Scapy - Wireshark Kullanımı

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

1)

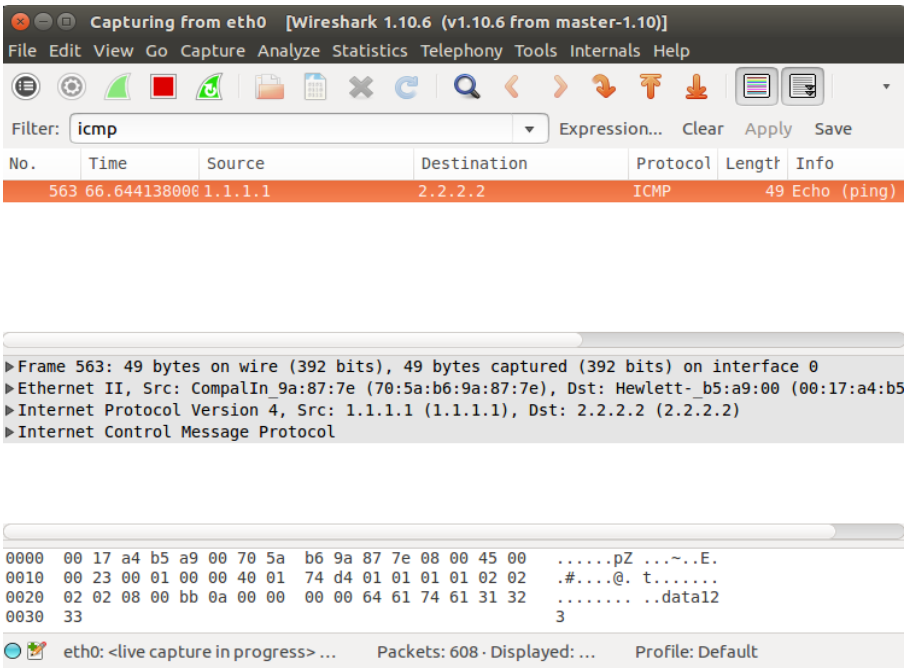
Scapy ile ICMP Paket Oluşturma

```
> 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)

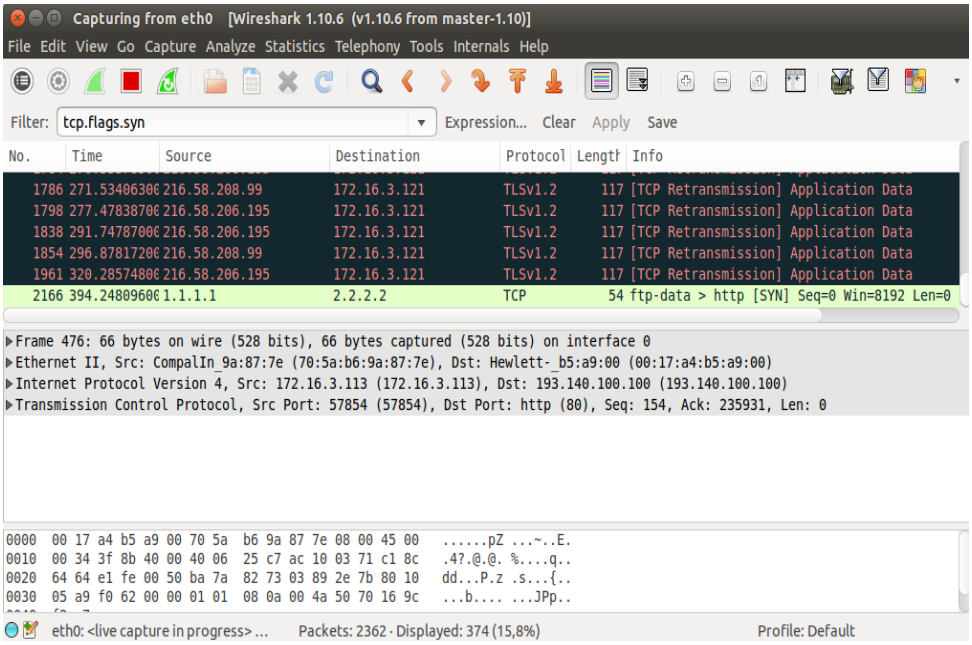
Scapy ile SYN Paketi Yollama

```
> 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:



Görüldüğü üzere scapy ile oluşturduğumuz SYN paketi ekrana düşmüştür.

3)

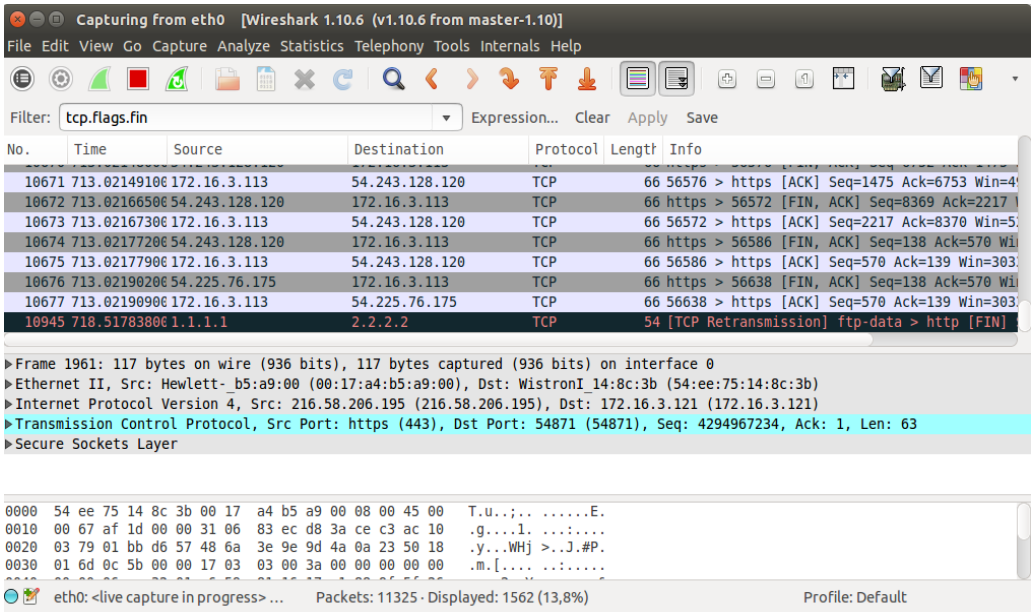
Scapy ile FIN Paketi Yollama

```
> 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:



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

4)

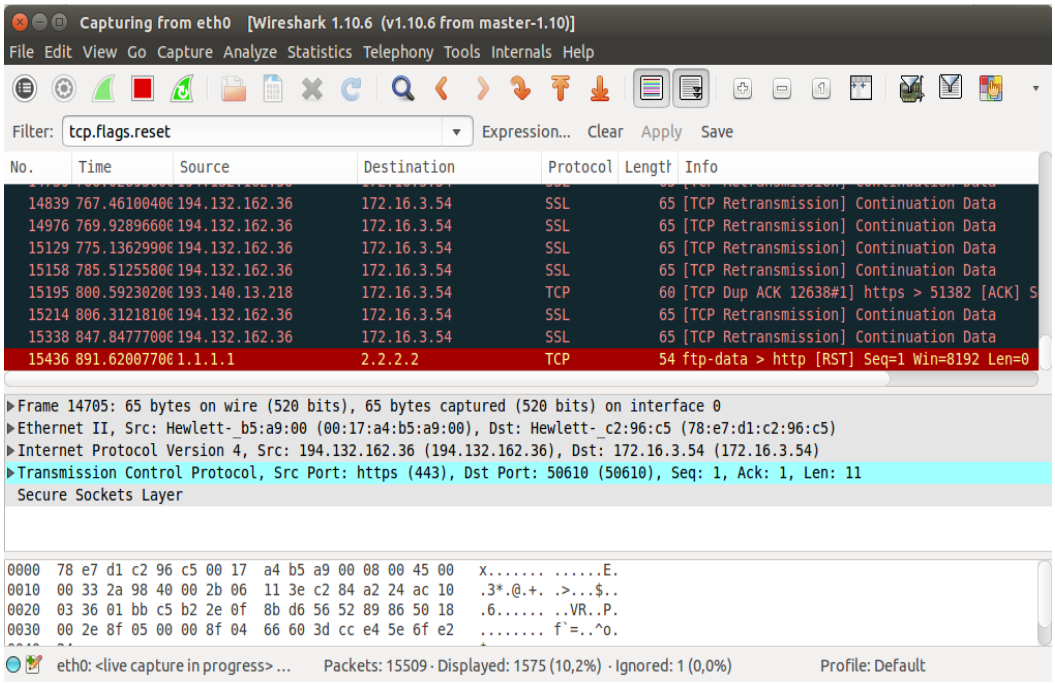
Scapy ile Reset Paketi Yollama

```
> 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:



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

5)

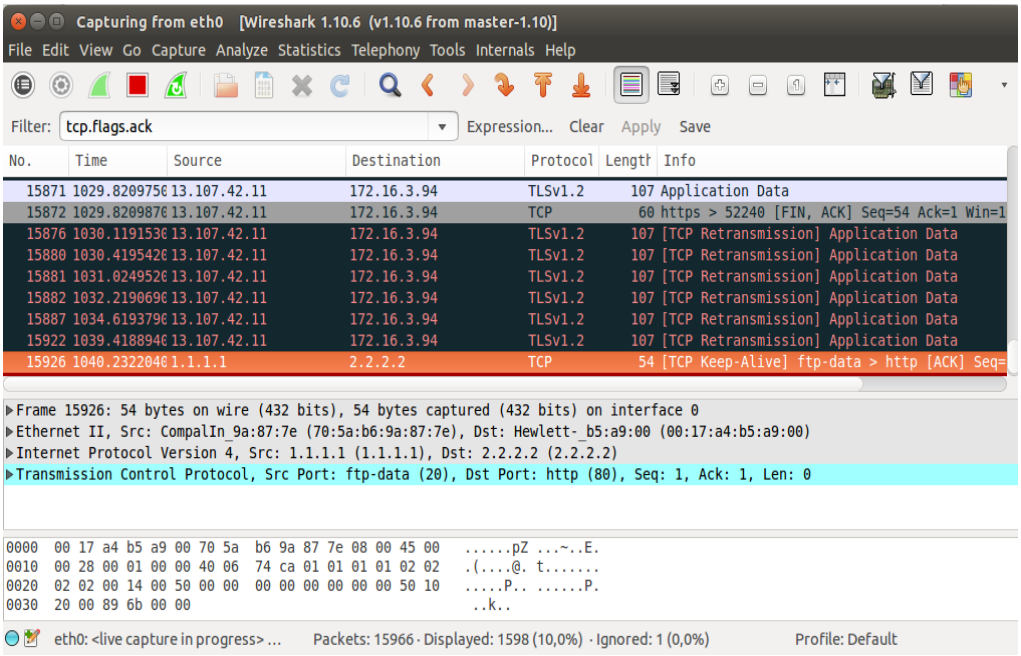
Scapy ile Ack Paketi Yollama

```
> 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:



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

6)

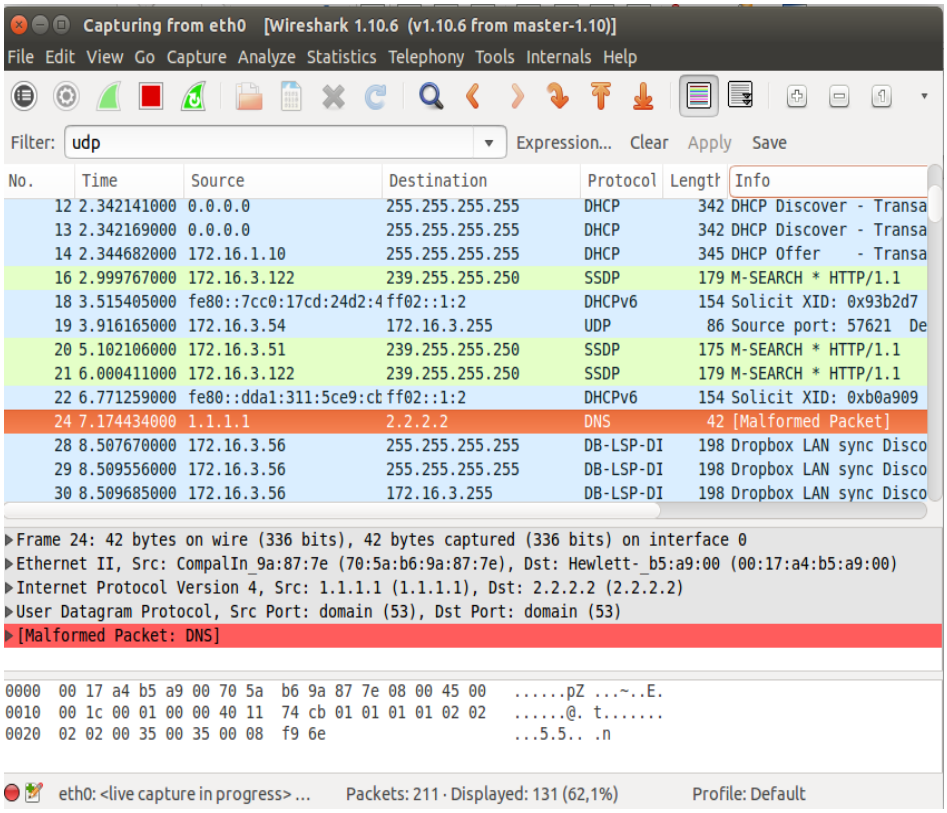
Scapy ile Udp Paketi Yollama

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

Wireshark ile Yakalama

Filter : udp

Output:



Turuncu renkle gösterilen kayıttan görebileceği üzere UDP paketimiz ekrana düşmüştür.

7)

Scapy ile Arp Paketi Yollama

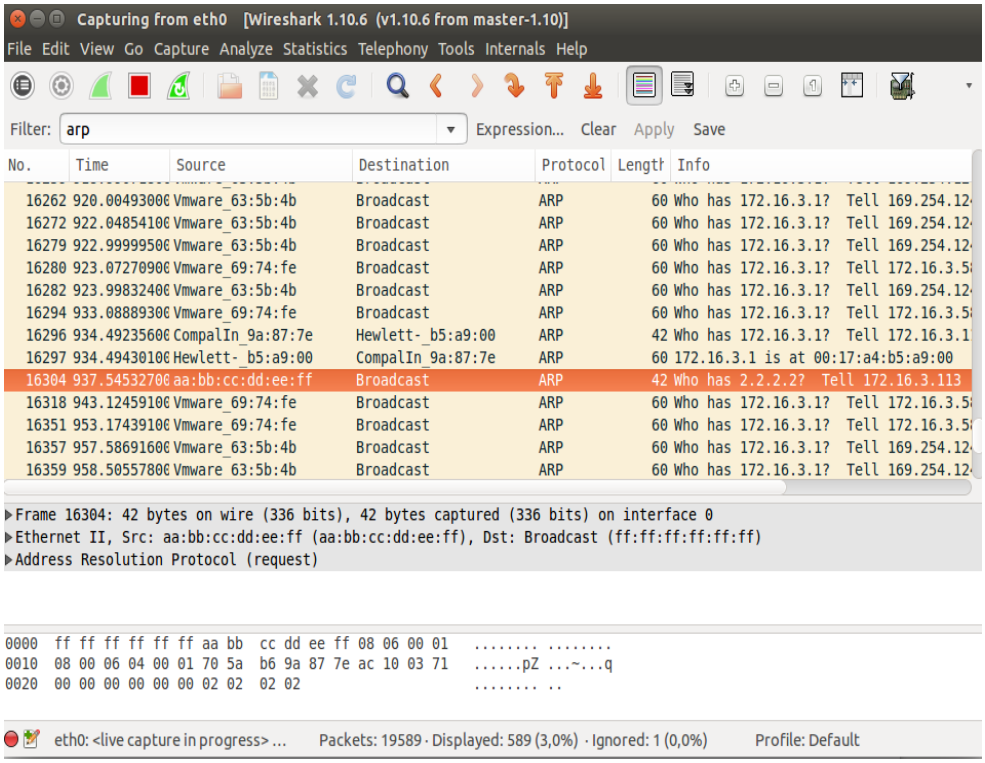
```
> sudo su
> scapy
>>> sendp(Ether(src="aa:bb:cc:dd:ee:ff",dst="ff:ff:ff:ff:ff:ff")/ARP(pdst="2.2.2.2"))
```

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:



Turuncu renkle gösterilen kayıttan görülebileceği üzere ARP sorgumuz ekrana düşmüştür.

Ekstra

1)

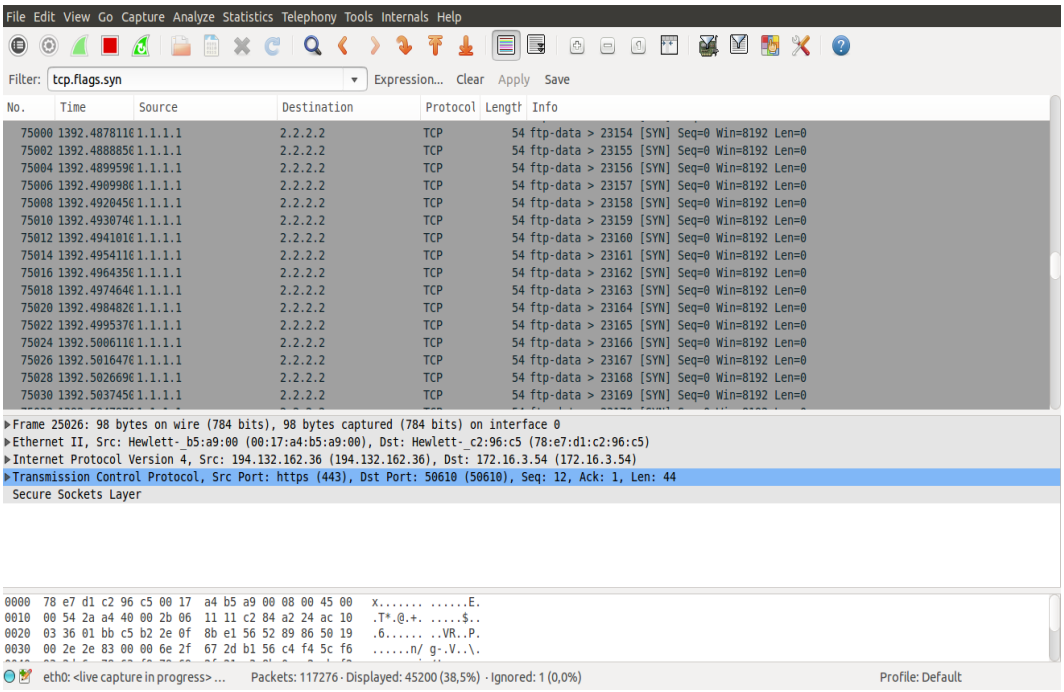
Scapy ile Syn Taraması Yapma

```
> 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:



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"))
```

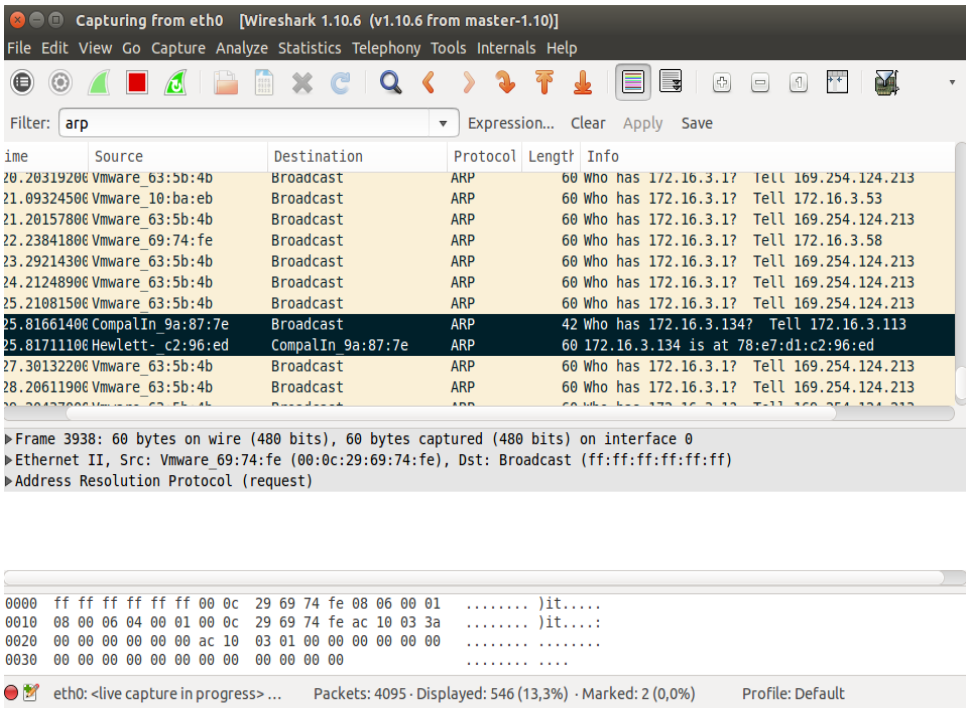
^	^
|	|
Kendi Mac Adresim	Sorgulanan IP
(Tubitak Laptop)	(Tubitak Masaüstü)

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:



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 kayıtta 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 gözükmese 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 kayıtta kendi mac adresimizden broadcast yapıldığı, ikinci kayıtta 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"))
```

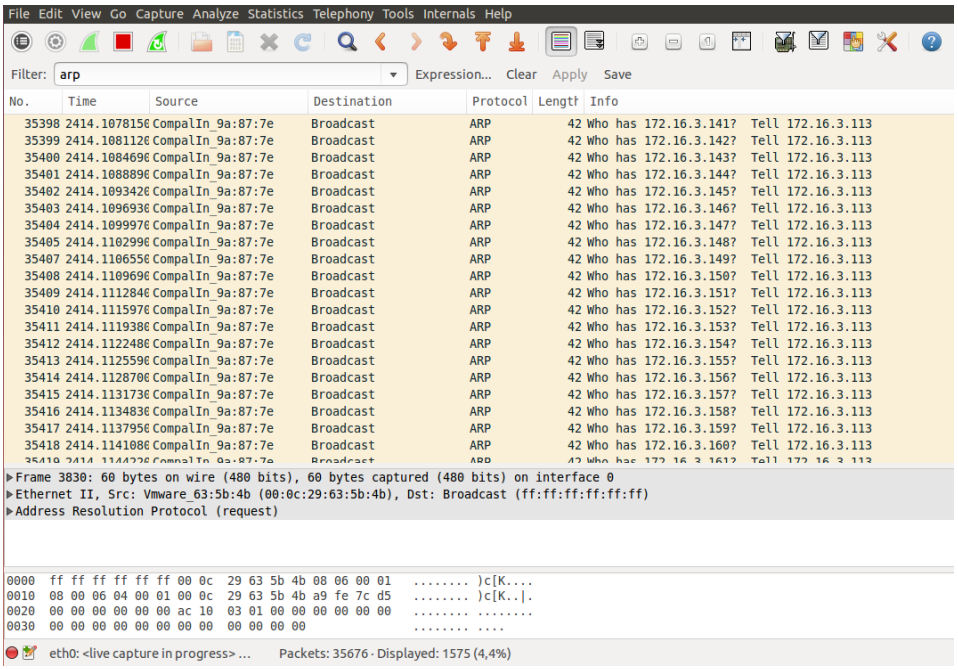
^	^
|	|
Kendi Mac Adresim	Sorgulanan IP Bloğu
(Tubitak Laptop)	(Tubitak Network)

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

Wireshark ile Görüntüleme

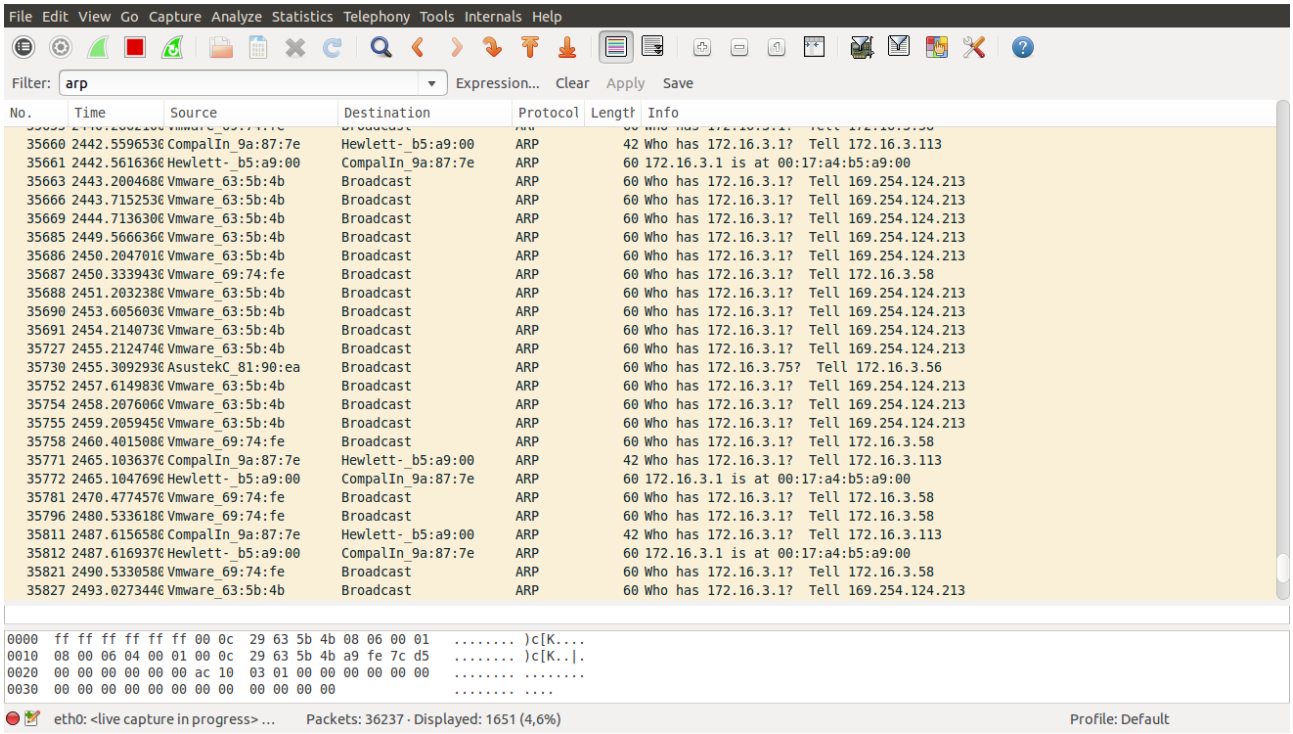
Filter : arp

Output:



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 şeklinde paket yollayacaktırlar. İşte onlardan bazıları aşağıdaki kayıtlarda görülmektedir.



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)

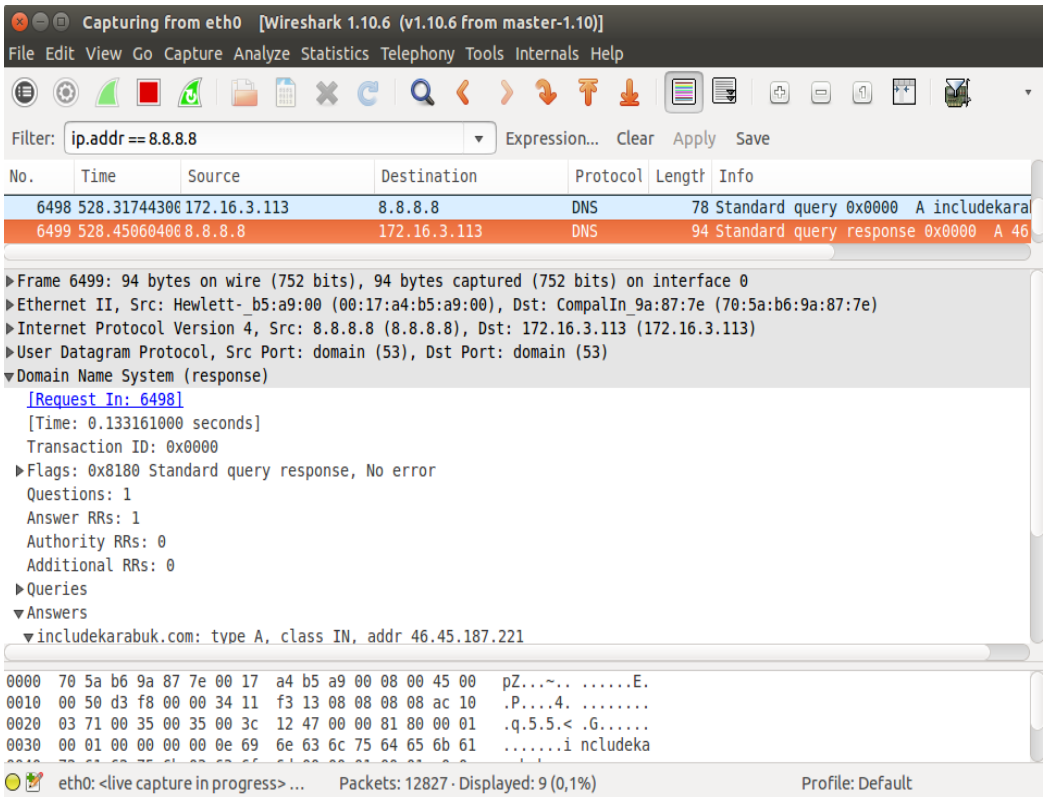
Scapy ile DNS Sorgusu Yapma

```
> 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