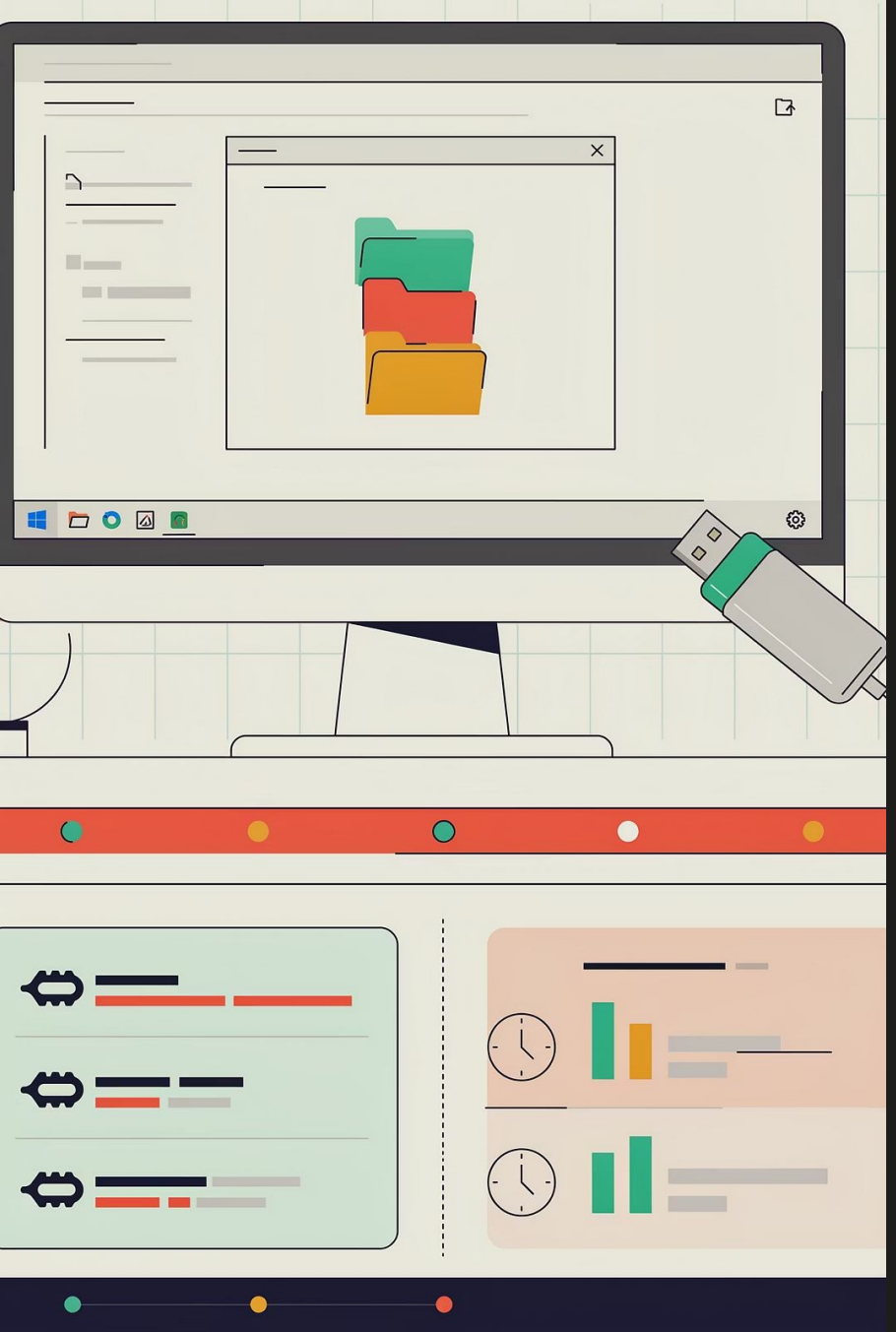


USB Timeline Reconstruction

DI-103 USB FORENSICS ESSENTIALS | MODUL 4

🔍 Rekonstruksi Peristiwa Digital

Susun ulang urutan peristiwa dari artefak digital yang tersebar untuk membangun gambaran lengkap insiden.

🔗 Korelasi Berbagai Artefak

Gabungkan bukti dari registry, event log, dan sistem file menjadi satu narasi investigasi yang kohesif.

📅 Bangun Timeline Investigasi

Produksi timeline kronologis berbasis bukti yang dapat dipertahankan di hadapan analisis forensik maupun pelaporan resmi.

Author: Edy Susanto – Founder C-SIX Security **www.csixsecurity.com**

Timeline Perangkat USB

Setiap interaksi antara perangkat USB dan sistem Windows meninggalkan jejak digital yang dapat direkonstruksi secara kronologis. Memahami urutan waktu ini adalah fondasi dari setiap investigasi forensik USB yang efektif.

1

08:30 — USB Dimasukkan

Windows mendeteksi koneksi perangkat baru secara fisik ke port USB.

2

08:31 — Windows Mendeteksi Perangkat

Sistem operasi mulai mengidentifikasi perangkat dan mempersiapkan proses enumerasi.

3

08:32 — Driver Terinstal

SetupAPI mencatat instalasi driver. Registry USBSTOR diperbarui dengan informasi perangkat.

4

08:35 — File Diakses

Pengguna membuka dan menjelajahi isi perangkat USB. File Explorer mencatat aktivitas ini.

5

08:40 — File Disalin

Operasi transfer file dilakukan. Metadata file dan log aktivitas mencatat peristiwa ini.

6

08:45 — USB Dilepas dengan Aman

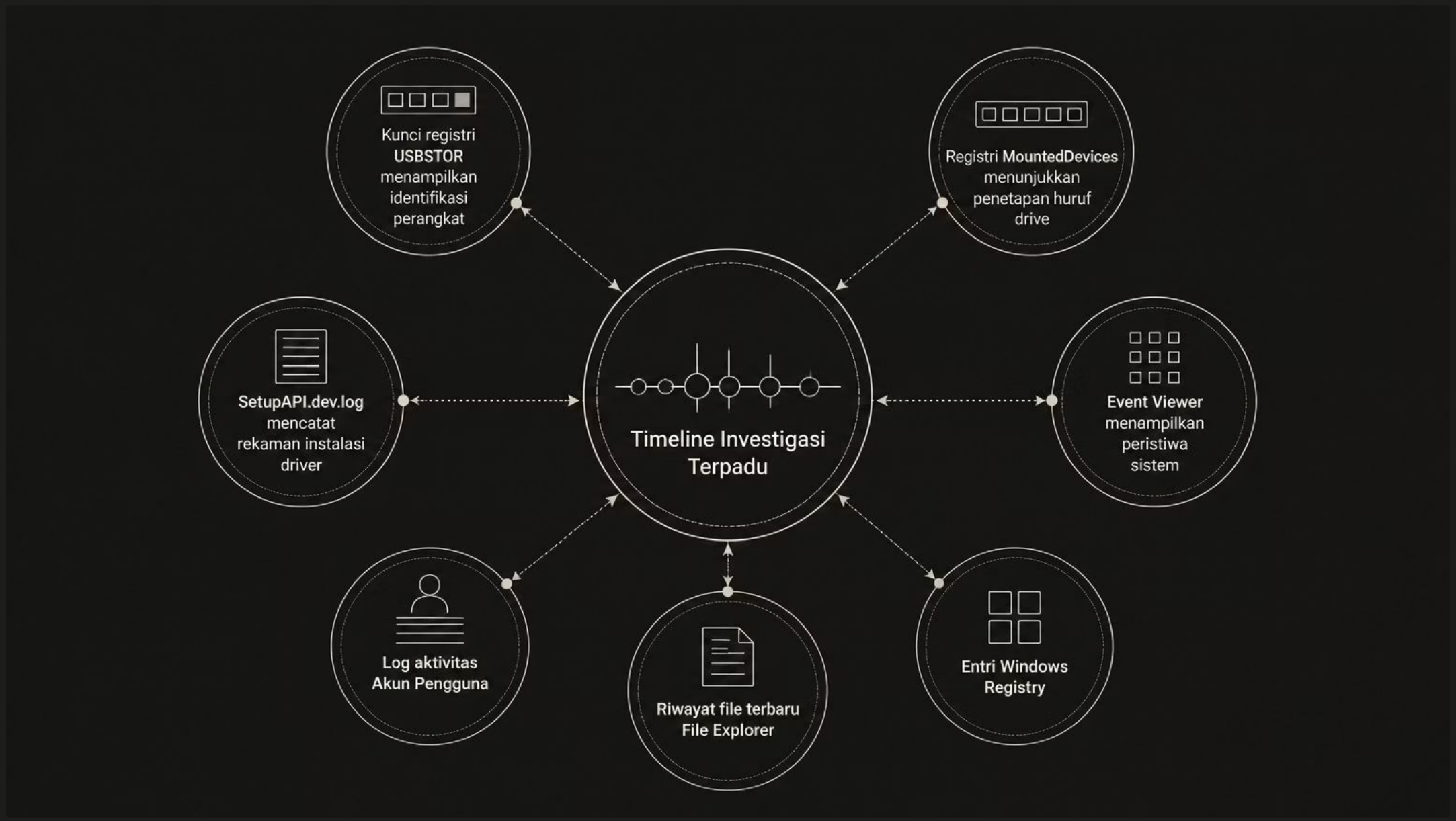
Proses eject yang aman dicatat oleh Windows Event Log sebagai pelepasan perangkat resmi.

Setiap tindakan menciptakan bukti digital — tidak ada aktivitas USB yang benar-benar tidak terlihat oleh sistem Windows.

Author: Edy Susanto – Founder C-SIX Security **www.csixsecurity.com**

Korelasi Bukti Digital

Investigasi forensik USB yang kuat tidak bergantung pada satu sumber bukti saja. Kekuatan analisis terletak pada kemampuan menggabungkan dan menghubungkan artefak dari berbagai sumber menjadi satu timeline investigasi yang komprehensif dan dapat dipertahankan.



> Satu artefak adalah petunjuk. Banyak artefak yang dikorelasikan mengungkap **keseluruhan cerita** di balik insiden USB.

Author: Edy Susanto – Founder C-SIX Security **www.csixsecurity.com**

Siapa yang Menggunakan USB?

Mengidentifikasi pengguna yang berinteraksi dengan perangkat USB adalah komponen krusial dalam setiap investigasi insiden. Dengan menghubungkan artefak akun pengguna, registry perangkat, dan log aktivitas, investigator dapat membangun gambaran yang jelas tentang siapa melakukan apa dan kapan.

Korelasi Pengguna

Identifikasi akun Windows yang aktif pada saat perangkat USB terhubung melalui Security Event Log (Event ID 4624).

Korelasi Perangkat

Cocokkan serial number USB dari USBSTOR dengan MountedDevices untuk mengkonfirmasi identitas perangkat yang digunakan.

Korelasi Aktivitas

Analisis LNK files, Jump Lists, dan Recent Files untuk merekonstruksi file apa saja yang diakses atau dipindahkan selama sesi berlangsung.

Author: Edy Susanto – Founder C-SIX Security **www.csixsecurity.com**

Membangun Timeline Investigasi

Timeline investigasi yang profesional menyusun seluruh bukti secara kronologis dalam format tabel yang terstruktur. Setiap entri harus memiliki timestamp yang akurat, sumber bukti yang jelas, dan deskripsi aktivitas yang spesifik agar dapat digunakan dalam laporan forensik resmi.

⏱️ Waktu	📁 Sumber Bukti	⚡ Aktivitas	📝 Deskripsi	✅ Status
08:30:12	🗂️ Registry – USBSTOR	USB Dimasukkan	Perangkat USB terdeteksi oleh sistem. Key USBSTOR dibuat dengan VID, PID, dan serial number perangkat.	✔️ Dikonfirmasi
08:31:05	📋 SetupAPI.dev.log	Driver Terinstal	Log SetupAPI mencatat instalasi driver USB Mass Storage. Timestamp pertama kali koneksi tercatat.	✔️ Dikonfirmasi
08:32:44	🗂️ Registry – MountedDevices	Drive Letter Ditetapkan	Windows menetapkan huruf drive (misalnya E:) kepada perangkat USB yang terhubung.	✔️ Dikonfirmasi
08:35:20	📄 File Explorer / LNK	File Diakses	LNK files dan Jump Lists mencatat akses pengguna terhadap file di dalam perangkat USB.	🔍 Dalam Analisis
08:40:33	📋 Event Viewer	File Disalin	Aktivitas transfer file tercatat. Metadata file menunjukkan perubahan timestamp pada dokumen target.	🔍 Dalam Analisis
08:45:01	📋 Event Log (ID 2003)	USB Dilepas	Event ID 2003 mencatat pelepasan perangkat USB secara aman dari sistem Windows.	✔️ Dikonfirmasi

Buat timeline investigasi yang jelas dan berbasis bukti — setiap entri harus dapat diverifikasi dan dipertahankan dalam laporan forensik resmi.

Author: Edy Susanto – Founder C-SIX Security **www.csixsecurity.com**

Case File 004 – Rekonstruksi Timeline

🕵️ MISI INVESTIGASI

Objektif Investigasi

01

Identifikasi waktu penyisipan USB

Temukan timestamp pertama dari registry USBSTOR dan SetupAPI log.

02

Tentukan waktu instalasi driver

Analisis SetupAPI.dev.log untuk mencatat kapan driver USB pertama kali diinstal.

03

Temukan peristiwa akses file

Periksa LNK files, Jump Lists, dan Recent Files untuk mengidentifikasi file yang diakses.

04

Tentukan waktu pelepasan USB

Cari Event ID 2003 di Windows Event Log untuk mengkonfirmasi waktu perangkat dilepas.

05

Korelasikan semua bukti

Gabungkan seluruh artefak dari berbagai sumber menjadi satu narasi kronologis yang kohesif.

06

Produksi timeline investigasi lengkap

Hasilkan laporan timeline profesional yang siap digunakan untuk pelaporan insiden resmi.

💬 Kutipan Penutup

> "A timeline transforms scattered digital artifacts into a clear sequence of events, allowing investigators to understand what happened, when it happened, and how the evidence is connected."

Rekonstruksi timeline bukan hanya tentang mengumpulkan fakta — ini tentang menyusun fakta tersebut menjadi narasi yang dapat dipahami, diverifikasi, dan dipertahankan dalam setiap forum investigasi forensik digital.

Author: Edy Susanto – Founder C-SIX Security **www.csixsecurity.com**