Project 04 – Wireshark 802.11 Wireless Analysis

Beacon Frames, Authentication, Association & Roaming Behavior

1. Overview

This report presents an in-depth analysis of IEEE 802.11 wireless traffic captured from a real home Wi-Fi environment. Unlike wired Ethernet analysis, this investigation focuses on Layer-2 wireless communication, including how wireless devices discover access points, authenticate, associate, exchange data, roam between access points, and recover from failed connection attempts.

Using Wireshark's 802.11 protocol dissection, I examined management, control, and data frames to reconstruct the complete lifecycle of a wireless client interacting with multiple access points. The analysis reflects real-world scenarios encountered in wireless troubleshooting, SOC investigations, and network forensics.

2. Analysis Environment

• Analysis Tool: Wireshark
• Capture File: Wireshark_802_11.pcap
• Wireless Standard: IEEE 802.11g
• Observed Access Points (SSIDs):
o 30 Munroe St
o linksys_ses_24086
• Wireless Host (STA) MAC Address: 00:13:02:d1:b6:4f
• Primary Access Point (BSSID): 00:16:b6:f7:1d:51

3. Initial Packet Capture Review

At the beginning of the capture, I observed that the wireless host was already associated with the **30 Munroe St** access point. The trace contains beacon frames from multiple access points, management frames, and wireless data traffic, providing visibility into both intended traffic and ambient wireless activity on the channel.

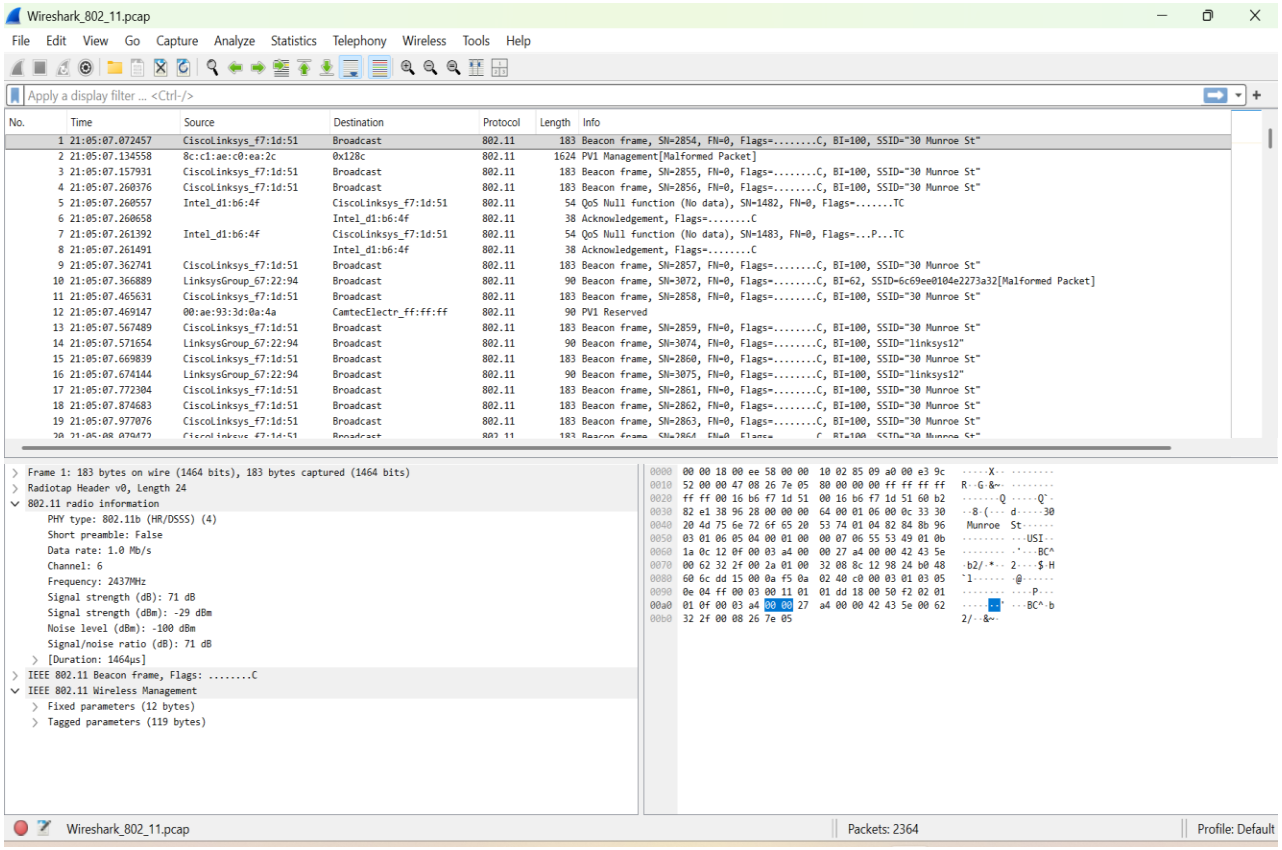

Figure 1: Screenshot of the resulting Wireshark display after opening the .pcap file (Screenshot file: *wifi-startup.png*)

4. Wireless Data Transmission over 802.11

During the capture, I observed the wireless host initiating two HTTP requests over the Wi-Fi connection:

• At 24.82 seconds, the host sends an HTTP GET request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt

• At 32.82 seconds, the host sends an HTTP GET request to http://www.cs.umass.edu

These frames confirmed that the wireless connection was functioning correctly and that TCP/IP traffic was successfully encapsulated within 802.11 data frames prior to the roaming event.

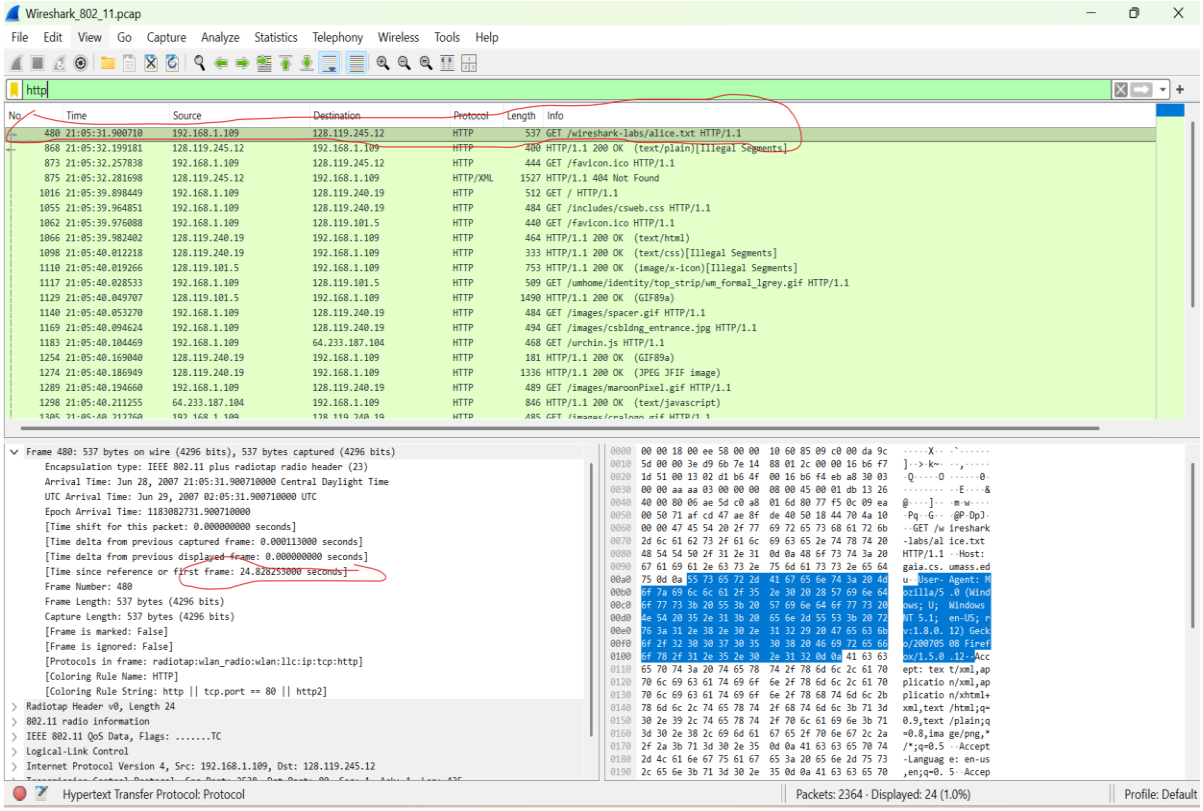

Figure 2: HTTP request made by the host at 24.82s to *alice.txt*
(Screenshot file: *http-request-1.png*)

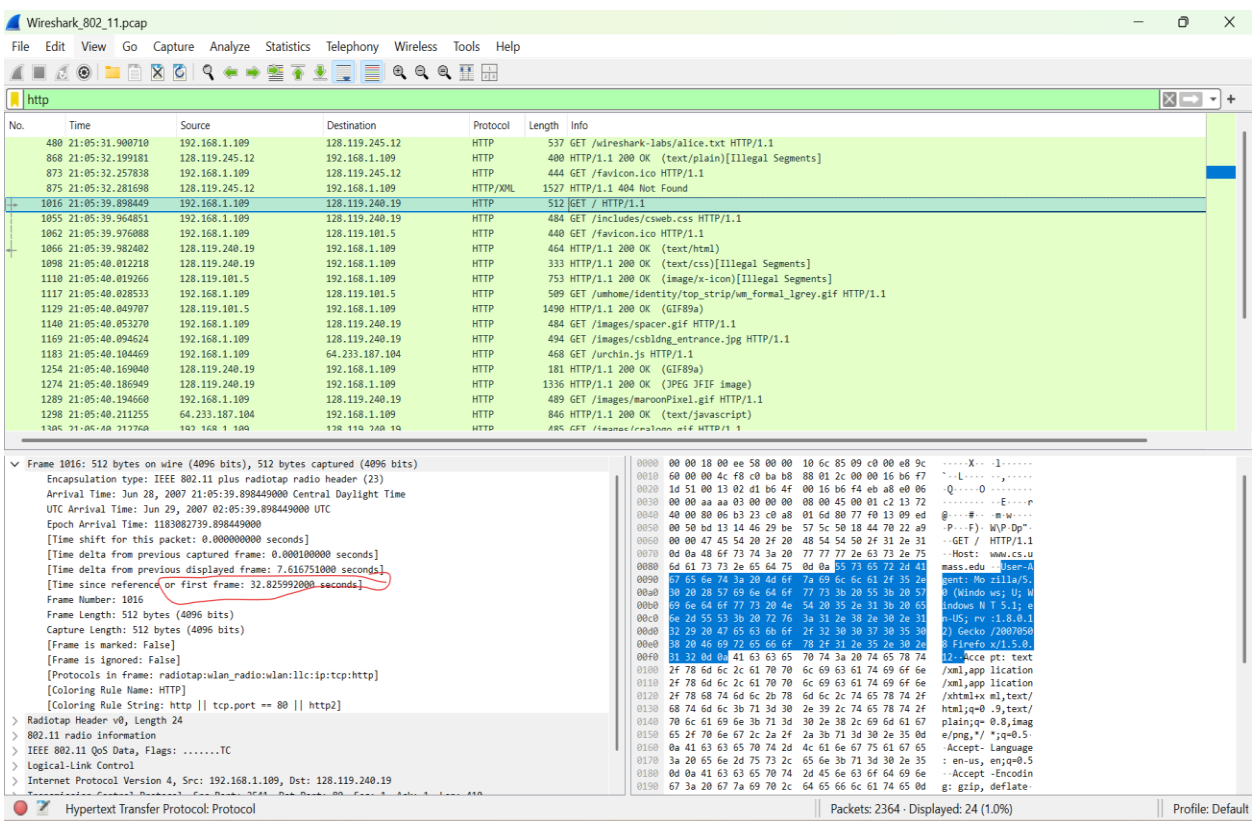

Figure 3: HTTP request made by the host at 32.82s to www.cs.umass.edu
(Screenshot file: *http-request-2.png*)

5. Roaming Attempt between Access Points

At approximately 49.58 seconds, I observed the wireless host disconnecting from the **30 Munroe St** access point and attempting to connect to the **linksys_ses_24086** access point. This roaming attempt was unsuccessful, and the host was unable to complete the association process with the new access point.

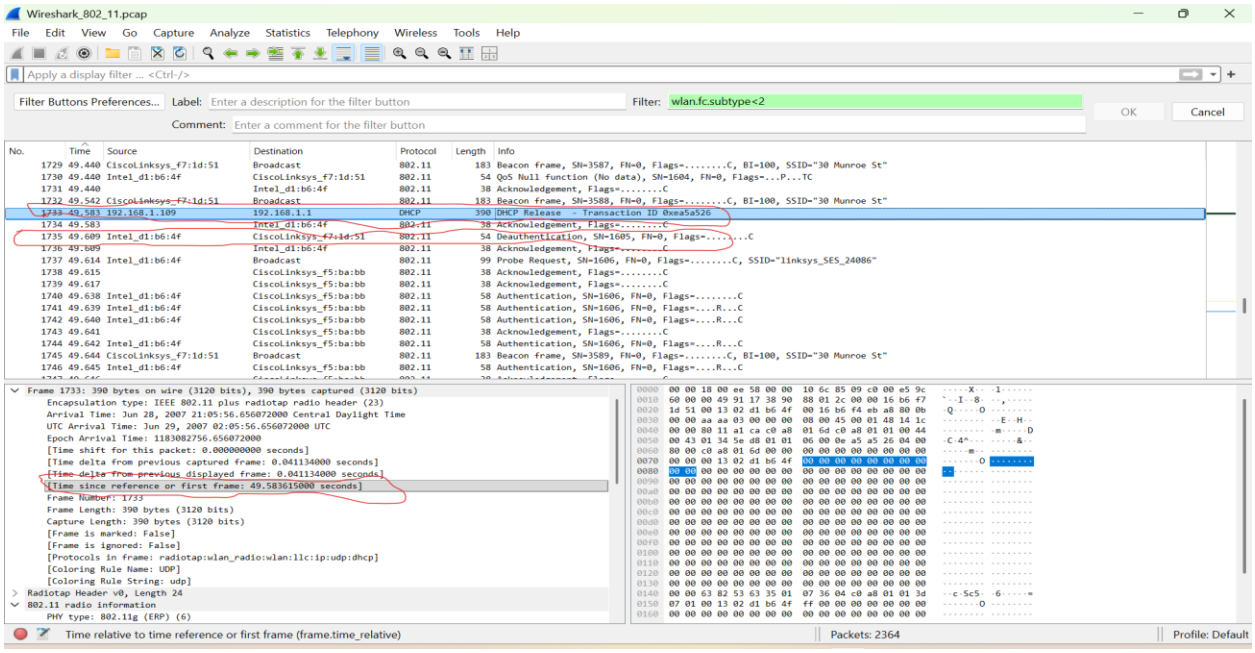

Figure 4: Host disconnects from *30 Munroe St* and attempts to connect to *linksys_ses_24086* (Screenshot file: *roam-attempt.png*)

After multiple failed attempts, I observed that the host abandoned the roaming attempt.

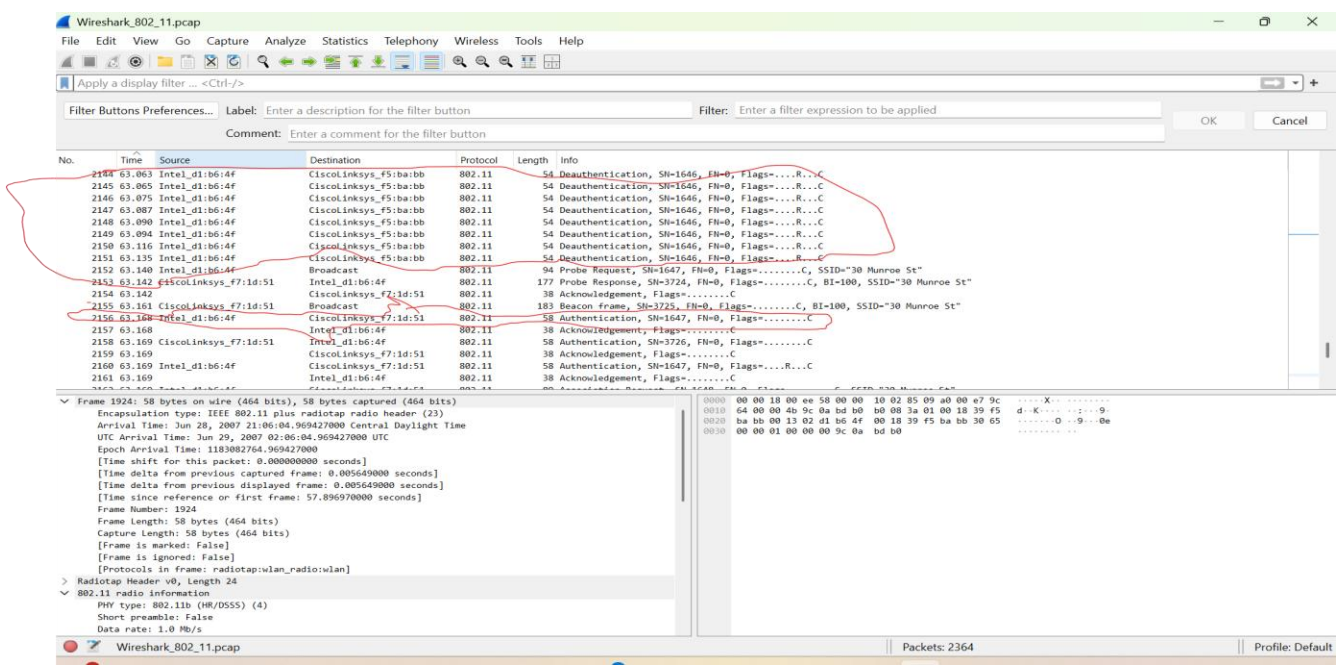

Figure 5: Host gives up associating with *linksys_ses_24086* and later reconnects to *30 Munroe St* (Screenshot file: *failed-association.png*)

6. Beacon Frame Analysis

6.1 SSIDs Observed

By filtering for beacon frames (wlan.fc.type_subtype == 0x08), I identified two access points broadcasting most frequently during the capture:

- 30 Munroe St
- linksys_ses_24086

These SSIDs were determined by examining the SSID information element within the beacon frames.

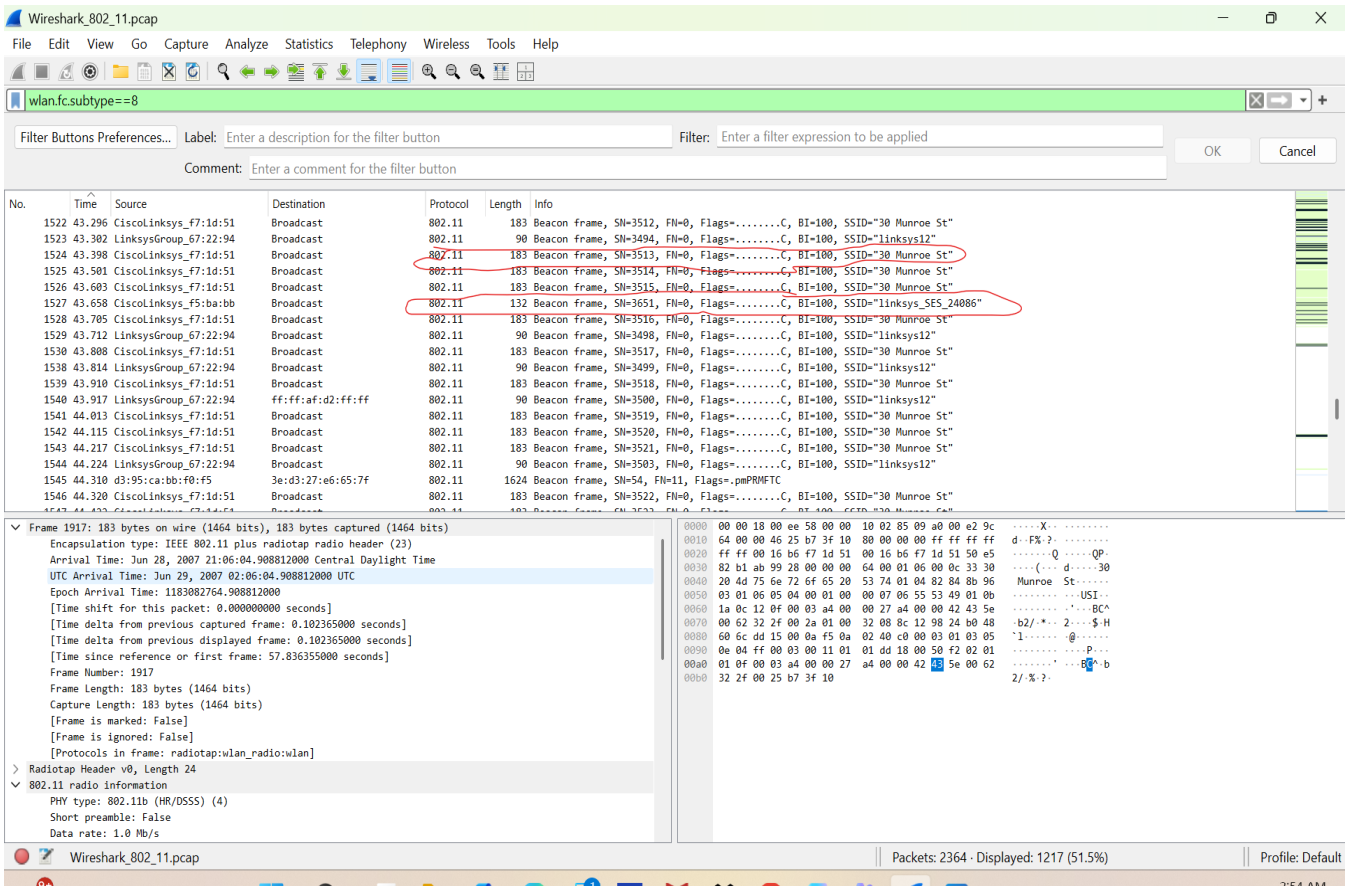

Figure 6: SSIDs of the two access points involved in the capture
(Screenshot file: *ssid-list.png*)

6.2 Beacon Interval

Inspection of the beacon interval field shows that both access points transmit beacon frames at an interval of approximately **0.1024 seconds**, which is consistent with standard 802.11 behavior.

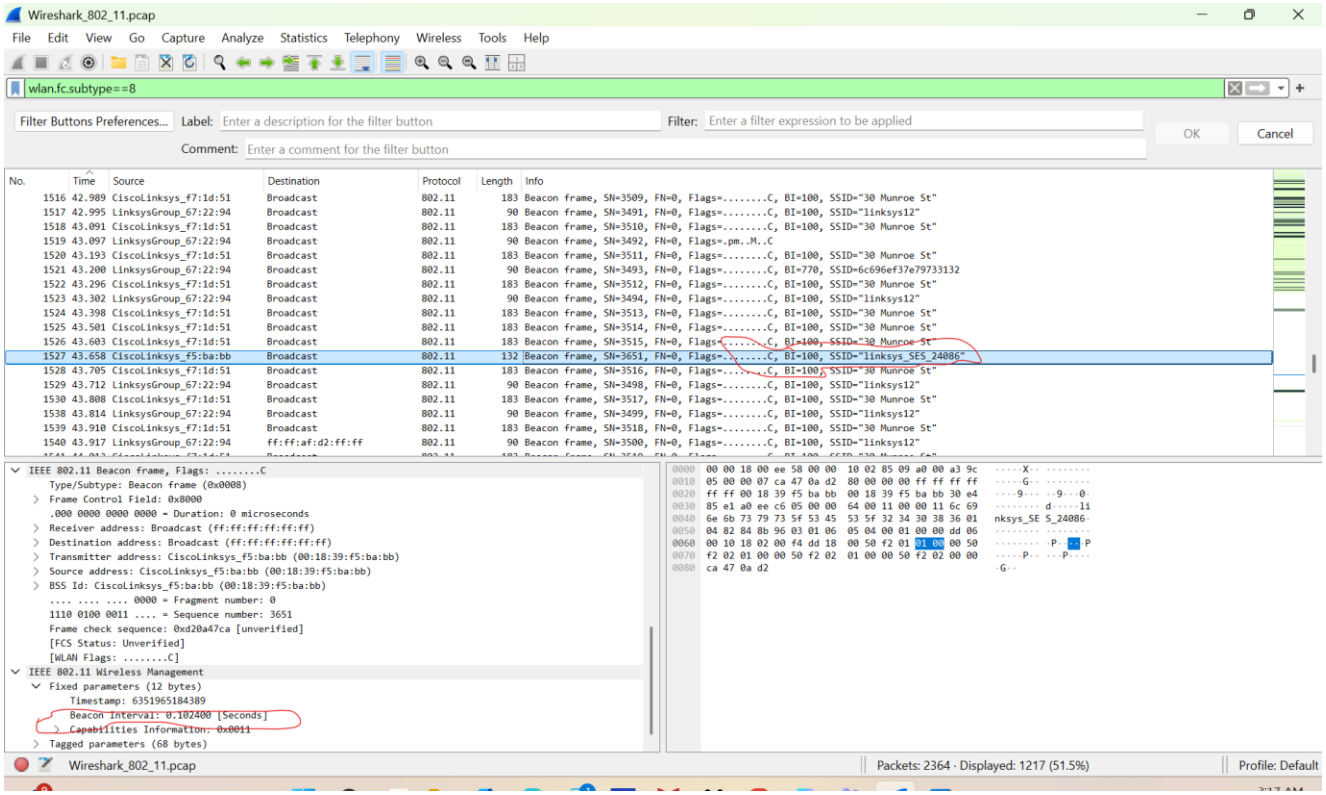

Figure 7a: Beacon interval for *linksys_ses_24086*
(Screenshot file: *beacon-interval-linksys.png*)

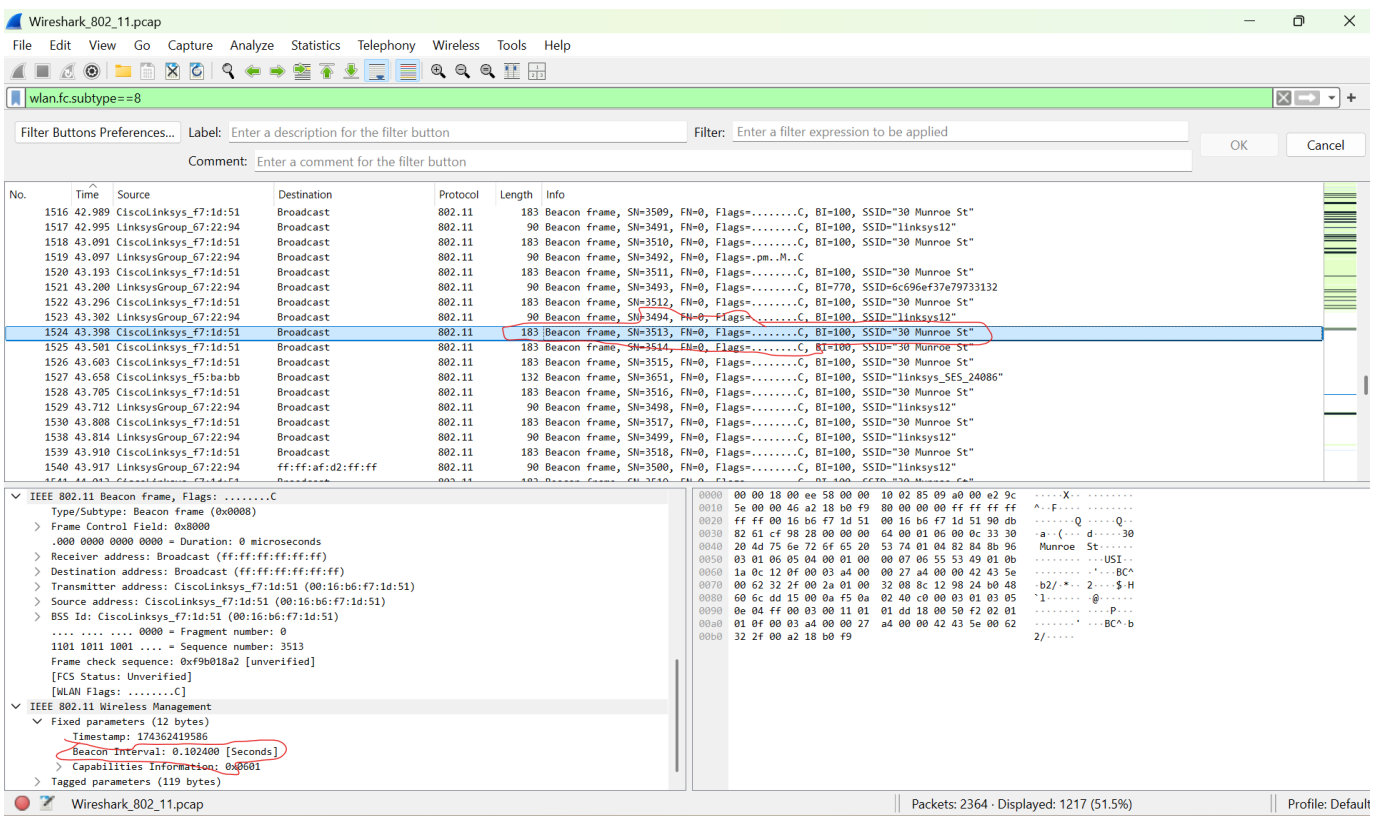

Figure 7b: Beacon interval for *30 Munroe St*
(Screenshot file: *beacon-interval-munroe.png*)

6.3 Beacon MAC Address Fields

The beacon frame transmitted by **30 Munroe St** uses the following MAC addresses:

- Source MAC Address: 00:16:b6:f7:1d:51
- Destination MAC Address: ff:ff:ff:ff:ff:ff (broadcast)

This confirms standard access point advertisement behavior.

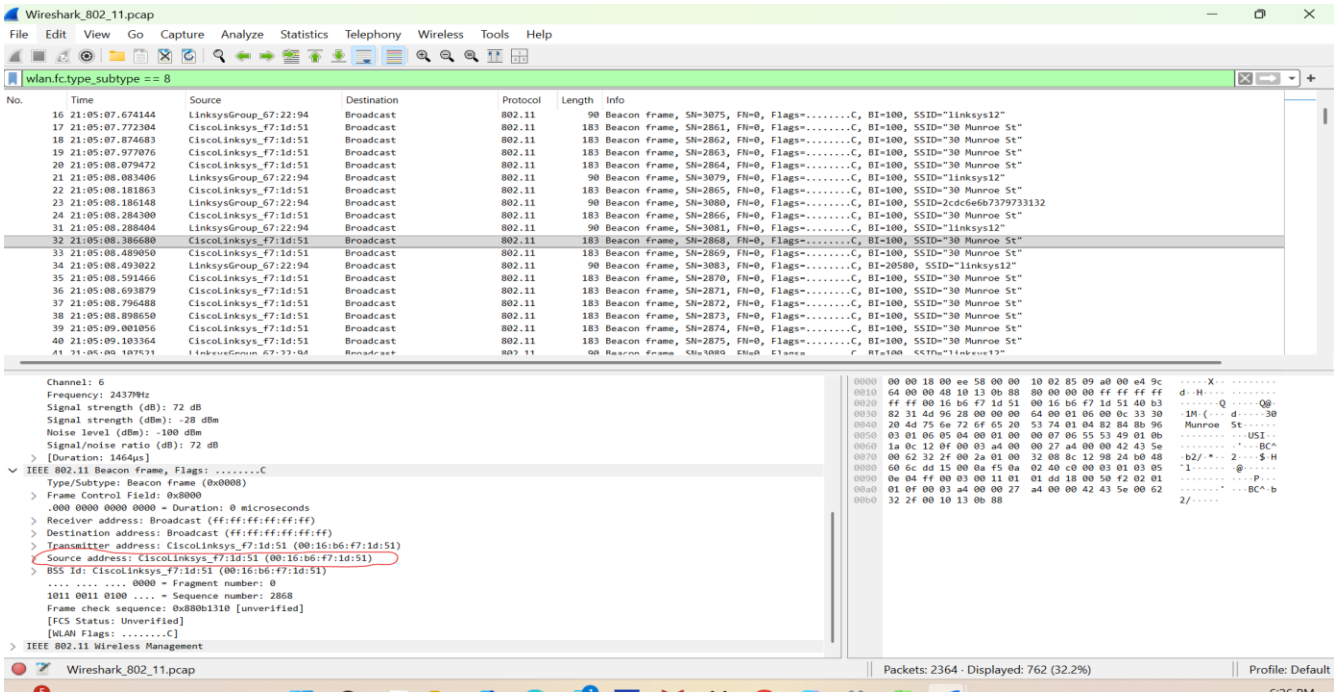

Figure 8: Source MAC address for *30 Munroe St* access point
(Screenshot file: *source-mac.png*)

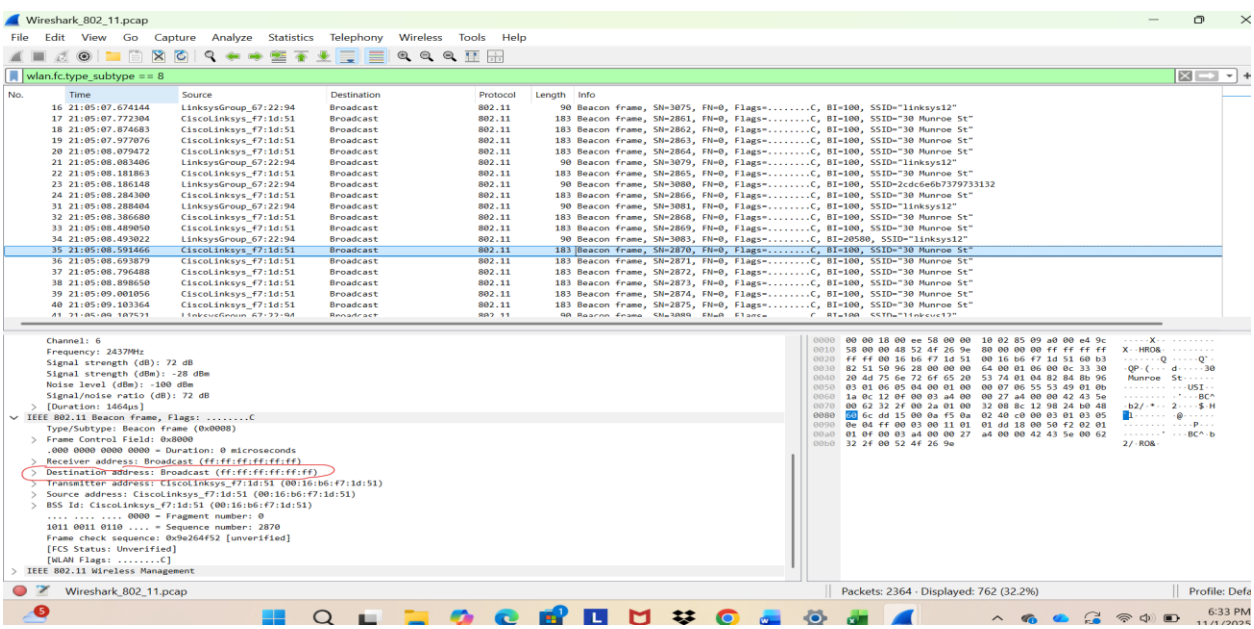

Figure 9: Destination MAC address (broadcast) in beacon frame
(Screenshot file: *broadcast-dest.png*)

6.4 BSSID Identification

The BSSID advertised by the **30 Munroe St** access point is 00:16:b6:f7:1d:51, which uniquely identifies the wireless network at Layer 2.

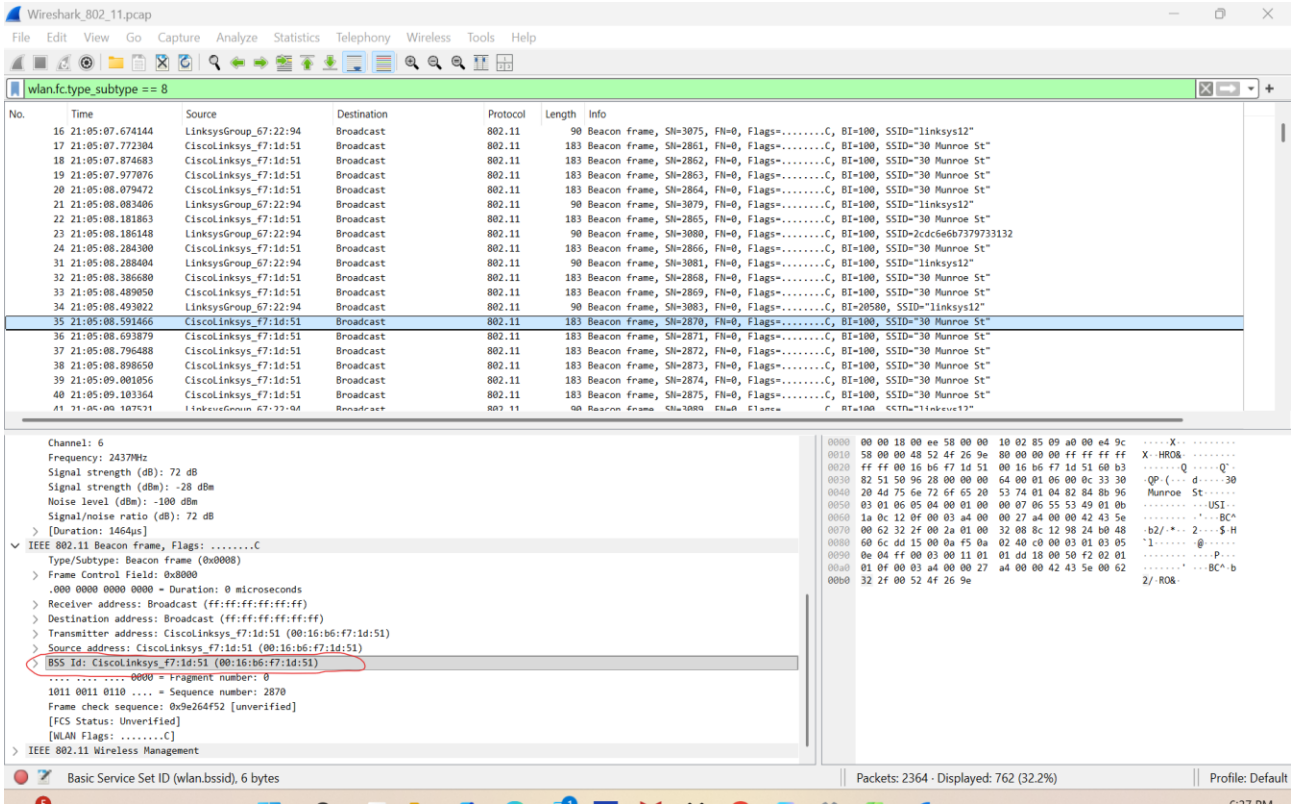

Figure 10: BSSID field in the beacon frame for *30 Munroe St*
(Screenshot file: *bssid.png*)

6.5 Supported Data Rates

Beacon frames from the access point advertise the following supported transmission rates:

- Standard Rates: 1, 2, 5.5, 11 Mbps
- Extended Rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

This indicates backward compatibility with legacy clients while supporting higher throughput.

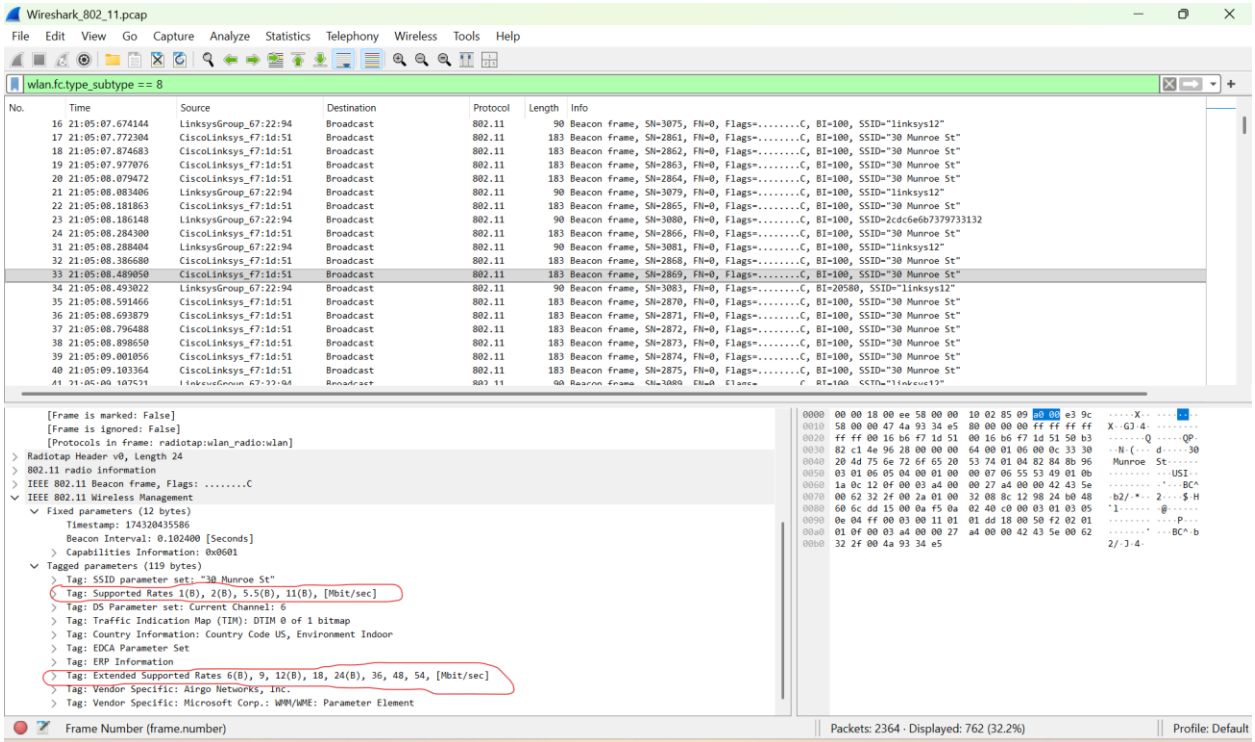

Figure 11: Supported data rates advertised by *30 Munroe St* access point
(Screenshot file: *supported-rates.png*)

7. MAC Address Roles & TCP Encapsulation

Analysis of 802.11 data frames carrying TCP traffic reveals multiple MAC address roles:

- Wireless Host (STA): 00:13:02:d1:b6:4f
- Access Point (BSSID): 00:16:b6:f7:1d:51
- First-Hop Router: 00:16:b6:f4:eb:a8
- Host IP Address: 192.168.1.109
- Destination IP Address: 128.119.245.12

This demonstrates how wireless frames handle Layer-2 delivery while IP routing occurs beyond the access point.

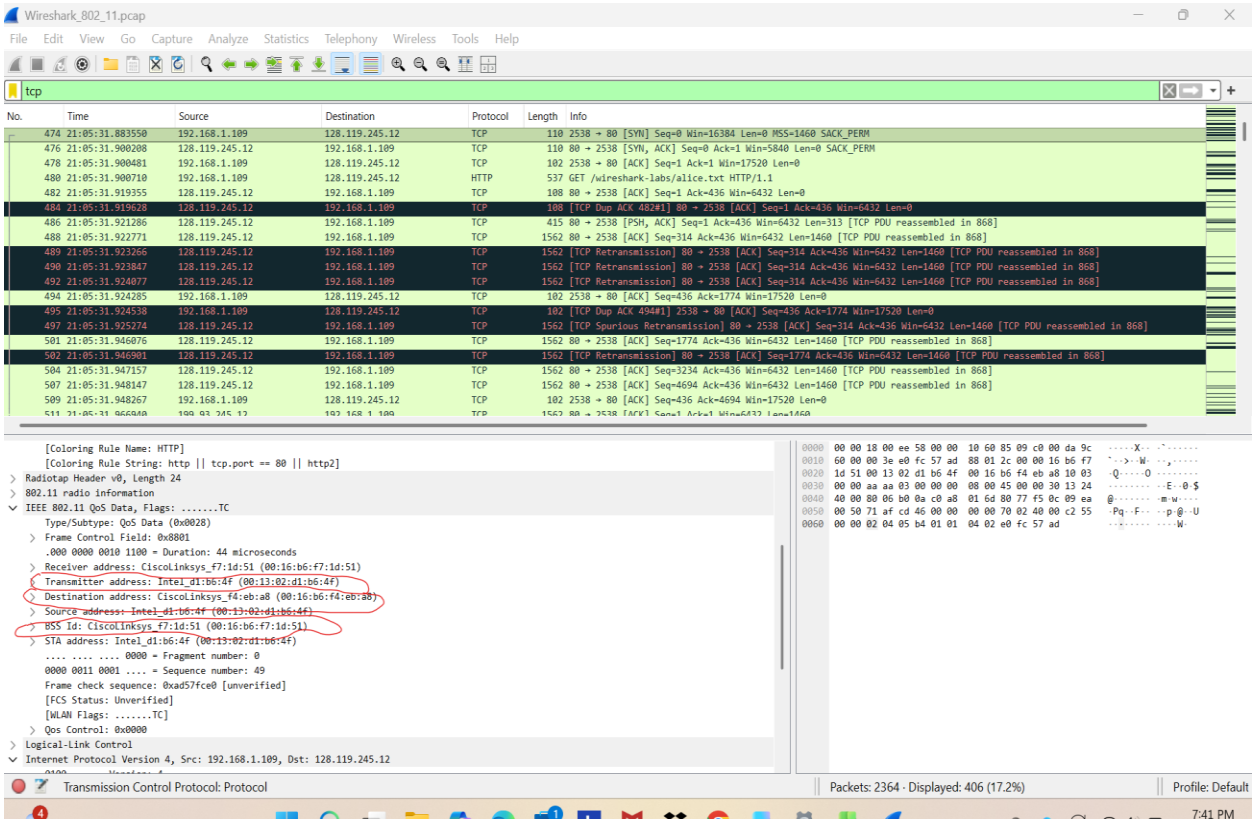

Figure 12a: MAC and IP addressing roles in 802.11 frames-1
(Screenshot files: *mac-role-1*)

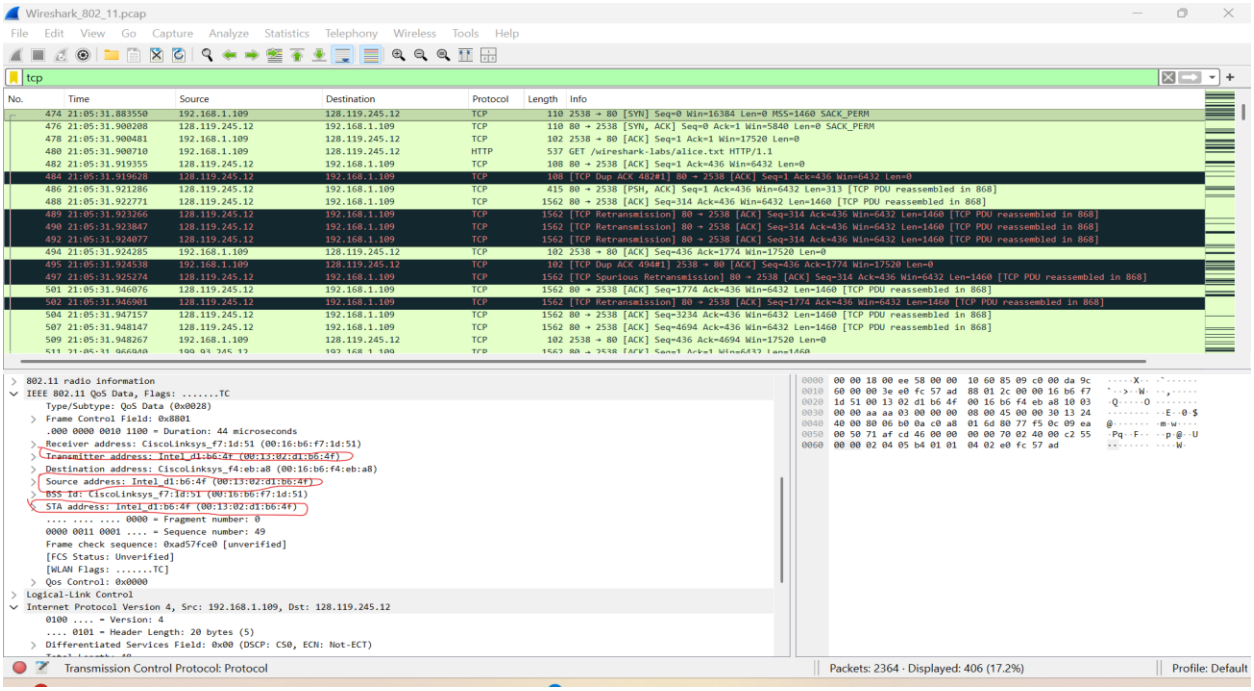

Figure 12b: MAC and IP addressing roles in 802.11 frames-2
(Screenshot files: *mac-roles-2*)

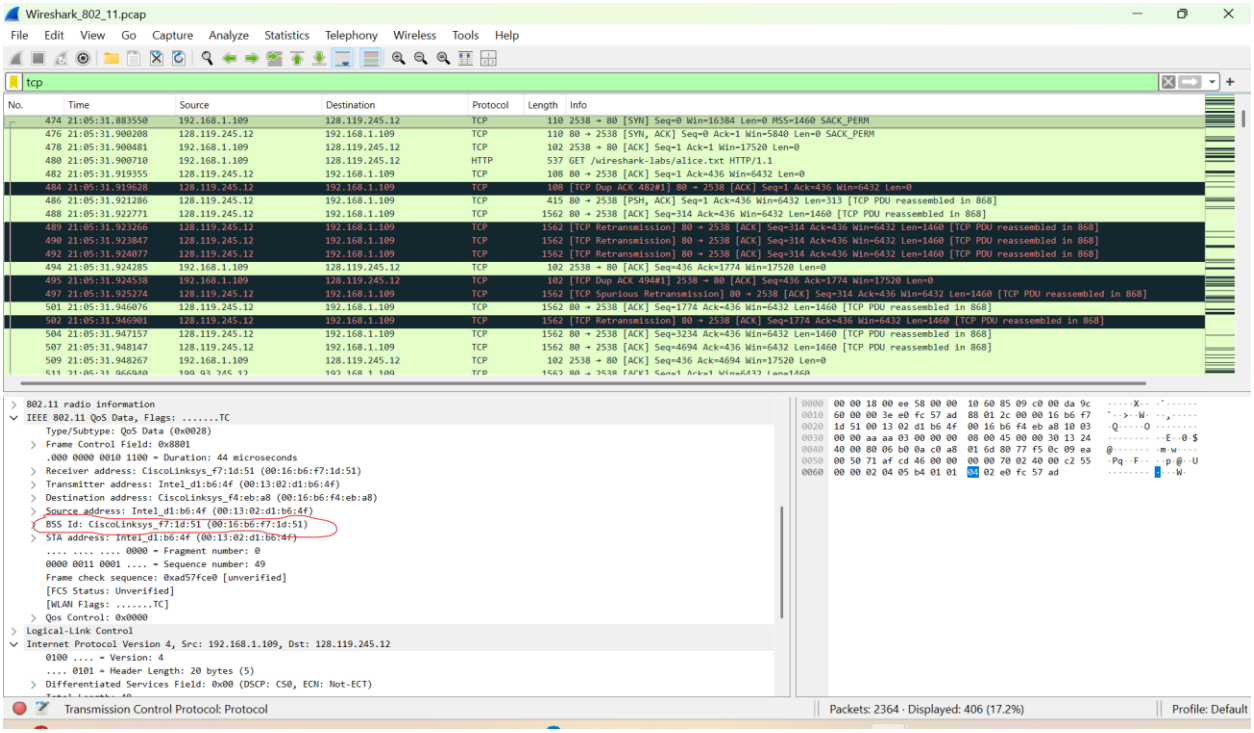

Figure 12c: MAC and IP addressing roles in 802.11 frames-3
(Screenshot files: *mac-roles-3*)

8. SYN/ACK Frame Analysis

When analyzing a TCP SYN/ACK segment encapsulated within an 802.11 frame, I observed three distinct MAC address fields:

- Receiver (Destination): Wireless host
- Source: First-hop router
- Transmitter / BSSID: Access point

This observation highlights the separation between IP endpoints and wireless hop forwarding.

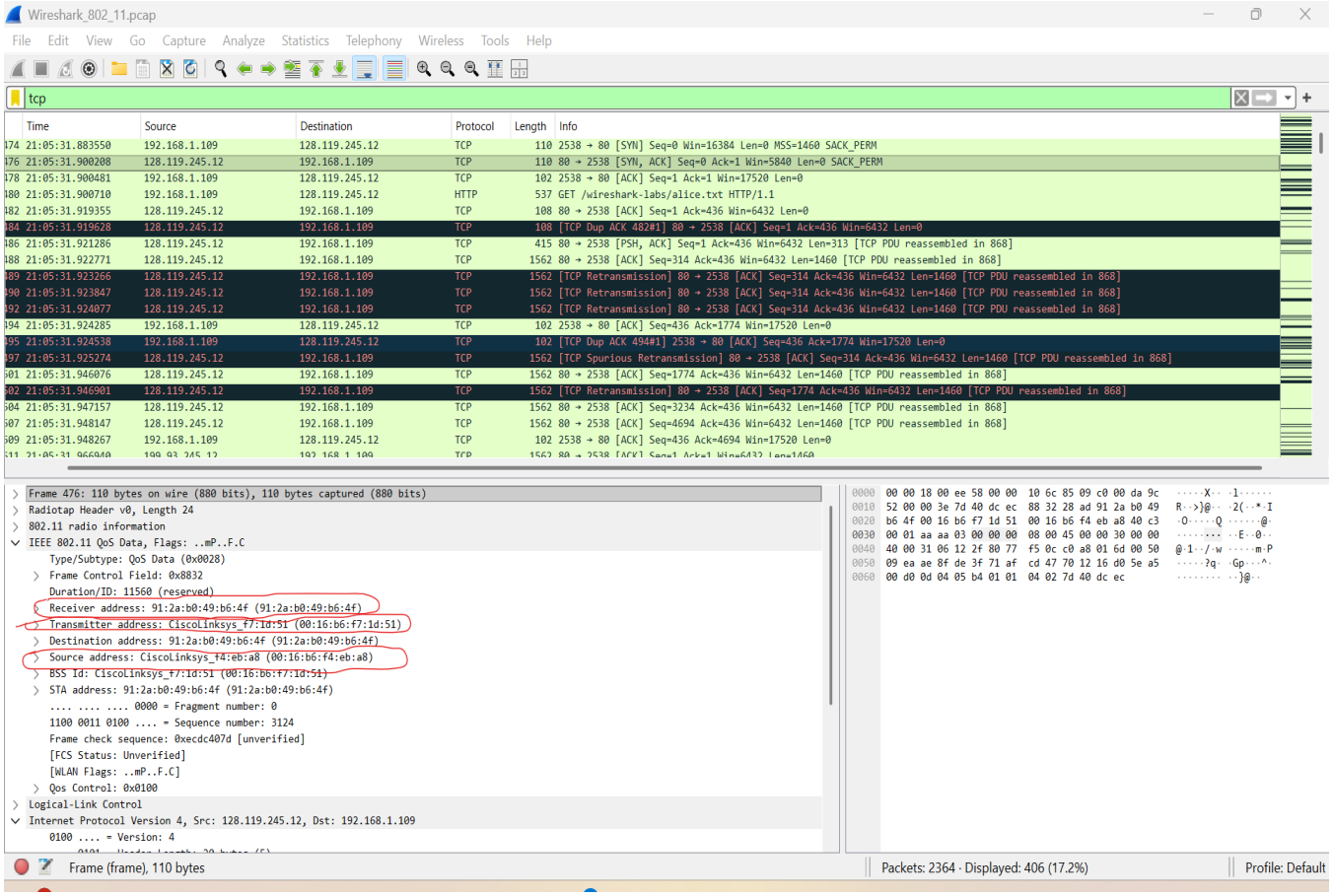

Figure 13a: MAC address roles in the SYN/ACK frame
(Screenshot file: *synack-mac-analysis.png*)

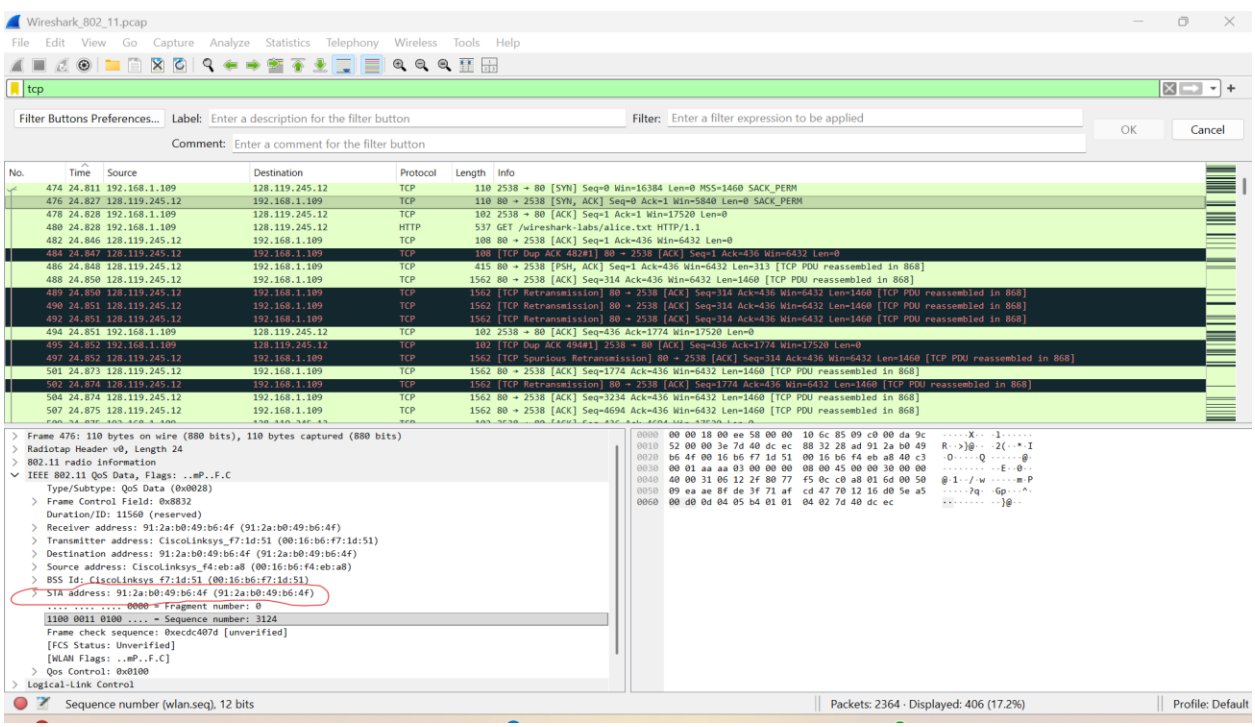

Figure 13b: MAC address roles in the SYN/ACK frame
(Screenshot file: *synack-mac-analysis-2.png*)

9. Disconnection & Deauthentication

At approximately 49.58 seconds, I observed the host terminating its connection with the **30 Munroe St** access point by:

1. Sending a DHCP Release message at the IP layer
2. Sending an 802.11 Deauthentication frame at the MAC layer

No disassociation frames were observed in the capture.

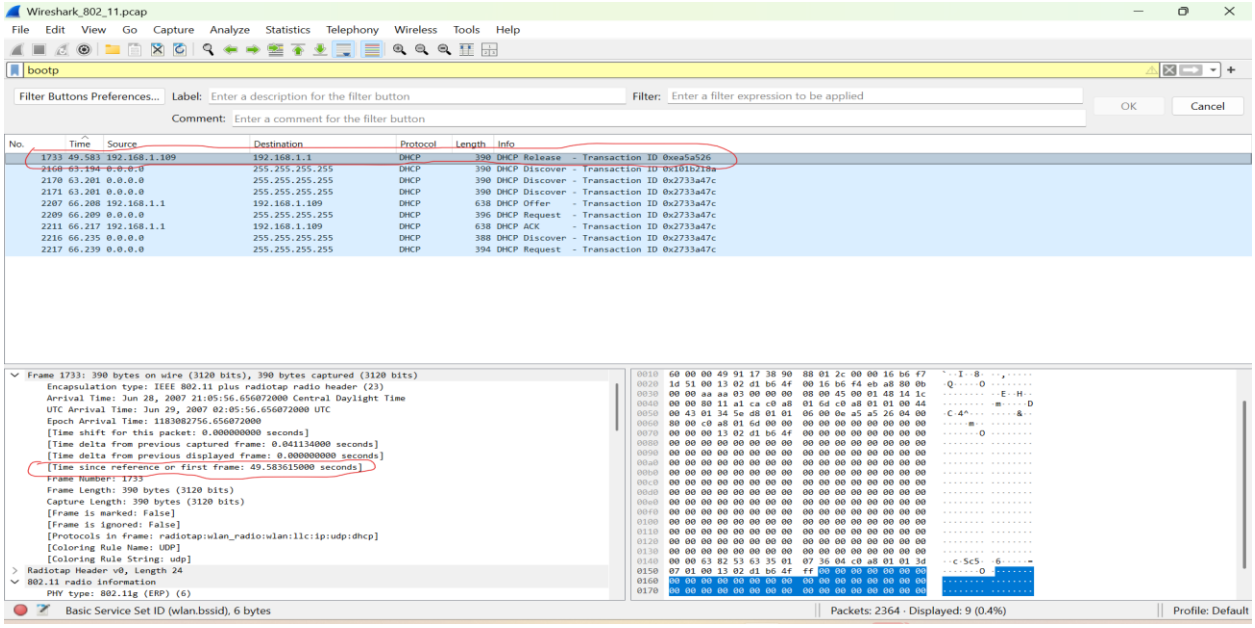

Figure 14a: DHCP Release frame
(Screenshot file: *dhcp-release.png*)

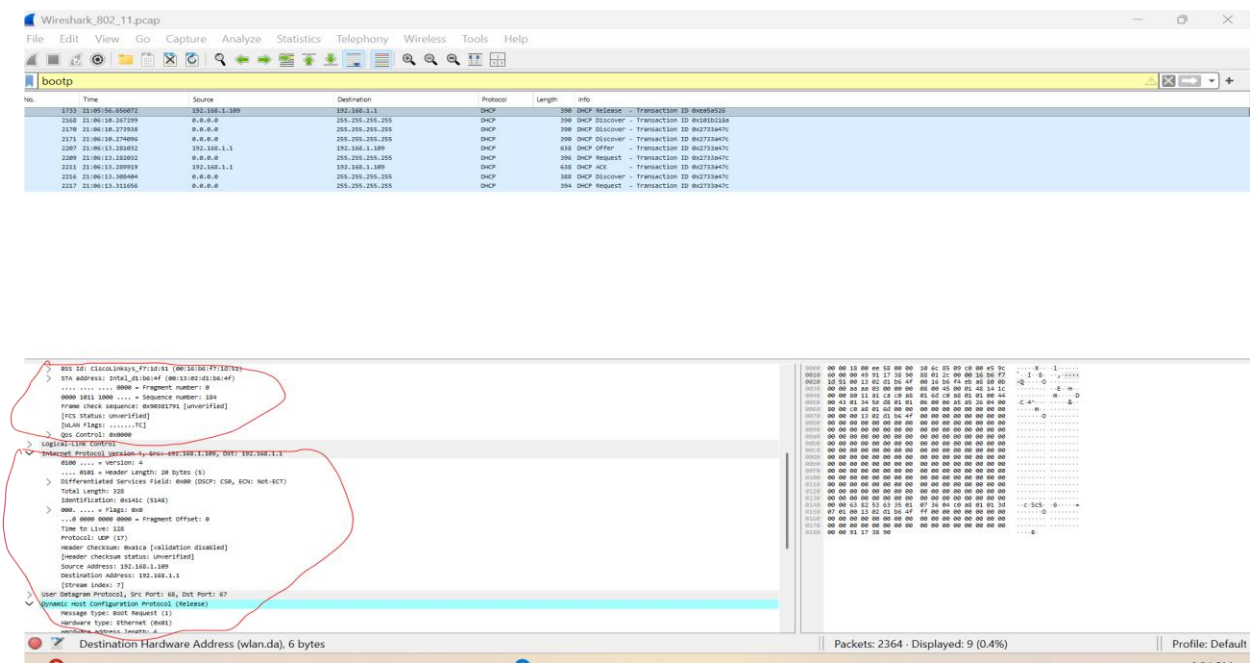

Figure 14b: DHCP Release details
(Screenshot file: *dhcp-release-2.png*)

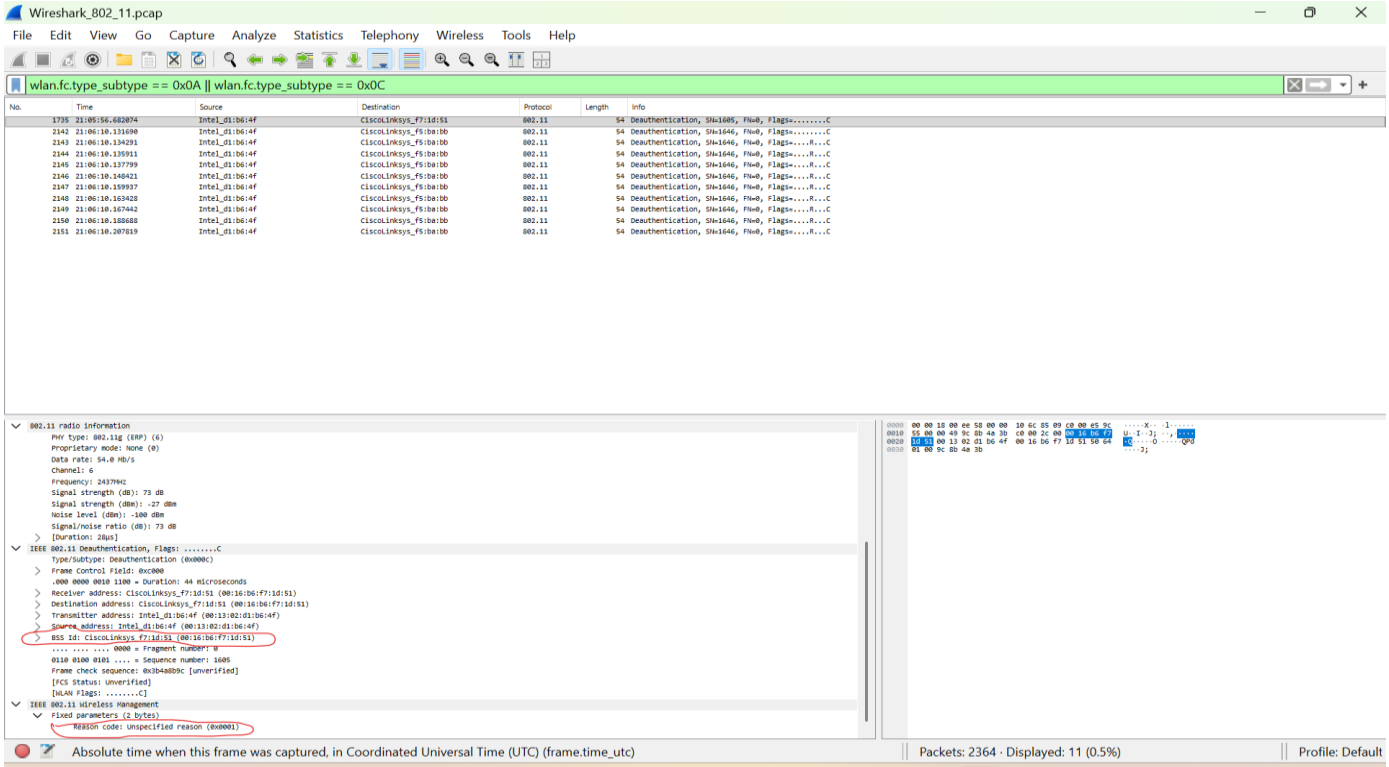

Figure 14c: 802.11 Deauthentication frame
(Screenshot file: *deauth-frame.png*)

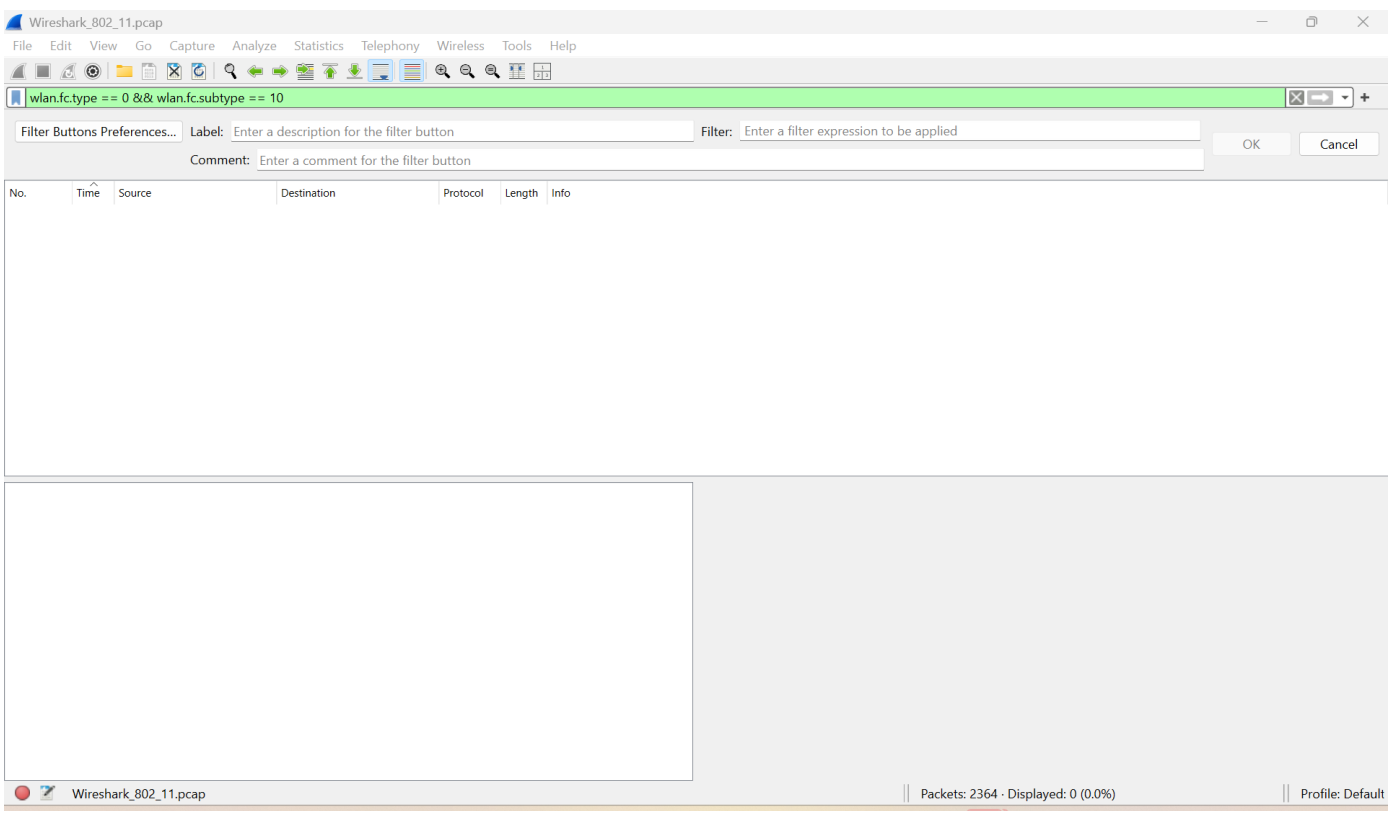

Figure 14d: Absence of disassociation frames
(Screenshot file: *no-disassoc.png*)

10. Authentication Attempts and Failure

I observed the host attempting to authenticate with **linksys_ses_24086** using Open System Authentication:

- Six authentication frames were transmitted
- No encryption key was required
- No authentication response (SEQ=2) was received from the access point

As a result, the authentication attempt failed.

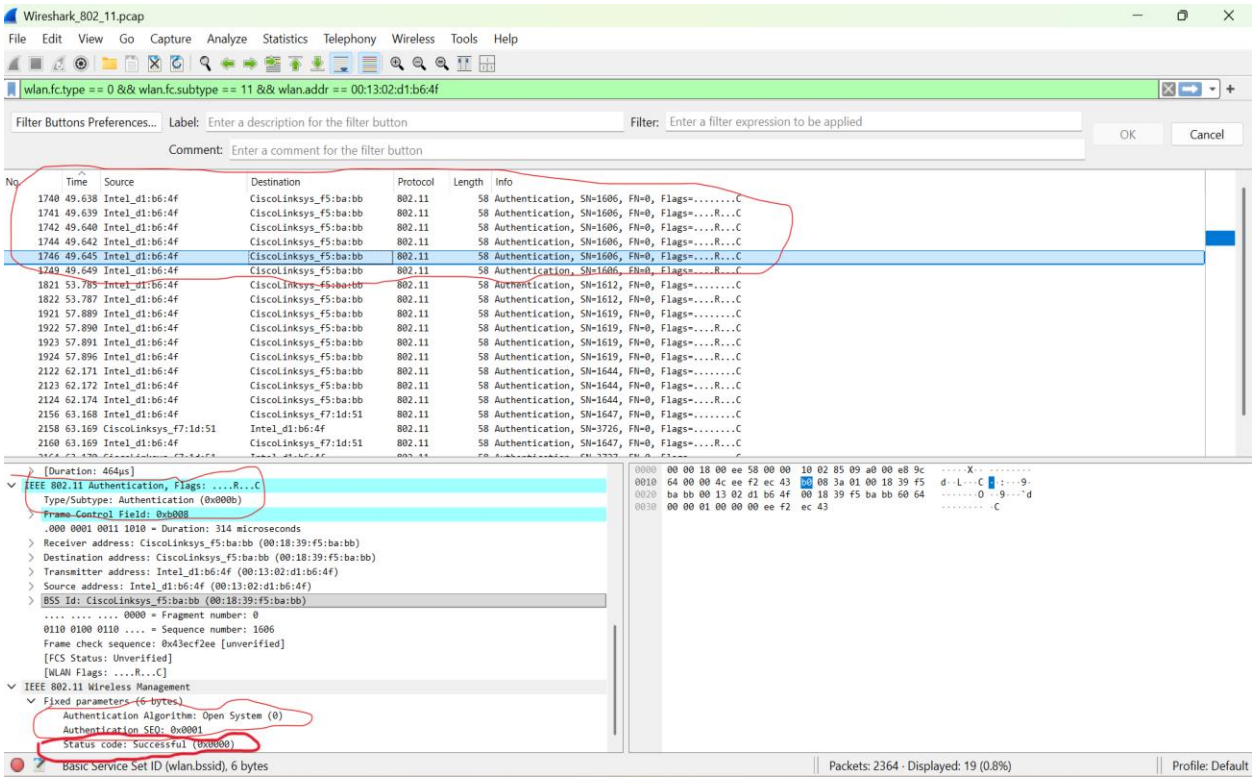

Figure 15: Authentication frames sent to *linksys_ses_24086*
(Screenshot file: *auth-attempts.png*)

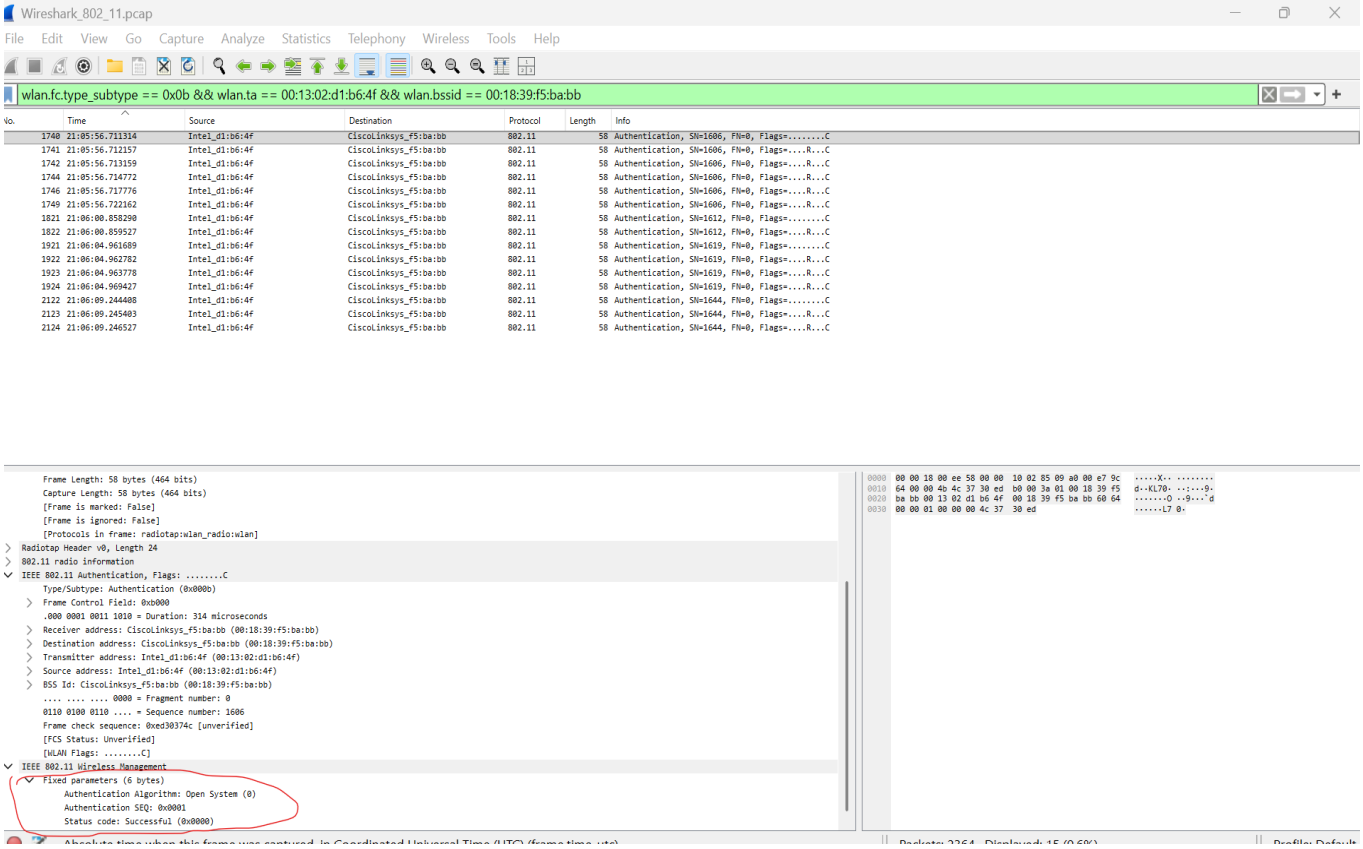

Figure 16: Open System Authentication (no key required)
(Screenshot file: *open-auth.png*)

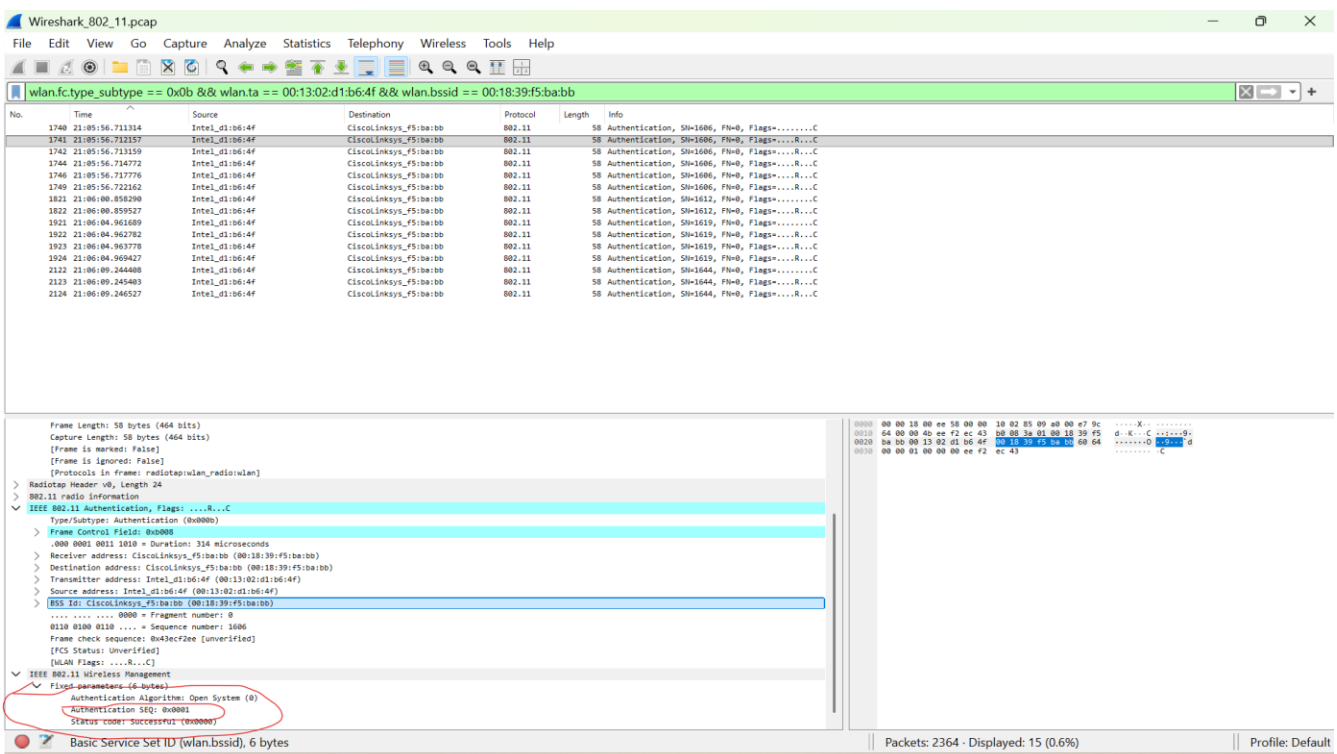

Figure 17: Missing authentication response from the access point
(Screenshot file: *no-auth-response.png*)

11. Successful Reassociation

After abandoning the failed roaming attempt, I observed the host successfully authenticating and associating with the **30 Munroe St** access point at **63.169 seconds**.

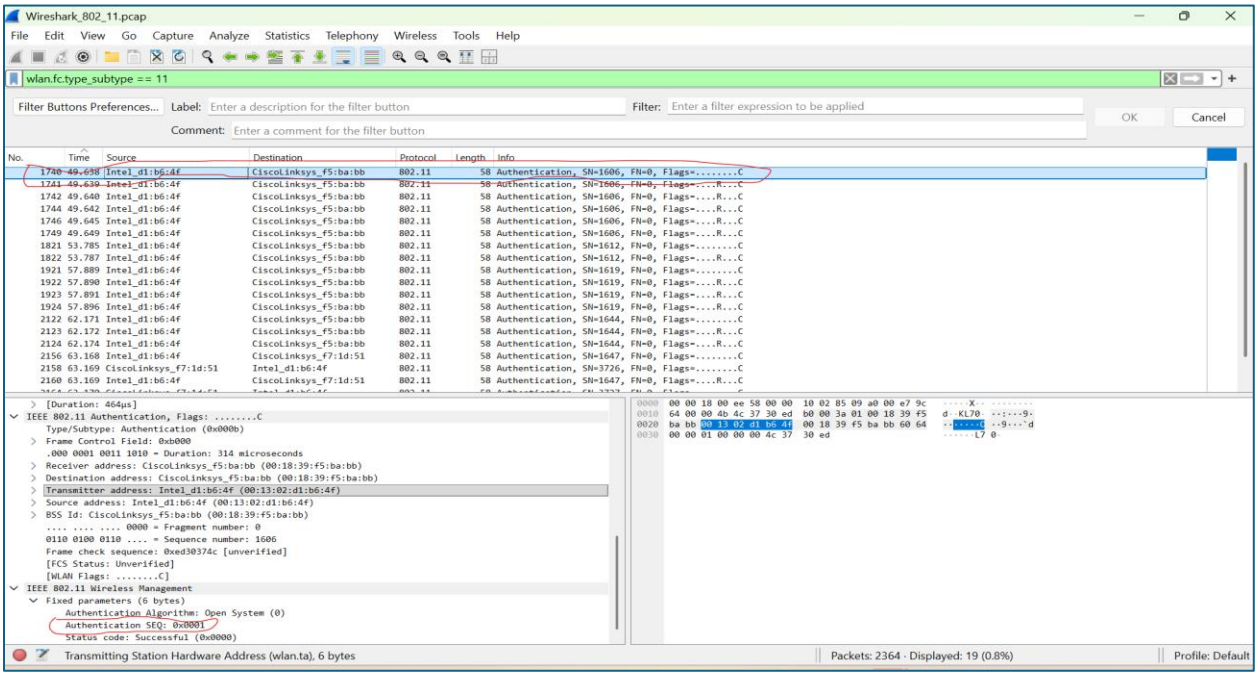

Figure 18a: Frame1740, AUTHENTICATION frame from the host to the 30 Munroe St.
(Screenshot files: *failed-auth.png, successful-auth.png*)

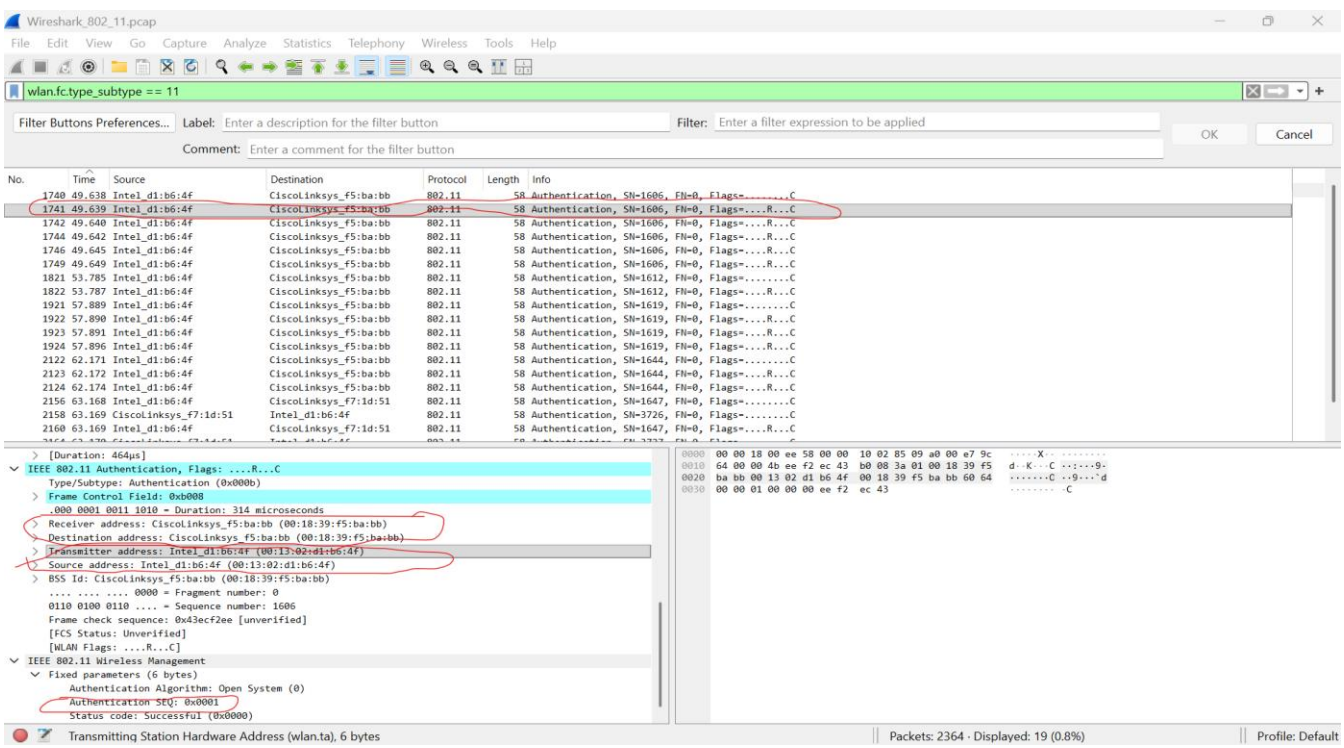

Figure 18b: Frame 1741, AUTHENTICATION frame from the host to the 30 Munroe St.

(Screenshot files: *failed-auth.png, successful-auth-2.png*)

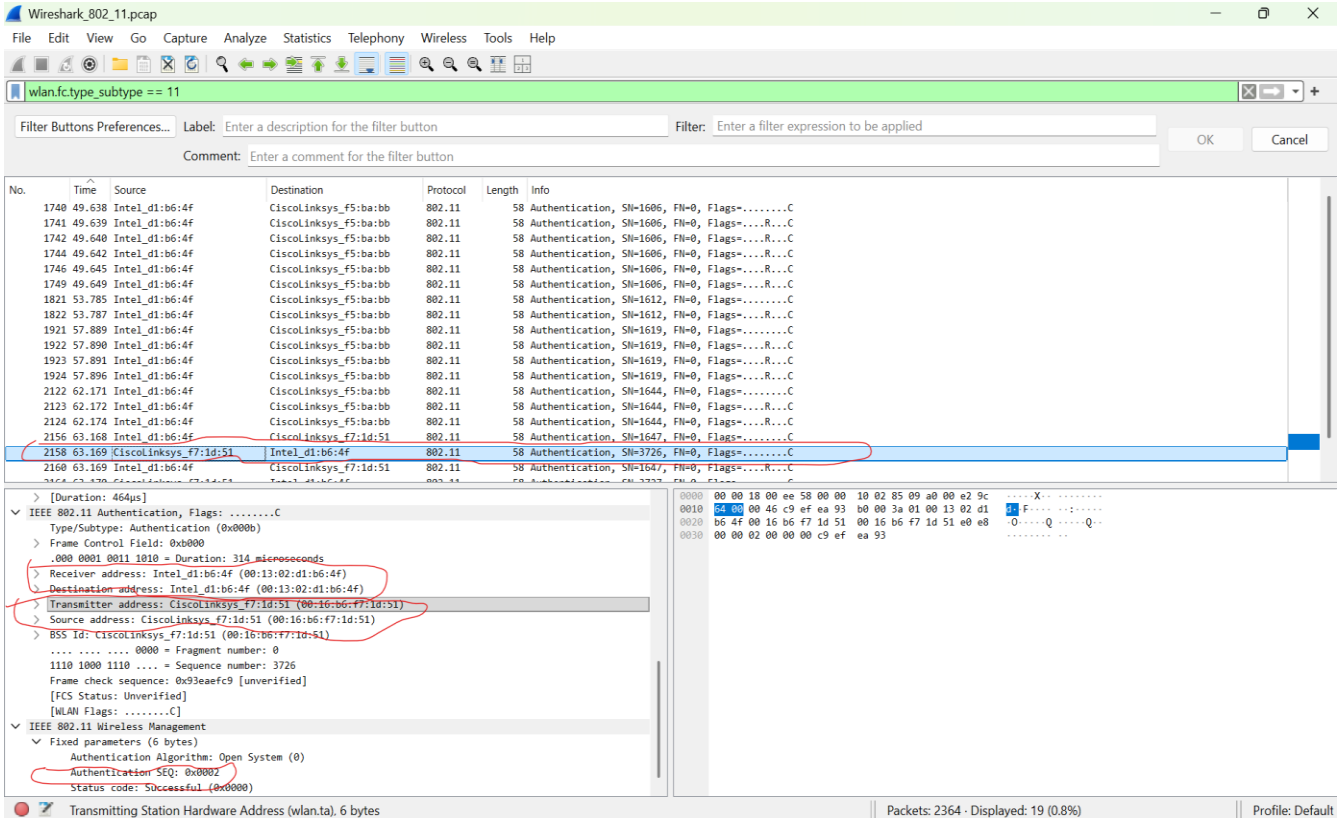

Figure 18c: Frame 2158, AUTHENTICATION frame from the host to a different AP

(Screenshot files: *failed-auth.png, successful-auth-3.png*)

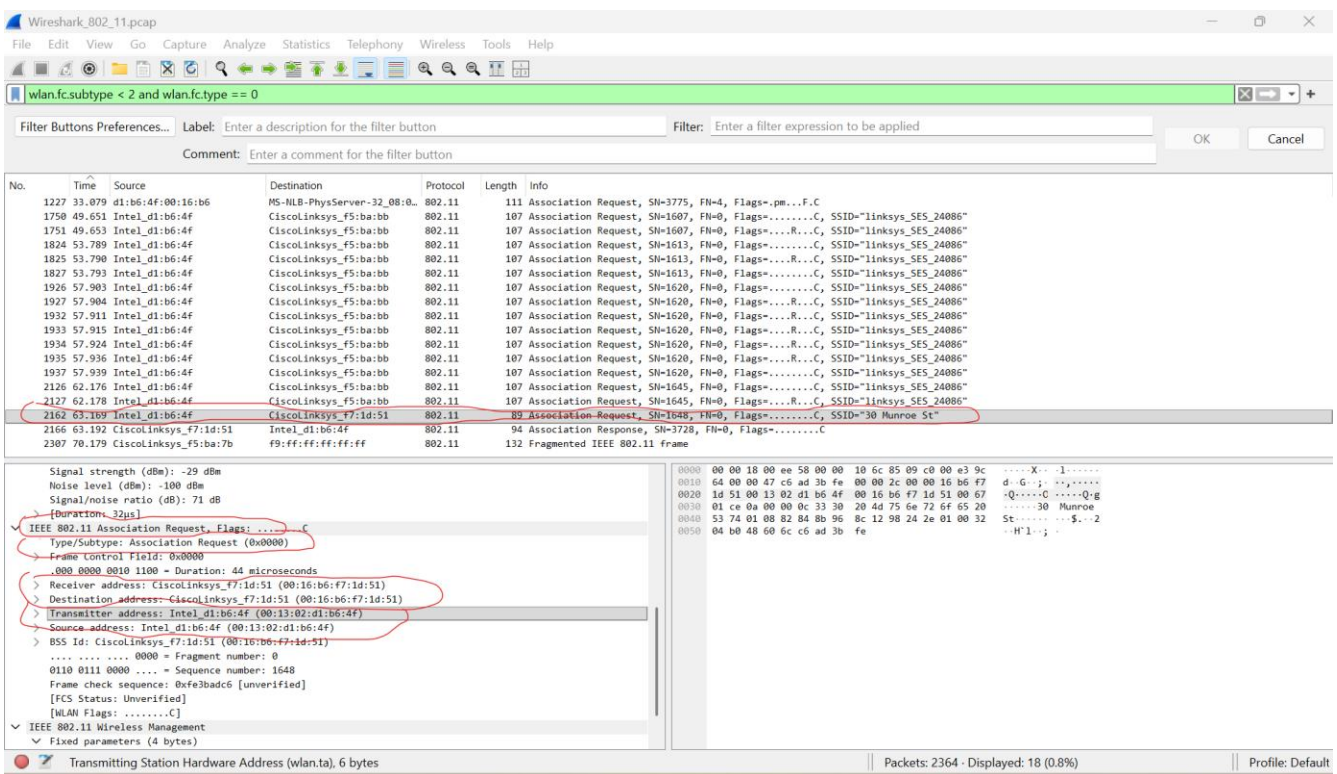

Figure 19a: Association Request frame

(Screenshot file: *assoc-request.png*)

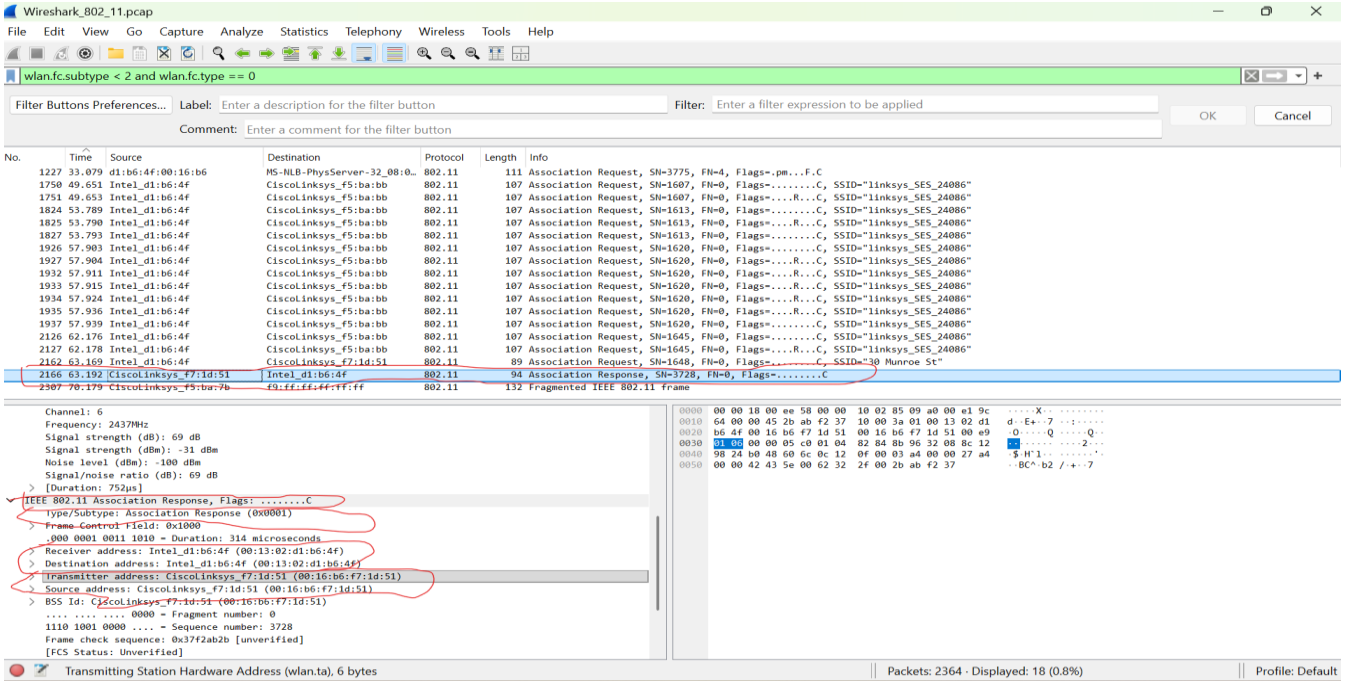

Figure 19b: Association Response frame
(Screenshot file: *assoc-response-2.png*)

12. Transmission Rates Willing to Use

The final analysis confirms the transmission rates supported by both the host and the access point:

- Host: 1, 2, 5.5, 11 Mbps
- Access Point: 1–54 Mbps

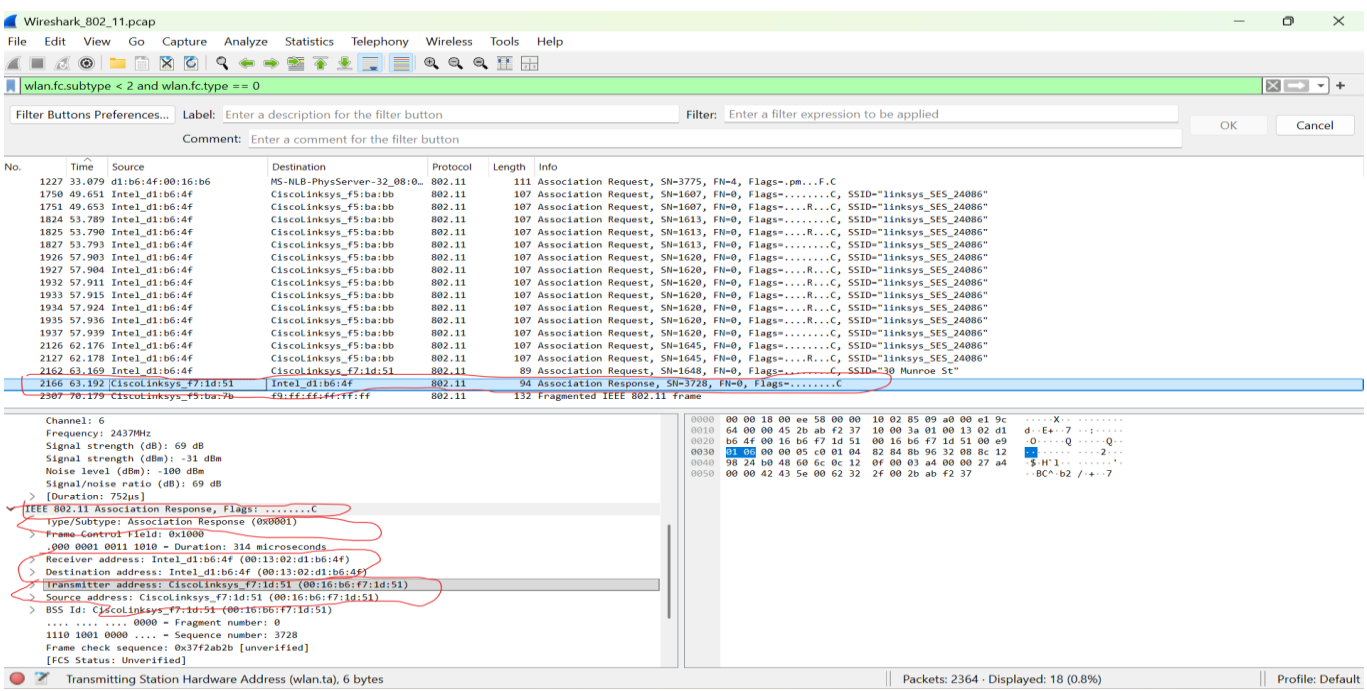

Figure 20: Transmission rates supported by the host and access point
(Screenshot file: *host-rates.png*)

13. Conclusion

This project provides a complete end-to-end analysis of IEEE 802.11 wireless communication, demonstrating:

- Beacon-based network discovery
- MAC-layer addressing roles
- TCP encapsulation within wireless frames
- Deauthentication and DHCP release behavior
- Failed roaming attempts
- Successful reassociation and recovery

The investigation reflects real-world wireless security analysis, SOC monitoring, and network troubleshooting workflows and strengthened my practical skills in:

- Wireless forensics
- Wi-Fi troubleshooting
- Layer-2 protocol analysis
- Roaming behavior interpretation
- Incident reconstruction