М.Г. Карпов, Д.Ю. Семенов, И.Р. Зулькарнеев
Тюменский государственный университет, г. Тюмень
УДК 04.056:343.98

АНАЛИЗ ПРОБЛЕМ РЕАЛИЗАЦИИ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ НИЗКОБЮДЖЕТНЫХ ПЛАТ ДЛЯ ЦЕЛЕЙ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ

Аннотация. Авторами поднимается вопрос об обеспечении целостности исследуемых объектов при проведении криминалистических экспертиз. Предложены методы аппаратной реализации поставленной цели и способы снижения ее стоимости. Приведены результаты экспериментов с платой Raspeberry Pi по дублированию данных. Описаны проблемы, препятствующие реализации конечного устройства сохранения целостности или снижающие его эффективность. Предложены способы их решения.

Ключевые слова: компьютерно-техническая экспертиза, форензика, микроконтроллеры, дубликаторы, блокираторы записи, ARM-контроллеры.

Современные методики исследования данных на накопителях на жестком магнитном диске (НЖМД) используют “холодный” анализ, при котором диск не подключен к стендовому компьютеру. Такая методика обязывает эксперта использовать два различных подхода к исследованию НЖМД: дубликация данных и/или использование блокираторов записи. Каждый из таких устройств имеет как программную, так и аппаратную реализацию, обладает своими преимуществами и недостатками. Исследования авторов показали, что аппаратный подход к дублированию информации представляет собой наиболее оптимальный уровень соотношения показателей эффективности и надежности [1]. Аппаратное дублирование информации представляет собой способ сохранения целостности, при котором устройство создает полную посекторную копию исследуемого накопителя, оперируя исключительно командами прошивки этих накопителей и выполняя последующую обработку информации (вычисление контрольных сумм, анализ степени повреждения данных) (см. рисунок 1). Однако, такие устройства имеют крайне высокую стоимость, что

делает их недоступными для небольших экспертных лабораторий. Решить такую проблему могут разработки, использующие в своей аппаратной архитектуре низкобюджетные платы, которыми и занимаются авторы в рамках реализации аппаратного криминалистического дубликатора данных.

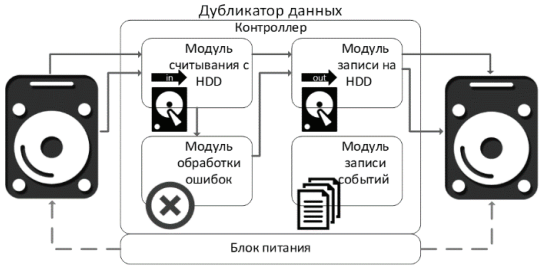

Рис. 1. Схема дубликатора данных

Авторы отмечают особую важность создания полной копии НЖМД, так как существующие системные механизмы накопителя, обеспечивающие корректную работоспособность, могут быть использованы для сокрытия информации [2, 3].

К таким механизмам относится HPA (Host Protected Area) – зарезервированная область на НЖМД, которая используется для искусственного уменьшения объема НЖМД информации. Эту область никак не определяет операционная система, следовательно, существует возможность использования такой области НЖМД для сокрытия информации.

В рамках исследования влияния HPA на целостность данных был проведен эксперимент. На исследуемом НЖМД в последнем секторе была размещена контрольная информация, далее средствами Linux (утилитой hdparm) два последних сектора были выделены под HPA. При попытке произвести полную копию данных с исследуемого НЖМД с помощью программы Acronis True Image контрольная информация обнаружена не была, что доказывает необходимость обработки сценариев работы с областью HPA при разработке дубликатора данных. Для работы с HPA существуют три

команды IDENTIFY DEVICE, SET MAX ADDRESS и READ NATIVE MAX ADDRESS. Первая команда считывает данные с регистра НЖМД, в котором хранится максимальный адрес сектора. Именно эту команду используют операционные системы для определения размера НЖМД. Информацию в регистре можно изменять при помощи команды SET MAX ADDRESS, которая устанавливает новое значение максимального адреса. Таким образом, после уменьшения значения регистра, область за новым максимальным значением будет не видна операционной системе. Для определения исходного максимального адреса, используется команда READ NATIVE MAX ADDRESS, значение которой нельзя подменить. Следовательно, при копировании данных стоит использовать команду READ NATIVE MAX ADDRESS, тем самым игнорировать зарезервированную область. После копирования данных и подключении целевого НЖМД к ЭВМ, данная область будет считаться неразмеченной [4].

Разрабатывая аппаратный дубликатор данных, авторы учли необходимость принимать во внимание особенности аппаратной платформы. С целью установить особенности поведения платы Raspberry Pi 3 при дублировании данных был проведен эксперимент, суть которого состояла в попытке создать полную копию НЖМД. При сравнении с другими платами, Raspberry Pi является хорошим выбором для проведения эксперимента, как минимум в виду наличия операционной системы. Таким образом, можно установить на Raspberry операционную систему семейства Linux, и при помощи встроенных средств производить клонирование жестких дисков. В эксперименте участвовало следующее оборудование: Raspberry Pi 3, два НЖМД объемом 90 ГБ, два адаптера USB 2.0 - SATA. Исходный НЖМД (№1) содержал контрольную информацию, предназначенную для копирования на целевой НЖМД (№2).

В ходе эксперимента был выявлен перечень проблем, препятствующих созданию полноценной копии контрольной информации:

- при использовании Raspberry Pi 3 в качестве дубликатора данных, происходит нагрев платы и, в связи с этим, быстрый выход ее из строя. Наиболее поддающимися нагреву местами являются процессор, вследствии большой нагрузки, и стабилизатор напряжения;
- использование операционной системы в качестве управляющей прослойки упрощает процесс создания дубликатора, но влияет на скорость клонирования. Также наличие возможных незадекларированных возможностей и лишнего функционала влияют на производительность и безопасность;
- использование экспериментальной аппаратной архитектуры не позволяет развить скорость более 12 Мбайт/с;
- в процессе передачи и обработки данных происходит искажение информации в случайном секторе.

На основании проведенного эксперимента сделан вывод о необходимости внедрения дополнительного охлаждения в аппаратную составляющую конфигурацию дубликатора. Вывод о невозможности использования операционной системы, сделанный авторами в предыдущем исследовании, подтвердился - наличие операционной системы не только уменьшает скорость передачи данных, но и влияет на целостность передаваемых данных [1]. С целью контроля таких искажений следует использовать механизм проверки целостности, основанный на контрольных суммах. При этом для эффективного детектирования искаженных битов оптимально вычислять контрольную сумму от каждого сектора НЖМД, а не общую ото всех секторов [5].

Стоит отметить, что исследования в сфере разработок криминалистических устройств на основе низкобюджетных плат происходят и в других исследовательских центрах мира. Так, в работе “Raspberry Pi Write Blocker for Forensics Environment” описывается результат успешной реализации аппаратного блокиратора данных на основе Raspberry Pi, что подтверждает возможность использования подобных плат в разработке оборудования для компьютерной криминалистики [6].

Все вышеизложенные проблемы необходимо учесть при реализации аппаратного дублирования данных, которое бы позволяло делать полноценную копию диска, при этом, не нарушая целостности исследуемого объекта компьютерно-технической экспертизы. Авторы описали возникнувшие проблемы и их решения, которые были протестированы в ходе разработки криминалистического аппаратного дубликатора данных [1].

СПИСОК ЛИТЕРАТУРЫ

1. И.Р. Зулькарнеев, М.Г. Карпов, В.О. Нестор, Д.Ю. Семенов Безопасность в информационной сфере. // Вестник УрФО № 1(27) / 2018, с. 42–46.

2. А. А. Шулепанов, А. Р. Смолина. Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы. // Доклады Томского государственного университета систем управления и радиоэлектроники. Том 19 № 1. С. 31-34.

3. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

4. Jim Hatfield. ATA Security feature Set Clarifications // T13 Technical Committee. URL: http://www.t13.org/documents/UploadedDocuments/docs2006/e05179r4-ACS-SecurityClarifications.pdf

5. Сергей Прокопенко. Проблемы копирования данных с накопителей с дефектными секторами при производстве компьютерно-технических экспертиз // Лаборатория компьютерной криминалистики ЕПОС. URL: http://www.epos.ua/cp/pf/publications/data/upimages/imaging-bad-sectors-computer-forensics_prokopenko.pdf (дата обращения: 15.11.2017)

6. Diogo Coito Gomes. FC6P01 Project. Final Report. Raspberry Pi Write Blocker for Forensics Environment // London Metropolitan University 2017