

# Bilgi Toplama

---

Necmettin ÇARKACI – Ahmet Alperen BULUT



Biz kimiz

---



# İstihbarat Çeşitleri

---

## Pasif Bilgi Toplama

- Hedef sistemden bağımsız

## Aktif Bilgi Toplama

- Hedef sistemle doğrudan iletişime geçerek

# Aktif Bilgi Toplama



# Traceroute

---

- ⌚ Traceroute bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösteren programdır.



# Dig

---

- ⌚ Detaylı DNS sorgulaması yapan gelişmiş bir araçtır.

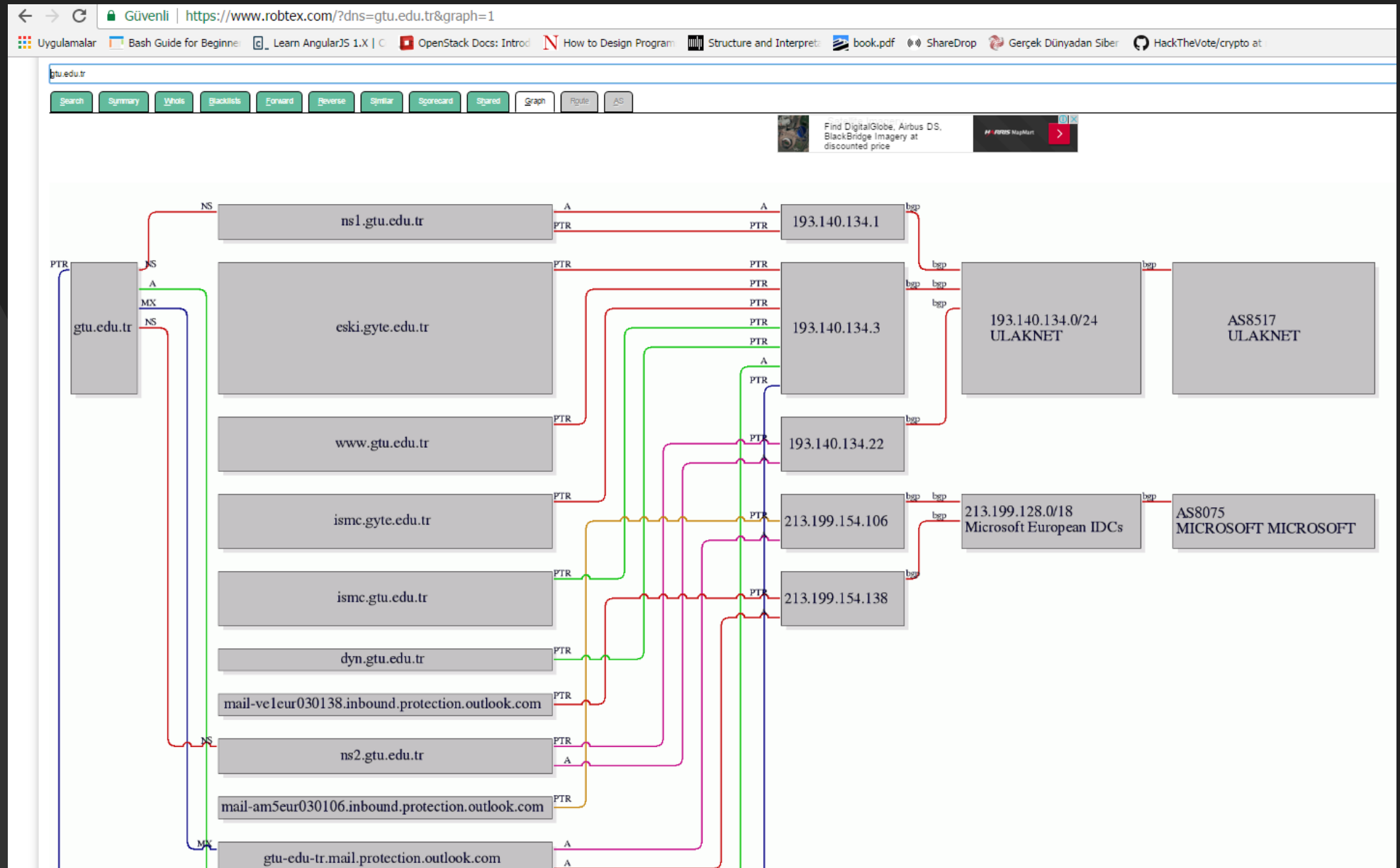


# Dirbuster

---

- ⌚ Hedef adresin alt dizinlerini bulmak için kullanılır.

# Robtex





**Capture Filter:** Yakalanacak paketlerin türü portu protokol bilgisi önceden belirtilerek hedef odaklı bir paket analizi yapılabilir.

# Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is a TCP SYN packet from 192.168.2.7 to 178.210.160.70 on port 21.

Overlaid on the main window is the "Wireshark: Capture Options" dialog box. The "Capture" tab is active, showing a table of interfaces to capture on:

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MB]	Mon. Mode	Capture Filter
<input checked="" type="checkbox"/>	Wi-Fi: en0 fe80::22c9:d0ff:fe86:5691 192.168.2.7	Ethernet	enabled	default	2	disabled	tcp port 21
<input type="checkbox"/>	p2p0	Raw IP	enabled	default	2	n/a	
<input type="checkbox"/>	Loopback: lo0 fe80::1 127.0.0.1	BSD loopback	enabled	default	2	n/a	

Below the table, the "Capture on all interfaces" checkbox is unchecked, and the "Use promiscuous mode on all interfaces" checkbox is checked. The "Capture Filter" field is set to "tcp port 21", which is highlighted with a red box. A red arrow points from this field to the "tcp port 21" entry in the table above. The "Compile selected BPFs" button is visible to the right of the filter field.

The "Capture Files" section at the bottom shows options for saving the capture, including "Use multiple files", "Use pcap-ng format", and "Next file every" settings.

The "Display Options" section on the right includes checkboxes for "Update list of packets in real time", "Automatically scroll during live capture", "Hide capture info dialog", "Resolve MAC addresses", and "Resolve network-layer names".



**Display Filter:** Yakalanan paketlerin içerisinde istenilen özelliklerdeki paketlerin ayıklanması kısmında kullanılabilir.

Wireshark

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The filter bar at the top contains the text "Filter: tcp.srcport == 80" and buttons for "Expression...", "Clear", "Apply", and "Save".

The main packet list pane displays a table of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The packets are all HTTP requests from 64.15.117.144 to 192.168.2.7, all with a length of 1506 bytes and containing the text "1506 Continuation or non-HTTP traffic".

The packet details pane for the selected packet (No. 1) shows the following information:

- Frame 1: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface 0
- Ethernet II, Src: AirtiesW\_59:5e:25 (00:1c:a8:59:5e:25), Dst: Apple\_86:56:91 (20:c9:d0:86:56:91)
- Internet Protocol Version 4, Src: 64.15.117.144 (64.15.117.144), Dst: 192.168.2.7 (192.168.2.7)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 49219 (49219), Seq: 1, Ack: 1, Len: 1452
  - Source port: http (80)
  - Destination port: 49219 (49219)
  - [Stream index: 0]
  - Sequence number: 1 (relative sequence number)
  - [Next sequence number: 1453 (relative sequence number)]
  - Acknowledgment number: 1 (relative ack number)
  - Header length: 20 bytes
  - Flags: 0x010 (ACK)
  - Window size value: 304
  - [Calculated window size: 304]
  - [Window size scaling factor: -1 (unknown)]
  - Checksum: 0xd8c4 [validation disabled]
  - [SEQ/ACK analysis]
- Hypertext Transfer Protocol

The packet bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII format.

File: "/var/folders/jb/czplsn..." Packets: 1255 · Displayed: 731 (58,2%) · Dropped: 0 (0,0%) Profile: Default



# Kelime arama : İzlenen trafik içerisinde kelime arama;

# Wireshark

The image shows the Wireshark 1.10.0 interface. The main packet list displays various network traffic. A red arrow points from the 'berbergokmen' text in the search box of the 'Wireshark: Find Packet' dialog to the packet details pane, specifically to the 'Domain Name System (query)' section where the query name is 'berbergokmen.com: type A, class IN'.

**Wireshark: Find Packet**

Find-  
By: ☐ Display filter ☐ Hex value ☒ String

☒ Filter: **berbergokmen**

Search In:  
☐ Packet list  
☐ Packet details  
☒ Packet bytes

String Options:  
☐ Case sensitive  
Character width:  
Narrow & wide

Direction:  
☐ Up  
☒ Down

**Packet Details:**

- Frame 264: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface
- Ethernet II, Src: Apple\_86:56:91 (20:c9:d0:86:56:91), Dst: Airtim
- Internet Protocol Version 4, Src: 192.168.2.7 (192.168.2.7), Dst:
- User Datagram Protocol, Src Port: 50757 (50757), Dst Port: domain
- Domain Name System (query)
  - [Response In: 265]
  - Transaction ID: 0xa2a2
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - berbergokmen.com: type A, class IN
      - Name: berbergokmen.com
      - Type: A (Host address)
      - Class: IN (0x0001)



**Protokol detayı :** Protokol detaylarının gösterilmesi. Özellikle DDOS saldırılarında saldırı tipini belirlemek için kullanılır.

Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A red box highlights the 'Protocol Hierarchy Statistics' window, which provides a detailed breakdown of the captured traffic by protocol.

**Protocol Hierarchy Statistics (Display filter: none)**

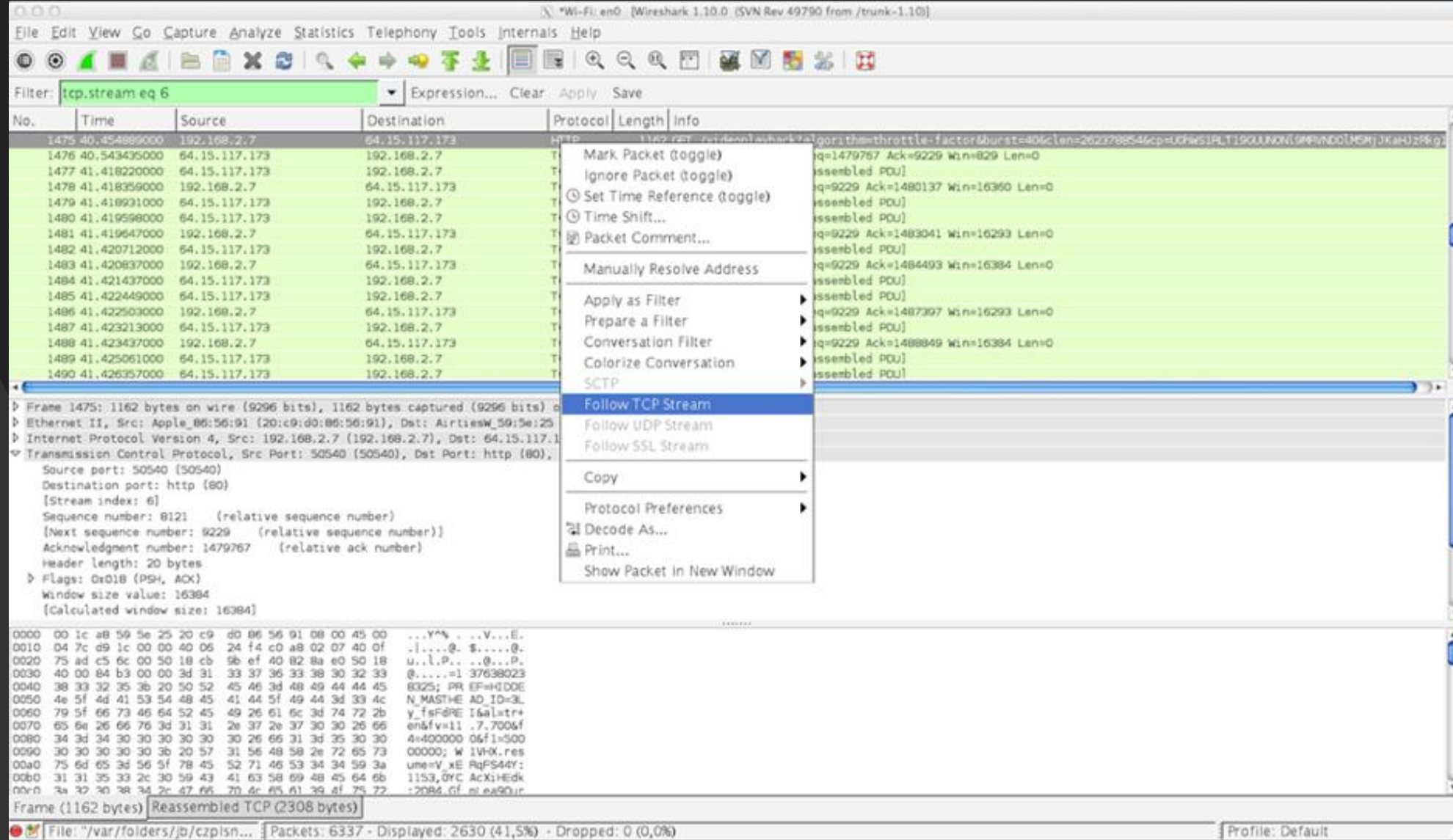
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Ethernet	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Internet Protocol Version 4	99,07 %	6278	99,96 %	6154583	0,435	0	0	0,000
User Datagram Protocol	1,01 %	64	0,12 %	7296	0,001	0	0	0,000
Domain Name Service	0,98 %	62	0,11 %	6730	0,000	62	6730	0,000
Hypertext Transfer Protocol	0,03 %	2	0,01 %	566	0,000	2	566	0,000
Transmission Control Protocol	98,04 %	6213	99,84 %	6147217	0,435	6021	6068695	0,429
Secure Sockets Layer	2,30 %	146	0,70 %	42941	0,003	144	41111	0,003
Secure Sockets Layer	0,03 %	2	0,03 %	1830	0,000	2	1830	0,000
Hypertext Transfer Protocol	0,66 %	42	0,50 %	30937	0,002	24	18724	0,001
Media Type	0,27 %	17	0,18 %	11353	0,001	17	11353	0,001
Line-based text data	0,02 %	1	0,01 %	860	0,000	1	860	0,000
Malformed Packet	0,06 %	4	0,08 %	4644	0,000	4	4644	0,000
Internet Control Message Protocol	0,02 %	1	0,00 %	70	0,000	1	70	0,000
Address Resolution Protocol	0,93 %	59	0,04 %	2478	0,000	59	2478	0,000

The bottom status bar indicates: Text item (text), 31 bytes | Packets: 6337 - Displayed: 6337 (100,0%) - Dropped: 0 (0,0%) | Profile: Default

**TCP follow :** TCP oturumlarında paket birleştirme, HTTP bağlantısındaki tüm giden gelen paketlerin birleştirilip session hakkında bilgi verilmesi.

# Wireshark

Birleştirilmek istenilen protokol paketi üzerinde sağ tıklanır ve "Follow TCP Stream" seçeneği seçilir.





## İstek sayıları : http istek sayılarının görüntülenmesi.

# Wireshark

The image shows the Wireshark network protocol analyzer interface. The main packet list on the left displays a series of captured packets, with packet 337 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. A summary window titled 'HTTP/Requests with filter:' is open in the foreground, displaying a table of HTTP requests by host. The table has columns for Topic / Item, Count, Rate (ms), and Percent. The data is as follows:

Topic / Item	Count	Rate (ms)	Percent
HTTP Requests by HTTP Host	972	0,001136	
res.reklamport.com	15	0,000018	1,54%
www.sahibinden.com	30	0,000035	3,09%
banner2.sahibinden.com	90	0,000105	9,26%
image5.sahibinden.com	40	0,000047	4,12%
b.scorecardresearch.com	55	0,000064	5,66%
pubads.g.doubleclick.net	10	0,000012	1,03%
ad.reklamport.com	10	0,000012	1,03%
gatr.hit.gemius.pl	21	0,000025	2,16%
www.google-analytics.com	32	0,000037	3,29%
csi.gstatic.com	1	0,000001	0,10%
ds.serving-sys.com	1	0,000001	0,10%
kelebekgaleri.hurriyet.com.tr	50	0,000058	5,14%
www.hurriyet.com.tr	21	0,000025	2,16%
api1.hurpass.com	15	0,000018	1,54%
imgkelebek.hurriyet.com.tr	22	0,000026	2,26%
adonline.e-kolay.net	7	0,000008	0,72%
sayac.hurriyet.com.tr	9	0,000011	0,93%
ad.e-kolay.net	19	0,000022	1,95%
www.facebook.com	16	0,000019	1,65%

The bottom status bar indicates the capture is live on the Wi-Fi interface 'en0', with 94674 packets displayed (100,0% of the total).

# Kaynakça

---

- ⌚ Paket/Protokol Analizi Amaçlı Wireshark Kullanımı,  
[http://wiki.bgasecurity.com/Paket/Protokol\\_Analizi\\_Amaçlı\\_Wireshark\\_Kullanımı](http://wiki.bgasecurity.com/Paket/Protokol_Analizi_Amaçlı_Wireshark_Kullanımı)