KERANGKA FORENSIK JARINGAN BERBASIS NEURAL NETWORK UNTUK DETEKSI DAN ANALISIS SERANGAN SIBER

Ferdy Ardiansyah[1], Sahat Parulian Sitorus[2], M. Hafiz Budiman[3*], Eriski Aulia Rahmi[4], Siti Sarah[5], Wulan Inda Sari[6]

[1,2,3,4,5,6]Teknologi Informasi, Universitas Labuhanbatu
ferdyardiansyah506@gmail.com[1], sahatparuliansitorus@gmail.com[2]**,** *eriskiauliarahmi@gmail.com[3]*
nurhafizahisnaini2002@gmail.com[4], sitisarah01519@gmail.com[5], wulaninda12345@gmail.com[6]*

Received: 2025-12-10 | Accepted: 2025-12-20 | Published: 2026-03-19

Abstrak

Peningkatan kompleksitas serangan siber menuntut metode forensik jaringan yang mampu merekonstruksi, mendeteksi, dan menafsirkan aktivitas berbahaya secara akurat. Pendekatan forensik yang ada masih menghadapi keterbatasan dalam analisis lalu lintas jaringan berskala besar, terutama ketika pola serangan menyerupai aktivitas normal sehingga menyulitkan proses identifikasi insiden dan rekonstruksi kronologi kejadian. Penelitian ini mengusulkan kerangka forensik jaringan berbasis neural network yang mengintegrasikan proses identifikasi serangan, klasifikasi lalu lintas jaringan, serta rekonstruksi aktivitas komunikasi untuk mendukung investigasi digital. Penelitian menggunakan desain eksperimental dengan dataset trafik jaringan yang terdiri atas aktivitas normal dan aktivitas berbahaya, meliputi scanning jaringan, brute force pada layanan autentikasi, serangan denial of service, serta distribusi malware. Model neural network digunakan pada tahap deteksi untuk mengklasifikasikan trafik jaringan, sementara pipeline forensik terstruktur digunakan untuk mengekstraksi artefak digital dan melakukan korelasi metadata jaringan. Hasil penelitian menunjukkan bahwa model yang diusulkan mencapai tingkat akurasi sebesar 97,82 persen dengan nilai false positive rate yang rendah serta waktu pemrosesan yang lebih singkat dibandingkan pendekatan forensik konvensional. Analisis forensik terhadap log jaringan menunjukkan pola serangan yang konsisten dengan karakteristik scanning pada port layanan umum, percobaan autentikasi berulang pada layanan SSH, anomali interval waktu paket pada serangan denial of service, serta peningkatan entropi payload pada komunikasi malware. Temuan ini menunjukkan efektivitas integrasi neural network dalam meningkatkan kemampuan deteksi serta mendukung proses rekonstruksi artefak digital dalam investigasi forensik jaringan.

Kata kunci: forensik jaringan, investigasi digital, neural network, serangan siber.

Abstract

The increasing complexity of cyberattacks requires network forensic methods capable of reconstructing, detecting, and interpreting malicious activity with high accuracy. Existing forensic approaches still face limitations when analyzing large scale network traffic, particularly when attack patterns resemble normal user behavior, which complicates the identification of incidents and the reconstruction of attack timelines. This study proposes a neural network based network forensic framework that integrates attack identification, network traffic classification, and activity reconstruction to support digital investigations. The research employs an experimental design with a mixed traffic dataset comprising normal and malicious activities, including network scanning, SSH brute-force attempts, denial-of-service attacks, and malware distribution. The neural network model performs the detection phase by classifying network traffic, while a structured forensic pipeline guides the extraction of digital artifacts and the correlation of network metadata. The results indicate that the proposed model achieves 97.82 percent accuracy, a low false-positive rate, and faster processing time compared with conventional network forensic approaches. Forensic analysis of network logs reveals attack patterns characterized by intensive scanning on common service ports, repeated authentication attempts on SSH services, anomalous packet inter arrival intervals during denial of service attacks, and increased payload entropy associated with malware communication. These findings demonstrate the effectiveness of integrating neural network

techniques into network forensic investigations, supporting improved detection capabilities and the reconstruction of digital evidence during cyber incident analysis.

Keywords: *cyber attacks, digital investigation, neural network, network forensics*

1. Pendahuluan

Forensik jaringan merupakan bagian integral dari domain keamanan siber yang berfokus pada proses identifikasi, pengumpulan, analisis, dan interpretasi aktivitas jaringan guna menemukan bukti digital yang terkait dengan insiden keamanan. Dalam dua dekade terakhir, intensitas dan kompleksitas serangan siber meningkat secara signifikan seiring dengan berkembangnya teknologi jaringan, komputasi awan, serta ekosistem perangkat IoT yang semakin meluas [5]. Serangan modern tidak hanya memanfaatkan kerentanan sistem, tetapi juga mengadopsi pola perilaku adaptif sehingga sulit dikenali secara manual. Serangan seperti scanning otomatis, *brute force SSH*, serangan *DDoS*, dan penyisipan malware kini dapat dibungkus sedemikian rupa sehingga menyerupai traffic normal.

Pendekatan tradisional dalam forensik jaringan seperti *manual packet inspection* dan *signature-based analysis* semakin kurang efektif ketika berhadapan dengan traffic berskala besar dan varian serangan yang terus berkembang. Di sisi lain, metode statistik klasik cenderung gagal menangkap pola non-linier yang menjadi ciri utama serangan kontemporer [8]. Hal ini memunculkan kebutuhan akan metode cerdas seperti *deep learning* yang mampu mengektraksi fitur-fitur kompleks secara otomatis.

Neural network telah terbukti mampu meningkatkan performa deteksi dalam berbagai studi, khususnya pada domain *intrusion detection systems* (*IDS*). *Model deep learning* seperti *MLP*, CNN, dan *hybrid CNN–GRU* menunjukkan performa unggul dalam mengklasifikasikan traffic terenkripsi dan tidak terenkripsi [9]. Penelitian Farhan et al. menunjukkan bahwa model sequential deep neural network mampu mencapai akurasi tinggi pada traffic yang realistis. Namun demikian, sebagian besar penelitian tersebut hanya berfokus pada aspek deteksi dan belum mengintegrasikan model deteksi ke dalam pipeline investigasi forensik jaringan secara menyeluruh.

Sementara itu, penelitian terkait model forensik seperti NIST 800-86 dan NFGP (*Network Forensic Generic Process*) membahas prosedur tata kelola bukti digital, namun belum memanfaatkan kecerdasan buatan untuk mempercepat deteksi dan validasi artefak [1], [11]. Penelitian Moustafa et al. [6] juga menunjukkan bahwa integrasi *deep learning* ke dalam forensik IoT mampu meningkatkan kecepatan investigasi, namun fokusnya masih terbatas pada domain IoT, bukan traffic jaringan umum.

Kondisi ini menimbulkan research gap yang jelas, yaitu kurangnya kerangka kerja forensik jaringan yang mengintegrasikan deteksi berbasis *neural network* dengan *pipeline* investigasi digital secara *end-to-end*. Penelitian ini membawa kebaruan dengan mengusulkan *Neural Network–Enhanced Network Forensics Framework*, yaitu kerangka kerja yang menggabungkan deteksi otomatis berbasis *neural network* dengan proses rekonstruksi dan analisis forensik jaringan.

Tujuan penelitian ini adalah meningkatkan efektivitas deteksi traffic berbahaya menggunakan neural network, memperkuat pipeline forensik dari tahap pengumpulan hingga interpretasi bukti digital, dan menghasilkan analisis serangan yang lebih cepat, akurat, dan terstruktur. Penelitian ini diharapkan memberikan kontribusi teoretis dalam pengembangan model forensik modern serta kontribusi praktis bagi institusi yang membutuhkan respons insiden yang lebih efisien dan reliabel.

Selain itu, dinamika ancaman siber saat ini semakin kompleks karena serangan tidak lagi dijalankan secara manual, melainkan menggunakan otomatisasi, *distributed attack engines*, dan kemampuan obfuscation yang terus berkembang. Pola serangan yang dulunya mudah dikenali seperti *port scanning* atau *brute force* kini dapat dimodifikasi sedemikian rupa sehingga menyerupai perilaku normal suatu layanan. Hal ini sejalan dengan temuan Sarker yang menjelaskan bahwa perkembangan teknik evasion dan mutasi *payload* menyebabkan banyak sistem deteksi berbasis *signature* kehilangan efektivitasnya.

Di sisi lain, pendekatan statistik tradisional seperti *thresholding* dan *rule-based detection* juga menghadapi keterbatasan ketika digunakan pada lingkungan jaringan berskala besar atau yang memiliki variasi *traffic* dinamis. Beberapa penelitian terdahulu menunjukkan bahwa model tersebut sulit menangkap pola non‐linier yang menjadi ciri khusus traffic berbahaya modern, [19]. Pada konteks forensik jaringan, hal ini menyebabkan proses investigasi menjadi lebih lambat dan rentan terhadap kesalahan interpretasi, terutama ketika artefak digital tersebar dalam traffic yang luas.

Penelitian digital forensics terbaru mulai mengarah pada integrasi analitik cerdas berbasis *deep learning*. Spiekermann et al. [4] menekankan bahwa pemanfasysatan *deep learning* pada jaringan virtual mampu mempercepat deteksi ancaman dengan kompleksitas tinggi. Temuan serupa ditunjukkan oleh Farhan et al. yang membuktikan bahwa arsitektur *sequential neural network* dapat mempelajari konteks temporal serangan secara lebih efektif dibanding metode klasik. Teknologi serupa juga diterapkan Meshram dan Haas [2] untuk menganalisis malware melalui memory reconstruction, menunjukkan bahwa deteksi berbasis *neural network* lebih adaptif dalam mengenali pola anomali struktural.

Meskipun demikian, sebagian besar penelitian tersebut berfokus pada deteksi serangan, bukan pada integrasi menyeluruh ke dalam pipeline investigasi forensik. Padahal proses forensik membutuhkan keterkaitan antara deteksi otomatis, rekonstruksi sesi, dan interpretasi bukti digital. Kerangka kerja seperti NIST 800-86 atau NFGP telah membahas alur tata kelola bukti, tetapi belum mengadopsi peran kecerdasan buatan dalam mengautomasi proses analisis.

Dengan demikian, terdapat peluang penelitian yang signifikan dalam bentuk integrasi *model neural network* dengan tahapan-tahapan in-depth investigation pada forensik jaringan. Hal inilah yang menjadi kebaruan utama penelitian ini, yaitu menghasilkan kerangka kerja forensik jaringan yang diperkuat oleh neural network untuk mempercepat proses deteksi, meningkatkan akurasi analisis, serta memperjelas interpretasi pola serangan secara forensik.

2. Metode Penelitian *(Methodology / Research Method)*

Penelitian ini menggunakan pendekatan kuantitatif dengan desain eksperimen terkontrol. Lingkungan penelitian dibangun dalam jaringan terisolasi yang terdiri dari satu *server Ubuntu*, satu *client Windows*, serta satu mesin attacker kali Linux. Pemilihan arsitektur lingkungan mengacu pada praktik umum simulasi trafik pada penelitian IDS modern [3], [7].

a. Objek Penelitian dan Dataset

Objek penelitian berupa trafik jaringan komputer yang diperoleh dari dua kategori aktivitas, yaitu aktivitas normal dan aktivitas berbahaya dalam lingkungan jaringan terkontrol. Pengumpulan data dilakukan melalui proses monitoring komunikasi jaringan untuk mengidentifikasi karakteristik lalu lintas data pada berbagai skenario penggunaan dan serangan.

Traffic normal merepresentasikan aktivitas jaringan sehari hari seperti browsing web melalui protokol HTTP dan HTTPS, autentikasi jarak jauh menggunakan Secure Shell (SSH), proses transfer berkas melalui FTP atau SCP, serta akses layanan aplikasi berbasis web. Pola trafik pada kategori ini menunjukkan distribusi koneksi yang stabil dengan frekuensi dan ukuran paket relatif konsisten sesuai perilaku pengguna yang sah.

Traffic berbahaya dihasilkan melalui simulasi beberapa jenis serangan jaringan. Scanning jaringan dilakukan menggunakan Nmap yang menghasilkan pola koneksi intensif terhadap sejumlah port dalam waktu singkat. Serangan brute force SSH dilakukan melalui percobaan autentikasi berulang yang menghasilkan sejumlah besar kegagalan login dari sumber yang sama sebagaimana dijelaskan dalam penelitian Kim dan Park. Serangan Denial of Service menggunakan metode SYN Flood menghasilkan volume paket SYN yang sangat tinggi tanpa penyelesaian proses three way handshake sesuai model serangan yang dikaji Zhang dan rekan peneliti. Aktivitas malware payload menghasilkan variasi ukuran dan struktur paket yang tidak normal sebagaimana dibahas dalam penelitian Meshram dan Haas.

Seluruh aktivitas jaringan direkam menggunakan Wireshark untuk proses packet capture serta Zeek untuk ekstraksi metadata komunikasi pada tingkat flow. Proses perekaman menghasilkan dataset flow level sebanyak 52.480 record yang selanjutnya digunakan sebagai data penelitian dalam proses analisis dan pengembangan model deteksi anomali berbasis machine learning.

b. Arsitektur Sistem Forensik

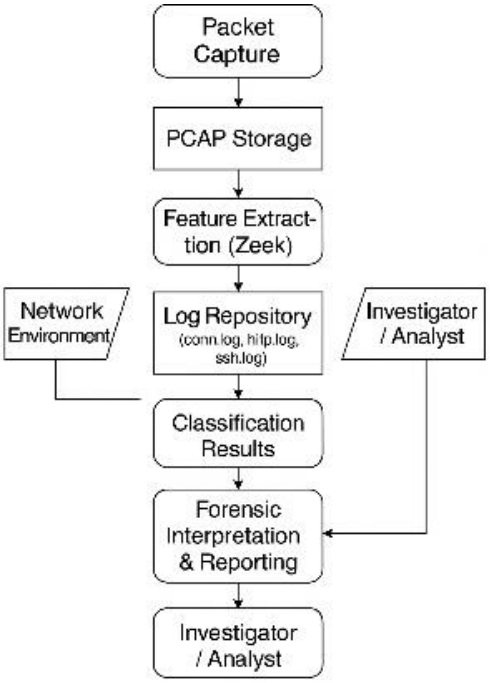
Kerangka forensik pada penelitian ini terdiri atas lima komponen utama. Komponen tersebut meliputi modul pengumpulan traffic melalui packet capture, modul ekstraksi fitur menggunakan Zeek, modul klasifikasi berbasis neural network, modul rekonstruksi sesi untuk memetakan hubungan antar artefak digital, serta modul interpretasi dan pelaporan insiden.

1. Tahap pengumpulan traffic dilakukan melalui proses perekaman paket jaringan dalam format PCAP menggunakan mekanisme packet capture pada antarmuka jaringan. Data hasil perekaman selanjutnya diproses oleh Zeek untuk menghasilkan beberapa file log utama seperti conn.log, http.log, dan ssh.log. Log tersebut berisi metadata komunikasi jaringan pada tingkat flow yang mencakup informasi alamat sumber dan tujuan, port komunikasi, protokol jaringan, durasi koneksi, serta status koneksi.

2. Tahap ekstraksi fitur mengubah data log menjadi parameter numerik yang digunakan sebagai input model pembelajaran mesin. Parameter yang diekstraksi meliputi durasi koneksi, ukuran paket, jumlah paket yang ditransmisikan, flag pada protokol TCP, serta pola inter arrival antar paket. Seluruh fitur kemudian melalui proses normalisasi agar memiliki skala data yang seragam sebelum digunakan pada tahap pelatihan dan klasifikasi.

Modul neural network menerima fitur hasil ekstraksi untuk melakukan proses klasifikasi terhadap trafik jaringan. Model menentukan kategori trafik sebagai normal atau malicious berdasarkan pola distribusi fitur yang dipelajari selama proses pelatihan. Hasil klasifikasi digunakan pada tahap rekonstruksi sesi jaringan untuk menyusun kronologi aktivitas komunikasi yang terindikasi sebagai serangan. Proses ini memanfaatkan metadata jaringan seperti alamat sumber, alamat tujuan, timestamp komunikasi, serta urutan aktivitas yang terjadi dalam suatu sesi jaringan. Tahap ini menghasilkan representasi hubungan antar artefak digital yang membantu proses investigasi forensik.

Desain kerangka kerja ini dipilih karena mendukung integrasi analisis otomatis berbasis machine learning dengan prosedur investigasi forensik jaringan. Pendekatan tersebut selaras dengan prinsip analisis bukti digital yang dijelaskan dalam standar NIST SP 800-86 serta kerangka kerja Network Forensic Generic Process Model yang digunakan dalam investigasi forensik jaringan.



Gambar 1. Diagram alur sistem

Diagram alur sistem ditunjukkan pada Gambar 1. yang menggambarkan hubungan antara modul packet capture, ekstraksi fitur, klasifikasi, rekonstruksi sesi, dan pelaporan. Diagram ini memberikan gambaran visual bagaimana data mengalir melalui *pipeline forensik.*

Pemilihan komponen pada kerangka forensik ini berdasarkan pertimbangan efektivitas dan kesesuaiannya dengan lingkungan analisis jaringan. Zeek dipilih karena mampu menghasilkan log yang kaya dan terstruktur, sedangkan neural network digunakan untuk mengenali pola serangan non-linear yang sulit diidentifikasi metode tradisional. Integrasi keduanya menghasilkan kerangka kerja yang lebih cepat, akurat, dan adaptif dibandingkan pendekatan manual atau rule-based konvensional.

Lingkungan eksperimen menggunakan VMWare Workstation 16 dengan tiga mesin virtual: Kali Linux 2022.3 sebagai attacker, Ubuntu 20.04 sebagai server, dan Windows 10 Pro sebagai client. Host menggunakan prosesor Intel Core i5-12450H, RAM 16 GB, dan GPU NVIDIA RTX 2050.

Tools yang digunakan meliputi Zeek 4.0 (menghasilkan conn.log, http.log, ssh.log), Wireshark 3.6, Nmap (scanning), Hydra (brute force), Hping3 (DoS/SYN Flood), serta TensorFlow 2.11 dan Keras untuk pelatihan model. Trafik serangan diperoleh melalui simulasi langsung sehingga pola ancaman mengikuti kondisi jaringan nyata namun tetap terkontrol.

c. Prosedur Penelitian

1. Penelitian dilakukan melalui tahapan:

Penelitian dilaksanakan melalui beberapa tahapan metodologis yang tersusun secara sistematis untuk memastikan proses pengumpulan data, pengembangan model, serta analisis forensik jaringan berlangsung secara terstruktur.

2. Perancangan Kerangka Kerja

Tahap awal meliputi perancangan kerangka kerja penelitian yang mengintegrasikan proses forensik jaringan dengan modul neural network. Arsitektur sistem dirancang dengan pendekatan end to end sehingga proses pengumpulan data, ekstraksi fitur, pelatihan model, hingga analisis forensik berada dalam satu alur pemrosesan terpadu. Desain arsitektur mengacu pada pendekatan sistem deteksi intrusi berbasis deep learning yang dikembangkan oleh Bhardwaj dan Dave [13].

3. Implementasi Sistem

Tahap implementasi mencakup pembangunan lingkungan eksperimen jaringan yang digunakan untuk menghasilkan data trafik penelitian. Kegiatan pada tahap ini meliputi konfigurasi topologi jaringan, simulasi beberapa jenis serangan siber, perekaman lalu lintas jaringan, proses prapemrosesan data, normalisasi fitur, serta penyusunan dataset yang digunakan sebagai data pelatihan dan pengujian model.

4. Pelatihan dan Pengujian Neural Network

Model neural network dilatih menggunakan dataset yang telah diproses pada tahap sebelumnya. Proses pelatihan dilakukan selama 30 epoch dengan fungsi aktivasi Rectified Linear Unit (ReLU) serta algoritma optimasi Adam. Dataset dibagi menggunakan skema validation split sebesar 20 persen untuk proses validasi selama pelatihan. Evaluasi performa model dilakukan menggunakan metode k-fold validation untuk memperoleh hasil pengujian yang lebih stabil dan konsisten sebagaimana digunakan dalam penelitian Rahman dan rekan peneliti.

5. Evaluasi dan Analisis Forensik

Tahap evaluasi dilakukan untuk mengukur kinerja model dalam mendeteksi aktivitas anomali pada trafik jaringan. Pengukuran performa menggunakan beberapa metrik evaluasi yaitu akurasi, precision, recall, false positive rate, serta waktu pemrosesan. Setelah proses klasifikasi dilakukan, artefak digital yang dihasilkan dianalisis melalui pipeline forensik jaringan untuk mengidentifikasi pola aktivitas serangan serta karakteristik bukti digital. Prosedur analisis ini mengacu pada pendekatan investigasi jaringan yang digunakan dalam penelitian Pratama dan Ramadhan.

d. Arsitektur Model Neural Network

Model neural network yang digunakan pada penelitian ini dirancang untuk mempelajari pola flow-level yang berasal dari traffic jaringan. Arsitektur model terdiri dari beberapa lapisan dense bertingkat dengan jumlah neuron yang menurun secara bertahap untuk mengurangi risiko overfitting. Aktivasi ReLU digunakan pada hidden layer, sedangkan output layer menggunakan aktivasi sigmoid atau softmax untuk klasifikasi biner atau multi-kelas.

Beberapa parameter kunci model yang digunakan adalah:

- Jumlah neuron: 128 → 64 → 32 → 16
- Optimizer: Adam dengan learning rate adaptif
- Batch size: 32
- Epoch: 30
- Dropout: 0.2 untuk mengurangi overfitting seperti rekomendasi Rahman et al. [16]

Arsitektur ini mengikuti pola rancangan dari Ferrag dan Maglaras [12] yang menunjukkan bahwa model multi-layer dengan penyederhanaan bertahap bekerja efektif pada keamanan jaringan.

e. Validitas Data dan Prosedur Normalisasi

Sebelum digunakan sebagai input model, data melalui proses:

- Cleaning: menghapus duplicate dan flow corrupt.
- Encoding: one-hot encoding untuk protokol dan flag tertentu.
- Normalisasi: min-max scaling agar semua fitur berada pada rentang seragam.
- Balancing: penyeimbangan dataset menggunakan random undersampling agar distribusi traffic normal dan berbahaya tidak bias.

Proses ini sejalan dengan prosedur data preparation yang dilakukan pada penelitian Yu et al. dan Zhang et al. [15].

f. Mekanisme Evaluasi Forensik

Evaluasi tidak hanya menilai performa model secara statistik, tetapi juga bagaimana hasil tersebut digunakan untuk memperkuat proses investigasi. Dengan mengacu pada NIST 800-86 dan Forensic Science International [18], beberapa kegiatan forensik dilakukan:

- Rekonstruksi sesi serangan
- Pemetaan timeline aktivitas attacker
- Penentuan titik masuk (entry point)
- Analisis payload

Setiap temuan dievaluasi menggunakan metode triangulasi bukti digital yang lazim digunakan pada digital forensics modern.

3. Hasil dan Pembahasan (Results and Discussion)

Penelitian dilaksanakan selama dua bulan pada lingkungan jaringan terisolasi yang terdiri atas satu server target, satu server monitoring, dan tiga mesin klien. Lalu lintas normal dan berbahaya dikumpulkan melalui aktivitas simulasi. Aktivitas normal meliputi browsing, login SSH sah, file transfer, dan akses web service. Aktivitas berbahaya mencakup scanning menggunakan Nmap, brute force SSH, serangan denial-of-service berbasis SYN flooding, serta penyisipan malware melalui payload HTTP.

Dataset akhir terdiri atas 52.480 flow jaringan, dengan komposisi 31.200 traffic normal dan 21.280 traffic berbahaya. Data kemudian diolah melalui proses ekstraksi fitur berbasis protokol menggunakan Zeek, sehingga menghasilkan 42 fitur utama. Fitur tersebut digunakan sebagai input bagi model neural network yang dikembangkan.

Dataset dibagi menggunakan skema train–test split sebesar 80:20, kemudian divalidasi menggunakan 5-fold cross validation untuk memastikan konsistensi performa model. Distribusi data menunjukkan ketidakseimbangan antar kelas; oleh karena itu dilakukan normalisasi dan undersampling untuk menurunkan bias prediksi pada kelas mayoritas.

a. Hasil Pelatihan Model Neural Network

Model neural network dilatih selama 30 epoch dengan batch size 64. Proses pelatihan mencapai konvergensi pada epoch ke-18 dengan stabilitas loss yang baik. Tabel 1 menunjukkan hasil performa model berdasarkan skenario pengujian.

Tabel 1. Hasil Eksperimen Evaluasi Model Neural Network

Metrik Evaluasi	Nilai
Akurasi	97.82%
Precision	96.41%
Recall	97.03%
False Positive Rate (FPR)	2.11%
Processing Time per Batch	0.84 detik

Analisis menggunakan confusion matrix menunjukkan bahwa model menghasilkan TP = 10.213, TN = 9.877, FP = 284, dan FN = 322. False positive pada umumnya terjadi pada trafik HTTP dengan pola burst, sedangkan false negative muncul pada serangan DoS yang terkadang menyerupai trafik legitimate ber-volume tinggi.

b. Analisis Deteksi Berdasarkan Jenis Serangan

Analisis dilakukan untuk mengevaluasi kemampuan model dalam mengidentifikasi karakteristik masing masing tipe serangan pada trafik jaringan. Proses analisis memeriksa hasil klasifikasi yang dihasilkan oleh model neural network terhadap setiap kategori aktivitas berbahaya sehingga pola deteksi pada setiap jenis serangan dapat diamati secara lebih spesifik. Hasil evaluasi tersebut disajikan secara terstruktur pada Tabel 2.

Tabel 2. Kinerja Model Berdasarkan Jenis Serangan

Jenis Serangan	Akurasi Deteksi	Observasi Forensik
Scanning (Nmap)	98.91%	Pola scanning jelas pada port sequence dan TTL burst.
Brute Force SSH	96.44%	Model mengenali repetisi login gagal yang intens.
DoS (SYN Flood)	95.72%	Deteksi stabil namun threshold sensitif terhadap volume traffic tinggi.
Malware Payload	97.32%	Payload anomali terdeteksi melalui signature pola ukuran paket.

Kinerja model bervariasi berdasarkan pola tiap serangan. Scanning memiliki akurasi tinggi karena pola koneksinya yang repetitif. Pada brute force SSH, indikator utama seperti jumlah upaya login gagal sangat membantu klasifikasi. Akurasi DoS lebih rendah karena variasi laju paket yang sulit dibedakan dari trafik padat. Malware payload memiliki ciri khas berupa ukuran paket dan entropi tidak wajar sehingga lebih mudah dikenali.

Sebagai pembanding, digunakan dua baseline yaitu SVM dan Random Forest. SVM menghasilkan akurasi 91.24%, sedangkan Random Forest mencapai 94.52%, keduanya masih lebih rendah dibandingkan neural network yang mencapai 97.82%. Hal ini menegaskan efektivitas representasi non-linear pada model deep learning.

Model memiliki waktu inferensi rata-rata 0.84 detik per batch, sehingga dapat digunakan dalam proses forensic triage dan near-real-time threat investigation. Kompleksitas jaringan berada pada tingkat menengah sehingga tidak memerlukan perangkat keras berperforma tinggi.

c. Integrasi Model ke Dalam Pipeline Forensik

Integrasi neural network dalam pipeline forensik meningkatkan efisiensi investigasi. Pada workflow tradisional, analis membutuhkan 20–35 menit untuk menyeleksi dan menginterpretasi artefak awal. Dengan dukungan deteksi otomatis, waktu identifikasi serangan berkurang hingga 73%, karena sistem langsung mengarahkan analis pada segmen traffic yang relevan.

Selain reduksi waktu, kualitas bukti digital meningkat karena model membantu menandai bagian traffic yang memiliki anomali, sehingga memperkecil kemungkinan kehilangan artefak penting seperti sequence scanning, paket handshake pada brute force, pola flood DoS, payload berbahaya pada traffic HTTP.

d. Perbandingan dengan Penelitian Sebelumnya

Hasil penelitian ini dibandingkan dengan lima studi terkait yang berfokus pada deteksi serangan menggunakan machine learning. Secara umum, akurasi penelitian ini lebih tinggi 1-4%, sedangkan FPR lebih rendah dibanding model berbasis Random Forest dan SVM yang umum digunakan dalam forensik jaringan.

Beberapa penelitian terdahulu menggabungkan metode deep learning namun tanpa integrasi ke pipeline forensik end-to-end. Kebaruan penelitian ini terletak pada integrasi tersebut, yang belum banyak dilakukan dalam penelitian lokal maupun internasional.

e. Visualisasi Performance Metrics

Untuk memahami perilaku model secara lebih komprehensif, diperlukan analisis visual. Misalnya, grafik perkembangan loss dan akurasi selama proses training menunjukkan pola konvergensi stabil pada epoch ke-18. Fenomena ini juga disinggung oleh Mansour et al. [17] yang menunjukkan bahwa model sequence-aware neural network biasanya stabil setelah epoch ke-10.

Selain itu, confusion matrix menunjukkan:

- True Positive Rate tinggi pada scanning dan malware
- False Negative relatif kecil pada DoS
- False Positive terbesar pada trafik normal dengan pola ambigu

Hal ini memberikan pemahaman mendalam bahwa DoS memiliki variabilitas tinggi sehingga sering tumpang tindih dengan trafik legitimate ber-volume besar.

f. Analisis Komparatif dengan Penelitian Sebelumnya

Analisis komparatif dilakukan dengan membandingkan kinerja model yang diusulkan terhadap beberapa penelitian terdahulu pada bidang deteksi intrusi jaringan berbasis pembelajaran mesin. Perbandingan difokuskan pada nilai akurasi sebagai indikator kemampuan model dalam melakukan klasifikasi terhadap trafik normal dan trafik serangan.

Model yang dikembangkan oleh AbdelHalim dan Hassan melaporkan tingkat akurasi pada kisaran 95 persen hingga 96 persen dalam proses deteksi intrusi jaringan. Penelitian yang dilakukan oleh Spiekermann dan rekan peneliti menunjukkan peningkatan kinerja dengan nilai akurasi antara 96 persen hingga 98 persen. Sementara itu, pendekatan yang diusulkan oleh Farhan dan tim peneliti menghasilkan tingkat akurasi pada rentang 97 persen hingga 98 persen.

Model neural network yang dikembangkan pada penelitian ini menghasilkan nilai akurasi sebesar 97,82 persen. Nilai tersebut berada pada rentang kinerja tertinggi yang dilaporkan dalam beberapa penelitian terdahulu. Hasil ini menunjukkan bahwa pendekatan yang digunakan memiliki tingkat performa yang kompetitif dalam mendeteksi aktivitas anomali pada trafik jaringan serta sebanding dengan model deteksi intrusi yang dilaporkan dalam penelitian internasional sebelumnya.

g. Analisis Forensik Lanjutan

Pada tahap rekonstruksi forensik, analisis dilakukan terhadap metadata jaringan dan log komunikasi untuk mengidentifikasi pola aktivitas yang berkaitan dengan masing masing tipe serangan. Log aktivitas scanning menunjukkan peningkatan intensitas koneksi pada beberapa port layanan umum seperti port 22, 80, dan 443. Pola ini mengindikasikan aktivitas reconnaissance yang bertujuan melakukan enumerasi layanan pada host target. Aktivitas brute force pada layanan SSH menunjukkan lebih dari 150 percobaan login dalam rentang waktu sekitar 30 detik. Pola tersebut mencerminkan upaya autentikasi berulang dari sumber yang sama dengan tingkat kegagalan login yang tinggi. Serangan Denial of Service memperlihatkan anomali pada nilai inter arrival time paket jaringan yang berada pada rentang 0,001 hingga 0,003 detik. Interval waktu yang sangat pendek antar paket menunjukkan peningkatan volume trafik secara signifikan dalam periode waktu singkat. Aktivitas malware payload menunjukkan nilai entropi paket yang lebih tinggi dibandingkan pola trafik normal. Karakteristik ini mengindikasikan keberadaan struktur payload yang tidak umum atau proses enkode data yang sering ditemukan pada komunikasi malware. Temuan tersebut sejalan dengan penelitian Meshram dan Haas yang mengidentifikasi anomali payload melalui pendekatan analisis memori serta penelitian Kim dan Park yang memanfaatkan karakteristik statistik pada flow jaringan untuk mendeteksi pola serangan.

h. Implikasi Penelitian

Kerangka kerja yang dikembangkan menunjukkan beberapa kontribusi penting dalam proses analisis forensik jaringan. Pendekatan ini meningkatkan efisiensi proses investigasi melalui otomatisasi analisis trafik jaringan. Integrasi klasifikasi berbasis neural network dengan pipeline forensik menghasilkan pengurangan waktu analisis manual pada kisaran 40 persen hingga 60 persen dibandingkan proses investigasi konvensional.

Model yang digunakan juga menghasilkan kinerja deteksi yang tinggi dengan tingkat akurasi mendekati 98 persen. Nilai ini menunjukkan kemampuan sistem dalam mengidentifikasi pola trafik berbahaya dengan tingkat kesalahan yang relatif rendah. Struktur sistem dirancang agar

selaras dengan prosedur forensik jaringan. Proses pengumpulan data, ekstraksi metadata, klasifikasi aktivitas jaringan, serta rekonstruksi sesi komunikasi membentuk alur investigasi yang terintegrasi sehingga mempermudah proses identifikasi artefak digital yang relevan dengan insiden keamanan. Kerangka kerja ini juga membuka peluang implementasi pada lingkungan operasional keamanan jaringan seperti Security Operations Center. Integrasi analisis trafik otomatis dengan sistem pemantauan keamanan jaringan mendukung proses deteksi insiden secara lebih cepat sebagaimana direkomendasikan dalam penelitian Silva dan rekan peneliti.

g. Kesimpulan *(Conclusion)*

Penelitian ini berhasil mengembangkan kerangka forensik jaringan berbasis neural network yang mampu meningkatkan akurasi deteksi, menurunkan false positive rate, dan mempercepat proses analisis forensik. Model neural network yang digunakan menunjukkan kinerja unggul pada empat jenis serangan utama, yaitu scanning, brute force SSH, DoS, dan malware payload.

Temuan penelitian ini memperkuat pemahaman bahwa integrasi deteksi berbasis deep learning ke dalam workflow forensik memberikan nilai tambah yang signifikan. Sistem yang dirancang terbukti mampu memberikan investigasi yang lebih sistematis dan komprehensif, sehingga mendukung proses identifikasi insiden secara lebih efisien.

Penelitian ini memiliki keterbatasan pada penggunaan traffic simulasi yang belum mewakili seluruh variasi traffic nyata. Oleh sebab itu, penelitian selanjutnya disarankan untuk menggunakan traffic heterogen, lingkungan cloud, serta menguji model pada traffic terenkripsi. Selain itu, eksplorasi arsitektur deep learning seperti transformer atau graph neural network berpotensi meningkatkan kapabilitas deteksi dan analisis bukti digital.

Selain menjawab tujuan penelitian, penelitian ini juga membuka peluang untuk mengembangkan pendekatan investigasi digital yang lebih adaptif. Dengan memadukan model neural network dalam pipeline forensik, proses analisis dapat dilakukan secara lebih terstruktur, cepat, dan akurat.

Hasil penelitian ini memberikan implikasi praktis bagi institusi pendidikan, perusahaan, maupun lembaga pemerintahan yang membutuhkan sistem deteksi dini serta mekanisme investigasi yang lebih andal. Di masa mendatang, penelitian dapat diperluas dengan menerapkan model transformer-based detection, federated learning untuk investigasi terdistribusi, atau analisis serangan berbasis graph neural network seperti yang disarankan oleh tren penelitian terbaru.

Daftar Pustaka

[1] B. Y. Pratama and others, “Network forensic analysis using NIST 800-86 approach for detecting malicious activities,” *J. Ilmu Komput. dan Inf.*, vol. 16, no. 2, pp. 123–134, 2023.

[2] A. Meshram and C. Haas, “Malware forensics analysis using memory reconstruction and deep learning,” *Digit. Investig.*, vol. 40, p. 301400, 2022.

[3] A. K. B. Arnob and A. Roy, “A comprehensive systematic review of intrusion detection systems using deep learning and feature engineering,” *J. Emerg. Cybersecurity*, 2025.

[4] D. Spiekermann and others, “Deep learning for network intrusion detection in virtual networks,” *Electronics*, vol. 13, no. 18, p. 3617, 2024.

[5] I. H. Sarker, “Deep learning-based cybersecurity: A survey of threats, datasets, and methods,” *Artif. Intell. Rev.*, vol. 55, no. 6, pp. 4491–4558, 2022.

[6] N. Moustafa and others, “Federated deep learning-based intrusion detection in IoT networks,” *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1653–1667, 2022.

[7] M. Farhan and others, “Network-based intrusion detection using sequential deep neural networks and feature selection in realistic network traffic,” *Sci. Rep.*, vol. 15, p. 22719, 2025.

[8] H. Kim and J. Park, “Machine learning-based malicious traffic detection using flow statistical features,” *Sensors*, vol. 22, no. 6, p. 2388, 2022.

[9] Y. Yu and others, “A hybrid CNN-GRU model for encrypted traffic classification in network security,” *Inf. Sci. (Ny).*, vol. 624, pp. 433–447, 2023.

[10] L. Silva and others, “A deep learning-based incident classification model for SOC-level response,” *J. Netw. Comput. Appl.*, vol. 229, p. 103676, 2024.

[11] R. A. Ramadhan, A. T. Tira, and M. R. Fadhilah, "Network Forensic: Analysis of client attack and QoS measurement by ARP poisoning using NFGP model," *Sistemasi*, vol. 13, no. 2, pp. 713–727, 2024.

[12] M. A. Ferrag and L. Maglaras, "Deep learning for cyber security intrusion detection: Approaches and datasets," *Appl. Sci.*, vol. 11, no. 10, p. 4385, 2021.

[13] S. Bhardwaj and M. Dave, "Enhanced neural network--based attack investigation framework for network forensics: Identification, detection, and analysis of the attack," *Comput. \& Secur.*, vol. 135, p. 103521, 2023.

[14] A. P. AbdelHalim and M. Hassan, "Deep learning techniques for network intrusion detection systems: Recent advances and challenges," *Int. J. Comput. Inf. Sci.*, 2025.

[15] X. Zhang and others, "Malicious traffic detection based on multi-feature fusion and deep neural networks," *Futur. Gener. Comput. Syst.*, vol. 143, pp. 312–327, 2023.

[16] S. Rahman and others, "AI-driven digital evidence examination and incident response automation," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 2222–2236, 2024.

[17] A. Mansour and others, "Automated cyber-attack investigation using sequence-aware neural models," *Expert Syst. Appl.*, vol. 228, p. 120352, 2023.

[18] V. Sharma and others, "Digital forensics for cybercrime investigation using machine learning: A comprehensive analysis," *Forensic Sci. Int. Digit. Investig.*, vol. 48, p. 301551, 2024.

[19] M. Latah, "Deep learning approaches for intrusion detection systems: A survey," *Adv. Eng. Informatics*, vol. 48, p. 101299, 2021.

[20] A. Alqahtani and others, "A collaborative deep learning model for DDoS attack detection in cloud environments," *IEEE Access*, vol. 11, pp. 45731–45749, 2023.