УДК 343.983 DOI: 10.18698/2541-8009-2019-04-465

УСТАНОВЛЕНИЕ ОБСТОЯТЕЛЬСТВ РАБОТЫ С USB-УСТРОЙСТВАМИ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

А.В. Карлова carlova.anastasia@yandex.ru
SPIN-код: 8696-6670

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

Аннотация

Исследованы факты использования USB-устройств с помощью реестра операционной системы Windows, а также специализированного программного обеспечения. Выделены разделы реестра операционной системы Windows, которые содержат криминалистически значимую информацию про подключенные USB-устройства, а также журналы событий. Приведен перечень специализированного программного обеспечения, который автоматизирует работу эксперта при исследовании факта использования USB-устройств. Разработаны методические рекомендации для экспертов в области судебной компьютерно-технической экспертизы для ответа на вопросы о том, какие USB-устройства, когда и кем подключались к исследуемому компьютеру.

Ключевые слова

Реестр операционной системы, USB-устройства, институт SANS, VID и PID USB-устройства, GUID, использование USB-устройства, Windows Registry Recovery, USB Deview, Windows Registry Analyser, Last Activity View

Поступила в редакцию 21.02.2019

Введение. Ни для кого уже не секрет, что информация о разного рода активности многочисленных компонентов операционной системы попадает в реестр. Из всего многообразия подобной информации в рамках данной статьи нас будет интересовать история использования USB-устройств. Данные устройства сразу стали источником проблем как для безопасности персональных данных самого пользователя, так и безопасности компаний. Если порты USB находятся без надлежащего контроля, то любое приспособление может послужить средством обхода безопасности и кражи конфиденциальной информации. Поэтому в случае возникновения инцидента информационной безопасности, связанного с эксплуатацией USB-устройств, все действия с USB-устройствами могут рассматриваться как доказательная база при возникновении преступления. В связи со всем перечисленным достаточно важно иметь доступ к истории USB-подключений в системе.

Актуальность данной темы обусловлена тем, что современная преступность приобрела качественно новые формы, значительно возросло число компьютерных преступлений, в большинстве случаев перед судебным экспертом ставится вопрос: «Какие USB-устройства подключались к исследуемому компьютеру?». Обычно данные устройства используют для кражи данных либо внедрения вредоносных программ [1]. Отметим, что в настоящее время технико-криминалистическое и ин-

формационно-компьютерное обеспечение выявления, раскрытия, расследования и предупреждения этих преступлений находится в стадии разработки; не закончен процесс формирования криминалистических рекомендаций по тактике подготовки и производства отдельных следственных действий, связанных с обнаружением, фиксацией, изъятием и исследованием компьютерной информации и средств ее обработки [2, с. 14]. Информацию об использовании USB-устройств можно выявить при изучении системного реестра Windows.

Реестр Windows является основным компонентом операционной системы Windows и содержит значительную информацию о конфигурации системы. Кроме того, в реестре хранится историческая информация о деятельности пользователя; реестр содержит подробные сведения об установленных и открытых приложениях, а также о подключаемых устройствах. Таким образом, системный реестр — иерархически построенная база данных параметров и настроек операционной системы Windows.

Вся эта информация может быть чрезвычайно ценной для судебного эксперта, особенно при попытке установить временной интервал активности пользователя в системе. Однако данная информация может быть полезна только в том случае, если судебный эксперт знает об ее существовании и о том, как ее найти или использовать [3, с. 19].

Среди всего многообразия подобной информации в рамках данной статьи нас будет интересовать исключительно история использования USB-устройств. Следы подключения USB-устройств, содержащиеся в виде различных данных в файлах/реестре, принято называть *артефактами*. Система создает артефакты в момент обнаружения (инициализации) устройства (сменных накопителей, модемов и иных устройств) в системном реестре.

Реестр Windows состоит из пяти ветвей [4]:

– 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 для запуска системы.

Физически системный реестр Windows находится в папке Windows\System32\config.

Американский институт SANS (SysAdmin, Audit, Network, Security) подготовил плакат, содержащий категории артефактов, которые имеют доказательственное значение.

Институт SANS был создан в 1989 г. в качестве исследовательской и образовательной организации. Он разрабатывает, поддерживает и бесплатно предо-

ставляет самую большую коллекцию исследовательских документов по различным аспектам информационной безопасности [5]. В плакате SANS выделены следующие артефакты.

Идентификация устройства. Абсолютно все без исключения когда-либо пронумерованные устройства, подключаемые к компьютеру и конфигурируемые PnP-менеджером, отображаются в ветви реестра HKLM\System\CurrentControlSet\Enum.

Подключ USB содержит подключи, описывающие вообще все пронумерованные USB-устройства системы. В подключе USBSTOR отображаются подключаемые накопители с интерфейсом USB [6, с. 607].

Информация о USB-устройствах, подключенных к исследуемому компьютеру, находится в ветви HKEY_LOCAL_MACHINE:

– SYSTEM\CurrentControlSet\Enum\USB

– SYSTEM\CurrentControlSet\Enum\USBSTOR

С помощью данных параметров можно определить производителя, уникальное USB-устройство, время подключения. Во-первых, под ключом Enum\USBSTOR можно найти, где указаны устройства, сначала ключ, известный как идентификатор класса устройства (ID) и уникальный идентификатор экземпляра, как показано на рис. 1.

Как показано на рис. 2, идентификатор класса устройства дает немного информации самом устройстве (в этом случае устройство представляет собой накопитель компании Seagate объемом 500 Гб). Под идентификатором класса устройства понимают два уникальных идентификатора (VID и PID). В каждом случае уникальный идентификатор экземпляра содержит информацию об устройствах в данных реестра, включая устройство FriendlyName (ST950032 5A2 USB Drive). VID (Vendor ID) — это идентификатор производителя устройства. При присвоении идентификатора производителя соответствующее числовое значение вносится в реестр производителей. PID (Product ID) представляет собой идентификатор продукта и назначается производителем устройства. PID используется для дифференциации продуктов в рамках одного производителя [7].

Рис. 1. USB-устройство в ключе Enum\USBSTOR

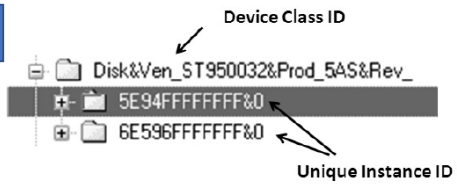


Рис. 2. USB-устройство в ключе Enum\USBSTOR

Однако не каждое USB-устройство имеет серийный номер. В таких случаях Windows назначает уникальный идентификатор экземпляра на устройство. Чтобы выяснить это, нужно посмотреть на уникальный идентификатор экземпляра для устройства. Если второй символ идентификатора — &, то этот уни-

кальный идентификатор экземпляра был создан и назначен операционной системой, а не извлечен из дескриптора устройства (рис. 3). Дескрипторы USB — структуры данных, которые позволяют операционной системе получить информацию об устройстве. Каждый дескриптор содержит информацию об устройстве в целом или об отдельном элементе в рамках устройства.

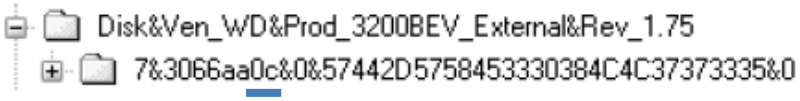


Рис. 3. Уникальный идентификатор экземпляра USB-устройства, созданный операционной системой

Таким образом, каждое USB устройство должно иметь как минимум идентификатор производителя (VID), идентификатор продукта (PID), и серийный номер (Serial). На основе этих параметров формируется уникальный идентификатор оборудования, тем самым обеспечивается уникализация USB-устройства в пределах системы и вносятся изменения в конфигурацию оборудования (рис. 4) [8].

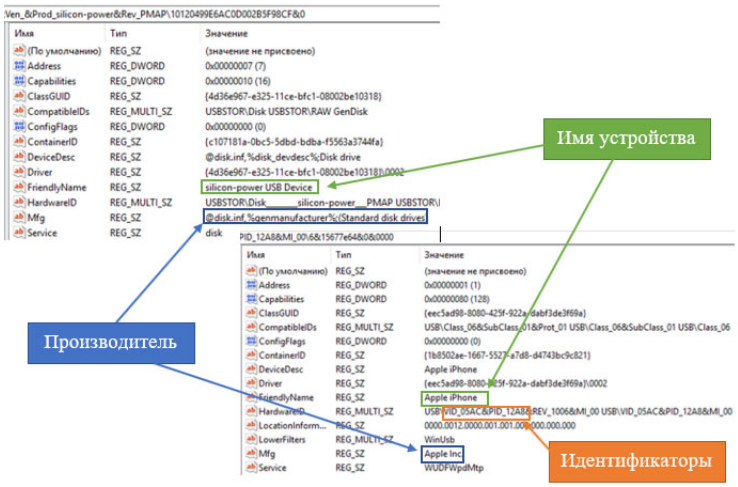


Рис. 4. Значение параметров USB-устройств

После того как у устройства запрошены ключевые параметры, для USB-устройства создается уникальный идентификатор HardwareID (CompatibleID), однозначно идентифицирующий устройство/класс устройства. Драйвер USB-устройства уведомляет специализированный модуль ядра — диспетчер Plug-n-Play (PnP Manager) — о новом устройстве. Диспетчер PnP получает идентификаторы HardwareID и CompatibleID устройства и пытается обнаружить устройства с аналогичными идентификаторами HardwareID/CompatibleID. В этот момент в системе создается узел устройства, что является, по сути, первым отпечатком USB-устройства в системе [9, с. 143].

Представленные выше параметры и их значения фактически формируют отпечаток для каждого USB-устройства, поскольку следы подключения USB-

устройства в системе Windows состоят из подобных уникальных значений/названий.

Первое и последнее использование устройства. Дату первого использования в версии операционной системы Windows XP можно найти по пути C:\Windows\setupapi.log, а в версии Windows 7/8/10 — C:\Windows\inf\setupapi.dev.log (рис. 5) [10], либо в следующем кусте системного реестра: \CurrentControlSet\Enum\USBSTOR\Ven_ Prod_Version\USB.

```
>>>  [Device Install (Hardware initiated) - USB\VID_04E8&PID_6860\41075e737a167f8d]
>>>  Section start 2018/07/11 14:11:58.444
     dvi: {Build Driver List} 14:11:58.464
     dvi:      Searching for hardware ID(s):
     dvi:           usb\vid_04e8&pid_6860&rev_0400
     dvi:           usb\vid_04e8&pid_6860
     dvi:      Searching for compatible ID(s):
     dvi:           usb\ms_comp_mtp
     dvi:           usb\class_06&subclass_01&prot_01
     dvi:           usb\class_06&subclass_01
     dvi:           usb\class_06
     dvi:      Created Driver Node:
     dvi:           HardwareID   - USB\MS_COMP_MTP
     dvi:           InfName      - C:\WINDOWS\System32\DriverStore\FileRepository
\wpdmtp.inf_amd64_79762cfde1a9fe38\wpdmtp.inf
     dvi:           DevDesc      - USB -устройство MTP
     dvi:           Section      - MTP.NT
     dvi:           Rank         - 0x00ff2000
     dvi:           Signer Score - INBOX
     dvi:           DrvDate      - 06/21/2006
     dvi:           Version      - 10.0.17134.1
     dvi:      Created Driver Node:
     dvi:           HardwareID   - USB\Class_06&SubClass_01&Prot_01
     dvi:           InfName      - C:\WINDOWS\System32\DriverStore\FileRepository
```

Рис. 5. Фрагмент файла setupapi.dev.log, содержащий дату первого использования USB-устройства

Пользователь, который использовал USB-устройство. Чтобы выявить пользователя, который использовал USB-устройство, необходимо посмотреть идентификатор GUID пользователя в SYSTEM\MountedDevices. GUID — статистически уникальный 128-битный идентификатор. Его главной особенностью является уникальность, которая позволяет создавать расширяемые сервисы и приложения, не опасаясь возникновения конфликтов, вызванных совпадением идентификаторов. В более ранних версиях операционной системы можно выявить пользователя с помощью пути HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\.

Этот идентификатор GUID будет использоваться рядом с именем пользователя, подключенного к устройству. Последнее время записи этого ключа также соответствует последнему времени, когда устройство было подключено к машине этим пользователем.

Куст HKEY_ CURRENT_USER предназначен для хранения данных, специфичных для конкретного пользователя, зарегистрированного в системе.

Имя тома. В реестре присутствует ключ HKLM\SYSTEM\MountedDevices, который содержит подключи, описывающие все когда-либо смонтированные в системе накопители (рис. 6). Имеют тип REG_BINARY и содержат в своем значении информацию (UTF) о пути, наименовании и GUID накопителя. К тому же, в этом же ключе присутствуют такие интересные параметры как \DosDevices\X:, где

буква (X:) после обратного слеша означает имя тома. Параметров может быть несколько, обычно по количеству подключенных в системе букв дисков. У всех этих параметров значением будет путь к последнему сопоставленному с данной литерой физическому устройству.

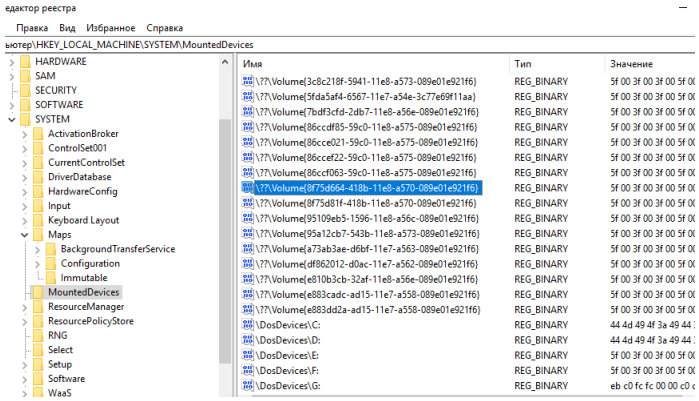


Рис. 6. Информация о пользователях, использующих USB-устройство в ключе SYSTEM\MountedDevices

В версии операционной системы Windows XP можно найти следующие подразделы:

– SYSTEM\CurrentControlSet\Enum\USBSTOR;

– SYSTEM\MountedDevices;

а в версии Windows 7/8/10:

– SOFTWARE\Microsoft\Windows Portable Devices\Devices;

– SYSTEM\MountedDevices (рис. 7).

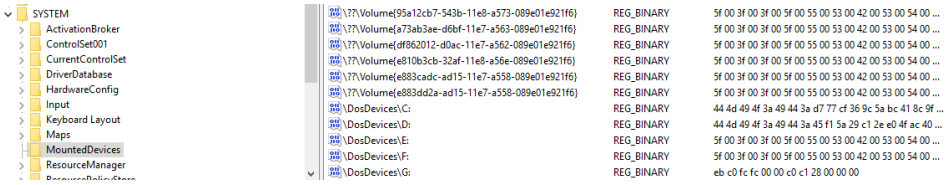


Рис. 7. Наименования USB-устройств ключе SYSTEM\MountedDevices

Возможно определение USB-устройства, которое было последним сопоставлено с конкретной буквой диска. Этот метод будет работать только для отображения последнего диска. Он не содержит исторических записей каждой буквы диска, сопоставленной со съемным диском.

Файлы ярлыков (LNK). Открытие локальных и удаленных файлов данных и документов приведет к созданию файла ярлыков (.lnk). Чтобы узнать название подключаемых USB-устройств, необходимо перейти по следующим ссылкам:

– %USERPROFILE%\Recent (Windows XP);

– %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent (Win7/8/10) (рис. 8).

Можно выявить следующие обстоятельства:
– дату создания ярлыка (LNK);
– дату последнего подключения.

Рис. 8. USB-устройства и дата их подключения к исследуемому компьютеру

События PnP. При попытке установки драйвера PnP служба будет регистрировать событие с ID: 20001 (рис. 9). Отметим, что это событие будет запускаться для любого устройства, поддерживающего PnP.

Можем просмотреть данные события через файл журнала событий: %systemroot%\System32\winevt\logs\System.evtx (Win7/8/10) (рис. 10). В данном файле содержится информация об устройстве, его серийный номер, состояние (0 — нет ошибок) [3].

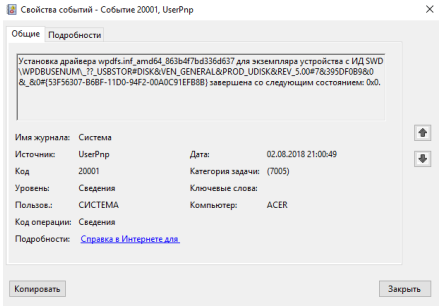


Рис. 9. Свойства события 20001, UserPnp

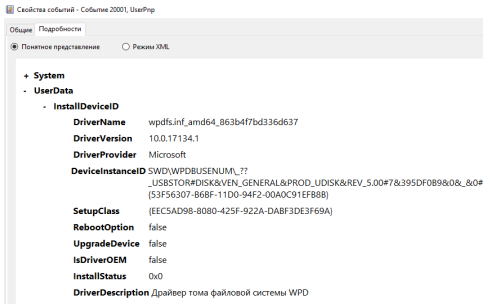
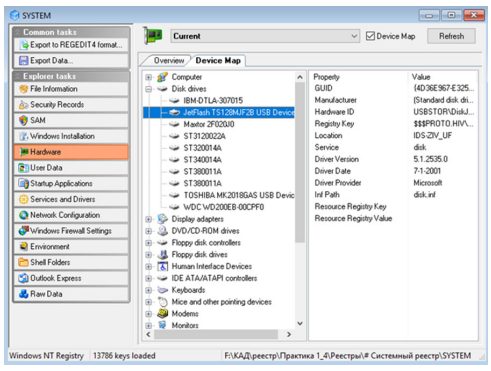


Рис. 10. Полное представление о событии, содержащее информацию о USB-устройстве

Программное обеспечение для выявления подключенных USB-устройств и работы с ними. *Windows Registry Recovery* — программа для просмотра файлов реестра операционной системы Windows, содержимое открытого файла отображается в виде стандартного оформления программы RegEdit (рис. 11) [11].

Рис. 11. USB-устройства, которые были подключены, программа Windows Registry Recovery



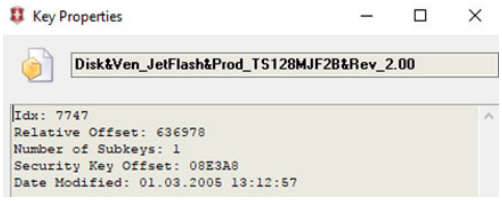


Рис. 12. Информация о USB-устройстве в программе Windows Registry Recovery

Чтобы увидеть дату последнего подключения, нужно перейти во вкладку Properties (рис. 12).

С помощью данной программы можно выявить все подключенные USB-устройства, идентификатор GUID пользователя, который применял данное устройство, а также дату первого и последнего подключения устройства, наименование/описание устройства.

Для просмотра информации о подключенных устройствах можно использовать утилиту USBDeview [12]. Для каждого устройства программа показывает: дату и время, когда устройство было добавлено, и время последнего подключения, наименование/описание устройства, серийный номер, производителя и т. д. (рис. 13). Однако данная утилита работает только с активным реестром.

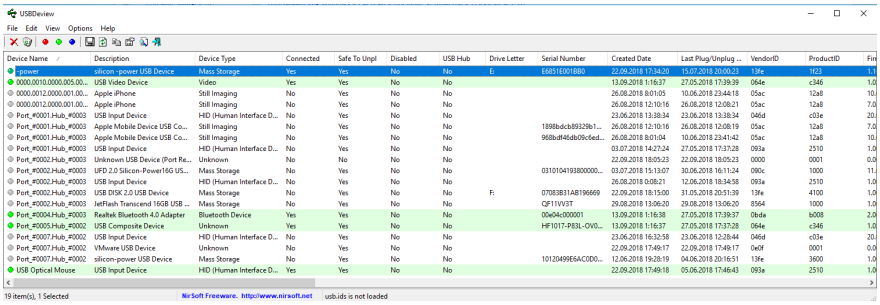


Рис. 13. Подключенные к исследуемому компьютеру устройства. Окно программы USBDeview

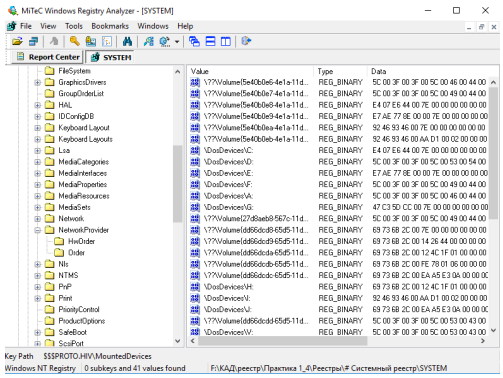


Рис. 14. Загрузка ветви SYSTEM в программу Windows Registry Analyzer

Утилита Windows Registry Analyser позволяет работать с неактивным реестром, необходимо загрузить файл с ранее сохраненными данными реестра [13]. Эта программа дает возможность просмотреть содержимое папок данной ветви реестра (рис. 14).

Чтобы увидеть программ и файлы, которые открывались с этих носителей, используем утилиту LastActivityView. Она предназначена для сбора информации об активности пользователя компьютера и отображения журнала событий [14]. Программа позволяет узнать, какие исполнительные файлы запускались, время данного события, сведения о времени включения и выключения компьютера, используемые сетевые подключения и устанавливаемые приложения и т. п. (рис. 15).

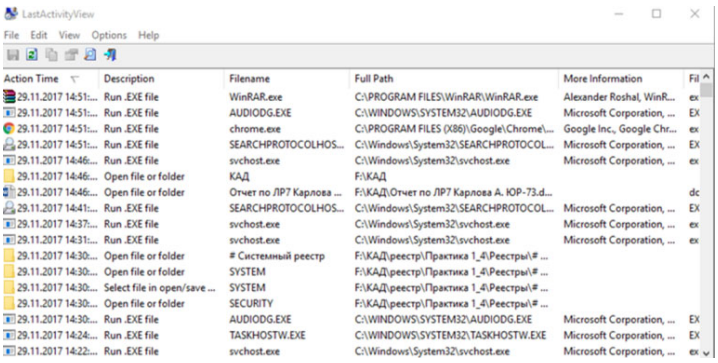


Рис. 15. Все устройства и открываемые с них файлы в программе LastActivityView

В результате проведения анализа различных методик подготовлены рекомендации по действиям эксперта для решения следующих вопросов: какие USB-устройства были подключены к исследуемому компьютеру и какую информацию можно получить: серийный номер устройства (VID, PID); дату подключения; имя тома, под которым оно было подключено; а также каким конкретно пользователем. Перечисленные программы позволяют существенно ускорить производство компьютерных экспертиз для выявления подключаемых USB-устройств. Данное программное обеспечение повысило скорость и качество проведения экспертиз.

Результаты, которые выдает программа, максимально приближены к той форме, которая удобна для копирования с целью размещения в заключении эксперта или справке специалиста. Однако любая программа — лишь инструмент в руках профессионала. Каждый эксперт или специалист должен понимать, что в случае возникновения сомнений он может перепроверить полученные результаты с помощью других программных средств или вручную (методику мы показали в данной статье), поскольку заключение дает и несет ответственность за него именно человек, а не программа.

Литература

[1] Akhmadieva R.Sh., Ignatova L.N., Bolkina G.I., et al. An attitude of citizens to state control over the internet traffic. *EJAC*, 2018, vol. 13, no. 1, art. em82. DOI: 10.29333/ejac/102247 URL: http://www.eurasianjournals.com/An-Attitude-of-Citizens-to-State-Control-Over-the-Internet-Traffic,102247,0,2.html

[2] Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Волгоград, ВА МВД России, 2008.

[3] Буренина В.И. Система законодательства, регулирующего научно-техническую деятельность: проблемы и противоречия. *Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики*, 2013, № 9-1(35), с. 19–24.

[4] Что такое реестр Windows 10/8/7? *it-uroki.ru: веб-сайт*. URL: http://it-uroki.ru/uroki/opytnyj-polzovatel/chto-takoe-reestr-windows.html (дата обращения: 21.09.2018).

[5] Windows forensic analysis — SANS. *sans.org: веб-сайт*. URL: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (дата обращения: 21.09.2018).
[6] Буренина В.И., Арсенькина Л.С. Применение технических средств обучения в современном образовательном процессе. *Будущее машиностроения России*. М., МГТУ им. Н.Э. Баумана, 2008, с. 607–609.
[7] Shaaban A., Sapronov K. Practical windows forensics. Packt Publishing, 2016.
[8] Carvey H. Windows registry forensics: advanced digital forensic analysis of the windows registry. Elsevier, 2011.
[9] Буренина В.И. Научно-техническая деятельность как объект государственного управления. *Евразийский юридический журнал*, 2012, № 12(55), с. 142–144.
[10] USB devices in Windows forensic analysis. *andreafortuna.org: веб-сайт*. URL: https://www.andreafortuna.org/forensics/usb-devices-in-windows-forensic-analysis/ (дата обращения: 21.09.2018).
[11] Windows registry recovery. *techworld.com: веб-сайт*. URL: https://www.techworld.com/download/backup-recovery/windows-registry-recovery-155-3214253/ (дата обращения: 21.09.2018).
[12] USBDeview v2.80. *nirsoft.net: веб-сайт*. URL: https://www.nirsoft.net/utils/usb_devices_view.html (дата обращения: 21.09.2018).
[13] Free registry analyzer for Windows XP, Vista, 7, 8 and 10. *new-utilities.net: веб-сайт*. URL: http://www.new-utilities.net/nt_registry_analyzer.html (дата обращения: 21.09.2018).
[14] LastActivityView v1.32. *nirsoft.net: веб-сайт*. URL: https://www.nirsoft.net/utils/computer_activity_view.html (дата обращения: 21.09.2018).

Карлова Анастасия Владимировна — студентка кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

ESTABLISHING THE CIRCUMSTANCES OF WORKING WITH USB-DEVICES IN THE WINDOWS OPERATING SYSTEM

A.V. Carlova carlova.anastasia@yandex.ru
SPIN-code: 8696-6670

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper is concerned with the facts of the use of USB-devices using the registry of the Windows operating system, and specialized software. The author highlighted Windows registry keys that contain forensic information about connected USB-devices, and event logs. In this paper showed the list of specialized software that automates the work of an expert in the study of the use of USB-devices. In his paper the author developed guidelines foe experts in the field of forensic computer and technical expertise to answer questions about which USB-devices, when b who connected to the computer under investigation.

Keywords

Operating system registry, USB-devices, SANS institute, VID and PID USB-devices, GUID, use of USB-device, Windows Registry Recovery, USB Deview, Windows Registry Analyser, Last Activity View

Received 21.02.2019

References

[1] Akhmadieva R.Sh., Ignatova L.N., Bolkina G.I., et al. An attitude of citizens to state control over the internet traffic. *EJAC*, 2018, vol. 13, no. 1, art. em82. DOI: 10.29333/ejac/102247 URL: http://www.eurasianjournals.com/An-Attitude-of-Citizens-to-State-Control-Over-the-Internet-Traffic,102247,0,2.html

[2] Vekhov V.B. Osnovy kriminalisticheskogo ucheniya ob issledovanii i ispol'zovanii komp'yuternoy informatsii i sredstv ee obrabotki [Forensic theory fundamentals of research and usage of computer information and information-processing equipment]. Volgograd, VA MVD Rossii Publ., 2008 (in Russ.).

[3] Burenina V.I. System of legislation regulating scientific-technical activity: problems and contradictions. *Istoricheskie, filosofskie, politicheskie i yuridicheskie nauki, kul'turologiya i iskusstvovedenie. Voprosy teorii i praktiki* [Historical, philosophical, political and law sciences, culturology and study of art. Issues of Theory and Practice], 2013, no. 9-1(35), pp. 19–24 (in Russ.).

[4] Chto takoe reestr Windows 10/8/7? [What is Windows 10/8/7 register?]. *it-uroki.ru: website* (in Russ.). URL: http://it-uroki.ru/uroki/opytnyj-polzovatel/chto-takoe-reestr-windows.html (accessed: 21.09.2018).

[5] Windows forensic analysis - SANS. *sans.org: website*. URL: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (accessed: 21.09.2018).

[6] Burenina V.I., Arsen'kina L.S. Primenenie tekhnicheskikh sredstv obucheniya v sovremennom obrazovatel'nom protsesse [Using teaching techniques in contemporary teaching process]. *Budushchee mashinostroeniya Rossii* [Future of Russian machine engineering]. Moscow, Bauman MSTU Publ., 2008, pp. 607–609 (in Russ.).

[7] Shaaban A., Sapronov K. Practical windows forensics. Packt Publishing, 2016.

[8] Carvey H. Windows registry forensics: advanced digital forensic analysis of the windows registry. Elsevier, 2011.

[9] Burenina V.I. Scientific and technical activities as an object of state administration. *Evraziyskiy yuridicheskiy zhurnal* [Eurasian Law Journal], 2012, no. 12(55), pp. 142–144 (in Russ.).
[10] USB devices in Windows forensic analysis. *andreafortuna.org: website*. URL: https://www.andreafortuna.org/forensics/usb-devices-in-windows-forensic-analysis/ (accessed: 21.09.2018).
[11] Windows registry recovery. *techworld.com: website*. URL: https://www.techworld.com/download/backup-recovery/windows-registry-recovery-155-3214253/ (accessed: 21.09.2018).
[12] USBDeview v2.80. *nirsoft.net: website*. URL: https://www.nirsoft.net/utils/usb_devices_view.html (accessed: 21.09.2018).
[13] Free registry analyzer for Windows XP, Vista, 7, 8 and 10. *new-utilities.net: website*. URL: http://www.new-utilities.net/nt_registry_analyzer.html (accessed: 21.09.2018).
[14] LastActivityView v1.32. *nirsoft.net: website*. URL: https://www.nirsoft.net/utils/computer_activity_view.html (accessed: 21.09.2018).

Carlova A.V. — Student, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.