**Hacking Wireless Networks**

**Wireless Terminology:**

**GSM**

Global System for Mobile Communications (GSM) is a standard for mobile phone networks, providing digital cellular communication worldwide. It allows for voice and data services across different countries, ensuring interoperability. GSM supports roaming, SMS, and mobile data by utilizing frequency bands for communication, offering widespread network connectivity.

**Bandwidth**

Bandwidth refers to the maximum data transfer rate of a network or communication channel. It measures how much data can be transmitted in a given period, typically in bits per second (bps). Higher bandwidth allows for faster data transfer, making it crucial for applications like streaming, gaming, and large file downloads.

**Access Point (AP)**

An Access Point (AP) is a device that enables wireless devices to connect to a wired network. It acts as a bridge between wireless clients and a wired infrastructure, facilitating internet access, data transmission, and communication within a local area network (LAN), often used in Wi-Fi networks.

**BSSID**

The Basic Service Set Identifier (BSSID) is the unique MAC address assigned to an Access Point (AP) in a wireless network. It identifies the AP within a Basic Service Set (BSS), enabling devices to distinguish between different wireless networks or APs, aiding in connection and communication within the network.

**ISM Band**

The ISM band refers to specific frequency ranges reserved internationally for industrial, scientific, and medical applications. These bands are used for short-range, unlicensed wireless communication technologies like Wi-Fi, Bluetooth, and microwave ovens, allowing devices to transmit without needing a government license for most applications.

**Hotspot**

A hotspot is a physical location where wireless internet access is provided to the public. It typically involves a Wi-Fi network that allows devices such as smartphones and laptops to connect to the internet. Hotspots are common in cafes, airports, hotels, and other public areas for easy access to the internet.

**Association**

Association is the process through which a wireless device connects to an Access Point (AP) in a wireless network. This process involves the device identifying available APs, selecting one, and establishing a communication link, enabling the device to access the network and share data.

**Service Set Identifier (SSID)**

A Service Set Identifier (SSID) is a unique name that identifies a wireless local area network (WLAN). It is a string of up to 32 characters that distinguishes one network from another. Devices use SSID to connect to a specific WLAN and can either broadcast or hide the SSID.

**Orthogonal Frequency-division Multiplexing (OFDM)**

Orthogonal Frequency-Division Multiplexing (OFDM) is a method of encoding digital data onto multiple carrier frequencies. By splitting the data stream into smaller sub-channels, OFDM reduces interference and improves the efficiency of data transmission, widely used in broadband communication technologies like Wi-Fi, 4G, and 5G.

**Multiple Input, Multiple Output Orthogonal Frequency-Division Multiplexing (MIMO-OFDM)**

MIMO-OFDM is an advanced wireless technology combining Multiple Input, Multiple Output (MIMO) antennas with Orthogonal Frequency Division Multiplexing (OFDM). It enhances data transmission speeds and capacity in 4G and 5G networks by transmitting multiple data streams simultaneously over different antennas, improving wireless network performance and reliability.

**Direct-sequence Spread Spectrum (DSSS)**

Direct-sequence Spread Spectrum (DSSS) is a method of transmitting data by spreading the signal over a wide frequency band. The original data signal is multiplied by a pseudo-random noise sequence, making the transmission resistant to interference and enabling secure, robust wireless communication, often used in older Wi-Fi standards.

**Frequency-hopping Spread Spectrum (FHSS)**

Frequency-Hopping Spread Spectrum (FHSS) is a technique used to transmit data by rapidly switching between different frequency channels. This method reduces interference, increases security, and improves the reliability of communication by avoiding static frequency use, commonly applied in Bluetooth and older wireless systems.

**Wireless Networks:**

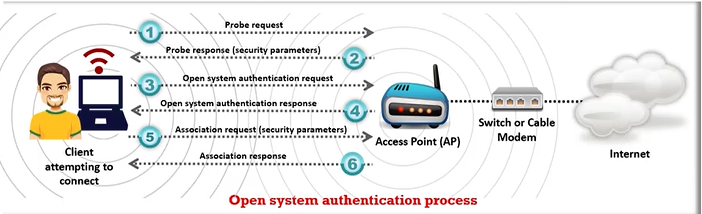
Wireless networks use radio waves or infrared signals to transmit data between devices without physical cables. They allow for mobility and flexibility, enabling devices like smartphones, laptops, and IoT devices to connect to the internet or other systems. Common examples include Wi-Fi, Bluetooth, and cellular networks.

Types of wireless networks:

1. Extension to a wired network
2. Multiple access points
3. LAN-to-LAN wireless network
4. 3G/4G Hotspot

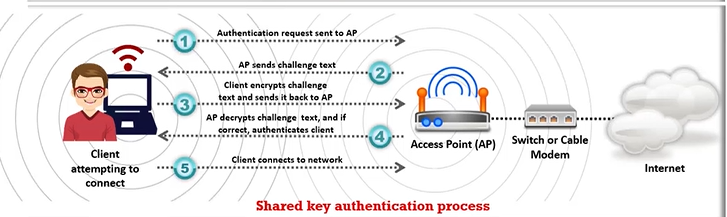
**Wi-Fi Authentication Modes:**

1. Open System authentication process



Any wireless device can be authenticated with the AP, thus allowing the device to transmit data only when its WEP key matches to that of the AP.

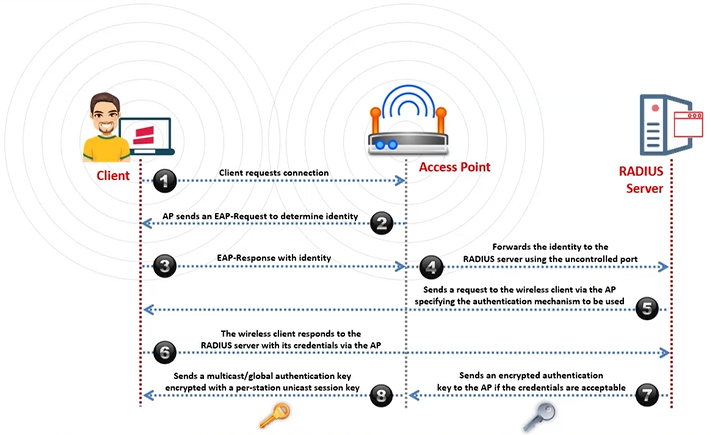
1. Shared key authentication process



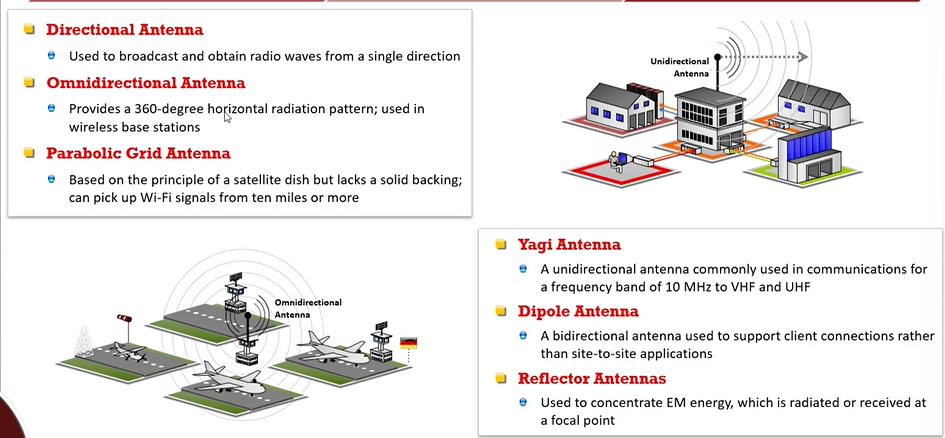
The station and AP use the same WEP key to provide authentication, which means that this key should be enabled and configured manually on both the AP and client.

**Wi-Fi Authentication Process Using a Centralized Authentication Server:**

Wi-Fi authentication using a centralized server involves the device sending credentials to an Access Point (AP). The AP forwards these credentials to a centralized authentication server (e.g., RADIUS). The server verifies the credentials, and if valid, grants network access. This ensures secure, centralized management of user authentication.

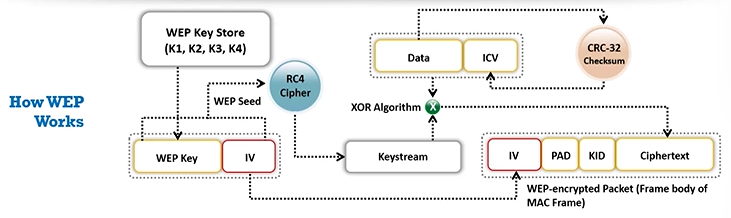


**Types of Wireless Antennas:**



**Wired Equivalent Privacy (WEP) Encryption:**

Wired Equivalent Privacy (WEP) is an outdated wireless network security protocol designed to provide data confidentiality similar to wired networks. It uses 64-bit or 128-bit encryption keys but is vulnerable to attacks due to weak encryption methods and predictable key management, making it largely obsolete today.



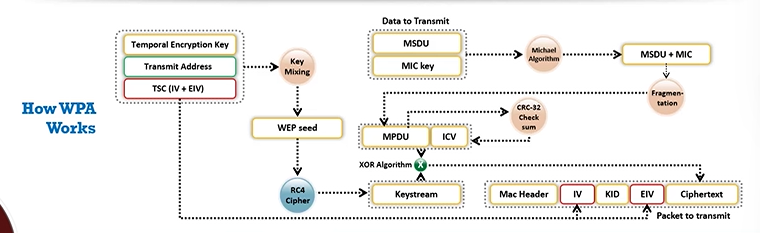
WEP's weaknesses include:

1. **Weak Encryption**: It uses the RC4 algorithm, which is vulnerable to attacks like the "FMS attack," allowing hackers to crack the encryption key easily.
2. **Fixed Initialization Vector (IV)**: The IV is too short (24 bits), leading to reuse of keys and making it easier to decrypt traffic.
3. **Weak Key Management**: WEP's method for generating and distributing keys is flawed, making it susceptible to brute-force and dictionary attacks.
4. **No Integrity Checking**: WEP lacks robust mechanisms for ensuring data integrity, allowing attackers to modify packets without detection.

**Wi-Fi Protected Access (WPA) Encryption:**

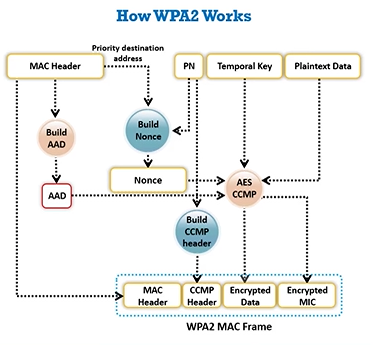
Wi-Fi Protected Access (WPA) is a wireless security protocol designed to improve upon WEP by using stronger encryption methods, such as Temporal Key Integrity Protocol (TKIP) and later, Advanced Encryption Standard (AES). WPA provides better protection against attacks and offers stronger data integrity, making it more secure than WEP.

WPA overcomes WEP's weaknesses by replacing its weak RC4 encryption with stronger algorithms like Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). WPA also addresses WEP's short 24-bit Initialization Vector (IV) by using dynamic key generation, ensuring unique encryption keys for each session. Additionally, WPA includes robust data integrity checks, preventing unauthorized packet alterations.



**WPA2 Encryption:**

WPA2 is an improved version of WPA, offering enhanced security through the use of Advanced Encryption Standard (AES) for encryption instead of the weaker Temporal Key Integrity Protocol (TKIP). It provides stronger protection against attacks, including improved data integrity and authentication mechanisms. WPA2 is the standard for most modern Wi-Fi networks, offering superior security compared to WPA and WEP.



**WPA3 Encryption:**

WPA3 is the latest Wi-Fi security protocol, offering stronger encryption and improved protection compared to WPA2. It uses 256-bit encryption with Advanced Encryption Standard (AES) and introduces the Simultaneous Authentication of Equals (SAE) protocol for more secure key exchanges. WPA3 also enhances protection against offline dictionary attacks and provides better security on open networks through Opportunistic Wireless Encryption (OWE).

**Rogue AP Attack:**

A Rogue Access Point (AP) attack occurs when an attacker sets up an unauthorized wireless access point within a legitimate network, mimicking a trusted AP. Here's how the attack works:

1. **Setup**: The attacker configures a device (often a laptop or router) to act as an access point with the same name (SSID) as a legitimate AP within the target network.
2. **Deauthentication**: The attacker may use deauthentication attacks to disconnect users from the legitimate AP, causing them to automatically reconnect to the rogue AP.
3. **Connection**: Once users connect to the rogue AP, the attacker can intercept or manipulate network traffic, gaining access to sensitive data like passwords or session cookies.
4. **Exploitation**: The attacker can also launch man-in-the-middle (MITM) attacks, redirect traffic, or use the rogue AP to distribute malware.

This type of attack exploits user trust and vulnerabilities in wireless security, highlighting the need for strong encryption (e.g., WPA3) and proper network monitoring.

**Client Mis-association:**

A Client Mis-association attack occurs when an attacker manipulates a wireless client into connecting to a rogue access point (AP) instead of the legitimate one. This is typically achieved by spoofing the AP’s SSID or sending deauthentication/disassociation frames, causing the victim to unknowingly associate with the attacker's AP, exposing their data.

**Misconfigured Access Point (AP) attack:**

A Misconfigured Access Point (AP) attack occurs when an attacker exploits improper or insecure configurations in a wireless access point. This may involve:

1. **Weak Encryption**: Using outdated or weak security protocols (e.g., WEP or WPA) that are vulnerable to cracking.
2. **Open Networks**: APs left without encryption, allowing unauthorized access.
3. **Improper SSID Broadcasting**: Misconfigured SSIDs can make the network visible and easily targeted.

Attackers can exploit these misconfigurations to gain unauthorized access, launch man-in-the-middle attacks, intercept data, or spread malware within the network. Proper AP security and regular configuration audits are essential to prevent such attacks.

**Unauthorized association:**

Unauthorized association occurs when a device connects to a wireless access point (AP) without permission, often by exploiting weak security settings or misconfigured APs. Attackers can gain access to sensitive network resources or intercept traffic by forcing devices to connect to rogue APs, bypassing authentication and security measures.

**Ad-Hoc connection attack:**

An Ad-Hoc connection attack occurs when an attacker sets up a rogue ad-hoc network, allowing devices to connect directly without a central access point. By exploiting this, attackers can intercept data, inject malicious traffic, or launch man-in-the-middle attacks, potentially compromising the confidentiality and integrity of communications.

**Honeypot Access Point (AP) attack:**

A Honeypot Access Point (AP) attack involves setting up a fake, enticing wireless access point designed to lure unsuspecting devices. Once connected, attackers can monitor, intercept, and manipulate traffic, or install malware. Honeypots exploit trust to capture sensitive data or conduct further attacks on vulnerable devices.

**AP MAC spoofing:**

AP MAC spoofing involves an attacker altering the MAC address of a rogue access point (AP) to mimic a legitimate AP. This deceives devices into connecting to the attacker’s AP, enabling data interception, man-in-the-middle attacks, or unauthorized access to the network, compromising security and privacy.

**Denial-of-Service (DoS) attack:**

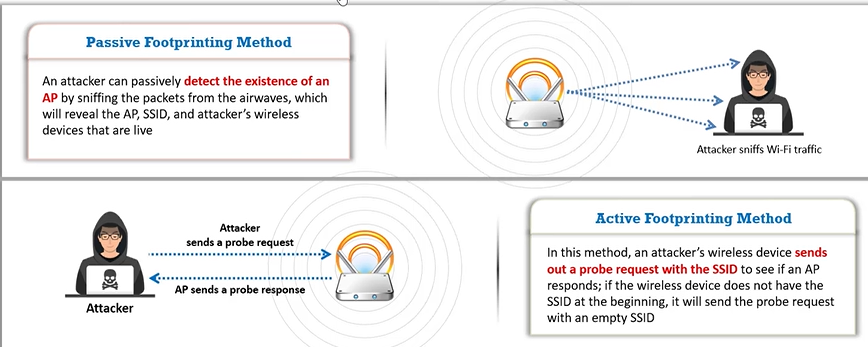
A Denial-of-Service (DoS) attack on a wireless network aims to disrupt connectivity by overwhelming or disabling the network. In wireless networks, this can involve flooding the AP with deauthentication or disassociation frames, disconnecting clients, or jamming radio frequencies, rendering the network unavailable for legitimate users.

**Jamming Signal attack:**

A Jamming Signal attack targets wireless networks by flooding the frequency channel with excessive noise or random signals, disrupting communication. This prevents devices from receiving or sending data, causing network slowdowns or complete disconnection. Jamming attacks can affect both Wi-Fi and other wireless communication systems, reducing network reliability.

**Wi-fi discovery: Wireless Network Footprinting:**

Wi-Fi discovery or wireless network footprinting is the process of identifying and mapping available wireless networks in a specific area. It involves gathering details such as network names (SSIDs), signal strength, encryption types, and access points. This information is used for security analysis, vulnerability assessments, or unauthorized network access.



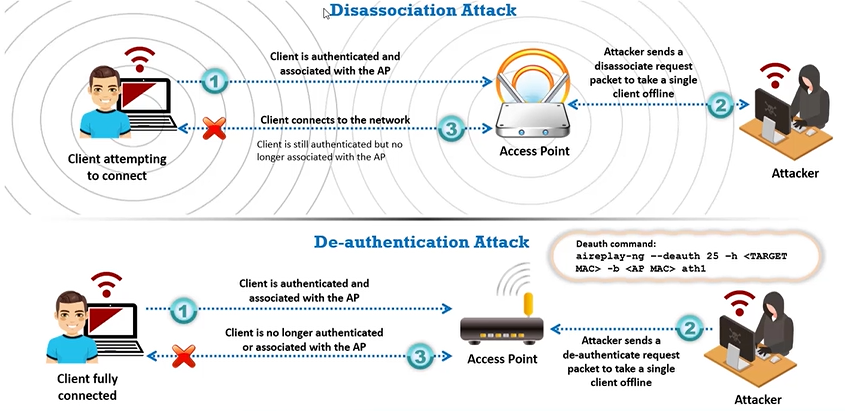
**Sniffing wireless traffic:**

Sniffing wireless traffic is an eavesdropping technique where attackers capture ongoing communications on a Wi-Fi network. By enabling monitor mode on their Wi-Fi cards, they analyze traffic using tools like Wireshark, Kismet, and CommView. This allows attackers to gather sensitive data or launch further attacks on the target network.

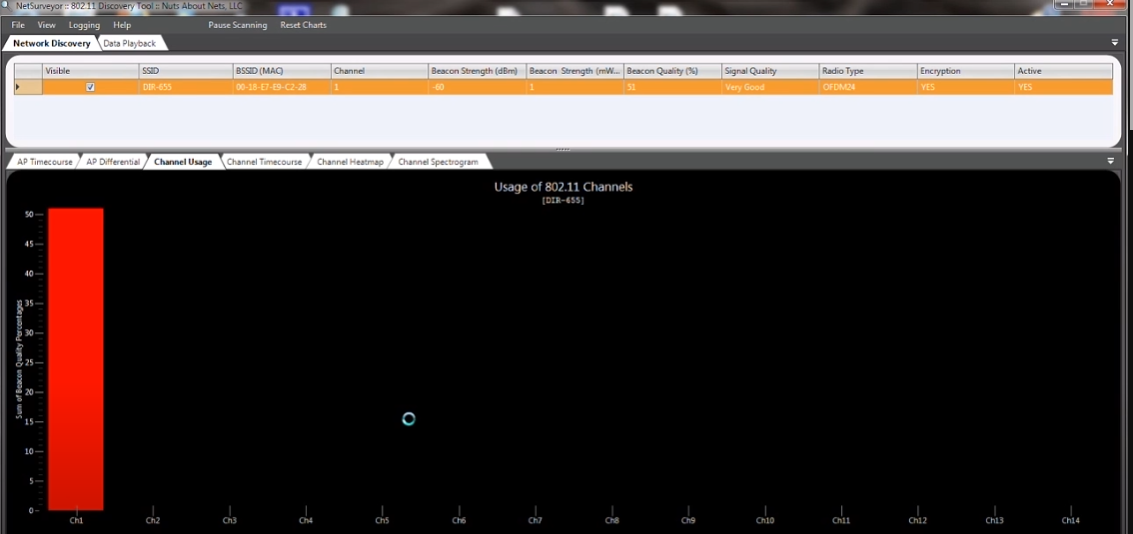
**MAC spoofing:**

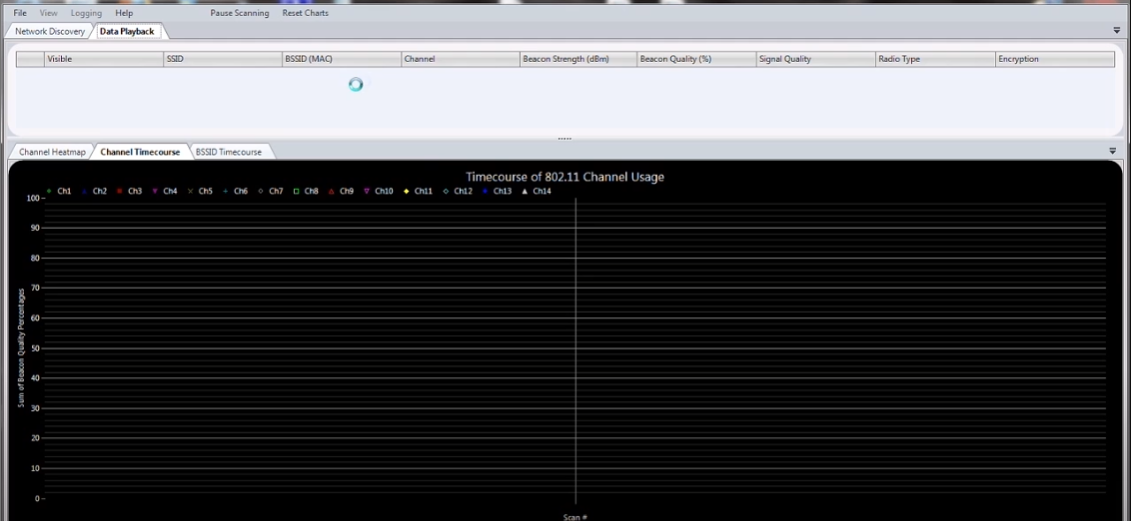
MAC spoofing is an attack where attackers change their device's MAC address to mimic an authenticated user, bypassing MAC filtering on access points (AP). By altering the MAC address using tools like Technitium MAC Address Changer, attackers gain unauthorized network access, posing security risks to wireless networks.

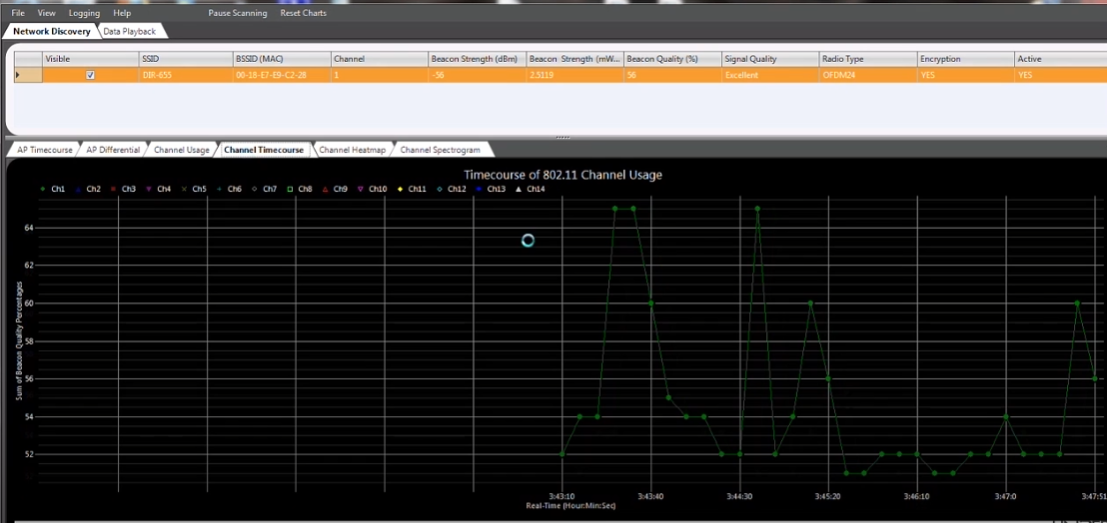
**Denial-of-Service: Disassociation and De-authentication Attacks:**

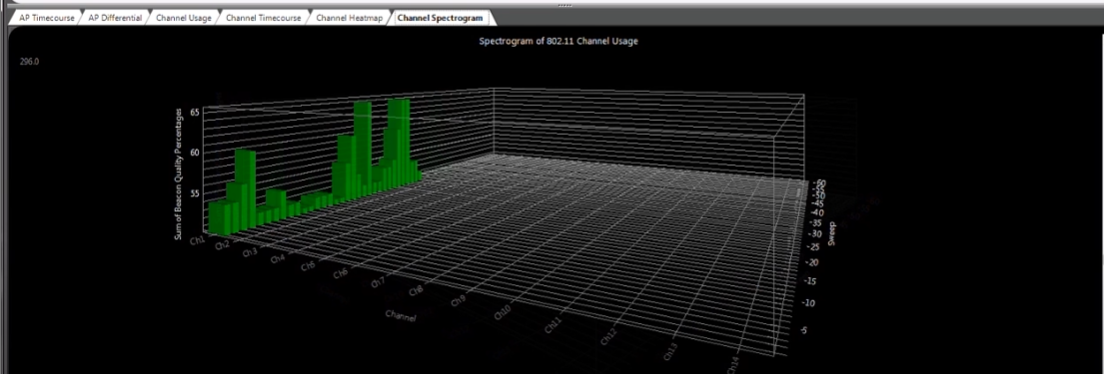


**Finding Wi-Fi network in range using Net Surveyor:**

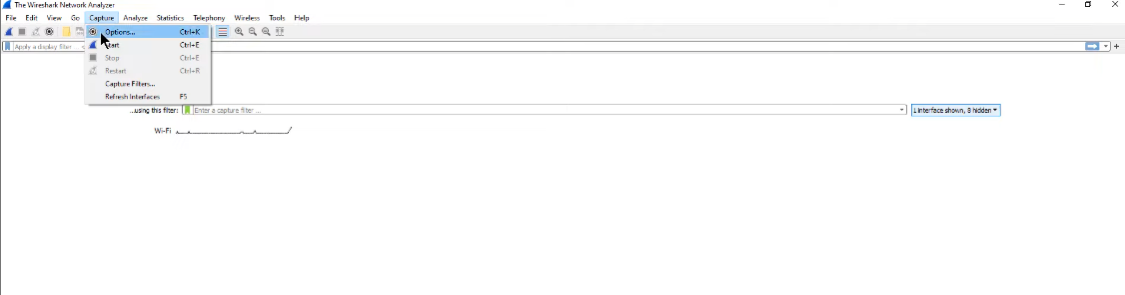


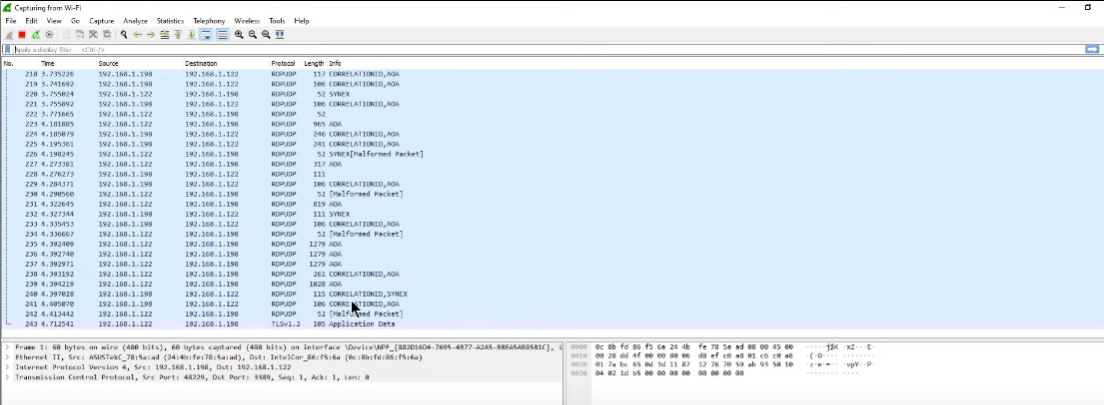


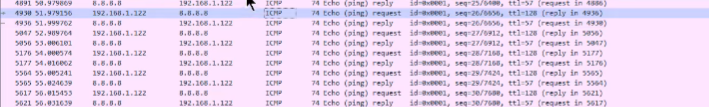




**Find wi-fi networks and sniff Wi-Fi packets using wash and Wireshark:**

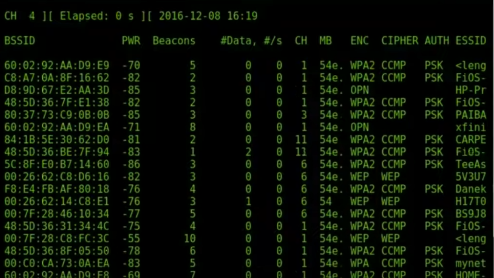


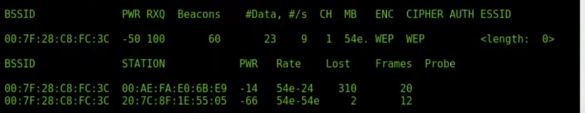


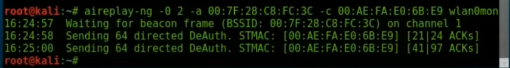


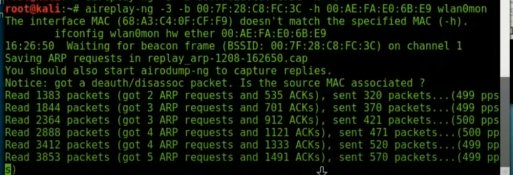
**Crack a WEP network using Aircrack-ng:**

****

****

****

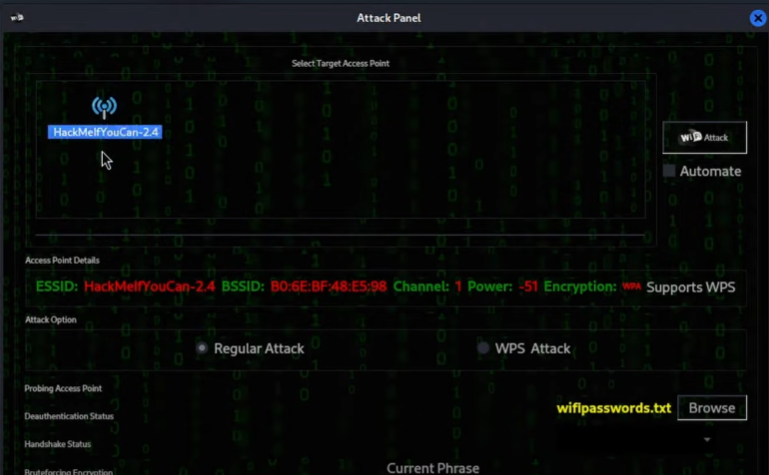
****

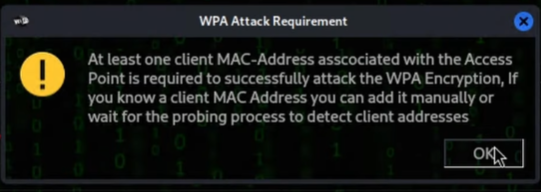
****

****

**Crack a WPA network using Fern Wi-fi Cracker:**

****

****

****