Верихова Дарья Петровна
Студентка Российского Государственного Социального университета г.Москва 4 курса факультета Юриспруденция

Verikhova Daria Petrovna
4-year student of the Russian State Social University, Moscow, Faculty of Law

МОБИЛЬНАЯ КРИМИНАЛИСТИКА
MOBILE FORENSICS

Аннотация: Революционный рывок технологий в последние десятилетия значительно упростил решение многих сложных задач, однако, данный процесс породил и целый ряд негативных воздействий, как на общество, так и на государство. Намеренные действия, совершенные с использованием компьютерных, мобильных и сетевых технологий, стали обыденностью

Ключевые слова: мобильная криминалистика, компьютерная криминалистика, iOS.

Absrtacts: The revolutionary leap of technology in recent decades has significantly simplified the solution of many complex tasks, however, this process has also generated a number of negative impacts on both society and the state. Deliberate actions committed using computer, mobile, and network technologies have become commonplace

Key words: mobile forensic, computer forensic, iOS.

Криминалистическая экспертиза мобильных устройств как область исследований датируется концом 1990-х - началом 2000-х годов. Роль мобильных телефонов в преступлении давно признана правоохранительными органами. С увеличением доступности таких устройств на потребительском рынке и расширением спектра поддерживаемых ими коммуникационных платформ (например, электронная почта, просмотр веб-страниц) спрос на судебно-медицинскую экспертизу вырос. Ранние попытки исследовать

мобильные устройства использовали методы, аналогичные первым компьютерным криминалистическим исследованиям: анализ содержимого телефона непосредственно через экран и фотографирование важного содержимого. Однако это оказалось трудоемким процессом, и по мере того, как количество мобильных устройств начало расти, исследователи потребовали более эффективных средств извлечения данных. Предприимчивые мобильные судебно-медицинские эксперты иногда использовали программное обеспечение для синхронизации сотовых телефонов или КПК для «резервного копирования» данных устройства на судебно-медицинский компьютер для визуализации, а иногда просто выполняли компьютерную экспертизу на жестком диске подозрительного компьютера, на котором данные были синхронизированы. Однако программное обеспечение этого типа могло писать в телефон, а также читать его, и не могло восстанавливать удаленные данные. Некоторые судебно-медицинские эксперты обнаружили, что они могут извлекать даже удаленные данные с помощью «флешеров» или «твистеров», инструментов, разработанных OEM-производителями для «прошивки» памяти телефона для отладки или обновления. Тем не менее, флешеры инвазивны и могут изменять данные; может быть сложно использовать; и, поскольку они не разработаны как инструменты судебной экспертизы, не выполняют ни хеш-проверок, ни (в большинстве случаев) контрольных журналов. Следовательно, для судебно-медицинских экспертиз оставались необходимы лучшие альтернативы. Чтобы удовлетворить эти требования, появились коммерческие инструменты, позволяющие исследователям восстанавливать память телефона с минимальными нарушениями и анализировать ее отдельно. Со временем эти коммерческие методы получили дальнейшее развитие, и восстановление удаленных данных с проприетарных мобильных устройств стало возможным с помощью некоторых специализированных инструментов. Более того, коммерческие инструменты даже автоматизировали большую часть процесса извлечения, что позволяет даже минимально обученным службам быстрого реагирования - которые в настоящее время гораздо чаще сталкиваются с подозреваемыми с мобильными устройствами в их распоряжении, чем с компьютерами - выполнять базовые извлечения для сортировки и сортировки. в целях предварительного просмотра данных.

В докладе правительству РФ о деятельности прокуратуры за 2019 год генеральный прокурор Юрий Чайка отметил, что есть проблемы с противодействием киберпреступности. Он отмечает резкий рост преступлений, совершенных с помощью использованием IT-технологий, и

крайне малый процент их раскрываемости. За прошедший год было раскрыто всего 8 % мошеннических действий. На данный момент Уголовный кодекс Российской Федерации содержит четыре состава преступлений в сфере компьютерной информации – статьи 272, 273, 274, 274.1 главы 2. Данная глава называется «Преступления в сфере компьютерной информации». Термин «компьютерные преступления» является более широким и обобщенным, так как включает в себя также такие преступления, как кардинг, социальную инженерию, промышленный шпионаж и т. д. Развитие технологий в вопросах совершения преступления и противодействия ему является обоюдоострым оружием. С одной стороны, с развитием технологий появляется возможность совершать злонамеренные действия с использованием новых орудий преступления, с другой, появляются дополнительные возможности раскрытия преступлений. Кроме того, развитие технологий порождает новые общественные отношения, которые могут являться предметом посягательств со стороны злоумышленника.

В связи со сложившейся обстановкой остро стоит вопрос расследования преступлений, совершаемых в IT-сфере. Подобные преступления отличаются от классического мошенничества или преступления, совершенного с причинением вреда здоровью или посягательства на жизнь. Эксперты-криминалисты могут обнаружить улики подобных преступлений и впоследствии предоставить в качестве доказательств в суде. Проблема при доказательстве преступлений, отнесенных к сфере компьютерной информации, заключается в том, что доказательством подобных преступлений является информация (следы, оставленные злоумышленником при совершении преступления), хранящаяся на компьютерах, мобильных и сетевых устройствах. Такую информацию очень просто уничтожить, как намеренно, так и случайно, или подделать. Суть проблемы в том, что такие доказательства невозможно воспринимать напрямую органами чувств человека. Из вышесказанного следует, что задача компьютерной криминалистики заключается в получении, документировании и представлении доказательств на судебных заседаниях, а также в сохранении неизменности получаемой информации. Компьютерная криминалистика является прикладной наукой о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации, о применяемых для этого технических средствах.

В настоящее время существует более общий термин «цифровая криминалистика», она включает в себя компьютерную, мобильную и сетевую криминалистику.

Предметом рассмотрения данной статьи была выбрана мобильная криминалистика. Она имеет три направления: исследование устройств, функционирующих на базе операционных систем iOS, Android и BlackBerry.

Существует довольно много инструментов для работы с мобильными устройствами, как «open source» решения, так и коммерческие продукты, часть из них доступна только для покупки, найти подобные программные продукты в сети Интернет не представляется возможным. Далее приведены наиболее популярные программные продукты. Libimobiledevice – кроссплатформенная программная библиотека, использующая протоколы iPhone, iPod Touch, iPad и AppleTV для связи с этими устройствами. В отличие от других проектов она не зависит от существующих программных библиотек и не требует получение полного доступа к файловой системе (jailbreak) устройства. Также она включает другое программное обеспечение для легкого доступа к файловой системе устройств получения информации об устройстве, органах управления, резервных копиях устройства, управления установленными приложениями, пересылки контактов, календарей, заметок и закладок и синхронизации музыки и видео. Данная библиотека развивается с августа 2007 года, ее цель – поддержка i–устройств операционными системами семейства Linux. Для исследования устройств на базе iOS используется Elcomsoft Ios Forensic Toolkit. Это – специализированный продукт для криминалистического исследования устройств на основе Apple iOS. iOS Forensic Toolkit позволяет экспертам правоохранительных органов производить сбор информации и проводить судебные и компьютерно-технические экспертизы устройств iPhone, iPad и iPod производства компании Apple, работающих под управлением iOS версий с 3 по 11. С помощью iOS Forensic Toolkit возможно получить полный доступ к информации, хранящейся в поддерживаемых устройствах. Продукт обеспечивает целостность и неизменность исследуемых данных. С помощью iOS Forensic Toolkit специалисты могут получить доступ к расшифрованному образу файловой системы устройства, расшифровать коды, пароли и прочую защищенную информацию. Доступ к основному массиву данных осуществляется мгновенно, в реальном времени.

Главный недостаток данного программного продукта заключается в том, что он не имеет демонстрационных версий, и при этом его цена довольно высока. Еще один мощный инструмент для проведения криминалистической экспертизы любого устройства – MOBILedit Forensic Express. Этот продукт служит для извлечения данных, как из самого устройства, так и из облака, имеет функционал анализатора данных и генерирует отчеты. Все эти функции являются частью единого решения.

MOBILedit Forensic Express – мощный 64–битный инструмент, использующий физическое и логическое извлечение данных. К достоинствам данного продукта можно отнести возможность работать с устройствами, функционирующими под управлением разных операционных систем, и возможность работать в интеграции с другими продуктами и решениями компании Compelson. Этот программный продукт является прямым конкурентом Elcomsoft iOS Forensic Toolkit, имеет ту же модель распространения, т. е. не имеет демонстрационных версий.

Исходя из того, что наиболее доступным инструментом является

libimobiledevice, воспользуемся им чтобы продемонстрировать наглядно работу мобильного криминалиста. В качестве устройства для тестов был выбран iPhone 4s, использующий операционную систему iOS версии 8.4.1. В качестве операционной системы, используемой в работе, выступает BackBox Linux – свободно распространяемая ОС для «этичного хакинга».

Устройства под управлением операционной системы iOS имеют файловую систему HFSX. HFSX – файловая система, разработанная Apple Inc в качестве замены HFS – Hierarchical File System («иерархическая файловая система»), являющейся главной файловой системой, используемой на компьютерах Mac.

HFSX является почти полной копией HFS+, их различие состоит в том что первая позволяет работать в режиме с учетом регистра имен. Если речь идет о восстановлении данных из HFS или HFS+, используется метод карвинга. Большинство карверов восстанавливают данные, опираясь на заголовки и расширения. Проблема состоит в том, что Apple для защиты данных на своих устройствах использует технологию Data Protection. 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. Вследствие этого, мы имеем данные в свободной области устройства, но не можем их прочитать, так как они зашифрованы. Для извлечения данных из устройств на базе iOS существует три основных метода.

1 Извлечение данных на логическом уровне. С помощью резервного копирования извлекается часть файловой системы. Недостаток этого метода в том, что невозможно получить такую информацию, как электронная почта, базы данных геолокации, кэш приложений, а часто именно она является важной с точки зрения криминалистики.

2 Извлечение на уровне файловой системы. Данный метод позволяет извлечь все данные, видимые на уровне операционной системы,

однако, нет возможности восстановить удаленные файлы, кроме баз данных SQLite и миниатюр удаленных изображений.

3 Извлечение на физическом уровне (физическое извлечение). Данный метод является наиболее эффективным и позволяет извлечь максимальное количество данных, в том числе и удаленных. Для осуществления этого метода, необходим jailbreak устройства.

Приступая к исследованию устройства, сначала необходимо его идентифицировать. Делается это для того, чтобы можно было представить строго за документированные доказательства в суде.

Значение мобильной криминалистики в наши дни трудно переоценить.

Рассмотрев в данной работе методы извлечения данных из устройства на базе iOS и убедившись, что даже будучи ограниченным в методах и средствах, специалист по мобильной криминалистике может извлечь данные, которые впоследствии будут использоваться как доказательства вины или же невиновности. Однако рассмотренный эксперимент демонстрирует только возможным, доступным экспертам-криминалистам.

Библиография:

1. Генпрокурор указал на проблемы с киберпреступностью [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/blog/company/CABIS/341493.php.
2. Федотов Н.Н. Форензика – компьютерная криминалистика
3. Компьютерная криминалистика (форензика) – обзор инструментария и трениро- [Электронный ресурс] – Режим https://habrahabr.ru/company/pentestit/blog/327740/.
4. Криминалистический анализ устройств iPhone/iPad/iPod на основе Apple iOS [Электронный ресурс] – Режим доступа: https://www.elcomsoft.ru/eift.html.
5. Гоголь А.А., Никодимов И.Ю. ОЧЕРКИ ИСТОРИИ РАЗВИТИЯ СВЯЗИ В РОССИИ Санкт-Петербург, 1999. Сер. «Телекоммуникации России: прошлое, настоящее, будущее».

6. Никодимов И.Ю., Морева В.Д. ИСПОЛЬЗОВАНИЕ МЕССЕНДЖЕРОВ ПРИ ПЛАНИРОВАНИИ ТЕРРОРИСТИЧЕСКИХ АКТОВ В сборнике: Проблемы назначения и исполнения наказания и мер уголовно-правового характера. Сборник статей. Под редакцией В.Ю. Голубовского. Москва, 2018. С. 63-67
7. Ильченко Е.А., Никодимов И.Ю. МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В сборнике: УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ И НАКАЗАНИЕ.ОПЫТ РОССИИ И ЗАРУБЕЖНЫХ СТРАН. сборник статей по материалам научно-практической конференции. 2019. С. 77-85.
8. Никодимов И.Ю., Мансырев М.П., Пономарев С.П. ПЛАНИРОВАНИЕ СЕТИ GSM Электросвязь. 2000. № 3. С. 10
9. Никодимов И.Ю., Бучнев Д.Н. ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬНОЙ БАЗЫ И ПРАКТИКИ РЕГУЛИРОВАНИЯ ОПЕРАТОРСКОЙ ДЕЯТЕЛЬНОСТИ Мобильные системы. 1999. № 8. С. 11.
10. Гоголь А.А., Никодимов И.Ю. НОВЫЙ ЭТАП РАЗВИТИЯ ОТРАСЛИ СВЯЗИ: ЗАРОЖДЕНИЕ И РАЗВИТИЕ СОТОВОЙ СВЯЗИ Санкт-Петербург, 2000. Сер. Телекоммуникации России: прошлое, настоящее, будущее (2-е издание, исправленное и дополненное)