Modul 1: Introduction to Browser Forensics

Menyingkap Jejak Digital di Balik Layar

EDY SUSANTO — FOUNDER CSIX SECURITY

Apa Itu Browser Forensics?

Seni Menemukan Jejak

Mengidentifikasi aktivitas digital yang tersisa di web browser setelah sesi berakhir.

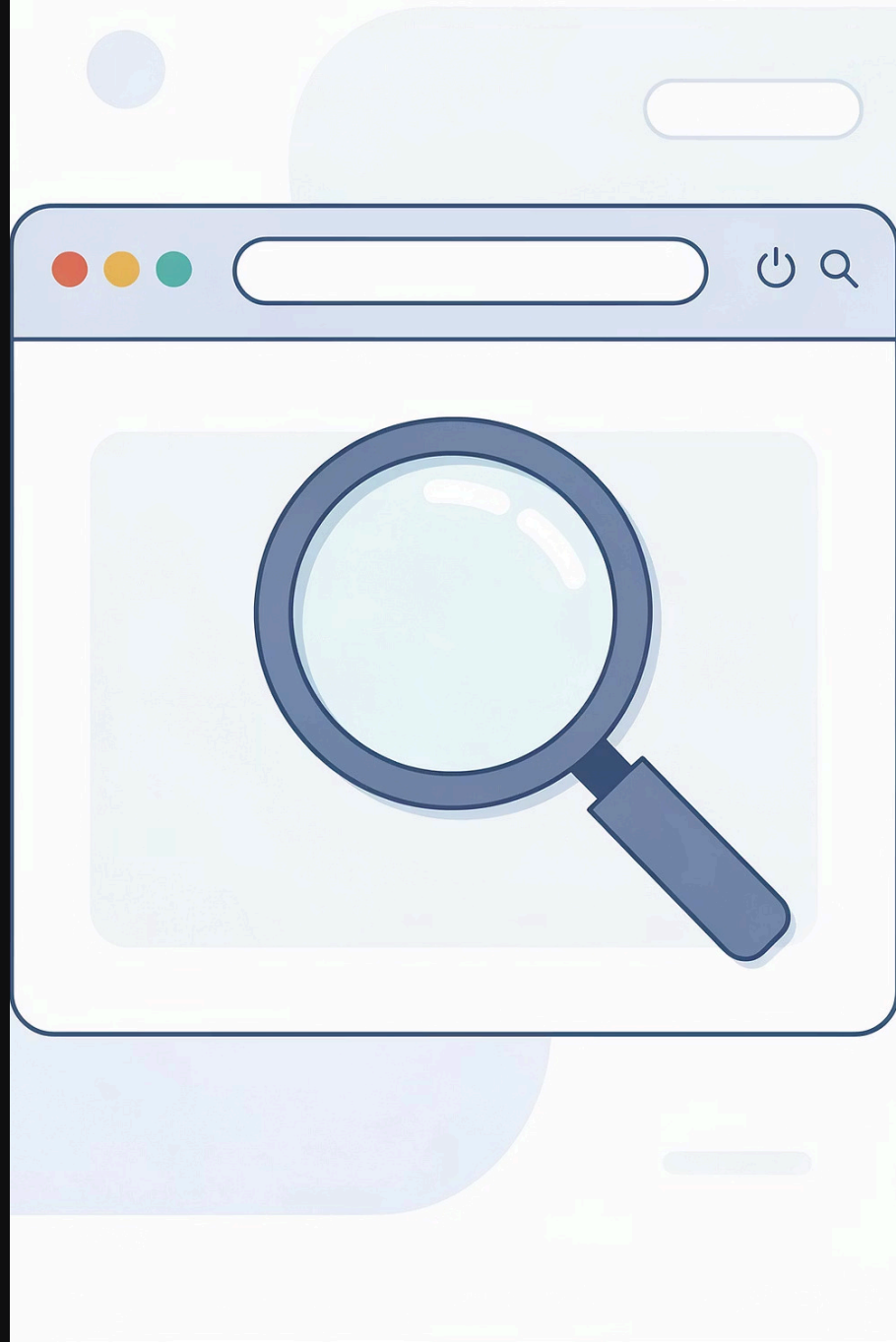
Dari Data ke Bukti Hukum

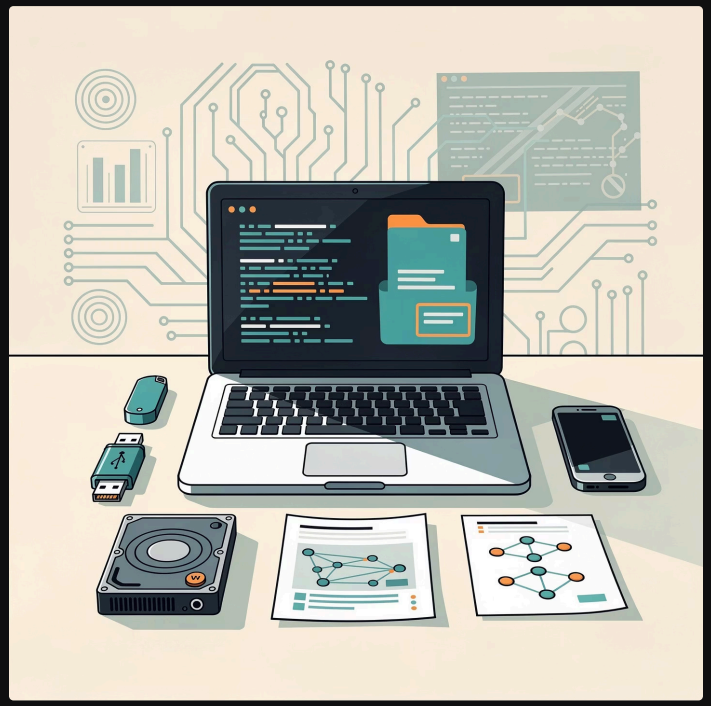
Mengubah data teknis mentah menjadi bukti digital yang sah secara hukum.

Rekonstruksi Perilaku

Bukan sekadar riwayat URL — melainkan pembuktian pola dan niat pengguna.

Edy Susanto — Founder CSIX Security





DIGITAL EVIDENCE

Browser sebagai Digital Evidence

Peramban adalah **pintu gerbang utama** hampir semua kejahatan siber modern. Setiap aksi meninggalkan artefak yang dapat dianalisis.

Edy Susanto — Founder CSIX Security

Sumber Bukti Vital

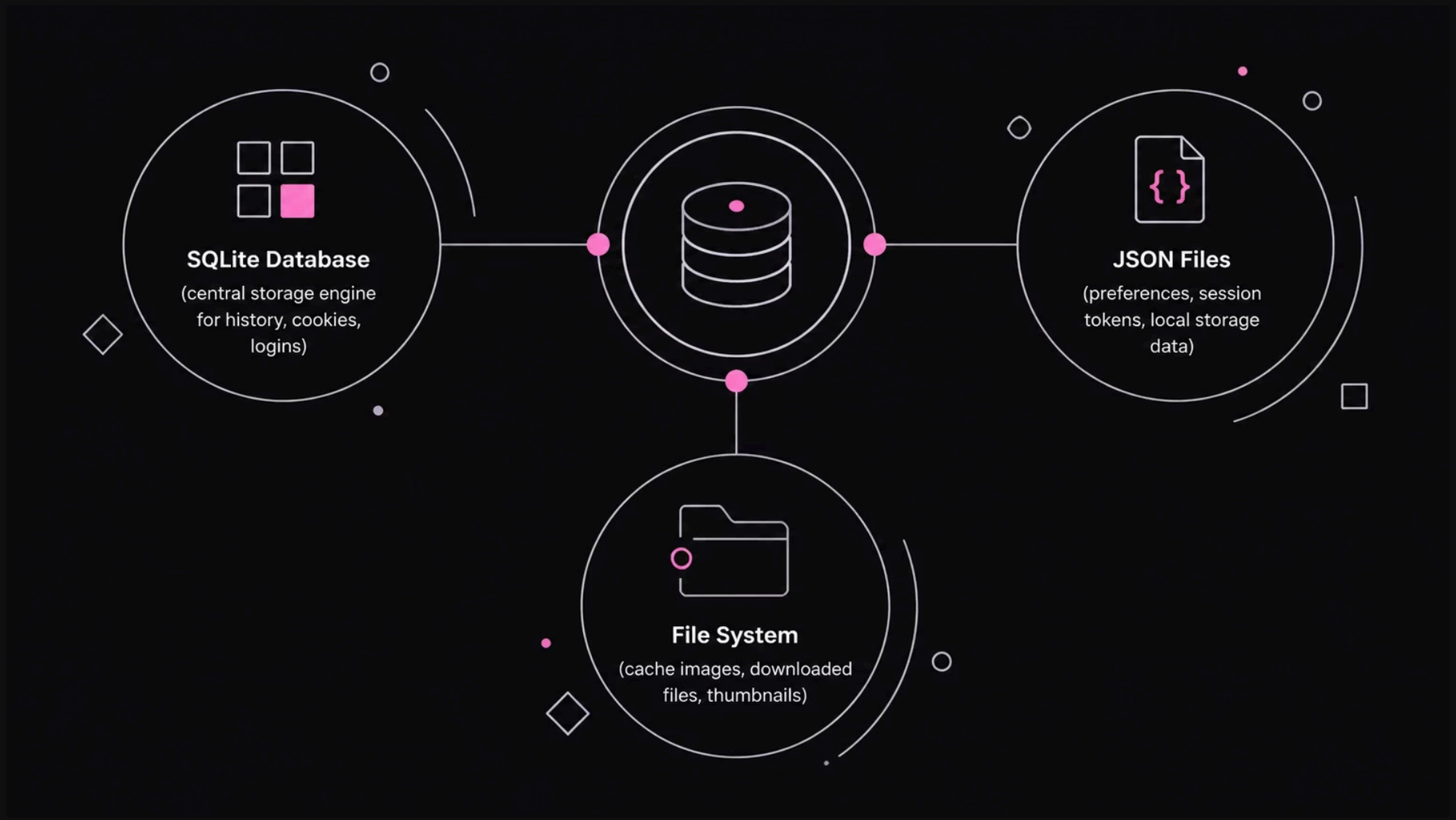
Email, hoax, ujaran kebencian, hingga transaksi penipuan daring.

Rekonstruksi Kejadian

Mengungkap alur lengkap dari sisi korban maupun pelaku.

Browser Storage Architecture

Bagaimana browser menyimpan seluruh memori aktivitas Anda — dari kunjungan situs hingga sesi login.



Edy Susanto — Founder CSIX Security

Chromium vs Firefox

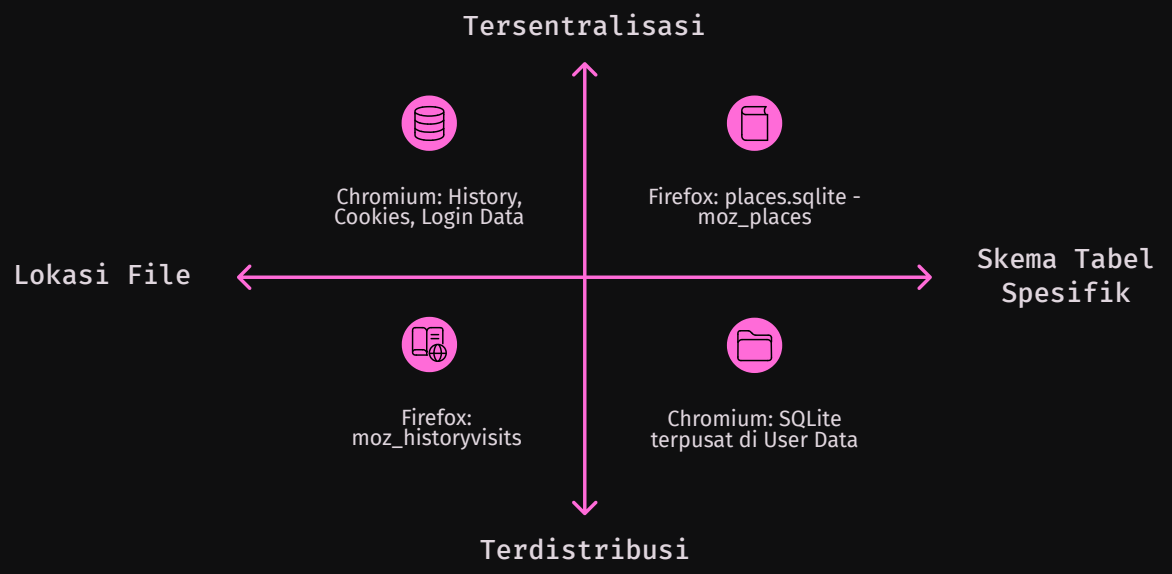
Memahami perbedaan arsitektur kedua ekosistem browser terbesar adalah kunci untuk ekstraksi data yang akurat.

🔵 Chromium-Based

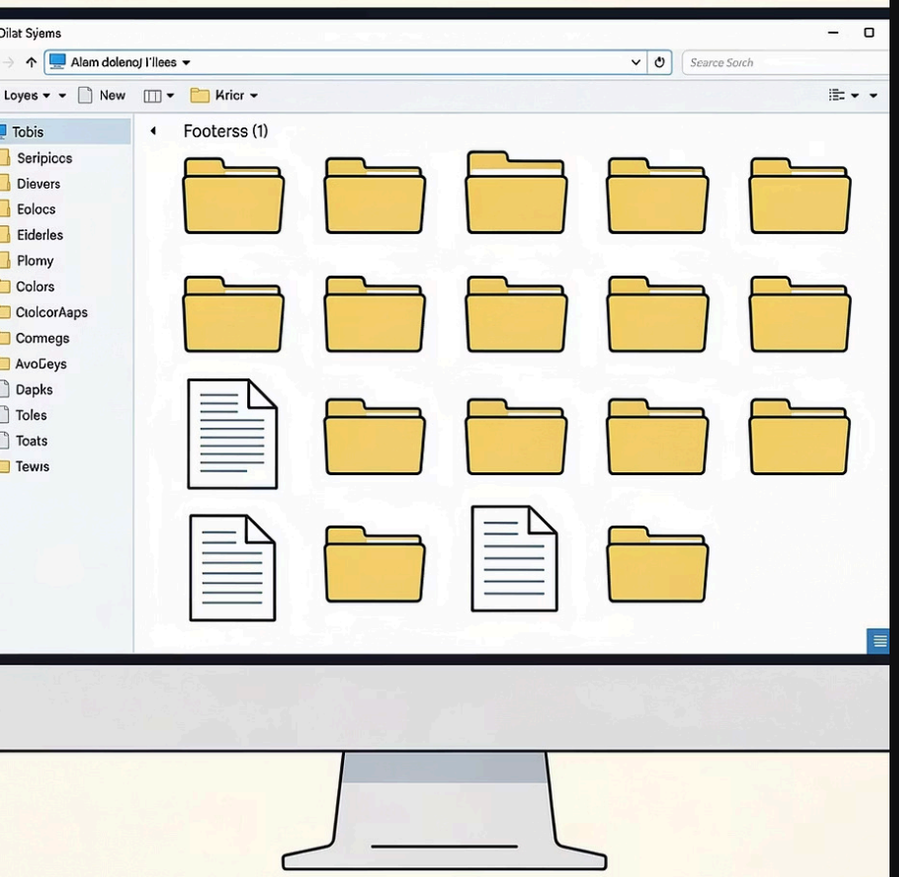
Chrome, Edge, Opera menggunakan **database SQLite terpusat** dengan tabel yang seragam di folder User Data.

🦊 Firefox

Menggunakan file **places.sqlite** dengan skema relasi berbeda, memerlukan pendekatan ekstraksi tersendiri.



Edy Susanto — Founder CSIX Security



Mengintip Isi File System

Data browser bersembunyi di folder tersembunyi sistem operasi. Berikut jalur lokasi utama di **Windows**:

1	**Google Chrome** `%USERPROFILE%\AppData\Local\Google\Chrome\User Data\`
2	**Microsoft Edge** `%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\`
3	**Mozilla Firefox** `%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\`

Edy Susanto — Founder CSIX Security

Praktik: Lokasi Data Browser

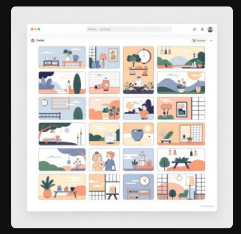
Empat kategori artefak utama yang menjadi target investigator forensik dalam setiap pemeriksaan browser:

History

Rekam jejak situs yang dikunjungi beserta timestamp akses.

Cookies

Token identitas sesi pengguna yang menyimpan status autentikasi.



Cache

Potongan gambar dan teks halaman web yang tersimpan lokal.

Download

Daftar file yang pernah diunduh, lengkap dengan URL sumber.

LAB SESSION

Lab: Bedah Profil Pengguna

Sesi langsung mengakses dan menganalisis profil browser secara forensik menggunakan tool khusus.

Edy Susanto — Founder CSIX Security

01

Akses Profil

Navigasi ke folder profil Chrome, Edge, dan Firefox.

02

Buka Database History

Gunakan SQLite browser untuk membaca file `History`.

03

Analisis Tabel

Eksplorasi tabel `visits` dan `keyword_search_term`.

Tantangan Utama: Incognito Mode

❌ Mitos

Mode penyamaran tidak meninggalkan jejak apapun dan aktivitas sepenuhnya tersembunyi dari investigator.

✅ Fakta

Live Forensic dan analisis **RAM dump** mampu mengungkap aktivitas incognito yang dianggap telah terhapus. Data residu tetap eksis selama sesi berlangsung.

⚠ Investigator harus selalu mempertimbangkan analisis memori volatile dalam setiap kasus.

Edy Susanto — Founder CSIX Security

Outcome: Menjadi Investigator Forensik

Pemahaman Arsitektur

Peserta memahami struktur penyimpanan browser secara mendalam.

Ekstraksi Sistematis

Siap melakukan akuisisi dan analisis artefak browser secara terstruktur.

Kesiapan Investigatif

Mampu menghadapi skenario nyata termasuk tantangan incognito mode.

> *"Setiap klik meninggalkan jejak, setiap jejak menceritakan sebuah kisah."*
>
> *Edy Susanto — Founder CSIX Security*