Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

MENGANALISIS KEBOCORAN DATA AKIBAT SERANGAN CYBER DI PT. ANALIS FORENSIK DIGITAL.

Raden Jagat Sageri[1], Yuli Komalasari[2*]

Program Studi Teknologi Informasi[1,2],
Fakultas Teknik dan Informatika[1,2],
Universitas Bina Sarana Informatika[1,2],

Correspondent Email: yuli.yks@bsi.ac.id

Author Email: raden.rjs1@gmail.com[1], yuli.yks@bsi.ac.id[2]

Received: September 30, 2025**. Revised:** October 20, 2025**. Accepted:** October 23,20025**. Issue Period:** Vol.9 No.4 (2025), Pp: 1486-1492

Abstrak: Di era digital yang semakin kompleks, kebocoran data akibat serangan cyber menjadi ancaman serius bagi instansi pemerintah maupun sektor swasta. Penelitian ini bertujuan untuk menganalisis proses forensik digital dalam investigasi insiden kebocoran data di PT Analis Forensik Digital sebagai bagian dari kegiatan Program Studi Independen Bersertifikat (MSIB). Metodologi yang digunakan meliputi observasi partisipatif, studi literatur, praktik langsung, serta diskusi dengan para ahli. Penelitian difokuskan pada identifikasi teknik anti-forensik, penggunaan perangkat lunak forensik seperti FTK Imager, Autopsy, Volatility, dan Wireshark, serta rekonstruksi insiden melalui artefak digital. Hasil investigasi menunjukkan bahwa serangan cyber yang disimulasikan melalui pengiriman email dengan file berbahaya (.zip) mampu menimbulkan jejak digital yang kompleks, namun masih dapat diidentifikasi melalui prosedur forensik yang sistematis. Teknik pengamanan data seperti enkripsi dan penghapusan permanen dapat diatasi melalui akuisisi bit-per-bit dan verifikasi nilai hash. Analisis metadata, log sistem, serta artefak RAM dan jaringan memungkinkan penyusunan kronologi kejadian secara rinci dan valid secara hukum. Temuan ini menggarisbawahi pentingnya forensic readiness dalam organisasi, serta perlunya peningkatan kapabilitas SDM di bidang forensik digital sebagai bagian dari respons terhadap eskalasi kejahatan cyber di Indonesia.

Kata kunci: Anti-Forensik; Forensik Digital; Investigasi Digital; Kebocoran Data; Serangan Cyber

Abstract: In today's increasingly complex digital era, data breaches resulting from cyberattacks have become a serious threat to both government institutions and the private sector. This study aims to analyze the digital forensic process in investigating data breach incidents at PT Analis Forensik Digital, as part of the Merdeka Certified Independent Study Program (MSIB). The research methodology includes participatory observation, literature review, hands-on practice, and expert discussions. The study focuses on identifying anti-forensic techniques, utilizing forensic tools such as FTK Imager, Autopsy, Volatility, and Wireshark, and reconstructing incidents through digital artifacts. The results of the investigation indicate that cyberattacks simulated through malicious email attachments (.zip files) can generate complex digital traces, which can still be identified through systematic

DOI: 10.52362/jisamar.v9i4.2106

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

forensic procedures. Data protection techniques such as encryption and permanent deletion were successfully countered through bit-by-bit acquisition and hash verification. Metadata analysis, system logs, and RAM and network artifacts enabled the reconstruction of incident timelines in a detailed and legally valid manner. These findings emphasize the importance of forensic readiness within organizations and the need to improve human resource capabilities in digital forensics as a response to the increasing trend of cybercrime in Indonesia.

Keywords: Anti-Forensics; Cyberattack; Data Breach; Digital Forensics; Digital Investigation

I. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan pada berbagai aspek kehidupan, namun juga diiringi dengan meningkatnya ancaman keamanan siber [1].Di Indonesia, insiden kebocoran data dan peretasan sistem menjadi perhatian utama karena dampak serius yang ditimbulkannya. Kasus-kasus besar seperti kebocoran data nasabah Bank Syariah Indonesia (BSI) pada tahun 2023 [2] dan klaim peretasan data pemerintah oleh "Bjorka" pada tahun 2022 [3] menunjukkan urgensi kebutuhan akan tenaga ahli forensik digital.

Forensik digital adalah disiplin ilmu yang menerapkan proses identifikasi, pengumpulan, analisis, dan presentasi bukti digital untuk tujuan investigasi hukum [4]. Disiplin ini menjadi krusial karena kejahatan dunia maya terus meningkat, baik dari segi jumlah maupun kompleksitasnya [5]. Dalam menghadapi kejahatan siber yang semakin canggih, pelaku seringkali menggunakan teknik anti-forensik seperti enkripsi, steganografi, dan penghapusan data untuk menghindari deteksi [6]. Oleh karena itu, pemahaman mendalam mengenai teknik-teknik ini dan cara mengatasinya menjadi krusial.

Penelitian ini dilakukan berdasarkan pengalaman penulis selama mengikuti Program Merdeka Studi Independen Bersertifikat (MSIB) di PT Analis Forensik Digital. Fokus penelitian adalah menganalisis proses forensik digital dalam sebuah studi kasus simulasi serangan siber, mengidentifikasi teknik anti-forensik yang digunakan pelaku, dan mengevaluasi efektivitas perangkat forensik dalam mengungkap insiden tersebut. Tujuannya adalah untuk memberikan kontribusi pada pengembangan kompetensi forensik digital di Indonesia [7].

II. METODE DAN MATERI

Metode Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Pengumpulan data dilakukan melalui beberapa teknik selama periode program MSIB dari September hingga Desember 2024. Manajemen keamanan siber di era digital menuntut pendekatan proaktif, tidak hanya reaktif setelah insiden terjadi [8]. Yang digunakan dalam penelitian ini harus mampu menggambarkan model proses pengukuran atau penyelesaian masalah yang dikembangkan. Untuk mendapatkan informasi yang komprehensif, penelitian ini menggunakan beberapa metode pengumpulan data:

1. Observasi Partisipatif: Penulis terlibat langsung dalam program pelatihan forensik digital di PT Analis Forensik Digital melalui program MSIB. Selama program, penulis mengamati dan berpartisipasi dalam berbagai aktivitas pembelajaran, termasuk sesi live teaching, pengerjaan tugas praktis dengan tools forensik, dan diskusi virtual.

2. Studi Literatur: Untuk membangun landasan teoretis, dilakukan kajian terhadap berbagai sumber referensi seperti buku teks, artikel jurnal ilmiah, laporan teknis, dan dokumentasi resmi dari tools forensik yang digunakan.

3. Praktik Langsung: Penulis melakukan praktik langsung menggunakan berbagai tools forensik untuk mengumpulkan dan menganalisis bukti digital. Praktik ini mencakup akuisisi data volatile (memori)

DOI: 10.52362/jisamar.v9i4.2106

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

dan non-volatile (disk) menggunakan FTK Imager, analisis bukti dengan Autopsy, dan simulasi investigasi insiden keamanan siber seperti kasus ransomware.

4. Diskusi dengan Ahli: Penulis melakukan diskusi dengan mentor dan para ahli forensik digital di PT Analis Forensik Digital untuk mendapatkan wawasan praktis yang lebih mendalam, termasuk sesi tanya jawab, diskusi studi kasus, dan konsultasi mengenai tantangan dalam investigasi. Materi penelitian mencakup konsep-konsep dasar yang relevan, di antaranya adalah Forensik Digital sebagai cabang ilmu forensik untuk identifikasi, pelestarian, dan analisis data digital sebagai barang bukti. Selanjutnya, konsep Kebocoran Data (data breach) dipahami sebagai insiden di mana informasi rahasia diakses oleh pihak yang tidak berwenang. Terakhir, materi mengenai Serangan Siber (Cyber Attack) yang mencakup berbagai tindakan jahat untuk mencuri, merusak, atau memanipulasi informasi digital.

5. Skenario Kasus: Penelitian berpusat pada sebuah studi kasus di mana sebuah perangkat menjadi korban serangan *ransomware* yang disebarkan melalui lampiran email berbahaya. Tahapan investigasi mengikuti kerangka kerja dari *National Institute of Standards and Technology* (NIST) yang terdiri dari identifikasi, koleksi, pemeriksaan, analisis, dan pelaporan [9]

Penelitian berpusat pada sebuah studi kasus di mana sebuah perangkat menjadi korban serangan *ransomware* yang disebarkan melalui lampiran email berbahaya. Tahapan investigasi mengikuti kerangka kerja dari *National Institute of Standards and Technology* (NIST) yang terdiri dari identifikasi, koleksi, pemeriksaan, analisis, dan pelaporan [9]. Pendekatan ini memastikan bahwa bukti digital yang ditemukan dapat dipertanggungjawabkan dan memiliki keabsahan di mata hukum [10]. Analisis lalu lintas jaringan dengan alat seperti Wireshark juga menjadi bagian penting untuk mendeteksi aktivitas ilegal [11]. Selain itu, konfigurasi jaringan seperti penerapan *Quality of Service* (QoS) dengan metode *Hierarchical Token Bucket* (HTB) pada perangkat Mikrotik dapat memperkuat analisis forensik dengan memungkinkan pengelolaan lalu lintas secara presisi untuk mendeteksi anomali *bandwidth* yang disebabkan oleh malware atau serangan DDoS [12].

III. PEMBAHASA DAN HASIL

Proses investigasi digital dilakukan terhadap sebuah kasus di mana terdapat email mencurigakan yang dikirimkan oleh pelaku. Email tersebut berisi lampiran sebuah file berbahaya bernama putri folina.zip yang diduga mengandung malware atau ransomware. Tujuan utama pemeriksaan adalah untuk merekonstruksi kronologi insiden dan menelusuri sumber serangan.Temuan Barang Bukti elektronik yang diterima berupa file email dan lampirannya. Dari email yang dikirim oleh mayaputri.inspires@gmail.com pada tanggal 19 November 2024, ditemukan lampiran Lamaran kerja maya follina.zip.

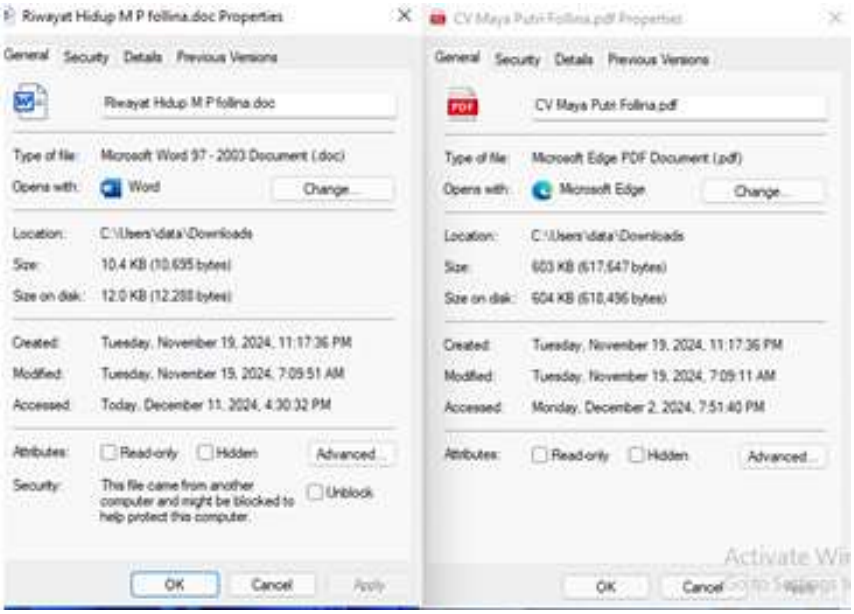
Sumber: (Penelitian,2025)

Gambar 1. Email yang Diterima dari Pelaku

Setelah file ZIP diekstrak, ditemukan dua dokumen di dalamnya, yaitu Riwayat Hidup M P folina.doc dan CV Maya Putri Folina.pdf.

DOI: 10.52362/jisamar.v9i4.2106

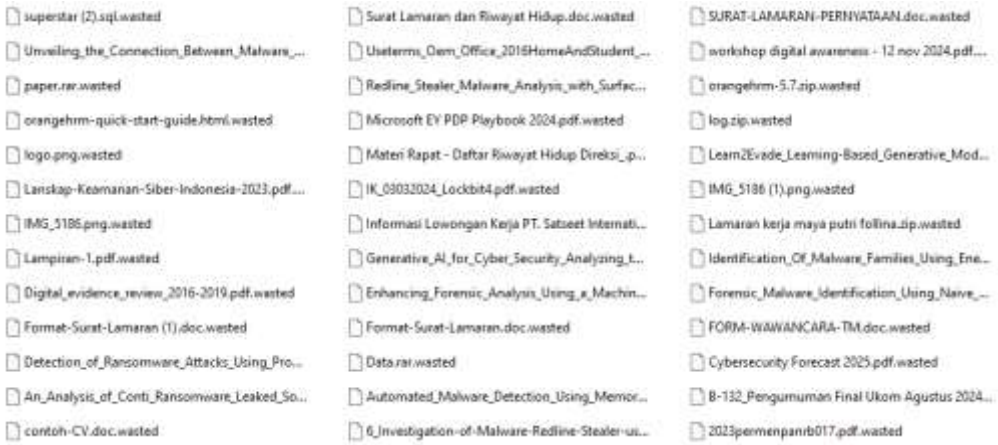
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)



Sumber: (Penelitian,2025)

Gambar 2. File ZIP dan Isi Dokumen Setelah Diekstraksi

Saat dokumen tersebut dibuka, terjadi proses enkripsi pada beberapa file di komputer korban, yang ditandai dengan perubahan ekstensi menjadi .wasted.



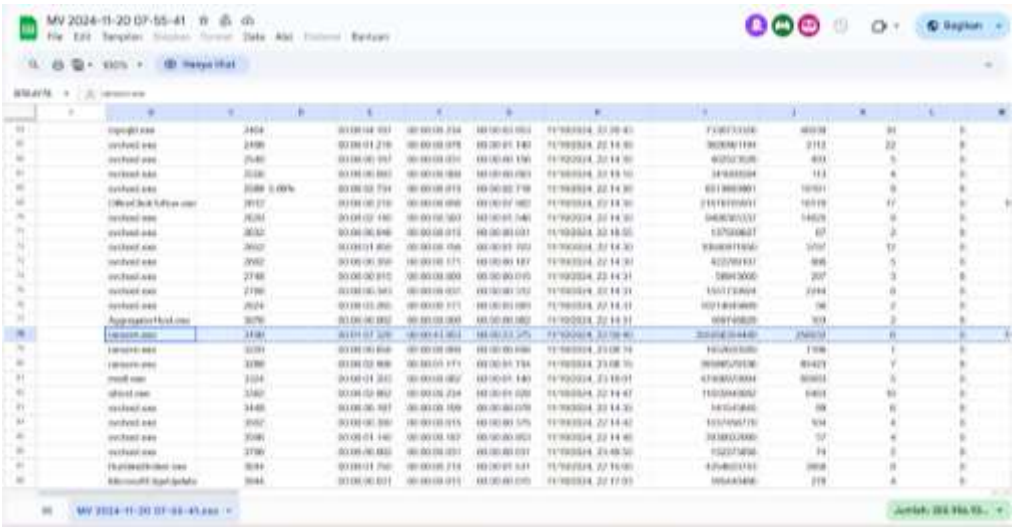
Sumber: (Penelitian,2025)

Gambar 3. Contoh File yang Terenkripsi dengan Ekstensi .wasted

Proses Analisis forensik dilakukan pada memory dump sistem korban menggunakan tools OS Forensics. Hasilnya, ditemukan sebuah program mencurigakan bernama ransome.exe yang sedang berjalan pada saat insiden terjadi.

DOI: 10.52362/jisamar.v9i4.2106

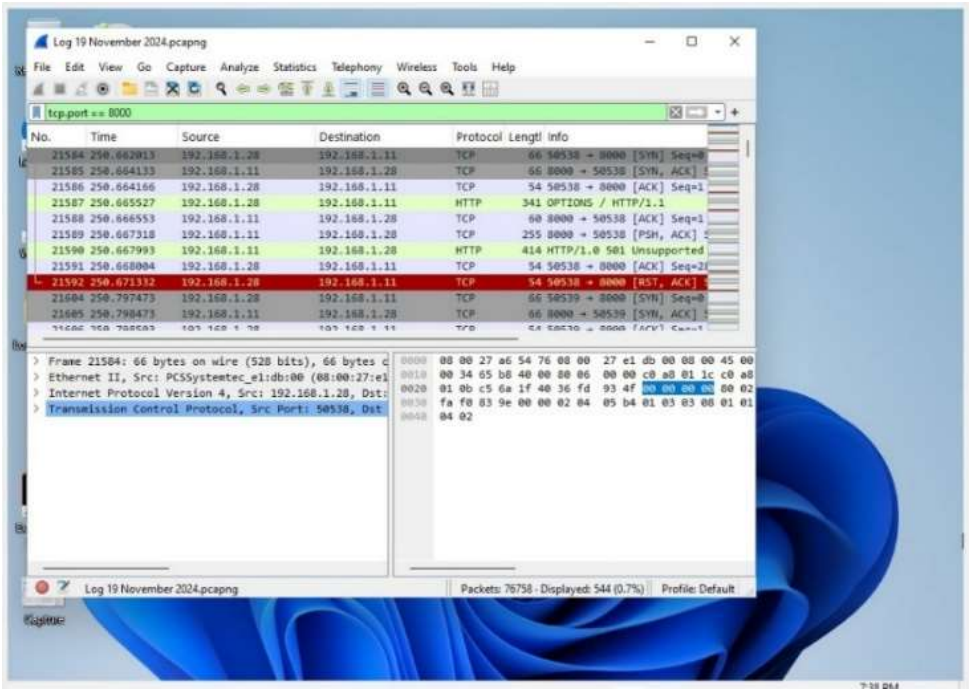
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)



Sumber: (Penelitian,2025)

Gambar 4. Penemuan Proses ransome.exe Melalui Analisis Memori

Selanjutnya, analisis lalu lintas jaringan menggunakan Wireshark menunjukkan adanya komunikasi antara dua alamat IP (192.168.1.28 dan 192.168.1.11) sesaat setelah file berbahaya dibuka, yang mengindikasikan aktivitas komunikasi oleh malware.



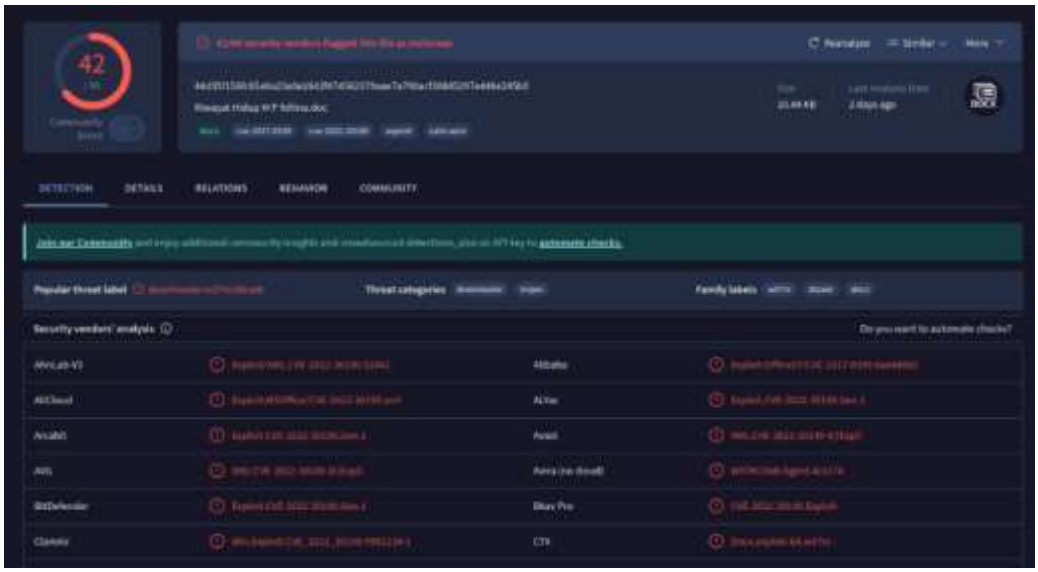
Sumber: (Penelitian,2025)

Gambar 5. Log Jaringan yang Menunjukkan Komunikasi Mencurigakan

DOI: 10.52362/jisamar.v9i4.2106

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

Untuk mengonfirmasi sifat berbahaya dari file, dilakukan analisis statis dengan mengunggah Riwayat Hidup M P folina.doc ke VirusTotal.com. Hasil pemindaian menunjukkan bahwa 42 vendor antivirus mendeteksinya sebagai file berbahaya yang mengandung virus.



Sumber: (Penelitian,2025)

Gambar 6. Hasil Analisis Statis di VirusTotal

Analisis lebih lanjut pada metadata di VirusTotal mengungkap sebuah temuan krusial. File Riwayat Hidup M P.doc tersebut pada awalnya adalah sebuah file executable dengan nama Riwayat Hidup M P.exe. Pelaku mengubah ekstensi file tersebut menjadi .doc pada pukul 07:57, sebelum mengirimkannya melalui email, sebuah teknik anti-forensik untuk mengelabui korban.

Hasil investigasi berhasil merekonstruksi kronologi serangan secara rinci. Pelaku menggunakan teknik rekayasa sosial dengan mengirimkan email lamaran kerja palsu untuk memancing korban membuka lampiran. Teknik anti-forensik yang digunakan adalah penyamaran file .exe menjadi .doc. Meskipun demikian, melalui penerapan prosedur forensik yang sistematis mulai dari analisis statis hingga analisis memori dan jaringan jejak digital pelaku berhasil diidentifikasi. Temuan ini menegaskan bahwa bahkan dengan teknik penghindaran yang sederhana, investigasi forensik yang komprehensif mampu mengungkap mekanisme serangan dan mengumpulkan bukti digital yang valid [4]

IV. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa forensik digital memegang peranan krusial dalam investigasi insiden keamanan siber, khususnya pada kasus kebocoran data. Melalui tahapan proses forensik yang sistematis mulai dari akuisisi data, analisis artefak sistem dan jaringan, hingga penyusunan laporan penulis berhasil mengungkap kronologi serangan. Studi kasus terhadap file ZIP berbahaya yang dikirim melalui email menunjukkan adanya penggunaan teknik anti-forensik oleh pelaku, seperti penyembunyian metadata dan enkripsi data korban.Tantangan ini berhasil diatasi dengan penerapan metode akuisisi forensik yang sesuai standar, seperti penggunaan hashing dan imaging, serta pemanfaatan tools forensik seperti FTK Imager, Autopsy, dan Wireshark. Temuan ini menegaskan pentingnya kompetensi teknis dan metodologis yang adaptif untuk menghadapi dinamika ancaman siber saat ini. Secara keseluruhan, kegiatan ini memberikan

DOI: 10.52362/jisamar.v9i4.2106

pemahaman teoretis dan pengalaman praktis dalam mendeteksi, menganalisis, dan mengungkap insiden keamanan siber secara bertanggung jawab.

REFERENASI

[1] F. D. Silalahi, *Keamanan Siber*. 2022. Accessed: Sep. 08, 2025. [Online]. Available: https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/367

[2] Apatisme Dobrak, "Kebocoran Data BSI: Data Tercuri Tidak Dijamin Kembali," DISPLAY. Accessed: Sep. 08, 2025. [Online]. Available: https://display.ub.ac.id/news/kebocoran-data-bsi-data-tercuri-tidak-dijamin-kembali/

[3] Tifada Detha Arya and Winardi Ariandono Dijan, "Jejak Peretasan Bjorka: Potret Kegagalan Pemerintah Lindungi Data Pribadi," VOI. Accessed: Sep. 08, 2025. [Online]. Available: https://voi.id/memori/395545/jejak-peretasan-bjorka-potret-kegagalan-pemerintah-lindungi-data-pribadi?

[4] A. Zein, "Komputer Forensik," 2024. Accessed: Sep. 08, 2025. [Online]. Available: https://repository.penerbiteureka.com/media/publications/568412-komputer-forensik-4532782b.pdf

[5] M. N. A. Azmi, H. Saifudin, C. T. Purba, A. Suryaningtyas, and U. S. Situmorang, "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan," *JURNAL MULTIDISIPLIN ILMU AKADEMIK*, vol. 1, no. 6, pp. 448–458, Dec. 2024, doi: 10.61722/jmia.v1i6.3267.

[6] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime," 2020. doi: https://doi.org/10.14421/csecurity.2020.3.2.2144.

[7] M. G. B. Sitorus, N. Maria, and Y. N. Safa, "Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek: Identifikasi, Evaluasi, dan Mitigasi Ancaman," *Jurnal Manajemen Informatika (JAMIKA)*, vol. 14, no. 2, pp. 187–198, Jul. 2024, doi: 10.34010/jamika.v14i2.12887.

[8] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "Manajemen Keamanan Cyber di Era Digital," *Journal of Business and Entrepreneurship*, vol. 11, no. 1, pp. 23–33, 2023, doi: 10.46273/job&e.v11i1.365.

[9] M. Fitriana, "Penerapan Metode National Institude Of Standars And Technology (NIST) Dalam Analisis Forensic Digital Untuk Penanganan Cyber Crime Ditinjau Dari Aspek Hukum Yang Berlaku," 2020. Accessed: Sep. 08, 2025. [Online]. Available: http://repository.ar-raniry.ac.id/id/eprint/15051

[10] M. Soleh and Z. Tjenreng, "Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital," *JKP) Journal of Government, Social and Politics*, vol. 11, 2024, doi: https://doi.org/10.25299/jkp.2025.vol11(1).20524.

[11] R. Hanipah and H. Dhika, "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark," *Journal of Computer and Information Technology*, vol. 4, no. 1, 2020, [Online]. Available: http://e-journal.unipma.ac.id/index.php/doubleclickTelepon:

[12] R. B. S. Wibowo and Y. Komalasari, "Penerapan Quality of Service Menggunakan Hierarchical Token Bucket Pada Jaringan Internet Menggunakan Mikrotik di PT. Triwall Indonesia," *Jurnal Komputer Antartika*, vol. 3, no. 2, pp. 42–46, May 2025, doi: 10.70052/jka.v3i2.734.

DOI: 10.52362/jisamar.v9i4.2106