



Laboratuvar Raporu 3

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Ferdi İslam Yılmaz

152120191055

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İindekiler

2	Giriş.....	3
3	Laboratuvar Uygulaması.....	3
3.1	UDP	3
4	Kaynaka.....	6

2 Giriş

UDP iki katmanlı bir aktarım protokolüdür. Bu rapor, UDP protokolü üzerinde yapılan uygulamaların incelenmesini amaçlamaktadır. UDP, İletişim Odaklı Protokolün (UDP) bir parçası olan bir taşıma protokolüdür ve genellikle gerçek zamanlı veri akışları için kullanılır. Bu protokol, verilerin hızlı bir şekilde iletilmesini sağlar ve ağdaki cihazlar arasında düşük gecikmeli iletişim sağlar. Bu raporun amacı, UDP protokolü üzerinde gerçekleştirilen uygulamaları incelemektir. (1)

3 Laboratuvar Uygulaması

3.1 UDP

1. Taramamızdan bir tane UDP paketini seçiyoruz. Bu paketin UDP başlığında kaç tane alan vardır ve bu alanların isimleri nelerdir?

```
▼ User Datagram Protocol, Src Port: 49708, Dst Port: 50008
  Source Port: 49708
  Destination Port: 50008
  Length: 220
  Checksum: 0xf2b4 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  > [Timestamps]
  UDP payload (212 bytes)
```

Seçtiğim bir UDP paketinde;

Source Port, Destination Port, Length ve Checksum bildileri yer alıyor.

2. Seçtiğimiz pakette her bir UDP başlık alanının kapladığı alan byte ölçüsü olarak alındığında 2 byte yer kapladığını görüyoruz.

> Frame 149: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF{...}	0000	b0 95 75 59 20 3e 34 7d f6 e0 5f 83
> Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95:75:59:20:3e)	0010	00 f0 d8 63 00 00 80 11 00 00 c0 a8
> Internet Protocol Version 4, Src: 192.168.0.108, Dst: 66.22.238.156	0020	ee 9c c2 2c c3 58 00 dc f2 b4 90 78
> User Datagram Protocol, Src Port: 49708, Dst Port: 50008	0030	71 d3 00 06 7a 30 be de 00 01 f2 a6
Source Port: 49708	0040	90 c4 2f f5 e7 37 7b f1 0e 11 a7 6a
Destination Port: 50008	0050	6c 79 1c 56 7a d9 b1 bb 0e 88 a3 9e
Length: 220	0060	91 1f c4 1a db 6f 57 22 e2 43 f6 4b
Checksum: 0xf2b4 [unverified]	0070	25 ad 80 29 68 5f 47 97 c1 76 32 37
[Checksum Status: Unverified]	0080	8f 77 cd 35 2c 21 9c ae 17 16 3d d9
[Stream index: 0]	0090	b5 25 0e d9 66 88 0e b9 4d 87 5d 87
> [Timestamps]	00a0	69 97 11 3e 21 1e 53 59 1e 27 36 8c
UDP payload (212 bytes)	00b0	b2 4f 76 fe 7e cb 9a b8 c1 01 2d a3
> Data (212 bytes)	00c0	4d 60 77 90 02 85 9a 95 e2 30 01 0c
	00d0	1c 4a 92 af a3 57 cf fa 0a ac 59 1d
	00e0	00 53 22 ba ab db 99 06 3c e6 19 47

3. Length alanındaki değeri neyin lengthidir?

> Frame 149: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF{...}	0000 b0 95 75 59 20 3e 34 7d f6 e0 5f 83
> Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95:75:59:20:3e)	0010 00 f0 d8 63 00 00 80 11 00 00 c0 a8
> Internet Protocol Version 4, Src: 192.168.0.108, Dst: 66.22.238.156	0020 ee 9c c2 2c c3 58 00 dc f2 b4 90 78
> User Datagram Protocol, Src Port: 49708, Dst Port: 50008	0030 71 d3 00 06 7a 30 be de 00 01 f2 a6
Source Port: 49708	0040 90 c4 2f f5 e7 37 7b f1 0e 11 a7 6a
Destination Port: 50008	0050 6c 79 1c 56 7a d9 b1 bb 0e 88 a3 9e
Length: 220	0060 91 1f c4 1a db 6f 57 22 e2 43 f6 4b
Checksum: 0xf2b4 [unverified]	0070 25 ad 80 29 68 5f 47 97 c1 76 32 37
[Checksum Status: Unverified]	0080 8f 77 cd 35 2c 21 9c ae 17 16 3d d9
[Stream index: 0]	0090 b5 25 0e d9 66 88 0e b9 4d 87 5d 87
> [Timestamps]	00a0 69 97 11 3e 21 1e 53 59 1e 27 36 8c
UDP payload (212 bytes)	00b0 b2 4f 76 fe 7e cb 9a b8 c1 01 2d a3
> Data (212 bytes)	00c0 4d 60 77 90 02 85 9a 95 e2 30 01 0c
	00d0 1c 4a 92 af a3 57 cf fa 0a ac 59 1d
	00e0 00 53 22 ba ab db 99 06 3c e6 19 47

Length alanındaki değeri 220'dir. Bunun içerisindeki 4 header toplam 8 byte yer kaplar, geri kalan 212 byte ise encapsulated data'dır.

4. UDP payloadında kullanılabilecek alan en fazla kaç byte'tır?

UDP payload'ında en fazla kullanılabilecek alan 2^{16} eksi hali hazırda kullanılan headerların çıkarılmasıyla bulunur.

$2^{16} = (65536 - 1) - 8 = 65527$ byte olarak hesaplanabilir.

5. Kullanılabilecek en büyük kaynak port numarası kaçtır?

Yine aynı işlemi yaparak blabiliriz. 2^{16} hesabından giderek 65536 tane port adresi vardır ve en büyüğü 65535'dir.

6. UDP'nin protocol numarası kaçtır?

Total Length: 240	0000 b0 95 75 59 20 3e 34 7d
Identification: 0xe97a (59770)	0010 00 f0 e9 7a 00 00 80
> 000. = Flags: 0x0	0020 ee 9c e6 90 c3 58 00 dc
...0 0000 0000 0000 = Fragment Offset: 0	0030 4c d3 00 06 7a 30 be de
Time to Live: 128	0040 ed 64 ff 25 89 b4 e7 10
Protocol: UDP (17)	0050 bc fd ce a7 cf 85 e2 1c
Header Checksum: 0x0000 [validation disabled]	0060 7e cf 1f 6f f7 be 5b c9
[Header checksum status: Unverified]	0070 2a 29 d6 8d 09 39 e6 91
Source Address: 192.168.0.108	0080 9e c0 c7 02 56 0e 89 cf
Destination Address: 66.22.238.156	0090 9c c7 16 43 26 7c 78 54
	00a0 0f 2b 3a 89 d4 aa f0 a7

UDP'nin protocol numarası 17'dir. Hexadecimal formatı ise 0x11'dir.

7. Bir çift UDP paketi inceleyeceğiz. Port adresleri arasındaki ilişkiyi açıklayacağız.

28287	537.967737	192.168.0.108	192.168.0.1	DNS	74	Standard query	0xb0a8 A www.google.com
28288	537.968034	192.168.0.108	192.168.0.1	DNS	74	Standard query	0xfc6a HTTPS www.google.com
28291	537.971953	192.168.0.1	192.168.0.108	DNS	121	Standard query response	0xc3b3 A cas.criteo.com CNA
28295	537.973437	192.168.0.108	192.168.0.1	DNS	77	Standard query	0x4d0e A static.criteo.net
28296	537.973731	192.168.0.108	192.168.0.1	DNS	77	Standard query	0x72f7 HTTPS static.criteo.net
28300	537.980050	192.168.0.1	192.168.0.108	DNS	85	Standard query response	0xce64 A s0.wp.com A 192.0.
28301	537.982423	192.168.0.1	192.168.0.108	DNS	131	Standard query response	0x00b4 HTTPS s0.wp.com SOA
28302	537.983703	192.168.0.108	192.168.0.1	DNS	85	Standard query	0x380f A tpc.googlesyndication.com
28303	537.984158	192.168.0.108	192.168.0.1	DNS	85	Standard query	0x9009 HTTPS tpc.googlesyndication.c
28304	537.991496	192.168.0.1	192.168.0.108	DNS	99	Standard query response	0xfc6a HTTPS www.google.com
28305	537.991496	192.168.0.1	192.168.0.108	DNS	90	Standard query response	0xb0a8 A www.google.com A 1
28306	537.991496	192.168.0.1	192.168.0.108	DNS	337	Standard query response	0xa0a9 A jnn-pa.googleapis.
28310	537.999955	192.168.0.1	192.168.0.108	DNS	138	Standard query response	0xc890 HTTPS jnn-pa.googlelea
28314	538.002278	192.168.0.1	192.168.0.108	DNS	127	Standard query response	0x4d0e A static.criteo.net

> Frame 28287: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Dev	0000	b0 95 75 59 20 3e 34 7d f6 e0 5f
> Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95:7	0010	00 3c 60 99 00 00 00 11 00 00 c0
> Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.1	0020	00 01 cc 5f 00 35 00 28 81 f7 b0
> User Datagram Protocol, Src Port: 52319, Dst Port: 53	0030	00 00 00 00 00 00 03 77 77 77 06
Source Port: 52319	0040	65 03 63 6f 6d 00 00 01 00 01
Destination Port: 53		
Length: 40		
Checksum: 0x81f7 [unverified]		
[Checksum Status: Unverified]		
[Stream index: 132]		
[Timestamps]		
[Time since first frame: 0.00000000 seconds]		
[Time since previous frame: 0.00000000 seconds]		
UDP payload (32 bytes)		
Domain Name System (query)		

Google sitesine gönderilen paketi incelediğimizde kaynak portumuzun 52319 ve hedef portumuzun 53 olduğunu görüyoruz.

28287	537.967737	192.168.0.108	192.168.0.1	DNS	74	Standard query	0xb0a8 A www.google.com
28288	537.968034	192.168.0.108	192.168.0.1	DNS	74	Standard query	0xfc6a HTTPS www.google.com
28291	537.971953	192.168.0.1	192.168.0.108	DNS	121	Standard query response	0xc3b3 A cas.criteo.com CNA
28295	537.973437	192.168.0.108	192.168.0.1	DNS	77	Standard query	0x4d0e A static.criteo.net
28296	537.973731	192.168.0.108	192.168.0.1	DNS	77	Standard query	0x72f7 HTTPS static.criteo.net
28300	537.980050	192.168.0.1	192.168.0.108	DNS	85	Standard query response	0xce64 A s0.wp.com A 192.0.
28301	537.982423	192.168.0.1	192.168.0.108	DNS	131	Standard query response	0x00b4 HTTPS s0.wp.com SOA
28302	537.983703	192.168.0.108	192.168.0.1	DNS	85	Standard query	0x380f A tpc.googlesyndication.com
28303	537.984158	192.168.0.108	192.168.0.1	DNS	85	Standard query	0x9009 HTTPS tpc.googlesyndication.c
28304	537.991496	192.168.0.1	192.168.0.108	DNS	99	Standard query response	0xfc6a HTTPS www.google.com
28305	537.991496	192.168.0.1	192.168.0.108	DNS	90	Standard query response	0xb0a8 A www.google.com A 1
28306	537.991496	192.168.0.1	192.168.0.108	DNS	337	Standard query response	0xa0a9 A jnn-pa.googleapis.
28310	537.999955	192.168.0.1	192.168.0.108	DNS	138	Standard query response	0xc890 HTTPS jnn-pa.googlelea
28314	538.002278	192.168.0.1	192.168.0.108	DNS	127	Standard query response	0x4d0e A static.criteo.net

> Frame 28305: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Dev	0000	34 7d f6 e0 5f 83 b0 95 75 59 20 3e
> Ethernet II, Src: Tp-LinkT_59:20:3e (b0:95:75:59:20:3e), Dst: IntelCor_e0:5f:83 (34:7d:f	0010	00 4c 22 c9 00 00 35 11 e1 1a c0 a
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.108	0020	00 6c 00 35 cc 5f 00 38 e6 7f b0 a
> User Datagram Protocol, Src Port: 53, Dst Port: 52319	0030	00 01 00 00 00 00 03 77 77 77 06 e
Source Port: 53	0040	65 03 63 6f 6d 00 00 01 00 01 c0 e
Destination Port: 52319	0050	00 00 00 68 00 04 8e fa bb 64
Length: 56		
Checksum: 0xe67f [unverified]		
[Checksum Status: Unverified]		
[Stream index: 132]		
[Timestamps]		
[Time since first frame: 0.023759000 seconds]		
[Time since previous frame: 0.023759000 seconds]		
UDP payload (48 bytes)		
Domain Name System (response)		

Google'un bize gönderdiği cevap paketine baktığımızda ise kaynak portunun 53, hedef portunun ise 52319 olduğunu görüyoruz. Giden pakete göre tam tersi.

4 Kaynakça

<https://turk.net/blog/udp-user-datagram-protocol-nedir/> (1)