PERINTIS
Persatuan Saintis Muslim Malaysia

PERINTIS eJournal
Vol. 16, No. 1, June 2026, pp. 1 -16
e-ISSN: 2232-0725, DOI: 10.5281/zenodo.20838056

Functional Evaluation of Open-Source Network Monitoring Tools for Comprehensive WLAN Management

Abdalla Ali Abdalla Osman[1], Ibrahim Elimam[1], Yunusa Mohammed Jeddah2
[1] Department of Communications Engineering, Faculty of Engineering, Al Neelain University, Sudan
[2] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia

Corresponding author: yunusmj2@gmail.com
https://doi.org/ 10.5281/zenodo.20838056
Received 10 21, 2025
Revised 01 15, 2026
Accepted 02 16, 2026
This is an open access article under the CC BY-NC license

ABSTRACT

Wireless Local Area Networks (WLANs) are vital for modern connectivity, but they pose inherent security risks that necessitate effective monitoring solutions. Open-source tools such as Wireshark, Kismet, PRTG, Nagios, and Ettercap provide cost-effective alternatives to commercial options. However, their disparate features can leave network administrators without clear guidance for comprehensive deployment. This study systematically evaluates these tools across five key monitoring domains: discovery, mapping, monitoring, alerting, and reporting, in a controlled WLAN environment. The results reveal that no single tool comprehensively covers all functions: PRTG and Nagios offer enterprise-level automation but require paid licenses, whereas Wireshark and Kismet excel in packet and wireless analysis, yet lack integrated alerting and reporting features. Ettercap is useful for niche security testing but has limited scope for overall monitoring. The study highlights the importance of integrating different tools, proposing specific combinations (such as Wireshark with Nagios for small networks, PRTG for larger ones), and exposes gaps within current open-source solutions. These insights enable administrators to make informed decisions and guide future developments toward unified, comprehensive WLAN monitoring frameworks.

Keywords: Open-Source Monitoring Tools; WLAN Management; Network Security Auditing; Toolchain Integration; Functional Benchmarking

1.0 INTRODUCTION

WLANs remain essential for modern connectivity, based on IEEE 802.11 standards that allow high-speed data transfer (up to 54 Mbps in earlier versions [1]) without physical connections. Their widespread use across various sectors is due to benefits like cost savings, mobility, and scalability [2]. However, because they use radio frequencies, they face inherent security risks such as eavesdropping, impersonation, and unauthorized access, which wired networks do not encounter [3]. Although encryption protocols like WPA3 help reduce some risks, the constantly evolving threat environment requires ongoing network monitoring as an additional security measure.

Open-source tools for network monitoring are vital for maintaining WLAN security, providing functions from device detection to intrusion prevention. Tools such as Wireshark (for packet analysis) and Nagios (for infrastructure monitoring) are popular because they deliver detailed insights into network traffic and system health [4]. However, these tools focus on different areas: Wireshark specializes in protocol analysis but lacks automated alerts and large-scale

monitoring [5]. While Kismet offers wireless threat detection and passive monitoring, it does not include advanced reporting or visualization features [6].

Most research has examined individual open-source monitoring tools separately, but there's a notable lack of systematic comparison across the five key functions needed for effective WLAN management: device discovery, topology visualizations via mapping, real-time traffic monitoring, anomaly alerts, and reporting. Existing studies have not assessed whether these tools collectively meet operational needs or identify the best tool combinations for different environments, such as small networks versus large enterprise systems. This gap leaves network administrators without evidence-based advice on selecting and integrating the right monitoring solutions.

2.0 LITERATURE REVIEW

In this study, we evaluated five open-source tools- Wireshark, Kismet, PRTG, Nagios, and Ettercap- in a diverse WLAN environment. We measure their performance across five essential functions and assess how well they work together. Results show that while PRTG and Nagios provide the most comprehensive monitoring options, they require paid licenses for advanced features. Wireshark and Kismet excel at detailed packet and wireless-level analysis but need third-party tools for alerting and reporting. No single tool can fully cover all five functions, highlighting the need for integrated open-source frameworks. Our findings give network administrators a practical guide for choosing suitable tools based on their needs and point to key areas where the open-source community can focus on improving functionality.

Wireless networks are more vulnerable to intrusion attacks than wired ones. Attackers often exploit these weaknesses by creating rogue access points or using techniques like packet sniffing and man-in-the-middle (MITM) attacks to steal sensitive data. As WLANs become more integral to organisations, effective monitoring tools to detect and respond to threats are essential. While commercial solutions are available, open-source tools provide a cost-effective and adaptable alternative, especially for educational and small business settings.

Recent studies continue to validate the effectiveness of open-source tools in wireless network auditing, particularly in identifying vulnerabilities and enhancing security. Airgeddon and Fluxion, two open-source Wi-Fi auditing tools, were evaluated for their ability to simulate Evil Twin attacks. The study found that while both tools are capable of setting up malicious access points, they require significant troubleshooting to work with various adapters. The commercial WiFi Pineapple Tetra was found to be more user-friendly [7].

A comparative analysis of Nagios, OpenNMS, and Zabbix, three commonly used open-source network monitoring tools, was conducted by [3], revealing that each has diverse strengths across performance, fault, and security management. They emphasized the importance of choosing tools based on precise network requirements and operational circumstances.

The recent integration of Raspberry Pi with Kali Linux has been enhanced through Nexmon firmware patches, which enable onboard Wi-Fi interfaces to support monitor mode and frame injection. This eliminates the need for external adapters and makes the Raspberry Pi a more viable platform for portable wireless assessments [8].

In educational environments, WPA2 and WPA3 vulnerabilities remain a serious concern. A recent study by [9] simulated attacks on these protocols using Proof of Concepts, revealing exploitable weaknesses and proposing targeted preventive measures to improve protocol resilience.

A focused study on WPA2-Enterprise privacy in higher education highlighted metadata exposure risks and the need for stronger authentication protocols [10]. The research

emphasized that while WPA2-Enterprise is widely adopted, its implementation often lacks sufficient privacy safeguards.
While these studies contribute valuable insights, there is limited comparative analysis of different open-source tools across core functions such as discovery, mapping, monitoring, alerting, and reporting. This creates an opportunity to evaluate and benchmark these tools together, giving network administrators practical guidance on their deployment and performance.

Although existing research confirms the usefulness of open-source tools, many focus on individual tools or specific attack types. There is limited comparative analysis across multiple tools for key network monitoring tasks, highlighting the need for a comprehensive evaluation to help administrators choose the best solutions.

3.0 METHODOLOGY

This study employed a systematic experimental approach to evaluate five open-source network monitoring tools in a controlled wireless LAN environment. The methodology was designed to objectively assess each tool's capabilities across five critical network monitoring functions: device discovery, network mapping, traffic monitoring, alert generation, and reporting.

3.1 Tool Selection Rationale

The selected tools - Wireshark, Kismet, PRTG, Nagios, and Ettercap - were chosen based on their open-source availability, cross-platform compatibility, relevance to WLAN auditing tasks, and active community support. These criteria ensured the evaluation focused on widely adopted tools with sustainable development ecosystems.

3.2 Experimental Configuration

The test environment consisted of a heterogeneous WLAN comprising three commercial routers (TP-Link Archer C7, ASUS RT-AX55, and MikroTik hAP ac²) and twelve client devices spanning multiple operating systems. Each tool was deployed on its optimal platform: Wireshark and Ettercap on Kali Linux 2023.3, Kismet on Ubuntu 22.04 LTS, PRTG on Windows 11 Pro, and Nagios Core via its preconfigured VMware image.

3.3 Evaluation Framework

The assessment followed a rigorous functional testing protocol examining each tool's performance across five core capabilities. Discovery functionality was evaluated by measuring detection rates for both visible and hidden network devices. Mapping capabilities were assessed through topology visualization and geolocation features. Monitoring performance was tested via real-time traffic analysis and protocol filtering. Alert systems were evaluated based on notification customization and anomaly detection. Reporting functionality was examined through log generation and data export options.

3.4 Data Collection and Analysis

Quantitative metrics included packet capture rates, device detection times, and alert response latency. Qualitative assessment focused on configuration complexity, interface usability, and interoperability between tools. All tests were conducted three times to ensure result consistency, with performance metrics averaged across trials.

3.5 Workflow Visualization

The experimental workflow followed a standardized sequence as illustrated in Figure 1. The process began with tool installation and configuration, proceeded through function-specific testing phases, and concluded with comparative analysis. This systematic approach ensured consistent evaluation conditions across all tools while maintaining real-world applicability.

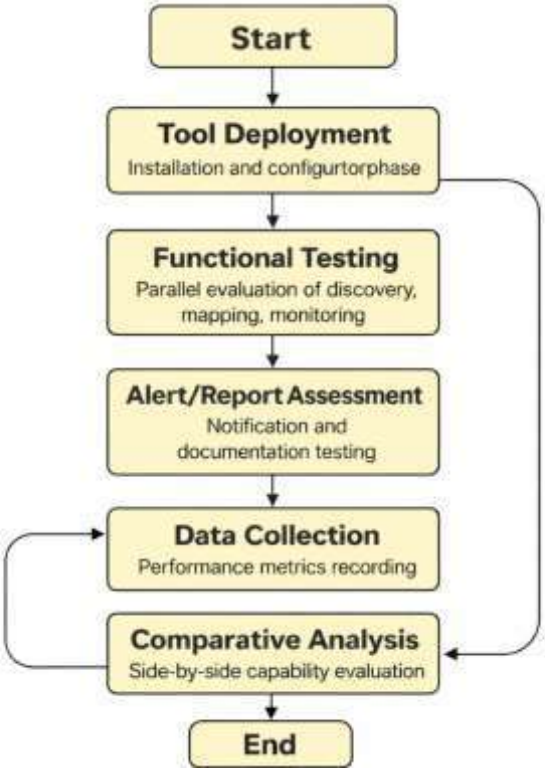

Figure 1. WLAN Auditing Workflow Diagram

4.0 RESULTS AND DISCUSSION

4.1 Functional Performance of Network Monitoring Tools

Five open-source tools: Wireshark, Kismet, PRTG, Nagios, and Ettercap, were evaluated for their capabilities in discovery, mapping, monitoring, alerting, and reporting. Below, we present their performance in a controlled Wi-Fi network environment.

Wireshark demonstrated superior packet-level analysis capabilities, successfully identifying all active hosts when the wireless interface (TL-WN722NC) was set to monitor mode using the command sudo airmon-ng start wlan0. Targeted scanning was achieved through channel selection (e.g., *Channel 1, 2.412 GHz, 20 MHz bandwidth*), as illustrated in Figure 2. While the tool offered limited geolocation support via IP-based mapping, the reliability of this feature was compromised by IPv4 spoofing risks. For monitoring, Wireshark captured real-time traffic with protocol-specific filters (e.g., ip.src == 192.168.8.176) (Figures 3 - 5) and provided granular frame-level details, including MAC addresses and radio tap headers (Figures 6 - 8). However, it lacked native alerting systems and required manual extraction of packet data for reporting, posing limitations for automated network management.

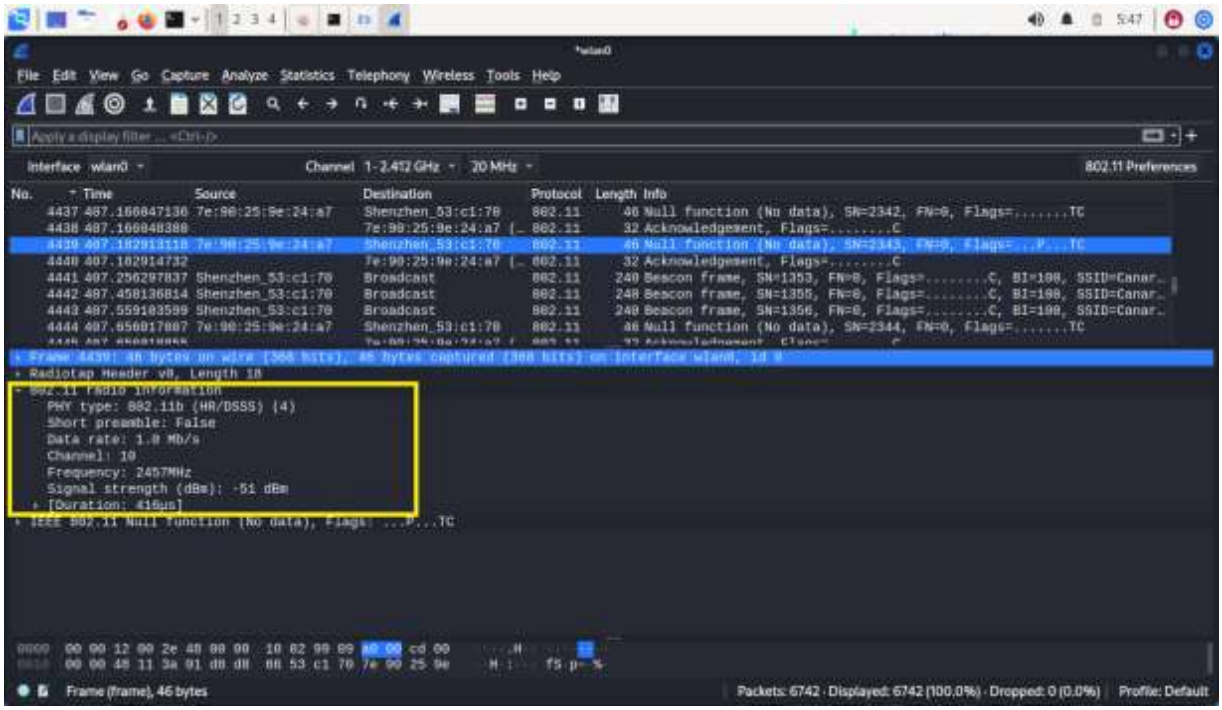

Figure 2 IEEE 802.11 Radio information

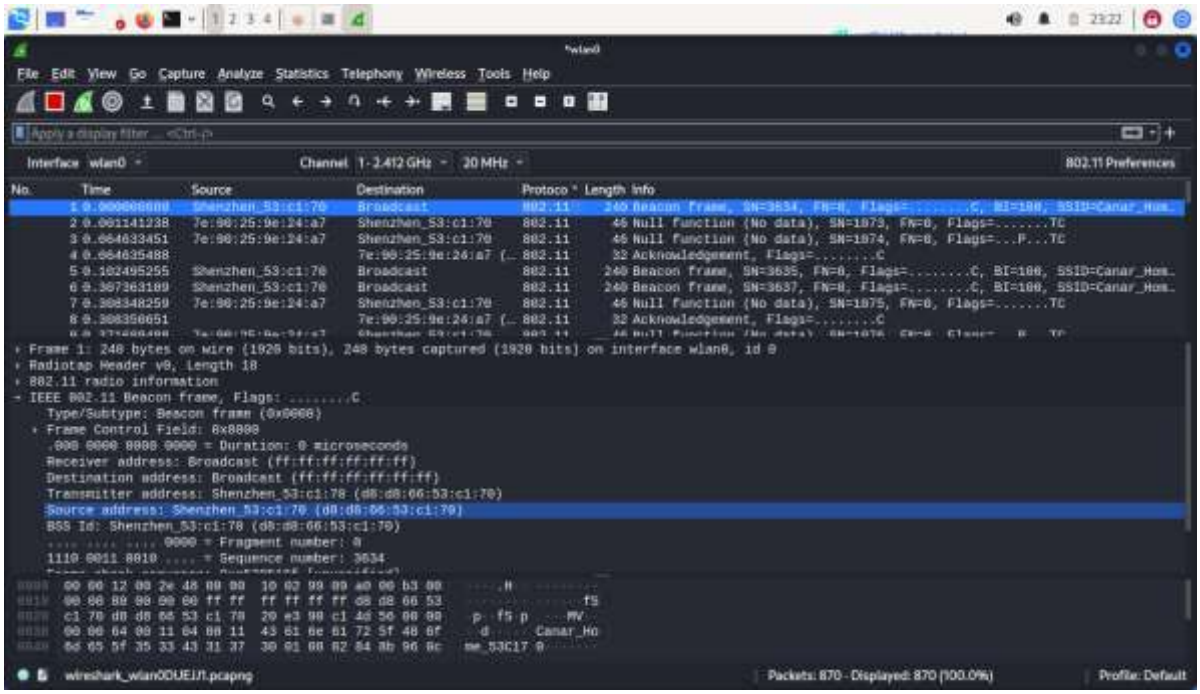

Figure 3 Live packet capture

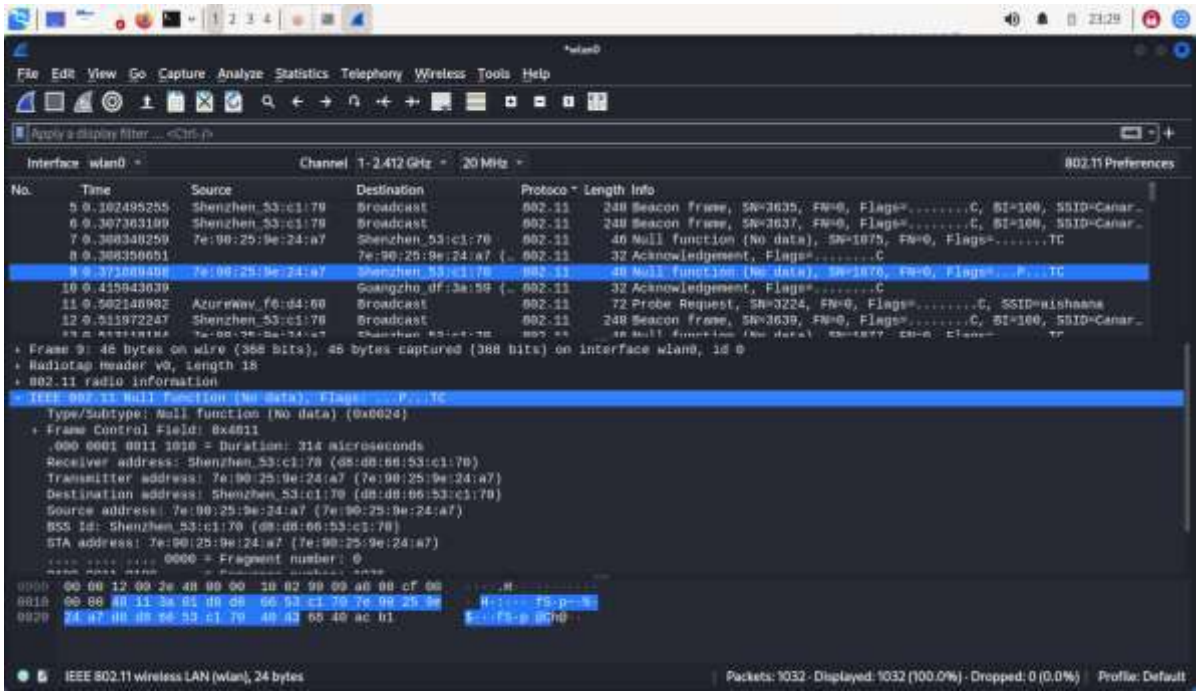

Figure 4 Details of the packet.

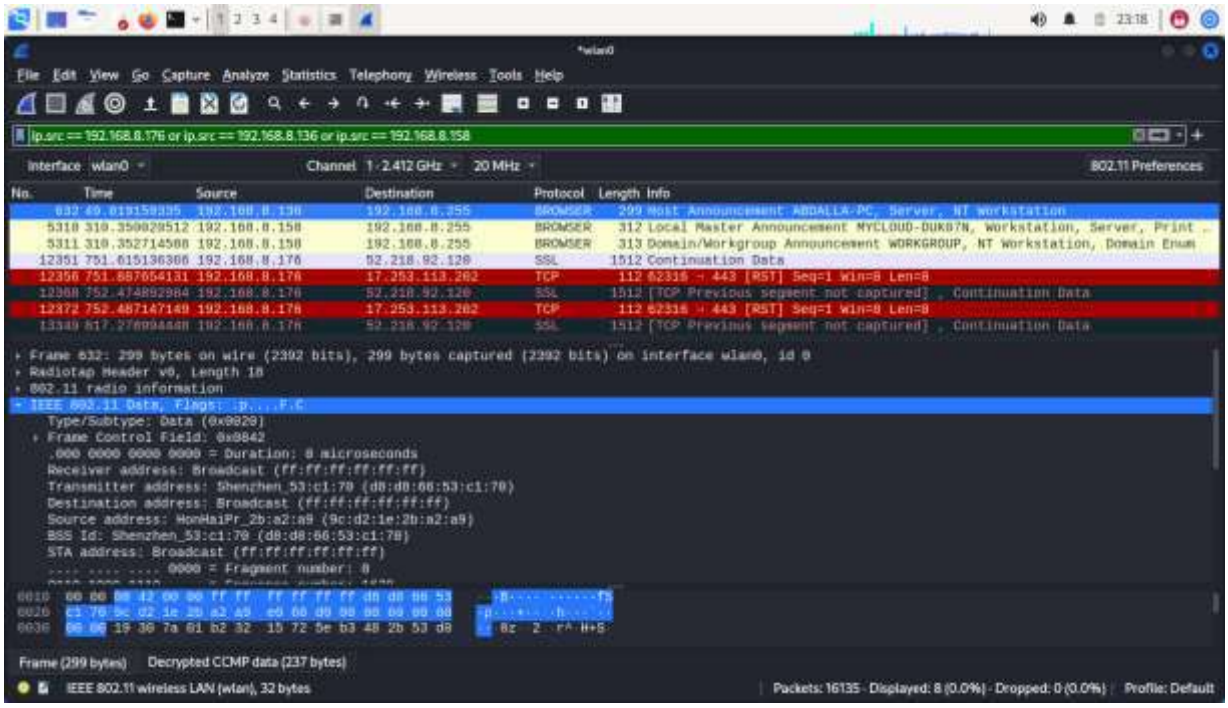

Figure 5 Details of filter packets.

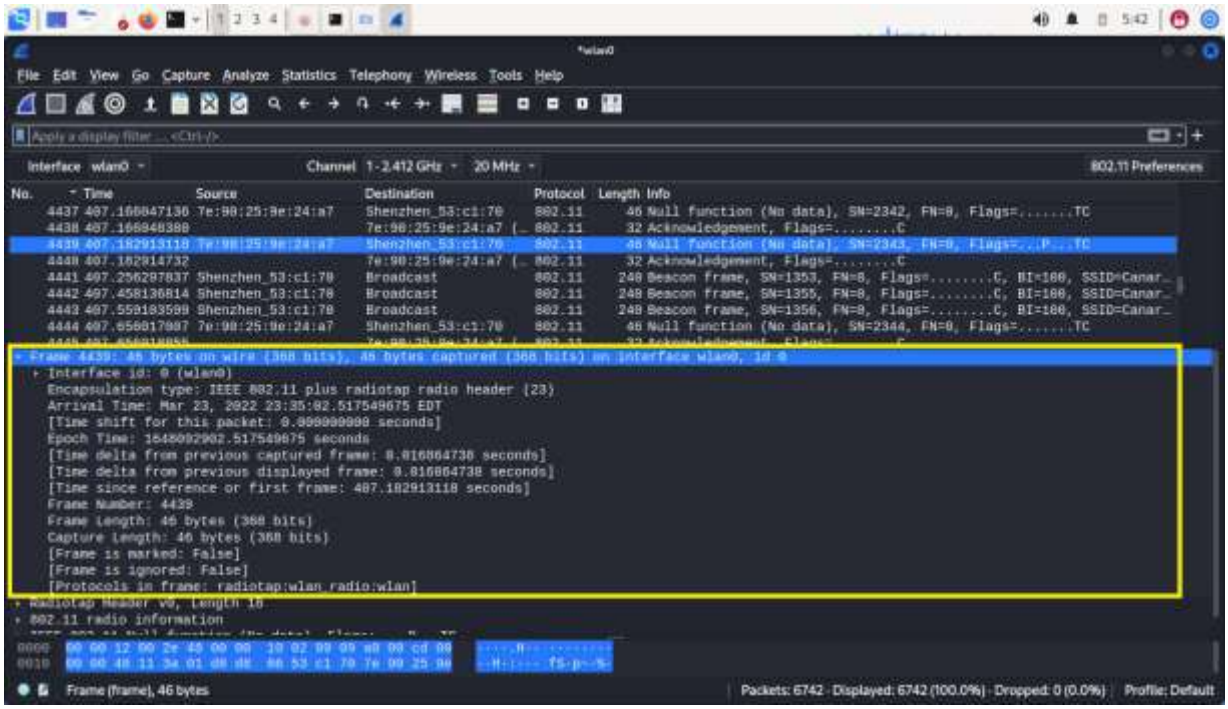

Figure 6 Frame details in the yellow box.

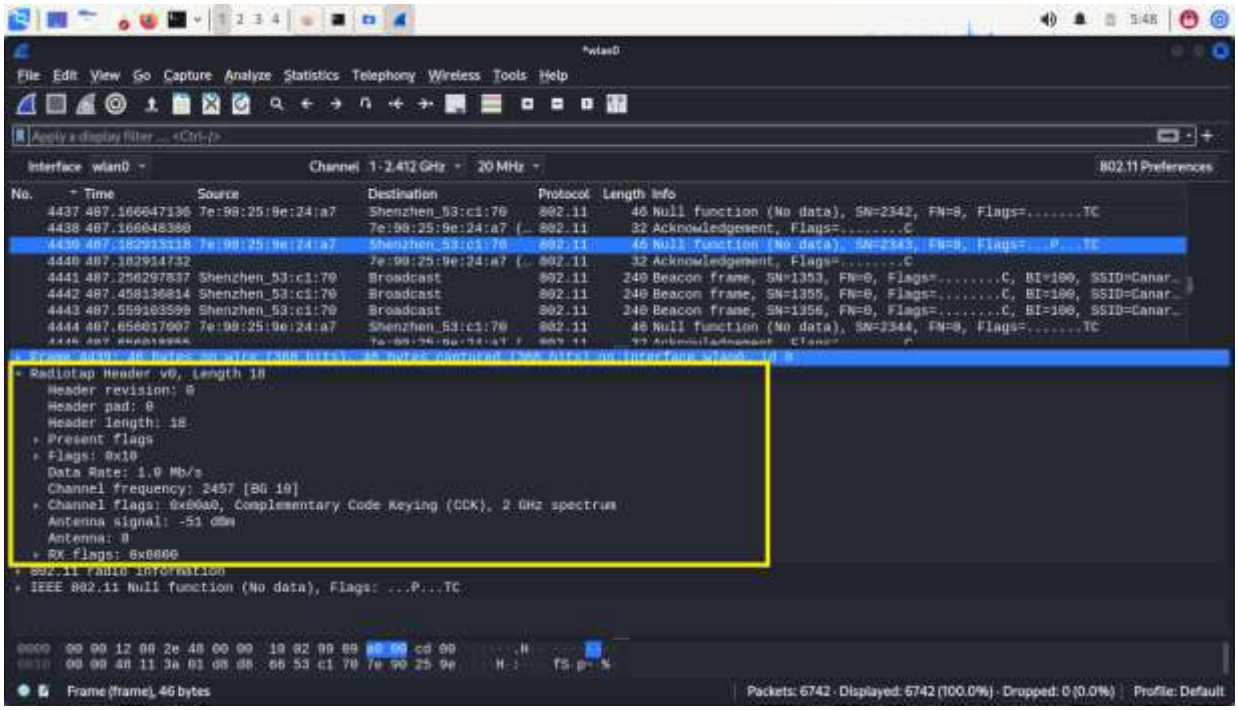

Figure 7 Radio tap Header.

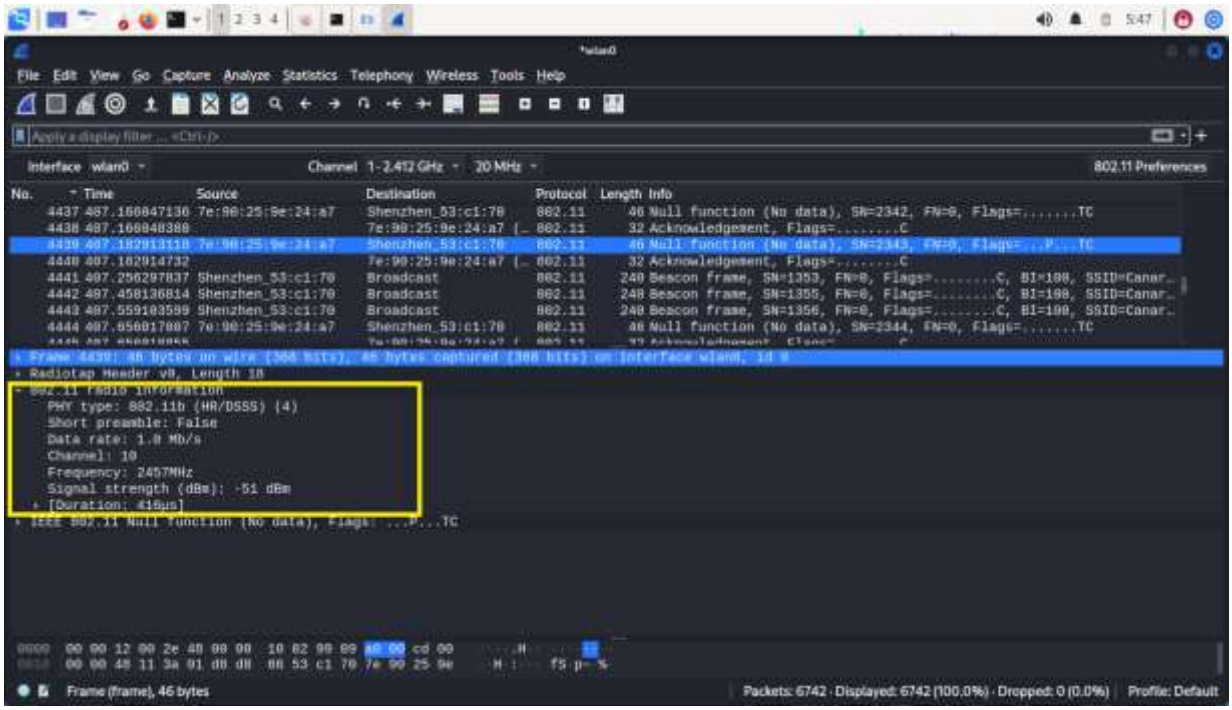

Figure 8 IEEE 802.11 Radio information.

Kismet excelled in wireless network discovery and intrusion detection, detecting hidden SSIDs and connected devices (Figures 9 - 10) after activating monitor mode (*iwconfig INTERFACE mode monitor*). The tool supported GPS integration (*GPSd*) for physical network mapping, though this feature remained untested due to hardware constraints. Kismet's real-time intrusion alerts, delivered via its message bus (Figure 9), enhanced its utility for security monitoring. Captured data could be exported in *.pcap* format for further analysis in Wireshark, bridging functionality between the two tools.

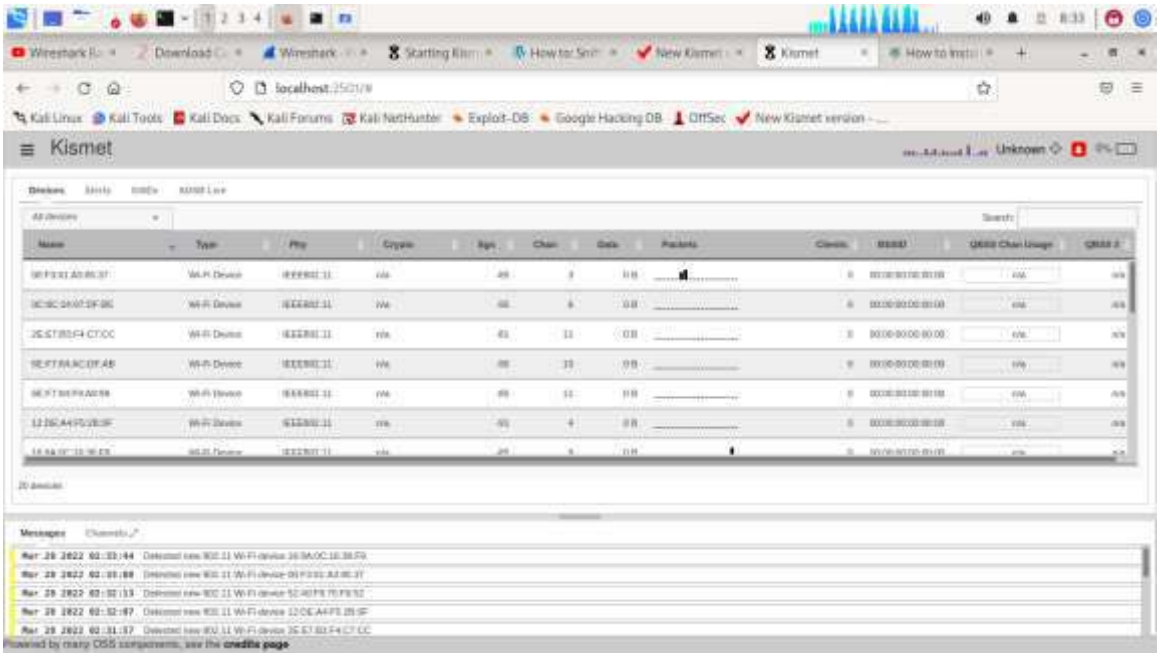

Figure 9 Live data capturing.

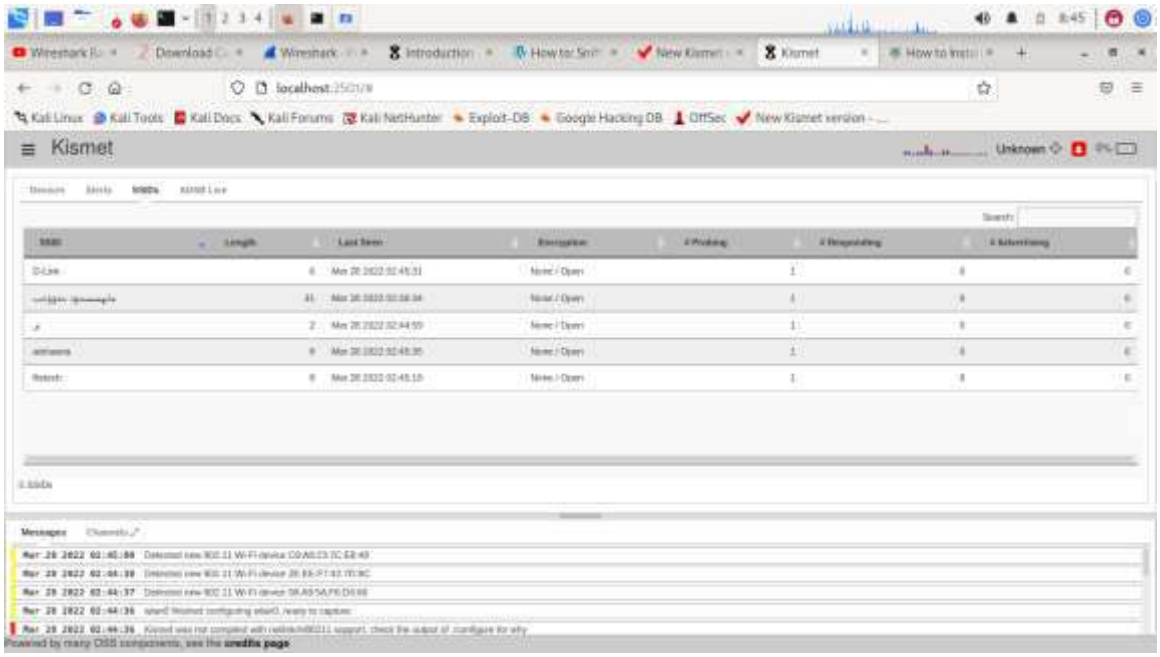

Figure 10 Captured SSIDs

PRTG (Paessler) provided enterprise-grade network monitoring with automated reporting. The system automatically detected devices via router IP scanning (Figure 11) and presented real-time performance graphs for bandwidth utilisation, disk usage, and HTTP sensors (Figures 12 - 15). Sensor-based alerts, including disk space warnings (Figure 16), alongside customizable HTML and PDF reports (Figure 17), enhanced network administration efficiency. The free version was used for this study, which is limited in sensor count, while advanced features such as Google Maps integration required a paid license, and the 30-day trial constrained extended use without purchase.

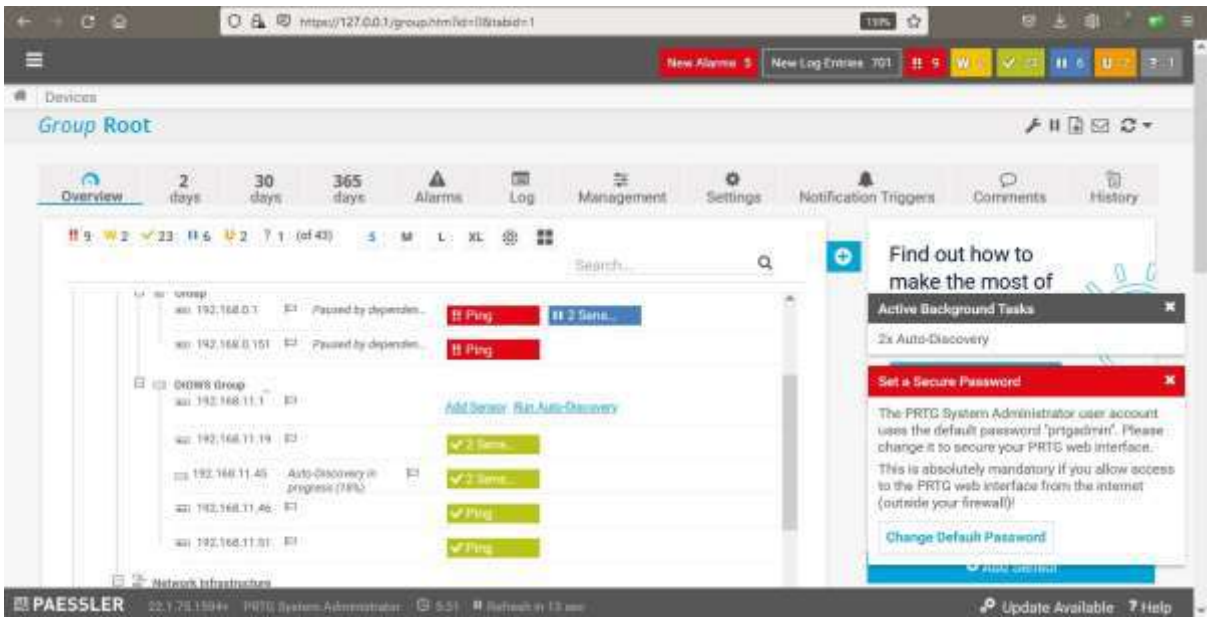

Figure11 DIOWS Group

Figure 12 Local probe graph

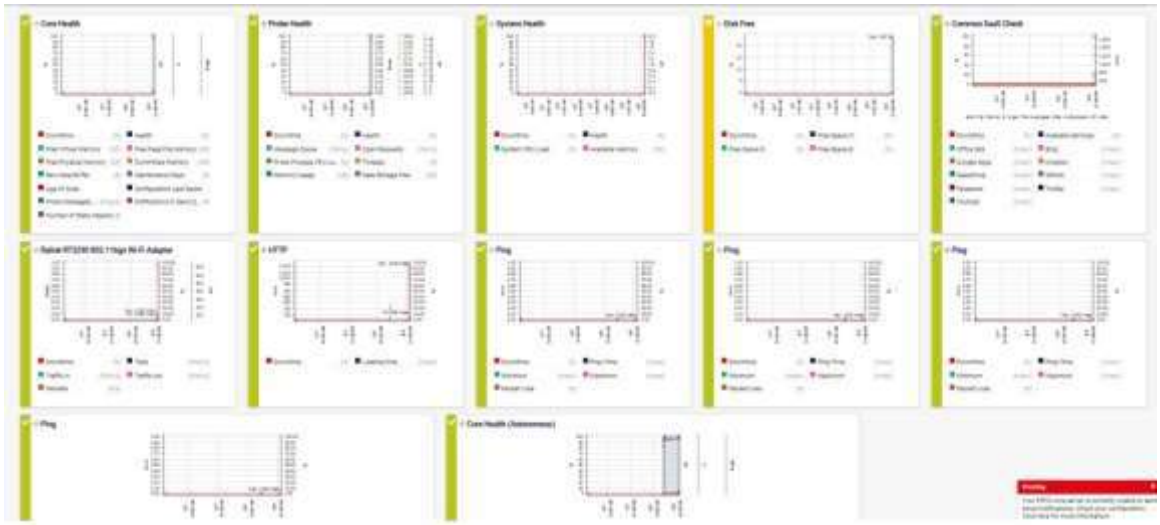

Figure13 Entire local probe with all the sensors

Figure 14 Wi-Fi Sensor with Ok Massage

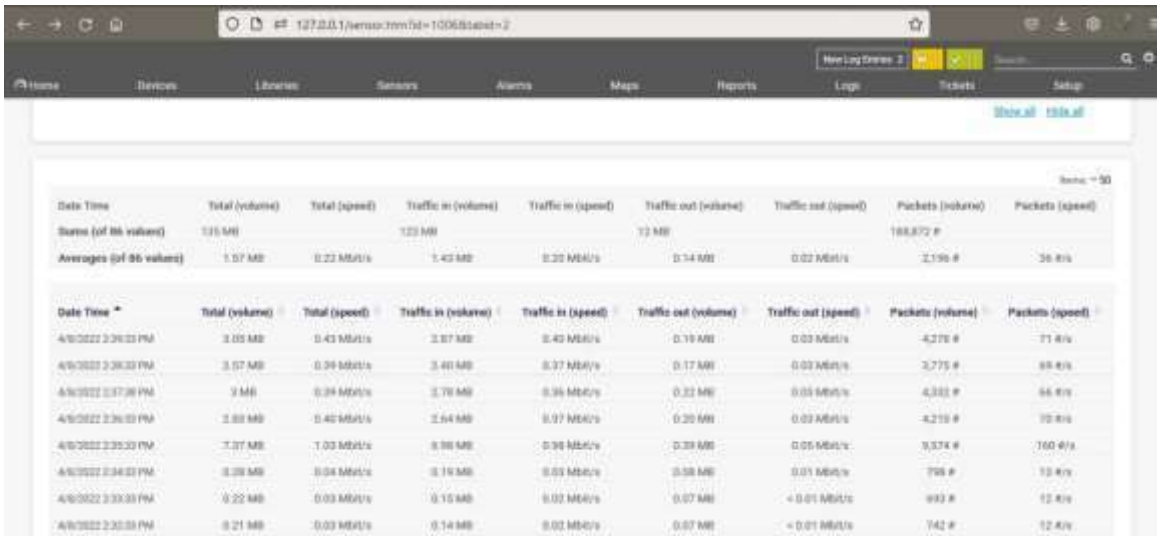

Figure 15 Captured Data for Wi-Fi Sensor

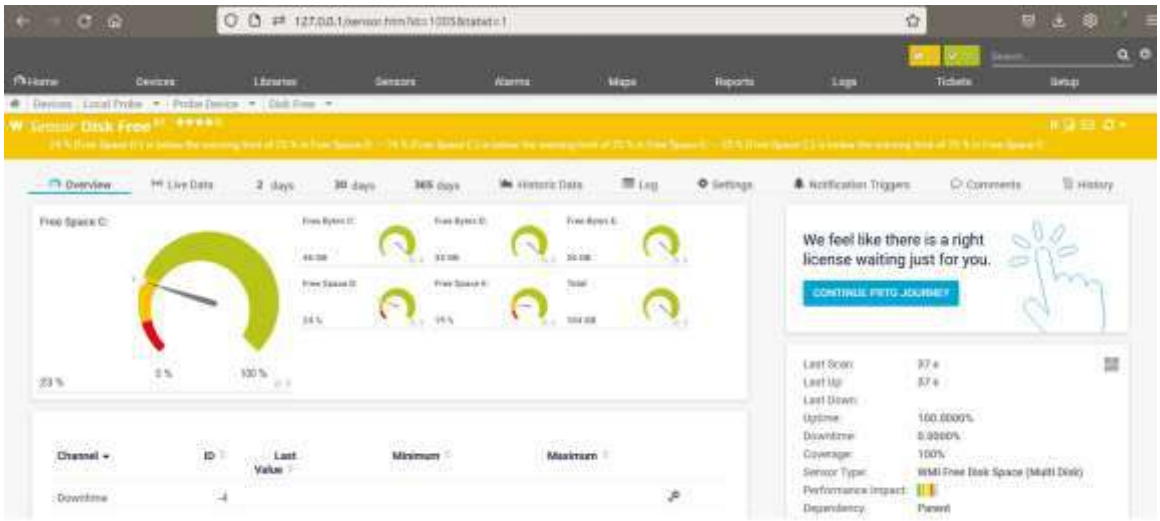

Figure 16 Disk Space sensor sends warning

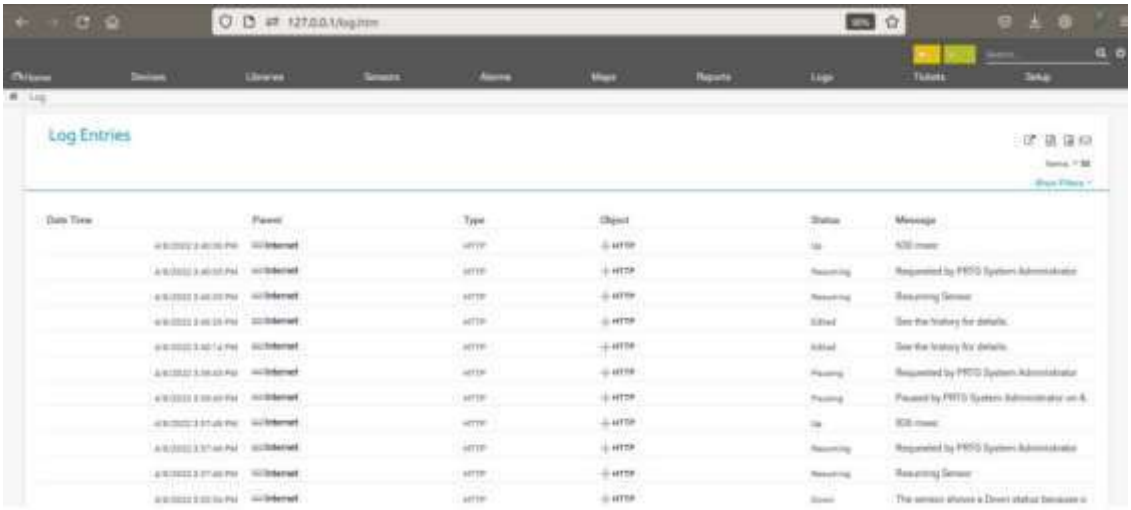

Figure 17 Total log entries

Nagios proved effective for infrastructure monitoring, categorizing hosts as *Up*, *Down*, or *Unreachable* (Figures 18 - 20) and tracking service statuses (e.g., HTTP, disk space) with detailed warnings and critical alerts (Figures 21 - 22). Its dashboard provided incident logs and performance trends, but the free version was limited to small-scale deployments. Additionally, the setup process was complex, requiring multiple component installations.

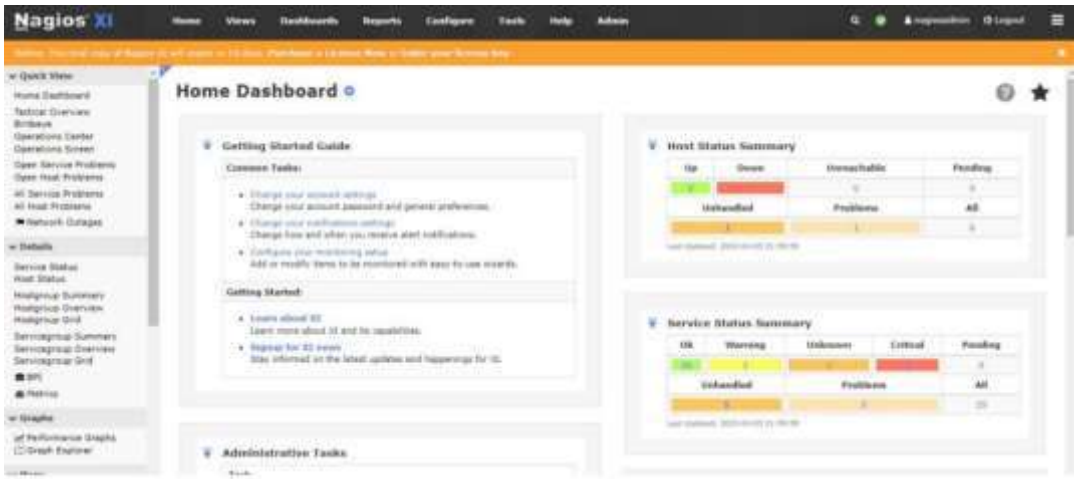

Figure 18 Home Dashboard

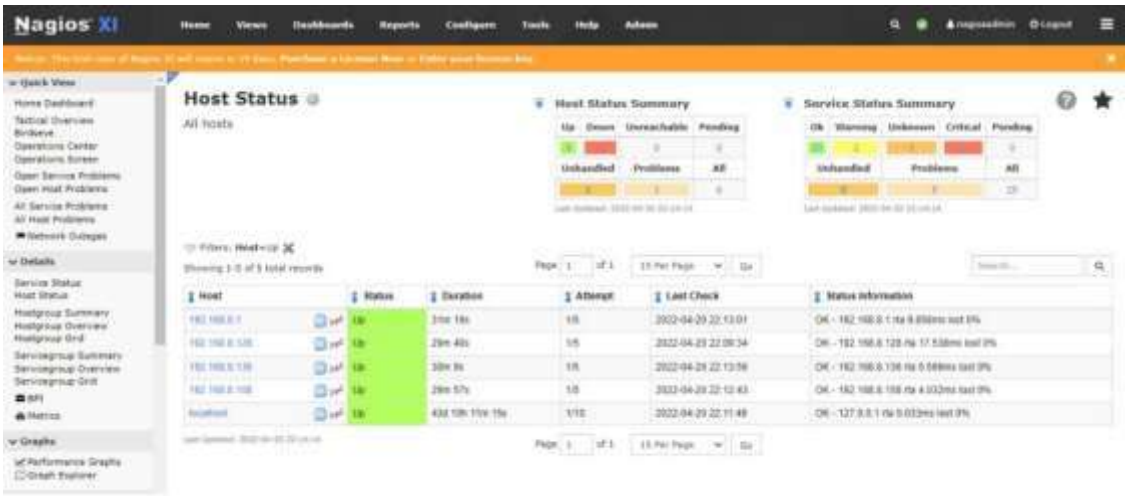

Figure 19 All Up Hosts

Figure 20 Down Hosts

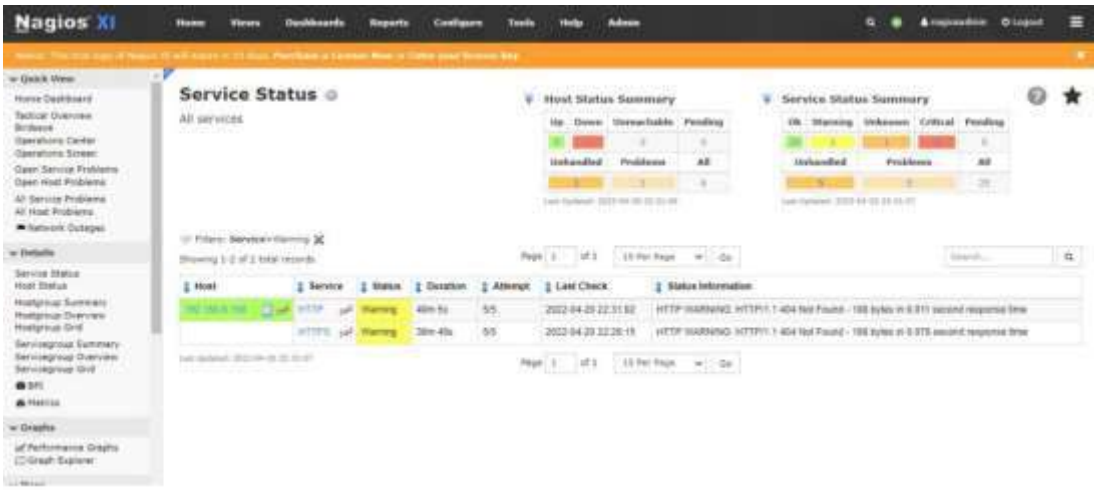

Figure 21 Services with warnings

Figure 22 Services with critical warnings

Ettercap was employed for security vulnerability assessments, identifying connected hosts via ARP scanning (Figure 23) and executing Man-in-the-Middle (MITM) attacks through ARP poisoning (Figure 24). While valuable for penetration testing, the tool lacked built-in mapping, reporting, or alerting features, relegating it to a specialized security-auditing role rather than a comprehensive monitoring solution.

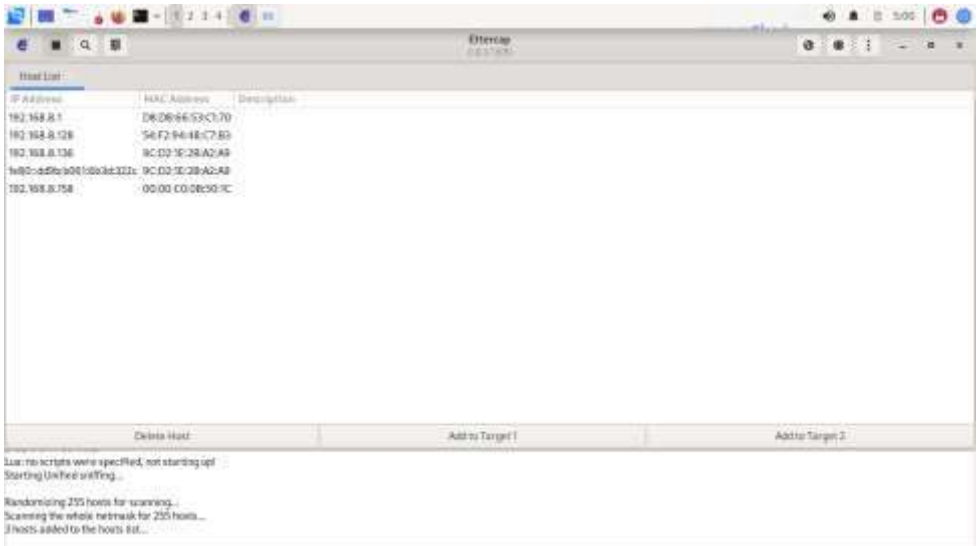

Figure 23 Viewing Available Hosts

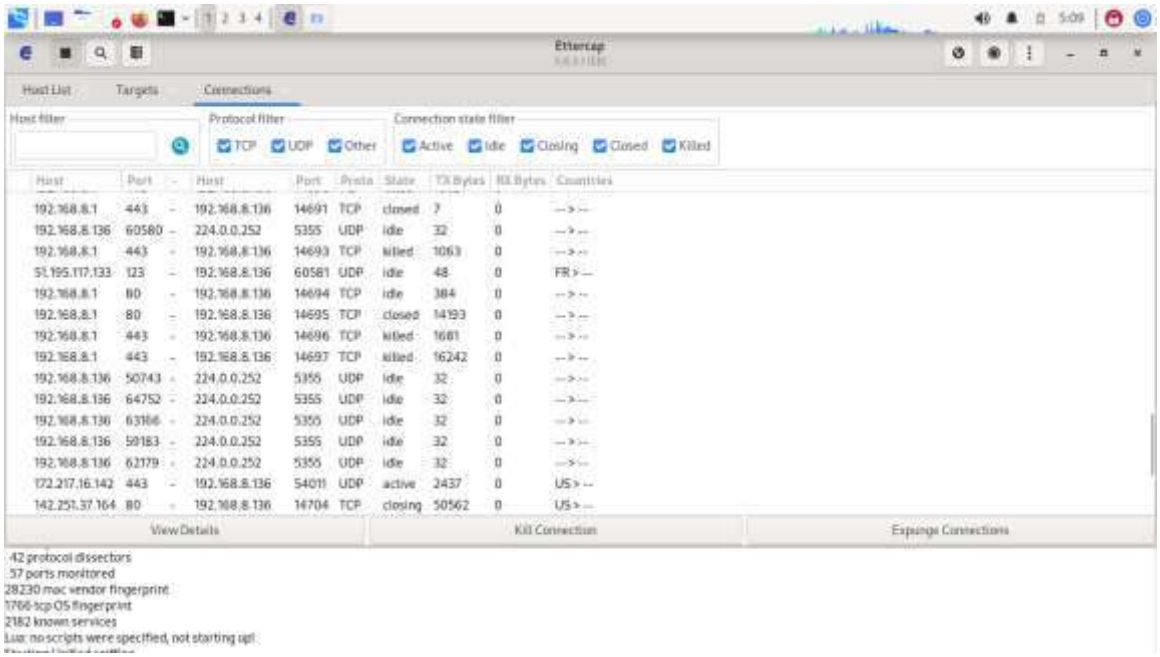

Figure 24 Viewing current target connections.

4.2 Comparative Analysis

A systematic comparison of the tools (Table 1) reveals trade-offs between functionality and use-case suitability:

Table 1. Comparative Performance of Network Monitoring Tools

Tool	Discover	Map	Monitor	Alert	Report
Wireshark	✅ (Packet capture)	❌ (IP-only)	✅ (Real-time)	❌	❌ (Manual export)
Kismet	✅ (Hidden SSIDs)	✅ (GPSd-enabled)	✅ (Wireless)	✅ (Intrusion)	❌ (. pcap only)
PRTG	✅ (Auto-scan)	⚠️ (Paid feature)	✅ (Sensor-based)	✅ (Custom)	✅ (HTML/PDF)
Nagios	✅ (Host status)	❌	✅ (Services)	✅ (Logs)	✅ (Trends)
Ettercap	✅ (ARP scan)	❌	⚠️ (MITM only)	❌	⚠️ (Logs)

✅ = Fully Supported ⚠️ = Limited or Indirect Support ❌ = Not Supported

4.3 Comparative Analysis and Key Findings

All the evaluated tools demonstrated host discovery capabilities, though Kismet and Wireshark provided more advanced functionality through packet-level and wireless-specific detection methods, respectively. Geographic mapping features were uniquely available in Kismet (via GPSd integration) and PRTG (through premium licensed features). Monitoring implementations varied significantly, with PRTG and Nagios offering fully automated solutions while Wireshark and Kismet necessitated manual configuration and operation. The alerting and reporting functions showed particularly stark contrasts - PRTG and Nagios delivered comprehensive, enterprise-ready alert systems and reporting frameworks, whereas Ettercap and Wireshark either lacked these features entirely or provided only basic implementations.

Critical evaluation revealed several key insights: First, no individual tool provided complete coverage across all five core functions (discovery, mapping, monitoring, alerting, and reporting). For specialized security auditing tasks, Kismet and Ettercap proved most effective, though their utility was somewhat limited by reporting deficiencies. PRTG and Nagios emerged as the most complete solutions for administrative purposes, despite their commercial licensing requirements for full functionality. Wireshark maintained its essential role for detailed packet analysis, though practitioners would need to supplement it with additional tools to achieve comprehensive monitoring capabilities, including alerts and reports. These findings underscore the importance of tool selection based on specific operational requirements and the potential value of integrated solutions combining multiple specialized tools.

5.0 CONCLUSION

This study assessed five open-source network monitoring tools, Wireshark, Kismet, PRTG, Nagios, and Ettercap, across five key functions: discovery, mapping, monitoring, alerting, and reporting, within a controlled WLAN environment. The results offer comparative, evidence-based insights to assist network administrators and security experts in choosing and implementing suitable monitoring solutions.

The findings confirm that no single tool fully supports all five functions. Function coverage analysis shows only two tools (40%), PRTG and Nagios, support four or more categories, due to their automated monitoring, alerting, and reporting features. Wireshark and Kismet each cover three functions (60%), excelling in packet-level and wireless-specific monitoring but lacking integrated alerting or reporting. Ettercap has the narrowest scope, supporting only two functions (40%), confirming its role as a specialized security auditing tool rather than an all-in-one monitoring platform.

Discovery and monitoring are the most consistently supported functions, with all tools enabling some form of host detection and traffic monitoring. Conversely, mapping and reporting are less supported, native in only 40% of the tools, and often limited by licensing or hardware needs. Alerting is available in 60% of the tools, reflecting a clear divide between enterprise monitoring systems and analysis tools.

From an implementation standpoint, the results suggest that tool choice should align with operational needs. Wireshark is vital for detailed traffic analysis but should be complemented by alerting systems like Nagios for practical use. PRTG's sensor-based design suits large-scale deployments, though its free version limits sensors. Combining Kismet's wireless detection with Ettercap's penetration testing enhances security monitoring, supported by external reporting tools. Overall, the study reveals a significant gap in the open-source ecosystem: the absence of a fully integrated, license-free solution offering complete discovery, mapping, alerting, and reporting. These findings highlight the need for integrated frameworks and guide future research toward scalable, intelligent WLAN monitoring solutions.

ACKNOWLEDGEMENT

The authors appreciate all those who contributed to this study.

CONFLICT OF INTEREST

No relevant disclosures.

REFERENCES

[1] E. Lafargue, “Wireless Network Audits Using Open Source Tools,” SANS White Papers. [Online]. Available: https://www.sans.org/white-papers/1235. Accessed: Aug. 14, 2025.
[2] H. Andrea, “25 Best Open Source & Free Network Monitoring Software Tools (Guide),” 2020. [Online]. Available: https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/. Accessed: Aug. 14, 2025.
[3] A. Al Shidhani, K. Al Maawali, D. Al Abri, and H. Bourdoucen, “A Comparative Analysis of Open Source Network Monitoring Tools,” International Journal of Open Source Software and Processes, vol. 7, no. 2, pp. 1–19, 2016, doi: 10.4018/IJOSSP.2016040101.
[4] PeerSpot, “Nagios XI vs. Wireshark vs. Zabbix Comparison.” [Online]. Available: https://www.peerspot.com/products/comparisons/nagios-xi_vs_wireshark_vs_zabbix. Accessed: Aug. 14, 2025.
[5] A. Yahia and E. Atwell, “Evaluation of the Capabilities of Wireshark as Network Intrusion System,” Journal of Global Research in Computer Science, vol. 9, no. 8, pp. 1–8, 2018.
[6] J. W. S. Parker, “How Does Kismet Compare to Other Wireless Network Analysis Tools?,” Cyberly. [Online]. Available: https://www.cyberly.org/en/how-does-kismet-compare-to-other-wireless-network-analysis-tools/index.html. Accessed: Aug. 14, 2025.
[7] A. Wakhloo, I. Ghergulescu, and A.-N. Moldovan, “Investigation of WiFi Security Auditing Tools for Evil Twin Attacks and Detection,” in Hybrid Intelligent Systems, A. Bajaj, P. M. Mishra, and A. Abraham, Eds. Cham, Switzerland: Springer Nature Switzerland, 2025, pp. 257–267.
[8] Kali, “The Raspberry Pi’s Wi-Fi Glow-Up,” Kali Linux Blog. [Online]. Available: https://www.kali.org/blog/raspberry-pi-wi-fi-glow-up/. Accessed: Aug. 14, 2025.
[9] L. Lakshmanan, P. Reshma, and R. Sushmitha, “Unveiling the Hidden Threat: Exploring Wi-Fi Vulnerabilities,” AIP Conference Proceedings, vol. 3257, no. 1, Art. no. 020164, 2025, doi: 10.1063/5.0277070.
[10] T. Perković, A. Dagelić, M. Bugarić, and M. Čagalj, “On WPA2-Enterprise Privacy in High Education and Science,” Security and Communication Networks, vol. 2020, no. 1, Art. no. 3731529, 2020.