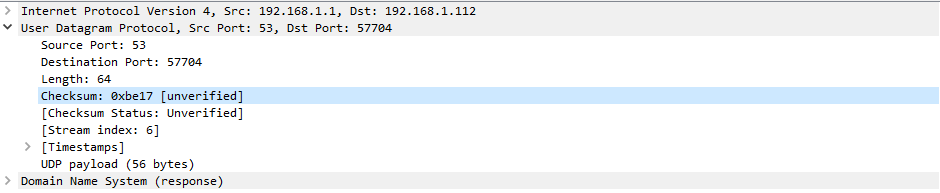
# Lab 3: Wireshark – UDP

Ian Kaiserman

1. Select one packet. From this packet, determine how many fields there are in the UDP header. (Do not look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields. Best would be to have an example from the data retrieved via Wireshark.

**There are four fields:**

1. **Source port**
2. **Destination port**
3. **Length**
4. **Checksum**

****

1. From the packet content field, determine the length (in bytes) of each of the UDP header fields. What is that length?
   1. **2 bytes**





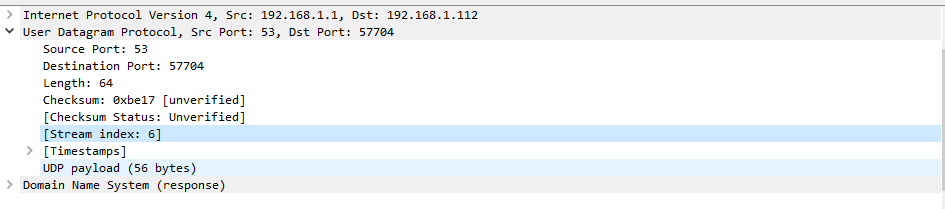




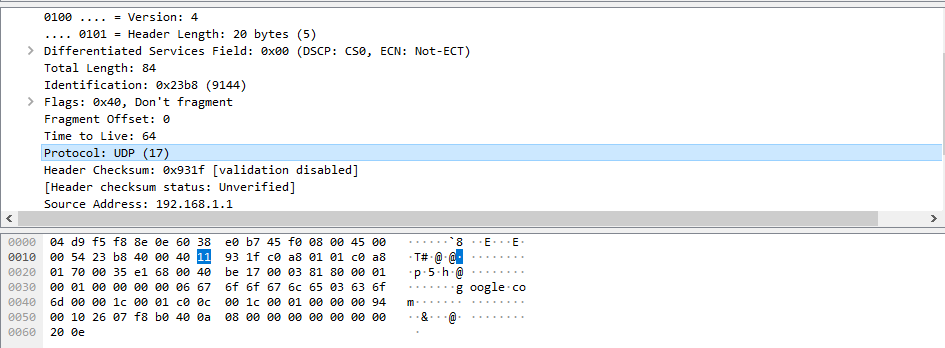
**Also shown in hexadecimal data**

****

1. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.
   1. **The value of the Length field is the sum of the headers (8, shown above) plus the UDP payload (56 in this case)**



1. What is the maximum number of bytes that can be included in a UDP payload?
   1. **Max number of bytes is 65535 (2^16 – 1) – 8 (length of headers) = 65527**
2. What is the largest possible source port number?
   1. **65535 (2^16 – 1)**
3. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. (To answer this question, you will need to look into the IP header.)
   1. **Hexadecimal: 0x11**
   2. **Decimal: 17**



1. Search “UDP” in Google and determine the fields over which the UDP checksum is calculated. What are those fields?
   1. **Three fields are used:**
      1. **IP header**
      2. **UDP header**
      3. **“data” aka UDP payload**

**(pseudo-header)**

1. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets. Again, good to illustrate with lines from the Wireshark tool to back up your answer.
   1. **The source and destination ports trade spots in the response compared to the initial query.**



