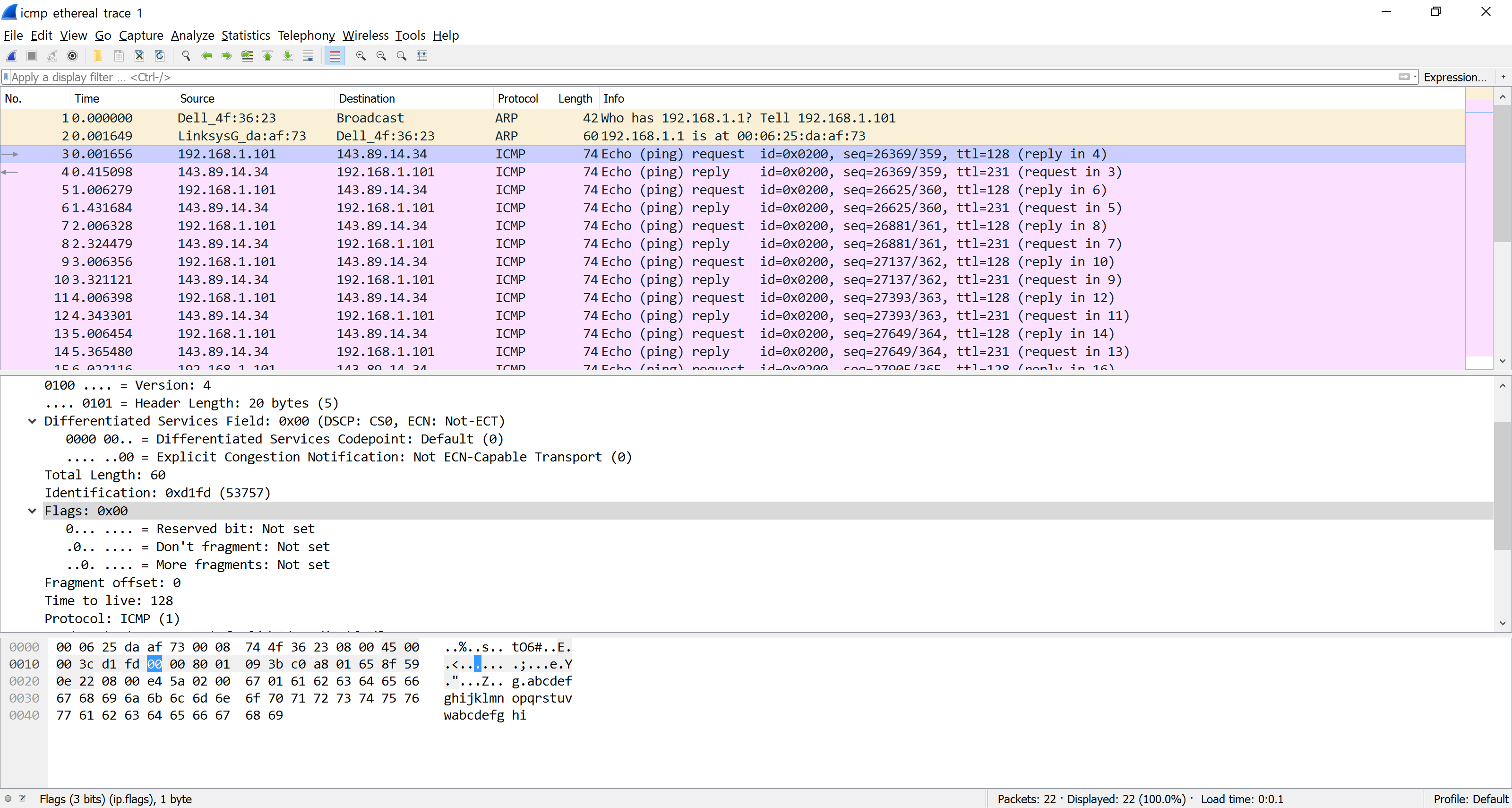
**Wireshark ICMP**

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

IP address of my host: 192.168.1.101

IP address of the destination host 143.89.14.34



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

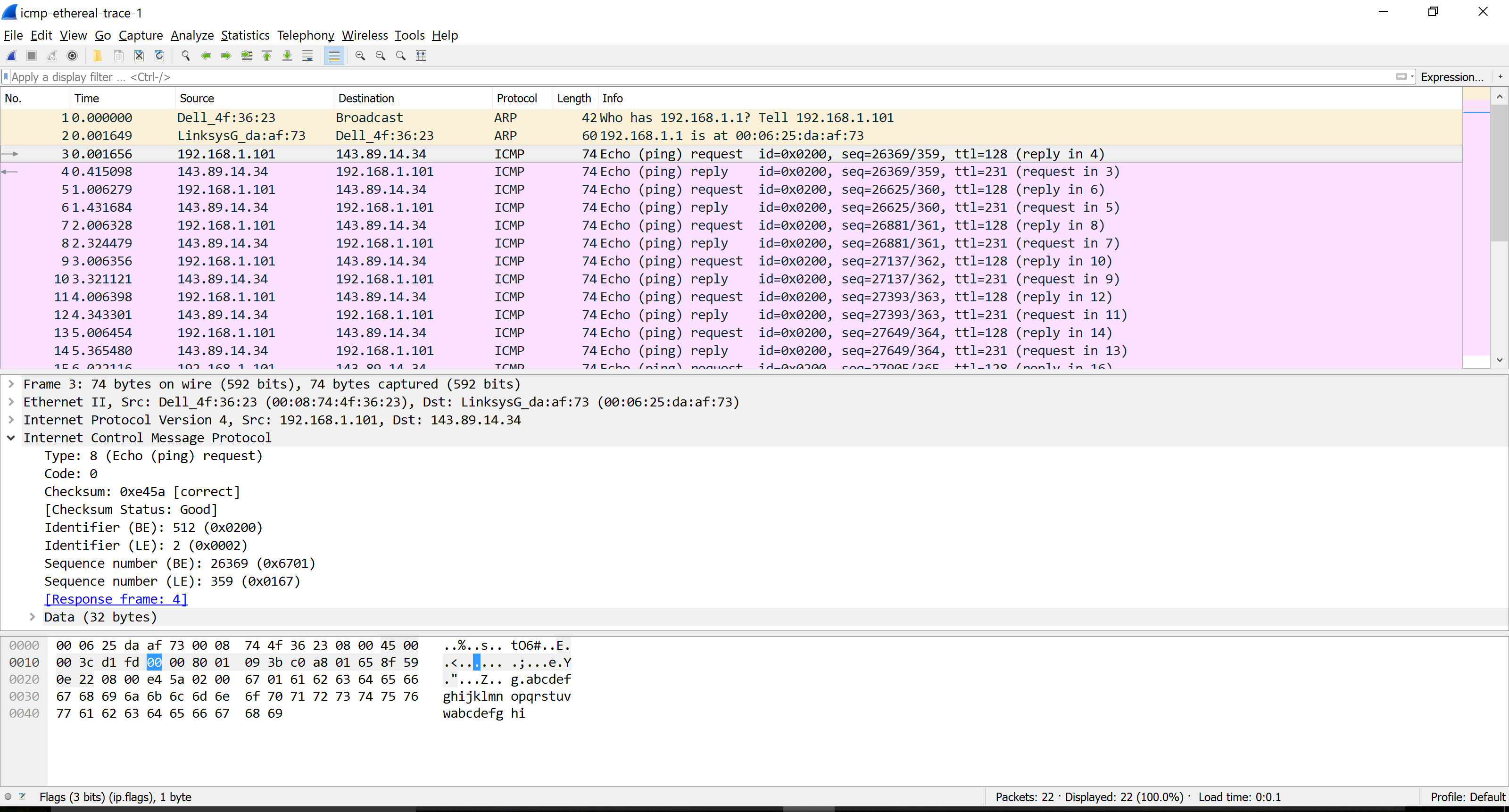
Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received.  
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

ICMP type: 8

ICMP code: 0

The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

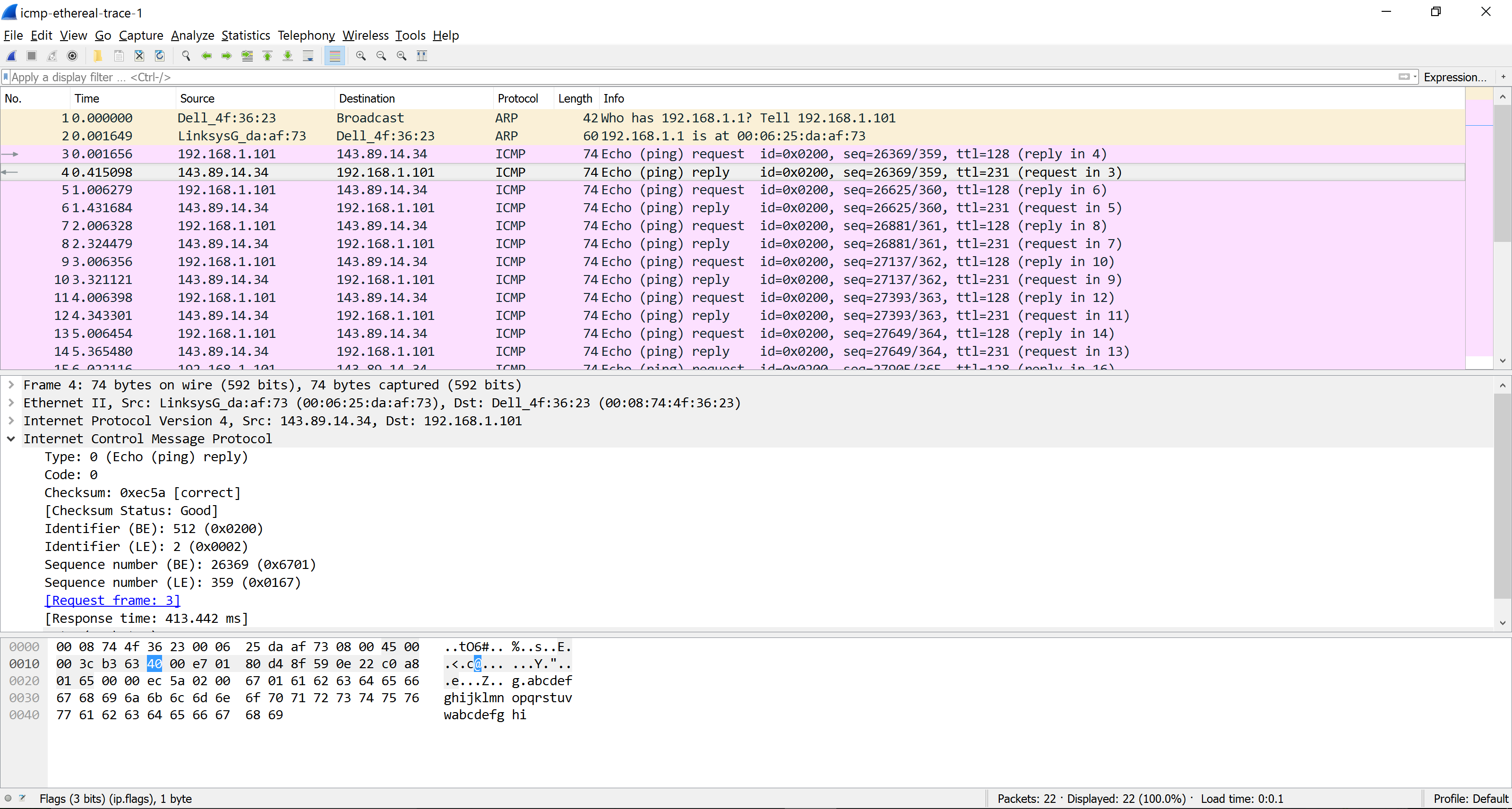
**4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**



ICMP type: 0

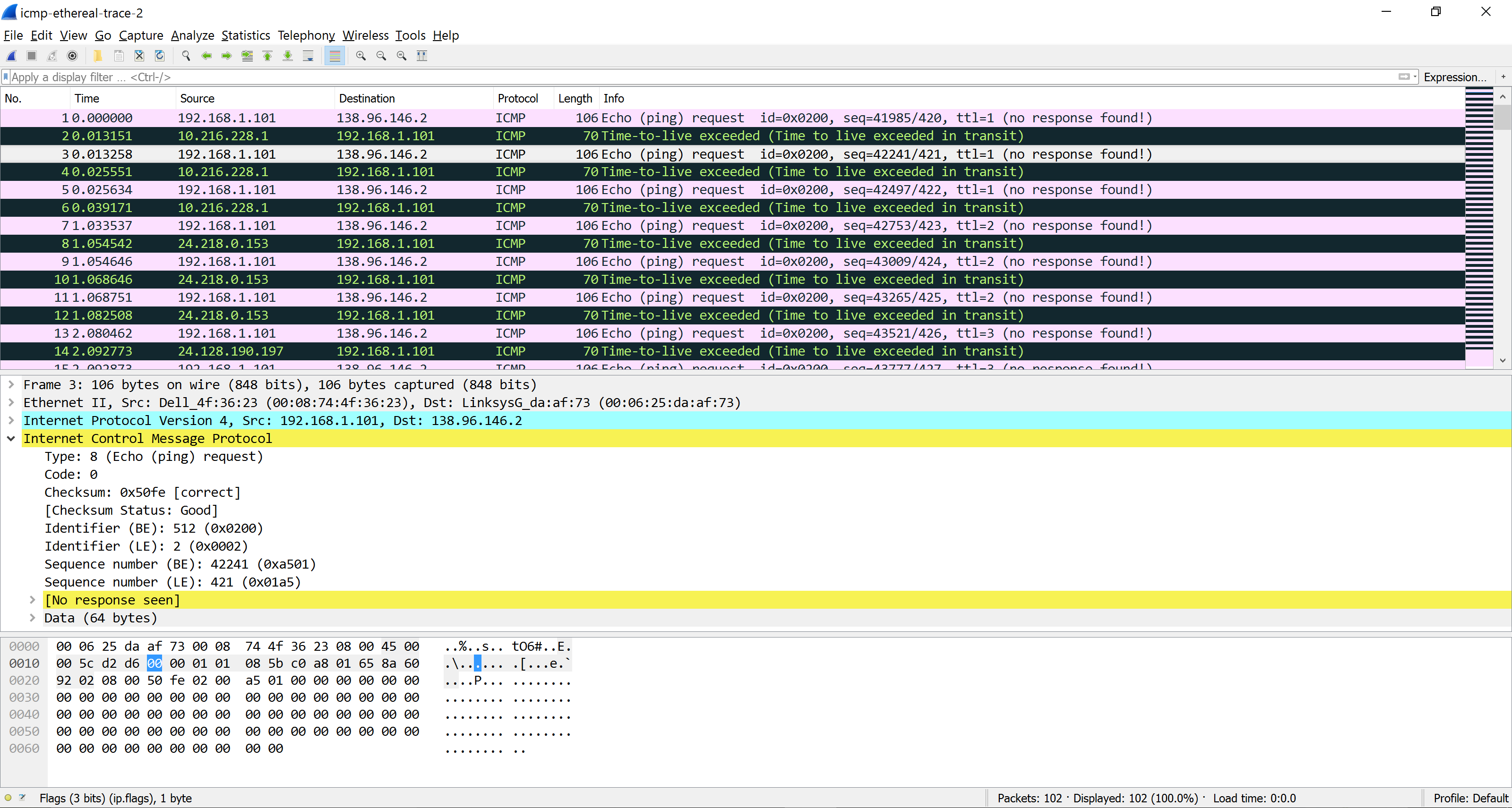
ICMP code: 0

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?**

The IP address of my host: 192.168.1.101.

The IP address of the destination host: 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?**

No. The IP protocol number should be 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?**

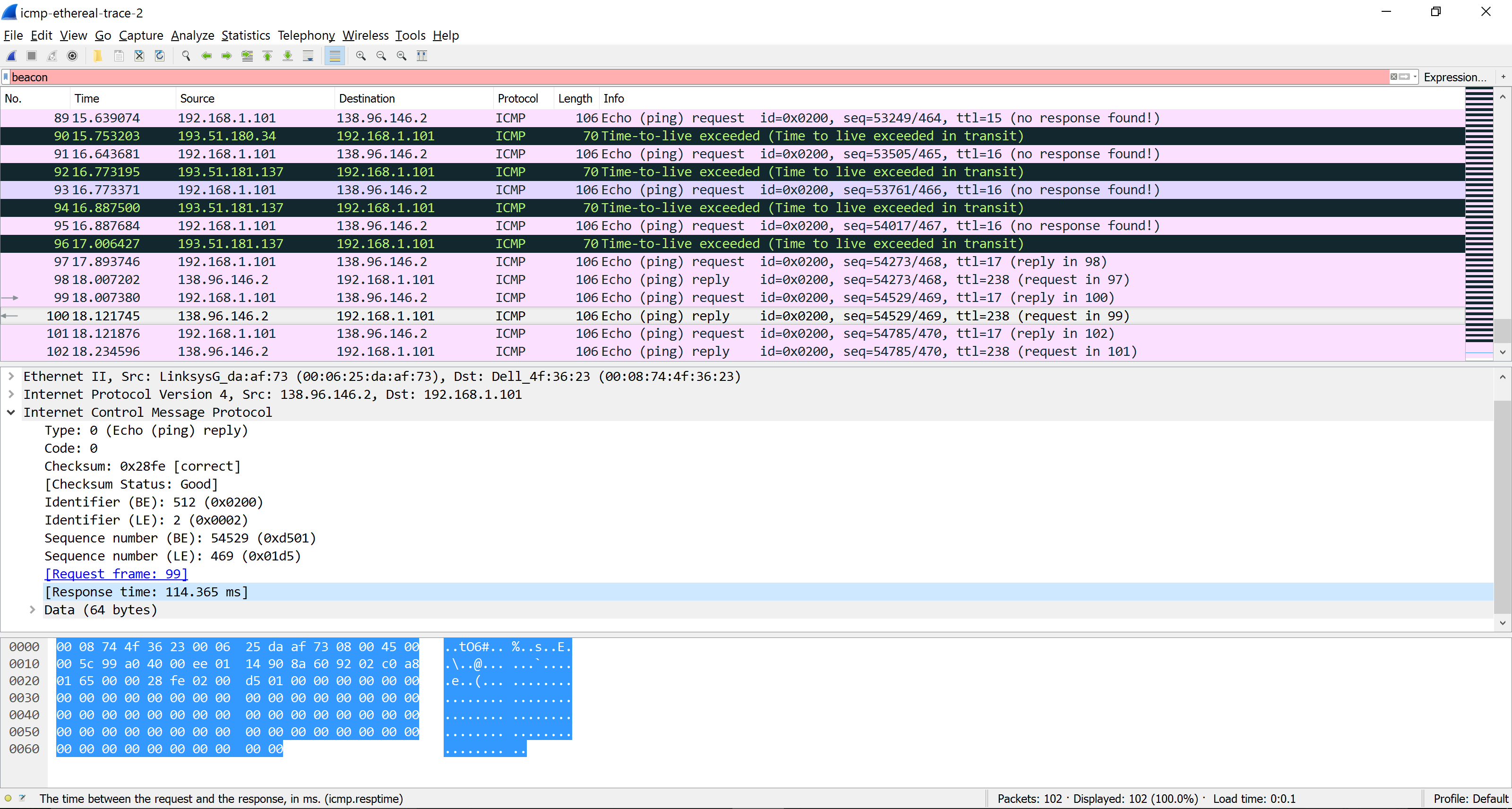
The ICMP echo packet has the same fields as the ping query packets.

**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 echo packet does not have the same fields as the ping query packets. It contains the IP header and the first 8 bytes of the original ICMP packet.

**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 packets have type 0 meaning echo reply not type 11 meaning TTL expires because the packets manage to the destination host before expiring.



**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?**

Step 11 and 12 lave longer delay. The routers is from New York to Aubervilliers, France. In figure 4 is from New York to Pastourelle, France.

