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 файлов из журнала транзакций $LogFile

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Полтавец Дмитрия Александровича

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

NTFS – стандартная файловая система семейства операционных систем Windows NT фирмы Microsoft.

NTFS является отказоустойчивой системой, которая способна привести себя в корректное состояние при практически любых сбоях.

Одним из средств, которые помогают данной файловой системе сократить число ошибок является журналирование. Журналирование предполагает ведение журнала, который хранит список изменений и помогает сохранить целостность файловой системы.

Любая современная файловая система основана на понятии транзакция. Транзакция – это группа последовательных операций, которая представляет собой логическую единицу работы с данными. Для реализации транзакций в главной файловой таблице NTFS присутствует специальный файл с именем $LogFile – журнал транзакций. Файловая система хранит в этом файле список изменений, которые она будет проводить, перед фактической записью данных.

Кроме данных о самих транзакциях, $LogFile хранит фрагменты файлов, с которыми производились какие-либо действия. Фрагменты файлов могут быть полезны не только обычному пользователю в случае сбоев и ошибок системы, но и специалистам в области компьютерной экспертизы, так как они могут содержать информацию важную с криминалистической точки зрения.

В связи с этим целью данной работы является получение данных о действиях с файлами, записи о которых хранятся в журнале транзакций $LogFile файловой системы NTFS, и, по возможности, получение частей файлов, хранящихся также в журнале транзакций $LogFile.

В процессе работы необходимо выполнить следующие задачи:

1) изучить структуру файловой системы NTFS;
2) изучить структуру главной таблицы файлов $Mft;
3) изучить структуру журнала транзакций $LogFile;

4) изучить структуру журнала изменений $UsnJrnl;

5) проанализировать события, хранящиеся в журнале транзакций $LogFile;

6) разработать и реализовать программу для получения данных об операциях над файлами в файловой системе NTFS, а также восстанавливающая содержимое файлов, хранящихся в журнале транзакций $LogFile.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 111 страниц, из них 39 страниц – основное содержание, включая 36 рисунков и 2 таблицы, список использованных источников из 14 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе «Файловая система NTFS» приведены основные определения и основные сведения о файловой системе NTFS, в том числе описана главная таблица файлов $Mft согласно [1] и журнал изменений $UsnJrnl основываясь на [2] и [3].

В разделе «Журнал транзакций» рассказывается о сервисе журналирования, в частности о том, как протоколируются действия в системе и о прядке восстановления в случае сбоя в соответствии с [4]. Затем описывается журнал транзакций $LogFile и его структура согласно [5] и [6].

В 3 разделе «Программа получения данных файлов из файла $LogFile» описывается интерфейс и особенности работы разработанной программы, написанной на языке C++ с использованием библиотек WinApi. Так же в этом разделе приведен анализ записей содержащихся в журнале транзакций $LogFile. Последним пунктом раздела является описание примера работы программы, в котором показаны события, получаемые программой из анализируемых файлов, при создании, удалении и переименовании тестовых файлов.

ЗАКЛЮЧЕНИЕ

В Windows используется файловая система NTFS, в которой присутствуют встроенные средства восстановления данных. В связи с этим ситуации, когда пользователь должен запускать на томе NTFS программу восстановления диска, достаточно редки. Даже в случае краха системы NTFS имеет возможность автоматически восстановить непротиворечивость файловой системы, используя журнал транзакций и информацию контрольных точек.

В то же время NTFS – это сложная реляционная база данных, которая поддерживает возможности протоколирования и восстановления данных, а также множественные потоки данных и индексирование атрибутов файлов.

В ходе работы были изучена файловая система NTFS, а также метафайлы этой файловой системы, такие как таблица файлов $Mft, журнал изменений $UsnJrnl и журнал транзакций $LogFile. Были проанализированы события, хранящиеся в записях журнала транзакций $LogFile.

В результате проделанной работы была разработана и реализована программа, получающая данные об операциях над файлами в файловой системе NTFS, а также восстанавливающая содержимое файлов, хранящихся в журнале транзакций $LogFile.

По окончанию работы, задачи были решены и цель курсовой работы была достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Котельников, Е. В. Лекция 11: Файловая система NTFS [Электронный ресурс] / Е. В. Котельников // ИНТУИТ.РУ : Национальный Открытый Университет. URL: http://www.intuit.ru/studies/courses/10471/1078/lecture/16586?page=1 (дата обращения: 29.11.2017). Загл. с экрана. Яз. рус.

2 Вернигора, А. Эволюция журналов в Windows [Электронный ресурс] // Издательство «Открытые системы» [Электронный ресурс] : [сайт]. URL: https://www.osp.ru/winitpro/2008/05/5529377/ (дата обращения: 5.12.2017). Загл. с экрана. Яз. рус.

3 6.5.13 Журнал изменений, журнал USN и файл журнала изменений [Электронный ресурс] // Delphiplus – ежедневные новости IT-технологий [Электронный ресурс] : [сайт]. URL: http://www.delphiplus.org/sistemy-khraneniya-dannykh-v-windows/6513-zhurnal-izmenenii-zhurnal-usn-i-fail-zhurnala-izmenenii.html (дата обращения: 5.12.2017). Загл. с экрана. Яз. рус.

4 Руссинович, М. Сервис файла журнала [Электронный ресурс] / М. Руссинович, Д. Соломон // e-reading.club [Электронный ресурс]: [сайт]. URL: http://www.e-reading.club/chapter.php/89562/68/Russinovich,_Solomon_-_4.Vnutrennee_ustroiistvo_Windows_(gl._12-14).html (дата обращения: 9.11.2017). Загл. с экрана. Яз. рус.

5 NTFS Log Tracker [Электронный ресурс] // forensicinsight.org [Электронный ресурс] : [сайт]. URL: http://forensicinsight.org/wp-content/uploads/2013/06/F-INSIGHT-NTFS-Log-TrackerEnglish.pdf?ckattempt=1 (дата обращения: 11.11.2017). Загл. с экрана. Яз. англ.

6 NTFS Transaction Journal [Электронный ресурс] // NTFS — New Technology File System [Электронный ресурс] : [сайт]. URL: http://ntfs.com/transaction.htm (дата обращения: 15.11.2017). Загл. с экрана. Яз. англ.

7 Баранов, А. Записки исследователя NTFS [Электронный ресурс] // citforum.ru [Электронный ресурс]: [сайт]. URL: http://citforum.ru/operating_systems/windows/ntfs/ (дата обращения: 29.11.2017). Загл. с экрана. Яз. рус.

8 Файл $LogFile [Электронный ресурс] // Delphiplus – ежедневные новости IT-технологий [Электронный ресурс] : [сайт]. URL: http://www.delphiplus.org/kriminalisticheskii-analiz-failovykh-sistem/fail-logfile.html (дата обращения: 14.11.2017). Загл. с экрана. Яз. рус.

9 Выделение записей Mft и атрибутов [Электронный ресурс] // Delphiplus – ежедневные новости IT-технологий [Электронный ресурс] : [сайт]. URL: http://www.delphiplus.org/kriminalisticheskii-analiz-failovykh-sistem/vydelenie-zapisei-mft-i-atributov.html (дата обращения: 27.11.2017). Загл. с экрана. Яз. рус.

10 Сенкевич, Г. Е. Искусство восстновления данных / Г. Е. Сенкевич; ред. Е. Кондукова. СПб. : БХВ-Петербург, 2011. 304 с.

11 Ramanan, T. Undelete a file in NTFS [Электронный ресурс] // CODE PROJECT [Электронный ресурс]: [сайт]. URL: https://www.codeproject.com/Articles/9293/Undelete-a-file-in-NTFS (дата обращения: 23.11.2017). Загл. с экрана. Яз. англ.

12 TOMOYO Linux Cross Reference Linux/fs/ntfs/ [Электронный ресурс] // Tomoyo Linux [Электронный ресурс]: [сайт]. URL: http://tomoyo.osdn.jp/cgi-bin/lxr/source/fs/ntfs/ (дата обращения: 10.11.2017). Загл. с экрана. Яз. англ.

13 Convert utf-8 to ANSI (Windows-1252) and back in Visual C++ 6.0 (and 7.0, 8.0) [Электронный ресурс] // Chilkat Software [Электронный ресурс]: [сайт]. URL: https://www.chilkatsoft.com/p/p_348.asp (дата обращения: 21.11.2017). Загл. с экрана. Яз. англ.

14 Uijtewaal, F. UsnJrnl Parsing for File System History Project Report [Электронный ресурс] / F. Uijtewaal, J. Prooijen // SNE Master Research Projects 2017 - 2018 [Электронный ресурс]: [сайт]. URL: http://rp.delaat.net/2015-2016/p18/report.pdf (дата обращения: 30.11.2017). Загл. с экрана. Яз. англ.