

# UDP ATÖLYESİ

## ATÖLYENİN HEDEFİ:

Bu atölyede UDP paketinin nasıl alındığını öğreneceksiniz.

## ATÖLYENİN AMACI:

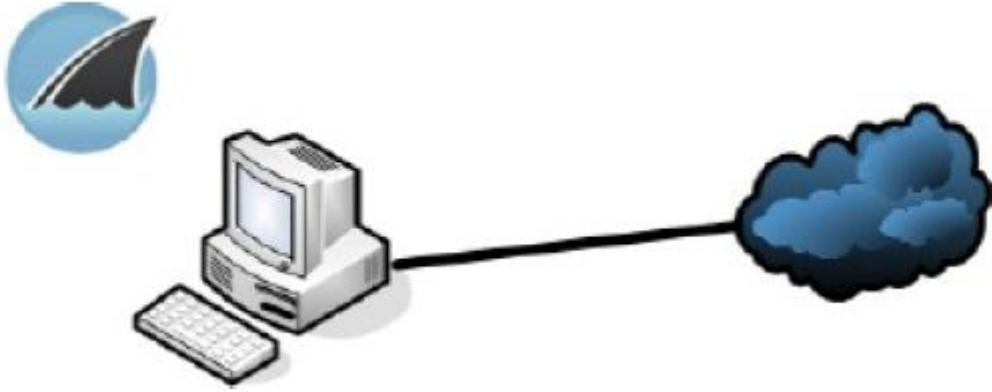
User Datagram Protocol (UDP) ise RIP, DNS, SNMP ve DHCP gibi hizmet ve protokolleri barındırır. UDP paketleri, TCP paketlerine göre daha az yüke sahiptir ancak paketin düşüp düşmediği bilinmez.

## ATÖLYE ARACI:

Wireshark'ı ev bilgisayarınızda veya VM'de kolaylıkla çalıştırabilirsiniz.

## ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için aşağıdaki topolojiyi kullanmanız tavsiye edilir.



## ATÖLYE ANLATIMI:

### Adım1:

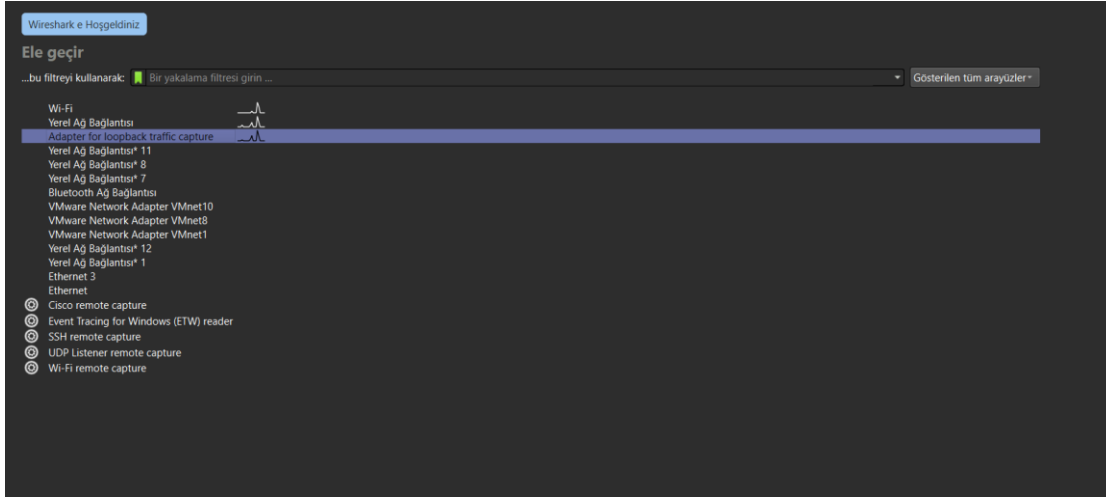
Wireshark'ı veya başka bir packet sniffer'ı bilgisayarınıza indirin.

### Adım 2:

Bir web tarayıcısı açın, ancak herhangi bir URL girmeyin.

### Adım 3:

Wireshark'ı açarak yakalamak istediğimiz bağlantıyı seçelim. Ben “yerel ağ bağlantısı”nı seçtim.



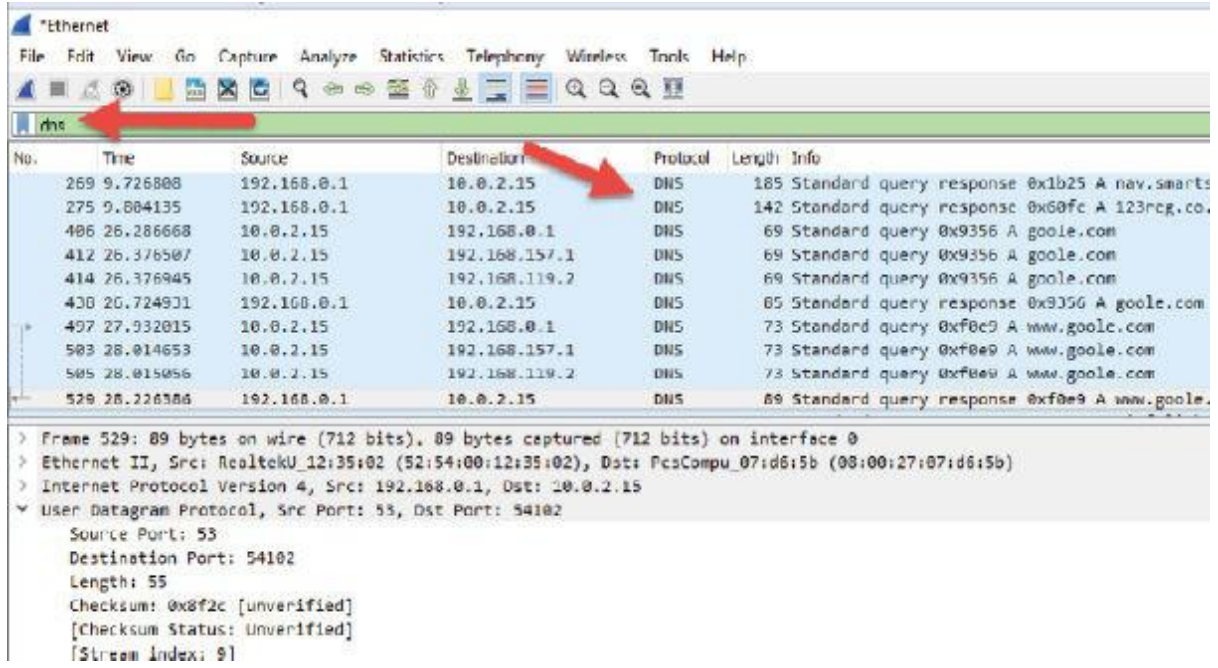
### Adım 4:

Bir web sitesine gidin. Bir DNS araması yapmamız gerekiyor (çünkü UDP kullanılıyor).



### Adım 5:

Wireshark'a gidin. Kırmızı kareye basarak yakalamaları durdurun. Daha sonra DNS'i aramak için filtre çubuğunu kullanın. Arama için küçük harf kullanmanız gerekiyor.



No.	Time	Source	Destination	Protocol	Length	Info
269	9.726808	192.168.0.1	10.0.2.15	DNS	185	Standard query response 0x1b25 A nav.smarts
275	9.804135	192.168.0.1	10.0.2.15	DNS	142	Standard query response 0x60fc A 123reg.co.
406	26.286668	10.0.2.15	192.168.0.1	DNS	69	Standard query 0x9356 A gooile.com
412	26.376507	10.0.2.15	192.168.157.1	DNS	69	Standard query 0x9356 A gooile.com
414	26.376945	10.0.2.15	192.168.119.2	DNS	69	Standard query 0x9356 A gooile.com
430	26.724931	192.168.0.1	10.0.2.15	DNS	85	Standard query response 0x9356 A gooile.com
497	27.932015	10.0.2.15	192.168.0.1	DNS	73	Standard query 0xf0c9 A www.gooile.com
503	28.014653	10.0.2.15	192.168.157.1	DNS	73	Standard query 0xf0c9 A www.gooile.com
505	28.015056	10.0.2.15	192.168.119.2	DNS	73	Standard query 0xf0c9 A www.gooile.com
529	28.226386	192.168.0.1	10.0.2.15	DNS	89	Standard query response 0xf0e9 A www.gooile.com

> Frame 529: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0  
 > Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_07:d6:5b (08:00:27:07:d6:5b)  
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 10.0.2.15  
 > User Datagram Protocol, Src Port: 53, Dst Port: 54102  
 Source Port: 53  
 Destination Port: 54102  
 Length: 55  
 Checksum: 0x8f2c [unverified]  
 [Checksum Status: Unverified]  
 [Stream Index: 9]

## Adım 6:

DNS girişlerinden birine tıklayın ve paket yakalamayı inceleyin.

Girişleri aşağıdaki UDP görüntüsüne göre kontrol edin. Sıra numarası ve flag gibi birçok TCP alanının eksik olduğunu fark edin.

> Frame 529: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0  
 > Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_07:d6:5b (08:00:27:07:d6:5b)  
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 10.0.2.15  
 > User Datagram Protocol, Src Port: 53, Dst Port: 54102  
 Source Port: 53  
 Destination Port: 54102  
 Length: 55  
 Checksum: 0x8f2c [unverified]  
 [Checksum Status: Unverified]  
 [Stream Index: 9]

> Domain Name System (response)

0000	08 00 27 07 d6 5b 52 54 00 12 35 02 08 00 45 00	..*..[RT..S...E..
0010	00 4b 2e 86 00 00 40 11 7f 64 c0 a8 00 01 0a 00	..K...@...d.....
0020	02 0f 00 35 d3 56 00 37 8f 2c f0 e9 81 80 00 01	...S.V-7... ..
0030	00 01 00 00 00 00 03 77 77 77 05 67 6f 6f 6c 65	.....w ww:goole
0040	03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00	..com.....
0050	00 0e 10 00 04 d9 a0 00 c9	.....

## Adım 7:

UDP'nin hata denetimi için bir checksum'ı vardır. Checksum alanları için yukarıdaki paket yakalamayı kontrol edin.

UDP alanlarını kontrol etmek için aşağıdaki görseli referans olarak kullanabilirsiniz.

## UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

Not: DNS gibi bazı protokoller, başlamak için UDP'yi kullanır ancak daha sonra yanıt yoksa veya bölge transferleri için TCP'ye geçer, bunu aklınızda bulundurun.