

## Analisis Monitoring Untuk Pencegahan Akses Ilegal di Dalam Jaringan Departement TI PT. PUSRI

Tamsir Ariyadi<sup>1</sup>, M.Alzi Ikrar Agamuri<sup>2</sup>, Rahmat Wiratama<sup>3</sup>, Dasril Kholid<sup>4</sup>

<sup>1, 2, 3, 4</sup>Universitas Bina Darma, Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, 30264, Indonesia

### INFORMASI ARTIKEL

#### Sejarah Artikel:

Diterima Redaksi: 26 Februari 2025

Revisi Akhir: 14 Maret 2025

Diterbitkan Online: 15 Maret 2025

### KATA KUNCI

Wireshark, Monitoring, Teknologi, PT.Pusri

### KORESPONDENSI

E-mail: [tamsirariyadi@binadarma.ac.id](mailto:tamsirariyadi@binadarma.ac.id)

### ABSTRACT

Technology plays an important role in human survival in daily activities that cannot be separated from technology. Information technology makes it easy for humans to share information or search for information. Cyber attacks such as malware attacks or hacking attempts are a serious threat to IT networks. The purpose of network security is to anticipate the risk of network threats that can disrupt daily computer network operations. In this study, the author used the Action Research method. This study aims to test and develop, find and design. The network in the IT Department of PT. Pupuk Srwidjaja Palembang is quite safe because when network monitoring was carried out for 10 days on June 6, 2023 to June 22, 2023, there was no illegal access.

## 1. PENDAHULUAN

Diera digitalisasi saat ini, teknologi memegang peranan penting kelangsungan hidup manusia dalam aktivitas sehari-hari tidak lepas dari teknologi [1]. [2] Masalah ini berubah dari cara berpikir menjadi acuan bagi kemajuan peradaban manusia dan menangani dan memecahkan setiap masalah pola pikir yang kompleks agar tidak tersesat dengan perkembangan dan dukungan teknologi informasi [3] didukung oleh berbagai penemuan dan inovasi banyak perubahan dalam hidup seseorang [4]. [5] Itu juga menyebabkan pengembangan bersama pembangunan dan teknologi Perangkat keras, secara langsung atau tidak langsung Informasi telah menjadi bagian penting dalam berbagai aspek kehidupan untuk dukungan sederhana tenaga kerja manusia [6]. [7] Departemen TI sering kali bertanggung jawab untuk mengelola dan menjaga keamanan data sensitive seperti informasi karyawan, informasi pelanggan, atau data bisnis penting lainnya. Monitoring dan pencegah akses ilegal membantu mencegah upaya pencurian atau pengungkapan data yang tidak sah di PT Pupuk Sriwidjaja (PUSRI).

Teknologi informasi memudahkan manusia berbagi informasi atau mencari informasi [8]. Kamu bisa melihatnya Tentang perkembangan teknologi internet dan jaringan. Baru-baru ini internet adalah untuk pertukaran informasi dan untuk mencari informasi [9]. [10] Jaringan komputer adalah suatu sistem yang terdiri dari dari beberapa komputer yang dirancang

untuk pertukaran data, informasi dan sumber daya. [11] Jaringan komputer adalah suatu sistem yang terdiri dari beberapa komputer yang dirancang untuk pertukaran data, informasi dan sumber daya. Tujuan dari jaringan komputer adalah Setiap bagian dari jaringan komputer dapat meminta dan menyediakan layanan informasi dan data. [12] Pihak yang meminta atau menerima layanan kepada siapa pelanggan merujuk dan siapa yang mengirim atau menyampaikan layanan disebut *server* [13].

Serangan siber seperti serangan *malware* atau upaya peretasan merupakan ancaman serius bagi jaringan TI [14]. Dengan memantau lalu lintas jaringan dan menerapkan tindakan pencegahan yang tepat, departemen TI dapat mengidentifikasi serangan yang sedang berlangsung dan mengambil tindakan untuk menghentikannya sebelum menjadi sangat merusak bagi Perusahaan [15]. Pada pasal 30 ayat 1 UU ITE No 19 Tahun 2016, Perbuatan ini dapat dikategorikan yang dinyatakan dalam Pasal 30 ayat (1) UU ITE yaitu setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau system elektronik milik orang lain dengan cara apapun.

Tujuan dari keamanan jaringan adalah untuk mengantisipasi resiko ancaman jaringan yang dapat mengganggu operasional jaringan komputer sehari-hari [16]. Nirkabel diperlukan di kantor Karena nirkabel dapat membantu menyelesaikan pekerjaan. Perkembangan teknologi *Wireless Fidelity (WI-FI)* mengalami kemajuan yang sangat pesat untuk memenuhi kebutuhan sistem. [17] Teknologi *WI-FI* banyak

digunakan pada *hotspot* komersial, keamanan jaringan Internet *Service Provider (ISP)* di sekolah dan perkantoran sangat penting, namun hanya sebagian operator jaringan saja yang memperhatikan keamanan lalu lintas data pada jaringan *WI-FI*. Salah satu ancaman keamanan jaringan paling umum yang ditimbulkan oleh penjahat dunia maya adalah serangan paket. *Sniffing* paket adalah bentuk serangan yang menangkap data dari paket yang melintasi jaringan. Informasi ini mungkin termasuk nama pengguna, kata sandi, dan informasi penting lainnya yang dikirimkan melalui jaringan dalam bentuk teks. Tidak hanya satu paket yang harus ditangkap, bisa ratusan bahkan ribuan. Hal ini dapat merugikan pengguna jaringan komputer.

Dalam lingkungan TI yang kompleks, penggunaan ilegal atau aktivitas jaringan yang mencurigakan dapat mengganggu ketersediaan sistem. Dengan menggunakan solusi pemantauan yang tepat, departemen TI dapat mengidentifikasi masalah dan kesalahan jaringan dengan lebih cepat dan mengambil tindakan segera untuk menjaga ketersediaan sistem. Serangan yang berhasil dapat mengakibatkan gangguan pada proses bisnis. Mengontrol dan mencegah penggunaan ilegal dapat meminimalkan risiko kerusakan finansial dan reputasi yang mungkin diakibatkan oleh serangan atau pelanggaran keamanan.

Dalam penelitian ini penulis melakukan penelitian dengan menggunakan metode Action Research yang bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara-cara pendekatan baru dan untuk memecahkan masalah dengan cara penerapan langsung pada objek penelitian.

Sehubungan dengan hal tersebut di atas PT. Pupuk Sriwidjaja Palembang di perlukannya melakukan *monitoring* dan pencegahan dari akses ilegal pada jaringan menggunakan *wireshark*. *Administrator* jaringan dapat mengambil tindakan penanggulangan ketika akses ilegal terdeteksi melalui jaringan komputer akses ilegal yang di maksud adalah seperti pengguna atau user membuka situs atau webstie yang berbahaya dan tingkat keamanannya sangat lemah, Oleh karena itu *administrator* memerlukan alat yang tepat untuk memantau jaringan yaitu *wireshark*, *Software Wireshark* karena alat ini mampu menangkap paket data atau informasi dan sekaligus memantau lalu lintas antara Wlan (*Wireless Local area Network*).

## 2. TINJAUAN PUSTAKA

### 2.1 Monitoring

Monitoring merupakan aktivitas mengumpulkan dan menganalisis data berdasarkan faktor yang ditetapkan secara teratur kemudian dilanjutkan pada aktivitas program sehingga bisa melakukan tindakan koreksi untuk menyempurnakan aktivitas program tersebut [18].

### 2.2 Analisis

Analisis adalah kegiatan untuk mencari pola, atau cara berpikir yang berkaitan dengan pengujian secara sistematis terhadap sesuatu untuk menentukan bagian, hubungan antar bagian, serta hubungannya dengan keseluruhan.

### 2.3 Pencegahan

Menurut Kamus Besar Bahasa Indonesia (KBBI), kata mencegah /mencegah dapat didefinisikan sebagai berikut.

- 1) Mengkhintarkan supaya jangan terjadi
- 2) Merintang; melarang
- 3) Menahan agar sesuatu tidak terjadi; menegahkan; tidak menurutkan

### 2.4 Wireless

Wireless atau yang dikenal dengan jaringan nirkabel wireless atau wireless Network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Teknologi wireless adalah salah satu pilihan yang tepat untuk menggantikan teknologi jaringan yang terdiri dari banyak kabel dan merupakan sebuah solusi akibat jarak antar jaringan yang tidak mungkin dihubungkan melalui kabel. Keuntungan terbesar dari wireless yaitu sangat praktis, dimana komputer dapat terhubung ke jaringan tanpa membutuhkan kabel.

### 2.5 Web Traffic

Traffic pada website merupakan jumlah orang yang mengunjungi website, membuka halaman website, dan durasi saat pengunjung membuka dan membaca halaman pada website kamu. Jadi, saat seseorang mengunjungi website kamu, kunjungan serta semua link yang mereka klik dan follow akan direkam oleh domain kamu. Nantinya angka-angka akan memberi ide tentang seberapa populernya website kamu.

### 2.6 Cyber Crime

Cyber Crime merupakan aktivitas individu maupun kelompok yang menggunakan jaringan komputer sebagai media untuk melakukan tindakan kriminal, atau menjadikan komputer sebagai sasaran kejahatan

### 2.7 Jaringan Komputer

Jaringan Komputer merupakan hubungan dengan beberapa perangkat yang bisa saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup komputer desktop, samrthphone, tablet, router, switch, dan hub

### 2.8 Keamanan Jaringan

Jaringan Komputer merupakan hubungan dengan beberapa perangkat yang bisa saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup komputer desktop, samrthphone, tablet, router, switch, dan hub.

### 2.9 Wireshark

Wireshark merupakan tool yang ditunjukan untuk menganalisa paket data jaringan, Wireshark juga disebut Network Packet Analyzer yang memilki fungsi untuk menangkap paket data dalam jaringan dan berusaha memperlihatkan informasi dipaket tersebut secara rinci.

### 2.10 Perangkat

#### a. Router

Router merupakan salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau internet menuju sasaran, melalui sebuah proses yang di kenal

sebagai routing, Router berfungsi sebagai penghubung antar 2 (dua) atau lebih jaringan untuk meneruskan dari satu jaringan ke jaringan lainnya

b. Proxy

Proxy adalah sistem yang menengahi pengguna dan internet untuk menyembunyikan identitas asli pengguna, sehingga data yang dikirim ke website tujuan akan menggunakan alamat IP dari proxy server, bukan alamat IP pengguna.

c. Hub

Hub adalah perangkat jaringan yang memungkinkan Anda menghubungkan beberapa PC kesatu jaringan. Perangkat ini digunakan untuk menghubungkan segmen LAN. Sebuah hub memiliki berbagai macam port, jadi ketika sebuah paket tiba di satu port, itu disalin ke berbagai port lainnya.

d. Switch

switch adalah sebuah komponen jaringan yang tugasnya untuk menghubungkan beberapa perangkat, untuk bisa melakukan pertukaran paket data, baik dalam proses penerimaan, serta meneruskan data keperangkat lain

e. Kabel UTP

UTP merupakan singkatan dari Unshield Twisted Pair. Sesuai namanya “Unshield”, yang berarti kabel ini tidak dilengkapi dengan pelindung aluminium sehingga kabel ini kurang tahan dengan interferensi elektromagnetik, berbeda dengan saudaranya STP (Shield Twisted Pair).

f. Kabel Fiber Optic

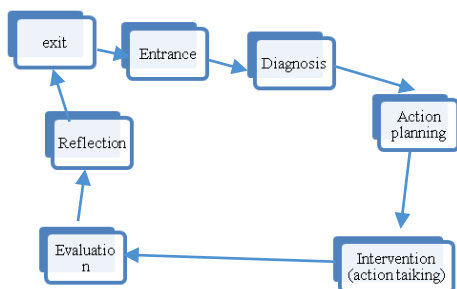
Fiber Optik adalah saluran transmisi atau sejenis kabel yang terbuat dari kaca atau plastik yang sangat halus dan lebih kecil dari sehelai rambut, dan dapat digunakan untuk mentransmisikan sinyal cahaya dari suatu tempat ketempat lain. Sumber cahaya yang digunakan biasanya adalah laser atau LED.

g. Kabel Coaxial

Kabel coaxial merupakan kabel yang mempunyai 2 konduktor yakni copper pada bagian tengahnya atau pusat inti yang terbuat dari tembaga bertekstur keras dan dilapisi dengan isolator. Sementara konduktor kedua adalah yang melingkar pada bagian luar isolator pertama serta tertutup dengan insulator luar.

3. METODOLOGI

Dalam penelitian ini penulis menggunakan metode *Action Research*



Metode *Action Research* ini di bertujuan untuk pengujian dan pengembangan, menemukan dan merancang[19], langkah-langkah ini diterapkan di tempat kerja (Objek), Dengan menggunakan metode ini pekerjaan akan menjadi lebih muda, lebih cepat dan hasilnya lebih baik dan lebih berkualitas.

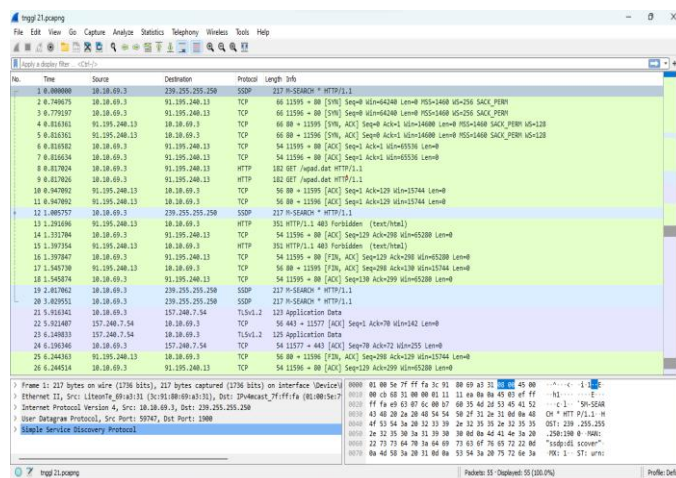
2.11 Diagnose (Diagnosis)

Setelah melaksanakan magang di PT Pupuk Sriwidjaja Palembang, Peneliti Melakukan diagnosis setelah melihat beberapa karyawan mencoba masuk ke situs web yang mungkin belum memiliki standar keamanan, sehingga informasi pribadi seperti *Pasword* atau *email* dapat di kenali, Jika informasi penting seperti alamat email pengguna internet dapat di dideteksi meskipun email tersebut di tautkan kebanyak akun lain, ini dapat lebih berbahaya bagi pengguna internet dan memungkinkan orang lain untuk menyalahgunakan.

4. HASIL DAN PEMBAHASAN

4.1 Filtering Protokol HTTP

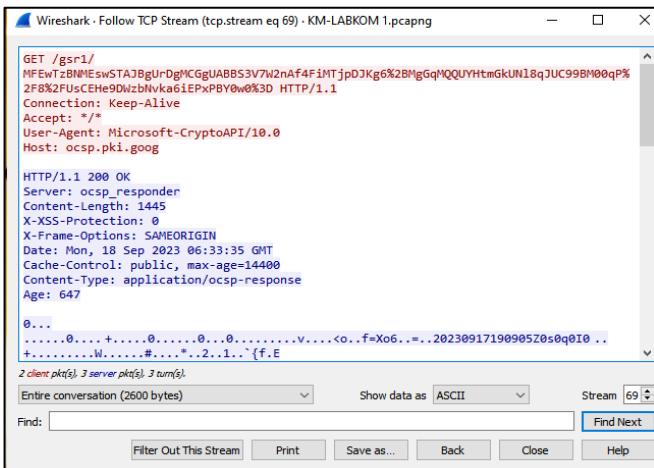
Disini penulis akan melakukan filtering paket data yang melewati protokol http pada beberapa jaringan yang ada di PT.Pupuk Sriwidjaja Palembang, selanjutnya ketikkan http pada kolom address filter.



Gambar 2. Filtering Protocol http

Bisa di analisis user-agent yang di pakai pada jaringan Pusri.id New menggunakan Mozilla/5.0 (windows NT 10.0; WIN 64; x64)AppleWebKit/537.36 (KHTML, Like gecko) Chrome/115.0.0.0 Safari /537/36 Dan Host mysql - phi - intergration.com, Selain itu dapat di ketahui date yaitu 22 juni 2023 01:32 41 GMT DAN Full Request Get Uri Http, Disini bisa di lihat bahwa adanya aktivitas yang sedang mengakses laman web Gambar Capture TCP Stream Wireshark dibahwa ini dapat melihat info get yang sedang di buka

4.2 TCP Streaming



Gambar 3. TCP Stream

Tabel 1. Website yang di akses pengguna pada jaringan PT.Pusri

NO	Website Yang Di Akses	Jenis Brwoser
1	http://mysql-phi-integration	Google Mozila
2	Blog.spot.com	Google Mozila
3	<a href="http://www.msftconnecttest.com">www.msftconnecttest.com</a> ,	Google Mozila
4	ocsp.pki.goog	Google Mozila

TIME	SOURCE	DESTINATION	PROTOCOL
0.069188	10.10.69.3	91.195.240.13	HTTP
650.037090	103.121.18.2 02	192.168.11.17	HTTP
86.281421	10.10.70.97	142.251.12.94	HTTP
72.863219	10.10.69.3	204.79.197.203	HTTP

Tabel 2.data ip akses protocol http

## 5. KESIMPULAN DAN SARAN

Jaringan pada departemen TI PT. Pupuk Srwidjaja Palembang sudah cukup aman di karenakan pada saat di lakukannya monitoring jaringan selama 10 hari pada tanggal 6 juni 2023 sampai dengan 22 juni 2023 tidak ada terjadinya akses illegal. Wireshark memiliki keunggulan pada bagian sniffing di bandingkan software monitoring lainnya dan wireshark juga dapat membaca hasil capture dari software monitoring lainnya. Wireshark adalah sebuah perangkat lunak yang dapat melakukan Monitoring traffic jaringan sekaligus sniffing , Namun tidak berlaku untuk semua website di karenakan beberapa website sudah terenkripsi dengan baik.

Meskipun wireshark dapat melakukan sniffing, alangkah baiknya jika di gunakan untuk kepentingan yang baik atau positif seperti dengan mengetahui kekurangan dari suatu keamanan tertentu dapat lebih di tingkatkan lagi keamanan jaringannya. Untuk menghindari sniffing dapat menggunakan keamanan firewall yang dapat menutup traffic yang datang baik incoming network traffic maupun out going network traffic berdasarkan sumber atau tujuan traffic tersebut. Selain itu dapat menggunakan protocol yang memiliki standar aman yang sudah di lengkapi dengan enkripsi data seperti IPSec, HTTPS, SMB Signing, dan sebagainya.

## UCAPAN TERIMA KASIH

Terimakasih kepada PT.Pupuk Sriwidjaja Palembang dan Universitas Bina darma yang telah mendukung keterlaksanaannya penelitian ini serta pihak Jurnal Informatika Universitas Putra Batam.

## DAFTAR PUSTAKA

- [1] H. Hasriadi, "Metode Pembelajaran Inovatif di Era Digitalisasi," *Jurnal Sinestesia*, vol. 12, no. 1, Art. no. 1, Jun. 2022.
- [2] B. S. Permana, L. A. Hazizah, and Y. T. Herlambang, "Teknologi Pendidikan: Efektivitas Penggunaan Media Pembelajaran Berbasis Teknologi Di Era Digitalisasi," *Khatulistiwa: Jurnal Pendidikan dan Sosial Humaniora*, vol. 4, no. 1, pp. 19–28, Jan. 2024, doi: 10.55606/khatulistiwa.v4i1.2702.
- [3] D. Wiriany, S. Natasha, and R. Kurniawan, "Perkembangan Teknologi Informasi dan Komunikasi terhadap Perubahan Sistem Komunikasi Indonesia," *jnk*, vol. 8, no. 2, pp. 242–252, Nov. 2022, doi: 10.26905/nomosleca.v8i2.8821.
- [4] T. Ariyadi, M. Fikri, I. Irwansyah, and H. Yudiastuti, "PENERAPAN MONITORING JARINGAN DENGAN ZABBIX PADA PT. PLN (PERSERO) UIP BAGIAN SUMBAGSEL," *JURNAL ILMIAH INFORMATIKA*, vol. 12, no. 02, Art. no. 02, Sep. 2024, doi: 10.33884/jif.v12i02.9283.
- [5] R. Raihana, S. S. Jagat, and R. Perdana, "Pengaruh Perkembangan Teknologi Terhadap Kemajuan Hukum Di Indonesia," *Jurnal Pendidikan dan Konseling (JPDK)*, vol. 5, no. 2, pp. 5628–5633, Apr. 2023, doi: 10.31004/jpdk.v5i2.14551.
- [6] M. Husaini, "PEMANFAATAN TEKNOLOGI INFORMASI DALAM BIDANG PENDIDIKAN (E-education)," *MIKROTIK: Jurnal Manajemen Informatika*, vol. 2, no. 1, Art. no. 1, Mar. 2017, Accessed: Feb. 14, 2025. [Online]. Available: <https://ojs.umm metro.ac.id/index.php/mikrotik/article/view/314>
- [7] S. Syahputra and C. E. Gunawan, "Perancangan Database Aplikasi Tabungan Sampah PT Pusri Palembang," *SEMESTER: Seminar Nasional Teknologi Informasi & Ilmu Komputer*, vol. 2, no. 1, pp. 336–348, Dec. 2023, doi: 10.31849/semester.v2i1.18648.
- [8] E. Fauzi, M. V. Sinatrya, N. D. Ramdhani, R. Ramadhan, and Z. M. R. Safari, "Pengaruh kemajuan teknologi informasi terhadap perkembangan akuntansi," *Jurnal Riset*

*Pendidikan Ekonomi*, vol. 7, no. 2, Art. no. 2, Oct. 2022, doi: 10.21067/jrpe.v7i2.6877.

- [9] T. Ariyadi and M. R. Pohan, "Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators," *Jurnal Penelitian Pendidikan IPA*, vol. 9, no. 12, Art. no. 12, Dec. 2023, doi: 10.29303/jppipa.v9i12.5551.
- [10] T. Ariyadi, T. D. Purwanto, and M. M. Fajar, "IMPLEMENTASI DESAIN JARINGAN HOTSPOT BERBASIS MIKROTIK DENGAN METODE NDLC (NETWORK DEVELOPMENT LIFE CYCLE) PADA PT KIRANA PERMATA," *JURNAL ILMIAH INFORMATIKA*, vol. 11, no. 02, Art. no. 02, Sep. 2023, doi: 10.33884/jif.v11i02.8032.
- [11] W. Maula and T. Ariyadi, "PERANCANGAN TOPOLOGI JARINGAN BERBASIS OSPF DI SMA N 4 METRO LAMPUNG MENGGUNAKAN CISCO PACKET TRACER," *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. 3, no. 4, Art. no. 4, Nov. 2024, doi: 10.55123/storage.v3i4.4486.
- [12] F. A. Hasibuan and Subhiyanto, "Jaringan Komputer Berbasis Radius Server untuk Meningkatkan Pemanfaatan Internet di Madrasah Aliyah Al-Azhaar Ummu Suwanah," *Jurnal Teknik Informatika*, vol. 7, no. 1, Art. no. 1, Feb. 2021, doi: 10.51998/jti.v7i1.349.
- [13] Y. R. Adi, O. D. Nurhayati, and E. D. Widiyanto, "Perancangan Sistem Cluster Server untuk Jaminan Ketersediaan Layanan Tinggi pada Lingkungan Virtual," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 5, no. 2, Art. no. 2, 2016.
- [14] T. G. Laksana and S. Mulyani, "PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN," *Jurnal Ilmiah Multidisiplin*, vol. 3, no. 01, pp. 109–122, Jan. 2024, doi: 10.56127/jukim.v3i01.1143.
- [15] A. Oktaviani and E. Rusdiana, "ALTERNATIF PIDANA BAGI PELAKU TINDAK PIDANA PERETASAN DI INDONESIA DALAM UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK," *NOVUM: JURNAL HUKUM*, pp. 249–264, Jan. 2023, doi: 10.2674/novum.v0i0.50394.
- [16] J. A. Amien, "IMPLEMENTASI KEAMANAN JARINGAN DENGAN IPTABLES SEBAGAI FIREWALL MENGGUNAKAN METODE PORT KNOCKING," *JURNAL FASILKOM*, vol. 10, no. 2, Art. no. 2, Aug. 2020, doi: 10.37859/jf.v10i2.2098.
- [17] "Design and Analysis of Light Fidelity Network for Indoor Wireless Connectivity | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 25, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9567691>
- [18] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and Future of Network Security Monitoring," *IEEE Access*, vol. 9, pp. 112744–112760, 2021, doi: 10.1109/ACCESS.2021.3067106.
- [19] T. Ariyadi, I. Irwansyah, and M. S. H. Mubarak, "ANALISIS KEAMANAN JARINGAN WIFI MAHASISWA UBD DARI SERANGAN PACKET SNIFFING," *JURNAL ILMIAH INFORMATIKA*, vol. 12, no. 01, Art. no. 01, Mar. 2024, doi: 10.33884/jif.v12i01.8739.

## BIODATA PENULIS



### Tamsir Ariyadi, M.Kom.

Penulis merupakan dosen pada Program Studi Teknik Komputer Universitas Bina Darma, beberapa publikasi berkaitan tentang *Network Security & Computer Network*.



### M. Alzi Ikrar Agamuri

Penulis merupakan mahasiswa pada Program Studi Teknik Komputer Universitas Bina Darma



### Rahmat Wiratama

Penulis merupakan mahasiswa pada Program Studi Teknik Komputer Universitas Bina Darma



### Dasril Kholid

Penulis merupakan mahasiswa pada Program Studi Teknik Informatika Universitas Bina Darma