Assignment - Wireshark

DNS

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of the DNS response message?
3. To what IP address is the DNS query message sent?
4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
5. Examine the DNS response message. How many "Answers, Authoritative & Additional" are provided? What does each of these answers contain?

   Provide a screenshot of all the above questions with answers

TCP/IP

6. Which field indicates the version of Internet protocol in use?
7. What are the Source and destination IP addresses of the IP Packet?
8. What is the IP Header Length and what is the size of the field used to indicate it?
9. What is the Length of the IP packet whose source address is your IP? (Choose any one packet)
10. Which field indicates whether the IP Packet has been fragmented or not and how?
11. What is the TTL value of the IP packet?
12. Which field verifies the integrity of the IP Header?

   Upload screenshots of all the above questions with answer