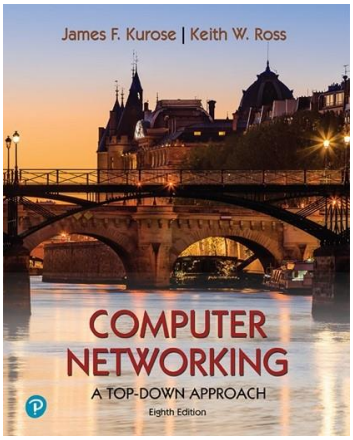
Wireshark Lab: UDP v8.0

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



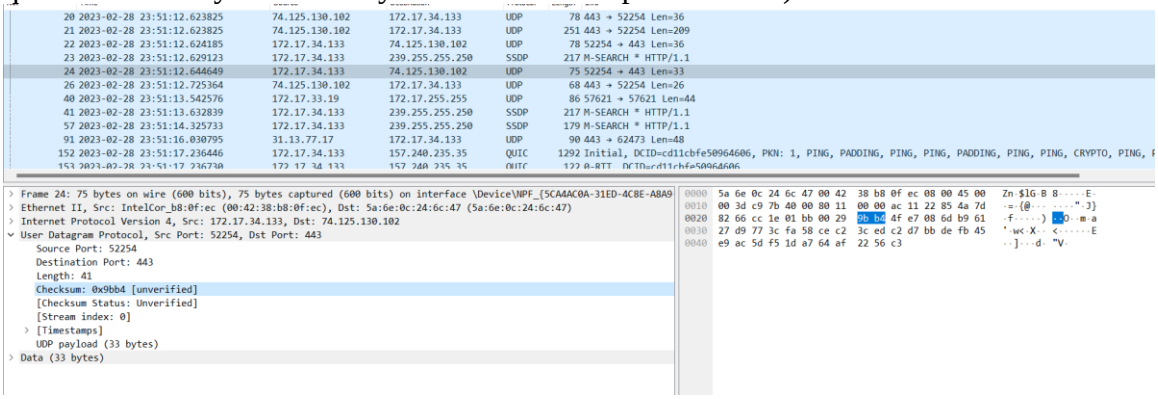
Student Name :Nguyễn Hữu Hiếu

Student ID : 2013149

In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3 of the text[1], UDP is a streamlined, no-frills protocol. You may want to re-read section 3.3 in the text before doing this lab. Because UDP is simple and sweet, we'll be able to cover it pretty quickly in this lab. So if you've another appointment to run off to in 30 minutes, no need to worry, as you should be able to finish this lab with ample time to spare.

At this stage, you should be a Wireshark expert. Thus, we are not going to spell out the steps as explicitly as in earlier labs. In particular, we are not going to provide example screenshots for all the steps.

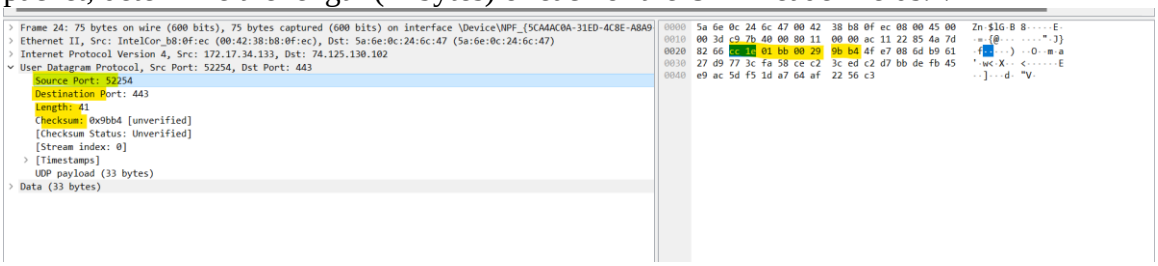
1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.



The header only contains 4 fields: the source port, destination port, length, and checksum

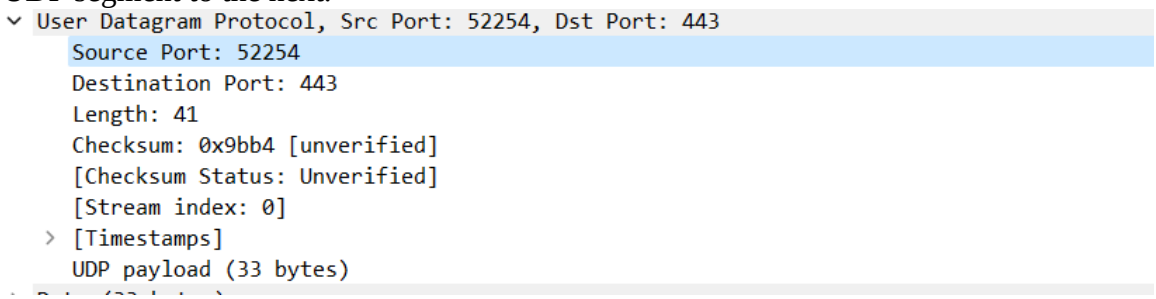
[1] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.*

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. \



The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.

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.
The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.



The length of UDP payload for selected packet is 33 bytes. 41 bytes - 8 bytes = 32 bytes

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)

The maximum number of bytes that can be in the payload is 2^16- the bytes already being used by the header field (8).
Therefore the maximum payload is 65535-8= 65527 bytes

5. What is the largest possible source port number? (Hint: see the hint in 4.)

The largest possible source port number is (2^16 – 1) = 65535.

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 (see Figure 4.13 in the text, and the discussion of IP header fields).

```
> Frame 24: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Dev
> Ethernet II, Src: IntelCor_b8:0f:ec (00:42:38:b8:0f:ec), Dst: 5a:6e:0c:24:6c:47 (5a:6
v Internet Protocol Version 4, Src: 172.17.34.133, Dst: 74.125.130.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0xc97b (51579)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.17.34.133
    Destination Address: 74.125.130.102
v User Datagram Protocol, Src Port: 52254, Dst Port: 443
```

The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

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.

```
v User Datagram Protocol, Src Port: 443, Dst Port: 52254
    Source Port: 443
    Destination Port: 52254
    Length: 34
    Checksum: 0xa215 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (26 bytes)
```

```
v User Datagram Protocol, Src Port: 52254, Dst Port: 443
    Source Port: 52254
    Destination Port: 443
    Length: 41
    Checksum: 0x9bb4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (33 bytes)
```

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.