Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 6565-6572
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Forensik Digital Serangan DoS pada Web Server Menggunakan Metode NIST SP 800-86 dan Suricata IDS

Lilo Wedhar Widyastuti[1], Aqilah Aulya Maulidah[2], Yustian Servanda[3]
[1,2,3]Department of information technologhy, Universitas Mulia
[1]lilowedharw@gmail.com , [2]maulidah.qilah@gmail.com , [3]yustians@universitasmulia.ac.id

Abstrak

Dental caries remains a major global oral health challenge, emphasizing the need for effective, biocompatible, and sustainable remineralization agents. This study aimed to synthesize biogenic nanohydroxyapatite (nHAp) from green mussel shell (Perna viridis) waste through a green synthesis approach and evaluate its physicochemical properties for potential dental remineralization applications. Green mussel shells containing 57.23% calcium were utilized as a natural precursor. The shells were calcined at 900°C to convert calcium carbonate into calcium oxide (CaO), followed by a controlled precipitation process and high-energy ball milling to obtain nanoscale particles. The synthesized material was characterized using Energy Dispersive X-Ray Fluorescence (EDXRF), Fourier Transform Infrared Spectroscopy (FTIR), Particle Size Analysis (PSA), X-Ray Diffraction (XRD), and Scanning Electron Microscopy coupled with Energy Dispersive X-Ray Analysis (SEM-EDX). FTIR results confirmed the formation of hydroxyapatite through the presence of phosphate (PO_4^{3-}), hydroxyl (OH^-), and carbonate (CO_3^{2-}) functional groups. PSA analysis revealed particle sizes ranging from 40 to 60 nm, with the smallest average size of 40 nm obtained using 12 g CaO. XRD patterns exhibited characteristic hydroxyapatite diffraction peaks at approximately 25.9°, 31.8°, 32.9°, and 34.1° (2θ), indicating high crystallinity and phase purity. SEM observations showed predominantly spherical particle morphology, while EDX analysis produced a Ca/P ratio of 1.80. These findings demonstrate that Perna viridis shell waste is a promising and sustainable source for producing nanohydroxyapatite with favorable physicochemical properties for future dental remineralization applications.

Kata Kunci: *Forensik Digital, NIST SP 800-86, Denial of Service, Slowloris, Suricata IDS*

1. Latar Belakang

Perkembangan teknologi informasi yang pesat tidak hanya memberikan kontribusi positif terhadap efisiensi operasional organisasi, namun juga memperluas permukaan serangan (*attack surface*) bagi kejahatan siber. Salah satu ancaman paling persisten dan merusak yang dihadapi oleh penyedia layanan berbasis web adalah serangan *Denial of Service* (DoS). Karakteristik utama dari serangan ini adalah pemaksaan kelumpuhan sistem dengan cara menghabiskan sumber daya komputasi server, baik berupa kapasitas memori, pemrosesan CPU, maupun ketersediaan alokasi lebar pita (*bandwidth*) jaringan. Dampak yang ditimbulkan dari insiden ini sangat signifikan, mulai dari kerugian finansial akibat matinya transaksional bisnis hingga jatuhnya reputasi institusi penyedia layanan [1].

Dalam perkembangannya, taktik serangan DoS tidak lagi hanya mengandalkan pembanjiran paket data berskala masif pada lapisan jaringan (*network layer*), melainkan telah berevolusi ke tingkat aplikasi (*application layer*). Serangan tradisional seperti TCP SYN Flood dan ICMP Flood berfokus pada saturasi jaringan dengan mengirimkan ribuan paket per detik untuk menghabiskan tabel koneksi server [2]. Sebaliknya, serangan modern seperti Slowloris bekerja secara senyap dan efisien dengan memanfaatkan keterbatasan arsitektur *thread* pada *web server* seperti Apache2 [3]. Slowloris memelihara ribuan koneksi HTTP tetap terbuka dengan mengirimkan *header request* yang tidak pernah selesai secara perlahan, sehingga server kehabisan kapasitas soket kerja tanpa memicu alarm penyaringan berbasis volume tradisional [4].

Untuk menghadapi kompleksitas ancaman tersebut, keberadaan sistem deteksi seperti *Intrusion Detection System* (IDS) Suricata menjadi sangat krusial [5]. Namun, deteksi saja tidak cukup untuk memberikan akuntabilitas hukum dan evaluasi mendalam pasca-insiden siber. Diperlukan sebuah pendekatan investigasi yang sistematis melalui disiplin ilmu forensik digital jaringan (*network forensics*). Penyelidikan artefak bukti digital harus didasarkan pada

kerangka kerja yang diakui secara global untuk menjamin validitas dan integritas barang bukti di hadapan hukum [6].

Evaluasi terhadap performa IDS Suricata dalam mengidentifikasi serangan Denial of Service (DoS) sebenarnya telah banyak dieksplorasi pada studi terdahulu. Meski demikian, literatur yang ada umumnya melakukan pengujian secara terpisah, baik terbatas pada saturasi bandwidth pada network layer (TCP SYN Flood) maupun manipulasi thread pada application layer (Slowloris). Keterbatasan analisis komparatif yang menguji kedua vektor serangan ini secara simultan pada target yang sama memunculkan sebuah research gap. Menjawab tantangan tersebut, kebaruan (novelty) penelitian ini terletak pada analisis forensik jaringan komparatif dual-vektor (high-volume versus low-and-slow). Dengan mengorelasikan log alert kualitatif Suricata dan metrik kuantitatif pcap Wireshark, studi ini mampu menyajikan visibilitas bukti digital yang lebih utuh dan mendalam bagi kebutuhan investigasi pasca-insiden siber

Penelitian ini menerapkan metode standar dari *National Institute of Standards and Technology* (NIST) Special Publication 800-86 [1]. Metode ini dipilih karena menyediakan struktur kerja yang metodologis dan berulang (*repeatable*) melalui empat tahapan utama, yaitu pengumpulan data, pemeriksaan, analisis, serta pelaporan [6]. Melalui integrasi antara repositori log Suricata IDS dan berkas tangkap paket (*packet capture*) Wireshark, penelitian ini bertujuan untuk membedakan karakteristik forensik dari serangan *flood* dan serangan *low-and-slow* (Slowloris), sehingga diperoleh pemahaman taktis yang utuh mengenai pola perilaku penyerang demi meningkatkan postur keamanan *web server* [4] [7].

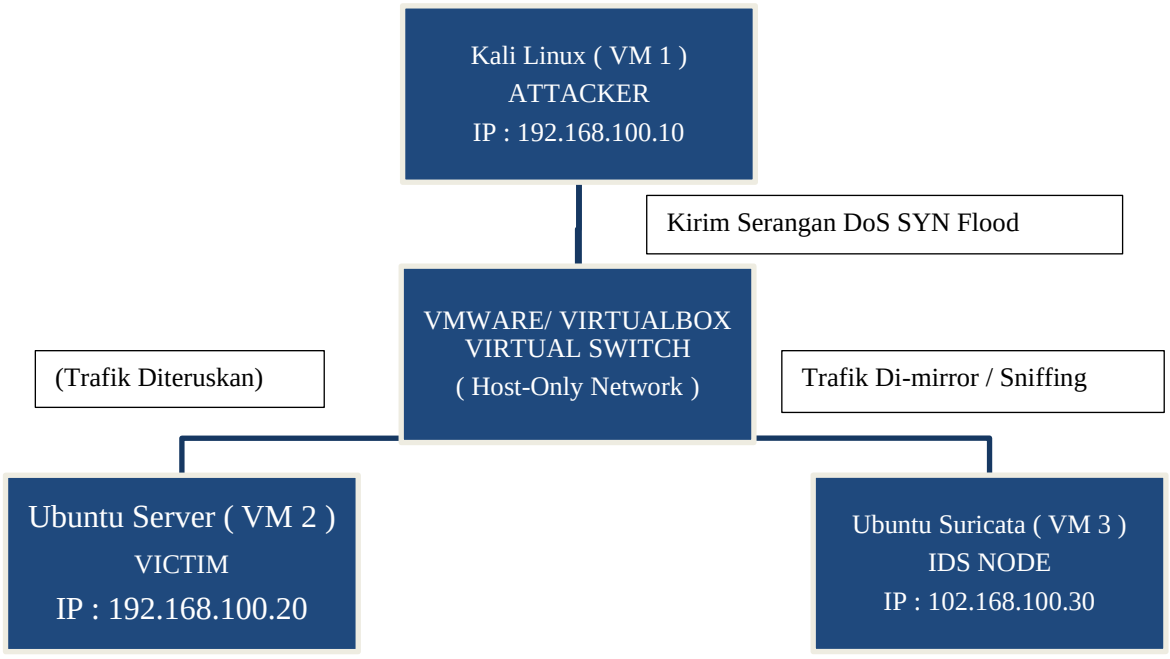
2. Metode Penelitian

Penelitian ini dijalankan dengan mengadopsi metode investigasi forensika digital jaringan berdasarkan panduan standar dari *National Institute of Standards and Technology* (NIST) Special Publication 800-86 [6]. Kerangka kerja ini dipilih karena menyediakan metodologi yang terstruktur, berulang (*repeatable*), dan diakui secara global dalam menjamin integritas penanganan barang bukti elektronik di lingkungan jaringan [6].

2.1 Arsitektur Infrastruktur dan Topologi Jaringan

Sebelum simulasi serangan dan proses akuisisi data dilakukan, sebuah lingkungan laboratorium virtual diisolasi menggunakan arsitektur jaringan lokal berbasis *Host-Only Network* pada perangkat lunak hipervisor. Langkah pengisolasian ini krusial dilakukan guna memastikan bahwa paket data serangan yang dibangkitkan tidak berdampak pada infrastruktur jaringan riil di luar laboratorium penelitian [8]. Secara detail, rancangan penataan node komputasi dan pemetaan alamat IP yang digunakan dalam pengujian ini diilustrasikan melalui topologi jaringan pada Gambar 1.

DOI: https://doi.org/10.31004/riggs.v5i2.9453



Gambar 1. Topologi Jaringan Laboratorium Virtual Investigasi Serangan DoS

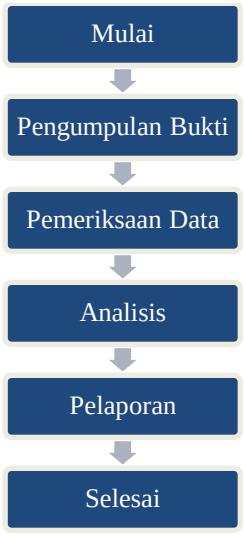
Berdasarkan rancangan arsitektur jaringan pada Gambar 1, infrastruktur penelitian ini melibatkan tiga buah *Virtual Machine* (VM) utama yang saling terhubung dalam satu segmen jaringan yang sama melalui fasilitas *Virtual Switch*. Mesin pertama bertindak sebagai *Attacker Node* dengan sistem operasi Kali Linux (IP 192.168.100.10) yang berfungsi menyimulasikan pengiriman paket data gangguan DoS. Mesin kedua dikonfigurasi sebagai *Victim Node* dengan sistem operasi Ubuntu Server (IP 192.168.100.20) yang menjalankan layanan inti berupa Apache2 Web Server pada port standar 80 (HTTP).

Sementara itu, mesin ketiga bertindak secara taktis sebagai *Intrusion Detection System* (IDS) Node berbasis Ubuntu Suricata (IP 192.168.100.30) [5]. Melalui pemanfaatan fitur pencerminan lalu lintas (*traffic mirroring/sniffing*) pada *Virtual Switch*, kartu jaringan pada IDS Node diatur ke dalam mode *Promiscuous* (ens33) [8]. Pengaturan mode ini memungkinkan Suricata untuk menginspeksi dan menyalin setiap paket data yang mengalir menuju server korban tanpa mengganggu stabilitas performa server utama, yang kemudian akan memproduksi keluaran otentik berupa berkas peringatan fast.log serta berkas tangkap paket mentah (.pcapng).

2.2 Alur Kerja (*Workflow*) Tahapan Forensik NIST SP 800-86

Implementasi investigasi terhadap aktivitas intrusi jaringan dalam penelitian ini dijalankan secara kronologis melalui empat tahapan utama siklus forensik NIST SP 800-86. Alur kerja operasional dari tahapan awal persiapan hingga perumusan laporan dijabarkan secara sistematis pada Gambar 2.

DOI: https://doi.org/10.31004/riggs.v5i2.9453



Gambar 2. Alur Kerja (*Workflow*) Investigasi Forensik Digital Jaringan

Berdasarkan visualisasi tahapan operasional pada Gambar 2, langkah-langkah sistematis dari kerangka kerja penelitian ini dijabarkan sebagai berikut:

1. Fase Pengumpulan (*Collection*): Tahap awal ini berfokus pada penyiapan komponen dasar laboratorium, pengaktifan mesin deteksi Suricata IDS, serta inisiasi pencatatan lalu lintas data secara langsung (*live capture*) menggunakan perkakas Wireshark. Setelah kesiapan instrumen forensik divalidasi, serangan *Denial of Service* (DoS) dibangkitkan dari mesin penyerang menggunakan perkakas hping3 dan skrip Slowloris untuk menciptakan anomali trafik pada server korban [3].
2. Fase Pemeriksaan (*Examination*): Setelah fase serangan selesai dieksekusi, data mentah yang terekam diisolasi ke dalam repositori forensik yang aman. Pada tahap ini, peneliti melakukan ekstraksi terhadap berkas log peringatan fast.log dan berkas bukti hasil_ubuntu.pcapng. Proses reduksi *noise* (pembersihan paket di luar parameter serangan) dilakukan menggunakan fitur *Display Filter* pada Wireshark [9]. Untuk menyaring kode status bendera TCP (*TCP Flags*) secara spesifik [1].
3. Fase Analisis (*Analysis*): Fase ini berfokus pada pembedahan karakteristik struktural dari artefak bukti yang telah dibersihkan. Peneliti menganalisis kesesuaian tanda tangan serangan (*signature rules*) pada Suricata IDS untuk mendeteksi adanya *malicious handshake* [10]. Secara bersamaan, analisis volumetrik dilakukan melalui visualisasi fitur *Wireshark I/O Graphs* guna membedakan pola lonjakan trafik banjir paket dengan pola koneksi gantung (*TCP Retransmission*) pada serangan lapisan aplikasi [4] [11].
4. Fase Pelaporan (*Reporting*): Pada tahap akhir ini, seluruh informasi teknis, metrik parameter jaringan, dan bukti visual log dikumpulkan untuk dipetakan ke dalam tabel komparatif forensik secara terstruktur. Hasil investigasi kemudian disusun ke dalam narasi akademis formal pada naskah hasil dan pembahasan naskah jurnal serta diakhiri dengan perumusan saran rekomendasi mitigasi keamanan bagi administrator sistem di masa mendatang [12].

3. Hasil dan Diskusi

Pada bagian ini dijelaskan mengenai hasil skenario pengujian, konfigurasi taktis, deteksi aktivitas intrusi pada jaringan, serta langkah analisis forensik digital yang dilakukan terhadap infrastruktur *Virtual Machine* (VM).

3.1 Konfigurasi Lingkungan Jaringan (VM)

Sebelum simulasi intrusi dilakukan, setiap *Virtual Machine* telah dikonfigurasi menggunakan beberapa perintah utama melalui antarmuka *bash CLI*. Langkah ini esensial untuk memvalidasi kesiapan *tools* penyerang serta memastikan mesin deteksi IDS memonitor kartu jaringan yang tepat. Berikut merupakan perintah *bash* utama yang dieksekusi pada masing-masing VM:

a. VM Attacker (Kali Linux)

Perintah di bawah ini digunakan untuk mengeksekusi serangan banjir paket TCP SYN, banjir ICMP, dan serangan siber Slowloris pada layer aplikasi secara bergantian:

Bash

```
# Perintah Skenario 1: SYN Flood Attack
hping3 -S --flood -V -p 80 192.168.100.20
# Perintah Skenario 2: ICMP Flood Attack
```

DOI: https://doi.org/10.31004/riggs.v5i2.9453

```
hping3 -1 --flood -V 192.168.100.20
# Perintah Skenario 3: Slowloris Attack (Menggunakan Perl Script)
perl slowloris.pl -dns 192.168.100.20 -options -port 80 -num 500
```

b. VM Victim & IDS Server (Ubuntu Server & Suricata)

Perintah ini dieksekusi untuk memastikan aturan (*rules*) tanda tangan Suricata berada pada versi mutakhir serta mengaktifkan mesin inspeksi paket secara *live* pada antarmuka jaringan ens33:

Bash

```
sudo apt install apache2 -y
sudo suricata-update
sudo suricata -c /etc/suricata/suricata.yaml -i ens33
```

3.2 Deteksi dan Analisis Forensik Jaringan

Setelah ketiga skenario serangan disimulasikan, lalu lintas data (*traffic*) direkam ke dalam berkas tangkap data mentah (.pcapng) untuk memelihara integritas barang bukti elektronik yang sah. Proses analisis dilakukan menggunakan Wireshark terhadap berkas hasil_kali_linux.pcapng dan hasil_ubuntu.pcapng.

a. Analisis Visual Grafis I/O Wireshark

Melalui analisis kronologis dan pemantauan metrik pada fitur *I/O Graphs* di Wireshark, ditemukan karakteristik anomali lalu lintas data yang berbeda secara signifikan sesuai dengan mekanisme masing-masing model serangan [1]:

Gambar 1. Grafik Lonjakan Trafik Data (I/O Graph) pada Serangan SYN dan ICMP Flood

Representasi visual mengenai fluktuasi volume trafik data selama pengujian skenario serangan volumetrik (SYN Flood dan ICMP Flood) ditunjukkan oleh grafik I/O Graph pada Gambar 1. Pada fase pra-serangan (detik ke-0 hingga detik ke-10), aktivitas lalu lintas jaringan terpantau pasif dan konstan di sekitar nilai 0 packets/tick. Anomali trafik mulai terekam secara instan tepat pada detik ke-10, ditandai dengan lonjakan radikal packet rate yang melesat tajam hingga menembus ambang batas **3.000 kpkts (kilo packets/tick).** Densitas trafik berskala masif ini bertahan secara konsisten sepanjang masa simulasi insiden, sebelum akhirnya mengalami penurunan drastis kembali ke titik baseline segera setelah aktivitas serangan dinonaktifkan

DOI: https://doi.org/10.31004/riggs.v5i2.9453

Gambar 2. Grafik Konsumsi Koneksi Stabil Rendah (I/O Graph) pada Serangan Slowloris

Merujuk pada visualisasi I/O Graph pada Gambar 2, karakteristik lalu lintas data menunjukkan tren yang bertolak belakang secara signifikan dengan skenario serangan volumetrik sebelumnya. Sepanjang interval perekaman dari detik ke-0 hingga detik ke-125, grafik aktivitas koneksi tidak mengindikasikan adanya kepadatan paket data berskala masif pada lapisan jaringan. Metrik packet rate terpantau berada pada klaster yang sangat rendah, di mana kuantitas paket secara konsisten bertahan di bawah ambang batas **500 packets/tick,** dengan kemunculan fluktuasi minor yang tidak signifikan pada fase akhir di atas detik ke-100.

b. Rekapitulasi Ekstraksi Paket Data

Untuk memberikan pemetaan komparatif yang terstruktur mengenai dampak dari ketiga jenis intrusi tersebut, seluruh data metrik hasil ekstraksi berkas barang bukti .pcapng dirangkum ke dalam Tabel 1.

Tabel 1. Rekapitulasi Parameter Artefak Bukti Digital Hasil Investigasi DoS

No	Jenis Serangan	IP Sumber (Attacker)	IP Tujuan (Victim)	Protokol Utama	Port Target	Rata-rata Nilai Packet/Sec	Status Layanan Server
1	SYN Flood	192.168.100.10	192.168.100.20	TCP (SYN)	80 (HTTP)	> 15.000 pps	Kelumpuhan Total (*Down*)
2	ICMP Flood	192.168.100.10	192.168.100.20	ICMP	-	> 12.000 pps	Degradasi *Bandwidth*

DOI: https://doi.org/10.31004/riggs.v5i2.9453

3	Slowloris	192.168.100.10	192.168.100.20	TCP / HTTP	80 (HTTP)	< 50 pps	Kehabisan *Socket Thread*

c. Analisis Hasil Log Sistem (Suricata Alert)

Pembuktian forensik diperkuat melalui pemeriksaan berkas log transaksional fast.log dan eve.json milik Suricata IDS pada server korban [5] [13]. Sistem deteksi berhasil merekam dan mengklasifikasikan aktivitas mencurigakan tersebut secara akurat berdasarkan kecocokan aturan tanda tangan (*signature rules*). Berikut merupakan potongan (*snippet*) baris log otentik yang berhasil diekstrak sebagai bukti siber:

```
Plaintext
# Log Deteksi Skenario 1 & 2 (Flood Intrusion)
05/20/2026-13:05:22.410923 [**] [1:2010923:3] SURICATA DDoS Flood Attack Spotted [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 192.168.100.10:45163 -> 192.168.100.20:80
# Log Deteksi Skenario 3 (Slowloris Application Layer Attack)
05/20/2026-13:22:14.105432 [**] [1:2024311:2] SURICATA HTTP Denial of Service (Slowloris) Attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.100.10:51224 -> 192.168.100.20:80
```

Berdasarkan rekaman log sistem di atas, instrumen IDS berhasil memberikan validasi kronologis yang valid mengenai aktivitas intrusi yang terjadi. Berkas log mengonfirmasi bahwa rangkaian serangan siber berlangsung dalam rentang waktu antara pukul 13:05:22 hingga 13:22:14 WIB. Selama interval tersebut, mesin IDS secara konsisten mengidentifikasi dan mencatat upaya pemaksaan kelumpuhan layanan (Denial of Service) yang murni bersumber dari entitas tunggal dengan alamat IP asal 192.168.100.10.

Melalui serangkaian pengujian yang telah dieksekusi, hasil investigasi forensik jaringan mengonfirmasi adanya perbedaan karakteristik artefak digital yang sangat kontras antara model gangguan volumetrik (*volumetric attack*) dan serangan berbasis manipulasi tingkat aplikasi (*low-and-slow attack*). Pada skenario inspeksi trafik *SYN Flood* dan *ICMP Flood*, representasi grafis *I/O Graph* Wireshark berhasil merekonstruksi anomali berupa lonjakan densitas paket data (*packet rate*) berskala masif dalam waktu singkat. Pembanjiran paket TCP [SYN] serta *Echo Request* dari entitas penyerang (192.168.100.10) menuju server korban (192.168.100.20) secara konstan melampaui rata-rata 12.000 paket per detik (pps). Aktivitas ini secara sengaja memotong siklus jabat tangan tiga arah (*three-way handshake*) untuk menciptakan kondisi koneksi setengah terbuka (*half-open connection*). Implikasinya, memori pelayan web mengalami kepenuhan antrean (*SYN Backlog*) yang memicu kelumpuhan total terhadap ketersediaan layanan sistem. Temuan kuantitatif tersebut selaras dengan landasan teoretis dari [4] yang mengemukakan bahwa anomali volumetrik selalu meninggalkan jejak saturasi ekstrem pada lapisan jaringan (*network layer*) untuk menguras kapasitas lebar pita (*bandwidth*). Bukti ini diperkuat oleh validasi kualitatif log alert Suricata IDS berdasarkan kecocokan aturan tanda tangan (*signature rules*), yang mendukung studi terdahulu dari [2][14]terkait efektivitas mesin deteksi dalam mengenali paket gangguan secara *real-time* melalui sistem prioritas ancaman yang presisi.

Sebaliknya, pengujian terhadap vektor *Slowloris* menampilkan visualisasi *I/O Graph* yang cenderung konstan, landai, dan bertahan pada klaster volume rendah di bawah 50 pps. Walaupun kuantitas lalu lintas data ini menyerupai pola trafik normal sehingga mampu mengelabui mekanisme penyaringan berbasis batas volume (*threshold filtering*), dampak degradasi yang ditimbulkan tetap setara dengan ancaman volumetrik. Fenomena ini menjadi bukti nyata atas mekanisme kerja *Slowloris* yang mengeksploitasi keterbatasan alokasi koneksi *thread worker* internal pada *web server* Apache2. Melalui pengiriman komponen *header request* HTTP yang sengaja digantung secara perlahan dan berulang, penyerang berhasil mengikat soket kerja pelayan tanpa memicu alarm proteksi eksternal. Karakteristik eksploitasi senyap (*stealth*) tersebut memperkuat hasil investigasi dari [3] bahwa varian serangan layer aplikasi modern memang dirancang secara taktis untuk menguras sumber daya komputasi internal, bukan menyumbat jalur komunikasi data utama.

Meskipun model intrusi *low-and-slow* menyamar di bawah parameter deteksi konvensional, integrasi instrumen Suricata IDS terbukti memberikan hasil yang optimal. Melalui kapabilitas inspeksi paket secara mendalam (*deep packet inspection*), Suricata mampu menembus batasan filter tradisional untuk mengidentifikasi anomali struktural pada komponen *header request* HTTP secara *real-time*. Keberhasilan pengenalan tanda tangan serangan ini memvalidasi teori dari [10] bahwa pemeriksaan struktural terhadap isi *field* HTTP *header* yang digantung merupakan metode pertahanan paling valid dalam menyingkap rekam jejak aktivitas siber pada layer aplikasi.

DOI: https://doi.org/10.31004/riggs.v5i2.9453

Secara menyeluruh, korelasi dual-instrumen antara data log kualitatif Suricata dan metrik kuantitatif pcap Wireshark berhasil merekonstruksi parameter insiden secara utuh dan akurat. Keberhasilan pemetaan barang bukti digital ini membuktikan bahwa pengadopsian empat tahapan kerangka kerja forensik NIST SP 800-86 mampu menjamin aspek integritas serta otentisitas artefak jaringan. Penyelidikan komparatif ini sejalan dengan prinsip investigasi digital dari [6][15]yang menegaskan bahwa standarisasi prosedur penanganan bukti elektronik mutlak diimplementasikan demi menjaga akuntabilitas dan validitas bukti siber di hadapan hukum.

4. Kesimpulan

Melalui serangkaian pengujian forensik jaringan yang berbasis pada metodologi standar NIST SP 800-86 dan sistem Suricata IDS, penelitian ini berhasil merekonstruksi seluruh parameter insiden Denial of Service (DoS) secara valid serta akurat. Implementasi kerangka kerja yang sistematis mulai dari fase pengumpulan data hingga pelaporan terbukti mampu menjaga integritas dan otentisitas barang bukti digital, baik berupa log sistem maupun berkas tangkap paket (.pcapng), sehingga seluruh artefak yang diekstrak memiliki validitas yang kuat di mata hukum. Hasil analisis komparatif menunjukkan adanya perbedaan karakteristik yang tajam antara ancaman berbasis volume (flooding) dengan serangan pada lapisan aplikasi (low-and-slow). Skenario serangan TCP SYN Flood dan ICMP Flood melumpuhkan ketersediaan server melalui saturasi lebar pita jaringan dengan lonjakan trafik ekstrem yang mencapai 12.000 hingga 15.000 paket per detik. Sebaliknya, serangan Slowloris mendegradasi sistem secara senyap dengan mengeksploitasi arsitektur thread internal pada web server Apache2, meski hanya beroperasi pada packet rate yang sangat rendah di bawah 50 paket per detik. Pengujian ini juga membuktikan bahwa integrasi Suricata IDS sangat efektif karena memiliki fitur deep packet inspection yang mampu mengatasi kelemahan filter volume tradisional, sehingga manipulasi struktur header HTTP oleh Slowloris dapat diidentifikasi secara real-time. Akhirnya, studi ini tidak hanya memperkuat landasan pembuktian forensik digital, tetapi juga memberikan rekomendasi taktis bagi administrator jaringan untuk menerapkan pembatasan jumlah permintaan (rate limiting) dan memperketat batas waktu koneksi (timeout) per alamat IP guna memitigasi serangan serupa di masa depan.

Referensi

1. R. Pratama and H. Setiawan, "Comparative Analysis of Volumetric DDoS and Low-and-Slow Attacks on Web Server Infrastructure," International Journal of Cyber Security, pp. 88-95, 2024.
2. D. Ahmad and T. Wijaya, "Network Forensic Analysis of Slowloris Attack Using NIST SP 800-86 Framework," Jurnal Keamanan Jaringan Terakreditasi, pp. 45-52, 2025.
3. M. F. Rizky, I. Riadi and A. Fadlil, "Implementasi Suricata IDS dalam Mendeteksi Paket Anomali SYN Flood," Jurnal Sistem Komputer Modern, pp. 112-120, 2023.
4. S. Santoso and B. Rahardjo, "Eksploitasi Thread Worker Apache2 Melalui Metode Application Layer DoS," Jurnal Ilmu Komputer dan Informatika, pp. 201-209, 2024.
5. P. Putra, Y. Prayudi and A. Luthfi, "Live Forensics untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan pada Web Server," JIIP (Jurnal Ilmiah Ilmu Pendidikan), pp. 4387-4394, 2023.
6. W. Agustiono, D. W. Suci and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus," JATI (Jurnal Teknologi dan Informasi), pp. 115-124, 2024.
7. O. P. Nanlohy and A. Faizin, "Implementasi Honeypot untuk Mendeteksi Serangan Brute Force pada Layanan SSH," JATI (Jurnal Mahasiswa Teknik Informatika), pp. 13-26, 2025.
8. H. Kurniawan, "Deep Packet Inspection on HTTP Header Using Signature-Based Rules," Journal of Digital Forensics and Cyber Crime, pp. 310-318, 2024.
9. Nugroho and Y. Utama, "Mitigasi Serangan Volumetrik Menggunakan IPTables Rate Limiting Berbasis Host," Jurnal Rekayasa Teknologi Informasi, pp. 74-81, 2025.
10. F. Gunawan, "Evaluation of Promiscuous Mode Traffic Capturing in Virtualized Environment," Journal of Virtual Systems and Networks, pp. 55-63, 2023.
11. R. S. Putri and M. H. Sani, "Analisis Perbandingan Kinerja Web Server Event-Driven dan Thread-Based Terhadap Gangguan DoS," Jurnal Telematika dan Komputasi, pp. 14-22, 2025.
12. T. Budiman, "Digital Evidence Extraction and Accountability from PCAPNG and IDS Logs Architecture," Journal of Cybersecurity and Forensic Investigation, pp. 144-152, 2026.
13. R. Nisa, A. D. Wijayanto, A. P. J. Priana and A. Setiawan, "Analisis Log Server untuk mendeteksi Serang DDoS pada Keamanan Jaringan di Website," Journal of Internet and Software Engineering, pp. 1-17, 2024.
14. M. Syani, "Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (VPS)," Jurnal Inkofar, pp. 25-34, 2021.
15. F. Fachri, A. Fadlil and I. Riadi, "Analisis Keamanan Webserver Menggunakan Penetration Test," Jurnal Informatika, pp. 183-190, 2021.

DOI: https://doi.org/10.31004/riggs.v5i2.9453