СУДОВА КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА

М. В. Полякова, старший науковий співробітник Одеського НДІСЕ,
В. С. Рукавішников, старший науковий співробітник Одеського НДІСЕ,
О. М. Шабля, завідувач лабораторії Одеського НДІСЕ, кандидат технічних наук, старший науковий співробітник

ОСОБЛИВОСТІ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ ФАЙЛОВИХ СТРУКТУР, ТИПОВИХ ДЛЯ ФУНКЦІЮВАННЯ ОКРЕМИХ ІНТЕРНЕТ-БРАУЗЕРІВ

Розглянуто особливості дослідження файлових структур, які створюються на накопичувачі на жорстких магнітних дисках персонального комп'ютера під час використання користувачем певних Інтернет-браузерів для доступу до сайтів всесвітньої мережі Інтернет.

Рассмотрены особенности исследования файловых структур, которые создаются на накопителе на жестких магнитных дисках персонального компьютера во время применения пользователем определенных Интернет-браузеров для доступа к сайтам всемирной сети Интернет.

Експертна практика засвідчує постійне збільшення кількості експертних завдань щодо пошуку на комп'ютерних носіях інформації, яка стосується роботи користувача персонального комп'ютера (ПК) у глобальній мережі Інтернет, тобто звернення його на конкретні сайти, хронології чи історії звернень тощо. Це зумовлено збільшенням кримінальних справ, пов'язаних з противоправним поширенням у глобальній мережі певної інформації, у тому числі кримінального характеру (щодо торгівлі людьми, розповсюдження порнографічних зображень тощо).

Завдання пошуку на комп'ютерному носії даних, які стосуються відвідування користувачем певних сайтів, є важливим і складним, а шляхи його вирішення значною мірою залежать від установлених на досліджуваному ПК типу операційної системи (ОС) та Інтернет-браузера. З оглядом на наявну експертну практику можна констатувати, що найчастіше підлягають дослідженню ПК, на яких встановлено ОС сімейств MS Windows і Linux з відповідними браузерами (Internet Explorer, Opera, Firefox, Safari та ін.), кожний з яких має свою специфіку. Це додатково ускладнює завдання пошуку інформації, яка передавалася, у тому числі тієї, що була видалена або знищена.

Як правило, експертне завдання в постанові про призначення експертизи комп'ютерної техніки та програмного забезпечення формулюється таким чином: «Чи відвідував користувач персонального комп'ютера Інтернет-сайти: (перелік назв)?» Для експерта це завдання трансформується в пошук відповідних файлових структур як відбитків дій користувача в Мережі.

Для вирішення цього експертного завдання перш за все необхідно визначитися з наявною можливістю такої роботи, тобто чи оснащений наданий на дослідження ПК (стаціонарний чи портативний) відповідним апаратним і програмним забезпеченням (мережевою картою, Інтернет-браузером); якщо для досліджень надано окремий накопичувач на жорстких магнітних дисках (НЖМД), то слід з'ясувати склад установленого на ньому програмного забезпечення. У разі наявності комплексу технічної та програмної можливостей відповідно до визначених операційної системи й програмного забезпечення можна починати досліджувати сліди роботи користувача в Мережі, а саме файлові структури Cookies, Cache та журналів. Якщо такий комплекс відсутній, то цілком зрозуміло, що на цьому етапі дослідження експерт не може сказати, що слідів роботи користувача не виявлено. Треба відновити й дослідити видалену інформацію, і тільки після цього (залежно від результатів цих дій) остаточно визначитися щодо їхньої наявності.

Нагадаємо деякі терміни, що використовуються в цьому напрямі досліджень.

Cookies – це спеціальна текстова інформація, яку сервер передає браузеру та яка зберігається на комп'ютері користувача за запитом веб-сервера, а згодом передається йому при повторних відвідуваннях. Браузер зберігатиме цю інформацію й передаватиме її серверу з кожним запитом як частку HTTP-заголовка. Деякі значення Cookies можуть зберігатися тільки протягом однієї сесії та видалятися після закриття браузера; деякі, встановлені на певний проміжок часу, записуються у файл.

Більшість сучасних браузерів підтримують Cookies. Користувач може обирати, чи повинні Cookies використовуватися чи ні. Найбільш поширеними є такі налаштування браузерів:

— повне відключення Cookies;

— видалення Cookies під час закриття браузера;

— відрізнення сторонніх Cookies з третьої сторони та відповідні дії з ними (наприклад, їх обмеження чи заборона);

— оброблення Cookies на основі «білого» та/або «чорного» списку, які поновлює користувач чи виробник браузера (Cookies з «чорного списку» блокуються);

— заборона Cookies від певних доменів (різновид «чорного списку»);

— установлення розумних строків зберігання Cookies.

Cache (кеш) – це ділянка пам'яті (оперативної чи дискової), у якій розташовуються використані дані для прискорення повторного доступу до них: браузери часто зберігають у кешу копії відвідуваних веб-сторінок, аби повторно не завантажувати їх з Інтернету.

Історія відвідування веб-сторінок зберігається у журналі – списку раніше відвідуваних сторінок (наприклад, IE, Mozilla Firefox).

У табл. 1–3 наведено шляхи розташування зазначених файлових структур для найбільш популярних браузерів, які працюють під керуванням ОС сімейств MS Windows (XP), Unix/Linux і Mac OS.

Таблиця 1

Інтернет-браузер	Сімейство MS Windows (XP)		
	Cookies	Cache	History
Internet Explorer, Maxthon, Avant	\Documents and Settings\ *Ім'я Облікового Запису*\ Cookies\	\Documents and Settings\ *Ім'я Облікового Запису* \Local Settings\Temporary Internet Files\ Content.IE5\	\Documents and Settings\ *Ім'я Облікового Запису* \Local Settings\History\ History.IE5\
Google Chrome	Documents and Settings\ *Ім'я Облікового Запису* \Local Settings\Application Data\Google\Chrome\ User Data\Default\ Cookies	Documents and Settings\ *Ім'я Облікового Запису* \Local Settings\Application Data\Google\Chrome\ User Data\Default\ Cache\	Documents and Settings\ *Ім'я Облікового Запису* \Local Settings\Application Data\Google\Chrome\ User Data\Default\ History
Mozilla Firefox	\Documents and Settings\ *Ім'я Облікового Запису* \Application Data\ Mozilla\ Firefox\ Profiles\ *послідовність символів*. default \	\Documents and Settings\ *Ім'я Облікового Запису* \Local Settings\ Application Data\Mozilla\ Firefox\ Profiles\ *послідовність символів*. default \Cache\	\Documents and Settings\ *Ім'я Облікового Запису* \Application Data\ Mozilla\Firefox\ Profiles\ *послідовність символів*. default\ history.dat
Opera	\Documents and Settings\ *Ім'я Облікового Запису* \Application Data\ Opera\Opera\profile\ cookies4.dat	\Documents and Settings\ *Ім'я Облікового Запису* \Application Data\ Opera\ Opera \ profile\ cache4\	\Documents and Settings\ *Ім'я Облікового Запису* \Application Data\ Opera\ Opera\p rofile\
Safari	\Documents and Settings\ *Ім'я Облікового Запису* \Application Data\ Apple Computer\ Safari\Cookies\ Cookies.plist.	\Documents and Settings\ *Ім'я Облікового Запису* \Local Settings\ Application Data\ Apple Computer\ Safari\ Cache.db, SafeBrowsing.db та WebpageIcons.db	\Documents and Settings\ *Ім'я Облікового Запису* \Application Data\ Apple Computer\ Safari\ History.plist

Як відомо, при проведенні судової експертизи комп'ютерної техніки та програмного забезпечення загальний підхід до дослідження інформації, що міститься на цифровому носії (у нашому випадку – НЖМД), полягає у тому, аби жодним чином не внести зміни до неї в ході проведення дослідження. Саме тому, як правило, дослідження починаються з дублювання інформації (створення образу носія). В окремих випадках можливо проведення досліджень безпосередньо носія, якщо ОС завантажується із зовнішнього накопичувача (оптичного диску або флеш-носія). Це, так би мовити, традиційні підходи до дослідження.

Таблиця 2

Інтернет-браузер	Сімейство Unix/Linux		
	Cookies	Cache	History
Mozilla Firefox	/home/<ім'я користувача> /.mozilla/firefox/ *послідовність символів*.default/ cookies.sqlite	/home/<ім'я користувача> /.mozilla/firefox/ *послідовність символів*.default/ cache/	home/<ім'я користувача> /.mozilla/firefox/ *послідовність символів*.default/ places.sqlite
Opera	/home/<*ім'я користувача*> /.opera/	home/<*ім'я користувача*>/. opera/cache/	/home/<*ім'я користувача*>/. opera/sessions/

Таблиця 3

Інтернет-браузер	Mac OS		
	Cookies	Cache	History
Safari	/<*ім'я користувача*> /Library/Cookies/Cookies.plist	/<*ім'я користувача*> /Library/Cache/	/<*ім'я користувача*> /Library/Safari/

На наш погляд, у деяких випадках можливо запровадити альтернативний підхід, який полягає у такому: по-перше, зробити дублікат (тобто точну, працездатну копію, з якої можна проводити завантаження ОС і всього комплексу наявного програмного забезпечення) досліджуваного НЖМД, який надійшов у складі ПК; по-друге, замість досліджуваного вмонтувати НЖМД-дублікат, і завантаження ОС та подальші дослідження проводити на цьому носії; по-третє, по закінченні досліджень повернути НЖМД до складу наданого ПК.

У рамках першого підходу всі дослідження проводяться з образом носія засобами програмного забезпечення, за допомогою якого він був створений або дозволяє переглядати його та дослідити (WinHex/X-Ways

Forensics, Encase, ILook тощо). Якщо ці засоби не забезпечують всебічне дослідження, можна скопіювати необхідну інформацію на носій експерта (назвемо його експериментальним) і продовжити подальші дослідження на експериментальному носії спеціалізованими програмними засобами для цього виду інформації.

У разі завантаження ОС із зовнішнього носія та дослідження НЖМД безпосередньо у складі наданого ПК (тобто «наживо») інформація досліджується програмними засобами, які містяться на зовнішньому носії. Необхідно, аби до їхнього складу входили як мінімум файл-менеджер, спеціалізовані програмні засоби для певного виду інформації й програми з відновлення видаленої та ушкодженої інформації.

Якщо запровадити третій (нетрадиційний) підхід, то інформації може досліджуватися як засобами, що містяться на НЖМД, так і, якщо їх недостатньо, додатково спеціалізованими програмами, котрі можна завантажувати із зовнішніх носіїв.

У необхідних випадках можна комбінувати застосування підходів, наприклад, перший і третій.

Слід зазначити, що більшість Інтернет-браузерів має опціонні налаштування (як попередні, так і такі, що можна встановити під час роботи) з видалення файлів Cookies, Cache та History. Звичайно, користувач може видалити ці файлові структури як засобами ОС, так спеціально розробленими для таких дій (наприклад вільне ПЗ CookiesEater). Тому експерт повинен відновити та дослідити видалену інформацію (наприклад, використовуючи ПЗ R-Studio, GetDataBack for NTFS, GetDataBack for FAT, Ontrack EasyRecovery Professional тощо). Якщо серед видаленої та такої, яку можна відновити інформації, наявні відповідні файлові структури, то треба їх дослідити.

Додатково зазначимо, що, орієнтуючись на часові параметри створення та останнього змінення файлів структур Cookies, Cache та журналів на носії, можна вказати на останній вихід користувача в Мережу з використанням певного браузера, звичайно з урахуванням відносності часових параметрів комп'ютерної інформації.

Паралельно з пошуком назв певних Інтернет-сайтів за визначеними адресами для досліджуваних Інтернет-браузерів на НЖМД можна додатково проводити пошукові дослідження з використанням ключових слів.

З оглядом на викладені підходи розглянемо програмні засоби, які можна застосовувати для дослідження зазначених файлових структур.

Інтернет-браузери Internet Explorer, Maxthon, Avant. Для дослідження файлових структур Cookies, Cache та History можна використати програми-в'юєри, як вбудовані з реалізованим переліком кодувань (Hex, Unicode, UTF-8 тощо), так і зовнішні, наприклад Universal Viewer. Можливо використання таких вільних програмних засобів, як CacheView, CookieView, HistoryView, Cookie Monster. Це ПЗ знаходить необхідні файлові структури за адресами за умовчанням, що корисно при застосування третього підходу.

Зазначене ПЗ можна запускати також з консолі (командного рядку) з позначенням шляху розміщення файлів, що відповідає першому та другому підходам. Застосування вільного програмного забезпечення MAXA Cookie Manager можливо при третьому підході.

Такі дії можливі напряму, якщо дані файлові структури присутні в наявному вигляді на накопичувачі. У протилежному разі, колі ці структури видалено або засобами перелічених Інтернет-браузерів, або іншими програмними засобами, відновлюємо видалену інформацію, шукаємо серед неї відповідні файлові структури та досліджуємо їх в описаний спосіб.

Інтернет-браузер Google Chrome. Для дослідження файлових структур Cookies, Cache та History в середовищі ОС Windows XP можна використовувати програми-в'юєри: вбудовані з реалізованим переліком кодувань (Hex, Unicode, UTF-8 тощо) або зовнішні (Universal Viewer, SQLite Database Browser).

Інтернет-браузер Opera. Для дослідження файлових структур Cookies, Cache та History у середовищі ОС Windows XP можна використовувати програми-в'юєри: вбудовані з реалізованим переліком кодувань (Hex, Unicode, UTF-8 тощо), зовнішні (Universal Viewer), а також плагіни до файл-менеджера Total Commander. Можливо використання таких вільних програмних засобів, як Cookie Monster, MAXA Cookie Manager.

Для дослідження файлових структур Cookies, Cache та History в середовищі ОС Linux можна використовувати програми-в'юєри, вбудовані у файл-менеджер Midnight Commander з реалізованим переліком кодувань (Hex, Unicode, UTF-8 тощо), а також в емулюваному середовищі ОС Windows (наприклад, за допомогою Wine) відповідні програмні засоби, притаманні цьому середовищу.

Інтернет-браузер Firefox. Для дослідження файлових структур Cookies, Cache та History, створених у середовищі ОС Windows XP, можна використовувати програми-в'юєри, як вбудовані з реалізованим переліком кодувань (Hex, Unicode, UTF-8 тощо), так і зовнішні, наприклад Universal Viewer. Можливо використання таких вільних програмних засобів, як Mozilla CacheView, Mozillahistoryview, mzcv, Cookie Monster, MAXA Cookie Manager.

Для дослідження файлових структур Cookies, Cache та History в середовищі ОС Linux можна використовувати програми-в'юєри, вбудовані у файл-менеджер Midnight Commander з реалізованим переліком кодувань (Hex, Unicode, UTF-8 тощо), SQLite Database Browser, GUI editor for SQLite Database, а також в емулюваному середовищі ОС Windows (наприклад за допомогою Wine) відповідні програмні засоби, притаманні цьому середовищу.

Інтернет-браузер Safari. Для дослідження файлових структур Cookies, Cache та History в середовищі ОС Windows XP можна використовувати програми-в'юєри: вбудовані з реалізованим переліком кодувань (Hex, Unicode, UTF-8 тощо) або зовнішні (Universal Viewer, SQLite Database Browser; ПЗ MAXA Cookie Manager).

Для дослідження файлових структур Cookies, Cache та History в середовищі Mac OS можна використовувати внутрішні програми-в'юєри з відповідними кодуваннями (Hex, Unicode, UTF-8 тощо), а також ПЗ: File Juicer, яке дозволяє (крім іншого) одержати файли формату HTML з кешу браузера; HistoryHound, яке дає змогу проводити сканування зазначених файлових структур і пошук за ключовими словами (у реалізації другого та третього підходів).

Отже, підсумовуючи викладене, можна сформулювати таку послідовність дій експерта при вирішення питання, пов'язаного з визначенням того, чи відвідував користувач певні сайти:

— перевірити працездатність наданого обладнання: ПК (стаціонарний чи портативний), окремий носій (НЖМД);

— провести дублювання інформації (створення образу носія/носіїв) і подальші дослідження здійснювати з нею (за винятком окремих випадків);

— визначитися з наявністю можливості виходу користувача до Інтернету, а саме: чи оснащений наданий на дослідження ПК відповідним апаратним і програмним забезпеченням (один чи декілька Інтернет-браузерів). Якщо для досліджень надано окремий НЖМД, то слід визначитися з наявністю встановленого (встановлених) Інтернет-браузера;

— відновити видалену інформацію та визначитися, чи присутні у відновленій інформації файлові структури Cookies, Cache та History відповідного (відповідних) Інтернет-браузера;

— виходячи з відомого розташування файлових структур Cookies, Cache та History відповідного (відповідних) Інтернет-браузера, провести їхнє дослідження зазначеними програмними засобами. Додатково можна здійснити пошук по всьому простору накопичувача (накопичувачів) за переліком ключових слів, складеним з назв веб-сайтів, що вказані ініціатором експертизи;

— за результатами досліджень надати відповідь на запитання, чи відвідував користувач конкретні сайти, та вказати проміжок часу, коли здійснювалося відвідування.

Уважаємо за доцільне продовжити дослідження в цьому напрямі у зв'язку з подальшим розширенням застосування всесвітньої мережі Інтернет, розробленням та появою нових Інтернет-браузерів (наприклад Google Chrome) і нових операційних систем.