ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

ИЗМЕНЕНИЯ В НОВОЙ ВЕРСИИ
Август 2020

Elcomsoft iOS Forensic Toolkit

Версия 6.30

Elcomsoft iOS Forensic Toolkit помогает экспертам-криминалистам осуществлять физическое и логическое извлечение данных из устройств под управлением Apple iOS путем создания и дешифрования образа файловой системы устройства и извлечения секретов устройства (паролей, ключей шифрования и защищённых данных).

Краткий обзор

В обновлении Elcomsoft iOS Forensic Toolkit 6.30 расширен список версий iOS, для которых доступно извлечение образа файловой системы без джейлбрейка. Извлечение посредством агента-экстрактора теперь доступно для всех 64-битных устройств iPhone и iPad под управлением всего спектра версий iOS 9. Кроме того, добавлена возможность извлекать из файловой системы только данные пользователя, пропуская системные файлы и библиотеки.

Важные изменения

Полная поддержка iOS 9 без установки джейлбрейка

В Elcomsoft iOS Forensic Toolkit 6.30 мы расширили поддержку старых версий iOS. В новой версии инструментария добавлена поддержка расшифровки Связки ключей и извлечения файловой системы для 64-разрядных устройств Apple, работающих под управлением всех версий iOS 9. Поддержка старых версий iOS важна для работников криминалистических лабораторий, в которые поступают устройства, многие из которых не обновлялись годами или ни разу с момента приобретения.

Важно отметить, что поддерживаются все версии iOS 9 на всех устройствах, для которых они были доступны. В число поддерживаемых устройств вошли смартфоны iPhone 5s, iPhone 6 и 6 Plus, iPhone 6s и 6s Plus. Также поддерживается первая версия iPhone SE, выпущенная с iOS 9.3. Наконец, новый метод извлечения работает на планшетах iPad Air, iPad Air 2, iPad Mini 2 - 4, а также на первом поколении iPad Pro.

Для установки агента необходимо использовать Apple ID, зарегистрированный в Программе разработчика Apple. Подробнее об этом в статье Мобильная криминалистика: учётные записи Apple для разработчиков.

Новый режим извлечения данных пользователя

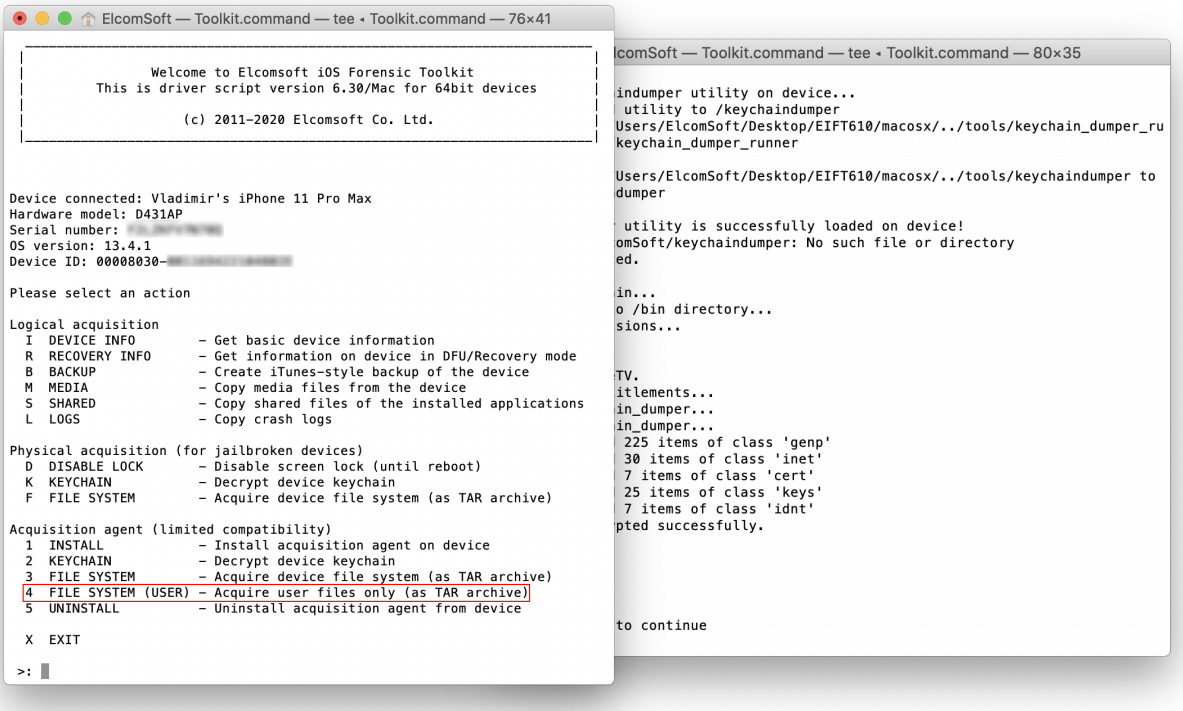
В текущем обновлении представлен и новый режим извлечения данных. В новом режиме из файловой системы извлекаются только данные пользователя, но не файлы операционной системы, что экономит время и место на диске. В системном разделе iOS содержатся исполняемые файлы и библиотеки, необходимые для работы операционной системы. За исключением случаев с использованием джейлбрейка, содержимое системного раздела совпадает на устройствах одной и

той же модели, работающих под управлением одной и той же версии iOS, и не представляет ценности для расследования.

Основные преимущества нового метода – ускорение извлечения данных и упрощение их анализа. Так для iPhone малой ёмкости новая опция может ускорить извлечение в два-три раза. На устройствах с большей ёмкостью новый метод существенно упрощает работу с данными.

Список изменений в версии 6.30

- Добавлена полная поддержка (извлечение файловой системы и Связки ключей) для iOS 9 (агент-экстрактор без джейлбрейка)
- Добавлена возможность извлечения только пользовательской области файловой системы (системные файлы не извлекаются)



Дальнейшие действия

1. Всем активным пользователям Elcomsoft iOS Forensic Toolkit предлагается загрузить новую версию 6.30 с сайта компании. Для этого необходимо ввести действующий регистрационный ключ в онлайн-форме https://www.elcomsoft.com/key.html.
2. Пользователи, у которых истёк срок действия лицензии Elcomsoft iOS Forensic Toolkit, могут продлить свою лицензию по соответствующей цене, которую можно узнать на сайте, введя регистрационный ключ в онлайн-форме (https://www.elcomsoft.com/key.html).

Свяжитесь с нами по электронной почте sales@elcomsoft.com для получения более подробной информации по обновлению или продлению лицензии.