

## 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.

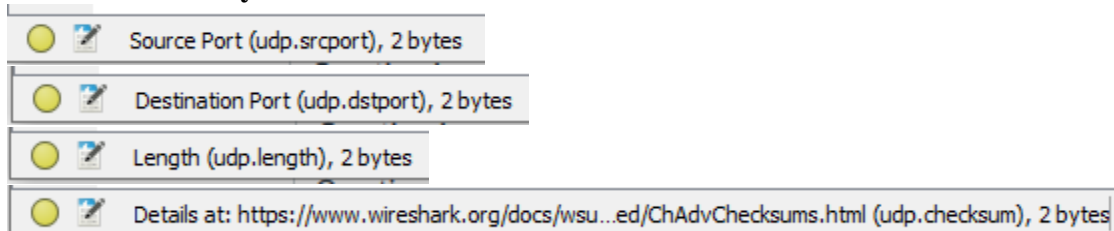
**There are four fields:**

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

```
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.112
▼ User Datagram Protocol, Src Port: 53, Dst Port: 57704
  Source Port: 53
  Destination Port: 57704
  Length: 64
  Checksum: 0xbe17 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 6]
  > [Timestamps]
  UDP payload (56 bytes)
> Domain Name System (response)
```

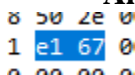
2. From the packet content field, determine the length (in bytes) of each of the UDP header fields. What is that length?

a **2 bytes**



The screenshot shows the 'Packet Details' pane in Wireshark. It lists four UDP header fields, each with a yellow circle icon and a pencil icon, indicating they can be edited. The fields are: 'Source Port (udp.srcport), 2 bytes', 'Destination Port (udp.dstport), 2 bytes', 'Length (udp.length), 2 bytes', and 'Details at: https://www.wireshark.org/docs/wsuo...ed/ChAdvChecksums.html (udp.checksum), 2 bytes'.

**Also shown in hexadecimal data**



The screenshot shows the 'Packet Bytes' pane in Wireshark. It displays the first two bytes of the packet in hexadecimal: 'e1 67'. The first byte 'e1' is highlighted in blue.

3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

a **The value of the Length field is the sum of the headers (8, shown above) plus the UDP payload (56 in this case)**

```
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.112
▼ User Datagram Protocol, Src Port: 53, Dst Port: 57704
  Source Port: 53
  Destination Port: 57704
  Length: 64
  Checksum: 0xbe17 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 6]
  > [Timestamps]
  UDP payload (56 bytes)
> Domain Name System (response)
```

4. What is the maximum number of bytes that can be included in a UDP payload?  
a **Max number of bytes is 65535 ( $2^{16} - 1$ ) - 8 (length of headers) = 65527**
5. What is the largest possible source port number?

a **65535 ( $2^{16} - 1$ )**

6. 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.)

a **Hexadecimal: 0x11**

b **Decimal: 17**

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x23b8 (9144)
> Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x931f [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1

0000  04 d9 f5 f8 8e 0e 60 38 e0 b7 45 f0 08 00 45 00  ....8...E...
0010  00 54 23 b8 40 00 40 11 93 1f c0 a8 01 01 c0 a8  -T#@@...
0020  01 70 00 35 e1 68 00 40 be 17 00 03 81 80 00 01  -p5h:
0030  00 01 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f  ....g oogle.co
0040  6d 00 00 1c 00 01 c0 0c 00 1c 00 01 00 00 00 94  m.....
0050  00 10 26 07 f8 b0 40 0a 08 00 00 00 00 00 00 00  --&...@...
0060  20 0e
```

7. Search “UDP” in Google and determine the fields over which the UDP checksum is calculated. What are those fields?

a **Three fields are used:**

i **IP header**

ii **UDP header**

iii **“data” aka UDP payload**

(pseudo-header)

8. 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.

a **The source and destination ports trade spots in the response compared to the initial query.**

```
▼ User Datagram Protocol, Src Port: 57703, Dst Port: 53
  Source Port: 57703
  Destination Port: 53

▼ User Datagram Protocol, Src Port: 53, Dst Port: 57703
  Source Port: 53
  Destination Port: 57703
```