CS 455: Computer Communications and Networking
Lab - 2: Digging DNS

Grading, submission and late policy:

- You are expected to complete this lab **on your own** (not with a partner)
- This lab accounts for **3%** of your final grade
- The standard late policy applies - Late penalty for this lab will be 15% for each day. Submissions that are late by 3 days or more will not be accepted
- You will submit your solution via Blackboard

DNS tool: Domain Information Groper (dig)

As we discussed in class, the Domain Name System (DNS) translates hostnames to IP addresses. In this assignment, we will take a detailed look at the client-side of DNS. nslookup and dig are two important tools that can help us query DNS servers through the command line. Given the similarities between the two, we will mostly focus on dig in this assignment. dig allows the host running the tool to query any specified DNS server for information about a specified hostname or domain. It can send DNS queries and receive DNS reply. The received reply is displayed on the command line. We will also observe these queries and responses through Wireshark packet capture.

Install dig on your computer:

- dig is installed by default on most Linux/Unix and Mac OS x systems.
- For Windows systems, follow the instructions available at https://help.dyn.com/how-to-use-binds-dig-tool/ to install dig
- Also, use https://techdocs.akamai.com/edge-diagnostics/docs/domain-details-dig to understand the output of the dig command

Running dig and Wireshark

- Open the command line and run the following to know if dig is installed and running.

  $> dig -v
- Open Wireshark and start a packet capture. Since we are only interested in DNS related packets in this assignment, enter "dns" in the display filter on top. This filter will not show any packets other than DNS protocol packets going out or coming into your computer.

Using dig and Wireshark to understand DNS

Section 1: Consider the following command:

$> dig <hostname>

Running this command for any specific hostname provides you its translation (ANSWER SECTION) to IP address and other DNS information. Now start the Wireshark capture with the "DNS" filter on, and run the following command. Stop your Wireshark capture shortly after you see the dig output on the command line.

$> dig cs.gmu.edu

Note that using dig by default uses Extended DNS (EDNS), resulting in an additional optional record (type: OPT) in query and response. You can ignore that record while answering the questions below.

Answer the following questions based on dig output and Wireshark DNS packets.

a. Provide the dig output and a screenshot of the DNS query and response messages from Wireshark.
b. Locate the DNS query and response messages in Wireshark capture. What is the IP address of your local DNS server?
c. Are the DNS query and response messages sent over UDP or TCP? What is the destination port for the DNS query message? What is the source port for the DNS response message?
d. Examine the DNS query message. What "type" of DNS query is it?
e. Examine the DNS response message. How many "answers" are provided (ignore the type OPT records as stated above)? What is the IP address that the hostname resolves to?

Section 2: Consider the following command:

$> dig <hostname/domain name> <record type>

As we learned in class, the record type can be A, NS, MX, or CNAME. Using this command, answer the following questions. As before, make sure to run Wireshark with the "DNS" filter before you run the dig command, and stop the capture shortly after the dig output is displayed.

For each of the questions below, provide the dig output and a screenshot of the DNS query and response messages from Wireshark along with the answer to the question.

a. Let's run the above command to know the DNS servers of Virginia Tech University.

   $> dig vt.edu NS

   List the DNS servers of vt.edu using dig output and DNS response message.
b. Using the same command, find all DNS servers used by gmu.edu domain.
c. Using MX as the type, find out the mail servers for yahoo.com.
d. Using CNAME as the type, find out the canonical name (CNAME) of www.wikipedia.org.

What to submit?

- Submit the answers to the above questions in a document (word or pdf).
- The pcap files for each of the 5 dig runs above. You can name dig1.pcapng to dig5.pcapng.