Отзыв научного руководителя
на курсовую работу студента 344 группы
Грабового Филиппа Николаевича
“Дешифрация образа диска с защитой BitLocker To Go инструментами анализа дампа памяти”

В связи с широким распространением полнодисковой шифрации реального времени, такой как BitLocker компании Microsoft, возникает целый ряд несколько неожиданных задач. Одной из таких задач является извлечение данных, связанных с криминалистическим исследованием носителя информации, имеющего отношение к некоторому уголовному делу. Владелец такого носителя может попытаться скрыть данные об использовании устройства с помощью шифрации. Дешифрация современных средств шифрования с помощью полного перебора или методов brute force представляется практически невозможной в силу чрезвычайно большого времени, требуемого такими подходами (миллиарды лет). В то же время, имея слепок оперативной памяти исследуемого устройства, можно попытаться найти ключи дешифрации и расшифровать носитель за гораздо меньшее время.

В рамках курсовой работы перед Грабовым Ф.Н. были поставлены следующие задачи:

1) Ознакомиться с алгоритмом шифрации BitLocker, а также инструментами снятия слепков памяти и дисков, отладки Windows, раскладкой процессов в памяти Windows
2) Предложить способ извлечения ключей дешифрации из слепков памяти
3) Реализовать извлечение ключей дешифрации и саму дешифрацию носителя информации
4) Апробировать решение в коммерческом продукте цифровой криминалистики Evidence Center компании «Белкасофт»

Филипп Николаевич полностью выполнил поставленные перед ним задачи. Проделанную Филиппом Николаевичем работу я характеризую как качественную и существенную. Считаю, что работа заслуживает оценки “отлично”.

Научный руководитель:
Губанов Ю. А.