



Araştırma Görevlisi
Dilara DEĞERLİYURT

WIRESHARK

- Bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkan tanır.
- Bilgisayara bağlı her türlü ağ kartlarındaki tüm TCP/IP mesajlarını analiz edebilen bir programdır.
- Kurulum için gereken dosyaları <http://www.wireshark.org> adresinden elde edebilirsiniz.

WIRESHARK ÖZELLİKLERİ

- Unix ve Windows işletim sistemleri için uygundur.
- Yerel ağ arayüzünden paketleri tutar ve ayrıntılı bir biçimde protokol bilgileriyle görüntüler
- Tutulan paketleri kaydetme özelliği vardır
- Çeşitli kriterlerde paket arar ve filtreler
- Alınan ve gönderilen paketleri filtrelemeyi baz alarak renklere ayırır ve kategorize eder.
- Çeşitli istatistikleri yapılan ayarlar doğrultusunda kullanıcıya sunar.
- 750'nin üzerinde protokolü analiz eder

Kullanım alanları;

- Paketlerdeki ikili veri seklindeki bilgileri, okunabilir bir formata dönüştürmede kullanılır.
- Ağdaki problemleri çözmede kullanılır.
- Ağın performansını analiz etmek için kullanılır.
- Ağa izinsiz girenleri tespit etmede kullanılır.
- Uygulamaların gerçekleştirdiği operasyonları analiz etmede kullanılır.
- Ağ kartındaki hataları bulmada kullanılır.

Ana Pencere

Menu Bar File Edit View Go Capture Analyze Statistics Help

Tool Bar [Icons: Open, Save, Print, Copy, Paste, Undo, Redo, Find, Filter, etc.]

Filter Bar Filter: [Text Field] Expression... Clear Apply

Summary Window

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [FIN, PSH, ACK] Seq=
2	0.000031	192.168.0.15	192.168.0.33	TCP	2123 > bgp [ACK] Seq=0 Ack=1 w1
3	0.000422	192.168.0.15	192.168.0.33	TCP	2123 > bgp [FIN, ACK] Seq=0 Ack
4	0.006057	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [ACK] Seq=1 Ack=1 wi
5	7.999977	192.168.0.15	192.168.0.33	TCP	2124 > bgp [SYN] Seq=0 Len=0 MS
6	8.003909	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [SYN, ACK] Seq=0 Ack
7	8.003954	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=1 Ack=1 wi
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
9	8.208048	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK] Seq=1 Ack=30 w
10	8.337997	192.168.0.33	192.168.0.15	BGP	OPEN Message
11	8.338027	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=30 Ack=30
12	8.338115	192.168.0.15	192.168.0.33	BGP	KEEPALIVE Message

Protocol Tree Window

- Frame 8 (83 bytes on wire, 83 bytes captured)
 - Ethernet II, Src: DellComp_23:c5:95 (00:c0:4f:23:c5:95), Dst: Cisco_35:0e:1c (00:00:0c:35:0e:1c)
 - Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.33)
 - Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1, Len: 1
 - Border Gateway Protocol

Data View Window

Offset	Hex	ASCII
0000	00 00 0c 35 0e 1c 00 c0 4f 23 c5 95 08 00 45 00	...5.... 0#....E.
0010	00 45 48 e9 40 00 40 06 70 49 c0 a8 00 0f c0 a8	.EH.0.0. pI.....
0020	00 21 08 4c 00 b3 d6 33 9d 62 7a 40 e0 46 50 18	!.L...3 .bz0.FP.
0030	7d 78 19 03 00 00 ff ff ff ff ff ff ff ff ff ff	}x.....
0040	ff ff ff ff ff ff 00 1d 01 04 fe 09 00 b4 c0 a8	
0050	00 0f 00	...

File: "C:\Wireshark\bgp.pcap" 1911 Bytes 00:00:08 P: 20 D: 20 M: 0

Information Field

Display Information Field

Ana Pencere Bileşenleri

Pencere Bileşeni Tanımı

- **Menu Bar** :Menudeki maddelerin, grafiksel ara yüzünü içeren klasik bir uygulamadır.
- **Tool Bar** :Wireshark'ın sık kullanılan fonksiyonlarının kısa yollarını içerir. Kullanıcıya göre ayarlanabilir.
- **Filter Bar** :Yakalanan paketleri, istenilen şekilde ayrılarak gösterilmesini sağlar.
- **Summary Window** :Yakalan paketlerin her biri için, bir satırlık özet bilgi sunar.
- **Protocol Tree Window** :Summary window'da seçili olan paketin detaylı bilgilerini, kullanıcıların anlayacağı şekilde düzenleyerek sunar.
- **Data View Window** :Summary window'da seçili olan paketin, detaylı bilgilerini, herhangi bir düzenleme yapmadan sunar.
- **Display Information Field** :Paketlerin numaralarını, güncel olarak gösterir.

Summary Window

Yakalanmış paketlerin tamamına buradan bakılabilir. Her bir dosyanın içeriği bir satır olarak sunulur, satırlar belli özelliklerine göre sütunlara ayrılır.

Sütun Adı	Tanımı
No	Yakalanan dosyanın içindeki paketlerin numarasını temsil eder. Görüntüleme filtresi (display filter) kullanılmadığı sürece bu numara değiştirilemez.
Time	Paketin zaman damgasıdır.
Source	Paketin nereden geldiğini gösterir.
Destination	Paketin nereye gittiğini gösterir.
Protocol	Protokol isminin kısa versiyonudur.
Info	Paket içeriği hakkında ekstra bilgi gösterir.

Summary Window

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [FIN, PSH, ACK] Seq=...
2	0.000031	192.168.0.15	192.168.0.33	TCP	2123 > bgp [ACK] Seq=0 Ack=1
3	0.000422	192.168.0.15	192.168.0.33	TCP	2123 > bgp [FIN, ACK] Seq=0 Ack=...
4	0.006057	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [ACK] Seq=1 Ack=1
5	7.999977	192.168.0.15	192.168.0.33	TCP	2124 > bgp [SYN] Seq=0 Len=0
6	8.003909	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [SYN, ACK] Seq=0 Ack=...
7	8.003954	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=1 Ack=1
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
9	8.208048	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK] Seq=1 Ack=30
10	8.337997	192.168.0.33	192.168.0.15	BGP	OPEN Message
11	8.338027	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=30 Ack=30
12	8.338115	192.168.0.15	192.168.0.33	BGP	KEEPALIVE Message

Sütun Adı	Değeri
No	8
Time	8.004042 (yakalama işlemine başlanıldığından itibaren)
Source	IP numarası 192.168.0.15
Destination	IP numarası 192.168.0.33
Protocol	Border Gateway Protocol (BGP)
Info	OPEN Message

Protocol Tree Window

- Paketi bütün protokol'lerin bir üst ağacı(tree) olarak canlandırılabilir. Her bir protokol için ağaç düğümü(tree node) oluşturulur. Bu ağaç düğümleri sayesinde, protokol alanı daha geniş bir şekilde tanımlanabilir. Herhangi bir ağaç düğümünün alt ağaca sahip olması,onun daha geniş bilgiler gösterecek şekilde genişletilebileceğini veya sadece özet bilgiler gösterecek şekilde daraltılabileceğini gösterir.

Protocol Tree Window

Frame 8 (83 bytes on wire, 83 bytes captured)
Ethernet II, Src: DellComp_23:c5:95 (00:c0:4f:23:c5:95), Dst: Cisco_35:0e:1c (00:00:0c:35:0e:1c)
Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.33)
Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1, Len: 1
Border Gateway Protocol

Katman	Protocol	Tanım
Packet Meta Data	Frame	83 bytes on wire, 83 bytes Captured
Data Link (Layer 2/L2)	Ethernet II	Src Addr: 00:c0:4f:23:c5:95, Dst Addr: 00:00:0c:35:0e:1c
Network (Layer 3/L3)	IP	Src Addr: 192.168.0.15, Dst Addr: 192.168.0.33
Transport (Layer 4/L4)	Transmission Control Protocol (TCP)	Src Port: 2124, Dst Port: bgp(179), Seq: 2593706850, Ack ...
Application Layer (Layer 7/L7)	BGP	

Protocol Tree Window

The image shows the Wireshark interface with the title bar "bgp.pcap - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, capture, and analysis. Below the toolbar is a filter bar with a text input field labeled "Filter:" and buttons for "Expression...", "Clear", and "Apply".

The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Info
7	8.003954	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=1 Ack=1
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
9	8.208048	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK] Seq=1 Ack=30
10	8.237007	192.168.0.33	192.168.0.15	BGP	OPEN Message

The packet details pane shows the expanded details of Frame 8 (83 bytes on wire, 83 bytes captured):

- Ethernet II, Src: DellComp_23:c5:95 (00:c0:4f:23:c5:95), Dst: Cisco_35:0e:1c (00:00:0c:35:0e:1c)
- Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.33)
- Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1, Len: 29
- Border Gateway Protocol
 - OPEN Message
 - Marker: 16 bytes
 - Length: 29 bytes
 - Type: OPEN Message (1)
 - Version: 4
 - My AS: 65033
 - Hold time: 180
 - BGP identifier: 192.168.0.15
 - Optional parameters length: 0 bytes

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

```
0000  00 00 0c 35 0e 1c 00 c0 4f 23 c5 95 08 00 45 00  ...5.... 0#....E.
0010  00 45 48 e9 40 00 40 06 70 49 c0 a8 00 0f c0 a8  .EH.@.@. pI.....
0020  00 21 08 4c 00 b3 d6 33 9d 62 7a 40 e0 46 50 18  .!.L...3 .bz@.FP.
0030  7d 78 19 03 00 00 ff ff ff ff ff ff ff ff ff  }x.....
0040  ff ff ff ff ff ff ff ff 01 04 fe 09 00 b4 c0 a8  .....
0050  00 0f 00
```

The status bar at the bottom indicates "BGP message type (bgp type), 1 byte" and "P: 20 D: 20 M: 0".

Data View Window

Protocol Tree window bölümünden, BGP Message Type alanı seçilmiştir. Data view window bölümünde belirginlesen “0040” offset’i paketin, 0x40 hexadecimal’lik ya da 64 byte’lık olduğunu göstermektedir. Belirginlesen 9. Byte “01” değerini göstermektedir. Bu değer ASCII tablosundaki karşılığını (şekildeki üçüncü yuvarlak) “.” işareti bulunmaktadır.

Offset of
First Octet
in Row
(in Hex)

The image shows the Wireshark Data View window for a BGP message. The top pane shows the packet list with the following entries:

No.	Time	Source	Destination	Protocol	Info
7	8.003954	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK]
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
9	8.208048	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK]
10	8.337997	192.168.0.33	192.168.0.15	BGP	OPEN Message
11	8.338027	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK]
12	8.338115	192.168.0.15	192.168.0.33	BGP	KEEPALIVE Message
13	8.342206	192.168.0.33	192.168.0.15	BGP	KEEPALIVE Message
14	8.349836	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK]
15	8.344101	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK]

The middle pane shows the details of the selected BGP message (packet 8):

- Marker: 16 bytes
- Length: 29 bytes
- Type: OPEN Message (1)
- Version: 4
- My AS: 65033
- Hold time: 180
- BGP Identifier: 192.168.0.15

The bottom pane shows the raw data in hex and ASCII:

Offset	Hex	ASCII
0000	00 00 0c 35 0e 1c 00 c0 4f 23 c3 93 08 00 43 00	...5...0F...E.
0010	00 45 48 e9 40 00 40 06 70 49 c0 a8 00 0f c0 a8	.EH.@.@.pI.....
0020	00 21 08 4c 00 b3 d6 33 9d 62 7a 40 e0 46 50 18	.!L...3.bz@.FP.
0030	7d 78 19 03 00 00 ff ff ff ff ff ff ff ff	}x.....
0040	ff ff ff ff ff ff 00 1d 04 fe 09 00 b4 c0 a8	
0050	00 0f 00	...

The offset 0040 is circled in the hex column. The hex value 04 is circled in the hex column. The ASCII value "." is circled in the ASCII column.

Bytes in Field (in Hex) 04 fe 09 00 b4 c0 a8

Bytes in Field (in ASCII)

BGP message type (bgp.type), 1 byte

P: 20 D: 20 M: 0

Display Information Field

1	0.000000	192.168.1.102	192.168.1.104	SNMP	92 get-request 1.3.6.1.4.1.11.
2	0.017529	192.168.1.104	192.168.1.102	SNMP	93 get-response 1.3.6.1.4.1.11.
3	3.017792	192.168.1.102	192.168.1.104	SNMP	92 get-request 1.3.6.1.4.1.11.
4	3.034939	192.168.1.104	192.168.1.102	SNMP	93 get-response 1.3.6.1.4.1.11.
5	6.035232	192.168.1.102	192.168.1.104	SNMP	92 get-request 1.3.6.1.4.1.11.
6	6.055514	192.168.1.104	192.168.1.102	SNMP	93 get-response 1.3.6.1.4.1.11.
7	7.196100	192.168.1.102	128.119.245.12	TCP	62 visicron-vs > http [SYN] Seq=
8	7.236504	128.119.245.12	192.168.1.102	TCP	62 http > visicron-vs [SYN, ACK]
9	7.236533	192.168.1.102	128.119.245.12	TCP	54 visicron-vs > http [ACK] Seq=
10	7.236929	192.168.1.102	128.119.245.12	HTTP	555 GET /ethereal-labs/lab2-4.h
11	7.258634	128.119.245.12	192.168.1.102	TCP	60 http > visicron-vs [ACK] Seq=
12	7.260813	128.119.245.12	192.168.1.102	HTTP	1057 HTTP/1.1 200 OK (text/html)
13	7.284335	192.168.1.102	165.193.123.218	TCP	62 compx-lockview > http [SYN]
14	7.285795	192.168.1.102	134.241.6.82	TCP	62 dserver > http [SYN] Seq=0
15	7.305086	165.193.123.218	192.168.1.102	TCP	62 http > compx-lockview [SYN,
16	7.305115	192.168.1.102	165.193.123.218	TCP	54 compx-lockview > http [ACK]

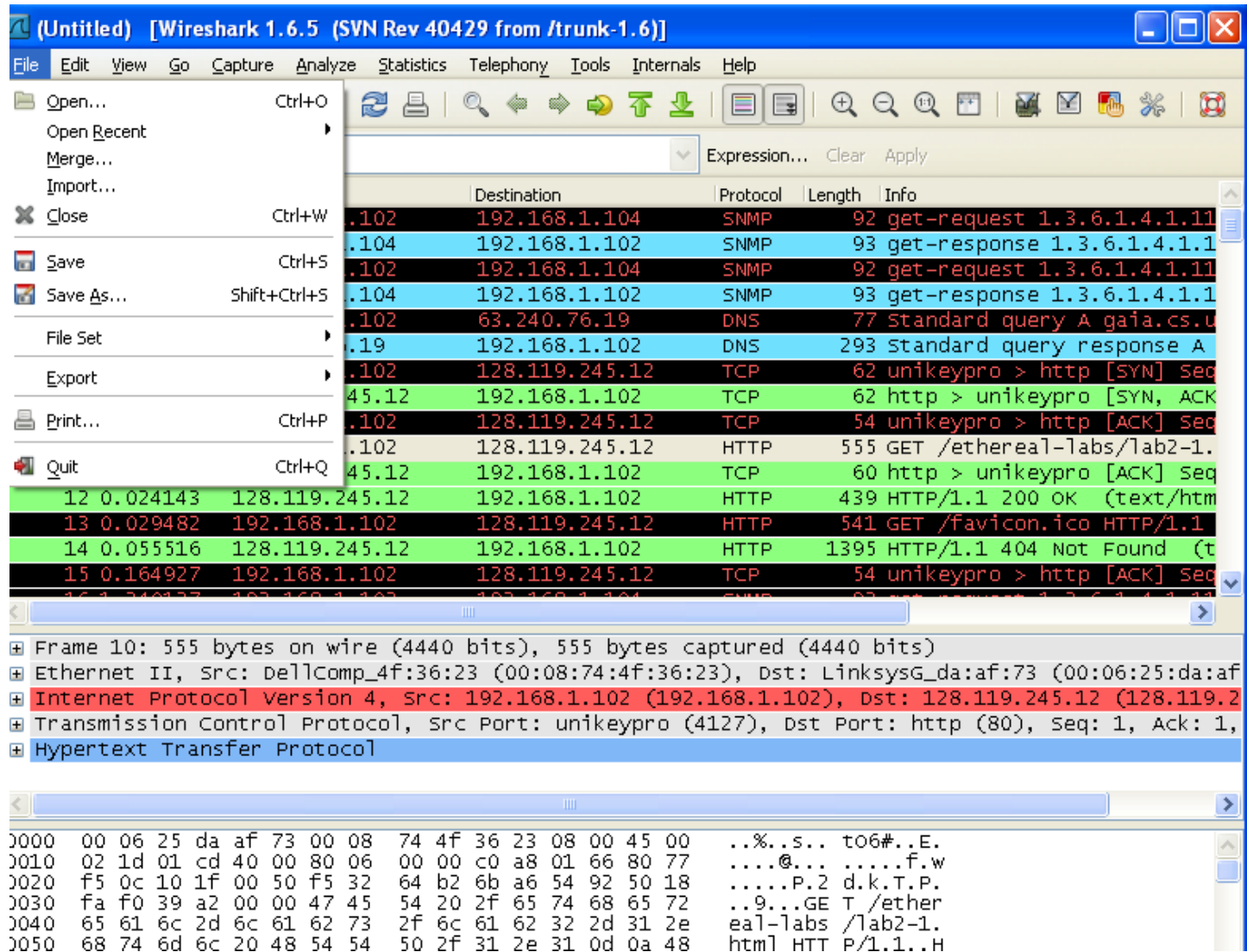
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)

Internet Protocol version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)

0000	00 08 74 4f 36 23 00 06	25 da af 73 08 00 45 00	..TO6#.. %.S..E.
0010	04 13 74 4b 40 00 37 06	94 07 80 77 f5 0c c0 a8	..tk@.7. ...w....
0020	01 66 00 50 10 d3 8c 57	c6 b8 fd 1d 3e 97 50 18	.f.P...w>.P.
0030	19 20 a6 22 00 00 48 54	54 50 2f 31 2e 31 20 32	. ."..HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 54 75 65	00 OK..D ate: Tue
0050	2c 20 32 33 20 53 65 70	20 32 30 30 33 20 30 35	, 23 Sep 2003 05
0060	3a 33 38 3a 34 34 20 47	4d 54 0d 0a 53 65 72 76	:38:44 G MT..Serv
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 30 2e 34	er: Apac he/2.0.4
0080	30 20 28 52 65 64 20 48	61 74 20 4c 69 6e 75 78	0 (Red H at Linux
0090	29 0d 0a 4c 61 73 74 2d	4d 6f 64 69 66 69 65 64	)..Last- Modified
00a0	3a 20 54 75 65 2c 20 32	33 20 53 65 70 20 32 30	: Tue, 23 Sep 20
00b0	30 33 20 30 35 3a 33 38	3a 30 30 20 47 4d 54 0d	03 05:38 :00 GMT.
00c0	0a 45 54 61 67 3a 20 22	31 62 66 66 39 2d 32 62	.ETag: " 1bff9-2b

File: "C:\Documents and Settings\Dilara\Desktop..." Packets: 61 Displayed: 61 Marked: 0 Load time: 0:00.015 Profile: Default

File Menüsü



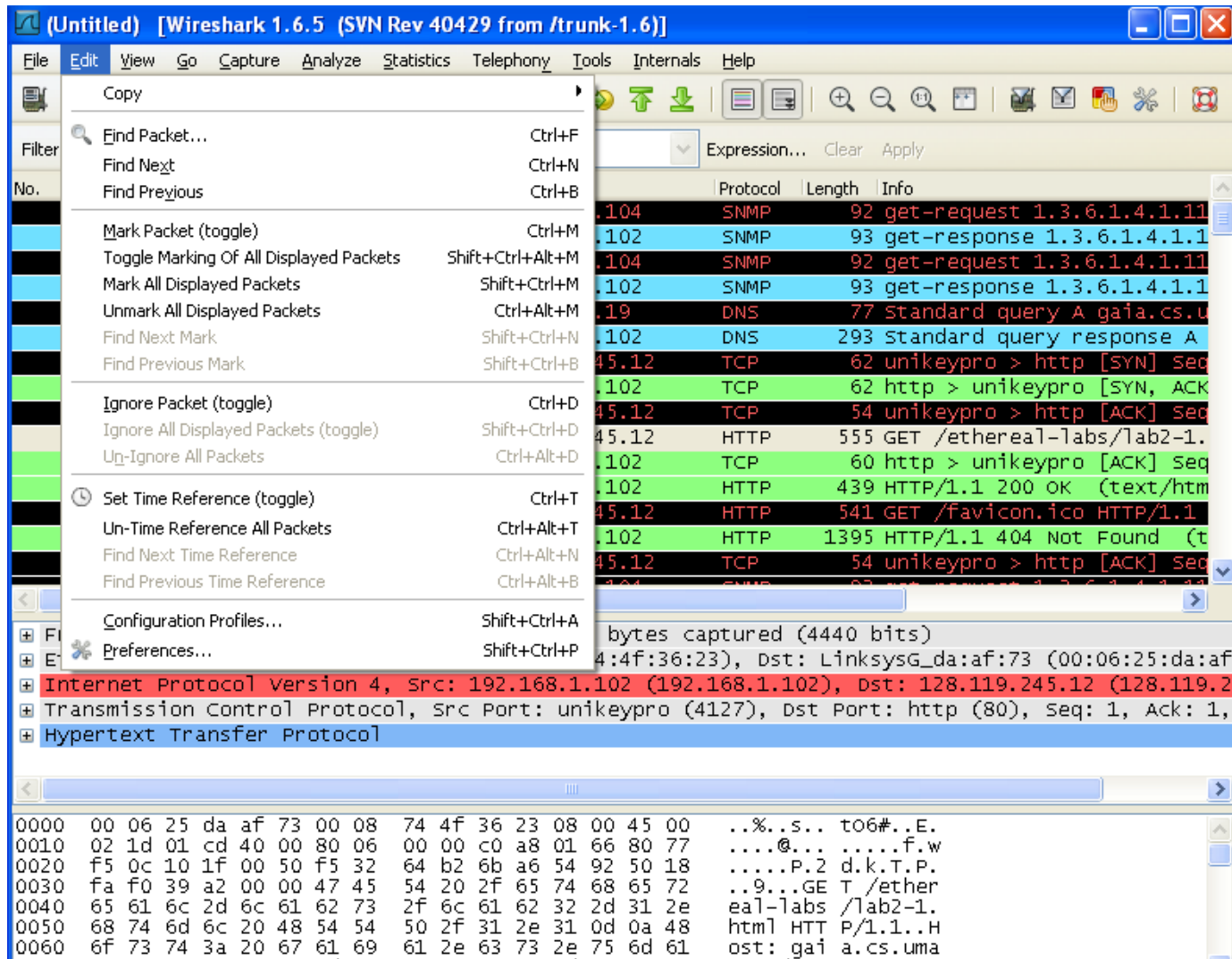
File Menüsü

Menü Seçeneği

Tanım

Open :	Kayıtlı olan bir wireshark dosyasını açmamıza yarar
Open Recent :	Son işlem gören wireshark dosyalarını listeler ve açmamıza yardımcı olur
Merge :	İki tane ayrı dosyayı tek bir dosyaymış gibi gösterir
Close:	Yakaladığımız dosyaları kapatır
Save:	Kaydet
Save As:	Kayıtlı olan bir dosyada yapılan değişiklikleri baska bir lokasyonda bağımsız olarak kaydetmemize olanak sağlar
File Set:	Dosyadaki bilgileri düzenlemek için bir altmenüdür
Export :	Baska bir dosyayı export etmemizi sağlar
Print :	Yazıcıdan çıktı alır
Quit:	Wireshark uygulamasından çıkar

Edit Menüsü



Edit Menüsü

Menü Seçeneği

Tanım

Find Packet(Paket Bul) :

Kullanılan filtreye, hex değere ya da stringe göre arama yapar ve bulduğu paketleri listeler

Find Next(Sonrakini Bul) :

Aramayla eslesen paketten bir sonraki paketi bulur

Find Previus(Öncekini Bul):

Aramayla eslesen paketten bir önceki paketi bulur

Mark Packet:

Summary Window da seçili olan paketi isaretler

Find Next Mark :

İsaretli olan paketler arasında bir sonraki isaretli paketi bulur

Find Previus Mark :

İsaretli olan paketler arasında bir önceki isaretli paketi bulur

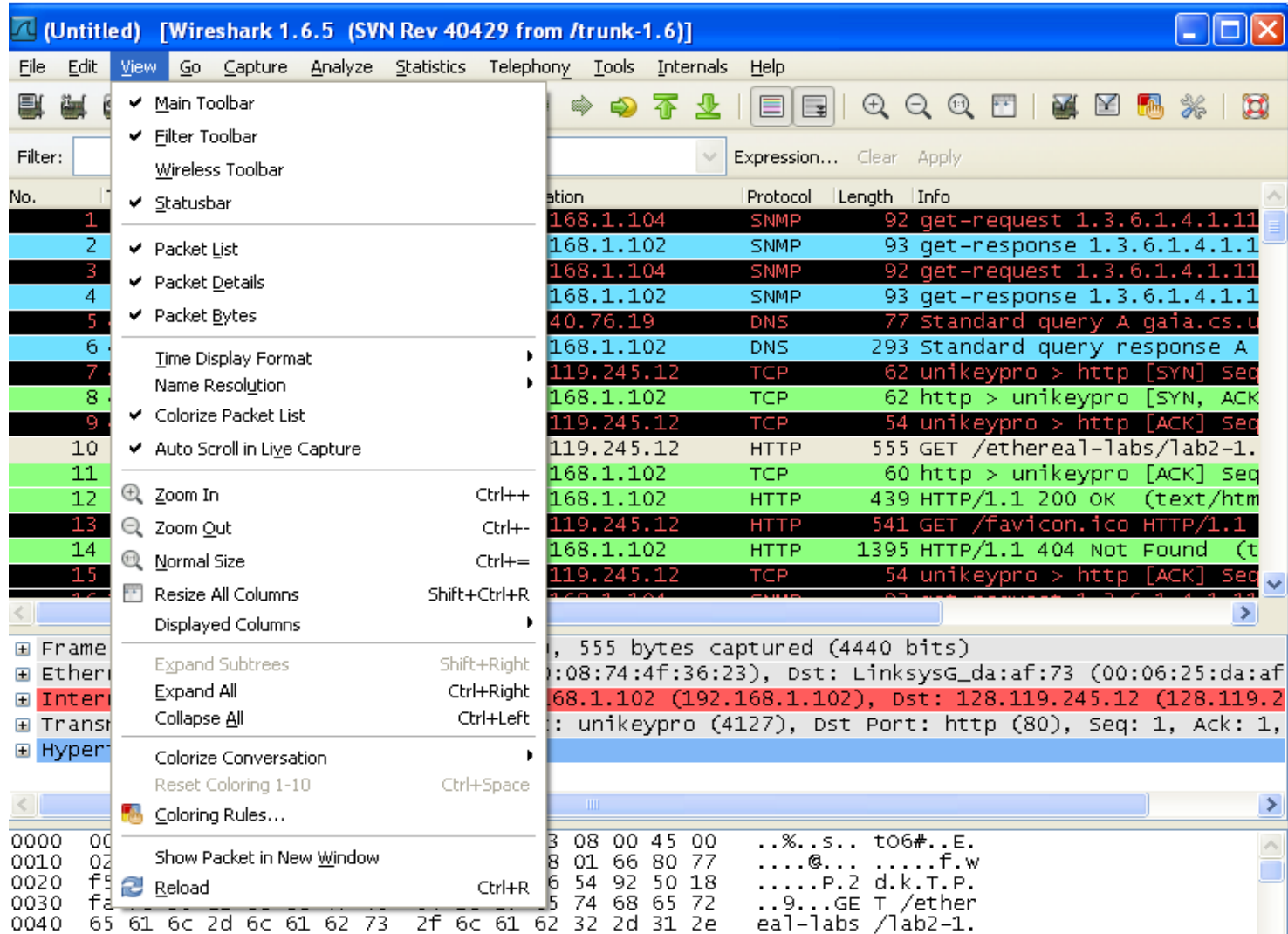
Set Time Referance :

Seçilen paketi zaman referansı olarak alır ve sonraki paketlerde o zaman değerlerine göre değerini alır.

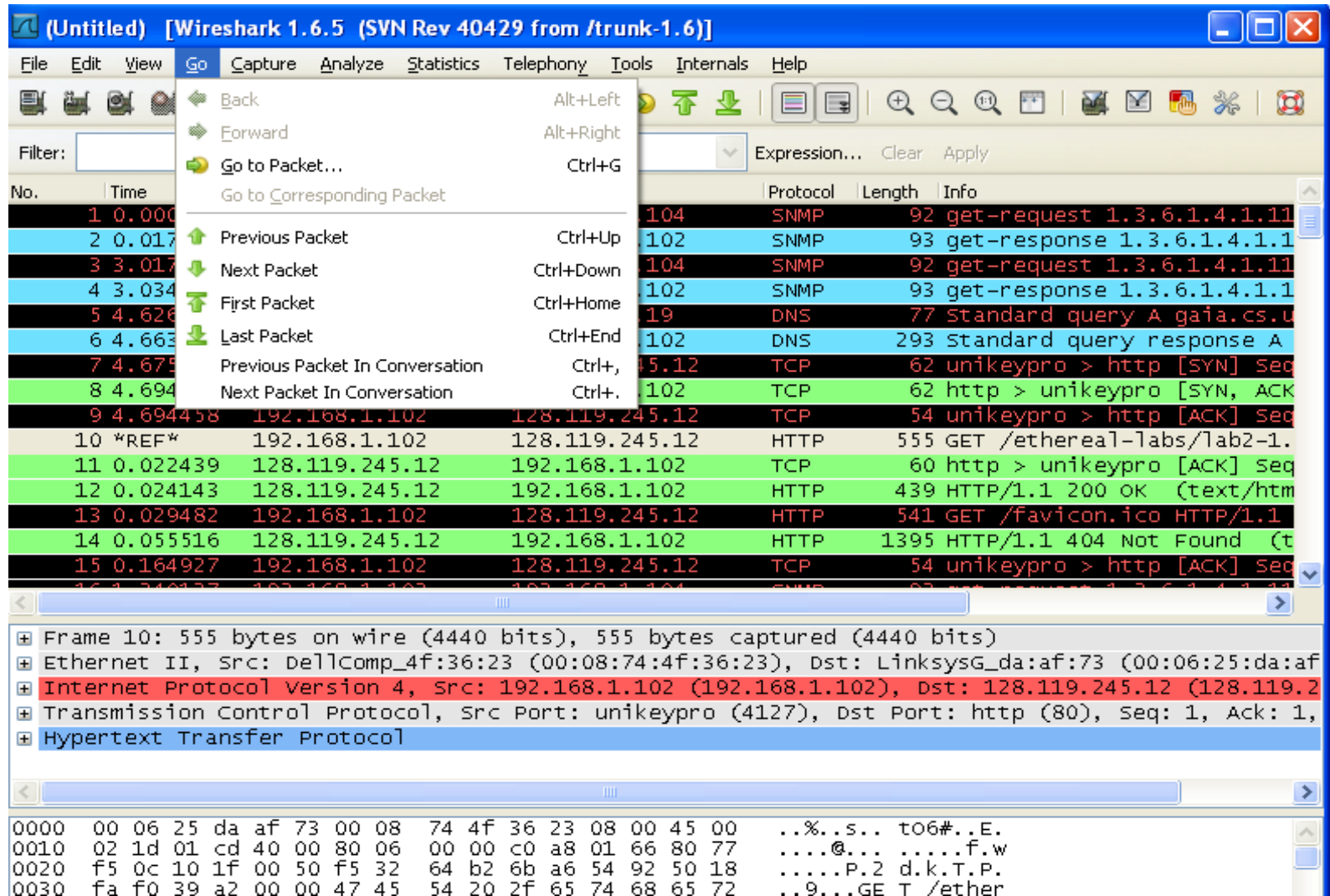
Preferences :

Kullanıcı tanımlı ayarları değiştirir

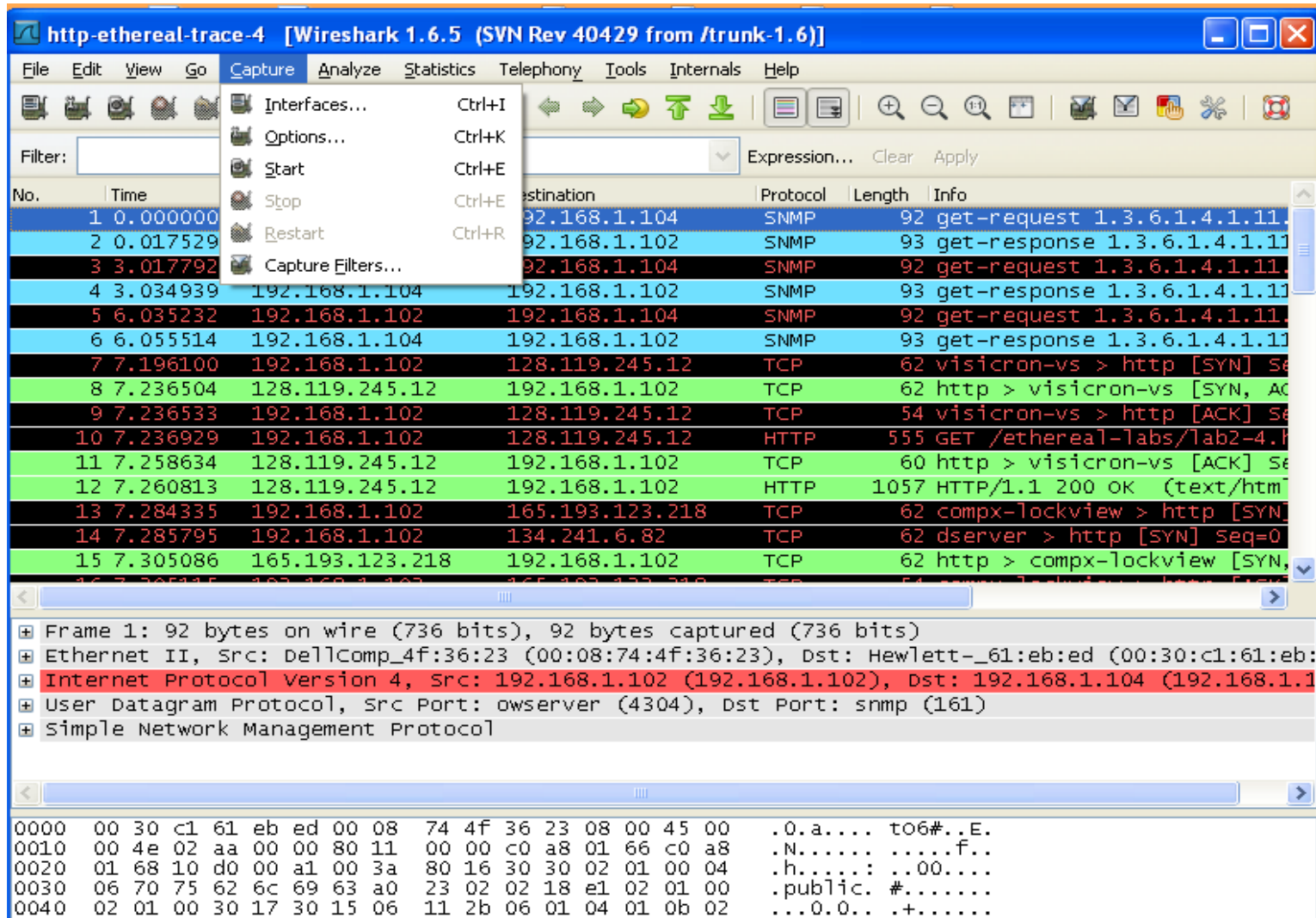
View Menüsü



Go Menüsü



Capture Menü



Capture Menüsü

Menü Seçeneği

Tanım

Interfaces:	Programda paket yakalama islemini baslattığımız yer
Options:	Paket ayarlama menüsünü açar
Start:	Paket yakalama islemini başlatır
Stop :	Paket yakalama islemini durdurur
Restart :	Durdurulan paket yakalama işlemine tekrar devam eder
Capture Filters :	Yakalama filtresini ayarlar

Analyze Menü

The image shows the Wireshark 1.6.5 interface. The title bar reads "http-ethereal-trace-4 [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]". The menu bar includes File, Edit, View, Go, Capture, **Analyze**, Statistics, Telephony, Tools, Internals, and Help. The Analyze menu is open, showing options: Display Filters..., Display Filter Macros..., Apply as Column, Apply as Filter, Prepare a Filter, Enabled Protocols... (Shift+Ctrl+E), Decode As..., User Specified Decodes..., Follow TCP Stream, Follow UDP Stream, Follow SSL Stream, Expert Info Composite, and Conversation Filter. The packet list on the right shows a series of SNMP and TCP packets. The packet details pane shows the structure of a packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Network Management Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Filter:

No.	Time	Source
1	0.000000	192.
2	0.017529	192.
3	3.017792	192.
4	3.034939	192.
5	6.035232	192.
6	6.055514	192.
7	7.196100	192.
8	7.236504	128.
9	7.236533	192.
10	7.236929	192.
11	7.258634	128.
12	7.260813	128.
13	7.284335	192.168.1.102
14	7.285795	192.168.1.102
15	7.305086	165.193.123.218

Enabled Protocols... Shift+Ctrl+E

Decode As...

User Specified Decodes...

Follow TCP Stream

Follow UDP Stream

Follow SSL Stream

Expert Info Composite

Conversation Filter

Protocol	Length	Info
SNMP	92	get-request 1.3.6.1.4.1.11.
SNMP	93	get-response 1.3.6.1.4.1.11.
SNMP	92	get-request 1.3.6.1.4.1.11.
SNMP	93	get-response 1.3.6.1.4.1.11.
SNMP	92	get-request 1.3.6.1.4.1.11.
SNMP	93	get-response 1.3.6.1.4.1.11.
TCP	62	visicron-vs > http [SYN] Se
TCP	62	http > visicron-vs [SYN, AC
TCP	54	visicron-vs > http [ACK] se
HTTP	555	GET /ethereal-labs/lab2-4.f
TCP	60	http > visicron-vs [ACK] se
HTTP	1057	HTTP/1.1 200 OK (text/htm
TCP	62	comp-x-lockview > http [SYN]
TCP	62	dserver > http [SYN] Seq=0
TCP	62	http > comp-x-lockview [SYN]

Frame 6: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)

Ethernet II, Src: Hewlett-_61:eb:ed (00:30:c1:61:eb:ed), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)

Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.102 (192.168.1.102)

User Datagram Protocol, Src Port: snmp (161), Dst Port: pinghgl (4306)

Simple Network Management Protocol

Offset	Hex	ASCII
0000	00 08 74 4f 36 23 00 30 c1 61 eb ed 08 00 45 00	..to6#.0 .a....E.
0010	00 4f ed 8a 00 00 3c 11 0c f5 c0 a8 01 68 c0 a8	.O....<. h..
0020	01 66 00 a1 10 d2 00 3b 6c 0e 30 31 02 01 00 04	.f.....; 1.01....
0030	06 70 75 62 6c 69 63 a2 24 02 02 18 e3 02 01 00	.public. \$......
0040	02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02	...0.0.. +.....

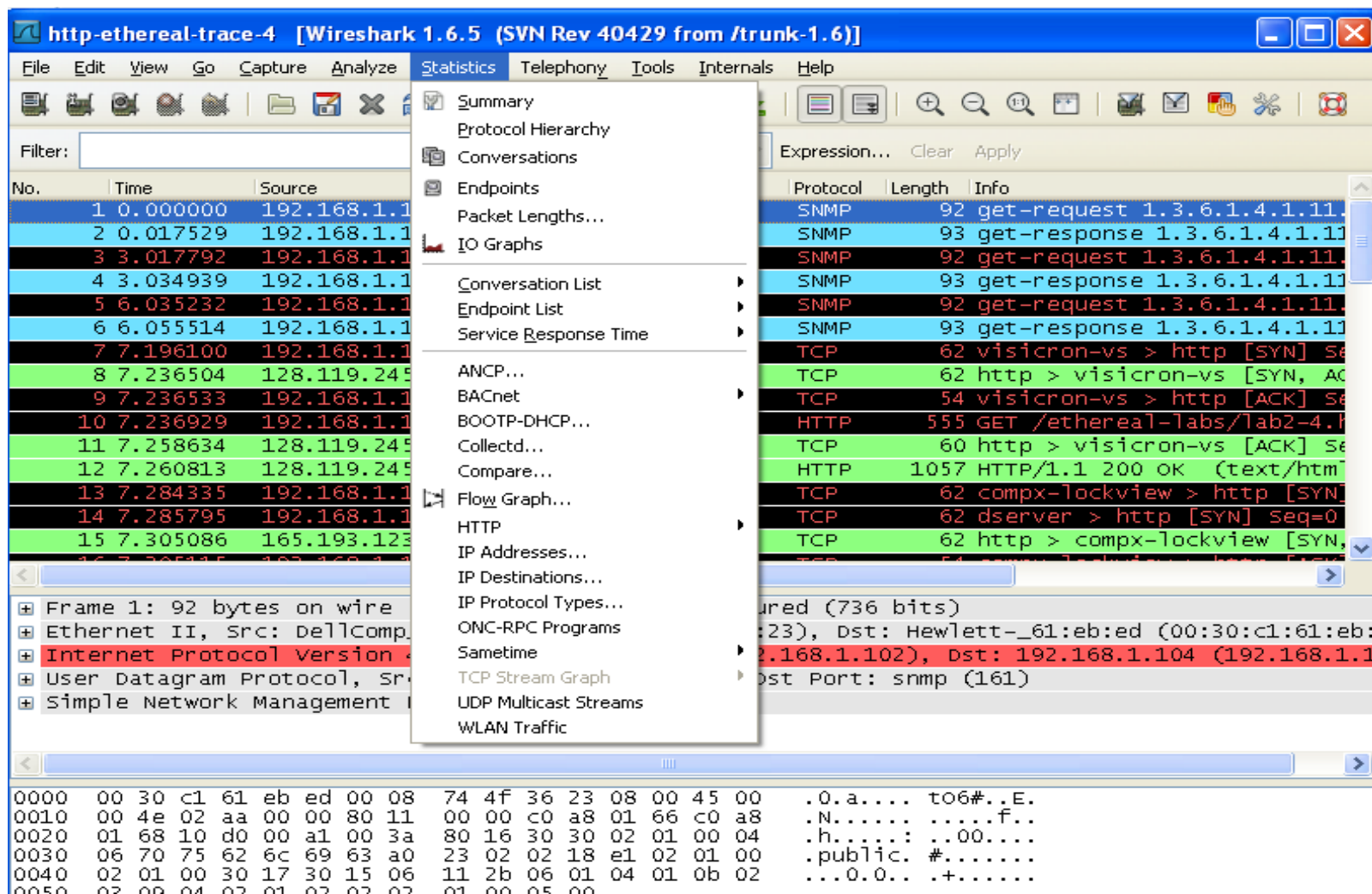
Analyze Menüsü

Menü Seçeneği

Tanım

Display Filter:	Yakalanan paketleri belirtilen ifadelere göre sıralar.
Decode As:	Paketleri belirli protokollere göre decode eder
User Specified Decodes:	Kullanıcının belirlediği çevrimleri görüntüler
Follow TCP Stream:	Seçilen paketle ilgili tcp bağlantılarının tüm tcp segmentlerini ayrı bir pencerede gösterir.
Expert Info:	İletişimde meydana gelen olayların kayıt sistemidir.Yakalanan paketleri errors,notes,warnings,chats kriterlerine göre ayırır.

Statistics Menüsü



The image shows the Wireshark 1.6.5 interface with the Statistics menu open. The menu lists various analysis tools and statistics. The background shows a packet capture of an HTTP trace.

Statistics Menu Options:

- Summary
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths...
- IO Graphs
- Conversation List
- Endpoint List
- Service Response Time
- ANCP...
- BACnet
- BOOTP-DHCP...
- Collectd...
- Compare...
- Flow Graph...
- HTTP
- IP Addresses...
- IP Destinations...
- IP Protocol Types...
- ONC-RPC Programs
- Sametime
- TCP Stream Graph
- UDP Multicast Streams
- WLAN Traffic

Packet Capture Data (Selected Packet 15):

No.	Time	Source
1	0.000000	192.168.1.1
2	0.017529	192.168.1.1
3	3.017792	192.168.1.1
4	3.034939	192.168.1.1
5	6.035232	192.168.1.1
6	6.055514	192.168.1.1
7	7.196100	192.168.1.1
8	7.236504	128.119.245
9	7.236533	192.168.1.1
10	7.236929	192.168.1.1
11	7.258634	128.119.245
12	7.260813	128.119.245
13	7.284335	192.168.1.1
14	7.285795	192.168.1.1
15	7.305086	165.193.123

Packet Details (Selected Packet 15):

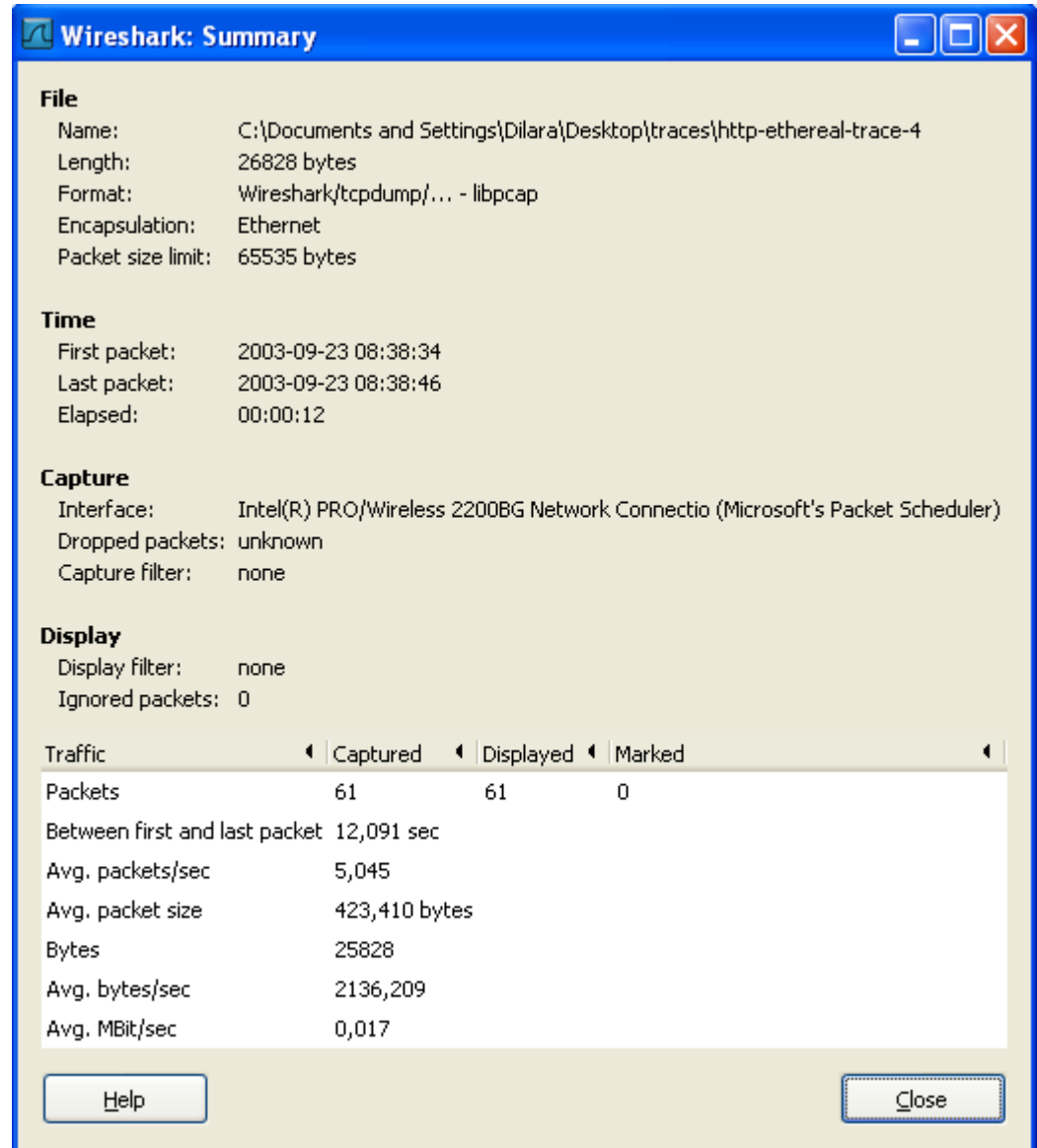
- Frame 15: 92 bytes on wire (736 bits)
- Ethernet II, Src: DellComp...
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
- User Datagram Protocol, Src Port: 54, Dst Port: 161
- Simple Network Management Protocol (SNMP), Type: GET-REQUEST (1)

Packet Bytes:

```
0000  00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00  .0.a...to6#..E.
0010  00 4e 02 aa 00 00 80 11 00 00 c0 a8 01 66 c0 a8  .N.....f..
0020  01 68 10 d0 00 a1 00 3a 80 16 30 30 02 01 00 04  .h.....:00...
0030  06 70 75 62 6c 69 63 a0 23 02 02 18 e1 02 01 00  .public.#.....
0040  02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02  ...0.0..+.....
0050  02 00 04 02 01 02 02 02 01 00 05 00
```

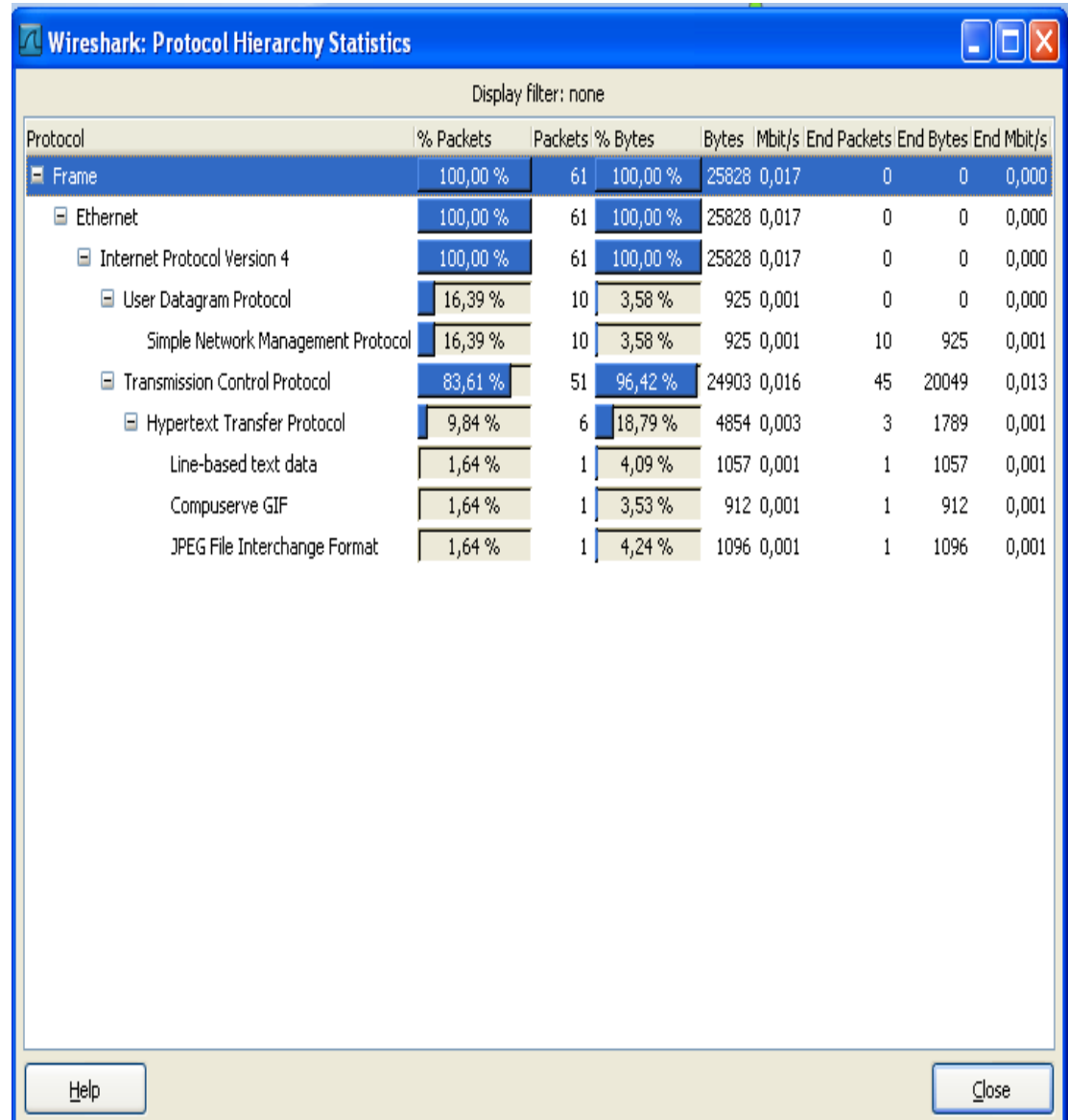
Statistics Menüsü

Summary: Açık olan yakalama dosyasında dosya formatı, paket sayısı, boyut, ilk ve son paket yakalama zamanları , filtre ve yakalama arabirimine ilişkin verileri içerir.



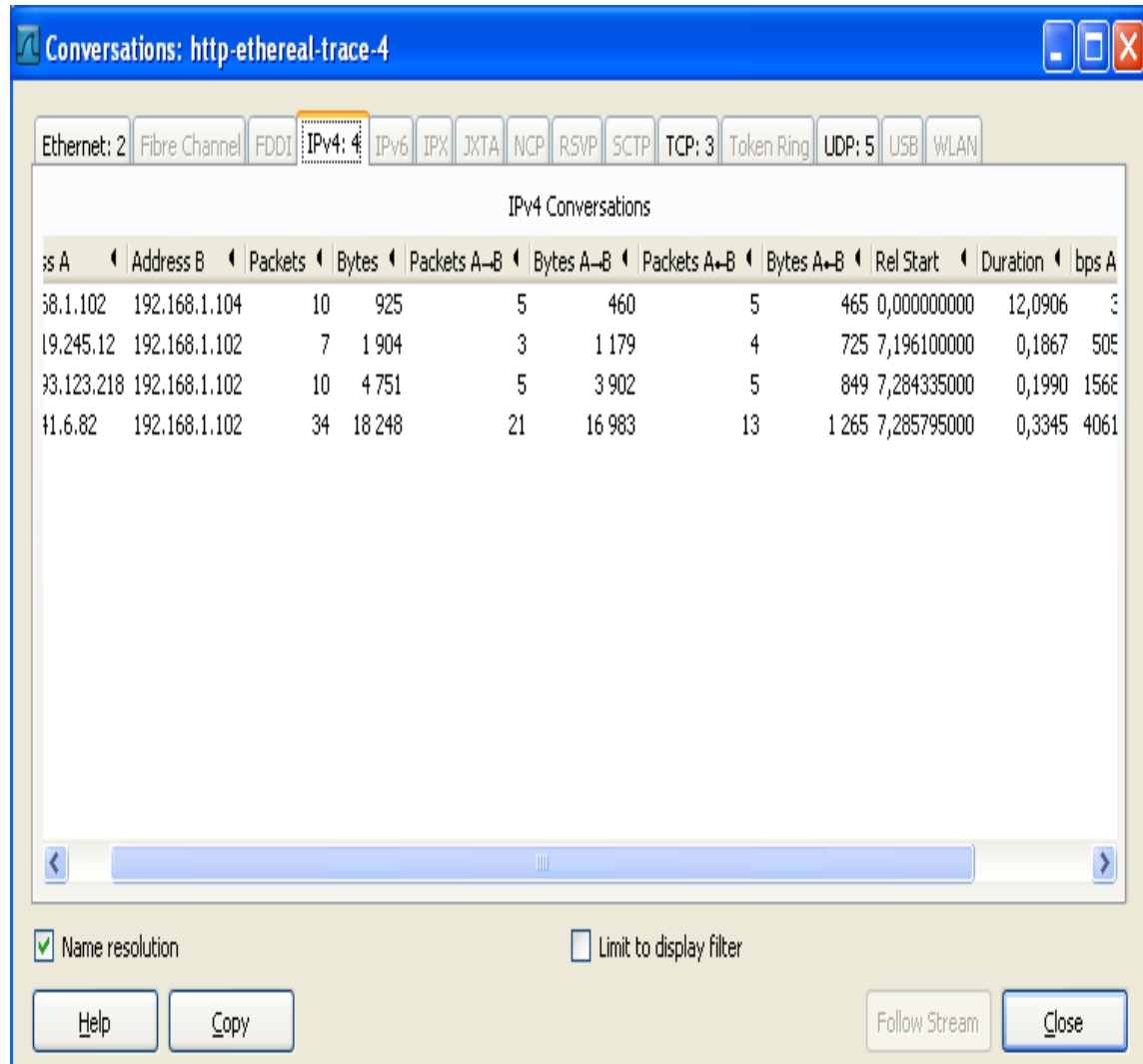
Statistics Menüsü

Protocol Hierarchy :
Yakalanan paketlerin
ağaç şeklinde katman
ve protokol
hiyerarşisini gösterir.



Statistics Menüsü

Conversations: Kaynak ve hedef noktaları arasındaki trafiğin istatistik bilgisini verir. Noktalar arasındaki toplam gelen giden paket ve byte miktarı portlara göre listelenir.



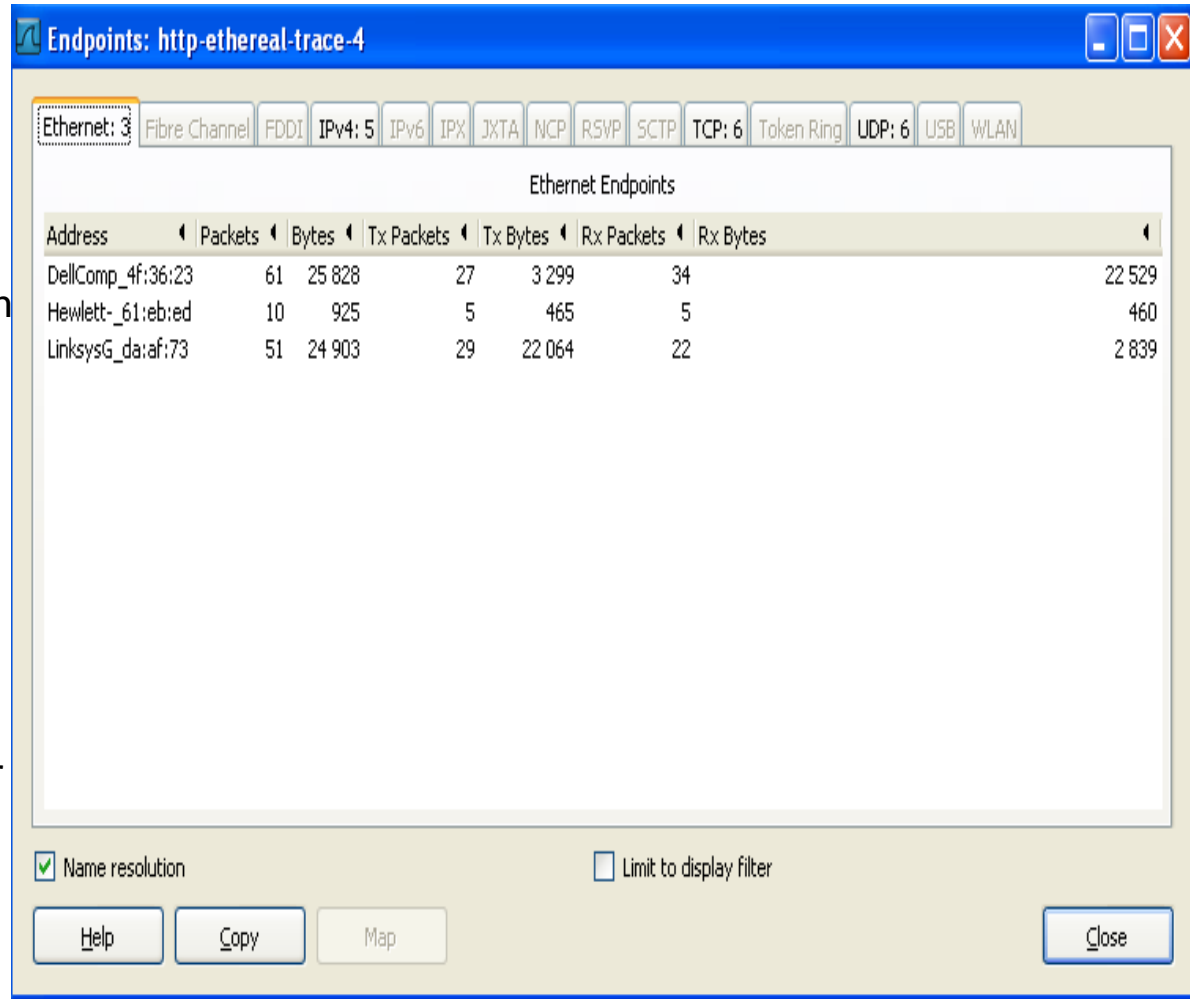
The screenshot shows the 'Conversations: http-ethereal-trace-4' window in Wireshark. The 'IPv4: 4' tab is selected, displaying a table of IPv4 conversations. The table has columns for Address A, Address B, Packets, Bytes, and bidirectional traffic statistics. The data shows four distinct conversations between various source IP addresses and the destination 192.168.1.102.

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Rel Start	Duration	bps A
58.1.102	192.168.1.102	10	925	5	460	5	465	0,000000000	12,0906	3
19.245.12	192.168.1.102	7	1 904	3	1 179	4	725	7,196100000	0,1867	505
33.123.218	192.168.1.102	10	4 751	5	3 902	5	849	7,284335000	0,1990	1566
11.6.82	192.168.1.102	34	18 248	21	16 983	13	1 265	7,285795000	0,3345	4061

At the bottom of the window, there are checkboxes for 'Name resolution' (checked) and 'Limit to display filter' (unchecked). Buttons for 'Help', 'Copy', 'Follow Stream', and 'Close' are also present.

Statistics Menüsü

Endpoints: Hedef ve kaynak adresi ayrımı yapmadan her son nokta için istatistik bilgisini verir. Desteklenen her protokol için ayrı bir sekme mevcuttur. Her sekmede yakalanan son nokta sayıları belirtilmektedir. Örneğin ethernet:3 hali hazırda 3 tane ethernet son noktasının yakalandığını söylemektedir. Eğer protokolle ilgili yakalanmış son nokta yoksa ilgili sekme silik şekilde görünmektedir. Her sıra bir son nokta için istatistiksel değerleri göstermektedir.



Endpoints: http-ethereal-trace-4

Ethernet: 3 | Fibre Channel | FDDI | IPv4: 5 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 6 | Token Ring | UDP: 6 | USB | WLAN

Ethernet Endpoints

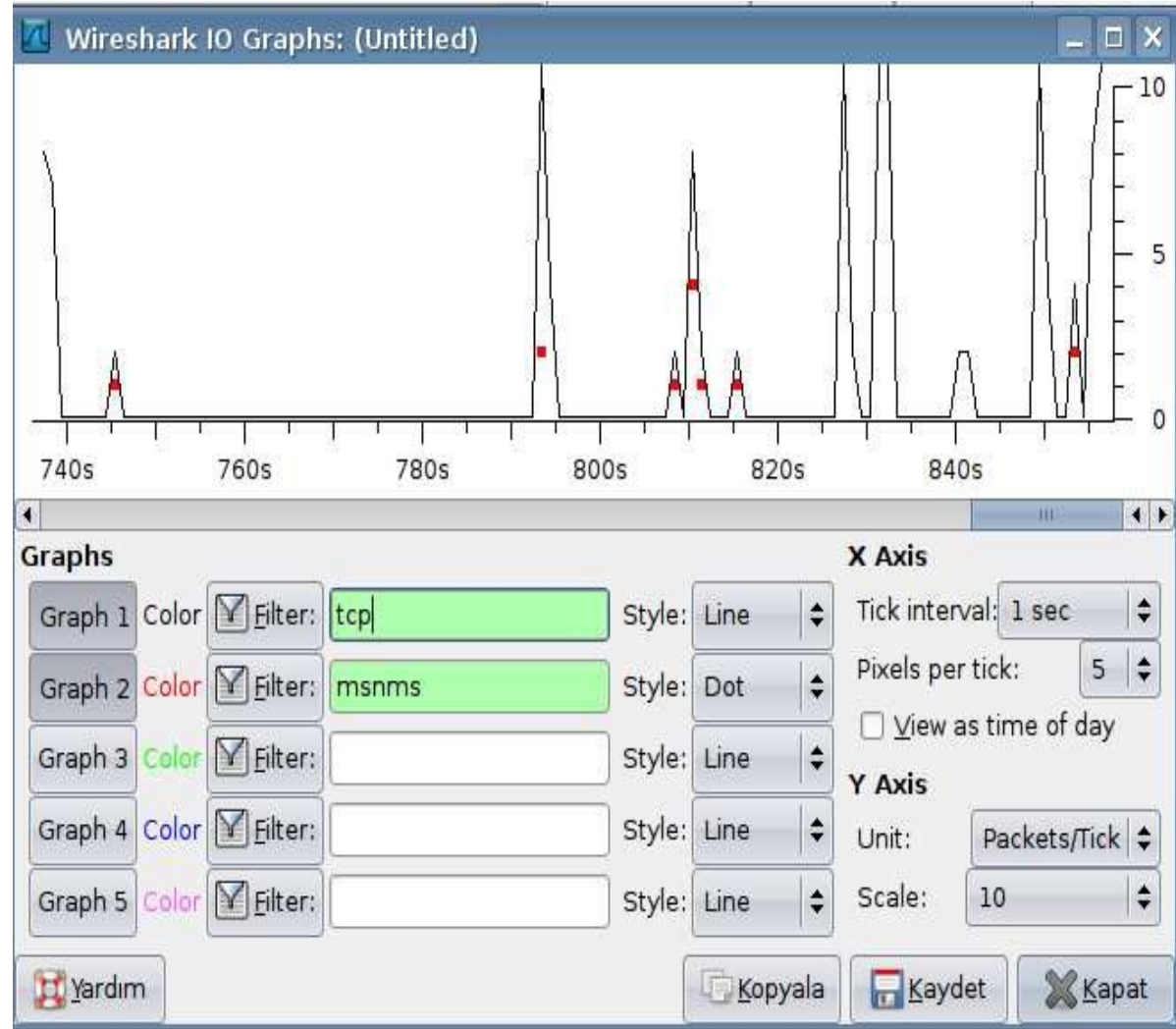
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
DellComp_4f:36:23	61	25 828	27	3 299	34	22 529
Hewlett_61:eb:ed	10	925	5	465	5	460
LinksysG_da:af:73	51	24 903	29	22 064	22	2 839

☒ Name resolution ☐ Limit to display filter

Help Copy Map Close

Statistics Menüsü

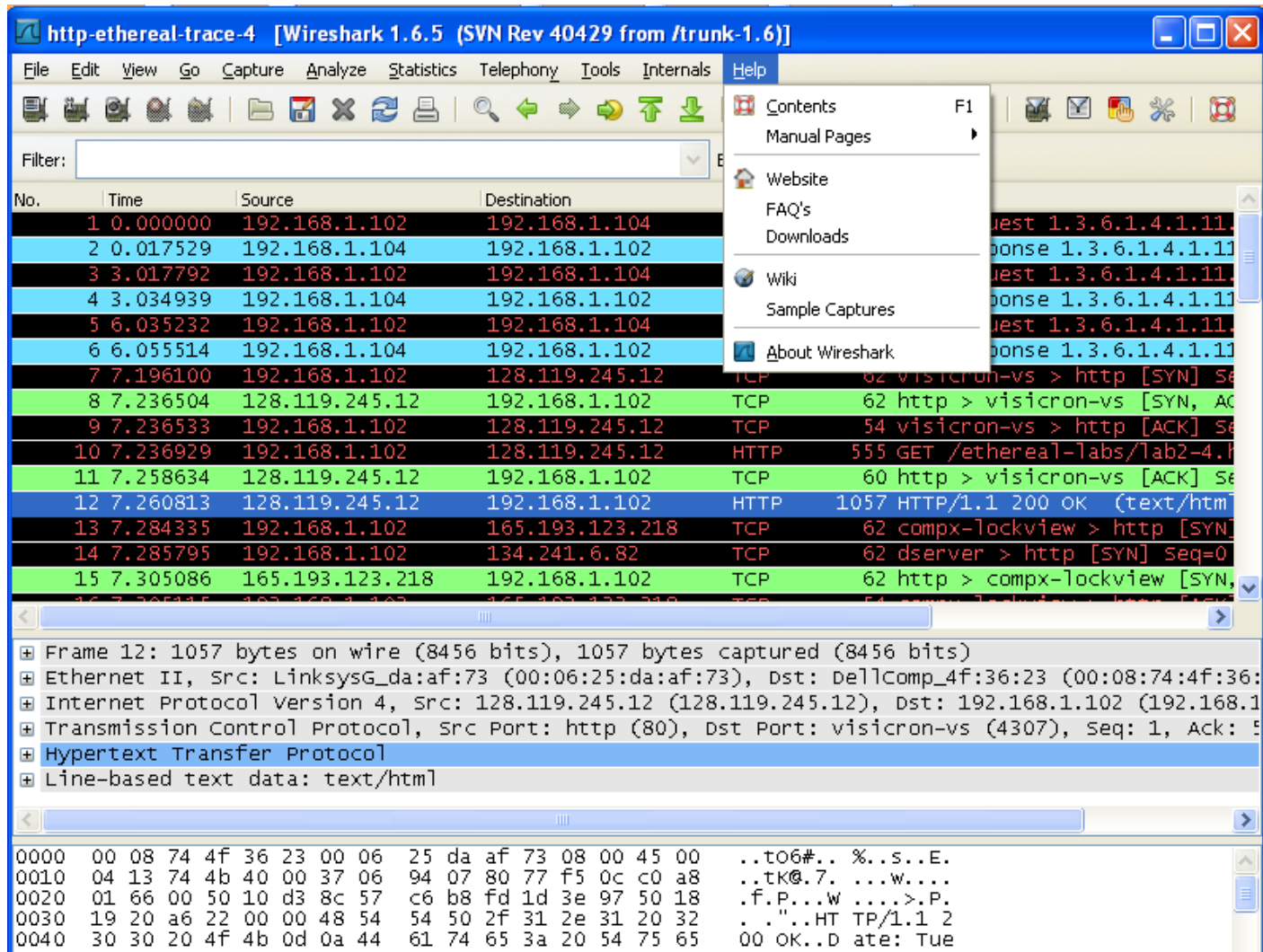
IO Graphs: Belirtilen özelliklerde paketlerin zamana göre akış grafiğini verir. Ağda durum kontrolü için oldukça faydalı bir özelliktir. Bu özellik ile normal paket akış diyagramında ağda meydana gelecek herhangi bir anormallik hemen farkedilebilir.



Statistics Menüsü

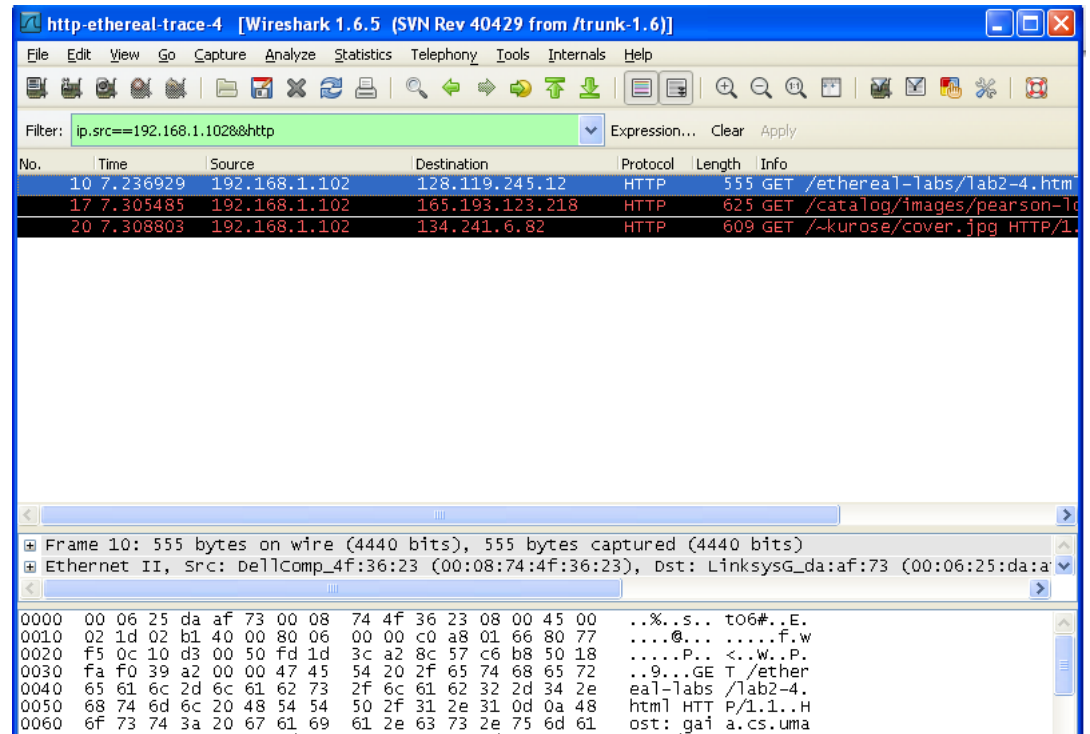
- **Service Response Time**: İstek ve cevap arasındaki zamanı gösterir.
- **Wlan Traffic Statics**: Yakalanan kablosuz ağ trafiğinin istatistik bilgisinin sunar.

Help Menüsü



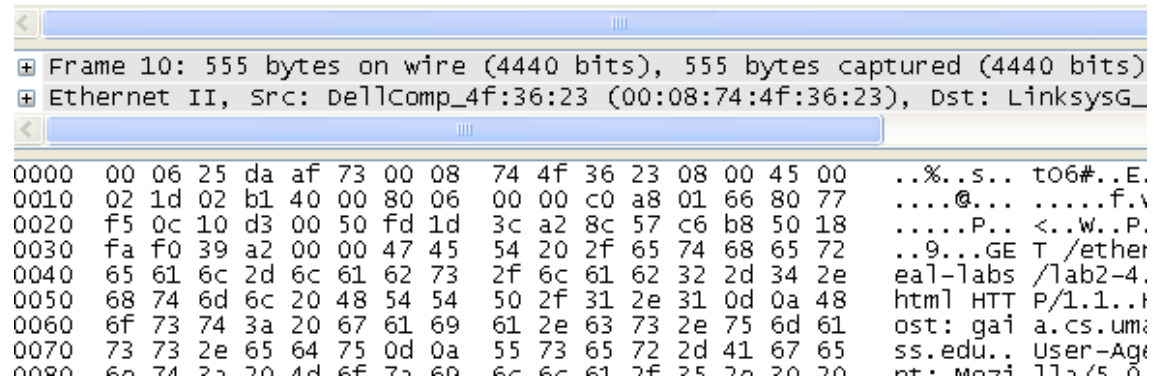
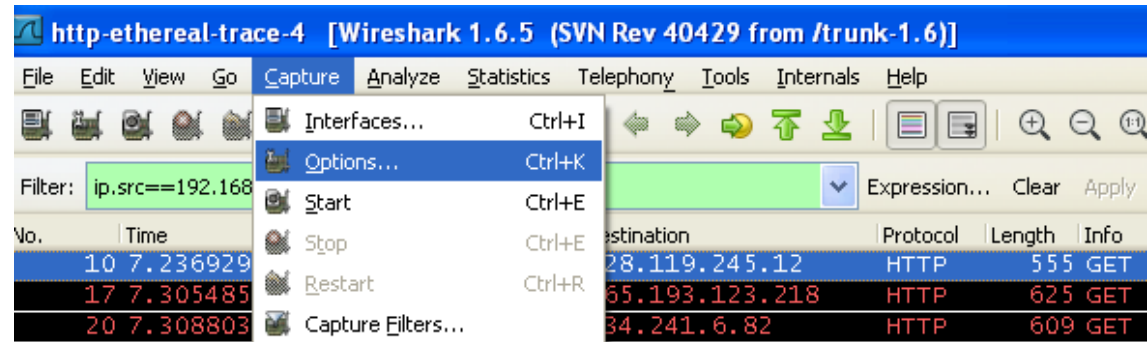
Filtreleme

Filter Bar summary window daki aldığımız paketleri filtre etmemize yarayan kısımdır. Filter Bar a herhangi bir filtre girdisi yaptığımızda summary window da sadece filtrelediğimiz paketler görünür olacaktır. Filter Bar da gördüğümüz filtre paketlerin durumlarını belirtir.



Fitreleme

Capture, options
penceresinden
belirtilen capture
filter, paket yakalama
sırasında wiresharkın
uyacağı koşulları
belirtir.



Wireshark: Capture Options

Capture

Interface: Local Intel(R) PRO/Wireless 2200BG Network Connectio (Microsoft's Pack

IP address: 192.168.2.104

Link-layer header type: Ethernet Wireless Settings

☒ Capture packets in promiscuous mode Remote Settings

☐ Capture packets in pcap-ng format

☒ Limit each packet to 65534 bytes Buffer size: 1 megabyte(s)

Capture Filter: Compile BPF

Capture File(s)

File: Browse...

☒ Use multiple files

☒ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☐ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Display Options

☒ Update list of packets in real time

☒ Automatic scrolling in live capture

☒ Hide capture info dialog

Name Resolution

☒ Enable MAC name resolution

☐ Enable network name resolution

☒ Enable transport name resolution

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Help Start Cancel

Wireshark: Capture Filter - Profile: Default

Edit

Capture Filter

Ethernet address 00:08:15:00:08:15

Ethernet type 0x0806 (ARP)

No Broadcast and no Multicast

No ARP

IP only

IP address 192.168.0.1

IPX only

TCP only

UDP only

TCP or UDP port 80 (HTTP)

HTTP TCP port (80)

No ARP and no DNS

Non-HTTP and non-SMTP to/from www.wireshark.org

New Delete

Properties

Filter name:

Filter string:

Help OK Cancel

Görüldüğü gibi capture filter penceresinde Wiresharkın paket yakalama sırasında uyacağı kurallar için bir liste sunulmuştur.

- **Ethernet address 00:08:15:00:08:15** : Ethernet II altında kaynak veya hedef adreslerinde belirtilen mac adresine ait paketleri yakalar.
- **Ethernet type 0x0806 (ARP), 0x0800 (IP), 0x8035(RARP), 0x6003 (DECNET), 0x6004 (DEC LAT), 0x6002 (MOP RC), 0x6001 (MOP DL)**
- **not broadcast and not multicast**: Broadcasting ve multicasting paketlerini yakalamaz.
- **not arp**: Arp pakelerini yakalamaz.
- **IP address 192.168.0.1** : Belirtilen ip adresini hedef yada kaynak adres kısımlarında barındıran paketler yakalanır.
- **IPX only** : İlgili protokole ilişkin paketleri yakalar.
- **TCP only** : İlgili protokole ilişkin paketleri yakalar.
- **UDP only** : İlgili protokole ilişkin paketleri yakalar.
- **TCP or UDP port 80 (http)** : Port 80 için tcp ve udp paketlerini yakalar.
- **HTTP TCP port (80)** : Port 80 için http ve tcp paketlerini yakalar.
- **No ARP and no DNS** : DNS ve ARP paketleri harici paketleri yakalar
- **NonHTTP and nonSMTP to/from www.wireshark.org** : Belirtilen adres için http ve smtp harici paketleri yakalar.