ВОЗМОЖНОСТИ МОБИЛЬНОЙ КРИМИНАЛИСТИКИ

Извлекаем, исследуем,
раскрываем преступления

GROUP-IB

ОГЛАВЛЕНИЕ

Что такое мобильная криминалистика?

Мобильная криминалистика – это наука о криминалистическом исследовании мобильных устройств.

Большинство людей использует в повседневной жизни мобильные девайсы. К ним относятся: сотовые телефоны, смартфоны, планшеты, MP3-плееры, смарт-часы, фитнес браслеты и т.д. В настоящее время подавляющее большинство мобильных устройств работает под управлением операционных систем Android и iOS.

Мобильные девайсы содержат больше персональных данных и иных сведений о их владельцах, чем их компьютеры и ноутбуки.

Они содержат следующие основные типы криминалистических артефактов: контакты (телефонная книга), вызовы, СМС-сообщения, ММС-сообщения, чаты, электронную почту, мультимедиа файлы (графика, видео), данные геолокации, документы, установленные приложения, вредоносные программы и иные артефакты, указывающие на:

- Наличие на мобильном устройстве вредоносной программы;
- Осуществление несанкционированного доступа к мобильному устройству;
- Отправку с него платежных поручений, компрометации данных и т.д.

В цифровой криминалистике исследование мобильных устройств выделяют в отдельное направление по следующим причинам:

- **Данные устройства имеют собственные аппаратные решения, которые отличны от используемых в компьютерах.**
- **Мобильные устройства имеют собственные операционные системы (Android, iOS, Blackberry OS, Windows Mobile), отличные от тех, что используются на серверах, персональных компьютерах и ноутбуках;**
- **Мобильные устройства имеют собственное системное и прикладное программное обеспечение.**

Типы извлечения

Эти группы методов различаются по количеству извлекаемых данных и по трудоемкости работ по их извлечению из мобильных устройств. Для разных мобильных устройств (в зависимости от аппаратной архитектуры устройства, системного программного обеспечения, используемых настроек безопасности) возможно использование одного или нескольких методов извлечения данных.

Основные типы извлечения данных из мобильных устройств

- Логическое извлечение;
- Создание резервной копии мобильного устройства;
- Извлечение файловой системы мобильного устройства;
- Извлечение физического дампа памяти устройства.

16% ЛЮДЕЙ

старше 16 лет ломали свое мобильное устройство (чаще всего, смартфон).

25% ПОВРЕЖДЕНИЙ

всех мобильных устройств приходится на смартфоны, поврежденные в результате попадания устройства в воду.

10 НЕДЕЛЬ

среднее время, через которое iPhone приходит в неисправность после покупки

19%

всех поврежденных мобильных устройств приходится на те, которые были уронены в туалете.

ТИП ИЗВЛЕЧЕНИЯ	ОПИСАНИЕ МЕТОДА	ИЗВЛЕКАЕМЫЕ ДАННЫЕ	ОСОБЕННОСТИ МЕТОДА
Логический	Из устройства извлекаются только основные типы данных, находящиеся на нем в явном виде (исключение составляют базы данных формата SQLite, из которых возможно произвести восстановление удаленных записей)	Возможно восстановление удаленных: - контактов; - вызовов; - СМС–сообщений; - ММС– сообщений; - мультимедиа файлов (графика, видео); - документов; - данных геолокации.	Выявление фактов несанкционированного доступа к данным, находящимся на мобильном устройстве, отправки (и получения) СМС-сообщений платежных операций, осуществленных с помощью исследуемого мобильного устройства.
Создание резервной копии мобильного устройства	Кроме основных типов артефактов извлекаются дополнительные, которые заданы для конкретной модели устройства. Извлечение некоторых данных возможно только при наличии соответствующих настроек операционных систем. Например, в iPhone можно просмотреть электронную почту на устройстве, но письма нельзя экспортировать. Также нельзя извлечь приложения из iPhone, который не подвергали джейлбрейку, что затрудняет идентификацию вредоносных программ на таких устройствах.	Возможно восстановление удаленных: - контактов; - вызовов; - СМС –сообщений; - ММС– сообщений; - чатов; * - электронной почты, если письма хранятся в базе данных формата SQLite. * - мультимедиа файлов (графика, видео); - документов; - данных геолокации; - установленных приложений. * * типы данных, что возможно извлечь только при наличии соответствующих надстроек операционных систем.	Обнаружение фактов несанкционированного доступа к данным, находящимся на мобильном устройстве, отправки (и получения) СМС-сообщений платежных операций, осуществленных с помощью исследуемого устройства. Иногда можно установить, какое вредоносное мобильное приложение было установлено на мобильном устройстве и его функциональные особенности.
Извлечение файловой системы мобильного устройства	Извлекается максимальное число логических артефактов (в том числе, электронная почта, чаты и т.п.). Также как для методов логического извлечения, бэкапов мобильных устройств, с помощью данного метода нельзя восстановить удаленные файлы.	Возможно восстановление удаленных: - контактов; - вызовов; - СМС-сообщений; - ММС-сообщений; - чатов; - мультимедиа файлов (графика, видео); - документов; - электронной почты; - данных геолокации; - установленных приложений.	Обнаружение фактов несанкционированного доступа к данным, находящимся на мобильном устройстве, отправки (и получения) СМС-сообщений платежных операций, осуществленных с помощью исследуемого устройства. Можно определить, какое вредоносное мобильное приложение было установлено на этом устройстве и его функциональные особенности.
Извлечение физического дампа устройства	При этом методе создается полная копия физической памяти устройства и из него возможно восстановление как максимального количества различных артефактов, так и удаленных файлов.	Возможно восстановление удаленных: - контактов; - вызовов; - СМС-сообщений; - ММС-сообщений; - чатов; - мультимедиа файлов (графика, видео); - документов (в том числе, удаленных); - электронной почты; - данных геолокации; - установленных приложений.	Выявление фактов несанкционированного доступа к данным, находящимся на мобильном устройстве, отправки (и получения) СМС-сообщений платежных операций, осуществленных с помощью исследуемого устройства. Можно установить, какое вредоносное мобильное приложение было установлено на этом устройстве и его функциональные особенности, восстановить удаленные файлы и иные артефакты, указывающие на совершение инцидентов ИБ.

Таким образом, максимальное количество криминалистических артефактов можно извлечь из устройства, используя метод создания физического дампа мобильного устройства. Однако, этот метод неприменим в флагманских моделях Android устройств (начиная с Android 6) и iOS-устройств (с версий выше 9.3.5). В данных устройствах применяется дополнительная мера для защиты личных данных владельца устройства – шифрование, что делает невозможным восстановление удаленных файлов и серьезно затрудняет извлечение информации из подобных устройств. Однако, и в этом случае есть возможность оценить, какие данные находились на устройстве. Так, в случае удаления графических файлов и видео, мы не можем восстановить удаленные файлы, однако можем извлечь миниатюры подобных файлов из памяти устройства и оценить, какие изображения они содержали.

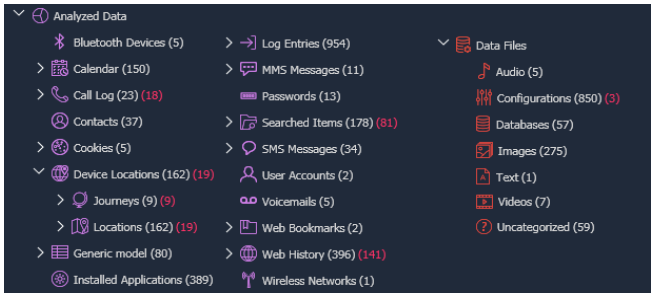
Услуги Group-IB по мобильной криминалистике

Извлечение данных из заблокированных устройств

Достаточно распространенным запросом клиентов является извлечение данных из заблокированного устройства (пин-кодом или графическим паттерном).

Специалисты Лаборатории компьютерной криминалистики Group-IB могут извлечь данные практически из любого подобного, в том числе, и зашифрованного устройства.

Также эта услуга доступна для флагманских мобильных устройств, работающих под управлением операционных систем Android и iOS.



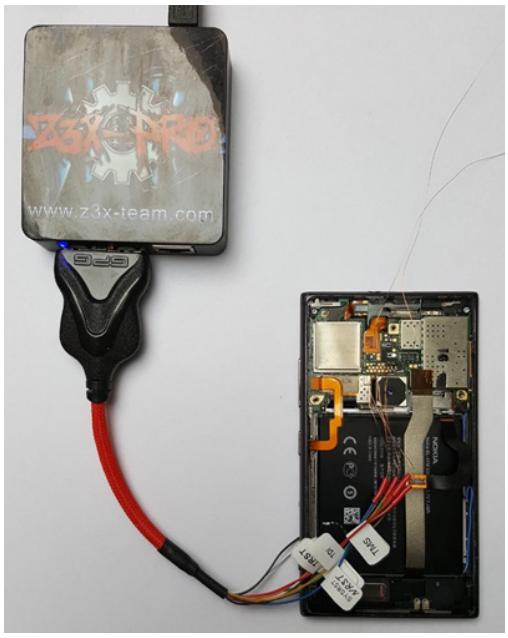
Пример типов данных, извлеченных из заблокированного iPhone (красным цветом указано количество восстановленных данных).

Извлечение данных из поврежденных устройств

Сотрудники Лаборатории криминалистики Group-IB могут восстановить данные практически из любого поврежденного мобильного устройства.

Исключения составляют:

- устройства с разрушенными или отсутствующими микросхемами памяти;
- мобильные устройства под управлением операционных систем iOS и Android с поврежденной платой электроники;
- некоторые иные модели смартфонов.

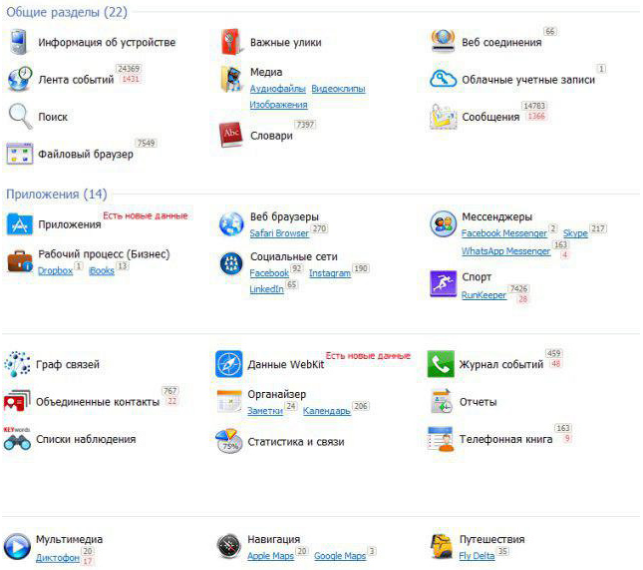


Извлечение данных из поврежденного смартфона.

Криминалистический анализ мобильного устройства

Криминалистический анализ мобильного устройства позволяет извлечь из него максимально возможное число артефактов (в соответствии с примененным методом исследования).

Часто правоохранительные органы и иные частные лаборатории не имеют достаточного оснащения и квалифицированный персонал, который бы мог обеспечить полноту извлечения информации из мобильного устройства. Это приводит к тому, что заказчик (или правоохранительные органы) не имеет полной информации о произошедшем событии и, соответственно, имеет ложное представление о повлекших его причинах.



Пример типов данных, извлеченных из мобильного устройства.
Красным приведены значения восстановленных данных для каждого типа.

Поиск вредоносного ПО и программ слежения

Специалисты Лаборатории криминалистики Group-IB способны обнаружить такие программы, установить их функционал (какие сведения собирает программа на устройстве и куда их передает), зафиксировать факт несанкционированного доступа к данным клиента.

Для функционирования вредоносной программе (например, банковскому трояну) не требуется предоставления ей прав от имени суперпользователя на мобильном устройстве.

Основные источники заражения мобильных устройств:

- Фальшивые приложения;
- Скомпрометированные веб-ресурсы;
- Чаты и соцсети;
- Электронная почта;
- Близкие родственники (могут установить программу мониторинга, полученную из ненадежного источника, что может привести к заражению устройства вредоносным программным обеспечением).

Примеры реальных кейсов Group-IB

«Киберфашисты или 5-й рейх»

В компанию Group-IB обратилось несколько граждан, у которых произошло несанкционированное списание денежных средств с их банковских счетов.
В результате исследования их смартфонов было обнаружено вредоносное мобильное приложение, которое подменяло экран программы «Google Pay», отображая на дисплее устройства аналогичный «Google Pay» интерфейс. Владелец устройства вводил в соответствующие поля этого интерфейса данные его банковской карты (номер карты, данные владельца, информацию об окончании срока действия, CVV-код), после чего эти сведения передавались на сервер злоумышленников.

Все программы имели схожую функциональность и стиль программирования. В результате проведенного расследования были обнаружены хакеры, входившие в группировку «5-й рейх», которые в последующем были задержаны сотрудниками правоохранительных органов.

«Проверка партнера по бизнесу»

Один из наших заказчиков предполагал, что партнер обманывает его насчет того, где он находился в определенные периоды времени. В ходе исследования мобильного устройства партнера наши эксперты обнаружили фитнес-приложение, в базе которого фиксировалось местоположение устройства через каждые две секунды. В результате анализа перемещения устройства разночтений между показаниями партнера и данными из его устройства не обнаружено.

«Самоубийство в воинской части»

В воинской части был обнаружен труп рядового, покончившего жизнь самоубийством. Первоначальной версией следствия было доведение до самоубийства сослуживцами. Получить доступ к данным, находящимся в памяти смартфона самоубийцы, не было возможности, так как устройство было заблокировано паролем.

После разблокировки смартфона и извлечения из него данных специалисты Group-IB установили, что причиной самоубийства был шантаж рядового третьими лицами, угрожающими распространить о нем компрометирующие сведения.

Траектория перемещения мобильного устройства, зафиксированная по данным фитнес-приложения и иных геометок, извлеченных из памяти устройства.

О Лаборатории компьютерной криминалистики Group-IB

Крупнейшая в Восточной Европе Лаборатория компьютерной криминалистики и исследования вредоносного кода предоставляет комплексный набор услуг по предотвращению целевых атак, реагированию на инциденты разной степени сложности, фиксации цифровых доказательств и криминалистическому исследованию, используя компетенции сертифицированных экспертов и собственные технологии Group-IB, признанные во всем мире.

55 000+
часов реагирования на инциденты

GREM | GCFA
международные сертификаты наших специалистов

15+
стран, в которых проводились обучения экспертами Group-IB

О компании Group-IB

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

Многолетний опыт Group-IB воплощен в системе раннего обнаружения киберугроз – линейке высокотехнологичных продуктов для мониторинга, выявления и предупреждения киберугроз, основанной на самых актуальных данных кибермразведки и глубоком анализе реальных хакерских атак.

15 лет
практического опыта

1000+
расследований по всему миру

$300 млн
было возвращено клиентам благодаря нашей работе

300+
специалистов и разработчиков

Официальный партнёр EUROPOL и INTERPOL

INTERPOL | EUROPOL

Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester, Gartner и IDC

IDC | GARNER | FORRESTER

Рекомендована Организацией по Безопасности и Сотрудничеству в Европе

OSCE

Наши продукты

- **Threat Intelligence**
- **Threat Detection System (TDS)**
- **Secure Bank**
- **Secure Portal**
- **Brand Protection**

Аудит и Оценка рисков

- Тестирование на проникновение
- Исследование уязвимостей
- Выявление фактов компрометации
- Имитация целевых атак (Red Teaming)
- Проверка готовности к реагированию на инциденты (Pre-IR)
- Оценка соответствия

Threat Hunting и Реагирование

- Проактивное выявление угроз
- 24/7 мониторинг и реагирование
- Реагирование “по подписке” *(целевые атаки, утечки и др.)*

Криминалистика

- Криминалистическое исследование
- Анализ вредоносного кода

Расследования

- Целевые атаки
- Инциденты информационной безопасности
- Финансовые и корпоративные преступления

Свяжитесь с нами, чтобы узнать больше

+7 (495) 984 33 64 info@group-ib.ru www.group-ib.ru