Journal of Computer Science and Technology
Volume 4 ; Number 3 ; September 2026 ; Page 226-234
DOI : https://doi.org/10.59435/jocstec.v4i3.744
https://jurnal.padangtekno.com/index.php/jocstec
E-ISSN : 2985-4318
P-ISSN : 2985-5772

Traffic Analysis of Data Packets on a WPA2-Personal WLAN Network Using Wireshark

Ari Alviandry[1*], Husnul Hotimah[2], Sarboyni[3], Febri Dristyan[4]

[1,2,3,4]D4 Software Engineering Technology Study Program, Politeknik Jambi
[1*]arialviandry277@gmail.com, [2]husnulnul2020@gmail.com, [3]sarboyniboy@gmail.com, [4]fdristyan@gmail.com

ABSTRACT

The reliability of data packet transmission within the deployed Wireless Local Area Network (WLAN) security protocol is highly crucial to ensure user data confidentiality. This study aims to analyze the security implementation of the WPA2-Personal protocol-based WLAN through direct observation of data packet traffic. A qualitative-descriptive research method was applied by conducting packet capturing using the Wireshark application on a small-scale test network utilizing a smartphone as an access point and a laptop as a client. The results demonstrate that all local and internet data communication activities operated stably and were recorded consistently. Packet analysis successfully identified various major protocols, including ARP, DNS, TCP, UDP, TLS, and HTTPS. The implementation of TLS encryption on HTTPS traffic proved capable of protecting the confidentiality of application data content, preventing it from being read in plaintext even though the packets were successfully captured. This study concludes that the combination of WPA2-Personal authentication and the HTTPS communication protocol still provides adequate security protection and remains highly viable for small-scale wireless network environments.

Keywords: network security, WLAN, WPA2-Personal, Wireshark, packet capturing.

INTRODUCTION

Wireless Local Area Network (WLAN) has become the primary infrastructure in modern data communication due to its ease of installation, mobility, and cost efficiency compared to wired networks. However, because its transmission medium is open radio waves, WLAN is far more vulnerable to eavesdropping, access-point spoofing, and various forms of cyberattacks than conventional wired networks. Therefore, security protocols are a crucial component in ensuring the confidentiality, integrity, and availability of data transmitted over WLAN.

Wi-Fi Protected Access 2 (WPA2) is a security protocol that has been widely used since it was ratified in 2004 and relies on a 4-way handshake authentication scheme along with CCMP-AES encryption. Nevertheless, research conducted by Vanhoef and Piessens demonstrated that WPA2 has a serious vulnerability known as the Key Reinstallation Attack (KRACK), which allows an attacker to force nonce reuse during the handshake so that encrypted traffic can be decrypted without knowing the network password [1]. In addition, WPA2 is also vulnerable to offline dictionary attacks through the capture of PMKID packets or handshake packets [2], [3], [4].

To address these various weaknesses, the Wi-Fi Alliance introduced WPA3 in 2018, bringing a new authentication scheme called Simultaneous Authentication of Equals (SAE) that replaces the Pre-Shared Key used in WPA2, and requiring the use of Protected Management Frames (PMF) to protect management frames from deauthentication attacks [5]. However, research by Vanhoef and Ronen through the Dragonblood project showed that the implementation of the Dragonfly handshake in WPA3 still has gaps in the form of information leakage through side-channel timing and cache attacks, as well as the potential for downgrade attacks to the WPA2 transition mode [6]. A systematic literature review by Halbouni et al. further confirmed that a number of attacks, such as denial-of-service and downgrade attacks, can still penetrate WPA3-based networks [6].

Several prior studies have examined the topic of WLAN security from various perspectives. Reddy and Srikanth conducted a comprehensive review of the vulnerabilities of WEP, WPA, WPA2, and WPA3, along with their testing tools [6]. Okario and Suputra applied a penetration testing method to uncover security gaps in WPA- and WPA2-based networks [3], which was further reinforced by Saputra et al. in analyzing wireless security using the Penetration Testing Execution Standard (PTES) [7]. Idifitriani compared the performance and security of the WPA2 and WPA3 protocols using a mixed-methods approach in a campus case study [4]. Haeruddin and Kurniadi tested the security of WPA2-PSK on home router devices through simulated brute-force attacks [8], while Fitrian et al. also conducted an in-depth comparative evaluation of the resilience of WPA2 and WPA3 against deauthentication and brute-force attacks [9]. Mulyanto et al. also analyzed WLAN security against brute-force attacks in a healthcare institution case study [4]. Although these studies have extensively examined wireless security, a gap remains in the form of a lack of in-depth research focusing on the direct analysis and visualization of data packet traffic characteristics to evaluate the effectiveness of WPA2-Personal encryption in small-scale networks.

Based on this gap, this study aims to analyze the security implementation of a WPA2-Personal protocol-based WLAN through direct observation of data packet traffic using the Wireshark application.

Technically, WLAN security is governed by the IEEE 802.11i standard, which defines the Robust Security Network (RSN) authentication and encryption mechanisms that form the basis for WPA2 and were later refined in WPA3. Beyond the vulnerabilities in the handshake and authentication scheme, protection against attacks at the network management layer has also received attention, as shown by Schepers, Ranganathan, and Vanhoef, who evaluated the resilience of various countermeasure mechanisms against deauthentication attacks on modern Wi-Fi networks [10]. Adbeib further asserted that the complexity of WLAN security configuration is often, in practice, a major factor contributing to vulnerabilities, regardless of the strength of the protocol used [11]. Meanwhile, Moly, Mau, and Ledi emphasized in their research that comprehensive security evaluation through *penetration testing* methods is essential for identifying security gaps, such as vulnerability to attacks involving *sniffing* on unencrypted data transmission [12].

RESEARCH METHOD

Research Approach

This study uses a **qualitative-descriptive** method with an implementation and observation approach to the security of the *Wireless Local Area Network* (WLAN) network using the **WPA2-Personal** protocol. This approach aims to analyze the implementation of wireless network security through observation of the data communication process occurring on the WLAN network using the Wireshark application.

In addition to direct implementation on the test network, this study is also supported by a literature review sourced from national and international journals, books, and the IEEE 802.11i standard. The literature review is used as a basis for comparing the implementation results obtained with theories on WPA2 security mechanisms and the development of the WPA3 protocol.

Research Stages

The stages of this study consist of five main steps, as follows.

a. **Literature Review.** The initial stage was conducted by collecting various references discussing WLAN network security, particularly the WPA2 and WPA3 protocols. References were obtained from scientific journals, books, the IEEE 802.11i standard, and official publications related to wireless network security.

b. **Network Topology Design.** This study uses a simple WLAN topology consisting of an Android smartphone as an access point (hotspot) configured with WPA2-Personal security and a Windows 10 laptop as the client device as well as the network analysis device using Wireshark.

c. **Network Implementation.** At this stage, the Android smartphone was configured as a hotspot with WPA2-Personal security using the AES encryption algorithm. The Windows 10 laptop was then

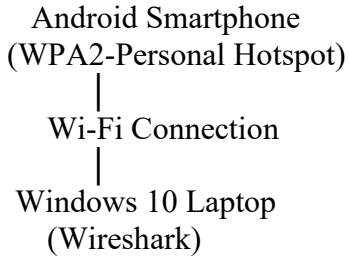
connected to the hotspot network so that the authentication process proceeded normally and data communication could take place.

d. **Data Collection.** Data collection was carried out using the Wireshark application running on the Windows 10 laptop. During the testing process, several network activities were carried out, such as accessing websites, performing ping tests, and using internet services to generate data traffic that could be recorded.

e. **Data Analysis.** The recorded network packet data was analyzed to identify the types of protocols used, network communication patterns, the packet exchange process, and the security mechanisms applied to the WPA2-Personal-based WLAN network. The analysis results were then compared with theory and prior research.

Test Network Topology

The network topology used in this study consists of one Android smartphone functioning as an access point (hotspot) with WPA2-Personal security and one Windows 10 laptop as the client device as well as the analysis device using Wireshark.



In this topology, the smartphone provides the WLAN network service using the WPA2-Personal authentication mechanism, while the Windows 10 laptop is used to access the network as well as to observe the data traffic passing through it.

Tools and Materials

The equipment used in this study consists of the following hardware and software.

Hardware:

a. Android smartphone as an access point (hotspot).
b. Laptop running the Windows 10 operating system.
c. Laptop's built-in Wi-Fi adapter.

Software:

a. Wireshark as the application for capturing and analyzing network packets.
b. Microsoft Word as the medium for preparing the research report.
c. Google Chrome as the application for generating network activity during the testing process.

Testing Implementation

The research implementation was carried out through the following steps.

a. Activating the hotspot on the Android smartphone using WPA2-Personal security with the AES encryption algorithm.
b. Connecting the Windows 10 laptop to the hotspot network until it automatically obtains an IP address.
c. Running the Wireshark application and selecting the Wi-Fi network interface currently in use.
d. Starting the packet capture process using Wireshark.
e. Carrying out network activities such as opening several web pages, running the **ping** command, and accessing internet services to generate data traffic.
f. Stopping the recording process after the required data has been obtained.
g. Analyzing the successfully recorded packets, including the identification of ARP, DNS, TCP, UDP, TLS, and HTTP/HTTPS protocols.
h. Documenting all test results in the form of screenshots and capture result files (*.pcapng*) as research data.

Testing was carried out three times under the same network conditions to obtain consistent results.

Test Parameters

The parameters observed in this study are presented in Table 1

Table 1. Test Parameters

No	Parameter	Observation Indicator
1	WLAN connection status	Successful or failed
2	Device IP address	IP obtained from the hotspot
3	Number of packets recorded	Number of packets captured
4	Protocol type	ARP, DNS, TCP, UDP, TLS, HTTP/HTTPS
5	Capture duration	Packet recording duration
6	Network activity	Browsing, ping, and data communication

Data Analysis Technique

The data analysis technique was carried out descriptively by observing the results of network packet recording using Wireshark. The analysis focused on identifying the types of protocols used, communication patterns between devices, and the data exchange mechanisms occurring on the WLAN network with WPA2-Personal security.

The observation results were then compared with WLAN security theory and prior research on WPA2 implementation. This analysis aims to provide an overview of the application of WPA2-Personal security in a small-scale network environment and to evaluate its effectiveness based on the characteristics of the observed network traffic.

RESULTS AND DISCUSSION

This section presents the results of implementing a *Wireless Local Area Network* (WLAN) network using the WPA2-Personal security protocol, along with an analysis of the network traffic obtained through the Wireshark application on the Windows 10 operating system. Testing was carried out on a simple network using an Android smartphone as an access point (hotspot) and a Windows 10 laptop as the client device. The observation data was then analyzed and compared with theory and prior research on WLAN network security.

WPA2-Personal Network Implementation Results

The initial stage of the study was carried out by configuring the Android smartphone as an access point using WPA2-Personal security with the AES encryption algorithm. After the configuration was complete, the Windows 10 laptop successfully connected to the hotspot network and automatically obtained an IP address through the DHCP service provided by the smartphone.

While the device was connected to the network, the Wireshark application was run to record the data traffic passing through the wireless network interface. The recording process was carried out while the user performed several network activities, such as accessing websites and testing connectivity using the *ping* command, as well as accessing other internet services.

The implementation results show that the WLAN connection ran well without any disruptions during the testing process. All network activity was successfully recorded by Wireshark so that it could be used as material for analyzing data communication on the WPA2-Personal network.

Figure 1. WPA2-Personal hotspot configuration on the Android smartphone.

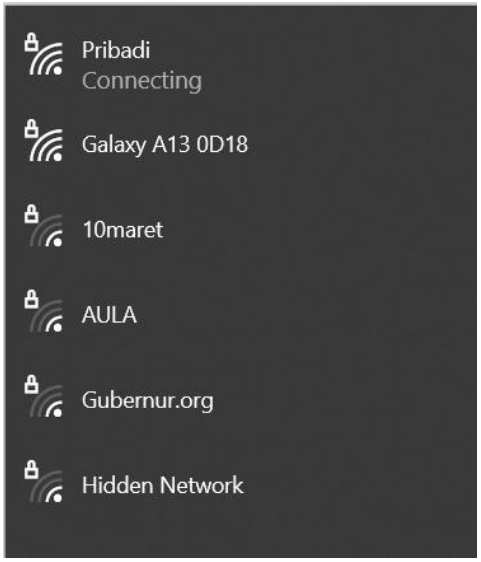


Figure 2. Windows 10 laptop successfully connected to the hotspot network.

Packet Capture Results Using Wireshark

The *capture* process was carried out using Wireshark on the Wi-Fi network interface connected to the hotspot. During testing, Wireshark successfully recorded various communication packets used in the data exchange process between the client device and the network.

Based on the observation results, several network protocols that were successfully identified include:

- Address Resolution Protocol (ARP)
- Domain Name System (DNS)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Transport Layer Security (TLS)
- Hypertext Transfer Protocol Secure (HTTPS)

The presence of ARP packets indicates the process of resolving device addresses on the local network before communication takes place. DNS packets are used to translate domain names into IP addresses when the user accesses a website. Data communication then proceeds using the TCP protocol, while the security of internet communication is observed through the use of TLS in HTTPS connections.

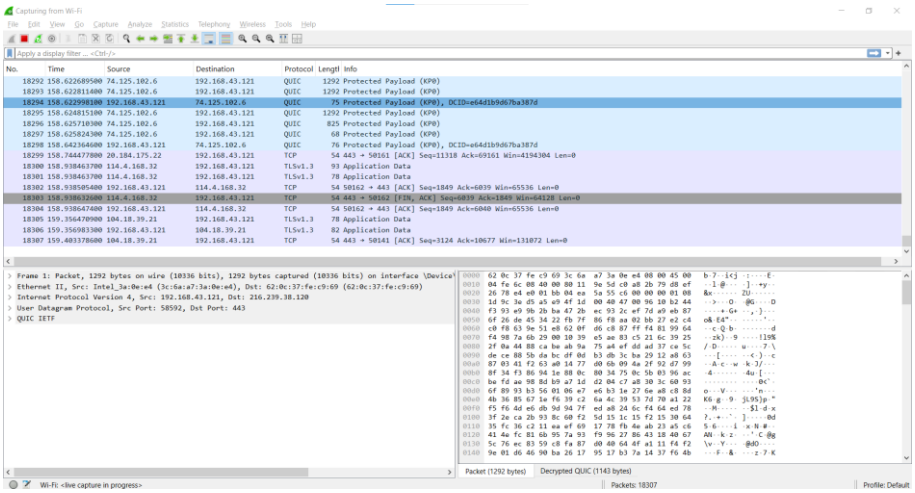


Figure 3. Wireshark packet capture results.

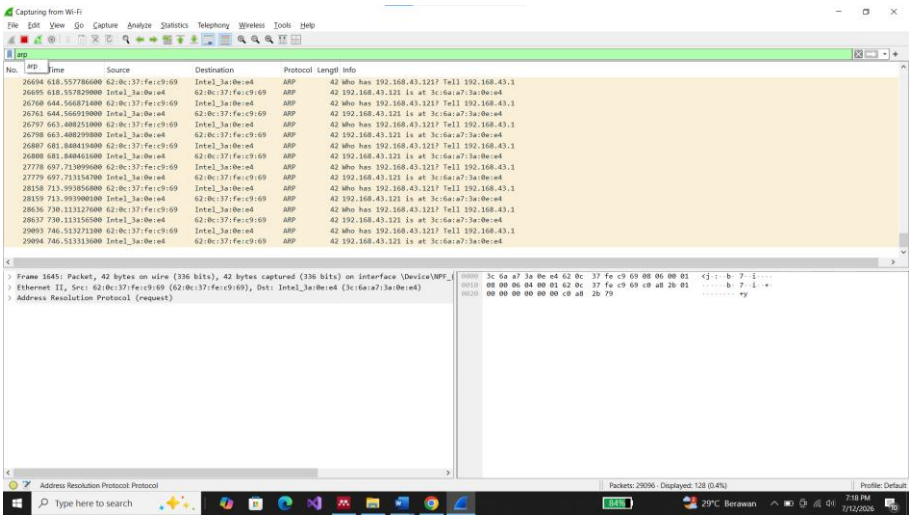


Figure 4. ARP Packet Detection.

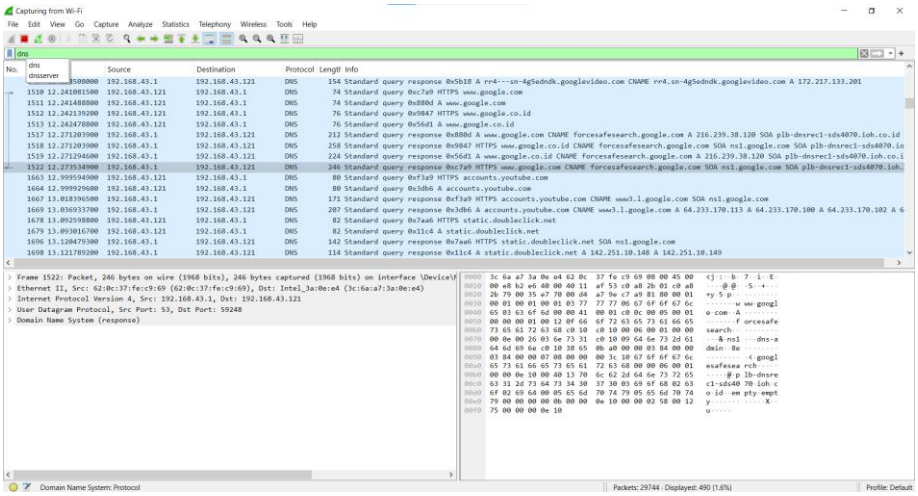


Figure 5. DNS Packet Detection.

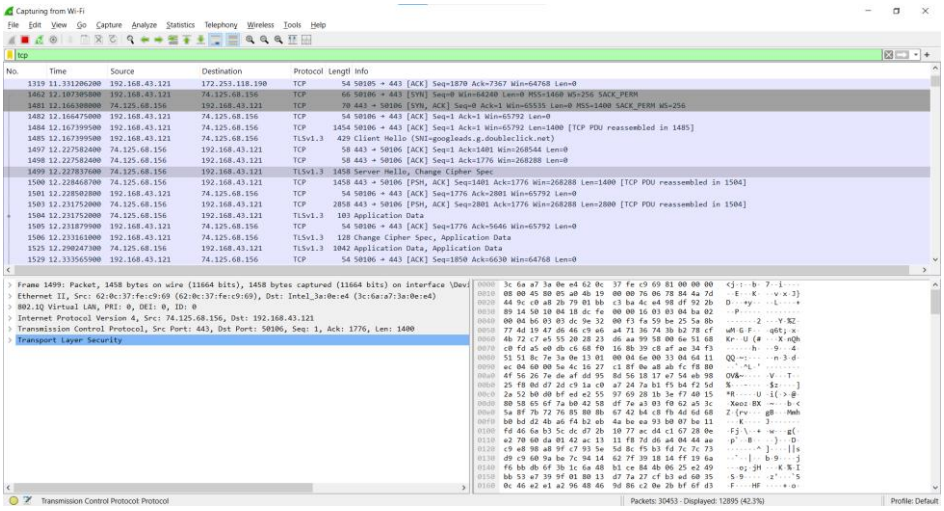


Figure 6. TCP Packet Detection.

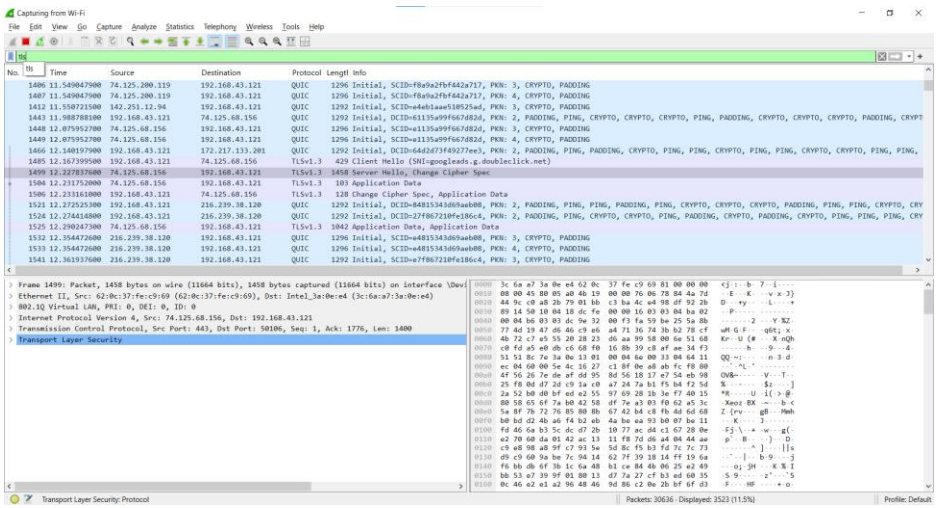


Figure 7. TLS Packet Detection.

Network Traffic Analysis

Analysis of the *capture* results shows that the communication process on the WPA2-Personal network proceeded normally. No disruptions were found in the authentication process or in inter-device communication during testing.

The recorded packets show that most internet communication uses the HTTPS protocol running on top of TLS. This indicates that the application data has obtained additional protection through the encryption process, so that the content of the communication cannot be read directly even though the packets were successfully recorded using Wireshark.

In addition, Wireshark only displays information such as the *source address* and *destination address*, along with the protocol type, packet size, and packet transmission time. The content of encrypted application data cannot be displayed as *plaintext*, so that the confidentiality of user information remains protected.

These findings indicate that the combination of WPA2-Personal authentication and the use of the HTTPS protocol provides fairly good protection for data communication on a small-scale WLAN network.

Discussion

The implementation results show that the WPA2-Personal protocol can still provide an adequate level of security for small-scale WLAN networks when configured with the AES encryption algorithm and a strong password. During testing, communication between the smartphone as the

access point and the laptop as the client device proceeded stably and was successfully recorded using Wireshark for analysis purposes.

Based on the observation results, Wireshark was able to capture network traffic passing through the Wi-Fi interface, but could not display the content of communications using the HTTPS protocol in plain text because it was protected by the TLS encryption mechanism. This condition shows that although packets can be observed, the confidentiality of user data remains protected during the transmission process.

These findings are consistent with previous research explaining that WPA2 uses an authentication mechanism based on *Pre-Shared Key* (PSK) and AES-CCMP encryption to maintain the confidentiality of communication on WLAN networks. However, various studies also show that WPA2 still has several weaknesses, such as vulnerability to **Key Reinstallation Attack (KRACK)** and **dictionary attack** if an attacker succeeds in obtaining the authentication process (*4-Way Handshake*) and the user uses a weak password. This vulnerability was not directly observed in this study because the research focused on the implementation and analysis of network traffic using Wireshark.

Compared to WPA2, the WPA3 protocol offers improved security through the **Simultaneous Authentication of Equals (SAE)** mechanism, which replaces the *Pre-Shared Key*-based authentication. In addition, WPA3 requires the use of **Protected Management Frames (PMF)**, making it more resistant to *deauthentication* and *dictionary attack* attacks conducted *offline*. Therefore, although this study's implementation uses WPA2-Personal, the literature review results indicate that migration to WPA3 remains recommended for improving WLAN network security in the future.

Table 2. Summary of WPA2-Personal Network Implementation Results

Test Parameter	Result
WPA2-Personal hotspot configuration	Successful
Laptop connected to the network	Successful
IP address obtained automatically	Successful
Capture process using Wireshark	Successful
ARP packets detected	Yes
DNS packets detected	Yes
TCP/UDP packets detected	Yes
TLS/HTTPS packets detected	Yes
HTTPS communication content readable	No
Connection stability during testing	Stable

Based on the implementation results, it can be concluded that the WLAN network based on WPA2-Personal was successfully implemented and observed using Wireshark. The network communication process proceeded well, while the encryption mechanism in the HTTPS protocol continued to protect the confidentiality of the transmitted information. Although this study did not conduct direct penetration testing, the observation results show that WPA2-Personal implementation remains viable for small-scale networks when combined with the use of strong passwords, regular software updates, and the application of secure communication protocols.

CONCLUSION

Based on the implementation and analysis carried out, it can be concluded that a *Wireless Local Area Network* (WLAN) network using the WPA2-Personal security protocol was successfully implemented using an Android smartphone as an access point (hotspot) and a Windows 10 laptop as the client device. The data communication process on the network could be observed using the Wireshark application, so that various network packets such as ARP, DNS, TCP, UDP, TLS, and HTTPS were successfully recorded and analyzed. The observation results show that network

communication proceeded normally and stably throughout the testing process. Although Wireshark was able to capture network traffic, the content of communications using the HTTPS protocol could not be read in *plaintext* form because it was protected by the TLS encryption mechanism. This shows that the combined use of WPA2-Personal and a secure communication protocol provides protection for the confidentiality of data during the transmission process.

Based on the literature review conducted, WPA2-Personal remains a viable security protocol for small-scale WLAN networks when configured with the AES algorithm, a strong password, and supported by regular software updates. However, various prior studies show that WPA2 still has several limitations, such as vulnerability to **Key Reinstallation Attack** (KRACK) and *dictionary attack* if an attacker succeeds in obtaining the authentication process and the user applies a weak password. Therefore, the application of good security practices remains necessary to minimize this risk. As a recommendation for future research, testing can be developed by directly comparing WPA2 and WPA3 implementations, using network security software such as Aircrack-ng to analyze the resilience of the *4-Way Handshake*, expanding the testing scope with multiple client devices and dedicated access points, and examining the effectiveness of additional security mechanisms such as VPN, PMF, and intrusion detection systems (IDS) to improve communication security on wireless networks.

REFERENCES

[1] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks," pp. 1313–1328, 2017, doi: 10.1145/3133956.3134027.

[2] B. Indira Reddy and V. Srikanth, "Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 5, no. 4, pp. 28–35, 2019, doi: 10.32628/cseit1953127.

[3] A. Okario, I. P. Gede, and H. Suputra, "Analisis Celah Keamanan Jaringan WPA dan WPA2 Dengan Menggunakan Metode Penetration Testing," vol. 1, pp. 1125–1130, 2023.

[4] Yudi Mulyanto, Shindyka Syalu Qanita, Dimas Wiryatari, and Farida Idifitriani, "Analisis Perbandingan Kinerja Dan Keamanan Protokol Wpa2 Dan Wpa3 Dengan Metode Penetration Testing," *J. Inform. dan Rekayasa Elektron.*, vol. 8, no. 1, pp. 140–148, 2025, doi: 10.36595/jire.v8i1.1539.

[5] A. Halbouni, L. Y. Ong, and M. C. Leow, "Wireless Security Protocols WPA3: A Systematic Literature Review," *IEEE Access*, vol. 11, no. October, pp. 112438–112450, 2023, doi: 10.1109/ACCESS.2023.3322931.

[6] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2020-May, pp. 517–533, 2020, doi: 10.1109/SP40000.2020.00031.

[7] Satria Galang Saputra, B. Parga Zen, and Abdurahman, "Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES)," *J. Sist. Inf. Galuh*, vol. 1, no. 2, pp. 43–51, 2023, doi: 10.25157/jsig.v1i2.3152.

[8] A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6)," vol. 1, no. 1, pp. 508–515, 2021.

[9] H. P. Fitrian, E. Eriyana, H. M. Ibrahim, R. P. Rizqullah, and S. P. Meliansyah, "Security Evaluation of WPA2 vs WPA3 Wireless Network Against Deauthentication and Brute Force Attacks using," vol. 5, no. 1, pp. 257–274, 2026.

[10] D. Schepers, *On the Robustness of Wi-Fi Deauthentication Countermeasures*, vol. 1, no. 1. Association for Computing Machinery, 2022. doi: 10.1145/3507657.3528548.

[11] W. A. P. Wep, "African Journal of Advanced Pure and Applied Sciences (AJAPAS) Comprehensive Study on Wi-Fi Security Protocols by Analyzing," vol. 2, no. 4, pp. 385–402, 2023.

[12] N. Januari, A. H. Moly, S. D. I. Mau, and D. F. Ledi, "Analisis Keamanan Jaringan Komputer Menggunakan Metode Penetration Testing dikelola oleh Universitas Andalas untuk mengumpulkan , mengelola , mendokumentasikan , dan Permasalahan utama pada situs Repository Universitas Andalas adalah masih digunakannya protokol HTTP dalam proses transmisi data , sehingga informasi yang kerentanan berbeda , sedangkan hingga saat ini belum ditemukan penelitian yang secara khusus," no. November 2025, 2026.