УДК 004.06; УДК 343.98.06

ИНФОРМАЦИОННЫЕ АРТЕФАКТЫ ЦИФРОВОГО СЛЕДА В КОМПЬЮТЕРНОЙ СИСТЕМЕ

Ф. П. ЦЫБУЛЬСКИЙ
(Представлено: канд. техн. наук, доц. И. Б. БУРАЧЁНОК)

Рассмотрены способы выявления цифрового следа в компьютерной системе на внешних и внутренних носителях памяти. Исследованы информационные артефакты и утилиты, автоматизирующие процесс выявления, фиксации и анализа цифрового следа. Выявлены наиболее ценные информационные артефакты позволяющие восстановить деятельность пользователя и (или) программного обеспечения в компьютерной системе.

Ключевые слова: *информационная безопасность, цифровой след, компьютерная система, кибербезопасность, киберпреступления, форензика, информационный артефакт.*

Введение. С каждым годом число планируемых или совершенных неправомерных действий с помощью средств информационно-компьютерных технологий увеличивается. В 2024 году подтвержденных хакерских атак в крупных IT-компаниях было зафиксировано на 30% больше, чем за предыдущий [1]. Правоохранительным органам приходится расследовать преступления в области цифровых технологий постфактум, при этом возникают трудности в процессах фиксации и установлении доказательной базы. Поэтому процесс ведения следствия противозаконной деятельности совершенной или планируемой с применением электронно-цифровых устройств предполагает вовлечение не только специалистов в области права, но и в области технических наук, в том числе кибербезопасности. Только квалифицированный специалист в сфере информационной безопасности может провести процесс изъятия и исследования носителей цифровой информации на предмет наличия ценных для следствия цифровых следов (ЦС).

Таким образом, процесс эволюции и усложнение компьютерных систем (КС), повлекли за собой необходимость в исследовании существующих способов выявления цифрового следа в КС, методов их фиксации и анализа, а также разработку новых, что несомненно является **актуальной задачей**.

Основная цель представленной работы – исследование ценных информационных артефактов, которые позволяют восстановить деятельность пользователя и (или) программного обеспечения (ПО) в компьютерной системе, а также способы фиксации и анализа цифровых следов.

Компонентами, представляющими интерес в указанной предметной области, являются внешние носители информации, такие как Solid-State Drive (SSD) и Hard Disk Drive (HDD). Особую важность для анализа представляют слепки внутренней энергозависимой памяти, такой как Random Access Memory (RAM). Криминалистически значимыми ЦС могут считаться документы, записи систем, почтовые отправления и так далее. Для структуризации ЦС была выбрана классификация А.Н. Колычевой [2], в которой выделяют 7 групп цифровых следов.

Первая группа – *файлы системного и прикладного программного обеспечения.* Данная группа включает в себя информацию об установленного на носителе системного и прикладного ПО. Например, как показано на рисунке 1, для КС под управлением Windows 10 можно получить перечень индексируемых программ с помощью графического пользовательского интерфейса или стандартной утилиты "Windows Management Instrumentation Command" (wmic).

```
C:\Users\username>wmic product get name,version
Name
Python 3.12.5 Standard Library (64-bit)
Python 3.12.5 Executables (64-bit)
Python 3.12.5 Tcl/Tk Support (64-bit)
CA AllFusion Process Modeler r7
Python 3.12.5 Core Interpreter (64-bit)
```

Рисунок 1. – Демонстрация работы утилиты "wmic"

Вторая группа – *файлы конфигурации программных приложений и операционных систем (ОС).* Если рассматривать ОС Windows, то она имеет иерархическую базу данных параметров – реестр. Наиболее информативным для выявления ЦС является набор пользовательских и системных настроек, представленных в следующих разделах реестра:

1 "HKEY_CURRENT_USER" (HKCU) [3] – ветвь реестра, содержащая конфигурации конкретной учетной записи пользователя. Получение доступа к ней позволяет построить портрет пользователя по следующим подразделам: "HKCU\SOFTWARE" – список индексируемого для конкретного пользователя ПО, "HKCU\AppEvents" – ключи индексируемых ОС реакций на определенные системные и прикладные события. Ветви хранятся локально в файле ntuser.dat по пути "C:\Users\[user_name]".

2 "HKEY_LOCAL_MACHINE" (HKLM) [3] – конфигурации системы, устройств и драйверов, используемых всеми пользователями системы. "HKLM\CurrentControlSet\Control\TimeZoneInformation" – данные о временных поясах системы, которые могут быть полезны для установления времени обработки критических исключений. "HKLM\System\CurrentControlSet\Services" – сведения о подключенных сервисах.

Среди сервисов особую криминалистически важную информацию могут предоставить следующие сервисы: Background Activity Moderator (BAM) – сервис, контролирующий активность фоновых программ, хранящий список записей SID с исполняемыми файлами в реестре по адресу "HKLM\SYSTEM\ControlSet00x\Services\bam" и EventLog – ключи службы ведения журналов-событий, записанные по пути реестра "HKLM\SYSTEM\ControlSet00x\Services\EventLog".

Конфигурации драйверов – безусловно важные ЦС, представляющие собой раздел "HKLM\SYSTEM\DriverDatabase". Компонент ShimCache (AppCompatCache) обеспечивает обратную совместимость старых приложений и добавляет исполняемые файлы, индексируемые системой в ShimCache. AppCompatCache записывает название исполняемого файла, путь к файлу и дату последнего изменения файла. Ключи конфигурации AppCompatCache и пути к журналу хранятся в предоставленном реестром разделе: "HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache".

Служба автозапуска не хранит все наборы ключей в одном месте, они представлены в нескольких ветвях реестра. Каждая такая ветвь содержит приписку "run", например: "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" или "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce". Прикладное ПО может создавать свои ветки реестра динамически, изменяя и дополняя ключи. Приведенный перечень директорий, представляющих интерес для специалиста по кибербезопасности не полный, рассмотренные ветви отображены на рисунке 2.

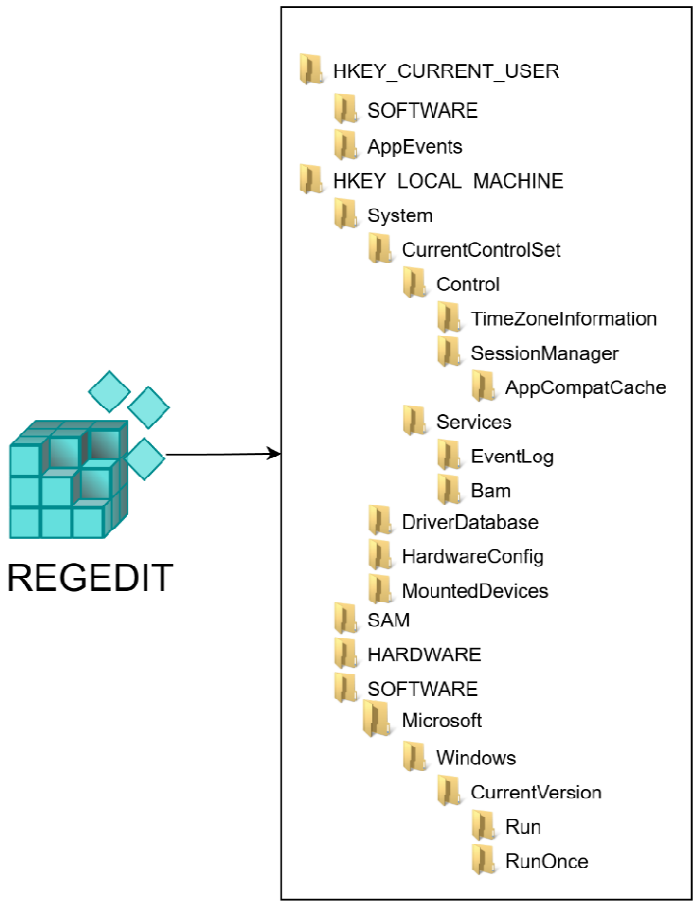

Рисунок 2 – Анализируемые директории реестра

С целью анализа автоматического анализа базы данных ключей разработаны приложения, базирующиеся на этой задаче. Для примера возьмем FastIR Collector [4], который делает выборку разделов реестра на ЦС и сохраняет результат в .json или .csv формат. Обращаться к коллекции значений также возможно через консольный пакет Regedit. Экспортирование значений в текстовый формат (рисунок 3) происходит через команду, она выглядит так: Regedit /e.

```
[HKEY_LOCAL_MACHINE\BCD00000000]

[HKEY_LOCAL_MACHINE\BCD00000000\Description]
"KeyName"="BCD00000000"
"System"=dword:00000001
"TreatAsSystem"=dword:00000001
"GuidCache"=hex:92,52,21,07,05,c1,d9,01,0b,27,00,00,6b,6d,8f,da,b4,e6,29,25,ac,\
  00,00,00
```

Рисунок 3. – Демонстрация работы команды Regedit /E /A [targetFile]

Третья группа – *файлы-журналы, создаваемые программным обеспечением в процессе работы.* Для примера возьмем ОС Windows. Стандартными путями, по которым располагаются файлы-журналы программного обеспечения считаются "C:\ProgramData" и "C:\Users\[user_name]\AppData", однако не редки исключения. Примером файла-журнала являются отчеты программы Windows Defender, они хранятся по адресу "C:\ProgramData\Microsoft\Windows Defender\Support" и имеют расширение .log. Защитник записывает информацию о проверенных процессах, фиксирует ошибки анализа и причину остановки. Отчет проверки процессов MPlog%Date%.log (рисунок 4) содержит в себе название исполняемого процесса, его Pid и путь к проверяемому файлу, а также время начала и конца проверки.

```
2024-07-02T02:40:49.560Z ProcessImageName: Discord.exe, Pid: 15236, TotalTime: 57076, Count: 8628, MaxTime: 31,
2024-07-02T02:40:49.560Z ProcessImageName: steam.exe, Pid: 12840, TotalTime: 50522, Count: 7113, MaxTime: 578,
2024-07-02T02:40:49.560Z ProcessImageName: opera.exe, Pid: 15792, TotalTime: 23889, Count: 4581, MaxTime: 296,
2024-07-02T02:40:49.560Z ProcessImageName: steamwebhelper.exe, Pid: 14928, TotalTime: 17805, Count: 3332, MaxTime: 15,
2024-07-02T02:40:49.560Z ProcessImageName: opera.exe, Pid: 15972, TotalTime: 13325, Count: 2186, MaxTime: 125,
2024-07-02T02:40:49.560Z ProcessImageName: ArmouryCrate.UserSessionHelper.exe, Pid: 6632, TotalTime: 12559, Count: 1938,
2024-07-02T02:40:49.560Z ProcessImageName: ArmouryCrate.UserSessionHelper.exe, Pid: 23256, TotalTime: 9318, Count: 1263,
2024-07-02T02:40:49.560Z ProcessImageName: explorer.exe, Pid: 20328, TotalTime: 8531, Count: 120, MaxTime: 3703,
2024-07-02T02:40:49.560Z ProcessImageName: cs2.exe, Pid: 20952, TotalTime: 7302, Count: 1067, MaxTime: 250, MaxTimeFile:
2024-07-02T02:40:49.560Z ProcessImageName: Agent.exe, Pid: 18780, TotalTime: 6451, Count: 1208, MaxTime: 31, MaxTimeFile
```

Рисунок 4. – Содержимое MPlog%Date%.log

ЦС, генерируемое функционалом фиксирования событий файловой и ОС, называют журналом событий. По умолчанию они содержаться по адресу "%SystemRoot%\System32\winevt\Logs" и имеют расширение .evtx. Журналы строго разделяются по назначению и сфере ответственности. Например, файл "Microsoft-Windows-GroupPolicy%4Operational.evtx" хранит записи о сеансах групповой политики, о изменениях и модификации таковой. Функционал работы с журналами событий допускается расширять при использовании утилиты "System Monitor" (Sysmon). А управление записями возможно осуществлять через терминал, прибегая к утилите "Wevtutil". Во многих ОС существует система фиксации изменений на съемном носителе. Для примера, ОС Windows 10 управляет журналами Update Sequence Number (USN) – внутренними системными списками файлов New Technology File System (NTFS). USN хранит информацию об изменениях данных на конкретном носителе с данной файловой системой. Новая информация записывается в конец потока журнала. Для каждого тома создается изолированный USN-журнал. Управление журналами USN осуществляется через консольную утилиту File System Utility (fsutil), как показано на рисунке 5, а функционал подробного анализа артефакта предоставляется сторонним ПО "NTFS USN Journal Parser" [5].

Сервис Windows Prefetch собирает информацию с помощью перехвата исполняемого файла и библиотек, с предварительно выделенным пространством на накопителе. При запуске исполняемого файлы по адресу "%SystemRoot%\Prefetch" создается файл с расширением Prefetcher (.pf). Он содержит список ресурсов, на которые ссылается исполняемый файл, включая файлы и каталоги. Анализ и чтение отчета Prefetch может быть осуществлен с помощью сторонних программ, таких как "WinPrefetchViewer" [6].

```
C:\Users\username>fsutil usn
---- Поддерживаемые команды USN ----

createJournal           Создает журнал USN
deleteJournal           Удаляет журнал USN
enableRangeTracking     Включает отслеживание диапазона записи для тома
enumData                Перечисляет данные USN
queryJournal            Запрашивает данные USN для тома
readJournal             Читает записи USN из журнала USN
readData                Читает данные USN для файла
```

Рисунок 5. – Функционал утилиты "fsutil usn"

При обработке критических ошибок в ОС Windows создаются слепки памяти, содержащие таблицы запущенных процессов, их Pid, адреса памяти и другую информацию. Наиболее интересны 3 вида создаваемых слепков: Minidump (до 256 КБ) хранится по адресу "%SystemRoot%\Minidump", kernel crash dump и Completely memory dump по пути "%SystemRoot%". Эти слепки содержат полную информацию о протекающих процессах и состоянии ядра КС. ПО Windows Debugger (WinDBG) позволяет анализировать дампы памяти.

Стоит отметить имеющиеся автоматизированные инструменты по поиску ЦС на носителях. Например, Kroll Artifact Parser and Extractor (KAPE) [7] широко применяется в форензике [3]. KAPE исследует носитель на предмет наличия артефактов, экономя время на этапах расследования. Belkasoft X Forensic [8] – аналог, который помимо функционала поиска, имеет удобные инструменты анализа ЦС.

Четвертая группа – *источники информации, образующиеся в ходе деятельности пользователя, в том числе их резервные копии и удаленные файлы*. Помимо самих файлов, метаданные фотографий, документов и файлов – ценная информация для специалиста в кибербезопасности. К метаданным относится информация о технических характеристиках файлов, о любой манипуляции с ним, а также периферийных описательных данных. Получить основные параметры файлов возможно с помощью графического интерфейса Windows, а более подробный анализ осуществляется с помощью предлагаемого программного обеспечения с открытым исходным кодом FOCA [9].

С целью работы с зашифрованными контейнерами информации можно предложить для применения следующие утилиты: Encryption Analyzer [10] – представляет инструменты по поиску зашифрованных документов на съемном носителе и подробную информацию, включая методы защиты и шифрования, а также ПО John the Rippe [11], позволяющий экспортировать файлы из защищенного архива .rar и .zip форматов.

Файловая система NTFS, как и многие другие, не зануляют сектора удаляемого контента на носителе, только теряет точку входа к нему из таблицы доступа тома. Недавно удаленную информацию можно восстановить с некоторым шансом. Такие программы как "RecuperaBit" считывают двоичную информацию с носителя без привязки к таблице томов и по сигнатурам известных форматов файлов восстанавливает утраченную информацию.

Пятая группа – *файлы, обеспечивающие аутентификацию и конфиденциальность пользователей.* Зачастую пароли от учетных записей, криптоконтейнеров или зашифрованных файлов служат ключевыми по значимости артефактами для следователя, так как открывают путь к тому, что хотят скрыть от посторонних глаз. Такая информация тщательно скрывается и может быть обнаружена в процессе поиска других групп данных. Основными точками интереса служат менеджеры паролей, такие как "KeePass" и базы данных систем. В ОС Windows 10 существует компонент Security Account Manager (SAM) – база данных Windows, содержащая учетные записи пользователей, включая имена и хешированные пароли. Получить доступ к SAM возможно через реестр по пути "HKEY_LOCAL_MACHINE\SAM" или по пути файловой системы "C:\Windows\System32\config\SAM".

Шестая группа – *информация, находящаяся в оперативной памяти или файле подкачки устройства.* Работа с внутренней энергозависимой памятью сопровождается трудностями. К ней не всегда удается получить прямой доступ в том же состоянии, как и в начале процесса изъятия. Для работы с Random Access Memory (RAM) необходимо предварительно создать слепок состояния [12]. Особенность RAM в том, что информацию она хранит не цельно, а по фрагментам. ПО Belkasoft live Ram Capturer [13] позволяет снимать слепки RAM памяти, при этом обходя защиты антидампинговых систем. Набор утилит Volatility [14] анализирует созданные ранее дампы памяти на предмет цифровых следов.

Седьмая группа – и*нформация, полученная с помощью соответствующих радиоэлектронных или специальных технических средств.* Выбор технического средства зависит от поставленной перед специалистом задачей. Для перехвата сетевого трафика используются роутеры-анализаторы с установленным

ПО, таким как WireShark [15] или System for Internet-Level (SiLK) [16]. Задача слежения за пользователем решается с помощью устройства "KeyGrabber". Для разворачивания и анализа поведения вредоносного ПО используются различные комплексы технических средств, создающие изолированную отслеживаемую программную среду. Для каждого случая может быть необходимо наличие уникального инструментария специалиста цифровой криминалистики.

Вывод: В представленной статье приведен далеко не полный перечень способов фиксации ЦС, однако любая активность в цифровом пространстве оставляет следы и приведенные в статье способы выявления цифровых следов в компьютерной системе позволяют специалистам информационной безопасности и юриспруденции эффективно решать проблему сбора данных (фиксации ЦС), их анализа и создавать более гибкие методики ведения криминалистического следствия. Приведенные в статье информационные артефакты и утилиты позволяют автоматизировать процесс выявления, фиксации и анализа цифрового следа, а также решать вопросы защиты информационных ресурсов.

ЛИТЕРАТУРА

1. Эксперты по кибербезопасности отмечают рост скорости взлома крупных компаний (kommersant.ru) [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/66918907tg. – Дата доступа: 18.08.2024.
2. 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.
3. Muhibullah, M. Windows Forensics Analyst Field Guide. Packt publishing, 2023. – 318 с.
4. Soft-Fastir Collector – Author Sébastien Larinier | Форум информационной безопасности – Codeby.net [Электронный ресурс]. – Режим доступа: https://codeby.net/threads/fastir-collector-author-sebastien-larinier.67056/. – Дата доступа: 18.09.2024.
5. NTFS USN Journal – E5h Forensic Solution Viewer. [Электронный ресурс]. – Режим доступа: https://e5hforensics.com/index.php/downloads/software/ntfs-journal-viewer/. – Дата доступа: 16.09.2024.
6. WinPrefetchView – Nir Sofer. [Электронный ресурс]. – Режим доступа: https://www.nirsoft.net/utils/win_prefetch_view.html. – Дата доступа: 16.09.2024.
7. Kroll Artifact Parser and Extractor – Cyber Risk. [Электронный ресурс]. – Режим доступа: https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape – Дата доступа: 16.09.2024.
8. Belkasoft X Forensic – Belkasoft. [Электронный ресурс]. – Режим доступа: https://www.belkasoft.com. – Дата доступа: 16.09.2024.
9. FOCA – Informatica64. [Электронный ресурс]. – Режим доступа: https://foca.softonic.ru – Дата доступа: 16.09.2024.
10. Encryption Analyzer – Passware. [Электронный ресурс]. – Режим доступа: https://www.passware.com/encryption-analyzer/ – Дата доступа: 17.09.2024.
11. John the Rippe – Openwall. [Электронный ресурс]. – Режим доступа: https://www.openwall.com/john/ Дата доступа: 17.09.2024.
12. Пантюхин, И.С. Снижение объема обрабатываемой информации в энергозависимой памяти при исследовании компьютерных инцидентов. / И.С. Пантюхин, Н.И. Белов, В.А. Катаева // Вопросы кибербезопасности, 2018. – №2(26), С.70-76.
13. Belkasoft live Ram Capturer – Belkasoft. [Электронный ресурс]. – Режим доступа: https://www.belkasoft.com. – Дата доступа: 16.09.2024.
14. Volatility – The Volatility Foundation. [Электронный ресурс]. – Режим доступа: https://volatilityfoundation.org. – Дата доступа: 16.09.2024.
15. WireShark – Endace. [Электронный ресурс]. – Режим доступа: https://www.wireshark.org. – Дата доступа: 16.09.2024.
16. SiLK – CERT NetSA. [Электронный ресурс]. – Режим доступа: https://tools.netsa.cert.org/silk/. – Дата доступа: 16.09.2024.