Ethan Tuning
5/2/2017
CSCD330
Lab#3

1. Run host or nslookup to obtain the IP address of a Web server in Asia.

   Name: china.com
   Addresses: 101.254.216.10
   222.186.130.58
   101.64.239.158

2. Run host or nslookup to determine the authoritative DNS servers for a university in Europe.

   ua.es: primary name server = aitana.cpd.ua.es

3. Run host or nslookup to obtain the the mail servers for Yahoo.com.

   Nslookup -type=mx yahoo.com
   It returned a lot.

4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

   UDP

5. What is the destination port for the DNS query message? What is the source port of DNS response message?

   Both are 53

6. To what IP address is the DNS query message sent?

   10.104.136.86

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

   It is standard query. No answers.

8. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

   There were 2 answers. They contain name of host, type, class, IP, data length, and the TTL.

9. This web page contains images. Before retrieving each image, does the host in the trace file issue new DNS queries?

   No