

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 olduđu bilgisayarda;

- Ađ trafiđinin anlık olarak izlenmesini
- İzlenen bu trafiđin kayıt edilmesini
- Daha sonra incelenmesini sađlamaktadır.
- Bunların dıřında bir hatayı çözmek amacı ile de kullanılabilir. (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.

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

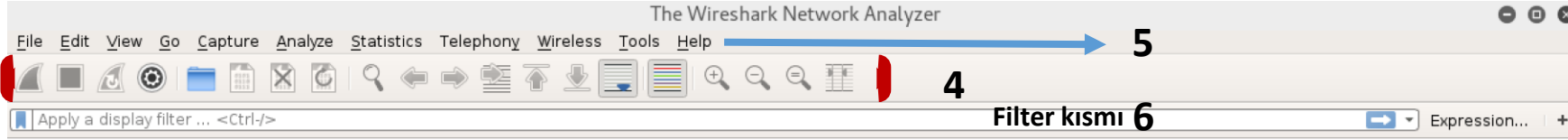
Wireshark aracı için asıl işi yapan kısım:

- 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.

Wireshark Aracının Açılış Arayüzünü Tanıyalım



1) Daha önce açılan dosyalar gösterilmektedir.

2) Ağ trafiğini izlemek amacı ile kullanılabilir ağ kartları gösterilmektedir

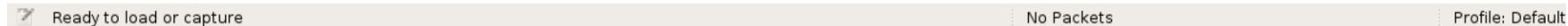
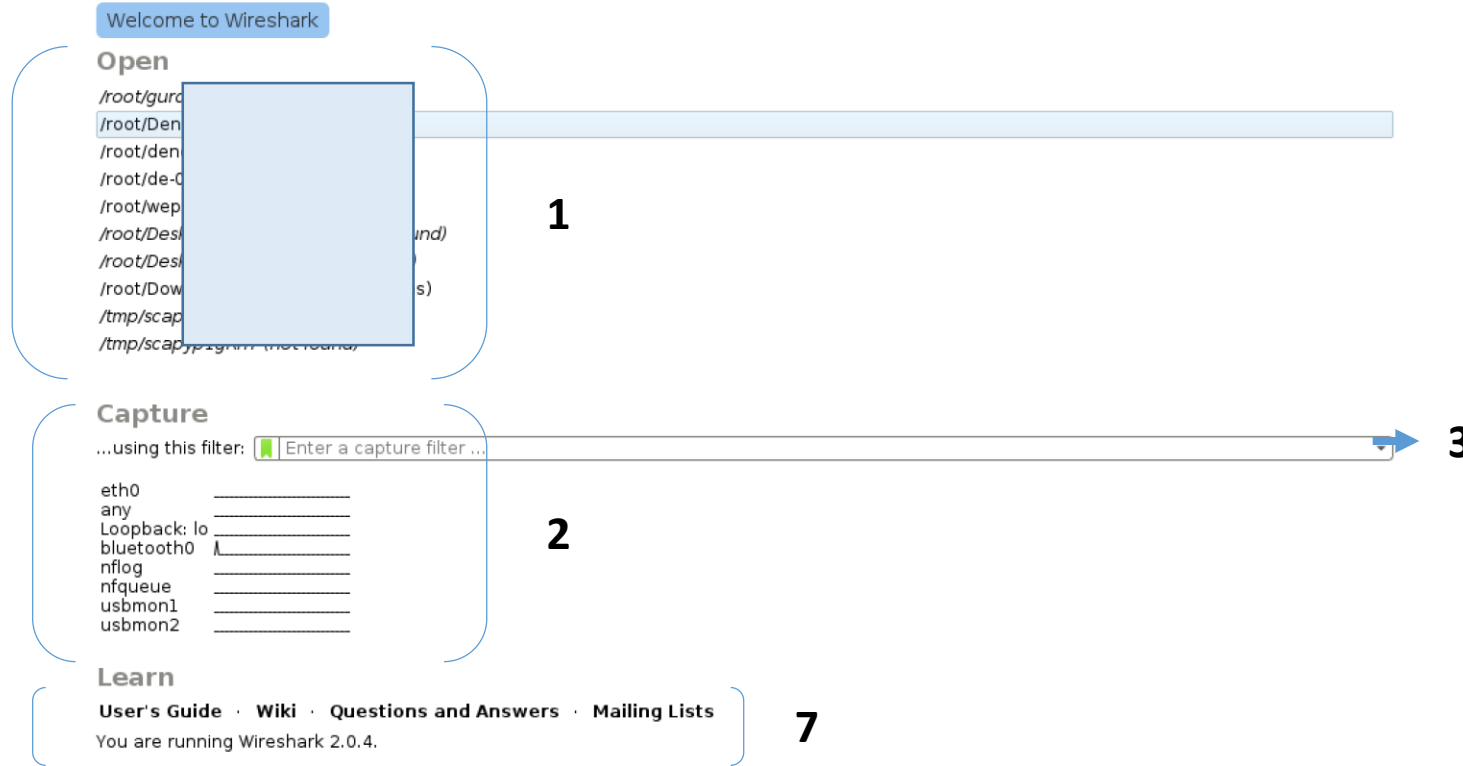
3) Ağ trafiğini izlemek amacı ile kullanılabilir ağ kartları için paket yakalamaya başladığında kullanılabilecek filtre tanımlanabilmektedir.

4) Sık sık kullanılabilir işlemlerin kısayol atamalarının bulunduğu yerdir.

5) Ana menü bulunduğu kısımdır. Bu bölümü daha yakından inceleyeceğiz.

6) Ağ trafiği için filtremele kullanılabileceğiniz çok özel bir kısımdır.

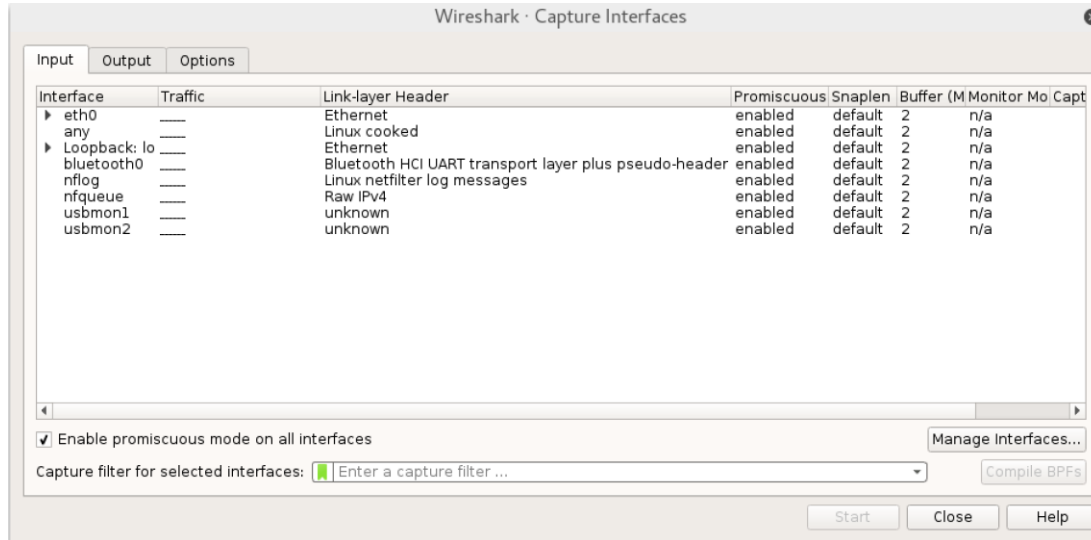
7) Wireshark hakkında daha fazla bilgi edinmek ve manuel dosyalarına erişmek amacı ile kullanılabilir bir bölümdür. Bu bölüme 5 numara ile tanımlanan ana menüde **Help** kısmından erişebilirsiniz.



Wireshark aracı ile paket yakalama işlemi

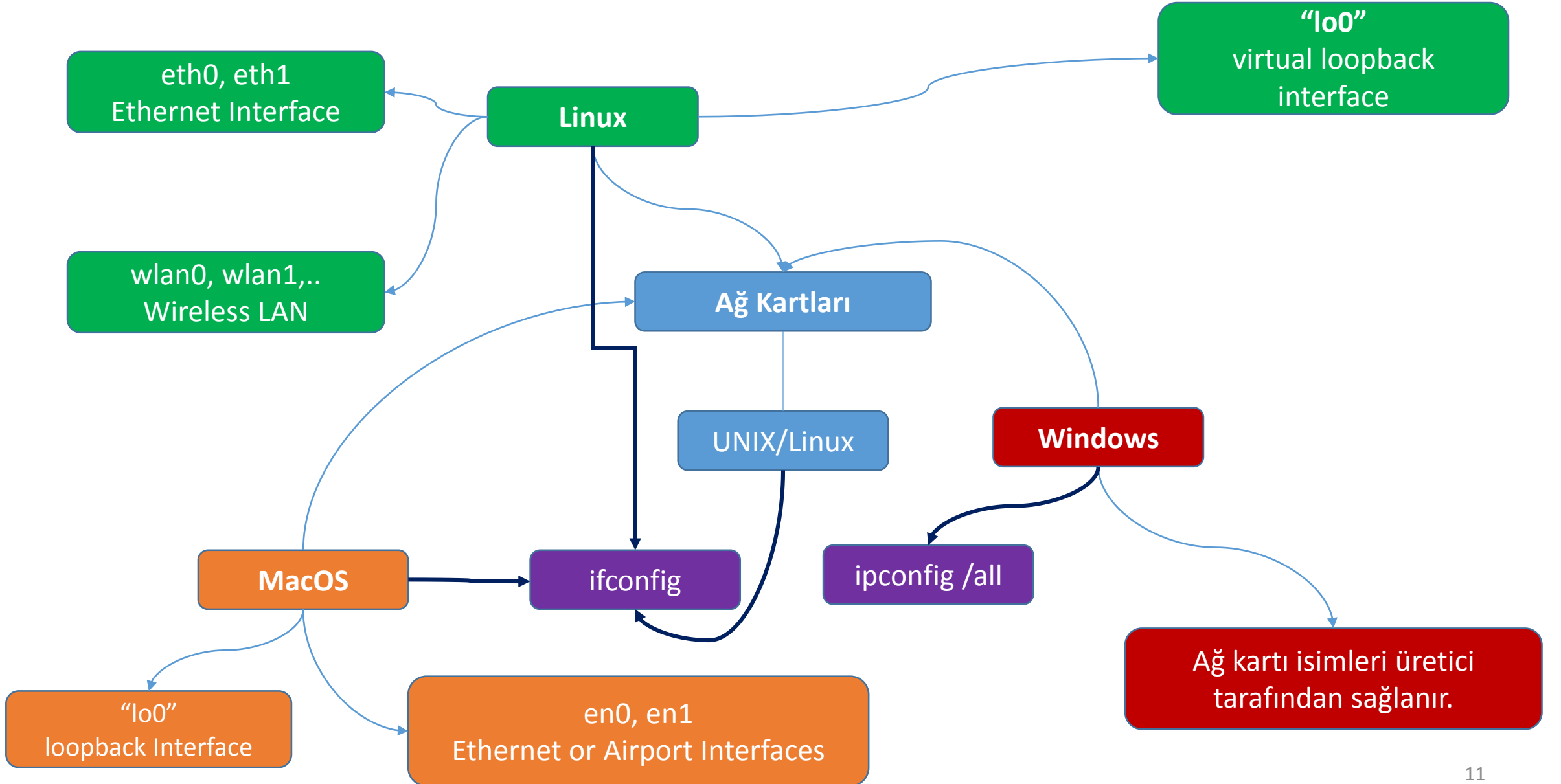
Bu işlem için iki seçeneğiniz bulunmaktadır. Ama unutmamamız gereken şey, Wireshark aracını **root (en yetkili)** kişi hakları ile çalıştırmaktır. Bunun sebebi, wireshark aracının bizim ağ kartlarımıza erişmek istemesidir.

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



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

Wireshark ile Paket Yakalama – Ağ Kartları



Wireshark aracı ile paket yakalama işleminde ki ara yüzü tanıyalım

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

The screenshot shows the Wireshark interface with the following components:

- 1**: Filter bar at the top with the text "Apply a display filter ... <Ctrl-/>".
- 2**: Packet list pane showing a table of captured packets. The table has columns: No., SSID, Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 6) is highlighted in blue.
- 3**: Packet details pane showing the structure of the selected packet. It includes fields like "Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)", "Ethernet II, Src: Apple_bc:c5:b1 (ac:bc:32:bc:c5:b1), Dst: Airtiesw_ac:54:a8 (18:28:61:ac:54:a8)", "Internet Protocol Version 4, Src: 192.168.2.39, Dst: 144.2.0.1", and "Transmission Control Protocol, Src Port: 55354 (55354), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 0".
- 4**: Hex dump pane showing the raw data of the selected packet in hexadecimal and ASCII. The hex dump starts with "0000 18 28 61 ac 54 a8 ac bc 32 bc c5 b1 08 00 45 00" and ends with "0040 cd 50".
- 5**: Status bar at the bottom showing "Packets: 46 · Displayed: 46 (100.0%) Profile: Default".

1) Yakalanan paketler ile ilgili filtreleme seçeneklerinin bulunduğu kısımdır.

2) Yakalanan paketlerin listelendiği kısımdır.

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

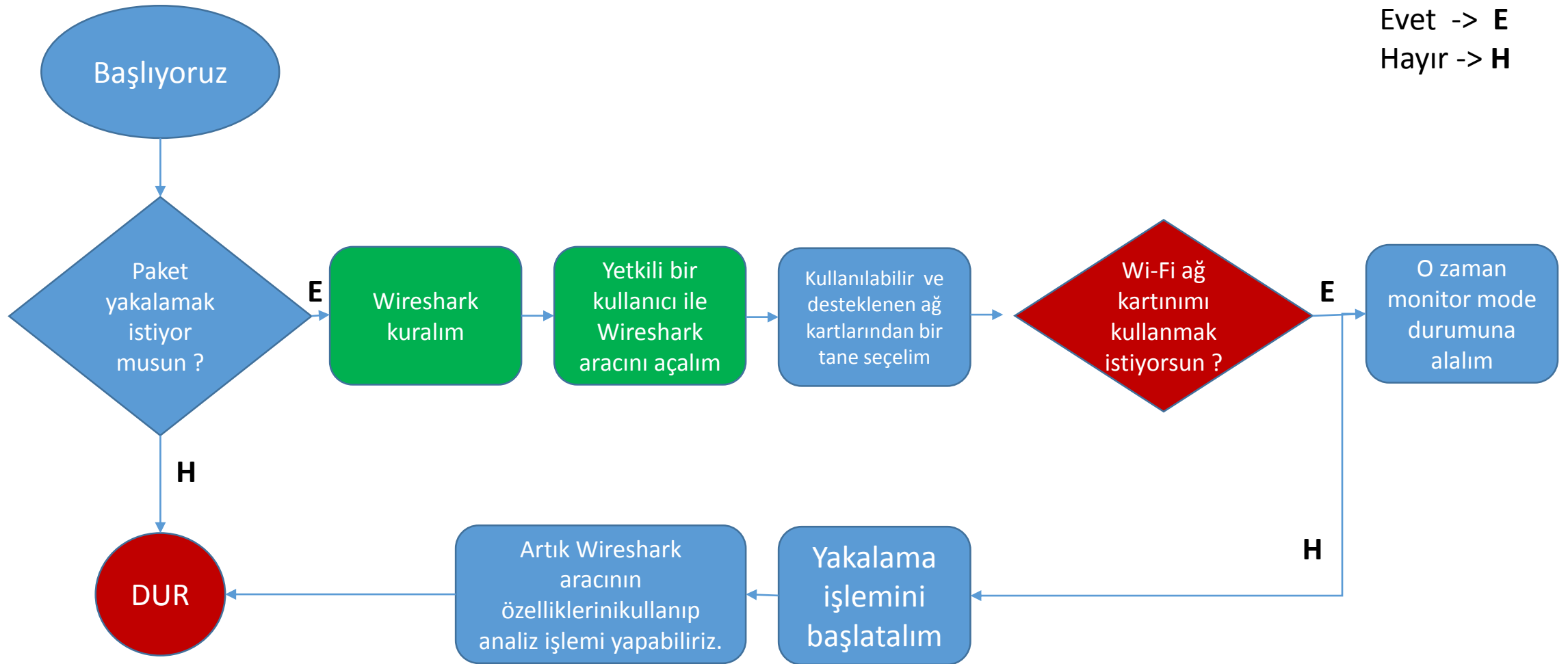
4) Seçilen paket için hex dump halini gösterir.

5) Genel bilgilendirmelerin yer aldığı kısımdır. Bu kısımda :

- 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 Kullanılabilir Filtreler

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

TCP İçin Kullanılabilir Filtreler

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

FTP İçin Kullanılabilir Filtreler

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

ICMP İçin Kullanılabilir Filtreler

- icmp.type
- icmp.code

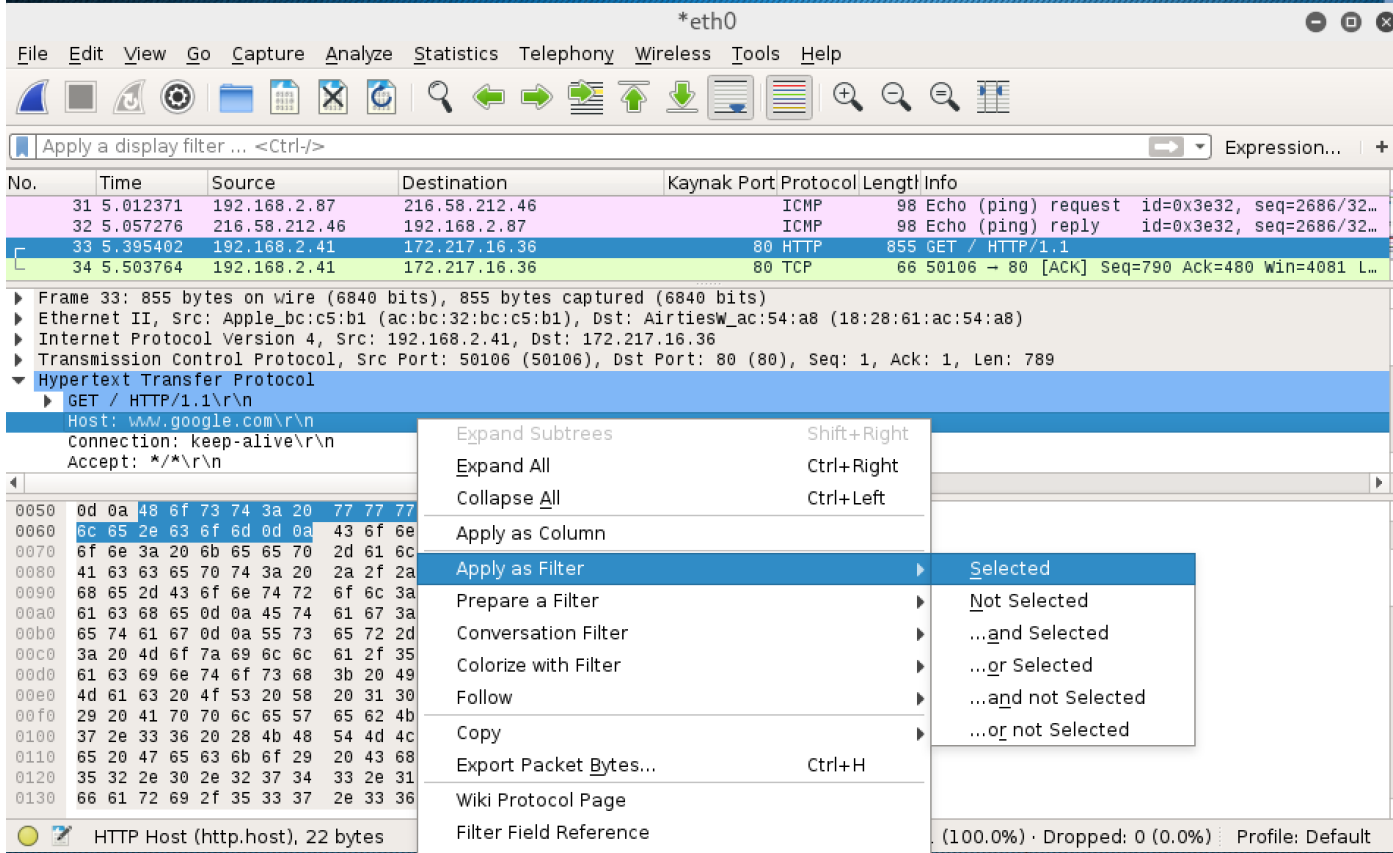
Karşılaştırma Operatörleri

- 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 için Kendi Filtrelerinizi Oluşturun



The screenshot shows the Wireshark interface with the following details:

- Interface: *eth0
- Filter: Apply a display filter ... <Ctrl-/>
- Packet List:

No.	Time	Source	Destination	Kaynak Port	Protocol	Length	Info
31	5.012371	192.168.2.87	216.58.212.46		ICMP	98	Echo (ping) request id=0x3e32, seq=2686/32...
32	5.057276	216.58.212.46	192.168.2.87		ICMP	98	Echo (ping) reply id=0x3e32, seq=2686/32...
33	5.395402	192.168.2.41	172.217.16.36	80	HTTP	855	GET / HTTP/1.1
34	5.503764	192.168.2.41	172.217.16.36	80	TCP	66	50106 → 80 [ACK] Seq=790 Ack=480 Win=4081 L...

Packet 33 details:

- Frame 33: 855 bytes on wire (6840 bits), 855 bytes captured (6840 bits)
- Ethernet II, Src: Apple_bc:c5:b1 (ac:bc:32:bc:c5:b1), Dst: Airtiesw_ac:54:a8 (18:28:61:ac:54:a8)
- Internet Protocol Version 4, Src: 192.168.2.41, Dst: 172.217.16.36
- Transmission Control Protocol, Src Port: 50106 (50106), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 789
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Host: www.google.com\r\n
 - Connection: keep-alive\r\n
 - Accept: */*\r\n

Context menu options:

- Expand Subtrees (Shift+Right)
- Expand All (Ctrl+Right)
- Collapse All (Ctrl+Left)
- Apply as Column
- Apply as Filter (Selected)
- Prepare a Filter (Not Selected)
- Conversation Filter (...and Selected)
- Colorize with Filter (...or Selected)
- Follow (...and not Selected)
- Copy (...or not Selected)
- Export Packet Bytes... (Ctrl+H)
- Wiki Protocol Page
- Filter Field Reference

Bottom status: (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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

export-objects-smb_01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb contains "SHARKFEST" Expression... +

No.	Time	Source	Destination	Kaynak Port	Protokol	Length	Info
36	0.006094	10.0.0.10	10.0.0.20	139	SMB	522	Write AndX Request, FID: 0x8004, 15000 bytes ...
79	7.171726	10.0.0.10	10.0.0.20	139	SMB	1095	Write AndX Request, FID: 0x8007, 15573 bytes ...
139	15.113900	10.0.0.20	10.0.0.10	1036	SMB	450	Read AndX Response, FID: 0x4000, 16393 bytes
186	22.248494	10.0.0.20	10.0.0.10	1036	SMB	947	Read AndX Response, FID: 0xc005, 16890 bytes

Frame 36: 522 bytes on wire (4176 bits), 522 bytes captured (4176 bits)
Ethernet II, Src: Vmware_00:ce:44 (00:0c:29:00:ce:44), Dst: Vmware_4f:5a:74 (00:0c:29:4f:5a:74)
Internet Protocol version 4, Src: 10.0.0.10, Dst: 10.0.0.20
Transmission Control Protocol, Src Port: 1036 (1036), Dst Port: 139 (139), Seq: 15589, Ack: 893, Len: 468
[11 Reassembled TCP Segments (15068 bytes): #23(1460), #24(1460), #25(1460), #26(1460), #28(1460), #29(1460), #31(1460), #33(1460), #
NetBIOS Session Service
SMB (Server Message Block Protocol)

0000 00 0c 29 4f 5a 74 00 0c 29 00 ce 44 08 00 45 00 ...)0Zt..)..D..E.
0010 01 fc 11 59 40 00 80 06 d3 85 0a 00 00 0a 0a 00 ...Y@.....
0020 00 14 04 0c 00 8b a5 d1 be b4 30 03 92 19 50 180...P.
0030 f9 b8 9e 9c 00 00 3d 28 28 22 68 74 74 70 73 3a=("https:
0040 22 3d 3d 6d 64 6f 63 75 6d 65 6e 74 2e 6c 6f 63 61 "=="docum ent.locat
0050 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 29 3f 22 tion.pro tocol)?"
0060 68 74 74 70 73 3a 2f 2f 73 73 6c 2e 22 3a 22 68 https:// ssl.": "h
0070 74 74 70 3a 2f 2f 77 77 77 2e 22 29 3b 64 6f 63 ttp://w w.");doc
0080 75 6d 65 6e 74 2e 77 72 69 74 65 28 75 6e 65 73 ument.wr ite(unes
0090 63 61 70 65 28 22 25 33 43 73 63 72 69 70 74 20 cape("%3 Cscript
00a0 73 72 63 3d 27 22 2b 67 61 4a 73 48 6f 73 74 2b src=" "g aJsHost+
00b0 22 67 6f 6f 67 6c 65 2d 61 6e 61 6c 79 74 69 63 "google- analytic
00c0 73 2e 63 6f 6d 2f 67 61 2e 6a 73 27 20 74 79 70 s.com/ga .js' typ

Frame (522 bytes) Reassembled TCP (15068 bytes)

export-objects-smb_01 Packets: 199 · Displayed: 4 (2.0%) · Load time: 0:0.8 Profile: Default

http_witp_jpegs.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http contains "jpeg" Expression... +

No.	Time	Source	Destination	Kaynak Port	Protokol	Length	Info
259	6.777805	10.1.1.1	10.1.1.101	3198	HTTP	542	HTTP/1.1 200 OK (JPEG JFIF ...
269	6.785744	10.1.1.1	10.1.1.101	3199	HTTP	824	HTTP/1.1 200 OK (JPEG JFIF ...
278	10.836425	10.1.1.101	10.1.1.1	80	HTTP	691	GET /websidan/2004-07-seawor...
479	11.109333	10.1.1.1	10.1.1.101	3200	HTTP	1445	HTTP/1.1 200 OK (JPEG JFIF ...

Frame 269: 824 bytes on wire (6592 bits), 824 bytes captured (6592 bits)
Ethernet II, Src: Kye_20:6c:df (00:c0:df:20:6c:df), Dst: SncNetwo_22:5a:03 (00:04:e2:22:5a:03)
Internet Protocol version 4, Src: 10.1.1.1, Dst: 10.1.1.101
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 3199 (3199), Seq: 10221, Ack: 633, Len: 770
[8 Reassembled TCP Segments (10990 bytes): #249(1460), #255(1460), #261(1460), #263(1460), #264(1460), #266(1460), #26
Hypertext Transfer Protocol
JPEG File Interchange Format

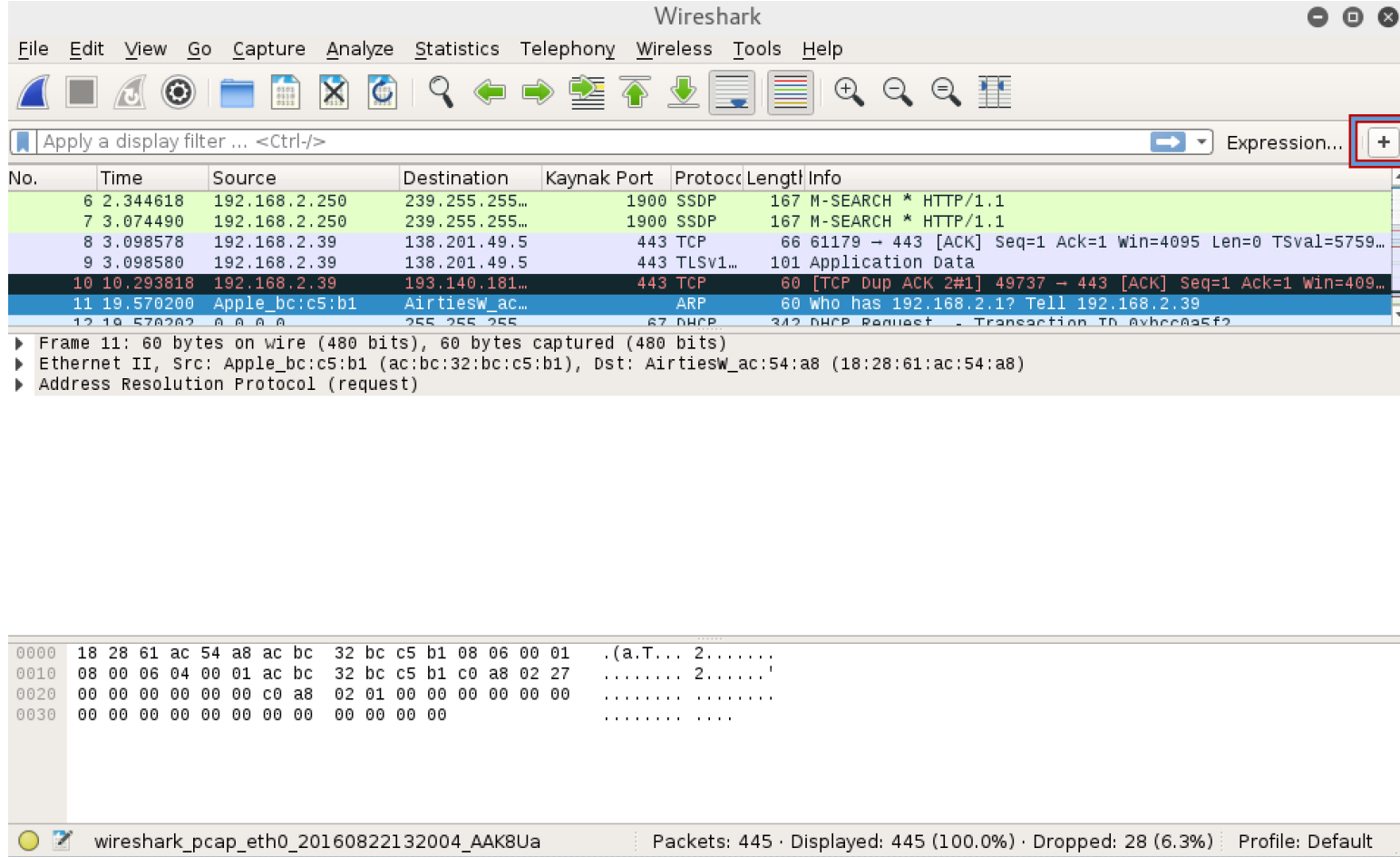
0000 00 04 e2 22 5a 03 00 c0 df 20 6c df 08 00 45 00 ... "Z... .1...E.
0010 03 2a e5 31 40 00 40 06 3c 35 0a 01 01 01 0a 01 ...*.1@.<5.....
0020 01 65 00 50 0c 7f 38 74 df 00 34 c1 64 d0 50 19 ...e.P..8t...4.d.P.
0030 1b 28 ac 5a 00 09 24 ed c8 dd b3 f4 a5 5d 6a e3 ...(.Z.\$...].j.
0040 db 24 9a 55 e1 59 cc 80 1f 22 4d 57 d3 e4 0b 8c ...\$.U.Y... "MW....
0050 9e 2b 3c b5 dc cd bd 1c e3 cf 3d b9 17 81 ef fd ...+<.....=.
0060 b8 d4 13 1e cd 6b 6d 01 1f cd e2 e7 f3 35 66 2ekm.5f.
0070 b3 be bc 7c 5f 30 9d 4f 05 59 17 1f a5 2a 2b 23 ...|_0_0 .Y...*#
0080 76 75 c7 ce b7 47 44 39 de bf 8d 37 46 f7 d1 f4 vu...GD9...7F...
0090 ce 78 91 b9 af 20 c8 78 d7 6a b7 38 cf 6a d9 27 ...x...x .j.8.j.'
00a0 0f 22 a8 75 c0 ef 8a 5d b5 d4 50 5c 45 1a b1 c9 ...".u...].P\E...
00b0 38 cd 16 1b 66 04 3e d6 cf aa d6 6c b2 93 e0 e0 ...8...f.>...1....
00c0 75 78 7d 2c 9a 45 96 98 21 0c 63 cb 76 18 f4 a9 ux},.E...!c.V...
00d0 54 ab 29 c2 8c 81 8c ee 15 49 62 5c 86 8f 7a 11 T.).... !B\..Z.

Frame (824 bytes) Reassembled TCP (10990 bytes)

http_witp_jpegs Packets: 483 · Displayed: 24 (5.0%) · Load time: 0:0.7 Profile: Default

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

Filtreleme Butonu Oluşturmak



The image shows the Wireshark interface with a packet capture. The filter bar at the top contains the text "Apply a display filter ... <Ctrl-/>" and a button with a plus sign (+). A red arrow points to this button. Below the filter bar is a table of captured packets. The status bar at the bottom shows "Packets: 445 · Displayed: 445 (100.0%) · Dropped: 28 (6.3%) · Profile: Default".

No.	Time	Source	Destination	Kaynak Port	Protocoll	Length	Info
6	2.344618	192.168.2.250	239.255.255...	1900	SSDP	167	M-SEARCH * HTTP/1.1
7	3.074490	192.168.2.250	239.255.255...	1900	SSDP	167	M-SEARCH * HTTP/1.1
8	3.098578	192.168.2.39	138.201.49.5	443	TCP	66	61179 → 443 [ACK] Seq=1 Ack=1 Win=4095 Len=0 TSval=5759...
9	3.098580	192.168.2.39	138.201.49.5	443	TLSv1...	101	Application Data
10	10.293818	192.168.2.39	193.140.181...	443	TCP	60	[TCP Dup ACK 2#1] 49737 → 443 [ACK] Seq=1 Ack=1 Win=409...
11	19.570200	Apple_bc:c5:b1	AirtiesW_ac...		ARP	60	who has 192.168.2.1? Tell 192.168.2.39
12	19.570202	0.0.0.0	255.255.255...	67	DHCP	342	DHCP Request - Transaction ID 0xbcc0a5f2

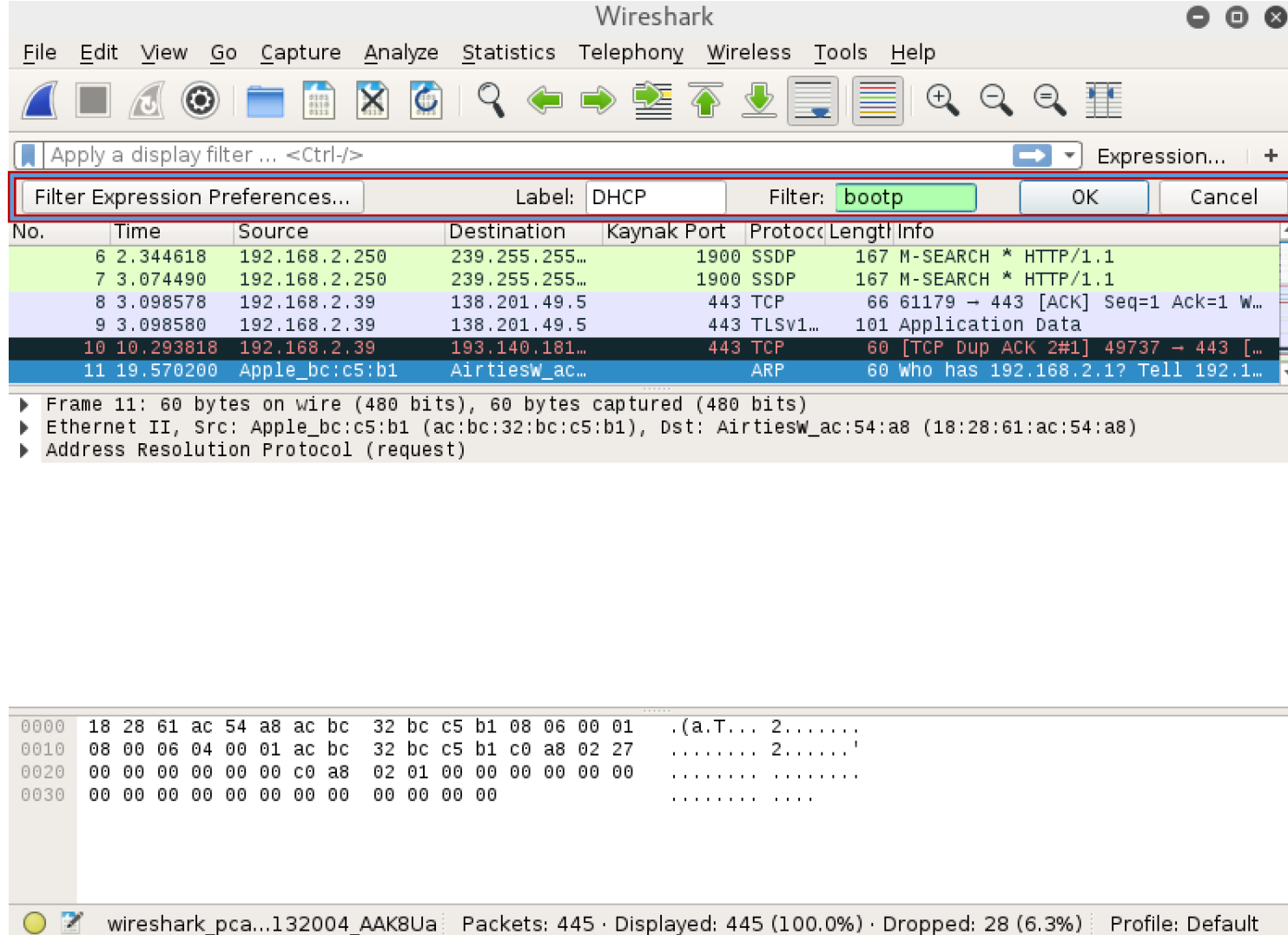
```
0000  18 28 61 ac 54 a8 ac bc 32 bc c5 b1 08 06 00 01  .(a.T... 2.....
0010  08 00 06 04 00 01 ac bc 32 bc c5 b1 c0 a8 02 27  .....! 2.....'
0020  00 00 00 00 00 00 c0 a8 02 01 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

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



The image shows the Wireshark interface with a packet capture. The packet list pane shows several packets, with packet 11 selected. The packet details pane shows the structure of packet 11: Ethernet II, Src: Apple_bc:c5:b1 (ac:bc:32:bc:c5:b1), Dst: Airtiesw_ac:54:a8 (18:28:61:ac:54:a8), and Address Resolution Protocol (request). The packet bytes pane shows the raw data of the ARP request.

A dialog box titled "Filter Expression Preferences..." is open, showing the "Label" as "DHCP" and the "Filter" as "bootp". The dialog has "OK" and "Cancel" buttons. A red box highlights the dialog, and a blue arrow points from it to the text box on the right.

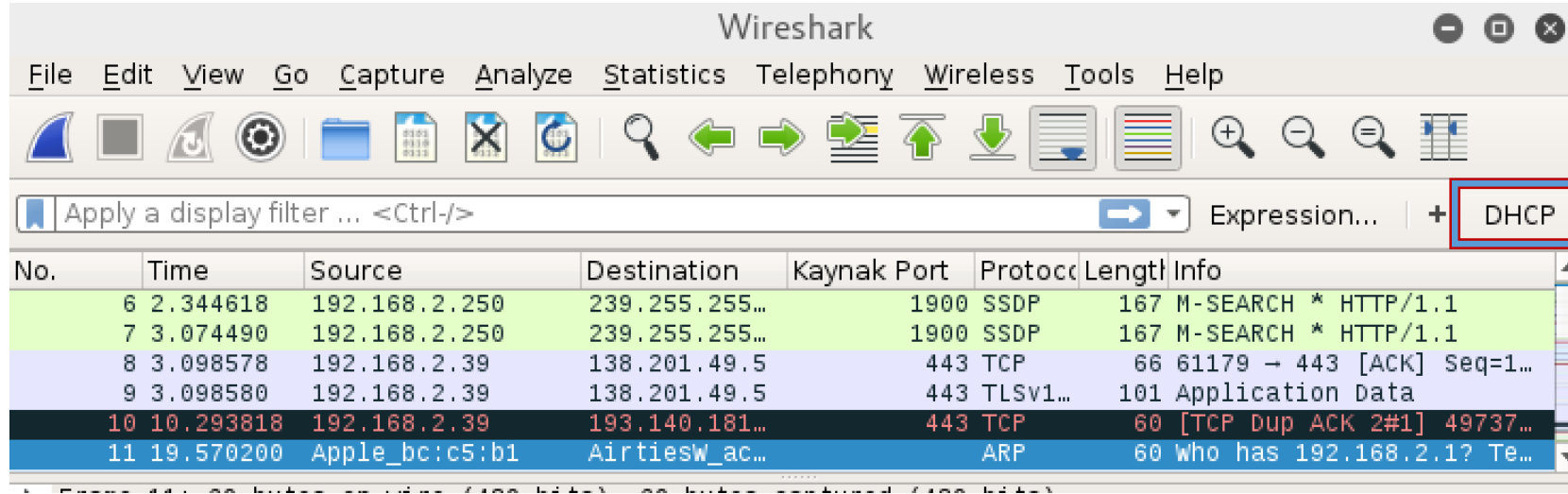
No.	Time	Source	Destination	Kaynak Port	Protoc	Length	Info
6	2.344618	192.168.2.250	239.255.255...	1900	SSDP	167	M-SEARCH * HTTP/1.1
7	3.074490	192.168.2.250	239.255.255...	1900	SSDP	167	M-SEARCH * HTTP/1.1
8	3.098578	192.168.2.39	138.201.49.5	443	TCP	66	61179 → 443 [ACK] Seq=1 Ack=1 W...
9	3.098580	192.168.2.39	138.201.49.5	443	TLSV1...	101	Application Data
10	10.293818	192.168.2.39	193.140.181...	443	TCP	60	[TCP Dup ACK 2#1] 49737 → 443 [...]
11	19.570200	Apple_bc:c5:b1	Airtiesw_ac...		ARP	60	Who has 192.168.2.1? Tell 192.1...

```
0000  18 28 61 ac 54 a8 ac bc 32 bc c5 b1 08 06 00 01  .(a.T... 2.....
0010  08 00 06 04 00 01 ac bc 32 bc c5 b1 c0 a8 02 27  ..... 2.....!
0020  00 00 00 00 00 00 c0 a8 02 01 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00  .....

```

+ tuşuna bastıktan sonra bu menü açılmaktadır. Açılan menüde filtrelemeler için kullanabileceğiniz butonun ismi ve filtreleme seçeneğini yazacağınız bölümler bulunmaktadır.

Filtreleme Butonu Oluşturmak

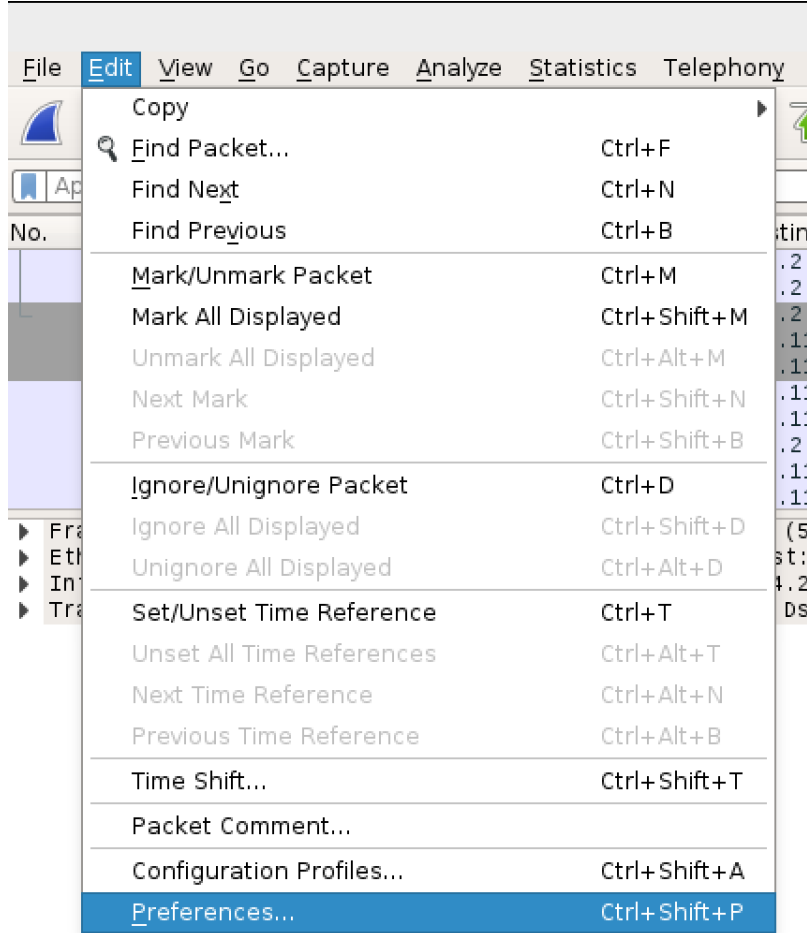


The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture, and analysis. The main display area is divided into three panes: the top pane shows the display filter 'DHCP' (highlighted with a red box), the middle pane shows a list of captured packets, and the bottom pane shows the details of the selected packet (No. 11, ARP protocol).

No.	Time	Source	Destination	Kaynak Port	Protocoll	Length	Info
6	2.344618	192.168.2.250	239.255.255...	1900	SSDP	167	M-SEARCH * HTTP/1.1
7	3.074490	192.168.2.250	239.255.255...	1900	SSDP	167	M-SEARCH * HTTP/1.1
8	3.098578	192.168.2.39	138.201.49.5	443	TCP	66	61179 → 443 [ACK] Seq=1...
9	3.098580	192.168.2.39	138.201.49.5	443	TLSv1...	101	Application Data
10	10.293818	192.168.2.39	193.140.181...	443	TCP	60	[TCP Dup ACK 2#1] 49737...
11	19.570200	Apple_bc:c5:b1	AirtiesW_ac...		ARP	60	Who has 192.168.2.1? Te...

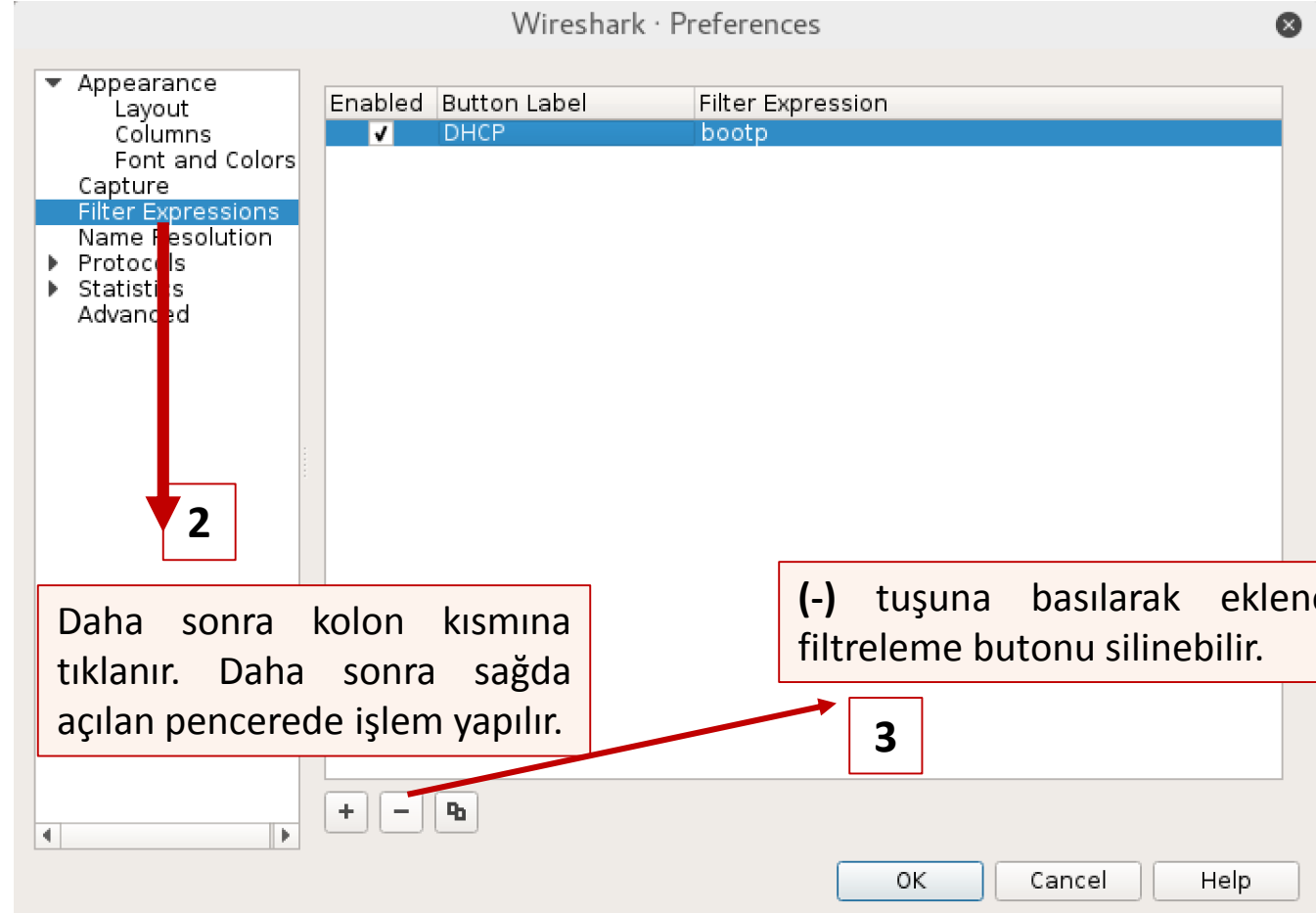
Yapılan işlemler sonunda görünüm kutucuk içine alınan kısım gibi olacaktır. Artık **DHCP** isminde ve **dhcp paketlerini** filtreleyen bir **filtreleme butonumuz** olmuştur.

Filtreleme Butonu Silmek



1

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



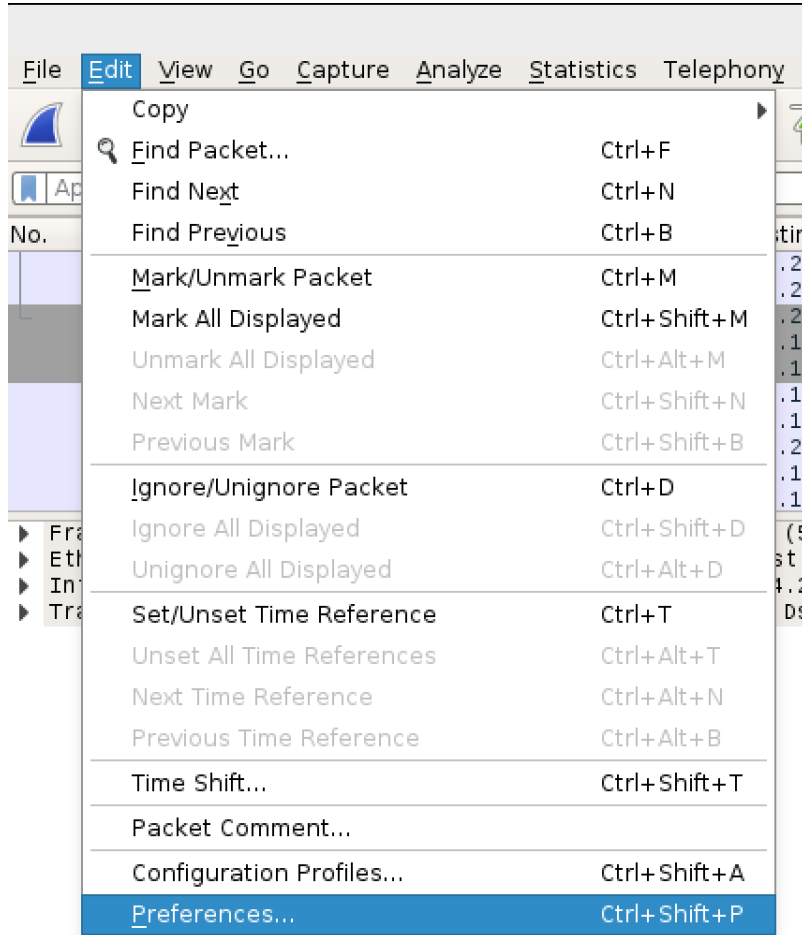
2

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

(-) tuşuna basılarak eklenen filtreleme butonu silinebilir.

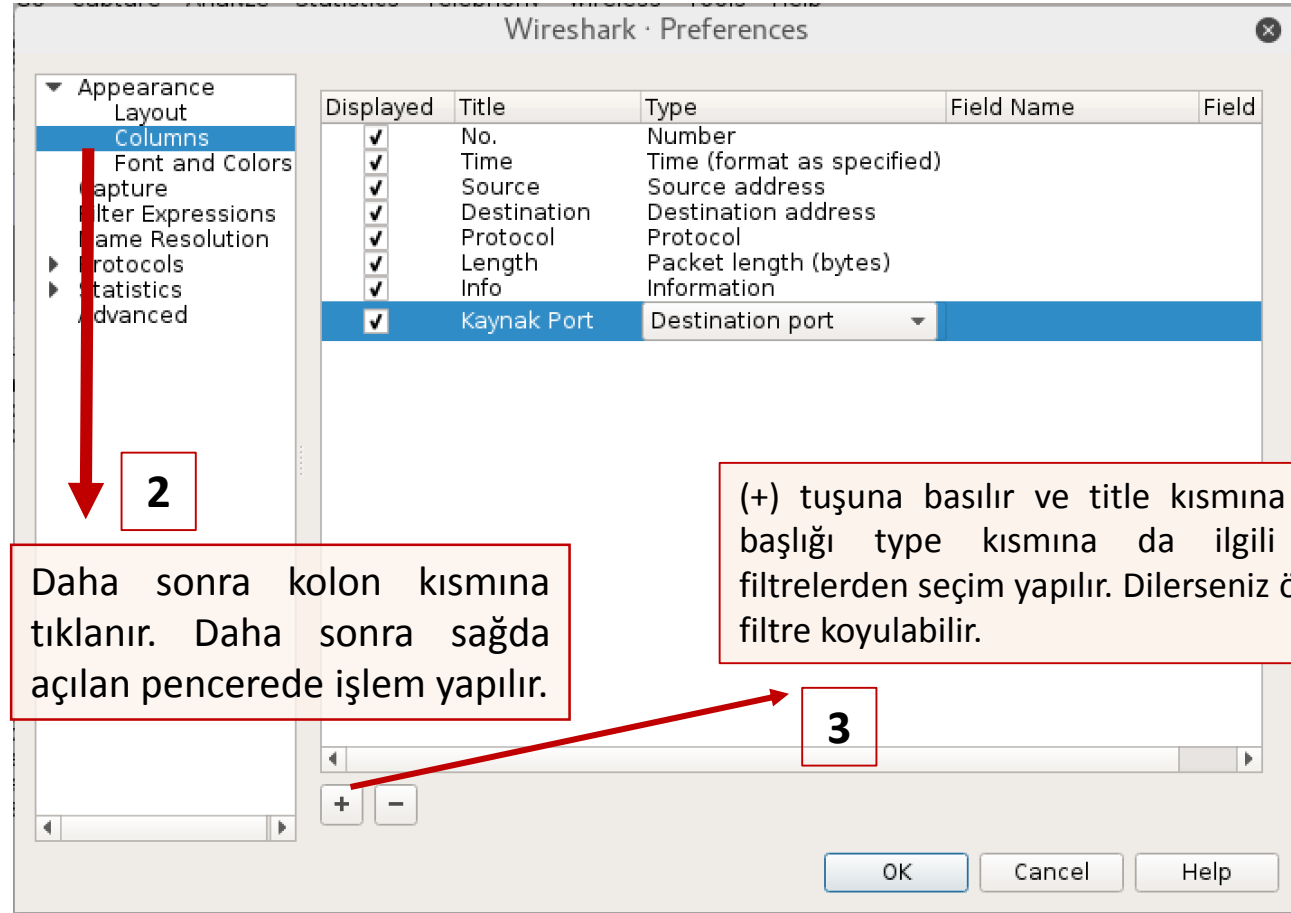
3

Özel Olarak Kolon Eklemek



1

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



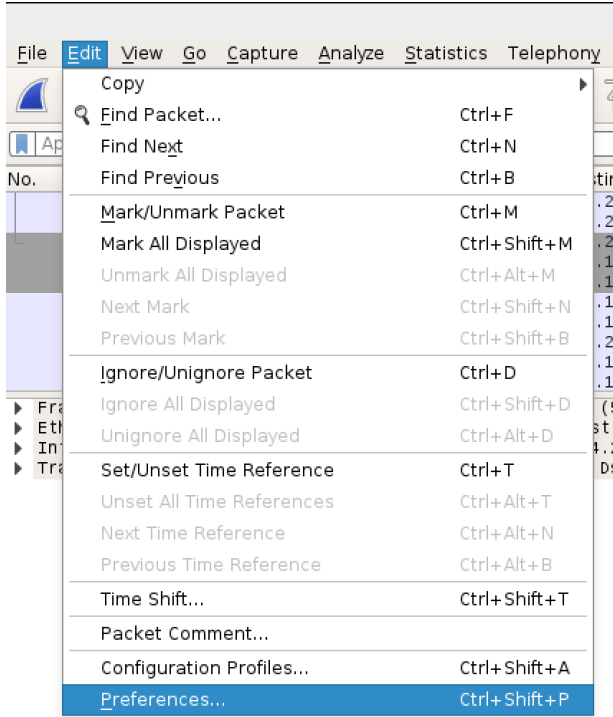
2

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.

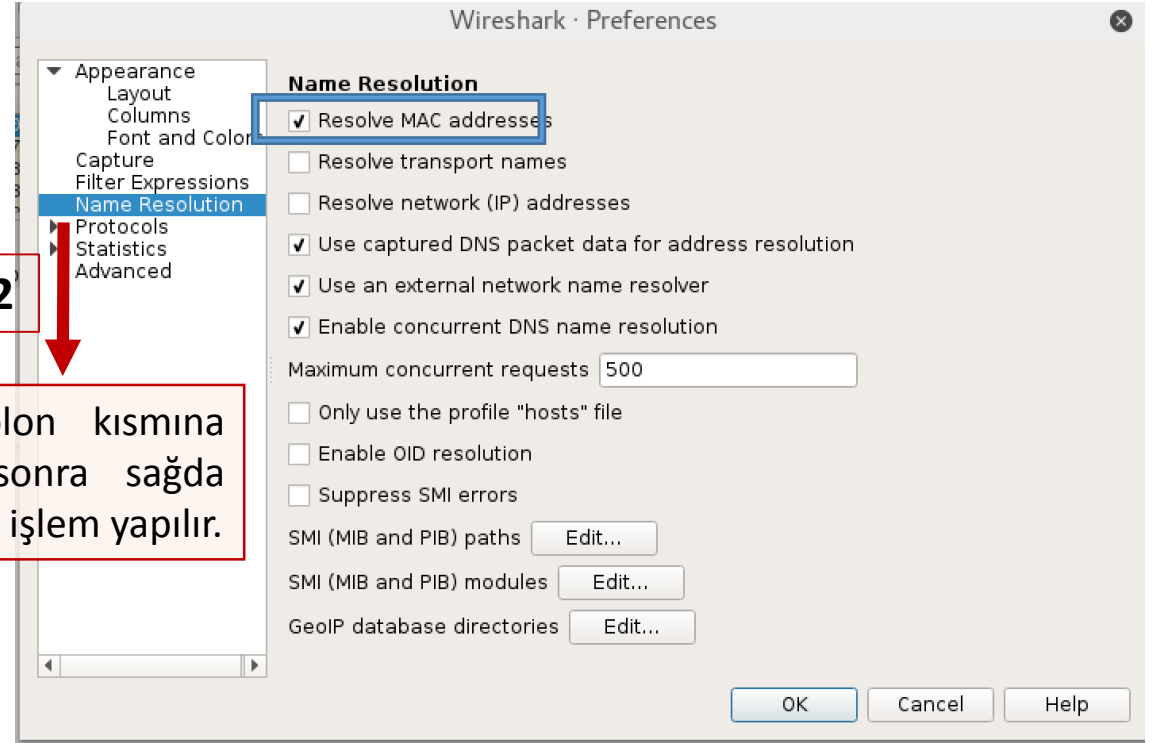
3

Wireshark – Adres Çözümlemenin Aktif Edilmesi



1

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



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

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 Çözümlemenin Aktif Edilmesi

```
root@kali: /usr/share/wireshark
File Edit View Search Terminal Help
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:~# cd /usr/share/wireshark/
```

```
manuf
/usr/share/wireshark
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 Auspex # AUSPEX 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 TSC PR
```

Peki wireshark bu adres
çözümlemeyi nasıl yapıyor ?

Wireshark içerisinde bulunan manuf isimli
dosyayı sürekli güncellemekte ve bu dosyayı
kullanarak adres çözümlerini
gerçekleştirmektedir.

HTTP İsteklerinin Analiz Edilmesi

The image shows the Wireshark Statistics window for the 'http' protocol. The 'Statistics' menu is open, and the 'HTTP' option is selected, which has opened a sub-menu with 'Requests' highlighted. The main window displays a list of captured packets with the following data:

No.	Time	Source
15223	54.285609	192.168.2.87
15227	54.289724	192.168.2.87
15232	54.320872	216.58.212.10
15260	54.351161	216.58.212.10
15312	54.615713	192.168.2.87
15313	54.701296	216.58.212.10

The packet list shows that the selected packet (No. 15223) is a Hypertext Transfer Protocol request. The packet details pane shows the following information:

- Frame 39: 375 bytes on wire (3000 bits)
- Ethernet II, Src: Vmware_13:a8:9a:00:00:00, Dst: Vmware_6e:af:d2:18:28:61:6e:af:d2
- Internet Protocol Version 4, Src: 192.168.2.87, Dst: 216.58.212.10
- Transmission Control Protocol, Src Port: 54285, Dst Port: 80
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the packet, including the HTTP request line: GET /maps-api-v3/api/js/...

1

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



The image shows the Wireshark Requests window, which displays a list of HTTP requests by host. The list includes the following hosts:

- xn--meryemakdoan-myb.com
- www.xn--meryemakdoan-myb.com
- www.innoverabt.com
- www.google.com.tr
- w3.sdu.edu.tr
- twitter.com
- static.addtoany.com
- sr.symcd.com
- sdu.edu.tr
- s2.symcb.com
- ocsp.digicert.com
- maps.googleapis.com
- gravatar.com
- google.com
- fonts.gstatic.com
- fonts.googleapis.com
- csi.gstatic.com
- clients1.google.com
- 239.255.255.250:1900

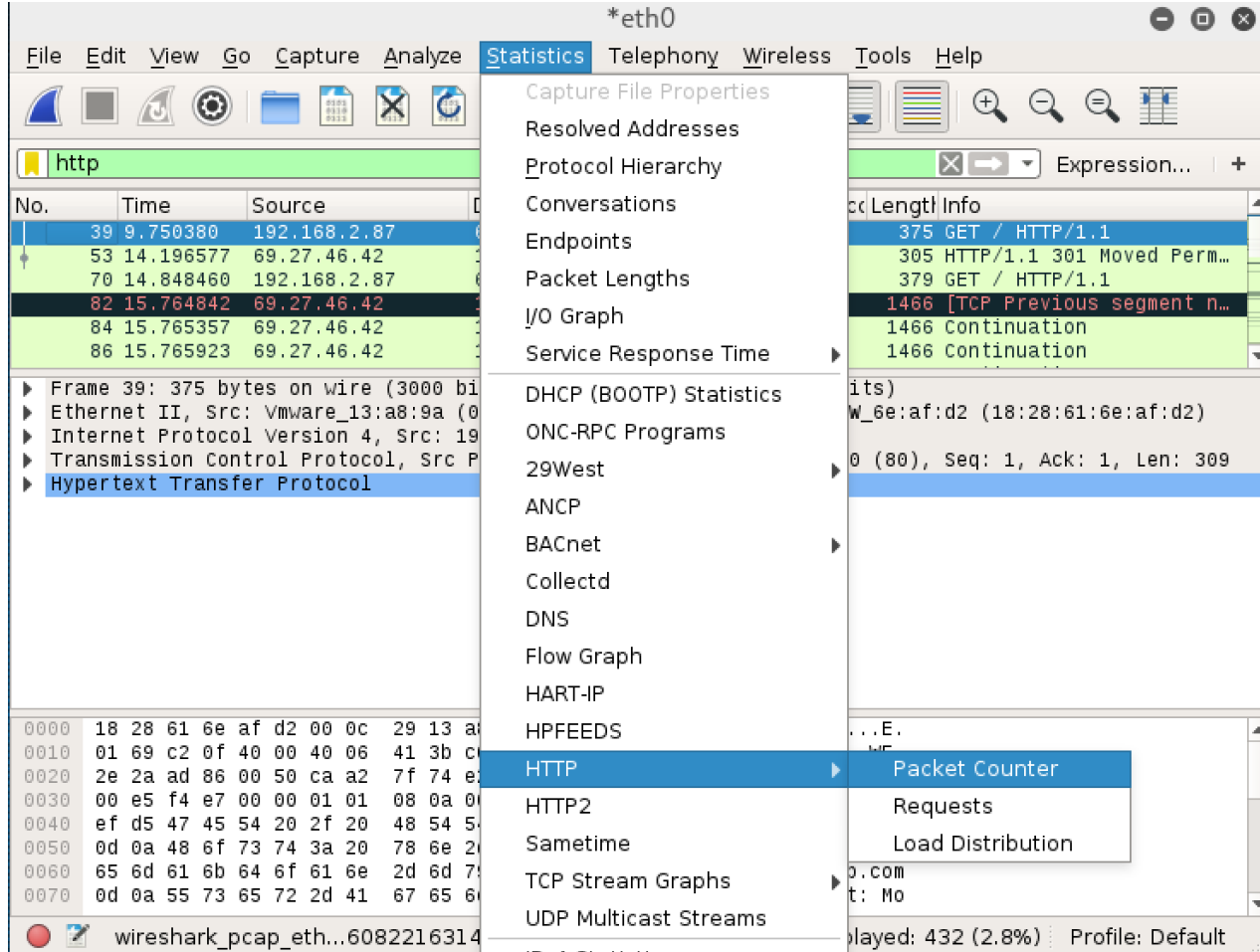
The window also includes a display filter field and buttons for Copy, Save as..., and Close.



2

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

HTTP İsteklerinin Analiz Edilmesi



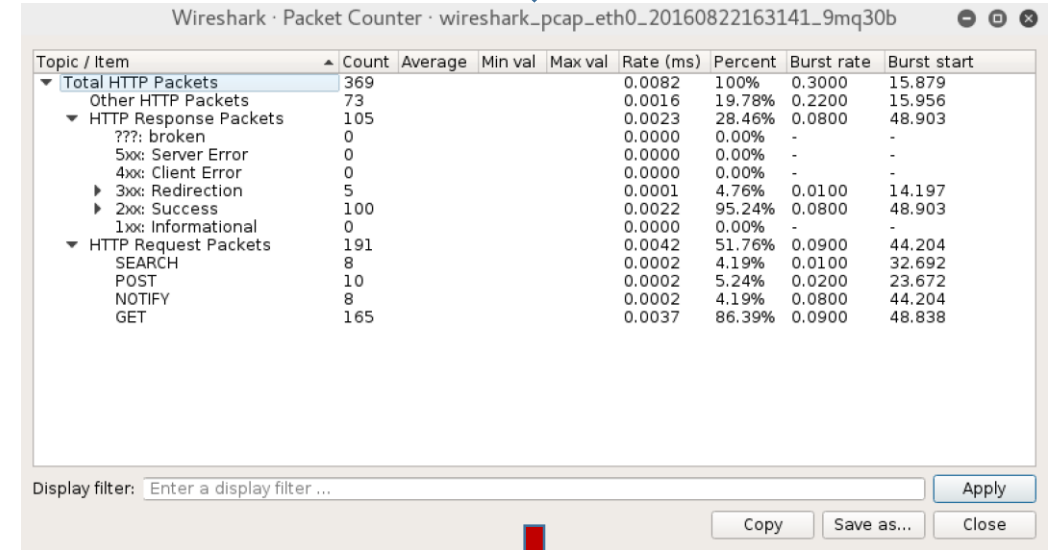
The image shows the Wireshark Statistics window for the 'http' protocol. The 'Statistics' menu is open, and the 'HTTP' option is selected, which has opened a sub-menu with 'Packet Counter' highlighted. The main window displays a list of captured packets, with packet 39 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source
39	9.750380	192.168.2.87
53	14.196577	69.27.46.42
70	14.848460	192.168.2.87
82	15.764842	69.27.46.42
84	15.765357	69.27.46.42
86	15.765923	69.27.46.42

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

1

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



The image shows the Wireshark Packet Counter window for the 'http' protocol. The window displays a table of statistics for various HTTP topics and items. The 'GET' method is highlighted, showing a count of 165 requests.

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

The screenshot shows the Wireshark interface with the Statistics menu open. The menu path is: Statistics -> IPv4 Statistics -> All Addresses. The main window displays a list of captured packets, with the selected packet (No. 7) showing details for the Hypertext Transfer Protocol.

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



The screenshot shows the 'All Addresses' statistics window in Wireshark. The table displays the following data:

Topic / Item	Cour	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			0.000
149.154.167.91	1	0.0000	0.25%	0.0100	0.000			21.746
17.188.139.157	1	0.0000	0.25%	0.0100	0.000			20.700
224.0.0.2	1	0.0000	0.25%	0.0100	0.000			20.647
17.172.232.214	2	0.0001	0.50%	0.0200	0.001			21.774
17.188.161.18	2	0.0001	0.50%	0.0200	0.001			22.358
193.140.181.27	2	0.0001	0.50%	0.0100	0.001			0.224
23.102.4.253	2	0.0001	0.50%	0.0100	0.001			1.651
0.0.0.0	3	0.0001	0.75%	0.0100	0.001			19.570
74.125.133.109	3	0.0001	0.75%	0.0200	0.001			20.190
74.125.140.109	3	0.0001	0.75%	0.0100	0.001			20.030
192.168.2.255	4	0.0001	1.00%	0.0200	0.001			21.554
192.168.2.87	4	0.0001	1.00%	0.0200	0.001			24.668
216.58.213.68	4	0.0001	1.00%	0.0200	0.001			21.497
255.255.255.255	4	0.0001	1.00%	0.0100	0.001			19.570
138.201.49.5	6	0.0002	1.50%	0.0200	0.002			3.099
195.175.113.51	6	0.0002	1.50%	0.0500	0.002			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. The main pane shows a list of packets with the 'Internet Control Message Protocol' selected. The 'Statistics' menu includes options like 'Capture File Properties', 'Resolved Addresses', 'Conversations', 'Endpoints', 'Packet Lengths', 'I/O Graph', 'Service Response Time', 'DHCP (BOOTP) Statistics', 'ONC-RPC Programs', '29West', 'ANCP', and 'BACnet'.

The screenshot shows the 'Wireshark · Protocol Hierarchy Statistics · wireshark_pcapng_eth0_20160823095708_iYNyzz' window. It displays a table of protocol statistics:

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	2007
Secure Sockets Layer	31.1	2073	53.7	2401320	397 k	1996	2309
NetBIOS Session Service	0.0	3	0.0	484	80	0	0
Malformed Packet	0.2	13	0.4	18460	3053	13	18460
Hypertext Transfer Protocol	1.7	115	1.5	67786	11 k	80	4511
Portable Network Graphics	0.0	2	0.0	1733	286	2	1733
Online Certificate Status Protocol	0.4	27	0.4	18032	2982	27	18032
Line-based text data	0.1	5	0.1	2297	379	5	2297
JavaScript Object Notation	0.0	1	0.0	585	96	1	585
Data	0.2	16	0.5	23734	3926	16	23734
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	8820
Address Resolution Protocol	0.2	12	0.0	612	101	12	612

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)**

The screenshot shows the 'Wireshark · Protocol Hierarchy Statistics · wireshark_pcapng_eth0_20160823095708_iYNyzz' window. The 'Hypertext Transfer Protocol' is selected, and a context menu is open over it. The menu options are:

- 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

The image shows the Wireshark interface with the Statistics menu open. The 'Capture File Properties' option is highlighted. The background shows a packet list with columns for No., Time, and Source. The packet details pane shows the SMB (Server Message Block Protocol) details for the selected packet.

The image shows the 'Wireshark · Capture File Properties · export-objects-smb_01' dialog box. The 'Details' section is expanded, showing the following information:

- File**
 - Name: /root/Desktop/export-objects-smb_01.pcap
 - Length: 90 kB
 - Format: Wireshark/tcpdump/... - pcap
 - Encapsulation: Ethernet
 - Snapshot length: 65535
- Time**
 - First packet: 2011-10-23 15:47:29
 - Last packet: 2011-10-23 15:47:56
 - Elapsed: 00:00:26
- Capture**
 - Hardware: Unknown
 - OS: Unknown
 - Application: Unknown
- Interfaces**
 - Interface: ...
 - Dropped: ...
 - Capture filter: ...
 - Link type: ...
 - Packet size limit: ...
- Capture file comments

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

The screenshot shows the Wireshark interface for the file 'export-objects-smb_01.pcap'. The 'Statistics' menu is open, and 'Resolved Addresses' is highlighted. The main packet list shows five frames from source 10.0.0.10 to 10.0.0.20. The packet details pane shows the first frame's structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, NetBIOS Session Service, and SMB (Server Message Block Protocol).

The 'Resolved Addresses' dialog box is open, displaying a list of resolved addresses. A configuration window is also open, showing options for displaying resolved addresses. The configuration window has the following settings:

- IPv4 and IPv6 Addresses (hosts)
- Comment
- IPv4 Hash Table
- IPv6 Hash Table
- Port names (services)
- Ethernet Addresses
- Ethernet Manufacturers
- Ethernet Well-Known Addresses
- Show All
- Hide All

Yakalanan paketlerin tamamı için bir adres çözümleme yapmak istersek **Statistics -> Resolved Addresses** yolunu takip etmemiz yeterli olacaktır.

Wireshark ile ARP Saldırılarını Tespit Etmek

The image shows the Wireshark network protocol analyzer interface. The filter bar at the top contains the expression `arp.duplicate-address-frame`. The packet list pane shows four ARP packets. Packet 6265 is highlighted in yellow, indicating a duplicate IP address. The packet details pane for packet 6265 shows the following information:

- 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

The packet bytes pane shows the raw data of the ARP request:

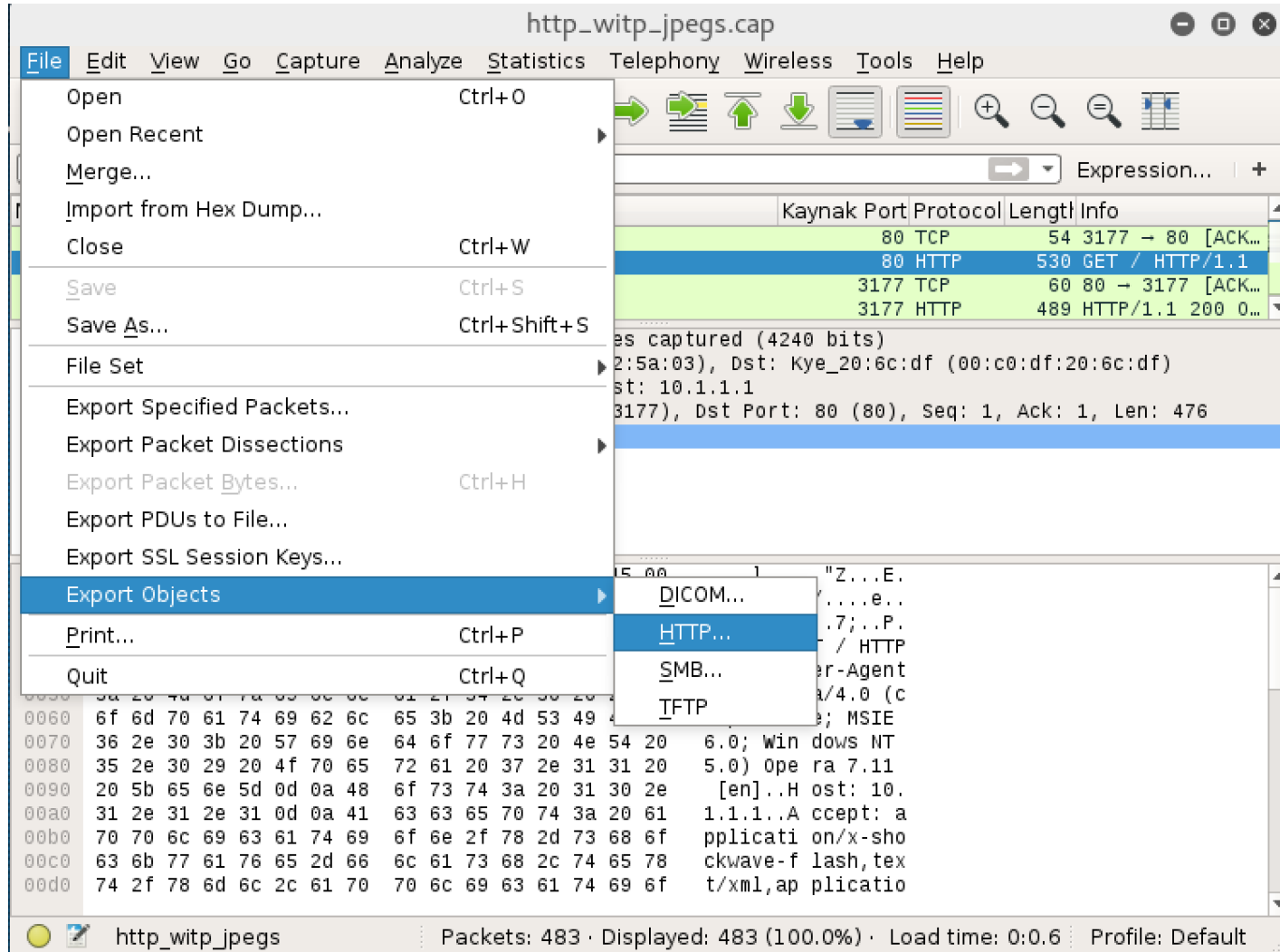
```
0000  c4 6e 1f 17 ed b3 e0 06 e6 26 10 99 08 06 00 01  .n..... &.....
0010  08 00 06 04 00 01 e0 06 e6 26 10 99 c0 a8 01 01  .....&.....
0020  00 00 00 00 00 00 c0 a8 01 25  .....%
```

The status bar at the bottom indicates: 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`

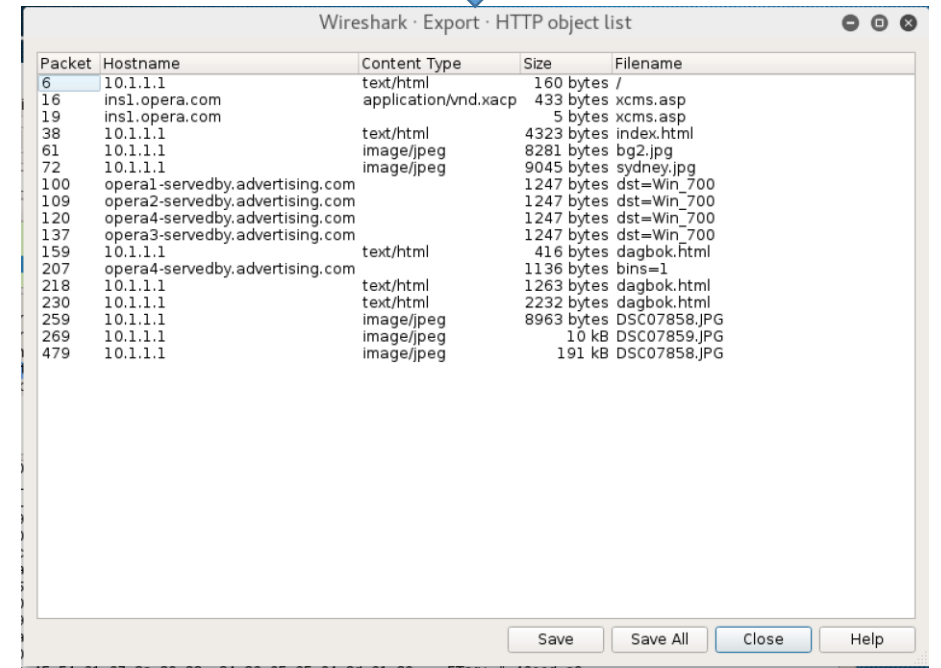
Trafik İçerisindeki Verilerin Export Edilmesi



The image shows the Wireshark File menu with 'Export Objects' selected. The menu options are: Open (Ctrl+O), Open Recent, Merge..., Import from Hex Dump..., Close (Ctrl+W), Save (Ctrl+S), Save As... (Ctrl+Shift+S), File Set, Export Specified Packets..., Export Packet Dissections, Export Packet Bytes... (Ctrl+H), Export PDUs to File..., Export SSL Session Keys..., Export Objects (highlighted), Print... (Ctrl+P), and Quit (Ctrl+Q). The 'Export Objects' sub-menu is open, showing options: DICOM..., HTTP... (highlighted), SMB..., and IFTP. The background shows a packet capture for 'http_witp_jpegs.cap' with a list of packets and a hex dump view.

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

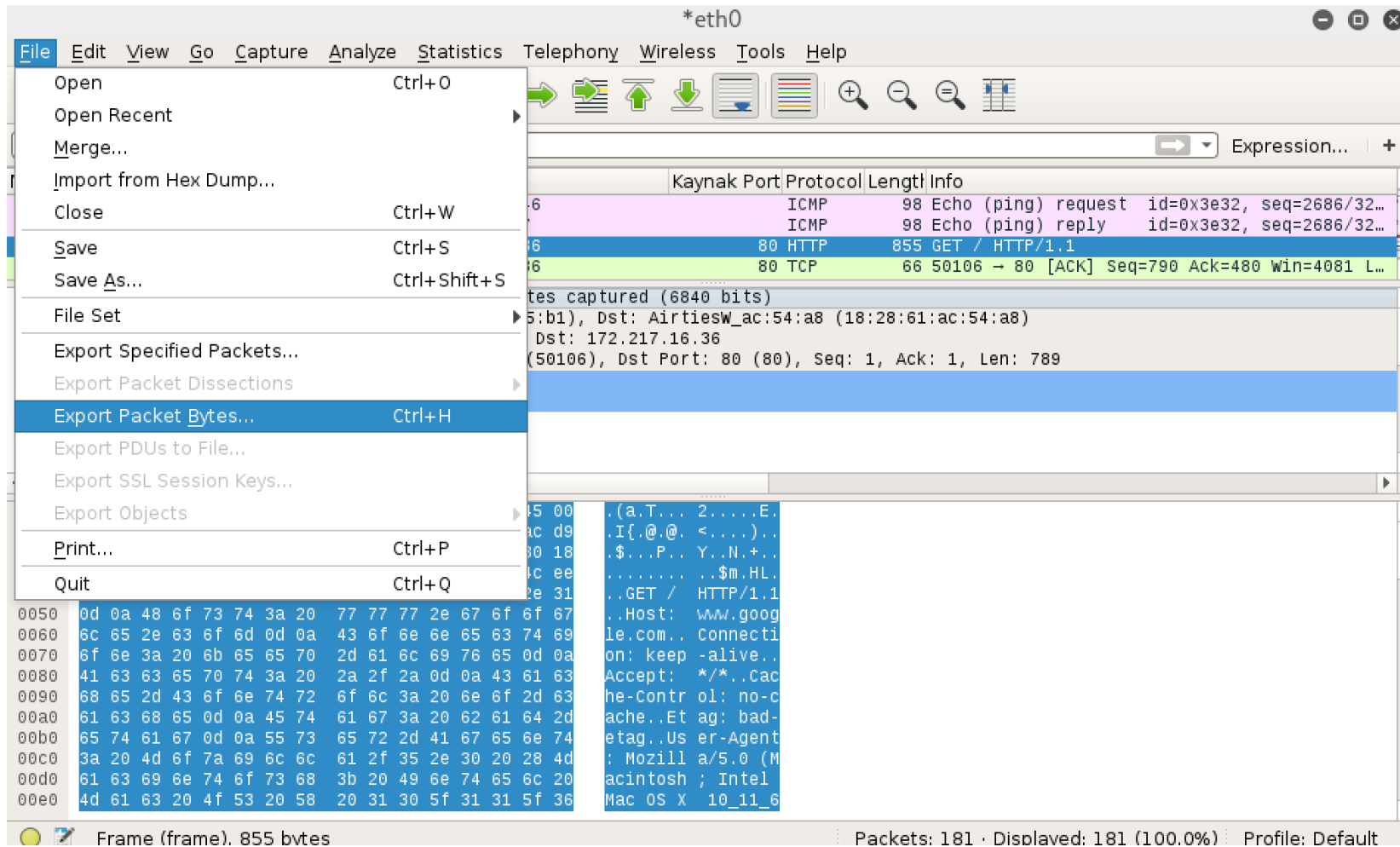
- **File -> Export Objects** yolunu takip ediyoruz.



The image shows the 'Wireshark · Export · HTTP object list' dialog box. It contains a table with the following columns: Packet, Hostname, Content Type, Size, and Filename. The table lists various objects exported from the capture, including HTML files, XACML files, and images.

Packet	Hostname	Content Type	Size	Filename
6	10.1.1.1	text/html	160 bytes	/
16	ins1.opera.com	application/vnd.xacml	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

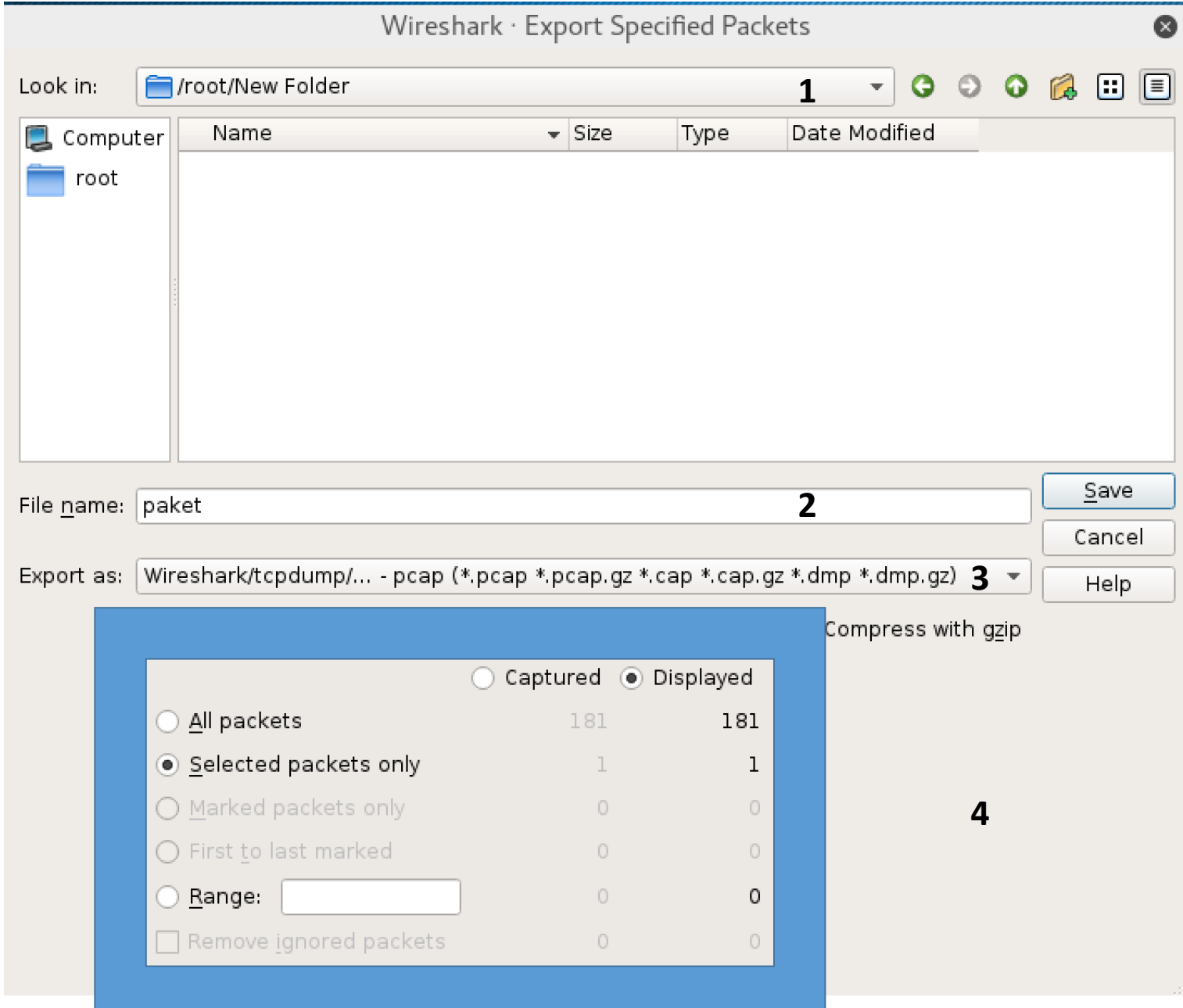


Wireshark ile çalışırken herhangi bir paketi export etmek ve daha sonra incelemek istersek yapmamız gerekenler aslında çok basit.

İlk olarak bir paketin üzerine tıklayıp daha sonra da ;

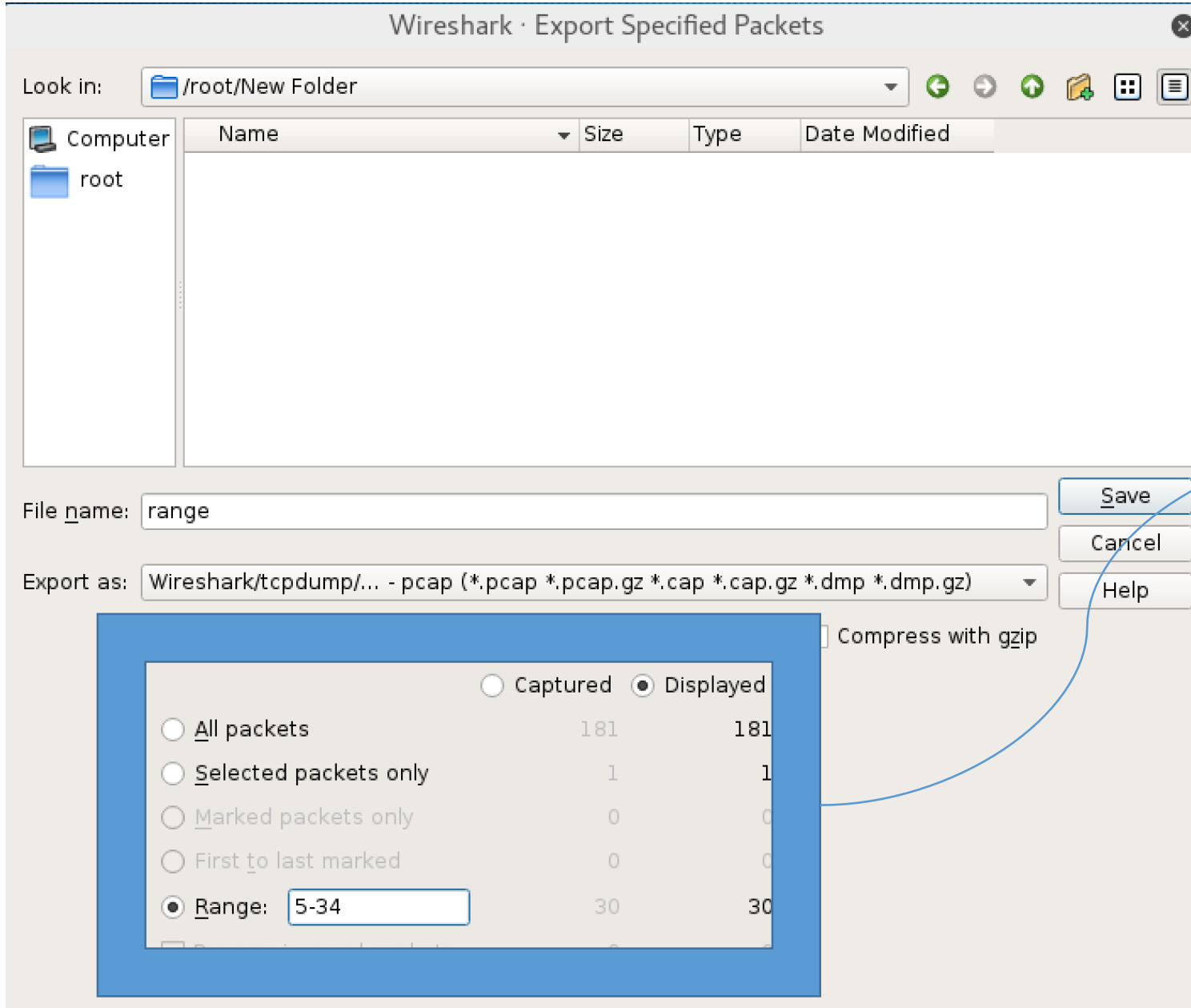
File -> Export Specified Packets yolunu takip ediyoruz.

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.

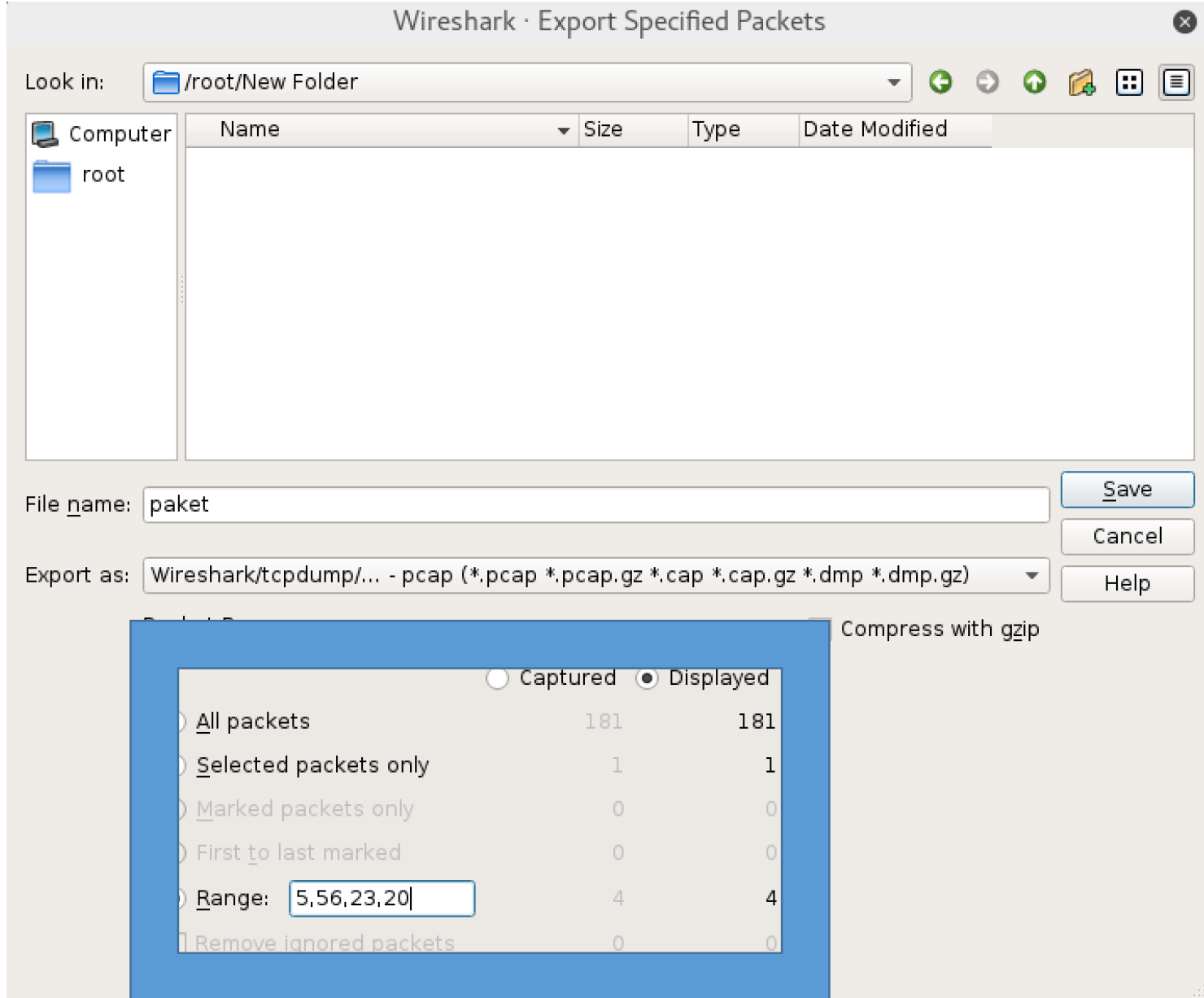
Trafik İçerisindeki Paketlerin Export Edilmesi - 3



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

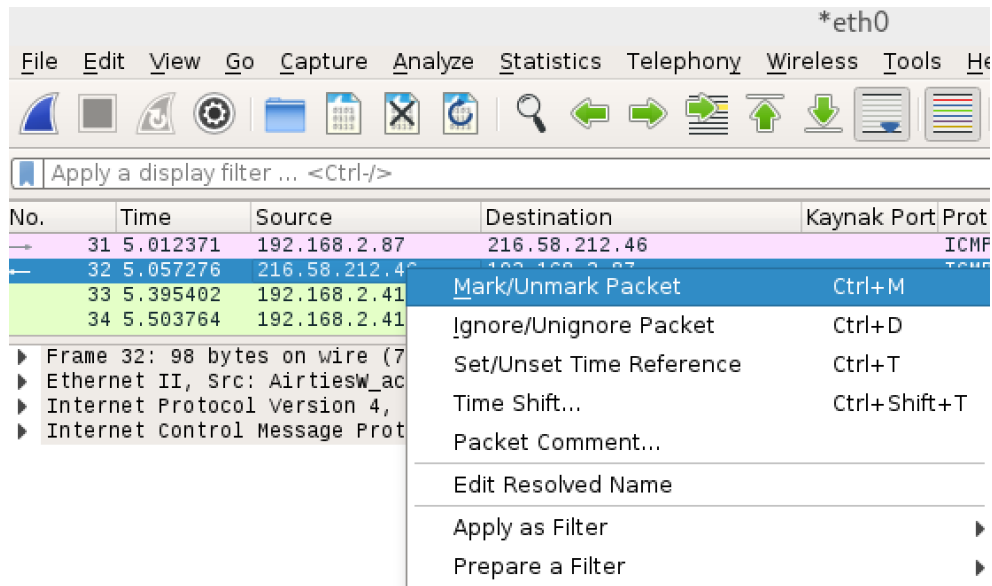
Bunun için kutu içerisine alınan alanda **"Range"** kısmını seçip istediğimiz aralığı belirtmemiz yeterli olacaktır.

Trafik İçerisindeki Paketlerin Export Edilmesi - 4



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

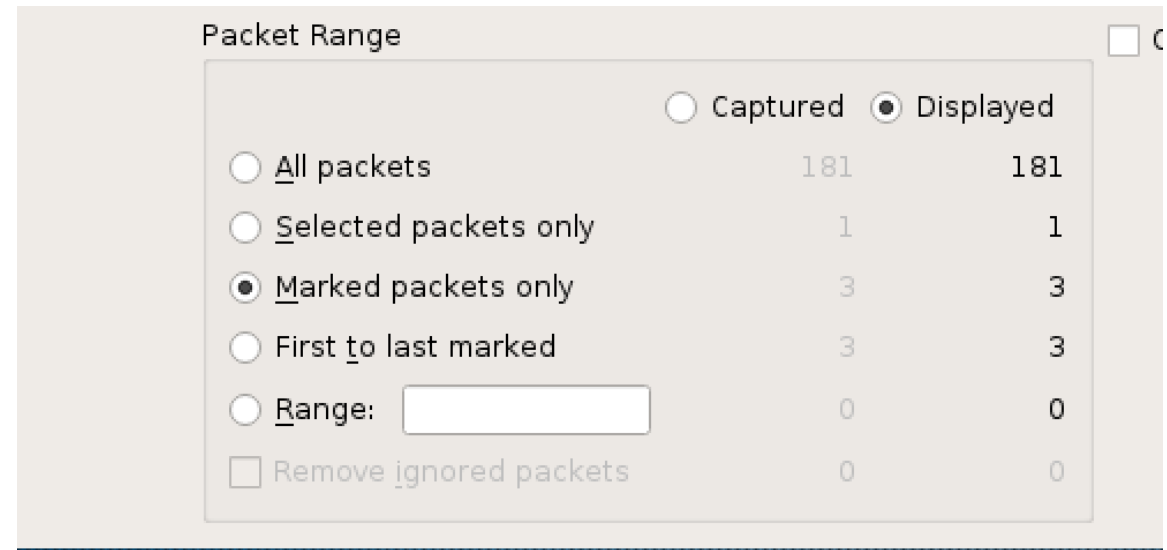
Trafik İçerisindeki Paketlerin Export Edilmesi - 5



The screenshot shows the Wireshark interface for the interface *eth0. The packet list pane displays several packets, with packet 32 selected. A context menu is open over packet 32, showing options such as 'Mark/Unmark Packet', 'Ignore/Unignore Packet', 'Set/Unset Time Reference', 'Time Shift...', 'Packet Comment...', 'Edit Resolved Name', 'Apply as Filter', and 'Prepare a Filter'. The packet details pane shows the structure of packet 32: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol.

No.	Time	Source	Destination	Kaynak Port	Prot
31	5.012371	192.168.2.87	216.58.212.46		ICMP
32	5.057276	216.58.212.46	192.168.2.87		TCP
33	5.395402	192.168.2.41			
34	5.503764	192.168.2.41			

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



The screenshot shows the 'Packet Range' dialog box in Wireshark. The 'Displayed' radio button is selected. The 'Marked packets only' option is selected, showing 3 captured and 3 displayed packets. The 'Range' field is empty, and the 'Remove ignored packets' checkbox is unchecked.

Option	Captured	Displayed
<input type="radio"/> All packets	181	181
<input type="radio"/> Selected packets only	1	1
<input checked="" type="radio"/> Marked packets only	3	3
<input type="radio"/> First to last marked	3	3
<input type="radio"/> Range: <input type="text"/>	0	0
<input type="checkbox"/> Remove ignored packets	0	0

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

```
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.

```
root@kali: ~/meryemakdogan
File Edit View Search Terminal Help
root@kali:~/meryemakdogan# 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:~/meryemakdogan#
```

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

Gördüğümüz üzere bu dosyanın **paket1.pcap** ve **paket2.pcap** isimli iki dosyanın birleştirilmesi sonucu oluştuğunu belirtiyor.