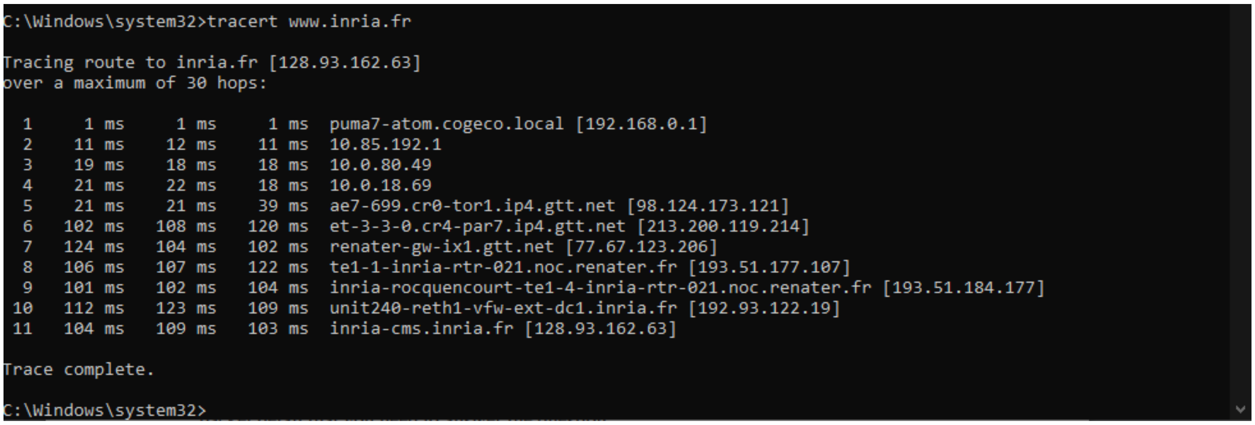
COMP-3670 Lab 4 – Wireshark Lab: ICMP

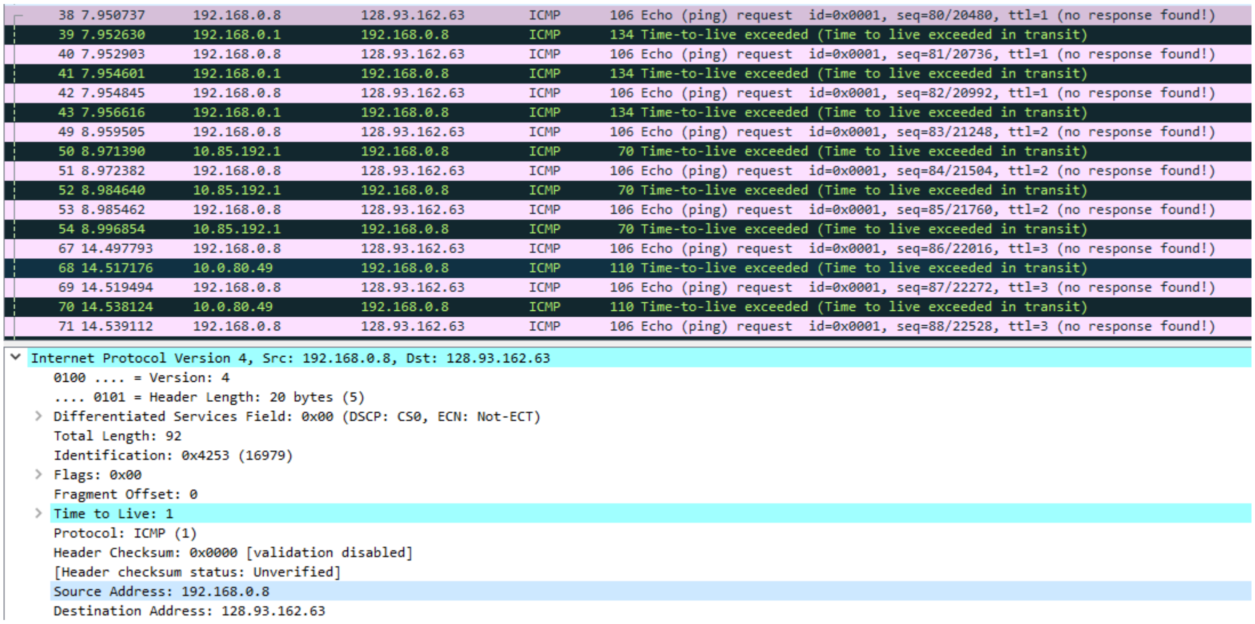
Donovan Longo

105011200



```
C:\Windows\system32>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.63]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  puma7-atom.cogeco.local [192.168.0.1]
  2    11 ms    12 ms    11 ms  10.85.192.1
  3    19 ms    18 ms    18 ms  10.0.80.49
  4    21 ms    22 ms    18 ms  10.0.18.69
  5    21 ms    21 ms    39 ms  ae7-699.cr0-tor1.ip4.gtt.net [98.124.173.121]
  6   102 ms   108 ms   120 ms  et-3-3-0.cr4-par7.ip4.gtt.net [213.200.119.214]
  7   124 ms   104 ms   102 ms  renater-gw-ix1.gtt.net [77.67.123.206]
  8   106 ms   107 ms   122 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
  9   101 ms   102 ms   104 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 10   112 ms   123 ms   109 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 11   104 ms   109 ms   103 ms  inria-cms.inria.fr [128.93.162.63]

Trace complete.

C:\Windows\system32>
```

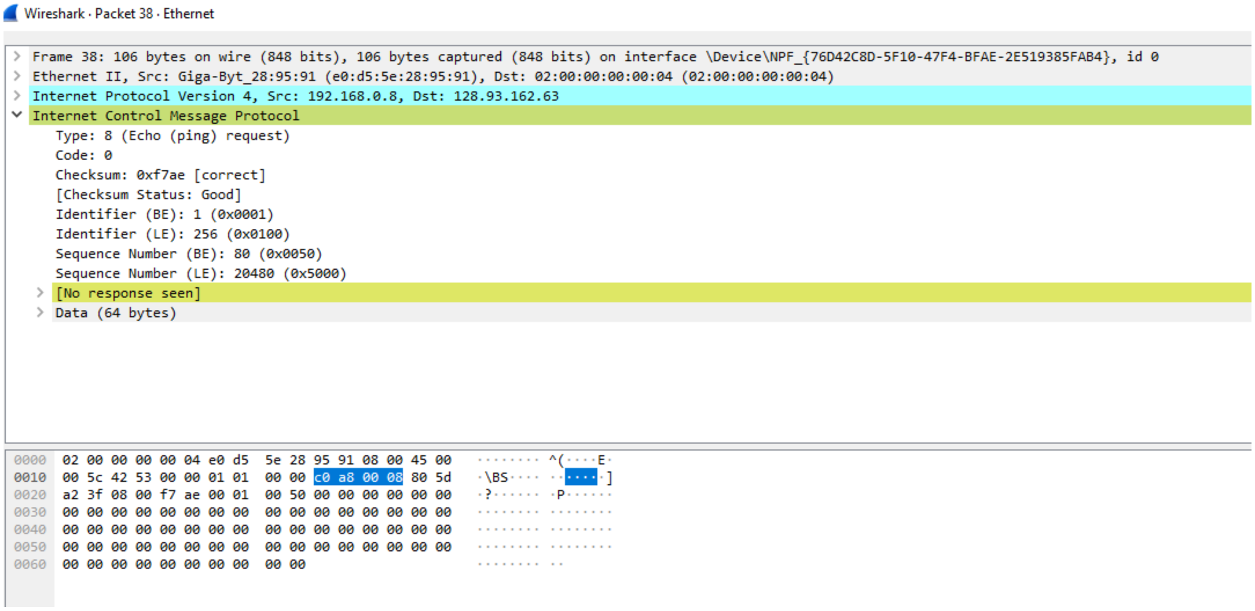
5) Above is a screenshot of my trace root where I used the suggested destination: www.inria.fr. The IP address of my host is: 192.168.0.8 and the IP address of the target destination host is: 128.93.162.63. To confirm when typing in the destination IP into a URL, the browser navigates to the Inria website. Below is a screenshot from the Wireshark trace where I got this data.



```
38 7.950737    192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=80/20480, ttl=1 (no response found!)
39 7.952630    192.168.0.1    192.168.0.8     ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
40 7.952903    192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=81/20736, ttl=1 (no response found!)
41 7.954601    192.168.0.1    192.168.0.8     ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
42 7.954845    192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=82/20992, ttl=1 (no response found!)
43 7.956616    192.168.0.1    192.168.0.8     ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
49 8.959505    192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=83/21248, ttl=2 (no response found!)
50 8.971390    10.85.192.1    192.168.0.8     ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
51 8.972382    192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=84/21504, ttl=2 (no response found!)
52 8.984640    10.85.192.1    192.168.0.8     ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
53 8.985462    192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=85/21760, ttl=2 (no response found!)
54 8.996854    10.85.192.1    192.168.0.8     ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
67 14.497793   192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=86/22016, ttl=3 (no response found!)
68 14.517176   10.0.80.49     192.168.0.8     ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
69 14.519494   192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=87/22272, ttl=3 (no response found!)
70 14.538124   10.0.80.49     192.168.0.8     ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
71 14.539112   192.168.0.8    128.93.162.63   ICMP   106 Echo (ping) request  id=0x0001, seq=88/22528, ttl=3 (no response found!)

v Internet Protocol Version 4, Src: 192.168.0.8, Dst: 128.93.162.63
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x4253 (16979)
  > Flags: 0x00
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.8
    Destination Address: 128.93.162.63
```

6) If ICMP sent UDP packets the IP protocol number would be 17 compared to 1.

7) Using the screenshot below of the second ICMP echo packet of this trace to a ping packet in the first half of the lab we can see that both packets have the same fields. What differs between the two are the data within the fields: Checksum and both Sequence Numbers (BE and LE), which makes sense because they are separate packets.

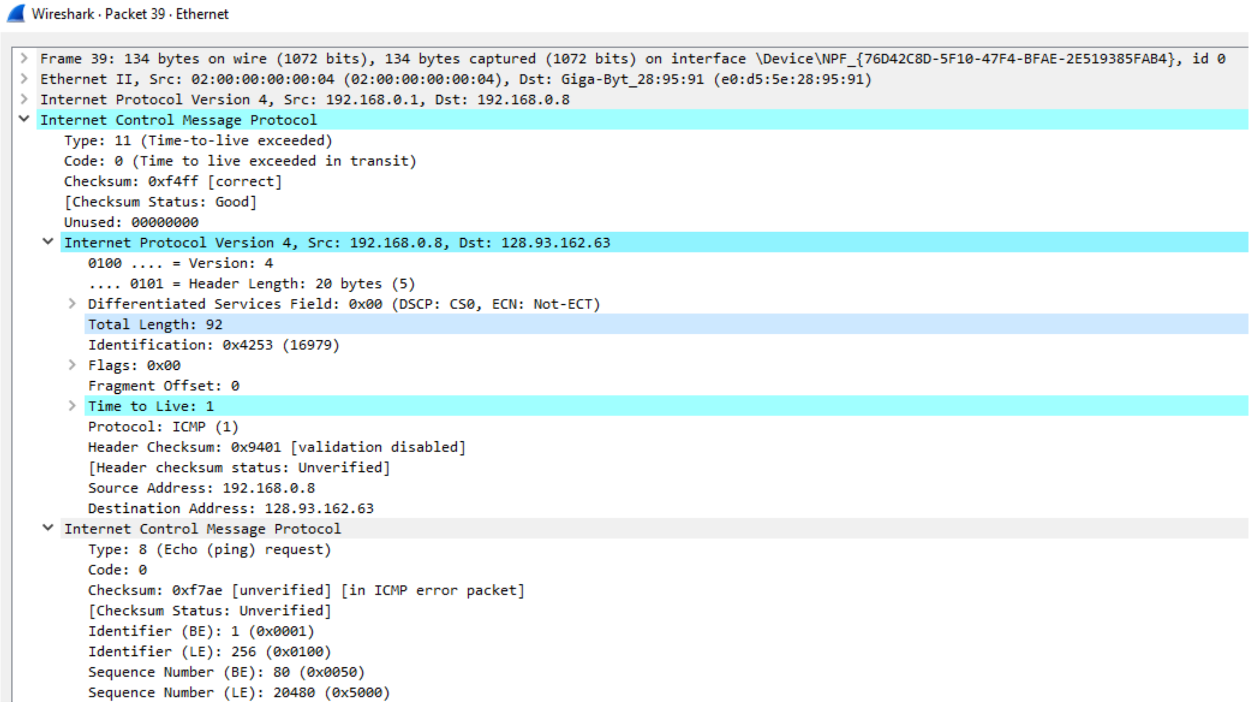


Wireshark · Packet 38 · Ethernet

```
> Frame 38: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{76D42C8D-5F10-47F4-BFAE-2E519385FAB4}, id 0
> Ethernet II, Src: Giga-Byt_28:95:91 (e0:d5:5e:28:95:91), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
> Internet Protocol Version 4, Src: 192.168.0.8, Dst: 128.93.162.63
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ae [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 80 (0x0050)
    Sequence Number (LE): 20480 (0x5000)
  > [No response seen]
  > Data (64 bytes)
```

```
0000  02 00 00 00 00 04 e0 d5  5e 28 95 91 08 00 45 00   ········ ^(····E·
0010  00 5c 42 53 00 00 01 01  00 00 c0 a8 00 08 80 5d   ·\BS···· ······]
0020  a2 3f 08 00 f7 ae 00 01  00 50 00 00 00 00 00 00   ·?······ ·P······
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                     ········ ··
```

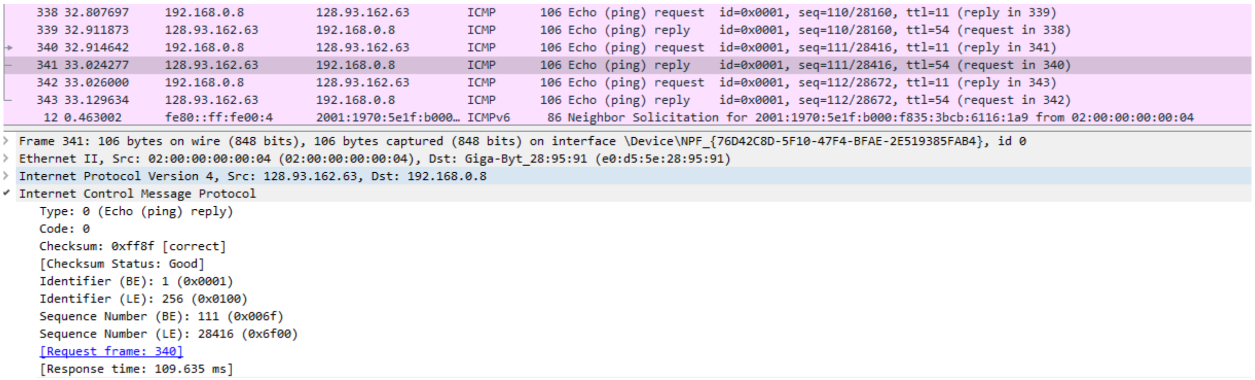
8) The ICMP error packet details can be seen in the screenshot below. We can see that the error packet includes the IP header. This would be the IP header of the packet that prompted the error. The error packet also includes the first 8 bytes from the same packet that triggered the error.



Wireshark · Packet 39 · Ethernet

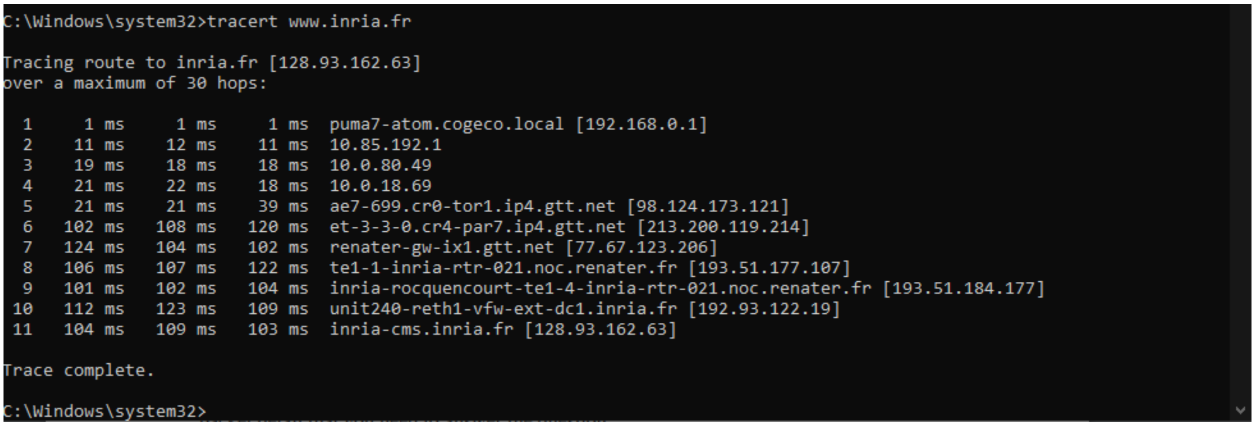
```
> Frame 39: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{76D42C8D-5F10-47F4-BFAE-2E519385FAB4}, id 0
> Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: Giga-Byt_28:95:91 (e0:d5:5e:28:95:91)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.8
v 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
  v Internet Protocol Version 4, Src: 192.168.0.8, Dst: 128.93.162.63
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 92
      Identification: 0x4253 (16979)
    > Flags: 0x00
      Fragment Offset: 0
    > Time to Live: 1
      Protocol: ICMP (1)
      Header Checksum: 0x9401 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.0.8
      Destination Address: 128.93.162.63
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7ae [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 80 (0x0050)
      Sequence Number (LE): 20480 (0x5000)
```

9) The last 3 ICMP reply packets are different from the error packets because the did not exceed TTL. We can see in the screenshots below they are type 0 (echo (ping) reply) which means they completed their transit to the destination before TTL past.



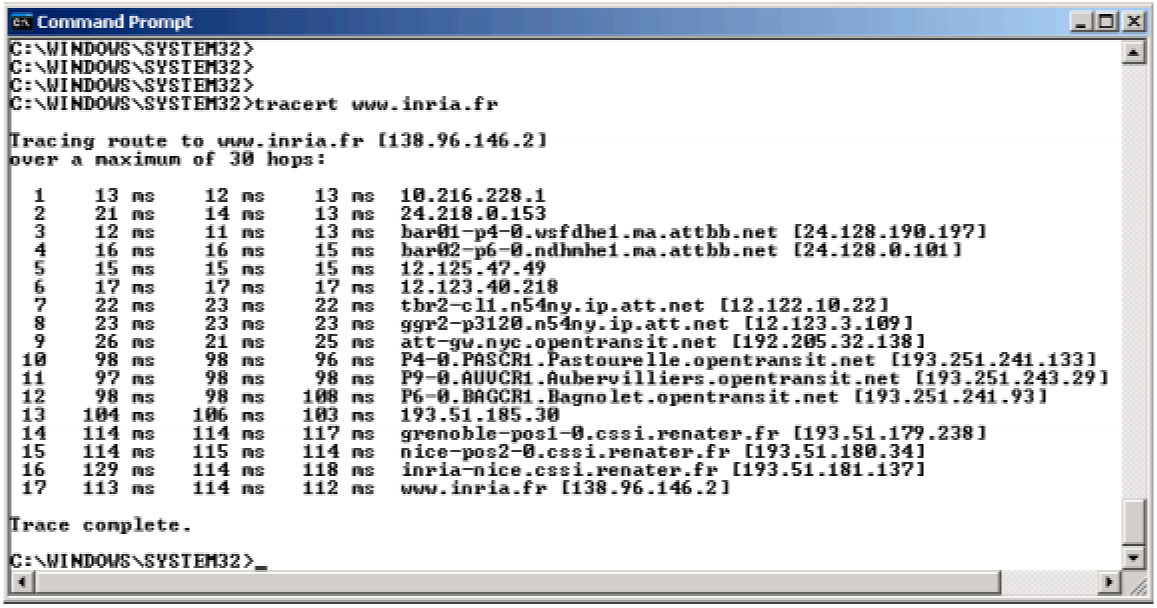
```
  338 32.807697    192.168.0.8        128.93.162.63      ICMP     106 Echo (ping) request  id=0x0001, seq=110/28160, ttl=11 (reply in 339)
  339 32.911873    128.93.162.63      192.168.0.8        ICMP     106 Echo (ping) reply    id=0x0001, seq=110/28160, ttl=54 (request in 338)
  340 32.914642    192.168.0.8        128.93.162.63      ICMP     106 Echo (ping) request  id=0x0001, seq=111/28416, ttl=11 (reply in 341)
  341 33.024277    128.93.162.63      192.168.0.8        ICMP     106 Echo (ping) reply    id=0x0001, seq=111/28416, ttl=54 (request in 340)
  342 33.026000    192.168.0.8        128.93.162.63      ICMP     106 Echo (ping) request  id=0x0001, seq=112/28672, ttl=11 (reply in 343)
  343 33.129634    128.93.162.63      192.168.0.8        ICMP     106 Echo (ping) reply    id=0x0001, seq=112/28672, ttl=54 (request in 342)
   12 0.463002     fe80::ff:fe00:4    2001:1970:5e1f:b000… ICMPv6  86 Neighbor Solicitation for 2001:1970:5e1f:b000:f835:3bcb:6116:1a9 from 02:00:00:00:00:04

> Frame 341: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{76D42C8D-5F10-47F4-BFAE-2E519385FAB4}, id 0
> Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: Giga-Byt_28:95:91 (e0:d5:5e:28:95:91)
> Internet Protocol Version 4, Src: 128.93.162.63, Dst: 192.168.0.8
✓ Internet Control Message Protocol
     Type: 0 (Echo (ping) reply)
     Code: 0
     Checksum: 0xff8f [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 111 (0x006f)
     Sequence Number (LE): 28416 (0x6f00)
     [Request frame: 340]
     [Response time: 109.635 ms]
```

10) Below is the screenshot from the trace root used for this section of the lab. (Equivalent to the first image of this report). We can clearly see that from steps 5 to 6 there is a large jump in the response delay.



```
C:\Windows\system32>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.63]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  puma7-atom.cogeco.local [192.168.0.1]
  2    11 ms    12 ms    11 ms  10.85.192.1
  3    19 ms    18 ms    18 ms  10.0.80.49
  4    21 ms    22 ms    18 ms  10.0.18.69
  5    21 ms    21 ms    39 ms  ae7-699.cr0-tor1.ip4.gtt.net [98.124.173.121]
  6   102 ms   108 ms   120 ms  et-3-3-0.cr4-par7.ip4.gtt.net [213.200.119.214]
  7   124 ms   104 ms   102 ms  renater-gw-ix1.gtt.net [77.67.123.206]
  8   106 ms   107 ms   122 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
  9   101 ms   102 ms   104 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 10   112 ms   123 ms   109 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 11   104 ms   109 ms   103 ms  inria-cms.inria.fr [128.93.162.63]

Trace complete.

C:\Windows\system32>
```

Referring to figure 4 included in the lab (seen below). The increase in the response delay is from steps 9 to 10. Using the names of the routers I can infer that in step 9 the location of the router is located in New York City and in step 10, the location of the router is located in Pastourelle which I can only assume is in France because we are trying to ping a French website.



```
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>_
```