DI-103 USB Forensics Essentials

Modul 1 – Pengantar USB Forensics

Selamat datang di modul pertama DI-103. Dalam modul ini, kita akan menjelajahi dasar-dasar forensik USB — bagaimana perangkat USB meninggalkan jejak digital di sistem Windows, dan bagaimana seorang investigator dapat mengungkap bukti tersebut.

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

Pengantar USB Forensics

Apa itu USB Forensics?

USB Forensics adalah cabang dari digital forensics yang berfokus pada identifikasi, pengumpulan, dan analisis bukti digital yang ditinggalkan oleh perangkat USB ketika terhubung ke sistem komputer. Proses ini mencakup penelusuran artefak sistem operasi, registry, dan log kejadian.

Mengapa USB Penting sebagai Bukti Digital?

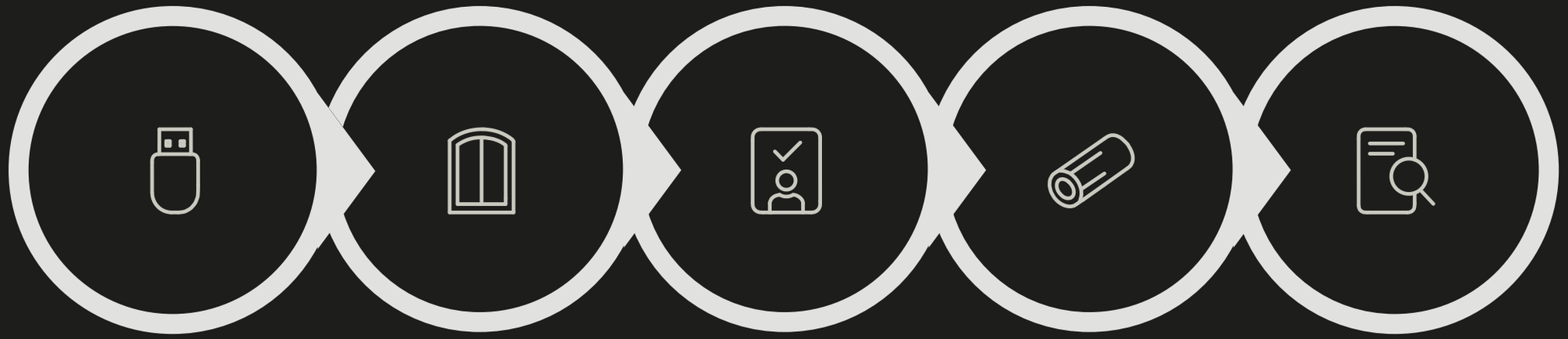
Perangkat USB adalah salah satu vektor transfer data yang paling umum digunakan. Dalam banyak kasus kejahatan siber, pencurian data, atau kebocoran informasi, perangkat USB memainkan peran kunci. Setiap koneksi USB meninggalkan jejak yang dapat dilacak oleh investigator.

- Transfer data yang sulit dipantau secara real-time
- Digunakan dalam insider threat dan data exfiltration
- Meninggalkan artefak permanen di sistem Windows

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

Bagaimana Windows Mendeteksi Perangkat USB?

Setiap kali sebuah perangkat USB dihubungkan ke sistem Windows, sistem operasi secara otomatis mencatat aktivitas tersebut ke berbagai lokasi penyimpanan artefak digital. Proses ini terjadi secara transparan tanpa sepengetahuan pengguna biasa.



Alur deteksi ini bersifat otomatis dan terjadi dalam hitungan detik. Registry Windows menyimpan metadata perangkat seperti Vendor ID, Product ID, dan Serial Number, sementara Event Log mencatat waktu pertama dan terakhir perangkat terhubung. Kombinasi kedua sumber ini menjadi fondasi investigasi USB forensics.

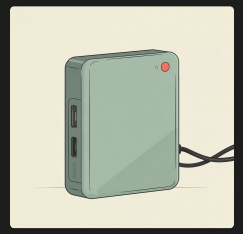
Author: **Edy Susanto** – Founder C-SIX Security | **www.csixsecurity.com**

Jenis-Jenis Perangkat USB yang Umum

Tidak hanya flash drive — hampir semua perangkat yang terhubung melalui port USB dapat meninggalkan artefak digital yang bernilai forensik. Berikut adalah jenis perangkat yang paling sering ditemui dalam investigasi:

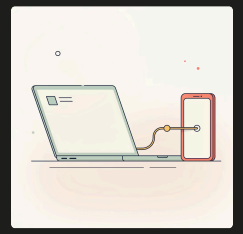
USB Flash Drive

Media penyimpanan portabel paling umum, sering digunakan untuk transfer data.



External HDD / SSD

Penyimpanan kapasitas besar yang sering digunakan untuk backup atau exfiltrasi data masif.



Smartphone & Kamera

Perangkat mobile yang saat terhubung via USB dapat mentransfer foto, video, dan data pribadi.

Adaptor & Periferal

Keyboard, mouse, dan WiFi adapter juga tercatat di registry sebagai perangkat USB.

> Setiap perangkat USB yang pernah terhubung meninggalkan artefak digital — bahkan jika perangkat tersebut telah dicabut.

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

Bukti Digital Apa yang Dapat Ditemukan?

Sistem Windows menyimpan berbagai metadata perangkat USB yang sangat berharga bagi investigator forensik. Berikut adalah artefak utama yang dapat diidentifikasi dari setiap koneksi USB:

Vendor ID (VID)

Kode unik 4 digit yang mengidentifikasi produsen perangkat USB. Ditetapkan oleh USB Implementers Forum.

Product ID (PID)

Kode unik yang mengidentifikasi model spesifik perangkat dari seorang vendor tertentu.

Serial Number

Nomor seri unik yang membedakan satu unit perangkat dari unit lain dengan model yang sama.

First & Last Connected

Timestamp pertama dan terakhir perangkat terhubung, dicatat oleh Event Log dan Registry.

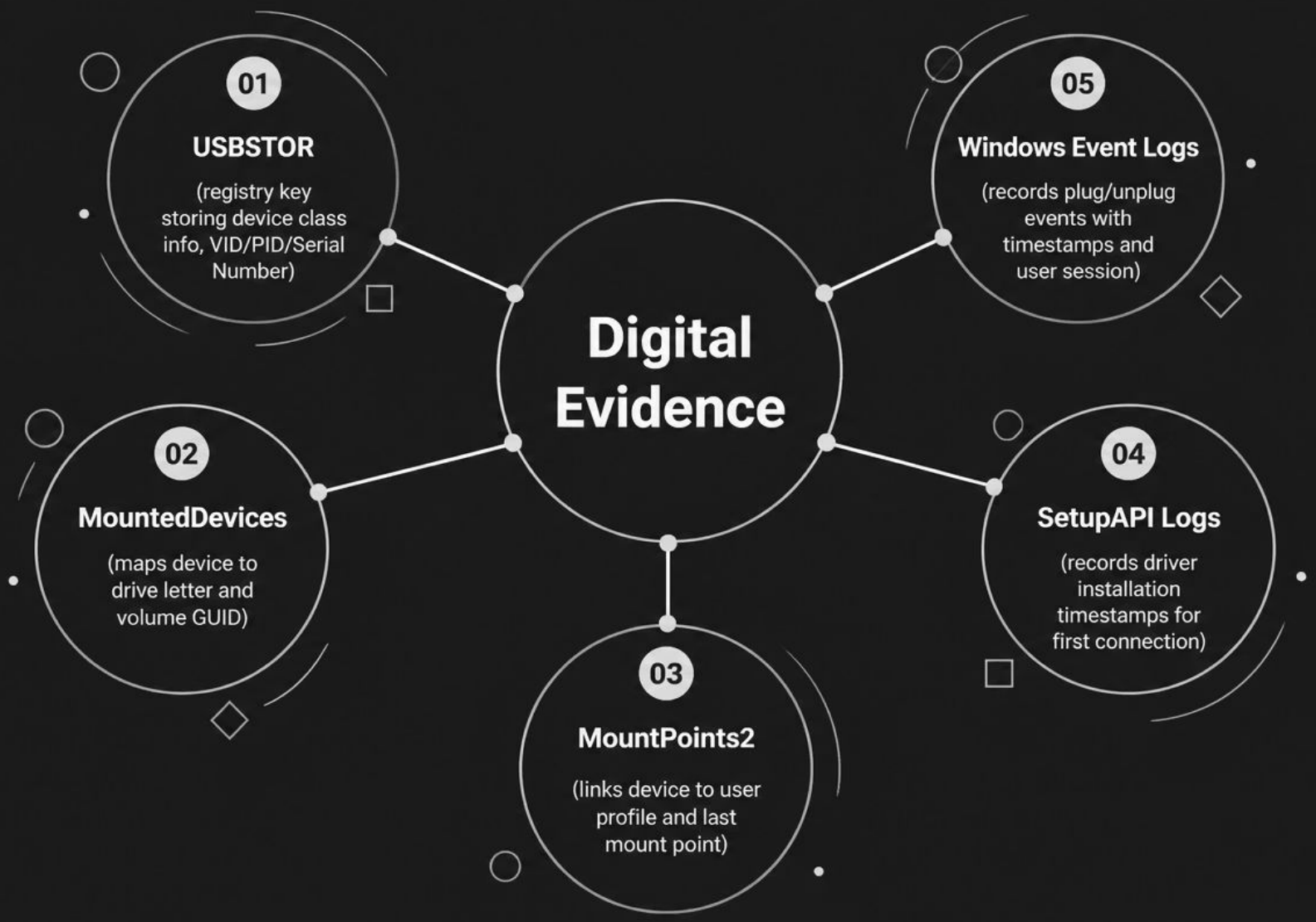
Drive Letter & User Account

Huruf drive yang ditetapkan sistem dan akun pengguna Windows yang aktif saat perangkat terhubung.

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

Di Mana Bukti USB Tersimpan?

Artefak USB tersebar di beberapa lokasi kritis dalam sistem Windows. Seorang investigator harus memeriksa semua lokasi berikut untuk mendapatkan gambaran bukti yang lengkap dan akurat:



Registry Keys Utama

- **USBSTOR**: HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
- **MountedDevices**: HKLM\SYSTEM\MountedDevices
- **MountPoints2**: HKCU\Software\Microsoft\Windows\...\MountPoints2

Log & Setup Files

- **SetupAPI**: C:\Windows\INF\setupapi.dev.log
- **Event Logs**: System, Security, dan Microsoft-Windows-DriverFrameworks

---

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

Case File 001 – Siapa yang Mencolokkan USB?

Misi Investigasi

Anda berperan sebagai investigator digital forensics. Sebuah insiden telah dilaporkan: ada pihak yang tidak berwenang diduga telah mencolokkan perangkat USB ke workstation sensitif perusahaan. Tugas Anda adalah mengungkap identitas perangkat dan pelakunya.

01

Identifikasi Perangkat USB

Temukan entri perangkat di registry USBSTOR dan catat informasi dasar perangkat.

02

Ekstrak VID, PID & Serial Number

Catat Vendor ID, Product ID, dan nomor seri untuk mengidentifikasi perangkat secara unik.

03

Tentukan Waktu Koneksi

Gunakan SetupAPI log dan Event Viewer untuk menentukan kapan pertama dan terakhir perangkat terhubung.

04

Korelasikan dengan Aktivitas Pengguna

Periksa MountPoints2 dan Security Event Log untuk mengidentifikasi akun pengguna yang aktif saat perangkat terhubung.

05

Susun Laporan Investigasi

Dokumentasikan seluruh temuan dalam laporan forensik yang terstruktur dan dapat dipertanggungjawabkan di pengadilan.

> *"Every USB device leaves a digital footprint. An investigator's task is to discover the story behind it."*

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