# Analisis Kinerja Jaringan *Wireless* Rumah Sakit Akademik UGM berdasarkan Parameter *QoS*

## *Analysis of Wireless Network Performance at UGM Academic Hospital based On QoS Parameter*

**[1]Rahmat Gunawan Ediyasanto*, [2]Danur Wijayanto**
[1,2]Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas 'Aisyiyah Yogyakarta
[1,2]Jl. Siliwangi (Ring Road Barat) No. 63 Nogotirto, Gamping, Sleman, Yogyakarta. 55292
*e-mail: rahmatis666@gmail.com

(***received*:** 30 July 2026, ***revised*:** 3 August 2026, ***accepted*:** 6 August 2026)

**Abstrak**

RSA UGM mengintegrasikan fungsi pelayanan kesehatan, pendidikan, dan penelitian sehingga sangat bergantung pada jaringan wireless yang andal. Namun, kinerja jaringan wireless RSA UGM kerap menurun saat pengguna mencapai kapasitas maksimum access point, terutama di area publik seperti auditorium dan ruang tunggu pasien, menyebabkan interferensi kanal, penurunan throughput, dan peningkatan waktu respons. Penelitian ini menganalisis kinerja jaringan berdasarkan parameter Quality of Service (QoS) sekaligus mengintegrasikan pendekatan forensik digital untuk membedakan lonjakan trafik pengguna sah (flash crowd) dari serangan Distributed Denial of Service (DDoS). Metode yang digunakan adalah Action Research, meliputi diagnosis, perencanaan, pelaksanaan tindakan, dan evaluasi. Pengukuran QoS dilakukan menggunakan iPerf3 dan Wireshark/tcpdump selama tiga hari pada tiga sesi waktu, disertai simulasi serangan SYN Flood di laboratorium yang mereplikasi topologi jaringan rumah sakit. Parameter QoS dianalisis menggunakan Standar TIPHON (throughput, packet loss, delay, jitter), sementara integritas bukti digital diverifikasi melalui hashing SHA-256 dan chain of custody. Hasil menunjukkan bahwa pada kondisi normal (11 sampel), throughput berkisar 9.877,75–23.452,12 Kbps dengan Indeks TIPHON 4,00 (sangat baik); pada flash crowd, throughput melonjak hingga 104.602,77 Kbps namun parameter lain tetap stabil sehingga indeks tetap 4,00; sedangkan pada serangan DDoS (7 sampel), packet loss meningkat drastis hingga 42,64%, delay dan jitter meningkat signifikan, sehingga Indeks TIPHON turun menjadi 3,25–3,75. Temuan ini mengungkap bahwa throughput saja tidak cukup membedakan flash crowd dan serangan DDoS, sedangkan packet loss menjadi parameter pembeda paling signifikan. Seluruh 19 barang bukti digital (C-01–C-19) dinyatakan match pada verifikasi hash SHA-256, membuktikan integritas data tetap terjaga. Penelitian ini menyimpulkan bahwa integrasi analisis QoS berbasis Standar TIPHON dengan forensik digital mampu mendukung deteksi dini dan investigasi insiden keamanan jaringan secara akurat, khususnya pada lingkungan rumah sakit yang menuntut keandalan tinggi.
**Kata kunci:** *Digital Forensik, DdoS, RSA UGM, TIPHON, Jaringan Wireless, QoS*

***Abstract***

*RSA UGM integrates healthcare, education, and research services, making it highly dependent on reliable wireless network infrastructure. However, the performance of the RSA UGM wireless network often deteriorates when user demand approaches the maximum capacity of access points, particularly in public areas such as auditoriums and patient waiting rooms. This condition may result in channel interference, reduced throughput, and increased response times. This study analyzes wireless network performance based on Quality of Service (QoS) parameters while integrating a digital forensics approach to distinguish legitimate user traffic surges (flash crowds) from Distributed Denial-of-Service (DDoS) attacks. The study employs an Action Research methodology consisting of diagnosis, planning, action implementation, and evaluation. QoS measurements were conducted using iPerf3 and Wireshark/tcpdump over three days across three time sessions, accompanied by a SYN Flood attack simulation in a laboratory environment replicating the hospital network topology. QoS parameters were analyzed based on the TIPHON standard, including throughput, packet loss, delay,*

 ISSN:2302-8149
e-ISSN:2540-9719

*and jitter, while the integrity of digital evidence was verified using SHA-256 hashing and a chain-of-custody procedure. The results show that under normal conditions (11 samples), throughput ranged from 9,877.75 to 23,452.12 Kbps, with a TIPHON Index of 4.00, indicating very good performance. Under flash crowd conditions, throughput increased sharply to 104,602.77 Kbps, while the other QoS parameters remained stable, resulting in a TIPHON Index of 4.00. In contrast, during the DDoS attack condition (7 samples), packet loss increased substantially to 42.64%, accompanied by significant increases in delay and jitter, causing the TIPHON Index to decline to 3.25–3.75. These findings indicate that throughput alone is insufficient to distinguish between flash crowds and DDoS attacks, whereas packet loss represents the most significant distinguishing parameter. All 19 digital evidence items (C-01–C-19) matched during SHA-256 hash verification, demonstrating that data integrity was preserved throughout the investigation. The study concludes that integrating TIPHON-based QoS analysis with digital forensics can support early detection and accurate investigation of network security incidents, particularly in hospital environments where high network reliability is essential.*
***Keywords:*** *Digital Forensics, DdoS, RSA UGM, TIPHON, Wireless Network, QoS*

## 1 Pendahuluan

Rumah Sakit Akademik Universitas Gadjah Mada (RSA UGM) merupakan salah satu rumah sakit pendidikan utama yang berperan dalam menunjang kegiatan pelayanan kesehatan, pendidikan, dan penelitian Fakultas Kedokteran Universitas Gadjah Mada. Jaringan yang digunakan harus mampu menopang kebutuhan operasional sistem informasi rumah sakit seperti rekam medis elektronik, telemedicine, serta aplikasi pendukung pelayanan kesehatan lainnya. Selain itu, jaringan juga harus dapat mengakomodasi kebutuhan akademik, seperti pembelajaran daring, riset berbasis data, dan kegiatan konferensi virtual. Sebagai institusi yang mengintegrasikan tiga fungsi utama tersebut, RSA UGM menghadapi tantangan dalam penyediaan infrastruktur jaringan wireless yang handal, stabil, dan efisien.

Salah satu tantangan nyata yang dihadapi adalah permasalahan jaringan wireless ketika jumlah pengguna mencapai kapasitas maksimum access point. Kondisi ini terjadi di area publik seperti auditorium dan ruang tunggu pasien, di mana banyak perangkat terkoneksi secara bersamaan. Lonjakan jumlah koneksi menyebabkan terjadinya interferensi kanal, penurunan throughput, serta meningkatnya waktu respons jaringan. Hal ini tidak hanya mengganggu kenyamanan pengguna, tetapi juga berpotensi menghambat layanan kritis rumah sakit yang membutuhkan koneksi stabil dan real-time.

Dengan adanya berbagai kendala tersebut, pengelolaan jaringan menjadi semakin kompleks dan memerlukan pendekatan yang tidak hanya berfokus pada pemantauan performa, tetapi juga pada penerapan standar kualitas layanan (*Quality of Service*/QoS) serta pemahaman mendalam mengenai bagaimana jaringan bekerja dan faktor-faktor teknis yang memengaruhinya. Pemahaman ini menjadi landasan penting dalam memastikan bahwa jaringan mampu mendukung kebutuhan operasional dan komunikasi digital di lingkungan rumah sakit.

Tantangan ini semakin nyata mengingat semakin banyaknya perangkat bergerak yang terhubung di lingkungan rumah sakit, sehingga kebutuhan akan jaringan wireless yang stabil dan merata menjadi sangat penting. Konektivitas yang tidak stabil dapat berdampak pada keterlambatan akses data medis, gangguan komunikasi antar tenaga kesehatan, hingga terganggunya proses pembelajaran dan penelitian. Oleh karena itu, penelitian ini berfokus pada analisis kinerja jaringan wireless di lingkungan Rumah Sakit Akademik Universitas Gadjah Mada menggunakan parameter QoS (*Quality of Service*). Hasil penelitian diharapkan dapat menjadi acuan dalam pengembangan dan perencanaan jaringan wireless yang lebih andal, efisien, dan mampu mendukung pelayanan kesehatan serta kegiatan akademik di RSA UGM secara optimal.

Sejumlah penelitian terdahulu telah membahas analisis QoS pada jaringan wireless di berbagai institusi, namun sebagian besar berfokus pada evaluasi performa jaringan secara umum tanpa mengaitkannya dengan aspek forensik digital. Sebagai contoh, penelitian Damanik dkk. dan Morib dkk. mengukur QoS pada jaringan kampus, tetapi penurunan performa yang ditemukan tidak

 ISSN:2302-8149
e-ISSN:2540-9719

diverifikasi lebih lanjut untuk memastikan apakah penyebabnya murni kepadatan pengguna atau berpotensi merupakan indikasi serangan siber. Penelitian mengenai jaringan wireless di lingkungan rumah sakit juga masih terbatas dan umumnya hanya membahas evaluasi performa jaringan secara deskriptif [1],[2]. Padahal lingkungan rumah sakit memiliki karakteristik beban trafik dan tuntutan keandalan yang berbeda dari lingkungan kampus maupun perkantoran. Kesenjangan inilah yang mendasari penelitian ini, yaitu belum adanya kajian yang mengintegrasikan analisis QoS berbasis Standar TIPHON dengan pendekatan forensik digital untuk membedakan lonjakan trafik pengguna sah dari serangan DDoS pada lingkungan rumah sakit. Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk menganalisis kinerja jaringan wireless RSA UGM berdasarkan parameter QoS Standar TIPHON pada kondisi normal, flash crowd, dan serangan DDoS. Dan mengintegrasikan prosedur forensik digital berupa hashing SHA-256 dan chain of custody guna menjamin integritas bukti serta mendukung deteksi dini insiden keamanan jaringan di lingkungan rumah sakit.

## 2 Tinjauan Literatur

### 2.1 Jaringan Komputer

Dalam konteks teknis, jaringan komputer dapat diartikan sebagai suatu sistem yang menghubungkan dua atau lebih perangkat komputasi untuk memungkinkan pertukaran informasi dan berbagi sumber daya, baik melalui media transmisi kabel (*wired*) maupun tanpa kabel (*wireless*). Interkoneksi ini memungkinkan berbagai layanan kolaboratif seperti berbagi data, penggunaan aplikasi terpusat, hingga komunikasi digital secara real time [3]. Prinsip otonomi pada jaringan menunjukkan bahwa setiap perangkat dalam jaringan beroperasi secara independen tanpa kontrol langsung terhadap perangkat lainnya.

### 2.2 Quality of Service (QoS)

Seiring meningkatnya kebutuhan terhadap akses jaringan yang cepat dan stabil, efisiensi sistem jaringan harus dijaga agar performa tetap optimal. Salah satu pendekatan yang digunakan untuk memastikan kualitas jaringan adalah melalui analisis *Quality of Service* (QoS) [4]. QoS merupakan ukuran tingkat kualitas suatu jaringan, di mana pengguna dapat merasakan performa yang lebih baik melalui mekanisme manajemen lalu lintas data, pengaturan prioritas, serta peningkatan parameter-parameter teknis jaringan seperti throughput, packet loss, delay, dan jitter. Analisis QoS memungkinkan pengelola jaringan untuk memahami kondisi aktual performa jaringan dan melakukan optimalisasi berdasarkan hasil pengukuran yang diperoleh [5].

### 2.3 Teknologi Jaringan Wireless

Selain aspek pengukuran kualitas layanan, pemahaman terhadap teknologi jaringan wireless yang digunakan turut menjadi bagian penting dari kerangka analisis. Salah satu teknologi jaringan wireless yang paling umum digunakan adalah *Wireless Fidelity* (Wi-Fi). Jaringan wireless beroperasi pada pita frekuensi 2.4 GHz dan 5 GHz, dan telah berkembang melalui berbagai standar IEEE 802.11 seperti 802.11b/g/n/ac hingga generasi terbaru IEEE 802.11ax yang dirancang untuk menyediakan efisiensi tinggi pada lingkungan pengguna padat [6]. Setiap evolusi standar tersebut membawa peningkatan signifikan dalam hal kecepatan transfer data, efisiensi penggunaan kanal frekuensi, serta kemampuan melayani lebih banyak pengguna secara simultan. Teknologi seperti *Multiple Input Multiple Output* (MIMO) dan *Multi-User MIMO* (MU-MIMO) juga telah diterapkan untuk meningkatkan throughput dan efisiensi transmisi sinyal [7].

## 3 Metode Penelitian

Dalam penelitian ini digunakan metode Action Research, yaitu pendekatan yang tidak hanya dipahami sebagai kegiatan ilmiah, tetapi juga sebagai proses pelaksanaan tindakan nyata yang bertujuan untuk memperbaiki, memahami, serta mengevaluasi suatu permasalahan secara langsung di lapangan [8]. Metode Action Research mempunyai beberapa tahapan yaitu:

### 3.1 Melakukan Diagnosa

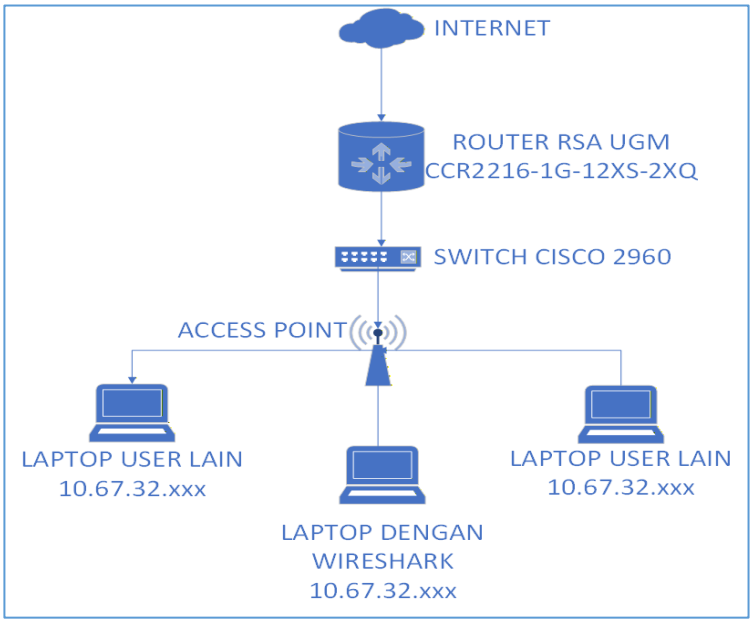
Penelitian ini diawali dengan tahap diagnosis. Tahap ini mencakup proses pemahaman terhadap konteks permasalahan, konsultasi dengan para pemangku kepentingan, analisis terhadap data

 ISSN:2302-8149
e-ISSN:2540-9719

pendukung, serta observasi awal untuk memvalidasi temuan di lapangan, dengan tujuan merumuskan permasalahan utama yang berkaitan dengan kualitas layanan di RSA UGM. Konsultasi dengan para pemangku kepentingan di RSA UGM mengidentifikasi satu masalah utama, yaitu latensi yang meningkat ketika jumlah pengguna mencapai kapasitas maksimum access point. Kondisi ini menyebabkan koneksi client pada ruangan tersebut menjadi lambat. Temuan ini kemudian menjadi dasar dalam merumuskan fokus penelitian untuk mengevaluasi serta mengoptimalkan performa jaringan wireless di RSA UGM.

### 3.2 Tindakan Perencanaan

Pada tahap ini, peneliti menyusun rencana penelitian yang mencakup serangkaian langkah sistematis, antara lain melakukan pencarian referensi dari berbagai jurnal yang relevan dengan metode yang digunakan, menentukan pendekatan penelitian kuantitatif, serta menyiapkan prosedur pengumpulan data yang akan digunakan sebagai dasar dalam proses analisis. Pada tahap ini SSID jaringan wireless yang akan diteliti yaitu SSID UGM-Hotspot. SSID ini menerapkan login menggunakan akun email UGM, oleh karena itu pengguna harus memiliki akun email UGM atau akun khusus untuk tamu atau pasien yang dapat dibuat oleh pegawai TI RSA UGM. Untuk skema jaringan yang sekarang ada dan berjalan seperti berikut:




**Gambar 1 Skema jaringan di RSA UGM**

Skema pada Gambar 1 menggambarkan arsitektur jaringan wireless RSA UGM dalam kondisi operasional sehari-hari, mulai dari koneksi internet yang masuk ke infrastruktur jaringan rumah sakit, diteruskan melalui access point dengan SSID UGM-Hotspot, hingga terhubung ke perangkat pengguna (client) seperti laptop, smartphone, dan perangkat pendukung layanan kesehatan lainnya. Skema ini menjadi acuan dalam merancang skenario pengukuran QoS maupun simulasi serangan pada tahap penelitian selanjutnya, sehingga kondisi jaringan yang diuji tetap merepresentasikan kondisi nyata di lapangan.

Penelitian ini dirancang dalam dua skenario yaitu: (1) Skenario Lapangan (RSA UGM): Pengukuran QoS aktual pada kondisi normal dan padat pengguna di lingkungan RSA UGM, (2) Skenario Laboratorium (Simulasi Forensik): Simulasi serangan DDoS yang mereplikasi konfigurasi jaringan RSA UGM, untuk memperoleh pola QoS khas dari serangan. Baik pada skenario lapangan maupun skenario laboratorium, infrastruktur jaringan yang digunakan disusun agar merepresentasikan kondisi nyata RSA UGM. Pada masing-masing skenario digunakan dua unit access point Unifi U6-Pro dengan SSID UGM-Hotspot yang terhubung pada koneksi internet berkapasitas 1 Gbps (1000 Mbps), access point dikonfigurasi pada kanal (channel) 1, 6, dan 11 untuk pita frekuensi 2,4 GHz, serta kanal 149, 153, 157, dan 161 untuk pita frekuensi 5 GHz, guna meminimalkan tumpang tindih kanal (co-channel interference) antar access point yang berdekatan. Secara keseluruhan, jaringan

 ISSN:2302-8149
e-ISSN:2540-9719

wireless RSA UGM melayani sekitar 1.600 pengguna aktif terdaftar, sedangkan pada area pengukuran (ruang manajemen) yang menjadi fokus penelitian ini, jumlah client yang terkoneksi secara bersamaan pada saat pengukuran berkisar 60 pengguna. Rasio antara jumlah client aktif dengan kapasitas layanan access point pada area tersebut menjadi salah satu faktor yang memengaruhi terjadinya kepadatan trafik ketika kapasitas maksimum access point tercapai.

### 3.3 Melakukan Tindakan

Tahap tindakan dibagi menjadi dua sub-tahap: pengukuran di lapangan dan simulasi di laboratorium.

#### 3.3.1 Pengukuran QoS di Lingkungan RSA UGM

Pengambilan data dilakukan di lingkungan rumah sakit, khususnya pada area-area dengan tingkat aktivitas tinggi seperti ruang manajemen. Pengukuran dilakukan selama tiga hari pada tiga sesi waktu: Pagi (09.00 – 10.00 WIB), Siang (12.00 – 13.00 WIB), dan Sore (16.00 – 17.00 WIB). Pemilihan tiga sesi waktu (pagi, siang, dan sore) bertujuan untuk merepresentasikan siklus dinamis beban kerja manajemen rumah sakit secara komprehensif. Sesi pagi (09.00–10.00) dipilih sebagai periode puncak koordinasi dan administrasi pasca-briefing shift, sesi siang (12.00–13.00) mewakili fase transisi antar-shift serta rekapitulasi data paruh waktu dengan tingkat multitasking tinggi, sedangkan sesi sore (16.00–17.00) mencakup fase penutupan, finalisasi laporan harian, dan persiapan handover yang biasanya diiringi lonjakan sinkronisasi data akhir. Durasi satu jam per sesi diterapkan untuk memperoleh sampel data yang stabil dan spesifik, sementara pengulangan selama tiga hari bertujuan mengakomodasi variasi beban kerja antarhari (misalnya awal, tengah, dan akhir pekan), sehingga hasil pengukuran menjadi representatif dan tidak terpengaruh oleh kondisi anomali pada satu hari tertentu.

Perangkat yang digunakan adalah laptop Lenovo ROG Intel i5-13450HX. Berbeda dengan pendekatan konvensional, penelitian ini tidak menggunakan Speedtest Ookla karena keterbatasan dalam hal integritas data (server di luar kendali peneliti dan hasil berupa grafik yang mudah dimanipulasi). Sebagai gantinya, pengukuran dilakukan menggunakan: (1) iPerf3 dengan server lokal yang dikendalikan peneliti untuk mengukur throughput dan jitter secara akurat. (2) Wireshark dan tcpdump untuk full packet capture (PCAP) pada setiap sesi pengukuran.

#### 3.3.2 Skenario Serangan di Laboratorium (Forensik)

Untuk memenuhi aspek digital forensik, penelitian ini melakukan simulasi serangan pada lingkungan laboratorium terisolasi yang mereplikasi konfigurasi jaringan RSA UGM. Topologi laboratorium disusun sebagai berikut:

- 1 Laptop Host (Fisik): Berfungsi sebagai titik *capture* tunggal dengan *monitor mode* pada antarmuka jaringan wireless internal.
- VM1 (Ubuntu Server): Sebagai server target (IP: 10.67.28.159) yang menjalankan layanan web dan iPerf3 server.
- VM2 (Kali Linux): Sebagai *attacker* dengan USB wireless adapter *passthrough* untuk mengirim serangan.
- PC Windows: Sebagai *legitimate user* yang menjalankan JMeter untuk simulasi *flash crowd*.
- Access Point Fisik: Menyediakan koneksi wireless dengan SSID "UGM-Hotspot".

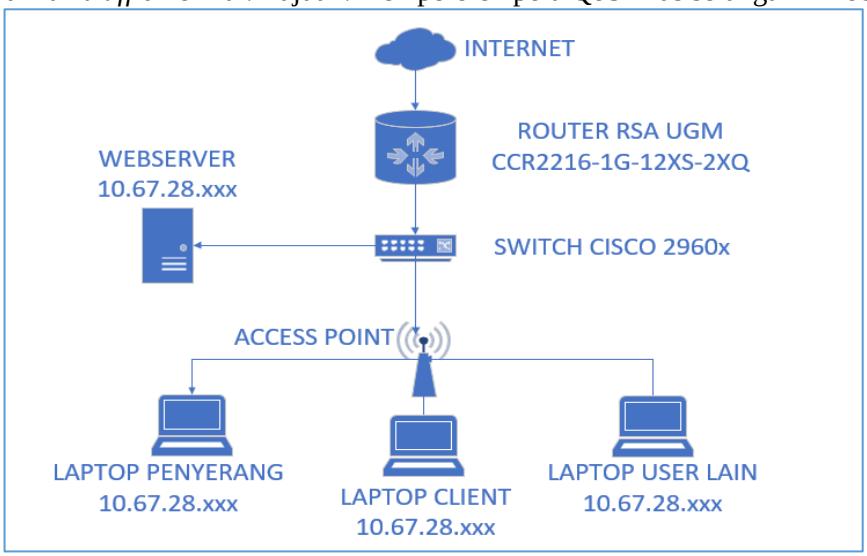
Seluruh perangkat terhubung ke *access point* fisik yang sama pada kanal yang sama, sehingga laptop host dalam mode *monitor* dapat merekam semua *traffic wireless* yang melewati kanal tersebut dalam satu file PCAP tunggal. Dua Skenario dijalankan berurutan dalam durasi masing – masing 1 Jam:

- Skenario 1:
  PC Windows menjalankan *ping* normal dan iPerf3 dengan VM1. Tidak ada serangan dari VM2. Tujuan: memperoleh pola QoS normal sebagai *baseline* perbandingan. Kemudian PC Windows menjalankan JMeter dengan 50 *thread* paralel untuk

 ISSN:2302-8149
e-ISSN:2540-9719

mengakses layanan web di VM1, mensimulasikan lonjakan pengguna sah. VM2 dalam kondisi diam. Tujuan: memperoleh pola QoS akibat kelebihan kapasitas normal.

- Skenario 2:
  VM2 menjalankan hping3 dengan perintah sudo hping3 -S -p 80 --flood --rand-source 10.67.28.159 untuk mengirimkan serangan SYN Flood ke VM1. PC Windows tetap menjalankan *traffic* normal. Tujuan: memperoleh pola QoS khas serangan DDoS.




**Gambar 2 Skema jaringan simulasi laboratorium di RSA UGM**

Gambar 2 menunjukkan topologi jaringan pada lingkungan laboratorium yang dirancang untuk mereplikasi kondisi jaringan RSA UGM secara terisolasi. Seluruh perangkat, yaitu Laptop Host sebagai titik capture, VM1 sebagai server target, VM2 sebagai attacker, dan PC Windows sebagai pengguna sah, terhubung pada access point fisik yang sama dengan SSID UGM-Hotspot dan berada pada kanal yang sama. Konfigurasi ini memungkinkan Laptop Host merekam seluruh lalu lintas data dalam satu berkas PCAP tunggal, sehingga pola QoS pada kondisi normal, flash crowd, maupun serangan DDoS dapat dibandingkan secara konsisten dari satu sumber data yang sama.

### 3.3.3 Prosedur capture dan preservasi bukti digital

Untuk memenuhi prinsip digital forensik, setiap sesi *capture* mengikuti prosedur berikut:

- Sinkronisasi waktu.
- Buka Wireshark dan setup monitor settingnya.
- Memulai capture dengan Wireshark.
- Hashing (SHA-256): Setelah setiap sesi *capture* selesai, file PCAP dihitung nilai hash SHA-256-nya
- Chain of Custody Log: dicatat dalam tabel log yang berisi: *timestamp*, investigator, lokasi, jenis skenario, hash file, dan tindakan yang dilakukan.

### 3.3.4 Perbedaan Network Monitoring dan Network Forensics

Penting untuk membedakan antara *Network Monitoring* dan *Network Forensics*. *Network Monitoring* bertujuan untuk pemantauan performa secara real-time atau periodik, seperti deteksi penurunan throughput atau kenaikan latensi karena kelebihan kapasitas. *Network Forensics*, di sisi lain, adalah proses pengumpulan, preservasi, dan analisis bukti digital dari jaringan setelah terjadi insiden (NIST SP 800-86) [9]. Forensik memerlukan pemicu berupa insiden keamanan (misalnya serangan *DDoS*, *deauthentication*, atau *ARP spoofing*), serta prosedur *Chain of Custody* untuk menjaga integritas bukti, sebagaimana diterapkan pada penelitian forensik jaringan sebelumnya yang mengombinasikan pengukuran performa dengan investigasi bukti digital [10], [11], [12]. Penelitian ini mengintegrasikan kedua pendekatan: pengukuran QoS sebagai baseline performa, dan simulasi

 ISSN:2302-8149
e-ISSN:2540-9719

serangan di laboratorium sebagai skenario forensik untuk membandingkan pola QoS antara kondisi normal, flash crowd, dan serangan.

### 3.4 Melakukan Evaluasi

Pada tahap ini, peneliti melakukan evaluasi terhadap hasil yang diperoleh dari pengujian performa jaringan *wireless* berdasarkan parameter *Quality of Service (QoS)*. Data hasil pengukuran kemudian dianalisis dengan menggunakan parameter *QoS Standar TIPHON*. *Standar TIPHON*(Telecommunications and Internet Protocol Harmonization Over Networks) merupakan standar evaluasi parameter *Quality of Service (QoS)* yang dikembangkan dan diterbitkan oleh European Telecommunications Standards Institute (ETSI). Standar ini berfungsi sebagai acuan dalam pengukuran dan penilaian kualitas layanan jaringan berbasis protokol internet maupun telekomunikasi, sehingga memungkinkan terciptanya keseragaman dalam evaluasi performansi jaringan di berbagai lingkungan sistem komunikasi, sebagaimana diterapkan pada berbagai studi kasus jaringan wireless terkini [13], [14], [15], [16], [17]. Berikut Tabel 1 standar QoS berdasarkan parameter menurut *Telecommunications and Internet Protocol Harmonization Over Networks:*

**Tabel 1 Standar QoS TIPHON**

| Kategori | Persentase | Indeks |
|---|---|---|
| Sangat Bagus | 95 - 100 | 4 |
| Bagus | 75 – 94,75 | 3 |
| Sedang | 50 – 74,75 | 2 |
| Jelek | 25 – 49,75 | 1 |

*a.* *Throughput* merupakan representasi dari *bandwidth* aktual yang dapat terukur pada rentang waktu tertentu ketika proses pengunduhan atau pengiriman data berlangsung dengan ukuran berkas tertentu. Meskipun memiliki satuan yang sama dengan *bandwidth*, yaitu bits per second (bps), *throughput* menggambarkan kapasitas efektif jaringan yang benar-benar digunakan untuk mentransfer data [18]. *Throughput* dapat dianggap sebagai representasi nyata dari *bandwidth* yang benar-benar digunakan dalam kondisi operasional jaringan. Menghitung nilai *throughput* digunakan persamaan (1):

$$Throughput = \frac{Bytes}{Time\ Span} \quad (1)$$

Berikut Tabel 2 standar QoS berdasarkan Throughput dalam bentuk % menurut *Telecommunications and Internet Protocol Harmonization Over Networks*:

**Tabel 2 Standar tabel throughput**

| Kategori | Throughput | Indeks |
|---|---|---|
| Sangat Bagus | 100 | 4 |
| Bagus | 75 | 3 |
| Sedang | 50 | 2 |
| Jelek | < 25 | 1 |

*b.* *Packet Loss* merupakan salah satu parameter penting yang digunakan untuk menunjukkan jumlah total paket data yang hilang selama proses transmisi dalam suatu jaringan. Kondisi ini dapat terjadi akibat berbagai faktor, salah satunya adalah kapasitas *buffer* yang berlebihan pada setiap *node*, yang menyebabkan sebagian paket tidak dapat diteruskan dan akhirnya terbuang [19]. Untuk Menghitung nilai *Packet Loss* digunakan persamaan (2):

$$Packet\ loss = \frac{(Paket\ dikirim - paket\ diterima)}{Paket\ dikirim} x\ 100\% \quad (2)$$

 ISSN:2302-8149
e-ISSN:2540-9719

Berikut Tabel 3 standar QoS berdasarkan Packet loss dalam bentuk % menurut *Telecommunications and Internet Protocol Harmonization Over Networks:*

**Tabel 3 Standar tabel packet loss**

| Kategori | Packet loss | Indeks |
|---|---|---|
| Sangat Bagus | 0% | 4 |
| Bagus | ≥ 3 % | 3 |
| Sedang | ≥ 15 % | 2 |
| Jelek | ≥ 25 % | 1 |

*c.* Delay merupakan waktu yang dibutuhkan oleh suatu paket data untuk menempuh perjalanan dari sumber ke tujuan dalam jaringan. Besarnya nilai delay dipengaruhi oleh berbagai faktor, seperti jarak transmisi, jenis media fisik yang digunakan, tingkat kongesti jaringan, serta waktu pemrosesan pada setiap node [20]. Nilai delay dapat dihitung menggunakan persamaan (3) sebagai berikut:

$$Delay = \frac{Total\ Delay}{Paket\ data\ yang\ diterima} \quad (3)$$

Berikut Tabel 4 standar QoS berdasarkan Delay dalam bentuk millisecond menurut *Telecommunications and Internet Protocol Harmonization Over Networks:*

**Tabel 4 Standar tabel delay**

| Kategori | Delay | Indeks |
|---|---|---|
| Sangat Bagus | < 150 ms | 4 |
| Bagus | 150 ms – 300 ms | 3 |
| Sedang | 300 ms – 450 ms | 2 |
| Jelek | > 450 ms | 1 |

*d.* *Jitter*, yang juga dikenal sebagai variasi delay, merupakan perbedaan waktu tunda (delay) antara satu paket data dengan paket berikutnya selama proses transmisi berlangsung. Besarnya variasi delay ini dapat memengaruhi kualitas data yang ditransmisikan, terutama pada layanan yang bersifat real-time seperti *video streaming* dan *voice over IP (VoIP)*. Selain itu, *buffer jitter* memiliki peran penting dalam menentukan tingkat toleransi jaringan terhadap variasi *delay* tersebut. Dengan kata lain, semakin besar kapasitas *buffer jitter* yang tersedia, maka semakin baik kemampuan jaringan dalam mereduksi dampak *jitter*. Nilai *jitter* dapat dihitung menggunakan persamaan (4) sebagai berikut:

$$Jitter = \frac{Total\ Variasi\ Delay}{Paket\ data\ yang\ diterima - 1} \quad (4)$$

Berikut Tabel 5 standar QoS berdasarkan Jitter menurut *Telecommunications and Internet Protocol Harmonization Over Networks:*

**Tabel 5 Standar tabel jitter**

| Kategori | Delay | Indeks |
|---|---|---|
| Sangat Bagus | < 150 ms | 4 |
| Bagus | 150 ms – 300 ms | 3 |
| Sedang | 300 ms – 450 ms | 2 |
| Jelek | > 450 ms | 1 |

 ISSN:2302-8149
e-ISSN:2540-9719

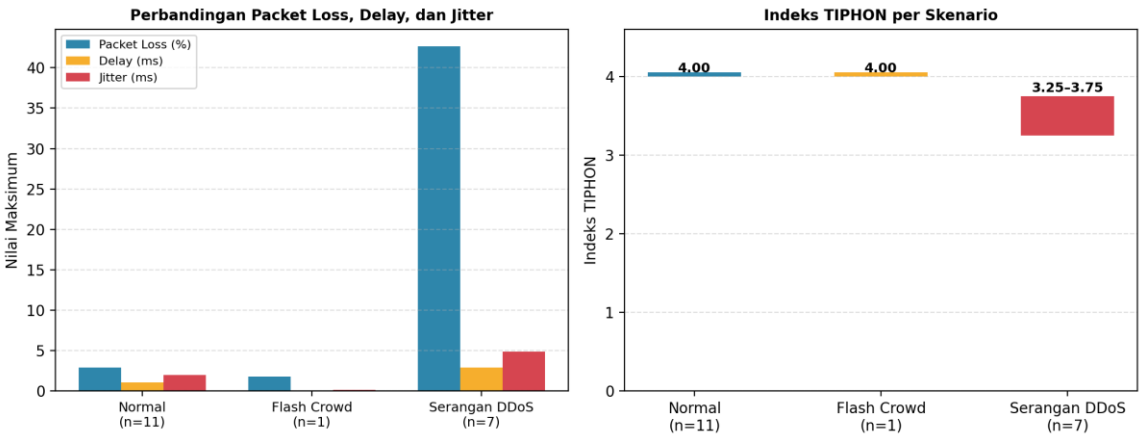
# 4 Hasil dan Pembahasan

## 4.1 Hasil Pengukuran QoS di RSA UGM

Pengukuran QoS pada jaringan wireless dilakukan pada skenario: lalu lintas normal, flash crowd, serta skenario serangan DDoS, dengan parameter throughput, packet loss, delay, jitter, dan indeks TIPHON. Hasil menunjukkan bahwa setiap pola lalu lintas menghasilkan karakteristik QoS yang berbeda. Pada kondisi normal, throughput berkisar 9.877,75–23.452,12 Kbps, packet loss 0,04–2,90%, delay 0,08–1,03 ms, dan jitter 0,13–1,98 ms, dengan Indeks TIPHON 4,00 (sangat baik). Pada skenario flash crowd, throughput meningkat hingga 104.602,77 Kbps, namun parameter lain tetap stabil (PL 1,77%, delay 0,08 ms, jitter 0,13 ms), sehingga indeks TIPHON tetap 4,00. Sebaliknya, pada serangan DDoS terjadi perubahan signifikan: throughput fluktuatif (384,86–148.123,91 Kbps), packet loss meningkat drastis hingga 42,64%, delay maksimum 2,89 ms, dan jitter maksimum 4,90 ms. Kondisi ini menurunkan Indeks TIPHON menjadi 3,25–3,75, mengindikasikan penurunan kualitas layanan jaringan. Ringkasan nilai-nilai parameter QoS pada ketiga skenario tersebut disajikan pada Tabel 6.

**Tabel 6 Rekapitulasi pengukuran QoS berdasarkan skenario**

| Parameter | Normal | Flash crowd | Serangan |
|---|---|---|---|
| Jumlah Sampel | 11 | 1 | 7 |
| Throughput (Kbps) | 9.877,75–23.452 Kbps | 104.602,77 Kbps | 384,86–148.124 Kbps |
| Packet Loss (%) | 0,04–2,90 % | 1,77 % | 1,17–42,64 % |
| Delay (ms) | 0,08–1,03 ms | 0,08 ms | 0,04–2,89 ms |




**Gambar 3. Perbandingan parameter QoS (packet loss, delay, jitter, dan indeks TIPHON) antar skenario**

Gambar 3 memvisualisasikan perbandingan nilai packet loss, delay, dan jitter, serta rentang Indeks TIPHON pada ketiga skenario pengujian (normal, flash crowd, dan serangan DDoS). Grafik batang pada sisi kiri menunjukkan bahwa ketiga parameter tersebut relatif rendah dan stabil pada kondisi normal maupun flash crowd, namun melonjak tajam pada skenario serangan DDoS, terutama pada packet loss. Grafik pada sisi kanan memperlihatkan bahwa Indeks TIPHON tetap berada pada kategori sangat baik (4,00) selama kondisi normal dan flash crowd, tetapi menurun ke rentang 3,25–3,75 saat terjadi serangan DDoS. Hasil pengujian menunjukkan bahwa throughput tidak dapat dijadikan indikator tunggal untuk membedakan skenario flash crowd dan serangan DDoS, karena kedua kondisi tersebut sama-sama menunjukkan peningkatan throughput yang signifikan. Perbedaan antara kedua skenario justru terlihat pada parameter QoS lainnya. Pada flash crowd, peningkatan throughput diikuti oleh nilai packet loss, delay, dan jitter yang tetap rendah, mengindikasikan bahwa lonjakan trafik berasal dari permintaan pengguna sah (legitimate traffic) sehingga jaringan masih mampu melayani tanpa degradasi berarti. Sebaliknya, pada serangan DDoS, peningkatan throughput

 ISSN:2302-8149
e-ISSN:2540-9719

disertai dengan lonjakan packet loss yang sangat tinggi, dan pada beberapa kasus throughput justru menurun drastis akibat kelebihan beban sumber daya. Parameter packet loss terbukti menjadi indikator pembeda yang paling signifikan, dengan nilai 1,77% pada flash crowd dan 42,64% pada serangan DDoS. Nilai jitter dan delay yang lebih tinggi selama serangan juga mengindikasikan ketidakstabilan waktu pengiriman paket akibat queue congestion. Secara teknis, kondisi ini dapat dijelaskan dari sisi kapasitas infrastruktur: dengan hanya 2 access point yang melayani sekitar 60 client secara bersamaan pada area pengukuran, beban rata-rata tiap access point berada pada kisaran 30 client, yang secara teoritis masih berada dalam batas wajar kapasitas access point modern seperti Unifi U6-Pro. Namun demikian, kedua access point tersebut dikonfigurasi pada kanal 1, 6, dan 11 (2,4 GHz) serta 149, 153, 157, dan 161 (5 GHz) yang bersifat non-overlapping, sehingga interferensi antar-kanal (co-channel interference) dapat diminimalkan dan penurunan throughput yang teramati pada kondisi normal maupun flash crowd lebih disebabkan oleh kontensi akses medium (channel contention) antar client dalam satu kanal yang sama, bukan oleh tumpang tindih kanal.

Pada serangan DDoS, sebaliknya, paket SYN Flood yang dikirimkan secara masif membanjiri kapasitas pemrosesan pada sisi server (VM1) dan jalur uplink menuju internet berkapasitas 1 Gbps, sehingga terjadi antrean paket (queue) yang berlebihan pada buffer perangkat jaringan. Kondisi inilah yang menyebabkan packet loss meningkat tajam hingga 42,64% serta delay dan jitter ikut memburuk, sekalipun kapasitas access point dan bandwidth internet secara nominal masih mencukupi untuk trafik pengguna normal. Dengan kata lain, penurunan QoS pada skenario serangan DDoS bersifat volumetrik dan disengaja (menyerang kapasitas pemrosesan), berbeda dengan flash crowd yang murni disebabkan oleh peningkatan jumlah permintaan pengguna sah dalam batas kapasitas jaringan yang tersedia. Dari perspektif digital forensik, perubahan nilai QoS dapat dimanfaatkan sebagai indikator awal deteksi anomali jaringan. Pola normal dan flash crowd menghasilkan kualitas layanan optimal, namun flash crowd ditandai peningkatan throughput tanpa degradasi QoS. Sebaliknya, serangan DDoS menunjukkan pola berbeda: fluktuasi throughput, packet loss tinggi, peningkatan jitter, dan penurunan indeks TIPHON.

Karakteristik ini menjadi dasar pembeda antara lonjakan trafik pengguna sah dan serangan. Hasil ini menegaskan bahwa integrasi QoS dengan forensik digital tidak hanya mengevaluasi kualitas jaringan, tetapi juga mendukung deteksi dini dan investigasi insiden di lingkungan rumah sakit. Temuan ini juga sejalan dengan hasil penelitian serupa yang dilakukan di lingkungan kampus lain. Penelitian Damanik et al. (2022) pada jaringan WLAN Universitas Papua menunjukkan bahwa nilai throughput hanya berada pada kategori sedang, sedangkan delay dan jitter justru tergolong baik hingga sangat baik. Hal ini mengindikasikan bahwa keterbatasan kapasitas access point lebih berpengaruh terhadap throughput dibandingkan terhadap parameter waktu pengiriman paket. Temuan yang serupa juga dilaporkan oleh Morib et al. (2025) di Universitas Sepuluh Nopember Papua, di mana kualitas jaringan yang sangat baik pada jam sepi (dengan packet loss 0%) berubah signifikan menjadi 86,21% pada jam sibuk akibat tingginya jumlah pengguna biasa, tanpa disertai adanya indikasi serangan siber. Kedua penelitian tersebut menegaskan bahwa lonjakan packet loss yang tinggi tidak selalu mencerminkan adanya insiden keamanan jaringan. Oleh karena itu, verifikasi forensik terhadap file PCAP sebagaimana dilakukan dalam penelitian ini menjadi langkah penting untuk membedakan antara kepadatan trafik yang wajar dengan pola anomali yang mengindikasikan adanya serangan siber.

### 4.2 Chain of Custody dan Integritas Bukti Digital

Tabel 7 menyajikan log chain of custody untuk seluruh barang bukti digital yang dikumpulkan selama periode pengambilan data, mencakup identitas bukti (ID), tanggal dan sesi waktu pengambilan, nilai hash SHA-256, serta status verifikasinya.

Berdasarkan hasil verifikasi chain of custody pada Tabel 7, dapat disimpulkan bahwa dari total 19 barang bukti digital (C-01 hingga C-19) yang dikumpulkan pada rentang waktu 15 Juni hingga 1 Juli, dengan tiga sesi pengambilan pada setiap harinya yaitu pagi, siang, dan sore, seluruh nilai hash SHA-256 dinyatakan cocok tanpa satu pun mengalami ketidaksesuaian. Konsistensi hasil ini membuktikan bahwa setiap file bukti digital berupa PCAP tidak mengalami perubahan, kerusakan, maupun manipulasi sejak proses akuisisi awal hingga tahap analisis dilakukan, sehingga integritas data tetap terjaga sepanjang keseluruhan proses investigasi. Selain itu, hasil ini juga menunjukkan

 ISSN:2302-8149
e-ISSN:2540-9719

bahwa proses penanganan bukti telah sesuai dengan kaidah forensik digital, di mana penerapan hash SHA-256 sebagai metode verifikasi terbukti efektif dalam menjamin keaslian dan keandalan bukti sepanjang rantai penyimpanan (*chain of custody*). Dengan tidak ditemukannya satu pun ketidakcocokan hash, seluruh hasil analisis QoS yang bersumber dari data-data ini memiliki dasar validitas yang kuat serta dapat dipertanggungjawabkan secara ilmiah maupun secara hukum apabila diperlukan dalam proses investigasi lebih lanjut terkait insiden keamanan siber. Dengan demikian, dapat disimpulkan bahwa metode chain of custody yang diterapkan dalam penelitian ini berhasil menjaga integritas seluruh rangkaian bukti digital secara konsisten, sehingga turut mendukung kredibilitas dan keabsahan hasil penelitian secara keseluruhan.

**Tabel 7 Log chain of custody dan verifikasi integritas bukti digital (Hash-256)**

| ID | Tanggal | Waktu | Hash | Status |
|---|---|---|---|---|
| C-01 | 01/07 | Pagi | 11f3604104d073568160fc3c54f0304271452f4fd0e828e19c68b83913603288 | ✓ Match |
| C-02 | 15/06 | Pagi | 35a76c7065fee651dfaf5161312ee5d58be205534e389abf37c86b2fedd8811d | ✓ Match |
| C-03 | 15/06 | Siang | 58c3f6917e77205760aa0b114115777272d4ed8a4b512b66c8a01782ac7067a3 | ✓ Match |
| C-04 | 15/06 | Sore | c1ed41620a23530eded8cfb605fe3a0b12bb0ea1dc71a34de12e38d34ff82dda | ✓ Match |
| C-05 | 17/06 | Pagi | 48970e4155358e92bae3d1f0453f6e7e4470b6caa02db4cc032c34a64013e932 | ✓ Match |
| C-06 | 17/06 | Siang | 901b3718bf006f49823daf9e5646369c80da0c2ac88201a9f9bf02d7f4c6bb5b | ✓ Match |
| C-07 | 17/06 | Sore | 90f028345ead56e1e76aad3ce25c1aad1b0099dbf10ec676d82107ba74ca7ffe | ✓ Match |
| C-08 | 18/06 | Pagi | 7fe947566ae0caa266dbae0ed1c6df4db834eb5a2e2e8552e21e07acd7ec3806 | ✓ Match |
| C-09 | 18/06 | Siang | d7a6b6f708e1911b0d1bfe9d98a650fea9858b0aa040254fecb5541a6f2fc199 | ✓ Match |
| C-10 | 18/06 | Sore | cf7ddc1ec2e43d5e746be90e60e5c1b659c2c06d9e316d179b197609c9701ae0 | ✓ Match |
| C-11 | 22/06 | Pagi | 26bf288b567c45f4e648178ed93f8e45f518078ced03dd6fd67481cb0fd37f70 | ✓ Match |
| C-12 | 22/06 | Siang | f78e77918543cd375e980e89e27f57afd74395d0cdea839bdfc064172990584b | ✓ Match |
| C-13 | 22/06 | Sore | fe092b451dd3a7cb954cd2b5ac77a27a065dc9a878466c3b185c1e6ea6c1ae49 | ✓ Match |
| C-14 | 24/06 | Pagi | cc84193b391e3fa2409b130a4789c1854e4d7e0cd5fe92802aea06290ff70207 | ✓ Match |
| C-15 | 24/06 | Siang | 531afc72121fcebd422ee1de0243edaa10a7238f7c2071a8ffd1ceee2e77d157 | ✓ Match |
| C-16 | 24/06 | Sore | ae00dc08c2358a4ec20238a27ffb1682112bd1b1c3908b86cd0e4a8eab01d333 | ✓ Match |
| C-17 | 25/06 | Pagi | eb9992e32cb3a769d867a0ac69b14a0fa1b6a7b4bf5af9282b4f588653b0bf7d | ✓ Match |
| C-18 | 25/06 | Siang | 67e4d8fd4145d0ffcbce94a1504d5dd7e7cde6d38a1393b4d3d0a43891ca0fdb | ✓ Match |
| C-19 | 25/06 | Sore | 30b9811cf6d8493fc32cb67bf428d4caabfe0c605a13b674fc50c97e32e2604b | ✓ Match |

## 5 Kesimpulan

Penelitian ini berhasil mencapai tujuan yang ditetapkan, yaitu menganalisis kinerja jaringan wireless RSA UGM berdasarkan parameter QoS Standar TIPHON pada kondisi normal, flash crowd, dan serangan DDoS, sekaligus mengintegrasikan prosedur forensik digital untuk menjamin integritas bukti. Masalah utama penelitian, yaitu sulitnya membedakan lonjakan trafik pengguna sah dari serangan siber, berhasil dijawab melalui temuan bahwa packet loss, bukan throughput, merupakan parameter paling signifikan dalam membedakan kedua kondisi tersebut, dengan seluruh 19 barang bukti digital (C-01–C-19) terverifikasi cocok melalui hashing SHA-256 sehingga integritas data forensik tetap terjaga. Dampak dari penelitian ini adalah tersedianya kerangka kerja praktis yang dapat diadopsi oleh RSA UGM maupun institusi kesehatan sejenis untuk mendeteksi dini dan menginvestigasi insiden keamanan jaringan secara lebih akurat tanpa mengganggu layanan operasional. Meskipun demikian, penelitian ini memiliki keterbatasan pada jumlah sampel (19 sesi) yang relatif kecil serta identifikasi sesi serangan DDoS di lapangan yang masih bersifat inferensial berdasarkan kemiripan pola dengan simulasi laboratorium, tanpa analisis mendalam terhadap log firewall atau root cause PCAP. Oleh karena itu, penelitian selanjutnya disarankan untuk memperluas jumlah sampel dan durasi observasi, mengonfirmasi indikasi serangan melalui investigasi forensik yang lebih mendalam, serta mengembangkan kombinasi parameter QoS dan Indeks TIPHON menjadi sistem deteksi dini otomatis guna mendukung respons keamanan jaringan secara real-time.

## Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada pihak Rumah Sakit Akademik Universitas Gadjah Mada (RSA UGM) atas izin dan dukungan yang diberikan selama proses pengumpulan data lalu lintas jaringan dalam penelitian ini, serta kepada tim IT dan staf terkait yang telah membantu proses akuisisi berkas PCAP dan memberikan akses terhadap infrastruktur jaringan yang dibutuhkan. Penulis juga

 ISSN:2302-8149
e-ISSN:2540-9719

menyampaikan apresiasi yang mendalam kepada dosen pembimbing atas arahan, bimbingan, dan masukan yang sangat berharga selama proses penyusunan penelitian ini, mulai dari tahap perencanaan hingga penyelesaian akhir. Ucapan terima kasih turut disampaikan kepada seluruh pihak, baik institusi, kolega, maupun individu, yang telah memberikan kontribusi, dukungan, dan bantuan baik secara langsung maupun tidak langsung, sehingga penelitian ini dapat diselesaikan dengan baik dan diharapkan dapat memberikan manfaat bagi pengembangan ilmu pengetahuan di bidang keamanan jaringan dan forensik digital.

## Referensi

[1] S. Malau and A. Limbong, "*Analysis of Wi-Fi Network Performance at Gading Pluit Hospital to Increase User Productivity using QoS Method*", DOI: https://doi.org/10.36342/teika.v14i2.3800.

[2] M. Deagama, S. Antariksa, A. Aranta, I. Made, H. Wiweka, and J. Ganiwa, "Analisis Jaringan Komputer *Local Area Network* (LAN) di Rumah Sakit UNRAM (*Analysis of Local Area Network Computer Networks At UNRAM Hospital*)," *JBegaTI*, Vol. 3, No. 2, pp. 1–12, 2022, DOI: https://doi.org/10.29303/jbegati.v3i2.748.

[3] M. Firmansyah, H. Hendarti, A. Aslimah, H. Hartanto, I. Purwanti, and T. T, "Perancangan Infrastruktur Jaringan Komputer dengan Media Transmisi Wired dan Nirkabel menggunakan *Cisco Packet Tracer*," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, Vol. 4, No. 3, pp. 1063–1071, Jul. 2024, DOI: 10.57152/malcom.v4i3.1420.

[4] E. Damanik, C. D. Suhendra, and L. F. Marini, "*Quality of Service (QoS)* Jaringan Wireless *Local Area Network (WLAN)* pada Universitas Papua (*Quality of Service* (*QoS*) *Wireless Local Area Network (WLAN) in Papua University*)," *Journal of Information Science and Technology*, Vol. 11, No. 1, pp. 1–7, Apr. 2022, DOI: 10.30862/jistech.v11i1.57.

[5] Y. Morib, N. Satya Irjanto, and R. H. Kiswanto, "Analisis *Quality of Service* (*QoS*) Jaringan Internet pada Universitas Sepuluh Nopember Papua," *Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, pp. 1–9, Apr. 2025, DOI: 10.35889/jutisi.v14i1.2517.

[6] Y. M. Putra and T. Wellem, "Simulasi Jaringan IEEE 802.11AX WIFI 6 menggunakan Simulator NS-3 untuk Pengukuran *Throughput* pada Band Frekuensi 6Ghz," *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, Vol. 4, No. 3, pp. 913–923, Sep. 2023, DOI: 10.35870/jimik.v4i3.298.

[7] M. L. Arsalan, F. Sains, and D. Teknologi, "Keamanan Jaringan *Wireless Fidelity* (WIFI) terhadap Serangan *Packet Sniffing* menggunakan *Firewall Rule* ( Studi Kasus: PT Akurat Sentra Media)," *CyberSecurity dan Forensik Digital*, Vol. VOL. 6, Nov. 2023, DOI: 10.14421/csecurity.2023.6.2.4075.

[8] Yevi Grata Putra and Tata Sutabri, "Analisis *Qualitiy of Service* (*QoS*) Jaringan Internet menggunakan Metode *Action Research* pada Balai Diklat Keagamaan Palembang," *Jurnal Sistem Informasi dan Ilmu Komputer*, Vol. 2, No. 4, pp. 100–111, Nov. 2024, DOI: 10.59581/jusiik-widyakarya.v2i4.4250.

[9] W. Agustiono, D. Wulan Suci, and N. Prastiti, "Analisis Forensik Digital menggunakan Metode *NIST* untuk memulihkan Barang Bukti yang dihapus *Digital Forensic Analysis using the NIST Method for Recovering Deleted Evidence*," *Jurnal Teknologi dan Informasi (JATI)*, Vol. 14, 2024, DOI: 10.34010/jati.v14i2.

[10] R. A. Ramadhan, A. T. Tira, and M. R. Fadhilah, "SISTEMASI: Jurnal Sistem Informasi Forensik Jaringan: Analisis Serangan *Client* dan Pengukuran *Quality of Service* oleh ARP *Poisoning* menggunakan *Network Forensic Generic Process (NFGP)* Model *Network Forensic: Analysis of Client Attack and Quality of Service Measurement by Arp Poisoning using Network Forensic Generic Process (NFGP) Model*", DOI: https://doi.org/10.32520/stmsi.v13i2.3804.

[11] A. Wijayanto, I. Riadi, and Y. Prayudi, "*TAARA Method to Processing on the Network Forensics in the Event of an ARP Spoofing Attack*," *Jurnal RESTI*, Vol. 7, no. 2, pp. 208–217, Apr. 2023, DOI: 10.29207/resti.v7i2.4589.

[12] S. Suharti, A. Yudhana, and I. Riadi, "Forensik Jaringan *DDoS* menggunakan Metode *ADDIE* dan HIDS pada Sistem Operasi *Proprietary*," *MATRIK : Jurnal Manajemen, Teknik*

*Informatika dan Rekayasa Komputer*, Vol. 21, No. 3, pp. 567–582, Jul. 2022, DOI: 10.30812/matrik.v21i3.1732.

[13] A. Y. Syarif, C. Adipradana, and C. P. Prasetyo, "Analisis Kinerja Jaringan WLAN menggunakan Metode *QoS* Versi *TIPHON* di SMKS Al-Mahrusiyah Kota Kediri," *TECNOSCIENZA*, Vol. 8, Apr. 24AD, DOI: https://doi.org/10.51158/tecnoscienza.v8i2.1200.

[14] H. Ruli Oktaseli and A. A. Slameto, "*Evaluation of Wireless LAN Quality of Service (QoS) in Primary Education using TIPHON Standards*," 2025. [Online]. Available: http://jurnal.polibatam.ac.id/index.php/JAIC

[15] I. S. N. Nisa, Rahmat Miyarno Saputro, Tegar Fatwa Nugroho, and Alfirna Rizqi Lahitani, "Analisis *Quality of Service (QoS)* menggunakan Standar Parameter *Tiphon* pada Jaringan Internet Berbasis Wi-Fi Kampus 1 Unjaya," *Teknomatika: Jurnal Informatika dan Komputer*, Vol. 17, No. 1, pp. 1–9, Apr. 2024, DOI: 10.30989/teknomatika.v17i1.1307.

[16] B. Pamungkas and F. Andreas Sutanto, "Penerapan Metode *Quality of Service (QoS*) dalam Analisis Kualitas Jaringan Internet Burjo Pantry Semarang," *Jurnal JTIK: Teknologi Informasi dan Komunikasi*, Vol. 8, No. 2, p. 2024, 2024, DOI: 10.35870/jti.

[17] M. Rifki Wardana and D. B. Santoso, "Analisis *Throughput* Distribusi Jaringan Nirkabel pada Politeknik Bumi Akpelni," *Jurnal Riset Sistem Informasi dan Teknik Informatika (JURASIK)*, Vol. 8, No. 2, pp. 558–567, 2023, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[18] S. Turangga and Y. Arie, "Analisis Internet menggunakan Parameter *Quality of Service* pada Alfamart Tuparev 70," *Jurnal Mahasiswa Teknik Informatika*, Vol. 6, No. 1, pp. 1–7, 2022, DOI: 10.36040/jati.v6i1.4693.

[19] B. Nakulo *et al.*, "Analisis *Quality of Service (QoS)* pada Akses Game Online menggunakan Standar *Tiphon*," *Teknomatika*, Vol. 15, pp. 1–6, 2022, [Online]. Available: http://ejournal.unjaya.ac.id/index.php/Teknomatika/

[20] A. Budiman, M. Ficky Duskarnaen, and H. Ajie, "Analisis *Quality of Service (QoS)* pada Jaringan Internet SMK Negeri 7 Jakarta," *Jurnal Pendidikan Teknik Informatika dan Komputer*, Vol. 4, pp. 1–5, 2020, DOI: 10.21009/pinter.4.2.6.