

Дослідження вебоглядача Tor Browser

Іван Старенький

Одеський НДІСЕ, м. Одеса, Україна, ORCID: <https://orcid.org/0009-0004-2271-8512>,
e-mail: ivan_starenkii@ukr.net

Розглянуто рекомендаційні дії щодо дослідження вебоглядача Tor Browser під час виконання експертиз за спеціальністю «Дослідження комп'ютерної техніки та програмних продуктів».

Ключові слова: вебоглядач; браузер; посилання; onion; носій інформації; база даних; таблиця; стовпчик.

Investigation of the Tor Browser

Ivan Starenkiy

The author considers the recommendation actions for the investigation of the Tor Browser during examinations in the specialty "Research of computer hardware and software products".

Keywords: web-browser; browser; link; onion; information carrier; databases; table; column.

Одним із аспектів проведення судових експертиз зі спеціальності «Дослідження комп'ютерної техніки та програмних продуктів» є дослідження вебоглядачів, що забезпечують користувачеві доступ до вебресурсів в інтернеті.

Під час дослідження вебоглядачів із конфігураційних файлів певного браузера можна одержати таке: інформацію щодо закладок; інформацію щодо WEB Cookies; історію завантаження з інтернету; текстову інформацію щодо автозаповнення на сайтах; історію відвідування вебресурсів в інтернеті; інформацію щодо збережених авторизаційних даних до вебресурсів інтернету; історію пошуку за допомогою пошукових систем. Більшість наведених свідчень можна отримати за допомогою спеціалізованого криміналістичного програмного забезпечення (далі — СКПЗ), наприклад, Autopsy-Digital Forensics [1] (далі — Autopsy) (рис. 1).



Рис. 1. Приклад зібраної інформації з конфігураційних файлів вебоглядачів за допомогою СКПЗ Autopsy

Але бувають випадки, коли СКПЗ під час сканування побітової копії носія інформації «навмисно» пропускає сканування теки з конфігураційними файлами вебоглядача із причини, що тека вебоглядача розміщена не за стандартним шляхом свого розміщення. Саме до таких вебоглядачів належить Tor Browser [2].

Tor Browser — це вебоглядач, який організовано на базі браузера Mozilla Firefox [3] і призначено для забезпечення анонімного та безпечного відвідування інтернету. Основна його функція полягає в маршрутизації трафіку через різні вузли мережі Tor (The Onion Router), що дає змогу приховати вебактивність користувача від прослуховування та відстеження.

На відміну від інших браузерів, Tor Browser дає користувачеві доступ до onion-сайтів, які є частиною так званого «тіньового інтернету», або DarkNet (далі — даркнет).

Onion-сайти — це вебресурси, доступні лише в мережі Tor і мають доменне ім'я, яке закінчується на .onion. Ці сайти створюються й підтримуються в даркнеті, вони мають такі особливості порівняно з іншими вебресурсами: анонімність, приватність, безпеку, можливість розміщення будь-якої інформації.

Із позицій порушення законодавчих норм України, такі onion-сайти можуть бути використані для розміщення оголошень із продажу наркотичних речовин, або для розміщення в даркнеті файлів, які містять зображення оголених людей, зокрема дітей, тощо. Такі дії підпадають під ознаки кримінальних правопорушень, передбачених різними статтями Кримінального кодексу України [4].

Отже, дослідження конфігураційних файлів вебоглядача Tor Browser у разі виявлення його в пам'яті накопичувача інформації є вкрай важливим елементом у дослідницькій частині експертизи.



Як було зазначено, вебоглядач Tor Browser організовано на базі Mozilla Firefox, тому в разі виявлення кореневої теки даного браузера, необхідно дослідити файл бази даних SQL «places.sqlite», який розміщують за шляхом Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/.

Інтересом для дослідження в базі даних places.sqlite є таблиці moz_bookmarks, moz_origins та moz_places, приклади інформаційного вмісту яких наведено на рис. 2—4.

Рис. 2. Приклад вмісту таблиці moz_bookmarks

Рис. 3. Приклад вмісту таблиці moz_origins

Рис. 4. Приклад вмісту таблиці moz_places

У таблиці moz_bookmarks міститься інформація щодо збережених користувачем закладок у вебоглядачеві Tor Browser.

Таблиця moz_origins відповідає за зберігання інформації про початкові (оригінальні) джерела (звідки завантажуються вебресурси) для різних елементів історії та закладок у вебоглядачеві. Ця таблиця допомагає Вебоглядачеві визначати, із яких джерел завантажено вміст, вона грає роль у відстеженні різних джерел вебресурсів.

Таблиця moz_places відповідає за зберігання інформації про відвідані користувачем вебресурси. Ця таблиця грає ключову роль у веденні історії перегляду та в управлінні закладками.

У таблиці moz_places бази даних places.sqlite стовпчик frecency об'єднує терміни frequency (частота) і recency (остання активність). Це поле використовують для визначення популярності та актуальності відвідуваних сторінок.

Frecency є комбінацією двох чинників:

- частота (Frequency) — кількість разів відвідування користувачем конкретного вебресурсу. Чим частіше сторінка відвідується, тим вище її частота;
- остання активність (Recency) — тривалість часу з моменту останнього відвідування вебсторінки. Чим ближче до поточного моменту час відвідування, тим вищий рівень останньої активності.

Сума цих двох чинників визначає frecency і використовується для сортування та визначення порядку відображення сторінок в історії вебоглядача або під час автозаповнення адресної стрічки. Вебресурси з вищим frecency тенденційно будуть вище в списку, що полегшує користувачеві швидший доступ до часто відвідуваних та недавно відвіданих ресурсів.

Із позицій проведення експертного дослідження, користуючись стовпчиком Frecency таблиці moz_places, можна дійти висновку щодо частоти відвідування певного вебресурсу за допомогою вебоглядача Tor Browser, а значення стовпчика URL цієї ж таблиці дає змогу встановити перелік вебресурсів, що відвідувалися користувачем, та які не були включені до звіту СКПЗ, сформованого за результатами сканування побітової копії носія інформації.

Перелік джерел посилання

1. Autopsy-Digital Forensics. URL: <https://www.autopsy.com/> (дата звернення: 01.04.2024).
2. Tor Browser. URL: <https://www.torproject.org/ru/download/> (дата звернення: 01.04.2024).
3. Mozilla Firefox. Вікіпедія: вільна енциклопедія. URL: https://ru.wikipedia.org/wiki/Mozilla_Firefox (дата звернення: 01.04.2024).
4. Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#> (дата звернення 01.04.2024).