УДК 343.148.6

А. А. Павлова
ФГБУ «Центр экспертиз координации информатизации», Москва,
e-mail: AnniaPavlova@yandex.ru

Ю. В. Молодцова
ФГБОУ ВО «Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет)», Москва, e-mail: Mol_ji@mail.ru

ПОЛУЧЕНИЕ ДОСТУПА К ДАННЫМ, СОДЕРЖАЩИМСЯ В RAID 0

Ключевые слова: RAID, последовательность накопителей информации, уровень RAID, получение доступа к данным, исследование данных в шестнадцатеричном формате, экспертиза, судебная компьютерно-техническая экспертиза, цифровая кримиминалистика.

Статья посвящена исследованию накопителей информации, объединенных RAID 0, в рамках производства судебной компьютерно-технической экспертизы. Приведено описание практического исследования возможностей получения доступа к данным, содержащимся в накопителях информации, объединённых в RAID 0, после их извлечения из системного блока. С учетом особенностей записи и хранения информации в RAID 0 разработан алгоритм обнаружения таких криминалистически значимых параметров для получения доступа к данным как последовательность накопителей информации при записи на них информации и уровень RAID. Ко всему прочему, проведено исследование возможностей получения доступа к данным при наличии части RAID 0. Результаты получены путем исследования данных (содержащихся в накопителях информации), представленных в шестнадцатеричном формате, и с помощью программных средств «UFS Explorer Professional Recovery», «R-studio», «PC-3000 Data Extractor UDMA RAID Edition».

A. A. Pavlova
Center for Expertise Coordination of Information, Moscow, e-mail: AnniaPavlova@yandex.ru

J. V. Molodsova
Bauman Moscow State Technical University, Moscow, e-mail: Mol_ji@mail.ru

OBTAINING ACCESS TO DATA CONTAINED IN RAID 0

Keywords: RAID, data storage devices sequence, RAID level, obtaining access to data, study information in hexadecimal format, expertise, forensic computer-technical expertise, criminalistics.

The article is devoted to the study of data storage devices, united by RAID, as part of forensic computer-technical expertise.

A description is given of a practical study of the possibilities of obtaining access to the data contained in data storage devices integrated into RAID 0 after they were extracted from the system unit. Taking into account the peculiarities of recording and storing information in RAID 0, an algorithm has been developed for detecting such criminologically relevant parameters for accessing data as a sequence of storage devices of recording information on it and the RAID level. In addition, a study was conducted of the possibilities of accessing data with part of RAID 0. The results were obtained by examining data (contained in data storage devices) presented in hexadecimal format and using the «UFS Explorer Professional Recovery» software, «R-studio», «PC-3000 Data Extractor UDMA RAID Edition».

Введение

В настоящее время разработаны и используются различные накопители для хранения компьютерной информации. Федеральным законом от 28 июля 2012 г. № 143–ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» был обозначен новый вид вещественных доказательств – электронные носители информации [1]. Накопители информации, объединенные в RAID (от англ. «Redundant Array of Inexpensive/Independent Disks» – «Избыточный Массив Недорогих/Независимых Дисков») [5], также относятся к таким доказательствам. Так, с целью повышения производительности совершаемых операций использование RAID 0 получило широкое применение. При выполнении операции чтения данных из массива RAID 0 поступает запрос к контроллеру массива (который «знает» как располагаются данные между накопителями ифнормации),

после чего, блоки данных считываются одновременно с двух накопителей информации, что почти вдвое увеличивает скорость чтения [3, с. 4] по сравнению с однодисковым вариантом хранения данных. На данный момент времени RAID-контроллеры, поддерживающие RAID 0, интегрированы в материнские платы системных блоков персональных компьютеров, что позволяет с легкостью объединять устройства в RAID 0 пользователю, не обладающему специальными знаниями в области компьютерных технологий. Ко всему прочему, для хранения информации на носителях серверного оборудования использование RAID является необходимым [2, с. 9]. В связи с чем, в рамках производства судебной компьютерно-технической экспертизы ставятся задачи по исследованию информации, содержащейся в RAID 0. Вышеизложенные обстоятельства определяют актуальность темы исследования, ее теоретическую и практическую значимость.

Цель исследования

Изучение практических аспектов, связанных с получением доступа к данным, содержащимся в накопителях на жёстких магнитных дисках (далее – НЖМД), объединенных в RAID 0, а именно, с учетом особенностей уровня RAID была поставлена задача разработать алгоритм обнаружения таких криминалистически значимых параметров как последовательность накопителей при записи на них информации и уровень RAID.

Материалы и методы исследования

Материалы исследования составили НЖМД, объединенные в RAID 0, а также программные средства «UFS Explorer Professional Recovery», «R-studio», «PC-3000 Data Extractor UDMA RAID Edition». Методологическую основу исследования составили источники, содержащие особенности записи и хранения информации в массивах RAID 0. В процессе исследования применялись следующие методы – анализ, синтез, дедукция, сравнение, выдвижение и проверка гипотез.

Результаты исследования и их обсуждение

Подготовительный этап исследования. В ходе производства исследования важной задачей, стоящей перед экспертом, является обеспечение сохранности криминалистически значимой компьютерной информации в неизменном виде.

В аппаратных RAID схема трансляции адресов полностью определяется контроллером, в связи с чем, попытка получения доступа к информации на другой электронно-вычислительной машине может повлечь уничтожение данных.

Следовательно, прежде чем начать исследование информационного массива данных, содержащегося в накопителях информации, объединенных в RAID, необходимо выполнение ряда действий.

Во-первых, предоставленные накопители информации должны быть сфотографированы по правилам масштабной детальной фотосъемки, а также должен быть произведен внешний осмотр объектов исследования, например, на наличие повреждений. Отметим, что целостность и работоспособность предоставленного накопителя информации может играть определяющую роль для производства дальнейшего исследования.

Во-вторых, во избежание случайной записи информации, предоставленные накопители информации должны быть подключены к аппаратному блокиратору записи, а при его отсутствии необходимо воспользоваться программным аналогом.

Следующим обязательным этапом является создание образа с накопителя информации. Данный процесс может быть реализован с помощью программы «AccessData FTK Imager». Создание образа позволит не допустить какого-либо редактирования информации непосредственно на самом носителе.

После успешного выполнения всех действий, физические устройства должны быть отключены, а дальнейшая работа производится с логическими устройствами – с образами.

Далее выполняется монтирование созданных образов. Данный процесс также может быть реализован с помощью программного средства «AccessData FTK Imager». После проведенных манипуляций, образы накопителей информации программными средствами будут восприниматься как подключенное логическое устройство.

После корректного выполнения вышеперечисленных действий, переходим

к исследованию информационной составляющей предоставленных объектов.

Получение доступа к данным, содержащимся в RAID 0. В данном разделе будет рассмотрен алгоритм определения последовательности накопителей при записи на них информации, уровня RAID и начального сектора при наличии следующих объектов исследования: два накопителя на жестких магнитных дисках (далее – НЖМД № 0.1 и НЖМД № 0.2), объединенных в RAID 0 через BIOS персонального компьютера.

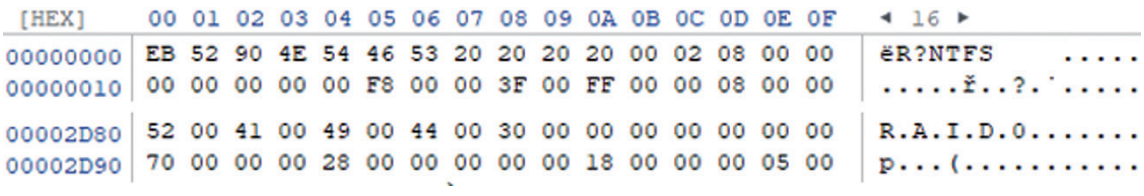
Отметим, что нередки случаи, когда автоматическое определение параметров RAID с помощью программных средств невозможно. В связи с чем, эксперту необходимо обладать навыками «ручного» определения криминалистически значимых параметров RAID. Одними из таких являются последовательность накопителей информации при записи на них информации и расположение метки «RAID».

Для этого необходимо провести анализ данных, представленных в шестнадцатеричном формате, каждого накопителя информации. Для определения последовательности накопителей информации необходимо анализировать расположение «метки» о файловой системе («метка» файловой системы «NTFS» представляет собой следующую запись в шестнадцатеричном формате – «EB52904E544653»). Как правило, в массивах RAID 0 запись о типе файловой системы в первоочередных в последовательности записи информации накопителях, расположена на нулевом смещении (или же близко к нулевому).

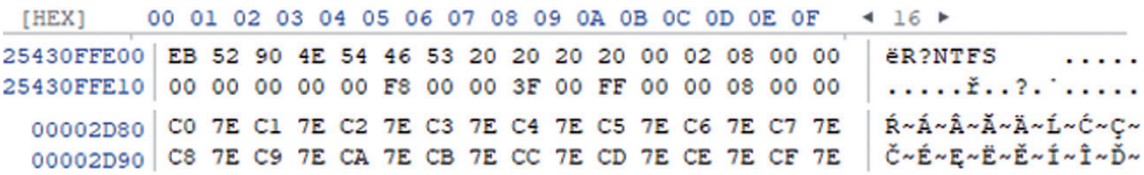
Так, на НЖМД № 0.2 «метка» о файловой системе была обнаружена на смещении «00000000», в то время как на НЖМД № 0.1 данная «метка» была найдена на смещении «25430FFE00», а на нулевом смещении была найдена запись «h.h.h.» (рис. 1). Полученные результаты дают основание полагать, что НЖМД № 0.2 является первым в последовательности записи информации.

Во-вторых, для корректного сбора массива необходимо определить месторасположение метки «RAID», свидетельствующей о том, что исследуемый накопитель информации является составной частью RAID. Анализ содержимого показал, что метка «R.A.I.D.0» содержится на НЖМД № 0.2 («метка» «RAID» представляет собой следующую запись в шестнадцатеричном формате – «52004100490044») (рисунок).

Затем необходимо определить начальный сектор, с которого начинается запись первого раздела. Как правило, данный параметр определяется автоматически для каждого накопителя информации. Однако существуют и альтернативные способы его определения, например, с помощью программного средства «NTFS Disk Explorer». Так, в ходе исследования у НЖМД 0.1. и НЖМД 0.2 был определено значение начального сектора – «2048».



а



б

Данные, представленные в шестнадцатеричном формате, обнаруженные на: а – НЖМД № 0.2; б – НЖМД № 0.1

Далее для сбора RAID при работе в программном средстве «UFS Explorer Professional Recovery» необходимо выбрать пункт меню «Построить RAID», при работе в программном средстве «R-studio» выбрать пункты меню «Создать виртуальный RAID» – «Создание виртуального блочного RAID и Автодетектирование», при использовании программного средства «PC-3000 Data Extractor UDMA RAID Edition» выбрать пункт меню «Добавить RAID» и выбрать исследуемые устройства (НЖМД № 0.2 и НЖМД № 0.1). Акцентируем внимание, что, вне зависимости от используемого программного средства при сборе RAID необходимо строгое соблюдение последовательности при выборе накопителей информации. Так как НЖМД № 0.2 является первым в последовательности записи информации, при сборе RAID он должен стоять первым в списке выбранных устройств.

В появившемся диалоговом окне указываем значения начального сектора – 2048, уровень RAID – RAID 0, и размер страйпа – 64 КБ. Результатом выполнения указанных действий, будет являться собранный массив RAID 0 с доступными для просмотра данными, записанными на НЖМД № 0.1 и НЖМД № 0.2, объединенными в RAID 0.

В рамках проведенного исследования, при использовании «ручного» способа получения доступа к данным, с помощью программных средств «UFS Explorer Professional Recovery», «PC-3000 Data Extractor UDMA RAID Edition» была восстановлена вся пользовательская информация, а именно: каталог «Документы», «Загрузки», «Книга мама», «Мпасик», «Мои Яндекс.Картинки», «Скриншоты», «Фотокамера», каталог «Лето 2016», каталог «Мама», файл «Разработка штатива.png». Средствами «R-studio» при использовании автоматического режима сбора RAID были также восстановлены вышеперечисленные файлы и каталоги, когда при использовании «ручного» способа не были восстановлены каталоги «Фотокамера», «Лето 2016», «Мама». Однако был найден каталог «Дополнительно Найденные Файлы», содержащий удаленные изображения, доступные для воспроизведения.

Акцентируем внимание, что в экспертной практике возможны ситуации, когда на исследование предоставляется лишь часть RAID. В ряде случаев, не исключена возможность восстановления данных при наличии одного из накопителей, являющего составной частью массива RAID 0.

Так, при предоставлении на исследование части массива RAID 0, для восстановления данных, накопитель информации должен являться первоочередным в последовательности записи информации в массив. Обратим внимание, что в виду отсутствия НЖМД 0.1 на этапе выбора устройств для их объединения в RAID 0 (минимальное количество выбранных устройств должно быть равным двум) в программном средстве «UFS Explorer Professional Recovery» был дважды выбран НЖМД № 0.2, для «R-studio» был создан «пустой накопитель информации», а у «PC-3000 Data Extractor UDMA RAID Edition» предусмотрена функция виртуализации «пустого накопителя», отображающегося в программном средстве как «dump drive». Подчеркнем, что в рамках исследования части RAID строгое соблюдение последовательности добавляемых устройств также является необходимым для получения доступа к данным.

В результате исследования средствами «UFS Explorer Professional Recovery» и «PC-3000 Data Extractor UDMA RAID Edition» была восстановлена структура всех файлов и каталогов: каталоги «Документы», «Загрузки», «Книга мама», «Мпасик», «Мои Яндекс.Картинки», «Скриншоты», «Фотокамера», «Лето 2016», «Мама», файл «Разработка штатива.png». Однако поскольку массив уровня RAID 0 является массивом без избыточности, а именно, файл делится на блоки, согласно установленному размеру страйпа, запись которых осуществляется параллельно на объединенные в RAID накопители, доступ к полученным данным может быть ограничен. Однако возможны случаи восстановления всего содержимого файла при наличии части массива RAID 0, например, если размер файла не превышает размер страйпа. Так, из каталога «Фотографии» был восстановлен файл «IMG_8531.jpg» размером 34 КБ.

С помощью программного средства «R-studio» при исследовании НЖМД № 0.2 были восстановлены следующие файлы и каталоги: «Документы», «Загрузки», «Книга мама», а также был найден каталог, содержащий удаленные изображения, пригодные для воспроизведения.

Отметим, что возможности программного средства «PC-3000 Data Extractor UDMA RAID Edition» позволили восстановить структуру файлов и каталогов при исследовании в отдельности как НЖМД 0.2, так и НЖМД 0.1 (являющемся вторым в последовательности записи информации в RAID 0), однако доступ к содержимому был частично ограничен, в виду отсутствия недостающего накопителя информации.

Подводя итоги исследования НЖМД № 0.1 и НЖМД № 0.2, являющихся составными частями RAID 0, отметим, путем исследования данных, представленных в шестнадцатеричном формате, представилось возможным определить такие параметры как последовательность устройств при записи на них информации и уровень RAID. Неправильное указание вышеперечисленных параметров будет являться следствием отсутствия доступа к файлам и каталогам, записанным в RAID. Основные результаты исследования НЖМД № 0.1 и НЖМД № 0.2, являющихся составными частями RAID 0, представлены в таблице.

Алгоритм определения криминалистически значимых параметров в RAID 0

Тип массива	RAID 0
Краткая характеристика	Файл делится на страйпы (блоки), которые параллельно записываются на накопители информации [4]. Минимальное количество накопителей информации – 2
Метка ФС	Содержится на первом в последовательности записи накопителе информации на нулевом смещении (или близко к нулевому). На втором в последовательности записи накопителе информации расположена не на нулевом смещении (или близко к такому). На нулевом смещении содержится запись «h.h.h.h»
Метка «R.A.I.D»	Содержится на первом в последовательности записи накопителе информации. На втором в последовательности записи накопителе информации отсутствует
Результаты восстановления данных при наличии всех составляющих RAID 0	С помощью «UFS Explorer Professional Recovery», «PC-3000 Data Extractor UDMA RAID Edition» восстановлены все пользовательские файлы и каталоги, удаленные файлы обнаружены не были. С помощью «R-studio» (при использовании «ручного способа») не было обнаружено 3 каталога, однако был восстановлен каталог, содержащий удаленные файлы
Результаты восстановления данных при наличии части RAID 0	При наличии первого в последовательности записи накопителя информации с помощью «UFS Explorer Professional Recovery» и «PC-3000 Data Extractor UDMA RAID Edition» восстановлена структура всех пользовательских файлов и каталогов и получен частичный доступ к их содержимому. С помощью «R-studio» восстановлено три каталога (из девяти), а также каталог, содержащий удаленные файлы. При наличии второго в последовательности записи накопителя информации с помощью «PC-3000 Data Extractor UDMA RAID Edition» была восстановлена структура всех файлов и каталогов (содержимое недоступно)

Заключение

В результате проведенного исследования были изучены практические аспекты, связанные с получением доступа к данным, содержащимся на накопителях на жёстких магнитных дисках, объединенных в RAID 0, а именно, с учетом особенностей уровней RAID был разработан алгоритм обнаружения таких криминалистически значимых параметров как последовательность накопителей при записи на них информации и уровень RAID.

Библиографический список

1. Федеральный закон от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 01 августа 2012. № 174.

2. Ажогин Е.Ю., Квятковская И.Ю. Корпоративная база знаний как инструмент обеспечения бесперебойной работы информационных систем // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2010. № 2. С. 7–14.

3. Алексеев Д.С., Выродов М.А. Обеспечение отказоустойчивости серверов с использованием сопряжения технологий RAID 6 и RAID 0 // Белгород: Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова. 2015. С. 2717–2721.

4. Краткий обзор технологии RAID [Электронный ресурс]. URL: http://parallel.ru/computers/reviews/raid-technology.html (дата обращения: 11.04.2019).

5. David A. Patterson, Garth Gibson, and Randy H. Katz. A Case for Redundant Arrays of Inexpensive Disks (RAID). [Электронный ресурс]. URL: https://www2.eecs.berkeley.edu/Pubs/TechRpts/1987/CSD-87-391.pdf (дата обращения: 08.04.2019).