https://doi.org/10.31643/2018.028
22 November 2018

Байбусинов Азамат Сансызбаевич, магистрант
Казахский Агротехнический университет им. С. Сейфуллина
г.Астана, Казахстан, E-mail: azamat_b_astana@mail.ru
ORCID 0000-0002-9714-278X

ОСОБЕННОСТЬ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ РЕЕСТРА ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS 8.1 (x64)

Azamat Baibussinov
S. Seifullin Kazakh AgroTechnical university
Astana, Kazakhstan
E-mail: azamat_b_astana@mail.ru
ORCID 0000-0002-9714-278X

PECULIARITY OF CRIMINALISTICS RESEARCH OF REGISTER OF THE OPERATING SYSTEM WINDOWS 8.1 (x64)

***Annotation**: The article discusses specifics of the operating system Windows 8.1 (x64) while conducting a forensic investigation of the registry based on the example of a criminal case of confidential information theft.*

***Keywords:** digital forensics, computer crimes, criminalistics analysis of register of the operating system windows, specifics of the Windows 8.1 (x64).*

***Аннотация:** В статье рассматривается особенность работы операционной системы Windows 8.1 (x64) при проведении криминалистического исследования системного реестра на примере уголовного дела по факту кражи конфиденциальной информации.*

***Ключевые слова:** "цифровая" криминалистика, компьютерные преступления, криминалистическое исследование реестра операционной системы Windows, особенности Windows 8.1 (x64)*

Введение. Гражданину "А" в период с августа по декабрь 2017 года по служебной необходимости был предоставлен доступ к ноутбуку компании "Б" с конфиденциальной информацией. В этот период, у гражданина "А" возник преступный умысел, который заключался в похищении конфиденциальной информации и дальнейшей его передачи третьим лицам за материальное вознаграждение. В целях реализации своего преступного умысла гражданин "А" в период с ноября по декабрь 2017 года подключал личный внешний жесткий диск с интерфейсом USB, не зарегистрированный в компании "Б", к служебному ноутбуку и осуществлял копирование конфиденциальной информации.

Позднее факт хранения конфиденциальной информации компании "Б" на незарегистрированном внешнем жестком диске с интерфейсом USB был зафиксирован и подтвержден.

Задача: подтвердить факт подключения незарегистрированного внешнего жесткого диска с интерфейсом USB, принадлежащего гражданину "А", к ноутбуку компании "Б", а также установить дату и время подключения.

Исследовательская часть. Объектом осмотра был ноутбук компании "Б" с установленной операционной системой "Windows 8.1 Профессиональная", тип системы 64-разрядная, процессор "Intel Core i3", частота 2.27 ГГц, ОЗУ 3 Гигабайт, а также незарегистрированный внешний жесткий диск с интерфейсом USB, принадлежащий гражданину "А".

В процессе осмотра незарегистрированного внешнего жесткого диска с интерфейсом USB, принадлежащего гражданину "А", с использованием программного обеспечения "USBDeview" (*v2.65*) [1], предназначенного для просмотра истории

подключения всех USB-устройств в системе, установлен его серийный номер – 20170423020401F.

В процессе осмотра ноутбука компании "Б" с помощью программного обеспечения "USBDeview" (*v2.65*), "цифровых следов" подключения незарегистрированного внешнего жесткого диска с интерфейсом USB, принадлежащего гражданину "А", не обнаружено (рисунок 1).

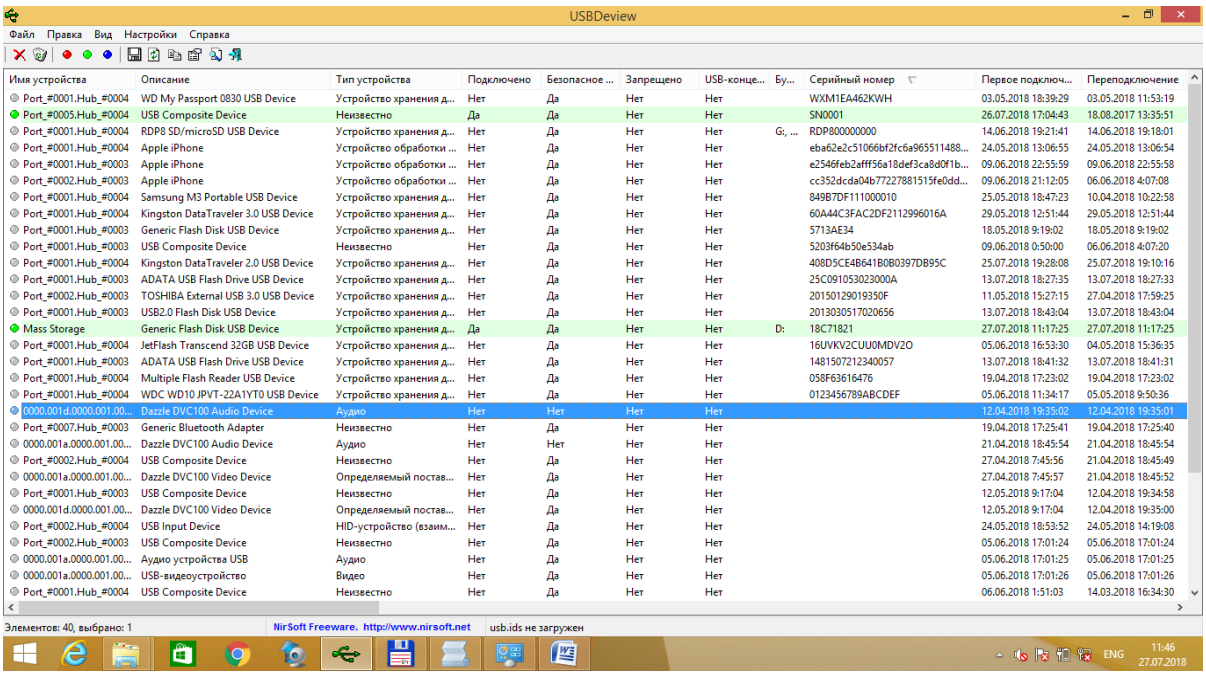

Рисунок 1 – Работа программы "USBDeview"

Из работы Гортинского А.В. и Мордвинкина М.М. известно, что информация о первом подключении USB-устройства хранится в файле C:\Windows\inf\setupapi.dev.log [2], поэтому специалистом был осмотрен указанный файл, в результате чего записи о подключении USB-устройства с серийным номером 20170423020401F не обнаружено. Информацию о подключении USB-устройства с серийным номером 20170423020401F обнаружени в файле C:\Windows\inf\setupapiapp.20180426_074719.dev.log (рисунок 2).

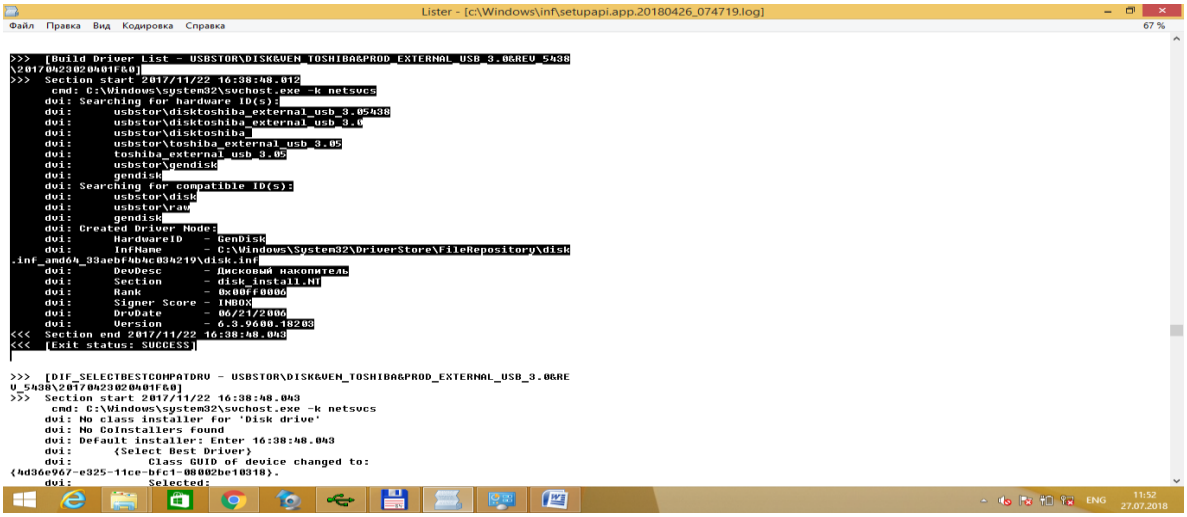

Рисунок 2 – запись о подключении USB-устройства с серийным номером 20170423020401F

https://doi.org/10.31643/2018.028
22 November 2018

Кроме того, специалистом была обнаружена еще одна "интересная" запись об USB-устройстве с серийным номером 20170423020401F (рисунок 3).

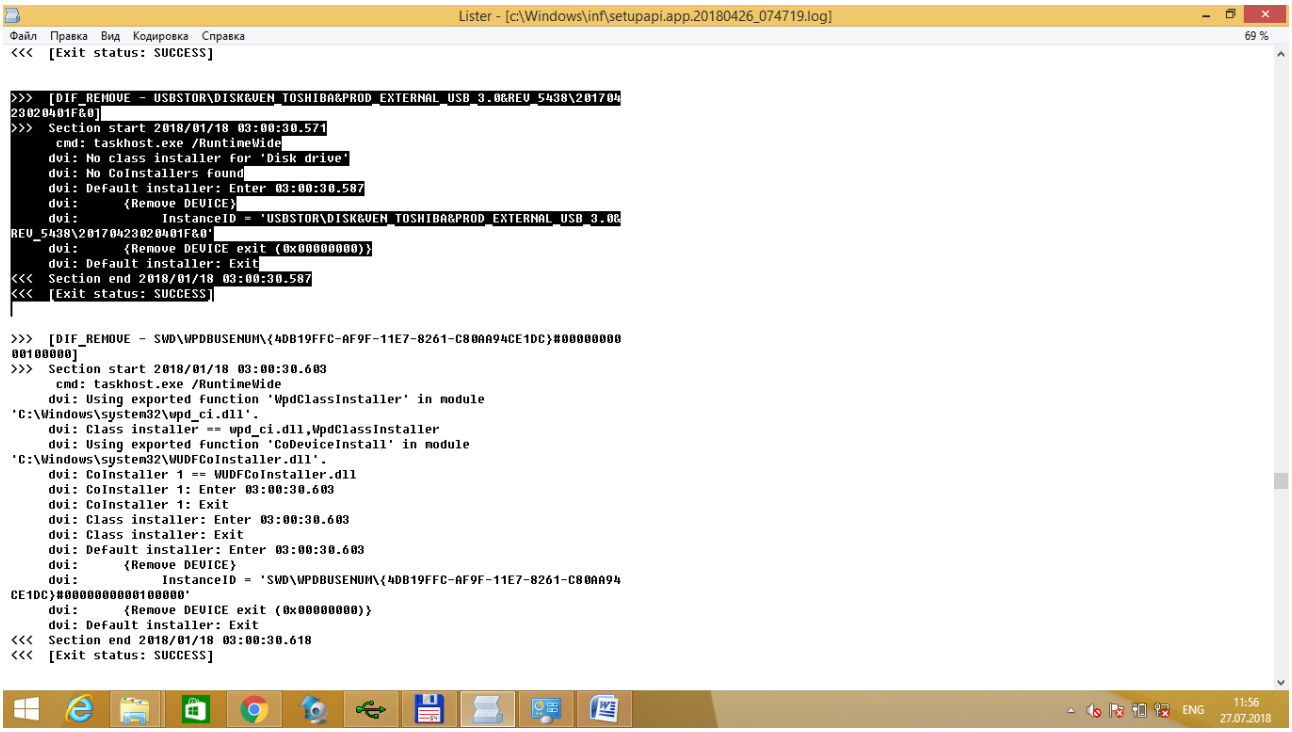

Рисунок 3 – запись об USB-устройстве с серийным номером 20170423020401F

Из официальной документации компании "Microsoft" стало известно, что запрос DIF_REMOVE уведомляет установщика о том, что операционная система собирается удалить устройство и дает установщику возможность подготовиться к удалению [3]. Таким образом, операционная система 18 января 2018 года в 03:00ч. удалила из реестра запись о подключении USB-устройства, тогда как гражданин "А" последний раз имел доступ к служебному ноутбуку в декабре 2017 года.

Отсюда возникают две версии возникшей ситуации:

1. ОС Windows "чистит" реестр в соответствии со своими внутренними настройками.

2. В компании "Б" имеется гражданин "В", сообщник гражданина "А", который "почистил" следы подключения USB-устройства.

Экспериментальная часть. Для подтверждения или опровержения первой версии был проведен эксперимент, в котором использовался тестовый компьютер с виртуальной средой "VMWare" и с установленной операционной системой Windows 8.1 (*x64*), программное обеспечение "USBDeview" (*v2.65*), одно USB-устройство 2.0 (*с/н 900062BD85CE6E30*) и одно USB-устройство 3.0 (*с/н 01GU9CCQF4CRA0RP*). Дата и время в виртуальной среде модифицировалось путем изменения системных настроек на тестовом компьютере.

В результате проведенного эксперимента стало известно, что операционная система Windows 8.1 (x64) в соответствии со своими настройками проводит "очистку" реестра при длительном (*более 30 дней*) отсутствии подключения USB-устройств (*2.0*) и сохраняет об этом действии запись в файл C:\Windows\inf\setupapi.dev.log (рисунок 4). Соответственно, вторую версию можно исключить.

https://doi.org/10.31643/2018.028
22 November 2018

Разработчики ОС Windows руководствуются правилом, которое подтверждается все чаще в мире компьютеров и заключается в том, что, независимо от размера емкости жесткого диска компьютера, пользователь, в конечном итоге, ее заполнит. В то время как средний размер жесткого диска компьютера со временем значительно увеличился, приложения также выросли соответственно, в результате чего пользователи ищут способы создать больше свободного места на жестком диске. Доступное пространство также уменьшается из-за множества временных файлов, создаваемых приложениями для резервного копирования или повышения производительности. Когда дисковое пространство становится низким, становится необходимым уменьшить объем пространства, используемого приложениями. Дисковое пространство может быть освобождено с помощью различных средств, в том числе: удаления файлов, сжатия файлов, перемещения файлов на резервный носитель, перенос файлов на удаленный сервер. Файлы, которые являются хорошими "кандидатами" для очистки, включают: файлы, которые пользователю больше не понадобятся, временные файлы, файлы, которые можно восстановить, если необходимо, с установочного компакт-диска, файлы данных, которые, возможно, были заменены более новыми версиями, такими как старые файлы резервных копий, старые файлы, которые не использовались в течение длительного времени [4].

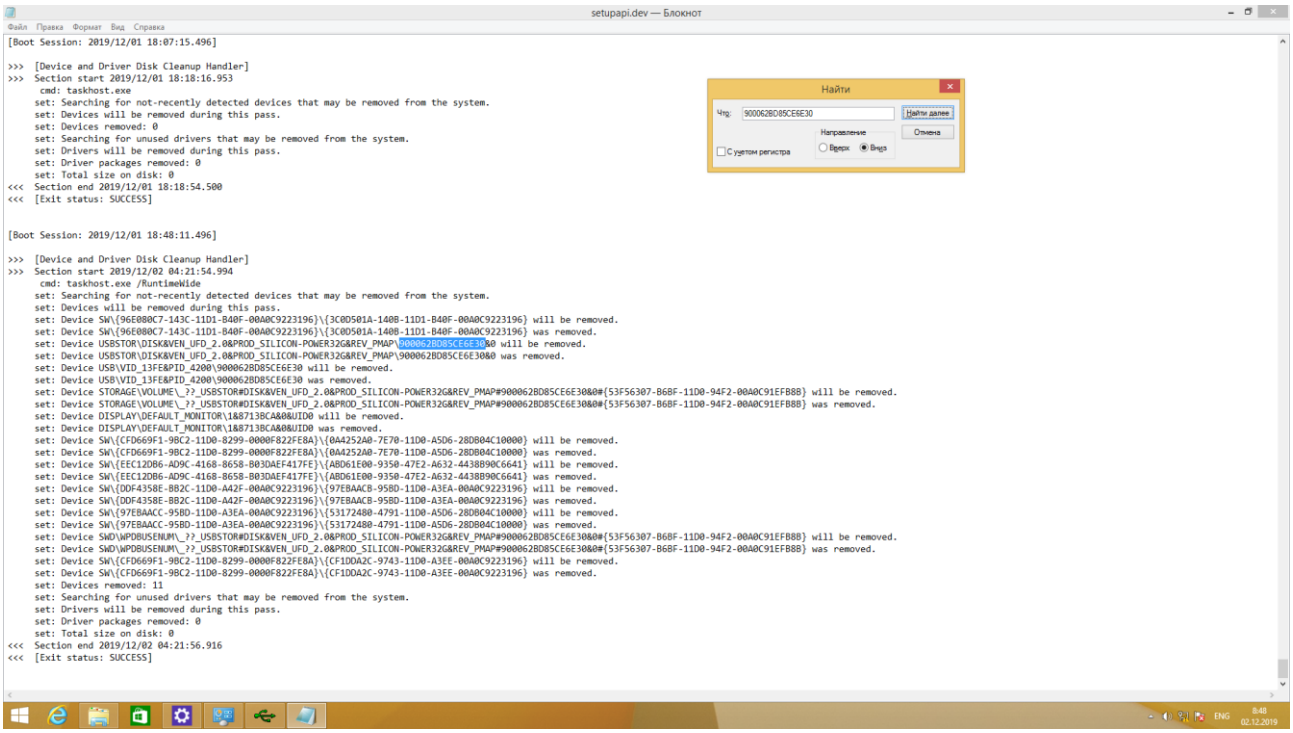

Рисунок 4 – запись об удалении USB-устройства 2.0 с серийным номером 900062BD85CE6E30

Ожидание того, что пользователь вручную очистит файловую систему, не является хорошим решением. Пользователь может не знать, где находятся многие файлы, или как определить, какие из них можно удалить безопасно. Кроме того, существует риск, что пользователь может удалить необходимые файлы. ОС Windows включает в себя "Disk Cleanup", утилиту, которая облегчает пользователю управление доступным дисковым пространством. Утилита "Disk Cleanup" предназначена для освобождения максимально возможного объема дискового пространства и снижения риска случайного удаления важных файлов [4].

https://doi.org/10.31643/2018.028
22 November 2018

Выводы. Таким образом, факт подключения незарегистрированного жесткого диска с интерфейсом USB, принадлежащего гражданину "А", к ноутбуку компании "Б", подтвержден, зафиксированы дата и время подключения. Результаты эксперимента исключили версию наличия сообщника гражданина "А" в компании "Б", что позволило сэкономить силы и средства на его поиски. Кроме того, специалистам следует иметь в арсенале несколько программных средств с актуальными обновлениями, что позволит получать больше "цифровых следов" преступной деятельности, а также перепроверять источники их получения [5]. Необходимо продолжить эксперименты с подключением USB-устройств в другие версии ОС Windows, с целью получения дополнительной информации об особенностях их работы.

Список литературы

1. [Электрон.ресурс] – URL (дата обращения 26.07.2018): Сайт https://www.nirsoft.net/utils/usb_devices_view.html.
2. [Электрон.ресурс] – URL (дата обращения 27.07.2018): Статья "Некоторые особенности судебно-экспертного исследования реестра Windows", Гортинский А.В., Мордвинкин М.М., https://cyberleninka.ru/article/n/nekotorye-osobennosti-sudebnoekspertnogo-issledovaniya-reestra-windows.
3. [Электрон.ресурс] – URL (дата обращения 27.07.2018): Сайт https://docs.microsoft. com/en-us/windows-hardware/drivers/install/dif-remove.
4. [Электрон.ресурс] – URL (дата обращения 05.11.2018): Сайт https://docs.microsoft.com/en-us/windows/desktop/lwef/disk-cleanup.
5. [Электрон.ресурс] – URL (дата обращения 05.11.2018): Статья "Разработка программного обеспечения для криминалистического исследования реестра операционной системы Windows", Жантлесов Ж.Х., Байбусинов А.С., https://doi.org/10.31643/2018.018.