З огляду на викладене, з метою покращення можливостей розслідування даної категорії злочинів необхідне вдосконалення як процесуального законодавства так і криміналістичного (постійної розробки новітньої методиці збирання та дослідження електронних доказів на досудовому провадженні, та методика дослідження цих доказів у судовому засіданні). З урахуванням сучасних можливостей криміналістики необхідно підвищити принаймні базовий рівень знань у галузі ІТ технологій усіх осіб, які здійснюватимуть пошук і фіксацію та досліджуватимуть електронні докази.

Одержано 01.11.2017

УДК 343.1 + 004

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент, професор кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ ПРАКТИКИ ЗАБЕЗПЕЧЕННЯ НАЛЕЖНОСТІ ДОКАЗІВ, ОТРИМАНИХ З ОНЛАЙН РЕСУРСІВ

Злочини, що пов'язані із торгівлею людьми, широко застосовують інформаційні технології шляхом: організації в онлайн-режимі секс-чатів, відео трансляцій сексуальних дій; вербування жертв через веб-сайти з оголошеннями про працевлаштування; публікації на різноманітних ресурсах в Інтернеті пропозицій щодо надання сексуальних послуг; і таке інше.

При розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій, здійснюється пошук доказів, на підставі яких суд буде вирішувати питання про вину підозрюваних в учиненні кримінального злочину. Онлайн-ресурси в Інтернеті, пов'язані із торгівлею людьми, можна розглядати як цифрові джерела речових доказів, які мають певні унікальні характеристики порівняно із традиційними доказами.

Відповідно до ст. 94 Кримінального процесуального кодексу України кожен доказ у кримінальному провадженні має оцінюватися з точки зору належності, допустимості, достовірності. При оцінці належності доказів із цифрових джерел інформації можуть використовуватися критерії: справжності, повноти, надійності, переконливості.

Для забезпечення належності доказів, отриманих з онлайн ресурсів в Інтернеті, представляється доцільним використання

поряд із традиційними методами специфічних практик документування, що наводяться нижче.

Відео захоплення екрану (video screen capture). Доцільно разом із записом на відеокамеру процесу огляду онлайн ресурсів використовувати спеціальні програми цифрового відеозапису інформації, яка виводиться на екран. Доречним є використання безкоштовних програм з відкритим вихідним кодом, наприклад, ShareX (https://getsharex.com/).

Підтвердження справжності веб-сторінки. Для визначення справжності веб-сторінки, що буде оглядатися, по-перше, доцільно за допомогою утиліт командного рядка типу tracert (traceroute) зафіксувати маршрут прямування даних до сервера, на якому розміщено веб-сайт. По-друге, зафіксувати процес отримання непрямого доступу (через проксі) до веб-сторінки, наприклад через сервіс Google Translate. Для цього в адресному рядку браузеру потрібно ввести адресу цільового сайту (xxxx.xxx):

https://translate.google.com/translate?sl=en&tl=ru&u=http://xxxx.xxx,

де виставити напрям перекладу на оригінальну мову веб-сторінки. В цьому випадку сервер Google підключається до серверу, де знаходиться потрібна веб-сторінка, запитує зазначений веб-ресурс і передає отримані дані. Якщо записати процес перевірки на відео, то можна підтвердити, що здійснюється огляд справжньої веб-сторінки, при цьому час і дата відвідування Google Translate, IP-адреса і URL будуть відображені в журналах серверів Google.

Збереження вихідного HTML-коду веб-сторінки. Для збереження вихідного HTML-коду веб-сторінки достатньо у браузері вибрати опцію «Зберегти сторінку як» або «Файл - Зберегти як». Також у контекстному меню є опція «Подивитися вихідний код», який можна зберегти як текстовий файл.

Створення повної копії веб-сайту. В деяких випадках у судовому процесі потрібно демонструвати повний вміст веб-сайту. З метою фіксації вмісту усього веб-сайту, а не окремої веб-сторінки, можна створити копію сайту для перегляду в автономному режимі, наприклад, за допомогою програми HTTrack Website Copier (http://www.httrack.com), яка завантажує пов'язані веб-об'єкти за визначеною глибиною і дозволяє відкрити веб-сайт з усіма зображеннями в автономному режимі.

Фіксація метаданих об'єктів веб-сторінки. Розширення HttpFox для браузеру Mozilla Firefox дозволяє вибрати будь-який елемент веб-сторінки і зафіксувати метадані, наприклад, час і дату останньої модифікації.

Фіксація стороннім сервісом дати і локального часу веб-серверу, на якому розміщений веб-ресурс. Щоб збільшити доказову силу відеозапису, можна продемонструвати додаткові технічні дані досліджуваної веб-сторінки, які надає сторонній сервіс, наприклад, http://www.webconfs.com/http-header-check.php, який відображає HTTP-заголовки заданого домену. Як правило, заголовок містить поле «дата», в якому міститься дата і локальний час наданий веб-сервером, де розміщений сайт.

Встановлення внутрішнього ідентифікатора об'єкту соціальної мережі. Соціальні мережі широко використовують внутрішні ідентифікатори (ID) для відстеження будь-якої активності на сайті (користувачі, фотографії, чати, сеанси, групи, позначки «мені подобається» і т.д.). Наприклад, Facebook використовує ідентифікатор «fbid» (https://www.facebook.com/photo.php?fbid=10103832396388711). Поряд із отриманням скріншоту профіля, зображення і т.п. підозрюваного доцільно встановити його внутрішній ідентифікатор в базі даних соціальної мережі.

Ідентифікатори встановлюються або в адресному рядку браузера або через їх пошук у вихідному коді веб-сторінки. Для Facebook ідентифікатор профілю у вихідному коді можна знайти за запитом ?id=, а для Twitter – за запитом data-user-id. Для перевірки правильності знайденого значення внутрішнього ідентифікатору можна скористуватися сторонніми сервісами, наприклад, https://findmyfbid.in/.

Після збереження відповідних файлів на підготовлений цифровий носій (наприклад, DVD-R) з метою подальшого контролю цілісності отриманої інформації потрібно обчислити їх дайджест (хеш-функцію). На сьогодні безпечним алгоритмом з найменшим розміром дайджесту визнаний алгоритм хешування SHA-2, який, наприклад, реалізований у програмі з відкритим вихідним кодом QuickHash (https://quickhash-gui.org).

Розглянуті практики забезпечення належності доказів, отриманих з онлайн ресурсів, не є вичерпними і можуть змінюватися разом із зміною інформаційних технологій.

Одержано 18.10.2017