



**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN
DENGAN ROUTER SERVER UNTUK MENDETEKSI
FLOODING ATTACK MENGGUNAKAN METODE LIVE
FORENSIC GUNA PENINGKATAN PERFORMA JARINGAN
KOMPUTER**



**ARIS DIANTO
NIM 55423110005**

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCU BUANA
JAKARTA
2026**



**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN
DENGAN ROUTER SERVER UNTUK MENDETEKSI
FLOODING ATTACK MENGGUNAKAN METODE LIVE
FORENSIC GUNA PENINGKATAN PERFORMA JARINGAN
KOMPUTER**



TESIS

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Magister

**UNIVERSITAS
MERCU BUANA**

**ARIS DIANTO
NIM 55423110005**

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCU BUANA
JAKARTA
2026**

HALAMAN PENYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Aris Dianto
NIM : 55423110005
Fakultas/Program Studi : Teknik / Magister Teknik Elektro

Menyatakan dengan sebenar-benarnya bahwa Tesis berjudul:

“Analisis Dan Implementasi Keamanan Jaringan Dengan Router Server Untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic Guna Peningkatan Performa Jaringan Komputer”

adalah hasil karya saya sendiri, tidak mengandung unsur plagiarisme, pelanggaran hak cipta, atau konten ilegal dalam bentuk apapun dan tidak melanggar hukum atau hak pihak manapun.

Apabila di kemudian hari ditemukan pelanggaran terhadap pernyataan ini, saya bersedia menanggung seluruh konsekuensi hukum dan membebaskan Universitas Mercu Buana dari segala bentuk tuntutan hukum dan saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

Jakarta, Februari 2026



1000
METERAI
TEMPEL
1ECBFANX029701521

Aris Dianto

SURAT KETERANGAN HASIL *SIMILARITY*

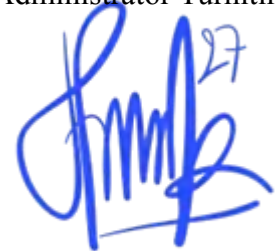
Menerangkan bahwa Jurnal / Karya Ilmiah / Laporan Tugas Akhir pada BAB I, BAB III, BAB IV, dan BAB V / Praktek Keinsinyuran atas nama:

Nama : ARIS DIANTO
NIM : 55423110005
Program Studi : Magister Teknik Elektro
Judul Tugas Akhir / Tesis
/ Praktek Keinsinyuran : Analisis Dan Implementasi Keamanan Jaringan Dengan Router Server Untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic Guna Peningkatan Performa Jaringan Komputer

Telah dilakukan pengecekan *Similarity* menggunakan aplikasi/sistem *Turnitin* pada **Selasa, 3 Maret 2026** dengan hasil presentase sebesar **9 %** dan dinyatakan memenuhi standar sesuai dengan ketentuan yang berlaku di Fakultas Teknik Universitas Mercu Buana.
Demikian surat keterangan ini dibuat dan digunakan sebagaimana mestinya.

Jakarta, 3 Maret 2026

Administrator Turnitin,



Itmam Haidi Syarif

HALAMAN PENGESAHAN

Laporan Tesis ini diajukan oleh:

Nama : Aris Dianto
NIM : 55423110005
Fakultas/Program Studi : Teknik / Magister Teknik Elektro
Judul Tesis : Analisis Dan Implementasi Keamanan Jaringan
Dengan Router Server Untuk Mendeteksi
Flooding Attack Menggunakan Metode Live
Forensic Guna Peningkatan Performa Jaringan
Komputer.

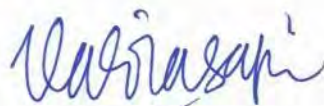
Telah berhasil dipertahankan pada sidang tanggal 13 Februari 2026 di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister pada Program Studi Magister Teknik Elektro, Fakultas Teknik Universitas Mercu Buana.

Disahkan oleh:

Ketua Penguji : Prof. Dr. Ir. Setiyo Budiyo, S.T., M.T., (.....)
IPU., ASEAN Eng., APEC Eng., ACPE
NIDN : 0312118206
Ketua Penguji : Prof. Dr. Ir. Andi Adriansyah, M.Eng. (.....)
NIDN : 0327027002
Anggota Penguji : Fadli Sirait, S.Si., M.T., Ph.D. (.....)
NIDN : 0320057603

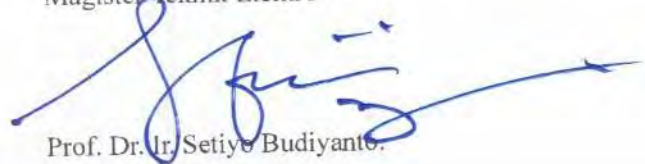
Jakarta, 18 Februari 2026
Mengetahui,

Dekan Fakultas Teknik



Dr. Zulfa Fitri Ikatinasari, M.T.
NIDN. 0307037202

Ketua Program Studi
Magister Teknik Elektro



Prof. Dr. Ir. Setiyo Budiyo,
S.T., M.T., IPU., ASEAN
Eng., APEC Eng., ACPE.
NIDN. 0312118206

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Tesis ini. Penulisan Tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magistek Teknik Elektro pada Fakultas Teknik Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Tesis ini, sangatlah sulit bagi saya untuk menyelesaikan Tesis ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Prof. Dr. Ir. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana
2. Dr. Zulfa Fitri Ikatrinasari, M.T. selaku Dekan Fakultas Teknik
3. Prof. Dr. Ir. Setiyo Budiyo, S.T., M.T., IPU., ASEAN Eng., APEC Eng., ACPE. selaku Ketua Program Studi Magister Teknik Elektro
4. Prof. Dr. Ir. Setiyo Budiyo, S.T., M.T., IPU., ASEAN Eng., APEC Eng., ACPE. selaku Dosen Pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan Tesis ini;
5. Rekan – rekan MTE angkatan 33.
6. Istri, anak – anak dan kedua orang tua yang memberikan semangat dan dukungan untuk menyelesaikan perkuliahan di jurusan MTE Universitas Mercu Buana.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Tesis ini membawa manfaat bagi pengembangan ilmu.

Jakarta, Februari 2026
Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama : Aris Dianto
NIM : 55423110005
Fakultas/Program Studi : Teknik / Magister Teknik Elektro
Judul Tesis : Analisis Dan Implementasi Keamanan Jaringan Dengan Router Server Untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic Guna Peningkatan Performa Jaringan Komputer

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tesis saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 13 Februari 2026

Yang menyatakan,



Aris Dianto

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DENGAN ROUTER SERVER UNTUK MENDETEKSI FLOODING ATTACK MENGUNAKAN METODE LIVE FORENSIC GUNA PENINGKATAN PERFORMA JARINGAN KOMPUTER

ARIS DIANTO

ABSTRAK

Permasalahan utama di lapangan adalah serangan DDoS SYN Flood yang tinggi di Indonesia (38,2% menurut BSSN 2023) merusak router tidak hanya secara logika jaringan tetapi juga secara fisik, namun teknik investigasi forensik yang ada (*post-mortem*) gagal menangkap bukti volatil. Penelitian ini bertujuan membuktikan dampak fisik serangan dan mengembangkan metode *live forensics* praktis untuk router embedded. Eksperimen dilakukan pada router MikroTik RB750r2 dan RB951-2n dengan variasi intensitas serangan. Hasilnya, serangan menyebabkan kenaikan suhu CPU drastis hingga 75,9°C dan konsumsi daya hingga 68,8%, yang secara teori Arrhenius memperpendek umur router (MTBF turun >67%). Untuk menjawab kebutuhan akuisisi bukti, dikembangkan RFT v1.0 yang terbukti ringan (tambah beban CPU 11-16%) dan berhasil mengambil bukti kunci seperti status koneksi dengan keberhasilan 93,6%. Dibanding metode *post-mortem*, pendekatan *live* ini 59,4% lebih lengkap datanya dan 53,6% lebih cepat proses investigasinya (29 menit vs 62,5 menit). Yang tak kalah penting, seluruh prosedur dirancang agar buktinya sah di pengadilan Indonesia, dengan skor kepatuhan UU ITE/PP PSTE mencapai 86%. Kesimpulannya, penelitian ini berhasil membuat solusi forensik yang efektif, cepat, dan legal untuk investigasi serangan DDoS pada router, yang dapat langsung diadopsi oleh admin jaringan atau penyidik di Indonesia.

Kata Kunci: *Live Forensics*, Router MikroTik, SYN Flood, Dampak Hardware, Forensik Jaringan, UU ITE.

**NETWORK SECURITY ANALYSIS AND IMPLEMENTATION WITH A
ROUTER SERVER TO DETECT FLOODING ATTACKS USING THE LIVE
FORENSIC METHOD FOR IMPROVING COMPUTER NETWORK
PERFORMANCE**

ARIS DIANTO

ABSTRACT

The prevalence of DDoS SYN Flood attacks in Indonesia (38.2% as reported by BSSN 2023) presents a critical challenge, as these attacks compromise routers not only at the network logic layer but also induce physical hardware degradation. Conventional forensic investigation techniques, particularly post-mortem analysis, fail to capture volatile evidence essential for attack reconstruction. This study aims to empirically quantify the physical impact of SYN Flood attacks and develop a practical live forensic methodology tailored for embedded router systems. Experimental evaluation was conducted on MikroTik RB750r2 (MIPS) and RB951-2n (ARM) routers under varying attack intensities. Results demonstrate that attacks cause a significant rise in CPU temperature (up to 75.9°C) and power consumption (increase up to 68.8%), which, according to the Arrhenius theory, accelerates hardware aging, reducing the Mean Time Between Failure (MTBF) by more than 67%. To address the evidence acquisition gap, a Router Forensic Toolkit (RFT v1.0) was developed. The toolkit operates with low overhead (additional CPU load of 11-16%) and successfully captured critical volatile artifacts, such as connection states, with a 93.6% success rate. Compared to the post-mortem approach, the live forensic method demonstrated a 59.4% higher evidence completeness rate and reduced the total investigation time by 53.6% (29 minutes vs. 62.5 minutes). Crucially, the entire forensic procedure was designed to comply with Indonesian digital evidence regulations, achieving an 86% compliance score against the Electronic Information and Transactions Law (UU ITE) and its implementing regulations (PP PSTTE). In conclusion, this research provides an effective, rapid, and legally admissible forensic solution for DDoS attack investigation on routers, which can be directly adopted by network administrators and digital investigators in Indonesia.

Keywords: *Live Forensics, MikroTik Router, SYN Flood, Hardware Impact, Network Forensics, UU ITE.*

DAFTAR ISI

SAMPUL	ii
PERNYATAAN KARYA SENDIRI	iii
SURAT KETERANGAN HASIL UJI TURNITIN.....	iv
HALAMAN PENGESAHAN.....	v
KATA PENGANTAR.....	vi
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR	vii
ABSTRAK	viii
ABSTRACT.....	ix
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	5
1.4 Tujuan Masalah	6
1.5 Manfaat Penelitian.....	7
1.6 Metode Penelitian	8
BAB II TINJAUAN PUSTAKA	
2.1 Kajian Literatur.....	10
2.1.1 Analisis Sintesis dari kajian Penelitian Terdahulu	10
2.1.2 Kajian Penelitian Terdahulu Terkait Topik Penelitian	12
2.1.3 Penelitian Dampak Serangan Siber pada Kinerja Hardware Jaringan	19
2.1.4 Penelitian Tentang Live Forensics Untuk Perangkat Embedded	20
2.1.5 Penelitian Tentang Forensik Jaringan Dalam Konteks Regulasi Indonesia	21
2.1.6 Identifikasi Research Gap	21
2.2 Landasan Teori	21
2.2.1 Teori Sistem Embedded dan Arsitektur Router	21
2.2.2 Teori Keamanan Jaringan dan Serangan Flooding	22
2.2.3 Teori Forensik Digital dan Chain of Evidence	22
2.2.4 Teori Thermal Management dan Reliability Elektronik	23
2.3 Kerangka Konseptual	23
2.3.1 Integrasi Disiplin Ilmu	23
2.3.2 Framework Live Forensics Untuk Router	24
2.3.3 Model Dampak Serangan Pada Kinerja Router	24
2.4 Hipotesis Penelitian	25
2.5 Definisi Operasional	25
BAB III METODE PENELITIAN	
3.1 Paradigma Penelitian dan Pendekatannya	27
3.2 Desain Eksperimen dan Konfigurasi	28
3.2.1 Desain Eksperimen	28
3.2.2 Konfigurasi Environment Lab	30
3.3 Prosedur Teknis Eksperimen	31

3.3.1	Tahapan Eksperimen	31
3.3.2	Teknik Akuisisi Live Forensics Spesifik	32
3.4	Instrumentasi dan Matrik Pengukuran	35
3.4.1	Instrumentasi Hardware	35
3.4.2	Metriks dan Formula Perhitungan	36
3.5	Pengembangan Router Forensic Toolkit (RFT)	37
3.5.1	Arsitektur RFT v1.0	37
3.5.2	Komponen Utama RFT	38
3.5.3	Algoritma Akuisisi Optimal	40
3.6	Teknik Analisis Data	41
3.6.1	Statistical Analysis Plan	41
3.6.2	Forensic Artifact Analysis	43
3.6.3	Legal Compliance Alaysis	44
3.7	Validasi dan Verifikasi	46
3.7.1	Validasi Metodologi	46
3.7.2	Realibility Testing	46
3.7.3	Replication Protocol	47
3.8	Pengolahan Data	48
3.8.1	Data Processing Pipeline	48
3.8.2	Software Stack Untuk Analisis	49
3.8.3	Machine Learning untuk Pattern Recognition	49
3.9	Protokol Keamanan dan Etika	51
3.9.1	Safety Protocols	51
3.9.2	Ethical Compliance	51
3.10	Batasan Metodologi dan Mitigasi	51
3.10.1	Identifikasi Batasan	51
3.10.2	Sensitivty Analysis	52
3.11	Rencana Implementasi dan Timeline	52
3.11.1	Timeline Penelitian	52
3.11.2	Resource Requirements	53
BAB IV HASIL DAN PEMBAHASAN		
4.1	Karakteristik Teknis dan Dampak Fisik Serangan SYN Flood Pada Router MikroTik	55
4.1.1	Karakteristik Implementasi Serangan	55
4.1.2	Hasil Pengukuran Konsumsi Daya (PCI)	56
4.1.3	Hasil Packet Loss dan Latency	59
4.1.4	Hasil Lengkap Pengukuran Termal dan Thermal Stress Indeks	61
4.1.5	Estimasi Penurunan MTBF	63
4.2	Implementasi dan Evaluasi Metodologi Live Forensics Pada Router Mikro Tik	63
4.2.1	Evaluasi Performance dan Minimal Invasiveness.....	63
4.2.2	Evaluasi Acquisition Success & Compatibility	65
4.2.3	Evaluasi Appropriate & Non-Disruptive Technique	65
4.2.4	Evaluasi Integrity & Evidence Management	66
4.3	Identifikasi Artefak Forensik dan Pengelolaan Bukti Digital yang Selaras dengan Regulasi Indonesia	67
4.3.1	Identifikasi dan Analisis Artefak	68
4.3.2	Rosedur Integritas (Hashing) dan Validasi Forensik	69

4.3.3	Implementasi Audit Trail dan Chain of Custody	70
4.4	Analisis Komparatif Efektivitas Live Forensics vs Post-Mortem Forensics	71
4.4.1	Desain Eksperimen Komparatif dan Metrik Evaluasi	72
4.4.2	Hasil Perbandingan Completeness of Evidence	73
4.4.3	Hasil Perbandingan Investigation Time	73
4.4.4	Hasil Perbandingan Admissibility in Court	74
4.4.5	Analisis Integratif dan Trade-off Analysis	76
BAB V SIMPULAN DAN SARAN		
5.1	Kesimpulan	78
5.2	Saran	79
DAFTAR PUSTAKA		80
LAMPIRAN		87



Daftar Tabel

Tabel 2.1	Kajian Penelitian Terdahulu Terkait Topik Penelitian	18
Tabel 2.2	Ringkasan penelitian tentang dampak fisik serangan pada perangkat jaringan.....	19
Tabel 3.1	Matriks Desain Eksperimen Faktorial	29
Tabel 3.2	Spesifikasi dan Kalibrasi Instrumentasi	35
Tabel 3.3	Komponen RFT dan Spesifikasi	39
Tabel 3.4	Klasifikasi Artefak Forensik Pada Router	43
Tabel 3.5	Checklist Compliance Dengan UU ITE dan PP PSTE	44
Tabel 3.6	Protokol Replikasi Eksperimen	47
Tabel 3.7	Software Stack Analisis Data	49
Tabel 3.8	Batasan Metodologi dan Strategi Mitigasi	51
Tabel 3.9	Kebutuhan Sumber Daya Penelitian	53
Tabel 4.1	Validasi Karakteristik Teknis Serangan	55
Tabel 4.2	Hasil Power Consumption Increase (PCI)	56
Tabel 4.3	Hasil ANOVA 3-way untuk Variabel Dependen PCI	57
Tabel 4.4	Hasil Penelitian Packet Loss dan Latency	59
Tabel 4.5	Hasil Uji Paket Loss	60
Tabel 4.6	Hasil Lengkap Pengukuran Termal dan Thermal Stress Indeks	61
Tabel 4.7	Hasil Uji untuk TSI_CPU	62
Tabel 4.8	Estimasi MTBF Berdasarkan Model Arrhenius Termal elektrik.....	63
Tabel 4.9	Hasil Pengukuran Resource Usage RFT v1.0	64
Tabel 4.10	Tingkat Keberhasilan Akuisisi Artefak Forensik	65
Tabel 4.11	Hasil Pengujian Prinsip Non-disruptive dan Atomicity	66
Tabel 4.12	Hasil Penilaian Compliance dengan Regulasi Indonesia	66
Tabel 4.13	Klasifikasi dan Karakteristik Artefak Forensik	68
Tabel 4.14	Implementasi Prosedur Integritas dan Hasil Validasi	69
Tabel 4.15	Protokol Chain of Custody dan Kesesuaian Regulasi	71
Tabel 4.16	Perbandingan Kelengkapan Bukti per kategori Artefak	73
Tabel 4.17	Analisis Perbandingan Waktu Investigasi	73
Tabel 4.18	Perbandingan Kelayakan Bukti di Pengadilan Berdasarkan Checklist Regulasi.....	74
Tabel 4.19	Matriks Trade-off Live vs Post-Mortem Forensic	76

Daftar Gambar

Gambar 1.1	Distribusi jenis serangan jaringan di Indonesia Tahun 2023	2
Gambar 2.2	Perbandingan Arsitektur Memory Management pada Berbagai Platform	20
Gambar 3.1	Desain Penelitian Sequential Explanatory Design	27
Gambar 3.2	Topologi Jaringan Laboratorium	30
Gambar 3.3	Research Framework	31
Gambar 3.3	Arsitektur Router Forensic Toolkit	37
Gambar 3.4	Pipeline Pengolahan Data	48
Gambar 3.5	Timeline Penelitian 12 Bulan	52
Gambar 4.1	Garfik Ukuran efek Hasil ANOVA 3-way terhadap PCI	59

