USB Artifacts Overview

DI-103 | MODUL 2 – INVESTIGASI ARTEFAK USB

Setiap kali perangkat USB dihubungkan ke sistem Windows, sistem operasi secara otomatis mencatat jejak digital di berbagai lokasi — mulai dari Registry Windows, Event Log, hingga profil pengguna. Jejak-jejak ini disebut **USB Artifacts**.

Apa itu USB Artifacts?

Rekaman digital yang tertinggal setiap kali perangkat USB terhubung ke sistem Windows.

Mengapa Bernilai sebagai Bukti?

Artefak mengungkap identitas perangkat, waktu koneksi, dan aktivitas pengguna — krusial dalam investigasi digital.

Setiap Koneksi Meninggalkan Jejak

Registry, log instalasi, dan profil pengguna menjadi saksi bisu dari setiap perangkat yang pernah terhubung.

Sumber Artefak Utama

- Windows Registry (USBSTOR)
- Windows Event Log
- SetupAPI.dev.log
- User Profile & LNK Files
- Timeline & Prefetch

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

SLIDE 2 – REGISTRY FORENSICS

USBSTOR Registry Key

Registry key `HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR` adalah sumber forensik utama untuk mengidentifikasi setiap perangkat penyimpanan USB yang pernah terhubung ke sistem Windows. Setiap subkey mewakili satu perangkat unik.

Vendor ID (VID)

Mengidentifikasi produsen perangkat USB. Contoh: `VID_0781` = SanDisk.

Product ID (PID)

Mengidentifikasi model spesifik perangkat. Contoh: `PID_5567` = Cruzer Blade.

Serial Number

String unik yang membedakan satu unit perangkat dari unit lainnya — kunci identifikasi forensik.

Device Description

Nama deskriptif perangkat seperti `USB Mass Storage Device` yang dicatat Windows secara otomatis.

Path lengkap: `HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR\[DeviceType&VID&PID]\[SerialNumber]`

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

SLIDE 3 – VOLUME & USER MAPPING

MountedDevices & MountPoints2

Dua registry key ini bekerja bersama untuk mencatat **hubungan antara perangkat USB, huruf drive yang ditetapkan, dan profil pengguna** yang menggunakannya. Informasi ini sangat penting untuk membuktikan siapa yang menggunakan perangkat tertentu.

MountedDevices

`HKLM\SYSTEM\MountedDevices` — Menyimpan pemetaan antara perangkat fisik dan huruf drive (E:, F:, G:) yang ditetapkan oleh sistem.

MountPoints2

`HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2` — Mencatat huruf drive per profil pengguna, menunjukkan akses individual.

Nilai Forensik

Menghubungkan perangkat USB spesifik dengan akun pengguna Windows yang melakukan mount, memperkuat rantai kepemilikan bukti.

Alur Hubungan Forensik

Profil Pengguna

Akun Windows yang melakukan mount perangkat

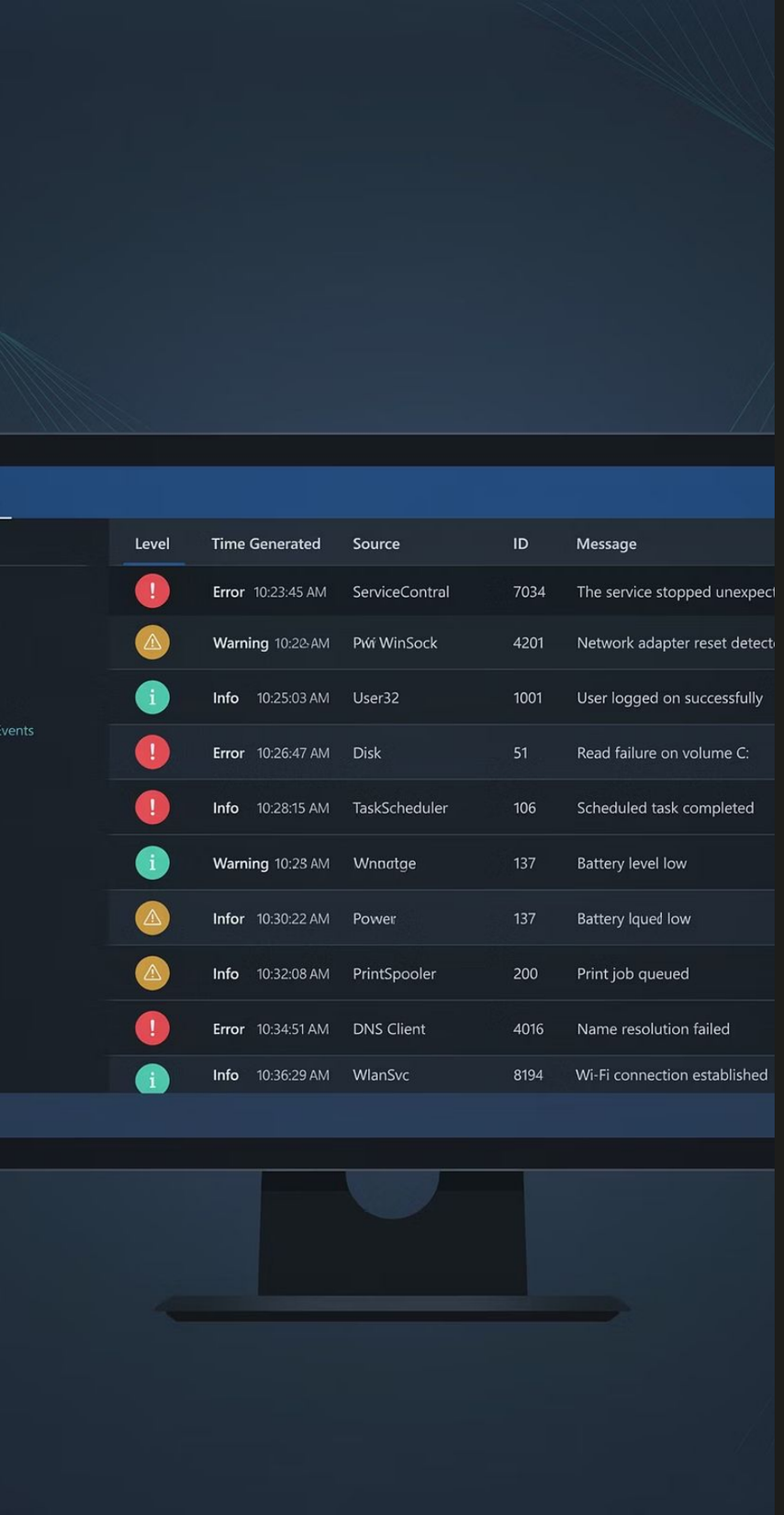
Huruf Drive (E:, F:, G:)

Drive letter yang ditetapkan sistem

Perangkat USB

Identitas fisik perangkat (VID/PID/Serial)

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



SLIDE 4 – LOG & INSTALLATION HISTORY

SetupAPI.dev.log & Windows Event Logs

Dua sumber log ini mencatat **riwayat instalasi driver dan aktivitas hardware perangkat USB** secara kronologis, memberikan bukti berbasis timestamp yang sangat akurat untuk rekonstruksi timeline forensik.

SetupAPI.dev.log

File log di `C:\Windows\INF\setupapi.dev.log` — mencatat setiap instalasi driver USB beserta **timestamp pertama koneksi**. Ideal untuk membuktikan kapan perangkat pertama kali digunakan.

Windows Event Log

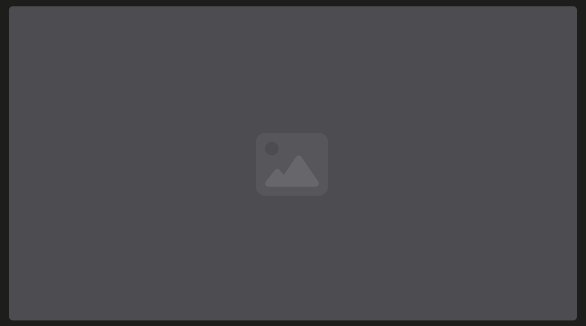
Event ID `2003, 2010, 2100` di `Microsoft-Windows-DriverFrameworks-UserMode` mencatat koneksi dan pemutusan perangkat USB secara real-time.

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

SLIDE 5 – DIGITAL EVIDENCE DASHBOARD

Bukti yang Dapat Dikumpulkan

Dari satu perangkat USB yang pernah terhubung, seorang analis forensik dapat mengumpulkan sembilan kategori bukti digital berikut — membentuk profil lengkap aktivitas perangkat tersebut.



9

Kategori Bukti

Per perangkat USB yang terkoneksi

3+

Sumber Registry

USBSTOR, MountedDevices, MountPoints2

2

Sumber Log

SetupAPI.dev.log & Windows Event Log

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

CASE FILE 002 – PRAKTIKUM INVESTIGASI

Identifikasi Perangkat USB

Dalam latihan praktikum ini, Anda berperan sebagai analis forensik yang ditugaskan untuk mengidentifikasi perangkat USB mencurigakan yang ditemukan terhubung ke workstation terduga. Ikuti langkah-langkah investigasi berikut secara sistematis.

01

Lokasi USBSTOR

Navigasi ke `HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR` dan catat semua subkey yang ada.

02

Identifikasi VID & PID

Ekstrak Vendor ID dan Product ID dari nama subkey untuk menentukan produsen dan model perangkat.

03

Temukan Serial Number

Catat serial number unik perangkat sebagai kunci identifikasi dalam rantai bukti.

04

Tentukan Waktu Koneksi

Gunakan SetupAPI.dev.log untuk first connection dan Event Log untuk last connection.

05

Dokumentasi Bukti Digital

Susun semua temuan dalam laporan forensik yang dapat dipertanggungjawabkan secara hukum.

Checklist Investigator

- ✅ USBSTOR ditemukan
- ✅ Vendor ID diidentifikasi
- ✅ Product ID diidentifikasi
- ✅ Serial Number dicatat
- ✅ First Connection ditentukan
- ✅ Last Connection ditentukan
- ✅ Bukti didokumentasikan

> "Every USB artifact is a clue. When combined, they reveal the complete story behind a device's activity."

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