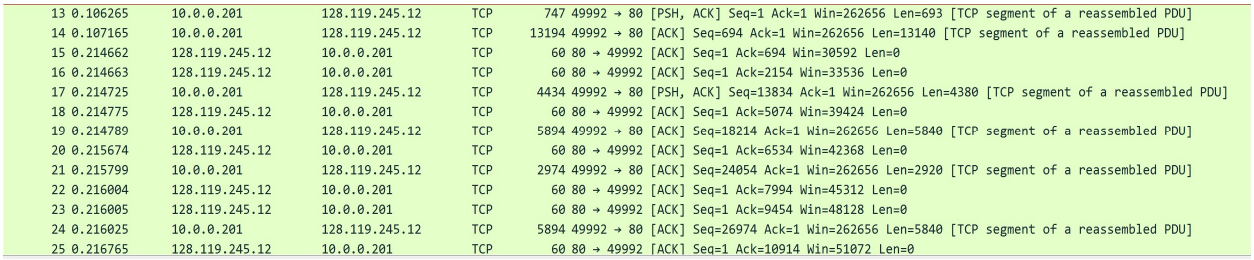
Alex Banning

Wireshark Lab 2 – Computer Networks

November 7, 2019

PART 1:

a) What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?



13	0.106265	10.0.0.201	128.119.245.12	TCP	747 49992 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=693 [TCP segment of a reassembled PDU]
14	0.107165	10.0.0.201	128.119.245.12	TCP	13194 49992 → 80 [ACK] Seq=694 Ack=1 Win=262656 Len=13140 [TCP segment of a reassembled PDU]
15	0.214662	128.119.245.12	10.0.0.201	TCP	60 80 → 49992 [ACK] Seq=1 Ack=694 Win=30592 Len=0
16	0.214663	128.119.245.12	10.0.0.201	TCP	60 80 → 49992 [ACK] Seq=1 Ack=2154 Win=33536 Len=0
17	0.214725	10.0.0.201	128.119.245.12	TCP	4434 49992 → 80 [PSH, ACK] Seq=13834 Ack=1 Win=262656 Len=4380 [TCP segment of a reassembled PDU]
18	0.214775	128.119.245.12	10.0.0.201	TCP	60 80 → 49992 [ACK] Seq=1 Ack=5074 Win=39424 Len=0
19	0.214789	10.0.0.201	128.119.245.12	TCP	5894 49992 → 80 [ACK] Seq=18214 Ack=1 Win=262656 Len=5840 [TCP segment of a reassembled PDU]
20	0.215674	128.119.245.12	10.0.0.201	TCP	60 80 → 49992 [ACK] Seq=1 Ack=6534 Win=42368 Len=0
21	0.215799	10.0.0.201	128.119.245.12	TCP	2974 49992 → 80 [ACK] Seq=24054 Ack=1 Win=262656 Len=2920 [TCP segment of a reassembled PDU]
22	0.216004	128.119.245.12	10.0.0.201	TCP	60 80 → 49992 [ACK] Seq=1 Ack=7994 Win=45312 Len=0
23	0.216005	128.119.245.12	10.0.0.201	TCP	60 80 → 49992 [ACK] Seq=1 Ack=9454 Win=48128 Len=0
24	0.216025	10.0.0.201	128.119.245.12	TCP	5894 49992 → 80 [ACK] Seq=26974 Ack=1 Win=262656 Len=5840 [TCP segment of a reassembled PDU]
25	0.216765	128.119.245.12	10.0.0.201	TCP	60 80 → 49992 [ACK] Seq=1 Ack=10914 Win=51072 Len=0

Client IP Address: 10.0.0.201

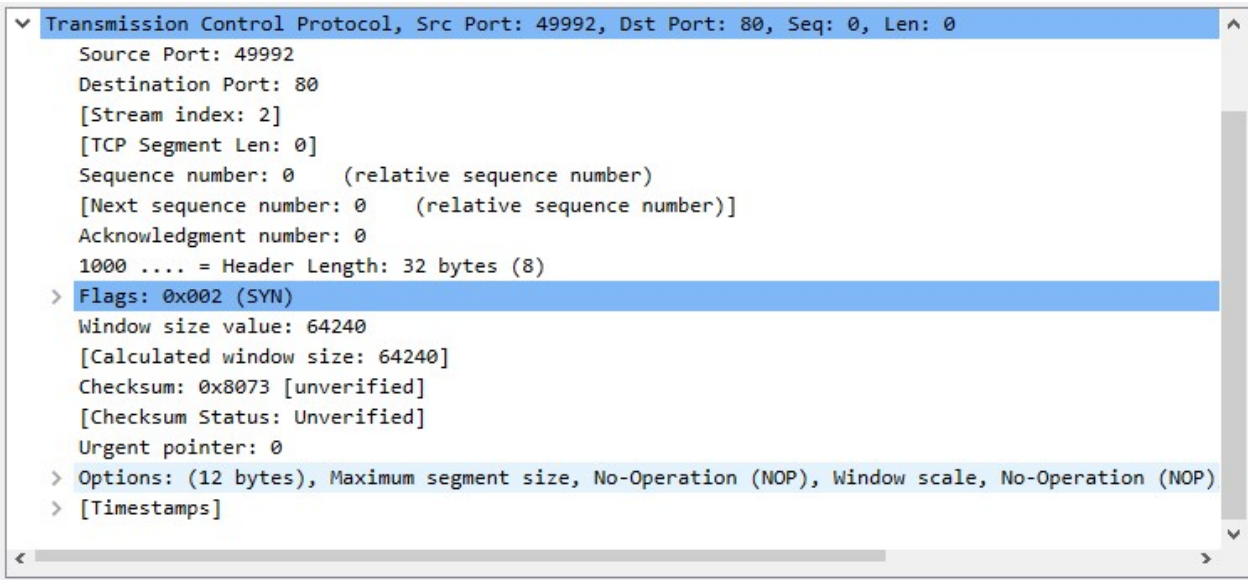
Port Client: 49992

b) What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Server IP Address: 128.119.245.12

Port Server: 80

c) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

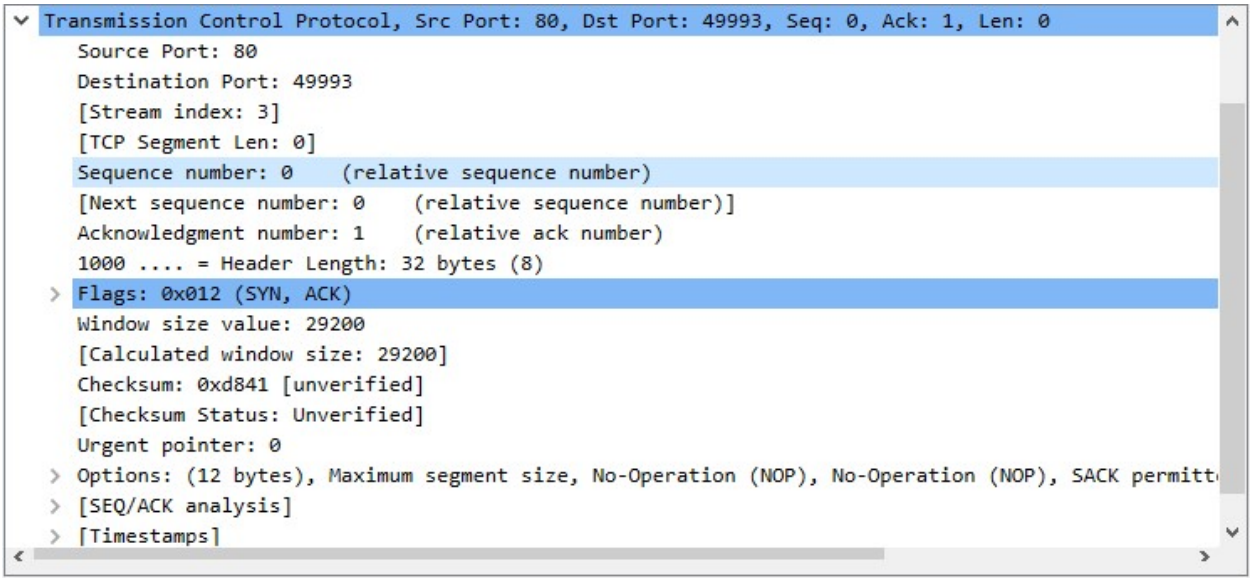


```
Transmission Control Protocol, Src Port: 49992, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 49992
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x8073 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP)
  > [Timestamps]
```

Sequence Number: 0

The flags designate the segment as a SYN segment.

d) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

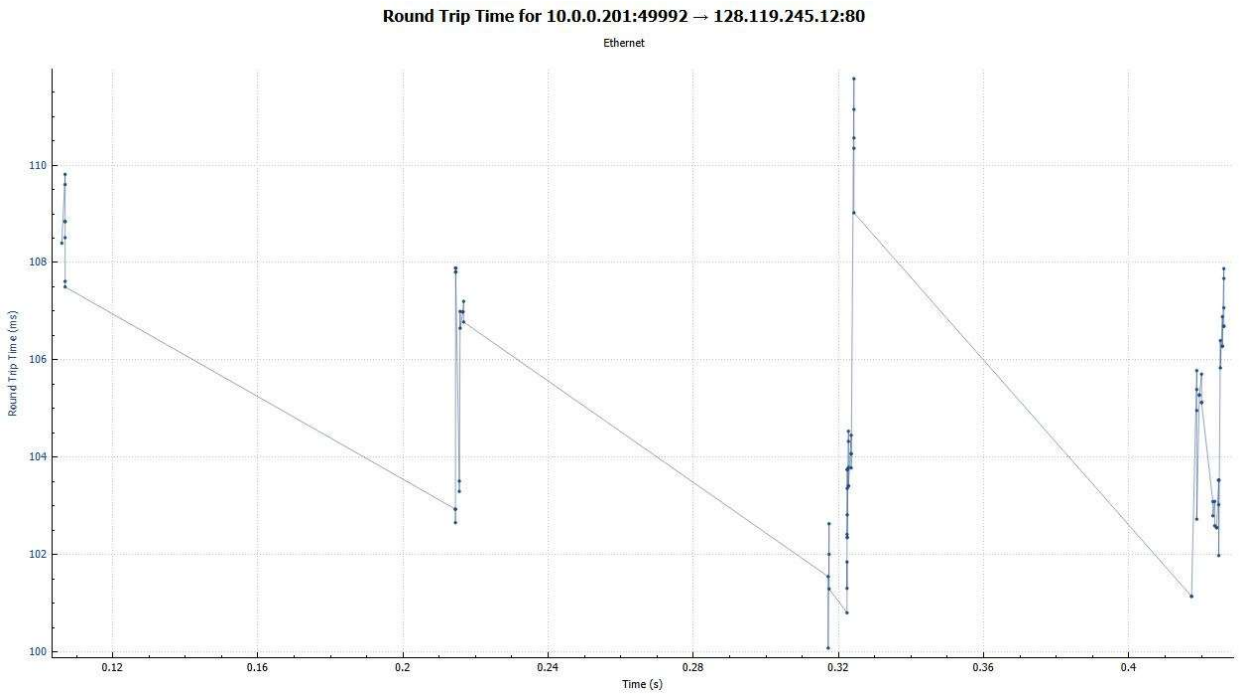


Sequence Number: 0

ACK Flag = 1

The flags indicate 0x012. 0x01 is ACK=1, and 0x002 is SYN=1.

e) Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select the first TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics >TCP Stream Graph- >Round Trip Time Graph. Include this graph in your report and determine which two packets have the longest and shortest RTT.



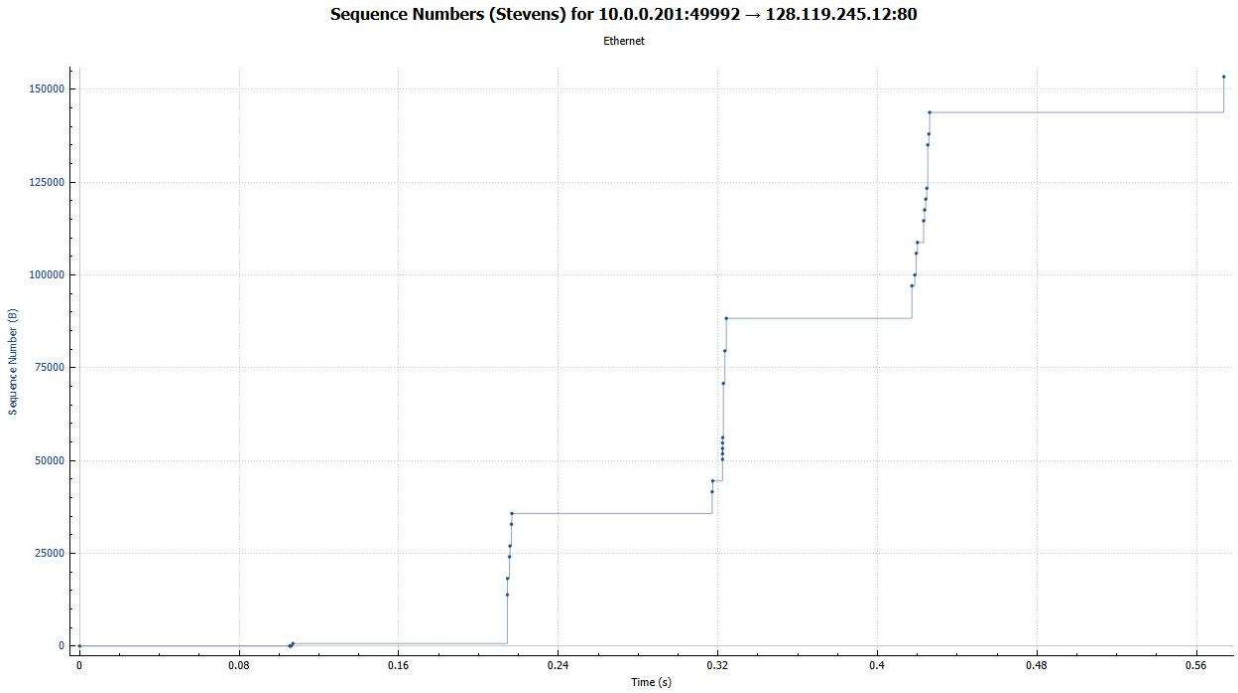
f) What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

```
Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Technico_c6:ba:3e (80:d0:4a:c6:ba:3e), Dst: AsustekC_c4:7c:b1 (4c:ed:fb:c4:7c:b1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.201
Transmission Control Protocol, Src Port: 80, Dst Port: 49992, Seq: 1, Ack: 694, Len: 0
    Source Port: 80
    Destination Port: 49992
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 694    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window size value: 239
    [Calculated window size: 30592]
    [Window size scaling factor: 128]
    Checksum: 0xe72f [unverified]
    [Checksum Status: Unverified]
```

Minimum Buffer Space: 30,592 bytes

No, the lack of buffer space does not throttle the sender.

g) Select the first TCP segment in the Wireshark's "listing of captured-packets" window. Then select the menu: Statistics ->TCP Stream Graph -> Time-Sequence -> Graph(Stevens). You should see a plot that looks similar to the following plot.



There are no places to identify slow start in this graph. The increase in each sequence number tells us that no segments were retransmitted.

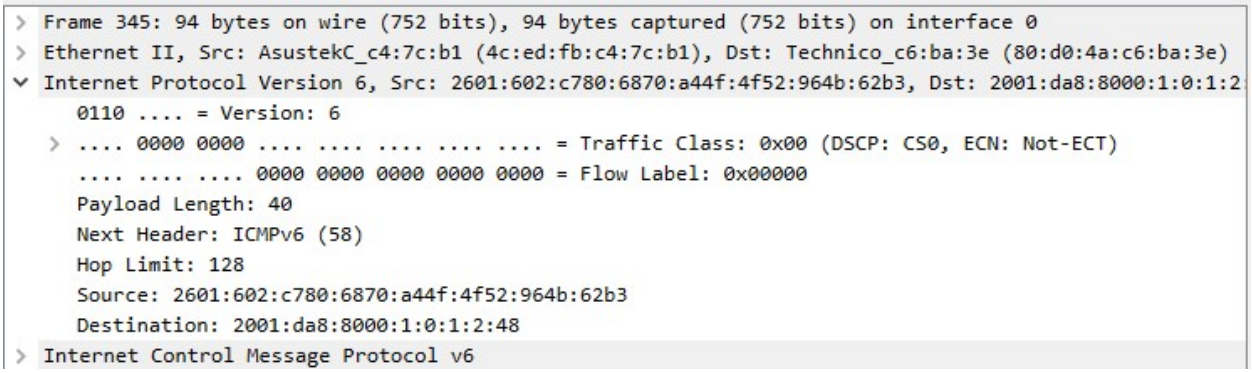
If slow start occurs anywhere, it would be between 0 and 0.21. Everywhere else, there is congestion avoidance occurring.

PART 2:

```
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\abanning>ping -n 10 en.sjtu.edu.cn

Pinging en.sjtu.edu.cn [2001:da8:8000:1:0:1:2:48] with 32 bytes of data:
Reply from 2001:da8:8000:1:0:1:2:48: time=220ms
Reply from 2001:da8:8000:1:0:1:2:48: time=220ms
Reply from 2001:da8:8000:1:0:1:2:48: time=221ms
Reply from 2001:da8:8000:1:0:1:2:48: time=221ms
Reply from 2001:da8:8000:1:0:1:2:48: time=220ms
Reply from 2001:da8:8000:1:0:1:2:48: time=219ms
Reply from 2001:da8:8000:1:0:1:2:48: time=220ms
Reply from 2001:da8:8000:1:0:1:2:48: time=222ms
Reply from 2001:da8:8000:1:0:1:2:48: time=219ms
Reply from 2001:da8:8000:1:0:1:2:48: time=219ms

Ping statistics for 2001:da8:8000:1:0:1:2:48:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 219ms, Maximum = 222ms, Average = 220ms

C:\Users\abanning>
```

a) What is the IP address of your host? What is the IP address of the destination host?

When using the ping program on international websites like this one, my computer/router uses IPv6. My ICMP version is therefore also v6, so my answers for this section display that.



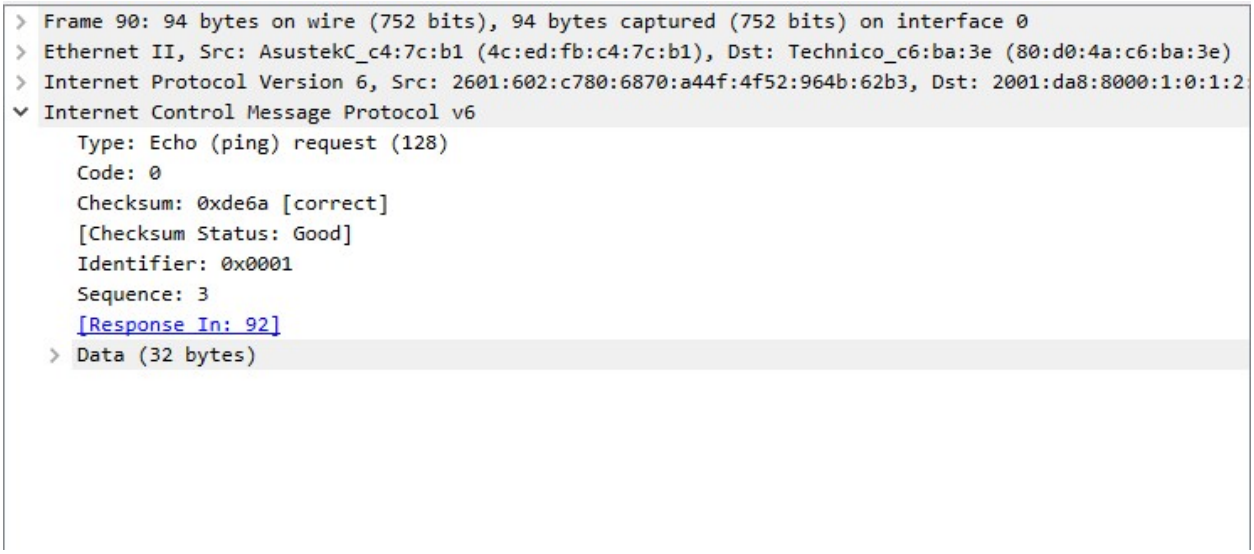
Host IP: 2601:602:c780:6870:a44f:4f52:964b:62b3

Destination IP: 2001:da8:8000:1:0:1:2:48

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

ICMP packet does not require a port number because it is not an application-layer protocol. It is meant to communicate on the network layer, so it only needs IPs.

c) 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?



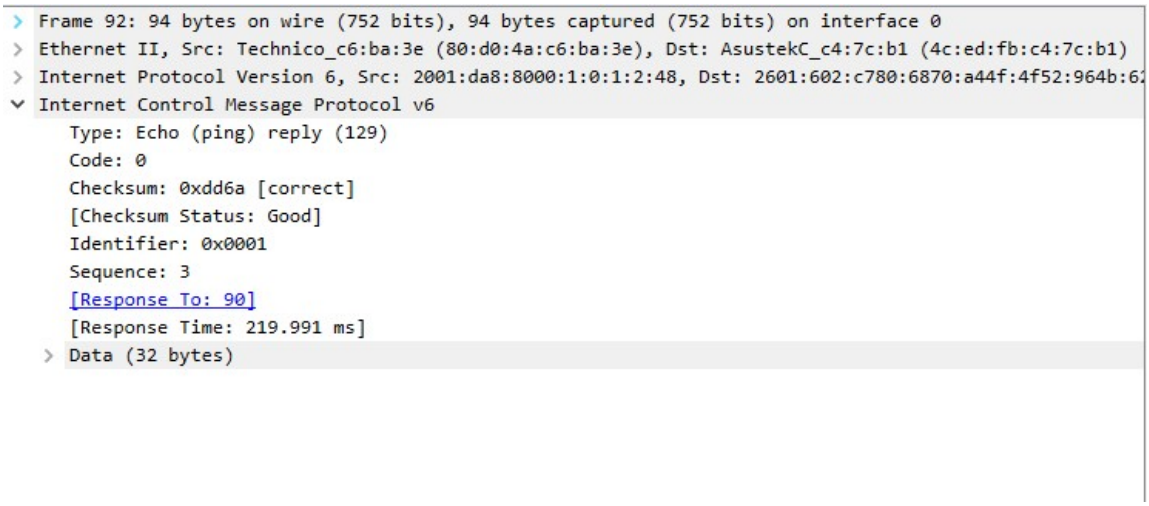
Type: 128 (Echo (ping) request) → This is the IPv6 version. If I recall correctly, IPv4 Type for Echo ping request is 8.

Code: 0

Other fields: Checksum=0xde6a (correct), Identifier=0x0001, Sequence#=3, Response#=92, and the Data.

These are all two bytes per field, except for the data.

d) 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: 129 (Echo (ping) reply) → IPv4 = 0

Code: 0

Other fields: Checksum=0xdd6a(correct), Identifier=0x0001, Sequence#=3, ResponseTo#=90, ResponseTime=219.991ms, and the Data.

These are all two bytes

PART 3:

```
C:\Users\abanning>tracert en.sjtu.edu.cn

Tracing route to en.sjtu.edu.cn [2001:da8:8000:1:0:1:2:48]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  2601:602:c780:6870:82d0:4aff:fec6:ba3e
  2    15 ms    14 ms    17 ms  2001:558:4082:d6::1
  3     7 ms     9 ms     6 ms  po-301-1222-rur02.spokane.wa.seattle.comcast.net [2001:558:a2:2071::1]
  4    15 ms    15 ms    15 ms  be-37-ar01.seattle.wa.seattle.comcast.net [2001:558:a0:2e::1]
  5     *        *        *     Request timed out.
  6     *       14 ms     *     be-10847-pe02.seattle.wa.ibone.comcast.net [2001:558:0:f5b8::2]
  7    16 ms    16 ms    16 ms  10gigabitethernet2-12.core1.sea1.he.net [2001:470:0:3c5::1]
  8    31 ms    17 ms    17 ms  100ge15-1.core1.pdx1.he.net [2001:470:0:3c2::2]
  9    44 ms    39 ms    59 ms  100ge5-1.core1.lax2.he.net [2001:470:0:229::1]
 10     *        *        *     Request timed out.
 11   194 ms   197 ms   194 ms  cernet2.net [2001:252:0:302::1]
 12     *        *        *     Request timed out.
 13   200 ms   196 ms   196 ms  cernet2.net [2001:252:0:1::1]
 14   198 ms   198 ms   198 ms  2001:da8:2:2::2
 15   205 ms   204 ms   203 ms  2001:da8:2:27::2
 16   221 ms   221 ms   229 ms  2001:da8:2:11::1
 17   221 ms   220 ms   220 ms  2001:da8:2:103::2
 18   221 ms   221 ms   221 ms  cernet2.net [2001:da8:a4:2::2]
 19   223 ms   221 ms   219 ms  2001:da8:8000:102::206
 20   221 ms   219 ms   220 ms  2001:da8:8000:12f::2
 21   221 ms   222 ms   224 ms  2001:da8:8000:80e::2
 22   220 ms   220 ms   222 ms  2001:da8:8000:1:202:120:2:21
 23   222 ms   219 ms     *     2001:da8:8000:1:0:1:2:48
 24     *      219 ms   220 ms  2001:da8:8000:1:0:1:2:48

Trace complete.
```

No.	Time	Source	Destination	Protocol	Length	Info
5	0.564622	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=11, hop limit=1 (no response found!)
6	0.565522	2601:602:c780:6870:…	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
7	0.566088	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=12, hop limit=1 (no response found!)
8	0.566434	2601:602:c780:6870:…	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
9	0.566875	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=13, hop limit=1 (no response found!)
10	0.567108	2601:602:c780:6870:…	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
25	2.433321	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=14, hop limit=2 (no response found!)
26	2.448990	2001:558:4082:d6::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
27	2.449604	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=15, hop limit=2 (no response found!)
28	2.464131	2001:558:4082:d6::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
29	2.464829	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=16, hop limit=2 (no response found!)
30	2.481917	2001:558:4082:d6::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
33	3.509503	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=17, hop limit=3 (no response found!)
34	3.516729	2001:558:a2:2071::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
35	3.517350	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=18, hop limit=3 (no response found!)
36	3.527237	2001:558:a2:2071::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
37	3.527790	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=19, hop limit=3 (no response found!)
38	3.534565	2001:558:a2:2071::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
42	4.573459	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=20, hop limit=4 (no response found!)
43	4.588416	2001:558:a0:2e::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
44	4.589148	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=21, hop limit=4 (no response found!)
45	4.604137	2001:558:a0:2e::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
46	4.604949	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=22, hop limit=4 (no response found!)
47	4.620574	2001:558:a0:2e::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
52	5.650453	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=23, hop limit=5 (no response found!)
59	9.462491	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=24, hop limit=5 (no response found!)
71	13.462144	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=25, hop limit=5 (no response found!)
81	17.463681	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=26, hop limit=6 (no response found!)
93	21.462987	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=27, hop limit=6 (no response found!)
94	21.477536	2001:558:0:f5b8::2	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
95	21.478135	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=28, hop limit=6 (no response found!)
103	25.486899	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=29, hop limit=7 (no response found!)
104	25.503354	2001:470:0:3c5::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
105	25.504156	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=30, hop limit=7 (no response found!)
106	25.520207	2001:470:0:3c5::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
107	25.520854	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=31, hop limit=7 (no response found!)
108	25.537119	2001:470:0:3c5::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
112	26.583859	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=32, hop limit=8 (no response found!)
113	26.615012	2001:470:0:3c2::2	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
114	26.615693	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=33, hop limit=8 (no response found!)
115	26.633204	2001:470:0:3c2::2	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
116	26.633836	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=34, hop limit=8 (no response found!)
117	26.651627	2001:470:0:3c2::2	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
120	27.689707	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=35, hop limit=9 (no response found!)
121	27.733825	2001:470:0:229::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
123	27.734668	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=36, hop limit=9 (no response found!)
124	27.774553	2001:470:0:229::1	2601:602:c780:6870:…	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
125	27.775364	2601:602:c780:6870:…	2001:da8:8000:1:0:1…	ICMPv6	126	Echo (ping) request id=0x0001, seq=37, hop limit=9 (no response found!)

Not all of the output!

a) What is the IP address of your host? What is the IP address of the target destination host?

Again, this is IPv6 for some reason.

```
> Frame 5: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
> Ethernet II, Src: AsustekC_c4:7c:b1 (4c:ed:fb:c4:7c:b1), Dst: Technico_c6:ba:3e (80:d0:4a:c6:ba:3e)
v Internet Protocol Version 6, Src: 2601:602:c780:6870:a44f:4f52:964b:62b3, Dst: 2001:da8:8000:1:0:1:2
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 72
    Next Header: ICMPv6 (58)
    Hop Limit: 1
    Source: 2601:602:c780:6870:a44f:4f52:964b:62b3
    Destination: 2001:da8:8000:1:0:1:2:48
> Internet Control Message Protocol v6
```

Source IP: 2601:602:c780:6870:a44f:4f52:964b:62b3

Destination IP: 2001:da8:8000:1:0:1:2:48

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

No, if ICMP sent UDP packets instead, the IP protocol number would be 0x11.

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

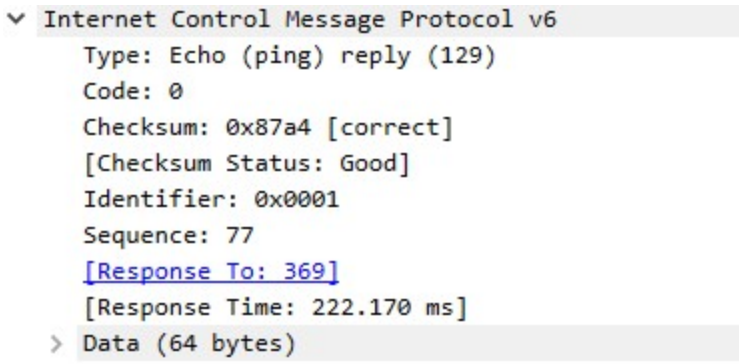
```
Internet Control Message Protocol v6
    Type: Time Exceeded (3)
    Code: 0 (hop limit exceeded in transit)
    Checksum: 0x3727 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  > Internet Protocol Version 6, Src: 2601:602:c780:6870:a44f:4f52:964b:62b3, Dst: 2001:da8:8000:1:
  v Internet Control Message Protocol v6
        Type: Echo (ping) request (128)
        Code: 0
        Checksum: 0x88e6 [unverified] [in ICMP error packet]
        [Checksum Status: Unverified]
        Identifier: 0x0001
        Sequence: 11
      > Data (64 bytes)
```

It has the header and sender/receiver information of the packet that caused the error to occur.

d) Examine the last ICMP packets received by the source host from the target host. How do they differ from the ICMP error packets? Why are they different?

```
Internet Control Message Protocol v6
    Type: Time Exceeded (3)
    Code: 0 (hop limit exceeded in transit)
    Checksum: 0x6901 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  > Internet Protocol Version 6, Src: 2601:602:c780:6870:a44f:4f52:964b:62b3, Dst: 2001:da8:8000:1:
  v Internet Control Message Protocol v6
        Type: Echo (ping) request (128)
        Code: 0
        Checksum: 0x88a5 [unverified] [in ICMP error packet]
        [Checksum Status: Unverified]
        Identifier: 0x0001
        Sequence: 76
      > Data (64 bytes)
```

Last Packet that experiences timeout



First successful ping reply

The difference between these are the type and code. When a timeout occurs, it sends a Type: 3 - Code: 0 (in IPv4 this is Type:11 – Code:0), but when the packet successfully reaches its destination it sends an ICMP message with Type: 129 – Code: 0 (in IPv4 this is Type: 3 – Code: 3).

e) **Within the Traceroute 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?**

Yes, a few of them. The links with significant delays timed out in both cases.