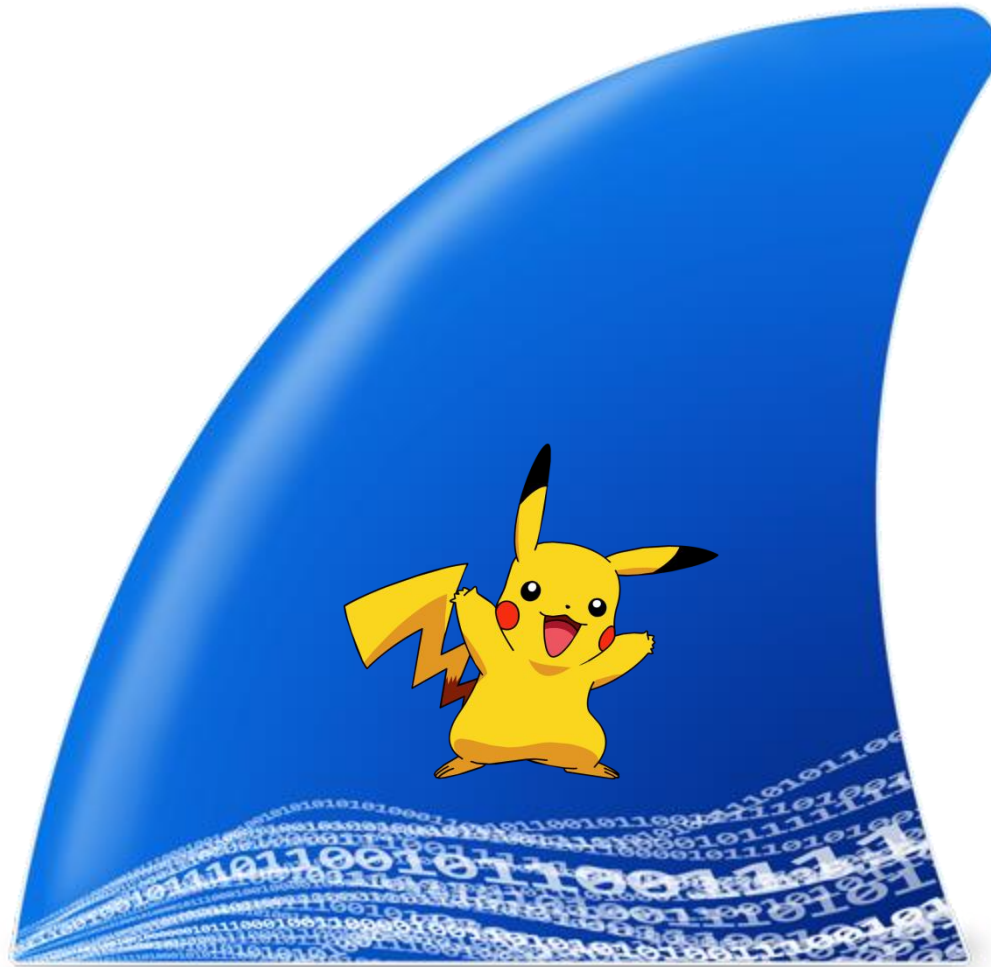




WIFI ATTACK AND DEFENSE

Besim ALTINOK
Security Engineer

Wireshark ile Kablosuz Ağ Analizi



Wireshark Hakkında

Ücretsiz

Kullanıcı Dostu

Çok fazla protokolü desteklemektedir.

Wireshark Hakkında

Desteklenen Sistemler



Wireshark Hakkında

Sistem Gereksinimleri

- 400 MHZ işlemci veya daha hızlısı
- 60 MB boş alan
- Promiscuous destekli bir kart
- WinPcap driver

Wireshark Hakkında

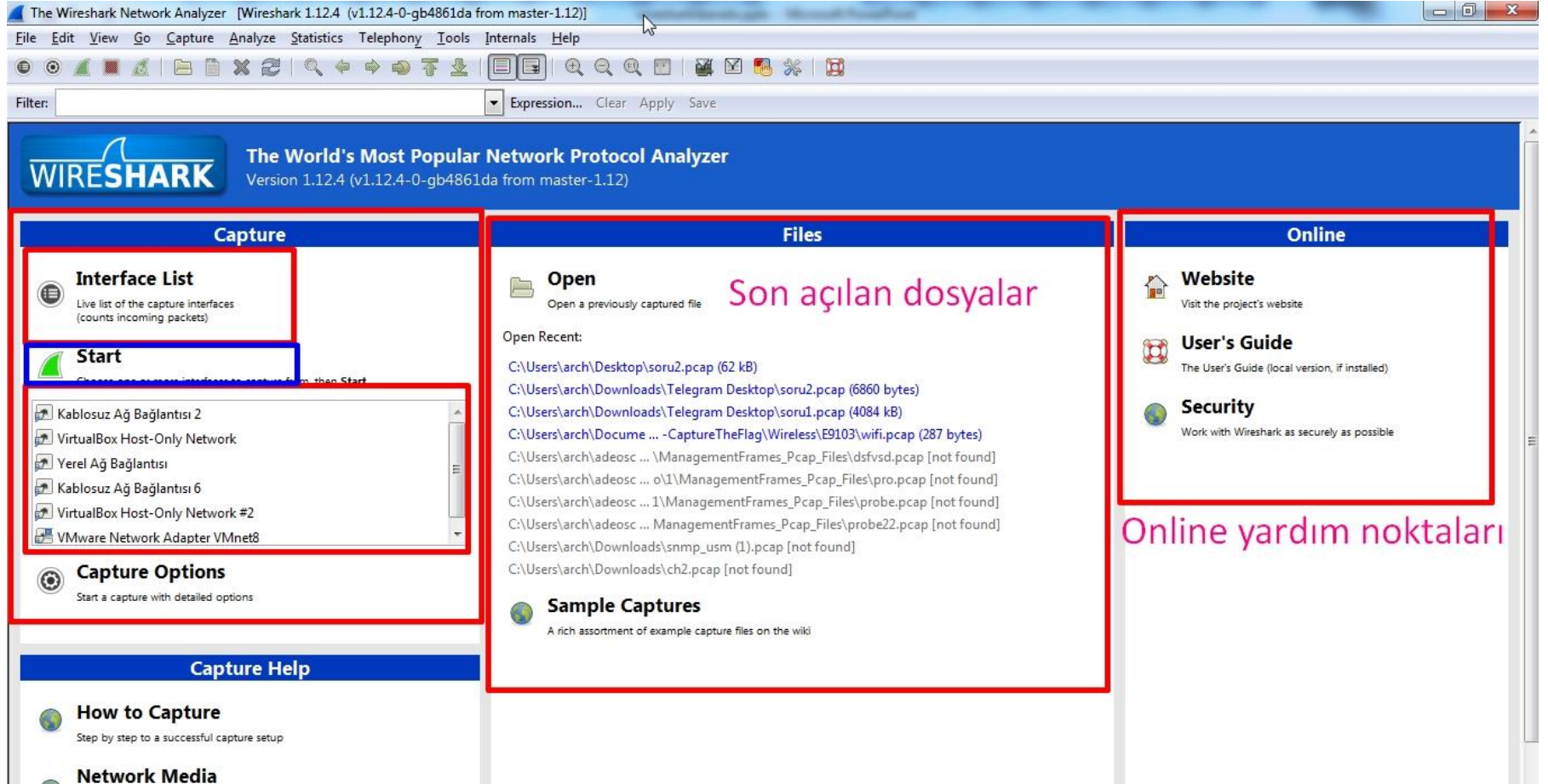
Kurulum

- **RPM based systems** : `rpm -ivh wireshark*.rpm`
- **DEB based systems** : `apt-get install wireshark`
- **Windows Systems** : Next – Next – Next

Kablosuz Sniffing için Öneriler

- Sniff edeceğiniz cihazlara yakın olmaya çalışın, ya da kablosuz ağ kartınızın mesafe algısına dikkat edin.
- Sniffing işlemi sırasında yakınlarda bulunan diğer vericileri devre dışı bırakın
- Sniffing işleminde CPU kullanımınızı azaltın.
- Ağ kartınızın sniff ettiğiniz kablosuz ağın standartlarını desteklemesine dikkat edin.
- Channel hopping işlemini çevredeki mevcut kablosuz ağları tespit etmek istediğinizde kullanın. Bunun dışında özel bir ağ için sniff işlemi yaparsanız ağ kartınızın aynı kanal numarasında olmasına dikkat ediniz. Böylece paket kayıplarını minimum seviyeye indireceksiniz.

Wireshark ile Kablosuz Ağ Analizi



Wireshark Aracını Tanıyalım

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help Menü

Kisayollar

Filter: Filtre Kısmı Expression... Clear Apply Save

No.	Time	SSID	Source	Destination	Protocol	Length	Info
68	26.726913		192.168.2.80	216.58.208.110	TCP	66	38458→443 [S
69	26.732809		192.168.2.80	216.58.208.110	QUIC	1392	CID: 1546533
70	26.768446		216.58.208.110	192.168.2.80	TCP	66	443→38458 [S
71	26.768492		192.168.2.80	216.58.208.110	TCP	54	38458→443 [A
72	26.768911		192.168.2.80	216.58.208.110	TLSv1.2	273	Client Hello
73	26.782521		216.58.208.110	192.168.2.80	QUIC	1392	CID: 0, Seq:
74	26.784849		192.168.2.80	216.58.208.110	QUIC	79	CID: 1546533
75	26.785120		192.168.2.80	216.58.208.110	QUIC	1294	CID: 1546533
76	26.785852		192.168.2.80	216.58.208.110	QUIC	309	CID: 1546533
77	26.811671		216.58.208.110	192.168.2.80	TCP	54	443→38458 [A
78	26.813292		216.58.208.110	192.168.2.80	TLSv1.2	1466	Server Hello
79	26.813942		216.58.208.110	192.168.2.80	TCP	1466	[TCP segment
80	26.813969		192.168.2.80	216.58.208.110	TCP	54	38458→443 [A

Yakalanan paketlerin Listesi

Frame 68: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: Besim_26:10:99 (e0:06:e6:26:10:99), Dst: Airtiesw_6e:af:d2 (18:28:61:6e:af:d2)

Internet Protocol Version 4, Src: 192.168.2.80 (192.168.2.80), Dst: 216.58.208.110 (216.58.208.110)

Transmission Control Protocol, Src Port: 38458 (38458), Dst Port: 443 (443), Seq: 0, Len: 0

Seçilen bir paketin detayları

Raw Data

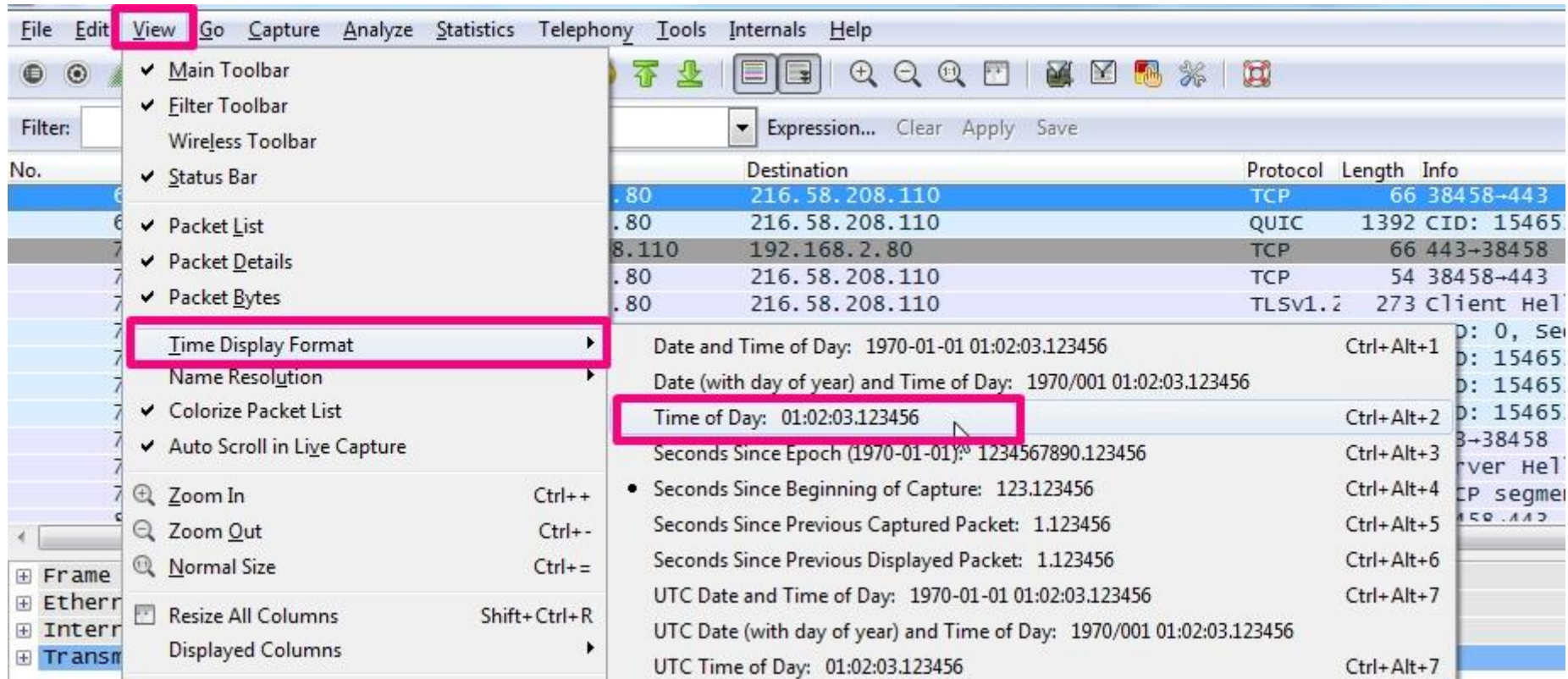
```
0000 18 28 61 6e af d2 e0 06 e6 26 10 99 08 00 45 00 .(an....&....E.
0010 00 34 69 da 40 00 80 06 25 48 c0 a8 02 50 d8 3a .4i.@...%H...P.:
0020 d0 6e 96 3a 01 bb ec ce d8 d5 00 00 00 00 80 02 .n:.....
0030 20 00 85 da 00 00 02 04 05 b4 01 03 03 02 01 01 .....
0040 04 02 ..
```

File: "C:\Users\arch\Desktop\soru2.pcap" 62... Packets: 381 · Displayed: 381 (100,0%) · Load time: 0:00.005

Genel bilgilendirme

Wireshark Aracını Tanıyalım

Zaman damgası formatını değiştirmek için



The image shows the Wireshark application window with the 'View' menu open. The 'Time Display Format' option is highlighted, and its submenu is displayed. The submenu lists various time display formats and their corresponding keyboard shortcuts. The 'Time of Day: 01:02:03.123456' option is highlighted in the submenu.

View Menu Options:

- ✓ Main Toolbar
- ✓ Filter Toolbar
- Wireless Toolbar
- ✓ Status Bar
- ✓ Packet List
- ✓ Packet Details
- ✓ Packet Bytes
- Time Display Format**
- Name Resolution
- ✓ Colorize Packet List
- ✓ Auto Scroll in Live Capture
- Zoom In (Ctrl++)
- Zoom Out (Ctrl+-)
- Normal Size (Ctrl+=)
- Resize All Columns (Shift+Ctrl+R)
- Displayed Columns

Time Display Format Submenu Options:

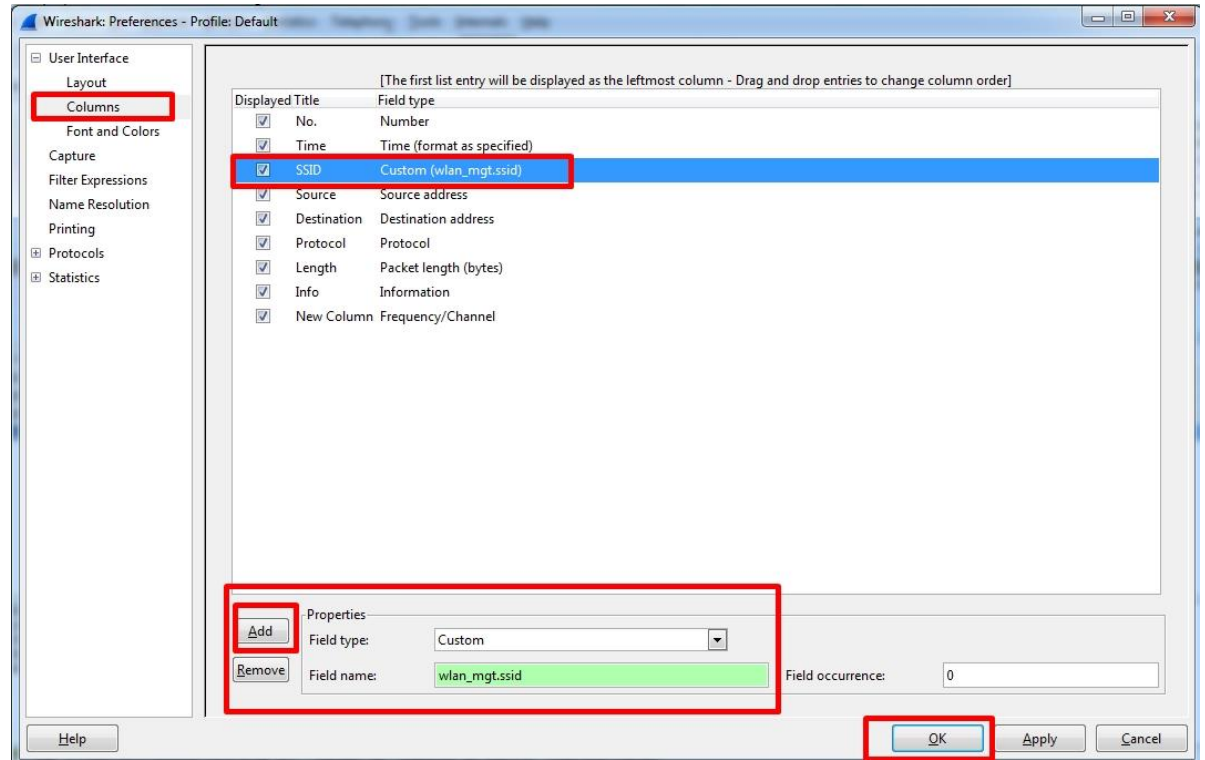
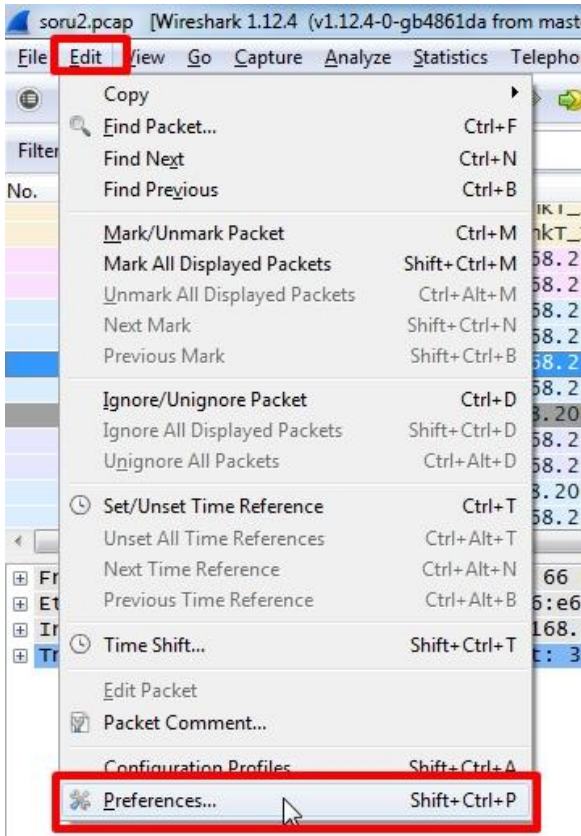
- Date and Time of Day: 1970-01-01 01:02:03.123456 (Ctrl+Alt+1)
- Date (with day of year) and Time of Day: 1970/001 01:02:03.123456
- Time of Day: 01:02:03.123456 (Ctrl+Alt+2)**
- Seconds Since Epoch (1970-01-01): 1234567890.123456 (Ctrl+Alt+3)
- Seconds Since Beginning of Capture: 123.123456 (Ctrl+Alt+4)
- Seconds Since Previous Captured Packet: 1.123456 (Ctrl+Alt+5)
- Seconds Since Previous Displayed Packet: 1.123456 (Ctrl+Alt+6)
- UTC Date and Time of Day: 1970-01-01 01:02:03.123456 (Ctrl+Alt+7)
- UTC Date (with day of year) and Time of Day: 1970/001 01:02:03.123456
- UTC Time of Day: 01:02:03.123456 (Ctrl+Alt+7)

Packet List Table:

No.	Destination	Protocol	Length	Info
6.80	216.58.208.110	TCP	66	38458→443
6.80	216.58.208.110	QUIC	1392	CID: 15465
8.110	192.168.2.80	TCP	66	443→38458
8.80	216.58.208.110	TCP	54	38458→443
8.80	216.58.208.110	TLSv1.2	273	Client Hello

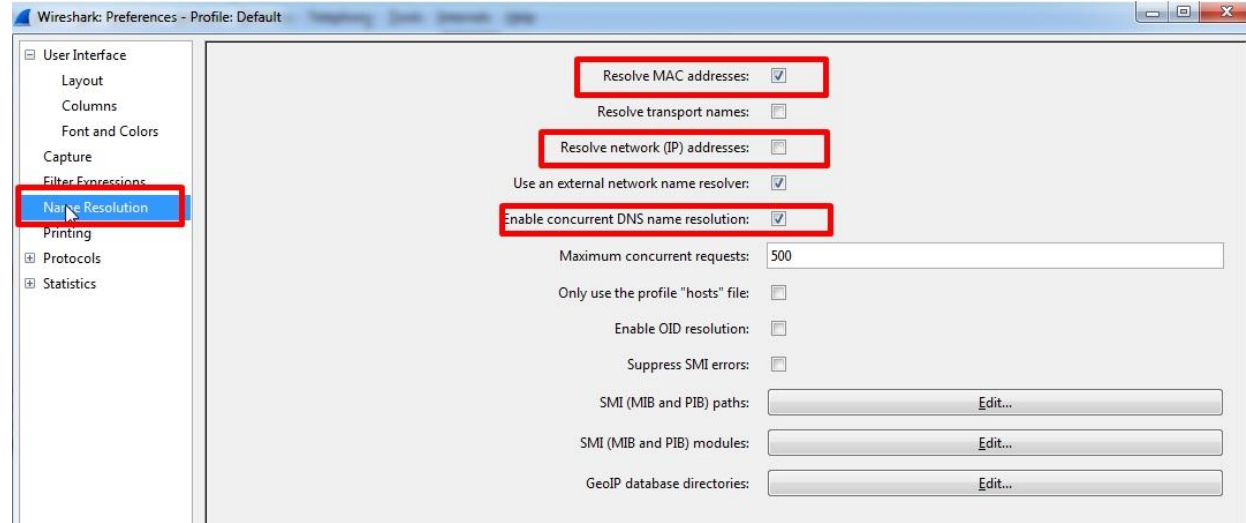
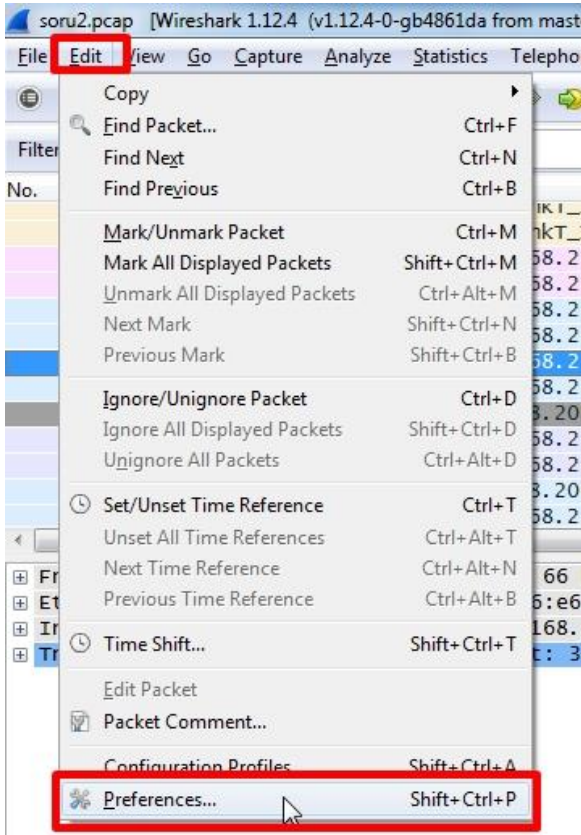
Wireshark Aracını Tanıyalım

Yeni bir kolon eklemek için



Wireshark Aracını Tanıyalım

Adres çözümlemelerini aktifleştirmek



Analiz sırasında MAC adresi ve IP adresi gibi bilgiler için adres çözümleme özelliğini aktif edebiliriz.

Wireshark Aracını Tanıyalım

Yakalanan paketler ile ilgili özet bilgilere erişmek

The screenshot shows the Wireshark interface with the Statistics menu open. The 'Summary' option is highlighted. The Summary pane on the right displays file, time, capture, and display statistics.

File

- Name: C:\Users\arch\Desktop\soru2.pcap
- Length: 62220 bytes
- Format: Wireshark/tcpdump/... - pcap
- Encapsulation: Ethernet
- Packet size limit: 262144 bytes

Time

- First packet: 2015-12-02 02:40:44
- Last packet: 2015-12-02 02:42:54
- Elapsed: 00:02:10

Capture

Capture file comments:

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	262144 bytes

Display

Display filter: none
Ignored packets: 0 (0,000%)

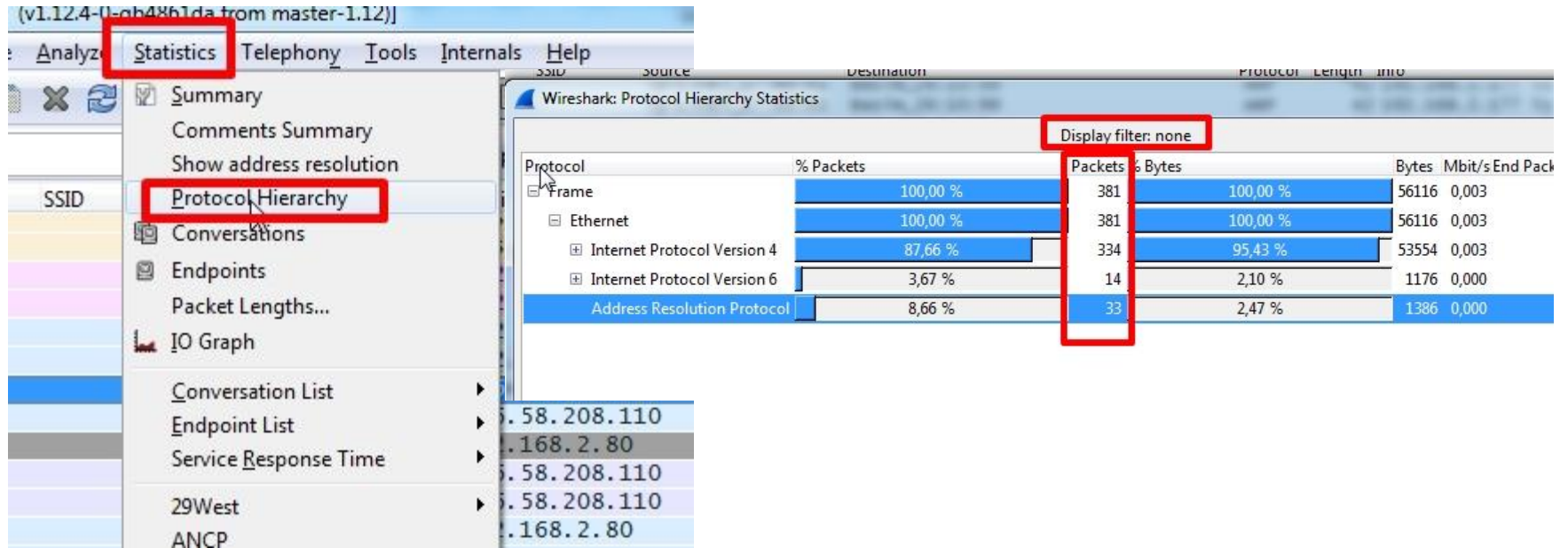
Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	381	381	100.000%	0	0,000%

Between first and last packet 130,069 sec

Avg. packets/sec	2,929
Avg. packet size	147 bytes
Bytes	56116
Avg. bytes/sec	431,433
Avg. MBit/sec	0,003

Wireshark Aracını Tanıyalım

Yakaladığımız paketlerin protokolleri hakkında genel bilgiler almak için



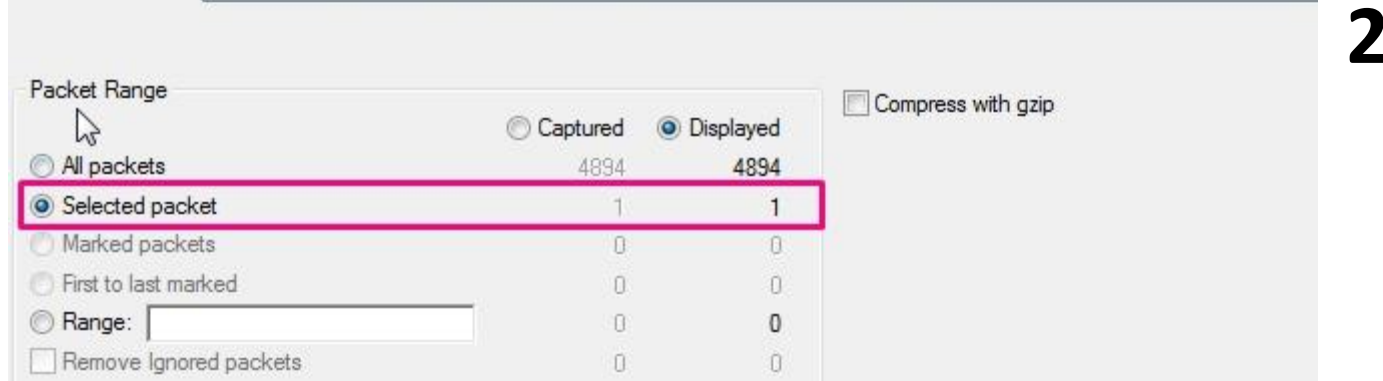
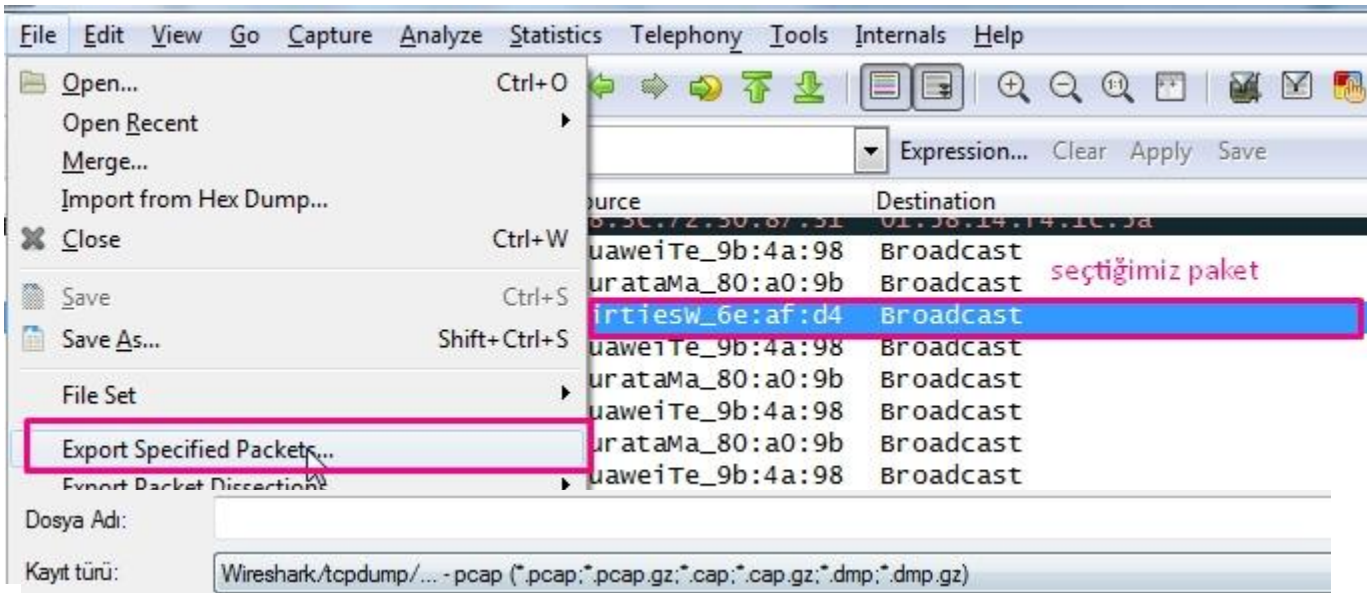
The image shows the Wireshark Protocol Hierarchy Statistics window. The 'Statistics' menu is open, and 'Protocol Hierarchy' is selected. The window displays a table of protocol statistics. The table has columns for Protocol, % Packets, Packets, % Bytes, Bytes, and Mbit/s End Pack. The data is as follows:

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s End Pack
Frame	100,00 %	381	100,00 %	56116	0,003
Ethernet	100,00 %	381	100,00 %	56116	0,003
Internet Protocol Version 4	87,66 %	334	95,43 %	53554	0,003
Internet Protocol Version 6	3,67 %	14	2,10 %	1176	0,000
Address Resolution Protocol	8,66 %	33	2,47 %	1386	0,000

The 'Display filter: none' button is also visible in the top right corner of the window.

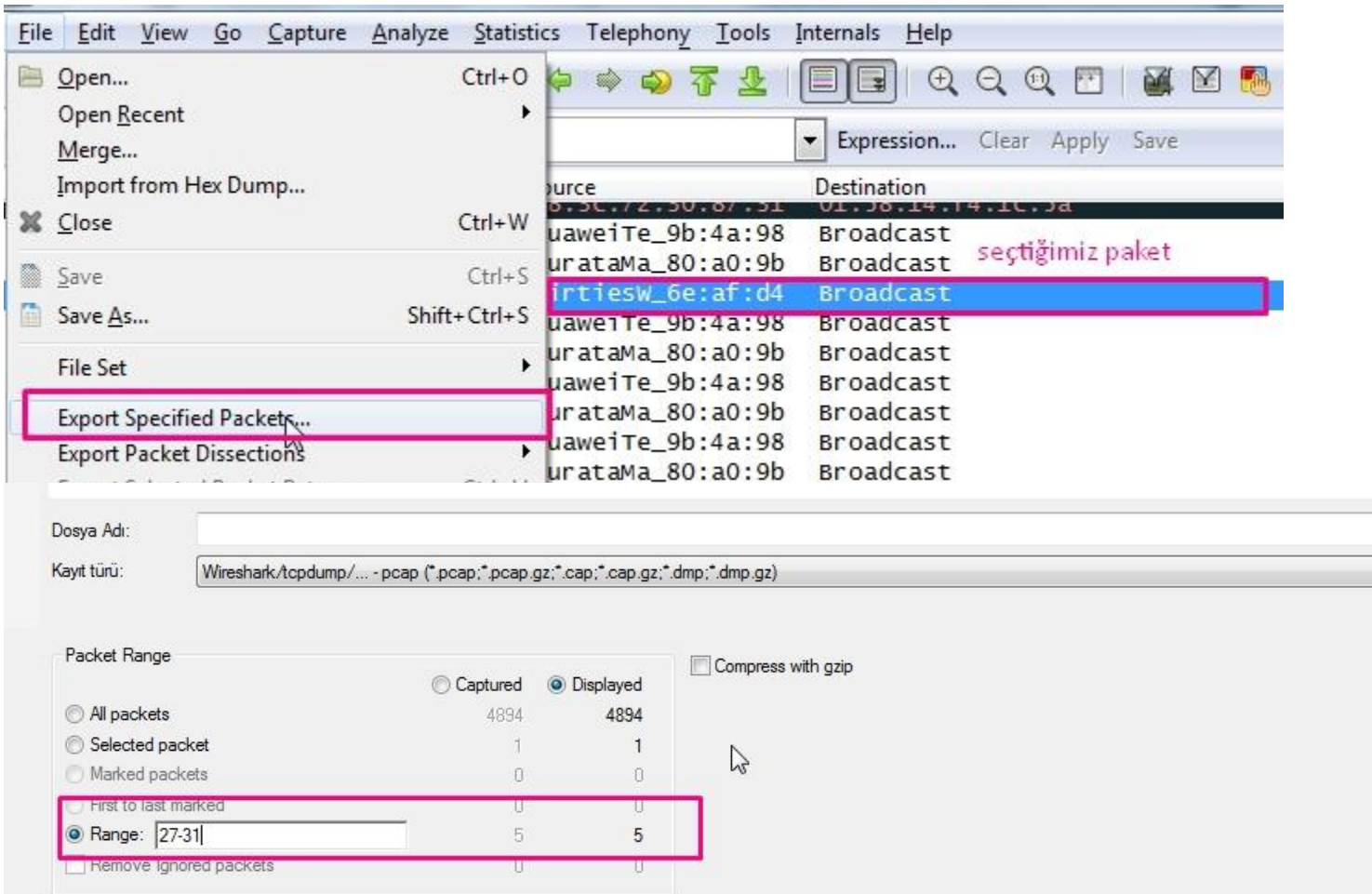
Wireshark Aracını Tanıyalım

Yakaladığımız paketlerden sadece bir tanesini incelemek için export etmek istiyorsak



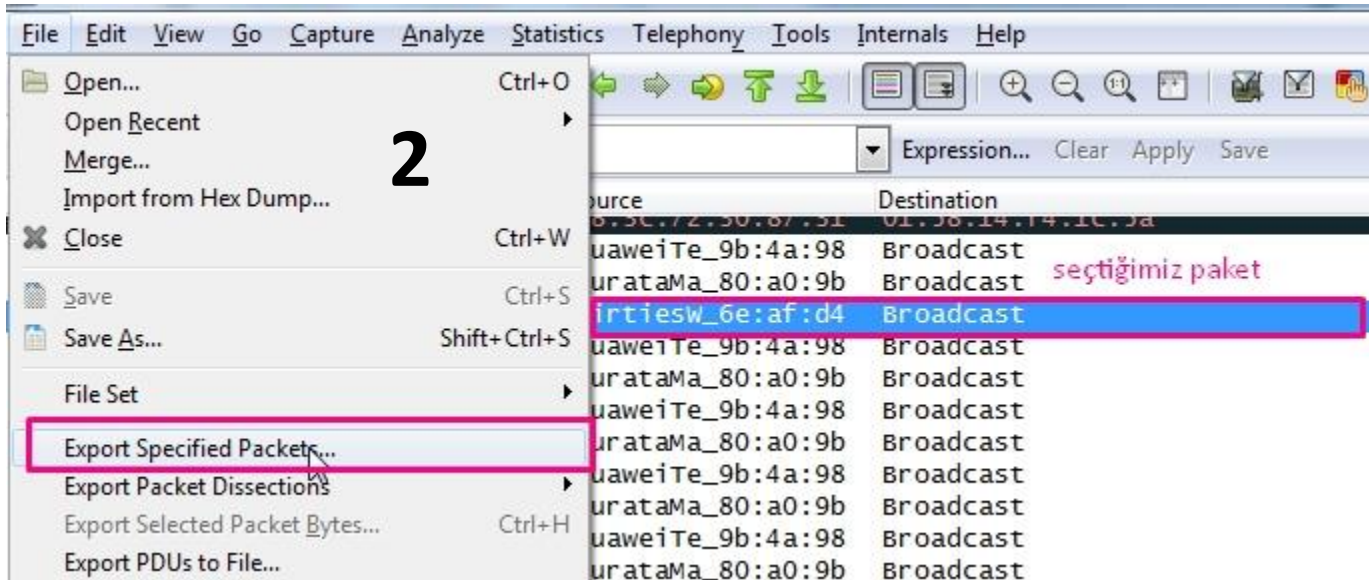
Wireshark Aracını Tanıyalım

Yakaladığımız paketlerden sadece **belli aralıkta** paketi incelemek için export etmek istiyorsak



Wireshark Aracını Tanıyalım

Yakaladığımız paketler arasından istediğimiz paketleri seçip incelemek için export etmek istiyorsak



Kullanışlı Wireshark Filtreleri

Kablosuz ağ analizi aşamasında kullanabileceğimiz wireshark filtreleri

Managment Frame

wlan.fc.type == 0

Data Frame

wlan.fc.type == 2

Control Frame

wlan.fc.type == 1

Beacon Frame

wlan.fc.subtype == 8

Probe Request

wlan.fc.subtype == 4

Probe Response

wlan.fc.subtype == 5

De-Authentication Packet

wlan.fc.subtype == 12

Only Beacon Frame

wlan.fc.subtype == 8 and
!(wlan.fc.type_subtype == 36)

Only Data and not NULL Data

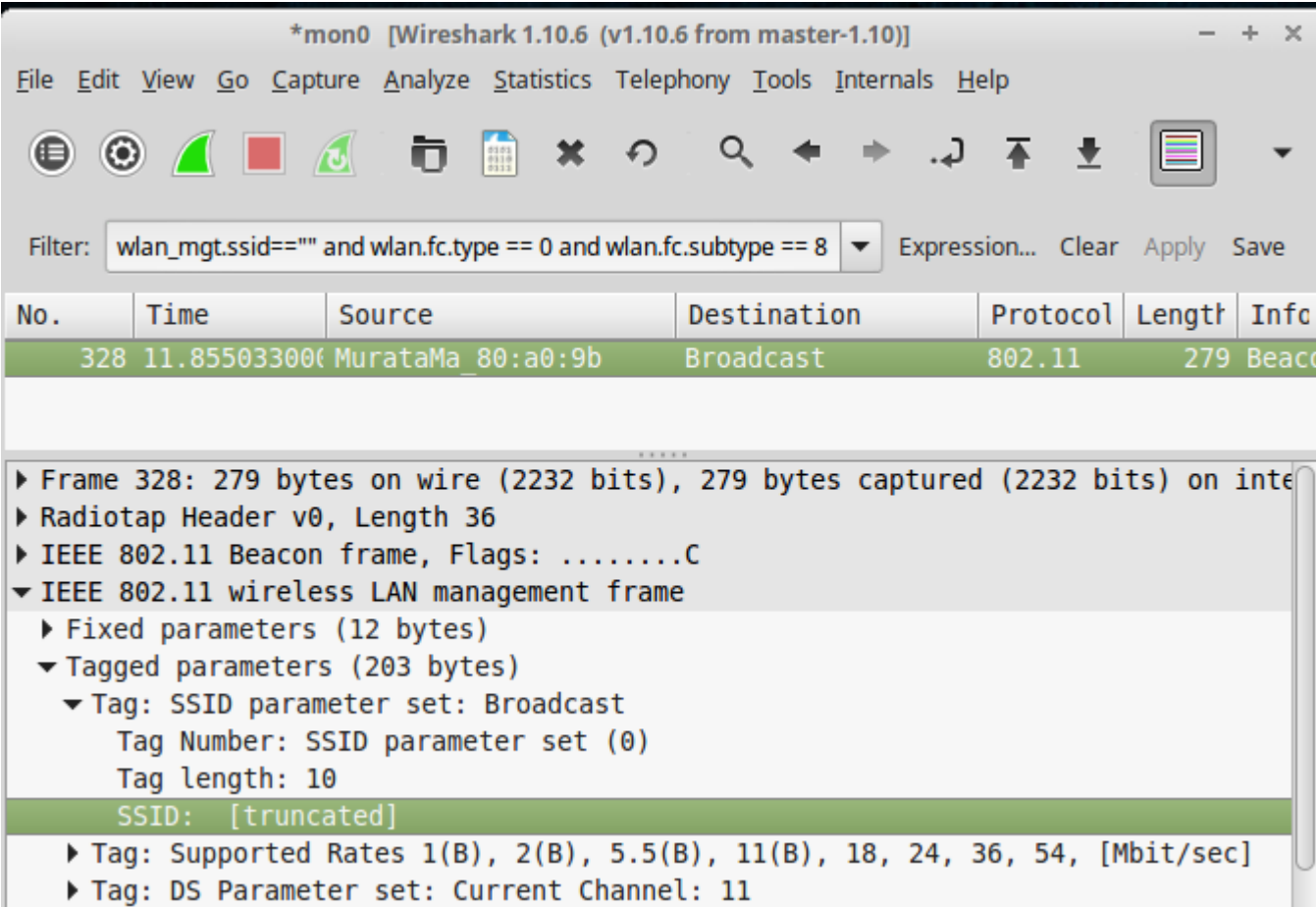
wlan.fc.subtype == 2 and
!(wlan.fc.type_subtype == 36)

Kullanışlı Wireshark Filtreleri- Uygulamalar

- Wireshark ile şifresiz kablosuz ağları tespit etmek
- Wireshark ile WEP şifrelemesi kullanan ağları tespit etmek
- Wireshark ile kablosuz ağların sinyal gücünü analiz etmek
- Wireshark ile kanal numarasına göre filtrelemeler yapmak
- Wireshark ile WPS destekli kablosuz ağları bulmak
- Wireshark ile sahte kablosuz ağları tespit etmek
- Wireshark ile WPA/WPA2 tip ağları filtrelemek
- Wireshark ile WEP trafiklerini decrypt etmek **



Wireshark ile Gizli SSID Yayınları Tespit Etmek



The image shows the Wireshark 1.10.6 interface with the following components:

- Filter:** `wlan_mgt.ssid=="" and wlan.fc.type == 0 and wlan.fc.subtype == 8`
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
328	11.855033006	MurataMa_80:a0:9b	Broadcast	802.11	279	Beacon

- Packet Details:**

 - ▶ Frame 328: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits) on interface
 - ▶ Radiotap Header v0, Length 36
 - ▶ IEEE 802.11 Beacon frame, Flags:C
 - ▼ IEEE 802.11 wireless LAN management frame
 - ▶ Fixed parameters (12 bytes)
 - ▼ Tagged parameters (203 bytes)
 - ▼ Tag: SSID parameter set: Broadcast
 - Tag Number: SSID parameter set (0)
 - Tag length: 10
 - SSID: [truncated]
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
 - ▶ Tag: DS Parameter set: Current Channel: 11

Wireshark ile Sadece Bir AP Cihazından Çıkan Paketleri Analiz Etmek

Filter: `wlan.bssid == 18:28:61:6e:af:d4` Expression... Clear Apply Save

No.	SSID	Time	Source	Destination	Protocol	Length	Info
	Aman_OBBU	0.102332	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame
	Aman_OBBU	0.357627	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame
	Aman_OBBU	0.614930	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame
	Aman_OBBU	0.869629	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame
	Aman_OBBU	1.125604	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame
	Aman_OBBU	1.381656	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame
	Aman_OBBU	1.637532	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame
	Aman_OBBU	1.893558	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame

Frame 47: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits)

Radiotap Header v0, Length 26

IEEE 802.11 Beacon frame, Flags:C

Type/Subtype: Beacon frame (0x08)

Frame Control Field: 0x8000

.000 0000 0000 0000 = Duration: 0 microseconds

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

Wireshark ile Kanal Numarasına Göre Analiz Yapmak

Filter: wlan_mgt.ds.current_channel == 13

No.	SSID	Time	Source	Destination	Protocol
	dejavu-2	94.559050000	Tp-LinkT_c1:07:e8	Broadcast	802.11
	dejavu-2	94.661628000	Tp-LinkT_c1:07:e8	Broadcast	802.11
	dejavu-2	105.822732000	Tp-LinkT_c1:07:e8	Broadcast	802.11
	dejavu-2	105.925079000	Tp-LinkT_c1:07:e8	Broadcast	802.11
	dejavu-2	109.099756000	Tp-LinkT_c1:07:e8	Broadcast	802.11
	dejavu-2	109.201798000	Tp-LinkT_c1:07:e8	Broadcast	802.11
	dejavu-2	109.304171000	Tp-LinkT_c1:07:e8	Broadcast	802.11

.....

- + Fixed parameters (12 bytes)
- Tagged parameters (94 bytes)
 - + Tag: SSID parameter set: dejavu-2
 - + Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 12, 24, 36, [Mbit/sec]
 - Tag: DS Parameter set: Current Channel: 13
 - Tag Number: DS Parameter set (3)
 - Tag length: 1

Current Channel: 13

.....

- Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmaps

.....

0000	00 00 1a 00 2f 48 00 00	e0 9b 0e 00 00 00 00 00H..
0010	10 02 a3 09 c0 00 a9 00	00 00 80 00 00 00 ff ff
0020	ff ff ff ff 54 e6 fc c1	07 e8 54 e6 fc c1 07 e8T... ..T.....
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

Wireshark ile Sinyal Gücüne Göre Analiz Yapmak

Filter: radiotap.dbm_antsignal >= -88

No.	SSID	Time	Source	Destination	Proto
		341.83165700			802.11
	merkoterm	341.84887800	5e:f4:ab:38:57:04	Broadcast	802.11
		341.94004900			802.11
	merkoterm	341.95189300	5e:f4:ab:38:57:04	Broadcast	802.11
		342.91866800	AirtiesW_72:50:70	IntelCor_e3:92:07	802.11
		342.91909000	IntelCor_e3:92:07	AirtiesW_72:50:70	802.11
		342.92053500	84:11:9e:71:2d:3b	Broadcast	802.11
		342.92215600	IntelCor_e3:92:07	AirtiesW_72:50:70	802.11

Channel type: 802.11g (pure-g) (0x00c0)

SSI Signal: -69 dBm

Antenna: 0

RX flags: 0x0000

IEEE 802.11 Beacon frame, Flags:C

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Tagged parameters (335 bytes)

0010 10 02 8a 09 c0 00 bb 00 00 00 80 00 00 00 ff ff
0020 ff ff ff ff 5e f4 ab 38 57 04 5e f4 ab 38 57 04^..8 W.^..8W.
0030 20 42 4a 71 57 20 04 00 00 00 64 00 11 0c 00 09 R1nW d

Wireshark ile WPS Destekli Ağları Analiz Etmek

Filter: **wlan_mgt.wfa.ie.type == 0x04** Expression... Clear Apply Save

No.	SSID	Time	Source	Destination	Protocol
	NazliToraman	340.9311030	Tp-LinkT_39:c6:e0	Broadcast	802.11
	merkoterm	341.8488780	5e:f4:ab:38:57:04	Broadcast	802.11
	merkoterm	341.9518930	5e:f4:ab:38:57:04	Broadcast	802.11
	ARS_CAFE	344.8192560	e8:37:7a:5c:84:13	Broadcast	802.11
	REYHAN	344.8434840	ZyxelCom_f9:48:b1	Broadcast	802.11
	REYHAN	345.0482790	ZyxelCom_f9:48:b1	Broadcast	802.11
	SineK	345.9684780	HuaweiTe_89:2a:e7	9b:bb:f4:ff:ff:ff	802.11

Tag: Overlapping BSS Scan Parameters: Undecoded

- Tag: Extended Capabilities (8 octets)
- Tag: Vendor Specific: Microsof: WPS
 - Tag Number: Vendor Specific (221)
 - Tag length: 24
 - OUI: 00-50-f2 (Microsof)
 - Vendor Specific OUI Type: 4
 - Type: WPS (0x04)

Version: 0x10

00a0 00 3d 16 01 08 04 00 00 00 00 00 00 00 00 00 .=.
00b0 00 00 00 00 00 00 00 00 00 4a 0e 14 00 0a 00 2c J ,
00c0 01 c8 00 14 00 05 00 19 00 7f 08 05 00 00 00 00
00d0 00 00 40 dd 18 00 50 f2 04 10 4a 00 01 10 10 44

Wireshark ile OPEN Ağları Analiz Etmek

Filter: wlan_mgt.fixed.capabilities.privacy == 0

No.	SSID	Time	Source	Destination	Protocol	Length
		104.74650100	Tp-LinkT_f8:15:1b	Broadcast	802.11	96
	openetwotk	105.83315600	MurataMa_80:a0:9b	Broadcast	802.11	247
	datanet_sehri gul	105.88729900	Ubiquiti_66:f4:07	Broadcast	802.11	329
	openetwotk	105.93713900	MurataMa_80:a0:9b	Broadcast	802.11	247
	datanet_sehri gul	105.98970900	Ubiquiti_66:f4:07	Broadcast	802.11	329
	openetwotk	106.03803300	MurataMa_80:a0:9b	Broadcast	802.11	247
		106.94973200	08:10:78:a6:d3:08	Broadcast	802.11	316
	openetwotk	109.10987800	MurataMa_80:a0:9b	Broadcast	802.11	247

.... = IBSS status: Transmitter belongs to a BSS
....0. 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
....0 = Privacy: AP/STA cannot support WEP
....0. = Short Preamble: Not Allowed
....0. = PBCC: Not Allowed
....0... = Channel Agility: Not in use
....0 = Spectrum Management: Not Implemented
....1.. = Short Slot Time: In use

0030 e0 15 83 71 f2 01 00 00 00 00 64 00 01 04 00 0a ...q.... ..d....
0040 6f 70 65 6e 65 74 77 6f 74 6b 01 08 82 84 8b 96 openetwo tk.....
0050 24 30 48 6c 03 01 0b 05 04 01 02 00 00 2a 01 00 \$OHL.....*..
0060 2f 01 00 32 04 0c 12 18 60 2d 1a 2d 10 17 ff 00 /..2....`-.....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Wireshark ile WPA Destekli Ağları Analiz Etmek

wlan_mgt.wfa.ie.wpa.version == 1 and !(wlan_mgt.rsn.version == 1)

The image shows a Wireshark network traffic capture. A red box highlights the filter bar with the expression: `wlan_mgt.wfa.ie.wpa.version == 1 and !(wlan_mgt.rsn.version == 1)`. Below the filter bar is a table of captured packets. The table has columns: No., SSID, Time, Source, Destination, and Protocol. The packets are filtered to show only those with WPA version 1 and RSN version not equal to 1. The details pane shows the selected packet's structure, including the Vendor Specific: Microsoft: WPA Information Element and the Multicast Cipher Suite: 00-50-f2 (Microsoft) AES (CCM).

No.	SSID	Time	Source	Destination	Protocol
	BUZZ YAZILIM SINEK	81.610376000	TendaTec_fb:b4:70	Broadcast	802.11
	BUZZ YAZILIM SINEK	81.712579000	TendaTec_fb:b4:70	Broadcast	802.11
	REYHAN	81.890375000	ZyxeCom_fb:48:b1	Broadcast	802.11
	BUZZ YAZILIM SINEK	81.917533000	TendaTec_fb:b4:70	Broadcast	802.11
	BUZZ YAZILIM SINEK	82.122246000	TendaTec_fb:b4:70	Broadcast	802.11
	BUZZ YAZILIM SINEK	82.329015000	TendaTec_fb:b4:70	Broadcast	802.11
	BUZZ YAZILIM SINEK	82.346948000	TendaTec_fb:b4:70	64:bc:0c:0f:b7:f7	802.11
	BUZZ YAZILIM SINEK	82.356289000	TendaTec_fb:b4:70	64:bc:0c:0f:b7:f7	802.11

Tag: Vendor Specific: Microsoft: WPA Information Element
Tag Number: Vendor Specific (221)
Tag length: 24
OUI: 00-50-f2 (Microsoft)
Vendor Specific OUI Type: 1
Type: WPA Information Element (0x01)
WPA Version: 1
Multicast Cipher Suite: 00-50-f2 (Microsoft) AES (CCM)

0050 45 4b 01 08 82 84 8b 96 24 30 48 6c 03 01 01 05 EK..... \$OHl....
0060 04 02 03 00 00 2a 01 04 2f 01 04 32 04 0c 12 18*.. /..2....
0070 60 2d 1a 7e 18 1b ff 00 00 00 00 00 00 00 00 00 ~.~.....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 3d 16 01=..

Wireshark ile WPA2 Destekli Ağları Analiz Etmek

!(wlan_mgt.wfa.ie.wpa.version == 1) and (wlan_mgt.rsn.version == 1)

Filter: (wlan_mgt.wfa.ie.wpa.version == 1) and (wlan_mgt.rsn.version == 1) Expression... Clear Apply Save

No.	SSID	Time	Source	Destination	Protocol
	TTNET_ZyXEL_NMMN	126.03995700	e8:37:7a:3d:0f:e3	Broadcast	802.11
		133.94013100	Tp-LinkT_56:22:d8	Broadcast	802.11
	kiraz	133.96953400	Zte_70:1e:34	Broadcast	802.11
	kiraz	134.07237100	Zte_70:1e:34	Broadcast	802.11
		134.14505000	Tp-LinkT_56:22:d8	Broadcast	802.11
	kiraz	134.17431600	Zte_70:1e:34	Broadcast	802.11
	SSID	140.54389200	90:ef:68:0d:18:5f	Azurewav_62:17:c9	802.11

Tag: Vendor Specific: Microsof: WPS
Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
Tag: ERP Information
Tag: RSN Information
Tag Number: RSN Information (48)
Tag length: 20
RSN Version: 1
Group Cipher Suite: 00-0f-ac (Ieee8021) TKIP

0050 01 06 32 04 0c 18 30 60 07 06 54 52 20 01 0d 14 ..2...0` ..TR ...
0060 33 08 20 01 02 03 04 05 06 07 33 08 21 05 06 07 3.3.!...
0070 08 09 0a 0b dd 27 00 50 f2 04 10 4a 00 01 10 10'.P ...J....
0080 44 00 01 02 10 47 00 10 bc 32 9e 00 1d d8 11 b2 D....G.. .2.....
0090 86 01 9c d2 4b 70 1e 34 10 3c 00 01 00 05 04 00Kn.4 .<.....

Wireshark ile Analiz Yaparken Malformed Paketlerden Kurtulmak

Filter: **!(expert.group == 0x07000000)** Expression... Clear Apply Save

No.	SSID	Time	Source	Destination	Protocol	Length	Info
	TTNET_TP-LINK_FDA2	560.3222980	Tp-LinkT_38:fd:a2	Broadcast	802.11	319	Beacon frame,
	TTNET_TP-LINK_FDA2	560.6293660	Tp-LinkT_38:fd:a2	Broadcast	802.11	319	Beacon frame,
	TTNET_TP-LINK_FDA2	560.7317860	Tp-LinkT_38:fd:a2	Broadcast	802.11	319	Beacon frame,
		560.8503570			802.11	49	QoS Data[Malfo
	TTNET_TP-LINK_FDA2	561.0389920	Tp-LinkT_38:fd:a2	Broadcast	802.11	319	Beacon frame,
		561.2729270			802.11	51	QoS Data[Malfo
	TTNET_TP-LINK_FDA2	561.7556850	Tp-LinkT_38:fd:a2	Broadcast	802.11	319	Beacon frame,
	TTNET_TP-LINK_FDA2	561.9500000	Tp-LinkT_38:fd:a2	Broadcast	802.11	319	Beacon frame,

⊕ Tag: ERP Information

⊕ Tag: RSN Information

⊖ Tag: Reserved (182)

[Malformed Packet: IEEE 802.11]

[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]

[Message: Malformed Packet (Exception occurred)]

[Severity level: Error]

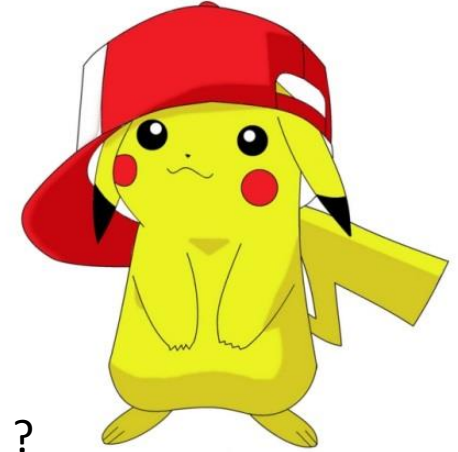
Wireshark ile Analizde Channel Hopping Bash Script

Temelde 'iwconfig' komutunu kullanarak ağ kartını yapılandırmayı amaçlar.

```
root@WifiAttacks:~/wifiAnaliz# iwconfig --help
Usage: iwconfig [interface]
        interface essid {NNN|any|on|off}
        interface mode {managed|ad-hoc|master|...}
        interface freq N.NNN[k|M|G]
        interface channel N
        interface bit {N[k|M|G]|auto|fixed}
        interface rate {N[k|M|G]|auto|fixed}
        interface enc {NNNN-NNNN|off}
        interface key {NNNN-NNNN|off}
        interface power {period N|timeout N|saving N|off}
        interface nickname NNN
        interface nwid {NN|on|off}
        interface ap {N|off|auto}
        interface txpower {N|N dBm|off|auto}
```

```
1  #!/bin/bash
2  echo "Channel Hopping Started"
3  while true
4  do
5      for i in {1..11}
6      do
7          iwconfig wlan0mon channel $i
8          sleep 5
9      done
10 done
```

Wireshark - Sıkça Sorulan Sorular



- Wireshark ile saldırı tespiti yapılabilir mi ?
- Wireshark ile kablosuz ağ şifresi kırabilir mi ?
- Kismet ile yakaladığım dataları analiz edebilir miyim ?
- Netstumbler ile yakaladığım paketleri analiz edebilir miyim ?
- Wireless analiz için en iyi kart hangisi ?
- Bir AP cihazına bağlı olduğum sürece, Wireshark ile sniff yapabilir miyim ?
- Wireshark ile 802.11a/b/g standartlarını destekleyen cihazlar sniff edilebilir mi ?
- Kablosuz ağın sinyal gücünü wireshark ile görebilir miyim ?