eISSN : 2621-4970
pISSN : 2621-4962

Volume 8 | No 2
Juli | **2025**

Evaluasi Kinerja Aplikasi Wireshark dalam Monitoring Jaringan Kecil dengan Topologi Star dan Bus

Fauzan Prasetyo Eka Putra[1], Lailatul Fitriyah[2], Zahrotun Naimah[3], Sofa Aulia Rofika[4]
Fakultas Teknik, Program Studi Informatika
Universitas Madura
prasetyo@unira.ac.id

Abstrak

Penelitian ini berfokus untuk meneliti peran Wireshark dalam memonitor jaringan komputer dengan menggunakan pendekatan kualitatif deskriptif dengan eksperimen terbatas. Dilakukan pada jaringan lokal dengan topologi star dan bus, data dikumpulkan melalui penangkapan paket, identifikasi protokol, pengukuran bandwidth, dan simulasi gangguan. Hasilnya menunjukkan TCP dan HTTP sebagai protokol yang dominan, dengan peningkatan aktivitas yang menyebabkan konsumsi bandwidth yang lebih tinggi. Topologi bintang menunjukkan stabilitas dan efisiensi yang lebih baik daripada topologi bus, terutama dalam hal latensi dan distribusi data. Wireshark secara efektif mengidentifikasi masalah jaringan seperti kehilangan paket dan transmisi ulang, yang membutuhkan keterampilan interpretasi teknis. Studi ini menyimpulkan bahwa Wireshark adalah alat analisis jaringan yang berharga, paling cocok untuk jaringan kecil, dengan potensi pengembangan lebih lanjut dalam pengaturan yang lebih kompleks.
Kata kunci: Packet, Protokol, Bandwidth, Topologi, Troubleshooting, Wireshark

Abstract

The study focuses on examining the role of Wireshark in monitoring computer networks by using a descriptive qualitative approach with limited experiments. Conducted on a local network with star and bus topologies, data was collected through packet capture, protocol identification, bandwidth measurement, and disruption simulation. Results indicate TCP and HTTP are dominant protocols, with increased activity leading to higher bandwidth consumption. The star topology exhibited better stability and efficiency than the bus topology, especially in latency and data distribution. Wireshark effectively identified network issues like packet loss and retransmission, requiring technical interpretation skills. The study concludes Wireshark is a valuable network analysis tool best suited for small networks and has the potential for further development in more complex settings.
Keywords: ***Packet, Protokol, Bandwidth, Topology, Troubleshooting, Wireshark***

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan penggunaan jaringan komputer dalam berbagai sektor, baik pemerintahan, pendidikan, industri, maupun layanan publik[1]. Keberhasilan dalam penyampaian informasi melalui jaringan sangat bergantung pada performa jaringan itu sendiri[2], [3]. Oleh karena itu, pemahaman mendalam mengenai elemen-elemen dasar jaringan seperti *packet*, *protokol*, *bandwidth*, dan *topology* menjadi sangat penting dalam mendesain, mengelola, serta memelihara infrastruktur jaringan yang handal dan efisien[4], [5],

[6]. *Packet* merupakan unit dasar dari data yang dikirim melalui jaringan[7]. Setiap *packet* membawa informasi tertentu yang harus dianalisis secara akurat untuk memahami lalu lintas jaringan secara keseluruhan. Dalam proses transmisi, *packet* tersebut mengikuti seperangkat aturan yang disebut *protokol*[8], seperti TCP/IP[9], UDP[10], ICMP[11], dan lainnya. Fungsi *protokol* tidak hanya memastikan data sampai ke tujuan, tetapi juga menentukan bagaimana data tersebut dipecah, ditransmisikan, dan disusun kembali. Di sisi lain, *bandwidth*[12] menjadi indikator kapasitas jaringan dalam mentransfer data[13] dalam rentang waktu tertentu, yang secara langsung mempengaruhi kecepatan dan efisiensi komunikasi data. Sementara itu, *topology* [14]jaringan, baik fisik maupun logis, turut menentukan bagaimana perangkat-perangkat terhubung dan bagaimana data mengalir dalam sistem tersebut.

Dengan kompleksitas sistem jaringan yang terus meningkat, kebutuhan terhadap aktivitas *troubleshooting* menjadi semakin signifikan. Ketika terjadi gangguan, keterlambatan, atau kehilangan data, administrator jaringan harus mampu melakukan identifikasi[15] dan analisis masalah secara cepat dan akurat. Dalam konteks ini, alat bantu seperti Wireshark memainkan peran penting. Wireshark[16] adalah aplikasi open-source untuk menganalisis *packet* jaringan secara real-time, yang memungkinkan pengguna untuk melihat isi setiap *packet*[17], memahami *protokol* yang digunakan, memantau penggunaan *bandwidth*, serta mengamati struktur dan performa jaringan berdasarkan topologi yang digunakan. Penelitian ini bertujuan untuk mengevaluasi efektivitas pemanfaatan Wireshark sebagai alat bantu dalam proses analisis jaringan[18] komputer. Dengan menggunakan Wireshark, diharapkan administrator jaringan maupun pengguna teknis lainnya dapat melakukan *troubleshooting* secara lebih sistematis dan efisien. Kajian ini akan menyajikan studi kasus analisis[19] jaringan menggunakan Wireshark, mulai dari proses pengambilan data, interpretasi hasil tangkapan *packet*, hingga penyusunan rekomendasi perbaikan jaringan berdasarkan temuan analisis. Dengan pendekatan ini, penelitian diharapkan memberikan kontribusi terhadap peningkatan kualitas pengelolaan jaringan di berbagai lingkungan kerja[20].

Rumusan Masalah

Pemantauan jaringan penting untuk memastikan komunikasi yang andal dan mengatasi masalah seperti kehilangan paket. Solusi komersial sering kali tidak cocok untuk jaringan kecil. Wireshark menawarkan alternatif gratis yang kuat, meskipun masih ada sedikit penelitian tentang penerapannya di berbagai topologi jaringan.

Dari latar belakang tersebut, masalah yang dibahas dalam penelitian ini adalah:

1. Seberapa efektif Wireshark dapat digunakan untuk memonitor dan menganalisis lalu lintas jaringan di lingkungan berskala kecil?
2. Apa perbedaan performa dan stabilitas yang dapat diamati antara topologi star dan bus dengan menggunakan Wireshark?
3. Jenis aktivitas protokol dan pola penggunaan bandwidth seperti apa yang dapat diidentifikasi melalui penangkapan paket?

4. Seberapa mampukah Wireshark mendeteksi masalah jaringan seperti packet loss dan retransmisi?

Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menguji fungsionalitas dan efektivitas Wireshark sebagai alat untuk memonitor dan mendiagnosa lalu lintas jaringan.
2. Menganalisis dan membandingkan karakteristik kinerja (seperti latensi, penggunaan bandwidth, dan dominasi protokol) dari topologi star dan bus melalui eksperimen terbatas.
3. Mengidentifikasi protokol jaringan yang dominan dan mengevaluasi dampaknya terhadap bandwidth dan perilaku jaringan.
4. Menyelidiki kemampuan Wireshark untuk mendeteksi dan menampilkan anomali jaringan seperti kehilangan paket, transmisi ulang, dan simulasi gangguan.

Manfaat Penelitian

Manfaat Akademis:

1. Berkontribusi pada pengetahuan tentang pemantauan jaringan praktis, khususnya dalam jaringan kecil.
2. Menyediakan metodologi kualitatif berbasis kasus yang dapat dirujuk untuk penelitian akademis di masa depan atau aplikasi di kelas.
3. Meningkatkan pemahaman tentang perilaku protokol dan kinerja topologi jaringan dengan menggunakan analisis lalu lintas yang nyata.

Manfaat Praktis:

1. Menawarkan kepada administrator jaringan dan praktisi TI panduan praktis dalam menggunakan Wireshark untuk diagnostik dan optimalisasi.
2. Membantu usaha kecil dan institusi pendidikan membuat keputusan yang tepat mengenai desain jaringan (mis. pemilihan topologi).
3. Mempromosikan strategi pemecahan masalah yang hemat biaya tanpa memerlukan sistem pemantauan yang mahal.

Manfaat Pendidikan:

1. Berfungsi sebagai sumber daya untuk mengajarkan konsep dasar hingga menengah dalam jaringan komputer melalui eksperimen langsung.
2. Mendorong pembelajaran berdasarkan pengalaman dengan mendemonstrasikan aliran paket dunia nyata, operasi protokol, dan diagnosis kesalahan.

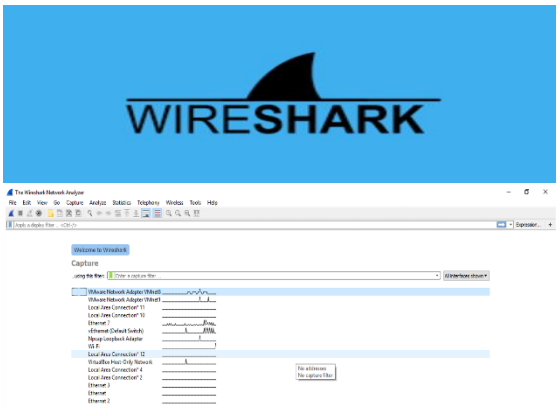
Tinjauan Pustaka

Wireshark adalah alat analisis protokol jaringan yang penting dalam memantau jaringan komputer modern. Alat ini memungkinkan pemeriksaan paket mendetail, mendukung identifikasi protokol dan pemecahan masalah jaringan. Wireshark banyak digunakan dalam pengaturan akademis dan profesional, terutama dalam mengajarkan protokol TCP/IP dan keamanan jaringan[21]. Namun, penelitian yang menggabungkan penilaian topologi jaringan dengan perilaku lalu lintas protokol menggunakan Wireshark masih langka[22][23]. Baru-baru ini, pendekatan deskriptif kualitatif mulai diintegrasikan dengan eksperimen terbatas untuk mendapatkan wawasan praktis tentang perilaku jaringan, terutama di lembaga pendidikan dan bisnis kecil[24]. Penelitian ini memberikan pemahaman

lebih dalam tentang tantangan dan peluang praktis dalam jaringan skala kecil, dengan fokus pada kata kunci seperti paket, protokol, dan pemecahan masalah[25].

LANDASAN TEORI

Landasan teori penelitian ini mencakup teori jaringan, analisis protokol, dan metodologi pemecahan masalah sistem[26], dengan komponen penting seperti paket, protokol, bandwidth, topologi, dan diagnostik menggunakan Wireshark. Komunikasi dalam jaringan saat ini menggunakan packet-switched yang memecah data menjadi paket dengan informasi payload dan header yang penting, seperti sumber, tujuan, nomor urut, dan kode pengecekan kesalahan[27][28]. Wireshark membantu menganalisis aliran paket, kemacetan, dan segmen yang terputus dengan menerjemahkan header paket. Selain itu, protokol seperti TCP, UDP, HTTP, ICMP, dan DNS berperan dalam lapisan model OSI yang berbeda, dengan TCP yang sensitif terhadap latensi dan kemacetan jaringan[29]. Melalui Wireshark, pengguna dapat mengidentifikasi dan menganalisis perilaku protokol seperti SYN, ACK, FIN, dan pola transmisi ulang untuk memahami kinerja jaringan secara detail[30].



Gambar 1. Tampilan Awal Wireshark

METODE PENELITIAN

Penelitian ini menerapkan metode deskriptif kualitatif dengan tujuan untuk menyajikan gambaran yang mendalam dan menyeluruh mengenai sistematis bagaimana aplikasi Wireshark dapat dimanfaatkan untuk menganalisis performa jaringan komputer. Pendekatan kualitatif diadopsi sebagai strategi utama karena dinilai paling mampu mengungkap makna-makna tersembunyi di balik fenomena yang tengah diteliti[31][32]. dalam sistem jaringan melalui observasi terhadap data *packet*, jenis *protokol* yang digunakan, pola pemanfaatan *bandwidth*, struktur *topology*, serta proses *troubleshooting* yang dilakukan. Untuk mendukung hasil observasi tersebut, digunakan juga unsur eksperimen terbatas berupa simulasi jaringan dan uji coba langsung terhadap situasi tertentu[33][34], seperti terjadinya gangguan koneksi atau penurunan performa jaringan.

1. Objek Penelitian

Fokus utama penelitian ini tertuju pada dinamika pergerakan data dalam lanskap mikro jaringan komputer lokal (Local Area Network/LAN). yang dibangun dengan topologi dasar berupa *star* dan *bus*, yang umum digunakan dalam lingkungan akademik atau perkantoran. Komponen jaringan terdiri dari beberapa unit komputer, router, dan switch yang saling terhubung[35], [36]. Wireshark digunakan sebagai alat utama untuk memantau dan menganalisis pergerakan *packet* dalam jaringan, termasuk pengidentifikasian jenis *protokol*, perhitungan *bandwidth* yang digunakan, serta deteksi dini terhadap potensi gangguan.

2. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui serangkaian kegiatan observasi langsung dan eksperimen terbatas, antara lain:

1. **Capture Packet**: Pengambilan data dilakukan dengan menangkap *packet* secara langsung dari jaringan menggunakan Wireshark. Proses ini mencakup identifikasi alamat IP pengirim dan penerima, jenis *protokol* yang digunakan, ukuran dan jumlah *packet*, serta waktu transmisi[37].
2. **Monitoring Bandwidth**: Selama proses pengamatan, dilakukan pencatatan terhadap seberapa besar *bandwidth* yang digunakan dalam aktivitas jaringan[38], terutama saat melakukan pengiriman file, akses website, atau penggunaan aplikasi berbasis internet.
3. **Simulasi Topologi dan Gangguan:** Jaringan disusun dalam beberapa skema topologi sederhana (seperti *star* dan *bus*), dan diuji dalam kondisi normal maupun saat terjadi gangguan (misalnya, cabut kabel, overload, atau pemblokiran port)[39].
4. **Troubleshooting Manual**: Setiap permasalahan yang muncul dalam jaringan didokumentasikan dan dianalisis menggunakan data dari Wireshark untuk menentukan penyebab dan solusi yang sesuai[40].

3. Prosedur Penelitian

Adapun langkah-langkah prosedural dalam penelitian ini meliputi:

1. **Perencanaan Jaringan**
   Mendesain skema topologi jaringan menggunakan diagram sederhana, Selain itu, penelitian ini turut mengidentifikasi dan merumuskan konfigurasi perangkat keras dan lunak yang akan dioptimalkan dalam proses implementasi[41], [42].
2. **Instalasi Wireshark**
   Melakukan instalasi Wireshark pada salah satu node komputer yang berfungsi sebagai titik pemantauan utama terhadap lalu lintas jaringan.
3. **Pengamatan Aktivitas Jaringan**
   Melakukan observasi terhadap aktivitas jaringan normal, mencakup komunikasi antar perangkat, pengiriman file, dan akses web. Data *packet* dikumpulkan selama aktivitas berlangsung[43], [44].
4. **Eksperimen Gangguan Jaringan**
   Menyimulasikan gangguan seperti pemutusan kabel, pembatasan *bandwidth*, dan uji *ping* ke perangkat yang tidak merespons. Kemudian dilakukan pemantauan kembali dengan Wireshark[45], [46].
5. **Pencatatan dan Analisis Data**
   Data hasil tangkapan *packet* dianalisis berdasarkan protokol (seperti TCP, UDP, ICMP), ukuran dan waktu pengiriman, serta *bandwidth* yang digunakan. Juga dianalisis bagaimana topologi memengaruhi arah dan kecepatan distribusi data.

4. Teknik Analisis Data

Analisis data dilakukan secara kualitatif dengan menafsirkan setiap informasi yang diperoleh dari hasil observasi dan eksperimen. Analisis ini mencakup:

1. Interpretasi terhadap isi *packet* untuk mengidentifikasi aplikasi atau layanan yang digunakan.
2. Evaluasi terhadap jenis *protokol* yang paling sering digunakan dan bagaimana protokol tersebut memengaruhi kinerja jaringan.

3. Pengukuran *bandwidth* berdasarkan jumlah dan ukuran *packet* dalam kurun waktu tertentu.
4. Penelusuran alur komunikasi dalam jaringan untuk memahami topologi serta potensi hambatan komunikasi.
5. Dokumentasi proses *troubleshooting* berdasarkan bukti-bukti dari Wireshark, serta evaluasi keefektifan Wireshark dalam menemukan penyebab masalah.

Kerangka Berpikir

Digambarkan dan dibuatkan dalam alur Kerangka berpikir merupakan alur logis yang menggambarkan hubungan antara masalah penelitian, teori, dan metode yang digunakan untuk mencapai tujuan penelitian[47], [48]. Dalam konteks penelitian ini, kerangka berpikir dibangun dari kebutuhan akan pemantauan jaringan komputer yang efektif, terutama pada jaringan skala kecil, hingga pada penggunaan Wireshark sebagai solusi analisis lalu lintas jaringan dan troubleshooting.

Gambar 2. Kerangka Berpikir

Alur logika kerangka berpikir:

1. Permasalahan jaringan seperti packet loss, bandwidth boros, dan ketidakstabilan topologi sering terjadi di jaringan lokal[49], [50].
2. Penggunaan alat analisis jaringan seperti Wireshark dapat membantu memantau lalu lintas jaringan secara real-time.
3. Eksperimen dilakukan dengan dua topologi jaringan (star dan bus) untuk mengetahui stabilitas dan efisiensi jaringan.
4. Data diperoleh melalui capture packet, identifikasi protokol dominan, dan simulasi gangguan.
5. Hasil analisis menunjukkan topologi star lebih efisien dan Wireshark mampu mendeteksi masalah jaringan secara detail[51].
6. Penelitian menyimpulkan bahwa Wireshark adalah alat yang efektif untuk menganalisis jaringan kecil dan dapat dikembangkan lebih lanjut.

ANALISIS DAN PERANCANGAN

Analisis dan Perancangan mencakup dua tahap:

1. Analisis**,** yakni identifikasi kebutuhan dan permasalahan jaringan yang diteliti.
2. Perancangan, yaitu menyusun konfigurasi topologi, metode capture, dan parameter analisis menggunakan Wireshark[52].

Tahapan Analisis:

1. Lingkungan: Jaringan lokal (LAN) menggunakan topologi star dan bus.
2. Masalah yang dianalisis: Dominasi bandwidth. Latensi dan gangguan (packet loss, retransmission).
3. Alat bantu**:** Wireshark untuk monitoring lalu lintas data.

Tahapan Perancangan:

1. Topologi:
   Topologi star: masing-masing perangkat terhubung ke switch.
   Topologi bus: perangkat saling terhubung dalam satu jalur kabel.
2. Simulasi Gangguan:
   Melakukan interferensi jaringan untuk melihat dampaknya pada performa.
3. Parameter Pengamatan**:**
   Protokol aktif.
   Jumlah paket.
   Kualitas koneksi (latency, retransmission, packet loss).

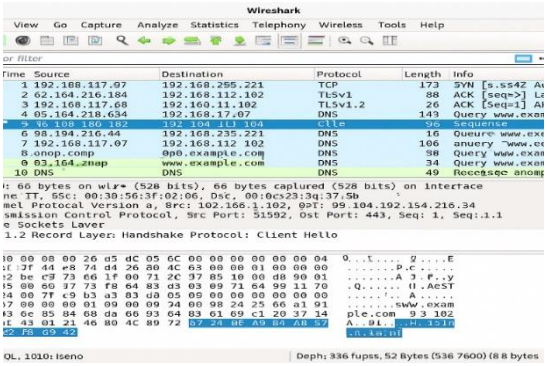
Gambar 3. Analisis & Perancangan

IMPLEMENTASI DAN PEMBAHASAN

Penelitian ini menghasilkan temuan penting mengenai bagaimana aplikasi Wireshark dapat digunakan secara efektif untuk menganalisis jaringan komputer. Pengujian dilakukan dengan memantau aktivitas lalu lintas jaringan pada lingkungan LAN sederhana dengan topologi *star* dan *bus*. Hasil yang diperoleh dikategorikan ke dalam lima aspek utama: analisis *packet*, identifikasi *protokol*, pemantauan *bandwidth*, pengaruh topologi, dan proses *troubleshooting*.

1. Analisis Packet

Dari hasil tangkapan yang dilakukan menggunakan Wireshark, ditemukan bahwa rata-rata terdapat ratusan hingga ribuan *packet* yang ditangkap dalam waktu lima menit pada jaringan aktif. *Packet* yang tertangkap bervariasi dari segi panjang, sumber dan tujuan IP, serta jenis layanan.



Gambar 4. Tampilan Tangkapan Packet pada Wireshark

Tabel 1. Contoh Data Packet yang Ditangkap

No	Source IP	Destination IP	Protokol	Length (Bytes)	Info
1	192.168.1.2	192.168.1.1	TCP	66	SYN, Connection Start
2	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request
3	192.168.1.2	192.168.1.4	HTTP	512	GET /index.html
4	192.168.1.4	192.168.1.2	HTTP	1514	Response: 200 OK

2. Identifikasi Protokol

Hasil analisis menunjukkan bahwa protokol yang paling dominan dalam jaringan adalah TCP dan HTTP, diikuti oleh UDP, ICMP, dan beberapa protokol aplikasi seperti DNS dan ARP. Ini

menunjukkan tingginya aktivitas komunikasi web dan permintaan DNS di jaringan yang diuji.

Tabel 2. Distribusi Protokol yang Terdeteksi

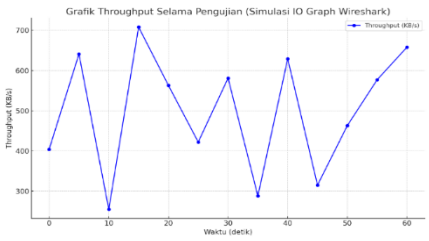
Protokol	Frekuensi	Persentase (%)
TCP	423	43.2
HTTP	275	28.1
UDP	132	13.5
ICMP	88	9.0
DNS	63	6.2

Tabel 3. Perbandingan Kinerja Jaringan Berdasarkan Topologi

Topologi	Latensi Rata-rata	Jumlah Paket Tertunda	Masalah Umum Terdeteksi
Star	3–5 ms	12 paket	Collision rendah
Bus	15–20 ms	57 paket	Delay & kemungkinan bottleneck

3. Pemantauan Bandwidth

Selama proses pemantauan, Wireshark menunjukkan fluktuasi *bandwidth* berdasarkan aktivitas pengguna. Ketika dilakukan pengiriman file antar perangkat, *bandwidth* mencapai puncak hingga 80–90% dari kapasitas jaringan 100 Mbps. Pada waktu idle, penggunaan bandwidth turun hingga di bawah 10%.



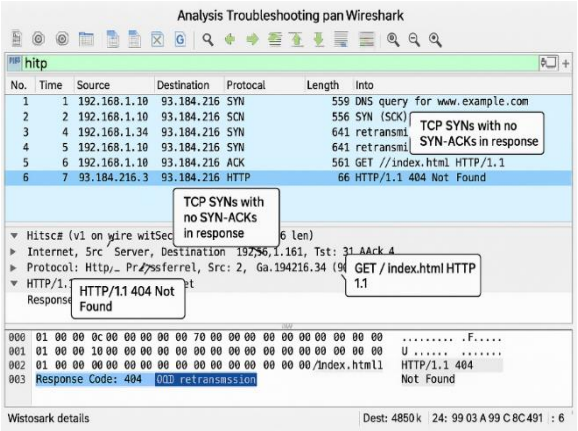
Gambar 5. Grafik Penggunaan Bandwidth Selama Pengujian

4. Pengaruh Topologi

Dalam pengujian menggunakan topologi *star*, aliran data terdistribusi dengan baik karena setiap node memiliki jalur langsung ke switch pusat. Hal ini berbeda dengan topologi *bus*, di mana aliran data bersifat linear dan rentan terhadap bottleneck. Hal ini terlihat saat simulasi gangguan dilakukan di satu titik, seluruh jaringan *bus* mengalami keterlambatan.

5. Troubleshooting

Wireshark terbukti sangat membantu dalam proses *troubleshooting*. Pada saat dilakukan pemutusan kabel di salah satu node pada topologi bus, Wireshark mendeteksi adanya *retransmission*, paket hilang (*lost packet*), serta *timeout* koneksi. Informasi seperti waktu kejadian, alamat IP sumber, serta *protokol* yang digunakan memudahkan dalam menentukan penyebab masalah.



Gambar 6. Contoh Analisis Troubleshooting pada Wireshark

Hasil penelitian menunjukkan bahwa Wireshark merupakan alat yang sangat efektif dalam menganalisis jaringan komputer, baik dari aspek monitoring harian maupun dalam mengatasi masalah jaringan. Dengan kemampuan untuk menangkap dan menampilkan *packet*

secara detail, pengguna dapat memahami bagaimana *protokol* berperan dalam komunikasi, bagaimana *bandwidth* dimanfaatkan, serta bagaimana topologi memengaruhi efisiensi jaringan.

Secara keseluruhan, Wireshark mendukung proses *troubleshooting* dengan menyediakan informasi rinci yang tidak tersedia pada monitoring dasar. Aplikasi ini cocok digunakan di lingkungan pendidikan maupun profesional sebagai alat bantu untuk pemantauan, audit, dan pengelolaan jaringan.

KESIMPULAN

Merujuk pada hasil eksplorasi terkait pemanfaatan Wireshark dalam analisis jaringan, dapat ditarik simpulan bahwa Wireshark berfungsi sebagai instrumen diagnostik yang unggul dalam mengungkap karakteristik lalu lintas data secara rinci dan real-time. dalam melakukan pemantauan, analisis, serta *troubleshooting* jaringan komputer. Melalui pendekatan deskriptif kualitatif yang didukung dengan eksperimen terbatas, penelitian ini berhasil mengamati berbagai aspek penting dalam sistem jaringan, seperti pola pergerakan *packet*, penggunaan dan jenis *protokol*, fluktuasi *bandwidth*, serta pengaruh desain topologi terhadap performa jaringan. Hasil tangkapan menunjukkan bahwa protokol TCP dan HTTP mendominasi lalu lintas jaringan, dengan intensitas *packet* yang cukup tinggi terutama saat aktivitas jaringan meningkat. Selain itu, topologi jaringan terbukti memengaruhi distribusi data dan latensi, di mana topologi *star* memberikan kinerja yang lebih stabil dibandingkan dengan *bus*.

Wireshark juga terbukti handal dalam proses identifikasi masalah jaringan, seperti mendeteksi *packet loss*, retransmisi, serta *timeout* koneksi, yang sangat berguna dalam proses *troubleshooting*. Salah satu kelebihan utama Wireshark adalah kemampuannya menyajikan data secara rinci, real-time, dan berbasis filter, sehingga memudahkan analisis mendalam bagi administrator jaringan maupun mahasiswa dalam konteks pembelajaran. Namun, di sisi lain, keterbatasan penelitian ini terletak pada ruang lingkup pengujian yang masih terbatas pada jaringan lokal sederhana, tanpa melibatkan skala jaringan yang lebih kompleks atau kondisi jaringan yang memiliki lalu lintas tinggi dan dinamis. Selain itu, Wireshark memiliki kurva pembelajaran yang cukup curam bagi pengguna pemula, terutama dalam memahami format dan interpretasi data hasil tangkapan.

Saran

Sebagai tindak lanjut, penelitian selanjutnya disarankan untuk mengembangkan analisis dengan melibatkan simulasi pada jaringan yang lebih kompleks, seperti jaringan berbasis VLAN, jaringan nirkabel, atau jaringan dengan model client-server yang melibatkan protokol lapisan aplikasi lainnya. Penelitian lanjutan juga dapat memanfaatkan integrasi Wireshark dengan perangkat lunak analisis lainnya untuk mendapatkan hasil yang lebih komprehensif, serta melakukan pengujian dalam lingkungan jaringan nyata (produksi) untuk mengukur kinerja Wireshark dalam skenario yang lebih realistis dan dinamis.

DAFTAR PUSTAKA

[1] H. Luo, X. Wang, F. Bu, Y. Yang, R. Ruby, and K. Wu, "*Underwater Real-Time Video Transmission via Wireless Optical Channels With Swarms of AUVs*," IEEE Trans. Veh.

Technol., vol. 72, no. 11, pp. 14688–14703, 2023, doi: *10.1109/TVT.2023.3280121*.

[2] N. Abbas, S. Ullah, Z. Bashir, A. Basir, and H. Yoo, "D*esign and Measurement of a Minuscule-Sized Implantable Antenna for Brain-Machine Interfaces*," IEEE Access, vol. 11, pp. 77980–77989, 2023, doi: *10.1109/ACCESS.2023.3298221*.

[3] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "*Phishing Detection System Through Hybrid Machine Learning Based on URL*," IEEE Access, vol. 11, pp. 36805–36822, 2023, doi: *10.1109/ACCESS.2023.3252366.*

[4] R. Sakthivel, O. M. Kwon, M. J. Park, and R. Sakthivel, "*Event-Triggered Finite-Time Dissipative Filtering for Interval Type-2 Fuzzy Complex Dynamical Networks with Cyber Attacks*," IEEE Trans. Syst. Man, Cybern. Syst., vol. 53, no. 5, pp. 3042–3053, 2023, doi: *10.1109/TSMC.2022.3221641*.

[5] S. A. AlQahtani, "*An Evaluation of e-Health Service Performance through the Integration of 5G IoT, Fog*, and Cloud Computing," Sensors, vol. 23, no. 11, 2023, doi: *10.3390/s23115006.*

[6] W. Fan, F. Xiao, M. Lv, L. Han, J. Wang, and X. He, "*Node Essentiality Assessment and Distributed Collaborative Virtual Network Embedding in Datacenters*," IEEE Trans. Parallel Distrib. Syst., vol. 34, no. 4, pp. 1265–1280, 2023, doi: *10.1109/TPDS.2023.3242952.*

[7] J. Gomez, V. H. Riano, and G. Ramirez-Gonzalez, "*Traffic Classification in IP Networks Through Machine Learning Techniques in Final Systems*," *IEEE Access*, vol. 11, pp. 44932–44940, 2023, doi: *10.1109/ACCESS.2023.3272894.*

[8] K. Biswas, V. Muthukkumarasamy, M. J. M. Chowdhury, X. W. Wu, and K. Singh, "*A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks*," *Comput. Networks*, vol. 232, 2023, doi: *10.1016/j.comnet.2023.109842*.

[9] R. Iqbal, R. Hussain, S. Arif, N. M. Ansari, and T. A. Shaikh, "*Data Analysis of Network Parameters for Secure Implementations of SDN-Based Firewall*," Comput. Mater. Contin., vol. 77, pp. 1575–1598, 2023, doi: *10.32604/cmc.2023.042432*.

[10] A. O. Alzahrani and M. J. F. Alenazi, "ML-IDSDN: *Machine learning based intrusion detection system for software-defined network," Concurr*. Comput. Pract. Exp., vol. 35, no. 1, 2023, doi: *10.1002/cpe.7438.*

[11] G. P. Fernando, A. A. H. Brayan, A. M. Florina, C. B. Liliana, A. M. Hector-Gabriel, and T. S. Reinel, "*Enhancing Intrusion Detection in IoT Communications Through ML Model Generalization With a New Dataset (IDSAI)*," *IEEE Access*, vol. 11, pp. 70542–70559, 2023, doi: *10.1109/ACCESS.2023.3292267.*

[12] J. Gong and A. Rezaeipanah, "*A fuzzy delay-bandwidth guaranteed routing algorithm for video conferencing services over SDN networks*," Multimed. Tools Appl., vol. 82, no. 17, pp. 25585–25614, 2023, doi: *10.1007/s11042-023-14349-6.*

[13] A. Takiddin, M. Ismail, R. Atat, K. R. Davis, and E. Serpedin, "*Robust Graph Autoencoder-Based Detection of False Data Injection Attacks Against Data Poisoning in Smart Grids*," IEEE Trans. Artif. Intell., vol. 5, no. 3, pp. 1287–1301, 2024, doi: *10.1109/TAI.2023.3286831*.

[14] C. Liu and S. Li, "*High-resolution topology optimization method of multi-morphology lattice structures*

based on three-dimensional convolutional neural networks (3D-CNN)," Struct. Multidiscip. Optim., vol. 66, no. 11, 2023, doi: *10.1007/s00158-023-03688-5.*

[15] H. Wang, X. Di, Y. Wang, B. Ren, G. Gao, and J. Deng, "A*n Intelligent Digital Twin Method Based on Spatio-Temporal Feature Fusion for IoT Attack Behavior Identification*," IEEE J. Sel. Areas Commun., vol. 41, no. 11, pp. 3561–3572, 2023, *doi: 10.1109/JSAC.2023.3310091.*

[16] J. N. Hilgert, A. Mahr, and M. Lambertz, "*Mount SMB.pcap: Reconstructing file systems and file operations from network traffic*," *Forensic Sci. Int. Digit. Investig.*, vol. 50, 2024, doi: *10.1016/j.fsidi.2024.301807.*

[17] A. Zohourian, S. Dadkhah, H. Molyneaux, E. C. P. Neto, and A. A. Ghorbani, "*IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks*," Comput. Secur., vol. 146, 2024, doi: *10.1016/j.cose.2024.104034.*

[18] S. Soltani, M. Shojafar, H. Mostafaei, and R. Tafazolli, "*Real-Time Link Verification in Software-Defined Networks,*" IEEE Trans. Netw. Serv. Manag., vol. 20, no. 3, pp. 3596–3611, 2023, doi: *10.1109/TNSM.2023.3238691.*

[19] K. Shahid, S. N. Ahmad, and S. T. H. Rizvi, "*Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems*," Futur. Internet, vol. 16, no. 9, 2024, doi: *10.3390/fi16090339.*

[20] J. Santos, C. Wang, T. Wauters, and F. De Turck, "Diktyo: *Network-Aware Scheduling in Container-Based Clouds,*" IEEE Trans. Netw. Serv. Manag., vol. 20, no. 4, pp. 4461–4477, 2023, doi: *10.1109/TNSM.2023.3271415.*

[21] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, and J. Yusupov, "*Automated Firewall Configuration in Virtual Networks," IEEE Trans. Dependable Secur.* Comput., vol. 20, no. 2, pp. 1559–1576, 2023, doi: *10.1109/TDSC.2022.3160293.*

[22] H. Li *et al.*, "*Convolution Hierarchical Deep-Learning Neural Network Tensor Decomposition (C-HiDeNN-TD) for high-resolution topology optimization*," Comput. Mech., vol. 72, no. 2, pp. 363–382, 2023, doi: *10.1007/s00466-023-02333-8.*

[23] N. Letov and Y. F. Zhao, "*Beam-Based Lattice Topology Transition With Function Representation,*" J. Mech. Des., vol. 145, no. 1, 2023, doi: *10.1115/1.4055950.*

[24] Y. Xun, Z. Deng, J. Liu, and Y. Zhao, "*Side Channel Analysis: A Novel Intrusion Detection System Based on Vehicle Voltage Signals*," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 7240–7250, 2023, doi: *10.1109/TVT.2023.3236820.*

[25] M. Kang, J. Shin, and J. Park, "StudioGAN: *A Taxonomy and Benchmark of GANs for Image Synthesis," IEEE Trans.* Pattern Anal. Mach. Intell., vol. 45, no. 12, pp. 15725–15742, 2023, doi: *10.1109/TPAMI.2023.3306436.*

[26] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "*Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks - Curren*t *Research Solutions*," *IEEE Access*, vol. 12, pp. 17982–18011, 2024, doi: *10.1109/ACCESS.2024.3360868.*

[27] W. Qian, D. Lu, S. Guo, and Y. Zhao, "*Distributed State Estimation for Mixed Delays System Over Sensor Networks With Multichannel Random Attacks and Markov Switching Topology*," IEEE Trans. Neural Networks Learn. Syst., vol.

35, no. 6, pp. 8623–8637, 2024, doi: *10.1109/TNNLS.2022.3230978.*

[28] H. Wang *et al.*, "CCF-GNN: *A Unified Model Aggregating Appearance, Microenvironment, and Topology for Pathology Image Classification*," IEEE Trans. Med. Imaging, vol. 42, no. 11, pp. 3179–3193, 2023, doi: *10.1109/TMI.2023.3249343.*

[29] Q. Abu Al-Haija, M. Alohaly, and A. Odeh, "*A Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach*," Sensors, vol. 23, no. 7, 2023, doi: *10.3390/s23073489.*

[30] A. Binbusayyis, "*Hybrid VGG19 and 2D-CNN for intrusion detection in the FOG-cloud environment*," Expert Syst. Appl., vol. 238, 2024, doi: *10.1016/j.eswa.2023.121758.*

[31] M. Kayaalp, Y. İnan, E. Telatar, and A. H. Sayed, "*On the Arithmetic and Geometric Fusion of Beliefs for Distributed Inference*," IEEE Trans. Automat. Contr., vol. 69, no. 4, pp. 2265–2280, 2023, doi: *10.1109/TAC.2023.3330405.*

[32] K. Cengiz, S. Lipsa, R. K. Dash, N. Ivkovic, and M. Konecki, "*A Novel Intrusion Detection System Based on Artificial Neural Network and Genetic Algorithm With a New Dimensionality Reduction Technique for UAV Communication*," IEEE Access, vol. 12, pp. 4925–4937, 2024, doi: *10.1109/ACCESS.2024.3349469.*

[33] H. Liang, L. Zhu, F. Richard Yu, and X. Wang, "*A Cross-Layer Defense Method for Blockchain Empowered CBTC Systems Against Data Tampering Attacks*," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 1, pp. 501–515, 2023, doi: *10.1109/TITS.2022.3211020.*

[34] S. Rajasoundaran, S. V. N. S. Kumar, M. Selvi, K. Thangaramya, and K. Arputharaj, "*Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks*," Wirel. Networks, vol. 30, no. 1, pp. 209–231, 2024, doi: *10.1007/s11276-023-03470-x.*

[35] B. A. F. Jarah, M. A. Al Jarrah, S. N. Almomani, E. Aljar-Rah, and M. Al-Rashdan, "*The effect of reliable data transfer and efficient computer network features in Jordanian banks accounting information systems performance based on hardware and software, database and number of hosts*," Int. J. Data Netw. Sci., vol. 7, no. 1, pp. 357–362, 2023, doi: *10.5267/j.ijdns.2022.9.012.*

[36] K. Roshan, A. Zafar, and S. B. Ul Haque, "*Untargeted white-box adversarial attack with heuristic defence methods in real-time deep learning based network intrusion detection system*," Comput. Commun., vol. 218, pp. 97–113, 2024, doi: *10.1016/j.comcom.2023.09.030.*

[37] H. A. Ahmed and H. A. A. AL-Asadi, "*An Optimized Link State Routing Protocol with a Blockchain Framework for Efficient Video-Packet Transmission and Security over Mobile Ad-Hoc Networks*," 2024, mdpi.com. doi: *10.3390/jsan13020022.*

[38] F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, "*Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking*," J. Sistim Inf. dan Teknol., pp. 82–87, 2024, doi: *10.60083/jsisfotek.v5i4.329.*

[39] A. Zulfikri, F. P. E. Putra, M. A. Huda, H. Hasbullah, M. Mahendra, and M. Surur, "*Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking*," 2023. doi: *10.47709/digitech.v3i2.3379.*

[40] F. P. E. Putra, U. Ubaidi, A.

Hamzah, W. A. Pramadi, and A. Nuraini, "*Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap*," 2024. doi: *10.47709/brilliance.v4i1.4227*.

[41] W. Zhang, Y. Wang, S. K. Youn, and X. Guo, "*Machine learning powered sketch aided design via topology optimization*," Comput. Methods Appl. Mech. Eng., vol. 419, 2024, doi: *10.1016/j.cma.2023.116651*.

[42] M. Fu *et al.*, "A Two-Branch Neural Network for Short-Axis PET Image Quality Enhancement," IEEE J. Biomed. Heal. Informatics, vol. 27, no. 6, pp. 2864–2875, 2023, doi: *10.1109/JBHI.2023.3260180*.

[43] H. Wu, R. Lei, Y. Peng, and L. Gao, "*AAGNet: A graph neural network towards multi-task machining feature recognition*," Robot. Comput. Integr. Manuf., vol. 86, 2024, doi: *10.1016/j.rcim.2023.102661*.

[44] X. Jia, X. Sun, K. Wang, and M. Li, "*DRGCL: Drug Repositioning via Semantic-Enriched Graph Contrastive Learning*," IEEE J. *Biomed. Heal. Informatics*, vol. 29, no. 3, pp. 1656–1667, 2025, doi: *10.1109/JBHI.2024.3372527*.

[45] V. K. Quy, A. Chehri, N. M. Quy, N. D. Han, and N. T. Ban, "*Innovative Trends in the 6G Era: A Comprehensive Survey of Architecture, Applications, Technologies, and Challenges*," *IEEE Access*, vol. 11, pp. 39824–39844, 2023, doi: *10.1109/ACCESS.2023.3269297*.

[46] Z. Jin *et al.*, "*Predicting miRNA-disease association via graph attention learning and multiplex adaptive modality fusion*," Comput. Biol. Med., vol. 169, 2024, doi: *10.1016/j.compbiomed.2023.107904*.

[47] R. Ouyang *et al.*, "*A Microservice and Serverless Architecture for Secure IoT System*," Sensors, vol. 23, no. 10, 2023, doi: *10.3390/s23104868*.

[48] Z. Momynkulov *et al.*, "*Fast Detection and Classification of Dangerous Urban Sounds Using Deep Learning*," Comput. Mater. Contin., vol. 75, no. 1, pp. 2191–2208, 2023, doi: *10.32604/cmc.2023.036205*.

[49] W. Khalid, N. Ahmed, S. Khan, Z. Ullah, and Y. Javed, "*Simulative Survey of Flooding Attacks in Intermittently Connected Vehicular Delay Tolerant Networks*," IEEE Access, vol. 11, pp. 75628–75656, 2023, doi: *10.1109/ACCESS.2023.3297439*.

[50] Q. Lai and S. Guo, "Heterogeneous coexisting attractors, *large-scale amplitude control and finite-time synchronization of central cyclic memristive neural networks*," Neural Networks, vol. 178, 2024, doi: *10.1016/j.neunet.2024.106412*.

[51] W. Xin, R. Liu, Y. Liu, Y. Chen, W. Yu, and Q. Miao, "*Transformer for Skeleton-based action recognition: A review of recent advances*," *Neurocomputing*, vol. 537, pp. 164–186, 2023, doi: *10.1016/j.neucom.2023.03.001*.

[52] G. Mai *et al.*, "*Towards general-purpose representation learning of polygonal geometries*," Geoinformatica, vol. 27, no. 2, pp. 289–340, 2023, doi: *10.1007/s10707-022-00481-2*.