IT – 304 | CN | LAB-7

(Harsh Gajjar – 202201140)

Lab-07-A

Exercise – 1:

1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark "protocol" column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

TCP:

```
2632 21:07:13.602876 10.200.20.109    128.119.245.12    TCP    66 61512 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2634 21:07:13.605510 128.119.245.12   10.200.20.109     TCP    66 80 → 61512 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2635 21:07:13.605612 10.200.20.109    128.119.245.12    TCP    54 61512 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

HTTP:

```
2655 21:07:13.833047 10.200.20.109    128.119.245.12    HTTP    488 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2695 21:07:14.399286 128.119.245.12   10.200.20.109     HTTP    530 HTTP/1.1 200 OK  (text/html)
```

QUIC:

```
2666 21:07:13.980471 10.200.20.109    142.250.192.100    QUIC    1294 Payload (Encrypted), PKN: 107, CID: 5022884714189422592
```

DNS:

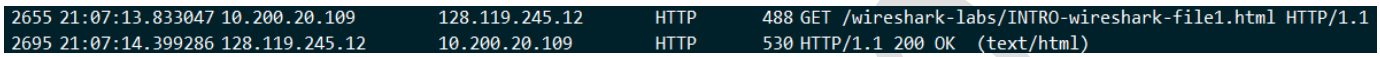
```
2633 21:07:13.603258 10.200.20.109    10.100.56.27      DNS     77 Standard query 0xb248 AAAA gaia.cs.umass.edu
2644 21:07:13.696145 10.200.20.109    10.100.56.25      DNS     77 Standard query 0xb248 AAAA gaia.cs.umass.edu
2645 21:07:13.721807 10.100.56.25     10.200.20.109     DNS     77 Standard query response 0xb248 AAAA gaia.cs.umass.edu
2656 21:07:13.833211 10.200.20.109    10.100.56.27      DNS     77 Standard query 0x971f Unknown (65) gaia.cs.umass.edu
2661 21:07:13.926938 10.200.20.109    10.100.56.25      DNS     77 Standard query 0x971f Unknown (65) gaia.cs.umass.edu
2664 21:07:13.948514 10.100.56.25     10.200.20.109     DNS    130 Standard query response 0x971f Unknown (65) gaia.cs.umass.edu SOA unix1.cs.umass.edu
```

TLSv1.2:

```
2648 21:07:13.773915 162.159.133.234    10.200.20.109    TLSv1.2    984 Application Data
```

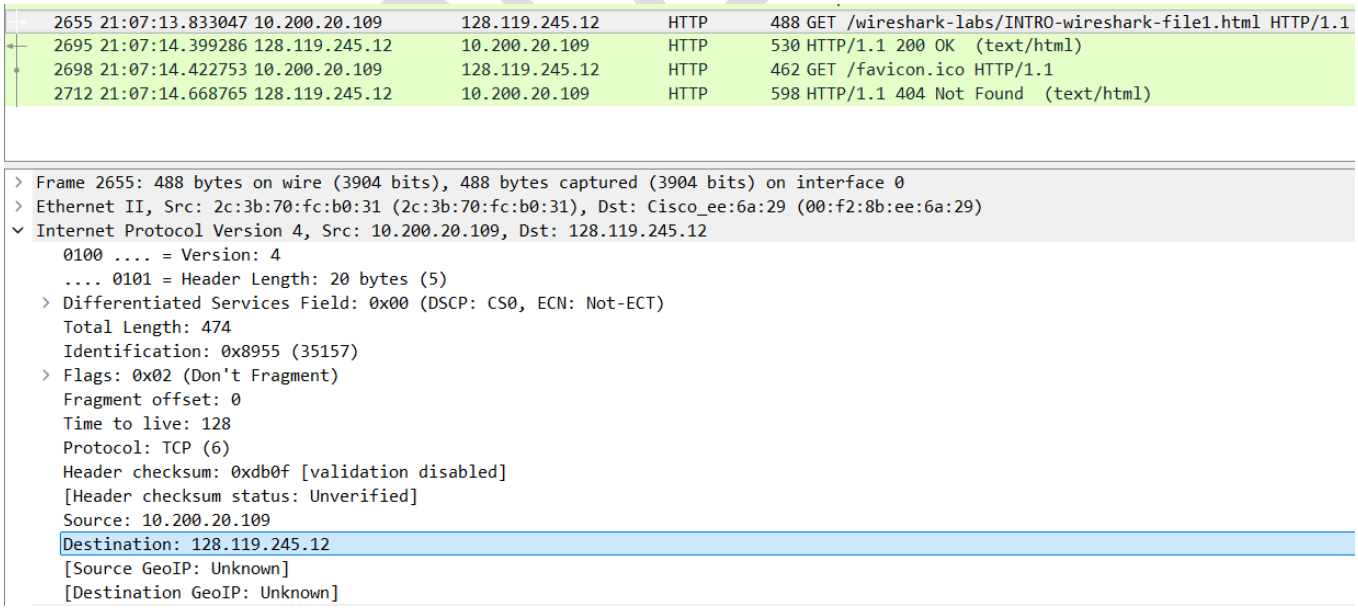
(PTO)

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. (If you want to display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



It took around 0.566239 seconds.

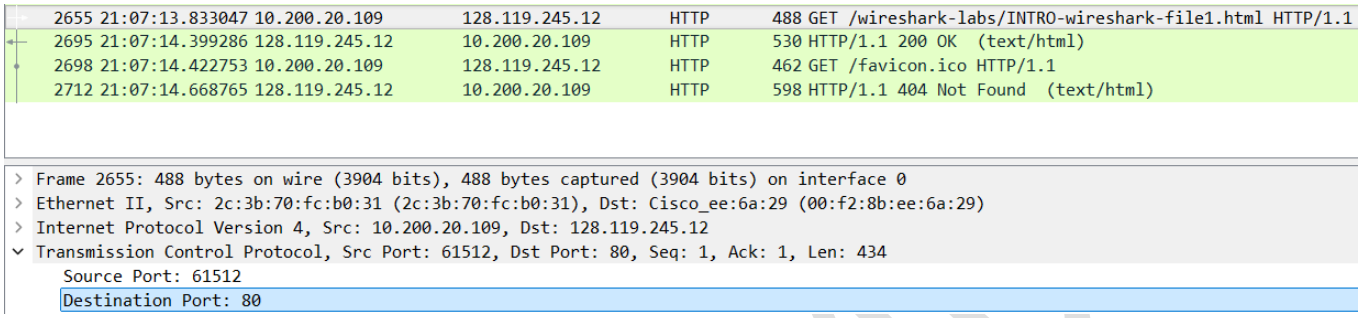
3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?



Destination IP address: 128.119.245.12 (after DNS resolution)

(PTO)

4. **See the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following "Dest Port:" for the TCP segment containing the HTTP request) and to which this HTTP request is being sent?**

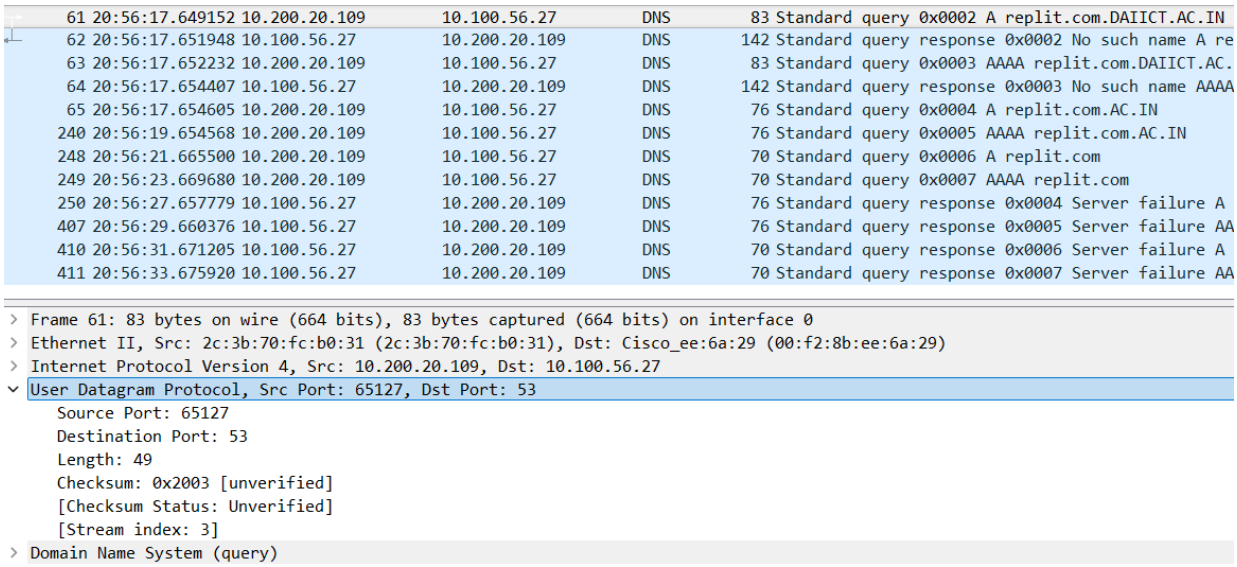


Destination Port Number: 80

Lab-07-B

Exercise – 2:

1. **Select the first UDP segment in your trace. What is the packet number of this segment in the trace report? What type of application-layer payload or protocol message is being carried in this UDP segment? Look at the details of this packet in Wireshark. How many fields there are in the UDP header? (You shouldn't look for any book to answer them! Answer these questions directly from what you observe in the packet trace.) What are the names of these fields?**



Packet Number: 61

Application-layer Protocol: DNS

UDP Header Fields: Source Port, Destination Port, Length, Checksum

2. **By consulting the displayed information in Wireshark's packet content field for this packet (or by consulting the textbook), what is the length (in bytes) of each of the UDP header fields?**

Source Port: 2 bytes (16 bits)

Destination Port: 2 bytes (16 bits)

Length: 2 bytes (16 bits)

Checksum: 2 bytes (16 bits)

Therefore, the total size of the UDP header is 8 bytes.

3. **The value in the Length field is the length of what? Verify your claim with your captured UDP packet.**

The Length field in the UDP header specifies the total length of the UDP segment, which includes both the header and the data (payload).

```
User Datagram Protocol, Src Port: 65127, Dst Port: 53
    Source Port: 65127
    Destination Port: 53
    Length: 49
    Checksum: 0x2003 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
```

UDP Header size: 8 bytes (standard)

Payload size: Total bytes (49 bytes) – 8 bytes = 41 bytes

This confirms that the packet is carrying a DNS query inside a UDP segment.

4. **What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)**

UDP header size (max.): 8 bytes

IP packet size (max.): 65,535 bytes (due to the 16-bit length field in the IP header)

IP header size = 20 bytes

Therefore, Payload size (max.):

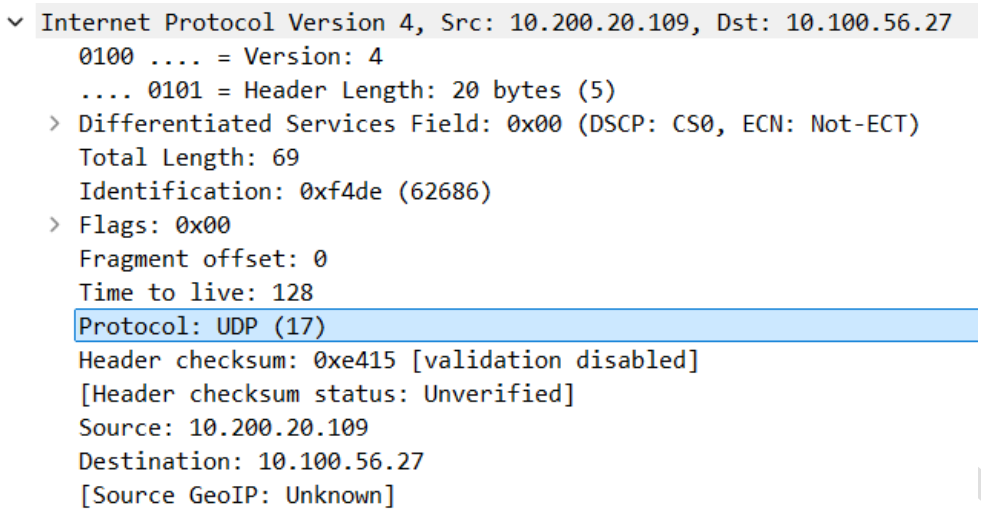
65,535 bytes−20 bytes (IP header) − 8 bytes (UDP header) = 65,507 bytes

5. **What is the largest possible source port number? (Hint: see the hint in 4.)**

Source Port field is 16 bits long.

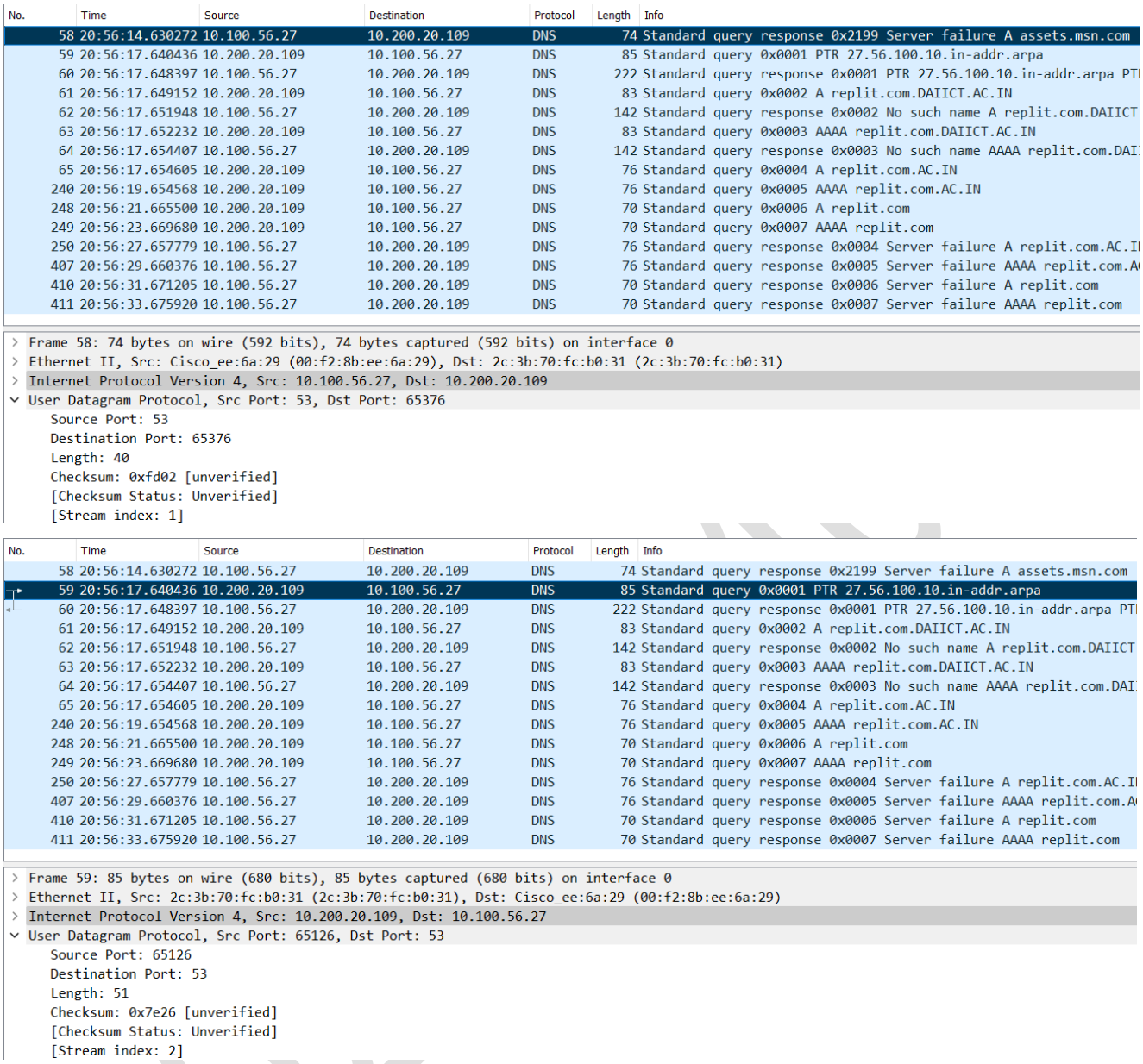
So, the maximum possible value for the source port is: $2^{16} - 1 = 65,535$.

6. **What is the protocol number for UDP? Give your answer in decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment.**



Protocol Number: 17

7. **Examine the pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). What is the packet number of the first of these two UDP segments in the trace file? What is the value in the source port field in this UDP segment? What is the value in the destination port field in this UDP segment? What is the packet number of the second of these two UDP segments in the trace file? What is the value in the source port field in this second UDP segment? What is the value in the destination port field in this second UDP segment? Describe the relationship between the port numbers in the two packets.**



No.	Time	Source	Destination	Protocol	Length	Info
58	20:56:14.630272	10.100.56.27	10.200.20.109	DNS	74	Standard query response 0x2199 Server failure A assets.msn.com
59	20:56:17.640436	10.200.20.109	10.100.56.27	DNS	85	Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
60	20:56:17.648397	10.100.56.27	10.200.20.109	DNS	222	Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PT
61	20:56:17.649152	10.200.20.109	10.100.56.27	DNS	83	Standard query 0x0002 A replit.com.DAIICT.AC.IN
62	20:56:17.651948	10.100.56.27	10.200.20.109	DNS	142	Standard query response 0x0002 No such name A replit.com.DAIICT
63	20:56:17.652232	10.200.20.109	10.100.56.27	DNS	83	Standard query 0x0003 AAAA replit.com.DAIICT.AC.IN
64	20:56:17.654407	10.100.56.27	10.200.20.109	DNS	142	Standard query response 0x0003 No such name AAAA replit.com.DAI
65	20:56:17.654605	10.200.20.109	10.100.56.27	DNS	76	Standard query 0x0004 A replit.com.AC.IN
240	20:56:19.654568	10.200.20.109	10.100.56.27	DNS	76	Standard query 0x0005 AAAA replit.com.AC.IN
248	20:56:21.665500	10.200.20.109	10.100.56.27	DNS	70	Standard query 0x0006 A replit.com
249	20:56:23.669680	10.200.20.109	10.100.56.27	DNS	70	Standard query 0x0007 AAAA replit.com
250	20:56:27.657779	10.100.56.27	10.200.20.109	DNS	76	Standard query response 0x0004 Server failure A replit.com.AC.I
407	20:56:29.660376	10.100.56.27	10.200.20.109	DNS	76	Standard query response 0x0005 Server failure AAAA replit.com.A
410	20:56:31.671205	10.100.56.27	10.200.20.109	DNS	70	Standard query response 0x0006 Server failure A replit.com
411	20:56:33.675920	10.100.56.27	10.200.20.109	DNS	70	Standard query response 0x0007 Server failure AAAA replit.com

```
> Frame 58: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: 2c:3b:70:fc:b0:31 (2c:3b:70:fc:b0:31)
> Internet Protocol Version 4, Src: 10.100.56.27, Dst: 10.200.20.109
v User Datagram Protocol, Src Port: 53, Dst Port: 65376
    Source Port: 53
    Destination Port: 65376
    Length: 40
    Checksum: 0xfd02 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
```


No.	Time	Source	Destination	Protocol	Length	Info
58	20:56:14.630272	10.100.56.27	10.200.20.109	DNS	74	Standard query response 0x2199 Server failure A assets.msn.com
59	20:56:17.640436	10.200.20.109	10.100.56.27	DNS	85	Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
60	20:56:17.648397	10.100.56.27	10.200.20.109	DNS	222	Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PT
61	20:56:17.649152	10.200.20.109	10.100.56.27	DNS	83	Standard query 0x0002 A replit.com.DAIICT.AC.IN
62	20:56:17.651948	10.100.56.27	10.200.20.109	DNS	142	Standard query response 0x0002 No such name A replit.com.DAIICT
63	20:56:17.652232	10.200.20.109	10.100.56.27	DNS	83	Standard query 0x0003 AAAA replit.com.DAIICT.AC.IN
64	20:56:17.654407	10.100.56.27	10.200.20.109	DNS	142	Standard query response 0x0003 No such name AAAA replit.com.DAI
65	20:56:17.654605	10.200.20.109	10.100.56.27	DNS	76	Standard query 0x0004 A replit.com.AC.IN
240	20:56:19.654568	10.200.20.109	10.100.56.27	DNS	76	Standard query 0x0005 AAAA replit.com.AC.IN
248	20:56:21.665500	10.200.20.109	10.100.56.27	DNS	70	Standard query 0x0006 A replit.com
249	20:56:23.669680	10.200.20.109	10.100.56.27	DNS	70	Standard query 0x0007 AAAA replit.com
250	20:56:27.657779	10.100.56.27	10.200.20.109	DNS	76	Standard query response 0x0004 Server failure A replit.com.AC.I
407	20:56:29.660376	10.100.56.27	10.200.20.109	DNS	76	Standard query response 0x0005 Server failure AAAA replit.com.A
410	20:56:31.671205	10.100.56.27	10.200.20.109	DNS	70	Standard query response 0x0006 Server failure A replit.com
411	20:56:33.675920	10.100.56.27	10.200.20.109	DNS	70	Standard query response 0x0007 Server failure AAAA replit.com

```
> Frame 59: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
> Ethernet II, Src: 2c:3b:70:fc:b0:31 (2c:3b:70:fc:b0:31), Dst: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29)
> Internet Protocol Version 4, Src: 10.200.20.109, Dst: 10.100.56.27
v User Datagram Protocol, Src Port: 65126, Dst Port: 53
    Source Port: 65126
    Destination Port: 53
    Length: 51
    Checksum: 0x7e26 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
```

The first UDP packet in the pair is packet number 58.

- Source IP: 10.100.56.27
- Destination IP: 10.200.20.109
- Source Port: 53
- Destination Port: 65376

The corresponding reply is packet number 59.

- Source IP: 10.200.20.109
- Destination IP: 10.100.56.27

- Source Port: 65376
- Destination Port: 53

Relationship between the port numbers:

The source and destination ports are swapped between the two packets. This is typical for request-response pairs. The client sends a request from a random high port (65376) to a well-known service port (53, which is for DNS). The server then responds by sending from the service port (53) back to the client's original port (65376).

This pattern allows the client to match the response to its original request and ensures the response goes back to the correct application on the client machine.

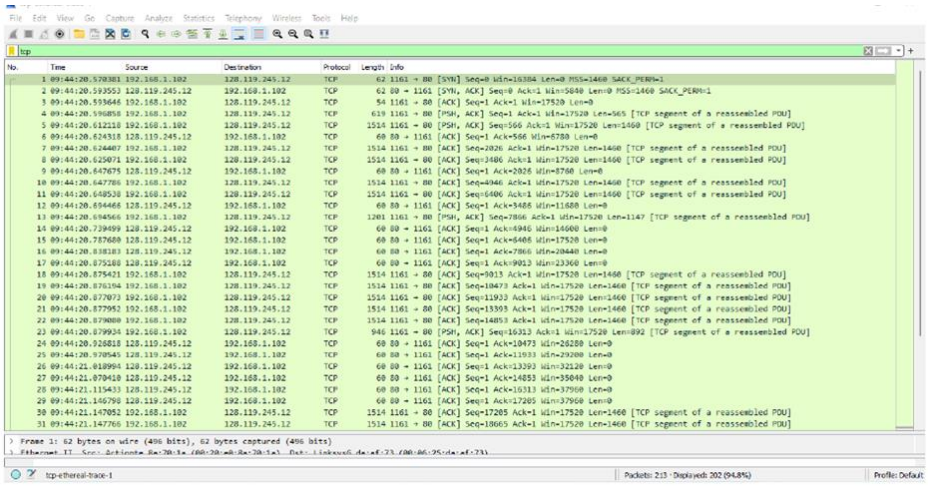
Lab-07-C

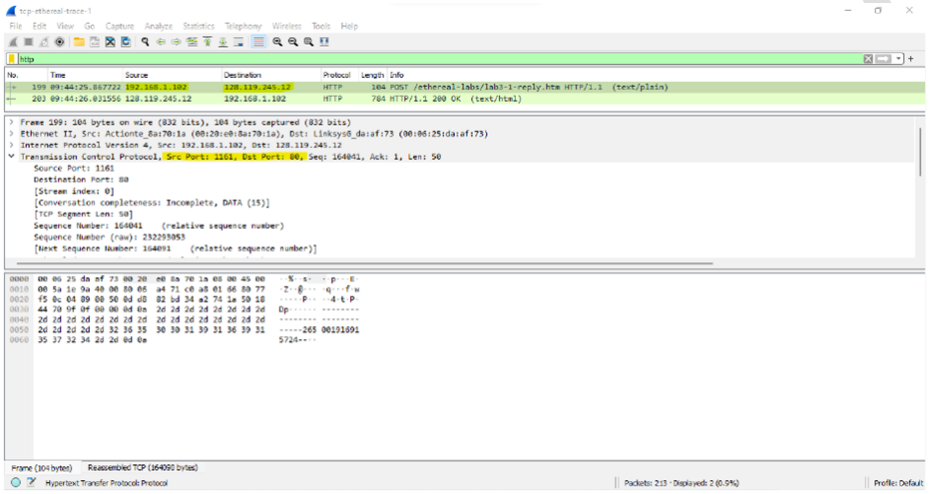
Exercise – 3:

1. **What is the IP address and TCP port number used by the client computer (source) that is transferring the alice.txt file to gaia.cs.umass.edu? (Hint: Explore the details of a TCP Packet).**

Source port: 1161

IP: 192.168.1.102





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?

Destination port: 80

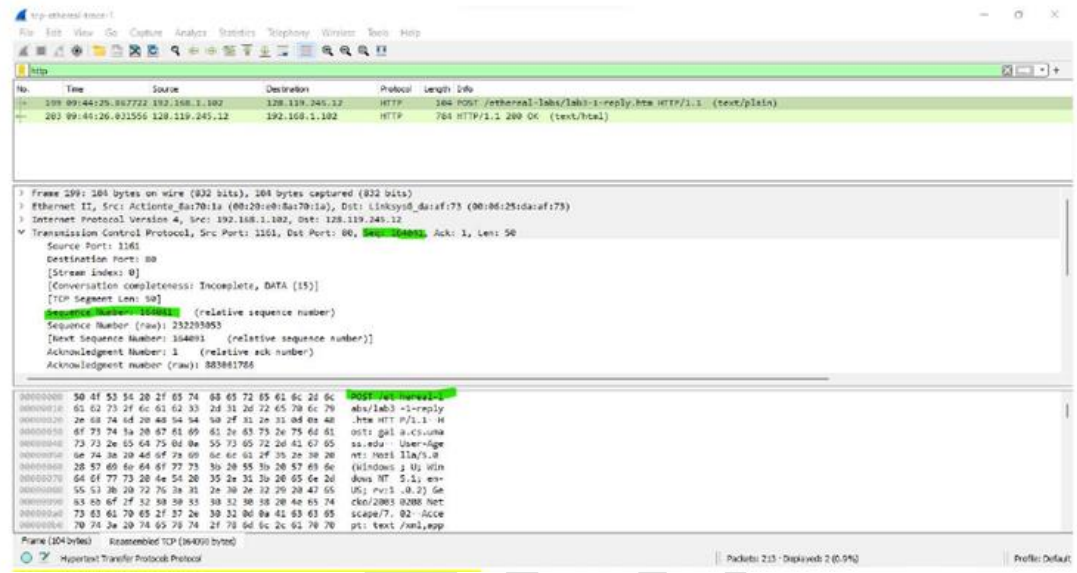
IP:128.119.245.12

3. 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 this TCP segment that identifies the segment as a SYN segment? (Hint: Refer note)

Seq=0

The keyword [SYN] identifies it as a SYN segment.

4. **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 it in the segment that identifies the segment as a SYNACK segment? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? (Hint: To know the client, check your PC's IP address)**



Sequence number: Seq=1

Value of Acknowledgement field: Ack=1

gaia.cs.umass.edu determine that value by adding 1 to the sequence number of the previous segment This segment is identified as a [SYN,ACK segment acknowledgement and syn bits are both set.

5. **Count the no. of packets required for transferring the whole file('Alice.txt'). Don't include the packets used for connection re/establishment. (Hint: Check for 'ACK' packets which went from client to server, and the 'Len' is not '0')**

To count the packets required for transferring:

1. Open the packet capture in Wireshark

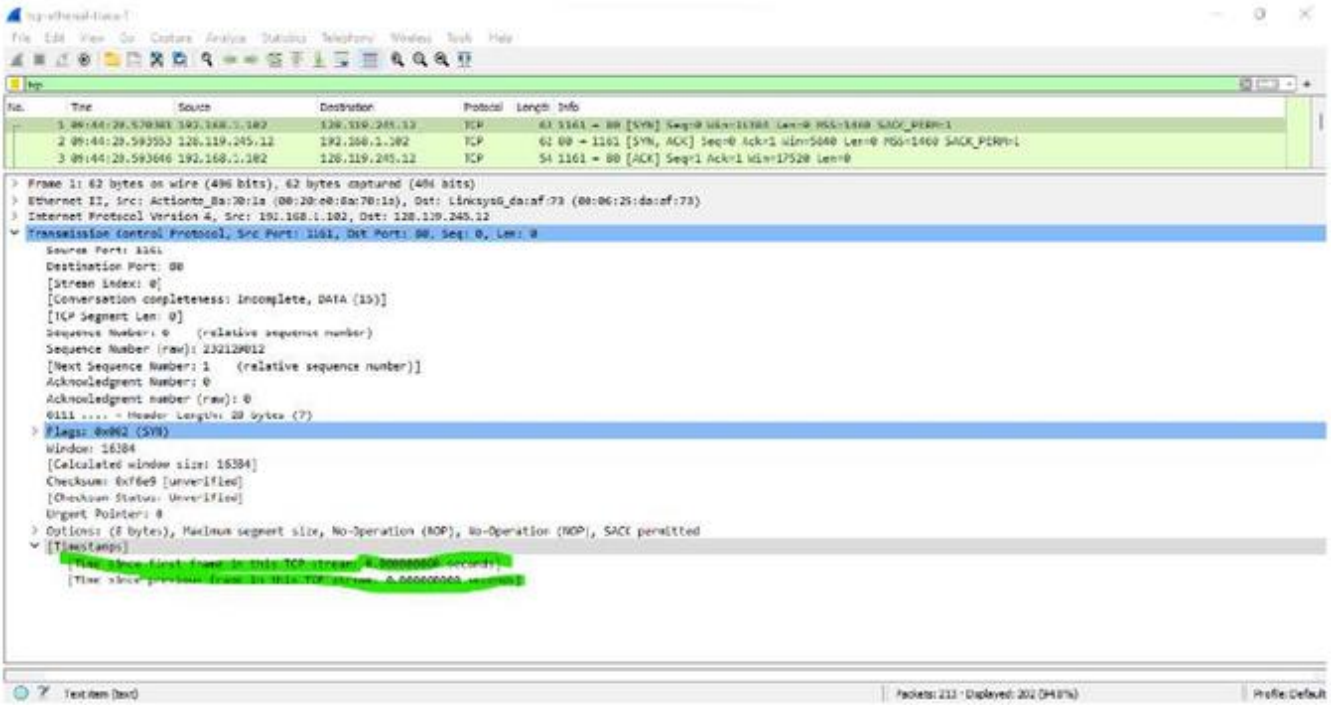
2. Filter for TCP packets from client to server with ACK flag and non-zero length

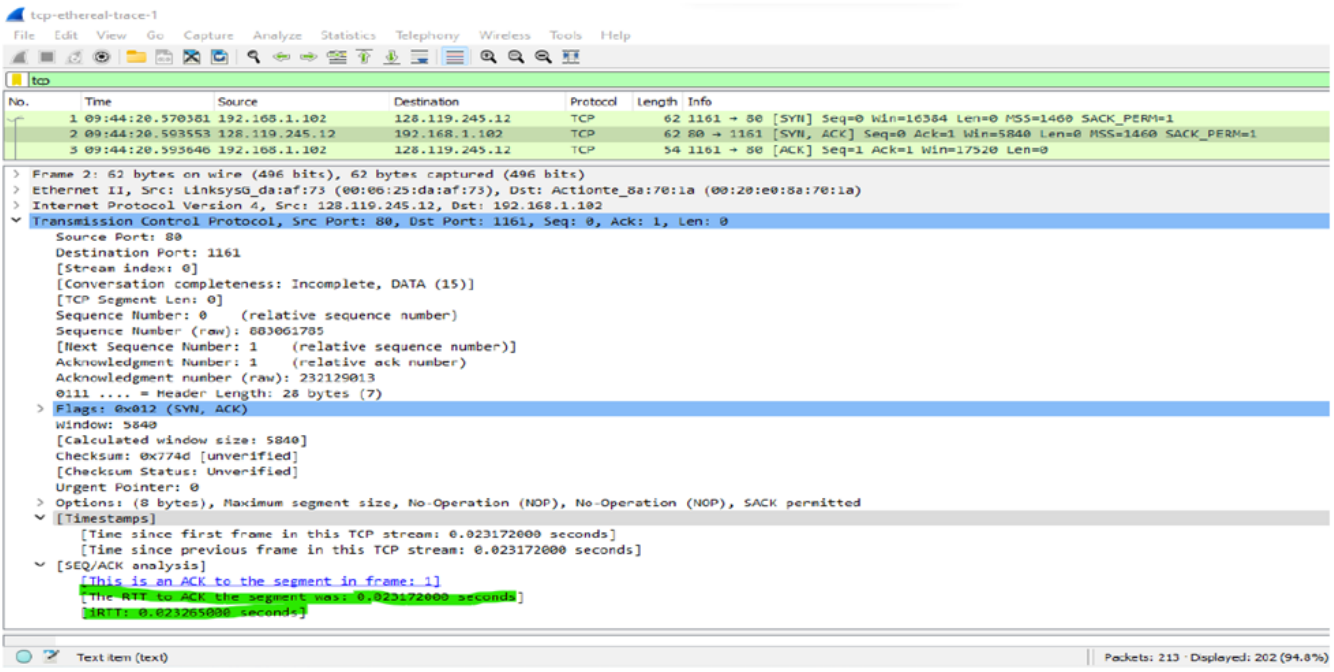
3. Count these packets, excluding connection establishment packets

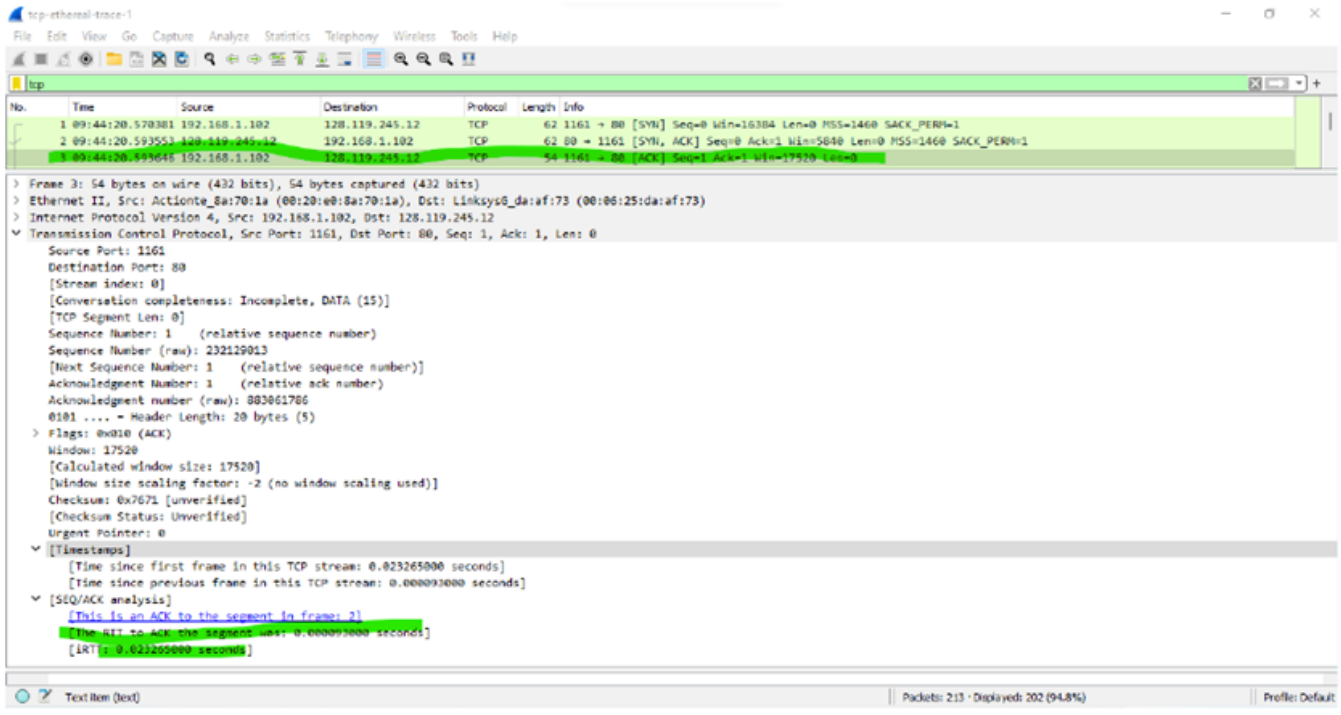
The exact number can't be determined from the information provided in the lab document. You would need to analyse the full capture file to get the accurate count.

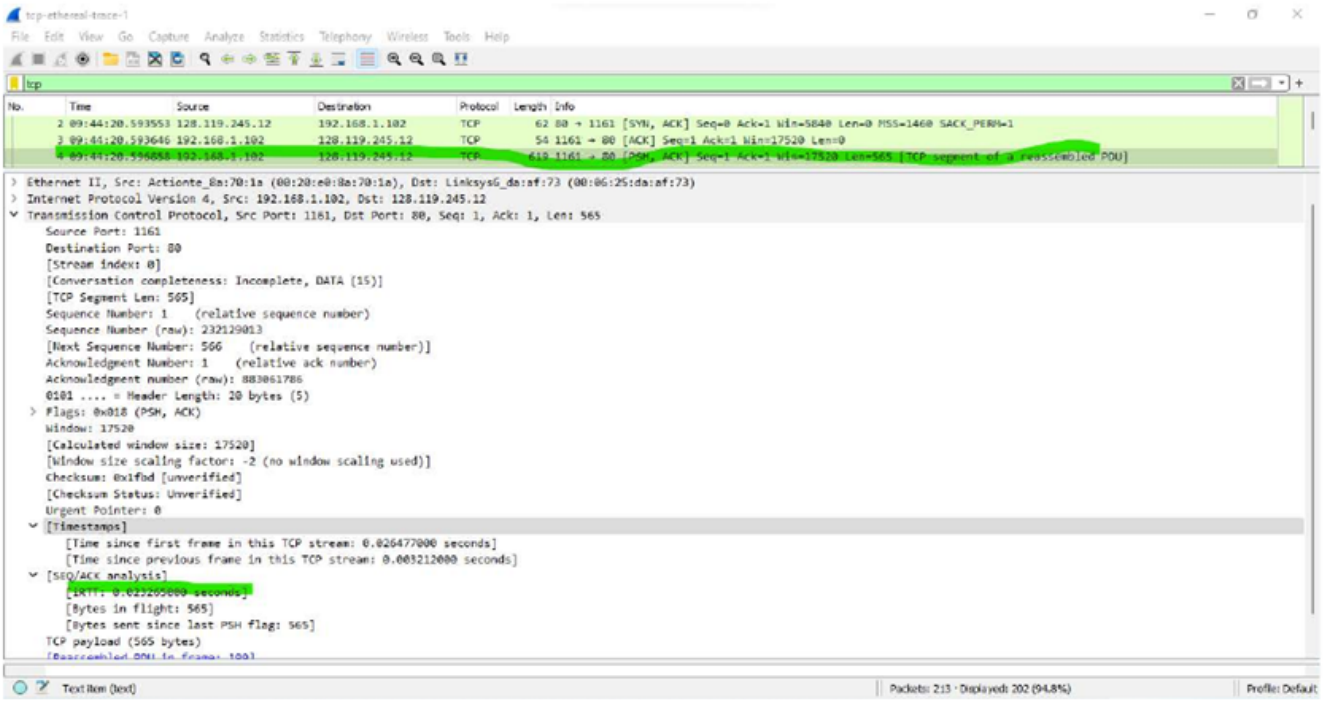
6. **Consider the TCP segment containing the HTTP "POST" as the first segment in the data transfer part of the TCP connection. • At what time was the first segment (the one containing the HTTP POST) in the data-transfer part of the TCP connection sent? • At what time was the ACK for this first data-containing segment received? • What is the RTT for this first data-containing segment? • What is the RTT value the second data-carrying TCP segment and its ACK?**

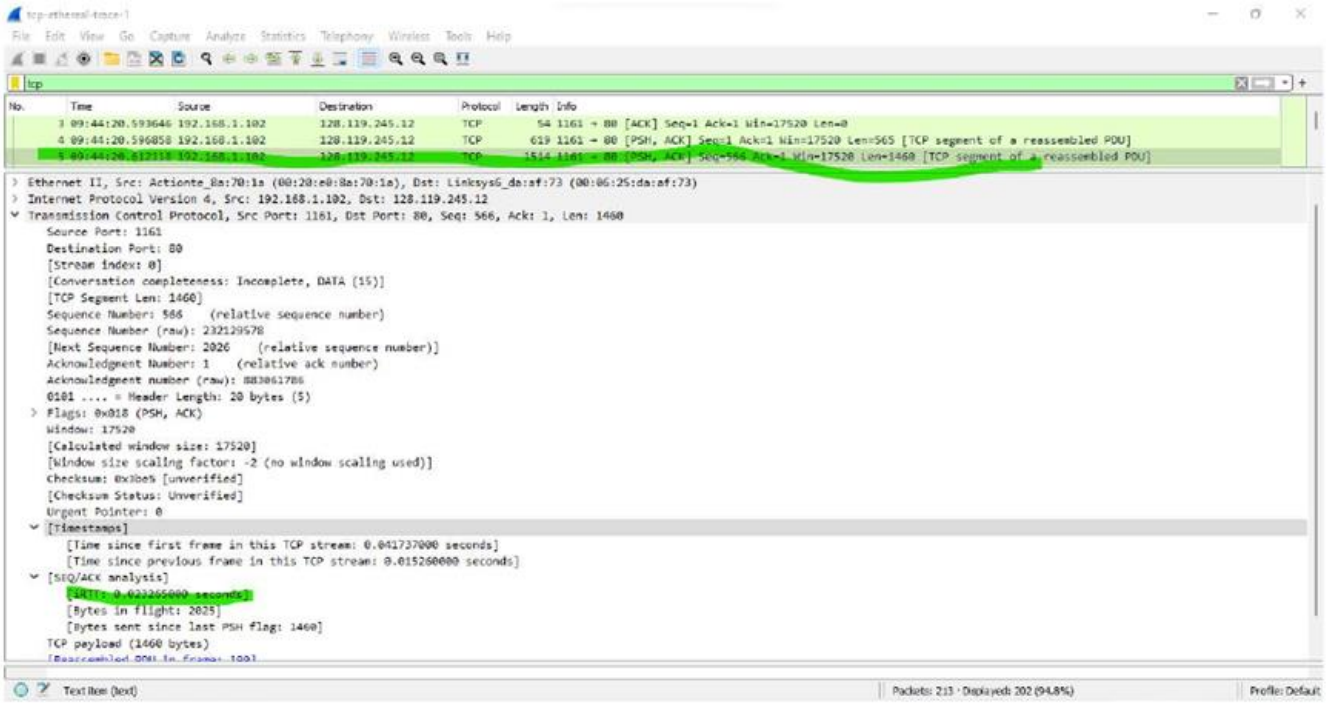
Seg1: Sequence number=0

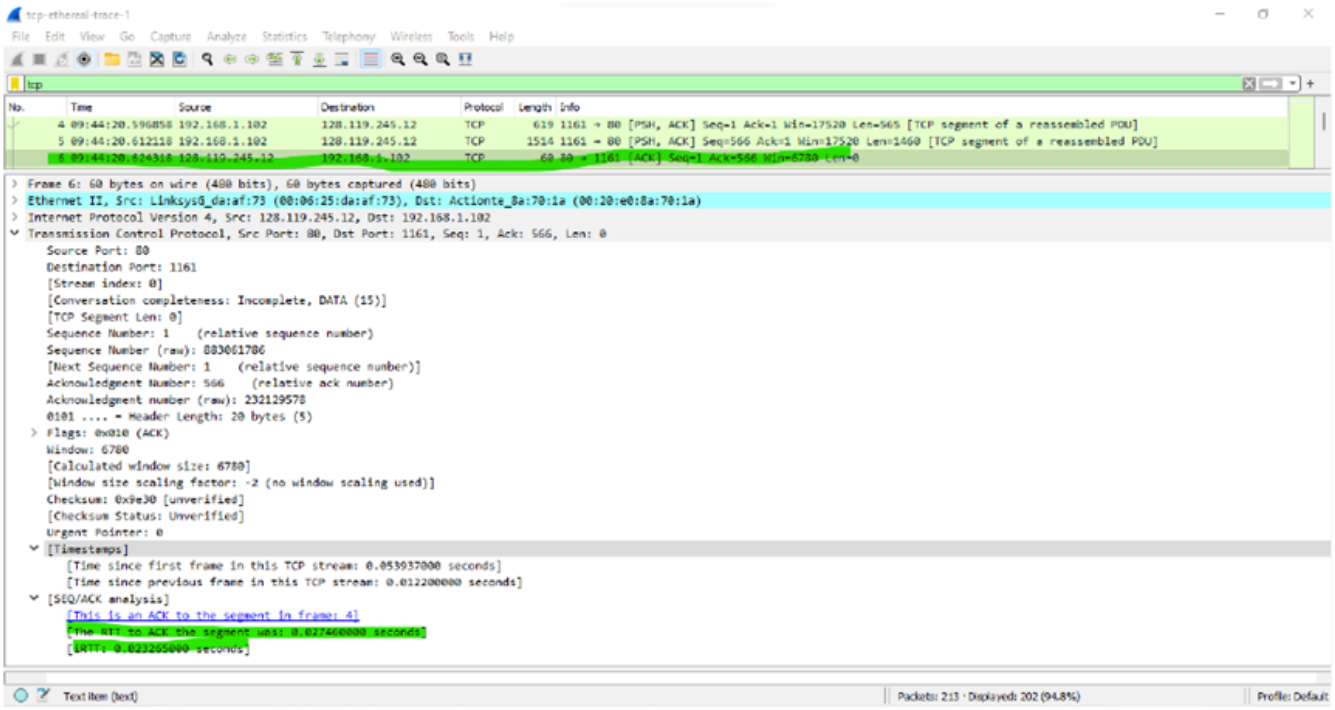



tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1 09:44:20.570381 192.168.1.102 128.119.245.12 TCP 62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2 09:44:20.593553 128.119.245.12 192.168.1.102 TCP 62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3 09:44:20.593646 192.168.1.102 128.119.245.12 TCP 54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 1161
[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
[Timestamps]
[Time since first frame in this TCP stream: 0.023172000 seconds]
[Time since previous frame in this TCP stream: 0.023172000 seconds]
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 1]
[The RTT to ACK the segment was: 0.023172000 seconds]
[iRTT: 0.023265000 seconds]
Text item (text)
Packets: 213 · Displayed: 202 (94.8%)

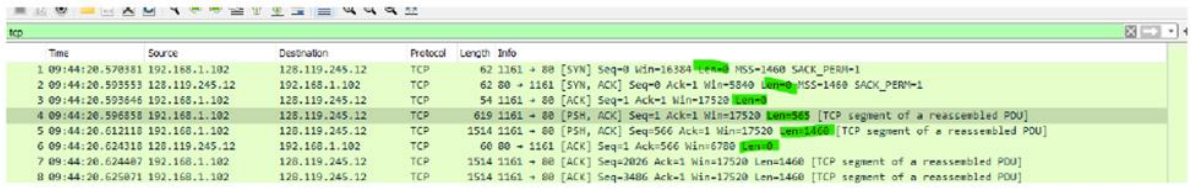

tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1 09:44:20.570381 192.168.1.102 128.119.245.12 TCP 62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2 09:44:20.593553 128.119.245.12 192.168.1.102 TCP 62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3 09:44:20.593646 192.168.1.102 128.119.245.12 TCP 54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
Frame 3: 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: 1, Ack: 1, Len: 0
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 232129013
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x7671 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.023265000 seconds]
[Time since previous frame in this TCP stream: 0.000093000 seconds]
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 2]
[The RTT to ACK the segment was: 0.000093000 seconds]
[iRTT: 0.023265000 seconds]
Text item (text)
Packets: 213 · Displayed: 202 (94.8%)
Profile: Default


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
2 09:44:20.593553 128.119.245.12 192.168.1.102 TCP 62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3 09:44:20.593646 192.168.1.102 128.119.245.12 TCP 54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4 09:44:20.596858 192.168.1.102 128.119.245.12 TCP 619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
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: 1, Ack: 1, Len: 565
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)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1fbd [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.026477000 seconds]
[Time since previous frame in this TCP stream: 0.003212000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.023265000 seconds]
[Bytes in flight: 565]
[Bytes sent since last PSH flag: 565]
TCP payload (565 bytes)
Text item (text)
Packets: 213 · Displayed: 202 (94.8%)
Profile: Default


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
3 09:44:20.593646 192.168.1.102 128.119.245.12 TCP 54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4 09:44:20.596858 192.168.1.102 128.119.245.12 TCP 619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5 09:44:20.612318 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
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: 566, Ack: 1, Len: 1460
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 1460]
Sequence Number: 566 (relative sequence number)
Sequence Number (raw): 232129578
[Next Sequence Number: 2026 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x3be6 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.041737000 seconds]
[Time since previous frame in this TCP stream: 0.015260000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.023265000 seconds]
[Bytes in flight: 2025]
[Bytes sent since last PSH flag: 1460]
TCP payload (1460 bytes)
Text item (text)
Packets: 213 · Displayed: 202 (94.8%)
Profile: Default



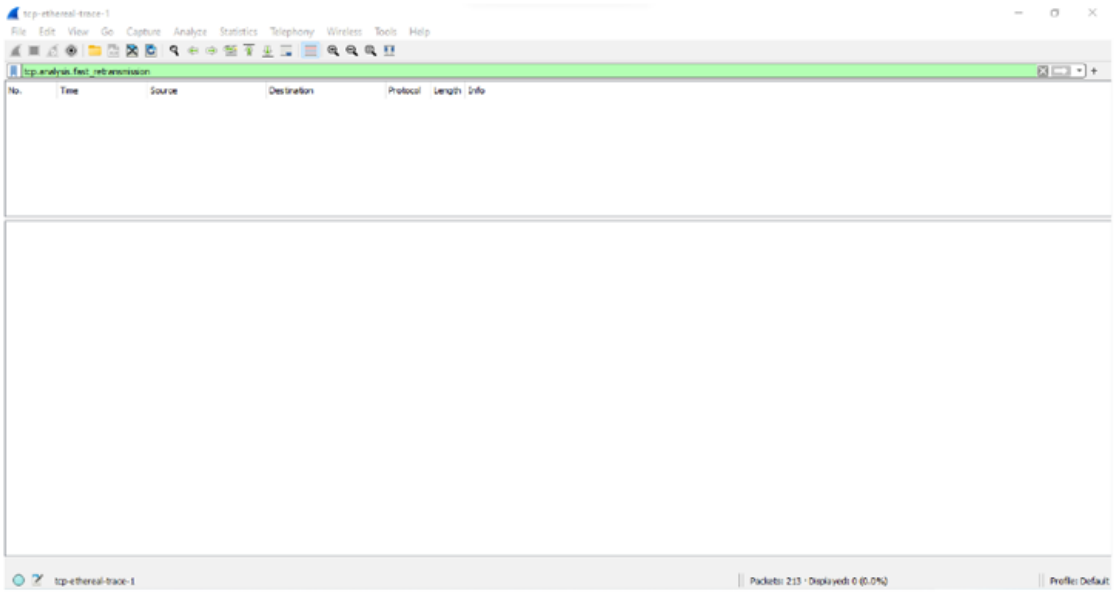
7. What is the length (header plus payload) of each of the first four data-carrying TCP segments?



8. What is the minimum amount of available buffer space advertised to the client by gaia.cs.umass.edu among these first four data-carrying TCP segments1? Does the lack of receiver buffer space ever throttle the sender for these first four data-carrying segments?

The minimum amount of available buffer space is advertised as (Calculated window size): 5840 bytes. The lack of receiver buffer space does not ever throttle the sender.

9. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?



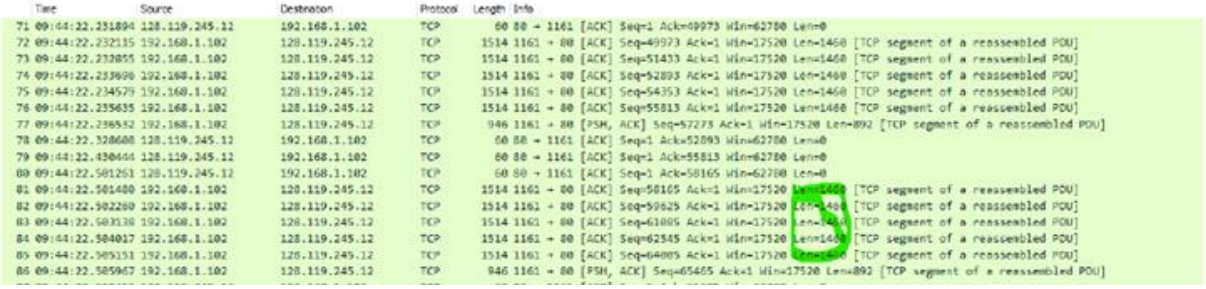
No there are no retransmissions

To check the retransmitted segments, look for the following:

1) The next expected sequence number is greater than current

2) Look for any repeating segment number

10. How much data does the receiver typically acknowledge in an ACK among the first ten datacarrying segments sent from the client to gaia.cs.umass.edu? Can you identify cases where the receiver is ACKing every other received segment among these first ten data-carrying segments?



11. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

Throughput = size of the file / Total time = 23413.45 bytes/sec

12. 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. Consider the "fleets" of packets sent around t = 0.025, t = 0.053, t = 0.082 and t = 0.1. Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase. Figure 6 shows a slightly different view of this data.

TCP is in its slow start phase. There's a fleet of 3 packets, then a fleet of six packets, then a fleet of 12 packets, then a fleet of 24 packets.

13. These "fleets" of segments appear to have some periodicity. What can you say about the period?

14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

I apologize, but I don't have access to the specific trace file that you gathered when transferring a file from your computer to gaia.cs.umass.edu. Without that data, I can't provide a detailed analysis of your personal trace.

However, I can address the first question about the periodicity of the "fleets" of segments:

1. These "fleets" of segments appear to have some periodicity. What can you say about the period?

Based on the information provided in the lab document, we can observe that there are fleets of packets sent around t = 0.025, t = 0.053, t = 0.082, and t = 0.1.

Looking at these time values, we can calculate the approximate periods between these fleets:

- Between first and second fleet: 0.053 - 0.025 = 0.028 seconds

- Between second and third fleet: 0.082 - 0.053 = 0.029 seconds

- Between third and fourth fleet: 0.1 - 0.082 = 0.018 seconds

While not exactly consistent, there seems to be a rough periodicity of about 0.028 to 0.029 seconds between the first three fleets, with a shorter period to the fourth fleet.

This periodicity likely corresponds to the round-trip time (RTT) between the client and the server. In TCP's slow start phase, the sender typically waits for acknowledgments before sending the next fleet of packets. The time between fleets often represents the time it takes for the previous fleet to be acknowledged, which is roughly one RTT.

The shorter period to the fourth fleet might indicate a transition in TCP's behaviour, possibly moving from slow start to congestion avoidance, or it could be due to network conditions changing.

For the second part of your question, to properly answer it for your specific trace, you would need to perform a similar analysis on your own captured data, looking at the timing and size of the packet fleets in your personal trace file.