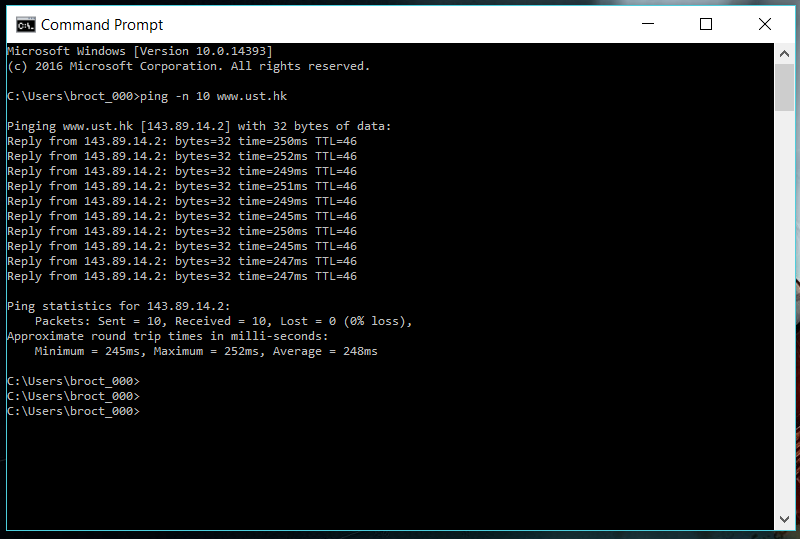
Broc Nickodemus

Lab4b



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

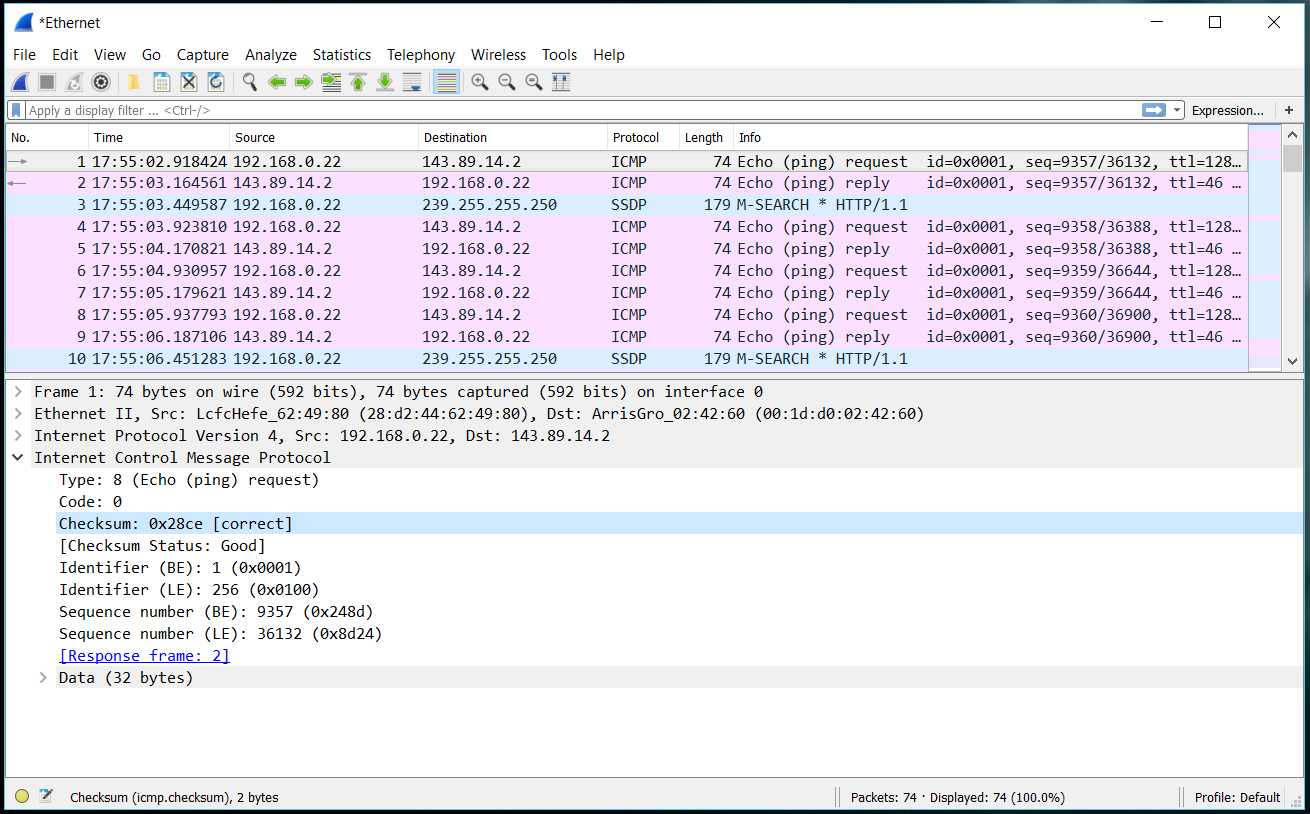
The IP of my host is 192.168.0.22 the IP of the destination is 143.89.14.2

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

An ICMP packet does not have a source and a destination port because it communicates through hosts and router.

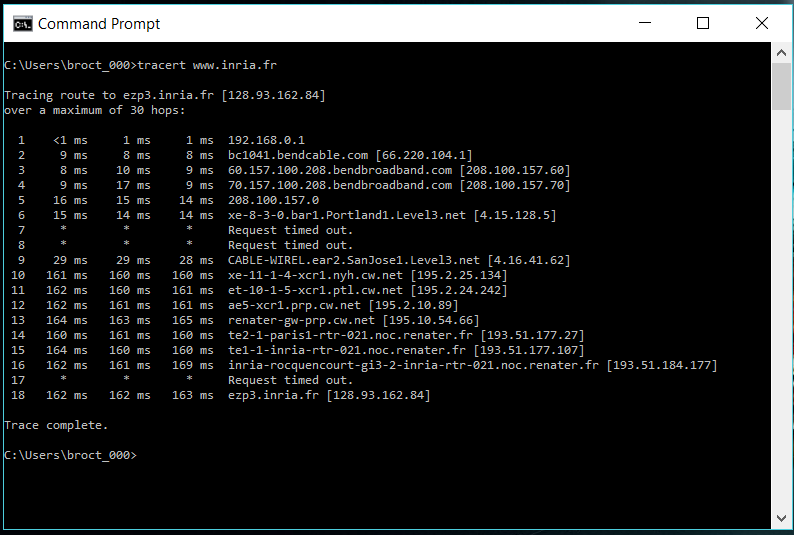
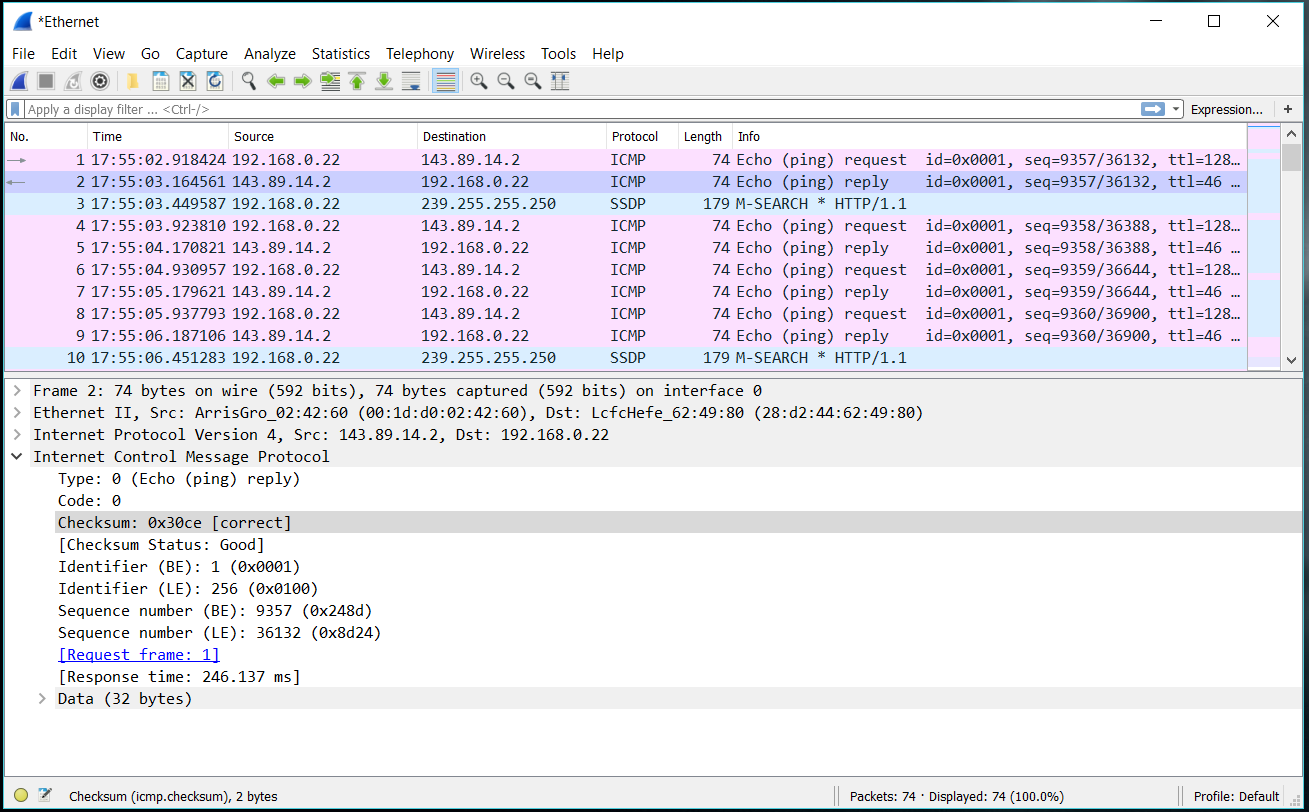
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

The ICMP is type 8 and the code number is 0. The ICMP also has a checksum, identifier, sequence number, and data fields. The checksum and sequence number have 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?

The ICMP is type 0 and the code number is 0. The ICMP also has a checksum, identifier, sequence number, and data fields. The checksum and sequence number have 2 bytes.



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

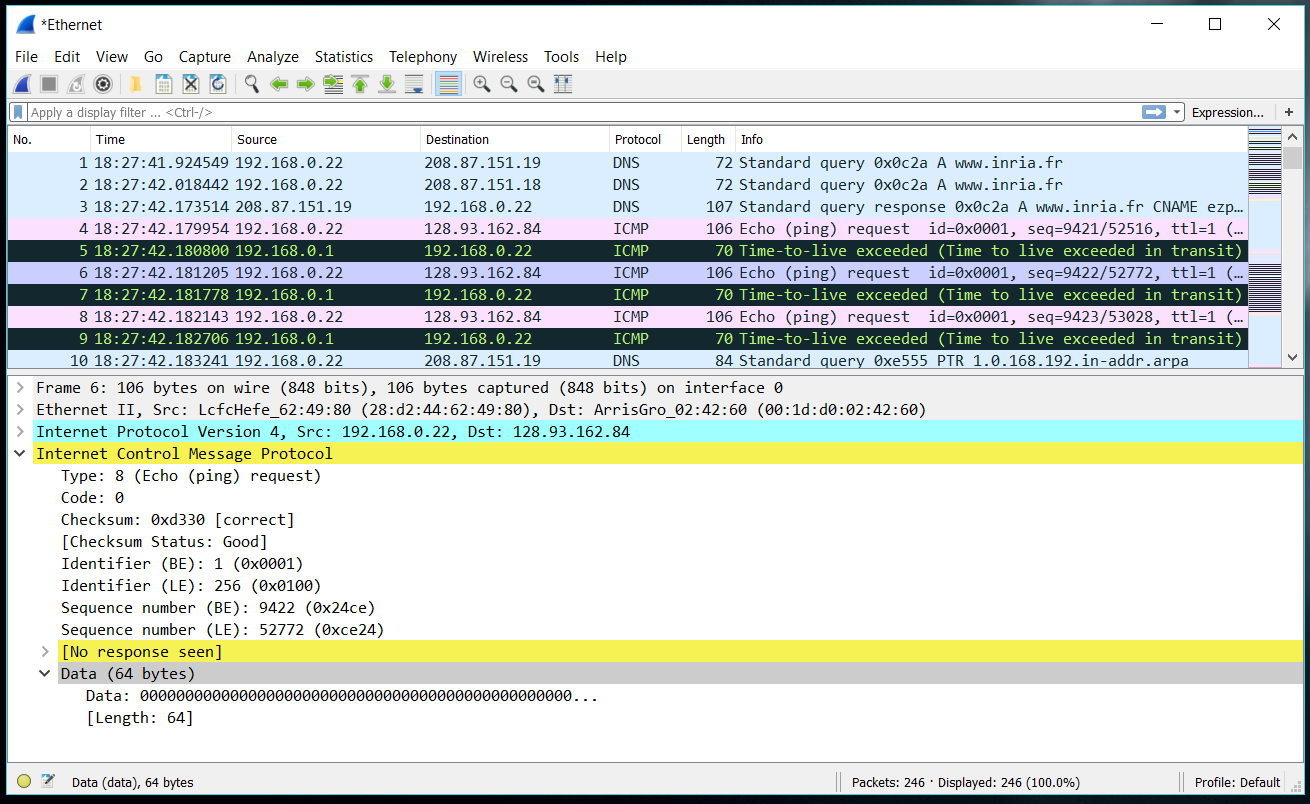
The IP of my host is 192.168.0.22 the IP of the destination is 128.93.162.84

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?

No, the IP protocol of ICMP is 0x11

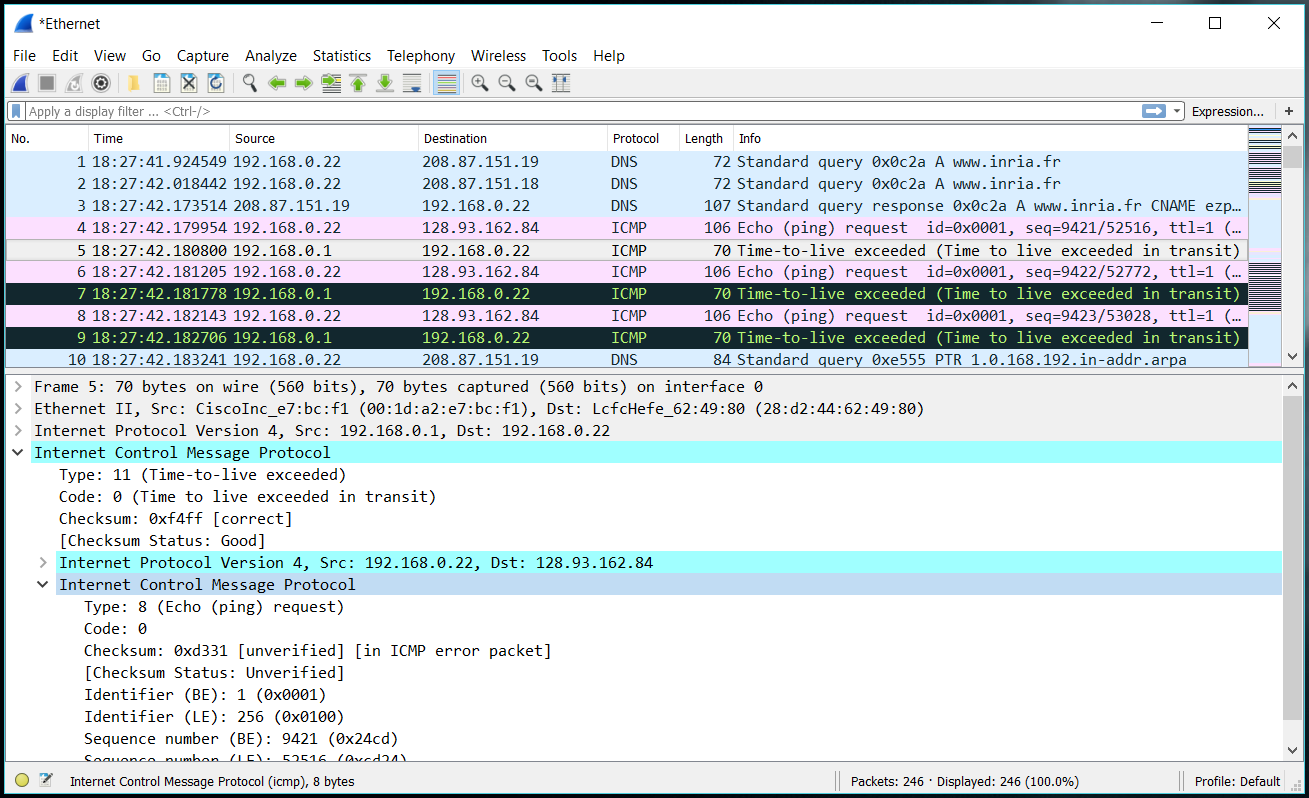
7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

The ICMP echo packet has the same fields as the ping



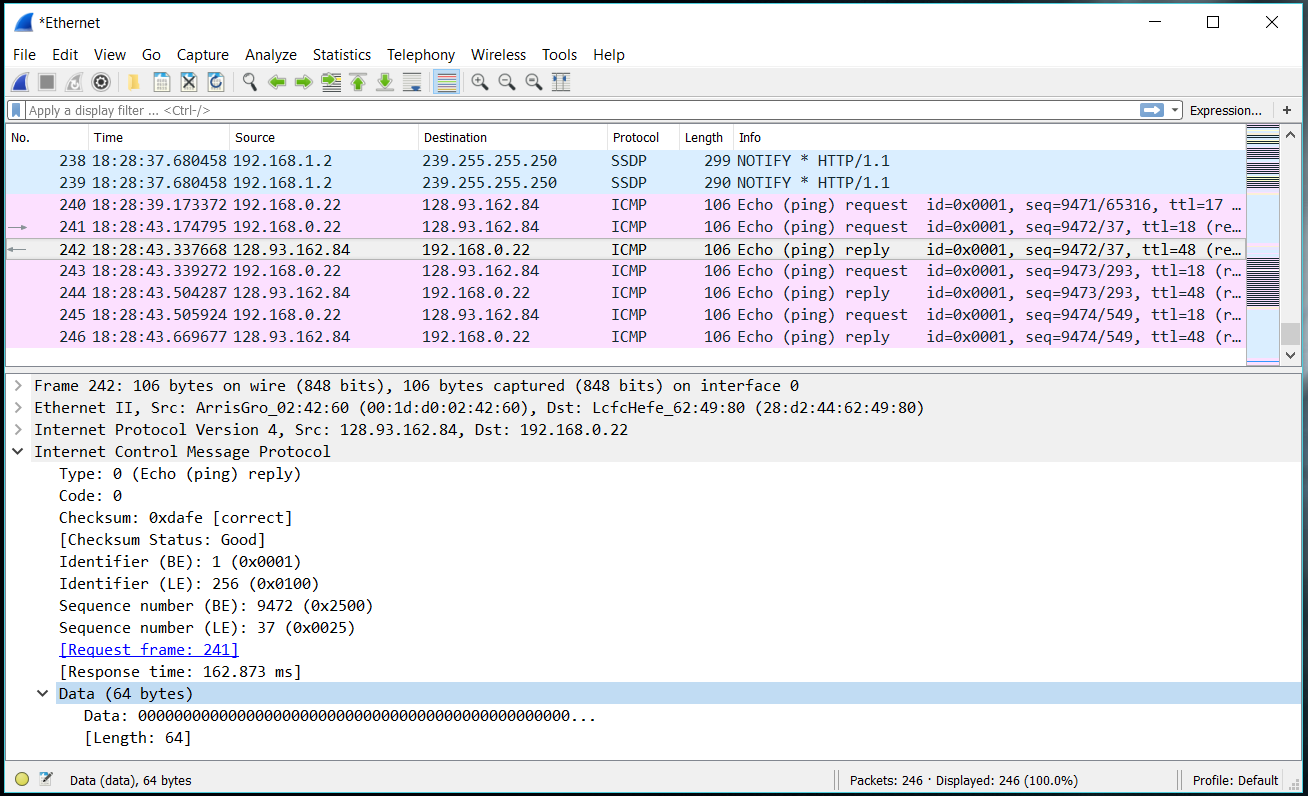
8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

The ICMP error packet is not the same as the ping packet. It has the IP header and the first 8 bytes the error is for.

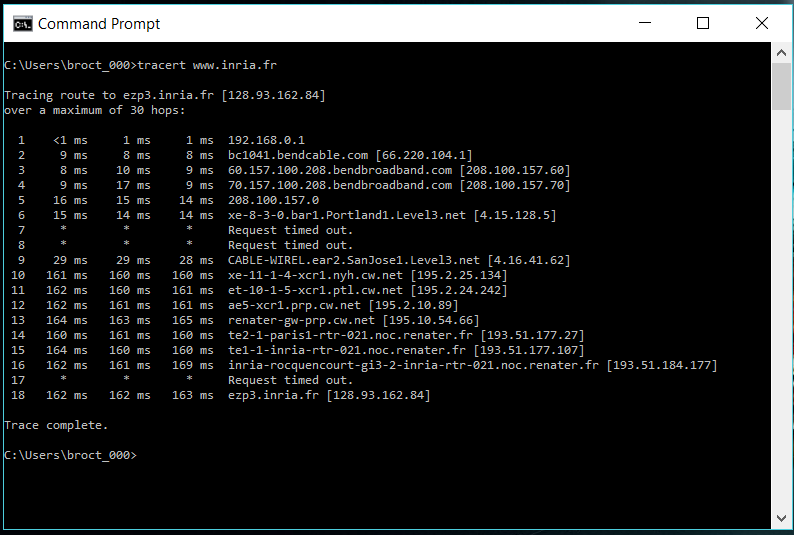


9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

The last three ICMP packets have type 0 rather than 11. They are different because they made it to the host destination 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?



Steps 9 to 10 have a longer delay. This delay is from SanJose, California to cw (Curacao). In figure 4 the link is from New York City to Pastourelle, France.

Answer the following questions:

~~3. Extra Credit~~ (I don’t have the time)

For one of the programming assignments you created a UDP client ping program. This ping program, unlike the standard ping program, sends UDP probe packets rather than ICMP probe packets. Use the client program to send a UDP packet with an unusual destination port number to some live host. At the same time, use Wireshark to capture any response from the target host. Provide a Wireshark screenshot for the response as well as an analysis of the response.