ISSN 1992-4437

ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ
ЕКСПЕРТНО-КРИМІНАЛІСТИЧНИЙ ЦЕНТР
МВС УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

КРИМІНАЛІСТИЧНИЙ ВІСНИК

Науково-практичний збірник

Виходить 2 рази на рік
Заснований у 2003 р.

№ 2 (26), 2016

Київ 2016

УДК 343.9
ББК 67.99 (4Укр) 94
К82

Внесено до Переліку наукових фахових видань України з юридичних наук :
наказ Міністерства освіти і науки України від 09.03.2016 № 241

Схвалено до друку науковою радою ДНДЕКЦ МВС України
(протокол від 26 грудня 2016 року № 51)
Схвалено до друку Вченою радою НАВС
(протокол від 26 грудня 2016 року № 37-ЗР)

К82 Криміналістичний вісник : наук.-практ. зб. / [голов. ред. В.В. Чернєй] / ДНДЕКЦ МВС України; НАВС. — К. : ПК «Типографія від «А» до «Я», 2016. — № 2 (26). — 188 с. : іл.

Містить праці з теоретичних, методичних, нормативно-правових, практичних, історичних, організаційних проблем судової експертизи та криміналістики. На сторінках вісника відображено матеріали багатого передового досвіду проведення криміналістичних досліджень, інтегровано все нове, що з'являється в галузі науки криміналістики.

Для фахівців з питань судово-експертного та техніко-криміналістичного забезпечення діяльності правоохоронних органів із запобігання, виявлення, розкриття й розслідування злочинів та інших правопорушень, а також науковців, викладачів, аспірантів і студентів юридичних навчальних закладів.

УДК 343.9
ББК 67.99 (4Укр) 94

ЗМІСТ

МЕТОДОЛОГІЯ ТА ОРГАНІЗАЦІЯ ЕКСПЕРТНО-КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ

ВИКОРИСТАННЯ ДОСЯГНЕНЬ НАУКИ ТА ТЕХНІКИ В ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

ПРОБЛЕМИ ДОСЛІДЖЕННЯ РЕЧОВИХ ДОКАЗІВ

ПЕРЕДОВИЙ ДОСВІД В ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

ВИДАТНІ ДІЯЧІ ТА ВИЗНАЧНІ ПОДІЇ В ГАЛУЗІ КРИМІНАЛІСТИКИ

УДК 621.377.6

Я.Ю. Коліса, *головний судовий експерт Полтавського науково-дослідного експертно-криміналістичного центру МВС України*

ПОШУК І ФІЛЬТРУВАННЯ ІНФОРМАЦІЇ, ЩО МІСТИТЬСЯ НА ЦИФРОВОМУ НОСІЇ

Досліджено методи відновлення та пошуку інформації на цифрових носіях, запропоновано спеціалізовані комп'ютерні програми для проведення дослідження, наведено приклади фільтрації інформації.

Ключові слова: цифровий носій, файлова система, сигнатура, ключова послідовність, індексна машина.

Исследованы методы восстановления и поиска информации на цифровых носителях, предложены специализированные компьютерные программы для проведения исследования, приведены примеры фильтрации информации.

Ключевые слова: цифровой носитель, файловая система, сигнатура, ключевая последовательность, индексная машина.

Methods of recovery and search information on digital data medium are investigated, specialized computer programs for research are offered, possible examples of information filtering are resulted.

Keywords: digital data medium, file system, signature, key sequence, index machine.

Правопорушники, прагнучи уникнути відповідальності, зазвичай намагаються заплутати слідство чи приховати сліди правопорушення. Не є винятком і сфера використання електронно-обчислювальних машин (комп'ютерів), хоча до того моменту, коли комп'ютерні злочини реально почали розслідувати, зловмисники залишали безліч слідів своєї активності [1].

Сьогодні протидія криміналістичному дослідженню комп'ютерної інформації стає дедалі активнішою. Правопорушники намагаються знищити інформацію, яка підтверджує їх діяння, шляхом видалення її з цифрових носіїв комп'ютера [2].

Водночас пошук інформації на цифрових носіях має важливе значення для розслідування комп'ютерних злочинів.

Метою статті є визначення методів виявлення, відновлення та пошуку інформації на цифровому носії.

Хибною є думка про те, що після завершення процесу видалення інформації з диска (цифрового носія) повністю видаляються всі дані без можливості їх відновлення [3].

Можливість збереження інформації на цифровому носії зумовлена основними принципами збереження файлів на дисках.

Для ефективнішого використання дискового простору інформація про файл і його вміст зберігається на диску в різних місцях. На диску є таблиця, в якій є інформація про файли: імена файлів, імена каталогів (шляхи до файлів), час створення або модифікації файлів та інформація про те, в якому місці диска знаходиться вміст

кожного файлу (де початок і де кінець файлу). В операційній системі (далі — ОС) Windows підтримуються дві файлові системи: FAT і NTFS. Зазначені таблиці для них називаються відповідно «таблиця розміщення файлів» (File Allocation Table або FAT) і «головна файлова таблиця» (Master File Table або MFT). Великий обсяг інформації про файли зберігається саме у FAT або MFT, хоча деяка інформація про структуру файлів та папок може перебувати і в інших місцях диска [3].

У разі видалення файлу з файлової таблиці затирається інформація про ім'я файлу, структуру каталогу і фізичне розташування файлу на диску, але сам файл залишається на диску непошкодженим, доки на його місце не буде записано інший файл.

Те саме відбувається під час форматування цифрового носія.

Іншими словами, операції видалення та форматування зачіпають насамперед файлову таблицю, а не саму інформацію на диску. Отже, у разі проведення швидкого форматування дисків під будь-яку ОС або повного форматування під ОС Windows XP (чи більш ранню версією ОС Windows) їх можна ефективно відновити. Найголовніше — це почати відновлення перш ніж інформація буде перезаписана іншим файлом або ОС. Диски після повного форматування під ОС Windows Vista або пізнішу версію ОС Windows, як правило, відновити неможливо [3].

Для відновлення файлів застосовують комп'ютерну програму R-Studio, розроблену компанією R-Tools Technology Inc. з використанням технології IntelligentScan. Ця програма дозволяє відновлювати файли навіть з пошкоджених файлових систем або з розділів цифрового носія, які були переформатовані в іншу файлову систему.

При відновленні даних не буває повністю однакових ситуацій. Часто вдається відновити усі втрачені файли з оригінальними іменами і структуру каталогів. В інших випадках вдається відновити лише вміст файлів, а інші параметри (наприклад, імена, структура каталогів, де вони перебували, часові позначки тощо) виявляються втраченими. Бувають також випадки, коли всі відновлені файли виявляються пошкодженими.

Існує два методи відновлення файлів, які не були перезаписані. В усіх програмах відновлення використовують або один з них, або обидва.

За допомогою першого методу проводять відновлення файлів шляхом аналізу інформації про файли та папки. Цей метод використовують першим у програмах відновлення інформації, і у разі успішного його застосування відновлюють не лише файли з оригінальними іменами, шляхами, відмітками дати та часу, а й саму інформацію. Якщо файлова система диска серйозно не пошкоджена, то цілком ймовірно, що вдасться повністю відновити структуру папок і файлів. У разі сильного пошкодження файлової системи цей метод не дозволяє відтворити повну структуру папок. У цьому випадку відновлені файли міститимуться у папках з присвоєними їм віртуальними іменами.

Другий метод відновлення файлів передбачає сканування файлів відомих типів (пошуку файлів за сигнатурами).

Пошук файлів за сигнатурами проводять у випадку, якщо за допомогою першого методу на вдається досягти бажаного результату. Цей метод дозволяє відновити більше інформації, однак при цьому не вдається отримати оригінальні імена файлів, відмітки дати та часу чи повну структуру папок і файлів на диску.

Використання заданої сигнатури дозволяє відновлювати файли певного типу в тому випадку, коли частково або повністю бракує (пошкоджена) інформації щодо структури каталогів та імен файлів.

Зазвичай для визначення місця розташування файлів використовують таблицю розділів диска. Якщо порівняти диск із книгою, то таблиця розділів диска схожа з її змістом. Під час сканування програма R-Studio шукає файли відомих типів у таблиці розділів диска за певними заданими сигнатурами. Це стає можливим завдяки тому, що практично кожен тип файлу має унікальну сигнатуру або шаблон даних. Файлові сигнатури (у вигляді шістнадцяткового коду) знаходяться у певному місці на початку або в кінці файлу. Під час сканування R-Studio зіставляє знайдену інформацію із сигнатурами файлів відомих типів, що дозволяє їх ідентифікувати та відновити інформацію [4].

За допомогою технології сканування файлів відомих типів можна відновити інформацію з дисків, які були переформатовані і таблиці розділів яких були перезаписані. Якщо розділ диска було перезаписано, пошкоджено або видалено, то сканування файлів відомих типів є єдино можливим методом відновлення інформації.

Етап відновлення видаленої інформації є базою для її пошуку.

Для пошуку інформації застосовують два методи: прямий пошук або пошук за допомогою індексної машини.

Прямий пошук передбачає послідовне відкриття спеціалістом кожного файлу та знаходження ключової послідовності. Пошук можна здійснювати і за допомогою програми, що має функції пошуку за файлами. Тривалість пошуку залежить від обсягу інформації, яку оброблюють, і може тривати від кількох секунд до кількох годин для однієї ключової послідовності — послідовності символів, що складається у слово чи словосполучення без урахування кодової сторінки чи інших особливостей. При цьому різні ОС по-різному ототожнюють той самий символ та число, і навпаки, а отже, є вірогідність незнаходження потрібного тексту, що містить ключову послідовність. Не дасть певних результатів і пошук за так званим стоп-словом, що означає послідовність символів, яка найчастіше трапляється в усіх найбільш відомих документах [2, с. 12].

Загалом метод прямого пошуку здебільшого є малоефективним, адже потребує не лише доволі багато часу, а й повторного сканування кожного файлу на нову ключову послідовність (а кожна нова послідовність подвоює, потроює тощо витрати часу на пошук інформації).

Другий метод пошуку інформації передбачає застосування індексної машини, яка сканує усі файли із вмістом розшукуваного тексту. Машина розбиває текст на токени (слова, словосполучення), після чого відбувається створення індексу файлів і токенів, що містяться в них. Створення індексу залежить від обсягу обробленої інформації та може тривати від кількох секунд до кількох годин. Після створення індексу можна відразу проводити пошук інформації за ключовими послідовностями.

Прикладом ефективної індексної машини є комп'ютерна програма Архіваріус 3000 компанії Likasoft. Архіваріус 3000 розуміє запити природною мовою (наприклад, російською, англійською). Документи можуть бути знайдені за ключовими словами або з використанням мови запитів (як у звичайних пошукових системах Інтернету). Під час пошуку програма автоматично використовує усі граматичні форми слова і забезпечує пошук на 18 мовах [5].

У процесі індексування документів і поштових повідомлень Архіваріус 3000 відшуковує і зберігає всю інформацію. Навіть якщо документ фізично недоступний, програма знайде його за вмістом і визначить, на якому диску знаходиться розшукуваний файл [5].

Проте, навіть застосовуючи цю комп'ютерну програму, експерту доводиться візуально переглядати тисячі текстів і зображень, адже органи слідства часто цікавить, чи належить виявлена інформація до розслідуваної справи. Звісно, для відповіді на це запитання експерт має ознайомитися з матеріалами кримінального провадження.

На цьому етапі є змога відсіяти інформацію, яка не цікавить слідство, але при цьому може збільшити тривалість дослідження. Для фільтрації інформації потрібна взаємодія зі слідством і визначення ним пріоритетів. Тобто органи слідства мають або враховувати час, потрібний експерту для фільтрації виявленої під час пошуку інформації, або проводити цю роботу самостійно.

Слід зазначити, що файли з текстовим, графічним, табличним або комбінованим змістом часто містять багато службової інформації, яка не доступна користувачу персонального комп'ютера, і він навіть не підозрює про її існування. Проте експерту про неї відомо, і він може вилучити її з файлу. Наприклад, у файлах формату JPEG (jpg) зберігається інформація про модель фотоапарата, час знімка, використання спалаху тощо. У файлах формату MS-Word зберігається ідентифікатор (логін) користувача, який створив файл, початкове розміщення файлу тощо [6, с. 271]. Тому як при дослідженні окремих файлів (крім найпростіших текстових або ASCII-файлів), так і при дослідженні комп'ютерів, дисків, інших носіїв інформації для фільтрування інформації має значення виявлення прихованої службової інформації, передбаченої відповідним форматом файлу.

З огляду на те, що, крім самого файлу, на цифровому носії зберігається інформація про нього у різних місцях, то навіть коли файл затертий, знищений без можливості його відновлення, можна встановити факт його наявності у минулому за непрямими доказами. Цими доказами можуть бути фрагменти файлу, його заголовок, згадування імені файлу та його атрибутів в історії програм, які з ним взаємодіяли, мініатюри (thumbnails), які створює ОС, і деякі програми перегляду для прискорення перегляду списку файлів.

У деяких випадках немає потреби відновлювати знищену або зашифровану інформацію, достатньо лише довести її наявність на досліджуваному цифровому носії. Наприклад, експерт шукав на носії підозрюваного електронні зображення грошових купюр, у підробці яких його підозрюють. Файли із зображеннями купюр виявилися затертими без можливості відновлення, але збереглися мініатюри, які ОС автоматично створила для зазначення списку файлів у каталозі. Для графічних файлів мініатюра являє собою зменшене зображення оригіналу. Незважаючи на невеликий розмір мініатюри, її зміст видно достатньо добре. Експериментальним шляхом експерт створює з великого зображення грошової купюри таку саму мініатюру, що підтверджує гіпотезу [6, с. 281].

Як найпростіший приклад можна навести файл «Thumbs.db», який містить мініатюри файлів (наприклад, графічних, текстових) або історію розміщення файлів каталогу за їх мініатюрними зображеннями, хоча самих файлів каталог вже не містить [2, с. 33].

Підбиваючи підсумки, слід окреслити такі основні висновки:

– пошуку інформації передує оцінка структурованості інформації, рівня її відновлення, фізичної спроможності носія інформації до відновлення. Для відновлення інформації застосовують два методи: аналіз інформації про файли та папки і сканування файлів відомих типів (пошук файлів за сигнатурами);

– інформацію шукають за допомогою методів прямого пошуку та пошуку за допомогою індексної машини;

– дослідження з відновлення та пошуку інформації зазвичай потребують великих витрат апаратних ресурсів обчислення та безперервного і тривалого часу дослідження. Водночас терміни виконання досліджень експертами спеціалізованих установ МВС України обмежені, а отже, органи слідства мають враховувати цей чинник, що має важливе значення для об'єктивності експертного дослідження під час проведення досудового слідства.

Список використаної та рекомендованої літератури

1. *Криминалистический* подход к анализу временных атрибутов файлов в операционной системе семейства Microsoft windows и файловой системе ntfs [Электронный ресурс]. — Режим доступа : https://xakep.ru/2013/02/22/60167/.

2. *Дослідження* інформації на цифрових носіях / [укл. Бобрицький С.М., Чишкала О.В., Серий В.В. та ін.]. — Харків : ХНДІСЕ Мін`юсту України, 2009. — 41 с.

3. *Восстановление* диска и реконструкция RAID [Электронный ресурс]. — Режим доступа : http://www.unformat-unerase.com/ru/#3.

4. *Создание* пользовательского известного типа файла для R-Studio [Электронный ресурс]. — Режим доступа : http://www.r-tt.com/ru/Articles/Creating_Custom_File_Type_R-Studio/.

5. *Архивариус* 3000 Поиск документов : Likasoft [Электронный ресурс]. — Режим доступа : http://www.likasoft.com/ru/document-search/index.shtml.

6. *Федотов Н.Н.* Форензика — компьютерная криминалистика / Н.Н. Федотов. — М. : Юрид. мир, 2007. — 432 с.

7. *Кримінальний* кодекс України : станом на 15 бер. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/2341-14.

8. *Принципы* восстановления данных [Электронный ресурс]. — Режим доступа : http://www.r-tt.com/ru/Articles/File_Recovery_Basics/.

Наукове видання

ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ
ЕКСПЕРТНО-КРИМІНАЛІСТИЧНИЙ ЦЕНТР
МВС УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

КРИМІНАЛІСТИЧНИЙ ВІСНИК

Науково-практичний збірник

Виходить 2 рази на рік
Заснований у 2003 р.

№ 2 (26), 2016

Свідоцтво про державну реєстрацію, видане Державною реєстраційною службою України,
від 09.02.2011, серія АА № 421285

Надруковано з оригіналу-макета, виготовленого ПК «Типографія від «А» до «Я»
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
від 26.05.2014, серія ДК № 4724

Редактор А.В. Джулай
Коректор І.О. Пашкевич
Комп'ютерна верстка С.М. Гавриляк

Підп. до друку 15.12.2016. Формат 70x100/16
Папір оф. №1. Гарнітура Pragmatica. Друк. офс.
Ум. друк. арк. 15,6. Фіз. друк. арк – 12
Тираж 310 пр. Зам. № 78.

Віддруковано на ПК «Типографія від «А» до «Я»
02660, м. Київ, вул. Колекторна, 38/40, тел./факс 562-37-03
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
від 26.05.2014, серія ДК № 4724

Адреса редакції: вул. Велика Окружна, 4, м. Київ, 03680, Україна
тел.: (044) 374-34-23, факс: (044) 405-74-69
dndekc@mvs.gov.ua http:// dndekc.mvs.gov.ua