УДК 347.948.2

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 5

Ключевые слова – RAID 5, последовательность накопителей информации, уровень RAID, получение доступа к данным, исследование данных в шестнадцатеричном формате, экспертиза, судебная компьютерно-техническая экспертиза, криминалистика, криминалистически значимые параметры.

Статья посвящена исследованию накопителей информации, объединенных в RAID 5, в рамках производства судебной компьютерно-технической экспертизы. В частности, приведено описание практического исследования возможностей получения доступа к данным, содержащимся в накопителях информации, объединённых в RAID 5, после их извлечения из системного блока, а также изучены возможности получения доступа к данным при наличии части RAID 5. С учетом особенностей записи и хранения информации в RAID 5 разработан алгоритм определения таких криминалистически значимых параметров для получения доступа к содержимому как последовательность накопителей при записи на них информации и уровень RAID путем исследования данных, представленных в шестнадцатеричном формате.

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

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

OBTAINING ACCESS TO DATA CONTAINED IN RAID 5

Keywords: RAID 5, data storage devices sequence, RAID level, obtaining access to data, study information in hexadecimal format, expertise, forensic computer-technical technical expertise, criminalistics, criminologically relevant parameters.

The article is devoted to the study of data storage devices, united by RAID 5, as part of forensic computer-technical expertise. In particular, 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 5 after they were extracted from the system unit and the possibilities of gaining access to data in the presence of a RAID 5 part are studied. Considering the features of recording and storage information in RAID 5, 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 by examining data represented in hexadecimal format.

Введение

В настоящее время разработаны и используются различные накопители для хранения компьютерной информации. Федеральным законом от 28 июля 2012 г. N 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») [6], также относятся к таким доказательствам. Существует несколько уровней RAID (3,4,5,6 и другие), в технологии хранения и записи информации которых используются блоки четности, содержащие контрольные суммы записанных блоков данных. Такие массивы носят название «отказоустойчивый массив с распределенной четностью», среди которых RAID 5 является одним из самых распространенных [4, с.426]. Данный факт обусловлен сочетанием характеристик, обеспечивающих повышенную надёжность хранения информации с сохране-

нием высокого уровня производительности выполнения операций с данными, так как блоки данных и контрольные суммы записываются циклически на все накопители массива [2, с.2718]. В связи с чем, в рамках производства судебной компьютерно-технической экспертизы ставятся задачи по исследованию информации, содержащейся в RAID 5. 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 5. С учетом особенностей уровня RAID была поставлена задача разработать алгоритм определения 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 5 и специализированные программные средства. Методологическую основу исследования составили источники, содержащие особенности записи и хранения информации в массивах RAID 5. В процессе исследования применялись следующие методы – анализ, синтез, дедукция, сравнение, выдвижение и проверка гипотез.

Результаты исследования и их обсуждение.

Подготовительный этап исследования. В ходе компьютерно-технического исследования важной задачей, ставящейся перед экспертом, является обеспечение сохранности криминалистически значимой компьютерной информации в неизменном виде. В связи с чем, прежде чем приступить к исследованию содержимого объектов, необходимо произвести ряд подготовительных действий: сфотографировать объекты исследования [5, с.44], создать их образ содержимого, выполнить «монтирование» созданных образов и т.д. [3, с.107].

Получение доступа к данным, содержащимся в RAID 5. На данном этапе исследования представлен алгоритм определения последовательности накопителей при записи на них информации и уровня RAID на примере следующих объектов исследования: три накопителя на жестких магнитных дисках (далее – НЖМД №5.1, НЖМД №5.2, НЖМД №5.3).

В ходе проведения исследования было проанализировано содержимое предоставленных НЖМД в шестнадцатеричном формате. В результате анализа было выявлено, что у НЖМД №5.1 на смещении «45430380» содержится метка «R.A.I.D.5» («52004100490044003500»), в то время как на нулевом смещении данных обнаружено не было (рис. 1).

На НЖМД №5.2 на смещении «00000000» были обнаружены данные, свидетельствующие о том, что объект является не первоочередным накопителем информации при записи данных (как правило, имеют представление в виде символов «€..€..€» либо «h.h.h»). Метка «R.A.I.D.» отсутствует (рис. 2).

[HEX]	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	◂ 16 ▸
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
45430380	08	02	52	00	41	00	49	00	44	00	35	00	5F	00	7E	00	..R.A.I.D.5._.~.

Рис.1. Данные, обнаруженные на НЖМД №5.1 (на смещениях «00000000» и «45430380»)

[HEX]	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	◂ 16 ▸
00000000	80	80	00	00	80	80	01	00	80	80	02	00	80	80	03	00	€€..€€..€€..€€..
00000010	80	80	04	00	80	80	0C	00	80	80	0D	00	80	80	18	00	€€..€€..€€..€€..
00000020	80	80	28	00	80	80	3E	00	80	80	79	00	80	80	AB	00	€€(.€€>.€€y.€€«.
00000030	80	80	38	01	80	80	6C	01	00	00	00	00	00	00	00	00	€€8.€€l.........

Рис.2. Данные, обнаруженные на НЖМД №5.2 (на смещении «00000000»)

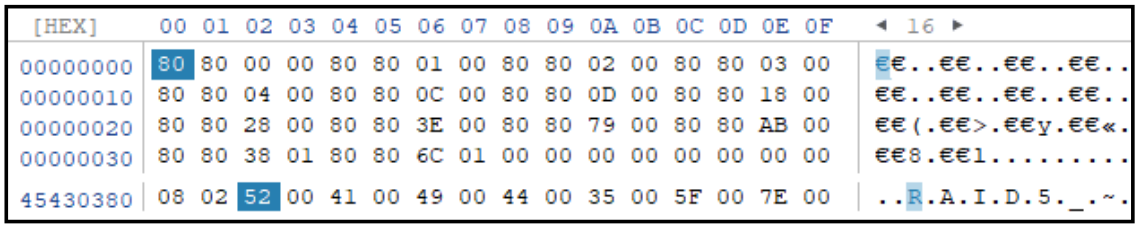

Рис.3. Данные, обнаруженные на НЖМД №5.3 (на смещениях «00000000» и «45430380»)

При исследовании НЖМД №5.3 на смещении «00000000» были также обнаружены данные, свидетельствующие о том, что накопитель информации является не первоочередным при записи данных (представлены в виде символов «€..€..€»). Метка «R.A.I.D.5» была найдена на смещении «45430380» (рис. 3).

На основе полученных данных было установлено, что НЖМД №5.1 имеет первый порядковый номер при записи информации, НЖМД №5.2 является вторым в последовательности записи информации, НЖМД №5.3 имеет третий порядковый номер.

Далее, выбрав объекты исследования с соблюдением установленного порядка и указав такие параметры как начальный сектор «135168», уровень RAID – RAID 5 и размер страйпа – 512 КБ, распределение четности – «левое, симметричное», с помощью программных средств «UFS Explorer Professional Recovery», «R-studio», «PC-3000 Data Extractor UDMA RAID Edition» был получен доступ к файловой системе (ext 4) собранного массива. Отметим, что исследуемый RAID был создан посредством использования возможностей операционной системы Linux, в связи с чем, для получения доступа к пользовательским файлам необходимо перейти по пути «home-usr-рабочий стол». Сравнительным анализом данных, записанных в RAID 5 и полученных в результате объединения НЖМД в массив, было выявлено, что был получен доступ ко всей пользовательской информации: каталоги: «Дети зоопарк», «Дипломы, сертификаты», файл «Purple документы.png», «конференция-конструктор.docx», «Конференция.pdf».

Обратим внимание, что не исключены ситуации, когда в результате утери или повреждения накопителей информации, на исследование предоставляется лишь часть RAID. Так как в технологии хранения и записи информации RAID 5 используются блоки четности, содержащие контрольные суммы записанных блоков данных [4, с.426], возможно восстановление данных при отсутствии одного из накопителей информации.

Для сбора массива RAID 5 с помощью программных средств «UFS Explorer Professional Recovery», «PC-3000 Data Extractor UDMA RAID Edition» минимальное количество накопителей информации должно ровнять трем, в связи с чем, необходима замена отсутствующего объекта. Это возможно путем добавления «пустого» накопителя информации либо путем дублирования одного из присутствующих накопителей информации. Отметим, что в результате исследования, было выявлено, что получение доступа к данным возможно при условии наличия первых двух в последовательности записи накопителей информации. Так, например, при наличии НЖМД №5.1 и №5.2 для восстановления данных в пункте меню «Построить RAID», выберем НЖМД №5.1, НЖМД №5.2 и продублируем НЖМД №5.2. Анализ восстановленных данных показал, что при отсутствии третьего в очередности записи информации накопителя, был получен доступ к содержимому всех ранее записанных файлов и каталогов.

Акцентируем внимание, что при восстановлении данных в условиях отсутствия одного из накопителей информации, соблюдение очередности при выборе накопителей оказывает существенное влияние на результативность. Так, при отсутствии НЖМД №5.3 при объединении накопителей информации в следующем порядке: НЖМД №5.1, НЖМД №5.1, НЖМД №5.2, также была восстановлена структура всех файлов и каталогов. Однако часть файлов отображалась некорректно: при восстановлении файла «Purple документы.png» было изменено содержимое, а также была нарушена четкость изображения (рис. 4).

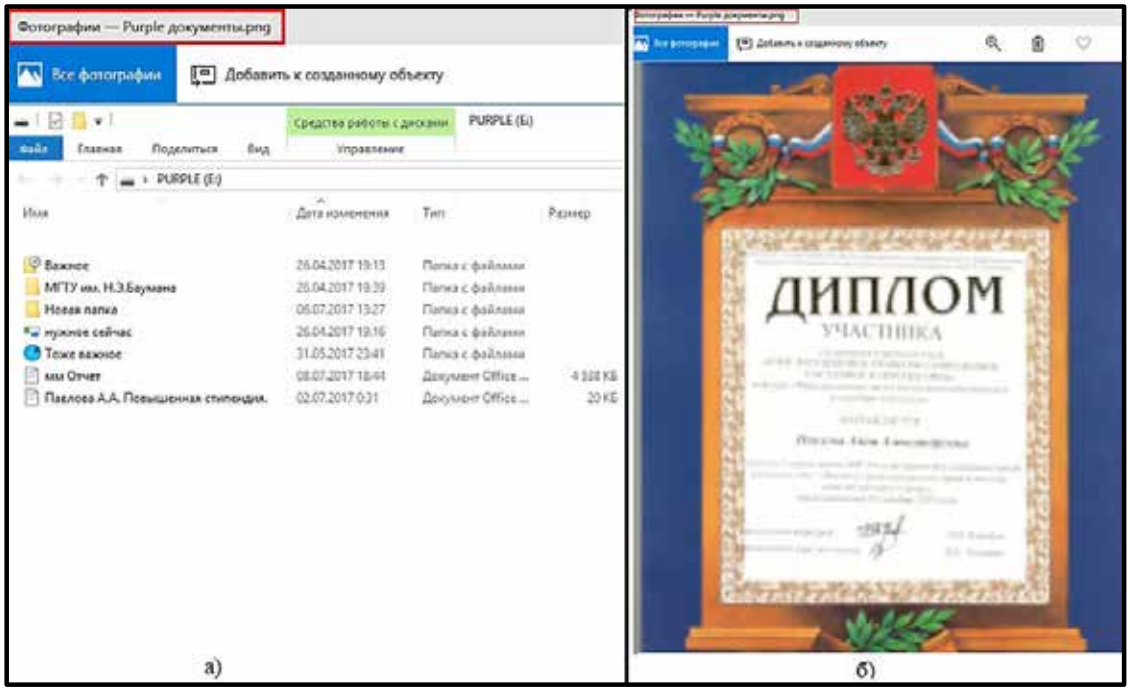

Рис.4. Файл «Purple документы.png», восстановленный в результате сбора RAID 5 из а) НЖМД №5.1, НЖМД №5.2, НЖМД №5.2; б) НЖМД №5.1, НЖМД №5.1, НЖМД №5.2

Алгоритм определения криминалистически значимых параметров в RAID 5

Тип массива	**RAID 5**
Краткая характеристика	Файл делится на блоки данных (страйпы), которые параллельно записываются на накопители информации. Для повышения надежности используется запись контрольных сумм. Минимальное количество накопителей информации – 3.
Метка «R.A.I.D»	На первом (в последовательности записи) накопителе информации (НЖМД №5.1) содержится метка «R.A.I.D». На нулевом смещении информация отсутствует. На втором накопителе информации метка «R.A.I.D» отсутствует (НЖМД №5.2). На нулевом смещении содержится информация (как правило, в виде символов «€..€..€» либо «h.h.h»). На третьем накопителе информации (НЖМД №5.3) содержится метка «R.A.I.D». На нулевом смещении содержится информация (как правило, в виде символов «€..€..€» либо «h.h.h»).
Результаты восстановления данных при наличии всех составляющих RAID	С помощью специализированных программных средств восстановлены все пользовательские файлы и каталоги.
Результаты восстановления данных при наличии части RAID	При наличии первого и второго в последовательности записи информации накопителя с помощью «UFS Explorer Professional Recovery» и «PC-3000 Data Extractor UDMA RAID Edition» восстановлены все пользовательские файлы и каталоги при условии соблюдения их последовательности. При наличии первого и второго накопителя информации при несоблюдении их последовательности была восставлена структура всех файлов и каталогов, однако содержимое файлов было видоизменено.

Обобщая итоги исследования НЖМД №5.1, НЖМД №5.2, НЖМД №5.3, являющихся составными частями RAID 5, отметим, что в связи с используемой технологией записи информации, представляется возможным получить доступ к данным, в том числе и при отсутствии одного из накопителей информации (при условии наличия

первых двух в очередности записи информации накопителей). Путем исследования данных каждого составляющего массива в шестнадцатеричном формате, представилось возможным определить последовательность устройств при записи на них информации и уровень RAID. Основные результаты исследования НЖМД №5.1, НЖМД №5.2, НЖМД №5.3, являющихся составными частями RAID 5, представлены в таблице.

Заключение

В результате проведенного исследования были изучены практические аспекты, связанные с получением доступа к данным, содержащимся на накопителях на жёстких магнитных дисках, объединенных RAID 5, а именно, с учетом особенностей уровня RAID был разработан алгоритм определения 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. 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.

3. Павлова А.А., Молодцова Ю.В. Получение доступа к данным, содержащимся в RAID 0 // Вестник Алтайской академии экономики и права. 2019. № 7-1. С. 106-111.

4. Терентьев Д.И., Николаев А.Б., Остроух А.В. Исследование дисковых массивов RAID по параметрам надежности и быстродействия // Международный журнал экспериментального образования. 2015. № 3-3. С. 423-427.

5. Усов А.И., Карпухина Е.С., Хатунцев Н.С., Эджубов Л.Г. Методы исследования в судебной компьютерно-технической экспертизе // *Т*еория и практика судебной экспертизы. 2008. №3 (11). С. 31-46.

6. Patterson D.A., Gibson G., Katz R.H. 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: 08.04.2022).