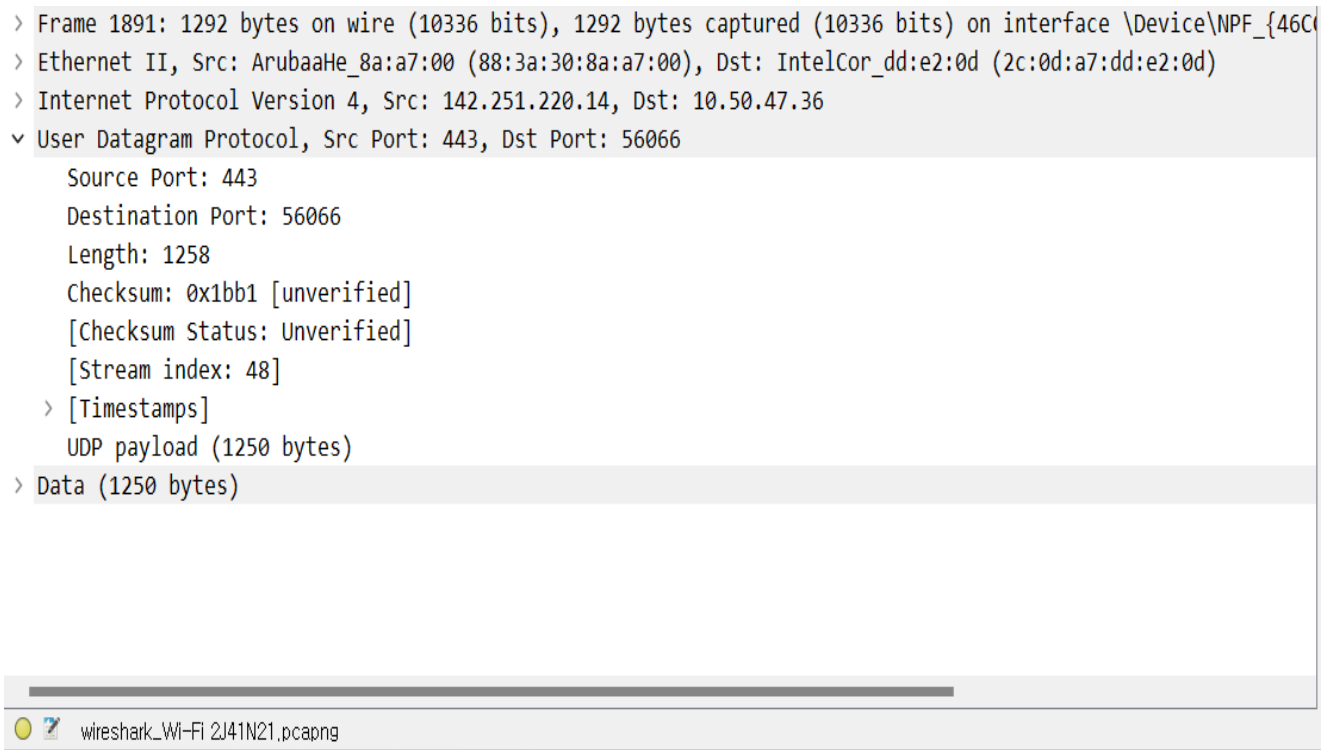
# COMPUTER NETWORK
# <Wireshark UDP Analysis Project>

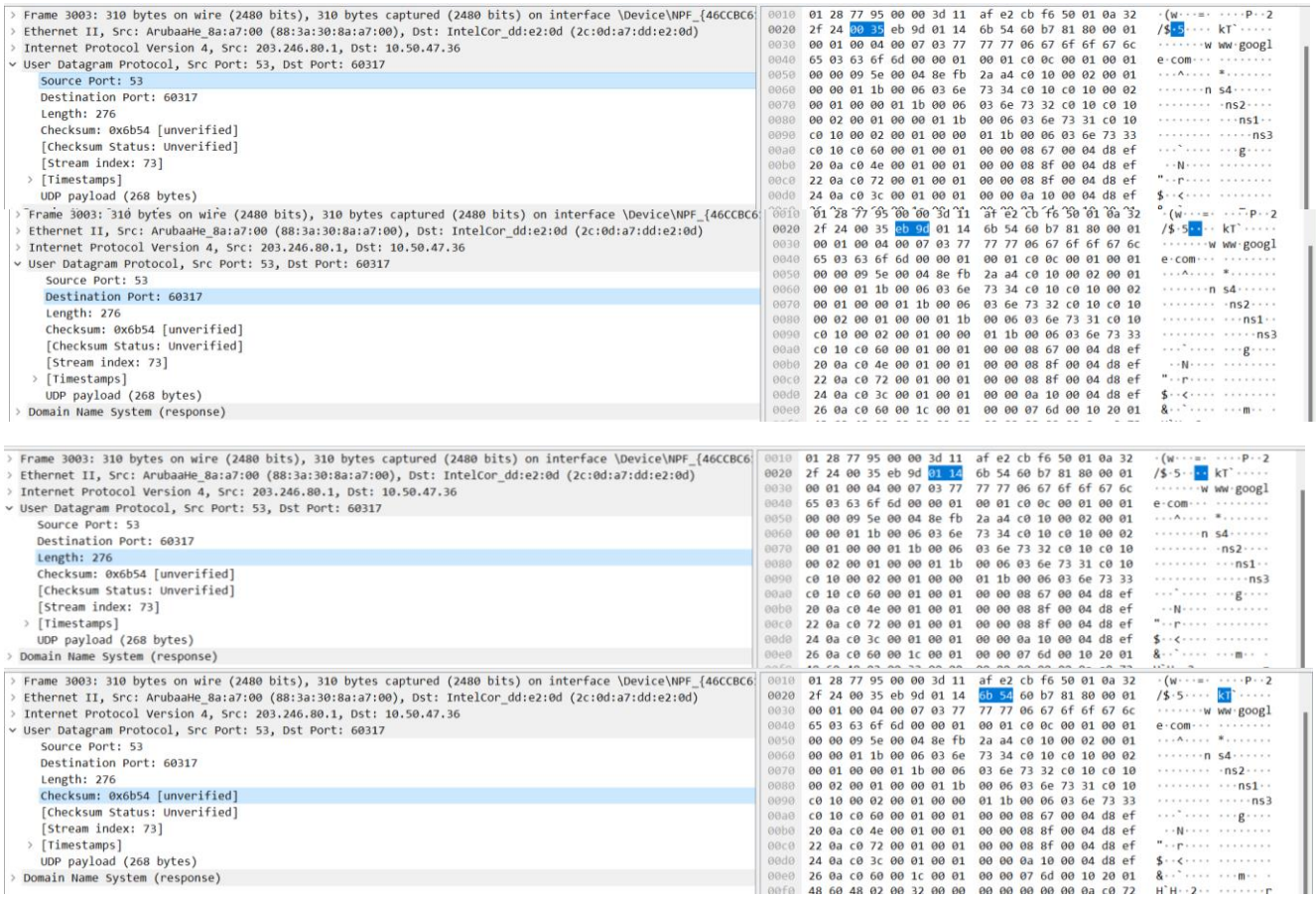
**ITM 19102127**
**Suho Lee**

## 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.




: 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.




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.


⇨ 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 bytes – 8bytes = 268 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.)

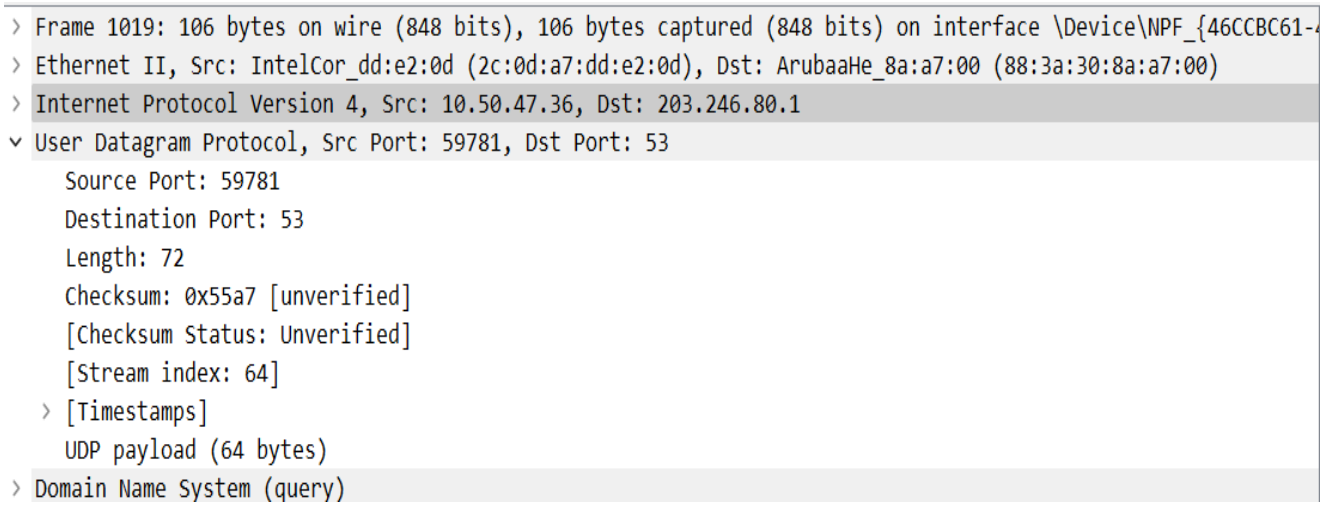
⇨ The largest possible source port number is (2^16-1) = 65535.

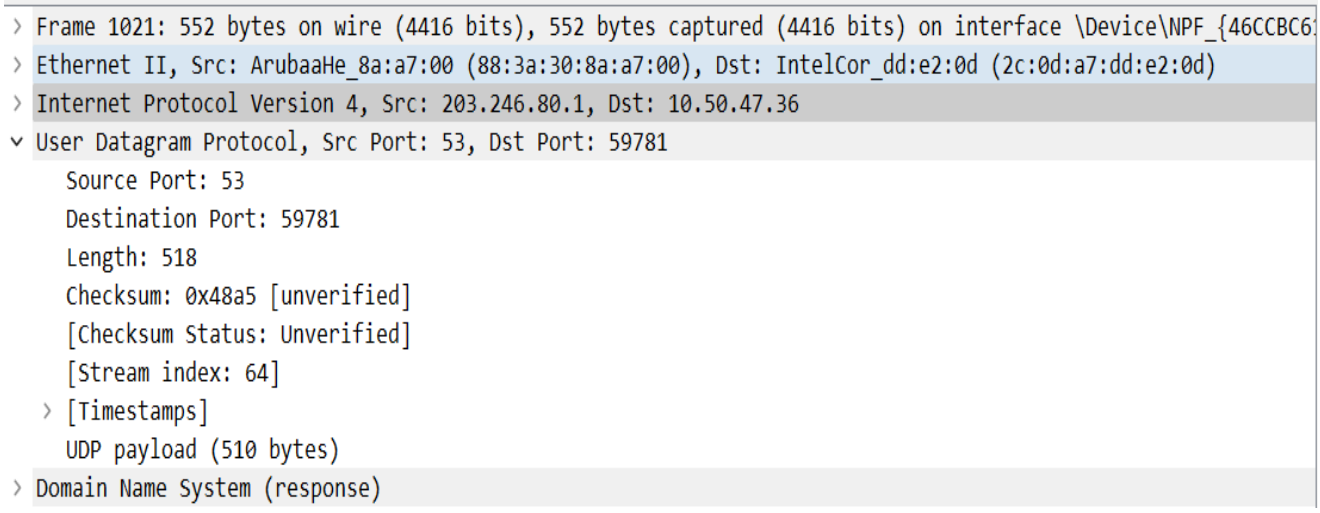
**6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).**

```
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.**




⇨ 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.