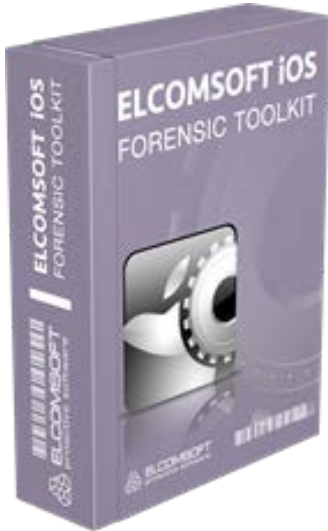


## iOS Forensic Toolkit 3.0 с поддержкой iOS 10 и 11



Москва, Россия – 20 февраля 2018 - компания «Элкомсофт» выпускает крупное обновление [Elcomsoft iOS Forensic Toolkit](#), продукта для криминалистического анализа мобильных устройств под управлением Apple iOS. В версии 3.0 появилась возможность физического извлечения данных из ранее не поддерживаемых версий iOS 10, а также iOS 11 вплоть до версии 11.1.2. Таким образом, в последней редакции инструментария физическое извлечение данных поддерживается для всех совместимых комбинаций аппаратного и программного обеспечения, работающих под управлением всех версий iOS 10 и iOS 11 вплоть до iOS 11.1.2. Для работы инструментария требуется установка jailbreak.

Кроме того, в [iOS Forensic Toolkit 3.0](#) появился режим извлечения локальных данных ряда приложений без установки jailbreak. Для извлечения требуется разблокировать устройство при помощи пароля блокировки, сканера лица или датчика отпечатков пальцев. Из заблокированных устройств данные приложений могут быть извлечены посредством lockdown-файла.

### Поддержка iOS 10 и 11

Физическое извлечение данных из устройств под управлением iOS требует низкоуровневого доступа, который обеспечивается через установку jailbreak. Выход работоспособных инструментов jailbreak для свежих версий iOS позволил разработчикам Элкомсофт получить неограниченный доступ к физическому накопителю и файловой системе устройств под управлением уязвимых версий iOS, скопировать и расшифровать данные. В последней версии инструментария поддерживаются все версии iOS 10 без исключения, а также сборки iOS 11 с 11.0 по 11.1.2 включительно.

Для старых устройств, оснащённых 32-разрядными процессорами (таких, как iPhone 4s, 5 и 5c) эксперты смогут получить доступ к полностью расшифрованному образу раздела данных устройства, а также к расшифрованному защищённому хранилищу keychain независимо от установленного класса защиты для отдельных записей.

Для современных 64-битных устройств, оснащённых защитой Secure Enclave, iOS Forensic Toolkit извлекает полный образ файловой системы, включая данные из защищённых областей приложений, чаты, текстовые и почтовые сообщения, журналы системных событий и многое другое.

По сравнению с логическим извлечением через резервные копии, с помощью физического анализа дополнительно доступны такие данные, как временные файлы веб-браузера, подробная история местоположения, сообщения электронной почты, а также данные приложений, запретивших резервное копирование. Также доступна история переписки через программы мгновенного обмена сообщениями, включая защищённые приложения Telegram, Signal, WhatsApp, Skype и Facebook Messenger.

### **Извлечение данных приложений**

Для устройств, на которые невозможна установка jailbreak, добавлена возможность извлечения данных из многих приложений. Извлекаются локальные копии документов из мобильных приложений Adobe Reader и Microsoft Office, база данных паролей MiniKeePass, файлы и документы из многих других приложений. Для извлечения этих данных необходимо разблокировать устройство либо использовать lockdown-запись.

### **Совместимость**

[Elcomsoft iOS Forensic Toolkit 3.0](#) работает на компьютерах под управлением Windows и macOS. Возможность извлечения данных из устройств под управлением iOS зависит от типа устройства и установленной версии iOS. Физическое извлечение данных доступно только после установки jailbreak. Поддерживаются все версии iOS 10, а также iOS 11.0 - 11.1.2. Для всех прочих устройств поддерживается логическое извлечение данных.

## О продукте Elcomsoft iOS Forensic Toolkit

[iOS Forensic Toolkit](#) – 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 11 включительно.

Благодаря поддержке метода физического извлечения данных, iOS Forensic Toolkit предоставляет самый полный 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/7/8/Plus, iPhone X и всех версий iPad.

## 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» является членом Российской Криптологической Ассоциации, 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. Для получения более подробной информации посетите <http://www.elcomsoft.ru>