Рецензия

на выпускную квалификационную работу студента 4 курса
Кафедры системного программирования СПбГУ
Медведева Андрея Александровича
Тема работы: Восстановление данных с дисков, повреждённых современными вредоносными программами

В работе рассматривается актуальная на сегодняшний день задача восстановления удаленных файлов с жестких дисков различных файловых систем. Несмотря на то, что внимание концентрируется на файловых системах FAT, NTFS, предложенный алгоритм способен будет работать и на других современных файловых системах. Автором предложены решения двух задач.

Первая состоит в восстановлении таблицы разделов MBR путем поиска сигнатур разделов и подстановки стандартного кода загрузчика. Автор достаточно подробно описывает структуру памяти MBR-записи, что говорит о достаточной глубине проработки темы.

Вторая состоит в восстановлении содержимого файлов на разделах типа NTFS, на которых была удалена таблица MFT. Примечательной особенностью алгоритма восстановления является то, что он позволяет восстанавливать файлы, которые были фрагментированы при хранении на жестком диске. Такое восстановление выполнено автором для файлов изображений в формате JPEG на основе введенной эвристики, которая связана с цветовыми особенностями самих изображений. Благодаря ей удается восстанавливать большее число файлов изображений, чем при применении утилиты Android Photo Forensic.

В качестве аналогов приводятся и другие утилиты, однако стоит отметить, что при данных тестовых условиях они не способны работать, так как не рассчитаны на работу с фрагментированными данными.

Работа имеет перспективу промышленного внедрения в инструменте цифрового криминалистического анализа Belkasoft Evidence Center.

В работе имеются следующие недостатки:

- Следует более точно описывать процесс тестирования: не приведено время выполнения анализа, хотя оно является немаловажной характеристикой подобного рода инструментов.
- Стоило провести более богатый обзор аналогов. Так не был рассмотрен популярный инструмент R-studio. В свете новизны результата преимущество приведенного автором подхода к восстановлению изображений могло бы выглядеть более весомым.
- Поскольку во вступлении был приведен в качестве примера вирус Petya, который шифрует MFT-запись раздела NTFS, следовало сделать вывод о том, насколько разработанное решение нивелирует его угрозу.
- Не было приведено аналогов по восстановлению таблицы разделов диска и был приведен лишь один тест.

В целом результат, полученный в работе, является оригинальным, он решает актуальную современную проблему, доказана эффективность по сравнению с аналогичным решением. Студент заслуживает оценку «отлично».

Ханов Артур Рафаэльевич,
Старший преподаватель СПбГУ

дата: 5 июня 2018