Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN PENGESAHAN ii
PERNYATAAN BEBAS PLAGIASI iii
HALAMAN PERSEMBAHAN iv
KATA PENGANTAR v
DAFTAR ISI vi
DAFTAR TABEL ix
DAFTAR GAMBAR xi
DAFTAR SINGKATAN xiii
INTISARI xiv
ABSTRACT xv
BAB I Pendahuluan 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Tugas Akhir 3
1.4 Batasan Tugas Akhir 4
1.5 Manfaat Tugas Akhir 6
1.6 Sistematika Penulisan 6
BAB II Tinjauan Pustaka dan Dasar Teori 8
2.1 Tinjauan Pustaka 8
2.2 Dasar Teori 15
2.2.1 Keamanan Jaringan Komputer 15
2.2.2 *Malware* dan Klasifikasinya 15
2.2.3 *Intrusion Detection System* dan *Network Intrusion Detection System* 16
2.2.4 *Network Forensics* 16
2.2.5 Format *Packet Capture* (PCAP) 17
2.2.6 *Chain of Custody* (Rantai Pengawasan Barang Bukti) 17
2.2.7 Fungsi *Hash* Kriptografis untuk Verifikasi Integritas Bukti 18
2.2.8 Deteksi Anomali pada Lalu Lintas Jaringan 19
2.2.9 *Autoencoder* untuk *One-Class Anomaly Detection* 19
2.2.10 Klasifikasi Multikelas dengan XGBoost 21
2.2.11 Permasalahan Kelas Tumpang Tindih (*Class Overlap*) pada Klasifikasi Multikelas 22
2.2.12 Sistem Berbasis Aturan (*Rule-Based Reasoning*) 22
2.2.13 *Human-in-the-Loop* dan Kolaborasi Manusia-AI dalam Pengambilan Keputusan 22

UNIVERSITAS GADJAH MADA
Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

2.2.14 *Application Programming Interface* (API) dan Arsitektur RESTful 23
2.2.15 Antarmuka Pengguna Berbasis Komponen dan *Single-Page Application* 23
2.2.16 *Large Language Model* untuk Pembuatan Laporan Terstruktur 24
2.2.17 Metrik Evaluasi Sistem Deteksi Intrusi 24
2.2.17.1 Metrik Klasifikasi Biner 25
2.2.17.2 Metrik Deteksi IOC 26
2.2.17.3 Metrik Evaluasi Lintas Dataset 26
2.3 Analisis Perbandingan Metode 27
BAB III Metode Tugas Akhir 30
3.1 Alat dan Bahan Tugas Akhir 30
3.1.1 Alat 30
3.1.1.1 Perangkat Keras 30
3.1.1.2 Perangkat Lunak 30
3.1.2 Bahan 31
3.1.2.1 Dataset UNSW-NB15 31
3.1.2.2 Dataset *malware-traffic-analysis.net* 31
3.1.2.3 Dataset CTU-13 32
3.2 Metode yang Digunakan 32
3.3 Alur Tugas Akhir 34
3.3.1 Studi Literatur 35
3.3.2 Pengumpulan dan Persiapan Data 35
3.3.3 Perancangan Sistem 35
3.3.4 Implementasi Sistem 36
3.3.4.1 Ekstraksi Fitur 36
3.3.4.2 Pelatihan Model 37
3.3.4.3 Integrasi *Pipeline* 37
3.3.4.4 *Rule Engine* 39
3.3.5 Pengujian dan Evaluasi 40
3.3.6 Analisis Hasil dan Pelaporan 41
BAB IV Hasil dan Pembahasan 42
4.1 Hasil Implementasi Sistem 42
4.1.1 Arsitektur dan Komponen *Pipeline* 42
4.1.2 Implementasi Antarmuka Aplikasi Web 44
4.1.2.1 *Backend* REST API 44
4.1.2.2 *Frontend* 45
4.1.2.3 Integrasi LLM untuk Laporan Forensik 45
4.1.3 *Rule Engine*: Deteksi *Hard Classes* Berbasis Aturan 46
4.1.4 Mekanisme Verifikasi Manusia (*Human-in-the-Loop*) 48

UNIVERSITAS GADJAH MADA
**Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan**
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

4.1.4.1 Alur Kerja Verifikasi 48
4.1.4.2 Integrasi dengan *Chain of Custody* 48
4.1.4.3 Finalisasi dan Penyegelan Akhir 49
4.1.4.4 Ekspor dan Verifikasi Integritas Rantai 50
4.1.4.5 Demonstrasi Deteksi Modifikasi Tidak Sah 50
4.1.5 Keluaran Laporan Forensik 51
4.1.6 Integrasi LLM untuk Sintesis Laporan Forensik 52
4.1.6.1 Struktur Masukan 52
4.1.6.2 *System Prompt* dan Format Keluaran 52
4.1.6.3 Mekanisme *Fallback* 53
4.2 Evaluasi dan Validasi Kinerja 53
4.2.1 Evaluasi pada Dataset Benchmark UNSW-NB15 53
4.2.1.1 Definisi Metrik 53
4.2.2 Validasi Deteksi IOC pada Kasus *Malware* Dunia Nyata 56
4.2.2.1 Definisi Metrik 56
4.2.2.2 Evaluasi Deteksi IOC 56
4.2.2.3 Perbandingan dengan Security Onion 2.4 57
4.2.3 Evaluasi Generalisasi Lintas Dataset pada CTU-13 59
4.2.3.1 Metodologi Ekstraksi PCAP Terfokus 59
4.2.3.2 Definisi Metrik 60
4.2.4 Analisis Kontribusi Komponen *Pipeline* 63
4.3 Perbandingan dengan Penelitian Terdahulu 66
BAB V Kesimpulan dan Saran 70
5.1 Kesimpulan 70
5.2 Saran 70
DAFTAR PUSTAKA 72
LAMPIRAN L-1
L.1 Daftar Lampiran L-1
L.2 Cuplikan Kode Sumber Sistem AI-NIDS L-2
L.2.1 Arsitektur *Autoencoder* L-2
L.2.2 Pipeline Inferensi Multitahap L-3
L.2.3 *Rule-based Hard-class Handler* dan Deteksi *Zero-Day* L-6
L.3 Bukti Pelaksanaan Analisis dan Perbandingan Sistem L-12
L.4 Contoh Laporan Forensik Hasil *Generate* Sistem L-24

UNIVERSITAS GADJAH MADA
Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR TABEL

Tabel 2.1 Perbandingan penelitian terdahulu dan penelitian yang diusulkan. ... 11
Tabel 2.2 Perbandingan metode deteksi anomali *unsupervised* untuk Tahap 1A. 27
Tabel 2.3 Perbandingan metode klasifikasi multikelas *supervised* untuk Tahap 2. ... 28

Tabel 3.1 Spesifikasi perangkat keras yang digunakan. ... 30
Tabel 3.2 Perangkat lunak yang digunakan. ... 30

Tabel 4.1 Komponen model AI-NIDS dan parameter kunci. ... 42
Tabel 4.2 Endpoint REST API aplikasi web AI-NIDS. ... 45
Tabel 4.3 Aturan deteksi pada *rule engine* AI-NIDS. ... 46
Tabel 4.4 Hasil verifikasi rantai sebelum dan sesudah simulasi modifikasi tidak sah. ... 51
Tabel 4.5 Metrik evaluasi biner *end-to-end* AI-NIDS pada *test set* UNSW-NB15. ... 53
Tabel 4.6 Performa per kelas AI-NIDS pada *test set* UNSW-NB15 (diurutkan dari F1 tertinggi). ... 54
Tabel 4.7 Hasil deteksi IOC pada 10 kasus *malware* dari malware-traffic-analysis.net. ... 56
Tabel 4.8 Perbandingan deteksi IOC: AI-NIDS versus Security Onion 2.4. ... 58
Tabel 4.9 Hasil evaluasi lintas dataset AI-NIDS pada CTU-13. ... 61
Tabel 4.10 Hasil analisis kontribusi komponen metrik biner per konfigurasi *pipeline* pada *test set* UNSW-NB15. ... 63
Tabel 4.11 F1-score per kelas per konfigurasi *pipeline* (diurutkan dari F1 C3 tertinggi). ... 65
Tabel 4.12 Perbandingan AI-NIDS dengan penelitian terdahulu yang relevan. ... 68

Tabel L.1 Nilai SHA-256 artefak model yang digunakan pada seluruh kasus analisis. ... L-13
Tabel L.2 Metadata bukti analisis Pikabot + Cobalt Strike. ... L-13
Tabel L.3 Perbandingan deteksi IOC kasus Pikabot + Cobalt Strike. ... L-13
Tabel L.4 Metadata bukti analisis Gozi/ISFB + Cobalt Strike. ... L-15
Tabel L.5 Perbandingan deteksi IOC kasus Gozi/ISFB + Cobalt Strike. ... L-15
Tabel L.6 Metadata bukti analisis SSLoad + Cobalt Strike. ... L-16
Tabel L.7 Perbandingan deteksi IOC kasus SSLoad + Cobalt Strike. ... L-16
Tabel L.8 Metadata bukti analisis DarkGate. ... L-17
Tabel L.9 Perbandingan deteksi IOC kasus DarkGate. ... L-17
Tabel L.10 Metadata bukti analisis IcedID Bokbot + BackConnect VNC. ... L-18
Tabel L.11 Perbandingan deteksi IOC kasus IcedID Bokbot + BackConnect VNC. ... L-18
Tabel L.12 Rekapitulasi perbandingan deteksi IOC untuk 5 kasus perbandingan langsung. ... L-19
Tabel L.13 Rangkuman hasil evaluasi lintas dataset pada tiga skenario CTU-13. L-20
Tabel L.14 Metadata rekaman analisis CTU-13. ... L-20
Tabel L.15 Distribusi kelas *output* sistem ML: Botnet-46 (Virut, Skenario 5). ... L-21
Tabel L.16 Distribusi kelas *output* sistem ML: Botnet-47 (DonBot, Skenario 6). L-21

Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Tabel L.17 Distribusi kelas *output* sistem ML: Botnet-52 (RBot, Skenario 11). . . L-22
Tabel L.18 Rekaman *chain of custody* EVD-4AAE7BAC2755 sebelum modifikasi. L-22
Tabel L.19 Keluaran lengkap pengujian deteksi modifikasi tidak sah. L-23

Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR GAMBAR

Gambar 2.1 Diagram alur logika *chain of custody* dalam penanganan bukti digital. 18
Gambar 2.2 Arsitektur *autoencoder* [1]..... 20
Gambar 2.3 Ilustrasi proses *gradient boosting* [2]. 21
Gambar 3.4 Diagram alur logika *pipeline* AI-NIDS. 33
Gambar 3.5 Diagram alur tugas akhir. 34
Gambar 3.6 Arsitektur *pipeline* AI-NIDS. 36
Gambar 3.7 Arsitektur platform uji coba AI-NIDS. 38
Gambar 3.8 Alur kerja pengguna pada antarmuka web AI-NIDS. 38
Gambar 4.9 Kurva konvergensi pelatihan *autoencoder* Tahap 1A selama 30 epoch. 44
Gambar 4.10 Rekaman *chain of custody* AI-NIDS. 49
Gambar 4.11 *Confusion matrix* evaluasi AI-NIDS pada *test set* UNSW-NB15.. 55
Gambar 4.12 Perbandingan *Precision*, *Recall*, dan *F1-score* per kelas AI-NIDS pada *test set* UNSW-NB15. 55
Gambar 4.13 Perbandingan deteksi IOC: AI-NIDS versus Security Onion 2.4.. 59

UNIVERSITAS
GADJAH MADA
**Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan**
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR SINGKATAN

ACK	=	*Acknowledgment*
AE	=	*Autoencoder*
AE-GMM	=	*Autoencoder-Gaussian Mixture Model*
AI	=	*Artificial Intelligence* (Kecerdasan Buatan)
AI-NIDS	=	*Artificial Intelligence Network Intrusion Detection System*
API	=	*Application Programming Interface*
ATT&CK	=	*Adversarial Tactics, Techniques, and Common Knowledge*
C&C	=	*Command and Control*
CTU-13	=	*Czech Technical University* Dataset 2013
DGA	=	*Domain Generation Algorithm*
DNS	=	*Domain Name System*
DoS	=	*Denial of Service*
DR	=	*Detection Rate* (Tingkat Deteksi)
F1	=	F1-*score* (rata-rata harmonik *Precision* dan *Recall*)
FAR	=	*False Alarm Rate* (Tingkat Alarm Palsu)
FN	=	*False Negative*
FP	=	*False Positive*
HITL	=	*Human-in-the-Loop*
HTML	=	*HyperText Markup Language*
HTTP	=	*HyperText Transfer Protocol*
HTTPS	=	*HyperText Transfer Protocol Secure*
IAT	=	*Inter-Arrival Time* (Selang Waktu Antarpaket)
ICMP	=	*Internet Control Message Protocol*
IDS	=	*Intrusion Detection System* (Sistem Deteksi Intrusi)
IOC	=	*Indicator of Compromise*
IP	=	*Internet Protocol*
IPS	=	*Intrusion Prevention System* (Sistem Pencegahan Intrusi)
IRC	=	*Internet Relay Chat*
JSON	=	*JavaScript Object Notation*
LLM	=	*Large Language Model* (Model Bahasa Besar)
MITRE	=	*MITRE Corporation*
ML	=	*Machine Learning* (Pembelajaran Mesin)
NIDS	=	*Network Intrusion Detection System* (Sistem Deteksi Intrusi Jaringan)
OvR	=	*One-vs-Rest*

UNIVERSITAS
GADJAH MADA
**Implementasi AI-Assisted Network Forensics Berbasis Deteksi Multitahap (Autoencoder dan XGBoost)
untuk Otomatisasi Deteksi, Klasifikasi, dan Analisis Serangan Jaringan**
Timotius Kristafael Harjanto, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

PCAP	=	*Packet Capture* (Berkas Tangkapan Paket)
PDF	=	*Portable Document Format*
RDP	=	*Remote Desktop Protocol*
REST	=	*Representational State Transfer*
RFC	=	*Request for Comments*
RST	=	*Reset* (Bendera TCP)
SHA	=	*Secure Hash Algorithm*
SHAP	=	*SHapley Additive exPlanations*
SIEM	=	*Security Information and Event Management*
SMB	=	*Server Message Block*
SMTP	=	*Simple Mail Transfer Protocol*
SPA	=	*Single-Page Application*
SSH	=	*Secure Shell*
SVM	=	*Support Vector Machine*
SYN	=	*Synchronize* (Bendera TCP)
TCP	=	*Transmission Control Protocol*
TLS	=	*Transport Layer Security*
TN	=	*True Negative*
TP	=	*True Positive*
UDP	=	*User Datagram Protocol*
UGM	=	Universitas Gadjah Mada
UNSW-NB15	=	*University of New South Wales Network Benchmark* 2015
VNC	=	*Virtual Network Computing*
XGBoost	=	*Extreme Gradient Boosting*