

Lab 2: DNS – UDP - TCP

- + Take as many screen pictures as possible and insert into your answer sheet
- + Return your answer in pdf or docfile with file name likes this

GROUP-CODE-NAME-DNS-UDP-TCP

Ex: [SE0709](#)- [SE02436](#)-[Linhlm](#)-DNS-UDP-TCP

I - DNS

1. Run nslookup to obtain the IP address of a Web server FU (www.fpt.edu.vn).
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
3. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

II - UDP

1. Select one packet. From this packet, determine how many fields there are in the UDP header. (Do not look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.
2. From the packet content field, determine the length (in bytes) of each of the UDP header fields.
3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.
4. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. (To answer this question, you'll need to look into the IP header.)

III. TCP

1. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu? What is the IP address and port number used by gaia.cs.umass.edu to receive the file.
2. 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 it in the segment that identifies the segment as a SYN segment ?
3. 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 ? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

4. What is the sequence number of the TCP segment containing the HTTP POST command ?
Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.