# KEAMANAN JARINGAN KOMPUTER NIRKABEL DENGAN ANALISA WEB BROWSING

Franky Leonard
CIMB Niaga, Jakarta
Jl. Taman Kedoya Raya, Jakarta 11520
Email*: franky.napitupulu@cimbniaga.co.id

***Abstract***

*The performance of the Wi-Fi network in the office workspace can be seen from the signal received by the access point (AP) user. This study was conducted to analyze the Wi-Fi security system and optimize it by taking a case in one of the CIMB NIAGA Bank Office Rooms on the GN 1 Floor 2nd Floor by analyzing data packets using the Wireshark application and checking the performance of the access point using the Wifi Analyzer. The purpose of this attack is to make the computer that accesses it cannot run normally so that this wireshark can help detect attacks that will occur so that internet network users are not worried about these attacks by analyzing what parameters are used to carry out attacks. Users are also expected to know the website security system in the form of certification and its validity period.*

***Keywords :*** *Access Point, Sertification, Wifi Analyzer, Wireshark*

**Abstrak**

Kinerja jaringan Wi-Fi di ruang kerja kantor dapat dilihat dari sinyal yang diterima oleh pengguna akses point (AP). Penelitian ini dilakukan untuk menganalisis sistem keamanan Wi- Fi dan mengoptimalkan dengan mengambil kasus di Salah Satu Ruangan Kantor Bank CIMB NIAGA pada lantai GN 1 Lantai 2 dengan menganalisa paket data menggunakan aplikasi wireshark dan memeriksa kinerja akses point menggunakan Wifi Analizer. Tujuan serangan ini adalah untuk membuat komputer yang mengakses tidak bisa berjalan dengan normal sehingga wireshark ini dapat membantu untuk mendeteksi serangan yang akan terjadi sehingga pengguna jaringan internet tidak khawatir dengan serangan tersebut dengan manganalisa parameter apa yang dipakai untuk melakukan serangan. Pemakai juga diharapkan mengetahui sistem keamanan website berupa sertifikasi dan masa berlakunya.

**Kata kunci *:*** Akses Point, Sertifikasi, Wifi Analizer, Wireshark

## Pendahuluan

Pertumbuhan teknologi internet sangat kilat sekali serta penggunaannya telah menyebar di bermacam pelosok belahan bumi baik yang memakai jaringan kabel ataupun yang jaringan nirkabel (Jaringan WiFi). Teknologi wireless (tanpa kabel / nirkabel) dikala ini tumbuh sangat pesat paling utama dengan hadirnya fitur teknologi data serta komunikasi (Riadi et al., 2020). PC, notebook, PDA, telepon seluler( hp) serta pheriperalnya mendominasi konsumsi teknologi wireless yang diimplementasikan dalam sesuatu jaringan lokal kerap dinamakan WLAN( Wireless Local Area Network). Tetapi pertumbuhan teknologi wireless yang terus tumbuh sehingga ada sebutan yang mendampingi WLAN semacam WMAN (Metropolitan), WWAN (Wide), serta WPAN (Personal/ Private) (Ginanti et al., 2022). Dengan terdapatnya teknologi wireless seorang bisa bergerak ataupun berkegiatan kemana serta dimanapun buat melaksanakan komunikasi informasi ataupun suara (Supriyanto, 2006).

Jaringan wireless ialah teknologi jaringan pc tanpa kabel, ialah memakai gelombang berfrekuensi besar. Sehingga komputer- komputer itu dapat silih tersambung tanpa memakai kabel (Haerudin et al., 2017). Tetapi jaringan WiFi mempunyai lebih banyak kelemahan dibandingkan dengan jaringan kabel, tetapi dikala ini pertumbuhan teknologi WiFi sangat signifikan sejalan dengan kebutuhan sistem data yang mobile. Pemakaian penyedia jasa wireless antara lain ISP, Warnet, wifi, komersil, kampus- kampus ataupun perkantoran telah banyak yang menggunakan WiFi pada jaringan tiap- tiap, namun sangat sedikit yang mencermati keamanan komunikasi informasi pada jaringan wireless tersebut(Ignatov et al., 2021). Oleh sebab itu banyak hacker yang tertarik buat mengexplore kemampuannya dalam melaksanakan bermacam kegiatan yang umumnya illegal memakai WiFi.

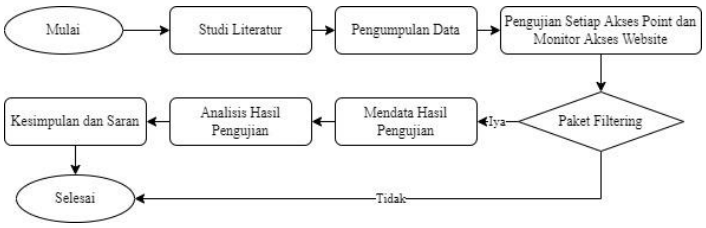
Konsumsi teknologi wireless secara universal dipecah atas tanpa pengamanan (nonsecure) serta dengan pengamanan (Share Key/ secure). Non Secure (open), ialah tanpa memakai pengaman, dimana PC

yang mempunyai pancaran gelombang bisa mendengar transmisi suatu pancaran gelombang serta langsung masuk ke dalam network. Sebaliknya share key, ialah alternatif buat konsumsi kunci ataupun password. Selaku contoh, suatu network yang memakai WEP.

## Metode Penelitian

Pada metode penelitian membahas tentang alur penelitian yang dilakukan dalam proses penyelesaian penelitian. Terdapat beberapa tahapan metode yang dilakukan untuk merealisasikan pembuatan tools ini agar selesai dan sesuai dengan yang diharapakan.

1. **Studi Literatur**
   Tahap ini dilakukan penelusuran yang berkaitan dengan penelitian. Studi literatur dilakukan untuk pengumpulan bahan-bahan referensi. Literatur yang digunakan dapat berupa jurnal ilmiah penelitian sebelumnya, buku-buku,dan data-data yang dapat digunakan untuk mendukung penyelesaian penelitian.
2. **Metode Pengumpulan**
   Data Metode pengumpulan data yang dilakukan dalam penelitian ini adalah dengan metode observasi dimana metode ini melakukan pengamatan secara langsung kegiatan yang sedang dilakukan pada penelitian ini pengumpulan data dilakukan dengan cara melakukan Monitoring Akses Point (AP), simulasi akses website, capture and filtering packet dan Analisa layer dan Packet. Dalam pengumpulan data dan informasi secara langsung yang dilakukan pada sistem keamanan WPA2-PSK pada jaringan publik wireless perlu mengetahui topologi jaringan wireless, manajemen jaringan, dan sistem keamanan wireless yang digunakan.
3. **Metode Penelitian**
   Langkah-langkah penelitian ini dapat dilihat pada diagram alur penelitian di bawah ini:




Gambar 1. Diagram Alur Penelitian

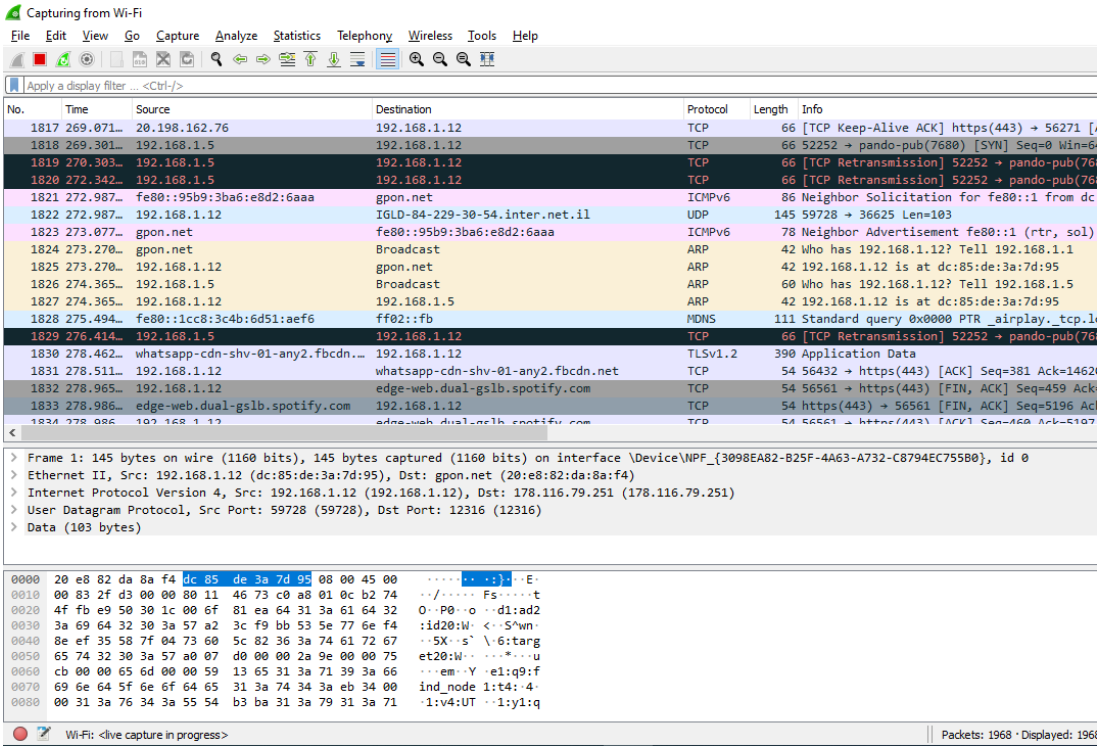
## Hasil dan Pembahasan

Dari gambar diatas terlihat 6 buah akses point dengan sistem keamanan masing-masing beserta satuan kuat sinyal dalam dBm yang mana untuk angka yang didepannya ada tanda minus (-) maka nilai semakin besar maka kekuatan sinyal akan semakin kecil.

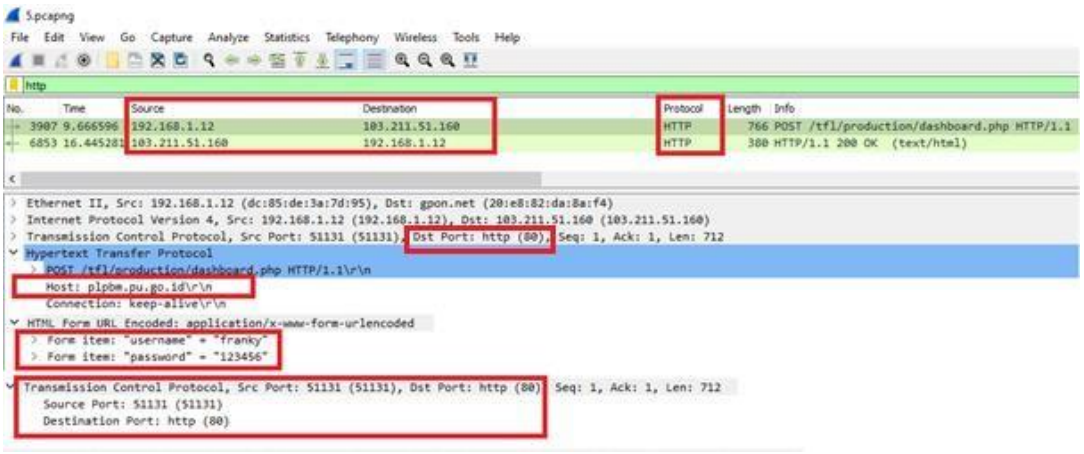

(a) (b)

Gambar 2. a Monitoring Akses Point
b. Detail 1 Akses Point

Pada Aplikasi Wifi Analyzer juga tertera authentication yaitu jenis sistem keamanan pada salah satu akses point yaitu menggunakan RSNA-PSK (WPA2) Berikut salah satu analisa paket-paket data browsing yang masuk pada masing-masing perangkat dengan mengetahui IP pengirim dan IP tujuan paket tersebut, adapun website yang akan dibrowsing yang kemudian paket datanya di analisa adalah http://plpbm.pu.go.id yang merupakan salah satu situs sosialisasi dari kementrian.




Gambar 3 Hasil Capturing Data Realtime




Gambar 4 Hasil Filtering Capturing Data

Dengan packet filtering pada wireshark kita dapat menghasilkan event yang dimaksud dengan mencocokkan IP asal. Dalam proses analisa aktivitas illegal di dalam jaringan, wireshark mampu untuk melihat atau menganalisis paket secara offline seperti ditunjukkan gambar 6 dimana penulis menyimpan file terlebih dahulu kedalam filter *.pcap. Dalam melakukan perancangan ini penulis memperoleh beberapa aktivitas data dalam file ini. Dengan menyaring aktivitas jaringan dengan parameter sebuah protokol http dan mengetahui IP adresss sumber dan tujuan maka akan didapat hasil pemantauan website berupa data MAC Address, port yang dipakai, username dan password sistem keamanan antar websire dan server berupa sertifikasi dan masa berlaku sertifikasi tersebut. Dari Data hasil capturing untuk penggunaan website http://plpbm.pu.go.id dinilai tidak aman karena dengan menggunakan port 80 maka data masukan berupa login dan password dapat terlacak.

## Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab sebelumnya, dalam penelitian yang berjudul Keamanan Jaringan Komputer Nirkabel dengan Analisa Aktivitas Ilegal ,penulis dapat menyimpulkan beberapa hal berupa: Sniffing adalah metode yang ampuh digunakan untuk menembus sistem keamanan jaringan nirkabel dengan menganalisa paket dan layer yang sedang bekerja. Penggunaan https pada protokol jaringan aplikasi dapat digunakan untuk penangguhan sniffing. Penggunaan port 80 dan 81 yang digunakan pada internet sangat rentan terhadap serangan untuk itu dipergunakanlah port 443. 4. Sistem keamanan dapat diperkuat dengan mengetahui seluk beluk SSL yaitu sistem keamanan antara web dan server dan juga memperbarui sertifikasi jika sudah kadaluarsa.

## Daftar Pustaka

Ginanti, D. E., Christian, A., & Hidayat, T. (2022). Analisa Dan Implementasi Jaringan Wireless Mac Address Menggunakan Filtering Pada Pt. Faya Kuntura Agung Konsultindo. *INTI Nusa Mandiri*, *16*(2), 79–84. https://doi.org/10.33480/inti.v16i2.2781

Haerudin, D. I., Aksara, L. B., & Yamin, M. (2017). Implementasi Wireless Distribution System (Wds) Pada Hotspot (Studi Kasus : Smk Negeri 1 Kendari). *SemanTIK*, *3*(2), 105–112.

Ignatov, A., Chiang, C. M., Kuo, H. K., Sycheva, A., Timofte, R., Chen, M. H., Lee, M. Y., Xu, Y. S., Tseng, Y., Xu, S., Guo, J., Chen, C. H., Hsyu, M. C., Tsai, W. C., Chen, C. W., Malivenko, G., Kwon, M., Lee, M., Yoo, J., … De Stoutz, E. (2021). Learned smartphone ISP on mobile NPUs with deep learning, mobile AI 2021 challenge: Report. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2503–2514. https://doi.org/10.1109/CVPRW53098.2021.00284

Riadi, I., Fadlil, A., & Hafizh, M. N. (2020). Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology. *Edumatic : Jurnal Pendidikan Informatika*, *4*(1), 21–29. https://doi.org/10.29408/edumatic.v4i1.2046

Supriyanto, A. (2006). Analisis Kelemahan Keamanan pada Jaringan Wireless. *Analisis Keamanan Jaringan Wireless*, *XI*(1), 38–46.