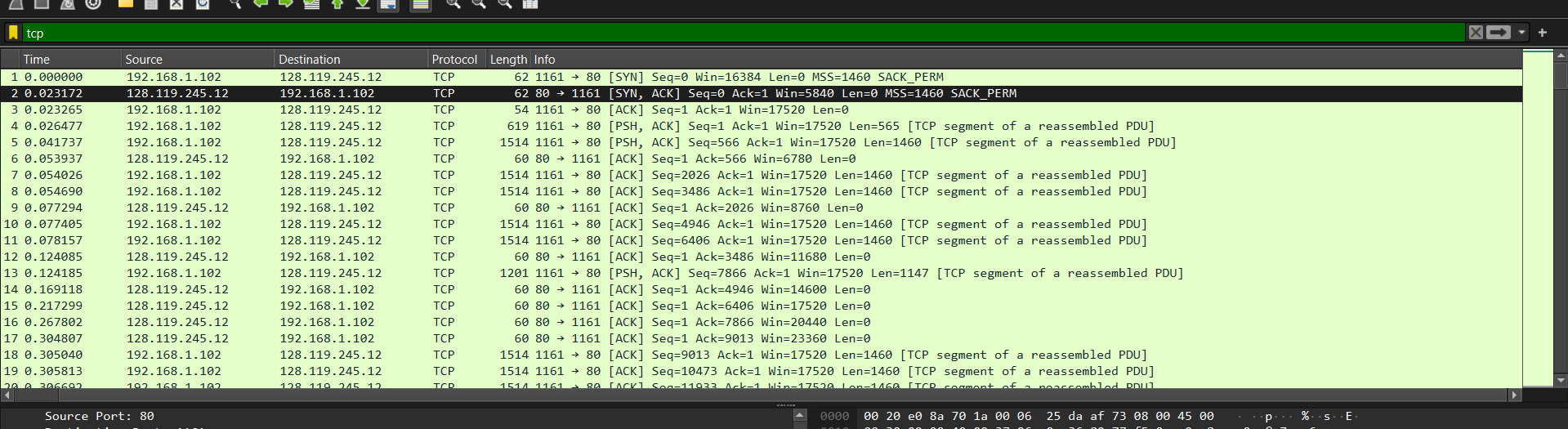
ASSIGNMENT NO.10: WIRESHARK LAB: TCP

Name : Harshavardhan Bamane

PRN : 22510112

1. **Capturing a bulk TCP transfer from your computer to a remote server**



1. **A first look at the captured trace**
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

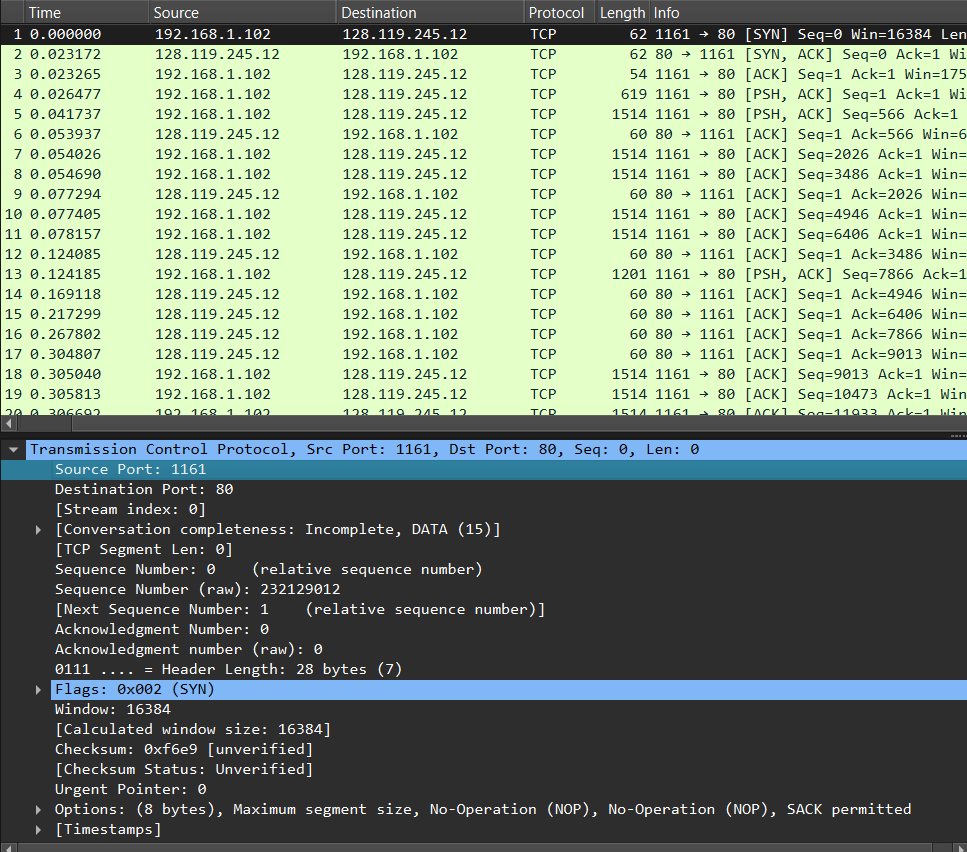
ANS: IP Address : 128.119.245.12

Port Number : 80

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

ANS: IP Address : 192.168.1.102

Port Number : 1161



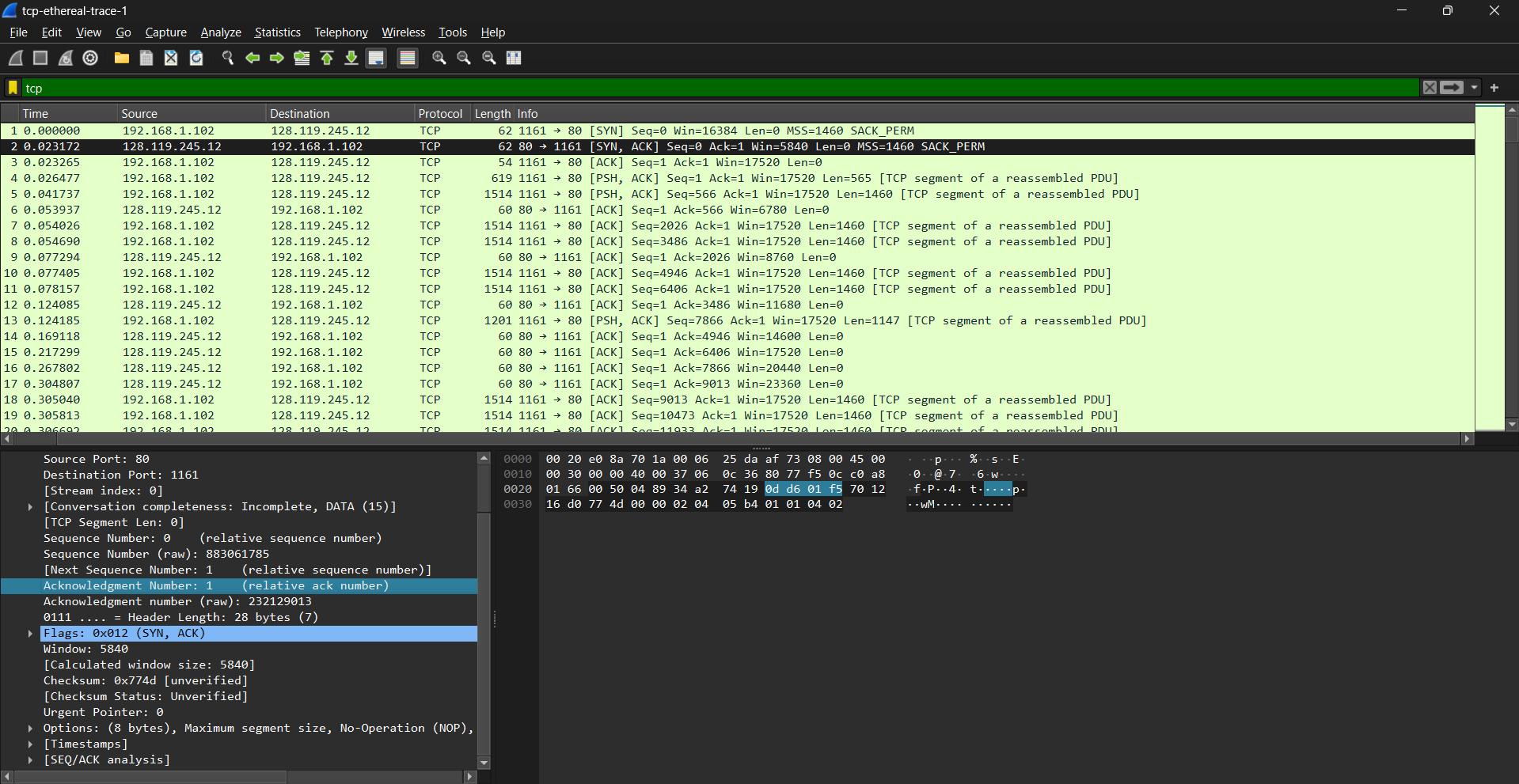
1. **TCP Basics**
2. What is the sequence number of the TCP SYN segment that is used to initiate theTCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

ANS :

Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. The value is 0 in this trace. The SYN flag is set to 1 (segment)

1. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.eduto 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?

ANS:



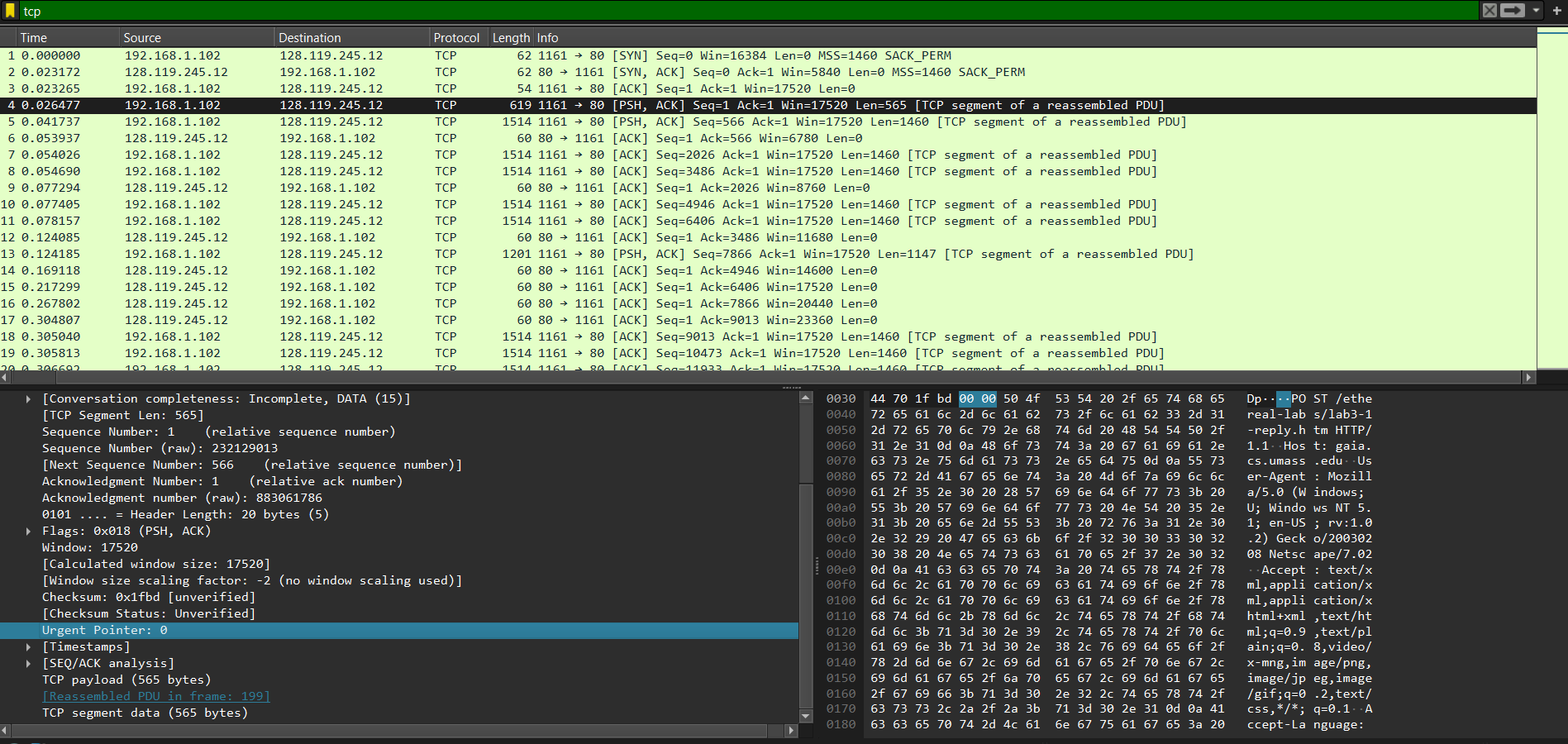
The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.The server adds 1 to SYN segment.

A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement flag in the segment are set to 1.

1. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST

command, you’ll need to dig into [ssthe packet content field at the bottom of the Wireshark window, looking for a segment with“POST” within its DATA field.

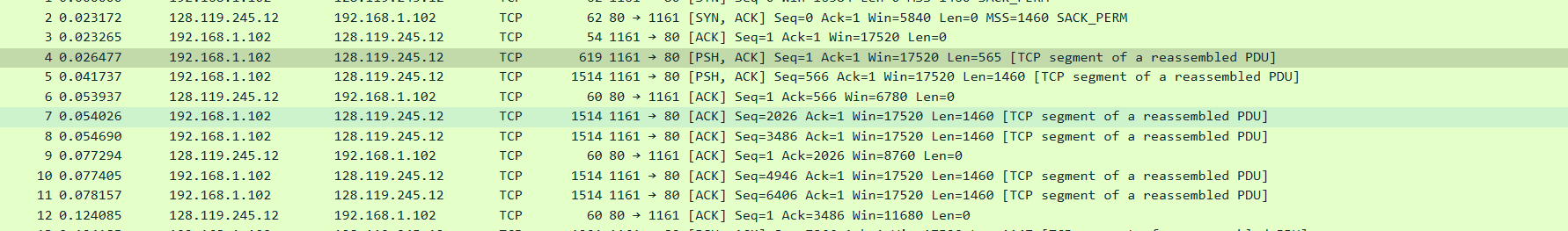
ANS:



The sequence number of the tcp segment containing HTTP POST Command is 1.

1. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection.What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)?

ANS:



* Segment 1 sequence number: 1
* Segment 2 sequence number: 566
* Segment 3 sequence number: 2026
* Segment 4 sequence number: 3486
* Segment 5 sequence number: 4946
* Segment 6 sequence number: 6406

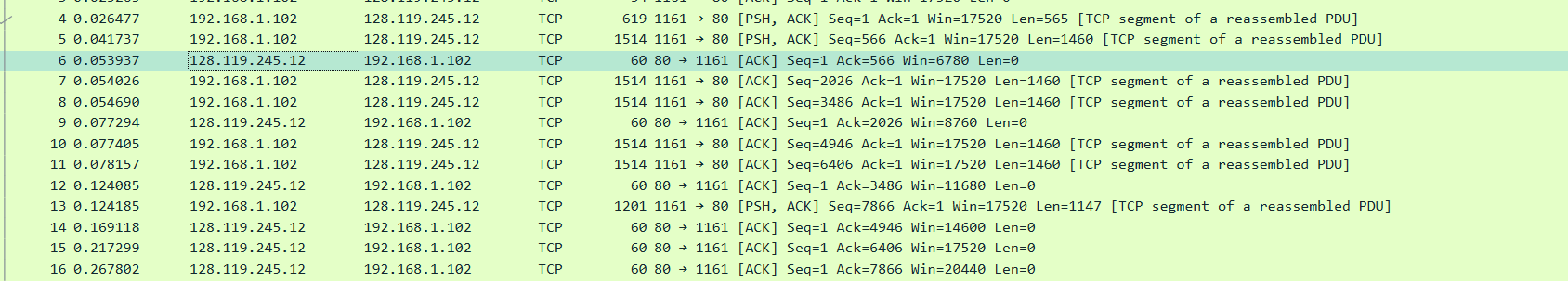
At what time was each segment sent?

ANS:

* Segment 1: 0.026477
* Segment 2: 0.041737
* Segment 3: 0.054026
* Segment 4: 0.054690
* Segment 5: 0.077405
* Segment 6:0.078157

When was the ACK for each segment received?

ANS:



* Segment 1: 0.053937
* Segment 2: 0.077294
* Segment 3: 0.124085
* Segment 4: 0.169118
* Segment 5: 0.217299
* Segment 6: 0.267802

Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments?

ANS:

* Segment 1: 0.02746
* Segment 2: 0.035557
* Segment 3: 0.070059
* Segment 4: 0.11443
* Segment 5: 0.13989
* Segment 6: 0.18964