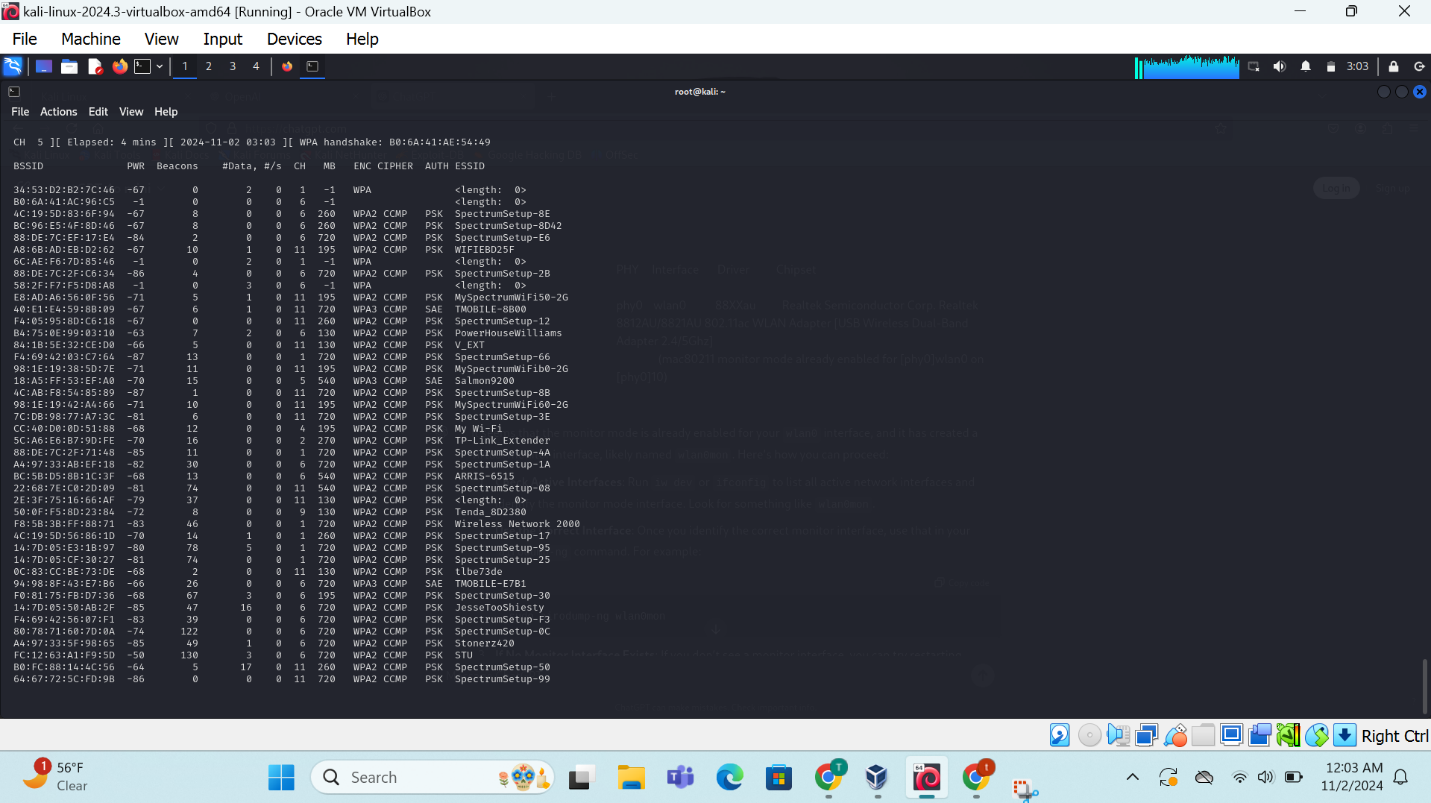
# WPA2 Handshake Capture and Analysis



Each line represents a single network, and the columns provide information about the network's:

* **BSSID:** The unique identifier of the network's access point.
* **RSSI:** The Received Signal Strength Indicator, a measure of the signal strength.
* **Data:** The number of data packets received from the network.
* **ENC:** The encryption type used by the network (e.g., WPA2, WPA3).
* **CIPHER:** The cipher suite used for encryption.
* **AUTH:** The authentication method used (e.g., PSK, SAE).
* **ESSID:** The network name (SSID).

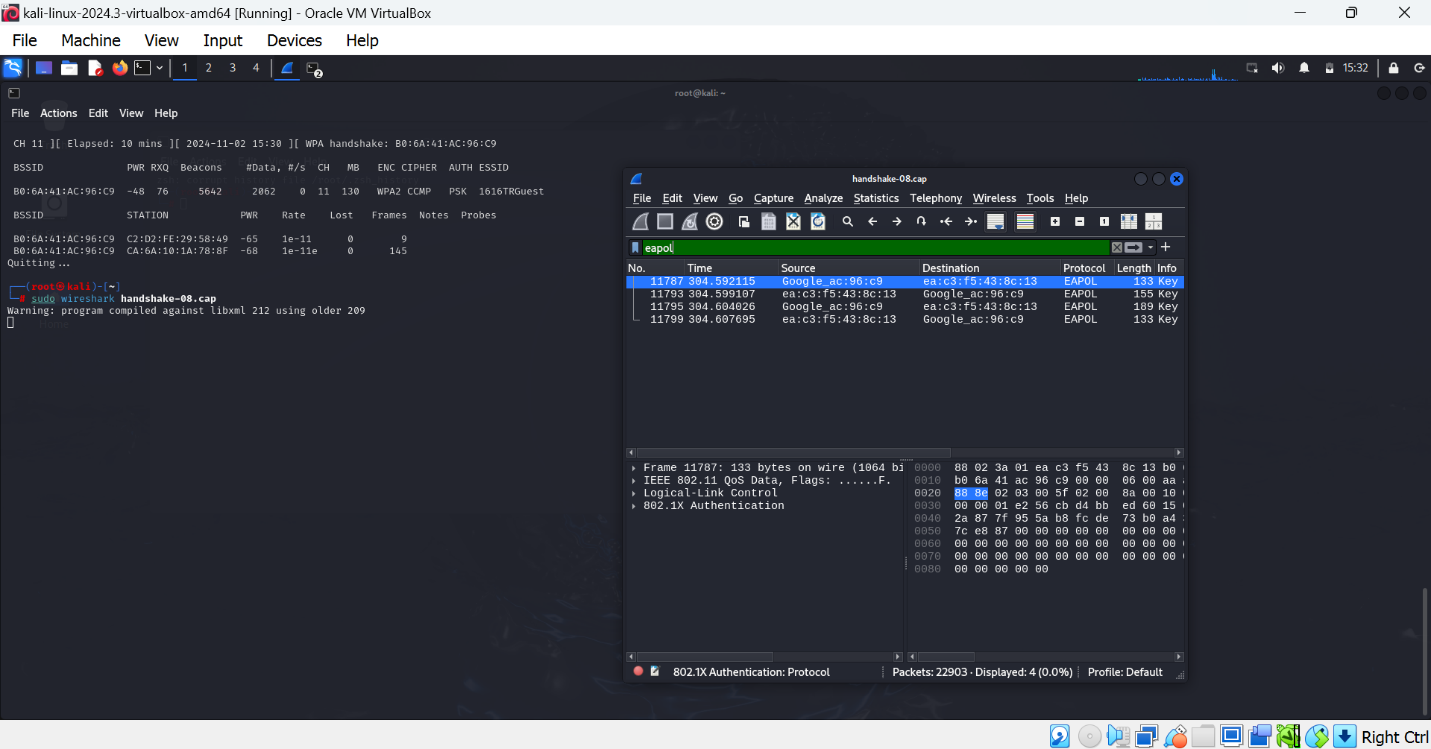
we can identify several potential security threats:

1. **Weak Encryption:**
   * Networks using older encryption standards like WEP or WPA are more vulnerable to attacks.
   * While WPA2 is generally considered secure, it's important to ensure that the network is configured correctly and using strong passwords.
   * WPA3 is the latest standard and offers improved security over WPA2.
2. **Default SSIDs and Passwords:**
   * Networks with default SSIDs and passwords are easy targets for attackers.
   * It's crucial to change the default settings and use strong, unique passwords.
3. **Rogue Access Points:**
   * Rogue access points are unauthorized access points that can be used to intercept traffic or provide unauthorized access to a network.
   * Kismet can detect rogue access points by identifying networks with unusual SSIDs, MAC addresses, or behavior.
4. **WPS Vulnerabilities:**
   * Wi-Fi Protected Setup (WPS) is a feature that allows easy network setup but is vulnerable to brute-force attacks.
   * It's recommended to disable WPS if possible.

A screenshot of a computer

Description automatically generated

Deauthentication attacks can disrupt wireless network connectivity, causing devices to disconnect from the network. While they can be annoying, they generally don't pose a significant security risk unless they are used to facilitate other attacks, such as man-in-the-middle attacks



The Wireshark capture window provides a detailed view of the network traffic, including individual packets. In this specific capture, we can see a series of EAPOL packets, which are used for authentication in 802.1X networks.