Wireshark Lab: ICMP

Yogesh P
201EE138

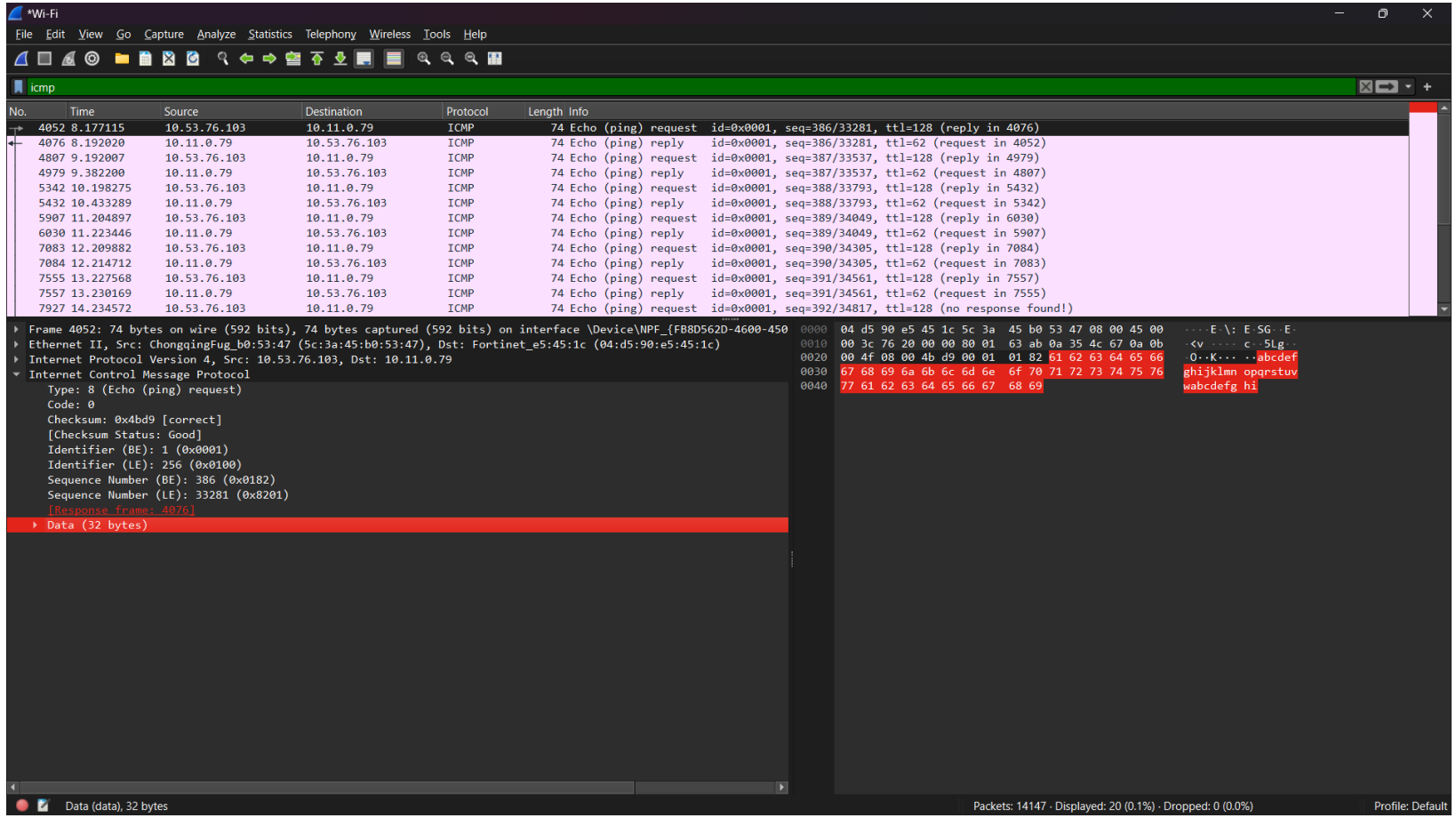
1. ICMP and Ping

```
C:\Users\Yogesh>ping -n 10 nitk.ac.in

Pinging nitk.ac.in [10.11.0.79] with 32 bytes of data:
Reply from 10.11.0.79: bytes=32 time=15ms TTL=62
Reply from 10.11.0.79: bytes=32 time=190ms TTL=62
Reply from 10.11.0.79: bytes=32 time=235ms TTL=62
Reply from 10.11.0.79: bytes=32 time=18ms TTL=62
Reply from 10.11.0.79: bytes=32 time=4ms TTL=62
Reply from 10.11.0.79: bytes=32 time=2ms TTL=62
Request timed out.
Reply from 10.11.0.79: bytes=32 time=2ms TTL=62
Reply from 10.11.0.79: bytes=32 time=1ms TTL=62
Reply from 10.11.0.79: bytes=32 time=1ms TTL=62

Ping statistics for 10.11.0.79:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 235ms, Average = 52ms

C:\Users\Yogesh>
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
4052 8.177115 10.53.76.103 10.11.0.79 ICMP 74 Echo (ping) request id=0x0001, seq=386/33281, ttl=128 (reply in 4076)
4076 8.192020 10.11.0.79 10.53.76.103 ICMP 74 Echo (ping) reply id=0x0001, seq=386/33281, ttl=62 (request in 4052)
4807 9.192007 10.53.76.103 10.11.0.79 ICMP 74 Echo (ping) request id=0x0001, seq=387/33537, ttl=128 (reply in 4979)
4979 9.382200 10.11.0.79 10.53.76.103 ICMP 74 Echo (ping) reply id=0x0001, seq=387/33537, ttl=62 (request in 4807)
5342 10.198275 10.53.76.103 10.11.0.79 ICMP 74 Echo (ping) request id=0x0001, seq=388/33793, ttl=128 (reply in 5432)
5432 10.433289 10.11.0.79 10.53.76.103 ICMP 74 Echo (ping) reply id=0x0001, seq=388/33793, ttl=62 (request in 5342)
5907 11.204897 10.53.76.103 10.11.0.79 ICMP 74 Echo (ping) request id=0x0001, seq=389/34049, ttl=128 (reply in 6030)
6030 11.223446 10.11.0.79 10.53.76.103 ICMP 74 Echo (ping) reply id=0x0001, seq=389/34049, ttl=62 (request in 5907)
7083 12.209882 10.53.76.103 10.11.0.79 ICMP 74 Echo (ping) request id=0x0001, seq=390/34305, ttl=128 (reply in 7084)
7084 12.214712 10.11.0.79 10.53.76.103 ICMP 74 Echo (ping) reply id=0x0001, seq=390/34305, ttl=62 (request in 7083)
7555 13.227568 10.53.76.103 10.11.0.79 ICMP 74 Echo (ping) request id=0x0001, seq=391/34561, ttl=128 (reply in 7557)
7557 13.230169 10.11.0.79 10.53.76.103 ICMP 74 Echo (ping) reply id=0x0001, seq=391/34561, ttl=62 (request in 7555)
7927 14.234572 10.53.76.103 10.11.0.79 ICMP 74 Echo (ping) request id=0x0001, seq=392/34817, ttl=128 (no response found!)
Frame 4052: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{FB8D562D-4600-450
Ethernet II, Src: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet_e5:45:1c (04:d5:90:e5:45:1c)
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 10.11.0.79
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4bd9 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 386 (0x0182)
Sequence Number (LE): 33281 (0x8201)
[Response frame: 4076]
Data (32 bytes)
0000 04 d5 90 e5 45 1c 5c 3a 45 b0 53 47 08 00 45 00
0010 00 3c 76 20 00 00 80 01 63 ab 0a 35 4c 67 0a 0b
0020 00 4f 08 00 4b d9 00 01 01 82 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
Data (data), 32 bytes
Packets: 14147 · Displayed: 20 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

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

A: 10.53.76.103, 10.11.0.79

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

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?

A: Type: 8 (Echo (ping) request), Code: 0, Other fields – checksum, identifier(BE) , identifier(LE), sequence number(BE), sequence number(LE), they are all two bytes

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?

A:Type: 0 (Echo (ping) reply), Code: 0, Other fields – checksum, identifier(BE) , identifier(LE), sequence number(BE), sequence number(LE), they are all two bytes

2. ICMP and Traceroute

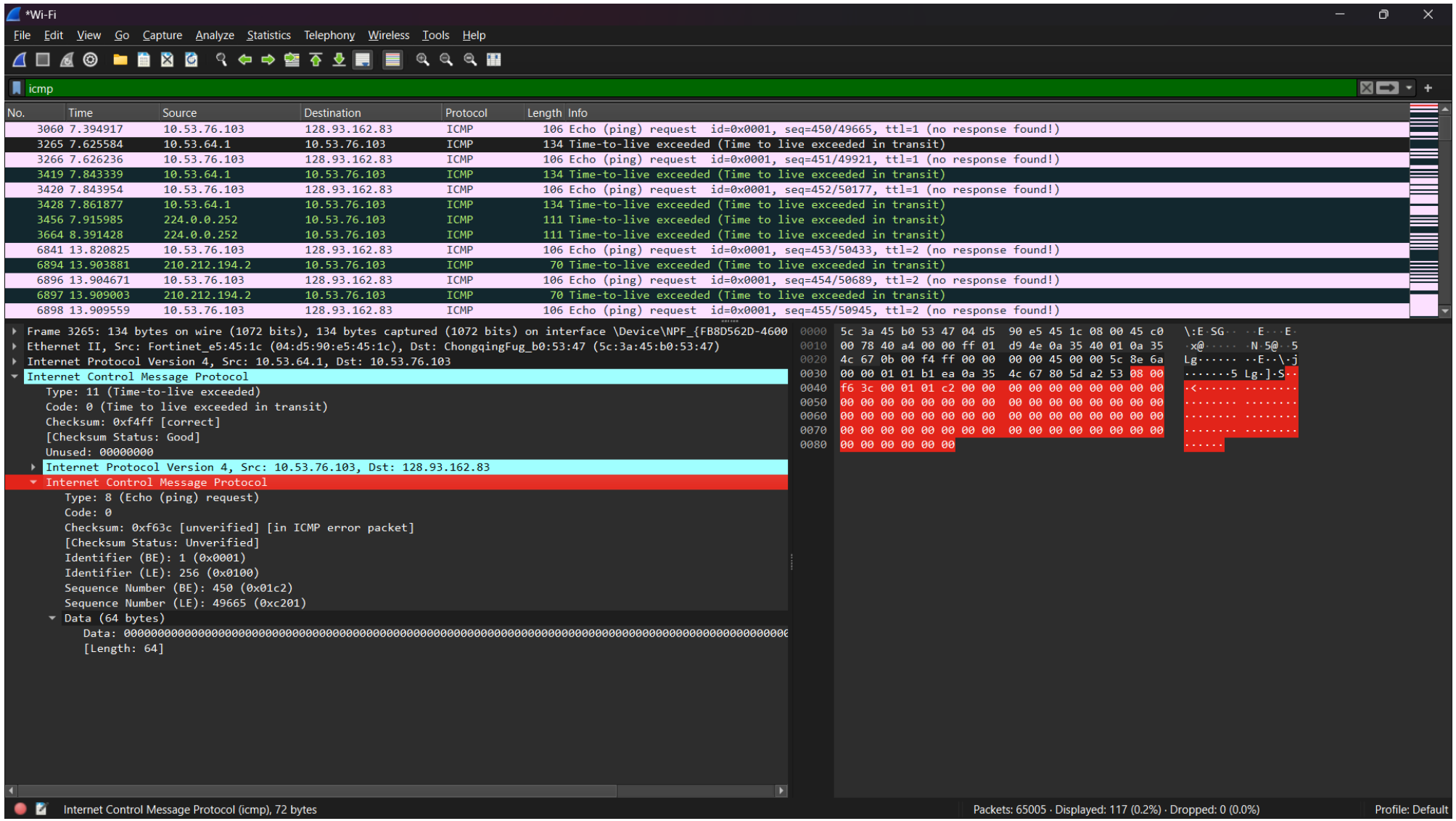
Tracing route cmd

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

  1   230 ms   217 ms    17 ms  10.53.64.1
  2    83 ms     4 ms   123 ms  210.212.194.2
  3     *      308 ms     *     117.216.207.216
  4    31 ms    21 ms    96 ms  117.216.207.217
  5    38 ms    69 ms   133 ms  115.110.161.21.static.vsnl.net.in [115.110.161.21]
  6     *        *        *     Request timed out.
  7     *      146 ms    90 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  8     *        *        *     Request timed out.
  9     *      317 ms     *     if-ae-12-2.tcore1.l78-london.as6453.net [180.87.39.21]
 10     *        *        *     Request timed out.
 11  1482 ms   391 ms   290 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 12  1057 ms   604 ms   408 ms  hu0-4-0-0-ren-nr-orsay-rtr-091.noc.renater.fr [193.51.180.131]
 13   394 ms   203 ms   230 ms  193.55.204.205
 14   171 ms   176 ms   484 ms  neoma-a42-ipv4-odeon-rtr-111.noc.renater.fr [193.55.202.203]
 15   190 ms   170 ms   177 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 16   530 ms     *        *     prod-inriafr-cms.inria.fr [128.93.162.83]
 17   356 ms   186 ms     *     prod-inriafr-cms.inria.fr [128.93.162.83]
 18   204 ms   192 ms   184 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Users\Yogesh>
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
3060 7.394917 10.53.76.103 128.93.162.83 ICMP 106 Echo (ping) request id=0x0001, seq=450/49665, ttl=1 (no response found!)
3265 7.625584 10.53.64.1 10.53.76.103 ICMP 134 Time-to-live exceeded (Time to live exceeded in transit)
3266 7.626236 10.53.76.103 128.93.162.83 ICMP 106 Echo (ping) request id=0x0001, seq=451/49921, ttl=1 (no response found!)
3419 7.843339 10.53.64.1 10.53.76.103 ICMP 134 Time-to-live exceeded (Time to live exceeded in transit)
3420 7.843954 10.53.76.103 128.93.162.83 ICMP 106 Echo (ping) request id=0x0001, seq=452/50177, ttl=1 (no response found!)
3428 7.861877 10.53.64.1 10.53.76.103 ICMP 134 Time-to-live exceeded (Time to live exceeded in transit)
3456 7.915985 224.0.0.252 10.53.76.103 ICMP 111 Time-to-live exceeded (Time to live exceeded in transit)
3664 8.391428 224.0.0.252 10.53.76.103 ICMP 111 Time-to-live exceeded (Time to live exceeded in transit)
6841 13.820825 10.53.76.103 128.93.162.83 ICMP 106 Echo (ping) request id=0x0001, seq=453/50433, ttl=2 (no response found!)
6894 13.903881 210.212.194.2 10.53.76.103 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
6896 13.904671 10.53.76.103 128.93.162.83 ICMP 106 Echo (ping) request id=0x0001, seq=454/50689, ttl=2 (no response found!)
6897 13.909003 210.212.194.2 10.53.76.103 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
6898 13.909559 10.53.76.103 128.93.162.83 ICMP 106 Echo (ping) request id=0x0001, seq=455/50945, ttl=2 (no response found!)
Frame 3265: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{FB8D562D-4600
Ethernet II, Src: Fortinet_e5:45:1c (04:d5:90:e5:45:1c), Dst: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47)
Internet Protocol Version 4, Src: 10.53.64.1, Dst: 10.53.76.103
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: 10.53.76.103, Dst: 128.93.162.83
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf63c [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 450 (0x01c2)
Sequence Number (LE): 49665 (0xc201)
Data (64 bytes)
Data: 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
[Length: 64]
0000 5c 3a 45 b0 53 47 04 d5 90 e5 45 1c 08 00 45 c0
0010 00 78 40 a4 00 00 ff 01 d9 4e 0a 35 40 01 0a 35
0020 4c 67 0b 00 f4 ff 00 00 00 00 45 00 00 5c 8e 6a
0030 00 00 01 01 b1 ea 0a 35 4c 67 80 5d a2 53 08 00
0040 f6 3c 00 01 01 c2 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 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00
Internet Control Message Protocol (icmp), 72 bytes
Packets: 65005 · Displayed: 117 (0.2%) · Dropped: 0 (0.0%)
Profile: Default

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

A: 10.53.76.103, 128.93.162.83

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?

A: 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?

A: No there is no difference from the packets in the first half.

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

A: The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

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?

A: The last three packets differ from the error packets in the Type which are 0 and 11 respectively. This is because the error packets exceeded the time to live and hence are of a different type from the echo reply.

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?

A: Yes, there is a link with a significantly longer delay observed at hop 11, reaching 1482 ms, compared to other hops. The routers at hops 11 and 12, named "**renater-gw-ix1.gtt.net**" and "**hu0-4-0-0-ren-nr-orsay-rtr-091.noc.renater.fr**," respectively, likely indicate routers within the Renater network in France. This delay may stem from network congestion or routing issues within Renater's infrastructure.