CSP334: Computer Networks
Homework Assignment No 6
Chap 3, Application Layer: DNS Wireshark Assignment

Date of submission : 23:59 hrs, 26$^{\text{th}}$ October 2018

Autumn Semester 2018-19

Instructions:

- The first review of this assigment (all questions in SET 1 and SET 2) will be done in the lab hours on 25^{th} OCtober 2018. The total marks for this exercise are 100, out of which the review would carry 50 marks.
- If you are not able to submit by the specified time, whtsoever may be the reason, without any late policy, the assignment grading will be zero.
- Understand the *nslookup* and *dig* command and their options and play with them before attempting the assignment questions.
- Understand various DNS Name record types as discussed in the class.

Use the "DNS_1.pcapng"for answering the following questions. This capture file was obtained while executing a single nslookup command. Use "dns "filter for seeing dns record.

SET 1: The Basic DNS :

1. Determine which transport layer protocol was used for sending the DNS queries? What are the benefits and drawbacks of using that protocol ?
2. What port numbers are used for sending and receiving the packet in packet #2 ?
3. What is the destination address of packet #2? What type of DNS query it is? What type of DNS server it is? What flags are set in the query ?
4. How many DNS servers are queried to for resolving the domain name du.edu.?
5. Which packet contains the response of the query sent in packet #2 ? Which flags are set in the response ?
6. How many answers do you get in the response? Is the response from authoritative server ?
7. What does the query in the packet #25 do ?
8. Which packet contains the response of the query sent ? What is the response ?

SET 2: Using the DNS_2.pcapng :

Use the "DNS_2.pcapng"file for answering the following question. This capture file is obtained while executing nslookup command twice.

- Packet #1-#9 are obtained while executing "nslookup du.edu. ns1.p24.dynect.net."
- And Packet #10-#15 are obtained while executing "nslookup mit.edu. ns1.p24.dynect.net."

1. In packet #10, what is the destination IP address of the server? To which DNS server request is being sent to?
2. Which packet contains the reply of the query that is sent in packet #10? Did DNS server reply ? Examine the flags of the response and what you infer from the flags?

3. To which DNS server, is the DNS request in #160 sent to? What does the DNS request ask from the DNS server?

4. What is the response from the DNS server in packet #160 ? Did the server resolve the DNS request? Explain in brief.

SET 3: Working with the DNS_3.pcapng :

Use the "DNS_3.pcapng "file for answering the following questions. This capture file is obtained when executing nslookup command. (Local DNS servers and its response)

1. To what IP address, is the DNS query sent in packet #1? What "type"of DNS server is that?

2. To what IP address is the DNS query sent in packet #2? What "type"of DNS server is that?

3. Which packet contains the response of the query that is sent in packet #2? What is your interpretation of the response?

4. What is the difference between query in packet #2 and that in #3 ?

5. What does the query in packet #8 do? Which DNS server is being queried?

6. Which packet contains the response of the query sent in packet #8? What flags are set in this response? Does it have the answer user wants? What information does it provide?

7. Which DNS server is being queried in the query of packet #16 ? Is it a local DNS server ?

8. Which packet contains the response of the query sent in packet #16? What flags are set in this response? Does it have the answer user wants? What information does it provide?

9. What does the query in packet #22 actually do? Which DNS server is being queried?

10. Which packet contains the response to the query sent in packet #22? What flags are set in this response? Does it have the answer user wants? What information does it provide?

SET 4 - Using dig command :

- What is the dig command used to determine the authoritative DNS servers for www.mit.edu?
- Using dig command determine the authoritative DNS servers for www.du.edu and www.ritchieschool.du.edu in a single dig command? Are DNS servers for both different?
- Use dig command with trace option to www.mit.edu (i.e. *dig +trace www.mit.edu*). What you can infer from the output?

*****

***

*