



WIFI ATTACK AND DEFENSE

Besim ALTINOK
Security Engineer

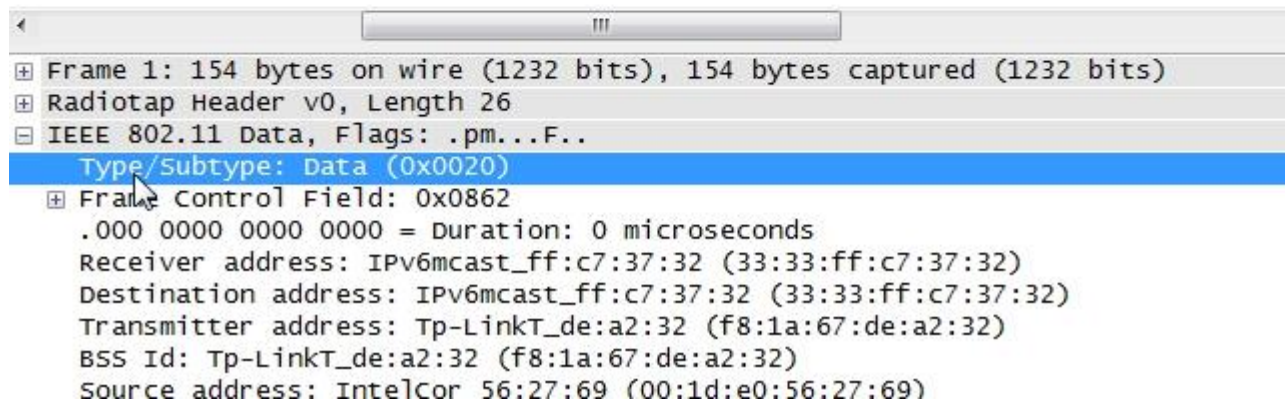
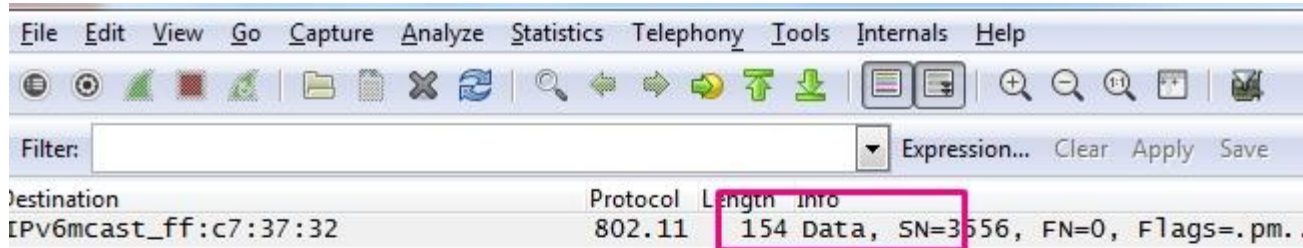
Önemli Kablosuz Ağ Paketleri



1. Data Frame
2. Control Frame
3. Management

Data Frame

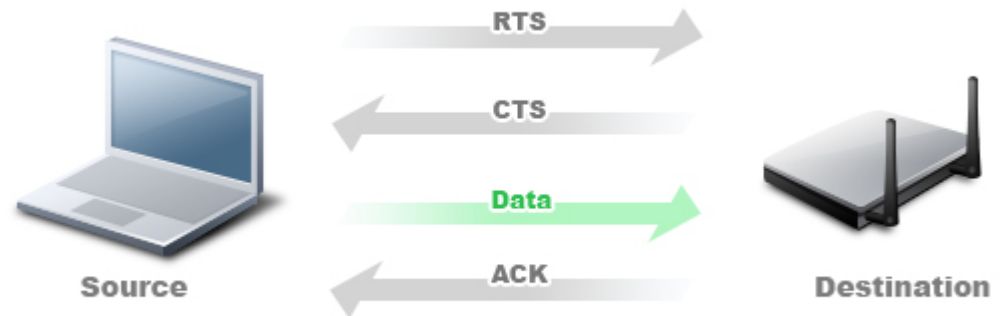
Kablosuz ağ üzerindeki dataların taşınmasında görev alır.



Control Frame

- İstemci ile AP cihazı arasında datanın uygun bir şekilde takas edilmesinden sorumludur.

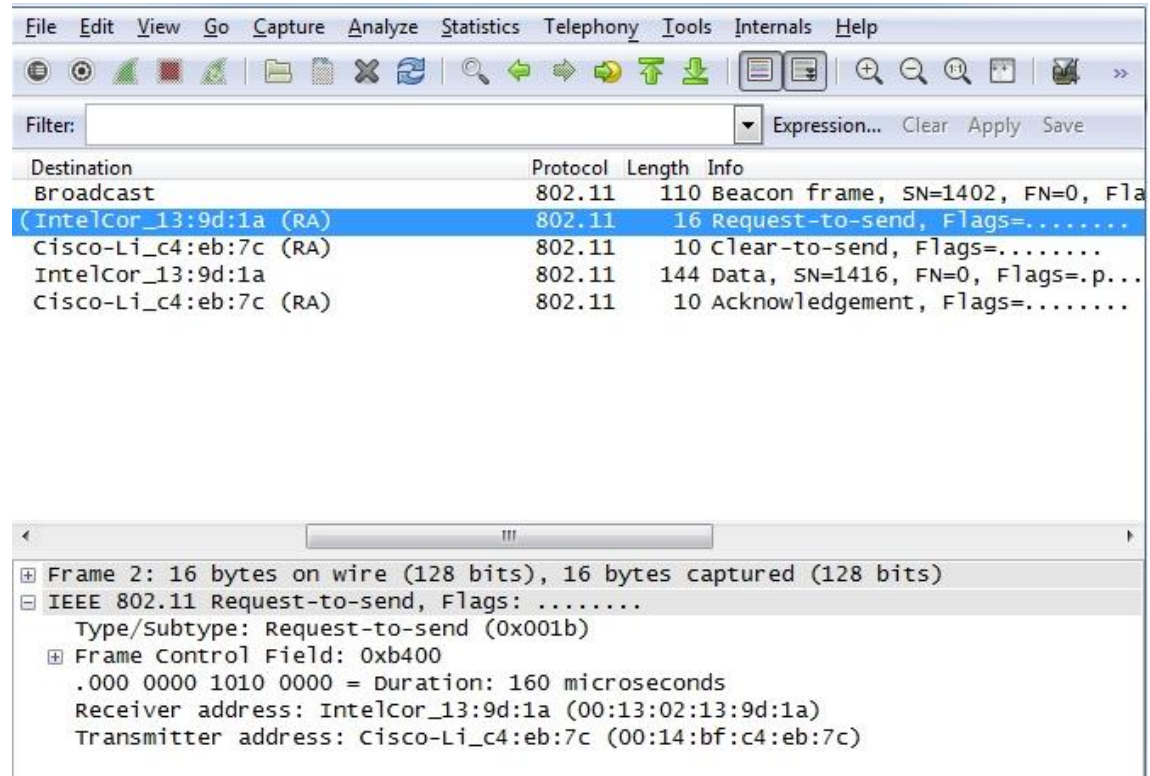
- ☐ Request to Send (RTS)
- ☐ Clear to Send (CTS)
- ☐ Acknowledgement (ACK)



Control Frame

- İstemci ile AP cihazı arasında datanın uygun bir şekilde takas edilmesinden sorumludur.

- ☐ Request to Send (RTS)
- ☐ Clear to Send (CTS)
- ☐ Acknowledgement (ACK)



Management Frame Yapısı

Ağ cihazı ile istemci arasındaki bağlantının sürdürülmesi ile ilgilidir.

Type Field	Subtype Field	Description
0	0	Association Request
0	1	Association Response
0	2	Re-association Request
0	3	Re-association Response
0	4	Probe Request
0	5	Probe Response
0	6	Measurement Pilot
0	7	Reserved
0	8	Beacon
0	9	ATIM
0	10	Disassociation
0	11	Authentication
0	12	Deauthentication
0	13	Action
0	14	Action No ACK
0	15	Reserved

Management Frame Yapısı

Ağ cihazı ile istemci arasındaki bağlantının sürdürülmesi ile ilgilidir.

Filter: wlan.fc.type == 0 Management Frames Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
4141	11.305604000	HuaweiTe_9b:4a:98	Broadcast	802.11	352	Beacon frame, SN=1669, FI
4144	11.313983000	AirtiesW_6e:af:d4	Broadcast	802.11	311	Beacon frame, SN=4043, FI
4161	11.337948000			802.11	40	Action[Malformed Packet]
4254	11.390263000	AirtiesW_88:06:11	Broadcast	802.11	182	Beacon frame, SN=1437, FI
4255	11.394230000			802.11	40	Association Response[Mal
4256	11.395351000			802.11	40	Reassociation Request[Ma
4260	11.407965000	HuaweiTe_9b:4a:98	Broadcast	802.11	352	Beacon frame, SN=1670, FI
4264	11.416950000			802.11	40	Deauthentication[Malform
4369	11.445126000			802.11	40	Reassociation Request[Ma
4375	11.449752000	Azurewav_94:d0:65	AirtiesW_6e:af:d4	802.11	63	Action, SN=3651, FN=0, F
4377	11.450622000	AirtiesW_6e:af:d4	Azurewav_94:d0:65	802.11	63	Action, SN=4044, FN=0, F
4381	11.457594000			802.11	40	Action No Ack[Malformed I
4382	11.460707000			802.11	40	Probe Response[Malformed
4390	11.481849000			802.11	40	Association Response[Mal
4392	11.487585000			802.11	40	Disassociate[Malformed P

Önemli Management Frame Alanları ve İçerikleri

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

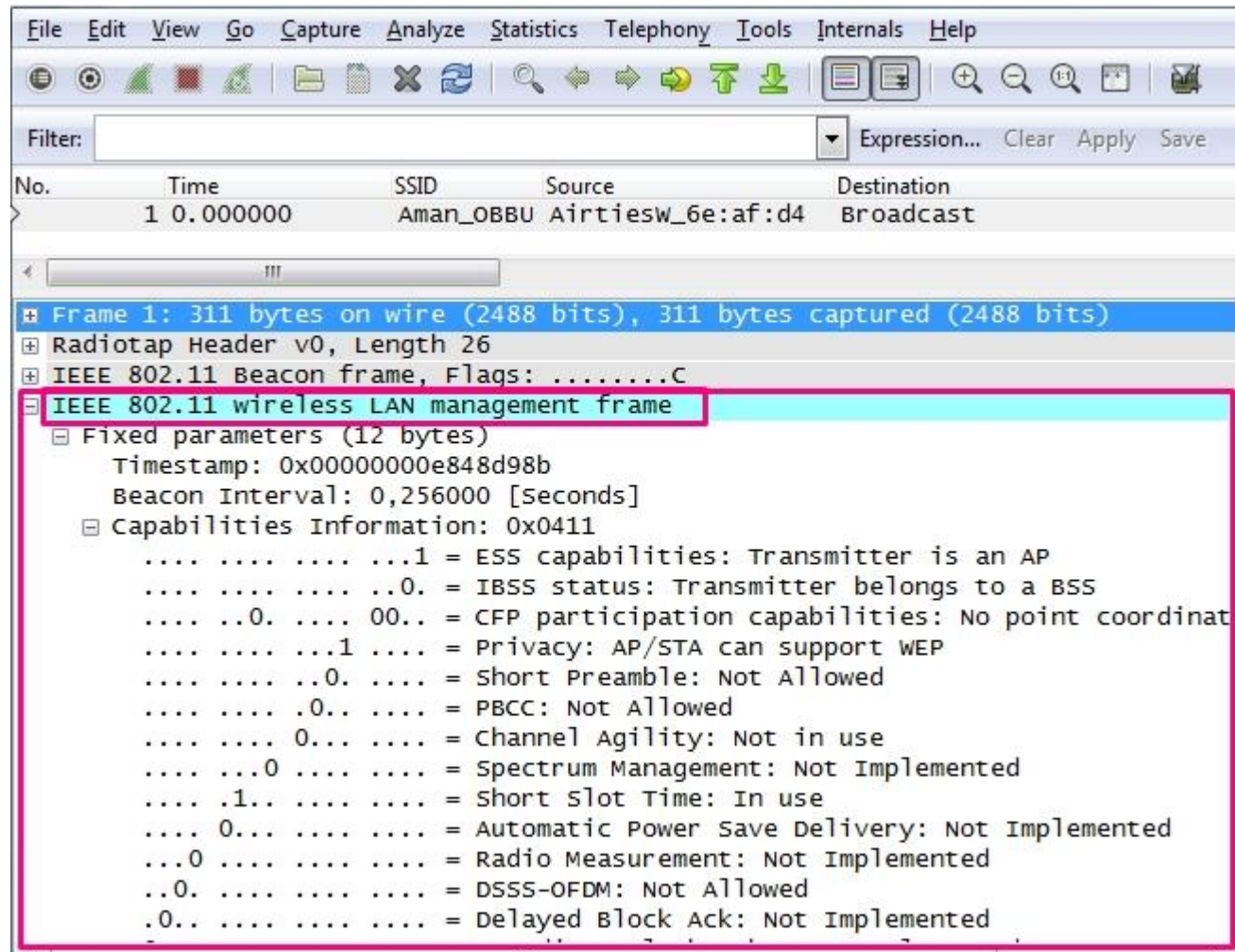
Filter: Expression... Clear Apply Save

No.	Time	SSID	Source	Destination
1	0.000000	Aman_OBBU	Airtiesw_6e:af:d4	Broadcast

IEEE 802.11 Beacon frame, Flags:C

- Type/Subtype: Beacon frame (0x0008)
- Frame Control Field: 0x8000
 -00 = Version: 0
 - 00.. = Type: Management frame (0)
 - 1000 = Subtype: 8
- Flags: 0x00
 -00 = DS status: Not leaving DS or network is operating in AD-HOC
 -0.. = More Fragments: This is the last fragment
 - 0... = Retry: Frame is not being retransmitted
 - ...0 = PWR MGT: STA will stay up
 - ..0. = More Data: No data buffered
 - .0.. = Protected flag: Data is not protected
 - 0... = Order flag: Not strictly ordered
- .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)
- Transmitter address: Airtiesw_6e:af:d4 (18:28:61:6e:af:d4)
- Source address: Airtiesw_6e:af:d4 (18:28:61:6e:af:d4)
- BSS Id: Airtiesw_6e:af:d4 (18:28:61:6e:af:d4)
- Fragment number: 0

Önemli Management Frame Alanları ve İçerikleri



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	SSID	Source	Destination
1	0.000000	Aman_OBBU	Airtiesw_6e:af:d4	Broadcast

Frame 1: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits)

- Radiotap Header v0, Length 26
- IEEE 802.11 Beacon frame, Flags:C
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters (12 bytes)
 - Timestamp: 0x00000000e848d98b
 - Beacon Interval: 0,256000 [Seconds]
 - Capabilities Information: 0x0411
 - ...1 = ESS capabilities: Transmitter is an AP
 - ...0. = IBSS status: Transmitter belongs to a BSS
 - ...0. 00.. = CFP participation capabilities: No point coordinat
 - ...1 = Privacy: AP/STA can 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
 - ...0... = Automatic Power Save Delivery: Not Implemented
 - ...0 = Radio Measurement: Not Implemented
 - ...0. = DSSS-OFDM: Not Allowed
 - ...0.. = Delayed Block Ack: Not Implemented

Önemli Management Frame Alanları ve İçerikleri

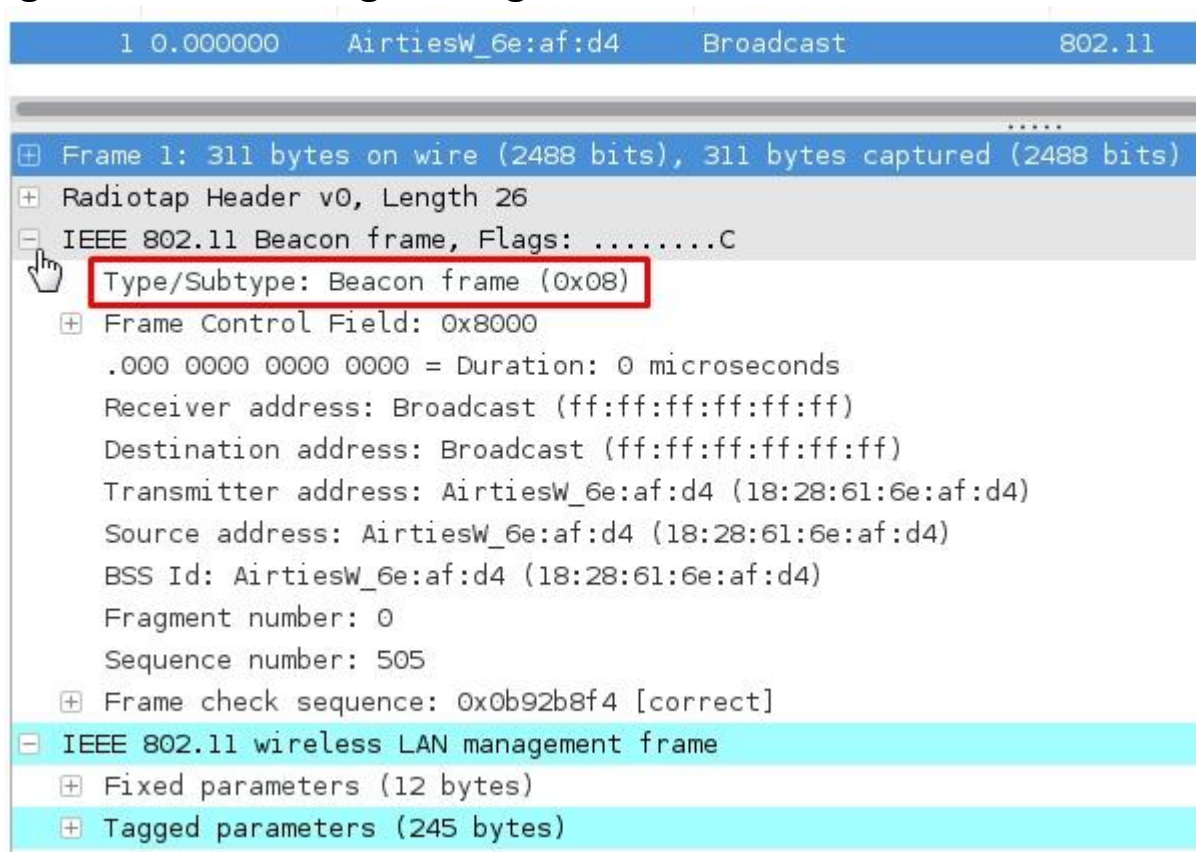
- **Timestamp Değeri**
 - Beacon ve Probe isteklerinde bulunur.
 - AP cihazının ne zaman aktif olduğunu gösterir.
 - İstemci kendi saatini ayarlamak için bu değeri kullanır.
- **Beacon Interval Değeri**
 - Beacon isteklerinin üretilme aralıklarını içerir.
- **Privacy Alanı**
 - Eğer bütün frameler için gizlilik gerekliyse bu alan set edilir.
 - Verileri koruma amaçlı kullanılan diğer gizlilik mekanizmaları **RSN** alanında ifade edilecektir.

Önemli Management Frame Alanları ve İçerikleri

- **Capability Information Alanı**
 - Buradaki değerler 0 ve 1 değerlerini almaktadır.
 - ESS: Paketin bir AP cihazından gelip gelmediğini işaret eder.
 - IBSS: Paketin bir Ad-Hoc Networkten gelip gelmediğini işaret eder.
- **QOS Alanı**
 - **QOS:** Ağ İletişimi Hizmet Kalitesi ([İngilizce](#) Quality of Service, kısaca QoS), Ağ üzerindeki uygulamaları önceliklendirerek zaman kaybını azaltmayı hedefleyen bir [ağ servisi](#)dir.
 - Bu alanın set edilmesi AP cihazının QoS servisini desteklediğini gösterir.

Beacon Frame Yapısı

Kablosuz ağ cihazları sürekli olarak içinde ismi(SSID) ve diğer bilgileri(frekans, tip, MAC vb.) barındıran Beacon Frame yayınlar. Böylece kullanıcılar yayın yapan AP cihazlarını görebilir ve buna göre bağlanabilir.



Probe Request Yapısı

AP cihazına bağlanmak amacı ile istemcinin gönderdiği bir pakettir.
Broadcast bir istektir.

The image shows a Wireshark packet capture interface. At the top, a packet list shows packet 1 at 0.000000 seconds, from Htc_85:b1:81 to Broadcast, with a length of 802.1. The packet details pane shows the following structure:

- Frame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bi)
- Radiotap Header v0, Length 26
- IEEE 802.11 Probe Request, Flags:C
 - Type/Subtype: Probe Request (0x04)
 - Frame Control Field: 0x4000
 - .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)
 - Transmitter address: Htc_85:b1:81 (e8:99:c4:85:b1:81)
 - Source address: Htc_85:b1:81 (e8:99:c4:85:b1:81)
 - BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
 - Fragment number: 0
 - Sequence number: 1645
- Frame check sequence: 0x6cd3f4fb [correct]
- IEEE 802.11 wireless LAN management frame
 - Tagged parameters (121 bytes)

Red boxes highlight the following fields: Type/Subtype: Probe Request (0x04), Destination address: Broadcast (ff:ff:ff:ff:ff:ff), and BSS Id: Broadcast (ff:ff:ff:ff:ff:ff). Red arrows point from these boxes to the text "Broadcast Yayın" on the right.

Probe Response Yapısı

Beacon Frame paket yapısına çok benzemektedir. Bunu daha rahat görebilmek açısından wireshark aracı ile Beacon Frame ve probe cevap paketleri incelenebilir.

Probe istekleri için dönülen cevaptır.

- **Probe Response**

No.	Time	Source	Destination	Protocol
1	0.000000	AirtiesW_6e:af:d4	Htc_85:b1:81	802.11

+	Frame 1: 438 bytes on wire (3504 bits), 438 bytes captured (3504 b
+	Radiotap Header v0, Length 26
-	IEEE 802.11 Probe Response, Flags:C
	Type/Subtype: Probe Response (0x05)
+	Frame Control Field: 0x5000
	.000 0001 0011 1010 = Duration: 314 microseconds
	Receiver address: Htc_85:b1:81 (e8:99:c4:85:b1:81)
	Destination address: Htc_85:b1:81 (e8:99:c4:85:b1:81)
	Transmitter address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)
	Source address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)
	BSS Id: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)
	Fragment number: 0
	Sequence number: 1459
+	Frame check sequence: 0x4c0c60d3 [correct]
-	IEEE 802.11 wireless LAN management frame
+	Fixed parameters (12 bytes)
+	Tagged parameters (372 bytes)

- **Beacon Frame**

1	0.000000	AirtiesW_6e:af:d4	Broadcast	802.11
---	----------	-------------------	-----------	--------

+	Frame 1: 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)
	Transmitter address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)
	Source address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)
	BSS Id: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)
	Fragment number: 0
	Sequence number: 505
+	Frame check sequence: 0x0b92b8f4 [correct]
-	IEEE 802.11 wireless LAN management frame
+	Fixed parameters (12 bytes)
+	Tagged parameters (245 bytes)

Deauthentication Frame Yapısı

Ağ cihazı veya istemci(bazen durumlarda saldırganlar) bağlantıyı koparmak istediğinde bu frame kullanılır.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	MurataMa_80:a0:9b	AirtiesW_6e:af:d4	802.11	38	Deauthentication, SN=
.....						
+ Frame 1: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)						
+ Radiotap Header v0, Length 12						
- IEEE 802.11 Deauthentication, Flags:						
Type/Subtype: Deauthentication (0x0c)						
+ Frame Control Field: 0xc000						
.000 0001 0011 1010 = Duration: 314 microseconds						
Receiver address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)						
Destination address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)						
Transmitter address: MurataMa_80:a0:9b (40:f3:08:80:a0:9b)						
Source address: MurataMa_80:a0:9b (40:f3:08:80:a0:9b)						
BSS Id: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)						
Fragment number: 0						
Sequence number: 1						
- IEEE 802.11 wireless LAN management frame						
+ Fixed parameters (2 bytes)						
Reason code: Class 3 frame received from nonassociated STA (0x0007)						

Bir istemciye yönelik AP cihazından düşürme testidir.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AirtiesW_6e:af:d4	Broadcast	802.11	38	Deauthentication, SN=
.....						
+ Frame 1: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)						
+ Radiotap Header v0, Length 12						
- IEEE 802.11 Deauthentication, Flags:						
Type/Subtype: Deauthentication (0x0c)						
+ Frame Control Field: 0xc000						
.000 0001 0011 1010 = Duration: 314 microseconds						
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)						
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)						
Transmitter address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)						
Source address: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)						
BSS Id: AirtiesW_6e:af:d4 (18:28:61:6e:af:d4)						
Fragment number: 0						
Sequence number: 0						
- IEEE 802.11 wireless LAN management frame						
+ Fixed parameters (2 bytes)						
Reason code: Class 3 frame received from nonassociated STA (0x0007)						

Bütün istemcilere yönelik AP cihazından düşürme testidir.

Deauthentication Reason Codes

Reason Code	Description	Meaning
0	No Reason Code	Normal operation
1	Unspecified Reason	Client associated but no longer authorized
2	Previous Authentication no longer valid	Client associated but not authorized
3	Deauthentication Leaving	Deauthenticated because sending STA is leaving IBSS or ESS
4	Disassociation Due to Inactivity	Client session timeout exceeded
5	Disassociation AP Busy	AP is busy and unable to handle currently associated clients
6	Class2 Frame from Non-Authenticated Station	Client attempted to transfer data before it was authenticated
7	Class3 Frame from Non-Associated Station	Client attempted to transfer data before it was associated
8	Disassociation STA has Left	STA is leaving or has left BSS
9	STA Request Association Without Authentication	STA (re)association is not authenticated with responding station
...
99	Missing Reason Code	Client momentarily in an unknown state

Association Frame

The image shows a Wireshark packet capture 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. A filter bar is present with a dropdown menu and buttons for Expression..., Clear, Apply, and Save.

The packet list pane shows the following packets:

Packet No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	adcast		802.11	59	Beacon frame, SN=378, FN=0, Flags=...
2	0.000000	adcast		802.11	42	Association Request, SN=30, FN=0, Flags=...
3	0.000000	adcast		802.11	10	Acknowledgement, Flags=.....
4	0.000000	adcast		802.11	36	Association Response, SN=751, FN=0, Flags=.....
5	0.000000	adcast		802.11	10	Acknowledgement, Flags=.....

The packet details pane shows the structure of the selected packet (Frame 4):

- Frame 4: 36 bytes on wire (288 bits), 36 bytes captured (288 bits)
- IEEE 802.11 Association Response, Flags:
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters (6 bytes)
 - Capabilities Information: 0x0001
 - Status code: Successful (0x0000)
 - ..00 0000 0000 0001 = Association ID: 0x0001
 - Tagged parameters (6 bytes)

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

```
0000 10 00 d5 00 00 15 6d 10 11 05 00 12 bf 12 32 29 .....m. ....2)
0010 00 12 bf 12 32 29 f0 2e 01 00 00 00 01 c0 01 04 .....2).. .....
0020 82 84 8b 96 .....
```