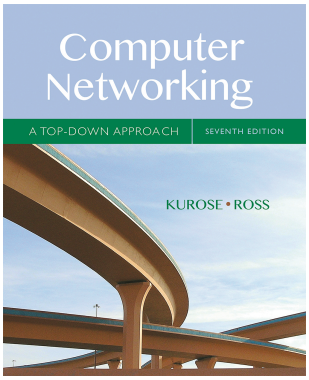
Wireshark Lab: ICMP
SOLUTION



Supplement to *Computer Networking: A Top-Down Approach, 7th ed.,* J.F. Kurose and K.W. Ross

---

The solutions below are based on the trace files *ICMP-ethereal-trace-1 and ICMP-ethereal-trace-2* in the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip .

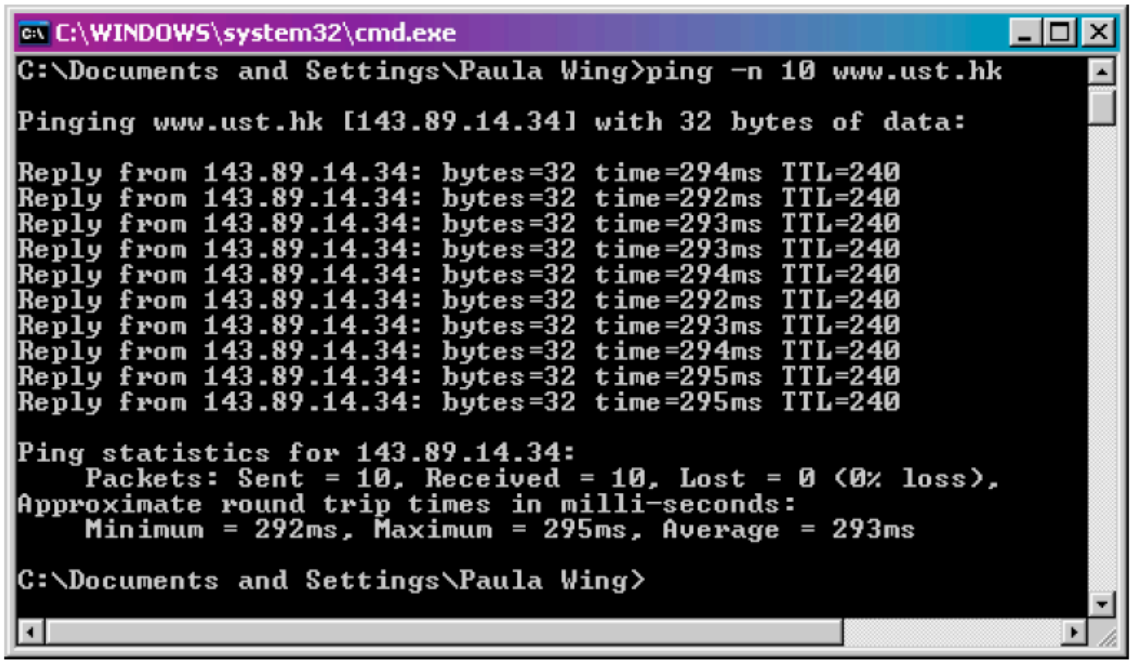


Figure 1: Screenshot after the PING request

1. What is the IP address of your host? What is the IP address of the destination host? ***ANSWER:*** *The IP address of my host is 192.168.1.101. The IP address of the destination host is 143.89.14.34.*
2. Why is it that an ICMP packet does not have source and destination port numbers? ***ANSWER:*** *The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the*

specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

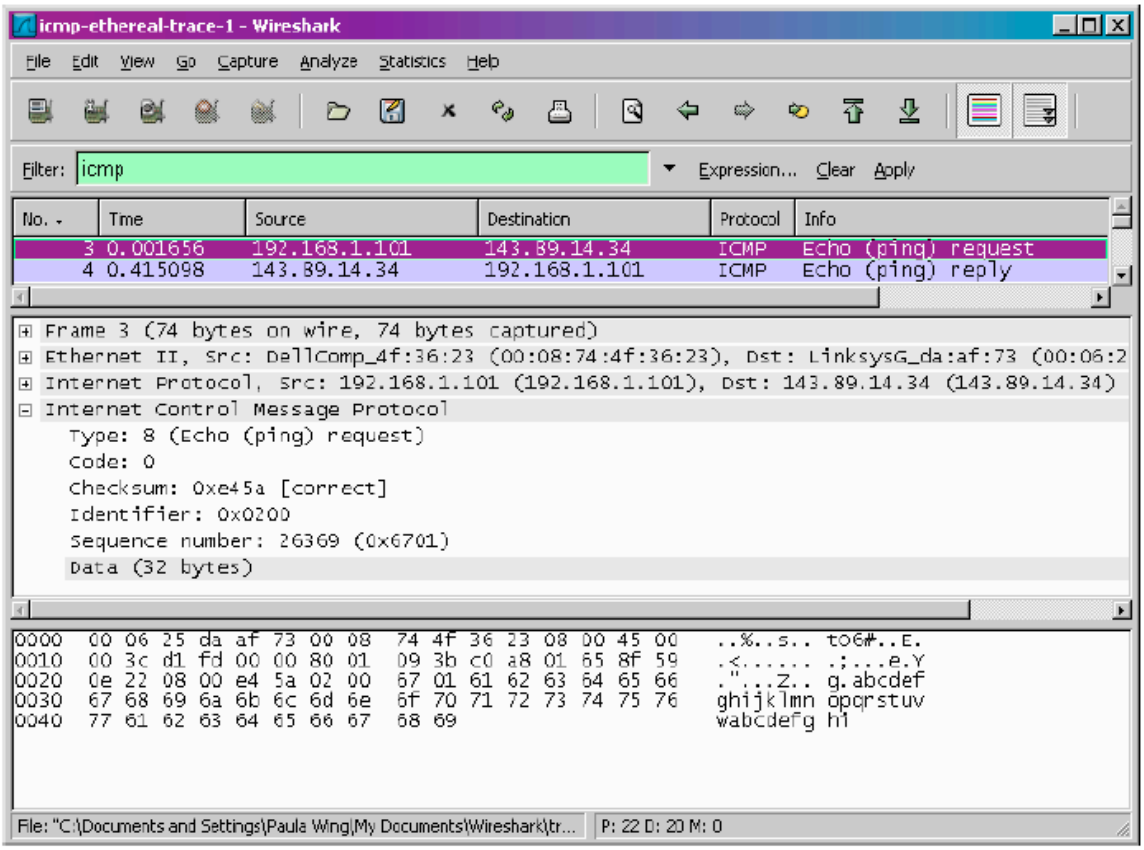


Figure 2: ICMP Echo Request message

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? ***ANSWER:*** *The ICMP type is 8, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.*

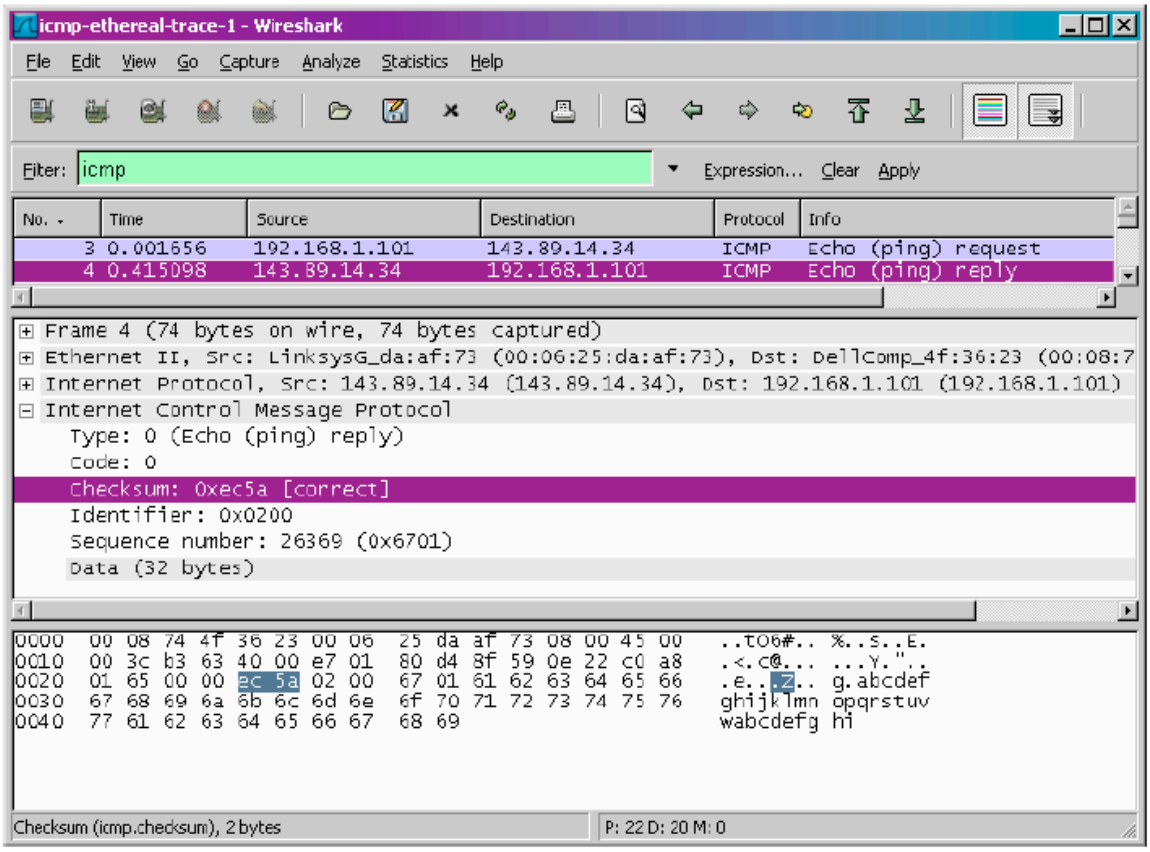


Figure 3: ICMP ECHO REPLY message

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? ***ANSWER:*** *The ICMP type is 0, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. 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? ***ANSWER:*** *The IP address of my host is 192.168.1.101. The IP address of the destination host is 138.96.146.2.*

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? ***ANSWER:*** *No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11.*

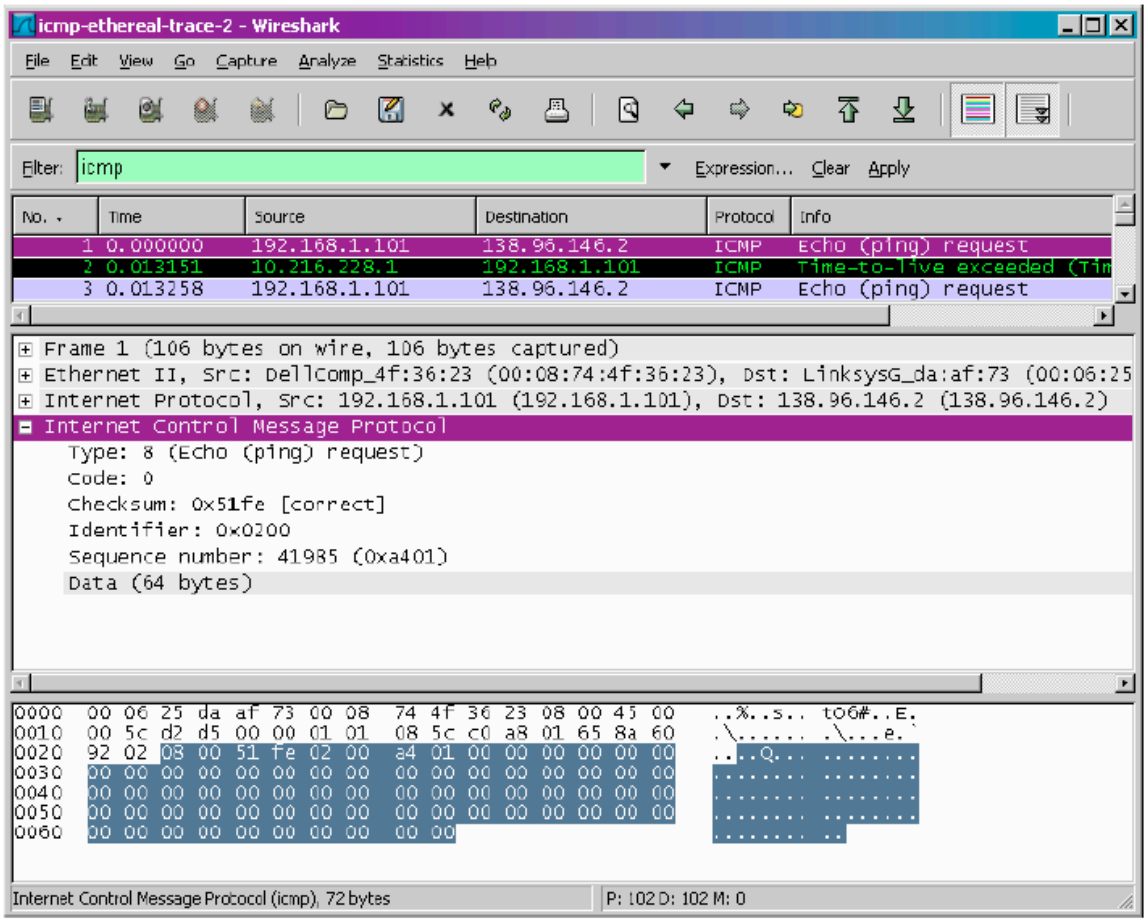


Figure 4: ICMP ECHO REQUEST message

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? ***ANSWER:*** *The ICMP echo packet has the same fields as the ping query packets.*

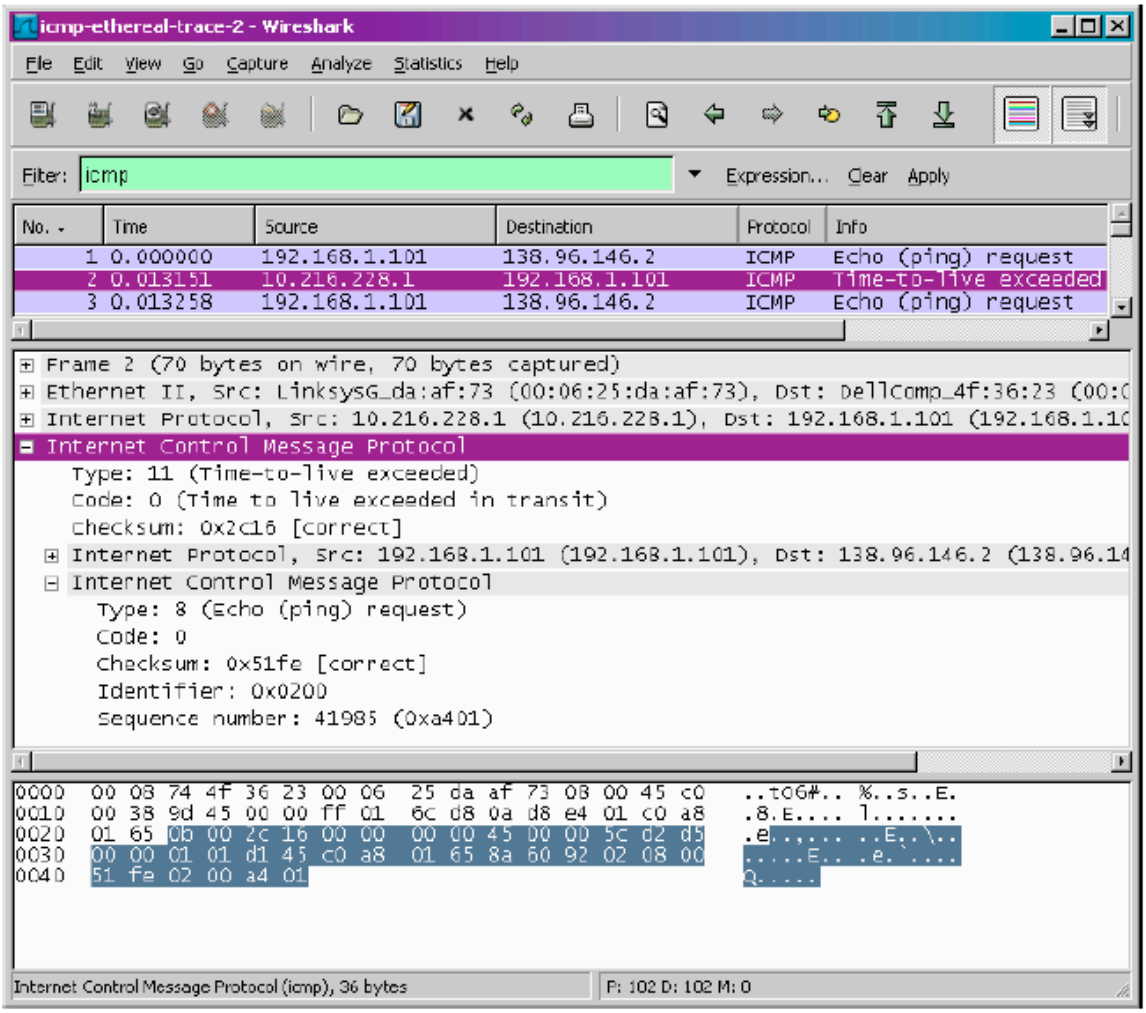


Figure 5: ICMP ERROR message

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

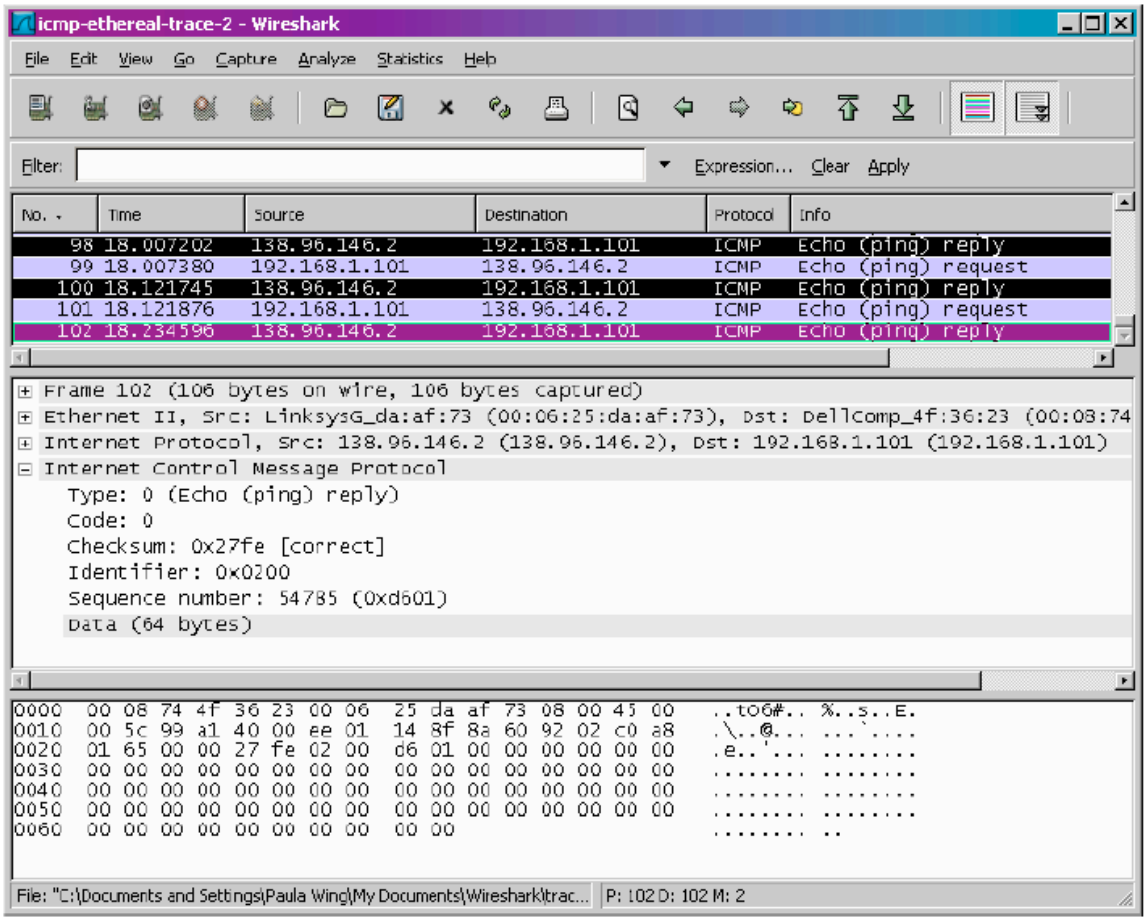


Figure 6: Last three ICMP packets

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?
   ANSWER: *The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.*

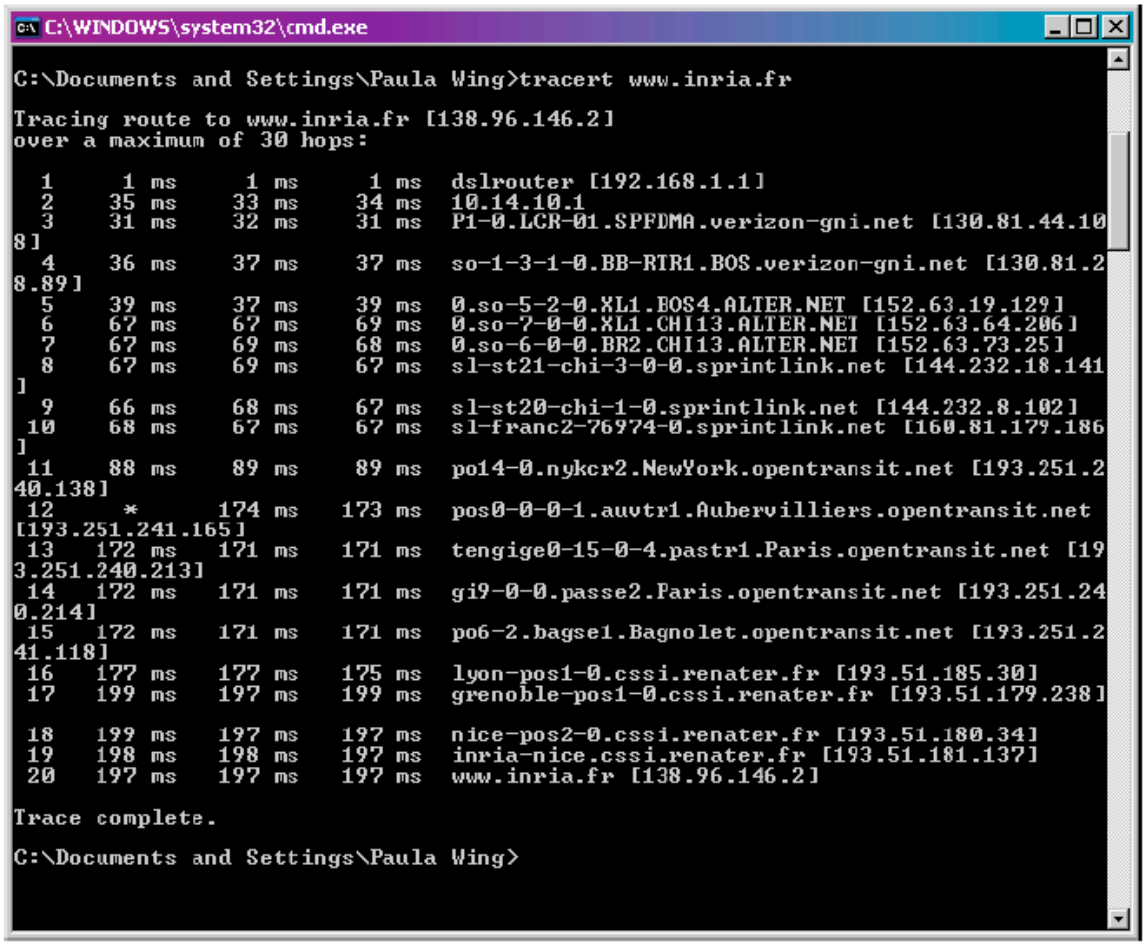


Figure 7: Command prompt for traceroute

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? ***ANSWER:*** *There is a link between steps 11 and 12 that has a significantly longer delay. This is a transatlantic link from New York to Aubervilliers, France. In figure 4 from the lab, the link is from New York to Pastourelle, France.*