1. What is the IP address of your host? What is the IP address of the destination host?

Source Host: 192.168.1.101

Destination Host: 143.89.14.34

2. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP packet is distinguished by request and reply so that the packet doesn't have source and destination port numbers.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

ICMP Type: 8

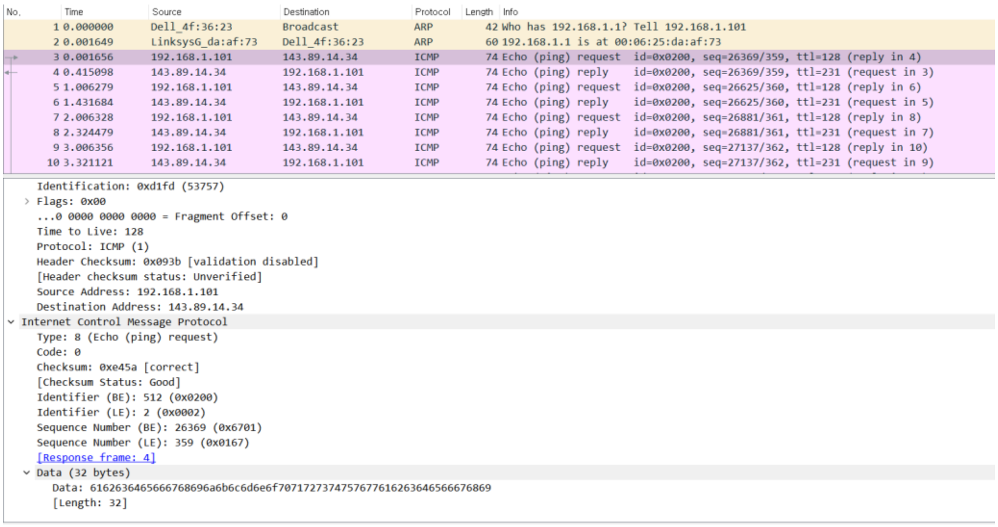
ICMP Code: 0

The packet has Checksum, Identifier, Sequence Number, and Data field.

Checksum: 2 bytes

Sequence Number: 4 bytes (BE: 2 bytes / LE: 2 bytes)

Identifier fields: 4 bytes (BE: 2 bytes / LE: 2 bytes)



```
No.   Time        Source             Destination     Protocol  Length Info
   1 0.000000    Dell_4f:36:23      Broadcast        ARP       42 Who has 192.168.1.1? Tell 192.168.1.101
   2 0.001649    LinksysG_da:af:73  Dell_4f:36:23    ARP       60 192.168.1.1 is at 00:06:25:da:af:73
   3 0.001656    192.168.1.101      143.89.14.34     ICMP      74 Echo (ping) request  id=0x0200, seq=26369/359, ttl=128 (reply in 4)
   4 0.415098    143.89.14.34       192.168.1.101    ICMP      74 Echo (ping) reply    id=0x0200, seq=26369/359, ttl=231 (request in 3)
   5 1.006279    192.168.1.101      143.89.14.34     ICMP      74 Echo (ping) request  id=0x0200, seq=26625/360, ttl=128 (reply in 6)
   6 1.431684    143.89.14.34       192.168.1.101    ICMP      74 Echo (ping) reply    id=0x0200, seq=26625/360, ttl=231 (request in 5)
   7 2.006328    192.168.1.101      143.89.14.34     ICMP      74 Echo (ping) request  id=0x0200, seq=26881/361, ttl=128 (reply in 8)
   8 2.324479    143.89.14.34       192.168.1.101    ICMP      74 Echo (ping) reply    id=0x0200, seq=26881/361, ttl=231 (request in 7)
   9 3.006356    192.168.1.101      143.89.14.34     ICMP      74 Echo (ping) request  id=0x0200, seq=27137/362, ttl=128 (reply in 10)
  10 3.321121    143.89.14.34       192.168.1.101    ICMP      74 Echo (ping) reply    id=0x0200, seq=27137/362, ttl=231 (request in 9)

    Identification: 0xd1fd (53757)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.101
    Destination Address: 143.89.14.34
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe45a [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 26369 (0x6701)
    Sequence Number (LE): 359 (0x0167)
    [Response frame: 4]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

(Frame Number: 3)

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

ICMP Type: 0

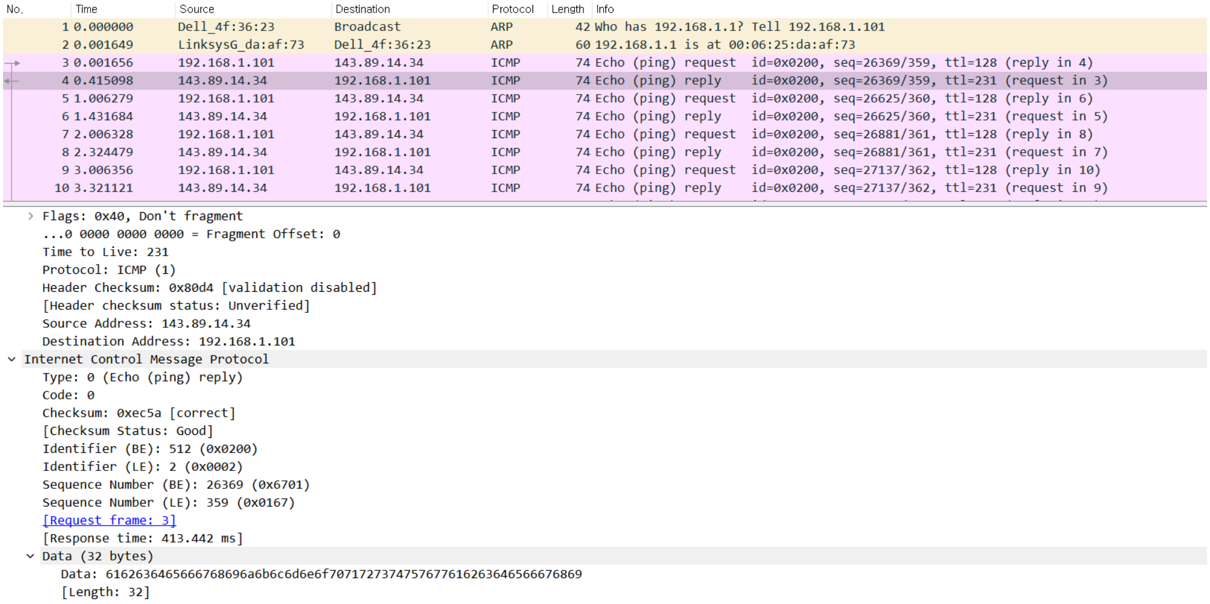
ICMP Code: 0

The packet has Checksum, Identifier, Sequence Number, and Data field.

Checksum: 2 bytes

Sequence Number: 4 bytes (LE: 2 bytes / BE: 2 bytes)

Identifier: 4 bytes (LE: 2 bytes / BE: 2 bytes)



```
No.   Time      Source           Destination     Protocol  Length  Info
   1 0.000000   Dell_4f:36:23    Broadcast       ARP        42 Who has 192.168.1.1? Tell 192.168.1.101
   2 0.001649   LinksysG_da:af:73 Dell_4f:36:23  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 0.001656   192.168.1.101    143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=26369/359, ttl=128 (reply in 4)
   4 0.415098   143.89.14.34     192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=26369/359, ttl=231 (request in 3)
   5 1.006279   192.168.1.101    143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=26625/360, ttl=128 (reply in 6)
   6 1.431684   143.89.14.34     192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=26625/360, ttl=231 (request in 5)
   7 2.006328   192.168.1.101    143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=26881/361, ttl=128 (reply in 8)
   8 2.324479   143.89.14.34     192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=26881/361, ttl=231 (request in 7)
   9 3.006356   192.168.1.101    143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=27137/362, ttl=128 (reply in 10)
  10 3.321121   143.89.14.34     192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=27137/362, ttl=231 (request in 9)
```

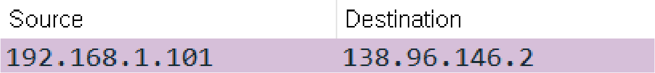
```
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 231
    Protocol: ICMP (1)
    Header Checksum: 0x80d4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 143.89.14.34
    Destination Address: 192.168.1.101
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xec5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 26369 (0x6701)
    Sequence Number (LE): 359 (0x0167)
    [Request frame: 3]
    [Response time: 413.442 ms]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

(Frame Number: 4)

5. What is the IP address of your host? What is the IP address of the target destination host?

Source Host: 192.168. 1.101

Target Destination Host: 138.96.146.2

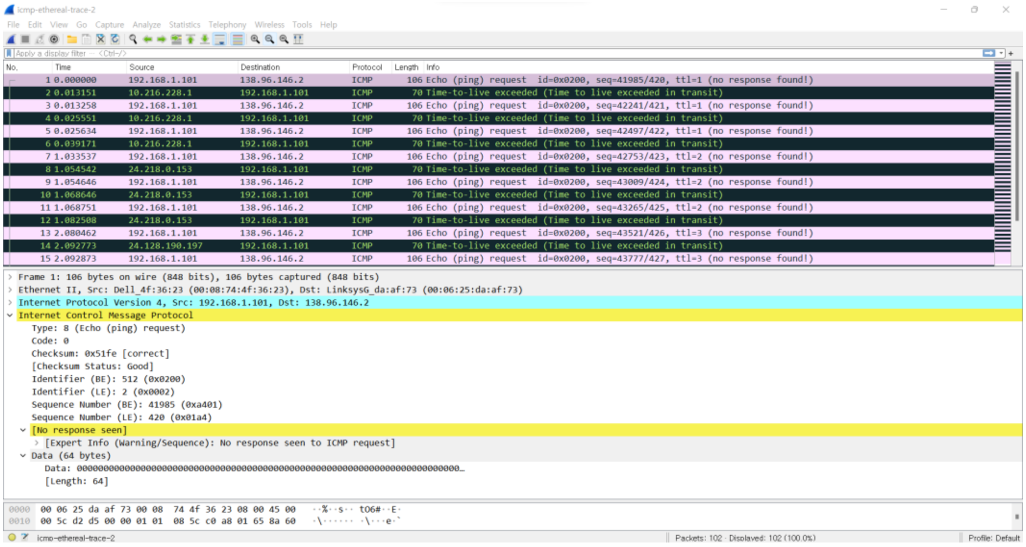


Source	Destination
192.168.1.101	138.96.146.2

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

If the ICMP sent UDP packets then, the IP protocol number will not be change from 01 because ICMP is in network layer, and UDP is in transport layer.

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?


icmp-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

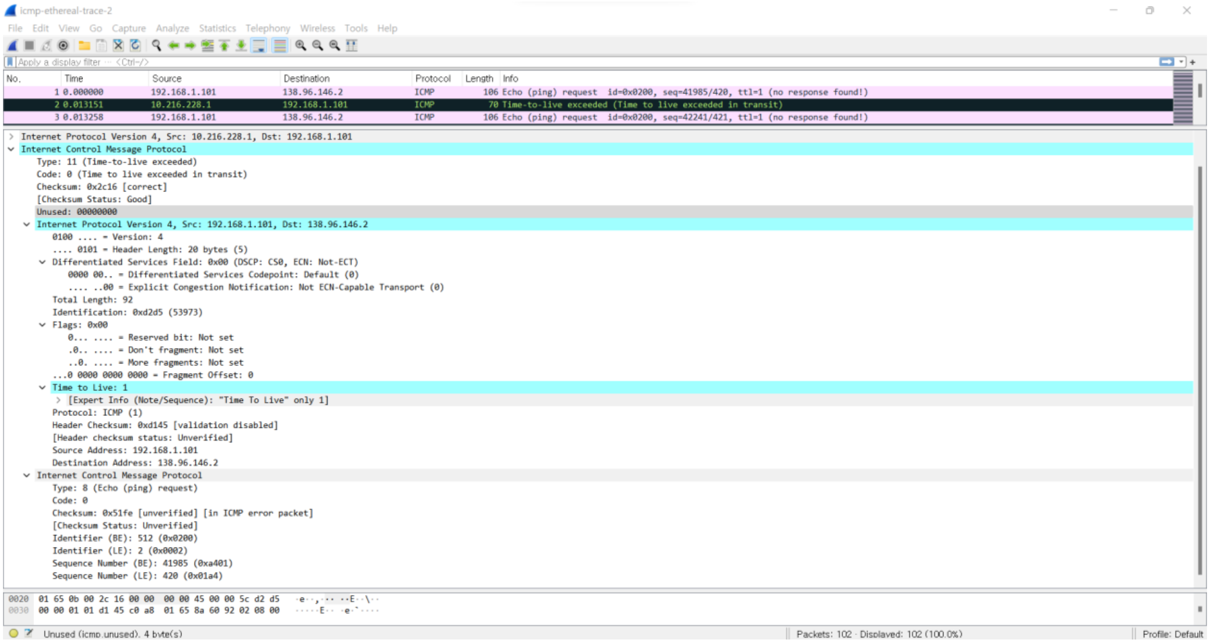
```
No.   Time      Source          Destination     Protocol  Length  Info
   1 0.000000   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=41985/420, ttl=1 (no response found!)
   2 0.013151   10.216.228.1    192.168.1.101   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   3 0.013258   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=42241/421, ttl=1 (no response found!)
   4 0.025551   10.216.228.1    192.168.1.101   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   5 0.025634   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=42497/422, ttl=1 (no response found!)
   6 0.039171   10.216.228.1    192.168.1.101   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   7 1.033537   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=42753/423, ttl=2 (no response found!)
   8 1.054542   24.218.0.153    192.168.1.101   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   9 1.054646   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=43009/424, ttl=2 (no response found!)
  10 1.068646   24.218.0.153    192.168.1.101   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  11 1.068751   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=43265/425, ttl=2 (no response found!)
  12 1.082508   24.218.0.153    192.168.1.101   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  13 2.080462   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=43521/426, ttl=3 (no response found!)
  14 2.092773   24.128.190.197  192.168.1.101   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  15 2.092873   192.168.1.101   138.96.146.2    ICMP      106 Echo (ping) request  id=0x0200, seq=43777/427, ttl=3 (no response found!)
```

```
> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
v 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)
  v [No response seen]
    > [Expert Info (Warning/Sequence): No response seen to ICMP request]
  v Data (64 bytes)
      Data: 0000000000000000000000000000000000000000000000000000000000000000…
      [Length: 64]
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  00 5c d2 d5 00 00 01 01  08 5c c0 a8 01 65 8a 60   ·\······ ·\···e·`
```

Yes, it is. There is no response frame in the ICMP echo packet.

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

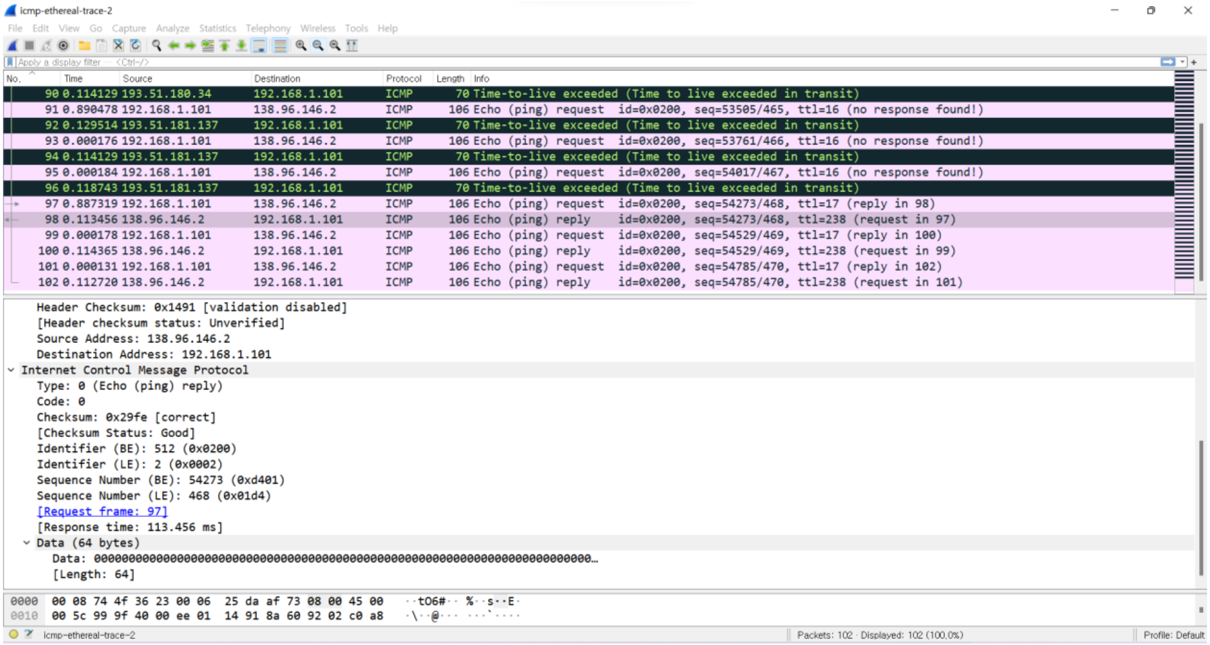

icmp-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source         Destination    Protocol Length Info
    1 0.000000  192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=41985/420, ttl=1 (no response found!)
    2 0.013151  10.216.228.1   192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    3 0.013258  192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=42241/421, ttl=1 (no response found!)

> Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x2c16 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  v Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
      Total Length: 92
      Identification: 0xd2d5 (53973)
    v Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment Offset: 0
    v Time to Live: 1
      > [Expert Info (Note/Sequence): "Time To Live" only 1]
      Protocol: ICMP (1)
      Header Checksum: 0xd145 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.1.101
      Destination Address: 138.96.146.2
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x51fe [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 512 (0x0200)
      Identifier (LE): 2 (0x0002)
      Sequence Number (BE): 41985 (0xa401)
      Sequence Number (LE): 420 (0x01a4)

0020  01 65 0b 00 2c 16 00 00  00 00 45 00 00 5c d2 d5   ·e··,··· ··E··\··
0030  00 00 01 01 d1 45 c0 a8  01 65 8a 60 92 02 08 00   ·····E·· ·e·`····

Unused (icmp.unused), 4 byte(s)          Packets: 102 · Displayed: 102 (100.0%)          Profile: Default
```

(Frame Number: 2)

In the ICMP error packet, there is IPV4 field which contains Source and Destination address, Flags, TTL, and other information.

9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

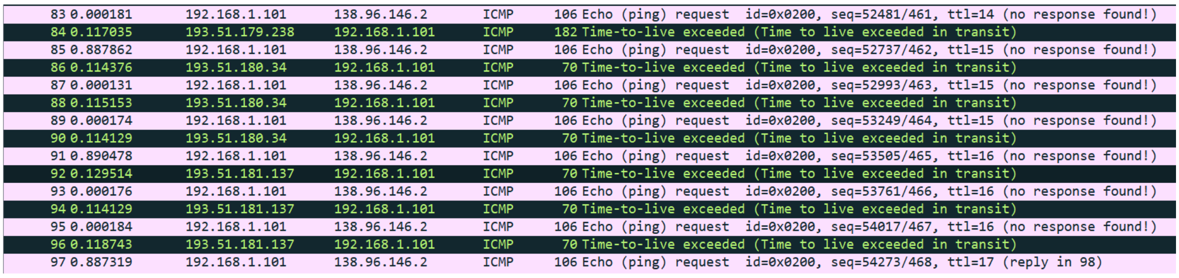

icmp-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time     Source         Destination    Protocol Length Info
   90 0.114129 193.51.180.34  192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   91 0.890478 192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=53505/465, ttl=16 (no response found!)
   92 0.129514 193.51.181.137 192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   93 0.000176 192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=53761/466, ttl=16 (no response found!)
   94 0.114129 193.51.181.137 192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   95 0.000184 192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54017/467, ttl=16 (no response found!)
   96 0.118743 193.51.181.137 192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   97 0.887319 192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54273/468, ttl=17 (reply in 98)
   98 0.113456 138.96.146.2   192.168.1.101  ICMP     106 Echo (ping) reply    id=0x0200, seq=54273/468, ttl=238 (request in 97)
   99 0.000178 192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54529/469, ttl=17 (reply in 100)
  100 0.114365 138.96.146.2   192.168.1.101  ICMP     106 Echo (ping) reply    id=0x0200, seq=54529/469, ttl=238 (request in 99)
  101 0.000131 192.168.1.101  138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54785/470, ttl=17 (reply in 102)
  102 0.112720 138.96.146.2   192.168.1.101  ICMP     106 Echo (ping) reply    id=0x0200, seq=54785/470, ttl=238 (request in 101)

    Header Checksum: 0x1491 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 138.96.146.2
    Destination Address: 192.168.1.101
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x29fe [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 54273 (0xd401)
    Sequence Number (LE): 468 (0x01d4)
    [Request frame: 97]
    [Response time: 113.456 ms]
  v Data (64 bytes)
      Data: 0000000000000000000000000000000000000000000000000000000000000000…
      [Length: 64]

0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ··tO6#·· %··s··E·
0010  00 5c 99 9f 40 00 ee 01  14 91 8a 60 92 02 c0 a8   ·\··@··· ···`····

icmp-ethereal-trace-2          Packets: 102 · Displayed: 102 (100.0%)          Profile: Default
```

There is request frame in the packet, and ICMP error packet did not have request frame. Moreover, the Code of the packet represents the packet is replay packet. The reason is that the packet sent by the source finally reached the destination.

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

Yes, there was a link whose delay was significantly longer than others.



```
   83 0.000181    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=52481/461, ttl=14 (no response found!)
   84 0.117035    193.51.179.238   192.168.1.101    ICMP    182 Time-to-live exceeded (Time to live exceeded in transit)
   85 0.887862    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=52737/462, ttl=15 (no response found!)
   86 0.114376    193.51.180.34    192.168.1.101    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   87 0.000131    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=52993/463, ttl=15 (no response found!)
   88 0.115153    193.51.180.34    192.168.1.101    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   89 0.000174    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=53249/464, ttl=15 (no response found!)
   90 0.114129    193.51.180.34    192.168.1.101    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   91 0.890478    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=53505/465, ttl=16 (no response found!)
   92 0.129514    193.51.181.137   192.168.1.101    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   93 0.000176    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=53761/466, ttl=16 (no response found!)
   94 0.114129    193.51.181.137   192.168.1.101    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   95 0.000184    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=54017/467, ttl=16 (no response found!)
   96 0.118743    193.51.181.137   192.168.1.101    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   97 0.887319    192.168.1.101    138.96.146.2     ICMP    106 Echo (ping) request  id=0x0200, seq=54273/468, ttl=17 (reply in 98)
```

(Frame 91~92 had the longest delay)

(Note: I set the time display as “since previous packet captured”. So, the time column represents the delay from previous packet.)

In Figure 4, the link, frame 9 to frame 10 had the significantly longer delay than others.

(72ms = 98ms – 26ms, 77ms = 98ms – 21ms, 71ms = 96ms – 25ms)

In frame 9, the router name includes ‘nyc’ so that the location of this router is New York City, and in frame 10, the router name includes ‘Pastourelle’ so that the location of this router is Paris, especially Pastourelle street.

(From: https://en.wikipedia.org/wiki/Rue_Pastourelle)