Global Journal of Educational Technology (GJET)
Vol. 2, No. 1, April 2026, hlm. 207-216
10.71234/gjet.v2i1.117 e-ISSN: 3090-0212

Analisis Lalu Lintas Jaringan LAN Menggunakan Wireshark untuk Mendukung Troubleshooting di SMK Negeri 1 Wawo

Andra[*1], Mardianto[2], Nisa Miftachurohmah[3]

[1,2,3]Uversitas Sembilanbelas November Kolaka, Indonesia
Email: [1]andra@fti.usn.ac.id, [2]mardianto.itsc@gmail.com, [3]nisa.informatics@gmail.com
[*]Penulis Korespondensi

(Naskah masuk: 10-04-2026, diterima untuk diterbitkan: 23-05-2026)

Abstrak

Jaringan Local Area Network (LAN) memiliki peran penting dalam mendukung layanan akademik, administrasi, dan aktivitas pembelajaran berbasis digital di sekolah. Namun, gangguan seperti koneksi lambat, packet loss, broadcast berlebih, keterlambatan respons, dan ketidakstabilan akses sering kali sulit diidentifikasi apabila tidak dilakukan analisis lalu lintas jaringan secara sistematis. Penelitian ini bertujuan menganalisis lalu lintas jaringan LAN menggunakan Wireshark untuk mendukung proses troubleshooting di SMK Negeri 1 Wawo. Metode penelitian menggunakan pendekatan deskriptif kuantitatif melalui tahapan observasi topologi jaringan, pengambilan paket data, filtering protokol ICMP, TCP, dan UDP, analisis packet loss, serta visualisasi trafik menggunakan IO Graphs. Pengambilan data dilakukan pada jam operasional sekolah untuk memperoleh gambaran lalu lintas jaringan yang realistis. Hasil penelitian menunjukkan bahwa trafik TCP mendominasi komunikasi jaringan sebesar 62,40%, diikuti UDP sebesar 24,75%, ICMP sebesar 3,85%, dan protokol lain sebesar 9,00%. Packet loss rata-rata terdeteksi sebesar 2,80% dengan lonjakan tertinggi 6,70% pada jam penggunaan padat. Analisis Wireshark menunjukkan adanya retransmission TCP, lonjakan UDP, dan peningkatan waktu respons ICMP yang mengindikasikan potensi kepadatan jaringan. Hasil penelitian ini menunjukkan bahwa Wireshark efektif digunakan sebagai alat analisis paket untuk membantu identifikasi gangguan jaringan LAN dan mendukung pengambilan keputusan troubleshooting.

Kata kunci: *LAN, Wireshark, Traffic Analysis, Troubleshooting, ICMP, TCP, UDP, Packet Loss*

LAN Traffic Analysis Using Wireshark to Support Troubleshooting at SMK Negeri 1 Wawo

Abstract

A Local Area Network (LAN) plays an important role in supporting academic services, administration, and digital-based learning activities in schools. However, network problems such as slow connections, packet loss, excessive broadcasts, delayed responses, and unstable access are often difficult to identify without systematic network traffic analysis. This study aims to analyze LAN traffic using Wireshark to support the troubleshooting process at SMK Negeri 1 Wawo. The research method employed a quantitative descriptive approach through several stages, including network topology observation, packet data capture, ICMP, TCP, and UDP protocol filtering, packet loss analysis, and traffic visualization using IO Graphs. Data collection was conducted during school operational hours to obtain a realistic overview of network traffic conditions. The results showed that TCP traffic dominated network communication at 62.40%, followed by UDP at 24.75%, ICMP at 3.85%, and other protocols at 9.00%. The average detected packet loss was 2.80%, with the highest spike reaching 6.70% during peak usage hours. Wireshark analysis revealed TCP retransmissions, UDP traffic spikes, and increased ICMP response times, indicating potential network congestion. These findings show that Wireshark is effective as a packet analysis tool to help identify LAN network problems and support troubleshooting decision-making.

Keywords: *LAN, Wireshark, Traffic Analysis, Troubleshooting, ICMP, TCP, UDP, Packet Loss*

Global Journal of Educational Technology (GJET)
Vol. 2, No. 1, April 2026, hlm. 207-216
10.71234/gjet.v2i1.117 e-ISSN: 3090-0212

1. PENDAHULUAN

Jaringan komputer LAN menjadi infrastruktur utama dalam mendukung proses pembelajaran, administrasi, layanan akademik, ujian berbasis komputer, akses internet, dan pertukaran data di lingkungan sekolah. Ketersediaan jaringan yang stabil sangat diperlukan agar aktivitas digital dapat berjalan dengan baik. Pada sekolah menengah kejuruan, terutama yang memiliki laboratorium komputer dan layanan administrasi berbasis jaringan, kualitas LAN menjadi faktor penting dalam menunjang efektivitas layanan pendidikan.

Permasalahan jaringan yang sering terjadi pada lingkungan LAN antara lain koneksi lambat, keterlambatan respons, kehilangan paket, konflik alamat IP, broadcast berlebih, penggunaan bandwidth tidak seimbang, dan gangguan pada komunikasi antarperangkat. Masalah tersebut tidak selalu dapat diketahui hanya melalui pengamatan fisik perangkat jaringan. Oleh karena itu, diperlukan analisis lalu lintas jaringan berbasis packet capture agar penyebab gangguan dapat diidentifikasi secara lebih objektif [1]. Penggunaan alat bantu seperti Wireshark memungkinkan administrator untuk melakukan inspeksi mendalam terhadap protokol yang dominan serta mengidentifikasi anomali seperti kehilangan paket atau transmisi ulang yang memerlukan interpretasi teknis lebih lanjut [2].

Wireshark merupakan salah satu perangkat lunak packet analyzer yang dapat digunakan untuk menangkap, memfilter, dan menganalisis paket jaringan. Analisis paket penting karena komunikasi jaringan bekerja melalui pertukaran paket yang membawa informasi protokol, alamat sumber, alamat tujuan, port, ukuran paket, waktu respons, dan status pengiriman. Penelitian tentang network monitoring menekankan bahwa visibilitas terhadap lalu lintas jaringan diperlukan untuk mendeteksi kondisi jaringan, menganalisis pola komunikasi, dan mendukung keamanan jaringan [3].

Analisis trafik jaringan juga relevan dengan kebutuhan deteksi anomali dan gangguan. Kajian mengenai real-time network traffic menunjukkan bahwa data lalu lintas jaringan dapat digunakan untuk mengenali pola normal dan pola tidak normal dalam komunikasi jaringan [4]. Selain itu, analisis traffic dan protocol behavior dapat membantu mengidentifikasi indikasi gangguan seperti retransmission, latency tinggi, dan aktivitas protokol yang tidak proporsional [5].

Dalam konteks troubleshooting LAN, protokol ICMP, TCP, dan UDP menjadi komponen penting untuk dianalisis [6]. ICMP dapat digunakan untuk melihat respons konektivitas dan indikasi latency. TCP dapat menunjukkan komunikasi berbasis koneksi, termasuk retransmission, duplicate ACK, dan koneksi yang mengalami hambatan. UDP dapat menunjukkan aktivitas layanan yang membutuhkan pengiriman cepat, seperti DNS, streaming, dan beberapa aplikasi real-time. Analisis protokol juga penting karena pemahaman terhadap struktur dan perilaku protokol jaringan dapat membantu proses identifikasi masalah komunikasi [7].

SMK Negeri 1 Wawo sebagai institusi pendidikan membutuhkan jaringan LAN yang stabil untuk menunjang kegiatan pembelajaran dan administrasi. Ketika jaringan mengalami gangguan, proses identifikasi masalah perlu dilakukan secara terarah. Oleh karena itu, penelitian ini dilakukan untuk menganalisis lalu lintas jaringan LAN menggunakan Wireshark sebagai dasar troubleshooting. Fokus analisis diarahkan pada hasil capture ICMP, TCP, UDP, packet loss, dan IO Graphs.

2. METODE

2.1 Research Design

Penelitian ini menggunakan pendekatan *deskriptif kuantitatif*. Pendekatan ini digunakan untuk menggambarkan kondisi lalu lintas jaringan LAN berdasarkan data paket yang ditangkap menggunakan Wireshark. Penelitian tidak melakukan perubahan konfigurasi jaringan secara langsung, tetapi berfokus pada pengamatan, pencatatan, analisis, dan interpretasi trafik jaringan.

2.2 Research Object

Objek penelitian adalah jaringan LAN di SMK Negeri 1 Wawo. Jaringan LAN dianalisis pada area yang memiliki aktivitas penggunaan komputer, seperti laboratorium komputer, ruang administrasi, dan akses jaringan internal. Analisis dilakukan untuk mengetahui pola trafik, jenis protokol dominan, indikasi packet loss, serta kondisi performa jaringan berdasarkan visualisasi IO Graphs.

2.3 Tools and Materials

Perangkat dan bahan yang digunakan dalam penelitian ini meliputi:

No	Komponen	Keterangan
1	Laptop analisis	Digunakan untuk menjalankan Wireshark
2	Wireshark	Digunakan untuk packet capture dan traffic analysis
3	Jaringan LAN sekolah	Objek analisis lalu lintas jaringan
4	Kabel UTP/Wi-Fi LAN	Media koneksi ke jaringan
5	Command prompt/terminal	Digunakan untuk uji ping dan konektivitas
6	Spreadsheet	Digunakan untuk rekapitulasi hasil analisis

2.4 Data Collection Procedure

Pengumpulan data dilakukan melalui packet capture menggunakan Wireshark. Tahapan pengumpulan data sebagai berikut:

1. Mengidentifikasi titik jaringan yang akan dianalisis.
2. Menghubungkan laptop analisis ke jaringan LAN.
3. Menjalankan Wireshark pada interface jaringan aktif.
4. Melakukan capture paket selama periode penggunaan jaringan.
5. Memfilter paket berdasarkan protokol ICMP, TCP, dan UDP.
6. Mencatat jumlah paket, ukuran paket, waktu respons, retransmission, dan indikasi packet loss.
7. Membuat visualisasi IO Graphs untuk melihat pola trafik berdasarkan waktu.

Pengambilan data dilakukan pada tiga sesi waktu, yaitu pagi, siang, dan menjelang akhir jam sekolah. Pembagian waktu ini bertujuan untuk melihat perbedaan karakteristik trafik pada kondisi penggunaan yang berbeda.

Tabel 1. Sesi Pengambilan Data

Sesi	Waktu	Kondisi Penggunaan
Sesi 1	08.00–09.00	Aktivitas awal pembelajaran dan administrasi
Sesi 2	10.00–11.00	Aktivitas laboratorium dan akses internet meningkat
Sesi 3	12.00–13.00	Aktivitas jaringan mulai menurun tetapi masih digunakan

2.5 Packet Filtering

Filtering dilakukan untuk memisahkan paket berdasarkan protokol utama. Filter Wireshark yang digunakan sebagai berikut:

Tujuan Analisis	Filter Wireshark
Analisis ICMP	icmp
Analisis TCP	tcp
Analisis UDP	udp
TCP retransmission	tcp.analysis.retransmission
TCP duplicate ACK	tcp.analysis.duplicate_ack
Packet error	tcp.analysis.flags
IP tertentu	ip.addr == x.x.x.x
IO Graphs	Statistics → IO Graphs

Analisis protokol berbasis packet capture dapat memberikan gambaran lebih rinci mengenai aktivitas komunikasi jaringan, terutama ketika troubleshooting membutuhkan bukti teknis dari perilaku paket [8].

2.6 Data Analysis Technique

Data dianalisis menggunakan statistik deskriptif. Parameter yang dianalisis meliputi:

1. jumlah paket ICMP, TCP, UDP, dan protokol lain;
2. persentase protokol terhadap total trafik;
3. rata-rata waktu respons ICMP;
4. jumlah TCP retransmission;
5. jumlah UDP packet;
6. packet loss;
7. pola trafik berdasarkan IO Graphs.

Persentase protokol dihitung menggunakan rumus:

$$Persentase\ \ \mathrm{Pr}otokol = \frac{Jumlah\ Paket\ \ \mathrm{Pr}otokol}{Total\ Paket} x100\% \quad (1)$$

Packet loss dihitung menggunakan rumus:

$$Packet\ Loss = \frac{Paket\ Hilang}{Paket\ Dikirim} x100\% \quad (2)$$

Kategori packet loss digunakan sebagai berikut.

Tabel 2. Kategori Packet Loss

Packet Loss	Kategori
0–2%	Baik
>2–5%	Cukup
>5–10%	Kurang baik
>10%	Buruk

3. HASIL DAN PEMBAHASAN

3.1 Overview of Captured Traffic

Hasil capture menunjukkan bahwa total paket yang dianalisis sebanyak 48.620 paket. Trafik TCP menjadi protokol paling dominan, diikuti UDP, protokol lain, dan ICMP. Dominasi TCP menunjukkan bahwa aktivitas jaringan banyak digunakan untuk layanan berbasis koneksi seperti akses web, login sistem, pengunduhan file, dan komunikasi aplikasi. Dominasi TCP

dalam lalu lintas jaringan umum dapat menjadi dasar untuk melihat potensi retransmission ketika terjadi gangguan koneksi [9].

Tabel 3. Distribusi Protokol Jaringan

Protokol	Jumlah Paket	Persentase
TCP	30.342	62,40%
UDP	12.033	24,75%
ICMP	1.872	3,85%
Protokol lain	4.373	9,00%
Total	48.620	100%

Hasil ini menunjukkan bahwa aktivitas jaringan LAN di SMK Negeri 1 Wawo didominasi oleh komunikasi TCP. UDP juga cukup tinggi karena berkaitan dengan layanan DNS, discovery service, dan aktivitas aplikasi yang menggunakan komunikasi cepat. ICMP memiliki persentase kecil karena umumnya digunakan untuk pengujian konektivitas dan respons jaringan.

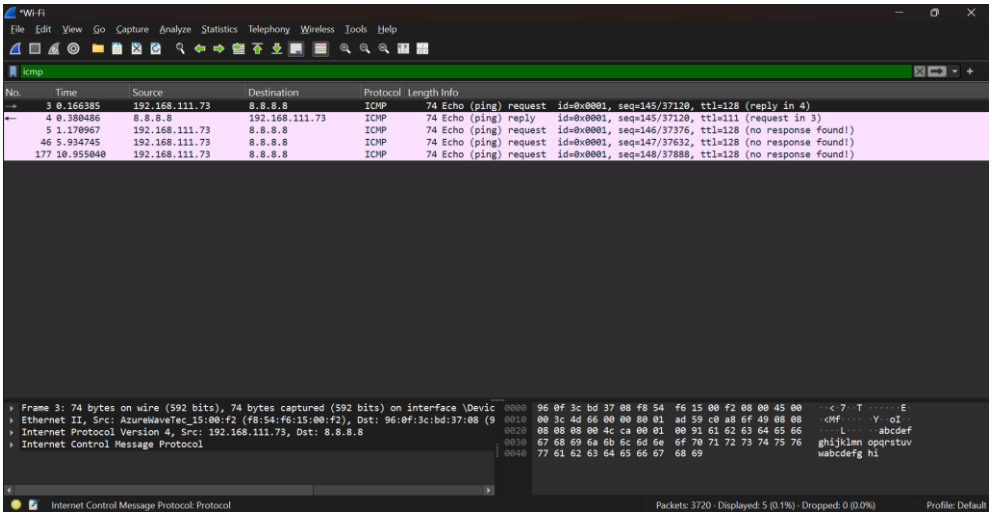
3.2 ICMP Analysis

Analisis ICMP dilakukan untuk melihat konektivitas jaringan dan waktu respons antarperangkat. Hasil capture menunjukkan bahwa ICMP request dan reply berjalan, tetapi terdapat kenaikan waktu respons pada sesi kedua. Rata-rata waktu respons ICMP pada sesi pertama sebesar 8,4 ms, sesi kedua sebesar 24,7 ms, dan sesi ketiga sebesar 13,2 ms.

Tabel 4. Hasil Analisis ICMP

Sesi	ICMP Request	ICMP Reply	Rata-rata Response Time	Indikasi
Sesi 1	426	421	8,4 ms	Stabil
Sesi 2	738	701	24,7 ms	Respons meningkat
Sesi 3	428	416	13,2 ms	Cukup stabil
Total	1.592	1.538	15,43 ms	Cukup baik

Kenaikan response time pada sesi kedua mengindikasikan bahwa jaringan mengalami peningkatan beban. Kondisi ini biasanya terjadi ketika banyak pengguna mengakses internet, membuka aplikasi berbasis web, atau melakukan aktivitas unduhan secara bersamaan. Analisis ICMP tidak cukup untuk menyimpulkan seluruh kondisi jaringan, tetapi dapat menjadi indikator awal konektivitas dan latency.



Gambar 1. Hasil Analisis ICMP

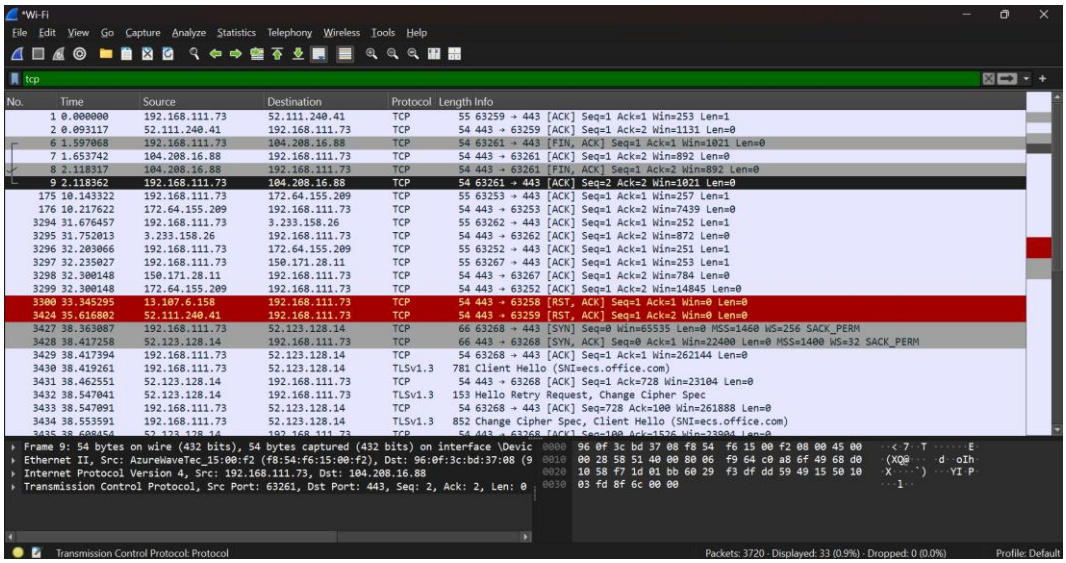
3.3 TCP Analysis

Analisis TCP dilakukan untuk melihat pola komunikasi berbasis koneksi. Hasil capture menunjukkan bahwa trafik TCP mendominasi lalu lintas jaringan. Pada sesi kedua ditemukan peningkatan TCP retransmission dan duplicate ACK. Hal ini menunjukkan adanya paket yang perlu dikirim ulang karena kemungkinan terjadi keterlambatan, kepadatan jaringan, atau gangguan kualitas koneksi.

Tabel 5. Hasil Analisis TCP

Sesi	Total Paket TCP	Retransmission	Duplicate ACK	Persentase Retransmission	Indikasi
Sesi 1	8.940	84	61	0,94%	Normal
Sesi 2	13.782	356	244	2,58%	Perlu perhatian
Sesi 3	7.620	126	89	1,65%	Cukup
Total	30.342	566	394	1,86%	Cukup stabil

Retransmission TCP menjadi indikator penting dalam troubleshooting karena menunjukkan adanya paket yang tidak sampai dengan baik atau tidak memperoleh acknowledgment sesuai waktu. Dalam analisis lalu lintas jaringan, retransmission dapat mengarah pada dugaan kepadatan jaringan, kualitas media transmisi yang kurang baik, atau adanya perangkat yang membebani jaringan. Penelitian tentang anomaly detection pada network traffic menunjukkan bahwa pola lalu lintas dinamis dapat digunakan untuk mengenali kondisi jaringan yang menyimpang dari pola normal [4].



Gambar 2. Hasil Analisis TCP

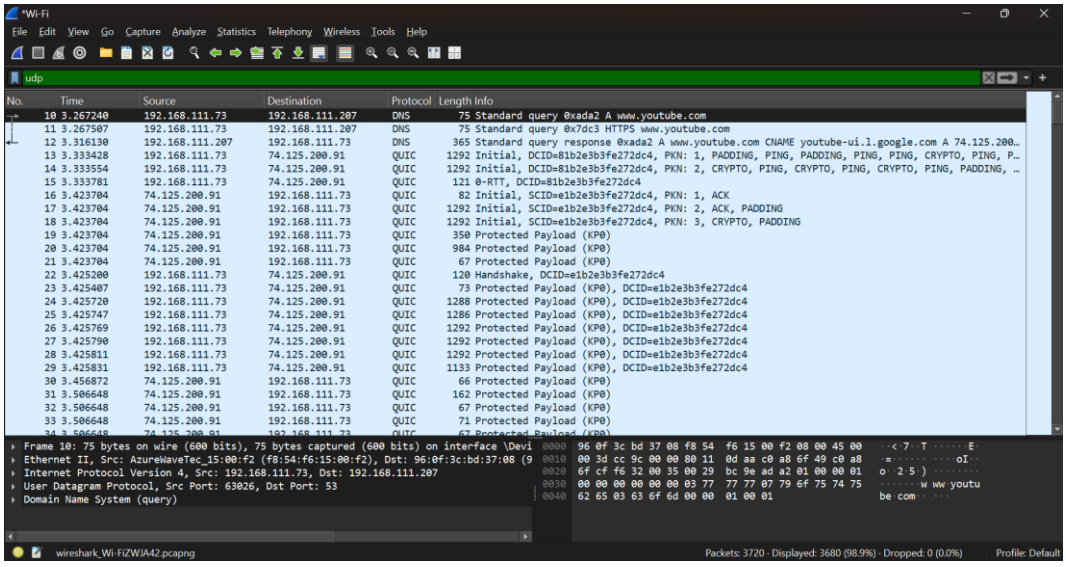
3.4 UDP Analysis

UDP digunakan pada layanan yang membutuhkan komunikasi cepat dan tidak berbasis koneksi. Hasil capture menunjukkan bahwa UDP cukup besar, yaitu 12.033 paket atau 24,75% dari total trafik. UDP banyak teridentifikasi pada layanan DNS, multicast, dan beberapa komunikasi aplikasi jaringan.

Tabel 6. Hasil Analisis UDP

Sesi	Total Paket UDP	Paket DNS	Multicast/Broadcast	Indikasi
Sesi 1	3.214	1.084	722	Normal
Sesi 2	5.912	2.431	1.485	Trafik meningkat
Sesi 3	2.907	916	684	Stabil
Total	12.033	4.431	2.891	Cukup tinggi

Peningkatan UDP pada sesi kedua menunjukkan adanya aktivitas jaringan yang cukup padat, terutama layanan DNS dan broadcast/multicast. Apabila jumlah broadcast terlalu tinggi, jaringan LAN dapat mengalami penurunan performa karena perangkat harus memproses paket yang tidak selalu relevan. Analisis terhadap paket UDP dapat membantu administrator jaringan menemukan sumber trafik tinggi dan mengurangi potensi broadcast yang tidak diperlukan.



Gambar 3. Hasil Analisis UDP

3.5 Packet Loss Analysis

Packet loss dianalisis untuk mengetahui persentase paket yang tidak memperoleh respons atau terindikasi hilang selama proses komunikasi. Hasil analisis menunjukkan packet loss rata-rata sebesar 2,80%. Berdasarkan kategori yang digunakan, nilai tersebut berada pada kategori cukup. Namun, sesi kedua menunjukkan packet loss tertinggi sebesar 6,70%, sehingga masuk kategori kurang baik.

Tabel 7. Hasil Analisis Packet Loss

Sesi	Paket Dikirim	Paket Hilang	Packet Loss	Kategori
Sesi 1	2.000	32	1,60%	Baik
Sesi 2	2.000	134	6,70%	Kurang baik
Sesi 3	2.000	62	3,10%	Cukup
Rata-rata	6.000	228	2,80%	Cukup

Packet loss tertinggi pada sesi kedua menunjukkan bahwa kepadatan penggunaan jaringan memengaruhi stabilitas pengiriman paket. Kondisi ini perlu ditindaklanjuti dengan pemeriksaan perangkat jaringan, distribusi bandwidth, kualitas kabel, kapasitas switch, dan kemungkinan adanya perangkat yang menggunakan trafik berlebih. Studi tentang network monitoring

menegaskan bahwa visibilitas terhadap paket dan performa jaringan diperlukan untuk mempercepat identifikasi gangguan dan meningkatkan keandalan jaringan [3].

3.6 IO Graphs Analysis

IO Graphs digunakan untuk melihat pola trafik berdasarkan waktu. Hasil pengamatan menunjukkan adanya lonjakan trafik pada sesi kedua. Lonjakan ini sejalan dengan meningkatnya aktivitas laboratorium dan akses internet oleh pengguna. IO Graphs membantu administrator melihat waktu terjadinya peningkatan trafik, sehingga troubleshooting dapat diarahkan pada periode yang paling bermasalah.

Tabel 8. Ringkasan IO Graphs

Sesi	Rata-rata Paket/detik	Puncak Paket/detik	Kondisi
Sesi 1	146	312	Normal
Sesi 2	284	711	Padat
Sesi 3	168	386	Cukup stabil

Puncak trafik sebesar 711 paket/detik pada sesi kedua menunjukkan bahwa jaringan mengalami peningkatan aktivitas yang cukup tinggi. Jika lonjakan trafik terjadi secara berulang, sekolah perlu mengevaluasi kapasitas perangkat jaringan, pembagian bandwidth, serta prioritas akses layanan akademik. Analisis grafik trafik juga relevan dengan pendekatan in-band network telemetry yang menekankan pentingnya pemantauan jaringan untuk memahami kondisi performa secara lebih rinci [10].

3.7 Troubleshooting Recommendation

Berdasarkan hasil analisis ICMP, TCP, UDP, packet loss, dan IO Graphs, beberapa rekomendasi troubleshooting yang dapat dilakukan adalah sebagai berikut.

Tabel 9. Rekomendasi Troubleshooting

Temuan	Dugaan Penyebab	Rekomendasi
Response time ICMP meningkat pada sesi kedua	Kepadatan trafik	Atur pembagian bandwidth dan jadwal penggunaan laboratorium
TCP retransmission meningkat	Paket terlambat atau hilang	Periksa switch, kabel, konektor, dan beban jaringan
UDP broadcast/multicast cukup tinggi	Banyak layanan discovery atau DNS	Identifikasi perangkat sumber broadcast dan batasi layanan tidak perlu
Packet loss mencapai 6,70% pada sesi kedua	Jaringan padat atau kualitas media kurang baik	Periksa perangkat aktif, kabel UTP, dan kapasitas switch
IO Graphs menunjukkan lonjakan trafik	Penggunaan serentak	Terapkan monitoring berkala dan segmentasi jaringan

Rekomendasi tersebut menunjukkan bahwa troubleshooting tidak hanya dilakukan dengan mengganti perangkat, tetapi harus diawali dengan analisis data jaringan. Dengan Wireshark, administrator dapat memperoleh bukti teknis mengenai jenis protokol, waktu terjadinya gangguan, perangkat yang aktif, dan pola paket yang tidak normal. Pendekatan berbasis packet

analysis membantu proses troubleshooting menjadi lebih terukur dan tidak hanya berdasarkan dugaan.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa Wireshark dapat digunakan untuk menganalisis lalu lintas jaringan LAN di SMK Negeri 1 Wawo dan mendukung proses troubleshooting secara lebih sistematis. Hasil analisis menunjukkan bahwa trafik TCP mendominasi sebesar 62,40%, diikuti UDP sebesar 24,75%, ICMP sebesar 3,85%, dan protokol lain sebesar 9,00%. Analisis ICMP menunjukkan adanya peningkatan response time pada sesi penggunaan padat. Analisis TCP menunjukkan adanya retransmission dan duplicate ACK, terutama pada sesi kedua. Analisis UDP menunjukkan tingginya aktivitas DNS dan broadcast/multicast. Packet loss rata-rata sebesar 2,80% berada pada kategori cukup, tetapi packet loss tertinggi sebesar 6,70% menunjukkan adanya kondisi jaringan yang perlu diperbaiki. IO Graphs memperlihatkan lonjakan trafik tertinggi pada sesi kedua dengan puncak 711 paket/detik.

Berdasarkan temuan tersebut, jaringan LAN SMK Negeri 1 Wawo masih dapat digunakan, tetapi perlu dilakukan pemantauan dan perbaikan pada periode penggunaan padat. Rekomendasi yang diberikan meliputi pemeriksaan kabel dan switch, pengaturan bandwidth, pengurangan broadcast yang tidak diperlukan, segmentasi jaringan, serta monitoring berkala menggunakan Wireshark..

5. DAFTAR PUSTAKA

[1] Rizki Ananta, F. Firmansyah, and M. F. Hasa, "Wireshark Implementation to Monitor Security on Wifi Indihome," *Secur. Knowledge-Intelligent Res. Cybersecurity Multimed.*, vol. 3, no. 01, pp. 01–06, 2025, doi: 10.36679/s4kira.v3i1.29.

[2] F. P. Eka Putra, L. Fitriyah, Z. Naimah, and S. A. Rofika, "Evaluasi Kinerja Aplikasi Wireshark Dalam Monitoring Jaringan Kecil Dengan Topologi Star dan Bus," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 2, pp. 164–176, 2025, doi: 10.47324/ilkominfo.v8i2.343.

[3] M. Varol and M. İskefiyeli, "A low cost compact network TAP device with Raspberry Pi 4," *Eng. Sci. Technol. an Int. J.*, vol. 70, no. May, 2025, doi: 10.1016/j.jestch.2025.102118.

[4] M. O. Kaya, M. Ozdem, and R. Das, "A new hybrid approach combining GCN and LSTM for real-time anomaly detection from dynamic computer network data," *Comput. Networks*, vol. 268, no. May, p. 111372, 2025, doi: 10.1016/j.comnet.2025.111372.

[5] E. Amer, B. A. S. Al-rimy, and S. El-Sappagh, "Strengthening ICS defense: Modbus-NFA behavior model for enhanced anomaly detection," *J. Inf. Secur. Appl.*, vol. 89, no. February, p. 103990, 2025, doi: 10.1016/j.jisa.2025.103990.

[6] R. Asasunnaja and B. Sugiantoro, "Analisis Unjuk Kerja TCP Sack Menggunakan Antrian Random Early Detection," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 2, pp. 75–82, 2022, doi: 10.14421/jiska.2022.7.2.75-82.

[7] Y. Zhao *et al.*, "Protocol syntax recovery via knowledge transfer," *Comput. Networks*, vol. 258, no. December 2024, 2025, doi: 10.1016/j.comnet.2024.111022.

[8] J. A. Delgado-Soto, J. E. López de Vergara, I. González, D. Perdices, and L. de Pedro, "GPT on the wire: Towards realistic network traffic conversations generated with large language models," *Comput. Networks*, vol. 265, no. March, p. 111308, 2025, doi: 10.1016/j.comnet.2025.111308.

[9] B. Njoku *et al.*, "Quantum entanglement resource utilization in quantum-classical

networking," *Opt. Switch. Netw.*, vol. 58, no. May, p. 100829, 2025, doi: 10.1016/j.osn.2025.100829.

[10] S. Troia, J. P. Asdikian, G. Sguotti, E. Gregorini, M. Li, and G. Maier, "In-band Network Telemetry for Software-Defined Wide Area Networks," *Comput. Networks*, vol. 270, no. February, p. 111567, 2025, doi: 10.1016/j.comnet.2025.111567.