Task1

Q1

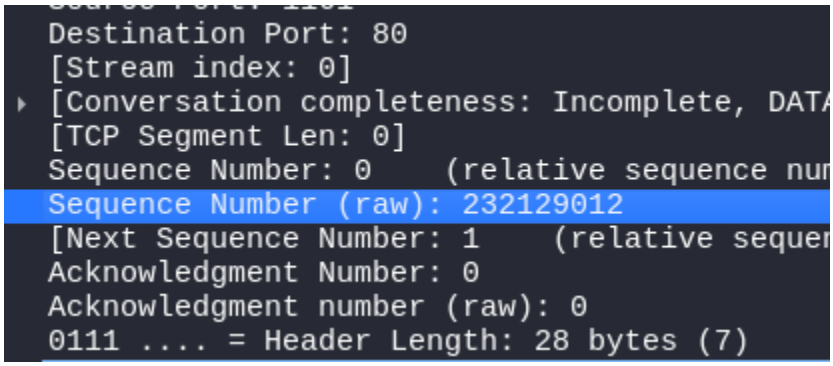
The source is the MIT address and the IP address and port no. of the source is
IP Address : 192.168.1.102
Port No : 1161

Q2

The destination is the gaia.cs.umass.edu and the IP address and port no. of the destination is
IP Address : 128.119.245.12
Port No : 80

Q3

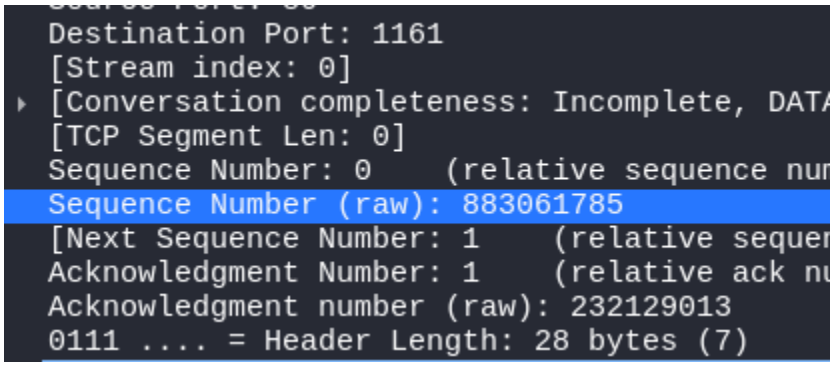
The “Seq=0” also tells that the connection is being established. The SYN Flag in the segment identifies that the segment is a SYN Segment.



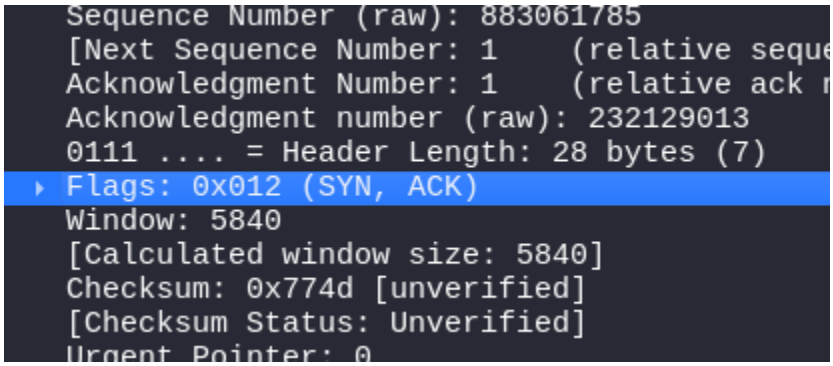
Q4

The seq no. is still 0. It will be 1 when the connection is established.

The value of the acknowledgement is the same as the sequence number of the previous packet (i.e the syn packet in Q3) - 232129013



The Flag 0x012 (SYN,ACK) tells us that this is a segment that



Q5

Q6

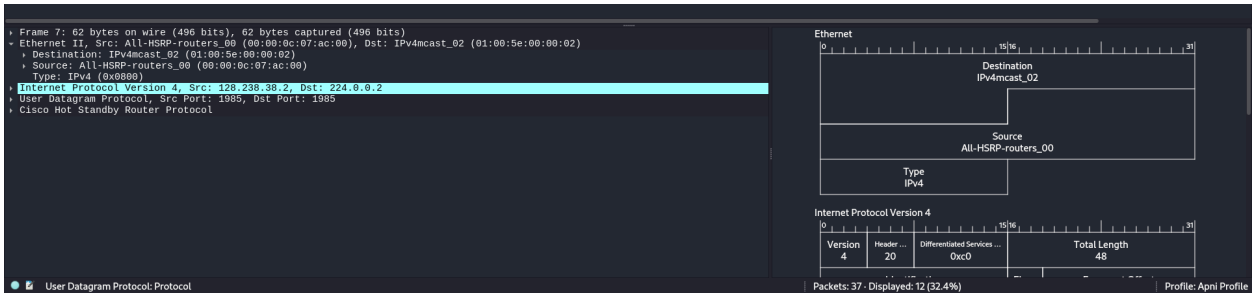
In both these questions the seq=1 indicates that the client is sending more data and isn't done sending the data yet. Meaning that this packet from the client is part of the ongoing data flow in the established connection. And the ACK tells the number of bytes to be expected by the client.

Q7

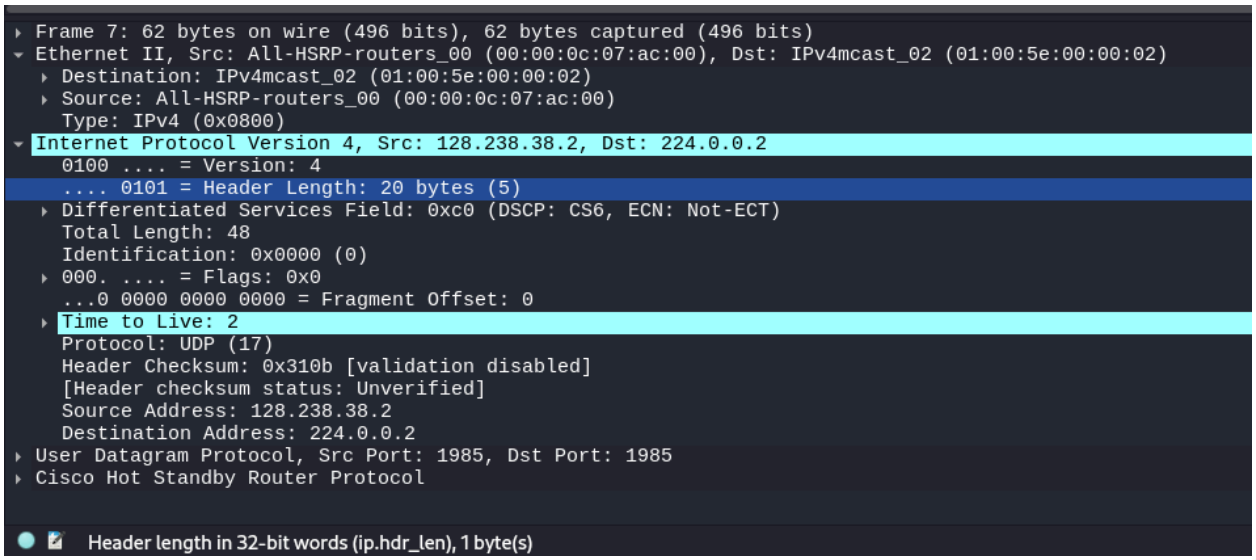
Wireshark uses relative sequence and acknowledgment numbers to make it easier to track data flow by starting counts from zero, rather than showing large, random numbers. The TCP seq numbers are usually very large numbers for security reasons. Relative seq and ack simplifies analysis and helps spot issues in TCP connections quickly.

Task2

Q1



There are 3 i think
The destination, the source and the type
The header length is 20 bytes



Q2

As already answered in Q1. The length of the header is 20 bytes for the 1st packet. All the other packets also have a header length of 20 bytes.

Q3

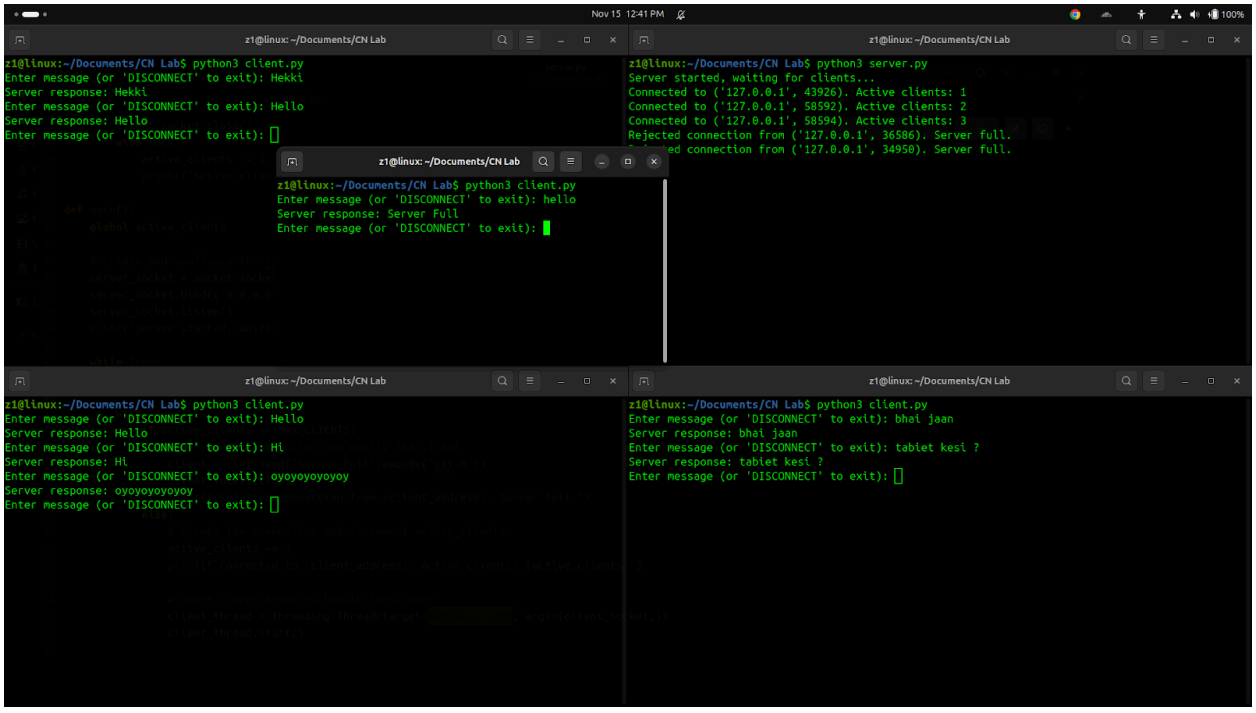
The length of the header is 20 bytes for all packets. All the other packets also have a header length of 20 bytes. The length however keeps varying because it tells you this
Length = header length + payload/data
Since the data being sent is different in each packet hence the length for each packet keeps changing.

Q4

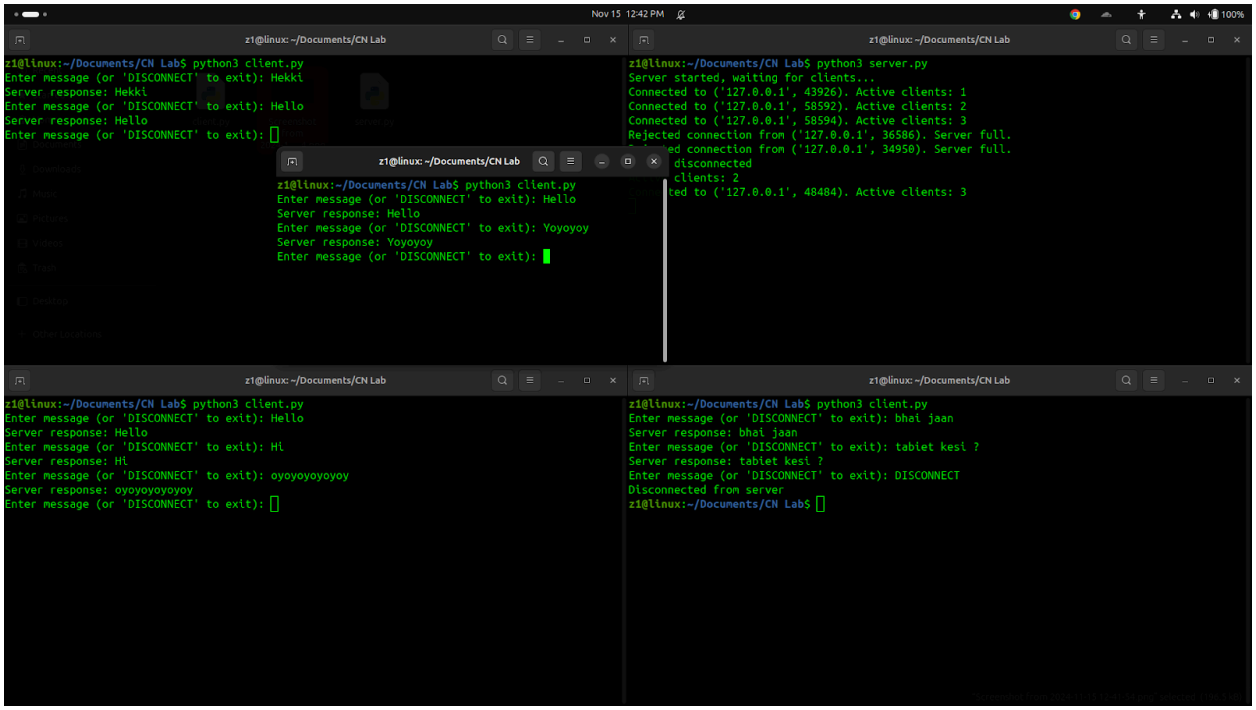
I think the port number to query the DNS server is 53.

But another possible thing is that it's 3740 because in the next packet the port changes to 3741 and then 3742. That means that the port is increasing one by one but the other port remains the same. That makes me think that port 53 is the client's port. Just a thought.

Task3



The top right is the server. The rest are clients. The smaller terminal in the middle is trying to connect when 3 users are already connected. This gives the error to the 4th client trying to connect.



The bottom right client i.e the 3rd client disconnects and the total active users in the server are decreased. So now the client that was denied access before can connect (i.e the box in the middle)