Due Nov 5th before noon on Gradescope

Tracing DNS with Wireshark

The Domain Name System (DNS) translates hostnames to IP addresses. As discussed in class, 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. We examine these interactions from the client’s perspective in these exercises.

Your computer will probably have a local cache of DNS records. This is good since it means that you need not dial directory information as often as you otherwise might. However, it is not so good for the following exercises since we will not be able to see DNS in action. Before we can trace DNS interactions we will need to clear this cache.

Now, follow these steps:

1. Fire up Wireshark and enter: `ip.addr=your_ip_address` into the filter, where `your_ip_address` is your IP address.
   - On the MAC you can find your IP address by selecting Network under System Preferences ... in the apple menu.
   - Alternatively, you can use either `ifconfig` (MAC) or `ipconfig` (Windows), or just Google your IP.
2. Open your browser and clear the cache.
3. Finally, open a terminal window and clear your local DNS cache.
4. Start the Wireshark capture and type `http://www.ietf.org` into your browser.
5. Stop the packet capture.¹

Problem 1.

a) Locate the DNS query and response messages. Are they sent over UDP or TCP?
b) What is the destination port for the DNS query message? What is the source port of the DNS response message?
c) To what IP address is the DNS query message sent? Use `ipconfig` to determine the IP address of your local DNS server. Are these two IP addresses the same?
d) Examine the DNS query message. What Type of DNS query is it? Does the query message contain any answers?
e) Examine the DNS response message. How many answers are provided? What do each of these answers contain?
f) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
g) This web page contains images. Before retrieving each image, does your host issue new DNS queries?

¹If you cannot clear your cache, you still have one shot at this. But it will only work the first time.
Problem 2.

Restart Wireshark capture and enter the following command: `nslookup -type=MX mit.edu`. Answer the following questions:

a) To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

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 MIT nameservers does the response message provide? Does this response message also provide IP addresses of MIT nameservers?

Tracing UDP with Wireshark

In these exercises we take a quick look at the UDP, a streamlined, no-frills transport-layer protocol. Since you are by now a Wireshark expert this handout does not spell out the steps quite as explicitly as in earlier exercises.

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. It’s also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace. In particular, the Simple Network Management Protocol (SNMP - chapter 9 in the text) sends SNMP messages inside of UDP, so it’s likely that you’ll find some SNMP messages (and therefore UDP packets) in your trace.²

After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer.

Problem 3.

a) Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn’t look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

b) By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

c) What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

d) What is the largest possible source port number? (Hint: see the hint in 3.)

e) What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you’ll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

f) Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: For a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

²If you saved your Wireshark sessions previous exercises, now would be a good time to haul it out.