Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer
Volume 5, Nomor 2, Juli 2025
p-ISSN: 2827-8135; e-ISSN: 2827-7953, Hal. 549-567
DOI: https://doi.org/10.55606/juisik.v5i2.1452
Available Online at: https://journal.sinov.id/index.php/juisik

Analisis Forensik pada Pemalsuan Email menggunakan Metode *National Institute of Justice* (NIJ)

Rokhmatun Nazila[1*], Fahmi Fachri[2]
[1-2]Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia

Alamat: Jl. Kutoarjo Km. 05, Wonoboyo, Jatisari, Kec. Kebumen, Kabupaten Kebumen, Jawa Tengah, 54317, Indonesia
Korespondensi penulis: nazilcerdas@gmail.com

Abstract*. Email spoofing is a form of cybercrime that often occurs by taking advantage of weaknesses in email protocols to deceive recipients through spoofing sender identities. This attack is a serious threat because it can be used to commit fraud, data theft, and the spread of malware. This study aims to analyze email spoofing cases with a digital forensic approach using the National Institute of Justice (NIJ) methodology, which includes five important stages: identification, collection, examination, analysis, and reporting. The main problem studied is the difficulty of detecting fake emails on internal networks that have not implemented modern email authentication mechanisms such as the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC). The research method used was qualitative, experimental, with controlled simulation. Some of the tools used in this experiment include Postfix, SWAKS, tcpdump, and Mozilla Thunderbird. In simulations, fake billing emails are sent from fake addresses (e.g. finance@bankxyz.com) through an open SMTP service to see the extent to which spoofing can be done without being detected. During this process, email traffic is recorded, and various digital artifacts such as .eml files, .pcap packet captures, SMTP logs, and PDF attachments are successfully collected for further analysis. The results of forensic analysis showed that there were inconsistencies in the email headers, especially in the Return-Path, From, and Received fields, which were the main indicators of spoofing activity. This study proves that email spoofing is very likely to occur on unprotected systems, so strengthening email server configuration and implementing authentication is an important step. In addition, the NIJ method has proven to be effective in providing a systematic and valid forensic investigation structure, and can be a reference in handling email-based cybercrime cases in the future.*

Keywords*: Cybersecurity, Digital Forensics, Email Spoofing, Header Analysis, NIJ Method.*

Abstrak. Email spoofing merupakan salah satu bentuk kejahatan siber yang sering terjadi dengan memanfaatkan kelemahan pada protokol email untuk menipu penerima melalui pemalsuan identitas pengirim. Serangan ini menjadi ancaman serius karena dapat digunakan untuk melakukan penipuan, pencurian data, hingga penyebaran malware. Penelitian ini bertujuan untuk menganalisis kasus email spoofing dengan pendekatan forensik digital menggunakan metodologi National Institute of Justice (NIJ), yang meliputi lima tahapan penting: identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Permasalahan utama yang dikaji adalah sulitnya mendeteksi email palsu pada jaringan internal yang belum mengimplementasikan mekanisme autentikasi email modern seperti Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), dan Domain-based Message Authentication, Reporting & Conformance (DMARC). Metode penelitian yang digunakan bersifat kualitatif eksperimental dengan simulasi terkendali. Beberapa alat bantu yang digunakan dalam eksperimen ini antara lain Postfix, SWAKS, tcpdump, dan Mozilla Thunderbird. Dalam simulasi, email tagihan palsu dikirim dari alamat palsu (misalnya finance@bankxyz.com) melalui layanan SMTP terbuka untuk melihat sejauh mana spoofing dapat dilakukan tanpa terdeteksi. Selama proses ini, lalu lintas email direkam, dan berbagai artefak digital seperti file .eml, hasil tangkapan paket .pcap, log SMTP, dan lampiran PDF berhasil dikumpulkan untuk dianalisis lebih lanjut. Hasil analisis forensik menunjukkan adanya ketidaksesuaian pada bagian header email, terutama pada field Return-Path, From, dan Received, yang menjadi indikator utama adanya aktivitas spoofing. Penelitian ini membuktikan bahwa email spoofing sangat mungkin terjadi pada sistem yang tidak terlindungi, sehingga penguatan konfigurasi server email dan penerapan autentikasi menjadi langkah penting. Selain itu, metode NIJ terbukti efektif dalam memberikan struktur investigasi forensik yang sistematis dan valid, serta dapat menjadi acuan dalam penanganan kasus kejahatan siber berbasis email di masa depan.

Kata Kunci: Analisis Header, Email Spoofing, Forensik Digital, Keamanan Siber, Metode NIJ.

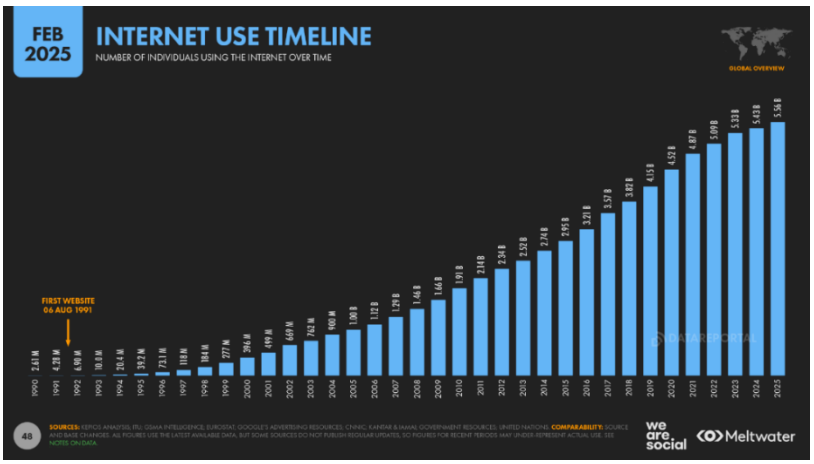
Received: Juni 29, 2025; Revised: Juli 13, 2025; Accepted: Juli 27, 2025; Online Available: Juli 29, 2025

1. LATAR BELAKANG

Layanan internet sangat berguna dalam kehidupan masyarakat saat ini. Masyarakat yang hidup di era industri 5.0 mengalami ketergantungan tinggi terhadap teknologi yang berkembang sangat pesat. Umat manusia pada era ini sangat bergantung pada teknologi; hal ini terlihat dari kepemilikan perangkat seperti ponsel, laptop, dan alat elektronik lainnya (Aryasatya & Wibawa, 2022). Peningkatan penggunaan perangkat elektronik tersebut tidak terlepas dari koneksi internet, karena sebagian besar layanan yang terdapat di dalamnya membutuhkan akses internet untuk dapat digunakan.

Internet menjadi sarana utama dalam pertukaran informasi, komunikasi, perdagangan, serta pelaksanaan berbagai program digital. Salah satu perkembangan teknologi yang relevan adalah *Internet of Things* (IoT), yang memungkinkan perangkat dikendalikan dan dimonitor dari jarak jauh, sehingga memberikan efisiensi dan kenyamanan bagi penggunanya (Haeruddin, 2024). Selain itu, internet juga telah merestrukturisasi perdagangan global, memudahkan transaksi dan mendukung interaksi antara penjual dan pembeli yang sebelumnya sulit dilakukan secara fisik (Pemikiran et al., 2023). Perkembangan ini berjalan secara berurutan, dimulai dari peningkatan perangkat elektronik, diikuti oleh penggunaan internet, dan berujung pada peningkatan layanan berbasis internet.

Peningkatan ini terus terjadi karena pengguna merasakan kemudahan, manfaat, bahkan dalam beberapa kasus, ketergantungan terhadap teknologi. Aktivitas manusia yang semakin sering dilakukan secara *online* turut mendorong terjadinya revolusi digital yang menuntut layanan internet berkualitas. Data terbaru menunjukkan bahwa jumlah pengguna internet global terus meningkat.



(Sumber: www.datareportal.com)

Gambar 1. Kenaikan User Internet Global

Per Februari 2025, tercatat jumlah pengguna internet global mencapai 5,56 miliar. Data dari DataReportal (www.datareportal.com) menunjukkan bahwa 5,32 miliar orang masih menonton siaran televisi linier seperti saluran konvensional dan kabel, namun angka tersebut hampir 250 juta lebih rendah dibandingkan jumlah pengguna internet. Hal ini menunjukkan bahwa internet telah menjadi media utama dalam kehidupan modern.

Kemajuan pesat teknologi internet menuntut tersedianya layanan yang lebih cepat, andal, dan berkualitas. Kualitas layanan ini menjadi kunci dalam mendukung akses ke berbagai platform digital (Saskara et al., 2024). Beberapa platform yang sangat umum digunakan seperti *email*, *e-learning*, dan *e-commerce*, sebagian besar mengharuskan pengguna untuk memiliki alamat email dalam proses registrasi dan autentikasi akun (Prado et al., 2024). Email merupakan sarana pertukaran informasi dan komunikasi daring yang memungkinkan pengiriman teks, gambar, video, berkas, dan berbagai fitur lainnya (Bachri & Gunawan, 2024). Kondisi ini menyebabkan email menyimpan banyak data pribadi, sehingga menjadikannya sasaran empuk bagi kejahatan siber (*cybercrime*).

Sekitar 75% dari pengguna internet global secara aktif menggunakan email. Pada tahun 2023, terdapat 4,37 miliar pengguna email, dan diperkirakan akan meningkat menjadi 4,89 miliar pada tahun 2027 (DataReportal, 2025). Jumlah ini menunjukkan tren peningkatan yang konsisten dari tahun ke tahun. Dengan posisi email sebagai identitas digital utama, potensi terjadinya kejahatan siber semakin besar. Pelaku kejahatan siber memanfaatkan berbagai celah dalam sistem email, termasuk penyimpanan data pengguna (Chen et al., 2023). Selain menyerang data pribadi, para *hacker* juga dapat menyerang lembaga, organisasi, bahkan pemerintah. Serangan bisa dilakukan secara individu maupun kelompok, menggunakan berbagai metode seperti *spoofing*, *malware*, *phishing*, dan serangan lainnya.

Salah satu kejahatan siber yang marak di Indonesia adalah *email spoofing*, di mana pelaku memalsukan *header* email dengan mengatasnamakan institusi terpercaya untuk menipu korban (Prabakaran et al., 2023). Dalam praktiknya, *email spoofing* juga dapat digunakan untuk menyebarkan *malware*, melakukan *phishing*, atau serangan *engineering* yang lebih kompleks (Rusydi et al., n.d.). Banyak masyarakat, bahkan organisasi besar sekalipun, sering kali tidak menyadari serangan ini karena minimnya jejak eksplisit dari pelaku (Liu et al., 2023). Hal ini diperparah oleh rendahnya kesadaran pengguna bahwa informasi pengirim email dapat dimanipulasi dengan mudah, dan tidak semua sistem email memiliki fitur keamanan seperti SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*), dan DMARC (*Domain-based Message Authentication, Reporting and Conformance*) untuk mendeteksi *spoofing* lebih awal (Ath-thaariq et al., 2023).

Per bulan Mei 2025 kasus pemalsuan *email* yang bermotif penipuan penerimaan pekerjaan dengan mengatasnamakan PT. KAI-Divre III Palembang, berakibat pada korban yang rugi jutaan rupiah (Saputra & Misinem, n.d.). Contoh lain adalah laporan dari Internet Crime Complaint Center (IC3) yang mencatat bahwa sejak 2019 hingga 2023, kasus *Business Email Compromise* (BEC) yang menggunakan teknik *email spoofing* terus meningkat, dengan total kerugian mencapai 2,9 miliar dolar AS (The Internet Crime Complaint Center, 2024). Kasus-kasus ini menunjukkan betapa serius dampak dari *email spoofing*, baik terhadap aspek finansial maupun reputasi korban.

Penanganan kasus *email spoofing* membutuhkan analisis forensik digital yang rinci dan sistematis terhadap email yang digunakan pelaku. Salah satu metode yang relevan adalah metode NIJ (*National Institute of Justice*), yang dinilai lebih sistematis, akurat, dan sah secara hukum dibandingkan metode lainnya (Marcellino et al., 2023). Metode NIJ memiliki tahapan yang lengkap mulai dari persiapan, pengumpulan, pemeriksaan, analisis, hingga pelaporan, sebagaimana disampaikan oleh (Anwar et al., 2024), menjadikannya metode komprehensif dalam menghadapi kejahatan siber.

Dalam penelitian ini, dilakukan simulasi menggunakan beberapa *tools* dan utilitas jaringan yang disesuaikan dengan tahapan metode NIJ. Alat yang digunakan meliputi Postfix, Swaks, TCPDUMP, Sendemail, dan Thunderbird. Postfix berperan sebagai *Mail Transfer Agent* (MTA) dari server palsu untuk mengirim email tanpa autentikasi, yang penting dalam pengujian kerentanan SMTP (Wijayanto, 2023). Untuk mengatur elemen seperti *From*, *To*, dan *Subject* dalam email *spoofing* serta menyisipkan lampiran, digunakan Swaks (Anabelle et al., 2024). Lalu lintas pengiriman direkam dengan TCPDUMP dalam format .pcap untuk dianalisis melalui Wireshark (Maulana, 2023). Visualisasi pesan email dianalisis dengan Mozilla Thunderbird, yang memungkinkan pemeriksaan manual terhadap konten dan *metadata*-nya (Angelone & Monaghan, 2022). Keempat alat tersebut membentuk satu alur eksperimen forensik digital yang saling terhubung dan sesuai dengan kerangka kerja metode NIJ.

Berdasarkan latar belakang yang telah diuraikan, tujuan dari penelitian ini adalah untuk menjelaskan proses analisis forensik terhadap email yang menjadi objek serangan *email spoofing* dengan menggunakan metode NIJ (*National Institute of Justice*). Penelitian ini juga bertujuan untuk mengetahui manfaat penggunaan berbagai *tools* forensik dalam menganalisis struktur teknis serta metadata header pada *email spoofing*. Selain itu, penelitian ini dimaksudkan untuk menilai sejauh mana efektivitas simulasi *email spoofing* dapat dimanfaatkan dalam mengidentifikasi karakteristik *spoofing* melalui analisis terhadap header email secara mendalam.

2. KAJIAN TEORITIS

Email merupakan sarana komunikasi digital yang sangat penting dalam kehidupan modern, baik dalam ranah pribadi, bisnis, maupun pemerintahan. Pengiriman pesan dalam sistem email didasarkan pada protokol SMTP (*Simple Mail Transfer Protocol*), yang meskipun efisien, memiliki kelemahan utama: minimnya mekanisme autentikasi. Hal ini membuka celah bagi pelaku kejahatan siber untuk melakukan email spoofing, yaitu teknik pemalsuan identitas pengirim dalam email dengan tujuan menipu penerima agar mempercayai pesan yang dikirim.

Serangan email spoofing sering kali digunakan dalam aksi phishing, penyebaran malware, serta manipulasi sosial. Ketika sistem belum menerapkan autentikasi seperti SPF, DKIM, dan DMARC, peluang keberhasilan serangan meningkat signifikan. Oleh karena itu, pendekatan keamanan dan analisis forensik menjadi krusial untuk mendeteksi serta mencegah serangan berbasis email ini.

Dalam konteks forensik digital, analisis terhadap artefak email seperti header, metadata, log SMTP, dan lampiran memungkinkan penyidik untuk mengidentifikasi pola komunikasi yang mencurigakan, memverifikasi keaslian pengirim, serta merekonstruksi alur serangan. Teknologi forensik ini sangat bermanfaat untuk menelusuri aktivitas kejahatan, baik dalam proses investigasi internal organisasi maupun dalam penyusunan alat bukti hukum.

Salah satu pendekatan yang sistematis dalam forensik digital adalah Metode *National Institute of Justice* (NIJ), yang meliputi lima tahap: identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Tahapan ini memberikan struktur kerja yang legal dan valid untuk memastikan bahwa setiap bukti digital dapat digunakan dalam proses penegakan hukum. Metode ini juga relevan dalam penguatan sistem keamanan organisasi melalui audit dan mitigasi risiko.

Dalam upaya memahami email spoofing lebih dalam, berbagai alat telah dikembangkan. Postfix digunakan sebagai mail transfer agent dalam simulasi pengiriman email palsu, SWAKS untuk manipulasi field email secara langsung, TCPDUMP untuk menangkap lalu lintas SMTP dalam format .pcap, serta Mozilla Thunderbird untuk menelusuri struktur email secara menyeluruh. Integrasi alat-alat ini mendukung eksperimen serta analisis forensik yang holistik.

Beberapa penelitian sebelumnya memberikan kontribusi penting terhadap studi ini. Meshram et al. (2024) mengembangkan sistem deteksi spoofing berbasis rule-based dengan analisis header email. Anabelle et al. (2024) menyoroti efektivitas Thunderbird sebagai alat utama analisis email. Penelitian oleh Widodo dan Aji (2022) menggunakan TCPDUMP untuk menangkap paket SMTP, sedangkan Wintolo et al. (2025) mengadopsi pendekatan NF-DLC untuk analisis jaringan.

Penelitian berbasis kecerdasan buatan juga mulai berkembang, seperti studi oleh Neha et al. (2025) yang mengintegrasikan analisis AI dalam deteksi spoofing, namun belum menggabungkan pendekatan NIJ. Selain itu, studi oleh Rahma dan Riadi (2022) serta Ihekweazu (2025) menunjukkan pentingnya integrasi metode investigasi manual, simulasi, dan analisis jaringan.

Temuan-temuan dari studi sebelumnya menunjukkan adanya kesenjangan dalam pendekatan investigasi email spoofing yang komprehensif. Penelitian ini berupaya menjembatani kesenjangan tersebut dengan menggabungkan metode NIJ, simulasi serangan, serta analisis multi-alat dalam lingkungan terkendali. Meskipun hipotesis tidak dinyatakan secara eksplisit, pendekatan ini diasumsikan mampu mengungkap bahwa email spoofing masih dapat dilakukan dan lolos dari deteksi jika sistem belum memiliki mekanisme perlindungan memadai.

Dengan dasar teori dan penelitian terdahulu, studi ini bertujuan untuk membuktikan efektivitas metode NIJ dalam membentuk kerangka kerja investigasi forensik email spoofing yang sistematis, valid, dan dapat direplikasi pada berbagai skenario keamanan siber.

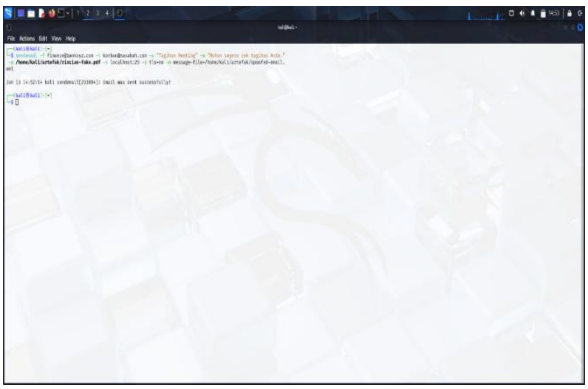
3. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan eksperimen. Metode ini dipilih karena mampu menjelaskan proses investigasi digital secara rinci dan menyeluruh terhadap kasus *email spoofing*. Pendekatan kualitatif eksperimen dalam konteks ini difokuskan untuk menggambarkan bagaimana serangan dilakukan serta bagaimana jejak digital dianalisis melalui pendekatan forensik. Penelitian ini tidak berorientasi pada perhitungan statistik, melainkan pada proses sistematis dalam mengungkap teknik manipulasi pengirim serta struktur teknis email yang dipalsukan. Rangka kerja analisis mengacu pada metode *National Institute of Justice* (NIJ) yang terdiri dari lima tahap utama, yaitu identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan (Anwar et al., 2024).

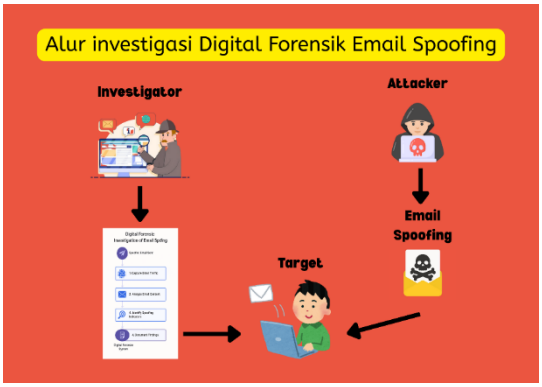
Alat utama yang digunakan dalam penelitian ini adalah laptop dengan spesifikasi Lenovo Ideapad 3 Slim generasi ke-11 yang mendukung semua tahapan simulasi dan analisis. Sistem operasi yang digunakan adalah Windows 11, didukung dengan mesin virtual VirtualBox versi 7.1.10 yang menjalankan Kali Linux berbasis Debian (64-bit) sebagai server SMTP palsu. Untuk mengirimkan email palsu (*spoofed*), digunakan aplikasi *Mail Transfer Agent* (MTA) Postfix yang memungkinkan pengiriman tanpa autentikasi. Proses manipulasi pengirim email dilakukan menggunakan SWAKS (*Swiss Army Knife for SMTP*) yang dapat mengatur elemen seperti *MAIL FROM*, *RCPT TO*, dan menyisipkan lampiran. TCPDUMP digunakan untuk

merekam lalu lintas SMTP secara waktu nyata dan menghasilkan file *.pcap* sebagai artefak digital. File tersebut kemudian dianalisis menggunakan Wireshark untuk memvisualisasikan komunikasi SMTP dan *payload spoofing*. Untuk analisis lebih mendalam terhadap struktur email dan *header*, digunakan Mozilla Thunderbird sebagai *email client*.

Skenario simulasi diawali dengan peran *attacker* yang mengumpulkan data dari lembaga resmi yang identitasnya akan dipalsukan, seperti nama bank, alamat email, gaya bahasa, dan logo. Selanjutnya, *attacker* mengirim email dengan identitas palsu kepada korban menggunakan Postfix dan SWAKS. Email dikirim melalui protokol SMTP tanpa autentikasi, memungkinkan manipulasi identitas pengirim. Setelah korban membuka email, kemungkinan besar mereka akan mengunduh lampiran atau mengklik tautan berbahaya yang memungkinkan pencurian data pribadi atau infeksi malware. Semua aktivitas digital tersebut direkam menggunakan TCPDUMP untuk kemudian dianalisis melalui pendekatan forensik.



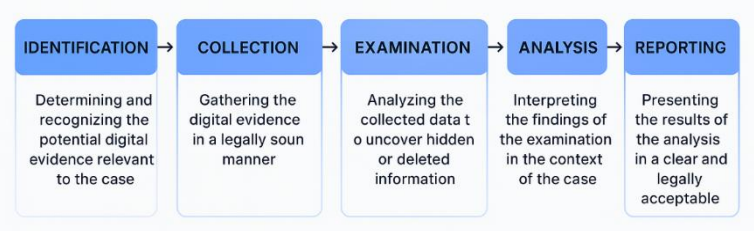
Gambar 2. Pelaku Berhasil mengirim email *spoofing* dengan beberapa tools



Gambar 3. Alur Analisis Digital Forensik

Dalam prosesnya, tahap pertama adalah identifikasi, di mana peneliti menentukan perangkat dan artefak digital yang menjadi bukti, seperti file *.eml*, log server, dan data jaringan. Tahap kedua adalah pengumpulan bukti, yang dilakukan dengan menangkap lalu lintas SMTP menggunakan TCPDUMP serta mengakses log aktivitas server Postfix. Selanjutnya pada tahap pemeriksaan, peneliti menganalisis struktur *header* email dan metadata SMTP menggunakan

Thunderbird. Pada tahap analisis, peneliti menelusuri asal IP pengirim, jalur distribusi email, serta mengidentifikasi pola komunikasi yang mencurigakan. Tahap terakhir adalah pelaporan, di mana hasil investigasi disusun dalam laporan forensik yang berisi temuan utama dan visualisasi hasil analisis, yang dapat dijadikan bukti teknis maupun referensi akademik.



Gambar 4. Alur Analisis

Pengumpulan data dalam penelitian ini dilakukan melalui dua cara, yaitu studi literatur dan observasi langsung. Studi literatur dilakukan dengan menelaah berbagai sumber ilmiah seperti jurnal, buku, artikel konferensi, dan situs daring terpercaya yang relevan dengan topik *email spoofing*, forensik digital, protokol SMTP, serta penggunaan perangkat lunak pendukung. Sementara itu, observasi dilakukan secara langsung terhadap seluruh aktivitas selama simulasi, mulai dari pengiriman email palsu, pencatatan tangkapan paket SMTP, hingga proses analisis menggunakan Thunderbird. Semua kegiatan tersebut dicatat secara sistematis untuk memperoleh data teknis yang mendukung validitas hasil penelitian.

4. HASIL DAN PEMBAHASAN

Bab ini menguraikan temuan yang diperoleh melalui simulasi serangan *email spoofing*, disertai dengan proses investigasi forensik digital berdasarkan pendekatan dari *National Institute of Justice* (NIJ). Setiap langkah, mulai dari akuisisi data hingga penyusunan laporan, disajikan secara runtut guna memperlihatkan bagaimana bukti digital dapat diperoleh, diperiksa, dievaluasi, dan disampaikan dalam konteks serangan *email spoofing*.

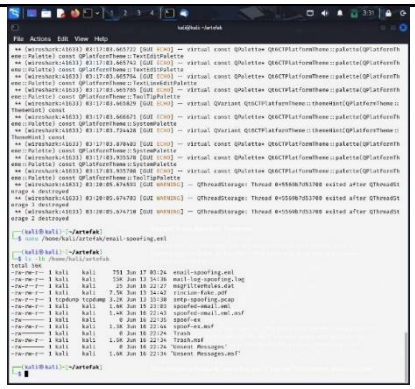
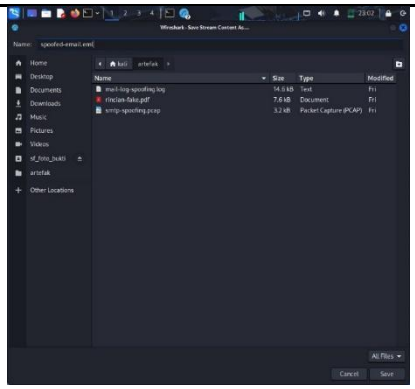
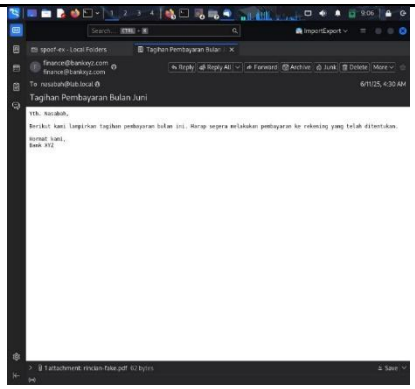
Eksperimen dilakukan dalam lingkungan laboratorium yang terkontrol dengan memanfaatkan perangkat lunak seperti *Postfix*, *SWAKS*, *tcpdump*, dan *Thunderbird*. Data yang dikumpulkan mencakup berbagai artefak digital, termasuk file *.eml*, *.pcap*, serta log SMTP. Seluruh artefak dianalisis untuk mendeteksi pola serangan *spoofing* dan mengidentifikasi celah keamanan dalam sistem pengiriman email. Hasil analisis kemudian dibandingkan dengan tujuan awal penelitian untuk menilai sejauh mana capaian yang diperoleh.

Dalam penelitian ini, terdapat beberapa tahap yang dilakukan guna menghasilkan analisis forensik yang dapat dipertanggungjawabkan dan diproses lebih lanjut. Tahapan tersebut disusun berdasarkan pendekatan NIJ sebagai berikut:

Tahap Identifikasi

Tahap ini bertujuan untuk mengidentifikasi artefak digital utama yang diperoleh dari hasil tangkapan lalu lintas jaringan dan file *email spoofing*. Beberapa artefak yang ditemukan mencakup *header email* yang mengindikasikan pemalsuan identitas pengirim, alamat IP yang digunakan dalam proses pengiriman, serta lampiran berformat PDF yang disertakan dalam email. Langkah ini menjadi fondasi bagi proses analisis mendalam di tahap selanjutnya.

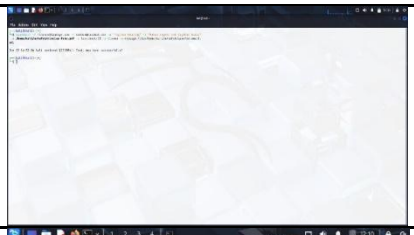
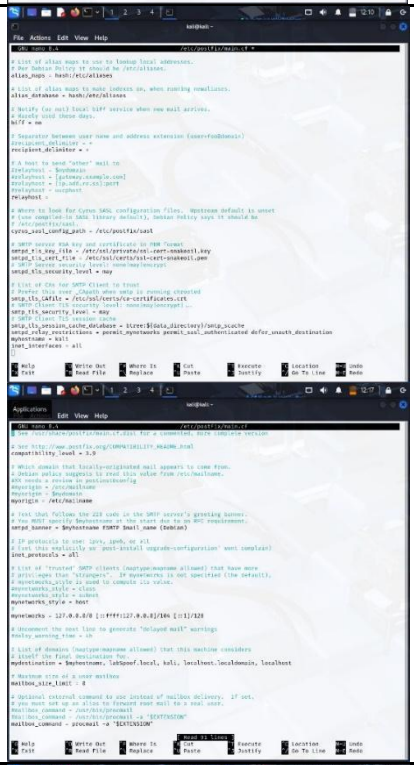
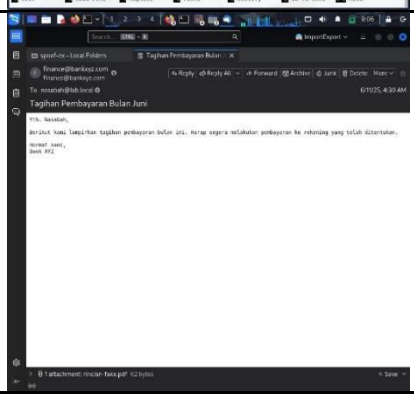
Tabel 1. Artefak Hasil Identifikasi Awal

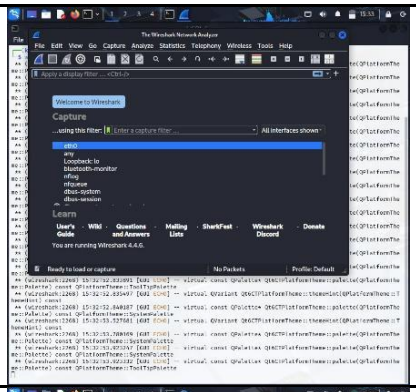
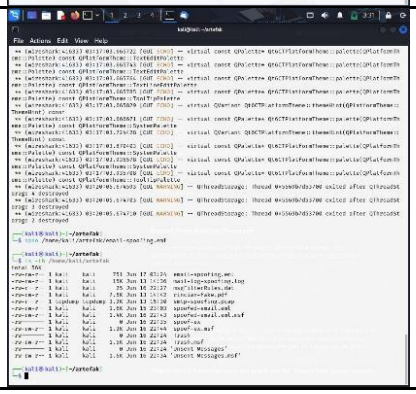
No	Screenshot Terminal	Command Line	Fungsi
1		● Isi direktori /artefak ● File *.eml* dibuka dengan *nano*	● Menunjukkan bahwa artefak telah dikumpulkan: *.eml*, *.pcap*, *.log*, *.pdf*. ● Menampilkan struktur *header* mentah: *From*, *Subject*, *Return-Path*, dan sebagainya.
2		● File *.eml* dibuka dengan *nano*	● Menunjukkan bahwa file *capture* SMTP siap dianalisis.
3		● Lampiran PDF terlihat di *Thunderbird*	● Bukti bahwa *spoofing* juga melibatkan rekayasa lampiran.

Tahap Pengumpulan Data (*Collection*)

Pada tahap ini, proses simulasi pengiriman *email spoofing* dilakukan menggunakan *Sendmail* dan *SWAKS*. Email palsu dikirim ke akun sasaran dan diterima melalui klien *Thunderbird*. Selama simulasi berlangsung, aktivitas jaringan saat pengiriman dan penerimaan email dipantau dan direkam menggunakan *Wireshark* dan *tcpdump*, yang kemudian dijadikan artefak digital untuk analisis lanjutan.

Tabel 2. Aktivitas dan Artefak Selama Proses Collection

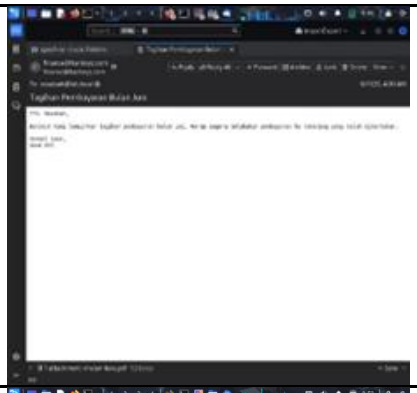
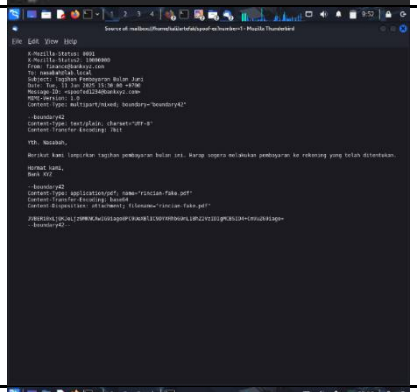
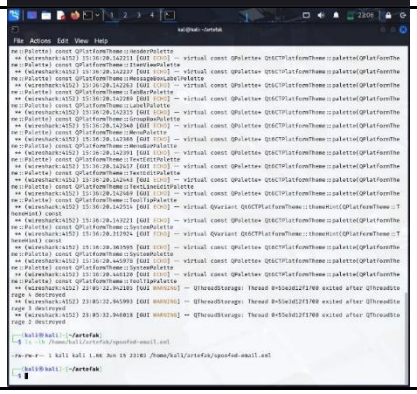
No	Screenshot Terminal	Command Line	Fungsi
1		● Perintah *SWAKS*/*Sendmail*	● Bukti bahwa simulasi *spoofing* dijalankan.
2		● Konfigurasi *Postfix*	● Menunjukkan bahwa *Postfix* telah diatur untuk menerima *email spoof*.
3		● Email masuk di *Mozilla Thunderbird*	● Bukti bahwa *email spoof* diterima oleh target.

4		● Proses *capture* dengan *tcpdump*	● Bukti bahwa proses berhasil direkam untuk forensik.
5		● Tampilan *Wireshark* saat *capture* aktif	● Visualisasi trafik SMTP saat pengiriman *email spoof* berlangsung.
6		● Isi direktori artefak	● Bukti bahwa seluruh file hasil simulasi telah terkumpul.

Tahap Pemeriksaan (*Examination*)

Tahapan ini menitikberatkan pada analisis mendalam terhadap artefak digital yang diperoleh, termasuk file *.eml* hasil *email spoofing*, rekaman lalu lintas jaringan berformat *.pcap*, serta log dari server email. Tujuannya adalah mengungkap ciri-ciri teknis dari serangan *spoofing* yang dapat diidentifikasi melalui penelaahan *header* email dan metadata SMTP.

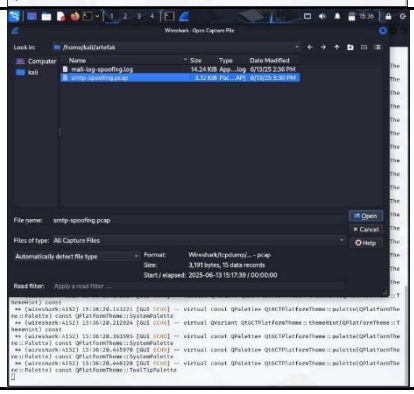
Tabel 3. Pemeriksaan Artefak Digital

No	Screenshot Terminal	*Command Line*	Fungsi
1		● Tampilan email spoof di *Thunderbird*	● Menampilkan subjek, pengirim palsu, dan isi email *spoofing*.
2		● Tampilan detail *header email*	● Analisis terhadap field *Received*, *From*, *Return-Path*, dan *Message-ID* untuk mengidentifikasi ketidaksesuaian identitas.
3		● Analisis *Follow TCP Stream* di *Wireshark* dan ekstraksi metadata SMTP	● Menelusuri jalur pengiriman email berdasarkan informasi *header* (routing trace). ● Menampilkan struktur MIME dan metadata mentah email.

Tahap Analisis

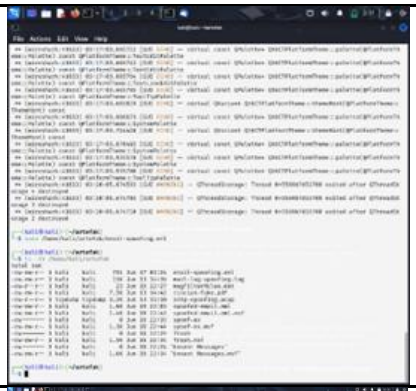
Analisis difokuskan pada pengolahan dan interpretasi artefak digital menggunakan *Wireshark*, *tcpdump*, dan *Thunderbird*. Beberapa temuan visual dirangkum sebagai berikut:

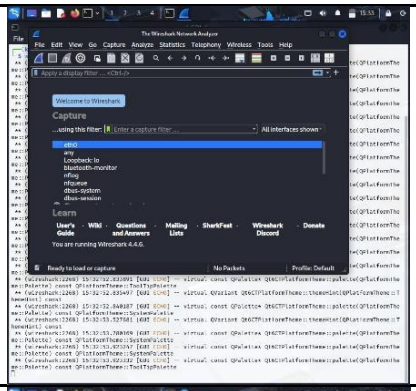
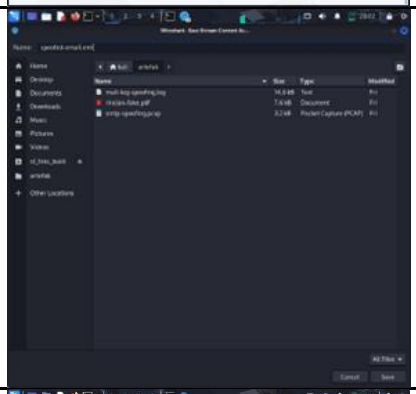
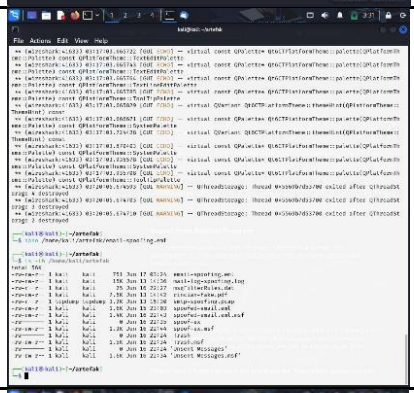
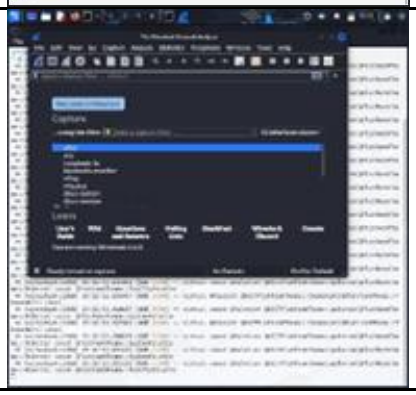
Tabel 4. Visualisasi Analisis SMTP

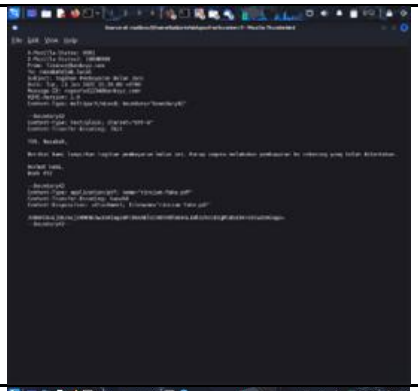
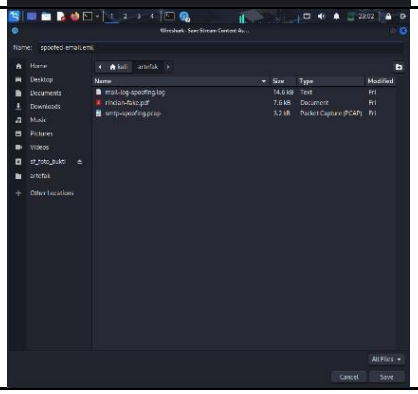
No	Screenshot Terminal	*Command Line*	Fungsi
1			● Proses capture trafik SMTP menggunakan *tcpdump* dan pengiriman *email spoof* menggunakan *Sendmail*.
2			● File *smtp-spoofing.pcap* dibuka dengan *Wireshark*.

Tahap Pelaporan (*Reporting*)

Tabel 5. Rekap Pelaporan Tahapan NIJ

Tahap NIJ	Screenshot Terminal	Fungsi
Identification		Struktur direktori artefak
Collection		Perintah *spoofing* di terminal
		Bukti bahwa proses ditangkap untuk forensik.

		Visualisasi trafik SMTP saat pengiriman *email spoof* berlangsung.
		• File hasil tangkapan trafik SMTP menggunakan tcpdump. • Email spoof hasil tangkapan dari Wireshark.
Examination		Isi file *.eml* dibuka dengan *nano* (analisis header awal).
		Tampilan *Follow TCP Stream* dari *Wireshark*

Analysis		Header lengkap *email spoof* dilihat di Thunderbird.
		Log SMTP saat *spoofing* dilakukan, berisi proses *relay*.

Laporan forensik disusun berdasarkan tahapan investigasi sebagai berikut:

Laporan Analisis Forensik Email Spoofing

Tanggal : 15 June 2025

Nama Peneliti : Rokhmatun Nazila

Instansi/Laboratorium : Universitas Ma'arif Nahdlatul Ulama Kebumen

a) Identitas Kasus

Kasus ini merupakan simulasi pengiriman *email spoofing* yang ditujukan kepada target dalam jaringan internal. Pengiriman dilakukan dengan memanfaatkan protokol SMTP lokal, menggunakan perangkat lunak *Sendmail* dan *SWAKS*, serta proses pemantauan dijalankan melalui *tcpdump* dan *Wireshark*. Tujuannya adalah untuk mereplikasi skenario serangan *email spoofing* secara realistis dan menganalisis potensi kelemahan sistem email internal dalam menangani ancaman tersebut.

b) Perangkat yang Digunakan

Dalam proses simulasi dan investigasi, digunakan beberapa perangkat utama. *Postfix* berperan sebagai server SMTP penerima email. *Sendmail* digunakan untuk mengirim email dengan alamat pengirim yang dipalsukan. *SWAKS* dimanfaatkan untuk melakukan pengujian protokol SMTP secara terkontrol. Sementara itu, *tcpdump* merekam lalu lintas SMTP, dan *Wireshark* digunakan untuk membuka serta menganalisis isi file *.pcap*.

Sebagai klien email, *Mozilla Thunderbird* dipakai untuk menampilkan isi email *spoofing* beserta *header*-nya guna mendukung proses analisis forensik.

c) Deskripsi Kasus

Pengujian dilakukan dengan mengirim *email spoof* yang menggunakan identitas palsu berupa alamat finance@bankxyz.com. Email tersebut memiliki subjek penagihan palsu dan dikirimkan ke alamat target dalam jaringan internal. Hasilnya menunjukkan bahwa email berhasil diterima oleh klien *Thunderbird* dan seluruh proses komunikasi terekam dalam file *.pcap* serta log server *Postfix*, yang kemudian dianalisis pada tahap selanjutnya.

d) Data yang Dikumpulkan

Beberapa data artefak digital dikumpulkan dari simulasi ini, di antaranya adalah file *.eml* yang memuat isi serta *header* dari email *spoofing*, file *.pcap* hasil rekaman aktivitas SMTP yang diperoleh melalui *tcpdump*, dan log *Postfix* yang mencatat seluruh aktivitas pengiriman serta penerimaan email selama simulasi berlangsung.

e) Analisis Header

Berdasarkan hasil pemeriksaan terhadap file *.eml*, ditemukan bahwa nilai pada *Return-Path*, *From*, dan *Received* menunjukkan ketidaksesuaian asal pengiriman email. Ketidaksesuaian ini mengindikasikan bahwa alamat pengirim telah dipalsukan. Selain itu, alamat IP pengirim juga diketahui berasal dari *host* lokal, bukan dari *mail server* resmi, yang semakin menguatkan bukti terjadinya *email spoofing*.

f) Hasil Analisis SMTP

Analisis terhadap file *.pcap* menggunakan *Wireshark* memperlihatkan alur komunikasi SMTP yang tidak valid. Ditemukan bahwa perintah HELO/EHLO dan DATA berasal dari sumber yang tidak terverifikasi, menunjukkan proses pengiriman dilakukan oleh entitas yang tidak memiliki otorisasi resmi. Proses *spoofing* ini terekam sepenuhnya dalam *Wireshark* dan *tcpdump*, yang memberikan gambaran detail mengenai metode yang digunakan pelaku untuk menyusupkan email palsu.

g) Kesimpulan

Berdasarkan seluruh proses simulasi dan analisis yang telah dilakukan, dapat disimpulkan bahwa teknik *email spoofing* dapat dilakukan dengan sangat mudah dalam jaringan internal, terutama jika sistem tidak dilengkapi dengan lapisan keamanan tambahan. Tanpa proteksi seperti SPF, DKIM, dan DMARC, sistem email menjadi sangat rentan terhadap penyamaran identitas pengirim dan potensi penyebaran konten berbahaya melalui email.

h) Rekomendasi

Untuk meningkatkan keamanan sistem email, disarankan agar administrator mengaktifkan dan mengonfigurasi protokol autentikasi seperti SPF, DKIM, dan DMARC. Selain itu, diperlukan penerapan filter terhadap lampiran PDF yang mencurigakan, serta pemantauan log *Postfix* secara berkala guna mendeteksi anomali dalam aktivitas pengiriman email yang dapat mengindikasikan adanya upaya *spoofing*.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa *email spoofing* dapat dilakukan dalam jaringan internal menggunakan alat seperti *Sendmail* dan *SWAKS* tanpa autentikasi, sehingga rawan dimanfaatkan untuk menyamarkan identitas pengirim. Proses investigasi forensik berbasis metode NIJ berhasil diterapkan pada seluruh tahap, menghasilkan artefak penting seperti file *.eml*, *.pcap*, log SMTP, dan lampiran spoof. Analisis menunjukkan ketidaksesuaian antara alamat pengirim dengan jalur pengiriman serta ketiadaan proteksi autentikasi seperti SPF, DKIM, dan DMARC, yang memungkinkan *spoofing* terjadi. Proses perekaman SMTP dengan *tcpdump* dan *Wireshark* berjalan efektif, sementara *Thunderbird* mempermudah analisis struktur *email*. Temuan ini menegaskan perlunya penguatan konfigurasi keamanan dan pemantauan log SMTP guna mendeteksi *spoofing* secara lebih dini.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Bapak Fahmi Fachri selaku dosen pembimbing atas bimbingan, waktu, dan dukungan yang telah diberikan selama proses penelitian ini. Arahan Bapak sangat membantu dan memberi banyak pelajaran berharga dalam perjalanan studi ini. Terima kasih juga saya sampaikan kepada keluarga dan teman-teman yang selalu hadir dengan doa dan semangat. Dukungan kalian menjadi bagian penting dari penyelesaian penelitian ini.

DAFTAR REFERENSI

Anabelle, Z. D., Lamada, M., Zain, S. G., Komputer, T., Makassar, U. N., & Kunci, K. (2024). Investigasi forensik email dengan berbagai pendekatan dan tools. *Jurnal Teknologi Komputer*, *2*(September), 78–89.

Angelone, M. D., & Monaghan, M. (2022). Email spoofing defence techniques: A comprehensive review and development of a novel measurement tool [Tesis, University of Liverpool].

Anwar, N., Widodo, A. M., Sekti, B. A., Ulum, M. B., Rahaman, M., & Ariessanti, H. D. (2024). Comparative analysis of NIJ and NIST methods for microSD investigations: A technopreneur approach. *Aptisi Transactions on Technopreneurship (ATT)*, *6*(2), 169–181. https://doi.org/10.34306/att.v6i2.407

Aryasatya, M. A., & Wibawa, A. (2022). Dampak perkembangan teknologi pada era society 5.0 terhadap lapangan pekerjaan. *Jurnal Inovasi Teknologi dan Edukasi Teknik*, *2*(3), 108–112. https://doi.org/10.17977/um068v2i32022p108-112

Ath-thaariq, M. R., Nurnawati, E. K., & Ariyana, R. Y. (2023). Perancangan otentikasi one time password menggunakan kode unik via email. *Jurnal Keamanan Siber*, *12*(1), 70–78.

Bachri, C. M., & Gunawan, W. (2024). Deteksi email spam menggunakan algoritma convolutional neural network (CNN). *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, *10*(1), 88–94.

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-01560-x

DataReportal. (2025). Global digital insights. https://www.datareportal.com

Haeruddin, H. (2024). Sistem pengendali alat elektronik rumah tangga berbasis Internet of Things (IoT) menggunakan voice recognition. *Journal of System and Computer Engineering (JSCE)*, *5*(1), 56–65. https://doi.org/10.61628/jsce.v5i1.1063

Ihekweazu, E. (2025). Digital forensics in action: A case study of tracing cybercriminals behind job offer spear phishing scams in academic institutions. https://www.cybercrimejournal.org

Liu, E., Akiwate, G., Jonker, M., Mirian, A., Ho, G., Voelker, G. M., & Savage, S. (2023). Forward pass: On the security implications of email forwarding mechanism and policy. *Proceedings - 8th IEEE European Symposium on Security and Privacy (Euro S&P 2023)*, 373–391. https://doi.org/10.1109/EuroSP57164.2023.00030

Marcellino, S., Seta, H. B., & Widi, I. W. (2023). Analisis forensik digital recovery data smartphone pada kasus penghapusan berkas menggunakan metode National Institute of Justice (NIJ). *Informatik: Jurnal Ilmu Komputer*, *19*(2), 141–156. https://doi.org/10.52958/iftk.v19i2.4676

Maulana, M. (2023). Klasifikasi serangan jaringan menggunakan support vector machine untuk investigasi forensik jaringan.

Meshram, B. B., Mendhe, V., & Singh, M. K. (2024). Tracing the invisible threads: A deep dive into email security & forensics. *Cybersecurity Journal*, January.

Neha, K. V., John, J. A., & Sajan, V. (2025). Enhancing email forensic analysis with deep learning and semantic techniques: A literature review. *International Journal of Forensic Computing*, 89–94.

Pemikiran, J., Ilmiah, M., Agribisnis, B., Di, K., & Pt, A. (2023). The influence of marketing mix on consumer purchasing decisions in the PT XYZ. *Mimbar Agribisnis*, *9*(2), 2279–2293.

Prabakaran, M. K., Meenakshi Sundaram, P., & Chandrasekar, A. D. (2023). An enhanced deep learning-based phishing detection mechanism to effectively identify malicious URLs using variational autoencoders. *IET Information Security*, *17*(3), 423–440. https://doi.org/10.1049/ise2.12106

Prado, P. V., Arechiga, C., Marson, K., Oviedo, Y., Vizcaíno, T., Gomez, M., Alvarez, A., Jimenez-Diecks, L., Guevara, S., Nava, A., Lopez, Z., Carrera, O., Hypes, R., Marquez, C., & Chamie, G. (2024). Indications of digital literacy during Latino-focused, community-based COVID-19 testing implementation. *JAMIA Open*, *7*(4). https://doi.org/10.1093/jamiaopen/ooae115

Rahma, Z., & Riadi, I. (2022). Email forensic from phishing attack using network forensics development life cycle method. *International Journal of Computer Applications*, *183*(46), 36–42. https://doi.org/10.5120/ijca2022921865

Rusydi, R., Hendrik, B., & Amri, Y. (n.d.). Forensik digital pengiriman e-mail spam terhadap keamanan cyber di Indonesia. *Jurnal Keamanan Siber*, *18*(2), 9–15.

Saputra, E., & Misinem. (n.d.). Investigation digital forensic terhadap serangan email spoofing pada PT KAI DIVRE III. *Jurnal Forensik Digital*, 1–10.

Saskara, G. A. J., Edy Listartha, I. M., Dharma Putra, I. P. S., & Arijaya Kusuma, K. A. (2024). Evaluasi kualitas jaringan Undiksha Harmoni dengan menggunakan metode quality of service. *Jurnal Teknologi dan Informasi*, *14*(1), 50–61. https://doi.org/10.34010/jati.v14i1.11993

The Internet Crime Complaint Center. (2024). Federal Bureau of Investigation Internet Crime Report, 2024. https://www.ic3.gov/

Widodo, T., & Aji, A. S. (2022). Pemanfaatan network forensic investigation framework untuk mengidentifikasi serangan jaringan melalui intrusion detection system (IDS). *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(1), 46–55. https://doi.org/10.14421/jiska.2022.7.1.46-55

Wintolo, H., Riadi, I., & Yudhana, A. (2025). Analisis deteksi penyusup pada layanan Open Journal System menggunakan metode Network Forensic Development Life Cycle. *Jurnal Forensik Jaringan*, *8*, 133–144.