

Trafik Dinleme, Sniffing

Bilgi Güvenliği AKADEMİSİ

Bölüm Amacı

- TCP/IP ağlarda “sniffing” ve paket analizi

Bölüm İçeriği

- Paket, protokol kavramları
- Temel kavramlar
- Sniffing
- Sniffing'e açık protokoller
- Sniffing çeşitleri
 - Aktif Sniff / Pasif Sniff
- Ortama göre sniffer yerleşimi
- Sniffing amaçlı kullanılan araçlar
- Network data carving

Paket Kavramı..

- İletişim == paket
- Ne işe yarar
 - Bilinmeyen Protokol Analizi
 - Ağ trafiği ölçümü
 - Anormal trafik gözleme
 - Firewall/IDS/IPS altyapısı..
- TCP, UDP Paketleri
- Protokoller
 - SMTP, FTP, P2P trafiği nasıl ayırt edilir

Temel Kavramlar

- Inline/Pasif Yerleşim
- Ethernet Çalışma modları
 - Unicast paketler
 - Multicast paketler
 - Broadcast paketler
 - Promiscuous Mode
- Snifferlar genelde Promiscuous modda çalışır.
- **# ifconfig eth0 –promisc**

Komutu arabirimi promisc modda çıkarır

Ethernet Kartlarında Filtreleme

- **Unicast**-> Kendi adresine gelen paketler
Broadcast -> Broadcast adresine gelen paketler
Multicast-> üye olunan multicast gruba ait paketler.
Promiscious -> Gelen paketin ne olduğuna bakmadan kabul edildiği durum.

L2 İletişim Ortamları

- HUB
- Switch
- Bridge



Sniffing ...

- Ağ trafiği dinleme
- Şifreli/şifresiz protokoller
- Sniffingde Amaç?
 - Good/Admins = “Protocol Analysis”
 - Bad/Hackers = “Sniffing The Wire”
 - Developers = “Is My Application Working



Google'dan

Sniffing'e Açık Protokoller

- Sniffing'e açık:İçerisinde taşıdığı veri okunabilir, şifrelenmemiş trafik
- Hemen hemen tüm protokoller
 - Telnet, Rlogin
 - HTTP/FTP
 - SMTP/POP/IMAP
- Güvensiz Protokollerin güvenli kullanımı
 - SSL Wrapper

Internette en sık kullanılan 10 port

TCP

1. 80
2. 23
3. 22
4. 443
5. 3389
6. 445
7. 139
8. 21
9. 135
10. 25

Şifreli=1
Şifresiz=9



SMTP Bağlantısı

Sniffer

The image displays a Wireshark packet capture interface. The top section shows a list of captured packets. The bottom section shows the details of the selected packet (Frame 1), which is an Ethernet II packet. The packet details show the source and destination MAC addresses and IP addresses. The packet is a TCP segment from 192.168.2.26 to 80.93.212.86, port 1302. The packet is a Telnet session to mail.lifeoverip.net. The Telnet session shows the user logging in as huzeyfe and sending a message. The message content is: "354 go ahead", "Subject: Egityine Gec Kalma", and "582 unimplemented (#5.5.1)".

No.	Time	Source	Destination	Protocol	Info
225	31.176307	80.93.212.86	192.168.2.26	TCP	smtp > 1302 [ACK] Seq=177 Ack=117 win=65535 Len=0
226	31.192354	192.168.2.26	80.93.212.86	SMTP	Message Body
227	31.300971	80.93.212.86	192.168.2.26	TCP	smtp > 1302 [ACK] Seq=177 Ack=118 win=65535 Len=0
228	31.573670	192.168.2.26	80.93.212.86	SMTP	Message Body
229	31.698158	80.93.212.86	192.168.2.26	TCP	smtp > 1302 [ACK] Seq=177 Ack=120 win=65535 Len=0
230	35.793040	192.168.2.26	80.93.212.86	SMTP	Message Body
231	35.905347	80.93.212.86	192.168.2.26	TCP	smtp > 1302 [ACK] Seq=177 Ack=121 win=65535 Len=0
232	38.997887	192.168.2.26	80.93.212.86	SMTP	Message Body
233	39.109223	80.93.212.86	192.168.2.26	TCP	smtp > 1302 [ACK] Seq=177 Ack=123 win=65535 Len=0
234	40.610490	192.168.2.26	80.93.212.86	SMTP	Message Body
235	40.719382	80.93.212.86	192.168.2.26	TCP	smtp > 1302 [ACK] Seq=177 Ack=125 win=65535 Len=0
236	42.131482	80.93.212.86	192.168.2.26	SMTP	Response: 250 ok 1227295115 qp 92294
237	42.296466	192.168.2.26	80.93.212.86	TCP	1302 > smtp [ACK] Seq=125 Ack=205 win=65531 [TCP CHECKSUM INCORRECT] Len=0
238	42.306863	80.93.212.86	192.168.2.26	SMTP	Response: 502 unimplemented (#5.5.1)
239	42.498610	192.168.2.26	80.93.212.86	TCP	1302 > smtp [ACK] Seq=125 Ack=233 win=65503 [TCP CHECKSUM INCORRECT] Len=0

Frame 1 (62 bytes on wire (62 bytes captured) on interface 0: Ethernet II, Src: 00:1f:d0:5a:1b:96 (00:1f:d0:5a:1b:96), Dst: Arcadyan_a7:22:5c (00:1a:2a:a7:22:5c)) Internet Protocol, Src: 192.168.2.26 (192.168.2.26), Dst: 80.93.212.86 (80.93.212.86) Transmission Control Protocol, Src Port: 1302 (1302), Dst Port: 25 (25), Seq: 125, Len: 0

Telnet mail.lifeoverip.net

```
220 mail.sistenbil.com ESMTP
ehlo huzeyfeninevi
250-mail.sistenbil.com
250-AUTH LOGIN CRAM-MD5 PLAIN
250-AUTH=LOGIN CRAM-MD5 PLAIN
250-PIPELINING
250 8BITMIME
mail from:huzeyfe
250 ok
rcpt to: huzeyfe@lifeoverip.net
250 ok
Data
354 go ahead
Subject: Egityine Gec Kalma
.
250 ok 1227295115 qp 92294
582 unimplemented (#5.5.1)
```

SMTP
Bağlantısı

SMTP Bağlantısı Detaylar

The image displays a Wireshark packet capture of an SMTP connection. The main window shows the 'Follow TCP Stream' view for the connection between mail.sistembil.com and mail.lifeoverip.net. The stream content shows the SMTP conversation, including the EHLO command, authentication (AUTH LOGIN CRAM-MD5 PLAIN), and the MAIL FROM command. A red arrow points to the 'Subject: Egityime Gec Kalma' line in the stream content. A callout box labeled 'Wireshark "FollowTCPStream" Ozelligi' points to the 'Follow TCP Stream' button in the toolbar. Below the main window, a Telnet session window shows the same SMTP conversation, with a red arrow pointing to the 'Subject: Egityime Gec Kalma' line. A blue speech bubble in the bottom right corner contains the text '#mailsnarf -i r10'.

Wireshark "FollowTCPStream" Ozelligi

#mailsnarf -i r10

Telnet Bağlantısı

The image displays a Wireshark packet capture of a Telnet session. The filter is set to `(ip.addr eq 80.93.212.86 and ip.addr eq 192.168.2.26)`. The packet list shows several Telnet data packets. The packet details pane shows the selected packet (No. 97) with the following structure:

- Frame 97 (60 bytes on wire)
- Ethernet II, Src: Arcadya
- Internet Protocol, Src: 80.93.212.86, Dst: 192.168.2.26
- Transmission Control Protocol, Seq: 154, Ack: 107, Win: 65535, Len: 0
- Telnet Data

The packet bytes pane shows the raw data of the selected packet, which is a Telnet login attempt. The data is displayed in ASCII, EBCDIC, and Hex formats. The ASCII view shows the following text:

```
FreeBSD/i386 (mail.sistembil.com) (ttty1)
login: ..oolmmaayyaann kkuu1111aannicci
Password:Buda parolası
Login incorrect
login:
```

The packet bytes pane also shows the raw data in Hex and EBCDIC formats. The packet bytes pane also shows the raw data in Hex and EBCDIC formats.

The packet bytes pane also shows the raw data in Hex and EBCDIC formats.

FTP Bağlantısı

Device: \Device\NPF_{D24EC5B3-18B8-43C9-959C-3095000CB9F5}: Capturing - Wireshark

Filter: (ip.addr eq 192.168.2.26 and ip.addr eq 193.14) Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.26	193.140.100.100	TCP	ms-sna-server > ftp [SYN] Seq=0 Len=0 MSS=1460
2	0.028126	193.140.100.100	192.168.2.26	TCP	ftp > ms-sna-server [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452
3	0.028165	192.168.2.26	193.140.100.100	TCP	ms-sna-server > ftp [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0
4	0.060320	193.140.100.100	192.168.2.26	FTP	response: 220 ftp.linux.org.tr
5	0.243612	192.168.2.26	193.140.100.100	TCP	ms-sna-server > ftp [ACK] Seq=1 Ack=23 Win=65513 [TCP CHECKSUM INCORRECT] Len=0
6	3.279189	192.168.2.26	193.140.100.100	FTP	Request: USER ftp
7	3.299648	193.140.100.100	192.168.2.26	FTP	Response: 331 Please specify the password.
8	3.462567	192.168.2.26	193.140.100.100	TCP	ms-sna-server > ftp [ACK] Seq=11 Ack=57 Win=65479 [TCP CHECKSUM INCORRECT] Len=0
9	10.068979	192.168.2.26	193.140.100.100	FTP	Request: PASS parolam_YOK
10	10.096160	193.140.100.100	192.168.2.26	FTP	Response: 230 Login successful.
11	10.203241				
12	13.284112				
13	13.307411				
14	13.308468				
15	13.355899				

Stream Content

220 ftp.linux.org.tr
USER ftp
331 Please specify the password.
PASS parolam_YOK
230 Login successful.
PORT 192,168,2,26,5,199
200 PORT command successful. Consider using PASV.
NLST
150 Here comes the directory listing.
226 Directory send OK.

Find Save As Print Entire conversation (252 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

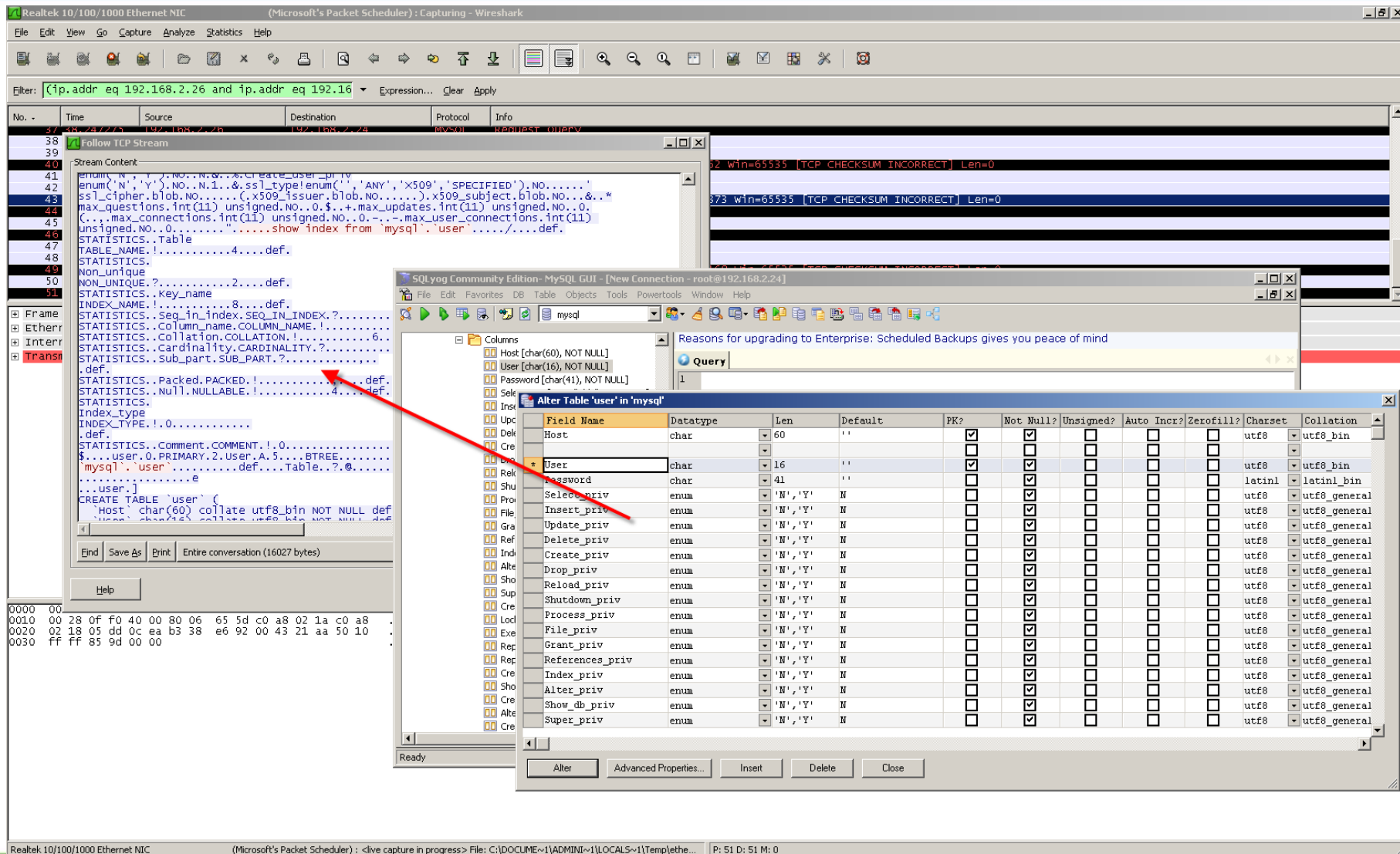
Help Close Filter Out This Stream

```
C:\WINDOWS\system32\cmd.exe - ftp ftp.linux.org.tr

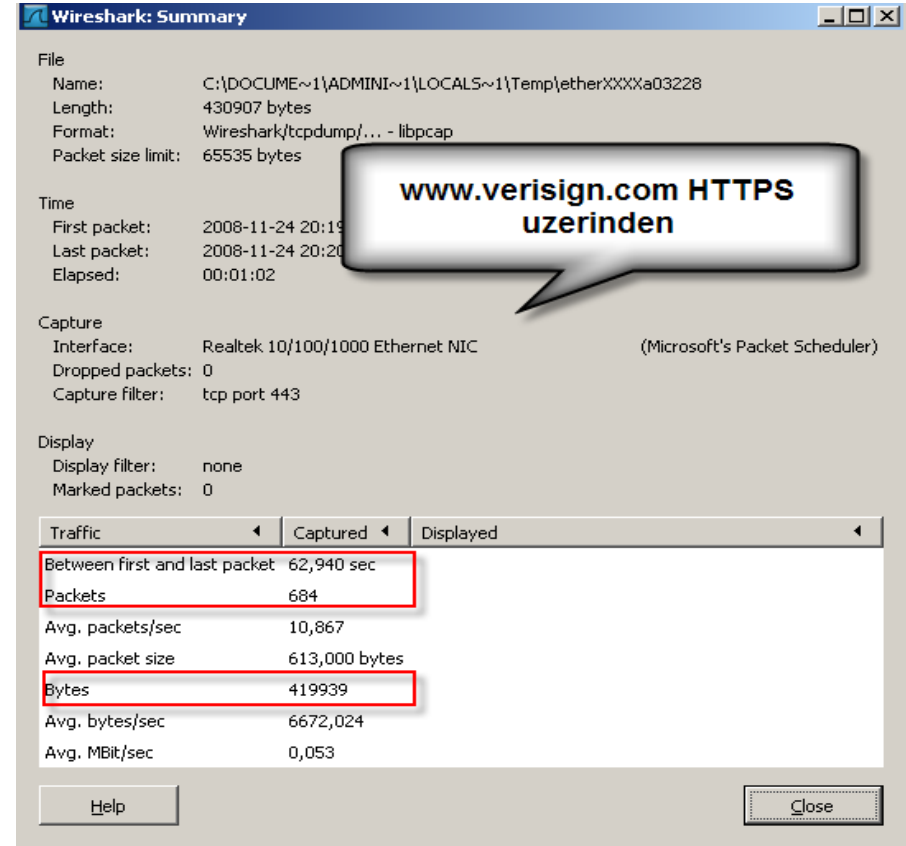
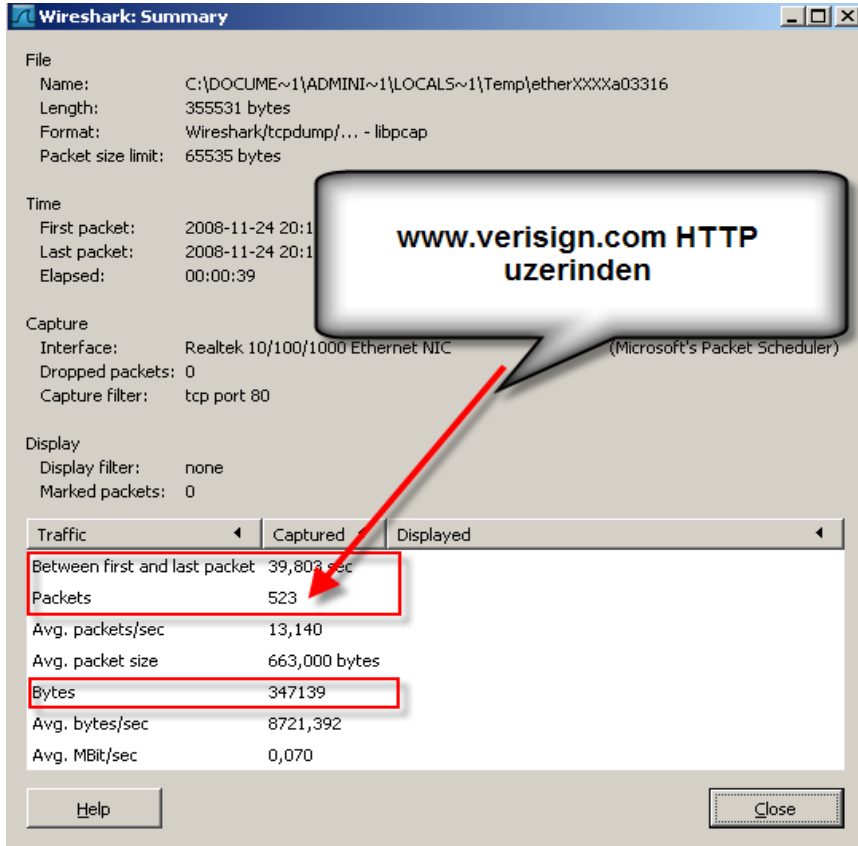
Connection to host lost.

C:\Documents and Settings\Administrator>ftp ftp.linux.org.tr
Connected to ftp.linux.org.tr.
220 ftp.linux.org.tr
User (ftp.linux.org.tr:(none)): ftp
331 Please specify the password.
Password:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
debian
debian-cd
pub
releases
ubuntu
226 Directory send OK.
ftp: 42 bytes received in 0.00Seconds 42000 kbytes/sec.
ftp> -
```

SQL Bağlantısı



Şifrelemenin Dezavantajı



Sniffing Çeşitleri

- Pasif Sniffing
 - Hedef sistemle iletişime geçilmez!
 - Sniffing'e dair iz bulunamaz
 - HUB kullanılan ortamlarda
- Aktif Sniffing
 - Hedef sistemle iletişime geçilir
 - Arkasında iz bırakır
 - Switch kullanılan Ağlarda yaygındır

Pasif Sniffing

- HUB/TAP kullanılan ortamlarda işe yarar
- Ortama dahil olan her sistem dolaşan tüm paketleri alır
- Promiscuous modda olanlar paketleri kabul eder/kaydeder.
- Sık Kullanılan Araçlar:
 - Tcpdump, Wireshark, Snort, Dsniff, Tshark

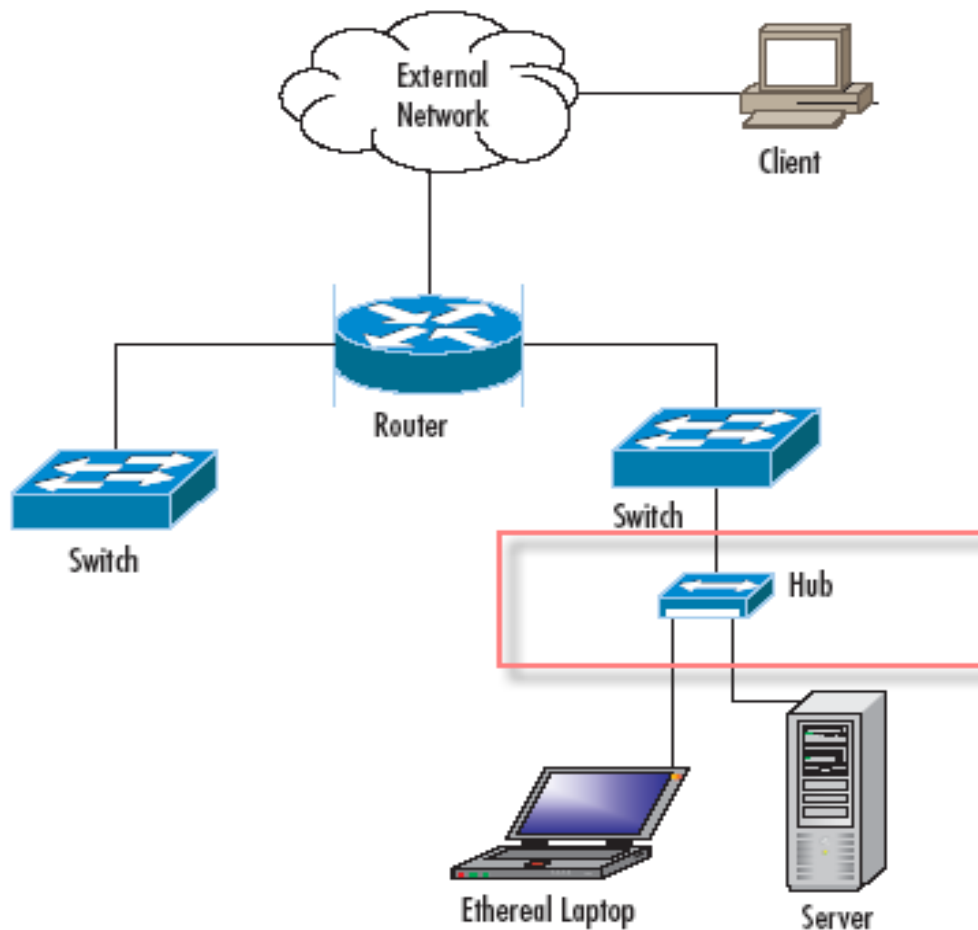
Aktif Sniffing

- Amaç: trafiği dinlenecek sistemin paketlerini üzerinden geçirme ya da kopyasını almak.
- Switch / HUB Farkını hatırlayalım
- Yöntemleri
 - MAC Flooding
 - ARP Spoofing/Poisoning
 - Icmp redirect
- Aktif Sniffing Araçları
 - Arpspoof(Dsniff)
 - Ettercap
 - Cain&Abel
 - Macof
- Kolay Yakalanabilir(?)

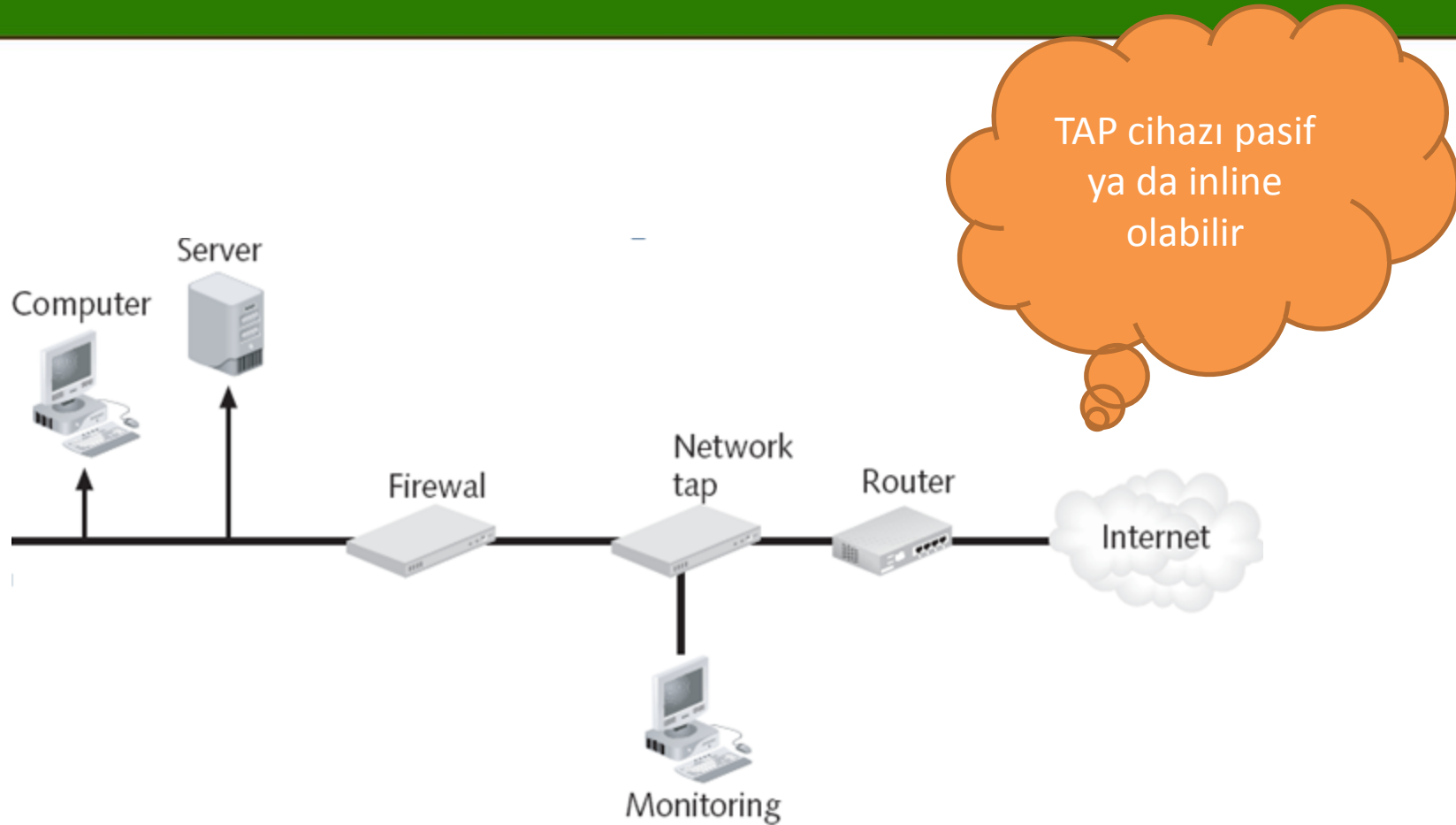
Sniffer Yerleşimi

- Ağ ortamının özelliğine göre Snifferlerin yerleşimi değişmektedir.
- TAP kullanılan ortamlarda
- HUB'lı ortamlarda
- Switch kullanılan ağlarda(Port mirroring)

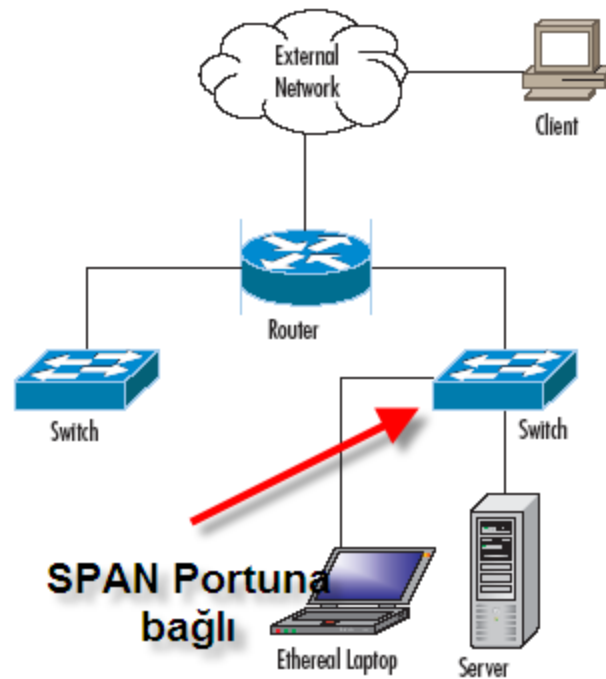
Sniffing için HUB Kullanımı



Sniffing için TAP Kullanımı

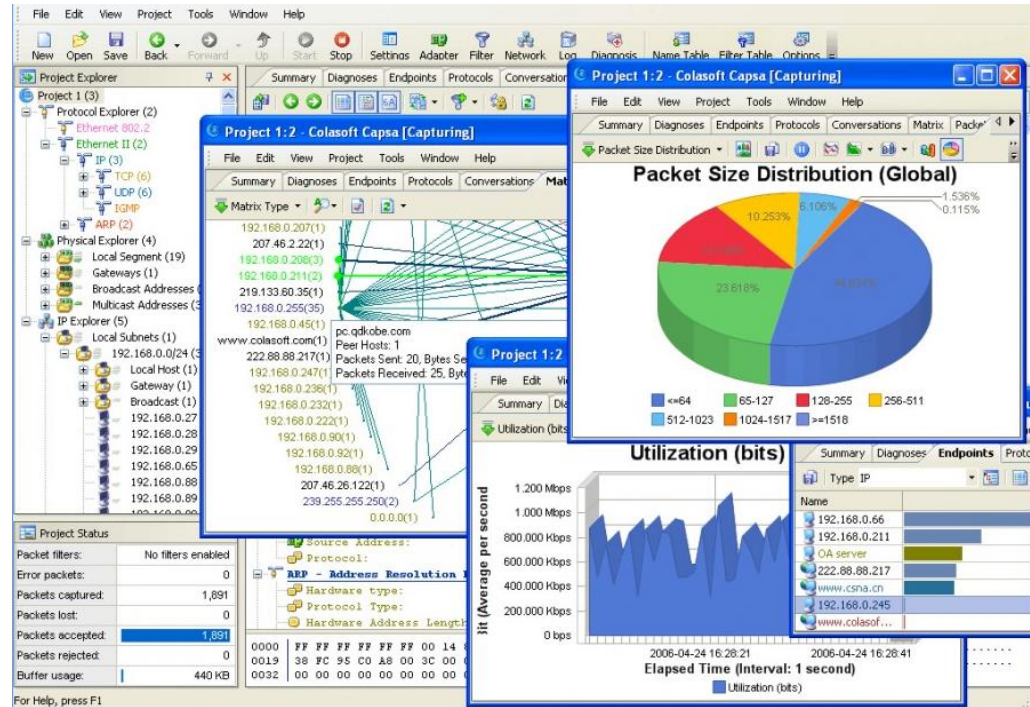


Sniffing için SPAN Port Kullanımı



Sniffing Amaçlı Araçlar

- Tcpdump
- Snoop
- Tshark
- Wireshark
- Eeye IRIS
- Dsniff
- Snort



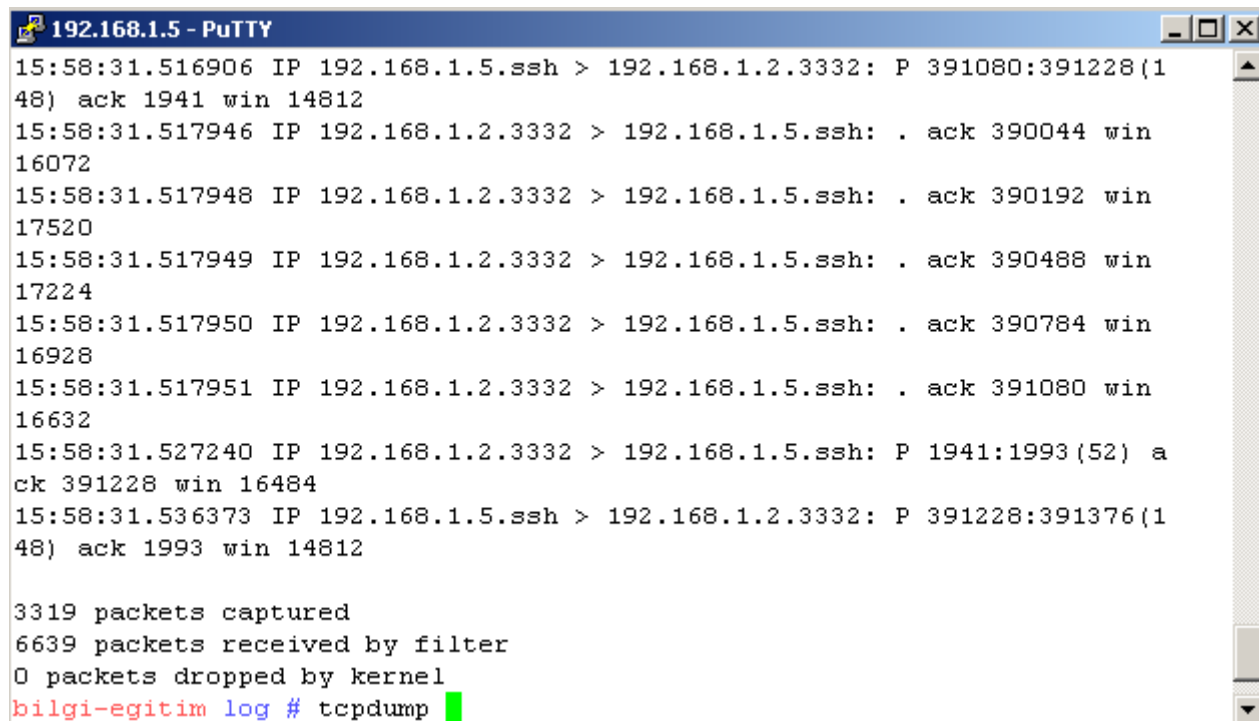
Sniffer olarak Tcpdump

- UNIX Tabanlı popüler sniffer yazılımı
 - Windows için windump
- Libpcap tarafından alınan ham veriler tcpdump tarafından işlenerek okunabilir hale gelir.
- Tamamen ücretsiz bir yazılım.
- Sorun giderme , trafik analizi, hacking amaçlı kullanılabilir.

Temel Kullanımı

- Tcpdump komut satırından çalışan bir araç olduğu için parametreler oldukça önemlidir.
- Uygun parametreler ve filtreler kullanılırsa yoğun trafikte bile istenilen amaca kolaylıkla ulaşılabilir.

Parametresiz kullanım örneği



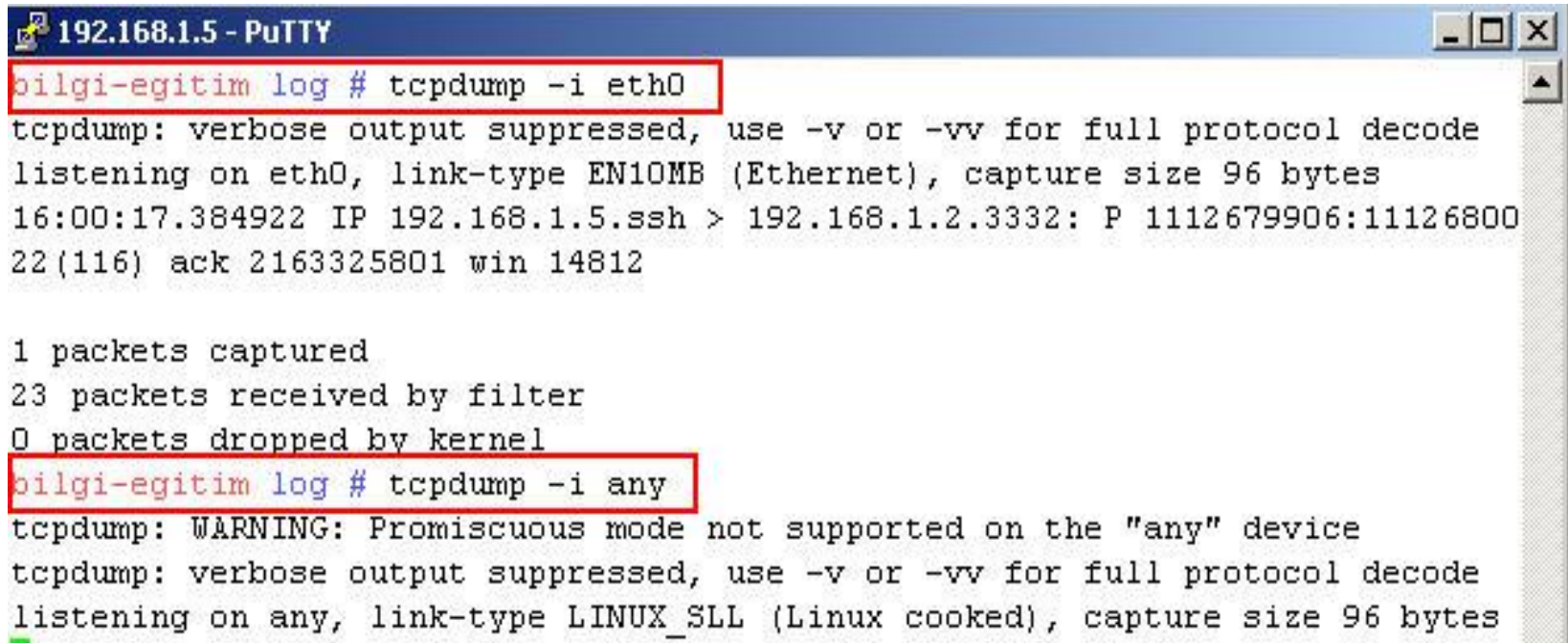
```
192.168.1.5 - PuTTY
15:58:31.516906 IP 192.168.1.5.ssh > 192.168.1.2.3332: P 391080:391228(148) ack 1941 win 14812
15:58:31.517946 IP 192.168.1.2.3332 > 192.168.1.5.ssh: . ack 390044 win 16072
15:58:31.517948 IP 192.168.1.2.3332 > 192.168.1.5.ssh: . ack 390192 win 17520
15:58:31.517949 IP 192.168.1.2.3332 > 192.168.1.5.ssh: . ack 390488 win 17224
15:58:31.517950 IP 192.168.1.2.3332 > 192.168.1.5.ssh: . ack 390784 win 16928
15:58:31.517951 IP 192.168.1.2.3332 > 192.168.1.5.ssh: . ack 391080 win 16632
15:58:31.527240 IP 192.168.1.2.3332 > 192.168.1.5.ssh: P 1941:1993(52) ack 391228 win 16484
15:58:31.536373 IP 192.168.1.5.ssh > 192.168.1.2.3332: P 391228:391376(148) ack 1993 win 14812

3319 packets captured
6639 packets received by filter
0 packets dropped by kernel
bilgi-egitim log # tcpdump
```

Tcpdump analizi

Değer	Açıklaması
16:21:24.174180	Zaman Damgası
192.168.60.3	Kaynak IP Adresi
34720	Kaynak Port numarası
>	Yön Belirteci
10.10.10.3	Hedef IP Adresi
3389	Hedef Port Numarası
S	TCP Bayrağı (SYN Bayrağı set edilmiş)
2354677536	TCP başlangıç seri numarası (ISN)
2354677536	Bir sonraki byte için beklenen sıra numarası
(0)	Bu segmentin içerdiği uygulama verisi hesabı
win 5840	Byte cinsinden Window size.
mss 1460	Maximum Segment Size (MSS)
sackOK	Selective acknowledgement
(DF)	Paketin DF(Parçalanmaması) özelliğinde olduğunu
.	

Arabirim seçimi



```
192.168.1.5 - PuTTY
bilgi-egitim log # tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
16:00:17.384922 IP 192.168.1.5.ssh > 192.168.1.2.3332: P 1112679906:11126800
22(116) ack 2163325801 win 14812

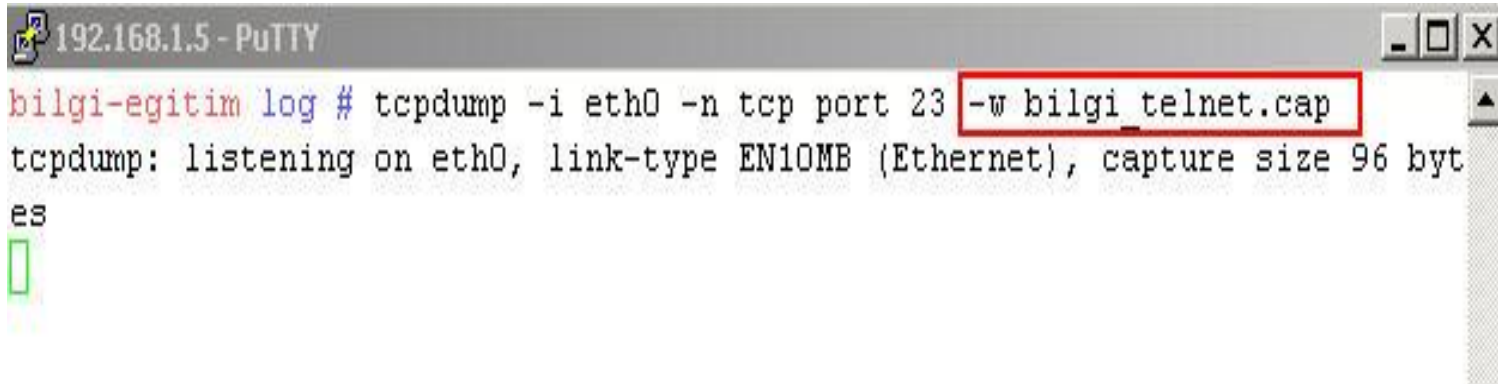
1 packets captured
23 packets received by filter
0 packets dropped by kernel
bilgi-egitim log # tcpdump -i any
tcpdump: WARNING: Promiscuous mode not supported on the "any" device
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
```

İsim çözümleme

```
# tcpdump
17:18:21.531930 IP huzeyfe.32829 > erhan.telnet: S 3115955894:3115955894(0)
win 5840
17:18:21.531980 IP erhan.telnet > huzeyfe.32829: R 0:0(0) ack 3115955895 win 0
-n parametresi ile kullanım;
# tcpdump -n
17:18:53.802776 IP 192.168.0.100.32835 > 192.168.0.1.telnet: S
3148097396:3148097396(0) win 5840
17:18:53.802870 IP 192.168.0.1.telnet > 192.168.0.100.32835: R 0:0(0) ack
3148097397 win 0
```

Yakalanan paketleri kaydetme

- Tcpdump'ın yakaladığı paketleri sonradan incelemek üzere dosyaya yazılabilir.
- Dosya formatı libpcap uyumludur.
- -w parametresi kullanılır.



The screenshot shows a PuTTY terminal window titled "192.168.1.5 - PuTTY". The prompt is "bilgi-egitim log #". The command entered is "tcpdump -i eth0 -n tcp port 23 -w bilgi_telnet.cap". The output of the command is "tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes". The cursor is on a new line, and a green box is visible at the bottom left of the terminal window.

```
192.168.1.5 - PuTTY
bilgi-egitim log # tcpdump -i eth0 -n tcp port 23 -w bilgi_telnet.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
es
█
```

Kaydedilmiş Paketleri Okuma

- -w ile kaydettığımız paketleri okumak içinde -r parametresini kullanılır.

```
# cd /tmp/  
# tcpdump -w log icmp  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes  
ctrl c  
  
# tcpdump -r log -nn  
reading from file log, link-type EN10MB (Ethernet)  
17:31:01.225007 IP 192.168.0.100 > 192.168.0.1: icmp 64: echo request seq 0  
17:31:01.225119 IP 192.168.0.1 > 192.168.0.100: icmp 64: echo reply seq 0  
17:31:02.224988 IP 192.168.0.100 > 192.168.0.1: icmp 64: echo request seq 1  
17:31:02.225111 IP 192.168.0.1 > 192.168.0.100: icmp 64: echo reply seq 1
```

Filtrelerle Çalışmak

- **host Parametresi**

- Sadece belli bir host a ait paketlerin izlenmesini istiyorsak host parametresi ile belirtim yapabiliriz.
- dst host (Hedef Host Belirtimi)
- src host (Kaynak Host Belirtimi)
- # tcpdump src host 10.1.0.59 and dst host 10.1.0.1

Filtrelerle Çalışmak

- **Port parametresi**

- belirli bir portu dinlemek istediğimizde kullanacağımız parametredir. Host gibi src ve dst öneklerini alabilir.
- src ile kaynak portu dst ile hedef portu belirtebiliriz .
dst ya da src önekini kullanmazsak hem kaynak hemde hedef portu alır.
- **# tcpdump src port 23 and dst port 9876**

Sniffer Olarak Snort

```
192.168.1.5 - PuTTY
bilgi-egitim ~ # snort -v -i eth0
Running in packet dump mode

==== Initializing Snort ====
Initializing Output Plugins!
Var 'any_ADDRESS' defined, value len = 15 chars, value = 0.0.0.0/0.0.0.0
Var 'lo_ADDRESS' defined, value len = 19 chars, value = 127.0.0.0/255.0.0.0
Verifying Preprocessor Configurations!

Initializing Network Interface eth0
Decoding Ethernet on interface eth0

==== Initialization Complete ====

/*_      -*> Snort! <*-
o"  )~   Version 2.6.1.2 (Build 34)
"      By Martin Roesch & The Snort Team: http://www.snort.org/team.html
      (C) Copyright 1998-2006 Sourcefire Inc., et al.

Not Using PCAP_FRAMES
12/14-09:43:26.916015 192.168.1.5:22 -> 192.168.1.2:2446
TCP TTL:64 TOS:0x10 ID:34434 IpLen:20 DgmLen:124 DF
***AP*** Seq: 0x8178B852 Ack: 0xB83E81F8 Win: 0x2180 TcpLen: 20
+++++
12/14-09:43:26.925202 192.168.1.5:22 -> 192.168.1.2:2446
TCP TTL:64 TOS:0x10 ID:34435 IpLen:20 DgmLen:124 DF
***AP*** Seq: 0x8178B8A6 Ack: 0xB83E81F8 Win: 0x2180 TcpLen: 20
+++++
12/14-09:43:26.925598 192.168.1.2:2446 -> 192.168.1.5:22
```

Sniffer Olarak Snoop

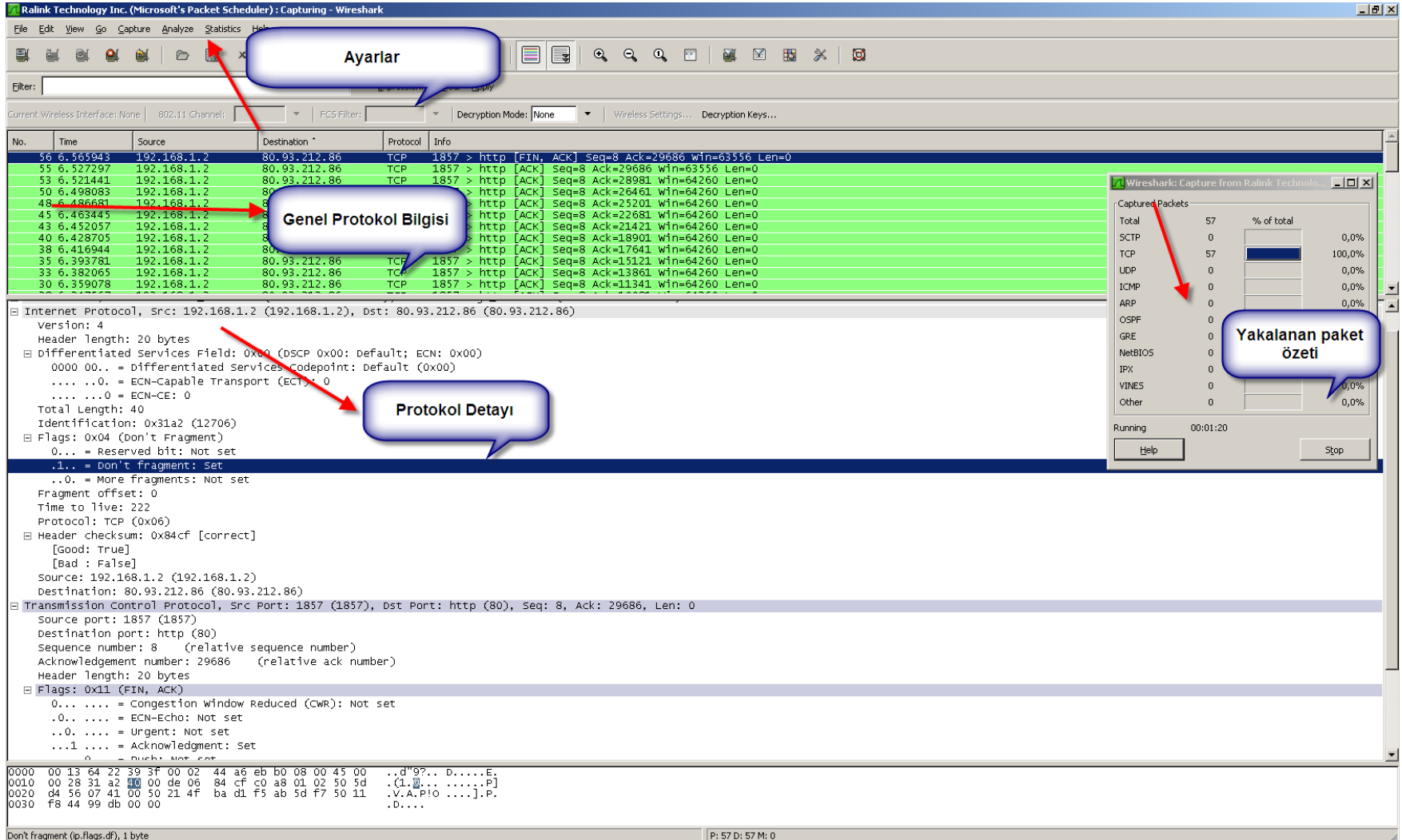
- Solaris sistemler için sniffer programı
- Tcpdump benzeri kullanıma sahiptir.

```
mailhost -> 82.83.105.207 SMTP R port=3706
mailhost -> 159.140.254.90 SMTP R port=1261
159.140.254.90 -> mailhost SMTP C port=1261
mailhost -> lsmtph87.yournewsletters.net SMTP R port=3300 421-5.7.1 your IP
or
lsmtph87.yournewsletters.net -> mailhost SMTP C port=3300
217.154.219.171 -> mailhost SMTP C port=3824
mailhost -> 217.154.219.171 SMTP R port=3824
217.154.219.171 -> mailhost SMTP C port=3824
mailhost -> tiger.inboxcircular12.com SMTP R port=56825 421-5.7.1 your IP c
```

Sniffer Olarak Wireshark

- Eski adı Ethereal
- Açık kaynak kodlu Sniffer aracı
- Grafik arabirimli/ komut satırı
- Bilinen çoğu işletim sistemlerinde çalışır
- Bilinen tüm protokolleri destekler
- Yakalanan paketleri kaydedebilme
- Kaydedilmiş paketleri diskten okuma
- Protokol renklendirme

Wireshark Ekranı



The screenshot shows the Wireshark interface with several callouts pointing to specific features:

- Ayarlar**: Points to the 'Settings' icon in the top toolbar.
- Genel Protokol Bilgisi**: Points to the 'General Protocol Information' section in the packet list.
- Protokol Detayı**: Points to the 'Protocol Details' pane showing the structure of the captured packet.
- Yakalanan paket özeti**: Points to the 'Captured Packets' summary window on the right, which shows a bar chart of packet counts by protocol.

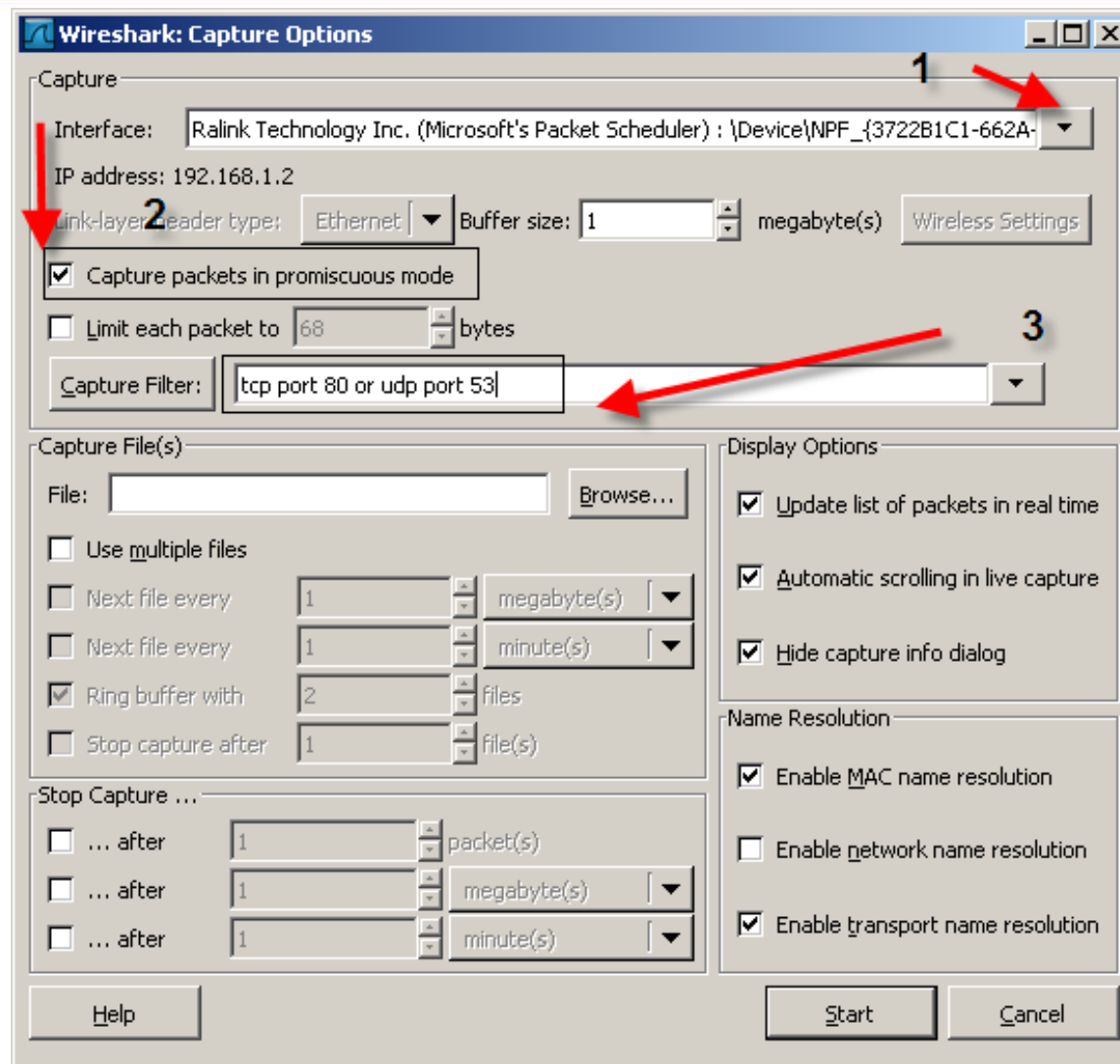
The main packet list shows a series of HTTP packets from 192.168.1.2 to 80.93.212.86. The selected packet is a FIN, ACK packet with sequence number 8 and acknowledgment number 29686.

The 'Protocol Details' pane shows the following structure:

- Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 80.93.212.86 (80.93.212.86)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - 0000 00.. = Differentiated Services Codepoint: Default (0x00)
 -0. = ECN-Capable Transport (ECT): 0
 -0. = ECN-CE: 0
 - Total Length: 40
 - Identification: 0x31a2 (12706)
 - Flags: 0x04 (Don't Fragment)
 - 0... = Reserved bit: Not set
 - .1.. = Don't Fragment: Set
 - ..0. = More Fragments: Not set
 - Fragment offset: 0
 - Time to live: 222
 - Protocol: TCP (0x06)
 - Header checksum: 0x84cf [correct]
 - [Good: True]
 - [Bad: False]
 - Source: 192.168.1.2 (192.168.1.2)
 - Destination: 80.93.212.86 (80.93.212.86)
- Transmission Control Protocol, Src Port: 1857 (1857), Dst Port: http (80), Seq: 8, Ack: 29686, Len: 0
 - Source port: 1857 (1857)
 - Destination port: http (80)
 - Sequence number: 8 (relative sequence number)
 - Acknowledgement number: 29686 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x11 (FIN, ACK)
 - 0... = Congestion window reduced (CWR): Not set
 - .0.. = ECN-Echo: Not set
 - ..0. = Urgent: Not set
 - ...1 = Acknowledgment: Set
 - = Push: Not set

The packet bytes pane shows the raw data of the packet, including the IP header, TCP header, and the FIN/ACK flag.

Paket Yakalama Seçenekleri

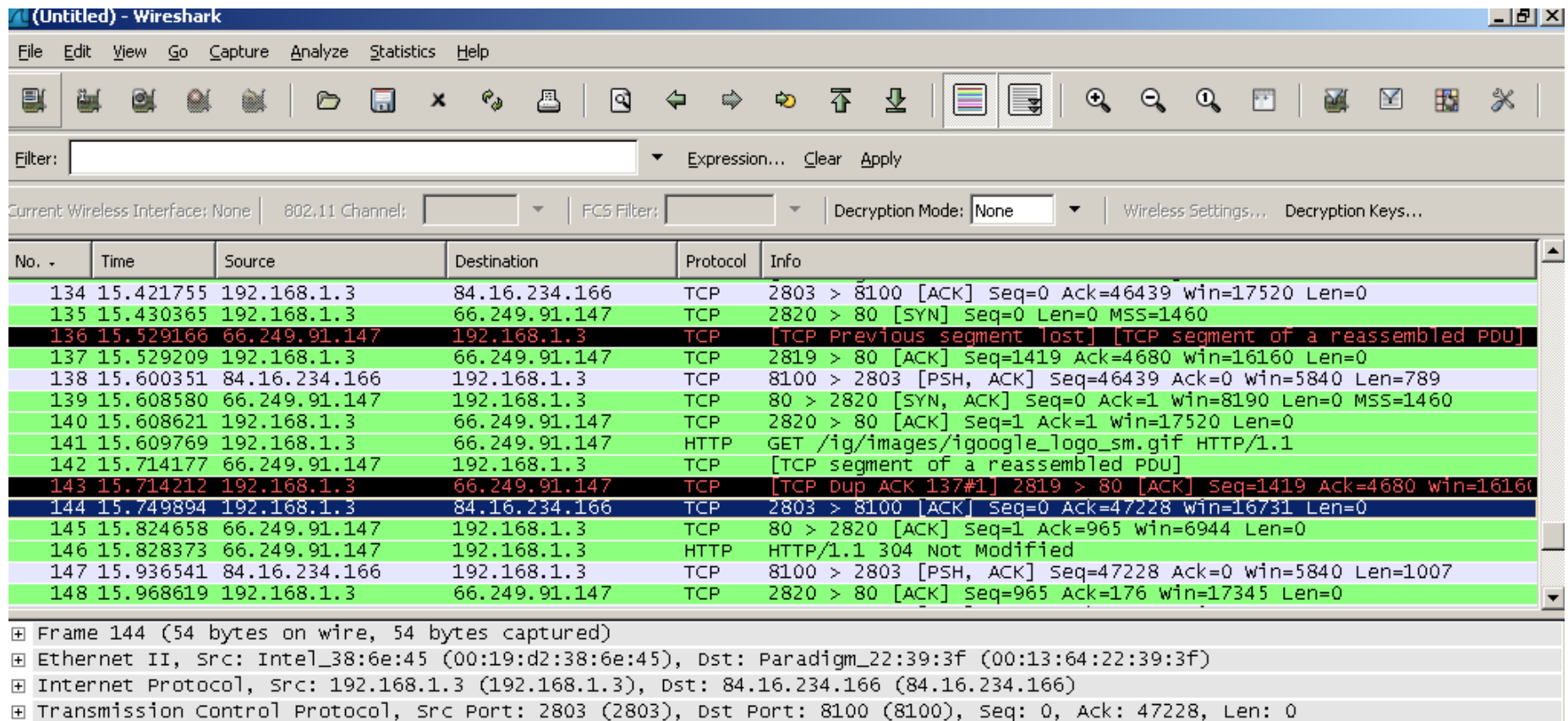


Yakalanan Paketler İçin İsim Çözme

Name Resolution

- ☒ Enable MAC name resolution
- ☐ Enable network name resolution
- ☒ Enable transport name resolution

Wireshark'da Filtresiz Yaşam



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

Current Wireless Interface: None 802.11 Channel: FCS Filter: Decryption Mode: None Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	Protocol	Info
134	15.421755	192.168.1.3	84.16.234.166	TCP	2803 > 8100 [ACK] Seq=0 Ack=46439 win=17520 Len=0
135	15.430365	192.168.1.3	66.249.91.147	TCP	2820 > 80 [SYN] Seq=0 Len=0 MSS=1460
136	15.529166	66.249.91.147	192.168.1.3	TCP	[TCP Previous segment lost] [TCP segment of a reassembled PDU]
137	15.529209	192.168.1.3	66.249.91.147	TCP	2819 > 80 [ACK] Seq=1419 Ack=4680 win=16160 Len=0
138	15.600351	84.16.234.166	192.168.1.3	TCP	8100 > 2803 [PSH, ACK] Seq=46439 Ack=0 win=5840 Len=789
139	15.608580	66.249.91.147	192.168.1.3	TCP	80 > 2820 [SYN, ACK] Seq=0 Ack=1 win=8190 Len=0 MSS=1460
140	15.608621	192.168.1.3	66.249.91.147	TCP	2820 > 80 [ACK] Seq=1 Ack=1 win=17520 Len=0
141	15.609769	192.168.1.3	66.249.91.147	HTTP	GET /ig/images/igoogle_logo_sm.gif HTTP/1.1
142	15.714177	66.249.91.147	192.168.1.3	TCP	[TCP segment of a reassembled PDU]
143	15.714212	192.168.1.3	66.249.91.147	TCP	[TCP Dup ACK 137#1] 2819 > 80 [ACK] Seq=1419 Ack=4680 win=16160
144	15.749894	192.168.1.3	84.16.234.166	TCP	2803 > 8100 [ACK] Seq=0 Ack=47228 win=16731 Len=0
145	15.824658	66.249.91.147	192.168.1.3	TCP	80 > 2820 [ACK] Seq=1 Ack=965 win=6944 Len=0
146	15.828373	66.249.91.147	192.168.1.3	HTTP	HTTP/1.1 304 Not Modified
147	15.936541	84.16.234.166	192.168.1.3	TCP	8100 > 2803 [PSH, ACK] Seq=47228 Ack=0 win=5840 Len=1007
148	15.968619	192.168.1.3	66.249.91.147	TCP	2820 > 80 [ACK] Seq=965 Ack=176 win=17345 Len=0

Frame 144 (54 bytes on wire, 54 bytes captured)

Ethernet II, Src: Intel_38:6e:45 (00:19:d2:38:6e:45), Dst: Paradigm_22:39:3f (00:13:64:22:39:3f)

Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 84.16.234.166 (84.16.234.166)

Transmission Control Protocol, Src Port: 2803 (2803), Dst Port: 8100 (8100), Seq: 0, Ack: 47228, Len: 0

Filtreler

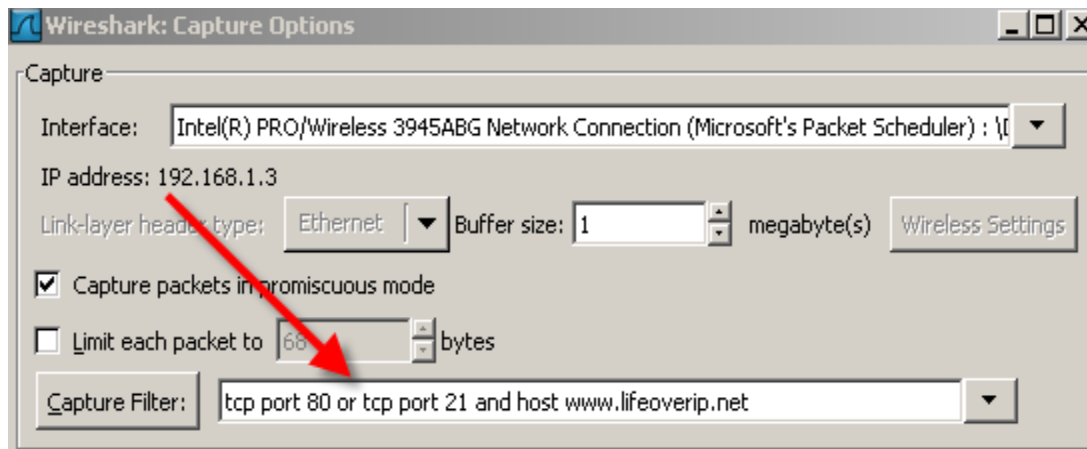
CAPTURE FILTER

- Yakalanacak paketlere uygulanır.
- Tcpdump formatı ile aynıdır.
- Tcp port 22 and host vpn.lifeoverip.net or icmp

DISPLAY FILTER

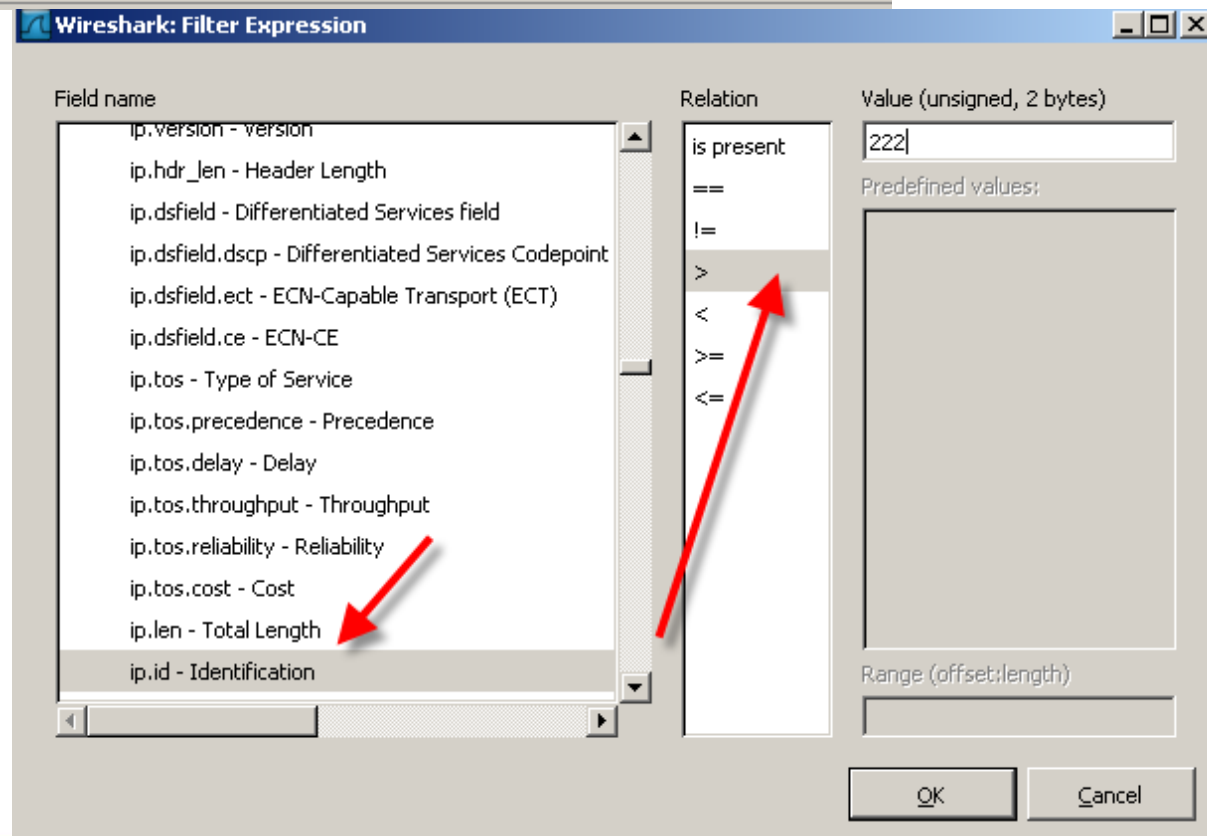
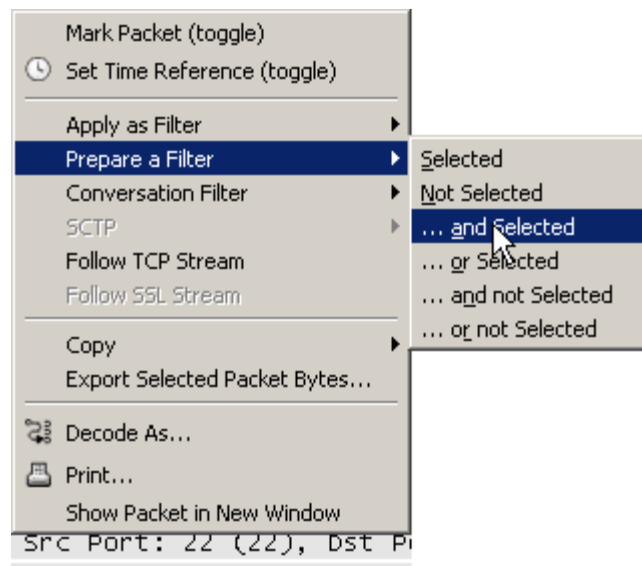
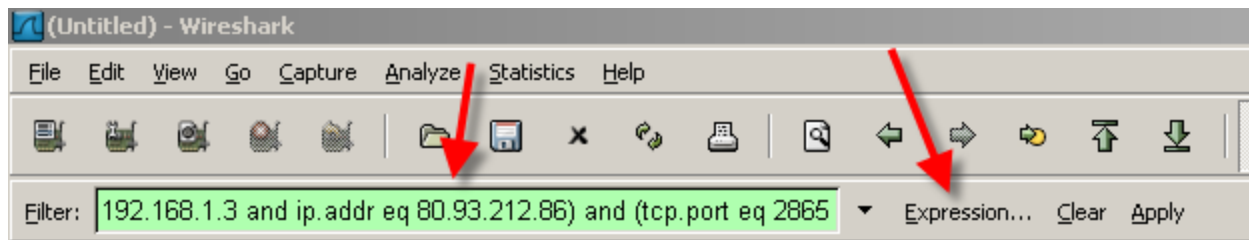
- Yakalanan paketler üzerinde analiz yapılırken kullanılır.
- Farklı bir formata sahiptir.
- (Tcp.port eq 22) and (ip.addr eq blabla...)
- Arabirimden filtre yazılabilir

Capture Filter



- **Tcp port 21**
- **Tcp port 21 and tcp port 1982**
- **Tcp port 22 and host vpn.lifeoverip.net or icmp**

Display Filter



TCP Oturumlarında Paket Birleştirme

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

Current Wireless Interface: None 802.11 Channel: FCS Filter: Decryption

No.	Time	Source	Destination	Protocol	Info
37	6.416875	80.93.212.86	192.168.1.2	HTTP	Continuation
36	6.405253	80.93.212.86	192.168.1.2	HTTP	Continuation
34	6.393730	80.93.212.86	192.168.1.2	HTTP	Continuation
32	6.382003	80.93.212.86	192.168.1.2	HTTP	Continuation
31	6.370743	80.93.212.86	192.168.1.2	HTTP	Continuation
29	6.359004	80.93.212.86	192.168.1.2	HTTP	Continuation
27	6.347501	80.93.212.86	192.168.1.2	HTTP	Continuation
26	6.335748	80.93.212.86	192.168.1.2	HTTP	Continuation
24	6.324002	80.93.212.86	192.168.1.2	HTTP	Continuation
22	6.312607	80.93.212.86	192.168.1.2	HTTP	Continuation
21	6.302372	80.93.212.86	192.168.1.2	HTTP	Continuation
19	6.290017	80.93.212.86	192.168.1.2	HTTP	Continuation
17	6.263374	80.93.212.86	192.168.1.2	HTTP	Continuation
16	6.250251	80.93.212.86	192.168.1.2	HTTP	Continuation
15	6.205459	80.93.212.86	192.168.1.2	HTTP	Continuation
13	3.960333	80.93.212.86	192.168.1.2	HTTP	Continuation
11	3.469833	80.93.212.86	192.168.1.2	HTTP	Continuation
9	3.337462	80.93.212.86	192.168.1.2	HTTP	Continuation
7	3.124206	80.93.212.86	192.168.1.2	HTTP	Continuation
5	2.878957	80.93.212.86	192.168.1.2	HTTP	Continuation

Internet Protocol, Src: 80.93.212.86 (80.93.212.86), Dst: 192.168.1.2 (192.168.1.2)

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Mark Packet (toggle)
Set Time Reference (toggle)
Apply as Filter
Prepare a Filter
Conversation Filter
SCTP
Follow TCP Stream
Follow SSL Stream
Decode As...
Print...
Show Packet in New Window

Follow TCP Stream

Stream Content

```
<!--include sidebar-->
<div id="r_sidebar">
<!--sidebar.php-->

<!--archives ordered per month-->
<h2>Archives</h2>
<ul>
<li><a href="http://blog.lifeoverip.net/index.php/2007/06/" title="June 2007">June 2007</a></li>
<li><a href="http://blog.lifeoverip.net/index.php/2007/05/" title="May 2007">May 2007</a></li>
<li><a href="http://blog.lifeoverip.net/index.php/2007/04/" title="April 2007">April 2007</a></li>
</ul>

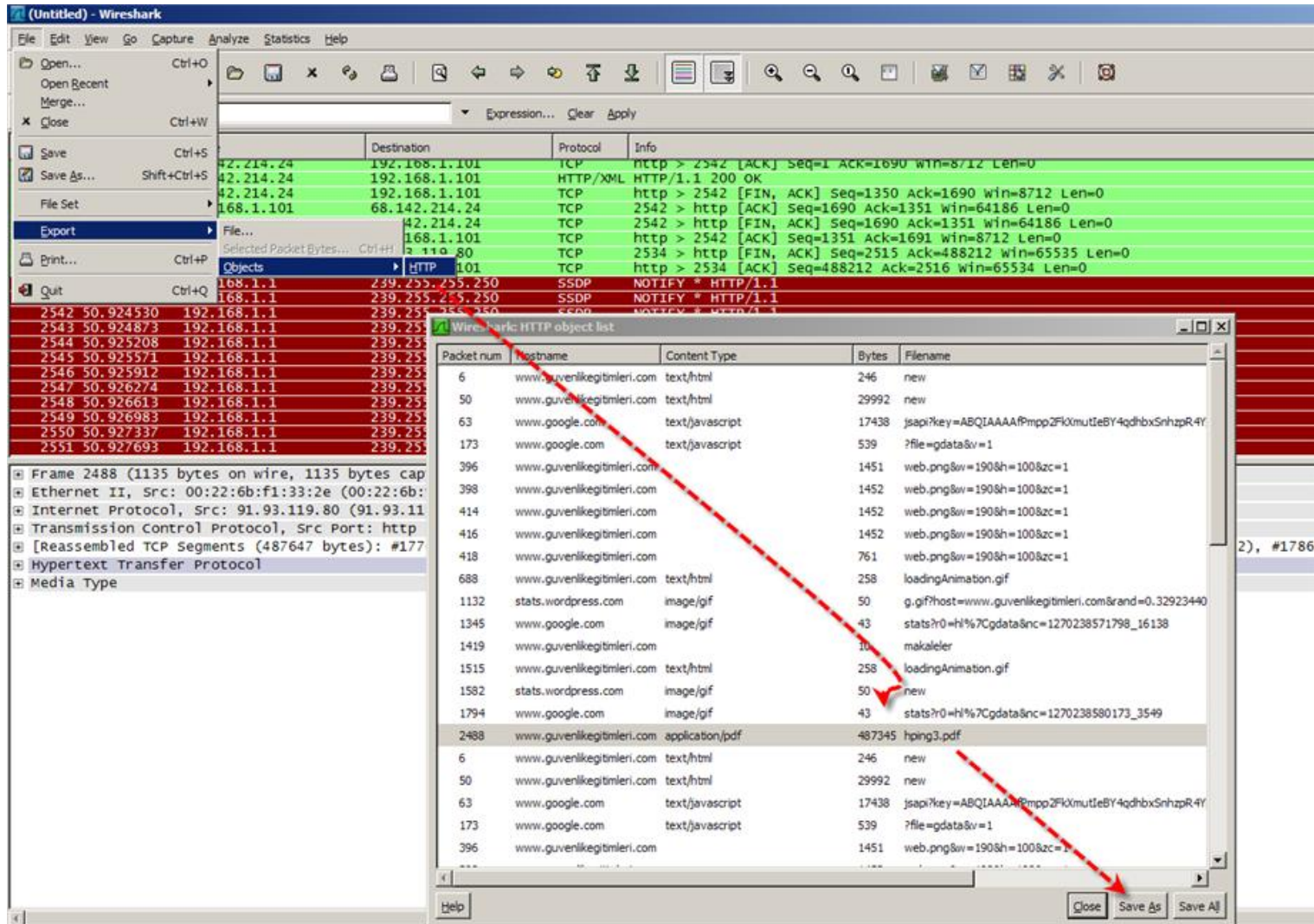
<!--links or blogroll-->
<h2>Friends</h2>
<ul>
<li><a href="http://adnan.lifeoverip.net">Adnan SANCAR</a></li>
<li><a href="http://www.alginerozan.com">Alginerozan</a></li>
<li><a href="http://www.burakdayiglu.net">Burak DAYIGLU</a></li>
<li><a href="http://agguvenligi.blogspot.com">Enis KARARSLAN</a></li>
<li><a href="http://ferruh.mavituna.com">Ferruh MAV. TUNA</a></li>
</ul>

<!--delete my network and put your own here-->
<h2>Life(Cover)IP Network</h2>
<ul>
<li><a href="http://seclists.com">Güvenlik listeleri</a></li>
<li><a href="http://netsec.huzeyfe.net">Netsec listesi</a></li>
</ul>
</div>
```

End Save As Print Entire conversation (29691 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Close Filter Out This Stream

Wireshark Data Carving



Tshark

- Wireshark komut satırı aracı
- Tcpdump benzeri parametrelerle çalışır
- Tcpdump'dan en önemli farkı protokol detaylarını gösterebilmesi ve protokol detaylarına göre filtreleme yapılabilirliğidir

```
home-labs ~ # tshark
```

```
Running as user "root" and group "root". This could be dangerous.
```

```
Capturing on eth0
```

```
0.000000 192.168.2.23 -> 80.93.212.86 ICMP Echo (ping) request
0.012641 80.93.212.86 -> 192.168.2.23 ICMP Echo (ping) reply
0.165214 192.168.2.23 -> 192.168.2.22 SSH Encrypted request packet len=52
0.165444 192.168.2.22 -> 192.168.2.23 SSH Encrypted response packet len=52
0.360152 192.168.2.23 -> 192.168.2.22 TCP pcia-rxp-b > ssh [ACK] Seq=53 Ack=53 Win=59896
Len=0
0.612504 192.168.2.22 -> 192.168.2.23 SSH Encrypted response packet len=116
1.000702 192.168.2.23 -> 80.93.212.86 ICMP Echo (ping) request
1.013761 80.93.212.86 -> 192.168.2.23 ICMP Echo (ping) reply
1.057335 192.168.2.23 -> 192.168.2.22 SSH Encrypted request packet len=52
16 packets captured
```


Tcpdump & tshark farkı

```
# tcpdump -i eth0 -n udp port 53 -vv
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
11:57:12.096474 IP (tos 0x0, ttl 128, id 21291, offset 0, flags [none], proto UDP (17), length 59)
```

```
192.168.2.23.1446 > 192.168.2.1.53: [udp sum ok] 2+ A? www.linux.com. (31)
```

```
11:57:12.820246 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 215)
```

```
192.168.2.1.53 > 192.168.2.23.1446: 2 q: A? www.linux.com. 2/3/3 www.linux.com. CNAME  
linux.com., linux.com. [ | domain]
```

```
Domain Name System (response)
```

```
[Request In: 1]
```

```
[Time: 0.001332000 seconds]
```

```
Transaction ID: 0x0001
```

```
Flags: 0x8100 (Standard query response, No error)
```

```
1... .. = Response: Message is a response
```

```
.000 0... .. = Opcode: Standard query (0)
```

```
....0... .. = Authoritative: Server is not an authority for domain
```

```
....0... .. = Truncated: Message is not truncated
```

```
....1... .. = Recursion desired: Do query recursively
```

```
....0... .. = Recursion available: Server can't do recursive queries
```

```
....0... .. = Z: reserved (0)
```

```
....0... .. = Answer authenticated: Answer/authority portion was not authenticated by the
```

```
server
```

```
.... .. 0000 = Reply code: No error (0)
```

```
Questions: 1
```

```
Answer RRs: 1
```

```
Authority RRs: 0
```

```
Additional RRs: 0
```

```
Queries
```

```
1.2.168.192.in-addr.arpa: type PTR, class IN
```

```
Name: 1.2.168.192.in-addr.arpa
```

```
Type: PTR (Domain name pointer)
```

```
Class: IN (0x0001)
```

```
Answers
```

```
1.2.168.192.in-addr.arpa: type PTR, class IN, RT
```

```
Name: 1.2.168.192.in-addr.arpa
```

```
Type: PTR (Domain name pointer)
```

```
Class: IN (0x0001)
```

```
Time to live: 2 hours, 46 minutes, 40 seconds
```

```
Data length: 4
```

```
Domain name: RT
```

Network Grep:Ngrep

- Grep: UNIX/Linux sistemlerde dosya içerisinde belirli düzene uyan stringlerin/satırların bulunmasını sağlar
- Ngrep(Network Grep): grep benzeri bir yazılım fakat klasik dosyalarda değil de ağ trafiğinde arama/bulma işlemi yapar.

Ngrep ile Ne Yapılabilir?

- http portu üzerinden kullanılan SSH bağlantılarını ngrep ile keşfedebilirsiniz
- Ağda şifresiz trafik kullananların parolalarını kaydedip uyarabilirsiniz.
- Tünelleme programlarını ortamda hiçbir IPS, Firewall vs ye ihtiyaç duymadan Ngrep ile yakalayabilirsiniz

```
# ngrep huzeyfe tcp port 25
```

```
interface: rl0 (111.111.111.11/255.255.255.248)
```

```
filter: (ip or ip6) and ( tcp port 25 )
```

```
match: huzeyfe
```

```
#####
```

```
|#####
```

```
T 212.252.168.253:37148 -> 80.93.212.86:25 [AP]
```

```
ehlo huzeyfe..
```

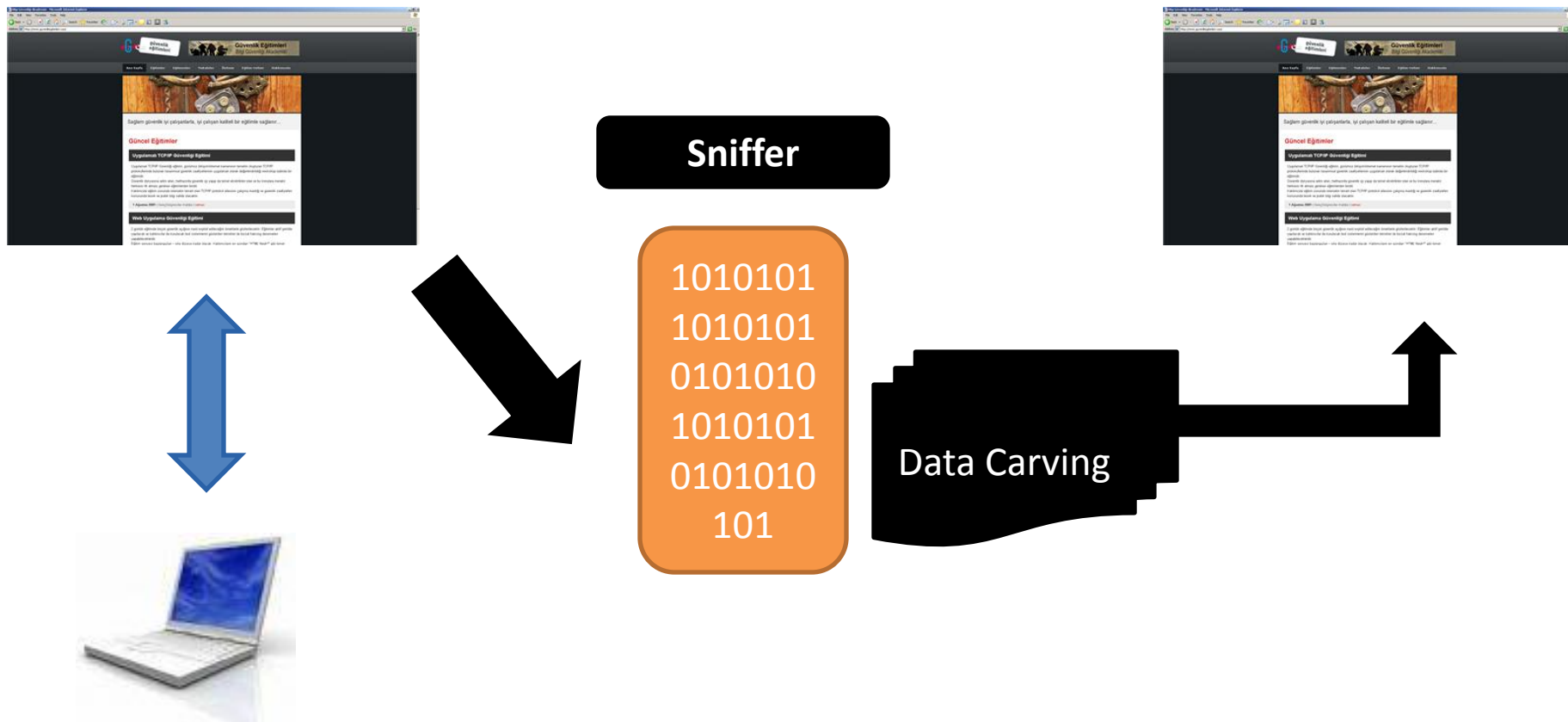
UrlSnarf

- Trafikten pasif olarak HTTP isteklerini ayıklar

```
[root@hackme ~]# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
dsl78.186-35229.ttnet.net.tr - - [04/Apr/2010:22:17:05 +0300] "GET http://hackme.lifeoverip.net/phpmyadmin/ HTTP/1.1" - - "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
dsl78.186-35229.ttnet.net.tr - - [04/Apr/2010:22:17:05 +0300] "GET http://hackme.lifeoverip.net/phpmyadmin/phpmyadmin.css.php?lang=en-iso-8859-1&convcharset=iso-8859-1&collation_connection=utf8_unicode_ci&token=5e379dd8c2ae7c51782243dc9c28ed98&js_frame=right&nocache=3780618665 HTTP/1.1" - - "http://hackme.lifeoverip.net/phpmyadmin/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
dsl78.186-35229.ttnet.net.tr - - [04/Apr/2010:22:17:05 +0300] "GET http://hackme.lifeoverip.net/phpmyadmin/print.css HTTP/1.1" - - "http://hackme.lifeoverip.net/phpmyadmin/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
dsl78.186-35229.ttnet.net.tr - - [04/Apr/2010:22:17:06 +0300] "GET http://hackme.lifeoverip.net/phpmyadmin/themes/original/img/logo_right.png HTTP/1.1" - - "http://hackme.lifeoverip.net/phpmyadmin/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
dsl78.186-35229.ttnet.net.tr - - [04/Apr/2010:22:17:06 +0300] "GET http://hackme.lifeoverip.net/phpmyadmin/themes/original/img/s_error.png HTTP/1.1" - - "http://hackme.lifeoverip.net/phpmyadmin/phpmyadmin.css.php?lang=en-iso-8859-1&convcharset=iso-8859-1&collation_connection=utf8_unicode_ci&token=5e379dd8c2ae7c51782243dc9c28ed98&js_frame=right&nocache=3780618665" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
```

Data Carving...

- Ham veriden orijinal veri elde etme yöntemi



ChaosReader

Go to Google Home [Advanced Search](#) [Preferences](#) [Language Tools](#) [Search Tips](#)
tcpdump home page

Search: ☒ the web ☐ pages from Australia

[Web](#) [Images](#) [Groups](#) [Directory](#) [News](#)

Searched the web for **tcpdump home page**.

[TCPDUMP public repository](#)

This **page** was started to collect various patches that have been floating around for LBL's **tcpdump** and **libpcap** programs, and to continue the work needed on both ...

www.tcpdump.org/ - 10k - [Cached](#) - [Similar pages](#)

[LBNL's Network Research Group](#)

Welcome to the **home page** of the Network Research Group (NRG) of the ... Network tools include: **tcpdump**, the protocol packet capture and dumper program;; **libpcap** ...

Description: Source for **tcpdump**, **libpcap**, and **traceroute**.

Category: [Computers](#) > [Software](#) > [Internet](#) > [Network Management](#)

ee.lbl.gov/ - 6k - [Cached](#) - [Similar pages](#)

[tdg: TcpDump Grapher](#)

tdg: **TcpDump** Grapher. Synopsis: tdg is used to produce time-sequence plots from **tcpdump** files. It is used to view a unidirectional ...

www.psc.edu/networking/tdg.html - 12k - 3 Nov 2003 - [Cached](#) - [Similar pages](#)

[Jon Snader's Home Page](#)

... The WinDump **Home Page** has a version of **tcpdump** that runs under Microsoft Windows. Also available are Windows versions of BPF and **libpcap**. ...

pw1.netcom.com/~jsnader/ - 12k - [Cached](#) - [Similar pages](#)

[Sandelman Software Works](#)

... Guests. Users on this system; Canadian **Tcpdump** mirror;

Hydro-Electric impact archive; OX **home page**; ...

Description: Network security consulting and contract programming. Project and contact information.

Category: [Regional](#) > [North America](#) > ... > [Computers](#) > [Consultants](#)

www.sandelman.ottawa.on.ca/ - 4k - [Cached](#) - [Similar pages](#)

Chaosreader:telnet-replay

```
Ubuntu 8.10
guvenlikod login: huzeyfe
Password:
Linux trcell 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
$ ls
chaosreader0.94  telnet.pcap
$ id
uid=1001(huzeyfe) gid=1001(huzeyfe) groups=1001(huzeyfe)
```

```
root@guvenlikod:/home/huzeyfe# tcpdump -s 0 tcp port 23 -w telnet.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C87 packets captured
87 packets received by filter
0 packets dropped by kernel
```

Telnet Replay-II

```

root@guvenlikod:/home/huzeyfe# perl chaosreader0.94 telnet.pcap
$* is no longer supported at chaosreader0.94 line 265.
Chaosreader ver 0.94

Opening, telnet.pcap

Reading file contents,          100% (7123/7123) 7/7123) 99/7123) 99/7123) 10 100% (85/87) 92% (80/87)
R 74% (64/87) packets, 55% (48/87)      37% (32/87)          18% (16/87)          0% (0/87)
Creating files...
  Num  Session (host:port <=> host:port)      Service
  0001  10.200.43.145:6501,10.200.169.163:23    telnet

index.html created.
root@guvenlikod:/home/huzeyfe# ls
chaosreader0.94  httplog.text  index.html  session_0001.telnet.html  telnet.pcap
getpost.html    image.html    index.text  session_0001.telnet.replay
root@guvenlikod:/home/huzeyfe# ./session_0001.telnet.replay 2
yyyy yy#yy'yyyúyyyúyú'y8yú'y8yúy8yyyúyy!Ubuntu 8.10
guvenlikod login: PuTTYguvenlikod login: huzeyfe
Password:
Linux trcell 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

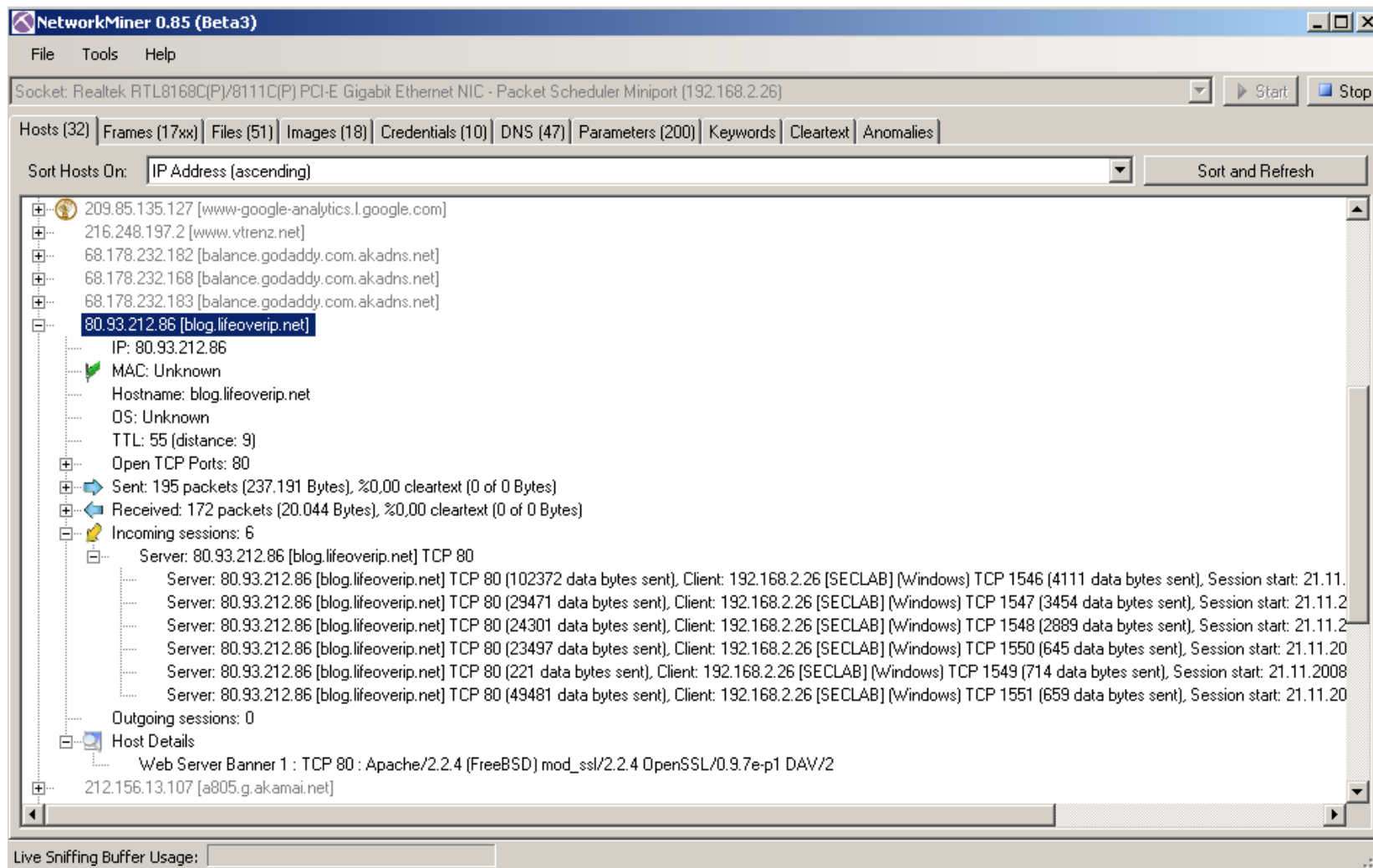
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
$ ls
chaosreader0.94  telnet.pcap
$ id
uid=1001(huzeyfe) gid=1001(huzeyfe) groups=1001(huzeyfe)
root@guvenlikod:/home/huzeyfe# PuTTY

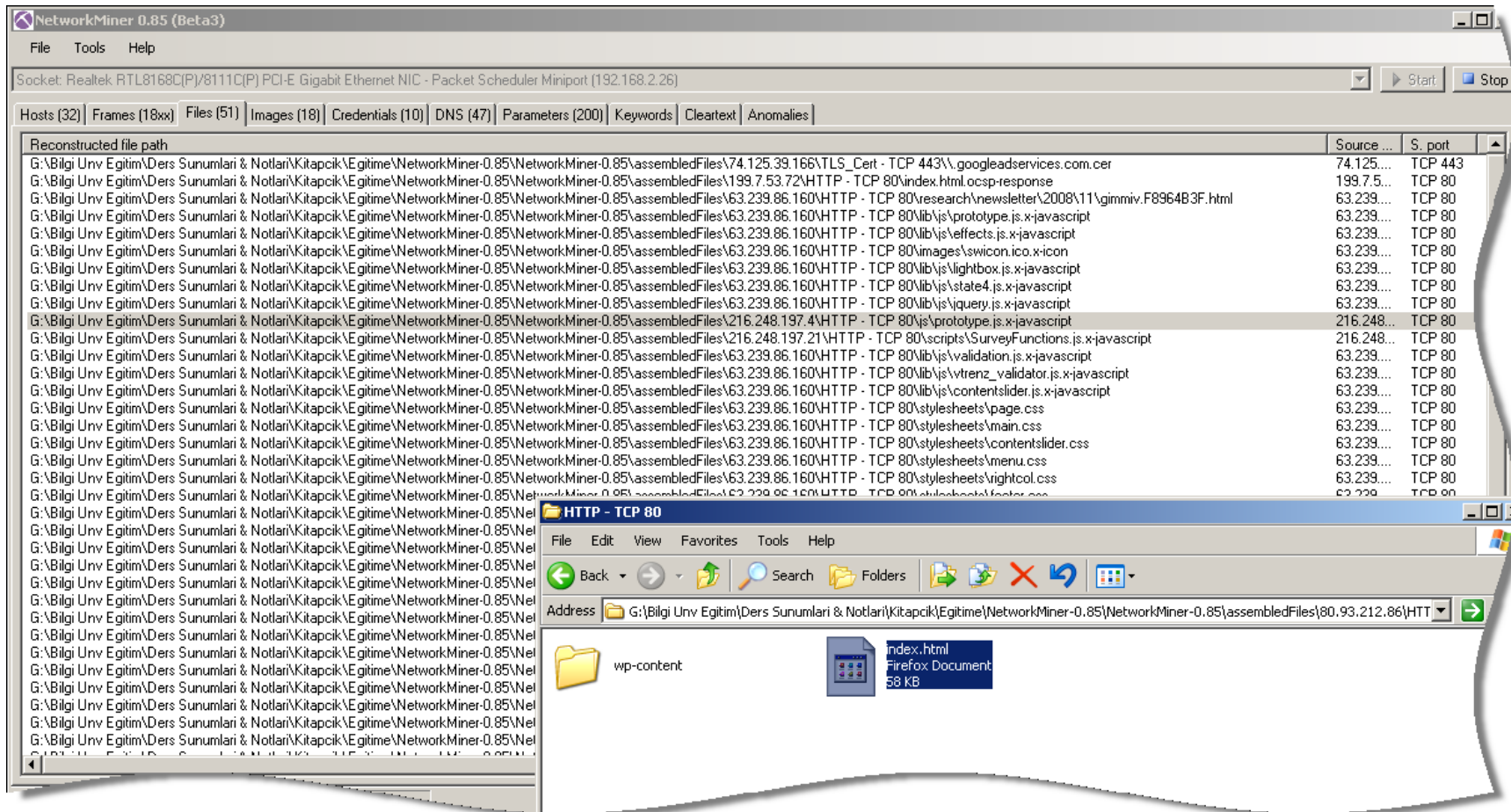
```

session replay

NetworkMiner



NetworkMiner-II



NetworkMiner

my phpGrapy site - Mozilla Firefox

Doğya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

http://www.lifeoverip.net/photos/?dir=kibris

En çok ziyaret edilenler İlk Adm Haberler

Download Roboform Close

Gmail - Inbox (5) - huzeyfe.onal@gmail... Complexity is the Enemy of Security... my phpGrapy site

PHPGRAPHY
root/kibris - 45 file(s)
last commented pictures | top rated pictures | last added pictures | last added pictures per directory

login random pic slideshow

2.00002.jpg

2.00006.jpg

DSC02140.JPG

DSC02141.JPG

NetworkMiner 0.85 (Beta3)

File Tools Help

Socket: Realtek RTL8168C(P)/8111C(P) PCI-E Gigabit Ethernet NIC - Packet Scheduler Miniport (192.168.2.26)

Hosts (32) | Frames (21x4) | Files (73) | Images (34) | Credentials (10) | DNS (50) | Parameters (215) | Keywords | Cleartext | Anomalies

headerbkg.gif 3x75, 190 B
headerlogo.gif 233x37, 3 319 B
contacticon.gif 16x15, 633 B
rssfeed.gif 13x13, 594 B
leftcolbkg_a.gif 180x3, 13 135 B
arrowpic.jpg 40x40, 2 318 B
phonepic.jpg 40x40, 2 313 B
leftnavtopbkg_a.gif 2x10, 13 165 B
_utm.gif.A1F60F2... 1x1, 35 B
topnav-off_b.gif 2x33, 13 245 B
sectionbkg_a.gif 2x45, 13 358 B

dot.gif 1x1, 49 B
transparent_spacer... 1x1, 43 B
loading.gif 32x32, 2 767 B
closelabel.gif 66x22, 979 B
armutlu-300x225.jpg 300x225, 23 971 B
sansur-300x199.jpg 300x199, 23 168 B
translaterileallatma... 300x187, 49 153 B
phpgraphy-banner.gif 200x40, 3 907 B
index.html.A76917E... 100x75, 2 486 B
index.html.52D251... 100x75, 2 142 B
border-top.gif 1x20, 67 B

index.html.CB9CE... 100x75, 2 469 B
index.html.1FE5CF... 100x75, 2 469 B
index.html.EF4001F... 100x75, 2 197 B
border-right.gif 20x1, 67 B
index.php.7C2D53... 75x100, 2 192 B
index.php.5CE6C... 75x100, 1 671 B
index.php.D69CFA... 75x100, 1 844 B
index.php.6ABD73... 100x75, 1 803 B
index.php.7C2D64... 100x75, 2 434 B
index.php.F107465... 100x75, 2 060 B
index.php.A6F70A0... 100x75, 2 035 B

Source: 80.93.212.86 [blog.lifeoverip.net] [www.lifeoverip.net]
Destination: 192.168.2.26 [SECLAB] [seclab] [vindows]
Reconstructed file path: G:\Bilgi Univ Eğitim\Ders Sunumları & Notları\Kitapçık\Eğitime\NetworkMiner-0.85\NetworkMiner-0.85\assembledFiles\80.93.212.86\HTTP - TCP 80\photos\index.php.1EC58475.jpeg

Live Sniffing Buffer Usage:

Xplico

Xplico Interface

User: deft

Help Logout

Cases

Sols

Email

Sip

Web

Images

Printer

Ftp

Mms

GeoMap

Search:

Go

Date	Subject	Sender	Receivers	Size
2007-08-14 11:06:50	*****SPAM***** Magic is real	"Shannon Palacios" <shruga.davenp	<info@iserm.com>	22907
2007-08-14 11:03:50	*****SPAM***** Ladies will love you	"Tania Moreno" <pkcensorial@mon	"f5cd67a3" <f5cd67a3@iserm.com>	3692
2007-08-14 11:02:50	Sorry for being late	"Bridgett" <tajnireiwfcs@advantexr	"Cleo Sanchez" <yoke@iserm.com>	2393
2007-08-14 08:24:10	This basic strategic insight supplied the tactics f	"Daniel Perth" <Daniel836@ecomme	a618f5cf@iserm.com	2303
2007-08-14 08:20:35	You would have been a formidable team.	"Carmela Fomenko" <Fomenkowlg@	<yoke@iserm.com>	5660
2007-08-14 08:18:34	They talked for five or ten minutes and then I he	"Gustavo Breck" <Gustavo_Breck@	<howledabstracted@iserm.com>	2378
2007-08-14 08:12:29	Accept Credit Cards on Your Web Site Today.	"Julie Amomonpon" <Julie.Amomon	<outplaying@iserm.com>	2240
2007-08-14 08:04:58	This report indicates which shows were watch	"Kingman Mulchan" <Mulchan@stef	beforehand@iserm.com	2285
2007-08-14 08:04:41	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D	<hucsoitmvm@iserm.com>	5021
2007-08-14 08:04:34	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D	<pafthsmqc@iserm.com>	5342
2007-08-14 08:04:33	Re: Hallo!	"Abel Chaney" <a-1@adultcashflow.	<solace@iserm.com>	1377
2007-08-14 08:04:31	Delivery Status Notification (Failure)	"Mail Delivery System" <MAILER-DAE	zylqsps@iserm.com	4552
2007-08-14 08:04:31	*****SPAM***** But the way SATA has been dev	"melica soo" <sooltjg@photoesc.co	<a618f5cf@iserm.com>	8125
2007-08-14 08:04:30	*****SPAM***** The girl eluded us.	"Mellissa Goedde" <Goeddejenx@w	<perishedcloudiness@iserm.com>	4229
2007-08-14 08:04:28	About last night	"Crystal Hamilton" <arismenidezorv	"Steve" <has@iserm.com>	2398
2007-08-14 08:04:28	*****SPAM***** Fwd: Thanks, we are accepting	"Drew Christensen" <Ignaciomercur	<howledabstracted@iserm.com>	6263
2007-08-14 08:04:28	Webster, Nesta - "World Revolution", London, ("wandersom Nyland" <wandersom@	<beforehand@iserm.com>	5258
2007-08-14 08:04:26	Just keep in touch	"Goldie Sanchez" <balstoreoamm@	"Lisandra" <guyanayoke@iserm.co	2268
2007-08-14 08:04:24	AUTHENTIC VIAGRA AND CIALIS	"Sales Department" <sales@design	"Luiz Everson" <loxdwvy@iserm.com	1387
2007-08-14 08:04:24	*****SPAM***** Fwd: Thank you, we are ready to	"Heath Randall" <Demetriuselastom	<outplaying@iserm.com>	6109
2007-08-14 08:04:23	Undeliverable: Thanks, we are ready to lend yo	"System Administrator" <administra	<jjowiaqwsit@iserm.com>	4962
2007-08-14 08:04:23	Undelivered Mail Returned to Sender	MAILER-DAEMON@smoothwall.local	xdlyiyiul@iserm.com	4762