

Scapy - Wireshark Kullanımı

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

1)

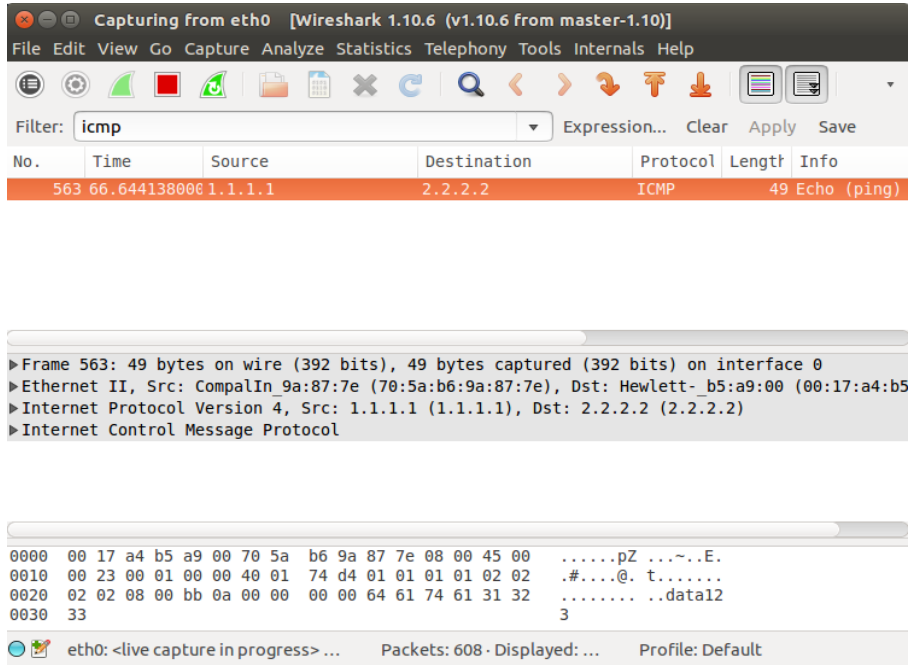
Scapy ile ICMP Paket Oluşturma

```
> sudo su
> scapy
>>> send(IP(src="1.1.1.1",dst="2.2.2.2")/ICMP()/"data123")
                                     ^
payload =====
```

Wireshark ile Yakalama

Filter : icmp

Output:



Görüldüğü üzere oluşturduğumuz icmp paketi wireshark ekranına düşmüştür. Ekranın altında yer alan paketin raw halinde data123 payload'umuzu da görebiliriz.

2)

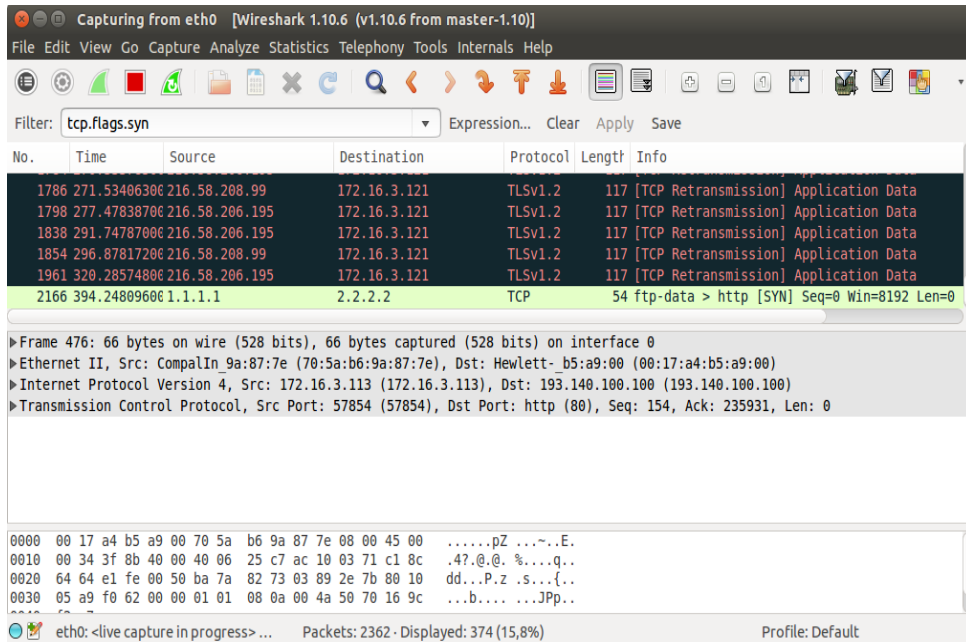
Scapy ile SYN Paketi Yollama

```
> sudo su
> scapy
>>> send(IP(src="1.1.1.1",dst="2.2.2.2")/TCP(dport=80,flags="S"))
```

Wireshark ile Yakalama

Filter : tcp.flags.syn

Output:



Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.flags.syn Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1786	271.534963800	216.58.208.99	172.16.3.121	TLSv1.2	117	[TCP Retransmission] Application Data
1798	277.478387000	216.58.206.195	172.16.3.121	TLSv1.2	117	[TCP Retransmission] Application Data
1838	291.747870000	216.58.206.195	172.16.3.121	TLSv1.2	117	[TCP Retransmission] Application Data
1854	296.878172000	216.58.208.99	172.16.3.121	TLSv1.2	117	[TCP Retransmission] Application Data
1961	320.285748000	216.58.206.195	172.16.3.121	TLSv1.2	117	[TCP Retransmission] Application Data
2166	394.248896000	1.1.1.1	2.2.2.2	TCP	54	ftp-data > http [SYN] Seq=0 Win=8192 Len=0

▶ Frame 476: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: CompalIn_9a:87:7e (70:5a:b6:9a:87:7e), Dst: Hewlett-b5:a9:00 (00:17:a4:b5:a9:00)
▶ Internet Protocol Version 4, Src: 172.16.3.113 (172.16.3.113), Dst: 193.140.100.100 (193.140.100.100)
▶ Transmission Control Protocol, Src Port: 57854 (57854), Dst Port: http (80), Seq: 154, Ack: 235931, Len: 0

0000 00 17 a4 b5 a9 00 70 5a b6 9a 87 7e 08 00 45 00pZ ...E.
0010 00 34 3f 8b 40 00 40 06 25 c7 ac 10 03 71 c1 8c .4?.@.%...q..
0020 64 64 e1 fe 00 50 ba 7a 82 73 03 89 2e 7b 80 10 dd...P.z .s...{..
0030 05 a9 f0 62 00 00 01 01 08 0a 00 4a 50 70 16 9c ...b....Jpp..
.....

eth0: <live capture in progress> ... Packets: 2362 - Displayed: 374 (15,8%) Profile: Default

Görüldüğü üzere scapy ile oluşturduğumuz SYN paketi ekrana düşmüştür.

3)

Scapy ile FIN Paketi Yollama

```
> sudo su
> scapy
>>> send(IP(src="1.1.1.1",dst="2.2.2.2")/TCP(dport=80,flags="F"))
```

Wireshark ile Yakalama

Filter : tcp.flags.fin

Output:

No.	Time	Source	Destination	Protocol	Length	Info
10671	713.02149100	172.16.3.113	54.243.128.120	TCP	66	56576 > https [ACK] Seq=1475 Ack=6753 Win=4
10672	713.02166500	54.243.128.120	172.16.3.113	TCP	66	https > 56572 [FIN, ACK] Seq=8369 Ack=2217
10673	713.02167300	172.16.3.113	54.243.128.120	TCP	66	56572 > https [ACK] Seq=2217 Ack=8370 Win=5
10674	713.02177200	54.243.128.120	172.16.3.113	TCP	66	https > 56586 [FIN, ACK] Seq=138 Ack=570 Wi
10675	713.02177900	172.16.3.113	54.243.128.120	TCP	66	56586 > https [ACK] Seq=570 Ack=139 Win=303
10676	713.02190200	54.225.76.175	172.16.3.113	TCP	66	https > 56638 [FIN, ACK] Seq=138 Ack=570 Wi
10677	713.02190900	172.16.3.113	54.225.76.175	TCP	66	56638 > https [ACK] Seq=570 Ack=139 Win=303
10945	718.51783800	1.1.1.1	2.2.2.2	TCP	54	[TCP Retransmission] ftp-data > http [FIN]

Frame 1961: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0
Ethernet II, Src: Hewlett-b5:a9:00 (00:17:a4:b5:a9:00), Dst: WistronI 14:8c:3b (54:ee:75:14:8c:3b)
Internet Protocol Version 4, Src: 216.58.206.195 (216.58.206.195), Dst: 172.16.3.121 (172.16.3.121)
Transmission Control Protocol, Src Port: https (443), Dst Port: 54871 (54871), Seq: 4294967234, Ack: 1, Len: 63
Secure Sockets Layer

0000 54 ee 75 14 8c 3b 00 17 a4 b5 a9 00 08 00 45 00 T.u.;.E.
0010 00 67 af 1d 00 00 31 06 83 ec d8 3a ce c3 ac 10 .g....l.
0020 03 79 01 bb d6 57 48 6a 3e 9e 9d 4a 0a 23 50 18 .y..WHj >..J.#P.
0030 01 6d 0c 5b 00 00 17 03 03 00 3a 00 00 00 00 .m.[... ..
eth0: <live capture in progress> ... Packets: 11325 - Displayed: 1562 (13,8%) Profile: Default

Siyah renkle gösterilen kayıttan görülebileceği üzere oluşturduğumuz FIN paketi ekrana düşmüştür.

4)

Scapy ile Reset Paketi Yollama

```
> sudo su
> scapy
>>> send(IP(src="1.1.1.1",dst="2.2.2.2")/TCP(dport=80,flags="R"))
```

Wireshark ile Yakalama

Filter : tcp.flags.reset

Output:

The screenshot shows the Wireshark interface with a filter set to 'tcp.flags.reset'. The packet list pane shows several packets, with the last one (No. 15436) highlighted in red. This packet is a TCP RST packet from 1.1.1.1 to 2.2.2.2. The packet details pane shows the following information:

- Frame 14705: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
- Ethernet II, Src: Hewlett_b5:a9:00 (00:17:a4:b5:a9:00), Dst: Hewlett_c2:96:c5 (78:e7:d1:c2:96:c5)
- Internet Protocol Version 4, Src: 194.132.162.36 (194.132.162.36), Dst: 172.16.3.54 (172.16.3.54)
- Transmission Control Protocol, Src Port: https (443), Dst Port: 50610 (50610), Seq: 1, Ack: 1, Len: 11
- Secure Sockets Layer

The packet bytes pane shows the raw data of the RST packet:

```
0000 78 e7 d1 c2 96 c5 00 17 a4 b5 a9 00 08 00 45 00  x.....E.
0010 00 33 2a 98 40 00 2b 06 11 3e c2 84 a2 24 ac 10  .3*.@.+ .>...$.
0020 03 36 01 bb c5 b2 2e 0f 8b d6 56 52 89 86 50 18  .6.....VR..P.
0030 00 2e 8f 05 00 00 8f 04 66 60 3d cc e4 5e 6f e2  .....f'=.^o.
```

Kırmızı renkle gösterilen kayıttan görebileceği üzere oluşturduğumuz RST paketi ekrana düşmüştür.

5)

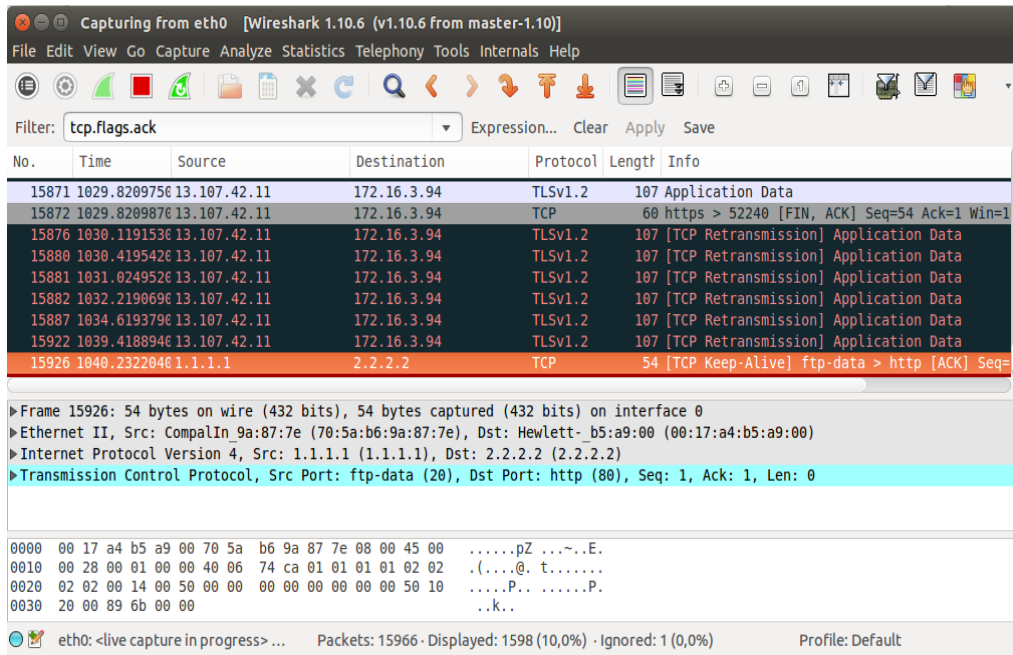
Scapy ile Ack Paketi Yollama

```
> sudo su
> scapy
>>> send(IP(src="1.1.1.1",dst="2.2.2.2")/TCP(dport=80,flags="A"))
```

Wireshark ile Yakalama

Filter : tcp.flags.ack

Output:



Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.flags.ack Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
15871	1029.8209750	13.107.42.11	172.16.3.94	TLSv1.2	107	Application Data
15872	1029.8209870	13.107.42.11	172.16.3.94	TCP	60	https > 52240 [FIN, ACK] Seq=54 Ack=1 Win=1
15876	1030.1191530	13.107.42.11	172.16.3.94	TLSv1.2	107	[TCP Retransmission] Application Data
15880	1030.4195420	13.107.42.11	172.16.3.94	TLSv1.2	107	[TCP Retransmission] Application Data
15881	1031.0249520	13.107.42.11	172.16.3.94	TLSv1.2	107	[TCP Retransmission] Application Data
15882	1032.2190690	13.107.42.11	172.16.3.94	TLSv1.2	107	[TCP Retransmission] Application Data
15887	1034.6193790	13.107.42.11	172.16.3.94	TLSv1.2	107	[TCP Retransmission] Application Data
15922	1039.4188940	13.107.42.11	172.16.3.94	TLSv1.2	107	[TCP Retransmission] Application Data
15926	1040.2322040	1.1.1.1	2.2.2.2	TCP	54	[TCP Keep-Alive] ftp-data > http [ACK] Seq=

► Frame 15926: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
► Ethernet II, Src: CompalIn 9a:87:7e (70:5a:b6:9a:87:7e), Dst: Hewlett- b5:a9:00 (00:17:a4:b5:a9:00)
► Internet Protocol Version 4, Src: 1.1.1.1 (1.1.1.1), Dst: 2.2.2.2 (2.2.2.2)
► Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

0000 00 17 a4 b5 a9 00 70 5a b6 9a 87 7e 08 00 45 00pZ ...E.
0010 00 28 00 01 00 00 40 06 74 ca 01 01 01 02 02 ..(...@. t.....
0020 02 02 00 14 00 00 00 00 00 00 00 00 00 50 10P.P.
0030 20 00 89 6b 00 00 ..k.

eth0: <live capture in progress> ... Packets: 15966 · Displayed: 1598 (10,0%) · Ignored: 1 (0,0%) Profile: Default

Turuncu renkle gösterilen kayıttan görebileceği üzere oluşturduğumuz ACK paketi ekrana düşmüştür.

6)

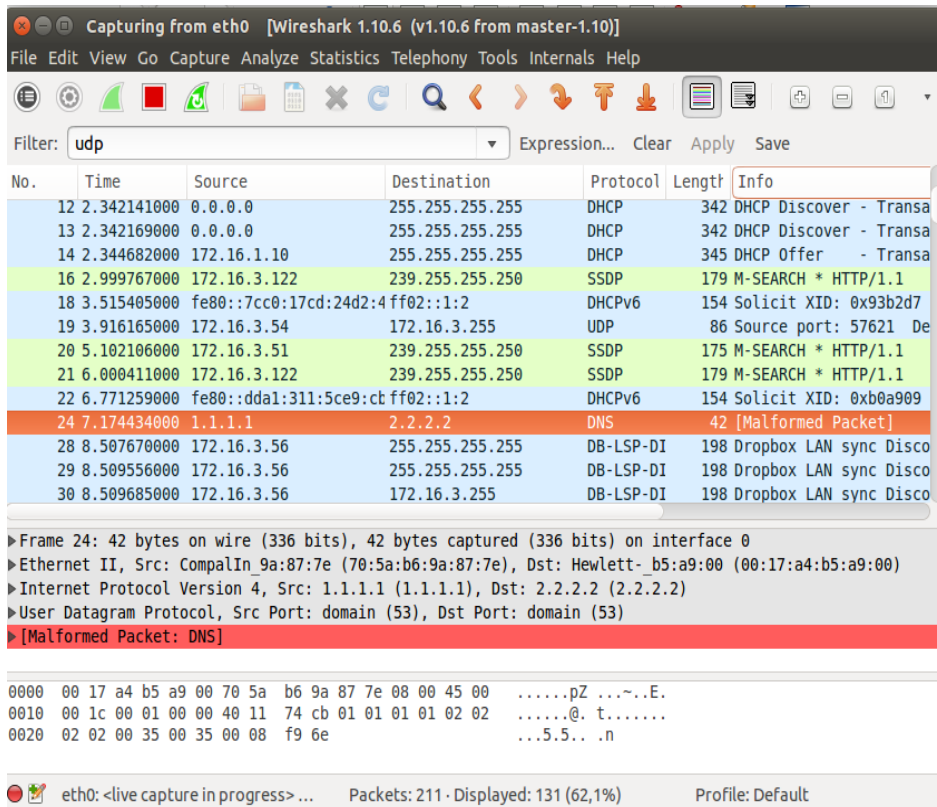
Scapy ile Udp Paketi Yollama

```
> sudo su
> scapy
>>> send(IP(src="1.1.1.1",dst="2.2.2.2")/UDP(dport="53"))
```

Wireshark ile Yakalama

Filter : udp

Output:



No.	Time	Source	Destination	Protocol	Length	Info
12	2.342141000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transa
13	2.342169000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transa
14	2.344682000	172.16.1.10	255.255.255.255	DHCP	345	DHCP Offer - Transa
16	2.999767000	172.16.3.122	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
18	3.515405000	fe80::7cc0:17cd:24d2:4ff02::1:2		DHCPv6	154	Solicit XID: 0x93b2d7
19	3.916165000	172.16.3.54	172.16.3.255	UDP	86	Source port: 57621 De
20	5.102106000	172.16.3.51	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
21	6.000411000	172.16.3.122	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
22	6.771259000	fe80::dda1:311:5ce9:ctff02::1:2		DHCPv6	154	Solicit XID: 0xb0a909
24	7.174434000	1.1.1.1	2.2.2.2	DNS	42	[Malformed Packet]
28	8.507670000	172.16.3.56	255.255.255.255	DB-LSP-DI	198	Dropbox LAN sync Disco
29	8.509556000	172.16.3.56	255.255.255.255	DB-LSP-DI	198	Dropbox LAN sync Disco
30	8.509685000	172.16.3.56	172.16.3.255	DB-LSP-DI	198	Dropbox LAN sync Disco

►Frame 24: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
►Ethernet II, Src: CompalIn_9a:87:7e (70:5a:b6:9a:87:7e), Dst: Hewlett_b5:a9:00 (00:17:a4:b5:a9:00)
►Internet Protocol Version 4, Src: 1.1.1.1 (1.1.1.1), Dst: 2.2.2.2 (2.2.2.2)
►User Datagram Protocol, Src Port: domain (53), Dst Port: domain (53)
►[Malformed Packet: DNS]

```
0000 00 17 a4 b5 a9 00 70 5a b6 9a 87 7e 08 00 45 00  ....pZ ...~.E.
0010 00 1c 00 01 00 00 40 11 74 cb 01 01 01 02 02  ....@. t.....
0020 02 02 00 35 00 35 00 08 f9 6e  ....5.5...n
```

eth0: <live capture in progress> ... Packets: 211 · Displayed: 131 (62,1%) Profile: Default

Turuncu renkle gösterilen kayıttan görebileceği üzere UDP paketimiz ekrana düşmüştür.

7)

Scapy ile Arp Paketi Yollama

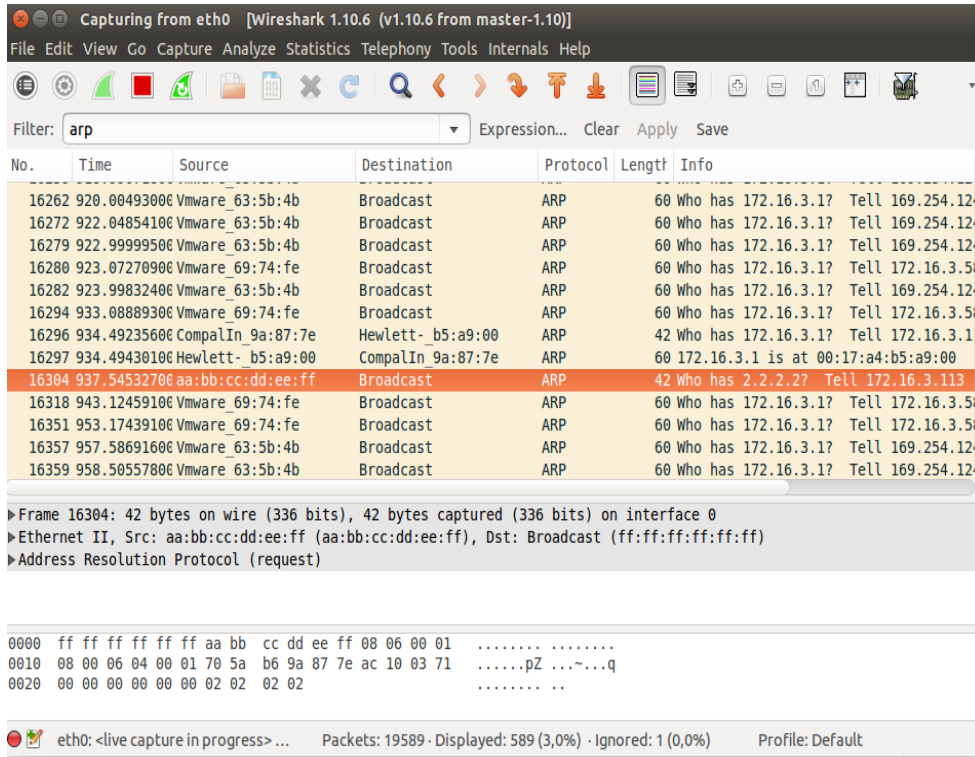
```
> sudo su
> scapy
>>> sendp(Ether(src="aa:bb:cc:dd:ee:ff",dst="ff:ff:ff:ff:ff:ff")/ARP(pdst="2.2.2.2"))
```

aa:bb:cc:dd:ee:ff mac adresimizle broadcast yaparak 2.2.2.2 ip'si hangi mac adresi üzerinde sorusunu sorarız.

Wireshark ile Yakalama

Filter : arp

Output:



Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: arp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16262	920.00493000	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.12...
16272	922.04854100	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.12...
16279	922.99999500	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.12...
16280	923.07270900	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.5...
16282	923.99832400	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.12...
16294	933.08889300	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.5...
16296	934.49235600	CompalIn_9a:87:7e	Hewlett_b5:a9:00	ARP	42	Who has 172.16.3.1? Tell 172.16.3.1...
16297	934.49430100	Hewlett_b5:a9:00	CompalIn_9a:87:7e	ARP	60	172.16.3.1 is at 00:17:a4:b5:a9:00
16304	937.54532700	aa:bb:cc:dd:ee:ff	Broadcast	ARP	42	Who has 2.2.2.2? Tell 172.16.3.113
16318	943.12459100	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.5...
16351	953.17439100	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.5...
16357	957.58691600	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.12...
16359	958.50557800	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.12...

▶ Frame 16304: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▶ Ethernet II, Src: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Address Resolution Protocol (request)

```
0000 ff ff ff ff ff aa bb cc dd ee ff 08 06 00 01 .....
0010 08 00 06 04 00 01 70 5a b6 9a 87 7e ac 10 03 71 .....pZ ...~...q
0020 00 00 00 00 00 00 02 02 02 02 ..... ..
```

eth0: <live capture in progress> ... Packets: 19589 - Displayed: 589 (3,0%) - Ignored: 1 (0,0%) Profile: Default

Turuncu renkle gösterilen kayıttan görülebileceği üzere ARP sorgumuz ekrana düşmüştür.

Ekstra

1)

Scapy ile Syn Taraması Yapma

```
> sudo su
> scapy
>>> send(IP(src="1.1.1.1",dst="2.2.2.2")/TCP(dport=(1,65535),flags="S"))
```

Port Aralığı =====

Wireshark ile Görüntüleme

Filter : tcp.flags.syn

Output:

The screenshot shows the Wireshark interface with the filter 'tcp.flags.syn' applied. The packet list pane displays a series of SYN packets from source 1.1.1.1 to destination 2.2.2.2 on various ports. The packet details pane shows the selected packet (No. 25026) with the following information:

- Frame 25026: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
- Ethernet II, Src: Hewlett- b5:a9:00 (00:17:a4:b5:a9:00), Dst: Hewlett- c2:96:c5 (78:e7:d1:c2:96:c5)
- Internet Protocol Version 4, Src: 194.132.162.36 (194.132.162.36), Dst: 172.16.3.54 (172.16.3.54)
- Transmission Control Protocol, Src Port: https (443), Dst Port: 50610 (50610), Seq: 12, Ack: 1, Len: 44
- Secure Sockets Layer

The packet bytes pane shows the raw data in hexadecimal and ASCII format:

```
0000 78 e7 d1 c2 96 c5 00 17 a4 b5 a9 00 08 00 45 00 x.....E.
0010 00 54 2a a4 40 00 2b 06 11 11 c2 84 a2 24 ac 10 .T*.@+. ...$.
0020 03 36 01 bb c5 b2 2e 0f 8b e1 56 52 89 86 50 19 .6.....VR..P.
0030 00 2e 2e 83 00 00 6e 2f 67 2d b1 56 c4 f4 5c f6 .....n/ g-.V.\.
```

Info sütunundan görülebileceği üzere sırasıyla her porta SYN paketi gönderilmektedir.

2)

Scapy ile ARP Sorgusu Yapma

```
> sudo su
> scapy
>>> sendp(Ether(src="70:5a:b6:9a:87:7e",dst="ff:ff:ff:ff:ff:ff")/ARP(pdst="172.16.3.134"))
```

^
|
Kendi Mac Adresim
(Tubitak Laptop)

^
|
Sorgulanan IP
(Tubitak Masaüstü)

Mac adresimizle broadcast yaparak 172.16.3.134 ip'si hangi mac adresi üzerinde sorusunu sorarız.

Wireshark ile Görüntüleme

Filter : ip.addr == 172.16.3.134

Output:

Filter: arp

Time	Source	Destination	Protocol	Length	Info
20.20319206	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
21.09324506	Vmware_10:ba:eb	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.53
21.20157806	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
22.23841806	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.58
23.29214306	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
24.21248906	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
25.21081506	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
25.81661406	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.134? Tell 172.16.3.113
25.81711106	Hewlett- c2:96:ed	CompalIn_9a:87:7e	ARP	60	172.16.3.134 is at 78:e7:d1:c2:96:ed
27.30132206	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
28.20611906	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213

Frame 3938: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Vmware_69:74:fe (00:0c:29:69:74:fe), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

```
0000 ff ff ff ff ff 00 0c 29 69 74 fe 08 06 00 01 ..... )it....
0010 08 00 06 04 00 01 00 0c 29 69 74 fe ac 10 03 3a ..... )it....
0020 00 00 00 00 00 00 ac 10 03 01 00 00 00 00 00 .....
0030 00 00 00 00 00 00 00 00 00 00 00 ..... ..
```

eth0: <live capture in progress> ... Packets: 4095 - Displayed: 546 (13,3%) - Marked: 2 (0,0%) Profile: Default

Siyah ile işaretlenmiş kayıtlardan ilki arp request'tir. İkincisi ise arp response'tur. İlkine bakacak olursak Info sütununda belirtildiği gibi kim 172.16.3.134 ip'sine sahip sorusu sorulmaktadır ve cevabın bizim IP'mize söylenmesi istenmektedir. İkinci kayıta ise Info sütunundan görülebileceği gibi 172.16.3.134 ip'si 78:c7:d1:c2:96:ed adresi üzerindedir bilgisi gelmektedir. Böylece scapy ile arp request yapmış olduk ve Arp request & arp response paketlerini wireshark ile görüntülemiş olduk.

Not: Kayıtlardaki source ve destination'lar ilk bakışta anlamlı gözükme de

	Source	Destination	Protocol
I.Kayıt	CompalIn 9a:87:7e	Broadcast	ARP
II.Kayıt	Hewlett c2:96:cd	CompalIn 9a:87:7e	ARP

aslında onla birer mac adresidirler. Mac adreslerinin ilk haneleri ağ kart donanımının üretici firma kimlik numarası olduğundan wireshark mac adreslerinin en başına üretici firma adını, geri kalan kısmını ise direk düz bir şekilde vermiştir. İlk kayıta kendi mac adresimizden broadcast yapıldığı, ikinci kayıta ise hedef mac adresinden kendi mac adresimize yanıt döndüğü görülmektedir.

3)

Scapy ile Tüm Network'e ARP Ping Yapma

```
> sudo su
> scapy
>>> sendp(Ether(src="70:5a:b6:9a:87:7e",dst="ff:ff:ff:ff:ff:ff")/ARP(pdst="172.16.3.134/24"))
```

^
|
Kendi Mac Adresim

(Tubitak Laptop)

^
|
Sorgulanan IP
Bloğu

(Tubitak Network)

Broadcast yaparak network'teki tüm ip'lerin mac adreslerini öğrenme sorgusu yollarız.

Wireshark ile Görüntüleme

Filter : arp

Output:

No.	Time	Source	Destination	Protocol	Length	Info
35398	2414.1078150	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.141? Tell 172.16.3.113
35399	2414.1081120	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.142? Tell 172.16.3.113
35400	2414.1084090	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.143? Tell 172.16.3.113
35401	2414.1088090	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.144? Tell 172.16.3.113
35402	2414.1093420	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.145? Tell 172.16.3.113
35403	2414.1096930	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.146? Tell 172.16.3.113
35404	2414.1099970	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.147? Tell 172.16.3.113
35405	2414.1102990	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.148? Tell 172.16.3.113
35407	2414.1106550	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.149? Tell 172.16.3.113
35408	2414.1109690	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.150? Tell 172.16.3.113
35409	2414.1112840	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.151? Tell 172.16.3.113
35410	2414.1115970	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.152? Tell 172.16.3.113
35411	2414.1119380	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.153? Tell 172.16.3.113
35412	2414.1122480	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.154? Tell 172.16.3.113
35413	2414.1125590	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.155? Tell 172.16.3.113
35414	2414.1128700	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.156? Tell 172.16.3.113
35415	2414.1131730	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.157? Tell 172.16.3.113
35416	2414.1134830	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.158? Tell 172.16.3.113
35417	2414.1137950	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.159? Tell 172.16.3.113
35418	2414.1141080	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.160? Tell 172.16.3.113
35419	2414.1144220	CompalIn_9a:87:7e	Broadcast	ARP	42	Who has 172.16.3.161? Tell 172.16.3.113

Frame 3830: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Vmware_63:5b:4b (00:0c:29:63:5b:4b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff 00 0c 29 63 5b 4b 08 06 00 01 ..... }c[K....
0010 00 00 06 04 00 01 00 0c 29 63 5b 4b a9 fe 7c d5 ..... }c[K...].
0020 00 00 00 00 00 00 ac 10 03 01 00 00 00 00 00 .....
0030 00 00 00 00 00 00 00 00 00 00 00 ..... .....
```

eth0: <live capture in progress> ... Packets: 35676 - Displayed: 1575 (4,4%)

Kayıtların Info sütunundan görülebileceği üzere sırayla tüm IP'lerin mac adresleri sorulmaktadır ve 172.16.3.113'e (yani bize) cevabı döndür denmektedir.

Arp ping esnasında arada taranan makinelerden ayakta olanlar benim Mac'im bu şekilde paket yollayacaktır. İşte onlardan bazıları aşağıdaki kayıtlarda görülmektedir.

The screenshot shows a Wireshark network traffic capture. The filter is set to 'arp'. The main pane displays a list of ARP packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are numbered from 35660 to 35827. The Info column shows details such as 'Who has 172.16.3.1? Tell 172.16.3.113' or '172.16.3.1 is at 00:17:a4:b5:a9:00'. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
35660	2442.5596536	CompalIn_9a:87:7e	Hewlett-_b5:a9:00	ARP	42	Who has 172.16.3.1? Tell 172.16.3.113
35661	2442.5616366	Hewlett-_b5:a9:00	CompalIn_9a:87:7e	ARP	60	172.16.3.1 is at 00:17:a4:b5:a9:00
35663	2443.2004686	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35666	2443.7152536	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35669	2444.7136306	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35685	2449.5666366	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35686	2450.2047016	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35687	2450.3339436	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.58
35688	2451.2032386	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35690	2453.6056036	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35691	2454.2140736	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35727	2455.2124746	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35730	2455.3092936	AsustekC_81:90:ea	Broadcast	ARP	60	Who has 172.16.3.75? Tell 172.16.3.56
35752	2457.6149836	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35754	2458.2076066	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35755	2459.2059456	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213
35758	2460.4015086	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.58
35771	2465.1036376	CompalIn_9a:87:7e	Hewlett-_b5:a9:00	ARP	42	Who has 172.16.3.1? Tell 172.16.3.113
35772	2465.1047696	Hewlett-_b5:a9:00	CompalIn_9a:87:7e	ARP	60	172.16.3.1 is at 00:17:a4:b5:a9:00
35781	2470.4774576	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.58
35796	2480.5336186	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.58
35811	2487.6156586	CompalIn_9a:87:7e	Hewlett-_b5:a9:00	ARP	42	Who has 172.16.3.1? Tell 172.16.3.113
35812	2487.6169376	Hewlett-_b5:a9:00	CompalIn_9a:87:7e	ARP	60	172.16.3.1 is at 00:17:a4:b5:a9:00
35821	2490.5330586	Vmware_69:74:fe	Broadcast	ARP	60	Who has 172.16.3.1? Tell 172.16.3.58
35827	2493.0273446	Vmware_63:5b:4b	Broadcast	ARP	60	Who has 172.16.3.1? Tell 169.254.124.213

```
0000  ff ff ff ff ff 00 0c 29 63 5b 4b 08 06 00 01  ..... )c[K....
0010  08 00 06 04 00 01 00 0c 29 63 5b 4b a9 fe 7c d5  ..... )c[K..].
0020  00 00 00 00 00 00 ac 10 03 01 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00  .....
eth0: <live capture in progress> ...  Packets: 36237 · Displayed: 1651 (4,6%)  Profile: Default
```

Kayıtlardan görülebileceği üzere bazı arp request'lerin hemen altına arp responlar gelmiştir. Arp response'ların Info sütunlarına bakacak olursak sorgulanan IP'nin şu şu Mac adresi üzerinde olduğu bilgilendirmeleri mevcuttur.

4)

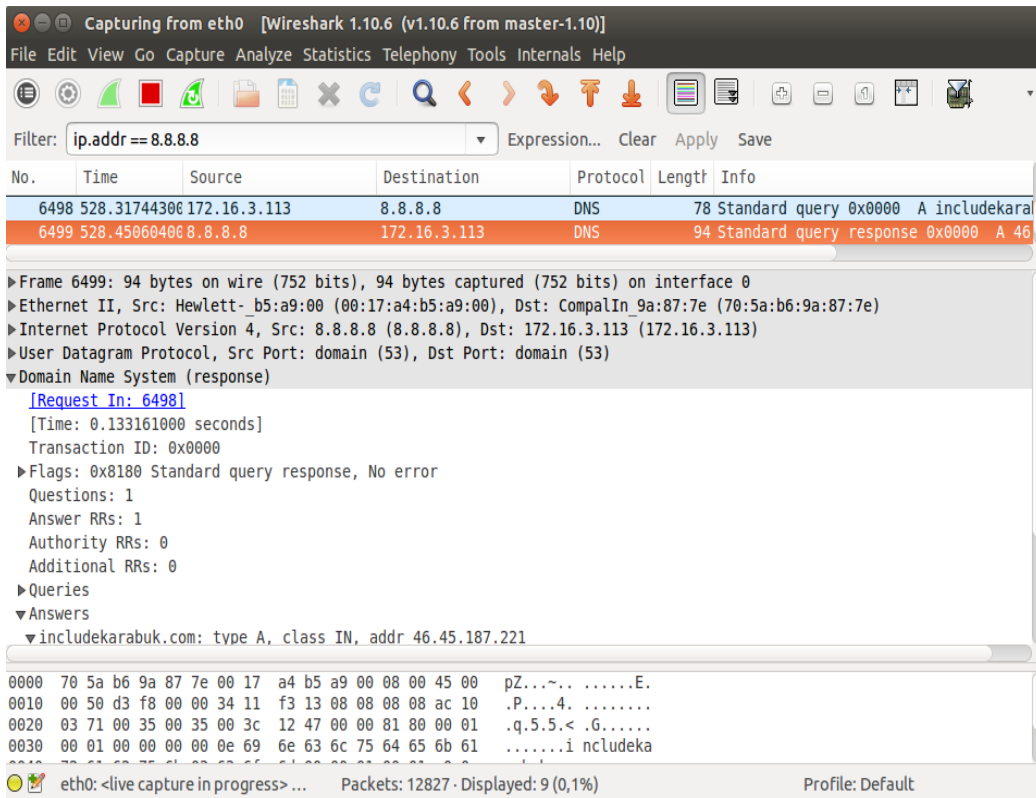
Scapy ile DNS Sorgusu Yapma

```
> sudo su
> scapy
>>> sr1(IP(dst="8.8.8.8")/UDP()/DNS(rd=1,qd=DNSQR(qname="includekarabuk.com",qtype="A")))
```

Wireshark ile Görüntüleme

Filter : ip.addr == 8.8.8.8

Output:



Kayıtlara baktığımızda görebileceğimiz üzere önce gönderdiğimiz DNS sorgusu ekrana düşmüştür. Ardından dns sunucudan gelen yanıt ekrana düşmüştür. DNS sunucudan gelen yanıt paketinin detaylarına baktığımızda ise Answer sekmesi altında sorduğumuz includekarabuk.com sitesinin ip'sinin geldiğini görmekteyiz. Böylece scapy ile bir dns sorgusu oluşturduk ve yanıtını alabildik.

Bazı Notlar

srp : Layer 2 paket gönderme fonksiyonu (send and receive)
sr : Layer 3 paket gönderme fonksiyonu (send and receive)

Kaynaklar

Tubitak YTE Eğitimleri Mayıs, 2017 (Defter notları)

<http://www.secdev.org/projects/scapy/doc/usage.html>