УДК 004.622

ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА ФАЙЛОВОЙ СИСТЕМЫ NTFS

Е.Н. Ливак, О.Р. Мысливец

В данной работе исследуются порядок и особенности проведения криминалистического анализа файловой системы NTFS. Исследуются существующие в файловой системе NTFS категории данных, анализируется их структура и содержание с целью проведения более эффективного криминалистического анализа.

Введение

Файловая система NTFS бесспорно является самой распространенной и используемой файловой системой. В связи с этим экспертам-криминалистам очень часто приходится проводить криминалистический анализ файловой системы NTFS с целью получения данных, которые смогут фигурировать как улики в уголовных делах. Однако спецификации файловой системы NTFS закрыты, что создает очевидные неудобства, как при проведении криминалистического анализа, так и при простом исследовании её структуры и принципов работы. Исходя из предоставленного компанией Microsoft базового описания файловой системы [1][2] и исследований проекта «Linux-NTFS» [3] можно судить о том, что NTFS довольно сложная файловая система, включающая в себя разные категории данных и использующая разнообразные возможности для эффективного хранения данных. Все эти факторы необходимо учитывать при проведении криминалистического анализа.

Анализ категорий данных

Согласно одной из существующих моделей анализа файловых систем [4], информацию, хранящуюся в файловой системе NTFS, можно разделить на следующие категории: данные файловой системы, содержимого файлов, метаданные, данные имен файлов и прикладные данные. Любая информация, хранящаяся в файловой системе, принадлежит к одной из вышеперечисленных категорий в независимости от того, какую роль она играет в NTFS. При этом данные файловой системы, содержимого файлов и метаданные относятся к необходимым данным, а остальные категории к вспомогательным. При поиске улик эксперту необходимо определить вид информации и категорию данных, в которой предполагаемые улики будет содержаться. Вид информации и категория данных в свою очередь определяют методы анализа информации. Для эксперта-криминалиста в первую очередь интерес представляют категории данных файловой системы, содержимого файлов и метаданных как относящиеся к необходимым.

Анализ категории данных файловой системы

К категории данных файловой системы относятся общие данные, описывающие строение файловой системы и местонахождение других важных

данных. Зачастую большая часть этих данных размещается в стандартных структурах

При криминалистическом анализе файловой системы NTFS в первую очередь следует проанализировать загрузочный сектор NTFS. Данный сектор содержит информацию об NTFS-разделе, и его структура схожа с аналогичным сектором файловой системы FAT32. Информация о данном секторе хранится в седьмой записи Master File Table, и это единственный файл метаданных файловой системы со статическим расположением. В загрузочном секторе полезными для эксперта-криминалиста могут оказаться следующие поля:

- BytesPerSector, находящееся по смещению 0x0B и отвечающее за количество байт в секторе;
- SectorsPerCluster, находящееся по смещению 0x0D и отвечающее за количество секторов в кластере;
- LogicalClusterNumberForMFT, находящееся по смещению 0x30 и отвечающее за адрес начального кластера Master File Table;

Без анализа вышеперечисленных полей загрузочного сектора NTFS невозможно получить базовую информацию о NTFS-разделе. Особое внимание следует уделить тому факту, что поля, описывающие Master File Table, имеют специальный формат [4].

После анализа загрузочного сектора следует приступить к анализу Master File Table. Базовый анализ файла $MFT может дать полезную информацию о файловой системе, а именно время создания файловой системы [5]. На основании данной информации можно определить продолжительность использования файловой системы, что может быть полезно при проведении расследования. Однако при анализе $MFT и всех остальных файлов метаданных файловой системы следует иметь в виду, что MFT-зона может быть фрагментирована. Несмотря на то, что под Master File Table изначально выделяется пространство с учетом будущего расширения её размера, некоторые пользовательские данные могут быть записаны в MFT-зону. Такое возможно, если в MFT-зоне существуют свободные блоки данных, размер которых позволяет записать в них пользовательские данные без фрагментации, и в пользовательской зоне нет идущих друг за другом свободных блоков данных, позволяющих записать в них информацию заданного размера.

Анализ категории данных содержимого файлов

К категории данных содержимого файлов относятся адреса ячеек информации, ассоциированных с файлами и каталогами. Информация о состоянии кластера в файловой системе NTFS хранится в файлах метаданных файловой системы $Bitmap и $BadClus. Не существует никаких особых обстоятельств, которые необходимо было бы учитывать при анализе категорий данных содержимого NTFS. Однако следует заметить, что в зависимости от ОС и драйвера файловой системы способ выделения свободных блоков данных может различаться. В ОС семейства Windows для выделения свободных блоков данных используется алгоритм оптимального подбора. Аналогичный алгоритм

используется в драйвере NTFS-3g, используемом в операционных системах на ядре Linux.

Также стоит отметить тот факт, что операционные системы семейства Windows выделяют блоки данных для файлов метаданных файловой системы непоследовательно. Как было сказано выше, файл $Boot всегда располагается в первых секторах файловой системы. Остальные файлы могут располагаться в первой половине файловой системы, причем между ними могут находиться свободные блоки данных. Расположение файлов метаданных файловой системы не носит детерминированный характер и зависит от общего размера файловой системы.

Знание вышеописанных особенностей расположения файлов метаданных файловой системы NTFS может быть полезно в случае, когда тип файловой системы заранее неизвестен, а эксперту-криминалисту требуется определить, с какой файловой системой ему предстоит работать. Тот факт, что в NTFS файлы метаданных файловой системы не следуют друг за другом, существенно отличает файловую систему NTFS от таких файловых систем как FAT32 и Extended File System, в которых файлы метаданных файловой системы следуют последовательно друг за другом. При неизвестном типе файловой системы следует провести поиск по сигнатурам, которые могут однозначно определить тип файловой системы. В качестве таких сигнатур для файловой системы NTFS можно использовать строку “NTFS” и проводить её поиск в загрузочном секторе NTFS и строку “FILE”, с которой начинается каждая запись Master File Table.

Анализ категории метаданных

К категории метаданных относятся данные, описывающие файлы и каталоги. Все метаданные в файловой системе NTFS хранятся в атрибутах. Так как целью проведения анализа в категории метаданных является получение дополнительной информации о файле или каталоге, то анализ сводится к получению информации о базовых атрибутах. Многие особенности, возникающие при анализе данной категории, относятся к восстановлению данных, нежели к криминалистическому анализу. Однако сжатые и шифрованные атрибуты также могут создать проблемы для эксперта-криминалиста. Еще одной особенностью может служить тот факт, что для сокрытия информации злоумышленник может использовать дополнительные атрибуты $Data или использовать неиспользуемые части записей MFT или атрибутов. Тем не менее, использование дополнительных атрибутов или неиспользуемых частей структур файловой системы сопряжено с рисками потери информации из-за динамической природы NTFS.

Заключение

Файловая система NTFS имеет очень эффективную и одновременно сложную структуру. Однако, из-за закрытых спецификаций файловой системы NTFS как разработчикам драйверов для свободных операционных систем, так и экспертам-криминалистам приходится заниматься обратной разработкой

файловой системы. Учитывая тот факт, что файловая система NTFS может быть также использована в операционных системах с открытым исходным кодом, возникает необходимость в более детальном и глубоком анализе структуры и принципов работы файловой системы NTFS с учетом используемой операционной системы.

Список литературы

1. How NTFS Works: Local File Systems [Electronic resource] / Microsoft TechNet Library – Mode of access: https://technet.microsoft.com/en-us/library/cc781134%28WS.10%29.aspx – Date of access: 27.03.2016
2. NTFS Organization and Structure [Electronic resource] / NTFS General Info – Mode of access: http://ntfs.com/ntfs.htm#basics – Date of access: 27.03.2016
3. Linux NTFS Project [Electronic resource] / Linux NTFS Project – Mode of access: https://flatcap.org/linux-ntfs/index.html – Date of access: 27.03.2016
4. Кэрриэ Б. Криминалистический анализ файловых систем/ Кэрриэ Б. – СПб.: Питер, 2007. – 470с.
5. Федотов, Н.Н. Форензика – компьютерная криминалистика / Федотов, Н.Н. – Москва: «Onebook.ru», 2015. – 420с.

Ливак Елена Николаевна, доцент кафедры системного программирования и компьютрной безопасности Гродненского государственного университета имени Янки Купалы, кандидат технических наук, доцент, livak@grsu.by

Мысливец Олег Романович, студент 1 курса II ступени высшего образования факультета математики и информатики Гродненского государственного университета имени Янки Купалы, myslivec.oleg@yandex.ru