



МОБИЛЬНЫЙ КРИМИНАЛИСТ ДЕТЕКТИВ **11.3**



АПРЕЛЬ 2019



461 уникальное приложение



9600+ версий приложений



27000+ устройств



67 облачных сервисов

Android KeyStore

Android KeyStore – системное хранилище уникальных программных и аппаратных ключей шифрования таких приложений, как Signal, Threema, Amazon Alexa и др. на устройствах с операционной системой Android.

Мобильный Криминалист первым в отрасли начал извлекать и расшифровывать ключи из Android KeyStore! Полученные ключи шифрования предоставляют доступ к полному объему данных приложения, для которого они предназначены. В настоящее время данная возможность реализована для приложения Signal. С каждым релизом список приложений, поддерживающих эту функциональность, будет пополняться.

Расшифровка физических образов

Аппаратное шифрование – серьезный барьер для исследования информации из современных мобильных устройств, так как аппаратные ключи шифрования, как правило, достаточно трудно извлечь, а без них невозможно произвести дешифровку полученных данных.

Мы нашли решение и первые в области мобильной криминалистики предоставляем извлечение и расшифровку физического образа устройств на чипсетах MT 6737, защищенных аппаратным шифрованием. Даже если на устройстве активирован режим Secure Startup, это не будет препятствовать расшифровке данных, поскольку программа позволяет ввести необходимый пароль. Полученный физический образ содержит полную файловую структуру исследуемого устройства.

ОБНОВЛЕННЫЕ

WhatsApp (2.19.30)
Telegram (5.4.1)
Viber (10.3)
Facebook (210.0)
VK (5.9.1)
OK (7.50.1)
Freeflight Pro (5.2.4)
Google Photos (4.10)

НОВЫЕ

Freeflight 6 (6.4.2)
Yandex.Taxi (4.66)
Telegram X (5.0.17)

ОБНОВЛЕННЫЕ

WhatsApp (2.19.86)
Telegram (5.3.1)
Signal (4.35.3)
Viber (10.3)
VK (5.24)
OK (19.3.26)
Freeflight Pro (5.2.4)
Google Photos (4.10)

НОВЫЕ

Freeflight 6 (6.4.1)
Yandex.Disk (4.08)

iOS

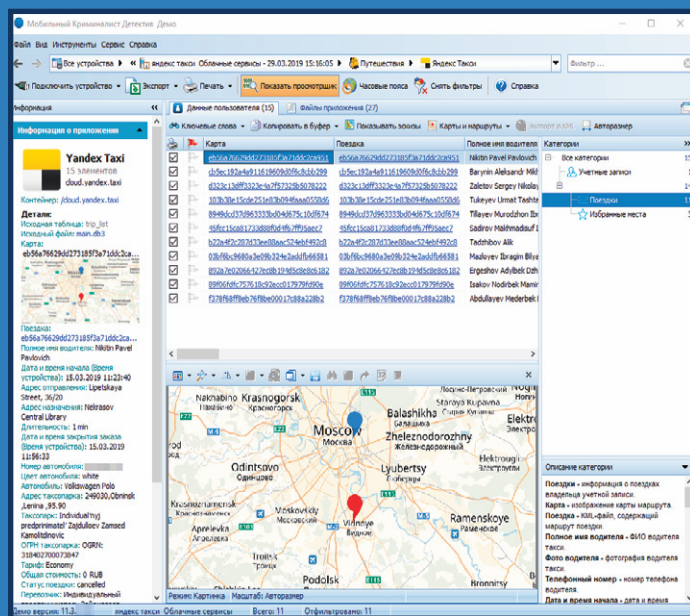
Android

Яндекс. Такси

Яндекс.Такси – самый популярный в России сервис онлайн-заказа такси. В версии 11.3 открыт доступ к данным приложения этого сервиса на iOS-устройствах и его облачного хранилища. Также добавлено извлечение новых категорий данных из Android-устройств – программа извлекает сохраненные адреса, информацию об учетной записи, кредитных картах, поездках и др.

Для iOS-устройств доступны данные учетной записи, информация о последней поездке и координаты последнего местоположения владельца устройства.

После авторизации по номеру телефона и коду из SMS или по токenu из облачного сервиса Яндекс.Такси извлекаются персональные данные владельца учетной записи, информация о поездках, водителях, автомобилях и избранных местах.



Apple Maps

Картографический сервис от компании Apple впервые появился на iOS-устройствах в версии 6 и заменил собой сервис Google Maps, который до этого предустанавливался на iPhone.

Мобильный Криминалист 11.3 реализует поддержку приложения и облачного сервиса Apple Maps. Из приложения можно извлечь избранные адреса, историю поиска мест и маршруты, построенные пользователем.

После авторизации по логину/паролю или по токenu от учетной записи Apple эксперты могут извлечь информацию о владельце учетной записи, гео-координаты и фотографии мест из истории поиска и избранных точек из облачного хранилища данного приложения.

Android XRY

Вы получили физический образ с помощью другой программы, но хотели бы извлечь из него больше данных и воспользоваться нашим аналитическим функционалом для их изучения? Мы добавили для этого новую возможность! Начиная с версии 7.11, программное обеспечение XRY зашифровывает извлеченные физические образы устройств при их экспорте. Мобильный Криминалист 11.3 позволяет не только импортировать данные физические образы, но и расшифровывает их.

Мобильный Криминалист Скаут

В версии 11.3 произведено масштабное обновление модуля Скаут. Мы переработали механизм поиска учетных данных, и теперь можно выбрать подходящий для вас режим: Быстрый, Оптимальный или Полный. При выборе режима Быстрый, поиск производится по заранее известным путям, как в предыдущих версиях программы. Оптимальный поиск осуществляется в заранее известных папках на фиксированную глубину, а Полный поиск исследует всю файловую систему ПК.

Также мы добавили функцию поиска и сохранения резервных копий iTunes. Во вкладке с резервными копиями выводится информация об имени устройства, шифровании, пароле, версии iOS и iTunes, IMEI, номере телефона, и др.

Наконец, реализован поиск паролей от учетной записи облачного сервиса My Parrot Cloud.

