УДК 004.056.57

Вестник УрФО № 1(39) / 2021, с. 21–26

Духан Е.И., Князева Н.С.

DOI: 10.14529/secur210103

АНАЛИЗ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ ИЗМЕНЕНИЙ ВРЕМЕННЫХ ОТМЕТОК ФАЙЛОВ

В статье рассмотрены работы, посвященные выявлению закономерностей изменения временных отметок при совершении файловых операций. Представлена авторская методика экспериментальных исследований временных отметок файлов. Полученные результаты исследований сведены в таблицу, которая наглядно представляет изменения временных отметок при выполнении пользователем операций над файлами. Систематизированные в виде таблицы данные могут явиться основой для разработки методики восстановления последовательности файловых операций, пригодной для автоматизации.

Ключевые слова: *временные отметки, NTFS, $STANDARD_INFORMATION, $FILE_NAME, файловые операции, компьютерная криминалистика.*

Duhan E.I., Knyazeva N.S.

ANALYSIS OF THE FILES TIMESTAMPS VARIATIONS INVESTIGATION RESULTS

In the article the papers concerning identification of patterns for timestamps variation during file operations being performed are observed. The authors suggest a unique method files timestamps experimental investigation. The obtained research results are summarized in a table that clearly shows the changes in time stamps when the user performs operations over files. Systematized data in the form of a table can be the basis for the development of a method for restoring a sequence of file operations that is suitable for automation.

Keywords: *timestamps, NTFS, $STANDARD_INFORMATION, $FILE_NAME, file operations, computer forensics.*

Современные информационные технологии не только способствуют активному развитию обществу, но и стимулируют рост преступлений, в которых компьютер выступает средством их совершения. Одним из распространенных вопросов, возникающих в ходе расследования компьютерных преступлений, является установление времени создания, изменения и распространения компьютерной информации, хранимой в виде конкретных файлов. Типовой задачей компьютерной криминалистики («Форензики») явля-

ется восстановление последовательности операций, совершенных пользователем над файлами [1]. Для решения криминалистической задачи исследуется служебная информация, регистрируемая в файловой системе (ФС) компьютера. Достоверность и глубина восстановления цепочки файловых операций (ФОп) зависит от объема информации, извлечение и анализ которой требуют большого объема ручной работы и высокой квалификации специалиста.

Файловая система представляет собой структурированное хранилище каталогов и файлов. С точки зрения восстановления файловых операций ФС следует рассматривать как дискретную динамическую систему, которая характеризуется состояниями в некоторые моменты времени. Под воздействием программного обеспечения во время активных действий пользователя компьютера эти состояния изменяются. Таким образом, восстановление последовательности ФОп является задачей системного анализа и сводится к определению траектории движения между начальным и конечным состояниями системы.

Состояниями системы называют совокупность значений некоторых ее характеристик [2]. Применительно к ФС такими характеристиками могут выступать метаданные файлов, а именно временные отметки (ВО). Обычно в ФС для одного файла хранятся три обязательных ВО: создания, последнего изменения и последнего доступа. В ФС NTFS, с которой работают наиболее распространенные операционные системы линейки Windows, для одного файла существуют четыре ВО: создания (**C**), последнего изменения (**M**), последнего доступа (**A**) и последней модификации метаданных (**X**) файла. Два комплекта таких меток хранятся соответственно в атрибутах файловой записи $STANDARD_INFORMATION и $FILE_NAME [3]. При этом одноименные метки, хранящиеся в различных атрибутах файла, при выполнении ФОп меняются поразному и несут информацию о действиях пользователя. Восстановление интересующей следствие хронологии событий возможно на основе тщательного исследования соотношений указанных 8 ВО.

На сегодняшний день существует несколько работ, посвященных изучению процессов изменения ВО. В этих работах используется единый подход к исследованию, который состоит в том, что закономерности в изменениях ВО выявляются экспериментальным путем. Авторы фиксируют и сравнивают значения ВО до и после совершения анализируемой ФОп. Следует добавить, что подобные исследования выполняются вручную и требуют колоссальных временных затрат и высокой квалификации эксперта. Ниже приведен краткий обзор наиболее информативных исследований.

Т. Кнутсон в работе [4] проводил наблюдения только за ВО из атрибута $STANDARD_INFORMATION в ОС Windows XP, 7, 8. Для извлечения и отображения ВО использовалась программа FTK Imager (версия 3.1.1.8). Опция обновления ВО **A** в ОС Windows 7, 8 была выключена1, а в ОС Windows XP — включена. В результате исследований Т. Кнутсон определил, как изменяются ВО при совершении 3 ФОп: копирование, перемещение, редактирование. В работе перемещение и копирование проводилось как в пределах одного тома с ФС NTFS, так и между томами.

В. Матвеева в работе [5] проводила наблюдения за ВО из атрибутов $STANDARD_INFORMATION и $FILE_NAME в ОС Windows XP, 7. Опция обновления ВО **A** была включена. Для извлечения и отображения ВО использовалась команда «istat» в программе TheSleuthKit (TSK). В результате исследований В. Матвеева определила характер изменений ВО при совершении 8 ФОп: переименование, перемещение, копирование, удаление, открытие, изменение файла, просмотр и изменение его атрибутов. Перемещение и копирование проводилось как в пределах одного тома, так и между томами.

GS. Cho в работе [6] проводил наблюдения за ВО из атрибутов $STANDARD_INFORMATION и $FILE_NAME в ОС Windows 7. Опция обновления ВО **A** была выключена. В результате исследований GS. Cho определил, как изменяются ВО при совершении 5 ФОп: переименование, перемещение, копирование, редактирование файла, изменение его атрибутов. Перемещение и копирование проводилось как в пределах одного тома, так и между томами.

[1] В файловой системе NTFS существует возможность отключать обновление времени последнего доступа к файлам. Согласно документации Microsoft, эта возможность предназначалась для увеличения быстродействия. Чтобы активировать эту опцию необходимо параметр HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate установить в значение 0. В ОС Windows 7, 8, 10 данный параметр по умолчанию выключен. В ходе экспериментов выявлено, что характер изменений ВО зависит от состояния этой опции.

Представленные в [4, 5, 6] исследования позволили авторам выявить ряд закономерностей процесса изменения ВО при выполнении над файлами различных операций и предложить частные методики восстановления последовательности ФОп, которые могут оказаться полезными экспертам-специалистам. Однако эти изыскания носят весьма разрозненный, не системный характер и не обеспечивают полноту исследований и широту охвата разнообразия ФОп и вариантов их выполнения, поэтому не могут являться основой для создания автоматизированного инструментария для восстановления последовательности ФОп. Кроме того, для извлечения требуемой информации о ВО файлов авторы использовали программы, не гарантирующие ее полноту.

Тем не менее, вышеописанные результаты исследований позволяют говорить о целесообразности системного подхода к анализу ВО. Авторами статьи была разработана методика проведения исследования ВО [7, 8]. Методика состоит из трех этапов: подготовка совокупности объектов исследования; совершение множества разнообразных ФОп; фиксирование изменений ВО.

Важное преимущество разработанной методики состоит в том, что в качестве объектов исследования используется специальным образом подготовленный набор файлов разных форматов, размеров (обеспечивается хранение содержимого файла как в файловой записи таблицы MFT, так и во внешних кластерах ФС), с установленными атрибутами («архивный», «только чтение», «системный» или «скрытый»). Исследования проводятся в двух возможных режимах: с включенной и выключенной опцией обновления ВО последнего доступа. Перечень ФОп расширен и охватывает вопросы, которые в большинстве случаев задают эксперту-криминалисту при постановке задачи на проведение компьютерного исследования. ФОп выполняются с использованием различных программ, выбор которых обусловлен статистикой их использования обычными пользователями персональных компьютеров. Кроме того, для реализации методики была создана программа, которая извлекает одновременно все ВО с точностью их хранения 10^{-7} с.

В результате исследований процессов изменения ВО по предложенной методике были получены следующие результаты.

1. Подтверждены результаты исследований GS. Cho, T. Кнутсон, B. Матвеевой для ФОп: копирование, перемещение, редактирование, открытие, удаление файла, просмотр и изменение его атрибутов.

2. Уточнены изменения ВО для ФОп: редактирование в пакете MicrosoftOffice и перемещение между томами (из FAT в NTFS).

Ранее T. Кнутсон определил, что при перемещении из FAT в NTFS у файла ВО **A** и **X** синхронно изменяются, а ВО **C** и **M** наследуются от исходного файла. В результате использования представленной методики дополнительно определено, что ВО **M** округляется до секунд (нули в семи младших разрядах точной ВО), ВО **C** округляется до миллисекунд (нули в пяти младших разрядах точной ВО). Это объясняется тем, что в NTFS точность фиксирования ВО равна 10^{-7} с, а в FAT точность фиксирования ВО **M** равна 1 с, ВО C— 10^{-2} с.

GS. Cho при исследовании операции редактировании файла в приложении MicrosoftOffice обнаружил, что у файла синхронно изменяются ВО **M = A = X**. В результате использования методики дополнительно определено, что изменившиеся ВО не абсолютно идентичны, а имеют некоторые отличия в десятых долях секунд. Это объясняется затянутым процессом сохранения файла на основе глобального шаблона Normal.dot.

3. Обнаружены новые значимые комбинации изменения ВО.

Например, при перемещении файла с установленными атрибутами «только чтение», «системный» или «скрытый» в файловом менеджере TotalCommander ВО **C, M, A** из атрибута $FILE_NAME наследуют значения ВО **C, M, A** из атрибута $STANDARD_INFORMATION соответственно, а ВО **X** из обоих атрибутов синхронно изменяются.

В результате исследований был получен большой объем данных, который был систематизирован и представлен в виде сводной таблицы (см. табл. 1), удобной для их дальнейшего анализа.

Для удобства анализа табл. 1 введены следующие обозначения: символами **«C», «M», «A», «X»** отображены соответственно ВО создания, модификации, последнего доступа к файлу и последней модификации метаданных. Символами **«SI»** обозначены ВО, извлеченные из атрибута $STANDARD_INFORMATION, символами **«FN»** — ВО, извлеченные из атрибута $FILE_NAME. Таким образом, например, **«SIA»** обозначает ВО последнего доступа из атрибута $STANDARD_INFORMATION, а **«FNC»** — ВО создания из

атрибута $FILE_NAME. Серые ячейки таблицы указывают на синхронное изменение ВО после выполнения ФОп. Белые ячейки — на отсутствие изменений. Символом Т в ячейках обозначается время выполнения ФОп, аббревиатуры **SIC, SIM, SIA, SIX** — наследование ВО значений из атрибутов $STANDARD_ INFORMATION.

Сформированная обобщенная таблица изменения ВО позволяет восстанавливать последнюю ФОп, совершенную над файлом. Например, если у исследуемого файла ВО **SIM=SIA=SIX**, и они изменились позже ВО **SIC, FNC, FNM, FNA, FNX,** то по таблице можно определить, что данной комбинации ВО соответствует операция «редактирование». Для того, чтобы восстановить цепочку из нескольких ФОп, необходимо знать возможные комбинации ВО, которые могут возникать при последовательном выполнении тех или

Таблица 1

Таблица изменений ВО

Файловая операция	SI				FN			
	C	M	A	X	C	M	A	X
Копированиев ОС Windows 7 (вкл. SIA) (исходный объект[2])			T					
Копирование (выкл. SIA) (исходный объект)								
Копирование в ОС Windows XP, Windows 8, 10 или в файловых менеджерах TotalCommander, FarManager (новый объект[3])	T		T		T	T	T	T
Копирование в ОС Windows 7 (новый объект)	T		T	T	T	T	T	T
Перемещение/переименование (новый объект)				T	SIC	SIM	SIA	SIX
Перемещение/переименование в файловом менеджере TotalCommander для файлов с установленными атрибутами «только чтение», «системный» или «скрытый» (новый объект)				T	SIC	SIM	SIA	T
Перемещение/переименование из файловой системы FAT в файловую систему NTFS (новый объект)			T	T	T	T	T	T
Просмотр атрибутов (вкл. SIA)			T					
Просмотр атрибутов (выкл. SIA)								
Изменение атрибутов				T				
Открытие в ОС Windows XP в оболочке Explorer(вкл. SIA)			T	T				
Открытиев ОС Windows 7, 8, 10 и в ОС Windows XP (не в оболочке Explorer) (вкл. SIA)			T					
Открытиев ОС Windows 7 (выкл. SIA)				T				
Открытие в ОС Windows XP, Windows 8, 10 или в файловых менеджерах TotalCommander, FarManager(выкл. SIA)								
Исполнение (запуск) в ОС WindowsXP в оболочке Explorer(вкл. SIA)			T	T				

[2] файл, над которым выполняли ФОп.

[3] новый файл, который был создан в результате выполнения ФОп над исходным объектом.

Продолжение таблицы 1

Файловая операция	SI				FN			
	C	M	A	X	C	M	A	X
Исполнение (запуск) в ОС Windows 7, 8, 10 и в ОС WindowsXP (не в оболочке Explorer) (вкл. SIA)			T					
Исполнение (запуск) в ОС Windows 7 (выкл. SIA)				T				
Исполнение (запуск) в ОС WindowsXP, Windows 8, 10 или в файловых менеджерах TotalCommander, FarManager								
Удаление (вкл. SIA)			T	T				
Удаление (выкл. SIA)				T				
Редактирование (вкл. SIA)		T	T	T				
Редактирование (выкл. SIA)		T		T				
Редактирование в пакете MicrosoftOffice		T	T	T		T	T	T
Разархивирование (вкл. SIA) (исходный объект)			T					
Разархивирование (выкл. SIA) (исходный объект)								
Разархивирование архиватором 7-Zip и встроенным архиватором Windows файлов с расширением 7z, rar, tar и архиватором WinRAR файлов с расширением zip, 7z, rar, tar, wim(новый объект)	T		T	T	T	T	T	T
Разархивирование архиваторами 7-Zip и встроенным архиватором Windows файлов с расширением zip (новый объект)				T	T	T	T	T

иных ФОп. На основе таблицы изменений ВО с целью сопоставления возможных последовательностей ФОп наблюдаемым вариантам состояний ВО файлов была разработана модель изменения значений ВО при выполнении ФОп [9]. Эту модель целесообразно было строить на основе теории конечных автоматов, которая традиционно используется для представления динамических систем [10]. В модели в качестве входных символов, которые подаются на вход автомата, рассматриваются ФОп, в качестве состояний автомата — комбинации ВО. Функция переходов между состояниями, сформированная на основе таблицы изменений ВО, описывает, каким образом ФОп изменяют состояния ВО. Адекватность модели подтверждена в ходе многочисленных экспериментов.

Результаты экспериментального исследования по специально разработанной методике, их систематизированное представление в виде таблицы и модель изменения значений ВО позволяют автоматизировать проведение компьютерного исследования, задачей которого является восстановление последовательности ФОп.

Литература

1. Федотов Н.Н. Форензика - компьютерная криминалистика. М.: Юридический мир, 2007. 432 с.

2. Гайдук А.Р. Непрерывные и дискретные динамические системы. М.: УМ и ИЦ « Учебная литература», 2004. 252 с.

3. Кэрриэ Б. Криминалистический анализ файловых систем. СПб. : Питер, 2007. 480 с.

4. Knutson T. Filesystem Timestamps: What Makes Them Tick? 2016. [Электронный ресурс]. Режим доступа: https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842. (дата обращения: 21.12.2020)

5. Матвеева В.С. Криминалистический подход к анализу временных атрибутов файлов в операционной системе семейства MicrosoftWindows и файловой системе NTFS // Безопасность информационных технологий. 2013. Вып. 1.

6. Cho GS. A computer forensic method for detecting timestamp forgety in NTFS // Computer & Security. 34 (2013). С. 36-46.

7. Духан Е.И., Князева Н.С. Методика и результаты исследования изменений временных отметок файловых объектов. // Радиотехника. 2020.Том 84, № 2 (4). С. 64-72.

8. Knyazeva N., Khorkov D., Vostretsova E. Building Knowledge Bases for Timestamp Changes Detection Mechanisms in MFT Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. С. 553-556.

9. Knyazeva N., Duhan E. Timestamp Change Model in Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. С. 623-626.

10. Перегудов Ф.И., Тарасенко Ф.П. Основы системного анализа. Томск: Изд-во НТЛ, 1997.396 с.

References

1. Fedotov N. Forenzika - Computer Forensics [Forenzika —komp'juternajakriminalistika]. M.: Juridicheskij Mir[M.: The Legal World], 2007. 432 p.

2. Gajduk A. Continuous and Discrete Dynamical Systems [Nepreryvnyeidiskretnyedinamicheskiesistemy]. M.:Uchebno-metodicheskijiizdatel'skijcentr «Uchebnajaliteratura»[M.: Educational-Methodical and Publishing Center «Educational Literature»], 2004. 252 p.

3. CarrierB.File System Forensic Analysis, 2007. 480 p.

4. Knutson T. Filesystem Timestamps: What Makes Them Tick? 2016. available at: https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842.(accessed 21December2020)

5. Matveeva V. Forensic Approach to the Analysis of Temporary File Attributes in the Operating System of the Microsoft Windows Family and the NTFS File System [Kriminalisticheskijpodhod k analizuvremennyhatributovfajlov v operacionnojsistemesemejstva Microsoft Windows ifajlovojsisteme NTFS] // Bezopasnostinformacionnyhtehnologij[Information Technology Security]. 2013. no. 1.

6. Cho GS. A Computer Forensic Method for Detecting Timestamp Forgety in NTFS // Computer & Security. 2013. Vol. 34, pp. 36-46.

7. Duhan E., KnyazevaN. Methodology and Results of the Study of Changes in the Timestamps of File Objects [Metodikairezul'tatyissledovanijaizmenenijvremennyhotmetokfajlovyhobektov]. // Radiotehnika[Radio Engineering]. 2020. Vol. 84, no 2 (4). pp. 64-72.

8. Knyazeva N., Khorkov D., Vostretsova E. Building Knowledge Bases for Timestamp Changes Detection Mechanisms in MFT Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. pp. 553-556.

9. Knyazeva N., Duhan E. Timestamp Change Model in Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. pp. 623-626.

10. Peregudov F., Tarasenko F. Fundamentals of System Analysis [Osnovysistemnogoanaliza]. Tomsk: Izd-vo NTL[Tomsk: Publishing House of Scientific and Technical Literature]. 1997.396 p.

ДУХАН Евгений Изович, доктор технических наук, доцент, доцент учебно-научного центра «Информационная безопасность, Уральский Федеральный Университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: eduhan@pm.convex.ru

КНЯЗЕВА Наталия Сергеевна, старший преподаватель учебно-научного центра «Информационная безопасность», Уральский Федеральный Университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: npalceva@inbox.ru

DUHAN Evgenij, Doctor of Technology, Associate Professor, Associate Professor of educational and scientific center «Information security», Ural Federal University named after the first President of Russia B.N.Yeltsin, 620002, Yekaterinburg, Mira str., 32. E-mail: eduhan@pm.convex.ru

KNYAZEVA Natalija, Senior lecturer of educational and scientific center «Information security», Ural Federal University named after the first President of Russia B.N.Yeltsin, 620002, Yekaterinburg, Mira str., 32. E-mail: npalceva@inbox.ru