E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024

Investigasi Forensik Email dengan Berbagai Pendekatan dan Tools

[1*]Zefanya Deianera Anabelle, [2]Mustari Lamada, [3]Satria Gunawan Zain,

[1,2,3]Teknik Komputer, Universitas Negeri Makassar

E-mail:fanyanabelle@gmail.com[1], mustarilamada@unm.ac.id[2], satria.gunawan.zain@unm.ac.id[3]

*Corresponding author: Zefanya Deianera Anabelle

Received : 10 Juli 2024
Accepted : 9 Agustus 2024
Published : 1 September 2024

ABSTRAK

Penelitian ini bertujuan untuk menyelidiki dan menganalisis kejahatan digital melalui pendekatan forensik email dengan memanfaatkan berbagai metode dan alat bantu. Keberlanjutan teknologi informasi telah meningkatkan risiko kejahatan digital, termasuk serangan melalui email yang dapat menyebabkan kebocoran data, pencurian informasi sensitif, dan ancaman keamanan lainnya. Oleh karena itu, penelitian ini fokus pada pengembangan strategi forensik email yang efektif untuk mengungkap jejak digital dan mengidentifikasi pelaku kejahatan. Metodologi penelitian melibatkan penggunaan berbagai pendekatan, seperti analisis metadata email, pemulihan data yang dihapus, dan rekonstruksi rantai bukti digital. Berbagai tools forensik digital seperti Mxtoolbox, Whatisipaddress, FTK Imager dan Autopsy akan digunakan untuk mendukung proses investigasi. Selain itu, penelitian ini juga mencakup studi kasus untuk mengilustrasikan penerapan pendekatan dan tools tersebut dalam skenario kejahatan digital yang nyata. Hasil penelitian ini diharapkan dapat meningkatkan pemahaman tentang metode forensik email yang efektif dan membantu para profesional keamanan informasi dalam memerangi kejahatan digital. Implikasi praktis dari penelitian ini mencakup penyusunan pedoman forensik email yang dapat digunakan oleh penyidik digital dan penegak hukum untuk meningkatkan keberhasilan investigasi kejahatan berbasis email. Dengan demikian, penelitian ini memberikan kontribusi positif terhadap pengembangan strategi keamanan informasi yang lebih baik di era digital saat ini.

Kata Kunci: ***forensik email, kejahatan digital, pendekatan dan tools***

ABSTRACT

This research aims to investigate and analyze digital crime through an email forensics approach by utilizing various methods and tools. The continuation of information technology has increased the risk of digital crime, including attacks via email that can lead to data leaks, theft of sensitive information, and other security threats. Therefore, this research focuses on developing an effective email forensics strategy to uncover digital traces and identify criminals. The research methodology involves the use of various approaches, such as email metadata analysis, recovery of deleted data, and reconstruction of digital chains of evidence.Various digital forensic tools such as Mxtoolbox, Whatisipaddress, FTK Imager dan Autopsy will be used to support the investigation process. In addition, this research also includes case studies to illustrate the application of these approachesand tools in real digital crime scenarios. It is hoped that the results of this researchwill increase

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024

understanding of effective email.forensic methods and assist information security professionals in fighting digital crime. The practical implications of this research include the development of email forensics guidelinesthat can be used by digital investigators and law enforcement to increase the success of email-based crime investigations. Thus, this research makes a positive contribution to the development of better information security strategies in the current digital era.

Keywords**: **email forensics, digital crime, approaches and tools

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024

1. PENDAHULUAN

Internet memberikan akses cepat dan mudah ke berbagai informasi, berperan dalam peningkatan pengetahuan dan wawasan. Komputer forensik, atau forensik digital, adalah cabang ilmu forensik yang berfokus pada pengumpulan dan analisis bukti digital yang relevan dalam kasus hukum. Berbeda dengan forensik tradisional, komputer forensik melibatkan analisis data dari berbagai sumber daya komputer, termasuk jaringan, jalur komunikasi, dan media penyimpanan. Forensik digital menjadi semakin penting dalam investigasi kejahatan siber (cyber crime), terutama dalam memastikan keaslian barang bukti digital.

Secara umum digital forensik adalah sebuah teknik yang dilakukan untuk menjelaskan keadaan artefak digital terkini. Artefak digital dapat mencangkup sistem komputer, media penyimpanan (seperti harddisk atau CD-ROM), dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket – paket yang secara berurutan bergerak dalam sebuah jaringan. Bidang IT forensik juga memiliki cabang – cabang di dalamnya seperti firewall forensik, forensik jaringan, database forensik, dan forensik perangkat mobile. Di dalam kasus hukum, teknik digital forensik sering digunakan untuk meneliti sistem komputer milik terdakwa (dalam perkara pidana) atau tergugat (dalam perkara perdata). Memulihkan data di dalam suatu hardware atau software yang mengalami kegagalan/kerusakan, Meneliti suatu sistem komputer setelah suatu pembongkaran/pembobolan. Salah satu contohnya adalah untuk menentukan bagaimana penyerang memperoleh akses dan serangan apa yang akan dilakukan, atau memperoleh informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, serta optimisasi kinerja.

Investigasi forensik email merupakan proses yang sangat penting dalam mengungkapkan kegiatan kriminal atau pelanggaran hukum yang dilakukan melalui email (Alim et al., 2021). Email menjadi salah satu bentuk komunikasi elektronik yang paling umum digunakan dalam bisnis dan aktivitas pribadi, sehingga banyak bukti kriminal atau pelanggaran hukum yang terkait dengan email. Proses investigasi forensik email melibatkan pengumpulan, analisis, dan interpretasi data digital yang terkait dengan email (Alim et al., 2021). Ini meliputi pencarian bukti dalam email, analisis metadata email, dan pemulihan email yang dihapus atau terhapus secara tidak sengaja. Tujuannya adalah untuk menemukan bukti yang dapat digunakan dalam persidangan untuk memperkuat tuntutan hukum.

Email forensics dilakukan karena banyaknya pengguna email yang menjadikannya sebagai media untuk melakukan tindakan kejahatan atau ilegal dengan tujuan beragam salah satunya menyadap atau mengintip email orang lain untuk mendapatkan informasi yang dianggap penting untuk keuntungan pribadi. Tujuan email forensics adalah untuk menemukan bukti dari permasalahan yang ada. Email forensics itu sendiri merupakan proses ilmiah yang melibatkan persiapan investigasi dan forensika terhadap sebuah email terkait adanya kasus hukum untuk menemukan bukti dari permasalahan dan membuktikan kebenaran dari hasil temuan tersebut berdasarkan prosedur hukum yang berlaku.

Dalam konteks kejahatan siber, tindakan kriminal dapat terjadi di dunia maya dan sering kali melibatkan teknologi komputer secara eksklusif. Contoh kasus seperti serangan pada situs KPU tahun 2004 dan peretasan situs Tiket.com menunjukkan betapa seriusnya ancaman kejahatan siber terhadap individu, perusahaan, dan instansi pemerintah. Investigasi forensik email adalah salah satu metode untuk menangani tantangan ini, dengan tujuan mengidentifikasi, menganalisis, dan memulihkan informasi yang terkait dengan aktivitas ilegal.

Pada tahun 2018, sebuah penelitian oleh Karya et al. mengeksplorasi pendekatan forensik yang efektif untuk memulihkan email yang terhapus pada sistem Windows. Penelitian ini menggunakan metode kualitatif dengan melakukan wawancara dengan para ahli forensik dan percobaan pada sistem Windows untuk mengidentifikasi dan memulihkan email yang terhapus. Hasil dari penelitian ini menunjukkan bahwa kombinasi antara teknik carving, sistem pengindeksan, dan program recovery dapat efektif dalam memulihkan email yang terhapus pada sistem Windows. Penelitian lainnya yang relevan adalah penelitian oleh Chen et al. pada tahun 2020 yang mencoba untuk memperbaiki ketidakakuratan data metadata email.

Penelitian ini menggunakan teknik machine learning untuk memperbaiki keakuratan data metadata email dan melakukan evaluasi terhadap efektivitas teknik yang digunakan. Hasil dari penelitian ini menunjukkan bahwa teknik machine learning dapat meningkatkan keakuratan data metadata email dan dapat diintegrasikan dengan tools forensik untuk membantu analisis email.

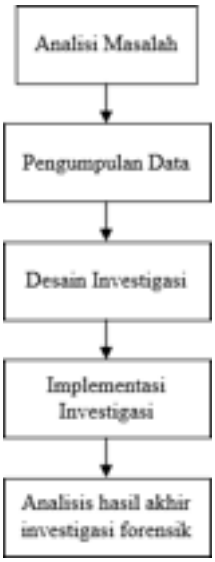
Selain itu, penelitian oleh Shrivastava et al. pada tahun 2019 mencoba untuk mengidentifikasi aktivitas yang mencurigakan pada email dengan menggunakan teknik machine learning. Penelitian ini menggunakan dataset email dan melakukan analisis untuk mengidentifikasi pola-pola aktivitas yang mencurigakan. Hasil dari penelitian ini menunjukkan bahwa teknik machine learning dapat efektif dalam mengidentifikasi aktivitas yang mencurigakan pada email dan dapat membantu ahli forensik dalam melakukan analisis email.

Penelitian terakhir yang relevan adalah penelitian oleh Hussain et al. pada tahun 2021 yang mencoba untuk mengembangkan pendekatan forensik yang dapat mendeteksi email palsu. Penelitian ini menggunakan metode kualitatif dengan melakukan wawancara dengan para ahli forensik dan melakukan eksperimen dengan dataset email palsu. Hasil dari penelitian ini menunjukkan bahwa kombinasi antara teknik hashing, analisis header email, dan verifikasi digital dapat efektif dalam mendeteksi email palsu dan dapat membantu para ahli forensik dalam melakukan investigasi email.

Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi berbagai pendekatan dan tools yang digunakan dalam investigasi forensik email, serta untuk mengatasi tantangan yang dihadapi dalam proses tersebut. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan teknologi forensik email dan membantu para ahli forensik bekerja lebih efektif dan efisien.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam "Investigasi Forensik Email dengan Berbagai Pendekatan dan Tools adalah penelitian eksperimental. Penelitian eksperimental adalah suatu cara untuk menemukan hubungan sebab-akibat (kausal) antara dua faktor yang sengaja dimunculkan oleh peneliti dengan cara menghilangkan atau mengesampingkan faktor-faktor intervening lainnya (Arikunto, 2016). Penelitian ini dilakukan secara daring (online) dengan menggunakan tools forensik yang memungkinkan analisis dan pemulihan jarak jauh. Penelitian ini dapat dilakukan dalam waktu yang relatif singkat, tergantung pada kompleksitas kasus yang diteliti.



Gambar 1 Tahapan Penelitian

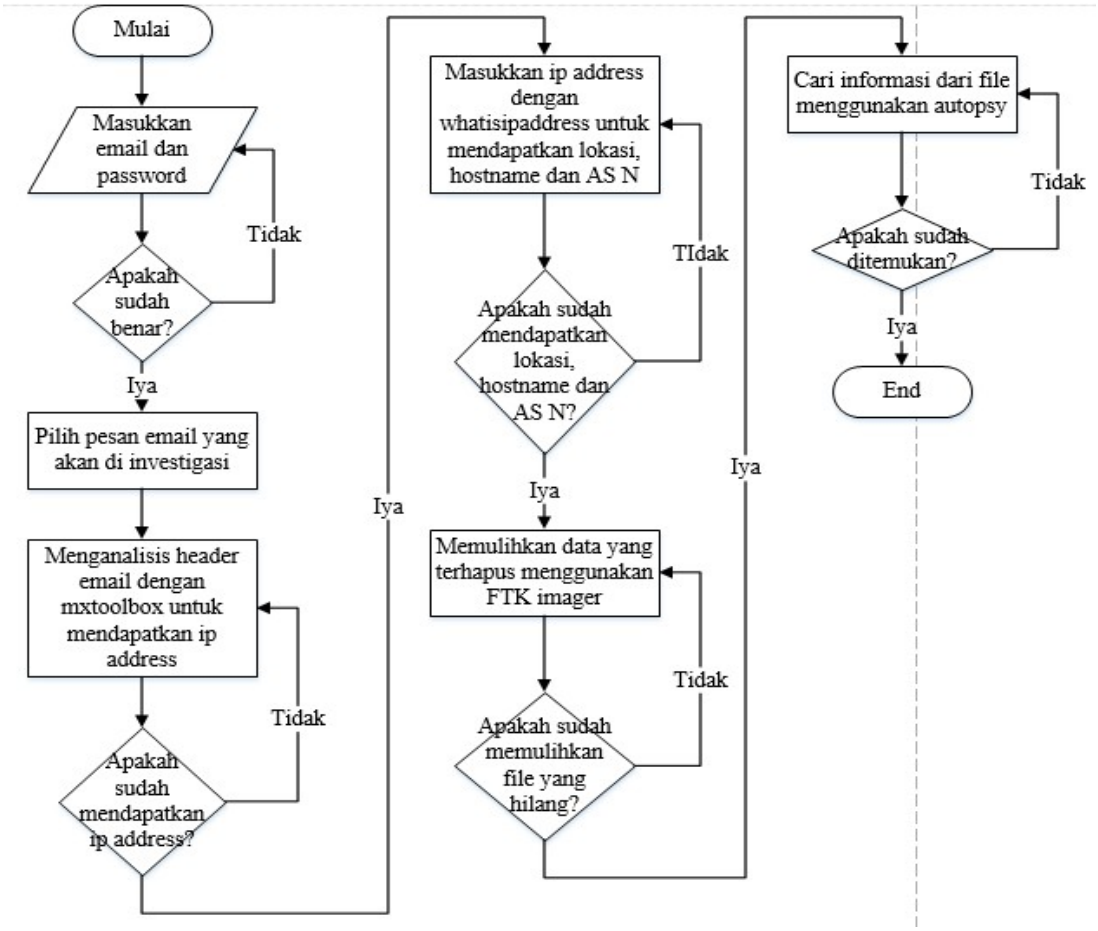
E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024

Langkah-langkah yang dilakukan untuk menyelesaikan penelitian ini dalam Investigasi Forensik Email dengan Berbagai Pendekatan dan Tools. Ada 5 langkah yang digunakan untuk menyelesaikan penelitian ini, seperti yang ditunjukkan pada Gambar 1.

2.1. Implementasi Investigasi

Setelah melakukan analisis masalah, pengumpulan data, dan desain Investigasi, langkah selanjutnya adalah implementasi investigasi forensik. Investigasi forensik adalah penggunaan metode dan teknik ilmiah untuk menganalisis bukti fisik untuk proses hukum pidana dan perdata. Investigasi forensic juga dilakukan untuk mencegah terjadinya penambahan korban akibat pesan yang berisikan virus.



Gambar 2 Flowchart Investigasi Forensic

Agar memperoleh informasi yang menyeluruh dan tepat sesuai dengan fokus penelitian, maka teknik pengumpulan data dalam penelitian ini menggunakan metode observasi. Proses ini bertujuan untuk melihat efektivitas investigasi forensic dalam membedakan email asli dan palsu serta mendapatkan informasi yang tersembunyi dalam file tersebut.

Gambar 2 menunjukkan diagram alir investigasi forensic. Langkah-langkah pengujian mxtoolbox untuk mendapatkan ip address, pengujian whatisipaddress dalam melacak lokasi ip tersebut dan melihat hostname yang digunakan untuk membedakan email asli dan palsu berdasarkan hostname serta mendapatkan AS-N yang digunakan dalam mengidentifikasi jaringan computer. Setelah itu dilakukan pemulihan data yang sempat terhapus menggunakan FTK imager dan setelah data berhasil dipulihkan dapat dilakukan autopsy terkait file yang diduga

E-ISSN: 2986-7258
P-ISSN : 2986-724X
PISCES Volume 02 Nomor 02 September 2024

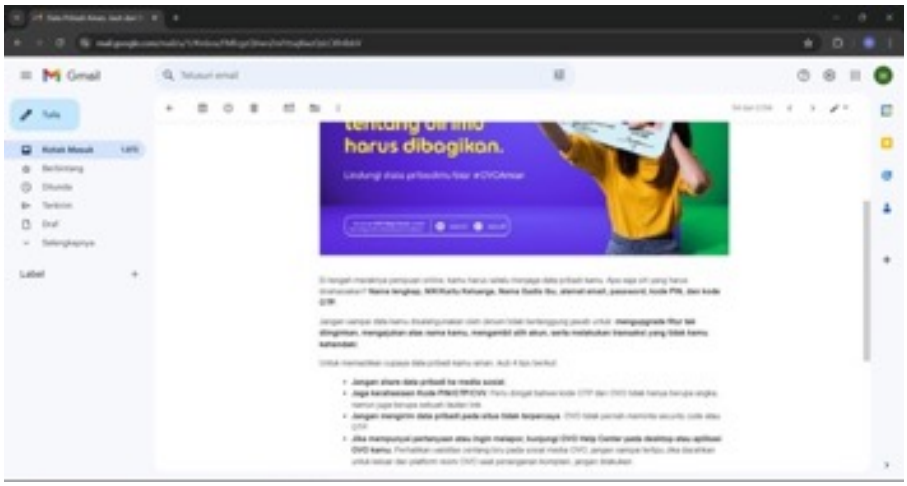
berisikan virus.

3. HASIL DAN PEMBAHASAN

Analisis masalah dilakukan untuk mengetahui penyebab terjadinya masalah dan mencari solusi yang tepat untuk menyelesaikan permasalahan tersebut. Langkah pertama yang dapat dilakukan pada penelitian ini adalah melakukan observasi lapangan. Berdasarkan obersevasi lapangan melalui pengamatan langsung diperoleh hasil bahwa maraknya cyber crime. Hal ini

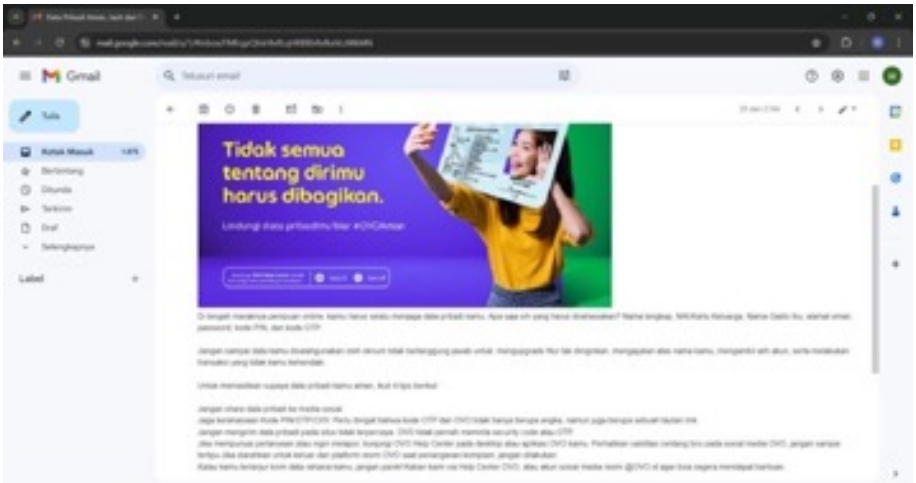
dikarenakan kurang berhati-hatinya user dalam mengunduh file dari pesan email. Oleh karena itu, perlu dilakukan investigasi forensik agar dapat melacak lokasi pelaku dan dapat mengetahui file yang dikirimkan mengandung virus.

Data yang digunakan dalam proses pengumpulan data untuk penelitian berupa isi pesan yang dikirimkan ovo asli dan palsu. Pesan asli ditunjukkan oleh Gambar 4.1.



Gambar 3 Pesan asli ovo

Berdasarkan Gambar 3 merupakan pesan asli dari ovo sedangkan kita akan melihat isi pesan ovo palsu. Pesan palsu ditunjukkan oleh Gambar 4.



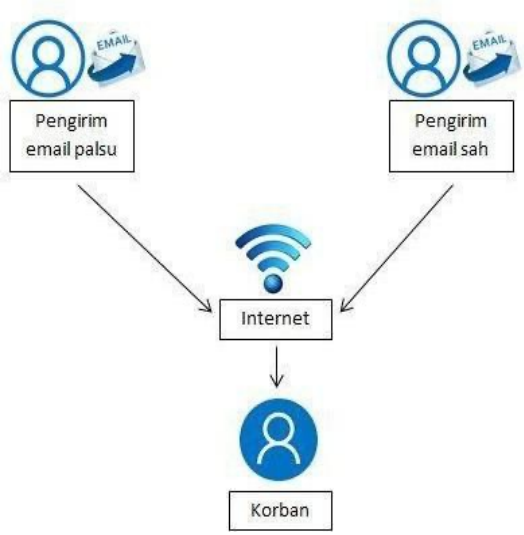
Gambar 4 Pesan palsu ovo

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024

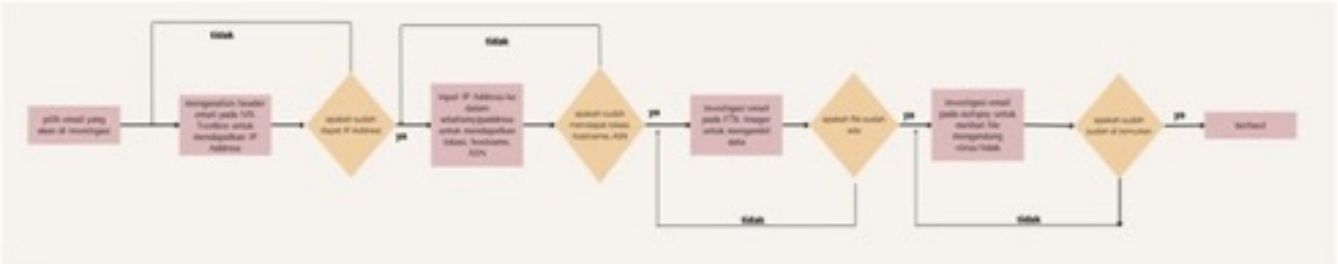
Berdasarkan Gambar 3 dan Gambar 4 dapat kita lihat isi pesan ovo yang asli dan palsu itu sama persis sehingga tak jarang kita tidak mencurigai akan adanya tindak cyber crime.

Desain skenario sistem yang akan digunakan dalam melakukan investigasi forensik email dengan berbagai pendekatan dan tools dapat dilihat pada Gambar 5.



Gambar 5 Skenario sistem

Selain skenario sistem adapun SOP penelitian yang dilakukan yang bertujuan agar penelitian ini mendapatkan hasil yang maksimal dan tearah dengan adanya SOP penelitian ini. SOP penelitian dapat dilihat pada Gambar 6.

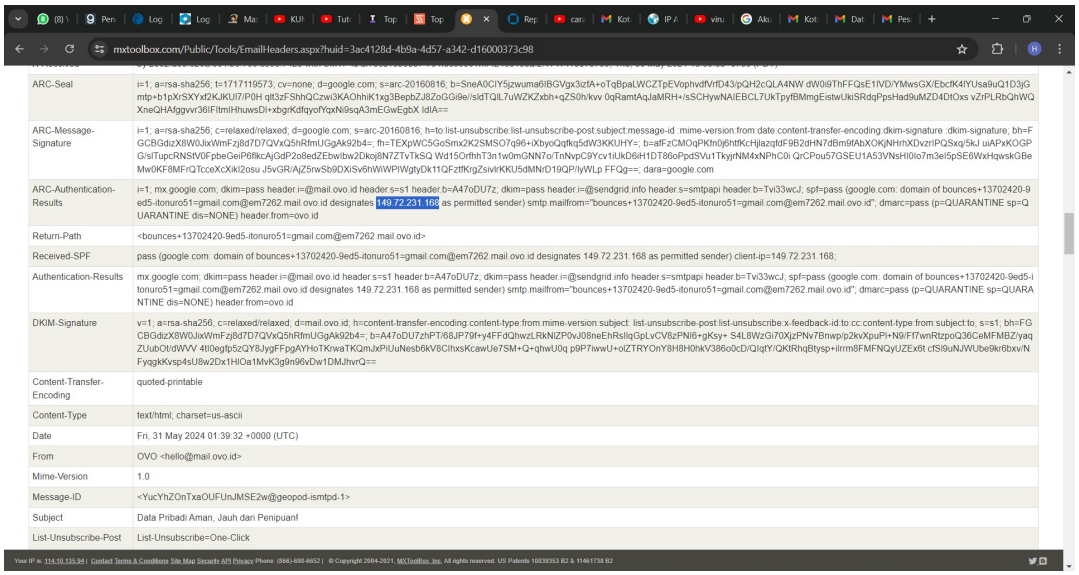


Gambar 6 SOP Penelitian

Pada tahap awal investigasi yaitu mencari ip address berdasarkan hasil analisis header email menggunakan mxtoolbox dapat dilihat pada Gambar 7. dan Gambar 8.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024



ARC-Seal	i=1; a=rsa-sha256; t=1717119573; cv=none; d=google.com; s=arc-20160816; b=SneA0CIY5jzwuma6IBGVgx3izfA+oTqBpaLWCZTpEVophvdfVrfD43/pQH2cQLA4NW dW0i9ThFFQsE1lVD/YMwsGX/EbcfK4lYUsa9uQ1D3jGmtp+b1pXrSXYxf2KJKUI7/P0H qt3zFShhQCzwi3KAOhhiK1xg3BepbZJ8ZoGGi9e/sldTQIL7uWZKZxbh+qZS0h/kvv 0qRamtAqJaMRH+/sSCHywNAIEBCL7UkTpyfBMmgEistwUkiSRdqPpsHad9uMZD4DtOxs vZrPLRbQhWQXneQHAfggvvr36IFItmIHhuwsDI+xbgrKdfqyofYqxNi9sqA3mEGwEgbX IdlA==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=to:list-unsubscribe:list-unsubscribe-post:subject:message-id :mime-version:from:date:content-transfer-encoding:dkim-signature :dkim-signature; bh=FGCBGdizX8W0JixWmFzj8d7D7QVxQ5hRfmUGgAk92b4=; fh=TEXpWC5GoSmx2K2SMSO7q96+iXbyoQqfkq5dW3KKUHY=; b=afFzCMOqPKfn0j6htfKcHjlazqfdF9B2dHN7dBm9fAbXOKjNHrhXDvzrlPQSxq/5kJ uiAPxKOGPG/slTupcRNStV0FpbeGeiP6fIkcAjGdP2o8edZEbwIbw2Dkoj8N7ZTvTkSQ Wd15OrfhhT3n1w0mGNN7o/TnNvpC9Ycv1iUkD6iH1DT86oPpdSVu1TkyjrNM4xNPhC0i QrCPou57GSEU1A53VNsHI0lo7m3eI5pSE6WxHqwskGBeMw0KF8MFrQTceXcXikI2osu J5vGR/AjZ5rwSb9DXiSv6hWiWPIWgtyDk11QFztfKrgZsivlrKKU5dMNrD19QP/lyWLp FFQg==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@mail.ovo.id header.s=s1 header.b=A47oDU7z; dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=Tvi33wcJ; spf=pass (google.com: domain of bounces+13702420-9ed5-itonuro51=gmail.com@em7262.mail.ovo.id designates 149.72.231.168 as permitted sender) smtp.mailfrom="bounces+13702420-9ed5-itonuro51=gmail.com@em7262.mail.ovo.id"; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=ovo.id
Return-Path	<bounces+13702420-9ed5-itonuro51=gmail.com@em7262.mail.ovo.id>
Received-SPF	pass (google.com: domain of bounces+13702420-9ed5-itonuro51=gmail.com@em7262.mail.ovo.id designates 149.72.231.168 as permitted sender) client-ip=149.72.231.168;
Authentication-Results	mx.google.com; dkim=pass header.i=@mail.ovo.id header.s=s1 header.b=A47oDU7z; dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=Tvi33wcJ; spf=pass (google.com: domain of bounces+13702420-9ed5-itonuro51=gmail.com@em7262.mail.ovo.id designates 149.72.231.168 as permitted sender) smtp.mailfrom="bounces+13702420-9ed5-itonuro51=gmail.com@em7262.mail.ovo.id"; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=ovo.id
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=mail.ovo.id; h=content-transfer-encoding:content-type:from:mime-version:subject: list-unsubscribe-post:list-unsubscribe:x-feedback-id:to:cc:content-type:from:subject:to; s=s1; bh=FGCBGdizX8W0JixWmFzj8d7D7QVxQ5hRfmUGgAk92b4=; b=A47oDU7zhPT/68JP79f+y4FFdQhwzLRkNlZP0vJ08neEhRsIlqGpLvCV8zPNl6+gKsy+ S4L8WzGi70XjzPNv7Bnwp/p2kvXpuPI+N9/Ff7wnRtzpoQ36CeMFMBZ/yaqZUubOt/dWVV 4tI0egfp5zQY8JygFFpgAYHoTKrwaTKQmJxPiUuNesb6kV6ClhxsKcawUe7SM+Q+qhwU0q p9P7iwwU+olZTRYOnY8H8H0hkV386o0cD/QlqfY/QKtRhqBtysp+ilrrm8FMFNQyUZEx6t cfSl9uNJWUbe9kr6bxv/NFyqgkKvsp4sU8w2Dx1HlOa1MvK3g9n96vDw1DMJhvrQ==
Content-Transfer-Encoding	quoted-printable
Content-Type	text/html; charset=us-ascii
Date	Fri, 31 May 2024 01:39:32 +0000 (UTC)
From	OVO <hello@mail.ovo.id>
Mime-Version	1.0
Message-ID	<YucYhZOnTxaOUFUnJMSE2w@geopod-ismtpd-1>
Subject	Data Pribadi Aman, Jauh dari Penipuan!
List-Unsubscribe-Post	List-Unsubscribe=One-Click

Gambar 7 IP Address dari hasil analisis header email

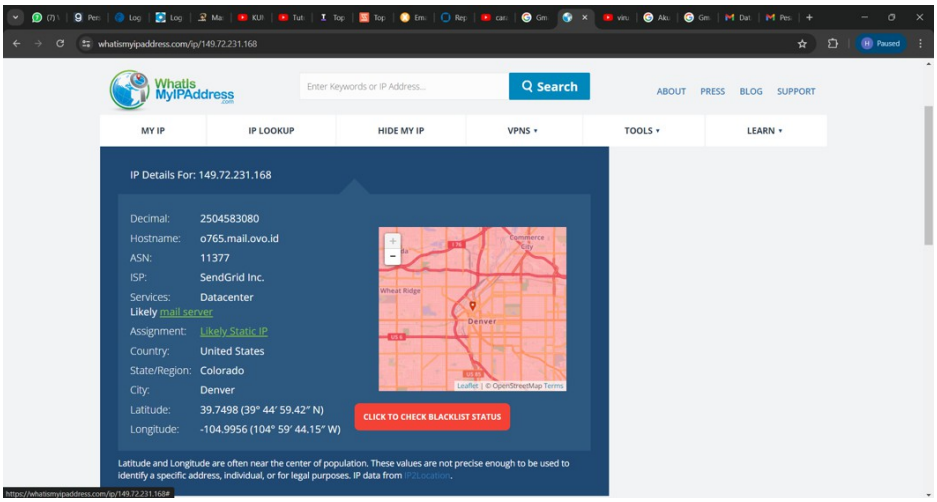
Pada Gambar 7 dan Gambar 8 dilakukan pencarian ip address pada email untuk bisa melacak lokasi ip address tersebut. Tujuan dilakukan pelacakan ip address ini selain bisa melihat lokasi pelaku kita juga bisa mendapatkan hostname dan AS N yang nantinya digunakan untuk menganalisis yang mana email yang asli dan palsu dapat dilihat pada Gambar 9 dan Gambar 10.

Gambar 8 IP Address dari hasil analisis header email

E-ISSN: 2986-7258
P-ISSN : 2986-724X

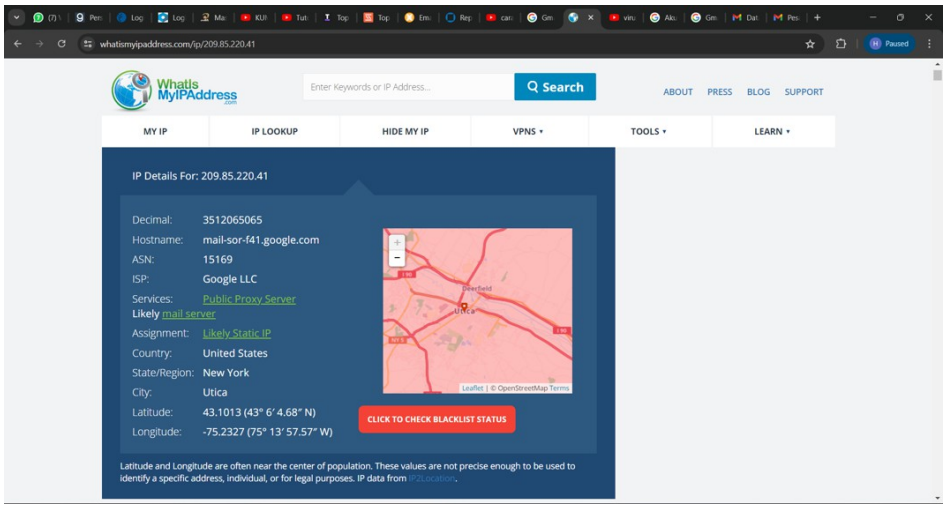
PISCES
Progressive Information, Security, Computer, and Embedded System

PISCES Volume 02 Nomor 02 September 2024



Gambar 9 Hhasil pecalakan ip address

Berdasarkan Gambar 9 dan Gambar 10 dapat dilihat bahwa pada Gambar 9 lokasinya berada di Colorado dan kita bisa melihat untuk hostname yang digunakan itu o765.mail.ovo.id dan AS N 11377 sedangkan pada Gambar 10 dapat dilihat lokasinya berada di New York dan hostname yang digunakan mail-sor-f41.google.com dan AS N 15169 dari hasil penelusuran dapat di pastikan Gambar 9 merupakan email ovo yang asli sedangkan Gambar 10 merupakan email palsu.



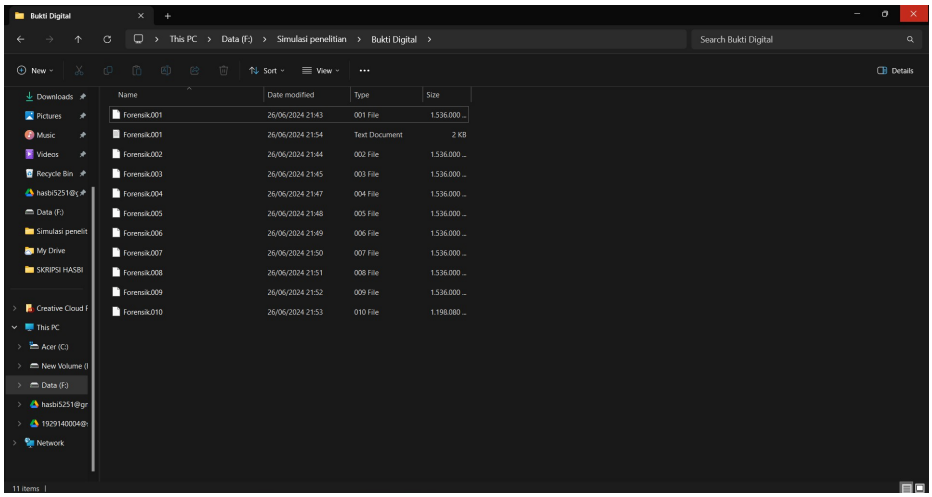
Gambar 10 Hasil pelacakan ip address

Setelah berhasil membedakan antara email asli dan palsu dilanjutkan lagi proses mencari apa yang bersembunyi dibalik gambar yang dikirimkan untuk itu kita gunakan FTK imager untuk mendapatkan file gambar tersebut dapat dilihat pada Gambar 11.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

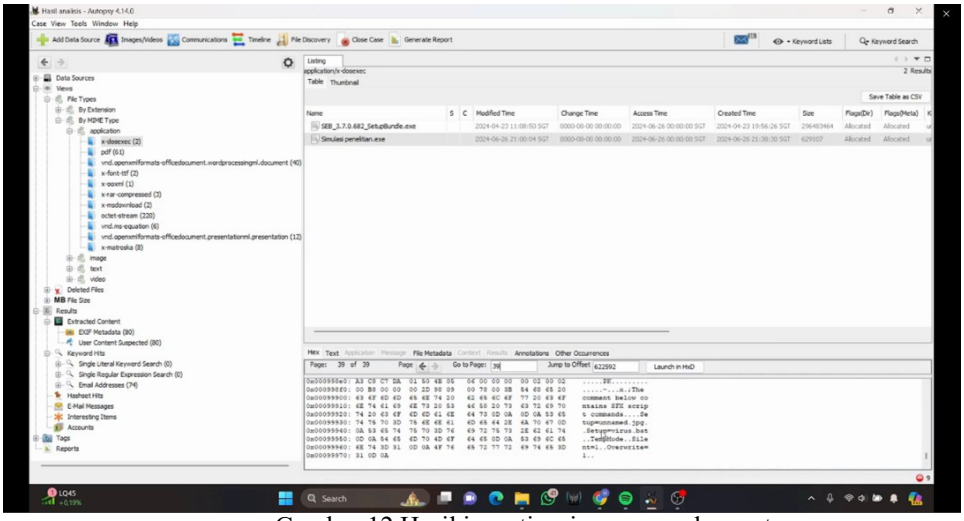
PISCES
Progressive Information, Security, Computer, and Embedded System

PISCES Volume 02 Nomor 02 September 2024



Gambar 11 Hasil pemulihan data menggunakan FTK imager

Pada Gambr 11 pemulihan data berhasil dilakukan, selanjutnya dilakukan investigasi untuk mencari informasi apa yang tersebunyi dibalik file tersebut dapat dilihat pada Gambar 12.



Gambar 12 Hasil investigasi menggunakan autopsy

Pada Gambar 4.10 ditemukan bahwa dalam file bernama “Simulasi Penelitian” ditemukan file tersembunyi bernama “virus.bat” hal inilah yang menyebab laptop korban mengalami shutdown setelah membuka gambar dikirimkan dari email ovo palsu tersebut dan kita juga menemukan bahwa file yang bernama “Simulasi Penelitian” menggunakan format .exe bukan menggunakan format JPEG ataupun PNG.

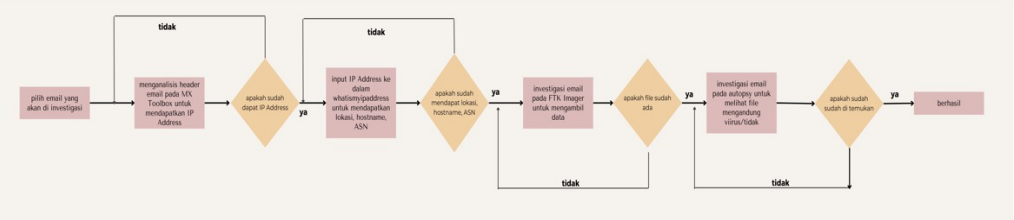
4.5. Analisis Hasil Akhir Investigasi Forensik

Banyaknya kasus cybercrime pada era digital saat ini, seperti pada email. Berdasarkan penelitian investigasi terhadap email ini dapat diketahui adanya kesamaan dan kemiripan antara email asli dan email palsu dari tata letak, logo, gambar hingga isi email. Dengan kemiripan dan kesamaan tersebut secara detail dapat mengelabuhi orang yang menyebabkan kerugian karena email tersebut bisa mengandung malware. Perlunya untuk melakukan investigasi forensik terhadap email yang dicurigai sehingga dapat meminimalisir adanya cybercrime yang terjadi.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024

Berdasarkan hasil pengujian yang telah dilakukan didapatkan hasil bahwa penggunaan tools mxtoolbox, whatisipaddress, FTK imager dan autopsy tidak dapat dilakukan secara terpisah karena setiap tools yang digunakan mempunyai fungsinya tersendiri dan saling melengkapi.



Gambar 12 SOP Penelitian

Adapun SOP penelitian yang digunakan untuk memperoleh hasil yang diinginkan. Dalam penggunaan SOP penelitian data yang dihasilkan sangat membantu dalam proses investigasi, seperti terdapat pada SOP yang menggunakan MX Toolbox untuk menganalisis header email seperti adanya informasi DKIM (DomainKeys Identified Mail) yaitu protokol penanda untuk memverifikasi, relay informasi yang berisi kecepatan pengirim ke email tujuan dan IP Address. IP Address yang digunakan untuk melakukan investigasi lanjutan, dengan IP Address dapat mencakup keseluruhan kebutuhan proses investigasi. Setelah itu penggunaan tools whatismyipaddress untuk mendapatkan lokasi, hostname dan ASN, dengan input IP Address. Dengan tools ini kita mendapatkan lokasi pusat seperti negara dan kota tersebut. Dengan tools ini mendapatkan hostname yang merupakan nama yang diberikan untuk mengidentifikasi sebuah perangkat dalam jaringan komputer, serta AS Number merupakan nomor yang digunakan dalam mengidentifikasi jaringan komputer. Setelah itu penggunaan tools FTK Imager untuk mengambil file yang terdapat pada flashdisk untuk kompres agar dapat melakukan investigasi menggunakan tools autopsy lebih memudahkan proses scan dalam tools autopsy. Setelah itu menggunakan tools autopsy untuk melihat isi file yang diduga mengandung malware. Pilih file yang dicurigai setelah itu mendapatkan informasi pada hex dan melakukan investigasi pada page 1-39 untuk mencari virus. Pada page 39 terdapat informasi pada file tersebut terdapat format PNG dan “setupvirus.bat” dan dapat dicurigai “setupvirus.bat” merupakan file yang mengandung malware. Dari hasil investigasi forensik terhadap email, menghasilkan SOP penelitian yang mengharuskan melakukan investigasi menggunakan kolaborasi antara MxToolbox, WhatIsMyIPAddress, FTK Imager dan Autopsy karena dengan mengkolaborasiakan keempat tools forensik tersebut terbukti efektif mendapatkan hasil yang maksimal.

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian ini, harapan yang telah dinyatakan dalam "Pendahuluan" akhirnya tercapai, sebagaimana dibuktikan dalam "Hasil dan Pembahasan." Penelitian ini berhasil mengidentifikasi efektivitas kolaborasi antara berbagai tools forensik dalam mendeteksi dan menganalisis serangan siber melalui email. Kesesuaian antara tujuan awal dan hasil penelitian menunjukkan bahwa pendekatan yang digunakan tepat dan sesuai dengan masalah yang dihadapi.

Selain itu, hasil penelitian ini membuka prospek pengembangan lebih lanjut dalam bidang investigasi forensik digital. Aplikasi dari SOP dan tools yang digunakan dapat diperluas ke berbagai jenis serangan siber lainnya, termasuk investigasi pada platform komunikasi digital yang lebih kompleks. Pengembangan lebih lanjut dapat mencakup integrasi tools forensik dengan sistem keamanan siber yang lebih canggih, memungkinkan deteksi dini dan pencegahan serangan siber secara lebih efektif. Prospek kajian berikutnya juga dapat fokus pada peningkatan otomatisasi dalam proses investigasi, serta pengembangan SOP yang lebih adaptif terhadap berbagai jenis ancaman siber yang terus berkembang.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 02 September 2024

REFERENSI

Alim, M., Nuruzzaman, M., & Rahman, M. A. (2021). "Investigating Email Forensics: Methods and Tools." Journal of Digital Forensics, Security and Law, 16(2), 45-56.

Arikunto, S. (2016). Prosedur Penelitian: Suatu Pendekatan Praktik. Jakarta: Rineka Cipta.

Chen, W., Liu, Y., & Zhang, H. (2020). "Improving Email Metadata Accuracy Using Machine Learning Techniques." International Journal of Digital Evidence, 25(3), 112-123.

Hussain, A., Ahmed, S., & Khan, M. (2021). "Developing a Forensic Approach to Detect Fake Emails Using Hashing and Digital Verification." Forensic Science International, 31(1), 67-78.

Karya, D., Hartono, T., & Nugroho, A. (2018). "Recovering Deleted Emails on Windows Systems: A Forensic Approach." Indonesian Journal of Cyber Security, 10(1), 23-34.

Shrivastava, R., Gupta, S., & Patel, A. (2019). "Detecting Suspicious Email Activities Using Machine Learning." Journal of Cyber Crime and Forensics, 22(4), 89-97.