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

Восстановление информации из сильно поврежденной NTFS

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Фаюстова Дениса Сергеевича

Научный руководитель

старший преподаватель _____ И. Ю. Юрин

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В. Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

Восстановление данных всегда является актуальной задачей и существует множество различных инструментов для её решения. Однако в большинстве случаев рассматриваются относительно оптимистичные варианты состояния исследуемой файловой системы (далее – ФС). В реальности же можно встретить случаи, когда существующие инструменты просто неспособны извлекать значимую для исследователя информацию, если повреждения слишком существенны.

Результат разбора одного из таких случаев лег в основу данной работы. Отсутствие необходимых инструментов привело к необходимости подробного изучения проблемы и разработке собственных методов восстановления.

Независимо от того насколько значительно повреждена ФС, всегда можно применять обычный сигнатурный поиск (ищем заголовки известных файловых форматов и пытаемся восстанавливать). Этот метод прост (если не вдаваться в особенности файловых форматов) и крайне эффективен. Однако, он не способен восстанавливать фрагментированные данные, а также воссоздавать связи между объектами ФС и извлекать метаданные (это, например, время редактирования, история имен файла) [1].

Если отстраниться от форматов файлов, которые хранятся на компьютере, и ограничиться лишь поиском низкоуровневых структур ФС, то вполне возможно, что собранная информация, объединённая в единое целое, поможет восстанавливать данные, которые ранее извлечь было нельзя.

В таком случае необходим глубокий анализ внутренних структур, а это значит, что придётся ограничиться лишь одной конкретной ФС. В качестве объекта исследования была выбрана NTFS, как одна из самых популярных, а значит и востребованных в сфере восстановления информации.

Данная работа посвящена теме восстановления информации из NTFS в случае её сильного повреждения. Определим, что мы будем понимать под сильными повреждениями:

- невозможность обычной адресации внутри тома (определяющий фактор);
- недоступность части критических структур ФС;
- присутствие структур ФС, относящихся к другому тому.

В работе рассматриваются только тома NTFS созданные операционными системами семейства «Windows» начиная с «Windows XP» (NTFS версии 3.1). Такой выбор сделан из-за наличия некоторых отличий в дисковых структурах старых версий NTFS, в частности отсутствия полезного поля «MFT Record Number» в файловых записях. Кроме того, не рассматриваются случаи со сжатием данных или шифрованной файловой системой («EFS» – «Encrypted File System»).

Цели работы:

1. Рассмотреть основные структуры NTFS и методы их нахождения.
2. Разработать метод восстановления адресации на сильно поврежденном томе NTFS.
3. Предложить способы группировки найденных структур (каждая группа должна содержать только те, что принадлежат одному тому).
4. Разработать программу, которая реализует описанные методы и предоставляет пользователю интерфейс для просмотра и сохранения восстановленных данных.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе «Основная информация» в первую очередь приводятся необходимые определения согласно источникам [2-4]. Затем описывается ситуация, которая приводит к необходимости разработки новых методов восстановления информации из NTFS (на основе выводов из [5]). Кратко описываются базовые принципы работы ФС согласно [1,18] и попутно называются классические стратегии восстановления удаленных файлов, основываясь на [6]. Помимо перечисленного выше, обосновывается актуальность поставленной задачи и приводятся возможные сценарии использования результатов работы.

Во 2 разделе работы «Методы восстановления» приводится необходимая информация для реализации разработанных в рамках данной работы алгоритмов восстановления информации. В частности, на основании информации из источников [7-12] и [19-20] даются практические рекомендации по поиску и анализу низкоуровневых структур NTFS, описывается разработанный в процессе данной дипломной работы метод восстановления адресации внутри тома NTFS, а также предлагаются его усовершенствования согласно [13-15]. Предложенный метод восстановления адресации в значительной степени полагается на отсутствие структур с других томов NTFS (такое возможно, если в восстанавливаемым образе более двух разделов с этой ФС), поэтому дополнительно предлагаются алгоритмы группировки найденных низкоуровневых структур. В разделе также приводятся доводы в пользу извлечения и использования записей журнала «$UsnJrnl».

В 3 разделе работы «Программная реализация» описывается программа, которая была создана по результатам проведенного исследования. Разработка основана на библиотеке, которая была написана ранее в процессе преддипломной практики и после в значительной мере доработана для решения

новой задачи. Её применение позволило значительно упростить реализация предложенных в работе алгоритмов. В разделе описывается интерфейс и основные возможности.

В 4 разделе работы «Существующие аналоги» приводятся несколько программ, которые способны извлекать информацию в случае сильного повреждения NTFS. Одним из наиболее качественных продуктов является [16]. Именно возможности данной программы послужили вдохновением для глубокого изучения проблемы и поиска своих методов восстановления. Чуть менее удобными, но при этом не менее полезными, являются консольные утилиты из [17]. Их большим преимуществом является открытость исходных кодов и бесплатность, поэтому они без проблем могут быть использованы любым исследователем.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 124 страниц, из них 33 страницы – основное содержание, включая 27 рисунков и 4 таблицы, список использованных источников из 20 наименований.

ЗАКЛЮЧЕНИЕ

В результате данной дипломной работы были разработаны методы восстановления информации из сильно поврежденной ФС NTFS, которые включают себя:

- поиск значимых структур NTFS;
- объединение полученных структур по группам;
- восстановление первоначальной адресации внутри тома.

Была доработана библиотека для работы со структурами NTFS, а также разработана программа демонстрирующая результат работы алгоритмов.

В процессе выполнения данной дипломной работой были определены возможные направления для дальнейшего улучшения алгоритмов восстановления.

Разбор страниц журнала «$LogFile» позволит извлекать дополнительные файловые и индексные записи (на данный момент все они отбрасываются как некорректные из-за отсутствующей защиты «USN» массивом), которые образуют одну группу еще при базовом распределении.

Большой интерес представляет и восстановление дескрипторов безопасности (служебный файл «$Secure»). Метод нахождения этих записей был предложен в рамках преддипломной практики, однако на данный момент не было найдено критериев объединения этих данных с остальными группами.

Особо стоит выделить также и нахождение файлов специфичных для операционной системы «Windows». Это в первую очередь файлы реестра (их внутренняя структура позволяет «склеивать» фрагментированные части, ориентируясь на перекрестные ссылки между фрагментами). Другой интересный формат это «Windows Events» («*.evtx»), его страничная структура позволяет легко находить все фрагментированные части.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Кэрри, Б. Криминалистический анализ файловых систем. [Электронный ресурс] / Б. Кэрри // Компьютерные книги [Электронный ресурс] : [сайт]. URL: http://computersbooks.net/index.php?id1=4&category=rukovodstvo-po-po&author=kerrie-b&book=200 (дата обращения: 23.12.2017). Загл. с экрана. Яз. рус.

2 Лекция 11: Файловая система NTFS // Национальный Открытый Университет "ИНТУИТ" [Электронный ресурс] : [сайт]. URL: https://www.intuit.ru/studies/courses/10471/1078/lecture/16586 (дата обращения: 11.12.2017). Загл. с экрана. Яз. рус.

3 NTFS // COEN 252 Computer Forensics [Электронный ресурс] : [сайт]. URL: http://www.cse.scu.edu/~tschwarz/coen252_07Fall/Lectures/NTFS.html (дата обращения: 11.12.2017). Загл. с экрана. Яз. англ.

4 Sammes, A. Forensic Computing [Электронный ресурс] / A. Sammes, B Jenkinson // Google Книги [Электронный ресурс] : [сайт]. URL: https://books.google.ru/books?id=Ee9PF6Zv_tMC (дата обращения: 22.11.2017). Загл. с экрана. Яз. англ.

5 Extracting data from damaged NTFS drives | by Andrea Lazzarotto // eForensic [Электронный ресурс] : [сайт]. URL: https://eforensicsmag.com/extracting-data-damaged-ntfs-drives-andrea-lazzarotto/ (дата обращения: 11.12.2017). Загл. с экрана. Яз. англ.

6 Гультяев, К. Восстановление данных [Электронный ресурс] / К. Гультяев // ЛитРес – самая большая библиотека электронных книг [Электронный ресурс] : [сайт]. URL: https://www.litres.ru/static/trials/00/17/63/00176374.a4.pdf (дата обращения: 05.01.2018). Загл. с экрана. Яз. рус.

7 NTFS Reference Sheet [Электронный ресурс] // writeblocked [Электронный ресурс] : [сайт]. URL: http://www.writeblocked.org/resources/ntfs_cheat_sheets.pdf (дата обращения: 11.12.2017). Загл. с экрана. Яз. англ.

8 NTFS Documentation [Электронный ресурс] // Develop and Download Open Source Software [Электронный ресурс] : [сайт]. URL: https://osdn.net/projects/sfnet_ntfsofuefi/downloads/NTFS%20Reference%20Documents/ntfsdoc.pdf/ (дата обращения: 20.11.2017). Загл. с экрана. Яз. англ.

9 Руссинович, М. Внутреннее устройство Microsoft Windows [Электронный ресурс] / М. Руссинович, Д. Соломон // Большая онлайн библиотека e-Reading [Электронный ресурс] : [сайт]. URL: https://www.e-reading.club/book.php?book=89563 (дата обращения: 05.01.2018). Загл. с экрана. Яз. рус.

10 Записки исследователя NTFS [Электронный ресурс] // CIT Forum [Электронный ресурс] : [сайт]. URL: http://citforum.ru/operating_systems/windows/ntfs/ (дата обращения: 05.12.2017). Загл. с экрана. Яз. рус.

11 NTFS Log Tracker [Электронный ресурс] // FORENSIC INSIGHT [Электронный ресурс] : [сайт]. URL: http://forensicinsight.org/wp-content/uploads/2013/06/F-INSIGHT-NTFS-Log-TrackerEnglish.pdf (дата обращения: 30.11.2017). Загл. с экрана. Яз. англ.

12 USN_RECORD_V2 structure [Электронный ресурс] // MSDN – сеть разработчиков Microsoft [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/en-us/library/aa365722.aspx (дата обращения: 17.12.2017). Загл. с экрана. Яз. англ.

13 Incident Response with NTFS INDX Buffers – Part 1: Extracting an INDX Attribute [Электронный ресурс] // FireEye Inc [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: 30.11.2017). Загл. с экрана. Яз. англ.

14 Carvey, H. Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8 // H. Carvey // Google Книги [Электронный ресурс] : [сайт]. URL: https://books.google.ru/books?id=oiqSAgAAQBAJ (дата обращения: 27.12.2017). Загл. с экрана. Яз. англ.

15 File - $MFTMirr [Электронный ресурс] // NTFS Documentation [Электронный ресурс] : [сайт]. URL: https://flatcap.org/linux-ntfs/ntfs/files/mftmirr.html (дата обращения: 11.12.2017). Загл. с экрана. Яз. англ.

16 Active@ File Recovery [Электронный ресурс] // Active@ File Recovery for Windows provides the ability to effectively detect and recover files. [Электронный ресурс] : [сайт]. URL: http://www.file-recovery.com/ (дата обращения: 27.12.2017). Загл. с экрана. Яз. англ.

17 jschicht (Joakim Schicht) / Repositories · GitHub [Электронный ресурс] // The world's leading software development platform - GitHub [Электронный ресурс] : [сайт]. URL: https://github.com/jschicht?tab=repositories (дата обращения: 05.01.2018). Загл. с экрана. Яз. англ.

18 Ташков, П. Восстановление данных на 100% [Электронный ресурс] / П. Ташков // Большая онлайн библиотека e-Reading [Электронный ресурс] : [сайт]. URL: https://www.e-reading.club/bookreader.php/1025070/Tashkov_-_Vosstanovlenie_dannyh_na_100%25.html (дата обращения: 05.01.2018). Загл. с экрана. Яз. рус.

19 NTFS INDX Parsing // Willi Ballenthin [Электронный ресурс] : [сайт]. URL: http://www.williballenthin.com/forensics/indx/ (дата обращения: 11.12.2017). Загл. с экрана. Яз. англ.

20 NTFS $I30 Index Attributes: Evidence of Deleted and Overwritten Files // Forensic Methods [Электронный ресурс] : [сайт]. URL: http://forensicmethods.com/ntfs-index-attribute (дата обращения: 11.12.2017). Загл. с экрана. Яз. англ.