3. Ухвала Святошинського районного суду м. Києва від 13.11.2017 р. у справі № 759/2300/16-к (кримінальне провадження № 1-кп/759/35/17). URL: http://www.reyestr.court.gov.ua/Review/70172118.

4. Ухвала Сторожинецького районного суду Чернівецької області від 16.01.2017 р. у справі № 723/873/15-к (кримінальне провадження № 1-кп/723/216/17). URL: http://www.reyestr.court.gov.ua/Review/64054789.

5. Ухвала Чернівецького районного суду Вінницької області від 27.04.2018 р. у справі № 150/202/16-к (кримінальне провадження № 1-кп/150/1/18). URL: http://www.reyestr.court.gov.ua/Review/73661906.

6. Ухвала Чигиринського районного суду від 13.11.2018 р. у справі № 708/108/18 (кримінальне провадження № 1-кп/708/29/18). URL: http://www.reyestr.court.gov.ua/ Review/77802723.

7. Ухвала Хорольського районного суду Полтавської області від 13.04.2018 р. у справі № 548/657/18 (кримінальне провадження № 1-кс/548/204/18). URL: http://www.reyestr.court.gov.ua/Review/73439394.

8. Ухвала Царичанського районного суду Дніпропетровської області від 22.12.2016 р. у справі № 196/177/16-к (кримінальне провадження № 1-кп/196/65/2016). URL: http://www.reyestr.court.gov.ua/Review/63575087.

9. Ухвала Царичанського районного суду Дніпропетровської області від 10.08.2018 р. у справі № 196/177/16-к (кримінальне провадження № 1-кп/196/2/2018). URL: http://www.reyestr.court.gov.ua/Review/76061490.

Коліса Я.Ю.
головний судовий експерт
відділу комп'ютерно-технічних та телекомунікаційних досліджень,
Полтавський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

ЧАСОВА МІТКА WEBKIT / CHROME

Одним із завдань судової комп'ютерно-технічної експертизи є дослідження веб-браузерів на предмет пошуку історії.

Веб-браузер (англ. web browser, browser) – програмне забезпечення (далі – ПЗ) для комп'ютера або іншого електронного пристрою, як правило, під'єднаного до Інтернету, що дає можливість користувачеві взаємодіяти з текстом, малюнками або іншою інформацією на гіпертекстовій веб-сторінці. Популярними серед них є: Internet Explorer (операційна система Windows), Mozilla Firefox (вільне ПЗ), Safari (Mac OS або Windows), Opera (безкоштовно, починаючи з версії 8.50), Google Chrome (вільне ПЗ) та інші [1, с. 271–272].

Саме про історію веб-браузера Google Chrome далі піде мова. Його веб-історію (як і інших веб-браузерів) частенько ототожнюють зі списком раніше відвіданих веб-сайтів. Сам список зберігається в спеціальному файлі формату sqlite3, який є базою даних з іменем «history». Одним із способів переглянути його вміст є комп'ютерна програма «DB Browser for SQLite».

База даних «history» складається з 12 пов'язаних між собою таблиць (рис. 1).

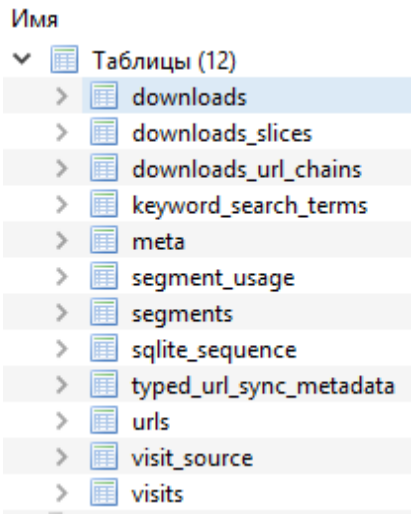

Рис. 1. Структура бази даних «history»

Як видно із рис. 1, в таблицях зберігається інформація не тільки про url відвіданих веб-сайтів, а і про завантаження та ключові слова пошукових запитів. І все це супроводжується прив'язкою до часової мітки (рис. 2).

Table: urls

	id	url	title	visit_count	typed_count	last_visit_time
	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр
1	588	https://www.drive-image.com/ru/		1	0	13193738156423689

Рис. 2. Демонстрація часової мітки в таблиці «urls»

На рис. 2 видно, що в стовбці «last_visit_time» міститься 17-значне число. За цим числом прихована дата і час події, яку треба лише перевести в зрозумілий людині формат.

Наведений приклад на рисунку 2 і є часовою міткою (англ. timestamp), тобто послідовність символів або закодованої інформації, яка показує, коли відбувалася певна подія.

Однією з найпоширеніших часових міток є Unix timestamp. Моментом початку відліку вважається північ (по UTC) з 31 грудня 1969 року на 1 січня 1970 року. Час з цього моменту називається «епохою UNIX» (англ. Unix Epoch) і рахується в секундах (10-значне число) [2; 3].

Також час може зберігатися не тільки в секундах, а й в мілісекундах (13-значне число, тобто помножене на 10^{-3}), мікросекундах (16-значне число) і наносекундах.

І саме в такому вигляді, відносно «епохи UNIX» зберігається час в базі даних веб-браузера Mozilla Firefox з іменем «places.sqlite» (рис. 3).

На рисунку 3 ми бачимо 16-значне число часової мітки в мікросекундах. Як перевести його в мережі Інтернет інформації достатньо. В тому числі його

можна скопіювати і помістити в онлайн конвертор [2]. Або ж можливо скористатися керівництвом по функціям SQLite [4].

Table: moz_historyvisits

	id	from_visit	place_id	visit_date	visit_type
	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр
1	1	0	5	1549964219704000	1

Рис. 3. Демонстрація часової мітки в таблиці «moz_historyvisits» веб-браузера Mozilla Firefox

Це є доцільним при необхідності автоматизувати процес переведення декількох сотень і більше міток. Скористаємся для цього наступним SQLite кодом:

«SELECT
StrfTime('%d.%m.%Y %H:%M:%S', moz_historyvisits."visit_date"/1000000, 'unixepoch') AS Time
FROM moz_historyvisits»,

де «SELECT … FROM moz_historyvisits» – витягує записи із таблиці «moz_historyvisits» [4];

«StrfTime» – функція, яка вираховує дату та поміщає її замість початкової;

«'%d.%m.%Y %H:%M:%S'» – задає формат часу [4];

«moz_historyvisits."visit_date"/1000000» – приведення числа в стовбці visit_date до секунд [5];

«'unixepoch'» – переведення секунд відносно початку епохи UNIX [4];

AS Time – заголовок стовбця зміниться із «visit_date» на «Time».

Тепер повернемося до наведеного прикладу на рисунку 2, файлу «history» і 17-значних чисел в ньому. Якщо виконати аналогічно команди, які застосовувалися для бази даних Firefox результат буде дивовижний (рис. 4).

SQL 1

```
1  SELECT StrfTime('%d.%m.%Y %H:%M:%S', urls."last_visit_time"/1000000, 'unixepoch') AS Time
2  FROM urls
```

	Time
1	04.02.2388 07:15:56

Рис. 4. Демонстрація результату виконання команд для часової мітки Chrome

Вся проблема полягає в тому, що число 17-значне. Тобто воно не пов’язане з «епохою UNIX», а є часовою міткою WebKit [6].

WebKit – це двигун веб-браузера, який використовується Safari, Mail, App Store і багатьма іншими додатками на MacOS, iOS і Linux [7]. Основним

завданням двигуна браузера – перетворити HTML-документи та інші ресурси веб-сторінки в інтерактивне візуальне уявлення на пристрої користувача.

17-значний формат часової мітки використовується у веб-браузерах, таких як Apple Safari (WebKit), Google Chrome, Opera (Chromium / Blink) [6]. Де Chromium – це проект браузера з відкритим вихідним кодом, метою якого є створення більш безпечного, швидкого і стабільного способу для всіх користувачів працювати в Інтернеті [8].

Саме на основі браузера Chromium був створений такий популярний Google Chrome. При цьому в Chromium був використаний веб-двигун «Blink» розроблений на основі WebKit (браузер Safari).

Також на основі веб-двигуна Blink та графічної оболонки Chromium були розроблені такі веб-браузери, як: Opera, Vivaldi, Uran, Brave, Яндекс.Браузер. Зрозуміло, що вони перейняли і основну тенденцію часової мітки. Тому її і можна вважати міткою WebKit.

Отже часова мітка WebKit/Chrome – 64-бітове значення для мікросекунд з 1 січня 1601 00:00 UTC [6]. Тобто 17-значне число показує кількість мікросекунд, які пройшли з 1601 року. Чому саме ця дата? Серед пояснень мабуть найбільш логічним є саме 400-річний цикл григоріанського календаря і 1601 – перший рік циклу, який закінчився в 2000 році [9]. В будь-якому разі саме від цієї дати потрібно починати відлік. Тому SQLite команди для переведення часу будуть наступні:

«SELECT

StrfTime('%d.%m.%Y %H:%M:%S', urls."last_visit_time"/1000000 + (StrfTime('%s', '1601-01-01')), 'unixepoch') AS Time

FROM urls»,

де «urls."last_visit_time"/1000000» – переводить число до значення в секундах;

«(StrfTime('%s', '1601-01-01'))» – визначає кількість секунд з 01.01.1970 до 01.01.1601. Дане число буде зі знаком мінус (-).

Далі відбувається сумування двох чисел, але так як друге число зі знаком (-), то в результаті віднімання отримуємо кількість секунд від початку «епохи UNIX» до настання шуканої події (рис. 5). Після чого секунди переводяться у формат зрозумілий людині.

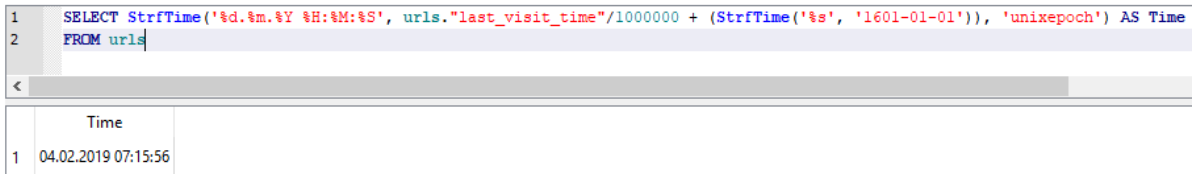

Рис. 5. Демонстрація перетворення 17-значного числа у форму зрозумілу людині

Таким чином в даній роботі наведений приклад та команди для перетворення часових міток WebKit/Chrome у зрозумілий формат.

Звісно може виникнути сумніви, щодо необхідності використання такого прийому дослідження. Адже на службі експерта існують спеціалізовані на цьому програми. Але в більшості випадків вони або вміють досліджувати історію найпоширеніших веб-браузерів, а саме: Internet Explorer, Mozilla Firefox та Google Chrome, або надавати лише список відвіданих веб-сайтів. Тобто у випадку необхідності вивести список завантажень або іншу інформацію прив'язану до часу, в експерта можуть виникнути трудності. Саме для цього і потрібна процедура з переведення часової мітки WebKit/Chrome.

Список використаних джерел:

1. Тлумачний словник з інформатики / Г. Г. Півняк, Б. С. Бусигін, М. М. Дівізінюк та ін. – Д., Нац. гірнич. ун-т, 2010. – 600 с.
2. Unix Timestamp конвертер. Epoch конвертер. Текущее unix время. – URL: https://www.cy-pr.com/tools/time/ (дата звернення: 12.02.2019).
3. Что такое временная метка Unix и зачем ее использовать? – URL: http://qaru.site/questions/61044/what-is-a-unix-timestamp-and-why-use-it (дата звернення: 12.02.2019).
4. SQLite Query Language: Date And Time Functions. – URL: https://www.sqlite.org/lang_datefunc.html (дата звернення: 12.02.2019).
2. Преобразование полей datetime в файле истории Chrome (sqlite) в удобочитаемый формат. – URL: https://stackoverrun.com/ru/q/438365 (дата звернення: 12.02.2019).
3. WebKit/Chrome Timestamp Converter. – URL: https://www.epochconverter.com/webkit (дата звернення: 12.02.2019).
4. WebKit. – URL: https://webkit.org/ (дата звернення: 12.02.2019).
5. The Chromium Projects. – URL: https://www.chromium.org/ (дата звернення: 12.02.2019).
6. Каков формат временных меток Chrome? – URL: http://qaru.site/questions/292211/what-is-the-format-of-chromes-timestamps (дата звернення: 12.02.2019).

Костюковська О.В.
студентка,
Київський національний університет
імені Тараса Шевченка

ПРОБЛЕМНІ АСПЕКТИ СУЧАСНОЇ ПРАКТИКИ ПРИТЯГНЕННЯ АДВОКАТА ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ТА ЗДІЙСНЕННЯ ОСОБЛИВОГО ПОРЯДКУ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЩОДО НЬОГО

Конституція України в статті 24 передбачає, що громадяни мають рівні конституційні права і свободи та є рівними перед законом. Так, не може бути привілеїв чи обмежень за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками [1].