Використання інформації щодо активності користувача в операційній системі Windows як джерело доказів під час досудового розслідування

Євгеній Тарасенко
завідувач сектору комп'ютерно-технічних та телекомунікаційних досліджень,
Сумський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України, м. Суми, Україна,
e-mail: t.expert.kte.sumy@gmail.com

Розглянуто актуальність дослідження активності користувача в операційній системі Windows та можливість використання цих даних під час досудового розслідування.

Ключові слова: *операційна система; користувач; журнал подій; досудове розслідування.*

Using Information About User Activity in the Windows Operating System as a Source of Evidence During a Pre-Court Investigation

Evgeniy Tarasenko

This work examines the relevance of the study of user activity in the Windows operating system and the possibility of using this usage data during a pre-trial investigation.

Keywords: *operating system; user; event log; pretrial investigation.*

У сучасних кримінальних провадженнях доволі часто фігурує комп'ютерна техніка, яку під час досудового розслідування досліджують на предмет різної інформації, яка може мати значення для слідства. В операційній системі *Windows* зберігається чимало журналів активності, які допоможуть визначити, які саме дії виконував користувач та в який час [1]. Під час розслідування можна порівняти журнали з показаннями фігурантів тієї чи тієї справи та визначити правдивість їх показань.

Нижче наведено основні типи журналів та інформація, яка в них зберігається:

- *системні журнали*. У них зберігається інформація про системні події: завантаження системи, установлення та видалення програмного забезпечення, інформація про встановлення служб та драйверів, інформація про обладнання, про підключені пристрої та інші системні події. Також в цій категорії зберігається інформація про останні відкриті файли та каталоги, а також запущені програми;
- *журнали безпеки*. У цих журналах зберігається інформація про події, пов'язані з безпекою системи: спроби входу, зміни прав доступу, записи антивірусного програмного забезпечення та інші дії, які можуть вплинути на безпеку системи;
- *журнали програмного забезпечення*. Тут зберігається інформація про роботу інстальовано-

го програмного забезпечення. У цих журналах може зберігатися інформація про запуск програмного забезпечення, налаштування та помилки, які виникли під час його роботи. Тип інформації, яка може зберігатися в таких журналах, відрізняється залежно від програмного забезпечення та його налаштувань [2].

Під час аналізу журналів подій та активності користувача перше, на що варто звернути увагу, це дата та час входу в систему. Не менш важливою є інформація про останні дії користувача, такі як відкриті файли або програмне забезпечення, яке було запущене в той чи той час. Інформація про підключені пристрої стане в пригоді, якщо потрібно встановити, чи підключався, наприклад, той чи той флеш-накопичувач до комп’ютера. Інформація про роботу інстальованого програмного забезпечення може мати значення залежно від його типу. Наприклад, якщо це програмне забезпечення призначене для віддаленого доступу, у його журналах може зберігатися інформація про дату та час таких підключень та, за можливості, інші дані: назва віддаленого комп’ютера або його *IP*-адреса. До активності користувача також може належати інтернет-історія браузера (програма для доступу до інтернет-ресурсів). У журналі браузера зберігається інформація про те, на який сайт був здійснений доступ та в який час, також можна виявити інформацію про пошукові запити, які вводив користувач. Важливо враховувати, що обсяг та тривалість зберігання журналів активності можуть бути обмеженими і залежати від налаштувань системи, а також від того, чи була увімкнена функція журналювання. Користувач може також чистити (видаляти) історію своєї активності [3].

Проаналізувавши інформацію про активність користувача в операційній системі Windows, ми можемо її порівняти з показаннями особи та визначити правдивість її тверджень під час допиту. Наприклад, коли особа вказує, що вона не працювала в цей час за комп’ютером, або не заходила на певні інтернет-ресурси, або не вчиняла інші дії, які були виявлені під час аналізу активності користувача. Такий метод розслідування допомагає виявити неправдиві свідчення та визначити, де саме починаються розходження з виявленою інформацією та показаннями, які дає особа.

Перелік джерел посилання

1. Yosifovich P., Russinovich M., Solomon D., Ionescu A. Windows Internals: System architecture, processes, threads, memory management, more. 2020. 800 p.
2. Windows Event log. Microsoft Ignite : web. URL: https://learn.microsoft.com/en-us/windows/win32/wes/windows-event-log (дата звернення: 28.08.2025).
3. Windows activity history and your privacy. URL: https://support.microsoft.com/en-us/windows/-windows-activity-history-and-your-privacy-2b279964-44ec-8c2f-e0c2-6779b07d2cbd (дата звернення: 28.08.2025).