CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 9, No. 1, Mei 2026, hlm. 10-15

Penerapan Metode SANS Pada Studi Kasus Serangan Ransomware Eksploitasi FOLLINA (CVE-2022-30190)

Muhammad Khairin

Jurusan Komputer dan Bisnis, Politeknik Negeri Tanah Laut,
Tanah Laut, Pelaihari, 70814, Indonesia.
Email: muhammad.khairin@mhs.politala.ac.id

Abstrak

Serangan siber modern pada era ini semakin kompleks, seringkali eksploitasi serangannya menggabungkan berbagai vektor untuk menembus pertahanan. Penelitian ini bertujuan untuk menganalisis secara mendalam sebuah studi kasus forensik digital terhadap serangan *ransomware* yang memanfaatkan kerentanan Follina (CVE-2022-30190). Metode yang diterapkan adalah Siklus Respons Insiden dari SANS Institute, sebuah pendekatan kualitatif yang membedah insiden dengan enam fase: *Preparation*, *Identification*, *Containment*, *Eradication*, *Recovery*, dan *Lessons Learned*. Hasil investigasi berhasil merekonstruksi seluruh rantai serangan yang dilakukan oleh kelompok BlackPython Team, dimulai dari melakukan pengintaian, infiltrasi melalui *spear-phishing*, eksekusi kode jarak jauh via eksploitasi Follina, hingga pemasangan *backdoor* dan eksekusi akhir *ransomware*. Analisis artefak digital dari sistem dan jaringan mengungkap setiap Taktik, Teknik, dan Prosedur (TTPs) yang digunakan pelaku. Kesimpulannya, penerapan metode SANS terbukti efektif untuk mengurai serangan multi-vektor yang canggih dan memberikan kerangka kerja yang komprehensif. Investigasi ini tidak hanya mengidentifikasi modus operandi pelaku tetapi juga menghasilkan rekomendasi mitigasi strategis untuk memperkuat postur keamanan siber berdasarkan setiap fase respons insiden.

Kata kunci: Forensik Digital, Respons Insiden, SANS, *Ransomware*, *CVE-2022-30190*

Application Of The SANS Method In A Case Study Of A Ransomware Attack Exploiting FOLLINA (CVE-2022-30190)

Abstract

Modern cyberattacks are increasingly complex, often combining multiple attack vectors to penetrate defenses. This research aims to conduct an in-depth digital forensic analysis of a ransomware attack exploiting the Follina vulnerability (CVE-2022-30190). The method applied is the SANS Institute's Incident Response Cycle, a qualitative approach that analyzes incidents into six phases: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. The investigation successfully reconstructed the entire attack chain carried out by the BlackPython Team, starting from reconnaissance, infiltration via spear-phishing, remote code execution via the Follina exploit, to backdoor installation and final ransomware execution. Analysis of digital artifacts from the system and network revealed every Tactic, Technique, and Procedure (TTP) used by the perpetrator. In conclusion, the application of the SANS method proved effective in unraveling sophisticated multi-vector attacks and provided a comprehensive framework. This investigation not only identified the perpetrator's modus operandi but also generated strategic mitigation recommendations to strengthen cybersecurity posture based on each phase of the incident response.

***Keywords**: Digital Forensics, Incident Response, SANS, Ransomware, CVE-2022-30190*

1. PENDAHULUAN

Di era digital sekarang, kemajuan teknologi informasi sangatlah pesat, ini memicu transformasi fundamental di hampir semua aspek kehidupan, termasuk dalam dunia industri. Untuk tetap dapat bersaing, perusahaan modern secara masif mengadopsi teknologi digital untuk membantu meningkatkan efisiensi, mempercepat proses bisnis, dan memberikan pelayanan terbaik kepada pelanggan. Ketergantungan akan hal ini menjadikan infrastruktur digital, mulai dari server hingga aplikasi bisnis, berperan sebagai tulang punggung operasional yang sangat krusial. Namun, seiring dengan meningkatnya ketergantungan ini, muncul pula risiko siber yang semakin kompleks dan berbahaya. Ancaman seperti *malware*, peretasan sistem, hingga pencurian data telah menjadi tantangan bisnis yang serius, yang dapat mengakibatkan kerugian finansial, gangguan operasional, serta penurunan kepercayaan pelanggan (Gian Aditya Asbath et al., 2025).

Konteks pada negara Indonesia menunjukkan betapa nyatanya ancaman ini. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2024 saja tercatat total 330.527.636 aktivitas anomali trafik siber (Pratiwi et al., 2024; Sandrina Ayu et al., 2025), yang mengindikasikan bahwa sistem digital di Indonesia berada di bawah ancaman yang konstan. Ketika sebuah serangan siber berhasil terjadi, kemampuan organisasi untuk merespons secara efektif menjadi kunci. Di sinilah forensik digital memainkan perannya sebagai disiplin ilmu yang krusial untuk melakukan investigasi pasca-insiden (Montasari, 2016; Firmansyah, 2025). Melalui pendekatan forensik yang sistematis, sebuah organisasi dapat mengidentifikasi sumber serangan, memahami metode yang digunakan pelaku, dan memperoleh wawasan untuk memperkuat pertahanan di masa depan. Kerangka kerja respons insiden seperti yang dipopulerkan oleh SANS Institute dan National Institute of Standards and Technology (NIST) menyediakan pendekatan terstruktur untuk menangani insiden keamanan (Kent et al., 2006; SANS Institute, 2025).

Meskipun terdapat banyak penelitian forensik digital yang pernah dilakukan, sering kali analisisnya berfokus pada komponen serangan yang terisolasi. Sebagai contoh, studi oleh (Biswas et al., 2018)berfokus pada analisis teknis kerentanan *Remote Code Execution* (RCE), sementara penelitian dari (Adu-Manu et al., 2023) secara spesifik membahas metode deteksi *phishing*. Namun, masih terdapat keterbatasan dalam literatur yang menyajikan analisis komprehensif terhadap serangan multi-vektor, yang mampu merekonstruksi seluruh attack chain dari pengintaian awal hingga dampak akhir dalam konteks korporat. Penelitian ini hadir untuk mengisi celah tersebut dengan menyajikan analisis forensik digital yang mendalam terhadap studi kasus serangan siber kompleks yang menimpa PT. Satseet International pada periode 5 hingga 19 November 2024. Insiden ini menjadi contoh nyata dari serangan modern, yang diawali dengan teknik *Directory Traversal* untuk pengintaian kerentanan aplikasi web (Ravindran and Potukuchi, 2022), dilanjutkan dengan infiltrasi melalui *spear-phishing*, eskalasi hak akses dengan mengeksploitasi kerentanan CVE-2022-30190 (Follina) (Sophos, 2022), hingga puncaknya pada penyebaran *Ransomware* oleh kelompok BlackPython Team(Gandotra et al., 2014; Al-rimy et al., 2018; Novita et al., 2023) Dengan menerapkan kerangka kerja Respons Insiden dari SANS, penelitian ini bertujuan untuk merekonstruksi secara utuh rantai serangan yang terjadi, menganalisis teknik yang digunakan pelaku, dan merumuskan rekomendasi mitigasi yang konkret.

2. METODE PENELITIAN

Penelitian ini menggunakan desain penelitian kualitatif dengan pendekatan studi kasus. Kerangka kerja (*framework*) yang diterapkan adalah *Incident Response Cycle* yang dipopulerkan oleh SANS Institute (Exabeam, 2025). Metode ini dipilih karena menyediakan pendekatan holistik yang tidak hanya berfokus pada analisis teknis, tetapi juga pada manajemen insiden secara keseluruhan, dari kesiapan hingga evaluasi pasca-kejadian, Pendekatan ini melengkapi kerangka kerja investigasi teknis lainnya seperti yang diatur oleh NIST(Fitriana et al., 2020; Rafi et al., 2025; Audita et al., 2025; Putra et al., 2024).

Gambar 1 Alur Proses Siklus Respons Insiden SANS

Proses investigasi dan analisis dalam penelitian ini dilakukan dengan mengikuti enam tahapan terstruktur dari siklus tersebut.

2.1. Metode Pengumpulan Data Penelitian

Metode pengumpulan data yang digunakan adalah akuisisi forensik terhadap artefak digital yang terkait dengan insiden di PT. Satseet International. Data utama yang dikumpulkan adalah *Image* Sistem, Data Memori (*Live Forensics*), dan Log Jaringan (*Network Logs*). Untuk menjaga integritas bukti, digunakan perangkat keras *write-blocker* selama proses akuisisi. Instrumen penelitian utama yang digunakan dalam studi kasus ini meliputi perangkat lunak forensik standar industri: Autopsy untuk pemeriksaan mendalam terhadap *image* sistem; Wireshark untuk menganalisis rekaman lalu lintas jaringan; serta VirusTotal dan Jotti sebagai layanan pemindaian *malware* online untuk menganalisis file mencurigakan dan mengonfirmasi eksploitasi kerentanan CVE-2022-30190.

2.2. Tahapan Penelitian

Proses investigasi dan analisis dalam penelitian ini dilakukan dengan mengikuti enam tahapan terstruktur dari *framework* SANS:

1. ***Preparation* (Persiapan):** Menganalisis kondisi awal keamanan perusahaan untuk mengidentifikasi kelemahan proaktif.

2. ***Identification*** **(Identifikasi):** Mengonfirmasi terjadinya insiden melalui bukti-bukti awal yang ditemukan.
3. ***Containment*** **(Penahanan):** Mengisolasi sistem yang terdampak dan melakukan akuisisi bukti digital secara forensik.
4. ***Eradication*** **(Pemberantasan):** Melakukan analisis mendalam terhadap bukti digital untuk merekonstruksi rantai serangan.
5. ***Recovery*** **(Pemulihan):** Menganalisis dan menjalankan proses pemulihan sistem dan data pasca-serangan.
6. ***Lessons Learned*** **(Pembelajaran):** Merumuskan kesimpulan dan rekomendasi strategis berdasarkan seluruh temuan.

3. HASIL DAN PEMBAHASAN

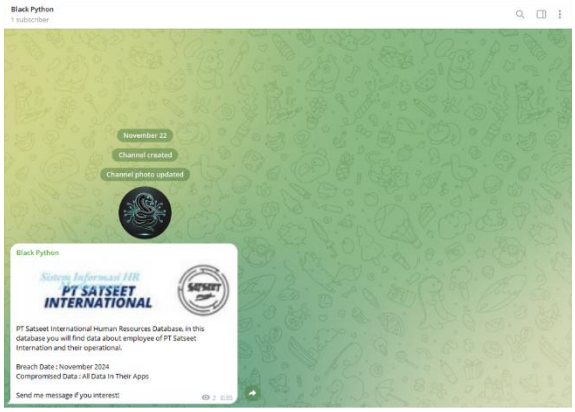
Analisis forensik ini berhasil merekonstruksi seluruh alur serangan yang kompleks. Tabel 1 di bawah ini menyajikan ringkasan kronologis dari kejadian utama, yang akan dibedah secara mendalam melalui enam fase siklus respons insiden SANS.

Tabel 1 Ringkasan Kronologi Kejadian

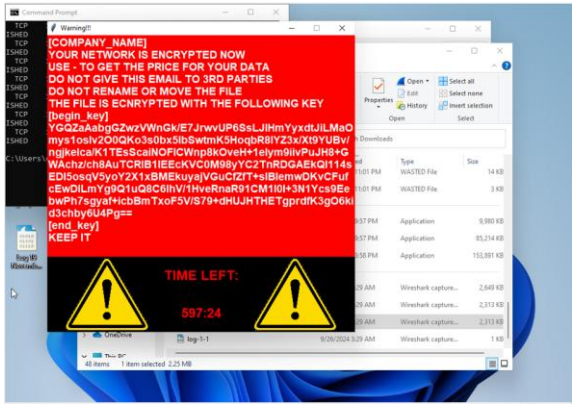
Tgl & Waktu (PST)	Alamat IP / Aktor	Aktivitas
5 Nov 2024, 02:45	Admin Perusahaan	Mempublikasikan informasi lowongan kerja yang menjadi pancingan awal.
19 Nov 2024, 15:18	192.168.1.28 (Korban)	Menerima email *phishing* berisi lampiran berbahaya.
19 Nov 2024, 15:18	192.168.1.28 (Korban)	Membuka dokumen yang mengeksploitasi Follina.
19 Nov 2024, 22:49	192.168.1.28 (Korban)	Mengunduh file *malware* update.exe dari IP penyerang (192.168.1.11).
19 Nov 2024, 22:50	192.168.1.28 (Korban)	Mengunduh file main_v2.exe (diubah nama menjadi ransom.exe).
19 Nov 2024, 22:59	192.168.1.1/ ransom.exe	*Ransomware* dijalankan, file mulai terenkripsi.

3.1. Konfirmasi Insiden dan Identifikasi Awal (SANS: *Identification*)

Setiap respons insiden dimulai ketika adanya sebuah anomali terdeteksi. Dalam kasus ini, proses masuk ke dalam fase *Identification*, yang dipicu oleh bukti dampak akhir. Bukti pertama adalah kemunculan sebuah pesan tebusan di komputer korban. Sebuah ciri khas utama dari serangan *ransomware* , seperti terlihat pada (Gambar 2). Bukti kedua ditemukan di platform Telegram, di mana kanal "Black Python" secara terbuka mengklaim telah berhasil meretas PT Satseet International dan memiliki data karyawan. Klaim ini (Gambar 3) mengonfirmasi bahwa serangan ini menggunakan taktik *double extortion* (enkripsi sekaligus pencurian data) (Zscaler, 2025).



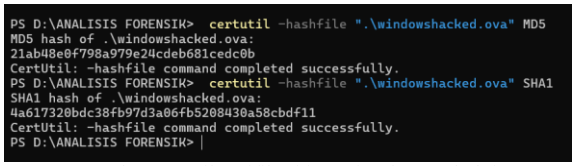
Gambar 2 Klaim di Telegram oleh Black Python.



Gambar 3 Pesan tebusan *ransomware* di komputer korban.

3.2. Pengamanan dan Akuisisi Bukti Digital (SANS: Containment)

Setelah insiden teridentifikasi, prioritas utama adalah menahan kerusakan, yang merupakan inti dari fase *Containment*. Tindakan pertama adalah mengisolasi sistem yang terdampak dari jaringan. Segera setelah itu, proses pengumpulan bukti digital dilakukan dengan hati-hati. Bukti yang berhasil dikumpulkan adalah *image* sistem (windowshacked.ova) , *data live forensics* , dan log jaringan (Log 19 November 2024.pcapng). Sebagai bagian fundamental dari fase ini, integritas bukti diverifikasi menggunakan *hashing* MD5 dan SHA1. Hasilnya menunjukkan status "*Match*" (Gambar 4), yang secara forensik mengonfirmasi bukti tetap asli dan tidak berubah.

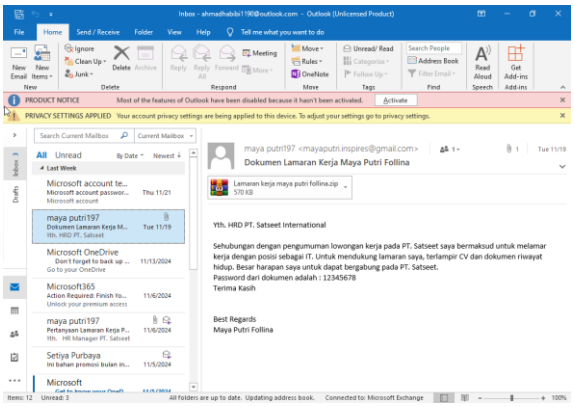


Gambar 4 Hasil verifikasi integritas barang bukti

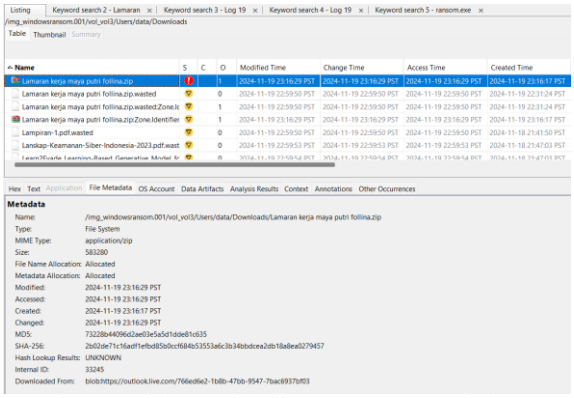
3.3 Rekonstruksi Rantai Serangan (SANS: *Eradication*)

Fase *Eradication* berfokus pada analisis mendalam untuk menemukan akar penyebab agar dapat dihilangkan sepenuhnya. Jejak awal menunjukkan penyerang melakukan pengintaian

melalui *Directory Traversal*, lalu melancarkan serangan *spear-phishing* yang sangat tertarget melalui email "Maya Putri Follina" (Gambar 5). Analisis metadata pada lampiran (Gambar 6) secara definitif membuktikan email yang berasal dari outlook.live.com adalah titik masuk utama serangan.

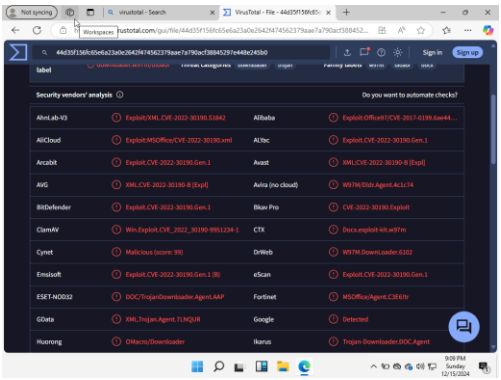


Gambar 5 Tampilan email *phishing* yang diterima korban



Gambar 6 Analisis metadata file lampiran Lamaran kerja maya putri follina.zip

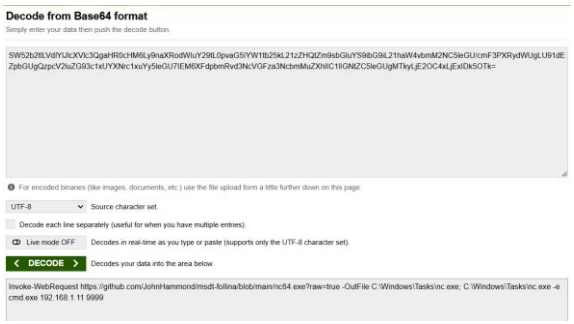
Saat korban membuka dokumen, kerentanan Follina (CVE-2022-30190) tereksploitasi, yang terkonfirmasi dari hasil pemindaian VirusTotal yang menandai file berbahaya (Gambar 7). Analisis log jaringan menemukan *payload* PowerShell yang disamarkan dengan Base64. Setelah didekode (Gambar 9), perintah asli terungkap: mengunduh tool Netcat (nc.exe) dan menciptakan koneksi *reverse shell* ke IP penyerang (192.168.1.11) pada *port* 9999.



Gambar 7 Hasil pemindaian VirusTotal yang mengidentifikasi eksploitasi CVE-2022-30190

Untuk memperkuat dan memvalidasi temuan dari VirusTotal, analisis lebih lanjut juga dilakukan menggunakan layanan pemindai *malware* Jotti. Hasilnya, seperti yang ditunjukkan pada (Gambar 8), konsisten dengan analisis sebelumnya, di mana berbagai vendor antivirus seperti ClamAV dan Kaspersky juga secara eksplisit mendeteksi adanya Exploit.CVE-2022-30190. Konsistensi temuan dari dua platform pemindaian yang berbeda ini memberikan bukti yang sangat kuat bahwa dokumen tersebut memang dilengkapi dengan kerentanan Follina.

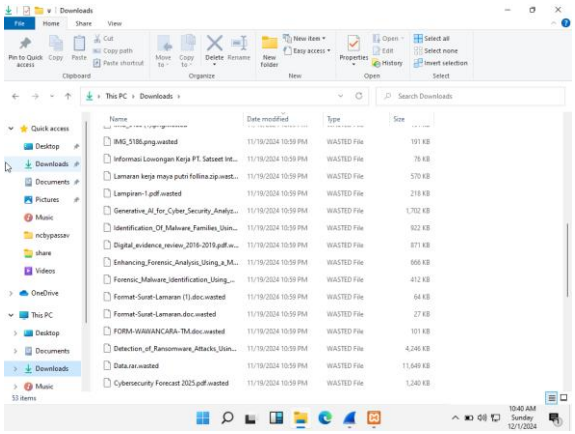
Gambar 8 Hasil validasi pemindaian menggunakan Jotti yang mengonfirmasi eksploitasi Follina



Gambar 9 Hasil dekode *payload* Base64 yang mengungkap perintah berbahaya

Dengan kendali penuh, penyerang mengunduh *backdoor* (update.exe) dan *ransomware* (ransom.exe), yang jejaknya terekam dalam lalu lintas jaringan (Gambar 10). Proses analisis dan klasifikasi kedua file ini dilakukan untuk memahami fungsinya (Gandotra et al., 2014; Khalda and Wibowo, 2025) Akhirnya, ransom.exe dieksekusi dan mengenkripsi file-file pengguna dengan ekstensi .wasted (Gambar 11).

Gambar 10 Log Wireshark yang mengonfirmasi permintaan unduh *malware*



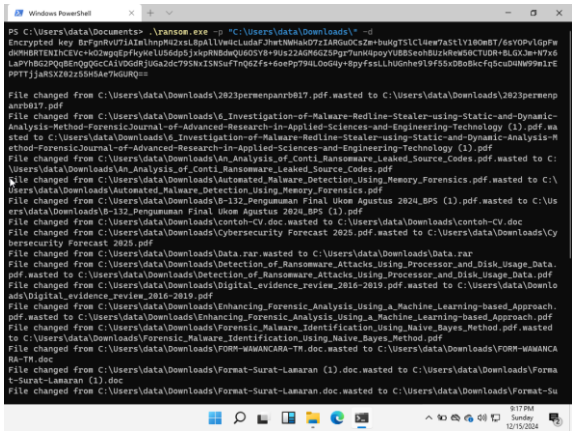
Gambar 11 Tampilan file-file pengguna yang telah dienkripsi dengan ekstensi .wasted

3.4 Pemulihan Sistem dan Data (SANS: *Recovery*)

Fase *Recovery* bertujuan mengembalikan sistem ke kondisi operasional yang aman. Dalam kasus ini, fokus utamanya adalah memulihkan data yang terenkripsi. Setelah proses analisis mendalam pada fase *Eradication*, ditemukan bahwa ransom.exe memiliki fungsi dekripsi bawaan. Proses dekripsi dilakukan dengan menjalankan perintah pada komputer korban.

```
ransom.exe -p "C:\Users\data\Downloads\" -d
```

Seperti yang didokumentasikan pada (Gambar 12), perintah ini berhasil mengembalikan *file wasted* ke format aslinya, menjadi langkah kunci dalam pemulihan operasional.



Gambar 12 Proses dekripsi file menggunakan fungsi bawaan *ransomware*

4. KESIMPULAN DAN SARAN

Berdasarkan analisis forensik digital yang telah dilakukan terhadap insiden siber di PT. Satseet International, kesimpulan utama menunjukkan bahwa serangan ini merupakan sebuah serangan siber berlapis yang terorganisir dan berhasil karena adanya kelemahan pada fase *Preparation* keamanan siber perusahaan. Penelitian ini berhasil mencapai tujuannya dengan merekonstruksi seluruh rantai serangan menggunakan metode SANS. Rantai serangan teridentifikasi dimulai dari tahap pengintaian melalui *Directory Traversal*, yang kemudian membuka jalan bagi vektor masuk utama melalui rekayasa sosial dalam bentuk email *spear-phishing*. Keberhasilan metode ini membuktikan bahwa faktor manusia menjadi mata rantai terlemah dalam keamanan siber perusahaan. Penyerang secara efektif memanfaatkan kerentanan spesifik CVE-2022-30190 (Follina) untuk melakukan eksekusi kode jarak jauh, yang puncaknya adalah enkripsi data oleh *Ransomware* oleh kelompok peretas BlackPython Team dengan motif finansial.

Berdasarkan kesimpulan di atas, beberapa saran direkomendasikan sebagai bagian dari fase *Lessons Learned*. Untuk PT. Satseet International, disarankan untuk segera melakukan audit keamanan untuk memperbaiki celah *Directory Traversal*, mengimplementasikan solusi keamanan email tingkat lanjut, dan menerapkan kebijakan manajemen pembaruan sistem (*patch management*) yang ketat untuk menutup kerentanan yang diketahui seperti CVE-2022-30190. Selain itu, sangat penting untuk mengadakan program pelatihan kesadaran keamanan dan simulasi *phishing* secara rutin bagi seluruh karyawan. Adapun untuk penelitian selanjutnya, dapat dilakukan analisis *reverse engineering* terhadap *malware* yang ditemukan untuk mengembangkan indikator kompromi (IoC), melakukan studi komparatif antara metode SANS dengan kerangka kerja forensik lainnya, serta mengintegrasikan temuan dengan platform *Cyber Threat Intelligence* (CTI).

DAFTAR PUSTAKA

Adu-Manu, K., Ahiable, R., Mensah, E. and Sarpong, K., 2023. Phishing Attacks in Social Engineering: A Review. *Journal of Cyber Security*, 122, p.29. https://doi.org/10.32604/jcs.2023.041095.

Ali, M.P.D., Wirawan Muhammad, A., Zen, B.P., Kisworini, R.Y. and Rohayati, T., 2024. Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86. *Jurnal Sistem Informasi Galuh*, [online] 2(1), pp.44–54. https://doi.org/https://doi.org/10.25157/jsig.v2i1.3695.

Al-rimy, B., Maarof, M. and Shaid, S., 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, 74. https://doi.org/10.1016/j.cose.2018.01.001.

Audita, D., Lestari, P. and Fattah, F., 2025. Digital Forensic Analysis of Data Recovery in File Deletion Cases Using the National Institute of Standards and Technology (NIST) Method. *Journal homepage: AKIRATECH :*

Journal of Computer and Electrical Engineering, [online] 2(1). Available at: <https://journal.ajbnews.com/index.php/akiratech>.

Biswas, S., Sohel, M., Sajal, Md.M., Afrin, T., Bhuiyan, T. and Hassan, M.M., 2018. A Study on Remote Code Execution Vulnerability in Web Applications. In: *International Conference on Cyber Security and Computer Science (ICONCS'18)*.

Exabeam, 2025. *SANS Incident Response: 6-Step Process & Critical Best Practices | Exabeam*. [online] Available at: <https://www.exabeam.com/explainers/incident-response/sans-incident-response-6-step-process-critical-best-practices/> [Accessed 19 August 2025].

Firmansyah, R.A., 2025. *Framework Integrasi Digital Forensic Readiness dan Information* Security *Management System di lingkungan Pemerintahan*. [online] Available at: <https://dspace.uii.ac.id/bitstream/handle/123456789/55373/20917051.pdf> [Accessed 30 October 2025].

Fitriana, M., Ar, K. and Marsya, J., 2020. PENERAPANA METODE NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PENANGANAN CYBER CRIME. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 4, p.29. https://doi.org/10.22373/cj.v4i1.7241.

Gandotra, E., Bansal, D. and Sofat, S., 2014. Malware Analysis and Classification: A Survey. *Journal of Information Security*, 05, pp.56–64. https://doi.org/10.4236/jis.2014.52006.

Gian Aditya Asbath, R., Putra Anugrah, R. and Setiawan, A., 2025. ANALISIS DAMPAK RANSOMWARE PADA KEAMANAN DATA PERUSAHAAN DAN STRATEGI MITIGASINYA. *Jurnal Kumpulan Ilmu Komputer Dan Perubahan Digital*, [online] 1(1). Available at: <https://jurnal.prestasiku.org/index.php/kompid/article/download/29/33> [Accessed 19 August 2025].

Kent, K., Chevalier, S., Grance, T. and Dang, H., 2006. *Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology*. [online] National Institute of Standards and Technology. Available at: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf> [Accessed 30 July 2025].

Khalda, K. and Wibowo, D.K., 2025. Malware Behavior Analysis Using Static and Dynamic Analysis Approaches. *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, 4(1), pp.1–8. https://doi.org/10.20885/snati.v4.i1.1.

Montasari, R., 2016. Review and Assessment of the Existing Digital Forensic Investigation Process Models. *International Journal of Computer Applications*, 147(7), pp.41–49. https://doi.org/10.5120/IJCA2016911194.

Novita, A.P., Fatmanegara, F., Runtuwene, J.J., Samuela, J.T., Syahbani, M.F., Studi, P., Informasi, S. and Kunci, K., n.d. CYBER SECURITY THREATS; ANALISIS DAN MITIGASI RESIKO RANSOMWARE DI INDONESIA. *Jurnal Simasi : Jurnal Ilmiah Sistem Informasi*, [online] 3(1), pp.160–169. https://doi.org/10.46306/sm.v3i1.

Pratiwi, F.I., Hennida, C., Soesilowati, S., Berliantin, N., Ekasari, D.Y., Dewi, C.S. and Intan, A.A., 2024. Cybersecurity Challenges in Indonesia: Threat and Responses Analysis. *Perspectives on Global Development and Technology*, [online] 22(3–4), pp.239–264. https://doi.org/https://doi.org/10.1163/15691497-12341660.

Rafi, M., Ihsan, I. and Voutama, A., 2025. Penerapan Metode NIST Dalam Analisis Forensik Digital Pasca Serangan Siber (Studi Kasus : Pt.Analis Digital Forensik) 1. *Jurnal Cyber Security dan Forensic Digital*, 8(1), pp.53–62. https://doi.org/https://doi.org/10.14421/csecurity.2025.8.1.5092.

Ravindran, U. and Potukuchi, R.V., 2022. A Review on Web Application Vulnerability Assessment and Penetration Testing. *Review of Computer Engineering Studies*, 9(1), pp.1–22. https://doi.org/10.18280/rces.090101.

Sandrina Ayu, R., Marshell Rivai, M., Al Mubarak, N. and Pratama, D., 2025. KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI: ANALISIS ANCAMAN SIBER DAN PENDEKATAN MITIGASI. *Pediaqu : Jurnal Pendidikan Sosial dan Humaniora*, 4(2), pp.2598–2609.

SANS Institute, 2025. *Respons Insiden | Institut SANS*. [online] Available at: <https://www.sans.org/security-resources/glossary-of-terms/incident-response> [Accessed 19 August 2025].

Sophos, 2022. *Threat Alerts - Socura*. [online] Available at: <https://socura.co.uk/threat-alerts/> [Accessed 30 July 2025].

Zscaler, 2025. *What Is Double Extortion Ransomware? | Zscaler*. [online] Available at: <https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware> [Accessed 30 July 2025].