PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Kelulusan
Jenjang Strata Satu Pada Program Studi Teknik Informatika

Oleh

Tri Witono Yuliantoro

2155201164

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH BENGKULU
2026

LEMBAR PERSETUJUAN

PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL

Oleh
Tri Witono Yuliantoro
2155201164

Tugas Akhir Ini Telah Diterima dan Disahkan
untuk Memenuhi Persyaratan Mencapai Gelar
SARJANA KOMPUTER(S.Kom)

Pada
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK UNIVERSITAS MUHAMMADIYAH BENGKULU

Bengkulu, 6 April 2026
Disetujui Oleh

Ketua Program Studi,	Dosen Pembimbing,
Ardi Wijaya, S.Kom., M.Kom.	Dr. Yulia Darmi, S.Kom., M.Kom.
NP. 19880511 201408 1 181	NIDN. 0210067002

LEMBAR PERSETUJUAN REVISI

PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL

Oleh

Tri Witono Yuliantoro

2155201164

Telah Melakukan Revisi Sesuai Dengan Perubahan
dan Perbaikan yang Diminta Pada Saat Sidang Tugas Akhir.

Bengkulu, 10 April 2026

Menyetujui

No	Nama Dosen	Keterangan	Tanda Tangan
1	RG Guntur Alam, M.Kom., Ph.D	Ketua Penguji	
2	A.R. Walad Mahfuzhi, S.Kom., M.Kom	Penguji 1	
3	Dr. Yulia Darmi, S.Kom., M.Kom	Penguji 2	

Mengetahui

Ketua Program Studi Teknik Informatika

Ardi Wijaya, S.Kom., M.Kom.

NP.19880511 201408 1 181

LEMBAR PENGESAHAN

PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Kelulusan
Jenjang Strata Satu Pada Program Studi Teknik Informatika

Oleh
Tri Witono Yuliantoro
2155201164

Bengkulu, 10 April 2026

No	Nama Dosen	Keterangan	Tanda Tangan
1	RG Guntur Alam, M.Kom,. Ph.D	Ketua Penguji	
2	A.R. Walad Mahfuzhi, S.Kom., M.Kom	Penguji 1	
3	Dr. Yulia Darmi, S.Kom., M.Kom.	Penguji 2	

Mengesahkan
Dekan Fakultas Teknik

RG Guntur Alam, M.Kom., Ph.D
NP. 19730101 200004 1 040

SURAT PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Tri Witono Yuliantoro
NPM	: 2155201164
Program Studi	: Teknik Informatika
Fakultas	: Teknik

Dengan ini saya menyatakan bahwa Skripsi yang saya tulis dengan judul **"PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL"** merupakan hasil karya saya sendiri dan bukan merupakan duplikasi atau plagiat dari peneltiti pihak lain. Sepengetahuan saya, topik dan judul skripsi ini belum pernah ditulis oleh orang lain sebelumnya. Apabila dikemudian hari terbukti bahwa skripsi ini merupakan hasil duplikasi atau plagiasi dari penelitian orang lain, saya siap menerima sanksi sesuai dengan ketentuan yang berlaku.

Demikian peryataan ini saya buat dengan sebenar-benarnya tanpa adanya tekanan atau paksaan dari pihak manapun.

Bengkulu, 8 April 2026

Yang Menyatakan,

Tri Witono Yuliantoro
NPM. 2155201164

DAFTAR RIWAYAT HIDUP

1. Data Pribadi

Nama	:	Tri Witono Yuliantoro
TTL	:	Pal Tiga Puluh, 02 Juli 2003
Agama	:	Islam
Anak ke	:	3 (tiga) dari 4 (empat) bersaudara
Alamat	:	Dusun Hibrida, Pal Tiga Puluh, Lais, Bengkulu Utara

2. Identitas Orang Tua

Nama Ayah	:	Suwita
Pekerjaan	:	Wiraswasta
Nama Ibu	:	Siti Wijiyati
Pekerjaan	:	Wiraswasta

3. Riwayat Pendidikan

1.	SD Negeri 18 Bengkulu utara	:	2009-2015
2.	MTs Negeri 3 Bengkulu Utara	:	2015-2018
3.	SMA Negeri 3 Bengkulu Utara	:	2018-2021
4.	Universitas Muhammadiyah Bengkulu	:	2021-2026

MOTTO DAN PERSEMBAHAN

MOTTO

“ Kebebasan memberikan kesesatan, manusia menyebutnya dengan pilihan.”

PERSEMBAHAN

Skripsi ini saya persembahkan kepada:

1. Kedua orang tuaku yang selalu setia memberikan doa, kasih sayang, dan dukungan tanpa syarat. Terima kasih atas segala pengorbanan, cinta, dan tuntunan yang tak pernah henti mengalir sejak saya lahir hingga hari ini. Setiap langkah yang saya capai adalah buah dari doa-doa panjang di malam hari yang kalian panjatkan untuk saya. Semoga karya sederhana ini bisa menjadi sedikit dari banyak hal yang membuat kalian bangga. Karya ini kupersembahkan sepenuh hati untuk kalian tiang utama dalam hidup saya.
2. Ibu Dr. Yulia Darmi, S.Kom., M.Kom. Selaku Dosen Pembimbing saya, Terimakasih telah membantu dalam memberikan pemikiran, ide, analisis, dan arahan kepada saya saat mengerjakan proposal dan skripsi hingga saat ini.
3. Sahabat-sahabat terbaikku, yang selalu ada di saat suka dan duka,di tengah lelah kuliah, deadline mepet, dan hari-hari penuh tantangan. Terima kasih atas dukungan, semangat, canda tawa, dan obrolan panjang yang menghangatkan hati. Kalian adalah bagian dari keberhasilan kecil yang kucapai hari ini. Semoga persahabatan kita terus tumbuh,di mana pun kita melangkah.
4. Diriku sendiri, yang tak pernah menyerah di tengah rasa ragu, lelah, dan tekanan. Terimakasih telah terus melangkah, meski kadang tanpa dukungan

yang cukup, meski hati ingin menyerah, kau tetap bangkit dan mencoba lagi. Dan tetap rendah hati, tetap berani bermimpi, dan semoga apa yang saya dapat bisa menjadi amanah bagi saya.

ABSTRAK

PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL

Nama : Tri Witono Yuliantoro

NPM 2155201164

Pembimbing : Dr. Yulia Darmi, S.Kom., M.Kom.

Keamanan informasi pada sistem akademik menjadi hal yang krusial seiring meningkatnya ancaman serangan siber terhadap platform pendidikan. Website SIAKAD Universitas Muhammadiyah Bengkulu yang mengadopsi prinsip Service Oriented Architecture (SOA) mengelola data sensitif mahasiswa dan akademik, sehingga memerlukan pengawasan terhadap aktivitas malicious request. Penelitian ini bertujuan merancang dan membangun aplikasi Log Parser menggunakan bahasa pemrograman Go (Golang) dengan metode DFRWS Investigative Model. Objek penelitian adalah raw access log server HestiaCP SIAKAD UMB sebanyak 45.645 baris yang dikumpulkan dalam kurun waktu sembilan hari. Hasil pengujian menunjukkan aplikasi mampu memproses seluruh log dalam 3,14 detik dengan akurasi parsing 100%. Terdeteksi 3.363 malicious request (7,37%) yang terdiri dari 8 kategori serangan, didominasi Scanning/Reconnaissance (50,6%), Bot/Automated Scanner (29,5%), dan SQL Injection (16,0%). Keterbatasan pada aspek chain of custody terjadi karena data log diperoleh melalui transfer dari staff UPTIK, serta seluruh request tercatat dari satu IP internal akibat konfigurasi reverse proxy yang tidak meneruskan header X-Forwarded-For. Validasi dilakukan melalui simulasi serangan di lingkungan lab menggunakan Wireshark dan menunjukkan konsistensi dengan temuan log server. Penelitian ini diharapkan dapat membantu UPTIK Universitas Muhammadiyah Bengkulu dalam melakukan audit keamanan jaringan dan mitigasi serangan siber secara dini.

Kata Kunci: Log Parser, Golang, DFRWS, SIAKAD, Malicious Request, Keamanan Jaringan.

ABSTRACT

PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL

Name : Tri Witono Yuliantoro

NPM 2155201164

Advisor : Dr. Yulia Darmi, S.Kom., M.Kom.

Information security in academic systems has become crucial as cyberattack threats against educational platforms continue to rise. The SIAKAD website of Universitas Muhammadiyah Bengkulu, which adopts the principles of Service Oriented Architecture (SOA), manages sensitive student and academic data, necessitating the monitoring of malicious request activities. This research aims to design and develop a Log Parser application using the Go (Golang) programming language with the DFRWS Investigative Model method. The research object is the raw access logs from the HestiaCP server of SIAKAD UMB, comprising 45,645 log entries collected over a nine-day period. Testing results show that the application is capable of processing all log entries in 3.14 seconds with 100% parsing accuracy. A total of 3,363 malicious requests (7.37%) were detected, consisting of 8 attack categories, dominated by Scanning/Reconnaissance (50.6%), Bot/Automated Scanner (29.5%), and SQL Injection (16.0%). Limitations in chain of custody occurred because log data was obtained via transfer from UPTIK staff, and all requests were recorded from a single internal IP address due to reverse proxy configuration that does not forward the X-Forwarded-For header. Validation was conducted through a simulated attack in a controlled lab environment using Wireshark, demonstrating consistency with log server findings. This research is expected to assist the UPTIK of Universitas Muhammadiyah Bengkulu in conducting network security audits and early cyberattack mitigation.

Keywords: Log Parser, Golang, DFRWS, SIAKAD, Malicious Request, Network Security.

KATA PENGANTAR

Assalamu'alaikum Warohmatullahi Wabarokatuh.

Puji syukur penulis ucapkan kehadirat Allah Subhanahu Wa Ta'ala, atas berkat, rahmat, ridho dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul: "PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL"

Pada kesempatan ini penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Bapak RG. Guntur Alam, M.Kom, Ph.D selaku Dekan Fakultas Teknik Universitas Muhammadiyah Bengkulu.
2. Bapak Ardi Wijaya, S.Kom, M.Kom selaku Ketua Program Studi Teknik Informatika Universitas Muhammadiyah Bengkulu
3. Dr. Yulia Darmi, S.Kom., M.Kom selaku Dosen Pembimbing dalam penyusunan skripsi
4. Keluarga tercinta yang telah memberikan dukungan moral maupun materi.
5. Sahabat dan teman-teman seperjuangan Teknik Informatika yang selalu memberikan inspirasi, motivasi dan selalu meluangkan waktunya ketika penulis dalam kesulitan.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari kata sempurna. Untuk itu, saran dan kritik yang bersifat membangun sangat penulis harapkan demi penyempurnaan di masa yang akan datang.

Semoga skripsi ini bermanfaat bagi penulis dan pembaca sekalian. Aamiin.

Wassalamu'alaikum Warohmatullahi Wabarokatuh.

Bengkulu, 10 April 2026

Tri Witono Yuliantoro

DAFTAR ISI

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada institusi pendidikan tinggi saat ini telah membawa perubahan besar dalam sistem tata kelola data akademik. Universitas Muhammadiyah Bengkulu (UMB) telah mengadopsi arsitektur layanan yang terintegrasi melalui konsep *Service Oriented Architecture* (SOA) pada Sistem Informasi Akademik (SIAKAD) untuk menjamin efisiensi distribusi layanan data antar unit. Penerapan prinsip SOA pada SIAKAD UMB tercermin dari struktur modularnya yang melayani berbagai unit secara terintegrasi, mulai dari modul kemahasiswaan, akademik, keuangan, hingga kepegawaian dalam satu platform terpusat. Pemanfaatan teknologi informasi ini menjadi faktor krusial dalam meningkatkan akurasi data serta daya saing institusi di era digital(Laudon & Laudon, 2018). Namun, seiring dengan kompleksitas arsitektur yang dibangun, risiko keamanan siber juga meningkat secara signifikan karena banyaknya titik akses layanan yang terbuka (Gilvy Langgawan Putra et al., n.d.). Selain itu, teknik live forensics juga dapat diterapkan untuk mengenali karakteristik serangan tertentu secara langsung pada web server guna meminimalisir dampak kerusakan system (Isriade putra, 2023). Oleh karena itu, penelitian ini berfokus pada pengembangan alat yang mampu melakukan analisis tersebut secara otomatis.

Keamanan aplikasi berbasis web saat ini menjadi tantangan utama karena sering kali gagal dalam memberikan perlindungan maksimal terhadap data sensitif

mahasiswa dan institusi. Banyak sistem aplikasi web yang memiliki celah keamanan kritis akibat kesalahan konfigurasi pada sisi *application server* maupun penggunaan komponen yang sudah tidak didukung keamanannya (Khatib Sulaiman & Pakuan, n.d.). Berdasarkan standar *Open Web Application Security Projec*t (OWASP) Top 10, celah-celah tersebut sering dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan manipulasi trafik atau pencurian data (Pahlawansah et al., 2025). Oleh karena itu, diperlukan mekanisme evaluasi dan monitoring yang ketat pada setiap *endpoint* layanan agar kerentanan dapat diidentifikasi sedini mungkin (Syaifudin et al., 2025).

Salah satu aset digital yang paling berharga dalam upaya deteksi dini serangan adalah rekaman jejak aktivitas pada log server. *Log server* mencatat setiap permintaan (*request*) yang masuk ke sistem, namun volume data yang dihasilkan sangat besar sehingga sulit untuk dianalisis secara manual oleh administrator (Lilhadiksi Razsanjani et al., 2024). Kurangnya kemampuan sistem dalam mendeteksi aktivitas mencurigakan pada log akses sering kali mengakibatkan eksploitasi berlangsung tanpa diketahui (Wibisono, 2025). Untuk mengatasi kendala tersebut, dibutuhkan sebuah alat bantu otomatis (log parser) yang dibangun menggunakan bahasa pemrograman berperforma tinggi. Penggunaan bahasa Go (Golang) dinilai sangat efektif untuk kebutuhan pengolahan string dan analisis log skala besar karena efisiensi memori dan kecepatan eksekusinya dibandingkan bahasa pemrograman lain (Lilhadiksi Razsanjani et al., 2024).

Selain melakukan analisis pada tingkat aplikasi melalui log server, validasi terhadap trafik jaringan secara real-time juga menjadi keharusan dalam proses

investigasi keamanan (Mubarok & Romli, 2024). Analisis jaringan yang mendalam diperlukan untuk mengamati pola serangan seperti Brute Force atau Path Traversal yang mungkin tidak sepenuhnya terdeteksi pada application layer (Mubarok & Romli, 2024). Penggunaan perangkat lunak seperti Wireshark memungkinkan peneliti untuk melakukan packet sniffing dan capturing guna melihat struktur paket data asli yang dikirimkan oleh penyerang (Gilvy Langgawan Putra et al., n.d.). Integrasi antara analisis log dan analisis trafik jaringan akan memberikan tingkat akurasi yang lebih tinggi dalam membedakan antara trafik normal dan malicious request (Rafi et al., 2025). Dalam penelitian ini, validasi jaringan dilakukan melalui simulasi serangan pada lingkungan lab terkontrol menggunakan localhost, sehingga karakteristik paket malicious request dapat direplikasi dan dianalisis tanpa bergantung pada trafik produksi SIAKAD.

Untuk menjamin hasil penelitian yang sistematis dan akurat, diperlukan sebuah metodologi forensik yang terstandarisasi dalam menangani insiden keamanan (Wintolo et al., 2025). Metode *DFRWS Investigative Model* menawarkan tahapan investigasi yang komprehensif, mulai dari fase identifikasi hingga analisis bukti digital secara mendalam (Wintolo dkk., 2025). Penerapan metode ini dinilai sangat relevan untuk membedah jejak digital serangan pada layanan SOA karena sifatnya yang terstruktur dan mampu menghasilkan bukti yang valid. Berdasarkan permasalahan tersebut, maka penelitian ini bertujuan untuk mengimplementasikan metode DFRWS Investigative Model dalam **PENGEMBANGAN APLIKASI LOG PARSER UNTUK DETEKSI POLA SERANGAN PADA WEBSITE**

SIAKAD BERBASIS SOA MENGGUNAKAN METODE DFRWS INVESTIGATIVE MODEL.

1.2 Pertanyaan Penelitian

Bagaimana merancang dan membangun aplikasi Log Parser berbasis Go (Golang) untuk menganalisis pola serangan pada website SIAKAD Universitas Muhammadiyah Bengkulu yang mengadopsi prinsip SOA menggunakan metode DFRWS Investigative Model?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

a. Membangun aplikasi Log Parser menggunakan bahasa pemrograman Go (Golang) untuk mengolah data log server SIAKAD UMB secara otomatis dan efisien.

b. Mengimplementasikan tahapan metode DFRWS Investigative Model dalam mengidentifikasi jejak digital serangan malicious request pada layanan yang mengadopsi prinsip SOA.

c. Melakukan **verifikasi teknis** fungsionalitas aplikasi melalui analisis paket data jaringan menggunakan Wireshark pada lingkungan simulasi terkontrol.

d. Menghasilkan laporan investigasi forensik dan rekomendasi mitigasi keamanan yang tepat guna meningkatkan ketahanan aset digital di lingkungan Universitas Muhammadiyah Bengkulu.

1.4 Kerangka Kerja Penelitian

Kerangka kerja penelitian ini disusun secara sistematis berdasarkan metode DFRWS Investigative Model untuk menjamin validitas hasil investigasi serangan. Tahapan tersebut meliputi :

Gambar 1. 1 Kerangka Kerja Penelitian

Adapun penjelasan teknis dari masing-masing tahapan pada Gambar 1.1 adalah sebagai berikut:

a. Identification (Identifikasi): Mengidentifikasi indikasi serangan pada website SIAKAD UMB melalui pengamatan awal terhadap anomali log dan trafik.

b. Preservation (Pengamanan): Menjamin integritas bukti digital (log server dan file PCAP) agar tetap asli selama proses investigasi forensik dilakukan.

c. Collection (Pengumpulan): Mengambil data log akses dari infrastruktur UPTIK UMB dan melakukan simulasi pengumpulan paket jaringan pada lingkungan lab terkontrol (localhost).

d. Examination (Pemeriksaan): Tahap inti di mana data log diolah menggunakan Aplikasi Log Parser berbasis Golang untuk menemukan pola malicious request secara cepat.

e. Analysis (Analisis): Melakukan verifikasi hasil parsing log dengan menganalisis trafik jaringan menggunakan Wireshark guna memastikan akurasi rule-based detection pada lingkungan simulasi.

f. Presentation (Laporan): Menyajikan hasil temuan bukti digital dalam bentuk laporan resmi serta memberikan rekomendasi mitigasi keamanan kepada pihak kampus.