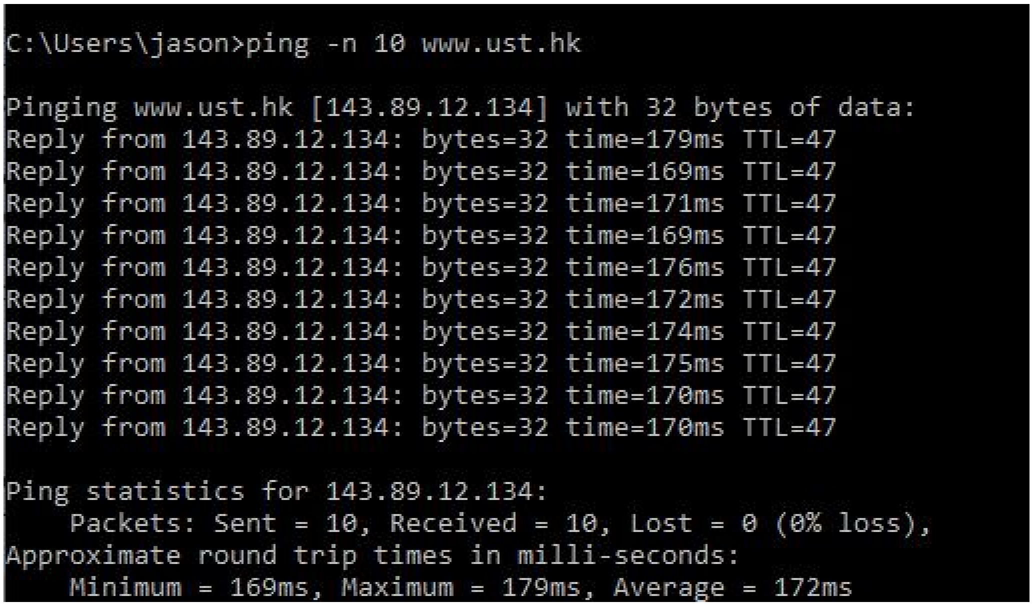
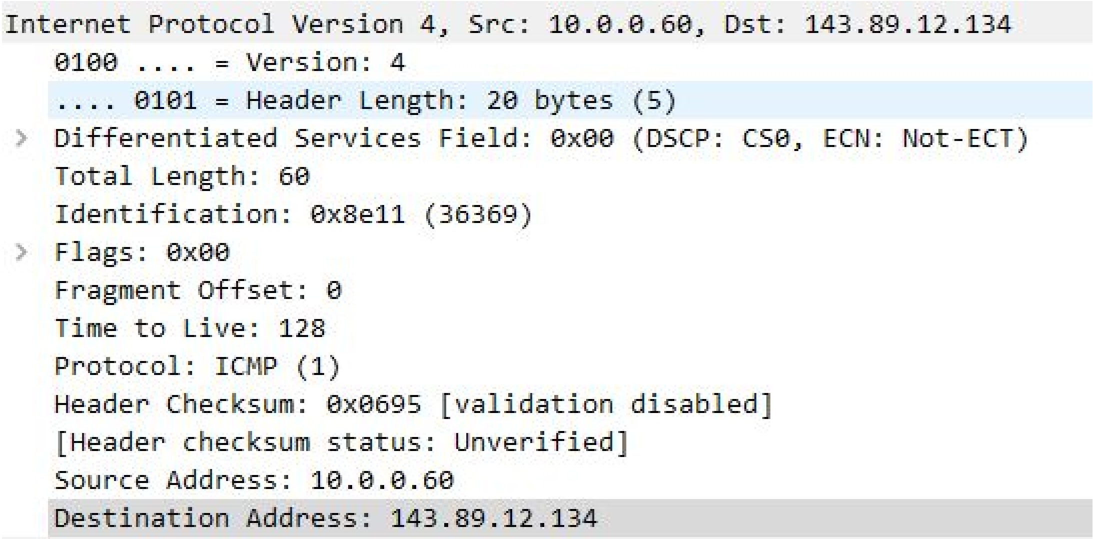
Jason Xin
ECS 152A

Programming 1: Wireshark ICMP Lab



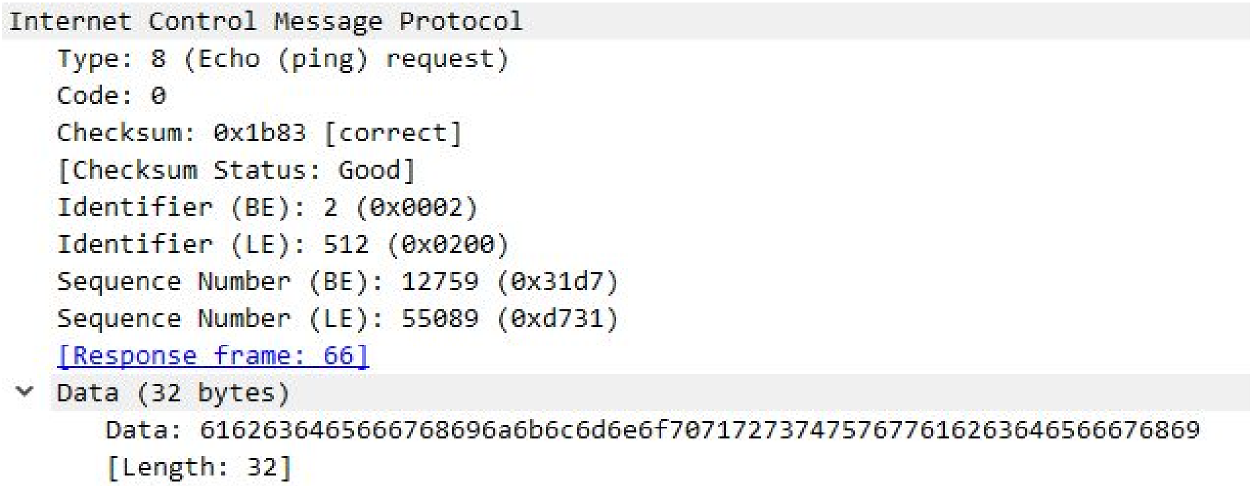
```
C:\Users\jason>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=179ms TTL=47
Reply from 143.89.12.134: bytes=32 time=169ms TTL=47
Reply from 143.89.12.134: bytes=32 time=171ms TTL=47
Reply from 143.89.12.134: bytes=32 time=169ms TTL=47
Reply from 143.89.12.134: bytes=32 time=176ms TTL=47
Reply from 143.89.12.134: bytes=32 time=172ms TTL=47
Reply from 143.89.12.134: bytes=32 time=174ms TTL=47
Reply from 143.89.12.134: bytes=32 time=175ms TTL=47
Reply from 143.89.12.134: bytes=32 time=170ms TTL=47
Reply from 143.89.12.134: bytes=32 time=170ms TTL=47

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 169ms, Maximum = 179ms, Average = 172ms
```

\



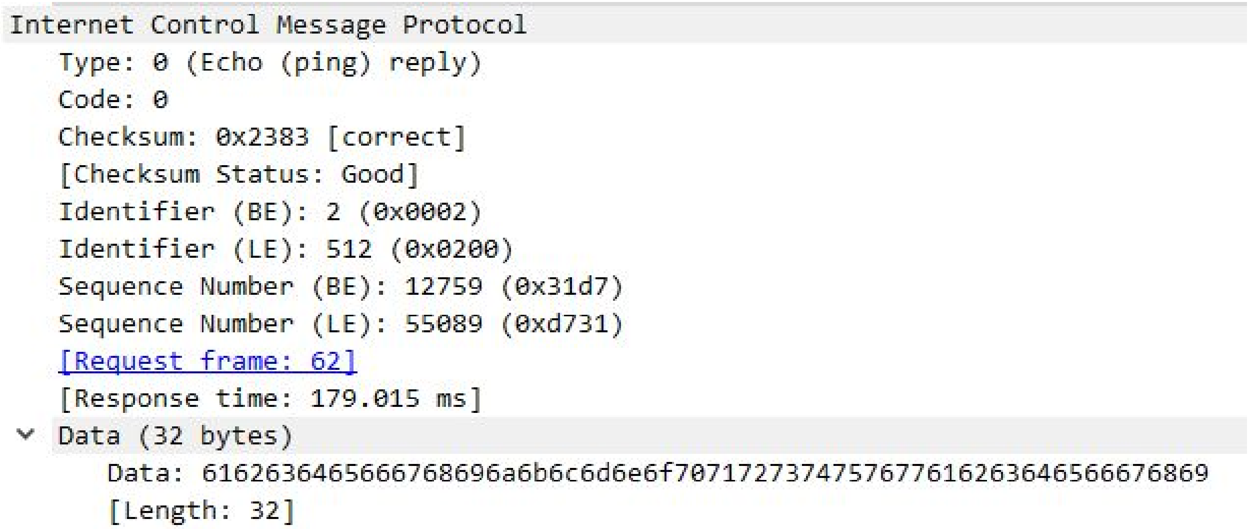
```
Internet Protocol Version 4, Src: 10.0.0.60, Dst: 143.89.12.134
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x8e11 (36369)
 > Flags: 0x00
   Fragment Offset: 0
   Time to Live: 128
   Protocol: ICMP (1)
   Header Checksum: 0x0695 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 10.0.0.60
   Destination Address: 143.89.12.134
```

1. The IP address of my host is 10.0.0.60 and the address of the destination host is 143.89.12.134.
2. ICMP Packets do not have Source/Destination port numbers because they are designed to communicate between hosts and routers on the network layer, and therefore do not need information about source and destination port numbers, which operate on the application layer.



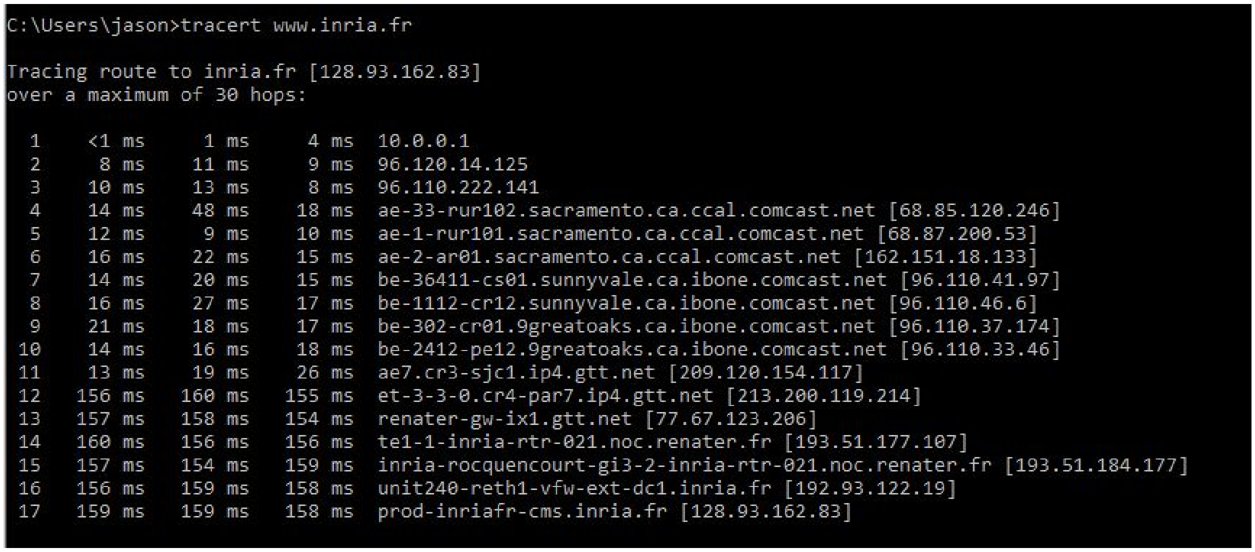
```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x1b83 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence Number (BE): 12759 (0x31d7)
    Sequence Number (LE): 55089 (0xd731)
    [Response frame: 66]
  ⌄ Data (32 bytes)
        Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
        [Length: 32]
```

3. The ICMP type of this reply is 8 (Echo (ping) request), and the code is 0. The other fields this packet has are checksum (and checksum status), BE and LE identifier, BE and LE sequence numbers, and data. The checksum, sequence number, and identifier fields are all two bytes.

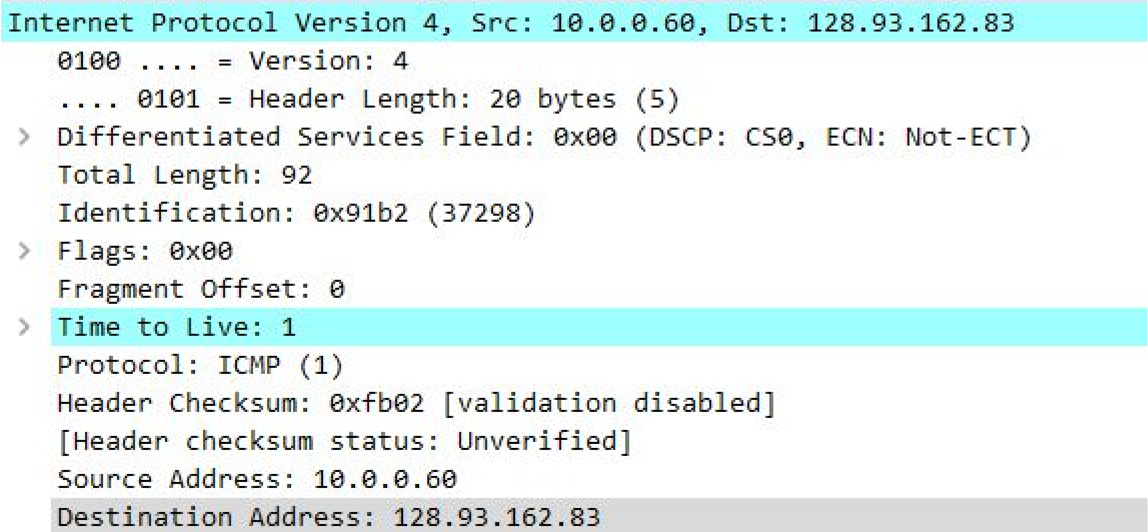


```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x2383 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence Number (BE): 12759 (0x31d7)
    Sequence Number (LE): 55089 (0xd731)
    [Request frame: 62]
    [Response time: 179.015 ms]
  ⌄ Data (32 bytes)
        Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
        [Length: 32]
```

4. The ICMP type of this request is 0 (Echo (ping) reply), and the code is 0. The other fields this packet has are checksum (and checksum status), BE and LE identifier, BE and LE sequence numbers, and data. The checksum, sequence number, and identifier fields are all two bytes.

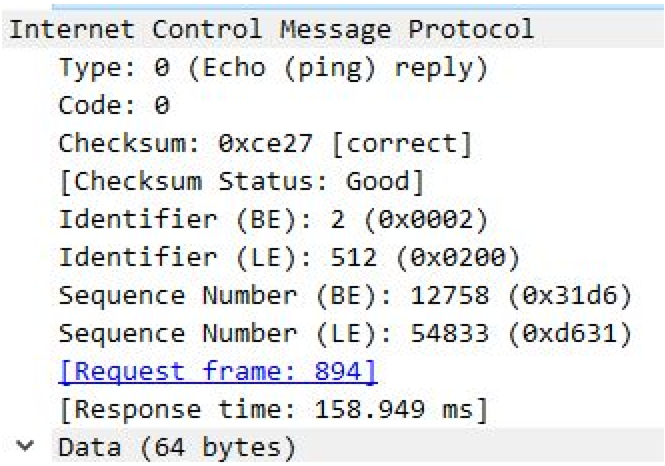


```
C:\Users\jason>tracert www.inria.fr

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

  1    <1 ms     1 ms     4 ms  10.0.0.1
  2     8 ms    11 ms     9 ms  96.120.14.125
  3    10 ms    13 ms     8 ms  96.110.222.141
  4    14 ms    48 ms    18 ms  ae-33-rur102.sacramento.ca.ccal.comcast.net [68.85.120.246]
  5    12 ms     9 ms    10 ms  ae-1-rur101.sacramento.ca.ccal.comcast.net [68.87.200.53]
  6    16 ms    22 ms    15 ms  ae-2-ar01.sacramento.ca.ccal.comcast.net [162.151.18.133]
  7    14 ms    20 ms    15 ms  be-36411-cs01.sunnyvale.ca.ibone.comcast.net [96.110.41.97]
  8    16 ms    27 ms    17 ms  be-1112-cr12.sunnyvale.ca.ibone.comcast.net [96.110.46.6]
  9    21 ms    18 ms    17 ms  be-302-cr01.9greatoaks.ca.ibone.comcast.net [96.110.37.174]
 10    14 ms    16 ms    18 ms  be-2412-pe12.9greatoaks.ca.ibone.comcast.net [96.110.33.46]
 11    13 ms    19 ms    26 ms  ae7.cr3-sjc1.ip4.gtt.net [209.120.154.117]
 12   156 ms   160 ms   155 ms  et-3-3-0.cr4-par7.ip4.gtt.net [213.200.119.214]
 13   157 ms   158 ms   154 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 14   160 ms   156 ms   156 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 15   157 ms   154 ms   159 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 16   156 ms   159 ms   158 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 17   159 ms   159 ms   158 ms  prod-inriafr-cms.inria.fr [128.93.162.83]
```



```
Internet Protocol Version 4, Src: 10.0.0.60, Dst: 128.93.162.83
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x91b2 (37298)
  > Flags: 0x00
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0xfb02 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.0.60
    Destination Address: 128.93.162.83
```

5. The IP address of my host is 10.0.060 and the address of the destination host is 128.93.162.83.
6. No, it would not be 0x01, and instead the IP protocol would be switched to 0x11.
7. No, it is not different, as it has the same fields as the first half of the lab.
8. The packet includes the IP header along with the first 8 bytes of the original ICMP packet that caused the error.



```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xce27 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence Number (BE): 12758 (0x31d6)
    Sequence Number (LE): 54833 (0xd631)
    [Request frame: 894]
    [Response time: 158.949 ms]
    Data (64 bytes)
```

9. The last three packets all have message type 0, marking a reply. These are different as the datagrams reached the destination host before the Time to Live had expired.
10. In my own tracert measurements, between steps 11 and 12, there is a large delay. In Figure 4, the delay is between steps 9 and 10. My guess is that this is the inter-continental hop, as routers go from .net addresses to .fr addresses.