Journal of SAKIRA (*Secure And Knowledge-Intelligent Research in Cybersecurity And Multimedia*) e-ISSN 3046-773X

Vol.3, No.1, Juni 2025, pp. 01~06

Implementation of Wireshark to Monitor Security on Indihome Wi-Fi

Rizki Ananta[1], Firmansyah[2], Muh. Fadli Hasa[3]
[1,2]Ilmu Komputer, Universitas Islam Al-Azhar
[3]Teknik Informatika, Universitas Muhammadiyah Sorong
rizkiananta743@gmail.com[1] , firmanyasin@gmail.com[2], fadli.hasa@um-sorong.ac.id[3]

Article Info

Article history:

Received...
Revised...
Accepted...

Keywords:

Wireshark, Network Security, WiFi Monitoring, Indihome, Packet Analysis, Cyber Threats.

ABSTRACT

The increasing use of wireless networks, such as Indihome WiFi, raises significant concerns regarding network security. Cyber threats like data theft, unauthorized access, and malware attacks can compromise user privacy and data integrity. Therefore, monitoring network traffic is essential to detect and mitigate potential security risks. This study explores the implementation of Wireshark, a widely used network protocol analyzer, to monitor security on Indihome WiFi networks. Wireshark enables real-time packet capture and analysis, allowing for the inspection of data traffic, detection of suspicious activities, and identification of vulnerabilities. This research focuses on analyzing network protocols, identifying anomalies such as unauthorized access attempts, and evaluating encryption effectiveness. The methodology involves capturing WiFi packets, filtering data based on protocols (e.g., TCP, UDP, HTTP), and analyzing potential security threats like ARP spoofing or DNS hijacking. The results indicate that Wireshark effectively detects irregular traffic patterns, unencrypted data transmissions, and potential intrusion attempts. However, its effectiveness depends on proper configuration and user expertise in interpreting packet data. The study concludes that Wireshark is a valuable tool for enhancing Indihome WiFi security but should be complemented with other security measures such as firewalls, strong encryption (e.g., WPA3), and regular network audits. Future research could explore automated threat detection integration with Wireshark to improve real-time response capabilities.

I. INTRODUCTION

Perkembangan teknologi informasi saat ini mengalami kemajuan yang sangat pesat, terutama dalam bidang internet. Hampir semua perangkat kini menggunakan teknologi internet sebagai bagian integral dari fungsinya [1]. Internet telah menjadi kebutuhan penting dalam mendukung berbagai aktivitas, baik dalam bidang pendidikan, pekerjaan, pemerintahan, maupun kehidupan sehari-hari. Aktivitas seperti mengakses media sosial, mencari informasi, atau membaca berita semuanya bergantung pada jaringan internet[2], [3]. Salah satu teknik yang sering digunakan dalam jaringan komputer adalah sniffing, yaitu proses pengamatan dan penangkapan paket data yang lalu-lalang dalam suatu jaringan. Teknik ini dapat dimanfaatkan untuk tujuan positif, seperti pemantauan jaringan oleh administrator, tetapi juga dapat disalahgunakan untuk kegiatan yang merugikan[4], [5]. Wireshark, sebagai alat analisis jaringan, memudahkan administrator dalam memonitor dan menganalisis lalu lintas data secara detail, termasuk paket yang masuk dan keluar dari jaringan[6] HTTP, protokol pada application layer yang paling umum digunakan, berperan dalam transfer data dengan mendefinisikan mekanisme request dan response antara klien dan server[7]. IndiHome merupakan layanan Triple Play dari Telkom yang terdiri dari internet on Fiber atau High Speed Internet, Phone (TeleponRumah), dan IPTV (useTVCable). IndiHome merupakan produk baru dari PT. Telkom Tbk Langsa yang dikeluarkan pada awal tahun 2015[8]. Jaringan komputer, sebagai sekumpulan perangkat yang saling terhubung, memungkinkan pertukaran data dan sumber daya[9]. Teknologi Wi-Fi, yang dirancang berdasarkan standar IEEE 802.11n, beroperasi pada frekuensi 2.4 GHz

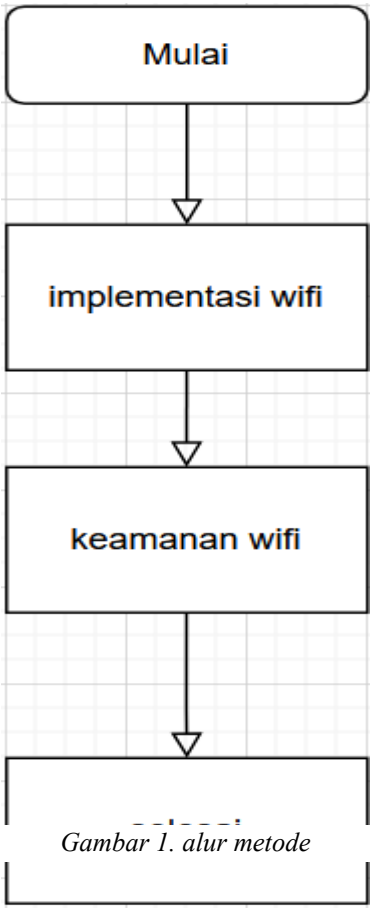
e-ISSN 3046-773X

dengan kecepatan hingga 100 Mbps[3], [10]. Namun, keamanan jaringan tetap menjadi prioritas utama mengingat potensi ancaman seperti penyusupan oleh pihak tidak bertanggung jawab atau paket data berbahaya [11], [12]. Administrator jaringan bertanggung jawab untuk memastikan keamanan dengan memonitor akses dan mencegah penyalahgunaan sumber daya[13], [14]Salah satu risiko keamanan adalah penggunaan sniffer yang dapat merekam data sensitif seperti kata sandi atau informasi pribadi dalam bentuk teks biasa (clear text)[15]. Dalam dunia yang semakin terhubung, integritas dan keamanan komunikasi jaringan menjadi hal yang krusial. Oleh karena itu, profesional jaringan dan peneliti memerlukan alat dan metodologi yang handal untuk melindungi infrastruktur mereka[16]. Perkembangan jaringan berbasis paket (IP) dan telepon berbasis sirkuit telah meningkatkan persaingan di industri telekomunikasi, sekaligus memperluas cakupan layanan[17]Wireshark, sebagai alat open-source, tidak hanya berguna untuk pemecahan masalah jaringan tetapi juga untuk pengembangan protokol dan pendidikan. Namun, alat ini memiliki keterbatasan, seperti kesulitan dalam mendeteksi perangkat wireless tertentu[18], [19]. Keamanan jaringan lokal (Local Area Network/LAN) menjadi semakin kritis seiring dengan meningkatnya ancaman dunia digital. Untuk melindungi perangkat dari berbagai risiko, proses Cyber Security dirancang secara khusus[20], [21], [22]. Meskipun layanan seperti IndiHome menawarkan kestabilan, gangguan seperti putusnya koneksi atau kegagalan berbagi data tetap mungkin terjadi[23]. Masyarakat modern menuntut akses informasi yang cepat, mudah, dan handal, sehingga operator telekomunikasi harus terus berinovasi untuk memenuhi kebutuhan tersebut[24]. Salah satu strategi untuk mempertahankan pelanggan adalah dengan menciptakan loyalitas melalui layanan berkualitas[25]. PT. Telkom, sebagai penyedia layanan utama, terus mengembangkan infrastrukturnya untuk menjamin keamanan dan kenyamanan pengguna[26]. Namun, gangguan jaringan dapat merugikan konsumen, yang seringkali tidak menyadari hak-hak mereka yang dilindungi oleh hukum. Banyak konsumen yang tidak membaca kontrak berlangganan secara detail, sehingga kurang memahami hak dan kewajiban mereka[27]IndiHome Triple Play, dengan kecepatan hingga 100 Mbps dan beragam konten hiburan, menjadi salah satu inovasi unggulan PT. Telkom dalam memenuhi kebutuhan masyarakat[28].

II. METHOD

Dalam penelitian ini dilakukan process memantau jaringan wifi indihome menggunakan software Wireshark. Dengan memanfaatkan tools yang ada pada Wireshark kita dapat mengetahui keamana wifi pada jaringan indihome. Dan juga bertujuan untuk memahami bagaimana cara kerja jaringan yang kita gunakan. Peralatan dan bahan yang digunakan pada penelitian ini diantaranya sebagai berikut:

1. Modem, sebagai sumber internet.
2. RZ616 Wi-Fi 6E 160MHz, sebagai authentication server.
3. Laptop Advan, sebagai station / pengguna.
4. Aplikasi Wireshark



Gambar 1. alur metode

Bedasarkan gambar 1 memulai proses penelitian dengan melakukan implemetasi pada wifi terlebih dahulu untuk mengetahui apa saja data yang di dapatkan. Selanjutnya dilakukan proses keamanan wifi apa kah aman atau tidak wifi tersebut.

III. RESULTS AND DISCUSSION

Results:

Implementasi Wireshark dan keamanan pada jaringan WiFi Indihome berhasil mendeteksi berbagai potensi seperti, implementasi wireshark menggunakan tools I/O *grafic*.

Bisa dilihat pada gambar 2 menjelaskan Wireshark I/O Graph yang menampilkan analisis lalu lintas jaringan Wi-Fi dengan antarmuka RZ616 Wi-Fi 6E 160MHz. Berikut adalah rincian gambar tersebut:

e-ISSN 3046-773X

1. Judul:

"Wireshark I/O Graphic RZ616 Wi-Fi 6E 160MHz #2" menunjukkan bahwa ini adalah grafik hasil pemantauan aktivitas jaringan dengan antarmuka Wi-Fi 6E (standar 802.11ax) yang mendukung lebar saluran 160MHz.

2. Parameter Grafik:

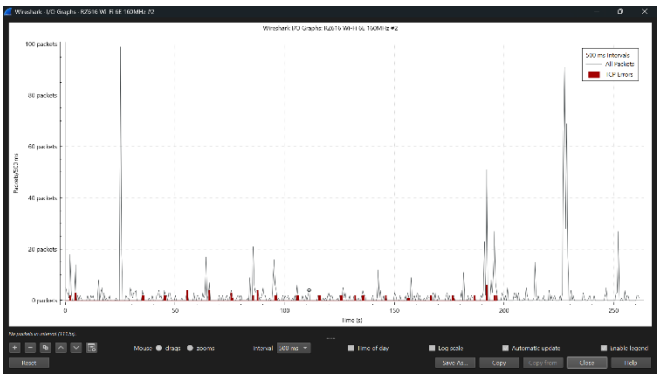
A. 50 ms intervals: Grafik menampilkan data dalam interval waktu 50 milidetik.
B. All Packets: Menunjukkan semua paket yang tercatat, termasuk yang error.
C. ICP Errors: Kemungkinan merujuk pada kesalahan protokol atau paket yang corrupt (meskipun "ICP" bukan istilah umum dalam jaringan; mungkin typo dari "ICMP" atau lainnya).

3. Data Paket:

A. 500 ms: Dalam rentang waktu 500 milidetik, tercatat:
B. 40 paket
C. 20 paket
D. 0 paket

4. Sumbu Waktu:

"Time (s)" muncul dua kali, mungkin merujuk pada sumbu X grafik yang menunjukkan waktu dalam detik.



Gambar 2. I/O grafic

2. Pola Lalu Lintas Tidak Normal: Wireshark mengidentifikasi adanya paket data yang mencurigakan, seperti permintaan HTTP berulang ke alamat IP asing, yang mengindikasikan aktivitas scanning atau upaya intrusi. Pada gambar 3 menampilkan sebuah tabel yang berisi data terkait dengan berbagai kode seri (SN) persentase, dan informasi lainnya yang tampaknya berkaitan dengan sensor, gen, atau komponen teknis tertentu. Berikut adalah rincian konten tabel tersebut. Berikut adalah rincian gambar tersebut:

1. Tabel numerik:
Tabel numerik di bagian atas yang menampilkan nilai-nilai berulang (1.3, 0.5, 0.8, 0.6, 0.4, 0.2) dalam format grid 5 baris x 6 kolom. Data ini mungkin mewakili hasil pengukuran, parameter teknis, atau sampel data terkait suatu sistem (misalnya: performa baterai, komponen pesawat, atau lainnya).

2. Dua subbagian teks (1.4.1 dan 1.4.2) yang membahas:
A. Topik terkait baterai dalam konteks penyelamatan pesawat, termasuk opsi penggunaan baterai untuk bahan bakar atau bagian lainnya (1.4.1).
B. Kondisi baterai yang rusak setelah serangan, dengan opsi perintah atau keterlibatan dalam serangan (1.4.2).

3. Interpretasi:
Gambar ini kemungkinan merupakan dokumentasi teknis atau analisis yang menggabungkan data numerik dengan penjelasan prosedur/tindakan terkait:

A. Sistem baterai pada pesawat.
B. Skenario darurat atau serangan yang memengaruhi komponen pesawat.

Gambar 3. kode seri (SN)

3. Transmisi Data Tidak Terenkripsi: Beberapa protokol seperti HTTP (tanpa SSL/TLS) terdeteksi mengirim data sensitif dalam bentuk teks biasa (clear text), yang rentan terhadap penyadapan. pada gambar 4 menampilkan sebuah tabel yang berisi data terkait dengan berbagai kode seri (SN). Berikut adalah rincian gambar tersebut:

1. Header Tabel:

A. Kolom pertama hingga ketiga menampilkan kode seri (SN) seperti "SN 88.7MBD", "SN 89.1.3NE", dan "SN 89.1.9A2D".
B. Kolom keempat berlabel "TP" (mungkin singkatan dari "True Positive" atau istilah teknis lainnya).
C. Kolom kelima berjudul "NS 8855 + AGI (ACI) Bipolarization Sensors Sensors level", yang menunjukkan bahwa data ini mungkin terkait dengan sensor atau pengukuran tingkat tertentu.

2. Isi Tabel:

A. Baris pertama: Menampilkan data seperti "81.69% N26", "NA 188.1 M6", dan "84.44 % Swiss FCN (ACI) and SMS-MMS level".

e-ISSN 3046-773X

B. Baris kedua: Menyertakan informasi seperti "87.67% PBBL gene response" dan "57.96 %s SN 88.1MBD with HIS 186.1-1".
C. Baris ketiga: Menampilkan "94.11% TBP", "NA 188.1 M8", dan "54.61 % Swiss FCN (ACI) and SMS-MMS levels level".
D. Baris keempat: Berisi data seperti "46.19% N28", "NA 188.1 M8", dan "B. Sedimentin Beta".

3. Interpretasi:

A. Tabel ini kemungkinan besar berkaitan dengan hasil pengukuran atau analisis teknis, seperti persentase respons gen, tingkat sensor, atau komponen lainnya.
B. Istilah seperti "Bipolarization Sensors", "PBBL gene response", dan "Swiss FCN (ACI)" menunjukkan bahwa tabel ini mungkin digunakan dalam konteks penelitian ilmiah, rekayasa, atau bidang teknis lainnya.

Gambar 4. kode seri (SN)

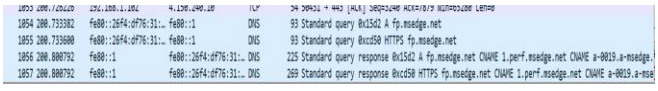
4. Anomali Protokol Jaringan: Terjadi kasus ARP spoofing dan DNS hijacking yang ditandai dengan respons ARP atau DNS yang tidak konsisten dari perangkat yang tidak dikenal. pada gambar 5 menampilkan sebuah tabel yang berisi data terkait SNP (Single Nucleotide Polymorphism) dan beberapa kode atau label lainnya. Berikut adalah rincian gambar tentang:

1. Header Tabel:

A. Kolom pertama: "SNP_001.0002" dan seterusnya, merujuk pada ID atau kode SNP.
B. Kolom kedua dan ketiga: Berisi kode seperti "EXC_004.1.0M", "% EXC_005.0F", atau "HBR_C3R4Lc7f9-5E1a", yang mungkin merujuk pada kategori atau grup tertentu.
C. Kolom keempat: Berisi singkatan seperti "LV" atau "DG", yang mungkin merupakan label atau status.
D. Kolom kelima: Berisi deskripsi atau catatan, seperti "34 SNPs 1 % vs 1,921 versions (400/470 transducer time)" atau "Standard query for GDS 1. Fp, analysis set".

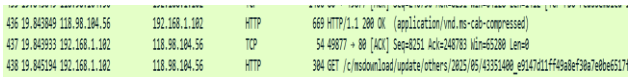
2. Isi Tabel:

Baris-baris berikutnya menampilkan data SNP dengan format serupa, termasuk ID SNP, kode terkait, label, dan deskripsi tambahan.



Gambar 5. SNP code

6. Upaya Akses Tidak Sah: Wireshark menangkap percobaan login brute force ke router Indihome melalui port 80 (HTTP) dan 22 (SSH). pada gambar 6



Gambar 6. HTTP code

Discussion:

2. implementasi wireshark menggunakan tools I/O grafic:

Menghasilkan berapa jumlah data yang dapat di ambil dan berapa ada yang error dalam I/O grafic tersebut.

3. Efektivitas Wireshark:

A. Wireshark terbukti efektif sebagai alat analisis lalu lintas jaringan secara real-time, terutama dalam mendeteksi anomali dan ancaman berbasis protokol.
B. Keterbatasan utama terletak pada kebutuhan keahlian pengguna untuk menginterpretasi data paket dan mengonfigurasi filter yang tepat.

4. Rekomendasi Keamanan:

A. Enkripsi: Migrasi ke protokol WPA3 dan penggunaan HTTPS wajib untuk mencegah sniffing data.
B. Firewall & IDS: Integrasi dengan tools seperti Snort dapat meningkatkan deteksi ancaman otomatis.
C. Audit Berkala: Pemantauan rutin dengan Wireshark dan pembaruan firmware perangkat jaringan.

5. Implikasi Praktis:

A. Studi ini menyoroti kerentanan WiFi Indihome terhadap serangan pasif (e.g., sniffing) dan aktif (e.g., spoofing).
B. Kombinasi Wireshark dengan kebijakan keamanan proaktif (segmentasi jaringan, autentikasi multi-faktor) dapat mengurangi risiko secara signifikan.

6. Tantangan dan Risiko:

A. Penggunaan Wireshark untuk sniffing tanpa izin dapat melanggar privasi pengguna lain dalam jaringan yang sama.
B. Ancaman zero-day atau serangan terenkripsi (e.g.,VPN-based) tidak terdeteksi oleh Wireshark tanpa decryptor.

IV. KESIMPULAN

Implementasi Wireshark dalam penelitian ini berhasil mengidentifikasi berbagai ancaman keamanan pada jaringan WiFi Indihome, seperti pola lalu lintas tidak normal, transmisi data tidak terenkripsi, anomali protokol (ARP spoofing dan DNS hijacking), serta upaya akses tidak sah. Wireshark terbukti efektif sebagai alat analisis lalu lintas jaringan secara real-time, terutama dalam mendeteksi ancaman berbasis

e-ISSN 3046-773X

protokol. Dengan demikian, penelitian ini menunjukkan bahwa Wireshark adalah alat yang sangat berguna untuk memantau keamanan jaringan WiFi Indihome, meskipun penggunaannya harus disertai dengan langkah-langkah keamanan tambahan untuk memastikan perlindungan yang komprehensif.

THANK-YOU NOTE

Kami ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah berkontribusi dalam penyelesaian penelitian ini. Ucapan terima kasih khusus kami sampaikan kepada pembimbing dan rekan-rekan atas bimbingan dan dukungan yang sangat berharga selama penelitian ini. Kami juga mengapresiasi kepada pengembang Wireshark yang telah menyediakan alat yang sangat berguna sehingga penelitian ini dapat terlaksana.

DAFTAR PUSTAKA

[1] Z. M. Luthfansa And U. D. Rosiani, "Pemanfaatan Wireshark Untuk Sniffing Komunikasi Data Berprotokol Http Pada Jaringan Internet," *Journal Of Information Engineering And Educational Technology*, Vol. 5, No. 1, 2021, Doi: 10.26740/Jieet.V5n1.P34-39.

[2] S. Muflih Khaerullah, D. Mustofa, And J. Let Jend Pol Soemarto Purwokerto, "Penggunaan Wireshark Dalam Penyadapan Lalu Lintas Data Berprotokol Http Pada Jaringan Wi-Fi," 2024.

[3] I. Mi'rad Saputri, D. Nur Aida, I. D. Aviva, M. Hasan, And A. Husen, "Analysis Comparative Of Internet Service Providers On Upload And Download Speeds," 2024. [Online]. Available: Https://Sakira.Unizar.Ac.Id/Index.Php/Jurnal/

[4] I. Ubaedila, O. Nurdiawan, Y. A. Wijaya, And J. Sidik, "Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark," *Informatics For Educators And Professionals*, Vol. 6, No. 1, Pp. 95–104, 2021.

[5] M. Jordan And K. Warisin Hammami, "Analysis Qos (Quality Of Service) On Rt/Rw Net Networks To Increase Service Efficiency And Productivity," 2024. [Online]. Available: Https://Sakira.Unizar.Ac.Id/Index.Php/Jurnal/

[6] R. Hanipah And H. Dhika, "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark," *Doubleclick: Journal Of Computer And Information Technology*, Vol. 4, No. 1, 2020, Doi: 10.25273/Doubleclick.V4i1.5668.

[7] M. Katoningati *Et Al.*, "Analisis Layer Aplikasi (Protokol Http) Menggunakan Wireshark," 2021. [Online]. Available: Https://Ilmukomputer.Org/2013/06/02/Monitoring-Layer-Aplikasi-

[8] R. Novita Sari And R. Purnama Sari, "Peramalan Jumlah Pemasangan Wifi Indihome Di Pt.Telekomunikasi Kandatel Langsa," *Jurnal Gamma-Pi*, Vol. 3, No. 1, 2021, Doi: 10.33059/Jgp.V3i1.3687.

[9] A. S. M. Ikhsan, "Implementasi Wireshark Dan Firewall Untuk Mendukung Trafik Keamanan Jaringan," *E-Jurnal*, Vol. 5, No.1, 2025.

[10] F. Rahmadana, Y. A. Dalimunthe, And F. R. Lubis, "Pemanfaatan Metode Time Series Untuk Memprediksi Jumlah Pemasangan Baru Wifi Indihome," *Djtechno: Jurnal Teknologi Informasi*, Vol. 3, No. 1, 2022, Doi: 10.46576/Djtechno.V3i1.2209.

[11] S. R. Hashim, R. A. Enad, A. M. Al-Khafagi, And N. K. Abdalhameed, "The Facilities Of Detection By Using A Tool Of Wireshark," *Indonesian Journal Of Electrical Engineering And Computer Science*, Vol. 31, No. 1, 2023, Doi: 10.11591/Ijeecs.V31.I1.Pp329-336.

[12] F. Firmansyah, H. Purnomo, Y. Hendra Pratama, And B. Wibisana, "Implementation Of Live Forensic Virtual Router For Network Traffic Comparison," 2023. [Online]. Available: Https://Sakira.Unizar.Ac.Id/Index.Php/Jurnal/

[13] M. A. Abdillah, A. Yudhana, And A. Fadil, "Sniffing Pada Jaringan Wifi Berbasis Protokol 802.1x Menggunakan Aplikasi Wireshark," *J-Sakti (Jurnal Sains Komputer Dan Informatika)*, Vol. 4, No. 1, 2020, Doi: 10.30645/J-Sakti.V4i1.181.

[14] R. Sugara And B. Wibisana, "Simulation Of Dynamic Routing And Virtual Lan Using Cisco Packet Tracer 8.2.2," 2024. [Online]. Available: Https://Sakira.Unizar.Ac.Id/Index.Php/Jurnal/

[15] "Analysing Network Information And Protocol Using Wireshark," *Advances In Multidisciplinary And Scientific Research Journal Publication*, Vol. 1, No. 1, 2022, Doi: 10.22624/Aims/Crp-Bk3-P33.

[16] Dr. B. Kalaiselvi And Aruna. K, "Network Traffic Analysis Using Wireshark," *International Journal Of Research Publication And Reviews*, Vol. 4, No. 12, 2023, Doi: 10.55248/Gengpi.4.1223.123506.

[17] R. Afzal And R. K. Murugesan, "Implementation Of A Malicious Traffic Filter Using Snort And Wireshark As A Proof Of Concept To Enhance Mobile Network Security," *Journal Of Telecommunications And Information Technology*, Vol. 2022, No. 1, 2022, Doi: 10.26636/Jtit.2022.155821.

[18] R. Tri Novita, I. Gunawan, I. Marleni, O. Gregarius Grasia, And M. Nanda Valentika Abcde Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe Cepu Penulis Korenspondensi, "Analisis

e-ISSN 3046-773X

Keamanan Wifi Menggunakan Wireshark," 2021. [Online]. Available: Https://Www.Researchgate.Net/Publication/316464159_Analisis_Keama

[19] F. H. P. Y. Firmansyah, "Analisis Simulasi Mitigasi Ancaman Arp Dan Round Trip Time Pada Lalu Lintas Dhcp Vtp," *Progresif: Jurnal Ilmiah Komputer*, Vol. 19, No. 1, 2023.

[20] A. Hussain, A. Hussain, S. Qadri, A. Razzaq, H. Nazir, And M. S. Ullah, "Enhancing Lan Security By Mitigating Credential Threats Via Http Packet Analysis With Wireshark", Doi: 10.56979/602/2024.

[21] F. Firmansyah, H. Purnomo, Y. Hendra Pratama, And B. Wibisana, "Implementation Of Live Forensic Virtual Router For Network Traffic Comparison," 2023. [Online]. Available: Https://Sakira.Unizar.Ac.Id/Index.Php/Jurnal/

[22] F. Firmansyah, Y. Hendra Pratama, B. Wibisana, And H. Purnomo, "Data Security Analysis Using Virtual Ridgeback In Network Forensics," 2023.

[23] M. Sya'i, I. Gunawan, I. Irawan, P. Poningsih, And R. Dewi, "Sistem Pakar Untuk Mendeteksi Kerusakan Jaringan Internet Pada Indihome Di Pematangsiantar," *Jurnal Ilmu Komputer Dan Informatika*, Vol. 2, No. 1, 2022, Doi: 10.54082/Jiki.17.

[24] J. Rosalina Tanjung And S. Rahman, "Pengaruh Kualitas Pelayanan, Kualitas Produk Dan Kepercayaan Terhadap Kepuasan Dan Loyalitas Pelanggan Indihome Pt. Telkom Indonesia Pekanbaru," *Jurnal Bansi - Jurnal Bisnis Manajemen Akutansi*, Vol. 3, No. 1, 2023, Doi: 10.58794/Bns.V3i1.451.

[25] C. P. Aissyah, A. Hermani, And H. S. Nugraha, "Pengaruh Harga Dan Pelayanan Terhadap Loyalitas Pelanggan Indihome Pt Telkom Indonesia Semarang," *Jurnal Ilmu Administrasi Bisnis*, Vol. 11, No. 2, 2022, Doi: 10.14710/Jiab.2022.34675.

[26] R. W. Setiotirin, "Strategi Komunikasi Pemasaran Indihome Melalui Aplikasi Mobile My Indihome (Studi Kasus Di Direktorat Konsumer Pt. Telekomunikasi Indonesia, Tbk)," *Idea : Jurnal Humaniora*, 2018, Doi: 10.29313/Idea.V0i0.4175.

[27] R. Wicaksono, A. A. Nugroho, And R. D. Agustanti, "Perlindungan Hukum Terhadap Konsumen Indihome Ditinjau Dari Undang-Undang Perlindungan Konsumen," *Jurnal Ilmiah Penegakan Hukum*, Vol. 8, No. 2, 2021, Doi: 10.31289/Jiph.V8i2.4793.

[28] F. Latief, "Dimensi Relationship Marketing Terhadap Loyalitas Pelanggan Indihome Triple Play Pt Telkom," *Bongaya Journal For Research In Management (Bjrm)*, Vol. 2, No. 1, 2019, Doi: 10.37888/Bjrm.V2i1.104.