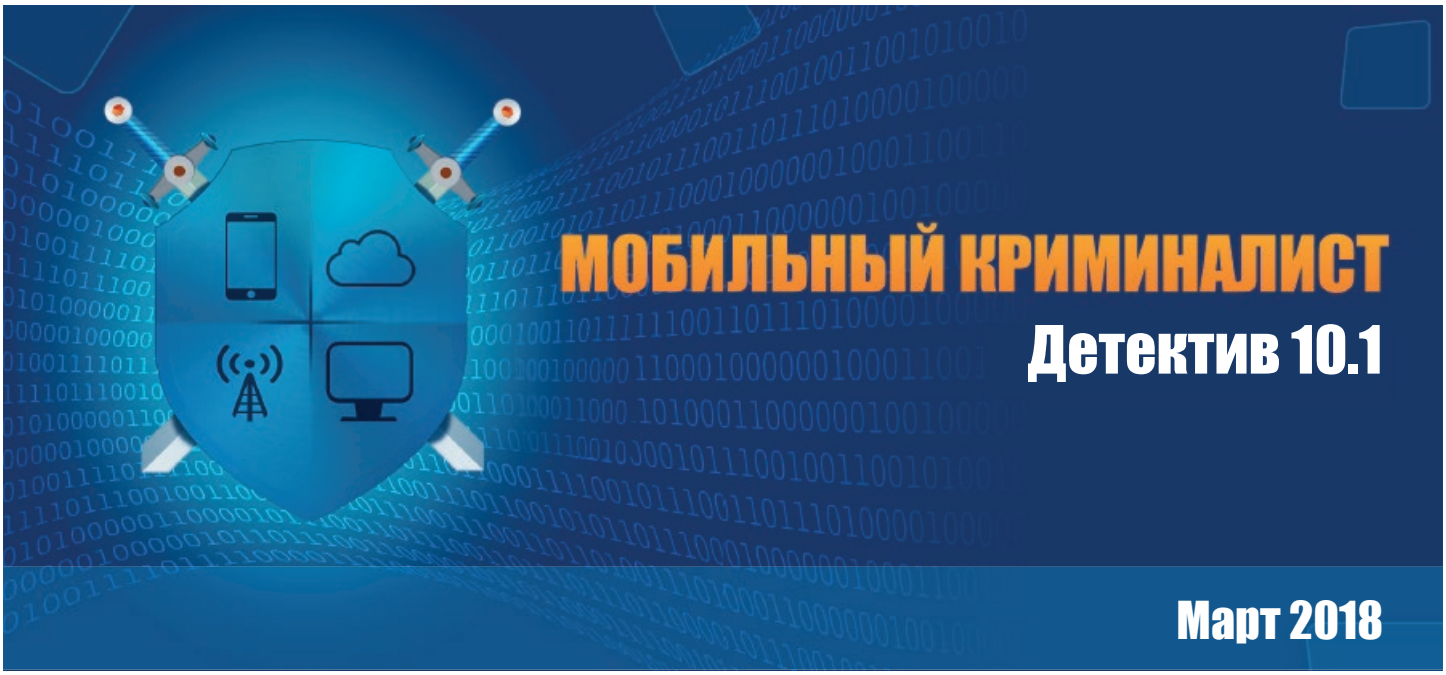
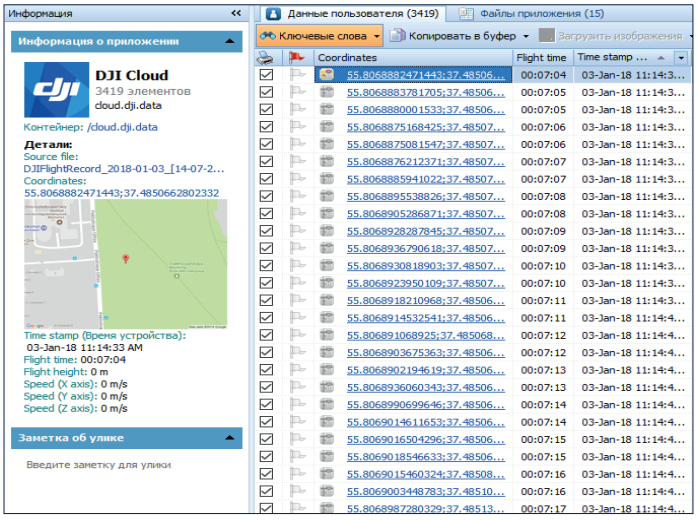


ОБЛАЧНЫЕ ХРАНИЛИЩА DJI

С сентября 2017 года программа «Мобильный Криминалист» поддерживает извлечение данных из дронов, а также мобильных приложений для управления этими устройствами. Однако некоторые данные передаются через интернет и хранятся в учетной записи пользователя на облачном сервере. Новая версия 10.1 позволит эксперту при помощи пароля или токена получить доступ к облачному серверу, используемому дронами, и извлечь следующие данные:

- информацию об аккаунте (имя пользователя, фото, биография, адрес веб-сайта, страну проживания, дата создания учетной записи, а также связанные с ней соцсети);
- данные дрона (модель, общее время полета, расстояние, количество совершенных полетов, посещенные аппаратом страны, максимальная скорость, высота, расстояние, длительность полета и т.д.);
- историю полетов, включая геоданные, временные отметки, скорость, высоту полетов и прочую информацию.



ИЗВЛЕЧЕНИЕ ANDROID УСТРОЙСТВ

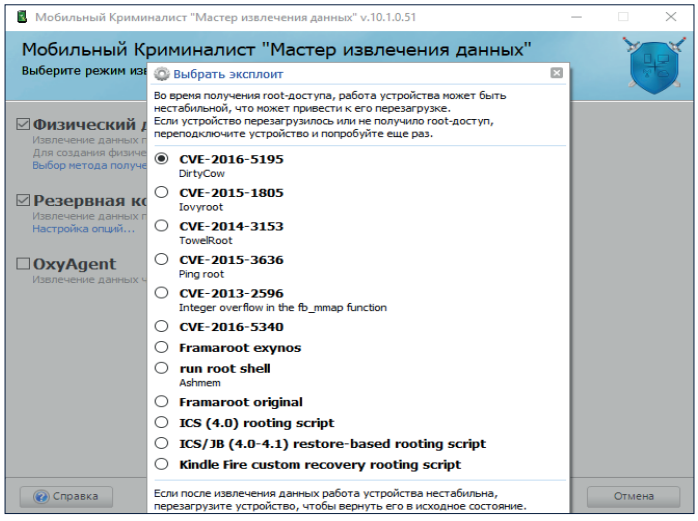
В «Мобильном Криминалисте» 10.1 были значительно улучшены как физические, так и логические методы извлечения данных из устройств под управлением ОС Android.

Прежде всего, был добавлен новый алгоритм получения прав суперпользователя, основанный на эксплойте DirtyCOW. Теперь получить рут-права можно на значительно большем количестве устройств до версии Android 6.0 включительно.

Более того, в новом «Мастере Извлечения Данных» в ручном режиме физического извлечения эксперт может сам выбрать необходимый эксплойт из списка доступных. В автоматическом режиме извлечения такой выбор не предоставлен, и подбор эксплойта осуществляется самой программой.

Третье нововведение – это возможность выбирать параметры снятия резервной копии Android. Теперь эксперты могут задавать параметры извлечения приложений из устройств и карты памяти.

И наконец, были значительны улучшены функциональность и интерфейс утилиты OxyAgent, применяемой для логического извлечения данных.



ООО «Оксиджен Софтвер», Россия, 105064, Москва,
Нижний Сусальный пер., д. 5, стр. 8Б, +7 495 2229277

Мобильный Криминалист Детектив 10.1

ПРИЛОЖЕНИЯ

420+ уникальных приложений

6200+ версий приложений

НОВЫЕ

IOS

Jaxx Blockchain Wallet (1.3.9)
Health (9.3.3)
LetGo (1.22.3)

ANDROID

BreadWallet (171)
Jaxx Blockchain Wallet (1.3.7)

WINDOWS PHONE

WeChat (6.0.8.17)

ОБНОВЛЕННЫЕ

IOS

Facebook Messenger (153.0)
Google Translate (5.17.0)
Instagram (32.0)
Skype (8.15)
Twitter (7.17.1
Viber (8.2.1)
WhatsApp (2.18.22)

ANDROID

Facebook (159.0.0.38.95)
Instagram (32.0)
Kik (12.4.1.19850)
Line (8.2.1)
Twitter (7.32.0)
Yahoo Mail (5.24.7)
Youtube (13.05.52)
И многие другие!

ОБЛАЧНЫЕ ДАННЫЕ

46 облачных сервисов

НОВЫЕ

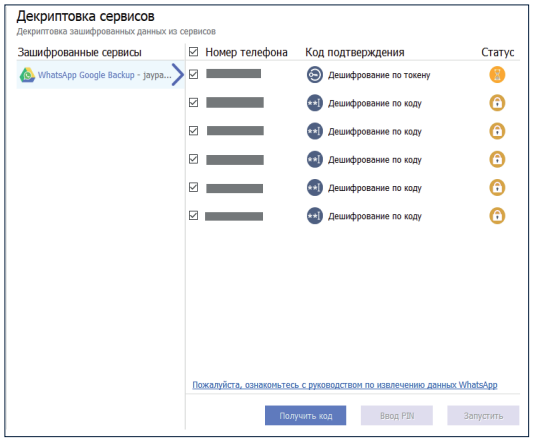
DJI drone

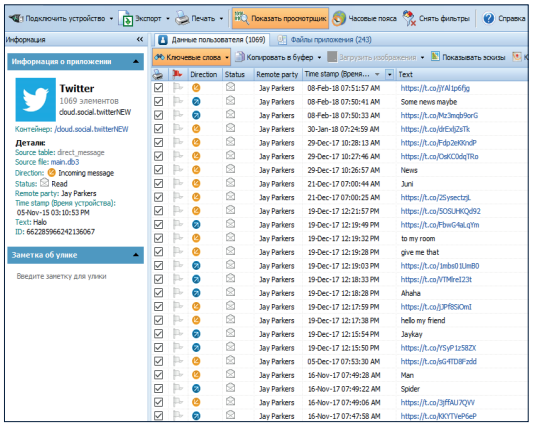
ОБНОВЛЕННЫЕ

Dropbox
Twitter
WhatsApp

РАСШИФРОВКА WHATSAPP

«Мобильный Криминалист» 10.1 теперь может расшифровывать данные резервной копии WhatsApp посредством токена авторизации. При отсутствии файла с ключом, необходимого для расшифровки, используется токен авторизации WhatsApp, что позволяет программе «Мобильный Криминалист», не оставляя каких-либо следов, расшифровать резервные копии, сохранённые в сервисах iCloud и Google Cloud.



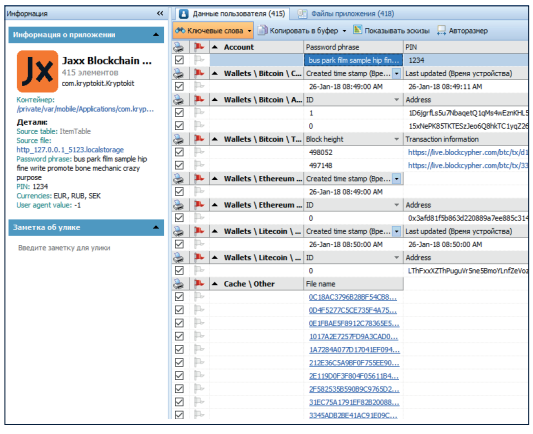


ДАННЫЕ ИЗ TWITTER

Были значительно улучшены алгоритмы извлечения данных из облачной учетной записи Twitter. Теперь новая версия программы «Мобильный Криминалист» поддерживает 2FA и авторизацию по токену. Новая версия модуля «Облачные сервисы» позволяет извлечь дополнительную информацию: личные сообщения, информацию о заблокированных и игнорируемых пользователях, листы и многое другое.

ПРИЛОЖЕНИЯ ДЛЯ КРИПТОВАЛЮТЫ

В «Мобильном Криминалисте» версии 10.1 представлены возможности расшифровки данных приложений для работы с криптовалютой, установленных на устройствах Apple iOS и Android. Благодаря этому эксперты смогут извлекать ценные данные из приложений BreadWallet и Jaxx Blockchain Wallet, включая информацию об учетной записи, виртуальном кошельке и транзакциях, а также кэшированные данные.



ПОДДЕРЖКА ФОРМАТА GPX

Модуль «Карты» теперь поддерживает импорт и визуализацию геокоординат в формате GPX. Этот формат широко используется мобильными приложениями для хранения данных о маршрутах.

ПОИСК ПО НАБОРАМ ХЭШ-ФУНКЦИЙ

Добавлена возможность поиска файлов по наборам хэш-функций (MD5, SHA1, SHA256), что позволит экспертам быстрее найти подозрительные файлы, связанные с незаконной деятельностью пользователя.

ООО «Оксиджен Софтвер», Россия, 105064, Москва,
Нижний Сусальный пер., д. 5, стр. 8Б, +7 495 2229277