

Wireshark Kullanım Rehberi

Önemli İpuçları



Meryem AKDOĞAN

İçindekiler

- Wireshark hakkında
- Wireshark kurulumu
- Wireshark aracını tanıma aşaması
- Paket yakalama işlemi
- Filtreler
- Mantıksal operatörler
- Özel filtre oluşturmak
- Wireshark Adres Çözümleme Özelliği
- Wireshark ile Kolon Oluşturma
- Wireshark İstatistik Özelliği
- Wireshark ile Trafik İçerisindeki Dosyaları Export Etmek
- Wireshark ile pcap formatındaki dosyaları birleştirmek
- capinfos aracı
- mergecap aracı

Wireshark, kurulu olduğu bilgisayarda;

- Ağ trafiginin anlık olarak izlenmesini
- İzlenen bu trafigin 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 protokollerin görebilmek için bu bağlantıyı takip edebilirsiniz.
 - <https://wiki.wireshark.org/ProtocolReference>
- Çoklu işletim sistemi desteği sağlama:
 - 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.

Wireshark aracının kullanım alanları:

- Protokol hatalarını çözümlemek
- Paket analiz işlemleri
- Ağ içerisindeki hataları tespit etmek
- Ağ hakkındaki 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

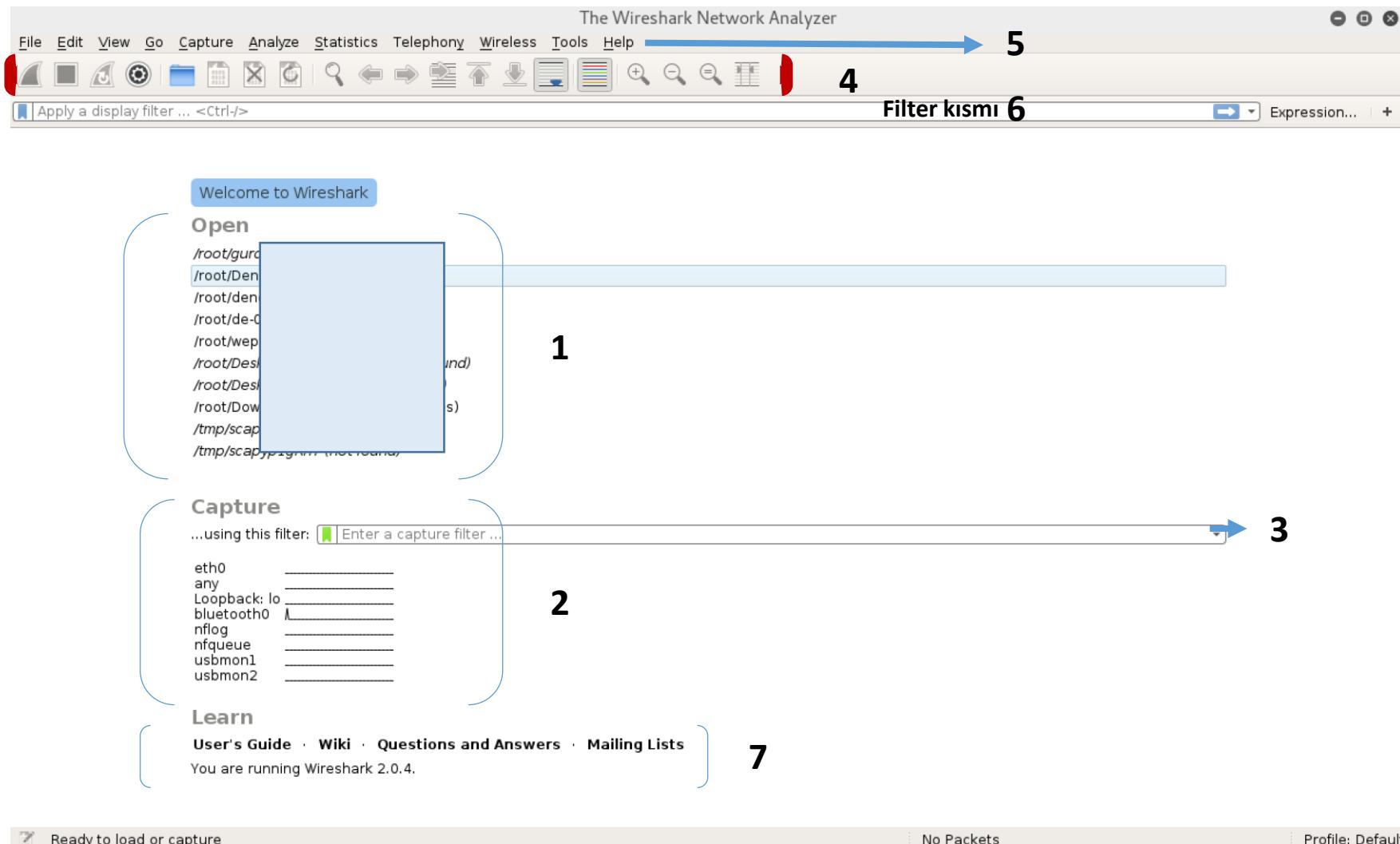
Wireshark aracı için asıl işi yapan kısım:

- Anlık ağ trafiginin yakalayıp wireshark aracına gönderen kısımdır.
- Wireshark aracı da kullanıcı dostu arayüzü sayesinde sizlerin bu ağ trafigini (paket akışını) görmeyi 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.

Wireshark Aracının Açılmış Arayüzünü Tanıyalım

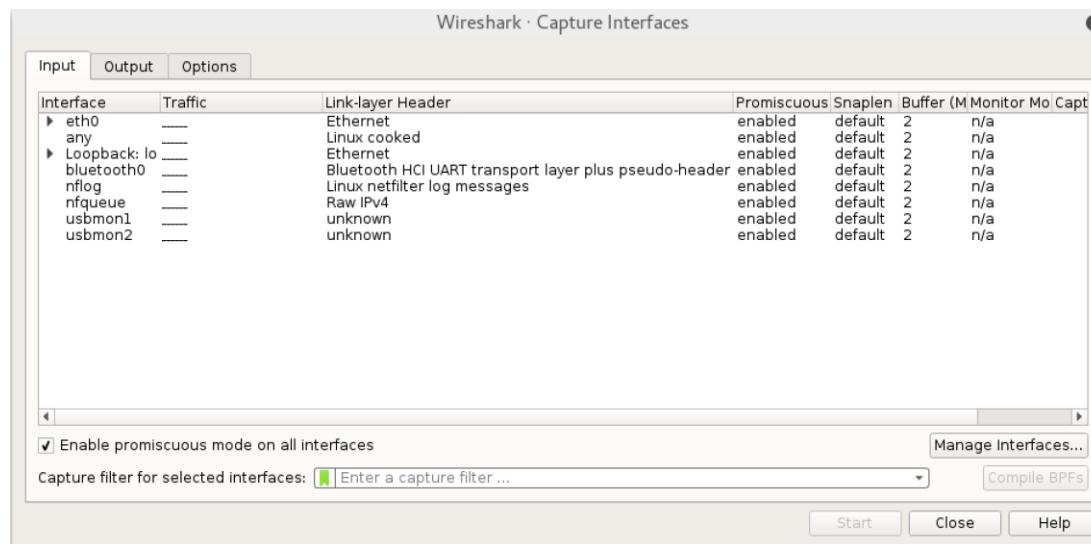


- 1) Daha önce açılan dosyalar gösterilmektedir.
- 2) Ağ trafiğini izlemek amacıyla kullanılabilecek ağ kartları gösterilmektedir.
- 3) Ağ trafiğini izlemek amacıyla kullanılabilecek ağ kartları için paket yakalamaya başladığında kullanabileceğiniz filtre tanımlanabilmektedir.
- 4) Sık sık kullanılabilecek 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 amacıyla kullanılabilecek bir bölümdür. Bu bölümde 5 numara ile tanımlanan ana menüde **Help** kismından erişebilirsiniz.

Wireshark aracı ile paket yakalama işlemi

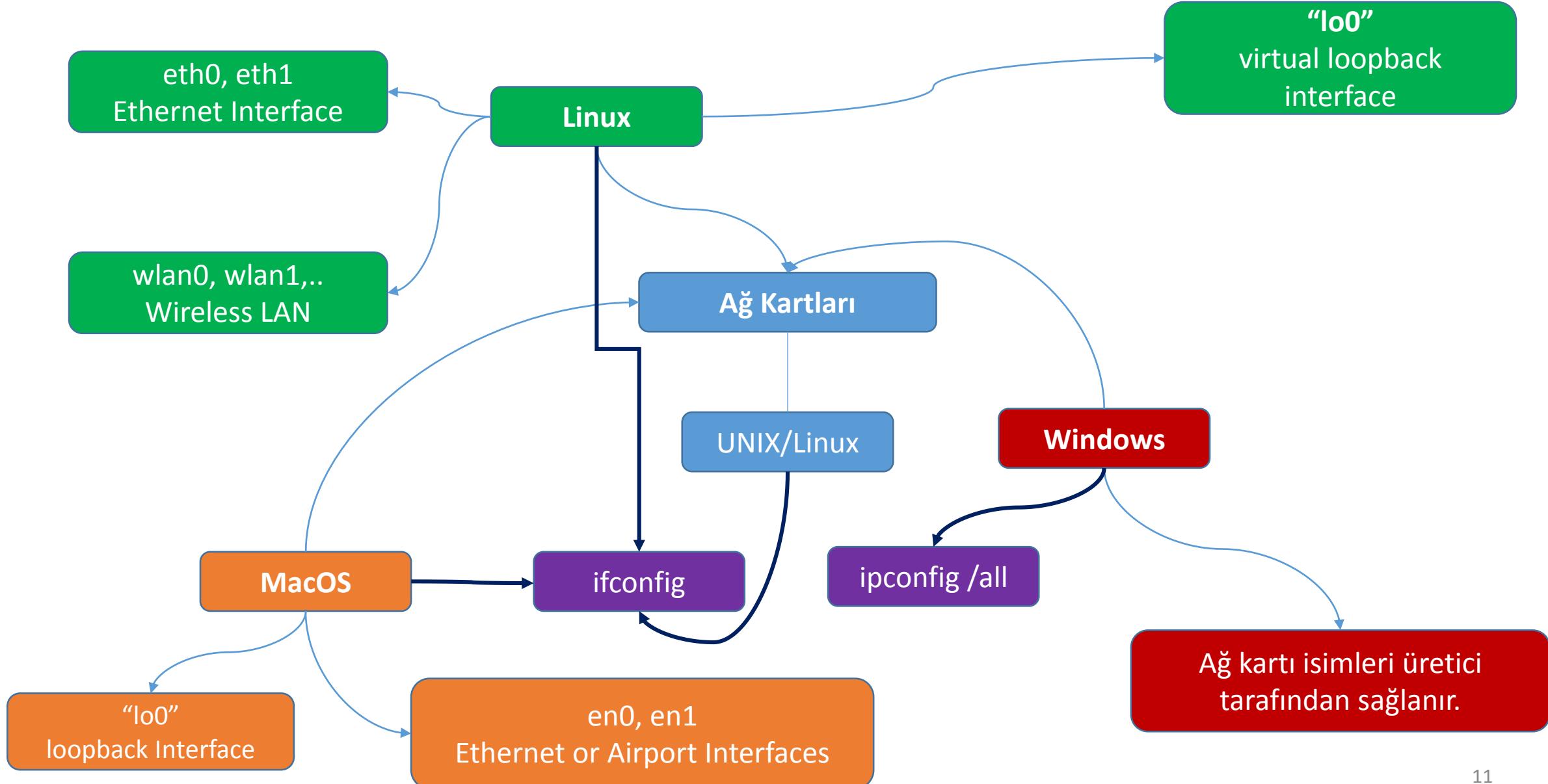
Bu işlem için iki seçenekiniz bulunmaktadır. Ama unutmamamız gereken şey, Wireshark aracını **root (en yetkili)** kişi hakları ile çalıştırılmaktır. Bunun sebebi, wireshark aracının bizim ağ kartlarımıza erişmek istemesidir.

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



- 2) Bu seçenekte ise programın ilk açılışında sizi karşılayan ekranada daha önceki slaytta 2 numara ile ifade edilen bölümden diledığınız ağ kartının üzerine tıklamaktır.

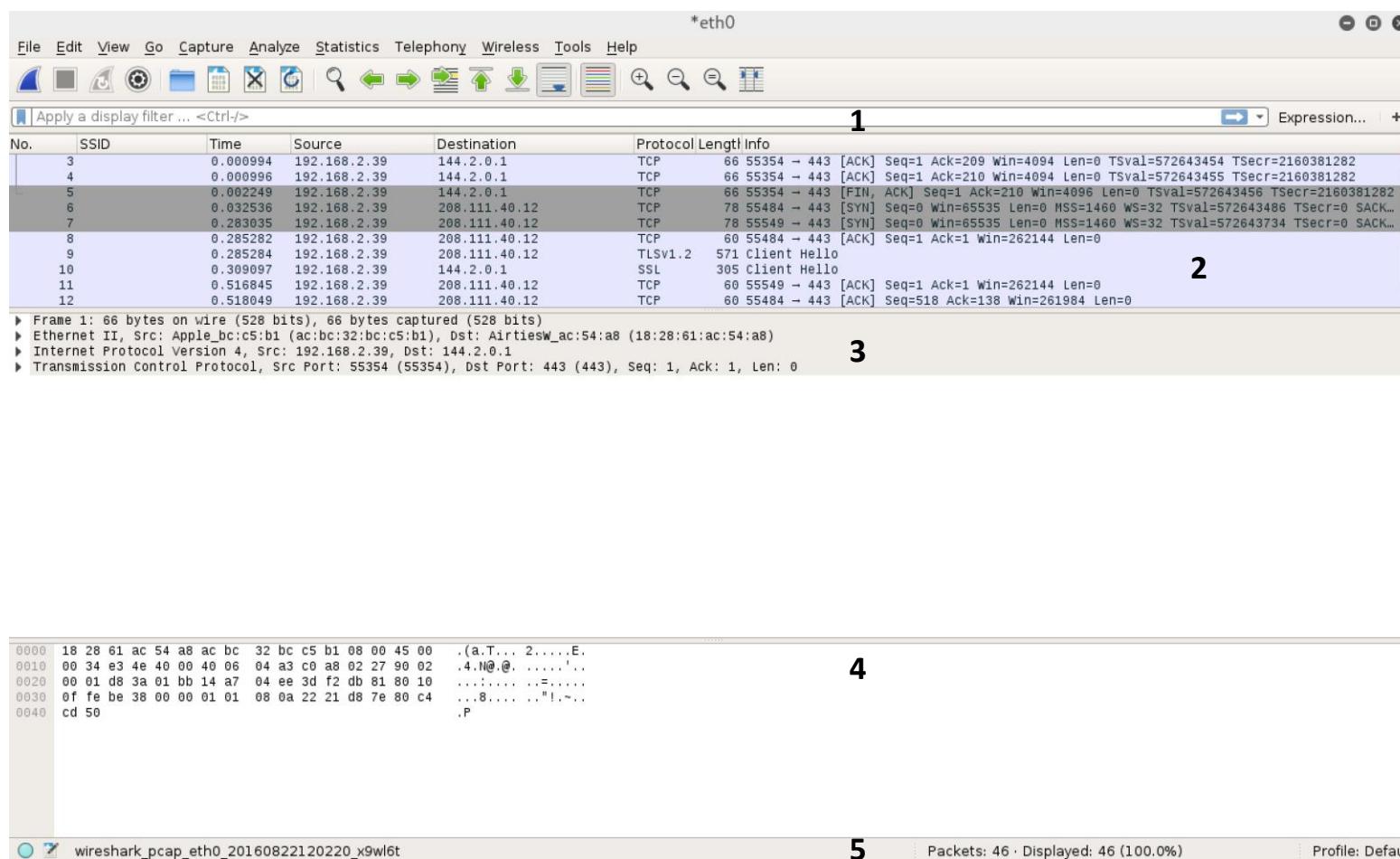
Wireshark İle Paket Yakalama – Ağ Kartları



Wireshark Aracının Paket Yakalama Arayüzü

Wireshark aracı ile paket yakalama işleminde ki ara yüzü tanıyalım

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



1) Yakalanan paketler ile ilgili filtreleme seçeneklerinin bulunduğu kısımdır.

2) Yakalanan paketlerin listelendiği kısımdır.

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

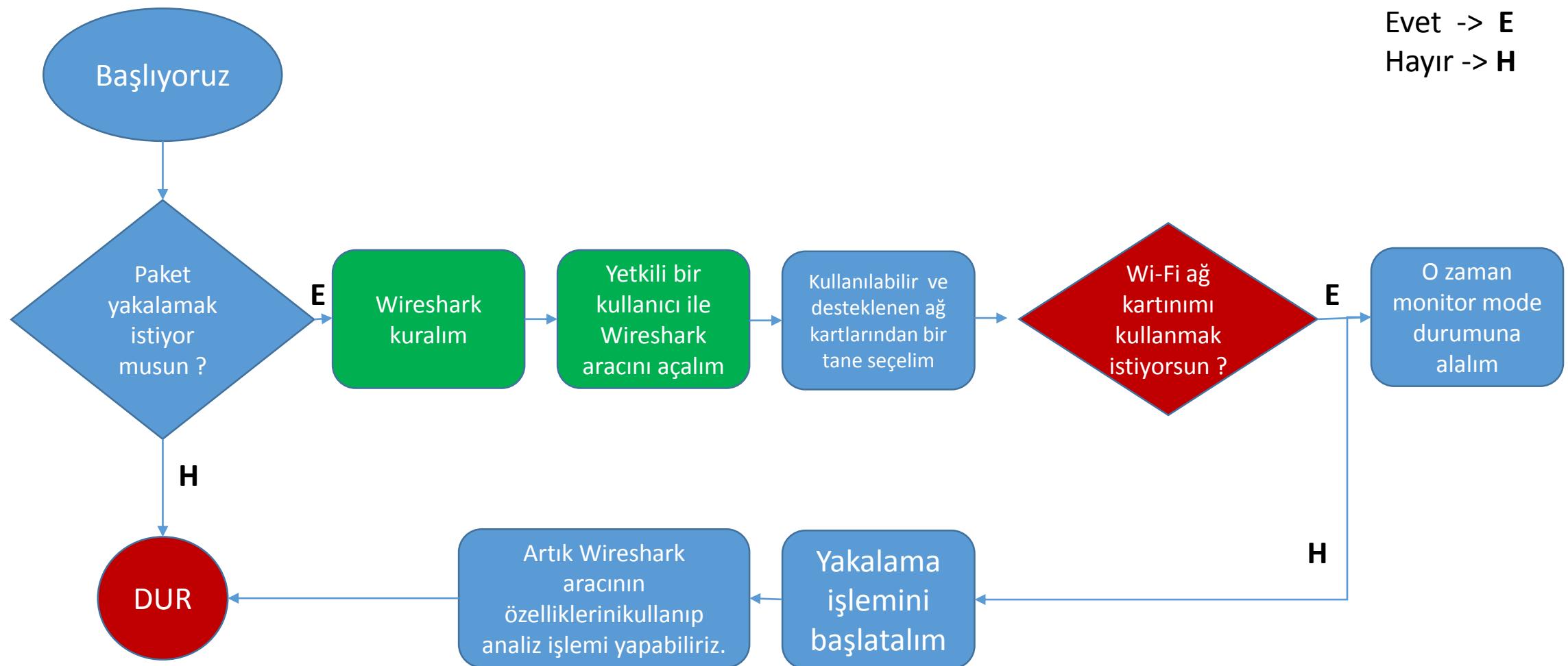
4) Seçilen paket için hex dump halini gösterir.

5) Genel bilgilendirmelerin yer aldığı kısımdır. Bu kısında :

- Yakalanan toplam paket
- Görüntülenen paket sayısı
- Profil ismi

gibi bilgiler yer almaktadır.

Wireshark - Paket Yakalama Algoritma Diagramı



DHCP İçin Kullanılabilecek 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 İçin Kullanılabilecek Filtreler

- http
- http.request.method=="GET"
- http.request.method=="POST"
- http.response.code == "200"
- http.user_agent == "User_Agent_Değeri"
- http.referer

ARP İçin Kullanılabilecek 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 İçin Kullanılabilecek Filtreler

- 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

İnternet Protokol İçin Kullanılabilecek Filtreler

- ip.addr
- ip.ttl
- ip.version == 4
- ip.src == 192.168.2.45
- ip.dst == 192.168.2.34

TCP İçin Kullanılabilecek Filtreler

- tcp.flags.syn == 1
- tcp.port == 80
- tcp.dstport == 443
- tcp.srcport == 80

FTP İçin Kullanılabilecek Filtreler

- ftp.request.command
- ftp.request
- ftp.request.command == "PASS"
- ftp.request.command == "USER"
- ftp.response.arg == "Login successful."

ICMP İçin Kullanılabilecek Filtreler

- icmp.type
- icmp.code

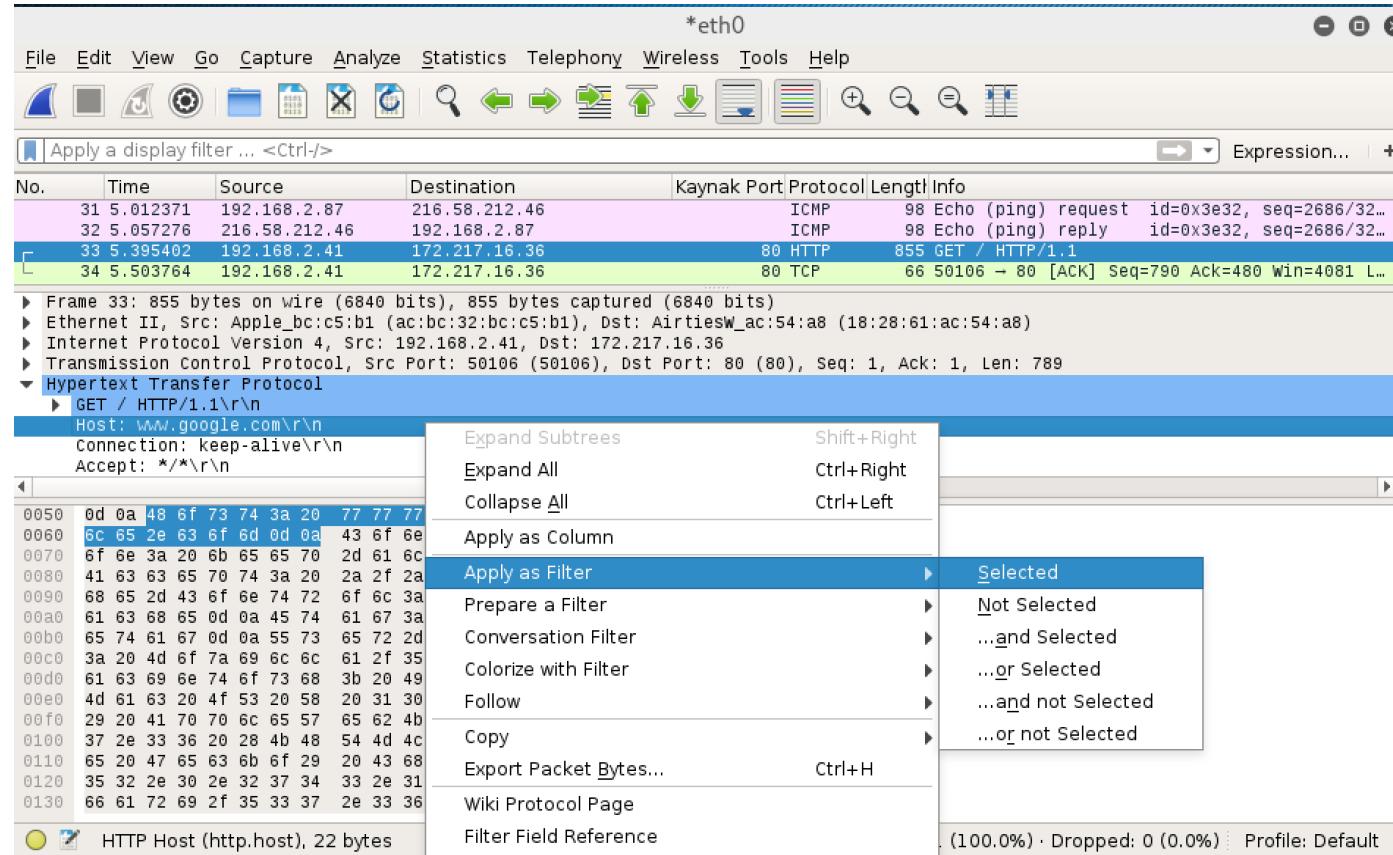
Karşılaştırma Operatörleri

- eq == Eşittir
- ne != Eşit değildir
- gt > Büyüktür.
- lt < Küçüktür
- ge >= Büyük eşittir
- le <= Küçük eşittir.

Mantıksal Operatörler

- and && = (ve anlamı katar)
- or || = (veya anlamı katar)
- xor ^ =
- not ! = (değil anlamı katar, dahil olmayan)

Wireshark İçin Kendi Filtrelerinizi Oluşturun



Wireshark kullanırken standart filtrelemeler dışında kendinize ait özel filtreler oluşturmak 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.

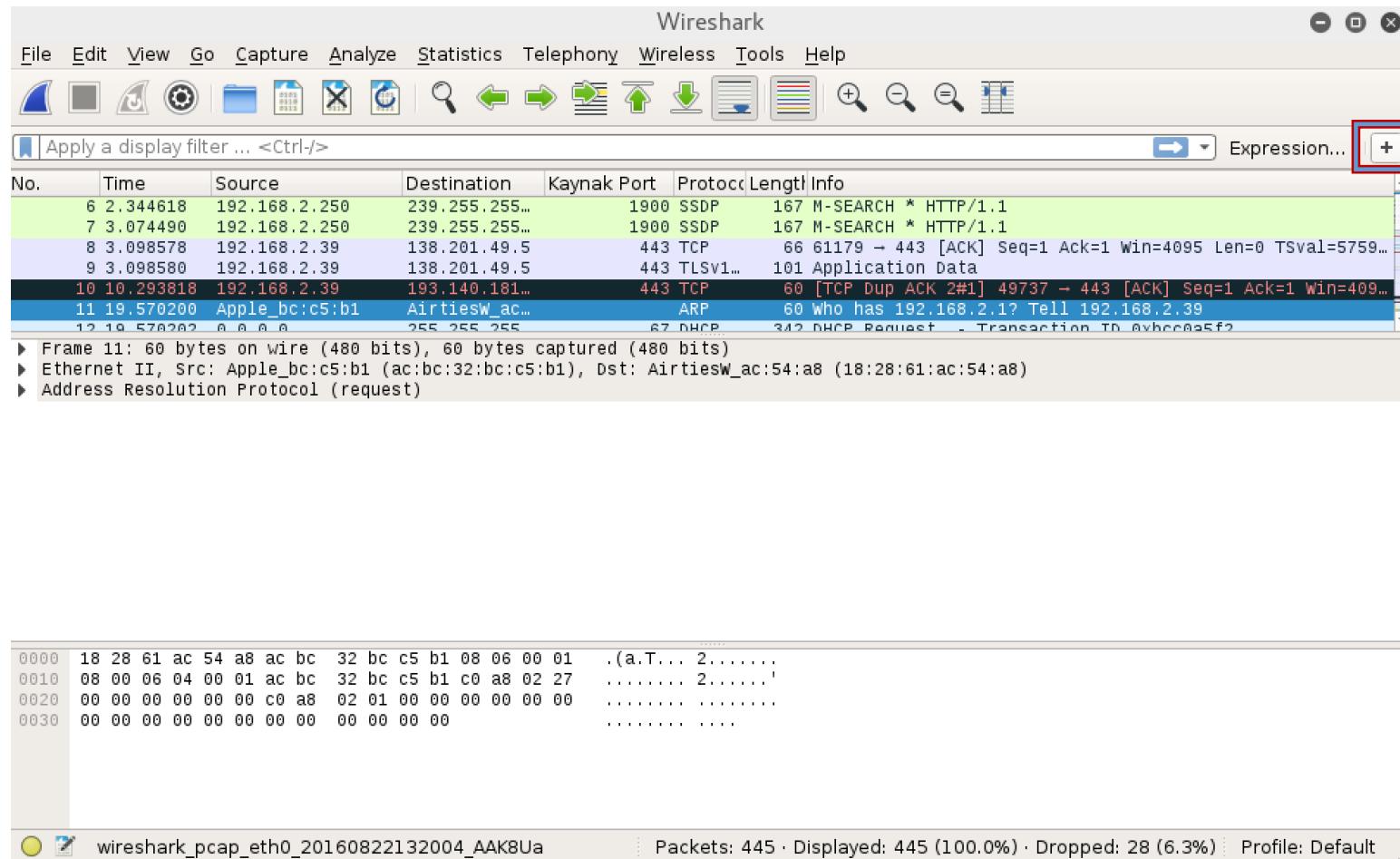
Wireshark – Contains İsimli Filtre İle Arama İşlemi

Wireshark interface showing SMB traffic capture. The search bar at the top contains the filter 'smb contains "SHARKFEST"'. The main pane displays several SMB frames, and the bottom pane shows the raw hex and ASCII data of a selected frame.

Wireshark interface showing HTTP traffic capture. The search bar at the top contains the filter 'http contains "jpeg"'. The main pane displays several HTTP frames, and the bottom pane shows the raw hex and ASCII data of a selected frame.

İstediğimiz protokol içerisinde arama yapabilmemizi sağlayan contains filtresi bize çok kolaylık sağlamaktadır. Örneklerde SMB ve HTTP trafikleri içerisinde bazı aramalar yapılmıştır.

Filtreleme Butonu Oluşturmak

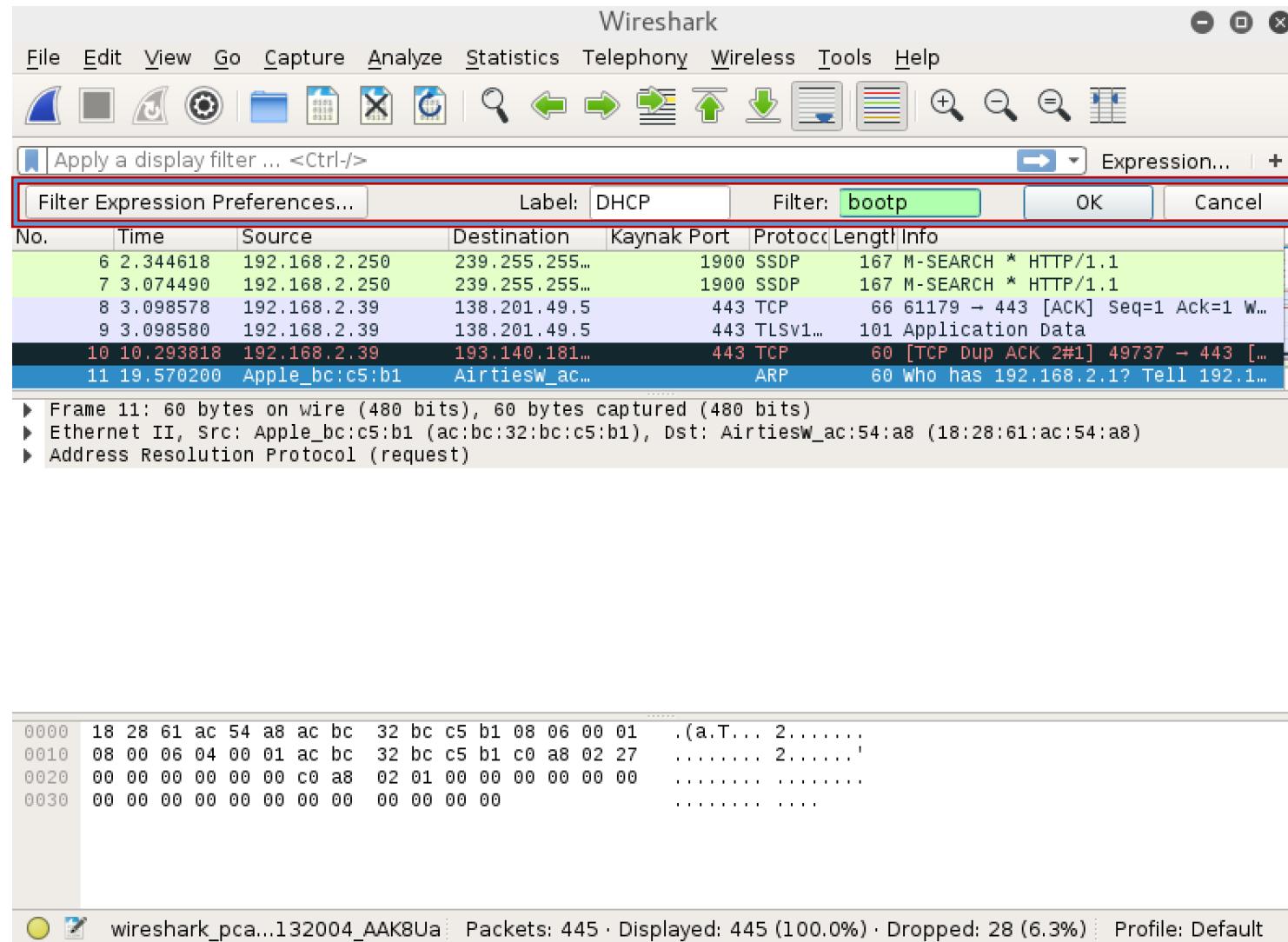


Filtreleme butonu eklemek için ilk olarak + butonuna basıyoruz.

NOT

Sürekli kullandığımız ve özellikle uzun filtreler için_filtreleme butonu oluşturarak her seferinde bunu yazma zahmetinden kurtularak işimizi tek buton ile halledebiliriz.

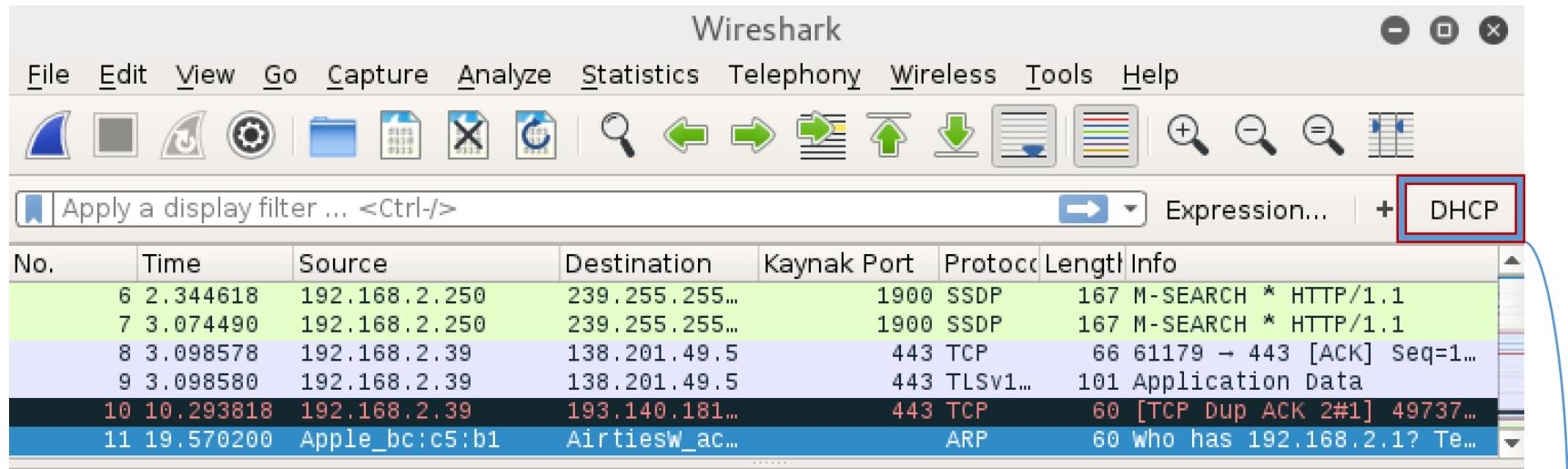
Filtreleme Butonu Oluşturmak



+ tuşuna bastıktan sonra bu menü açılmaktadır.

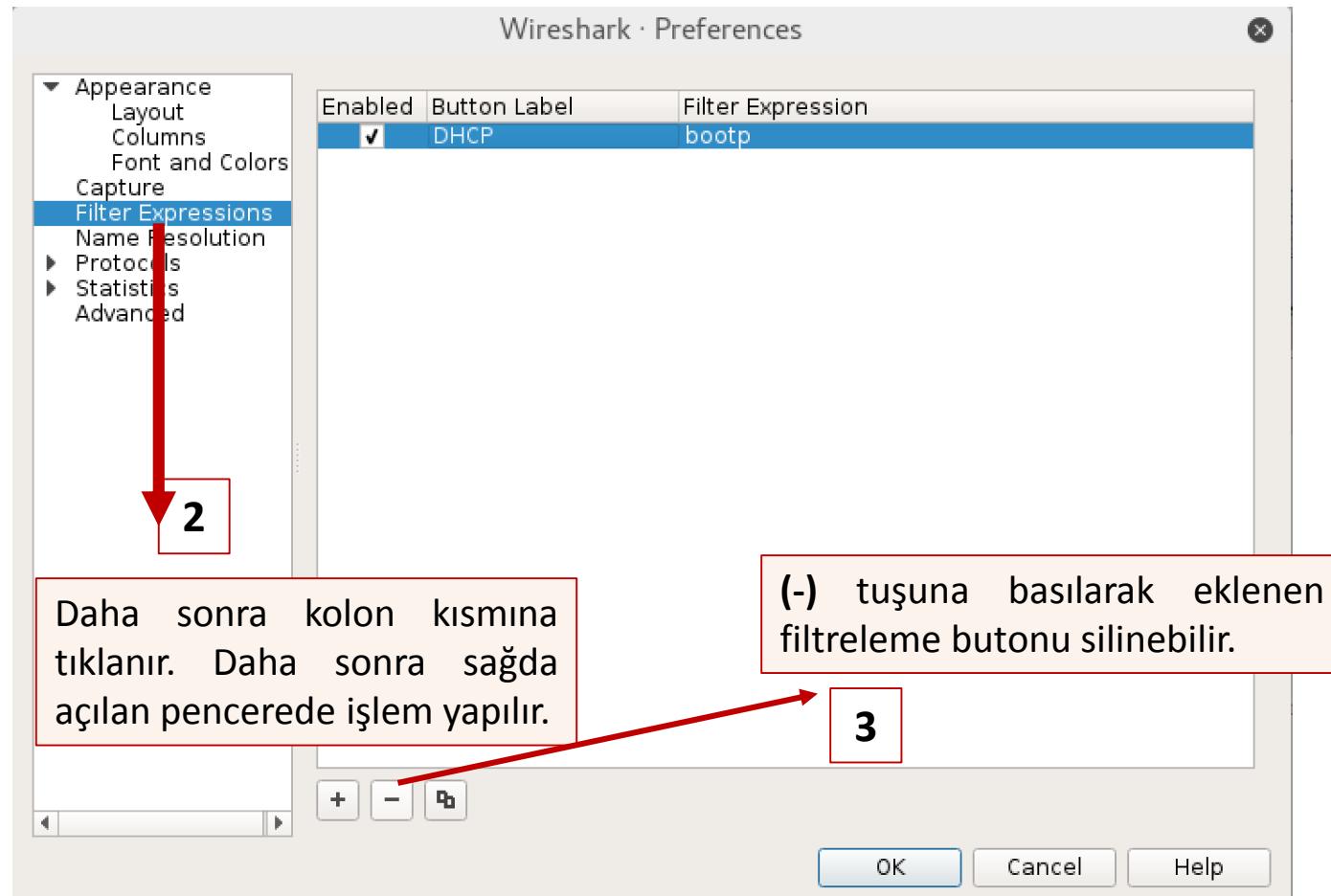
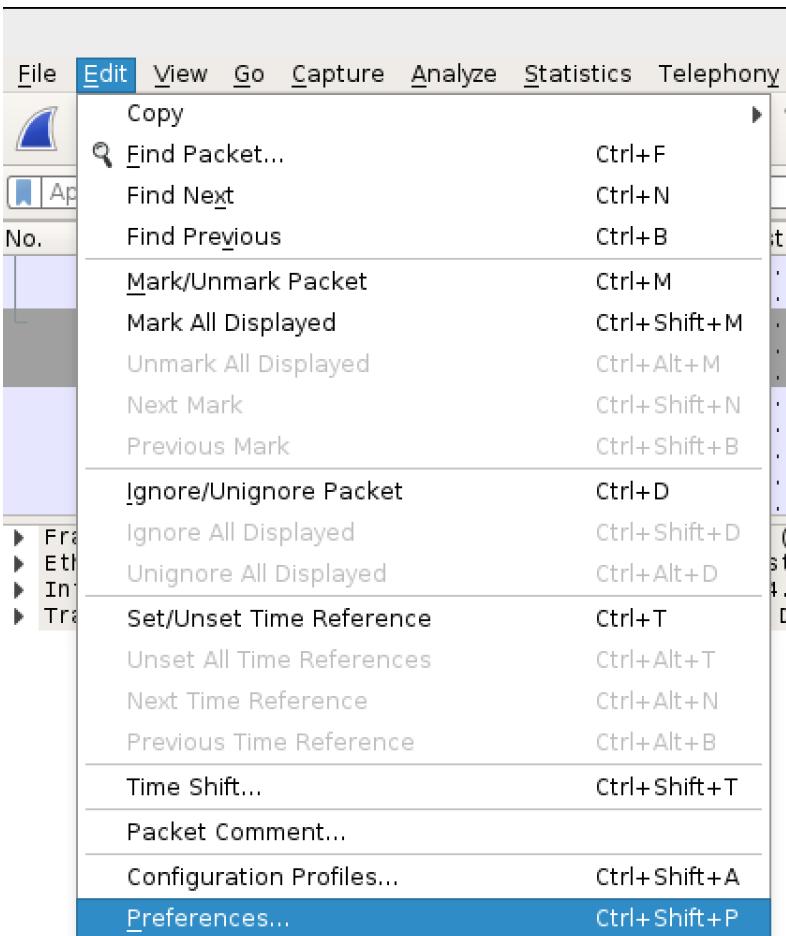
Açılan menüde filtrelemeler için kullanabileceğiniz butonun ismi ve filtreleme seçeneğini yazacağınız böлüm̄ler bulunmaktadır.

Filtreleme Butonu Oluşturmak



Yapılan işlemler sonunda görünüm kutucuk içine alınan kısım gibi olacaktır. Artık **DHCP** isminde ve **dhcp paketlerini** filtreleyen bir **filtreleme butonumuz** olmuştur.

Filtreleme Butonu Silmek



1

ilk olarak **Edit -> Preferences** yolunu takip
sağ tarafta bulunan pencerenin açılmasını sağlıyoruz. (Kısa yolu = **Ctrl + Shift + P**)

Özel Olarak Kolon Eklemek

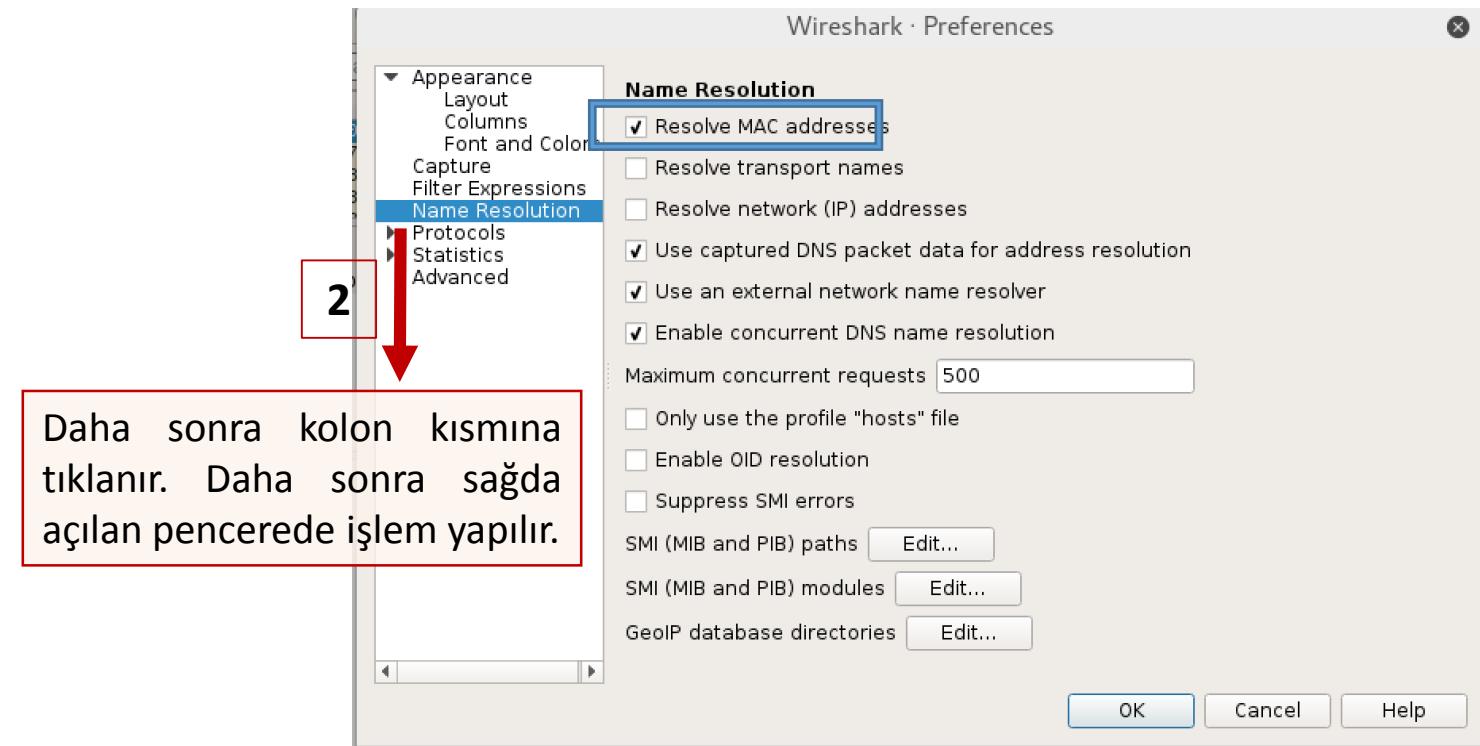
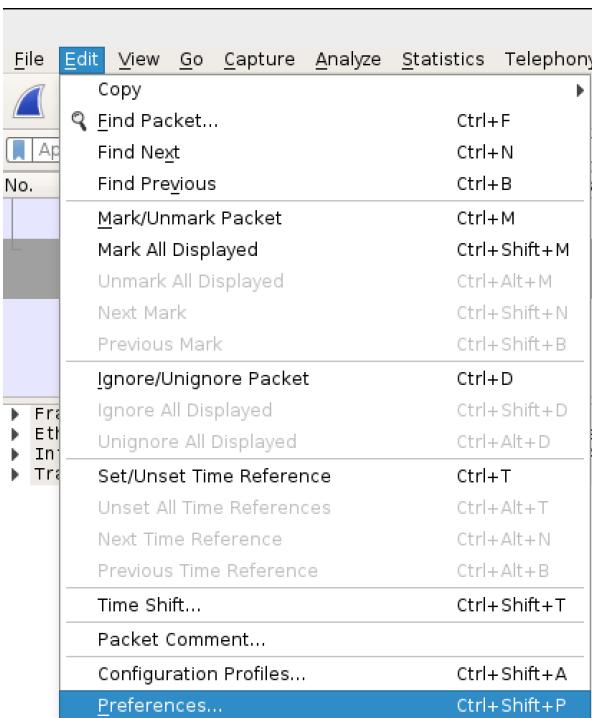
The screenshot shows the Wireshark interface. On the left, the 'Edit' menu is open, with 'Preferences...' highlighted. A red arrow labeled '1' points from the 'Preferences...' option to a callout box at the bottom left. The main window shows the 'Wireshark · Preferences' dialog. In the 'Columns' section of the tree view, a red arrow labeled '2' points to the 'Title' column header. A red box highlights the 'Title' column header. A red arrow labeled '3' points from the 'Title' column header to a callout box on the right containing explanatory text.

1 ilk olarak **Edit -> Preferences** yolunu takip
sağ tarafta bulunan pencerenin açılmasını sağlıyoruz. (Kısa yolu = **Ctrl + Shift + P**)

2 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.

Wireshark – Adres Çözümlemenin Aktif Edilmesi



Daha sonra kolon kısmına tıklanır. Daha sonra sağda açılan pencerede işlem yapılır.

ilk olarak **Edit -> Preferences** yolunu takip sağ tarafta bulunan pencerenin açılmasını sağlıyoruz. (Kısa yolu = **Ctrl + Shift + A**)

Bu örnek için sadece MAC adresleri için adres çözümlemesini aktifleştirdik. Bu sayede artık MAC adreslerinin ilk 24 biti çözümlenecek ve üretici firmayı trafik içerisinde görebileceğiz.

Wireshark – Adres Çözümlemeyi Aktif Edilmesi

The screenshot shows two windows side-by-side. On the left is a terminal window titled 'root@kali: /usr/share/wireshark' with the following command history:

```
root@kali:~# whereis wireshark
wireshark: /usr/bin/wireshark /etc/wireshark /usr/share/wireshark /usr/
share/man/man1/wireshark.1.gz
root@kali:~# cd /usr/share/wireshark/
root@kali:/usr/share/wireshark#
```

On the right is a Wireshark configuration file window titled 'manuf /usr/share/wireshark'. It lists various manufacturer names and their corresponding hex codes. The file is a plain text file with the following content:

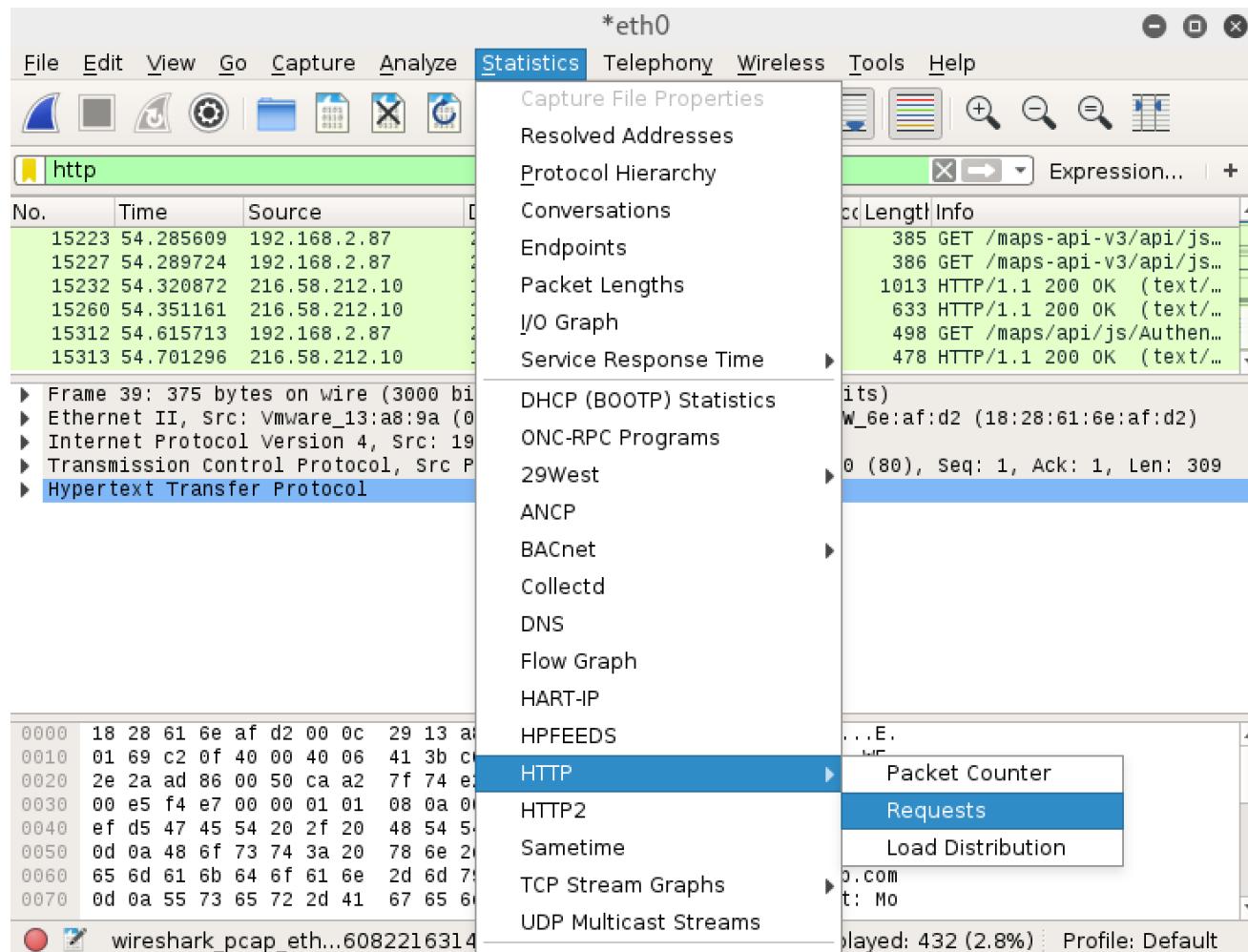
Hex Address	Manufacturer Name	Description
00:00:2A	Trw-Sedd	# TRW - SEDD/INP
00:00:2B	CrispAut	# CRISP AUTOMATION, INC
00:00:2C	Autotote	# AUTOTOTE LIMITED
00:00:2D	Chromati	# CHROMATICS INC
00:00:2E	SocieteE	# SOCIETE EVIRA
00:00:2F	Timeplex	# TIMEPLEX INC.
00:00:30	VgLabora	# VG LABORATORY SYSTEMS LTD
00:00:31	QpsxComm	# QPSX COMMUNICATIONS, LTD.
00:00:32	MarconiP	# Marconi plc
00:00:33	EganMach	# EGAN MACHINERY COMPANY
00:00:34	NetworkR	# NETWORK RESOURCES CORPORATION
00:00:35	Spectrag	# SPECTRAGRAPHICS CORPORATION
00:00:36	AtariCor	# ATARI CORPORATION
00:00:37	OxfordMe	# OXFORD METRICS LIMITED
00:00:38	CssLabs	# CSS LABS
00:00:39	ToshibaC	# TOSHIBA CORPORATION
00:00:3A	ChyronCo	# CHYRON CORPORATION
00:00:3B	IControl	# i Controls, Inc.
00:00:3C	Auspek	# AUSPEK SYSTEMS INC.
00:00:3D	AT&T	
00:00:3E	Simpact	# SIMPACT
00:00:3F	Syntrex	# SYNTREX, INC.
00:00:40	Applicon	# APPLICON, INC.
00:00:41	IceCorpo	# ICE CORPORATION
00:00:42	MetierMa	# METIER MANAGEMENT SYSTEMS LTD.
00:00:43	MicroTec	# MICRO TECHNOLOGY
00:00:44	Castelle	# CASTELLE CORPORATION
00:00:45	FordAero	# FORD AEROSPACE & COMM. CORP.
00:00:46	TCR PR	

Peki wireshark bu adres çözümlemeyi nasıl yapıyor ?



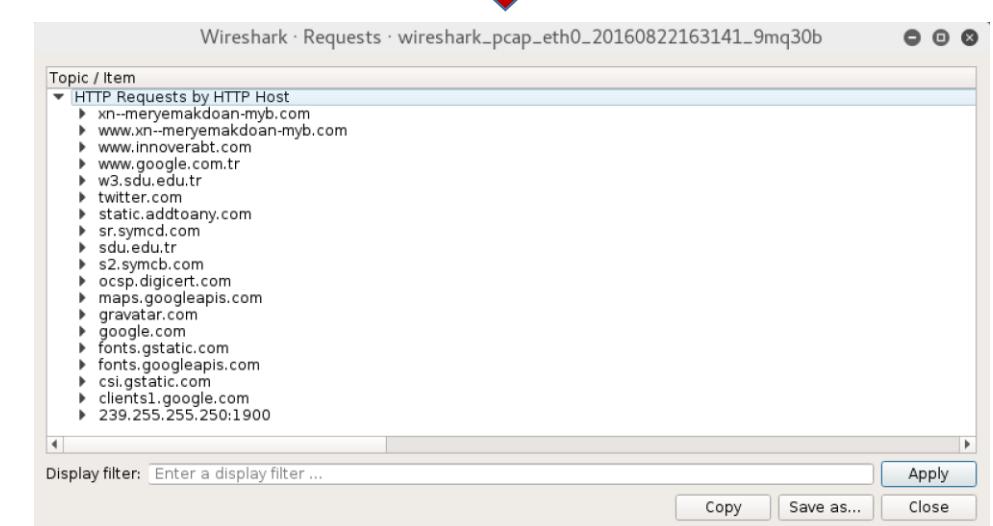
Wireshark içerisinde bulunan manuf isimli dosyayı sürekli güncellendirmekte ve bu dosyayı kullanarak adres çözümlerimeleri gerçekleştirmektedir.

HTTP İsteklerinin Analiz Edilmesi



1 Statistics -> HTTP -> Requests yolunu takip ederek ziyaret edilen ve web site istatistiklerini görebilirsiniz.

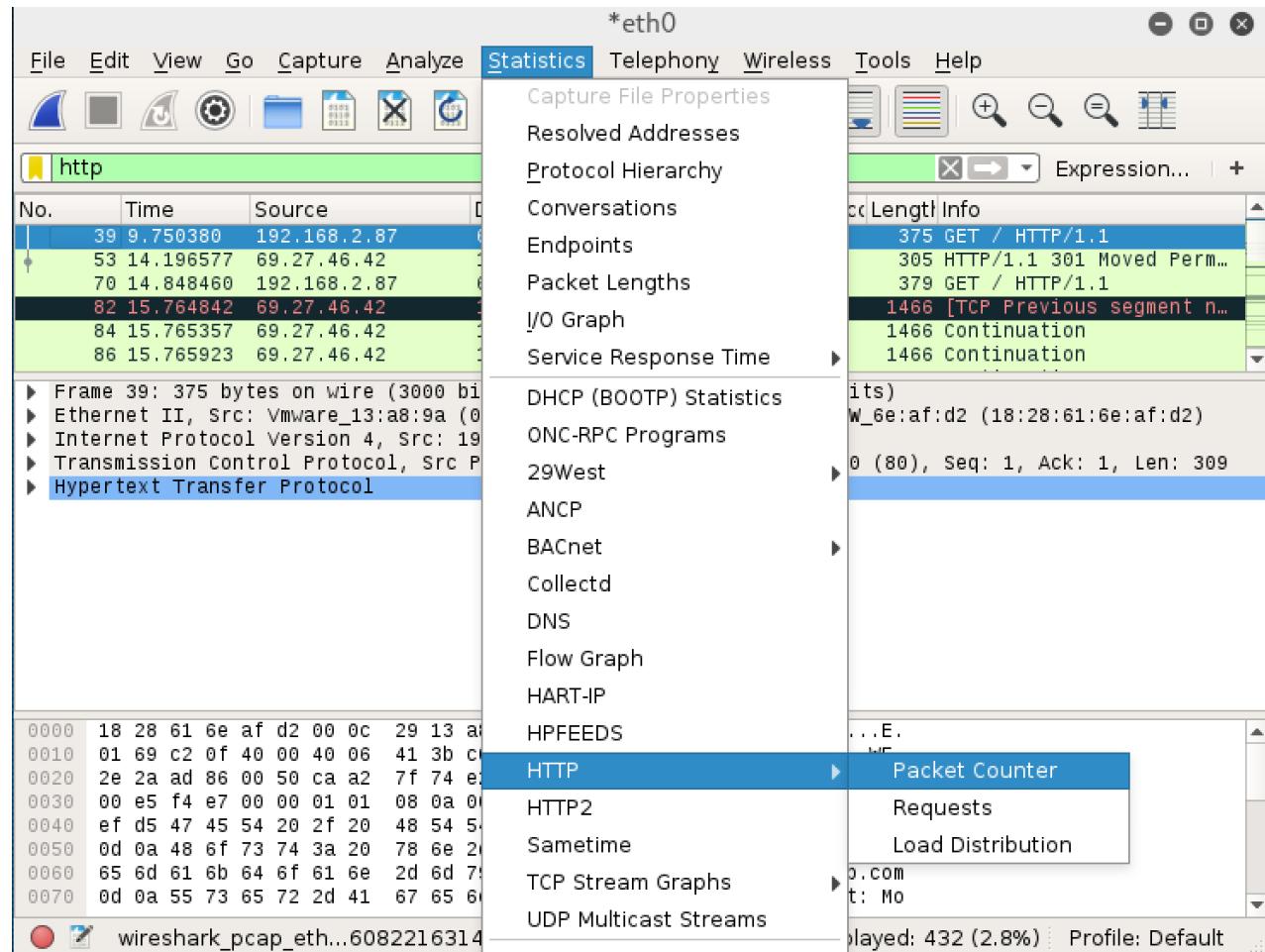
1



2 Bu kısımda url üzerine tıklayarak o url adresine ait trafiği ve yüklenme aşamalarını görebilirsiniz.

2

HTTP İsteklerinin Analiz Edilmesi



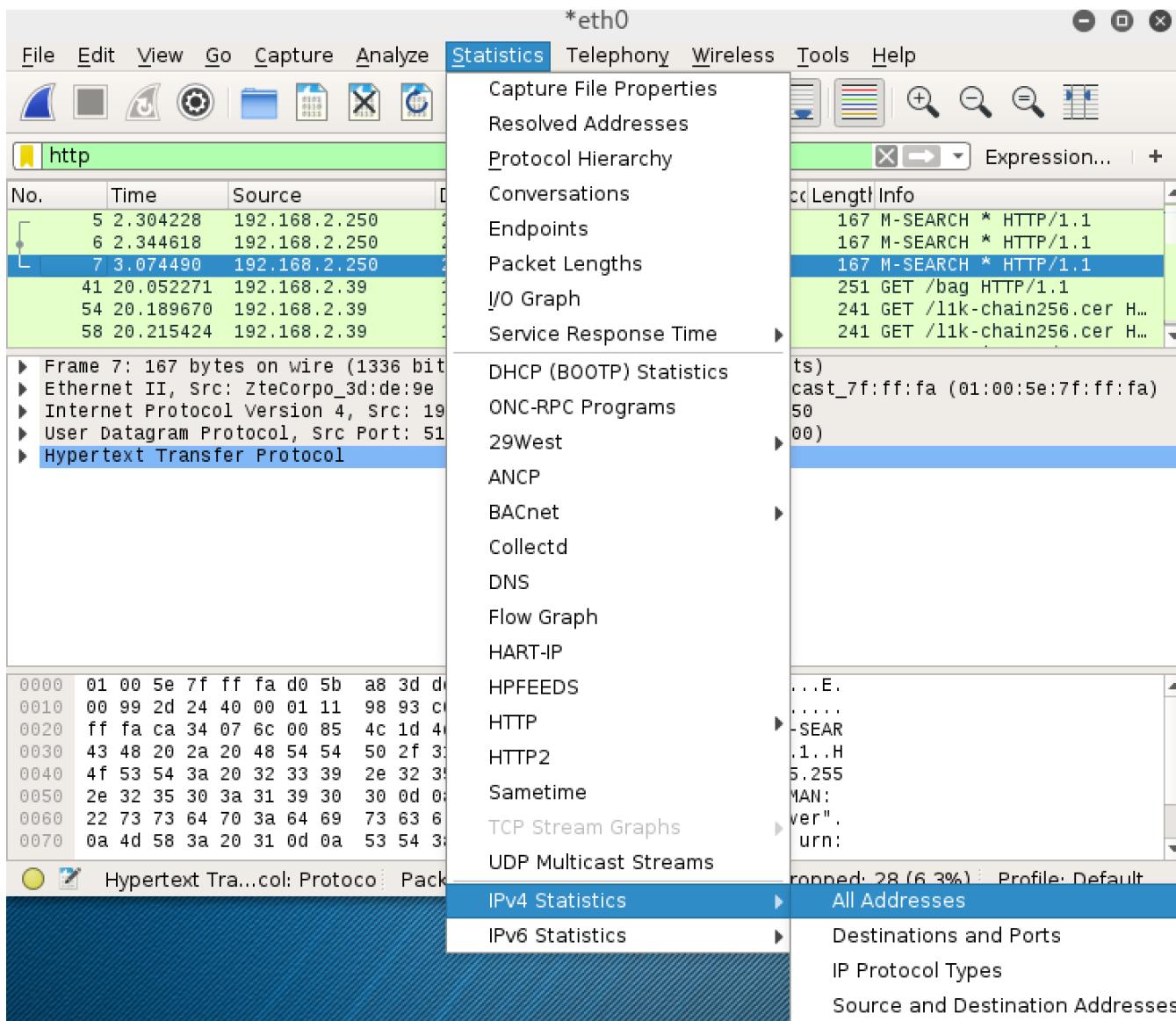
1 Statistics -> HTTP -> Packet Counter yolunu takip ederek HTTP Response Packet durumlarını analiz edebilirsiniz.

The screenshot shows the "Packet Counter" dialog box from Wireshark, displaying the following data:

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Total HTTP Packets	369	0.0082	100%	0.3000	15.879			
Other HTTP Packets	73	0.0016	19.78%	0.2200	15.956			
▼ HTTP Response Packets	105	0.0023	28.46%	0.0800	48.903			
???: broken	0	0.0000	0.00%	-	-			
5xx: Server Error	0	0.0000	0.00%	-	-			
4xx: Client Error	0	0.0000	0.00%	-	-			
► 3xx: Redirection	5	0.0001	4.76%	0.0100	14.197			
► 2xx: Success	100	0.0022	95.24%	0.0800	48.903			
► 1xx: Informational	0	0.0000	0.00%	-	-			
▼ HTTP Request Packets	191	0.0042	51.76%	0.0900	44.204			
SEARCH	8	0.0002	4.19%	0.0100	32.692			
POST	10	0.0002	5.24%	0.0200	23.672			
NOTIFY	8	0.0002	4.19%	0.0800	44.204			
GET	165	0.0037	86.39%	0.0900	48.838			

2 Bu kısımda HTTP cevap kodlarına ait istatistikleri görebilirsiniz. Örnek olarak • GET kullanılan 165 http isteği varmış

IP Adreslerinin Analiz Edilmesi



1 Statistics -> IPv4 Statistics -> All Addresses yolunu takip ederek IP adres istatistiklerinin bulunduğu kısma erişebiliriz.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
All Addresses	401	0.0104	100%	0.2500	22.057			
104.209.190.8	1	0.0000	0.25%	0.0100	0.000			
149.154.167.91	1	0.0000	0.25%	0.0100	21.746			
17.188.139.157	1	0.0000	0.25%	0.0100	20.700			
224.0.0.2	1	0.0000	0.25%	0.0100	20.647			
17.172.232.214	2	0.0001	0.50%	0.0200	21.774			
17.188.161.18	2	0.0001	0.50%	0.0200	22.358			
193.140.181.27	2	0.0001	0.50%	0.0100	0.224			
23.102.4.253	2	0.0001	0.50%	0.0100	1.651			
0.0.0.0	3	0.0001	0.75%	0.0100	19.570			
74.125.133.109	3	0.0001	0.75%	0.0200	20.190			
74.125.140.109	3	0.0001	0.75%	0.0100	20.030			
192.168.2.255	4	0.0001	1.00%	0.0200	21.554			
192.168.2.87	4	0.0001	1.00%	0.0200	24.668			
216.58.213.68	4	0.0001	1.00%	0.0200	21.497			
255.255.255.255	4	0.0001	1.00%	0.0100	19.570			
138.201.49.5	6	0.0002	1.50%	0.0200	3.099			
105.175.11.251	6	0.0002	1.50%	0.0500	20.124			

2 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.

Wireshark Protocol Hierarchy

The screenshot shows the Wireshark interface with the 'Statistics' menu open. The 'Protocol Hierarchy' option is highlighted. A blue arrow points from this menu item to the corresponding section in the second screenshot.

Statistics **Protocol Hierarchy**

No. Time Source

6625	47.70381...	104.31.69.117
6626	47.70384...	192.168.2.87
6627	47.71127...	192.168.2.87
6628	47.82387...	104.31.69.117
6629	48.09185...	192.168.2.87
6630	48.13189...	216.58.212.46
6631	48.21617...	192.0.80.242

Frame 1: 98 bytes on wire (784 bits)
Ethernet II, Src: VMware_13:a8:9a (00:0c:29:13:a8:9a), Dst: 00:0c:29:13:a8:9a (192.168.2.87)
Internet Protocol Version 4, Src: 192.168.2.87
Internet Control Message Protocol

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

Wireshark · Protocol Hierarchy Statistics · wireshark_pcappng_eth0_20160823095708_iYNyzz

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End
Frame	100.0	6657	100.0	4467819	739 k	0	0
Ethernet	100.0	6657	100.0	4467819	739 k	0	0
Internet Protocol Version 6	0.0	2	0.0	244	40	0	0
Internet Protocol Version 4	99.8	6643	100.0	4466963	738 k	0	0
User Datagram Protocol	3.9	261	0.7	30370	5023	0	0
Transmission Control Protocol	94.5	6288	99.1	4427533	732 k	4145	200
Secure Sockets Layer	31.1	2073	53.7	2401320	397 k	1996	230
NetBIOS Session Service	0.0	3	0.0	484	80	0	0
Malformed Packet	0.2	13	0.4	18460	3053	13	1846
Hypertext Transfer Protocol	1.7	115	1.5	67786	11 k	80	451
Portable Network Graphics	0.0	2	0.0	1733	286	2	173
Online Certificate Status Protocol	0.4	27	0.4	18032	2982	27	180
Line-based text data	0.1	5	0.1	2297	379	5	229
JavaScript Object Notation	0.0	1	0.0	585	96	1	585
Data	0.2	16	0.5	23734	3926	16	237
Internet Group Management Protocol	0.1	4	0.0	240	39	4	240
Internet Control Message Protocol	1.4	90	0.2	8820	1458	90	882
Address Resolution Protocol	0.2	12	0.0	612	101	12	612

Wireshark · Protocol Hierarchy Statistics · wireshark_pcappng_eth0_201

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	6657	100.0
Ethernet	100.0	6657	100.0
Internet Protocol Version 6	0.0	2	0.0
Internet Protocol Version 4	99.8	6643	100.0
User Datagram Protocol	3.9	261	0.7
Transmission Control Protocol	94.5	6288	99.1
Secure Sockets Layer	31.1	2073	53.7
NetBIOS Session Service	0.0	3	0.0
Malformed Packet	0.2	13	0.4
Hypertext Transfer Protocol	1.7	115	1.5
Portable Network Graphics	0.0	2	0.0
Online Certificate Status Protocol	0.4	27	0.4
Line-based text data	0.1	5	0.1
JavaScript Object Notation	0.0	1	0.0
Data	0.2	16	0.5
Internet Group Management Protocol	0.1	4	0.0
Internet Control Message Protocol	1.4	90	0.2
Address Resolution Protocol	0.2	12	0.0

Apply as Filter ▾ Selected

Prepare a Filter ▾ Not Selected

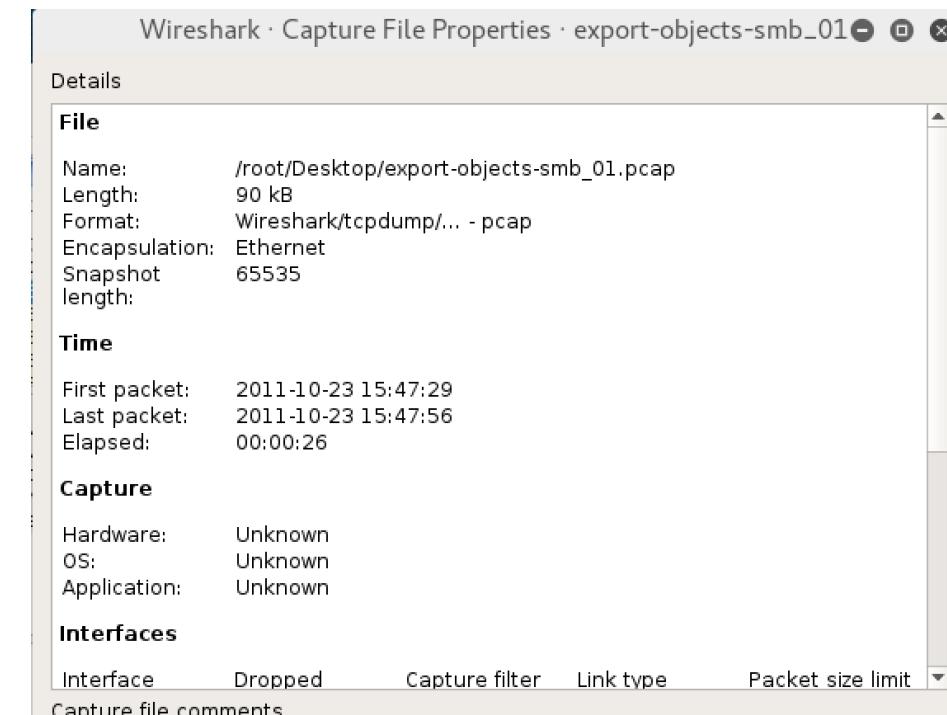
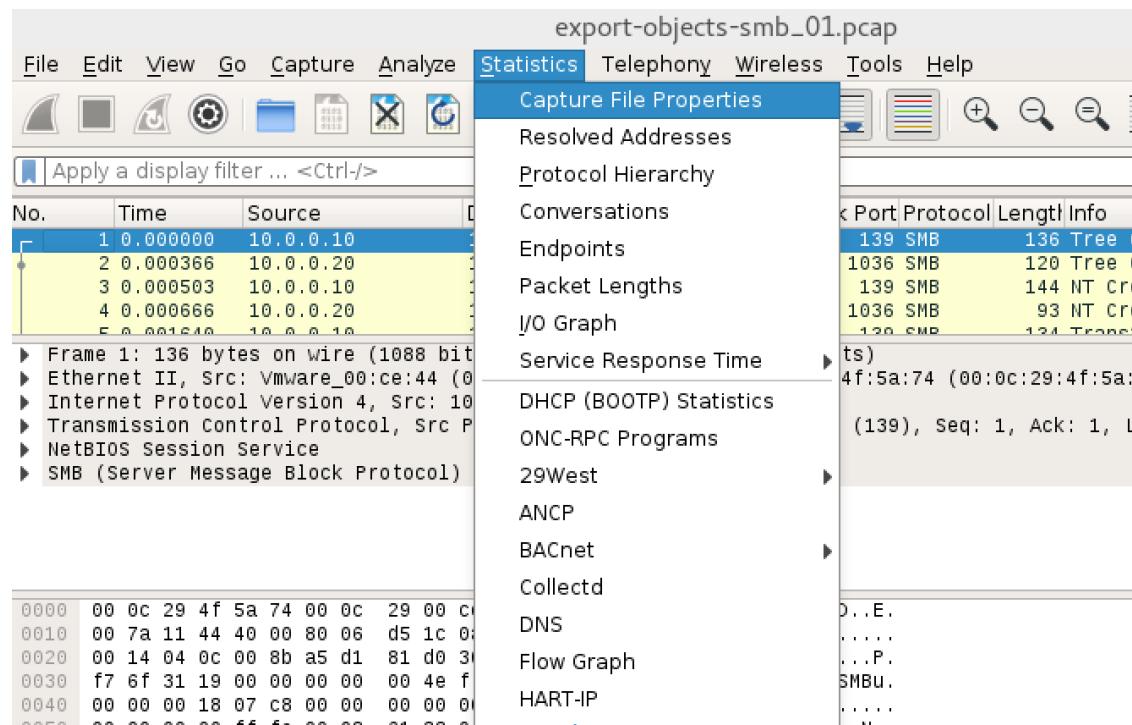
Find ...and Selected

Colorize ...or Selected

Copy as CSV ...and not Selected

Copy as YAML ...or not Selected

Wireshark - Capture File Properties

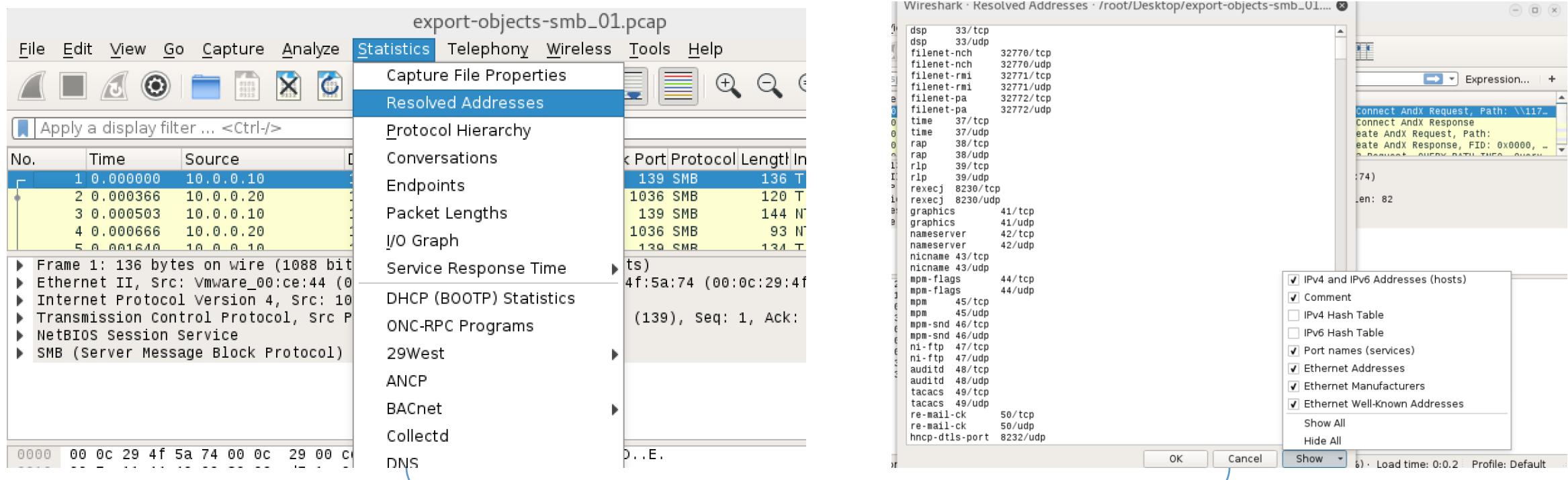


Yakalanan paket hakkında özet bilgiler elde etmek istersek
Statistics -> Capture File Properties yolunu takip etmemiz yeterli olacaktır.

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

arp.duplicate-address-frame

No.	Time	Source	Destination	Kaynak Port	Protocol	Length	Info
6264	237.712846	HonHaiPr_26:10:99	Tp-LinkT_17:ed:b3		ARP	42	Who has 192.168.1.37? Tell 192.168.1.1 (dup...)
6265	237.712880	Tp-LinkT_17:ed:b3	HonHaiPr_26:10:99		ARP	42	192.168.1.37 is at c4:6e:1f:17:ed:b3 (dupli...
6267	237.712903	HonHaiPr_26:10:99	Tp-LinkT_17:ed:b3		ARP	42	192.168.1.1 is at e0:06:e6:26:10:99
6469	243.483471	HonHaiPr_26:10:99	Tp-LinkT_17:ed:b3		ARP	42	Who has 192.168.2.177? Tell 192.168.2.1 (du...

Frame 6264: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: HonHaiPr_26:10:99 (e0:06:e6:26:10:99), Dst: Tp-LinkT_17:ed:b3 (c4:6e:1f:17:ed:b3)
[Duplicate IP address detected for 192.168.1.1 (e0:06:e6:26:10:99) - also in use by f8:3d:ff:89:2a:d6 (frame 5261)]
[Frame showing earlier use of IP address: 5261]
[Seconds since earlier frame seen: 57]
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4

0000 c4 6e 1f 17 ed b3 e0 06 e6 26 10 99 08 06 00 01 .n.....&.....
0010 08 00 06 04 00 01 e0 06 e6 26 10 99 c0 a8 01 01&.....
0020 00 00 00 00 00 00 c0 a8 01 25%.

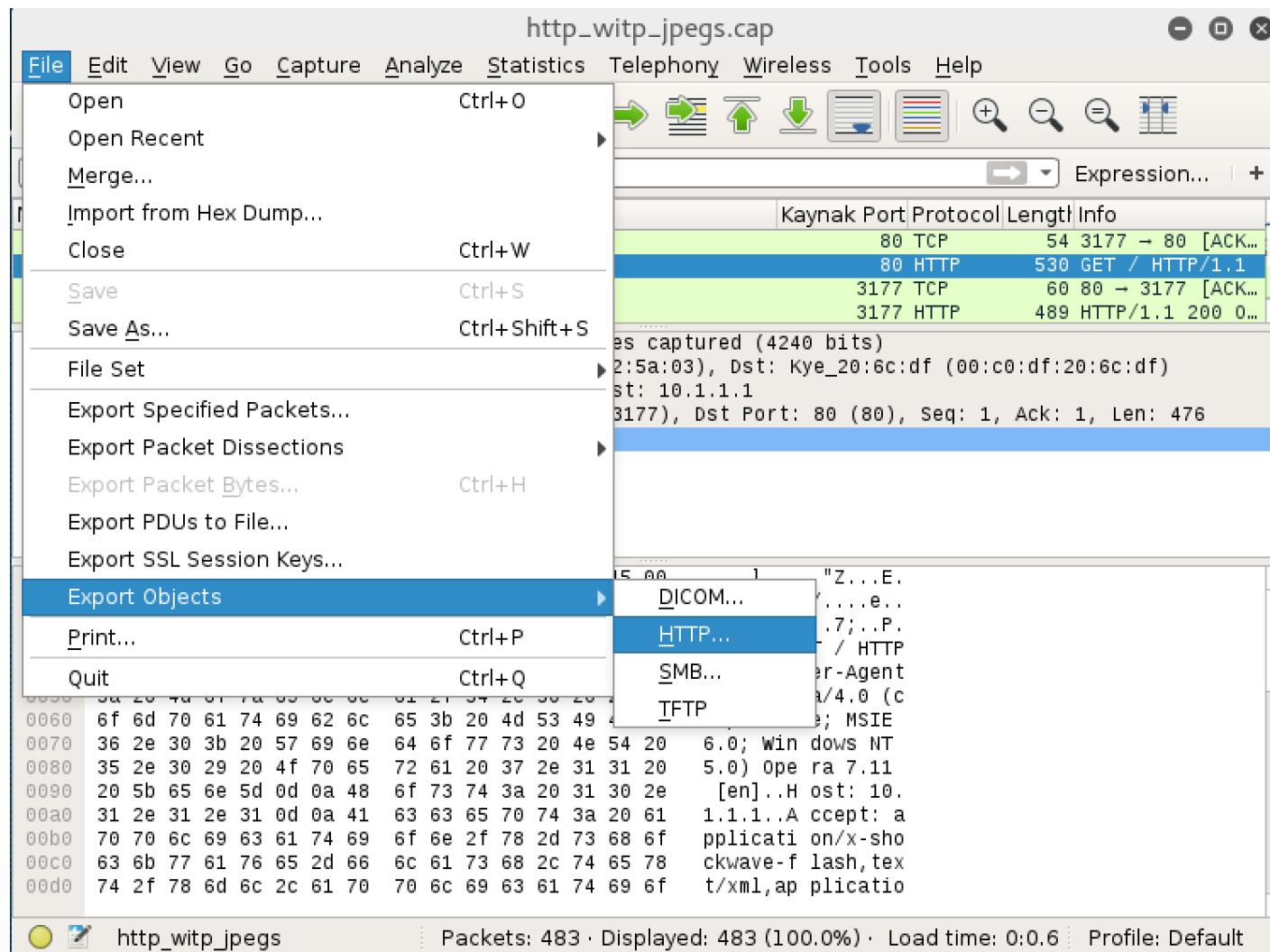
arpctf

Packets: 7485 · Displayed: 11 (0.1%) · Load time: 0:0.49 · Profile: Default

Aşağıda belirtilen filtreleri kullanarak sisteminize yönelik muhtemel ARP saldırısını tespit edebilirsiniz.

- arp.duplicate-address-frame
- arp.duplicate-address-detected

Trafik İçerisindeki Verilerin Export Edilmesi



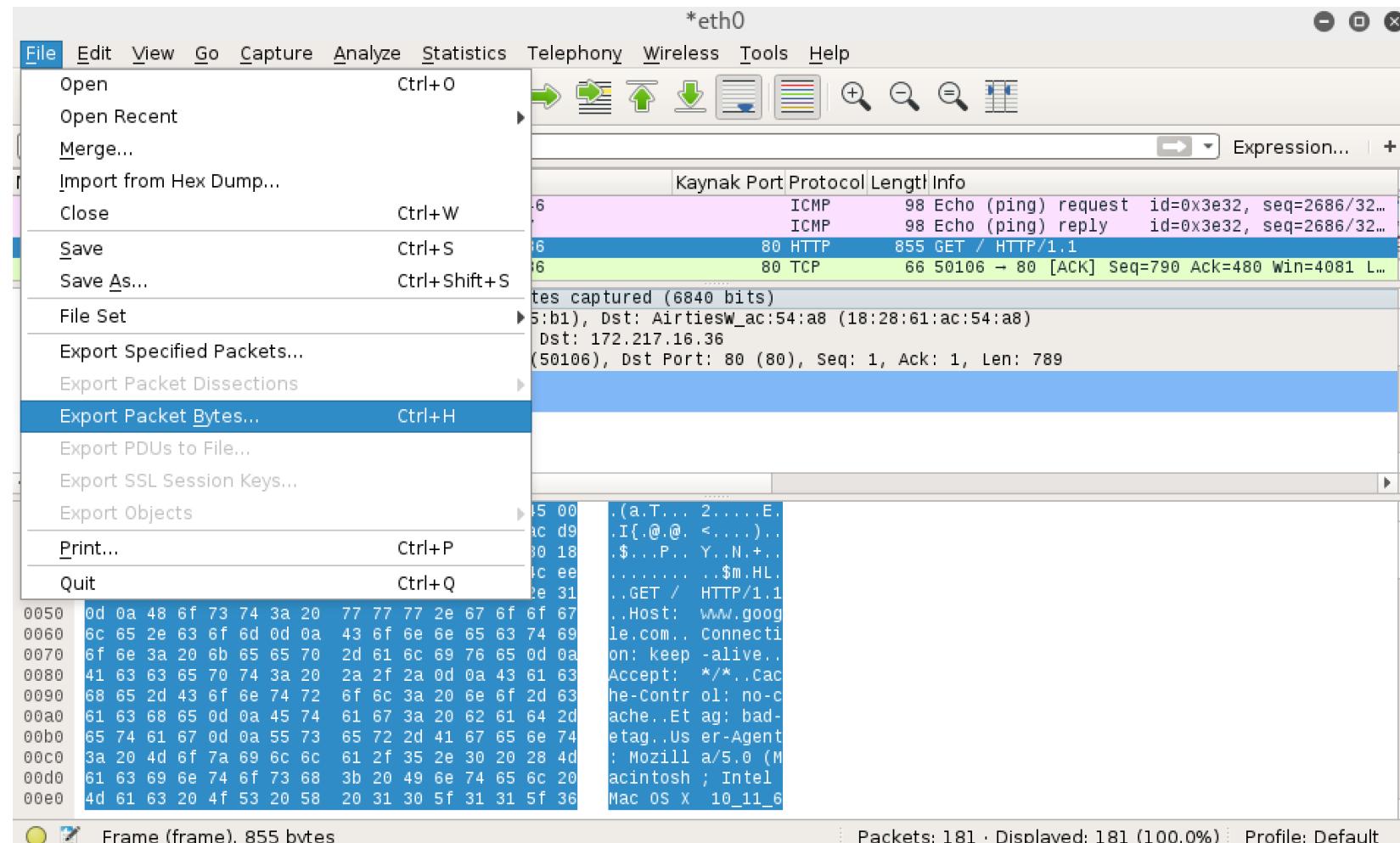
Wireshark ile çalışırken trafik içerisinde geçen bazı objeleri export etmek isteyebilirsiniz. Bunu yapabilmek için:

- **File -> Export Objects** yolunu takip ediyoruz.

A separate dialog box titled "Wireshark · Export · HTTP object list" is shown. It contains a table with columns: Packet, Hostname, Content Type, Size, and Filename. The table lists various files such as index.html, bg2.jpg, sydney.jpg, etc., with their respective details. At the bottom of the dialog are buttons for Save, Save All, Close, and Help.

Packet	Hostname	Content Type	Size	Filename
6	10.1.1.1	text/html	160 bytes	/
16	ins1.opera.com	application/vnd.xacp	433 bytes	xcms.asp
19	ins1.opera.com		5 bytes	xcms.asp
38	10.1.1.1	text/html	4323 bytes	index.html
61	10.1.1.1	image/jpeg	8281 bytes	bg2.jpg
72	10.1.1.1	image/jpeg	9045 bytes	sydney.jpg
100	opera1-servedby.advertising.com		1247 bytes	dst=Win_700
109	opera2-servedby.advertising.com		1247 bytes	dst=Win_700
120	opera4-servedby.advertising.com		1247 bytes	dst=Win_700
137	opera3-servedby.advertising.com		1247 bytes	dst=Win_700
159	10.1.1.1	text/html	416 bytes	dagbok.html
207	opera4-servedby.advertising.com		1136 bytes	bins=1
218	10.1.1.1	text/html	1263 bytes	dagbok.html
230	10.1.1.1	text/html	2232 bytes	dagbok.html
259	10.1.1.1	image/jpeg	8963 bytes	DSC07858.JPG
269	10.1.1.1	image/jpeg	10 kB	DSC07859.JPG
479	10.1.1.1	image/jpeg	191 kB	DSC07858.JPG

Trafik İçerisindeki Paketlerin Export Edilmesi - 1

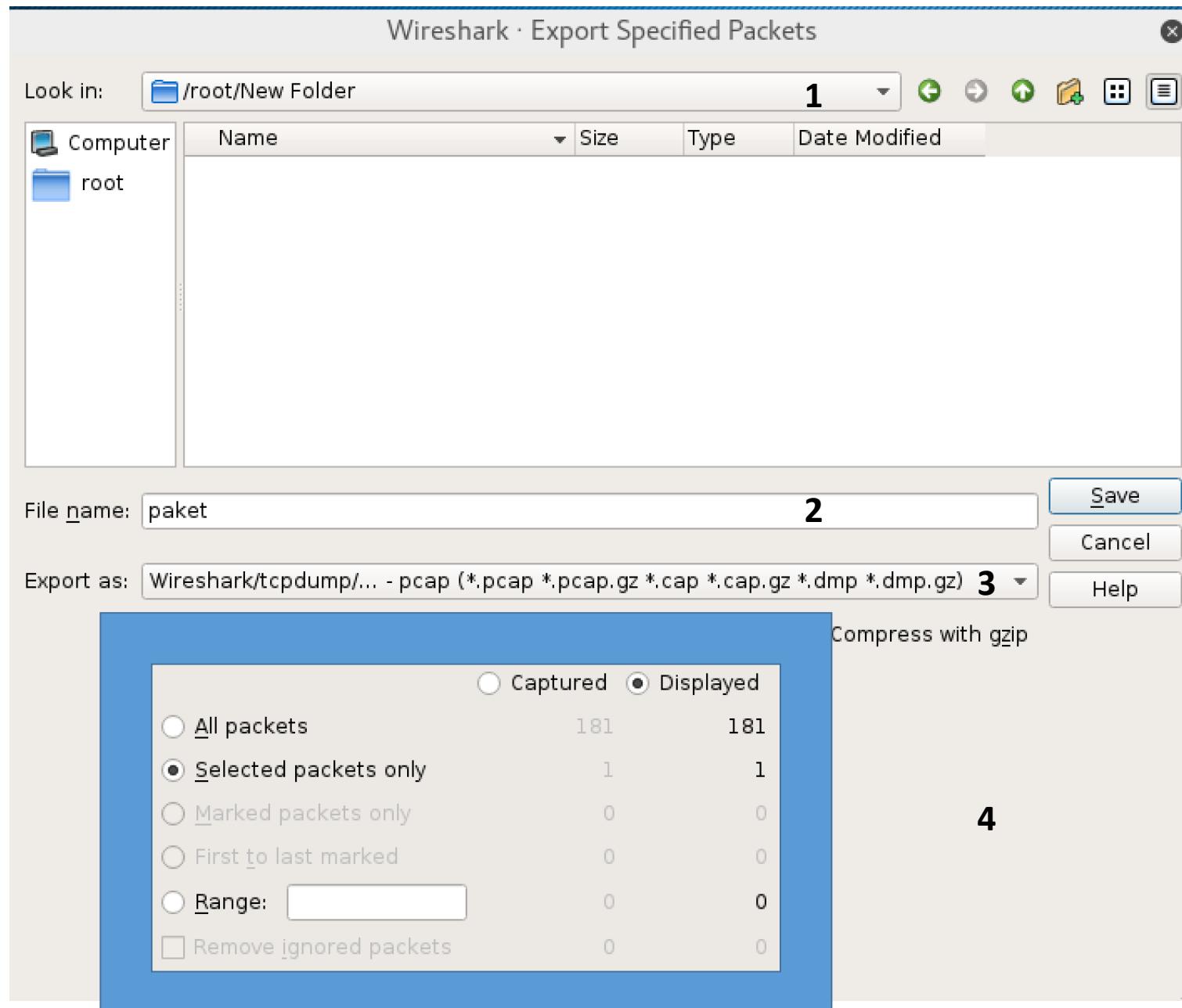


Wireshark ile çalışırken herhangi bir paketi export etmek ve daha sonra incelemek istersek yapmamız gerekenler aslında çok basit.

İlk olarak bir paketin üzerine tıklayıp daha sonra da ;

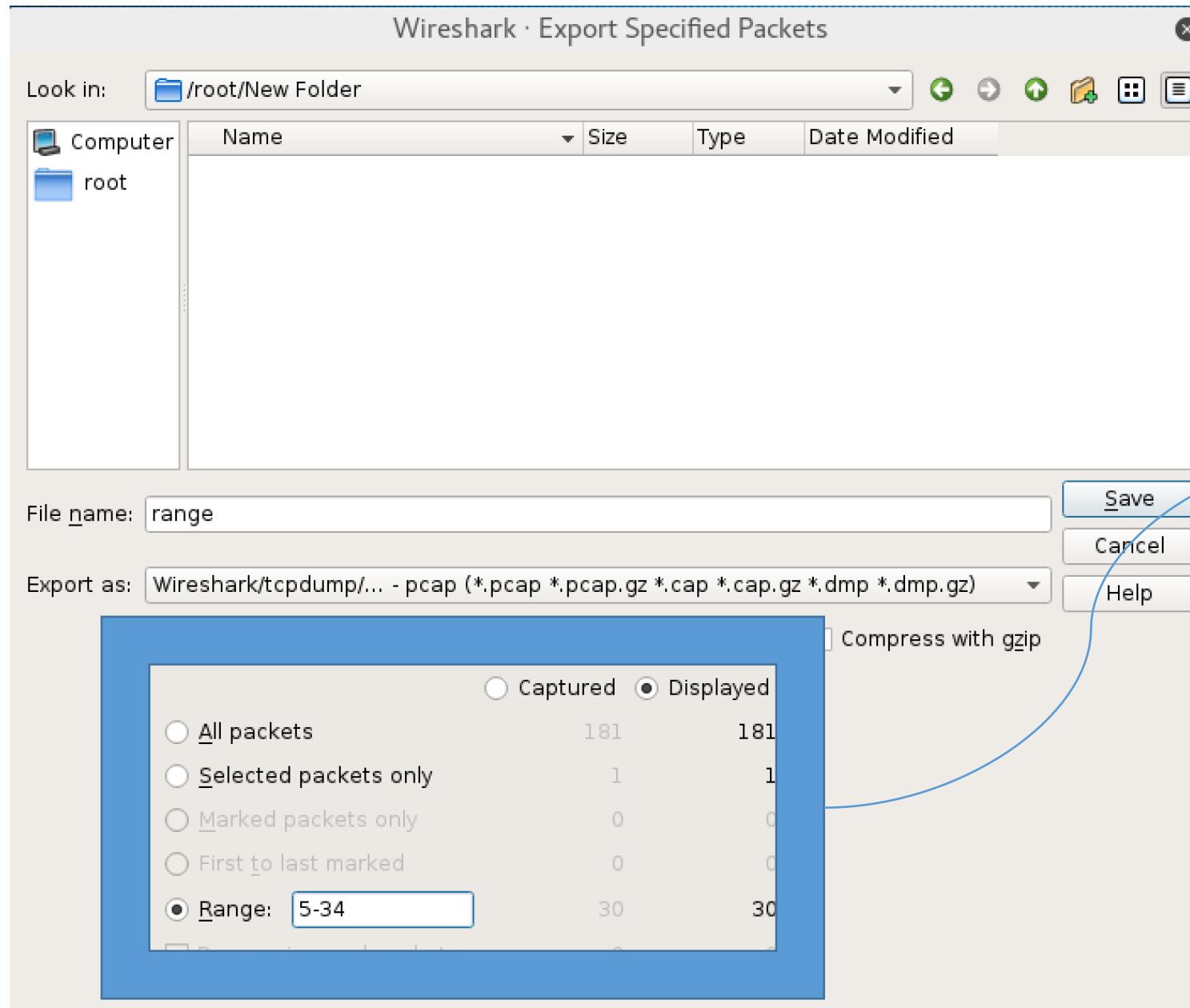
File -> Export Specified Packets yolunu takip ediyoruz.

Trafik İçerisindeki Paketlerin Export Edilmesi - 2



- 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.

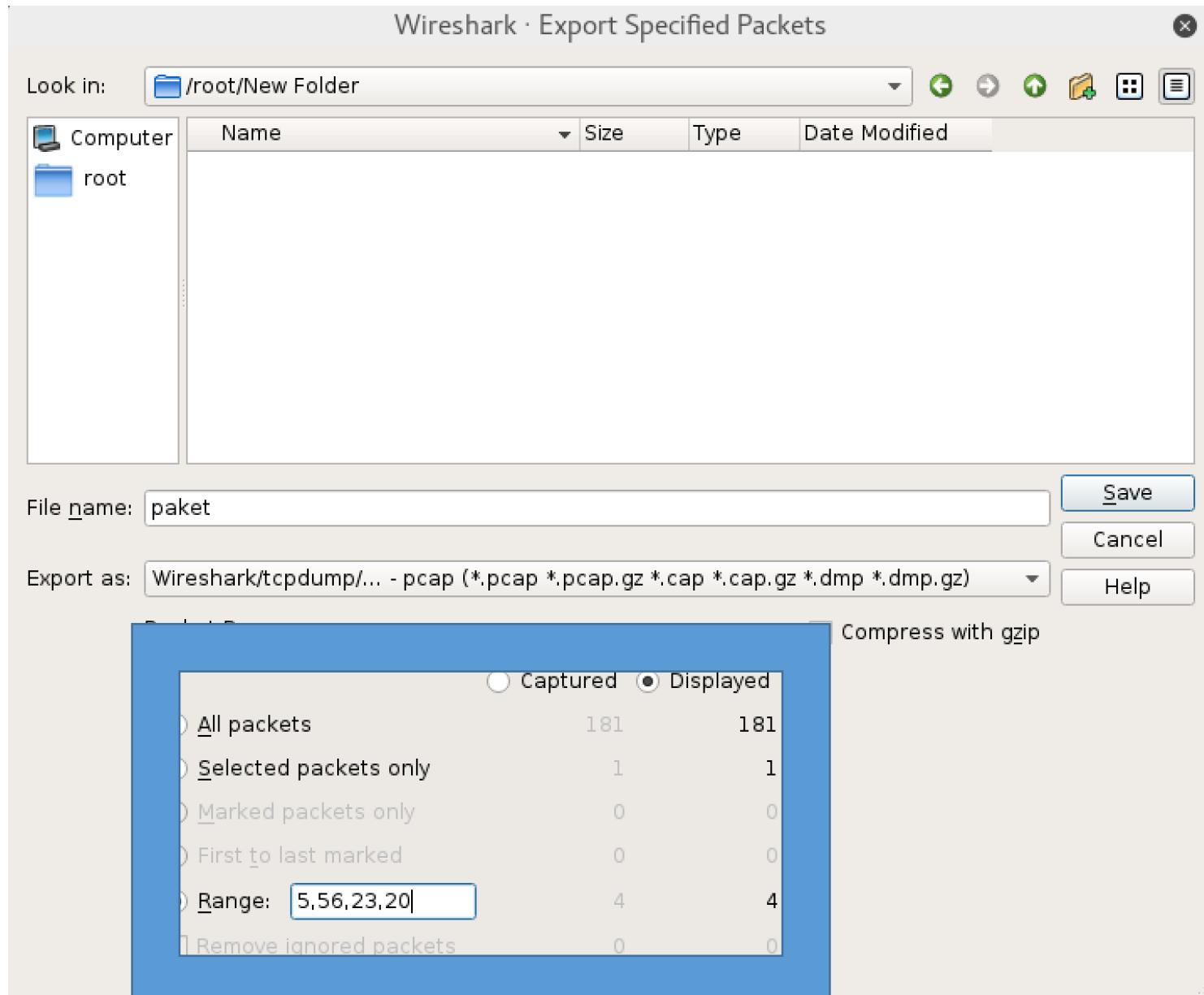
Trafik İçerisindeki Paketlerin Export Edilmesi - 3



Bu seferki süreçte belli aralıkta istediğimiz paketleri daha sonra incelemek için kayıt edeceğiz.

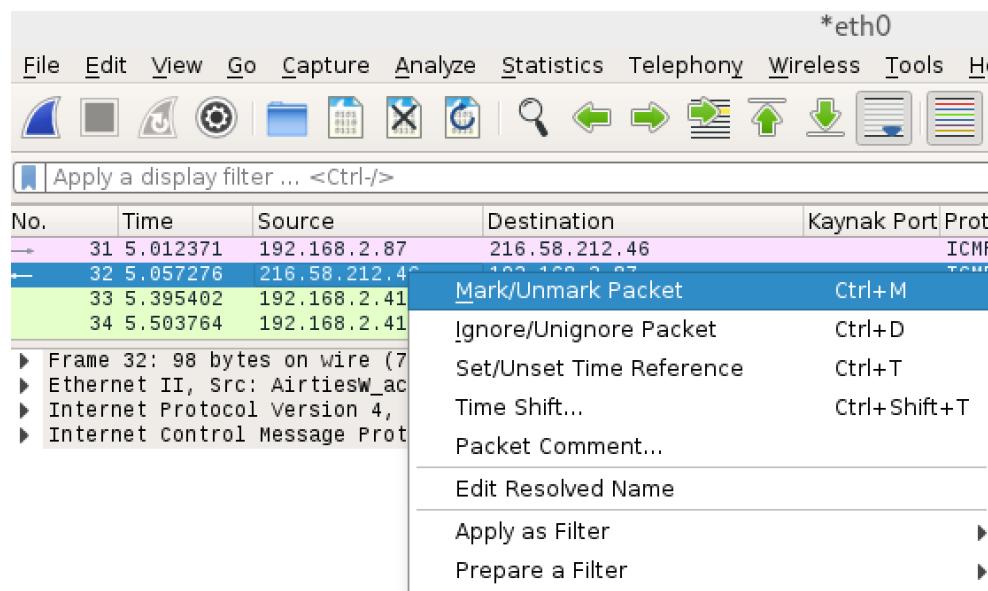
Bunun için kutu içerisinde alınan alanda “**Range**” kısmını seçip istediğimiz aralığı belirtmemiz yeterli olacaktır.

Trafik İçerisindeki Paketlerin Export Edilmesi - 4

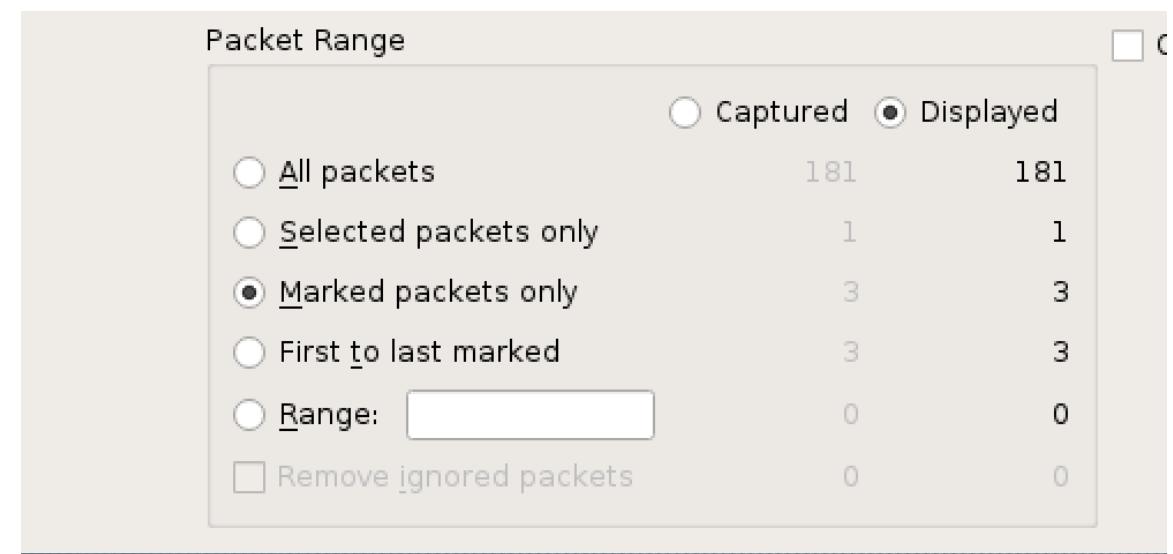


Bu sefer kutu içerisinde alınan alanda “**Range**” kısmını seçip istediğimiz paketlerin numaralarını virgül ile ayırarak belirtmemiz yeterli olacaktır.

Trafik İçerisindeki Paketlerin Export Edilmesi - 5



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



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

Wireshark Dahili Araçlar – Mergecap

```
root@kali: ~/meryemakdogan
File Edit View Search Terminal Help
root@kali:~/meryemakdogan# ls
meryem.txt paket1.pcap paket2.pcap
root@kali:~/meryemakdogan# mergecap -w yenipaket paket1.pcap paket2.pcap
root@kali:~/meryemakdogan# ls
meryem.txt paket1.pcap paket2.pcap yenipaket
root@kali:~/meryemakdogan#
```

Wireshark ile birlikte kurulu gelen mergecap isimli araç iki farklı pcap ve diğer desteklenen dosya ağ trafiği değeri taşıyan dosyayı birleştirebilmektedir.

Wireshark Dahili Araçlar – capinfos

```
root@kali:~/meryemakdогan# capinfos yenipaket
File name:          yenipaket
File type:          Wireshark/... - pcapng
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit:  file hdr: (not set)
Number of packets: 16
File size:          2260 bytes
Data size:          1537 bytes
Capture duration:  59.905903 seconds
First packet time: 2016-08-23 14:41:56.730797
Last packet time:  2016-08-23 14:42:56.636700
Data byte rate:    25 bytes/s
Data bit rate:    205 bits/s
Average packet size: 96.06 bytes
Average packet rate: 0 packets/s
SHA1:              61b1637a0474c3b74f643535e648e371c098f106
RIPEMD160:         0513b4272e89246dac455208e27635f8c5c1da65
MD5:               0f55bee01299897f645878b1841167fa
Strict time order: True
Capture comment:   File created by merging: File1: paket1.pcap File2: paket2.pcap
Capture oper-sys:  Linux 4.3.0-kali1-686-pae
Capture application: mergecap
Number of interfaces in file: 1
Interface #0 info:
  Name = UNKNOWN
  Description = NONE
  Encapsulation = Ethernet (1/1 - ether)
  Speed = 0
  Capture length = 262144
  FCS length = -1
  Time precision = microseconds (6)
  Time ticks per second = 1000000
  Time resolution = 0x06
  Filter string = NONE
  Operating system = UNKNOWN
  Comment = NONE
  BPF filter length = 0
  Number of stat entries = 0
  Number of packets = 16
root@kali:~/meryemakdоган#
```

Elinizde bulunan pcap, cap gibi formatlarda olan wireshark tarafından desteklenen dosyalar hakkında bilgi toplamak amacıyla kullanılabilen ve wireshark ile gelen ek bir araçtır.

Gördüğünüz üzere bu dosyanın **paket1.pcap** ve **paket2.pcap** isimli iki dosyanın birleştirilmesi sonucu olduğunu belirtiyor.