Lab Statement 1

Question 1

Client IP Address: 192.168.1.102
Client TCP Port Number: 1161

Question 2

IP address of gaia.cs.umass.edu: 128.119.245.12
Port number of gaia.cs.umass.edu: 80

Question 3

Sequence number of the TCP SYN: 0
The SYN flag = 1 which means that the segment is SYN.

Question 4

sequence number of the SYNACK: 0
value of the Acknowledgement field in the SYNACK segment: 1
The SYN flag = 1 and the Acknowledgment flag = 1 which means that the segment is a SYNACK segment.

Question 5

ACK=2026 indicates that 2026 bytes of data were successfully read, whereas Seq = 1 represents the Ack number of the previous connection, which was ACK=1 in frame=5. When we add seq num and the Len of the bytes in frame 5, we get 2026, which is the Ack number.

Question 6

ACK=7866 indicates that 7866 bytes of data were successfully read, and Seq = 1 indicates the last connection's Ack number, which was Ack =1 in frame =11. When we add seq num and the Len of the bytes in frame 11, we get 7866, which is the Ack number.

Question 7

Because relative sequence and ack make the values much smaller and easier to read and compare than real values, Wireshark employs them. The ACK signifies that the host has acknowledged receiving data.

Lab Statement 2

Question 1

There are 4 fields in the UDP header. These are source port, destination port length and checksum.

Question 2

The length of each of the UDP header fields is 2 bytes.

Question 3

The number of bytes in the UDP segment, which is the total of header and data bytes, is the value in the Length field.

For example, the length of packet number 16 is the sum of 8 header bytes plus 76 encapsulated data bytes, for a total length of 84 bytes.

Question 4

Port number to query the DNS Server: 53

Lab Statement 3:

1- Are ICMP messages sent over UDP or TCP?	UDP
2- What is the link-layer (e.g., Ethernet) address of the host?	Address: IntelCor_55:7b:ac (60:67:20:55:7b:ac)
3- Which kind of request is sent through these ICMP packets?	Echo request
4- How many requests are sent through the host?	4
5- What is the IP address of your host? What is the IP address of the destination host?	IP address of host: 192.168.33.110 IP address of the destination host: 172.217.27.36
6- Why is it that an ICMP packet does not have source and destination port numbers?	Because it sends network-layer information between hosts and routers rather than between application layer processes, the ICMP packet lacks source and destination port numbers..
7- What values in the ICMP request message differentiate this message from the ICMP reply message?	The ICMP type is used to distinguish between request and reply messages. The request message type is 8 and the response is 0.
8- Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?	ICMP code=0 and type=8. Checksum, data fields, sequence number, and identification are among the other fields found in an ICMP packet. Each of the checksum, sequence number, and identification fields is two bytes in length..
9- Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?	ICMP code=0 and type=0 Checksum, data fields, sequence number, and identification are among the

10- Examine the packet no 56. What are the ICMP type and code numbers? Why is the IP and TCP Header included in the ICMP Header? What does these headers depict?	Code=3 and type=3. The ICMP Header contains the IP and TCP headers, allowing the end system to determine which packet failed.