УДК 343.148.6 DOI: 10.18698/2541-8009-2017-12-215

ИССЛЕДОВАНИЕ USB-НАКОПИТЕЛЕЙ В РАБОТЕ СУДЕБНОГО КОМПЬЮТЕРНО-ТЕХНИЧЕСКОГО ЭКСПЕРТА

А.А. Павлова AnniaPavlova@yandex.ru

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

Аннотация

Рассмотрены USB-накопители, в частности, внутренние компоненты USB-устройства, современные комплексы, используемые в рамках производства судебной компьютерно-технической экспертизы при работе с USB-накопителями информации, а именно: аппаратно-программный комплекс PC-3000 flash, позволяющий восстановить данные с поврежденных USB-устройств, и программный комплекс Encase Forensic, который применяется для поиска, анализа и восстановления данных с USB-устройств.

Ключевые слова

USB-накопитель, судебная компьютерно-техническая экспертиза, программные средства, поврежденные устройства, восстановление данных, поиск данных

Поступила в редакцию 06.10.2017

Введение. Актуальность исследования USB-накопителей обусловлена их широким использованием в настоящее время, поскольку это наиболее удобные и практически незаменимые переносные устройства для хранения данных, которые способны сочетать в себе такие свойства, как компактность и возможность хранения большого объема информации. В связи с этим данные устройства нередко становятся объектами исследования при проведении судебной компьютерно-технической экспертизы, поскольку могут содержать криминалистически важную информацию.

USB-накопитель — это запоминающее устройство, используемое для хранения и записи данных с интегрированным интерфейсом USB [1]. Все данные записываются и хранятся в микросхеме памяти, для записи и чтения которых необходимо подключить USB-накопитель в любое считывающее устройство, где предусмотрен интерфейс USB [2].

Безусловно, на сегодняшний день USB-накопитель является одним из наиболее компактных и удобных запоминающих устройств, в котором отсутствуют движущиеся элементы, как в оптических или в жестких магнитных дисках. Это — набор микросхем, в чипах которых способна храниться цифровая информация, поэтому нет необходимости использовать батарейки или аккумуляторы при работе с устройством.

Кроме того, существует множество производителей данных устройств, выпускающих USB-накопители с различным объемом памяти (до 1 Тбайт) и различной пропускной способностью (USB 2.0, 3.0, 3.1 и др.).

Структура USB-накопителя. Устройство USB-накопителя может включать в себя до восьми составляющих элементов (рис. 1) [3].

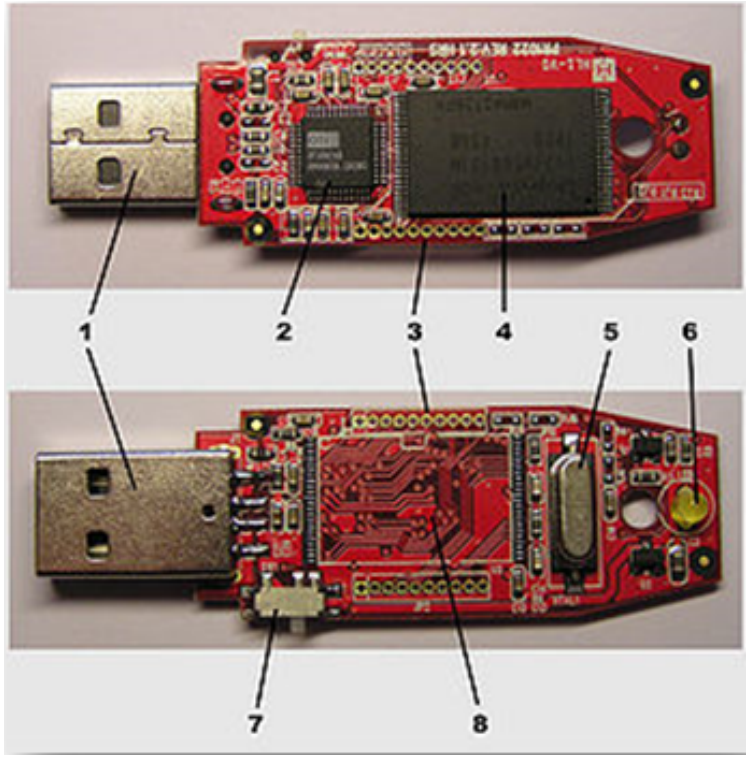

Рис. 1. Внутреннее строение USB-накопителя:

1 — разъем USB; *2* — микроконтроллер; *3* — контрольные точки; *4* — чип (микросхема) флэш-памяти; *5* — кварцевый резонатор; *6* — светодиод; *7* — переключатель (защита от записи); *8* — дополнительное место для микросхемы памяти

Следует отметить, что в современных USB-накопителях многие элементы имеют значительно меньший размер и впаяны непосредственно в саму конструкцию USB-устройства, которую полностью разобрать без повреждения работоспособности устройства не представляется возможным (рис 2). Такие элементы, как светодиод, защита от записи, дополнительное место для микросхемы памяти могут в USB-устройстве отсутствовать.

Рис. 2. Современный USB-накопитель в разобранном виде (производитель SAnDick Cruzer Facet; 2 Гбайта)

Рассмотрим подробнее составные части USB-накопителя (см. рис. 1). USB-разъем (интерфейс) предназначен для подключения USB-накопителя к устройствам чтения/записи, что обеспечивает физическое соединение устройства с компьютером. Наиболее чаще используются USB 2.0, USB 3.0, USB-C и microUSB. Основная разница стандартных USB-интерфейсов заключается в производительности и скорости, например, скорость USB 3.0 рассчитана на 4,8 Гбайта в секунду, что в 10 раз больше скорости USB 2.0 [4].

Любое взаимодействие USB-устройства с компьютером осуществляется с помощью микроконтроллера — микросхемы, которая управляет памятью и передает информацию [5]. В нем содержатся данные о производителе и типе памяти, хранится необходимая служебная информация, обеспечивающая правильное функционирование флэш-накопителя. Микроконтроллер — это «мозг» устройства, сочетающий функции процессора с интегрированными в микросхему устройствами ввода-вывода и оперативную память. Зачастую, именно по его вине происходит выход из строя флэш-накопителя. Одной из причин этого служит неправильное извлечение микроконтроллера из считывающего устройства.

Микросхема памяти — это энергонезависимая память, которая отвечает за хранение информации и может электрически стираться и перепрограммироваться [6]. Существует несколько технологий построения структуры USB-памяти, наиболее распространенными из которых являются NOR (NOT OR) и NAND (NOT AND). В USB-накопителях используется память типа NAND. В первую очередь это обусловлено тем, что сфера использования USB-памяти типа NOR применяется для хранения небольшого объема данных (до 256 Мбайт), что недопустимо при разработке USB-накопителей, в то время как USB-память типа NAND предназначена для хранения большого объема данных.

Кварцевый резонатор используется для построения опорной частоты, необходимой для функционирования логики контроллера и флэш-памяти. При выходе из строя компьютер определяет USB-накопитель как «неизвестное устройство» или просто его «не видит».

Светодиод не является обязательным и не влияет на внутреннюю работу USB-устройства, но позволяет определить его исправность, поскольку при подключении к компьютеру загорается световой индикатор, а также он мигает при обращении к диску (в процессе записи или чтения) [7].

Некоторыми производителями USB-накопителей реализуется механическая защита от изменений в виде переключателя (защита от записи), разрешающего или запрещающего запись. Обычно он располагается на боковой части носителя и отмечается значком замка. Для снятия механической блокировки необходимо передвинуть рычаг в противоположное направление [8].

Экспертные исследования, проводимые судебным компьютерно-техническим экспертом, обеспечивают получение результатов, имеющих наибольшее доказательственное значение при расследовании преступлений [9].

Следует отметить, что в последнее время законодатель стал уделять повышенное внимание электронным доказательствам, в том числе особенностям ра-

боты с ними [10] и все чаще по уголовным делам стали использоваться электронные доказательства [11].

Развитие аппаратно-программных средств также имеет немаловажное значение для получения объективного, полного и достоверного результата.

Нередко в экспертной практике при проведении судебной компьютерно-технической экспертизы появляется необходимость восстановления информации с поврежденных USB–накопителей. Для этого широко используется комплекс PC-3000 flash.

Восстановление данных с поврежденных USB-устройств. Комплекс PC-3000 flash. Данный комплекс использует собственную технологию прямого доступа к микросхемам флэш-памяти. При этом микросхема выпаивается из накопителя и считывается на специальном считывающем устройстве — Flash reader, входящем в состав комплекса, что позволяет получить доступ к данным в случаях, когда контроллер накопителя неисправен. Эта технология дает возможность увеличить вероятность успешного восстановления данных даже в случае физического повреждения накопителей [12].

Современные микросхемы памяти представляют собой достаточно сложные устройства, подверженные явлениям износа, что является основной причиной логического повреждения накопителя.

Рассмотрим принцип работы комплекса PC-3000 flash. Объектом исследования является поврежденный USB-накопителя производителя Transcend (рис. 3).

Прежде чем начать работу, эксперт должен выпаять микросхему памяти из основной конструкции (при температуре 320–350 °C), причем так, чтобы «ножки» микросхемы не были повреждены, поскольку возрастает вероятность того, что комплекс восстановит только часть данных или вообще не сможет считать микросхему памяти. Если потребуется необходимо произвести зачистку ножек.

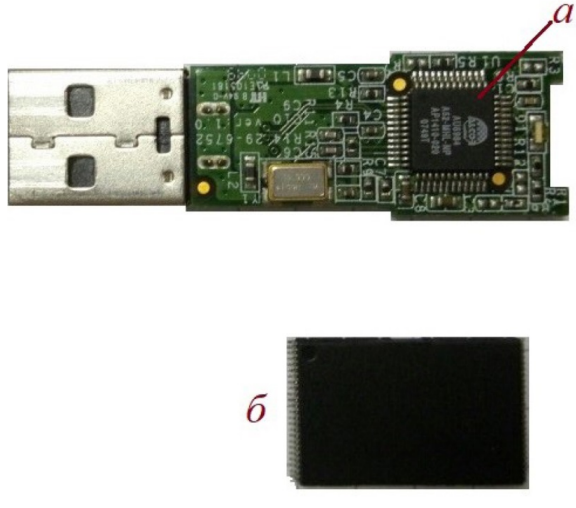

Рис. 3. USB-устройство Transcend с выпаянной микросхемой памяти:

а — контроллер; *б* — микросхема памяти

После подготовки объекта к исследованию эксперт загружает программную часть комплекса PC-3000 flash. После того как пройдет инициализация (рис. 4), выпаянная микросхема памяти вставляется в устройство со строгим соблюдением методических рекомендаций, а именно: кружочек, отмеченный на микросхеме, должен совпасть с обозначением (синим флажком) на аппаратуре, в противном же случае данные могут быть утеряны (рис. 5).

Рис. 4. Инициализация Flash-reader. Окно работы комплекса PC-3000 flash

Рис. 5. Считывающее устройство Flash-reader комплекса со вставленной микросхемой памяти

После осуществления указанных действий программа считывает микросхему. Сначала она будет иметь статус «неизвестной» микросхемы. В дальнейшем необходимо выбрать опцию «чтение микросхемы» (рис. 6) и запустить про-

грамму для считывания данных (рис. 7). Отметим, что микросхема состоит из двух частей и каждая часть должна считываться с двух сторон.

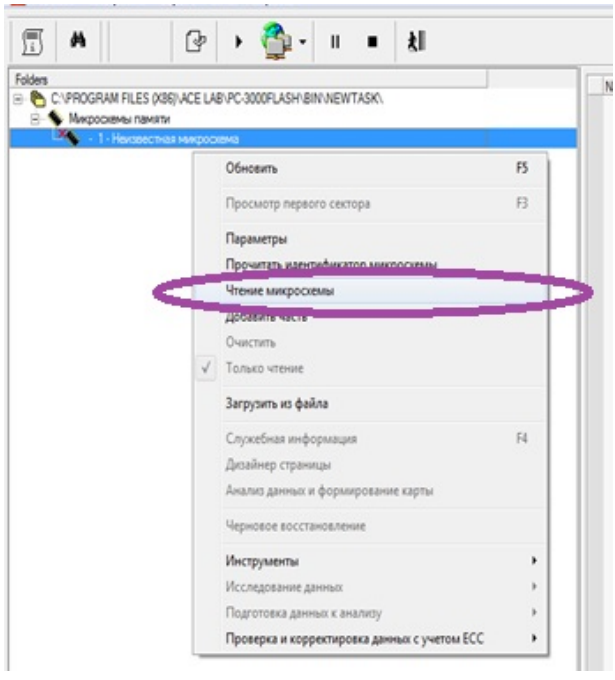

Рис. 6. Выбор опции «чтение микросхемы памяти»

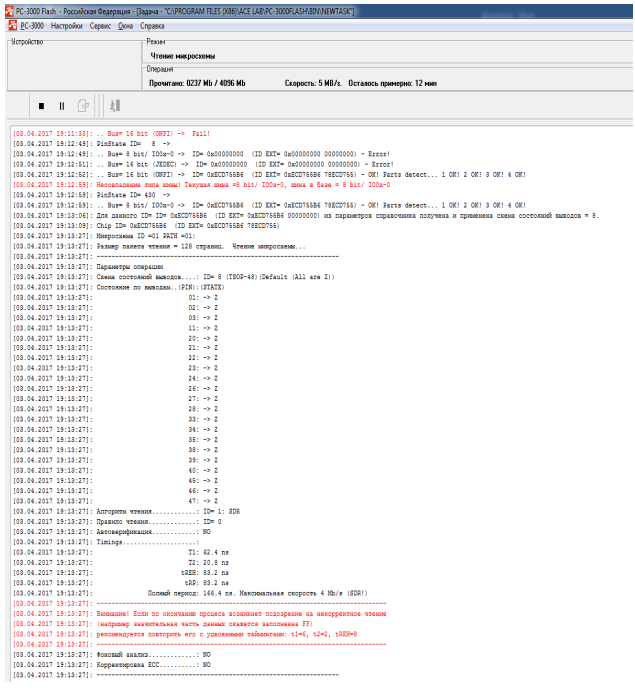

Рис. 7. Чтение микросхемы памяти

После завершения указанной процедуры эксперт переходит к использованию «системы решений», которая позволяет найти решение по восстановлению данных для комплекса PC-3000 flash (рис. 8).

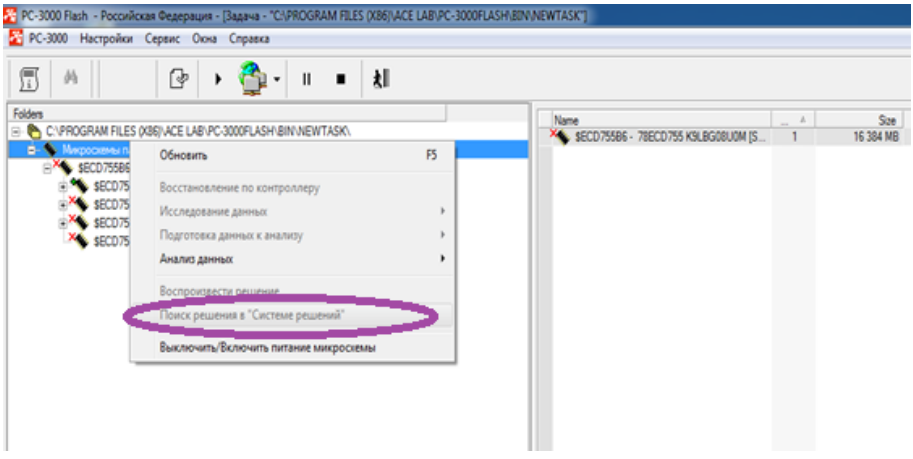

Рис. 8. Выбор опции «поиск в «системе решений»

Для получения решения необходимо виртуализировать контроллер устройства, заполнив необходимые поля данных (рис. 9). Система выдаст решение, которое может быть загружено, и, считав его, программа приступит к восстановлению данных.

Рис. 9. Поиск решения в «системе решений»

Возможность виртуализации контроллера играет важную роль в работе эксперта, поскольку нередко не представляется возможным восстановить данные с USB-устройства иными способами вследствие нерабочего состояния контроллера.

При исследовании USB-накопителей помимо аппаратно-программного комплекса PC-3000 flash в экспертной практике широко применяется программный комплекс Encase Forensic Assistant.

Программный Комплекс Encase Forensic Assistant. Этот программный комплекс как незаменимое программное средство в экспертной деятельности работает на различных платформах, таких, как Windows, Linux, AIX, OS X, Solaris и др., а также позволяет найти на исследуемом объекте нужные файлы, нужную информацию. Кроме того, возможности данного комплекса не ограничиваются только поиском информации, с его помощью можно найти удаленные файлы, а также просмотреть их [13].

Рассмотрим принцип работы комплекса Encase Forensic. В качестве объекта исследования использовался USB-накопитель SanDick Cruzer Facet объемом памяти 2 Гбайта (рис. 10, 11). Была поставлена задача: найти пользовательские текстовые файлы (в том числе заархивированные) на USB-накопителе.

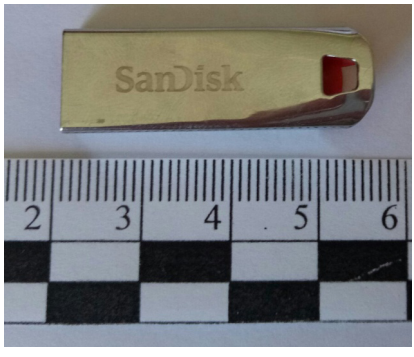

Рис. 10. Внешний вид объекта исследования SanDick Cruzer Facet с объемом памяти 2 Гбайта

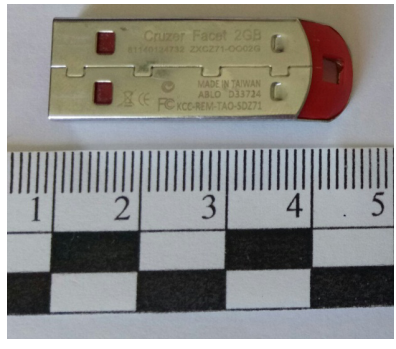

Рис. 11. Внешний вид тыльной стороны объекта исследования SanDick Cruzer Facet с объемом памяти 2 Гбайта

Прежде чем начать работу с устройством, следует выполнить некоторые действия. Во-первых, подключить USB-накопитель к блокиратору, которым, как правило, обладает каждый компьютерно-технический эксперт.

Во-вторых, подключая носитель информации к программе, во избежание потери определенных данных или их изменения необходимо создать образ. Для этого нужно выбрать Create image-Physical drive: E01–Compression (0–9)–Finish–Start, с которым эксперт может производить любые манипуляции. Недопустимо вносить изменения в первоначальное состояние информационной составляющей объекта исследования. Поэтому эксперт работает непосредственно с созданным образом. Данный образ можно создать с помощью программы Forensic Toolkit(FTK), что позволит не допустить какого-либо редактирования информации непосредственно на самом носителе.

Создав образ USB-накопителя, необходимо проверить устройство на вирусы. После успешного выполнения всех действий USB-накопитель можно отсоединить.

Однако в распоряжении эксперта не всегда есть специализированные приспособления или программы, не позволяющие вносить изменения в данные на устройстве. Поэтому эксперту важно знать, как «запретить» компьютеру вносить какие-либо изменения в подключенные к нему устройства.

Перед подключением объекта исследования к компьютеру в настройках компьютера необходимо установить защиту от записи. Для этого нажатием клавиши Пуск — regedit заходим в реестр — HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control. В разделе Control создаем раздел StorageDevicePolicies, в котором устанавливаем параметр WriteProtect (тип dword). Изменяем значение параметра с 0 (режим записи) на 1 (режим чтения) (рис. 12).

Подключив устройство (для проверки первоначально рекомендуется использовать иное устройство, но не объект исследования), можем убедиться, что удалить или изменить данные не представляется возможным.

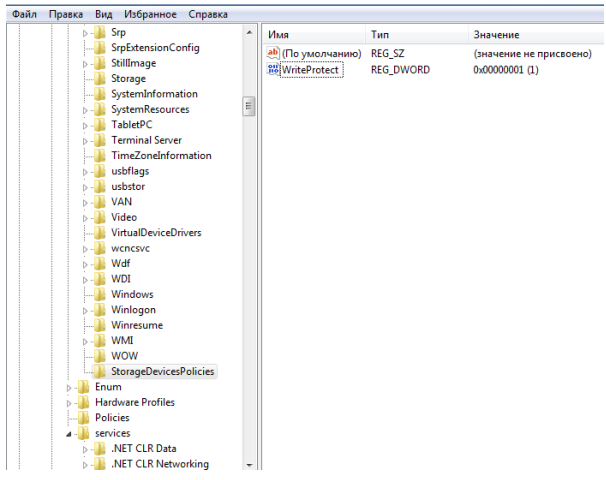

Рис. 12. Установки защиты от записи на USB-устройство

Затем подключаем USB-устройство и запускаем программу. Перед решением основной задачи необходимо осуществить подготовительный этап, а именно: дать название дела (рис. 13), выбрать нужное устройство (рис. 14), произвести считывание хэш-значений и сигнатуры (рис. 15).

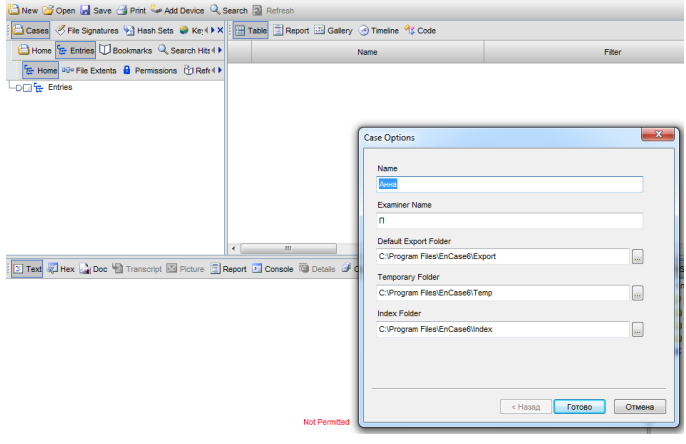

Рис. 13. Запуск комплекса и заполнение начальных данных

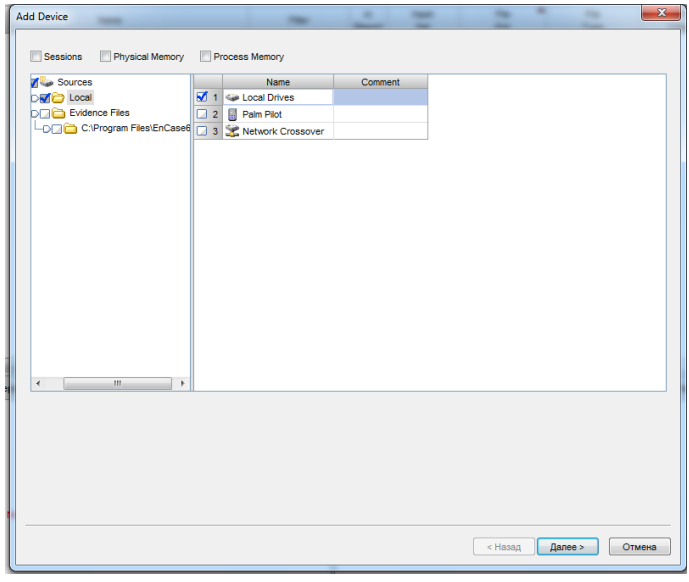

Рис. 14. Выбор устройства исследования

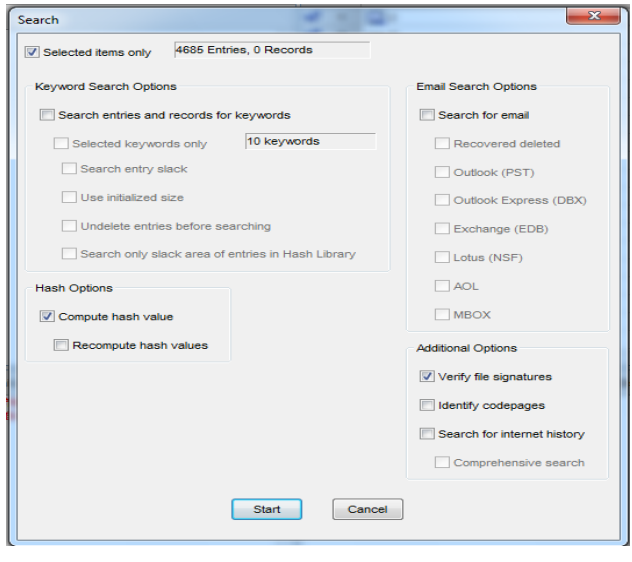

Рис. 15. Считывание хэш-значений и сигнатур

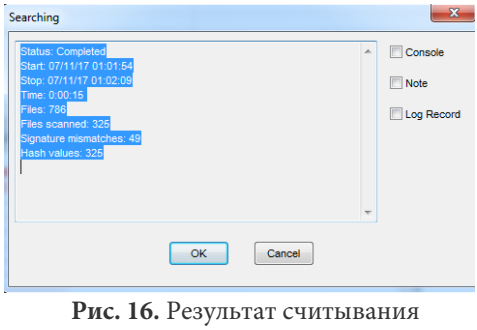

Рис. 16. Результат считывания хэш-значений и сигнатур

Подчеркнем, что для продолжения работы с устройством число просканированных файлов и полученные хэш-значения должны совпадать, в противном случае понадобится устранить разночтение прежде чем перейти к следующему этапу работы (рис. 16).

Успешно выполнив необходимые действия, эксперт может перейти к решению поставленной задачи. Для этого задается условие, правильное составление которого является основой получения необходимого результата. С правой стороны экрана необходимо перейти в опцию «Conditions». И, выбрав опции «Signature(Find)», «File Ext», эксперт задает условия (рис.17, 18).

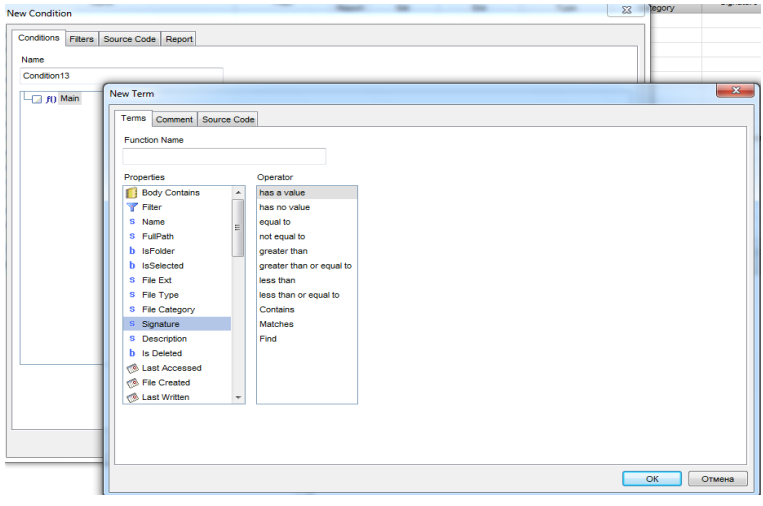

Рис. 17. Задание условия для решения поставленной задачи

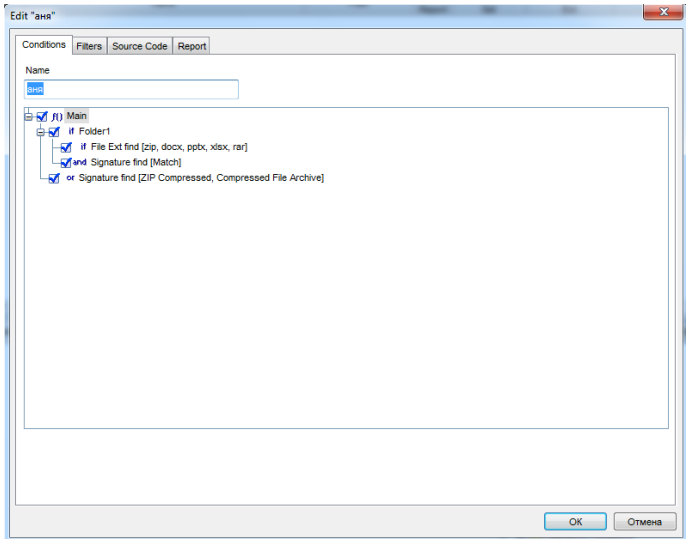

Рис. 18. Условия для решения поставленной задачи

Выбрав условие (путем нажатия на него), получаем соответствующие ему данные, содержание которых, при необходимости, также можно проанализировать (рис. 19).

Таким образом, путем совершения нескольких манипуляций программа Encase Forensic позволяет успешно решить поставленную перед экспертом задачу.

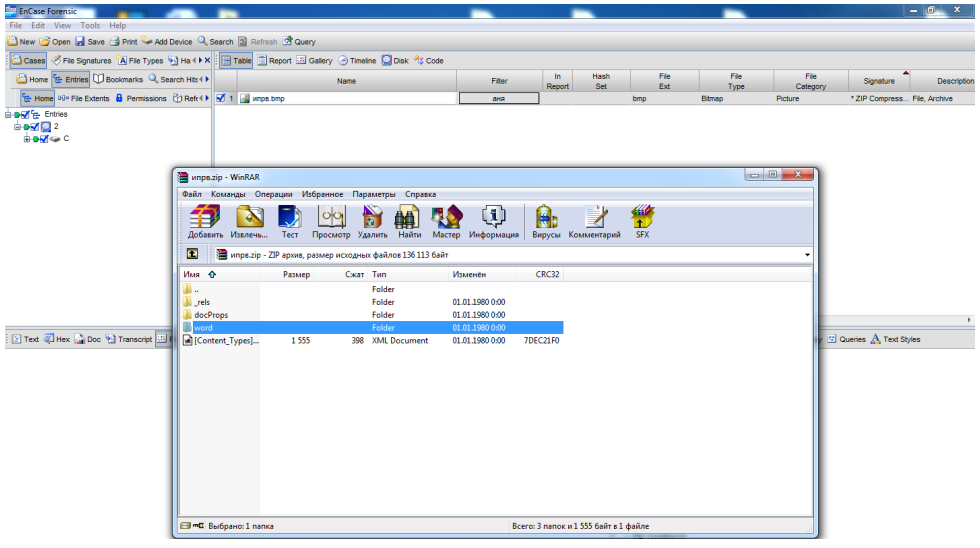

Рис. 19. Результат исследования

Обобщая все вышеизложенное, можно сделать вывод о том, что на сегодняшний день USB-накопители являются наиболее удобными и практически незаменимыми переносными устройствами для хранения и чтения/записи информации, которые способны сочетать в себе такие свойства, как компактность и возможность хранения большого объема данных, поэтому USB-накопитель часто становится объектом экспертного исследования в рамках проведения судебной компьютерной технической экспертизы.

Программное обеспечение эксперта постоянно совершенствуется: разработаны различные программные средства, которые позволяют решать все более сложные экспертные задачи. Например, с помощью комплекса PC-3000 flash можно восстановить информацию даже с поврежденных USB-устройств (при условии, что микросхема памяти не была деформирована), а при использовании комплекса Encase Forensic есть возможность быстро найти необходимую информацию. Для корректного восстановления данных с таких устройств эксперт должен знать внутреннюю структуру USB-накопителя и соблюдать предельную осторожность при разборе устройства.

Литература

[1] Чугунков В. *Выбираем флешку. Основные характеристики USB-флеш-накопителей: что такое флэш-накопитель*. URL: http://www.compbegin.ru/articles/view/_116 (дата обращения 22.11.2017).

[2] *What is a flash drive*? URL: https://www.lifewire.com/what-is-a-flash-drive-2625794 (дата обращения 10.09.2017).

[3] *Принцип работы и устройство USB-флешки*. URL: https://hobbyits.com/cifrovye-texnologii/princip-raboty-i-ustrojstvo-usb-fleshki.html (дата обращения 10.09.2017).

[4] *В чем отличия USB-флешек USB 3.0 от USB 2.0*. URL: http://otnaspodarok.ru/v-chem-otlichiya-fleshek-usb-3-0-ot-usb-2-0/ (дата обращения 10.09.2017).

[5] Полежаев П.Н. Ахиллесова пята. USB-устройства: атака и защита. *Философские проблемы информационных технологий и киберпространства*, 2015, № 1. URL: http://cyberspace.pglu.ru/issues/detail.php?ELEMENT_ID=98191.
[6] Спиряев О. *Технологии флеш-памяти*. URL: https://www.bytemag.ru/articles/detail.php?ID=8660 (дата обращения 11.09.2017).
[7] *USB-флешки: что это и зачем они нужны*. URL: http://www.novintex.ru/read/actions/usb_flash (дата обращения 28.09.2017).
[8] *Снятие защиты от записи с флешки*. URL: http://bsodstop.ru/kak-snyat-zashchitu-ot-zapisi-s-fleshki (дата обращения 28.09.2017).
[9] Усов А.И. *Концептуальные основы судебной компьютерно–технической экспертизы*. Дис. ... док. юрид. наук. Москва, 2002, 402 с.
[10] Вехов В.Б. Использование компьютерных технологий в криминалистической деятельности и в уголовном процессе. *Вестник Академии Следственного комитета Российской Федерации*, 2014, № 1, с. 70–73.
[11] Кучин О.С., ред. *Электронные носители информации в криминалистике*. Москва, Юрлитинформ, 2017, 304 с.
[12] *PC-3000 flash*. URL: http://www.acelab.ru/dep.pc/pc3000.flash.php (дата обращения 17.08.17).
[13] *Encase Forensic*. URL: https://old.dialognauka.ru/products/encase_forensic/ (дата обращения 22.08.17).

Павлова Анна Александровна — студентка кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — М.А. Скворцова, ассистент кафедры «Информационное управление 6», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

STUDY OF USB DRIVES IN WORK OF A COMPUTER FORENSIC EXPERT

A.A. Pavlova AnniaPavlova@yandex.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The article considers USB drives, in particular, internal components of the USB-device, as well as systems used at present within computer forensic examination in work with USB drives. The special attention is given to the hardware-software package PC-3000 flash, which allows for data recovery from damaged USB devices, and Encase Forensic software package, which is used to search, analyze and restore data from USB devices.

Keywords

USB drive, computer forensic examination, software, damaged devices, data recovery, data retrieval

References

[1] Chugunkov V. Vybiraem fleshku. Osnovnye kharakteristiki USB-flesh-nakopiteley: chto takoe flesh-nakopitel' [Select the flash drive. The main characteristics of USB flash drives: what is a flash drive]. Available at: http://www.compbegin.ru/articles/view/_116 (accessed 22.11.2017).

[2] What is a flash drive? Available at: https://www.lifewire.com/what-is-a-flash-drive-2625794 (accessed 10 September 2017).

[3] Printsip raboty i ustroystvo USB-fleshki [Operating principle and structure of the USB stick]. Available at: https://hobbyits.com/cifrovye-texnologii/princip-raboty-i-ustrojstvo-usb-fleshki.html (accessed 10 September 2017).

[4] V chem otlichiya USB-fleshek USB 3.0 ot USB 2.0 [What's the difference between USB 3.0 and USB 2.0 memory sticks]. Available at: http://otnaspodarok.ru/v-chem-otlichiya-fleshek-usb-3-0-ot-usb-2-0/ (accessed 10 September 2017).

[5] Polezhaev P.N. "The Achilles heel" of USB-devices: attack and defense. *Filosofskie problemy informatsionnykh tekhnologiy i kiberprostranstva* [Philosophical problems of IT and Cyberspace], 2015, no. 1. Available at: http://cyberspace.pglu.ru/issues/detail.php?ELEMENT_ID=98191.

[6] Spiryaev O. Tekhnologii flesh-pamyati [USB-memory technologies]. Available at: https://www.bytemag.ru/articles/detail.php?ID=8660 (accessed 11 September 2017).

[7] USB-fleshki: chto eto i zachem oni nuzhny [USB stick: what is it and what do we need them for]. Available at: http://www.novintex.ru/read/actions/usb_flash (accessed 28 September 2017).

[8] Snyatie zashchity ot zapisi s fleshki [Write deprotection of USB stick]. Available at: http://bsodstop.ru/kak-snyat-zashchitu-ot-zapisi-s-fleshki (accessed 28 September 2017).

[9] Usov A.I. Kontseptual'nye osnovy sudebnoy komp'yuterno–tekhnicheskoy ekspertizy. Dis. dok. yurid. nauk [Conceptual foundations of computer forensic examination. Dok. jur. sci. diss.]. Moscow, 2002, 402 p.

[10] Vekhov V.B. Application of computer technologies in criminalistics activity and criminal procedure. *Vestnik Akademii Sledstvennogo komiteta Rossiyskoy Federatsii*, 2014, no. 1, pp. 70–73.

[11] Kuchin O.S., ed. Elektronnye nositeli informatsii v kriminalistike [Electronic data storage devices in criminalistics]. Moscow, Yurlitinform publ., 2017, 304 p.

[12] RS-3000 flash. Available at: http://www.acelab.ru/dep.pc/pc3000.flash.php (accessed 17.08.2017).
[13] Encase Forensic. Available at: https://old.dialognauka.ru/products/encase_forensic/ (accessed 22.08.2017).

Pavlova A.A. — student, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — M.A. Skvortsova, Assistant, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.