Analisis Forensik Windows Timeline untuk Rekonstruksi Aktivitas Pengguna Berbasis NIST SP 800-86

Dika Maulidal Musthofa
Teknologi Informasi, Fakultas Informatika, Universitas Telkom Surabaya, me.dikamaulidal@gmail.com

Riwayat Artikel

Dikirim 17 Feb 2026
Diterima 13 Apr 2026
Diterbitkan 28 Apr 2026

Kata kunci:

Forensik Digital
Windows Timeline
NIST SP 800-86
ActivitiesCache.db
KAPE

Keywords:

Digital Forensics
Windows Timeline
NIST SP 800-86
ActivitiesCache.db
KAPE

Abstrak

Penelitian ini mengevaluasi karakteristik artefak *Windows Timeline* dalam mendukung rekonstruksi aktivitas pengguna berdasarkan kerangka kerja NIST SP 800-86 melalui pendekatan perbandingan dengan *ground truth* pada skenario terkontrol. Eksperimen dilakukan dalam lingkungan terbatas dengan sembilan aktivitas tunggal yang mencakup penggunaan aplikasi perkantoran, peramban, dan clipboard untuk mengamati kesesuaian data yang dihasilkan dalam basis data *ActivitiesCache.db*. Hasil menunjukkan adanya konsistensi temporal yang tinggi pada informasi waktu (*timestamp*) antara artefak *dan ground truth*, meskipun ditemukan keterbatasan pada kelengkapan data seperti tidak selalu tersedianya detail konten atau URL spesifik. Temuan ini mengindikasikan bahwa artefak *Windows Timeline* berpotensi menjadi sumber informasi pendukung dalam analisis forensik digital, namun belum dapat digunakan sebagai satu-satunya dasar pembuktian. Dengan mempertimbangkan keterbatasan jumlah sampel, variasi perangkat, dan kondisi sistem yang belum merepresentasikan lingkungan nyata, penelitian ini bersifat eksploratif dan memerlukan pengujian lanjutan dengan skenario yang lebih kompleks dan beragam.

Abstract

This study evaluates the characteristics of Windows Timeline artifacts for supporting user activity reconstruction, based on the NIST SP 800-86 framework, by comparing them with ground truth under controlled scenarios. The experiment was conducted in a limited environment with nine discrete activities, including office applications, web browsing, and clipboard usage, to examine the consistency of data stored in the ActivitiesCache.db database. The results indicate initial consistency in timestamp information between the artifacts and the ground truth, although limitations in data completeness were observed, such as the absence of detailed content or specific URLs. These findings suggest that Windows Timeline artifacts have potential as a supplementary source in digital forensic analysis, but cannot be relied upon as a sole source of evidence. Given the limited sample size, single-device setup, and lack of real-world system variability, this study is exploratory and requires further validation in more diverse and complex scenarios.

1. PENDAHULUAN

Perkembangan sistem operasi Windows yang masif membawa tantangan baru dalam bidang forensik digital, terutama dalam hal rekonstruksi aktivitas pengguna. Salah satu artefak paling signifikan yang diperkenalkan sejak Windows 10 versi 1803 adalah *Windows Timeline* [1]. Fitur ini terintegrasi langsung dengan antarmuka Task View yang dapat diakses oleh pengguna melalui pintasan tombol Windows + Tab pada *keyboard*. Fitur ini dirancang untuk meningkatkan produktivitas dengan merekam riwayat aplikasi, dokumen, dan situs web yang diakses pengguna dalam rentang waktu 30 hari terakhir [2]. Namun, bagi investigator forensik, fitur ini merupakan sumber bukti digital yang sangat kaya karena mampu memberikan gambaran kronologis mengenai perilaku pengguna di masa lalu [3].

Data utama *Windows Timeline* disimpan dalam basis data SQLite bernama *ActivitiesCache.db* [4]. Penelitian sebelumnya menunjukkan bahwa database ini tidak hanya mencatat waktu eksekusi aplikasi, tetapi juga rincian spesifik seperti konten *clipboard* melalui *Activity Type* 16 [5]. Meskipun memberikan peluang besar untuk investigasi, sifat dinamis dari database ini menuntut metode penanganan bukti yang ketat agar integritas data tetap terjaga. Ketidakakuratan dalam penanganan bukti dapat menyebabkan hilangnya detail penting atau perubahan pada *timestamp* yang krusial bagi validitas rekonstruksi kejadian [6].

Untuk mengatasi tantangan tersebut, penelitian ini menerapkan kerangka kerja NIST SP 800-86 (*Guide to Integrating Forensic Techniques into Incident Response*) [7]. Standar ini menyediakan metodologi sistematis yang mencakup tahap *Collection, Examination, Analysis,* dan *Reporting* untuk memastikan bahwa setiap temuan teknis memiliki landasan ilmiah yang kuat [8]. Penggunaan *framework* ini krusial untuk menjaga rantai bukti (*chain of custody*) saat berhadapan dengan artefak yang sering berubah seperti pada Windows 10 [9].

Beberapa penelitian terbaru telah mulai mengeksplorasi artefak *timeline* pada versi Windows yang lebih baru, termasuk tantangan yang muncul akibat perbedaan fitur keamanan dan skema sinkronisasi antara Windows 10 dan Windows 11 [10]. Meskipun evolusi sistem operasi terus berlanjut, Windows 10 Pro versi 22H2 masih digunakan secara masif di berbagai sektor, sehingga pemahaman mendalam mengenai artefak aktivitasnya tetap menjadi kebutuhan krusial [11]. Saat ini, masih diperlukan analisis yang secara spesifik membandingkan hasil ekstraksi artefak secara langsung dengan catatan aktivitas manual (*ground truth*) dalam skenario terkontrol guna membuktikan tingkat akurasi temporal dan reliabilitas artefak ini secara presisi. Oleh karena itu, penelitian ini bertujuan untuk melakukan analisis forensik pada *Windows Timeline* menggunakan pendekatan eksperimen laboratorium guna merekonstruksi aktivitas pengguna dengan akurasi tinggi. Hasil dari penelitian ini diharapkan dapat memberikan panduan teknis bagi praktisi forensik dalam memanfaatkan *ActivitiesCache.db* sebagai bukti yang reliabel dan autentik [12].

2. LANDASAN TEORI

2.1. Forensik Digital

Forensik digital didefinisikan sebagai penerapan prinsip-prinsip ilmiah untuk pemulihan, identifikasi, dan analisis bukti digital guna merekonstruksi peristiwa masa lalu [8]. Fokus utamanya adalah menjaga integritas bukti melalui prosedur yang terdokumentasi dengan baik agar temuan dapat diterima dalam proses hukum maupun teknis.

2.2. Framework NIST SP 800-86

Standar NIST SP 800-86 menyediakan metodologi sistematis yang terbagi menjadi empat fase utama: *Collection* (pengumpulan data), *Examination* (pemeriksaan teknis), *Analysis* (penarikan kesimpulan), dan *Reporting* (pelaporan temuan) [7]. Kerangka kerja ini menekankan integrasi teknik forensik ke dalam respons insiden untuk meminimalkan risiko kontaminasi data.

2.3. Windows Timeline

Windows Timeline adalah fitur yang diperkenalkan sejak Windows 10 (versi 1803) untuk menyimpan riwayat aktivitas pengguna hingga 30 hari [2]. Artefak ini secara otomatis mencatat

interaksi pengguna terhadap aplikasi, file, dan situs web, yang kemudian disimpan secara lokal maupun disinkronkan ke akun Microsoft pengguna [1].

2.4. Artefak ActivitiesCache.db dan Mekanisme SQLite

Seluruh data *timeline* disimpan dalam database SQLite bernama *ActivitiesCache.db* yang terletak di direktori profil pengguna [4]. Mekanisme penyimpanan SQLite menggunakan tabel-tabel terelasi yang mencatat ID aplikasi, stempel waktu, dan detail aktivitas dalam format JSON pada kolom *payload* [12]. Artefak pendukung seperti berkas -wal (*Write-Ahead Log*) dan -shm (*Shared Memory*) juga krusial karena sering kali menyimpan data aktivitas terbaru yang belum ditulis sepenuhnya ke database utama.

2.5. Klasifikasi Activity Type

Windows mengklasifikasikan aktivitas menggunakan kode numerik yang unik. Beberapa tipe kunci dalam penelitian ini meliputi:

- Tipe 5 (ExecuteOpen)**:** Mencatat saat aplikasi atau dokumen pertama kali dibuka [3].
- Tipe 6 (InFocus)**:** Menunjukkan durasi aktif pengguna berinteraksi dengan jendela aplikasi tertentu [2].
- Tipe 16 (Clipboard)**:** Berfungsi sebagai indikator aktivitas salin-tempel (*copy-paste*). Berdasarkan studi terbaru, tipe ini menyimpan metadata aktivitas seperti waktu dan aplikasi sumber, sementara konten isinya sering kali tersimpan secara terpisah melalui mekanisme *Cloud Clipboard* atau *Clipboard History* (Win+V) [5]. Jika fitur riwayat aktif, konten tersebut dapat disinkronkan dan dianalisis lebih lanjut untuk mendapatkan nilai bukti yang lebih mendalam [1].

2.6. Integritas Data dan Validasi Hash

Menjaga autentisitas bukti digital memerlukan penggunaan fungsi *hashing* kriptografis seperti SHA-1. Nilai *hash* bertindak sebagai sidik jari digital unik; perubahan sekecil apa pun pada file akan menghasilkan nilai *hash* yang berbeda, sehingga menjamin bahwa artefak tidak mengalami modifikasi selama proses investigasi [9].

2.7. Perangkat Lunak Forensik (Software Tools)

Penelitian ini memanfaatkan perangkat lunak terspesialisasi seperti KAPE untuk akuisisi artefak yang cepat dan terstandarisasi, serta WxTCmd untuk melakukan *parsing* terhadap database SQLite yang kompleks menjadi format yang dapat dianalisis manusia. Timeline Explorer digunakan untuk memvisualisasi data guna mempermudah proses pemfilteran berdasarkan kronologi.

2.8. *Ground Truth* dan Validasi Eksperimen

Ground truth merupakan rekaman aktivitas manual yang dilakukan oleh peneliti selama eksperimen terkontrol. Validasi dilakukan dengan membandingkan data *ground truth* terhadap hasil ekstraksi artefak untuk mengukur tingkat akurasi dan presisi sistem dalam mencatat kejadian riil [11].

2.9. Analisis Temporal dan Micro-sequencing

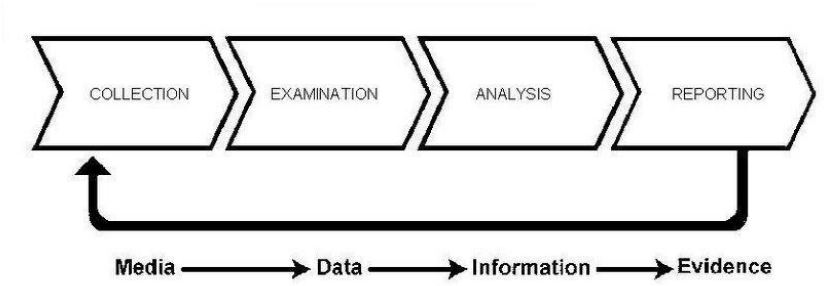
Analisis temporal melibatkan interpretasi stempel waktu (*timestamps*) dalam format UTC dan konversinya ke zona waktu lokal. *Micro-sequencing* adalah teknik untuk membedah urutan aktivitas yang terjadi dalam interval waktu yang sangat singkat (detik), yang memungkinkan investigator membedakan urutan kejadian logis meskipun terjadi hampir bersamaan [6].

3. METODE PENELITIAN

Penelitian ini menerapkan metode eksperimen laboratorium terkontrol dengan mengacu pada kerangka kerja NIST SP 800-86. Fokus utama penelitian ini adalah rekonstruksi kronologis aktivitas pengguna melalui analisis artefak *Windows Timeline* pada sistem operasi Windows 10 Pro 22H2.

3.1. Prosedur Kerja NIST SP 800-86

Alur penelitian disusun secara sistematis untuk menjamin integritas bukti digital dari fase akuisisi hingga pelaporan [7], sebagaimana diilustrasikan pada Gambar 1.



Gambar 1. Alur Penelitian Berbasis NIST SP 800-86

Rangkaian prosedur teknis yang dilakukan dalam penelitian ini mencakup empat pilar utama yang dirancang untuk menjaga autentisitas artefak. Prosedur tersebut dijabarkan sebagai berikut:

1. Collection**:** Akuisisi data dilakukan secara *live forensics* menggunakan alat KAPE. Target utama pengumpulan data adalah direktori profil pengguna pada path: *%LocalAppData%\ConnectedDevicesPlatform\L.<User>* untuk mengambil berkas utama *ActivitiesCache.db* beserta berkas pendukungnya (-wal dan -shm). Integritas bukti dijamin melalui pencatatan nilai hash SHA-1 segera setelah proses koleksi, untuk memastikan data mentah tidak mengalami modifikasi.
2. Examination**:** Berkas database SQLite yang bersifat biner diproses menggunakan tool WxTCmd. Proses ini bertujuan untuk melakukan *parsing* atau ekstraksi *record* aktivitas pengguna ke dalam format CSV agar dapat dianalisis secara tekstual tanpa mengubah kandungan data aslinya.
3. Analysis**:** Dilakukan identifikasi terhadap *Activity Type* kunci, yaitu Tipe 5 (*ExecuteOpen*), Tipe 6 (*InFocus*), dan Tipe 16 (*Clipboard metadata*). Seluruh stempel waktu (*timestamp*) asli yang tersimpan dalam format UTC dikonversi ke zona waktu lokal (WIB, UTC+7) guna memastikan sinkronisasi yang akurat dengan catatan aktivitas manual (*ground truth*).
4. Reporting**:** Menyusun temuan dalam bentuk tabel kronologis dan dokumentasi teknis. Tahap ini diakhiri dengan pengujian akurasi melalui perbandingan langsung antara hasil ekstraksi artefak dan log aktivitas manual yang telah didokumentasikan oleh peneliti.

3.2. Perangkat dan Spesifikasi Pengujian

Untuk mendukung validitas eksperimen, digunakan spesifikasi perangkat sebagaimana dirinci pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Penelitian

Kategori	Komponen/Software	Fungsi Teknis
Hardware	ThinkPad X270	Host target aktivitas dan objek forensik
Sistem Operasi	Windows 10 Pro 22H2	Lingkungan pengujian aktivitas
Acquisition	KAPE 1.3.0.2	Target-based artifact collection
Parsing	WxTCmd 1.1.0.0	Command-line SQLite parsing
Visualization	Timeline Explorer 2.1.0.0	Analisis temporal dan filtering data

3.3. Skenario Eksperimen dan Ground Truth

Skenario ini dirancang untuk menyimulasikan penggunaan komputer sehari-hari yang meninggalkan jejak pada *Windows Timeline*. Setiap tindakan didokumentasikan dalam *ground truth* sebagai standar pembanding akurasi, sebagaimana ditunjukkan pada Tabel 2.

Tabel 2. Rincian Skenario Aktivitas Terkontrol

Aktivitas	Jam Eksekusi (WIB)	Target Artefak	Deskripsi Tindakan
Manipulasi Dokumen	12:11:30 – 12:12:40	Tipe 5 & 6	Membuka dan menyunting DokumenUji.docx
Akses Materi PDF	12:13:10 - 12:14:10	Tipe 5 & 6	Membaca MateriUji.pdf via Microsoft Edge
Navigasi Website	12:14:30 - 12:15:40	Tipe 5 & 6	Akses Wikipedia dan interaksi halaman
Clipboard Event	12:16:50	Tipe 16	Salin teks dari Notepad ke Word

3.4. Metrik Evaluasi dan Analisis Kuantitatif

Analisis data dilakukan dengan membandingkan parameter temporal dan tingkat keberhasilan identifikasi artefak. Untuk mengukur tingkat akurasi hasil rekonstruksi aktivitas dari seluruh skenario eksperimen, digunakan perhitungan persentase akurasi sebagaimana pada persamaan (1).

$$Accuracy(\%) = \frac{Jumlah\ Aktivitas\ Terdeteksi}{Total\ Aktivitas\ Diuji} \times 100\% \quad (1)$$

di mana *Jumlah Aktivitas Terdeteksi* adalah jumlah aktivitas yang berhasil diidentifikasi berdasarkan kesesuaian *Activity Type* dengan skenario eksperimen, dan *Total Aktivitas Diuji* adalah jumlah keseluruhan aktivitas yang dilakukan selama pengujian.

Selanjutnya, perhitungan selisih waktu atau *time skew* dilakukan untuk mengevaluasi presisi temporal artefak menggunakan persamaan (2).

$$TimeSkew = \left| T_{\{ground\ truth\}} - T_{\{timeline\}} \right| \quad (2)$$

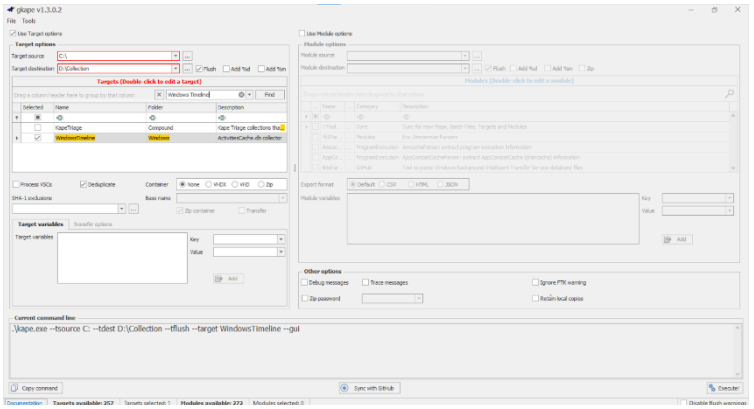
di mana *TimeSkew* adalah selisih waktu dalam satuan detik, $T_{\{ground\ truth\}}$ adalah stempel waktu aktivitas yang dicatat secara manual oleh peneliti, dan $T_{\{timeline\}}$ adalah stempel waktu yang tercatat pada artefak *ActivitiesCache.db* setelah dilakukan konversi ke zona waktu lokal (WIB). Parameter ini digunakan untuk mengevaluasi tingkat presisi temporal dalam merekonstruksi aktivitas pengguna.

4. HASIL DAN PEMBAHASAN

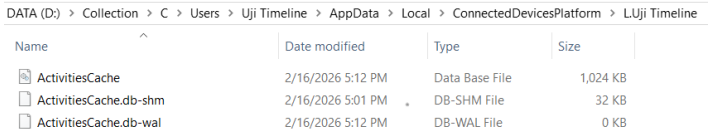
4.1. Tahap Pengumpulan (Collection)

Tahap ini berfokus pada identifikasi dan pengambilan data dari sistem target dengan tetap menjaga integritas bukti digital sesuai dengan kerangka kerja NIST SP 800-86. Akuisisi dilakukan secara *live forensics* pada laptop ThinkPad X270 menggunakan alat Kroll Artifact Parser and Extractor (KAPE). Proses koleksi dilakukan dengan menargetkan direktori profil pengguna untuk mengambil artefak utama ActivitiesCache.db beserta berkas pendukungnya, sebagaimana diilustrasikan pada Gambar 2 dan Gambar 3.

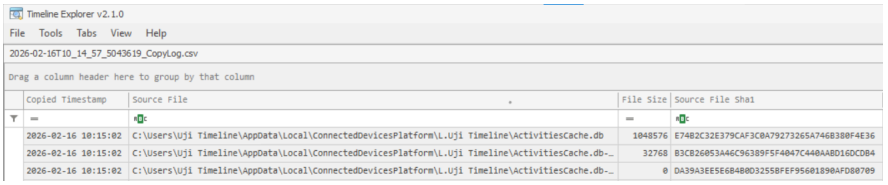
Selama proses akuisisi, integritas data dijamin melalui perhitungan nilai hash SHA-1 yang dilakukan secara otomatis oleh KAPE. Hal ini bertujuan untuk memastikan bahwa data mentah tetap autentik dan tidak mengalami modifikasi selama proses pemindahan, sesuai dengan prinsip dasar penanganan bukti digital. Hasil inventaris bukti dan verifikasi nilai *hash* dirinci pada Tabel 3, sementara dokumentasi log verifikasi ditunjukkan pada Gambar 4.



Gambar 2. Eksekusi Target-based Collection menggunakan KAPE



Gambar 3. Struktur direktori artefak pada sistem target



Gambar 4. Dokumentasi verifikasi nilai hash SHA-1 pada CopyLog

Berdasarkan hasil akuisisi, berkas *ActivitiesCache.db-wal* ditemukan berukuran 0 KB saat proses koleksi dilakukan. Kondisi ini menunjukkan tidak adanya log transaksi aktif pada mekanisme *Write-Ahead Log* SQLite saat proses akuisisi berlangsung, sehingga tidak terdapat data tambahan yang belum di-*commit* ke database utama. Meskipun demikian, nilai *hash* tetap dihitung untuk menjaga konsistensi verifikasi integritas bukti digital

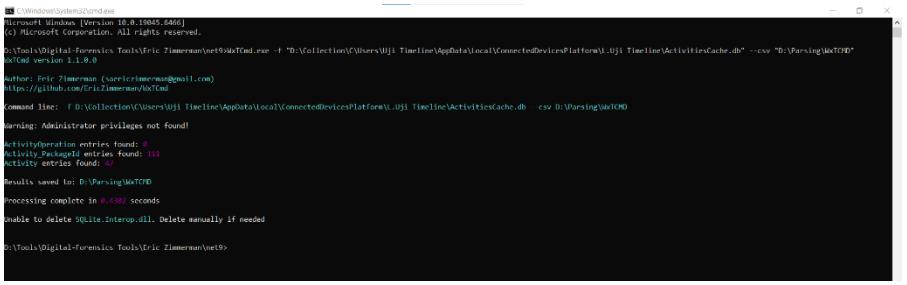
Tabel 3. Inventaris Bukti Digital dan Verifikasi Hash

Artefak	Ukuran	HASH (SHA-1)	Keterangan
ActivitiesCache.db	1,024 KB (1048576 Bytes)	E74B2C32E379CAF3C0A79273265A746B380F4E36	Database utama aktivitas
ActivitiesCache.db-shm	32 KB (32768 Bytes)	B3CB26053A46C96389F5F4047C440AABD16DCDB4	*Shared memory* SQLite
ActivitiesCache.db-wal	0 KB (0 Bytes)	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709	Log transaksi (*Write-Ahead Log*)

4.2. Tahap Pemeriksaan (Examination)

Tahap pemeriksaan melibatkan transformasi data biner menjadi format yang terstruktur agar dapat diinterpretasikan tanpa mengubah integritas konten aslinya. Artefak *ActivitiesCache.db* yang merupakan basis data SQLite diproses menggunakan alat WxTCmd 1.1.0.0 untuk mengekstraksi record aktivitas ke dalam format CSV. Perintah yang dieksekusi dalam proses ini adalah sebagai berikut:

WxTCmd.exe -f <path_to_ActivitiesCache.db> --csv <destination_folder>



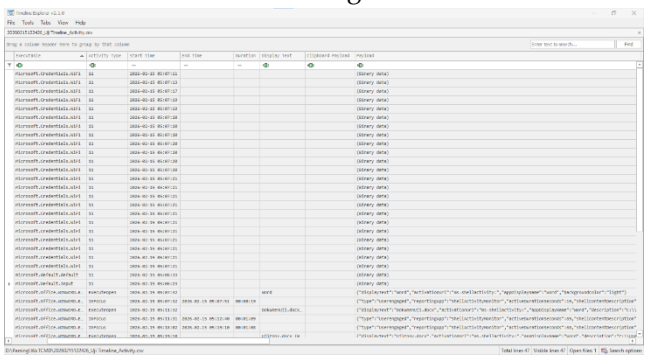
Gambar 5. Proses parsing database Windows Timeline menggunakan WxTCmd

Hasil ekstraksi ini menghasilkan sekumpulan data terstruktur yang memvalidasi parameter-parameter krusial seperti *Executable*, *ActivityType*, *StartTime*, *EndTime*, *DisplayText*, dan *Payload*. Ringkasan hasil ekstraksi awal ditunjukkan pada Tabel 4.

Tabel 4. Ekstraksi Data Hasil Examination

Executable	Activity Type	Start Time	End Time	Display Text	Payload
Microsoft.Default.Input	11	2026-02-15 05:06:23	-	-	(Binary data)
microsoft.default.default	11	2026-02-15 05:06:33	-	-	(Binary data)
MSEdge	ExecuteOpen	2026-02-15 05:07:02	-	*Microsoft Edge*	*JSON metadata*
Microsoft.Credentials.WiFi	11	2026-02-15 05:07:11	-	-	(Binary data)

Data hasil *parsing* tersebut kemudian divisualisasikan menggunakan Timeline Explorer 2.1.0.0. Penggunaan alat ini memudahkan investigator dalam memetakan urutan kejadian secara kronologis serta melakukan pemfilteran terhadap aktivitas sistem (seperti tipe 11) yang tidak relevan, sebelum dilakukan korelasi mendalam dengan catatan aktivitas manual (*ground truth*).



Gambar 6. Visualisasi timeline menggunakan Timeline Explorer

4.3. Tahap Analisis (Analysis)

Pada tahap ini, dilakukan analisis korelasi antara data hasil pemeriksaan dan catatan aktivitas manual (*ground truth*) untuk merekonstruksi kronologi aktivitas pengguna secara presisi. Seluruh stempel waktu (*timestamp*) yang tersimpan dalam format UTC pada database dikonversi ke Waktu Indonesia Barat (WIB, UTC+7) guna memastikan sinkronisasi yang akurat dengan catatan manual peneliti. Evaluasi presisi temporal dalam bentuk *time skew* pada setiap pengujian dihitung menggunakan Persamaan (2).

4.3.1. Analisis Dokumen Word

Analisis pada aktivitas manipulasi DokumenUji.docx menunjukkan bahwa *Windows Timeline* mencatat inisiasi file melalui Activity Type 5 (ExecuteOpen) dan durasi interaksi melalui Activity Type 6 (InFocus). Berdasarkan data pada berkas *ActivitiesCache.db*, aktivitas *InFocus* terekam mulai pukul 17:05:37 WIB.

Tabel 5. Korelasi Analisis Aktivitas Dokumen Word

Aktivitas	Ground Truth (WIB)	Timeline (WIB)	Selisih (Time Skew)
Buka Dokumen	17:05:35	17:05:37	2 Detik
Tutup Dokumen	17:06:30	17:06:31	1 Detik

Berdasarkan perhitungan pada Persamaan (2), terdeteksi selisih waktu (*time skew*) sebesar 2 detik pada saat pembukaan file dibandingkan dengan *ground truth*. Hal ini mengindikasikan adanya *write-latency* saat sistem melakukan *commit* data ke basis data SQLite. Sementara itu, pada saat penutupan dokumen, terdeteksi selisih waktu sebesar 1 detik. Rincian korelasi data disajikan pada Tabel 5. Hasil artefak *Activity Type* 5 dan 6 dapat dilihat pada Gambar 7.

Microsoft.Office.WINWORD.E…	InFocus	2026-02-16 10:05:37	2026-02-16 10:06:31	00:00:54	
Microsoft.Office.WINWORD.E…	ExecuteOpen	2026-02-16 10:05:45			DokumenUji.docx (Word)

Gambar 7. Artefak Activity Type 5 dan 6 pada pengujian Dokumen Word

4.3.2. Analisis Aktivitas File PDF

Analisis pada berkas MateriUji.pdf yang diakses menggunakan Microsoft Edge menunjukkan bahwa sistem merekam inisiasi dokumen melalui Activity Type 5 (ExecuteOpen**)** dan durasi penggunaannya melalui Activity Type 6 (InFocus). Berdasarkan data pada berkas *ActivitiesCache.db*, aktivitas inisiasi PDF terekam pada pukul 17:07:11 WIB.

Tabel 6. Korelasi Analisis Aktivitas File PDF

Aktivitas	Ground Truth (WIB)	Timeline (WIB)	Selisih (Time Skew)
Buka PDF	17:07:10	17:07:11	1 Detik
Tutup PDF	17:08:10	17:08:11	1 Detik

Berbeda dengan aplikasi pengolah kata, akses PDF menunjukkan selisih waktu (*time skew*) yang sangat minimal yakni 1 detik, terhadap *ground truth* berdasarkan hasil perhitungan Persamaan (2). Hal ini membuktikan bahwa *Windows Timeline* secara konsisten mampu merekam penggunaan aplikasi pihak ketiga maupun *built-in browser* sebagai pembaca dokumen dengan akurasi temporal yang sangat baik. Detail korelasi stempel waktu disajikan pada Tabel 6. Hasil Rekonstruksi durasi akses berkas PDF pada *Timeline Explorer* disajikan pada Gambar 8.

MSEdge	InFocus	2026-02-16 10:07:11	2026-02-16 10:08:11	00:01:00	
MSEdge	ExecuteOpen	2026-02-16 10:07:11			MateriUji.pdf (Microsoft …

Gambar 8. Rekonstruksi durasi akses berkas PDF pada Timeline Explorer

4.3.3. Analisis Navigasi Browser

Analisis aktivitas navigasi situs Wikipedia menunjukkan bahwa *Windows Timeline* merekam inisiasi peramban melalui Activity Type 5 (ExecuteOpen) dan durasi interaksi melalui Activity Type 6 (InFocus). Berdasarkan data pada berkas *ActivitiesCache.db*, aktivitas inisiasi Microsoft Edge terekam pada pukul 17:09:02 WIB.

Tabel 7. Korelasi Analisis Aktivitas Web Browser

Aktivitas	Ground Truth (WIB)	Timeline (WIB)	Selisih (Time Skew)
Buka Browser	17:09:00	17:09:02	2 Detik
Tutup Browser	17:10:00	17:10:01	1 Detik

Berdasarkan perhitungan pada Persamaan (2), terdeteksi selisih waktu (*time skew*) sebesar 2 detik pada saat pembukaan peramban dibandingkan dengan *ground truth*. Hal ini memperkuat indikasi adanya *write-latency* pada sistem saat melakukan penulisan data ke dalam basis data SQLite. Sementara itu, saat penutupan peramban yang dicatat melalui tipe *InFocus*, terdeteksi selisih waktu sebesar 1 detik. Meskipun demikian, kolom *payload* pada Windows 10 versi 22H2

terkadang tidak menyimpan URL secara lengkap, sehingga diperlukan korelasi dengan artefak *browser history* untuk hasil rekonstruksi yang komprehensif. Bukti riwayat penggunaan aplikasi browser pada *ActivitiesCache.db* disajikan pada Gambar 9.

Brave	ExecuteOpen	2026-02-16 10:09:02			Brave
Brave	InFocus	2026-02-16 10:09:02	2026-02-16 10:10:01	00:00:59	

Gambar 9. Bukti riwayat penggunaan aplikasi browser pada ActivitiesCache.db

4.3.4. Analisis Aktivitas Clipboard

Analisis aktivitas penyalinan teks dari Notepad ke Microsoft Word menunjukkan bahwa sistem secara konsisten mencatat inisiasi aplikasi melalui Activity Type 5 (ExecuteOpen) dan durasi penggunaannya melalui Activity Type 6 (InFocus). Aktivitas penyalinan teks tersebut terekam secara spesifik melalui Activity Type 16 (Clipboard) pada pukul 17:11:11 WIB.

Tabel 8. Korelasi Analisis Aktivitas Clipboard

Aktivitas	Ground Truth (WIB)	Timeline (WIB)	Selisih (Time Skew)
Buka Notepad	17:10:30	17:10:31	1 Detik
Tutup Notepad	17:11:42	17:11:43	1 Detik
Copy Teks	17:11:10	17:11:11	1 Detik

Berdasarkan perhitungan pada Persamaan (2), terdeteksi selisih waktu (*time skew*) yang konsisten sebesar 1 detik untuk seluruh rangkaian aktivitas dibandingkan dengan *ground truth*. Meskipun metadata waktu terekam dengan presisi tinggi, artefak ini hanya menyimpan riwayat eksekusi tanpa menyertakan isi konten yang disalin. Oleh karena itu, untuk mendapatkan isi konten, investigator dapat memanfaatkan fitur *Clipboard History* (Win+V) atau melakukan analisis memori tambahan jika fitur tersebut tidak tersedia. Detail korelasi stempel waktu disajikan pada Tabel 8. Hasil ekstraksi metadata tersebut disajikan pada Gambar 10.

System32\notepad.exe	InFocus	2026-02-16 10:10:31	2026-02-16 10:11:43	00:01:12	
System32\notepad.exe	CopyPaste	2026-02-16 10:11:11	2026-02-16 10:11:11		
System32\notepad.exe	ExecuteOpen	2026-02-16 10:10:31			Notepad

Gambar 10. Ekstraksi metadata Clipboard (Tipe 16) menggunakan Timeline Explorer

4.4. Tahap Pelaporan (Reporting)

Tahap akhir melibatkan penyajian temuan secara objektif untuk menjawab tujuan penelitian mengenai reliabilitas artefak *Windows Timeline*. Berdasarkan hasil korelasi antara data forensik dan ground truth, seluruh aktivitas pada skenario pengujian (9 dari 9 aktivitas) berhasil diidentifikasi dengan tepat.

Kriteria kesesuaian ditentukan berdasarkan tiga parameter utama, yaitu kesesuaian *Activity Type*, kesesuaian stempel waktu setelah konversi zona waktu, serta konsistensi urutan kronologis aktivitas. Tingkat keberhasilan identifikasi artefak dari seluruh skenario eksperimen dihitung menggunakan Persamaan (1). Variasi *time skew* yang terdeteksi berada dalam rentang 1–2 detik dan tidak memengaruhi identifikasi jenis maupun urutan kejadian.

Tabel 9. Rekapitulasi Akurasi Pelaporan

Parameter	Total Aktivitas	Terdeteksi	Tidak Terdeteksi	Akurasi
Dokumen Word	2	2	0	100 %
Akses PDF	2	2	0	100 %
Navigasi Browser	2	2	0	100 %
Clipboard Event	3	3	0	100 %
Total	**9**	**9**	**0**	**100 %**

Berdasarkan hasil yang dipaparkan pada Tabel 9, perhitungan menggunakan Persamaan (1) menunjukkan nilai akurasi sebesar 100% untuk semua kategori aktivitas yang diuji. Hal ini membuktikan bahwa *Windows Timeline* merupakan sumber bukti digital yang andal dalam ruang lingkup pengujian ini untuk merekonstruksi aktivitas pengguna pada sistem operasi Windows 10. Perlu dicatat bahwa nilai akurasi 100% ini harus dipahami dalam konteks skenario terkontrol yang terbatas dan tidak serta merta dapat digeneralisasi ke kondisi sistem nyata. Dalam skenario terbatas yang diuji, artefak menunjukkan konsistensi terhadap *ground truth*, namun belum dapat digeneralisasi.

4.5. Pembahasan

Hasil eksplorasi keterbatasan dan karakteristik artefak *Windows Timeline* dalam kondisi terkontrol menunjukkan konsistensi terhadap *ground truth*, namun belum dapat digeneralisasi. Pemanfaatan *Activity Type* 5, 6, dan 16 terbukti efektif dalam mengidentifikasi interaksi aplikasi serta metadata aktivitas *clipboard* secara spesifik. Korelasi waktu antara *ground truth* dan hasil *parsing* menunjukkan tingkat kesesuaian penuh dengan variasi *time skew* minor pada rentang 1–2 detik. Variasi tersebut tidak memengaruhi identifikasi jenis aktivitas maupun urutan kronologis kejadian, dan diduga kuat berkaitan dengan mekanisme *write-latency* pada sistem manajemen basis data SQLite.

Keterbatasan penelitian ini terletak pada ruang lingkup pengujian yang terbatas pada sistem operasi Windows 10 Pro 22H2 dengan satu akun pengguna lokal dalam lingkungan laboratorium. Selain itu, artefak *Windows Timeline* tidak selalu menyimpan konten aktivitas secara utuh, seperti URL lengkap atau isi teks *clipboard*, sehingga fungsinya lebih berperan sebagai penunjuk (*pointer*) aktivitas dibandingkan sebagai penyimpan konten utama. Meskipun demikian, kemampuan artefak dalam merekam urutan kejadian dengan presisi hingga satuan detik menunjukkan potensi *micro-sequencing* yang signifikan. Hal ini sangat relevan dalam investigasi forensik untuk memvalidasi secara akurat urutan perilaku pengguna dalam interval waktu yang sangat singkat.

5. KESIMPULAN

Berdasarkan hasil eksperimen dan analisis yang telah dilakukan, artefak yang tersimpan dalam berkas *Windows Timeline* yang tersimpan dalam berkas *ActivitiesCache.db* memiliki indikasi konsistensi terhadap aktivitas pengguna pada skenario pengujian yang terbatas dan terkontrol. Kesesuaian antara *ground truth* dan hasil ekstraksi pada sembilan aktivitas memberikan gambaran awal bahwa artefak ini dapat digunakan untuk membantu rekonstruksi kronologi aktivitas pengguna.

Meskipun demikian, temuan tersebut belum dapat digeneralisasi sebagai ukuran reliabilitas yang tinggi. Keterbatasan jumlah sampel, variasi skenario, serta penggunaan satu perangkat dan satu kondisi sistem menyebabkan hasil penelitian ini bersifat eksploratif dan belum merepresentasikan kondisi lingkungan yang dinamis.

Selain itu, analisis menunjukkan bahwa meskipun *timestamp* relatif konsisten, artefak ini memiliki keterbatasan dalam hal kelengkapan data, seperti URL spesifik atau isi clipboard yang tidak selalu tersedia. Oleh karena itu, *Windows Timeline* tidak dapat digunakan sebagai sumber bukti tunggal, melainkan perlu dikombinasikan dengan artefak forensik lainnya untuk memperoleh rekonstruksi yang lebih komprehensif.

Dengan demikian, penelitian ini diposisikan sebagai studi eksploratif awal mengenai karakteristik artefak *Windows Timeline*. Penelitian selanjutnya disarankan untuk memperluas jumlah dan variasi skenario pengujian, serta mempertimbangkan kondisi sistem yang lebih kompleks, termasuk pengaruh *background process* dan mekanisme penyimpanan SQLite, guna memperoleh validasi empiris yang lebih kuat.

REFERENSI

[1] D. V. Marziale, "An Incomplete Tour of the Windows 10 Activity Timeline," in *Proceedings of the Digital Forensic Research Conference (DFRWS 2019 USA)*, BlackBag Technologies, 2019. [Online]. Available: https://dfrws.org

[2] I. Mikhailov, "No Time to Waste," GROUP-IB. Accessed: Feb. 14, 2026. [Online]. Available: https://www.group-ib.com/blog/windows10-timeline-for-forensics/

[3] D. V. Marziale, "Exploring the Windows Activity Timeline, Part 1: The High Points," Cellebrite. Accessed: Feb. 14, 2026. [Online]. Available: https://cellebrite.com/en/blog/exploring-the-windows-activity-timeline-part-1-the-high-points/

[4] I. Shawahna, "Extracting Digital Artefacts from Windows 10 Timeline Activities Cache Database," *Researchgate*, 2022, [Online]. Available: https://www.researchgate.net/publication/357505459_Extracting_Digital_Artefacts_from_Windows_10_Timeline_Activities_Cache_Database

[5] D. V. Marziale, "Exploring the Windows Activity Timeline, Part 3: The Value of Clipboard Content," Cellebrite. Accessed: Feb. 14, 2026. [Online]. Available: https://cellebrite.com/en/blog/exploring-the-windows-activity-timeline-part-3-the-value-of-clipboard-content/

[6] F. Breitinger, H. Studiawan, and C. Hargreaves, "SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges," *Forensic Sci. Int. Digit. Investig.*, vol. 53, 2025, doi: 10.1016/j.fsidi.2025.301932.

[7] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.

[8] E. Casey, *Forensic Science, Computers, and the Internet*. 2011.

[9] N. Reddy, *Windows Forensics*. 2019. doi: 10.1007/978-1-4842-4460-9_2.

[10] A. Rathbun, "Windows 10 vs. Windows 11, What Has Changed?," 2022, *SANS Institute*.

[11] D. S. Jinu, L. K. Varghese, and S. Shaji, "Uncovering Digital Evidence through Timeline Artifact Analysis in Windows OS Systems," *Int. J. Recent Eng. Res. Dev.*, vol. 10, no. 2, pp. 13–19, 2025, doi: 10.56581/ijrerd.10.02.13-19.

[12] M. Owens, *The definitive guide to SQLite*. 2010. doi: 10.1007/978-1-4302-0172-4.