МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Получение значимых данных об операциях и файлах из $LogFile

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Климовой Елены Вячеславовны

Научный руководитель
к.ю.н., доцент _____ 23.01.2021 г. А. В. Гортинский

Заведующий кафедрой
д. ф.-м. н., доцент _____ 23.01.2021 г. М. Б. Абросимов

Саратов 2021

ВВЕДЕНИЕ

Всем компьютерам были необходимы средства долгосрочного хранения данных и обеспечения доступа к ним, именно по этой причине появились файловые системы — наборы соглашений, определяющих организацию данных на носителях информации. С их помощью операционная система, другие программы и пользователи могут работать с файлами и каталогами.

В данной работе будет рассмотрена современная файловая система NTFS, которая гарантирует корректное состояние системы даже после ошибок или сбоев. Для этого разработчики дополнили ее файлом $LogFile, который ведет записи обо всех совершаемых транзакциях и позволяет системе при необходимости сделать откат этих транзакций.

Цель дипломной работы — исследование основных концепций файловой системы NTFS операционной системы Windows и анализирование файла журнала транзакций $LogFile.

Задачи дипломной работы — раскрытие общих принципов работы файловой системы NTFS, изучение структуры файла журнала транзакций $LogFile и предоставление программы для его наглядного просмотра и поиска записей об операциях над файлами данного диска.

Дипломная работа состоит из введения, 2 разделов (3 подразделов), заключения, списка использованных источников и 3 приложений. Общий объем работы — 173 страницы, из них 41 страница — основное содержание, включая 23 рисунка и 2 таблицы, список использованных источников из 11 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе «Теоретическая часть» приводятся основной теоретический материал, базовые понятия и структуры, позволяющие раскрыть архитектуру файловой системы NTFS, содержимое файла $LogFile и его транзакций.

В первом подразделе «Файловая система NTFS» рассматривается система NTFS в целом, а также таблица $MFT, основные метафайлы и некоторые способы обеспечения безопасности в системе NTFS.

NTFS — стандартная файловая система для семейства операционных систем Windows NT фирмы Microsoft, целью создания которой были:

- высокая надежность;
- безопасность;
- поддержка носителей информации большой емкости.

Девизом файловой системы NTFS можно считать выражение «Все данные — файлы». Вся информация, как пользовательская, так и системная, хранится в файлах.

В определенном месте тома находится основная структура файловой системы NTFS — главная таблица файлов (Master File Table, MFT), в записях которой находится вся информация о расположении файлов в томе. Если файлы небольшие, они целиком хранятся прямо в записях MFT, такие файлы называют резидентными. Те файлы, которые не умещаются в записях MFT (поэтому хранятся в другом, указанном месте в томе), называют нерезидентными.

В файловой системе NTFS существует достаточно много метафайлов, среди которых — $LogFile — файл журнала транзакций. NTFS регистрирует в него все операции, которые влияют на структуру тома NTFS. $LogFile применяется и для восстановления тома NTFS после аварии системы.

NTFS — отказоустойчивая система, которая может привести себя в корректное состояние почти при любой ошибке. Она является такой, в частности, благодаря существованию процесса журналирования будущих изменений. Журналирование нужно для того, чтобы при возникновении ошибки в процессе

изменения файловая система после восстановления не находилась в каком-нибудь промежуточном состоянии. Это основано на понятии транзакции: действие либо совершено полностью и корректно, либо не совершено вообще.

Транзакции журналирования обладают свойствами:

- атомарности: они являются единым целым. Все действия в рамках транзакции либо произошли, либо не происходят. Во втором случае система возвращается в состояние, в котором она была до транзакции;
- непротиворечивости: после завершения транзакции данные должны подчиняться правилам, которые определены для данного набора данных;
- изоляции: все транзакции выполняются обособливо и не влияют на работу друг друга;
- долговечности: система не сможет вернуться в то состояние, в котором она была до начала завершенной транзакции.

Во втором подразделе «Структура журнала транзакций $LogFile» описывается общая структура файла $LogFile, рассматриваются структуры страницы и операционной записи, приводится таблица с кодами операций «Повторить»/«Отменить».

$LogFile состоит из Области перезапуска и Области регистрации.

Базовая единица каждой области — страница.

Область перезапуска содержит информацию о последней/текущей операции. Она занимает 2 страницы. Каждая страница перезапуска начинается с «магического числа» RSTR.

В области регистрации записываются текущие записи операций.

Эта область разделена на «Область страниц буфера» и «Область обычных страниц». «Область страниц буфера» занимает первые две страницы области регистрации. «Область обычных страниц» занимает остальную часть области регистрации.

Страница состоит из одного заголовка и нескольких операционных записей, описывающих одну транзакцию. В заголовке страницы хранятся метаданные страницы.

Транзакция состоит из нескольких последовательных операционных записей.

Структура операционной записи содержит такие важные поля, как:

- текущий LSN: LSN текущей записи;
- предыдущий LSN: LSN предыдущей записи;
- LSN операции «Отменить» клиента: для случая исправления ошибки данная запись имеет следующую операцию «Отменить»;
- длина данных клиента: размер записи (от поля «Повторить операцию» до конца записи);
- тип записи: 0x02 (запись контрольной точки), 0x01 (остальная запись);
- флаги: 0x01 (запись пересекает текущую страницу), 0x00 (запись не пересекает текущую страницу);
- операция «Повторить»: код операции «Повторить»;
- операция «Отменить»: код операции «Отменить»;

В третьем подразделе «Определение содержимого транзакции» указывается способ определения вида транзакции, рассмотрены операции над файлом и их структуры.

По значениям кодов полей «Повторить»/«Отменить» можно определить, какой именно была данная транзакция:

- создание файла/директории — 0x02/0x00;
- удаление файла/директории — 0x0F/0x0E;
- запись (модификация) данных в тело файла — 0x07/0x07;
- переименование файла/директории — 0x06/0x05 (0x05/0x06).

Структура записи об операции создания файла следующая:

- заголовок операционной записи;
- заголовок файловой записи;
- атрибуты.

Структура записи об операции удаления файла следующая:

- заголовок операционной записи;
- атрибут $FILE_NAME.

Структура записи об операции записи (модификации) данных в теле файла следующая:

- заголовок операционной записи;
- атрибут $DATA после модификации;
- атрибут $DATA до модификации.

Структура записей о переименования файла (т.е. об операции удаления/добавления атрибута $FILE_NAME файла) следующая:

- заголовок операционной записи;
- атрибут $FILE_NAME.

Таким образом, в первом разделе были рассмотрены общие принципы устройства и работы файловых систем NTFS, их составляющие, надежность и безопасность, а также рассмотрено содержимое файла $LogFile, указан способ определения вида транзакции, рассмотрены структуры записей об операциях над файлом.

Во втором разделе «Практическая часть» демонстрируется разработанная программа *Анализатор файла $LogFile* и проводится обзор аналога — программы *NTFS Log Tracker*.

С помощью программы *Анализатор файла $LogFile* можно сделать следующее:

- вывести все хранящиеся в теле файла $LogFile операции;
- найти резидентные/нерезидентные тела файлов;
- вывести дополнительную информацию, полученную в результате работы программы, такую как: серийный номер тома, количество байт в секторе, количество секторов в кластере и т.д.;
- вывести дамп тела файла $LogFile.

В первом подразделе «Получение информации об операциях над файлами» описываются результаты отчета, полученного после проведенного опыта над файлами.

На диске были созданы два файла: «Резидентный файл.rtf» и «Нерезидентный файл.txt», которые имеют резидентное и нерезидентное тело соответственно. Затем они были удалены.

После запуска программы *Анализатор файла $LogFile* был получен отчет, в котором можно найти операции, производимые над каждым из файлов.

Для резидентного файла были найдены:

- операция создания файла
- несколько операций записи тела файла, в том числе та запись, которое содержит искомое тело файла;
- несколько операций переименования файла, которые удаляют и добавляют атрибуты имени файла, в том числе было найдено искомое имя файла.

Для нерезидентного файла были найдены аналогичные операции. Среди операций над этим файлом была операция записи тела нерезидентного файла с блоком данных, содержащим:

- количество кластеров, занимаемых данными;
- адрес начала блока данных.

После вставки этой информации в соответствующие поля программы было получено тело нерезидентного файла.

Также были найдены операции удаления для этих файлов. Операция удаления файла включает в себя несколько операций удаления, содержащих информацию об атрибутах имени, которые были у данного файла.

Кроме искомых операций над данными файлами были также найдены операции над системными файлами, такими как: $Quota, _restore{916E3A09-4348-426F-AEE6-8AFFCAADB317}, desktop.ini и т.п.

В программе также выводится дополнительная информация:

- серийный номер тома;
- количество байт в секторе;
- количество секторов в кластере;
- адрес стартового кластера MFT;
- адрес начала блока данных файла $LogFile;
- количество кластеров, занимаемых данными файла $LogFile.

И дамп тела файла $LogFile.

Во втором подразделе «Обзор аналога» рассматриваются возможности программы *NTFS Log Tracker* при анализе файла $LogFile, а также производится сравнение ее с разработанной программой *Анализатор файла $LogFile*.

NTFS Log Tracker распознает следующие виды событий (операций) над файлом:

- создание файла;
- запись резидентных/нерезидентных данных;
- удаление файла;
- переименование файла;
- перемещение файла.

На выходе программа выдает таблицу, содержащую следующие важные столбцы:

- LSN — логический порядковый номер;
- Event — событие;

- Detail — более конкретная информация о событии; например: при переименовании файла указаны старое и новое имена, а в случае записи резидентных/нерезидентных данных указывается их местоположение на диске (номер начального кластера и количество кластеров, занимаемых данными);
- File/Directory Name — имя файла;
- Create Time — время создания файла;
- Modified Time — время изменения файла;
- MFT_Modified Time — время изменения файловой записи;
- Access Time — время последнего чтения файла;
- Redo — операция «Повторить».

Программа *Анализатор файла $LogFile*, в дополнение к результату работы программы *NTFS Log Tracker*, может получить информацию о некоторых дополнительных полях.

Также программа *Анализатор файла $LogFile* позволяет получить само тело резидентного/нерезидентного файла, в то время как программа *NTFS Log Tracker* выдает лишь список отрезков, указывающий местоположение тела на диске.

В отличие от *NTFS Log Tracker* программа *Анализатор файла $LogFile* группирует всю информацию о конкретном файле в один блок, что значительно упрощает анализ полученной информации.

Таким образом, во втором разделе была продемонстрирована разработанная программа *Анализатор файла $LogFile*, которая может распознать виды операций и получить сведения об имени, теле, времени создания файла и т.д. Также был проведен обзор аналога — программы *NTFS Log Tracker*, и рассмотрены преимущества над ней программы *Анализатор файла $LogFile.*

ЗАКЛЮЧЕНИЕ

В первой главе данной работы были рассмотрены общие принципы устройства и работы файловых систем NTFS, их составляющие, надежность и безопасность, а также рассмотрена структура $LogFile.

NTFS надежна, отказоустойчива, журналируема, обеспечивает разграничение доступа. Основная ее структура — MFT, в которой каждый файл и каталог представлен хотя бы одной записью.

Файловая система NTFS содержит один из важнейших файлов – файл журнала транзакций $LogFile, благодаря которому в случае возникновения ошибок или сбоев операционная система восстанавливает статус файловой системы в том состоянии, в котором она была до возникновения проблемы.

Таким образом, файловая система NTFS гарантирует корректность своего состояния при любых ситуациях.

Во второй главе данной работы была продемонстрирована работа программы *Анализатор файла $LogFile*, которая позволяет сделать следующее:

- вывести все хранящиеся в теле файла $LogFile операции, производимые над каждым из файлов на данном диске;
- вывести тело нерезидентного атрибута $DATA файла по информации, содержащейся в списке отрезков;
- вывести дополнительную информацию, полученную в результате работы программы: серийный номер тома, количество байт в секторе, количество секторов в кластере, адрес стартового кластера MFT, адрес начала блока данных файла $LogFile, количество кластеров, занимаемых данными файла $LogFile;
- вывести дамп тела файла $LogFile.

Также был проведен обзор аналога — программы *NTFS Log Tracker*, и рассмотрены преимущества над ней программы *Анализатор файла $LogFile.*

Таким образом, все поставленные задачи были решены, цель дипломной работы была достигнута.