Modul 3: Firefox Artifact Analysis

Analisis mendalam artefak digital browser Mozilla Firefox untuk keperluan investigasi forensik digital.

EDY SUSANTO — FOUNDER CSIX SECURITY

Arsitektur Profil Firefox

Lokasi Profil

Windows: `%APPDATA%\Mozilla\Firefox\Profiles\`
Linux: `~/.mozilla/firefox/`

Sumber Bukti Utama

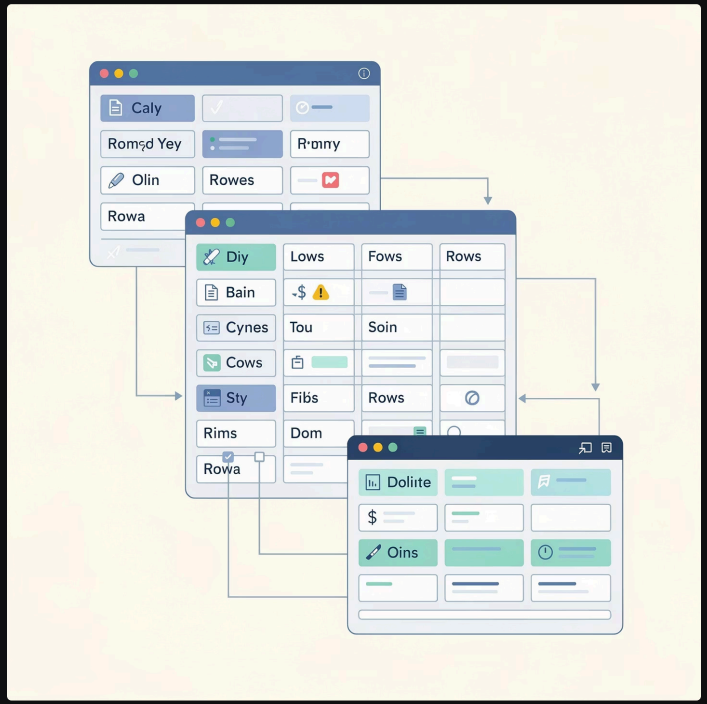
Folder profil menyimpan seluruh jejak aktivitas pengguna — dari riwayat browsing hingga kredensial sesi.

Format SQLite

Hampir semua data forensik Firefox tersimpan dalam database `.sqlite` yang dapat dianalisis secara langsung.

Author: Edy Susanto — Founder CSix Security

Places.sqlite: Inti Forensik Firefox



Dua Tabel Kunci

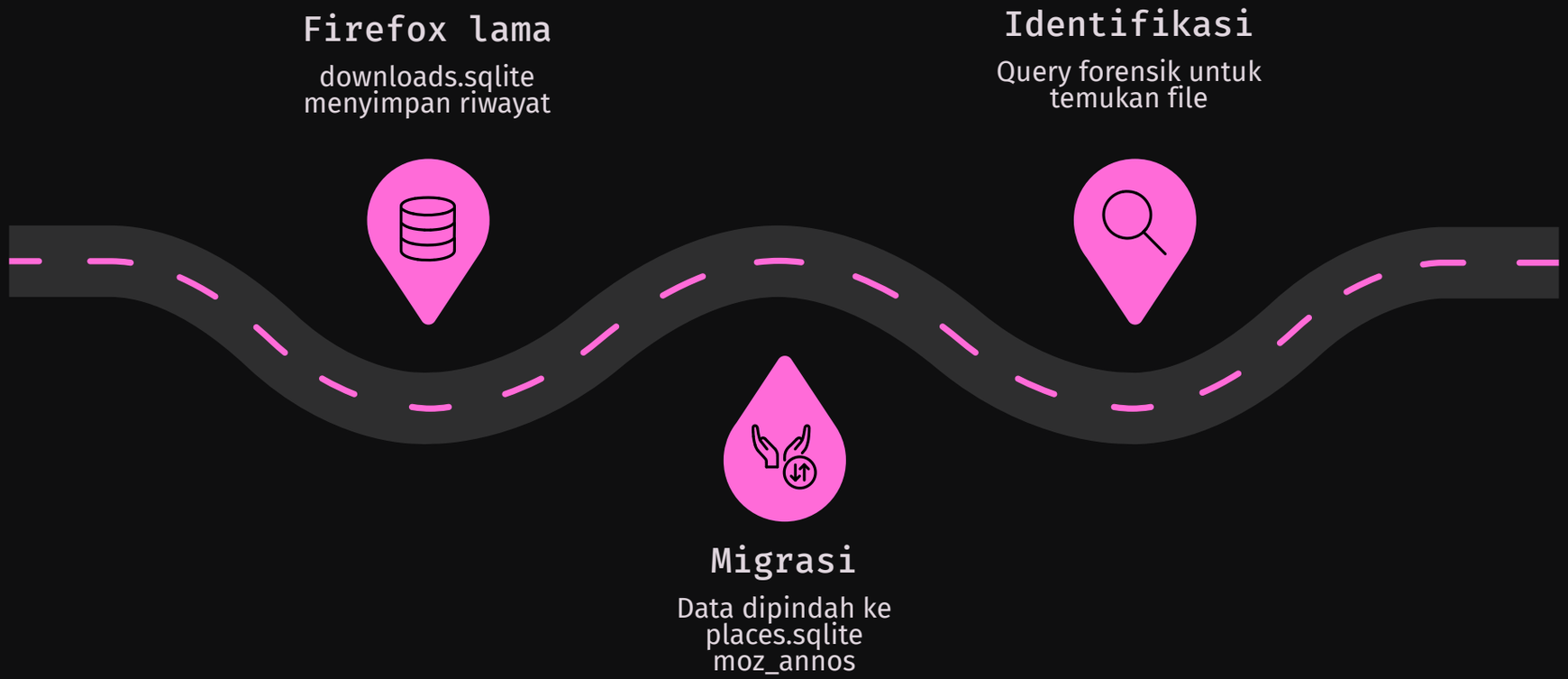
moz_places — menyimpan URL lengkap, judul halaman, jumlah kunjungan, dan metadata situs.

moz_historyvisits — mencatat setiap kunjungan individual dengan timestamp UNIX presisi tinggi.

Korelasi antara kedua tabel ini mengungkap pola kunjungan yang detail dan kronologi aktivitas pengguna secara akurat.

Author: Edy Susanto — Founder CSix Security

Melacak Riwayat Unduhan



Jejak Transfer Data

File yang pernah diunduh meninggalkan metadata penting: URL sumber, ukuran file, waktu mulai dan selesai unduhan.

Relevansi Forensik

Riwayat unduhan menjadi bukti kuat dalam kasus transfer data tidak sah atau eksfiltrasi informasi sensitif.

Author: Edy Susanto — Founder CSix Security

Cookies dan Sesi Aktif

cookies.sqlite

Menyimpan nama, nilai, domain, dan waktu kedaluwarsa cookie. Kunci untuk melacak sesi web yang pernah aktif.

Kredensial & Preferensi

Cookie sering menyimpan token autentikasi dan preferensi login — informasi krusial dalam investigasi akun.

Aktivitas Login

Menganalisis timestamp dan domain cookie dapat mengungkap kapan dan di mana pengguna pernah login ke suatu layanan.

Author: Edy Susanto — Founder CSix Security

Form History dan Session Restore

formhistory.sqlite

Menyimpan semua teks yang pernah diketik pengguna ke dalam form web — termasuk kata kunci pencarian, nama, dan alamat. Data ini sering diabaikan namun sangat bernilai dalam rekonstruksi aktivitas.

- Riwayat input otomatis (autocomplete)
- Kata kunci yang pernah dicari
- Hitungan frekuensi penggunaan tiap entri

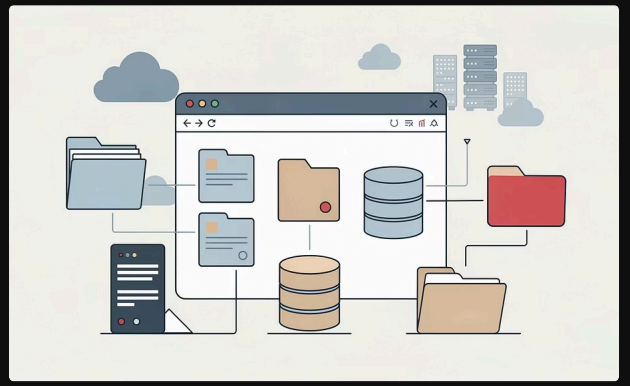
Session Restore

File `sessionstore.jsonlz4` merekam kondisi terakhir browser sebelum ditutup, termasuk tab yang terbuka, scroll position, dan konten formulir yang belum dikirim.

> Data sesi sangat krusial untuk merekonstruksi konteks aktivitas tepat sebelum insiden terjadi.

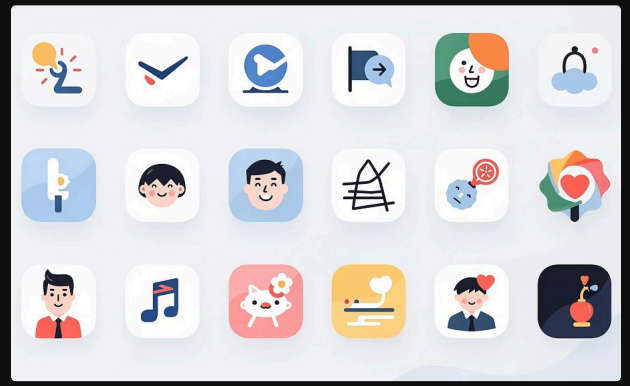
Author: Edy Susanto — Founder CSix Security

Visualisasi Artefak: Cache dan Favicons



Cache Browser

Menyimpan sisa konten web seperti gambar, skrip, dan halaman HTML. Cache dapat mengungkap situs yang dikunjungi meski riwayat telah dihapus.

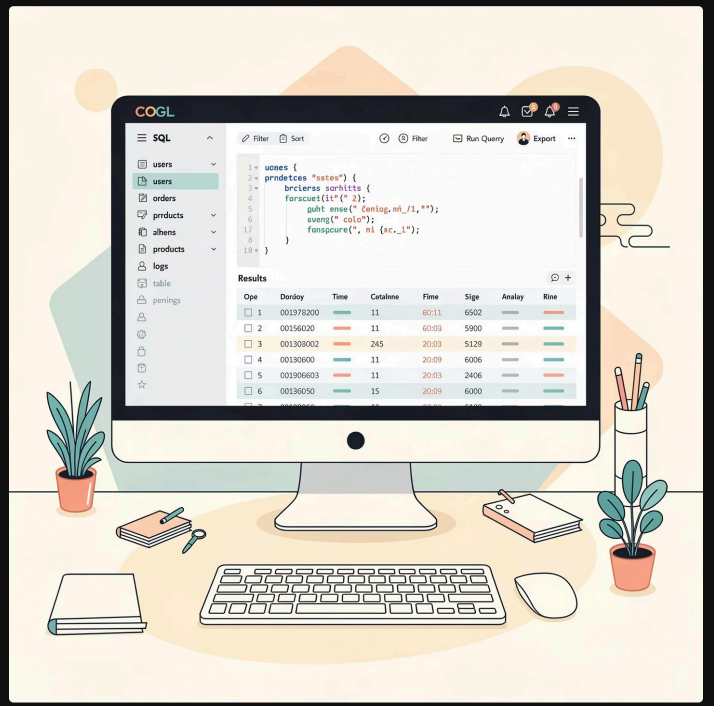


Favicons.sqlite

Menyimpan ikon situs web yang pernah dikunjungi. Pada Firefox versi terbaru, favicon dipisah ke database khusus `favicons.sqlite`.

Author: Edy Susanto — Founder CSix Security

Praktik Analisis Database



Tools & Teknik

DB Browser for SQLite adalah alat utama untuk membuka dan mem-parsing file database Firefox secara visual maupun melalui query.

- Eksplorasi struktur tabel secara langsung
- Query SQL untuk ekstraksi data spesifik
- Join tabel relasional untuk korelasi bukti

> Contoh query: `SELECT url, visit_date FROM moz_places JOIN moz_historyvisits ON id = place_id;`

Author: Edy Susanto — Founder CSix Security

Lab: Rekonstruksi Aktivitas Browsing

01

Muat Profil Latihan

Buka folder profil Firefox yang disediakan sebagai bahan latihan investigasi.

02

Parsing Database

Gunakan DB Browser untuk membuka `places.sqlite`, `cookies.sqlite`, dan `formhistory.sqlite`.

03

Rekonstruksi Kronologi

Korelasikan timestamp dari berbagai artefak untuk membangun timeline aktivitas pengguna secara akurat.

04

Identifikasi Pola Perilaku

Analisis frekuensi kunjungan, unduhan, dan input form untuk mengungkap niat dan kebiasaan pengguna.

Author: Edy Susanto — Founder CSix Security

Kesimpulan dan Outcome

Yang Telah Dipelajari

Peserta kini memahami secara mendalam struktur artefak Firefox — dari places.sqlite hingga session restore — dan cara mengekstrak bukti digital yang valid.

Kompetensi Utama

- Memahami perbedaan struktur tiap artefak Firefox
- Menerapkan metodologi forensik yang presisi dan terulang
- Menerjemahkan data teknis menjadi narasi bukti digital yang dapat dipertanggungjawabkan di hadapan hukum

EDY SUSANTO — FOUNDER CSIX SECURITY