Wireshark Lab -- ICMP

Jiaying Li
jl10919

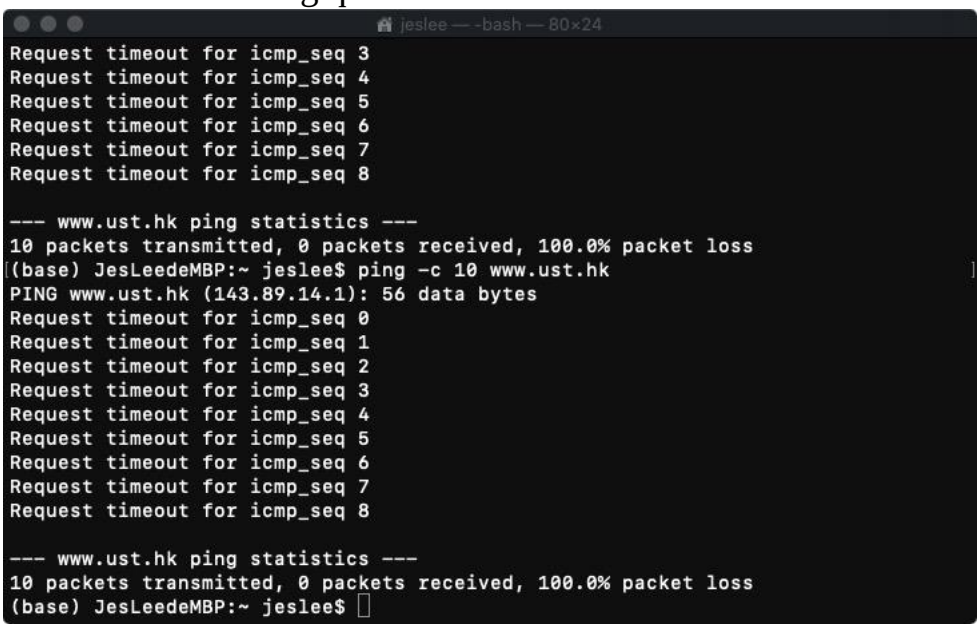
Lab environment:

Answer: My PC uses macOS Catalina 10.15.6, shows the following setting with *ifconfig*:

```
jeslee — -bash
(base) JesLeedeMBP:~ jeslee$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether ac:bc:32:7b:7f:83
        inet6 fe80::1c81:c11c:970e:3b33%en0 prefixlen 64 secured scopeid 0x4
        inet 192.168.1.155 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:13:09:8a:17:40
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:13:09:8a:17:41
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 82:13:09:8a:17:40
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 5 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 6 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        options=400<CHANNEL_IO>
        ether 0e:bc:32:7b:7f:83
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        options=400<CHANNEL_IO>
        ether e2:8b:ae:0c:af:c5
        inet6 fe80::e08b:aeff:fe0c:afc5%awdl0 prefixlen 64 scopeid 0x9
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether e2:8b:ae:0c:af:c5
        inet6 fe80::e08b:aeff:fe0c:afc5%llw0 prefixlen 64 scopeid 0xa
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::f58d:6031:ca37:b987%utun0 prefixlen 64 scopeid 0xb
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::af3a:6b7e:729f:e148%utun1 prefixlen 64 scopeid 0xc
        nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::8888:4408:7f6e:76ea%utun2 prefixlen 64 scopeid 0xd
        nd6 options=201<PERFORMNUD,DAD>
utun3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::2b53:b72c:6e42:c414%utun3 prefixlen 64 scopeid 0xe
        nd6 options=201<PERFORMNUD,DAD>
```

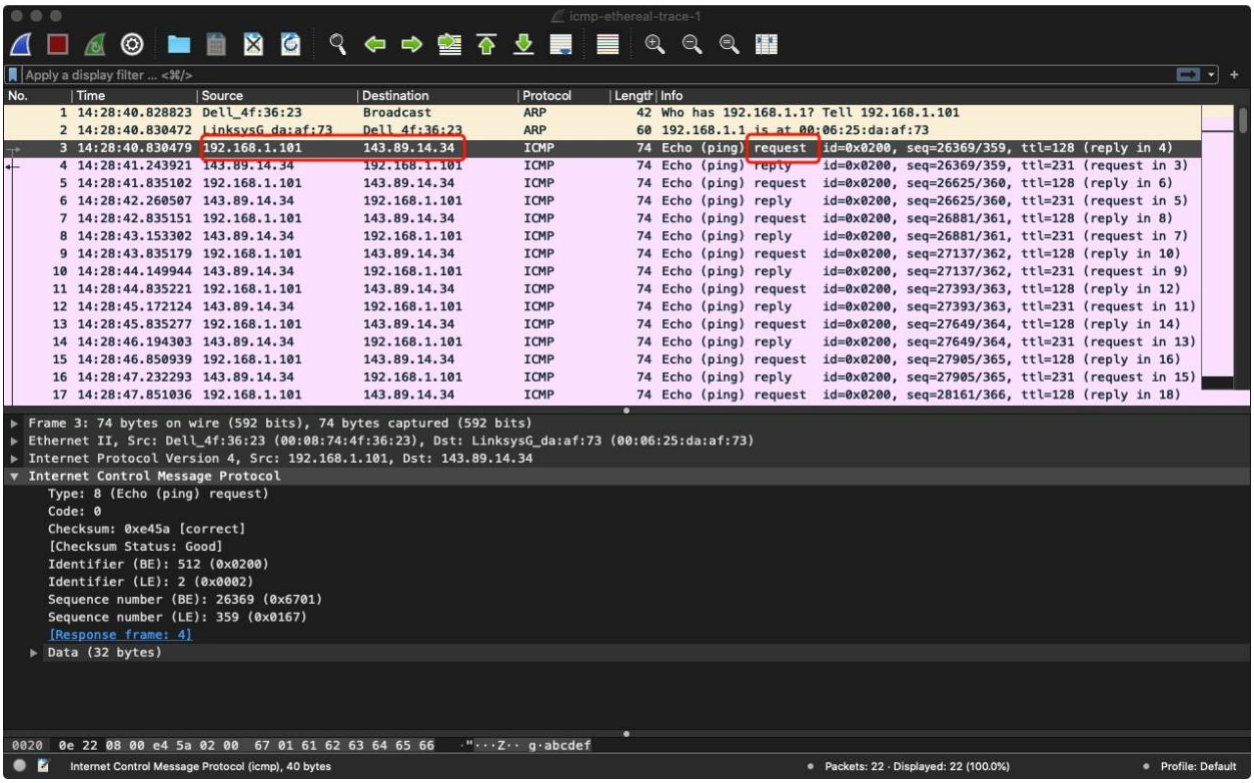
1. ICMP and Ping

As the screenshot shown below, my pc cannot successfully ping www.ust.hk. Thus, I will use file ICMP-ethereal-trace-1 provided by http://gaia.cs.ynass.edu to answer the following questions.



Q1. What is the IP address of your host? What is the IP address of the destination host?

Answer: As shown in the screenshot below, the IP address of my computer(source) is 192.168.1.101. The IP address of the destination hose is 143.89.14.34.



the first ICMP Request message sent:

No. Time Source Destination Protocol Length Info

3 14:28:40.830479 192.168.1.101 143.89.14.34 ICMP 74 Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)

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)

0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop

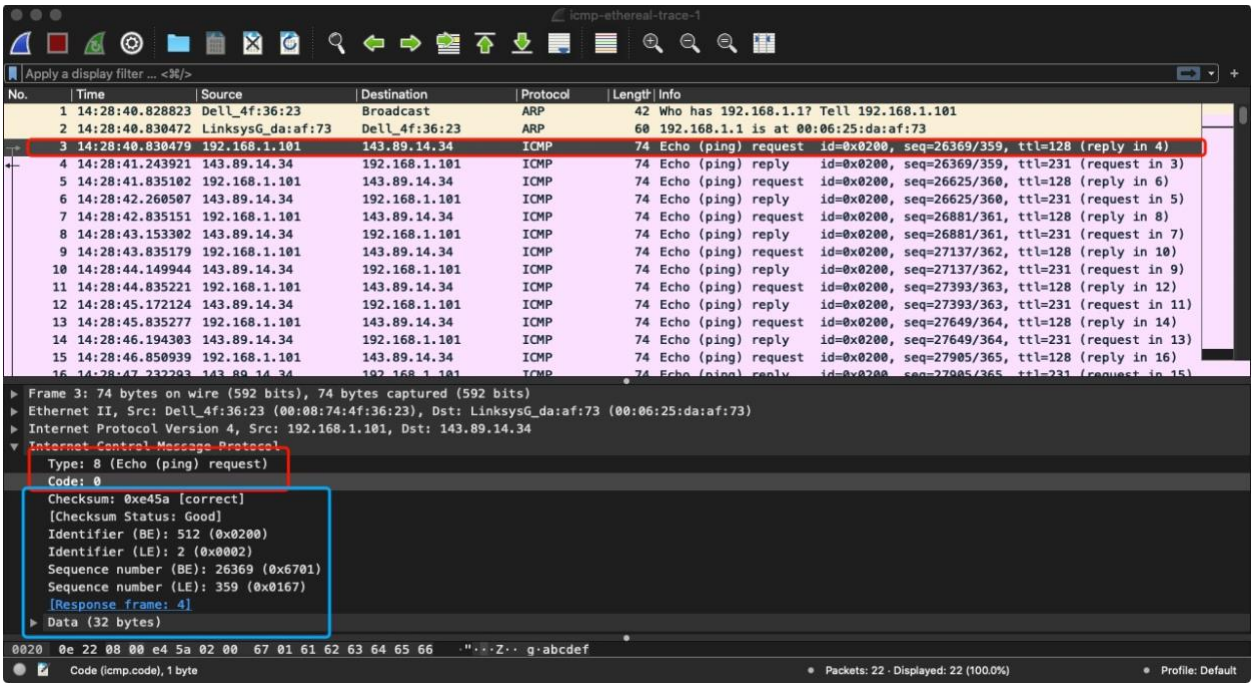
0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

Q2. Why is it that an ICMP packet does not have source and destination port numbers?

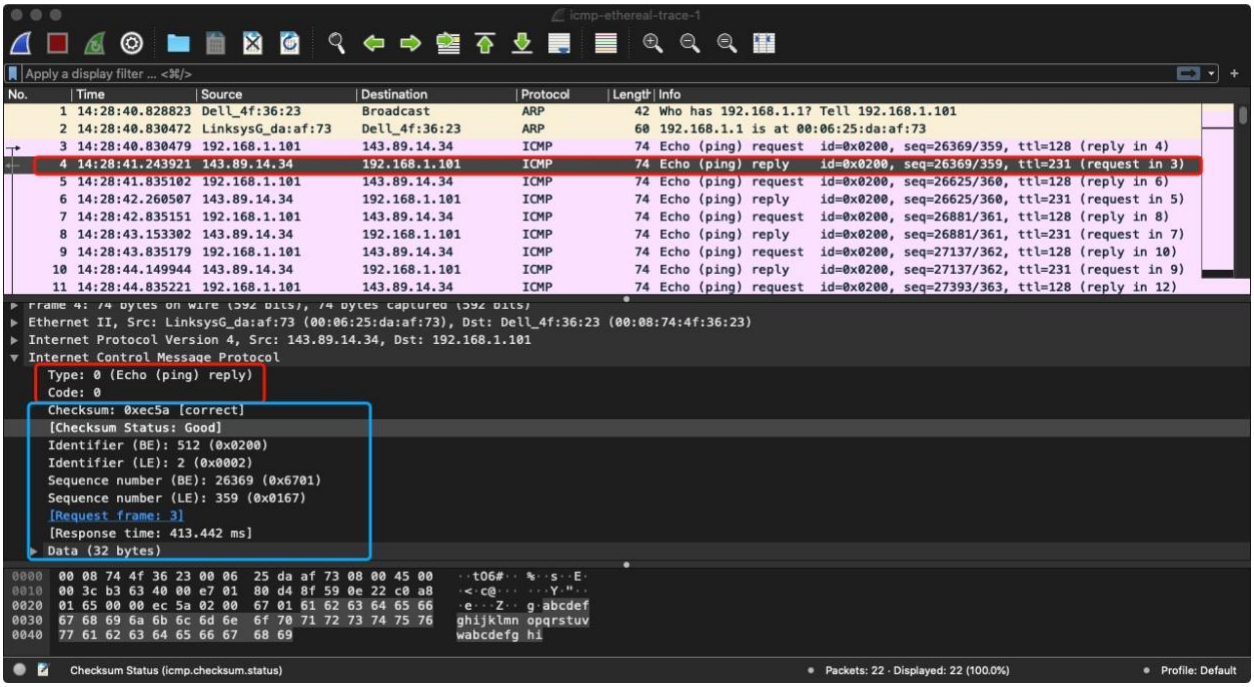
Answer: ICMP is a network-layer protocol, and ICMP is for network-layer information communication between hosts and routers. There is no TCP or UDP port number associated with ICMP packets as these numbers are associated with the transport layer above. The fields “Type” and “Code” can identify the specific message being received. What’s more, for network software, it can

interpret the ICMP messages, thus port number isn't necessary to direct ICMP info to the application layer process.

Q3. 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: As shown in the screenshot below and the print-out packet info, the ICMP type is 8 and code number is 0. There are other fields: checksum, identifier(identifier(BE), identifier(LE)), sequence number(sequence number(BE), sequence number(LE)) and data. The checksum, sequence number and identifier fields are all 2 bytes each.



Q4. 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: As shown in the screenshot below, the type is 0 and the code is 0. There are other fields: checksum, identifier(identifier(BE), identifier(LE)), sequence number(sequence number(BE), sequence number(LE)) and data. The checksum, sequence number and identifier fields are all 2 bytes each.



The reply packet of the first quest packet
No. Time Source Destination Protocol Length Info
4 14:28:41.243921 143.89.14.34 192.168.1.101 ICMP 74 Echo (ping)
reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
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)
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

2. ICMP and Traceroute

As the screenshot shown below, here is the result of the traceroute command. Since my pc is in MacOS system, I will use file ICMP-ethereal-trace-2 provided by http://gaia.cs.ynass.edu to answer the following questions.

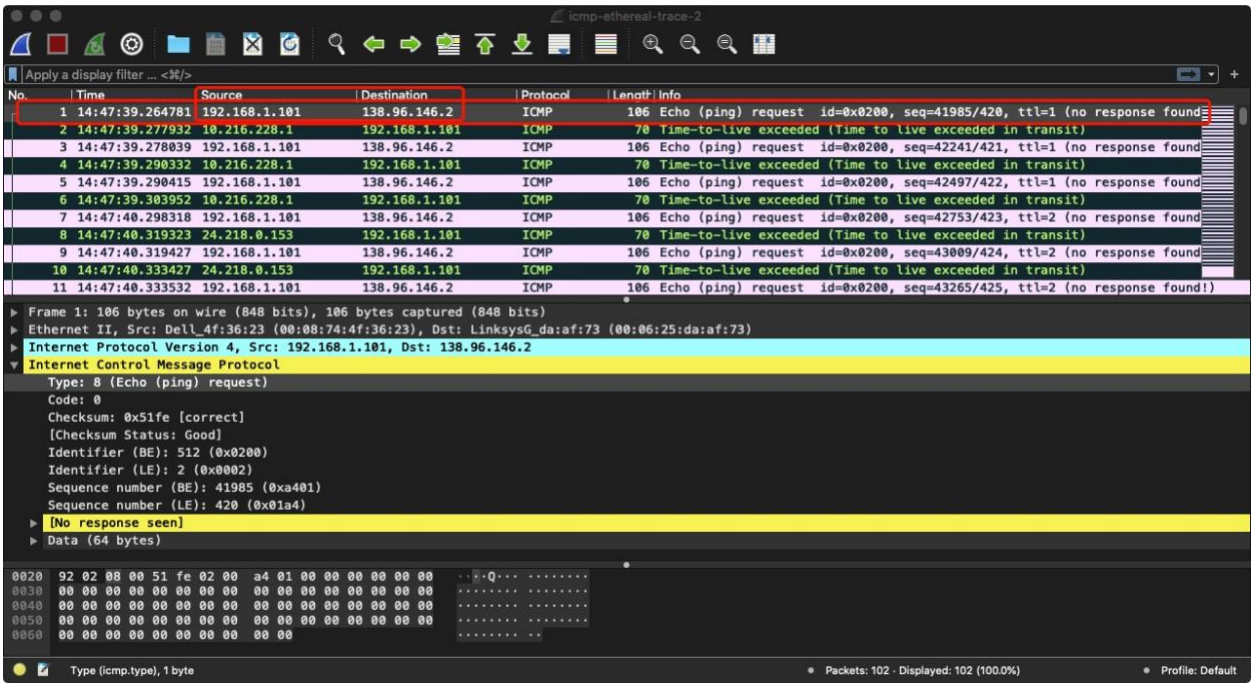
jeslee — -bash — 110×53

```
(base) JesLeedeMBP:~ jeslee$ traceroute www.inria.fr
traceroute to inria-cms.inria.fr (128.93.162.63), 64 hops max, 52 byte packets
 1  g3100 (192.168.1.1)  1.963 ms  1.216 ms  1.023 ms
 2  * * *
 3  b3313.nwrknj-lcr-22.verizon-gni.net (130.81.216.230)  10.430 ms
    b3313.nwrknj-lcr-21.verizon-gni.net (130.81.216.228)  12.892 ms  9.005 ms
 4  * * *
 5  0.ae1.br1.ewr6.alter.net (140.222.237.223)  6.589 ms  12.838 ms
    0.ae2.br1.ewr6.alter.net (140.222.237.225)  9.648 ms
 6  &#10.0.193.152.in-addr.arpa (152.193.0.114)  6.548 ms  6.281 ms  12.002 ms
 7  et-3-3-0.cr4-par7.ip4.gtt.net (213.200.119.214)  80.270 ms  81.803 ms  83.465 ms
 8  renater-gw-ix1.gtt.net (77.67.123.206)  90.283 ms  94.695 ms  87.342 ms
 9  * * *
10  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr (193.51.184.177)  87.203 ms  86.045 ms  88.767 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
31  * * *
32  * * *
33  * * *
34  * * *
35  * * *
36  * * *
37  * * *
38  * * *
39  * * *
40  * * *
41  * * *
42  * * *
43  * * *
44  * * *
45  * * *
46  * * *
47  * * *
48  * * *
49  * * *
```

jeslee — -bash — 110×18

```
48  * * *
49  * * *
50  * * *
51  * * *
52  * * *
53  * * *
54  * * *
55  * * *
56  * * *
57  * * *
58  * * *
59  * * *
60  * * *
61  * * *
62  * * *
63  * * *
64  * * *
(base) JesLeedeMBP:~ jeslee$ traceroute www.inria.fr
```

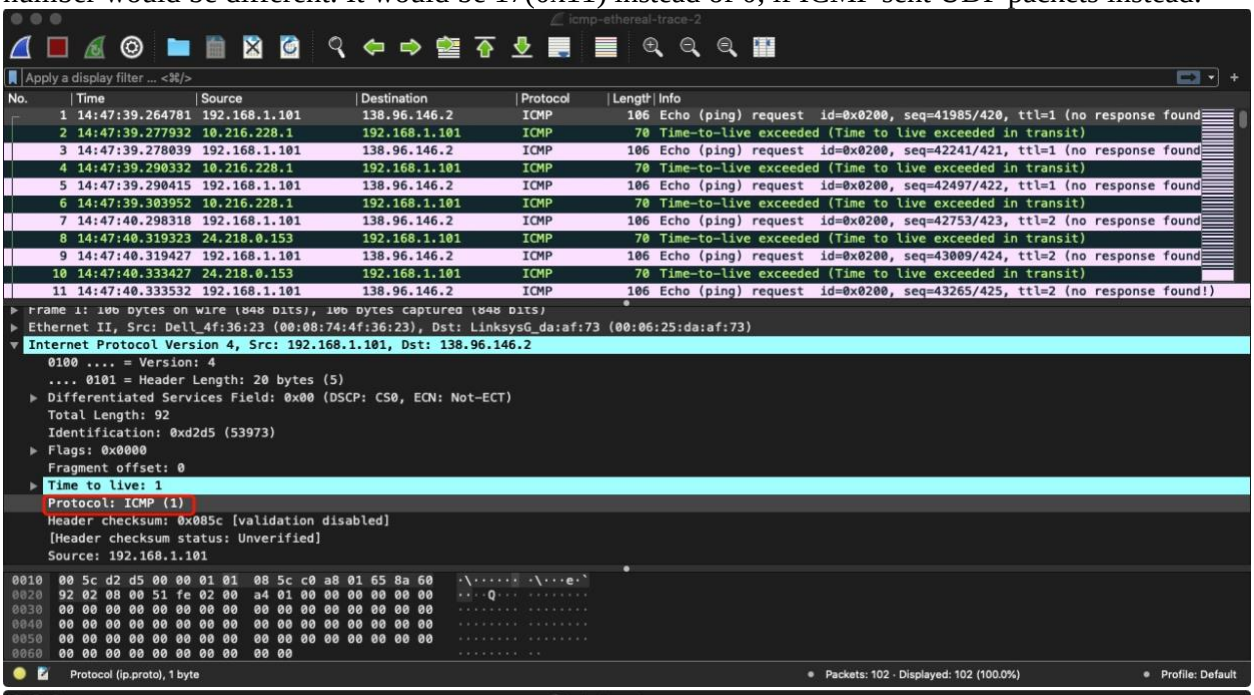
Q5. What is the IP address of your host? What is the IP address of the target destination host?
Answer: As the screenshot shown below, the IP address of my host is 192.168.1.101, and the IP address of target destination host is 138.96.146.2

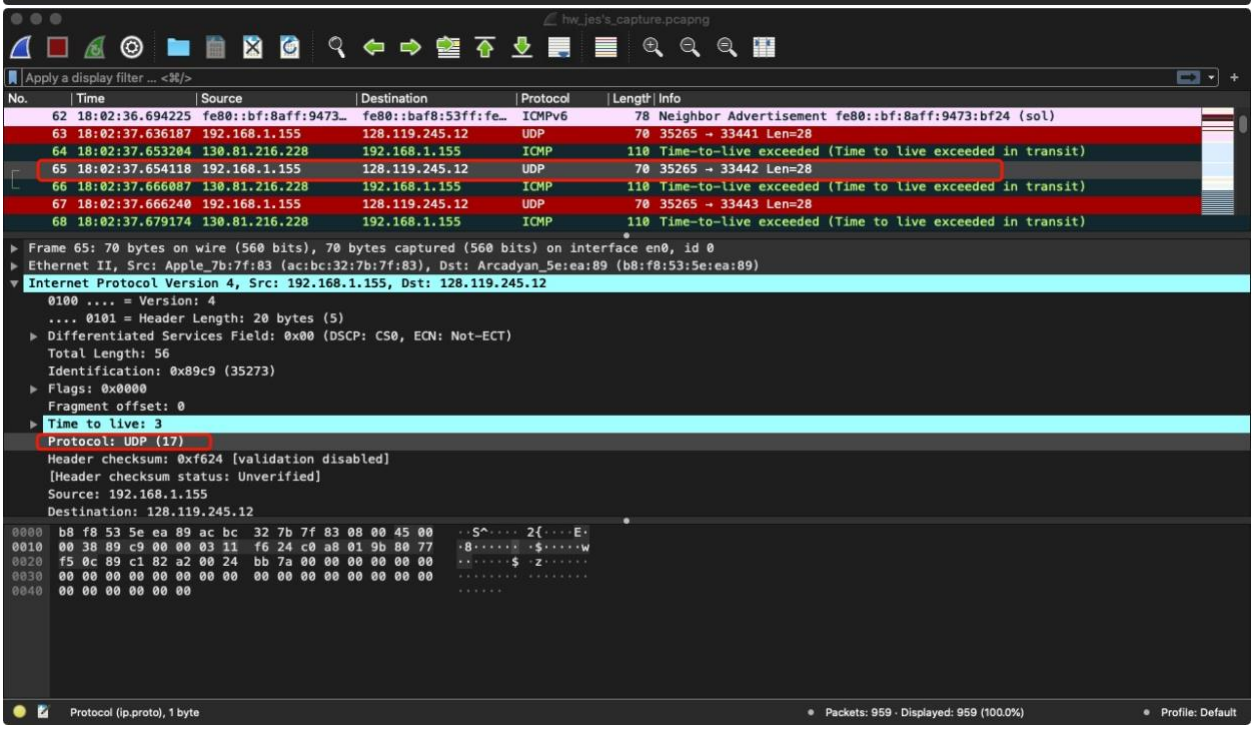


The first ICMP echo packet info:
No. Time Source Destination Protocol Length Info
1 14:47:39.264781 192.168.1.101 138.96.146.2 ICMP 106 Echo (ping)
request id=0x0200, seq=41985/420, ttl=1 (no response found!)
Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_4f:36:23 (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
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 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 .....

Q6. 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: As the screenshots shown below, the first one is the ICMP packet sent by the source (my PC), and the second one is the UDP packets sent by my PC while doing traceroute. The IP protocol number would be different. It would be 17(0x11) instead of 0, if ICMP sent UDP packets instead.





Q7. 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: There is no big difference between the echo packet and the ICMP ping packet. They have the same fields. Except the sequence number value and the checksum value.

As we can see from the packet info shown above, in the ICMP ping request packet:

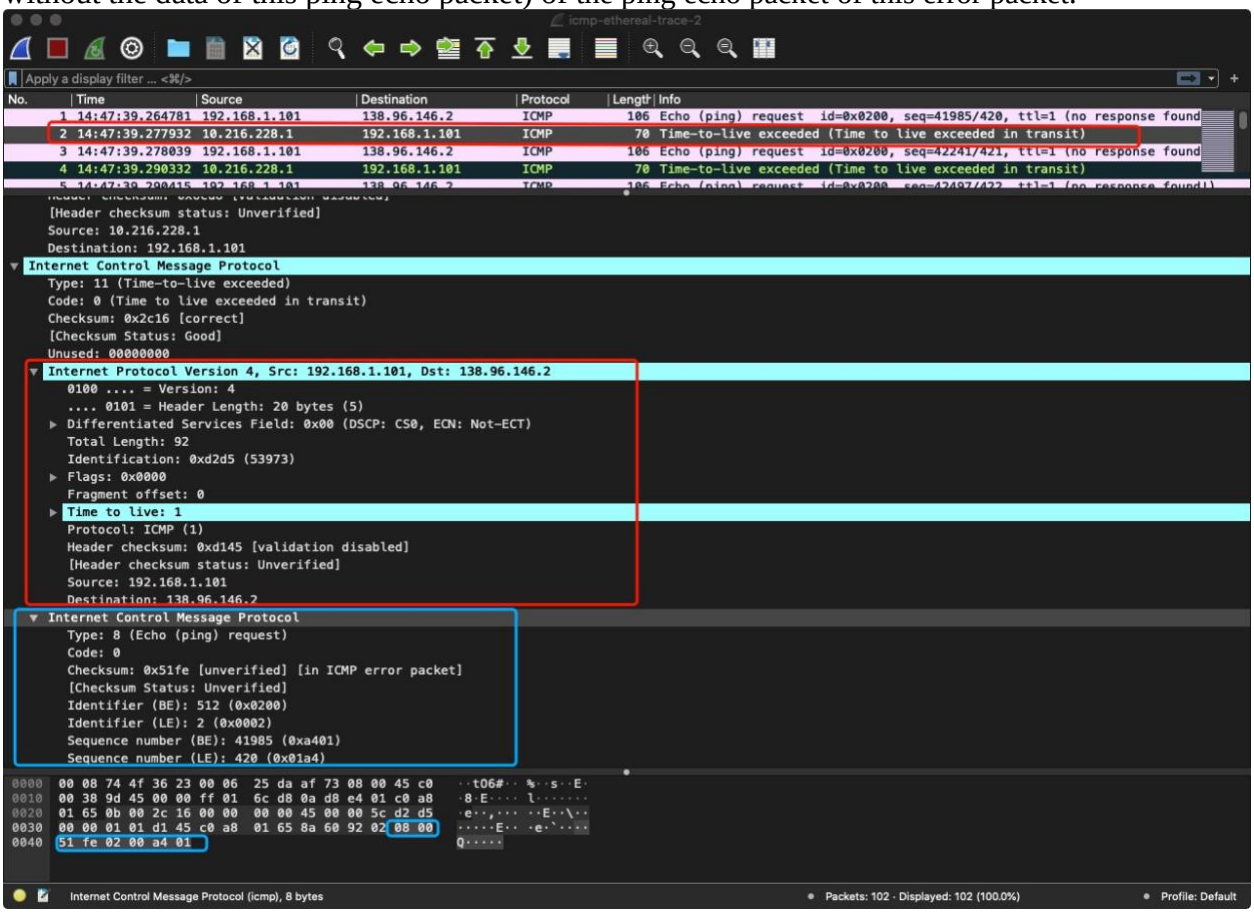
Checksum: 0xe45a [correct]
Sequence number (BE): 26369 (0x6701)
Sequence number (LE): 359 (0x0167)

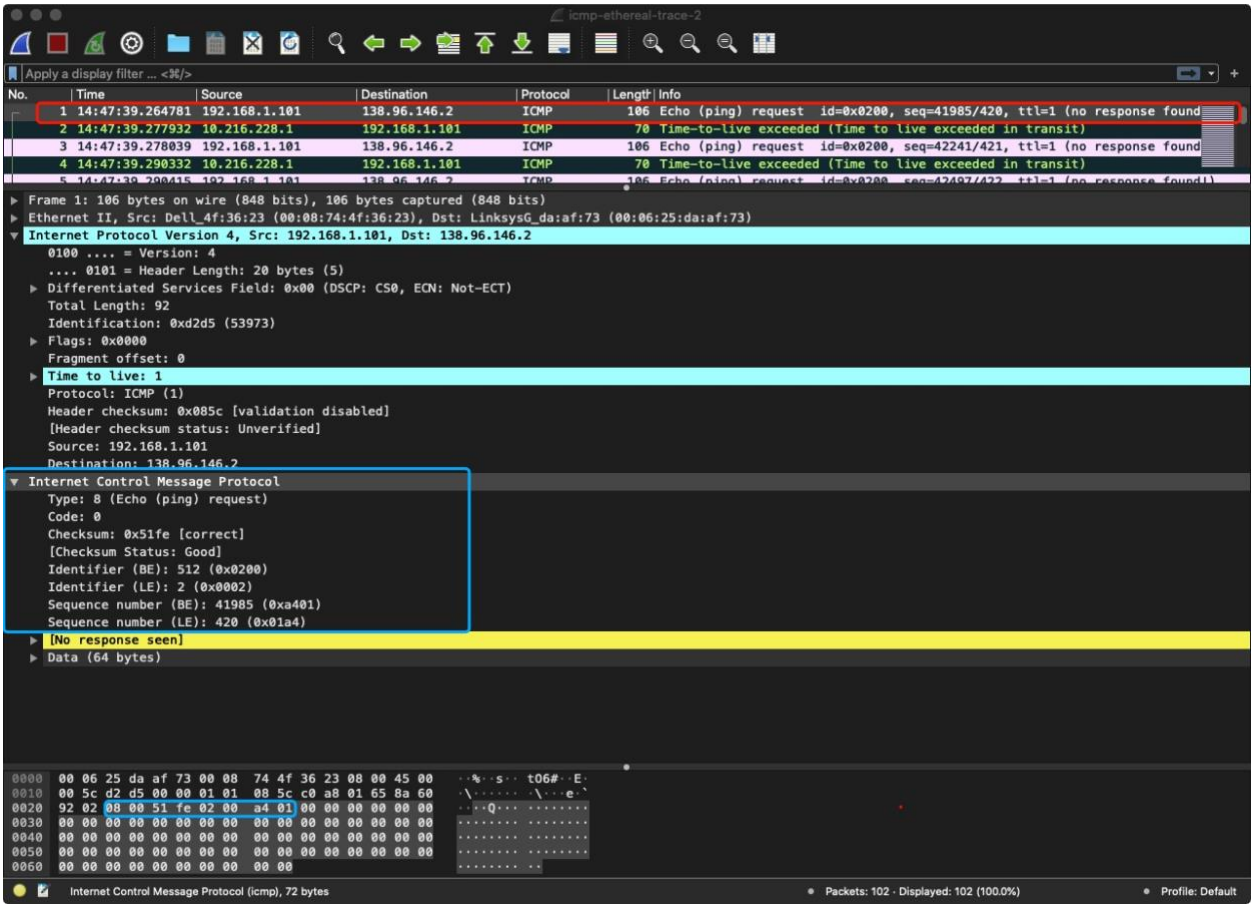
In the first ICMP echo packet:

Checksum: 0x51fe [correct]
Sequence number (BE): 41985 (0xa401)
Sequence number (LE): 420 (0x01a4)

Q8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

Answer: As shown in the screenshots below, the first one is the error packet and the second one is the ping echo packet of this error packet. The ICMP error packet is very different from the ping query packets. Under "ICMP", It contains the IP header (20 bytes) and the ICMP header (first 8 bytes, without the data of this ping echo packet) of the ping echo packet of this error packet.



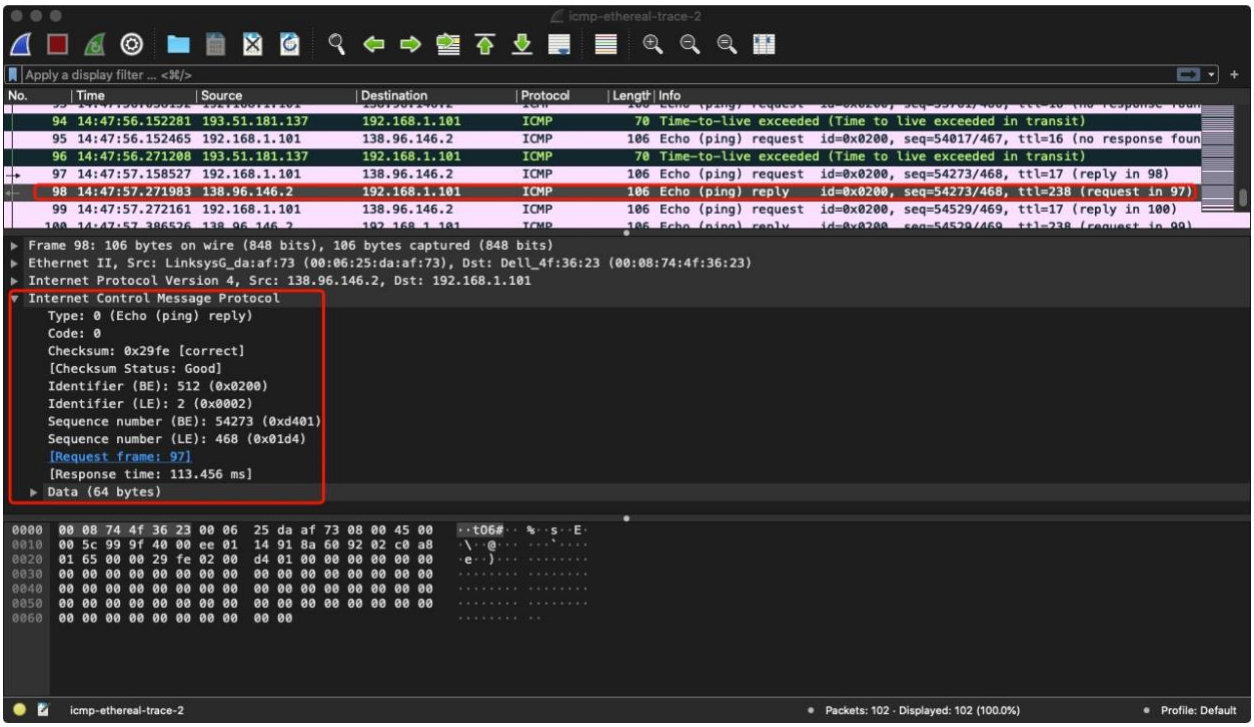


The first ICMP error packet info:

No. Time Source Destination Protocol Length Info
2 14:47:39.277932 10.216.228.1 192.168.1.101 ICMP 70 Time-tolive
exceeded (Time to live exceeded in transit)
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
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
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0xd2d5 (53973)
Flags: 0x0000
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0xd145 [validation disabled]

[Header checksum status: Unverified]
Source: 192.168.1.101
Destination: 138.96.146.2
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)

Q9. 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: As shown in the screenshot below, the last three ICMP packets received by the source host are different from the ICMP error packets. The "type" of the last three ICMP packets is "0 (Echo (ping) reply) while the "type" of the error packets is "11 (Time-to-live exceeded)". And the last three ICMP packets don't have the IP header (20 bytes) and the ICMP header (first 8 bytes, without the data of this ping echo packet) of their ping echo packets. The reason why they are different is that the datagrams of these last three ICMP packets have successfully reach to the destination host before their TTL expired.



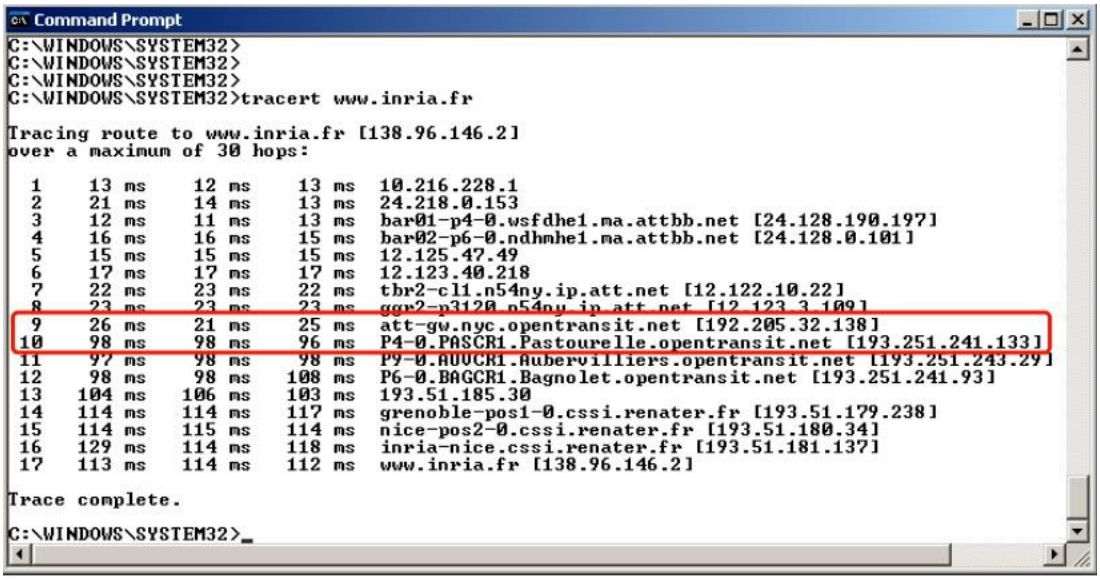
The third ICMP packet received by the source host from the end:

No. Time Source Destination Protocol Length Info
98 14:47:57.271983 138.96.146.2 192.168.1.101 ICMP 106 Echo (ping)
reply id=0x0200, seq=54273/468, ttl=238 (request in 97)
Frame 98: 106 bytes on wire (848 bits), 106 bytes captured (848 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: 138.96.146.2, Dst: 192.168.1.101
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]
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 .....

Q10. 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: As shown in the screenshots below. The first one is the Figure 4 in assignment description, and the second one is the tracert result on my pc. Both of them has a link whose delay is significantly longer than others. In the first screenshot, the location of two routers on the end of this link should be New York City in US and Pastourelle in France, and this link is between step 9 and 10. In the second screenshot, the most delay link should be the link between step 6 and 7. Since all the router names are encoded by Verizon, I cannot guess the location of them based on the router names.



```
Command Prompt
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr

Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:

  1    13 ms    12 ms    13 ms  10.216.228.1
  2    21 ms    14 ms    13 ms  24.218.0.153
  3    12 ms    11 ms    13 ms  bar01-p4-0.wsfdhe1.ma.attbb.net [24.128.190.197]
  4    16 ms    16 ms    15 ms  bar02-p6-0.ndhmhe1.ma.attbb.net [24.128.0.101]
  5    15 ms    15 ms    15 ms  12.125.47.49
  6    17 ms    17 ms    17 ms  12.123.40.218
  7    22 ms    23 ms    22 ms  tbr2-cl1.n54ny.ip.att.net [12.122.10.22]
  8    23 ms    23 ms    23 ms  ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
  9    26 ms    21 ms    25 ms  att-gw.nyc.opentransit.net [192.205.32.138]
 10    98 ms    98 ms    96 ms  P4-0.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
 11    97 ms    98 ms    98 ms  P9-0.AUVCR1.Aubervilliers.opentransit.net [193.251.243.29]
 12    98 ms    98 ms   108 ms  P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
 13   104 ms   106 ms   103 ms  193.51.185.30
 14   114 ms   114 ms   117 ms  grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
 15   114 ms   115 ms   114 ms  nice-pos2-0.cssi.renater.fr [193.51.180.34]
 16   129 ms   114 ms   118 ms  inria-nice.cssi.renater.fr [193.51.181.137]
 17   113 ms   114 ms   112 ms  www.inria.fr [138.96.146.2]

Trace complete.

C:\WINDOWS\SYSTEM32>_
```

```
jeslee — -bash — 110×18
(base) JesLeedeMBP:~ jeslee$ traceroute www.inria.fr
traceroute to inria-cms.inria.fr (128.93.162.63), 64 hops max, 52 byte packets
 1  g3100 (192.168.1.1)  1.963 ms  1.216 ms  1.023 ms
 2  * * *
 3  b3313.nwrknj-lcr-22.verizon-gni.net (130.81.216.230)  10.430 ms
    b3313.nwrknj-lcr-21.verizon-gni.net (130.81.216.228)  12.892 ms  9.005 ms
 4  * * *
 5  0.ae1.br1.ewr6.alter.net (140.222.237.223)  6.589 ms  12.838 ms
    0.ae2.br1.ewr6.alter.net (140.222.237.225)  9.648 ms
 6  &#10.0.193.152.in-addr.arpa (152.193.0.114)  6.548 ms  6.281 ms  12.002 ms
 7  et-3-3-0.cr4-par7.ip4.gtt.net (213.200.119.214)  80.270 ms  81.803 ms  83.465 ms
 8  renater-gw-ix1.gtt.net (77.67.123.206)  90.283 ms  94.695 ms  87.342 ms
 9  * * *
10  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr (193.51.184.177)  87.203 ms  86.045 ms  88.767 ms
11  * * *
12  * * *
13  * * *
14  * * *
```