

08, август 2017

УДК 004.35, 34

**Особенности исследования мобильных устройств под управлением
операционной системы IOS современными техническими средствами в
области криминалистики**

*Павленко К.И., студент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Юриспруденция, интеллектуальная собственность и судебная экспертиза»*

*Скворцова М.А. ассистент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Компьютерные системы и сети»,
magavrilova@bmstu.ru*

*Мочалкина И.С., студент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Юриспруденция, интеллектуальная собственность и судебная экспертиза»*

*Сиротина А.С., студент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Экономика и организация производства»*

Введение

В современном мире мобильное устройство каждого человека может рассказать о своем владельце гораздо больше информации, чем самые близкие люди. Поэтому расследование преступлений все чаще и чаще начинается с исследования информации, которая храниться на мобильном устройстве.

В мобильной криминалистике для извлечения данных из мобильных устройств используется три основных метода:

Извлечение данных на физическом уровне. Это самый оптимальный способ, который позволяет криминалисту получить наибольшее количество данных, в том числе удаленных.

Извлечение данных на уровне файловой системы. Это второй по значимости способ: при его использовании криминалист извлекает все данные, видимые на уровне файловой системы. При этом восстановить удаленные файлы невозможно. Исключение

составляют удаленные записи из баз данных SQLite, а также миниатюры удаленных пользователем изображений.

Извлечение данных на логическом уровне. Этот метод позволяет извлечь часть файловой системы, что достигается резервным копированием. К сожалению, с его помощью нельзя получить такую важную с точки зрения криминалистики информацию, как электронная почта, базы с геолокационными данными (при этом подобные данные можно извлечь из изображений благодаря EXIF) или кеш приложений.

Далее рассмотрим, как хранятся данные на мобильных устройствах под управлением операционной системы «iOS». Apple использует технологию, именуемую «Data Protection», чтобы защитить данные, хранимые в памяти устройства. При создании нового файла генерируется уникальный 256-битный ключ (File Key), он шифруется так называемым Class Key и хранится в метаданных файла, а те, в свою очередь, шифруются ключом файловой системы (EMF Key), который генерируется на основе UID устройства[1]. Что это значит? Все просто: применение классического файлового картинга не даст никаких результатов, так как все данные в свободной области файловой системы будут зашифрованы. Правда, некоторые исследователи утверждают, что сравнительным анализом файла каталога и журнального файла можно получить информацию об удаленных файлах, включая расположение их метаданных, временные метки и прочее. Таким образом можно восстановить удаленные файлы, найти их ключи и расшифровать их. Но это все теория. И в мире компьютерной криминалистики принято условное правило: физическое извлечение данных с мобильных устройств под управлением операционной системы «iOS» невозможно, пока не будет доказано обратное.

В статье рассмотрены примеры исследования мобильного устройства под управлением операционной системы «iOS» - iPhone 5S с помощью самых распространённых криминалистических программно-аппаратных комплексах.

Стоит отметить, что iPhone 5S, участвующий в эксперименте, был выбран с размером памяти 16 Гб, из которых 10 Гб были отмечены устройством как «Занято».

1. Криминалистическое исследование iPhone 5s с использованием аппаратно-программного комплекса UFED Touch

UFED Touch компании «Cellebrite» – «это устройство для предоставления комплекса решений по обслуживанию мобильных устройств в течение всего срока их службы»[2]. Устройство представляет собой аппаратно-программный комплекс, состоящий из устройства Cellebrite Touch, комплекта data-кабелей для подключения к

мобильным устройствам, блока питания устройства Cellebrite Touch, адаптера Multi-SIM, щетки для очистки разъема передачи данных мобильного устройства.

При изучении правил эксплуатации, полученных на официальном сетевом портале компании «Cellebrite» складывается предположение о том, что UFED Touch позволяет исследовать подключаемые к нему устройства как на логическом, так и на физическом уровне[3], однако при подключении к нему смартфонов iPhone 4S и более новых моделей, с операционной системой IOS 7 и других поздних версий, становится очевидно, что физическое извлечение данных для таких смартфонов невозможно, так как с момента выхода iPhone 4S, Apple использует систему шифрования данных, которая делает невозможным полное извлечение, так называемое – физическое извлечение данных. В связи с этим, при подключении смартфона к Cellebrite Touch, а дисплее аппарата отображаются только два варианта извлечения данных: логическое извлечение и извлечение файловой системы.

Это демонстрирует первый минус работы UFED Touch: невозможность восстановления удаленной информации со смартфонов iPhone 4S и более поздних версий.

Для наиболее полного изучения особенностей извлечения данных с мобильных телефонов было осуществлено и логическое извлечение, и извлечение файловой системы. Создаваемые образы мобильного устройства были сохранены на внешний носитель информации – твердотельный накопитель (далее – SSD).

После успешного окончания процесса, SSD с извлеченными данными был подключен к рабочей станции с заранее установленным программным обеспечением UFED Physical Analyzer 5. Проанализировав полученные результаты, были получены следующие результаты извлечения, которые отмечаются и в логическом извлечении и в извлечении файловой системы: системную информацию о мобильном устройстве (название устройства, версия операционной системы, IMEI, номер телефона); телефонная книга; календарь; заметки; фотоизображения: аудиофайлы; сообщения Imessage; поисковые запросы в браузере (Safari);

Дополнительно для извлечения файловой системы можно выделить: извлечение электронной переписки из программ, детектированных как программы мгновенного обмена сообщениями – "мессенджерами» (Viber, WhatsApp, Telegram); SMS; информация о истории навигации; журнал звонков; сохраненные документы формата .pdf, .docx и т.д.; точки доступа к сети Wifi; логин Apple ID; список используемых приложений для социальных сетей (VK, OK, Instagram)

Демонстрацией второго минуса работы комплекса, является извлечение паролей, так как пароли извлекаются не в явном, а в зашифрованном виде, плюс ко всему количество паролей извлекается ограниченное, например, в образе исследованного мобильного устройства пароль был детектирован только к одной учетной записи в социальной сети VKontakte. Следует отметить, что пароль от учетной записи Apple ID не был детектирован.

Подводя итог исследования UFED Touch, следует отметить, что не все заявленные на официальном сетевом портале возможности реализуются и достаточно криминалистически-важная информация извлекается в нечитабельном виде, либо не извлекается вообще.

2. Криминалистическое исследование iPhone 5s с использованием программного комплекса Oxygen Software

Комплекс Мобильный криминалист версии – Детектив» компании «Oxygen Software» – «программный комплекс для исследования мобильных устройств, извлечения данных из облачных хранилищ и анализа биллингов операторов сотовой связи[4]. Комплекс состоит из программы обработки мобильного устройства «Мобильный криминалист версии – Детектив» и программы просмотра полученных данных с мобильного устройства «Просмотрщик данных»

По заявленным характеристикам на официальном сетевом ресурсе компании «Oxygen Software» рассматриваемый программный комплекс дает возможность извлекать данные из нескольких устройств одновременно. Обходит пароли на блокировку экрана у IOS устройств. Находит пароли к зашифрованным iTunes и Android бекапам, а также образам устройств Android. Имеет встроенный Модуль Извлечения Данных из Облачных Сервисов. Модуль поддерживает следующие службы: Apple (контакты и календари iCloud) и другие. Имеет встроенный Модуль Карт для работы с гео-данными. Модуль автоматически показывает наиболее часто посещаемые пользователем места, строит маршруты передвижения и находит места, в которых одновременно были несколько владельцев устройств[5].

Однако при исследовании смартфона iPhone 5S с помощью данного комплекса можно наблюдать то, что программой «Мобильный криминалист версии – Детектив» были получены сведения о названии устройства, операционной системе и ее версии, IMEI, номере телефона, соединениях по сети Wifi, сохраненных документы формата .pdf, .docx и т.д., календаре, заметках, сделанных устройством фотоизображениях, SMS, журнале звонков, информация из браузера Safari, координаты навигации, аудиозаписях, некоторых социальных сетях («ВКонтакте», «Skype»), мессенджерах Viber, WhatsApp, Telegram. Данный комплекс не предоставил сведения о Apple ID, о времени последней активации

устройства; не обошел пароль на блокировку экрана; не распознал пароли от социальных сетей, не предоставил сведения о наличии некоторого части данных на устройстве (не распознано приложение «Instagram», потовые службы, телефонная книга)

Таким образом, «Мобильный криминалист версии – Детектив» может распознать гораздо больше зашифрованных данных, в отличии от UFED Touch, однако криминалистически важная информация, которая представляет собой пароль к заблокированному устройству, пароли к приложениям, удаленные пользователем данные, не могут быть получены с помощью комплекса программ от Oxygen Software.

3. Криминалистическое исследование iPhone 5s с использованием программного комплекса Magnet.

Программный комплекс Magnet Internet Evidence Finder – это программный комплекс компании «Magnet». Компания, созданная в 2007 году, сделала много разработок программного обеспечения для деятельности компьютерных криминалистов. Для извлечения данных из мобильных устройств были разработаны программы «Magnet Acquire», позволяющую извлекать данные из мобильного устройства и программы «Magnet Internet Evidence Finder» (далее – Magnet IEF), которая используется для просмотра полученных ранее данных.

При проведении исследования программой «Magnet IEF» были получены сведения о названии устройства, сохраненных документах формата .pdf, .docx и др., сделанных устройством фотоизображениях, SMS и Imessage.

По сравнению с UFED Touch и «Мобильный криминалист – Детектив» полученная информация программой «Magnet IEF» содержит предельно малое количество данных. При этом программа «Magnet IEF» является самой затратной с финансовой точки зрения, так как годовая лицензия на этот программный продукт составляет около восьми тысяч долларов (США).

В таблице представлена сравнительная характеристика результатов работы всех рассмотренных комплексов.

Характеристики	«UFED Touch»		«Мобильный криминалист - Детектив»	«Magnet IEF»
	Логическое извлечение	Файловая система		
Название устройства	Есть	Есть	Есть	Есть
ОС, версия	Есть	Есть	Есть	-
IMEI	Есть	Есть	Есть	-

	«UFED Touch»		«Мобильный	
Apple ID	-	-	-	-
Номер телефона	Есть	Есть	Есть	-
Wifi точки	-	-	-	-
Время последней активации	Есть	Есть	-	-
Документы (.pdf .docx ...ect)	-	Есть	Есть	Есть
Телефонная книга	-	Есть	Частично	-
Календарь	Есть	Есть	Есть	-
заметки	Есть	Есть	Есть	-
Фото	-	Есть	Есть	Есть
Приложения	-	-	-	-
Браузер	Есть	Есть	Есть	-
SMS	Частично	Есть	Есть	Есть
Журнал звонков	-	Есть	Есть	-
Навигация	-	Есть	Есть	-
Пароли	-	-	-	-
Аудиозаписи	Есть	Есть	Есть	-
Imessage	-	Есть	Есть	Есть
WhatsApp	-	Есть	Есть	-
Viber	-	Есть	Есть	-
Telegram	-	Есть	Есть	-
VK, Instagram	-	Частично	Частично	-

Заключение

Таким образом, можно сделать вывод, что ни один из существующих аппаратно-программных комплексов, предназначенных для криминалистического исследования мобильных устройств не может исследовать и получить сведения об удаленной информации с устройства и не может обходить пароль на заблокированном экране. Это связано с тем, что мобильные устройства под управлением операционной системой «IOS» являются одними из самых безопасных, благодаря своему алгоритму шифрования данных.

Начиная с версии «iPhone 4S», физическое извлечение данных не может быть выполнено. Из этого следует, что удаленная информация с такого мобильного телефона не

может быть восстановлена. Это крайне усложняет работу следственных органов, так как важная следствию информация может быть удалена за секунду до начала производства следственных действий без возможности восстановления доступными криминалистическими способами – аппаратно-программным обеспечением «UFED Touch», «Мобильный криминалист - Детектив», «Magnet IEF» и др. Единственным способом получить удаленные данные устройств под управлением операционной системы «IOS» является обращение к производителю – компании «Apple». Однако на сегодняшний день известен только один случай взаимодействия правоохранительных органов (Федеральной бюро расследований в США) и компании «Apple» в рамках проведения исследования мобильного телефона «iPhone».

В целях решения данной проблемы, следует заключить соглашение о проведении исследований компании «Apple» и правоохранительными органами. Как отмечали Mattia Epifani и Pasquale Stirparo довольно часто в компанию «Apple» поступают запросы о получении информации из мобильных устройств под управлением операционной системы IOS, однако большинство таких устройств заблокированы пользователем и обычная процедура брутфорса становится недоступной [6]. Все потому, что при десяти неудачных попыток ввода пароля для разблокировки экрана происходит автоматическое удаление данных с устройства (функция реализуется, если пользователь заранее ее активировал). Данная технология и представляет мобильные устройства компании «Apple» как одни из самых «безопасных» в области защиты персональных данных устройств в мире.

Согласно предполагаемому соглашению коммерческая тайна компании не будет оглашена, так как часть исследования «Apple» будет проводить самостоятельно, без участия посторонних лиц. Это будет способствовать раскрытию, расследованию преступлений и привлечет дополнительные финансовые средства в компанию «Apple».

Список литературы

- [1]. Andrew Hoog, Katie Strzempka. iPhone and iOS forensics : investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices. British Library Cataloguing-in-Publication Data, 2011. 309 p.
- [2]. Cellebrite Touch – запрос на покупку. Режим доступа: <http://www.cellebrite.com/ru/Mobile-Lifecycle/Products/cellebrite-touch> (дата обращения 17.10.2017)

- [3]. Правила эксплуатации Cellebrite Touch. Режим доступа:
http://www.cellebrite.com/Media/Default/Files/Lifecycle/RU/Touch-and-Desktop_DataSheet.pdf (дата обращения 19.11.2017)
- [4]. Мобильный криминалист – Детектив. Режим доступа:
<http://www.oxygensoftware.ru/ru/features> (дата обращения 19.04.2017)
- [5]. Модуль "Passware Kit Mobile". Режим доступа:
<http://www.oxygensoftware.ru/ru/features/detective> (дата обращения 19.11.2017)
- [6]. Mattia Epifani, Pasquale Stirparo Learning iOS Forensics Packt Publishing, 2015. 220 p.