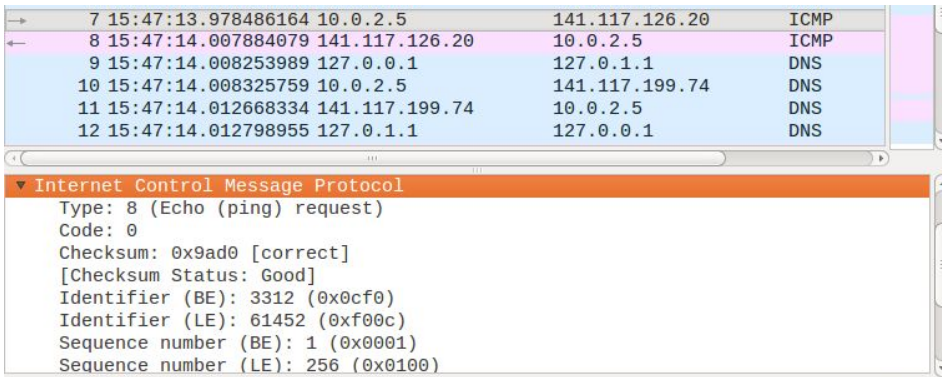
CPS 706 - Wireshark ICMP

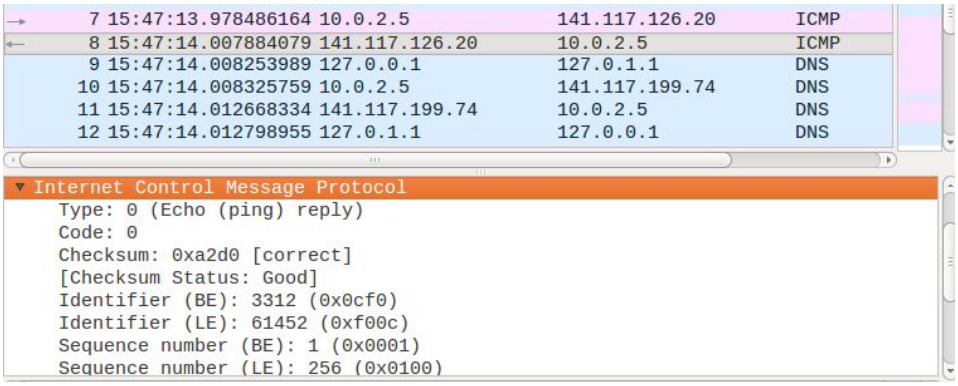
```
[03/10/20]seed@VM:~$ ping www.ryerson.ca
PING www.ryerson.ca (141.117.126.20) 56(84) bytes of data.
64 bytes from 141.117.126.20: icmp_seq=1 ttl=252 time=29.4 ms
64 bytes from 141.117.126.20: icmp_seq=2 ttl=252 time=5.36 ms
64 bytes from 141.117.126.20: icmp_seq=3 ttl=252 time=5.50 ms
64 bytes from 141.117.126.20: icmp_seq=4 ttl=252 time=5.55 ms
64 bytes from 141.117.126.20: icmp_seq=5 ttl=252 time=6.24 ms
64 bytes from 141.117.126.20: icmp_seq=6 ttl=252 time=5.00 ms
64 bytes from 141.117.126.20: icmp_seq=7 ttl=252 time=5.79 ms
64 bytes from 141.117.126.20: icmp_seq=8 ttl=252 time=5.89 ms
64 bytes from 141.117.126.20: icmp_seq=9 ttl=252 time=5.86 ms
64 bytes from 141.117.126.20: icmp_seq=10 ttl=252 time=5.71 ms
^C
--- www.ryerson.ca ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 5.000/8.034/29.407/7.131 ms
```

1. *What is the IP address of your host? What is the IP address of the destination host?*
    - IP address of my host: 10.0.2.5
    - IP address of destination host: 141.117.126.20

2. *Why is it that an ICMP packet does not have source and destination port numbers?*
    - Port numbers are a feature of the transport layer protocols (i.e. TCP & UDP), ICMP is a part of the network layer protocol rather than the transport layer. Therefore, ICMP does not need any source and destination port numbers
    - They are designed to communicate network-layer information between hosts and routers, not between application layer processes



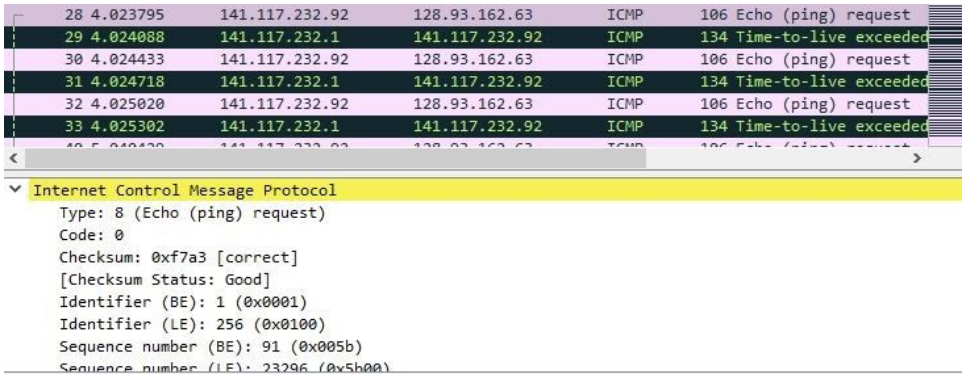
3. *Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?*
    - Type: 8 (Echo Ping Request)
    - Code numbers: 0
    - Fields in ICMP packet: Type, Code, Checksum, Identifier, Sequence number, Timestamp
    - Checksum, sequence number and identifier fields each has 2 bytes



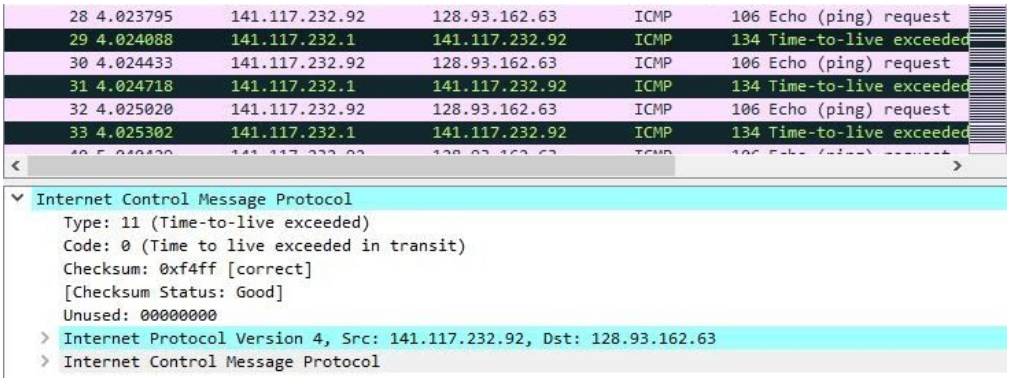
4. *Examine the corresponding ping reply packet. What are the ICMP type and code numbers/ What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?*
    - Type: 0 (Echo Ping Reply)
    - Code numbers: 0
    - Fields in ICMP packet: Type, Code, Checksum, Identifier, Sequence number, Timestamp
    - Checksum, sequence number and identifier fields each has 2 bytes

5. *What is the IP address of your host? What is the IP address of the target destination host?*
    - IP address of my host: 141.117.232.92
    - IP address of destination: 128.93.162.63

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?*
    - No, if ICMP is sent with UDP packets, the IP protocol number would be 0x11

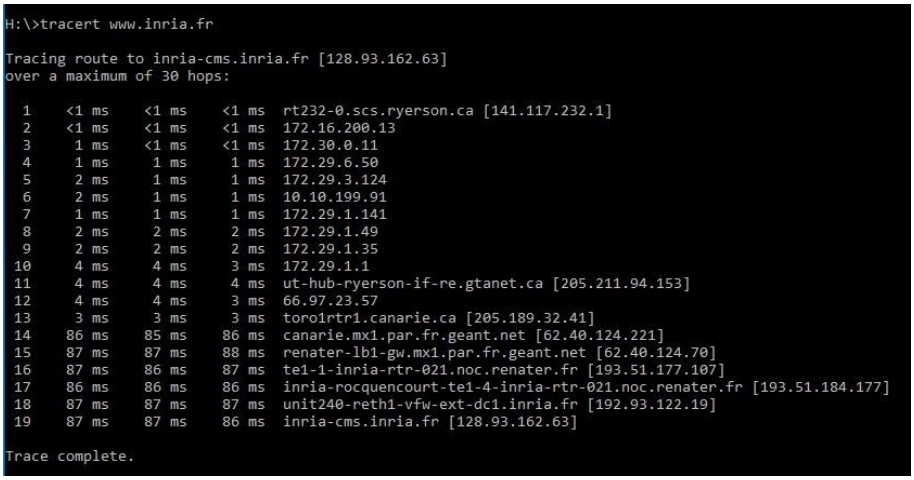


7. *Examine the ICMP echo packet in your screenshot. Is this different from ICMP ping query packets in the first half of the lab? If yes, how so?*
    - ICMP echo packet has the same field as the ping query packets



8. *Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?*
    - ICMP error packet has more fields. It contains an additional 8 bytes IP header for the error.

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?*
    - The last three ICMP packets received by the source host have type 0 (echo ping reply) which is different from the error packets that have type 11 (Time-to-live exceeded). They are different because the last 3 ICMP packets made it 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?*
    - Yes, when there is a significantly longer delay, it means there is a transatlantic / transoceanic link. It's travelling further than the packets that have a shorter time delay. In the traceroute above, it happens on the 14th hop.