UDP

네트워크프로그래밍

휴먼지능정보공학과
201810776 소재휘

Lab03: UDP on Wireshark

Instructions

•Start capturing packets in Wireshark.

•Stop capturing packets.

Questions

1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.

2.Find out the length (in bytes) of each of the UDP header fields.

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

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)

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

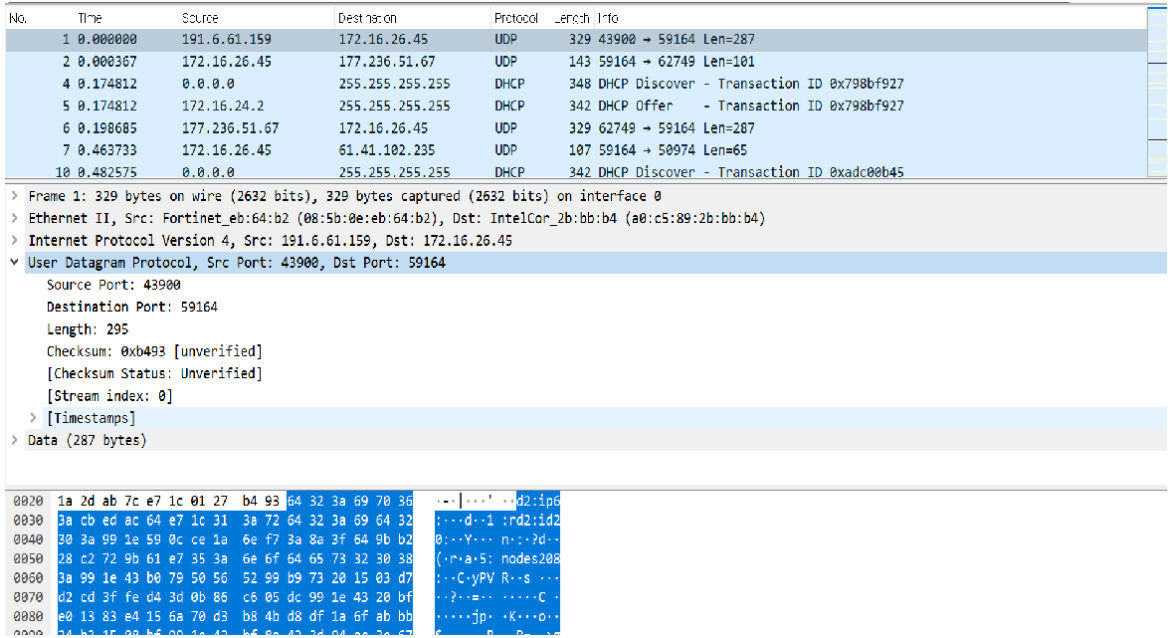
6.What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP packet containing this UDP segment.

7.Examine a pair of UDP packets. (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.

#1 UDP On Wireshark

Network programming

1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.
2.Find out the length (in bytes) of each of the UDP header fields.



UDP 패킷 중 하나를 선택하였다.

#1 UDP On Wireshark

Network programming

1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.
2.Find out the length (in bytes) of each of the UDP header fields.

```
Ethernet II, Src: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2), Dst: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4)
> Destination: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4)
> Source: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
  Type: IPv4 (0x0800)
```

Physical layer, Network layer : Ethernet II

#1 UDP On Wireshark

Network programming

1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.
2.Find out the length (in bytes) of each of the UDP header fields.

```
Internet Protocol Version 4, Src: 191.6.61.159, Dst: 172.16.26.45
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
v  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
   Total Length: 315
   Identification: 0x0ef5 (3829)
>  Flags: 0x0000
   Time to live: 113
   Protocol: UDP (17)
   Header checksum: 0x76da [validation disabled]
   [Header checksum status: Unverified]
   Source: 191.6.61.159
   Destination: 172.16.26.45
```

Header length(1)	Differentiated Service Field(1)	Total length(2)	Identification(2)	Flags(2)	TTL(2)
Protocol : UDP(1)	Checksum(2)	Source(4)	Destination(4)		

Network layer : IPv4

#2 UDP On Wireshark

Network programming

1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.
2.Find out the length (in bytes) of each of the UDP header fields.

다음이 UDP 헤더에 포함되는 패킷이다. 필드의 수는 총 4개를 확인할 수 있었고 송신지와 수신지가 명시되어 있고 Length와 오류 검출을 위한 Checksum이 있다.

```
User Datagram Protocol, Src Port: 43900, Dst Port: 59164
   Source Port: 43900
   Destination Port: 59164
   Length: 295
   Checksum: 0xb493 [unverified]
   [Checksum Status: Unverified]
   [Stream index: 0]
 ⌄ [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
```

Transport layer : UDP

#2 UDP On Wireshark

Network programming

1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.
2.Find out the length (in bytes) of each of the UDP header fields.

```
Data (287 bytes)
   Data: 64323a6970363acbedac64e71c313a7264323a696432303a…
   [Length: 287]
```

Data(287)

헤더들 뒤에는 287바이트의 Data가 있었다.

#3 UDP On Wireshark

Network programming

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

```
User Datagram Protocol, Src Port: 43900, Dst Port: 59164
   Source Port: 43900
   Destination Port: 59164
   Length: 295
   Checksum: 0xb493 [unverified]
   [Checksum Status: Unverified]
   [Stream index: 0]
 [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
```

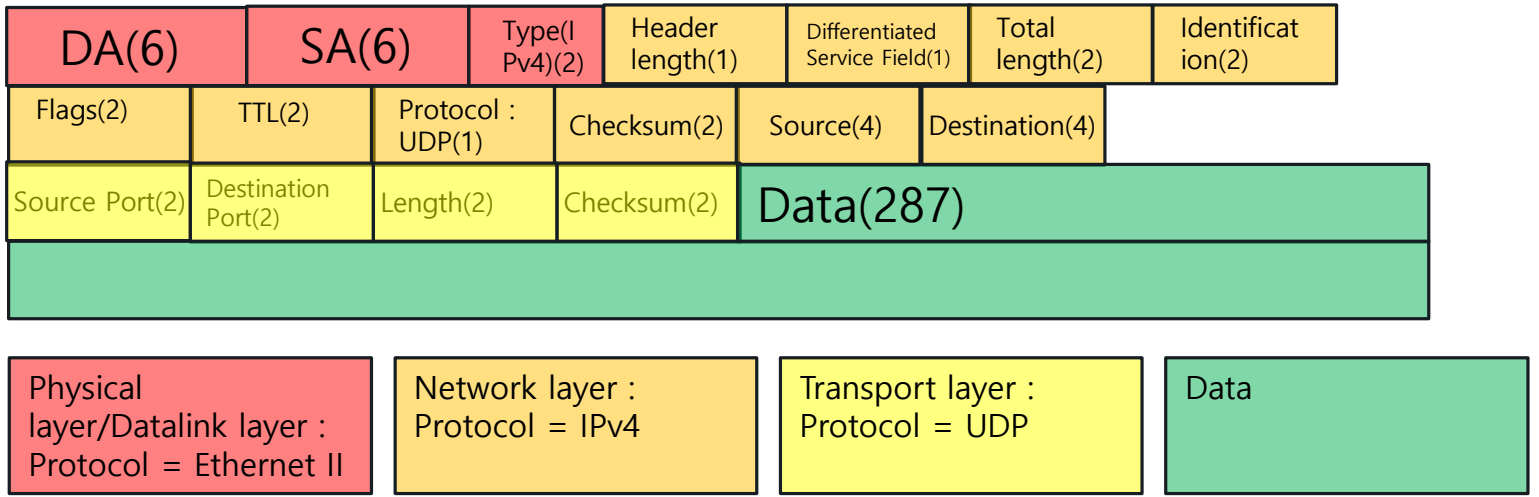
Length 필드의 값의 의미는 캡슐화된 UDP Header의 길이(바이트)와 데이터 필드의 길이(바이트)의 합을 byte로 표시한 것을 의미한다.
따라서 8byte+287byte=295byte로 Length의 값은 295이다.

#3 UDP On Wireshark

Network programming

1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.
2.Find out the length (in bytes) of each of the UDP header fields.
3.The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

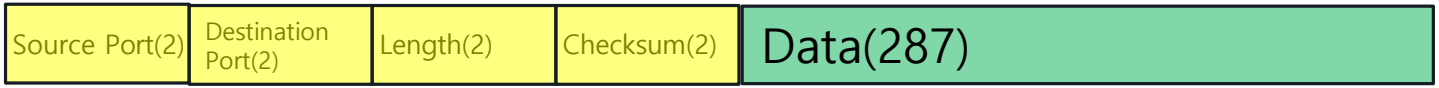
Encapsulation 구조



#4 UDP On Wireshark

Network programming

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)

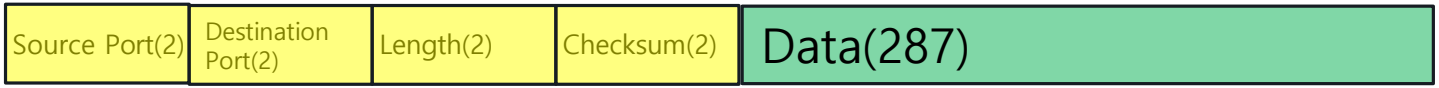


앞에서 Length 필드의 값의 의미는 UDP Header의
길이(바이트)와 데이터 필드의 길이(바이트)의 합을 byte로
표시한 것, 즉 총 길이를 2byte로 표현한 것이라고 명시하였다.
Length는 2Byte이므로 16bit이다.
따라서 UDP의 최대 길이(Byte)는 (2^16)-1=65535이어야 한다.
여기서 Length의 Byte는 UDP 헤더의 Byte수도 포함하므로
UDP Payload의 Byte의 최대 크기는65535-8=65527이다.

#5 UDP On Wireshark

Network programming

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

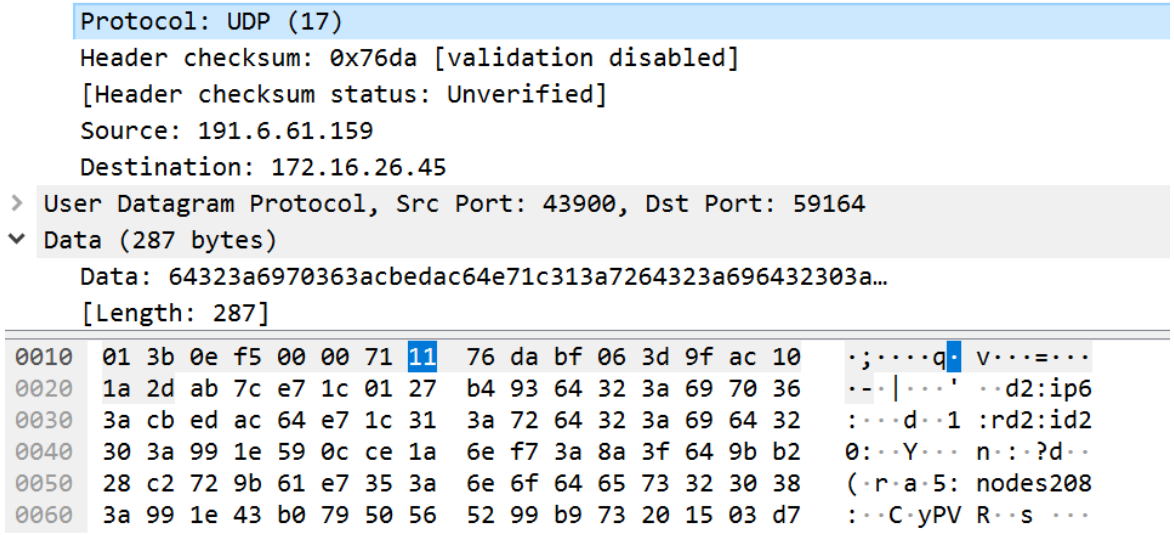


Source Port와 Destination Port는 각각 2바이트이다. 따라서 표현가능한 최대 포트 번호는 (2^16)-1=65535이다.

#6 UDP On Wireshark

Network programming

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 packet containing this UDP segment.



UDP의 Protocol number은 $17_{(10)}$ 이고 밑의 Packet Bytes Window를 참고하여 Hexadecimal로 $11_{(16)}$ 임을 알 수 있었다.

#7 UDP On Wireshark

Network programming

7. Examine a pair of UDP packets. (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.

```
1 0.000000      191.6.61.159      172.16.26.45      UDP      329 43900 → 59164 Len=287
2 0.000367      172.16.26.45      177.236.51.67     UDP      143 59164 → 62749 Len=101
```

```
User Datagram Protocol, Src Port: 43900, Dst Port: 59164
    Source Port: 43900
    Destination Port: 59164
User Datagram Protocol, Src Port: 59164, Dst Port: 62749
    Source Port: 59164
    Destination Port: 62749
```

첫번째 UDP 패킷의 Destination Port는 59164이고 두번째 UDP 패킷의 Source Port는 59164이다. 따라서 첫번째 패킷이 Port 59164로 질의하는 패킷임을 확인할 수 있으며 두번째 패킷의 Source Port가 59164이므로 첫번째 패킷에 대한 응답 패킷임을 확인할 수 있다.