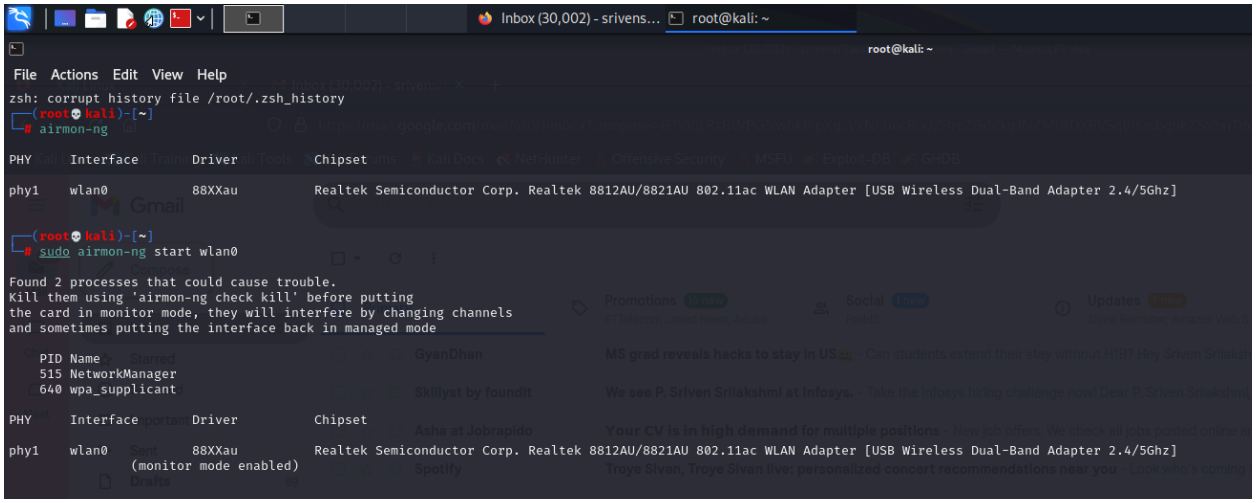
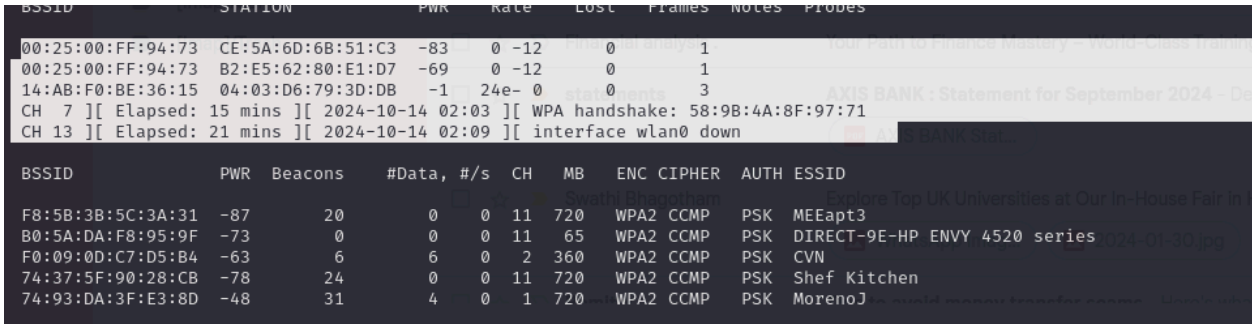
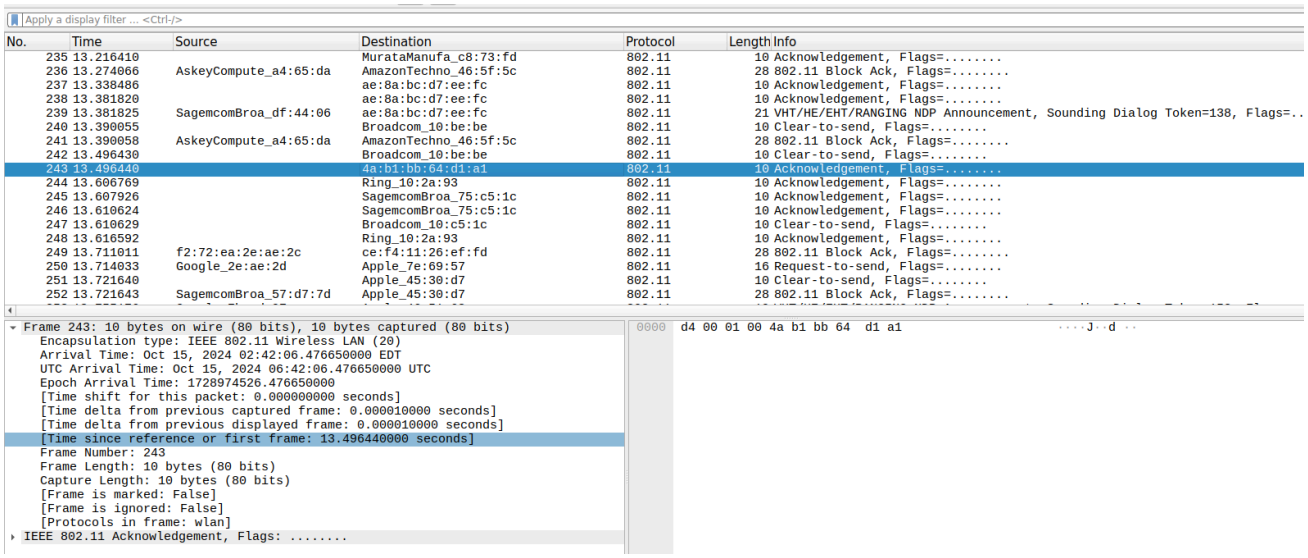
WPA2 Handshake Capture and Analysis





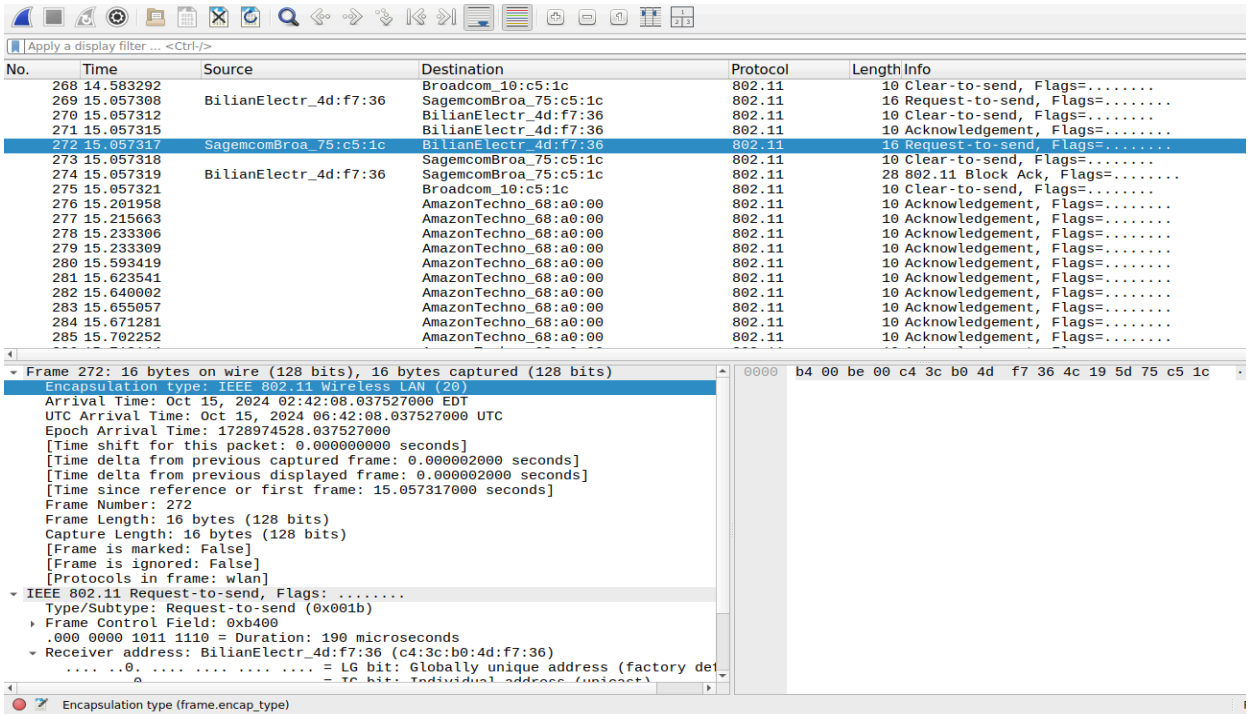
Acknowledgment (ACK) Frame:

- What It Is: The ACK frame is a type of control frame sent by the receiver to the sender to confirm successful reception of a data frame.
- Purpose: It ensures reliable communication between wireless devices. If a data frame is sent from one device to another (e.g., from a client to an access point), the receiving device must send an ACK frame to let the sender know that the frame was received correctly. If the sender doesn't receive an ACK within a certain time frame, it will assume the transmission failed and will resend the frame.
- In Wi-Fi Handshake: While ACKs aren't directly part of the WPA2 4-way handshake, every data transmission, including the handshake packets (such as EAPOL messages), will involve ACK frames to confirm successful delivery.



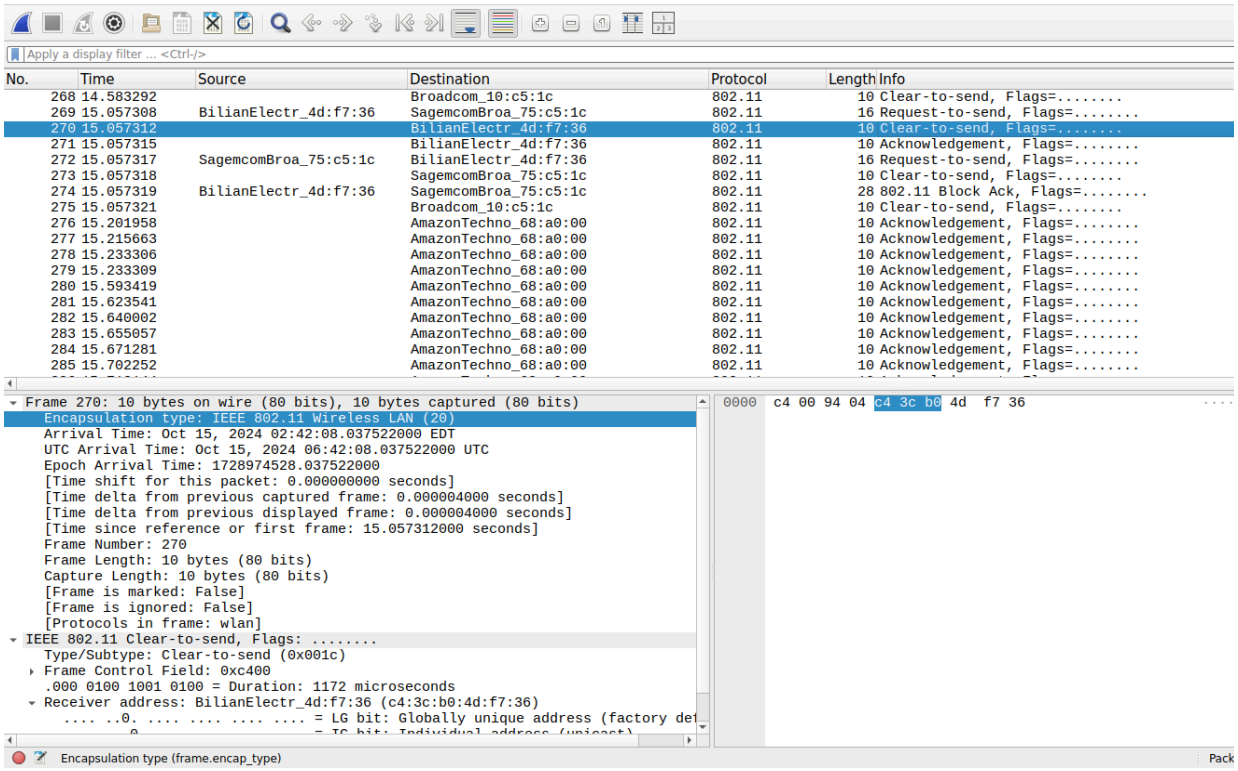
2. Request to Send (RTS) Frame:

- What It Is: RTS is another type of control frame used to clear the channel before sending large data frames.
- Purpose: RTS is used to avoid collisions in a Wi-Fi network, especially in environments where multiple clients might be trying to communicate with the same access point (AP) at the same time.
    - Before sending a large packet of data, the sender will send an RTS frame to the AP, asking for permission to transmit.
    - The RTS frame contains the duration for which the sender wants to use the wireless channel.
- In Wi-Fi Handshake: RTS is part of the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism in Wi-Fi but is not directly related to the WPA2 handshake. However, before the handshake or any other communication can begin, the client may send an RTS frame to request permission to use the channel.



3. Clear to Send (CTS) Frame:

- What It Is: CTS is the response to an RTS frame, sent by the receiver (typically the AP) to the sender to grant permission to send data.
- Purpose: After receiving an RTS frame, the AP checks whether the channel is free, and if it is, it responds with a CTS frame. This frame grants the sender permission to send data without worrying about interference from other devices during that time window.
    - The CTS frame also contains a duration value that tells other devices in the network to remain silent for a specific period, allowing the sender to transmit its data without interference.
- In Wi-Fi Handshake: Similar to RTS, CTS is not directly part of the WPA2 4-way handshake, but it plays a role in controlling access to the wireless medium before the handshake or other communications take place.



How These Frames Relate to the WPA2 Handshake:

- RTS/CTS and ACK frames are part of the medium access control (MAC) layer operations in the 802.11 protocol, and they manage how devices on a Wi-Fi network share the wireless medium and avoid collisions. These frames help ensure that the EAPOL (Extensible Authentication Protocol over LAN) packets used in the WPA2 4-way handshake are delivered reliably.
- The actual WPA2 handshake involves EAPOL packets, which are sent over the wireless medium, but before any transmission occurs, the medium must be clear. RTS/CTS can be used to avoid collisions when multiple clients are attempting to communicate with the same AP.
- After the handshake packets (or any other data packets) are sent, ACK frames confirm their successful reception.

Trigger-based Beamforming in Wi-Fi 6:

In Wi-Fi 6, **trigger-based beamforming** is a technique where the **access point (AP)** triggers the **client devices** to respond in a certain manner to enable beamforming, which is optimized for multi-user communication. This is crucial for efficient network management, especially in dense environments like offices or public hotspots. Wi-Fi 6 networks are designed to handle a much higher number of connected devices compared to previous generations. The combination of OFDMA and MU-MIMO, along with trigger-based beamforming, allows Wi-Fi 6 to:

- **Improve network efficiency** by serving multiple devices at once.
- **Reduce latency** by handling high traffic more efficiently.
- **Enhance coverage and reliability** through better signal direction and reduced interference.