Browser Timeline Reconstruction

Modul 5 — Forensik Browser Digital

Menyusun urutan aktivitas pengguna secara sistematis berdasarkan artefak browser. Modul ini dirancang untuk profesional forensik digital dan investigator keamanan siber yang ingin memahami teknik rekonstruksi timeline secara mendalam.

EDY SUSANTO — FOUNDER CSIX SECURITY

Modul 5 — Browser Timeline Reconstruction

Tujuan Pembelajaran

Pada akhir modul ini, peserta diharapkan mampu merekonstruksi aktivitas browser secara sistematis, menganalisis korelasi antar artefak digital, dan mendokumentasikan temuan sebagai bukti yang dapat digunakan dalam proses investigasi.

Rekonstruksi Timeline

Menyusun urutan aktivitas pengguna dari artefak browser secara kronologis dan terstruktur.

Analisis Korelasi

Menghubungkan data dari berbagai sumber artefak untuk membangun gambaran aktivitas yang utuh.

Dokumentasi Bukti

Menyusun laporan investigasi yang akurat, terverifikasi, dan siap digunakan secara legal.

EDY SUSANTO — FOUNDER CSIX SECURITY

Modul 5 — Browser Timeline Reconstruction

Struktur Materi Modul

Modul ini mencakup enam topik utama yang dirancang secara berurutan untuk membangun kompetensi investigasi browser dari dasar hingga tingkat lanjut.

01

Timeline Analysis

Teknik dasar penyusunan kronologi aktivitas dari data artefak browser.

02

Correlation Analysis

Metode menghubungkan artefak dari berbagai sumber untuk validasi temuan.

03

Browser Sessions

Identifikasi dan analisis sesi browsing termasuk tab, window, dan waktu aktif.

04

Multiple Browser Investigation

Investigasi lintas browser: Chrome, Firefox, Edge, dan browser lainnya secara simultan.

05

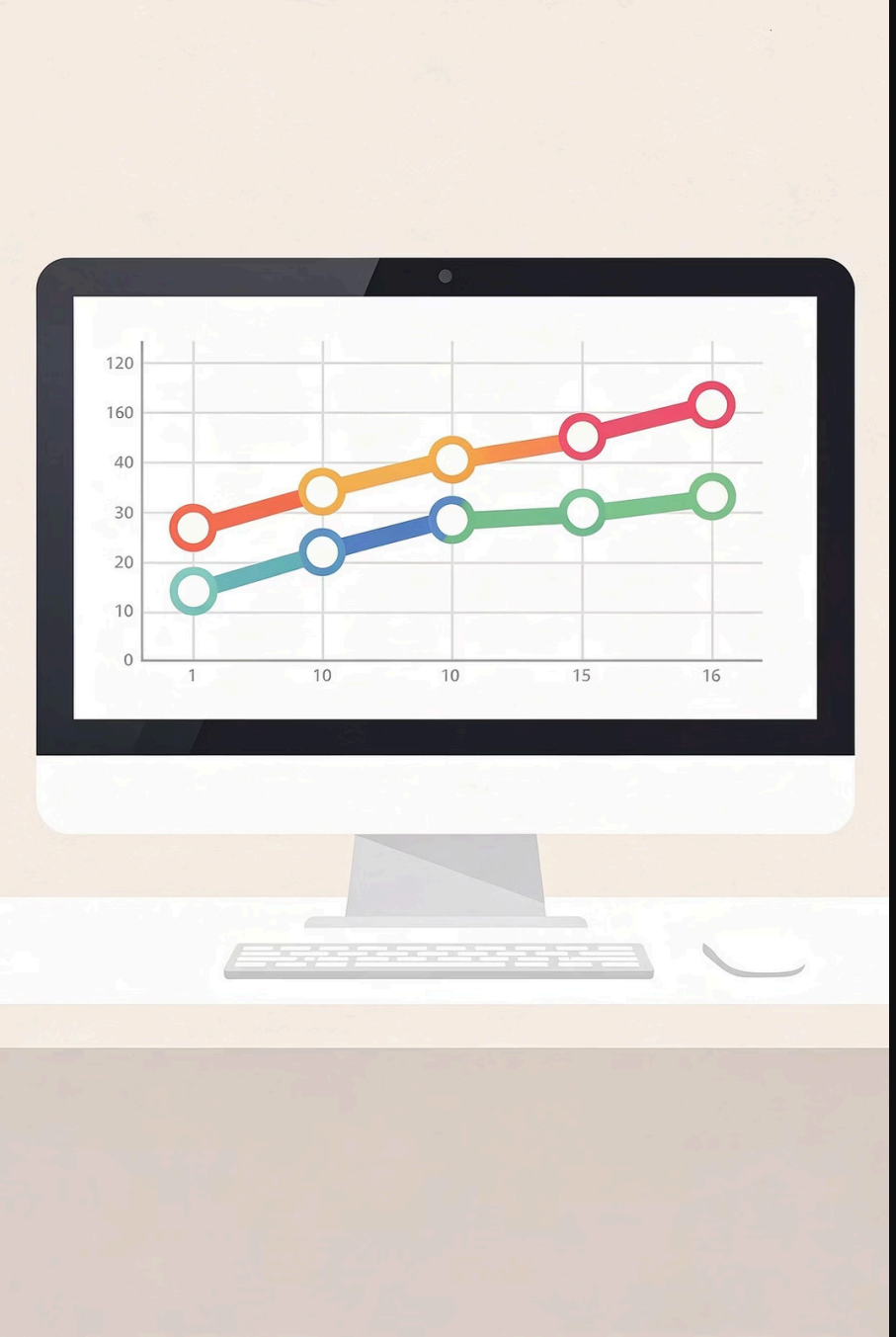
Evidence Correlation

Mengkorelasikan bukti digital dari browser dengan artefak sistem lainnya.

06

Case Documentation

Standar penulisan laporan forensik yang komprehensif dan dapat dipertanggungjawabkan.



Materi 1 — Modul 5

Timeline Analysis

Timeline Analysis adalah fondasi dari seluruh proses rekonstruksi aktivitas browser. Investigator harus mampu mengekstrak, mengurutkan, dan menginterpretasikan data temporal dari artefak browser secara akurat.

Sumber Data Timeline

- History file (SQLite/JSON)
- Cache metadata & timestamps
- Download records
- Cookie creation & expiry
- Bookmark timestamps

Teknik Analisis

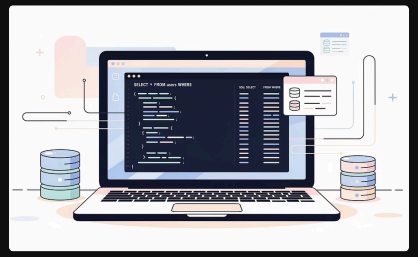
- Sorting berdasarkan epoch time
- Konversi timezone & normalisasi waktu
- Identifikasi gap dalam aktivitas
- Pendeteksian anomali pola kunjungan
- Visualisasi data temporal

EDY SUSANTO — FOUNDER CSIX SECURITY

Materi 2 — Modul 5

Correlation Analysis

Correlation Analysis menghubungkan berbagai artefak digital yang terpencar untuk menghasilkan gambaran aktivitas yang kohesif dan dapat diverifikasi. Teknik ini krusial dalam membantah atau mengonfirmasi hipotesis investigasi.

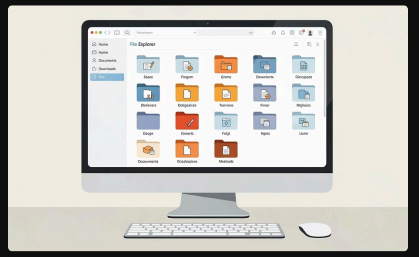


Korelasi Lintas Artefak

Menghubungkan data history, cache, cookie, dan log sistem untuk menemukan pola aktivitas yang tersembunyi.

Korelasi dengan Log Jaringan

Memvalidasi URL yang dikunjungi dengan log DNS, firewall, atau proxy server untuk konfirmasi independen.



Korelasi dengan Sistem File

Mengaitkan artefak browser dengan file yang diunduh, dokumen yang dibuka, dan metadata sistem operasi.

EDY SUSANTO — FOUNDER CSIX SECURITY

Materi 3 — Modul 5

Browser Sessions

Memahami struktur sesi browser memungkinkan investigator untuk merekonstruksi konteks lengkap dari sebuah aktivitas — bukan hanya URL yang dikunjungi, tetapi urutan, durasi, dan pola interaksi pengguna secara keseluruhan.

Session Storage vs. Persistent Data

Session storage bersifat sementara dan terhapus saat browser ditutup, sementara persistent cookies dan history tetap tersimpan. Memahami perbedaan ini kritis dalam analisis forensik.

Tab & Window Reconstruction

Browser modern menyimpan informasi tentang tab yang terbuka, urutan navigasi, dan riwayat "back/forward". Data ini memungkinkan rekonstruksi sesi browsing secara sangat detail.

Private/Incognito Sessions

Meskipun tidak menyimpan history, sesi incognito meninggalkan jejak di RAM, swap file, dan log sistem. Teknik memory forensics dapat digunakan untuk merecovery artefak ini.

Crash Recovery Files

File recovery sesi yang disimpan otomatis oleh browser saat crash mengandung informasi berharga tentang sesi aktif yang sedang berlangsung sebelum gangguan terjadi.

EDY SUSANTO — FOUNDER CSIX SECURITY

Materi 4 — Modul 5

Multiple Browser Investigation

Pengguna seringkali menggunakan lebih dari satu browser, baik untuk memisahkan aktivitas maupun untuk menghindari deteksi. Investigator harus mampu menganalisis artefak dari berbagai browser secara paralel dan mengintegrasikannya ke dalam satu timeline yang terpadu.

Google Chrome

SQLite database di folder `User Data\Default`. File utama: `History`, `Cookies`, `Cache`.

Mozilla Firefox

SQLite database di folder profil. File utama: `places.sqlite`, `cookies.sqlite`, `formhistory.sqlite`.

Microsoft Edge

Berbasis Chromium, struktur serupa Chrome. Lokasi profil berbeda di folder `Microsoft\Edge`.

Safari

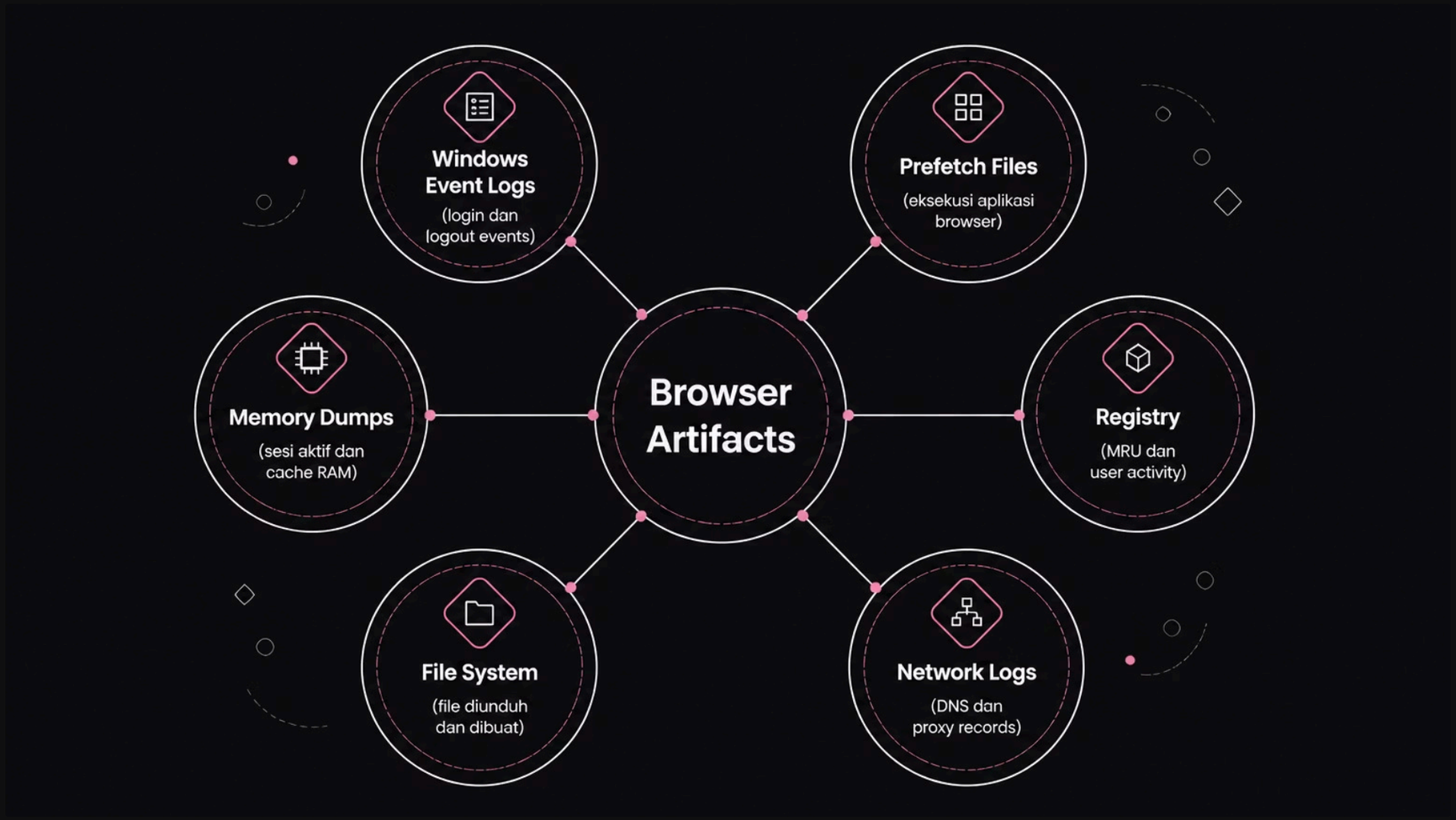
Menggunakan format plist dan database proprietary. Relevan untuk investigasi di lingkungan macOS dan iOS.

EDY SUSANTO — FOUNDER CSIX SECURITY

Materi 5 — Modul 5

Evidence Correlation

Evidence Correlation adalah proses lanjutan yang mengintegrasikan artefak browser dengan bukti digital dari sumber lain di dalam sistem. Tujuannya adalah membangun narasi investigasi yang kuat, konsisten, dan tahan terhadap sanggahan.



Setiap sumber bukti memberikan perspektif berbeda. Konvergensi dari beberapa sumber secara independen memperkuat kesimpulan forensik dan meningkatkan kredibilitas temuan di hadapan otoritas hukum.

EDY SUSANTO — FOUNDER CSIX SECURITY

Materi 6 — Modul 5

Case Documentation

Dokumentasi yang baik adalah pembeda antara investigasi yang dapat digunakan secara hukum dan yang tidak. Laporan forensik harus memenuhi standar admissibilitas bukti digital dan dapat direproduksi oleh pihak ketiga yang independen.

Komponen Laporan Forensik

- Executive summary untuk pembaca non-teknis
- Chain of custody yang lengkap dan terdokumentasi
- Metodologi dan tools yang digunakan
- Temuan teknis dengan screenshot & hash value
- Timeline kronologis aktivitas terrekonstruksi
- Kesimpulan dan rekomendasi tindak lanjut

Standar & Best Practice

- Referensi standar SWGDE & ACPO
- Preservasi integritas bukti dengan hash MD5/SHA-256
- Dokumentasi setiap langkah investigasi secara real-time
- Penggunaan tools yang tervalidasi dan diakui industri
- Peer review laporan sebelum disubmit secara resmi

EDY SUSANTO — FOUNDER CSIX SECURITY

Praktik & Lab — Modul 5

Investigasi Studi Kasus & Lab Timeline

Peserta akan menerapkan seluruh materi modul melalui dua sesi praktis: studi kasus investigasi nyata dan lab menyusun timeline dari mesin uji yang telah disiapkan.

1. **Persiapan**
   Menerima image forensik mesin uji. Verifikasi integritas dengan hash. Setup tools investigasi.

2. **Ekstraksi Artefak**
   Ekstrak history, cache, cookies, dan session data dari semua browser yang teridentifikasi di mesin uji.

3. **Rekonstruksi Timeline**
   Susun semua artefak ke dalam timeline terpadu. Korelasikan dengan log sistem dan artefak lainnya.

4. **Dokumentasi**
   Tulis laporan forensik lengkap sesuai standar. Presentasikan temuan kepada kelompok untuk peer review.

EDY SUSANTO — FOUNDER CSIX SECURITY

Outcome — Modul 5

Kompetensi yang Dicapai

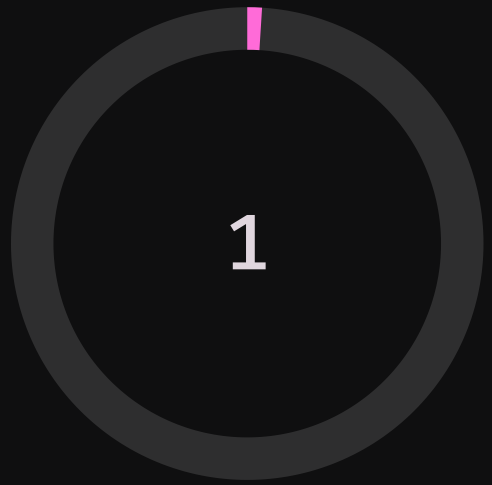
Setelah menyelesaikan Modul 5, peserta telah memiliki kemampuan menyeluruh untuk melakukan investigasi forensik browser secara mandiri dan profesional — dari pengumpulan artefak hingga penyusunan laporan siap saji.

Topik Materi

Enam topik utama yang mencakup seluruh aspek forensik browser secara komprehensif.

Browser Dianalisis

Chrome, Firefox, Edge, dan Safari dipelajari dengan pendekatan forensik masing-masing.



Lab Praktis

Satu sesi lab intensif dengan mesin uji nyata untuk membangun pengalaman investigasi langsung.

Peserta yang telah menyelesaikan modul ini siap melanjutkan ke Modul 6: Advanced Artifact Analysis & Reporting.