Lab : 7

Nafisha Akhter(40)
Israt Jahan Mim(52)

UDP

1.
Select the first UDP segment in your trace. What is the packet number of this segment in the trace file?
Ans:
Packet number : 5

What type of application-layer payload or protocol message is being carried in this UDP segment?
Ans:
Type of application-layer payload or protocol message is being carried in this UDP segment : Simple Service Delivery Protocol.

How many fields are there in the UDP header? What are the names of these fields?
Ans:
There are 4 fields in the UDP header.
Names of 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?

Ans:
Each UDP header field is **2 bytes** long. (total header fields length 4 *2=8 bytes)

3.
The value in the Length field is the length of what? Verify your claim with your captured UDP packet.
Ans:
The value in the Length field is = UDP Header (8 bytes) + UDP Data (payload)
My captured UDP packet total length = 283 bytes
UDP payload length = 275bytes
Which basically : 283 − 8 = 275 bytes

4.
What is the maximum number of bytes that can be included in a UDP payload?
Ans:
2^16−1=65,535 bytes
The largest number that can be stored in 16 bits (2 bytes *8=16 bits)

5.
What is the largest possible source port number?
Ans:
The Source Port field is also 2 bytes (16 bits) long.The largest possible source port number is 65,535.

6.
What is the protocol number for UDP? Give your answer in decimal notation.
Ans:
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.

What is the packet number of the first of these two UDP segments in the trace file?

Ans:

Packet no: 15(1st one send by host)

What is the value in the source port field in this UDP segment?

Ans:

Src port: 58350

(1st one send by host)

What is the value in the destination port field in this UDP segment?

Ans:

Des port: 53

(1st one send by host)

What is the packet number of the second of these two UDP segments in the trace file?

Ans:

Packet no: 17(2nd one reply to this first one)

What is the value in the source port field in this second UDP segment?

Ans:

Src port: 53

(2nd one reply to this first one)

What is the value in the destination port field in this second UDP segment?

Ans:

Des port: 58350

(2nd one reply to this first one)

Describe the relationship between the port numbers in the two packets.
Ans:

In the first UDP packet (sent by the host), the source port (58350) is a randomly chosen ephemeral port used by the client, and the destination port (53) is the well-known port for DNS on the server.

In the reply packet, the source and destination ports are reversed —
the source port becomes 53 (from the DNS server), and the destination port becomes 58350 (the client's port).

This way, the client's UDP socket can match the incoming reply to its original request.

TCP

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?
Ans:
IP : 192.168.86.68
TCP port number : 55639

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 : 128.119.245.12
Port number:80

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?
Ans:
Sequence number: 0
Sequence number(raw): 4236649187

What is it in this TCP segment that identifies the segment as a SYN segment?
Ans:
Flag: 0x 002(SYN). This identifies the segment as a SYN segment.

Will the TCP receiver in this session be able to use Selective Acknowledgments?
Ans:
Yes,
Because below the TCP header, in the Option section, SACK permitted.

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?
Ans :
Sequence Number(raw): 1068969752

What is it in the segment that identifies the segment as a SYNACK segment?
Ans :
Flag: 0x012(SYN,ACK). This identifies the segment as a SYNACK segment.

What is the value of the Acknowledgement field in the SYNACK segment?

ANS:
4236649188

How did gaia.cs.umass.edu determine that value?
Ans:
4236649187+1=4236649188
Means gaia.cs.umass.edu received the 4236649187 and it now wants the 4236649187+1=4236649188 basically next one.

5.
What is the sequence number of the TCP segment containing the header of the HTTP POST command?
Ans:
Sequence number 4236801228

How many bytes of data are contained in the payload (data) field of this TCP segment?
Ans:
Payload = 1385 byte.

Did all of the data in the transferred file alice.txt fit into this single Segment?
Ans:
No. They are in multiple segments.

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?
Ans:
0.147682 seconds.

At what time was the ACK for this first data-containing segment received?
Ans:
0.192625 seconds

What is the RTT for this first data-containing segment?
RTT1 = t2 - t1
0.192625 seconds - 0.147682 seconds = 0.044943 seconds

7.
What is the length (header plus payload) of each of the first four data-carrying TCP segments?
Ans:
TCP segment length (header + payload) = TCP header + Payload
= 32 + 1448
= 1480 bytes

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 segments?
Ans:
131712.

Does the lack of receiver buffer space ever throttle the sender for these first four data carrying segments?
Ans:
Window size ≥ payload.
No throttling.

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

No, there are no retransmitted segments in the trace file.Data packet with seq no 17377 was lost as the ack for this packet never arrived,but this was not retransmitted in the file.

10.

How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying 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?

Ans:

The receiver generally sends an ACK for 1448 bytes of data within the first ten segments transmitted from the client to the server.

11.

What is the throughput for the TCP connection? Explain how you calculated this value.

Ans:

0.192625 - 0.024047 = 0.168578

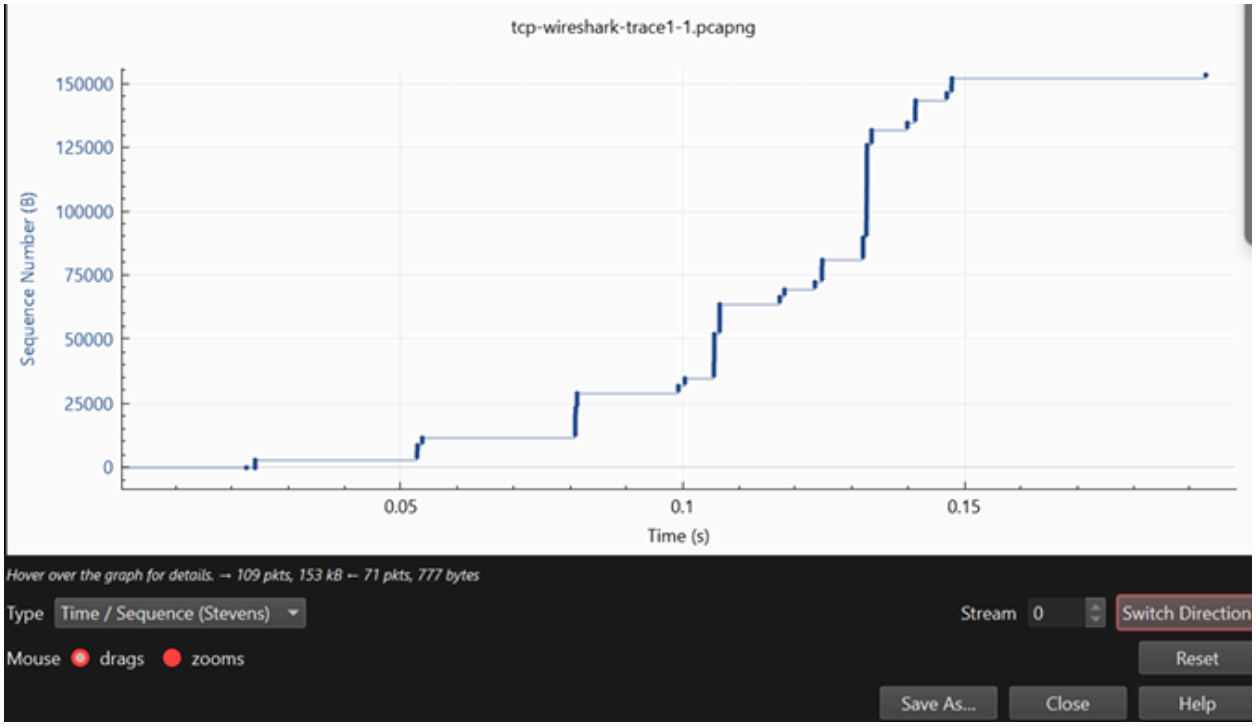
Throughput: 153,425/0.16857 = 909,641 bytes/s

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.

Ans:

Initially, the connection exhibits slow-start behavior during the indicated fleets, and later the pattern transitions into congestion-avoidance.



13.

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

Ans:

The differences between the fleet times are as follows:

- 0.053 − 0.025 = 0.028 s
- 0.082 − 0.053 = 0.029 s
- 0.100 − 0.082 = 0.018 s

Taking the two largest gaps, the average difference is around 0.028–0.03 seconds (28–30 ms). This interval represents the round-trip time (RTT) for the connection, meaning each fleet is sent approximately one RTT apart.

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

Ans: