Отзыв научного руководителя

на курсовую работу студента 344 группы

Медведева Андрея Александровича

"Исследование файла гибернации ОС Windows 10"

Файл гибернации Windows является одним из источников информации для специалистов цифровой криминалистической экспертизы. Этот файл хранит в себе артефакты последних действий, совершённых пользователем. Являясь некоторым слепком оперативной памяти, файл гибернации может содержать данные, которые нельзя найти в файлах на диске, такие как переписка в социальных сетях и других веб-приложениях, данные об открытых сетевых соединениях, история посещения интернет-сайтов в режиме анонимности, ключи дешифрации для зашифрованных разделов и т.п.

С выходом Windows 8 и затем Windows 10 формат хранения данных гибернации был изменён, в связи с чем его анализ старыми программными средствами оказался невозможен. При этом официального описания формата нет, а есть лишь догадки энтузиастов, которые экспериментируют с операционной системой, как с чёрным ящиком.

В рамках данной курсовой работы перед Андреем Александровичем были поставлены следующие задачи:

* Изучить структуру файла гибернации Windows 10
* Провести обзор существующих решений для анализа файла гибернации Windows 10
* Провести сравнительный анализ файла гибернации последней версии ОС Windows 10 с предыдущими версиями
* Разработать прототип программы на языке C++, позволяющей анализировать файл гибернации ОС Windows 10

Андрей Александрович полностью справился с предложенными задачами.

Текст курсовой работы написан хорошим русским языком, но имеет некоторые недостатки. Например, большое внимание уделено описанию формата файла гибернации, в то время как о прототипе сказано довольно скупо. Для понятности изложения кое-где не хватает рисунков и блок-схем. Несмотря на эти недостатки, считаю, что работа выполнена на высоком уровне и достойна оценки "отлично".

Научный руководитель
ст.преп. каф.сист.прогр.
Ю.А. Губанов