

**Wireshark Kullanım**

**Rehberi**

**Önemli İpuçları**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mustafa Ensar Sadıkoğlu 23370031017** | **Ahmet Melik İnce 23370031063** | **Tolga Turgut 23370031002** | **Alperen Kurt 23370031060** | **Süleyman Toytoy 22370031072** | **Cenker Bardakçı 22370031048** |

* Wireshark hakkında
* Wireshark kurulumu
* Wireshark aracını tanıma aşaması
* Paket yakalama işlemi
* Filtreler
* Mantıksal operatörler
* Özel filtre oluşturmak

İçindekiler

* Wireshark Adres Çözümleme Özelliği
* Wireshark ile Kolon Oluşturma
* Wireshark İstatistik Özelliği
* Wireshark ile Trafik İçerisindeki Dosyaları Export Etmek
* Wireshark ile pcap formatındaki dosyaları birleştirmek

**Wireshark, kurulu olduğu bilgisayarda;**

* Ağ trafiğinin anlık olarak izlenmesini • İzlenen bu trafiğin kayıt edilmesini
* Daha sonra incelenmesini sağlamaktadır.

# • Bunların dışında bir hatayı çözmek amacı ile de kullanılabilmektedir. (Bu işlem trafik izlenerek anlık filtreleme çözümleri kullanılarak sorun saptanmaya çalışılır.)

**Wireshark aracının en önemli özellikleri:**

* Kullanıcı Dostu
* Ücretsiz kullanılabilmesi
* Geniş protokol desteği
* Desteklenen protokolleri görebilmek için bu bağlantıyı takip edebilirsiniz.

## • https://wiki.wireshark.org/ProtocolReference

* Çoklu işletim sistemi desteği sağlaması:
* Windows
* Linux
* MacOS
* Bir çok kritere göre paket filtreleme desteği
* Yakalanan paketlerin çeşitli formatlarda kayıt edilebilmesi
* Çeşitli istatistikler oluşturabilmesi
* Anlık olarak paket yakalayıp görüntüleyebilme gibi çok fazla dikkat çeken özelliği bulunmaktadır.

**Kullanım Alanları**

**Wireshark aracının kullanım alanları:**

# • Protokol hatalarını çözümlemek • Paket analiz işlemleri • Ağ içerisinde ki hataları tespit etmek • Ağ hakkında ki istatistikleri görüntüleyebilmek • Canlı olarak veya elinizde bulunan pcap gibi formatlarda olan verileri görüntülemek

• Tersine mühendislik çalışmaları gibi bir çok farklı konuda tercih edilen bir araçtır.

**Wireshark aracı için en düşük sistem gereksinimleri:**

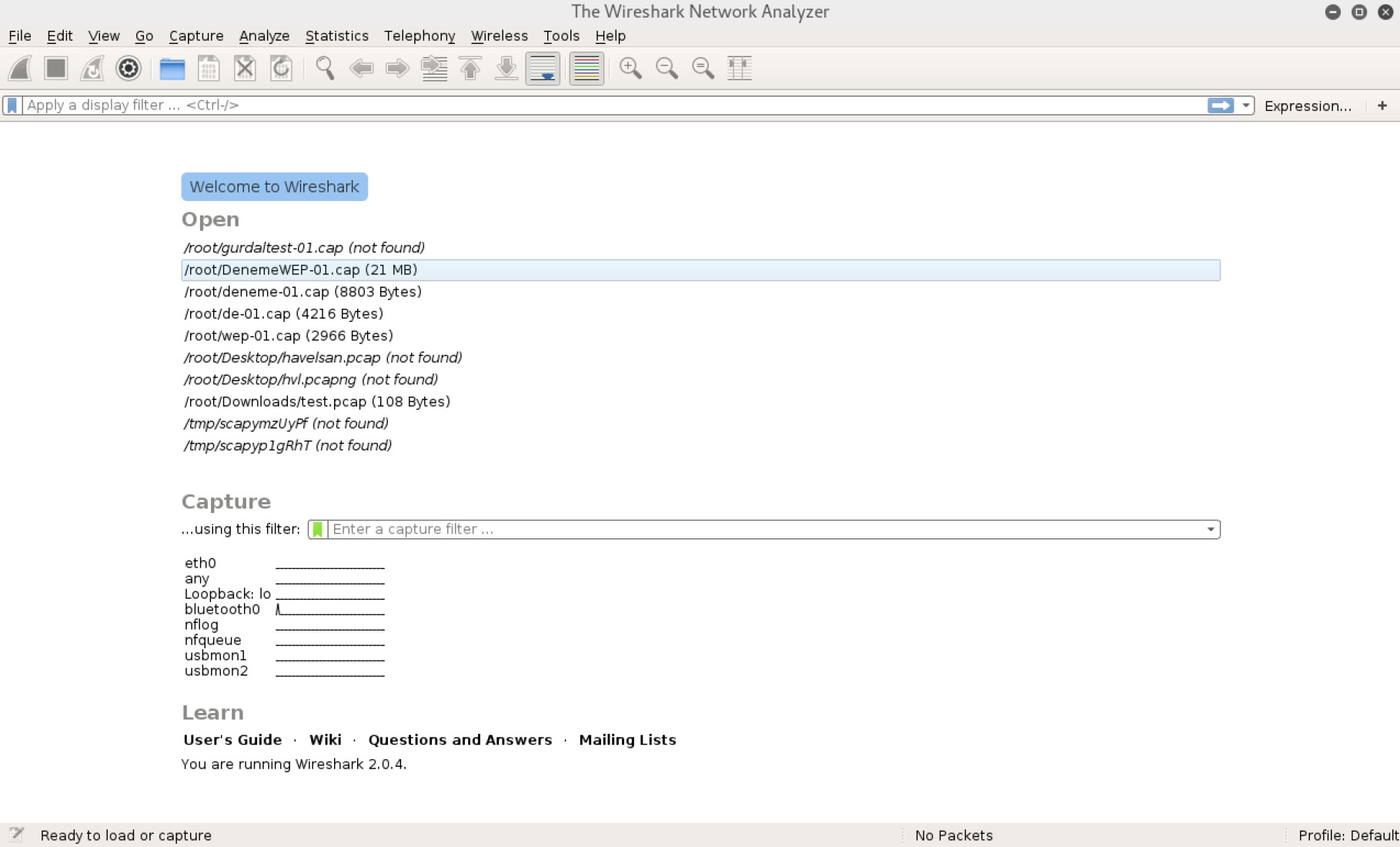
* Bu aracı bilgisayarınızda sağlıklı bir şekilde çalıştırabilmeniz için aşağıda belirtilen sistem gereksinimlerini karşılıyor olmanız gerekmektedir :
* 400 Mhz işlemci
* 60 MB boş alan
* Promiscuous mode destekli bir ağ kartı
* WinPcap driver

**Wireshark aracı için asıl işi yapan kısım:**

* Anlık ağ trafiğinin yakalayıp wireshark aracına gönderen kısımdır.
* Wireshark aracı da kullanıcı dostu arayüzü sayesinde sizlerin bu ağ trafiğini (paket akışını) görmenizi sağlamaktadır.

**Wireshark aracı için kurulum adımları:**

* İndirme adresi :
* <https://www.wireshark.org/download.html>
* **Linux** tabanlı sistemlerde kurulum:
* **DEB-based sistemler**
* apt-get install wireshark
* **RPM-based sistemler**
* rpm –ivh wireshark\*.rpm
* **Windows** sistemlerde kurulum
* Gerekli dosya indirildikten sonra kurulum yönergeleri sayesinde kurulabilir.**Tanıyalım**



**1**

**2**

**3**

**4**

**5**

**6**

**Filter kısmı**

**7**

**1**

**)**

Daha önce açılan dosyalar gösterilmektedir.

**2)**

Ağ trafiğini izlemek amacı ile

kullanılabilecek ağ kartları gösterilmektedir

**3**

**)**

Ağ trafiğini izlemek amacı ile

kullanılabilecek ağ kartları için paket

yakalamaya başladığında kullanabileceği filtre

tanımlanabilmektedir.

**4**

**)**

Sık sık kullanılabilecek işlemlerin kısayol

atamalarının bulunduğu yerdir.

**5**

**)**

Ana menün bulunduğu kısımdır. Bu bölümü

daha yakından inceleyeceğiz.

**6)**

Ağ trafiği için filtremele kullanabileceğiniz

çok özel bir kısımdır.

**7**

**)**

Wireshark hakkında daha fazla bilgi

edinmek ve manuel dosyalarına erişmek amacı

ile kullanılabilecek bir bölümdür. Bu bölüme 5

numara ile tanımlanan ana menüde

**Help**

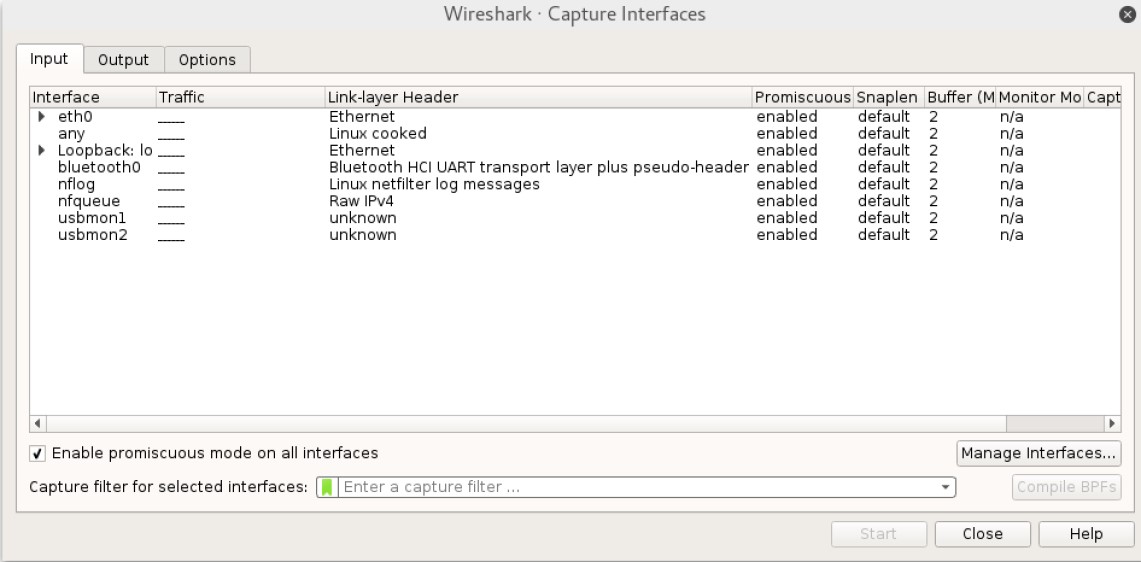
kısmından erişebilirsiniz.

**Wireshark İle Paket Yakalama**

## Wireshark aracı ile paket yakalama işlemi

Bu işlem için iki seçeneğiniz bulunmaktadır. Ama unutmamamız gereken şey, Wireshark aracını **root (en yetkili)** kişi hakları ile çalıştırmaktır. Bunun sebebi, wireshark aracının bizim ağ kartlarımıza erişmek istemesidir.

1. **)** Ana menüden Capture -> Options yolunu takip ederek aşağıdaki menüye erişmek



1. **)** Bu seçenekte ise programın ilk açılışında sizi karşılayan ekranda daha önceki slaytta 2 numara ile ifade edilen bölümden dilediğiniz ağ kartının üzerine tıklamaktır.

**Paket Yakalama Arayüzü**

**Wireshark**

**İle Paket Yakalama**

**–**

**Ağ Kartları**

**Ağ Kartları**

UNIX/Linux

**MacOS**

Ağ kartı

isimleri üretici

tarafından sağlanır.

**“lo0”**

virtual

loopback

interface

“lo0”

loopback

Interface

en0, en1

Ethernet

or

Airport

Interfaces

**Windows**

**Linux**

wlan0, wlan1,..

Wireless LAN

eth0, eth1

Ethernet

Interface

ifconfig

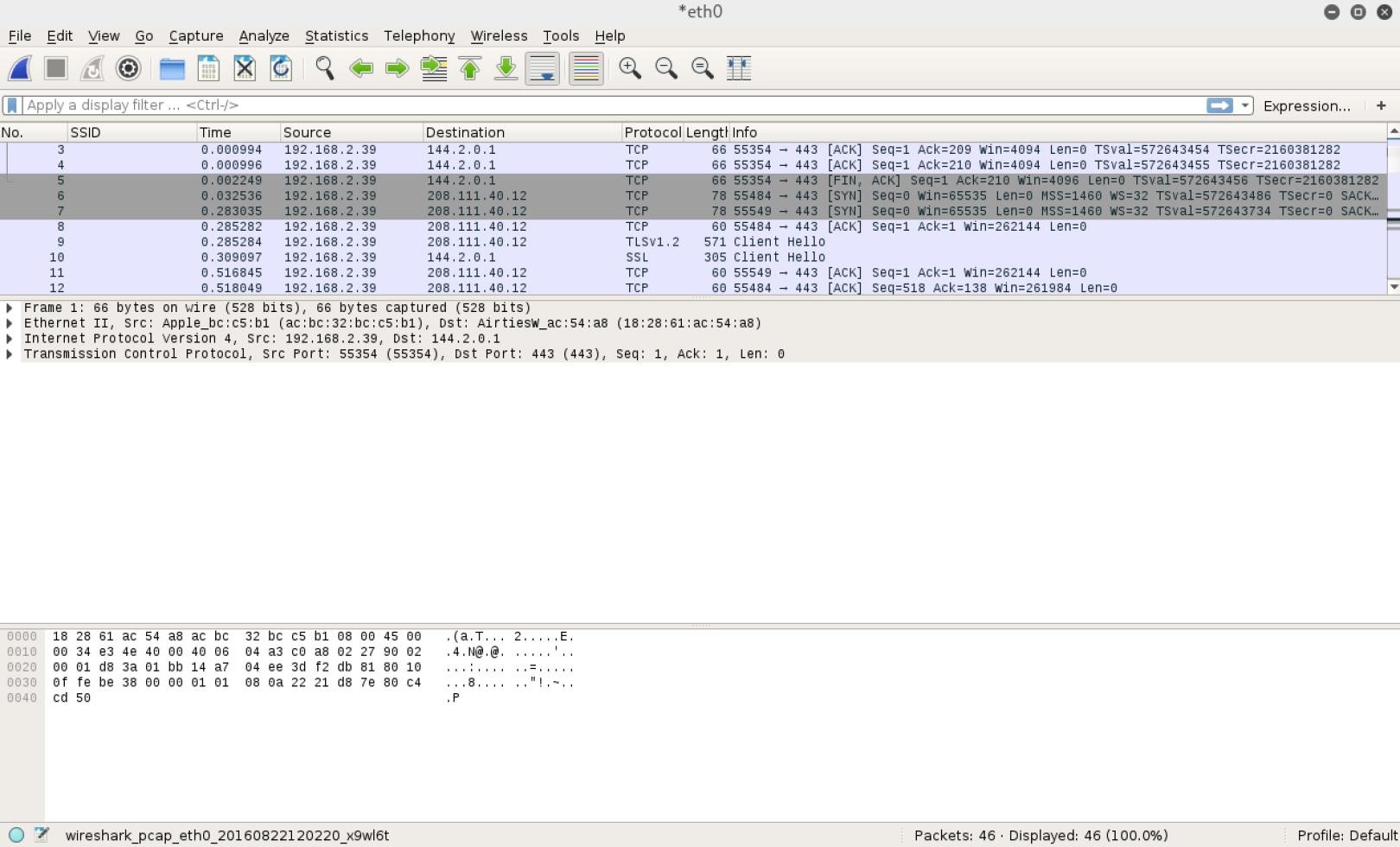
ipconfig

/

all

## Wireshark aracı ile paket yakalama işleminde ki ara yüzü tanıyalım

Paket yakalama işlemi başladığında katmanlar halinde bir ara yüz bizi karşılayacaktır.



**1**

**2**

**3**

**4**

**5**

**1 )** Yakalanan paketler ile ilgili filtreleme seçeneklerinin bulunduğu kısımdır.

**2)** Yakalanan paketlerin listelendiği kısımdır.

**3 )** Yakalanan paketlerden birini seçtiğimiz zaman onunla ilgili detayın görüntülendiği kısımdır.

1. Seçilen paket için hex dump halini gösterir.
2. Genel bilgilendirmelerin yer aldığı kısımdır. Bu kısımda : • Yakalanan toplam paket

• Görüntülenen paket sayısı • Profil ismi gibi bilgiler yer almaktadır.

Başlıyoruz

Paket

yakalamak

istiyor

musun ?

DUR

Wi

-

Fi ağ

kartınımı

kullanmak

istiyorsun ?

Wireshark

kuralım

Yetkili bir

kullanıcı ile

Wireshark

aracını açalım

Kullanılabilir ve

desteklenen ağ

kartlarından bir

tane seçelim

O zaman

monitor mode

durumuna

alalım

Artık Wireshark

aracının

özelliklerinikullanıp

analiz işlemi yapabiliriz.

Yakalama

işlemini

başlatalım

**E**

**H**

**E**

**H**

Evet

-

>

**E**

Hayır

-

>

**H**

**Wireshark- Kullanışlı Filtreler**

DHCP İçin Kullanılabilecek HTTP İçin Kullanılabilecek

Filtreler Filtreler

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | • | port 67 or port 68 | | • | bootp | | • | bootp.option.dhcp == 1 (DISCOVER Packets) | | • | bootp.option.dhcp == 2 (OFFER Packets) | | • | bootp.option.dhcp == 3 (REQUEST Packets) | | • | bootp.option.dhcp == 4 (ACK Packets) | | • | bootp.option.hostname | | |  |  | | --- | --- | | • | http | | • | http.request.method=="GET” | | • | http.request.method==”POST” | | • | http.response.code == “200” | | • | http.user\_agent == “User\_Agent\_Değeri” | | • | http.referer | |

ARP İçin Kullanılabilecek DNS İçin Kullanılabilecek

Filtreler Filtreler

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | • | arp | | • | arp.src.hw\_mac == “Kaynak mac adresi” | | • | arp.dst.hw\_mac == “Hedef mac adresi” | | • | arp.duplicate-address-frame | | • | arp.opcode == 1 | | • | arp.opcode == 2 | | |  |  | | --- | --- | | • | dns.qry.name == "google.com” | | • | “dns.qry.type == 1 (A Record Type)dns.qry.type ==  255 (ANY Record Type) | | • | dns.qry.type == 2 (NS name server)dns.qry.type == 15(MX mail exchange | | • | dns | |

14

### Wireshark- Kullanışlı Filtreler

İnternet Protokol İçin TCP İçin Kullanılabilecek

Kullanılabilecek Filtreler Filtreler

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | • | ip.addr | | • | ip.ttl | | • | ip.version == 4 | | • | ip.src == 192.168.2.45 | | • | ip.dst == 192.168.2.34 | | |  |  | | --- | --- | | • | tcp.flags.syn == 1 | | • | tcp.port == 80 | | • | tcp.dstport == 443 | | • | tcp.srcport == 80 | |

FTP İçin Kullanılabilecek ICMP İçin Kullanılabilecek

Filtreler Filtreler

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | • | ftp.request.command | | • | ftp.request | | • | ftp.request.command == "PASS” | | • | ftp.request.command == ”USER" | | • | ftp.response.arg == "Login successful." | | |  |  | | --- | --- | | • | icmp.type | | • | icmp.code | |

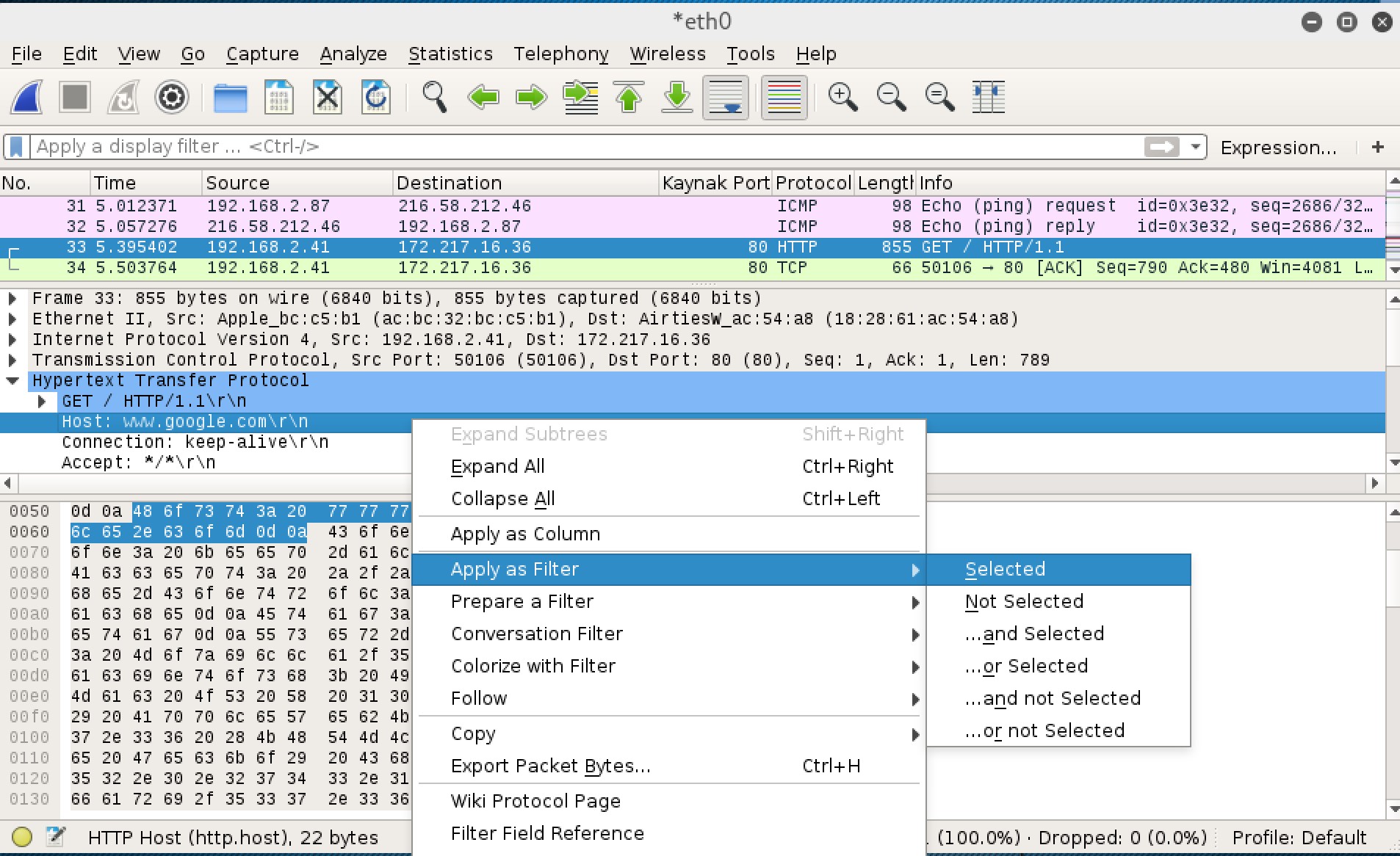
**Wireshark- Operatörler**

Karşılaştırma Operatörleri

Mantıksal Operatörler

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | • | eq == Eşittir | | • | ne != Eşit değidir | | • | gt > Büyüktür. | | • | lt < Küçüktür | | • | ge >= Büyük eşittir | | • | le <= Küçük eşittir. | | |  |  | | --- | --- | | • | and && = (ve anlamı katar) | | • | or || = (veya anlamı katar) | | • | xor ^^ | | • | not ! = (değil anlamı katar, dahil olmayan | |

**Filtrelerinizi Oluşturun**



Wireshark

kullanırken

standart

filtrelemeler

dışında

kendinize

ait

özel

filtreler

oluştumak

isterseniz,

wireshark

size

bu

özelliği

sunmaktadır

.

Bunu

yapabilmek

için

filtrelemek

istediğiniz

durumun

üzerine

sağ

tış

yapıp,

**“**

**Apply**

**as**

**Filter”**

demeniz

ve

çıkan

durumlardan

birini

kendinize

göre

seçmeniz

yeterli

olacaktır

.

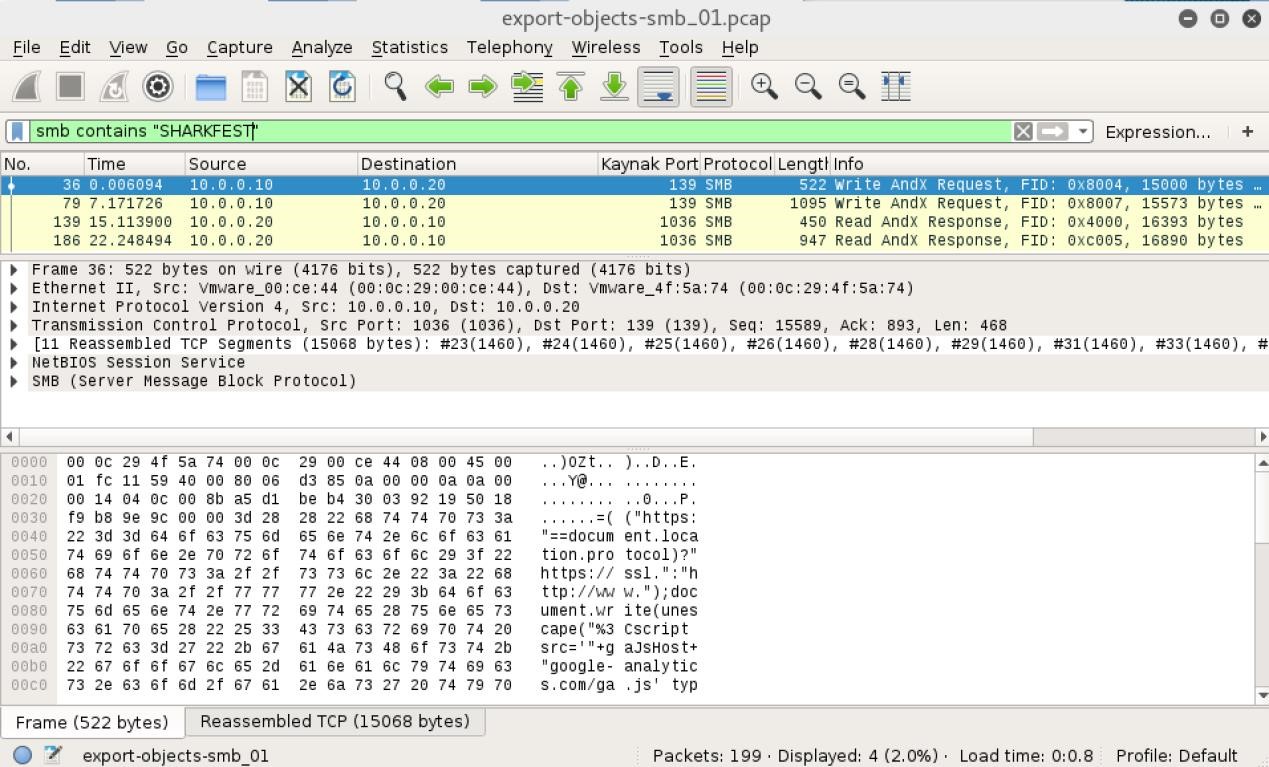
**Wireshark**

**–**

**Contains**

**İ**

**simli Filtre İle Arama İşlemi**



İstediğimiz

protokol

içerisinde

arama

yapabilmemizi

sağlayan

contains

filtresi

bize

çok

kolaylık

sağlamaktadır

.

Örneklerde

SMB

ve

HTTP

trafikleri

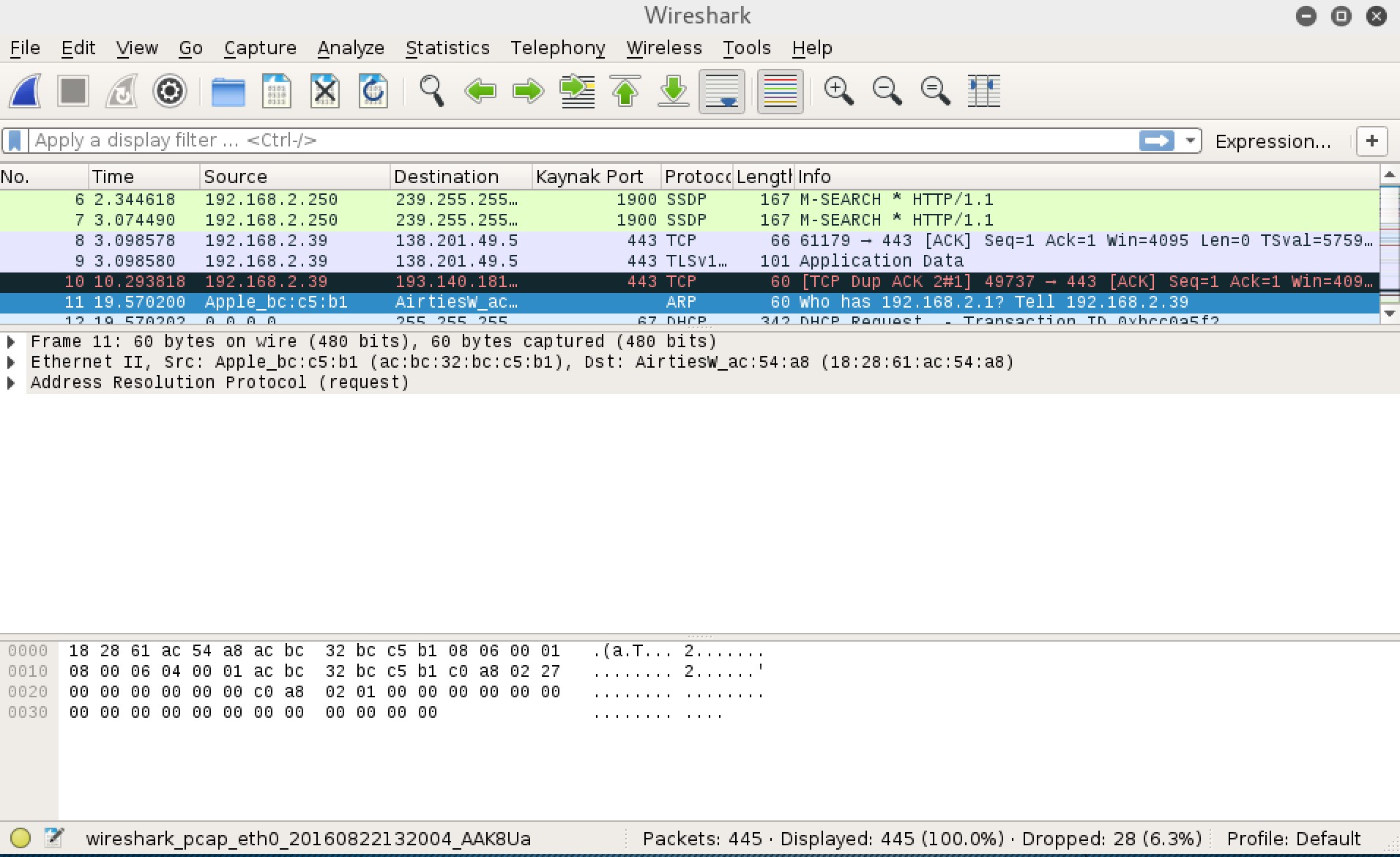
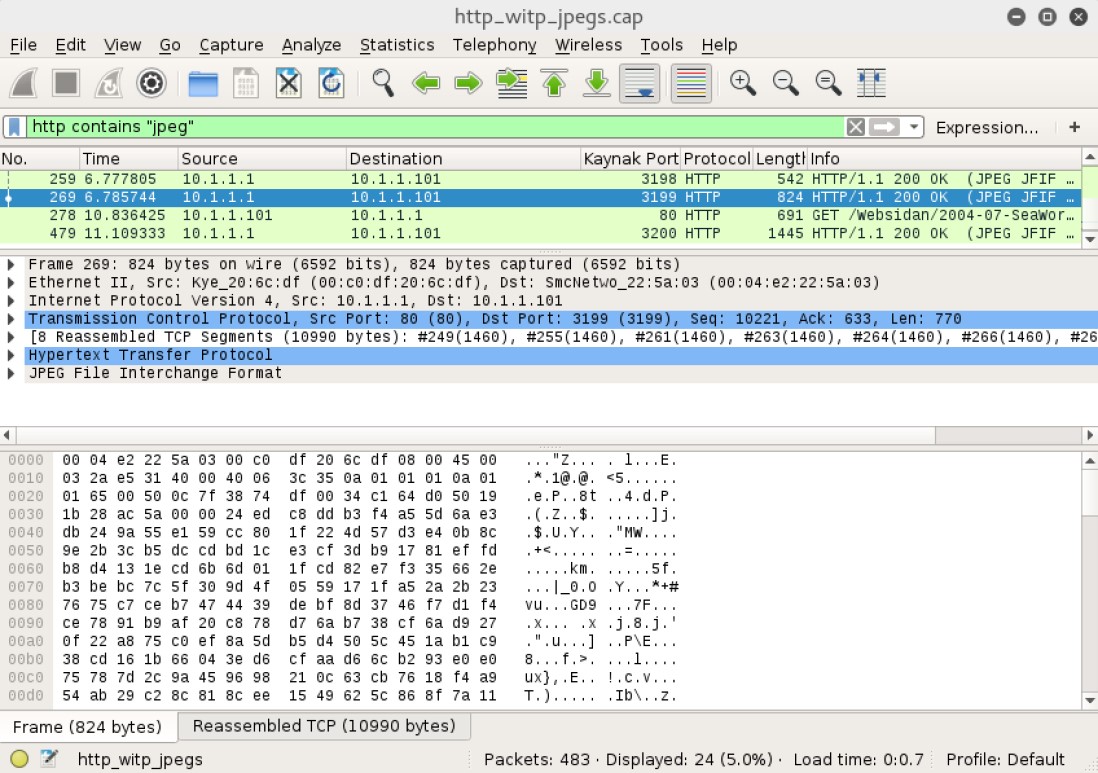
içerisinde

bazı

aramalar

yapılmıştır

.



Filtreleme

butonu

eklemek

için

ilk

olarak

**+**

butonuna

basıyoruz

.

Sürekli kullandığımız ve özellikle

uzun filtreler için filtreleme butonu

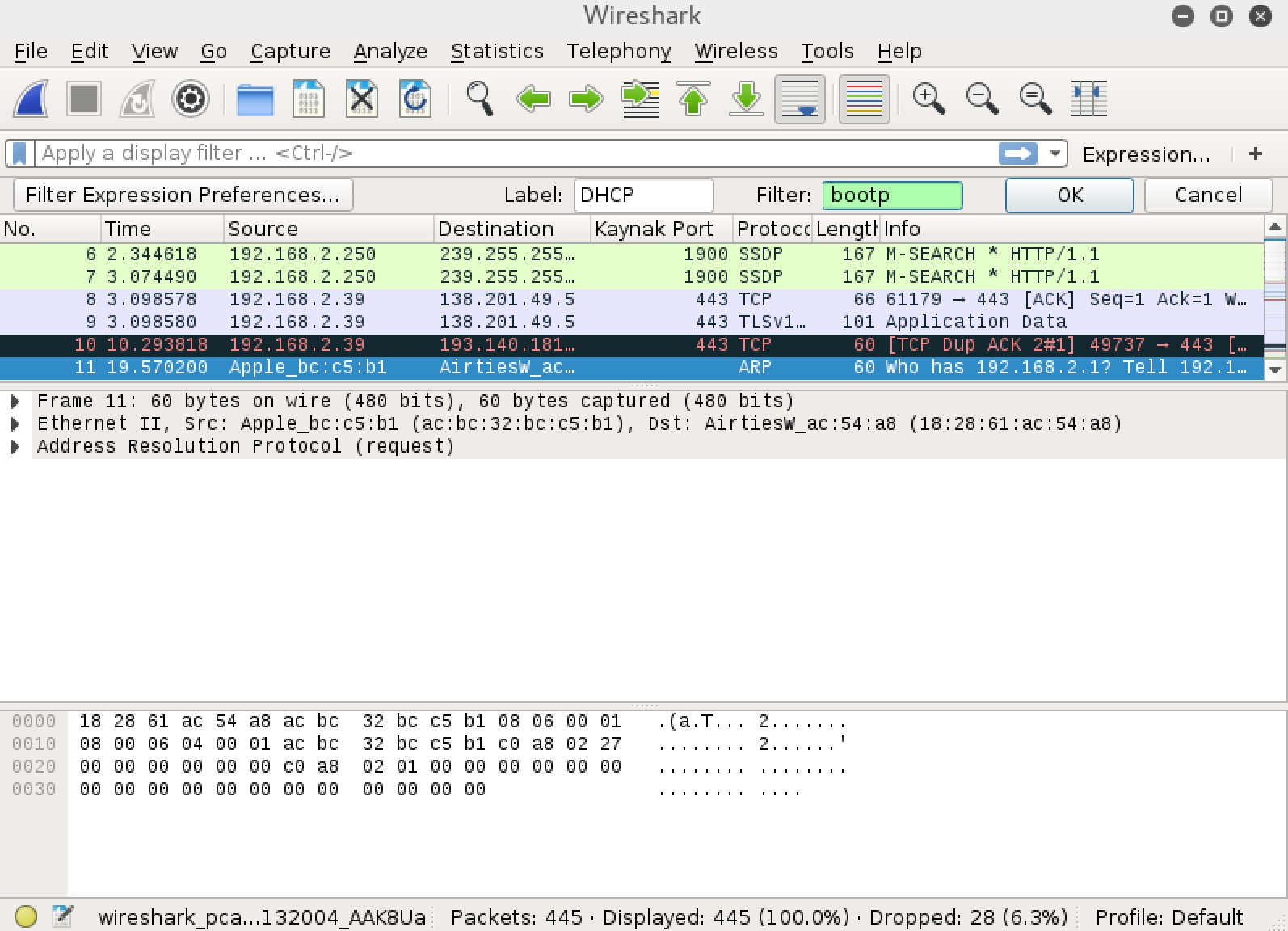
oluşturarak her seferinde bunu

yazma zahmetinden kurtularak

işimizi tek buton ile halledebiliriz.

NOT

açılmaktadır.



**+**

tuşuna

bastıktan

sonra

bu

menü

Açılan

menüde

filtrelemeler

için

kullanabileceğiniz

butonun

ismi

ve

filtreleme

seçeneğini

yazacağınız

bölümler

bulunmaktadır

.

Yapılan

işlemler

sonunda

görünüm

kutucuk

içine

alınan

kısım

gibi

olacaktır

.

Artık

**DHCP**

isminde

ve

**dhcp**

**paketlerini**

filtreleyen

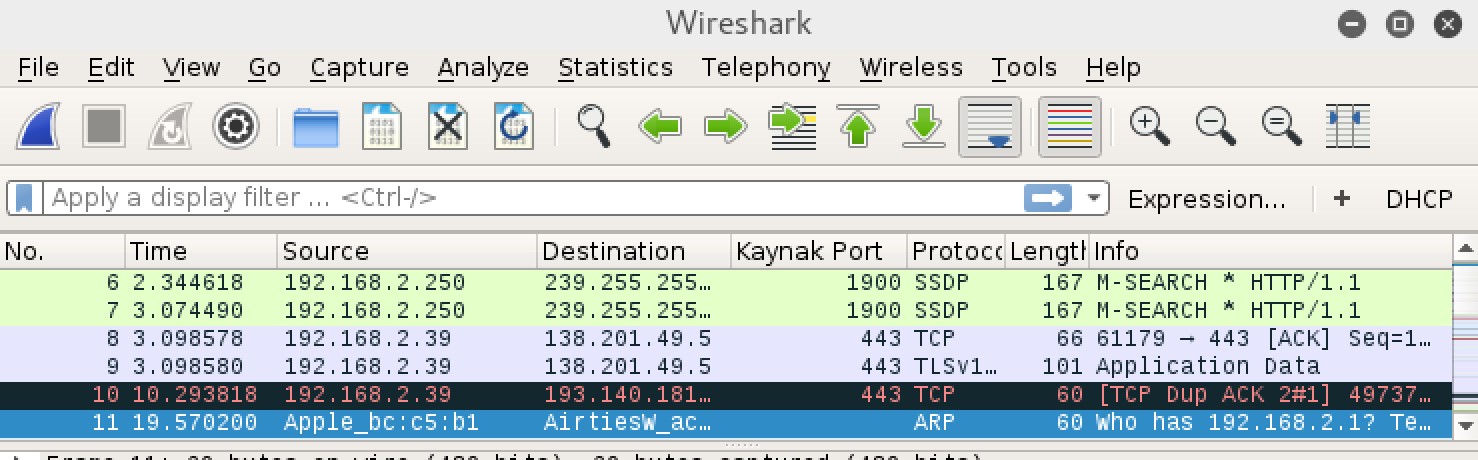
bir

**filtreleme**

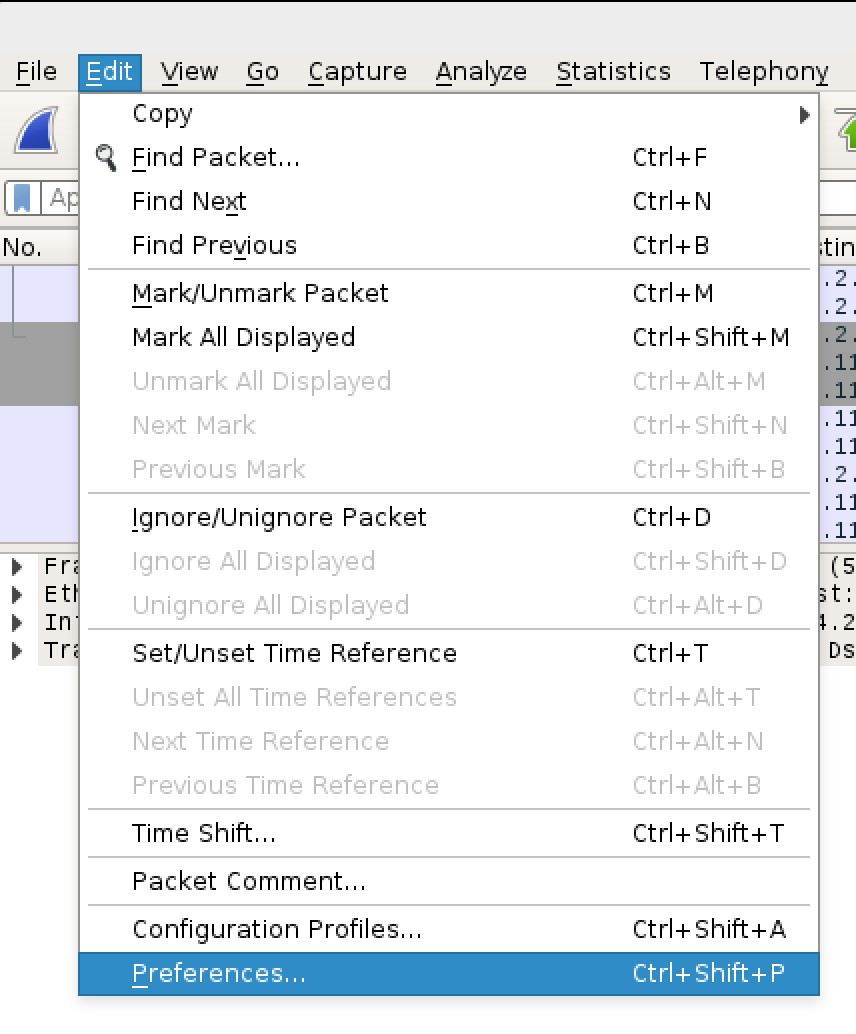
**butonumuz**

olmuştur

.



sağ tarafta bulunan pencerenin açılmasını sağlıyoruz. (Kısa yolu = **Ctrl + Shift + P**)



ilk olarak

**Edit**

**-**

**Prefences**

**>**

yolunu takip

**1**



Daha

sonra

kolon

kısmına

tıklanır

.

Daha

sonra

sağda

açılan

pencerede

işlem

yapılır

.

**2**

**(**

**-**

**)**

tuşuna

basılarak

eklenen

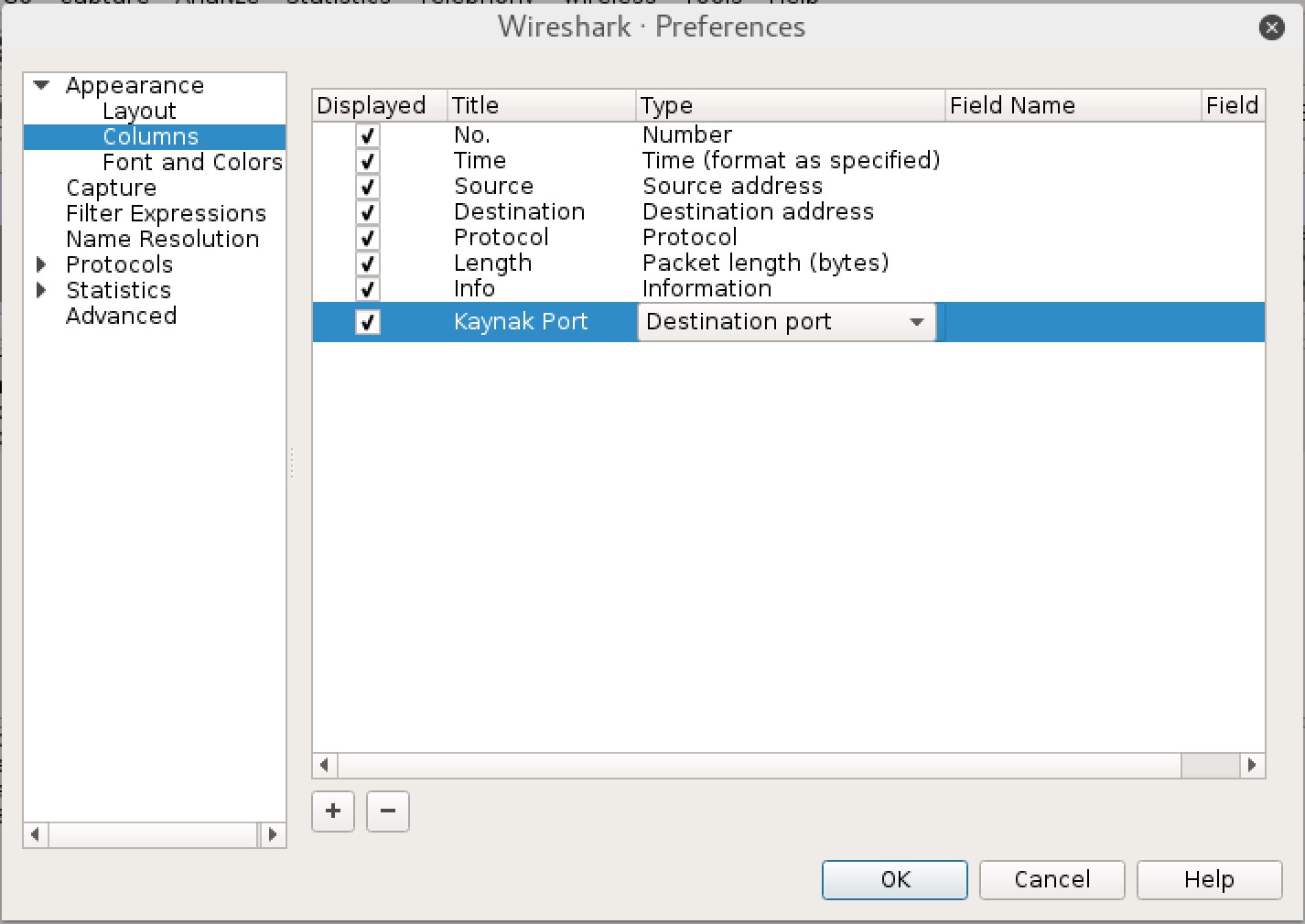
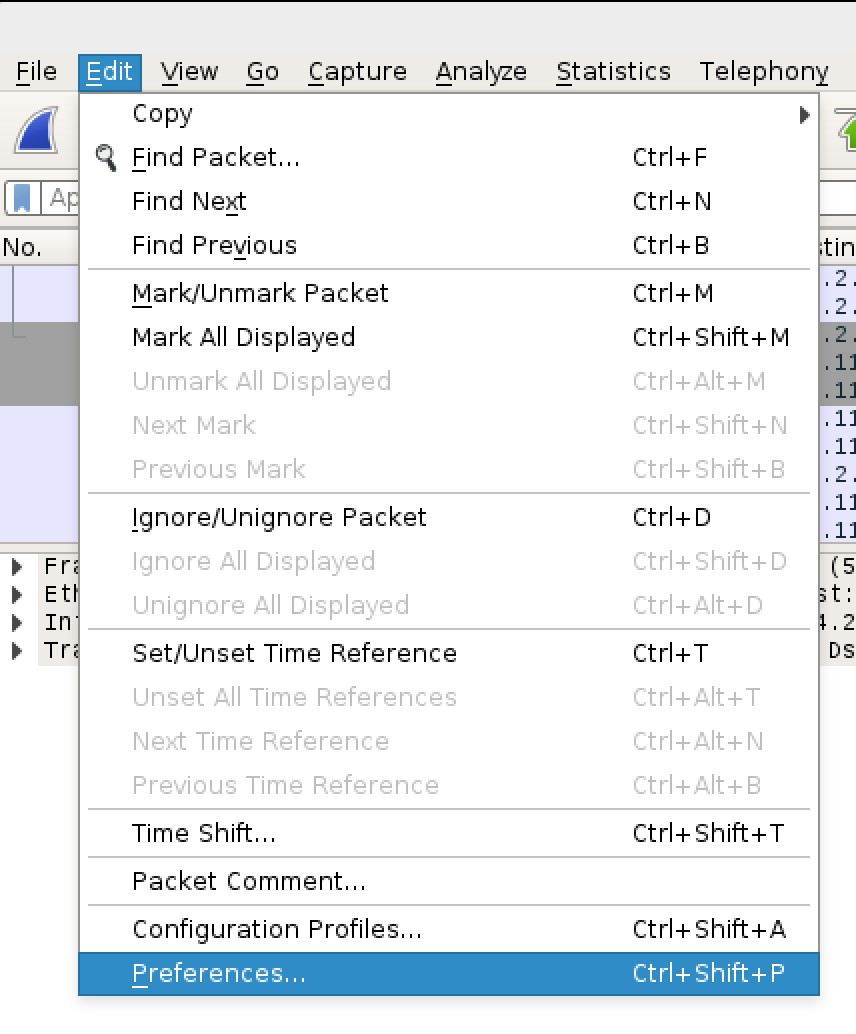
filtreleme

butonu

silinebilir

.

**3**



Daha

sonra

kolon

kısmına

tıklanır

.

Daha

sonra

sağda

açılan

pencerede

işlem

yapılır

.

(+)

tuşuna

basılır

ve

title

kısmına

kolon

başlığı

type

kısmına

da

ilgili

hazır

filtrelerden

seçim

yapılır

.

Dilerseniz

özel

bir

filtre

koyulabilir

.

**2**

**3**

ilk olarak

**Edit**

**-**

**>**

**Prefences**

yolunu takip

sağ tarafta bulunan pencerenin açılmasını sağlıyoruz. (Kısa yolu =

**C**

**trl +**

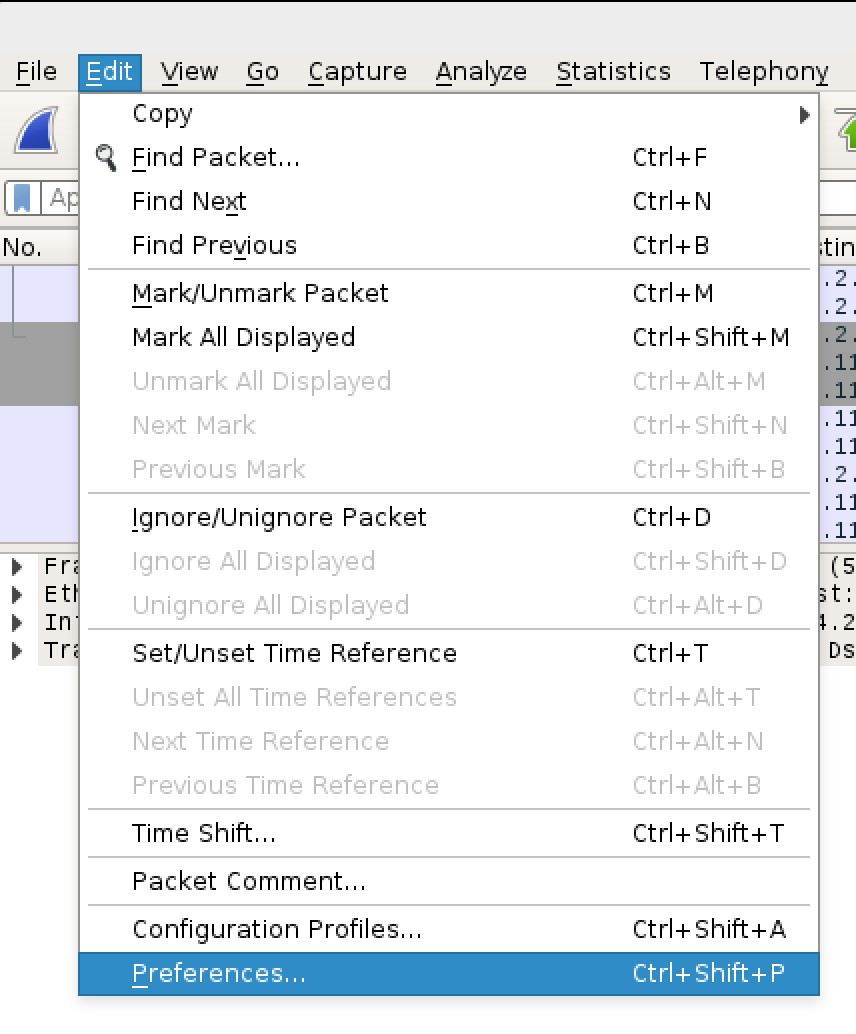
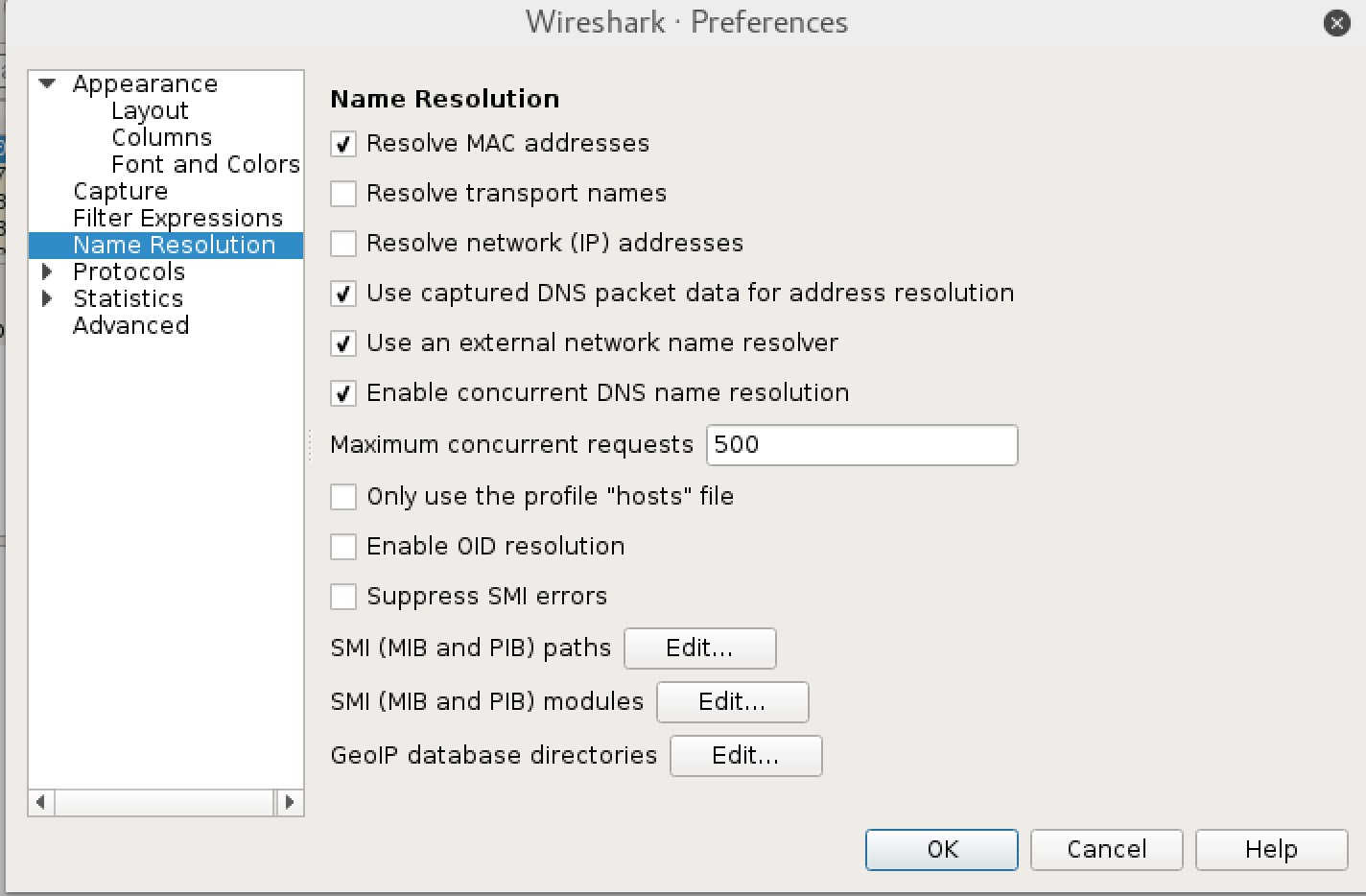
**S**

**hift + P**

)

**1**

**Wireshark – Adres Çözümlemenin Aktif Edilmesi**



ilk olarak

**Edit**

**-**

**Prefences**

**>**

yolunu takip

sağ tarafta bulunan pencerenin açılmasını sağlıyoruz. (Kısa

yolu =

**C**

**trl +**

**S**

**hift + A**

)

Daha

sonra

kolon

kısmına

tıklanır

.

Daha

sonra

sağda

açılan

pencerede

işlem

yapılır

.

**2**

**1**

Bu örnek için sadece MAC adresleri için adres çözümlemesini

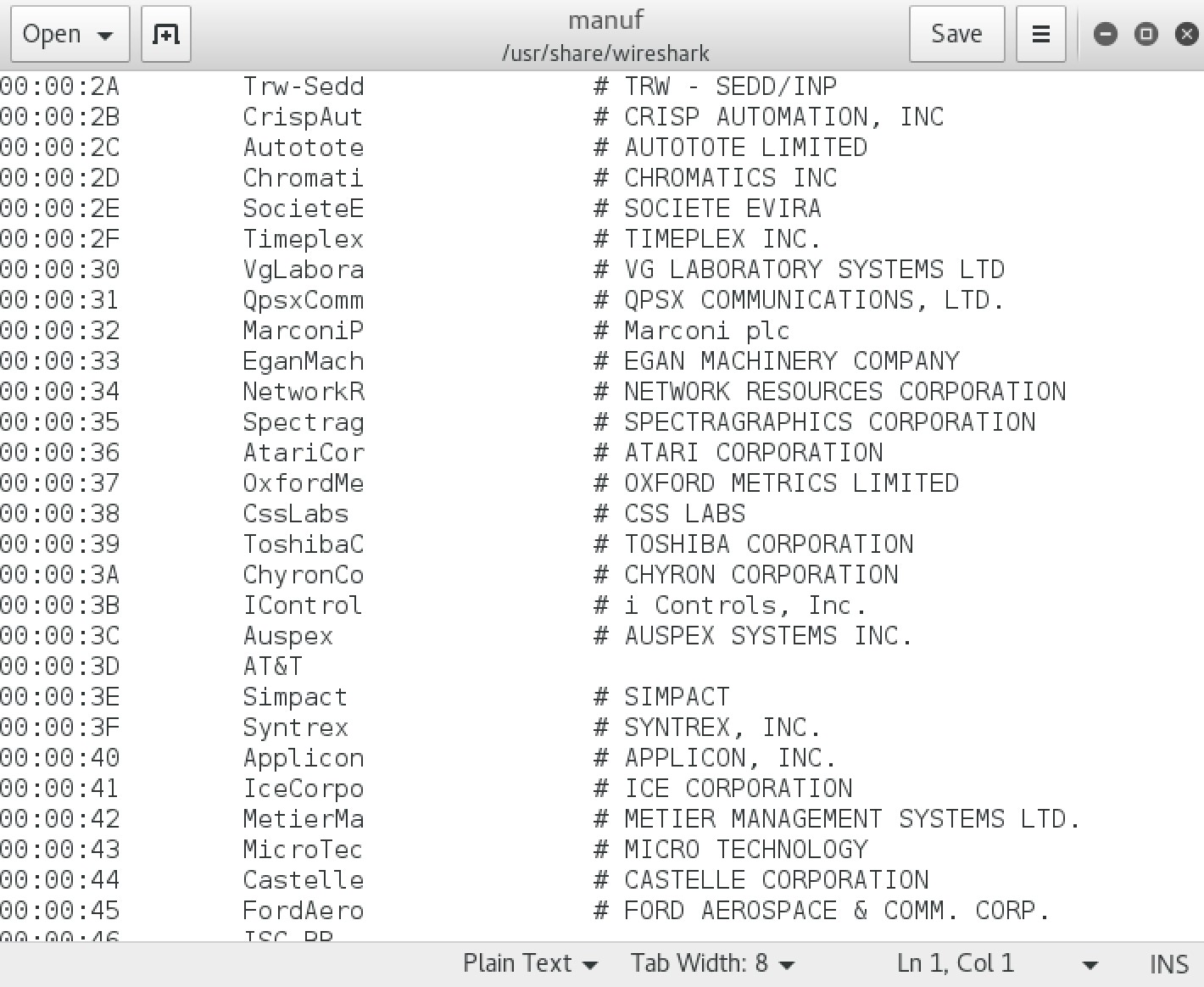
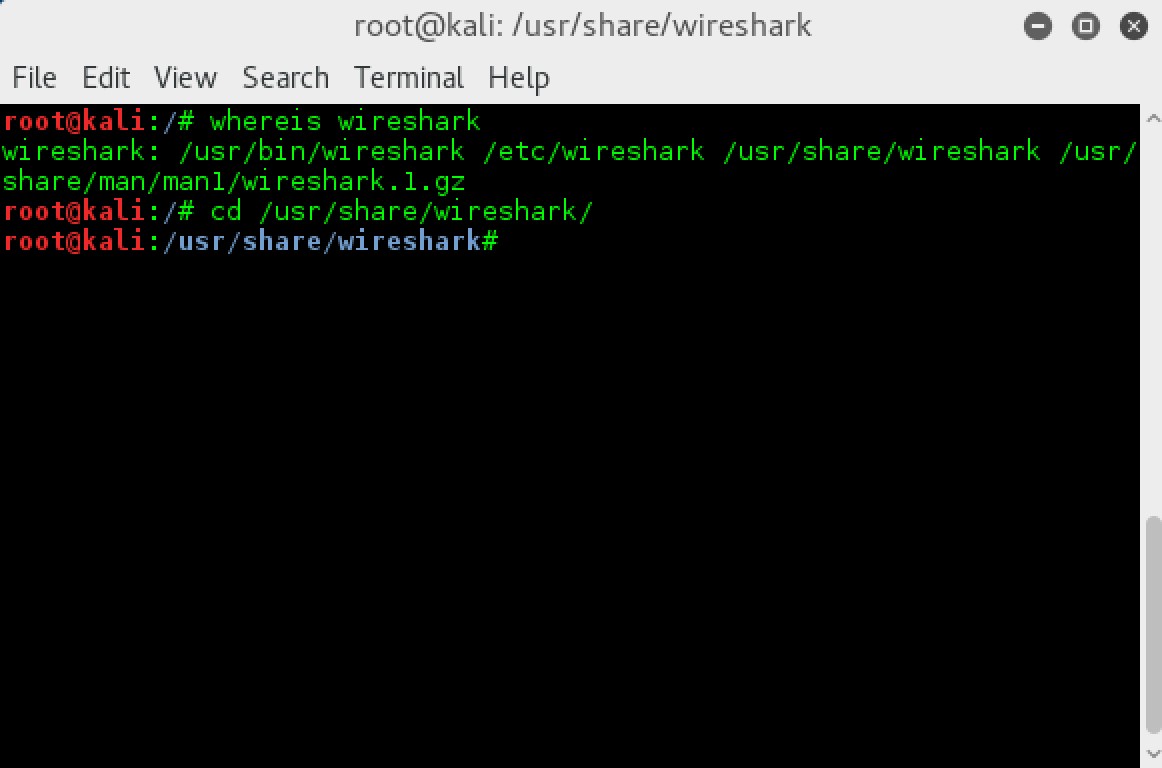
aktifleştirdik. Bu sayede artık MAC adreslerinin ilk 24 biti

çözümlenecek ve üretici firmayı trafik

ieçrisinde

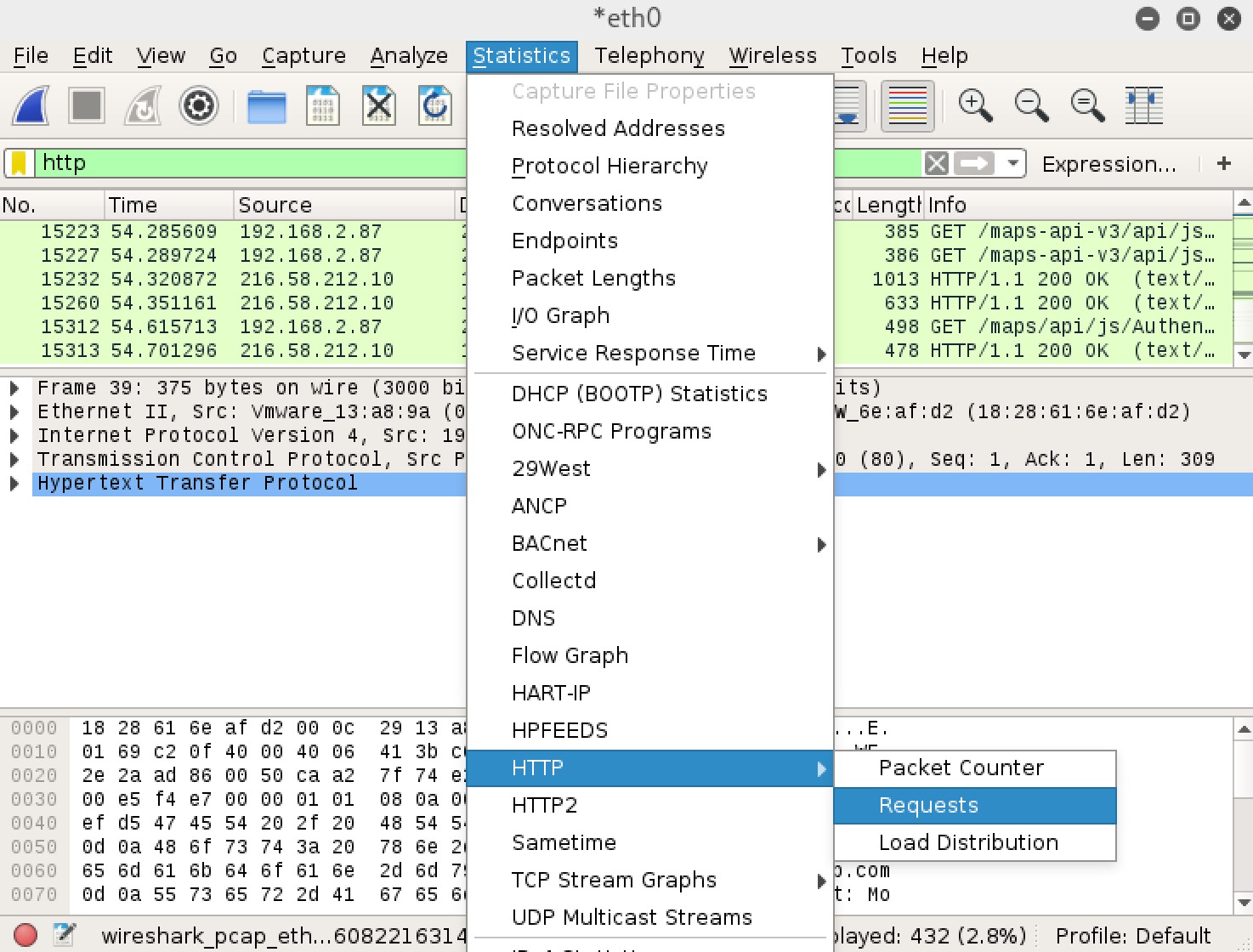
görebileceğiz.

**Wireshark – Adres Çözümlemenin Aktif Edilmesi**



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  | | --- | | Peki wireshark bu adres çözümlemeyi nasıl yapıyor ? | |  | |  | | --- | | Wireshark içersinde bulunan manuf isimli dosyayı sürekli güncellemekte ve bu dosyayı kullanarak adres çözümlerimeleri gerçekleştirmektedir. | |

**HTTP İsteklerinin Analiz Edilmesi**



Statistics

-

>

HTTP

-

>

Requests

yolunu

takip

ederek

ziyaret

edilen

ve

web

site

istatistiklerini

görebilirsiniz

.

Bu

kısımda

url

üzerine

tıklayarak

o

url

adresine

ait

trafiği

ve

yüklenme

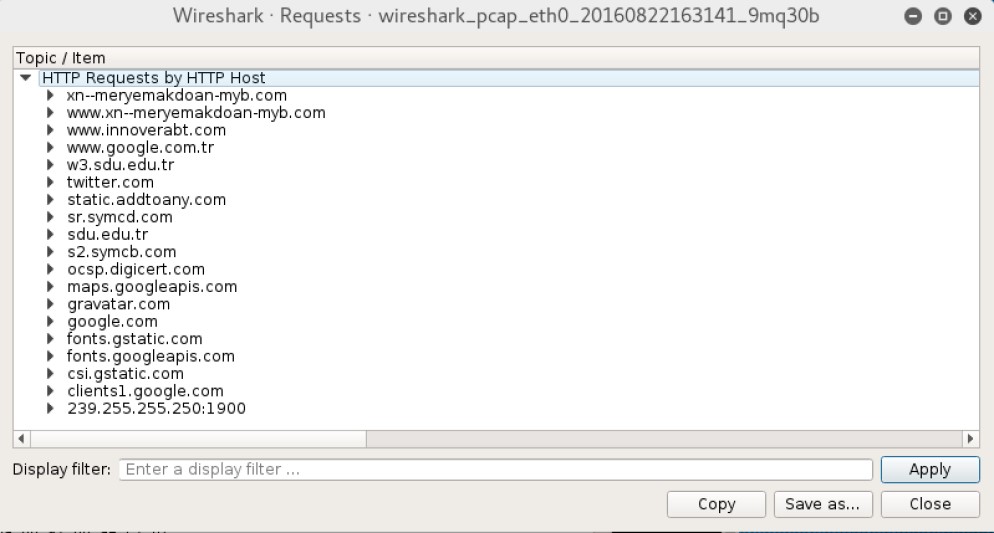
aşamalarını

görebilirsiniz

.

**1**

**2**



**HTTP İsteklerinin Analiz Edilmesi**

Statistics

-

>

HTTP

-

>

Packet

Counter

yolunu

takip

ederek

HTTP

Response

Packet

durumlarını

analiz

edebilirsiniz

.

Bu

kısımda

HTTP

cevap

kodlarına

ait

istatistikleri

görebilirsiniz

.

Örnek

olarak

•

**GET**

kullanılan

**165**

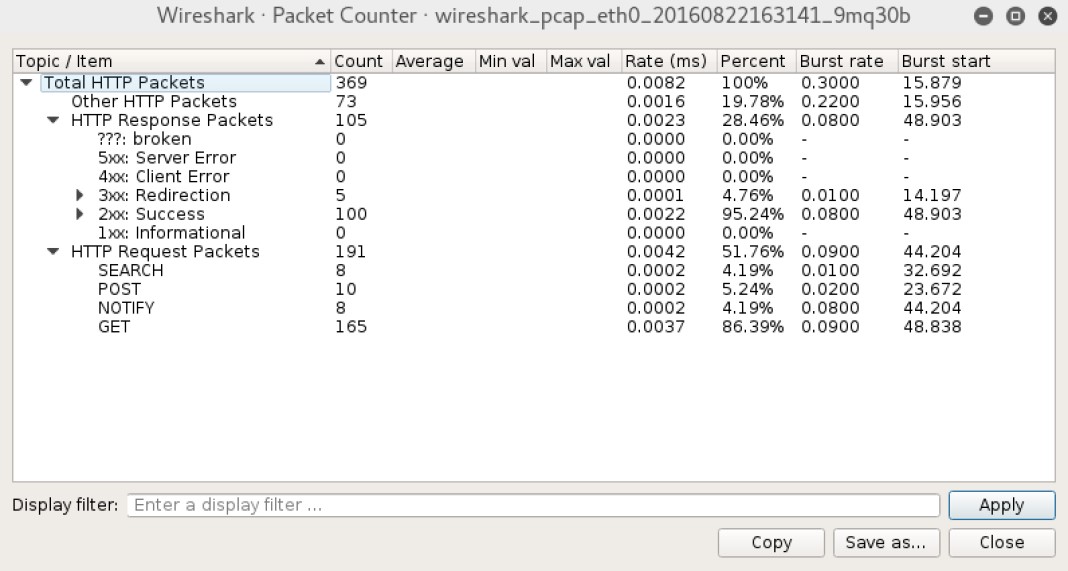
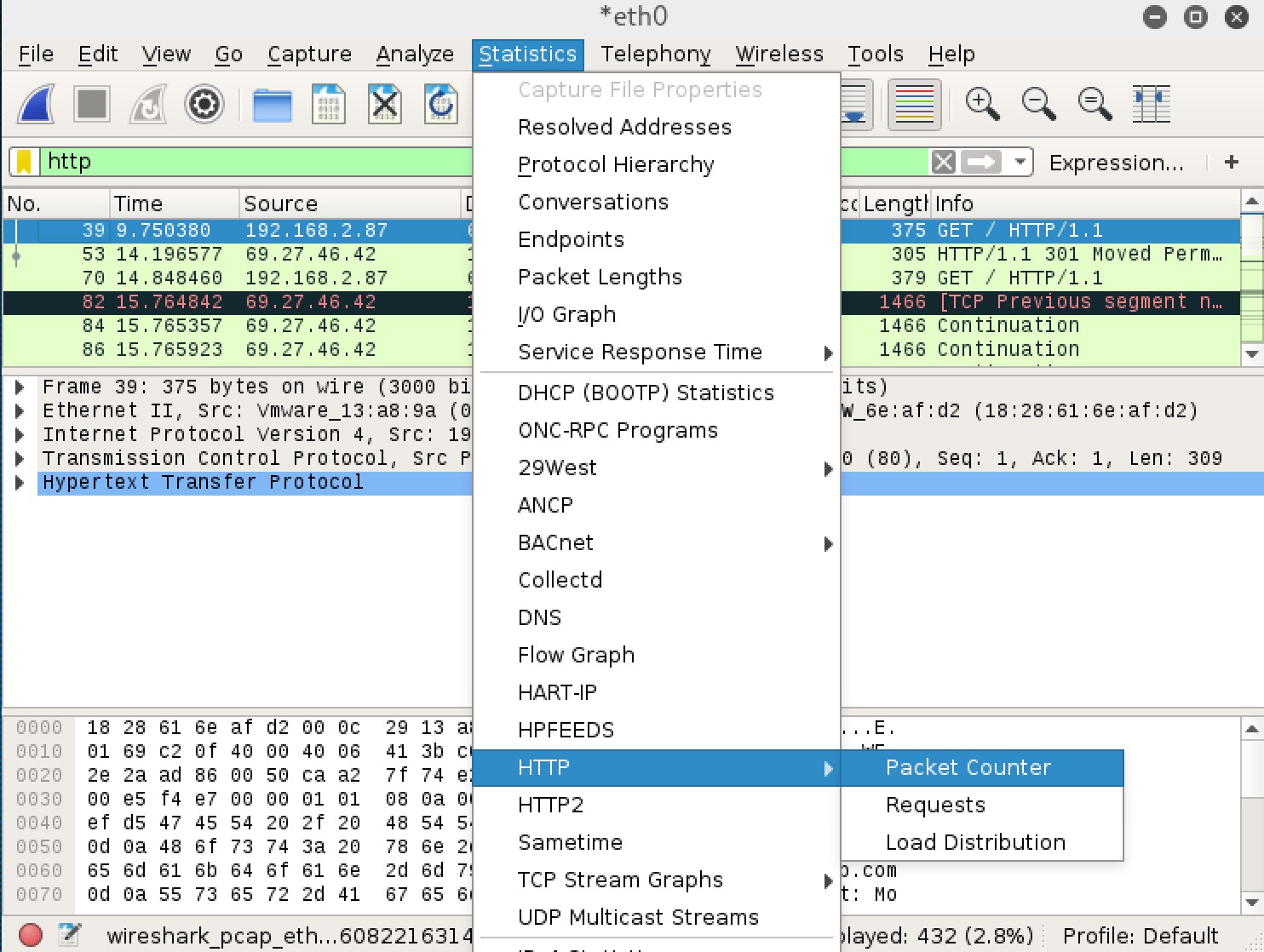
http

isteği

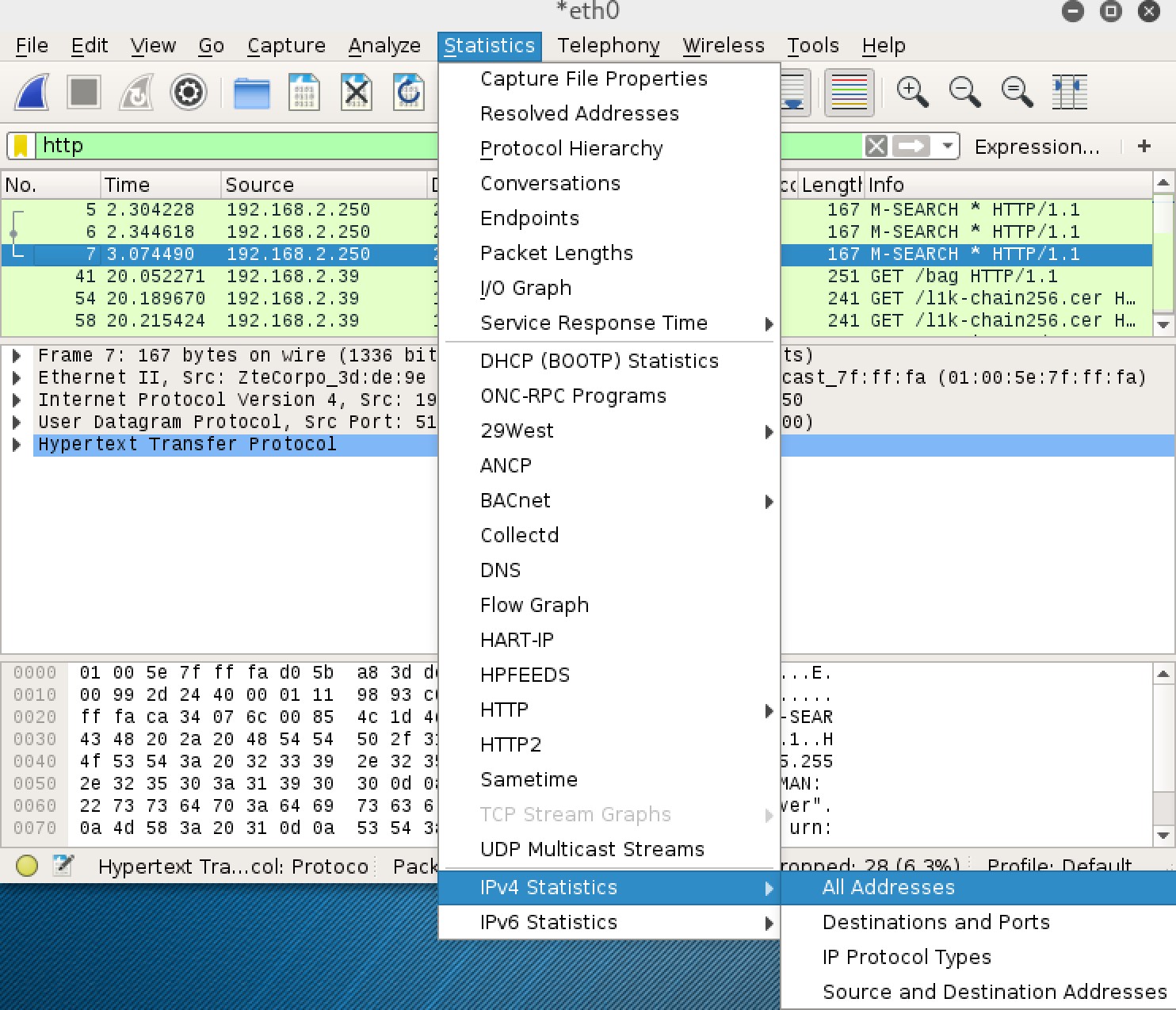
varmış

**1**

**2**



**IP Adreslerinin Analiz Edilmesi**



Statistics

-

>

IPv

4

Statistics

-

>

All

Addresses

yolunu

takip

ederek

IP

adres

istiatistiklerinin

bulunduğu

kısma

erişebiliriz

.

Bu

kısımda

IP

adreslerinin

trafik

içerisinde

kaç

defa

geçtiğini

bulabilirsiniz

.

Display

Filter

kısmından

da

bir

filtre

belirtip

hangi

ip

adreslerinin

o

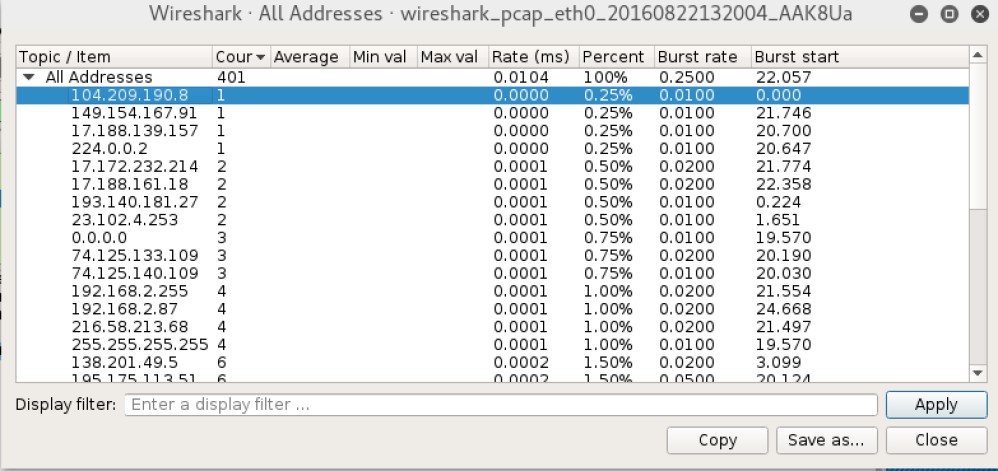
filtrede

geçerli

olduğunu

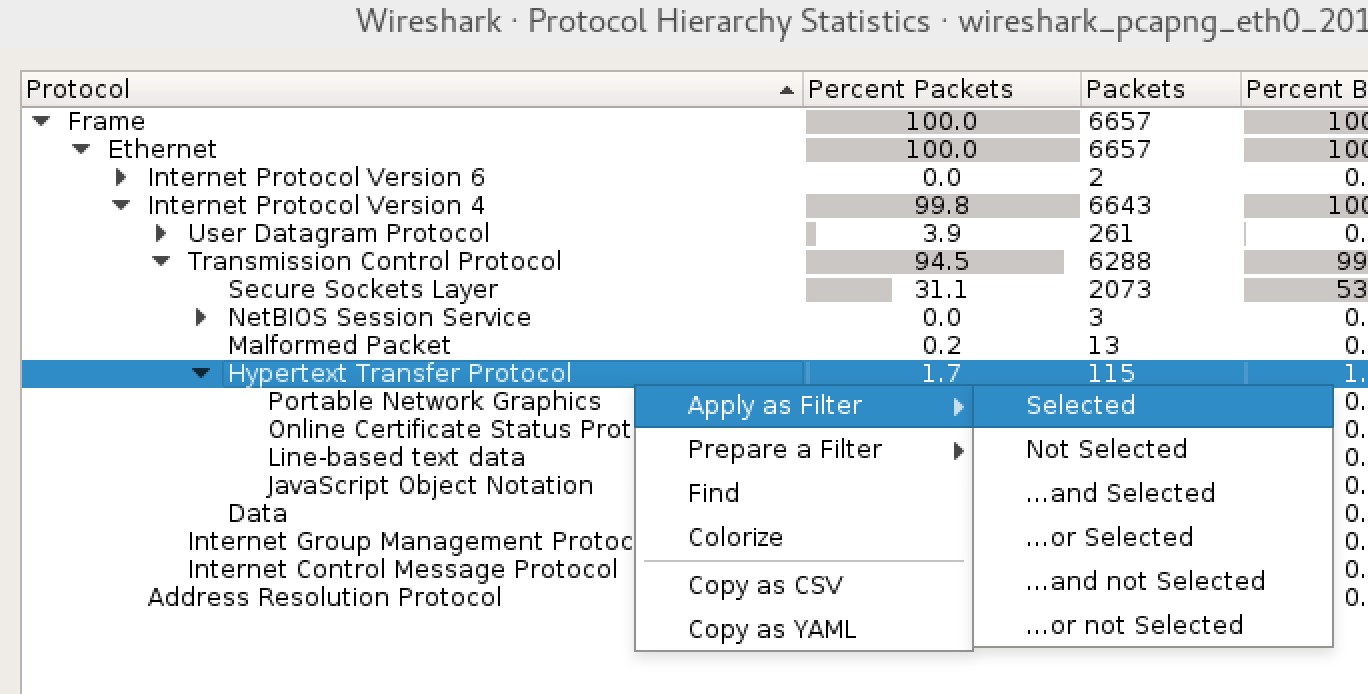
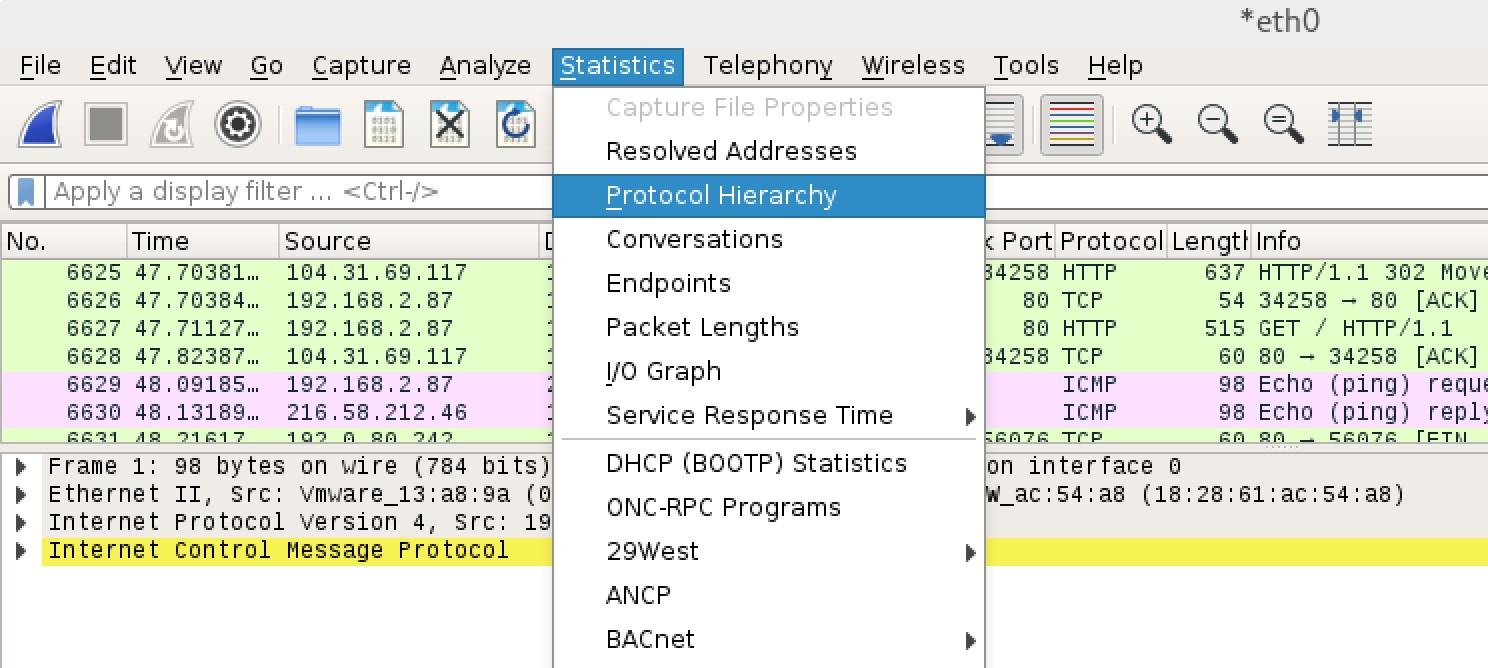
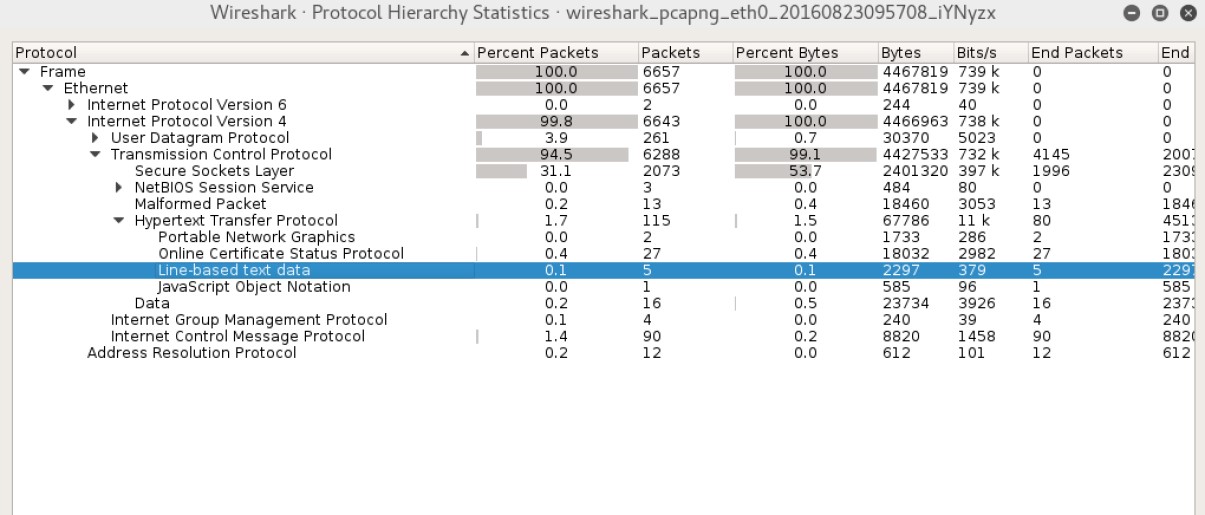
bulabilirsiniz

.



**1**

**2**



**Statistics**

**-**

**>**

**Protocol**

**Hierarchy**

yolunu takip ederek

**1**

numaralı görseldeki

gibi bir pencere ile karşılaşıyoruz. Bu pencerede hangi protokolden kaç tane

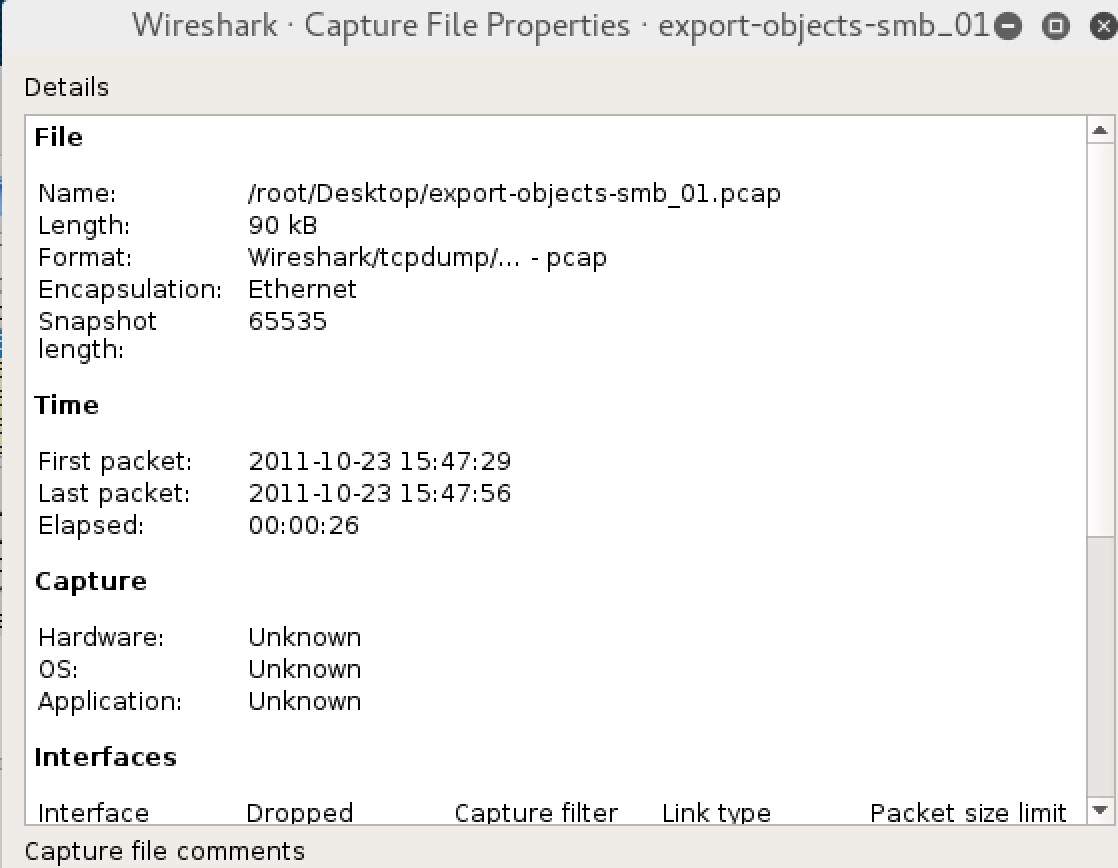
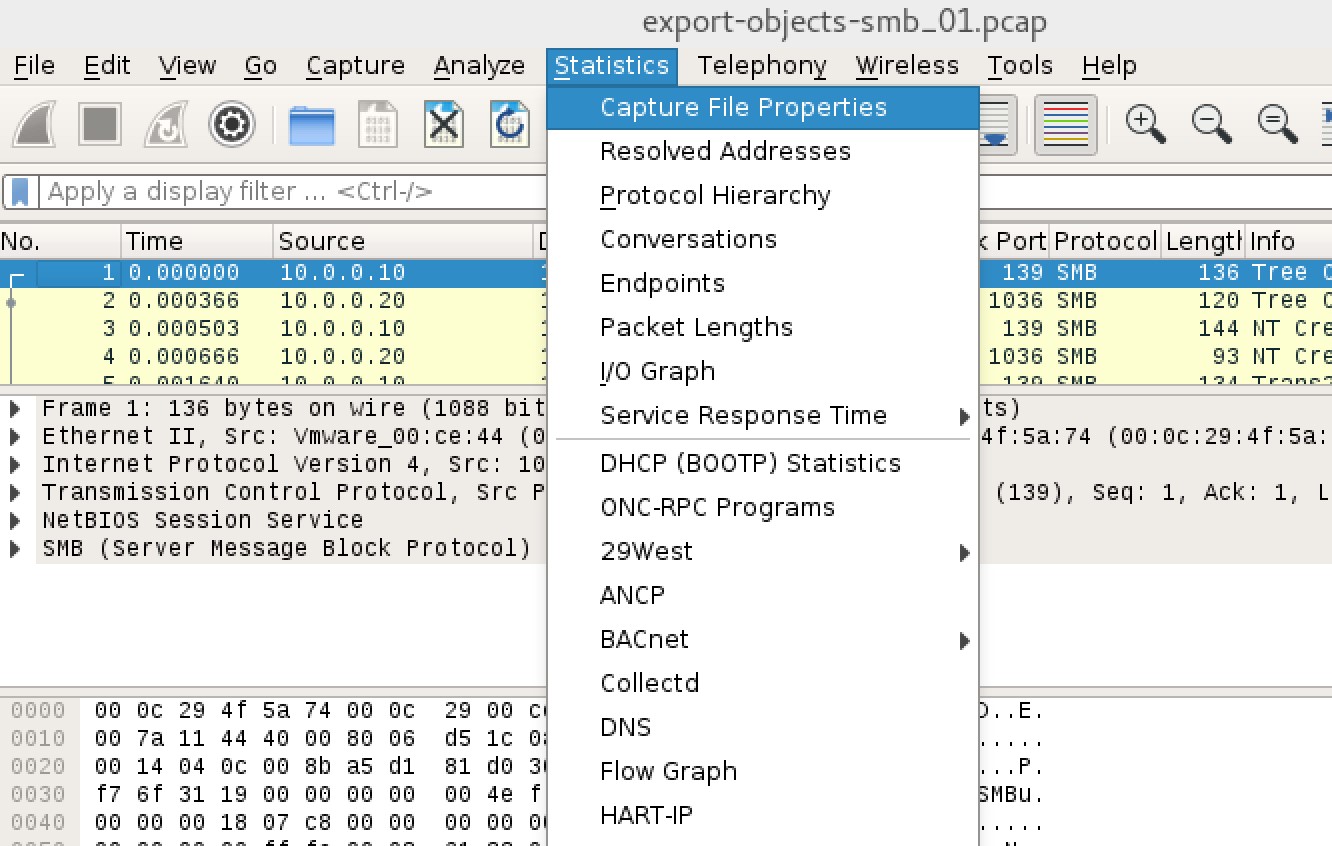
paket olduğunu görebilir ve istediğiniz bir protokol üzerine sağ tuş yapıp bir

filtre uygulayabilirsiniz

**.**

**(2)**

**1**



Yakalanan

paket

hakkında

özet

bilgiler

elde

etmek

istersek

**Statistics**

**-**

**>**

**Capture**

**File**

**Properties**

yolunu

takip

etmemiz

yeterli

olacaktır

.

Elde

edilebilecek

bilgiler

:

•

Dosya

ismi

•

Paket

yakalam

işlemi

ne

zaman

başladı,

ne

zaman

durdu,

ne

kadar

sürdü

•

Paket

yakalama

işlemi

özel

filtre

ile

mi

başlatıldı

.

•

Kaç

paket

yakalandı

**Wireshark – Resolved Addresses**

Yakalanan

paketlerin

tamamı

için

bir

adres

çözümleme

yapmak

istersek

**Statistics**

**-**

**>**

**Resolved**

**Addresses**

yolunu

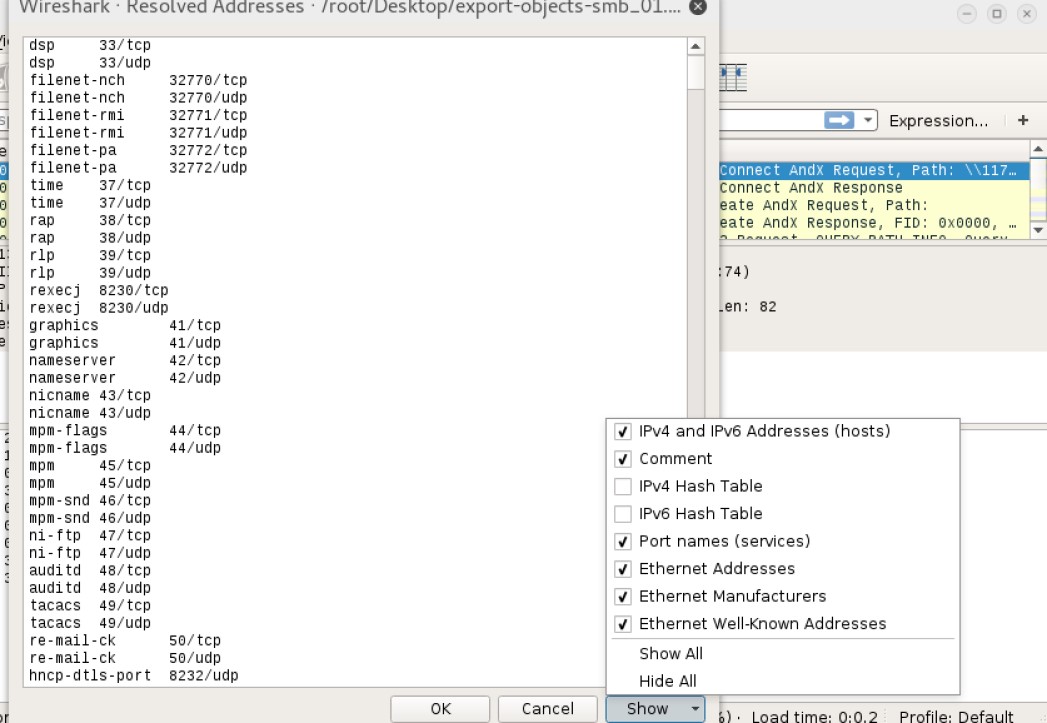
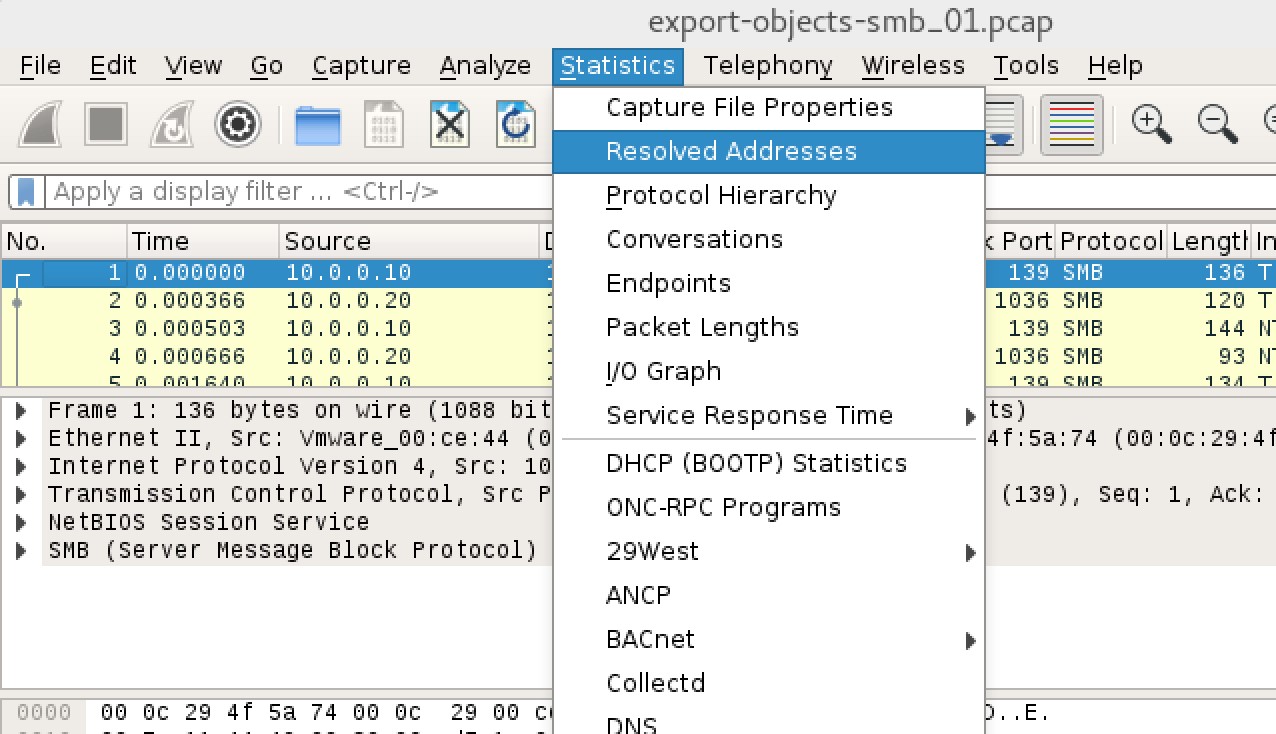
takip

etmemiz

yeterli

olacaktır

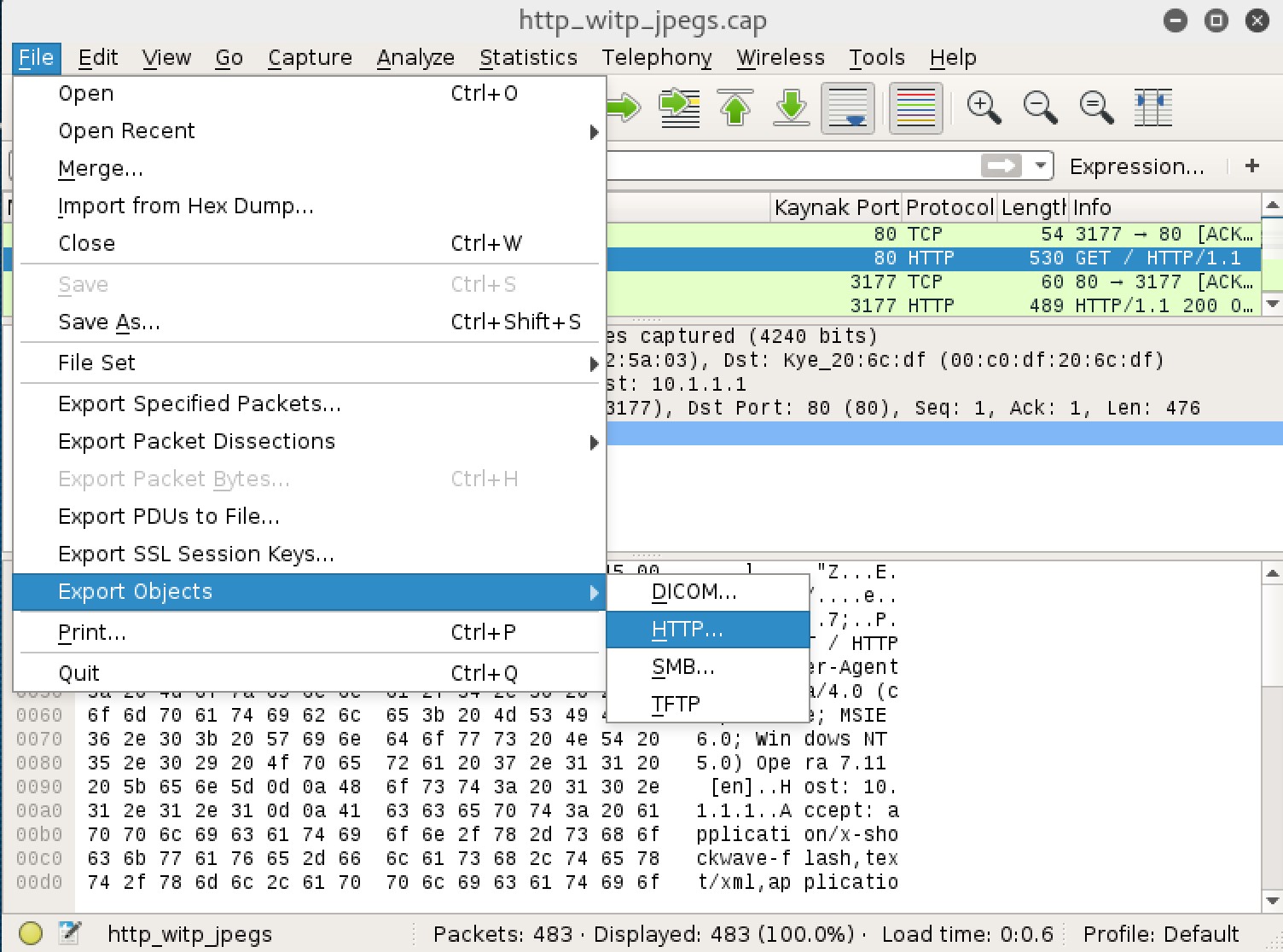
.



**Wireshark ile ARP Saldırılarını Tespit Etmek**

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | Aşağıda belirtilen filtreleri kullanarak sisteminize yönelik muhtemel ARP saldırısını tespit edebilirsiniz.   * arp.duplicate-address-frame * arp.duplicate-address-detected | |

**Trafik İçerisindeki Verilerin Export Edilmesi**



Wireshark

ile

çalışırken

trafik

içerisinde

geçen

bazı

ojeleri

export

etmek

isteyebilirsiniz

.

Bunu

yapabilmek

için

:

•

**File**

**-**

**>**

**Export**

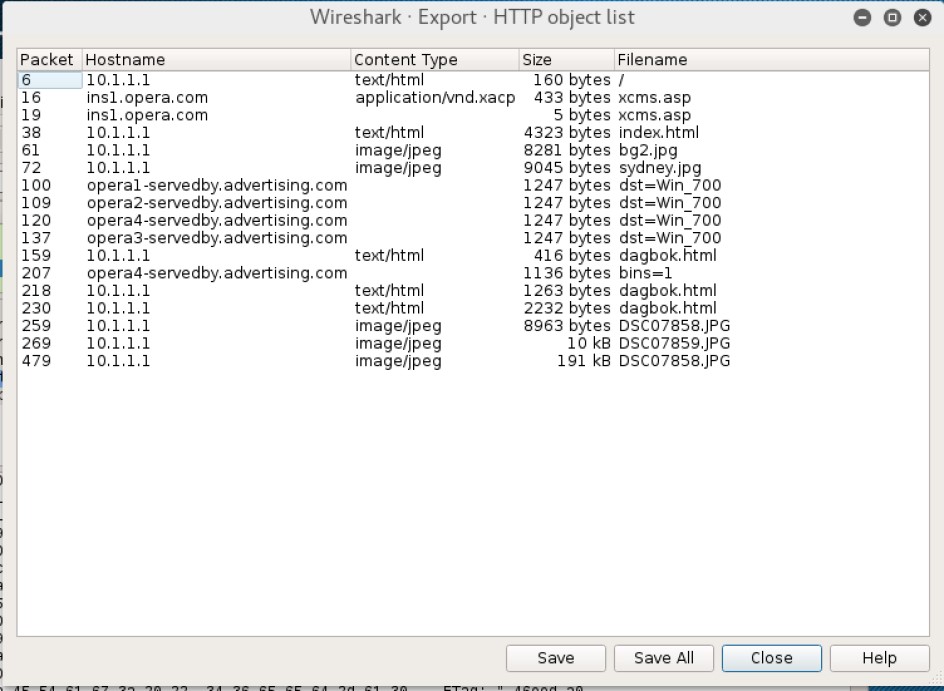
**Objects**

yolunu

takip

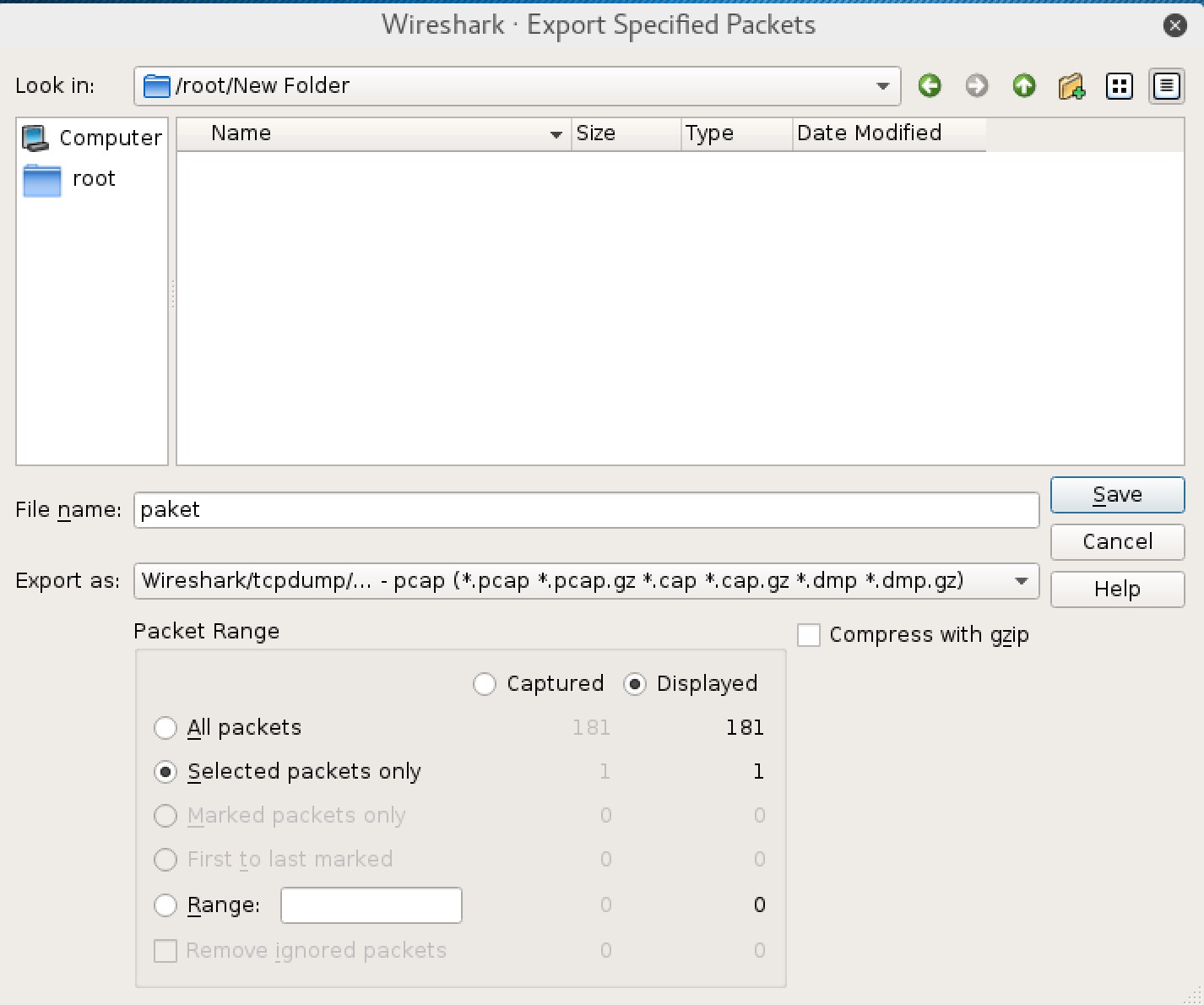
ediyoruz

.



|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | Wireshark ile çalışırken herhangi bir paketi export etmek ve daha sonra incelemek istersek yapmamız gerekenler aslında çok basit.  İlk olarak bir paketin üzerine tıklayıp daha sonra da ;  **File -> Export Specified Packets** yolunu takip ediyoruz. | |

**2**



**1**

**2**

**3**

**4**

**1**

**)**

Paketin kayıt edileceği yeri

seçeriz.

**2)**

Kayıt edilecek paketin adını

seçeriz.

**3**

**)**

Kayıt edilecek paketin tipi

hakkında bir seçim yapabilir ve

çeşitli uzantılarda kayıt edebiliriz

.

**4**

**)**

Burası en önemli kısım. Biz bu

slaytta sadece

**“**

**Selected**

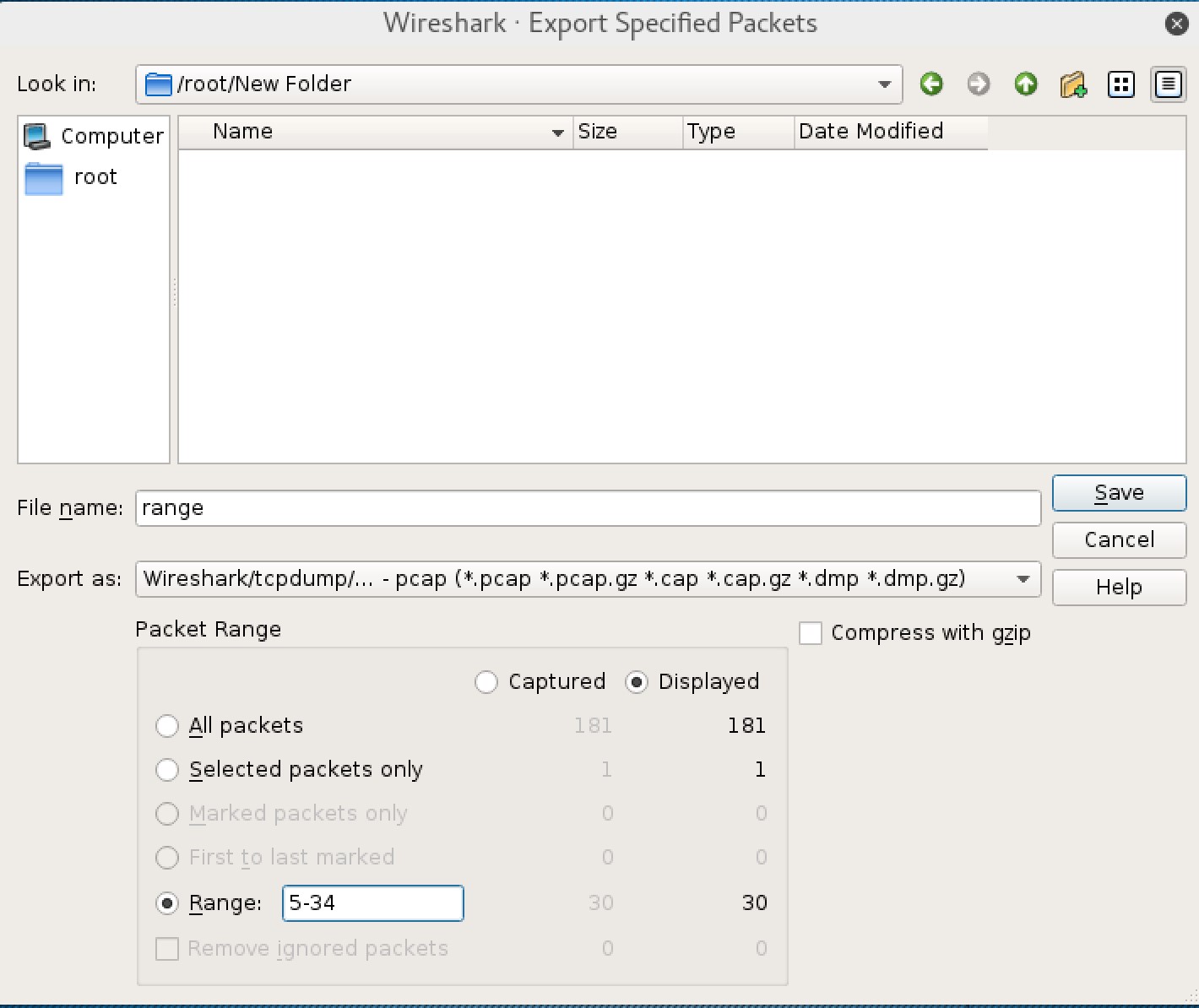
**packets**

**only**

**”**

ile sadece seçtiğimiz paketi

kayıt edeceğimizi belirtiyoruz.



Bu seferki süreçte belli aralıkta

istediğimiz paketleri daha sonra

incelemek için kayıt edeceğiz.

B

unun için kutu içerisine alınan

alanda

**“Range”**

kısmını seçip

istediğimiz aralığı belirtmemiz

yeterli olacaktır.

Bu sefer kutu içerisine alınan

alanda

**“Range”**

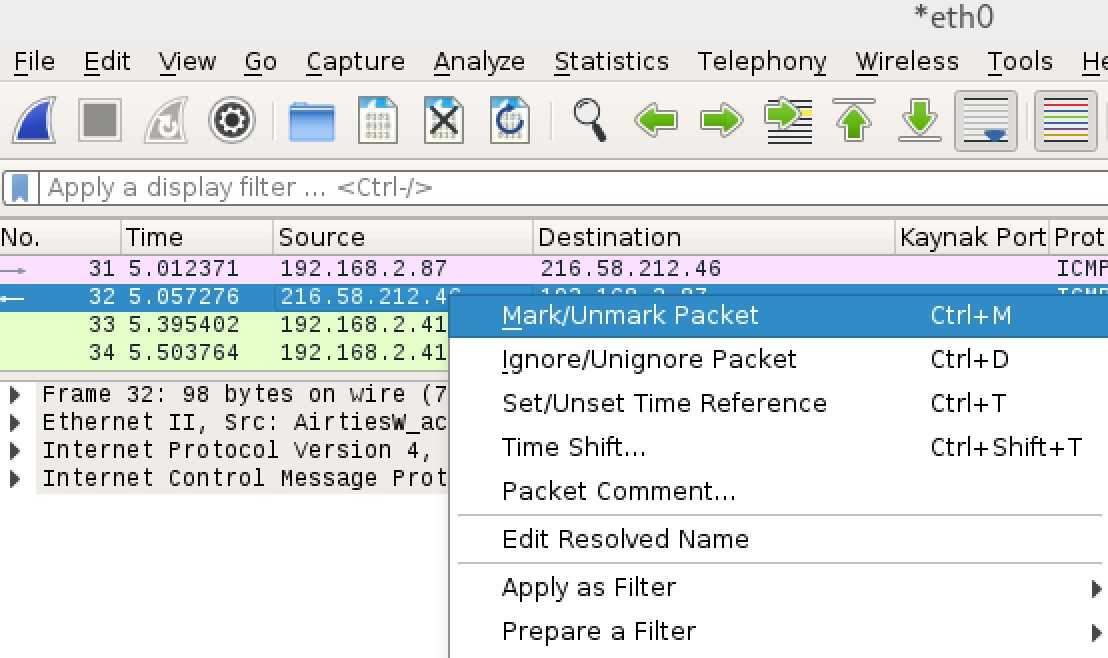
kısmını seçip

istediğimiz paketlerin numaralarını

virgül ile ayırarak belirtmemiz

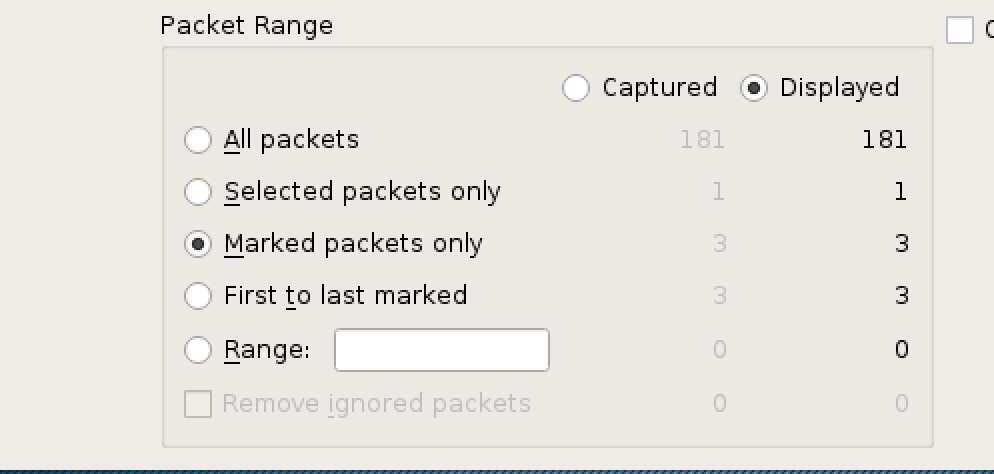
yeterli olacaktır.





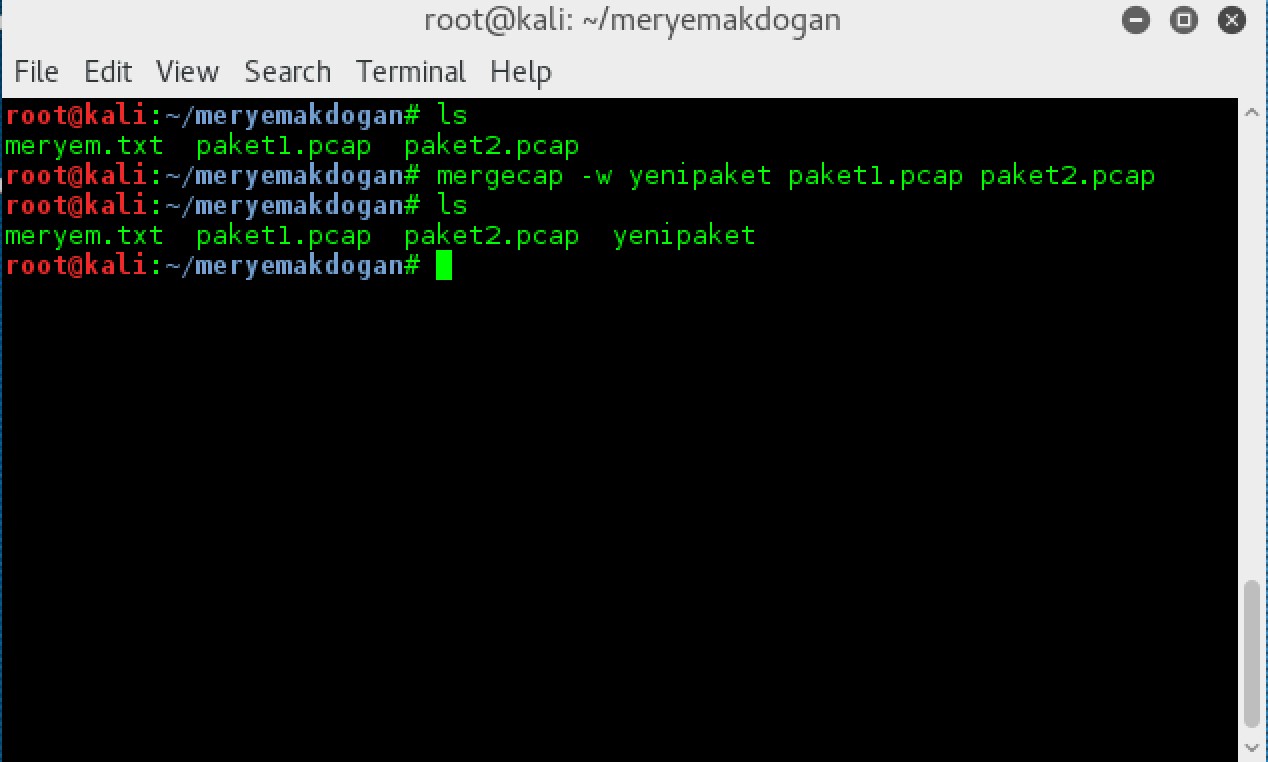
Seçmek istediğimiz paketlerin üzerine gelip sağ tuş yapıp **Mark/Unmark Packet** kısmına tıklıyoruz.

**5**



Bu kısımdan da **Marked packets only** seçeneğini işaretleyip sadece seçili olan paketlerin kayıt edilmesini istiyoru.

**Wireshark Dahili Araçlar – Mergecap**



Wireshark

ile

birlikte

kurulu

gelen

mergecap

isimli

araç

iki

farklı

pcap

ve

diğer

desteklenen

dosya

ağ

trafiği

değeri

taşıyan

dosyayı

birleştirebilmektedir

.

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | Elinizde bulunan pcap, cap gibi formatlarda olan wireshark tarafından desteklenen dosyalar hakkında bilgi toplamak amacı ile kullanılabilen ve wireshark ile gelen ek bir araçtır. | |
| |  | | --- | | Gördüğünüz üzere bu dosyanın **paket1.pcap ve paket2.pcap** isimli iki dosyanın birleştirilmesi sonucu oluştuğunu belirtiyor. | |