# Part 1:

You should hand in a screenshot of the Command Prompt window similar to Figure 1 above. Save the displayed packet(s) and answer the following questions.

Answer the following questions:

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

**Host address:128.175.20.61**

**Destination address: 143.89.14.2**

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

**No. port number is used in transport layer, but ICMP is in internet layer**

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**

**Checksum fields, identifier, 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?

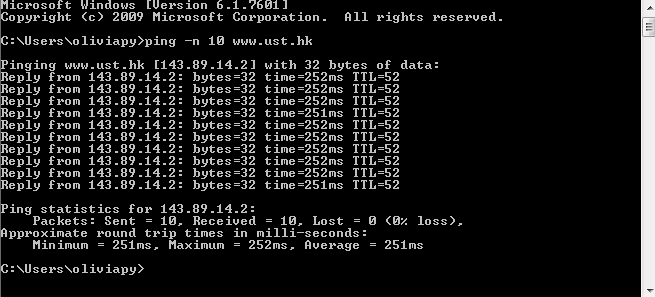
**Type:0**

**Code:0**

**Checksum fields, identifier fields, sequence number fields**

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?

**First RTT:0.252371**

**Yes, they are almost the same**

# Part 2:

You should hand in a screenshot of the Command Prompt window similar to Figure 4 above. Save the displayed packet(s) and answer the following questions.

Answer the following questions:

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

**Host address: 128.175.20.61**

**Destination address: 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?

**Yes. Because in the first part, the TTL is the TTL for the destination while in this part the TTL is adding up, until it equals the TTL for the destination.**

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?

**Ping request in error message (a copy of the original request, because it causes the error). It tells where the error comes from**

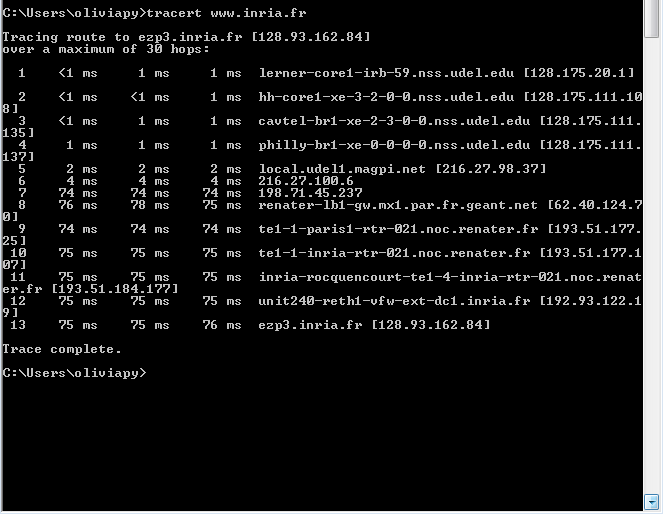
1. Examine the **last three** ICMP packets **received by the source** host. How are these packets different from the ICMP error packets? Why are they different?

**The color is different, and they don’t return error messages.**

**Because they have reached the destination so they don’t return 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?

**Yes. From the 7th on, the delays are much longer than previous ones.**

**Yes, the two routers on the end of this link should be in France because the TLD server is “fr”.**

# Part 3:

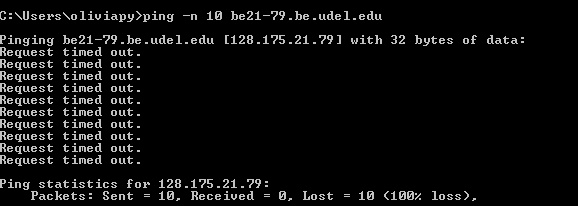
For this part of the lab, you should hand in the screenshot(s) of the Command Prompt window that display the steps you performed in this troubleshooting process.

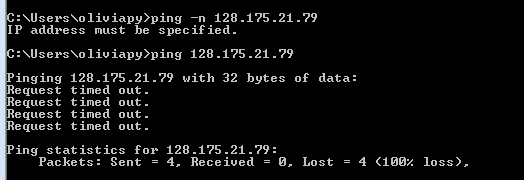
Answer the following questions:

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

**128.175.21.79**

**No because it still doesn’t work when you type in ping 128.175.21.79 directly**

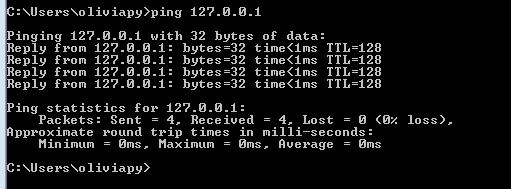




1. Are there any problems with your local computer? Why?

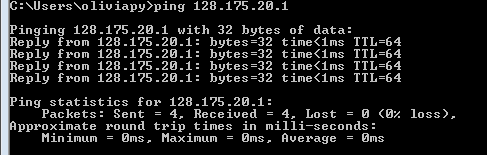
**No because the Wi-Fi is on and it works when you type in ping 127.0.0.1**





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

**No. because it works when you ping the default gateway**



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.

**I think the destination host may be blocking ICMP packets, or the destination host may not exist on the network. Because when I ping udel.edu, it works, so there is no routing problem and the destination network is reachable. But we need to contact the people who is taking charge of the destination host to find out, which is impossible for me ☹**

