PART I

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?

The IP address of the source is 192.168.1.102 and port number is 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?

The IP address of gaia.cs.umass.edu is 128.119.245.12 and port number is 80 as it is an http session

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?

The sequence number of that segment is 0. In that segment the SYN flag of the TCP header is true which indicates that it is a SYN segment

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?

The sequence number of that segment is also 0, ACK value is 1. In that segment, the SYN and ACK flag of the TCP header is true/1 which indicates that it is a SYNACK segment

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

The ACK number indicates that what is the next sequence number the destination has to send after the packet is received on the other end. So in this case, the data up to 2025 has been received and next required sequence number is 2026. Whereas on the source side, the sequence number is the starting byte number of the data which is being send. So in this case the sequence number is 1 so starting from 0 byte number 1 is the starting byte of the data being sent in the segment.

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

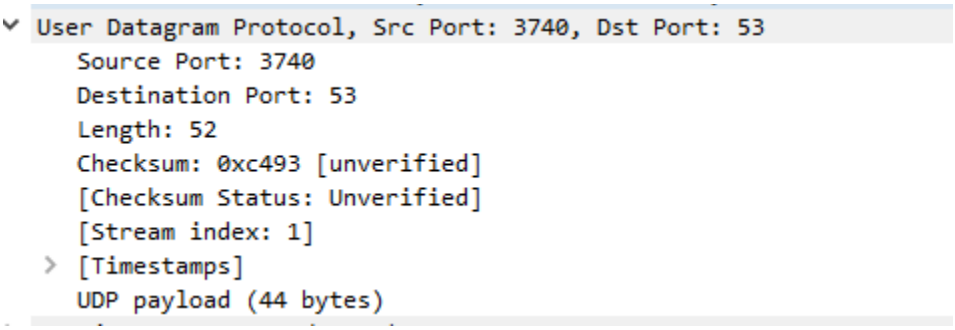
The ACK number indicates that what is the next sequence number the destination has to send after the packet is received on the other end. So in this case, the data up to 7865 has been received and next required sequence number is 7866. Whereas on the source side, the sequence number is the starting byte number of the data which is being send. So in this case the sequence number is 1 so starting from 0 byte number 1 is the starting byte of the data being sent in the segment.

Question 7: Why Wireshark uses relative sequence and ack?

The relative sequence and ack as easier to understand for us as users, therefore wireshark uses relative modes.

PART II

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



There are 4 fields i.e. Source port, dest port, length and checksum

Question 2: From the packet content field (click on any header and observe the display in the Packet Bytes Window), determine the length (in bytes) of each of the UDP header fields.

Each UDP header is of 2 bytes.

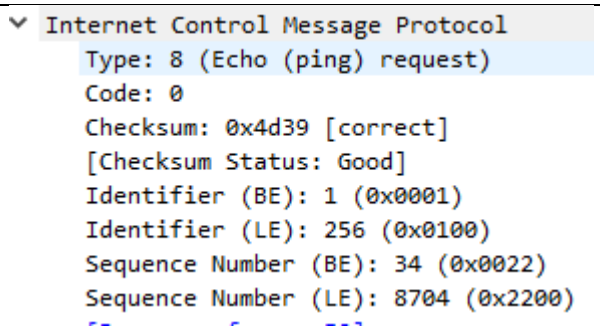
Question 3: The value in the Length field is the length of what? Verify your claim using the selected packet.

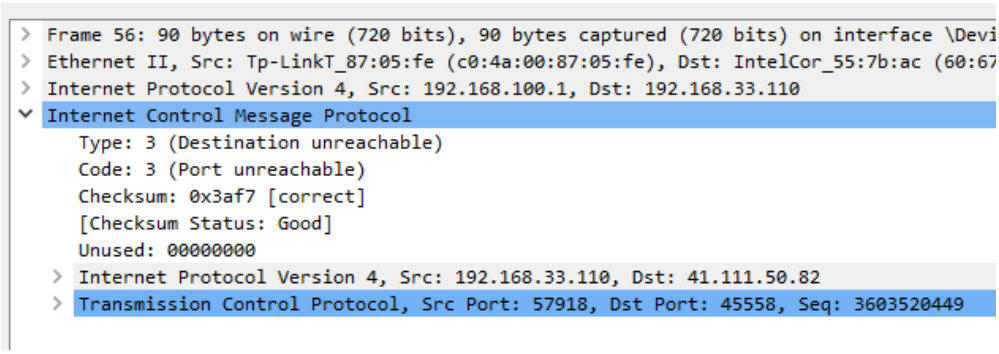
This is the size of content + size of header.

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

The port number is 53

PART III

1- Are ICMP messages sent over UDP or TCP?	ICMP neither uses UDP nor TCP
2- What is the link-layer (e.g., Ethernet) address of the host?	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?	172.217.27.36 & 192.168.33.110
6- Why is it that an ICMP packet does not have source and destination port numbers?	Connectionless protocol
7- What values in the ICMP request message differentiate this message from the ICMP reply message?	We can identify that with packet number wireshark provide
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	 The icmp type number is 8 and code number is 0. Other fields are checksum, identifier, sequence number Each field is 2 bytes.

and identifier fields?	
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?	Internet Control Message Protocol Type: 0 (Echo (ping) reply) Code: 0 Checksum: 0x5539 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence Number (BE): 34 (0x0022) Sequence Number (LE): 8704 (0x2200) [Request frame: 48] [Response time: 98.363 ms] The icmp type number is 0 and code number is 0. Other fields are checksum, identifier, sequence number Each field is 2 bytes.
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?	 The icmp type number is 3 and code number is 3 The TCP & IP header is wrapped inside ICMP header. It is used to send back error message when destination is unreachable.