Розв'язання проблем, зазначених вище, має бути комплексним, адже без розв'язання окремих питань шляхом удосконалення законодавства, неможливе складання відповідних методик та їх застосування у дослідженнях.

Сьогодні особливості проведення судової комп'ютерно-технічної експертизи утворюють нові можливості розвитку державної політики у сфері забезпечення інформаційної безпеки та протидії кіберзлочинності. Пріоритетним напрямком розвитку комп'ютерно-технічної експертизи повинно стати удосконалення науково-методичного та інформаційного забезпечення судово-експертної діяльності. Поруч з цим, необхідне удосконалення закону про «Заборону грального бізнесу в Україні», або прийняття закону, який би надавав юридичне роз'яснення поняттям «гральне обладнання», «вимоги до грального обладнання», «гральний автомат», «комп'ютерний симулятор» тощо, адже закон, який регламентує заборону грального бізнесу на сьогодні не є досконалим і не завжди дозволяє спиратися на нього у дослідницькій діяльності.

Список використаних джерел:

1. Про заборону грального бізнесу в Україні : закон України від 15 трав. 2009 № 1334–VI URL: http: //zakon2.rada.gov.ua/laws/show/1334–17.

2. Експертизи у судочинстві України : наук.-практ. посіб. / заг. ред. В. Г. Гончаренка, І. В. Гори. Київ : Юрінком Інтер, 2014. 504 с.

3. Гора И. В. Организационные проблемы судебно-экспертной деятельности в Украине. Criminalistics and forensic expertology: science, studies, practice. Vilnius, Varsuva, 2016. С. 263–278.

4. Галинская А. Е. Особенности использования специальных знаний в деятельности сторон и их представителей по делам о правонарушениях в сфере информационных технологий. *Теория и практика судебной экспертизы*. 2017. Том 12 № 1. С. 30–37.

5. Сімакова-Єфремян Е. Б., Балинян Т. Є., Дереча Л. М. Про критерії оцінювання методик проведення судових експертиз в Україні. *Теорія та практика судової експертизи і криміналістики* : збірник наук. праць. 2010. Вип. 10. Харків : Право, 2010. 367 с.

УДК 004.02

Литвицький О. П., *завідувач сектору Запорізького НДЕКЦ МВС України,*
e-mail: litvicki@ukr.net

ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ ІНФОРМАЦІЇ, РОЗПОВСЮДЖУВАНОЇ ЗА ДОПОМОГОЮ ПРОТОКОЛУ ТОРРЕНТ У РІЗНИХ ПРОГРАМАХ-КЛІЄНТАХ

В наш час важко уявити життя суспільства без комп'ютерної техніки. Щосекунди в світі передаються колосальні об'єми інформації. Це підвищило комунікаційні можливості – для спілкування більше не потрібно гаяти багато часу та витрачати значні кошти: за допомогою мережі Інтернет можна сягнути найвіддаленіших куточків планети в лічені миті.

Але такий шалений розвиток сучасних технологій не міг лишитися поза діяльністю злочинного світу.

Сьогодні в світі протокол торрент є одним з найпоширеніших засобів злочинного розповсюдження різноманітного медіа-контенту, тому актуальність питання дослідження даного протоколу та способів поширення інформації за його допомогою лишається достатньо високою.

Автором і розробником пірингового протоколу BitTorrent є Брем Коен, саме він у 2001 році працював над даною розробкою, а також написав перший торрент-клієнт мовою Python, та в маї 2005 р. оприлюднив його.

BitTorrent – пірінговий (P2P) мережевий протокол, який використовується для обміну файлами між користувачами через Інтернет [1].

Файли передаються частинами, причому кожен клієнт починає «роздавати» вже скачані частини іншим клієнтам, що дозволяє розвантажити джерело, та забезпечує постійну доступність до всіх частин даних.

Раніше програмою, яка реалізовувала торрент протокол, був лише µTorrent. Але через те, що формат кодування у торрент-файла – це bencode, а структура Bencode-формат дозволяє зберігати такі типи даних:

— Строки, має формат <довжина строки>: <строка>;
— Числа, має формат <ключ i><число><ключ e>;
— Списки, мають формат <ключ l><bencoding дані><ключ e>;

— Директиви, мають формат <ключ d><строка bencoding><елемент bencoding><ключ e> [2].

На сьогодні реалізована велика кількість альтернатив звичного і знайомого всім торрент-клієнта µTorrent, тому проводячи дослідження інформації, пов'язаної з розповсюдженням файлів із забороненим контентом, для отримання найбільш повних і достовірних результатів висновків при пошуку інформації, яка розповсюджувалася за допомогою пірінгових мереж треба розглядати в ширшому сенсі, не обмежуючись лише програмою µTorrent.

Так, на сьогодні за статистикою [3], крім класичного µTorrent, серед користувачів популярні такі клієнти:

— ComboPlayer;
— qBittorent;
— BitComet;
— BitTorent;
— Vuze;
— Deluge;
— Halite;
— Shareaza.

Всі програми написані різними розробниками, тому кожна має свою специфіку. Наприклад, для відповіді на питання – які файли було скачано/розповсюджено з певної комп'ютерної техніки, необхідно знайти і дослідити файл «історії», а його назва і місцезнаходження у різних програм буде відрізнятися.

Саме через це важливо дослідити структуру хоча б найпоширеніших клієнтів, оскільки програмне забезпечення створене різними програмістами не має єдиної специфікації розміщення службових файлів і може розміщуватися де завгодно.

Дослідження місця зберігання історії завантажень/роздач в різних торрент-клієнтах проводилось в операційній системі Microsoft Windows 7. Оскільки дослідження проводилося в операційній системі Microsoft Windows 7, для інших операційних систем місця розташування потрібних файлів можуть відрізнятися.

Результати дослідження наведені в таблиці 1.

Таблиця 1

Результати дослідження місця зберігання історії завантажень/роздач в різних торрент-клієнтах

Назва	Розташування файлів історії
µtorrent	C: \Пользователи\ %Username %\AppData\Roaming\uTorrent\resume.dat
ComboPlayer	C: \Пользователи\ %Username %\AppData\Roaming\ComboPlayer\ db_broadcasts.sqlite Документ db_broadcasts.sqlite містить інформацію про файли, що поширювались за допомогою даного клієнта.
qBittorent	C: \Пользователи\ %Username %\AppData\Local\qBittorent\logs\ qbittorrent.log Документ qbittorrent.log містить інформацію про події даної програми, в тому числі інформацію про розповсюдження контенту.
BitComet	C: \Пользователи\ %Username %\AppData\Roaming\BitComet\Downloads.xml Документ Downloads.xml містить інформацію про файли, що поширювались за допомогою даного клієнта.
BitTorrentWeb	C: \Users\Comp\AppData\Roaming\BitTorrent Web\ C: \Users\Comp\AppData\Roaming\BitTorrent Web\ C: \Users\Comp\AppData\Roaming\BitTorrent Web\ C: \Пользователи\ %Username %\AppData\Roaming\TorrentWeb\ resume.dat Документ resume.dat містить інформацію про файли, що поширювались за допомогою даного клієнта
Vuze	C: \Users\Comp\AppData\Local\Halite\resume C: \Users\Comp\AppData\Roaming\Azureus\torrents C: \Users\Comp\AppData\Roaming\Azureus\torrents C: \Users\Comp\AppData\Roaming\Azureus\torrents У папці torrents зберігаються файлі у форматі *.torrent, якы були завантажені/роздані

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