Разработка системы криминалистического анализа мобильных устройств

Кондратьев Александр Владимирович,
Университет ИТМО, sany-94@mail.ru
Пантюхин Игорь Сергеевич, Университет ИТМО

Введение

В настоящее время мобильный телефон-это многофункциональное устройство, которое позволяет нам не только совершать звонки, но и обмениваться смс, делать снимки, оплачивать покупки и так далее. Люди используют его как для личного пользования, так и для работы. Из-за больших возможностей устройства растет количество и ценность обрабатываемой им информации. Криминалисты все чаще и чаще сталкиваются с проблемой, как извлечь максимум данных из устройства.

Цель

Проанализировав огромное количество существующих решений, такие как «Мобильный криминалист», «Nowsecure», были выявлены недостатки. Большинство программных комплексов предназначены для какой-то определенной операционной системы и требуют огромных денежных затрат. Поэтому было принято решение разработать свою систему криминалистического анализа мобильных устройств, которая была бы проста в использовании, кроссплатформенна и не менее функциональна, чем существующие аналоги.

Общие сведения

Большинство мобильных приложений хранит всю информацию в базе данных sqllite, которая легко извлекается. Проанализировав, а иногда декомпилировав(процесс воссоздания исходного кода декомпилятором) наиболее известные приложения, удалось достать данные пользователя. Информацию о владельце можно вытащить и из backup(процесс создания резервной копии данных) файла. Резервная копия может храниться в системе или в облаке(iCloud, Google). Это может быть как один файл, так и несколько. Чаще всего backup файл - это архив, который легко распаковывается. Собрав все возможные источники информации о пользователе вместе, мы получаем максимум данных из устройства.

Результаты

В ходе работы был произведен анализ наиболее известных мобильных операционных систем и получено, что телефон хранит в себе гораздо

больше информации, чем видит пользователь на экране. Даже удаленные данные остаются в памяти в виду их особенности хранения. Результатом проделанной работы является полностью функционирующая система, которая позволяет извлекать из мобильных телефонов максимум информации. Вся система работает в виде web-приложения, что позволило добиться кроссплатформенности и модульности.