USB Investigation Toolkit

DI-103 | MODUL 3

Selamat datang di Modul 3 – USB Investigation Tools. Pada modul ini, Anda akan mempelajari seperangkat alat forensik digital yang digunakan oleh para investigator profesional untuk menganalisis aktivitas perangkat USB pada sistem Windows. Mulai dari melihat riwayat perangkat hingga menganalisis Registry dan membuat laporan investigasi yang komprehensif.

🆓 Free Tools

Semua alat dapat diunduh secara gratis

⚡ Fast Investigation

Investigasi cepat dan efisien

🗂️ Registry Analysis

Analisis mendalam Windows Registry

🔍 USB Artifact Collection

Kumpulkan artefak USB secara terstruktur

🕑 Timeline Analysis

Rekonstruksi kronologi kejadian

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

TOOL #1

USBDeview

USBDeview adalah utilitas ringan namun sangat powerful dari NirSoft yang memungkinkan investigator melihat seluruh riwayat perangkat USB yang pernah terhubung ke sistem Windows — baik yang sedang aktif maupun yang telah dicabut. Setiap entri memuat detail teknis lengkap yang sangat berguna dalam proses investigasi forensik digital.

Fitur Utama

→ Riwayat Perangkat USB

Menampilkan semua perangkat USB yang pernah terhubung, lengkap dengan detail historis koneksi.

→ Status Koneksi Aktif & Non-Aktif

Membedakan perangkat yang sedang terhubung dan yang telah dicabut dari sistem.

→ Informasi Vendor & Produk

Menampilkan Vendor ID dan Product ID untuk identifikasi merek dan tipe perangkat.

→ Serial Number Perangkat

Serial number unik yang dapat digunakan sebagai bukti digital dalam laporan investigasi.

→ Timestamp Koneksi Pertama & Terakhir

Merekam waktu pertama kali dan terakhir kali perangkat USB terhubung ke sistem.

Kolom Data Penting di USBDeview

Kolom	Keterangan
Device Name	Nama perangkat USB yang terdeteksi
Vendor ID	ID produsen perangkat (4 digit hex)
Product ID	ID produk spesifik (4 digit hex)
Serial Number	Identifikasi unik perangkat
First Connected	Waktu pertama kali terkoneksi
Last Plug/Unplug	Waktu koneksi atau pemutusan terakhir

USBDeview dapat mengekspor data ke format CSV, HTML, dan XML untuk keperluan dokumentasi laporan forensik.

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

TOOL #2 & #3

Registry Explorer & RegRipper

Windows Registry menyimpan jejak digital yang sangat berharga terkait aktivitas USB. Dua alat ini bekerja secara komplementer: **Registry Explorer** memberikan antarmuka grafis yang canggih untuk membuka dan menjelajahi hive Registry, sementara **RegRipper** mengotomatiskan proses ekstraksi artefak USB secara menyeluruh melalui skrip plugin yang telah dikembangkan khusus untuk forensik.

🗂️ Registry Explorer

- Buka file Registry hive offline (SYSTEM, SOFTWARE, NTUSER.DAT)
- Navigasi ke kunci `USBSTOR` dan `MountedDevices`
- Tampilkan nilai, tipe data, dan timestamp modifikasi
- Bookmarking kunci penting untuk referensi cepat
- Antarmuka modern dan ramah pengguna oleh Eric Zimmerman

⚙️ RegRipper

- Otomatisasi parsing Registry menggunakan plugin Perl
- Ekstrak artefak USB dengan perintah tunggal di command line
- Output laporan teks terstruktur yang siap didokumentasikan
- Plugin `usbstor.pl` dan `usb.pl` untuk forensik USB
- Sangat efisien untuk investigasi skala besar

> Gunakan RegRipper dengan plugin `usb` dan `usbstor` untuk hasil ekstraksi artefak USB yang cepat dan terstruktur.

Kunci Registry USB Penting

Kunci Registry	Informasi
`SYSTEM\USBSTOR`	Daftar perangkat USB storage
`SYSTEM\MountedDevices`	Drive letter yang pernah ditetapkan
`SOFTWARE\Windows\CurrentVersion\Explorer`	Recent USB access history

Manfaat Kombinasi Kedua Alat

Analisis Visual

Registry Explorer untuk navigasi manual

Otomatisasi

RegRipper untuk parsing cepat

Validasi

Silang cek hasil dari dua alat

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

TOOL #4

FTK Imager

FTK Imager dari AccessData (kini Exterro) adalah standar industri dalam forensik digital untuk membuka, mem-browse, dan mengekspor isi forensic image tanpa mengubah bukti asli. Alat ini bersifat **read-only**, sehingga integritas barang bukti digital tetap terjaga sepenuhnya — memenuhi standar chain of custody yang dipersyaratkan dalam proses hukum.

Buka Forensic Image

Mendukung format .E01, .dd, .AFF, dan raw image. Buka bukti digital tanpa risiko modifikasi data asli.

Browse Bukti Secara Aman

Navigasi struktur direktori Windows, termasuk folder sistem, file tersembunyi, dan slack space.

Ekspor File Registry

Ekstrak hive Registry (SYSTEM, SOFTWARE, NTUSER.DAT) langsung dari image untuk dianalisis lebih lanjut.

Preservasi Bukti Asli

Mode read-only memastikan tidak ada perubahan pada forensic image. Hash MD5/SHA1 diverifikasi otomatis.

Analisis Read-Only

Setiap aksi dilakukan tanpa menulis ke media asli. Aman untuk investigasi hukum dan audit internal.

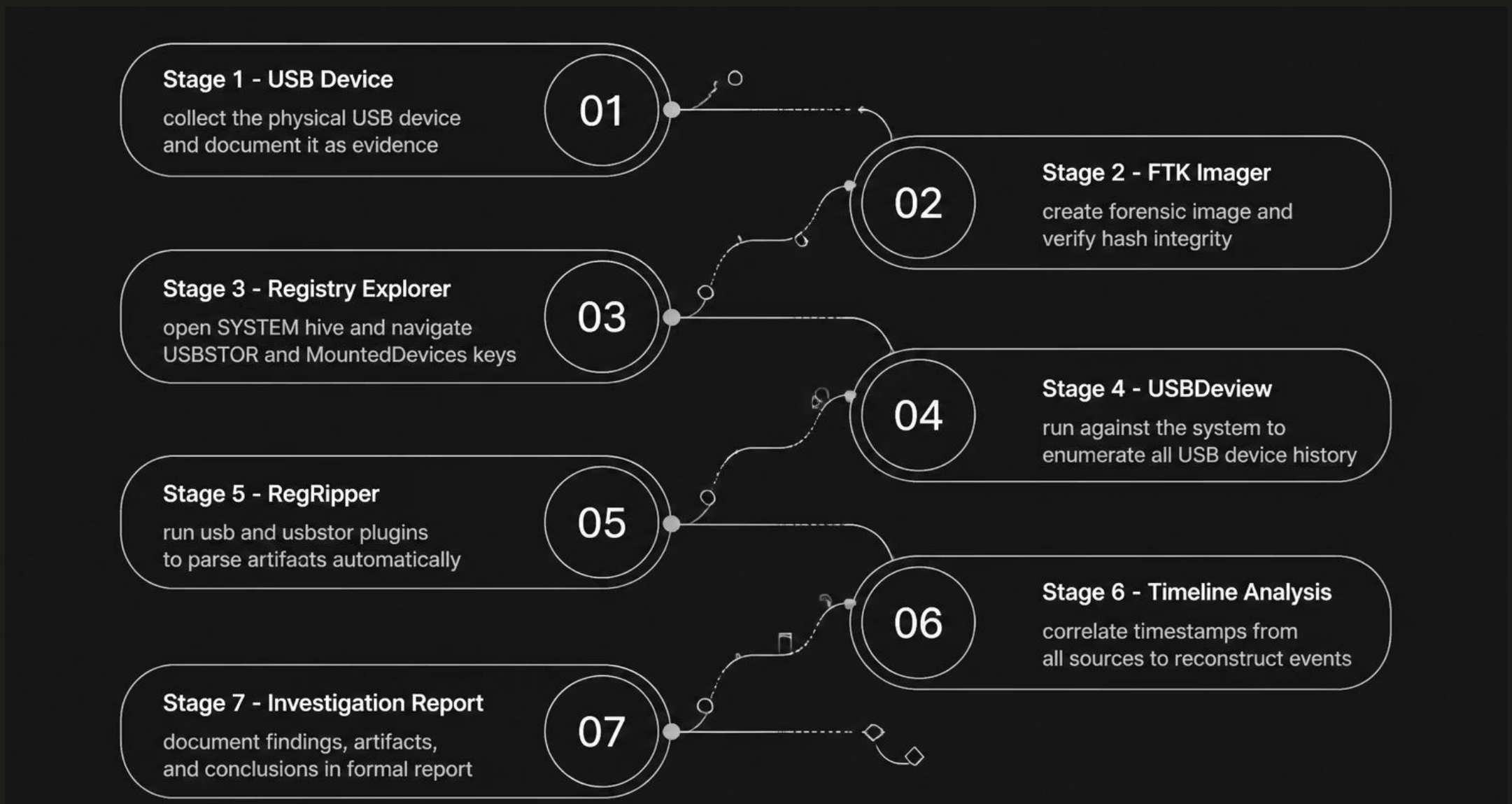
Selalu verifikasi hash MD5 dan SHA-1 sebelum dan sesudah membuka forensic image menggunakan FTK Imager untuk memastikan integritas barang bukti digital.

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

WORKFLOW INVESTIGASI

Alur Investigasi USB yang Direkomendasikan

Berikut adalah alur kerja DFIR (Digital Forensics and Incident Response) yang terstruktur dan sistematis untuk menginvestigasi aktivitas perangkat USB. Setiap tahapan dirancang untuk memastikan bukti digital terkumpul, dianalisis, dikorelasikan, dan dilaporkan dengan standar forensik yang dapat dipertanggungjawabkan secara hukum.



1

🗂️ Collect

Kumpulkan perangkat USB dan buat forensic image menggunakan FTK Imager

2

🔍 Analyze

Analisis Registry dengan Registry Explorer dan ekstrak artefak dengan RegRipper

3

🔗 Correlate

Korelasikan data dari USBDeview, Registry, dan timestamp untuk membangun timeline

4

📄 Report

Dokumentasikan seluruh temuan dalam laporan investigasi yang terstruktur dan formal

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

CASE FILE 003

Which Tool Should You Use?

Dalam investigasi forensik nyata, seorang analis tidak hanya mengandalkan satu alat. **Case File 003** menantang Anda untuk membuka bukti forensik, mengidentifikasi artefak USB, dan membandingkan hasil dari beberapa alat sekaligus — layaknya seorang investigator profesional yang memvalidasi setiap temuan sebelum menarik kesimpulan.

🎯 Misi Investigasi Anda

01

Buka Forensic Evidence

Gunakan FTK Imager untuk membuka forensic image dan verifikasi integritas hash.

02

Identifikasi USB Artifacts

Navigasi ke USBSTOR dan MountedDevices menggunakan Registry Explorer.

03

Bandingkan Hasil Beberapa Alat

Jalankan USBDeview dan RegRipper, lalu bandingkan temuan dari masing-masing alat.

04

Validasi Temuan

Silang cek serial number, timestamp, dan vendor ID dari semua sumber data.

05

Catat Bukti Digital

Dokumentasikan setiap artefak yang ditemukan beserta sumber dan konteksnya.

06

Siapkan Catatan Investigasi

Susun investigation notes yang terstruktur sebagai dasar laporan akhir.

Perbandingan Cepat: Pilih Alat yang Tepat

Skenario	Alat Utama	Alat Pendukung
Lihat riwayat USB cepat	USBDeview	–
Analisis Registry mendalam	Registry Explorer	RegRipper
Buka forensic image	FTK Imager	Registry Explorer
Parsing otomatis cepat	RegRipper	USBDeview
Investigasi lengkap DFIR	Semua alat	Timeline Analysis

> *"The best investigators never rely on a single tool. They verify every finding using multiple sources of digital evidence."*

Selalu gunakan minimal dua alat yang berbeda untuk memvalidasi setiap artefak USB yang Anda temukan dalam investigasi forensik.

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