Southern University of Science and Technology

Computer Networking Lab Report

Name： 吴培霖 **Student Number：** 11711717

Major: None

Time： 2018/11/10

Introduction：

Assignment 6.1

Select one UDP packet from your trace.

1. From this packet, determine how many fields there are in the UDP header. Name these fields.
2. consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.
3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.
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)
5. What is the largest possible source port number? (Hint: see the hint in 4.)
6. What is the protocol number for UDP?(Give your answer in both hexadecimal and decimal notation.)

•

Examine a 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.

1. Describe the relationship between the port numbers in the two packets.

Assignment 6.2 TCP

Finish the question 3~10 question of Wireshark_TCP_v7.0.pdf

Procedure:

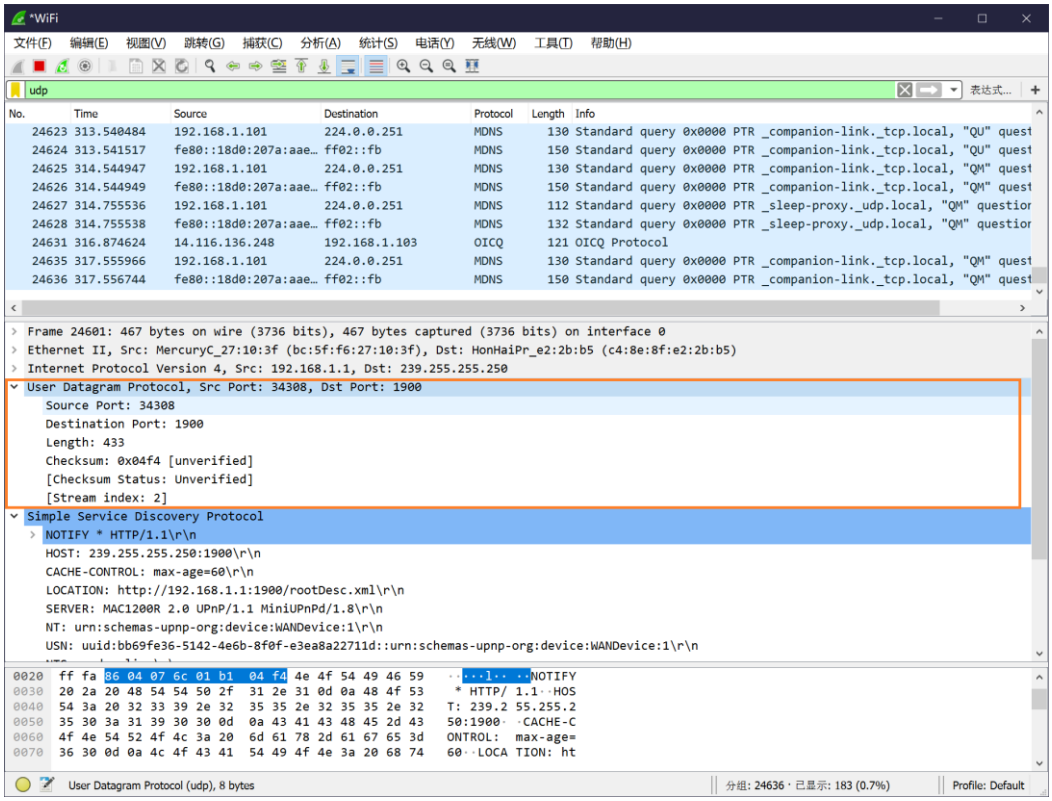
Assignment 6.1

1. Open the Wireshark, select WiFi to monitor, then type ‘udp’ to filter the message.
2.Then we can see the result in the fig.1 showed in result. The message in the User Datagram Protocol is the head of UDP header.
3.After search in the Internet showed in the fig.2, we know the information of each header fields.
4.The hexadecimal data is showed in the fig.3.
5.We can find the protocol number of UDP in the IP field in the fig.4.

Assignment 6.2 TCP

1.First we download the alice.txt from http://gaia.cs.umass.edu/wiresharklabs/ alice.txt.
2. Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.. Attach alice.txt to the browser(fig.5). Open the Wireshark to start the package capture. Click upload (fig.6), then stop Wireshark capture.
3.Then filter TCP result, we can find many packages show in the Wireshark. (fig7)

Result:



(fig.1 The header field of this UDP package)

Source port number

This field identifies the sender's port when meaningful and should be assumed to be the port to reply to if needed. If not used, then it should be zero. If the source host is the client, the port number is likely to be an ephemeral port number. If the source host is the server, the port number is likely to be a well-known port number.[4]

Destination port number

This field identifies the receiver's port and is required. Similar to source port number, if the client is the destination host then the port number will likely be an ephemeral port number and if the destination host is the server then the port number will likely be a well-known port number.[4]

Length

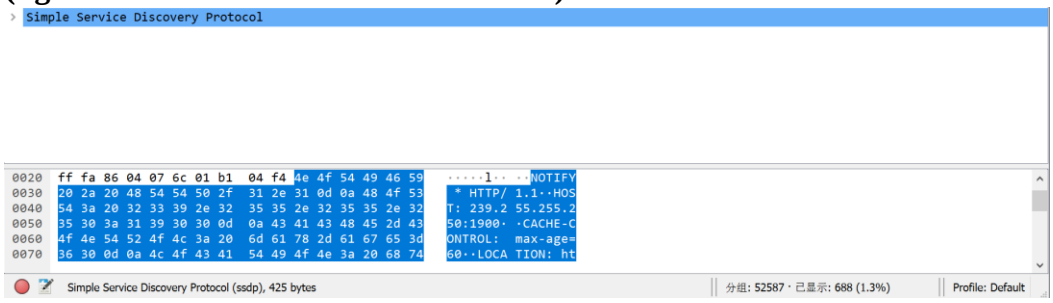
A field that specifies the length in bytes of the UDP header and UDP data. The minimum length is 8 bytes because that is the length of the header. The field size sets a theoretical limit of 65,535 bytes (8 byte header + 65,527 bytes of data) for a UDP datagram. However the actual limit for the data length, which is imposed by the underlying IPv4 protocol, is 65,507 bytes (65,535 − 8 byte UDP header − 20 byte IP header).[4]

In IPv6 jumbograms it is possible to have UDP packets of size greater than 65,535 bytes.[5] RFC 2675 specifies that the length field is set to zero if the length of the UDP header plus UDP data is greater than 65,535.

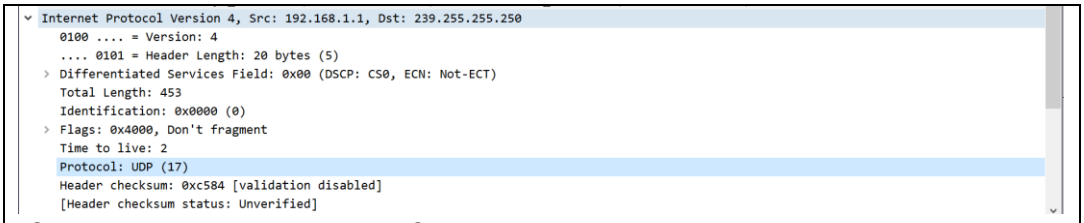
Checksum

The checksum field may be used for error-checking of the header and data. This field is optional in IPv4, and mandatory in IPv6.[6] The field carries all-zeros if unused.[7]

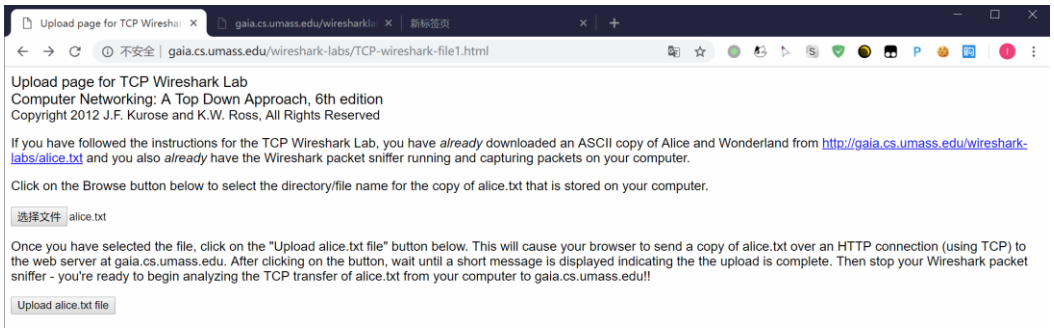
(fig.2 The information found in the Wiki)



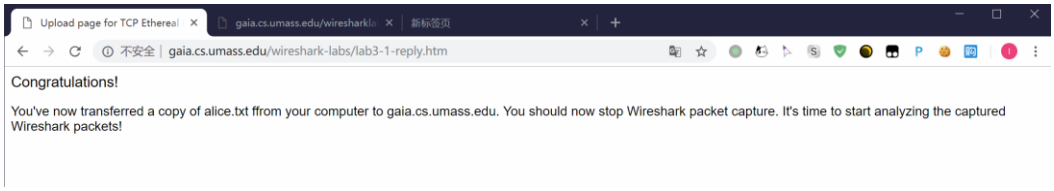
(fig.3 The hexadecimal data of the content of this UDP package *not all data are showed above*)



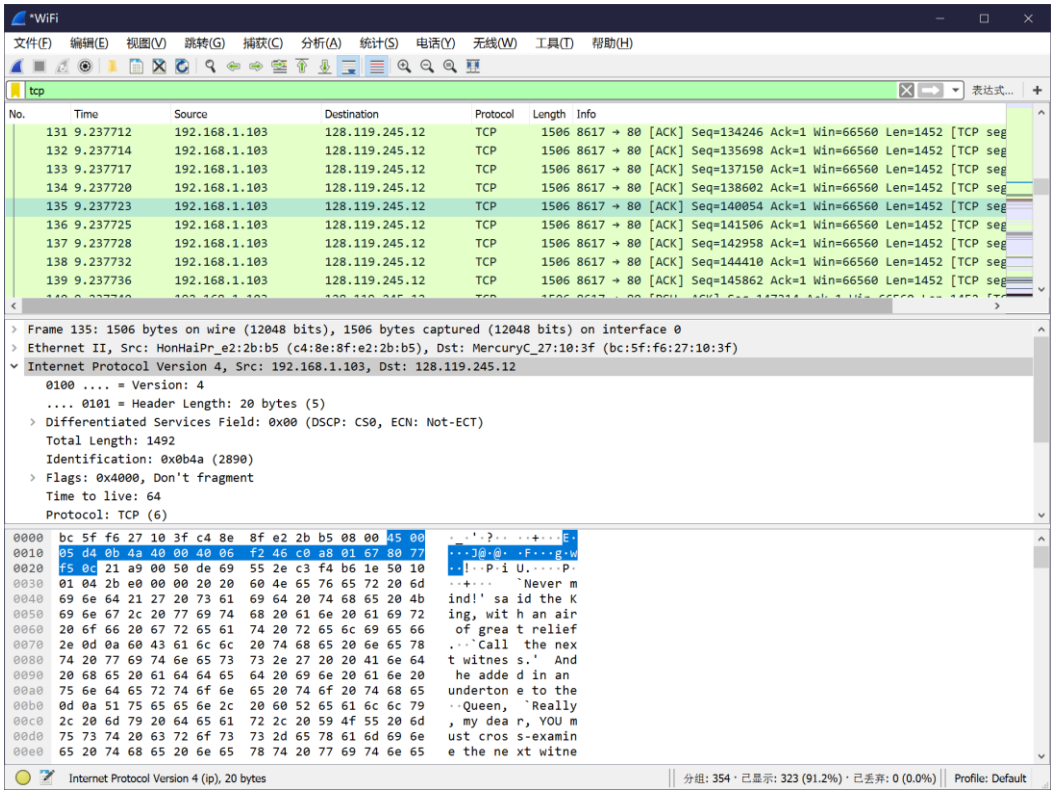
(fig.4 The protocol number of UDP)



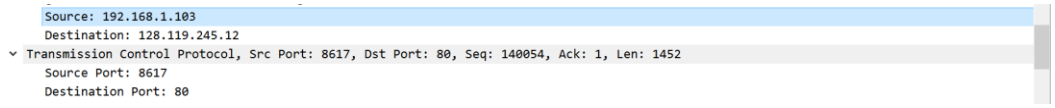
(fig.5 Attach alice.txt to the browser)



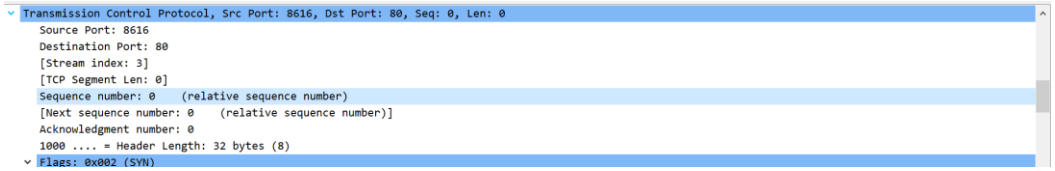
(fig.6 Upload alice.txt)



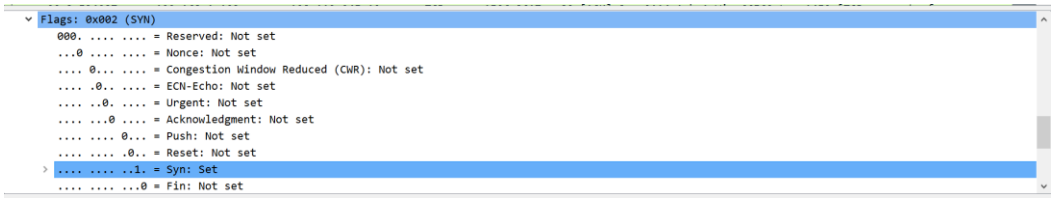
(fig.7 Packages captured by Wireshark)



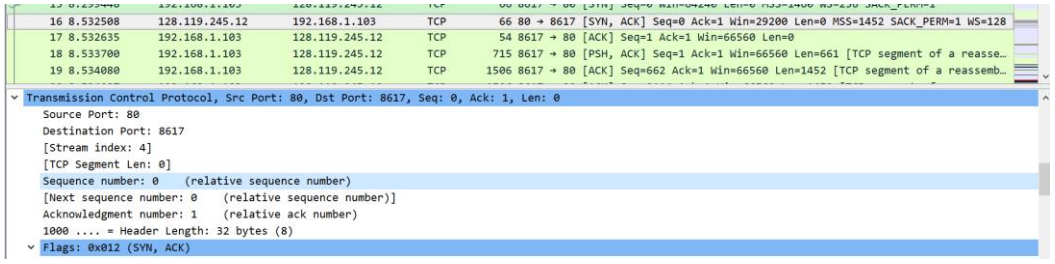
(fig.8 Source IP and source port)



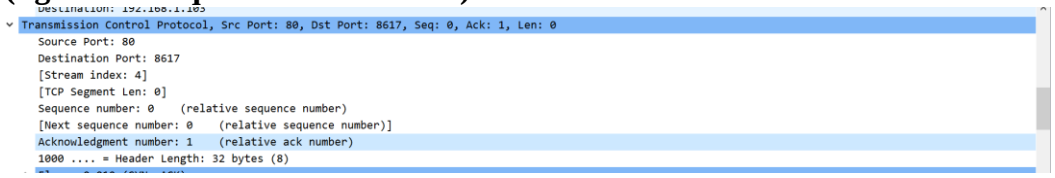
(fig.9 Sequence number of SYN segment)



(fig.10 Flag field identify the segment as a SYN segment)

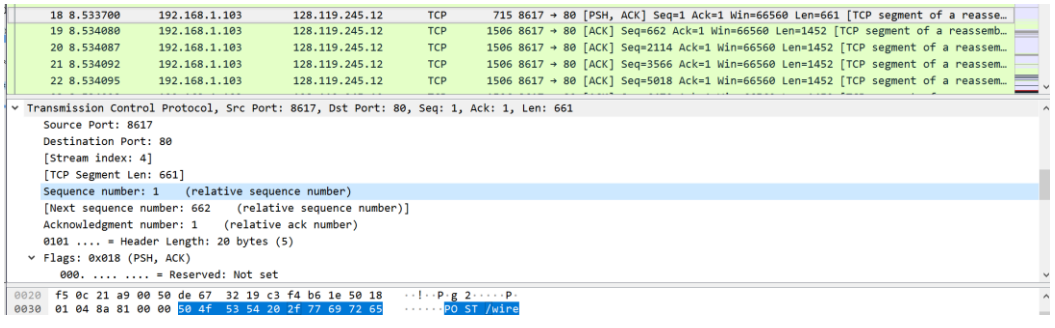


(fig.11 The sequence of SYNACK)



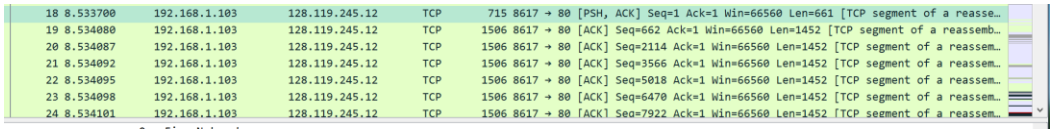
(fit.12 The acknowledgement field of SYNACK)

(fig.13 Flag field)

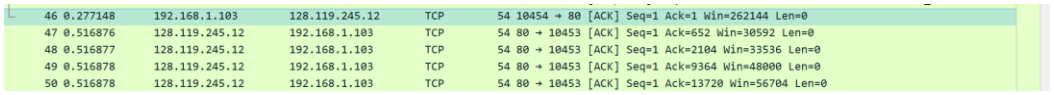


(fig.14 The sequence number of the TCP segment contain HTTP POST)

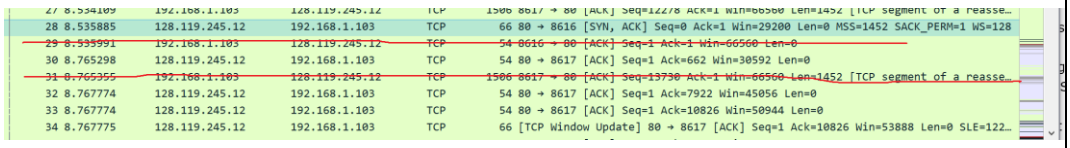
(fig.15 POST is in the line 0030)



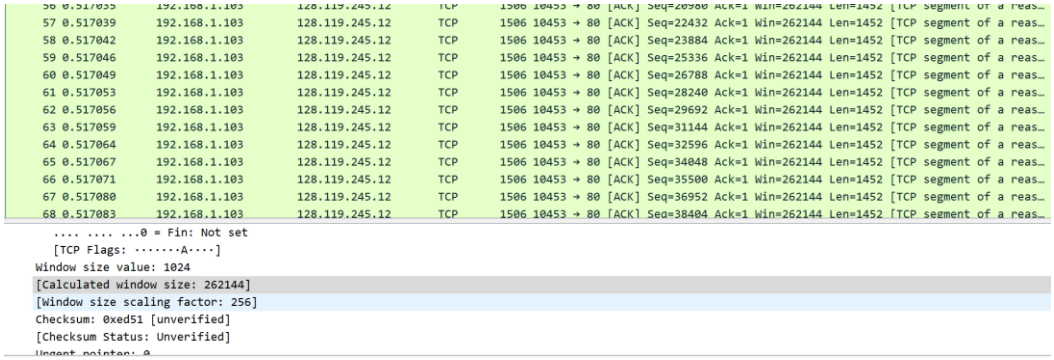
(fig.16 Sequence number of the first six segments: No.35~40)



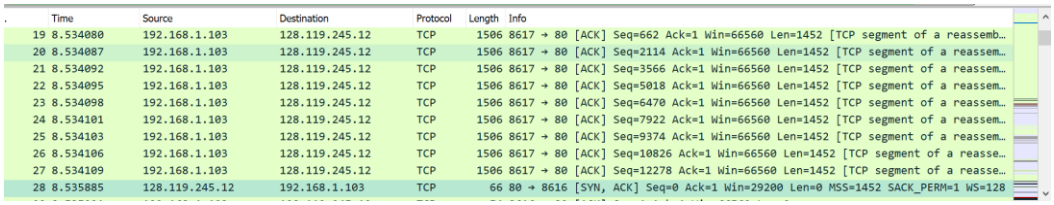
(fig.17 The time when ACK for each segment received)



(fig.18 The length of first six segment)



(fig.19 The calcluated window size in entire connection)



(fig.20 No package is retransimited)

Analysis(including answer of question):

Assignment 6.1

1.From the fig.1 we can see there are four fields in the UDP header.
They are: **Source port, Destination Port, Length and Checksum.**

2.The fig.2 shows that each function of the header fields in the UDP header.
The length of each of the UDP header fields is **2 bytes.**

3.From the fig.1, we can see the length field in the length is **433.**
We can verify by counting the byte number of the content showed in the fig.3.

4.From question 2, we learn that the length of length field is 2 bytes. 2 bytes contain 2*8=16 bits, so that the maximum number of the length is 2^16=65536. But IP field take up 20bytes, UDP header take up 8 bytes. So the answer is **65536-28=65507 bytes.**

5.The length of source port number is 2bytes. The largest possible source port number is **2^16=65536.**

6. See the fig.4, we can learn the protocol number is **$(17)_{10}$ or $(11)_{16}$.**

Assignment 6.2 TCP

3.Q: What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?
A: From fig.8, we can know the IP address and TCP port number by you client are **192.168.1.103 and 8617.**

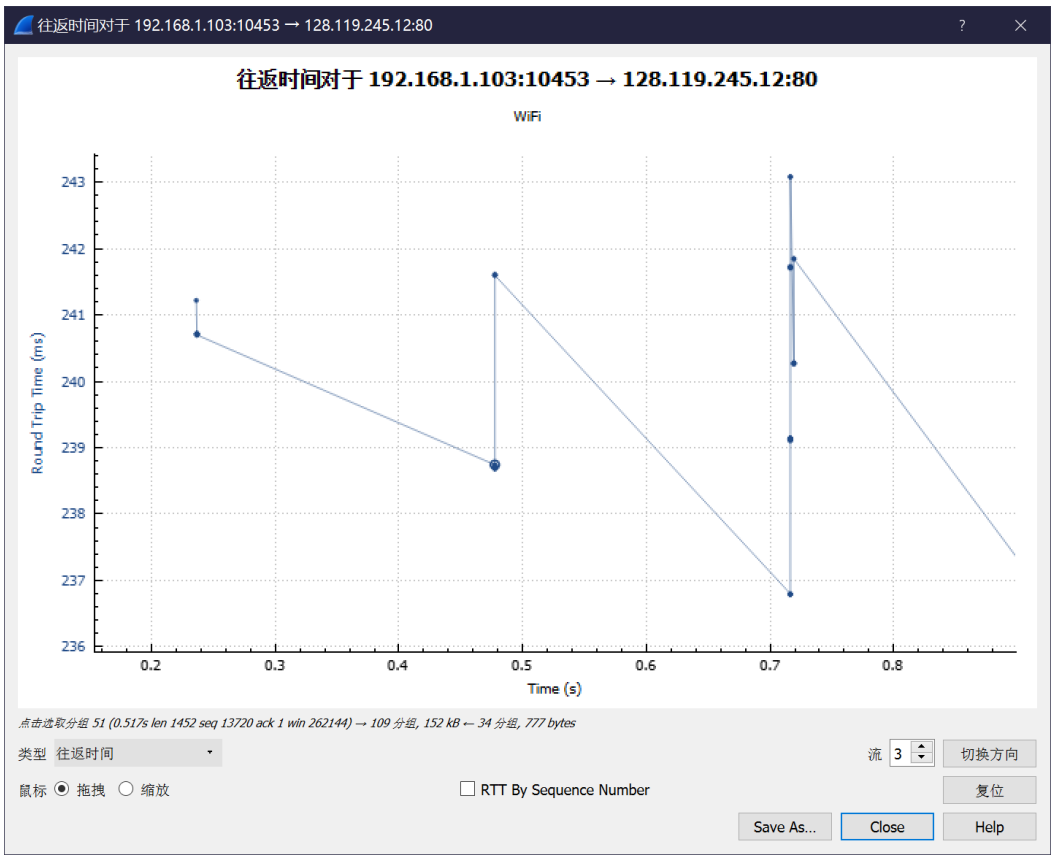
4.Q: What is the sequence number of the TCP SYN segment that is used to initiate the
TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
A: (1) The sequence number of the TCP SYN segment is **0(fig.9).**
(2) The **flag segment** identify this segment as a SYN segment.

5.Q: 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?
A: (1) The sequence of SYNACK is **0(fig.11).**
(2) The value of the acknowledgement field is **1(fig.12).**
(3) Server add 1 to the sequence number of SNY segment.

(4) The flag field identify the segment as a SYNACK segment **by set Acknowledgement as value 1(fig.13).**

6. Q: 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.
A: (1) The sequence number showed in the fig.14 is **1.**
(2) The 'POST' is shown in the fig.15.

7. Q: 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 EstimatedRTT value (see Section 3.5.3, page 242 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.
Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph->Round Trip Time Graph.
A: (1) **1, 662, 2114, 3566, 5008, 6460 (fig.16)**
(2) **0.516876, 0.516877,0.516878,0.516878,0.516878,0.516878(fig.17)**
(3) **0.241217, 0.240723, 0.240717, 0.240616, 0.240619, 0.240622(fig.16,17)**
(4) EstimatedRTT value=**0.240947**



8. Q: What is the length of each of the first six TCP segments?

A: The length of them are **66, 54, 54, 54, 54, 66(fig.18).**

9. Q: 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?

A: (1) The minimum amount of buffer space is the calculated window size value **262144(fig.19).**

(2) No, the buffer space of the receiver is large enough so that it does not throttle the sender.

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

A: No, there is no segment is retransmitted. We can check if the sequence number of packages sent by client are duplicated**(fig.20).**

Conclusion and Experience：

From this assignment, we learn how to use Wireshark to capture TCP package and how to analysis it. Also, we learn the principle of UDP protocol, TCP protocol and how it works.

Tips：