Секция «Криминалистика»

Восстановление данных с поврежденных флеш-накопителей

Научный руководитель – Крутов Сергей Александрович

Павлова Анна Александровна

Студент (специалист)

Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия

E-mail: AnniaPavlova@yandex.ru

Актуальность исследования возможностей восстановления данных с флеш-накопителей обусловлена их широким использованием в настоящее время, поскольку это наиболее удобные и практически незаменимые переносные устройства для хранения данных, которые способны сочетать в себе такие свойства, как компактность и возможность хранения большого объема информации. В связи с этим данные устройства нередко становятся объектами исследования при проведении судебной компьютерно-технической экспертизы, поскольку могут содержать криминалистически важную информацию. Экспертные исследования, проводимые судебным компьютерно-техническим экспертом, обеспечивают получение результатов, имеющих доказательственное значение при расследовании преступлений [2]. Следует отметить, что в последнее время законодатель стал уделять повышенное внимание электронным доказательствам [3], в том числе особенностям работы с ними [1]. Нередко в экспертной практике появляется необходимость восстановления информации с поврежденных флеш–накопителей. Развитие аппаратно-программных средств также имеет немаловажное значение для получения объективного, полного и достоверного результата. Так, широкое распространение при работе с указанными объектами исследования получил комплекс PC-3000 flash. Данный комплекс использует собственную технологию прямого доступа к микросхемам флэш-памяти. При этом микросхема выпаивается из накопителя и считывается на специальном считывающем устройстве — Flash reader, входящем в состав комплекса, что позволяет получить доступ к данным в случаях, когда контроллер накопителя неисправен. Эта технология дает возможность увеличить вероятность успешного восстановления данных даже в случае физического повреждения накопителей. После подготовки объекта к исследованию (извлечения микросхемы памяти и зачистки «ножек» микросхемы памяти) эксперт загружает программную часть комплекса PC-3000 flash. После того как пройдет инициализация, выпаянная микросхема памяти вставляется в программатор со строгим соблюдением методических рекомендаций [4]. В дальнейшем программа считывает микросхему, что позволит получить эксперту данные о наличии повреждений непосредственно в микросхеме памяти. После завершения указанной процедуры эксперт переходит к использованию базы данных «система решений» (далее – система), которая позволяет найти решение по восстановлению данных для конкретного типа флеш-накопителя. Для получения решения необходимо виртуализировать контроллер устройства. После чего «система» предложит решение, которое может быть загружено, и, считав его, программа приступит к восстановлению данных. Результатом исследования поврежденного флеш-накопителя производителя «Transcend» с использованием указанного метода являлось восстановленное содержимое с сохранением структуры файлов и каталогов. Однако поиск готового решения с помощью «системы» не всегда представляется возможным, что может быть обусловлено нетипичностью исследуемого устройства и иными факторами. В данном случае эксперту необходимо произвести восстановление файловой структуры флеш-накопителя с использованием метода «черновое

восстановление». Для этого с помощью программного комплекса PC-3000 flash, определяем параметр «ECC», позволяющий получить данные о возможном типе файловой структуры. После чего возможно использование одного из трех методов: объединение по байтам, побитовое инвертирование, преобразование XOR страницы. Отметим, что поскольку исследуемая микросхема памяти состоит из одного логического устройства, то использование метода объединения по байтам невозможно. В свою очередь метод побитового инвертирования результатов не дал. Так, дальнейшее исследование производилось методом преобразования XOR страницы. Далее переходим к этапу чернового восстановления данных. В результате произведенных манипуляций были получены данные о системных файлах и типе пользовательских файлов (jpg, png), хранящихся на устройстве. Однако на данном этапе просмотр их содержимого невозможен. Взяв за основу системный файл «boot», используя функцию комплекса «дизайнер страницы» был восстановлен формат файловой структуры файла (в том числе разделено пространство, предназначенное для пользовательских и служебных файлов). Полученные результаты показали, что проверочный размер остального содержимого накопителя увеличился, что является необходимым условием для дальнейшего восстановления данных. Так, применив, полученный формат файловой структуры ко всему внутреннему пространству накопителя, производим повторный анализ данных, в результате которого были восстановлены файлы и каталоги, содержащиеся на поврежденном флеш-накопителе.

Источники и литература

1 Вехов В.Б. Использование компьютерных технологий в криминалистической деятельности и в уголовном процессе. Вестник Академии Следственного комитета Российской Федерации, 2014, № 1, С. 70–73.

2 Усов А.И. Концептуальные основы судебной компьютерно–технической экспертизы. Дис. ... док. юрид. наук. Москва, 2002, 402 с.

3 Кучин О.С., ред. Электронные носители информации в криминалистике. Москва, Юрлитинформ, 2017, 304 с.

4 www.acelab.ru/dep.pc/pc3000.flash.php (PC-3000 flash)