Хуртин Тимофей Игоревич
курсант
ФГКОУ ВО «Московская академия
Следственного комитета Российской Федерации»
г. Москва

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ОБНАРУЖЕНИЯ ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЙ НА СМАРТФОНЕ ВИЗУАЛЬНЫМ СПОСОБОМ

Аннотация: *в статье освящены особенности, связанные с обнаружением цифровых следов преступления на смартфоне. Автором изучена сущность смартфона и его операционных систем. Рассмотрена классификация способов обнаружения цифровых следов преступления на смартфоне. Автором предложен универсальный тактический комплекс по обнаружению данных следов и описан, опираясь на практический опыт правоохранительных органов.*

Ключевые слова*: цифровая криминалистика, цифровые следы, собирание доказательств, криминалистически значимая информация.*

На данный момент преступления, совершенные с использованием информационно-телекоммуникационных средств и компьютерных сетей, являются наиболее актуальной проблемой в сфере уголовного судопроизводства, поскольку доказательственная база по данным уголовным делам состоит почти исключительно из цифровых следов, оставленных преступником на определенных носителях информации, в том числе и на смартфоне.

Смартфон – мобильный телефон, обладающий широким спектром функциональности – является одним из самых технически сложных видов носителей информации, который может содержать криминалистически значимую информацию. Остается проблематичным выделить основную общую тактику собирания цифровых следов преступления со смартфонов, поскольку для каждой операционной системы смартфона нужен индивидуальный подход, так как каждая из них уникальна по своей структуре [1].

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

В данный момент, исходя из действующей практики правоохранительных органов, целесообразно классифицировать поиск и обнаружение цифровых следов преступления на следующие способы:

− собственноручный, или же визуальный, в ходе которого самостоятельно, без использования тех или иных технических средств, производится осмотр хранящихся на смартфоне данных путем наблюдения и описания;

− с помощью технико-криминалистических средств, которые непосредственно предназначены для узкой направленности – собиранию цифровых следов преступления («Мобильный криминалист», «UFED», «XRY» и другие);

− с помощью специальных программных обеспечений, разработанных частными лицами – «энтузиастами» в сфере IT-технологий (например, различного рода «чекеры» (от англ. checker – проверяющий) – онлайн-сервисы или программные обеспечения, предназначенные для проверки оставленных цифровых следов в сети «Интернет» или на определенных операционных системах).

Исходя из особенностей строения операционной системы смартфона и действительных на данный момент инструментов, практично выделить универсальный тактический комплекс по обнаружению цифровых следов преступления, который охватывает общие аспекты данной деятельности. Следовательно, уместно поделить осмотр смартфона на:

1) этап осмотра данных, которые непосредственно передаются, хранятся и обрабатываются с помощью штатных механизмов операционной системы;

2) этап осмотра данных, которые непосредственно передаются, хранятся и обрабатываются с помощью иных механизмов, которые не предусмотрены операционной системой смартфона;

Первый этап подразумевает собой использование инструментов и механизмов, встроенные изначально в операционную систему. Так, с помощью собственноручного способа позволительно осмотреть приложения, находящиеся и предусмотренные операционной системой смартфона. В основном, к ним относятся следующие приложения:

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

− приложение для просмотра и упорядочивания контактных мобильных номеров, представляющуюся контактной книжкой («*Контакты*»), непосредственно связанная с сим-картой владельца, которая содержит сохраненные номера мобильных телефонов и историю исходящих и входящих телефонных звонков с данного устройства, с помощью которой можно не только установить факт связанности того или иного записанного контакта с преступником, чтобы в будущем с помощью процессуальных действий раскрыть владельцев мобильных номеров [2], но и выявить все недавние взаимодействия преступника с другими абонентами связи, в том числе путем получения информации о соединениях между абонентами и (или) абонентскими устройствами, предусмотренной ст. 186.1 УПК РФ [3];

− приложение для просмотра, упорядочивания и управления изображениями, фотографиями и видеозаписями («*Галерея*»), содержание которой может иметь существенное значение для целей расследования преступлений, так как субъекты преступления могут использовать фото- и видеофиксацию своих действий, издевательств над жертвами и т.д; кроме непосредственного содержания фотоснимков (наличия на них определенных лиц, местности, зданий и сооружений, иных элементов обстановки), криминалистическое значение может иметь дополнительная информация, отмеченная на кадре: дата и время съемки, геотеги и т. д.; в свойствах файла фотографии также имеется информация о времени и дате съемки, а во многих случаях – о дополнительных параметрах съемки: диафрагма, выдержка, уровень светочувствительности (ISO), применение вспышки, фильтров и тому подобное [4];

− приложение для хранения, обработки и просмотра различного формата файлов («*Файлы*»), на которых могут находится документы (форматов: DOC, DOCX, JPEG, PNG, XLS, SCV, PPT, TXT, RTF, PDF, TIFF и др.); требует особо пристального внимания, поскольку существуют много способов «спрятать» файл, имеющий криминалистически значимую информацию, например, текстовый файл в формате изображения, закодировав сам текст в содержимом файла изображения;

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

− приложение для выхода в сеть «Интернет» («*Браузер*»), в котором сохраняется информация о последних открытых страницах, поисковых запросах, закладках.

− и иные приложения, по типу заметок, геолокаторов, входящих и исходящих SMS-писем и т. д.

Кроме приложений, операционная система предлагает нам функцию просмотров лог-файлов смартфона. Лог-файлы – это файлы, в которых записываются различные события и действия, происходящие на устройстве. Они могут содержать информацию о процессах, ошибках, предупреждениях и других событиях, происходящих как на уровне операционной системы, так и на уровне приложений.

Лог-файлы часто содержат детальную информацию, такую как дату и время события, уровень важности события, текстовое описание происходящего и другие подробности. Они могут быть полезными как для решения проблем с устройством, анализа производительности, так и для получения криминалистически значимой информации [5].

Выделяется несколько способов работы с лог-файлами:

− использование специальных программ непосредственно встроенные на смартфоне;

− подключение к компьютеру, чтобы просмотреть содержимое папки лог-файлов самостоятельно, либо с помощью программного обеспечения для компьютера, например – ADB (Android Debug Bridge) – инструмента для взаимодействия с устройством через командную строку компьютера;

− анализ стандартных лог-файлов устройства – чтобы получить доступ к логам, нужно зайти в настройки устройства, найти раздел «О телефоне» или «О устройстве» и нажать на пункт «Версия Android» несколько раз подряд, после этого станет доступен раздел «Разработчик», где можно включить режим отладки и просмотреть стандартные лог файлы.

Второй этап подразумевает осмотр приложений, установленных владельцем из иных источников – в общем, к ним можно отнести социальные сети и мессенджеры, а также клиенты электронной почты и другие приложения для связи.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Цифровые следы преступления в мессенджерах и социальных сетях могут включать различные виды данных и информации, которые могут быть использованы в ходе расследования преступления. Самые важные из них:

− сообщения (текстовые сообщения, которые могут содержать угрозы, шантаж, мошенничество или другие преступные действия; фотографии и видео, которые могут служить доказательствами преступлений (например, кибербуллинг, распространение порнографии; голосовые сообщения, которые могут содержать признания или другие важные сведения);

− метаданные (время и дата отправки сообщений; геолокация (если включена), которая может помочь установить местоположение преступника; IP-адреса и другие технические данные, которые могут быть использованы для идентификации устройства);

− группы и каналы (участие в группах и каналах, которые могут быть связаны с преступной деятельностью; сообщения и файлы, обмененные в этих группах);

− профиль пользователя (имя и фамилия, которые могут быть использованы для идентификации подозреваемого, фотографии профиля и обложки, которые могут служить доказательствами, биографическая информация, которая может содержать важные сведения о подозреваемом);

− и так далее.

На самом деле, перечень данных приложений не является исчерпываемым, так как в настоящий момент приложения, которые имеют функции хранения, обработки и передачи информации, появляются ежедневно.

Вывод напрашивается очевидный – смартфон в умелых преступных руках будет являться некой «песочницей», в которой нетрудно имеется возможность спрятать криминалистически значимую информацию различными, неочевидными способами. И вся ответственность по решению данных задач будет ложиться на обычного, рядового следователя.

Список литературы

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

1. Полякова М.А. Оценки операционных систем смартфонов / М.А. Полякова, Ю.В. Кузнецова, В.Е. Герасимова // Актуальные проблемы авиации и космонавтики. – 2012. – Т. 2, №8. – С. 57–58. EDN TAPLTP

2. Casadei F. Savoldi A., Gubian P. Forensics and SIM cards: an overview / F. Casadei, A. Savoldi, P. Gubian // International Journal of Digital Evidence. – 2006. – Т. 5, №1.

3. Уголовно-процессуальный кодекс Российской Федерации: федеральный закон от 18.12.2001 №174-ФЗ.

4. Смушкин А.Б. Криминалистическое исследование мобильных устройств / А.Б. Смушкин // Электронное приложение к Российскому юридическому журналу. – 2020. – №2. – С. 48–52. DOI 10.34076/2219-6838-2020-2-48-52. EDN YILTLI

5. Кутыев А.Т. Среда имитационного моделирования генерации лог-файлов при мониторинге событий / А.Т. Кутыев, Я.А. Бекенева // Известия СПбГЭТУ ЛЭТИ. – 2022. – №1. – С. 14–21. DOI 10.32603/2071-8985-2022-15-1-14-21. EDN TFZBUG

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)