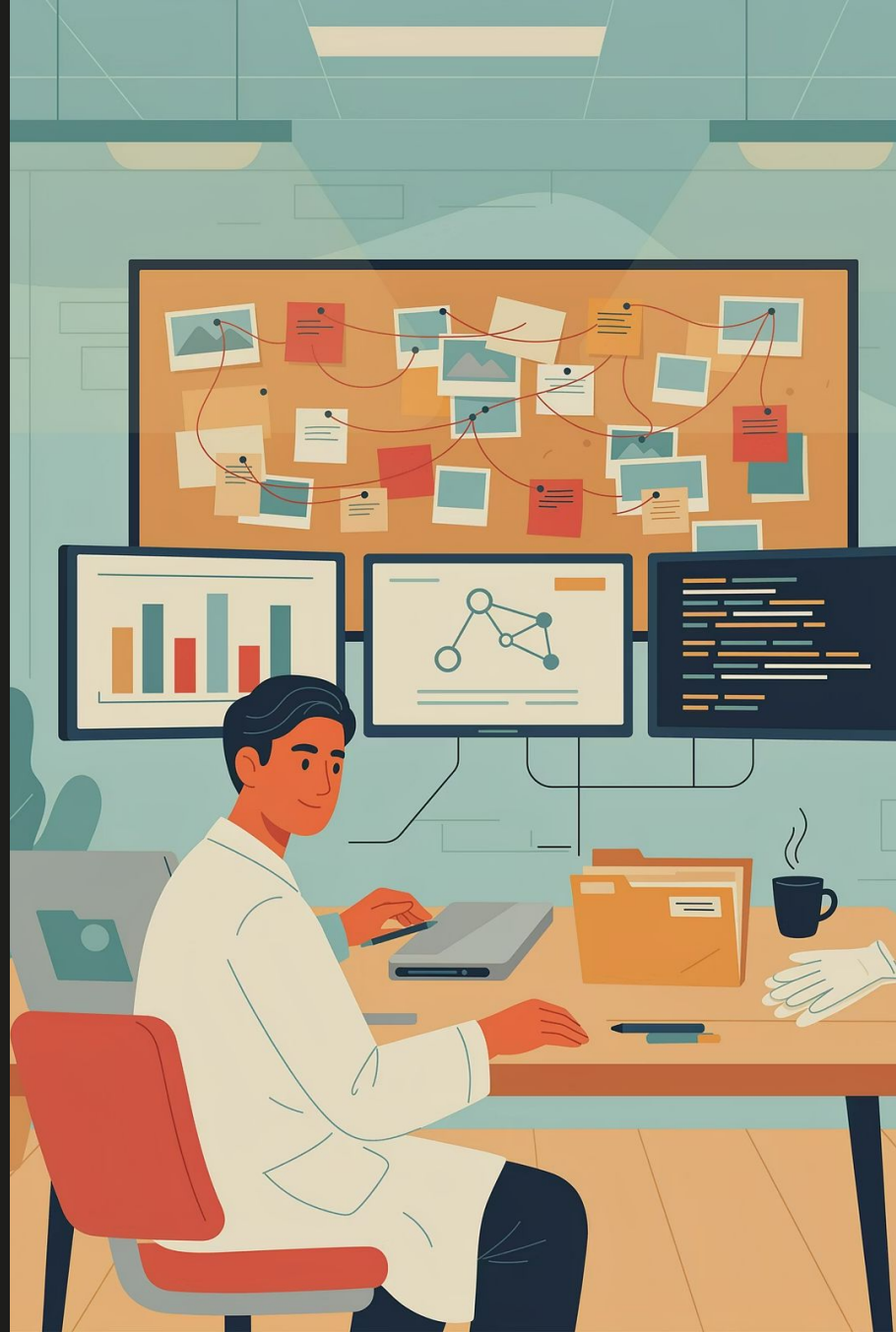
Final Investigation Challenge

Module 6 – Hands-on Lab & Final Challenge

Sebuah perusahaan mencurigai dokumen rahasia telah disalin ke USB flash drive yang tidak diketahui. **Misi Anda** adalah mengidentifikasi perangkat, merekonstruksi timeline, dan menyiapkan laporan investigasi yang komprehensif dan dapat dipertanggungjawabkan secara forensik.

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



Mission Objectives

Setiap investigasi forensik digital dimulai dengan tujuan yang jelas. Berikut adalah daftar pencapaian yang harus Anda selesaikan untuk menuntaskan tantangan akhir ini secara profesional.

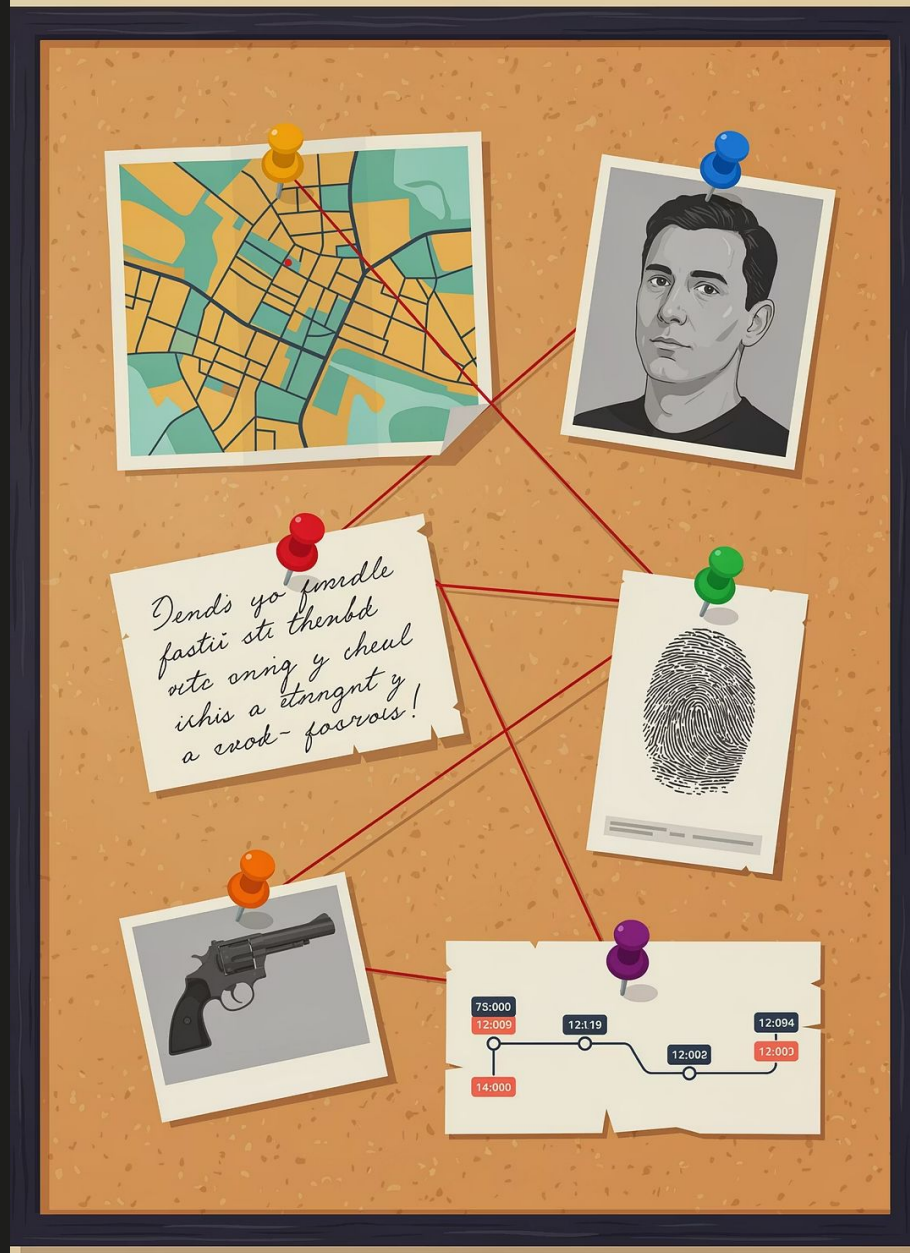
Identifikasi Perangkat

- [x] ~~Identifikasi USB Device~~
- [x] ~~Temukan Vendor ID (VID)~~
- [x] ~~Temukan Product ID (PID)~~
- [x] ~~Pulihkan Serial Number~~
- [x] ~~Tentukan First Connected~~

Investigasi & Pelaporan

- [x] ~~Tentukan Last Connected~~
- [x] ~~Identifikasi Drive Letter~~
- [x] ~~Korelasikan User Account~~
- [x] ~~Bangun Investigation Timeline~~
- [x] ~~Dokumentasikan Semua Bukti~~

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



Investigation Workflow

Alur Kerja DFIR – Digital Forensics & Incident Response

Setiap investigasi USB forensics mengikuti alur kerja yang terstruktur dan berulang. Memahami setiap tahapan memastikan tidak ada artefak digital yang terlewatkan dan seluruh bukti dapat dipertahankan di hadapan hukum.

Setiap tahap dalam alur kerja ini menghasilkan artefak yang menjadi input bagi tahap berikutnya, membangun rantai bukti yang kuat dan tidak terputus dari akuisisi hingga pelaporan akhir.

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

Digital Evidence Dashboard

Dashboard investigasi digital mengintegrasikan seluruh artefak dari berbagai sumber ke dalam satu tampilan terpadu. Setiap panel memberikan informasi kritis yang saling terhubung untuk membangun gambaran lengkap tentang insiden yang terjadi.

USB Device Info

VID, PID, Serial Number, Manufacture String dari Registry USBSTOR

Registry Artifacts

SYSTEM, SOFTWARE, NTUSER.DAT – kunci dan nilai yang mengungkap riwayat koneksi

Event Logs

Windows Event ID 2003, 2100, 7045 – log koneksi dan aktivitas perangkat

User Activity

Korelasi akun pengguna, sesi login, dan waktu koneksi USB

Timeline

Rekonstruksi kronologi lengkap: kapan perangkat pertama dan terakhir digunakan

Investigation Status

Status pengumpulan bukti, verifikasi hash, dan kesiapan laporan final

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

Final Investigation Report

Struktur Laporan Forensik Profesional

Bagian Laporan

01

Executive Summary

Ringkasan singkat temuan dan dampak untuk manajemen

02

Scope & Evidence Collected

Ruang lingkup investigasi dan daftar bukti yang dikumpulkan

03

Analysis & Timeline of Events

Analisis mendalam artefak dan kronologi kejadian

04

Findings, Conclusion & Recommendations

Temuan utama, kesimpulan forensik, dan rekomendasi tindak lanjut

FORENSIC INVESTIGATION REPORT

CASE NO. 2024-FR-0847

EVIDENCE LOG — ITEMIZED RECORD OF COLLECTED MATERIALS

ITEM #	DESCRIPTION	LOCATION	DATE	STATUS
	Latent Fingerprint	Door Handle	03/14/24	Analyzed
	9mm Bullet Casing	Floor, Bedroom	03/14/24	Analyzed
	DNA Sample	Cup Rim	03/15/24	Pending
	Blood Stain	Wall, Hallway	03/14/24	Analyzed
	Shoe Print	Back Door	03/14/24	Pending
	Fiber Strand	Carpet Edge	03/15/24	Pending
006	Tool: Screwdriver	Analyzed	per Fingers	001

Total Items Collected: 6 | Analyzed: 3 | Pending: 3

Investigator Signature *Date*

Investigator profesional hanya melaporkan **fakta yang telah diverifikasi** dan didukung oleh bukti digital yang dapat direproduksi. Tidak ada asumsi — hanya data.

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

MISSION ACCOMPLISHED

Selamat, Investigator! 🎉

Pencapaian yang Telah Diraih

- [x] ~~USB Artifact Investigation~~
- [x] ~~Evidence Collection~~
- [x] ~~Registry Analysis~~
- [x] ~~Timeline Reconstruction~~
- [x] ~~Digital Investigation Reporting~~

> "Every digital device leaves traces. The true investigator knows where to find them, how to analyze them, and how to transform evidence into truth."

Siap untuk Misi Berikutnya?

Lanjutkan perjalanan forensik Anda bersama **DI-104 Windows Artifact Investigation** — menyelami artefak Windows lebih dalam untuk investigasi yang lebih kompleks.

DI-103 USB FORENSICS ESSENTIALS – SELESAI ✓

DI-103 USB FORENSICS ESSENTIALS

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