УДК 681.3.06(075)

С. Д. Прокопенко, С. Р. Коженевский
Лаборатория компьютерной криминалистики
ул. Верхний Вал, 44, 04071 Киев, Украина
тел.: (044) 425-23-42

О копировании данных НЖМД с дефектными секторами при производстве компьютерно-технических экспертиз

Описаны проблемы копирования данных накопителей на жестких магнитных дисках, имеющих дефектные сектора. Приведены результаты тестирования различных аппаратных блокираторов записи при копировании данных с дефектных дисков. Предложен специализированный блокиратор записи собственной разработки с функцией восстановления информации.

***Ключевые слова**: копирование данных, компьютерно-технические экспертизы, НЖМД, дефектный сектор, блокиратор записи.*

В подавляющем количестве случаев процесс производства компьютерно-технических экспертиз на цифровых носителях информации начинается с создания точной побитовой копии исследуемого накопителя. Поэтому от целостности и полноты копии зависят все последующие этапы экспертного исследования.

При этом в процессе создания копии должна быть обеспечена защита от случайного или намеренного внесения изменений в данные на исследуемых носителях информации. Для выполнения этого требования при производстве компьютерно-технических экспертиз обязательно применение аппаратных блокираторов записи (hardware write blocker). Указанный блокиратор — это специализированное устройство, блокирующее передачу через интерфейс на исследуемый накопитель всех команд, которые могут привести к модификации данных, но обеспечивающее прозрачный доступ к данным в режиме чтения [1].

В настоящее время на рынке доступно сравнительно большое количество различных моделей блокираторов записи, которые отличаются поддерживаемыми интерфейсами, наборами используемых команд, скоростью передачи и т.п. При этом производители зачастую не предоставляют подробного технического описания предлагаемых устройств. В первую очередь это касается их работы с поврежденными и нестабильно работающими накопителями на жестких магнитных дисках (НЖМД). Однако для экспертов критически важно иметь полное представление о возможностях и ограничениях используемых ими инструментов, чтобы быть уверенными в их надежности и целостности полученных результатов.

Одной из наиболее распространенных проблем при копировании данных НЖМД является разрушение его рабочих поверхностей, которое проявляется в появлении нечитаемых участков магнитной поверхности (в виде дефектных секторов). Причинами их возникновения могут стать: естественный износ, удары и повышенная вибрация при транспортировке, перегрев, перепады напряжения питания и другие факторы.

При обращении к дефектному сектору, управляющий контроллер НЖМД завершает команду с формированием признака ошибки. Механизм обработки данных при возникновении такой ситуации зависит от приложений, операционной системы (ОС), набора драйверов, аппаратной реализации контроллера хоста, типа интерфейса накопителя. Во многих случаях обращение к дефектному сектору приводит к нестабильной работе компьютера и часто к зависанию ОС и приложений. Многие специальные экспертные средства, как программные, так и аппаратные, не обеспечивают возможность обмена данными с НЖМД, имеющими дефектные сектора, что приводит к невозможности создания полной побитовой копии данного накопителя либо к значительным временным задержкам при создании его побитовой копии.

Так, в [2] проведено сравнение программного обеспечения (ПО) для копирования данных при работе с дефектными НЖМД. По результатам тестирования, только 2 из 5-ти исследуемых программных продуктов обеспечили возможность копирования всех неповрежденных секторов.

Авторами было проведено тестирование доступных в Украине аппаратных блокираторов записи интерфейса SATA при работе с дефектными НЖМД. Тестирование проводилось на НЖМД, имеющем 48 дефектных секторов с известными адресами. Копирование осуществлялось при помощи ПО: X-Ways Forensics, FTK Imager. Результаты тестирования приведены в таблице.

Результаты тестирования блокираторов записи

	EPOS WriteProtector	**ICS SuperDriveLock**	**Tableau T35es**
Количество непрочитанных секторов	48	26*	214
Средняя скорость копирования, ГБ/мин	2,37	2,38	2,0

* Прибор завис при копировании. Полная копия не была получена.

Второй проблемой копирования данных с дефектных НЖМД является то, что при обнаружении дефектного сектора ОС выполняет многократные последовательные попытки чтения данных из такого сектора. Однако кроме увеличения времени копирования, это создает еще одну проблему. В ряде случаев разрушение поверхности быстро прогрессирует, причем с определенного момента этот процесс становится необратимым. Это может привести к полной потере данных в процессе их копирования.

Как показывает практика, до начала копирования эксперт не имеет возможности оценить состояние НЖМД и наличие дефектных и нестабильно читаемых секторов, особенно при проведении работ вне лаборатории. В результате это мо-

жет приводить к потере информации и/или значительным временным затратам на этапе создания побитовой копии. Таким образом, требуются специализированные инструментальные средства, обеспечивающие возможность работы с дефектными НЖМД.

Такие средства должны удовлетворять следующим основным требованиям:

1) предотвращать возможность модификации данных на НЖМД-источнике;

2) обеспечивать копирование доступных данных из рабочих (не дефектных) секторов;

3) осуществлять пропуск дефектных секторов;

4) производить запись по адресам дефектных секторов в копии специальных данных — маркеров, которые позволят идентифицировать их присутствие на НЖМД при дальнейших этапах экспертного исследования.

Кроме того, эти средства должны обладать простым интерфейсом и обеспечивать максимально достижимую для конкретного дефектного НЖМД скорость копирования.

Изложенные требования реализованы в специально разработанном блокираторе записи EPOS BadDrive Adapter, который предназначен для работы с дефектными НЖМД с интерфейсом ATA.

EPOS BadDrive Adapter представляет собой компактный прибор, который включается в разрыв между ПК и жестким диском и анализирует передаваемые по интерфейсу команды (рис. 1).

Рис. 1. Внешний вид прибора EPOS BadDrive Adapter

При отсутствии на НЖМД ошибок прибор работает в режиме традиционного аппаратного блокиратора записи. Если при попытке чтения из дефектного сектора команда завершается с ошибкой или не выполняется в установленное время, он перехватывает управление диском, блокируя передачу сообщения об ошибке в систему. При этом в зависимости от характера дефекта в компьютер передаются

либо считанные данные, либо маркер дефектного сектора. Функциональная схема прибора EPOS BadDrive Adapter приведена на рис. 2.

При отсутствии дефектных секторов на исследуемом НЖМД (источнике) прибор работает прозрачно для рабочей станции эксперта (хоста), выполняя только функцию блокировки записи.

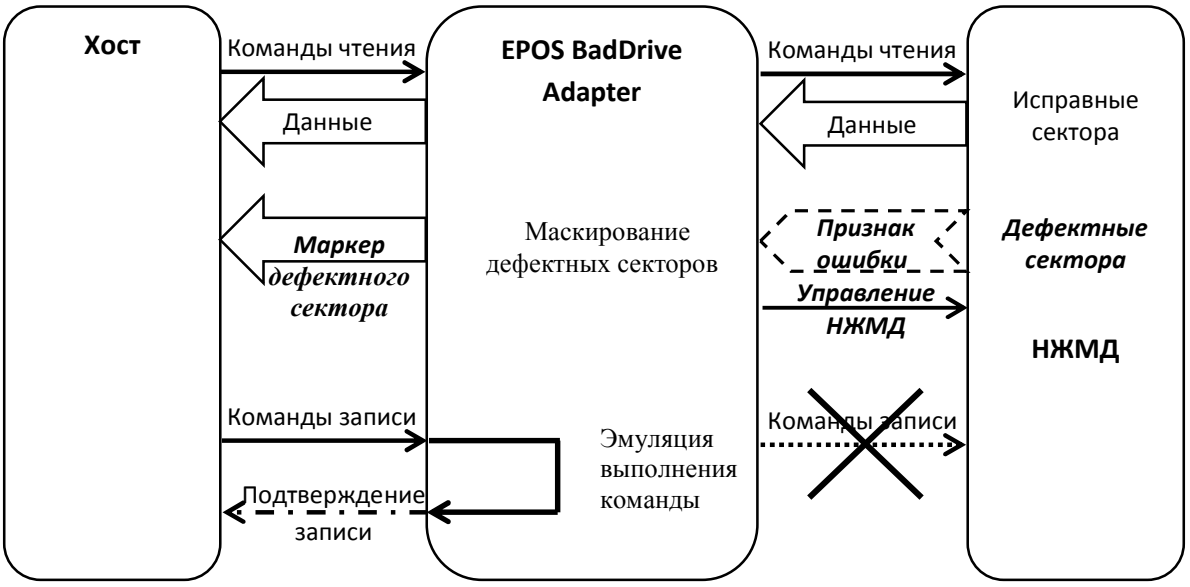

Рис. 2. Функциональная схема прибора EPOS BadDrive Adapter

При обнаружении дефектного сектора на НЖМД прибор может работать в одном из двух режимов [3].

1. Маскирование дефектных секторов. В этом режиме задается определенный временной интервал выполнения команды, величина которого выбирается меньше таймаута, устанавливаемого хост-системой.

Если до завершения этого временного интервала команда завершается с ошибкой, то прибор не транслирует хосту признак ошибки. Вместо этого в хост передается подтверждение успешного выполнения команды. Если НЖМД не успевает выполнить команду в течение заданного временного интервала, то прибор прерывает выполнение текущей операции путем выдачи сигнала HRESET на накопитель и готовит его к приему следующей команды хоста.

В обоих случаях вместо непрочитанных данных хосту передается маркер дефектного сектора. Хост при этом не получает сообщений об ошибках.

2. Перехват и выполнение команды под управлением прибора. В этом режиме перехватываются и анализируются все команды чтения, передаваемые по интерфейсу. Если команда завершается с ошибкой, прибор захватывает управление диском и осуществляет ряд повторных чтений данных.

Благодаря маскированию признака ошибки для хост-системы все такие команды завершаются успешно. Содержание данных, передаваемых прибором в хост-систему, зависит от результатов чтения этих секторов прибором. Если по-

вторное считывание завершается успешно, в компьютер передаются считанные данные. Для секторов, данные из которых считать не удалось, передается маркер дефектного сектора. Как и в предыдущем случае, хост не получает сообщений об ошибках.

В результате стандартная ОС и приложения получают возможность работать с поврежденными НЖМД как с исправными, без возможных сообщений об ошибках и зависаний. Прибор совместим с ПО для создания образов и анализа данных X-Ways Forensics, FTK, EnCase и др. и обеспечивает возможность копирования и исследования данных на НЖМД с интерфейсами SATA и PATA любых производителей.

Таким образом, применение EPOS BadDrive Adapter при производстве компьютерно-технических экспертиз позволяет сократить временные затраты на создание копий и повысить эффективность работы экспертов.

Выводы

1. До начала процесса копирования данных эксперт не имеет возможности оценить работоспособность НЖМД и наличие на нем дефектных и нестабильно читаемых секторов, что может приводить к потере информации на НЖМД и/или значительным временным затратам на этапе создания его побитовой копии.

2. Для копирования данных с НЖМД, имеющих дефектные сектора, требуются специализированные инструментальные средства.

3. Специализированный блокиратор записи EPOS BadDrive Adapter позволяет сократить временные затраты на создание копий и повысить эффективность работы экспертов.

1. *Коженевский С.Р.* Методика тестирования аппаратных блокираторов записи, применяемых в процессе расследования компьютерных происшествий / С.Р. Коженевский, С.Д. Прокопенко // Реєстрація, зберігання і оброб. даних. — 2011. — Т. 13, № 3. — С. 63–71

2. *James R. Lyle.* Issues with Imaging Drives Containing Faulty Sectors / James R. Lyle, Mark Wozar // Digital Investigation. — 2007. — P. S13–S15.

3. *Блокиратор* записи EPOS BadDriveAdapter. Руководство пользователя. Вер. 1.0. ООО «ЕПОС». — 2011. — Режим доступа: www/URL: http://forensictools.com.ua/attachment.php?id_attachment=33.

Поступила в редакцию 08.11.2013