3. КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА.

КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА ЯК НОВИЙ ВИД ІНЖЕНЕРНО-ТЕХНІЧНИХ ЕКСПЕРТИЗ

Воробей В. М., студент 4-го курсу навчально-наукового інституту права та психології Національної академії внутрішніх справ

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).

З метою дослідження комп'ютерів, їх комплектуючих і тієї інформації, що в них знаходиться, призначається комп'ютерно-технічна експертиза.

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 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.

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.

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, спеціалі-зовані програмні засоби для певного виду інформації й програми з відновлення видаленої та ушкодженої інформації.

Якщо запровадити третій (нетрадиційний) підхід, то інформація 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.

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.

КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Добришин Ю.Є., кандидат технічних наук, доцент, заступник директора Коледжу економіки, права та інформаційних технологій Університету «КРОК»