8. Логирование информации /.hostinfo [Електронний ресурс]. — Режим доступу: http://hostinfo.ru/articles/security/rubric157/1062/
9. Лог / wikipedia [Електронний ресурс]. — Режим доступу:
10. http://uk.wikipedia.org/wiki/Лог
11. Файл регистрации / wikipedia [Електронний ресурс]. — Режим доступу: http://ru.wikipedia.org/wiki/Файл_регистрации

Резюме

В статье раскрывается понятие лог-файлов сервисов, приводятся их типы. Раскрывается понятие файлов-отчетов диагностических утилит. Также в статье рассмотрены параметры логирования. В конце статьи приводятся основные моменты, которые необходимо уточнить при получении на исследование лог-файла или файла-отчета для эффективного исследования этих файлов.

Summary

In the paper notion of log-files of services is disclosed, their types are specified. Notion of diagnostic report files is disclosed. Also log parameters are considered in the paper. At the end of the paper basic points are given, which need to be clarified, when a log-file or a report file is received for examination in order to examine them efficiently.

С.Д. Прокопенко, нач. лаборатории

ООО "ЕПОС"

ПРОБЛЕМЫ КОПИРОВАНИЯ ДАННЫХ С НАКОПИТЕЛЕЙ С ДЕФЕКТНЫМИ СЕКТОРАМИ ПРИ ПРОИЗВОДСТВЕ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

В соответствии с Криминальным процессуальным кодексом Украины [1] в обязанности эксперта входит обеспечение сохранности объекта экспертизы. При производстве компьютерно-технических экспертиз это требование фактически означает необходимость предотвращения внесения изменений в данные на исследуемых носителях информации.

В большинстве случаев, как свидетельствует практика, для выполнения этого требования эксперты создают побитовую копию исследуемого накопителя на жестких магнитных дисках (НЖМД) и в дальнейшем проводят исследование именно копии, не работая с оригиналом. Поэтому от целостности и полноты копии зависят все последующие этапы экспертного исследования.

Одной из наиболее распространенных проблем при копировании данных является разрушение рабочих поверхностей НЖМД, которое

проявляется в форме нечитаемых участков, т.н. дефектных секторов. Причинами их возникновения могут быть естественный износ, удары и вибрация при транспортировке, перегрев, перепады напряжения и другие факторы.

При обращении к дефектному сектору НЖМД завершает команду с признаком ошибки. Механизм обработки такой ситуации зависит от приложения, операционной системы (ОС), набора драйверов, аппаратной реализации контроллера хоста, типа интерфейса накопителя. Во многих случаях обращение к дефектному сектору приводит к нестабильной работе и зависаниям ОС и приложений. Многие специальные экспертные средства, как программные, так и аппаратные, не обеспечивают возможность работы с НЖМД с дефектными секторами, что приводит к невозможности создания полной побитовой копии либо к значительным временным задержкам.

Так, в одной из работ [2] проведено сравнение ПО для копирования данных при обращении с дефектными НЖМД. По результатам тестирования, только 2 из 5 исследуемых программных продукта обеспечили возможность копирования всех неповрежденных секторов. Авторами было проведено тестирование популярных в Украине аппаратных блокираторов записи при работе с дефектными НЖМД. Тестирование проводилось на НЖМД, имеющем 48 дефектных секторов с известным месторасположением. Копирование осуществлялось с помощью ПО X-Ways Forensics, FTK Imager. Результаты тестирования приведены в табл. 1.

Второй проблемой копирования данных с дефектных НЖМД является то, что при обнаружении дефектного сектора ОС выполняет многократные последовательные попытки чтения данных такого сектора. Однако, кроме увеличения времени копирования, это создает еще одну проблему. В ряде случаев разрушения поверхности быстро прогрессируют, причем с определенного момента этот процесс стано-

Таблица 1. **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.

вится 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 на нем дефектных и нестабильно читаемых секторов, особенно при работе на выезде. В результате это может 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 следующие основные требования: предотвращение возможности модификации данных на НЖМД-источнике; копирование всех данных из недефектных секторов; пропуск без зависаний дефектных секторов; запись в копию на место дефектных секторов специальных данных — маркеров, которые позволят идентифицировать их наличие на дальнейших этапах экспертного исследования.

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

Описанные принципы реализованы в специализированном блокираторе записи EPOS BadDrive Adapter (рис. 1), предназначенного для работы с дефектными НЖМД с интерфейсом SATA. При отсутствии дефектных секторов на исследуемом накопителе прибор работает прозрачно для рабочей станции эксперта (хоста), выполняя только функцию защиты от записи.

При обращении к дефектному сектору 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 интервала команда завершается с ошибкой, то прибор не транслирует хосту признак ошибки. Вместо это-

Рис. 1. Внешний вид EPOS BadDrive Adapter

го в хост передается подтверждение успешного выполнения команды. Если НЖМД не успевает выполнить команду в течение заданного временного интервала, то прибор прерывает выполнение 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 повторное 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.

EPOS BadDrive Adapter представляет собой компактный адаптер, который включается в разрыв между ПК и жестким диском и анализирует передаваемые по интерфейсу команды. При отсутствии на НЖМД ошибок, он 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 сосчитанные данные, либо маркер дефектного сектора.

В результате стандартная ОС и приложения получают возможность работать с поврежденными HDD, 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. Таким образом, применение EPOS BadDrive Adapter при производстве компьютерно-технических экспертиз позволяет сократить временные затраты на создание копий и повысить эффективность работы экспертов.

Выводы. До начала копирования эксперт не имеет возможности оценить наличие на НЖМД дефектных и нестабильно читаемых секто-

ров, что может приводить к потере информации и/ или значительным временным затратам на этапе создания побитовой копии.

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

Применение специализированного блокиратора записи EPOS BadDrive Adapter позволяет сократить временные затраты на создание копий и повысить эффективность работы экспертов.

Список использованной литературы

1. Кримінальний процесуальний кодекс України. Відомості Верховної Ради України (ВВР). — 2013. — № 9–10, № 11–12, № 13, ст. 88.
2. Lyle J.R., Wozar M. Issues with imaging drives containing faulty sectors / J.R. Lyle, M. Wozar // Digital Investigation. 2007. S13-S15.
3. Блокиратор записи EPOS BadDriveAdapter. Руководство пользователя. Вер. 1.0. ООО "ЕПОС". 2011. — Режим доступу: Www/ URL: http://forensictools.com.ua/attachment.php?id_attachment=33.

С.О. Юлов, судовий експерт

Одеський НДІ судових експертиз

ДО ПИТАННЯ ВСТАНОВЛЕННЯ ФАКТУ ЗАСТОСУВАННЯ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА У ЗДІЙСНЕННІ ГРАЛЬНОГО БІЗНЕСУ

Комп'ютерно-технічні дослідження — поширена і важлива ділянка судової експертної діяльності. Сьогодні експертна практика зіштовхується зі збільшенням кількості експертиз та експертних досліджень комп'ютерної техніки та програмних продуктів, пов'язаних з визначенням факту використання персонального комп'ютера (ПК) у здійсненні грального бізнесу. Це обумовлено збільшенням кількості кримінальних проваджень, пов'язаних з розслідуванням діяльності гральних закладів (у відповідності до Закону "Про заборону грального бізнесу в Україні").

Виконання вказаних досліджень щільно пов'язано з такими завданнями судової комп'ютерно-технічної експертизи, як встановлення технічного стану комп'ютерно-технічних засобів та виявлення інформації і програмного забезпечення, що містяться на комп'ютерних носіях. При цьому експерт має визначитися з технічними та програмними складовими наданого для досліджень комп'ютеру, які надавали б