УДК 004.06; 343.98.06

ЖУРНАЛЫ СОБЫТИЙ WINDOWS КАК ЗНАЧИМЫЙ ИСТОЧНИК ЦИФРОВЫХ СЛЕДОВ

И.Б. Бурачёнок, канд. техн. наук, доц.,
Ф.П. Цыбульский, студент
Полоцкий государственный университет имени Евфросинии Полоцкой, Новополоцк, Беларусь

Проведено исследование структуры Windows XML EventLog (.evtx) формата. Выявлены встроенные утилиты Windows XML EventLog (.evtx), позволяющие различными способами извлечь информацию о внутренних элементах компьютерной системы Windows. Исследованы файлы-журналы Windows как криминалистически значимые артефакты и практически значимые источники цифрового следа.

Ключевые слова: *информационная безопасность, кибербезопасность, цифровой след, журналы событий, операционная система, структура файла, сигнатура файла, форензика.*

Введение. Повышение эффективности процессов установления доказательной базы является важной потребностью криминалистического следствия. В современных условиях злоумышленники часто прибегают к использованию электронно-цифровых устройств в планировании и совершении преступных деяний [1]. При ведении такого рода дел применяется анализ электронных информационных носителей и операционной системы на предмет наличия цифрового следа 2]. Так как самой популярной операционной системой (ОС) в нашей стране остаётся Microsoft Windows, то целесообразно на ее примере рассмотреть инструменты для ведения хронологического журналирования уведомлений системы и прикладного программного обеспечения. Журналы событий, генерируемые этими инструментами, содержат сведения о деятельности пользователя и системы в удобном формате данных. Таким образом, актуальность исследования журналов событий продиктована научной и практической значимостью при разработке новых программных решений, повышающих эффективность профессиональной деятельности специалистов в области кибербезопасности и форензики, что является актуальным на этапе цифровой трансформации в приоритетных отраслях экономики.

Основная цель исследования заключается в изучении структуры журнала событий Windows XML EventLog и хранимых в нём данных для выявления практической применимости артефактов при осуществлении криминалистической трасологии, как источника доказательной базы.

События Windows (Event Log) – системная служба, регистрирующая важные аппаратные и программные события, индексируемые ОС [3]. Поступающие от различных источников уведомления дифференцируются по коллекциям, соответствующим конкретной области ответственности – журналам событий.

Журнал событий представляет собой файл в формате Windows XML EventLog (.evtx). Большинство журналов событий хранятся по следующему адресу: %SystemRoot%\System32\winevt\Logs. Как цифровой след журнал можно рассматривать в качестве файлов-журналов, создаваемых программным обеспечением в процессе работы в соответствии с классификацией А.Н. Колычевой [4]. Для подробного исследования формата проведём побайтовый анализ файла “Microsoft-Client-LicensingPlatform%4Admin.evtx”. Шестнадцатеричный код файла был получен с помощью методов обратной разработки [5]. Формат журнала .evtx состоит из 2 частей: заголовка журнала и блоков записей. Далее рассмотрим эти части подробнее.

Заголовок файла представляет собой первые 4096 байт журнала. 8 байт по смещению 0 отвечают за цифровую подпись “ElfFile\x00”. Следующие 24 байта содержат номера первого и последнего блока и идентификатора записи, занимающие по 8 байт соответственно. 4 байта на смещении 32 хранят число 128 – размер активной заголовочной части. На смещении 36 видим два сегмента по 4 байта, содержащие версии формата. Следующие 2 байта содержат число 4096 – размер сегмента заголовка файла. Еще 2 байта хранят количество блоков записей. На смещении 124 находится сегмент, занимающий 4 байта и хранящий контрольную сумму CRC32, состоящую из первых 120 байтов. Последующие 3968 байт представляют собой заполняющие нулевые значения. Визуально структура заголовочного файла показана на рисунке 1.

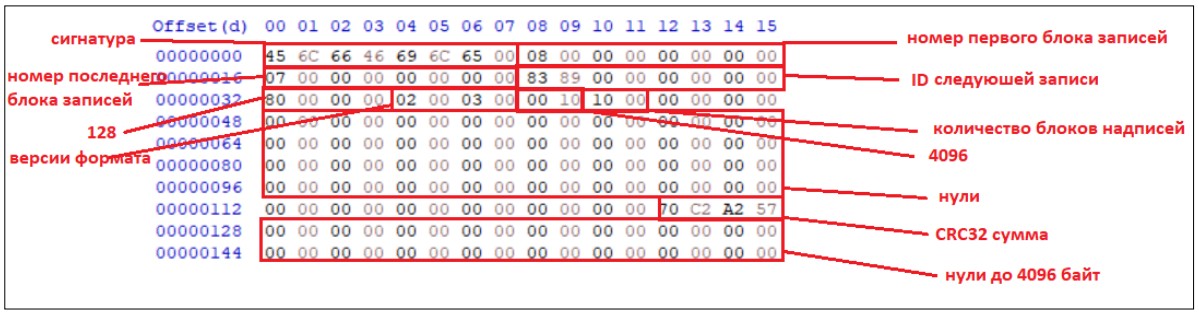

Рисунок 1. – Структура заголовка формата .evtx

Начиная со смещения 4096 байт создаются блоки записей (сегменты памяти, занимающие 65536 байт). Блок начинается с подписи, длинной 8 байт “ElfChnk\x00”. Блок состоит из 2 частей: заголовка и записях событий. Исследуем их подробнее.

Заголовок блока занимает первые 512 байт и несет функцию хранения технической информации и параметров для соответствующего блока. По смещению 8 относительно начала блока по 40-й байт находятся разделенные по 8 байт значения номеров первой и последней содержащейся записи, а также их идентификаторы. По смещению 40 находится сегмент 4 байт, содержащий размер заголовка, равный 128. На 44 позиции находятся два сегмента по 4 байта, содержащие указатели на конец и начало блока. На 52 смещении расположена ячейка контрольной суммы CRC32 размером 4 байт. Сумма собрана на основе байтов записей событий. 68 байт хранят флаги и параметры для блока записей. Следующие 4 байт заняты контрольной суммой CRC32 заголовочной части, собранной на основе 120 байтов по смещениям 128 и 512. Следующие 256 байт

по смещению 128 содержит массив смещений общей строки. Визуально структура заголовка блока показана на рисунке 2.

Запись события имеет переменный размер. Началу записи соответствует сигнатура “\x2a\x2a\x00\x00”. 4 байт содержат значение размера записи, начиная со смещения сигнатуры. 8 байт содержат ID записи события, еще 8 байт отвечают за хранение даты создания записи в формате FILETIME. По смещению 24 относительно начала записи содержится XML. Завершают запись 4 байта, копирующие значение размера. При наличии не задействованной памяти, она заполняется байтами (Hex\x00).

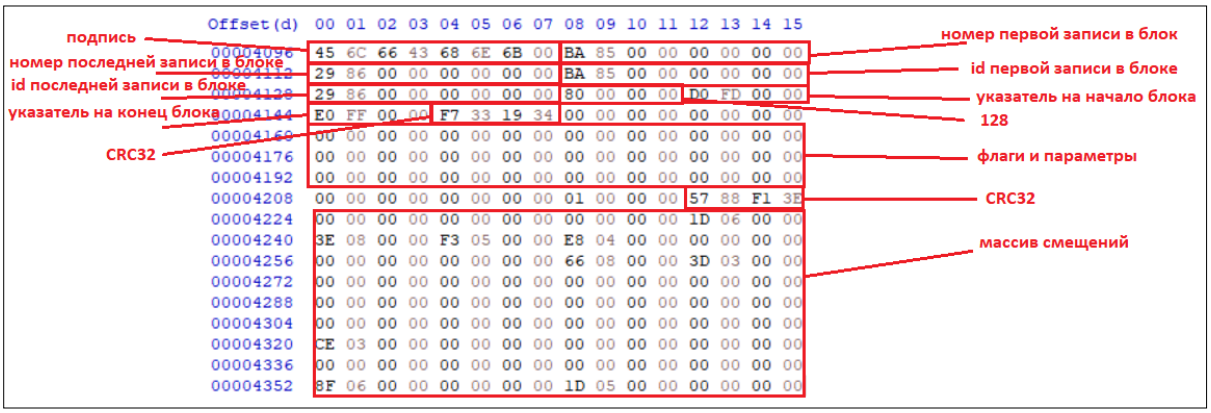

Рисунок 2. – Структура заголовка блока записей

XML структура данных содержит следующие атрибуты:

– идентификатор события (EventID) – занимает 4 байта и представляет собой объединение кода события и средства (28 бит), 1 бит зарезервирован системой и двух флагов – флага использования (1 бит) и флага серьезности (2 бит). Изучим первую запись исследуемого журнала. Первые 16 бит занимает число 101 – код события. 12 бит соответствуют значению facility. 1 бит зарезервирован системой. Еще 1 равен 0, что определяет системное событие. Последние 2 бита определяет уведомляющий характер.

– уровень события (Level) – занимает 1 байт и представляет собой флаг, определяющий серьезность события. Значение используется для предотвращения переполнения журнала. В нашем случае этот флаг соответствует уровню 4;

– **ключевые слова** (Keywords) – занимает 8 байт и представляет собой числовой флаг, определяющий то, в какие журналы следует занести событие. Зарезервирован системой и связан с конкретными журналами на локальном носителе. Нашему примера соответствует следующий keyword: 0x2000000000000001 (Service Keyword);

– дополнительные параметры, зависящие от типа уведомления. Событие может содержать ссылки на внешние ресурсы, пути, или значения.

Абстрагированность формата от стандартных утилит поощряет внедрение и разработку новых решений для анализа журналов событий, что определяет практическую значимость в криминалистике и форензике. Анализ содержимого журналов позволяет восстанавливать хронологические цепочки деятельности пользователя, приложений, а также аппаратной части цифрового устройства.

Настройки хранения, управления и содержимого журналов событий находятся в иерархической базе данных параметров Windows – реестре. Путь реестра для службы журналов – “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog”.

Для осуществления обработки данных с помощью утилиты “reg” возможно скопировать подразделы на информационный носитель со следующими параметрами: red export [ветка реестра]. В пользовательской директории сгенерируется документ Events с расширением реестра (.reg). Содержимое файла показано на рисунке 3.

Файл Events.reg имеет следующую структуру: элементы реестра разделены пустыми строками, первая строка элемента содержит адрес ветви, по которому хранится элемент. Следующие за ним строки содержат параметры в формате «ключ-значение». Криминалистический анализ содержимого этого файла даст представление о существующих журналах событий, что является значимым цифровым следом.

Рисунок 3. – Структура файла Events.reg

Выводы. По результатам исследования структуры формата Windows XML EventLog и анализа содержимого журнала событий как источника цифрового следа можно сделать вывод, о том, что журналы Windows имеют критическое значение для криминалистического следствия и практическую применимость в расследовании преступных деяний с использованием элементов электронно-цифровых устройств. Разработка и внедрение новых решений при анализе журналов Windows и цифрового следа позволят специалистам по кибербезопасности и юриспруденции эффективно формировать доказательную базу.

ЛИТЕРАТУРА

1. МВД: число преступлений с использованием IT-технологий выросло на 23,5% (vedomosti.ru) [Электронный ресурс]. – Режим доступа: https://www.vedomosti.ru/society/news/2024/04/08/1030570-chislo-prestuplenii-s-ispolzovaniem-it-tehnologii-viroslo. – Дата доступа: 25.10.2024.
2. Нестеров, С.А. Понятие цифрового следа и анализ цифрового следа в образовании. / С.А. Нестеров, Е.М. Смолина // SAEC. 2023. №3. [Электронный ресурс]. – Режим доступа: URL: https://cyberleninka.ru/article/n/ponyatie-tsifrovogo-sleda-i-analiz-tsifrovogo-sleda-v-obrazovanii.– Дата доступа: 24.10.2024.

3. Ведение журнала событий (установщик Windows) [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru-ru/windows/win32/msi/event-logging.– Дата доступа: 24.10.2024.
4. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук: 12.00.12 / А.Н. Колычева. – Москва, 2019. – С. 25.
5. Eilam Eldad. Reversing: secrets of reverse engineering. – John Wiley & Sons, 2005. –– P. 595. – ISBN: 0-7645-7481-7.