Prosiding Seminar Nasional UNIMUS
Volume 7, 16 Oktober 2024
e-ISSN : 2654-3168 | p-ISSN : 2654-3257

Digital Forensik Untuk Investigasi Pasca Kejadian *Platform* & *Web Security*

Digital Forensics for Post Incident Investigation Platform & Web Security

Muiz Riffai Achmad, Laily Muntasiroh
Universitas Muhammadiyah Semarang, Semarang
Corresponding authors: riffaiachmad5@gmail.com

Abstrak

Penelitian ini berfokus pada investigasi forensik digital untuk menganalisis serangan siber yang terjadi pada jaringan, khususnya serangan Denial of Service (DoS) dan brute force, dengan menggunakan alat analisis seperti Wireshark. Tim investigasi dibagi menjadi beberapa kelompok untuk menangani analisis forensik memori, jaringan, dan penyusunan laporan. Hasil penelitian menunjukkan adanya beberapa serangan DoS, seperti SYN Flood, UDP Flood, dan DNS Amplification, serta bukti satu serangan brute force jenis Hybrid Attack. Namun, selama investigasi tidak ditemukan indikasi adanya aktivitas malware. Kendala yang dihadapi selama proses investigasi antara lain keterbatasan perangkat dan waktu analisis yang menyebabkan hambatan dalam penyelidikan lebih mendalam. Penelitian ini menekankan pentingnya penggunaan alat yang lebih komprehensif dan metodologi yang lebih maju dalam investigasi forensik jaringan untuk memastikan deteksi yang akurat dan lengkap terhadap ancaman siber.
Kata Kunci: Forensik Digital, Serangan DoS, Wireshark

Abstract

This study focuses on digital forensic investigations to analyze cyber attacks that occur on networks, especially Denial of Service (DoS) and brute force attacks, using analysis tools such as Wireshark. The investigation team was divided into several groups to handle forensic analysis of memory, networks, and report preparation. The results of the study showed several DoS attacks, such as SYN Flood, UDP Flood, and DNS Amplification, as well as evidence of one brute force attack of the Hybrid Attack type. However, during the investigation no indication of malware activity was found. Obstacles faced during the investigation process included limited devices and analysis time which caused obstacles in further investigation. This study emphasizes the importance of using more comprehensive tools and more advanced methodologies in network forensic investigations to ensure accurate and complete detection of cyber threats.
***Keywords**: Digital Forensics, DoS Attacks, Wireshark*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam hal komunikasi, bisnis, dan aktivitas sehari-hari lainnya. Internet dan berbagai platform digital telah menjadi bagian integral dari kehidupan modern, memungkinkan pertukaran data secara cepat dan efisien. Namun, di sisi lain, kemajuan teknologi ini juga diikuti oleh ancaman yang semakin kompleks, salah satunya adalah meningkatnya serangan siber yang mengancam keamanan jaringan dan data. Kejahatan siber atau cybercrime tidak hanya merugikan individu, tetapi juga organisasi dan perusahaan yang bergantung pada keamanan data untuk menjaga kelangsungan operasi mereka.

Salah satu bentuk kejahatan siber yang sering terjadi adalah serangan terhadap platform digital dan situs web. Serangan ini dapat melumpuhkan sistem, mencuri informasi sensitif, atau bahkan menyebabkan kerugian finansial yang besar bagi para korbannya. Kejahatan siber ini melibatkan berbagai teknik serangan seperti *Denial of Service* (DoS), *brute force*, penyebaran malware, hingga eksploitasi kelemahan protokol

Prosiding Seminar Nasional UNIMUS
Volume 7, 16 Oktober 2024
e-ISSN : 2654-3168 | p-ISSN : 2654-3257

jaringan. Oleh karena itu, penanganan insiden keamanan siber menjadi semakin penting, terutama dalam hal investigasi pasca-kejadian untuk mengidentifikasi sumber serangan, memahami teknik yang digunakan oleh penyerang, dan mencegah terulangnya kejadian serupa di masa mendatang.

Di sinilah peran digital forensik menjadi krusial. Digital forensik adalah cabang ilmu forensik yang berkaitan dengan pengumpulan, analisis, dan pelaporan bukti digital dari sistem komputer, jaringan, atau perangkat digital lainnya yang terkait dengan insiden kejahatan siber. Dalam konteks keamanan jaringan, digital forensik memainkan peran penting dalam menganalisis aktivitas mencurigakan di jaringan, mengidentifikasi pola serangan, serta memastikan integritas data dan sistem tetap terjaga. Investigasi digital forensik memungkinkan para ahli untuk melacak jejak digital yang ditinggalkan oleh penyerang dan membantu dalam proses hukum jika diperlukan.

Dalam penelitian ini, fokus utama adalah pada investigasi forensik jaringan yang dilakukan pasca-kejadian serangan terhadap sebuah platform digital. Tim investigasi forensik yang terdiri dari tiga bagian, yaitu Tim DFIR (Digital Forensic Incident Response), Tim Forensik Memori, dan Tim Forensik Jaringan, memainkan peran yang berbeda namun saling terkait dalam proses investigasi ini. Tim DFIR bertugas untuk melakukan survei di Tempat Kejadian Perkara (TKP) dan mengumpulkan data awal dari jaringan yang terdampak serangan. Sementara itu, Tim Forensik Jaringan bertanggung jawab untuk menganalisis data yang diperoleh dari TKP menggunakan berbagai alat dan teknik analisis jaringan, seperti Wireshark, untuk mendeteksi aktivitas mencurigakan dalam jaringan.

Penggunaan alat forensik jaringan seperti Wireshark sangat penting dalam investigasi ini. Wireshark adalah salah satu alat analisis jaringan yang paling banyak digunakan oleh para ahli forensik untuk mengamati lalu lintas data yang melewati jaringan dan mendeteksi anomali yang mengindikasikan adanya serangan siber. Dalam konteks penelitian ini, Wireshark digunakan untuk menganalisis serangan DoS (*Denial of Service*) dan *brute force*. Serangan DoS adalah jenis serangan yang bertujuan untuk membuat sebuah layanan atau sumber daya jaringan menjadi tidak tersedia bagi pengguna yang sah dengan cara membanjiri sistem dengan lalu lintas yang sangat besar. Beberapa jenis serangan DoS yang diidentifikasi dalam penelitian ini antara lain SYN *Flood*, UDP *Flood*, ICMP *Flood*, DNS *Amplification*, dan HTTP *Flood*.

Selain serangan DoS, penelitian ini juga menyoroti serangan *brute force*, di mana penyerang mencoba berbagai kombinasi kata sandi atau kunci enkripsi untuk mendapatkan akses yang tidak sah ke sistem atau data. Salah satu temuan dalam investigasi ini adalah adanya serangan *Hybrid Attack*, yang merupakan kombinasi dari dictionary attack dan *brute force* murni. Teknik ini melibatkan penggunaan daftar kata sandi umum yang kemudian dimodifikasi atau ditambah dengan karakter tertentu untuk mencoba berbagai kemungkinan kombinasi kata sandi.

Hasil dari analisis jaringan yang dilakukan oleh Tim Forensik Jaringan menunjukkan adanya bukti kuat tentang berbagai jenis serangan DoS yang dialami oleh jaringan, seperti SYN *Flood* dan UDP *Flood*. Serangan-serangan ini berhasil mengganggu ketersediaan layanan di jaringan yang diserang, meskipun tidak ada bukti signifikan yang mengarah pada penyebaran malware. Selain itu, dalam analisis statistik

Prosiding Seminar Nasional UNIMUS
Volume 7, 16 Oktober 2024
e-ISSN : 2654-3168 | p-ISSN : 2654-3257

jaringan, protokol seperti TCP, UDP, IPv4, dan IPv6 digunakan untuk memantau percakapan dan lalu lintas data yang mencurigakan. Meskipun ditemukan adanya indikasi serangan brute *force*, namun aktivitas terkait malware tidak terdeteksi selama proses investigasi ini.

Salah satu kendala utama yang dihadapi selama proses investigasi adalah keterbatasan perangkat keras. Dalam kasus ini, perangkat yang digunakan untuk analisis jaringan harus dibagi dengan anggota keluarga, yang menyebabkan keterlambatan dalam proses analisis dan pelaporan. Keterbatasan perangkat keras ini menjadi salah satu faktor penghambat dalam investigasi forensik, mengingat analisis jaringan membutuhkan sumber daya yang memadai untuk menangani volume data yang besar dan melakukan analisis yang mendalam.

Penelitian ini memberikan gambaran yang jelas tentang pentingnya forensik jaringan dalam investigasi pasca-kejadian serangan terhadap platform digital. Selain itu, penelitian ini juga menyoroti berbagai teknik serangan yang umum digunakan oleh penyerang siber dan bagaimana serangan tersebut dapat dideteksi menggunakan alat forensik seperti Wireshark. Kendati demikian, penelitian ini juga mengungkapkan tantangan yang dihadapi dalam melakukan investigasi digital, terutama terkait dengan keterbatasan sumber daya dan perangkat keras. Oleh karena itu, penelitian ini tidak hanya berkontribusi pada pemahaman tentang teknik-teknik serangan siber, tetapi juga memberikan rekomendasi tentang pentingnya memperkuat infrastruktur dan sumber daya untuk mendukung proses investigasi forensik yang lebih efektif di masa mendatang.

Dengan semakin kompleksnya ancaman siber, organisasi dan perusahaan harus semakin waspada terhadap risiko keamanan jaringan yang mereka hadapi. Investasi dalam keamanan siber, termasuk pelatihan staf dalam teknik forensik digital dan peningkatan perangkat keras yang diperlukan, adalah langkah penting yang harus diambil untuk melindungi sistem dari serangan siber yang merusak. Digital forensik telah terbukti menjadi alat yang sangat berguna dalam mengidentifikasi, menganalisis, dan mencegah serangan siber, dan penelitian ini menegaskan pentingnya peran forensik dalam upaya tersebut. Di masa depan, diharapkan penelitian lebih lanjut akan dilakukan untuk mengembangkan teknik-teknik baru dalam deteksi dan pencegahan serangan siber, sehingga keamanan platform digital dapat terus ditingkatkan.

METODE PENELTIAN

Metode penelitian yang digunakan dalam studi ini adalah metode kualitatif deskriptif dengan pendekatan studi kasus. Penelitian kualitatif deskriptif dipilih karena fokus utama dari penelitian ini adalah menggambarkan dan menganalisis proses investigasi forensik digital secara mendalam, terutama dalam konteks pasca-kejadian serangan pada platform digital dan keamanan web. Data yang digunakan dalam penelitian ini diperoleh melalui teknik observasi, pengumpulan data digital, serta analisis dari alat-alat forensik jaringan seperti Wireshark. Pendekatan studi kasus digunakan untuk menggali secara rinci mengenai satu insiden spesifik terkait serangan siber, yaitu serangan *Denial of Service* (DoS) dan *brute force*, guna mempelajari pola serangan dan langkah-langkah forensik yang diambil dalam penanganannya.

Prosiding Seminar Nasional UNIMUS
Volume 7, 16 Oktober 2024
e-ISSN : 2654-3168 | p-ISSN : 2654-3257

Proses pengumpulan data melibatkan tiga tim investigasi, yaitu, Tim DFIR (Mengumpulkan data di lapangan), Tim Lab. *Forensik* (Menganalisis *cybercrime* dari data yang diperoleh Tim DFIR), dan Tim Pelaporan (Membuat Laporan Forensik). Untuk proses pengumpulan oleh Tim DFIR itu sudah mencakup capture jaringn, capture memori data *volatiliy* dan *non volatily*. Setiap tim melakukan pengumpulan dan analisis bukti digital dengan cara yang terstruktur, termasuk memantau lalu lintas jaringan, memeriksa jejak serangan, dan mengidentifikasi teknik serangan yang digunakan oleh pelaku. Data yang diperoleh kemudian dianalisis menggunakan teknik analisis data jaringan yang terfokus pada pengidentifikasian serangan, pengolahan log jaringan, dan interpretasi hasil analisis dari protokol jaringan seperti TCP, UDP, IPv4, dan IPv6. Melalui metode ini, penelitian dapat menghasilkan pemahaman yang mendalam mengenai teknik investigasi forensik digital serta memberikan rekomendasi untuk memperkuat keamanan jaringan.

HASIL DAN PEMBAHASAN

1. Proses Identifikasi Serangan Brute Force Dilakukan Menggunakan Wireshark

Proses identifikasi serangan *brute force* menggunakan Wireshark merupakan salah satu metode investigasi yang efektif dalam analisis keamanan jaringan. Serangan brute force adalah jenis serangan di mana penyerang mencoba berbagai kombinasi username dan password secara otomatis untuk mendapatkan akses tidak sah ke suatu sistem. Dalam kasus ini, Wireshark berfungsi sebagai alat utama untuk menangkap dan menganalisis lalu lintas jaringan secara real-time. Dengan fitur-fitur seperti filter protokol, statistik, dan kemampuan untuk melihat paket data secara rinci, Wireshark memungkinkan peneliti untuk mengidentifikasi pola lalu lintas yang mencurigakan yang menunjukkan adanya upaya serangan brute force.

Langkah pertama dalam proses identifikasi adalah melakukan capture terhadap lalu lintas jaringan selama periode waktu tertentu. Wireshark menangkap semua paket data yang masuk dan keluar dari jaringan, termasuk percobaan koneksi dari penyerang ke server target. Paket-paket ini berisi informasi penting, seperti alamat IP sumber, tujuan, protokol yang digunakan, serta data yang dikirimkan. Dalam serangan brute force, aktivitas mencurigakan sering kali melibatkan sejumlah besar percobaan login dalam waktu singkat dari satu alamat IP atau beberapa alamat IP. Oleh karena itu, langkah pertama adalah mengidentifikasi lalu lintas yang mencurigakan dengan melihat pola percobaan login yang berulang kali gagal.

Setelah proses capture dilakukan, langkah selanjutnya adalah menggunakan filter untuk menyaring data yang relevan. Dalam kasus serangan brute force, protokol yang sering kali digunakan adalah FTP, SSH, atau HTTP, tergantung pada layanan yang menjadi target. Untuk menganalisis serangan terhadap layanan FTP, peneliti dapat menggunakan filter seperti tcp.port == 21, yang menyaring semua lalu lintas yang melewati port 21, yang merupakan port standar untuk FTP. Jika serangan diarahkan pada layanan SSH, maka filter yang digunakan adalah tcp.port == 22. Selain itu, jika serangan brute force dilakukan melalui halaman login berbasis web, seperti aplikasi web atau

Prosiding Seminar Nasional UNIMUS
Volume 7, 16 Oktober 2024
e-ISSN : 2654-3168 | p-ISSN : 2654-3257

server HTTP, filter yang relevan adalah http.request.method == "POST", yang memeriksa semua permintaan HTTP POST, sering kali digunakan untuk pengiriman data login ke server.

Dengan filter ini, Wireshark menyajikan hasil yang lebih spesifik dan fokus pada percobaan login. Salah satu ciri khas dari serangan brute force adalah adanya percobaan login yang gagal dalam jumlah besar dalam waktu singkat. Peneliti dapat memeriksa pola ini dengan melihat jumlah paket yang terkait dengan permintaan login dari satu alamat IP atau berbagai alamat IP yang berbeda. Untuk melihat detail ini, Wireshark menyediakan fitur Statistics > Conversations, yang menampilkan daftar semua komunikasi yang terjadi antara alamat IP sumber dan tujuan. Di sini, peneliti dapat melihat jumlah koneksi yang dibuat dari satu IP ke server target, serta apakah ada lonjakan aktivitas dari IP tertentu yang mencurigakan.

Selain itu, dalam serangan *brute force*, biasanya ada variasi kecil dalam data login yang digunakan. Hal ini bisa dilihat pada field push flag di dalam paket TCP, di mana filter tcp.flags.push == 1 dapat digunakan untuk memeriksa paket yang mengandung data login. Jika terdapat variasi kecil pada data yang dikirim dalam banyak percobaan login, hal ini merupakan indikasi adanya serangan brute force.

Selanjutnya, peneliti dapat menggunakan fitur lain dari Wireshark, yaitu Follow TCP Stream, untuk mengikuti aliran data antara penyerang dan server target. Fitur ini memungkinkan peneliti melihat setiap percakapan secara detail, termasuk data login yang dikirim dan respons dari server. Jika peneliti menemukan pola yang menunjukkan banyak percobaan login dengan variasi kecil dalam kata sandi atau username, ini bisa menjadi bukti adanya serangan brute force. Misalnya, jika penyerang menggunakan dictionary attack (bagian dari serangan brute force), mereka akan mencoba kata sandi dari daftar yang sudah disiapkan. Dalam TCP Stream, ini terlihat dari banyaknya percobaan pengiriman kata sandi yang berbeda namun dilakukan oleh satu IP.

Selain menganalisis percakapan antar IP, peneliti juga dapat memeriksa paket-paket yang ditandai sebagai gagal login. Dalam protokol FTP dan SSH, ketika percobaan login gagal, server biasanya mengirimkan respons yang menunjukkan kegagalan autentikasi. Wireshark memungkinkan peneliti untuk melihat paket-paket ini dan menghitung jumlah kegagalan dalam periode waktu tertentu. Semakin banyak kegagalan login dari satu IP, semakin besar kemungkinan bahwa IP tersebut sedang melakukan serangan brute force.

Namun, Wireshark tidak hanya berguna untuk mengidentifikasi serangan yang sedang berlangsung tetapi juga dapat membantu dalam analisis retrospektif. Jika ada laporan adanya pelanggaran keamanan, peneliti dapat membuka kembali file capture dari periode waktu sebelumnya dan menganalisis data tersebut. Dengan menggunakan filter dan fitur yang sama, peneliti dapat memeriksa apakah ada aktivitas mencurigakan yang terlewatkan selama pemantauan pertama. Hal ini sangat berguna dalam skenario di mana serangan brute force berlangsung dalam jangka waktu yang lama dengan upaya yang lebih halus sehingga tidak langsung terlihat.

Prosiding Seminar Nasional UNIMUS
Volume 7, 16 Oktober 2024
e-ISSN : 2654-3168 | p-ISSN : 2654-3257

Dalam proses identifikasi ini, terdapat juga beberapa tantangan. Salah satunya adalah jumlah data yang besar yang dihasilkan oleh Wireshark ketika menangkap lalu lintas jaringan. Dalam lingkungan jaringan yang sibuk, Wireshark bisa menangkap ribuan hingga jutaan paket dalam periode waktu yang singkat. Oleh karena itu, penggunaan filter yang tepat menjadi sangat penting untuk mengurangi kebisingan data dan fokus pada informasi yang relevan. Selain itu, ada kemungkinan bahwa penyerang menggunakan teknik-teknik pengelakan seperti penggunaan alamat IP yang berbeda untuk setiap percobaan login, yang membuat analisis menjadi lebih sulit.

Selain itu, kendala teknis seperti keterbatasan perangkat juga dapat mempengaruhi efektivitas investigasi. Dalam kasus ini, misalnya, peneliti menggunakan perangkat yang juga digunakan oleh orang lain, yang menyebabkan waktu analisis menjadi lebih lama. Meskipun demikian, dengan pemahaman yang mendalam tentang cara kerja Wireshark dan serangan brute force, peneliti tetap dapat mengidentifikasi serangan dengan akurat.

Kesimpulannya, Wireshark adalah alat yang sangat efektif untuk mengidentifikasi serangan brute force melalui analisis lalu lintas jaringan. Dengan menggunakan filter yang tepat, memeriksa percobaan login yang berulang, dan memantau pola lalu lintas, peneliti dapat mengidentifikasi serangan dengan cepat dan tepat. Meskipun ada tantangan teknis, penggunaan alat ini dapat membantu mengamankan jaringan dari upaya serangan yang bertujuan untuk mendapatkan akses tidak sah ke sistem.

2. Serangan Malware tidak Terdeteksi Selama Investigasi Forensik

Selama investigasi forensik jaringan yang dilakukan, tidak terdeteksinya serangan malware dapat dijelaskan dengan beberapa faktor yang berhubungan dengan metode analisis yang digunakan dan keterbatasan dalam proses identifikasi. Data yang diperoleh dari investigasi menunjukkan bahwa tidak ada pergerakan mencurigakan yang mengarah pada aktivitas malware. Ada beberapa alasan utama mengapa serangan malware mungkin tidak terdeteksi selama analisis.

a. Pertama, jenis malware yang mungkin terlibat dalam serangan bisa saja tidak aktif pada saat data dikumpulkan. Banyak malware dirancang untuk beroperasi hanya pada waktu tertentu atau setelah kondisi tertentu dipenuhi. Jika malware tersebut dirancang untuk melakukan aksi hanya setelah periode tertentu atau saat kondisi spesifik terpenuhi, maka tidak akan ada indikasi keberadaan malware pada saat data dikumpulkan. Dalam kasus ini, jika waktu analisis tidak bertepatan dengan waktu aktivasi malware, maka jejak aktivitas malware tidak akan terdeteksi.

b. Kedua, ada kemungkinan bahwa malware yang terlibat menggunakan teknik fileless, di mana malware tidak meninggalkan jejak fisik di sistem file tetapi beroperasi langsung di memori. Malware jenis ini menyembunyikan aktivitasnya di dalam memori, sehingga tidak ada file yang terdeteksi oleh alat forensik tradisional. Dalam data yang tersedia, tidak ada indikasi serangan fileless atau penggunaan teknik yang memungkinkan malware untuk beroperasi di memori tanpa meninggalkan jejak pada file sistem.

Prosiding Seminar Nasional UNIMUS
Volume 7, 16 Oktober 2024
e-ISSN : 2654-3168 | p-ISSN : 2654-3257

c. Ketiga, alat yang digunakan untuk analisis mungkin memiliki keterbatasan dalam mendeteksi jenis malware tertentu. Data penelitian menunjukkan penggunaan alat seperti Wireshark untuk analisis jaringan, Microsoft Word untuk pencatatan, dan Google Chrome untuk pencarian referensi. Meskipun Wireshark efektif dalam mendeteksi aktivitas yang mencurigakan dalam jaringan seperti serangan DOS dan brute force, alat ini mungkin tidak sepenuhnya mampu mendeteksi aktivitas malware, terutama jika malware berkomunikasi melalui saluran yang dienkripsi atau tersembunyi. Jika malware menggunakan enkripsi untuk komunikasi atau metode lain untuk menyembunyikan aktivitasnya, maka alat yang digunakan mungkin tidak dapat mengidentifikasi keberadaan malware secara efektif.

d. Keempat, analisis forensik yang dilakukan mungkin tidak mencakup seluruh aspek yang diperlukan untuk mendeteksi malware. Fokus analisis dalam penelitian ini adalah pada serangan DOS dan brute force. Jika perhatian lebih difokuskan pada jenis serangan ini, ada kemungkinan bahwa aspek lain dari jaringan atau sistem yang mungkin menyembunyikan malware tidak dianalisis dengan mendalam. Ini bisa termasuk tidak memeriksa pola komunikasi jaringan yang mencurigakan atau tidak menganalisis data memori yang mungkin mengandung jejak malware.

e. Kelima, selama proses analisis forensik, keterbatasan perangkat dan waktu mungkin juga berperan. Dinyatakan bahwa selama analisis, terdapat kendala terkait dengan keterbatasan perangkat yang digunakan bersama dengan anggota keluarga, yang dapat mempengaruhi efisiensi dan kedalaman analisis. Jika analisis tidak dilakukan secara menyeluruh atau jika perangkat yang digunakan tidak memadai untuk mendeteksi malware, hasil yang diperoleh mungkin tidak mencerminkan aktivitas jahat yang sebenarnya.

Secara keseluruhan, ketidakmampuan untuk mendeteksi serangan malware selama investigasi forensik dalam kasus ini disebabkan oleh kombinasi dari faktor-faktor tersebut, termasuk jenis malware yang mungkin tidak aktif saat data dikumpulkan, penggunaan teknik fileless, keterbatasan alat yang digunakan, fokus analisis yang tidak mencakup semua aspek potensial, dan kendala perangkat dan waktu. Untuk mengatasi masalah ini di masa depan, pendekatan yang lebih menyeluruh dan penggunaan alat deteksi yang lebih canggih mungkin diperlukan untuk memastikan bahwa semua potensi ancaman, termasuk malware, dapat diidentifikasi dengan lebih efektif.

KESIMPULAN

Dalam penelitian ini, analisis forensik jaringan berhasil mengidentifikasi beberapa serangan, terutama dalam kategori serangan Denial of Service (DoS) dan brute force, menggunakan alat seperti Wireshark. Serangan DoS terdeteksi melalui bukti seperti SYN Flood, UDP Flood, dan DNS Amplification, sementara serangan brute force hanya menunjukkan bukti Hybrid Attack. Meskipun demikian, tidak terdeteksinya malware selama proses investigasi dapat dihubungkan dengan beberapa faktor, termasuk kemungkinan malware tidak aktif pada saat data dikumpulkan, penggunaan teknik

fileless, keterbatasan alat dan metode analisis, serta kendala perangkat dan waktu. Temuan ini menggarisbawahi pentingnya penggunaan alat deteksi yang lebih canggih dan pendekatan analisis yang lebih menyeluruh untuk mengidentifikasi berbagai jenis ancaman siber secara efektif.

DAFTAR PUSTAKA

Hariyadi, D., Indriyanto, M. W., & Habibi, M. (2020). Investigasi dan Analisis Forensik Digital pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 dan Support Vector Machine. Cyber Security dan Forensik Digital, 3(2), 34-38.

Pratama, Y. (2017). Network Forensic pada Jaringan Berbasis Awan (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW).

Rahmad, A. Forensik Serangan Brute Force Pada Cloud Public Menggunakan Logika Fuzzy. Forensik Serangan Brute Force Pada Cloud Public Menggunakan Logika Fuzzy.

Reza, N. R. F. R. N., & Rozi, F. (2023). Analisis Network Incident Packet Capture (PCAP) Menggunakan Wireshark. Journal of Informatics and Communication Technology (JICT), 5(2), 163-176.

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2016). Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. JEPIN (Jurnal Edukasi dan Penelitian Informatika), 2(1), 1-8.

Widodo, W., & Sugiantoro, B. (2018). PENERAPAN FRAMEWORK HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS (HDFIP) UNTUK MENDAPATKAN ARTIFAK BUKTI DIGITAL PADA SMARTPHONE TIZEN. Cyber Security dan Forensik Digital, 1(2), 67-74.