МОБИЛЬНЫЙ КРИМИНАЛИСТ ДЕТЕКТИВ 11.2

ФЕВРАЛЬ 2019

457 уникальных приложений

9250+ версий приложений

26000+ устройств

64 облачных сервиса

Физический образ из устройств Qualcomm

Извлечение физического образа - важная задача экспертов при исследовании данных из современных мобильных устройств, так как физический дамп содержит в себе информацию абсолютно идентичную той, что хранится на устройстве.

“Мобильный Криминалист” включает в себя целый ряд инструментов, позволяющих извлекать физические образы из различных мобильных устройств. А в версии 11.2 такая функция появляется и у инструмента “Qualcomm EDL извлечения”, при помощи которого теперь можно извлечь физический образ из устройств на чипсетах Qualcomm MSM8909, MSM8916, MSM8952.

Второй не менее важной проблемой исследователей является шифрование данных, поскольку, даже если физический образ извлечен успешно, а данные в нем зашифрованы, их анализ становится невозможным. Наш продукт помогает с расшифровкой данных и из Qualcomm устройств . Так, уже в версии 11.2 при извлечении зашифрованного образа устройства на чипсете Qualcomm MSM8909, программа подбирает к нему пароль для успешной дешифровки данных.

Новые типы данных Telegram

Не так давно мессенджер Telegram поменял свой API, и наша команда не упустила это из виду. Мы не только обновили поддержку этого облачного сервиса, но и добавили новые типы извлекаемых данных. Теперь становится доступным извлечение и анализ данных опросов, списка звонков, сообщений от ботов, альбомов.

Apple Health

Мы продолжаем развитие направления в облачной криминалистике, связанного с данными фитнес-трекеров. Новая версия “Мобильного Криминалиста” поддерживает облачный сервис Apple Health.
Этот сервис достаточно популярен среди любителей яблочных гаджетов, а данные, которые он хранит, нередко становятся доказательствами при расследовании преступлений за рубежом. Из Apple Health можно извлечь информацию об учетной записи, тренировках, подключенных устройствах, жизненно важных показателях (пульс, давление, дыхание, температура и др.), здоровье, сне и др.

iOS

ОБНОВЛЕННЫЕ

Mail.Ru - Email App (9.15)
Facebook Messenger (198.0)
Viber (10.0)
TamTam (2.5.5)
Azar Messenger (1.33.1)
Google Duo (45.0)
Facebook (204.0)
Google Translate (5.26.0)

НОВЫЕ

VSCO (97.0)
CoverMe (3.0.1)
BlaBlaCar (5.30.0)

Android

ОБНОВЛЕННЫЕ

Mail.Ru - Email App (8.7.0)
Facebook Messenger (199.1.0.21.112)
Viber (10.0.0.14)
TamTam (2.4.0)
Azar Messenger (3.38.0)
Firefox (64.0.2)
Google Chrome (71.0.3578.99)
Google Keep (5.0.503.03.40)
Yahoo! Mail (5.36.0)
Flipboard (4.2.8)
Google Translate (5.26.0)

НОВЫЕ

BlaBlaCar (5.21.0)

BlaBlaCar

В конце 2018 года в России началась работа над ограничением функционирования приложения BlaBlaCar, крупного онлайн-сервиса поиска попутчиков. Обеспокоенность правозащитников вызвана участившимися несчастными случаями, происходящими как с водителями, так и с пассажирами.

Для расследования инцидентов важно иметь доступ к информации в облачном сервисе приложения BlaBlaCar, который впервые в отрасли предоставляет “Мобильный Криминалист”.

Программа извлекает информацию об учетной записи, данные о поездках (маршруты, способ оплаты и др.), информацию о водителях и попутчиках, чаты и отзывы, относящиеся к поездке.

TamTam

TamTam – российский мессенджер от Mail.Ru Group, разработанный в 2017 году. Имеет более 6 миллионов пользователей, число которых активно возросло после начала блокировки мессенджера Telegram.
В “Мобильном Криминалисте” 11.2 доступно извлечение данных мессенджера как из облачного сервиса, так и из приложения на iOS и Android устройствах.

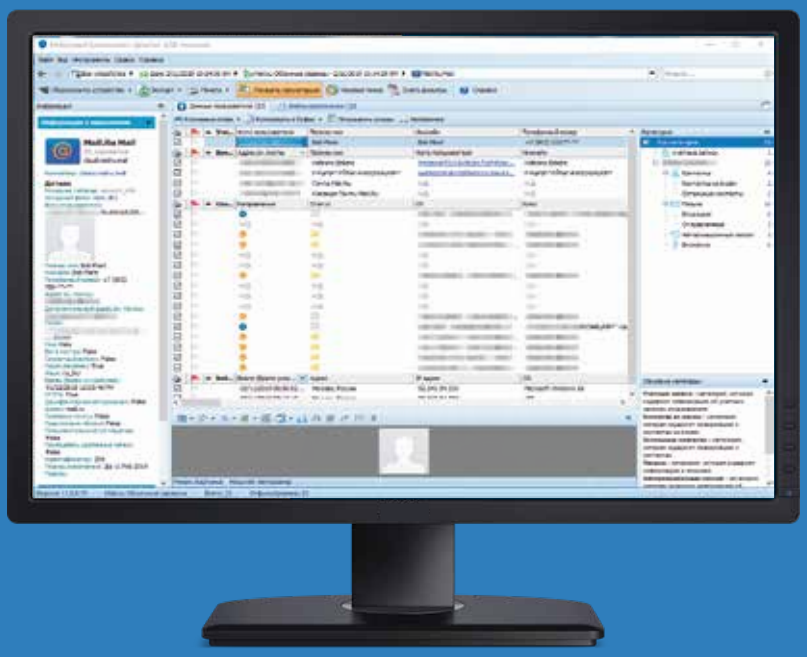
Авторизоваться в облачном сервисе можно по логину/паролю от соц.сети Одноклассники, номеру телефона или токену. После чего программа может извлечь криминалистически важные данные, такие как список контактов, чаты, списки участников групповых чатов, каналы, на которые подписан владелец аккаунта, звонки, авторизационные сессии. Из приложения доступно извлечение информации об аккаунте, контактов, информации о групповых чатах (включая список участников), чатов, каналов, звонков.

Почтовый клиент Mail.ru

Mail.ru - крупнейший в России бесплатный почтовый клиент, принадлежащий компании Mail.Ru Group.

Он позволяет использовать общие учетные записи для всех предоставляемых сервисов: Мой Мир, Знакомства, Одноклассники и др. В версии 11.2 мы обновили поддержку приложения и добавили облачный сервис почтового клиента Mail.ru.

Авторизация в сервисе возможна с помощью логина/пароля, токена или кода из SMS. После этого нам открывается доступ к списку контактов, содержимому писем, списку авторизационных сессий, данным учетных записей и др.



Parrot

Согласно исследованию консалтингового агентства J’son & Partners, в 2017 году беспилотники Parrot совместно с DJI были лидерами на мировом рынке квадрокоптеров для потребительских нужд. Внутренняя память этих дронов среди всей совокупности информации хранит самые важные данные - логи полетов, которые способны рассказать не только о маршруте передвижения дрона, но также о времени его полета, метаданных, связанных с грузом, и о многом другом. В версии 11.2 доступен импорт логов полета Parrot.

ООО «Оксиджен Софтвер», Россия, 105064, Москва, Нижний Сусальный пер., д. 5, стр. 8Б,
+7-495-222-9277
мобильный-криминалист.рф