УДК 343.983 DOI: 10.18698/2541-8009-2021-04-693

ПОЛУЧЕНИЕ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ПРИ ИССЛЕДОВАНИИ РЕЕСТРА

А.П. Скачкова
n.skachkova.145@gmail.com
SPIN-код: 7564-0049

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Исследованы методы и средства изучения системного реестра операционной системы (ОС) Windows. Выделены разделы реестра ОС Windows, содержащие криминалистически значимую информацию. Приведен перечень специализированного программного обеспечения, который автоматизирует работу эксперта при исследовании реестра. Рассмотрены конкретные экспертные задачи, такие как определение даты установки ОС, определение зарегистрированных в ОС пользователей, формирование перечня подключаемых к компьютеру внешних накопителей, установление факта запуска прикладных программ с внешних устройств. Методические рекомендации, изложенные в работе по исследованию реестра ОС Windows, помогут быстрому и тщательному проведению экспертного исследования, что будет способствовать раскрытию, расследованию и предупреждению преступлений.

Ключевые слова

Реестр, операционная система, Windows, криминалистика, криминалистически значимая информация, программные средства, исследование, UNIX-система

Поступила в редакцию 02.02.2021

Актуальность темы обусловлена тем, что с каждым годом число преступлений, совершаемых с использованием компьютеров увеличивается, а значит, растет и потребность в судебной компьютерно-технической экспертизе электронных носителей информации. Эксперту необходимо изучить все особенности информационной среды, а также научиться применять определенные методы и средства выявления и изучения следов в программной среде, работающей под управлением операционной системы (ОС) Windows. Это позволит использовать возможности цифровой криминалистики для раскрытия и расследования преступлений [1]. Одним из таких методов является изучение следов в системном реестре ОС Windows.

Реестр является компонентом ОС Windows и содержит значимую информацию о конфигурации системы. Кроме того, в реестре хранится информация о работе пользователя; также реестр содержит подробные сведения об установленных и запускаемых на выполнение приложениях и о подключаемых устройствах. Таким образом, системный реестр — иерархически организованная база данных параметров и настроек ОС Windows [2,3]. В этой базе данных можно найти огромное количество криминалистически значимой информации, а значит, каждому эксперту необходимо улучшать навыки поиска необходимой криминалистической информации в реестре ОС.

Рассмотрим основные задачи, которые судебный компьютерно-технический эксперт может решить посредством исследования системного реестра ОС Windows:

– определение даты установки ОС;

– определение зарегистрированных в ОС пользователей;

– формирования перечня подключаемых к компьютеру внешних накопителей;

– установление факта запуска с внешних устройств прикладных программ [4].

Реестр ОС Windows состоит из пяти ветвей:

– HKEY_CLASSES_ROOT — сведения, необходимые для запуска установленных в системе программ;

– HKEY_CURRENT_USER — информация о текущем пользователе компьютера, его личных настройках и файлах;

– HKEY_LOCAL_MACHINE — сведения об аппаратной части компьютера, подключенных устройствах и их драйверах;

– HKEY_USERS — данные обо всех профилях пользователей операционной системы;

– HKEY_CURRENT_CONFIG — информация о профиле оборудования, которое компьютер использует при запуске системы [2].

В ОС Windows 7 информацию о расположении файлов основных кустов реестра можно просмотреть с помощью редактора реестра. Файлы реестра располагаются также в каталоге \Windows\system32\config и имеют такие же имена.

Для определения даты и времени последнего крупного обновления ОС на работающем компьютере удобнее использовать команду systeminfo. Однако для исследования неработающего компьютера следует использовать ветку системного реестра Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\WindowsNT\ CurrentVersion, в которой содержится значения времени и даты установки последнего крупного обновления операционной системы (рис. 1). Данные содержатся в формате UNIX-системы (принята в Unix и других POSIX-совместимых операционных системах). Определяется как количество секунд, прошедших с полуночи (00:00:00 UTC) 1 января 1970 г. (четверг); этот момент называют «эпохой Unix» (англ. Unix Epoch) [5]. «Unix-время» представлено целым числом, которое увеличивается с каждой прошедшей секундой без необходимости вычислений для определения года, месяца, дня, часа или минуты для удобства восприятия человеком.

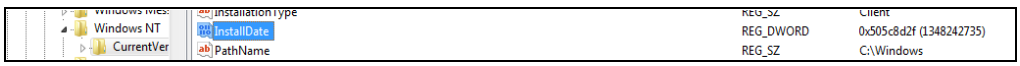

Рис. 1. Дата последнего крупного обновления и ее числовое значение

Для интерпретации полученного значения используем онлайн-ресурс epochconverter.com (рис. 2) [3].

На основе этих данных выявлена дата последнего крупного обновления — 21 сентября 2012 г. Многие считают эту дату датой установки ОС, но это не так. Дату установки ОС можно узнать по дате создания файла system.ini. Это файл

конфигурации ОС, который используется для хранения настроек компьютера (рис. 3). Данный файл можно найти, используя путь C:/Windows.

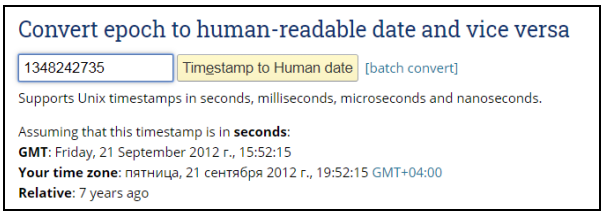

Рис. 2. Конвертирование значения даты и времени из формата Unix в наглядный вид

Рис. 3. Дата создания файла system.ini

Следующая задача, которая может быть поставлена перед экспертом, — определение зарегистрированных пользователей в данной ОС. Так, имеется один пользователь: «Администратор» (рис. 4). Путь к соответствующей ветке реестра имеет вид \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\.

Рис. 4. Информация о пользователе «Администратор»

Информация о подключенных ранее устройствах хранится в следующих ветках:
– HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR;
– HKLM\SYSTEM\CurrentControlSet\Enum\USB;
– HKLM\SYSTEM\MountedDevices.
Пример такой информации приведен на рис. 5.

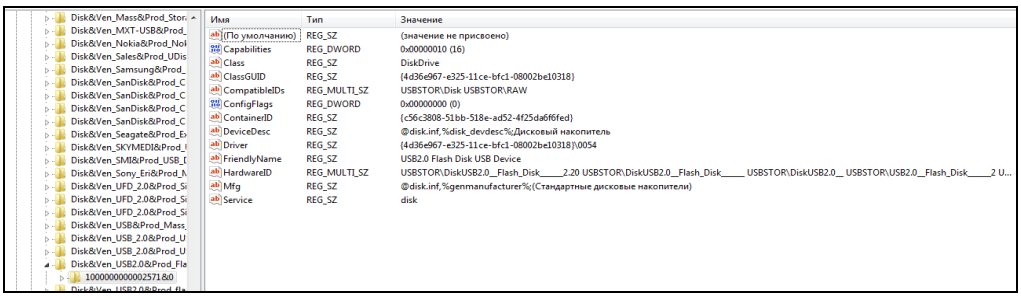

Рис. 5. Информация об устройстве USB 2.0

Следующая задача — установление факта запуска с внешних устройств прикладных программ. Каждая запущенная GUI-программа Windows оставляет запись в ключе реестра HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\UserAssist\{GUID}\Coun. Этот ключ содержит два подраздела GUID (запуск исполняемого файла CEBFF5CD, запуск файла ярлыков F4E57C4B); каждый подраздел поддерживает список системных объектов, таких как программы, ярлыки, к которым пользователь обратился. Значения реестра в этих подразделах зашифрованы не лучшим образом. Используется шифрование ROT-13, которое заменяет один символ другим, расположенным в 13-й позиции от него в таблице ASCII. Все значения кодируются ROT-13: .exe = .RKR .lnk = .YAX (рис. 6).

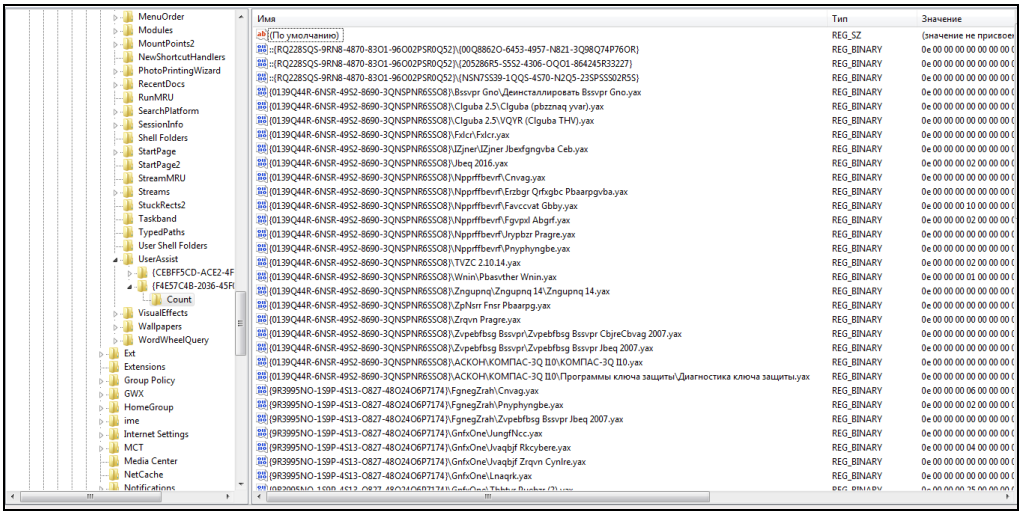

Рис. 6. Перечень программ, запуск которых выполнялся с различных устройств

Для изучения реестра имеется большое количество специализированного программного обеспечения (ПО). Самыми распространенными являются программные продукты System Mechanic [6], Ace Utilities [7], jv16 PowerTools [8], Registry Mechanic [9], Registrar Registry Manage [10]. Цель данного ПО — извлечение криминалистически значимой информации из реестра ОС Windows. Например, приложение System Mechanic обладает следующими преимуществами: позволяет выполнить быстрый и подробный анализ персонального компьютера (занял 2 мин), имеет удобный интерфейс, обладает возможностью извлечения криминалистически значимой информации — журнала браузера (рис. 7).

Главным преимуществом программы Ace Utilities является наличие команды Remove Junk File (удалить файлы, «засоряющие» систему). Данная команда позволяет удалить следы работы как в самом браузере, так и в реестре ПК. В программе jv16 powertools представлена общая информация о реестре, разбитая на определенные колонки. Это, конечно, удобно, но здесь отсутствует подробная информация, необходимая эксперту [6–10].

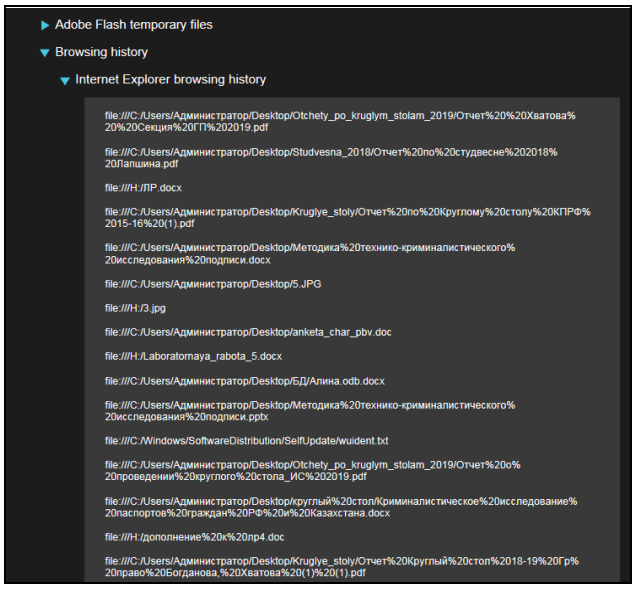

Рис. 7. Анализ журнала браузера на исследуемом компьютере

На основе вышеизложенного можно сделать вывод о том, что в ходе исследования реестра ОС Windows могут быть получены различные данные об активности пользователя в системе (дата и время инсталляции, сведения об установленном ПО, устройствах, подключаемых к компьютеру, и др.). Поиск указанных категорий данных может быть осуществлен как с помощью стандартных средств ОС (редактор реестра) работающего компьютера, так и с помощью специализированного ПО [11]. Поэтому необходимы методические рекомендации, которые помогут эксперту при решении задач судебной компьютерно-технической экспертизы. Данные методические рекомендации по исследованию реестра ОС Windows помогут быстрому и тщательному проведению экспертного исследования, что будет способствовать раскрытию расследованию и предупреждению преступлений.

Литература

[1] Яковлев А.Н. Цифровая криминалистика и ее значение для расследования преступлений в современном информационном обществе. *Совершенствование следственной деятельности в условиях информатизации. Сб. мат. межд. науч.-практ. конф.* Минск, Промышленно-торговое право, 2018, с. 357–362.

[2] Карлова А.В. Установление обстоятельств работы с USB-устройствами в операционной системе Windows. *Политехнический молодежный журнал*, 2019, № 4. DOI: http://dx.doi.org/10.18698/2541-8009-2019-4-465

[3] Карлова А.В. Некоторые особенности исследования графических файлов в шестнадцатеричном формате. *Политехнический молодежный журнал*, 2019, № 7. DOI: http://dx.doi.org/ 10.18698/2541-8009-2019-7-501

[4] Усов А.И. Межпрофессиональное сотрудничество как основное направление взаимодействия зарубежного судебно-экспертного сообщества. *Теория и практика судебной экспертизы*, 2017, т. 12, № 4, с. 106–109. DOI: https://doi.org/10.30764/1819-2785-2017-12-4-27-33

[5] Epoch & Unix timestamp conversion tools: веб-сайт. URL: https://www.unixtimestamp.com/ (дата обращения: 30.01.2020).
[6] New system mechanic ultimate defense: веб-сайт. URL: https://www.iolo.com (дата обращения: 30.01.2020).
[7] Ace utilities. *softportal.com: веб-сайт.* URL: https://www.softportal.com/software-1224-ace-utilities.html (дата обращения: 22.02.2020).
[8] Jv16 PowerTools: веб-сайт. URL: https://jv16powertools.com/ (дата обращения: 22.02.2020).
[9] Registry mechanic: веб-сайт. URL: https://registry-mechanic.ru.softonic.com (дата обращения: 22.02.2020).
[10] Registrar registry manager. *softportal.com: веб-сайт.* URL: https://www.softportal.com/software-25445-registrar-registry-manager.html (дата обращения: 22.02.2020).
[11] Вехов В.Б. Проблемы работы с электронными доказательствами. *Сб. мат. межд. конф. Современное уголовно-процессуальное право России: уроки истории и проблемы дальнейшего реформирования.* Орел, ОрЮИ МВД России, 2016, с. 84–87.

Скачкова Анастасия Петровна — студентка кафедры «Цифровая криминалистика», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — А.В. Карлова, ассистент кафедры «Цифровая криминалистика», МГТУ им. Н.Э. Баумана, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Скачкова А.П. Получение криминалистически значимой информации при исследовании реестра. *Политехнический молодежный журнал*, 2021, № 04(57). http://dx.doi.org/10.18698/ 2541-8009-2021-04-693

OBTAINING FORENSIC INFORMATION WHEN EXAMINING THE REGISTRY

A.P. Skachkova

n.skachkova.145@gmail.com
SPIN-code: 7564-0049

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper is devoted to the methods and means of studying the system registry of the Windows operating system (OS). Windows registry keys containing forensic information are highlighted. A list of specialized software that automates the work of an expert when examining the registry is given. Specific expert tasks are considered, such as determining the date of the OS installation, determining the users registered in the OS, forming a list of external drives connected to the computer, establishing the fact of launching application programs from external devices. The methodological recommendations to Windows registry outlined in the work will help to quickly and thoroughly conduct expert research, which will contribute to the detection, investigation and prevention of crimes

Keywords

Registry, operating system, Windows, forensics, forensic information, software, research, UNIX system

Received 02.02.2021

References

[1] Yakovlev A.N. [Digital criminalistics and its significance for crime investigation]. *Sovershenstvovanie sledstvennoy deyatel'nosti v usloviyakh informatizatsii. Sb. mat. mezhd. nauch.-prakt. konf.* [Improvement of Investigative Activities in Conditions of Informatization. Proc. Int. Sci.-Pract. Conf.]. Minsk, Promyshlenno-torgovoe pravo Publ., 2018, pp. 357–362 (in Russ.).

[2] Karlova A.V. Establishing the circumstances of working with USB-devices in the Windows operating system. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical Student Journal], 2019, no. 4. DOI: http://dx.doi.org/10.18698/2541-8009-2019-4-465 (in Russ.).

[3] Karlova A.V. Some features of study of image files in hexadecimal format. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical Student Journal], 2019, no. 7. DOI: http://dx.doi.org/10.18698/ 2541-8009-2019-7-501 (in Russ.).

[4] Usov A.I. Inter-professional collaboration as the main cooperation trend in the international forensic community. *Teoriya i praktika sudebnoy ekspertizy* [Theory and Practice of Forensic Science], 2017, vol. 12, no. 4, pp. 106–109. DOI: https://doi.org/10.30764/1819-2785-2017-12-4-27-33 (in Russ.).

[5] Epoch & Unix timestamp conversion tools: website. URL: https://www.unixtimestamp.com (accessed: 30.01.2020).

[6] New system mechanic ultimate defense: website. URL: https://www.iolo.com (accessed: 30.01.2020).

[7] Ace utilities. *softportal.com: website* (in Russ.). URL: https://www.softportal.com/ software-1224-ace-utilities.html (accessed: 22.02.2020).

[8] Jv16 PowerTools: website. URL: https://jv16powertools.com (accessed: 22.02.2020).
[9] Registry mechanic: website. URL: https://registry-mechanic.ru.softonic.com (accessed: 22.02.2020).
[10] Registrar registry manager. *softportal.com: website* (in Russ.). URL: https://www.softportal.com/software-25445-registrar-registry-manager.html (accessed: 22.02.2020).
[11] Vekhov V.B. [Problems of work with digital evidences]. *Sb. mat. mezhd. konf. Sovremennoe ugolovno-protsessual'noe pravo Rossii: uroki istorii i problemy dal'neyshego reformirovaniya* [Proc. Int. Conf. Modern Criminal Procedure Law of Russia: History Lessons and Problems of Further Reforming]. Orel, OrYuI MVD Rossii Publ., 2016, pp. 84–87 (in Russ.).

Skachkova A.P. — Student, Department of Digital Forensics, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Karlova A.V., Assistant, Department of Digital Forensics, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Skachkova A.P. Obtaining forensic information when examining the registry. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2021, no. 04(57). http://dx.doi.org/10.18698/2541-8009-2021-04-693.html (in Russ.).