Case File 005 – USB Digital Investigation

DI-103 USB FORENSICS ESSENTIALS | MODUL 5 – INVESTIGASI BERKAS KASUS & PELAPORAN

Sebuah dokumen rahasia perusahaan diduga telah disalin ke USB flash drive eksternal. Misi Anda adalah menganalisis bukti digital yang tersedia dan menentukan apa yang sebenarnya terjadi — siapa yang melakukannya, kapan, dan bagaimana.

> 🎯 **Misi Anda:** Analisis artefak digital, bangun timeline kejadian, dan hasilkan laporan investigasi yang komprehensif berdasarkan bukti yang ditemukan.

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

Pengumpulan Bukti Digital

LANGKAH 1 DARI 5

Investigasi USB forensik dimulai dengan identifikasi dan pengumpulan seluruh sumber artefak digital yang relevan. Setiap sumber data harus dikumpulkan, dipreservasi, diverifikasi, dan dikorelasikan secara sistematis sebelum analisis dilakukan.

🗂️ USBSTOR

Registry key yang menyimpan riwayat perangkat USB yang pernah terhubung ke sistem.

💾 MountedDevices

Informasi tentang drive letter yang ditetapkan untuk setiap perangkat USB.

📋 SetupAPI.dev.log

Log instalasi driver yang mencatat timestamp pertama kali perangkat terhubung.

📊 Event Viewer

Windows Event Log mencatat aktivitas koneksi dan diskoneksi perangkat USB.

👤 User Profile

Profil pengguna yang aktif saat perangkat USB dihubungkan ke sistem.

⏱️ Timeline

Rekonstruksi kronologis seluruh aktivitas perangkat USB berdasarkan timestamp artefak.

1

Kumpulkan

2

Preservasi

3

Verifikasi

4

Korelasikan

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

Analisis Bukti Digital

LANGKAH 2 DARI 5

Setelah bukti dikumpulkan, investigator melakukan analisis mendalam terhadap setiap artefak. Daftar periksa berikut memastikan tidak ada elemen penting yang terlewat dalam proses investigasi USB forensik.

Setiap item dalam checklist ini merupakan data point kritis yang membangun gambaran lengkap tentang aktivitas perangkat USB — mulai dari identitas perangkat hingga akun pengguna yang terlibat.

Dokumentasikan setiap temuan dengan screenshot dan hash nilai untuk menjaga integritas bukti digital.

01

Vendor ID (VID)

Identifikasi produsen perangkat USB dari registry USBSTOR.

02

Product ID (PID)

Kode unik produk yang membedakan model perangkat USB.

03

Serial Number

Nomor seri unik yang mengidentifikasi unit perangkat secara spesifik.

04

Device Name

Nama perangkat sebagaimana didaftarkan dalam sistem Windows.

05

First & Last Connected

Timestamp koneksi pertama dan terakhir dari SetupAPI.dev.log dan Event Log.

06

Drive Letter & User Account

Drive letter yang ditetapkan dan akun pengguna yang aktif saat koneksi terjadi.

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

Temuan Investigasi

LANGKAH 3 DARI 5

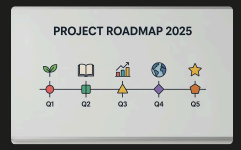
Setelah analisis artefak selesai dilakukan, investigator menyusun temuan ke dalam laporan investigasi yang terstruktur dan komprehensif. Setiap bagian laporan memiliki peran penting dalam menyampaikan kesimpulan investigasi secara objektif.

Ringkasan Eksekutif

Gambaran tingkat tinggi tentang temuan utama dan dampak insiden untuk manajemen.

Temuan Teknis

Detail artefak digital, nilai hash, dan data forensik yang mendukung kesimpulan investigasi.



Timeline Kejadian

Rekonstruksi kronologis aktivitas USB dari koneksi pertama hingga insiden terdeteksi.

Penilaian Risiko & Rekomendasi

Evaluasi dampak keamanan dan langkah mitigasi yang direkomendasikan kepada organisasi.

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

Penulisan Laporan Investigasi

LANGKAH 4 DARI 5

Laporan investigasi digital adalah dokumen formal yang mendokumentasikan seluruh proses dan temuan investigasi. Laporan yang baik harus mampu berdiri sendiri sebagai bukti yang dapat dipertahankan di hadapan manajemen, auditor, atau bahkan pengadilan.

> **"Seorang investigator yang baik mendokumentasikan fakta, bukan asumsi."**

Setiap bagian laporan harus ditulis dengan bahasa yang jelas, objektif, dan berbasis bukti. Hindari spekulasi — setiap pernyataan harus didukung oleh artefak digital yang terverifikasi.

1. **Informasi Kasus**
   Nomor kasus, tanggal, investigator, dan klasifikasi kerahasiaan.
2. **Ruang Lingkup**
   Sistem yang dianalisis, batasan investigasi, dan metodologi yang digunakan.
3. **Bukti yang Dikumpulkan**
   Daftar lengkap artefak digital beserta nilai hash dan chain of custody.
4. **Analisis & Timeline**
   Penjelasan teknis temuan dan rekonstruksi kronologis kejadian.
5. **Kesimpulan & Rekomendasi**
   Temuan akhir berbasis fakta dan langkah mitigasi yang disarankan.

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

Selamat — Misi Selesai!

✅ CASE FILE 005 – DITUTUP

Identifikasi Perangkat USB

VID, PID, Serial Number, dan Device Name berhasil diidentifikasi.

Pemulihan Artefak Digital

Seluruh artefak forensik berhasil dipulihkan dan diverifikasi integritas hash-nya.

Pembangunan Timeline

Kronologi kejadian lengkap berhasil direkonstruksi berdasarkan timestamp artefak.

Korelasi Bukti

Seluruh bukti digital berhasil dikorelasikan untuk membangun narasi investigasi yang kohesif.

Laporan Investigasi

Laporan investigasi formal berhasil disusun dan siap disampaikan kepada pemangku kepentingan.

> *"Bukti digital tidak dapat menceritakan kisahnya sendiri. Seorang investigator yang terampil menghubungkan bukti, memverifikasi fakta, dan menyajikan kesimpulan yang objektif."*

CASE CLOSED — USB FORENSICS ESSENTIALS COMPLETED

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