Deluge	C: \Пользователи\ %Username %\AppData\Roaming\deluge\state\ torrents.fastresume
Halite	C: \Users\Comp\AppData\Local\Halite\resume У папці resume зберігаються файлі у форматі *.fastresume, *.torrent_info, які містять інформацію про завантажені/роздані файли.
Shareaza	C: \Users\Comp\AppData\Roaming\Shareaza\Torrents У папці Torrents зберігаються файлі у форматі *.torrent, які роздаються

Було досліджено ряд найпоширеніших, на даний час, торрент-клієнтів, які можуть бути використані як альтернатива клієнту µTorrent, під час дослідження виявлено місця зберігання різними торрент-клієнтами інформації про завантажену/розповсюджену інформацію.

Список використаних джерел:

1. А в вашей жизни были приключения интереснее, чем в компьютерных играх? 10 лет uTorrent: краткая история одного из самых популярных в мире приложений. URL: https: //habr.com (дата звернення: 23.01.2019).

2. Bit Torrent Specification. URL: https: //wiki.theory.org/index.php/BitTorrentSpecification (дата звернення: 01.02.2019).

3. Торрент клиенты для windows. URL: http: //softcatalog.info/ru/obzor/torrent-klienty-dlya-windows (дата звернення: 15.01.2019).

УДК 343.98

Бородай О. В., *ад'юнкт Харківського національного університету внутрішніх справ,* ¶
ORCID: https: //orcid.org/0000–0003–1321–6401,
e-mail: a1ek5borodaj@gmail.com

СТВОРЕННЯ ПОБІТОВИХ ОБРАЗІВ НОСІЇВ ІНФОРМАЦІЇ ТА ЇХ ЗНАЧЕННЯ ПІД ЧАС РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ У РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ АБО МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Досудове розслідування злочинів, пов'язаних з використанням комп'ютерної техніки, зокрема, розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку, має свою специфіку. Під час розслідування зазначеної категорії кримінальних проваджень є отримання та аналіз інформації, що зберігається на електронних носіях інформації, з метою отримання належних та допустимих доказів.

Як правило, огляд електронних носіїв інформації на місці проведення слідчої дії має складності, а для виявлення слідів злочину, які містяться в даних, що зберігаються на носіях інформації, потрібен тривалий час. З цієї причини доцільно тимчасово вилучати такі носії інформації для проведення огляду з фахівцем або проведення судової комп'ютерно-технічної експертизи.

Однак на практиці нерідко виникають ситуації, коли поряд зі значущою для слідства інформацією на електронних носіях, які планується вилучити, можуть перебувати важливі для їх законних власників дані, що не мають відношення до кримінального провадження. Неможливість подальшого використання власником носіїв інформації у зв'язку з їхнім вилученням може завдати йому невиправданий збиток. Такі ситуації часто виникають, коли необхідно досліджувати комп'ютери потерпілої сторони.

В цьому випадку чинне кримінально-процесуальне законодавство передбачає можливість копіювання слідчим або прокурором із залученням спеціаліста інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах.

Природа цифрових доказів зазвичай досить тендітна і схильна до змін, тому під час виготовлення копій варто уникати будь-яких дій з носіями інформації, наслідки яких не можна передбачити заздалегідь.

Щоб створений образ носія інформації був криміналістично достовірний, потрібно, по-перше, в процесі його створення не змінювати вміст досліджуваного носія, а по-друге, після вилучення образ повинен побітово відповідати досліджуваному носію – оригіналу. Такий

образ буде містити не тільки регулярні файли, але і службові дані, вільні області файлових систем та області, нерозмічені файловими системами, а також інформацію про видалені файли.

Однак потрібно враховувати, що електронний носій інформації при підключенні до непідготовленого комп'ютера схильний до підвищеного ризику зміни даних. Автоматичний процес монтування носія інформації може привести до таких змін, як індексація файлів або зміна часових міток на пристрої зберігання, особливо в нерозмічених секторах розділу, які містять видалені файли, що може призвести до перезапису або знищення потенційних доказів [1].

На твердотільних накопичувачах (SSD) через агресивну функцію TRIM і функцію збору сміття [2–4] ці зміни помітніші і ризик втрати потенційних цифрових даних вище. Якщо ж твердотільний накопичувач підключений до криміналістичної робочої станції з відключеним автоматичним монтуванням, то функція TRIM не виконується.

Щоб визначити достовірність цифрових доказів, використовуються алгоритми хешування для підтвердження ідентичності образу носія інформації оригіналу і цілісності даних [5].

Також при порівнянні значень хеш-функцій важливо враховувати стан носія інформації: значення хеш-функції, згенеровані для змонтованого пристрою, будуть відрізнятися від значень хеш-функції, згенерованих для пристрою, коли він не змонтований. Це пов'язано тільки зі станом носія інформації і не означає спотворення даних, що на ньому зберігаються.

Також практика показує, що використання різних кабелів і адаптерів при підключенні носія інформації теж може вплинути на результат обчислення значення хеш-функції.

Таким чином, для вилучення криміналістично достовірних побітових образів носіїв інформації треба дотримуватися таких рекомендацій:

1) відключити автоматичне завантаження та монтування носія інформації за допомогою одного з Forensic Live CD (Sumuri Paladin, DEFT Zero, CAINE, Kali Linux);

2) виконувати всі дії по верифікації та отриманню інформації, коли носій інформації не змонтований в операційну систему;

3) використовувати один і той же адаптер і/або кабель для хешування і створення побітового образу носія інформації;

4) підключити носій інформації до криміналістичної робочої станції, використовуючи апаратний або програмний блокувальник запису;

5) перевірити цілісність носія інформації, використовуючи алгоритм хешування SHA-1, і записати згенероване значення хеш-функції;

6) створити побітовий образ носія інформації за допомогою інструментів Forensic Live CD;

7) порівняти значення хеш-функції оригінального носія інформації і його образу, вони повинні збігатися.

Цей метод був протестований і перевірений з використанням операційних систем Linux і є рішенням, яке може використовуватися будь-яким слідчим, прокурором, фахівцем, експертом для створення криміналістично достовірних побітових образів носіїв інформації, які мають значення для проведення розслідування.

Список використаних джерел:

1. Nikkel B. Practical forensic imaging: securing digital evidence with Linux tools. San Francisco: No Starch Press, 2016. 292 p.

2. Bell, Graeme B. and Boddington, Richard. Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? *Journal of Digital Forensics, Security and Law*: Vol. 5: No. 3, Article 1. 2010. P. 1–20.

3. Nisbet, S. Lawrence, M. Ruff. A forensic analysis and comparison of solid state drive data retention with trim enabled file systems, digital investigation. SRI Security Research Institute, Edith Cowan University, Perth, Western Australia. 2013. P. 103–111.

4. King, T. Vidas, Empirical analysis of solid state disk data retention when used with contemporary operating systems, year investigation 8. 2011. S. 111–S117.

5. L. Chen, G. Wang, An efficient piecewise hashing method for computer forensics, in: Knowledge Discovery and Data Mining, 2008. WKDD 2008. First International Workshop on, IEEE. 2008. P. 635–638.