f 6e 20 49 43 4d 50 20 65 63 68 6f   Dragon ICMP echo
```

Figure 7: the last three ICMP about Q9

9. From the information about the last three ICMP packets above, we can see that they have different Types from the ICMP error packets. This is because different kinds of ICMP packets have different Types, for example, ICMP packets sent by the source host have **Type = 8 (Echo(ping) request),** ICMP packets received by the source host have **Type = 0 (Echo(ping) reply),** and ICMP error packets have **Type = 11 for Time-to-live exceeded.**
10. In my tracert measurement, it is clear to see that the **10th link** delay is significantly longer than the others. Refer to the screenshot in Figure 4 of the Lab file, we can see that it is also the **10th link** delay that is significantly longer than the others. But this might be a coincidence. Since based on the router names, the location of the two routers in the example is in **New York City(nyc)** and **France (Pastourellor is a word in French). In addiction, since I am in China now,** the location of the two routers in my measurement is in **Beijing and France.**