

Elcomsoft iOS Forensic Toolkit 2.10: поддержка iOS 9.3.3 и логического извлечения данных



Москва, Россия – 11 августа 2016 - Компания «Элкомсофт» обновляет криминалистический инструментарий для извлечения данных из устройств под управлением Apple iOS. В новой версии продукта добавлена совместимость с последними версиями iOS 9.2-9.3.3. Кроме того, в продукте появился режим логического извлечения данных, результатом работы которого является резервная копия данных устройства в формате iTunes.

*«Более четырёх месяцев эксперты не могли получить низкоуровневый доступ к iPhone и iPad с актуальными версиями iOS», комментирует **Владимир Каталов**, президент компании «Элкомсофт». «Выход jailbreak для актуальных версий системы позволил нам разработать механизм низкоуровневого извлечения данных. С развитием безопасности iOS мы прогнозируем дальнейшее увеличение срока, который будет проходить между обновлением ОС и выходом jailbreak. Чтобы дать возможность экспертам извлекать данные из актуальных устройств, jailbreak для которых не может быть установлен, мы внедрили альтернативный механизм доступа к данным через логическое извлечение.»*

Для проведения логического извлечения данных установка iTunes не требуется. Данные сохраняются в формате iTunes. Для авторизации устройства, заблокированного неизвестным паролем, могут быть использованы lockdown-файлы, извлечённые из компьютера пользователя. Процедура физического извлечения требует разблокирования устройства и установки jailbreak.

Логическое извлечение данных

Для работы [iOS Forensic Toolkit](#) со всеми современными устройствами (начиная с iPhone 4s) требуется установка jailbreak. С развитием операционной системы iOS получение низкоуровневого доступа становится всё сложнее, отнимая всё больше времени у разработчиков. Актуальные версии iOS 9.x оставались без jailbreak больше четырёх месяцев. С учётом этого можно прогнозировать дальнейшее увеличение срока, который будет проходить от выхода обновления ОС до разработки работоспособного jailbreak.

В то же время, эксперты правоохранительных органов нуждаются в актуальной информации в сжатые сроки. С этой целью «Элкомсофт» встроили в продукт iOS Forensic Toolkit возможность логического извлечения данных, которая не требует установки на устройство jailbreak. Если устройство заблокировано неизвестным паролем, продукт может использовать для разблокировки lockdown-файлы, создаваемые на компьютере пользователя для упрощения авторизации. Файлы Lockdown действуют до первой перезагрузки устройства.

Данные, полученные в результате процесса логического извлечения, можно проанализировать в [Elcomsoft Phone Viewer](#) или сторонних приложениях, поддерживающих формат данных iTunes. Если полученная резервная копия зашифрована неизвестным паролем, нужно использовать [Elcomsoft Phone Breaker](#) для подбора пароля и расшифровки данных.

Физическое извлечение данных на iOS 9.2-9.3.3

Для актуальных версий iOS (9.2-9.3.3) вышел jailbreak от команды Pangu. В iOS Forensic Toolkit 2.10 добавлена поддержка физического извлечения данных для последних версий операционной системы при условии установки jailbreak. Инструкции по его установке доступны на англоязычном сайте Pangu <http://en.pangu.io/help.html>

Физическое извлечение доступно для всех актуальных устройств под управлением iOS с установленным jailbreak. Для смартфонов и планшетов, оснащённых 64-битными процессорами (iPhone 5s/6/6s/Plus и т.п.) дополнительно требуется отключить блокировку паролем, для чего потребуются ввести пароль или PIN-код пользователя. Кроме того, при физическом извлечении из 64-разрядных устройств остаётся недоступной расшифровка keychain - который в новой версии продукта стало возможным извлечь и расшифровать с помощью процесса логического извлечения.

О продукте Elcomsoft iOS Forensic Toolkit

[iOS Forensic Toolkit 2.10](#) – мощный инструмент криминалистического анализа, не имеющий прямых аналогов. Продукт используется следственными и правоохранительными органами для извлечения данных, хранящихся в мобильных устройствах, с целью последующего криминалистического анализа. iOS Forensic Toolkit позволяет экспертам производить сбор информации и проводить судебные и компьютерно-технические экспертизы устройств iPhone, iPad и iPod производства компании Apple, работающих под управлением iOS версий с 3 по 9.3.3 включительно.

Благодаря поддержке извлечения данных как физическим, так и логическим способом, [iOS Forensic Toolkit](#) с наибольшей вероятностью предоставит доступ к информации, хранящейся в поддерживаемых устройствах. Продукт обеспечивает целостность и неизменность исследуемых данных. С помощью [iOS Forensic Toolkit](#) специалисты могут получить доступ к расшифрованному образу файловой системы устройства, расшифровать коды, пароли и прочую защищённую информацию. Доступ к основному массиву данных осуществляется в реальном времени.

Поддержка 64-разрядных устройств является уникальной возможностью продукта, не имеющей аналогов на рынке. С её помощью доступно извлечение данных из современных устройств поколений iPhone 5S/6/6S/Plus, iPad Air, mini 2 и более новых.

О компании «ЭлкомСофт»

Компания [«ЭлкомСофт»](#) – российский разработчик программного обеспечения и поставщик услуг в области восстановления паролей и данных. Решения компании «ЭлкомСофт» используются корпорациями, входящими в список Fortune 500, а также правительственными организациями, правоохранительными органами и спецслужбами по всему миру. Компания «ЭлкомСофт» имеет статус сертифицированного партнера Microsoft (Microsoft Gold Certified Partner) и Intel (Intel Software Partner). Компания основана в 1990 году, головной офис «ЭлкомСофт» находится в Москве.