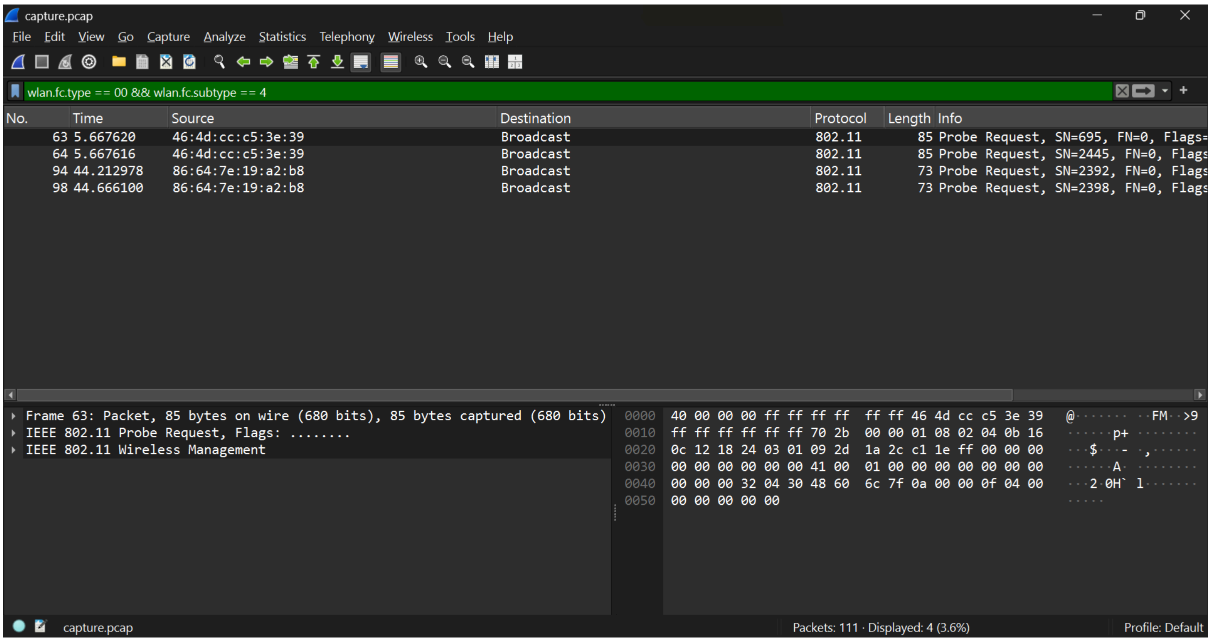
# Internet Protocol Lab Assignment-9

NAME-Kushagra Ojha

ENROLLMENT NUMBER –CB.SC.P2CYS25029

**1.**



capture.pcap

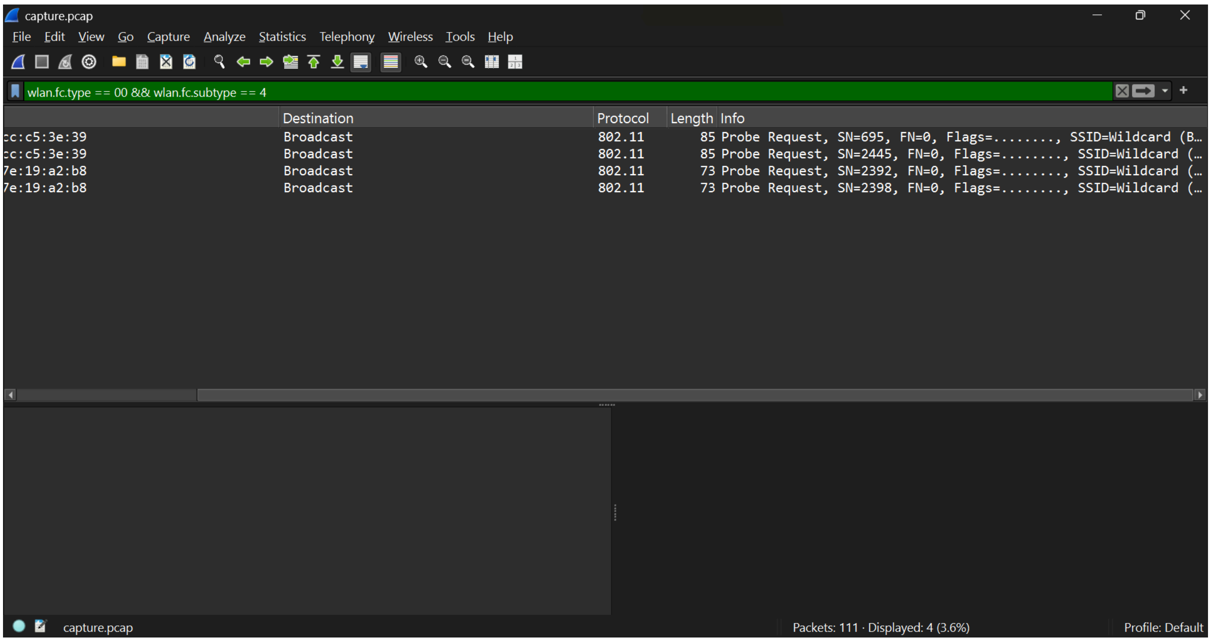
wlan.fc.type == 00 && wlan.fc.subtype == 4

```
No.  Time        Source              Destination   Protocol  Length Info
  63 5.667620    46:4d:cc:c5:3e:39   Broadcast     802.11    85 Probe Request, SN=695, FN=0, Flags=
  64 5.667616    46:4d:cc:c5:3e:39   Broadcast     802.11    85 Probe Request, SN=2445, FN=0, Flags
  94 44.212978   86:64:7e:19:a2:b8   Broadcast     802.11    73 Probe Request, SN=2392, FN=0, Flags
  98 44.666100   86:64:7e:19:a2:b8   Broadcast     802.11    73 Probe Request, SN=2398, FN=0, Flags
```

```
› Frame 63: Packet, 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
› IEEE 802.11 Probe Request, Flags: ........
› IEEE 802.11 Wireless Management
```

```
0000  40 00 00 00 ff ff ff ff  ff ff 46 4d cc c5 3e 39   @·······  ··FM··>9
0010  ff ff ff ff ff ff 70 2b  00 00 01 08 02 04 0b 16   ······p+  ········
0020  0c 12 18 24 03 01 09 2d  1a 2c c1 1e ff 00 00 00   ···$···-  ·,······
0030  00 00 00 00 00 00 41 00  01 00 00 00 00 00 00 00   ······A·  ········
0040  00 00 00 32 04 30 48 60  6c 7f 0a 00 00 0f 04 00   ···2·0H`  l·······
0050  00 00 00 00 00                                      ·····
```

capture.pcap | Packets: 111 · Displayed: 4 (3.6%) | Profile: Default



capture.pcap

wlan.fc.type == 00 && wlan.fc.subtype == 4

```
                  Destination   Protocol  Length Info
:c:c5:3e:39       Broadcast     802.11    85 Probe Request, SN=695, FN=0, Flags=........, SSID=Wildcard (B…
:c:c5:3e:39       Broadcast     802.11    85 Probe Request, SN=2445, FN=0, Flags=........, SSID=Wildcard (…
7e:19:a2:b8       Broadcast     802.11    73 Probe Request, SN=2392, FN=0, Flags=........, SSID=Wildcard (…
7e:19:a2:b8       Broadcast     802.11    73 Probe Request, SN=2398, FN=0, Flags=........, SSID=Wildcard (…
```

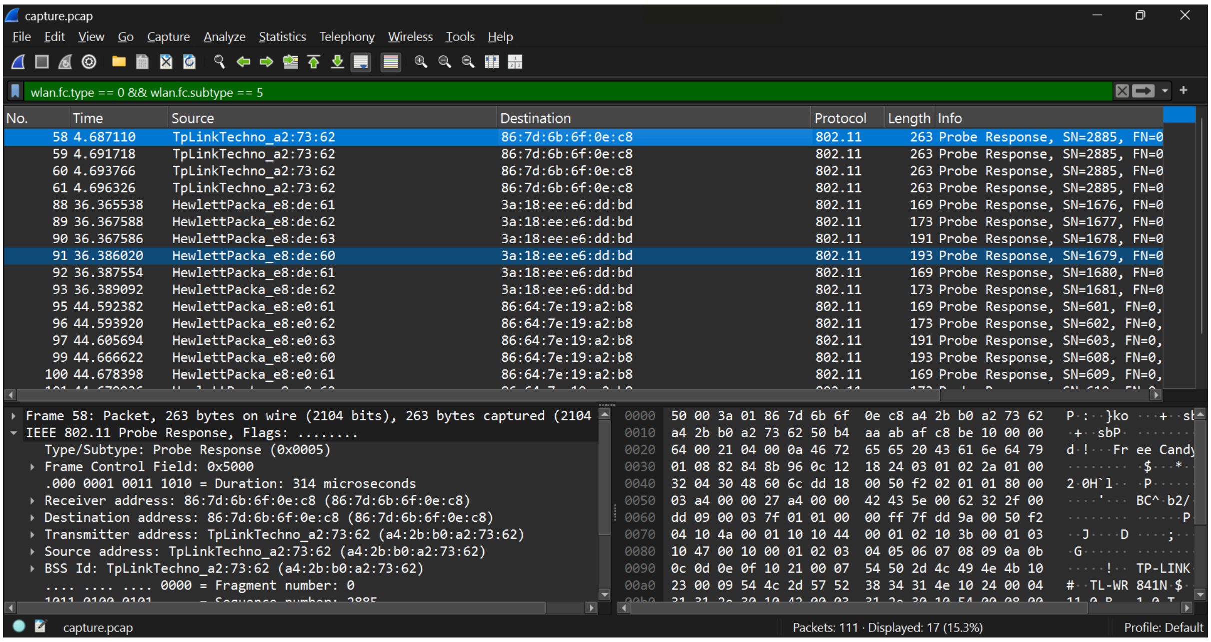
capture.pcap | Packets: 111 · Displayed: 4 (3.6%) | Profile: Default

Probe Request frames are sent by a **client device** to actively search for available Wi-Fi networks. These frames reveal information about the client such as:

- The **SSID** (network name) the client is trying to find — in this capture it shows **SSID: Wildcard (Broadcast)**, meaning the client is looking for *any available network*.
- The client's **supported data rates** and **802.11 capabilities** (like 802.11n support, channel preferences, and security types).
- The **source MAC address** of the client, which uniquely identifies its wireless interface.

The device sends probe requests **before connecting** to discover nearby access points more quickly than waiting for beacon frames, to check which APs are within range, and to select the one that best matches its supported rates and security settings for connection.

**2.**


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

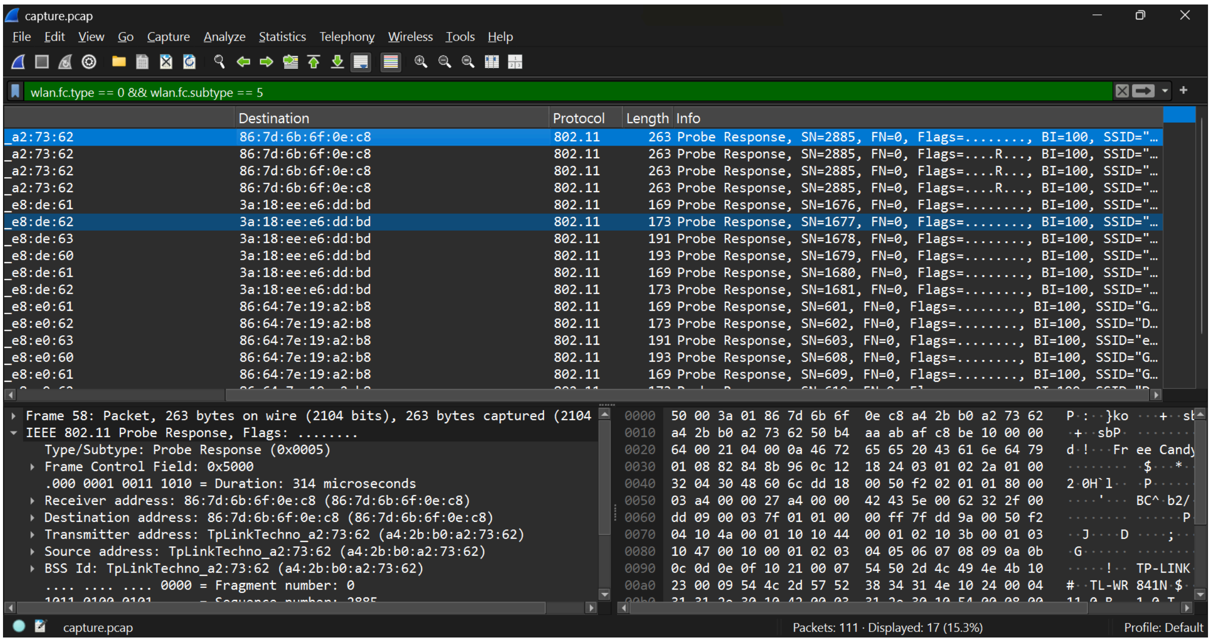
```
wlan.fc.type == 0 && wlan.fc.subtype == 5
```

```
No.   Time       Source                   Destination         Protocol  Length Info
   58 4.687110   TpLinkTechno_a2:73:62    86:7d:6b:6f:0e:c8   802.11    263 Probe Response, SN=2885, FN=0
   59 4.691718   TpLinkTechno_a2:73:62    86:7d:6b:6f:0e:c8   802.11    263 Probe Response, SN=2885, FN=0
   60 4.693766   TpLinkTechno_a2:73:62    86:7d:6b:6f:0e:c8   802.11    263 Probe Response, SN=2885, FN=0
   61 4.696326   TpLinkTechno_a2:73:62    86:7d:6b:6f:0e:c8   802.11    263 Probe Response, SN=2885, FN=0
   88 36.365538  HewlettPacka_e8:de:61    3a:18:ee:e6:dd:bd   802.11    169 Probe Response, SN=1676, FN=0
   89 36.367588  HewlettPacka_e8:de:62    3a:18:ee:e6:dd:bd   802.11    173 Probe Response, SN=1677, FN=0
   90 36.367586  HewlettPacka_e8:de:63    3a:18:ee:e6:dd:bd   802.11    191 Probe Response, SN=1678, FN=0
   91 36.386020  HewlettPacka_e8:de:60    3a:18:ee:e6:dd:bd   802.11    193 Probe Response, SN=1679, FN=0
   92 36.387554  HewlettPacka_e8:de:61    3a:18:ee:e6:dd:bd   802.11    169 Probe Response, SN=1680, FN=0
   93 36.389092  HewlettPacka_e8:de:62    3a:18:ee:e6:dd:bd   802.11    173 Probe Response, SN=1681, FN=0
   95 44.592382  HewlettPacka_e8:e0:61    86:64:7e:19:a2:b8   802.11    169 Probe Response, SN=601, FN=0,
   96 44.593920  HewlettPacka_e8:e0:62    86:64:7e:19:a2:b8   802.11    173 Probe Response, SN=602, FN=0,
   97 44.605694  HewlettPacka_e8:e0:63    86:64:7e:19:a2:b8   802.11    191 Probe Response, SN=603, FN=0,
   99 44.666622  HewlettPacka_e8:e0:60    86:64:7e:19:a2:b8   802.11    193 Probe Response, SN=608, FN=0,
  100 44.678398  HewlettPacka_e8:e0:61    86:64:7e:19:a2:b8   802.11    169 Probe Response, SN=609, FN=0,
```

```
▸ Frame 58: Packet, 263 bytes on wire (2104 bits), 263 bytes captured (2104
▾ IEEE 802.11 Probe Response, Flags: ........
    Type/Subtype: Probe Response (0x0005)
  ▸ Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
  ▸ Receiver address: 86:7d:6b:6f:0e:c8 (86:7d:6b:6f:0e:c8)
  ▸ Destination address: 86:7d:6b:6f:0e:c8 (86:7d:6b:6f:0e:c8)
  ▸ Transmitter address: TpLinkTechno_a2:73:62 (a4:2b:b0:a2:73:62)
  ▸ Source address: TpLinkTechno_a2:73:62 (a4:2b:b0:a2:73:62)
  ▸ BSS Id: TpLinkTechno_a2:73:62 (a4:2b:b0:a2:73:62)
    .... .... .... 0000 = Fragment number: 0
```

```
0000  50 00 3a 01 86 7d 6b 6f  0e c8 a4 2b b0 a2 73 62   P·:··}ko···+··sb
0010  a4 2b b0 a2 73 62 50 b4  aa ab af c8 be 10 00 00   ·+··sbP·········
0020  64 00 21 04 00 0a 46 72  65 65 20 43 61 6e 64 79   d·!···Free Candy
0030  01 08 82 84 8b 96 0c 12  18 24 03 01 02 2a 01 00   ·········$···*··
0040  32 04 30 48 60 6c dd 18  00 50 f2 02 01 01 80 00   2·0H`l···P······
0050  03 a4 00 00 27 a4 00 00  42 43 5e 00 62 32 2f 00   ····'···BC^·b2/·
0060  dd 09 00 03 7f 01 01 00  00 ff 7f dd 9a 00 50 f2   ··············P·
0070  04 10 4a 00 01 10 10 44  00 01 02 10 3b 00 01 03   ··J····D····;···
0080  10 47 00 10 00 01 02 03  04 05 06 07 08 09 0a 0b   ·G··············
0090  0c 0d 0e 0f 10 21 00 07  54 50 2d 4c 49 4e 4b 10   ·····!··TP-LINK·
00a0  23 00 09 54 4c 2d 57 52  38 34 31 4e 10 24 00 04   #··TL-WR841N·$··
```

capture.pcap
Packets: 111 · Displayed: 17 (15.3%)
Profile: Default


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 0 && wlan.fc.subtype == 5
```

```
              Destination          Protocol  Length Info
_a2:73:62     86:7d:6b:6f:0e:c8    802.11    263 Probe Response, SN=2885, FN=0, Flags=........, BI=100, SSID="…
_a2:73:62     86:7d:6b:6f:0e:c8    802.11    263 Probe Response, SN=2885, FN=0, Flags=....R..., BI=100, SSID="…
_a2:73:62     86:7d:6b:6f:0e:c8    802.11    263 Probe Response, SN=2885, FN=0, Flags=....R..., BI=100, SSID="…
_a2:73:62     86:7d:6b:6f:0e:c8    802.11    263 Probe Response, SN=2885, FN=0, Flags=....R..., BI=100, SSID="…
_e8:de:61     3a:18:ee:e6:dd:bd    802.11    169 Probe Response, SN=1676, FN=0, Flags=........, BI=100, SSID="…
_e8:de:62     3a:18:ee:e6:dd:bd    802.11    173 Probe Response, SN=1677, FN=0, Flags=........, BI=100, SSID="…
_e8:de:63     3a:18:ee:e6:dd:bd    802.11    191 Probe Response, SN=1678, FN=0, Flags=........, BI=100, SSID="…
_e8:de:60     3a:18:ee:e6:dd:bd    802.11    193 Probe Response, SN=1679, FN=0, Flags=........, BI=100, SSID="…
_e8:de:61     3a:18:ee:e6:dd:bd    802.11    169 Probe Response, SN=1680, FN=0, Flags=........, BI=100, SSID="…
_e8:de:62     3a:18:ee:e6:dd:bd    802.11    173 Probe Response, SN=1681, FN=0, Flags=........, BI=100, SSID="…
_e8:e0:61     86:64:7e:19:a2:b8    802.11    169 Probe Response, SN=601, FN=0, Flags=........, BI=100, SSID="G…
_e8:e0:62     86:64:7e:19:a2:b8    802.11    173 Probe Response, SN=602, FN=0, Flags=........, BI=100, SSID="D…
_e8:e0:63     86:64:7e:19:a2:b8    802.11    191 Probe Response, SN=603, FN=0, Flags=........, BI=100, SSID="e…
_e8:e0:60     86:64:7e:19:a2:b8    802.11    193 Probe Response, SN=608, FN=0, Flags=........, BI=100, SSID="G…
_e8:e0:61     86:64:7e:19:a2:b8    802.11    169 Probe Response, SN=609, FN=0, Flags=........, BI=100, SSID="G…
```

```
▸ Frame 58: Packet, 263 bytes on wire (2104 bits), 263 bytes captured (2104
▾ IEEE 802.11 Probe Response, Flags: ........
    Type/Subtype: Probe Response (0x0005)
  ▸ Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
  ▸ Receiver address: 86:7d:6b:6f:0e:c8 (86:7d:6b:6f:0e:c8)
  ▸ Destination address: 86:7d:6b:6f:0e:c8 (86:7d:6b:6f:0e:c8)
  ▸ Transmitter address: TpLinkTechno_a2:73:62 (a4:2b:b0:a2:73:62)
  ▸ Source address: TpLinkTechno_a2:73:62 (a4:2b:b0:a2:73:62)
  ▸ BSS Id: TpLinkTechno_a2:73:62 (a4:2b:b0:a2:73:62)
    .... .... .... 0000 = Fragment number: 0
```

```
0000  50 00 3a 01 86 7d 6b 6f  0e c8 a4 2b b0 a2 73 62   P·:··}ko···+··sb
0010  a4 2b b0 a2 73 62 50 b4  aa ab af c8 be 10 00 00   ·+··sbP·········
0020  64 00 21 04 00 0a 46 72  65 65 20 43 61 6e 64 79   d·!···Free Candy
0030  01 08 82 84 8b 96 0c 12  18 24 03 01 02 2a 01 00   ·········$···*··
0040  32 04 30 48 60 6c dd 18  00 50 f2 02 01 01 80 00   2·0H`l···P······
0050  03 a4 00 00 27 a4 00 00  42 43 5e 00 62 32 2f 00   ····'···BC^·b2/·
0060  dd 09 00 03 7f 01 01 00  00 ff 7f dd 9a 00 50 f2   ··············P·
0070  04 10 4a 00 01 10 10 44  00 01 02 10 3b 00 01 03   ··J····D····;···
0080  10 47 00 10 00 01 02 03  04 05 06 07 08 09 0a 0b   ·G··············
0090  0c 0d 0e 0f 10 21 00 07  54 50 2d 4c 49 4e 4b 10   ·····!··TP-LINK·
00a0  23 00 09 54 4c 2d 57 52  38 34 31 4e 10 24 00 04   #··TL-WR841N·$··
```

When the filter wlan.fc.type == 0 && wlan.fc.subtype == 5 is applied, the capture displays several **Probe Response** frames.

From the screenshot, the responding **Access Points (APs)** include:

- **TpLinkTechno_a2:73:62**
- **HewlettPacka_e8:6d:bd**

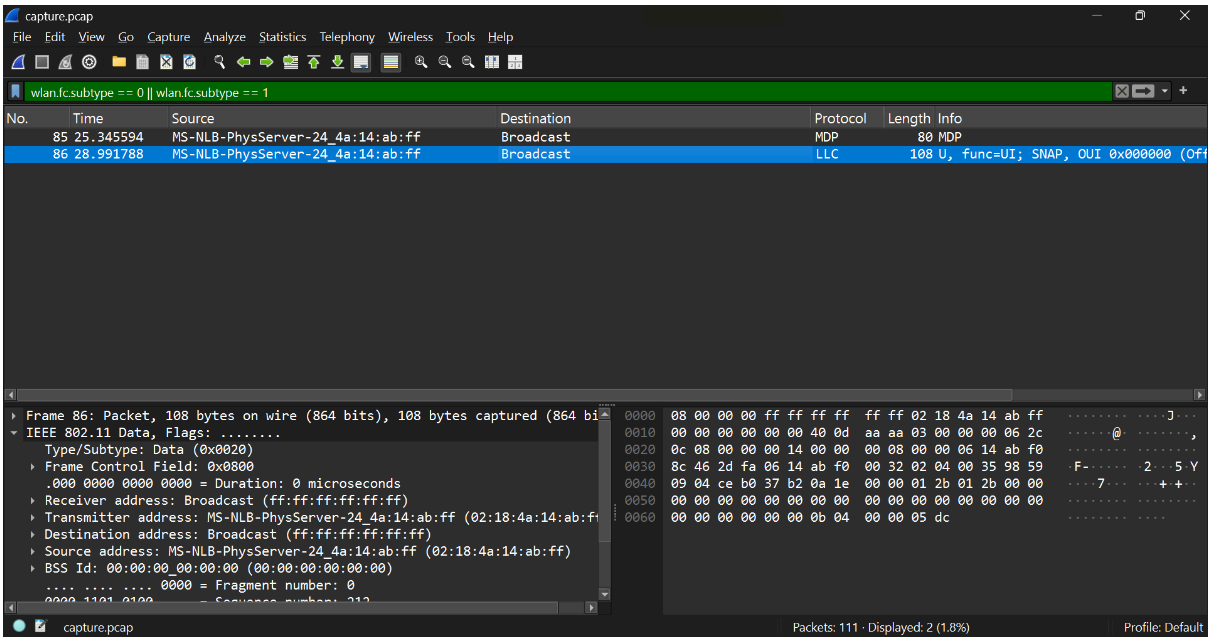
These access points are replying to clients that had earlier sent broadcast (wildcard) probe requests.

**Details shared by the APs in their Probe Response frames include:**

- **SSID:** The network name being advertised (e.g., *BT-100*, *TP-LINK_841N_5G*, etc.)
- **Channel/Frequency:** Indicates which radio channel (e.g., Channel 6 or Channel 11) the AP is operating on.
- **Supported Data Rates:** Lists transmission speeds and 802.11 standards (b/g/n/ac) supported.
- **Capabilities Information:** Includes security settings (e.g., WPA2, RSN), QoS support, and short preamble options.

- **BSSID:** The unique MAC address identifying the access point.
  **Explanation:**
  Probe Responses allow clients to learn detailed network parameters from nearby APs. Using this information—SSID, signal strength, and supported features—the client decides which access point offers the best compatibility and signal for association.

**3.**



capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

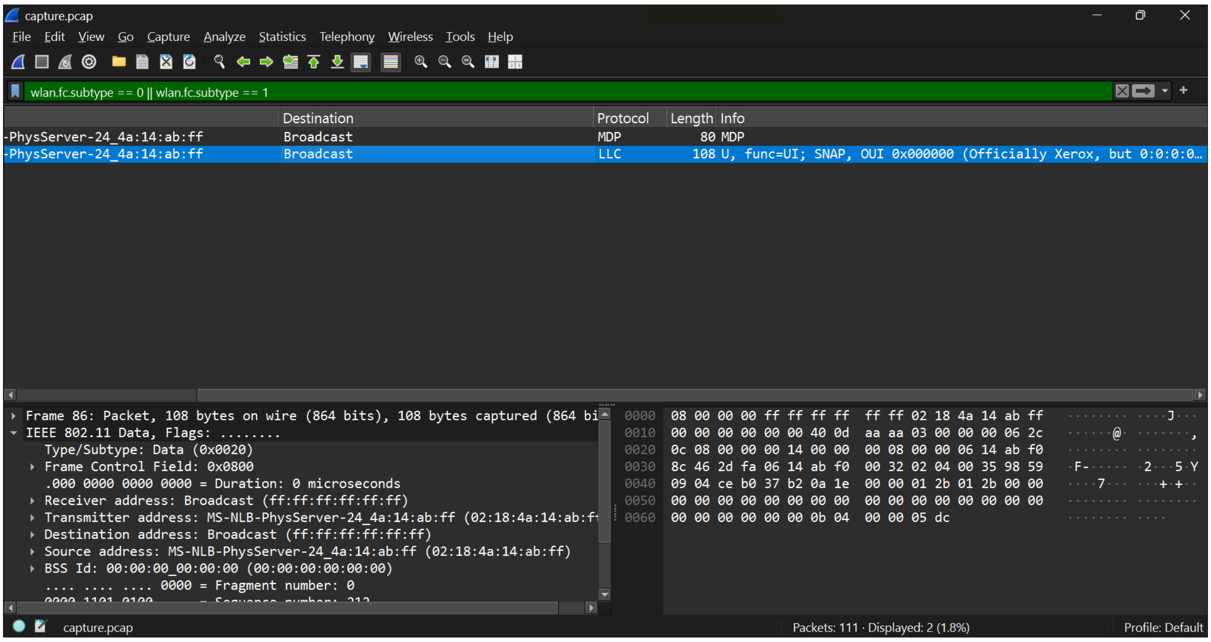
```
wlan.fc.subtype == 0 || wlan.fc.subtype == 1

No.    Time          Source                           Destination     Protocol  Length  Info
    85 25.345594     MS-NLB-PhysServer-24_4a:14:ab:ff Broadcast       MDP           80  MDP
    86 28.991788     MS-NLB-PhysServer-24_4a:14:ab:ff Broadcast       LLC          108  U, func=UI; SNAP, OUI 0x000000 (Off

› Frame 86: Packet, 108 bytes on wire (864 bits), 108 bytes captured (864 bi
⌄ IEEE 802.11 Data, Flags: ........
    Type/Subtype: Data (0x0020)
  › Frame Control Field: 0x0800
    .000 0000 0000 0000 = Duration: 0 microseconds
  › Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  › Transmitter address: MS-NLB-PhysServer-24_4a:14:ab:ff (02:18:4a:14:ab:f
  › Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  › Source address: MS-NLB-PhysServer-24_4a:14:ab:ff (02:18:4a:14:ab:ff)
  › BSS Id: 00:00:00_00:00:00 (00:00:00:00:00:00)
    .... .... .... 0000 = Fragment number: 0
    0000 1101 0100 .... = Sequence number: 212

0000  08 00 00 00 ff ff ff ff  ff ff 02 18 4a 14 ab ff   ········ ····J···
0010  00 00 00 00 00 00 40 0d  aa aa 03 00 00 00 06 2c   ······@· ·······,
0020  0c 08 00 00 00 14 00 00  00 08 00 00 06 14 ab f0   ········ ········
0030  8c 46 2d fa 06 14 ab f0  00 32 02 04 00 35 98 59   ·F-····· ·2··5·Y
0040  09 04 ce b0 37 b2 0a 1e  00 00 01 2b 01 2b 00 00   ····7··· ···+·+··
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 0b 04  00 00 05 dc               ········ ····

capture.pcap                Packets: 111 · Displayed: 2 (1.8%)            Profile: Default
```



capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.subtype == 0 || wlan.fc.subtype == 1

                                  Destination     Protocol  Length  Info
-PhysServer-24_4a:14:ab:ff        Broadcast       MDP           80  MDP
-PhysServer-24_4a:14:ab:ff        Broadcast       LLC          108  U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0…

› Frame 86: Packet, 108 bytes on wire (864 bits), 108 bytes captured (864 bi
⌄ IEEE 802.11 Data, Flags: ........
    Type/Subtype: Data (0x0020)
  › Frame Control Field: 0x0800
    .000 0000 0000 0000 = Duration: 0 microseconds
  › Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  › Transmitter address: MS-NLB-PhysServer-24_4a:14:ab:ff (02:18:4a:14:ab:f
  › Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  › Source address: MS-NLB-PhysServer-24_4a:14:ab:ff (02:18:4a:14:ab:ff)
  › BSS Id: 00:00:00_00:00:00 (00:00:00:00:00:00)
    .... .... .... 0000 = Fragment number: 0
    0000 1101 0100 .... = Sequence number: 212

0000  08 00 00 00 ff ff ff ff  ff ff 02 18 4a 14 ab ff   ········ ····J···
0010  00 00 00 00 00 00 40 0d  aa aa 03 00 00 00 06 2c   ······@· ·······,
0020  0c 08 00 00 00 14 00 00  00 08 00 00 06 14 ab f0   ········ ········
0030  8c 46 2d fa 06 14 ab f0  00 32 02 04 00 35 98 59   ·F-····· ·2··5·Y
0040  09 04 ce b0 37 b2 0a 1e  00 00 01 2b 01 2b 00 00   ····7··· ···+·+··
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 0b 04  00 00 05 dc               ········ ····

capture.pcap                Packets: 111 · Displayed: 2 (1.8%)            Profile: Default
```

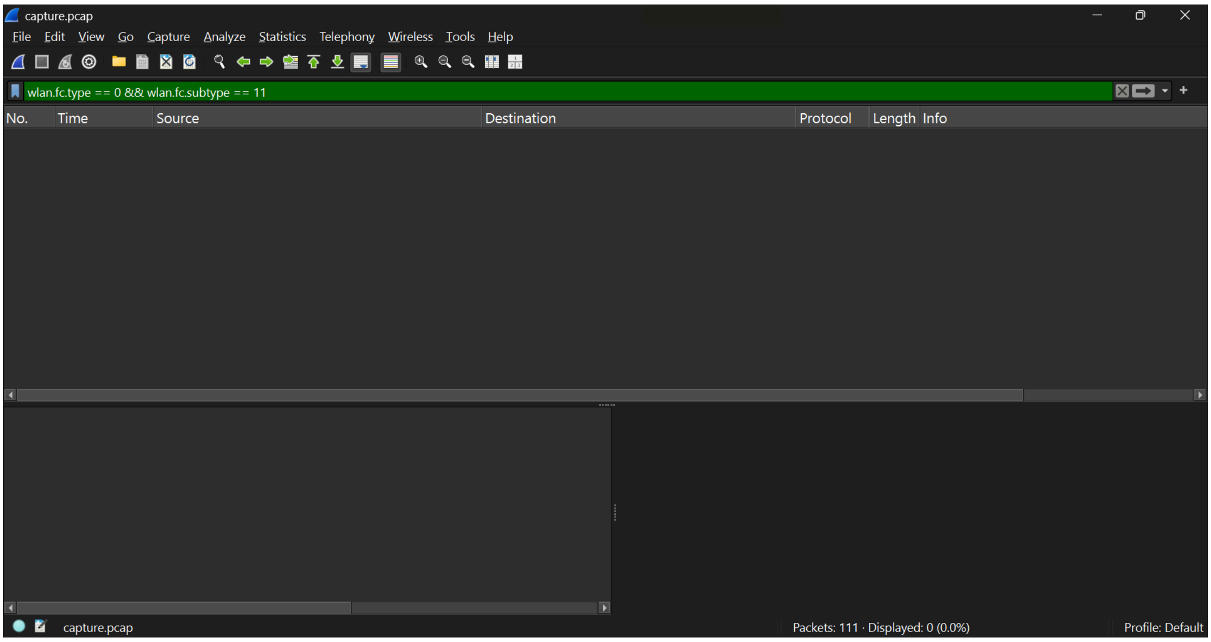
When the filter wlan.fc.subtype == 0 || wlan.fc.subtype == 1 is applied, the capture shows **Association Request** and **Association Response** frames exchanged between the client and the access point (AP).

**Parameters exchanged during association:**

- **SSID:** The network name the client wants to join.
- **Supported data rates:** Transmission speeds that the client can handle.
- **Capabilities information:** Such as QoS support, short preamble, and security features (e.g., WPA2/WPA3).
- **Listen Interval:** How often the client wakes up to listen for buffered traffic from the AP.
- **Association ID (AID):** Assigned by the AP in its response to identify the client in the network.
  **Explanation:**

- The **Association Request** is sent by the client after successful authentication to formally request connection to the AP.
- The **Association Response** from the AP includes an **AID** and confirmation that the client is now associated.
- These exchanges complete the **link-layer connection setup**, allowing the client to start data communication over the network.

**4.**



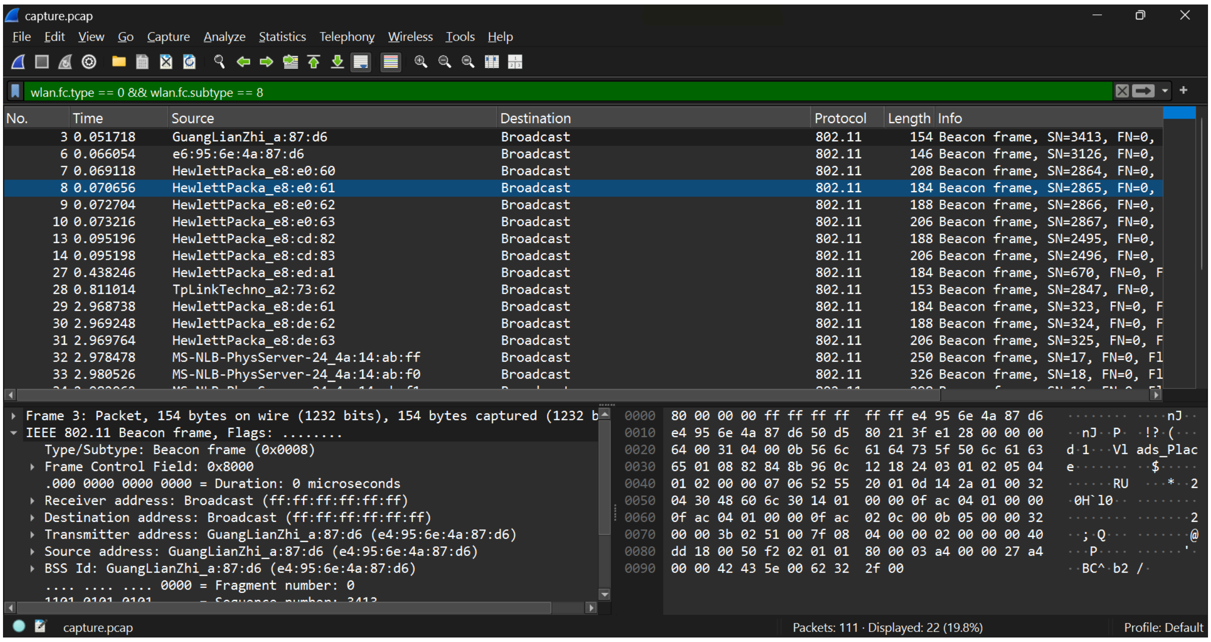
capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 0 && wlan.fc.subtype == 11
```

```
No.   Time   Source   Destination   Protocol   Length  Info
```

capture.pcap    Packets: 111 · Displayed: 0 (0.0%)    Profile: Default

**5.**



capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 0 && wlan.fc.subtype == 8
```

```
No.  Time      Source                           Destination  Protocol  Length Info
   3 0.051718  GuangLianZhi_a:87:d6             Broadcast    802.11    154 Beacon frame, SN=3413, FN=0,
   6 0.066054  e6:95:6e:4a:87:d6                Broadcast    802.11    146 Beacon frame, SN=3126, FN=0,
   7 0.069118  HewlettPacka_e8:e0:60            Broadcast    802.11    208 Beacon frame, SN=2864, FN=0,
   8 0.070656  HewlettPacka_e8:e0:61            Broadcast    802.11    184 Beacon frame, SN=2865, FN=0,
   9 0.072704  HewlettPacka_e8:e0:62            Broadcast    802.11    188 Beacon frame, SN=2866, FN=0,
  10 0.073216  HewlettPacka_e8:e0:63            Broadcast    802.11    206 Beacon frame, SN=2867, FN=0,
  13 0.095196  HewlettPacka_e8:cd:82            Broadcast    802.11    188 Beacon frame, SN=2495, FN=0,
  14 0.095198  HewlettPacka_e8:cd:83            Broadcast    802.11    206 Beacon frame, SN=2496, FN=0,
  27 0.438246  HewlettPacka_e8:ed:a1            Broadcast    802.11    184 Beacon frame, SN=670, FN=0, F
  28 0.811014  TpLinkTechno_a2:73:62            Broadcast    802.11    153 Beacon frame, SN=2847, FN=0,
  29 2.968738  HewlettPacka_e8:de:61            Broadcast    802.11    184 Beacon frame, SN=323, FN=0, F
  30 2.969248  HewlettPacka_e8:de:62            Broadcast    802.11    188 Beacon frame, SN=324, FN=0, F
  31 2.969764  HewlettPacka_e8:de:63            Broadcast    802.11    206 Beacon frame, SN=325, FN=0, F
  32 2.978478  MS-NLB-PhysServer-24_4a:14:ab:ff Broadcast    802.11    250 Beacon frame, SN=17, FN=0, Fl
  33 2.980526  MS-NLB-PhysServer-24_4a:14:ab:f0 Broadcast    802.11    326 Beacon frame, SN=18, FN=0, Fl
```

```
› Frame 3: Packet, 154 bytes on wire (1232 bits), 154 bytes captured (1232 b
⌄ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  › 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: GuangLianZhi_a:87:d6 (e4:95:6e:4a:87:d6)
  › Source address: GuangLianZhi_a:87:d6 (e4:95:6e:4a:87:d6)
  › BSS Id: GuangLianZhi_a:87:d6 (e4:95:6e:4a:87:d6)
    .... .... .... 0000 = Fragment number: 0
```

```
0000  80 00 00 00 ff ff ff ff  ff ff e4 95 6e 4a 87 d6   ········ ····nJ··
0010  e4 95 6e 4a 87 d6 50 d5  80 21 3f e1 28 00 00 00   ··nJ··P· ·!?·(···
0020  64 00 31 04 00 0b 56 6c  61 64 73 5f 50 6c 61 63   d·1···Vl ads_Plac
0030  65 01 08 82 84 8b 96 0c  12 18 24 03 01 02 05 04   e······· ··$·····
0040  01 02 00 00 07 06 52 55  20 01 0d 14 2a 01 00 32   ······RU  ···*··2
0050  04 30 48 60 6c 30 14 01  00 00 0f ac 04 01 00 00   ·0H`l0·· ········
0060  0f ac 04 01 00 00 0f ac  02 0c 00 0b 05 00 00 32   ········ ·······2
0070  00 00 3b 02 51 00 7f 08  04 00 00 02 00 00 00 40   ··;·Q··· ·······@
0080  dd 18 00 50 f2 02 01 01  80 00 03 a4 00 00 27 a4   ···P···· ······'·
0090  00 00 42 43 5e 00 62 32  2f 00                     ··BC^·b2 /·
```

capture.pcap    Packets: 111 · Displayed: 22 (19.8%)    Profile: Default

When the filter wlan.fc.type == 0 && wlan.fc.subtype == 8 is applied, the capture displays multiple **Beacon frames** transmitted by different access points (APs) such as **GuangLianZhi_a:87:d6**, **HewlettPacka_e8:0e:60**, and **TpLinkTechno_a2:73:62**.

**SSIDs being advertised:**

From the captured beacon frames, the SSIDs include names like:

- *ads_place*
- *BI-100*

- *TP-LINK_841N*

  (Each AP broadcasts its SSID to identify its wireless network.)

  **How often beacons are sent:**

- Beacons are transmitted **periodically**, typically every **100 milliseconds (0.1 seconds)**, to announce the presence of a wireless network and maintain synchronization with connected clients.

  **Network information broadcast through beacon frames:**

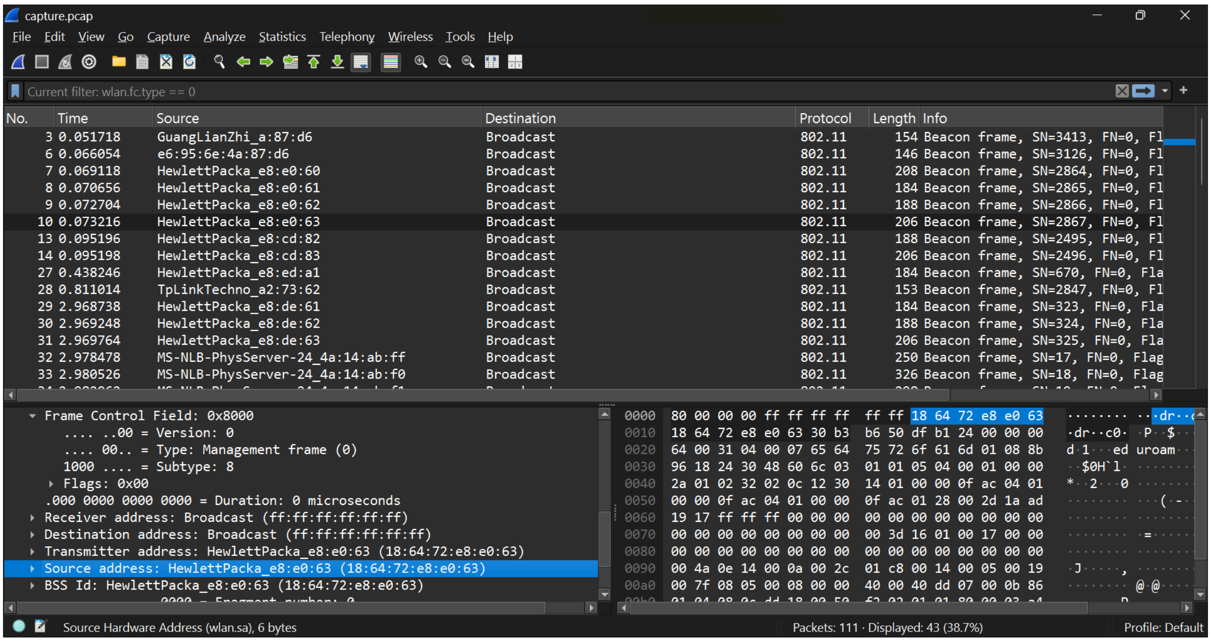
  Each beacon frame carries essential details about the AP and its network, including:

- **SSID** (network name)
- **BSSID** (MAC address of the AP)
- **Supported data rates and capabilities**
- **Channel number and frequency band**
- **Timestamp and beacon interval**
- **Security information** (e.g., WPA2/WPA3 RSN details)

  **Explanation:**

  Beacon frames allow nearby client devices to discover available wireless networks and obtain configuration parameters required to initiate a connection. They act as periodic advertisements that define the AP's identity and operating characteristics.

**6.**



capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: wlan.fc.type == 0

```
No.  Time      Source                             Destination  Protocol  Length Info
   3 0.051718  GuangLianZhi_a:87:d6               Broadcast    802.11    154 Beacon frame, SN=3413, FN=0, Fl
   6 0.066054  e6:95:6e:4a:87:d6                  Broadcast    802.11    146 Beacon frame, SN=3126, FN=0, Fl
   7 0.069118  HewlettPacka_e8:e0:60              Broadcast    802.11    208 Beacon frame, SN=2864, FN=0, Fl
   8 0.070656  HewlettPacka_e8:e0:61              Broadcast    802.11    184 Beacon frame, SN=2865, FN=0, Fl
   9 0.072704  HewlettPacka_e8:e0:62              Broadcast    802.11    188 Beacon frame, SN=2866, FN=0, Fl
  10 0.073216  HewlettPacka_e8:e0:63              Broadcast    802.11    206 Beacon frame, SN=2867, FN=0, Fl
  13 0.095196  HewlettPacka_e8:cd:82              Broadcast    802.11    188 Beacon frame, SN=2495, FN=0, Fl
  14 0.095198  HewlettPacka_e8:cd:83              Broadcast    802.11    206 Beacon frame, SN=2496, FN=0, Fl
  27 0.438246  HewlettPacka_e8:ed:a1              Broadcast    802.11    184 Beacon frame, SN=670, FN=0, Fla
  28 0.811014  TpLinkTechno_a2:73:62              Broadcast    802.11    153 Beacon frame, SN=2847, FN=0, Fl
  29 2.968738  HewlettPacka_e8:de:61              Broadcast    802.11    184 Beacon frame, SN=323, FN=0, Fla
  30 2.969248  HewlettPacka_e8:de:62              Broadcast    802.11    188 Beacon frame, SN=324, FN=0, Fla
  31 2.969764  HewlettPacka_e8:de:63              Broadcast    802.11    206 Beacon frame, SN=325, FN=0, Fla
  32 2.978478  MS-NLB-PhysServer-24_4a:14:ab:ff   Broadcast    802.11    250 Beacon frame, SN=17, FN=0, Flag
  33 2.980526  MS-NLB-PhysServer-24_4a:14:ab:f0   Broadcast    802.11    326 Beacon frame, SN=18, FN=0, Flag
```

```
▾ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  › Flags: 0x00
  .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: HewlettPacka_e8:e0:63 (18:64:72:e8:e0:63)
› Source address: HewlettPacka_e8:e0:63 (18:64:72:e8:e0:63)
› BSS Id: HewlettPacka_e8:e0:63 (18:64:72:e8:e0:63)
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 18 64 72 e8 e0 63   ........ ...dr..
0010  18 64 72 e8 e0 63 30 b3  b6 50 df b1 24 00 00 00   .dr..c0. .P..$...
0020  64 00 31 04 00 07 65 64  75 72 6f 61 6d 01 08 8b   d.1...ed uroam...
0030  96 18 24 30 48 60 6c 03  01 01 05 04 00 01 00 00   ..$0H`l. ........
0040  2a 01 02 32 02 0c 12 30  14 01 00 00 0f ac 04 01   *..2...0 ........
0050  00 00 0f ac 04 01 00 00  0f ac 01 28 00 2d 1a ad   ........ ...(.-..
0060  19 17 ff ff ff 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 3d 16 01 00 17 00 00   ........ .=......
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 4a 0e 14 00 0a 00 2c  01 c8 00 14 00 05 00 19   .J.....,  ........
00a0  00 7f 08 05 00 08 00 00  40 00 40 dd 07 00 0b 86   ........ @.@.....
```

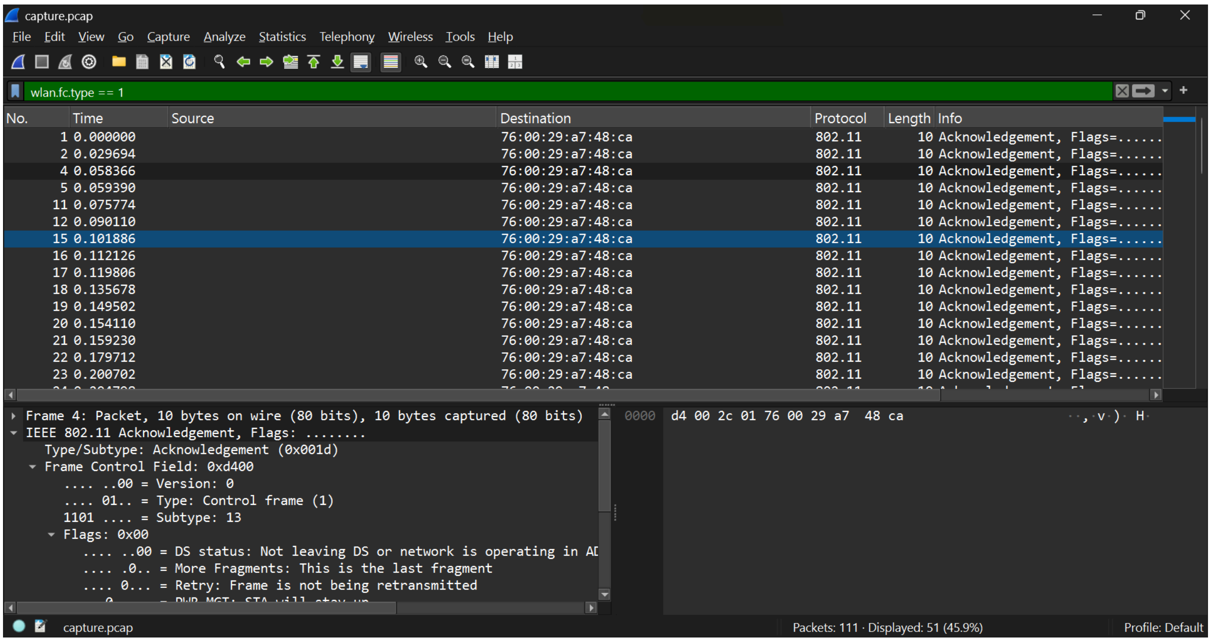
Source Hardware Address (wlan.sa), 6 bytes    Packets: 111 · Displayed: 43 (38.7%)    Profile: Default

**SA (Source Address):** the *device that transmitted* the frame (actual sender).

**DA (Destination Address):** the *intended receiver* of the frame (single station or broadcast).

**BSSID:** the identifier (MAC) of the **Basic Service Set** (usually the AP's MAC in infrastructure mode).

**7.**



capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 1
```

```
No.   Time       Source   Destination         Protocol  Length Info
    1 0.000000            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
    2 0.029694            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
    4 0.058366            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
    5 0.059390            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   11 0.075774            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   12 0.090110            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   15 0.101886            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   16 0.112126            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   17 0.119806            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   18 0.135678            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   19 0.149502            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   20 0.154110            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   21 0.159230            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   22 0.179712            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
   23 0.200702            76:00:29:a7:48:ca   802.11        10 Acknowledgement, Flags=......
```

```
Frame 4: Packet, 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
IEEE 802.11 Acknowledgement, Flags: ........
  Type/Subtype: Acknowledgement (0x001d)
  Frame Control Field: 0xd400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1101 .... = Subtype: 13
    Flags: 0x00
      .... ..00 = DS status: Not leaving DS or network is operating in AD
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
```

```
0000  d4 00 2c 01 76 00 29 a7  48 ca                     ··,·v·)· H·
```

When the filter wlan.fc.type == 1 is applied, the capture displays several **control frames**, specifically **Acknowledgement (ACK)** frames between wireless devices.

**Purpose and function of control frames:**

Control frames are used in IEEE 802.11 networks to **manage and coordinate access** to the shared wireless medium, helping to prevent collisions and ensure reliable delivery. The key types are:

- **RTS (Request to Send):** Sent by a station to reserve the channel before sending data.
- **CTS (Clear to Send):** Sent by the receiver in response to RTS, indicating the channel is clear.
- **ACK (Acknowledgment):** Sent by the receiver to confirm that a frame was successfully received.

**How they prevent collisions:**

- **RTS/CTS** helps avoid the *hidden node problem* by ensuring that all nearby stations are aware that the channel is reserved for transmission.
- **ACK** ensures reliable communication; if an ACK is not received, the sender retransmits the frame, reducing packet loss.

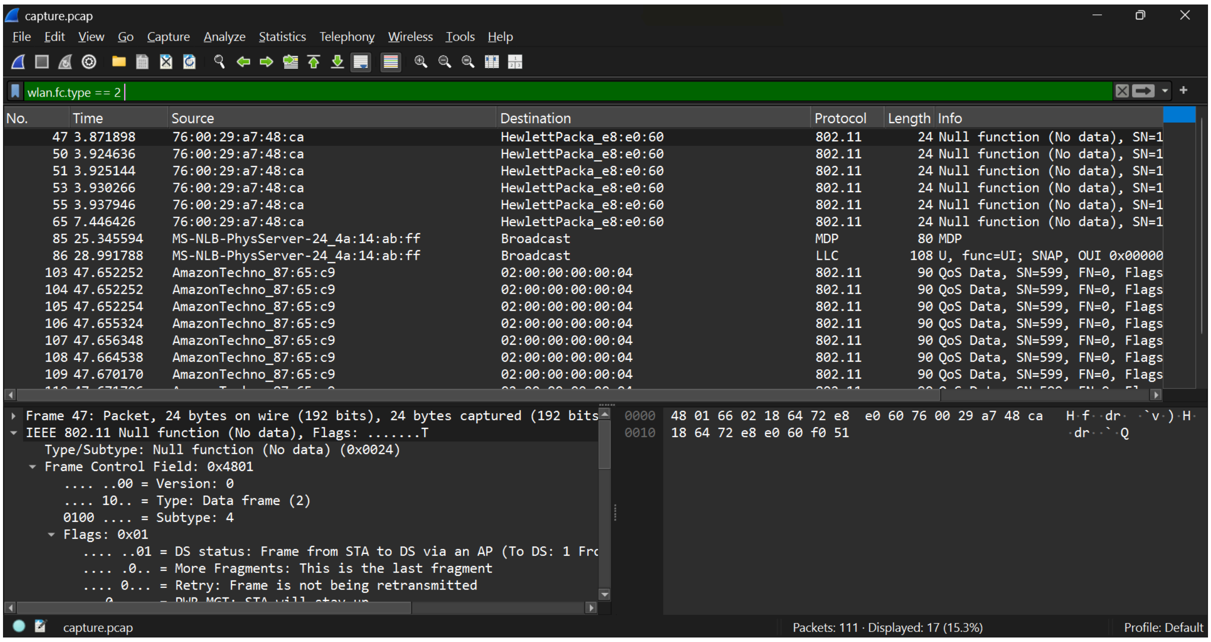
**From the capture:**

- Multiple **ACK frames** (Subtype 13) are seen, such as between source d4:00:2c:01:76:00 and destination 76:00:29:a7:48:ca.
- Each ACK frame is only **10 bytes long**, confirming receipt of a previous data frame.

**Conclusion:**

The ACK frames in the capture confirm successful frame delivery between wireless devices. Together with RTS and CTS mechanisms, these control frames maintain efficient and collision-free communication in Wi-Fi networks.

**8.**



capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

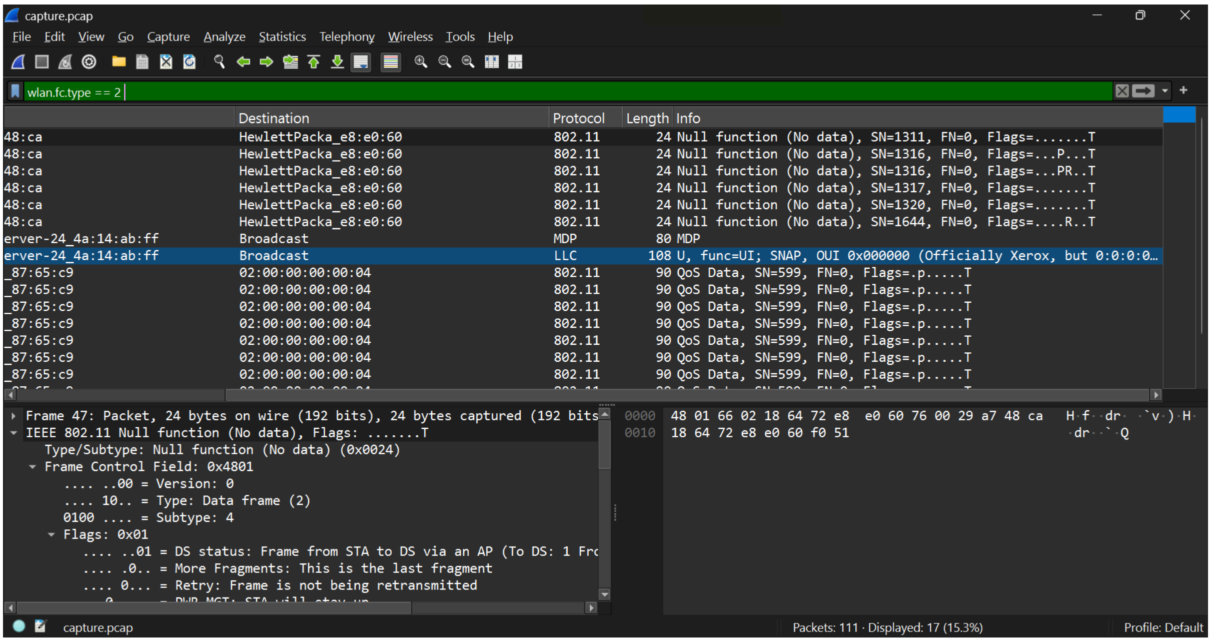
```
wlan.fc.type == 2
```

```
No.  Time        Source                          Destination              Protocol  Length Info
  47 3.871898    76:00:29:a7:48:ca               HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1
  50 3.924636    76:00:29:a7:48:ca               HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1
  51 3.925144    76:00:29:a7:48:ca               HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1
  53 3.930266    76:00:29:a7:48:ca               HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1
  55 3.937946    76:00:29:a7:48:ca               HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1
  65 7.446426    76:00:29:a7:48:ca               HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1
  85 25.345594   MS-NLB-PhysServer-24_4a:14:ab:ff Broadcast               MDP         80 MDP
  86 28.991788   MS-NLB-PhysServer-24_4a:14:ab:ff Broadcast               LLC        108 U, func=UI; SNAP, OUI 0x00000
 103 47.652252   AmazonTechno_87:65:c9           02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags
 104 47.652252   AmazonTechno_87:65:c9           02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags
 105 47.652254   AmazonTechno_87:65:c9           02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags
 106 47.655324   AmazonTechno_87:65:c9           02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags
 107 47.656348   AmazonTechno_87:65:c9           02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags
 108 47.664538   AmazonTechno_87:65:c9           02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags
 109 47.670170   AmazonTechno_87:65:c9           02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags
```

```
▸ Frame 47: Packet, 24 bytes on wire (192 bits), 24 bytes captured (192 bits
▾ IEEE 802.11 Null function (No data), Flags: .......T
    Type/Subtype: Null function (No data) (0x0024)
  ▾ Frame Control Field: 0x4801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    ▾ Flags: 0x01
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fro
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
```

```
0000  48 01 66 02 18 64 72 e8  e0 60 76 00 29 a7 48 ca   H·f··dr· ·`v·)·H·
0010  18 64 72 e8 e0 60 f0 51                            ·dr··`·Q
```

capture.pcap
Packets: 111 · Displayed: 17 (15.3%)
Profile: Default



capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 2
```

```
                        Destination              Protocol  Length Info
48:ca                   HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1311, FN=0, Flags=.......T
48:ca                   HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1316, FN=0, Flags=...P...T
48:ca                   HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1316, FN=0, Flags=...PR..T
48:ca                   HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1317, FN=0, Flags=.......T
48:ca                   HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1320, FN=0, Flags=.......T
48:ca                   HewlettPacka_e8:e0:60    802.11      24 Null function (No data), SN=1644, FN=0, Flags=....R..T
erver-24_4a:14:ab:ff    Broadcast                MDP         80 MDP
erver-24_4a:14:ab:ff    Broadcast                LLC        108 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0…
_87:65:c9               02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags=.p.....T
_87:65:c9               02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags=.p.....T
_87:65:c9               02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags=.p.....T
_87:65:c9               02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags=.p.....T
_87:65:c9               02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags=.p.....T
_87:65:c9               02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags=.p.....T
_87:65:c9               02:00:00:00:00:04        802.11      90 QoS Data, SN=599, FN=0, Flags=.p.....T
```

```
▸ Frame 47: Packet, 24 bytes on wire (192 bits), 24 bytes captured (192 bits
▾ IEEE 802.11 Null function (No data), Flags: .......T
    Type/Subtype: Null function (No data) (0x0024)
  ▾ Frame Control Field: 0x4801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    ▾ Flags: 0x01
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fro
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
```

```
0000  48 01 66 02 18 64 72 e8  e0 60 76 00 29 a7 48 ca   H·f··dr· ·`v·)·H·
0010  18 64 72 e8 e0 60 f0 51                            ·dr··`·Q
```

When the filter wlan.fc.type == 2 is applied, the capture shows **Data frames**, including **Null Data** and **QoS Data** frames.

**Encapsulation of user data:**

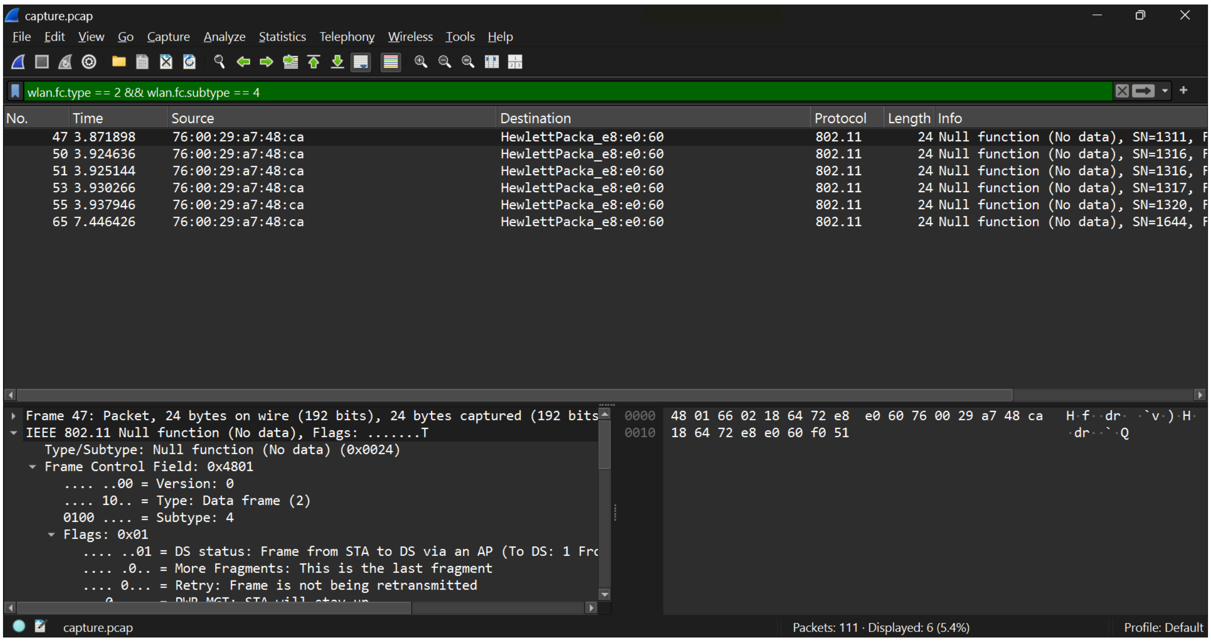
- The **802.11 Data frame** encapsulates user data (from higher layers like IP, TCP, or UDP) for wireless transmission.
- The data from upper layers is carried within the **frame body**, similar to how Ethernet carries payloads.
- Inside the payload, you'll find **LLC (Logical Link Control)** and **SNAP (Subnetwork Access Protocol)** headers, followed by the higher-layer data (like IP packets).

**Additional headers added at the 802.11 layer:**

1. **MAC Header** – contains:
    - Frame Control (type, subtype, flags)
    - Duration/ID
    - Address fields (Source, Destination, BSSID, Receiver/Transmitter)
    - Sequence Control
    - QoS Control (if QoS Data frame)
2. **Frame Body** – contains user data (IP, ARP, TCP, UDP, etc.)

3. **FCS (Frame Check Sequence)** – for error detection.
   **Explanation:**
   802.11 adds these extra headers to manage **wireless-specific functions** such as mobility, addressing through an AP, retransmissions, and quality of service. This encapsulation allows reliable delivery of user data over a shared and error-prone wireless medium.

**9.**


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

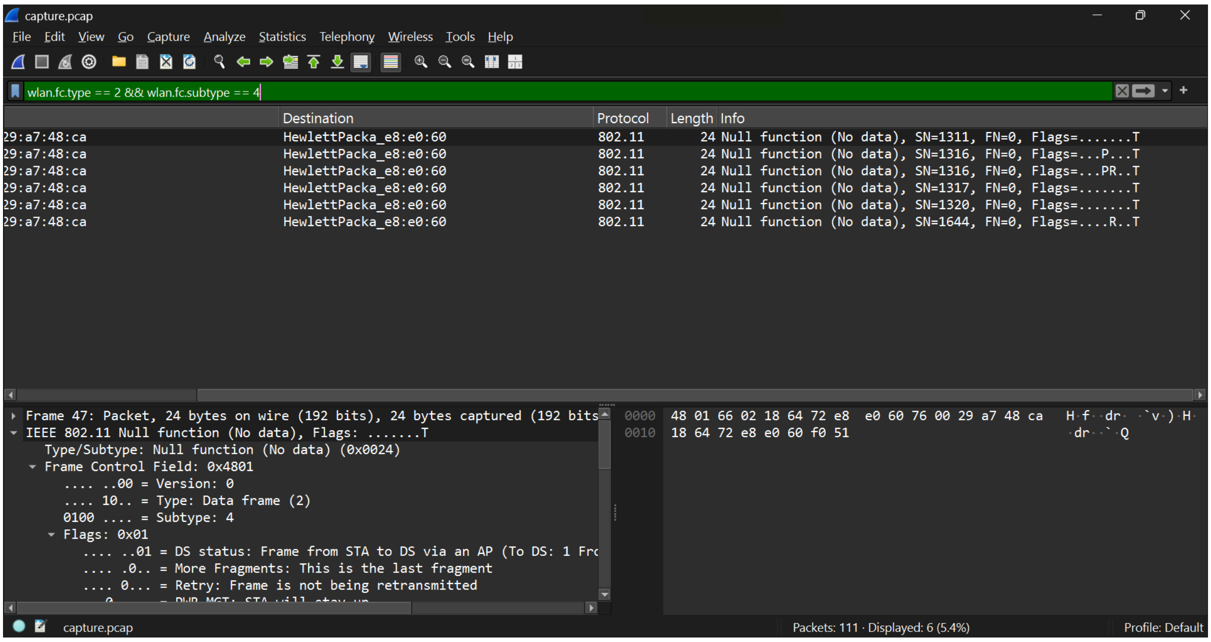
wlan.fc.type == 2 && wlan.fc.subtype == 4

```
No.   Time      Source              Destination           Protocol  Length Info
   47 3.871898  76:00:29:a7:48:ca   HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1311, F
   50 3.924636  76:00:29:a7:48:ca   HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1316, F
   51 3.925144  76:00:29:a7:48:ca   HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1316, F
   53 3.930266  76:00:29:a7:48:ca   HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1317, F
   55 3.937946  76:00:29:a7:48:ca   HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1320, F
   65 7.446426  76:00:29:a7:48:ca   HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1644, F
```

```
▸ Frame 47: Packet, 24 bytes on wire (192 bits), 24 bytes captured (192 bits
▾ IEEE 802.11 Null function (No data), Flags: .......T
    Type/Subtype: Null function (No data) (0x0024)
  ▾ Frame Control Field: 0x4801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    ▾ Flags: 0x01
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fro
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
```

```
0000  48 01 66 02 18 64 72 e8  e0 60 76 00 29 a7 48 ca   H·f··dr· ·`v·)·H·
0010  18 64 72 e8 e0 60 f0 51                            ·dr··`·Q
```

capture.pcap    Packets: 111 · Displayed: 6 (5.4%)    Profile: Default


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type == 2 && wlan.fc.subtype == 4

```
                   Destination            Protocol  Length Info
29:a7:48:ca        HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1311, FN=0, Flags=.......T
29:a7:48:ca        HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1316, FN=0, Flags=...P...T
29:a7:48:ca        HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1316, FN=0, Flags=...PR..T
29:a7:48:ca        HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1317, FN=0, Flags=.......T
29:a7:48:ca        HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1320, FN=0, Flags=.......T
29:a7:48:ca        HewlettPacka_e8:e0:60  802.11       24 Null function (No data), SN=1644, FN=0, Flags=....R..T
```

```
▸ Frame 47: Packet, 24 bytes on wire (192 bits), 24 bytes captured (192 bits
▾ IEEE 802.11 Null function (No data), Flags: .......T
    Type/Subtype: Null function (No data) (0x0024)
  ▾ Frame Control Field: 0x4801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    ▾ Flags: 0x01
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fro
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
```

```
0000  48 01 66 02 18 64 72 e8  e0 60 76 00 29 a7 48 ca   H·f··dr· ·`v·)·H·
0010  18 64 72 e8 e0 60 f0 51                            ·dr··`·Q
```

capture.pcap    Packets: 111 · Displayed: 6 (5.4%)    Profile: Default

When the filter wlan.fc.type == 2 && wlan.fc.subtype == 4 is applied, the capture shows several **Null Data (Null Function)** frames. These frames are special data-type frames that carry **no payload**.

**Purpose of Null Data frames:**

- Null data frames are used by **client stations (STAs)** to communicate **power management states** to the **Access Point (AP)** without sending actual data.
- They serve as control signals to indicate when a device is entering or leaving a low-power (sleep) mode.

**Power Management bit:**

- The **Power Management (PM)** bit is located in the **Frame Control field** of the 802.11 header.
- **PM = 1:** The station is entering **Power Save (sleep)** mode.

- The AP buffers incoming packets for that station until it wakes up.

- **PM = 0:** The station is **active** and ready to receive frames immediately.

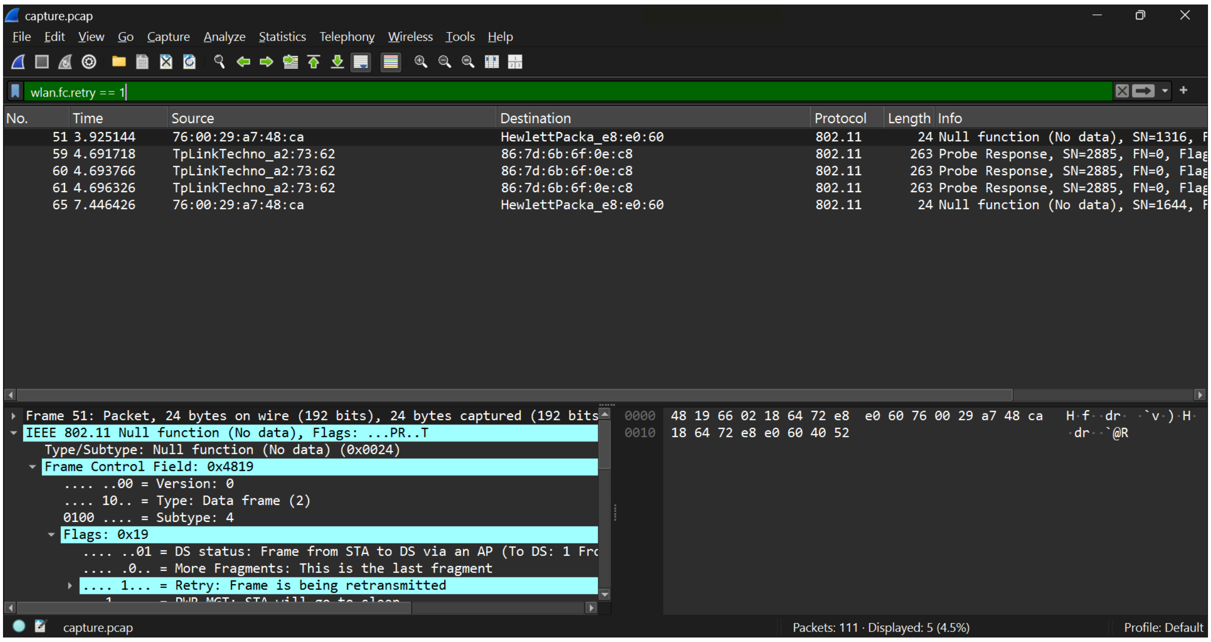
**How stations use this mechanism:**

1. A client sends a **Null Data frame** with **PM = 1** to notify the AP it is going to sleep.
2. The AP buffers all traffic destined for that client.
3. When the client wakes up, it sends another **Null Data frame** with **PM = 0**, signaling it is awake and ready to receive the buffered packets.

**In the capture:**

Frames from source 76:00:29:a7:48:ca to destination HewlettPacka_e8:e0:60 show **Null function (No data)**, indicating this power management signaling between a station and an AP.

**10.**



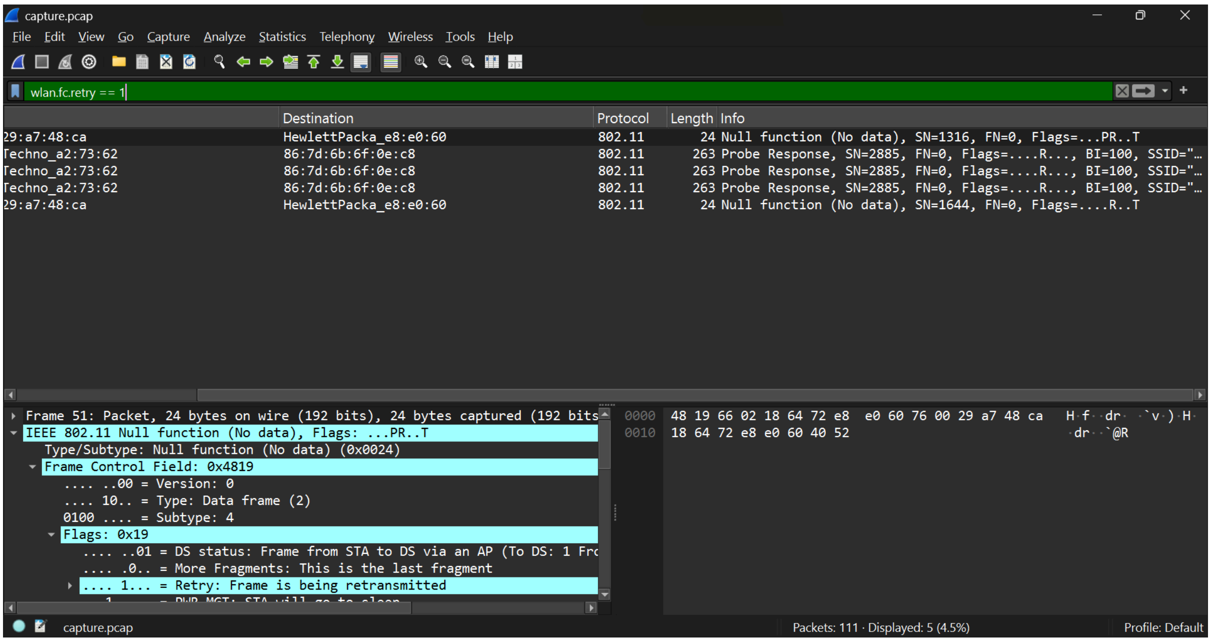
wlan.fc.retry == 1

```
No.   Time       Source                Destination             Protocol  Length Info
   51 3.925144   76:00:29:a7:48:ca     HewlettPacka_e8:e0:60   802.11      24 Null function (No data), SN=1316, F
   59 4.691718   TpLinkTechno_a2:73:62 86:7d:6b:6f:0e:c8       802.11     263 Probe Response, SN=2885, FN=0, Flag
   60 4.693766   TpLinkTechno_a2:73:62 86:7d:6b:6f:0e:c8       802.11     263 Probe Response, SN=2885, FN=0, Flag
   61 4.696326   TpLinkTechno_a2:73:62 86:7d:6b:6f:0e:c8       802.11     263 Probe Response, SN=2885, FN=0, Flag
   65 7.446426   76:00:29:a7:48:ca     HewlettPacka_e8:e0:60   802.11      24 Null function (No data), SN=1644, F
```

```
> Frame 51: Packet, 24 bytes on wire (192 bits), 24 bytes captured (192 bits
v IEEE 802.11 Null function (No data), Flags: ...PR..T
    Type/Subtype: Null function (No data) (0x0024)
  v Frame Control Field: 0x4819
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    v Flags: 0x19
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fro
        .... .0.. = More Fragments: This is the last fragment
      > .... 1... = Retry: Frame is being retransmitted
        ...1 .... = PWR MGT: STA will go to sleep
```

```
0000  48 19 66 02 18 64 72 e8  e0 60 76 00 29 a7 48 ca   H·f··dr· ·`v·)·H·
0010  18 64 72 e8 e0 60 40 52                             ·dr··`@R
```

capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packets: 111 · Displayed: 5 (4.5%)
Profile: Default



wlan.fc.retry == 1

```
                                      Destination             Protocol  Length Info
29:a7:48:ca                           HewlettPacka_e8:e0:60   802.11      24 Null function (No data), SN=1316, FN=0, Flags=...PR..T
Techno_a2:73:62                       86:7d:6b:6f:0e:c8       802.11     263 Probe Response, SN=2885, FN=0, Flags=....R..., BI=100, SSID="…
Techno_a2:73:62                       86:7d:6b:6f:0e:c8       802.11     263 Probe Response, SN=2885, FN=0, Flags=....R..., BI=100, SSID="…
Techno_a2:73:62                       86:7d:6b:6f:0e:c8       802.11     263 Probe Response, SN=2885, FN=0, Flags=....R..., BI=100, SSID="…
29:a7:48:ca                           HewlettPacka_e8:e0:60   802.11      24 Null function (No data), SN=1644, FN=0, Flags=....R..T
```

```
> Frame 51: Packet, 24 bytes on wire (192 bits), 24 bytes captured (192 bits
v IEEE 802.11 Null function (No data), Flags: ...PR..T
    Type/Subtype: Null function (No data) (0x0024)
  v Frame Control Field: 0x4819
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    v Flags: 0x19
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fro
        .... .0.. = More Fragments: This is the last fragment
      > .... 1... = Retry: Frame is being retransmitted
        ...1 .... = PWR MGT: STA will go to sleep
```

```
0000  48 19 66 02 18 64 72 e8  e0 60 76 00 29 a7 48 ca   H·f··dr· ·`v·)·H·
0010  18 64 72 e8 e0 60 40 52                             ·dr··`@R
```

capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packets: 111 · Displayed: 5 (4.5%)
Profile: Default

When the filter wlan.fc.retry == 1 is applied, the capture shows several **retransmitted frames**, such as **Null Function (No data)** frames and **Probe Response** frames with the retry flag set.

**Reason for retransmissions in Wi-Fi:**

Retransmissions occur when a sender (station or access point) does **not receive an acknowledgment**

**(ACK)** for a transmitted frame within a specified time. To ensure reliable delivery, the sender retransmits the frame.

**Common causes of retransmissions:**

1. **Weak signal strength** or **low RSSI** (distance from AP or physical obstacles).
2. **Radio interference** from other Wi-Fi networks or electronic devices.
3. **Channel congestion** due to multiple users sharing the same frequency.
4. **Collisions** caused by overlapping transmissions in busy environments.

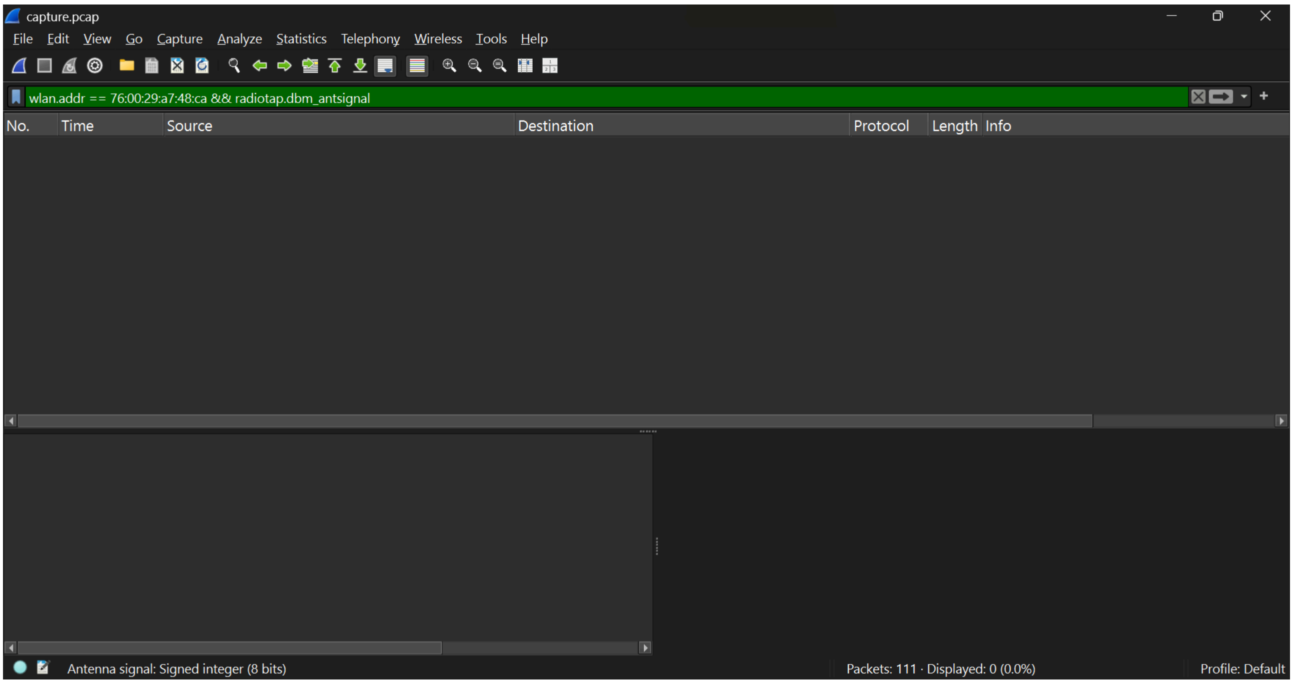
**Interpretation of frequent retries:**

- A high number of retransmissions indicates **poor wireless conditions**, such as noise, interference, or low signal quality.
- It can also point to **overlapping channels** or **network congestion**, leading to degraded throughput and latency.

**In the capture:**

Frames like those from source 76:00:29:a7:48:ca show the **Retry bit set (Flags: ....PR..T)**, confirming retransmissions caused by missed ACKs or weak signal conditions between the station and AP.

**11.**

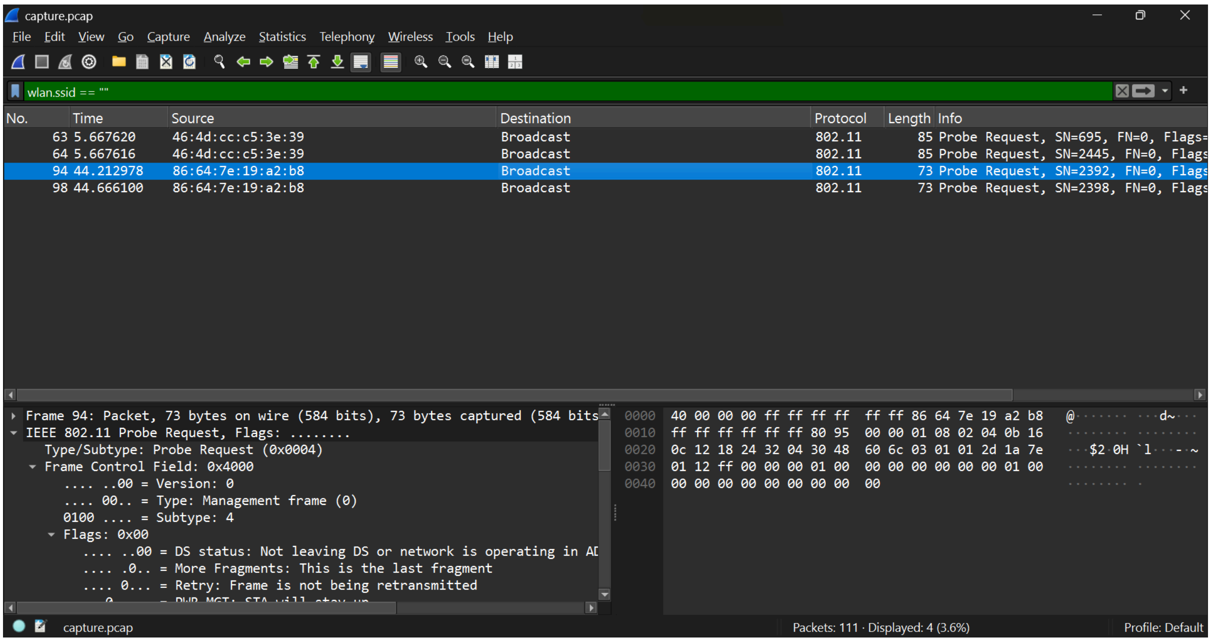

capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No.
Time
Source
Destination
Protocol
Length
Info
Profile: Default

wlan.addr == 76:00:29:a7:48:ca && radiotap.dbm_antsignal

Antenna signal: Signed integer (8 bits)

Packets: 111 · Displayed: 0 (0.0%)

**12.**



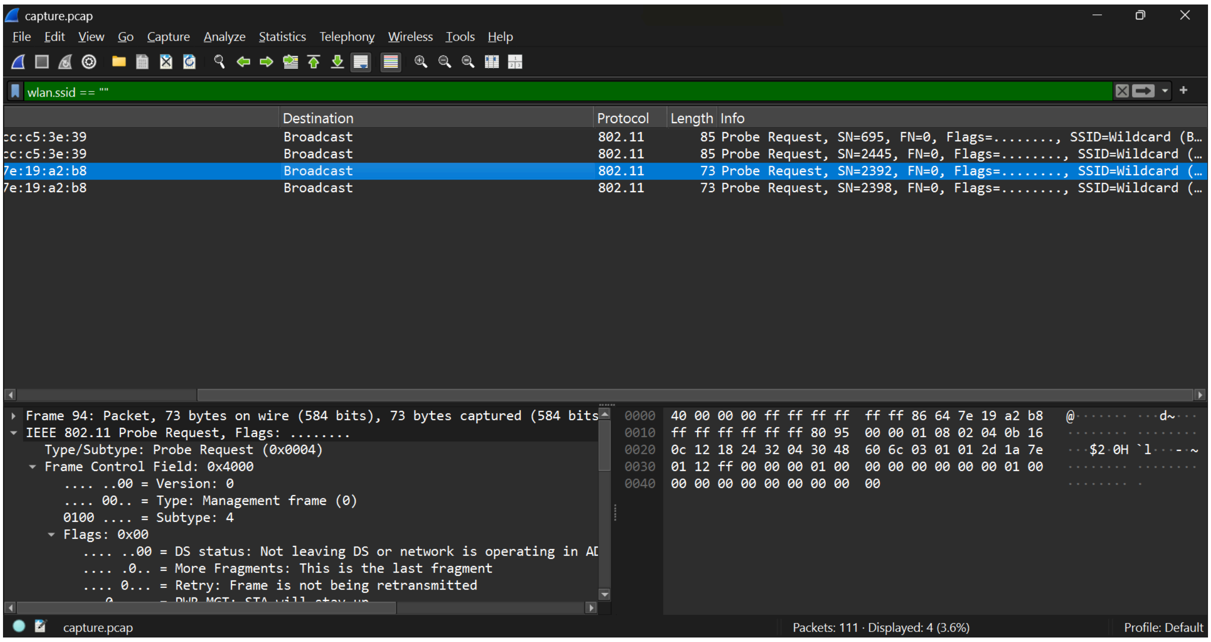
wlan.ssid == ""

```
No.   Time       Source              Destination  Protocol  Length Info
   63 5.667620   46:4d:cc:c5:3e:39   Broadcast    802.11       85 Probe Request, SN=695, FN=0, Flags=
   64 5.667616   46:4d:cc:c5:3e:39   Broadcast    802.11       85 Probe Request, SN=2445, FN=0, Flags
   94 44.212978  86:64:7e:19:a2:b8   Broadcast    802.11       73 Probe Request, SN=2392, FN=0, Flags
   98 44.666100  86:64:7e:19:a2:b8   Broadcast    802.11       73 Probe Request, SN=2398, FN=0, Flags
```

```
> Frame 94: Packet, 73 bytes on wire (584 bits), 73 bytes captured (584 bits
v IEEE 802.11 Probe Request, Flags: ........
    Type/Subtype: Probe Request (0x0004)
  v Frame Control Field: 0x4000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0100 .... = Subtype: 4
    v Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
```

```
0000  40 00 00 00 ff ff ff ff  ff ff 86 64 7e 19 a2 b8   @·······  ···d~···
0010  ff ff ff ff ff ff 80 95  00 00 01 08 02 04 0b 16   ········  ········
0020  0c 12 18 24 32 04 30 48  60 6c 03 01 01 2d 1a 7e   ···$2·0H `l···-·~
0030  01 12 ff 00 00 00 01 00  00 00 00 00 00 00 01 00   ········  ········
0040  00 00 00 00 00 00 00 00  00                        ········  ·
```

capture.pcap    Packets: 111 · Displayed: 4 (3.6%)    Profile: Default



wlan.ssid == ""

```
                    Destination  Protocol  Length Info
cc:c5:3e:39         Broadcast    802.11       85 Probe Request, SN=695, FN=0, Flags=........, SSID=Wildcard (B…
cc:c5:3e:39         Broadcast    802.11       85 Probe Request, SN=2445, FN=0, Flags=........, SSID=Wildcard (…
7e:19:a2:b8         Broadcast    802.11       73 Probe Request, SN=2392, FN=0, Flags=........, SSID=Wildcard (…
7e:19:a2:b8         Broadcast    802.11       73 Probe Request, SN=2398, FN=0, Flags=........, SSID=Wildcard (…
```

```
> Frame 94: Packet, 73 bytes on wire (584 bits), 73 bytes captured (584 bits
v IEEE 802.11 Probe Request, Flags: ........
    Type/Subtype: Probe Request (0x0004)
  v Frame Control Field: 0x4000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0100 .... = Subtype: 4
    v Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
```

```
0000  40 00 00 00 ff ff ff ff  ff ff 86 64 7e 19 a2 b8   @·······  ···d~···
0010  ff ff ff ff ff ff 80 95  00 00 01 08 02 04 0b 16   ········  ········
0020  0c 12 18 24 32 04 30 48  60 6c 03 01 01 2d 1a 7e   ···$2·0H `l···-·~
0030  01 12 ff 00 00 00 01 00  00 00 00 00 00 00 01 00   ········  ········
0040  00 00 00 00 00 00 00 00  00                        ········  ·
```

capture.pcap    Packets: 111 · Displayed: 4 (3.6%)    Profile: Default

When the filter wlan.ssid == "" is applied, the capture shows **Probe Request** or **Beacon** frames where the **SSID field is empty**.

**Meaning of empty SSID:**

- An **empty SSID** (also called a **hidden SSID**) means the access point (AP) is **not broadcasting its network name** in beacon frames.
- Such networks are referred to as **hidden networks** because they conceal their SSID from casual scanning.
- Instead of advertising the SSID in beacon frames, the AP leaves the SSID field **blank ("")**, making the network invisible in the default Wi-Fi list.

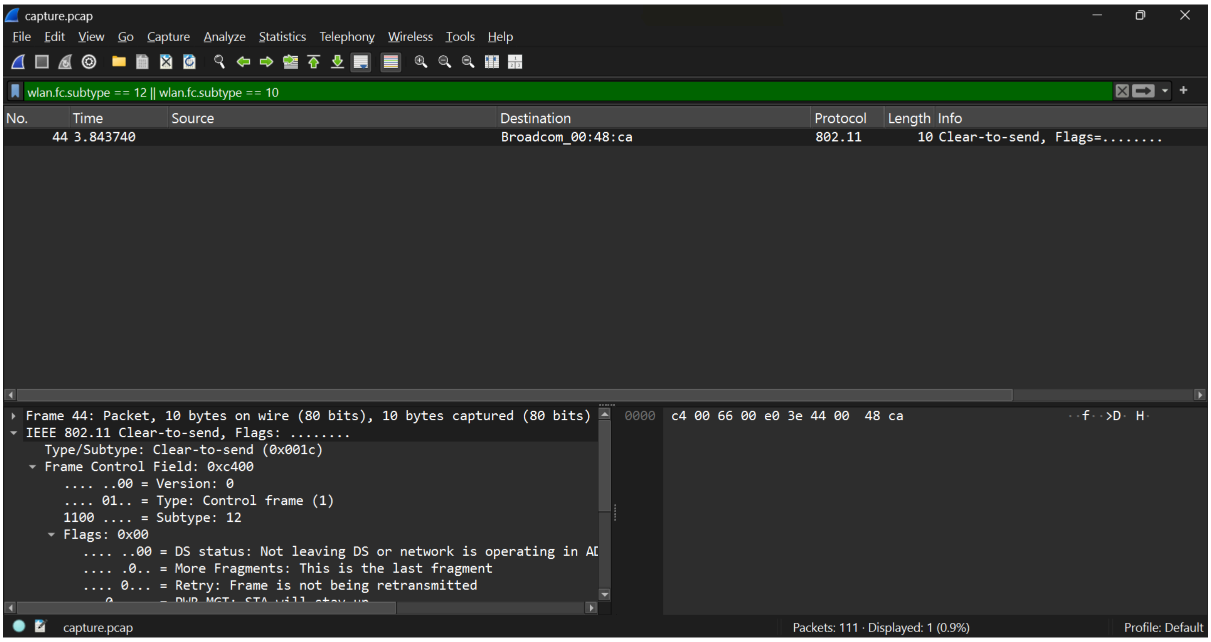
**How clients can still discover or connect:**

1. **Manual configuration:**
   - A client device that already knows the SSID can still connect by **sending a directed Probe Request** with the **specific SSID name** instead of the wildcard value.
   - The AP responds with a **Probe Response** if the SSID matches, allowing the device to connect.
2. **Stored profiles:**

- Devices remember previously connected hidden SSIDs and periodically probe for them automatically.

**In the capture:**
Frames with SSID: **Wildcard (Broadcast)** and **empty SSID (“”)** indicate clients searching for any available or hidden networks. This mechanism allows connection even when the network name isn’t openly advertised.

**13.**


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.subtype == 12 || wlan.fc.subtype == 10

No.  Time      Source  Destination          Protocol  Length Info
  44 3.843740          Broadcom_00:48:ca    802.11        10 Clear-to-send, Flags=........

Frame 44: Packet, 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
IEEE 802.11 Clear-to-send, Flags: ........
  Type/Subtype: Clear-to-send (0x001c)
  Frame Control Field: 0xc400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1100 .... = Subtype: 12
    Flags: 0x00
      .... ..00 = DS status: Not leaving DS or network is operating in AD
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted

0000  c4 00 66 00 e0 3e 44 00  48 ca        ··f··>D· H·

capture.pcap    Packets: 111 · Displayed: 1 (0.9%)    Profile: Default
```

When the filter wlan.fc.subtype == 12 || wlan.fc.subtype == 10 is applied, the capture shows **Control and Management frames**, such as the **Clear-to-Send (CTS)** or **Deauthentication/Disassociation** frames depending on the traffic captured.
Specifically for **Deauthentication (subtype 12)** and **Disassociation (subtype 10)** frames in IEEE 802.11:

**What triggers these frames:**

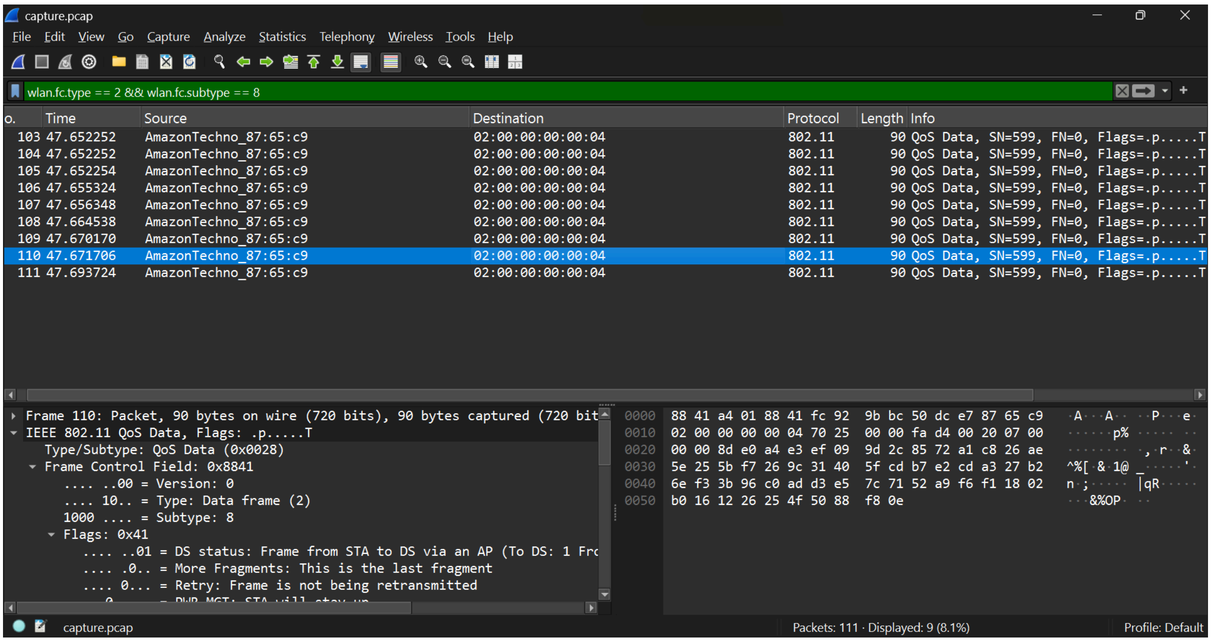
1. **Deauthentication frames** are sent when:
   - A client or AP wants to **terminate authentication** (logout).
   - The connection is closed intentionally (manual disconnect or roaming).
   - The AP enforces disconnection due to **idle timeout**, **security mismatch**, or **policy violation**.
   - During roaming, when the client moves to another AP.
2. **Disassociation frames** are sent when:
   - The client or AP wishes to **end the association** but keep the authentication intact.
   - This typically happens **before** deauthentication or when switching between APs.

**What happens after these frames are sent:**

- Once a **Disassociation** frame is sent, the client is no longer associated with the AP and cannot send or receive data frames.
- Once a **Deauthentication** frame is sent, the client is completely disconnected and must **restart the connection process** (authentication → association → data transfer).
- The AP releases resources (buffers, AID) used by that client.

**In the capture:**
The displayed frame shows a **Control-type CTS (Clear-to-Send)** frame under the same filter, which is closely related to managing the transmission channel. However, when **Deauthentication or Disassociation** frames are present, they indicate **session termination events** between a station and an access point, marking the end of a connection in the 802.11 link layer.

**14.**


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 2 && wlan.fc.subtype == 8
```

```
o.  Time       Source                 Destination         Protocol  Length Info
103 47.652252  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
104 47.652252  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
105 47.652254  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
106 47.655324  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
107 47.656348  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
108 47.664538  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
109 47.670170  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
110 47.671706  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
111 47.693724  AmazonTechno_87:65:c9  02:00:00:00:00:04   802.11        90 QoS Data, SN=599, FN=0, Flags=.p.....T
```

```
> Frame 110: Packet, 90 bytes on wire (720 bits), 90 bytes captured (720 bit
v IEEE 802.11 QoS Data, Flags: .p.....T
    Type/Subtype: QoS Data (0x0028)
  v Frame Control Field: 0x8841
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    v Flags: 0x41
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fro
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
```

```
0000  88 41 a4 01 88 41 fc 92  9b bc 50 dc e7 87 65 c9   ·A···A·· ··P···e·
0010  02 00 00 00 00 04 70 25  00 00 fa d4 00 20 07 00   ······p% ·····  ··
0020  00 00 8d e0 a4 e3 ef 09  9d 2c 85 72 a1 c8 26 ae   ········ ·,·r··&·
0030  5e 25 5b f7 26 9c 31 40  5f cd b7 e2 cd a3 27 b2   ^%[·&·1@ _·····'·
0040  6e f3 3b 96 c0 ad d3 e5  7c 71 52 a9 f6 f1 18 02   n·;····· |qR·····
0050  b0 16 12 26 25 4f 50 88  f8 0e                     ···&%OP· ··
```

```
capture.pcap                    Packets: 111 · Displayed: 9 (8.1%)                    Profile: Default
```

When the filter wlan.fc.type == 2 && wlan.fc.subtype == 8 is applied, the capture shows **QoS (Quality of Service) Data frames**, such as those transmitted from source AmazonTechno_87:65:c9 to destination 02:00:00:00:00:04.

**Role of Quality of Service (QoS) in Wi-Fi Communication**

QoS in IEEE 802.11 networks (defined in the **802.11e** amendment) is designed to **prioritize certain types of network traffic** to ensure that time-sensitive data receives better treatment than normal data.

It enables efficient sharing of the wireless medium by assigning **different priority levels** to various traffic categories.

QoS frames contain a **QoS Control field** that defines the traffic category or **Access Category (AC):**

1. **AC_VO (Voice)** – highest priority
2. **AC_VI (Video)** – high priority
3. **AC_BE (Best Effort)** – normal traffic (e.g., web browsing)
4. **AC_BK (Background)** – lowest priority (e.g., file downloads)

**How QoS Works**

- Wi-Fi uses **EDCA (Enhanced Distributed Channel Access)**, which gives each category different contention parameters (shorter wait time for higher priority).
- Frames belonging to higher priority traffic (like voice or video) get **faster access to the medium**, reducing delay and jitter.
- Lower priority frames wait longer, ensuring smooth transmission for critical real-time applications.

**Traffic Types that Benefit from QoS Prioritization**

- **Voice over IP (VoIP)** calls – need very low delay and jitter.
- **Video conferencing or streaming** – benefits from consistent throughput and minimal packet loss.
- **Online gaming** – improved responsiveness due to low latency.

Other traffic like web browsing or file transfers (best effort/background) can tolerate slight delays, so they receive lower priority.

**In the Capture**

The QoS Data frames from AmazonTechno_87:65:c9 indicate that the device is transmitting user data with QoS enabled, likely classifying packets into one of the above access categories to optimize wireless performance.

**15.**

**Common observations (2.4 GHz):**

- Channels mapped to frequencies:
  - 2412 MHz → Channel 1

    - 2437 MHz → Channel 6
    - 2462 MHz → Channel 11
- Most small deployments use **channels 1, 6, 11** to avoid overlap.

**How overlapping channels or interference degrade performance:**

- **Overlapping channels** (e.g., channel 3 overlapping 1 and 6) cause adjacent-channel interference: signals partially overlap in frequency and disrupt each other, increasing collisions and retransmits.
- **Co-channel interference** (many APs on same channel) increases contention — devices defer more often, throughput per device drops.
- **Non-Wi-Fi interference** (microwaves, Bluetooth, cordless phones) raises noise floor, reducing SNR and effective throughput.
- **Result:** increased latency, more retries, rate fallback, reduced throughput and reliability — worst impact is on latency-sensitive traffic (VoIP, gaming).