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

Установление особенности создания и обработки файлов офиса

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Тихолоза Дениса Валерьевича

Научный руководитель

доцент, к.ф.-м.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

Операционные системы Microsoft семейства Windows NT нельзя представить без файловой системы NTFS – одной из самых сложных и удачных из существующих на данный момент файловых систем.

Целью данной работы является:

1. Нахождение файлов контекстным поиском или по имени
2. Нахождение и восстановление удаленных файлов по их контексту.
3. Получение и сопоставление временных характеристик и получение информации как изменяются данные о времени при проведении операций копирования, удаления, перемещения и редактирования.
4. Нахождение файлов .lnk и сопоставление их временных характеристик
5. Нахождение сведений в реестре об этом файле
6. По полученным временным характеристикам нахождение удаленных файлов типа tmp.
7. Получение информации о владельце файла по SID.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и одного приложения, включающего в себя исходный код программы, разработанной в рамках дипломной работы. Общий объем работы – 81 страница, из них 41 страница – основное содержание, включая 19 рисунков и список использованных источников из 21 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы носит название «Файловая система NTFS» и разделяется на 10 подразделов. В ней описывается структура файловой системы NTFS семейства Windows, которая была разработана, чтобы удовлетворять требованиям быстродействующих файловых и сетевых серверов, а так же персональных ЭВМ и, при этом, обойти многие из ограничений, ранее сделанных в файловых системах FAT16 и FAT32. В данном разделе описываются расположение и структура MFT-зоны, ее поведение при переполнении всего свободного пространства и вид в котором находится вся информация о системе.

Первый подраздел описывает метафайлы файловой системы NTFS. В нем приводится список метафайлов, их расположение в файловой системе и описание того, за какой аспект работы системы они отвечают.

Во втором подразделе описываются такие понятия как файлы и потоки файловой системы NTFS, их расположение относительно MFT

В третьем подразделе описываются каталоги файловой системы NTFS, их структура, в виде бинарного дерева, которая позволяет осуществлять более быстрый поиск внутри каталога за счет нужного расположения файлов.

В четвертом подразделе описывается процесс получения информации о файлах или каталогах в файловой системе NTFS. Расположение файловых записей. Описываются атрибуты и их расположение в файловой записи, а так же информацию которую можно получить из них.

В пятом подразделе описывается атрибут $STANDARD_INFORMATION. Структура и информация, которая может быть из него получена, в частности временные штампы файла и идентификатор безопасности, с помощью которого происходит получения SID владельца файла.

В шестом подразделе описывается структура атрибута $FILE_NAME, и информация, которая может быть получена из данного атрибута, например четыре временных штампа, имя файла и имя родительского каталога.

В седьмом подразделе описывается атрибут $DATA, в котором находится все содержимое файла. Описывается структура резидентного и нерезидентного атрибута, и способ получения информации из них. Для нерезидентного атрибута описывается расположение тела атрибута $DATA за пределами MFT, и отрезок runlist с помощью которого можно получить расположения тела атрибута.

В восьмом подразделе описывается процесс удаления файлов и каталогов в файловой системе NTFS, изменения временных характеристик атрибута $STANDART_INFORMATION при удалении файла. Так же в данном подразделе описывается процесс восстановления удаленных фалов в файловой системе NTFS.

В девятом подразделе приводится описание идентификатора безопасности – SID. Идентификаторы безопасности – это основной строительный блок с моделью безопасности Windows. Они работают с определенными компонентами авторизации и технологиях управления доступом в инфраструктуре безопасности операционных систем Windows. Описывается структура данных, в которой находится идентификатор безопасности. NTFS всегда располагала функциями безопасности, позволяющими администратору указать пользователей, которым разрешен или запрещен доступ к тем или иным файлам и каталогам. В данном подразделе описывается технология консолидированной безопасности, которая оптимизирует выделение дискового пространства для хранения дескрипторов безопасности и позволяет быстро отыскивает дескрипторы безопасности в файле $Secure в ходе проверок безопасности. Так же в данном подразделе происходит описание метафайла $Secure, его атрибутов $SDH, $SII, $SDS и процесс, с помощью которого можно получить SID владельца файла.

Второй раздел дипломной работы посвящен файлам, которые используются при работе MS WORD и разделяется на три подраздела.

Первый подраздел описывает файл с расширением .DOCX – документ, созданный Microsoft Word, программой обработки текста. Содержит текст документа, изображений, форматирование, стили, нарисованные объекты и другие параметры документа. В данном подразделе описывается структура документа: XML-файлы и три папки, docProps, Word, и _rels содержащиеся в нем и описывающие свойства документа, содержание и отношения между файлами.

Второй подраздел представляет собой описание .lnk файлов использующихся в Windows, в качестве ссылки на исходный файл, программу или каталог

Третий подраздел включает в себя описание временных файлов, имеющих расширение .tmp, которые образуются при работе с файлами MS WORD. Описываются причины создания временных файлов, такие как быстродействие и целостность данных, возможности операционной системы при работе с этими файлами, так же описываются директории в ОС Windows, в которых создаются временные фалы при работе с документами MS WORD и при каких действиях это происходит.

Третий раздел дипломной работы описывает реализацию и обзор разработанного программного продукта. Раздел состоит из двух подразделов.

В первом подразделе приводится обзор аналогов разработанного программного продукта:

1. Belkasoft Evidence Center – программное обеспечение для произведения компьютерно-технических экспертиз, компьютерной криминалистики, разработанное специально для заказчиков из правоохранительных органов, и используется различными отделениями полиции и структурами правопорядка по всему миру.

2. EnCase – лидер списка разработчиков программных продуктов для E-Discovery. EnCase позволяет решать ряд задач присущих как E-Discovery, так и выполнять ряд задач стоящих перед отделом информационной безопасности любой организации. Термин Electronic Discovery (E-Discovery)

подразумевает под собой любой процесс поиска электронных данных, определение их местоположения и фиксация нарушения, либо автоматическое перемещение в установленное политиками безопасности хранилище.

Во втором подразделе приводится обзор разработанного программного продукта, приводится описание основных функций и структур, использованных при разработке продукта на языке C++. Так же в данном подразделе приведено описание областей в которых осуществляется поиск необходимой информации. В рамках данного подраздела приводится описание работы с графическим интерфейсом программного продукта.

ЗАКЛЮЧЕНИЕ

В процессе выполнения работы были изучены установления последовательности создания и обработки файлов офиса. Была написана программа на языке C++, которая делает предположения об операциях совершаемых над файлом, находит файлы и записи реестра, которые участвовали в его редактировании, определяет владельца файла, а так же осуществляет поиск и восстановление удаленных файлов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кэрриэ Б. Криминалистический анализ файловых систем [Электронный ресурс] / Кэрриэ Б. СПб. : Питер, 2007. 480 с. Загл. с экрана. Яз. рус.

2. Восстановление NTFS – undelete своими руками [Электронный ресурс] // samag.ru [Электронный ресурс] : [сайт]. URL: http://samag.ru/archive/article/414 (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

3. Касперски К. Восстановление данных. Практическое руководство [Электронный ресурс] / Касперски К. // Пер. с англ. СПб: БХВ – Петербург , 2006. 352 с. Загл. с экрана. Яз. рус.

4. Файловая система NTFS [Электронный ресурс] // ixbt.com [Электронный ресурс] : [сайт]. URL: http://www.ixbt.com/storage/ntfs.html (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

5. Файловая система NTFS [Электронный ресурс] // kge.msu.ru [Электронный ресурс] : [сайт]. URL: http://www.kge.msu.ru/techaid/ntfs.htm (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

6. Создание временных файлов Word [Электронный ресурс] // support.microsoft.com [Электронный ресурс] : [сайт]. URL: https://support.microsoft.com/ru-ru/kb/211632 (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

7. Марк Руссинович, Дэвид Соломон. Внутреннее устройство Microsoft Windows [Электронный ресурс] / Марк Руссинович, Дэвид Соломон. СПб. : Питер, 2014. 799с. Загл. с экрана. Яз. рус.

8. Консолидированная безопасность [Электронный ресурс] // osp.ru [Электронный ресурс] : [сайт]. URL: https://www.osp.ru/winitpro/2001/07/175039 (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

9. Восстановление данных в разделах NTFS [Электронный ресурс] // frolov-lib.ru [Электронный ресурс] : [сайт]. URL: http://www.frolov-lib.ru/datarecovery/articles/ntfs_recovery/index.html (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

10. NTFS - Files [Электронный ресурс] // flatcap.org [Электронный ресурс] : [сайт]. URL: https://flatcap.org/linux-ntfs/ntfs/files/index.html (дата обращения: 21.11.2017). Загл. с экрана. Яз. англ.

11. Атрибуты [Электронный ресурс] // citforum.ru [Электронный ресурс] : [сайт]. URL: http://citforum.ru/operating_systems/windows/ntfs/2.shtml (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

12. Нерезидентные атрибуты [Электронный ресурс] // studopedia.org [Электронный ресурс] : [сайт]. URL: https://studopedia.org/3-100586.html (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

13. Файлы NTFS [Электронный ресурс] // intuit.ru [Электронный ресурс] : [сайт]. URL: https://www.intuit.ru/studies/courses/10471/1078/lecture/16586?page=2 (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

14. Файловая система NTFS извне и изнутри [Электронный ресурс] // samag.ru [Электронный ресурс] : [сайт]. URL: http://samag.ru/archive/article/395 (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

15. Создание временных файлов Word [Электронный ресурс] // support.microsoft.com [Электронный ресурс] : [сайт]. URL: https://support.microsoft.com/ru-ru/help/211632/description-of-how-word-creates-temporary-files (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

16. Описание LNK [Электронный ресурс] // fileext.ru [Электронный ресурс] : [сайт]. URL: http://fileext.ru/lnk (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

17. Osterman, L. Larry Osterman's WebLog [Электронный ресурс] // blogs.msdn.microsoft.com [Электронный ресурс] : [сайт]. URL:

https://blogs.msdn.microsoft.com/larryosterman/2004/09/01/what-is-this-thing-called-sid/ (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

18. Structure of $Secure File [Электронный ресурс] // ntfs.com [Электронный ресурс] : [сайт]. URL: http://www.ntfs.com/ntfs-permissions-file-structure.htm (дата обращения: 21.11.2017). Загл. с экрана. Яз. англ.

19. Использование NtFsControlFile для получение информации о файле на NTFS [Электронный ресурс] // hex.pp.ua [Электронный ресурс] : [сайт]. URL: http://hex.pp.ua/NtFsControlFile.php (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.

20. Побегайло Александр Павлович Системное программирование в Windows [Электронный ресурс] / Побегайло Александр Павлович СПб. : Питер, 2006. 1056 с.

21. Технический обзор идентификаторы безопасности [Электронный ресурс] // technet.microsoft.com [Электронный ресурс] : [сайт]. URL: https://technet.microsoft.com/ru-ru/library/dn743661(v=ws.11).aspx (дата обращения: 21.11.2017). Загл. с экрана. Яз. рус.