Chapter 2

Lab 1: Introduction to Wireshark: Packet capture procedure, Filters, Analysis

2.1 Objective

To explore aspects such as packet capture procedure, filters and analysis that can be done using Wireshark. We will analyze delay and throughput when the packets are transmitted by the hosts. In this regard, we will invoke the ping and tracert commands.

2.2 Procedure

Do the following:

1. Start up the Wireshark packet sniffer, as described in the Preliminary chapter (but don't yet begin packet capture).
2. Wait a bit more than one minute, and then begin Wireshark packet capture.
3. Open the terminal window and perform the following steps
    a. Type the command "ipconfig /all" (without the quotation marks) and IPv4 address (that is the IP address assigned to the Ethernet interface of your PC).
    b. Type "ping 8.8.8.8" (this is Google's DNS server; more on DNS later)
    c. Type "tracert 8.8.8.8" (this performs several ping operations with different TTL values till the destination 8.8.8.8 is reached)
4. Stop Wireshark and type "icmp" (without the quotation marks) into the display filter and press the enter key
5. You should find the ICMP packets Echo (ping) request and Echo (ping) reply. The former packet is sent from your terminal while the later packet is received by your terminal.
6. Now analyze the throughput and delay during your experiment.

2.3 Analyses

1. How many Echo (ping) request and Echo (ping) reply packets were observed?
2. What were the sizes of Echo (ping) request and Echo (ping) reply packets?
3. Inspect the Echo (ping) reply and find out the response time (aka round trip time).
4. What is the type and code observed in the Echo (ping) request and Echo (ping) reply packets?

5. When you performed the “tracert 8.8.8.8” command, how many intermediate nodes identified TTL expiry? Write their IP addresses. What response did they send in when they observed TTL expiry? Specify the type and code in the responses.

6. Calculate the throughput experienced by your computer across all the ICMP packets. To calculate throughput you must add all the packet lengths and divide the sum by the difference of the time of receiving the last Echo (ping) reply and the time of sending the first Echo (ping) request.

Provide screenshots of the packet-listing window displaying the ICMP packets. Try the command “ip.src == 8.8.8.8” or “ip.addr == 8.8.8.8” in the display filter to know the packets sent from the IP address 8.8.8.8