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

Source Host: 192.168.1.101

Destination Host: 143.89.14.34

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

ICMP packet is distinguished by request and reply so that the packet doesn’t have source and destination port numbers.

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 packet has Checksum, Identifier, Sequence Number, and Data field.

Checksum: 2 bytes

Sequence Number: 4 bytes (BE: 2 bytes / LE: 2 bytes)

Identifier fields: 4 bytes (BE: 2 bytes / LE: 2 bytes)

테이블이(가) 표시된 사진

자동 생성된 설명

(Frame Number: 3)

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 packet has Checksum, Identifier, Sequence Number, and Data field.

Checksum: 2 bytes

Sequence Number: 4 bytes (LE: 2 bytes / BE: 2 bytes)

Identifier: 4 bytes (LE: 2 bytes / BE: 2 bytes)

테이블이(가) 표시된 사진

자동 생성된 설명

(Frame Number: 4)

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

Source Host: 192.168. 1.101

Target 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?

If the ICMP sent UDP packets then, the IP protocol number will not be change from 01 because ICMP is in network layer, and UDP is in transport layer.

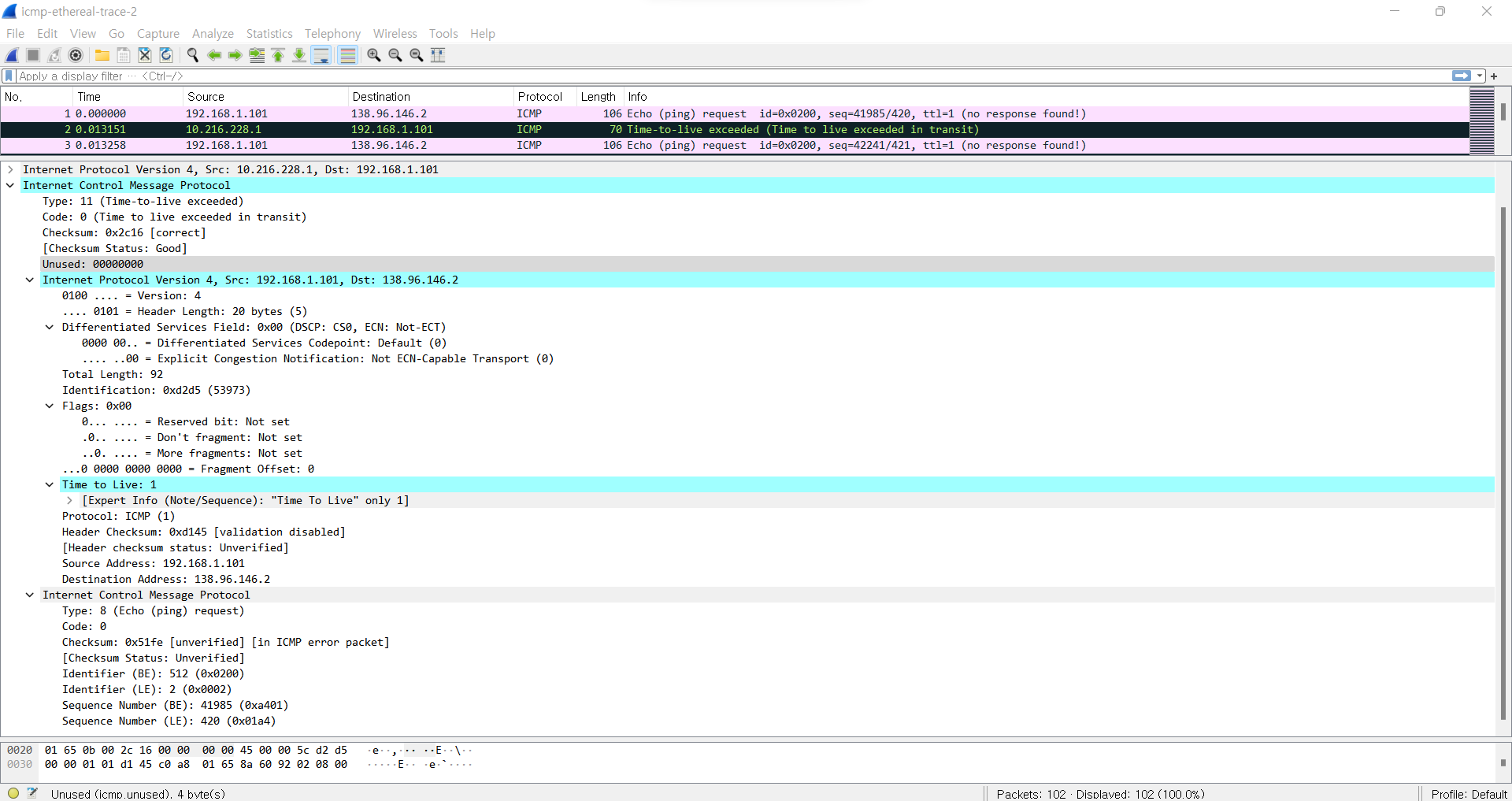
7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

테이블이(가) 표시된 사진

자동 생성된 설명

Yes, it is. There is no response frame in the ICMP echo packet.

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



(Frame Number: 2)

In the ICMP error packet, there is IPV4 field which contains Source and Destination address, Flags, TTL, and other information.

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?

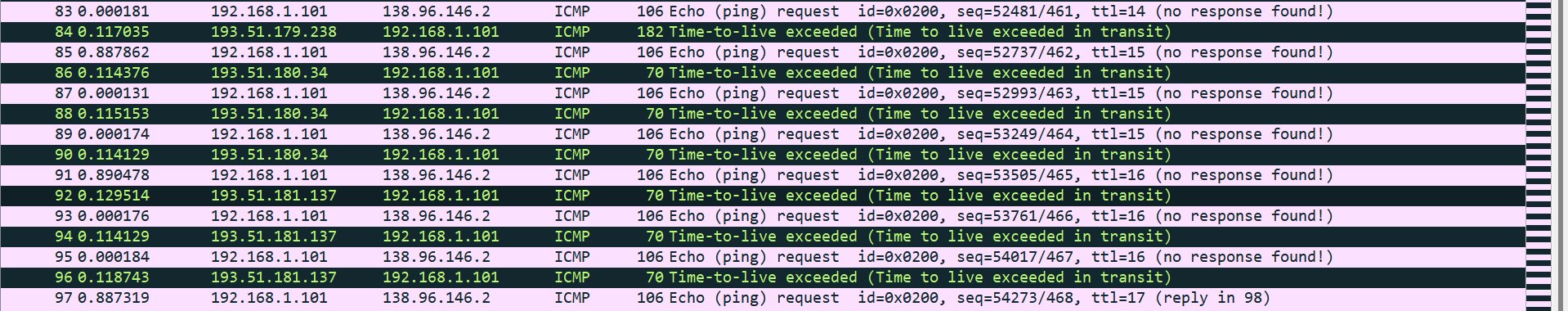
텍스트이(가) 표시된 사진

자동 생성된 설명

There is request frame in the packet, and ICMP error packet did not have request frame. Moreover, the Code of the packet represents the packet is replay packet. The reason is that the packet sent by the source finally reached the destination.

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?

Yes, there was a link whose delay was significantly longer than others.



(Frame 91~92 had the longest delay)

(Note: I set the time display as “since previous packet captured”. So, the time column represents the delay from previous packet.)

In Figure 4, the link, frame 9 to frame 10 had the significantly longer delay than others.

(72ms = 98ms – 26ms, 77ms = 98ms – 21ms, 71ms = 96ms – 25ms)

In frame 9, the router name includes ‘nyc’ so that the location of this router is New York City, and in frame 10, the router name includes ‘Pastourelle’ so that the location of this router is Paris, especially Pastourelle street.

(From: <https://en.wikipedia.org/wiki/Rue_Pastourelle> )