COMP9331 lab4 answer

Exercise 1: Understanding TCP using Wireshark

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

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=14
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Le

The IP address of gaia.cs.umass.edu is **128.119.245.12**, on port number **80.**

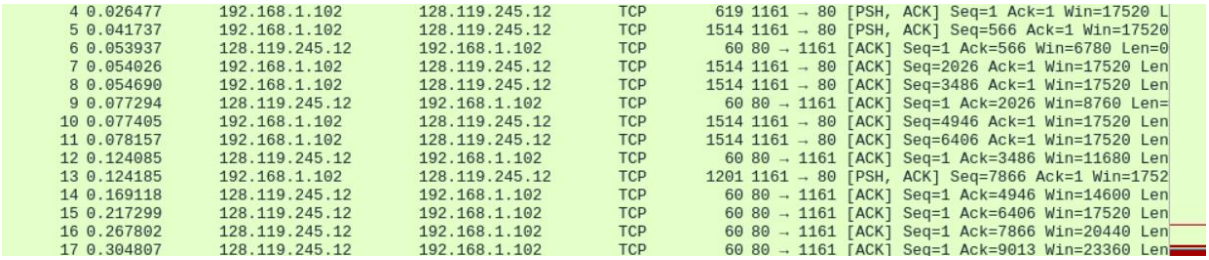
The client(source) IP address is **192.168.1.102** and the TCP port numbers is **1161**.

Question 2. **What is the sequence number of the TCP segment containing the HTTP POST command?**

```
▸ Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
▸ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG
▸ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
▾ Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, A
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 565]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 232129013
    [Next Sequence Number: 566    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 883061786
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
```

The sequence number is **232129013**.

Question 3.



```
     4 0.026477    192.168.1.102    128.119.245.12   TCP      619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 L
     5 0.041737    192.168.1.102    128.119.245.12   TCP     1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520
     6 0.053937    128.119.245.12   192.168.1.102    TCP       60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
     7 0.054026    192.168.1.102    128.119.245.12   TCP     1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len
     8 0.054690    192.168.1.102    128.119.245.12   TCP     1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len
     9 0.077294    128.119.245.12   192.168.1.102    TCP       60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=
    10 0.077405    192.168.1.102    128.119.245.12   TCP     1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len
    11 0.078157    192.168.1.102    128.119.245.12   TCP     1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len
    12 0.124085    128.119.245.12   192.168.1.102    TCP       60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len
    13 0.124185    192.168.1.102    128.119.245.12   TCP     1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=1752
    14 0.169118    128.119.245.12   192.168.1.102    TCP       60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len
    15 0.217299    128.119.245.12   192.168.1.102    TCP       60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len
    16 0.267802    128.119.245.12   192.168.1.102    TCP       60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len
    17 0.304807    128.119.245.12   192.168.1.102    TCP       60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len
```

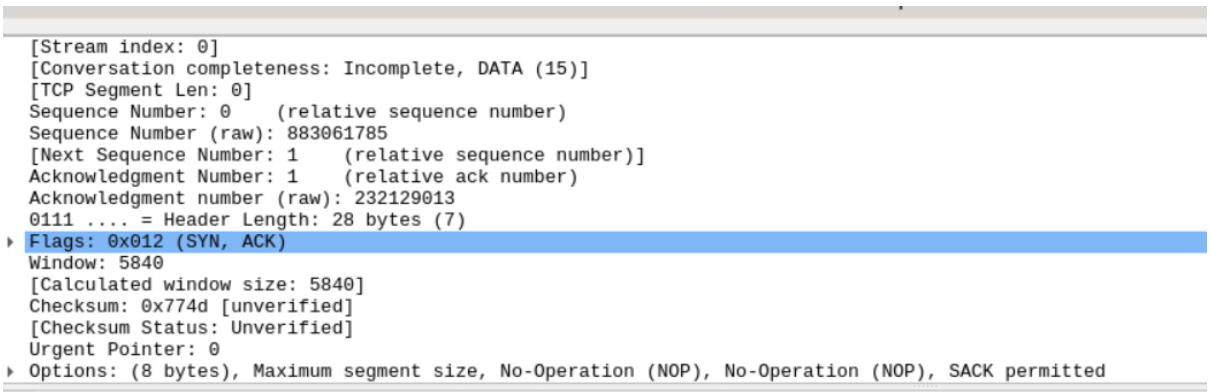
Segment	Sequence	Send time(sec)	Received time (se c)	Sample RTT (sec)	Estimated RTT (sec)
4	232129013	0.026477	0.053937	0.02746	0.02746
5	232129578	0.041737	0.077294	0.035557	0.028472
7	232131038	0.054026	0.124085	0.070059	0.03367
8	232132498	0.054690	0.169118	0.114428	0.043765
10	232133958	0.077405	0.217299	0.139894	0.055781
11	232135418	0.078157	0.267802	0.189645	0.072514

This is the information for question a b c.

(d) What is the length of each of the first six TCP segments?

The length of first Tcp segment is 565 bytes and others are 1460 bytes.

Question 4. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?



```
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 883061785
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 232129013
0111 .... = Header Length: 28 bytes (7)
▸ Flags: 0x012 (SYN, ACK)
Window: 5840
[Calculated window size: 5840]
Checksum: 0x774d [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
▸ Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

The minimum amount of available buffer space is 5840 bytes. No, the lack of receiver buffer space does not throttle the sender. This is because the sliding window mechanism in the TCP protocol allows the sender to continue sending data without waiting for confirmation until the data it sends reaches the receiver's window size.

Question 5. Are there any retransmitted segments in the trace file? To answer this question, what did you check for (in the trace)?

No, there are no retransmitted segments. To find this, I used tcp.analysis.retransmission and tcp.analysis.fast_retransmission and they did not show the output. We can also find this by checking the sequence number.

Question 6. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (recall the discussion about delayed acks from the lecture notes or Section 3.5 of the text)?

The receiver typically acknowledges **1460 bytes** data in an ACK.

55	1.119029	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=36509 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
56	1.119858	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=37969 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
57	1.120902	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=39429 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
58	1.121891	192.168.1.102	128.119.245.12	TCP	946 1161 → 80 [PSH, ACK] Seq=40889 Ack=1 Win=17520 Len=892 [TCP segment of a reassembled PDU]
59	1.200421	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=35049 Win=62780 Len=0
60	1.265026	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=37969 Win=62780 Len=0
61	1.362074	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=40889 Win=62780 Len=0
62	1.389886	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=41781 Win=62780 Len=0
63	1.390110	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=41781 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
64	1.390824	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=43241 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
65	1.391683	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=44701 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

the time between segments #59 and #60 is short, so the receiver might employ delayed acknowledgment. In this scenario, the receiver waits for a certain duration (typically a few hundred milliseconds) to see if additional packets arrive before sending an acknowledgment. Then, it sends a cumulative acknowledgment that includes the sequence numbers of all sequentially received packets, rather than sending individual acknowledgments for each packet.

Question 7. What is the TCP connection's throughput (bytes transferred per unit of time during the connection)?

Explain how you calculated this value.

```
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 232129013
```

```
Frame 206: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164091, Ack: 731, Len: 0
   Source Port: 1161
   Destination Port: 80
   [Stream index: 0]
   [Conversation completeness: Incomplete, DATA (15)]
   [TCP Segment Len: 0]
   Sequence Number: 164091    (relative sequence number)
   Sequence Number (raw): 232293103
```

Throughput = total amount data (bytes) /total transmission time (seconds) data

total amount data (bytes) = = 232293103 (bytes) – 232129013 (bytes) = 164090 (bytes)

total transmission time (seconds) data = 5.45583 (seconds) – 0.026477 (seconds) = 5.429353 (seconds)

Throughput = 164090 (bytes) / 5.429353 (seconds) = 30222.75 (bytes/second)

Exercise 2: TCP Connection Management

No	Source IP	Destination IP	Protocol	Info
295	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [SYN] Seq=2818463618 win=8192 MSS=1460
296	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [SYN, ACK] Seq=1247095790 Ack=2818463619 win=262144 MSS=1460
297	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [ACK] Seq=2818463619 Ack=1247095791 win=65535
298	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [PSH, ACK] Seq=2818463619 Ack=1247095791 win=65535
301	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [ACK] Seq=1247095791 Ack=2818463652 win=262096
302	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [PSH, ACK] Seq=1247095791 Ack=2818463652 win=262144
303	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [ACK] Seq=2818463652 Ack=1247095831 win=65535
304	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [FIN, ACK] Seq=2818463652 Ack=1247095831 win=65535
305	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [FIN, ACK] Seq=1247095831 Ack=2818463652 win=262144
306	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [ACK] Seq=2818463652 Ack=1247095832 win=65535
308	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [ACK] Seq=1247095831 Ack=2818463653 win=262144

Question 1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server?

The sequence number is **2818463618**.

Question 2. What is the sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did the server determine that value?

The sequence number is: **1247095790**.

The value of the Acknowledgement field is **2818463619**.

Plus 1 to value of the previous client sequence number to determine the value.

Question 3. What is the sequence number of the ACK segment sent by the client computer in response to the SYNACK? What is the value of the Acknowledgment field in this ACK segment? Does this segment contain any data?

The sequence number is: **2818463619**.

The value of the Acknowledgement field is **1247095791**.

No, this segment does not contain any data because the previous ACK is equal to the sequence number.

***Question 4*.** Who has done the active close? Is it the client or the server? How you have determined this? What type of closure has been performed? 3 Segment (FIN/FINACK/ACK), 4 Segment (FIN/ACK/FIN/ACK) or Simultaneous close?

Both the client and the server complete the active close because they sent FIN ACK to each other simultaneously, meaning it was simultaneous close.

***Question 5*.** How many data bytes have been transferred from the client to the server and from the server to the client during the whole duration of the connection? What relationship does this have with the Initial Sequence Number and the final ACK received from the other side?

Data transformed form the client to server = lastACK - ISN – 2 =

2818463653 – 2818463618 -2 = 33 bytes.

Data transformed form the server to client = lastACK - ISN – 2 =

1247095832– 1247095790-2 = 40 bytes.

The final acknowledgment number represents the next expected byte sequence to be received by the receiver, typically the final ACK received (ISN) plus the total data size received. Knowing the ISN and final acknowledgment number allows calculation of the total data bytes transferred. However, complexities such as packet loss, duplication, and segmentation/reassembly must be considered for accurate calculation in practical scenarios.