Chrome & Edge Artifact Analysis

Modul 2 — Forensik Browser Berbasis Chromium

Panduan teknis untuk menganalisis artefak digital yang tersimpan dalam browser Chrome dan Edge. Modul ini mencakup identifikasi, ekstraksi, dan interpretasi data forensik dari berbagai komponen database browser.

EDY SUSANTO — FOUNDER CSIX SECURITY

Gambaran Umum Modul

Apa yang Akan Kita Pelajari?

Modul 2 dirancang untuk membekali analis forensik dengan kemampuan membaca dan menginterpretasikan artefak browser berbasis Chromium secara menyeluruh — dari riwayat penelusuran hingga data sesi aktif.

🎯 Tujuan

Menganalisis artefak pada browser berbasis Chromium secara forensik dan metodologis

🛠️ Praktik

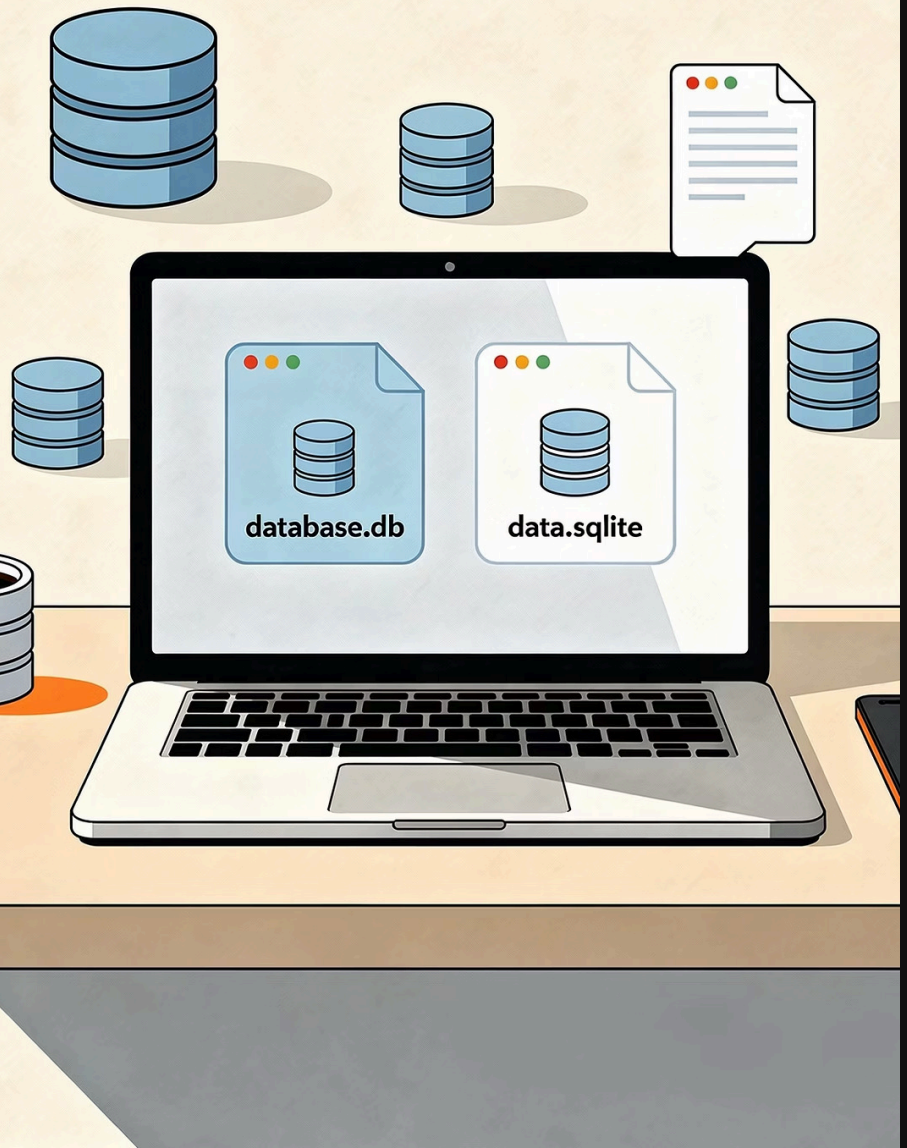
Menggunakan tools khusus untuk membaca database browser secara aman tanpa memodifikasi bukti

🔬 Lab

Investigasi aktivitas browsing nyata pada lingkungan latihan yang terkontrol

✅ Outcome

Peserta mampu mengidentifikasi dan mendokumentasikan riwayat penggunaan browser



Fondasi Teknis

Chromium & SQLite: Basis Penyimpanan Artefak

Browser berbasis Chromium — termasuk Google Chrome dan Microsoft Edge — menyimpan hampir semua data pengguna dalam format **SQLite database**. File-file ini terletak di direktori profil pengguna dan dapat dibaca menggunakan tools forensik tanpa perlu menjalankan browser.

Lokasi Profil Chrome

`C:\Users\[User]\AppData\Local\Google\Chrome\User Data\Default\`

Lokasi Profil Edge

`C:\Users\[User]\AppData\Local\Microsoft\Edge\User Data\Default\`

EDY SUSANTO — FOUNDER CSIX SECURITY

Artefak Utama

History Database & Visited URLs

File `History` adalah database SQLite yang menyimpan catatan lengkap aktivitas penelusuran pengguna. Ini merupakan salah satu sumber bukti paling kritis dalam investigasi forensik browser.

Tabel `urls`

URL yang dikunjungi, jumlah kunjungan, dan timestamp terakhir akses

Tabel `visits`

Detail setiap kunjungan termasuk durasi dan transition type (link, typed, redirect)

Tabel `keyword_search_terms`

Kata kunci yang diketikkan langsung di address bar atau search engine

Timestamp disimpan dalam format **WebKit/Chrome Time** — mikrosecond sejak 1 Januari 1601. Konversi diperlukan untuk membaca waktu yang dapat dibaca manusia.

Nilai forensik: Visited URLs dapat membuktikan kesadaran pengguna terhadap suatu konten, mengidentifikasi platform yang digunakan, dan membangun timeline aktivitas digital secara kronologis.

Artefak Utama

Downloads & Search Terms

Downloads

Tabel `downloads` dalam file History mencatat setiap file yang diunduh: path target, URL sumber, waktu mulai dan selesai, ukuran file, serta status unduhan. Bahkan file yang telah dihapus dari disk masih meninggalkan rekam jejak di sini. Ini menjadikannya bukti kuat untuk kasus eksfiltrasi data atau unduhan konten ilegal.

Search Terms

Tabel `keyword_search_terms` merekam istilah pencarian yang digunakan pengguna melalui search engine yang terdaftar. Data ini sangat bernilai untuk membuktikan *intent* atau niat pengguna — misalnya pencarian yang menunjukkan perencanaan suatu tindakan sebelum insiden terjadi.

Artefak Identitas Pengguna

Bookmarks, Autofill & Login Data

Kelompok artefak ini mengungkap kebiasaan, preferensi, dan kredensial pengguna — memberikan gambaran profil digital yang lebih dalam kepada investigator.

Bookmarks

Disimpan dalam file JSON `Bookmarks`. Berisi URL, judul, tanggal penambahan, dan struktur folder. Menunjukkan situs yang dianggap penting oleh pengguna.

Autofill Data

Database `Web Data` menyimpan formulir yang pernah diisi otomatis: nama, alamat, nomor telepon, dan data pribadi lainnya yang sering digunakan.

Login Data

File `Login Data` menyimpan kredensial terenkripsi menggunakan Windows DPAPI. Investigator dapat mengidentifikasi akun mana yang disimpan meski tidak dapat membaca password secara langsung.

Artefak Pelengkap

Cookies, Favicons & Top Sites

🍪 Cookies

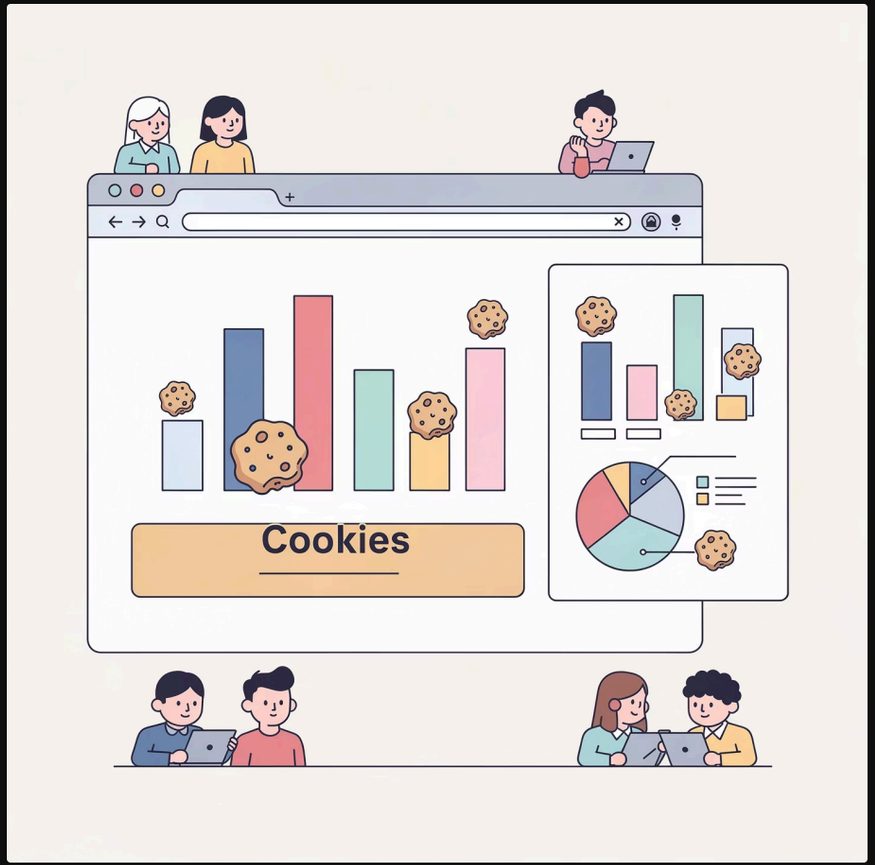
Database Cookies menyimpan data sesi web: nama cookie, domain, nilai (terenkripsi sejak Chrome 80+), waktu pembuatan, dan waktu kedaluwarsa. Cookies dapat membuktikan autentikasi ke suatu layanan pada waktu tertentu.

⭐ Favicons

Database Favicons menyimpan ikon situs yang pernah dikunjungi. Menariknya, favicon dapat tersimpan bahkan untuk situs yang telah dihapus dari riwayat — memberikan bukti tambahan yang tersembunyi.

📌 Top Sites

File Top Sites menyimpan daftar situs yang paling sering dikunjungi untuk tampilan halaman baru. Memberikan gambaran cepat tentang aktivitas rutin pengguna.



Favicons adalah artefak yang sering diabaikan namun sangat berguna — dapat membuktikan kunjungan ke situs yang riwayatnya telah sengaja dihapus.

EDY SUSANTO — FOUNDER CSIX SECURITY

Artefak Sesi

Session Data: Rekam Jejak Sesi Aktif

Session Data merekam kondisi browser saat ditutup — tab yang terbuka, URL masing-masing tab, dan urutan navigasi. File-file ini terletak di folder `Sessions` dan `Current Session` / `Last Session`.

1

Current Session

Tab dan window yang sedang terbuka saat browser aktif berjalan

2

Last Session

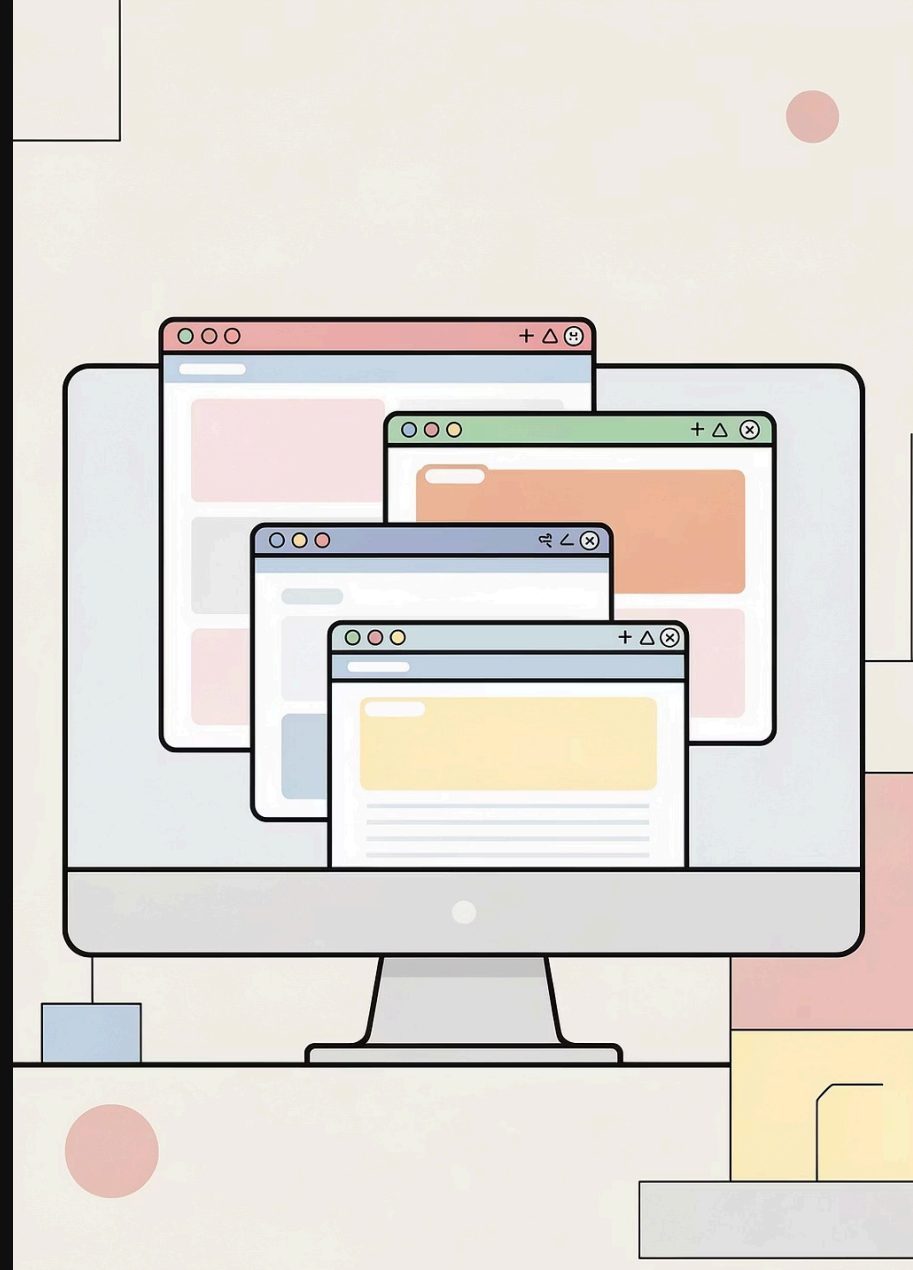
Snapshot sesi terakhir sebelum browser ditutup — dapat dipulihkan

3

Last Tabs

Daftar tab terakhir yang digunakan, berguna untuk membangun timeline aktivitas akhir pengguna

EDY SUSANTO — FOUNDER CSIX SECURITY



Praktik & Lab

Tools Forensik Browser Berbasis Chromium

Membaca database browser secara langsung berisiko mengubah metadata file. Gunakan tools forensik yang dirancang khusus untuk membaca artefak browser secara *read-only* dan menghasilkan laporan yang dapat digunakan sebagai bukti.

DB Browser for SQLite

Tools open-source untuk membuka dan menjalankan query SQL langsung pada file database Chrome/Edge tanpa mengubah konten asli.

BrowsingHistoryView

Tools dari NirSoft yang mengekstrak dan menampilkan riwayat dari berbagai browser secara bersamaan dengan format yang mudah dibaca dan diekspor.

Hindsight

Tools forensik khusus Chromium yang menganalisis seluruh artefak browser dan menghasilkan laporan timeline yang komprehensif dengan dukungan dekripsi cookie.

Autopsy / FTK

Platform forensik digital lengkap dengan modul browser artifact yang mengintegrasikan analisis Chrome/Edge dalam satu alur investigasi terpadu.

EDY SUSANTO — FOUNDER CSIX SECURITY

Ringkasan Modul 2

Outcome & Kompetensi yang Dicapai

Setelah Menyelesaikan Modul Ini

Peserta mampu secara mandiri melakukan analisis forensik browser berbasis Chromium dalam konteks investigasi nyata.

- Mengidentifikasi lokasi dan format semua artefak utama
- Membaca dan menginterpretasikan database SQLite browser
- Membangun timeline aktivitas browsing pengguna
- Menggunakan tools forensik secara aman dan terstandar
- Mendokumentasikan temuan sebagai bukti digital yang valid

01

History & URLs

Riwayat kunjungan, timestamp, dan transition type

02

Downloads & Search Terms

Bukti unduhan dan niat pencarian pengguna

03

Credentials & Autofill

Bookmarks, login data, dan data formulir

04

Cookies, Favicons & Sessions

Artefak sesi, autentikasi, dan bukti tersembunyi