Karapan Network Journal

Vol.I, No.I, October 2025
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Monitoring Jaringan Menggunakan Wireshark

Ryan Putra Pratama Agustin [1)*], Hoirul Umam[2)]

[1) 2)]*Universitas Madura, Pamekasan, Indonesia*

[1)] rynputrapratamaa@gmail.com, [2)] irullumam0@gmail.com

Abstrak

Dalam era digital yang semakin terhubung, jaringan komputer menjadi komponen penting bagi pertukaran data dan komunikasi. Namun, kinerja jaringan sering kali terganggu oleh masalah seperti collision domain dan broadcast domain yang tidak tertata dengan baik. Untuk mengatasi hal tersebut, diperlukan perancangan jaringan yang efisien dengan pemanfaatan perangkat seperti switch dan router. Salah satu pendekatan yang umum digunakan dalam jaringan berskala kecil hingga menengah adalah routing statis, yang memungkinkan pengaturan jalur komunikasi secara manual agar lebih terkontrol. Dalam konteks pemantauan dan analisis kinerja jaringan, Wireshark berperan sebagai alat utama yang mampu menangkap serta menampilkan paket data secara detail. Melalui Wireshark, administrator dapat menganalisis parameter penting seperti throughput, delay, jitter, dan packet loss untuk menilai kualitas layanan (Quality of Service/QoS). Selain itu, Wireshark juga membantu dalam proses troubleshooting dengan menelusuri jalur komunikasi dan mendeteksi kesalahan konfigurasi atau gangguan koneksi. Dari sisi keamanan, alat ini berfungsi untuk mengidentifikasi anomali lalu lintas, aktivitas mencurigakan, hingga potensi penyadapan data yang tidak terenkripsi. Berdasarkan studi literatur, Wireshark tidak hanya digunakan sebagai alat analisis kinerja, tetapi juga sebagai sarana verifikasi desain jaringan, seperti memastikan konfigurasi routing statis dan koneksi ke server DNS berjalan sesuai rancangan. Dengan demikian, pemanfaatan Wireshark terbukti sangat efektif dalam mendukung pengelolaan jaringan komputer yang andal, efisien, dan aman.

Kata Kunci**:** *jaringan komputer, pemantauan, routing statis, wireshark, keamanan jaringan*.

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Di era digital saat ini, jaringan komputer merupakan infrastruktur vital yang menopang hampir seluruh aktivitas pertukaran data dan informasi. Dalam perancangan sebuah jaringan yang andal dan efisien, dua konsep fundamental yang harus diperhatikan adalah *collision domain* (domain tabrakan) dan *broadcast domain* (domain siaran). Kegagalan dalam mengelola kedua domain ini dapat menyebabkan kejenuhan jaringan (*network congestion*) dan penurunan kinerja secara signifikan [1], [2]. Penggunaan perangkat *switch* modern secara efektif telah mengatasi masalah *collision domain*. Namun, pada jaringan skala besar yang hanya mengandalkan *switch*, lalu lintas siaran (*broadcast traffic*) yang berlebihan masih menjadi masalah. Untuk mengatasinya, diperlukan perangkat *router* yang berfungsi memisahkan *broadcast domain*. Salah satu konfigurasi yang umum digunakan untuk jaringan yang tidak terlalu kompleks adalah *routing* statis, terutama dalam implementasi yang melibatkan layanan spesifik seperti *Domain Name System* (DNS) [3], [4], [5]. Berkaitan erat dengan diagnostik adalah aspek keamanan. Literatur secara konsisten menyoroti Wireshark sebagai alat "dua sisi". Dari perspektif defensif, Wireshark digunakan untuk menetapkan baseline lalu lintas jaringan yang normal, sehingga administrator dapat mendeteksi anomali yang mengindikasikan adanya intrusi atau aktivitas malware. Wireshark juga digunakan untuk menganalisis jejak digital atau aktivitas ilegal yang terekam dalam jaringan. Di sisi lain, beberapa studi secara eksplisit menggunakan Wireshark untuk mendemonstrasikan kerentanan jaringan, seperti melakukan sniffing (penyadapan) username dan password yang dikirimkan sebagai plaintext (teks biasa) [6], [7], [8].

Merancang topologi jaringan saja tidak cukup. Administrator jaringan memerlukan kemampuan untuk memantau, mengelola, dan merencanakan jaringan secara berkelanjutan [9], [10]. Pemantauan ini krusial untuk melakukan analisis, pemecahan masalah (*troubleshooting*), dan pelaporan kinerja, serta memastikan keamanan dari akses yang tidak sah. Tanpa alat monitoring yang tepat, administrator akan kesulitan mendeteksi anomali atau mengidentifikasi akar penyebab masalah jaringan. yang menyediakan visibilitas granular hingga ke tingkat paket individual. Kemampuan fundamentalnya yang berulang kali dikutip adalah menangkap dan menampilkan seluruh isi paket termasuk header protokol dan payload data secara terperinci Dalam troubleshooting, kemampuan ini sangat transformatif. Seorang administrator tidak lagi terbatas. Dengan Wireshark, mereka dapat secara visual melacak

[*] Ryan

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.I.I.277-285

seluruh "percakapan" jaringan. Mereka dapat melihat secara pasti mengapa koneksi gagal mungkin paket TCP SYN terkirim tetapi tidak pernah menerima SYN-ACK mungkin permintaan DNS tidak pernah dijawab, atau mungkin sebuah perangkat salah mengonfigurasi subnet mask.. Visibilitas mendalam ini, seperti yang ditunjukkan dalam studi, secara drastis mempercepat Mean Time To Resolution (MTTR) untuk berbagai masalah jaringan [1], [11], [12], [13]. Untuk memenuhi kebutuhan analisis mendalam ini, penganalisa paket jaringan (*network packet analyzer*) menjadi alat yang esensial. Wireshark adalah salah satu penganalisa protokol jaringan berbasis *open-source* yang paling populer dan kuat. Wireshark digunakan secara luas untuk pemecahan masalah, analisis, pengembangan protokol komunikasi, dan edukasi. Wireshark memfasilitasi pergeseran fundamental dalam manajemen jaringan dari manajemen reaktif yang bersifat kualitatif, Wireshark bekerja dengan menangkap paket data secara *real-time* yang lewat di antarmuka jaringan dan menampilkannya secara detail untuk dianalisis [14], [15], [16]. pemanfaatan Wireshark untuk monitoring jaringan. Data yang disintesis dari berbagai studi yang relevan menunjukkan bahwa penggunaan Wireshark tidak terbatas pada satu fungsi, melainkan mencakup spektrum yang luas [17], [18], [19], [20].

Berbagai penelitian sebelumnya telah membuktikan kegunaan Wireshark dalam beragam skenario. Banyak studi menggunakannya untuk menganalisis *Quality of Service* (QoS) jaringan, analisis kinerja jaringan secara kuantitatif melalui Quality of Service (QoS), diagnostik jaringan dan pemecahan masalah (troubleshooting) serta forensik keamanan, dan validasi empiris serta verifikasi komparatif terhadap desain jaringan [21], [22], [23], [24], [25]. dengan mengukur parameter vital seperti *throughput* (jumlah data yang berhasil dikirim), *delay* (waktu tunda), *jitter* (variasi waktu tunda), dan *packet loss* (paket yang hilang) [26]. Administrator jaringan secara spesifik menggunakan Wireshark untuk *troubleshooting* guna mendeteksi masalah konektivitas dan menganalisis kinerja jaringan secara keseluruhan. Temuan yang paling dominan dan konsisten di seluruh literatur yang ditinjau adalah pemanfaatan Wireshark sebagai instrumen utama untuk analisis kinerja jaringan secara kuantitatif. tetapi sebagai sumber data mentah untuk kalkulasi kinerja. Secara spesifik, literatur yang ada menunjukkan konvergensi pada empat parameter kunci QoS yang diukur menggunakan Wireshark [3], [27], [28]. Wireshark mungkin mengungkap bahwa masalah video conference yang buruk bukan disebabkan oleh rendahnya throughput, melainkan oleh tingginya jitter presisi ini memungkinkan administrator untuk melakukan optimasi yang tertarget, seperti menerapkan kebijakan QoS pada router, alih-alih melakukan intervensi yang mahal dan tidak perlu seperti meningkatkan bandwidth. Kategori temuan utama kedua peran Wireshark sebagai alat diagnostik yang sangat diperlukan untuk pemecahan masalah dan analisis keamanan [25], [27], [29]. Penelitian ini diharapkan dapat memberikan kontribusi teoretis dan praktis. Secara teoretis, penelitian ini memperluas cakupan studi BI dengan memperkenalkan integrasi pemrosesan bahasa alami berbasis aspek (NLP) sebagai sumber data intelijen bisnis. Secara praktis, penelitian ini menawarkan model konseptual dan implementasi sistem prototipe yang dapat digunakan oleh pelaku industri F&B untuk memantau opini pelanggan di Instagram secara real-time dan mengonversinya menjadi rekomendasi strategis [27], [28]. Selain itu, hasil penelitian ini dapat digunakan sebagai dasar untuk mengembangkan dashboard analitis yang menggabungkan metrik kuantitatif (penjualan, tingkat keterlibatan, pembelian ulang) dengan metrik kualitatif (sentimen terhadap rasa, harga, layanan, kebersihan, dan suasana restoran) [9], [29], [30].

Masalah utama yang ingin diatasi dalam studi ini adalah bagaimana mengintegrasikan hasil analisis sentimen berbasis aspek (ABSA) ke dalam sistem intelijen bisnis (BI) untuk menghasilkan analisis komprehensif terhadap ulasan pelanggan di Instagram. Lebih spesifik lagi, penelitian ini bertujuan untuk menjawab beberapa pertanyaan [31][32], [33], yaitu bagaimana metode ABSA dapat diterapkan secara efektif untuk mengekstrak aspek dan sentimen dari ulasan pelanggan di platform media sosial Instagram, bagaimana hasil ABSA dapat diwakili dan diproses dalam kerangka kerja Business Intelligence (BI) untuk menghasilkan wawasan yang dapat ditindaklanjuti bagi manajemen, serta bagaimana integrasi antara ABSA dan BI dapat mendukung pemetaan pengalaman pelanggan secara holistik di industri Makanan dan Minuman (F&B) [34]. Secara khusus, Wireshark juga terbukti efektif untuk memverifikasi implementasi desain jaringan. Sebuah studi menunjukkan keberhasilan pemantauan jaringan yang dirancang dengan server DNS dan dikonfigurasi menggunakan *routing* statis, di mana Wireshark digunakan untuk menguji koneksi dan memastikan jaringan bekerja dengan baik [30], [31]. Oleh karena itu, makalah ini bertujuan untuk melakukan studi literatur mengenai pemanfaatan Wireshark sebagai alat monitoring utama untuk menganalisis kinerja dan memecahkan masalah pada jaringan komputer, dengan fokus pada implementasi desain yang umum seperti *routing* statis. Literatur memposisikan Wireshark sebagai "mikroskop" [5], [11], [12], [22].

II. TINJAUAN PUSTAKA

Monitoring jaringan adalah sebuah proses fundamental yang bertujuan untuk memantau, mengelola, dan merencanakan penggunaan jaringan komputer beserta komponen di dalamnya. Tujuan utamanya adalah untuk mengawasi keadaan komputer klien dan layanan (services) yang sedang berjalan [5], [11], [21], [32]. Aktivitas ini sangat penting bagi administrator jaringan untuk dapat melakukan analisis, pemecahan masalah (troubleshooting), dan

pelaporan kinerja jaringan, sekaligus berperan vital dalam aspek keamanan untuk mengawasi akses dan mencegah penyalahgunaan sumber daya [3], [23], [33]. Dalam konteks perancangan, penggunaan routing statis terbukti sesuai untuk jaringan yang tidak kompleks karena memudahkan administrator dalam mengelola jaringan. Untuk mengevaluasi kinerja jaringan tersebut, Wireshark dikenal sebagai penganalisa paket (packet analyzer) yang memungkinkan administrator mengumpulkan dan menganalisis data jaringan secara mendalam [4], [28], [34]. Sejumlah besar penelitian memanfaatkan Wireshark untuk menganalisis Quality of Service (QoS) sebuah jaringan. Parameter utama QoS yang sering diukur meliputi throughput (jumlah data yang berhasil dikirim), delay atau waktu tunda, jitter (variasi waktu tunda), dan packet loss (paket yang hilang). Parameter tersebut adalah throughput, yang merepresentasikan laju transfer data bersih yang berhasil terkirim [7], [13], [21], [28].

Studi-studi ini menggunakan Wireshark untuk mengidentifikasi masalah kinerja, menyelidiki gangguan konektivitas, dan memberikan rekomendasi optimasi jaringan [35], [36], [37]. Selain analisis QoS, Wireshark secara spesifik digunakan sebagai alat bantu utama untuk troubleshooting [6], [36]. Kemampuannya menangkap dan menampilkan semua informasi paket secara detail memungkinkan administrator melakukan debug protokol. Dari sisi keamanan, Wireshark juga digunakan untuk mendeteksi anomali lalu lintas, menganalisis aktivitas ilegal, atau menganalisis celah keamanan melalui sniffing [2], [21], [24], [38], [39]. Secara khusus, Wireshark terbukti efektif dalam memverifikasi dan menganalisis implementasi protokol routing. Sebuah penelitian yang relevan secara spesifik merancang jaringan komputer dengan server DNS dan routing statis [30], [31], [40]. Dalam penelitian tersebut, Wireshark digunakan sebagai penganalisa untuk memantau jaringan dan menguji konektivitas, yang hasilnya menunjukkan bahwa jaringan dan server DNS dapat bekerja dengan baik. Penelitian lain juga menggunakan Wireshark untuk membandingkan kinerja antar protokol routing, seperti membandingkan performa routing statis dengan routing dinamis OSPF, serta menganalisis perbandingan penerapan routing statis pada IPv4 dan IPv6 [4], [41], [42], [43].

III. METODE

Penelitian ini menggunakan metode Studi Literatur (Literature Review) atau Makalah Survei (Survey Paper). Fokus utama dari metodologi ini adalah untuk mengumpulkan, menganalisis, dan mensintesis temuan-temuan dari penelitian yang sudah ada sebelumnya mengenai topik terkait [1], [13], [29], [44]. Pendekatan ini tidak melibatkan eksperimen atau pengumpulan data primer baru, melainkan sepenuhnya bergantung pada analisis data sekunder yang berasal dari publikasi ilmiah yang relevan [10], [22], [45]. Proses penelitian dimulai dengan tahap pengumpulan literatur secara sistematis dari berbagai basis data akademik, seperti Google Scholar, IEEE Xplore, dan portal jurnal nasional. Pencarian dilakukan menggunakan kata kunci yang spesifik, meliputi "Monitoring Jaringan", "Wireshark", "Analisis Kinerja Jaringan", "Quality of Service", dan "Routing Statis" [6], [7], [46], [47].

Seluruh literatur yang terkumpul kemudian disaring secara ketat melalui kriteria inklusi dan eksklusi [8], [48]. Kriteria inklusi yang digunakan adalah makalah yang secara spesifik membahas implementasi Wireshark untuk monitoring, analisis parameter QoS (seperti throughput, delay, packet loss), atau studi kasus troubleshooting jaringan. Sementara itu, kriteria eksklusi digunakan untuk menyisihkan artikel yang hanya bersifat tutorial dasar penggunaan Wireshark atau yang tidak memiliki relevansi ilmiah [25], [49], [50], [51]. Makalah yang lolos seleksi kemudian dianalisis secara kualitatif. Temuan-temuan utama dari setiap studi diekstraksi, dikelompokkan berdasarkan tema yang relevan (seperti analisis Kinerja/QoS, troubleshooting, dan verifikasi desain jaringan), dan disintesis untuk memberikan gambaran komprehensif dalam penelitian ini [3], [11], [12], [52], [53].

I. HASIL

Berdasarkan tinjauan literatur sistematis yang telah dilakukan, bagian ini menyajikan temuan-temuan utama (Hasil) dan menguraikan implikasinya (Pembahasan) mengenai pemanfaatan Wireshark untuk monitoring jaringan. Data yang disintesis dari berbagai studi yang relevan menunjukkan bahwa penggunaan Wireshark tidak terbatas pada satu fungsi, melainkan mencakup spektrum yang luas. Temuan-temuan ini secara konsisten dapat dikelompokkan menjadi tiga kategori primer: analisis kinerja jaringan secara kuantitatif melalui Quality of Service (QoS), diagnostik jaringan dan pemecahan masalah (troubleshooting) serta forensik keamanan, dan validasi empiris serta verifikasi komparatif terhadap desain jaringan.

Kategori Pemanfaatan	**Deskripsi Singkat**	**Contoh analisis / kasus**
Analisis Kinerja Kuantitatif (QoS)	Mengukur parameter vital jaringan untuk manajemen proaktif berbasis data	Mengukur *throughput* (laju data) , *delay* (waktu tunda) , *jitter* (variasi tunda) , dan *packet loss* (paket hilang).

Diagnostik, Troubleshooting, & Keamanan	Berfungsi sebagai "mikroskop" jaringan untuk visibilitas granular dan mendeteksi anomaly.	Mempercepat *Mean Time To Resolution* (MTTR). Mendeteksi *sniffing* (penyadapan) *plaintext*
Validasi Desain & Analisis Komparatif	Menjadi jembatan antara desain teoretis dan implementasi dunia nyata.	Memverifikasi konfigurasi routing statis dan server DNS. Membandingkan kinerja (misal: Statis vs OSPF, IPv4 vs IPv6).

Tabel 1. Kategori Utama Pemanfaatan Wireshark dalam Monitoring Jaringan

Temuan yang paling dominan dan konsisten di seluruh literatur yang ditinjau adalah pemanfaatan Wireshark sebagai instrumen utama untuk analisis kinerja jaringan secara kuantitatif. Studi-studi ini menggunakan Wireshark bukan hanya sebagai alat penangkap paket, tetapi sebagai sumber data mentah untuk kalkulasi kinerja. Secara spesifik, literatur yang ada menunjukkan konvergensi pada empat parameter kunci QoS yang diukur menggunakan Wireshark. Parameter tersebut adalah throughput, yang merepresentasikan laju transfer data bersih yang berhasil terkirim; delay (atau latensi), yang mengukur waktu tempuh paket dari sumber ke tujuan; jitter, yang didefinisikan sebagai variasi statistik dalam delay antar paket; dan packet loss, yang menghitung persentase paket yang gagal mencapai tujuan. Signifikansi dari temuan ini adalah bahwa Wireshark memfasilitasi pergeseran fundamental dalam manajemen jaringan dari manajemen reaktif yang bersifat kualitatif ("jaringan terasa lambat") menjadi manajemen proaktif yang bersifat kuantitatif dan berbasis data. Kemampuan untuk mengisolasi parameter spesifik sangat krusial. Sebagai contoh, analisis Wireshark mungkin mengungkap bahwa masalah video conference yang buruk bukan disebabkan oleh rendahnya throughput, melainkan oleh tingginya jitter. Diagnosis presisi ini memungkinkan administrator untuk melakukan optimasi yang tertarget, seperti menerapkan kebijakan QoS pada router, alih-alih melakukan intervensi yang mahal dan tidak perlu seperti meningkatkan bandwidth.

Kategori temuan utama kedua adalah peran Wireshark sebagai alat diagnostik yang sangat diperlukan (indispensable) untuk pemecahan masalah (troubleshooting) dan analisis keamanan. Literatur memposisikan Wireshark sebagai "mikroskop" bagi administrator jaringan, yang menyediakan visibilitas granular hingga ke tingkat paket individual. Kemampuan fundamentalnya yang berulang kali dikutip adalah menangkap dan menampilkan seluruh isi paket termasuk header protokol dan payload data secara terperinci. Dalam konteks troubleshooting, kemampuan ini sangat transformatif. Seorang administrator tidak lagi terbatas pada output perintah 'ping' yang hanya menyatakan "request timed out". Dengan Wireshark, mereka dapat secara visual melacak seluruh "percakapan" jaringan. Mereka dapat melihat secara pasti mengapa koneksi gagal: mungkin paket TCP SYN terkirim tetapi tidak pernah menerima SYN-ACK; mungkin permintaan DNS tidak pernah dijawab; atau mungkin sebuah perangkat salah mengonfigurasi subnet mask-nya dan mengirim paket ke gateway yang salah. Visibilitas mendalam ini, seperti yang ditunjukkan dalam studi, secara drastis mempercepat Mean Time To Resolution (MTTR) untuk berbagai masalah jaringan. Berkaitan erat dengan diagnostik adalah aspek keamanan. Literatur secara konsisten menyoroti Wireshark sebagai alat "dua sisi" (dual-use). Dari perspektif defensif (pertahanan), Wireshark digunakan untuk menetapkan baseline lalu lintas jaringan yang normal, sehingga administrator dapat mendeteksi anomali yang mengindikasikan adanya intrusi atau aktivitas malware. Wireshark juga digunakan untuk menganalisis jejak digital atau aktivitas ilegal yang terekam dalam jaringan. Implikasi dari sifat "dua sisi" ini sangat mendalam. Di satu sisi, Wireshark adalah alat vital bagi administrator untuk mengamankan jaringan. Di sisi lain, beberapa studi secara eksplisit menggunakan Wireshark untuk mendemonstrasikan kerentanan jaringan, seperti melakukan sniffing (penyadapan) username dan password yang dikirimkan sebagai plaintext (teks biasa). Diskusi dalam literatur ini menggarisbawahi fakta bahwa keamanan jaringan tidak dapat bergantung pada "keamanan melalui ketidakjelasan" (security through obscurity). Sebaliknya, temuan ini memperkuat argumen bahwa enkripsi end-to-end (seperti HTTPS, SSL/TLS, dan SSH) adalah sebuah keharusan absolut di jaringan modern, karena Wireshark dapat dengan mudah mengungkap data apa pun yang tidak terenkripsi.

Temuan signifikan ketiga, yang sangat relevan dengan fokus abstrak penelitian ini, adalah aplikasi Wireshark untuk validasi empiris dari desain jaringan yang telah diimplementasikan. Sebuah studi kunci dalam literatur ini secara spesifik mendemonstrasikan proses perancangan jaringan yang melibatkan server DNS dan konfigurasi routing statis. Dalam studi tersebut, Wireshark digunakan sebagai alat verifikasi pasca-implementasi. Hasil pemantauan paketnya berhasil mengkonfirmasi bahwa kueri DNS diselesaikan dengan benar dan lalu lintas data secara akurat mengikuti jalur yang telah ditentukan oleh tabel routing statis. Temuan ini memiliki implikasi praktis yang penting. Dalam pendidikan dan praktik rekayasa jaringan, merancang topologi hanyalah langkah pertama. Literatur menunjukkan bahwa Wireshark berfungsi sebagai jembatan krusial antara desain teoretis dan implementasi dunia nyata. Wireshark menjawab pertanyaan fundamental: "Apakah jaringan ini berperilaku di dunia nyata persis seperti yang saya rancang

di atas kertas?" Dalam konteks routing statis, verifikasi ini sangat penting. Seorang administrator dapat salah mengkonfigurasi next-hop atau subnet mask dalam routing table, yang berpotensi menciptakan routing loop atau "lubang hitam" (black hole). Wireshark adalah satu-satunya alat yang dapat mengungkap anomali tersebut dengan memvisualisasikan jalur paket yang sebenarnya. Melanjutkan tema verifikasi, literatur juga mengungkap penggunaan Wireshark sebagai alat benchmarking (tolok ukur) standar untuk analisis komparatif. Peneliti tidak hanya memvalidasi satu desain, tetapi secara aktif membandingkan dua atau lebih desain untuk menentukan secara objektif mana yang memiliki kinerja superior dalam kondisi tertentu. Contoh yang ditemukan termasuk studi yang membandingkan kinerja routing statis dengan protokol routing dinamis seperti OSPF. Penggunaan Wireshark dalam analisis komparatif ini sangat vital untuk kemajuan ilmu jaringan. Hal ini memungkinkan bidang ini untuk beralih dari klaim teoretis ke pembuktian empiris. Sebagai contoh, sebuah studi yang membandingkan implementasi routing statis pada jaringan IPv4 versus jaringan IPv6 menggunakan Wireshark untuk mengukur secara presisi perbedaan throughput dan delay antara kedua protokol tersebut. Temuan semacam ini memberikan landasan data yang objektif bagi para insinyur jaringan untuk membuat keputusan penting dalam perancangan, seperti protokol mana yang harus dipilih saat melakukan migrasi atau peningkatan infrastruktur jaringan.

II. PEMBAHASAN

Studi literatur ini menegaskan bahwa Wireshark berfungsi jauh melampaui sekadar alat penangkap paket; ia merupakan instrumen analisis jaringan multifaset dengan aplikasi yang luas. Data yang disintesis dari berbagai studi yang relevan secara konsisten menunjukkan bahwa pemanfaatannya dapat dikategorikan ke dalam tiga ranah utama: analisis kinerja jaringan kuantitatif melalui Quality of Service (QoS), diagnostik jaringan dan pemecahan masalah (troubleshooting) serta forensik keamanan, dan validasi empiris serta verifikasi komparatif terhadap desain jaringan. Temuan-temuan ini menggarisbawahi peran transformatif Wireshark dalam manajemen jaringan modern. Dalam ranah analisis kinerja, Wireshark menjadi fondasi untuk mengukur Quality of Service (QoS) secara objektif. Banyak studi memanfaatkannya sebagai sumber data mentah untuk kalkulasi parameter vital seperti throughput, delay, jitter, dan packet loss. Signifikansinya terletak pada fasilitasi pergeseran fundamental dalam manajemen jaringan dari pendekatan reaktif kualitatif ("jaringan terasa lambat") menjadi manajemen proaktif kuantitatif berbasis data. Kemampuan mengisolasi parameter spesifik misalnya, membedakan antara masalah throughput rendah dan jitter tinggi pada konferensi video memungkinkan diagnosis presisi. Hal ini mengarah pada optimasi yang tertarget, seperti implementasi kebijakan QoS pada router, yang seringkali lebih efektif dan efisien daripada intervensi mahal seperti sekadar meningkatkan bandwidth. Kategori kedua menyoroti peran Wireshark sebagai alat diagnostik yang sangat diperlukan (indispensable) untuk pemecahan masalah (troubleshooting) dan analisis keamanan. Literatur sering menganalogikannya sebagai "mikroskop" jaringan, karena menyediakan visibilitas granular hingga ke tingkat paket individual, menampilkan header dan payload secara terperinci. Dalam troubleshooting, ini sangat transformatif; administrator dapat melacak seluruh "percakapan" jaringan untuk melihat mengapa koneksi gagal (misalnya, SYN terkirim tanpa SYN-ACK, DNS tidak merespons, routing salah), jauh melampaui output ping yang terbatas. Visibilitas mendalam ini terbukti mempercepat Mean Time To Resolution (MTTR). Terkait erat adalah aspek keamanan, di mana Wireshark berfungsi sebagai alat "dua sisi" (dual-use). Secara defensif, ia membantu menetapkan baseline lalu lintas normal untuk mendeteksi anomali (intrusi, malware) dan menganalisis jejak digital aktivitas ilegal. Namun, ia juga digunakan untuk mendemonstrasikan kerentanan, seperti menyadap (sniffing) kredensial plaintext pada HTTP, yang menggarisbawahi keharusan enkripsi end-to-end (seperti HTTPS) di jaringan modern.

Terakhir, Wireshark terbukti krusial untuk validasi empiris dan verifikasi komparatif desain jaringan. Studi kunci menunjukkan penggunaannya sebagai alat verifikasi pasca-implementasi, misalnya, untuk memastikan resolusi DNS berjalan benar dan lalu lintas mengikuti jalur routing statis yang dirancang. Wireshark berfungsi sebagai jembatan antara desain teoretis dan implementasi dunia nyata, menjawab pertanyaan "Apakah jaringan ini berperilaku sesuai rancangan?". Verifikasi ini sangat penting, terutama untuk konfigurasi manual seperti routing statis, di mana kesalahan konfigurasi (next-hop atau subnet mask) dapat menyebabkan routing loop atau black hole, anomali yang sulit dideteksi tanpa visualisasi jalur paket aktual oleh Wireshark. Selain validasi tunggal, Wireshark juga menjadi alat benchmarking standar untuk analisis komparatif, memungkinkan peneliti membandingkan kinerja antar desain (misalnya, routing statis vs. OSPF) secara objektif dan mendorong pergeseran dari klaim teoretis ke pembuktian empiris dalam ilmu jaringan.

III. KESIMPULAN

Studi literatur ini menegaskan bahwa Wireshark berfungsi jauh melampaui perannya sebagai alat penangkap paket; ia merupakan instrumen analisis jaringan multifaset yang esensial dan transformatif dalam manajemen jaringan modern. Kontribusi utama dari penelitian ini adalah sintesis dan kategorisasi pemanfaatan Wireshark yang konsisten di seluruh literatur relevan, yang menunjukkan bahwa penggunaannya dapat dikelompokkan ke dalam tiga ranah primer. Pertama, ia menjadi fondasi untuk analisis kinerja kuantitatif (QoS) dengan mengukur parameter vital seperti throughput, delay, jitter, dan packet loss , yang memungkinkan administrator beralih dari manajemen reaktif ke proaktif berbasis data. Kedua, Wireshark adalah alat diagnostik dan troubleshooting yang sangat diperlukan, menyediakan visibilitas granular hingga tingkat paket untuk mempercepat Mean Time To Resolution (MTTR). Sebagai alat "dua sisi", ia vital untuk pertahanan (mendeteksi anomali) sekaligus esensial untuk mendemonstrasikan kerentanan (seperti sniffing plaintext), yang menggarisbawahi keharusan enkripsi end-to-end. Ketiga, ia berfungsi sebagai jembatan krusial antara desain teoretis dan implementasi dunia nyata, digunakan untuk memvalidasi secara empiris bahwa konfigurasi, seperti routing statis dan server DNS, beroperasi sesuai rancangan dan untuk melakukan analisis komparatif antar desain jaringan. Keterbatasan utama penelitian ini adalah metodologinya sebagai studi literatur yang bergantung pada data sekunder. Untuk penelitian selanjutnya, disarankan beralih ke implementasi eksperimental dan studi kasus di lingkungan nyata untuk mengumpulkan data primer dan memvalidasi temuan-temuan ini secara langsung.

Kontribusi Penulis: [*Ryan*]: Konseptualisasi, Metodologi, Penulisan - Draf Awal, Penulisan - Telaah & Penyuntingan, Supervisi. Ryan merancang konsep dan metodologi penelitian, proses penulisan, serta melakukan penyuntingan dan validasi akhir naskah.
[*Hoirul*]: Perangkat Lunak, Investigasi, Kurasi Data, Penulisan - Draf Awal. Hoirul memverifikasi hasil akurasi data terhadap berbagai sumber jurnal, serta penyusunan draf akhir hasil penelitian.

Semua penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

Pendanaan: -
Ucapan Terima Kasih: -
Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.
Ketersediaan Data: -
Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.
Penulis Pertama: https: -
Penulis Kedua: https: -
Penulis Ketiga: -

REFERENSI

[1] T. A. Tamsir, E. Saputra, and M. T. Farizky, “Analisis Paket Icmp Website Universitas Binadarma Menggunakan Wireshark,” *STORAGE J. Ilm. …*, 2023, doi: DOI: https://doi.org/10.55123/storage.v2i2.1956.
[2] F. P. E. Putra, M. Riski, M. S. Yahya, and ..., “Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G,” *J. Sistim Inf. …*, 2023, doi: DOI: https://doi.org/10.37034/jsisfotek.v5i2.233.
[3] F. Prasetyo, A. B. Tamam, R. W. Efendi, and ..., “Pertahanan Tingkat Server Terhadap Serangan Dns Spoofing Di Jaringan Modern,” *Just It J. Sist. Inf. …*, 2024, doi: DOI: https://doi.org/10.55123/storage.v2i4.2531.
[4] Y. Natalia and T. Sutabri, “Rancangan Sistem Pemantauan Lingkungan Berbasis IoT untuk Pertanian Padi,” *Switch J. Sains dan Teknol. Inf.*, 2024, doi: DOI: https://doi.org/10.62951/switch.v2i6.282.
[5] N. Nendi and F. Maulana, “Monitoring Traffic Berbasis SNMP pada Jaringan Perumahan Permata Puri Harmoni 2,” *J. Sains dan Teknol.*, 2024, doi: DOI: https://doi.org/10.55338/saintek.v5i3.1346.
[6] R. Soepeno, “Wireshark: An Effective Tool for Network Analysis,” *CYBV-Introd. Methods Netw. Anal*, 2023, doi: DOI: 10.13140/RG.2.2.34444.69769.
[7] D. A. Rachman, Y. Muhyidin, and ..., “Analysis Quality of Service of Internet Network Fiber To the Home Service Pt. Xyz Using Wireshark,” *J. Inform. dan …*, 2023, doi: DOI: https://doi.org/10.23960/jitet.v11i3s1.3436.
[8] F. P. E. Putra, M. Irfan, M. Aziz, and ..., “Wireless Network Design at Pamekasan Regency Public Library,” *Brill. Res. …*, 2025, doi: DOI: https://doi.org/10.47709/brilliance.v5i1.5876.

[9] R. A. Octaviyana and B. Soewito, "Perancangan Ulang Topologi Jaringan Dengan Kerangka Kerja Ppdioo," *Teknol. J. Ilm. Sist. ...*, 2023, doi: https://doi.org/10.26594/teknologi.v13i1.3852.

[10] T. Sutiyono, I. Karimah, T. Hidayat, and ..., "Pelatihan Topologi Jaringan pada Sekolah Berbasis Cisco Paket Tracer," *J. Pengabdi. ...*, 2024, doi: DOI: https://doi.org/10.58291/abdisultan.v1i2.203.

[11] D. A. Rachman, Y. Muhyidin, and ..., "Analisis Kualitas Layanan Jaringan Internet Fiber to the Home PT. XYZ Menggunakan Wireshark," *STORAGE J. Ilm. ...*, 2023, doi: DOI: https://doi.org/10.55123/storage.v2i4.2531.

[12] S. M. Khaerullah and D. Mustofa, "Penggunaan Wireshark dalam Penyadapan Lalu Lintas Data Berprotokol HTTP pada Jaringan Wi-Fi," *J. Ilm. IT CIDA*, 2024, doi: DOI: https://doi.org/10.55635/jic.v10i1.203.

[13] A. Yusuf, K. Khairil, and E. P. Rohmawan, "AN ANALYSIS OF SERVICE QUALITY ON VSAT NETWORK USING WIRESHARK," *J. MEDIA INFOTAMA*, 2024, doi: DOI: https://doi.org/10.37676/jmi.v20i1.5338.

[14] F. Jawad, S. Sugiyono, M. Mirsandi, and ..., "Optimalisasi Keamanan dan Monitoring Jaringan Infrastruktur di Kantor DPRD Bekasi," *ARSY J. ...*, 2023, doi: DOI: https://doi.org/10.55583/arsy.v3i2.374.

[15] W. I. Ilahy, M. Ahmad, and B. P. Hartono, "Optimasi Jaringan Distribusi Air di Desa Gombolharjo Menggunakan Algoritma Prim," *J. Math. ...*, 2023, doi: DOI: https://doi.org/10.32665/james.v6i2.1896.

[16] A. Kautsar, A. Yulistia, and M. S. Ritonga, "Penerapan Teknologi Mikrotik Dalam Jaringan Point-To-Point Untuk Meningkatkan Kinerja Infrastruktur Jaringan," *JEKIN-Jurnal Tek. ...*, 2024, doi: DOI: https://doi.org/10.58794/jekin.v4i3.729.

[17] A. P. Sinaga and I. Syahputra, "Optimalisasi Jaringan Wifi (Wireless Fidelity) sebagai Fasilitas Pendukung Akademik Mahasiswa (Studi Kasus di UINSU)," *Cognoscere J. Komun. dan ...*, 2024, doi: DOI: https://doi.org/10.61292/cognoscere.244.

[18] N. M. Nggilu and A. Ahmad, "Optimalisasi Jaringan Dokumentasi Dan Informasi Hukum (JDIH) Dalam Pembentukan Produk Hukum Desa Tabongo Timur," *DAS SEIN J. Pengabdi. Huk. dan ...*, 2023, doi: DOI: https://doi.org/10.33756/jds.v0i0.15535.

[19] N. Asyifah and D. Ramayanti, "Optimasi Kinerja Jaringan Di Smk Al Fudhola Bekasi: Pengaturan Bandwidth Dengan Mikrotik Rb 951ui-2hnd Dan Penerapan Algoritma Simple Queue," *J. Ilm. Ilk. Komput. \& ...*, 2024, doi: DOI: https://doi.org/10.47324/ilkominfo.v7i1.210.

[20] M. Y. Fardiansyah and A. Nugroho, "OPTIMASI JARINGAN INTERNET MENGGUNAKAN KOMBINASI LOAD BALANCING DAN QUEUE PADA ROUTER MIKROTIK," *Elektrika*, 2024, doi: DOI: https://doi.org/10.26623/elektrika.v16i2.10337.

[21] V. Y. P. Ardhana and M. D. Mulyodiputro, "Analisis Quality of Service (QoS) Jaringan Internet Universitas Menggunakan Metode Hierarchical Token Bucket (HTB)," *J. Informatics ...*, 2023, doi: DOI: https://doi.org/10.47065/jimat.v3i2.257.

[22] J. Buttu and S. Suparman, "Analisis Kinerja Jaringan Wlan pada Sekolah Menengah Pertama Negeri 6 Palopo," *BANDWIDTH J. Informatics ...*, 2023, doi: DOI: https://doi.org/10.53769/bandwidth.v1i1.380.

[23] A. S. Wahyusesa, P. W. Hidayanto, and E. A. Ramdayani, "Solusi Cerdas: Meningkatkan Keamanan dan Kinerja Jaringan pada Warnet dengan Mengatasi Kelemahan Sistem," *Dike*, 2023, doi: DOI: https://doi.org/10.69688/dike.v1i2.39.

[24] Y. Sunardhi, A. Ikar, N. Lamhot, and L. Safira, "Analisis Kinerja Jaringan Distribusi LPG: Studi Kasus di Kecamatan Compreng," *Innov. J. Soc. ...*, 2025, doi: DOI: https://doi.org/10.31004/innovative.v5i1.16819.

[25] F. P. E. Putra, K. Mufidah, R. M. Ilhamsyah, and ..., "Tinjauan performa RouterOS Mikrotik dalam jaringan internet: Analisis kinerja dan kelayakan," *Digit. ...*, 2023, doi: DOI: https://doi.org/10.47709/digitech.v3i2.3446.

[26] W. Buana and A. Hariyandi, "Pengembangan Jaringan Local Area Network (Lan) Dan Wide Area Network (Wan) Pada Smkn 4 Padang Dengan Metode Research Dan Development," *JOISIE (Journal ...*, 2023, doi: DOI: https://doi.org/10.35145/joisie.v7i1.3268.

[27] F. P. E. Putra, U. Ubaidi, R. O. F. Kusuma, A. M. Syam, and S. A. Efendy, "Effect Of Distance On Wi-Fi Signal Quality In The Home Environment," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 391–398, Feb. 2024, doi: 10.47709/brilliance.v4i1.4319.

[28] F. P. E. Putra, N. Ramadhani, F. Fauzan, and M. Mursidi, "Service Quality Analysis of RFID-Based Smart Door Lock in Front One Azana Style Hotel Area," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 372–381, Feb. 2024, doi: 10.47709/brilliance.v4i1.4292.

[29] S. R. Hashim, R. A. Enad, A. M. Al-Khafagi, and ..., "The facilities of detection by using a tool of Wireshark," *Indones. J. ...*, 2023, doi: DOI: https://doi.org/10.11591/IJEECS.V31.I1.PP329-336.

[30] H. Sahputra, N. Nofriadi, C. Latiffani, and ..., "ANALISIS KINERJA PROTOKOL ROUTING OSPF DAN

EIGRP DALAM JARINGAN KOMPUTER SKALA MENENGAH," *... Sci. ...*, 2025, doi: DOI: https://doi.org/10.54314/jssr.v8i3.3865.

[31] F. G. Sembiring, S. Ashillah, and ..., "Analisis Kinerja Routing Dinamis Pada Jaringan Virtual Menggunakan Mikrotik CHR," *... dan Tek. Elektro ...*, 2025, doi: DOI: https://doi.org/10.23960/jitet.v13i3.6516.

[32] A. Kiswantono, "Transformasi Proteksi Tegangan: Sistem Monitoring IoT untuk Pemantauan Real-Time," *DIELEKTRIKA*, 2024, doi: DOI: https://doi.org/10.29303/dielektrika.v11i2.377.

[33] K. T. Antara, "Pengaruh IoT pada Transformasi Jaringan Multimedia: Literatur Review," *J. Ilmu Komput. Dan Sist. Inf. ...*, 2024, doi: DOI: https://doi.org/10.55338/jikomsi.v7i1.2736.

[34] F. P. E. Putra, U. Ubaidi, R. N. Saputra, and ..., "Application of Internet of Things Technology in Monitoring Water Quality in Fishponds," *Brill. Res. ...*, 2024, doi: DOI: https://doi.org/10.47709/brilliance.v4i1.4231.

[35] A. R. A. Negoro and J. L. Putra, "Optimasi jaringan internet menggunakan metode spillover pada PT. Gudang Ada Globalindo," *Just IT J. Sist. Informasi, Teknol. ...*, 2024, doi: DOI: https://doi.org/10.24853/justit.15.1.234-240.

[36] L. M. B. Aksara, M. Taslim, W. Alam, and ..., "Optimasi Jaringan Wireless Dengan Penerapan Antena Kathrein, Metode ECMP dan Metode Recursive Gateway Pada Dua Jaringan Seluler," *J. Fokus ...*, 2024, doi: DOI: https://doi.org/10.33772/jfe.v9i3.795.

[37] M. H. Adwel, M. Mulyono, T. Purnamirza, and ..., "Optimasi Jaringan 4G LTE Menggunakan Metode Automatic Cell Planning (ACP) di Wilayah Kubu Gulai Bancah," *Remik Ris. dan E ...*, 2023, doi: DOI: 10.33395/remik.v7i1.12033.

[38] K. Sabila, S. Rahayu, and T. Sumarni, "Peningkatan Efisiensi Penggunaan Sumber Daya Jaringan Melalui Teknik Load Balancing," *CEMERLANG J. Manaj. dan ...*, 2024, doi: DOI: https://doi.org/10.55606/cemerlang.v4i3.2989.

[39] A. B. Haqi, D. A. Siregar, M. Mutiara, and ..., "Pengenalan Jaringan Komputer Dasar Di Smk Negeri 1 Batang Onang," *J. ADAM J. ...*, 2023, doi: DOI: https://doi.org/10.37081/adam.v2i2.1443.

[40] A. A. N. Aisah, "Pengaruh Cisco Packet Tracer terhadap Pemahaman Konsep Jaringan Komputer di SMK Telkom Makassar," *J. Pendidik. Terap.*, 2025, doi: DOI: https://doi.org/10.61255/jupiter.v3i3.635.

[41] F. P. E. Putra, M. A. Mahmud, and I. S. Maqom, "Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus," *Digit. Transform*, 2023, doi: DOI: https://doi.org/10.47709/digitech.v3i2.3457.

[42] R. Gustanto and A. Risman, "Penggunaan Risiko Environmental, Social, Governance dalam Proses Identifikasi, Pengukuran, Pemantauan dan Pengendalian dalam Bisnis Berkelanjutan …," *Realible Account. J.*, 2025, doi: DOI: https://doi.org/10.36352/raj.v4i2.973.

[43] Q. Al Qorni, D. P. Pamungkas, S. A. Wibowo, and ..., "Pemantauan dan Pengingat Kondisi Kelembaban Lahan Menggunakan Esp8266 dan IoT," *MDP Student ...*, 2023, doi: DOI: https://doi.org/10.35957/mdp-sc.v2i1.4056.

[44] S. Arvind, S. Arvind, V. K. Silveri, G. Potey, and ..., "Network traffic virtualization using Wireshark and Google maps," *2023 Int. ...*, 2023, doi: DOI: 10.1109/ICDCECE57866.2023.10150823.

[45] B. W. Aulia, M. Rizki, P. Prindiyana, and ..., "Peran krusial jaringan komputer dan basis data dalam era digital," *... Sist. Inf. Dan ...*, 2023, doi: DOI: https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253.

[46] N. Alsharabi, M. Alqunun, and ..., "Detecting unusual activities in local network using snort and wireshark tools," *J. Adv. ...*, 2023, doi: DOI: 10.12720/jait.14.4.616-624.

[47] N. A. L. Mabsali, H. Jassim, and J. Mani, "Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic," *1st Int. Conf. ...*, 2023, doi: DOI: 10.2991/978-94-6463-110-4_10.

[48] F. P. E. Putra, U. Ubaidi, M. A. Huda, and ..., "Computer network management optimization through big data analysis using time series analysis method," *Brill. Res. ...*, 2024, doi: DOI: https://doi.org/10.47709/brilliance.v4i1.4373.

[49] F. P. E. Putra, U. Ubaidi, A. Hamzah, and ..., "Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap," *Brill. Res. ...*, 2024, doi: DOI: https://doi.org/10.47709/brilliance.v4i1.4227.

[50] F. P. E. Putra, A. Hamzah, W. Agel, and ..., "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," *J. Sistim Inf. ...*, 2023, doi: DOI: https://doi.org/10.60083/jsisfotek.v5i4.329.

[51] F. P. E. Putra, F. Muslim, N. Hasanah, R. Paradina, and ..., "Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses Push Notification," *J. Sistim Inf. ...*, 2023, doi: DOI: https://doi.org/10.60083/jsisfotek.v5i4.325.

[52] F. Prasetyo, U. R. Jannah, and M. U. Mansyur, "Penggunaan Stb Sebagai Media E-Learning Berbasis Moodle," *J. Inform.*, 2023, doi: DOI: 10.30873/ji.v23i1.3523.

[53] F. P. E. Putra, A. Zulfikri, G. Arifin, and ..., "Analysis of phishing attack trends, impacts and prevention methods: literature study," *... Res. Artif. ...*, 2024, doi: DOI: https://doi.org/10.47709/brilliance.v4i1.4357.