UJI EFEKTIVITAS METODE *STATISTICAL ANOMALY DETECTION* MENGGUNAKAN WIRESHARK DALAM MENDETEKSI AKTIVITAS MENCURIGAKAN PADA TRAFIK JARINGAN LOKAL

PROPOSAL TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat Penulisan Tugas Akhir
pada Sekolah Tinggi Manajemen Informatika Dan Komputer
(STMIK) Palangkaraya

OLEH

SHELLA APRIANTI KRISTINA
C2255201118
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2026

UJI EFEKTIVITAS METODE *STATISTICAL ANOMALY DETECTION* MENGGUNAKAN WIRESHARK DALAM MENDETEKSI AKTIVITAS MENCURIGAKAN PADA TRAFIK JARINGAN LOKAL

PROPOSAL TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat Penulisan Tugas Akhir
pada Sekolah Tinggi Manajemen Informatika Dan Komputer
(STMIK) Palangkaraya

OLEH

SHELLA APRIANTI KRISTINA
C2255201118
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2026

PERSETUJUAN

UJI EFEKTIVITAS METODE *STATISTICAL ANOMALY DETECTION* MENGGUNAKAN WIRESHARK DALAM MENDETEKSI AKTIVITAS MENCURIGAKAN PADA TRAFIK JARINGAN LOKAL

Proposal Tugas Akhir Ini Telah Disetujui dan Disahkan

Pembimbing I,	Pembimbing II,
Ir. Abdul Hadi, S.T,. M.Kom	Sam'ani, S.T,. M.Kom
NIK. 198505102021101	NIK. 197703252005105

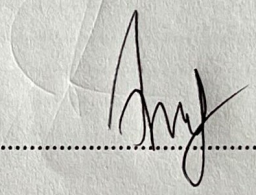
Mengetahui	Mengesahkan
Ketua STMIK Palangkaraya,	Ketua Prodi Teknik Informatika,
Ir. Hj. Siti Maryamah, M.M	Ir. Abdul Hadi, S.T., M.Kom
NIK. 196902021995004	NIK. 198505102021101

PENGESAHAN

UJI EFEKTIVITAS METODE *STATISTICAL ANOMALY DETECTION* MENGGUNAKAN WIRESHARK DALAM MENDETEKSI AKTIVITAS MENCURIGAKAN PADA TRAFIK JARINGAN LOKAL

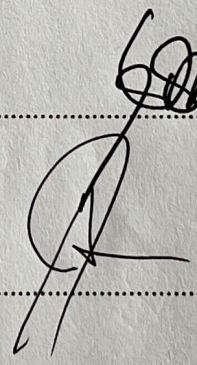
Proposal Tugas Akhir ini telah Diseminarkan, Dinilai, dan Disahkan
Oleh Tim Seminar pada Tanggal 15 Januari 2026

Tim Seminar Proposal :

1. Amaya Andri Damaini, S.Kom., M.T. ..... 
   Ketua

2. Ir. Abdul Hadi, S.T., M.Kom .....
   Sekretaris

3. Sam'ani, S.T., M.Kom .....
   Anggota



DAFTAR ISI

PERSETUJUAN iii
PENGESAHAN iv
DAFTAR ISI v
DAFTAR TABEL vi
DAFTAR GAMBAR vii
DAFTAR LAMPIRAN viii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan dan Manfaat 2
1.5 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 5
2.1 Kajian Teori 5
2.2 Penelitian Yang Relevan 13
BAB III METODOLOGI PENELITIAN 16
3.1 Tinjauan Umum 16
3.2 Jenis penelitian 16
3.3 Desain Penelitian 17
3.4 Instrumen Penelitian 22
3.5 Analisis Kebutuhan 23
3.6 Desain 30
3.7 Jadwal Penelitian 38
DAFTAR PUSTAKA

DAFTAR TABEL

Table 2. 1 Contoh table menggunakan sumber table.....12
Table 2. 2 Penelitian yang relavan.....13
Tabel 3. 1 Jadwal Penelitian Tugas Akhir.....39

DAFTAR GAMBAR

Gambar 3. 1. Flowchart Tahap Awal Desain Penelitian 19
Gambar 3. 2. Desain Sistem Analisis 31
Gambar 3. 3. Flowchart Proses Analisis 32
Gambar 3. 4. Desain Perangkat 35
Gambar 3. 5. Desain Jaringan 37

DAFTAR LAMPIRAN

Lampiran 1. Surat tugas pembimbing tugas akhir
Lampiran 2. Lembar konsultasi bimbingan Tugas Akhir
Lampiran 3. Surat izin penelitian
Lampiran 4. Surat keterangan telah melakukan penelitian
Lampiran 5. Lembar wawancara
Lampiran 6. Lembar dokumentasi wawancara
Lampiran 7. Surat tugas penguji seminar
Lampiran 8. Berita acara penilaian seminar proposal TA

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi mendorong peningkatan penggunaan jaringan komputer di lingkungan pendidikan, termasuk di STMIK Palangkaraya. Jaringan lokal (LAN) dimanfaatkan untuk mendukung berbagai aktivitas akademik dan administrasi, seperti sistem informasi akademik, e-learning, dan akses internet. Menurut Rahman dan Iswan (2024), tingginya aktivitas pengguna dan variasi pola komunikasi dapat memunculkan trafik jaringan yang menyimpang dari kondisi normal, sehingga berpotensi menjadi indikasi awal adanya gangguan atau ancaman keamanan jaringan.

Dalam proses pemantauan trafik jaringan, Putri, Hadi, dan Rusdiana (2025) menjelaskan bahwa Wireshark mampu menangkap dan menampilkan paket jaringan secara rinci untuk mengidentifikasi pola komunikasi dan aktivitas tidak normal. Namun, analisis paket secara manual memiliki keterbatasan pada jaringan dengan volume trafik yang tinggi karena membutuhkan waktu dan ketelitian yang besar, sehingga berpotensi memperlambat proses deteksi aktivitas mencurigakan.

Oleh karena itu, diperlukan pendekatan tambahan berbasis perhitungan statistik. Nugroho, Hariguna, dan Barkah (2025) menyatakan bahwa metode *Statistical Anomaly Detection* dapat digunakan untuk mendeteksi penyimpangan trafik jaringan dengan membandingkan pola trafik aktual terhadap pola trafik normal berdasarkan parameter statistik. Berdasarkan hal tersebut, penelitian ini bertujuan

untuk menguji efektivitas metode *Statistical Anomaly Detection* yang dikombinasikan dengan analisis paket menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal di STMIK Palangkaraya, sehingga diharapkan dapat meningkatkan akurasi dan efisiensi pemantauan keamanan jaringan di lingkungan pendidikan.

1.2 Perumusan Masalah

Bagaimana menguji efektivitas metode *Statistical Anomaly Detection* yang dikombinasikan dengan analisis paket menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal di STMIK Palangkaraya?

1.3 Batasan Masalah

Penelitian ini dibatasi pada proses pengujian efektivitas metode *Statistical Anomaly Detection* yang dikombinasikan dengan analisis paket menggunakan Wireshark dalam mengidentifikasi aktivitas mencurigakan pada trafik jaringan lokal (LAN) di STMIK Palangkaraya, berdasarkan data hasil penangkapan paket selama periode pengamatan tertentu.

1.4 Tujuan dan Manfaat

a. Tujuan

Untuk menguji dan menilai tingkat efektivitas metode *Statistical Anomaly Detection* yang dikombinasikan dengan analisis paket menggunakan Wireshark dalam mengidentifikasi aktivitas mencurigakan pada trafik jaringan lokal (LAN) di STMIK Palangkaraya berdasarkan hasil analisis data trafik jaringan selama periode pengamatan.

b. Manfaat

Manfaat Bagi Penulis: Penelitian ini diharapkan dapat meningkatkan pemahaman dan keterampilan penulis dalam menerapkan metode *Statistical Anomaly Detection* serta penggunaan Wireshark dalam menganalisis trafik jaringan, khususnya dalam konteks pengujian efektivitas metode deteksi aktivitas mencurigakan pada jaringan lokal di lingkungan pendidikan.

Bagi Institusi atau Tempat Penelitian: Hasil penelitian ini diharapkan dapat menjadi bahan evaluasi dan pertimbangan bagi pihak pengelola jaringan dalam meningkatkan sistem pemantauan dan pengamanan jaringan lokal, serta sebagai dasar dalam pengambilan keputusan terkait pengelolaan dan pencegahan potensi gangguan keamanan jaringan di lingkungan institusi.

Bagi STMIK Palangkaraya: Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan kebijakan dan strategi pengelolaan keamanan jaringan di STMIK Palangkaraya, serta mendukung peningkatan kualitas layanan teknologi informasi yang digunakan untuk menunjang kegiatan akademik dan administrasi.

Bagi Pengguna atau Praktisi: Penelitian ini diharapkan dapat menjadi referensi praktis bagi administrator jaringan, teknisi, dan praktisi teknologi informasi dalam menerapkan pendekatan statistik dan analisis paket jaringan sebagai bagian dari upaya pemantauan dan pengamanan trafik jaringan di lingkungan kerja masing-masing. .

1.5 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan sebagai dasar dan arah dalam pelaksanaan penelitian.

BAB II LANDASAN TEORI

Bab ini memuat kajian teori dan hasil penelitian terdahulu yang relevan dengan topik penelitian, meliputi konsep jaringan komputer, trafik jaringan, keamanan jaringan, Wireshark, metode *Statistical Anomaly Detection*, serta kerangka pemikiran yang digunakan sebagai landasan dalam pengujian efektivitas metode yang diterapkan.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan jenis dan pendekatan penelitian, lokasi dan waktu penelitian, sumber dan teknik pengumpulan data, kebutuhan perangkat keras dan perangkat lunak, tahapan pengujian metode *Statistical Anomaly Detection* dan analisis paket menggunakan Wireshark, serta teknik analisis data yang digunakan untuk mengukur tingkat efektivitas metode.

BAB II

TINJAUAN PUSTAKA

2.1 Kajian Teori

2.1.1 Keamanan Jeringan

Keamanan jaringan adalah upaya untuk melindungi jaringan komputer dari berbagai ancaman seperti akses ilegal, penyadapan data, atau aktivitas berbahaya yang dapat merusak sistem. Keamanan jaringan mencakup mekanisme untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan sistem (availability). Dalam proses pemantauan jaringan, aktivitas mencurigakan sering kali muncul sebagai penyimpangan dari pola trafik normal, yang dapat mengindikasikan adanya serangan seperti port scanning, brute force, hingga komunikasi malware.

Menurut Zhang dan Lazaro (2024), sistem keamanan jaringan modern tidak hanya berfokus pada pencegahan serangan, tetapi juga pada kemampuan mendeteksi aktivitas yang tidak normal sejak tahap awal. Aktivitas tersebut sering kali tidak langsung menimbulkan gangguan, namun menjadi indikator awal adanya ancaman terhadap jaringan.

Oleh karena itu, analisis trafik jaringan menjadi bagian penting dalam keamanan jaringan untuk mengidentifikasi aktivitas mencurigakan sebelum berkembang menjadi serangan yang lebih serius.

2.1.2 Trafik Jaringan

Trafik jaringan merupakan aliran data yang dikirim dan diterima antar perangkat dalam suatu jaringan komputer. Trafik ini dapat dianalisis berdasarkan jumlah paket, ukuran paket, waktu pengiriman, serta protokol yang digunakan. Priya dan Soumya (2024) menyatakan bahwa trafik jaringan normal memiliki pola yang relatif stabil dan konsisten dalam kondisi operasional normal.

Namun, perubahan yang signifikan terhadap pola trafik tersebut dapat mengindikasikan adanya gangguan atau aktivitas yang tidak wajar. Oleh karena itu, pemantauan trafik jaringan diperlukan untuk memahami pola komunikasi serta mendeteksi penyimpangan yang terjadi dalam jaringan lokal.

2.1.3 Anomali Trafik Jaringan

Anomali trafik jaringan merupakan kondisi di mana pola trafik menyimpang dari karakteristik trafik normal. Menurut Aswathy dan Rajkumar (2024), anomali trafik sering kali menjadi indikator awal adanya aktivitas mencurigakan pada jaringan komputer.

Deteksi anomali diperlukan karena tidak semua ancaman keamanan muncul secara langsung dalam bentuk serangan. Beberapa aktivitas mencurigakan hanya terlihat melalui perubahan pola trafik jaringan. Jika anomali tersebut tidak terdeteksi sejak dini, maka dapat berkembang menjadi gangguan jaringan atau ancaman keamanan yang lebih besar.

2.1.4 Contoh Aktivitas Mencurigakan Pada Trafik Jaringan

Berdasarkan penelitian Zhang dan Lazaro (2024) serta Nugroho (2025), beberapa contoh trafik jaringan yang tergolong sebagai anomali dan aktivitas mencurigakan antara lain:

1) Lonjakan trafik jaringan secara tiba-tiba dalam waktu singkat.

2) Pengiriman paket berulang dari satu sumber ke banyak tujuan.

3) Percobaan koneksi ke banyak port secara berurutan (port scanning).

4) Akses berulang ke alamat IP yang tidak dikenal.

5) Koneksi simultan dalam jumlah besar yang tidak sesuai dengan pola normal.

6) Penggunaan protokol yang jarang digunakan pada jaringan lokal.

Contoh-contoh tersebut menunjukkan bahwa aktivitas mencurigakan dapat diidentifikasi melalui penyimpangan pola statistik trafik jaringan.

2.1.5 *Statistical Anomaly Detection*

Statistical Anomaly Detection merupakan metode deteksi anomali yang menggunakan pendekatan statistik untuk mengidentifikasi penyimpangan data dari pola normal. Menurut Mohammed et al. (2022), metode statistik efektif digunakan pada jaringan dengan pola trafik yang relatif stabil karena mampu mendeteksi perubahan secara kuantitatif.

Metode *Statistical Anomaly Detection* merupakan teknik pendeteksian aktivitas mencurigakan dengan membandingkan trafik jaringan aktual dengan trafik normal berdasarkan parameter statistik seperti mean, standar deviasi, probabilitas

distribusi, atau threshold tertentu. Jika nilai trafik melebihi ambang batas statistik, maka trafik tersebut dianggap sebagai anomali. Pendekatan ini dinilai efektif untuk mendeteksi serangan yang tidak memiliki signature, karena fokus pada pola penyimpangan, bukan pola serangan tertentu. Apabila terjadi penyimpangan yang signifikan dari pola normal tersebut, maka trafik jaringan tersebut dapat diindikasi-kan sebagai anomali.

Pada tahap awal, trafik jaringan yang diperoleh dari proses *packet capture* menggunakan Wireshark dikumpulkan dalam bentuk data kuantitatif, seperti jumlah paket dalam interval waktu tertentu, ukuran paket, atau jumlah koneksi ke suatu port. Data tersebut kemudian dianalisis untuk menentukan pola trafik normal sebagai acuan pembanding.

Rumus Metode *Statistical Anomaly Detection*

Nilai rata-rata (mean) digunakan untuk menggambarkan kondisi umum atau karakteristik normal trafik jaringan dalam periode pengamatan. Secara matematis, nilai rata-rata dirumuskan sebagai berikut:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad (2.1)$$

di mana:

μ adalah nilai rata-rata trafik jaringan,

x_i adalah nilai trafik pada pengamatan ke-i,

$n$adalah jumlah total data trafik yang dianalisis.

Selain nilai rata-rata, diperlukan pengukuran tingkat variasi data terhadap nilai rata-rata tersebut yang dinyatakan dalam standar deviasi. Standar deviasi digunakan untuk mengetahui seberapa jauh penyebaran data trafik dari kondisi normal. Perhitungan standar deviasi dirumuskan sebagai berikut:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2} \qquad (2.2)$$

di mana:

σ merupakan standar deviasi trafik jaringan.

Berdasarkan nilai rata-rata dan standar deviasi tersebut, ditentukan ambang batas (threshold) untuk mengidentifikasi adanya anomali. Ambang batas ini digunakan sebagai batas toleransi antara trafik normal dan trafik tidak normal. Secara umum, ambang batas dinyatakan sebagai berikut:

$$x > \mu + k\sigma \qquad (2.3)$$

atau

$$x < \mu - k\sigma \qquad (2.4)$$

dengan keterangan:

x adalah nilai trafik jaringan yang diamati,

μ adalah nilai rata-rata trafik jaringan,

σ adalah standar deviasi trafik jaringan,

k merupakan konstanta yang menentukan tingkat sensitivitas pendeteksian anomali.

Semakin besar nilai k, maka sistem akan lebih toleran terhadap variasi trafik, sedangkan nilai k yang lebih kecil akan membuat sistem lebih sensitif dalam mendeteksi anomali.

Pendekatan *Statistical Anomaly Detection* memiliki keunggulan karena tidak bergantung pada pola serangan tertentu (*signature-based*), sehingga mampu mendeteksi aktivitas mencurigakan yang belum pernah teridentifikasi sebelumnya. Namun, metode ini juga memerlukan interpretasi lanjutan untuk memastikan bahwa anomali yang terdeteksi benar-benar merupakan aktivitas berbahaya dan bukan variasi trafik normal.

Oleh karena itu, dalam penelitian ini hasil pendeteksian anomali secara statistik digunakan sebagai indikator awal, yang selanjutnya dianalisis lebih mendalam melalui analisis paket menggunakan Wireshark. Dengan kombinasi metode statistik dan analisis paket, diharapkan identifikasi aktivitas mencurigakan pada trafik jaringan dapat dilakukan secara lebih akurat dan sistematis.

2.1.6 Wireshark sebagai Perangkat Analisis Trafik Jaringan

Wireshark adalah perangkat lunak network protocol analyzer yang digunakan untuk menangkap, membaca, dan menganalisis paket data yang melintas di jaringan secara real time. Software ini merupakan salah satu tools utama yang digunakan dalam penelitian ini, karena memiliki kemampuan untuk menampilkan setiap paket secara detail hingga ke level bit (frame), termasuk informasi protokol, port jaringan, alamat IP sumber dan tujuan, ukuran paket, maupun isi payload.

Wireshark bekerja dengan cara memonitor antarmuka jaringan (network interface) dan menangkap seluruh paket yang melewatinya. Data paket tersebut

disimpan dalam bentuk file .pcap yang kemudian dapat dianalisis lebih lanjut. Kemampuan ini sangat penting dalam penelitian analisis aktivitas mencurigakan, karena peneliti dapat melihat langsung pola komunikasi perangkat, frekuensi paket, dan indikasi anomali pada trafik

2.1.7 Kajian Teori Terkait Semua Pendukung Dalam Penelitian

Pendukung dalam penelitian ini mencakup perangkat lunak (software) dan metode analisis yang digunakan untuk mendeteksi aktivitas mencurigakan pada trafik jaringan lokal. Pendekatan yang digunakan merupakan metode kuantitatif dengan analisis statistik, di mana data trafik jaringan dianalisis berdasarkan parameter statistik untuk menguji efektivitas metode deteksi anomali. Wireshark digunakan untuk menangkap dan menganalisis paket data yang melintas di jaringan sehingga peneliti dapat mengamati pola komunikasi, protokol, dan indikasi trafik tidak normal. Data hasil tangkapan tersebut kemudian dianalisis menggunakan Statistical Anomaly Tools melalui perhitungan statistik seperti nilai rata-rata (mean), standar deviasi, dan ambang batas (threshold) untuk mengidentifikasi penyimpangan pola trafik dari kondisi normal. Kombinasi kedua pendukung ini memungkinkan proses identifikasi aktivitas mencurigakan pada trafik jaringan dilakukan secara sistematis dan terukur.

Tabel 2. 1. Contoh table menggunakan sumber table

No	Perangkat Lunak	Keterangan
1	Wireshark	Digunakan untuk menangkap (*capture*), merekam, dan menganalisis paket data yang melintas di jaringan. Wireshark membantu mengamati pola komunikasi,

No	Perangkat Lunak	Keterangan
		protokol, dan paket mencurigakan sebagai dasar identifikasi aktivitas luar biasa dalam trafik jaringan.
2	Statistical Anomaly Tools (Perhitungan Statistik Manual atau Spreadsheet)	Digunakan untuk melakukan perhitungan statistik terhadap data trafik jaringan, termasuk menghitung nilai rata-rata (*mean*), standar deviasi, dan ambang batas (*threshold*). Analisis statistik ini membantu membedakan trafik normal dan anomali berdasarkan karakteristik deviasi.

Sumber : Rahman & Iswan (2024), Nugroho *et al.* (2025)

Tabel 2.1 menampilkan perangkat lunak utama yang digunakan dalam penelitian ini. Wireshark digunakan karena mampu menangkap dan menganalisis paket jaringan secara rinci, sehingga memudahkan peneliti dalam mengamati pola komunikasi, alamat IP, serta port yang tidak wajar sebagai indikasi adanya aktivitas mencurigakan pada trafik jaringan. Pemanfaatan Wireshark sebagai alat analisis paket jaringan telah dibuktikan efektif dalam penelitian yang dilakukan oleh Rahman dan Iswan (2024) dalam mendeteksi anomali berdasarkan pola trafik jaringan.

Selain itu, pendekatan *Statistical Anomaly Detection* digunakan untuk mendukung proses analisis melalui perhitungan nilai statistik trafik jaringan, seperti nilai rata-rata (*mean*), standar deviasi, dan penentuan ambang batas (*threshold*). Pendekatan statistik ini berfungsi untuk mengidentifikasi penyimpangan pola trafik dari kondisi normal secara kuantitatif. Hal ini sejalan dengan penelitian yang dilakukan oleh Nugroho, Hariguna, dan Barkah (2025) yang menunjukkan bahwa

analisis statistik efektif digunakan sebagai indikator awal dalam mendeteksi anomali trafik jaringan.

Kedua pendekatan tersebut saling melengkapi, di mana Wireshark berperan dalam proses pengumpulan dan visualisasi data paket jaringan, sedangkan analisis statistik digunakan untuk mendeteksi penyimpangan pola trafik berdasarkan perhitungan kuantitatif. Kombinasi ini memungkinkan identifikasi aktivitas mencurigakan pada trafik jaringan dilakukan secara lebih sistematis dan akurat.

2.2 Penelitian Yang Relevan

Bagian ini membahas penelitian terdahulu yang memiliki keterkaitan dengan topik deteksi anomali, analisis trafik jaringan, dan penggunaan Wireshark. Penelitian relevan berfungsi sebagai acuan, perbandingan, serta penguat dalam merumuskan metode penelitian saat ini.

Tabel 2. 2. Penelitian yang relevan

No	Penulis / Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
1	Nugroho / 2025	Deteksi anomali trafik jaringan dan aktivitas pengguna	*Statistical Anomaly Detection (Isolation Forest)*	Menganalisis pola trafik jaringan dan aktivitas pengguna untuk mengidentifikasi penyimpangan dari kondisi normal	Metode Isolation Forest mampu mendeteksi anomali trafik jaringan secara efektif
2	Rozi / 2025	Analisis insiden jaringan berbasis packet capture	*Packet Analysis*	Melakukan inspeksi paket jaringan (PCAP) menggunakan Wireshark untuk mengidentifikasi aktivitas mencurigakan	Wireshark berhasil mengungkap pola serangan dan anomali pada lalu lintas jaringan

No	Penulis / Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
3	Rahman & Iswan / 2024	Analisis trafik jaringan media sosial	Analisis Trafik Jaringan	Menganalisis trafik jaringan untuk mendeteksi anomali komunikasi pada platform media sosial	Sistem mampu mengidentifikasi pola trafik tidak normal pada jaringan media sosial
4	Manalu & Hutabarat / 2024	Deteksi anomali trafik jaringan	*Machine Learning (Decision Tree)*	Mengklasifikasikan trafik jaringan normal dan abnormal menggunakan metode Decision Tree	Model Decision Tree menunjukkan tingkat akurasi yang baik dalam mendeteksi anomali
5	Putri, Hadi & Rusdiana / 2025	Analisis trafik jaringan untuk deteksi serangan deauthentication	Analisis Trafik Jaringan (Wireshark)	Menganalisis trafik Wi-Fi untuk mendeteksi serangan deauthentication pada perangkat jaringan	Serangan deauthentication berhasil diidentifikasi melalui pola paket jaringan
6	Zhang & Lazaro / 2024	Survey teknik analisis keamanan trafik jaringan	Studi Literatur	Mengkaji berbagai metode analisis trafik dan deteksi anomali jaringan	Memberikan gambaran komprehensif metode deteksi anomali yang efektif

Berdasarkan Tabel Penelitian yang Relevan, dapat diketahui bahwa penelitian-penelitian sebelumnya telah membahas deteksi anomali pada trafik jaringan menggunakan berbagai pendekatan, baik berbasis statistik maupun machine learning. Namun, sebagian besar penelitian tersebut masih berfokus pada hasil deteksi anomali secara umum tanpa disertai analisis lanjutan terhadap detail paket jaringan untuk mengetahui karakteristik aktivitas mencurigakan yang terjadi.

Selain itu, penelitian terdahulu umumnya menggunakan dataset trafik jaringan yang bersifat offline atau data uji yang telah tersedia, sehingga belum

sepenuhnya merepresentasikan kondisi trafik jaringan aktual yang dinamis. Penggunaan perangkat lunak Wireshark pada penelitian sebelumnya lebih banyak dimanfaatkan sebagai alat bantu pemantauan atau visualisasi trafik, dan belum dikombinasikan secara terintegrasi dengan metode *Statistical Anomaly Detection* dalam satu alur analisis yang sistematis.

Berdasarkan celah penelitian tersebut, penelitian ini menawarkan keterbaruan (novelty) dengan mengombinasikan metode *Statistical Anomaly Detection* dan analisis paket jaringan menggunakan Wireshark untuk menganalisis aktivitas mencurigakan pada trafik jaringan secara lebih komprehensif. Pendekatan ini tidak hanya mendeteksi anomali berdasarkan parameter statistik, tetapi juga melakukan analisis detail paket jaringan guna mengidentifikasi pola dan karakteristik aktivitas mencurigakan secara lebih jelas.

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi berupa pendekatan analisis yang lebih aplikatif dan mendalam dalam mendeteksi serta memahami aktivitas mencurigakan pada jaringan komputer, khususnya pada lingkungan jaringan dengan trafik yang bersifat dinamis seperti di lingkungan pendidikan.

BAB III

METODOLOGI PENELITIAN

3.1 Tinjauan Umum

Penelitian ini bertujuan untuk menguji efektivitas metode *Statistical Anomaly Detection* yang dikombinasikan dengan analisis paket menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal. Penelitian dilakukan pada lingkungan jaringan yang memiliki trafik dinamis akibat aktivitas pengguna yang beragam.

Data penelitian diperoleh melalui proses packet capture menggunakan Wireshark pada jaringan lokal yang diamati. Data trafik jaringan tersebut kemudian dianalisis menggunakan pendekatan statistik dengan menghitung parameter seperti nilai rata-rata (mean), standar deviasi, dan penentuan nilai ambang batas (threshold) untuk membedakan antara trafik normal dan trafik yang menyimpang.

Trafik jaringan yang menunjukkan penyimpangan dari pola normal diidentifikasi sebagai anomali dan dianalisis lebih lanjut menggunakan Wireshark untuk mengetahui karakteristik aktivitas mencurigakan yang terjadi. Melalui tahapan tersebut, penelitian ini mengevaluasi kemampuan metode *Statistical Anomaly Detection* dalam mendeteksi aktivitas mencurigakan secara efektif pada kondisi jaringan yang nyata.

3.2 Jenis penelitian

Penelitian ini menggunakan jenis penelitian eksperimen. Penelitian eksperimen dipilih karena penelitian ini bertujuan untuk menguji efektivitas metode

Statistical Anomaly Detection dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal.

Pada penelitian ini, metode *Statistical Anomaly Detection* diperlakukan sebagai perlakuan (treatment) yang diterapkan pada data trafik jaringan hasil packet capture menggunakan Wireshark. Data trafik jaringan dianalisis untuk melihat apakah metode tersebut mampu mendeteksi penyimpangan pola trafik yang mengindikasikan adanya aktivitas mencurigakan.

Hasil penerapan metode kemudian dianalisis untuk menilai tingkat efektivitas metode *Statistical Anomaly Detection* dalam kondisi jaringan lokal yang nyata. Dengan demikian, penelitian eksperimen ini sesuai dengan tujuan penelitian, yaitu melakukan pengujian dan evaluasi kinerja metode dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal.

3.3 Desain Penelitian

Desain penelitian yang digunakan dalam penelitian ini adalah desain penelitian eksperimen. Desain ini dipilih karena penelitian bertujuan untuk menguji efektivitas metode *Statistical Anomaly Detection* yang dikombinasikan dengan analisis paket menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal di lingkungan STMIK Palangkaraya.

Penelitian diawali dengan penentuan lokasi penelitian, yaitu menetapkan jaringan lokal STMIK Palangkaraya sebagai objek penelitian. Penetapan lokasi ini dilakukan untuk memastikan bahwa lingkungan penelitian memiliki karakteristik trafik jaringan yang aktif dan bervariasi sehingga sesuai untuk menguji kinerja metode deteksi anomali.

Tahap selanjutnya adalah survei awal lokasi, yang bertujuan untuk memperoleh gambaran awal mengenai kondisi fisik dan operasional jaringan. Pada tahap ini dilakukan pengamatan terhadap akses jaringan, lokasi perangkat jaringan, serta kondisi umum infrastruktur yang mendukung proses penelitian.

Setelah itu dilakukan identifikasi topologi dan infrastruktur jaringan, meliputi pengenalan terhadap perangkat jaringan seperti router, access point, serta perangkat client yang terhubung dalam jaringan lokal. Tahap ini bertujuan untuk memahami struktur jaringan dan alur lalu lintas data yang akan menjadi objek pengamatan.

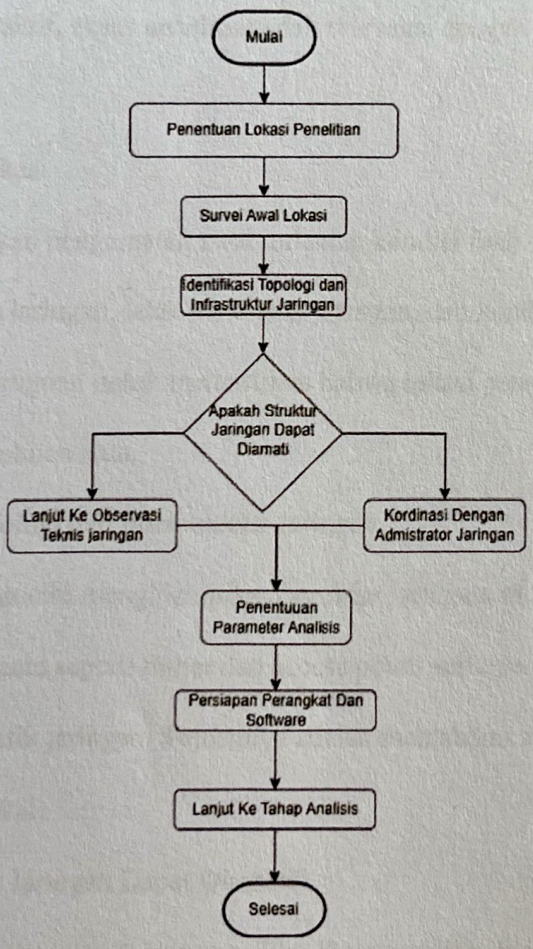
Berdasarkan hasil identifikasi tersebut, dilakukan pengambilan keputusan mengenai keteramatan struktur jaringan. Apabila struktur jaringan dapat diamati secara langsung, maka penelitian dilanjutkan ke tahap observasi teknis jaringan. Namun, apabila struktur jaringan tidak dapat diamati secara jelas, maka dilakukan koordinasi dengan administrator jaringan untuk memperoleh informasi tambahan atau melakukan penyesuaian lokasi dan waktu pengamatan.

Setelah struktur jaringan dan informasi teknis dinilai memadai, dilakukan penentuan parameter analisis yang akan digunakan dalam proses pengujian metode. Parameter tersebut meliputi jumlah paket, ukuran paket, interval waktu pengiriman paket, protokol, alamat IP, dan port yang digunakan dalam komunikasi jaringan.

Tahap berikutnya adalah persiapan perangkat dan perangkat lunak, yaitu menyiapkan laptop atau komputer peneliti, menginstal dan mengonfigurasi perangkat lunak Wireshark, serta menyiapkan alat bantu pengolahan data statistik yang akan digunakan dalam perhitungan metode *Statistical Anomaly Detection*.

Setelah seluruh persiapan selesai, penelitian dilanjutkan ke tahap analisis, yang mencakup proses pengambilan data trafik jaringan melalui packet capture, perhitungan statistik, penentuan nilai ambang batas (threshold), serta analisis lanjutan terhadap paket jaringan yang terindikasi sebagai aktivitas mencurigakan.

Dengan desain penelitian ini, proses pengujian metode dilakukan secara sistematis, terstruktur, dan sesuai dengan kondisi nyata jaringan lokal, sehingga hasil yang diperoleh dapat digunakan untuk mengevaluasi efektivitas metode *Statistical Anomaly Detection* secara objektif.



Gambar 3. 1. Flowchart Tahap Awal Desain Penelitian

Berikut penjelasan setiap tahapan pada flowchart yang digunakan dalam penelitian ini:

a. Mulai

Tahap awal yang menandai dimulainya seluruh rangkaian kegiatan penelitian.

b. Penentuan Lokasi Penelitian

Pada tahap ini peneliti menetapkan jaringan lokal STMIK Palangkaraya sebagai objek penelitian. Penentuan lokasi dilakukan berdasarkan pertimbangan ketersediaan jaringan aktif, akses penelitian, dan relevansi dengan tujuan penelitian.

c. Survei Awal Lokasi

Peneliti melakukan pengamatan awal terhadap kondisi fisik dan lingkungan jaringan, seperti akses jaringan, letak perangkat jaringan, dan kondisi operasional jaringan. Tahap ini bertujuan untuk memastikan bahwa lokasi penelitian mendukung proses pengambilan data.

d. Identifikasi Topologi dan Infrastruktur Jaringan

Pada tahap ini peneliti mengidentifikasi struktur jaringan, meliputi topologi jaringan, perangkat utama seperti router dan access point, serta perangkat client yang menghasilkan trafik jaringan. Tujuannya adalah memahami alur komunikasi data dalam jaringan lokal.

e. Apakah Struktur Jaringan Dapat Diamati?

Tahap ini merupakan titik keputusan. Jika Ya, penelitian dilanjutkan ke tahap observasi teknis jaringan. Jika Tidak, peneliti melakukan koordinasi dengan

administrator jaringan untuk memperoleh informasi tambahan atau melakukan penyesuaian lokasi dan waktu pengamatan.

f. Lanjut ke Observasi Teknis Jaringan

Peneliti melakukan pengamatan terhadap pola trafik jaringan secara umum, seperti jam sibuk, jenis aktivitas pengguna, serta karakteristik trafik normal yang muncul dalam jaringan.

g. Koordinasi dengan Administrator Jaringan

Apabila struktur jaringan tidak dapat diamati secara langsung, peneliti melakukan komunikasi dengan administrator jaringan untuk mendapatkan data teknis, penjelasan topologi, serta izin atau penyesuaian teknis yang diperlukan.

h. Penentuan Parameter Analisis

Berdasarkan hasil observasi dan informasi teknis yang diperoleh, peneliti menetapkan parameter yang akan digunakan dalam analisis statistik, seperti jumlah paket, ukuran paket, interval waktu pengiriman paket, protokol, alamat IP, dan port jaringan.

i. Persiapan Perangkat dan Software

Peneliti menyiapkan perangkat keras dan perangkat lunak, termasuk instalasi dan konfigurasi Wireshark serta alat bantu perhitungan statistik yang akan digunakan dalam proses pengujian metode.

j. Lanjut ke Tahap Analisis

Penelitian masuk ke tahap inti, yaitu pengambilan data trafik jaringan menggunakan Wireshark, penerapan metode *Statistical Anomaly Detection*, serta analisis paket jaringan yang terindikasi sebagai aktivitas mencurigakan.

k. Selesai

Tahap akhir yang menandai berakhirnya seluruh rangkaian proses penelitian tahap awal dan kesiapan untuk masuk ke tahap pelaporan dan pembahasan hasil penelitian.

3.4 Instrumen Penelitian

Instrumen penelitian merupakan alat yang digunakan untuk mendukung proses pengumpulan data dan pelaksanaan penelitian. Instrumen dalam penelitian ini disusun sesuai dengan tujuan penelitian, yaitu menguji efektivitas metode *Statistical Anomaly Detection* menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal.

Instrumen penelitian yang digunakan meliputi:

a. Observasi Jaringan

Observasi jaringan dilakukan pada jaringan lokal (Local Area Network/LAN) di lingkungan STMIK Palangkaraya. Observasi bertujuan untuk memahami kondisi jaringan, pola penggunaan jaringan, serta karakteristik trafik jaringan yang dihasilkan oleh aktivitas pengguna. Pada tahap ini, peneliti melakukan pengamatan terhadap infrastruktur jaringan dan aktivitas jaringan yang berlangsung tanpa melakukan perubahan atau gangguan terhadap sistem jaringan yang ada.

b. Pengambilan Data Trafik Jaringan

Pengambilan data trafik jaringan dilakukan melalui proses packet capture menggunakan perangkat lunak Wireshark. Laptop peneliti dihubungkan ke

jaringan lokal yang sama dengan perangkat pengguna sehingga perekaman trafik jaringan dapat dilakukan secara langsung.

Proses pengambilan data dilakukan selama 3 (tiga) hari berturut-turut pada jam operasional jaringan. Rentang waktu ini dipilih untuk memperoleh data yang merepresentasikan variasi pola trafik jaringan harian sehingga metode *Statistical Anomaly Detection* dapat diuji efektivitasnya pada kondisi jaringan yang nyata.

Data hasil packet capture disimpan dalam format .pcap atau .pcapng untuk dianalisis lebih lanjut.

c. Studi Pustaka

Studi pustaka dilakukan dengan mengkaji berbagai sumber referensi yang relevan dengan topik penelitian, seperti buku, jurnal ilmiah, dan publikasi terpercaya yang membahas keamanan jaringan, analisis trafik jaringan, penggunaan Wireshark, serta metode *Statistical Anomaly Detection*.

d. Dokumentasi

Dokumentasi digunakan sebagai instrumen pendukung untuk merekam seluruh kegiatan penelitian, meliputi tangkapan layar proses packet capture, hasil analisis data trafik jaringan, tabel perhitungan statistik, serta catatan pelaksanaan penelitian. Dokumentasi ini berfungsi sebagai bukti pelaksanaan penelitian dan pendukung penyusunan laporan hasil penelitian.

3.5 Analisis Kebutuhan

Analisis kebutuhan dalam penelitian ini disusun untuk mendukung pelaksanaan uji efektivitas metode *Statistical Anomaly Detection* menggunakan Wireshark

dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal. Setiap kebutuhan dianalisis berdasarkan perannya dalam proses pengambilan data trafik jaringan, penerapan metode statistik, serta evaluasi efektivitas metode yang diuji.

a. Kebutuhan Perangkat Keras

Perangkat keras yang dibutuhkan digunakan untuk memastikan proses perekaman dan analisis trafik jaringan dapat berjalan secara optimal. Laptop atau komputer peneliti digunakan sebagai perangkat utama untuk menjalankan Wireshark dan melakukan analisis data. Kartu jaringan (Network Interface Card) diperlukan agar perangkat peneliti dapat terhubung langsung ke jaringan lokal dan menangkap paket data yang melintas.

Perangkat jaringan lokal, seperti router atau access point, berfungsi sebagai media lalu lintas data jaringan yang menjadi objek pengamatan dalam penelitian ini.

b. Kebutuhan Perangkat Lunak

Perangkat lunak digunakan sebagai alat utama dalam proses uji efektivitas metode. Sistem operasi berfungsi sebagai platform untuk menjalankan seluruh aplikasi penelitian. Wireshark digunakan untuk melakukan packet capture dan menampilkan detail paket jaringan yang dianalisis.

Aplikasi pengolah data statistik digunakan untuk menghitung parameter statistik yang diperlukan dalam metode *Statistical Anomaly Detection*, seperti nilai rata-rata, standar deviasi, dan penentuan nilai ambang batas (threshold).

c. Kebutuhan Data Trafik Jaringan

Data yang dibutuhkan dalam penelitian ini adalah data trafik jaringan lokal yang diperoleh dari jaringan lokal di lingkungan STMIK Palangkaraya. Data dikumpulkan melalui proses packet capture menggunakan Wireshark selama 3 (tiga) hari berturut-turut pada jam operasional jaringan.

Data trafik jaringan ini digunakan sebagai dasar untuk membentuk pola trafik normal serta mengidentifikasi penyimpangan pola trafik yang mengiHari pengambilan data: Senin, Rabu, dan Jumat

Waktu pengambilan data:

Pagi : 08.00 – 10.00 WIB

Siang (waktu ramai/peak time) : 10.00 – 12.00 WIB

Sore : 13.00 – 15.00 WIB

Pengambilan data pada rentang waktu tersebut bertujuan untuk menangkap variasi pola trafik jaringan pada kondisi normal dan ramai (peak time), sehingga data yang diperoleh dapat merepresentasikan aktivitas jaringan secara menyeluruh.

Data trafik jaringan ini digunakan sebagai dasar untuk membentuk pola trafik normal serta mengidentifikasi penyimpangan pola trafik yang mengindikasikan adanya aktivitas mencurigakan.ndikasikan adanya aktivitas mencurigakan.

d. Kebutuhan Lingkungan Penelitian

Lingkungan penelitian yang dibutuhkan adalah jaringan lokal (LAN) di lingkungan STMIK Palangkaraya dengan aktivitas pengguna yang aktif dan beragam. Lingkungan ini dipilih karena memungkinkan munculnya variasi

trafik jaringan yang diperlukan untuk menguji efektivitas metode *Statistical Anomaly Detection* dalam mendeteksi aktivitas mencurigakan pada kondisi jaringan nyata.

e. Kebutuhan Metode dan Parameter Analisis

Metode *Statistical Anomaly Detection* membutuhkan parameter statistik sebagai dasar dalam proses deteksi anomali. Parameter yang digunakan meliputi jumlah paket, ukuran paket, interval waktu pengiriman paket, nilai rata-rata (mean), standar deviasi, serta nilai ambang batas (threshold).

Parameter-parameter tersebut digunakan untuk menentukan kondisi trafik normal. Trafik jaringan yang menunjukkan penyimpangan dan melebihi nilai threshold diidentifikasi sebagai anomali dan dianalisis untuk menilai efektivitas metode dalam mendeteksi aktivitas mencurigakan.

3.5.1 Analisis Data

Analisis data dalam penelitian ini dilakukan untuk mengetahui efektivitas metode *Statistical Anomaly Detection* menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal. Proses analisis data dilakukan secara bertahap mulai dari pengumpulan data hingga evaluasi hasil deteksi anomali.

a. Pengumpulan dan Persiapan Data

Data trafik jaringan dikumpulkan melalui proses packet capture menggunakan perangkat lunak Wireshark pada jaringan lokal di lingkungan STMIK Palangkaraya. Pengambilan data dilakukan selama 3 (tiga) hari berturut-turut pada jam operasional jaringan agar data yang diperoleh mencerminkan kondisi trafik jaringan yang nyata.

Data hasil perekaman disimpan dalam format .pcap atau .pcapng. Selanjutnya, data tersebut diseleksi untuk memastikan hanya data yang relevan dengan penelitian yang digunakan, seperti data paket yang menunjukkan aktivitas komunikasi jaringan.

b. Analisis Parameter Statistik

Data trafik jaringan yang telah disiapkan kemudian dianalisis berdasarkan parameter statistik yang telah ditentukan, meliputi jumlah paket, ukuran paket, dan interval waktu pengiriman paket. Dari parameter tersebut dihitung nilai rata-rata (mean) dan standar deviasi untuk menggambarkan karakteristik trafik jaringan normal.

Perhitungan statistik ini bertujuan untuk membentuk pola trafik normal yang menjadi acuan dalam proses pendeteksian anomali.

c. Penentuan Nilai Ambang Batas (Threshold)

Berdasarkan nilai rata-rata dan standar deviasi yang diperoleh, ditentukan nilai ambang batas (threshold) sebagai batas toleransi trafik jaringan normal. Nilai threshold digunakan untuk membedakan antara trafik jaringan yang masih dianggap normal dan trafik jaringan yang telah menyimpang dari pola normal.

Trafik jaringan yang melebihi nilai threshold dikategorikan sebagai trafik anomali.

d. Penerapan Metode *Statistical Anomaly Detection*

Metode *Statistical Anomaly Detection* diterapkan dengan cara membandingkan data trafik jaringan terhadap pola trafik normal dan nilai threshold

yang telah ditentukan. Apabila terdapat penyimpangan nilai parameter yang signifikan dan melewati threshold, maka trafik tersebut diidentifikasi sebagai indikasi adanya aktivitas mencurigakan.

Hasil deteksi anomali dianalisis lebih lanjut menggunakan Wireshark untuk melihat detail paket jaringan yang terindikasi mencurigakan, seperti lonjakan trafik, ukuran paket yang tidak wajar, atau pola komunikasi yang tidak normal.

e. Evaluasi Efektivitas Metode

Evaluasi efektivitas metode dilakukan dengan menilai kemampuan metode *Statistical Anomaly Detection* dalam mendeteksi aktivitas mencurigakan selama periode pengamatan. Evaluasi dilakukan dengan melihat konsistensi hasil deteksi anomali terhadap variasi pola trafik jaringan yang terjadi selama tiga hari pengambilan data.

Hasil evaluasi ini digunakan untuk menyimpulkan apakah metode *Statistical Anomaly Detection* efektif dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal di lingkungan STMIK Palangkaraya.

3.5.2 Analisis Kelemahan

Penelitian uji efektivitas metode *Statistical Anomaly Detection* menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal memiliki keterbatasan pada ketergantungan metode terhadap penentuan pola trafik normal. Pola trafik normal dibentuk berdasarkan data yang dikumpulkan dalam periode tertentu, sehingga apabila data tersebut belum sepenuhnya

merepresentasikan kondisi jaringan yang sebenarnya, maka hasil deteksi anomali berpotensi kurang akurat.

Penentuan nilai ambang batas (threshold) dalam metode *Statistical Anomaly Detection* juga menjadi salah satu kelemahan. Nilai threshold yang terlalu rendah dapat menyebabkan trafik normal teridentifikasi sebagai anomali, sedangkan threshold yang terlalu tinggi dapat mengakibatkan aktivitas mencurigakan tidak terdeteksi. Sensitivitas terhadap perubahan pola trafik jaringan ini memengaruhi tingkat keakuratan hasil deteksi.

Keterbatasan lain terdapat pada rentang waktu pengambilan data trafik jaringan yang relatif singkat, yaitu selama tiga hari berturut-turut. Rentang waktu tersebut mungkin belum mencakup seluruh variasi pola trafik jaringan, terutama pada kondisi tertentu seperti lonjakan aktivitas pengguna atau perubahan kebijakan jaringan yang terjadi di luar periode pengamatan.

Metode analisis yang digunakan dalam penelitian ini hanya memanfaatkan parameter statistik dasar, seperti jumlah paket, ukuran paket, dan interval waktu pengiriman paket. Pendekatan ini belum mampu menangkap karakteristik aktivitas mencurigakan yang lebih kompleks, sehingga hasil deteksi yang diperoleh masih bersifat umum dan belum spesifik pada jenis aktivitas tertentu.

Selain itu, proses pengambilan data trafik jaringan dilakukan melalui satu titik pengamatan menggunakan Wireshark pada perangkat peneliti. Kondisi ini memungkinkan tidak seluruh trafik jaringan dapat terekam secara menyeluruh, terutama pada jaringan dengan topologi yang lebih kompleks, sehingga hasil analisis belum sepenuhnya menggambarkan kondisi jaringan secara keseluruhan.

3.6 Desain

Desain dalam penelitian ini merupakan rancangan sistem analisis yang digunakan untuk menguji efektivitas metode *Statistical Anomaly Detection* yang dikombinasikan dengan analisis paket menggunakan Wireshark dalam mendeteksi aktivitas mencurigakan pada trafik jaringan lokal di lingkungan STMIK Palangkaraya.

Desain disusun untuk menggambarkan alur kerja penelitian secara sistematis, mulai dari proses pengambilan data trafik jaringan, pembentukan pola trafik normal, perhitungan parameter statistik, hingga proses identifikasi dan analisis lanjutan terhadap trafik yang terindikasi sebagai anomali.

Objek desain penelitian ini adalah jaringan lokal (LAN) STMIK Palangkaraya yang digunakan dalam aktivitas operasional sehari-hari, seperti akses sistem akademik, layanan internet, dan komunikasi data antar perangkat. Jaringan diamati dalam kondisi normal serta diberikan skenario peningkatan trafik secara terbatas dan terkendali untuk memunculkan pola penyimpangan yang dapat dianalisis secara statistik.

Komponen utama dalam desain sistem meliputi perangkat client sebagai penghasil trafik jaringan, router atau access point sebagai pengatur lalu lintas data, laptop peneliti yang menjalankan aplikasi Wireshark sebagai alat perekam paket jaringan, serta modul analisis statistik yang digunakan untuk menerapkan metode *Statistical Anomaly Detection*.

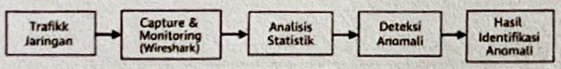
Alur desain sistem dimulai dari aktivitas komunikasi data pada perangkat client. Seluruh paket jaringan yang melintas direkam menggunakan Wireshark dan

disimpan dalam format .pcap atau .pcapng. Data tersebut kemudian diekstraksi untuk memperoleh parameter trafik jaringan, seperti jumlah paket, ukuran paket, dan interval waktu pengiriman paket. Parameter tersebut dianalisis secara statistik dengan menghitung nilai rata-rata (mean), standar deviasi, serta nilai ambang batas (threshold).

Hasil perhitungan statistik digunakan untuk mengidentifikasi adanya penyimpangan pola trafik yang mengindikasikan aktivitas mencurigakan. Trafik yang terdeteksi sebagai anomali selanjutnya dianalisis lebih lanjut menggunakan Wireshark untuk mengetahui karakteristik paket jaringan, seperti protokol yang digunakan, alamat IP sumber dan tujuan, serta port yang terlibat.

Desain sistem analisis ini bertujuan untuk memastikan bahwa proses deteksi aktivitas mencurigakan dilakukan secara terstruktur, terukur, dan dapat direplikasi sesuai dengan metode penelitian eksperimen.

Desain sistem analisis trafik jaringan pada penelitian ini dapat dilihat pada Gambar.



Gambar 3. 2. Desain Sistem Analisis

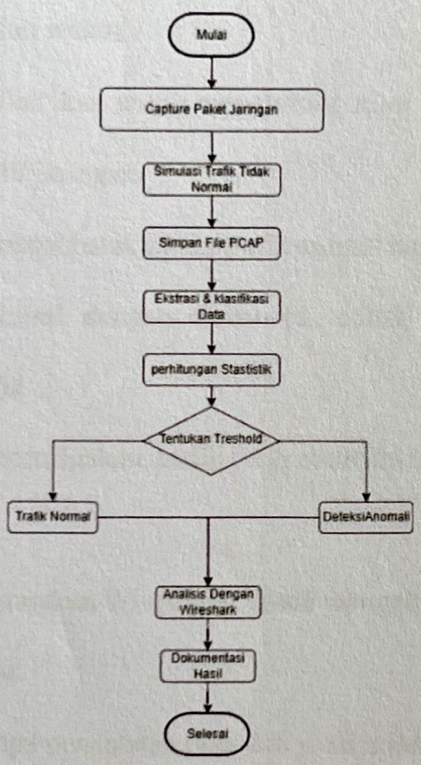
3.6.1 Desain Proses

Desain proses menggambarkan tahapan penelitian dalam bentuk alur kerja yang sistematis untuk mendeteksi aktivitas mencurigakan pada trafik jaringan menggunakan metode *Statistical Anomaly Detection* dan analisis paket Wireshark.

Desain ini disajikan dalam bentuk flowchart untuk memperjelas urutan langkah penelitian dari awal hingga akhir.

Proses penelitian diawali dengan perekaman trafik jaringan pada jaringan lokal STMIK Palangkaraya menggunakan aplikasi Wireshark. Trafik yang direkam mencakup aktivitas jaringan normal serta skenario peningkatan trafik secara terbatas dan terkendali, seperti peningkatan jumlah paket dalam interval waktu tertentu atau percobaan akses ke beberapa port jaringan, dengan tujuan memunculkan pola penyimpangan trafik jaringan.

Tahapan proses analisis adalah sebagai berikut.



Gambar 3. 3. Flowchart Proses Analisis

Tahapan proses analisis adalah sebagai berikut:

a. Mulai, menandakan proses analisis dimulai.
b. Capture paket jaringan, yaitu perekaman trafik jaringan menggunakan Wireshark.
c. Simulasi trafik tidak normal, dilakukan untuk menghasilkan pola anomali pada trafik jaringan.
d. Penyimpanan file PCAP, hasil tangkapan paket disimpan sebagai data penelitian.
e. Ekstraksi dan klasifikasi data, paket dipisahkan berdasarkan protokol, alamat IP, port, ukuran paket, dan waktu.
f. Perhitungan statistik, dilakukan untuk menghitung nilai rata-rata (mean) dan standar deviasi data trafik jaringan.
g. Penentuan threshold, sebagai batas antara trafik normal dan trafik tidak normal.
h. Perbandingan trafik aktual dengan threshold, untuk mendeteksi adanya penyimpangan pola trafik.
i. Identifikasi aktivitas mencurigakan, trafik yang melebihi threshold ditandai sebagai anomali.
j. Analisis lanjutan menggunakan Wireshark, untuk mengetahui karakteristik paket jaringan yang terlibat.
k. Dokumentasi hasil, berupa pencatatan pola dan jenis anomali yang terdeteksi.
l. Selesai, menandakan seluruh proses analisis telah selesai dilakukan.

3.6.2 Desain Perangkat

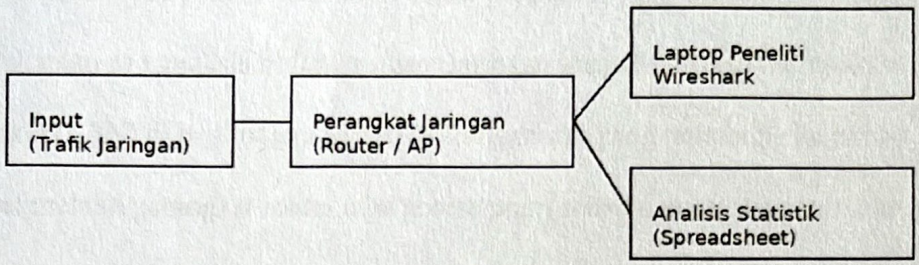
Desain perangkat digunakan untuk menggambarkan komponen perangkat keras dan perangkat lunak yang digunakan dalam proses analisis aktivitas mencurigakan pada trafik jaringan. Pada penelitian ini tidak dibuat aplikasi khusus dengan tampilan antarmuka, sehingga desain perangkat difokuskan pada perangkat keras, perangkat lunak, serta diagram blok sistem yang mendukung proses penelitian.

Perangkat keras yang digunakan dalam penelitian ini meliputi perangkat jaringan dan perangkat pemrosesan data. Perangkat jaringan berupa router atau access point berfungsi sebagai media lalu lintas data antar perangkat dalam jaringan lokal. Laptop atau komputer peneliti digunakan sebagai perangkat utama untuk menjalankan aplikasi Wireshark, menyimpan data hasil perekaman, serta melakukan pengolahan dan analisis data statistik.

Perangkat lunak yang digunakan terdiri dari sistem operasi yang mendukung proses analisis jaringan, aplikasi Wireshark sebagai alat perekam dan analisis paket jaringan, serta aplikasi pengolah data statistik seperti spreadsheet untuk membantu proses perhitungan nilai statistik. Seluruh perangkat lunak tersebut digunakan secara terintegrasi untuk mendukung proses penelitian.

Desain perangkat dalam penelitian ini juga digambarkan dalam bentuk diagram blok untuk menunjukkan hubungan antar komponen sistem. Diagram blok

menggambarkan alur input berupa trafik jaringan, proses perekaman dan analisis data, hingga keluaran berupa hasil identifikasi aktivitas mencurigakan.



Gambar 3. 4. Desain Perangkat

a. Input (Trafik Jaringan)

   Merupakan data berupa paket jaringan yang dihasilkan dari aktivitas komunikasi pada jaringan lokal.

b. Perangkat Jaringan (Router / Access Point)

   Berfungsi sebagai penghubung dan pengatur lalu lintas data antar perangkat dalam jaringan.

c. Laptop Peneliti dengan Wireshark

   Digunakan untuk merekam paket jaringan melalui proses *packet capture* serta melakukan analisis awal terhadap trafik jaringan.

d. Analisis Statistik (Spreadsheet)

   Digunakan untuk mengolah data trafik jaringan secara statistik guna mengidentifikasi penyimpangan pola trafik yang mengindikasikan aktivitas mencurigakan.

3.6.3 Desain Jaringan

Desain jaringan dalam penelitian ini menggambarkan arsitektur jaringan lokal yang menjadi objek pengamatan serta posisi perangkat yang digunakan dalam proses perekaman dan analisis trafik jaringan. Jaringan yang digunakan merupakan jaringan lokal (LAN) di lingkungan STMIK Palangkaraya yang terhubung ke jaringan internet melalui perangkat router atau access point sebagai pusat pengatur lalu lintas data.

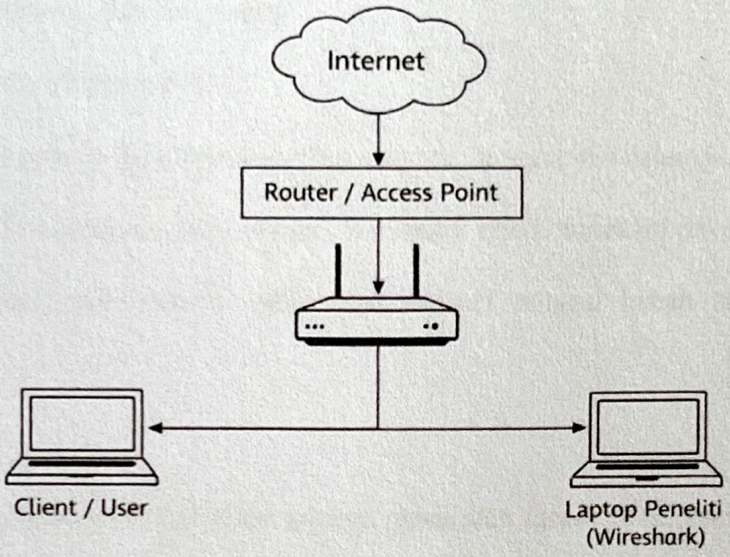
Arsitektur jaringan terdiri atas tiga komponen utama, yaitu jaringan internet sebagai sumber koneksi eksternal, router atau access point sebagai penghubung dan pengatur distribusi paket data, serta perangkat pengguna (client) dan laptop peneliti sebagai bagian dari jaringan internal. Seluruh perangkat terhubung dalam satu segmen jaringan sehingga memungkinkan proses perekaman paket dilakukan secara langsung tanpa mengganggu aktivitas operasional jaringan.

Perangkat client berfungsi sebagai penghasil trafik jaringan melalui aktivitas seperti akses sistem akademik, penelusuran internet, dan komunikasi data lainnya. Trafik yang dihasilkan oleh client akan melewati router atau access point sebelum diteruskan ke jaringan luar. Pada saat yang sama, laptop peneliti ditempatkan pada jaringan yang sama dan dikonfigurasikan untuk menjalankan aplikasi Wireshark guna melakukan packet capture terhadap paket data yang melintas.

Konfigurasi ini memungkinkan laptop peneliti untuk merekam dan mengamati trafik jaringan secara pasif, sehingga tidak memengaruhi kinerja jaringan maupun aktivitas pengguna lain. Data trafik yang terekam selanjutnya disimpan dalam format .pcap atau .pcapng dan digunakan sebagai input pada proses analisis

statistik untuk mendeteksi adanya penyimpangan pola trafik yang mengindikasikan aktivitas mencurigakan.

Dengan desain jaringan tersebut, proses penelitian dapat dilakukan secara terstruktur, aman, dan sesuai dengan kondisi jaringan nyata di lingkungan STMIK Palangkaraya, sehingga hasil analisis yang diperoleh dapat merepresentasikan kondisi operasional jaringan yang sesungguhnya.



Gambar 3. 5. Desain Jaringan

a. Internet

Internet berfungsi sebagai sumber dan tujuan komunikasi data. Seluruh permintaan dan respons data dari jaringan lokal berasal dan menuju ke jaringan internet.

b. Router / Access Point

Router atau access point menerima koneksi dari internet dan mendistribusikan akses jaringan ke perangkat yang terhubung di jaringan lokal.

Perangkat ini menjadi jalur utama keluar-masuk paket data antara internet dan jaringan lokal.

c. Client / User

Perangkat client terhubung ke router atau access point dan menghasilkan trafik jaringan melalui aktivitas penggunaan jaringan. Paket data dari client dikirim ke router untuk diteruskan ke internet, dan sebaliknya menerima respons data melalui jalur yang sama.

d. Laptop Peneliti (Wireshark)

Laptop peneliti juga terhubung ke router atau access point dalam jaringan yang sama. Perangkat ini menjalankan Wireshark untuk merekam paket data yang melintas antara client, router, dan internet sebagai bahan analisis penelitian.

e. Alur Data

Alur data berjalan dari client menuju router atau access point, kemudian diteruskan ke internet. Respons dari internet kembali melalui router menuju client. Pada saat yang sama, laptop peneliti merekam paket-paket yang melintas pada jaringan lokal tersebut.

3.7 Jadwal Penelitian

Jadwal penelitian ini disusun untuk menggambarkan tahapan kegiatan penelitian yang dilakukan oleh peneliti sesuai dengan metodologi dan desain penelitian yang telah dijelaskan pada bab sebelumnya. Penelitian ini dilaksanakan mulai bulan Oktober 2025 sampai Januari 2026. Rincian jadwal penelitian ditunjukkan pada Tabel 3.1.

Tabel 3. 2. Jadwal penelitian Tugas Akhir

No.	Tahapan	Oktober 2025				November 2025				Desember 2025				Januari 2025			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
1.	Identifikasi masalah dan penentuan judul	■	■														
2.	Studi literatur dan pengum-pulan referensi		■	■	■	■											
3.	Penyusunan proposal Tugas Akhir						■	■	■	■	■	■	■				
4.	Revisi proposal berdasarkan bimbingan										■		■	■	■		
5	Perancangan desain penelitian						■	■	■	■	■	■	■	■	■		
6	Perekaman trafik jaringan menggunakan Wireshark								■	■	■	■	■	■	■		
7	Analisis data trafik jaringan (Statistical Anomaly)						■	■	■	■	■	■	■	■	■		
8	Penyusunan laporan proposal akhir												■	■	■		

DAFTAR PUSTAKA

ASDF.id, 2025. Packet Sniffer: Arti, Kegunaan dari Segi Positif dan Negatif. Tersedia pada: https://www.asdf.id/packet-sniffer-adalah/

K.A., 2025. Deteksi anomali trafik jaringan dan aktivitas pengguna menggunakan *Isolation Forest*. Jurnal Pendidikan dan Teknologi Indonesia. Available at: https://jpti.journals.id/index.php/jpti/article/view/790

Nugroho, K.A., Hariguna, T. and Barkah, A.S., 2025. Deteksi anomali trafik jaringan dan aktivitas pengguna menggunakan Isolation Forest. Jurnal Pendidikan dan Teknologi Indonesia. Available at: https://jpti.journals.id/index.php/jpti/article/view/790

Pusat Komputer Universitas Medan Area (Puskom UMA), 2023. Wireshark: Perangkat Lunak Analisis Jaringan. Tersedia pada: https://puskom.uma.ac.id/2023/11/wireshark-perangkat-lunak-analisis-jaringan/

Putri, A.F., Hadi, A. and Rusdiana, L., 2025. Analisis trafik jaringan menggunakan Wireshark untuk deteksi serangan deauthentication. Jurnal Saintekom, 15(2). Available at: https://ojs.stmikplk.ac.id/index.php/saintekom/article/view/967

Rahman, R. and Iswan, E.F., 2024. Implementasi network traffic analysis untuk mendeteksi anomali jaringan pada Twitter/X dan Instagram. Digital Business and Entrepreneurship Journal, 2(2). Available at: https://journal.feb.uniku.ac.id/digibe/article/view/31

Rozi, N.R.F., 2025. Analisis network incident packet capture (PCAP) menggunakan Wireshark. Journal of Informatics and Communication Technology (JICT), 5(2). Available at: https://ejournal.akademitelkom.ac.id/j_ict/index.php/j_ict/article/view/239

Rusdiana, LManalu, M.I. and Hutabarat, F.P., 2024. Network traffic anomaly detection using the decision tree method. Jurnal Metrokom. Available at: https://ejournal.ypayb.or.id/index.php/metrokom/article/view/12Nugroho,

TKJ SMK Darmasis Sidoarjo, 2024. Cara Menggunakan Wireshark untuk Analisis Lalu Lintas Jaringan. Tersedia pada: https://tkj.smkdarmasiswasidoarjo.sch.id/2024/10/28/cara-menggunakan-wireshark/

Zhang, W. and Lazaro, J.P., 2024. A survey on network security traffic analysis and anomaly detection techniques. International Journal of Emerging Technologies and Advanced Applications. Available at: https://www.ijetaa.com/article/view/117

LAMPIRAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS PEMBIMBING TUGAS AKHIR
NO. 317/STMIK-3.C.2/AU/XI/2025

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan nama-nama tersebut di bawah ini :

1. Nama : Ir. Abdul Hadi, S.T., M.Kom
   NIK : 198505102021101
   Sebagai Pembimbing I dalam **PEMBUATAN PROGRAM**
2. Nama : Sam'ani, S.T., M.Kom
   NIK : 197703252005105
   Sebagai Pembimbing II dalam **PENULISAN TUGAS AKHIR**

Untuk membimbing Tugas Akhir mahasiswa :

Nama	:	SHELLA APRIANTI KRISTINA
NIM	:	C2255201118
Program Studi	:	TEKNIK INFORMATIKA (55201)
Tanggal Daftar	:	02/10/2025
Judul Tugas Akhir	:	ANALISIS AKTIVITAS MENCURIGAKAN PADA TRAFIK JARINGAN MENGGUNAKAN METODE STATISTICAL ANOMALY DAN WIRESHARK

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya, dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 01 Desember 2025

Ketua Program Studi,

Desember 2025

Ir. Abdul Hadi, S.T., M.Kom
NIP. 198505102021101

TEMBUSAN :
1. Pembimbing I dan II
2. Mahasiswa yang bersangkutan
3. Arsip Prodi TI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangkaraya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

KARTU KEGIATAN KONSULTASI TUGAS AKHIR

Nama Mahasiswa : CHELLA APRIANTI KRISTINA
NIM : C2255201118
Tanggal Persetujuan Judul : 29 November 2025
Judul Tugas Akhir : Analisis Aktivitas Mencurigakan Pada Trafik Jaringan Menggunakan Metode Statical Anomali dan Wireshark

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
1	12/12/2025	13/12/2025	menggantti warna gambar use case dari hitam menjadi putih	
2	12/12/2025	15/12/2025	memperbaiki daftar pustaka	
		17/12/25	- Bertambah penjelasan pada latar belakang masalah	
		9/12/25	- Revisi bab I	
		18/12/2025	Revisi Gagasan Instrumen penelitian.	
		18/12/25	- Revisi bab II	
		20/12/25	- perbaikan dana penelitian	
		20/12/25	- Revisi bab III	
		3/1/26	- Lengkapi naskah proposal	
		6/1/26	Acc Seminar	
		6/1/26	- Acc Daftar Seminar Proposal	

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS
PENGUJI SEMINAR PROPOSAL TUGAS AKHIR

377/STMIK-3.C.2/AU/I/2026

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan kepada nama-nama berikut :

1. Nama : Amaya Andri Damaini, S.Kom., M.T.
   NIK : 199309042018001
   Sebagai Ketua
2. Nama : Ir. Abdul Hadi, S.T., M.Kom
   NIK : 198505102021101
   Sebagai Sekretaris
3. Nama : Sam'ani, S.T., M.Kom
   NIK : 197703252005105
   Sebagai Anggota

Untuk menguji seminar proposal tugas akhir mahasiswa :

Nama Mahasiswa	:	Shella Aprianti Kristina
N I M	:	C2255201118
Hari / Tanggal Ujian	:	Kamis, 15 Januari 2026
Waktu	:	08.00 WIB
Ruangan	:	TI 3
Judul TA	:	ANALISIS AKTIVITAS MENCURIGAKAN PADA TRAFIK JARINGAN MENGGUNAKAN METODE STATISTICAL ANOMALY DAN WIRESHARK

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 12 Januari 2026

Ketua Program Studi Teknik Informatika,

Ir. Abdul Hadi, S.T., M.Kom
NIK. 198505102021101

Tembusan :
1. Dosen Penguji
2. Mahasiswa yang Bersangkutan
3. Arsip

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

BERITA ACARA
SEMINAR PROPOSAL TUGAS AKHIR

Periode : Januari 2026

Pada hari ini Kamis, 15 Januari 2026 Pukul 08.00 WIB sampai dengan ..... WIB telah dilaksanakan Seminar Proposal Tugas Akhir mahasiswa atas nama :

Nama Mahasiswa	:	Shella Aprianti Kristina
N I M	:	C2255201118
Program Studi	:	Teknik Informatika
Tahun Angkatan	:	2022
Judul TA	:	ANALISIS AKTIVITAS MENCURIGAKAN PADA TRAFIK JARINGAN MENGGUNAKAN METODE STATISTICAL ANOMALY DAN WIRESHARK

Dosen Penguji :

	Nama		Nilai	Tanda Tangan
1.	Amaya Andri Damaini, S.Kom., M.T	=	.....	(.....)
2.	Ir. Abdul Hadi, S.T., M.Kom	=	.....	(.....)
3.	Sam'ani, S.T., M.Kom	=	.....	(.....)

Hasil Ujian : **LULUS / ~~TIDAK LULUS~~** *) NILAI = ... 82,5 .....

Revisi (~~Tidak Ada~~ / ~~Minor~~ / Mayor *)

Catatan Penting :
1. Lama Perbaikan : ..... 10 ..... hari (Maks. 15 hari)
2. Jika lebih dari 1 (satu) bulan dikenakan denda Rp. 300.000,- (Tiga Ratus ribu rupiah) per bulan dari tanggal ujian.
3. Jika lebih dari 3 (tiga) bulan dari tanggal ujian maka hasil ujian dibatalkan dan wajib mengajukan judul dan pembimbing baru. Wajib membayar Denda dan membayar biaya seminar ulang.

Palangka Raya, 15 Januari 2026

Ketua Penguji,

Amaya Andri Damaini, S.Kom., M.T
NIK. 199309042018001

Mahasiswa,

Shella Aprianti Kristina
NIM. C2255201118

Mengetahui :
Ketua Program Studi Teknik Informatika,

Ir. Abdul Hadi, S.T., M.Kom
NIK. 196505102021101

Tembusan:
Mahasiswa yang bersangkutan
Berita acara ini diberikan setelah menyelesaikan semua revisi dari semua penguji
**) Coret yang tidak perlu*