Computer Networks

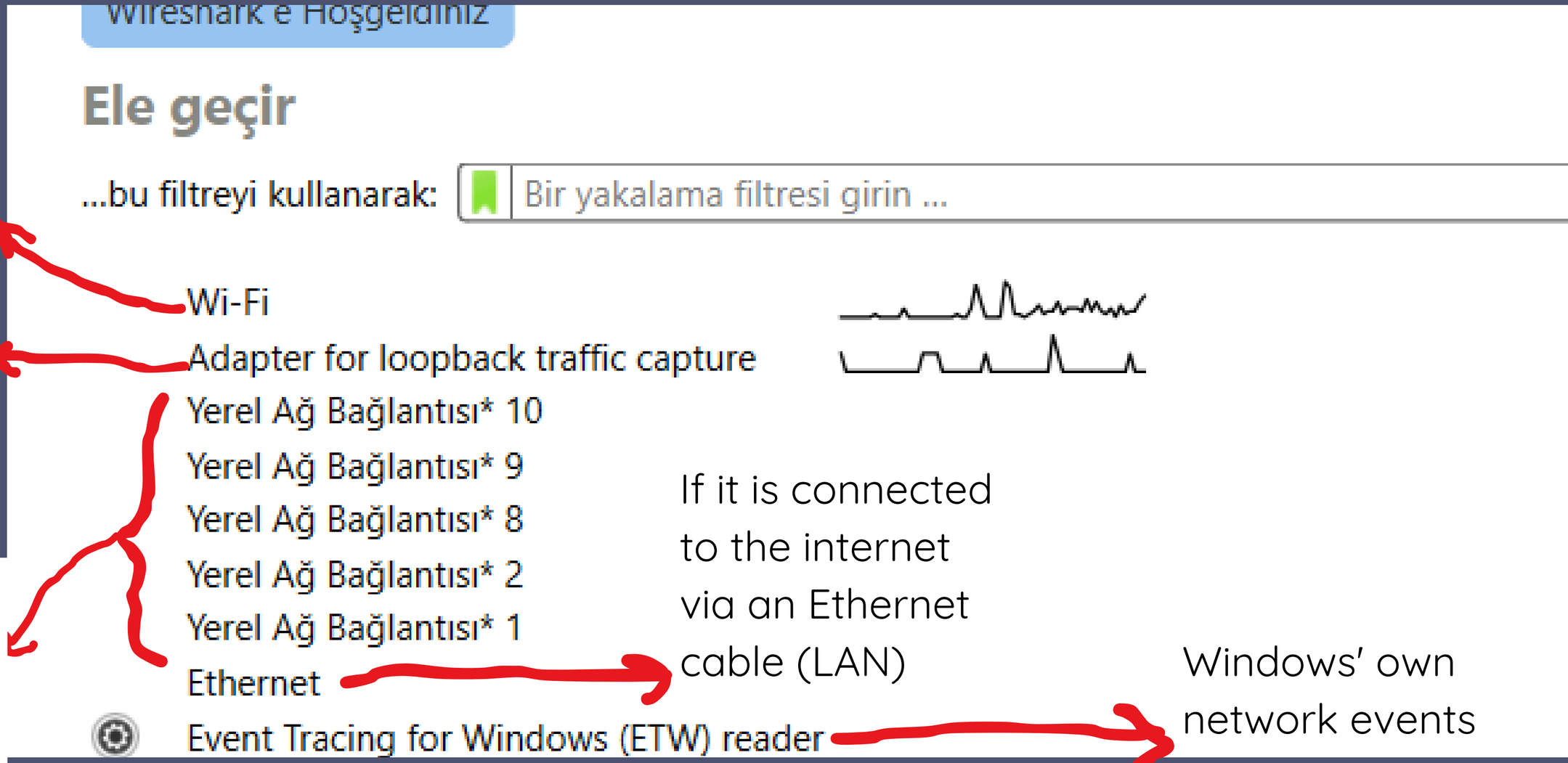
WIRESHARK

Res. Asst. Melek ŞENTÜRK

The device is using a wireless connection.

Traffic inside the computer (localhost, 127.0.0.1)

If there are multiple Ethernet cards, a VPN connection, or a virtual network adapter



If it is connected to the internet via an Ethernet cable (LAN)

Windows' own network events

Interfaces that can be used to capture network traffic are listed. The desired network interface can be selected by double-clicking.

UDP(USER DATAGRAM PROTOCOL)

UDP (User Datagram Protocol) is a connectionless and unreliable transport layer protocol.

UDP is used in applications that require fast and low-latency data transmission. However, since it lacks error control and packet sequencing mechanisms, packet loss or ordering errors may occur.

UDP(USER DATAGRAM PROTOCOL)

udp

No.	Time	Source	Destination	Protocol	Length	Info
4	1.012650	23.58.222.27	10.25.130.93	UDP	1278	443 → 52715 Len=1236
5	1.279426	193.140.13.75	10.25.130.93	UDP	63	443 → 50878 Len=21
6	2.680494	2.19.193.42	10.25.130.93	UDP	1292	443 → 54571 Len=1250
10	5.999318	2.19.193.42	10.25.130.93	UDP	137	443 → 54571 Len=95
11	6.436455	23.58.222.27	10.25.130.93	UDP	146	443 → 51478 Len=104
12	6.992422	23.58.222.27	10.25.130.93	UDP	146	443 → 52715 Len=104
13	7.668131	193.140.13.75	10.25.130.93	UDP	144	443 → 50878 Len=102

Wireshark · Paket 4 · Wi-Fi

```
> Frame 4: 1278 bytes on wire (10224 bits), 1278 bytes captured (10224 bits) on interface \Device\NPF_{937ABBDD-A154-45C0-8C41-4162E533F585}, id 0
> Ethernet II, Src: HuaweiTechno_7f:f7:b5 (ac:75:1d:7f:f7:b5), Dst: Intel_09:6d:11 (d0:ab:d5:09:6d:11)
> Internet Protocol Version 4, Src: 23.58.222.27, Dst: 10.25.130.93
> User Datagram Protocol, Src Port: 443, Dst Port: 52715
v Data (1236 bytes)
    Data […]: 49d1f312eb1cbbee2127721bebf2004a926c9191b0a5d25421b14c3e58e76d49c7d73ced1c4642fc845d1b870ffa4e2e8b34b15d3c8931c7cf94f6256bec51e3e096
    [Length: 1236]
```

UDP USAGE AREAS

DNS (Domain Name System): It performs fast queries to resolve the IP addresses of websites.

SSDP (Simple Service Discovery Protocol): It sends UDP broadcasts to discover network devices.

DHCP (Dynamic Host Configuration Protocol): It uses UDP to automatically assign IP addresses to devices.

DNS(DOMAIN NAME SYSTEM)

dns && frame contains "udemy"

No.	Time	Source	Destination	Protocol	Length	Info
2557	16.709494	192.168.1.101	192.168.1.1	DNS	69	Standard query 0x959d A udemy.com
2558	16.709730	192.168.1.101	192.168.1.1	DNS	69	Standard query 0xfa71 HTTPS udemy.com
2559	16.716843	192.168.1.101	192.168.1.1	DNS	69	Standard query 0x15f9 A udemy.com
2560	16.717042	192.168.1.101	192.168.1.1	DNS	69	Standard query 0x6293 HTTPS udemy.com
2561	16.721099	192.168.1.1	192.168.1.101	DNS	101	Standard query response 0x959d A udemy.com A 104.16.142.237 A 104.16.143
2562	16.721099	192.168.1.1	192.168.1.101	DNS	101	Standard query response 0x15f9 A udemy.com A 104.16.142.237 A 104.16.143

When we enter "udemy.com" in the browser, the computer tries to learn the IP address via "192.168.1.1".

SSDP (SIMPLE SERVICE DISCOVERY PROTOCOL

ssdp

No.	Time	Source	Destination	Protocol	Length	Info
292	58.810979	192.168.1.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
293	59.067901	192.168.1.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
294	59.327628	192.168.1.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
295	59.580310	192.168.1.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

SSDP is a discovery protocol that operates within the UPnP (Universal Plug and Play) framework and enables devices to find each other.

If there are UPnP-supported devices on the network, they will respond and advertise their services.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
31	1.025469	192.168.1.101	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0x84ede34
32	1.077106	192.168.1.1	192.168.1.101	DHCP	590	DHCP ACK - Transaction ID 0x84ede34

```
C:\Users\Melek>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet whi
No operation can be performed on Yerel Ağ Bağ
No operation can be performed on Yerel Ağ Bağ
```

It is a protocol that automatically assigns IP addresses, gateway, DNS servers, and other network configurations to devices on the network.

QUIC (QUICK UDP INTERNET CONNECTIONS)

udp && quic

No.	Time	Source	Destination	Protocol	Length	Info
6339	23.083580	212.156.180.14	192.168.1.101	QUIC	1292	Protected Payload (KP0)
6340	23.083580	212.156.180.14	192.168.1.101	QUIC	1292	Protected Payload (KP0)
6341	23.083580	212.156.180.14	192.168.1.101	QUIC	1292	Protected Payload (KP0)
6342	23.083580	212.156.180.14	192.168.1.101	QUIC	1292	Protected Payload (KP0)
6343	23.083705	192.168.1.101	212.156.180.14	QUIC	75	Protected Payload (KP0), DCID=ea3224b4e9e1cacb

The Destination Connection ID used on the target side of the connection (server side)

QUIC is a connection protocol that operates over UDP and is used especially by Google, YouTube, Chrome, and HTTP/3-based web services.

TCP(TRANSMISSON CONTROL PROTOCOL)

TCP is a connection-oriented protocol used to ensure communication security and data integrity.

A connection is established before communication begins between two devices (3-way handshake). After data is transmitted, the connection is closed in a controlled manner (4-way handshake).

Data is sent in order, and it is ensured that it reaches completely. Error checking and retransmission of lost packets are provided. The data rate is adjusted according to the receiver, so the sender does not overwhelm the receiver.

TCP(TRANSMISSON CONTROL PROTOCOL)

192.168.1.101	217.20.58.100	TCP	66	51142 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
217.20.58.100	192.168.1.101	TCP	66	80 → 51142 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=8
192.168.1.101	217.20.58.100	TCP	54	51142 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
192.168.1.101	217.20.58.100	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c32940e903be1acb HTTP/1.1
217.20.58.100	192.168.1.101	TCP	54	80 → 51142 [ACK] Seq=1 Ack=283 Win=66776 Len=0
217.20.58.100	192.168.1.101	HTTP	400	HTTP/1.1 304 Not Modified
192.168.1.101	217.20.58.100	TCP	54	51142 → 80 [ACK] Seq=283 Ack=347 Win=130816 Len=0

A TCP connection is established between the client and the server. The client sends an HTTP GET request to the server. The server responds with a 304 Not Modified (the cached version is available). Communication is completed with TCP ACK packets.

TLS (TRANSPORT LAYER SECURİTY)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	104.16.102.112	10.25.130.93	TLSv1.2	92	Application Data
2	0.001199	10.25.130.93	104.16.102.112	TLSv1.2	96	Application Data

Wireshark · Paket 1 · Wi-Fi

```
> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NP
> Ethernet II, Src: HuaweiTechno_7f:f7:b5 (ac:75:1d:7f:f7:b5), Dst: Intel_09:6d:11 (d0:ab:d5
> Internet Protocol Version 4, Src: 104.16.102.112, Dst: 10.25.130.93
> Transmission Control Protocol, Src Port: 443, Dst Port: 52368, Seq: 1, Ack: 1, Len: 38
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 33
      Encrypted Application Data: d9890bdb9b0a10402d2b8f011cef3bbdfc2e1ed777d9dd4c4619fb4a
      [Application Data Protocol: Hypertext Transfer Protocol]
```

ICMP PROTOKOLU

ICMP (Internet Control Message Protocol) is a network protocol that allows network devices (routers, computers, etc.) to exchange information about network connections.

ICMP is not used for data transmission; instead, it is used to report network errors and check the status of the network. It notifies whether packets have reached their destination.

ping command: Sends an ICMP Echo Request message to the target computer and measures the response time.
tracert (Windows) / traceroute (Linux): Detects the routers (hops) the packet passes through.

PING TRAFFIC WITH WIRESHARK

icmp

.	Time	Source	Destination	Protocol	Length	Info
51	5.979836	192.168.1.101	172.217.17.110	ICMP	74	Echo (ping) request id=0x0001, seq=296/10241, ttl=128 (reply in 53)
53	6.003961	172.217.17.110	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0001, seq=296/10241, ttl=56 (request in 51)
56	6.988251	192.168.1.101	172.217.17.110	ICMP	74	Echo (ping) request id=0x0001, seq=297/10497, ttl=128 (reply in 57)
57	7.012065	172.217.17.110	192.1			01, seq=297/10497, ttl=56 (request in 56)
64	8.012268	192.168.1.101	172.2			01, seq=298/10753, ttl=128 (reply in 65)
65	8.035842	172.217.17.110	192.1			01, seq=298/10753, ttl=56 (request in 64)
66	9.024822	192.168.1.101	172.2			01, seq=299/11009, ttl=128 (reply in 67)
67	9.048942	172.217.17.110	192.1			01, seq=299/11009, ttl=56 (request in 66)

Komut İstemi

```
C:\Users\Melek>ping google.com

Pinging google.com [172.217.17.110] with 32 bytes of data:
Reply from 172.217.17.110: bytes=32 time=24ms TTL=56
Reply from 172.217.17.110: bytes=32 time=24ms TTL=56
Reply from 172.217.17.110: bytes=32 time=23ms TTL=56
Reply from 172.217.17.110: bytes=32 time=24ms TTL=56

Ping statistics for 172.217.17.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 24ms, Average = 23ms
```

PING TRAFFIC WITH WIRESHARK

Wireshark · Paket 51 · Wi-Fi

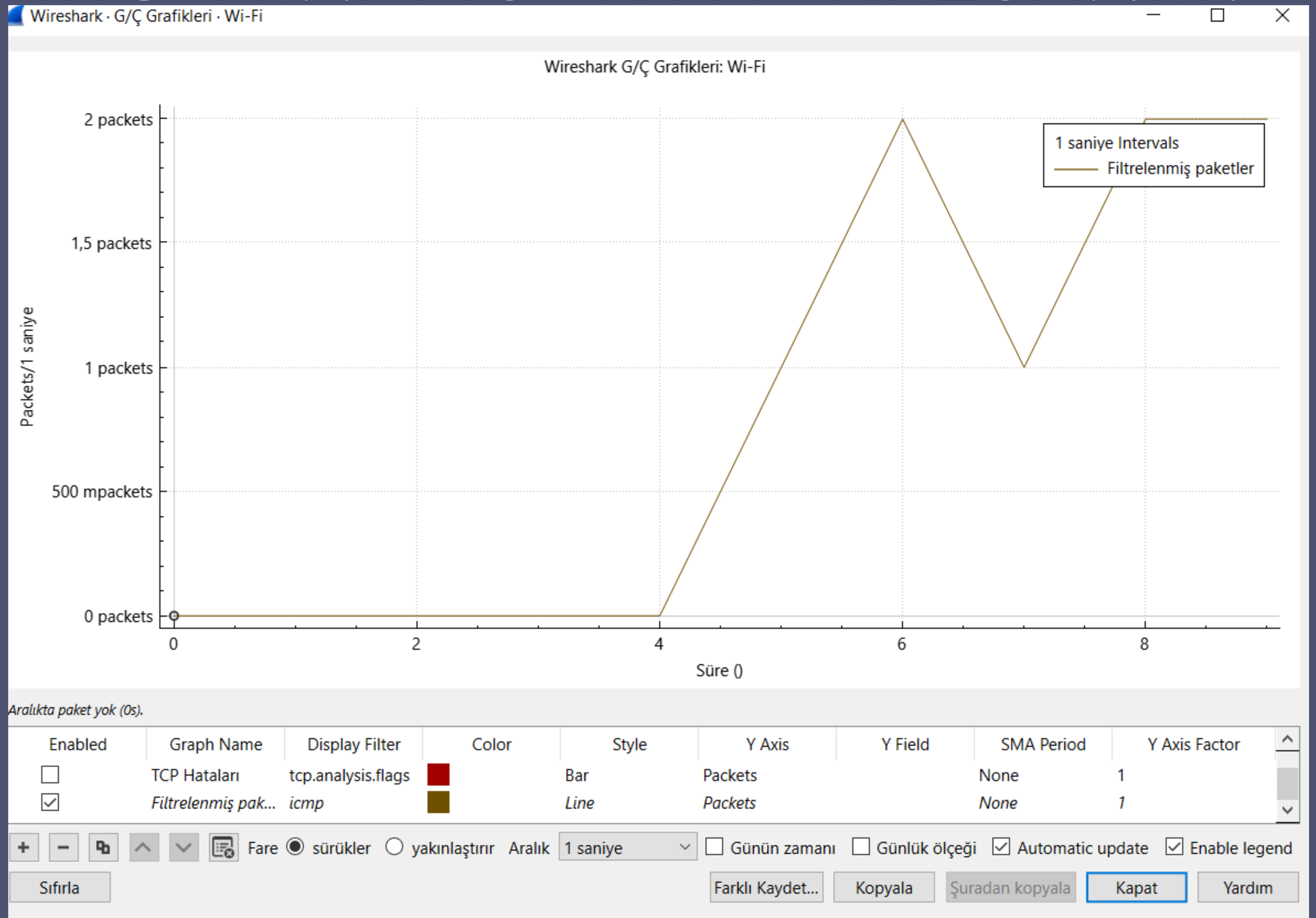
```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4c33 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 296 (0x0128)
    Sequence Number (LE): 10241 (0x2801)
    [Response frame: 53]
    Data (32 bytes)
        Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
        [Length: 32]

0000  4c d6 29 60 52 71 d0 ab  d5 09 6d 11 08 00 45 00   L·)`Rq·· ··m···E·
0010  00 3c ad d7 00 00 80 01  0c 95 c0 a8 01 65 ac d9   ·<····· ·····e··
0020  11 0e 08 00 4c 33 00 01  01 28 61 62 63 64 65 66   ····L3·· ·(abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Paket içeriğinin ASCII kodu

Paket içeriği

PING TRAFFIC WITH WIRESHARK



IP FILTER

ip.addr == 192.168.1.101 and icmp

No.	Time	Source	Destination	Protocol
51	5.979836	192.168.1.101	172.217.17.110	ICMP
53	6.003961	172.217.17.110	192.168.1.101	ICMP
56	6.988251	192.168.1.101	172.217.17.110	ICMP
57	7.012065	172.217.17.110	192.168.1.101	ICMP
64	8.012268	192.168.1.101	172.217.17.110	ICMP
65	8.035842	172.217.17.110	192.168.1.101	ICMP
66	9.024822	192.168.1.101	172.217.17.110	ICMP
67	9.048942	172.217.17.110	192.168.1.101	ICMP

HTTP-HTTPS

HTTP

Hypertext Transfer Protocol

HTTP (Hypertext Transfer Protocol) is a protocol used for data transmission on the web.

Web pages, images, videos, and other content on the internet are transmitted over HTTP.

HTTP is based on a request-response model that facilitates data exchange between the client (usually a web browser) and the server (the server hosting the website).

HTTPS

Hypertext Transfer Protocol Secure

It is the secure version of the HTTP protocol.

It ensures the encrypted transmission of data on the internet, protecting users' privacy and security.

HTTPS is used on websites where personal information (passwords, credit card details, etc.) needs to be transmitted and makes the communication between the user and the server secure.

HTTP REQUEST

http

No.	Time	Source	Destination	Protocol	Length	Info
7595	128.389091	192.168.1.101	34.223.124.45	HTTP	502	GET / HTTP/1.1
7602	128.607655	34.223.124.45	192.168.1.101	HTTP	915	HTTP/1.1 200 OK (text/html)

We are making an HTTP request from the browser.

HTTP

Wireshark · Paket 7595 · Wi-Fi

```
    Destination Address: 34.223.124.45
    [Stream index: 69]
> Transmission Control Protocol, Src Port: 50307, Dst Port: 80, Seq: 1, Ack: 1, Len: 448
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: neverssl.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/53
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Response in frame: 7602]
    [Full request URI: http://neverssl.com/]
```