LAB ASSIGNMENT WEEK # 1

DN Exercise # 1 Tracing DNS with Wireshark

1. DNS

The Domain Name System (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.

Some Important Commands: *nslookup*.

Exercise # 1 Tracing DNS with Wireshark

Answer the following questions using *dns-ethereal-trace-1* file:

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
3. 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?
4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
5. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
6. 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?
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Answer the following questions using *dns-ethereal-trace-2* file:

8. What is the destination port for the DNS query message? What is the source port of DNS response message?
9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
10. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
11. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
12. Provide a screenshot.

Answer the following questions using *dns-ethereal-trace-3* file:

13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
14. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

15. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
16. Provide a screenshot.

Answer the following questions using *dns-ethereal-trace-4* file:

17. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
18. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
19. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
20. Provide a screenshot.

2. UDP

Exercise # 2 Tracing UDP with Wireshark

Answer the following questions using *udp-wireshark-trace* file:

1. 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.
2. 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.
3. 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.
4. 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)
5. What is the largest possible source port number? (Hint: see the hint in 4.)
6. 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).
7. 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.