Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 8, Is. 2, pp. 70-77, 2016

DOI: 10.13187/vesp.2016.8.70
www.ejournal21.com


UDC 343.983.25

# Special Aspects of Digital Artifacts Forensic Analysis in Microsoft Windows 10 Operation System

[1] Yuri V. Naidenyshev
[2] Oleg V. Skulkin

[1] Sochi state university, Russian Federation
Senior Lecturer
E-mail: krimex@yandex.ru
[2] Interdistrict Department of Sochi and Tuapse of CEC of MD of MI of Krasnodar Krai, Russian Federation
Expert
E-mail: skulkin@inbox.ru

**Abstract**

In this article we will discuss both new sources of digital evidence, typical for the new version of operation system, such as Notification Center, Microsoft Edge web-browser and digital personal assistant Cortana, and some known artifacts, which changed its format, for example, Prefetch files. Also we'll discuss such important source of digital evidence, as Volume Shadow Copy, which first appeared in Microsoft Windows XP, but still available in the new version of Microsoft Windows OS.

**Keywords:** digital forensics, computer forensics, Windows 10 forensics, Notification Center forensics, Microsoft Edge forensics, Cortana forensics.

## Введение

Официальный релиз новой версии операционной системы Microsoft – Windows 10 состоялся 29 июля 2015 года. Некоторые исследователи, начавшие разбор новой ОС через призму цифровой криминалистики еще на стадии бета-версии, уже представили свои отчеты. Одним из них является Брент Мьюир (см. Muir 2015), работы которого, в том числе, составили теоретическую основу настоящего исследования.

## Центр уведомлений Windows 10

В новой версии Windows появился центр уведомлений, который позволяет приложениям выводить сообщения на экран подобно тому, как это происходит в операционных системах мобильных устройств. Эти сообщения, разумеется, могут содержать значимую, в том числе с криминалистической точки зрения, информацию.

Указанные сообщения хранятся в файле appdb.dat, который расположен в следующем каталоге:

*<Системный_раздел>\Users\<Имя_пользователя>\AppData\Local\Microsoft\Windows\Notifications*

При анализе указанного файла посредством hex-просмотрщика становится очевидно, что записи об уведомлениях, полученных пользователем, хранятся в формате XML (см. иллюстрацию 1).

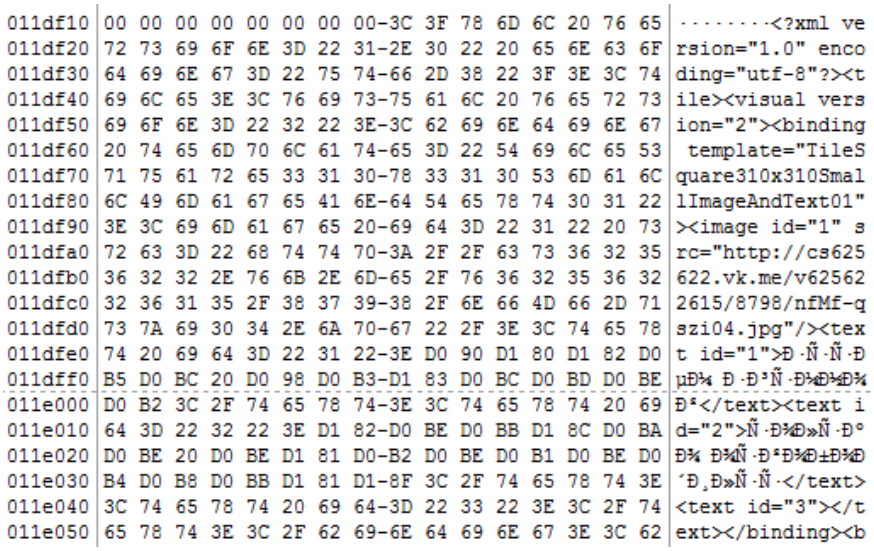



*Рис. 1.* Фрагмент файла appdb.dat, открытого в hex-просмотрщике ПП AccessData FTK Imager

Как видно на иллюстрации, используется разметка XML версии 1.0 и кодировка UTF-8. В рассматриваемом примере содержится уведомление о полученном сообщении в социальной сети «Вконтакте». Наиболее значимая информация содержится внутри дескрипторов <image> и <text>. Так внутри дескриптора <image> содержится ссылка на изображение профиля пользователя, передавшего сообщение, а внутри дескрипторов <text> – его имя и текст сообщения. Необходимо отметить, что на представленной иллюстрации вместо текста размещен набор бессвязных символов потому, что используемый hex-редактор не поддерживает кодировку UTF-8. Чтобы декодировать текст внутри дескрипторов <text>, можно воспользоваться одним из онлайн-сервисов, например, https://www.artlebedev.ru/tools/decoder/.

**Веб-браузер Microsoft Edge**

Начиная с десятой версии браузера Internet Explorer, разработчики Microsoft изменили формат хранения данных, отвернувшись от привычного многим специалистам в области цифровой криминалистики index.dat, и представив базу данных в формате ESE, хранящуюся в файле WebCacheV01.dat.

Несмотря на то, что с выходом Windows 10 разработчики представили новый веб-браузер – Microsoft Edge, носивший кодовое название «Spartan», традиционный для ОС Windows браузер Internet Explorer (одиннадцатой версии) также имеет место, а история просмотров веб-страниц по-прежнему хранится в следующем каталоге:

*<Системный_раздел>\Users\<Имя_пользователя>\AppData\Local\Microsoft\Windows\WebCache*

Но в файле WebCacheV01.dat, расположенном в указанном выше каталоге, хранится не только история браузера Internet Explorer, но и нового – Microsoft Edge. Помимо истории в базе данных хранятся и сведения о куки. Рассматриваемая БД может пребывать в состоянии «Dirty Shutdown», что может препятствовать исследованию цифровой информации, хранящейся в ней. Для того чтобы выяснить, в каком состоянии она находится, эксперт может воспользоваться утилитой esentutl.exe, которую можно найти в следующем каталоге:

*<Системный_раздел>\Windows\System32*

Чтобы получить сведения об исследуемой базе данных, необходимо, предварительно скопировав на рабочую станцию каталог \WebCache и перейдя в него, в командной строке ввести следующую команду:

*esentutl /mh WebCacheV01.dat*

Как видно на иллюстрации, помимо всего прочего, вывод команды содержит сведения о состоянии, в нашем случае – «Dirty Shutdown» (см. иллюстрацию 2).

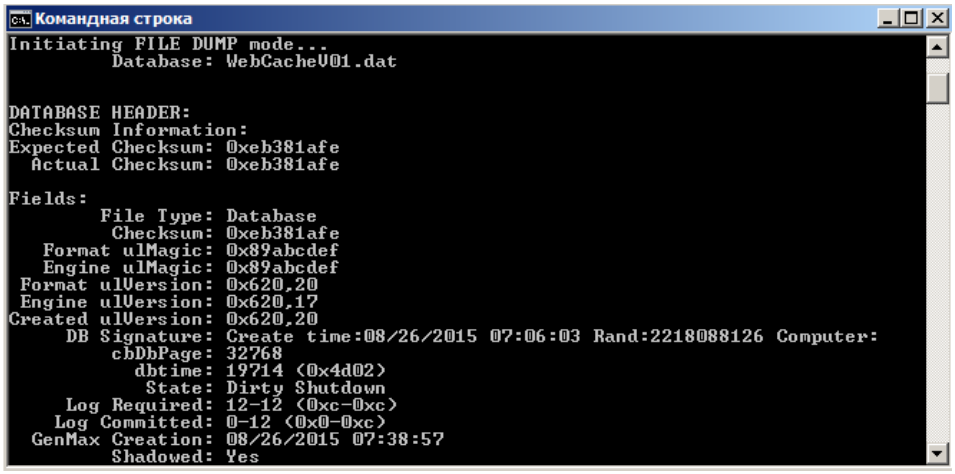


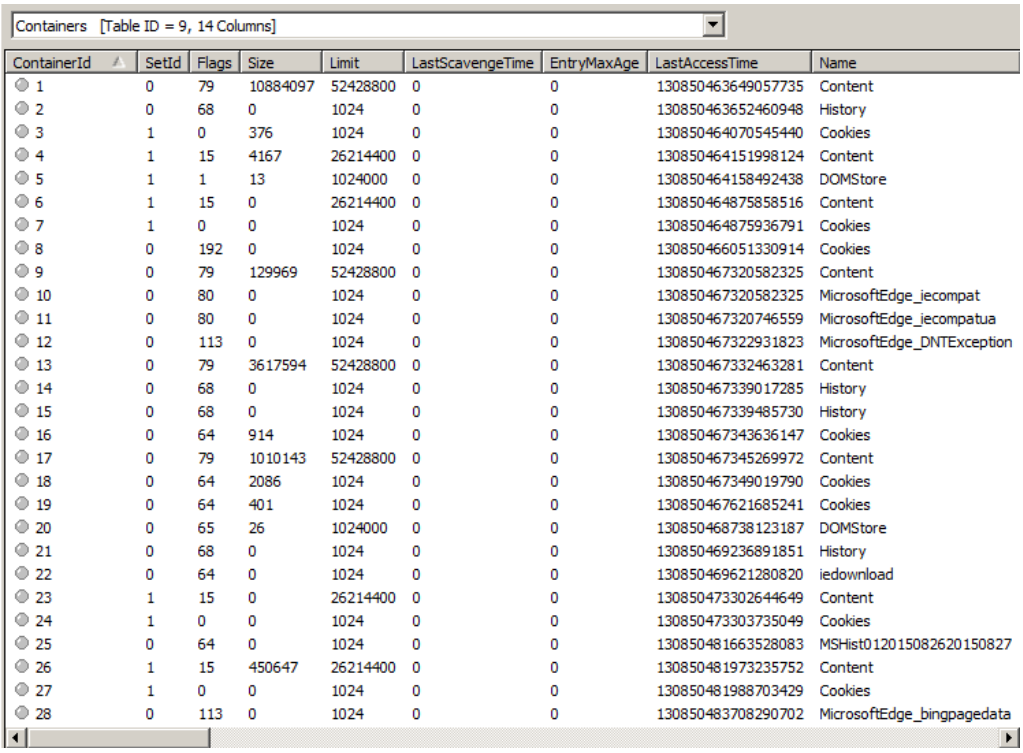

*Рис. 2.* Результат применения утилиты esentutl с ключом /mh

Для того чтобы привести БД к состоянию «Clean Shutdown», необходимо поместить в нее имеющиеся лог-файлы. Сделать это можно путем ввода следующей команды:

*esentutl /r V01 /d*

Ключ /d необходим для того, чтобы утилита искала лог-файлы только в текущей директории. При повторном запуске утилиты esentutl.exe с ключом /mh значение поля «State» поменяет значение на «Clean Shutdown».

Для просмотра содержимого базы данных может быть использован программный продукт ESEDatabaseView разработки NirSoft. Чтобы получить общую информацию о том, какие сведения хранятся в БД, необходимо перейти в таблицу «Containers». База данных, используемая в качестве примера, содержит 28 контейнеров (см. иллюстрацию 3).



Containers [Table ID = 9, 14 Columns]

| ContainerId | SetId | Flags | Size | Limit | LastScavengeTime | EntryMaxAge | LastAccessTime | Name |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 79 | 10884097 | 52428800 | 0 | 0 | 130850463649057735 | Content |
| 2 | 0 | 68 | 0 | 1024 | 0 | 0 | 130850463652460948 | History |
| 3 | 1 | 0 | 376 | 1024 | 0 | 0 | 130850464070545440 | Cookies |
| 4 | 1 | 15 | 4167 | 26214400 | 0 | 0 | 130850464151998124 | Content |
| 5 | 1 | 1 | 13 | 1024000 | 0 | 0 | 130850464158492438 | DOMStore |
| 6 | 1 | 15 | 0 | 26214400 | 0 | 0 | 130850464875858516 | Content |
| 7 | 1 | 0 | 0 | 1024 | 0 | 0 | 130850464875936791 | Cookies |
| 8 | 0 | 192 | 0 | 1024 | 0 | 0 | 130850466051330914 | Cookies |
| 9 | 0 | 79 | 129969 | 52428800 | 0 | 0 | 130850467320582325 | Content |
| 10 | 0 | 80 | 0 | 1024 | 0 | 0 | 130850467320582325 | MicrosoftEdge_iecompat |
| 11 | 0 | 80 | 0 | 1024 | 0 | 0 | 130850467320746559 | MicrosoftEdge_iecompatua |
| 12 | 0 | 113 | 0 | 1024 | 0 | 0 | 130850467322931823 | MicrosoftEdge_DNTException |
| 13 | 0 | 79 | 3617594 | 52428800 | 0 | 0 | 130850467332463281 | Content |
| 14 | 0 | 68 | 0 | 1024 | 0 | 0 | 130850467339017285 | History |
| 15 | 0 | 68 | 0 | 1024 | 0 | 0 | 130850467339485730 | History |
| 16 | 0 | 64 | 914 | 1024 | 0 | 0 | 130850467343636147 | Cookies |
| 17 | 0 | 79 | 1010143 | 52428800 | 0 | 0 | 130850467345269972 | Content |
| 18 | 0 | 64 | 2086 | 1024 | 0 | 0 | 130850467349019790 | Cookies |
| 19 | 0 | 64 | 401 | 1024 | 0 | 0 | 130850467621685241 | Cookies |
| 20 | 0 | 65 | 26 | 1024000 | 0 | 0 | 130850468738123187 | DOMStore |
| 21 | 0 | 68 | 0 | 1024 | 0 | 0 | 130850469236891851 | History |
| 22 | 0 | 64 | 0 | 1024 | 0 | 0 | 130850469621280820 | iedownload |
| 23 | 1 | 15 | 0 | 26214400 | 0 | 0 | 130850473302644649 | Content |
| 24 | 1 | 0 | 0 | 1024 | 0 | 0 | 130850473303735049 | Cookies |
| 25 | 0 | 64 | 0 | 1024 | 0 | 0 | 130850481663528083 | MSHist012015082620150827 |
| 26 | 1 | 15 | 450647 | 26214400 | 0 | 0 | 130850481973235752 | Content |
| 27 | 1 | 0 | 0 | 1024 | 0 | 0 | 130850481988703429 | Cookies |
| 28 | 0 | 113 | 0 | 1024 | 0 | 0 | 130850483708290702 | MicrosoftEdge_bingpagedata |

*Рис. 3.* Таблица «Containers» базы данных WebCacheV01.dat, открытая посредством ПП NirSoft ESEDatabaseView

Как видно на иллюстрации, сведения о просмотре веб-страниц хранятся в контейнерах 2, 14, 15 и 21. Рассматриваемая таблица содержит не только сведения о содержимом контейнеров, но и пути к файлам с данными.

Что касается временных меток в рассматриваемой БД, то их значения сначала необходимо конвертировать в шестнадцатеричный вид, а затем декодировать посредством, например, программного продукта DCode, используя формат «Windows: 64 bit Hex Value – Big Endian».

Необходимо отметить, что сведения о веб-страницах, посещенных пользователем в режиме «InPrivate», хранятся в тех же контейнерах. Таким страницам присваивается значение «8» в столбце «Flags» [Muir 2015: Электрон. ресурс].

Что касается сведений о загрузках пользователя, то они хранятся в контейнере 22, имеющем имя «iedownload». Информация в данном контейнере представлена в шестнадцатеричном виде и должна быть преобразована в ASCII.

Кэшированные браузером файлы хранятся в следующем каталоге:

*<Системный_раздел>\Users\<Имя_пользователя>\AppData\Local\Packages\Microsoft.MicrosoftEdge_***\AC\#!001\MicrosoftEdge\Cache*

Извлечение данных из рассмотренных файлов для последующего анализа в автоматическом режиме может быть осуществлено, например, посредством ПП Evidence Center разработки Belkasoft.

**Цифровой персональный ассистент Cortana**

Персональный ассистент Cortana впервые был представлен в Windows 8 как самостоятельное приложение. С выходом новой версии ОС Cortana стал полноценной частью системы. Несмотря на то, что на данный момент ассистент на русском языке недоступен, эксперту необходимо понимать, какие артефакты могут быть обнаружены в ходе исследования.

Сведения об использовании цифрового ассистента хранятся в базах данных в формате ESE – IndexedDB.edb и CortanaCoreDb.dat, которые расположены в следующих каталогах:

*<Системный_раздел>\Users\<Имя_пользователя>\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\AppData\Indexed DB*

*<Системный_раздел>\Users\<Имя_пользователя>\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\LocalState\ESEDatabase_CortanaCoreInstance*

Первая БД содержит сведения об индексированных Cortana данных, вторая – о взаимодействии пользователя с ассистентом. Необходимо отметить, что временные метки второй базы данных представлены в формате Google Chrome Value и могут быть декодированы посредством, например, ПП DCode разработки Digital Detective.

## Prefetch-файлы

Как известно, Prefetch-файлы содержат метаданные (данные о данных), которые очень важны при производстве криминалистического исследования цифровой информации или судебной компьютерной (компьютерно-технической) экспертизы. Например, указанные файлы содержат информацию о том, когда последний раз запускалось приложение, а также сколько всего раз оно запускалось. Кроме того, исследовав prefetch-файлы, эксперт может установить, с какого логического диска было запущено приложение (в том числе серийный номер тома), а также получить список DLL и других использованных им файлов.

Prefetch-файлы в операционной системе Microsoft Windows 10 по-прежнему хранятся в каталоге \Windows\Prefetch\ и имеют расширение «.pf», но, как отмечает в своим исследовании Франческо Пикассо [Picasso 2015: Электрон. ресурс], изменили свой формат.

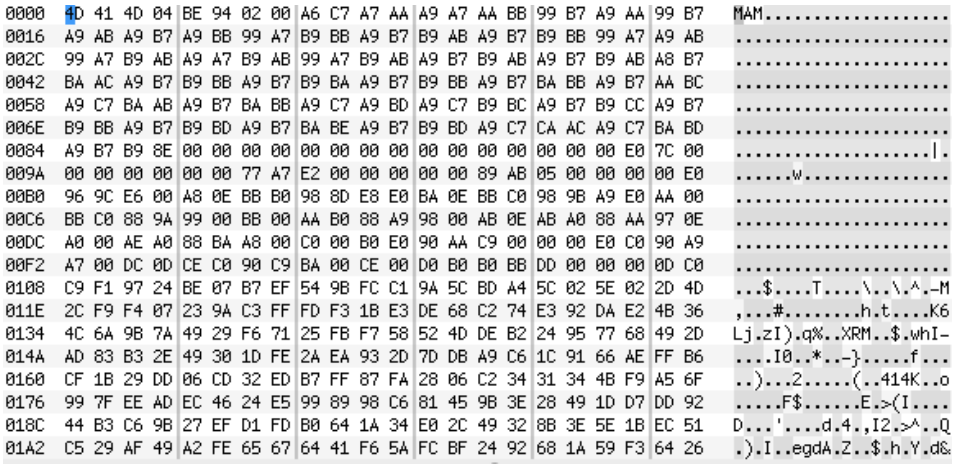



*Рис. 4.* Фрагмент файла VK.EXE-570D9FDD.pf, открытого в hex-редакторе 0xED

Как видно на иллюстрации, теперь файлы имеют сигнатуру «MAM», а символьные строки в них отсутствуют. Дело в том, что для сжатия рассматриваемых файлов используется алгоритм Xpress Huffman. В своей работе Пикассо представил скрипт, написанный на языке программирования Python, который позволяет распаковать prefetch-файлы нового формата. Данный скрипт может быть загружен по следующей ссылке: https://gist.github.com/dfirfpi/113ff71274a97b489dfd.

Необходимо отметить, что для запуска указанного скрипта необходимо использовать операционную систему Microsoft Windows версии 8.1 и выше. После распаковки файла данные могут быть извлечены при помощи специализированного программного обеспечения, например, Mitec Windows File Analyzer.

**Служба теневого копирования тома**

Как известно, служба теневого копирования томов была реализована корпорацией Microsoft с выходом операционной системы Windows XP. Но если в XP она позволяла восстанавливать раннее состояние системы через так называемые «точки восстановления», что уже на тот момент было ценным с точки зрения криминалистического анализа, ведь, например, могло быть восстановлено предыдущее состояние системного реестра ОС, то с появлением ОС Windows Vista теневые копии томов стали содержать не только ранние версии системных файлов, но и пользовательских. В новой версии операционной системы она по-прежнему является важным источником криминалистически значимой информации.

Чтобы посмотреть список теневых копий томов на работающей системе, можно воспользоваться командной строкой (с правами администратора) и ввести в нее команду vssadmin list shadows (см. иллюстрацию 5).

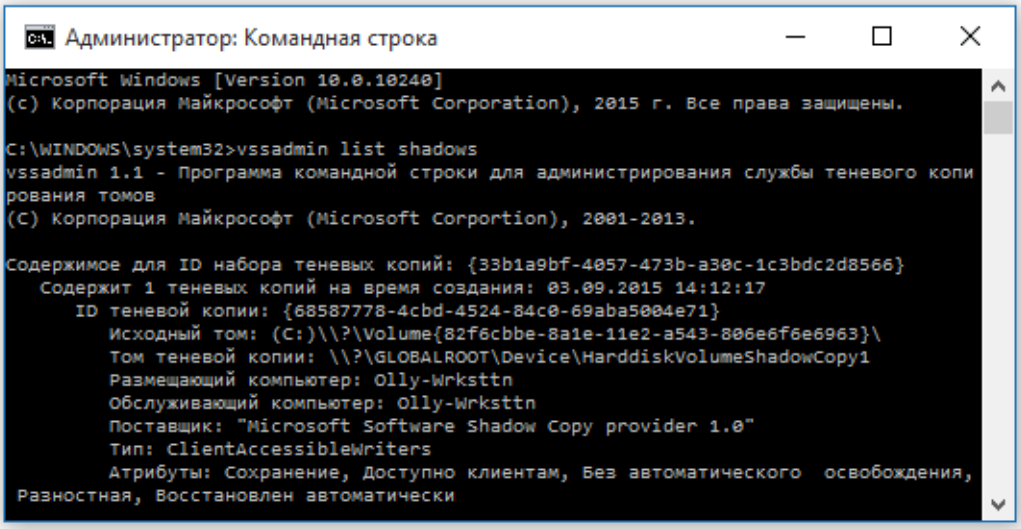



*Рис. 5.* Пример вывода команды vssadmin list shadows

Существуют и программные продукты с графическим пользовательским интерфейсом, например, Shadow Explorer (см. иллюстрацию 6).

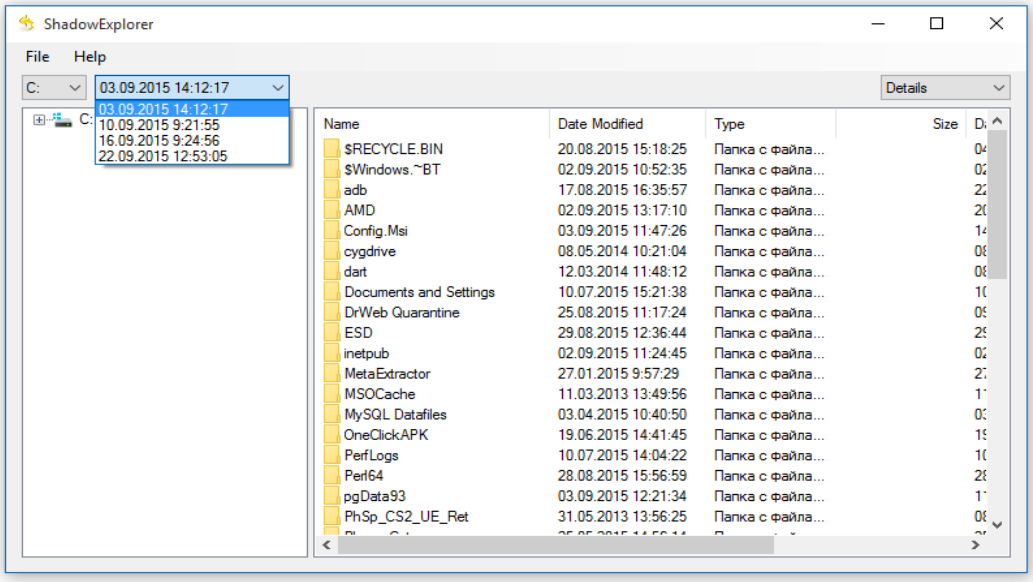



*Рис. 6.* Список теневых копий, отображенный посредством ПП Shadow Explorer

Разумеется, доступ к работающей системе эксперт получает довольно редко, обычно, в тех случаях, когда участвует в осмотре места происшествия или обыске в качестве специалиста. Извлечь теневые копии из образа можно, например, VHD-методом, предложенным Харланом Карви (см. Carvey 2014).

Во-первых, необходимо конвертировать образ (лучше сделать побитовую копию системного раздела отдельно) в формат VHD (Virtual Hard Disk), воспользовавшись утилитой vhdtool.exe.

Полученный файл необходимо смонтировать в режиме «только чтение», воспользовавшись «Панелью управления».

Посмотреть, сколько в исследуемом образе имеется теневых копий, можно при помощи утилиты vssadmin.exe (например так: vssadmin list shadows /for=n, где n – буква, соответствующая системному разделу смонтированного образа).

Чтобы получить доступ к файлам, необходимо создать ссылку на интересующую эксперта теневую копию. Сделать это можно при помощи команды mklink (например, mklink /d C:\<точка монтирования> \\?\GLOBALROOT\Device\HarddiskVolume ShadowCopy\, значение после точки монтирования можно скопировать из вывода vssadmin). После этого можно осуществлять действия с хранящимися в теневой копии файлами.

**Заключение**

В настоящей статье были рассмотрены наиболее значимые с криминалистической точки зрения артефакты, появившиеся в Microsoft Windows 10, а также некоторые уже имевшие место, но не потерявшие своей актуальности.

**Примечания:**

1. Muir, B. Windows 10 - Cortana & Notification Center Forensics [Электронный ресурс]. 2015. URL: http://bsmuir.kinja.com/windows-10-cortana-notification-center-forenics-1724511442

2. Muir, B. Windows 10 - Microsoft Edge Browser Forensics [Электронный ресурс]. 2015. URL: http://bsmuir.kinja.com/windows-10-microsoft-edge-browser-forensics-1733533818

3. Picasso, F. A first look at Windows 10 prefetch files [Электронный ресурс]. 2015. URL: http://blog.digital-forensics.it/2015/06/a-first-look-at-windows-10-prefetch.html

4. Carvey, H. Windows Forensic Analysis Toolkit, 4th Edition. Advanced Analysis Techniques for Windows 8. Waltham: Syngress, 2014. 350 p.

**References:**

1. Muir, B. Windows 10 - Cortana & Notification Center Forensics [Электронный ресурс]. 2015. URL: http://bsmuir.kinja.com/windows-10-cortana-notification-center-forenics-1724511442

2. Muir, B. Windows 10 - Microsoft Edge Browser Forensics [Электронный ресурс]. 2015. URL: http://bsmuir.kinja.com/windows-10-microsoft-edge-browser-forensics-1733533818

3. Picasso, F. A first look at Windows 10 prefetch files [Электронный ресурс]. 2015. URL: http://blog.digital-forensics.it/2015/06/a-first-look-at-windows-10-prefetch.html

4. Carvey, H. Windows Forensic Analysis Toolkit, 4th Edition. Advanced Analysis Techniques for Windows 8. Waltham: Syngress, 2014. 350 p.

УДК 343.983.25

## Особенности криминалистического исследования цифровых артефактов в операционной системе Microsoft Windows 10

[1] Юрий Владимирович Найденышев
[2] Олег Владимирович Скулкин

[1] Сочинский государственный университет, Российская Федерация
Старший преподаватель

E-mail: krimex@yandex.ru
[2] Межрайонного отдела по г. Сочи и Туапсинскому району ЭКЦ ГУ МВД России по Краснодарскому краю, Российская Федерация
Эксперт
E-mail: skulkin@inbox.ru

**Аннотация.** В рамках данной статьи будут рассмотрены принципиально новые источники цифровых доказательств, характерные для новой версии рассматриваемой операционной системы, в частности Центр уведомлений, новый веб-браузер Microsoft Edge и цифровой персональный ассистент Cortana, а также некоторые уже имевшие место, но изменившие свой формат, например, Prefetch-файлы. Кроме того, будет подробно рассмотрен такой важнейший источник цифровых доказательств, появившийся еще во времена Windows XP, но имеющий место и в новой версии операционной системы – служба теневого копирования тома.

**Ключевые слова:** цифровая криминалистика, компьютерная криминалистика, криминалистическое исследование Microsoft Windows 10, Центр уведомлений Windows, браузер Microsoft Edge, цифровой персональный ассистент Cortana.