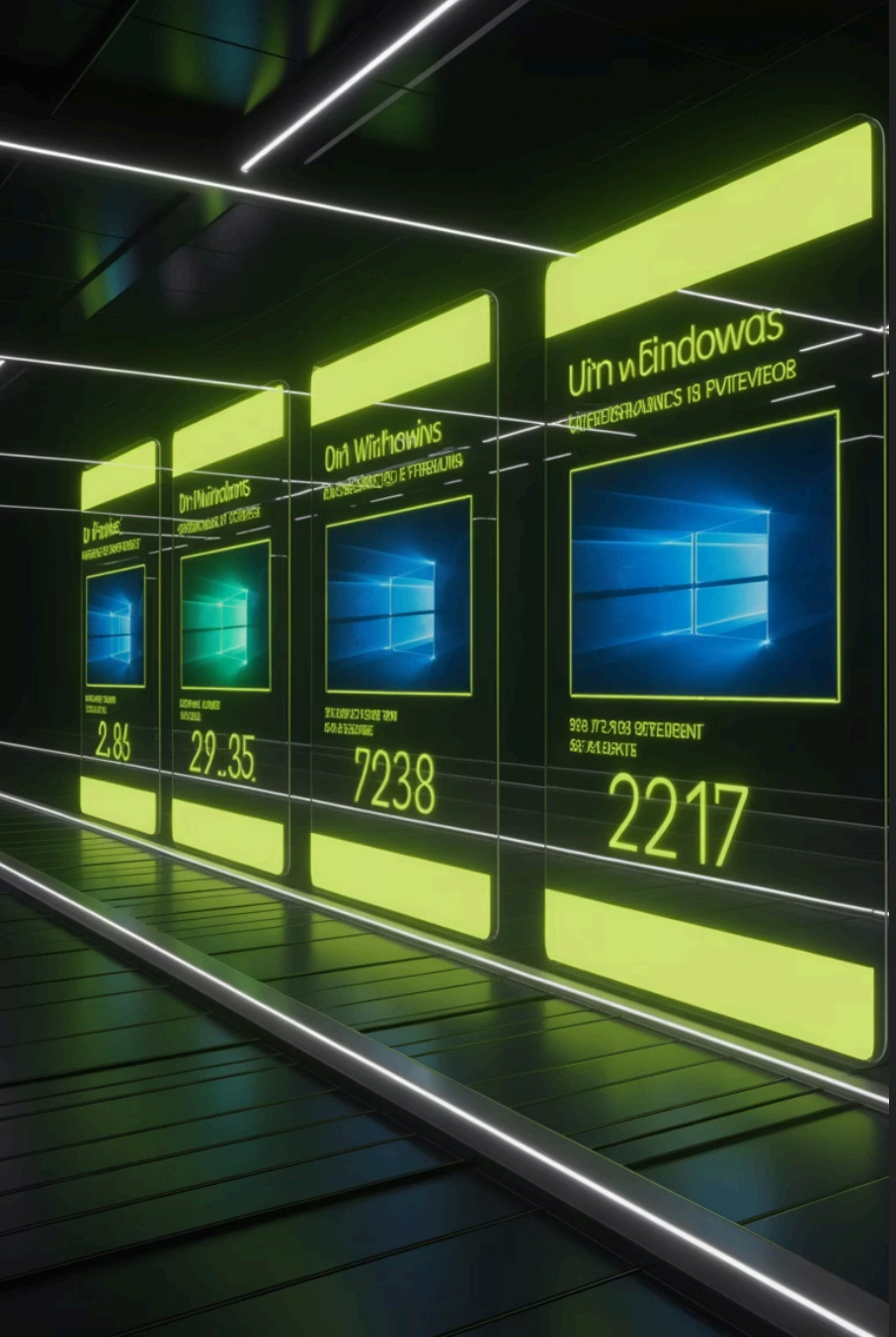
Modul 4 – Analisis Sistem Operasi Windows

Durasi: 4 jam

Author: Edy Susanto



Pengantar: Sistem Operasi Windows

Peran Windows

Sistem operasi Windows adalah perangkat lunak paling penting untuk menjalankan komputer. Windows mengelola sumber daya komputer, menyediakan layanan ke aplikasi, dan menawarkan antarmuka pengguna grafis (GUI) yang intuitif.

Evolusi Teknologi

Dari Windows 1.0 hingga Windows 10, Microsoft terus berinovasi dengan penambahan fitur keamanan, peningkatan kinerja, dan kemampuan forensik yang lebih canggih untuk mendukung investigasi digital.

Artefak Penting: Registry

Database Hierarkis

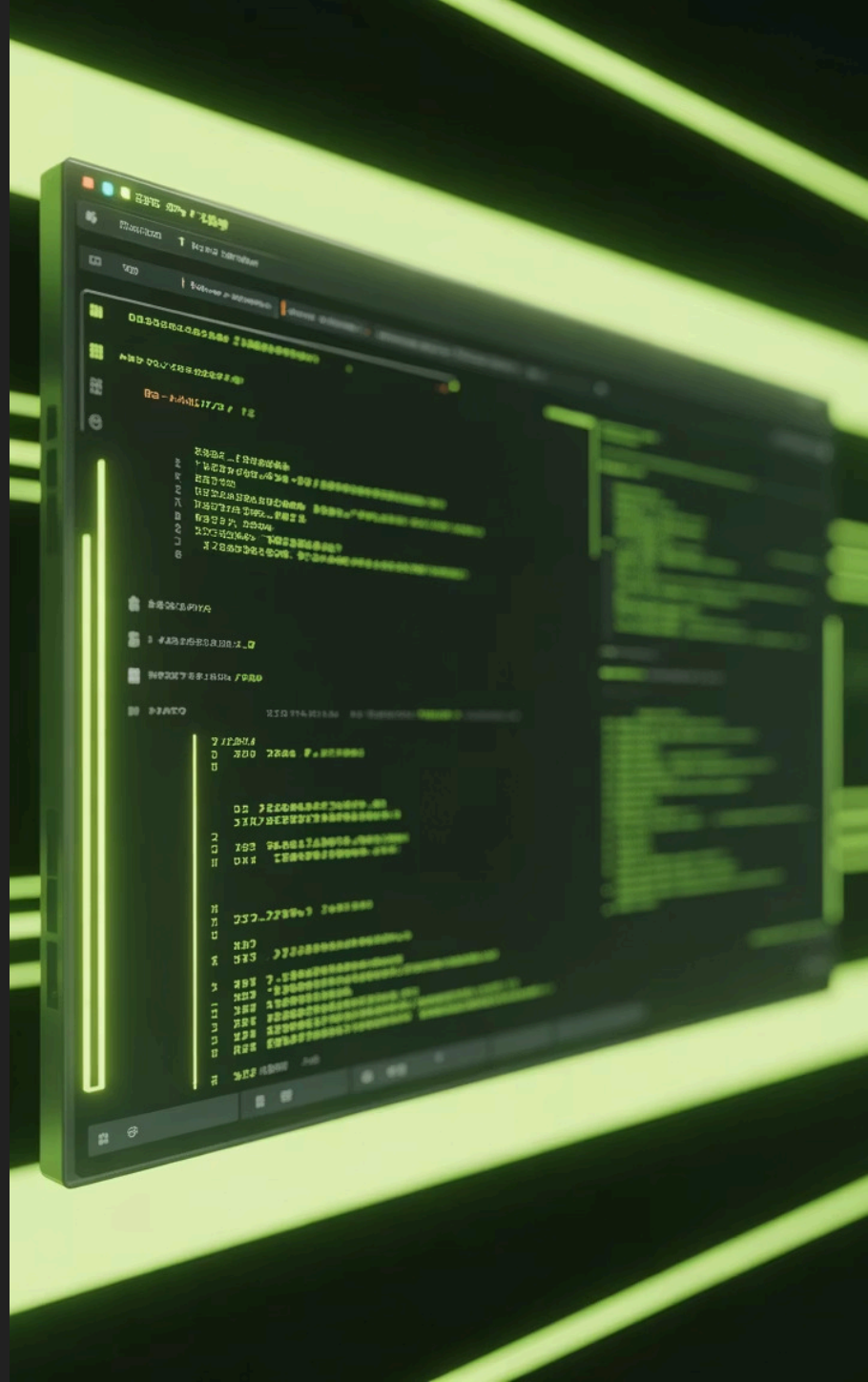
Registry menyimpan pengaturan konfigurasi untuk sistem operasi Windows dan semua aplikasi yang terinstal.

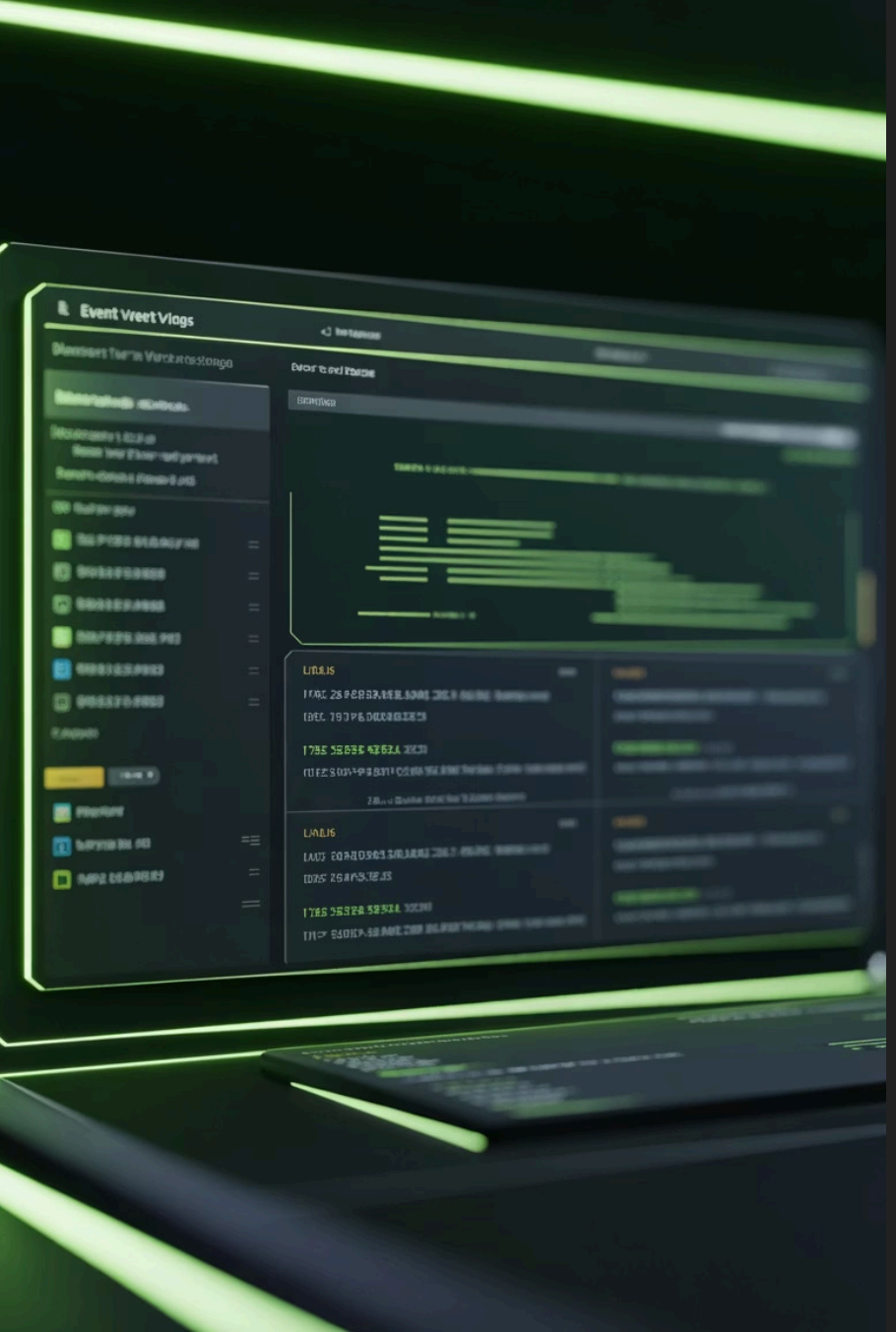
Informasi Sistem

Berisi data perangkat keras, perangkat lunak, preferensi pengguna, dan konfigurasi sistem secara menyeluruh.

Nilai Forensik

Analisis registry mengungkap aktivitas pengguna, instalasi software, dan perubahan sistem yang kritis.





Artefak Penting: Event Logs

01

Log Keamanan

Mencatat autentikasi, akses resource, dan perubahan kebijakan keamanan sistem.

02

Log Aplikasi

Merekam peristiwa dari aplikasi dan program yang berjalan di sistem.

03

Log Sistem

Menyimpan informasi tentang driver, layanan, dan komponen sistem operasi.

Event Logs sangat penting untuk mengidentifikasi insiden keamanan, melacak aktivitas mencurigakan, dan membangun timeline investigasi digital yang akurat.

Artefak Penting: Prefetch

Mekanisme Prefetch

Prefetch adalah fitur Windows yang meningkatkan waktu startup aplikasi dengan memuat file yang sering digunakan ke dalam memori secara proaktif.

Nilai Investigatif

File prefetch (.pf) menyimpan informasi krusial tentang aplikasi yang dijalankan, termasuk:

- Waktu eksekusi pertama dan terakhir
- Jalur file lengkap aplikasi
- File dan library yang dimuat
- Frekuensi eksekusi program

Artefak Penting: ShimCache

1

Application Compatibility Cache

ShimCache menyimpan metadata tentang file executable yang dijalankan pada sistem untuk tujuan kompatibilitas aplikasi.

2

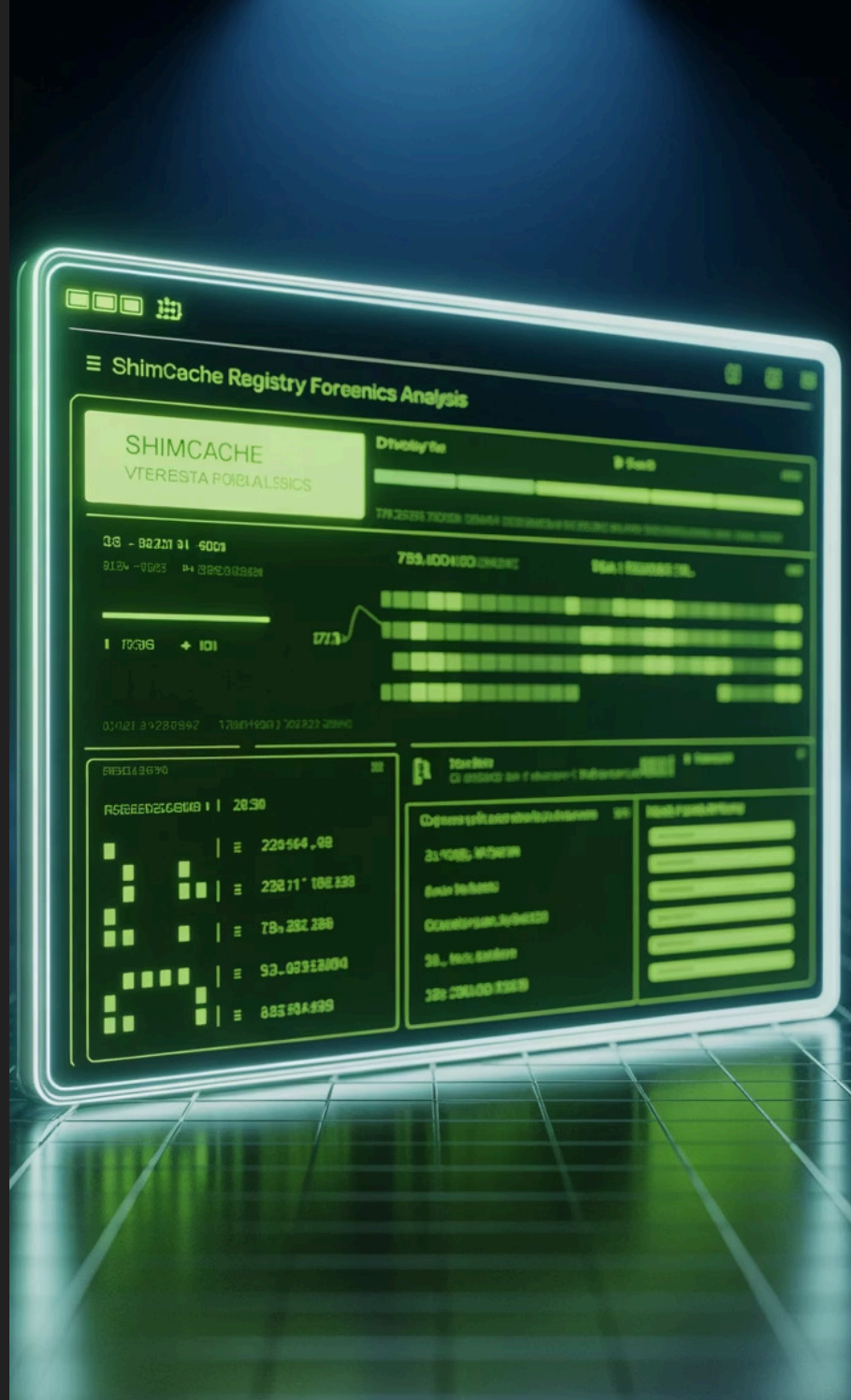
Informasi Tersimpan

Nama file, ukuran, waktu modifikasi terakhir, dan jalur file lengkap dari aplikasi yang pernah dieksekusi.

3

Keunggulan Forensik

Mengidentifikasi aplikasi yang dijalankan bahkan setelah file dihapus dari sistem, memberikan bukti eksekusi historis.



Artefak Penting: LNK Files

Shortcut Files

LNK files adalah file pintasan yang menunjuk ke file, folder, atau aplikasi target di sistem Windows.

Metadata Kaya

Berisi lokasi file target, timestamp akses, atribut file, dan informasi volume penyimpanan.

Tracking Aktivitas

Mengungkap file yang dibuka, folder yang diakses, dan aplikasi yang dijalankan oleh pengguna.

Artefak Penting: Scheduled Tasks

Penjadwalan Otomatis

Memungkinkan tugas dijalankan pada waktu tertentu atau sebagai respons terhadap event sistem.

Informasi Tugas

Nama tugas, trigger eksekusi, perintah yang dijalankan, dan kredensial akun pengguna.

Deteksi Ancaman

Mengidentifikasi malware persistence, backdoor, dan aktivitas berbahaya yang dijadwalkan.

User Artefacts: Browser History, Cookies, Recent Files

Browser History

Mencatat semua situs web yang dikunjungi, waktu akses, frekuensi kunjungan, dan kata kunci pencarian yang digunakan pengguna.

Cookies

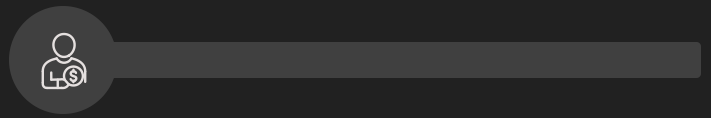
Menyimpan informasi sesi pengguna, preferensi website, data login, dan tracking aktivitas browsing untuk analisis perilaku.

Recent Files

Merekam file yang baru dibuka, aplikasi yang digunakan, dan timestamp akses untuk membangun pola aktivitas pengguna.

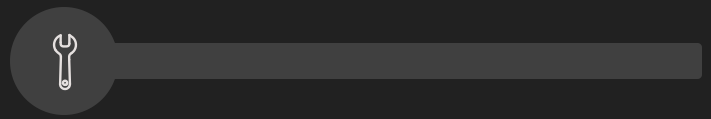
Analisis artefak pengguna ini sangat penting untuk memahami perilaku digital, membangun profil aktivitas, dan menyusun timeline investigasi yang komprehensif dan akurat.

Praktik: Ekstrak Timeline Aktivitas Pengguna



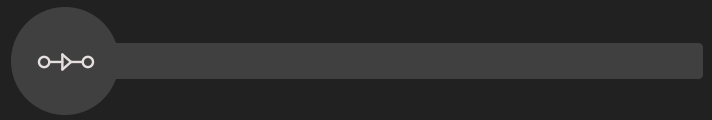
Pengumpulan Artefak

Kumpulkan registry, event logs, prefetch, ShimCache, LNK files, scheduled tasks, dan user artefacts dari sistem target.



Ekstraksi Data

Gunakan tool forensik seperti Autopsy, FTK Imager, atau RegRipper untuk mengekstrak dan parsing informasi dari artefak.



Pembuatan Timeline

Gabungkan informasi dari berbagai sumber untuk membuat timeline kasus yang komprehensif dan terkorelasi.

> **Kesimpulan:** Analisis sistem operasi Windows yang efektif memerlukan pemahaman mendalam tentang artefak forensik dan praktik analisis timeline untuk mengungkap bukti digital yang akurat dan dapat dipertanggungjawabkan.

Author: Edy Susanto