УДК 004.056:343.98 + 343.983.25:004.056 Вестник УрФО № 1(27) / 2018, с. 42–46

Зулькарнеев И. Р., Карпов М. Г., Нестор В. О., Семенов Д. Ю.

КОНЦЕПЦИЯ СОЗДАНИЯ КРИМИНАЛИСТИЧЕСКОГО ДУБЛИКАТОРА ДАННЫХ

В данной статье авторами поднимается вопрос о возможности и целесообразности реализации аппаратного дубликатора данных пригодного для проведения криминалистических экспертиз. Определены основные проблемы реализации аппаратного дубликатора и методы их решения. Проведен сравнительный анализ программируемых микроконтроллеров по заявленным критериям. Сделан вывод о возможности и необходимости создания подобного дубликатора.

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

Zulkarneev I. R., Karpov M. G., Nestor V. O., Semenov D. Y.

THE CONCEPT OF CRIMINALISTIC DATA DUPLICATOR DEVELOPING

The article considers the issues of possibility and feasibility of hardware data duplicator developing in computer forensics. It is defined the main problems of hardware duplicator creation and the methods of solving these problems. The comparative analysis of software microcontrollers was done by the declared criterias. It is concluded that hardware duplicator developing is possible and necessary.

Keywords: *computer forensics, microcontrollers, duplicators, write blocker*

При производстве компьютерно-технической экспертизы (КТЭ) необходимо следовать юридически закрепленным требованиям, регламентирующим данную деятельность. Одно из таких требований – обеспечение неизменности, сохранности объектов исследования [1].

В рамках КТЭ выделяют следующие группы объектов: аппаратные, программные, информационные, сетевые. Все перечисленные группы ориентированы на различные подходы к исследованию центрального объекта КТЭ – информации (данных). Принимая во внимание факт того, что информация хранится на различных типах устройств, необходимо конкретизировать область данного исследования. Самыми распространенными носителями информации, которые предоставляется эксперту, являются электронные накопители данных, в частности постоянные запоминающие устройства [2]. На текущий момент на отечественном рынке не существует надежного

способа сохранения целостности данных, использующих флеш-память. Как следствие, в данной статье под объектами исследования КТЭ будут пониматься накопители на жестких магнитных дисках (НЖМД).

Обеспечение целостности объектов исследования позволяет в рамках КТЭ реализовать:

- проведение повторной или дополнительной экспертизы, так как при нарушении целостности доказательства повторная экспертиза может дать отличное от предыдущего заключение;
- обеспечение сохранности улик, с целью исключения внесения изменений, в том числе непреднамеренных и срабатывания логических бомб на исследуемых объектах;
- обеспечение беспристрастности эксперта, ввиду невозможности его влияния на предоставленные для экспертизы материалы дела.

В случае внесения каких-либо изменений в вещественные доказательства без предварительного уведомления заказчика заключение эксперта признается недействительным, а само доказательство исключается из материалов дела. Все это позволяет говорить о необходимости обеспечения целостности объектов исследования, как об основном требовании проведения корректной и легальной компьютерно-технической экспертизы.

Обеспечить выполнение требования целостности данных возможно с использованием следующих методов, имеющих как программную, так и аппаратную реализацию: исследование устройства с применением блокиратора записи и создание копии данных исследуемого устройства [3].

Рассмотрим метод блокирования записи. Взаимодействии с НЖМД осуществляется с помощью команд группы «read», считывающих данные с диска, и команд группы «write», записывающих данные и вносящих какие-либо изменения на диск. Блокираторы записи позволяют производить исследование непосредственно на НЖМД, предотвращая реализацию команд группы «write». Это позволяет повысить скорость исследования (так как нет необходимости затрачивать время на создание дубликата НЖМД), а также производить необходимые действия без использования дополнительных накопителей (таким образом можно исследовать устройство любого объема). На рис. 1 представлена общая схема работы такого метода: блокиратор обрабатывает все операции между накопителем и ПК, кроме команд группы «write».

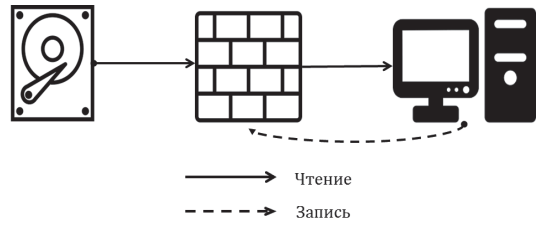

Рис. 1. Общая схема работы блокиратора записи

Программная реализация блокираторов записи может существовать как на уровне драйвера ядра операционной системы, так и в виде высокоуровневого драйвера фильтров. В первом случае, драйвер перехватывает любое обращение к устройству на низком уровне, блокируя посылаемые сигналы. Во втором случае, блокиратор также перехватывает запросы к драйверу устройства и фильтрует команды на запись, выполняя операции на высоком уровне.

Аппаратные блокираторы записи имеют две реализации: работающие в качестве транслятора и в качестве посредника команд. Блокираторы, работающие по принципу транслятора, получая команду, сверяют ее со списком разрешенных (или запрещенных) команд и далее, если было найдено совпадение, повторяют ее для целевого устройства (или отклоняют). Блокираторы, работающие в качестве посредника, представляют собой миникомпьютер со встроенной программной реализацией блокиратора, и, как следствие имеют операционную систему. Аппаратные блокираторы записи, не имеющие операционной системы, по сравнению с программными блокираторами являются более надежными, потому что спроектированы так, что в случае возникновения ошибок не смогут физически осуществить запись на НЖМД [4].

Метод дублирования данных позволяет не беспокоится о целостности исследуемого объекта во время проведения КТЭ, так как все данные предварительно копируются на сторонний накопитель, с которым и будет взаимодействовать эксперт. Дубликатор данных, создавая полную посекторную копию исследуемого накопителя, оперирует командами прошивки накопителя с последующей обработкой информации (вычисление контрольных сумм, для последующей валидации копии).

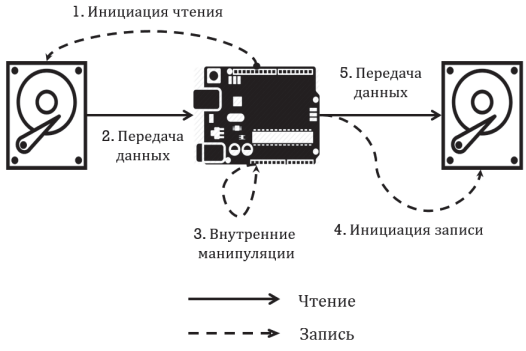

Рис. 2. Общая схема работа дубликаторов данных

Программная реализация дубликаторов функционирует на основе операционной системы, поэтому скорость копирования может быть ниже в сравнении с аппаратными реализациями, так как для взаимодействия с НЖМД программе необходимо обратиться к операционной системе, что влечет за собой лишние системные вызовы. На ОС запущено множество других процессов, которые занимают процессорное время, что также затормаживает копирование. Из недостатков данного подхода можно отметить, что подобная реализация, как правило, обладает недекларированными возможностями, следовательно есть вероятность испортить исследуемый объект при создании копии, повредив его целостность.

Аппаратные дубликаторы данных представлены в виде специального устройства, и в сравнении с их программными аналогами имеют значительно более высокие скорости копирования данных, так как взаимодействие программы с НЖМД осуществляется без операционной системы. Отсутствие ОС а также архитектура устройства (отсутствует канал «write» на аппаратном уровне) гарантирует, что дубликатор не нарушит целостности объекта исследования.

Обе реализации дубликаторов поддерживают два вида копирования данных: диск-диск и диск-образ. Первый способ производит полное посекторное копирование жесткого диска, итогом которого является новый НЖМД с аналогичными объемом и информацией. Второй способ «диск-образ» выполняет создание посекторной копии с преобразованием информации (сжатием). Итогом такого копирования является файл.

Стоит отметить, что существующие на рынке дубликаторы имеют зарубежное происхождение, а их стоимость высока для некрупных негосударственных экспертных учреждений. В связи с этим встает вопрос об исследовании возможности создания аппаратного дубликатора, который бы имел низкую себестоимость и реализовывал следующие функциональные возможности [5]:

реализация механизма создания копии НЖМД без возможности записи на оригинальный НЖМД на физическом уровне (криминалистически верная копия);

- генерация и валидация контрольных-сумм секторов НЖМД;
- журналирование событий.

Одна из проблем стоящих при создании дубликатора данных – это выбор программируемого микроконтроллера (ПМ). Для достижения целей исследования требуется оценка ПМ по следующим критериям:

- объем оперативной памяти – для обеспечения максимально возможной скорости копирования
- тактовая частота процессора;
- возможность работы без операционной системы;
- средняя стоимость.

Основным критерием является возможность работы без операционной системы для уменьшения вероятности сбоя блокировки записи при копировании НЖМД. В связи с этим в сравнении микроконтроллеров не участвовал Raspberry Pi. Для сравнения авторами были выбраны наиболее популярные и доступные ПМ: STM32F4, Teensy 3.6, Arduino Uno. Результаты отражены в таблице.

Характеристики программируемых микроконтроллеров

Характеристики	STM32F4 Discovery	Teensy 3.6	Arduino Uno
Тактовая частота процессора	168 МГц	180 МГц	16 МГц
Объем оперативной памяти	192 кБ	256 Кб	2 Кб
Возможность работы без ОС	Да	Да	Да
Средняя стоимость	1700	2 070	520

С учетом заявленных требований наиболее подходящим ПМ является Teensy 3.6.

При решении поставленной задачи может возникнуть проблема чтения поврежденных секторов. Предустановленное системное программное обеспечение на НЖМД, возвращает сообщение об ошибке в случае, если

значение бита достоверно неизвестно, следовательно, при считывании диск не сможет вернуть информацию с НЖМД. В качестве решения данной проблемы предполагается использование команды Read Long, благодаря которой верификация возвращаемой информации не осуществляется, а происходит считывание поврежденного сектора определенное количества раз и выбор наиболее часто встречающегося значения [6]. Данная команда поддерживается большинством современных НЖМД.

Разница в объемах целевого и исходного НЖМД также является проблемой, на которую следует обратить внимание. Для ее решения следует делать проверку, перед копированием данных. Если объем исходного диска больше объема целевого, то требуется выводить сообщение об ошибке, иначе необходимо установить HPA (Host Protected Area) равной разнице объемов на целевом жестком диске и начать копирование.

Помимо выше изложенных проблем необходимо принимать во внимание и другие неустранимые факторы, которые могут приводить к искажению информации в процессе ее передачи и записи. 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. Последняя проблема, которую предстоит решить – это самодостаточность и простота дубликатора. Устройство должно быть независимым от других устройств, а именно: снабжать питанием подключенные НЖМД, журналировать события и копировать данные самостоятельно. Следовательно, предположительная модель устройства должна выглядеть следующим образом: к дубликатору будут подключатся исходный и целевой НЖМД, информация с исходного будет проходить через дубликатор, где будет производится проверка на возможные ошибки считывания, на целевой НЖМД. Схема работы дубликатора представлена на рис. 3.

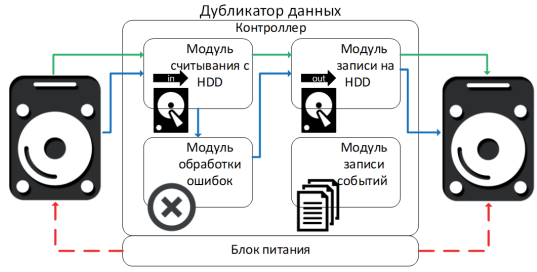

Рис. 3. Принципиальная схема дубликатора

Исходя из полученных данных можно сделать однозначный вывод о возможности и целесообразности создания аппаратного дубликатора на основе программируемого микроконтроллера с заявленным функционалом для небольших негосударственных экспертных учреждений. Коллектив авторов считает необходимым дальнейшее исследование данного вопроса и разработку прототипа дубликатора.

Литература

1. Федеральный закон от 31.05.2001 № 73-ФЗ (ред. от 08.03.2015) "О государственной судебно-экспертной деятельности в Российской Федерации». – URL: http://www.consultant.ru/document/cons_doc_LAW_31871(дата обращения: 19.12.2017)

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. Mark Menz, Steve Bress. The Fallacy of Software Write Protection in Computer Forensics // MyKey Technology Inc. URL: http://mykeytech.com/softwarewriteblocking2-4.pdf (дата обращения: 15.11.2017)

4. 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.

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. Берд Киви. Закон Мерфи для хранения данных // Цифровой журнал «Компьютерра» № 58 [28.02.2011 — 06.03.2011] URL: http://old.computerra.ru/own/kiwi/597770/

References

1. Federal'nyj zakon ot 31.05.2001 № 73-FZ (red. ot 08.03.2015) "O gosudarstvennoj sudebno-jekspertnoj dejatel'nosti v Rossijskoj Federacii" URL: http://www.consultant.ru/document/cons_doc_LAW_31871 (data obrashhenija: 19.12.2017)

2. Shulepanov, A. R. Smolina. Metodika provedenija podgotovitel'noj stadii issledovanija pri proizvodstve komp'juterno-tehnicheskoj jekspertizy. // Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki. Tom 19 № 1. S. 31–34.

3. Mark Menz, Steve Bress. The Fallacy of Software Write Protection in Computer Forensics // MyKey Technology Inc. URL: http://mykeytech.com/softwarewriteblocking2-4.pdf (data obrashhenija: 15.11.2017)

4. GOST R ISO/MJeK 27037-2014. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Rukovodstva po identifikacii, sboru, polucheniju i hraneniju svidetel'stv, predstavlennyh v cifrovoj forme.

5. Sergej Prokopenko. Problemy kopirovanija dannyh s nakopitelej s defektnymi sektorami pri proizvodstve komp'juterno-tehnicheskih jekspertiz // Laboratorija komp'juternoj kriminalistiki EPOS. URL: http://www.epos.ua/cp/pf/publications/data/upimages/imaging-bad-sectors-computer-forensics_prokopenko.pdf (data obrashhenija: 15.11.2017)

6. Berd Kivi. Zakon Mjorfi dlja hranenija dannyh // Cifrovoj zhurnal «Komp'juterra» № 58 [28.02.2011 — 06.03.2011] URL: http://old.computerra.ru/own/kiwi/597770/

ЗУЛЬКАРНЕЕВ Искандер Рашитович, старший преподаватель кафедры информационной безопасности Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: i.r.zulkarneev@utmn.ru

КАРПОВ Михаил Георгиевич, студент 4 курса направления «Информационная безопасность» Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: m.g.karpov@utmn.ru

НЕСТОР Владимир Олегович, студент 3 курса направления «Компьютерная безопасность» Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: r3seh@ya.ru

СЕМЕНОВ Дмитрий Юрьевич, студент 4 курса направления «Информационная безопасность» Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: sdu9692@gmail.com

ZULKARNEEV Iskander, Senior Lecturer, Information Security Department, Institute of Mathematics and Computer Science, Tyumen State University6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: i.r.zulkarneev@utmn.ru

KARPOV Mikhail, student of the 4th year of the course "Information Security" of the Institute of Mathematics and Computer Science of Tyumen State University. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: m.g.karpov@utmn.ru

NESTOR Vladimir, student of the 3rd year of the course "Computer Security" of the Institute of Mathematics and Computer Science of Tyumen State University. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: r3seh@ya.ru

SEMENOV Dmitry, student of the 4th year of the course "Information Security" of the Institute of Mathematics and Computer Science of Tyumen State University. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: sdu9692@gmail.com