Lab 4 - Internet Control Message Protocol
Computer Networks

Thang Huu Nguyen - 1713239

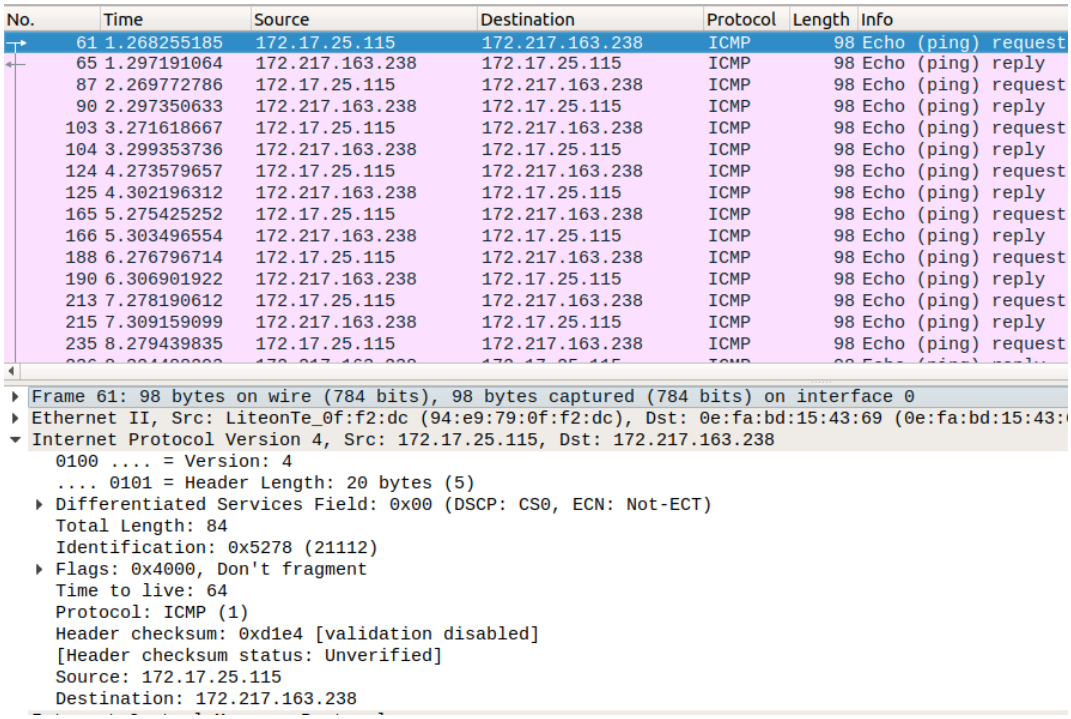
September, 2019

```
thang@thang:~$ ping -c 10 google.com
PING google.com (172.217.163.238) 56(84) bytes of data.
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=1 ttl=55 time=28.9 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=2 ttl=55 time=27.6 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=3 ttl=55 time=27.7 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=4 ttl=55 time=28.6 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=5 ttl=55 time=28.1 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=6 ttl=55 time=30.1 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=7 ttl=55 time=31.0 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=8 ttl=55 time=45.0 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=9 ttl=55 time=31.0 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=10 ttl=55 time=32.1 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 27.614/31.055/45.084/4.905 ms
```

1 ICMP and Ping

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

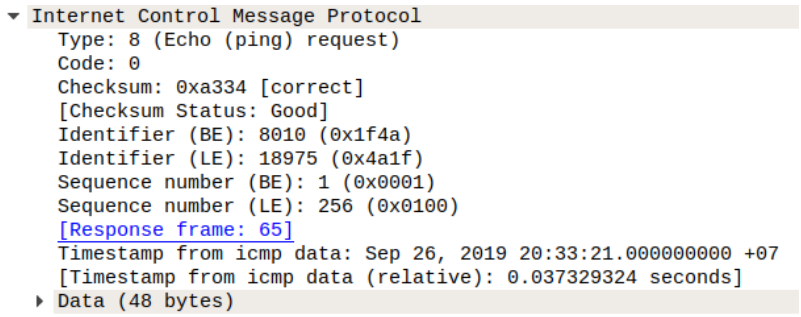


Answers: The IP address of my host is 172.17.25.115. And the IP address of the destination host is 172.217.163.238.

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

Answers: An ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer between source hosts and routers, not between application-layer processes. Each ICMP packet has a particularly **type** and **code** which combination identifies the specific message being received.

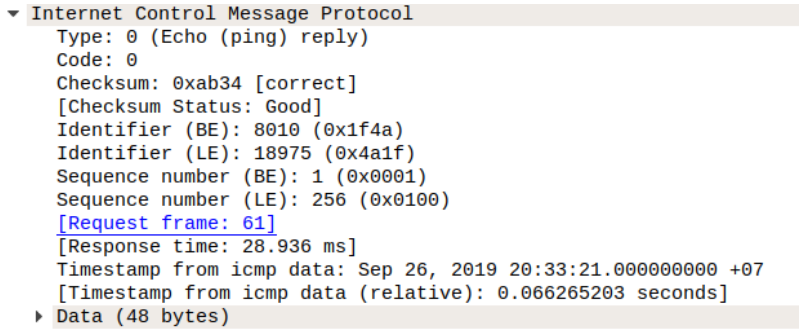
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?



Answers:

- The ICMP type number is 8.
- The ICMP code number is 0.
- The ICMP request packet also has Checksum, Identifier, Sequence number, Timestamp and Data fields.
- The Checksum, Sequence number and Identifier 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?



Answers:

- The ICMP type number is 0.
- The ICMP code number is 0.
- The ICMP reply packet also has Checksum, Identifier, Sequence number, Timestamp, Data fields.
- The Checksum, Sequence number and Identifier are two bytes each.

2 ICPM and Traceroute

```
thang@thang:~$ sudo traceroute --icmp google.com
[sudo] password for thang:
traceroute to google.com (172.217.163.238), 30 hops max, 60 byte packets
 1  * * *
 2  adsl.hnpt.com.vn (203.210.144.132)  27.900 ms  27.919 ms  27.918 ms
 3  172.17.5.65 (172.17.5.65)  27.929 ms  27.928 ms  27.926 ms
 4  static.vnpt.vn (113.171.48.125)  27.897 ms  27.897 ms  27.894 ms
 5  static.vnpt.vn (113.171.44.113)  47.096 ms  47.098 ms  47.102 ms
 6  static.vnpt.vn (113.171.50.230)  47.042 ms  52.084 ms  52.102 ms
 7  static.vnpt.vn (113.171.32.23)  52.100 ms  52.105 ms  52.111 ms
 8  * * *
 9  108.170.241.65 (108.170.241.65)  55.017 ms  35.854 ms  35.816 ms
10  172.253.64.111 (172.253.64.111)  35.810 ms  35.810 ms  38.451 ms
11  hkg12s18-in-f14.1e100.net (172.217.163.238)  38.441 ms  38.440 ms  38.438 ms
```

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

```
▾ Internet Protocol Version 4, Src: 172.17.25.115, Dst: 172.217.163.238
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xb6dd (46813)
  ▸ Flags: 0x0000
  ▸ Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0xec97 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.17.25.115
    Destination: 172.217.163.238
```

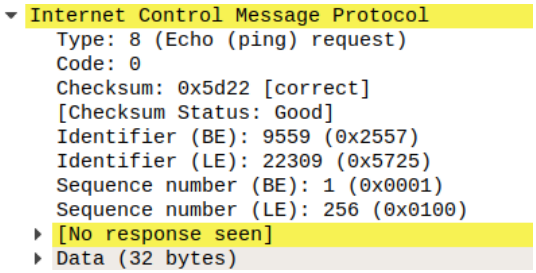
Answers: The IP address of my host is 172.17.25.115. And the IP address of the target destination host is 172.217.163.238.

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?

```
▾ Internet Protocol Version 4, Src: 172.17.25.115, Dst: 216.58.220.206
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x01a8 (424)
  ▸ Flags: 0x0000
  ▸ Time to live: 1
    Protocol: UDP (17)
```

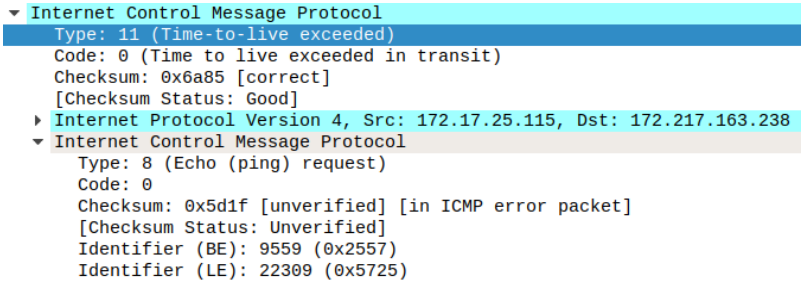
Answers: If ICMP sent UDP packets instead, The IP protocol number not still be 01 for the probe packets. It would be 17.

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?



Answers: The ICMP echo packet has the most fields as the ping query packets, but it has no timestamp field.

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

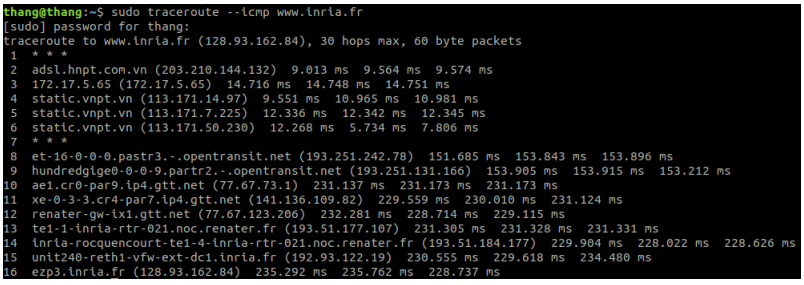


Answers: The ICMP error packet is not the same as the ICMP normal packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

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?

Answers: The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

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?



Answers: There is a link between steps 6 and 7 that has a significantly longer delay. This is a transatlantic link from Vietnam to Aubervilliers, France. In figure 4 from the lab, the link is from New York to Pastourelle, France.