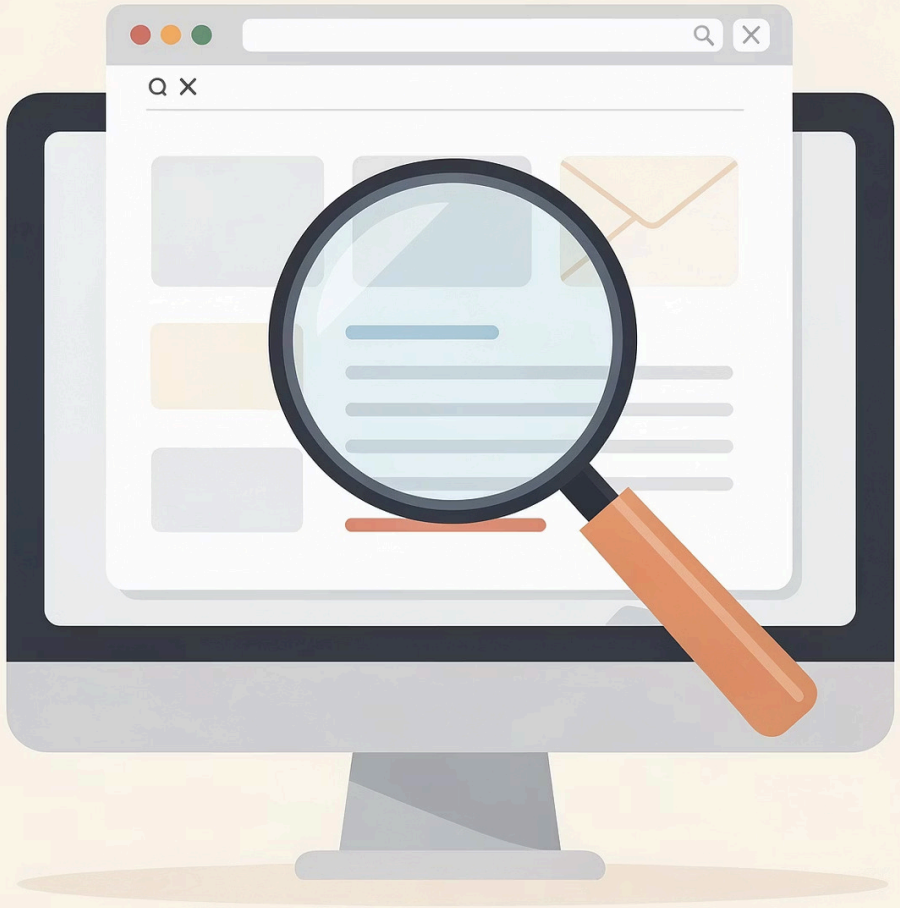
# Modul 4: Cache, Cookies & Download Investigation

Memahami informasi yang tersimpan selama aktivitas browsing — dari jejak cache hingga rekonstruksi kronologi digital.

EDY SUSANTO — FOUNDER CSIX SECURITY



# Mengapa Kita Memeriksa Jejak Browser?

## Jendela Aktivitas

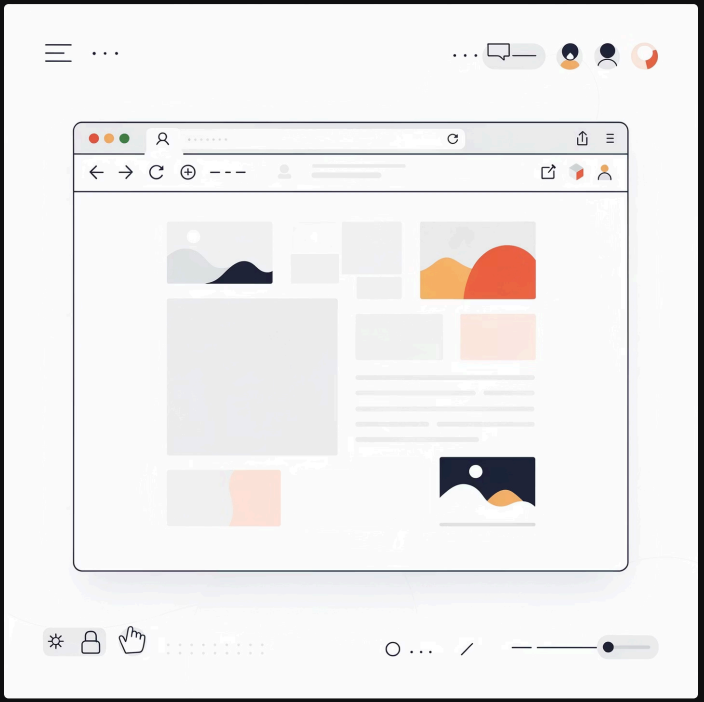
Browser adalah rekaman utama perilaku internet pengguna — setiap klik meninggalkan artefak nyata.

## Jejak Tak Kasat Mata

Data tersimpan di memori dan penyimpanan lokal, bahkan setelah sesi ditutup.

## Nilai Forensik

Menghubungkan subjek dengan aksi spesifik secara terukur dan dapat dibuktikan.



BROWSER CACHE

# Memori Instan Browser

Cache menyimpan elemen grafis, skrip, dan konten halaman agar loading lebih cepat saat kunjungan berikutnya.

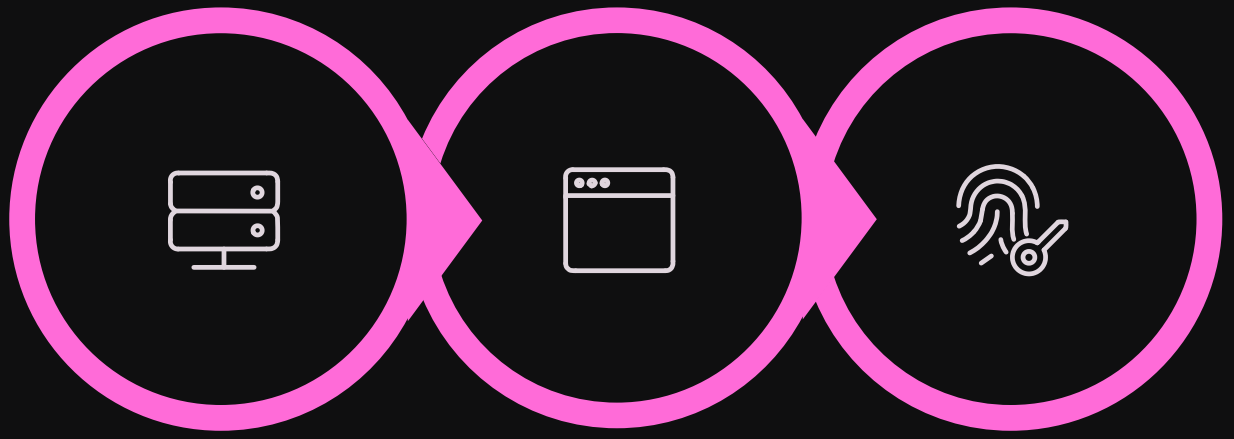
## Nilai Investigatif

Merekonstruksi tampilan visual yang pernah dilihat pengguna secara akurat.

## Tantangan

Data bersifat sementara — dapat dihapus, ditimpa, atau dikosongkan oleh pengguna.

# HTTP Cache: Di Balik Layar



Server Response

Browser Storage

Forensic Analysis

HTTP Cache mengungkap metadata kunjungan tersembunyi — membantu investigator memastikan apakah sebuah file benar-benar diunduh atau sekadar dimuat sementara oleh browser.

# Cookies: Identitas Digital Pengguna

## Kredensial & Preferensi

Menyimpan data login, preferensi tampilan, dan status autentikasi pengguna di situs target.

## Session Cookies

Melacak sesi aktif pengguna — kunci untuk membuktikan kapan dan berapa lama sesi berlangsung.

## Pola Personalisasi

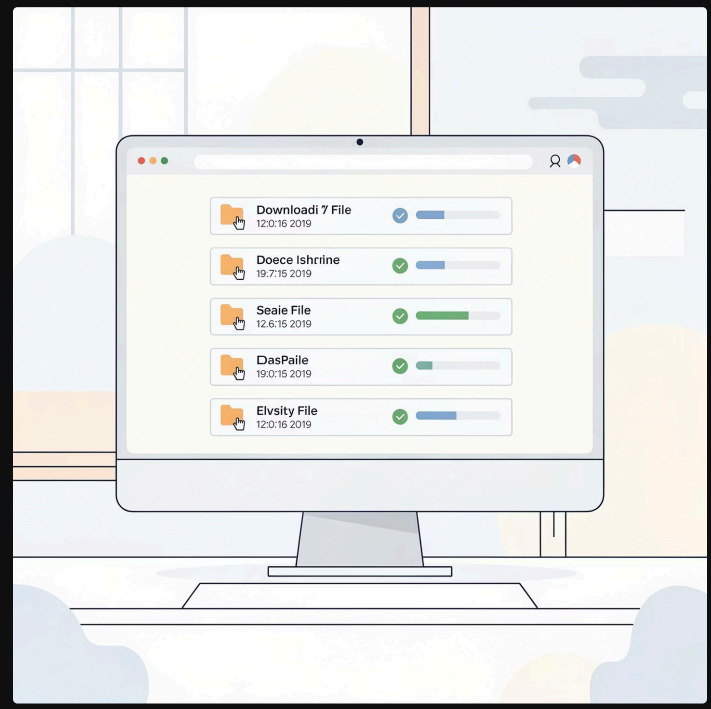
Mengungkap perilaku spesifik pengguna: situs yang sering dikunjungi, preferensi, dan jejak identitas digital.

DOWNLOAD & RECENT FILES

# Jejak Unduhan & File Terkini

Artefak unduhan mencatat riwayat lengkap file yang berpindah ke perangkat — waktu, sumber URL, dan lokasi penyimpanan.

- **Download History**: Log browser yang merekam setiap file yang diunduh beserta timestamp-nya.
- **Recent Files Windows**: Sering tumpang tindih dengan jejak unduhan, memperkuat bukti.
- **Indikasi Eksekusi**: Menemukan bukti file berbahaya atau dokumen sensitif yang pernah dibuka.



# Temporary Files: Gudang Bukti Tersembunyi

## Lokasi Khusus

OS dan browser menyimpan data sementara di direktori %TEMP% dan cache tersembunyi.

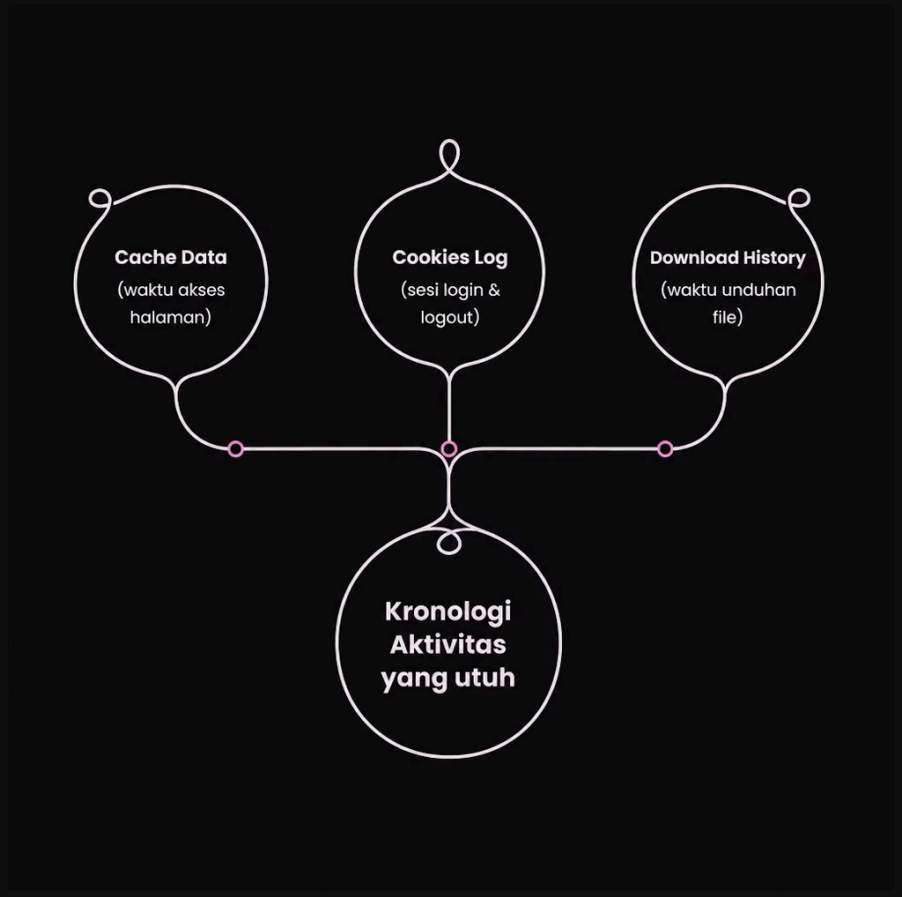
## Fragmen Terhapus

Sering berisi sisa file yang telah dihapus dari lokasi aslinya — masih dapat dipulihkan.

## Anti-Forensik

Menjadi lokasi persembunyian data ketika pengguna berusaha menutupi jejak aktivitasnya.

# Timeline Reconstruction: Menyusun Teka-Teki




Rekonstruksi timeline menggabungkan seluruh artefak menjadi satu narasi kronologis yang koheren.

### 1 Kumpulkan Semua Sumber

Cache, cookies, download log, dan recent files dikumpulkan secara bersamaan.

### 2 Korelasi Timestamp

Menyelaraskan waktu akses lintas artefak untuk mengisi celah dalam kronologi.

### 3 Kronologi Tak Terbantahkan

Hasil akhir: urutan aktivitas yang dapat dipertanggungjawabkan secara forensik di hadapan hukum.

# Praktik Lapangan: Analisis Dataset

1

## Ekstraksi Artefak

Mengambil cache, cookies, dan log unduhan dari dataset latihan yang telah disiapkan.

2

## Identifikasi Pola

Menganalisis riwayat unduhan untuk menemukan anomali dan aktivitas mencurigakan.

3

## Validasi Bukti

Memastikan integritas dan autentisitas bukti digital agar layak digunakan dalam investigasi.

# Kesimpulan: Menjadi Investigator Andal

> Artefak digital adalah saksi bisu yang tidak pernah berbohong — tugas investigator adalah membuatnya berbicara.

### Artefak Sebagai Bukti

Cache, cookies, dan log unduhan adalah bukti nyata yang menghubungkan subjek dengan aksi spesifik.

### Ketelitian adalah Kunci

Kemampuan menghubungkan titik data dari berbagai sumber menentukan keberhasilan pengungkapan kasus.

### Terapkan Sekarang

Metodologi forensik yang telah dipelajari siap diterapkan dalam investigasi dunia nyata Anda.

EDY SUSANTO — FOUNDER CSIX SECURITY