Studi Komparatif Kinerja Suricata dan Snort untuk Pemantauan Lalu Lintas dan Keamanan Jaringan Universitas Bakrie

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

MUHAMMAD ANSHOR

1222002013

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNIK DAN ILMU KOMPUTER UNIVERSITAS BAKRIE

JAKARTA

2026

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : **Muhammad Anshor**

NIM : **1222002013**

Tanda Tangan : 

Tanggal : **16 Februari 2026**

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Muhammad Anshor

NIM : 1222002013

Program Studi : Sistem Informasi

Fakultas : Fakultas Teknik dan Ilmu Komputer

Judul Skripsi : Studi Komparatif Kinerja Suricata dan Snort untuk Pemantauan Lalu Lintas dan Keamanan Jaringan Universitas Bakrie.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Sistem Informasi Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie.

DEWAN PENGUJI

Pembimbing 1 : Dita Nurmadewi S.Kom., M.Kom. ()

Pembimbing 2 : Dr. Shidiq Al Hakim S.T., M.Eng. ()

Penguji 1 : Zakiul Fahmi Jailani S.Kom., M.Sc. ()

Penguji 2 : Haris Rafi, S.Kom., M.Kom. ()

Ditetapkan di jakarta

Tanggal 16 Februari 2026

UNGKAPAN TERIMA KASIH

Puji Syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat, taufik, serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Studi Komparatif Kinerja Suricata dan Snort untuk Pemantauan Lalu Lintas dan Keamanan Jaringan Universitas Bakrie" dengan baik dan tepat waktu.

Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan program studi S1 Sistem Informasi di Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie. Dalam proses penyusunan dan penyelesaian skripsi ini, penulis telah menerima banyak dukungan, bimbingan, serta arahan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati penulis menyampaikan ucapan terima kasih dan penghargaan yang sebesar-besarnya kepada:

1. Ibu Dita Nurmadewi, S.Kom., M.Kom., selaku Dosen Pembimbing I, yang telah dengan sabar memberikan bimbingan, arahan, serta saran berharga dalam setiap tahap penyusunan skripsi ini.
2. Bapak Dr. Shidiq Al Hakim, S.T., M.Eng., selaku Dosen Pembimbing II, yang telah memberikan masukan, koreksi, serta motivasi yang membantu penyempurnaan penelitian ini.
3. Bapak Zakiul Fahmi Jailani, S.Kom., MSc., selaku Dosen Penguji I, yang telah memberikan kritik, saran, serta masukan konstruktif selama proses seminar proposal dan ujian skripsi sehingga membantu penulis dalam memperbaiki hasil penelitian ini.
4. Bapak Haris Rafi, S.Kom., M.Kom., selaku Dosen Penguji II, yang telah memberikan arahan, evaluasi, dan umpan balik yang sangat berharga dalam penyempurnaan isi serta hasil penelitian ini.
5. Seluruh dosen dan staf Program Studi Sistem Informasi Universitas Bakrie, yang telah memberikan ilmu, dukungan, dan pelayanan terbaik selama masa perkuliahan.
6. Seluruh keluarga besar *Bakrie Technology Information* (BTI) yang telah memberikan izin, waktu, dan data yang diperlukan dalam proses penelitian ini.
7. Kedua orang tua tercinta, Bapak Emelyon dan Ibu Evi Rahmi, atas doa, kasih sayang, serta dukungan yang tiada henti hingga penulis dapat menyelesaikan studi ini dengan baik.

8. Wulandari, yang senantiasa memberikan semangat, dukungan moral, serta doa yang tulus dalam setiap proses penyusunan skripsi ini.
9. Rekan-rekan terbaik, M Bagas Ferdiansyah, Ilham Rachmadhani, Sekar Salsabilla Putri, Siti Noor Meisyakirah, Putri Jihan Rahmadani, Nathasya Fauziani Kusuma dan Tya Armelia yang telah memberikan bantuan, dukungan, dan semangat selama penelitian ini berlangsung.
10. Serta seluruh pihak yang tidak dapat disebutkan satu per satu, namun telah membantu dan memberikan dukungan dalam penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi penyempurnaan karya ilmiah ini di masa mendatang. Semoga hasil penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang sistem informasi dan penerapan sistem monitoring pada pengembangan keamanan dan pemantauan jaringan.

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai sivitas akademik Universitas Bakrie, saya yang bertanda tangan dibawah ini:

Nama	: Muhammad Anshor
NIM	: 1222002013
Program Studi	: Sistem Informasi
Fakultas	: Fakultas Teknik dan Ilmu Komputer
Jenis Tugas Akhir	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif** (Non-exclusive Royalti-Free Right) atas karya ilmiah saya yang berjudul:

Studi Komparatif Kinerja Suricata dan Snort untuk Pemantauan Lalu Lintas dan Keamanan Jaringan Universitas Bakrie.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada Tanggal : 16 Februari 2026

Yang Menyatakan

(Muhammad Anshor)

Studi Komparatif Kinerja Suricata dan Snort untuk Pemantauan Lalu Lintas dan Keamanan Jaringan Universitas Bakrie

Muhammad Anshor

ABSTRAK

Perkembangan teknologi informasi meningkatkan risiko ancaman serangan siber seperti *Botnet* dan *Denial of Service* (DoS), yang dapat mengganggu layanan akademik. Saat ini, Biro Teknologi Informasi (BTI) Universitas Bakrie belum memiliki sistem *Intrusion Detection System* (IDS) yang terintegrasi, sehingga penanganan ancaman masih bersifat reaktif. Penelitian ini dilakukan untuk mengkaji perbandingan kinerja antara dua perangkat lunak IDS *open-source* populer, yaitu Suricata dan Snort, guna memberikan rekomendasi sistem yang paling sesuai untuk lingkungan kampus. Metode penelitian yang digunakan adalah eksperimen kuantitatif dengan simulasi pada lingkungan virtual menggunakan VirtualBox. Parameter pengujian meliputi akurasi deteksi, efisiensi penggunaan sumber daya (CPU dan RAM), serta latensi waktu deteksi terhadap serangan *Port Scanning* dan DoS. Hasil penelitian menunjukkan bahwa Suricata memiliki kinerja yang lebih baik dibandingkan Snort. Berkat arsitektur *multi-threading*, Suricata mampu mendistribusikan beban pemrosesan secara merata dengan penggunaan CPU aplikasi mencapai 44,6% saat serangan padat, sementara Snort mengalami *bottleneck* pada satu inti prosesor (penggunaan CPU aplikasi hanya 1,3%). Suricata juga mencatatkan latensi deteksi yang sangat rendah (< 1 ms) dibandingkan Snort (~100 ms). Dari sisi fungsionalitas, format log EVE JSON pada Suricata memberikan data forensik yang lebih detail dan modern dibandingkan log berbasis teks pada Snort.

Studi Komparatif Kinerja Suricata dan Snort untuk Pemantauan Lalu Lintas dan Keamanan Jaringan Universitas Bakrie

Muhammad Anshor

ABSTRACT

The rapid development of information technology increases the risk of cyber threats such as Botnets and Denial of Service (DoS), which can disrupt academic services. Currently, the Information Technology Bureau (BTI) of Bakrie University does not have an integrated Intrusion Detection System (IDS), making threat handling reactive rather than proactive. This study was conducted to perform a comparative analysis between two popular open-source IDS software, Suricata and Snort, to provide a system recommendation suitable for the campus environment. The research methodology employed was a quantitative experiment simulated in a virtual environment using VirtualBox. Testing parameters included detection accuracy, resource utilization efficiency (CPU and RAM), and detection latency against Port Scanning and DoS attacks. The results indicate that Suricata performed better than Snort. Due to its multi-threading architecture, Suricata efficiently distributed processing loads, reaching 44.6% application CPU usage during peak attacks, while Snort suffered from a bottleneck on a single processor core (only 1.3% application CPU usage). Suricata also recorded significantly lower detection latency (< 1 ms) compared to Snort (~100 ms). Functionally, Suricata's EVE JSON log format provides more detailed and modern forensic data than Snort's text-based logs.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN