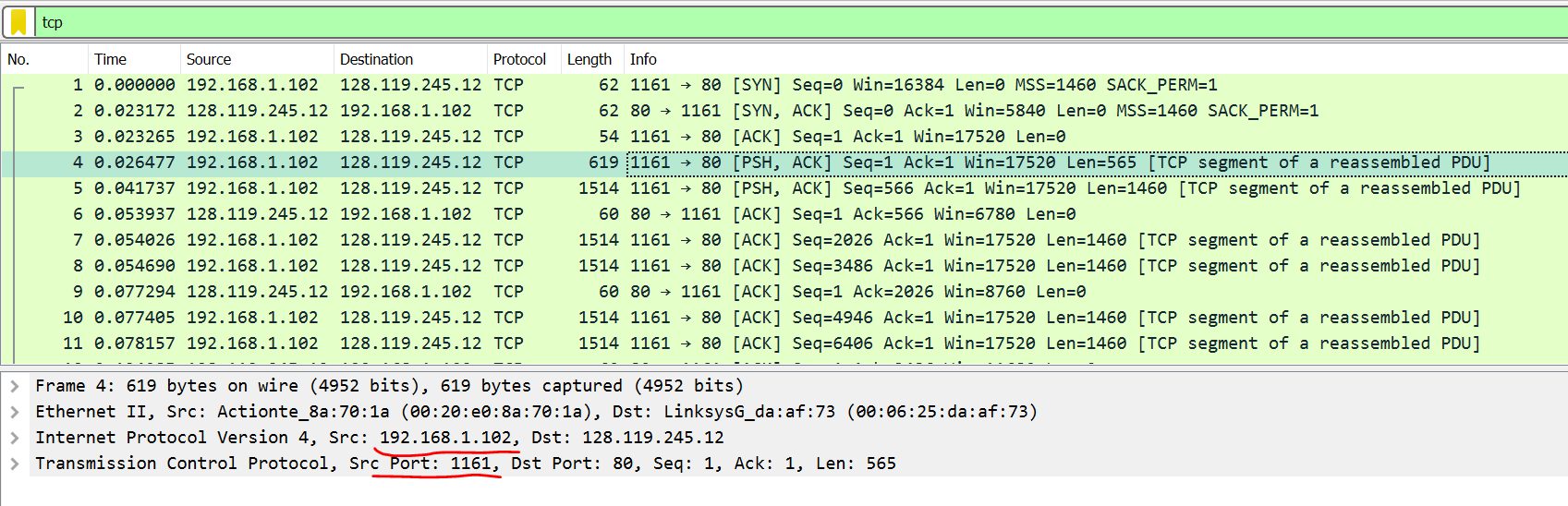
**Lab 08**

# Lab Statement 1: Analyzing TCP Packets using Wireshark (10)

**Question 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?

IP: 192.168.1.102

TCP port: 1161



**Question 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?

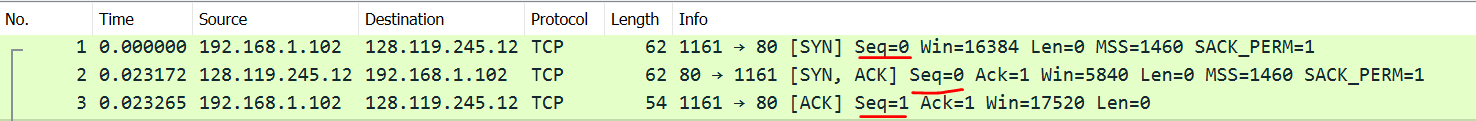
IP: 128.119.245.12

TCP port: 80

**Question 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 in the segment that identifies the segment as a SYN segment?

Sequence num=0

SYN segment is used to establish the connection between client and server



**Question 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 the value of the Acknowledgement field in the SYNACK segment? What is it in the segment that identifies the segment as a SYNACK segment?

Client to server 🡪 SYN: 0 SYNACK:0

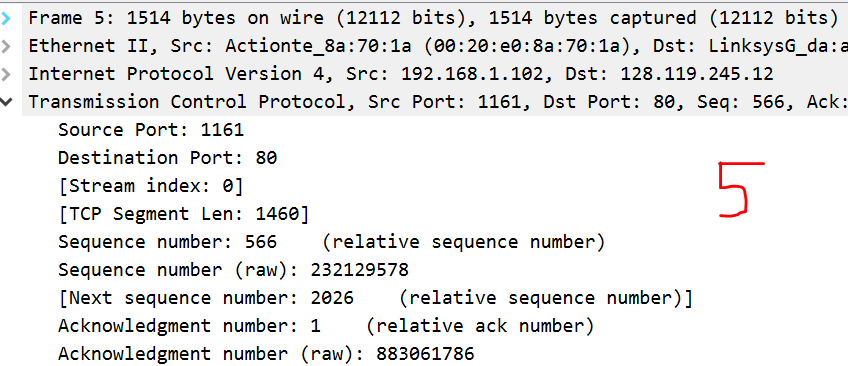
Sever to client: 🡪 SYN:0 SYNACK:1

Client to server 🡪 SYN:1 SYNACK:1

When SYN flag and ACK flag is 1, they identifies that the segment is SYNACK segment.

**\*Question 5:** In packet 9, **Ack = 2026** and **Seq = 1**. Explain these values?

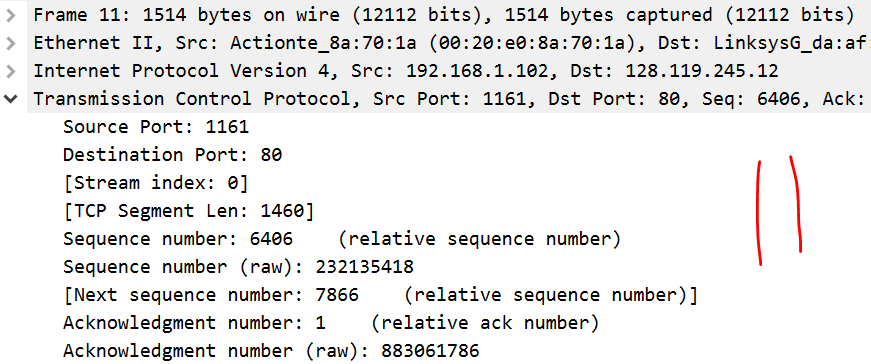
Packet 5 some details:



See the next seq numeber here is 2026. So the ack number in Packet 9 shows that this packet is connect to packet 5 and this packet is the ack segment for packet 5.

**\*Question 6:** In packet 16, **Ack = 7866** and **Seq = 1**. Explain these values?

Some packet 11 details:



See the next seq numeber here is 7866. So the ack number in Packet 16 shows that this packet is connect to packet 11 and this packet is the ack segment for packet 11.

**Question 7:** Why Wireshark uses relative sequence and ack?

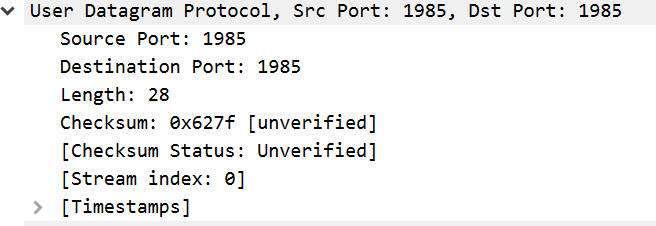
To make it easy to user to understand. To real numbers are difficult to compare and match so wireshark uses relative numbers to make it easy for us. You can also see the raw numbers in above picture

**Lab Statement 2: Analyzing UDP Packets using Wireshark (5)**

**Question 1:** Select the first DNS packet in the trace. Determine, how many fields there are in the UDP header.

Src port, dst port, length, checksum, stream index, timestamp

There are 6 fields as show below.

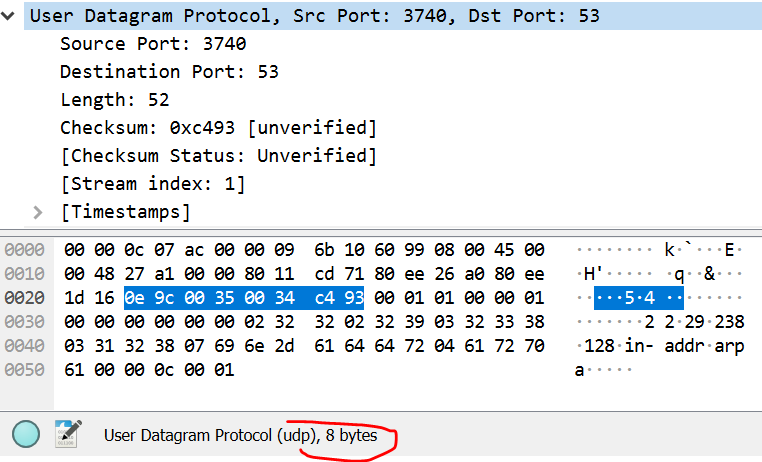


**Question 2:** From the packet content field (click on any hea

der and observe the display in the Packet Bytes Window), determine the length (in bytes) of each of the UDP header fields.

**Question 3:**  The value in the Length field is the length of what? Verify your claim using the selected packet.

This is the sum of header(8) and data(44) bytes.



**Question 4:**  What is the port number to query the DNS Server?

53