ENGR 3321 - Lab 4: Wireshark UDP

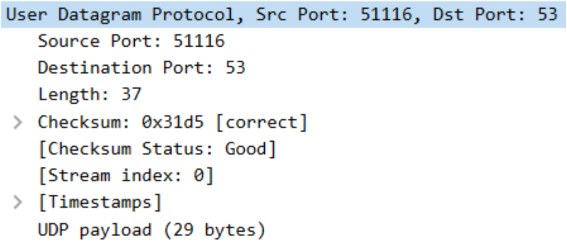
14 October 2022

Nathan Cauwet

873271826

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.*

There are 4 fields: source, destination, length, and checksum



```
User Datagram Protocol, Src Port: 51116, Dst Port: 53
    Source Port: 51116
    Destination Port: 53
    Length: 37
  > Checksum: 0x31d5 [correct]
    [Checksum Status: Good]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (29 bytes)
```

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.*

payload = 29 bytes, Length = 37, total length of IPv4 = 57, IPv4 header = 20

ipv4 length – ipv4 header length = 57-20 = 37 = Length

Length - payload = 8 bytes = UDP header size

If you click on User Datagram Protocol, it says the header is 8 bytes (verifying total UDP header size that I calculated above).

Since there are 4 header fields and the total header size is 8 bytes, **each header is 2 bytes**.

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.

Value in length field = 37 = the IPv4 packet (total size minus the header)

ipv4 packet = ipv4 length – ipv4 header length = 57-20 = 37 = Length

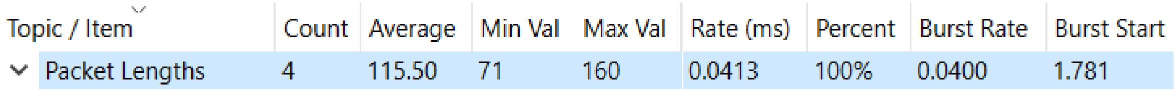
It is the length of the IPv4 packet

UDP payload + UDP header = 29 + 8 = 37 bytes = UDP packet length

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 length of a UDP packet is $(2^{16} - 1)$ bytes (including the 8 header bytes), therefore maximum number of bytes allowed in a UDP payload is $(2^{16} - 1)$bytes – 8bytes = **65527 bytes**



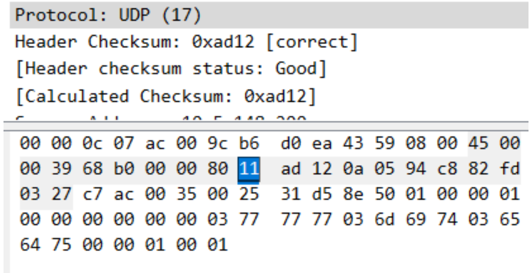
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	4	115.50	71	160	0.0413	100%	0.0400	1.781

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).*

UDP protocol number is 17 in decimal and 0x11 in hexadecimal

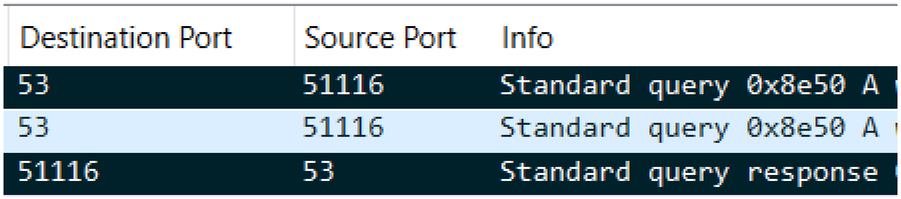


```
Protocol: UDP (17)
Header Checksum: 0xad12 [correct]
[Header checksum status: Good]
[Calculated Checksum: 0xad12]
```

```
00 00 0c 07 ac 00 9c b6  d0 ea 43 59 08 00 45 00
00 39 68 b0 00 00 80 11  ad 12 0a 05 94 c8 82 fd
03 27 c7 ac 00 35 00 25  31 d5 8e 50 01 00 00 01
00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65
64 75 00 00 01 00 01
```

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.*

The port numbers in the two packets are the same with the source and destination switched (src1 = dest2 and src2 = dest1).



Destination Port	Source Port	Info
53	51116	Standard query 0x8e50 A
53	51116	Standard query 0x8e50 A
51116	53	Standard query response

The expanded details from the selected packet are included below: