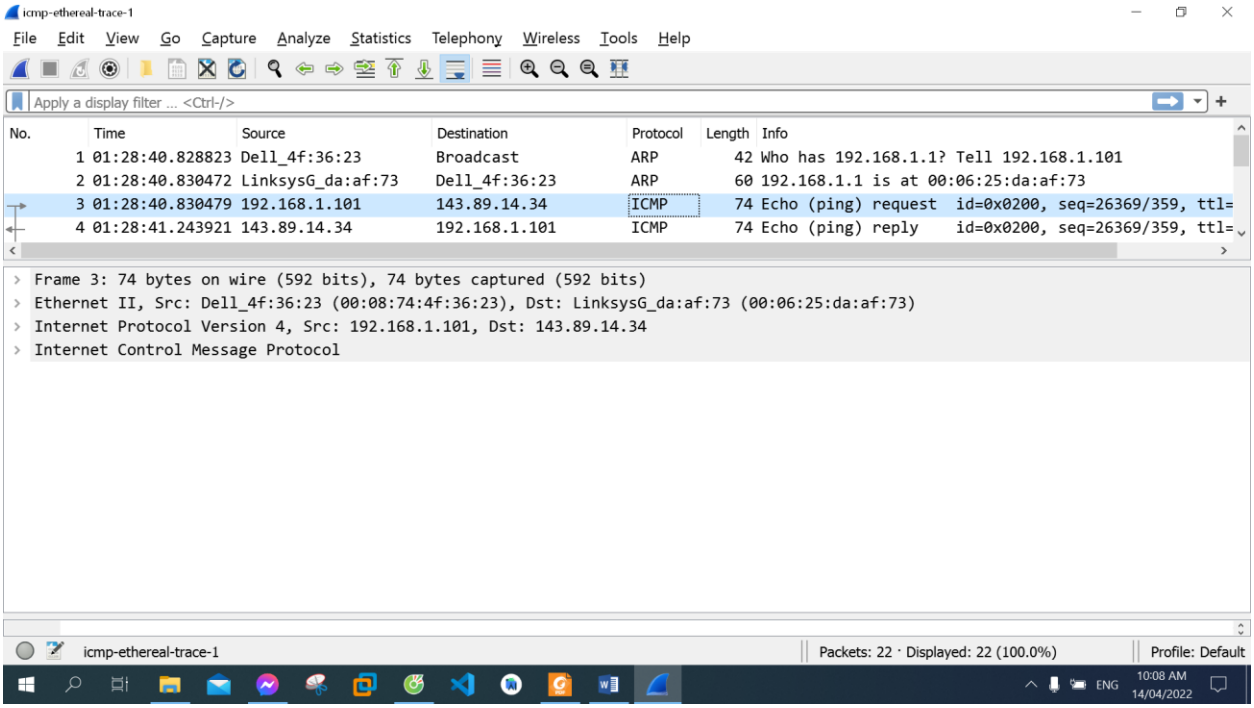
LAB 5
Wireshark Lab: ICMP v8.0

Name: Hồ Đức Trí
Student No: 1912288

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

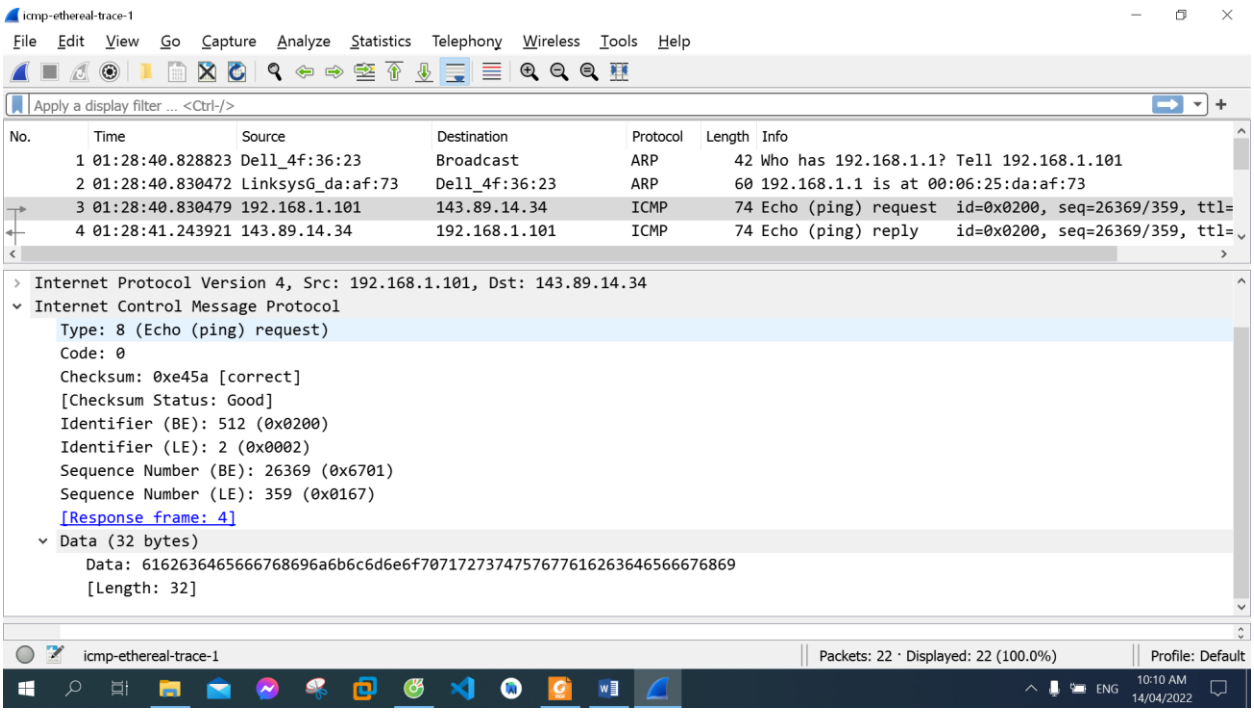


The IP address of my host: 192.168.1.101
The IP address of the destination host: 143.89.14.34

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

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.

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?



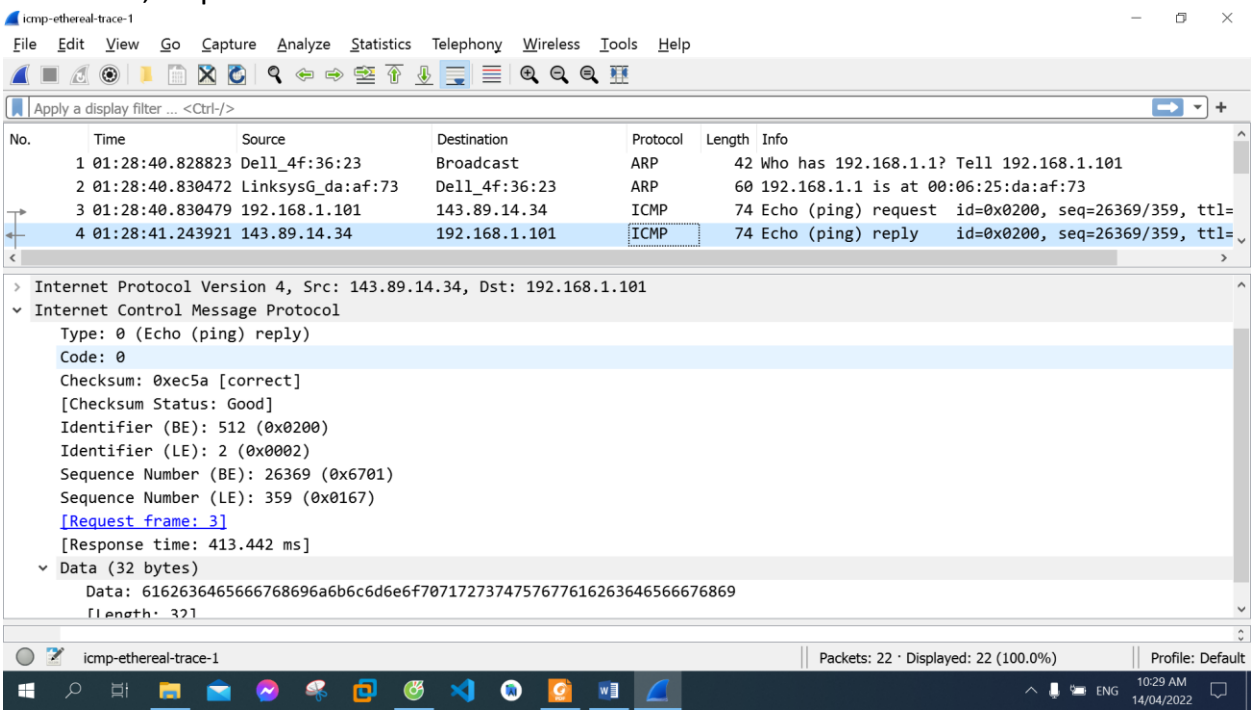
ICMP type: 8

Code number: 0

Other fields this ICMP packet have: Checksum, Identifier, Sequence Number, Data

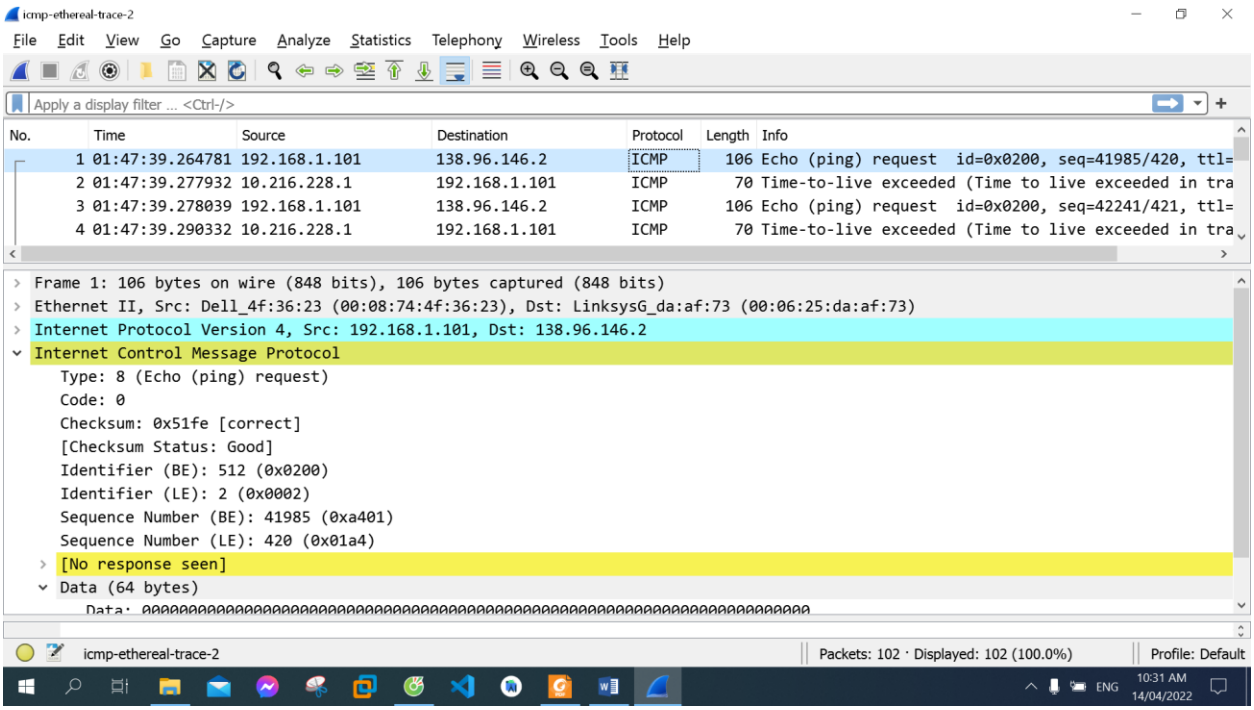
Each of them is 2 bytes

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?



ICMP type: 0
Code number: 0
Other fields this ICMP packet have: Checksum, Identifier, Sequence Number, Data
Each of them is 2 bytes

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



The IP address of my host: 192.168.1.101
The IP address of the target destination: 138.96.146.2

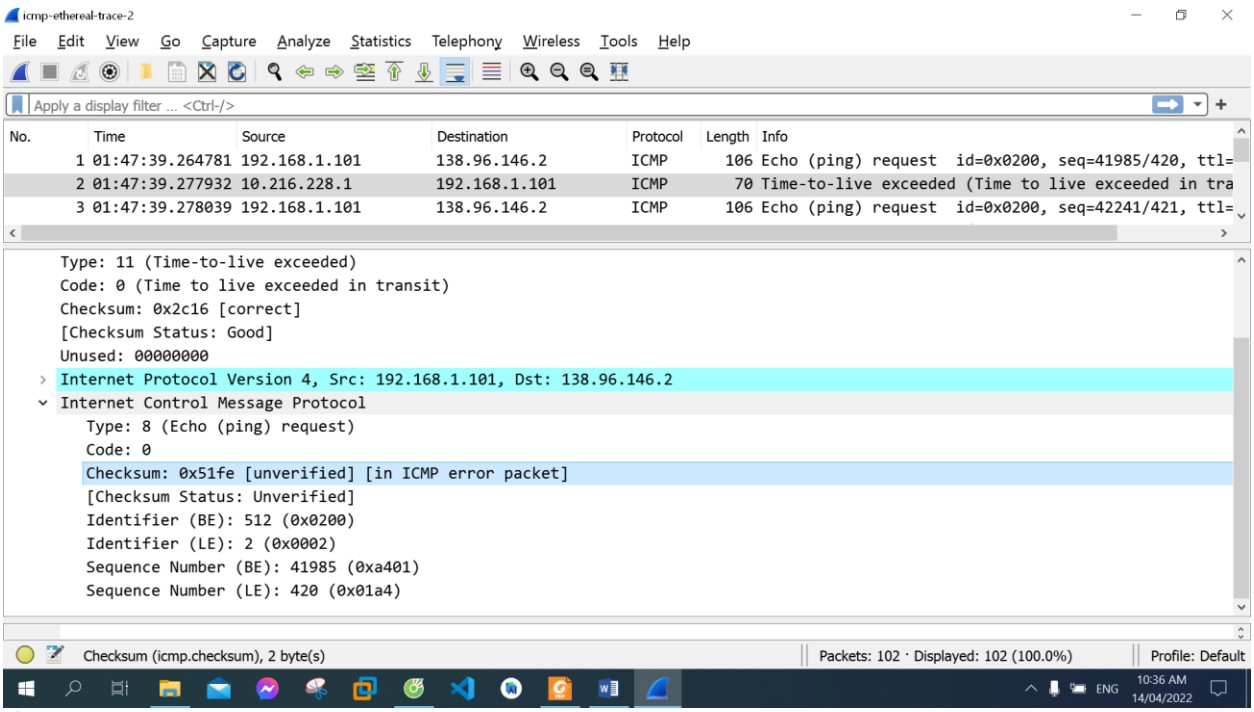
6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

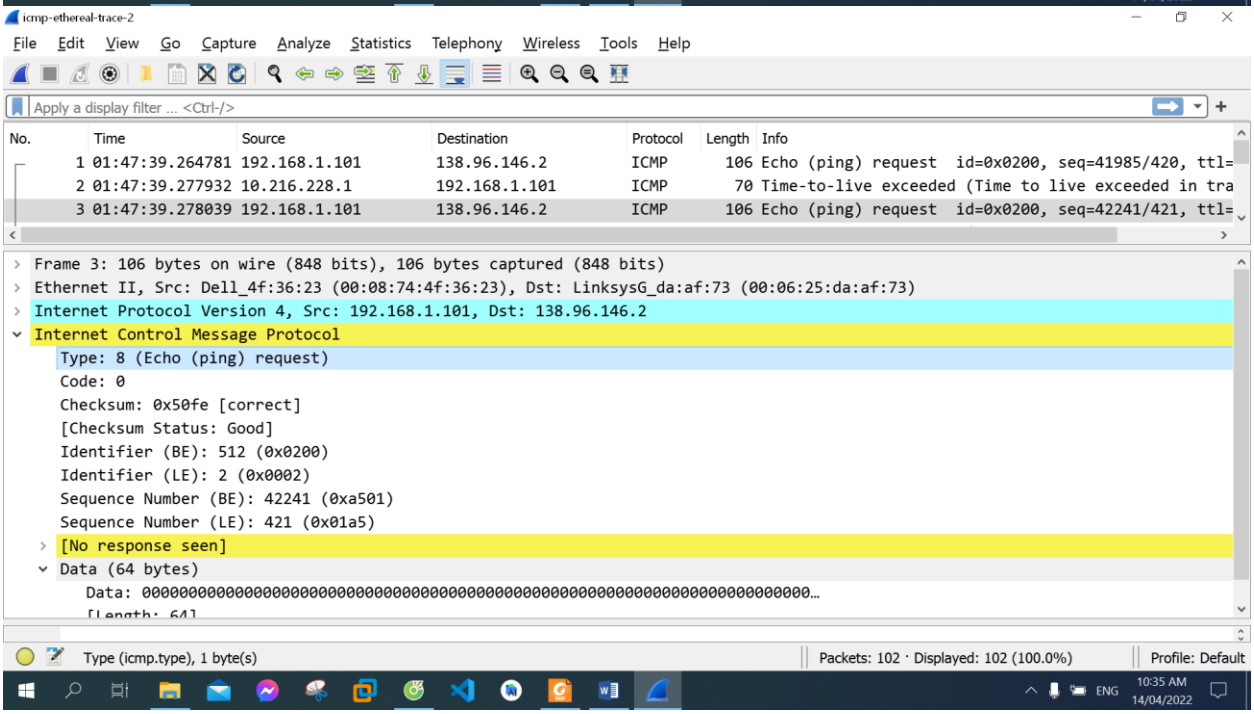
No, the IP protocol number would be 0x11

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?

They have same fields, same ICMP type (8) and code number (0)

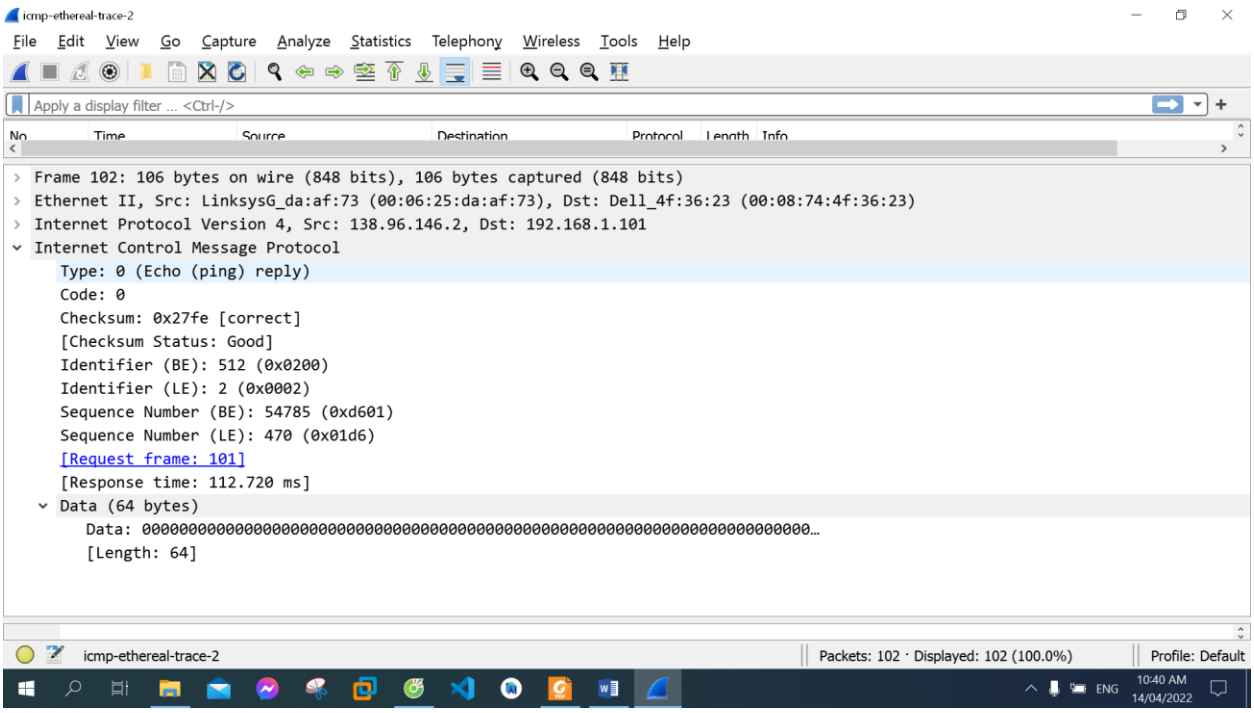
8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?





It includes all of IPv4 fields except Data field and information of the packet that was in error

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?



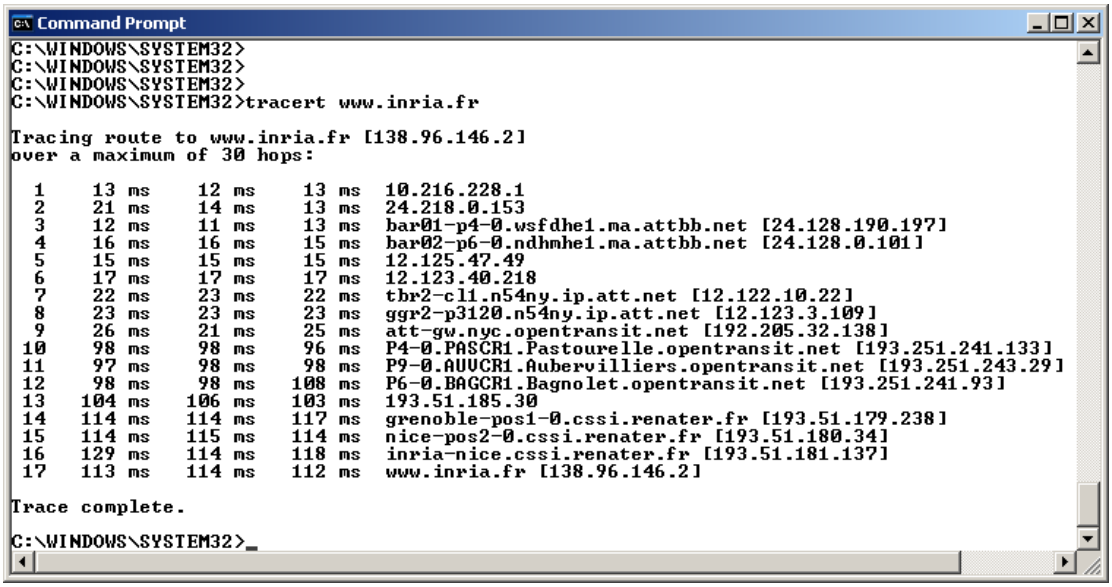
These packets have ICMP type = 0 while the error packets have ICMP type = 11, they have Response frame and Response time, they do not have IPv4 fields and information of the packet that was in error.

They are different because the destination host receive them successfully within the TTL.

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?

```
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

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

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

  1     *        *        *     Request timed out.
  2     7 ms     7 ms     7 ms  125.235.249.190.adsl.viettel.vn [125.235.249.190]
  3     9 ms    13 ms    11 ms  10.255.40.155
  4     6 ms     6 ms    19 ms  DESKTOP-8S8N8IR [27.68.237.186]
  5    40 ms    37 ms    36 ms  DESKTOP-8S8N8IR [27.68.237.139]
  6    28 ms    27 ms    43 ms  DESKTOP-8S8N8IR [27.68.250.169]
  7    35 ms    28 ms    44 ms  xe-2-2-3-xcr1.hke.cw.net [195.89.113.21]
  8    53 ms   178 ms   194 ms  ae4-xcr1.hkg.cw.net [195.2.10.97]
  9   190 ms   188 ms   177 ms  ae11-xcr1.lax.cw.net [195.2.8.33]
 10   181 ms   266 ms   187 ms  gtt-gw.lax.cw.net [195.2.14.46]
 11   317 ms   314 ms   314 ms  et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
 12   228 ms   226 ms   230 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 13   228 ms   234 ms   230 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 14   245 ms   235 ms   226 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 15   228 ms   228 ms   226 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 16   230 ms   230 ms   239 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Users\THINKPAD>_
```

There are 2 links whose delay are significantly longer than others, between 7 and 8, between 10 and 11



Refer to the screenshot in Figure 4, there is a link whose delay is significantly longer than others, between 9 and 10

In figure 4 from the lab, the link is from New York to France