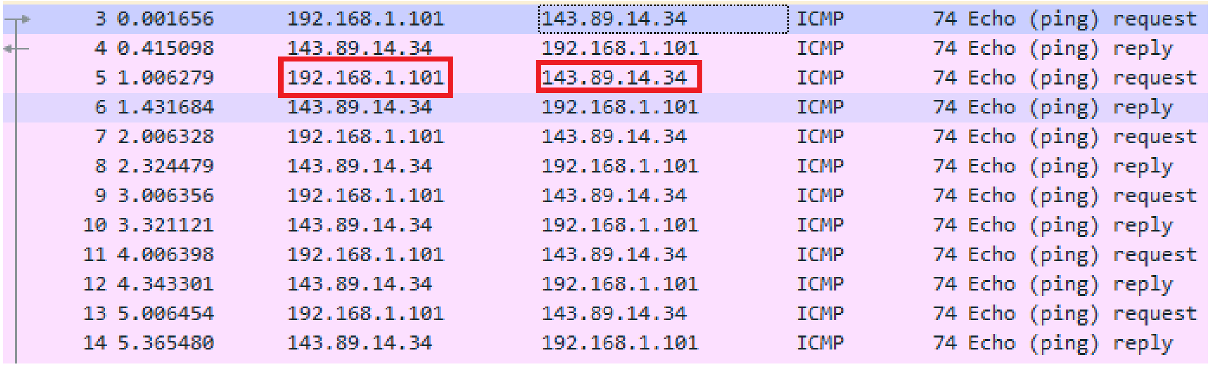
Lab_5_Wireshark_ICMP_v8.0

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

Answer:



```
 3 0.001656   192.168.1.101   143.89.14.34    ICMP   74 Echo (ping) request
 4 0.415098   143.89.14.34    192.168.1.101   ICMP   74 Echo (ping) reply
 5 1.006279   192.168.1.101   143.89.14.34    ICMP   74 Echo (ping) request
 6 1.431684   143.89.14.34    192.168.1.101   ICMP   74 Echo (ping) reply
 7 2.006328   192.168.1.101   143.89.14.34    ICMP   74 Echo (ping) request
 8 2.324479   143.89.14.34    192.168.1.101   ICMP   74 Echo (ping) reply
 9 3.006356   192.168.1.101   143.89.14.34    ICMP   74 Echo (ping) request
10 3.321121   143.89.14.34    192.168.1.101   ICMP   74 Echo (ping) reply
11 4.006398   192.168.1.101   143.89.14.34    ICMP   74 Echo (ping) request
12 4.343301   143.89.14.34    192.168.1.101   ICMP   74 Echo (ping) reply
13 5.006454   192.168.1.101   143.89.14.34    ICMP   74 Echo (ping) request
14 5.365480   143.89.14.34    192.168.1.101   ICMP   74 Echo (ping) reply
```

The IP address of my host is 192.168.1.101. The IP address of the destination host is 143.89.14.34.

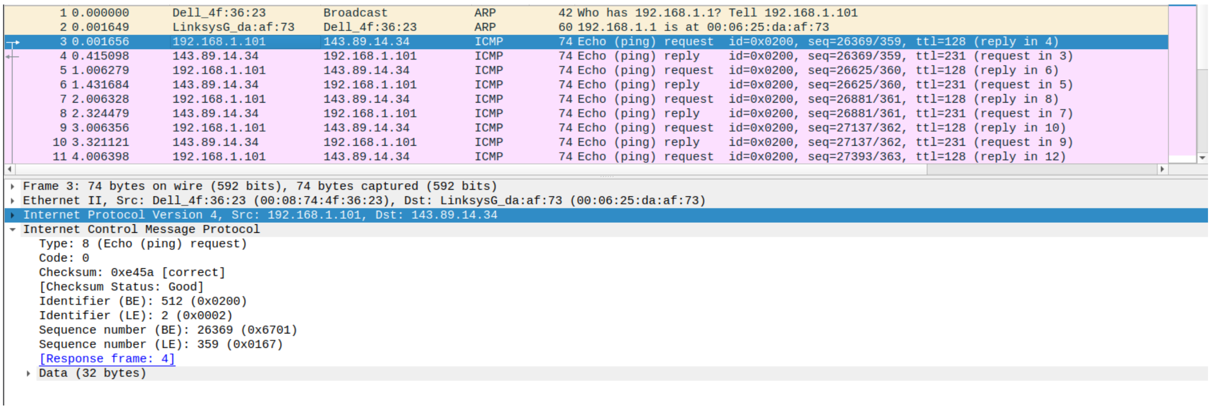
2. Why is it that an ICMP packet does not have source and destination port numbers?

Answer:

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

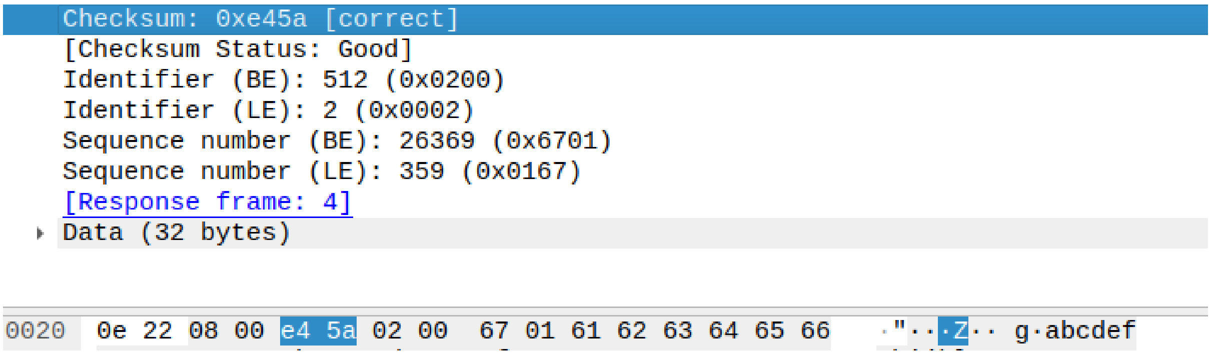
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Answer:

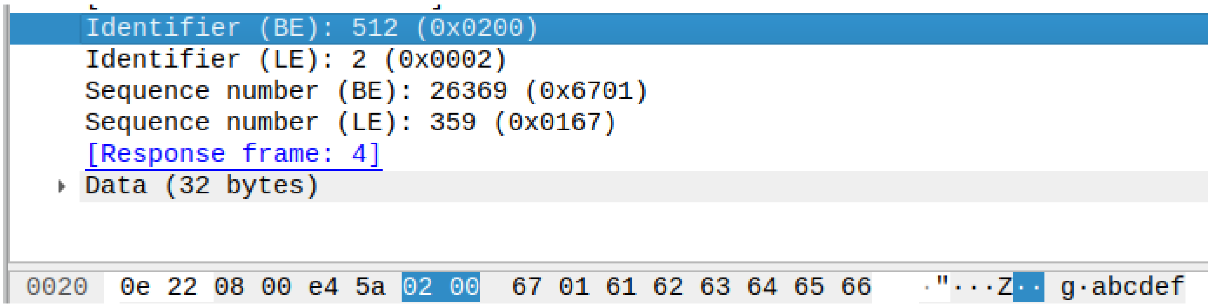


```
 1 0.000000   Dell_4f:36:23      Broadcast       ARP    42 Who has 192.168.1.1? Tell 192.168.1.101
 2 0.001649   LinksysG_da:af:73  Dell_4f:36:23   ARP    60 192.168.1.1 is at 00:06:25:da:af:73
 3 0.001656   192.168.1.101      143.89.14.34    ICMP   74 Echo (ping) request  id=0x0200, seq=26369/359, 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)
11 4.006398   192.168.1.101      143.89.14.34    ICMP   74 Echo (ping) request  id=0x0200, seq=27393/363, ttl=128 (reply in 12)
```

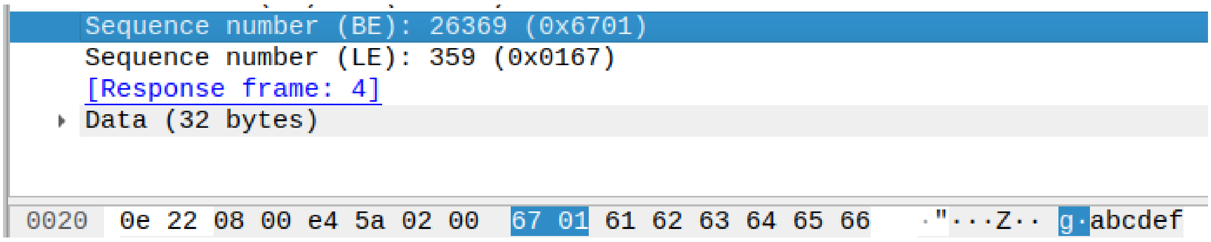
```
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  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]
  Data (32 bytes)
```



```
    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]
  ▸ Data (32 bytes)

0020  0e 22 08 00 e4 5a 02 00  67 01 61 62 63 64 65 66   ·"···Z·· g·abcdef
```



```
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence number (BE): 26369 (0x6701)
    Sequence number (LE): 359 (0x0167)
    [Response frame: 4]
  ▸ Data (32 bytes)

0020  0e 22 08 00 e4 5a 02 00  67 01 61 62 63 64 65 66   ·"···Z·· g·abcdef
```

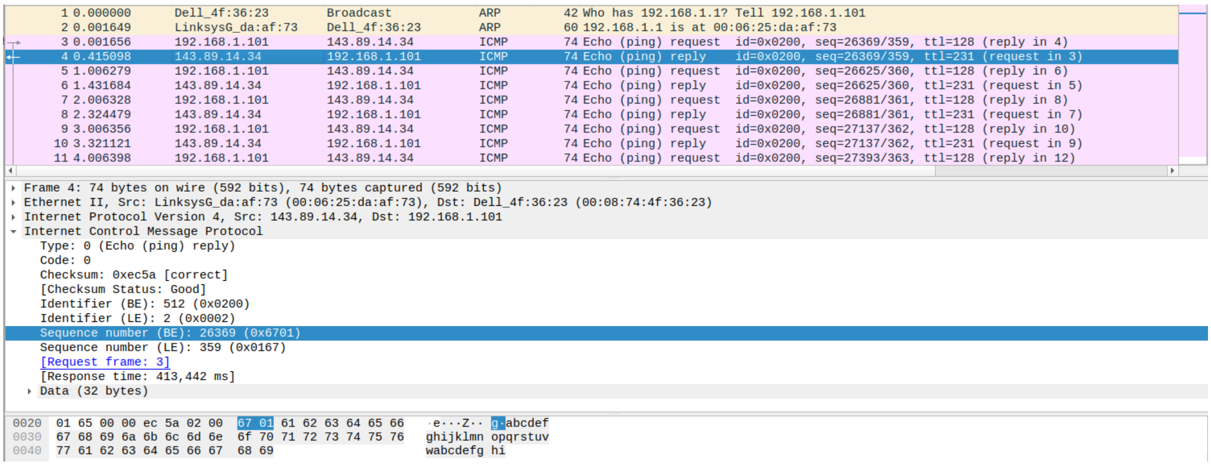


```
    Sequence number (BE): 26369 (0x6701)
    Sequence number (LE): 359 (0x0167)
    [Response frame: 4]
  ▸ Data (32 bytes)

0020  0e 22 08 00 e4 5a 02 00  67 01 61 62 63 64 65 66   ·"···Z·· g·abcdef
```

The ICMP type is 8, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

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?

Answer:

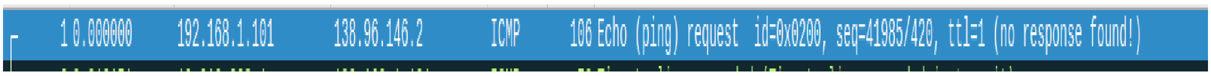


```
 1 0.000000   Dell_4f:36:23      Broadcast      ARP    42 Who has 192.168.1.1? Tell 192.168.1.101
 2 0.001649   LinksysG_da:af:73  Dell_4f:36:23  ARP    60 192.168.1.1 is at 00:06:25:da:af:73
 3 0.001656   192.168.1.101      143.89.14.34   ICMP   74 Echo (ping) request  id=0x0200, seq=26369/359, 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)
11 4.006398   192.168.1.101      143.89.14.34   ICMP   74 Echo (ping) request  id=0x0200, seq=27393/363, ttl=128 (reply in 12)

▸ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▸ Internet Protocol Version 4, Src: 143.89.14.34, Dst: 192.168.1.101
▾ 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]
  ▸ Data (32 bytes)

0020  01 65 00 00 ec 5a 02 00  67 01 61 62 63 64 65 66   ·e···Z·· g·abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

The ICMP type is 0, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

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

Answer:



```
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!)
```

The IP address of my host is 192.168.1.101. The IP address of the destination host is 138.96.146.2.

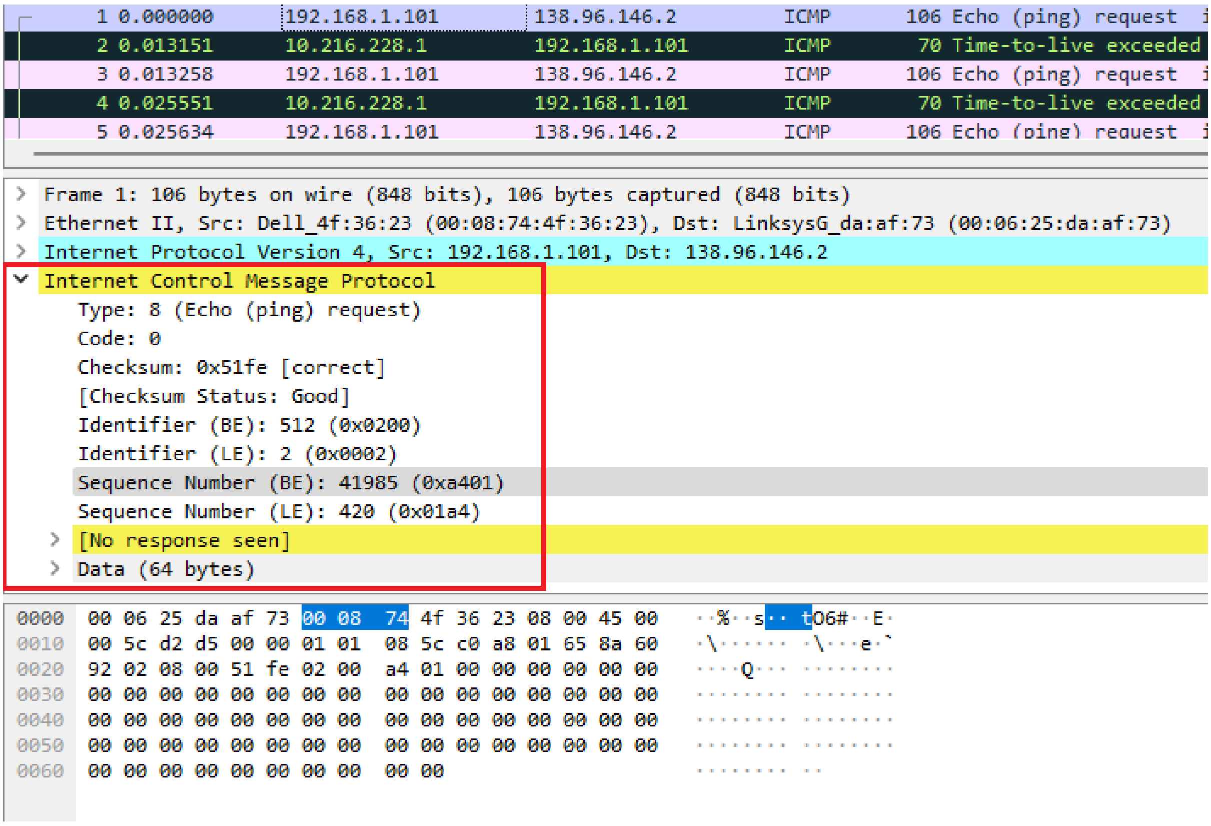
6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

Answer:

No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11

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?

Answer:

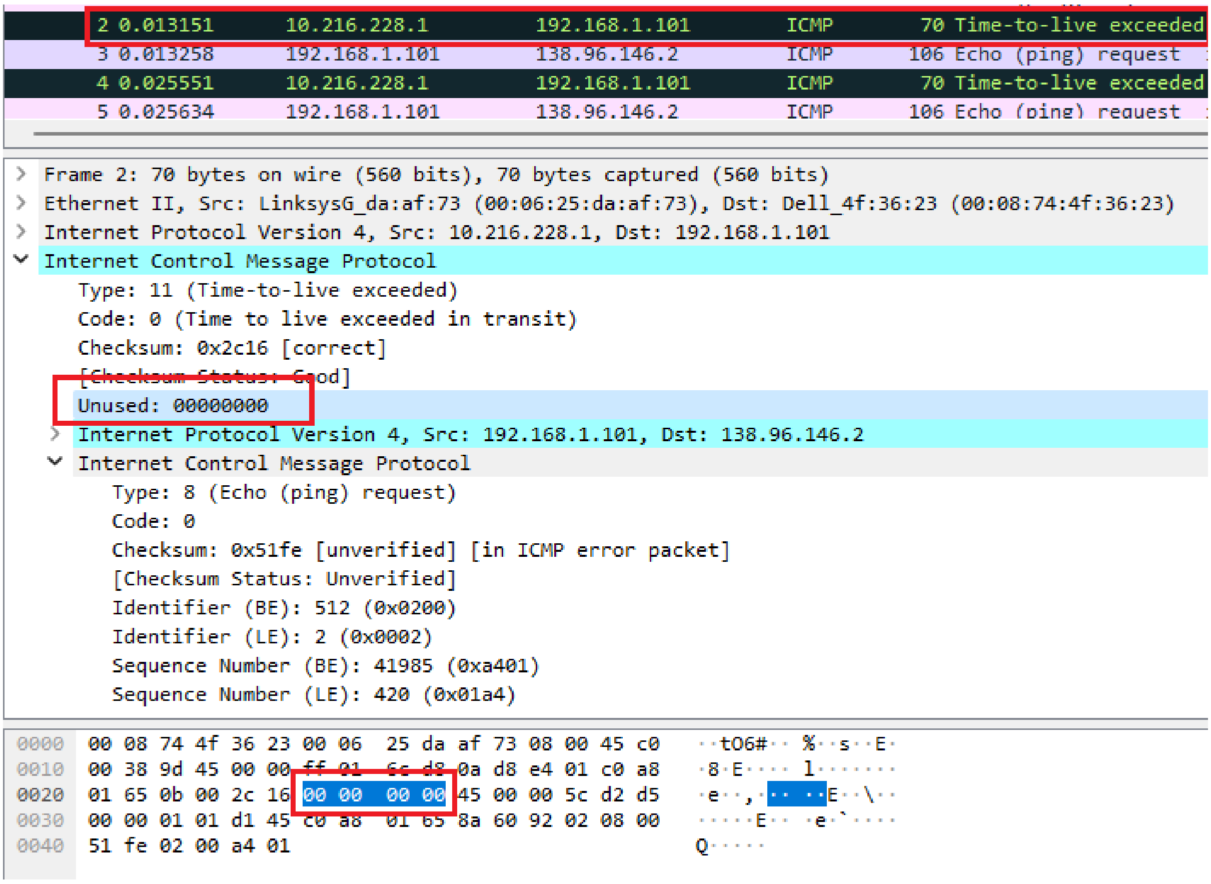


```
1 0.000000   192.168.1.101   138.96.146.2    ICMP   106 Echo (ping) request  i
2 0.013151   10.216.228.1    192.168.1.101   ICMP    70 Time-to-live exceeded
3 0.013258   192.168.1.101   138.96.146.2    ICMP   106 Echo (ping) request  i
4 0.025551   10.216.228.1    192.168.1.101   ICMP    70 Time-to-live exceeded
5 0.025634   192.168.1.101   138.96.146.2    ICMP   106 Echo (ping) request  i

> 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)
   > [No response seen]
   > Data (64 bytes)

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·`
0020  92 02 08 00 51 fe 02 00  a4 01 00 00 00 00 00 00   ····Q··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

The ICMP echo packet has the same fields as the ping query packets (includes: Type, Code number, Checksum, Identifier, Sequence number and Data fields)

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

Answer:



```
2 0.013151    10.216.228.1    192.168.1.101   ICMP    70 Time-to-live exceeded
3 0.013258    192.168.1.101   138.96.146.2    ICMP   106 Echo (ping) request
4 0.025551    10.216.228.1    192.168.1.101   ICMP    70 Time-to-live exceeded
5 0.025634    192.168.1.101   138.96.146.2    ICMP   106 Echo (ping) request

> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> 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
   > 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 [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)

0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 c0   ··tO6#·· %··s··E·
0010  00 38 9d 45 00 00 ff 01  6c d8 0a d8 e4 01 c0 a8   ·8·E···· l·······
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·`····
0040  51 fe 02 00 a4 01                                  Q·····
```

- The ICMP error packet is not the same as the ping query packets.
- It contains both the IP header and the first 8 bytes: Type -1 byte, Code – 1 byte, Checksum – 2 bytes, Unused – 4 bytes

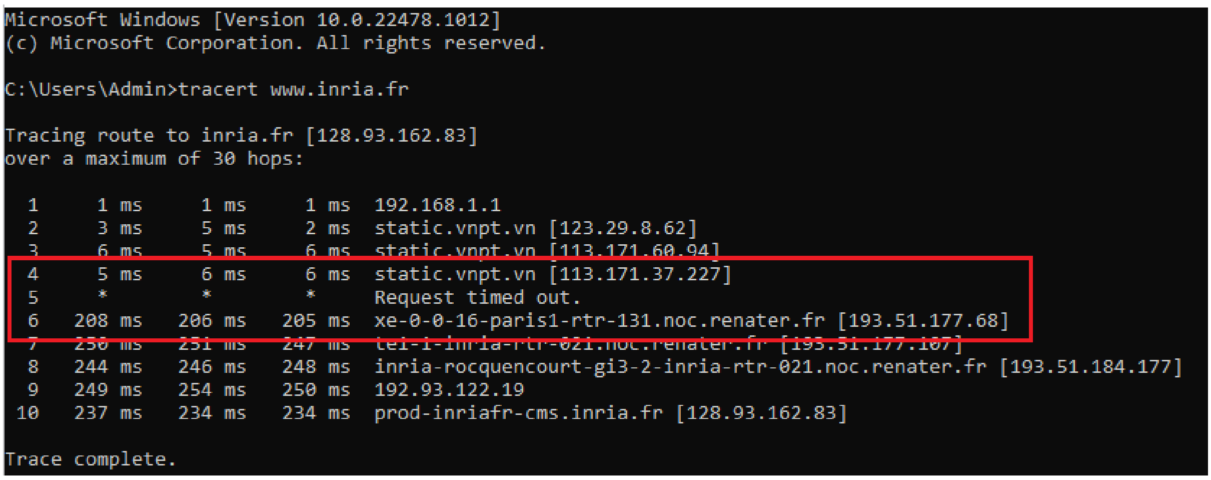
9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

Answer:

- The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired).
- They are different because the datagrams have made it all the way to the destination host before the TTL expired.

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?

Answer:



```
Microsoft Windows [Version 10.0.22478.1012]
(c) Microsoft Corporation. All rights reserved.

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

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

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     3 ms     5 ms     2 ms  static.vnpt.vn [123.29.8.62]
  3     6 ms     5 ms     6 ms  static.vnpt.vn [113.171.60.94]
  4     5 ms     6 ms     6 ms  static.vnpt.vn [113.171.37.227]
  5     *        *        *     Request timed out.
  6   208 ms   206 ms   205 ms  xe-0-0-16-paris1-rtr-131.noc.renater.fr [193.51.177.68]
  7   250 ms   251 ms   247 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
  8   244 ms   246 ms   248 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
  9   249 ms   254 ms   250 ms  192.93.122.19
 10   237 ms   234 ms   234 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.
```

- There is a link between steps 4 and 6 (step 5 is time out) that has a significantly longer delay.
- In figure 4 from the lab, the link is from New York to Pastourelle, France