Solutions to

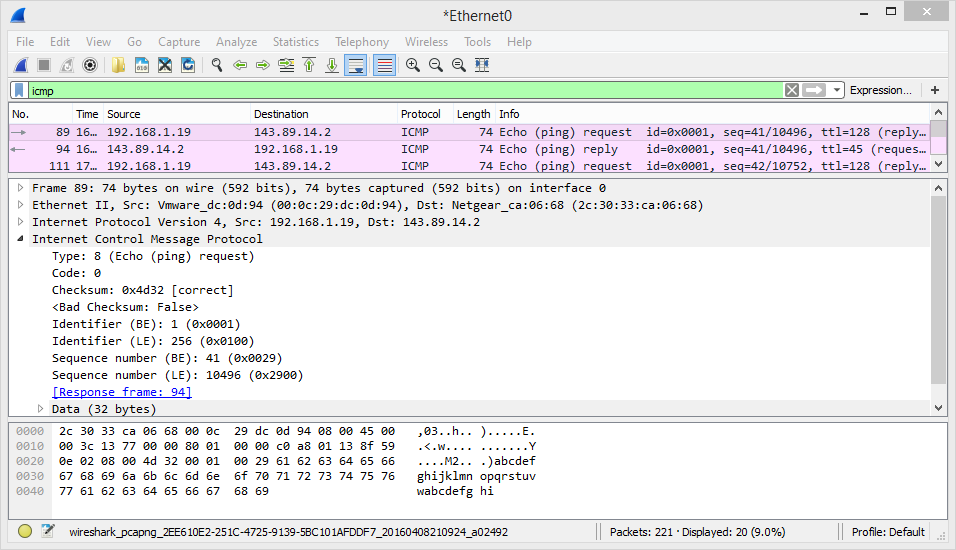
Wireshark Lab - 2: ICMP

Part I. ICMP and Ping

Screenshot of the Command Prompt window:

### 

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



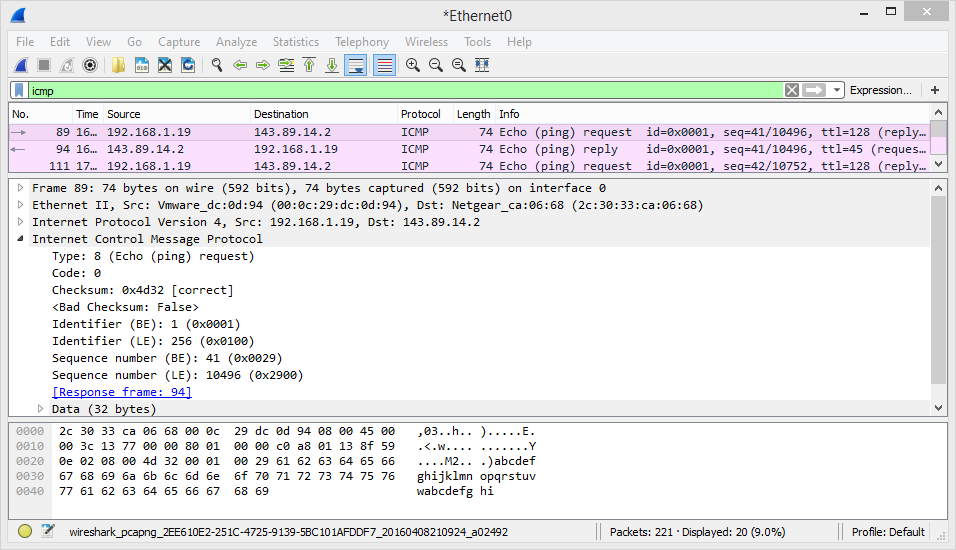
IP Address of my host = 192.168.1.19

IP Address of destination host = 143.89.14.2

1. Does an ICMP packet have source and destination **port** numbers? Why?

An ICMP is part of the Internet Layer and it does not require a connection to be established. Hence an ICMP Packet does not have a source or destination port.

1. 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?

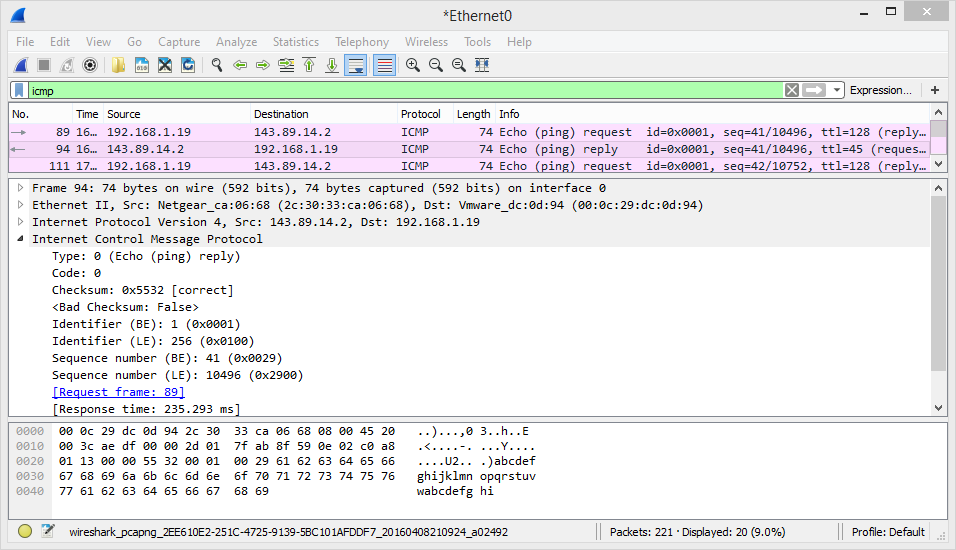


Type: 8

Code: 0

The request packet has a checksum for error control and a sequence number.

1. Examine the corresponding ping **reply** packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have?



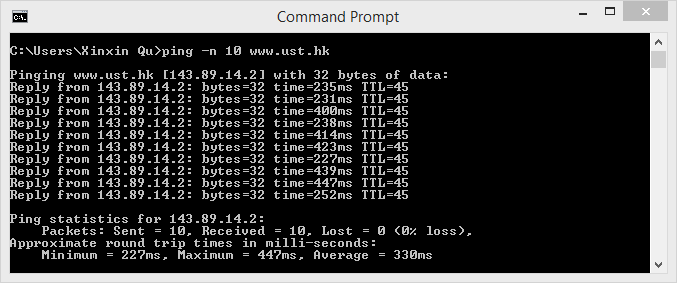
The corresponding reply has:

Type: 0

Code: 0

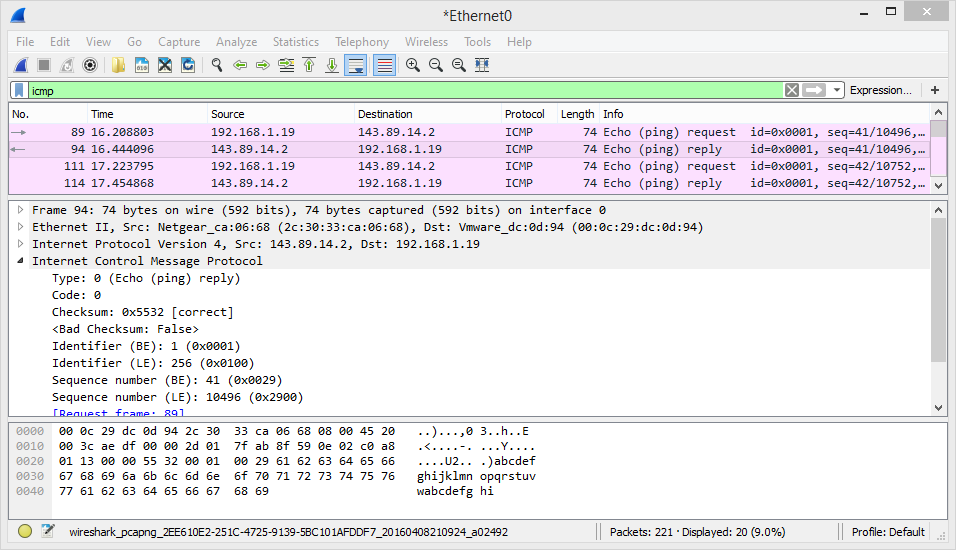
The reply packet has a checksum for error control and a sequence number.

1. For the first ping request/reply cycle, calculate the Round Trip Time (RTT) based on the time field in the Wireshark packet trace. Compare it with the RTT listed in the Command Prompt window. Are they the same?



From the command prompt,

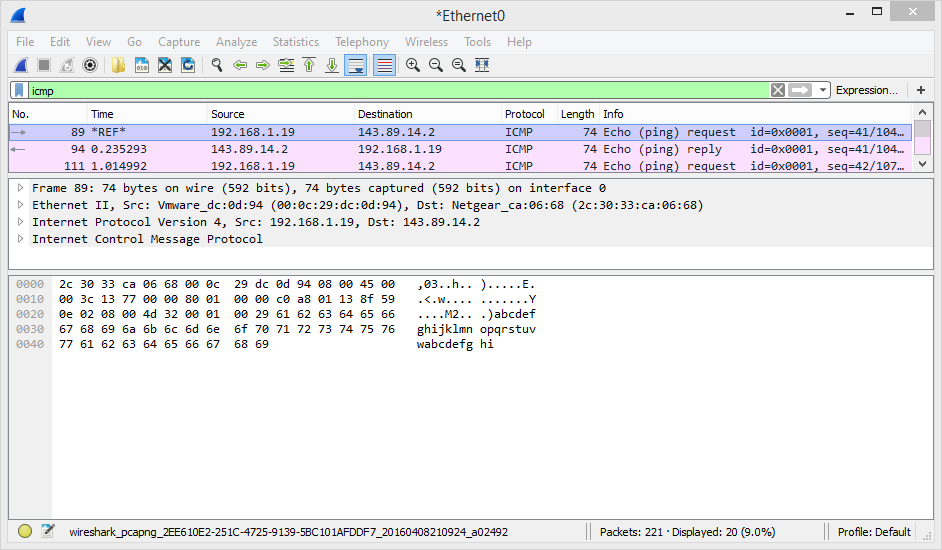
RTT=235ms



From Wireshark:

Request sent time is: 16.208803

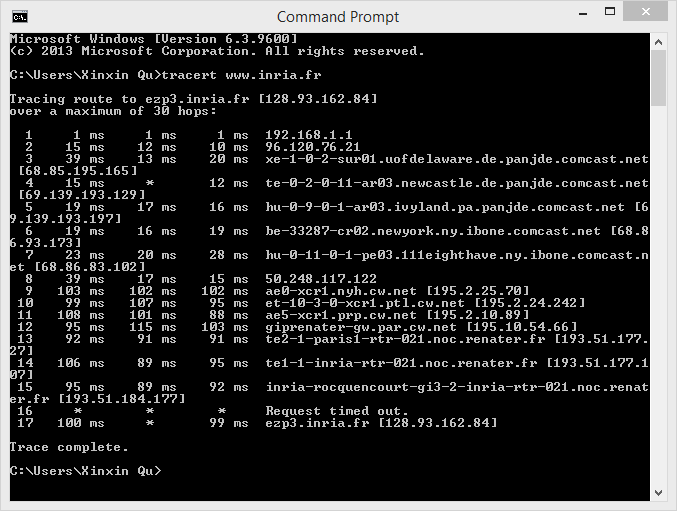
Reply received time is: 16.44096



If you set time reference on the first request, you can see the time difference of the two is 0.235293s, if you round this number to 3 decimal places, you will get exactly the same RTTs (0.235s which is 235ms) as listed in the Command Prompt window.

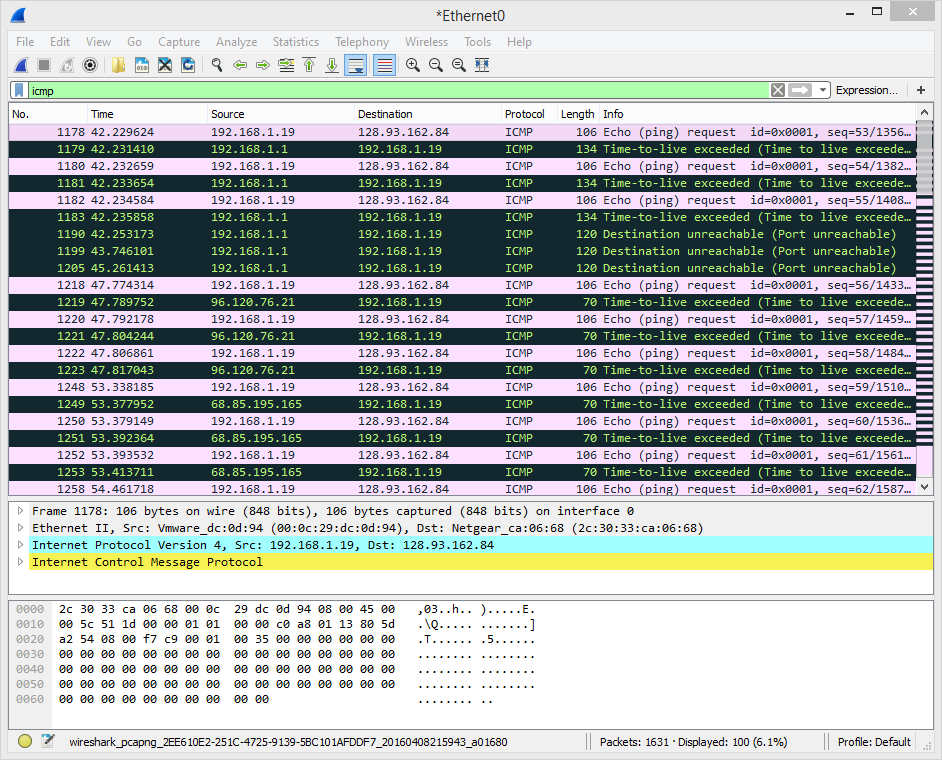
Part II. ICMP and Traceroute

Screenshot of the Command Prompt window:



Answer the following questions:

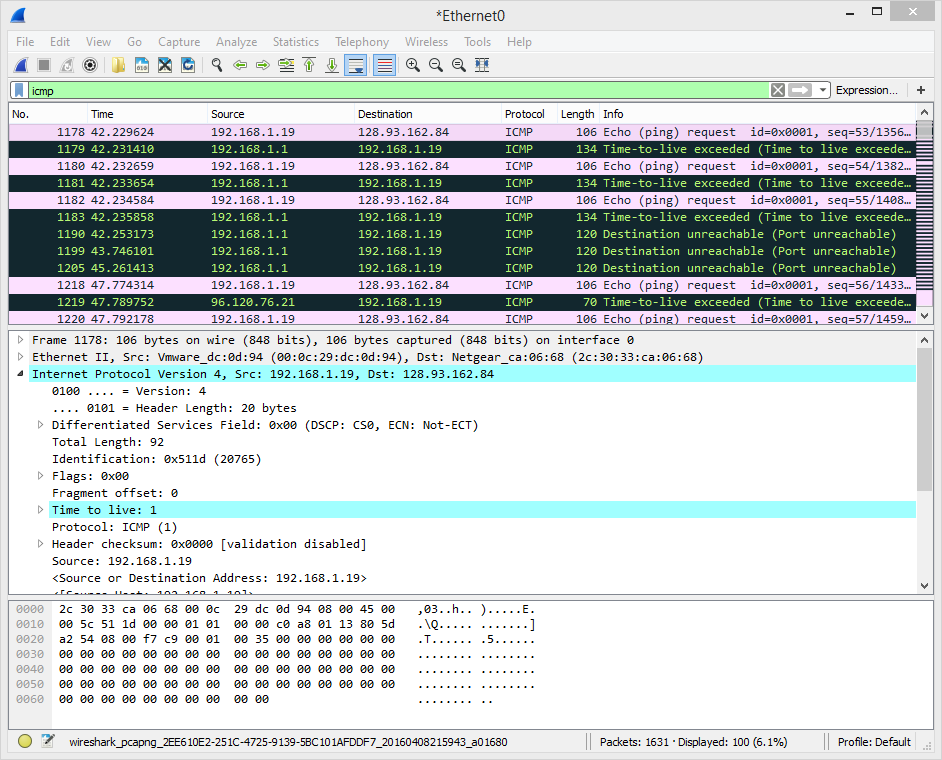
1. What is the IP address of your host? What is the IP address of the target destination host?

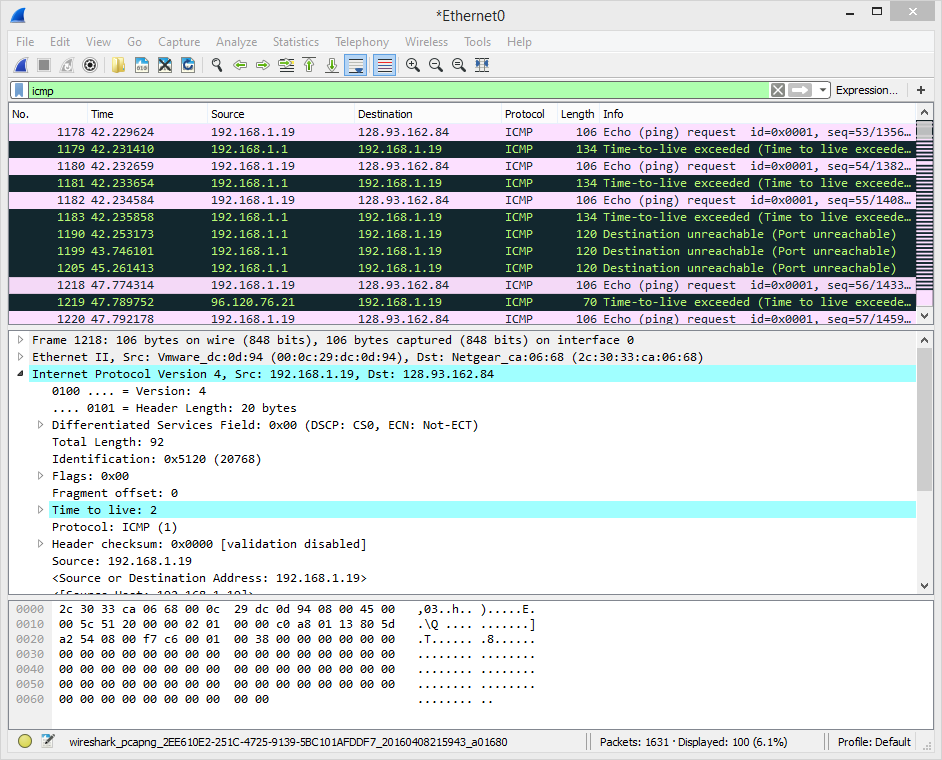


IP address of my host: 196.168.1.19

IP address of the destination host (www.inria.fr): 128.93.162.84

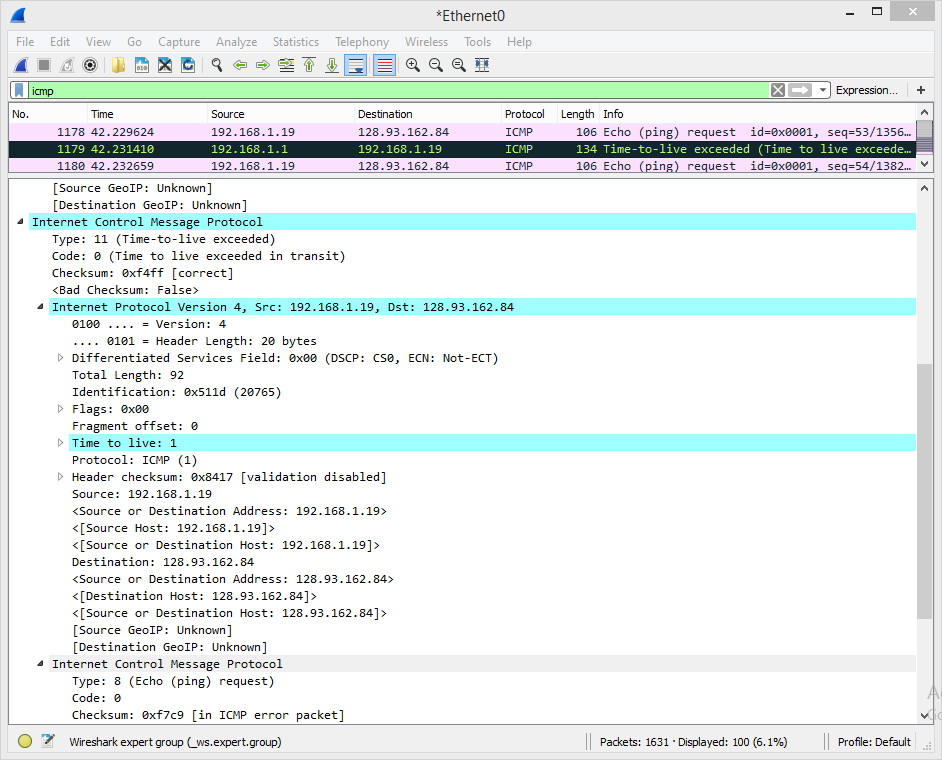
1. Examine the ICMP **echo** packet in your captured packets. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?





In the new ICMP query packets, the Time to live (TTL) field of the IP is incremented by 1 every 3 requests, whereas it was a constant (45) in the query packets of the previous part.

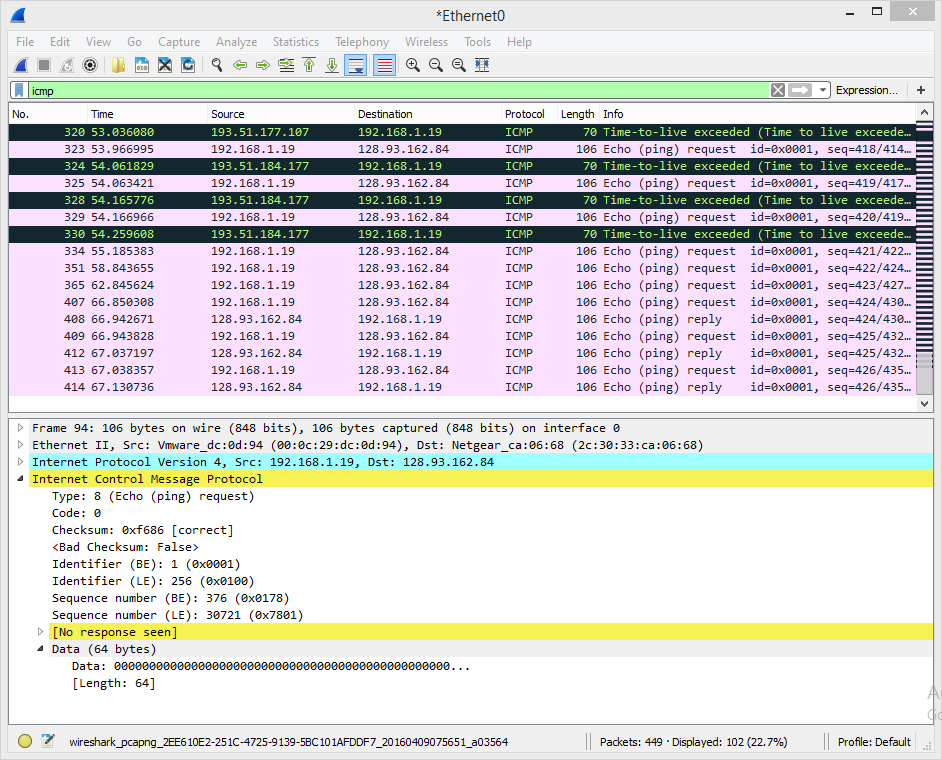
1. Examine the ICMP **error** packet in your captured packets. It has more fields than the ICMP echo packet. What are included in those fields?



The error packet contains the type and the code as the reply packet. This is as if saying to the sender, *here is what the error is and this is what caused it.*

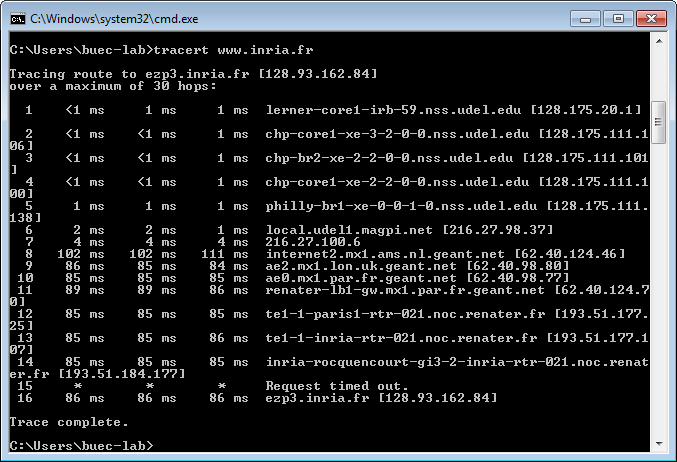
1. Examine the **last three** ICMP packets **received by the source** host. How are these packets different from the ICMP error packets? Why are they different?

The last three messages are reply messages and not error messages. They are different, as they do not contain the copy of the request message. They are sent by the destination host and hence are not error messages.



The last three messages are reply messages and not error messages. They are different as they do not contain the copy of the request message. They are sent by the destination host and hence are not error messages.

1. 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?

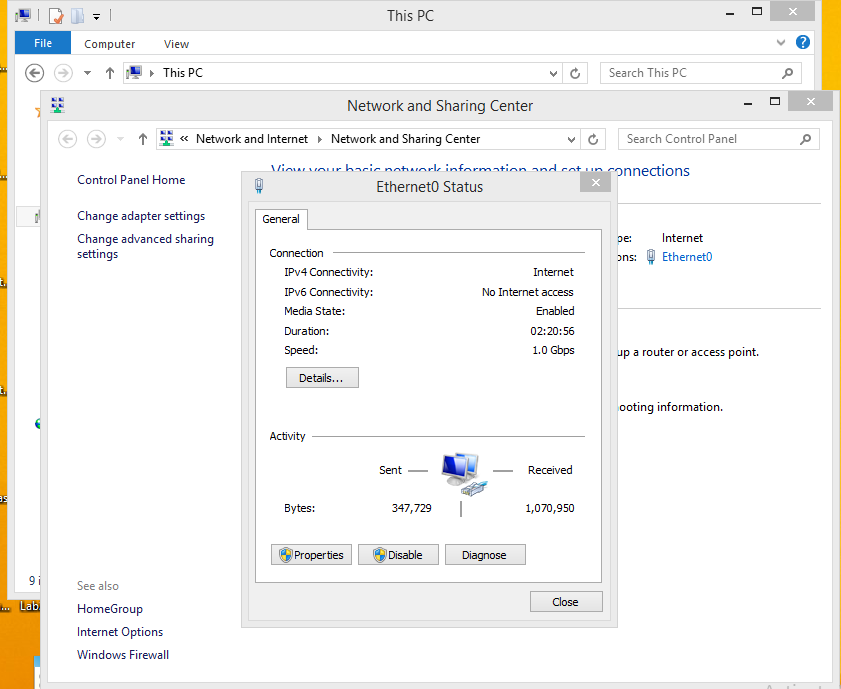


Step 8 represents a jump in the RTT. From the domain names, we can see that the message has hopped from a server in US to a server in Amsterdam of Netherlands, hence the delay.

The Next Step

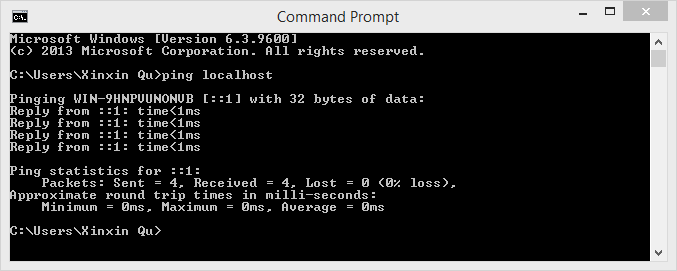
If both the name and the IP address fail, the following problems may exist.

1. **Your computer is not connected to the Internet.**   
   – How to find out? Check your wire or your wireless signal!



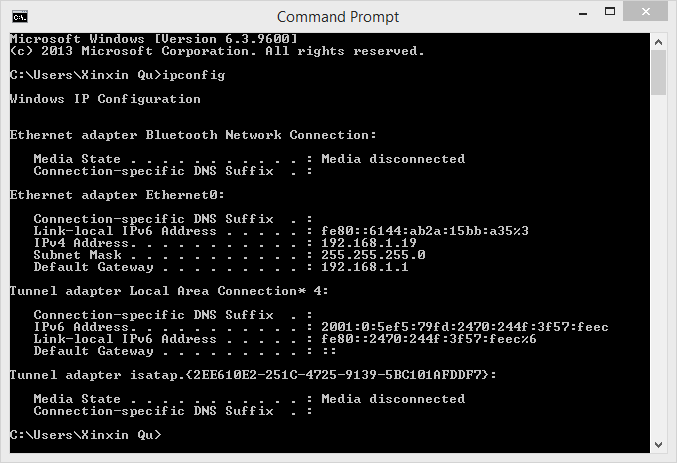
TEST PASSED

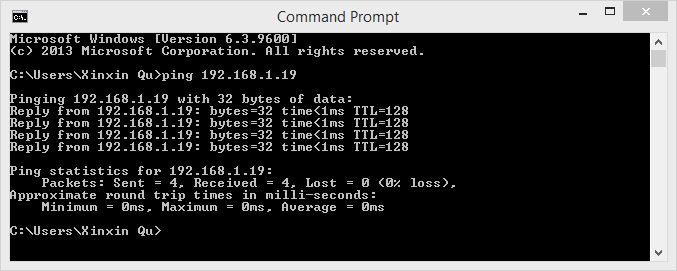
1. **Your computer’s TCP/IP protocol stack is damaged.**   
   – How to find out? Type “ping localhost” or “ping 127.0.0.1” (recall that 127.0.0.1 is the loopback IP address) in your Command Prompt window. If this ping command fails, you need to verify that your computer was restarted after TCP/IP was installed and configured. Or you might want to reinstall the TCP/IP protocol stack.



TEST PASSED

1. **Your computer’s IP address is not added to the network correctly.**– How to find out? Type “ping *IP\_address\_of\_local\_host*” (you can find your computer’s IP address by using the “ipconfig” utility) in your Command Prompt window. If this ping command fails, again you need to verify that your computer was restarted after TCP/IP was installed and configured.



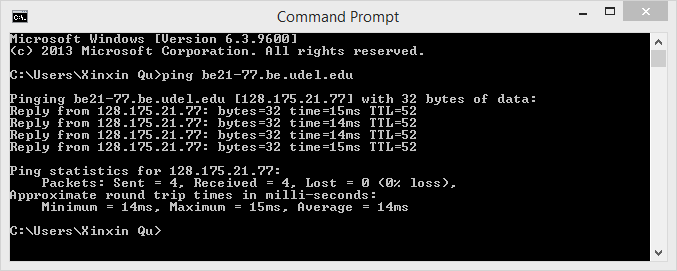


TEST PASSED

1. **Your default gateway (router) is not working appropriately.**   
   – How to find out? Type “ping IP\_address\_of\_default\_gateway” (you can find the default gateway by using the “ipconfig” utility). If this ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.

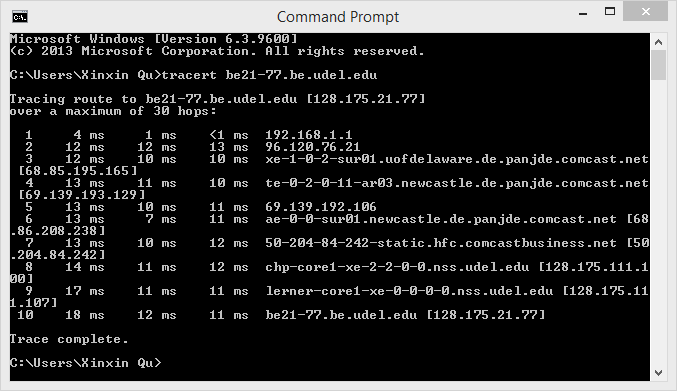
TEST PASSED

1. **There is a routing problem and the destination network is unreachable.**– How to find out? If you know the IP address of another server that is in the same destination network, try to ping and traceroute to that server. If it is successful, you can rule out this problem.



Based on the questions given below, if we know that server **be21-77.be.udel.edu** is in the same network as be21-79.be.udel.edu, we can ping **be21-77.be.udel.edu.**

Screenshot above shoes that ping to **be21-77.be.udel.edu** is successful.

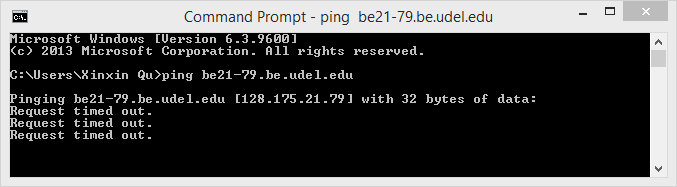


Traceroute to **be21-77.be.udel.edu** is also complete. So we can say it is not a problem of route itself.

1. Finally, the destination host may be **blocking ICMP packets**. Or, the destination host may **not exist on the network**. It could be disconnected, or turned off.  
   – That leaves us to only one possibility, which is the destination may be blocking ICMP packets. Or, the destination host may not exist on the network. It could be disconnected, or turned off.

To summarize and answer the questions:

1. What is the IP address of this destination host? Is there a DNS problem? Why?



The IP address of destination is 128.175.21.79.

There is no DNS problem as the IP address is looked up successfully.

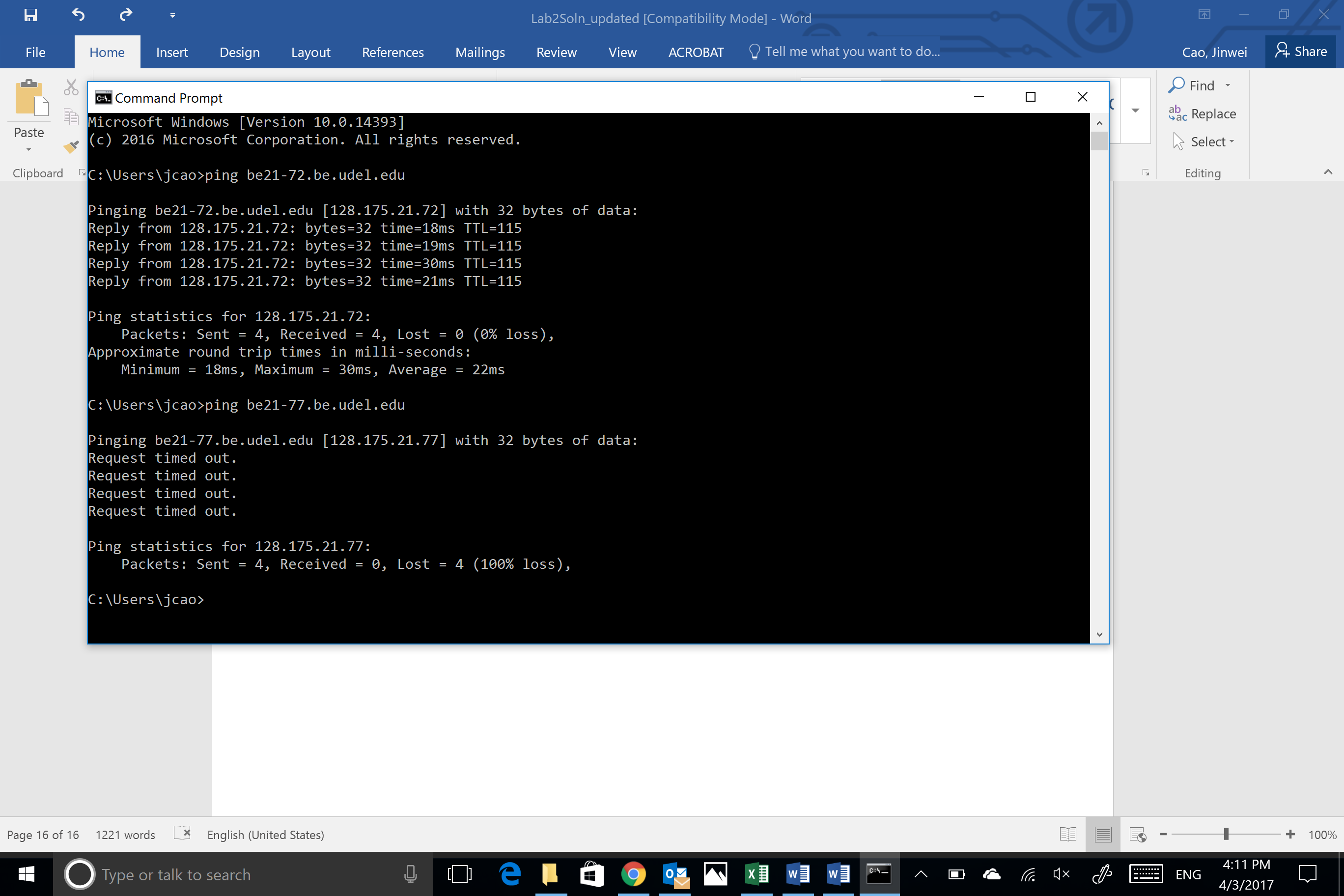
1. Are there any problems with your local computer? Why?

No. Because the computer identifies and connects to the local host IP.

1. Are there any problems with your local network? Why?

No. Because the computer connects to the default gateway successfully.

1. You know that the server “**be21-72.be.udel.edu**” is in the same network as the destination host. Based on this information, can you find out the possible problems with this destination host? Specify these possible problems.



The local computer can connect to **be21-72.be.udel.edu**. But it cannot connect to **be21-79.be.udel.edu.** Since both servers are in the same network, it is not a problem with the route. The problem has to be in the server **be21-79.be.udel.edu.** The possible problems are:

a. Server is temporarily disabled

b. The server does not respond to ICMP requests

In general, the destination host may be **blocking ICMP packets**. Or, the destination host may **not exist on the network**. It could be disconnected, or turned off.