

UDP

네트워크 프로그래밍

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.

No.	Time	Source	Destination	Protocol	Length	Info
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
4	0.174812	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x798bf927
5	0.174812	172.16.24.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x798bf927
6	0.190605	177.236.51.67	172.16.26.45	UDP	329	62749 → 59164 Len=287
7	0.463733	172.16.26.45	61.41.102.235	UDP	107	59164 → 50974 Len=65
10	0.482575	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xad00b45

UDP 패킷 중 하나를 선택하였다.

```
> Frame 1: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface 0
> Ethernet II, Src: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2), Dst: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4)
> Internet Protocol Version 4, Src: 191.6.61.159, Dst: 172.16.26.45
> 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]
> Data (287 bytes)
```

```
0020  1a 2d ab 7c e7 1c 01 27 b4 93 64 32 3a 69 70 36  ...|... ..d2:ip6
0030  3a cb ed ac 64 e7 1c 31 3a 72 64 32 3a 69 64 32  :...d...:rd2:ld2
0040  30 3a 99 1e 59 0c ce 1a 6e f7 3a 8a 3f 64 9b b2  0:...Y... n:...?d...
0050  28 c2 72 9b 61 e7 35 3a 6e 6f 64 65 73 32 30 38  (:...a:5: nodes208
0060  3a 99 1e 43 b0 79 50 56 52 99 b9 73 20 15 03 d7  :...C:yPV R...s ...
0070  d2 cd 3f fe d4 3d 0b 86 c6 05 dc 99 1e 43 20 bf  :?...=... ..C...
0080  e0 13 83 e4 15 6a 70 d3 b8 4b d8 df 1a 6f ab bb  :...j...K...o...
0090  b4 15 00 16 00 1a 13 b6 6a d2 26 04 0a 2a 67  f...p...B...o...
```



#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)
  ✓ 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]

Source Port(2)	Destination Port(2)	Length(2)	Checksum(2)
----------------	---------------------	-----------	-------------

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]

Source Port(2)	Destination Port(2)	Length(2)	Checksum(2)	Data(287)
----------------	---------------------	-----------	-------------	-----------

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

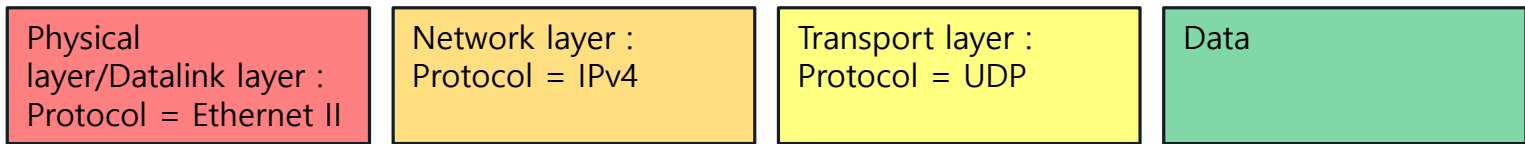
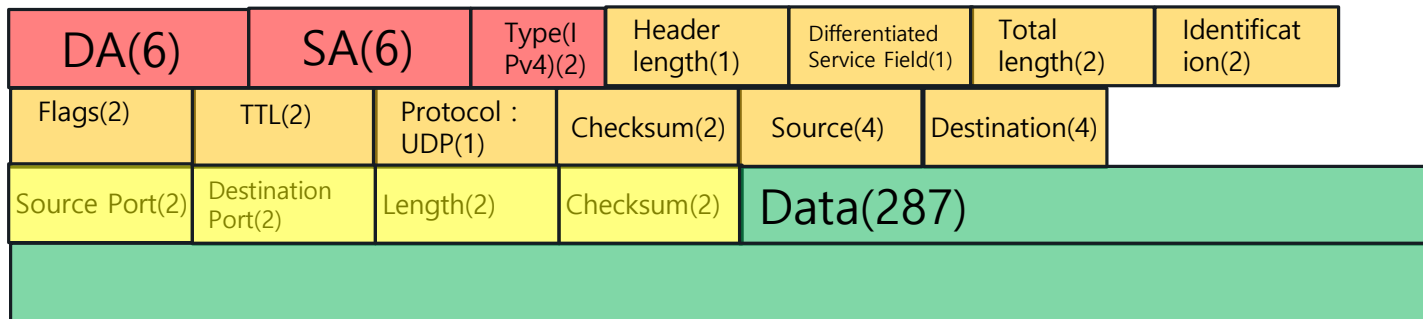


#3 UDP On Wireshark

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)

Source Port(2)	Destination Port(2)	Length(2)	Checksum(2)	Data(287)
----------------	---------------------	-----------	-------------	-----------

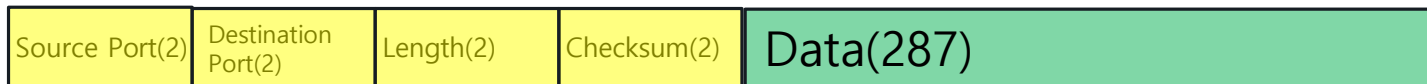
앞에서 Length 필드의 값의 의미는 UDP Header의 길이(바이트)와 데이터 필드의 길이(바이트)의 합을 byte로 표시한 것, 즉 총 길이를 2byte로 표현한 것이라고 명시하였다. Length는 2Byte이므로 16bit이다. 따라서 UDP의 최대 길이(Byte)는 $(2^{16}) - 1 = 65535$ 이어야 한다. 여기서 Length의 Byte는 UDP 헤더의 Byte수도 포함하므로 UDP Payload의 Byte의 최대 크기는 $65535 - 8 = 65527$ 이다.



#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 $(2^{16})-1=65535$ 이다.



#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.

Protocol: UDP (17)

Header checksum: 0x76da [validation disabled]

[Header checksum status: Unverified]

Source: 191.6.61.159

Destination: 172.16.26.45

> User Datagram Protocol, Src Port: 43900, Dst Port: 59164

▼ Data (287 bytes)

Data: 64323a6970363acbedac64e71c313a7264323a696432303a...

[Length: 287]

0010	01 3b 0e f5 00 00 71 11	76 da bf 06 3d 9f ac 10	.;....q. v...=...
0020	1a 2d ab 7c e7 1c 01 27	b4 93 64 32 3a 69 70 36	..- ...' ..d2:ip6
0030	3a cb ed ac 64 e7 1c 31	3a 72 64 32 3a 69 64 32	:...d..1 :rd2:id2
0040	30 3a 99 1e 59 0c ce 1a	6e f7 3a 8a 3f 64 9b b2	0:..Y... n:..?d..
0050	28 c2 72 9b 61 e7 35 3a	6e 6f 64 65 73 32 30 38	(.r.a.5: nodes208
0060	3a 99 1e 43 b0 79 50 56	52 99 b9 73 20 15 03 d7	:..C.yPV R..s ...

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.