Научная статья
УДК 343.148.6
doi 10.46741/2713-2811.2023.24.4.012

Установление факта запуска программного обеспечения в операционной системе Windows при помощи криминалистического анализа Prefetch-файлов

АРТЕМ ВЯЧЕСЛАВОВИЧ БЕЛЕЙ

Российский государственный университет правосудия, Москва, Россия, a.beley@facct.ru

Аннотация. В статье рассматривается актуальность исследования файлов трассировки, в частности Prefetch-файлов, в рамках содействия расследованию преступлений в условиях цифровой трансформации. Поднимается проблема необходимости введения обязательной инструкции к анализу Prefetch-файлов с учетом специфики работы с электронными носителями информации. Объясняется значимость таких файлов как источника криминалистически значимой информации при условии использования специализированного программного обеспечения для его исследования. Рассмотрена методика использования программного обеспечения при проведении экспертизы.

Ключевые слова: файл трассировки; Prefetch-файл; цифровая криминалистика; «PECmd»; парсер; временные метки; факт запуска; программное обеспечение; криминалистическое исследование жесткого диска; судебная компьютерно-техническая экспертиза.

5.1.4. Уголовно-правовые науки.

Для цитирования: Белей А. В. Установление факта запуска программного обеспечения в операционной системе Windows при помощи криминалистического анализа Prefetch-файлов // Ius publicum et privatum: сетевой научно-практический журнал частного и публичного права. 2023. № 4 (24). С. 111–121. doi 10.46741/2713-2811.2023.24.4.012.

Original article

Establishing the Fact of the Software Start in the Windows Operating System with the Help of Forensic Analysis of Prefetch files

ARTEM V. BELEI

Russian State University of Justice, Moscow, Russia, a.beley@facct.ru

Abstract. The article discusses the relevance of the study of trace files, in particular Prefetch files, in the framework of assisting the investigation of crimes in

the context of digital transformation. The problem of the need to introduce mandatory instructions for analyzing Prefetch files, taking into account the specifics of working with electronic media, is raised. The relevance and importance of such files as a source of criminally significant information is explained, provided that specialized software is used for its research. The methodology of using software in conducting expert research is considered.

Keywords: trace file; Prefetch file; digital forensics; “PECmd”; parser; timestamps; launch fact; software; forensic examination of the hard disk; forensic computer technical expertise.

5.1.4. Criminal law sciences.

For citation: Belei A.V. Establishing the fact of the software start in the Windows operating system with the help of forensic analysis of Prefetch files. *Ius publicum et privatum: online scientific and practical journal of private and public law*, 2023, no. 4 (24), pp. 111–121. doi 10.46741/2713-2811.2023.24.4.012.

Постоянное развитие и активное распространение коммуникационных систем, информатизация и автоматизация различных общественных процессов и активное внедрение Интернета вещей (IoT) уже давно стали неотъемлемым атрибутом существования нашего государства и общества. Однако стремительное совершенствование в данной области формирует необходимую среду для роста преступности, основной вектор которой представляет собой финансово мотивированные противоправные действия в отношении физических и юридических лиц и приводит к существенному материальному ущербу. В современных условиях многие геополитические конфликты и разногласия влекут за собой повышенный фон активной киберпреступной и диверсионной деятельности, направленной на объекты критической инфраструктуры и отдельных лиц. Действия, осуществляемые злоумышленниками в ходе совершения противоправных действий в отношении таких систем, находят в них или на отдельных электронных носителях информации свое отражение в качестве электронно-цифровых следов.

В условиях цифровой трансформации существенная часть преступлений совершается с применением IT-технологий. Так, за январь–июль 2023 г. киберпреступлений зарегистрировано на 27,9 % больше, чем за семь месяцев прошлого года. Подобная динамика сохраняется и в настоящее время [1].

Стоит отметить, что часто и классические преступления, которые напрямую не связаны с киберпреступностью, совершаются с косвенным и прямым применением компьютеров, смартфонов, планшетов, умных часов и иных высокотехнологичных устройств. Такие устройства нередко становятся объектами исследования в рамках расследования преступлений и в частности объектами судебной компьютерно-технической экспертизы (СКТЭ).

Кибепреступники все чаще используют более сложные техники и тактики для сокрытия следов преступных деяний. Поэтому данный факт напрямую влияет на показатели раскрываемости преступлений с применением IT-технологий, а также на количество времени, которое требуется субъекту, обладающему специальными знаниями, для осуществления содействия расследованию, эксперту при подготовке его заключения или сотруднику оперативно-технического подразделения при осуществлении оперативно-розыскных мероприятий (ОРМ).

Существует огромное количество случаев, когда в операционной системе (ОС) компьютера может остаться криминалистически значимая информация в виде электронно-цифровых следов. Учитывая, что основная масса таких преступлений совершается с применением злоумышленниками вредоносного программного обеспечения (ВПО) или соотносится с запуском приложения или программы для открытия электронных документов на личных устройствах, то одной из самых распространенных задач, с которыми в рамках своей работы может столкнуться эксперт СКТЭ или сотрудник оперативного подразделения, остается определение факта запуска программного обеспечения (ПО). При этом стоит помнить, что необходимость установления данного факта не соотносится только со ст. 273 УК РФ. Такая информация (например, наличие определенного электронного документа в файловой системе (ФС), осуществление интернет-сессии при помощи приложения с определенного устройства в определнное время, точное время и дата запуска и т. д.) может как напрямую отвечать на поставленный перед субъектом исследования вопрос о запуске той или иной программы на персональном компьютере, так и позволить в некоторых случаях осуществить атрибуцию преступной группировки, а также косвенно повлиять на поиск необходимой информации для ответа на иные вопросы в рамках расследования классических видов преступлений. Помимо этого, в ходе исследования фактов, которые необходимы для подтверждения запуска, может быть обнаружена и другая значимая информация, которая способна оказать влияние на ход дела. Таким образом, практическая применимость исследования факта запуска ПО касается не только преступлений в сфере компьютереной информации, но и любых других, где может фигурировать электронный носитель информации с установленной ОС как объект исследования.

В условиях недостаточности практических научных разработок и методических рекомендаций в области электронно-цифровых следов и компьютерной криминалистики многим специалистам бывает затруднительно работать с тем или иным объектом исследования или в некоторых случаях использовать альтернативные источники криминалистически значимой информации. Последнее зависит от обилия дистрибутивов ОС, а также от их постоянного обновления, программных и конструктивных (в случае электронных носителей информации) особенностей. Кроме того, данный факт влияет и на процесс получения академических знаний студентами, проходящими программы подготовки по соответствующим специальностям.

В настоящее время 69,26 % пользователей персональных компьютеров пользуются ОС «Windows» [2]. Исходя из этой информации, можно сделать вывод, что на практике субъект исследования чаще всего может столкнуться именно с этой ОС, что в свою очередь свидетельствует о том, что в ходе проведения исследования ему понадобятся знания и навыки работы с электронно-цифровыми следами именно на этой системе. Соответственно, для решения наиболее распространенной задачи по определению факта запуска ПО субъекту исследования придется проводить анализ артефактов запуска. ОС «Windows» отличается тем, что в ней существует ряд дублирующих друг друга по информации артефактов, однако для определения факта запуска ПО одним из самых надежных источников является Prefetch-файл.

Учитывая указанные выше факты, определяющие актуальность данной статьи, а также отсутствие научной криминалистической информации в широком доступе,

для повышения эффективности работы оперативных подразделений правоохранительных огранов и экспертов СКТЭ, а также для формирования научно-практической и теоретической базы для обучающихся по соответствущим специальностям предлагается сформировать методические рекомендации по работе с Prefetch-файлами с теоретической информацией и полным описанием процесса исследования.

ОС «Windows» создает Prefetch-файлы при первом запуске приложения из каталога, которые в дальнейшем используются для ускорения загрузки приложения. Prefetch-файлы хранятся в каталоге %SystemRoot%\Prefetch. Однако существуют и альтернативные источники. Ими могут служить теневые копии виртуальных машин «.vss», если нет возможности примонтировать виртуальную машину, или дампы оперативной памяти, из которых также можно получить Prefetch-файлы при помощи специализированного ПО, например «Volatility Framework» [3]. Данные файлы появились впервые в ОС «Windows XP» и присутствуют в последующих версиях. Изначально в ОС «Windows XP», «Windows Vista», «Windows 7» максимальное количество Prefetch-файлов составляло 128. Позже, начиная с ОС «Windows 8» их число было увеличено до 1024. Исходя из этого, можно отметить, что даже если система не переустанавливалась, то при активном использовании разных приложений не представляется возможным получить информацию обо всех когда-либо установленных приложениях. Это объясняется тем, что как только лимит Prefetch-файлов превышается, самый старый из них удаляется и освобождает место новому. Таким образом, само наличие Prefetch-файлов уже говорит о факте запуска ПО.

Принцип работы Prefetch-файла объясняет его ценность для эксперта СКТЭ. Его суть состоит в том, что данный файл осуществляет мониторинг в первые 10 секунд работы программы и записывает данные о времени последнего запуска, подключаемых библиотеках, файлах и каталогах. 10 секунд – это максимальное значение, в случае если программа не требует большого количества ресурсов ОС при запуске, то данное число может быть и меньше. Злоумышленники также знают об этом и иногда используют один из методов сокрытия следов путем отложенного старта программы, когда она первые 10 секунд не обращается к файлам или каталогам, что снижает количество потенциально криминалистически значимой информации [4].

Стоит отметить, что Prefetch-файлы по умолчанию включены для пользовательских версий операционной системы. Для версий ОС, созданных для серверов, они изначально выключены. Исходя из этого факта, описанная ниже методика исследования таких файлов актуальна при работе с ОС «Windows XP», «Vista», «7», «8», «8.1», «10» и «11» версии, а при работе с ОС «Windows Server» следует полагаться на другие артефакты. Также стоит отметить, что в случае установки ОС «Windows» на твердотельные накопители Prefetch-файлы тоже выключены.

Prefetch-файлы в среде ОС выглядят следующим образом (рис. 1). В данном случае мы воспользовались заранее снятым образом НЖМД, примонтировали его как образ физического электронного носителя информации при помощи специализированного ПО «AccessData FTK Imager 4.1.1.1» и просмотрели каталог. В дальнейшем для иллюстрации примеров анализа будут использованы Prefetch-файлы с разных версий ОС «Windows» и НЖМД. Способ, который описан выше, соответствует одному из этапов, что должны были бы быть выполнены до анализа самих Prefetch-файлов. Это создание копии НЖМД при помощи аппаратного или программного блокиратора, создание рабочей копии, монтирование и последующее исследование.

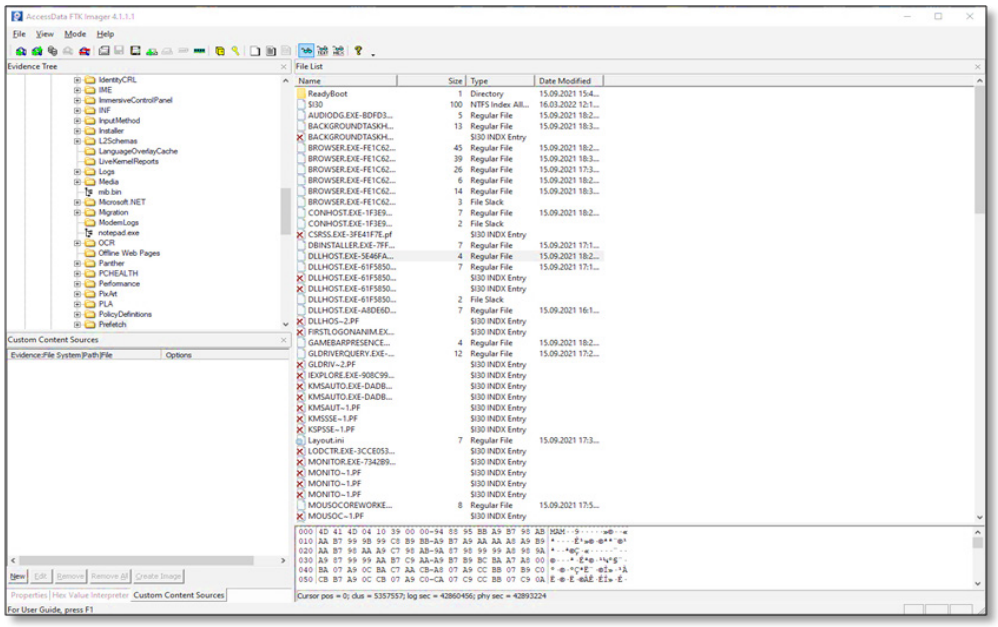


Рис. 1. Окно программы «AccessDataFTKImager 4.1.1.1» с информацией о содержимом каталога «Prefetch»

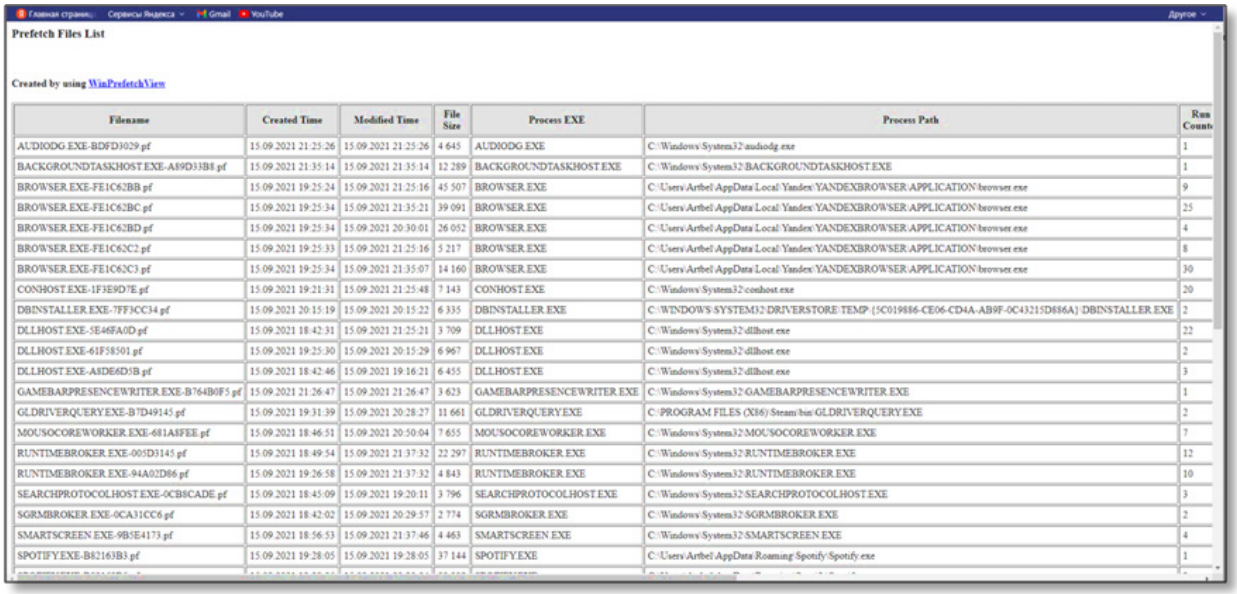
Prefetch-файлы состоят из названия приложения, соответствующего файлу, и хэш-суммы, которая создается из полного пути и имени приложения. Иногда, как например в случае с «svchost», в хэш-сумме могут оказаться и параметры командной строки при запуске приложения. Процесс генерации хэш-суммы происходит следующим образом:

1. Копируется полный путь до исполняемого файла, например: **«C:\Windows\NOTEPAD.EXE»**.
2. Путь конвертируется в строку Unicode.
3. Путь конвертируется в путь устройства, например: **«\DEVICE\HARDDISKVOLUMEX\WINDOWS\NOTEPAD.EXE»**.
4. Применяется хэш-функция.
5. Генерируется имя Prefetch-файла, например: **«NOTEPAD.EXE-XXXXXXXX.pf»**.

Также программа «AccessData FTK Imager 4.1.1.1» позволяет нам взглянуть на содержимое файла в шестнадцатеричном виде, где рядом представлена расшифровка в кодировке ASCII или Unicode. Мы видим, что Prefetch-файл начинается с «магического числа» «MAM». Такая сигнатура характерна для сжатых Prefetch-файлов ОС «Windows 10». Если они не сжаты, то характерным будет сигнатура «SCCA», как и для Prefetch-файлов операционных систем до «Windows 10». Это тоже может быть полезно и косвенно содействовать в обнаружении уже удаленных Prefetch-файлов. «AccessData FTK Imager 4.1.1.1» дает возможность исследовать неразмеченное пространство, среди которого могут сохраняться части удаленных Prefetch-файлов. Из этого пространства можно попробовать восстановить файлы при помощи карвинга, опираясь на структуру и сигнатуры, это трудоемко и не всегда эффективно, однако следы удаления будут обнаружены. Если же будет использовано специализированное ПО для удаления файла, например «SDelete», то будет создан Prefetch-файл самого «SDelete», что будет свидетельствовать о его использовании. Своего рода это будет постоянным маркером.

Помимо очевидных причин почему нельзя исследовать данные на работающей системе и следует делать побитовую копию диска и потом начинать анализ, есть еще одна причина, касающаяся экспорта и копирования всех файлов. Если просто перенести Prefetch-файл на съемный носитель или куда-либо из каталога, то изменится временная метка создания файла, а значит, мы внесем изменения в потенциальное доказательство. Поэтому следует использовать специализированное ПО, такое как, например, «AccessData FTK Imager 4.1.1.1», и, воспользовавшись функцией экспорта файла, перенести его на рабочую станцию эксперта с сохранением всех характеристик объекта, после чего можно приступить к исследованию.

Для успешного исследования Prefetch-файлов необходимо специализированное ПО. Существует огромное количество «парсеров» – программ или сервисов, которые собирают данные из файлов или веб-ресурсов и представляют их в читаемом виде для эксперта [5]. Среди известных инструментов можно перечислить такие, как «PECmd» от Эрика Циммермана, «WinPrefetchView v1.37» от «Nirsoft», «CQPrefetchParser» от «CQTools» и «pf64» от «TZWorks». Все инструменты, кроме «WinPrefetchView v1.37» от «Nirsoft», консольные. «WinPrefetchView v1.37», который имеет GUI-интерфейс, хорошо подходит, если перед экспертом стоит задача поиска информации именно о времени последнего запуска программ или при работе с образом диска, который примонтирован как физический, чтобы можно было запустить «WinPrefetchView v1.37» как на работающем ПК. Помимо этого, данное ПО формирует все в удобную таблицу, которую можно прикрепить к заключению (рис. 2).



Prefetch Files List

Created by using WinPrefetchView

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counts
AUDIODG.EXE-BDFD3029.pf	15.09.2021 21:25:26	15.09.2021 21:25:26	4 645	AUDIODG.EXE	C:\Windows\System32\audiodg.exe	1
BACKGROUNDTASKHOST.EXE-A89D33B8.pf	15.09.2021 21:35:14	15.09.2021 21:35:14	12 289	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	1
BROWSER.EXE-FE1C62BB.pf	15.09.2021 19:25:24	15.09.2021 21:25:16	45 507	BROWSER.EXE	C:\Users\Artbel\AppData\Local\Yandex\YANDEXBROWSER\APPLICATION\browser.exe	9
BROWSER.EXE-FE1C62BC.pf	15.09.2021 19:25:34	15.09.2021 21:35:21	39 091	BROWSER.EXE	C:\Users\Artbel\AppData\Local\Yandex\YANDEXBROWSER\APPLICATION\browser.exe	25
BROWSER.EXE-FE1C62BD.pf	15.09.2021 19:25:34	15.09.2021 20:30:01	26 052	BROWSER.EXE	C:\Users\Artbel\AppData\Local\Yandex\YANDEXBROWSER\APPLICATION\browser.exe	4
BROWSER.EXE-FE1C62C2.pf	15.09.2021 19:25:33	15.09.2021 21:25:16	5 217	BROWSER.EXE	C:\Users\Artbel\AppData\Local\Yandex\YANDEXBROWSER\APPLICATION\browser.exe	8
BROWSER.EXE-FE1C62C3.pf	15.09.2021 19:25:34	15.09.2021 21:35:07	14 160	BROWSER.EXE	C:\Users\Artbel\AppData\Local\Yandex\YANDEXBROWSER\APPLICATION\browser.exe	30
CONHOST.EXE-1F3E9D7E.pf	15.09.2021 19:21:31	15.09.2021 21:25:48	7 143	CONHOST.EXE	C:\Windows\System32\conhost.exe	20
DBINSTALLER.EXE-7FF3CC34.pf	15.09.2021 20:15:19	15.09.2021 20:15:22	6 335	DBINSTALLER.EXE	C:\WINDOWS\SYSTEM32\DRIVERSTORE\TEMP\{5C019886-CE06-CD4A-AB9F-0C43215D886A}\DBINSTALLER.EXE	2
DLLHOST.EXE-5E46FA0D.pf	15.09.2021 18:42:31	15.09.2021 21:25:21	3 709	DLLHOST.EXE	C:\Windows\System32\dllhost.exe	22
DLLHOST.EXE-61F58501.pf	15.09.2021 19:25:30	15.09.2021 20:15:29	6 967	DLLHOST.EXE	C:\Windows\System32\dllhost.exe	2
DLLHOST.EXE-A8DE6D5B.pf	15.09.2021 18:42:46	15.09.2021 19:16:21	6 455	DLLHOST.EXE	C:\Windows\System32\dllhost.exe	3
GAMEBARPRESENCEWRITER.EXE-B764B0F5.pf	15.09.2021 21:26:47	15.09.2021 21:26:47	3 623	GAMEBARPRESENCEWRITER.EXE	C:\Windows\System32\GAMEBARPRESENCEWRITER.EXE	1
GLDRIVERQUERY.EXE-B7D49145.pf	15.09.2021 19:31:39	15.09.2021 20:28:27	11 661	GLDRIVERQUERY.EXE	C:\PROGRAM FILES (X86)\Steam\bin\GLDRIVERQUERY.EXE	2
MOUSOCOREWORKER.EXE-681A8FEE.pf	15.09.2021 18:46:51	15.09.2021 20:50:04	7 655	MOUSOCOREWORKER.EXE	C:\Windows\System32\MOUSOCOREWORKER.EXE	7
RUNTIMEBROKER.EXE-005D3145.pf	15.09.2021 18:49:54	15.09.2021 21:37:32	22 297	RUNTIMEBROKER.EXE	C:\Windows\System32\RUNTIMEBROKER.EXE	12
RUNTIMEBROKER.EXE-94A02D86.pf	15.09.2021 19:26:58	15.09.2021 21:37:32	4 843	RUNTIMEBROKER.EXE	C:\Windows\System32\RUNTIMEBROKER.EXE	10
SEARCHPROTOCOLHOST.EXE-0CB8CADE.pf	15.09.2021 18:45:09	15.09.2021 19:20:11	3 796	SEARCHPROTOCOLHOST.EXE	C:\Windows\System32\SEARCHPROTOCOLHOST.EXE	3
SGRMBROKER.EXE-0CA31CC6.pf	15.09.2021 18:42:02	15.09.2021 20:29:57	2 774	SGRMBROKER.EXE	C:\Windows\System32\SGRMBROKER.EXE	2
SMARTSCREEN.EXE-9B5E4173.pf	15.09.2021 18:56:53	15.09.2021 21:37:46	4 463	SMARTSCREEN.EXE	C:\Windows\System32\SMARTSCREEN.EXE	4
SPOTIFY.EXE-B82163B3.pf	15.09.2021 19:28:05	15.09.2021 19:28:05	37 144	SPOTIFY.EXE	C:\Users\Artbel\AppData\Roaming\Spotify\Spotify.exe	1

Рис. 2. Фрагмент окна программы «Яндекс.Браузер», содержащий информацию о Prefetch-файлах и временных метках запуска программ

Проанализировав работу других инструментов, можно с уверенностью сказать, что «PECmd» и «pf64», в отличие от «CQPrefetchParser» [6], который работает с более старыми версиями, в полной мере подходят для глубокого анализа содержимого Prefetch-файлов, однако большей популярностью пользуется именно «PECmd». С помощью данного ПО рассмотрим основную криминалистически значимую инфор-

мацию, которую можно получить при помощи анализа Prefetch-файлов, а также методику работы с ней.

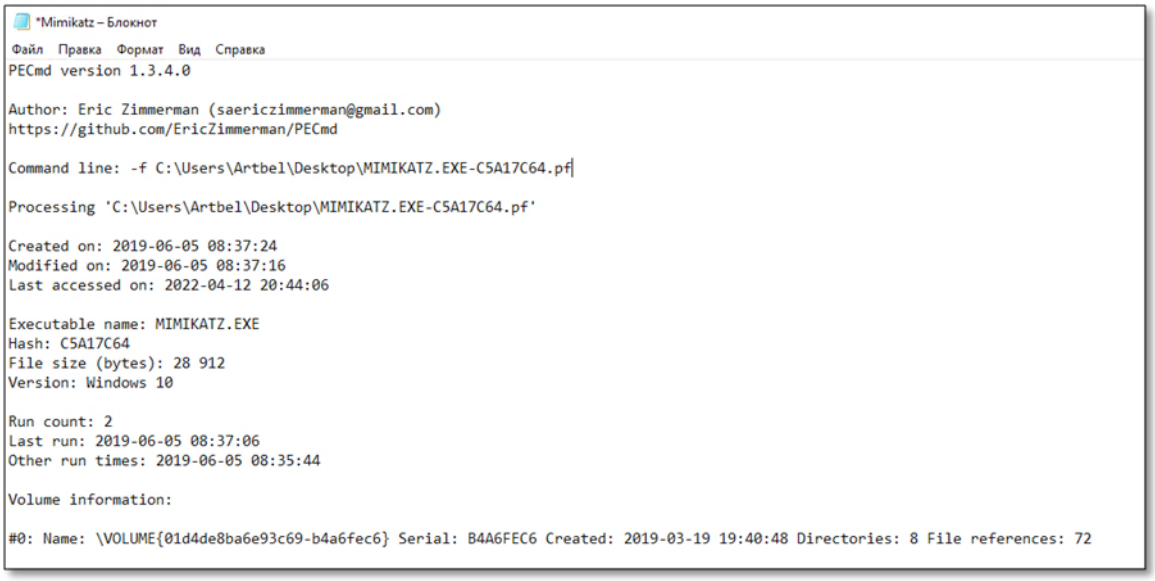
В рамках исследования был использован «WindowsPowerShell», помимо него можно работать и в командной строке, однако на результат работы это не влияет. Указываем путь к «PECmd» и запускаем его.

Если «PECmd» до этого не запускалось на данном компьютере, то потребуется принять лицензионное соглашение и начать работу. В данном выводе нам показаны параметры, при помощи которых мы можем работать с «PECmd». Вариантов множество, однако для анализа содержимого конкретного Prefetch-файла достаточно параметра **«–f»**, который указывает путь к нему.

Один из случаев, когда есть понимание, что необходимо исследовать тот или иной Prefetch-файл, довольно прост – название приложения и его функционал соответствуют искомым фактам. Например, в папке «Prefetch» одного из исследуемых образов НЖМД был обнаружен файл с именем **«MIMIKATZ.EXE-C5A17C64.pf»**. Само имя файла уже говорит о том, что, возможно, это довольно известное приложение с открытым исходным кодом, которое позволяет пользователям просматривать и сохранять учетные данные аутентификации. У рядового пользователя эта программа не встречается, зачастую это может быть признаком совершения высокотехнологичного киберпреступления. Вводим следующую команду **«C:\Users\Artbel\Desktop>.\PECmd.exe –fC:\Users\Artbel\Desktop\MIMIKATZ.EXE-C5A17C64.pf>C:\Users\Artbel\Desktop\Results\Mimikatz.txt».**

Данная команда позволяет вывести результат работы «PECmd» в текстовый файл по указанному пути.

На рис. 3 приведен результат работы программы.



```
*Mimikatz – Блокнот
Файл  Правка  Формат  Вид  Справка
PECmd version 1.3.4.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Users\Artbel\Desktop\MIMIKATZ.EXE-C5A17C64.pf

Processing 'C:\Users\Artbel\Desktop\MIMIKATZ.EXE-C5A17C64.pf'

Created on: 2019-06-05 08:37:24
Modified on: 2019-06-05 08:37:16
Last accessed on: 2022-04-12 20:44:06

Executable name: MIMIKATZ.EXE
Hash: C5A17C64
File size (bytes): 28 912
Version: Windows 10

Run count: 2
Last run: 2019-06-05 08:37:06
Other run times: 2019-06-05 08:35:44

Volume information:

#0: Name: \VOLUME{01d4de8ba6e93c69-b4a6fec6} Serial: B4A6FEC6 Created: 2019-03-19 19:40:48 Directories: 8 File references: 72
```

Рис. 3. Фрагмент окна программы «Блокнот», содержащего информацию о результате работы «PECmd»

Мы видим, что в документе отобразились три временные метки. В поле «Created on» отображается время создания файла, в поле «Modified on» – время последнего изменения файла. Иными словами, они отличаются на несколько секунд как раз с

вычетом времени мониторинга действий приложения, о чем упоминалось ранее. В поле «Last accessed on» отображается время последнего доступа к файлу, тут указывается время, в которое мы запустили «PECmd» для исследования данного файла.

Ниже, в поле «Executable name», отображается имя исполняемого файла. В поле «Hash» – хэш-сумма пути к исполняемому файлу, далее следует размер файла в байтах и версия ОС «Windows», с которой был получен данный Prefetch-файл.

Далее следует важнейшая информация, которую можно получить при определении обстоятельств запуска ПО при помощи анализа Prefetch-файлов. Это количество запусков программы, время последнего и предыдущих семи запусков. В нашем примере с файлом **«MIMIKATZ.EXE-C5A17C64.pf»** это не так хорошо проиллюстрировано, поэтому за основу был взят Prefetch-файл с другого образа НЖМД и программы Blender (профессиональное свободное и открытое программное обеспечение для создания трехмерной компьютерной графики), которая нагляднее иллюстрирует пользовательскую активность – **«BLENDER.EXE-EBACE203.pf»** (рис. 4).

Вводим команду **C:\Users\a.beley.LP-ABELEY\Desktop>.\PECmd.exe-fC:\Users\a.beley.LP-ABELEY\Desktop\BLENDER.EXE-EBACE203.pf**

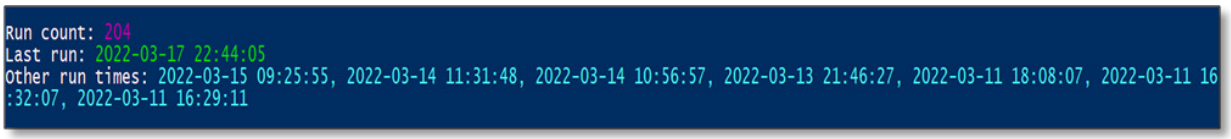


Рис. 4. Окно программы «WindowsPowerShell», содержащее информацию о значениях параметров об исследуемом файле «BLENDER.EXE-EBACE203.pf»

В поле «Run count» мы видим количество запусков этой программы – 204, в поле «Last run» – дату и время последнего запуска программы, что зачастую и является целью исследования. В поле «Other run times» мы можем видеть временные метки последних семи запусков.

Далее можно обнаружить информацию, которая может быть полезна в рамках исследования или установления следов высокотехнологичных преступлений. В поле «Volume information» мы можем видеть информацию о дисках, с которыми связаны директории или файлы, к которым обращался исследуемый исполняемый файл. Там отображаются серийный номер, дата создания, а также количество директорий и файлов, к которым обращался исполняемый файл. В данном случае дисков два.

В поле «Directories referenced» мы видим общее количество директорий, к которым обращался исполняемый файл при запуске. В выводе будет отображаться полный путь к данной директории. Это может быть полезно при исследовании следов совершения высокотехнологичных преступлений. Например, может быть обнаружено, что файл при запуске обращается к какой-то странной директории на самом ПК или к сетевой папке (рис. 5).

```
Volume information:

#0: Name: \VOLUME{01d6d4c526120f24-962697db} Serial: 962697DB Created: 2020-12-17 22:37:06 Directories: 5 File references: 15
#1: Name: \VOLUME{01d6d4c53a95c56e-283ac5d6} Serial: 283AC5D6 Created: 2020-12-17 22:37:41 Directories: 2 File references: 6

Directories referenced: 7

00: \VOLUME{01d6d4c526120f24-962697db}\STEAM
01: \VOLUME{01d6d4c526120f24-962697db}\STEAM\STEAMAPPS
02: \VOLUME{01d6d4c526120f24-962697db}\STEAM\STEAMAPPS\COMMON
03: \VOLUME{01d6d4c526120f24-962697db}\STEAM\STEAMAPPS\COMMON\BLENDER
04: \VOLUME{01d6d4c526120f24-962697db}\STEAM\STEAMAPPS\COMMON\BLENDER\BLENDER.CRT
05: \VOLUME{01d6d4c53a95c56e-283ac5d6}\WINDOWS
06: \VOLUME{01d6d4c53a95c56e-283ac5d6}\WINDOWS\SYSTEM32

Files referenced: 390
```

Рис. 5. Окно программы «WindowsPowerShell», содержащее информацию о значениях параметров об исследуемом файле «BLENDER.EXE-EBACE203.pf»

Далее следует поле «File referenced», в нем отображаются общее количество файлов, к которым обращался процесс, и пути к ним. Данный вывод может быть полезен. Он может свидетельствовать о том, что определенные файлы присутствовали в системе и использовались при запуске исполняемого файла и указать путь к ним, либо, например, указать на потенциальную инъекцию вредоносной библиотеки в процесс, если она подгружалась из подозрительной директории или имеет аномальное название. Кроме того, если речь идет об исследовании исполняемых файлов, которые связаны с активностью пользователя, то можно обнаружить следы активности пользователя и файлы, которые он открывал при последнем запуске. Например, исследуя Prefetch-файл программы «MicrosoftOfficeExcel», мы обнаружили следы запуска файла «TETROGRAF_BYUDZHET.xlsx из папки «Downloads» (см. рис. 6).

```
249: \VOLUME{01d62ac31e125d27-761e2f7f}\WINDOWS\SYSWOW64\GPAPI.DLL
250: \VOLUME{01d62ac31e125d27-761e2f7f}\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\4.18.2201.10-0\MSMPLICS.DLL
251: \VOLUME{01d62ac31e125d27-761e2f7f}\USERS\USER\DOWNLOADS\~$TETROGRAF_BYUDZHET.XLSX
252: \VOLUME{01d62ac31e125d27-761e2f7f}\PROGRAM FILES (X86)\COMMON FILES\MICROSOFT SHARED\OFFICE16\OREGRES.DLL
253: \VOLUME{01d62ac31e125d27-761e2f7f}\PROGRAM FILES (X86)\COMMON FILES\MICROSOFT SHARED\OFFICE16\RU-RU\OREGRES.DLL.M
UI
```

Рис. 6. Окно программы «WindowsPowerShell», содержащее информацию о значениях параметров об исследуемом файле «EXCEL.EXE-EASXD211.pf»

Последним в выводе работы утилиты указывается время выполнения, за которое программа распарсила исследуемый файл, но другой информации не выдает.

Таким образом, исходя из вышесказанного можно с уверенностью сказать, что исследование Prefetch-файлов позволяет субъекту исследования получить следующую криминалистически значимую информацию:

1. Время последнего запуска программы из определенной директории (при условии включенных Prefetch-файлов на момент снятия криминалистической копии).

2. Время предыдущих семи запусков исполняемого файла из определенной директории (при условии включенных Prefetch-файлов на момент снятия криминалистической копии).

3. Общее количество запусков программы с момента установки системы или включения Prefetch-файлов.

4. Информацию о директориях, файлах и дисках, к которым обращался исполняемый файл при запуске.

Учитывая результаты практического использования, стоит отметить, что исследование таких файлов является неотъемлемой частью методики проведения СКТЭ в рамках решения задач по обнаружению файлов, изучению пользовательской активности или подтверждению запуска определенного ПО в случае работы с криминалистической копией, снятой с ОС «Windows». Сформулированные и систематизированные положения и подходы позволят усовершенствовать процесс применения и использования специальных знаний в области установления фактов, связанных с запуском ПО, внесут вклад в развитие криминалистической техники в области СКТЭ, а также будут способствовать успешной деятельности правоохранительных органов и повышению скорости и эффективности проведения судебной компьютерно-технической экспертизы.

СПИСОК ИСТОЧНИКОВ

1. Краткая характеристика состояния преступности в Российской Федерации за январь–июль 2023 года. URL: https://мвд.рф/reports/item/40874008 (дата обращения: 21.09. 2023).
2. Для рынка настольных операционных систем по всему миру. URL: https://gs.statcounter.com/os-market-share/desktop/worldwide (дата обращения: 21.09.2023).
3. Волатильность. URL: https://github.com/volatilityfoundation/volatility (дата обращения: 21.09.2023).
4. Skulkin O., Courcier S. Windows Forensics Cookbook. Birminghem, 2017. 258 p.
5. Анализ предварительной выборки файлов в Windows. URL: https://www.magnetforensics.com/blog/forensic-analysis-of-prefetch-files-in-windows/ (дата обращения: 21.09.2023).
6. Как судебные эксперты используют предварительную выборку Windows. URL: https://cqureacademy.com/blog/hacks/prefetch-parser (дата обращения: 21.09.2023).

REFERENCES

1. *Kratkaya kharakteristika sostoyaniya prestupnosti v Rossiiskoi Federatsii za yanvar'–iyul' 2023 goda* [Brief description of the state of crime in the Russian Federation in January–July 2023]. Available at: https://mvd.rf/reports/item/40874008 (accessed September 21, 2023).
2. *Dlya rynka nastol'nykh operatsionnykh sistem po vsemu miru* [For the desktop operating system market worldwide]. Available at: https://gs.statcounter.com/os-market-share/desktop/worldwide (accessed September 21, 2023).
3. *Volatil'nost'* [Volatility]. Available at: https://github.com/volatilityfoundation/volatility (accessed September 21, 2023).
4. Skulkin O., Courcier S. *Windows forensics cookbook*. Birminghem, 2017. 258 r.
5. *Analiz predvaritel'noi vyborki failov v Windows* [Analysis of a preliminary sample of files in Windows]. Available at: https://www.magnetforensics.com/blog/forensic-analysis-of-prefetch-files-in-windows/ (accessed September 21, 2023).
6. *Kak sudebnye eksperty ispol'zuyut predvaritel'nuyu vyborku* Windows [How forensic experts use Windows pre-sampling]. Available at: https://cqureacademy.com/blog/hacks/prefetch-parser (accessed September 21, 2023).

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

АРТЕМ ВЯЧЕСЛАВОВИЧ БЕЛЕЙ – аспирант кафедры судебных экспертиз и криминалистики Российского государственного университета правосудия, Москва, Россия, a.beley@facct.ru

ARTEM V. BELEI – Postgraduate Student at the Department of Forensic Examinations and Criminalistics of the Russian State University of Justice, Moscow, Russia, a.beley@facct.ru

Статья поступила 01.09.2022