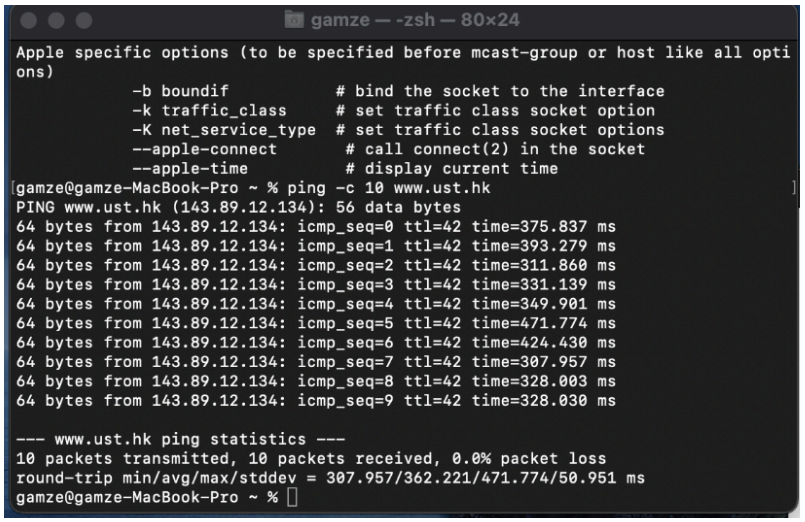
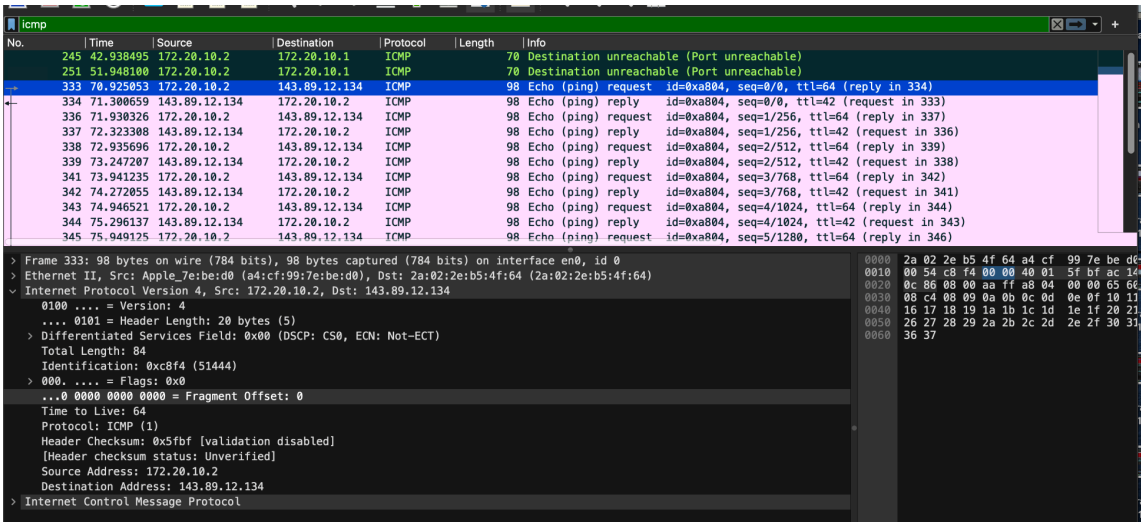
1. What is the IP address of your host? What is the IP address of the destination host?

- Host IP address: 172.20.10.2
- Destination IP address: 143.89.12.134

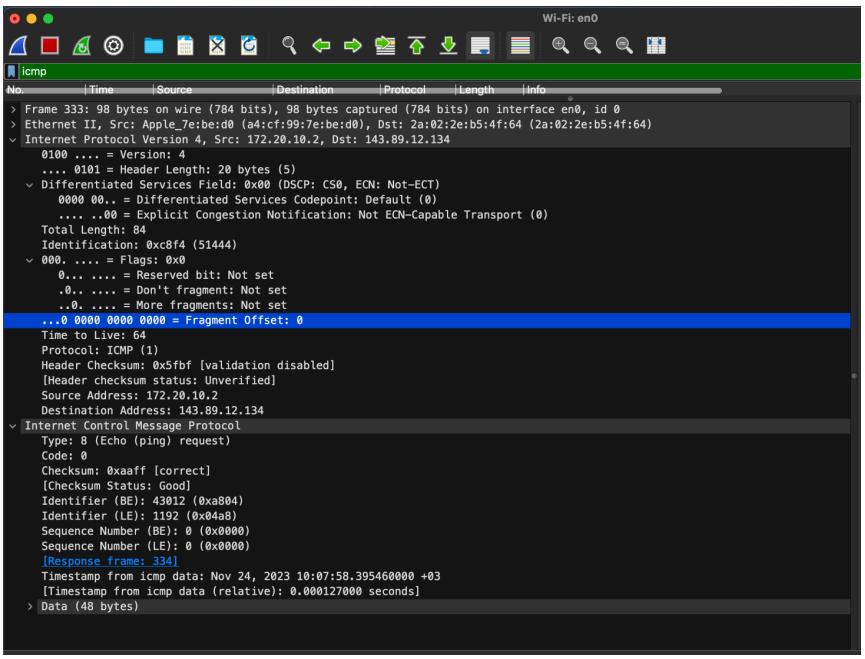




2. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP wasn't created for use between application layer processes but instead used for exchanging network layer information between hosts and routers.

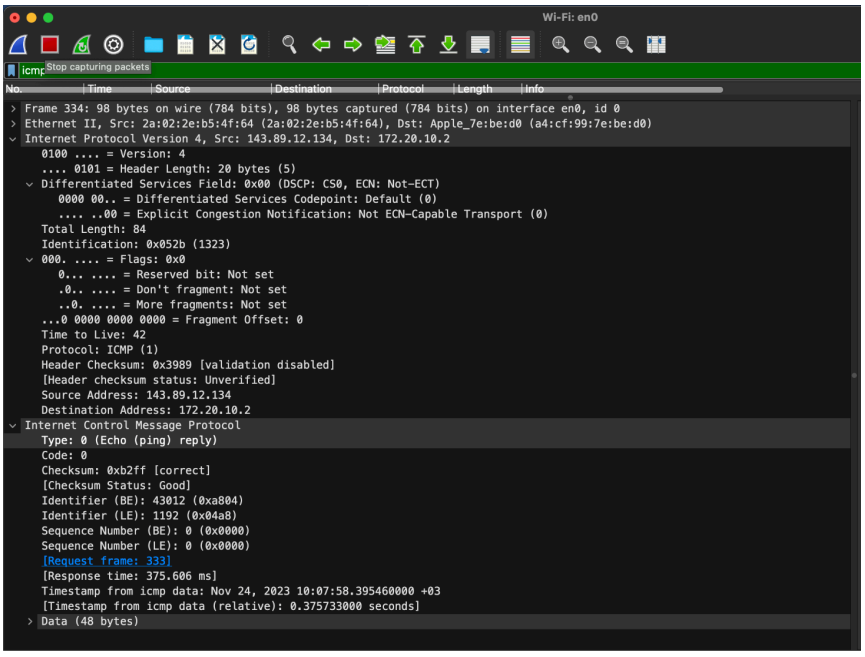
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields?



- Type: 8 (Echo (ping) request)
- Code: 0
- Other fields from this ICPM packet:
    - checksum
    - Identifiers
    - Sequence numbers
    - Data fields

Each of these data fields is two 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?



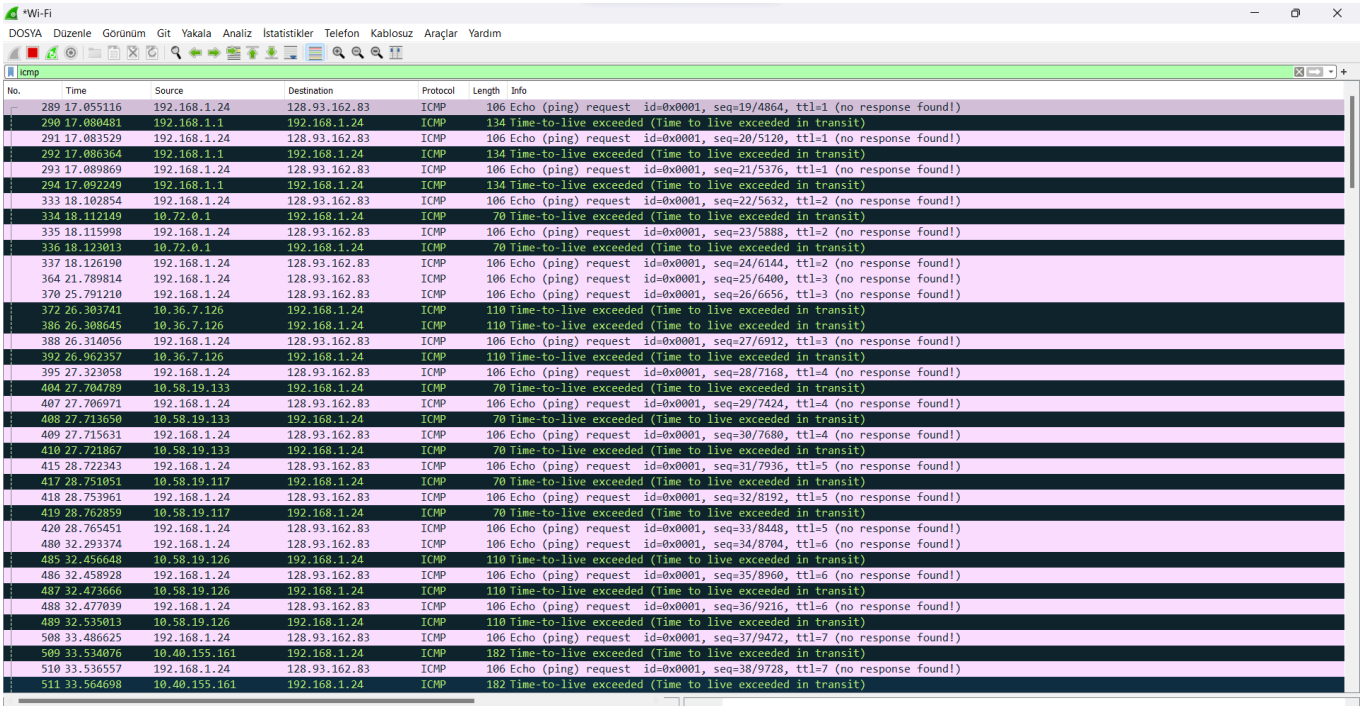
- Type: 0 (Echo (ping) reply)
- Code: 0
- Other fields from this ICPM packet:
    - checksum
    - Identifiers
    - Sequence numbers
    - Data fields

Each of these data fields is two bytes.

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

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

  1    25 ms     3 ms     2 ms  192.168.1.1
  2     9 ms     7 ms     *     10.72.0.1
  3     *      517 ms   648 ms  10.36.7.126
  4   382 ms     6 ms     6 ms  10.58.19.133
  5    29 ms     9 ms     *     10.58.19.117
  6   163 ms    15 ms    58 ms  10.58.19.126
  7    47 ms    28 ms     *     10.40.155.161
  8    21 ms     *        *     10.40.141.73
  9   665 ms    18 ms    15 ms  10.40.170.219
 10   552 ms   496 ms   642 ms  67.220.148.193
 11   528 ms  1872 ms  1084 ms  213.200.119.214
 12   915 ms    78 ms    65 ms  77.67.123.206
 13  2388 ms    59 ms  1204 ms  193.51.177.107
 14  1526 ms   730 ms    75 ms  193.51.184.177
 15    63 ms    57 ms    62 ms  192.93.122.19
 16    64 ms    99 ms   148 ms  128.93.162.83
```




```
No.     Time           Source                Destination           Protocol Length Info
    293 17.089869      192.168.1.24          128.93.162.83         ICMP     106    Echo (ping) request  id=0x0001, seq=21/5376, ttl=1 (no
response found!)
Frame 293: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{91D046C6-D7DA-47BD-A238-95655C493B71}, id 0
Ethernet II, Src: IntelCor_44:ac:c8 (c8:b2:9b:44:ac:c8), Dst: HuaweiTe_87:da:4f (f0:c8:50:87:da:4f)
Internet Protocol Version 4, Src: 192.168.1.24, Dst: 128.93.162.83
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 92
    Identification: 0xc995 (51605)
    000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.24
    Destination Address: 128.93.162.83
Internet Control Message Protocol
```

Source	Destination
192.168.1.24	128.93.162.83

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, it won't be 01 for the probe packets. It would be 0x11. This is because the protocol number in the IP header needs to accurately reflect the protocol used in the payload of the IP packet.

7. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP ping packet. What is included in those fields?
They both have the IP header and the first 8 bytes from the original ICMP packet that caused the error.

```
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (
   Total Length: 92
   Identification: 0xc995 (51605)
 ▾ 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment Offset: 0
 ▾ Time to Live: 1
   › [Expert Info (Note/Sequence): "Time To Live" only 1]
   Protocol: ICMP (1)
   Header Checksum: 0x0b9b [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.1.24
   Destination Address: 128.93.162.83
▾ Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0xf7e9 [unverified] [in ICMP error packet]
   [Checksum Status: Unverified]
   Identifier (BE): 1 (0x0001)
   Identifier (LE): 256 (0x0100)
   Sequence Number (BE): 21 (0x0015)
   Sequence Number (LE): 5376 (0x1500)
 › Data (64 bytes)
```

8. Within the traceroute measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in your figure, 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?
In my screenshot, we can see, specifically, notice the high round-trip times (RTTs) at hops 3, 4, 9, 10, 11, 12, and 13. The link is from New York to France.

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

  1    25 ms     3 ms     2 ms  192.168.1.1
  2     9 ms     7 ms     *     10.72.0.1
  3     *      517 ms   648 ms  10.36.7.126
  4   382 ms     6 ms     6 ms  10.58.19.133
  5    29 ms     9 ms     *     10.58.19.117
  6   163 ms    15 ms    58 ms  10.58.19.126
  7    47 ms    28 ms     *     10.40.155.161
  8    21 ms     *        *     10.40.141.73
  9   665 ms    18 ms    15 ms  10.40.170.219
 10   552 ms   496 ms   642 ms  67.220.148.193
 11   528 ms  1872 ms  1084 ms  213.200.119.214
 12   915 ms    78 ms    65 ms  77.67.123.206
 13  2388 ms    59 ms  1204 ms  193.51.177.107
 14  1526 ms   730 ms    75 ms  193.51.184.177
 15    63 ms    57 ms    62 ms  192.93.122.19
 16    64 ms    99 ms   148 ms  128.93.162.83

Trace complete.
```