Gretel Rajamoney

Wireshark Lab #3

May 10, 2021

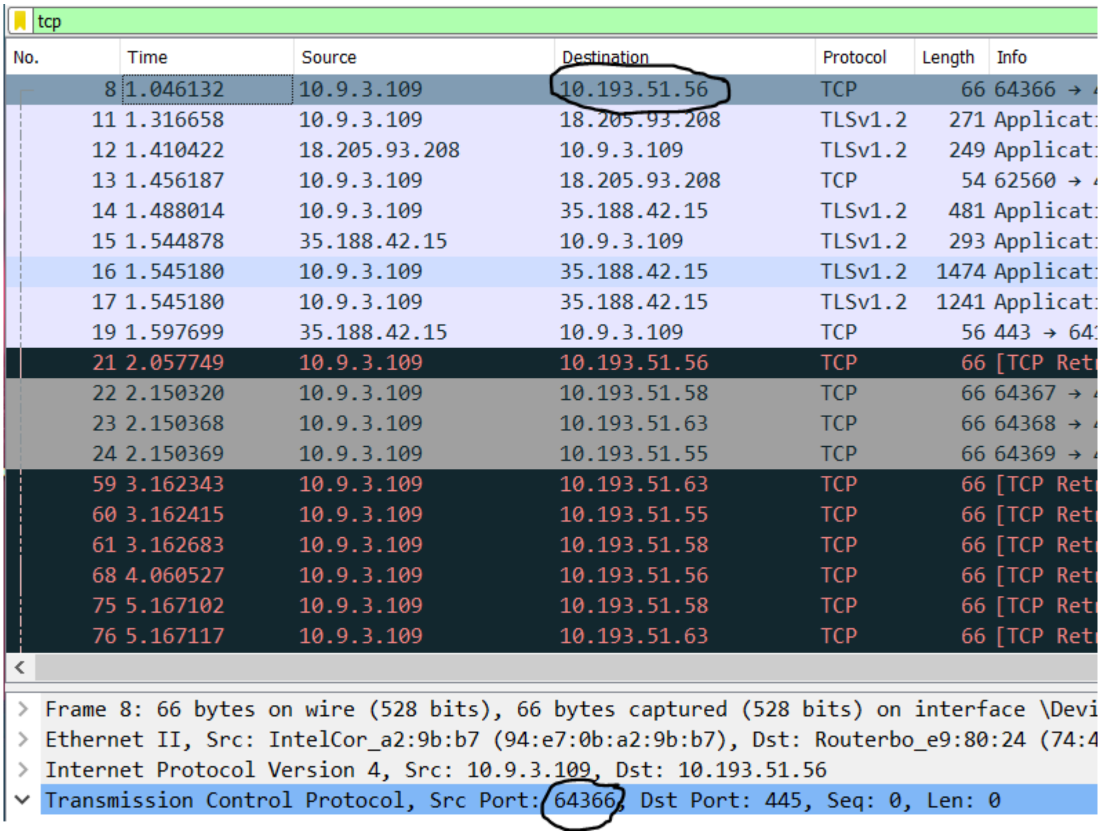
Part 1:

Part 2:

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?

   The IP address: 10.193.51.56

   The TCP port number: 64366

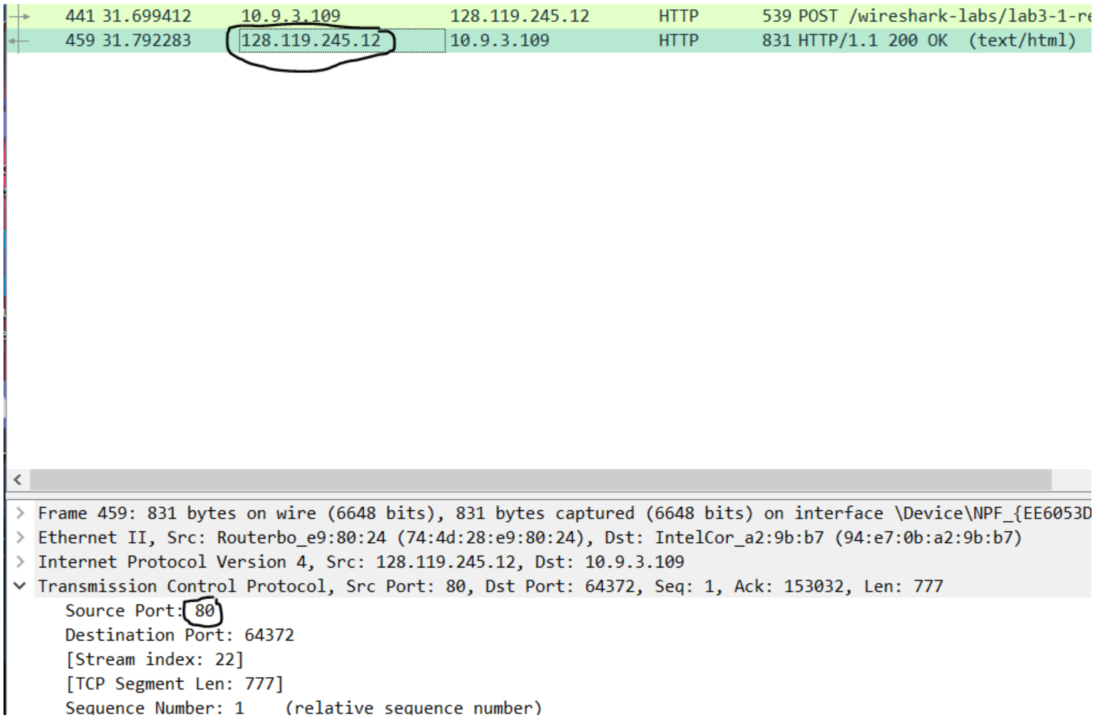


tcp

No.	Time	Source	Destination	Protocol	Length	Info
8	1.046132	10.9.3.109	10.193.51.56	TCP	66	64366 →
11	1.316658	10.9.3.109	18.205.93.208	TLSv1.2	271	Applicat
12	1.410422	18.205.93.208	10.9.3.109	TLSv1.2	249	Applicat
13	1.456187	10.9.3.109	18.205.93.208	TCP	54	62560 →
14	1.488014	10.9.3.109	35.188.42.15	TLSv1.2	481	Applicat
15	1.544878	35.188.42.15	10.9.3.109	TLSv1.2	293	Applicat
16	1.545180	10.9.3.109	35.188.42.15	TLSv1.2	1474	Applicat
17	1.545180	10.9.3.109	35.188.42.15	TLSv1.2	1241	Applicat
19	1.597699	35.188.42.15	10.9.3.109	TCP	56	443 → 64
21	2.057749	10.9.3.109	10.193.51.56	TCP	66	[TCP Ret
22	2.150320	10.9.3.109	10.193.51.58	TCP	66	64367 →
23	2.150368	10.9.3.109	10.193.51.63	TCP	66	64368 →
24	2.150369	10.9.3.109	10.193.51.55	TCP	66	64369 →
59	3.162343	10.9.3.109	10.193.51.63	TCP	66	[TCP Ret
60	3.162415	10.9.3.109	10.193.51.55	TCP	66	[TCP Ret
61	3.162683	10.9.3.109	10.193.51.58	TCP	66	[TCP Ret
68	4.060527	10.9.3.109	10.193.51.56	TCP	66	[TCP Ret
75	5.167102	10.9.3.109	10.193.51.58	TCP	66	[TCP Ret
76	5.167117	10.9.3.109	10.193.51.63	TCP	66	[TCP Ret

```
> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Devi
> Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24 (74:4
> Internet Protocol Version 4, Src: 10.9.3.109, Dst: 10.193.51.56
v Transmission Control Protocol, Src Port: 64366, Dst Port: 445, Seq: 0, Len: 0
```

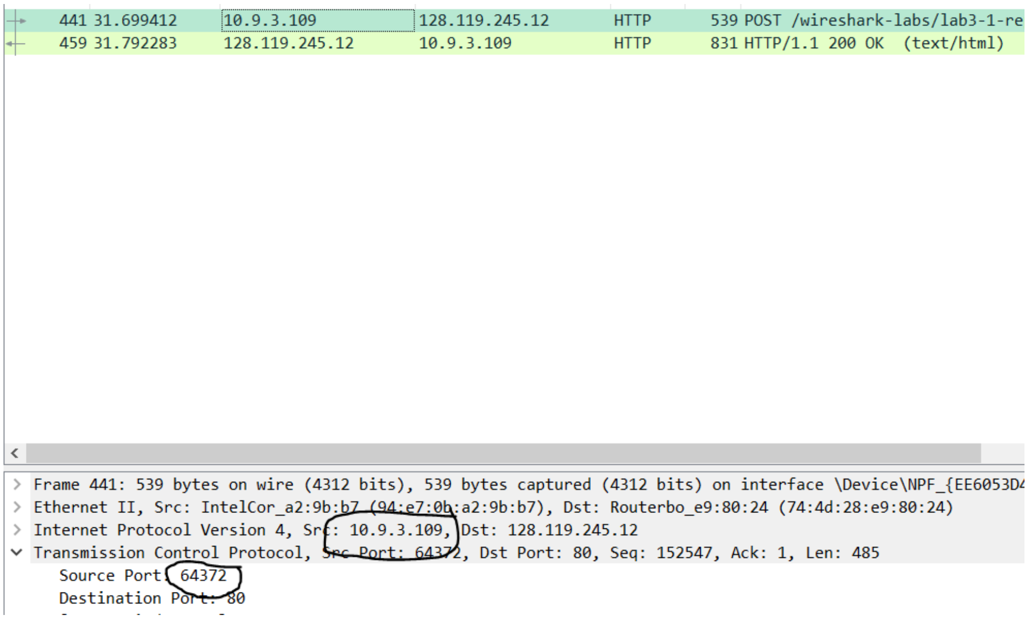
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
   The IP address of gaia.cs.umass.edu is 128.119.245.12
   The port number that it is sending and receiving TCP segments for the connection is: 80



```
441 31.699412    10.9.3.109       128.119.245.12    HTTP    539 POST /wireshark-labs/lab3-1-re
459 31.792283    128.119.245.12   10.9.3.109        HTTP    831 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 459: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{EE6053D
> Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.9.3.109
v Transmission Control Protocol, Src Port: 80, Dst Port: 64372, Seq: 1, Ack: 153032, Len: 777
    Source Port: 80
    Destination Port: 64372
    [Stream index: 22]
    [TCP Segment Len: 777]
    Sequence Number: 1    (relative sequence number)
```

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?
   IP address used by your client computer to transfer the file: 10.9.3.109
   TCP port number used by your client computer to transfer the file: 64372



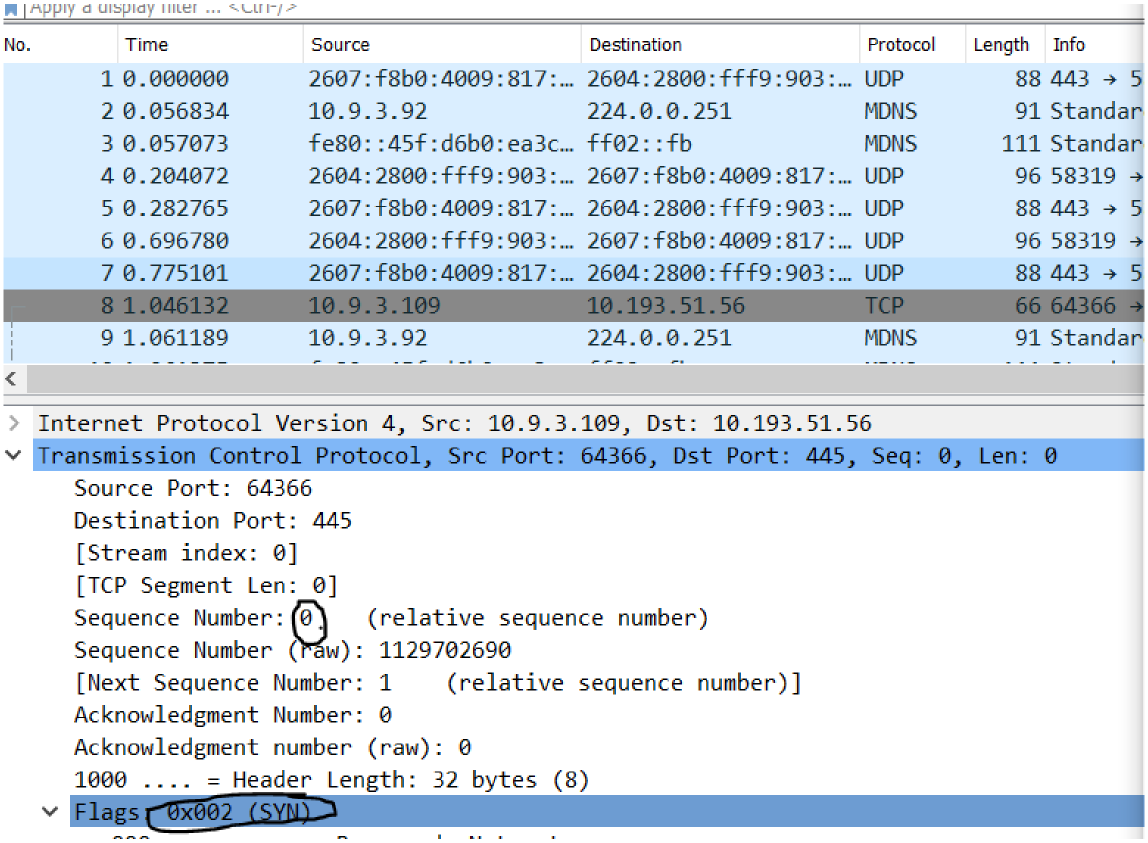
```
441 31.699412    10.9.3.109       128.119.245.12    HTTP    539 POST /wireshark-labs/lab3-1-re
459 31.792283    128.119.245.12   10.9.3.109        HTTP    831 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 441: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{EE6053D4
> Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
> Internet Protocol Version 4, Src: 10.9.3.109, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 64372, Dst Port: 80, Seq: 152547, Ack: 1, Len: 485
    Source Port: 64372
    Destination Port: 80
```

Part 3:

4. 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?

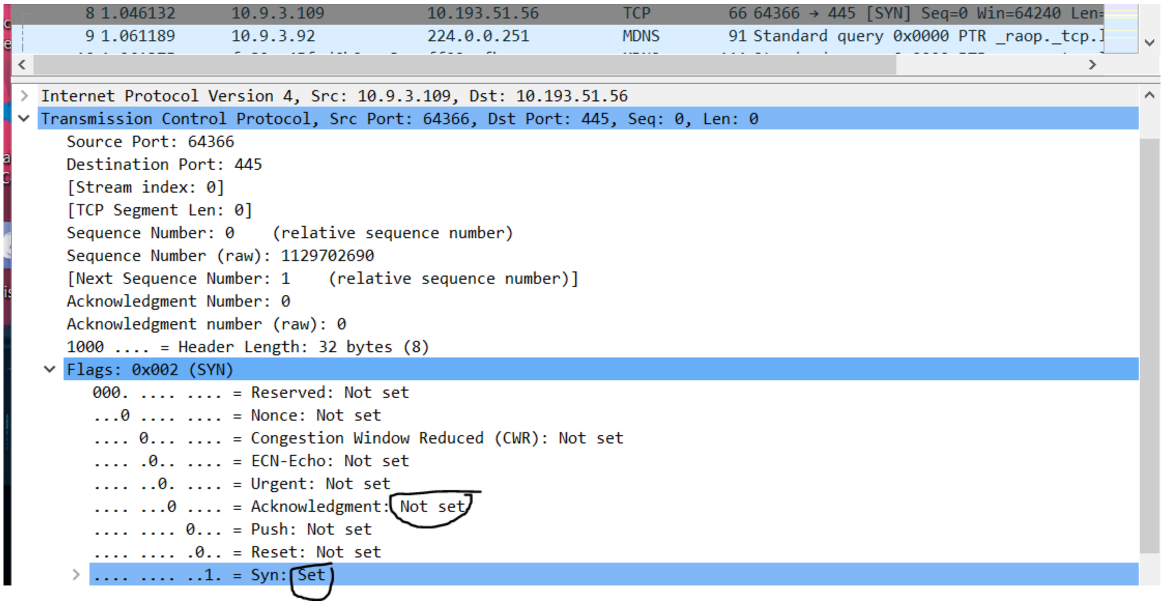
The TCP SYN segment sequence number is set to 0 and it is used to initiate the TCP connection.



```
Apply a display filter ... <Ctrl-/>
No.   Time         Source                  Destination             Protocol  Length  Info
    1 0.000000     2607:f8b0:4009:817:…    2604:2800:fff9:903:…    UDP           88  443 → 5
    2 0.056834     10.9.3.92               224.0.0.251             MDNS          91  Standar
    3 0.057073     fe80::45f:d6b0:ea3c…    ff02::fb                MDNS         111  Standar
    4 0.204072     2604:2800:fff9:903:…    2607:f8b0:4009:817:…    UDP           96  58319 →
    5 0.282765     2607:f8b0:4009:817:…    2604:2800:fff9:903:…    UDP           88  443 → 5
    6 0.696780     2604:2800:fff9:903:…    2607:f8b0:4009:817:…    UDP           96  58319 →
    7 0.775101     2607:f8b0:4009:817:…    2604:2800:fff9:903:…    UDP           88  443 → 5
    8 1.046132     10.9.3.109              10.193.51.56            TCP           66  64366 →
    9 1.061189     10.9.3.92               224.0.0.251             MDNS          91  Standar

> Internet Protocol Version 4, Src: 10.9.3.109, Dst: 10.193.51.56
v Transmission Control Protocol, Src Port: 64366, Dst Port: 445, Seq: 0, Len: 0
    Source Port: 64366
    Destination Port: 445
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1129702690
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
```

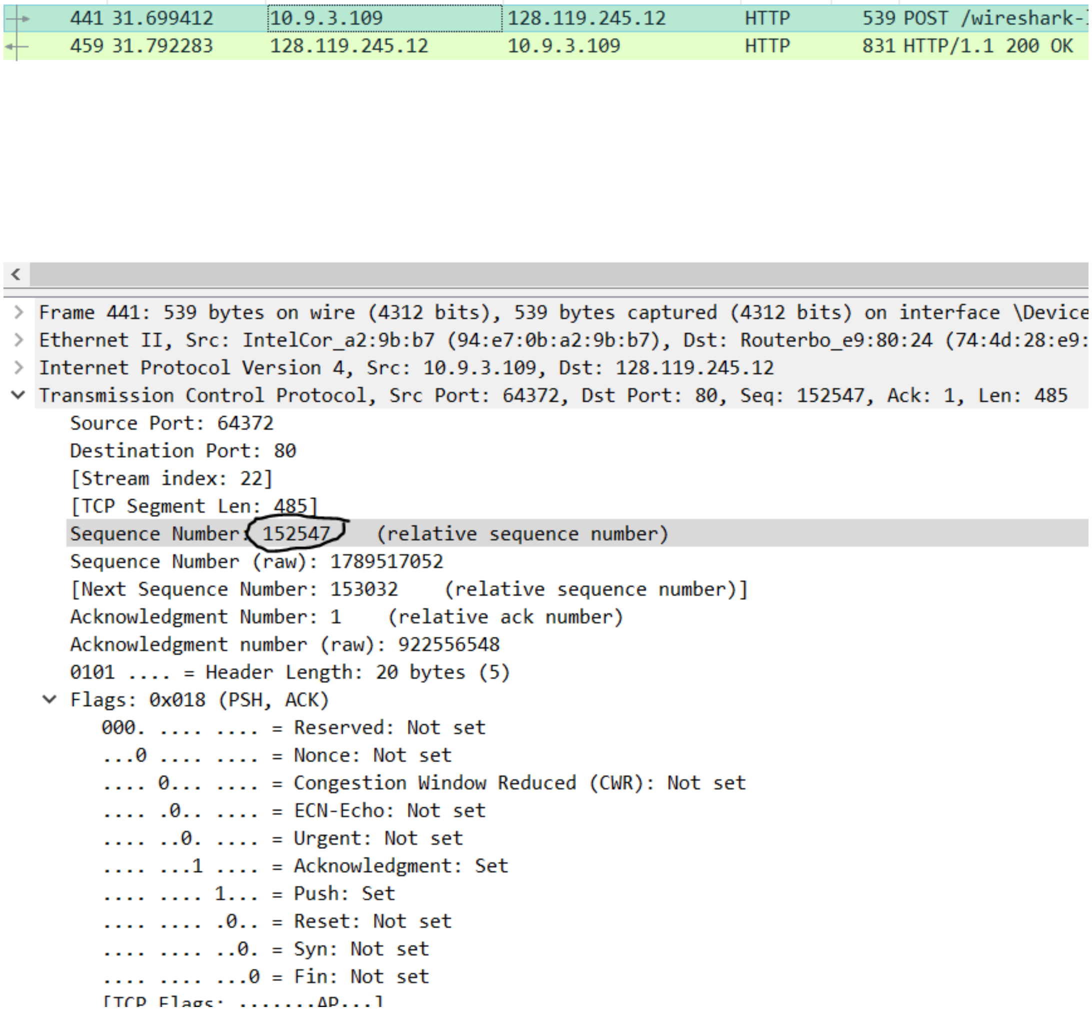
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
The SYNACK segment sequence number sent by gaia.cs.umass.edu to the client computer in reply to the SYN has a value of 1 and it is set, the acknowledgment field is 0 and not set.



```
    8 1.046132   10.9.3.109    10.193.51.56   TCP    66 64366 → 445 [SYN] Seq=0 Win=64240 Len=
    9 1.061189   10.9.3.92     224.0.0.251    MDNS   91 Standard query 0x0000 PTR _raop._tcp.l

> Internet Protocol Version 4, Src: 10.9.3.109, Dst: 10.193.51.56
v Transmission Control Protocol, Src Port: 64366, Dst Port: 445, Seq: 0, Len: 0
    Source Port: 64366
    Destination Port: 445
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1129702690
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
```

6. 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 the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.
The TCP segment containing the HTTP POST command has a sequence number of 152547

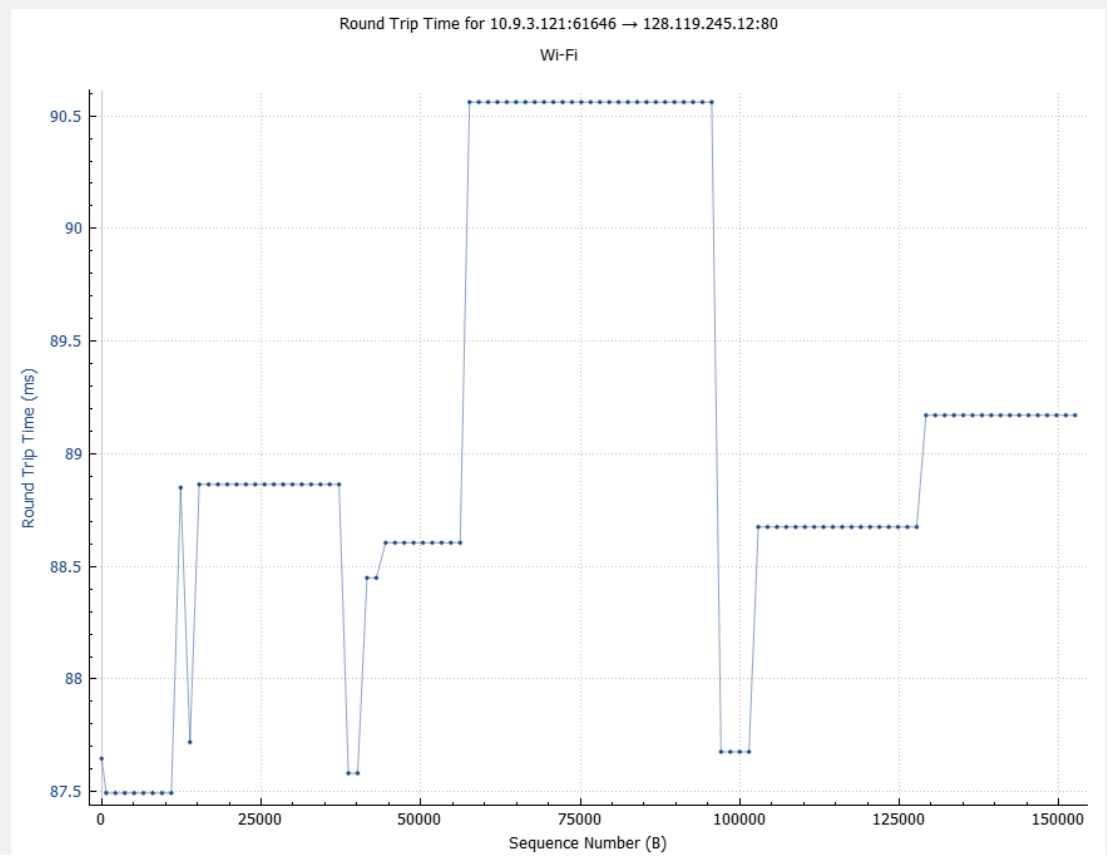


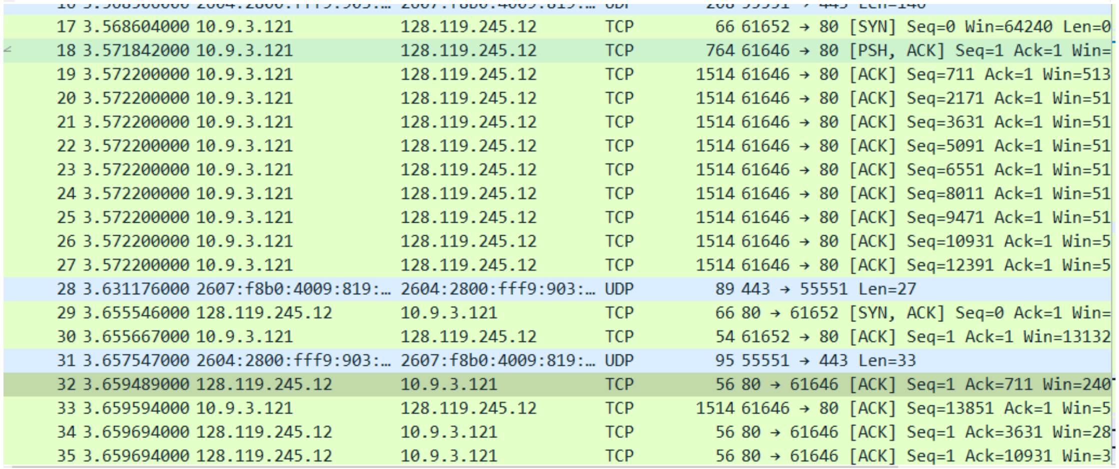
```
441 31.699412   10.9.3.109       128.119.245.12   HTTP    539 POST /wireshark-
459 31.792283   128.119.245.12   10.9.3.109       HTTP    831 HTTP/1.1 200 OK
```

```
> Frame 441: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device
> Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24 (74:4d:28:e9:
> Internet Protocol Version 4, Src: 10.9.3.109, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 64372, Dst Port: 80, Seq: 152547, Ack: 1, Len: 485
    Source Port: 64372
    Destination Port: 80
    [Stream index: 22]
    [TCP Segment Len: 485]
    Sequence Number: 152547    (relative sequence number)
    Sequence Number (raw): 1789517052
    [Next Sequence Number: 153032    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 922556548
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: .......AP...]
```

7. 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)? At what time was each segment sent? When was the ACK for each segment received? 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? What is the EstimatedRTTvalue (see Section 3.5.3, page 242 in text) after the receipt of each ACK?
The sequence numbers are: 1, 711, 2171, 3631, 5091, 6551
Time each segment was sent: 3.571842, 3.572200, 3.572200, 3.572200, 3.572200, 3.572200
Time each segment was received: 3.659489, 3.659594, 3.659594, 3.659594, 3. 659594, 3.659594
RTT of each segment: 0.087647, 0.087394, 0.087394, 0.087394, 0.087394, 0.087394
Estimated RTT: EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT
Estimated RTT for Segment 1: 0.087647

Estimated RTT for Segment 2: 0.087615375
Estimated RTT for Segment 3: 0.087615375
Estimated RTT for Segment 4: 0.087615375
Estimated RTT for Segment 5: 0.087615375
Estimated RTT for Segment 6: 0.087615375

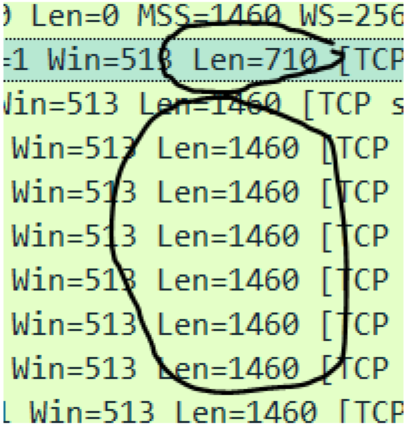




```
17 3.568604000 10.9.3.121          128.119.245.12      TCP     66 61652 → 80 [SYN] Seq=0 Win=64240 Len=0
18 3.571842000 10.9.3.121          128.119.245.12      TCP    764 61646 → 80 [PSH, ACK] Seq=1 Ack=1 Win=
19 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=711 Ack=1 Win=513
20 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=2171 Ack=1 Win=51
21 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=3631 Ack=1 Win=51
22 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=5091 Ack=1 Win=51
23 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=6551 Ack=1 Win=51
24 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=8011 Ack=1 Win=51
25 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=9471 Ack=1 Win=51
26 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=10931 Ack=1 Win=5
27 3.572200000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=12391 Ack=1 Win=5
28 3.631176000 2607:f8b0:4009:819:… 2604:2800:fff9:903:… UDP     89 443 → 55551 Len=27
29 3.655546000 128.119.245.12      10.9.3.121          TCP     66 80 → 61652 [SYN, ACK] Seq=0 Ack=1 Win=
30 3.655667000 10.9.3.121          128.119.245.12      TCP     54 61652 → 80 [ACK] Seq=1 Ack=1 Win=13132
31 3.657547000 2604:2800:fff9:903:… 2607:f8b0:4009:819:… UDP     95 55551 → 443 Len=33
32 3.659489000 128.119.245.12      10.9.3.121          TCP     56 80 → 61646 [ACK] Seq=1 Ack=711 Win=240
33 3.659594000 10.9.3.121          128.119.245.12      TCP   1514 61646 → 80 [ACK] Seq=13851 Ack=1 Win=5
34 3.659694000 128.119.245.12      10.9.3.121          TCP     56 80 → 61646 [ACK] Seq=1 Ack=3631 Win=28
35 3.659694000 128.119.245.12      10.9.3.121          TCP     56 80 → 61646 [ACK] Seq=1 Ack=10931 Win=3
```

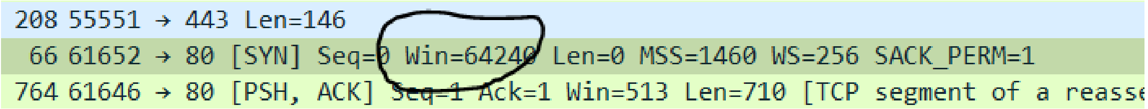
8. What is the length of each of the first six TCP segments?
   Segment 1 Length: 710
   Segment 2 Length: 1460
   Segment 3 Length: 1460

Segment 4 Length: 1460
Segment 5 Length: 1460
Segment 6 Length: 1460



```
) Len=0 MSS=1460 WS=256
=1 Win=513 Len=710 [TCP
Vin=513 Len=1460 [TCP s
 Win=513 Len=1460 [TCP
 Win=513 Len=1460 [TCP
 Win=513 Len=1460 [TCP
 Win=513 Len=1460 [TCP
 Win=513 Len=1460 [TCP
 Win=513 Len=1460 [TCP
l Win=513 Len=1460 [TCP
```

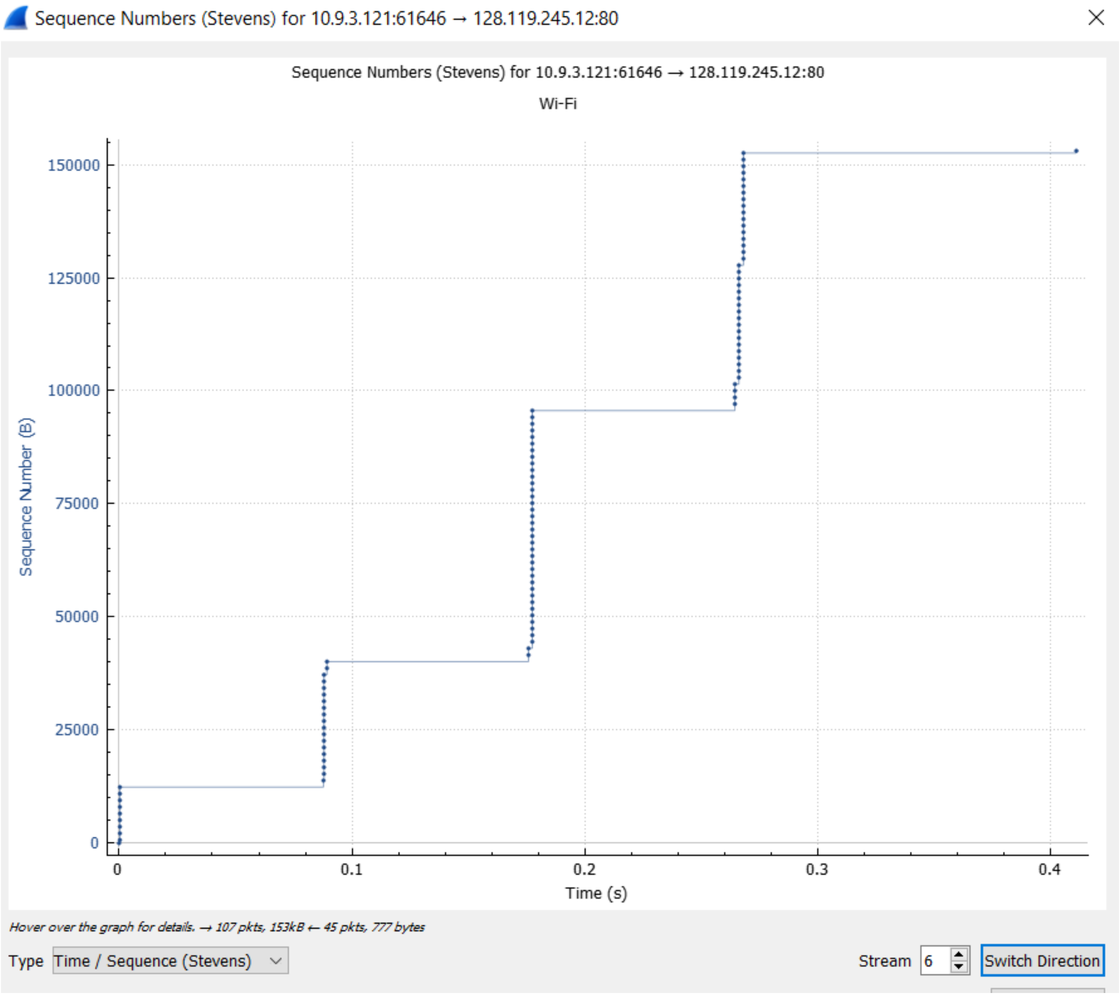
9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?
   The minimum amount of available buffer space is 64240 bytes, the lack of receiver buffer space will not throttle the sender.



```
208 55551 → 443 Len=146
 66 61652 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
764 61646 → 80 [PSH, ACK] Seq=1 Ack=1 Win=513 Len=710 [TCP segment of a reasse
```

10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
    There are no retransmitted segments in the trace file, I checked this by referring to the sequence numbers for the TCP segments within the trace file.
11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).
    The receiver typically acknowledges 1460 bytes of data in an ACK, I found this in the segment lengths posted in question 8 of this document.

12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.
    The throughput for the TCP connection is 3774.039669 bytes transferred per second.
    The acknowledged sequence number of the last ACK divided by the download time in seconds which is: 15032 bytes / 3.983 seconds



Sequence Numbers (Stevens) for 10.9.3.121:61646 → 128.119.245.12:80

Hover over the graph for details. → 107 pkts, 153kB ← 45 pkts, 777 bytes

Type Time / Sequence (Stevens)

Stream 6

Part 4:

13. Use the Time-Sequence-Graph (Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slow start phase begins and ends, and where congestion avoidance takes over?
    According to the graph above, the slow start begins at 0 and ends at approximately 0.09. The congestion avoidance takes over around approximately 0.19 and ends at approximately 0.28.
14. Answer Question13 for the trace that you captured when you transferred a file from your own computer to gaia.cs.umass.edu
    I did answer it for the trace that I captured in question 13.