Lab Exercise 3: Exploring DNS with Wireshark[1]

(Total: 20 points)

OBJECTIVE:

In this lab, we'll use Wireshark to take a close look at Domain Name System (DNS).

BACKGROUND:

Domain Name System (DNS) is discussed in Section 2.4 of the textbook. DNS translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a query to its local DNS server and receives a response back. As shown in Figures 2.19 and 2.20 in the textbook, much can go on "under the covers," invisible to the DNS clients, as the hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

LAB ACTIVITIES:

1. `ipconfig` (for Windows) and `ifconfig` (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we'll only describe `ipconfig`, although the Linux/Unix `ifconfig` is very similar (for example, `ifconfig -a, ifconfig en0).` `ipconfig` can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, if you all this information about your host simply by entering the following command into the Command Prompt:

   ```
   ipconfig /all
   ```

   `ipconfig` is also very useful for managing the DNS information stored in your host. We learned that a host can cache DNS records it recently obtained. To see these cached records, after the prompt C:\> provide the following command:

   ```
   ipconfig /displaydns
   ```

   Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter

   ```
   ipconfig /flushdns
   ```

   Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

2. In this lab, we'll make extensive use of the `nslookup` tool, which is available in most Linux/Unix and Microsoft platforms today. In it is most basic operation, `nslookup` tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or a local DNS server. To

[1] The lab materials are adapted from the textbooks "Computer Networking – A Top-Down Approach" by James Kurose and Keith Ross and the materials provided with them. They can only be used by students who registered for this course. Reproduction outside of this course use is prohibited.

accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

The general syntax of nslookup commands is:

```
nslookup -option1 -option2 host-to-find dns-server
```

In general, nslookup can be run with zero, one, two or more options. The dns-server is optional as well; if it is not supplied, the query is sent to the default DNS server.

Note that nslookup on Windows may automatically append the local domain suffix to the searched hostname. To prevent that, end the hostname by a period (representing the root domain), for example, using "www.cs.unb.ca." instead of "www.cs.unb.ca".

Run the following commands:

```
nslookup www.cs.unb.ca.

nslookup -type=NS unb.ca.

nslookup www.cs.unb.ca. ns1.dal.ca
```

a. The first command sends the query to the default DNS server to get the IP address for the host "www.cs.unb.ca.".

b. The second command has the option "-type=NS" and the domain "unb.ca.". It sends a query for a type-NS record to the default DNS server. In words, the query is saying, "please send me the host names of the authoritative DNS for unb.ca.". (When the -type option is not used, nslookup uses the default, which is to query for type A records.)
The answer with "non-authoritative" means that this answer came from the cache of some server rather than from an authoritative DNS server for the searched domain. Finally, the answer may also include the IP addresses of the authoritative DNS servers. Even though the type-NS query generated by nslookup did not explicitly ask for the IP addresses, the DNS server may return these "for free" and nslookup displays the result.

c. The third command sends the query to the DNS server ns1.dal.ca rather than to the default DNS server. Thus, the query and reply transaction takes place directly between the querying host and the designated DNS server. In this example, a DNS query is first sent to resolve the hostname of the designated DNS server (ns1.dal.ca) to get its IP address, and then a second DNS query is sent to the obtained IP address to find out the IP address of the searched host (www.cs.unb.ca.).

3. Now that we are familiar with nslookup and ipconfig, we're ready to get down to some serious business. Let's first capture the DNS packets that are generated by ordinary Web-surfing activity.

First, use ipconfig to empty the DNS cache in your host. Open your browser and empty your browser cache. Start packet capture in Wireshark. Open your browser and visit the Web page: https://www.cloudflare.com/. Stop packet capture. Then, enter "ip.addr == your_IP_address and dns" into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.

Based on your above capture, answer the following questions:

a. Locate the DNS query and response messages specifically for the hostname "www.cloudflare.com". What is their Transaction ID?

   b. Are these two 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 of the DNS response message?

   c. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? To what IP address is the DNS query message sent? Use `ipconfig` to determine the IP address of your default DNS server. Are these two IP addresses the same?

   d. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

4. Now run the following command and repeat the above experiment and answer the following questions:

   ```
   nslookup id415m01.cs.unb.ca. dns.google
   ```

   Note that this command uses Google Public DNS[2], which provides free DNS resolution.

   a. Locate the DNS query and response messages specifically to resolve the DNS server with hostname "`dns.google`"? What IP address(es) does the response show?

   b. Locate the DNS query and response messages specifically to resolve the hostname "`id415m01.cs.unb.ca.`". To what destination IP address is the DNS query message sent? Is this the IP address of one of your default DNS servers that were obtained above from `ipconfig /all`?

   c. Examine the DNS response message to resolve the hostname "`id415m01.cs.unb.ca.`", what is the IP address of the hostname being resolved? How long is the valid period of the resource record?

5. Now run the following command and repeat the above experiment and answer the following questions:

   ```
   nslookup -type=NS ubc.ca.
   ```

   a. Locate the DNS query and response messages specifically to resolve the domain name "`ubc.ca`". To what IP address is the DNS query message sent? Is this the IP address of one of your default DNS servers?

   b. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

   c. Examine the DNS response message. What DNS name servers does the response message provide? Does this response message also provide the IP addresses of these name servers?

LAB REPORT:

Go through the above lab activities and **write a report answering the questions listed items 3-5.**

- **Please follow the lab report template in Microsoft Word posted on D2L.** Once you are done, convert your Word document into **a single PDF file** and submit it to the corresponding dropbox on D2L by the due time.
- In your report, attach a screenshot of the packet trace to indicate where you find the answer to each question. You can capture the display in Wireshark using screen capture software and then annotate the output packet trace with color markups to show the information related to your answers.

[2] Google Public DNS: https://developers.google.com/speed/public-dns/.