CSCI 466 Lab 3 – UDP

Due Wednesday November 1st

In this lab, we'll take a quick look at the UDP transport protocol. As we saw in class, UDP is a streamlined, no-frills protocol. Because UDP is simple and sweet, this Wireshark lab is going to be short and easy.

Getting started

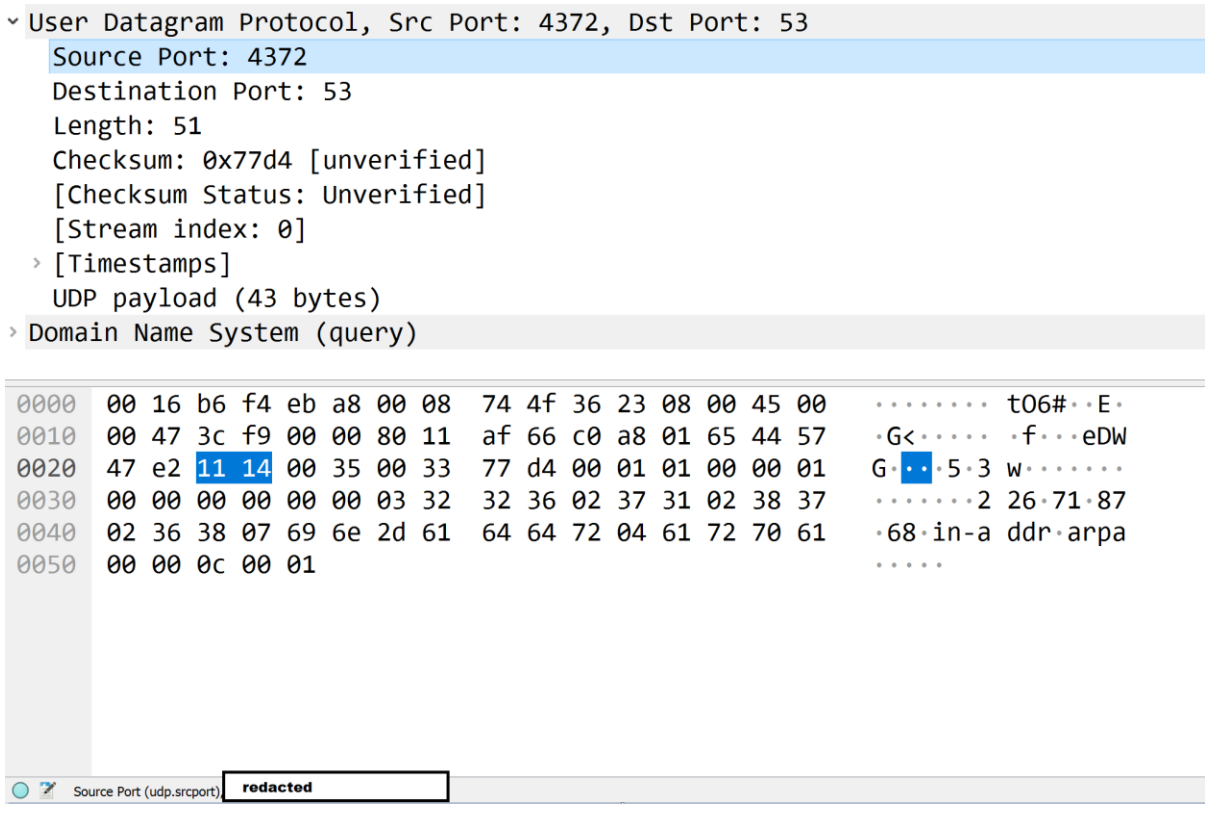
Inside the zip file you downloaded for lab 2, there is a Wireshark trace of UDP data (**`udp-wireshark-race`**). This is the trace you will be analyzing for the lab, so you will need to open this file in Wireshark for analysis.

This trace consists of several DNS queries, which uses UDP as the underlying transport layer protocol. To view UDP information, you will need to click on a DNS packet, and then expand the "User Datagram Protocol" tab.

The Assignment

Please answer the following questions regarding the trace:

1. Select one packet DNS/UDP packet and take a screenshot of the UDP information.
2. How many fields are there in the UDP header?
3. By consulting the displayed information in the Wireshark's "packet content" pane, determine the length (in bytes) for each of the UDP header fields. To do this, click on one of the header fields, and the length of that field should be displayed at the bottom of Wireshark



4. The value in the Length field is the length of what? *Hint:* Look at the “UDP Payload” value in Wireshark
5. What is the maximum number of bytes that can be included in a UDP payload? *Hint:* look at how many bits are allocated for the “length” field.
6. What is the largest possible source port number?
7. 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.
8. 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.