KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research (JSSR)
Vol.4, No.5 Oktober 2026
e-ISSN: 3025-9851, p-ISSN : 3025-986X, Hal 1208-1218
DOI : https://doi.org/10.61722/jssr.v4i5.12658

STUDI FORENSIK PERUBAHAN SISTEM AKIBAT EKSEKUSI FILE BERBAHAYA PADA WINDOWS MENGGUNAKAN EVENT LOG DAN PREFETCH

Muhammad Revi Akbar[1], Al-Khowarizmi[2]
[1,2] Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia
*Penulis Korespondensi: reviakbar46@gmail.com

Abstract. *Digital forensics on Windows requires correlation between artifacts to reconstruct program execution activities in a more structured manner. This study aims to analyze system changes related to program execution using Windows Event Log and Windows Prefetch and to develop a web-based application that integrates the analysis process. The research method follows the NIST SP 800-86 stages: collection, examination, analysis, and reporting. Testing was conducted on Windows 10 Pro 64-bit in a controlled virtual environment. The main artifacts, Security Event Log and Prefetch, were acquired, verified using MD5 and SHA-256 hashes, and processed by the application. The results show that 3,244 events were successfully processed from Security.evtx. Filtering identified Event ID 4688 recording the creation of the FORENSIC_TEST.exe process on 26 August 2026 at 09:55:33. The FORENSIC_TEST.EXE-D2028CEF.pf artifact recorded the same executable, a run count of 1, and an identical last run time. Correlation produced a 0-second time difference with a 100% (High) confidence score according to the application's scoring mechanism. These findings indicate that Event Log provides process-creation context, while Prefetch provides supporting evidence of program execution. Integrating both artifacts can assist investigators in constructing a more systematic activity timeline..*

Keywords: ***digital forensics, Windows Event Log, Prefetch, Event ID 4688, correlation, timeline***

Abstrak. Forensik digital pada sistem operasi Windows memerlukan korelasi antartefak agar aktivitas eksekusi program dapat direkonstruksi secara lebih terstruktur. Penelitian ini bertujuan menganalisis perubahan sistem akibat eksekusi program dengan memanfaatkan Windows Event Log dan Windows Prefetch serta mengembangkan aplikasi berbasis web untuk mengintegrasikan proses analisis. Metode penelitian mengacu pada tahapan NIST SP 800-86 yang meliputi collection, examination, analysis, dan reporting. Pengujian dilakukan pada Windows 10 Pro 64-bit dalam lingkungan virtual terkontrol. Artefak utama berupa Security Event Log dan Prefetch diakuisisi, diverifikasi menggunakan hash MD5 dan SHA-256, kemudian diproses oleh aplikasi. Hasil pengujian menunjukkan 3.244 event berhasil diproses dari Security.evtx. Penyaringan menemukan Event ID 4688 yang mencatat pembuatan proses FORENSIC_TEST.exe pada 26 Agustus 2026 pukul 09:55:33. Artefak FORENSIC_TEST.EXE-D2028CEF.pf mencatat executable yang sama, run count 1, dan last run time yang identik. Korelasi menghasilkan selisih waktu 0 detik dengan confidence 100% (High) berdasarkan mekanisme penilaian aplikasi. Hasil ini menunjukkan bahwa Event Log memberikan konteks pembuatan proses, sedangkan Prefetch memberikan bukti pendukung eksekusi program. Integrasi kedua artefak melalui aplikasi dapat membantu investigator menyusun timeline aktivitas secara lebih sistematis.

Kata kunci: **forensik digital, Windows Event Log, Prefetch, Event ID 4688, korelasi, timeline**

1. LATAR BELAKANG

Aktivitas pada sistem operasi Windows meninggalkan berbagai artefak digital yang dapat digunakan dalam proses investigasi. Artefak tersebut penting karena dapat memberikan informasi mengenai proses yang dijalankan, waktu kejadian, pengguna, dan perubahan yang muncul selama aktivitas sistem. Dalam investigasi insiden, pemeriksaan

Naskah Masuk:01 September 2026; Revisi: 02 September 2026; Diterima: 03 September 2026; Terbit: 10 September 2026

satu artefak saja dapat memberikan konteks yang terbatas sehingga diperlukan analisis lintas artefak untuk memperkuat rekonstruksi kejadian (Do et al., 2014; Shashidhar & Novak, 2015).

Windows Event Log merupakan salah satu sumber bukti yang merekam berbagai aktivitas sistem. Pada Security Event Log, Event ID 4688 dapat digunakan untuk mengidentifikasi pembuatan proses baru ketika audit process creation diaktifkan. Informasi ini relevan untuk mengetahui waktu dan nama proses yang dijalankan. Penelitian terdahulu menunjukkan bahwa Windows Event Log memiliki nilai penting dalam identifikasi aktivitas mencurigakan dan analisis malware (Sajan et al., 2025; Patil & Prabhu, 2025).

Selain Event Log, Windows Prefetch menyimpan informasi yang berkaitan dengan eksekusi aplikasi, seperti nama executable, waktu eksekusi, run count, dan file yang direferensikan. Shashidhar dan Novak (2015) menunjukkan bahwa Prefetch memiliki nilai forensik untuk mengidentifikasi riwayat eksekusi aplikasi. Namun, artefak digital dapat memiliki keterbatasan dan potensi manipulasi, sehingga interpretasi sebaiknya tidak hanya bergantung pada satu sumber bukti (Vanini et al., 2025).

Permasalahan yang diangkat dalam penelitian ini adalah bagaimana mengintegrasikan Event Log dan Prefetch dalam satu alur analisis sehingga investigator dapat melakukan pemeriksaan evidence, parsing, korelasi, dan penyusunan timeline secara lebih terstruktur. Penelitian mengembangkan aplikasi berbasis web yang mengolah kedua artefak dan melakukan korelasi berdasarkan nama executable serta kedekatan timestamp. Tujuan penelitian adalah mengidentifikasi perubahan sistem yang tercatat setelah aktivitas eksekusi program, menganalisis nilai forensik Event Log dan Prefetch, serta mengevaluasi kemampuan aplikasi dalam membantu rekonstruksi aktivitas Windows.

2. METODE PENELITIAN

Penelitian menggunakan pendekatan eksperimen terkontrol dan mengadaptasi NIST SP 800-86 sebagai kerangka kerja investigasi digital. Kerangka ini dipilih karena memberikan alur collection, examination, analysis, dan reporting yang dapat diterapkan pada pengelolaan bukti digital (Kent et al., 2006). Penerapan NIST SP 800-86 juga telah

digunakan dalam berbagai penelitian forensik digital dan dapat dikombinasikan dengan prinsip pengelolaan bukti pada ISO/IEC 27037 (Ramadhan et al., 2022; Faizal & Luthfi, 2024).

2.1 Lingkungan dan Skenario Pengujian

Pengujian dilakukan pada mesin virtual Windows 10 Pro 64-bit. Sebelum eksperimen, mesin virtual dikembalikan ke snapshot bersih untuk menjaga konsistensi kondisi awal. Audit Process Creation diaktifkan agar aktivitas pembuatan proses dapat direkam melalui Event ID 4688, sedangkan Windows Prefetch dipastikan aktif. FORENSIC_TEST.exe digunakan sebagai executable validasi yang aman untuk memastikan fungsi aplikasi dan mekanisme korelasi dapat diuji secara terkontrol.

Komponen	**Konfigurasi**
Sistem operasi	Windows 10 Pro 64-bit
Lingkungan	Oracle VirtualBox / virtual machine
Event Log utama	Windows Security Event Log (.evtx)
Event utama	Event ID 4688 - Process Creation
Artefak kedua	Windows Prefetch (.pf)
Executable validasi	FORENSIC_TEST.exe
Integritas evidence	MD5 dan SHA-256

2.2 Tahapan Analisis

Tahap NIST	**Aktivitas Penelitian**
Collection	Mengakuisisi Security.evtx dan file Prefetch dari lingkungan pengujian serta mencatat metadata evidence.
Examination	Memverifikasi integritas evidence, melakukan parsing EVTX dan PF, serta menormalisasi field yang diperlukan.

Analysis	Menyaring Event ID 4688, menganalisis metadata Prefetch, membandingkan executable dan timestamp, kemudian melakukan korelasi.
Reporting	Menyajikan hasil dalam dashboard, tabel korelasi, timeline aktivitas, dan laporan hasil analisis.

2.3 Mekanisme Korelasi

Korelasi dilakukan dengan menormalisasi nama executable dan membandingkan timestamp Event Log dengan last run time Prefetch. Hasil yang menunjukkan kecocokan nama executable pada Event ID 4688 dan Prefetch dikategorikan sebagai Process Creation + Prefetch. Aplikasi memberikan confidence score berdasarkan kedekatan waktu dan kecocokan parameter. Nilai confidence merupakan skor internal mekanisme aplikasi, bukan probabilitas bahwa executable tersebut merupakan malware. Timeline kemudian disusun untuk menampilkan hubungan temporal antartefak.

2.4 Pengembangan Aplikasi

Aplikasi dikembangkan berbasis web dengan modul autentikasi, pengelolaan kasus, evidence, Event Log, Prefetch, correlation, timeline, dan laporan. Model Waterfall digunakan untuk mendukung tahapan pengembangan yang terstruktur dari analisis kebutuhan hingga pengujian fungsi (Anis et al., 2023). Evidence yang diunggah disimpan bersama metadata dan nilai hash untuk mendukung pemeriksaan integritas.

3. HASIL DAN PEMBAHASAN

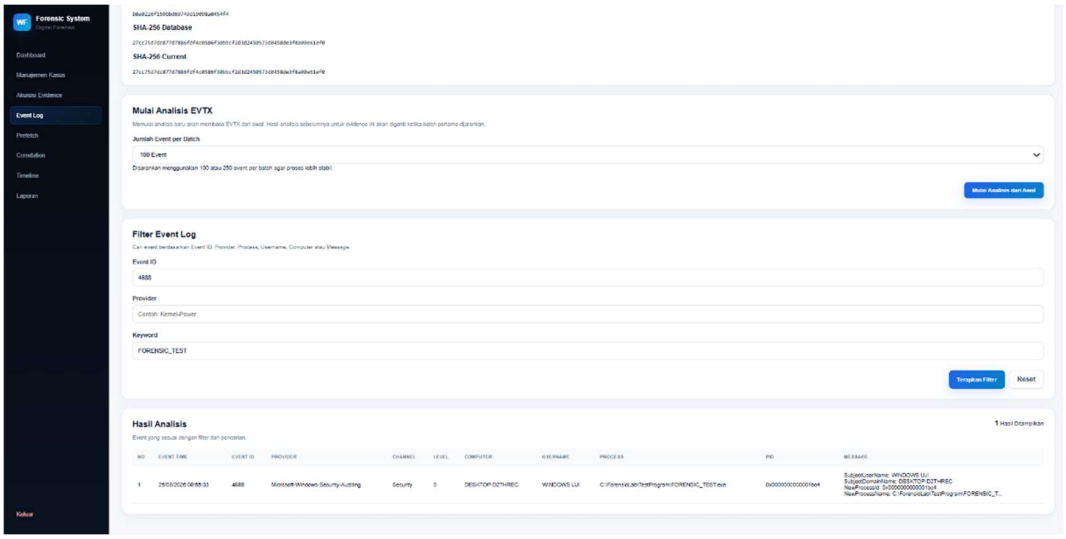
3.1 Akuisisi dan Integritas Evidence

Artefak utama yang dianalisis adalah Security.evtx dan FORENSIC_TEST.EXE-D2028CEF.pf. Sistem menghitung nilai MD5 dan SHA-256 pada evidence. Pemeriksaan integritas menunjukkan evidence yang dianalisis memiliki nilai hash yang sesuai dengan data akuisisi, sehingga dapat digunakan pada tahap pemeriksaan dan analisis tanpa indikasi perubahan selama proses pengolahan.

Evidence	**Ukuran**	**SHA-256**

Security.evtx	3.215.360 byte	27CC75D7DC877D7886FDF4C0586F30BBCF2D3D2450573D0458DE3F8A00E61EF0
FORENSIC_TEST.EXE-D2028CEF.pf	3.808 byte	CC004292E9E5B146D103CAA0A2D6756BD6B30854EAA7E8EA4B30520182BAA6B0

3.2 Hasil Analisis Windows Event Log



GAMBAR 1 - Hasil parsing Event Log / Event ID 4688

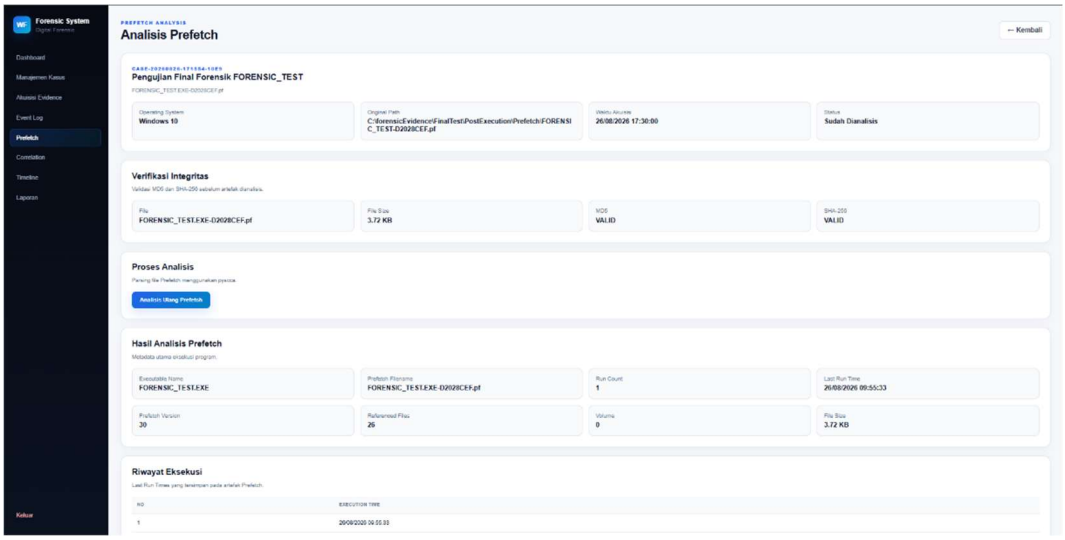
Pemrosesan Security.evtx menghasilkan 3.244 event. Jumlah tersebut merupakan keseluruhan event dalam evidence dan tidak seluruhnya berkaitan langsung dengan executable yang menjadi objek validasi. Oleh karena itu, dilakukan filtering terhadap Event ID 4688 dan keyword FORENSIC_TEST. Hasil penyaringan menemukan satu event yang berhubungan langsung dengan executable tersebut.

Parameter	**Hasil**
Event ID	4688
Provider	Microsoft-Windows-Security-Auditing
Aktivitas	Process Creation
Executable	FORENSIC_TEST.exe

Timestamp	26/08/2026 09:55:33

Temuan Event ID 4688 menunjukkan bahwa Windows mencatat pembuatan proses FORENSIC_TEST.exe pada timestamp pengujian. Event Log dalam konteks ini memberikan informasi mengenai kejadian process creation dan menjadi salah satu titik utama untuk dibandingkan dengan artefak Prefetch.

3.3 Hasil Analisis Windows Prefetch



GAMBAR 2 - Hasil analisis FORENSIC_TEST.EXE-D2028CEF.pf

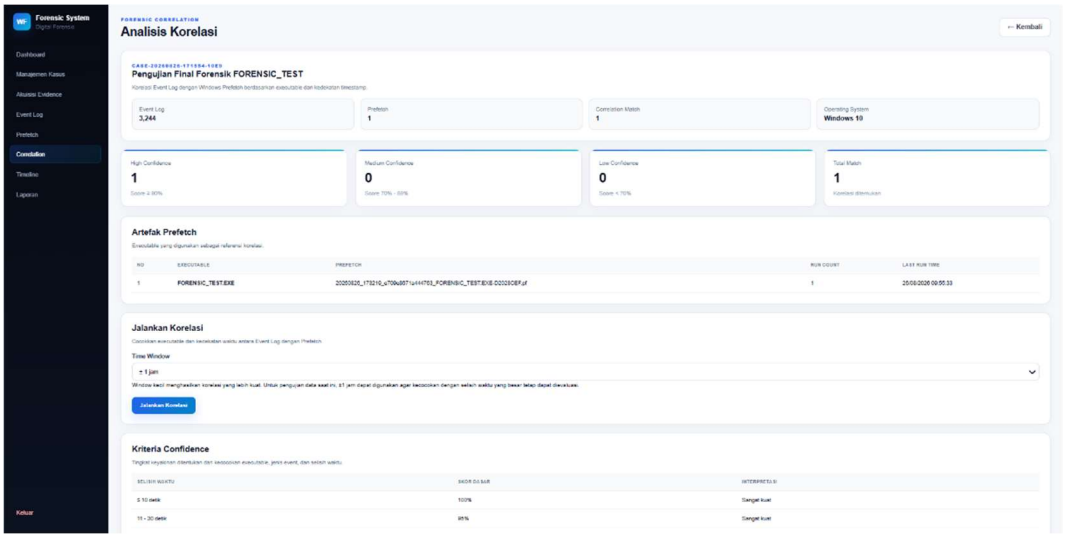
Parsing file FORENSIC_TEST.EXE-D2028CEF.pf menghasilkan informasi executable name, last run time, run count, versi Prefetch, volume, serta referenced files. Last run time yang diperoleh sama dengan timestamp Event ID 4688, yaitu 26/08/2026 09:55:33.

Parameter	**Hasil**
Prefetch filename	FORENSIC_TEST.EXE-D2028CEF.pf
Executable name	FORENSIC_TEST.EXE
Last run time	26/08/2026 09:55:33
Run count	1
Prefetch version	30
Volume count	1

Referenced files	22
Ukuran	3.72 KB / 3.808 byte

Run count 1 menunjukkan jumlah eksekusi yang tercatat pada artefak yang dianalisis. Keberadaan FORENSIC_TEST.EXE pada referenced files juga mendukung hubungan antara file Prefetch dengan executable yang diuji. Prefetch memberikan informasi yang berbeda tetapi saling melengkapi dengan Event Log.

3.4 Hasil Korelasi Event Log dan Prefetch



GAMBAR 3 - Hasil correlation: selisih 0 detik, confidence 100%

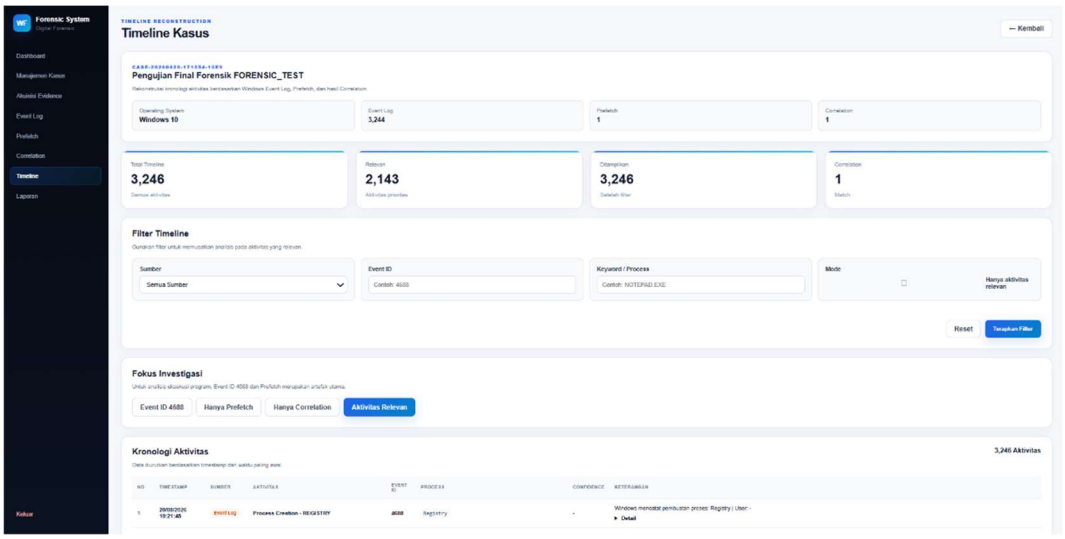
Hasil korelasi menunjukkan Event ID 4688 dan Prefetch mengarah pada executable yang sama. Timestamp kedua artefak identik sehingga diperoleh selisih waktu 0 detik. Berdasarkan mekanisme penilaian pada aplikasi, kondisi tersebut menghasilkan confidence 100% dengan level High.

Parameter Korelasi	**Hasil**
Executable Event Log	FORENSIC_TEST.exe
Executable Prefetch	FORENSIC_TEST.EXE
Timestamp Event Log	26/08/2026 09:55:33
Last Run Time Prefetch	26/08/2026 09:55:33
Selisih waktu	0 detik

Jumlah korelasi	1
Confidence	100% (High)
Tipe korelasi	Process Creation + Prefetch

Korelasi ini menunjukkan fungsi saling melengkapi kedua artefak. Event Log memberikan bukti bahwa Windows membuat proses FORENSIC_TEST.exe, sedangkan Prefetch memberikan bukti pendukung berupa artefak executable dan waktu terakhir program dijalankan. Confidence 100% harus dipahami sebagai hasil mekanisme pencocokan aplikasi berdasarkan executable dan timestamp, bukan tingkat kepastian universal bahwa suatu aktivitas merupakan malware.

3.5 Rekonstruksi Timeline



GAMBAR 4 - Timeline Event Log dan Prefetch

Timeline digunakan untuk menyusun aktivitas yang relevan secara kronologis. Dari keseluruhan aktivitas yang diproses, filter terhadap FORENSIC_TEST.EXE menghasilkan dua titik informasi pada timestamp yang sama: Event ID 4688 dan last run time Prefetch. Rekonstruksi dapat diringkas sebagai: eksekusi executable → Process Creation Event ID 4688 → pembentukan/aktivitas artefak Prefetch → korelasi timestamp → rekonstruksi aktivitas.

Waktu	**Sumber**	**Aktivitas**

26/08/2026 09:55:33	Security Event Log	Event ID 4688 - Process Creation FORENSIC_TEST.exe
26/08/2026 09:55:33	Windows Prefetch	Last Run Time FORENSIC_TEST.EXE

3.6 Pembahasan

Hasil penelitian memperlihatkan bahwa pemeriksaan Event Log dan Prefetch secara bersama dapat memberikan konteks yang lebih lengkap daripada penggunaan satu artefak. Temuan ini konsisten dengan karakteristik Event Log sebagai sumber peristiwa sistem dan Prefetch sebagai artefak riwayat eksekusi aplikasi (Do et al., 2014; Shashidhar & Novak, 2015). Korelasi berbasis executable dan timestamp mempermudah penyaringan informasi yang relevan dari ribuan event yang tersedia.

Aplikasi yang dikembangkan tidak berfungsi sebagai antivirus atau sistem klasifikasi malware. Fungsi utamanya adalah membantu investigator mengelola evidence, melakukan parsing, memeriksa integritas, mengorelasikan artefak, dan menyusun timeline. Oleh karena itu, kesimpulan mengenai sifat berbahaya suatu file harus tetap mempertimbangkan konteks eksperimen dan sumber identifikasi sampel. Pendekatan multi-artefak juga penting karena artefak forensik memiliki keterbatasan dan dapat dipengaruhi konfigurasi sistem, retensi log, maupun manipulasi (Vanini et al., 2025).

Dari sisi implementasi, aplikasi berhasil mengintegrasikan alur kerja yang sebelumnya dapat dilakukan melalui beberapa tahap terpisah. Penyajian hasil korelasi dan timeline membantu investigator melihat hubungan antara process creation pada Event Log dan riwayat eksekusi pada Prefetch secara lebih cepat. Meski demikian, penelitian dibatasi pada Windows 10 Pro 64-bit dan dua jenis artefak utama, sehingga generalisasi ke versi Windows lain atau artefak lain masih memerlukan pengujian lanjutan.

4. KESIMPULAN DAN SARAN

KESIMPULAN

Penelitian menunjukkan bahwa Windows Event Log dan Windows Prefetch dapat digunakan secara terintegrasi untuk mengidentifikasi dan merekonstruksi aktivitas eksekusi program pada Windows. Dari Security.evtx, aplikasi memproses 3.244 event

dan menemukan Event ID 4688 yang mencatat FORENSIC_TEST.exe pada 26 Agustus 2026 pukul 09:55:33. Prefetch mencatat executable yang sama dengan run count 1 dan last run time identik. Korelasi menghasilkan satu pasangan artefak dengan selisih waktu 0 detik dan confidence 100% (High) berdasarkan mekanisme aplikasi. Event Log memberikan konteks process creation, sedangkan Prefetch menjadi bukti pendukung riwayat eksekusi. Aplikasi berbasis web yang dikembangkan mampu mengintegrasikan pengelolaan evidence, verifikasi integritas, parsing, korelasi, timeline, dan laporan sehingga proses analisis menjadi lebih terstruktur.

SARAN

Penelitian selanjutnya dapat menambahkan artefak Windows lain seperti Registry, Amcache, ShimCache, SRUM, dan memory dump agar rekonstruksi aktivitas tidak hanya bergantung pada Event Log dan Prefetch. Pengujian juga dapat diperluas pada versi Windows dan skenario eksekusi yang berbeda. Mekanisme confidence dapat dikembangkan dengan lebih banyak parameter, sedangkan aplikasi dapat ditingkatkan melalui visualisasi timeline yang lebih interaktif, filtering lanjutan, dan integrasi analisis artefak tambahan.

DAFTAR REFERENSI

Adzirudin, A. A., Adiyatma, G. A., Putra, R. P., & Wibawa, T. A. H. (2025). Analisis forensik digital aplikasi Signal Desktop pada Windows 11 menggunakan metodologi forensik digital berbasis ISO/IEC 27037:2012 dan ISO/IEC 27042:2015. Cyber Security dan Forensik Digital, 8(2), 124–134. https://doi.org/10.14421/csecurity.2025.8.2.5387

Anis, Y., Mukti, A. B., & Rosyid, A. N. (2023). Penerapan model Waterfall dalam pengembangan sistem informasi aset destinasi wisata berbasis website. KLIK: Kajian Ilmiah Informatika dan Komputer, 4(2), 1134–1142. https://doi.org/10.30865/klik.v4i2.1287

Dalimunthe, A. A. Q. A., & Azhari, M. (2025). Analisis forensik digital terhadap perdagangan data pribadi di Dark Web menggunakan OSINT & Threat Intelligence. Jurnal Komputer Teknologi Informasi Sistem Komputer (JUKTISI), 4(1), 254–268. https://doi.org/10.62712/juktisi.v4i1.400

Do, Q., Martini, B., Looi, J., Wang, Y., & Choo, K.-K. R. (2014). Windows event forensic process. In Advances in Digital Forensics X (pp. 87–100). Springer. https://doi.org/10.1007/978-3-662-44952-3_7

Faizal, A., & Luthfi, A. (2024). Comparison study of NIST SP 800-86 and ISO/IEC 27037 standards as a framework for digital forensic evidence analysis. Journal of

Information Systems and Informatics, 6(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Hapsari, N. P., & Zen, B. P. (2024). Application of the NIST 800-86 framework to forensic digital evidence for Signal and Litmatch. Journal of Innovation Information Technology and Application (JINITA), 6(1), 1–11. https://doi.org/10.35970/jinita.v6i1.2025

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Kustian, N., Fathudin, D., & Ambarsari, E. W. (2022). Penggunaan Event Viewer pada Windows dalam menemukan masalah. Semnas Ristek, 6(1). https://doi.org/10.30998/semnasristek.v6i1.5826

Musthofa, D. M. (2026). Analisis forensik Windows Timeline untuk rekonstruksi aktivitas pengguna berbasis NIST SP 800-86. Info Kripto, 20(1). https://doi.org/10.56706/ik.v20i1.157

Patil, D., & Prabhu, A. (2025). Malware detection through memory forensics and Windows Event Log analysis. The International Arab Journal of Information Technology, 22(6), 1095–1111. https://doi.org/10.34028/iajit/22/6/5

Rahman, R., Nur Inayah, F. M., & Apriyani, D. (2026). Analisis digital forensik pada insiden serangan malware di sistem operasi. INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer, 1(3), 268–280.

Ramadhan, R. A., Setiawan, P. R., & Hariyadi, D. (2022). Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on ISO/IEC 27037:2012 and NIST SP800-86 framework. IT Journal Research and Development, 6(2), 162–168. https://doi.org/10.25299/itjrd.2022.8968

Sajan, P. P., Rajesh, A. R., Jenani, S., Milina, S. S., Vaishnavi Devi, R., & Vishnu Prabha, P. (2025). Analytical study on forensic relevance of Windows Event Logs. International Journal for Research in Applied Science & Engineering Technology, 13(7), 308–315. https://doi.org/10.22214/ijraset.2025.72991

Shashidhar, N., & Novak, D. (2015). Digital forensic analysis on Prefetch files. International Journal of Information Security Science, 4(2), 39–49.

Vanini, C., Hargreaves, C., & Breitinger, F. (2025). Evaluating tamper resistance of digital forensic artifacts during event reconstruction. Digital Threats: Research and Practice, 6(4), Article 29, 1–16. https://doi.org/10.1145/3765627