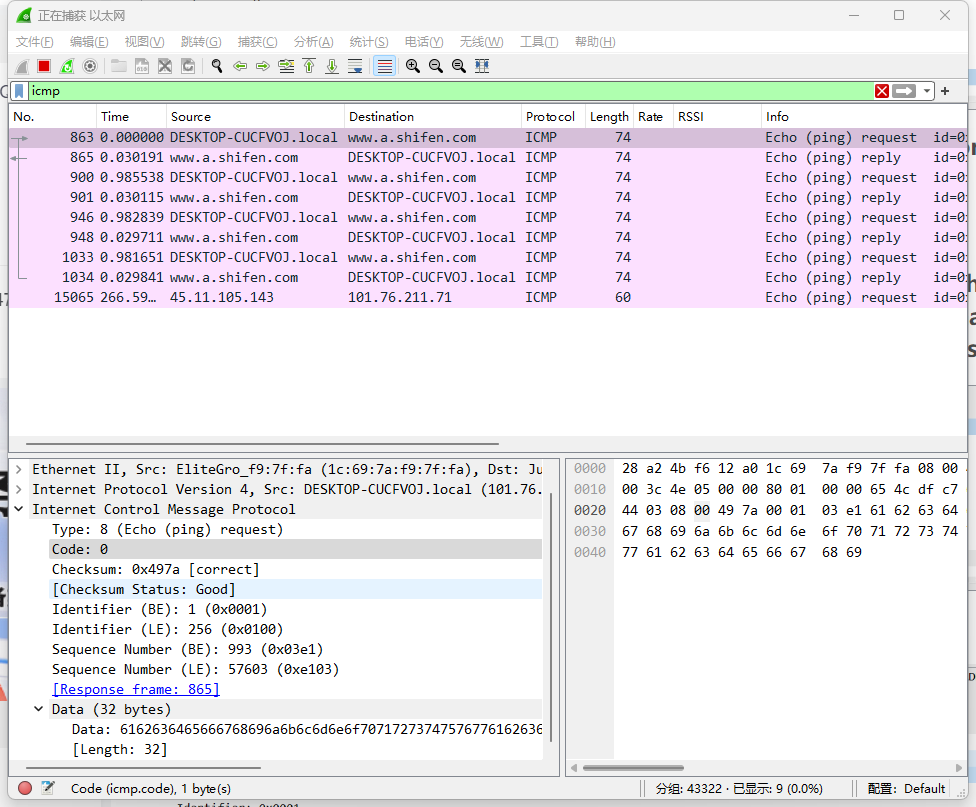
Wireshark Lab 5-2

202022300317 杨业昶

## 1. ICMP and Ping





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

>>> 101.76.223.199; 110.202.68.3

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

>>> ICMP is a network layer protocol, not an application layer protocol.

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?

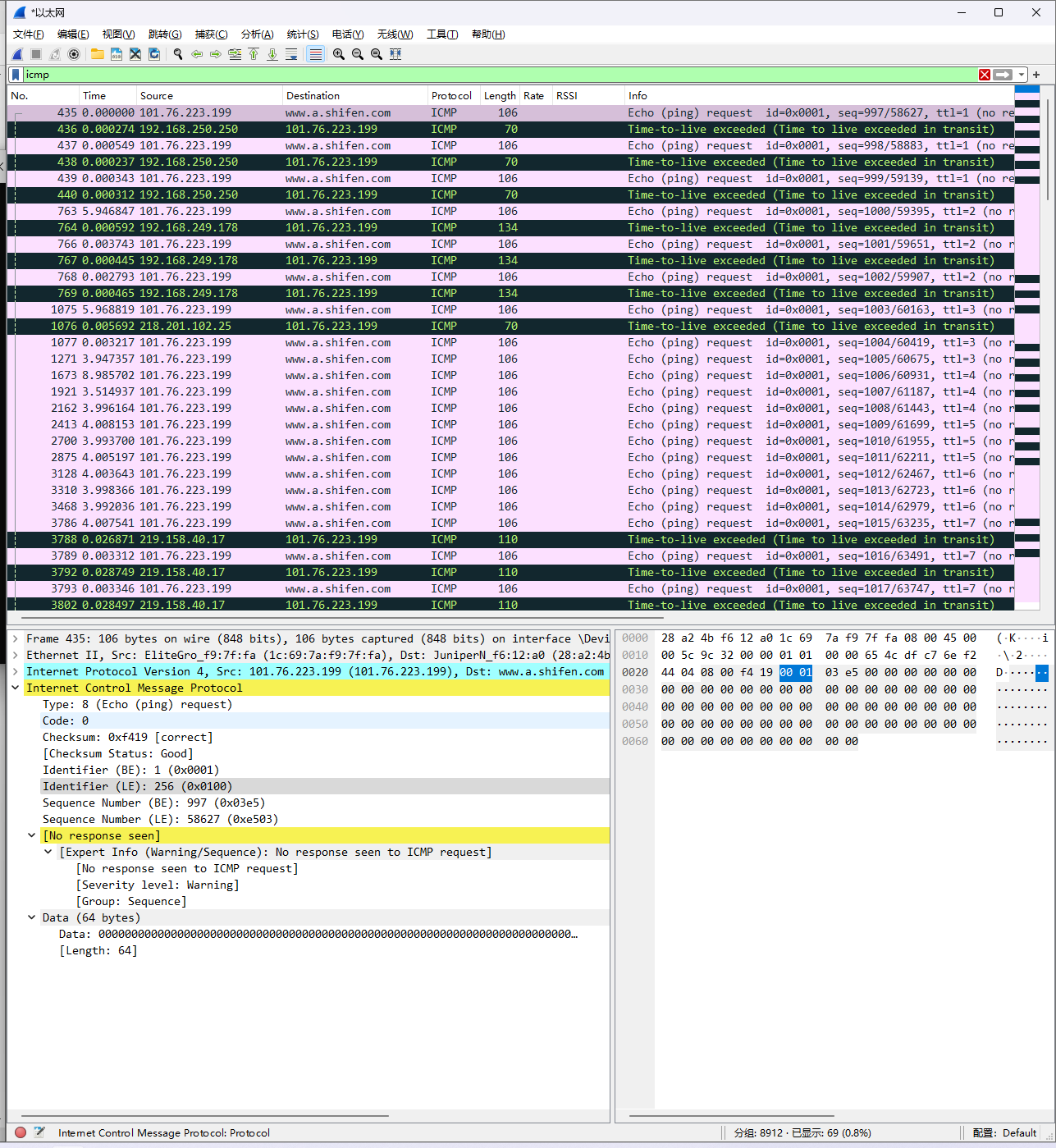
>>> Type: 8 (Echo (ping) request), Code: 0; Checksum, Identifier, Sequence Number, Data; 2, 2, 2

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?

>>> Type: 0 (Echo (ping) reply), Code: 0; Checksum, Identifier, Sequence Number, Data; 2, 2, 2

## 2. ICMP and Traceroute





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

>>> 101.76.223.199; 110.202.68.3

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; 0x11

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?

>>> Same fields, but no response seen.

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

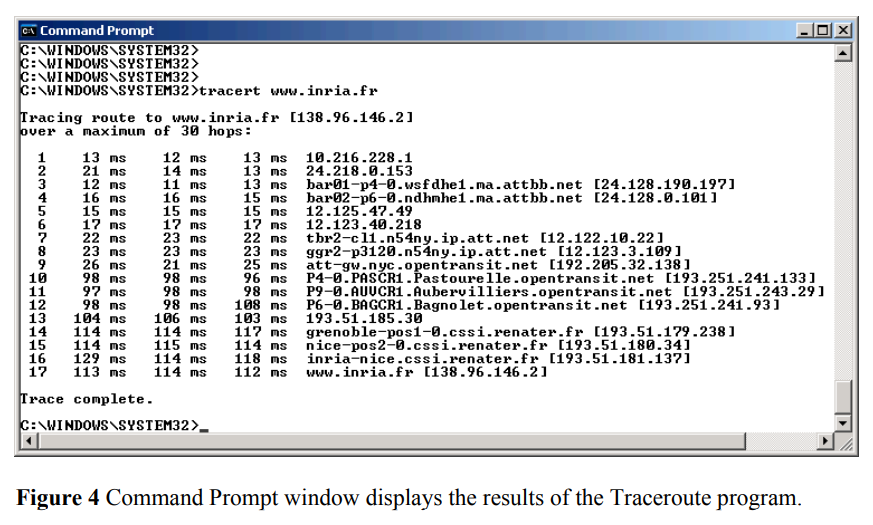
>>> IP packet fields, no Data fields.

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?

>>> Type: 0 (Echo (ping) reply), Type: 11 (Time-to-live exceeded); because last request arrived at destination host.

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?

>>> no significantly longer time in my tracert, but figure 4 here



>>> between 9 and 10, maybe the link across two countries.