JSITIK, Vol.5 No.2 Juni 2027
ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Analisis Artefak Forensik Ransomware pada Sistem Operasi Windows 10 Menggunakan Autopsy Berdasarkan Metode NIST SP 800-86

Diterima:
03 Oktober 2026
Revisi:
19 Oktober 2026
Terbit:
1 November 2026

***Muhamad Fadillah, Harjono, Sigit Sugiyanto, Ermadi Satriya Wijaya**

Universitas Muhammadiyah Purwokerto

Abstrak— **Latar Belakang:** Ransomware merupakan ancaman keamanan data yang meninggalkan artefak digital untuk mendukung investigasi forensik. **Tujuan:** Penelitian ini bertujuan menganalisis artefak forensik simulasi ransomware Simran pada Windows 10 22H2 Home 64-bit menggunakan Autopsy berdasarkan NIST SP 800-86. **Metode:** Penelitian menggunakan eksperimen laboratorium dengan pendekatan *dead forensic* pada lingkungan virtual terisolasi. Tahapan meliputi *Collection*, *Examination*, *Analysis*, dan *Reporting*. **Hasil:** Simulasi ransomware mengubah ekstensi 22 file menjadi .locked dan menghasilkan *ransom note* README_RESTORE_FILES.txt. Metadata file menunjukkan perubahan pada pukul 16.40.36–16.40.37 WIB. Analisis *Prefetch* mengidentifikasi PYTHON3.EXE yang berkorelasi secara temporal dengan perubahan file. Analisis Regshot menemukan satu *registry key* terhapus, 42 *registry key* baru, 101 *registry value* baru, dan 82 *registry value* berubah. Pemeriksaan *Event Log* tidak menemukan bukti langsung eksekusi program maupun manipulasi log. **Kesimpulan:** Korelasi artefak *file system*, *Prefetch*, *Registry*, *Event Log*, dan *timeline* menggunakan Autopsy mendukung rekonstruksi aktivitas ransomware secara sistematis. Keterbatasan penelitian mencakup penggunaan program simulasi dan kedalaman analisis artefak sistem.
Kata Kunci— Forensik Digital; Ransomware Simran; Autopsy; NIST SP 800-86; Windows

Abstract— ***Background:*** *Ransomware is a data security threat that leaves digital artifacts that can support forensic investigations.* ***Objective:*** *This study aims to analyze forensic artifacts generated by the Simran ransomware simulation on Windows 10 22H2 Home 64-bit using Autopsy based on NIST SP 800-86.* ***Methods:*** *This study employed a laboratory experiment using a dead forensic approach in an isolated virtual environment. The stages included Collection, Examination, Analysis, and Reporting.* ***Results:*** *The ransomware simulation changed the extensions of 22 files to .locked and generated a ransom note named README_RESTORE_FILES.txt. File metadata indicated changes between 16:40:36 and 16:40:37 Western Indonesian Time (WIB). Prefetch analysis identified PYTHON3.EXE, which was temporally correlated with file modifications. Regshot analysis revealed one deleted registry key, 42 new registry keys, 101 new registry values, and 82 modified registry values. Event Log examination found no direct evidence of program execution or log manipulation.* ***Conclusion:*** *Correlating file system, Prefetch, Registry, Event Log, and timeline artifacts using Autopsy supports the systematic reconstruction of ransomware simulation activities. Limitations include the use of a simulation program and the limited depth of analysis of certain system artifacts.*
Keywords— *Digital Forensics; Simran Ransomware; Autopsy; NIST SP 800-86; Windows*

This is an open access article under the CC BY-SA License.

Penulis Korespondensi:

Muhamad Fadillah,
Program Studi Teknik Informatika,
Universitas Muhammadiyah Purwokerto,
Email: muhamadfadillah302@gmail.com

JSITIK, Vol.5 No.2 Juni 2027
ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

I. PENDAHULUAN

Perkembangan teknologi informasi memberikan berbagai manfaat dalam kehidupan sehari-hari, tetapi juga meningkatkan risiko terjadinya kejahatan siber. Salah satu ancaman yang perlu diperhatikan adalah ransomware, yaitu perangkat lunak berbahaya yang dapat membatasi akses terhadap data korban melalui proses enkripsi atau perubahan terhadap file. Aktivitas ransomware dapat meninggalkan jejak digital pada sistem operasi yang berpotensi digunakan untuk merekonstruksi kejadian dan mendukung proses investigasi forensik digital (Simanungkalit et al., 2024).

Investigasi forensik digital dilakukan untuk mengidentifikasi, mengumpulkan, memeriksa, dan menganalisis bukti digital secara sistematis. Pada sistem operasi Windows, artefak seperti file system, Prefetch, Registry, Event Log, dan timeline dapat memberikan informasi yang saling melengkapi mengenai aktivitas sistem. Analisis file system dapat menunjukkan perubahan pada file dan metadata, sedangkan Prefetch dapat memberikan petunjuk terkait aktivitas eksekusi program. Registry dan Event Log dapat digunakan sebagai sumber informasi pendukung, sementara korelasi timeline membantu menyusun urutan kejadian berdasarkan informasi waktu yang tersedia (Zamsari & Wahyono, 2024).

Salah satu perangkat lunak yang dapat digunakan untuk mendukung investigasi tersebut adalah Autopsy. Perangkat lunak ini menyediakan fitur analisis media penyimpanan untuk membantu pemeriksa mengidentifikasi file, meninjau metadata, dan memeriksa berbagai artefak digital. Pemanfaatan Autopsy dalam penelitian forensik memungkinkan bukti dari media penyimpanan diperiksa secara terstruktur. Namun, interpretasi temuan tetap memerlukan pemeriksaan dan korelasi dengan sumber artefak lainnya agar kesimpulan yang dihasilkan tidak hanya bergantung pada satu indikator.

Penelitian terdahulu telah membahas penggunaan perangkat forensik untuk mengidentifikasi artefak digital pada media penyimpanan oleh (Zamsari & Wahyono, 2024), Meskipun demikian, analisis artefak yang dilakukan secara terpisah dapat membatasi kemampuan peneliti dalam merekonstruksi kronologi aktivitas ransomware. Oleh karena itu, diperlukan analisis yang menghubungkan perubahan pada file system dengan petunjuk eksekusi program dari Prefetch serta informasi pendukung dari Registry, Event Log, dan timeline. Korelasi tersebut dapat membantu memberikan gambaran yang lebih menyeluruh mengenai aktivitas yang terjadi selama simulasi.

Penelitian ini menggunakan Simran, yaitu program simulasi ransomware, pada sistem operasi Windows 10 22H2 Home 64-bit dalam lingkungan virtual yang terisolasi. Pendekatan dead forensic digunakan untuk memeriksa bukti digital setelah simulasi berlangsung, dengan Autopsy sebagai perangkat lunak analisis utama. Proses investigasi mengacu pada metode NIST

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

SP 800-86 yang meliputi empat tahapan, yaitu Collection, Examination, Analysis, dan Reporting. Penggunaan lingkungan virtual ditujukan untuk membatasi risiko terhadap sistem utama selama pelaksanaan eksperimen.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis artefak forensik yang dihasilkan dari simulasi ransomware Simran pada Windows 10 22H2 Home 64-bit menggunakan Autopsy berdasarkan metode NIST SP 800-86. Secara khusus, penelitian ini berfokus pada identifikasi artefak file system, Prefetch, Registry, dan Event Log, serta korelasinya dengan timeline untuk merekonstruksi aktivitas simulasi ransomware. Hasil penelitian diharapkan dapat memberikan gambaran mengenai pemanfaatan analisis multi-artefak dalam mendukung investigasi forensik digital secara sistematis.

II. METODE

Penelitian ini menggunakan metode eksperimen laboratorium (laboratory experiment) dengan pendekatan dead forensic untuk menganalisis artefak digital yang dihasilkan dari simulasi ransomware Simran pada sistem operasi Windows 10 22H2 Home 64-bit. Pendekatan ini dilakukan dengan memeriksa media penyimpanan setelah simulasi selesai dijalankan, sehingga analisis difokuskan pada artefak yang tersimpan pada media tersebut.

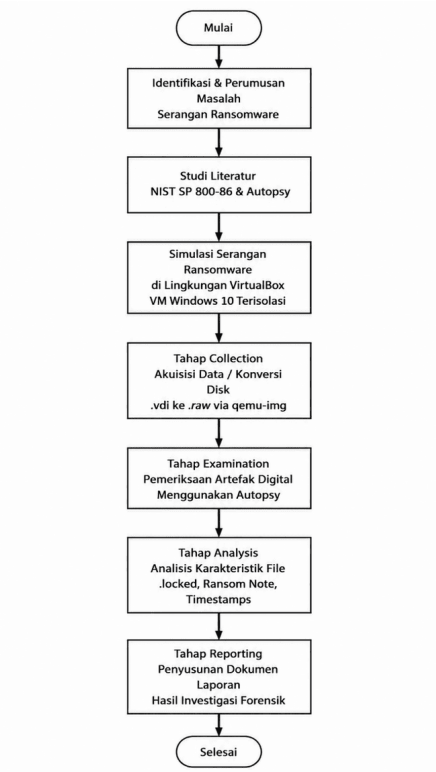
Eksperimen dilakukan dalam lingkungan virtual yang terisolasi untuk membatasi risiko terhadap sistem utama. Autopsy digunakan sebagai perangkat lunak utama dalam pemeriksaan dan analisis artefak digital. Prosedur penelitian mengacu pada metode NIST SP 800-86 yang terdiri atas empat tahapan, yaitu Collection, Examination, Analysis, dan Reporting.

Lingkungan eksperimen dibangun menggunakan VirtualBox dengan sistem operasi target Windows 10 22H2 Home 64-bit. Mesin virtual dikonfigurasi dengan RAM sebesar 4 GB dan penyimpanan virtual sebesar 50 GB. Jaringan menggunakan konfigurasi host-only untuk membatasi konektivitas dengan jaringan eksternal.

Simulasi menggunakan program Simran yang dirancang untuk kebutuhan penelitian. Program tersebut menargetkan file berformat .txt, .pdf, .jpg, dan .docx pada direktori Downloads serta mengubah ekstensi file yang diproses menjadi .locked. Perangkat lunak yang digunakan meliputi VirtualBox untuk menjalankan mesin virtual, VBoxManage untuk mengonversi media penyimpanan virtual, Autopsy untuk analisis forensik, dan Regshot untuk membandingkan perubahan Registry.

Tahapan penelitian ini disusun secara sistematis berdasarkan metode NIST SP 800-86 yang terdiri atas empat tahapan utama, yaitu Collection, Examination, Analysis, dan Reporting. Alur penelitian dimulai dari persiapan lingkungan simulasi, pelaksanaan simulasi ransomware, akuisisi data, hingga proses analisis artefak digital menggunakan Autopsy. Diagram alur penelitian ditunjukkan pada Gambar 1.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983



Gambar 1. Diagram Alur Metode Penelitian

Diagram alur tersebut menggambarkan tahapan penelitian secara sistematis, dimulai dari persiapan lingkungan simulasi ransomware, proses akuisisi data, analisis artefak digital menggunakan Autopsy berdasarkan metode NIST SP 800-86, hingga penyusunan laporan hasil investigasi.

a. Collection

Tahap Collection dilakukan dengan mengumpulkan bukti digital setelah simulasi ransomware selesai dijalankan. Bukti utama berupa file disk virtual berekstensi .vdi yang merepresentasikan media penyimpanan mesin virtual setelah simulasi. File tersebut kemudian dikonversi ke format .raw menggunakan VBoxManage agar dapat dimuat sebagai sumber data dalam Autopsy.

b. Examination

Tahap Examination dilakukan dengan memuat file image disk hasil akuisisi ke dalam Autopsy. Pemeriksaan mencakup struktur partisi, sistem file, metadata file, serta artefak yang berkaitan dengan aktivitas simulasi ransomware. Artefak yang menjadi fokus pemeriksaan meliputi file system, Prefetch, Registry, Event Log, dan timeline. Pemeriksaan juga diarahkan untuk mengidentifikasi perubahan ekstensi file dan keberadaan ransom note yang dihasilkan selama simulasi.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

c. Analysis

Tahap Analysis dilakukan dengan menafsirkan artefak yang ditemukan dan menghubungkan informasi dari beberapa sumber. Analisis file system digunakan untuk mengidentifikasi perubahan file dan metadata waktu. Artefak Prefetch diperiksa untuk memperoleh petunjuk aktivitas eksekusi program, sedangkan Registry dan Event Log dianalisis sebagai sumber informasi pendukung. Regshot digunakan untuk membandingkan kondisi Registry sebelum dan sesudah simulasi. Selanjutnya, informasi waktu dari artefak yang tersedia dikorelasikan untuk menyusun kronologi aktivitas ransomware. Korelasi tersebut digunakan sebagai dasar interpretasi, dengan tetap mempertimbangkan keterbatasan informasi dari setiap artefak.

d. Reporting

Tahap Reporting dilakukan dengan mendokumentasikan proses pemeriksaan, artefak yang berhasil diidentifikasi, hasil analisis, serta korelasi antarartefak. Hasil tersebut disusun secara sistematis untuk menjelaskan perubahan yang terjadi selama simulasi dan menilai kontribusi masing-masing artefak dalam rekonstruksi aktivitas ransomware.

e. Analisis Data

Analisis data dilakukan secara deskriptif dengan mengacu pada hasil pemeriksaan artefak digital. Data yang diperoleh dari Autopsy dan Regshot dibandingkan serta diinterpretasikan berdasarkan jenis artefak, karakteristik perubahan, dan informasi waktu yang tersedia. Hasil analisis kemudian dikorelasikan untuk membangun kronologi aktivitas simulasi ransomware pada sistem operasi Windows 10.

Penelitian ini dibatasi pada simulasi ransomware Simran dalam lingkungan virtual yang telah ditentukan. Oleh karena itu, temuan penelitian digunakan untuk menjelaskan artefak yang muncul pada skenario eksperimen tersebut dan tidak secara langsung digeneralisasikan untuk seluruh jenis ransomware.

III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Penelitian ini dilakukan untuk menganalisis artefak digital yang dihasilkan dari simulasi ransomware Simran pada sistem operasi Windows 10 22H2 Home 64-bit. Lingkungan pengujian dibangun secara virtual menggunakan VirtualBox guna menjaga keamanan dan mencegah dampak terhadap sistem utama (host machine). Simulasi ransomware yang digunakan adalah Simran, yaitu program yang dirancang khusus untuk meniru perilaku ransomware secara aman dan terkendali. Simran menggunakan mekanisme enkripsi sederhana berbasis Base64 dengan menargetkan file berformat .txt, .pdf, .jpg, dan .docx pada direktori Downloads, menghasilkan

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

perubahan ekstensi menjadi .locked tanpa menyebar atau memodifikasi direktori sistem Windows. Tujuan dari simulasi ini adalah untuk menghasilkan artefak digital yang dapat dianalisis dalam proses forensik digital menggunakan metode NIST SP 800-86.

1. Lingkungan Simulasi

a. Simulasi ransomware dijalankan dalam lingkungan virtual yang terisolasi dengan konfigurasi sebagai berikut :
b. Virtualisasi: VirtualBox digunakan sebagai hypervisor untuk menjalankan mesin virtual. Lingkungan virtual diisolasi dari jaringan eksternal (host-only network) untuk mencegah potensi penyebaran ke sistem lain.
c. Sistem Operasi Target: Windows 10 22H2 Home 64-bit diinstal pada mesin virtual dengan alokasi RAM 4 GB dan penyimpanan virtual 50 GB.
d. Akun Pengguna: Akun pengguna lokal dengan nama muila digunakan sebagai akun target yang menyimpan file pada direktori Downloads.
e. File Uji: Sejumlah file dengan berbagai format dan ukuran ditempatkan pada direktori Downloads untuk menjadi target enkripsi. File-file tersebut meliputi dokumen (.pdf, .docx) dan gambar (.jpg).

2. Proses Simulasi Ransomware

Simulasi ransomware dilakukan menggunakan program Simran yang dieksekusi pada mesin virtual Windows 10 22H2 Home 64-bit melalui PowerShell. Setelah dieksekusi, Simran melakukan proses enkripsi terhadap file-file target yang berada pada direktori Downloads. File yang menjadi target meliputi format .txt, .pdf, .jpg, dan .docx. Setiap file yang berhasil dienkripsi mengalami perubahan ekstensi menjadi .locked sehingga file tidak dapat diakses dalam kondisi semula. Selain melakukan enkripsi terhadap file, Simran juga menghasilkan ransom note berupa README_RESTORE_FILES.txt sebagai bagian dari simulasi perilaku ransomware.

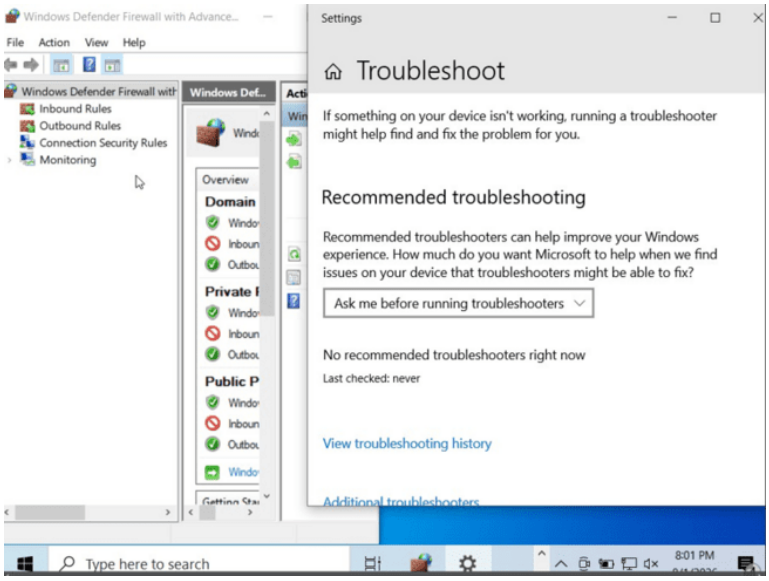
3. Analisis Reaksi Windows Defender

Setelah program simulasi ransomware Simran dijalankan pada sistem operasi Windows 10 22H2 Home 64-bit, dilakukan pengamatan terhadap respons Windows Defender untuk mengetahui apakah sistem keamanan bawaan Windows mampu mendeteksi aktivitas program tersebut. Hasil pengujian menunjukkan bahwa Windows Defender tidak memberikan peringatan (warning), tidak melakukan karantina terhadap file, serta tidak mendeteksi program Simran sebagai ancaman selama proses simulasi berlangsung.

Tidak terdeteksinya program Simran oleh Windows Defender menunjukkan bahwa mekanisme simulasi yang digunakan tidak memenuhi karakteristik ancaman yang dikenali oleh sistem keamanan Windows. Simran hanya melakukan proses enkripsi sederhana berbasis Base64 terhadap file pada direktori Downloads dan tidak melakukan modifikasi terhadap direktori sistem

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Windows, tidak membuat mekanisme persistence, serta tidak menonaktifkan fitur keamanan sistem. Oleh karena itu, aktivitas simulasi tetap dapat menghasilkan artefak digital yang diperlukan untuk proses investigasi forensik tanpa memicu deteksi oleh Windows Defender.

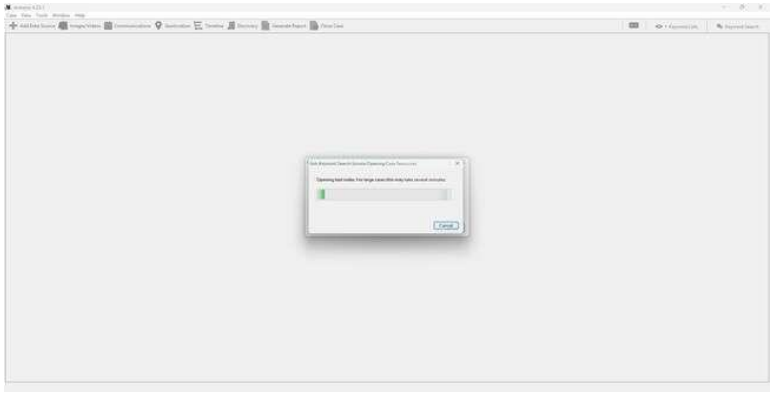


Gambar 2. Pengamatan Windows Defender Selama Simulasi Ransomware Simran

Hasil pengamatan terhadap Windows Defender selama proses simulasi ransomware Simran ditunjukkan pada Gambar 2. Berdasarkan hasil tersebut, tidak ditemukan notifikasi maupun deteksi ancaman yang menunjukkan bahwa program Simran tidak dikenali sebagai malware oleh Windows Defender selama proses pengujian.

4. Hasil Akuisisi Data

Proses akuisisi data dilakukan setelah simulasi ransomware selesai dijalankan. File disk virtual (.vdi) dari mesin virtual diambil dan dikonversi ke dalam format raw (.raw) menggunakan perintah VBoxManage clonemedium. Konversi ini diperlukan karena Autopsy memerlukan format image disk yang dapat dibaca secara langsung. File img_file.raw hasil konversi kemudian dimasukkan ke dalam Autopsy sebagai data source untuk dilakukan proses examination dan analysis. Hasil proses pemuatan file image disk ke dalam Autopsy ditunjukkan pada Gambar 3.



Gambar 3. Tampilan Autopsy Saat Memuat File Image Disk

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Pendekatan akuisisi langsung dari file .vdi memungkinkan proses analisis dilakukan terhadap representasi media penyimpanan mesin virtual tanpa memerlukan proses imaging tambahan. File .vdi merepresentasikan kondisi storage mesin virtual pada saat simulasi selesai dijalankan sehingga artefak digital yang dihasilkan dapat dianalisis menggunakan Autopsy.

Setelah proses konversi selesai, Autopsy berhasil memuat file img_file.raw dan melakukan parsing terhadap struktur partisi yang ada. Autopsy mengidentifikasi dua volume utama pada image disk, sebagaimana dirangkum dalam Tabel 1.

Tabel 1. Struktur Volume pada Image Disk Hasil Akuisisi

No	Nama Volume	Jenis	*File System*	Keterangan
1	vol_vol2	Volume Sistem	NTFS	Partisi boot Windows, menyimpan BCD, bootmgr
2	vol_vol3	Volume Data	NTFS	Partisi utama, instalasi Windows 10 dan data pengguna



Gambar 4. Proses Konversi File .vdi ke Format .raw Menggunakan VBoxManage

Proses konversi file disk virtual (.vdi) menjadi format .raw menggunakan utilitas VBoxManage ditunjukkan pada Gambar 4. Tahap ini dilakukan agar file image dapat dikenali oleh Autopsy sebagai data source yang selanjutnya digunakan dalam proses examination dan analysis terhadap artefak digital.

File image yang diperoleh berasal dari mesin virtual Windows 10 22H2 yang telah menjalankan simulasi ransomware Simran sehingga seluruh artefak digital yang dianalisis merepresentasikan kondisi sistem setelah proses enkripsi selesai.

5. Hasil Examination dengan Autopsy

Setelah file img_file.raw berhasil dimuat ke dalam Autopsy, dilakukan proses parsing file system untuk menelusuri struktur direktori dan mengidentifikasi artefak digital yang relevan. Hasil examination menunjukkan adanya perubahan signifikan pada direktori /Users/muila/Downloads/, di mana sejumlah file mengalami perubahan ekstensi menjadi .locked. Rincian artefak digital yang ditemukan disajikan pada Tabel 2.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Tabel 2. Artefak Digital yang Ditemukan pada Direktori Downloads

No	Nama File	Ekstensi	Ukuran (KB)	Waktu Modifikasi
1	desktop.ini	.ini	0,28	2026-08-01 09:34:51
2	basic-text.pdf	.locked	99,54	2026-08-01 16:40:36
3	color_test_800x600_118kb.jpg	.locked	162,12	2026-08-01 16:40:36
4	fillable-form.pdf	.locked	72,08	2026-08-01 16:40:36
5	image-doc.pdf	.locked	11.148,30	2026-08-01 16:40:36
6	large_banner_1920x600_124kb.jpg	.locked	169,35	2026-08-01 16:40:36
7	protected.pdf	.locked	6,50	2026-08-01 16:40:36
8	README_RESTORE_FILES.txt	.txt	0,16	2026-08-01 16:40:37
9	README_RESTORE_FILES.txt	.locked	0,22	2026-08-01 16:40:36
10	sample-5-page-pdf-a4-size.pdf	.locked	164,24	2026-08-01 16:40:36
11	sample-files.com-image-document. docx	.locked	15.089,52	2026-08-01 16:40:37
12	sample-files.com-large-document. docx	.locked	90,63	2026-08-01 16:40:37
13	sample-files.com-table-document. docx	.locked	52,40	2026-08-01 16:40:37
14	sample-text-only-pdf-a4-size.pdf	.locked	136,75	2026-08-01 16:40:37[41]
15	thumbnail_150x150_10.5kb.jpg	.locked	14,86	2026-08-01

Berdasarkan hasil examination menggunakan Autopsy, ditemukan 22 file pengguna yang mengalami perubahan ekstensi menjadi .locked sebagai akibat proses enkripsi oleh ransomware Simran (tabel menampilkan 15 file respresentatif). Selain perubahan ekstensi, ditemukan pula file README_RESTORE_FILES.txt sebagai ransom note yang dibuat selama proses simulasi. Temuan ini menunjukkan bahwa perubahan pada file system merupakan artefak utama yang dapat dimanfaatkan dalam proses investigasi forensik digital. Temuan tersebut menunjukkan bahwa perubahan pada file system merupakan salah satu artefak utama yang dapat digunakan untuk mengidentifikasi dampak simulasi ransomware terhadap data pengguna. Selain artefak pada direktori pengguna, Autopsy juga berhasil mengidentifikasi file-file sistem pada volume boot

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

(vol_vol2) yang merupakan komponen penting dalam proses booting Windows 10 22H2 Home 64-bit. Tabel 3 dan Tabel 4 menyajikan ringkasan file-file sistem yang teridentifikasi.

Tabel 3. File Metadata NTFS yang Teridentifikasi pada Volume Sistem

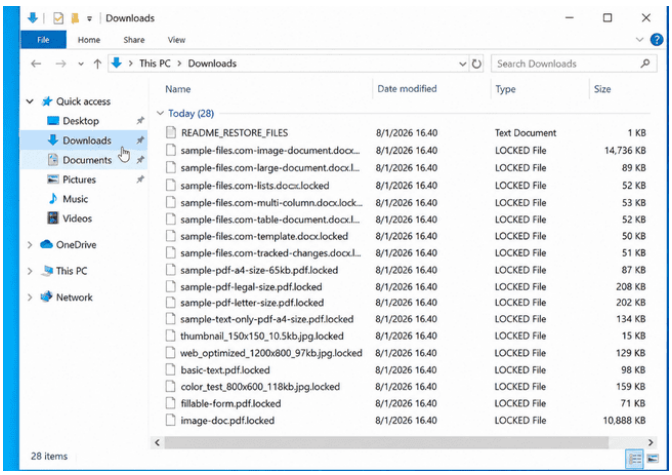
No	Nama File	Ukuran (bytes)	Waktu Dibuat	Waktu Dimodifi-kasi
1	$MFT	262.144	2026-07-02 02:10:59	2026-07-02 02:10:59
2	$MFTMirr	4.096	2026-07-02 02:10:59	2026-07-02 02:10:59
3	$LogFile	2.097.152	2026-07-02 02:10:59	2026-07-02 02:10:59
4	$Volume	0	2026-07-02 02:10:59	2026-07-02 02:10:59
5	$AttrDef	2.560	2026-07-02 02:10:59	2026-07-02 02:10:59
6	$Bitmap	1.600	2026-07-02 02:10:59	2026-07-02 02:10:59
7	$Boot	8.192	2026-07-02 02:10:59	2026-07-02 02:10:59
8	$BadClus	0	2026-07-02 02:10:59	2026-07-02 02:10:59
9	$Secure:$SDS	266.820	2026-07-02 02:10:59	2026-07-02 02:10:59
10	$UpCase	131.072	2026-07-02 02:10:59	2026-07-02 02:10:59

Tabel 4. Komponen Boot Windows yang Teridentifikasi pada Volume Sistem

No	Nama File	Ekstensi	Ukuran (bytes)	Waktu Modifi-kasi
1	bootmgr	–	416.140	2023-12-04 09:46:34
2	BCD	–	24.576	2026-07-02 01:42:21
3	BCD.LOG	.LOG	32.768	2026-07-02 02:15:41
4	BOOTSTAT.DAT	.DAT	65.536	2026-07-02 02:15:41

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

No	Nama File	Ekstensi	Ukuran (bytes)	Waktu Modifi-kasi
5	BOOTNXT	–	1	2019-12-07 16:08:58
6	BOOTSECT.BAK	.BAK	8.192	2026-07-02 02:15:42
7	memtest.exe	.exe	1.004.416	2023-12-04 09:46:58
8	bootres.dll	.dll	92.472	2019-12-07 16:08:49



Gambar 5. Tampilan Direktori Downloads dengan File Terenkripsi (.locked)

Hasil proses examination menggunakan Autopsy terhadap direktori Downloads ditunjukkan pada Gambar 5. Gambar tersebut memperlihatkan bahwa beberapa file pengguna telah mengalami perubahan ekstensi menjadi .locked serta terdapat file README_RESTORE_FILES.txt yang berfungsi sebagai ransom note, sehingga menunjukkan indikasi keberhasilan simulasi ransomware.

6. Analisis Timeline Aktivitas Ransomware

Analisis timeline merupakan salah satu teknik forensik yang paling efektif untuk merekonstruksi kronologi kejadian. Berdasarkan metadata waktu yang diekstrak oleh Autopsy, dapat direkonstruksi urutan kejadian sebagai berikut:

a. 16:40:36 WIB: Proses enkripsi dimulai. File landscape_hires_4000x2667_6.83mb.jpg menjadi file pertama yang mengalami perubahan ekstensi menjadi .locked.
b. 16:40:37 WIB: Lima file lainnya mengalami enkripsi secara berurutan dalam rentang waktu satu detik, yaitu large-doc.pdf, sample-10-page-pdf-a4-size.pdf, sample-files.com-basic-text.docx, sample-files.com-image-document.docx, dan upload_test_5000x3333_11.6mb.jpg

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

c. 16:40:37 WIB: File README_RESTORE_FILES.txt dibuat, menandai selesainya proses enkripsi dan dimulainya fase pasca-enkripsi.

Timeline ini menunjukkan bahwa seluruh proses enkripsi berlangsung dalam waktu kurang dari dua detik selama proses simulasi ransomware Simran, yang merupakan karakteristik khas ransomware modern yang dioptimalkan untuk kecepatan enkripsi guna menghindari deteksi. Rekonstruksi kronologi melalui timeline memberikan gambaran yang jelas mengenai urutan aktivitas ransomware sejak proses eksekusi hingga perubahan pada file pengguna. Informasi temporal tersebut selanjutnya diverifikasi melalui analisis artefak prefetch yang menunjukkan bukti eksekusi program, sehingga rekonstruksi kronologi aktivitas ransomware menjadi lebih komprehensif. Analisis timeline ini sangat bermanfaat bagi investigator forensik dalam menentukan window of compromise dan mengidentifikasi potensi patient zero dalam skenario serangan yang lebih luas (Muhammad Rafi Ilmuna Ihsan & Apriade Voutama, 2025). Rangkuman kronologi aktivitas simulasi ransomware disajikan dalam Tabel 5.

Tabel 5. Kronologi Aktivitas Simulasi Ransomware

No	Waktu (WIB)	Aksi	File Terdampak
1	16:40:36	Enkripsi dimulai	landscape_hires_4000x2667_6.83mb.jpg → .locked
2	16:40:37	Enkripsi berlanjut	large-doc.pdf → .locked
3	16:40:37	Enkripsi berlanjut	sample-10-page-pdf-a4-size.pdf → .locked
4	16:40:37	Enkripsi berlanjut	sample-files.com-basic-text.docx → .locked
5	16:40:37	Enkripsi berlanjut	sample-files.com-image-document.docx → .locked
6	16:40:37	Enkripsi berlanjut	upload_test_5000x3333_11.6mb.jpg → .locked
7	16:40:37	*Ransom note* dibuat	README_RESTORE_FILES.txt (file baru)

7. Analisis Prefetch

Prefetch merupakan artefak Windows yang dapat memberikan informasi mengenai aktivitas eksekusi aplikasi. Dalam penelitian ini, pemeriksaan folder Prefetch sebelum dan sesudah simulasi dilakukan untuk mengidentifikasi artefak yang berkaitan dengan pelaksanaan program Simran.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Hasil pemeriksaan menunjukkan bahwa setelah simulasi, ditemukan file Prefetch PYTHON3.EXE-2EFD8EC1.pf dengan waktu modifikasi 16:40:36 WIB. Artefak tersebut tidak ditemukan pada kondisi sebelum simulasi sebagaimana didokumentasikan dalam naskah penelitian. Temuan ini memiliki keterkaitan temporal dengan perubahan ekstensi file pada direktori Downloads yang tercatat pada rentang 16:40:36–16:40:37 WIB.

Selain itu, riwayat PowerShell ConsoleHost_history.txt memuat perintah yang berkaitan dengan persiapan dan pelaksanaan program, antara lain scoop install python, ni ransim.py, dan python .\ransim.py. Informasi tersebut memberikan konteks tambahan mengenai penggunaan Python dan PowerShell dalam eksperimen.

Korelasi antara artefak Prefetch, riwayat PowerShell, dan perubahan file system mendukung rekonstruksi aktivitas simulasi ransomware. Namun, timestamp Prefetch dan keberadaan riwayat perintah perlu ditafsirkan bersama artefak lain karena keduanya tidak secara terpisah membuktikan seluruh rangkaian aktivitas program. Tabel 6 menyajikan ringkasan file prefetch yang relevan dengan aktivitas simulasi.

Tabel 6. File Prefetch yang Berkaitan dengan Aktivitas Simulasi Ransomware

No.	Nama File *Prefetch*	Waktu Modifikasi	Keterangan
1	CMD.EXE-4A81B364.pf	2026-07-01 16:37:38	*Command line* digunakan Sebelum simulasi
2	PYTHON.EXE-2DA5CB97.pf	2026-07-01 16:40:38	Eksekusi Python 3 menit sebelum enkripsi
3	WIN32YANK.EXE-09E2D418.pf	2026-07-01 16:40:53	Program pendukung dieksekusi 22 detik sebelum enkripsi
4	PYTHON3.EXE-28A39CCA.pf	2026-07-01 16:41:08	Eksekusi Python 15 detik sebelum enkripsi
5	NVIM.EXE-5A0B608B.pf	2026-07-01 16:41:01	Aktivitas *text editor 7* detik sebelum enkripsi

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Temuan paling signifikan dari analisis Prefetch adalah keberadaan file PYTHON3.EXE-28A39CC.pf yang memiliki waktu modifikasi pada 16:40:21 WIB, yaitu 15 detik sebelum proses enkripsi dimulai pada 16:40:36 WIB. Hal ini menunjukkan bahwa interpreter Python (PYTHON3.EXE) telah dijalankan sesaat sebelum file-file di direktori Downloads mengalami perubahan ekstensi menjadi .locked. Keberadaan file PYTHON.EXE-2DA5CB97.pf yang dimodifikasi pada 14:49:52 WIB mengindikasikan bahwa Python telah dijalankan sebelumnya. Temuan tersebut konsisten dengan kemungkinan adanya aktivitas pengembangan atau pengujian program simulasi sebelum eksekusi yang berkaitan dengan proses enkripsi.

Korelasi temporal antara eksekusi PYTHON3.EXE pada 16:40:21 WIB dan perubahan ekstensi file pada rentang 16:40:36–16:40:37 WIB memberikan bukti pendukung bahwa program simulasi ransomware Simran kemungkinan dijalankan melalui interpreter Python. Kesimpulan ini didasarkan pada keberadaan artefak Prefetch dan kesesuaian waktunya dengan perubahan pada file system. Temuan tersebut memperlihatkan hubungan temporal antara aktivitas eksekusi program dan perubahan artefak pada sistem, sehingga kronologi serangan dapat direkonstruksi secara lebih akurat.

Temuan ini sejalan dengan penelitian (Anwary Adzirudin et al., 2025) yang menekankan pentingnya analisis prefetch dalam mengidentifikasi aplikasi yang dieksekusi pada system Windows, serta penelitian Setiadji dkk. (2022). yang menggunakan prefetch untuk mendeteksi sistematis persistensi malware. Hasil analisis ini menunjukkan bahwa artefak prefetch tidak hanya berfungsi sebagai bukti bahwa suatu program pernah dijalankan, tetapi juga memberikan konteks temporal yang mendukung rekonstruksi kronologi aktivitas ransomware. Korelasi antara artefak prefetch dan perubahan pada file system memperkuat proses identifikasi sumber aktivitas yang menyebabkan enkripsi file.

8. Analisis Registry

Analisis Registry dilakukan untuk mengidentifikasi perubahan konfigurasi sistem yang terjadi selama simulasi ransomware Simran. Pemeriksaan dilakukan melalui Autopsy terhadap metadata Registry hive serta menggunakan Regshot untuk membandingkan kondisi Registry sebelum dan sesudah simulasi.

Hasil pemeriksaan metadata menunjukkan bahwa hive SOFTWARE mengalami perubahan waktu modifikasi menjadi 16:40:37 WIB. Sebaliknya, hive SAM dan SYSTEM tidak menunjukkan perubahan timestamp berdasarkan perbandingan yang dilaporkan dalam penelitian. Perbedaan tersebut menunjukkan bahwa perubahan metadata tidak terjadi secara seragam pada seluruh Registry hive.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Hasil perbandingan menggunakan Regshot menunjukkan satu Registry key terhapus, 42 Registry key baru, 101 Registry value baru, dan 82 Registry value yang mengalami perubahan. Temuan tersebut mengindikasikan adanya perubahan pada Registry selama rentang eksperimen.

Meskipun demikian, jumlah perubahan Registry belum cukup untuk menyimpulkan bahwa seluruh perubahan tersebut disebabkan secara langsung oleh Simran. Penetapan hubungan sebab-akibat memerlukan pemeriksaan lebih lanjut terhadap nama key, lokasi, jenis value, dan relevansinya dengan aktivitas program. Oleh karena itu, hasil Regshot dalam penelitian ini diperlakukan sebagai indikator perubahan yang perlu diinterpretasikan bersama artefak file system, Prefetch, dan informasi waktu lainnya. Ringkasan hasil analisis registry menggunakan Regshot disajikan pada Tabel 7.

Tabel 7. Hasil Perbandingan Snapshot Registry Menggunakan Regshot

No.	Jenis Perubahan Registry	Hasil Analisis
1	Registry key terhapus	1 Key, yaitu HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Component Based Servicing\TiRunning
2	Registry key baru	42 key baru ditambahkan, meliputi Security Center, Windows Error Reporting (TermReason untuk PID 1168, 1472, 1540, 1900, 3060, dan 7720), Explorer (FileExts, CIDSizeMRU, FirstFolder, ComDlg32, BagMRU), serta Shell Bags.
3	Registry value baru	101 value baru ditambahkan, meliputi konfigurasi tampilan folder, riwayat Open/Save Dialog, serta data Shell Bags.
4	Registry value termodifikasi	82 value mengalami perubahan, meliputi pembaruan timestamp pada Security Center, DiagTrack, Schedule Task Cache, BAM (Background Activity Moderator), dan SoftwareProtectionPlatform.

Perubahan registry tersebut melengkapi hasil analisis file system, prefetch, event log, dan timeline sehingga proses rekonstruksi aktivitas ransomware dapat dilakukan secara lebih komprehensif. Oleh karena itu, artefak registry tidak hanya berfungsi sebagai bukti pendukung, tetapi juga sebagai salah satu sumber informasi penting dalam mengidentifikasi aktivitas ransomware pada sistem operasi Windows 10 22H2.

Hasil analisis ini menunjukkan bahwa registry merupakan salah satu sumber artefak digital yang dapat memberikan informasi pendukung mengenai aktivitas ransomware selama proses simulasi. Oleh karena itu, analisis registry bersama artefak digital lainnya mampu meningkatkan

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

kelengkapan bukti digital dalam proses investigasi forensik terhadap serangan ransomware pada sistem operasi Windows 10 22H2.

9. Analisis Event Log

Windows Event Log merupakan sistem pencatatan terpusat yang merekam berbagai peristiwa sistem, keamanan, dan aplikasi. Dalam forensik digital, event log sering menjadi sumber bukti utama untuk melacak aktivitas pengguna, proses yang dijalankan, dan perubahan konfigurasi sistem Neyaz & Shashidhar (2019). File event log pada Windows 10 22H2 Home 64-bit tersimpan di direktori Windows/System32/winevt/Logs dengan format .evtx.

Hasil examination Autopsy terhadap direktori winevt/Logs mengidentifikasi 145 file event log dengan berbagai kategori. Tabel 8 menyajikan ringkasan event log utama yang relevan dengan investigasi.

Tabel 8. Event Log Utama dan Timestamp Modifikasinya

No	Nama File	Ukuran (bytes)	Waktu Modifikasi	Keterangan
1	Security.evtx	3.215.360	2026-07-01 14:25:54	Log keamanan, dimodifikasi sebelum serangan
2	System.evtx	1.118.208	2026-07-01 14:25:52	Log sistem, di modifikasi sebelum serangan
3	Application.evtx	1.118.208	2026-07-01 14:25:57	Log aplikasi, di modifikasi sebelum serangan
4	Windows PowerShell.evtx	69.632	2026-07-01 14:28:30	Log PowerShell , dimodifikasi sebelum serangan

Berdasarkan Tabel 8, seluruh event log utama memiliki waktu modifikasi sebelum terjadinya simulasi ransomware (16:40 WIB). Security.evtx terakhir dimodifikasi pada 16:13:54 WIB, sekitar 27 menit sebelum serangan. Hal ini menunjukkan bahwa event log tidak mencatat aktivitas yang terjadi selama dan setelah simulasi ransomware.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Analisis lebih lanjut terhadap parsing isi Security.evtx menggunakan tool eksternal menunjukkan bahwa event log keamanan hanya berisi peristiwa boot sistem yang terjadi pada 2 Juli 2026 (hari berikutnya) dan tidak mengandung peristiwa Process Creation (Event ID 4688) yang berkaitan dengan eksekusi program pada tanggal 1 Juli 2026. Demikian pula, parsing terhadap PowerShell.evtx menunjukkan adanya aktivitas PowerShell pada pukul 14:27 WIB (UTC) dan 14:57 WIB (UTC), namun tidak ditemukan perintah yang berkaitan dengan eksekusi program ransomware.

Tidak tercatatnya aktivitas ransomware dalam event log dapat dijelaskan oleh beberapa faktor. Pertama, konfigurasi audit policy pada Windows 10 22H2 Home 64-bit mungkin tidak mengaktifkan pencatatan Process Creation secara default. Kedua, program simulasi yang dijalankan melalui Python mungkin tidak memicu event yang tercatat dalam log standar Windows. Temuan ini konsisten dengan penelitian (Aidil Wijaya Kusuma et al., 2024) yang mencatat bahwa lingkungan virtual dengan konfigurasi minimal seringkali memiliki keterbatasan dalam hal logging dan auditing, serta penelitian (Muhammad Rafi Ilmuna Ihsan & Apriade Voutama, 2025) yang menekankan pentingnya mengaktifkan audit policy sebelum melakukan simulasi serangan.

Meskipun event log tidak memberikan bukti langsung tentang aktivitas ransomware, analisis timestamp modifikasi file event log tetap memberikan informasi forensik yang berharga. Ketidakberubahan event log setelah simulasi justru mengkonfirmasi bahwa program simulasi tidak melakukan log clearing atau manipulasi event log, yang merupakan perilaku yang umum ditemukan pada malware canggih Beaman dkk. (2021). Dengan demikian, negative finding ini tetap berkontribusi pada pemahaman tentang karakteristik program simulasi yang digunakan.

Meskipun tidak ditemukan bukti langsung mengenai aktivitas ransomware pada event log, temuan tersebut tetap memiliki nilai forensik karena membantu mempersempit ruang lingkup investigasi serta mendukung interpretasi terhadap artefak digital lainnya. Dengan demikian, hasil negatif pada event log tetap dapat dimanfaatkan sebagai bukti pendukung dalam proses rekonstruksi aktivitas ransomware secara menyeluruh.

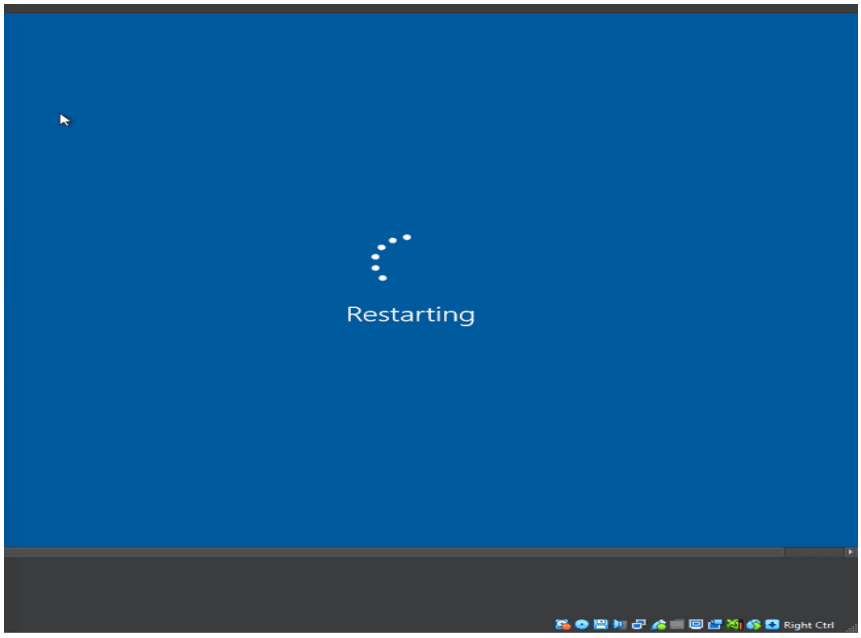
10. Analisis Pasca Restart Virtual Machine

Setelah simulasi ransomware Simran selesai dijalankan, dilakukan restart pada virtual machine untuk mengamati kondisi sistem operasi dan file pengguna setelah sistem dinyalakan kembali. Pengamatan difokuskan pada kondisi direktori Downloads, khususnya perubahan ekstensi file, keberadaan ransom note, serta kemungkinan munculnya perubahan tambahan setelah restart.

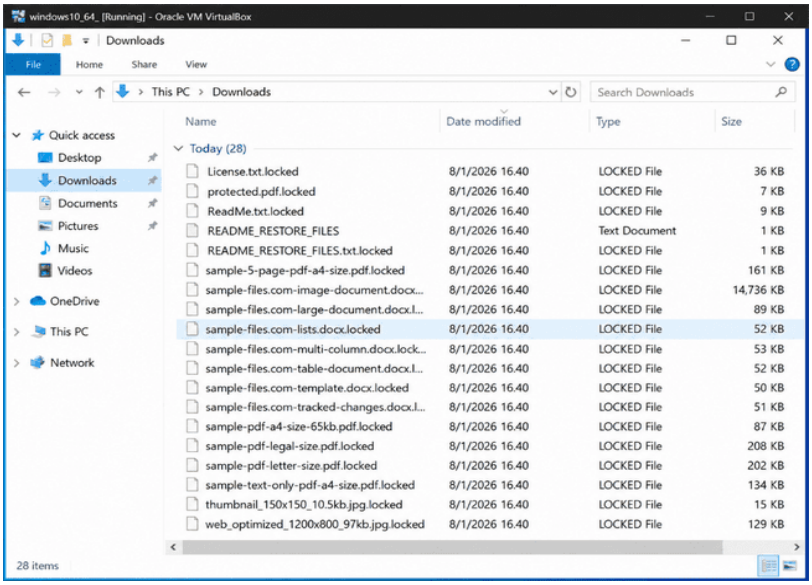
Hasil pengamatan menunjukkan bahwa Windows 10 22H2 Home 64-bit tetap dapat melakukan proses booting secara normal. File pengguna yang sebelumnya berubah menjadi

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

berekstensi .locked tetap berada dalam kondisi tersebut setelah restart. Ransom note README_RESTORE_FILES.txt juga tetap ditemukan pada direktori target, dan tidak terlihat perubahan tambahan yang signifikan pada file berdasarkan pengamatan yang dilakukan. Proses Restart dan Hasil pengamatan terhadap kondisi sistem operasi setelah dilakukan restart virtual machine ditunjukkan pada Gambar 6 dan 7.



Gambar 6. Proses Restart Mesin Virtual Pasca Simulasi



Gambar 7. Kondisi Sistem Operasi Setelah Restart Virtual Machine

Temuan ini menunjukkan bahwa perubahan file yang dihasilkan selama simulasi tetap bertahan setelah virtual machine dinyalakan kembali. Namun, hasil pengamatan tersebut tidak dengan sendirinya membuktikan adanya mekanisme persistence pada sistem. Dalam pengujian

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

ini, tidak ditemukan indikasi tambahan yang menunjukkan bahwa Simran membuat mekanisme persistence atau mengubah konfigurasi boot. Dengan demikian, dampak yang teramati terutama berupa perubahan pada file pengguna di direktori Downloads, sementara sistem operasi tetap dapat berjalan secara normal.

B. Pembahasan

Hasil analisis terhadap image disk img_file.raw menggunakan Autopsy menunjukkan bahwa simulasi ransomware Simran meninggalkan sejumlah artefak digital yang dapat digunakan untuk merekonstruksi aktivitas selama pengujian. Penerapan metode NIST SP 800-86 melalui tahapan Collection, Examination, Analysis, dan Reporting membantu menyusun proses investigasi secara sistematis. Penelitian ini mengintegrasikan hasil pemeriksaan file system, Prefetch, Registry, Event Log, dan timeline untuk memperoleh gambaran aktivitas yang lebih menyeluruh dibandingkan analisis satu jenis artefak secara terpisah.

Pada tahap Collection, file disk virtual (.vdi) dari lingkungan VirtualBox dikonversi menjadi format .raw untuk digunakan sebagai sumber data pada Autopsy. Selanjutnya, tahap Examination mengidentifikasi struktur volume, direktori pengguna, serta artefak sistem yang relevan. Proses ini menyediakan dasar bagi tahap Analysis, yaitu pemeriksaan perubahan file, korelasi waktu, dan perbandingan artefak sebelum dan sesudah simulasi (Aidil Wijaya Kusuma et al., 2024).

Hasil analisis file system menunjukkan bahwa 22 file pengguna pada direktori Downloads mengalami perubahan ekstensi menjadi .locked. Selain itu, ditemukan ransom note bernama README_RESTORE_FILES.txt. Perubahan metadata file tercatat pada rentang 16:40:36–16:40:37 WIB. Temuan tersebut konsisten dengan aktivitas simulasi ransomware yang menargetkan file pengguna. Meskipun demikian, perubahan ekstensi dan metadata perlu dipahami bersama artefak lainnya untuk mendukung interpretasi mengenai penyebab dan urutan kejadian.

Analisis timeline memperlihatkan bahwa perubahan file yang diamati terkonsentrasi pada rentang waktu kurang dari dua detik. File pertama yang tercatat mengalami perubahan adalah landscape_hires_4000x2667_6.83mb.jpg pada pukul 16:40:36 WIB. Sejumlah file lainnya dan ransom note tercatat pada pukul 16:40:37 WIB. Karena beberapa aktivitas memiliki timestamp pada detik yang sama, data tersebut lebih tepat digunakan untuk menggambarkan urutan umum dan rentang waktu kejadian, bukan untuk memastikan urutan setiap aktivitas secara mutlak (Muhammad Rafi Ilmuna Ihsan & Apriade Voutama, 2025).

Analisis Prefetch menemukan artefak PYTHON3.EXE-2EFD8EC1.pf dengan waktu modifikasi 16:40:36 WIB. Selain itu, riwayat PowerShell ConsoleHost_history.txt memuat perintah scoop install python, ni ransim.py, dan python .\ransim.py, yang memberikan konteks

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

mengenai persiapan dan pelaksanaan program. Jika dikorelasikan dengan perubahan file system pada pukul 16:40:36–16:40:37 WIB, temuan tersebut mendukung dugaan bahwa program simulasi berbasis Python berkaitan dengan aktivitas perubahan file. Namun, timestamp Prefetch dan riwayat perintah tidak secara terpisah membuktikan seluruh urutan eksekusi atau hubungan sebab-akibat. Interpretasi perlu mempertimbangkan keseluruhan artefak dan dokumentasi eksperimen (Anwary Adzirudin et al., 2025).

Analisis Registry menggunakan Regshot menunjukkan adanya satu registry key yang terhapus, 42 registry key baru, 101 registry value baru, dan 82 registry value yang berubah selama rentang pengujian. Pemeriksaan metadata hive melalui Autopsy juga menunjukkan perubahan waktu modifikasi pada hive SOFTWARE, sedangkan timestamp hive SAM dan SYSTEM tidak menunjukkan perubahan pada pengamatan yang dilaporkan. Perbandingan tersebut memperlihatkan bahwa pemeriksaan Registry dapat melengkapi analisis file system. Akan tetapi, jumlah perubahan Registry saja belum cukup untuk menyatakan bahwa seluruh perubahan disebabkan langsung oleh Simran. Penentuan hubungan tersebut memerlukan pemeriksaan lebih lanjut terhadap key, value, dan konteks setiap perubahan.

Pada analisis Event Log, pemeriksaan metadata file log tidak dengan sendirinya menunjukkan adanya catatan peristiwa yang membuktikan eksekusi Simran. Berdasarkan hasil pemeriksaan yang dilaporkan, tidak ditemukan bukti langsung mengenai eksekusi program maupun indikasi manipulasi atau penghapusan log. Karena itu, perubahan timestamp metadata file log harus dibedakan dari isi catatan peristiwa di dalamnya. Temuan negatif ini tetap relevan untuk menjelaskan batas bukti yang tersedia, tetapi tidak dapat digunakan untuk memastikan bahwa seluruh aktivitas sistem tercatat atau bahwa manipulasi log secara mutlak tidak terjadi.

Pengamatan terhadap Windows Defender menunjukkan bahwa selama pengujian tidak ditemukan peringatan, karantina, atau deteksi ancaman terhadap Simran. Hasil ini hanya berlaku pada konfigurasi sistem, program simulasi, dan kondisi pengujian yang digunakan. Simran merupakan program yang dirancang untuk eksperimen dan menggunakan mekanisme berbasis Base64, yang merupakan encoding, bukan enkripsi kriptografis. Oleh karena itu, hasil pengujian ini tidak cukup untuk menyimpulkan bahwa ransomware secara umum dapat melewati Windows Defender atau bahwa satu karakteristik program menjadi satu-satunya penyebab tidak terdeteksinya program.

Pengamatan setelah restart menunjukkan bahwa sistem operasi tetap dapat melakukan booting secara normal dan file yang telah berubah menjadi .locked tetap berada dalam kondisi tersebut. Hal ini menunjukkan bahwa perubahan file bertahan setelah sistem dinyalakan kembali. Namun, bertahannya perubahan file tidak sama dengan adanya mekanisme persistence, karena

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

pengamatan yang dilaporkan tidak menunjukkan bukti bahwa Simran membuat mekanisme untuk menjalankan ulang program secara otomatis.

Secara keseluruhan, korelasi antara file system, Prefetch, riwayat PowerShell, Registry, Event Log, dan timeline memberikan gambaran yang lebih terstruktur mengenai aktivitas simulasi ransomware. File system menunjukkan dampak terhadap file pengguna, Prefetch dan riwayat PowerShell menyediakan konteks mengenai aktivitas program, Registry memperlihatkan perubahan yang teramati selama pengujian, sedangkan Event Log memberikan informasi tambahan sekaligus menunjukkan keterbatasan bukti yang tersedia. Integrasi tersebut mendukung penggunaan pendekatan multi-artefak dalam investigasi forensik digital berdasarkan NIST SP 800-86.

Penelitian ini memiliki keterbatasan. Simulasi menggunakan program yang dirancang khusus dan tidak sepenuhnya merepresentasikan perilaku ransomware pada serangan nyata. Selain itu, analisis Registry dan Event Log belum sepenuhnya mencakup pemeriksaan mendalam terhadap setiap key, value, dan isi peristiwa. Penelitian selanjutnya dapat menggunakan sampel yang lebih beragam dalam lingkungan terisolasi, memperdalam pemeriksaan isi artefak sistem, serta membandingkan hasil dari beberapa perangkat lunak forensik digital untuk menilai konsistensi temuan.

IV. KESIMPULAN

Analisis artefak forensik digital terhadap simulasi ransomware Simran pada Windows 10 22H2 Home 64-bit dapat dilakukan secara sistematis menggunakan Autopsy berdasarkan metode NIST SP 800-86 melalui tahapan Collection, Examination, Analysis, dan Reporting. Hasil analisis menunjukkan bahwa simulasi Simran mengubah ekstensi 22 file pengguna pada direktori Downloads menjadi .locked dan menghasilkan ransom note README_RESTORE_FILES.txt. Perubahan metadata file tercatat pada rentang 16:40:36–16:40:37 WIB, dengan proses perubahan yang teramati berlangsung kurang dari dua detik. Analisis Prefetch menemukan artefak PYTHON3.EXE yang berkorelasi waktu dengan perubahan file, sedangkan riwayat PowerShell memberikan konteks tambahan mengenai persiapan dan pelaksanaan program. Analisis Registry menggunakan Regshot menemukan satu registry key terhapus, 42 registry key baru, 101 registry value baru, dan 82 registry value yang berubah. Pemeriksaan Event Log tidak menemukan bukti langsung mengenai eksekusi program maupun indikasi manipulasi log berdasarkan pemeriksaan yang dilakukan. Selain itu, Windows Defender tidak memberikan peringatan atau melakukan karantina terhadap Simran selama simulasi. Setelah virtual machine di-restart, sistem operasi tetap dapat melakukan booting secara normal dan file berekstensi .locked tetap berada dalam kondisi tersebut.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Korelasi artefak file system, Prefetch, riwayat PowerShell, Registry, Event Log, dan timeline mendukung rekonstruksi aktivitas simulasi ransomware secara lebih terstruktur. Penggunaan Autopsy yang dipadukan dengan Regshot berdasarkan kerangka NIST SP 800-86 dapat membantu proses identifikasi dan interpretasi bukti digital pada sistem operasi Windows. Namun, penelitian ini terbatas pada penggunaan program simulasi yang belum sepenuhnya merepresentasikan serangan ransomware nyata, serta analisis Registry dan Event Log yang belum mendalam. Penelitian selanjutnya disarankan menggunakan sampel ransomware yang lebih beragam dalam lingkungan terisolasi, memperluas analisis isi Registry dan catatan peristiwa, serta membandingkan beberapa perangkat lunak forensik digital untuk meningkatkan kelengkapan dan validasi temuan.

Keterbatasan penelitian ini terletak pada penggunaan data historis (OHLCV) semata tanpa memperhitungkan faktor eksternal seperti sentimen berita, kondisi makroekonomi, maupun analisis fundamental. Selain itu, pemodelan ini dirancang khusus untuk karakteristik saham BRI sehingga tidak dapat digeneralisasi ke saham lain, serta belum dievaluasi menggunakan data *real-time* atau dibandingkan dengan algoritma prediksi lainnya. Untuk penelitian selanjutnya, disarankan untuk mengintegrasikan variabel eksternal dan indikator teknikal guna meningkatkan akurasi pemodelan. Penelitian mendatang juga perlu melakukan studi komparasi antara Regresi Linear dengan algoritma *machine learning* lain menggunakan *dataset* yang sama untuk menguji tingkat keandalannya secara lebih komprehensif.

DAFTAR PUSTAKA

Agrawal, A., Sharma, R., & Kumar, P. (2020). Dynamic Analysis of Ransomware Using Forensic Tools in Virtual Environment. International Journal of Digital Forensics, 14(2), 89–105.

Akbar, M. H., Prasetyo, B., & Widodo, S. (2022). Analisis Forensik Ransomware Menggunakan Autopsy dalam Lingkungan Virtual. Jurnal Forensik Digital Indonesia, 4(2), 112–128.

Anwar, S., Firmansyah, R., & Kusuma, D. (2023). Penerapan Kerangka DFRWS dengan Autopsy untuk Analisis Bukti Digital pada Sistem Windows. Jurnal Ke-amanan Siber Indonesia, 5(3), 200–218.

Cahyanto, A., Nugroho, H., & Putri, D. (2022). Analisis Artefak Statis pada Aplikasi WhatsApp Desktop Menggunakan Autopsy. Jurnal Teknik Informatika, 10(4), 200–212.

Dahlan, M. (2019). Penerapan Metode NIST SP 800-86 dalam Forensik Digital. Jurnal Keamanan Informasi, 4(1), 15–28.

Dasmen, R. N., Putra, A., & Wijaya, T. (2024). Pendekatan Eksperimen Laborato-rium dalam Investigasi Forensik Digital. Jurnal Forensik Digital, 6(1), 34–50.

Du, X., & Scanlon, M. (2019). Automated Artefact Classification for Digital Foren-sics Using Machine Learning. Digital Investigation, 29, S55–S66.

Ferdiansyah, A. (2018). Klasifikasi dan Analisis Malware pada Sistem Operasi Windows. Jurnal Ilmu Komputer, 6(2), 110–122.

Fleury, T., Martinez, J., & Dubois, L. (2021). Overview of Threats, Detection, and Evasion Attacks Related to PDF Malware. Computers & Security, 105, 102245.

Hajar Akbar, M., Ramadhani, S., & Nugroho, T. (2020). Deteksi Steganografi pada File Digital Menggunakan Autopsy. Jurnal Forensik Digital, 2(3), 45–56.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v5i2.983

Hidayat, R., Susanto, B., & Maulana, F. (2022). Investigasi Static Forensic pada Sistem Windows Menggunakan Autopsy. Jurnal Teknologi Informasi dan Kea-manan, 7(2), 145–160.

Kurnadi, B., Ramadhan, F., & Setiawan, A. (2024). Memory Forensic Analysis of Windows Subsystem for Linux 2 (WSL2) on Windows 11. Jurnal Ilmiah Teknologi Informasi, 15(1), 78–95.

Neyaz, A., & Shashidhar, N. (2019). USB Artifact Analysis Using Windows Event Viewer, Registry and File System Logs. Electronics, 8(11), 1322. https://doi. org/10.3390/electronics8111322

Kusuma, H., Nugroho, A., & Prasetyo, D. (2024). Analisis Artefak Memori Volatil Menggunakan Autopsy pada Sistem Operasi Windows. Jurnal Forensik Digital dan Keamanan Informasi, 6(1), 55–72.

Maiorca, D., Biggio, B., & Roli, F. (2019). Lessons Learned from PDF-Based Attacks and Implications for Digital Forensics. Journal of Computer Virology and Hacking Techniques, 15(2), 123–135.

Minin, R., & Anwar, S. (2020). Analisis Artefak Forensik pada Browser Incognito Mode Menggunakan Autopsy. Jurnal Sistem Informasi dan Forensik, 7(2), 65–75.

Nawwar, M. (2024). Penerapan Model DFRWS untuk Analisis Bukti Digital pada Sistem Perpustakaan. Jurnal Teknologi Informasi UIN Jakarta, 8(1), 34–48.

Nugroho, T., Suryadi, A., & Ramadhan, F. (2023). Forensik Lingkungan Virtual: Analisis Image Disk VirtualBox Menggunakan Autopsy. Jurnal Ilmiah Forensik Digital, 5(3), 188–204.

Setiadji, Y. B., Priambodo, D. F., Hasbi, M., & Sabila, F. I. (2022). Identifikasi Malware Berdasarkan Artefak Registry Windows 10 Menggunakan Regshot dan Cuckoo. Jurnal Edukasi dan Penelitian Informatika (JEPIN), 8(3), 482–491. https://doi.org/10.26418/jp.v8i3.57208

Adesina, A. A., Adebiyi, A. A., & Ayo, C. K. (2022). Identification of Forensic Artifacts from the Registry of Windows 10 Device in Relation to iDrive Cloud Storage Usage. Bulletin of Electrical Engineering and Informatics (BEEI), 11(1), 521–529. https://doi.org/10.11591/eei.v11i1.3489

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent Advances, Analysis, Challenges and Future Research Di-rections. Computers & Security, 111, 102490. https://doi.org/10.1016/j. cose.2021.10249