У характеристиках файлу відбулося тільки одне змінення, яке на перший погляд придатне для виявлення редагування: додалася дата створення файлу – це поле, наприклад, цифровий диктофон Olympus WS100 залишає пустим. Змінення максимального бітрейту потребує більш ретельного вивчення. Якщо він виходить за межі діапазону бітрейтів, що підтримуються записуючим пристроєм, – це одна з ознак редагування файлу.

Як вбачається з наведеного опису форматів, а також практичного застосування програмного продукту AudioAnalizer, виявлення ознак редагування звукозаписів, виготовлених за допомогою цифрових диктофонів, подальше вдосконалення розробки, більш глибоке вивчення особливостей запису форматів звукових файлів кожним з них є нагальною потребою експертної практики. Подальше вдосконалення програмного продукту AudioAnalizer дасть можливість отримати інструмент, що серед інших відомих засобів вирішить питання дослідження ознак монтажу цифрових звукозаписів, прискорить виконання практичної експертної роботи.

А. В. Чишкала, старший научный сотрудник Харьковского НИИСЭ

ТВЕРДОТЕЛЬНЫЙ НАКОПИТЕЛЬ ИНФОРМАЦИИ КАК ОБЪЕКТ ИССЛЕДОВАНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

Твердотільні накопичувачі інформації (SSD), які містять важливі для слідства дані, часто можуть самі очищатися. Результатом цього процесу стає те, що інформація на SSD безперервно стирається або заміщається сторонніми даними – у такий спосіб, який абсолютно не властивий носіям на базі жорстких магнітних дисків. І, що принципово важливо, усі ці змінення інформації відбуваються за відсутності будь-яких команд від користувача або комп'ютерних програм.

Твердотельные накопители информации (SSD), содержащие важные для следствия данные, зачастую могут сами очищаться. Результатом этого процесса становится то, что информация на SSD непрерывно стирается или замещается посторонними данными – таким способом, который совершенно не свойственен носителям на базе жестких магнитных дисков. И, что принципиально важно, все эти изменения информации происходят при отсутствии каких-либо команд от пользователя или компьютерных программ.

Ныне все больше популярными носителями для хранения данных

становятся SSD-накопители[1]. Этот вид накопителей, а точнее подвид USB-Flash, вытесняют из обихода дискеты и лазерные диски. Преимущества SSD-накопителей практически общеизвестны: это высокая механическая надежность, отсутствие движущихся частей, малый вес, меньшее энергопотребление, «высокая» скорость чтения/записи.

Получив широкое распространение, данный вид накопителей все чаще становится объектом исследования в компьютерно-технической экспертизе. Исследовать SSD-накопители привычным способом, как это делалось с накопителями на жестких магнитных дисках (НЖМД), не совсем корректно, поскольку SSD-накопители при подключении питания уже сами могут изменять хранящуюся на них информацию без запроса операционной системы. Чтобы понять логику работы и почему это происходит, необходимо рассмотреть принцип хранения информации на SSD-накопителях.

Традиционный SSD-накопитель размером 2,5 дюйма внешне выглядит так же, как и обычный НЖМД, однако если снять защитный корпус, то внешний вид платы будет очень похож на USB-Flash. Внешний вид плат SSD и USB-Flash накопителей отображен на рис. 1, 2 соответственно. Как видно из них, отличий не так уж и много. По сути SSD-накопитель – это несколько увеличенный USB-Flash накопитель. В отличие от USB-Flash накопителя, в SSD используется микросхема DDR DRAM кеш-памяти в связи со спецификой работы и возросшей в несколько раз скоростью обмена данными между контроллером и интерфейсом SATA, а также несколько (обычно максимум до 16) модулей памяти Flash.

Flash модули сохраняют информацию в массиве транзисторов типа NAND с плавающим затвором, называемых ячейками (англ. cell). В настоящее время используются три типа памяти NAND: SLC (Single Level Cell), MLC (Multi Level Cell) и TLC (Three Level Cell). Отличие между ними только в том, что SLC позволяет хранить в каждой ячейке только один бит информации, MLC – два, а TLC – три (за счет использования разных уровней электрического заряда на плавающем затворе транзистора), что делает память MLC и TLC более дешевой относительно SLC.

Однако память MLC/TLC обладает меньшим ресурсом (100 тыс. циклов стирания у SLC, в среднем 10 тыс. для MLC, а для TLC – до 5 тыс.) и худшим быстродействием. С каждым допол-

[1] Полупроводниковый накопитель (англ. SSD, solid-state drive) – перезаписываемое компьютерное запоминающее устройство без движущихся механических частей. Называть его «диском» неправильно, так как в конструкции SSD не присутствуют диски как таковые: накопитель состоит из микросхем памяти и контроллера, подобно флеш-памяти. Следует различать полупроводниковые накопители, основанные на использовании энергозависимой (RAM SSD) и энергонезависимой (NAND, или Flash SSD) памяти [Электронный ресурс]. — Режим доступа : http://ru.wikipedia.org/wiki/SSD. — 16.05.2011.

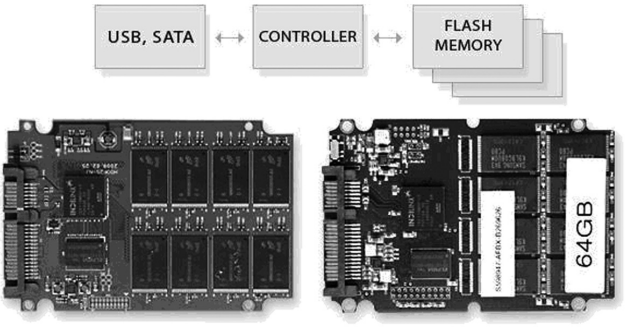

Рис. 1. Внешний вид платы SSD накопителя

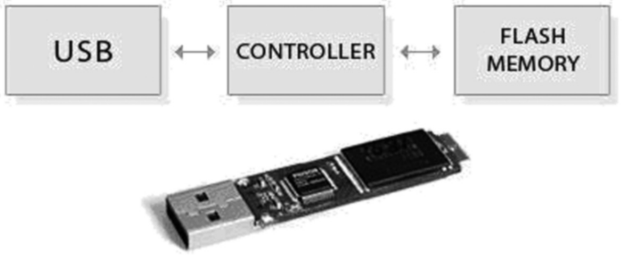

Рис. 2. Внешний вид платы USB-Flash накопителя

нительным уровнем усложняется задача распознавания уровня сигнала, увеличивается время поиска адреса ячейки, повышается вероятность ошибок. Поскольку SLC-чипы намного дороже и объем их памяти меньше, то для массовых решений применяют в основном MLC/TLC-чипы. На данный момент MLC/TLC память активно развивается и по скоростным характеристикам приближается к SLC. Низкую скорость MLC/TLC производители SSD-накопителей компенсируют алгоритмами чередования блоков данных между микросхемами памяти (одновременная запись/чтение в две микросхемы флэш-памяти, по байту в каждую) по аналогии с технологией хранения информации на нескольких устройствах (RAID 0), а низкий ресурс – перемешиванием и слежением за равномерным использованием ячеек. Плюс к этому в SSD резервируется часть объема памяти (иногда до 20 %). Это недоступная память для стандартных операций записи/чтения. Она необходима как резерв в случае износа ячеек по аналогии с НЖМД, который имеет резерв для замены сбойных блоков. Дополнительный резерв ячеек используется динамически и по мере физического изнашивания основных ячеек предоставляет резервные ячейки на замену.

Учитывая меньшие показатели количества перезаписей[1], при традиционном использовании, служебные области файловых систем (такие, как таблицы размещения файлов и др.) быстро расходовали ресурс некоторых ячеек, что приводило к полной невозможности дальнейшего использования устройства. Для решения этой проблемы сначала разработали модифицированные файловые системы (exFAT для Microsoft Windows и JFFS2, YAFFS для GNU/Linux), а впоследствии стали использовать программную часть контроллера и отказались от модифицированных файловых систем.

Главными задачами контроллера устройства являются обеспечение операций чтения/записи и управление структурой размещения данных. Основываясь на матрице размещения блоков (страниц), зная в какие ячейки уже проводилась запись, а в какие – еще нет, контроллер должен оптимизировать скорость записи и обеспечить максимально длительный срок службы SSD-накопителя. Вследствие особенностей построения NAND-памяти, используемой на Flash модулях, работать с ее каждой ячейкой отдельно нельзя. Ячейки объединены в страницы объемом по 4 Кб, и записать информацию можно, только полностью заняв страницу. Стирать данные можно по блокам, которые равны 512 Кб. Все эти ограничения накладывают определенные обязанности на правильный интеллектуальный алгоритм работы контроллера. Поэтому правильно настроенные и оптимизированные алгоритмы контролера могут существенно повысить производительность и долговечность работы SSD-накопителя.

Для чтения/записи блока данных на НЖМД сначала нужно вычислить, где он находится, потом переместить блок магнитных головок на нужную дорожку, подождать, пока необходимый сектор окажется под головкой, и произвести считывание/запись информации. Причем хаотические запросы к разным областям жесткого диска еще больше увеличивают время доступа/записи. При таких запросах НЖМД вынужден постоянно перемещать блок магнитных головок по всей поверхности жестких дисков.

В SSD-накопителе считывание информации выполняется просто – вычисляется адрес нужного блока и сразу же получают к нему доступ для чтения. Никаких механических операций – все время уходит на трансляцию адреса и считывание. Чем быстрее Flash-память, контроллер и внешний интерфейс, тем быстрее доступ к данным. При этом запись информации представляет собой нетривиальный процесс. Микросхемы NAND флэш-памяти оптимизированы для секторного выполнения операций. При модификации нескольких байт внутри некоторого блока или страницы контроллер выполняет следующую примерную последовательность действий:

[1] Для НЖМД этот показатель превышает 1 млн.

1) считывает страницу, содержащую модифицируемую страницу во внутренний буфер/кеш (4 Кб или 512 Кб в зависимости от занятого/измененного пространства);

2) модифицирует необходимые байты;

3) вычисляет новое местоположение блока в соответствии с требованиями алгоритма перемешивания;

4) стирает страницы (блок страниц) в микросхеме Flash-памяти, если она не приготовлена к записи;

5) записывает блок на новое место;

6) изменяет матрицу размещения блоков (страниц).

Но как только информация записана, страница не может быть перезаписана до тех пор, пока не будет очищена. Проблема заключается в том, что минимальный размер записываемой информации не может быть меньше 4 Кб, а минимальный размер стираемой информации не может быть меньше 512 Кб. Для этого контроллер группирует и переносит данные для освобождения целого блока.

Вот тут и сказывается оптимизация операционной системы (ОС) для работы с накопителями информации. При удалении файлов ОС не производит физическую очистку секторов на диске, а только помечает файлы как удаленные, и знает, что занятое ими место можно заново использовать. Работе самого SSD-накопителя это никак не мешает, и разработчиков интерфейсов этот вопрос раньше не «тревожил». Если такой метод удаления помогает повысить производительность при работе с НЖМД, то при использовании SSD-накопителя это становится серьезным ограничением при записи и уменьшает срок его службы.

В SSD-накопителе, как и в традиционных жестких дисках, данные все еще хранятся после того, как они были удалены ОС. Но дело в том, что ОС SSD-накопителя не знает, какие из хранящихся данных являются полезными, а какие – уже не нужными, и вынуждена обрабатывать все занятые блоки по длинному алгоритму: прочитать, модифицировать и снова записать на место после очистки затронутых операцией ячеек памяти, которые с точки зрения ОС уже «удалены». Следовательно, чем больше блоков на SSD-накопителе содержат удаленные данные, тем чаще приходится прибегать к процедуре чтение > модификация > очистка > запись вместо прямой записи. Здесь пользователи SSD-накопителей сталкиваются с тем, что их быстродействие заметно снижается по мере заполнения файлами. Накопителю просто не хватает заранее «стертых блоков» и их приходится подготавливать непосредственно перед записью целым блоком. Максимум производительности демонстрируют «чистые» накопители, а вот в ходе их эксплуатации реальная скорость понемногу начинает снижаться.

Раньше в интерфейсе ATA просто не было команд для физической очистки блоков данных после удаления файлов на уровне

ОС. Для НЖМД они просто не требовались, но появление SSD-накопителей заставило пересмотреть отношение к этому вопросу. В результате в спецификации ATA появилась новая команда DATA SET MANAGEMENT, известная как Trim. Она позволяет ОС на уровне драйвера собирать сведения об удаленных файлах и передавать освобожденные секторы контроллеру накопителя.

В периоды простоя ОС SSD-накопителя самостоятельно осуществляет очистку и дефрагментацию блоков, отмеченных в ней как удаленные. Контроллер перемещает данные так, чтобы получить как можно больше ячеек памяти с предварительно очищенной информацией, освобождая место для последующей записи. Это дает возможность сократить задержки, возникающие в ходе работы.

Нами были проведены некоторые исследования относительно записи и восстановления информации с SSD-накопителей. Для этого было проведено два исследования:

— на запись информации, ее частичное удаление и восстановление;

— полное удаление информации путем быстрого форматирования, и попытка ее восстановления.

Для первого исследования на SSD-накопитель (полностью очищенный, что равнозначно новому накопителю) были записаны 5 тыс. файлов (заполнено примерно 10 % его объема) в несколько потоков (для того, чтобы организовать дефрагментацию файлов и усложнить восстановление, имитируя обычную работу пользователя). Затем 100 файлов были произвольным образом изменены и еще 100 файлов удалены. После этого SSD-накопитель был отключен от ноутбука и подключен к стендовой машине с блокировкой записи. При сканировании поверхности информации SSD-накопителя программным продуктом X-Ways Forensics были обнаружены имеющиеся и удаленные файлы, которые можно было восстановить. При использовании дополнительных алгоритмов восстановления данных, нам частично удалось восстановить предыдущее состояние измененных 100 файлов. При подсчете контрольной суммы алгоритмом MD5 всего объема информации до и после исследования суммы не отличались.

Повторив операцию подготовки и записав на ноутбуке еще 5 тыс. файлов большего размера, чтобы заполнить примерно 90 % его объема, а затем, удалив 1000 произвольных файлов, мы провели еще одно исследование.

При сканировании всего объема информации SSD-накопителя программным продуктом X-Ways Forensics были обнаружены имеющиеся и удаленные файлы. При этом можно было восстановить всего примерно 400[1] удаленных файлов (было удалено 1100 файлов

[1] Под восстановлением подразумевается воссоздание информации в состояние перед удалением, поскольку ссылки на файлы остаются в таблице размещения

за два исследования). При повторном сканировании через 10 мин можно было восстановить уже не более 100 файлов. При подсчете контрольной суммы алгоритмом MD5 всего объема информации до и после исследования результаты *отличались*.

Для второго исследования SSD-накопитель был отформатирован средствами ОС в быстром режиме, а затем исследован на стендовом компьютере. При сканировании всего объема информации SSD-накопителя программным продуктом X-Ways Forensics были обнаружены удаленные файлы. При этом можно было восстановить примерно 100 удаленных файлов (было удалено более 10 тыс. файлов за два предыдущих исследования). При повторном сканировании через 10 мин восстанавливать было нечего, практически весь объем, за исключением служебных областей файловой системы, не содержал информации. При подсчете контрольной суммы алгоритмом MD5 всего объема информации до и после исследования результаты *отличались*.

Учитывая, что в момент исследования исключалась возможность записи на SSD--накопитель, единственным возможным вариантом изменения информации является внутренняя функция оптимизации[1], которая была запущена в момент включения питания на стендовом компьютере. Вероятно, функция оптимизации не запускалась в начале первого исследовании, поскольку было достаточно блоков для записи, и это не влияло на производительность SSD-накопителя в целом.

Кроме того, производители переносных устройств USB-Flash начинают применять алгоритмы записи, аналогичные SSD-накопителям, используя две микросхемы памяти и усложненный контроллер.

У нас был на исследовании USB-Flash Survivor емкостью 16 Гб и файловой системой NTFS, с которого был снят образ и проведено исследование с подсчетом контрольной суммы алгоритмом MD5, после чего образ был удален. В процессе исследования других накопителей по этому же делу обнаружилась информация, которая могла содержаться и на USB-Flash Survivor. При повторном исследовании оказалось, что информация, содержащаяся на носителе, отличалась от первоначального исследования, поскольку отличалась контрольная сумма MD5. В дальнейшем было установлено, что были частично очищены удаленная и перезаписанная области данных. Это свидетельствует об аналогичных алгоритмах, применяемых на SSD-накопителях.

Исходя из способа записи на SSD-накопитель, можно сделать следующие выводы:

файлов, ПП X-Ways Forensics эти ссылки восстанавливает, однако SSD-накопитель уже обнулил секторы, содержащие удаленные файлы. Это означает, что файл невозможно восстановить.

[1] Эта функция известна как «уборка мусора» (от англ. **cleaning garbage).**

— при перезаписи информации в файле, можно с большой вероятностью восстановить его предыдущее состояние (ибо старая и новая копии хранятся на накопителе одновременно, при этом старая копия может быть перезаписана/стерта новыми данными с малой вероятностью);

— при удалении файла его можно восстановить с большей вероятностью, чем на НЖМД (ибо алгоритм перемешивания и увеличения срока службы накопителя нескоро позволит записать в данный блок информацию);

— существенно ограничить восстановление информации может команда Trim ATA интерфейса, которая позволяет подготавливать ячейки на запись для удаленных областей файловой системы (фактически удалять информацию);

— накопитель информации может самостоятельно без команды пользователя или ОС произвести очистку перезаписанных блоков (фактически удалять информацию о предыдущем состоянии файла);

— в процессе исследования ОС SSD-накопителя может изменять его состояние, т. е. эксперт фактически не обладает средствами, чтобы зафиксировать (создать точную копию-образ) хранящуюся на нем информацию.

Считаем, что для решения этих проблем необходим программно-аппаратный комплекс для снятия данных непосредственно с микросхем хранения данных Flash-памяти, минуя контроллер устройства. При исследовании Интернет-ресурсов нами был найден только программно-аппаратный комплекс PC-3000 Flash, который позволяет восстанавливать данные с SSD-накопителей с использованием выпаивания микросхем памяти. Однако этот способ не соответствует требованиям типичного исследования, поскольку приводит к последующей неработоспособности SSD-накопителя в целом, и может быть использован только для восстановления информации с поврежденного SSD-накопителя.

Текущее состояние исследований данных на SSD-накопителях представляется нам как словосочетание *«стереть нельзя восстановить»*, и правильно поставить запятую предстоит в ближайшем будущем.