Computer Networks 1

Lab 5

Wireshark Lab: ICMP v8.0

Student Name: **Nguyễn Quý Hải**

Student No.: **2052974**

I. Objectives

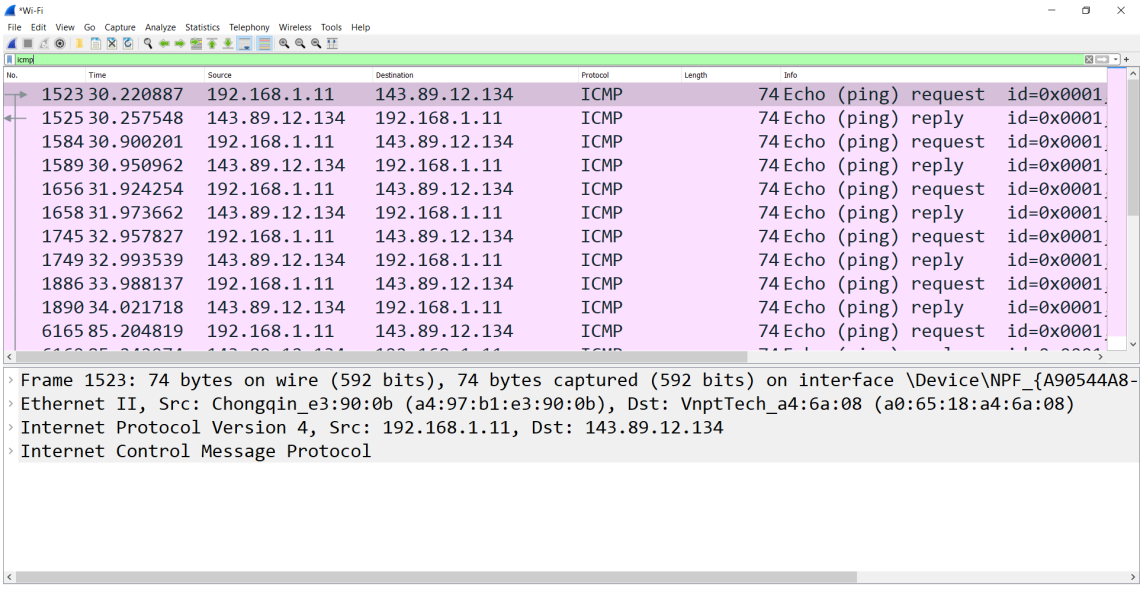
In this lab, we'll explore several aspects of the ICMP protocol:

- ICMP messages generating by the Ping program;
- ICMP messages generated by the Traceroute program;
- the format and contents of an ICMP message.

II. Content

Select Command Prompt

```
C:\Users\dell>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=384ms TTL=58
Reply from 143.89.12.134: bytes=32 time=51ms TTL=58
Reply from 143.89.12.134: bytes=32 time=49ms TTL=58
Reply from 143.89.12.134: bytes=32 time=36ms TTL=58
Reply from 143.89.12.134: bytes=32 time=34ms TTL=58
Reply from 143.89.12.134: bytes=32 time=38ms TTL=58
Reply from 143.89.12.134: bytes=32 time=35ms TTL=58
Reply from 143.89.12.134: bytes=32 time=36ms TTL=58
Reply from 143.89.12.134: bytes=32 time=34ms TTL=58
Reply from 143.89.12.134: bytes=32 time=35ms TTL=58

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 384ms, Average = 73ms
```



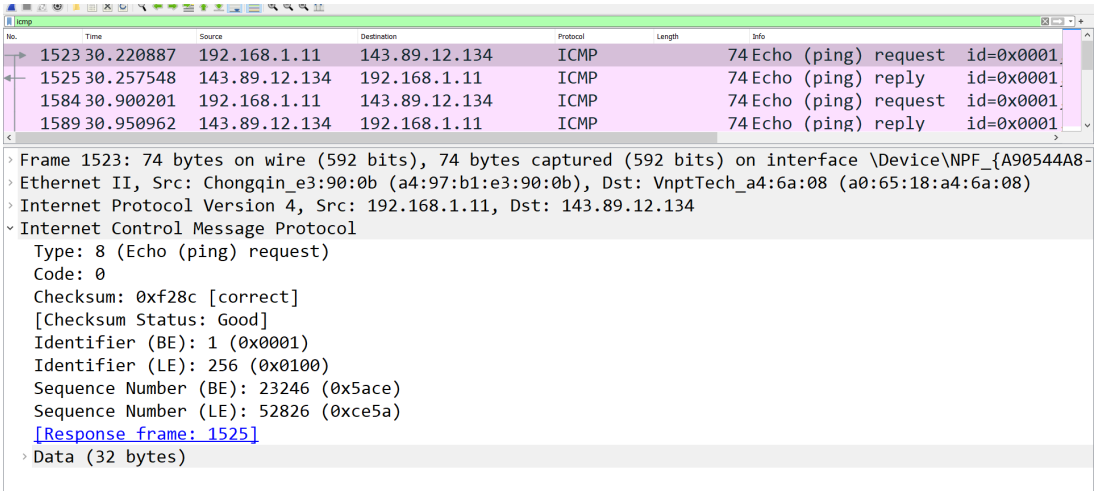
1. ICMP and Ping

- Q1: What is the IP address of your host? What is the IP address of the destination host?

  Answer: IP address of my host is 192.168.1.11. IP address of destination host is 143.89.12.134

- Q2. Why is it that an ICMP packet does not have source and destination port numbers?

  Answer: 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.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
1523	30.220887	192.168.1.11	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001
1525	30.257548	143.89.12.134	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001
1584	30.900201	192.168.1.11	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001
1589	30.950962	143.89.12.134	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001

```
> Frame 1523: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A90544A8-
> Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 143.89.12.134
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf28c [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 23246 (0x5ace)
    Sequence Number (LE): 52826 (0xce5a)
    [Response frame: 1525]
  > Data (32 bytes)
```

- Q3. 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?

  Answer: Type=8, Code=0. 2 bytes for checksum, 2 bytes for identifier and 2 bytes for sequence number.

  Internet Control Message Protocol

  Type: 8 (Echo (ping) request)

  Code: 0

  Checksum: 0xf28c [correct]

  [Checksum Status: Good]

  Identifier (BE): 1 (0x0001)

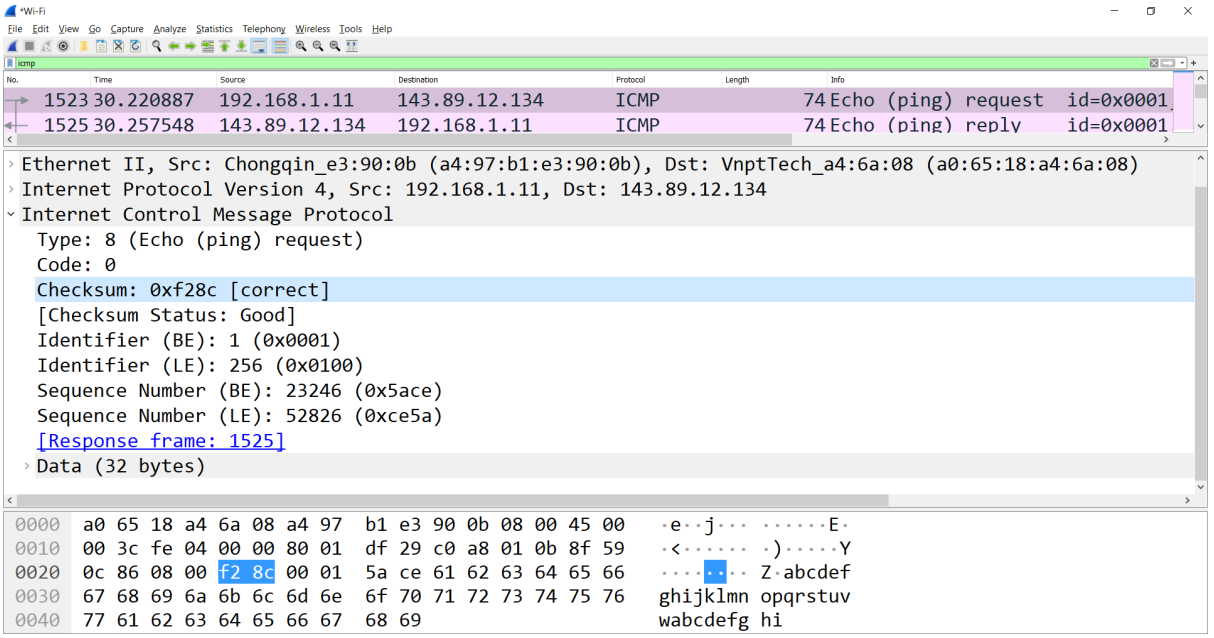
  Identifier (LE): 256 (0x0100)

  Sequence Number (BE): 23246 (0x5ace)

  Sequence Number (LE): 52826 (0xce5a)

  [Response frame: 1525]

  Data (32 bytes)



- Q4. 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?

  Answer: ICMP type = 0, code = 0. 2 bytes for checksum, sequence number and identifier fields. Other fields:

  Internet Control Message Protocol

  Type: 0 (Echo (ping) reply)

  Code: 0

  Checksum: 0xfa8c [correct]

  [Checksum Status: Good]

  Identifier (BE): 1 (0x0001)

  Identifier (LE): 256 (0x0100)

  Sequence Number (BE): 23246 (0x5ace)

  Sequence Number (LE): 52826 (0xce5a)

  [Request frame: 1523]

  [Response time: 36.661 ms]

  Data (32 bytes)

2. ICMP and Traceroute

Command Prompt

```
C:\Users\dell>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:

  1   474 ms     2 ms     2 ms  192.168.1.1
  2     5 ms     4 ms     9 ms  static.vnpt.vn [123.29.12.67]
  3    22 ms    19 ms    27 ms  static.vnpt.vn [113.171.46.214]
  4    19 ms    50 ms    18 ms  static.vnpt.vn [113.171.59.210]
  5    27 ms    24 ms    21 ms  static.vnpt.vn [113.171.37.111]
  6   284 ms   283 ms   282 ms  renater.par.franceix.net [37.49.236.19]
  7   286 ms     *        *     xe-1-0-9-paris1-rtr-131.noc.renater.fr [193
.51.177.146]
  8   291 ms   288 ms   286 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.
177.107]
  9     *      290 ms   288 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.
renater.fr [193.51.184.177]
 10     *      283 ms   283 ms  192.93.122.19
 11     *        *      280 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Users\dell>
```

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
244	5.014274	192.168.1.11	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001
245	5.019456	192.168.1.1	192.168.1.11	ICMP	134	Time-to-live exceeded (Time to
248	5.024567	192.168.1.11	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001
249	5.026938	192.168.1.1	192.168.1.11	ICMP	134	Time-to-live exceeded (Time to
250	5.031565	192.168.1.11	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001
251	5.033939	192.168.1.1	192.168.1.11	ICMP	134	Time-to-live exceeded (Time to
257	5.060979	192.168.1.1	192.168.1.11	ICMP	120	Destination unreachable (Port
328	6.561173	192.168.1.1	192.168.1.11	ICMP	120	Destination unreachable (Port
408	8.065417	192.168.1.1	192.168.1.11	ICMP	120	Destination unreachable (Port
535	10.579878	192.168.1.11	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001
536	10.584864	123.29.12.67	192.168.1.11	ICMP	70	Time-to-live exceeded (Time to
537	10.589286	192.168.1.11	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001
538	10.593531	123.29.12.67	192.168.1.11	ICMP	70	Time-to-live exceeded (Time to
539	10.597986	192.168.1.11	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001

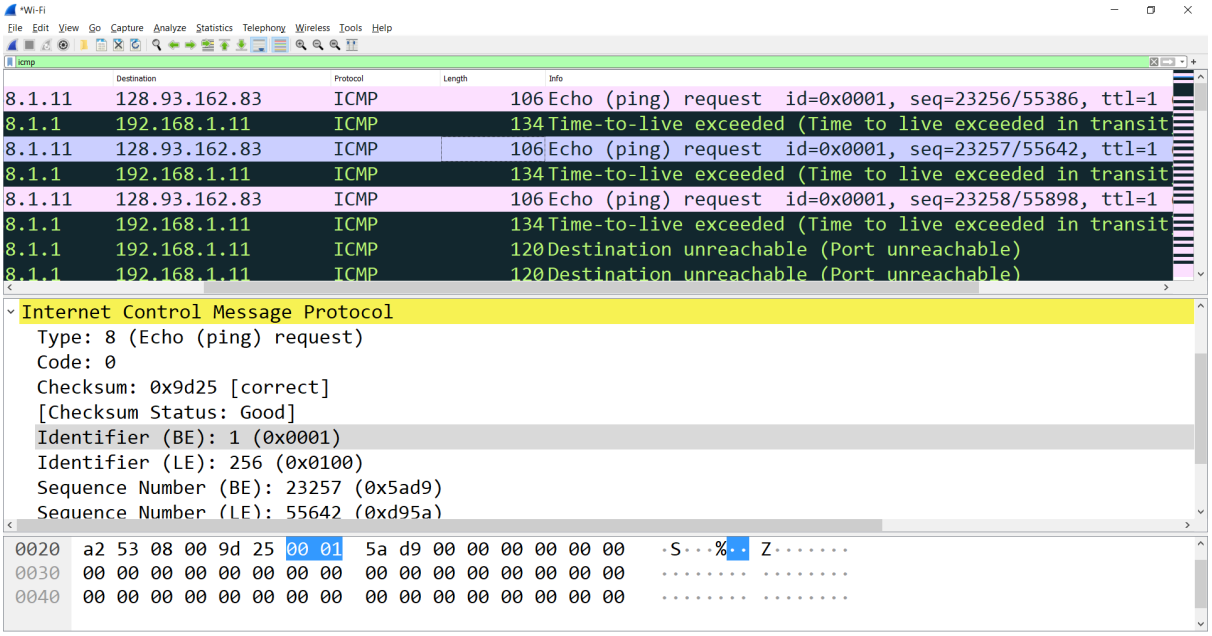
```
> Frame 244: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{A90544A
> Ethernet II, Src: Chongqin e3:90:0b (a4:97:b1:e3:90:0b), Dst: VnptTech a4:6a:08 (a0:65:18:a4:6a:08)

0020  a2 53 08 00 9d 26 00 01  5a d8 00 00 00 00 00 00   ·S···&·· Z·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00                     ........ ··
```

- Q5: What is the IP address of your host? What is the IP address of the target destination host?

  <u>Answer</u>: IP address of my host: 192.168.1.1. IP address of the target destination host: 128.93.162.83

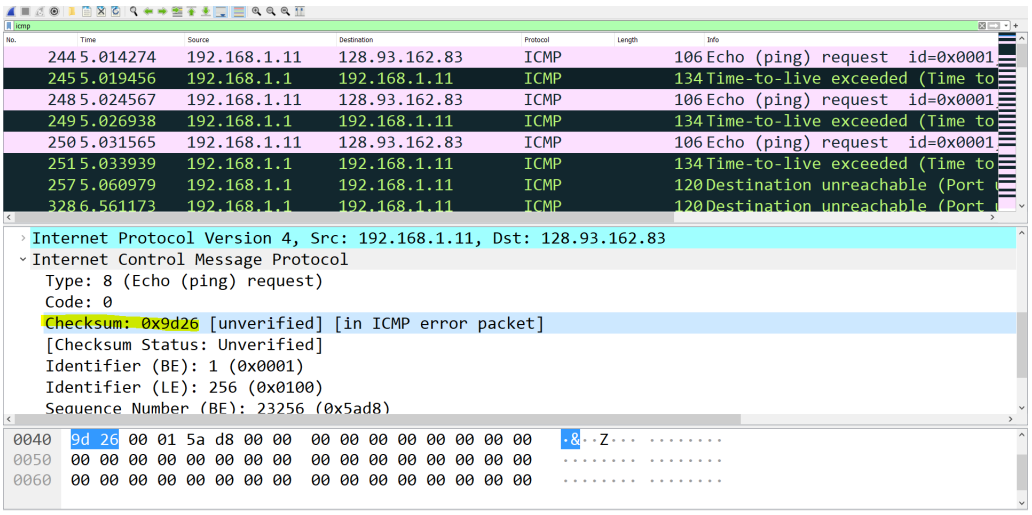
- Q6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

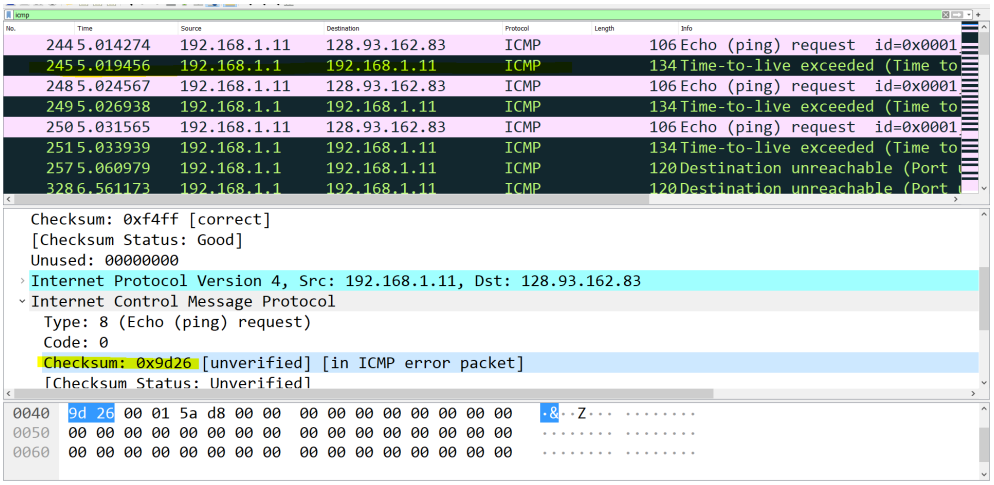
  Answer: Yes



- Q7. 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?

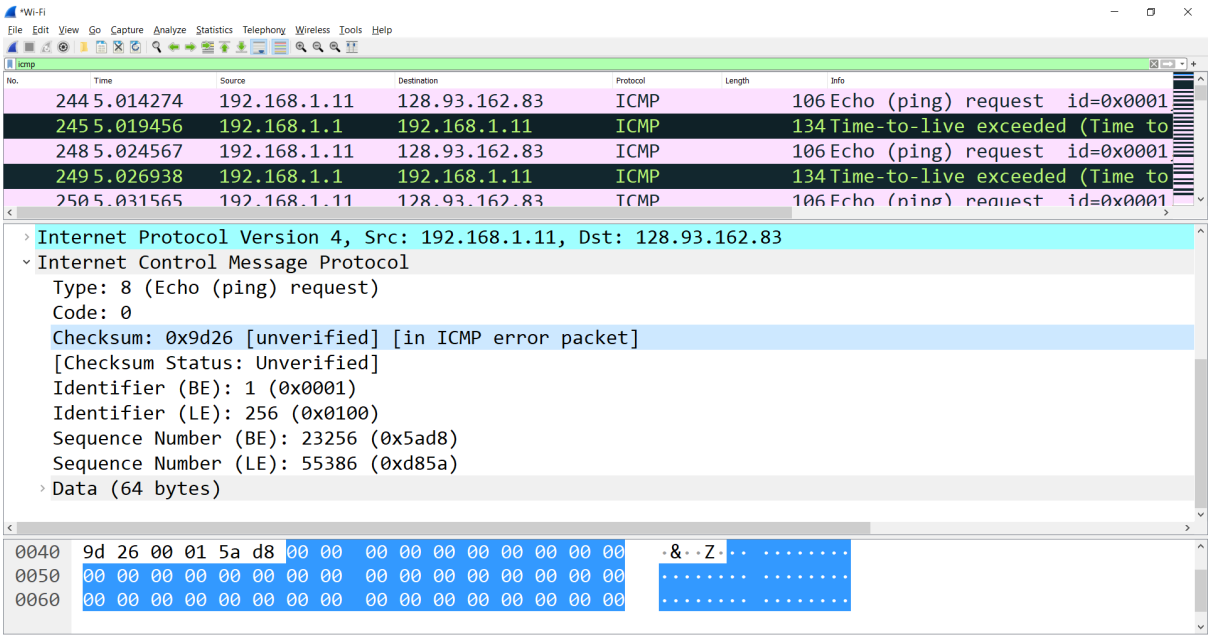
  Answer: No





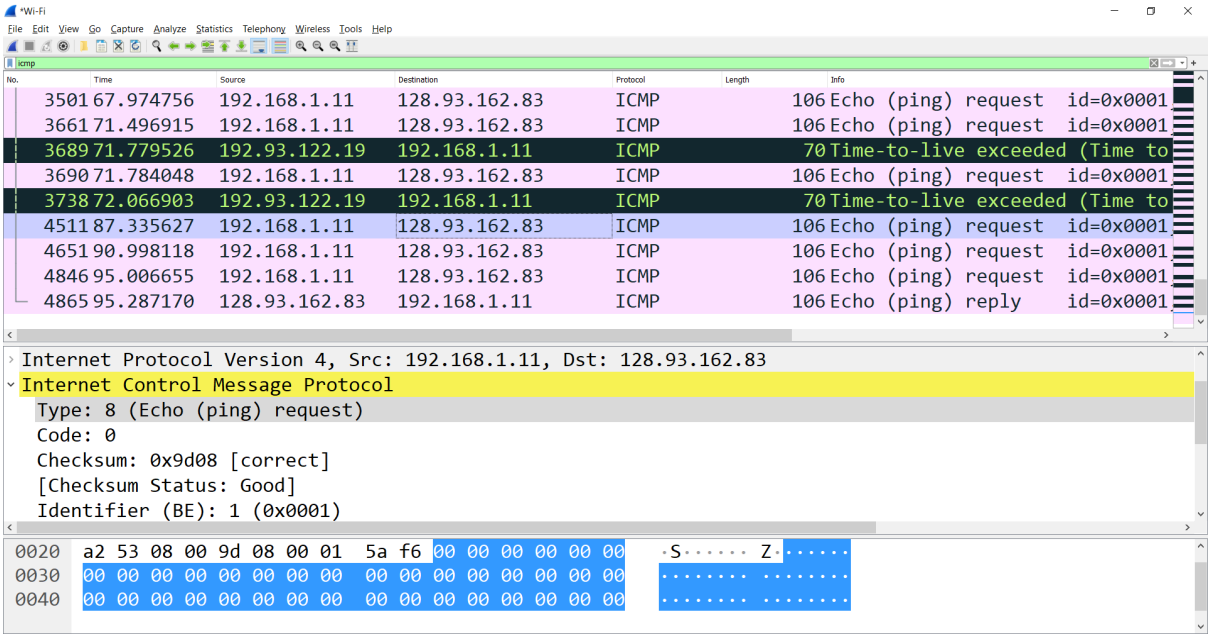
- Q8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

  Answer: IP header and 8 bytes of the original ICMP packet



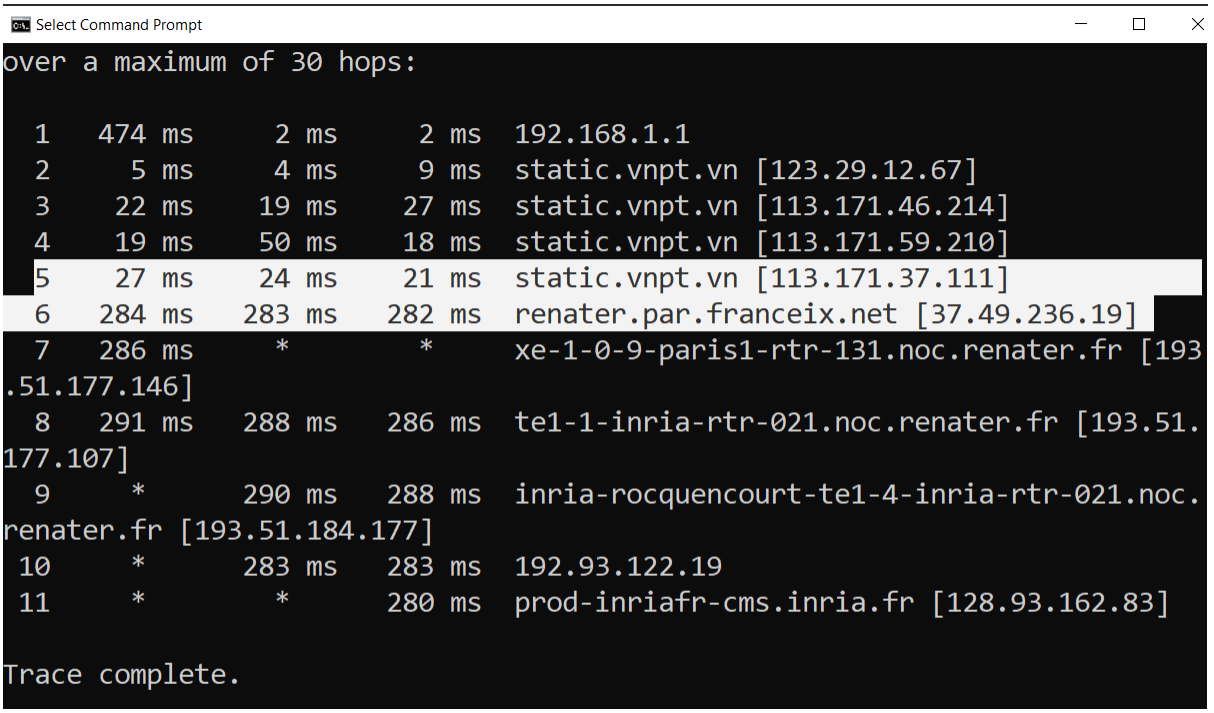
- Q9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

  Answer: The last 3 ICMP packets are Type: 8 (Echo (ping) request). They are different because the datagrams have made it all the way to the destination host before the TTL expired.



- Q10. 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?

  <u>Answer</u>: In my lab, it is between 5 and 6. In Figure 4, it is between 9 and 10 and the link is from New York to Pastourelle, France.



3. Extra Credit (No)