

Артефакти браузерів: зберігання та вилучення даних для цифрової криміналістики

Теоретична частина

1) Основні типи артефактів браузерів

- Історія відвідувань: URL, заголовок, час останнього відвідування, лічильники візитів.
- Завантаження: шлях до файлу, джерело, статус, час.
- Cookies: домен, ім'я, значення, атрибути (Secure, HttpOnly, SameSite), час життя.
- Облікові дані: зашифровані логіни/паролі, підказки автозаповнення, платіжні дані.
- Сховища: LocalStorage, SessionStorage, IndexedDB, Service Workers, Cache Storage.
- Стан сесій: відкриті вкладки/вікна, відновлення після падіння.
- Допоміжні: Favicons/Top Sites, історія пошуку, розширення, телеметрія.

2) Типові формати та сховища

- SQLite-бази: History, Cookies, Downloads, Login Data, Favicons, Top Sites.
- JSON/JSONL та LevelDB/IndexedDB каталоги для веб-сховищ.
- LZ4/стиснені формати у Firefox (sessions, favicons).
- Шифрування секретів: DPAPI (Windows), Keychain (macOS), Secret Service/KWallet (Linux).

3) Шляхи зберігання (типово)

- Windows

- Chromium-сімейство: C:\Users<user>\AppData\Local<Browser>\User Data\Default\
- Firefox:
C:\Users<user>\AppData\Roaming\Mozilla\Firefox\Profiles<profile>\.default\
- macOS
 - Chromium: ~/Library/Application Support/<Browser>/Default/
 - Firefox: ~/Library/Application Support/Firefox/Profiles/<profile>\.default/
- Linux
 - Chromium: ~/.config/<browser>/Default/
 - Firefox: ~/.mozilla/firefox/<profile>\.default/

Примітка: у Chromium-браузерів профілі можуть мати інші назви, напр. "Profile 1".

4) Криміналістично коректне вилучення

- Працювати з копіями, а не з живими файлами профілю.
- Перед копіюванням завершити процеси браузера.
- Фіксувати контрольні суми (hash) до/після копіювання.
- Зберігати часові метадані файлів (MACB) та вести журнал дій.

Практична частина

Варіант браузерів

Обрати 3 різні браузери. Рекомендації: Google Chrome/Chromium, Mozilla Firefox, Microsoft Edge, Opera, Brave, Safari (macOS).

Крок 1. Підготовка середовища

- Створити робочу директорію кейсу: Case_<Прізвище>_BrowserArtifacts.
- Зробити «холодну» копію профілів кожного браузера у підкаталоги /Evidence/<Browser>.
- Зафіксувати контрольні суми: SHA-256 для ключових файлів БД.

Крок 2. Виявлення ключових файлів

- Chromium-подібні (в каталозі профілю):
 - History (SQLite) — історія відвідувань та пошуку
 - Cookies (SQLite або контейнер із зашифрованими значеннями)
 - Downloads (SQLite, інколи таблиця в History)
 - Login Data (SQLite, логіни/паролі — значення зашифровані)
 - Top Sites, Favicons (SQLite)
 - Preferences, Secure Preferences (JSON)
 - Local Storage, Session Storage, IndexedDB, Service Worker, Cache — у відповідних підкаталогах
- Firefox:
 - places.sqlite — історія та закладки
 - cookies.sqlite — cookies
 - favicons.sqlite
 - logins.json + key4.db — логіни/паролі (шифровано)
 - formhistory.sqlite — автозаповнення
 - sessionstore-backups, recovery.jsonlz4 — сесії
 - storage/default, storage/permanent — LocalStorage/IndexedDB

Крок 3. Аналіз через SQLite Viewer

- Відкрити потрібну базу у SQLite Viewer / DB Browser for SQLite.
- Перейти на вкладку "Browse Data" і вибрати потрібну таблицю:
 - Chromium: urls, visits, downloads, cookies, logins, top_sites, favicons тощо.
 - Firefox: moz_places, moz_historyvisits, moz_cookies, logins.json не SQLite — переглянути текстом; formhistory, favicons тощо.
- Відфільтрувати дані через вбудовані поля пошуку/фільтрів (наприклад, за доменом або часовим інтервалом).
- Переглянути схему на вкладці "Database Structure" для розуміння полів і зв'язків.

- За потреби використати "Export" → CSV/JSON для обраної таблиці або результату фільтра.

Примітка: запити SQL писати не потрібно. Достатньо користуватись GUI-можливостями переглядача.

Крок 4. Cookies та захищені секрети

- Значення cookies у Chromium можуть бути зашифровані системним сховищем (DPAPI/Keychain/libsecret). Зафіксувати факт шифрування у звіті та чи можливо відобразити значення у вашому оточенні.
- У Firefox логіни зберігаються в logins.json і шифруються ключем із key4.db; без доступу до профілю/майстер-пароля розшифрування обмежене.

Крок 5. Сесії, локальні сховища, IndexedDB

- Firefox sessionstore *.jsonlz4 — декомпресувати та переглянути відкриті вкладки.
- Chromium сесії/вкладки — файли типу Current Session/Current Tabs.
- LocalStorage/SessionStorage — per-origin каталоги; формат LevelDB або SQLite залежно від браузера та версії.
- IndexedDB — каталоги origin-specific; зафіксувати приклад ключів/значень чи структуру обраного сховища.

Крок 6. Порівняння браузерів

- Заповнити таблицю:
 - Місця зберігання профілю
 - Основні БД і їх таблиці
 - Формати часу
 - Шифрування секретів
 - Особливості сесій і сховищ
 - Складність вилучення