Wireshark Lab 7

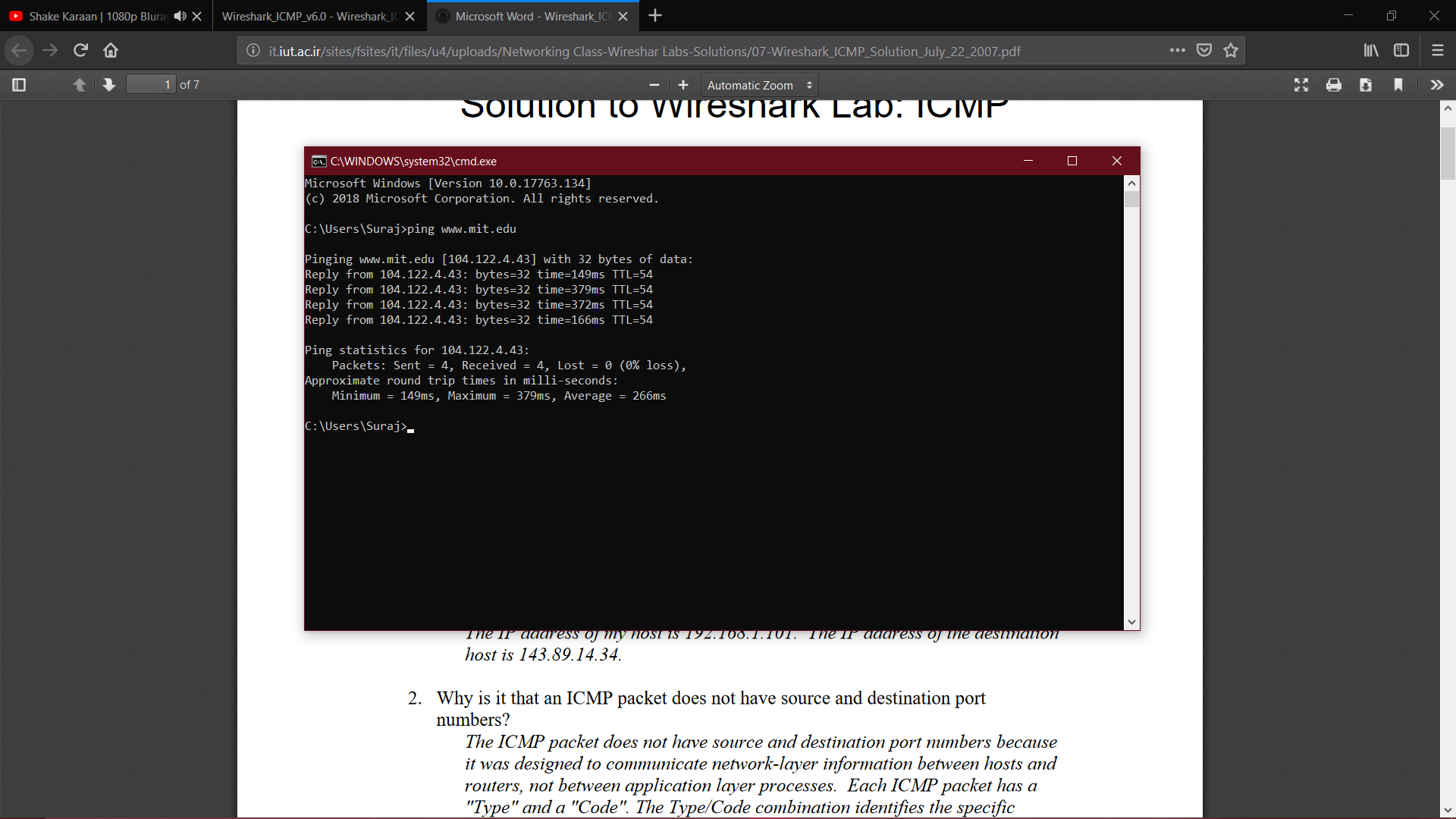
ICMP

Suraj Durgesht

(16EC06)

Instructor: Dr. Rajendra Hegadi

ICMP and Ping



Que1. What is the IP address of your host? What is the IP address of the destination host?

Solution:

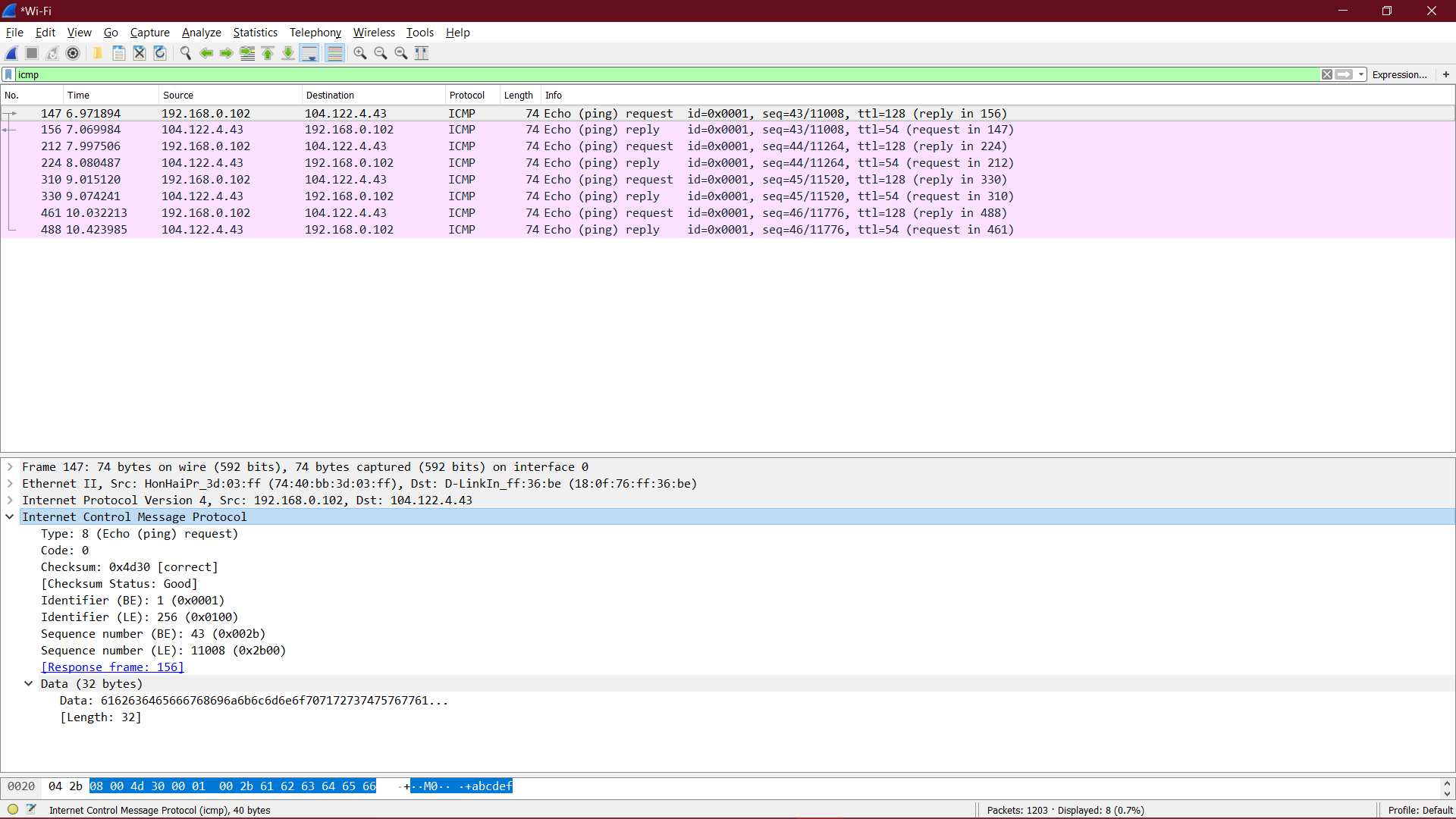
The IP address of my host is 192.168.0.102.

The IP address of the destination host is [104.122.4.43].

Que2. Why is it that an ICMP packet does not have source and destination port numbers?

Solution:

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.



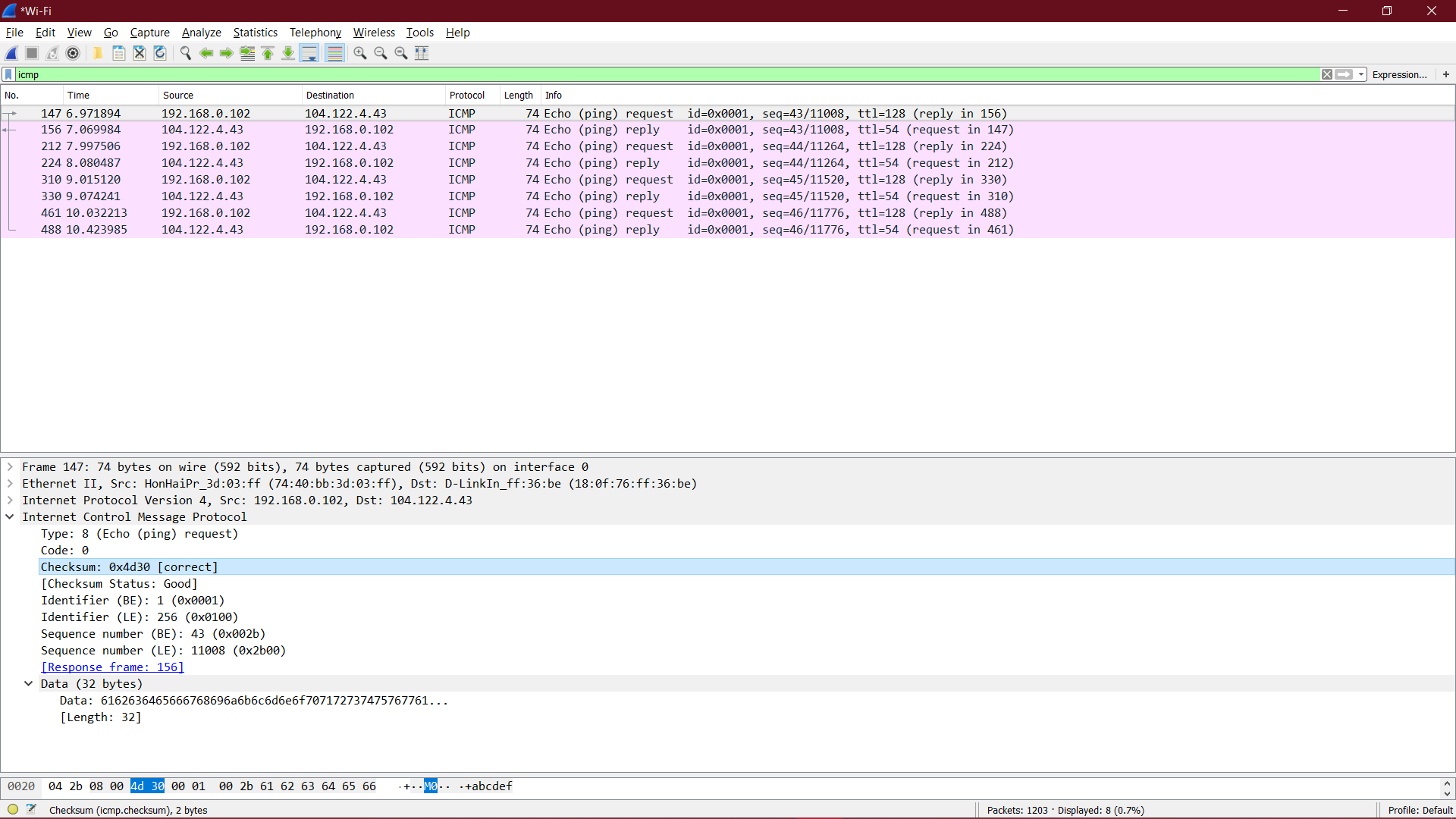
Que3. Examine one of the ping request packets sent by your host. What are the ICMP

type and code numbers? What other fields does this ICMP packet have? How

many bytes are the checksum, sequence number and identifier fields?

Solution:

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.



Que4. 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?

Solution:

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.

ICMP and Traceroute

Que5. What is the IP address of your host? What is the IP address of the target destination host?

Solution:

The IP address of my host is 192.168.0.102.

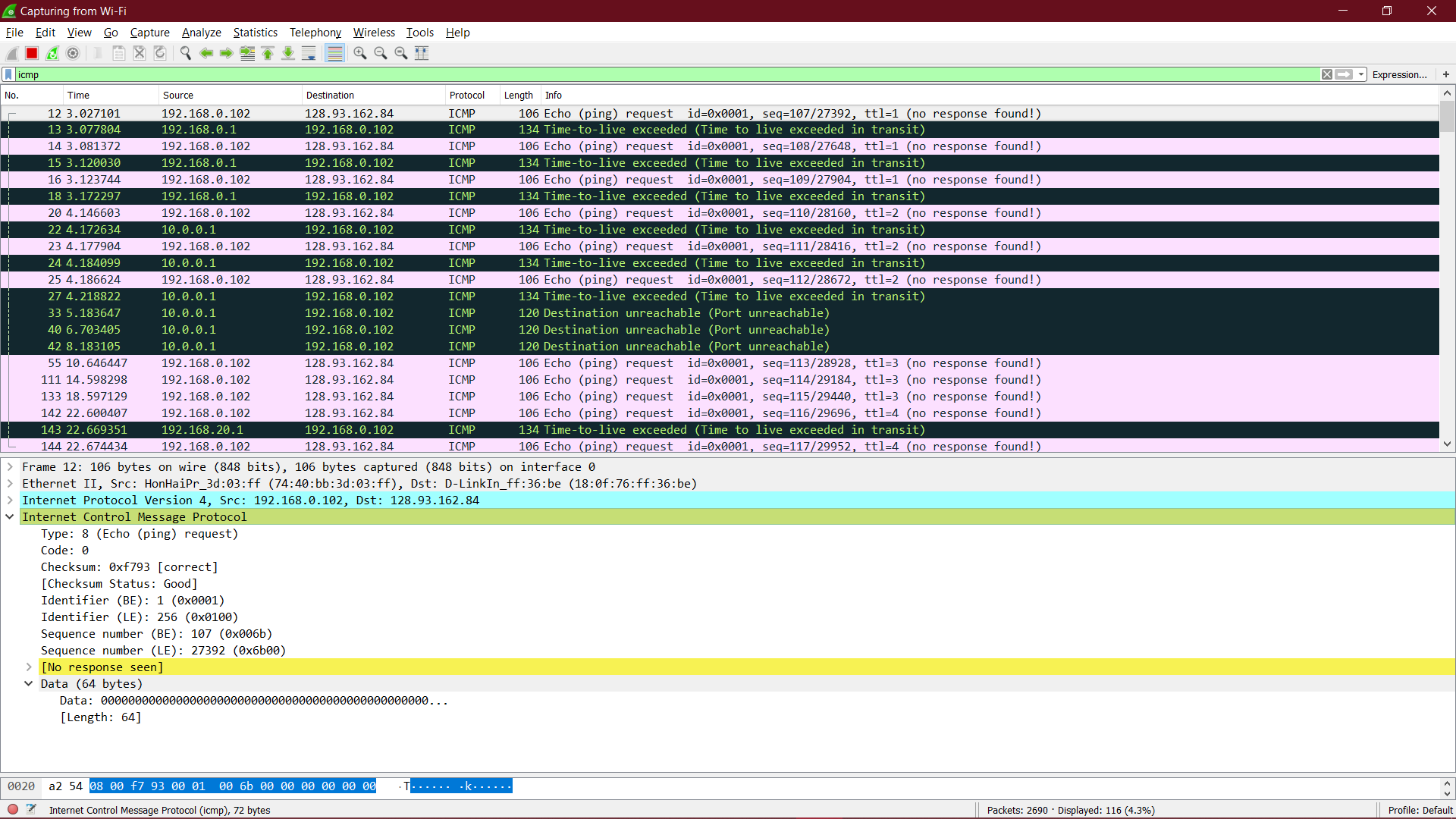
The IP address of the destination host is [128.93.162.84]

Que6. 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?

Solution:

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

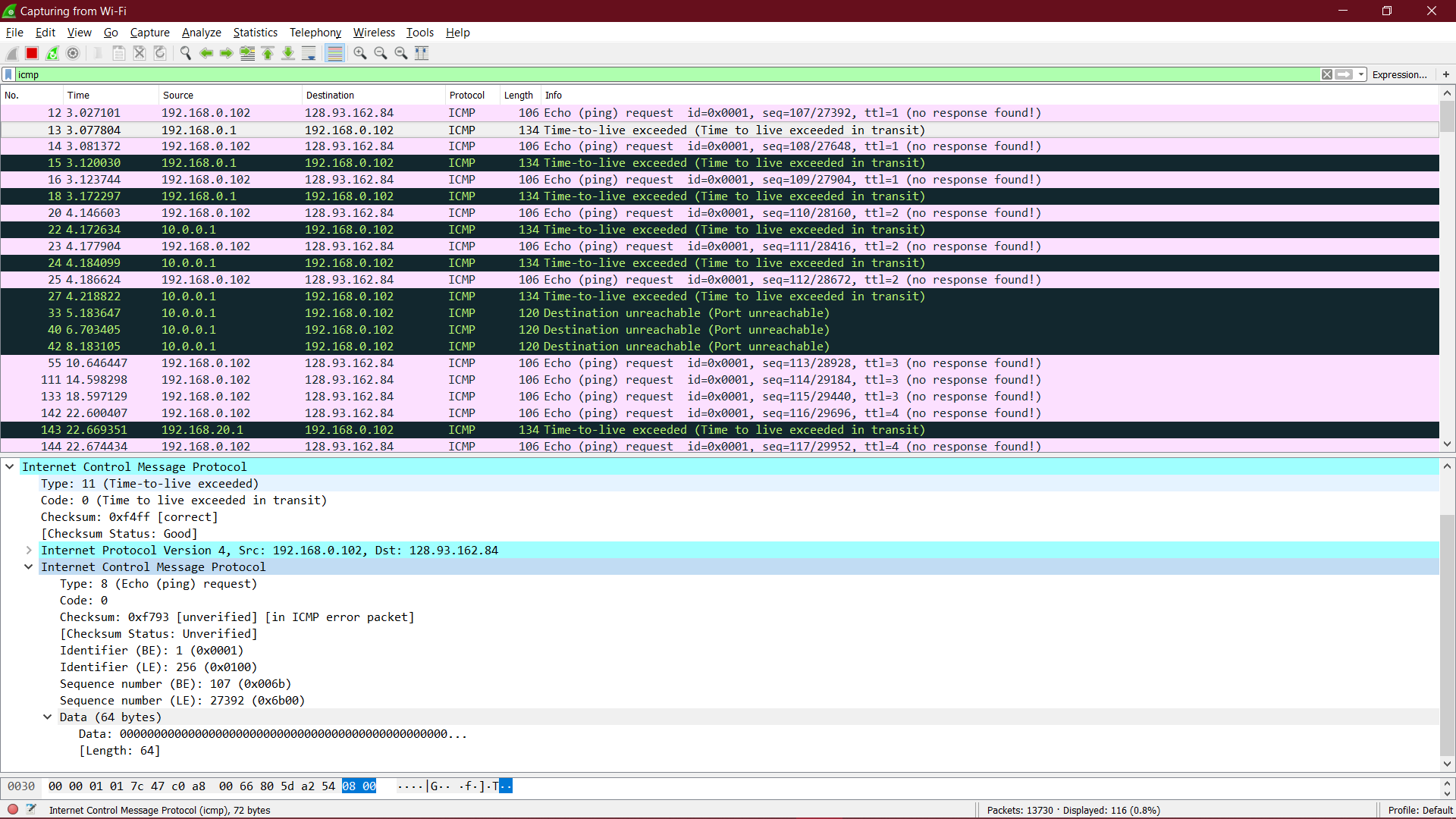


Que7. Examine the ICMP echo packet in your screenshot. Is this different from the

ICMP ping query packets in the first half of this lab? If yes, how so?

Solution:

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

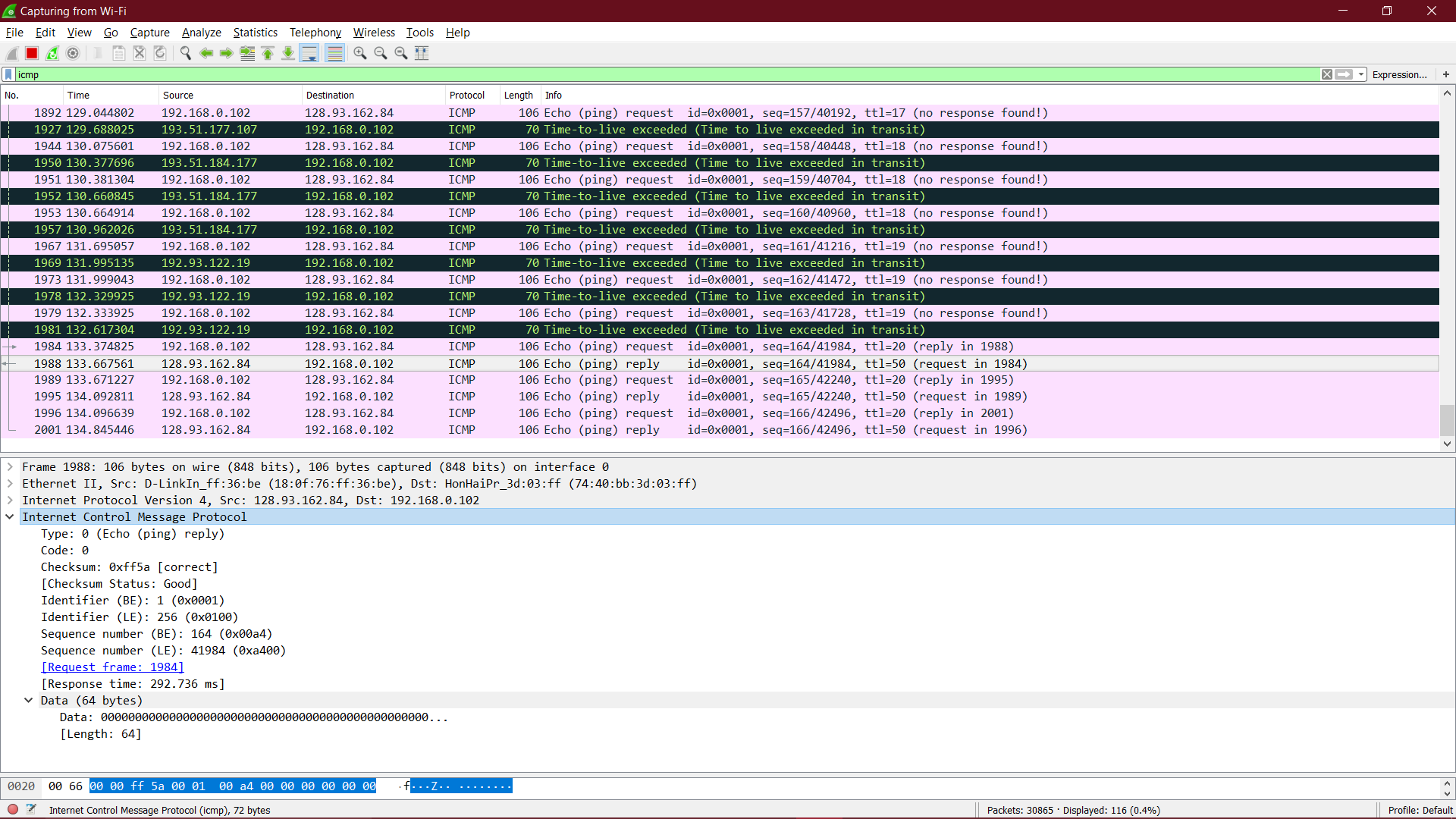


Que8. Examine the ICMP error packet in your screenshot. It has more fields than the

ICMP echo packet. What is included in those fields?

Solution:

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.

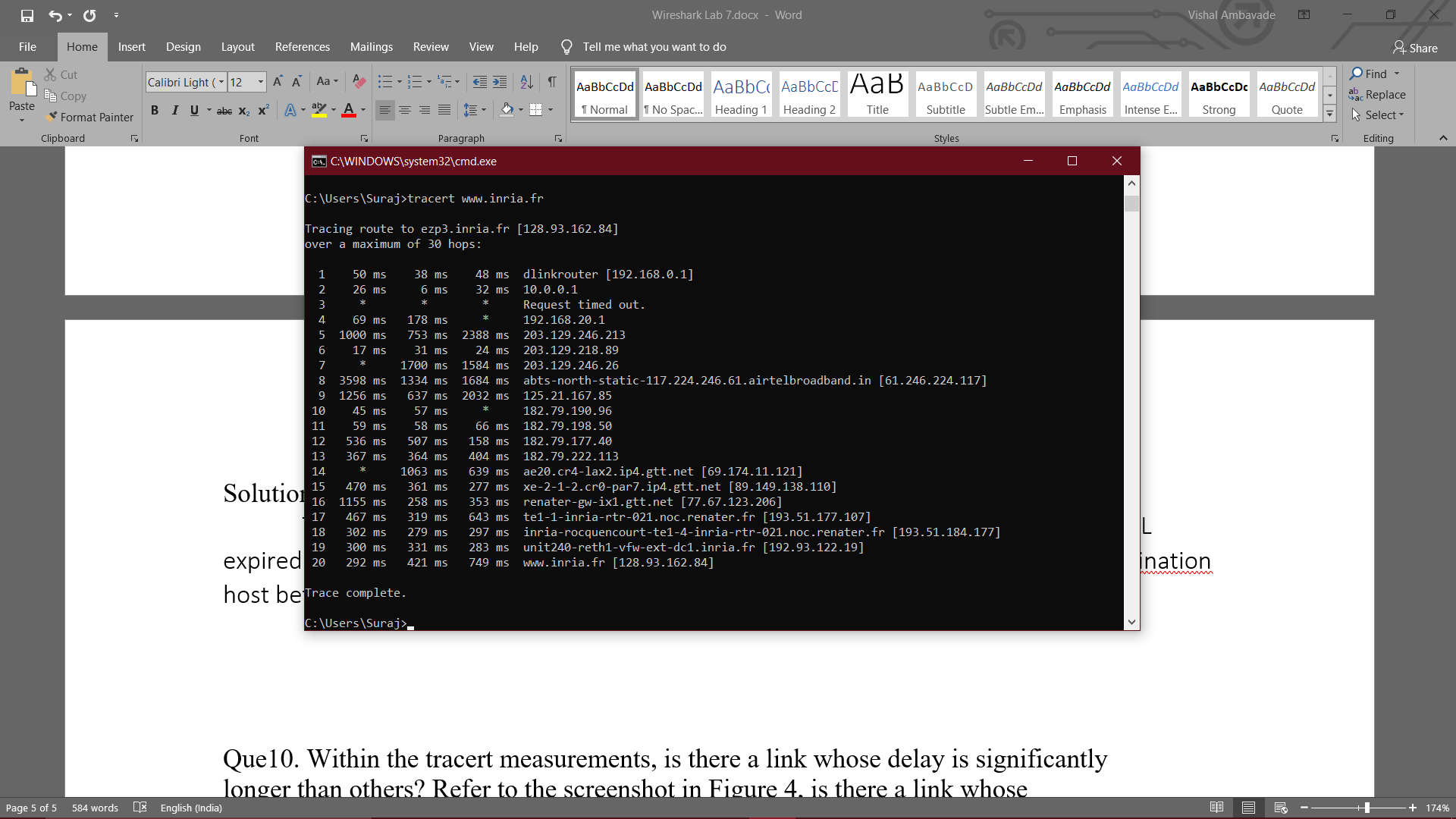


Que9. Examine the last three ICMP packets received by the source host. How are these

packets different from the ICMP error packets? Why are they different?

Solution:

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 estimation host before the TTL expired.



Que10. 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?

Solution:

There is a link between steps 8 and 9 that has a significantly longer delay. This is a transatlantic link from India to France. In figure, the link is from India to France.