

**Design and Develop The Deauthentication Attack Detection System on Wi-Fi
Networks Based on Python and TCPDUMP**

Lanny Catrin Dale

Politeknik Jakarta Internasional, Indonesia

Email: lanny.dale@jihs.ac.id

ARTICLE INFO

Published: July, 31st
2025

Key words: Design,
Python, TCPDUMP

ABSTRACT

The purpose of this research is to find out how to design and create a Deauthentication attack detection system using tcpdump and python programming language as the main detection programme for Politeknik Jakarta International. The author uses an experimental research approach with a scientific method used to systematically test the effect of a variable on other variables. This research produces a proof that the material used in this research is a trial both in the form of literature study, as well as the results of direct observation and testing conducted by the author. The deauthentication attack detection system is able to detect deauthentication attacks effectively at Politeknik Jakarta International.

INTRODUCTION

The design and development process is a detailed explanation of the work that will be carried out using various methods and techniques, with procedures and details for each step in the implementation process (Stephen, 2020). Network design can be considered as a process of engineering network traffic to create various network segments or IP addresses (Wibowo, 2020). The development process involves writing code using a programming language to create a system (Pressman, 2010).

One of the services that is highly needed today is computer networking. Computer networks provide more benefits compared to individual computers. By using computer networks, users can share data, software, and equipment collectively, enabling people to work in groups effectively and efficiently (Faulkner, 2001). Currently, network security has become a very important issue and will continue to evolve. Several cases related to system security now require significant handling costs. Defense systems, banking systems, and similar systems require very high security because they are part of critical systems (Wajong, 2012).

Wi-Fi networks can be available through hardware such as Access Points. An Access Point functions as a signal distributor for internet access to devices connected to it (Sugiyono, 2016). Denial of Service (DoS) is an attack effort to disable a targeted computer network system. When a computer network system is attacked by DoS, the system becomes

incapacitated, and no services are available on that computer (S. Nurweda, 2004). Deauthentication Attack is a method of network communication attack that can be categorized as a type of DoS attack, with impacts that can cause communication paralysis on a signal transmitting device, leading to disconnection of internet connection on a device currently connected. Deauthentication Attack is one type of DoS attack that results in the disruption of Wi-Fi services on the Access Point (Widiyanto, S,dkk, 2023) .

TCPdump is an open-source tool capable of providing an effective solution for detecting deauthentication attacks. In network security, deauthentication packets can be sent from the internal side of the access point/router (authenticated deauthentication packets or genuine deauthentication packets). Deauthentication packets can also be sent from external parties (unauthenticated deauthentication packets or fake deauthentication packets). If a deauthentication packet is sent from the internal side to a client connected to the access point/router, TCPdump cannot detect the deauthentication packet. TCPdump is only capable of detecting deauthentication packets sent by unauthenticated parties, thus enabling it to distinguish genuine deauthentication packets from fake ones.

METHOD

Research Design

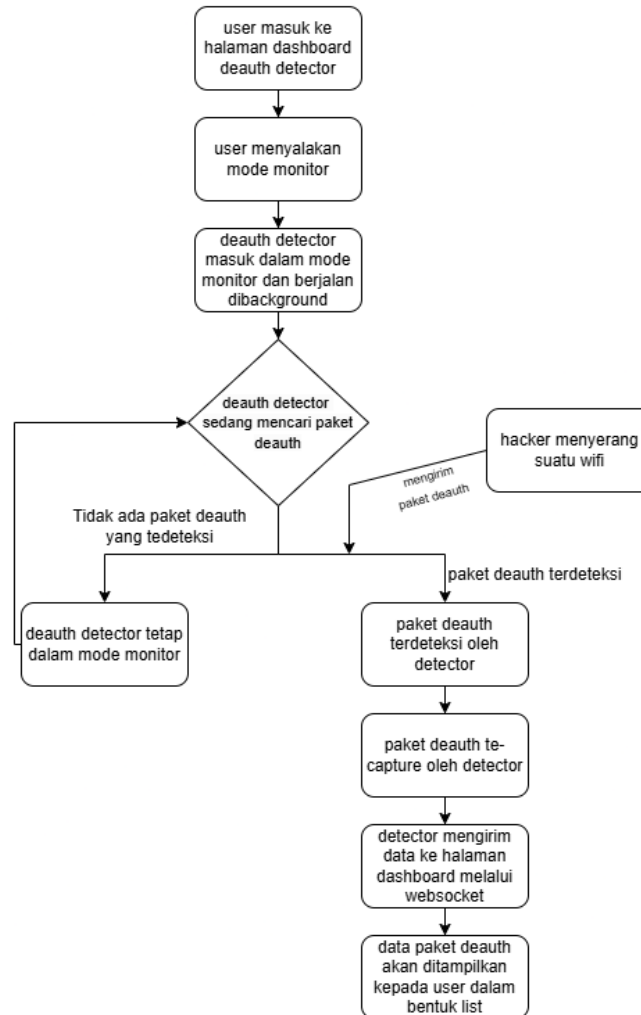
The research method used by the author is an experimental development method. This method was chosen with the aim of accurately testing the effectiveness of a new product that will be created and developed. The main objective of the deauthentication attack detection system development experiment is to demonstrate the system's ability to detect deauthentication packets compared to existing products. The materials used in this research consist of experimental trial tests, including literature studies, observation results, and direct testing conducted by the author. Figure 1 below illustrates the experiment of the detection system in the Laboratory Room at the Jakarta International Polytechnic Campus.



The tools and materials used in the development of the deauthentication packet detection system are listed in Table 1 below:

Hardware	Software
Laptop Redmibook 15	Visual Studio Code
Processor Intel i3-1115g4	Oracle VM Virtualbox
RAM 8Gb	Ubuntu Linux yang berjalan di dalam Oracle VM VirtualBox
GPU intel HD	Kali linux yang berjalan di dalam Oracle VM VirtualBox
Display 1920 x 1080, 60 Hz	Python 3.12
TP-Link WN72N Wifi Card (2 buah)	TCPdump

The research flowchart is a systematic process conducted to support the research process so that the study can proceed in accordance with the sequence of activities. Here is a research diagram that the author used, as shown in Figure 2 below:



RESULT AND DISCUSSION

The following are the results of the deauthentication attack detection system design along with an explanation of its operating principle:

1. Website address of the deauthentication attack detection system

The website address of the detection system is in the form of an IP (Internet Protocol) address and does not use the HTTPS transport protocol.

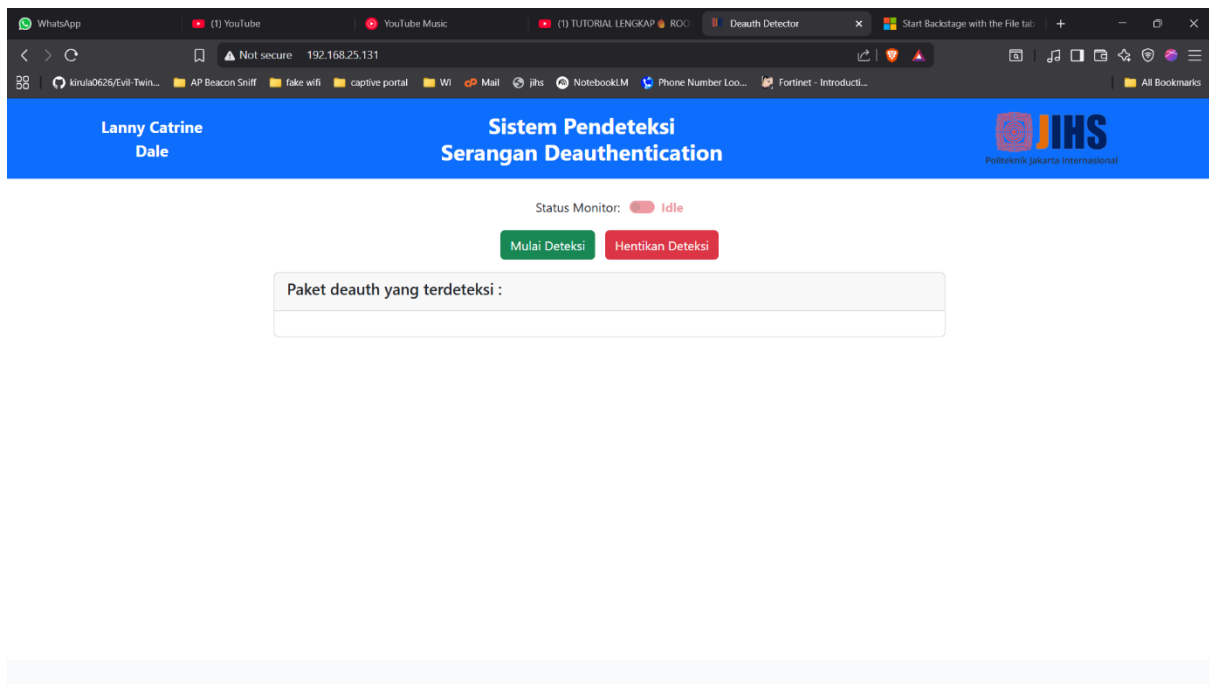
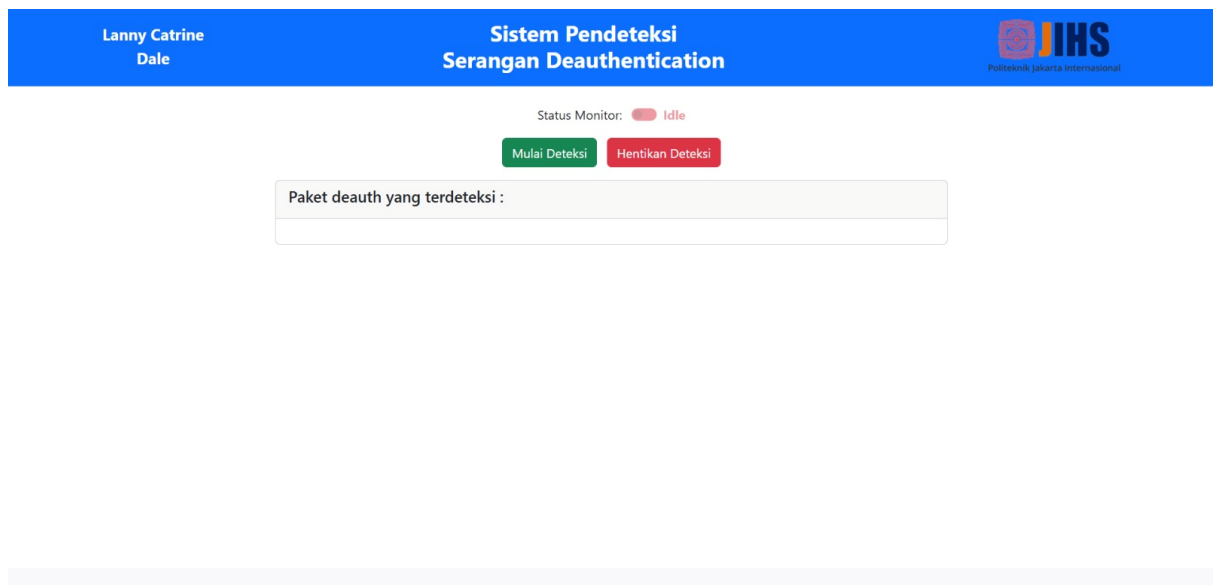


Figure 3. Website address of the deauthentication attack detection system

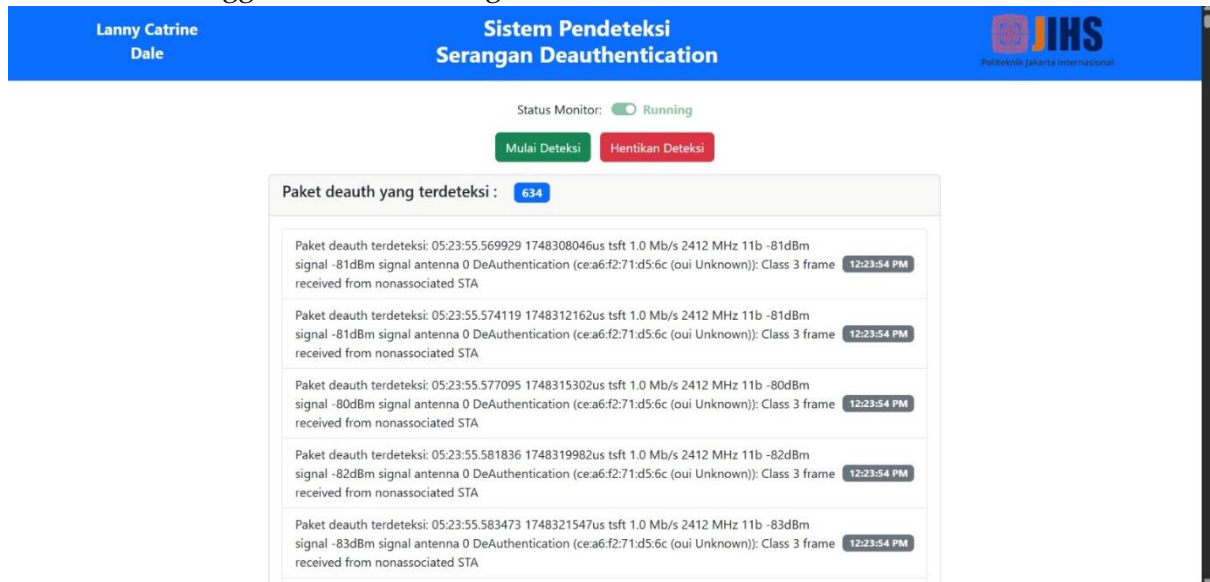
2. Main page when the system is not monitoring

The following is the main page of the deauthentication attack detection system. The "Status Monitor" toggle indicates whether the system is in monitoring mode or not. When toggled off, it will be red in color and there is a "Stop" label on the right side of the toggle.



3. Main page when the system is monitoring

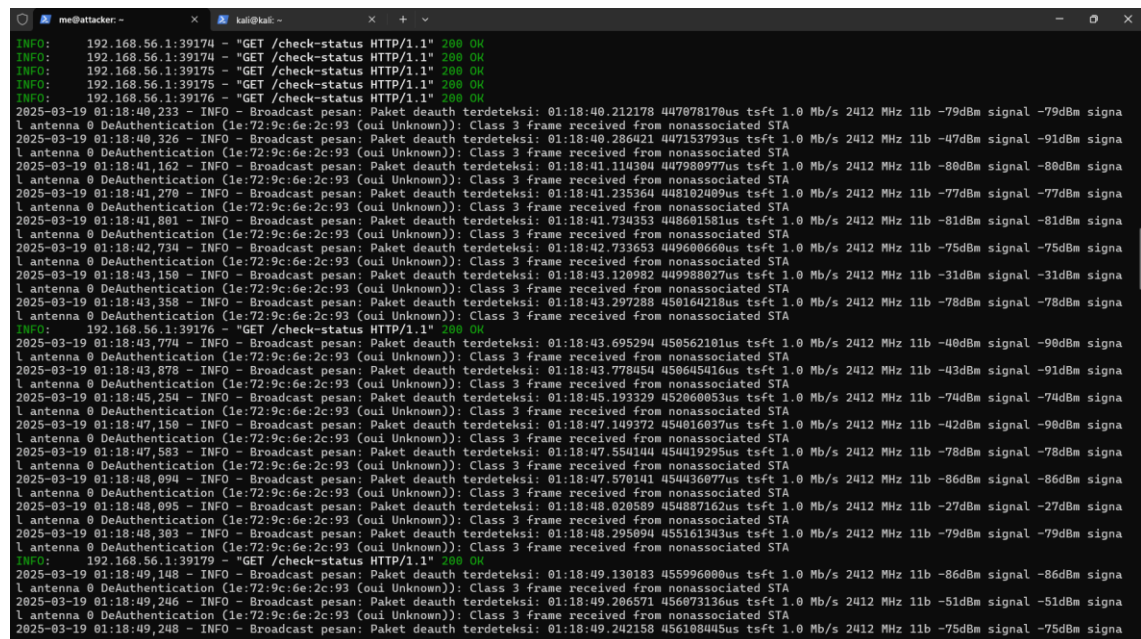
The toggle will be green in color and there will be a "



Monitoring" label on the right side of the toggle.

4. Results of deauthentication packet detection on the server

The detection system is capable of capturing fake deauthentication packets sent by attackers in a very short time. The captured deauthentication packets will be immediately displayed in the "Detected Deauth Attacks" table on the main page. The information displayed includes the time the deauthentication packet was detected, the packet type, and the MAC address of the sender of the deauthentication packet. Figure 4.4 shows an example of a detected and captured deauthentication packet by the TP-link WN722N Wi-Fi card device (Mubasyira, M,et al, 2025). Figure 4.4 is taken from the server side.



The deauthentication packets captured by the TP-Link WN722N Wi-Fi card will be processed by the server and displayed to the user on a website page in the same text format as on the


server. The captured deauthentication packets will be shown to the user in text form and as a list.

5. Results of deauthentication packet detection on the deauthentication attack detection system website.

The detection results carried out by the deauthentication attack detection system are able to capture deauthentication packets in a very short time, with intervals between captured packets in the microsecond range. The captured deauthentication packets have several properties. To explain these properties, the author uses a sample from the topmost deauthentication packet, which is: "Deauth packet detected: 08:10:24.351830 217374897us tsft 1.0 Mb/s 2412 MHz 11b -56dBm signal -56dBm signal antenna 0 DeAuthentication (46:a2:15:0c:46:c8 (oui Unknown)): Class 3 frame received from nonassociated STA":

Lanny Catrine
Dale

Sistem Pendeteksi
Serangan Deauthentication


Politeknik Jakarta Internasional

Status Monitor: Running

Mulai Deteksi

Hentikan Deteksi

Paket deauth yang terdeteksi: 634

Paket deauth terdeteksi: 05:23:55.569929 1748308046us tsft 1.0 Mb/s 2412 MHz 11b -81dBm
signal -81dBm signal antenna 0 DeAuthentication (ce:a6:f2:71:d5:6c (oui Unknown)): Class 3 frame
received from nonassociated STA 12:23:54 PM

Paket deauth terdeteksi: 05:23:55.574119 1748312162us tsft 1.0 Mb/s 2412 MHz 11b -81dBm
signal -81dBm signal antenna 0 DeAuthentication (ce:a6:f2:71:d5:6c (oui Unknown)): Class 3 frame
received from nonassociated STA 12:23:54 PM

Paket deauth terdeteksi: 05:23:55.577095 1748315302us tsft 1.0 Mb/s 2412 MHz 11b -80dBm
signal -80dBm signal antenna 0 DeAuthentication (ce:a6:f2:71:d5:6c (oui Unknown)): Class 3 frame
received from nonassociated STA 12:23:54 PM

Paket deauth terdeteksi: 05:23:55.581836 1748319982us tsft 1.0 Mb/s 2412 MHz 11b -82dBm
signal -82dBm signal antenna 0 DeAuthentication (ce:a6:f2:71:d5:6c (oui Unknown)): Class 3 frame
received from nonassociated STA 12:23:54 PM

Paket deauth terdeteksi: 05:23:55.583473 1748321547us tsft 1.0 Mb/s 2412 MHz 11b -83dBm
signal -83dBm signal antenna 0 DeAuthentication (ce:a6:f2:71:d5:6c (oui Unknown)): Class 3 frame
received from nonassociated STA 12:23:54 PM

The detection results carried out by the deauthentication attack detection system are able to capture deauthentication packets in a very short time, with intervals between captured packets in the microsecond range. The captured deauthentication packets have several properties. To explain these properties, the author uses a sample from the topmost deauthentication packet, which is: "Deauth packet detected: 08:10:24.351830 217374897us tsft 1.0 Mb/s 2412 MHz 11b -56dBm signal -56dBm signal antenna 0 DeAuthentication (46:a2:15:0c:46:c8 (oui Unknown)): Class 3 frame received from nonassociated STA".

1. "Deauth packet detected": The system has successfully captured a deauthentication packet around the TP-link WN722N Wi-Fi hardware device.
2. "08:10:24.351830": This is the time the deauthentication packet was detected. The time format used is hours:minutes:seconds.microseconds, and the time zone is "UTC now".
3. "217374897us tsft": The timestamp in microseconds from the receiving device.
4. "1.0Mb/s": The data transmission speed of the packet, which is 1 Megabit per second.
5. "2412 MHz": The frequency channel used, which is 2.4 GHz.
6. "11b": The IEEE 802.11b standard used for transmission.
7. "-56dBm signal": The received signal strength, measured in dBm (decibel-milliwatts).
8. "-56dBm signal antenna 0": The signal strength received by antenna 0.
9. "deAuthentication": The type of detected packet, which is a deauthentication packet.
10. "46:a2:15:0c:46:c8 (oui Unknown)": The MAC (Media Access Control) address of the device that sent the deauthentication packet. "OUI Unknown" means that the Organization Unique Identifier of the MAC address is not recognized.
11. "Class 3 frame received from nonassociated STA": An error message indicating that a Class 3 frame (which should only be sent by authenticated and associated devices) was received from a STA (station/device) that is not associated with the access point.

Conclusion

The deauthentication attack detection system is capable of capturing and detecting deauthentication packets sent by attackers. The system can effectively detect and capture deauthentication packets within millisecond intervals between packets. Based on the experiment, the conclusions of the deauthentication attack detection system are: the system can detect and capture fake deauthentication packets sent by attackers. Second, the system operates on a Linux-based operating system using the TCPdump program, making it an affordable and free solution for detecting deauthentication attacks. Third, the system can detect deauthentication attack packets within millisecond time intervals, enabling it to accurately and precisely count the number of deauthentication packets sent. Fourth, the system can notify users that a deauthentication attack has occurred, allowing users to take preventive measures against further attacks such as Rogue AP and Evil Twin AP.

REFERENCE

Mubasyira, M. T., Widiyanto, S., Rizkiyah, N., Setyastanto, A. M., Leksono, A. W., Suprpto, H. A., ... & Suyana, N. (2025). The Need Analysis for WriteMI Application as Digital Basic Writing Teaching Materials Based on Multiple Intelligences Approach. *International Journal on Advanced Science, Engineering & Information Technology*, 15(3).

- Pressman, & Lourenzo, D. (2021). *Analisis Absensi Digital Berbasis Aplikasi Website*
Manado : Universitas Negeri Manado.
- Stephen, W. (2017). *Cryptography and Internet Security: Experiment and Practice*
(7th ed.). Colorado US.
- S. Nurwenda, B. Irawan, And Irzaman, “Analisis Kelakuan Denial-Of-Service Attack
(Dos Attack) Pada Jaringan Komputer Dengan Pendekatan Pada Level
sekuritas,” 2004.
- Sugiyono, “Sistem Keamanan Jaringan Komputer Menggunakan Metode
Watchguard Firebox Pada Pt Guna Karya Indonesia,” *Jurnal Cki On Spot*,
Vol. 9, No. 1, 2016.
- Wajong, A. M. R. (2012). Kerentanan yang Dapat Terjadi di Jaringan Komputer pada
Umumnya. *ComTech: Computer, Mathematics and Engineering Applications*, 3(1),
474-481. <https://doi.org/10.21512/comtech.v3i1.2446>
- Wibowo, Dega & Wiro Sasmito, Ginanjar. (2020). *Rancang Bangun Keamanan Jaringan
Wireless Yang Terintegrasi Dengan Usermanager Menggunakan Mikrotik (Studi
Kasus: DIV Teknik Informatika Politeknik Harapan Bersama)*. *JURNAL PILAR
TEKNOLOGI Jurnal Ilmiah Ilmu Ilmu Teknik*. 5. 10.33319/piltek.v5i2.54.
- Widiyanto, S., Sunendar, D., Vernia, D. M., Alifah, S., Suprpto, H. A., & Leksono, A.
W. (2023). Learning Dayak Literature through Information Systems.
International Journal on Advanced Science, Engineering & Information Technology,
13(6).