IV Международный конкурс исследовательских работ школьников "Research start" 2020/2021

Цифровой след

Выполнила:
КОТЕНКОВА ЮЛИЯ АЛЕКСАНДРОВНА,
10 «д» класса

Научный руководитель:
учитель информатики
ДОРОНИН ИВАН АЛЕКСЕЕВИЧ

Дмитров, 2021 год

Содержание

Введение

В последние четыре года я написала несколько проектов об уникальных особенностях человека. Это были «Следы пальцев рук», «Почерк человека», «Человеческая ложь» «Запах, как главная улика». Темы очень разнообразные, но все они были связаны с работой следователя и эксперта, чья деятельность доставляет мне большой интерес. Задумываясь об очередной работе, я решила продолжить изучать тему следов человека, которые используют в расследованиях.

В 21 веке повсеместно внедряются информационные технологии, поэтому человек становится активным участником их применения, как в профессиональной, так и в повседневной деятельности.

Все больше потребность в общении между людьми удовлетворяется с помощью специальных технических средств и методов, среди которых сотовая связь, социальные сети, различные интернет ресурсы, используемые посредством мобильных телефонов, смартфонов, планшетов, компьютеров.

Распространение сотовой связи, как в нашей стране, так и во всем мире, привело к тому, что в настоящее время простой мобильный телефон или смартфон (англ. smartphone — умный телефон) имеется практически у каждого взрослого человека и даже ребенка.

По данным на 2019 год 59 % людей в России используют смартфоны, порядка 33 % - мобильные телефоны и лишь 8 % граждан не имеют ни того ни другого. При этом многие имеют по несколько мобильных устройств.

Так или иначе процесс использования человеком названных технических средств оставляет следы, но не биологические, а цифровые. Эти следы могут длительное время храниться, копироваться, использоваться, в том числе при раскрытии и расследовании преступлений.

Мне стало интересно, где и как найти цифровой след? Какие средства для этого используют следователи и эксперты? Что помогает установить цифровой след?

При подготовке к проекту я посетила криминалистическое подразделение Следственного комитета Российской Федерации, где нашла ответы на возникшие вопросы.

Цель работы:

Узнать, что такое цифровые следы, где и с помощью чего их можно обнаружить, как используют их следователи в своей работе.

Задачи проекта:

- Собрать и изучить материал о цифровом следе;
- Научиться обнаруживать цифровые следы в смартфонах и мобильных телефонах;
- Предостеречь ребят от плохих поступков.

1. Понятие цифрового следа и его особенности

В интернет-энциклопедии Википедия **Цифровой след** (или цифровой отпечаток; англ. digital footprint) — это уникальный набор действий в интернете или на цифровых устройствах. Во всемирной паутине можно найти также понятия «интернет-след», «кибер-тень», «электронный след» или «цифровая тень», — это информация, оставленная в результате просмотра веб-страниц и сохраненная в виде куков. Термин обычно применяется к одному пользователю, но может также относиться к какой-либо организации.

В литературе учеными-криминалистами Введенской О.Ю., Веховым В.Б., Александровой И.В. даются разные определения следов, зафиксированных в виртуальном пространстве. Используют такие понятия, как цифровые следы[1], виртуальные следы[2], электронные следы[3], компьютерно-технические следы.

Например, Смушкин А.Б. определяет, что электронные или виртуальные следы представляют собой следы совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей[4].

---

[1] Александрова И.В. Криминалистика: учебник для бакалавриата и магистратуры // И.В. Александрова. М.: Юрайт. 2016. С. 169-170.

[2] Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. № 4 (34). С. 209-216.

[3] Вехов В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, Б. П. Смагоринский, С. А. Ковалев // Судебная экспертиза. Волгоград. 2016. Вып. 2. С. 94-98. 127 с.

[4] Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43

Наиболее верным, на наш взгляд, является следующее определение цифрового следа – это информация о **деятельности человека в виртуальном пространстве и на электронно-цифровых устройствах**.

Такая информация представлена в форме электрических сигналов, содержащаяся на материальных источниках и обнаруженная посредством программно-технических устройств.

Цифровые следы можно классифицировать по принадлежности носителя:

- локальные, т.е. расположенные на техническом устройстве человека;

- сетевые, т.е. расположенные на серверах и коммуникационном оборудовании.

Локальные следы в свою очередь можно классифицировать по носителю, на котором они расположены на:

- следы на винчестере (жестком диске), стримере (магнитной ленте), оптическом диске, дискете, карте памяти и пр.;

- следы в оперативных запоминающих устройствах компьютера, смартфона, телефона;

- следы в оперативных запоминающих устройствах периферийного оборудования (принтеры, сканеры и т. д.);

- следы в оперативных запоминающих устройствах компьютерного оборудования связи и сетевого оборудования;

- следы в проводных, радиооптических и других электромагнитных системах и сетях связи.

Кроме того, цифровые следы по способу следообразования могут быть: активные и пассивные.

Активный цифровой след появляется, когда пользователь намеренно публикует свои персональные данные, чтобы рассказать о себе на веб-сайтах и в социальных медиа, специально создает записи, размещает фото, видео в мобильном устройстве. Их еще называют первичными следами, которые являются следствием непосредственного воздействия человека с использованием какой–либо информационной технологии.

Пассивный цифровой след — это данные, которые фиксируются в памяти устройства, либо на сервере независимо от воли человека. Их также называют вторичными следами, образующимися после появления активных следов, в результате воздействия технологических процессов без участия человека и вне его желания.

Важным **свойством цифрового следа** является невозможность его восприятия непосредственно органами чувств человека. Его обнаружить, зафиксировать и сохранить возможно только с помощью специальных устройств и программ.

Помимо применения в работе правоохранительных органов, цифровые следы широко используются в иных сферах деятельности. Так, цифровые следы используют для определения интернет-активности человека. Кроме того, изучение цифровых следов маркетологам помогает узнать, какие продукты или товары интересуют пользователя и повысить уровень продаж.

Социальные сети записывают действия и информацию о пользователях, что позволяет изучать интересы человека, социальных групп, поведение и местоположение пользователей. Многие социальные сети, собирают большой объем информации, которую можно использовать, чтобы узнать личность пользователя, его характер, психологический портрет, увлечения. Цифровой след возможно использовать без ведома его владельца, чтобы узнать его демографические характеристики, религиозные и политические взгляды, умственные способности. Например, это может иметь

значение при изучении кандидата для трудоустройства в организацию или поступлении в некоторые учебные заведения.

Поэтому школьники должны учитывать значение своего цифрового следа и возможное использование этой информации на разных этапах их жизни.

В работе следователя цифровые следы играют огромную роль, поскольку полученная с помощью них информация помогает:

- раскрывать преступления, то есть устанавливать виновных лиц, цели и мотивы преступления;

- формировать доказательства причастности или непричастности человека к совершению противоправного деяния;

- дает возможность устанавливать свидетелей преступления;

- может указывать на места сокрытия предметов и иных следов преступления.

Где же необходимо искать цифровые следы?

Субъекты преступной деятельности зачастую используют сотовую связь при подготовке, совершении и сокрытии преступлений, либо электронное мобильное устройство, которое находится при таком лице и автоматически регистрируется относительно базовых станций, точек сети WiFi, оснащено глобальной навигационной системой (ГЛОНАСС), что позволяет определить следователю координаты местоположения технического средства.

Преступники порой завладевают мобильными устройствами потерпевших, пользуются, либо уничтожают их, некоторое время передвигаются вместе с потерпевшим, что безусловно способствует установлению координат и времени нахождения таких устройств. Часто

подозреваемые пользуются транспортными средствами, в которых установлены навигаторы, оборудованные приемными и передающими модулями систем GPS, видеорегистраторы, работающие порой в постоянном режиме видеосъёмки, аналогичными устройствами могут быть оснащены автомобили потерпевшего или свидетеля.

Повсеместное использование электронной почты, программ мгновенного обмена сообщениями, переписки в социальных сетях, просмотры рекламных и иных сайтов, поиск необходимого товара, покупка через интернет-магазин, раскрывает для криминалистов новые возможности поиска цифровых следов в мобильных устройствах, компьютерах, в интернет-пространстве.

Информация о преступном событии порой фиксируется на цифровые устройства помимо воли лиц, его совершающих. Поэтому такая информация, хранящаяся в памяти данных устройств, может иметь для следователя важное доказательственное или ориентирующее значение. В связи с этим актуален вопрос, связанный с обнаружением, фиксацией, изъятием и исследованием информации, содержащейся в памяти таких устройств (дампы оперативной памяти и дампы трафиков, файлы и их обрывки, служебная информация об этих файлах, располагающаяся на материальных носителях информация в виде кодированных последовательностей и пр.)

Безусловно самым простым и распространенным способом раскрытия и расследования преступлений по цифровым следам является изъятие у физических или юридических лиц видеосъёмки тех или иных участков местности, помещений, зданий, сооружений и жилищ. Известно, что в крупных населенных пунктах остается все меньше территорий, не охваченных постоянной видеосъемкой. “Обстановка, зафиксированная видеокамерами, может и должна использоваться для получения значимой информации в процессе раскрытия и расследования преступлений о лицах, подлежащих привлечению к уголовной ответственности; механизме

совершения преступления; очевидцах преступления; местах нахождения лиц (автомобилей) в определенное время в конкретном месте; маршрутах подхода (отхода) к месту совершения преступления; иных обстоятельствах, имеющих значение для расследования преступлений”[5].

Еще одним перспективным направлением получения цифровых следов является возможность использования данных информационных спутниковых систем (далее – ИСС) при расследовании преступлений. В частности, таковыми являются фотоснимки, полученные при космическом дистанционном зондировании земли. Эти снимки, полученные из архива за прошлые годы, важны при расследовании незаконной организации мусорных полигонов, незаконном строительстве и др.

Электронные носители информации высокотехнологичны и для работы с ними лучше привлекать специалиста или эксперта, так как внешнего осмотра материальных носителей для получение нужной информации иногда недостаточно, такая информация может быть тщательно скрыта либо удалена.

Таким образом, у следствия есть несколько направлений работы с цифровыми следами независимо от вида и категории совершенного преступления:

1. Определение координат местоположения технического средства человека (сотовый телефон, смартфон, навигатор, часы, планшетный компьютер и т.п.) оборудованного приемными и передающими модулями систем GPS, ГЛОНАСС, по беспроводным сетям WiFi и по базовым станциям сотовой связи.
2. Извлечение и анализ полных данных о контактах, переписке, видео и аудио файлах, имеющихся в мобильном устройстве (в

[5] Дмитриев Е.Г., Котенков А.В. О некоторых особенностях использования информации систем видеонаблюдения в ходе расследования преступлений. Журнал «Российский следователь». 2013 № 1. С. 5

том числе удаленных), либо в компьютере или интернет пространстве, с помощью специальных программных средств.

3. Получение и осмотр видеосъёмки автомобильных регистраторов, видеокамер наружного наблюдения, спутниковых систем, в частности, фотоснимков, полученных при космическом зондировании земной поверхности.

Как уже было мною отмечено во введении, самыми распространенными техническими устройствами, используемыми людьми, являются мобильный телефон и смартфон, услуги сотовой связи очень востребованы в современном обществе.

На этом направлении поиска цифровых следов необходимо остановиться подробнее.

2. Принцип работы сотовой связи и мобильных устройств

Зная принципы работы сотовой связи и мобильных устройств, следователь может эффективно использовать криминалистически значимую информацию – цифровые следы, чтобы успешно раскрывать и расследовать любые преступления.

При этом важно то, что информация о преступном событии порой фиксируется на данные устройства помимо воли лиц, его совершающих (пассивные цифровые следы). Люди пользуются телефонами постоянно, как правило, не расстаются с ними, а их многофункциональность и постоянное совершенствование только расширяет пользовательские и, соответственно, криминалистические возможности.

К ним уже относится не только обычная телефонная связь - голосовая коммуникация и SMS-переписка, но и мобильный интернет: мессенджеры (системы мгновенного обмена сообщениями), социальные сети («ВКонтакте», Instagram, «Одноклассники», Facebook, Twitter), электронная почта и др. Смартфоны используют в качестве фото- видеокамеры, навигатора, шагометра, пульсометра, компаса, портативной точки доступа WI-FI для раздачи интернета, ими с помощью функции «near field communication» (NFC) оплачивают проезд в транспорте, покупки в магазинах и т.д.

Полезно знать, что же такое сотовая связь и как она работает (**Приложение 1**).

Основными элементами системы сотовой связи являются базовые станции – вышки с антеннами и мобильные радиотелефонные аппараты. Общая зона покрытия связью делится на ячейки (соты), которые являются зонами покрытия отдельных базовых станций. Все соты частично перекрываются между собой и вместе образуют сеть.

Зона покрытия каждой базовой станции напоминает шестиугольник - соту, поэтому и назвали связь сотовой.

Базовые станции с помощью антенн соединяются с мобильным телефоном и между собой, поэтому передают радиосигнал на большие расстояния к другому устройству. Таким образом обеспечивают связь между абонентами.

Базовые станции принадлежат компаниям (операторам) сотовой связи. Каждый факт соединения мобильного телефона или смартфона с базовой станцией, фиксируется и сохраняется в центре коммутации **оператора сотовой связи** на специальном оборудовании в течение 3 лет.

Соединение мобильного устройства с базовой станцией происходит при его включении и использовании (регистрация телефона в сети, посылка и прием вызова, отправка и получение смс сообщений, выход в интернет).

При этом, одной из технических особенностей работы радиотелефона в сотовой сети является его обязательное использование для установления и поддержания соединения специального модуля **SIM-карты** (СИМ-карты) Сим-карта имеет номер, который мы привыкли называть номером мобильного телефона. При продаже сим-карта регистрируется на конкретного человека – абонента сотовой связи (**Приложение 2**).

Помимо этого, каждый аппарат мобильной связи имеет свой уникальный номер - **IMEI (International Mobile Equipment Identity)** - «Международный идентификатор мобильного оборудования». Этот номер устанавливается на заводе при изготовлении, служит для идентификации устройства в GSM сети. Число IMEI обычно можно прочитать на специальной табличке, расположенной под аккумуляторной батареей, а также определить (у большинства аппаратов), введя на клавиатуре следующий код: *#06#. Код IMEI содержит 15 цифр (**Приложение 3**).

При любом соединении мобильного устройства с базовой станцией регистрируется номер сим-карты и уникальный номер телефона IMEI.

При каждом состоявшемся сеансе связи на коммутационном оборудовании оператора фиксируется определенный набор информации. Эту информацию принято называть **биллингом** или детализацией телефонных переговоров. Для оператора сотовой связи биллинг нужен, чтобы осуществлять расчеты с абонентом за предоставленные услуги связи, а следователю он позволяет устанавливать важные события при расследовании преступлений.

3. Работа с биллинговой информацией.

Следователь может получить биллинг у оператора сотовой связи по судебному решению, в котором будут указаны номер сим-карты или IMEI мобильного устройства интересующего человека.

(Общий вид биллинговой информации в **Приложении 4**).

В полученном биллинге следователь увидит данные о следующем:

- с кем связывался абонент, номер мобильного устройства собеседника;

- время совершения звонка (отправки или получения смс сообщения), длительность разговора;

- номер или адрес базовой станции, обеспечивающей связь.

- иную техническую информацию.

В данном случае **биллинг является цифровым следом**, относящимся по нашей классификации к **пассивному сетевому следу**.

Биллинг, или как его называют юридическим языком – информация о соединениях между абонентами или абонентскими устройствами, возможно истребовать за прошедший период от одного дня для до трех лет.

При осмотре полученного биллинга по адресу базовой станции можно установить место, где человек находился в конкретное время или в период времени, установить круг его общения, то есть с кем он разговаривал или переписывался.

Так, при расследовании уголовного дела о похищении человека с целью выкупа, при изучении биллинга одного из преступников удалось установить его связи – других соучастников преступления. А получив биллинг всех соучастников, получилось выяснить наиболее активного участника – организатора преступления. Кроме того, следователь без труда подтвердил, что преступники были на месте происшествия при подготовке преступления, когда следили за потерпевшим, а также в момент его

похищения, поскольку в их биллинге имелись сведения о базовых станциях сотовой связи, расположенных в районе совершения преступления.

По уголовному делу о хищении директором дома культуры денежных средств было установлено, что он фиктивно трудоустроил к себе родственницу на должность уборщицы. Его родственница на работу не выходила, а ее зарплату директор присваивал себе. Однако, в ходе допроса, директор утверждал, что уборщица регулярно приходила на работу. При осмотре биллинга родственницы было установлено, что во весь период трудоустройства она на рабочем месте ни разу не появлялась, а проживала в соседнем городе.

Для того, чтобы упростить работу следователю с биллинговой информацией существуют технические и программные средства. Например, в Следственном комитете Российской Федерации используется программный комплекс «Сегмент-С», который устанавливается на специальный компьютер.

С помощью него можно проанализировать биллинг одного абонента. Это позволит установить интенсивность сеансов связи лица с конкретным человеком, в конкретное время или месте. Программа позволяет нанести на карту места, откуда осуществлялся выход на связь.

Кроме того, комплекс «Сегмент-С» позволяет проводить анализ сразу нескольких биллингов разных абонентов. В этом случае биллинговая информация, полученная от оператора связи, в электронном виде загружается в программу и обрабатывается. В результате следователь может установить:

- взаимные связи нескольких лиц (общих знакомых, соучастников преступления, установление лидера группы);

- совместное пребывание абонентов в одно время в одном месте (совместное пребывание преступника с потерпевшим);

- нестандартное поведение абонента, явно отличающееся в отдельные периоды времени от обычного использования мобильного устройства (например, ребенок не позвонил родителям перед началом занятий о том, что пришел в школу, хотя ранее всегда это делал) (**Приложение 5**).

Для качественного анализа биллинговой информации иногда требуется установить, какие базовые станции сотовой связи работают в конкретном месте. Для этого используют **датчик оценки радиоэлектронной обстановки** (далее - датчик РЭО). Этот датчик необходимо использовать, когда не установлено, кто совершил преступление (**Приложение 6**).

Так, по уголовному делу о хищении в госпитале компьютерной техники первоначально не удалось установить виновных лиц. Однако было ясно, что преступники увезли похищенное на автомобиле. Тогда следователь использовал датчик РЭО и определил, что в месте, где совершено преступление осуществляют связь две базовые станции, по дороге, ведущей в сторону города еще несколько базовых станций. Получив биллинг на всех абонентов (всего 39 абонентов), чью связь фиксировали указанные две базовые станции он был проанализирован с помощью комплекса «Сегмент-С». В результате, среди абонентов удалось установить в основном местных жителей, а также двух лиц, чьи переговоры друг с другом фиксировались в районе госпиталя в ночь совершения преступления. Их личности были установлены и получен их биллинг за более длительный период до совершения преступления и после него. Анализом информации было установлено, что оба подозреваемых проживали в соседнем районе, а возле госпиталя их абонентские устройства фиксировались лишь за сутки до хищения и в ночь, когда было совершено преступление. Также по биллингу был установлен общий знакомый подозреваемых – сотрудник охраны госпиталя. После допроса друзей указанных подозреваемых, выяснилось, что последние после хищения предлагали продать компьютерную технику. В дальнейшем преступники сознались в совершении хищения.

4. Осмотр мобильных устройств связи

В настоящем разделе проекта пойдет речь об обнаружении локальных цифровых следов, хранящихся в мобильных устройствах.

Как мы неоднократно отмечали, мобильные устройства связи в настоящее время стали настолько неразрывно связаны с каждым человеком и хранят столько информации о личности, что теперь совершенно обоснованно можно изменить старую поговорку «Скажи мне, кто твой друг, я скажу – кто ты», на «дай изучить мне твой смартфон и я скажу, кто ты». Для расследования преступлений изучение мобильного устройства преступника или потерпевшего также играет большую роль в собирании доказательств.

К носителям информации устройств мобильной связи относятся:

- телефоны, смартфоны;

- сим – карты;

- карты памяти.

Исследование цифрового носителя информации в следственной практике проходит в несколько этапов, на каждом из которых применяется своя методика и специальная техника.

К этапам исследования мобильного устройства можно отнести следующее:

1. Извлечение данных из цифрового носителя и их копирование.
2. Преобразование (декодирование) полученной информации в вид, пригодный для дальнейшей обработки, чтения и анализа.
3. Анализ извлеченной информации. Составление отчета об извлечении информации. Поиск и изъятие значимых для расследования данных.

На сегодняшний день имеется несколько **основных направлений работы с цифровыми следами**, содержащимися в памяти мобильных устройств.

1) **Извлечение и анализ полных данных**:

- переписка в чатах, мессенджерах, SMS;

- список контактов, последние соединения;

- заметки, фото, видео, аудио файлы;

- используемые сайты, интернет история и пр.

2) **Определение местонахождения электронного устройства (а, следовательно, и его владельца)**.

С помощью спутниковой навигации - функции геопозиционирования (GPS/ГЛОНАСС) или соединения с точками доступа сети WiFi, а также метаданных фотоснимков, видеороликов, веб-сайтов возможно установить координаты местоположения мобильного устройства любого лица в определенное время.

Некоторую информацию можно получить непосредственно путем изучения содержимого телефона, без каких-либо специальных устройств. Это касается контактов, журнала звонков, СМС – переписки, содержания мессенджеров (WhatsApp, Viber и др.), переписки в социальных сетях[6], записной книжки, отметок календаря, интернет истории (журнал браузеров), фотографий и видео файлов.

С помощью же специальной высокотехнологичной криминалистической техники можно обойти пароли, установленные на мобильном устройстве, извлечь полную информацию, **включая удаленную** переписку в мессенджерах, смс, контакты и пр. из памяти мобильных телефонов, а также электронных накопителей карт памяти, СИМ-карт.

Кроме того, к носителям информации устройств мобильной связи, с учетом широкого распространения в последнее время, необходимо отнести также «облачные данные».

[6] Зачастую пользователи смартфонов сохраняют пароли при входе в социальные сети и вход происходит автоматически.

«Облачные данные» – сведения, которые хранятся на внешних устройствах, сервисах, хранилищах, серверах (общее определение «в облаке»), которые непосредственно связаны с мобильным устройством путем специфичных идентификационных данных, таких как: данные аккаунта (логин, пароль), токен авторизации, электронный сертификат. Обмен данными между мобильным устройством и «облаком» происходит посредством коммуникационных информационных сетей, наиболее распространенной из которых является сеть «Интернет».

Для извлечения информации из устройств мобильной связи в следственных органах наиболее широко используются специализированные аппаратно-программные комплексы марки:

- UFED;

- мобильный криминалист;

- XRY.

Данная криминалистическая техника позволяет работать практически с любой моделью мобильных устройств на основе любой операционной системы.

При подготовке к проекту я посетила криминалистические подразделения Следственного комитета Российской Федерации в г. Солнечногорске и г. Москве, где ознакомилась и сама попробовала работу с аппаратно-программными комплексами UFED 4PC, а также мобильный криминалист, версии «Детектив» (**Приложения 7, 8, 10**).

Особенность использования данных комплексов заключается в том, что с их помощью извлечению и систематизации с построением отчета подлежат и удаленные с устройств данные. Эта техника позволяет войти в систему большинства мобильных телефонов в обход блокировки вводом графического ключа, паролей, PIN-кода. В следственной практике извлечения сведений с цифровых носителей мобильных устройств зачастую

встречаются случаи, когда исследуемый носитель не исправен, не включается, на все попытки коммуникации не реагирует. Вместе с тем, в памяти цифрового носителя все еще содержится необходимая для следствия информация.

Примером таких устройств являются утопленные, разбитые, обгоревшие мобильные телефоны. Так же к таким устройствам можно отнести неисправные и поврежденные карты памяти, а также часть устройств (не использующих шифрование), доступ к памяти, которых не возможен по причине блокировки код-паролем устройства.

Каждый аппаратно-программный комплекс для осмотра мобильных устройств состоит из аппаратной части – планшетного или стационарного компьютера со специальным программным обеспечением, а также различными переходниками, проводами для подключения осматриваемого мобильного устройства к компьютеру. Отдельное устройство в виде адаптеров предназначено для осмотра сим-карты и карты памяти.

С помощью, например комплекса UFED, можно получить следующую информацию, которая **отображается в сводке об извлечении (Приложение 9)**:

- полные сведения о телефоне (IMEI и др.);
- сведение о SIM-карте;
- журнал вызовов, в том числе удаленные (время, имена, фото);
- журнал использования интернет-браузера;
- закладки интернет-сайтов;
- IP-подключения и беспроводные сети;
- пользовательский словарь;
- файлы Cookie;
- записи телефонной книги;

- SMS, MMS и голосовые сообщения;

- сообщения чатов и электронной почты;

- изображения;

- видео- и аудиофайлы;

- данные о местоположении (сети WiFi (MAC- адрес беспроводной сети за счет преобразования значений BSSID), ретрансляторы мобильной связи и навигационные приложения), маршрутах перемещения (можно просматривать в Google Earth и Google Maps), GPS-координат использования мобильного устройства;

- пароли, журналы вызовов, текстовые сообщения, контакты, мессенджеры, календарь, медиафайлы, геотеги, приложения, служебные данные – список IMSI, данные последней SIM-карты, коды блокировки.

- данные журнала «Lifeblog», содержащего список действий с телефоном.

На SIM-карте как правило выявляется следующая информация:

1) об операторе сотовой связи;

2) о номере IMSI абонента, который является уникальным идентификатором для каждого абонента в системе;

3) об SMS трафике – сведений об отправленных и полученных абонентом коротких текстовых прочитанных или непрочитанных сообщений;

4) о примерном местонахождении абонента, посредством извлечения информации о последней базовой станции, с помощью которой абонент был зарегистрирован системой GSM;

5) о последних набранных номерах;

6) о сохраненных в памяти SIM-карты контактных номерах других абонентов;

7) об оплате услуг, предоставляемых оператором сотовой связи.

В связи с современными возможностями удаленного доступа к памяти смартфонов, имеющих выход в Интернет и, находящихся в них электронных накопителей, с целью их блокирования или удаления информации, необходимо сразу же при обнаружении устройства помещать его в специальный чехол, поставляемый в комплекте с UFED – «Мешок Фарадея», который блокирует доступ к устройству, либо переводить устройство в авиа режим. Это не позволит преступнику дистанционно удалить из смартфона важную для следователя информацию.

Можно привести несколько примеров успешного использования следователями аппаратно-программных комплексов для осмотра мобильных устройств связи и извлечения из них цифровых следов.

Так, по уголовному делу о вымогательстве крупной суммы денег у предпринимателя подозреваемый был установлен лишь спустя несколько месяцев после совершения преступления. Он отрицал свою причастность к вымогательству, полагал свое задержание ошибкой следствия. Однако после осмотра его мобильного телефона с применением комплекса UFED удалось извлечь из памяти устройства ранее удаленные смс сообщения, в которых он обсуждал с подельником подготовку к преступлению, в частности указывал номер банковского счета, куда нужно было перевести потерпевшему деньги. Это явилось важным доказательством в суде.

По уголовному делу о жестоком обращении с животными видеозапись убийства двух собак была выложена неустановленными лицами в сеть Интернет. На записи не было видно лица преступников, однако по элементам их одежды, району, где имело место преступление и иным данным, было установлено, что оно совершено больше года назад, вероятно гражданином Т. и В. Первоначально Т. и В. дали показания, что не совершали преступления. Однако при осмотре их смартфонов с применением аппаратно-программного комплекса «Мобильный криминалист» была

обнаружена удаленная переписка в мессенджере WhatsApp, свидетельствующая об осуществлении В. съемки убийства собак на иной телефон. В ходе обыска этот телефон был изъят по месту работы В. и в нем обнаружена видеозапись убийства. После этого В. и Т. раскаялись в совершении преступления.

По уголовному делу о хищении в медицинском учреждении у врача дорогостоящего смартфона, подозреваемый был установлен в течение одного часа, им оказался пациент больницы. Он пояснил, что не похищал смартфон, всего лишь решил пошутить над врачом и спрятал устройство под кроватью своей палаты, намереваясь его вернуть. Однако при осмотре смартфона было установлено, что подозреваемый его выключил, вытащил сим-карту, которую выкинул в окно палаты. Это явно свидетельствовало о его намерении похитить смартфон и исключить возможность его найти законному владельцу. После включения смартфона и просмотра истории посещенных в интернете страниц, было установлено, что обвиняемый искал на различных интернет-ресурсах стоимость похищенного им мобильного телефона. Полученные цифровые следы в совокупности с иным доказательствами, позволили обвинить пациента в совершении кражи.

Заключение

Подводя итоги работы, следует отметить, что вопросы исследования цифровых следов в криминалистике являются очень актуальными, поскольку растет уровень цифровизации всех отраслей нашей жизни.

Я узнала особенности цифровых следов и механизм их образования. Оставить и обнаружить такие следы человеку возможно только с применением технических и программных средств.

Я узнала, как появляются цифровые следы в результате использования мобильных средств связи. Получила навыки работы с криминалистической техникой, с помощью которой осматривают мобильные телефоны и смартфоны.

Изучив архивные материалы следственных органов, я на конкретных примерах поняла значение цифровых следов в работе следователя.

При расследовании сложных и запутанных дел **цифровой след может выступать важным доказательством.**

ГЛОССАРИЙ

Абонент - физическое лицо (гражданин) или юридическое лицо, с которым заключен договор об оказании услуг подвижной связи при выделении для этих целей абонентского номера или уникального кода идентификации;

Абонентская станция (абонентское устройство) - пользовательское (оконечное) оборудование, подключаемое к сети подвижной связи.

Абонентский номер - номер, однозначно определяющий (идентифицирующий) подключенную к сети подвижной связи абонентскую станцию (абонентское устройство) с установленной в ней SIM-картой.

Аплеты – игровые и/или информационные приложения, устанавливаемые на абонентские устройства и предназначенные для воспроизведения на абонентских устройствах.

Биллинг (англ. billing — составление счёта) **–** это процесс расчета стоимости услуг или выписка счета по ним. Биллинговая система представляет собой программный комплекс, осуществляющий учет объема потребляемых услуг абонентами, расчет и списание средств со счетов абонентов в соответствии с тарифами на предоставляемые услуги.

Голосовой вызов – голосовое коммутируемое соединение, которое устанавливает оператор при помощи оборудования своей сети связи от абонентского устройства абонента.

Гостевой регистр местоположения (VLR) — содержит информацию об активных абонентах, т.е. тех, кто в данный момент находится в зоне действия коммутатора, к которому принадлежит гостевой регистр. Количество гостевых регистров местоположения равно количеству коммутаторов. Каждый гостевой регистр местоположения приписан к определенному коммутатору.

Домашний регистр местоположения (HLR) — представляет собой компьютерную базу данных о домашних абонентах-пользователях мобильной связи вне зависимости от того, включен или выключен их телефон. В базе содержатся опознавательные номера и адреса, а также параметры подлинности абонентов и список доступных услуг связи. Записанные данные позволяют абоненту пользоваться основными и дополнительными услугами сотовой связи.

Зона обслуживания сети подвижной связи - совокупность территорий, обслуживаемых всеми узлами связи сети подвижной связи одного и того же оператора связи.

Информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том

числе с использованием вычислительной техники и связи, реализующих информационные процессы.

Информационно-развлекательный контент – различная текстовая информация (гороскопы, анекдоты, новости, тосты, курсы валют, биоритмы, сонники и т.п.), предоставляемая Абоненту в период действия Услуги.

Короткое текстовое сообщение - сообщение, состоящее из букв или символов, набранных в определенной последовательности, предназначенное для передачи по сети подвижной связи.

Международный союз электросвязи (МСЭ) — международная организация, в рамках которой правительствами и частным сектором координируются глобальные сети и услуги электросвязи. Основанный в Париже в 1865 г. как Международный телеграфный союз, МСЭ получил свое нынешнее название в 1934 г., а в 1947 г. стал специализированным учреждением Организации Объединенных Наций.

Мобильный телефон - мобильное коммуникационное устройство, предназначенное преимущественно для голосового общения. Технологическую основу мобильной связи составляет радиосвязь.

Сервер - программно-аппаратное средство, реализующее определенные функции (хранение, обработка, передача информации и т.п.)

Слайдер - мобильный телефон, который состоит из двух частей, сдвигающихся друг относительно друга. Псевдораскладушка - внешне очень похожа на «раскладушку», но экран находится в нижней её части, а на откидной крышке только динамик. В отличие от флипа, верхняя крышка такого форм-фактора закрывает и дисплей. Часто в верхней крышке оставляют отверстие или делают часть крышки (а иногда и всю) прозрачной, чтобы можно было видеть дисплей в закрытом состоянии.

Смартфоны - мобильные телефоны с полноценной операционной системой: Symbian OS, Windows Mobile или Linux. Такие телефоны позволяют устанавливать новые программы, расширяющие их функциональность: ICQ-клиент, «чёрный список» и т. д.

Соединение по сети подвижной связи - установление в результате вызова взаимодействия между средствами связи, позволяющее абоненту передавать и (или) принимать голосовую и (или) неголосовую информацию.

Сотовая связь - разновидность систем связи, построенная в соответствии с сотовым принципом распределения частот по территории обслуживания и предназначенная для обеспечения радиосвязью большого числа подвижных абонентов с выходом на телефонную сеть общего пользования.

Сотовый телефон - мобильное коммуникационное устройство. Оно использует комбинацию радиопередачи и традиционной телефонной коммутации для осуществления телефонной связи на территории (зоны покрытия), состоящей из «сот», окружающих базовые станции сотовой сети.

Тарифный план - совокупность ценовых условий, на которых оператор связи предлагает пользоваться одной либо несколькими услугами подвижной связи.

Техническая возможность оказания услуг подвижной связи - наличие функционирующих технических средств и сооружений подвижной связи в зоне обслуживания сети подвижной связи оператора связи, необходимых для оказания абоненту услуг подвижной связи.

Центр аутентификации (AUC) — формирует параметры для процедуры аутентификации и определяет ключи шифрования мобильных станций абонентов. Процедура аутентификации – подтверждения подлинности абонента по параметрам законности и наличия прав на пользование услугами сотовой связи сети GSM. Выполнение данной процедуры исключает возможность появления несанкционированных пользователей («сотовых двойников»).

ADN (Abbreviated Dialing Numbers) - «Ускоренный набор номеров», записи телефонной книги, хранящиеся на SIM-карте.

GPRS (General Packet Radio Service) – технология беспроводной пакетной передачи данных.

GSM (Global System for Mobile Communications) - «Глобальная система мобильной связи», набор стандартов для сотовых сетей второго поколения, в настоящее время поддерживаемых проектом Партнерство третьего поколения (3GPP).

Hi-tech (high technology, high tech) - высокие технологии наиболее новые и прогрессивные технологии современности. Переход к использованию высоких технологий и соответствующей им техники является важнейшим звеном научно-технической революции (НТР) на современном этапе. К высоким технологиям обычно относят самые наукоёмкие отрасли промышленности.

ICCID (Integrated Circuit Card Identification) - «Номер идентификации чип-карты», уникальный и неизменный идентификатор, хранящийся на SIM-карте.

IM (Instant Messaging) - «Мгновенный обмен сообщениями», возможность обмениваться сообщениями в реальном масштабе времени с другими людьми в Интернете и отслеживать протекание разговора.

IMAP (Internet Message Access Protocol) - «Протокол доступа к сообщениям в Интернете», метод связи, используемый для чтения электронных сообщений, хранящихся на удаленном сервере.

IMEI (International Mobile Equipment Identity) - «Международный идентификатор мобильного оборудования», уникальный номер, запрограммированный в мобильные телефоны GSM.

IMSI (International Mobile Subscriber Identity) - «Международный идентификатор абонента мобильной связи», уникальный номер, связанный с каждым пользователем мобильного телефона GSM.

LND (Last Numbers Dialed) - «Последние набранные номера», журнал регистрации последних набранных номеров, подобный такому же журналу в телефоне, но хранящийся на SIM-карте без отметок даты/времени.

LOCI (Location Information) - «Информация о местонахождении» - «Идентификатор области местонахождения» («Location Area Identifier» (LAI)) текущего местонахождения телефона, постоянно хранящийся на SIM-карте, когда телефон включён, и сохраняемый в телефоне, когда тот выключен.

MMS (Multimedia Message Service) - мультимедийное сообщение, содержащее информацию в цифровом, текстовом, графическом, аудио, видео формате, которое передается Оператором при помощи оборудования своей сети связи по Цифровым идентификаторам.

MMS (Multimedia Messaging Service) - «Служба передачи мультимедиа-сообщений», принятый стандарт для передачи сообщений, который позволяет пользователям отправлять и получать сообщения с текстом, графическими файлами, фотографиями, аудио- и видео-файлами.

MSISDN (Mobile Subscriber Integrated Services Digital Network) - «Номер мобильного абонента сети ISDN», международный номер телефона, присвоенный абоненту сотовой связи.

PIM (Personal Information Management) - «Управление личной информацией», такие типы данных, как контакты, записи в календаре, задачи, примечания, записки и сообщения электронной почты, которые можно синхронизировать с ПК на устройство и наоборот.

POP (Post Office Protocol) - стандартный почтовый протокол, используемый для получения электронной почты с сервера.

SIM (Subscriber Identity Module) - «Модуль идентификации абонента», чип смарт-карты, специализированный для использования в оборудовании GSM.

SIM-карта - карта, с помощью которой обеспечивается идентификация абонентской станции (абонентского устройства), ее доступ к сети подвижной связи, а также защита от несанкционированного использования абонентского номера.

SMS (Short Message Service) - «Служба обмена текстовыми сообщениями», служба сети мобильных телефонов, которая позволяет пользователям отправлять и получать буквенно- цифровые текстовые сообщения до 160 символов на свой сотовый телефон или другое портативное устройство.

SMS Chat - «SMS-чат», возможность обмена сообщениями между пользователями мобильных телефонов в реальном времени через отправку

текстовых SMS- сообщений, которая позволяет просматривать предыдущие сообщения того же самого разговора.

URL – идентификатор направления информационного соединения в WEB/WAP, по которому абоненты могут отправить заказ (WEB/WAP-запрос).

WAP (Wireless Application Protocol) - «Протокол для приложений беспроводной связи», стандарт, определяющий способ, с помощью которого беспроводным мобильным устройствам предоставляется связь с Интернетом и другие расширенные услуги.

WEB – глобальное информационное пространство, основанное на физической инфраструктуре Интернета и протоколе передачи данных, доступ к которому осуществляется по сети передачи данных оператора с использованием абонентского устройства.

WiFi (Wireless Fidelity) - общий термин, относящийся к беспроводной локальной сети.

USB (**Universal Serial Bus** — «универсальная последовательная шина») — последовательный интерфейс передачи данных для среднескоростных и низкоскоростных периферийных устройств в вычислительной технике. Символом USB являются четыре геометрические фигуры: большой круг, малый круг, треугольник и квадрат, расположенные на концах древовидной блок-схемы.

Список литературы

1. Александрова И.В. Криминалистика: учебник для бакалавриата и магистратуры // И.В. Александрова. М.: Юрайт. 2016.

2. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. № 4 (34).

3. Вехов В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, Б. П. Смагоринский, С. А. Ковалев // Судебная экспертиза. Волгоград. 2016.

4. Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. № 8.

5. Дмитриев Е.Г., Котенков А.В. О некоторых особенностях использования информации систем видеонаблюдения в ходе расследования преступлений. Журнал «Российский следователь». 2013 № 1.

6. Багмет А.М., Скобелин С.Ю. Обнаружение, фиксация, изъятие и исследование мобильных средств связи, принадлежащих участникам уголовного судопроизводства. Учебное пособие Академии СК России, Москва 2017.

7. Яковлев А.Н. Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе. Цифровая криминалистика и право, Москва 2018.

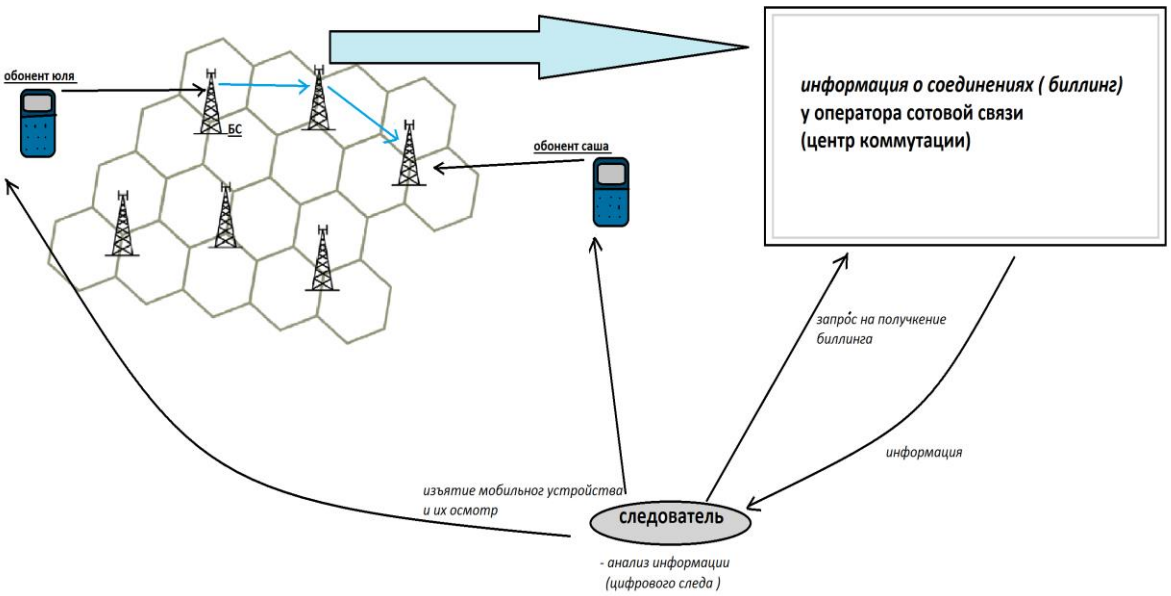
8. Обнаржение, фиксация, анализ и осмотр криминалистически значимой информации в социальных сетях. Учебно-методическое пособие Московской Академии СК России, Москва 2019.

9. Интернет-энциклопедия Википедия.

10. Архивные материалы Следственного комитета Российской Федерации.

Приложение 1

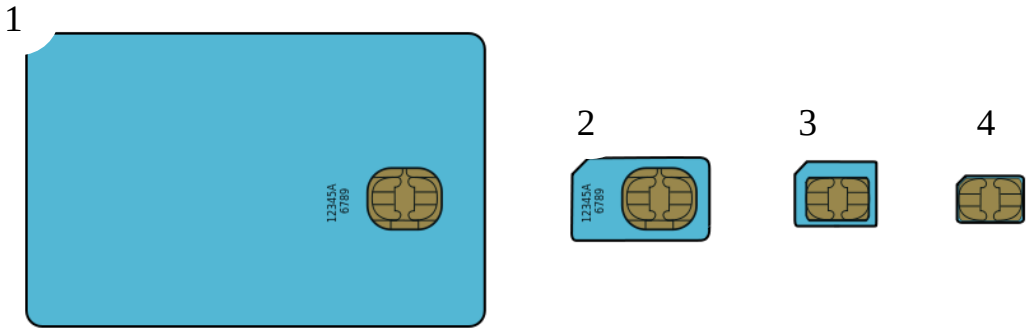
Принцип работы сотовой связи и получение следователем биллинговой информации



Приложение 2

Составные части и виды SIM-карты.

1. Контактная площадка микрочипа.
2. Полимерный корпус.
3. Уникальный код абонента IMSI (International Mobile Subscriber Identity).



Виды SIM-карт.

	Вид SIM-карты	Введена	Длина (мм)	Ширина (мм)	Толщина (мм)
	Классический вид (FF)	**1991**	**85.60**	**53.98**	**0.76**
	Мини-SIM (2FF)	**1998**	**25.00**	**15.00**	**0.76**
	Микро-SIM (3FF)	**2003**	**15.00**	**12.00**	**0.76**
	Нано-SIM (4FF)	**2012**	**12.30**	**8.80**	**0.67**

Пластиковая карта, предоставляемая оператором сотовой связи абоненту при заключении договора об оказании услуг связи.

1. SIM-карта на временном пятиэлементном крепеже.
2. Уникальный код абонента IMSI.
3. Стираемое покрытие (скретч-слой) под которым расположены цифровые обозначения PIN1, PIN2, PUK1, PUK2 кодов.
4. Логотип оператора сотовой связи.

Приложение 3

IMEI мобильного телефона

IMEI - International Mobile Equipment Identifier - число, являющееся уникальным для каждого выпущенного мобильного телефона. Устанавливается на заводе при изготовлении, служит для идентификации устройства в GSM сети. Число IMEI обычно можно прочитать на специальной табличке, расположенной под аккумуляторной батареей, а также определить (у большинства аппаратов), введя на клавиатуре следующий код: *#06#.

Код IMEI содержит 15 цифр и состоит из четырех частей:

IMEI = TAC + FAC + SNR + SP, где:

TAC (Type Approval Code) - шестизначный код выбранного типа телефона конкретной серии (первые 2 цифры - код страны фирмы - разработчика);

FAC (Final Assembly Code) - используемый фирмой-разработчиком двузначный код, по которому можно определить страну, где был изготовлен телефон (код страны финальной сборки);

SNR (Serial Number) - шестизначный серийный код, который присваивается конкретному мобильному телефону;

SP (Spare) - одна цифра, в зависимости от решения производителя контрольное или резервное число (у старых моделей почти всегда 0).

Коды TAC и FAC могут совпадать у телефонов одного типа и одной партии, выпущенной на одном и том же предприятии. Код SNR всегда индивидуален для каждого мобильного телефона.

Приложение 4

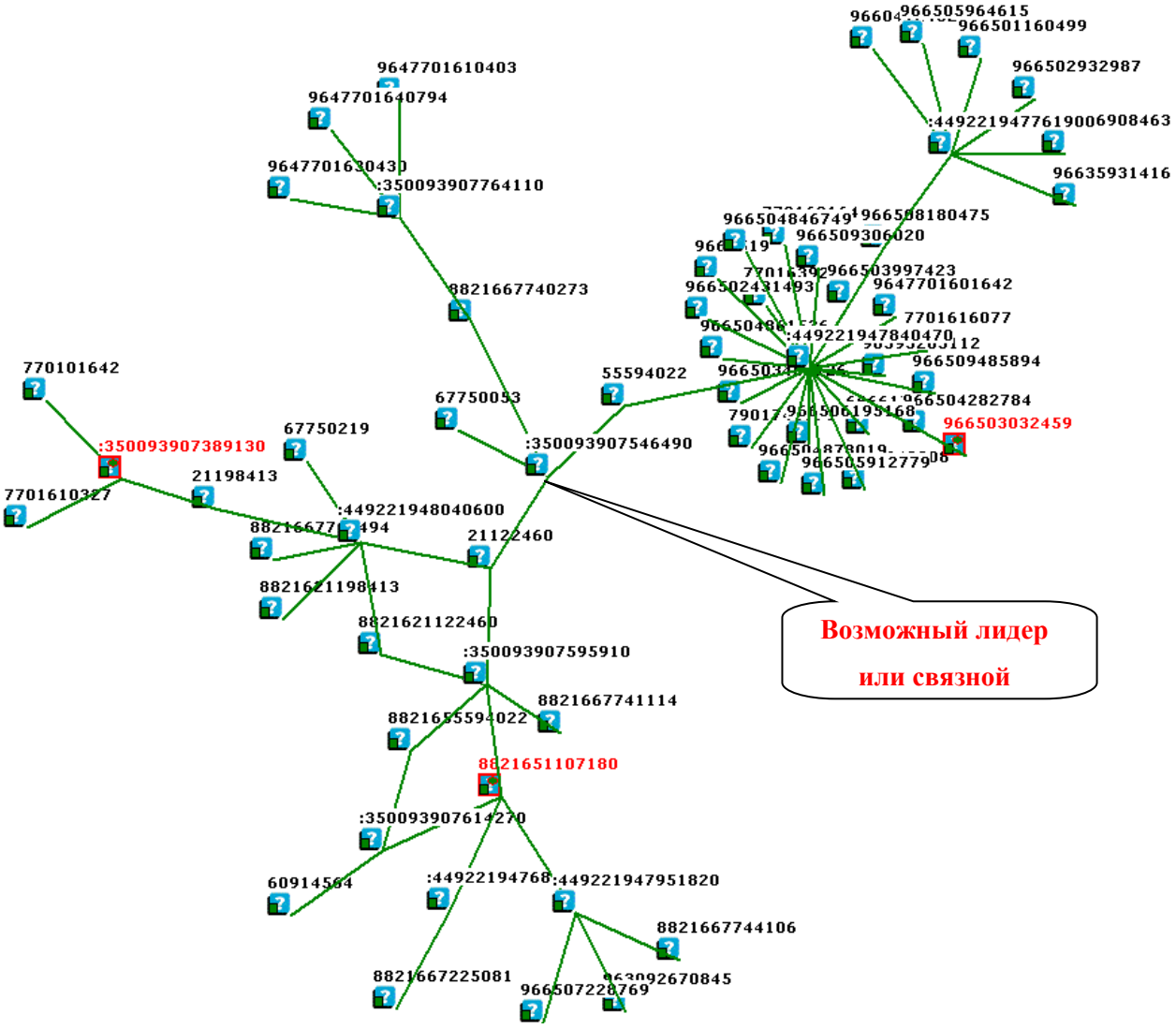
Образец биллинговой информации,
предоставленной оператором сотовой связи

Номер А	IMEI А	Номер Б	IMEI Б	Время	Длительность, сек	Тип	Код первой группы сот абонента А	базовой станции абонента А	Адрес первой БС абонента А	второй группы сот	последней базовой станции	Адрес последней БС абонента А	Код первой группы сот абонента Б	Номер первой базовой станции абонента Б
79257281403	356773086300300	79104501634		01.08.2018 07:57:21 +03:00	11	Звонок	5060	51192	Истринский р-н, пос. П	5060	51192	Истринский р-н, пос. Павловская		
79257281403	3567730863003004			01.08.2018 08:03:10 +03:00	292	GPRS сессия	7728	24934	Краснопресненский то					
79257281403	3567730863003004			01.08.2018 08:08:02 +03:00	1501	GPRS сессия	7728	24934	Краснопресненский то					
79257281403	3567730863003004			01.08.2018 08:33:01 +03:00	3600	GPRS сессия	5060	51192	Истринский р-н, пос. П					
79257281403	3567730863003004			01.08.2018 09:33:01 +03:00	867	GPRS сессия	5060	51192	Истринский р-н, пос. П					
79257281403	3567730863003004			01.08.2018 11:14:02 +03:00	3600	GPRS сессия	9078	52138						
79257281403	3567730863003004			01.08.2018 11:15:40 +03:00	3600	GPRS сессия	5078	2294	Одинцовский р-н., д. С					
mamadeti		79257281403	356773086300300	01.08.2018 11:28:05 +03:00	1	СМС								
mamadeti		79257281403	356773086300300	01.08.2018 11:28:08 +03:00	1	СМС								
mamadeti		79257281403	356773086300300	01.08.2018 11:28:17 +03:00	1	СМС								
mamadeti		79257281403	356773086300300	01.08.2018 11:28:18 +03:00	1	СМС								
mamadeti		79257281403	356773086300300	01.08.2018 11:28:19 +03:00	1	СМС								
mamadeti		79257281403	356773086300300	01.08.2018 11:28:20 +03:00	1	СМС								
79257281403	356773086300300	79104501634		01.08.2018 11:44:44 +03:00	39	Звонок	5078	5597	Одинцовский р-н, дер	5078	5597	Одинцовский р-н, дер. Лапино		
79257281403	356773086300300	79037258999		01.08.2018 11:56:49 +03:00	12	Звонок	5078	5599	Одинцовский р-н, дер	5078	5599	Одинцовский р-н, дер. Лапино		
79257281403	3567730863003004			01.08.2018 12:14:02 +03:00	3601	GPRS сессия	9078	52138						
79257281403	3567730863003004			01.08.2018 12:15:40 +03:00	3600	GPRS сессия	5078	2294	Одинцовский р-н., д. С					
79037258999		79257281403	356773086300300	01.08.2018 12:15:44 +03:00	191	Звонок							5078	59091
79370367939	359312062922270	79257281403		01.08.2018 13:35:09 +04:00	30	Звонок в роуми	5060	11606						
79257281403	3567730863003004			01.08.2018 13:05:57 +03:00	3600	GPRS сессия	5060	47100	Красногорский р-н, Но					
79257281403	356773086300300	74957543004		01.08.2018 13:06:36 +03:00	135	Звонок	7728	497		7728	492			
79257281403		74957543004		01.08.2018 13:06:36 +03:00	134	Звонок PSTN (бе								
79257281403	3567730863003004			01.08.2018 13:14:02 +03:00	3600	GPRS сессия	9078	52138						
79257281403	3567730863003004			01.08.2018 13:15:40 +03:00	3600	GPRS сессия	5078	2294	Одинцовский р-н., д. С					
79257281403		79262992442		01.08.2018 13:34:59 +03:00	0	Услуга дополнит								
79370367939	359312062922270	79257281403	356773086300300	01.08.2018 13:35:09 +03:00	30	Звонок	5060	11606	Истринский р-н, пос. П	5060	11606	Истринский р-н, пос. Павловская	7728	492
79257281403	3567730863003004			01.08.2018 14:14:02 +03:00	3600	GPRS сессия	9078	52138						
79257281403	3567730863003004			01.08.2018 14:15:40 +03:00	3600	GPRS сессия	5078	2294	Одинцовский р-н., д. С					
79257281403	3567730863003004			01.08.2018 15:14:02 +03:00	3600	GPRS сессия	9078	52138						
79257281403	3567730863003004			01.08.2018 15:15:40 +03:00	3600	GPRS сессия	5078	2294	Одинцовский р-н., д. С					
79257281403	3567730863003004			01.08.2018 16:05:57 +03:00	3600	GPRS сессия	5060	47100	Красногорский р-н, Но					
79257281403	3567730863003004			01.08.2018 16:14:02 +03:00	3600	GPRS сессия	9078	52138						
79257281403	3567730863003004			01.08.2018 16:15:40 +03:00	3600	GPRS сессия	5078	2294	Одинцовский р-н., д. С					
79257281403	3567730863003004			01.08.2018 17:14:02 +03:00	3600	GPRS сессия	9078	52138						
79257281403	3567730863003004			01.08.2018 17:15:40 +03:00	3600	GPRS сессия	5078	2294	Одинцовский р-н., д. С					
79037258999		79257281403	356773086300300	01.08.2018 17:57:57 +03:00	137	Звонок							5060	46373

Приложение 5

Результат работы программного комплекса «Сегмент-С».

Установление лидера преступной группы по его связям.



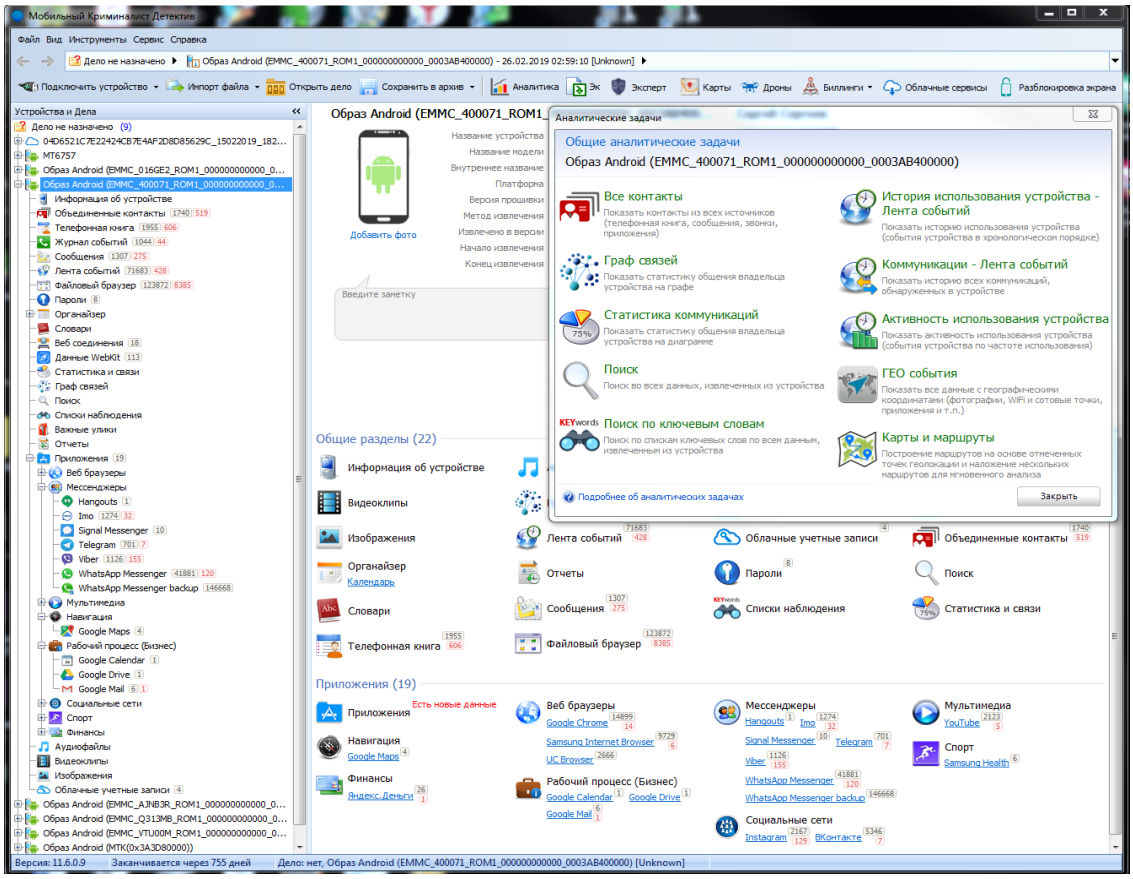
Приложение 6

Общий вид

датчика оценки радиоэлектронной обстановки (датчик РЭО).

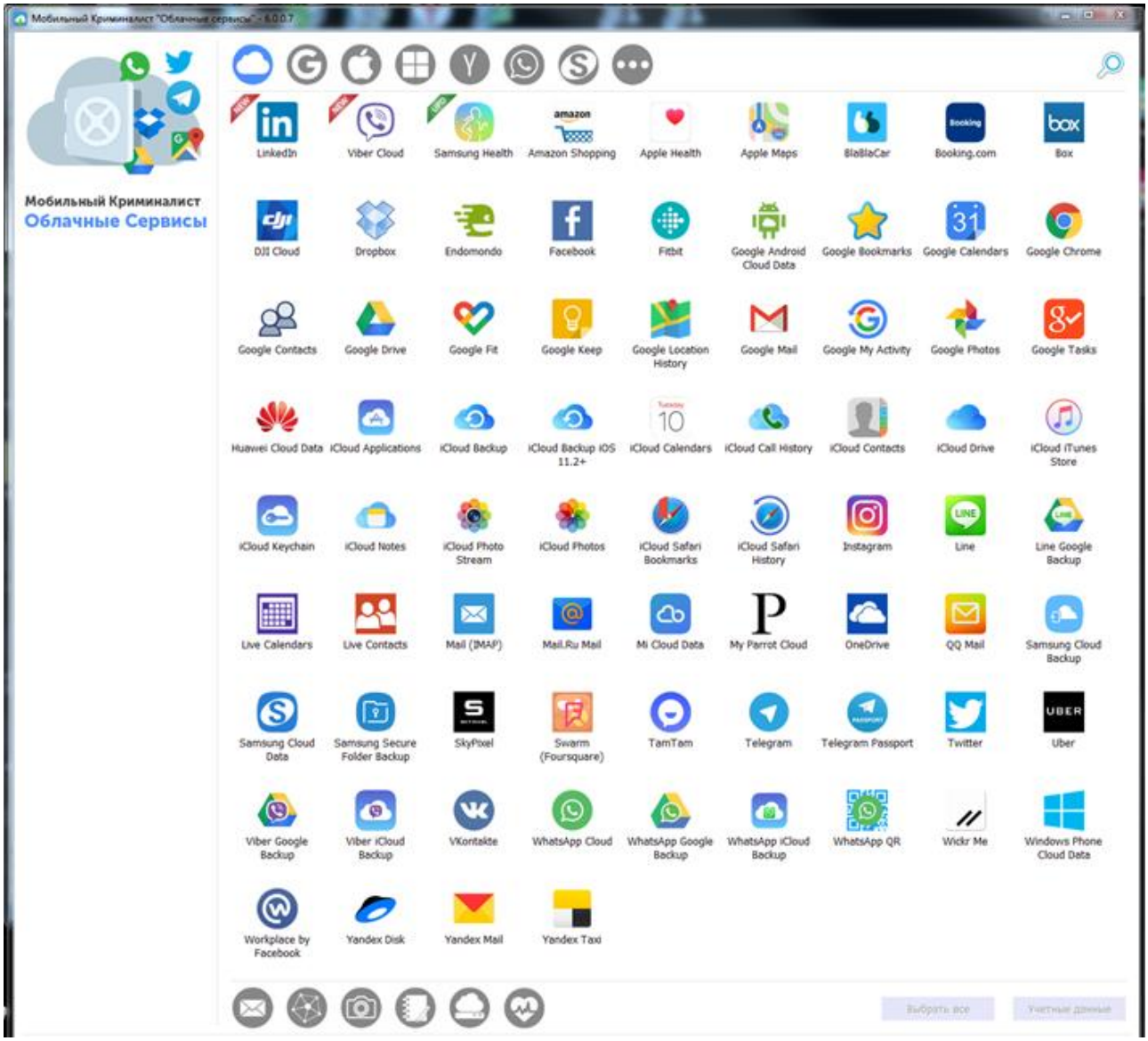
Приложение 7

Внешний вид приложения «Мобильный криминалист Детектив».



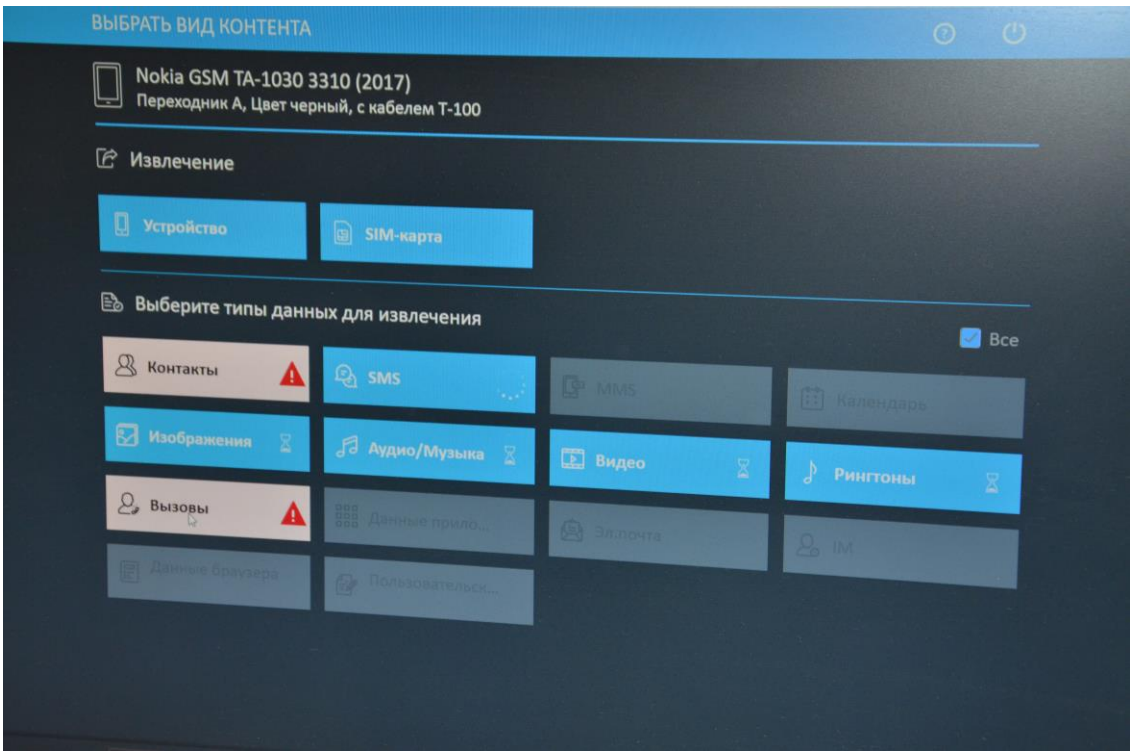
Список облачных сервисов, доступных

для извлечения в АПК «Мобильный криминалист Детектив».



Приложение 8

Осмотр мобильного телефона с помощью АПК UFED 4PS



Приложение 9

Пример отчета об извлечении информации из смартфона с помощью UFED 4 PS

Отчёт об извлечении

Apple iPhone

Сводка

Версия UFED Physical Analyzer	5.4.0.203
Время создания отчета	16.02.2017 11:11:39 +03:00
Выбор часового пояса (UTC)	Исходное значение UTC
Номер дела	33|12|0029-16
Название дела	фильтры
Имя эксперта	ЦСГ
Примечания	айфон 6С - А1633 файловая система

Извлечение из источника

Файловая система	
Дата/время начала извлечения	16.02.2017 9:49:11(UTC+3)
Дата/время окончания извлечения	16.02.2017 10:01:43(UTC+3)
Версия UFED	5.4.0.863
Внутренняя версия	4.3.14.863
Выбранный производитель	Apple
Имя выбранного устройства	iPhone 6s (A1633)
Тип соединения	Cable No. 210
Тип извлечения	Файловая система
Идентификатор извлечения	39CE8D58-A45A-49F3-9C26-C2E0EEEE1841

Сведения об устройстве

Имя	Значение
Файловая система	
iPhone Дмитрий	
Серийный номер	F97NT0LTFNJJ
Имя владельца	iPhone Дмитрий
IMEI	352009068913826
ICCID	89701010063863412676
MSISDN	+7 (917) 617-83-96
Версия ОС	10.2.1
Зашифровано	False
Уникальный идентификатор	1e357ed0400c868b8694def63eac63947a76830a
Модель обнаруженного телефона	iPhone6,1
Производитель обнаруженного телефона	iPhone 6s (A1433/A1463)
Модем	
Время последней активации	07.02.2017 7:07:26(UTC+0)
Учетная запись iCloud присутствует	True
Адрес устройства Bluetooth	20:a2:e4:b7:f7:1d
Серийный номер	F97NT0LTFNJJ
IMSI	250016386341267
IMEI	352009068913826
ICCID	89701010063863412676
Уникальный идентификатор	1e357ed0400c868b8694def63eac63947a76830a
Адрес WiFi	20:a2:e4:b7:fc:4e
Определенная модель	iPhone (N61AP)
Дата/время телефона	16.02.2017 6:63:12(UTC+0)
Модель обнаруженного телефона	iPhone6,1
Модель обнаруженного телефона	iPhone 6s (A1433/A1463)
Версия ОС	10.2.1
Apple ID	klevcov00@yandex.ru
Apple ID	klevtsovv6767@gmail.com
ICCID последнего пользователя	89701010063863412676
MSISDN	79176178396
Sync Data	
Sync host name	Computer: 1-PC\User: klevc
Phone Settings	
Службы определения местоположения включены	True
Функция "Найти мой iPhone" включена	True

1

Сведения о хэше образа (1)

⚠ Для этого проекта имеются данные хэша.

#	Имя	Информация	
1	FileDump	Путь	Apple_iPhone 6s (A1633).zip
		Размер (байт)	6206283640
		MD6	F60443FB70CD2BAB6B96F660E46428F7

Подключаемые модули

#	Имя	Автор	Версия
1	iPhone Backup Parser Parses all iPhone Backup/Logical/FS dumps, including decryption and/or FileSystem creation when necessary	Cellebrite	2.0
2	iPhone Databases Reads various databases on the iPhone, containing notes, calendar, locations, Safari bookmarks, cookies and history, Facebook friends and bluetooth pairings.	Cellebrite	2.0
3	QuicktimeMetadata Extracts metadata from Apple quicktime movies	Cellebrite	2.0
4	iPhone device info Decodes device information for iPhone devices	Cellebrite	2.0
5	Pre Project		
6	Garbage Cleaner		
7	ContactsCrossReference Cross references the phone numbers in a device's contacts with the numbers in SMS messages and Calls. Will fill in the Name field of calls and SMS if there's a match.	Cellebrite	2.0
8	Analytics Generates the Analytics section information	Cellebrite	2.0
9	Project Processor Finisher		
10	Post Project		

Содержание

Тип	Включено в отчет		Всего	
MMS-сообщения	21	(1 Удалено)	21	(1 Удалено)
SMS-сообщения	297	(1 Удалено)	297	(1 Удалено)
Беспроводные сети	20		20	
Веб-закладки	13		13	
Журнал звонков	223	(4 Удалено)	223	(4 Удалено)
Журнал просмотра веб-страниц	2776	(21 Удалено)	2776	(21 Удалено)
Записи	3	(1 Удалено)	3	(1 Удалено)
Записи журнала	182		182	
Записи календаря	46	(1 Удалено)	46	(1 Удалено)
Контакты	100	(1 Удалено)	100	(1 Удалено)
Местоположение	86	(1 Удалено)	86	(1 Удалено)
Пароли	1		1	
Поиск элементов	1108	(1 Удалено)	1108	(1 Удалено)
Примечания	8	(3 Удалено)	8	(3 Удалено)
Уведомления	66		66	
Установленные приложения	194		194	
Устройства Bluetooth	1		1	
Учетные записи пользователей	12		12	
Файлы Cookie	1668	(23 Удалено)	1668	(23 Удалено)
Чаты	2		2	
• iMessage: +79176178396	2		2	
Эл. почта	43		43	
Расписание	9183	(32 Удалено)	9183	(32 Удалено)
Файлы данных	42993	(1 Удалено)	42993	(1 Удалено)
• Аудио	2		2	
• Базы данных	374		374	
• Видеозаписи	67		67	
• Документы	4		4	
• Изображения	9626		9626	

Приложение 10

Посетила криминалистический отдел военного следственного управления Следственного комитета Российской Федерации по городу Москве