Санкт-Петербургский государственный университет

Математическое обеспечение и администрирование информационных систем

Системное программирование

Александрия Георгий Гуливерович

Криминалистический анализ системных файлов современных операционных систем семейства Windows

Бакалаврская работа

Научный руководитель:
ст. преп. Губанов Ю. А.

Рецензент:
старший эксперт экспертно-криминалистического отдела Следственного управления СКРФ по Свердловской обл. Михайлов И. Ю.

Санкт-Петербург
2016

SAINT-PETERSBURG STATE UNIVERSITY

Software and Administration of Information Systems

Area of Specialisation Software Engineering

Alexandriia Georgii

Forensic analysis of system files modern operating systems Windows family

Bachelor's Thesis

Scientific supervisor:
senior lecturer Yuri Gubanov

Reviewer:
senior expert of Department of Forensic Sciences of the Investigative Management of ICRF at Sverdlovsk region Igor Mikhaylov

Saint-Petersburg
2016

Оглавление

Введение

В современном мире с целью полного и всестороннего расследования обстоятельств совершенных преступлений и противоправных деяний зачастую прибегают к помощи компьютерного криминалистического анализа [2].

Электронные вычислительные машины (ЭВМ): компьютеры, ноутбуки, смартфоны и т.д., – а также устройства хранения информации: жесткие диски, флеш накопители и т.д., – имеющиеся у подозреваемого, в соответствии с судебным постановлением подвергаются различным видам исследований [18] в том числе, с помощью специализированных инструментов для проведения компьютерной экспертизы.

Объектами компьютерной экспертизы является совокупность хранимых на устройстве файлов, которые могут содержать интересующие данные (артефакты), и могут быть предъявлены в суде [7].

Содержащаяся в объектах исследования информация может подтвердить или опровергнуть причастность подозреваемого к совершенному деянию, а также выявить наличие у злоумышленника предметов, являющихся уликами преступления.

Файлы, представляющие непосредственный интерес для компьютерной экспертизы, можно разделить на две категории: файлы операционной системы и приложений. Во время работы операционной системы файлы первой категории постоянно модифицируются, так как в системе происходят некоторые действия, влияющие на данные файлы. К действиям, приводящим к модификации, относятся такие, как удаление или изменения файлов, установка сторонних программных продуктов, подключение или отключение внешних ЭВМ и т.д..

Одним из системных файлов является появившийся в последних версиях операционных систем Windows уведомление Toast Notification, также называемое тост уведомление (Тост). Тост представляет из себя оповещение, уведомление или событие, которое произошло в определенный момент времени с приложением или сервисом, к примеру, уведомление о получении новых сообщений в социальных сетях или в

почтовых сервисах. Данные уведомления отображаются в системной области, называемой Центр Уведомлений (Action Center) [22].

В расследуемых делах, когда часть данных была удалена подозреваемым, специалист в области компьютерной экспертизы может применить различные способы восстановления утерянной информации. В тех ситуациях, когда восстановление информации не принесло желаемого результата или когда интересующие данные были перезаписаны, эксперт проводит поиск резервных копий данных или предыдущих версий утерянной информации, чтобы проанализировать их взамен отсутствующих или перезаписанных данных.

Одной из технологий резервного копирования, встроенной в современные операционные системы семейства Windows, является технология Microsoft Volume Shadow Copy Service [16], основанная на формате логического раздела Volume Shadow Copy, также называемой теневой копией (ТК). Теневая копия представляет из себя копию логического раздела на определенный момент времени в прошлом. Теневые копии могут быть полными, дифференциальными или инкрементальными [21] копиями логического раздела. Теневые копии также могут быть копиями любого логического раздела вне зависимости от файловой системы, установленной на данном разделе.

1. Постановка задачи

Целью работы является исследование и анализ структур тост уведомления и формата теневой копии, разработка компонента программы цифровой криминалистики для анализа Тост, а также компонента программы цифровой криминалистики для исследования и поддержки теневых копий. Также компонент поддержки теневых копий должен восстанавливать содержимое логического раздела на момент создания копии раздела, для возможности провести компьютерную экспертизу на восстановленных областях памяти и файлах взамен удаленных или измененных.

В рамках данной работы были поставлены следующие задачи:

- Провести исследования и анализ структур Тост и формата ТК:
  - Определить их местоположения
  - Выявить их внутренние элементы структур
  - Выделить наиболее значимую извлекаемую информацию для криминалистической экспертизы
- Реализовать компоненты для анализа тост уведомления и формата теневой копии и провести их интеграцию в продукт цифровой криминалистики

2. Обзор теневой копии

2.1. Хронология

Теневая копия – это формат логического раздела, который впервые был представлен компанией Microsoft в операционной системе Windows XP. На тот момент могли создаваться только временные теневые копии, то есть, система при модифицировании каких-либо файлов копировала информацию о данных файлах и сохраняла их в оперативную память ЭВМ, то есть перезагрузка ЭВМ вела к потери сохраненных теневых копий.

Сохраняемые теневые копии впервые появились в Windows Server 2003, что позволило восстанавливать созданные теневые копии на ЭВМ. Наличие сохраненных теневых копий на сервере дала возможность получать к ним доступ по сети клиентским ЭВМ. Данная функция получила название "Shadow Copies for Shared Folders" для клиент-серверной архитектуры. Клиентская часть была включена в Windows XP SP2 вместе с набором утилит для работы с теневыми копиями.

Теневая копия была внедрена в систему резервирования и восстановления данных в Windows Vista, Windows Server 2008, Windows 7 и Windows Server 2008 R2, благодаря чему при восстановлении системы появилась возможность выбрать, какую из предыдущих копий логического раздела (называемой точкой восстановления) нужно восстановить. Помимо этого в графический интерфейс программы Проводника была добавлена новая вкладка, называемая 'Предыдущие версии', показанная на рисунке 1. Данное нововведение было предназначено для восстановления файлов и директорий из точек восстановления к тому состоянию, когда была создана теневая копия.

В упомянутых выше операционных системах теневые копии, по умолчанию, создаются:

- Автоматически, один раз в день
- Вручную, во время использования утилиты резервного копирования информации

- При установке внешних приложений, которые создают точки восстановления системы

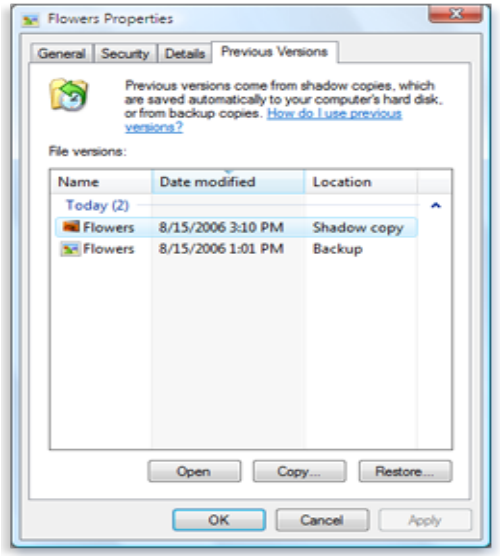


Рис. 1: Новая вкладка "Предыдущие версии"

В системах предусмотрены возможности изменения временного периода, используемого для автоматической генерации теневых копий, и объема памяти, выделенной под хранение теневой копии на логическом разделе диска.

В Windows 8 из программы Проводник была удалена графическая составляющая для просмотра, поиска и восстановления предыдущих копий логического раздела, однако в Windows 10 визуальная составляющая была возвращена. Изменения также затронули процесс создания теневых копий: теперь, по умолчанию, они не создавались с определенным временным интервалом. Чтобы генерировать теневые копий пользователю необходимо специально активировать функцию для создания теневых копий.

2.2. Общие сведения

Теневые копии могут быть полными, дифференциальными или инкрементальными копиями логического раздела, что подразумевает сохранение всей информации или только информации, подверженной из-

менениям, или только информации, которой будет производится изменении предыдущей. Ко всему прочему теневые копии могут быть копиями любого логического раздела, вне зависимости от установленной на нем файловой системы, однако сами теневые копии обязаны находится на разделе с файловой системой NTFS.

Теневые копии объединяются в коллекцию, называемую Shadow Copy Set. Данная коллекция включает теневые копии, взятые с различных логических разделов в одно и тоже время, чье количество не превышает 64-ых. По умолчанию для логического раздела предусмотрена возможность хранения 64-ых теневых копий, однако данное количество может быть увеличено до 512-и или уменьшено до одного путем изменения ключа регистра MaxShadowCopies, который расположен в HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VSS\Settings.

Рис. 2: Папка System Volume Information и файлы в ней

Теневая копия является неотъемлемой частью логического раздела с файловой системой NTFS также, как и метафайлы [17]: Boot, Master File Table и т.д., – за исключением того, что теневая копия не является метафайлом или каким-то одним файлом (из-за сложности элементов структуры формата теневой копии). Однако файловая система пытается отобразить информацию о теневых копиях как файлы логического раздела, которые расположены в корневой директории раздела, в папке

System Volume Information, как изображено на рисунке 2.

2.3. Существующие решения

С момента выпуска теневой копии были разработаны различные программы для компьютерной экспертизы, которые способны проанализировать устройство хранения информации на наличие теневых копий. Ниже представлены наиболее актуальные и востребованные из них:

- **Microsoft Volume Shadow Copy Service SDK (Microsoft SDK) [15]** – набор утилит и средств разработки от компании Microsoft для управления теневыми копиями и поиска метаинформации о имеющихся теневых копиях на подключенных устройствах хранения информации. Данный набор утилит не позволяет обнаруживать теневые копии на образах логических разделов и жестких дисков. Для отображения состояния раздела, файлов и директорий на момент создания копии логического раздела используется монтирование [6] этих копии при помощи генерации символьный ссылки на нее.

- **X-Ways Forensics (X-Ways) [24]** – программа компьютерной экспертизы. Позволяет отобразить содержимое логического раздела на момент генерации теневой копии, используя монтирование [6] копий логического раздела. Данная программа отображает метаинформацию о самой теневой копии, например, дату создания или GUID, на основе набора инструментов Microsoft.

- **EnCase Forensic (EnCase) [8]** – программа компьютерной экспертизы. Отображает файлы и директории, содержащиеся на теневой копии, предварительно создав символьную ссылку на него. Также предоставляет пользователю метаинформацию о самой копии раздела на основе набора инструментов Microsoft.

- **Internet Evidence Finder (IEF) [10]** – продукт для комплексной экспертизы ЭВМ, устройств хранения информации и их образов. Способен отображать содержимое логического раздела (директории и файлы) на момент создания копии раздела. Выдает довольно подробную метаинформацию о найденных теневых копиях, однако не обнаруживает их атрибуты создания.

- **Libvshadow [9]** – набор утилит с открытым исходным кодом для анализа теневых копий. Находит информацию о созданных теневых копиях в образах логических разделов лишь в Raw формате [20]. Не отображает состояние и содержимое раздела на момент создания теневой копии, а лишь монтирует [6] его, как полноценный логический раздел, при помощи сторонней утилиты для дальнейшего исследования программами криминалистического анализа.

- **Reconnoitre [19]** – программа для обнаружения копий логических разделов на устройствах хранения информации и их образах в форматах Raw, E01 и S01 [20]. Выдает подробную метаинформацию о теневых копиях, за исключением атрибутов создания и имени машины, на которой были созданы теневые копии. Позволяет отображать файлы и директории на момент создания теневых копии.

- **Forensic Explorer (FE) [5]** – программа комплексной компьютерной экспертизы ЭВМ, устройств хранения информации и их образов. Позволяет обнаруживать теневые копии на логическом разделе и отображать их содержимое, предварительно смонтировав [6] анализируемые теневые копии. Находит лишь часть метаинформации о самих теневых копиях, в частности, дату создания и GUID.

Все описанные выше программы способны восстанавливать логический раздел на момент создания теневой копии, однако некоторые из них для этого используют сторонние программы для монтирования [6] копий логического раздела или прибегают к созданию символьной

ссылки на копию логического раздела. Несмотря на то, что данные программы исследуют формат ТК, они предоставляют не всю желаемую информацию о теневой копии, например, не обнаруживают глобальный уникальный идентификатор (GUID) [23], или имя машины, создавшей копию тома и т.д., как отображено в таблице 1.

Параметры сравнения	Microsoft SDK	X-Ways	EnCase	IEF	Libvshadow	Reconnoitre	FE
Время создания	Да	Да[2]	Да[2]	Да	Да	Да	Да
Атрибуты	Да[1]	Да[2]	Да[2]	Нет	Да	Нет	Нет
Размер логического раздела	Да	Да	Да	Да	Да	Да	Да
GUID ТК	Да	Да[2]	Да[2]	Да	Да	Да	Да
GUID набора ТК	Да	Да[2]	Да[2]	Нет	Да	Нет	Нет
GUID дескриптора	Нет	Нет	Нет	Нет	Да	Нет	Нет
Имя операционной машины	Да	Да[2]	Да[2]	Да	Нет	Да	Нет
Имя сервисной машины	Да	Да[2]	Да[2]	Нет	Нет	Нет	Нет

Да[1] – отображает не все атрибуты создания

Да[2] – отображает информацию на основе инструментов Microsoft

Таблица 1: Сравнение извлекаемой информации существующими инструментами

3. Разбор и анализ формата теневой копии

3.1. Хранение данных

Так как теневая копия является частью файловой системы, то при изменении файлов область памяти, выделенная под файл, будет сохранена не целиком в формате ТК. Вместо этого для резервирования данных, происходит сохранение отдельных блоков памяти размером 16 KB. То есть, при модификации файлов будут сохранены блоки памяти по 16 KB, подвергшиеся изменениям.

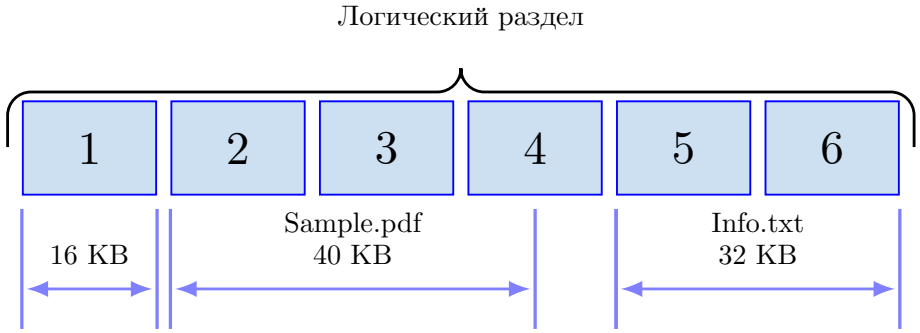


Рис. 3: Пример раздела, разбитого на блоки по 16 KB, с содержащимися на нем файлами

На рисунке 3 показан пример логического раздела, где проведем следующий эксперимент:

1. Изменим Info.txt и сохраним его
2. Удалим Sample.pdf
3. Изменим Info.txt и сохраним его

В первом и во втором действиях предположим, не умаляя общности, что изменения затронули только шестой блок на рисунке 3. Также будем создавать копии логического раздела после каждой операции. Тогда сгенерированные теневые копии будут содержать блоки данных, отображенные на рисунке 4.

При восстановлении предыдущих сгенерированных копий логический раздел будет содержать блоки данных, соответствующих копий, как это отображено на рисунке 5.

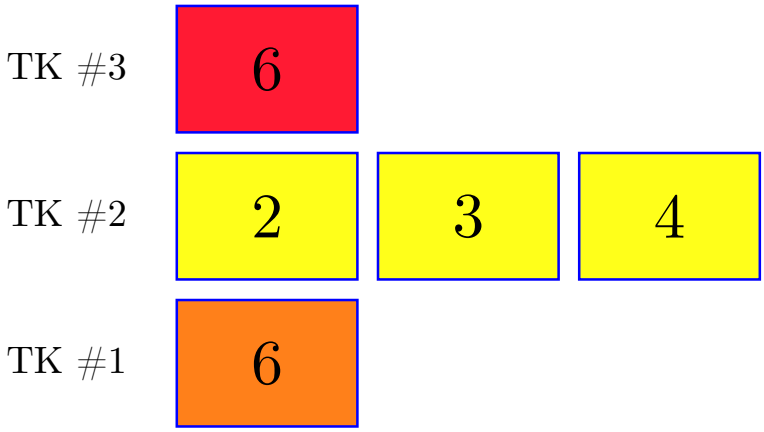


Рис. 4: Сгенерированные ТК и содержащиеся на нем блоки данных, где разным цветам соответствуют разная информация

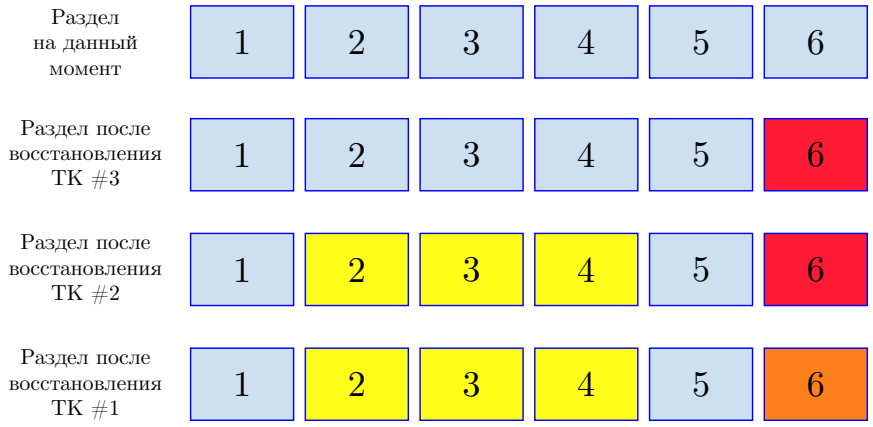


Рис. 5: Состояния раздела при восстановлении соответствующих теневых копий

Для восстановления логического раздела к моменту генерации конкретной теневой копии необходимо применить изменения из всех теневых копий, созданных поздней выбранного.

3.2. Структура формата

3.2.1. Местоположение

Для исследования и анализа структуры формата теневой копии и извлечения как можно большего объема данных анализировались последовательности байт логического раздела. Информация о них была

получена на основе методов обратной разработки [4].

Для генерации тестовых данных были написаны несколько сценариев, отвечающих за создание и удаление копий логического раздела, файлов и директории. В качестве входных данных, указанные сценарии принимали различные параметры: к примеру, количество создаваемых копий логического раздела, имена файлов и директорий для создания или удаления.

Первостепенной задачей являлось нахождение смещения формата на логическом разделе, основываясь на информации о структуре файловой системы NTFS. При анализе несколько первых тысяч байт у набора сгенерированных данных была обнаружена последовательность байт, показанная на рисунке 6, не совпадающая с сигнатурами NTFS файлов [17].

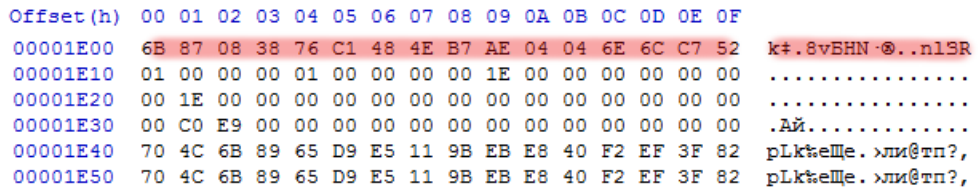


Рис. 6: Последовательность байт, предполагаемая как сигнатура теневой копии

Данная последовательность байт встречалась у всех сгенерированных тестовых данных по одному и тому же смещению – 0x00001e00, однако эта же сигнатура встречалась и по другим смещениям, поэтому было предположено, что по данному смещению находится некий заголовок формата.

При поиске информации о последовательности байт, предполагаемой как сигнатура, была найдена статья [11], которая подтвердила, что данная последовательность байт есть сигнатура. Для дальнейших исследований структуры формата использовалась, в качестве основы, найденная статья.

3.2.2. Внутреннее устройство

В статье [11] содержится подробное, хотя и не полное, описание структуры и ее элементов. В ходе работы при исследовании различных копий логических разделов и физических носителей некоторые из описанных в статье заголовков были дополнены и уточнены.

В рамках работы исследуемые элементы структуры, описанные в статье, проверялись при помощи созданных наборов тестовых данных. Для этого у тестовых данных извлекались последовательности байт, соответствующие проверяемым элементам, которые сравнивались с результатом работ набора утилит [15].

К подтвержденной информации относятся, к примеру, время создания теневой копии и размер логического раздела, показанные на рисунке 7, атрибуты создания теневой копии, имена операционной и сервисной машин, отображенные на рисунке 8.

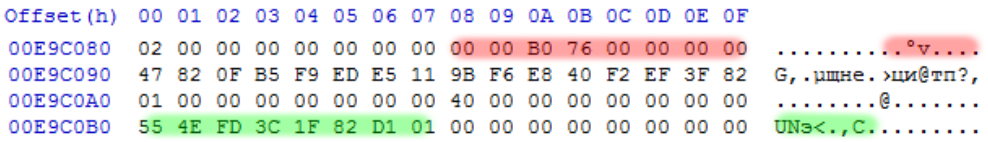


Рис. 7: Последовательности байт, соответствующие размеру логического раздела и времени создания теневой копии
– размер логического раздела
– время создания теневой копии

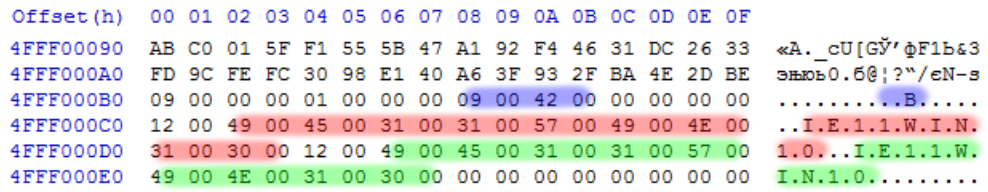


Рис. 8: Последовательности байт, соответствующие именам операционной и сервисной машин и атрибутам создания теневой копии
– имя операционной машины
– имя сервисной машины
– атрибуты создания теневой копии

В ходе дальнейших исследований встречались случаи, когда копия логического раздела не содержалась на разделе. После проведения до-

полнительных экспериментов на сгенерированных тестовых данных, в которых варьировалось количество теневых копий и изменение данных, было установлено, что на самом деле в этих случаях теневые копии содержатся на логическом разделе, однако они содержат не все компоненты структуры. Не вдаваясь в детальное описание компонентов, указанных в статье [11], будем говорить, что теневая копия содержит такие элементы, как дескриптор метаинформации и дескриптор измененных блоков данных, показанные на рисунке 9. В исследуемых примерах содержались дескрипторы метаинформации, но при этом отсутствовали дескрипторы измененных блоков данных.

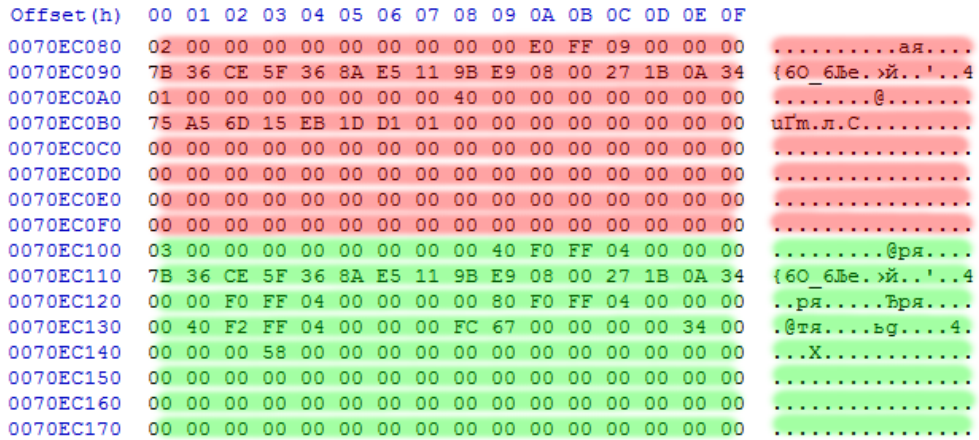


Рис. 9: Дескрипторы метаинформации и измененных блоков данных
– дескриптор метаинформации
– дескриптор измененных блоков данных

После обнаружения случаев, когда в теневых копиях могут отсутствовать дескрипторы, был проведен ряд экспериментов для выявления условий, при которых теневые копии не содержали бы дескрипторов. Для этого в сценарии создания и удаления копий логических разделов была добавлена фиксация записей о событиях, происходящих во время создания тестовых данных. Помимо этого при генерации разных количеств теневых копий у тестовых данных постоянно изменялся объем модифицируемой информации и лимит выделенной памяти для хранения теневых копий.

В ходе этих экспериментов было выявлено, что причиной отсутствия дескрипторов является превышение лимита выделенной памяти

под хранение копий логического раздела. Данный лимит мог быть превышен в следующих случаях:

- При большом количестве генерируемых теневых копий на логическом разделе
- При большом объеме измененных блоков памяти

При дальнейшем анализе было установлено, что можно восстановить содержимое логического раздела на момент создания теневой копии лишь при наличии обоих дескрипторов. Дескрипторы сопоставляются друг с другом при помощи их идентификаторов, которые совпадают у них для конкретной копии логического раздела, как показано на рисунке 10, поэтому дальнейшие исследования были направлены на решение вопроса о том, может ли отсутствующий дескриптор измененных блоков данных быть сохранен в каком-нибудь другом месте.

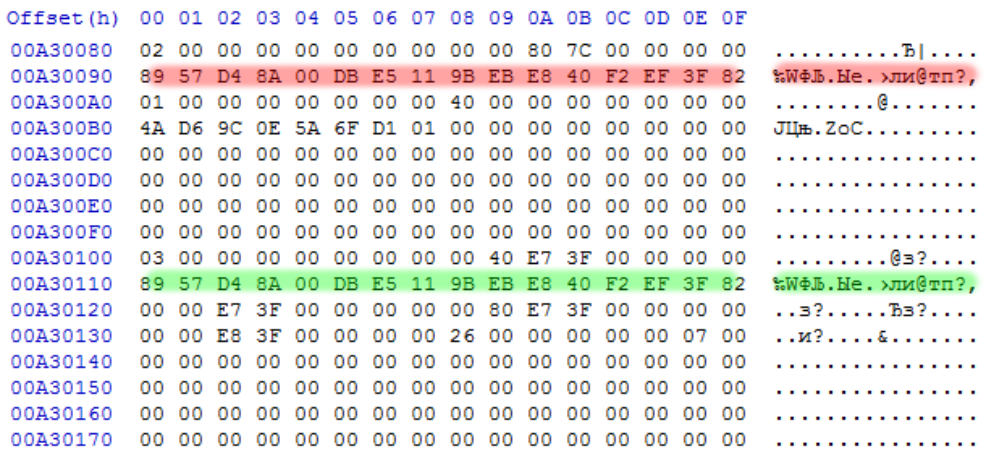


Рис. 10: Сопоставление дескрипторов метаинформациии и измененных блоков данных на основе совпадения GUID
– GUID дескриптора метаинформации
– GUID дескриптора измененных данных

В ходе дальнейших экспериментов были сгенерированы тестовые данные, содержащие несколько логических разделов. При исследовании этих тестовых данных были установлены случаи, когда дескриптор измененных блоков данных одного раздела при превышения лимита памяти сохранялся на другом разделе.

Следующие исследования и эксперименты в рамках данной работы были направлены на выявление способа, определяющего, на каком разделе могут хранится дескрипторы измененных блоков данных текущего раздела. При анализе отличий в заголовках и дескрипторах структуры формата было установлено, что в заголовке, расположенному по смещению 0x00001e00, есть два GUID, которые совпадают при наличии дескриптора метаинформации и дескриптора измененных блоков данных на одном логическом разделе, как отображено на рисунке 11, и отличаются иначе, как показано на рисунке 12. Также установлено, что если значения этих GUID различны, то второй из них совпадает с первым – другого раздела, где и может находится искомый дескриптор.

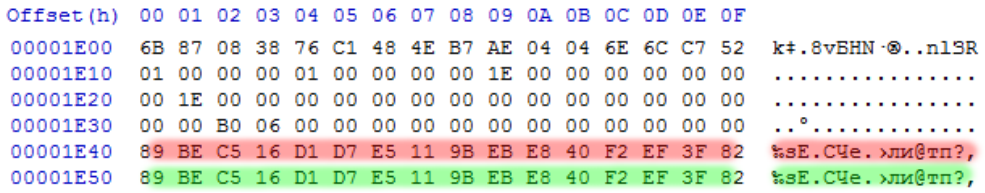


Рис. 11: Случай совпадения GUID текущего раздела и раздела, где может хранится дескриптор измененных данных

– GUID текущего раздела

– GUID раздела, где может хранится дескриптор измененных блоков данных

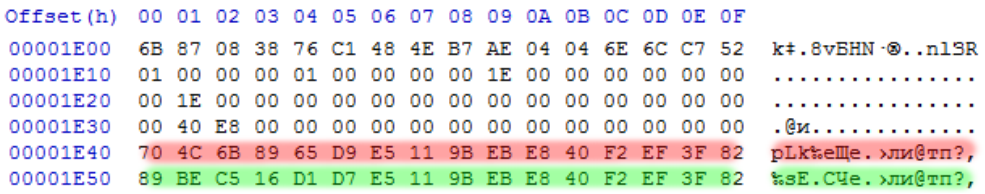


Рис. 12: Случай не совпадения GUID текущего раздела и раздела, где может хранится дескриптор измененных данных

– GUID текущего раздела

– GUID раздела, где может хранится дескриптор измененных блоков данных

3.2.3. Извлекаемая информация

Подтвержденные (в рамках работы) сведения из статьи [11] предоставляют возможность для извлечения следующих данных о теневой копии:

- Время создания копии логического раздела
- Атрибуты создания
- Размер логического раздела
- GUID теневой копии
- GUID набора теневых копий
- GUID дескриптора метаинформации, который совпадает с GUID дескриптора измененных блоков данных
- Имя операционной машины
- Имя сервисной машины

Установленные предположения позволяют извлекать вышеперечисленные данные, когда теневые копии содержит только дескриптор метаинформации, или только дескриптор измененных блоков данных, а также позволяет извлекать информацию, представленную ниже:

- GUID текущего раздела
- GUID раздела, на котором могут быть сохранены дескрипторы измененных блоков данных

Более того в качестве дополнительной информацией может быть указание типа теневой копии, зависящего от содержащихся в нем дескрипторов метаинформации и измененных блоков данных.

4. Разработка компонента поддержки и анализа теневой копии

Belkasoft Evidence Center (BEC) [1] – комплексный программный продукт, разрабатываемый компанией Belkasoft, предназначенный для компьютерных экспертиз, компьютерной криминалистики и расследования корпоративных инцидентов.

Большинство исследованных инструментов поддержки теневой копии не обнаруживают дополнительную информацию о теневых копиях или же поддерживают лишь небольшое количество специальных типов форматов образов устройств хранения информации.

Для возможности анализировать устройства хранения информации и их различные образы, было принято решение о реализации компонента, как часть BEC, так как он поддерживает разбор большого количества типов образов разделов и носителей.

Сперва было решено разработать прототип приложения на основе существующего инструмента Libvshadow с открытым исходным кодом. Изначально предполагалось, что инструмент извлекает всю необходимую информацию о теневой копии, и позволяет отобразить содержимое раздела на момент создания теневой копии.

Для монтирования [6] каждой теневой копии Libvshadow использует сторонний инструмент Dokan [3]. Для работоспособности проектируемого прототипа были созданы надстройки для вызова функции анализа Libvshadow и для управления сервисом [13]: его созданием, удалением, запуском и остановкой, – так как монтирование инструментами Dokan требует постоянной активности последних, контролируемой сервисом.

Полученные результаты работы прототипа оказались неудовлетворительными. На практике разработанный прототип для каждой теневой копии создает символьную ссылку, указывающую на последовательность байт раздела на момент создания теневой копии. Однако для получения содержимого восстановленного раздела необходимо разобрать данную последовательность байт как структуру полноценного раздела. Также не подтвердились предположения об извлечении всех

необходимых данных: к примеру, не извлекались имена операционной и сервисной машин.

При разработке компонента BEC был выбран другой подход, который подразумевал отказ от использования Dokan и разработку необходимого функционала для анализа, основанном на исходном коде инструмента Libvshadow и на дополнении его возможностей.

Первым этапом разработки являлось создание функционала обозначаемого "Analyze Components" для анализа и извлечения всех необходимых данных, наличие которых зависело от содержания в VSC дескрипторов. Следующим этапом была разработка надстройки называемой "Wrapper Handle" для возможности анализа и извлечения данных из всех образов носителей информации, поддерживаемых в BEC. Последним этапом стала реализация функционала обозначаемого "Reader" для чтения данных с копий логического раздела на основе нового функционала для анализа и создания надстройки называемой "Wrapper Reader" для взаимодействия прочитанных данных с ядром BEC, также называемым "Kernel BEC". Структура реализованного компонента показана на рисунке 13.

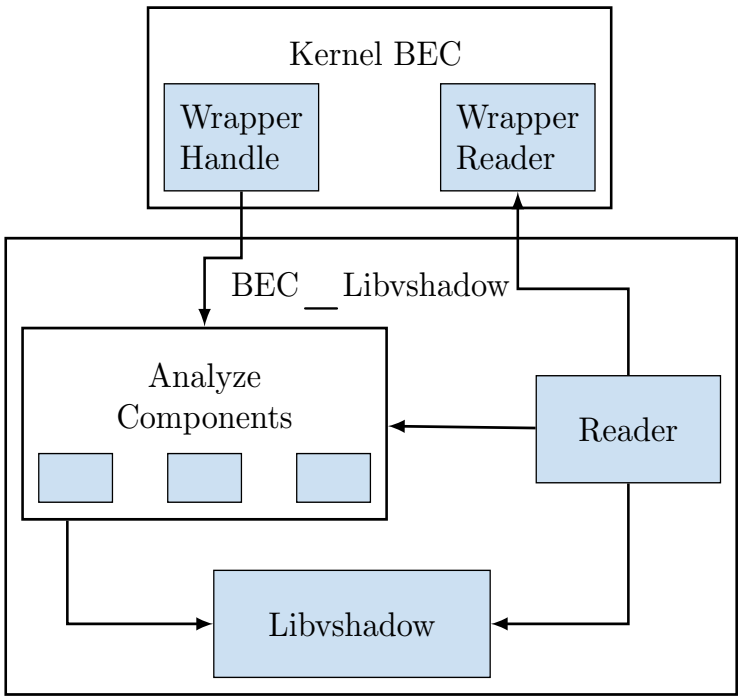


Рис. 13: Структура компонента поддержки и анализа теневой копии

Реализованный компонент извлекает всю отобранную на стадии анализа информацию и отображает содержимое логического раздела (директории и файлы) на момент генерации теневой копии. После тестирования работоспособности компонента поддержки и анализа теневой копии, была проведена его интеграция в BEC.

5. Обзор тост уведомления

Тост уведомление – это уведомление и оповещение о различных событиях или произошедших действиях в сервисах, к примеру, напоминание календаря о мероприятии, непрочитанное сообщение в почтовом сервисе или ответ на ваш пост в социальной сети. Приходящие уведомления отображаются в системной области, называемой Центром уведомлений, показанном на рисунке 14.

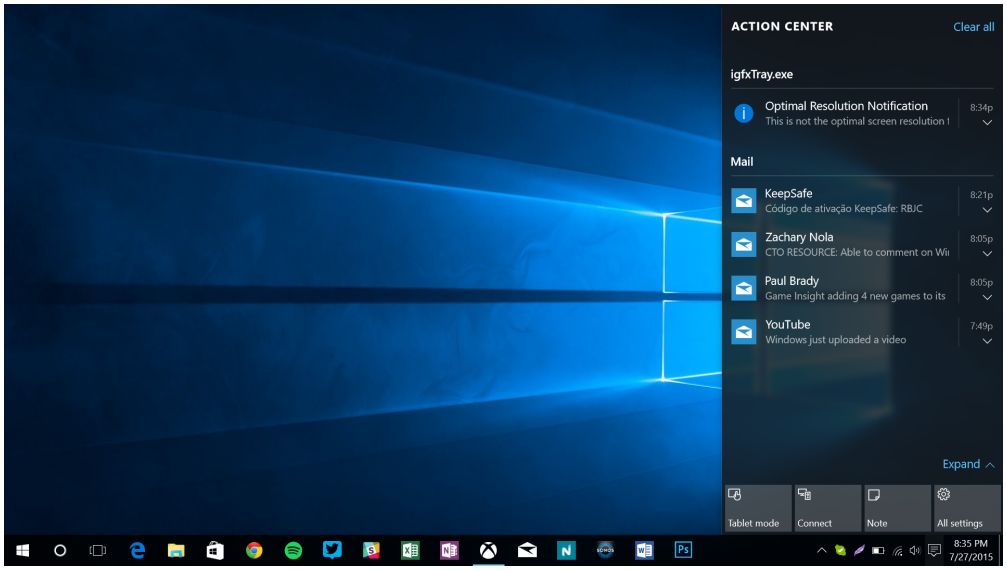
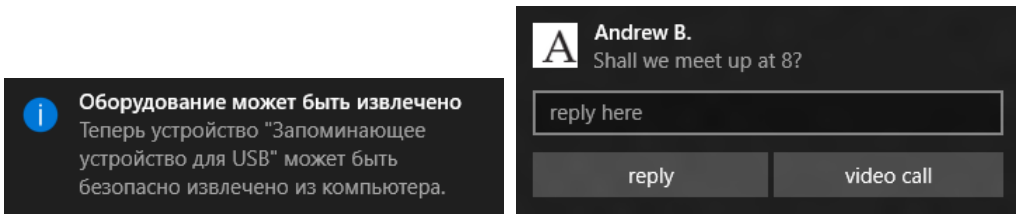


Рис. 14: Различные оповещения в Центре Уведомлений

Уведомления могут быть поделены на две группы: стандартные, имеющие только визуальную часть (тексты и изображения), как отображено на рисунке 15a, и интерактивные, показанные на рисунке 15b, включающие не только визуальную часть, но и различные элементы управления, такие как кнопки, выпадающие списки и поля ввода текста.



(a) Стандартный (b) Интерактивный

Рис. 15: Типы Тост

6. Разбор и анализ тост уведомления

6.1. Хранение данных

Хранение данных об уведомлениях представлено в виде XML разметки, как показано на рисунке 16.

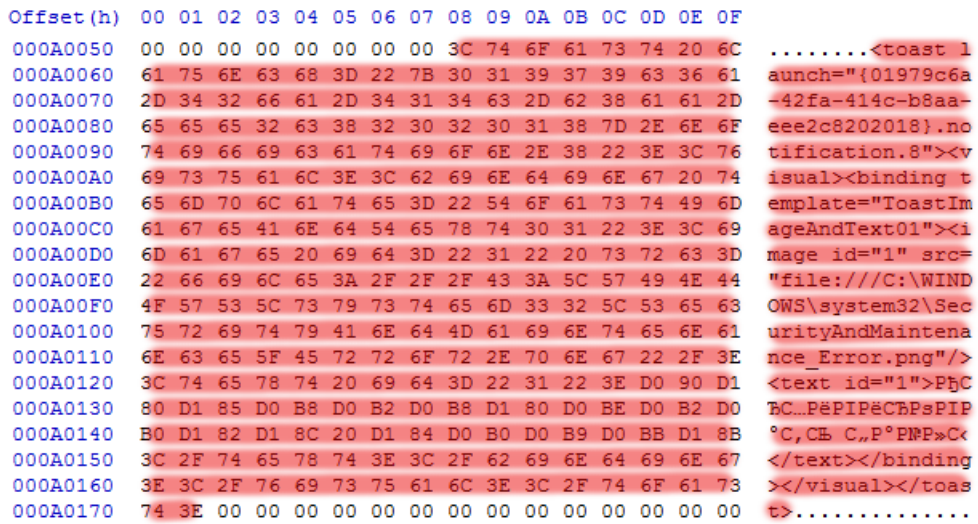


Рис. 16: Пример хранения данных об уведомлении

6.2. Структура

6.2.1. Местоположение

Информация о тост уведомлениях хранится в файле баз данных appdb.dat, который расположен в директории [SystemDisk]:\Users\[UserName]\AppData\Local\Microsoft\Windows\Notifications.

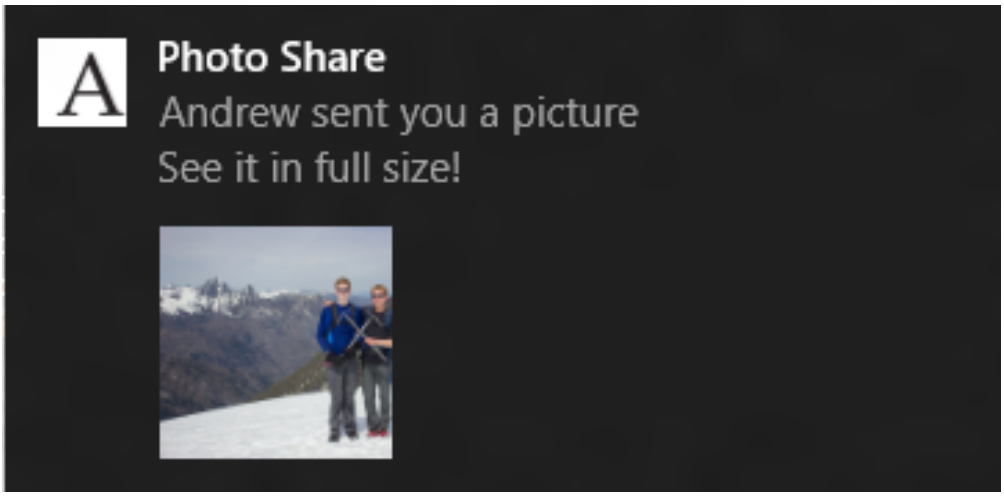
6.2.2. Внутреннее устройство

Основным элементом в структуре XML разметки уведомлений является ”toast”. Этот элемент имеет несколько потомков, обязательным из которых является потомок, называемый ”visual”. Другим потомком, представляющие интерес, является ”actions”. ”Visual”, как потомок toast, может содержать ровно один дочерний элемент – ”binding”, в котором находятся наиболее важные элементы анализа, называемые ”text” и

”image”, хранящие текст и изображение уведомлений соответственно. У элемента ”actions” же потомками являются ”input” и ”action”. Первый может хранит такие элементы управления, как выпадающие списки и поле ввода текста, второй же хранит кнопки, инициирующие определенное поведение. Более подробное описание структур представлено в [12], [14]. Ниже представлен пример структуры Тост, отображенной в листинге 1, и ее визуальное сопоставление, показанное на рисунке 17a.

```
<toast launch="app-defined-string">
  <visual>
    <binding template="ToastGeneric">
      <text>Photo Share</text>
      <text>Andrew sent you a picture</text>
      <text>See it in full size!</text>
      <image placement="appLogoOverride" src="A.png" />
      <image placement="inline" src="hiking.png" />
    </binding>
  </visual>
</toast>
```

Listing (1) Структура



(a) Визуализация

Рис. 17: Пример структуры уведомления и его визуализация

6.2.3. Извлекаемая информация

Исследование и анализ структуры тост уведомления предоставляет возможность для извлечения следующей информации:

- Тексты, которые могут являться частью переписки между пользователями
- Изображения
- Передаваемые в приложения аргументы – строки, которые при активации уведомлений будет переданы в соответствующие приложения, как входные параметры

7. Разработка компонента поддержки и анализа тост уведомления

Разработка компонента включала создание функционала обозначаемого ”Toast Analyzer” для анализ и извлечения необходимой информации, а также реализация надстройки называемой ”Toast Wrapper” для передачи извлеченных данных в BEC. Окончательная версия структуры разработанного компонента представлена на рисунке 18.

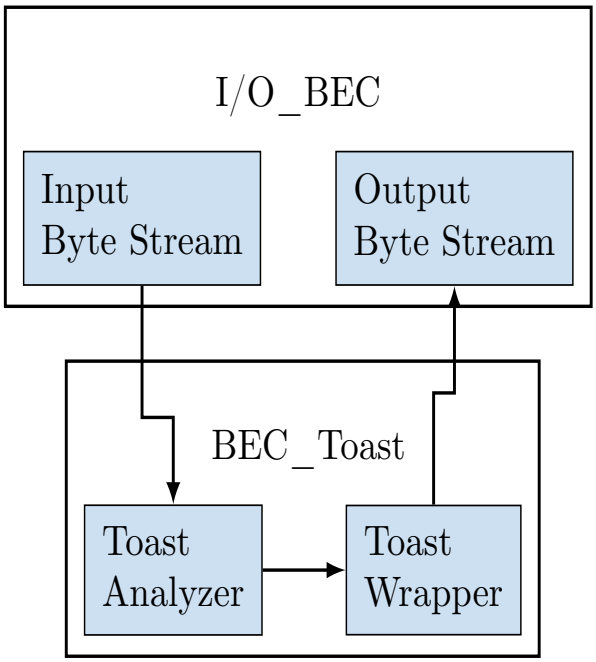


Рис. 18: Структура компонента анализа тост уведомления

Реализованный компонент извлекает всю отобранную на стадии анализа информацию. После тестирования работоспособности компонента анализа тост уведомления, была проведена его интеграция в BEC.

Заключение

В рамках данной работы были получены следующие результаты:

- Исследована структура формата теневой копии
  - Определены местоположение и внутренние элементы
  - Установлена новая информация, пригодная для извлечения, и, как следствие, выявлены различные состояния теневых копий
  - Выделена криминалистически значимая извлекаемая информация
- Исследована структура тост уведомления
  - Определены местоположение и внутренние элементы
  - Выделена криминалистически значимая извлекаемая информация
- Разработаны компоненты анализа тост уведомления и формата теневой копии, которые были интегрированы в продукт цифровой криминалистики

Дальнейшие пути развития:

- Восстановление содержимого логического раздела на момент создания теневой копии в тех случаях, когда дескриптор метаинформации и дескриптор измененных блоков данных находятся на разных логических разделах
- Реализовать восстановление не всего содержимого логического раздела на момент создания теневой копии, а лишь тех файлов и директорий, что подверглись изменениями.

Список литературы

[1] Belkasoft. Belkasoft Evidence Center. — 2015. — URL: https://belkasoft.com/ec (online; accessed: 29.10.2015).

[2] Computer forensics education / A. Yasinsac, R.F. Erbacher, D.G. Marks et al. — Piscataway, NJ, USA : IEEE Educational Activities Department, 2003. — July. — Vol. 1. — P. 15–23. — URL: dx.doi.org/10.1109/MSECP.2003.1219052 (online; accessed: 29.01.2016).

[3] Dokan. Dokan. — 2015. — URL: https://github.com/dokan-dev/dokany (online; accessed: 29.12.2015).

[4] Eilam Eldad. Reversing: secrets of reverse engineering. — John Wiley & Sons, 2005. — P. 595. — ISBN: 0-7645-7481-7.

[5] Forensic Explorer. Forensic Explorer. — 2016. — URL: http://www.forensicexplorer.com/ (online; accessed: 10.01.2016).

[6] Forensics Wiki. Mounting Disk Images // Wikipedia, the free encyclopedia. — 2011. — URL: http://www.forensicswiki.org/wiki/Mounting_Disk_Images (online; accessed: 16.01.2016).

[7] Forensics Wiki. Computer forensics // Wikipedia, the free encyclopedia. — 2013. — URL: http://forensicswiki.org/wiki/Computer_forensics (online; accessed: 27.10.2015).

[8] Guidance Software. EnCase Forensic. — 2016. — URL: https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r (online; accessed: 06.02.2016).

[9] Libyal. Libvshadow. — 2015. — URL: https://github.com/libyal/libvshadow (online; accessed: 12.11.2015).

[10] Magnet Forensics Inc. Internet Evidence Finder. — 2015. — URL: https://www.magnetforensics.com/ (online; accessed: 26.12.2015).

[11] Metz Joachim. Analysis the Windows NT VSS format. — 2013. — URL: https://390edf27cd124f5c044caae3c61c3ef563054824.googledrive.com/host/0B3fBvzttpiiSZDZXRFVMdnZCeHc/Volume%20Shadow%20Snapshot%20%28VSS%29%20format.pdf (online; accessed: 08.10.2015).

[12] Microsoft. Adaptive and interactive toast notifications for Windows 10 // Microsoft Developer, the official blog. — 2016. — URL: https://blogs.msdn.microsoft.com/tiles_and_toasts/2015/07/02/adaptive-and-interactive-toast-notifications-for-windows-10/ (online; accessed: 04.03.2016).

[13] Microsoft. Services // Windows Dev Center. — 2016. — URL: https://msdn.microsoft.com/en-us/library/ms685141.aspx (online; accessed: 20.01.2016).

[14] Microsoft. Toast // Windows Dev Center. — 2016. — URL: https://msdn.microsoft.com/en-us/library/windows/apps/br230846.aspx (online; accessed: 04.03.2016).

[15] Microsoft. Volume Shadow Copy Service. — 2016. — URL: https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb968832(v=vs.85).aspx (online; accessed: 11.01.2016).

[16] Russinovich Mark E., Solomon David A. Microsoft Windows Internals, Fourth Edition: Microsoft Windows Server(TM) 2003, Windows XP, and Windows 2000 (Pro-Developer). — Redmond, WA, USA : Microsoft Press, 2004. — P. 706–711. — ISBN: 0735619174. — URL: http://dl.acm.org/citation.cfm?id=1096142.

[17] Russon Richard, Fledel Yuval. NTFS documentation. — 2004. — URL: http://dubeyko.com/development/FileSystems/NTFS/ntfsdoc.pdf (online; accessed: 09.10.2015).

[18] SP 800-86. Guide to Integrating Forensic Techniques into Incident Response / Karen Kent, Suzanne Chevalier, Timothy Grance,

Hung Dang. — Gaithersburg, MD, United States : National Institute of Standards & Technology, 2006. — URL: http://dl.acm.org/citation.cfm?id=2206298.

[19] Sanderson Forensics. Reconnoitre. — 2016. — URL: http://sandersonforensics.com/forum/content.php?168-Reconnoitre (online; accessed: 15.02.2016).

[20] Vandeven Sally, Filkins Barbara. Forensic Images: For Your Viewing Pleasure. — SANS Institute InfoSec Reading Room, 2014. — 38 p. — URL: https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447.

[21] Wikipedia. Backup // Wikipedia, the free encyclopedia. — 2015. — URL: https://en.wikipedia.org/wiki/Backup (online; accessed: 13.11.2015).

[22] Wikipedia. Action Center // Wikipedia, the free encyclopedia. — 2016. — URL: https://en.wikipedia.org/wiki/Action_Center (online; accessed: 02.03.2016).

[23] Wikipedia. Globally unique identifier // Wikipedia, the free encyclopedia. — 2016. — URL: https://en.wikipedia.org/wiki/Globally_unique_identifier (online; accessed: 08.02.2016).

[24] X-Ways. X-Ways Forensics. — 2016. — URL: http://www.x-ways.net/forensics/index-m.html (online; accessed: 13.01.2016).