ISSN No:-2456-2165

Air Packet Capture Methods for Wi-Fi Clients Tutorial

Karthick Rajapandiyan
Principal Project Manager:
Fixed Networks, Broad Band Devices Nokia
Chennai, India

Mahendar K.
Principal Technical Specialist:
Fixed Networks, Broad Band Devices Nokia
Chennai, India

Abstract:- There are three different methods to capture Air Packets with Wifi Clients. These methods can be used for analyzing issues with respect to Wifi Clients. (1) Wifi Scanner (2) Air Magnet Wifi-analyzer (3) MacBook These three methods will be explained as tutorial in this paper.

Keywords:- *Air Packet Capture; Capture; Wifi Packet;*

I. INTRODUCTION

Understanding Wi-Fi networks is crucial in our increasingly wireless world. This document explores Wi-Fi scanning, detailing its active and passive methods and the information they provide. We'll examine various tools, from simple network scanners to advanced analyzers like AirMagnet, highlighting their applications in network design, troubleshooting, and security. We'll also cover built-in tools such as those found on Mac OS. By the end, readers will grasp how Wi-Fi scanning works and its diverse uses in managing effective wireless networks.

II. WI-FI SCANNER

Fig 1: Access Agility Wi-Fi Scanner Tool

How does Wi-Fi scanning work?

Wi-Fi Clients can scan for access points by using two different methods [1]

- Active method
- Passive method.

Active method scanning involves the process of Probe request message [2] [3] sent by Wi-Fi client and then waiting for a response from an Access point.

Passive method scanning, conversely, involves the client listening for beacon signals broadcast periodically by Access Points on each channel.

ISSN No:-2456-2165

WiFi Scanner is a user-friendly tool for designing, troubleshooting, and verifying 802.11a (5 GHz band)/802.11b (Wi-Fi 1 - 2.4 GHz band)/802.11g (2.4 GHz band)/802.11n (Wi-Fi 4)/802.11ac (Wi-Fi 5) networks. It functions as both a scanner and connection manager, providing details such as signal strength, noise levels, access point channel assignments, and manufacturer identification (based on MAC address prefixes)..

WiFi Scanner displays comprehensive information about nearby wireless access points, including channel usage, signal strength (Received Signal Strength Indicator), noise interference levels, channel bandwidth, MAC unique identifier, signal strength, maximum data transmission rate, Security encryption type, and other specification details.

This Wi-Fi scanner tool [5] supports 2.4 GHz band, 5 GHz band , and 6 GHz (6E) band networks (requiring a compatible 6E adapter on Windows). It handles all channel bandwidths (20 MHz, 40 MHz, 80 MHz, and 160 MHz) and displays detailed network parameters information including Service Set Identifier, Received Signal Strength Indicator, Basic Service Set Identifier, signal quality, channel, maximum data rate, and encryption type. Real-time graphical signal strength monitoring is included, along with filtering options (by SSID, channel, band, and signal strength) and graphical/tabular displays of connection statistics.

III. AIR MAGNET WI-FI ANALYZER

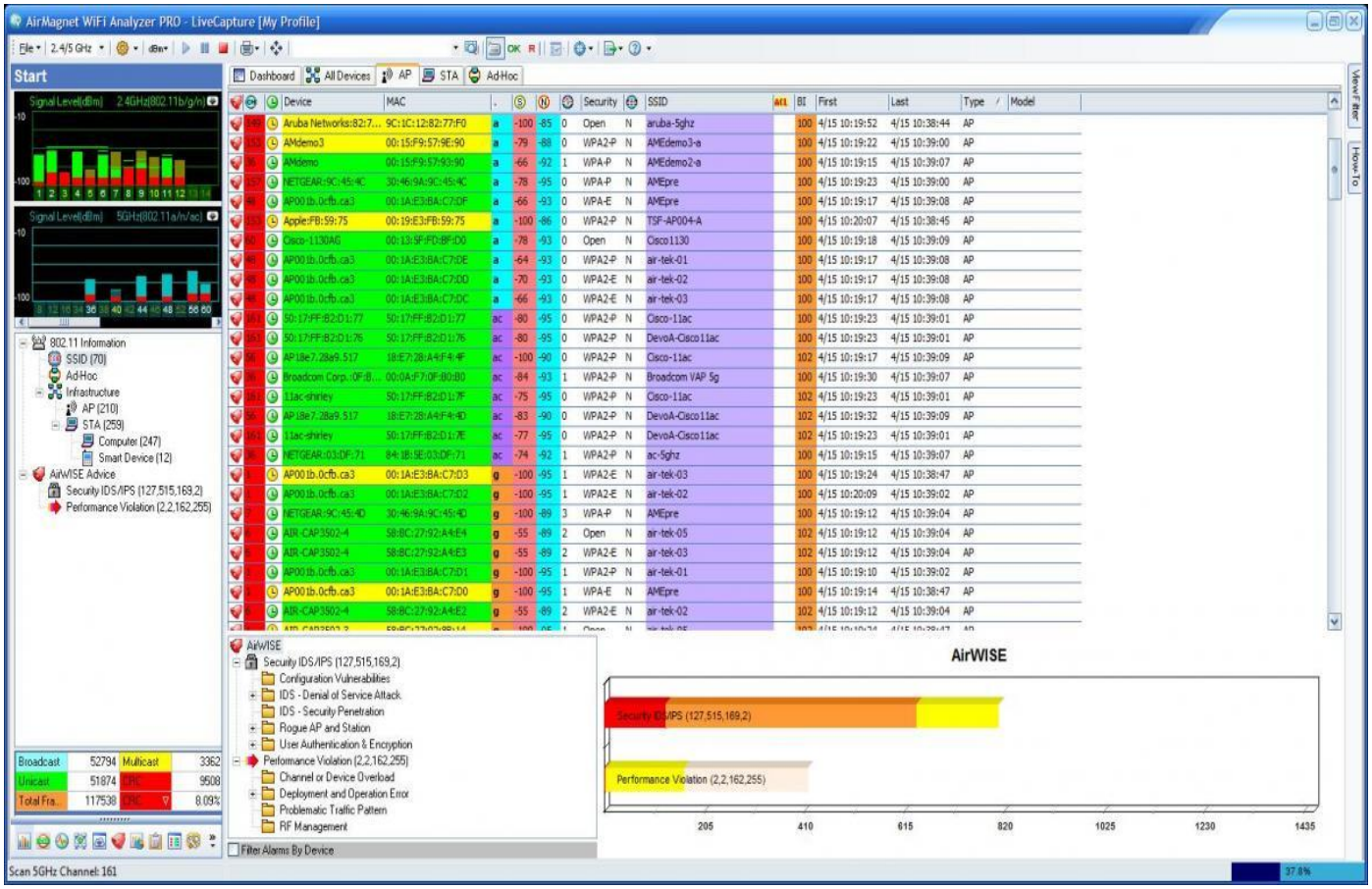

Fig 2: Air Magnet Wi-Fi Analyzer tool

AirMagnet WiFi Analyzer [4] offers in-depth analysis of all WLAN client roaming events, leveraging AirWISE® technology to provide detailed explanations for each roam, including the influencing device and channel parameters, and an assessment of the roam's success. This allows users to measure signal strength, scan for channels, troubleshoot connectivity problems, pinpoint interference sources, and perform other related tasks.

AirMagnet WiFi Analyzer captures 802.11 Wi-Fi traffic, displaying and analyzing real-time packets in its Decode Screen. Users can filter packets by channel, SSID, node, IP address, or frame type to isolate specific data. The analyzer can also decrypt WPA-PSK and WPA2-PSK encrypted packets macbook SNIFF.

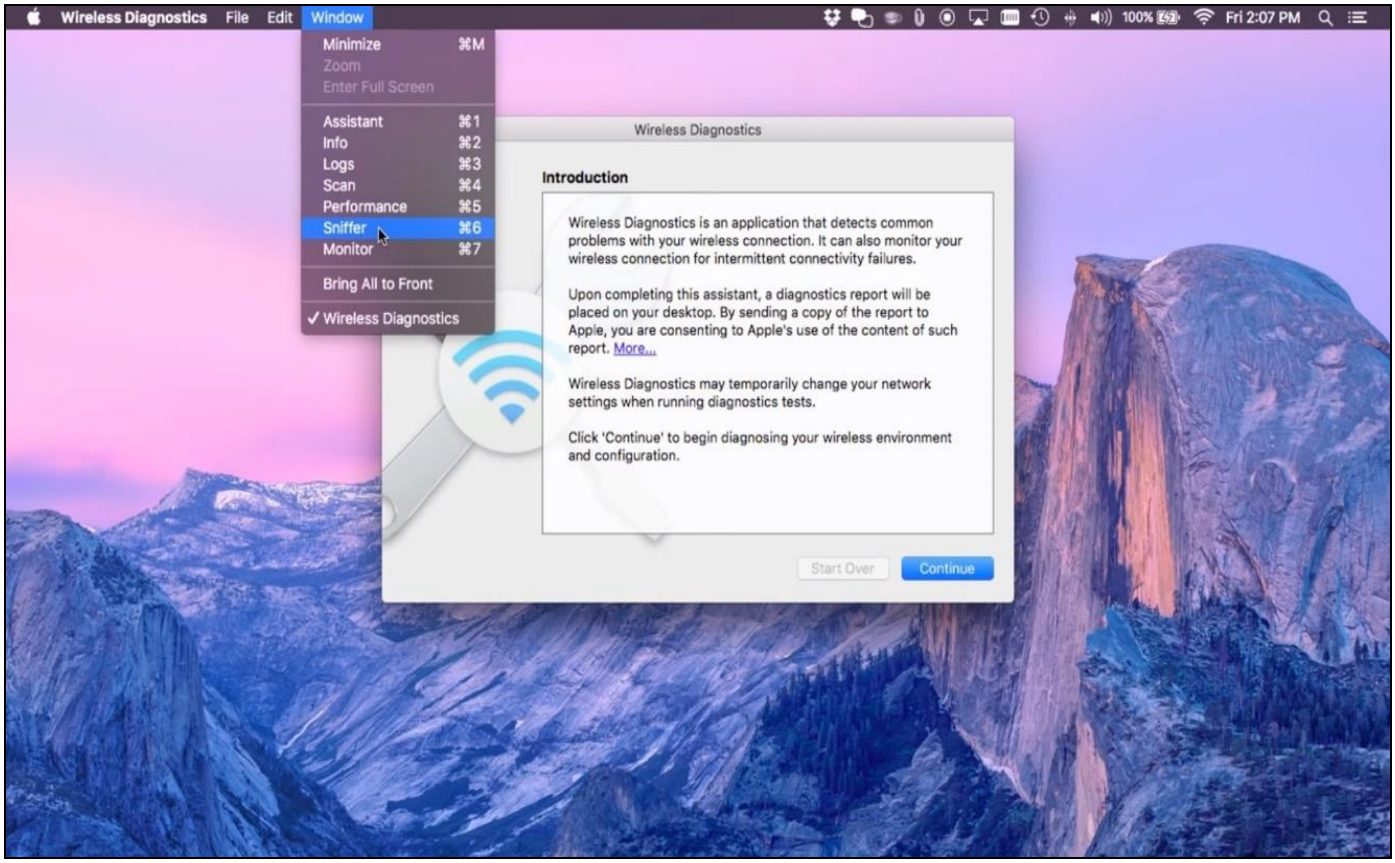

Fig 3: Mac System Sniff Tool Menu

MacBooks have a built-in utility, often referred to as a "sniffer," that can capture over-the-air (OTA) Wi-Fi data using the computer's wireless card. This functionality is useful for troubleshooting wireless network problems

How to use MacBook to take Over the Air (OTA) capture?

Mac users running OS X 10.6 or later can leverage their built-in capabilities to capture over-the-air (OTA) Wi-Fi data for troubleshooting wireless network issues.

➢ *How to Setup:*

- **Power On**: Ensure your MacBook (OS X 10.6 or later) is powered on.
- **Open Wireless Diagnostics**: Press Command + Space, type "Wireless Diagnostics," and open the utility.
- **Open Sniffer:** Go to the "Window" menu and select "Sniffer."
- **Select Channel:** Choose the desired channel from the channel dropdown menu.
- **Start Capture:** Click "Start" and enter your administrator password when prompted.
- **Capture Data:** Allow the capture to run for the necessary duration.
- **Stop and Save:** Click "Stop" to save the capture file (.wcap) to your desktop.

To verify the captures, use any packet capture analysis utility like Wireshark.

IV. CONCLUSION

In summary, understanding Wi-Fi scanning involves comprehending both active (probe request-based) and passive (beacon-listening) methods. Tools like the user-friendly Wi-Fi Scanner and the more advanced AirMagnet Wi-Fi Analyzer provide varying levels of detail and functionality for network design, troubleshooting, and security analysis. Even built-in macOS utilities offer surprisingly robust capabilities for capturing and analyzing over-the-air Wi-Fi data, highlighting the widespread availability of tools for understanding and improving Wi-Fi performance. The choice of tool ultimately depends on the user's specific needs and technical expertise.

REFERENCES

[1]. M. R. Jivthesh, M. R. Gaushik, P. Adarsh, G. H. Niranga and N. S. Rao, "A Comprehensive survey of WiFi Analyzer Tools," 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2022, pp. 1-8, doi: 10.1109/GCAT55367.2022.9972040. keywords: {Knowledge engineering; Wireless sensor networks; Visualization; Wireless networks; Employment; User interfaces; Planning; Wi-Fi; Wi-Fi analyzer; network; channel; signal intensity},

[2]. R. Rusca, F. Sansoldo, C. Casetti and P. Giaccone, "What WiFi Probe Requests can tell you," 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2023, pp. 1086-1091, doi: 10.1109/CCNC51644.2023.10060447. keywords: {Portable computers; Operating systems; Urban areas; Standardization; Communication system security; Security; Probes; Probe request; Passive sniffing; WiFi; People counting; MAC randomization},

[3]. J. Freudiger, “How talkative is your mobile device? an experimental study of Wi-Fi probe requests,” ser. ACM WiSec, New York, NY, USA, 2015. Zeb, M. Asim, W. Ali and N. Mufti, "Performance analysis of WLAN in the presence of co-frequency microwaves," 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 2017, pp. 7-11, doi: 10.1109/COMTECH.2017.8065741. keywords: {Wireless fidelity; Microwave ovens; Receivers; Microwave communication; Transmitters; Microwave Oven; Interference; Wi-Fi; WLAN; ISM; EMI},

[4]. P. Dhere, P. Chilveri, R. Vatti, V. Iyer and K. Jagdale, "Wireless Signal Strength Analysis in a Home Network," 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, 2018, pp. 1-5, doi: 10.1109/ICCTCT.2018.8550931. keywords: {Wireless fidelity; Wireless networks; Home automation; Standards; Throughput; Heating systems; Wi-Fi signal strength; access point; channel strength; Wi-Fi monitor; link speed; heat map;IP address}.