Browser Forensics Case Study

MODUL 6

Investigasi mendalam terhadap artefak browser — dari riwayat kunjungan hingga cookies — untuk membangun timeline kejadian dan menghasilkan laporan forensik yang komprehensif dan dapat dipertanggungjawabkan.

*Author: **Edy Susanto** — Founder, CSix Security*

Tujuan Modul

Pada modul ini, peserta akan menjalani proses investigasi forensik browser secara menyeluruh — mulai dari analisis artefak digital hingga penyusunan laporan resmi yang siap digunakan dalam konteks hukum maupun audit keamanan.

🔍 Identifikasi

Menentukan browser yang digunakan dan profil pengguna yang relevan dalam dataset latihan.

📊 Analisis Artefak

Mengekstrak dan menginterpretasikan history, pencarian, unduhan, bookmark, dan cookies.

🗓️ Timeline

Menyusun urutan kronologis aktivitas browser berdasarkan timestamp artefak digital.

📝 Pelaporan

Menulis laporan investigasi yang terstruktur, akurat, dan dapat dipertanggungjawabkan.

Author: Edy Susanto — Founder, CSix Security

Studi Kasus: Skenario Investigasi

Peserta menerima sebuah **image atau dataset latihan** yang berisi rekam jejak aktivitas browser dari subjek investigasi. Dataset ini mensimulasikan kondisi nyata di lapangan — termasuk artefak tersembunyi, data terhapus, dan jejak aktivitas yang memerlukan analisis mendalam.

> Dataset latihan dirancang untuk mencerminkan skenario forensik dunia nyata, sehingga peserta dapat melatih kemampuan analisis dalam lingkungan yang aman dan terkontrol.

Author: Edy Susanto — Founder, CSix Security

Tugas Investigasi Browser

Berikut adalah delapan tugas utama yang harus diselesaikan oleh setiap peserta selama proses investigasi. Setiap tugas menghasilkan temuan yang berkontribusi pada laporan akhir.

01

Identifikasi Browser

Tentukan jenis dan versi browser yang digunakan oleh subjek investigasi.

02

Analisis Website yang Dikunjungi

Ekstrak dan evaluasi daftar URL yang telah diakses beserta frekuensi kunjungan.

03

Analisis Riwayat Pencarian

Temukan kata kunci yang dicari melalui mesin pencari seperti Google, Bing, dll.

04

Analisis File yang Diunduh

Identifikasi file-file yang diunduh, termasuk nama, sumber URL, dan waktu unduh.

Author: Edy Susanto — Founder, CSix Security

Tugas Investigasi Browser (Lanjutan)

01

Analisis Bookmark

Periksa bookmark yang tersimpan untuk mengidentifikasi situs yang dianggap penting oleh subjek.

02

Analisis Cookies

Ekstrak data cookies untuk mengungkap sesi login, preferensi, dan aktivitas autentikasi.

03

Menyusun Timeline

Gabungkan semua artefak ke dalam satu garis waktu yang menggambarkan urutan aktivitas.

04

Menulis Laporan Investigasi

Dokumentasikan seluruh temuan secara sistematis dalam format laporan forensik resmi.

Author: Edy Susanto — Founder, CSix Security

Final Project: Deliverables

Sebagai puncak dari Modul 6, setiap peserta wajib menghasilkan **lima dokumen resmi** yang mencerminkan standar laporan forensik profesional. Dokumen-dokumen ini merupakan bukti kompetensi investigasi Anda.

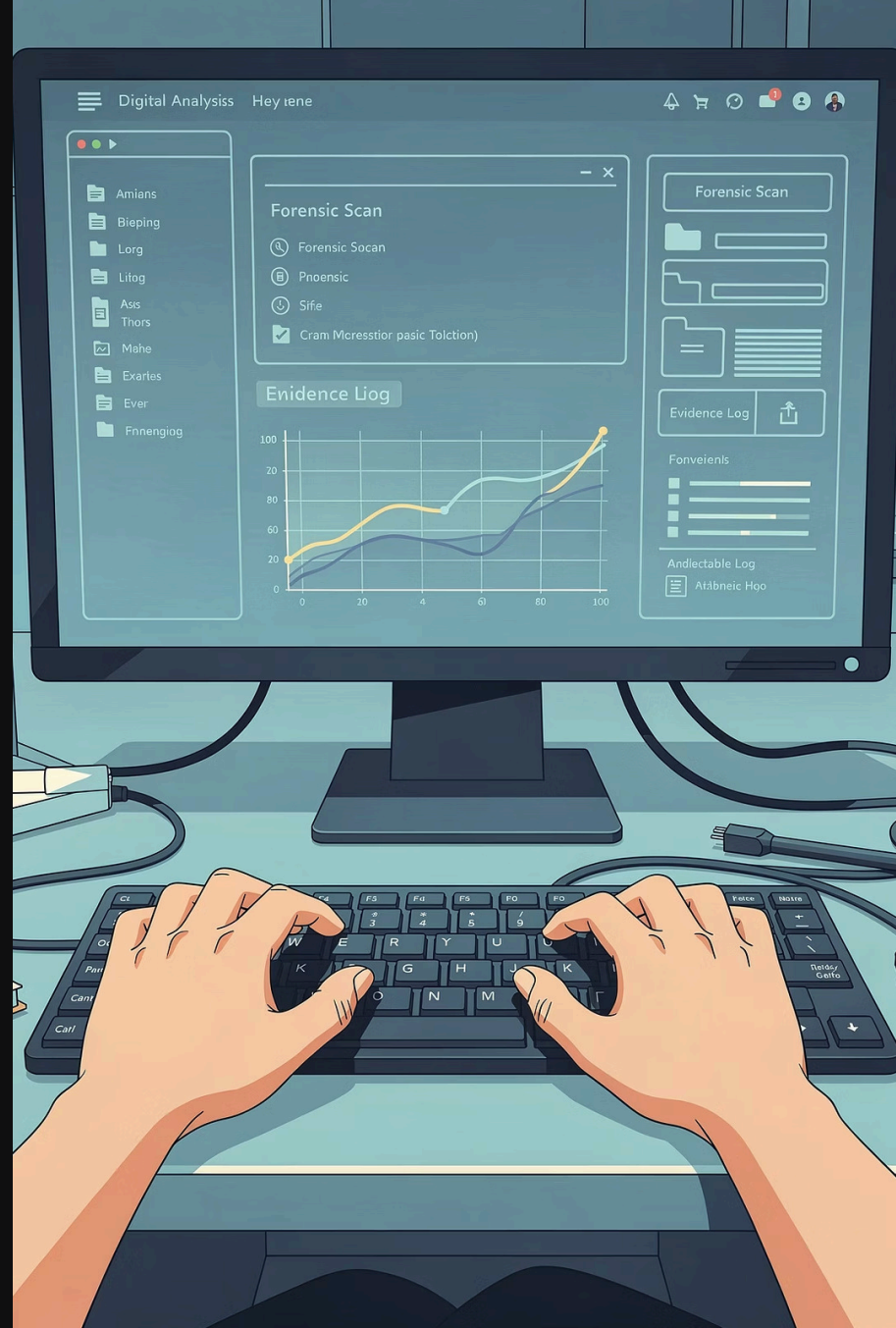
1	**Browser Investigation Report** Laporan teknis komprehensif yang mendokumentasikan seluruh artefak yang ditemukan dan metodologi analisis yang digunakan.
2	**Timeline of Events** Rekonstruksi kronologis aktivitas browser subjek dari awal hingga akhir periode investigasi.
3	**Executive Summary** Ringkasan eksekutif non-teknis untuk pemangku kepentingan, menyoroti temuan kritis dan dampaknya.
4	**Technical Findings** Rincian teknis mendalam mencakup data mentah, hash file, dan evidensi digital yang valid secara hukum.
5	**Recommendations** Rekomendasi tindak lanjut berdasarkan temuan — baik untuk keperluan hukum maupun perbaikan keamanan.

Author: Edy Susanto — Founder, CSix Security

Hands-on Lab

Laboratorium praktik dirancang agar peserta dapat langsung berinteraksi dengan dataset forensik nyata menggunakan tools yang tersedia. Setiap latihan mengarah pada pembangunan kemampuan investigasi yang holistik.

Author: Edy Susanto — Founder, CSix Security



Aktivitas Lab: Langkah demi Langkah

Peserta mengikuti alur investigasi yang terstruktur — dari ekstraksi data mentah hingga korelasi artefak menjadi satu narasi investigatif yang koheren.

1

History Browsing

Temukan dan ekstrak riwayat kunjungan website dari database browser.

2

Pencarian Google

Identifikasi query pencarian yang pernah dimasukkan oleh pengguna.

3

Riwayat Unduhan & Bookmark

Analisis file yang diunduh dan simpan bookmark untuk membangun pola perilaku.

4

Cache & Korelasi

Telusuri cache browser, lalu hubungkan semua artefak menjadi satu timeline terpadu.

Hasil akhir lab adalah **laporan investigasi lengkap** yang menggabungkan seluruh temuan dari setiap langkah di atas.

Author: Edy Susanto — Founder, CSix Security

Tools yang Digunakan

Investigasi forensik browser memerlukan kombinasi tools bawaan sistem dan aplikasi pihak ketiga. Berikut adalah ekosistem tools yang digunakan dalam modul ini.

🛠️ Built-in Tools

Tools yang sudah tersedia di sistem Windows tanpa instalasi tambahan:

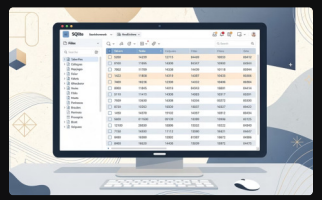
- **SQLite Database Browser** — membuka file database browser secara langsung
- **Windows Explorer** — navigasi dan lokasi file artefak browser
- **PowerShell** — otomatisasi ekstraksi dan analisis data berbasis skrip

🆓 Free & Optional Tools

- **DB Browser for SQLite** — antarmuka grafis untuk analisis database SQLite
- **NirSoft Browser Tools** — suite utilitas ringan untuk ekstraksi artefak browser
- **Hindsight** — analisis Chrome/Chromium berbasis Python (konsep & demo)
- **Browser History Examiner** — opsional, jika lisensi tersedia
- **Autopsy** — platform forensik lengkap untuk integrasi artefak browser

Author: Edy Susanto — Founder, CSix Security

Tools Snapshot: Fungsi Utama

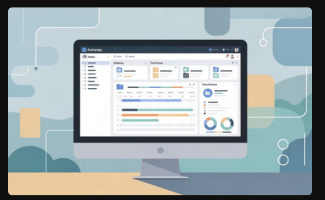


DB Browser for SQLite

Membuka dan menjalankan query SQL pada file `History`, `Cookies`, dan `Web Data` milik browser Chromium secara visual dan intuitif.

NirSoft Browser Tools

Kumpulan utilitas ringan seperti `BrowsingHistoryView` dan `ChromeCookiesView` yang mampu mengekstrak artefak tanpa instalasi rumit.



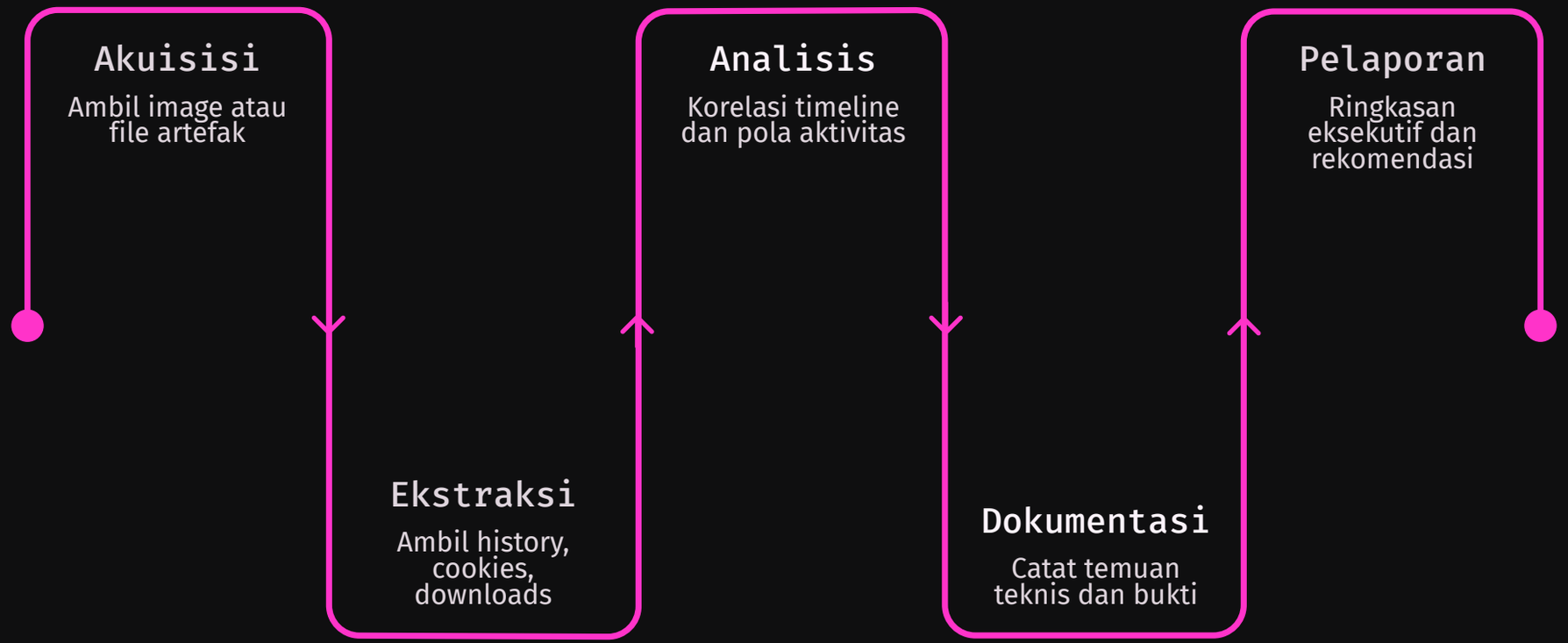
Autopsy

Platform forensik open-source yang mengintegrasikan analisis artefak browser dalam konteks investigasi disk image yang lebih luas.

Author: Edy Susanto — Founder, CSix Security

Alur Investigasi Browser: Gambaran Menyeluruh

Investigasi forensik browser mengikuti alur yang sistematis — dari akuisisi data mentah hingga penyampaian laporan akhir kepada pemangku kepentingan.



Setiap tahap dalam alur ini menghasilkan output yang menjadi input bagi tahap berikutnya, memastikan integritas dan ketertelusuran bukti digital sepanjang proses investigasi.

Author: Edy Susanto — Founder, CSix Security

Siap Menjadi Investigator Forensik Browser?

Modul 6 membekali Anda dengan keterampilan praktis dan metodologi profesional untuk mengungkap jejak digital melalui artefak browser — kompetensi kritis dalam setiap investigasi forensik digital modern.

🎯 Praktis

Hands-on lab dengan dataset nyata

🛠️ Terstruktur

Metodologi investigasi yang sistematis

📄 Profesional

Output laporan siap pakai dan standar industri

Edy Susanto *— Founder, CSix Security*