**Computer Network**

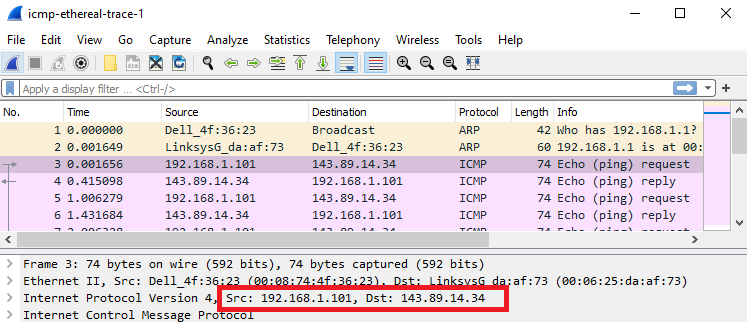
**Wireshark Lab 5: ICMP v8.0**

***Lecturer: Mr. Nguyễn Mạnh Thìn***

***Student: Trần Quốc Anh - 1852247***

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

* The IP address of my host: 192.168.1.101
* The IP address of destination host: 143.89.14.34

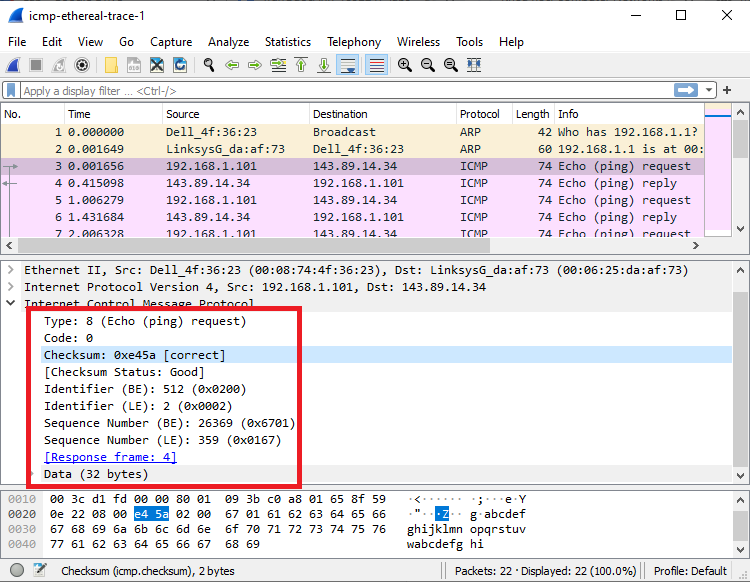
****

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

* An ICMP packet does not have source and destination port number because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. However, this is using a network layer so those are not needed.

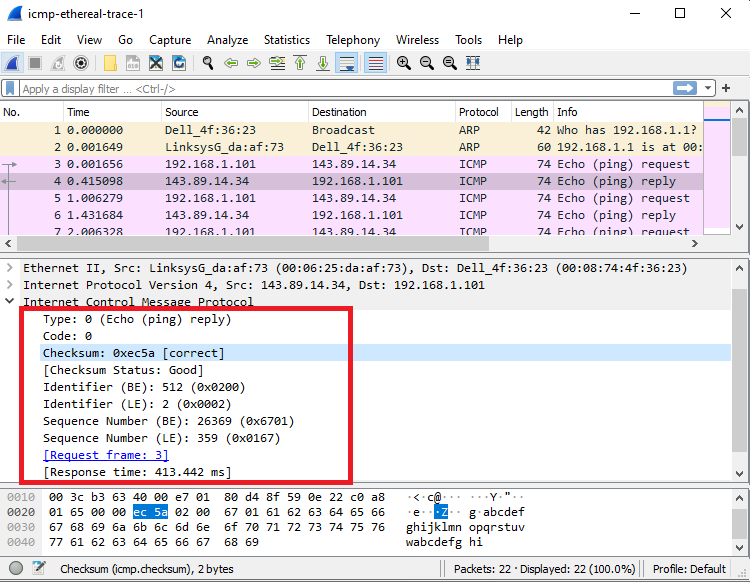
1. **Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

* The ICMP type: 8
* The ICMP code numbers: 0
* Other field: checksum, identifier, sequence number, and data fields
* The checksum, sequence number and identifier fields are two bytes each.

****

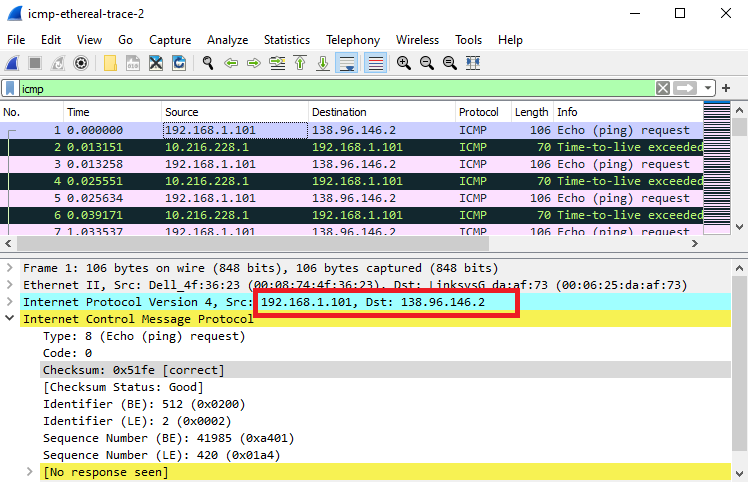
1. **Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

* The ICMP type: 0
* The ICMP code numbers: 0
* Other field: checksum, identifier, sequence number, and data fields
* The checksum, sequence number and identifier fields are two bytes each.

****

1. **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 destination host: 138.96.146.2

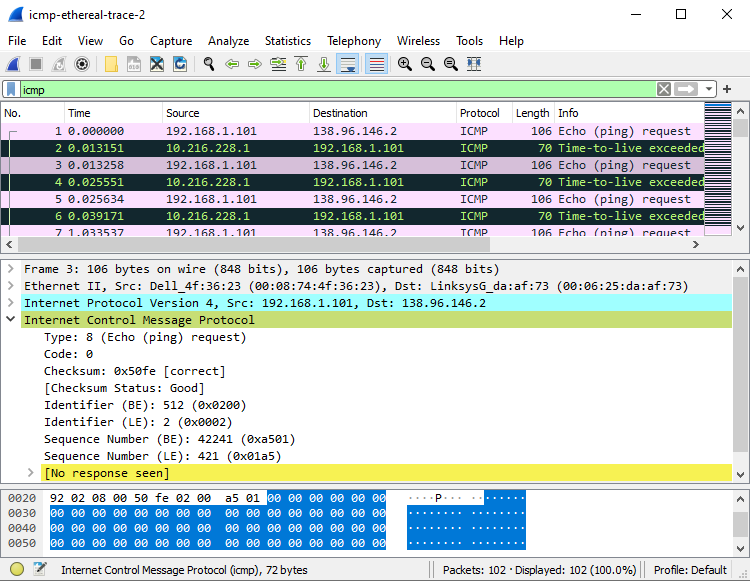
****

1. **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?**

* It would actually be different if ICMP sent UDP packets. Instead of 01 it would be switched to 0 X 11.

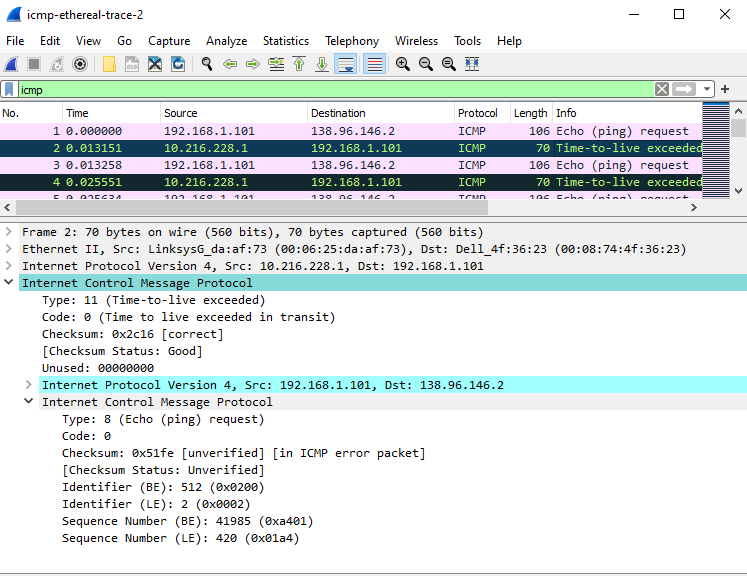
1. **Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?**

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



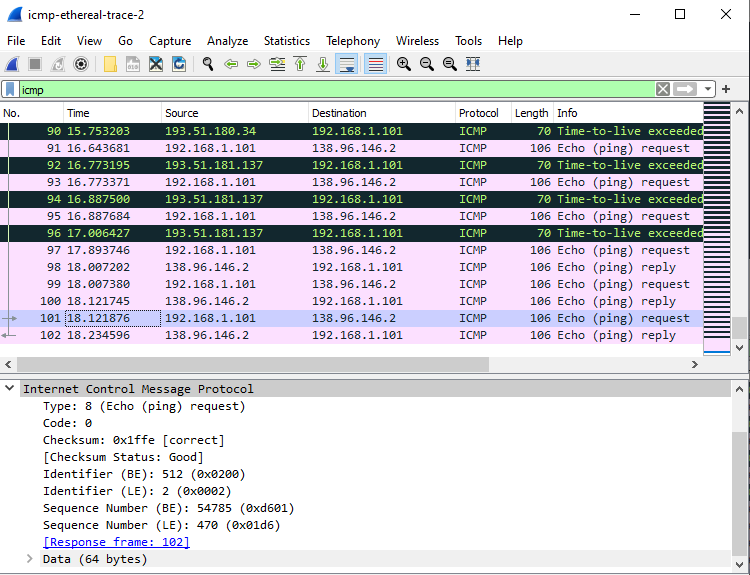
1. **Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?**

* The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.



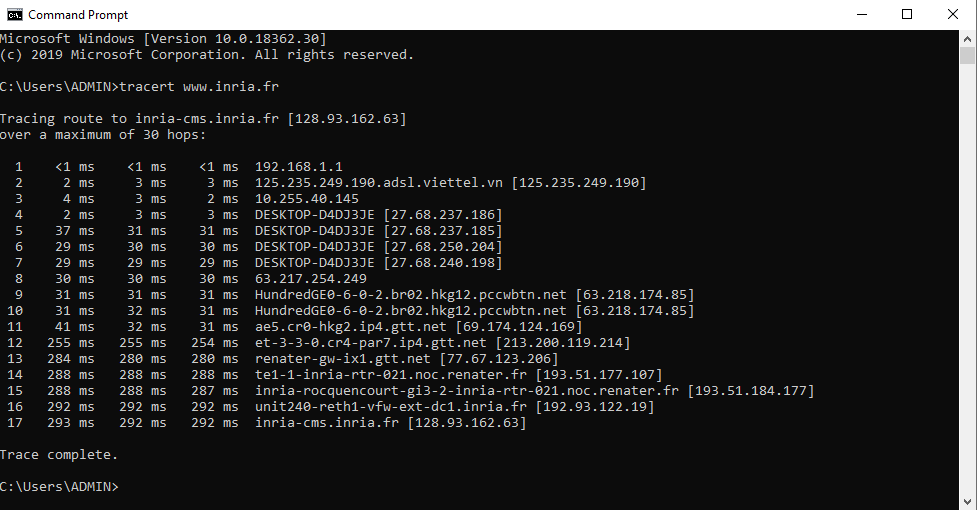
1. **Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?**

* Instead of being type 11, the last three packets are all type 0. They are different because they have all arrived before the TLL expires.

****

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?**

* Within the tracert measurements, the link between step 11 and 12 has significantly longer delay than others.
* In figure 4, the link between step 9 and 10 has significantly longer delay than others.
* The location of two delays is from USA(step 11) to Germany(step 12)

****