Chapter 4

Lab 3: Analyze the DNS query and response using Wireshark

4.1 Objective

Your experiment will be conducted in four parts. First, you will query for the IP address of the given host name. Second, you will query for the canonical host name of the given host name (it may be the mnemonic host name). Third, you will query for the authoritative DNS servers' host name of the given host name. And finally, you will query for the mail server's canonical host name using the given host name.

4.2 Procedure

1. Windows: Open command prompt and type *ipconfig /all* to determine the local DNS IP address and your host IP address. Ubuntu: In terminal, type *nmcli dev show enp2s0*

2. Windows: To view the DNS records stored in your system, type *ipconfig /displaydns*. And to clear all DNS records, type *ipconfig /flushdns*

3. Open and start Wireshark. Issue commands to query DNS records from command prompt. Save the Wireshark files after the DNS response for packet analysis. Repeat this step for each of the four types of queries.

4. For querying IP address of *ieeexplore.ieee.org*, type *nslookup –type=A ieeexplore.ieee.org* in command prompt.

5. For querying canonical hostname of *ieeexplore.ieee.org*, type *nslookup –type=CNAME www.ieee.org* in command prompt.

6. For querying the names of authoritative DNS servers of *www.pes.edu*, type *nslookup –type=NS www.pes.edu* in command prompt.

7. For querying the mail server alias host names of *mail.google.com*, type *nslookup –type=MX mail.google.com* in command prompt.

4.3 Analyses

1. What was the transport protocol used for DNS queries? Give source and destination port numbers for each query in the experiment.

2. Under the Type A query, what is the length of the DNS query message? (Hint: use UDP length, UDP header size and DNS header size)

3. What is the IP address returned for the Type A query? What was the TTL value? How many answers were returned?

4. What is the canonical name returned for the Type CNAME query? What was the TTL value? What was the additional information observed in the response?
5. What is the authoritative DNS servers' name returned for the Type NS query? What was the TTL value? Was any additional records observed in the response?
6. What is the canonical host name returned for the Type MX query? What was the TTL value? What was the name of the authoritative DNS server observed in the response?
7. Given that the DNS query and response use the same header format, how can you tell the difference between a DNS query and response?
8. Did the client request for recursive query? How can you tell?
9. Did the DNS server support recursive query? How can you tell?
10. What is the throughput under Type NS combining the DNS query and its response?