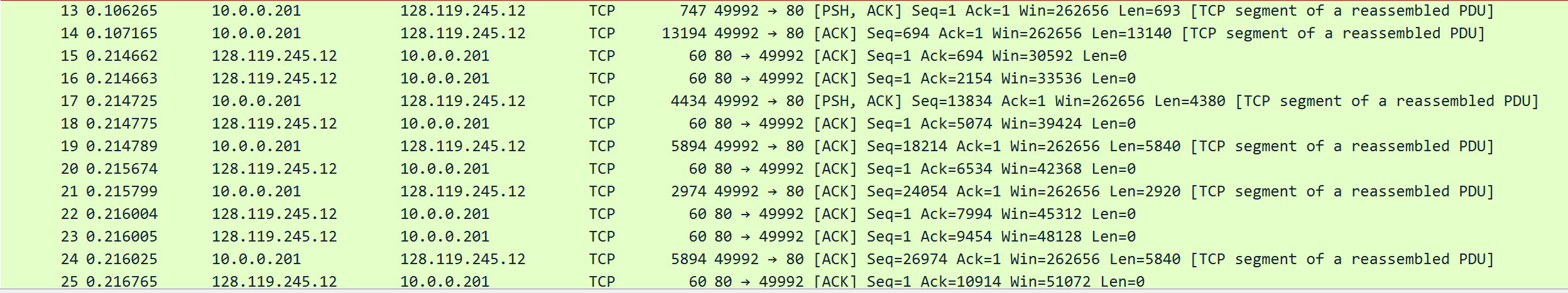
Alex Banning

Wireshark Lab 2 – Computer Networks

November 7, 2019

**PART 1:**

1. 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?



Client IP Address: 10.0.0.201

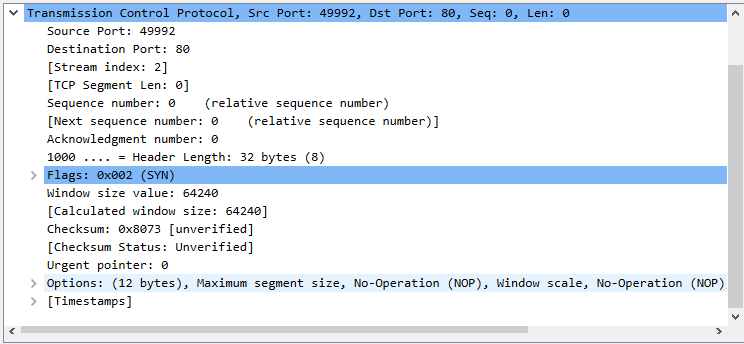
Port Client: 49992

1. 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

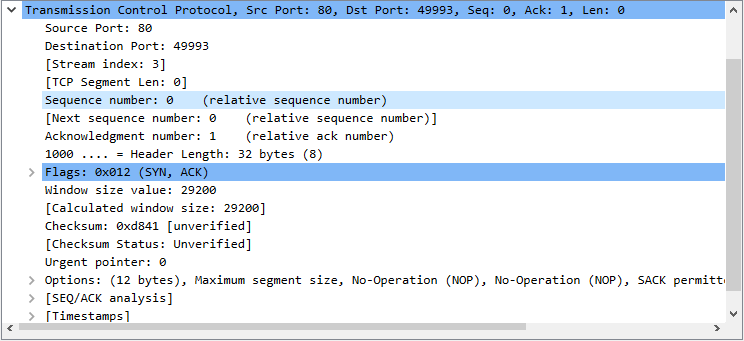
1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?



Sequence Number: 0

The flags designate the segment as a SYN segment.

1. 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

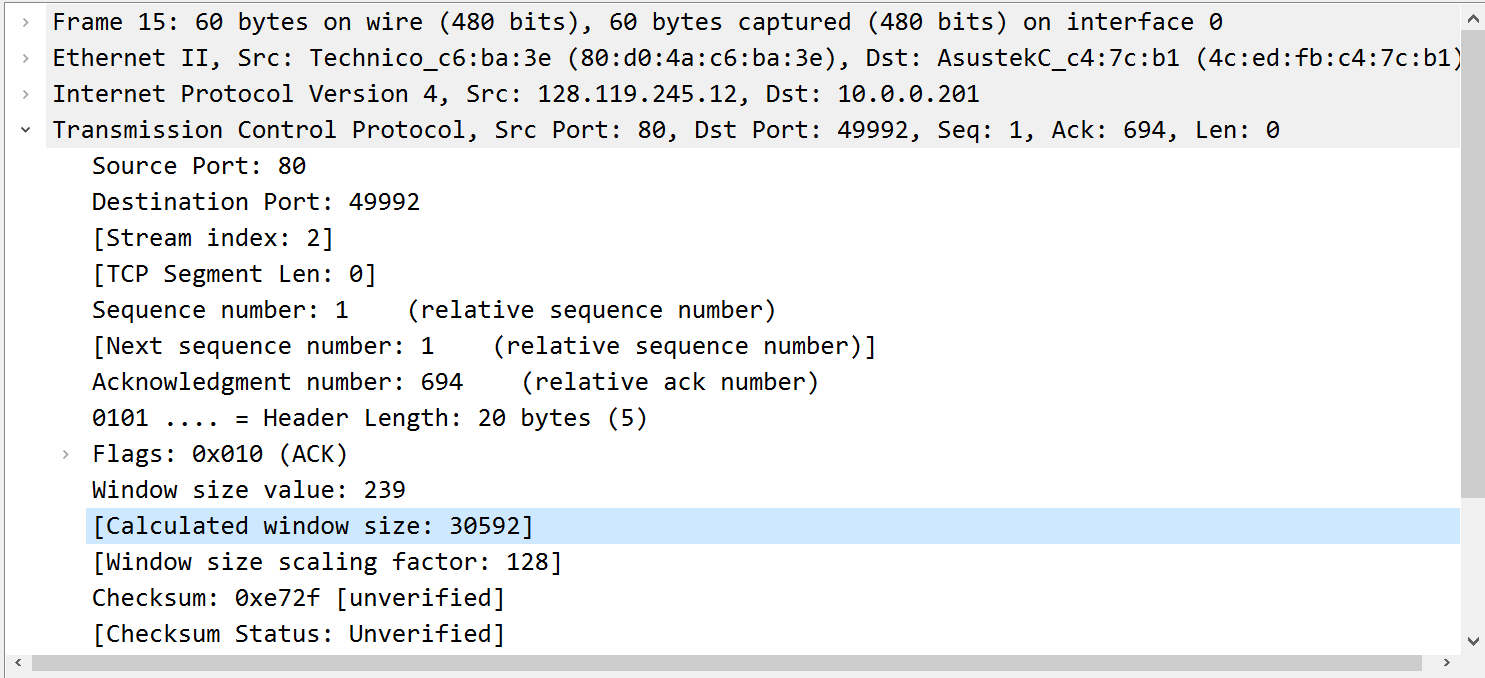
The flags indicate 0x012. 0x01 is ACK=1, and 0x002 is SYN=1.

1. 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.

A close up of a map

Description automatically generated

1. 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?



Minimum Buffer Space: 30,592 bytes

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

1. 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.

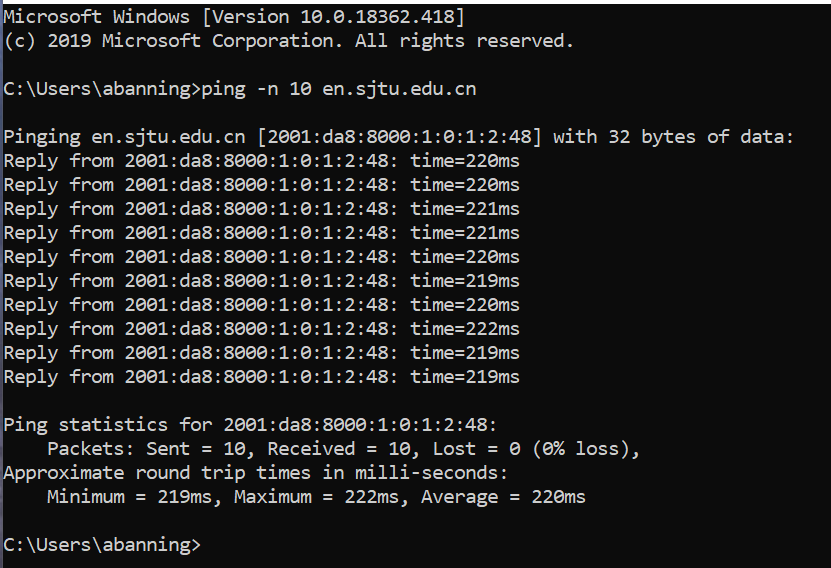
A picture containing text, map

Description automatically generated

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

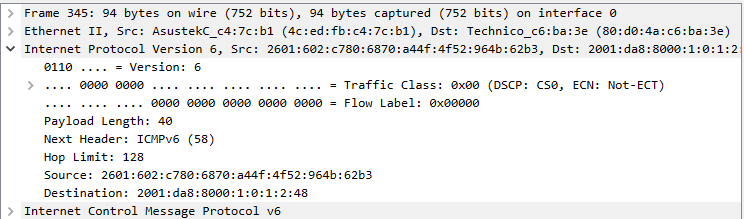
If slow start occurs anywhere, it would be between 0 and 0.21. Everywhere else, there is congestion avoidance occurring.

**PART 2:**



1. **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.



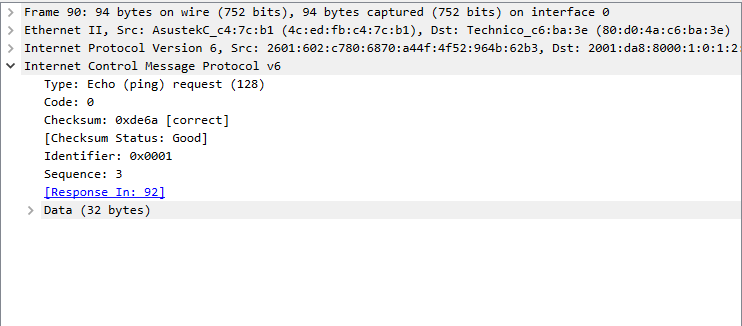
Host IP: 2601:602:c780:6870:a44f:4f52:964b:62b3

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

1. **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.

1. **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?**



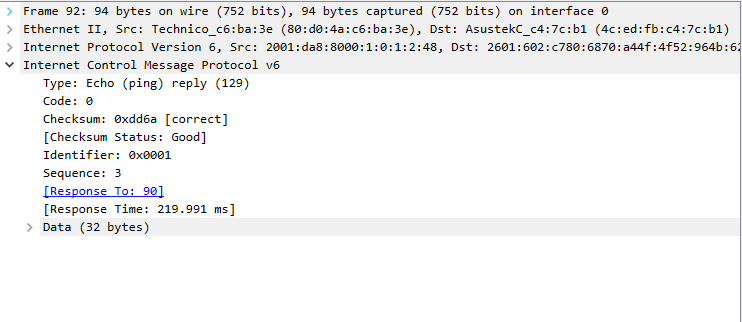
Type: 128 (Echo (ping) request) 🡪 This is the IPv6 version. If I recall correctly, IPv4 Type for Echo ping request is 8.

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.

1. **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?**



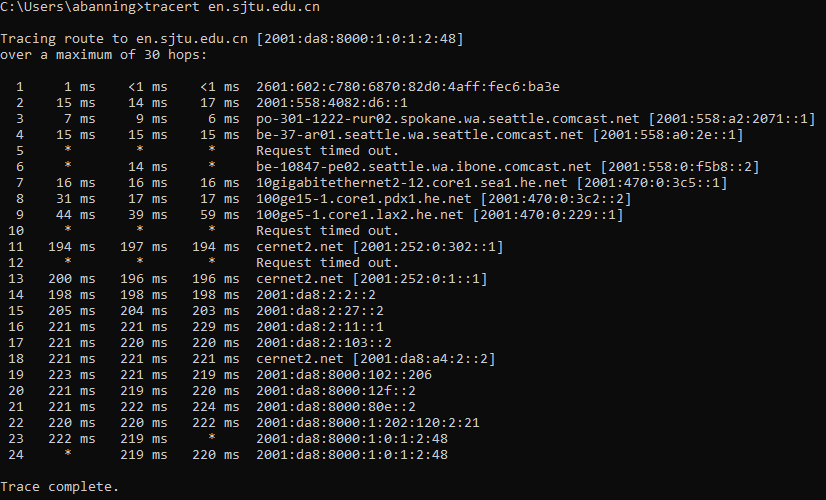
Type: 129 (Echo (ping) reply) 🡪 IPv4 = 0

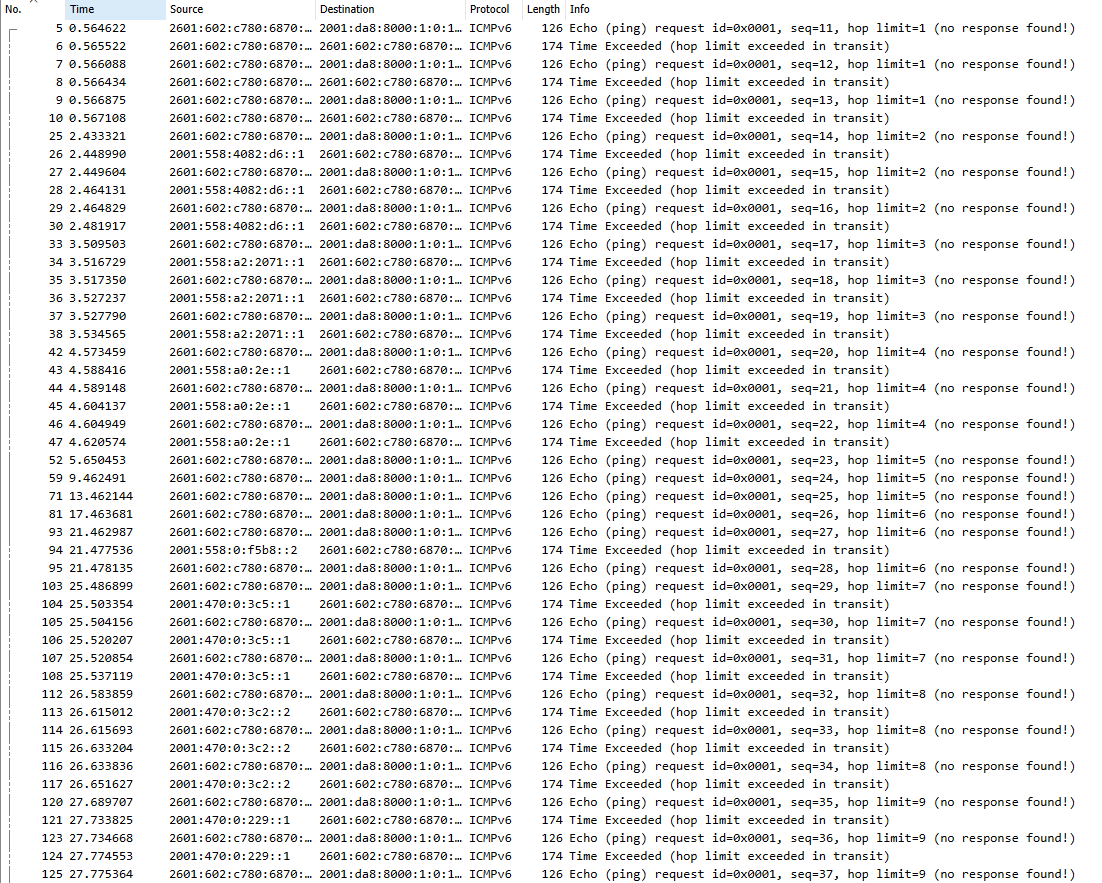
Code: 0

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

These are all two bytes

**PART 3:**

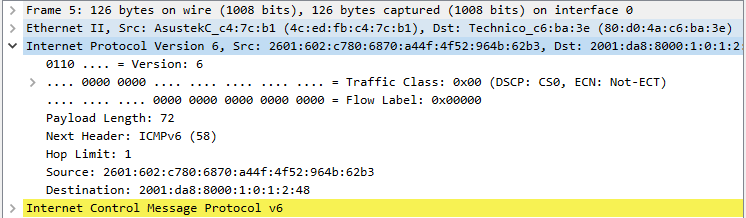




**Not all of the output!**

1. **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.**



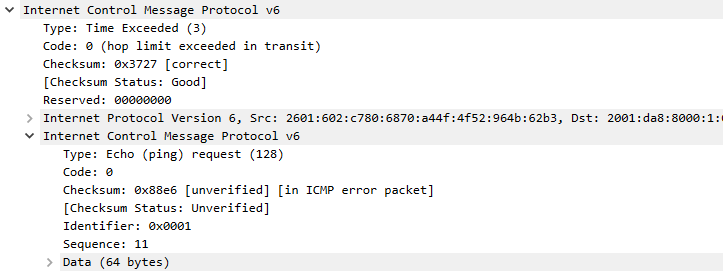
Source IP: 2601:602:c780:6870:a44f:4f52:964b:62b3

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

1. **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?**

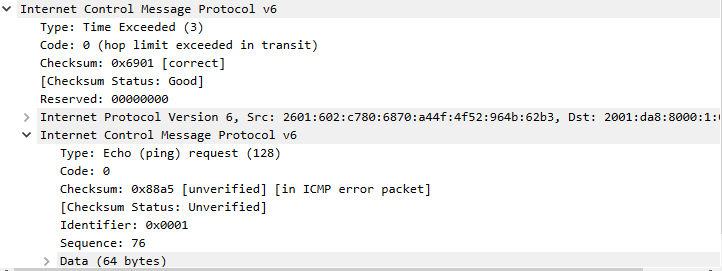
No, if ICMP sent UDP packets instead, the IP protocol number would be 0x11.

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

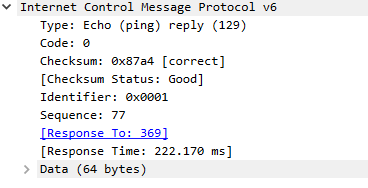


It has the header and sender/receiver information of the packet that caused the error to occur.

1. **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?**



**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).

1. **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.