CSCE 5580 COMPUTER NETWORKING

Lab Wireshark TCP

Ganesh Gundekarla

11700551

Question 01

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? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you’re uncertain about the Wireshark windows.

A screenshot of a computer

Description automatically generated

IP address of source is : (aka client computer) : 192.168.1.85

Source port of the client computer is : 57726(Dynamic Port Allocation)

Question 02

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?

Destination Ip address: 128.119.245.12 port : 80

A screenshot of a computer

Description automatically generated

Question 03

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

My IP address source is : sending on port no :

Question 04

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?

Here the process no(frame num) 38 initiates the connection with the client computer and the gaia.cs.umass.edu , so that is set up with a seq number with 0

**Sequence Number : 0** (relative sequence number) , **Sequence Number (raw): 2177923976**

Flags: 0x002 (SYN) identifies the segment as SYN segment and you can see in the below picture only the Syn: Set is turned on.

A screenshot of a computer

Description automatically generated

Question-5:

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?

**SynAck** is arriving from port 80(destination) to client’s computer.

1. **Sequence Number(relative one) = 0 , Sequence Number (raw): 3230991122**
2. **Acknowledgment Number: 1 (relative ack number),** **Acknowledgment number (raw): 2177923977**
3. **Basically determined by the [initial seq number +1]**
4. Identified using the Flags
5. **Flags: 0x012 (SYN, ACK) ,** this indicates that the flag is set to **SYNACK** and these are turned on in the flags section .
6. **Acknowledgement : Set**
7. **Syn : Set**

A screenshot of a computer

Description automatically generated

Question : 6

What is the sequence number of the TCP segment containing the HTTP POST command? Note that 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.

Frame no 44

Sequence number of the TCP segment containing the HTTP Post command is

Sequence Number: 1 (relative sequence number); Sequence Number (raw): 2177923977

In the below screenshot we can see the “post” in its data field.

A screenshot of a computer

Description automatically generated

Question : 7

What is the maximum segment size in the first ACK by server

The first ACK sent by the server to the client computer is in frame no 42

The ‘maximum segment size’ in the first ACK by the “server” is 1432 bytes.

A screenshot of a computer

Description automatically generated

Question : 8

What is round trip time (RRT) for the ACK received by the server?

Frame no 42

Round trip time for the ACK received by the server is

**[The RTT to ACK the segment was: 0.061738000 seconds]**

A screenshot of a computer

Description automatically generated

Question : 9

What is the calculated window size and checksum in the HTTP first packet?

Frame no 44 is the first packet that is being sent here in my case reason is that we see the PSH in the info and the data field contains POST .

[Calculated window size: 262144]

Checksum: 0xf42a [unverified]

A screenshot of a computer

Description automatically generated

Question 10 :

Is the PUSH flag set? If yes? What is its significance?

Yes , in many frames we can see the push flag that is being set to 1 .

Significance of PUSH flag:

1. Enables for more efficient data transfer and a much more efficient communication.
2. It is highly required for the applications that require real time data delivery or a connection that deals with the low-latency communication.
3. The general aim behind the push flag is that it is used to tell the sender is sending the data receiver without any further ado and there will be no buffer filling in this scenario.
4. This flag means that the data is directly ‘pushed’ to the received one’s application layer immediately.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Question : 11

What is the font face and acknowledgement number of the HTTP packet which has the status of 200 OK?

Font face = ="Arial, Helvetica, sans-serif" size="4"

Acknowledgment Number: 152937 (relative ack number)

Acknowledgment number (raw): 2178076913

A screenshot of a computer

Description automatically generated

Question: 12

How is the connection closed? (Hint: FIN flag) Attach the screenshot of flags which are set at the end?

The signals sent between sender and receiver, FIN flag is the signals termination of a connection . It means the connection is being closed for the frame.

Question : 13

Who has set the FIN bit? Is it server or client? Attach the screenshot?

Question: 14

What is the acknowledgement number of the last TCP ACK?

Acknowledgment Number: 778 (relative ack number)

Acknowledgment number (raw): 3230991900

A screenshot of a computer

Description automatically generated