ANALISIS *LIVE FORENSICS* MEMORI TERHADAP SERANGAN *EMAIL SPOOFING* DAN *PHISHING*

SKRIPSI

Estarriandhika Rakhmatullah Yusuf
2103040102

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
NOVEMBER 2025

ANALISIS *LIVE FORENSICS* MEMORI TERHADAP SERANGAN *EMAIL SPOOFING* DAN *PHISHING*

SKRIPSI

Diajukan untuk memenuhi salah satu syarat memperoleh gelar sarjana komputer

Estarriandhika Rakhmatullah Yusuf
2103040102

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
NOVEMBER 2025

HALAMAN PERSETUJUAN

Skripsi yang diajukan oleh :

Nama	: Estarriandhika Rakhmatullah Yusuf
NIM	: 2103040102
Program Studi	: Teknik Informatika
Fakultas	: Teknik dan Sains
Perguruan Tinggi	: Universitas Muhammadiyah Purwokerto
Judul	: Analisis Live Forensics Memori terhadap Serangan Email Spoofing dan Phishing

Telah diterima dan disetujui

Purwokerto, 27 November 2025

PEMBIMBING

Agung Purwo Wicaksono, S.T., M.Kom.

NIK. 2160518

HALAMAN PENGESAHAN

Skripsi yang diajukan oleh:

Nama	: Estarriandhika Rakhmatullah Yusuf
NIM.	: 2103040102
Program Studi	: Teknik Informatika
Fakultas	: Teknik dan Sains
Perguruan Tinggi	: Universitas Muhammadiyah Purwokerto
Judul	: Analisis Live Forensic Memori terhadap Serangan Email Spoofing dan Phishing.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada Program Studi Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto.

DEWAN PENGUJI

Penguji 1	: Mukhlis Prasetyo Aji, S.T., M.Kom.	(.....)
Penguji 2	: Ermadi Satriya Wijaya, S.T., M.Kom.	(.....)
Penguji 3 (Pembimbing)	: Agung Purwo Wicaksono, S.T., M.Kom.	(.....)

Ditetapkan di : Puwokerto

Tanggal : 2025

Mengetahui

Dekan Fakultas Teknik dan Sains

Dr. T. Ir. Iskahar, S.T., M.T

NIK.2160207

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertandatangan di bawah ini:

Nama	: Estarriandhika Rakhmatullah Yusuf
NIM.	: 2103040102
Program Studi	: Teknik Informatika
Fakultas	: Teknik dan Sains
Perguruan Tinggi	: Universitas Muhammadiyah Purwokerto

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah hasil karya saya dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar serta bukan hasil penjiplakan dari karya orang lain.

Dengan pernyataan ini saya buat dan apabila kelak di kemudian hari terbukti ada unsur penjiplakan, saya bersedia mempertanggungjawabkan sesuai dengan ketentuan yang berlaku.

Purwokerto, 27 November 2025
Yang membuat pernyataan

Estarriandhika Rakhmatullah Yusuf

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Purwokerto dan demi pengembangan ilmu pengetahuan, saya yang bertanda tangan di bawah ini:

Nama	: Estarriandhika Rakhmatullah Yusuf
NIM.	: 2103040102
Program Studi	: Teknik Informatika
Fakultas	: Teknik dan Sains
Perguruan Tinggi	: Universitas Muhammadiyah Purwokerto
Jenis Karya	: Skripsi

Menyetujui untuk memberikan Hak Bebas Royalti Nonekslusif (*Non-exelusive royalty-free right)* kepada Universitas Muhammadiyah Purwokerto atas karya ilmiah saya yang berjudul:

Analisis Live Forensic Memori terhadap Serangan Email Spoofing dan Phishing.

Beserta perangkat yang ada (jika diperlukan) Dengan Hak Bebas Royalti Nonekslusif ini Universitas Muhammadiyah Purwokerto berhak menyimpan, mengalihmedia/ mengalihformatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan memublikasikan skripsi saya dengan tetap mencantumkan nama saya sebagai penulis/ pencipta dan sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sebenarnya.

Purwokerto, 27 November 2025

Yang menyatakan,

Estarriandhika Rakhmatullah Yusuf

KATA PENGANTAR

Alhamdulillah, puji syukur saya panjatkan ke hadirat Allah Subhanahu wa Ta'ala atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul *"Analisis Live Forensic Memori terhadap Serangan Email Spoofing dan Phishing"* sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom).

Penulisan tugas akhir ini bertujuan untuk memahami lebih dalam mengenai teknik analisis memori digital, khususnya dalam mengidentifikasi kasus email spoofing dan phishing melalui pendekatan forensik statis. Penulis berharap penelitian ini dapat memberikan kontribusi bagi perkembangan ilmu forensik digital serta menjadi referensi bagi pihak-pihak yang berkepentingan dalam bidang keamanan siber.

Penulis menyadari bahwa tugas akhir ini tidak terlepas dari bantuan, dukungan, dan arahan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada dosen pembimbing, keluarga, serta semua pihak yang telah membantu dalam proses penyusunan tugas akhir ini.

Akhir kata, penulis menyadari bahwa tugas akhir ini masih jauh dari sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun untuk perbaikan di masa yang akan datang.

UCAPAN TERIMA KASIH

Selama proses penyusunan skripsi ini, penulis menyadari bahwa tidak sedikit tantangan dan hambatan yang dihadapi. Namun, berkat doa, dukungan, dan bantuan dari berbagai pihak, akhirnya skripsi ini dapat terselesaikan dengan baik. Untuk itu, penulis menyampaikan ucapan terima kasih yang tulus kepada:

1. Allah SWT, atas segala rahmat dan karunia yang tak terhingga.
2. Kedua orang tua tercinta, yang selalu memberikan dukungan moral, materi, serta doa yang tiada henti, sehingga penulis tetap semangat dalam menyelesaikan studi.
3. Bapak Agung Purwo Wicaksono, S.T., M.Kom. selaku dosen pembimbing yang dengan sabar memberikan arahan, masukan, dan bimbingan selama proses penyusunan skripsi ini.
4. Bapak Muhammad Hamka, S.T., M.Kom. selaku dosen pembimbing akademik yang dengan segala kesabaran dan keikhlasan membimbing dan mengarahkan saya dalam masa perkuliahan baik dalam hal akademik maupun non akademik.
5. Seluruh dosen dan staf Program Studi Teknik Informatika, Fakultas Teknik dan Sains Universitas Muhammadiyah Purwokerto, yang telah memberikan ilmu dan pengalaman berharga selama masa studi.
6. Teman-teman seperjuangan, khususnya di kelas Teknik Informatika angkatan 2021, atas kebersamaan, dukungan, dan semangat selama masa perkuliahan hingga penyusunan skripsi ini.
7. Semua pihak yang tidak dapat disebutkan satu per satu, namun telah memberikan bantuan dan dukungan, baik secara langsung maupun tidak langsung.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ANALISIS *LIVE FORENSICS* MEMORI TERHADAP SERANGAN *EMAIL SPOOFING* DAN *PHISHING*

Estarriandhika Rakhmatullah Yusuf [1], Agung Purwo Wicaksono [2]

ABSTRAK

Serangan email spoofing dan phishing merupakan ancaman siber yang semakin sering digunakan untuk mencuri informasi sensitif, baik pada individu maupun organisasi. Teknik forensik memori (*live memory forensics*) menjadi salah satu pendekatan penting untuk mengidentifikasi *artefak* serangan yang tidak terekam dalam media penyimpanan tradisional, mengingat banyak aktivitas berbahaya hanya berlangsung di memori aktif. Penelitian ini bertujuan untuk menganalisis bukti digital yang tersimpan dalam memori selama terjadinya serangan *email spoofing* dan *phishing*, dengan fokus pada proses berbahaya, koneksi jaringan yang mencurigakan, payload yang dijalankan, serta indikator kompromi (IoC) lainnya. Metodologi penelitian meliputi akuisisi memori secara live menggunakan memory dumping tools, diikuti analisis terperinci menggunakan forensic frameworks seperti *Volatility* untuk mengekstraksi dan menginterpretasi *artefak* yang relevan. Hasil analisis menunjukkan bahwa serangan meninggalkan jejak signifikan pada memori, termasuk proses tidak sah, skrip berbahaya, data kredensial yang berhasil dicuri, hingga penggunaan teknik obfuscation dan anti-forensic oleh penyerang. Selain itu, penelitian ini menegaskan bahwa analisis memori mampu mengungkap aktivitas serangan yang tidak terlihat melalui metode forensik tradisional. Temuan ini memperkuat peran *live memory forensics* sebagai komponen penting dalam investigasi insiden siber serta memberikan rekomendasi bagi praktisi keamanan untuk meningkatkan deteksi, mitigasi, dan respons terhadap serangan berbasis email.

Kata kunci: *email spoofing, phishing, live memory forensics, Volatility, siber, artefak, memori.*

AN ANALYYSIS OF LIVE MEMORY FORENSICS OF EMAIL SPOOFING AND PHISING ATTACKS

Estarriandhika Rakhmatullah Yusuf [1] , Agung Purwo Wicaksono [2]

ABSTRACT

Email spoofing and phishing attacks have become increasingly prevalent cyber threats used to steal sensitive information from both individuals and organizations. Memory forensics, particularly live memory forensics, serves as a crucial approach for identifying attack artifacts that are not captured in traditional storage-based investigations, as many malicious activities occur only within active memory. This study aims to analyze digital evidence stored in volatile memory during email spoofing and phishing attacks, focusing on malicious processes, suspicious network connections, executed payloads, and other indicators of compromise (IoCs). The research methodology involves live memory acquisition using memory dumping tools, followed by detailed examination with forensic frameworks such as Volatility to extract and interpret relevant artifacts. The findings reveal that these attacks leave significant traces in memory, including unauthorized processes, active malicious scripts, stolen credential data, and the presence of obfuscation or anti-forensic techniques employed by attackers. Furthermore, the results demonstrate that memory analysis can uncover attack behaviors that remain undetected through traditional forensic methods. Overall, this study reinforces the importance of live memory forensics as a key component in cyber incident investigations and provides recommendations for security practitioners to enhance detection, mitigation, and response strategies against email-based attacks.

Keywords: *email spoofing, phishing, live memory forensics, Volatility, cyber, artifacts, memory.*