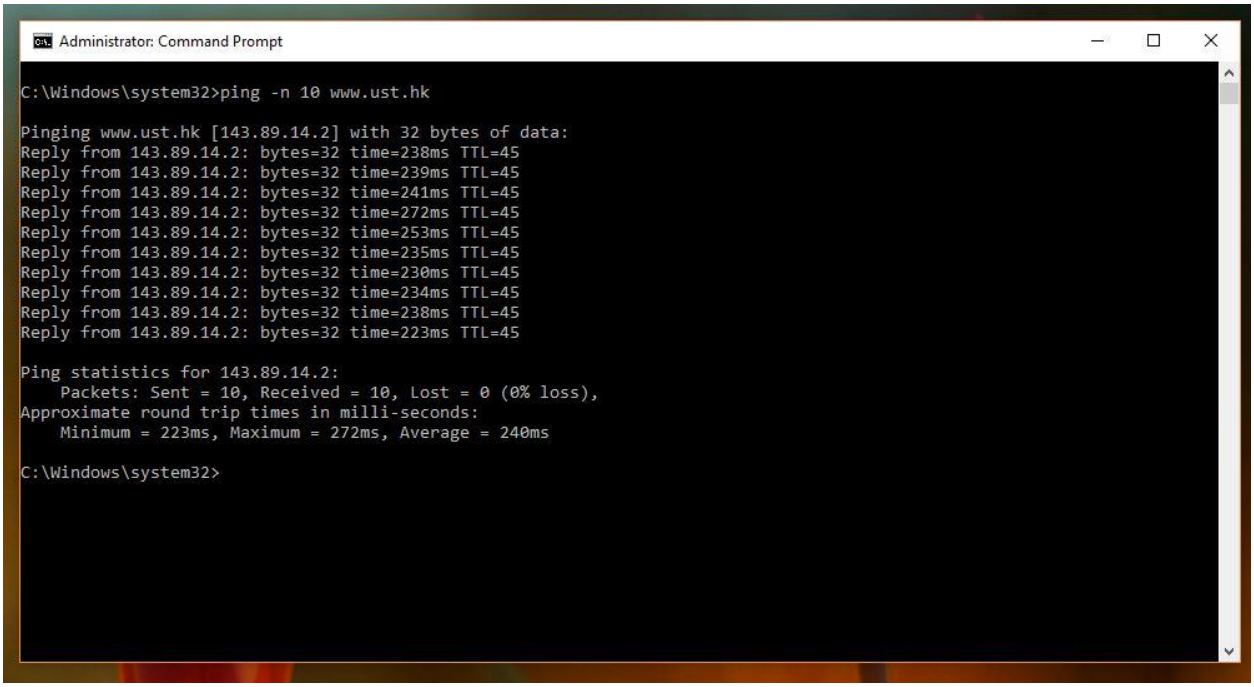
Lab 8 Solution

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

   ANS



   Host: 192.168.0.29

   Destination: 143.89.14.2

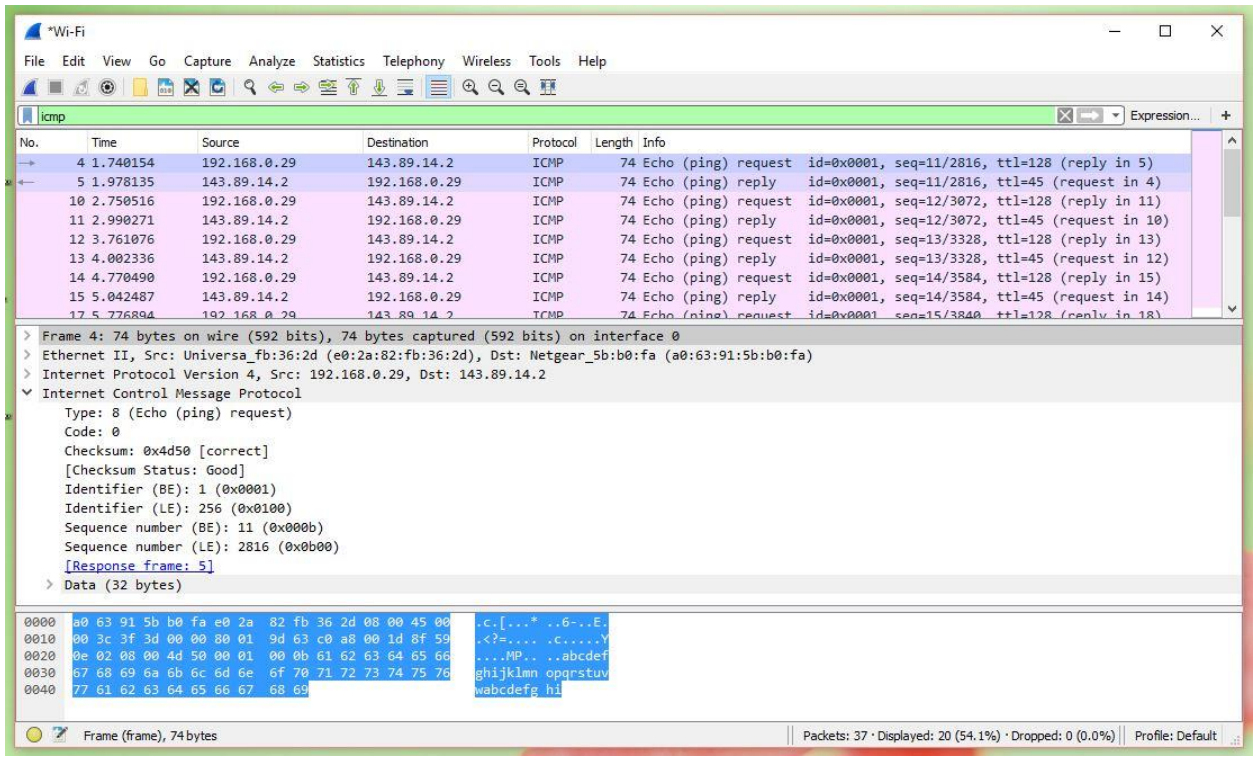
2. Why is it that an ICMP packet does not have source and destination port numbers?

   ANS

   It doesn't have source and destination port because it is designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a Type and a Code which identifies the specific message being received. The network software interprets all ICMP messages so 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?

ANS



Type: 8

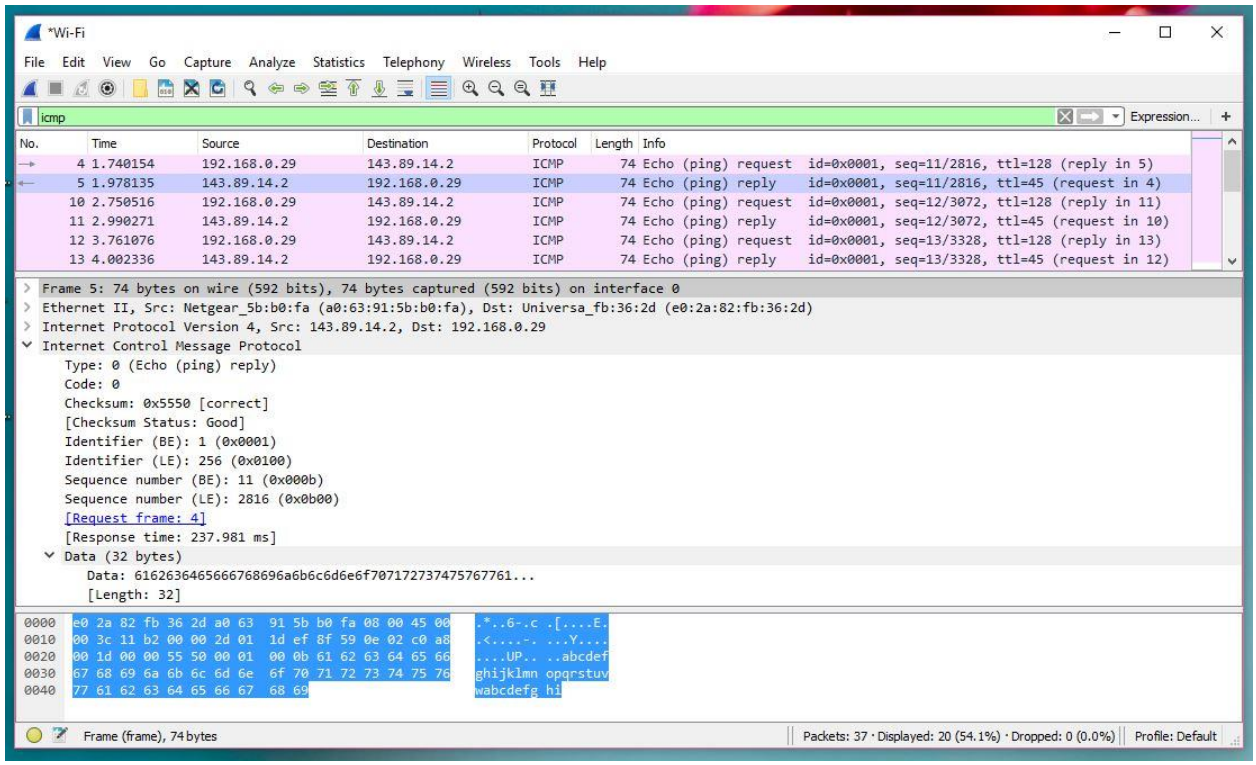
Code: 0

Other fields: Checksum, Identifier (BE)/(LE), sequence number(BE/LE) and Data field.

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?

ANS



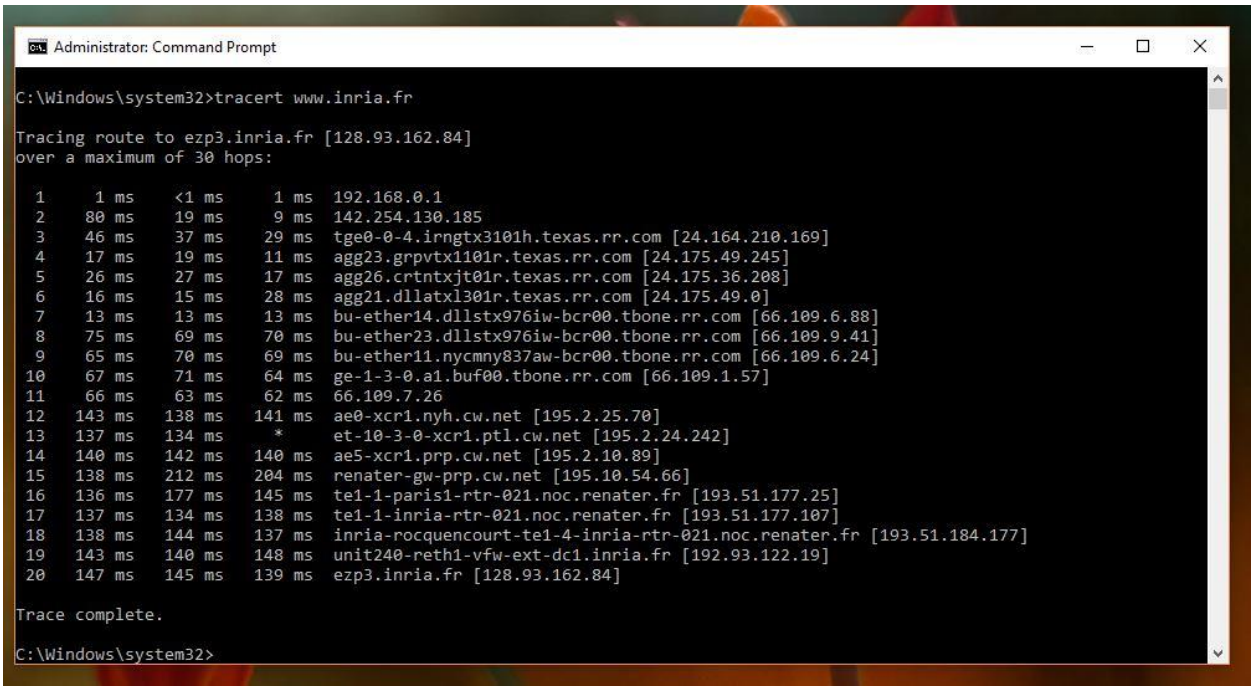
Type: 0

Code: 0

Other fields: Checksum, Identifier (BE)/(LE), sequence number(BE/LE) and Data field.

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?
   ANS



```
Administrator: Command Prompt

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

Tracing route to ezp3.inria.fr [128.93.162.84]
over a maximum of 30 hops:

  1     1 ms    <1 ms     1 ms  192.168.0.1
  2    80 ms    19 ms     9 ms  142.254.130.185
  3    46 ms    37 ms    29 ms  tge0-0-4.irngtx3101h.texas.rr.com [24.164.210.169]
  4    17 ms    19 ms    11 ms  agg23.grpvtx1101r.texas.rr.com [24.175.49.245]
  5    26 ms    27 ms    17 ms  agg26.crtntxjt01r.texas.rr.com [24.175.36.208]
  6    16 ms    15 ms    28 ms  agg21.dllatxl301r.texas.rr.com [24.175.49.0]
  7    13 ms    13 ms    13 ms  bu-ether14.dllstx976iw-bcr00.tbone.rr.com [66.109.6.88]
  8    75 ms    69 ms    70 ms  bu-ether23.dllstx976iw-bcr00.tbone.rr.com [66.109.9.41]
  9    65 ms    70 ms    69 ms  bu-ether11.nycmny837aw-bcr00.tbone.rr.com [66.109.6.24]
 10    67 ms    71 ms    64 ms  ge-1-3-0.a1.buf00.tbone.rr.com [66.109.1.57]
 11    66 ms    63 ms    62 ms  66.109.7.26
 12   143 ms   138 ms   141 ms  ae0-xcr1.nyh.cw.net [195.2.25.70]
 13   137 ms   134 ms     *     et-10-3-0-xcr1.ptl.cw.net [195.2.24.242]
 14   140 ms   142 ms   140 ms  ae5-xcr1.prp.cw.net [195.2.10.89]
 15   138 ms   212 ms   204 ms  renater-gw-prp.cw.net [195.10.54.66]
 16   136 ms   177 ms   145 ms  te1-1-paris1-rtr-021.noc.renater.fr [193.51.177.25]
 17   137 ms   134 ms   138 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 18   138 ms   144 ms   137 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 19   143 ms   140 ms   148 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 20   147 ms   145 ms   139 ms  ezp3.inria.fr [128.93.162.84]

Trace complete.

C:\Windows\system32>
```

   My host: 192.168.0.29
   Destination host: 128.93.162.84

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?
   ANS
   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?
   ANS
   The ICMP echo packet has the same fields as the ping query packets.

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?
   ANS
   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?
   ANS
   Last 3 ICMP packets are message type 0 and 8 rather than 11. 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?
    ANS
    I think there is a link between step 11 and 12 that has a significantly longer delay comparing to others.