Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Расширенное восстановление удаленной информации из файловых систем

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Яковца Александра Сергеевича

Научный руководитель

доцент, к.ю.н. _____ А.В. Гортинский

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

В современном мире ценность любой информации как никогда велика. Недоступность особо важных данных очень ощутима и чаще всего оборачивается финансовыми потерями. Современные устройства позволяют накапливать большие объемы данных и обладают высокой степенью защиты сохраненных файлов от повреждения и утери. Несмотря на это, часто возникают ситуации, когда информация удаляется случайно, либо теряется при выходе накопителей из строя. Поэтому очень важно иметь инструмент, с помощью которого можно восстановить утерянные данные. Чтобы восстановить информацию с диска, необходимо знать устройство и принципы работы файловой системы, которая установлена на исследуемый носитель информации. Зачастую понять внутреннее устройство файловой системы становится сложной задачей, так как разработчики наиболее распространенных файловых систем не публикуют подробную документацию на свои продукты. Описанию внутреннего устройства файловой системы NTFS посвящено много книг и статей, которые легли в основу данной дипломной работы. Файловая система EXFAT в силу своей относительной новизны является менее описанной, но принадлежность к семейству файловых систем FAT упрощает ее исследование.

В настоящий момент существует большое количество программ для восстановления данных из различных файловых систем. Некоторые из них направлены на восстановление информации при помощи оставшихся в файловой системе сведений о них, другие восстанавливают файлы, основываясь исключительно на поиске идентификаторов известных типов файлов (сигнатурный поиск), также существуют программные продукты, занимающиеся восстановлением поврежденной файловой системы. Современные средства восстановления комбинируют в себе все перечисленные

выше возможности, тем самым формируя универсальное инструмент для восстановления информации.

Целью дипломной работы является разработка и реализация приложения, с помощью которого можно восстановить потерянные файлы с дисков, отформатированных в файловых системах EXFAT или NTFS, а также с диска, имеющего поврежденную файловую систему. Для достижения цели работы необходимо решить следующие задачи: разбор внутреннего устройства файловых систем, разработка алгоритмов восстановления, разработка приложения.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 105 страниц, из них 46 страниц – основное содержание, включая 15 рисунков и 17 таблиц, список использованных источников из 15 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый пункт дипломной работы носит название «Внутренняя организация файловой системы EXFAT» и разделяется на семь подпунктов. Первый подпункт описывает основные особенности файловой системы. Во втором подпункте речь идет о структуре тома, отформатированного файловой системой EXFAT. Структура тома очень важна, так как именно с нее начинается исследование всей файловой системы. В остальных подпунктах первого пункта следует описание перечисленных областей тома. В третьем подпункте описана структура главного загрузочного сектора диска (MBR). При нарушении целостности данного сектора корректная работа операционной системы компьютера с таким диском будет не возможна, так как благодаря хранящейся в секторе информации компьютер определяет основные смещения в диске и основную информацию о нем. Четвертый подпункт посвящен таблице размещения файлов (FAT). В этой таблице содержится информация о расположении всех файлов в файловой системе. В подпункте также описан механизм ее заполнения. В пятом подпункте дано описание и принцип работы таблицы Bitmap. Указанная таблица необходима для ускоренного определения занятости того или иного кластера тома. В шестом подпункте рассказано о трех основных типах файловых записей, существующих в файловой системе EXFAT. С помощью этих файловых записей возможно определить является ли этот файл удаленным. Сведения, данные в этом подпункте, являются ключевыми для написания программы восстановления файлов из файловой системы EXFAT. Седьмой подпункт посвящен разработанному алгоритму восстановления файлов, который используется в реализованной программе.

Второй пункт дипломной работы описывает внутреннюю организацию файловой системы NTFS и разделен на 7 подпунктов. Первые подпункт содержит информацию об особенностях NTFS по сравнению с другими файловыми системами. Во втором подпункте речь идет о структуре тома,

отформатированного файловой системой NTFS. В остальных подпунктах второго пункта следует описание областей, необходимых для понимания принципов работы диска с файловой системой NTFS. В третьем подпункте описана структура загрузочной области ($Boot) диска. Первый сектор указанной области имеет схожую структуру с загрузочным сектором EXFAT тома. Он также содержит всю необходимую для работы операционной системы с диском информацию. Поэтому, как и в случае с MBR EXFAT тома, его повреждение приведет к неспособности компьютера корректно работать с диском. В четвертом подпункте рассказывается о структуре главной файловой таблицы (метафайл $MFT). Этот файл является одним из главных системных файлов файловой системы NTFS. Метафайл $MFT содержит в себе информацию о всех файлах, присутствующих на диске. В силу своей важности для корректной работы файловой системы этот метафайл имеет копию ($MFTMirr), которая содержит 4 первых записи из $MFT. В пятом подпункте подробно рассматривается структура записей, содержащихся в системном файле $MFT. В отличии от FAT $MFT содержит не только информацию о расположении. В $MFT хранится вся основная информация о файле: порядковый номер в файловой системе, его имя, размер, временные метки и атрибуты. В шестом подпункте внимание уделяется атрибутам файловых записей. Подробно рассмотрена структура заголовков атрибутов. В файловой системе NTFS существует большое количество атрибутов файловой записи. Атрибуты необходимы для более подробного описания файлов. Седьмой подпункт посвящен разбору некоторых основных атрибутов файлов. Подпункт разбит на 6 частей, в каждой части подробно описан один из атрибутов файловой системы. С помощью сведений, полученных из описанных подпунктов второго пункта, был разработан алгоритм восстановления данных из файловой системы NTFS. Разработанный алгоритм используется в реализованной программе, и его описание находится в восьмом подпункте.

Третий пункт дипломной работы называется «Восстановление файлов по сигнатурам» и содержит 2 подпункта. В пункте рассказывается о способе поиска файлов по набору байтов (т.е. сигнатура), нахождение которых обеспечивает идентификацию формат файла. В первом подпункте раздела приведен алгоритм сигнатурного поиска файлов известного типа. Описанный алгоритм был реализован в программе восстановления файлов. Во втором подпункте описаны преимущества и недостатки сигнатурного поиска.

Полный обзор разработанного программного продукта приведен в четвертом пункте дипломной работы. В рамках данного пункта приводится поэтапное описание работы с графическим интерфейсом программного продукта.

ЗАКЛЮЧЕНИЕ

Основным изменением в файловой системе EXFAT по сравнению с FAT является введение таблицы Bitmap, при помощи которой можно более эффективно отслеживать изменения, связанные с удалением, перемещением или переименованием файлов. В связи с этим нововведением способы восстановления файлов из EXFAT изменились по сравнению со способами, применяемыми к файловой системе FAT. Теперь для определения занятости кластера необходимо проверять содержимое соответствующего бита в таблице Bitmap. В остальном процедуры восстановления и поиска данных похожи.

В ходе дипломной работе были изучены файловые системы EXFAT и NTFS, а также разработаны алгоритмы, необходимые для реализации расширенного восстановления файлов.

В результате проделанной работы была разработана программа, осуществляющая анализ дисков и восстановление утерянных файлов.

Результат работы реализованного приложения сравнивался с результатами различных аналогов: R-studio и R.Saver. Эти программы были выбраны из-за наибольшей популярности, они обладают обширными возможностями в области восстановления файлов. Также они могут работать с различными файловыми системами и проводить восстановление файлов по известным сигнатурам. Сравнивая результаты работы программ, было замечено, что при восстановлении файлов по известным сигнатурам, расположенных на томе с файловой системой RAW, программа R-studio выдаёт неверный результат. Разработанная программа и R.Saver на том же томе дают корректный результат.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Википедия [Электронный ресурс] // exFAT [Электронный ресурс] : [сайт]. URL: https://ru.wikipedia.org/wiki/ExFAT (дата обращения: 01.12.2017). Загл. с экрана. Яз. рус.

2 SANS [Электронный ресурс] // Forensics [Электронный ресурс] : [сайт]. URL: https://www.sans.org/reading-room/whitepapers/forensics/reverse-engineering-microsoft-exfat-file-system-33274 (дата обращения: 09.09.2017). Загл. с экрана. Яз. англ.

3 Восстановление данных R.LAB [Электронный ресурс] // R.saver Бесплатная программа для восстановления данных [Электронный ресурс] : [сайт]. URL: http://rlab.ru/tools/rsaver.html (дата обращения: 10.11.2017). Загл. с экрана. Яз. рус.

4 R-Tools Technology Inc. [Электронный ресурс] // Утилита Восстановления Данных с Диска [Электронный ресурс] : [сайт]. URL: http://www.r-studio.com/ru/ (дата обращения: 10.11.2017). Загл. с экрана. Яз. рус.

5 Microsoft [Электронный ресурс] // CreateFile function [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/en-us/library/windows/desktop/aa363858(v=vs.85).aspx (дата обращения: 15.10.2017). Загл. с экрана. Яз. англ.

6 NTFS.com ExFAT overview [Электронный ресурс] // ExFAT overview [Электронный ресурс] : [сайт]. URL: http://www.ntfs.com/exfat-overview.htm (дата обращения: 10.11.2017). Загл. с экрана. Яз. англ.

7 data64 Cloud Campus [Электронный ресурс] // File System Forensic Analysis By Brian Carrier [Электронный ресурс] : [сайт]. URL: http://www.campus64.com/digital_learning/data/cyber_forensics_essentials/info_file_system_forensic_analysis.pdf (дата обращения: 01.12.2017). Загл. с экрана. Яз. англ.

8 Qt [Электронный ресурс] // Qt Documentation [Электронный ресурс] : [сайт]. URL: http://doc.qt.io/qt-5/ (дата обращения 23.10.2017). Загл. с экрана. Яз. англ.

9 Электронная библиотека RoyalLib.com [Электронный ресурс] // Касперски Крис. Восстановление данных. Практическое руководство [Электронный ресурс] : [сайт]. URL: https://royallib.com/read/kasperski_kris/vosstanovlenie_dannih_prakticheskoe_rukovodstvo.html#0 (дата обращения 09.11.2017). Загл. с экрана. Яз. рус.

10 Компьютерные книги [Электронный ресурс] // Брайан Кэрриэ Криминалистический анализ файловых систем [Электронный ресурс] : [сайт]. URL: http://computersbooks.net/index.php?id1=4&category=rukovodstvo-po-po&author=kerrie-b&book=2007 (дата обращения 27.10.2017). Загл. с экрана. Яз. рус.

11 NTFS Documentation [Электронный ресурс] // Index Record [Электронный ресурс] : [сайт]. URL: http://inform.pucp.edu.pe/~inf232/Ntfs/ntfs_doc_v0.5/concepts/index_record.html (дата обращения 03.01.2018). Загл. с экрана. Яз. англ.

12 Google Книги [Электронный ресурс] // Внутреннее устройство Microsoft Windows. 6-е изд. Основные подсистемы ОС Авторы: Руссинович М., Соломон Д., Ионеску Алекс [Электронный ресурс] : [сайт]. URL: https://books.google.de/books?id=hxzECwAAQBAJ&pg=PA507&lpg=PA507&dqt (дата обращения 03.01.2018). Загл. с экрана. Яз. нес.

13 FireEye [Электронный ресурс] // Incident Response with NTFS INDX Buffers – Part 1: Extracting an INDX Attribute [Электронный ресурс] : [сайт]. URL: https://www.fireeye.com/blog/threat-research/2012/09/striking-gold-incident-response-ntfs-indx-buffers-part-1.html (дата обращения 27.12.2017). Загл. с экрана. Яз. англ.

14 Microsoft TechNet [Электронный ресурс] // How NTFS Works [Электронный ресурс] : [сайт]. URL: https://technet.microsoft.com/en-

us/library/cc781134(v=ws.10).aspx (дата обращения 07.01.2018). Загл. с экрана. Яз. англ.

15 E-reading [Электронный ресурс] // Восстановление данных на 100% [Электронный ресурс] : [сайт]. URL: https://www.e-reading.club/book.php?book=1025070 (дата обращения 14.11.2017). Загл. с экрана. Яз. рус.