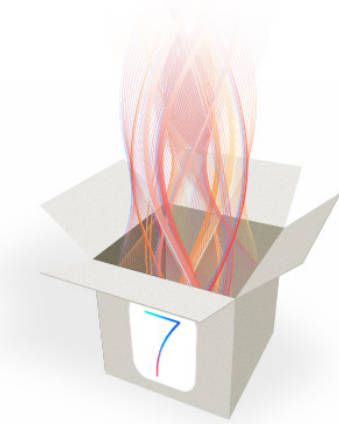


## Криминалистический анализ iOS 7: извлечение данных из защищённого хранилища keychain



Москва, Россия, 2 октября 2013 - Компания «Элкомсофт» обновляет [Elcomsoft Phone Password Breaker](#), добавив поддержку новой операционной системы iOS 7. В новой версии продукта стало возможным извлекать информацию и проводить криминалистический анализ данных, извлечённых из устройств, работающих под управлением последней версии мобильной операционной системы от Apple. Продукт расшифровывает локальные копии данных устройств iPhone, iPad и iPod Touch под управлением iOS 7 и всех предыдущих версий операционной системы, а также извлекает информацию из «облачного» хранилища iCloud.

Программа компании «Элкомсофт» - первый в мире криминалистический продукт, способный расшифровать данные из защищённого хранилища keychain в формате новой операционной системы. В защищённом хранилище доступны такие данные, как пароли от электронной почты и учётных записей приложений, регистрационные данные социальных сетей и учётные записи веб-сайтов.

В новой версии продукта расширена возможность выборочного доступа к пользовательским данным, хранящимся в «облачном» сервисе Apple iCloud. Для выборочного скачивания доступны множество новых категорий данных. Последняя версия Elcomsoft Phone Password Breaker поддерживает извлечение и анализ данных из «облачных» копий устройств под управлением iOS 7.

### Криминалистический анализ iPhone и iPad под управлением iOS 7

«Пользователи iPhone, iPad и других «яблочных» устройств традиционно быстро переходят на использование самых последних версий программного обеспечения и операционных систем», говорит Владимир Каталов, президент компании «Элкомсофт». «В iOS 7 усилена модель безопасности, улучшен пользовательский интерфейс и введено большое количество небольших улучшений. Чем более удобным и безопасным становится смартфон, тем больше информации хранят в нём пользователи, и тем большее количество важных для расследования данных мы можем извлечь при анализе такого устройства».

Согласно данным компании Apple, на предыдущую версию операционной системы iOS 6 в конечном итоге перешло 93% пользователей. Внедрение iOS 7 разворачивается гораздо более стремительно: в первый же день после выхода новой версии iOS на неё перешло 35% пользователей. С учётом скорости перехода на новые версии операционных систем, поддержка iOS 7 играет важную роль в криминалистическом исследовании устройств Apple.

### **Извлечение информации из защищённого хранилища keychain**

Elcomsoft Phone Password Breaker – первый на рынке криминалистический инструмент, позволяющий извлекать данные из защищённого системного хранилища keychain в последней версии iOS. В защищённом хранилище содержатся такие важные для расследования данные, как пароли к веб-сайтам и учётным записям пользователя, регистрационные данные приложений и социальных сетей, номера кредитных карт, пароли от электронной почты и многое другое.

С каждой новой версией мобильной операционной системы iOS разработчики Apple перемещают всё больше типов данных в зашифрованное локальное хранилище keychain. Не стала исключением и iOS 7. Помимо привычной тенденции, в новой операционной системе поменялся формат хранения данных.

Новая версия Elcomsoft Phone Password Breaker поддерживает извлечение и расшифровку пользовательских данных из защищённого хранилища keychain. Для этого требуется наличие защищённой паролем резервной копии данных устройства. Наличие парольной защиты обязательно: в открытая, незащищённой резервной копии локальное хранилище keychain будет защищено ключом шифрования, уникальным для конкретного устройства, в то время как в резервной копии, защищённой паролем, keychain расшифровывается так же, как и прочие данные.

### **Выборочный доступ к данным из «облачного» хранилища**

В новой версии [Elcomsoft Phone Password Breaker](#) улучшен алгоритм выборочного доступа к данным из «облачного» хранилища iCloud. Способ дистанционного извлечения данных из «облачного» хранилища не нов. Он появился в продукте Elcomsoft Phone Password Breaker больше года назад, открыв криминалистам удалённый доступ к резервным копиям пользовательской информации через онлайн-сервис. В предыдущей версии Phone Password Breaker у криминалистов появилась возможность выборочного скачивания данных по категориям. Для выборочного доступа были доступны такие категории данных, как информация об устройстве, фотографии, сообщения, вложения к сообщениям, история звонков, адресная книга и календарь. Выборочное извлечение информации позволяет существенно ускорить работу и сэкономить время.

В новой версии Elcomsoft Phone Password Breaker было добавлено множество дополнительных категорий данных, доступных для выборочного извлечения. В дополнение к ранее доступным категориям, эксперт может выбрать следующие типы данных:

- Общение через социальные сети Facebook, Twitter, LinkedIn, Foursquare, WhatsApp, Instagram, Skype
- Данные всех установленных приложений Google приложений (полный список доступен по адресу: <http://www.google.com/mobile/ios/>)
- Электронная переписка, уже скачанная на телефон, а также часто используемые адреса
- Пользовательские словари (использованные пользователем слова и термины, которые отсутствуют в словаре встроенной системы проверки орфографии)

- Данные Passbook (посадочные талоны, билеты, дисконтные карты и т.д.)
- Голосовая почта
- Данные карт Apple (закладки, маршруты и т.д.)

Возможность выборочного извлечения данных по категориям позволяет сэкономить несколько часов, которые обычно занимает первоначальное скачивание полной копии данных из iCloud. Последующие обновления скачиваются гораздо быстрее, т.к. скачиваются только изменённые данные.

Более подробная информация о выборочном извлечении данных из «облачного» хранилища доступна в блоге (англ.): <http://blog.crackpassword.com/2013/08/elcomsoft-phone-password-breaker-enhances-icloud-forensics-and-speeds-up-investigations/>

### **О продукте Elcomsoft Phone Password Breaker**

Elcomsoft Phone Password Breaker предоставляет криминалистам доступ к пользовательским данным из мобильных устройств производства Apple и BlackBerry. Информация извлекается из защищенных паролем резервных файлов, создаваемых устройствами Apple iPhone/iPod/iPad и смартфонами BlackBerry при синхронизации с компьютером пользователя.

Использование аппаратного ускорения перебора паролей при помощи игровых видеокарт AMD и NVIDIA позволяет увеличить скорость расшифровки в 20-40 раз по сравнению с алгоритмами, использующими только центральный процессор компьютера. Технология перебора паролей на графических картах позволяет получить вычислительную мощь суперкомпьютера по цене домашней графической карты. Применение атаки по словарю позволяет восстановить пароль значительно быстрее.

Продукт способен дистанционно извлекать информацию из «облачного» хранилища Apple iCloud при наличии логина (Apple ID) и пароля пользователя. Поддерживается полный и выборочный доступ к данным. Доступ к самому устройству при этом не требуется.

### **Редакции и системные требования**

В продаже доступны редакции Home и Professional. Для работы [Elcomsoft Phone Password Breaker](#) установка Apple iTunes или BlackBerry Desktop Software не требуется. Elcomsoft Phone Password Breaker совместим с 32- и 64-разрядными версиями Windows XP, Vista, Windows 7 и 8, Windows 2003, 2008 и 2012 Server.

### **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>