Wireshark Lab: UDP

In this lab, we'll take a quick look at the UDP transport protocol. Because UDP is simple and sweet, we'll be able to cover it pretty quickly in this lab.

The Assignment

Whenever possible, when answering a question below, you should hand in a screen print of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer.

For this lab use the Wireshark trace – udp-trace.pcap

1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are 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 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

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.