

COMPUTER NETWORK

<Wireshark UDP Analysis Project>

ITM 19102127
Suho Lee

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.

```
> Frame 1891: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{46C...}
> Ethernet II, Src: ArubaaHe_8a:a7:00 (88:3a:30:8a:a7:00), Dst: IntelCor_dd:e2:0d (2c:0d:a7:dd:e2:0d)
> Internet Protocol Version 4, Src: 142.251.220.14, Dst: 10.50.47.36
▼ User Datagram Protocol, Src Port: 443, Dst Port: 56066
    Source Port: 443
    Destination Port: 56066
    Length: 1258
    Checksum: 0x1bb1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 48]
> [Timestamps]
    UDP payload (1250 bytes)
> Data (1250 bytes)
```

: There are 4 fields in UDP header.

: 'Source Port', 'Destination Port', 'Length', and 'Checksum'

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.

> Frame 3003: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface \Device\NPF_{46CCBC6...}	0010 01 28 77 95 00 00 3d 11 af e2 cb f6 50 01 0a 32 (w... ..P...2
> Ethernet II, Src: ArubaHe_8a:a7:00 (88:3a:30:8a:a7:00), Dst: IntelCor_dd:e2:0d (2c:0d:a7:dd:e2:0d)	0020 2f 24 00 35 eb 9d 01 14 6b 54 60 b7 81 80 00 01 /\$-5-... kt'...
> Internet Protocol Version 4, Src: 203.246.80.1, Dst: 10.50.47.36	0030 00 01 00 04 00 07 03 77 77 77 06 67 6f 6f 67 6c ...w ww-googl
> User Datagram Protocol, Src Port: 53, Dst Port: 60317	0040 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 e-com... ..
Source Port: 53	0050 00 00 09 5e 00 04 8e fb 2a a4 c0 10 00 02 00 01 ...n s4...
Destination Port: 60317	0060 00 00 01 1b 00 06 03 6e 73 34 c0 10 c0 10 00 02 ...ns2...
Length: 276	0070 00 01 00 00 01 1b 00 06 03 6e 73 32 c0 10 c0 10 ...ns1...
Checksum: 0x6b54 [unverified]	0080 00 02 00 01 00 00 01 1b 00 06 03 6e 73 31 c0 10 ...ns3...
[Checksum Status: Unverified]	0090 c0 10 00 02 00 01 00 00 01 1b 00 06 03 6e 73 33 ...g...
[Stream index: 73]	00a0 c0 10 c0 60 00 01 00 01 00 00 08 67 00 04 d8 ef ...N...
> [Timestamps]	00b0 20 0a c0 4e 00 01 00 01 00 00 08 8f 00 04 d8 ef ...p...
UDP payload (268 bytes)	00c0 22 0a c0 72 00 01 00 01 00 00 08 8f 00 04 d8 ef ...<...
> Frame 3003: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface \Device\NPF_{46CCBC6...}	00d0 24 0a c0 3c 00 01 00 01 00 00 0a 10 00 04 d8 ef ...<...
> Ethernet II, Src: ArubaHe_8a:a7:00 (88:3a:30:8a:a7:00), Dst: IntelCor_dd:e2:0d (2c:0d:a7:dd:e2:0d)	00e0 26 0a c0 60 00 1c 00 01 00 00 07 6d 00 10 20 01 ...m...
> Internet Protocol Version 4, Src: 203.246.80.1, Dst: 10.50.47.36	00f0 48 60 48 02 00 32 00 00 00 00 00 00 0a c0 72 ...H...2...
> User Datagram Protocol, Src Port: 53, Dst Port: 60317	
Source Port: 53	
Destination Port: 60317	
Length: 276	
Checksum: 0x6b54 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 73]	
> [Timestamps]	
UDP payload (268 bytes)	
> Domain Name System (response)	

Source Port: 2 bytes

Destination Port: 2 bytes

Length: 2 bytes

Checksum: 2 bytes

Total: 8bytes

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.

```
▼ User Datagram Protocol, Src Port: 53, Dst Port: 60317
  Source Port: 53
  Destination Port: 60317
  Length: 276
  Checksum: 0x6b54 [unverified]
  [Checksum Status: Unverified]
```

⇒ 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 $276 \text{ bytes} - 8 \text{ bytes} = 268 \text{ bytes}$

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 $(2^{16}-1)$ the bytes already being used by the header field. Therefore, $2^{16}-8 = 65,527$ 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).

```
√ Internet Protocol Version 4, Src: 203.246.80.1, Dst: 10.50.47.36
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 538
    Identification: 0x6a7d (27261)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 61
    Protocol: UDP (17)
    Header Checksum: 0xbc08 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 203.246.80.1
    Destination Address: 10.50.47.36
```

⇒ 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.

```
> Frame 1019: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{46CCBC61-4
> Ethernet II, Src: IntelCor_dd:e2:0d (2c:0d:a7:dd:e2:0d), Dst: ArubaaHe_8a:a7:00 (88:3a:30:8a:a7:00)
> Internet Protocol Version 4, Src: 10.50.47.36, Dst: 203.246.80.1
v User Datagram Protocol, Src Port: 59781, Dst Port: 53
    Source Port: 59781
    Destination Port: 53
    Length: 72
    Checksum: 0x55a7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 64]
    > [Timestamps]
        UDP payload (64 bytes)
> Domain Name System (query)

> Frame 1021: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{46CCBC61-4
> Ethernet II, Src: ArubaaHe_8a:a7:00 (88:3a:30:8a:a7:00), Dst: IntelCor_dd:e2:0d (2c:0d:a7:dd:e2:0d)
> Internet Protocol Version 4, Src: 203.246.80.1, Dst: 10.50.47.36
v User Datagram Protocol, Src Port: 53, Dst Port: 59781
    Source Port: 53
    Destination Port: 59781
    Length: 518
    Checksum: 0x48a5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 64]
    > [Timestamps]
        UDP payload (510 bytes)
> Domain Name System (response)
```

⇒ First Picture shows that the 'Source Port: 59781' and 'Destination Port: 53'

Compare to the first Result, Second Picture shows the 'Source Port: 53' and 'Destination Port: 59781'

You can easily notify the src port and dst port are reversed.