Wireshark Lab: UDP

In this lab, we will be looking at the UDP transport protocol. We have discussed in our lecture that UDP is a streamlined, no-frills, and extension of the IP protocol. Because UDP is simple, you are expected to finish this lab activity early.

At this time, you should already be a Wireshark expert. Thus, the different steps are not going to be discussed in detail. By now, you already know how to answer the different problems and what supporting details to provide for your answers.

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 race (e.g. SNMP messages).

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.

Answer the following questions:

1. Select one UDP packet from your trace. From this packet, determine how many fields are there in the UDP header. 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 of the Length field is the length of what? Verify your claim with your captured UDP packet.
4. 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.
5. 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. Describe the relationship between the port numbers in the two packets.