Цей програмний комплекс — якісний інструмент для моделювання руху транспортних засобів із метою візуальної наочної демонстрації певних етапів у розгортанні події або демонструванні результатів автотехнічної експертизи. До того ж корисним є його функціонал, що дає змогу використовувати під час моделювання супутникові знімки місцевості для відображення реальних дорожніх умов.

Перелік джерел посилання

1. CYBID V-SIM 4.0. Моделирование движения и столкновений автотранспортных средств. Руководство пользователя. Краков, 2018. Версия документа 1.0 (версия программы 4.0). Лицензия № 67D6D200.
2. Дубінін О. А. Використання ПЕОМ при моделюванні механізму ДТП : методичні рекомендації. Київ, 2007. 49 с.
3. Кристи Н. М. Методические рекомендации по производству автотехнической экспертизы. Москва, 1971. 112 с.
4. Судебная автотехническая экспертиза. Часть II. Теоретические основы и методики экспертного исследования при производстве автотехнической экспертизы : пособие для экспертов автотехников, следователей и судей / отв. ред. В. А. Иларионова. Москва, 1980. 392 с.

Журнали подій операційних систем *Windows* у комп'ютерно-технічній експертизі

Юрій Божко,
Сумський НДЕКЦ МВС України, м. Суми, Україна, e-mail: yuriybozhko93job@gmail.com

Досліджено журнали операційних систем сімейства Windows, наведено перелік типових журналів, які в ній існують, проаналізовано записи цих журналів, оцінено роль таких журналів у цифровій криміналістиці.

Ключові слова*: журнали подій; операційні системи; Windows; цифрова криміналістика; Event Logs; журнал безпеки; журнал системи; журнал додатків.*

Event Logs of Windows Operating Systems in Computer Technical Expertise

Yurii Bozhko

Logs of operating systems of the Windows family were studied; a list of typical logs that existing in is given; the records of these logs were analyzed; role of such logs in digital forensics is assessed.

Keywords*: event logs; operating systems; Windows; digital forensics; Event logs; security log; system log; application log.*

Цифрова криміналістика в сучасному світі технологій відіграє важливу роль у розкритті, розслідуванні та протидії злочинам, які відбуваються з використанням комп'ютерної техніки. Через популярність конкретних операційних систем вони можуть стати мішенню для зловмисників. Одними з найпопулярніших сьогодні є операційні системи сімейства *Windows*. Значну роль у розслідуванні кіберінцидентів і злочинів, у яких фігурує комп'ютерна техніка, відіграють журнали подій операційних систем, які в певному вигляді існують майже в кожній операційній системі.

У цифровій криміналістиці журнали подій можна використовувати для виявлення зловмисницької діяльності: аналіз журналів подій сприяє виявленню незвичної та підозрілої активності (наприклад, несподіваних входів, невдалих спроб доступу, зміни конфігурації системи тощо). Такі події можуть свідчити про можливі спроби несанкціонованого доступу або активність шкідливого програмного забезпечення. Також аналіз журналів подій допомагає встановити послідовність подій, що призвели до інциденту, і дає змогу відновити хронологію дій зловмисників. Журнали подій, зокрема, можна використати як докази в судових справах: для підтвердження або

спростування дій обвинувачуваних. Інформація із журналів подій також може допомогти відновити дії, які призвели до втрати даних або відмови системи.

Журнали подій в операційних системах *Windows* є системними інструментами, що реєструють різноманітні події, які відбуваються під час роботи комп'ютера й активності користувачів і додатків в операційній системі. Ці події можуть бути пов'язані із входами та виходами користувачів, змінами конфігурації системи, запуском програм, спробами вторгнень тощо. Журнали подій містять записи із деталями про час, тип події, джерело, результат і, подеколи, указівник на додаткові дані. Кожний тип події має так званий *Event ID* (ідентифікатор події), унікальний для кожного типу події.

Основні типи журналів подій містять: журнал безпеки (*Security*), відслідковування подій, пов'язаних із безпекою системи (як-от спроби входу, зміни прав доступу, видалення файлів тощо).

Розглянемо кілька записів журналу безпеки (*Security*).

```
Джерело: Microsoft-Windows-Security-Auditing.
Подія: 4624.
Опис: успішний вхід користувача.
Користувач: DOMAIN\Username.
Тип входу: 10 (Network).
Деталі: користувач увійшов через мережу.
```

У цьому записі зазначено, що користувач успішно ввійшов у систему. Цей запис містить інформацію про тип входу й іншу інформацію.

```
Джерело: Microsoft-Windows-Security-Auditing.
Подія: 4719.
Опис: змінено політику локальної безпеки системи.
Деталі: політику локальної безпеки змінено.
```

Цей запис свідчить, що змінено політику безпеки системи: або змінено налаштування паролів, або політику доступу, або інші зміни, пов'язані з доступом.

```
Джерело: Microsoft-Windows-Security-Auditing.
Подія: 4663.
Опис: доступ до об'єкта ресурсу було здійснено.
Об'єкт: C:\Documents\HBI Data.txt.
Деталі: користувач мав доступ для читання файлу.
```

У цьому записі зазначено, що користувач мав доступ для читання до файлу *HBI Data.txt* за шляхом *C:\Documents\ HBI Data.txt*. Цей запис дає змогу відстежити, хто й коли мав доступ до конкретного ресурсу.

Журнал системи (*System*). У цьому журналі реєструють події, які відбуваються на рівні операційної системи, як-от: завантаження, вимкнення, апаратні події та помилки, події ядра операційної системи, зміни в конфігурації обладнання та драйверів.

Розглянемо кілька записів журналу системи (*System*).

```
Джерело: Microsoft-Windows-Kernel-General.
Подія: 12.
Опис: система була успішно завантажена.
```

Цей запис свідчить, що операційна система була успішно завантажена (без помилок).

```
Джерело: Microsoft-Windows-Kernel-PnP.
Подія: 219.
Опис: додано новий апаратний драйвер для пристрою.
Деталі: драйвер \Driver\ExampleDriver.
```

У цьому записі зазначено, що був доданий новий апаратний драйвер для певного пристрою. Деталі включають шлях до драйвера.

```
Джерело: Microsoft-Windows-HardwareEvents.
Подія: 18.
Опис: виявлено помилку апаратної частини.
Деталі: помилка апарату – 0x0000000a (IRQ_NOT_LESS_OR_EQUAL).
```

Журнал додатків (*Application*). Журнал додатків реєструє інформацію про події, які відбуваються в програмах, установлених на комп'ютері. Сюди надходять повідомлення про помилки, інформація про стан і роботу програм та служб операційної системи.

Розглянемо кілька записів журналу системи (*System*) додатків (*Application*).

```
Джерело: Application Error.
Подія: 1000.
Опис: помилка запуску додатку.
Деталі: назва додатку – ExampleApp.exe; помилка – збій програми (0xc0000005).
```

Цей запис свідчить, що додаток *ExampleApp.exe* не вдалося запустити через помилку з кодом *0xc0000005*. Це може бути важливою інформацією для розв'язання проблеми із цим додатком.

```
Джерело: Application.
Подія: 1001.
Опис: додаток «ExampleApp.exe» був завершений.
Деталі: код виходу – 0.
```

У цьому записі зазначено, що додаток *ExampleApp.exe* був успішно завершений із кодом виходу 0. Ця подія може свідчити про нормальну роботу додатку.

```
Джерело: Application Error.
Подія: 1002.
Опис: помилка додатку «ExampleUIApp.exe».
Деталі: помилка додатку – збій у вікні додатку (0xc0000417).
```

Цей запис свідчить, що додаток з інтерфейсом користувача *ExampleUIApp.exe* відпрацював із помилкою з кодом *0xc0000417*. Цей запис може свідчити про проблеми зі співпрацею додатка із графічним інтерфейсом.

Журнали подій операційних систем *Windows* сукупно з іншими джерелами даних можуть надати дослідникові більш повну картину того, що відбувалося в системі. Вони дають криміналістам змогу не тільки виявляти кіберзлочини, а й розслідувати їх і протидіяти їм. В аналізі інцидентів, пов'язаних з інформаційною безпекою, журнали подій є цінним джерелом інформації для криміналістів та аналітиків, сприяючи виявленню, аналізуванню й розв'язанню проблем безпеки в інформаційних системах.

Докладний аналіз журналів Windows може стати незаперечним доказом у кримінальних справах, оскільки вони надають об'єктивну інформацію про дії підозрюваних. Правильно використаний журнал подій може підтвердити або спростувати алібі, засвідчити час і характер дій особи, а також установити зв'язки між різними суб'єктами у справі.

Перелік джерел посилання

1. Windows Event Log / Microsoft : веб-сайт. URL: https://learn.microsoft.com/en-us/windows/win32/wes/windows-event-log (дата звернення: 25.08.2023).
2. Event Viewer / Wikipedia : веб-сайт. URL: https://en.wikipedia.org/wiki/Event_Viewer (дата звернення: 25.08.2023).
3. Investigating Windows Event Logs / ArtiFast : веб-сайт. 28/06/2022. URL: https://forensafe.com/blogs/event_logs.html (дата звернення: 28.08.2023).
4. Koppolu N. R. Utilizing Event Logs of Windows Operating System in Digital Crime Investigations. *International Journal of Engineering Research & Technology (IJERT).* 2021. Vol. 10. Is. 7. DOI: 10.17577/IJERTV10IS070327 (дата звернення: 01.09.2023).