РЕЦЕНЗИЯ

на выпускную квалификационную работу обучающегося СПбГУ

Фунт Дины Дмитриевны

«Криминалистический анализ файловой системы XFS с восстановлением данных из журнала»

Работа Д. Д. Фунт посвящена задаче анализа и восстановления данных, извлеченных с цифровых носителей с файловой системой XFS. Задача актуальна в случае повреждения носителя, сбоев в файловой системе, в также в криминалистике. Работа идеологически состоит из трех частей.

В первой части проводится обзор существующих решений (коммерческих и с открытым кодом), изучаются особенности файловой системы XFS и исследуются способы восстановления удаленных данных. Признано, что имеющиеся на рынке программные продукты не подходят для решения поставленной задачи, и нужно писать своё.

Во второй части разрабатывается алгоритм восстановления удаленных данных XFS на основе анализа журнала файловой системы. Особое внимание уделено не только извлечению файла как такового, но и метаданных о нём (имя, время создания, обновления и т. п.).

В третьей части реализуется программное обеспечение для чтения файловой системы и восстановления удаленных данных на основе разработанного алгоритма, а также с применением алгоритма, предлагаемого в утилите xfs_undelete. ПО реализовано как расширение библиотеки The Sleuth Kit (TSK). Проведены эксперименты по применению алгоритмов к восстановлению данных как в случае предварительно подготовленных образов, так и в режиме «черного ящика». По результатам экспериментов признано оптимальным использовать алгоритмы не по отдельности, а в виде комбинации.

Предложенные в работе алгоритмы восстановления данных реализованы на языке программирования C, объем кода превышает 6,200 строк. Бóльшая часть кода посвящена деталям организации XFS. Выбор языка мотивирован тем, что базовая библиотека TSK, которую расширяют алгоритмы, написана на C. Аргументация спорная, т. к., например, C++ (и большинство других языков высокого уровня) совместимы с библиотеками на C.

К работе есть замечание: вместо общепринятого термина «B-дерево» автор использует такие вариации как «Б-дерево», «би-дерево» или даже «дерево B». Выглядит как неконсистентный перевод с английского. Кроме того, в тексте имеется небольшое число опечаток, пунктуационных и грамматических ошибок. Однако указанные недостатки не умаляют общего положительного впечатления.

Работа Д. Д. Фунт соответствует требованиям, предъявляемым к бакалаврским ВКР, содержание работы и её структура соответствуют заявленной теме, которая в полной мере раскрыта.

Считаю, что работе Д. Д. Фунт может быть выставлена оценка «отлично».

Канд. физ.-мат. наук,
ст. спец. по тестированию
«ТехЦентр Дойче Банка»
Машарский С. М.

« 12 » мая 2022 г.