Криминалистический анализ устройств с iOS 7: извлечение данных на физическом уровне из iPhone 5 и 5C, последних поколений iPad и iPad Mini

Москва, Россия – 30 января 2014 - Компания «Элкомсофт» обновляет линейку продуктов для криминалистического анализа мобильных устройств под управлением Apple iOS. В новой версии Elcomsoft iOS Forensic Toolkit добавлена поддержка последней версии iOS 7, что делает возможным извлечение данных на физическом уровне из устройств под управлением этой системы, включая новейшие модели iPhone 5, 5C, iPad Mini. Для успешной работы с этими устройствами требуется предварительное наличие или успешная установка "jailbreak". Более старые устройства вплоть до iPhone 4 по прежнему поддерживаются без ограничений. Кроме того, в новом релизе добавлена поддержка версий iOS 6.1.3-6.1.5.

В настоящее время 83% пользователей мобильных устройств Apple перешли на последнюю версию iOS 7. На текущий момент в мире продано более 800 миллионов устройств под управлением iOS, из них более 3 миллионов – в России.

«*Поддержка последних версии аппаратного и программного обеспечения Apple – одна из приоритетных задач нашей компании»,* заявил Владимир Каталов, президент и CEO компании «Элкомсофт». *«По сложившейся традиции, пользователи мобильных устройств Apple весьма динамичны и быстро переходят на свежие версии программного обеспечения. Поддержка последней версии iOS в наших продуктах позволит криминалистам получить доступ к информации, хранящейся в телефонах iPhone и планшетах iPad всех моделей, включая недавно выпущенные*».

Одной из интересных особенностей iOS 7 является возможность хранения в защищённом системном хранилище “keychain” информации из защищённой области «облачного» хранилища iCloud. При наличии соответствующих настроек, которые устанавливаются пользователем, в этой области хранятся данные о паролях, персональной и финансовой информации со всех устройств, зарегистрированных под данной учётной записью. В результате становятся доступными данные из резервных копий, созданных всеми зарегистрированными устройствами пользователя. Для доступа к этим данным используется продукт Elcomsoft Phone Password Breaker.

Кроме того, опять же при наличии соответствующих настроек, из хранилища могут извлекаться пароли, защищающие доступ к учётным записям Apple ID, – что позволяет криминалисту отслеживать местоположение всех зарегистрированных под данной учётной записью устройств в реальном времени. Для отслеживания местоположения пользователя используется «облачный» сервис Find My Phone с сайта Apple iCloud.

Извлечение данных на физическом уровне из новых устройств под управлением iOS 7 требуется либо наличие “jailbreak”, либо возможность его установки криминалистом, что становится возможным, если пароль на устройстве не установлен или известен эксперту.

Для извлечения данных из более старых устройств установка “jailbreak” не требуется вне зависимости от установленной версии iOS. Устройства iPhone до версии 4, первое поколение iPad и iPod Touch версий с 1 по 3 поддерживаются без ограничений. В то же время для успешного извлечения данных из устройств последних поколений, включая iPhone 4S и 5, а также iPad 2, 3 и 4, iPad Mini и iPod Touch 5, требуется наличие в устройстве установленного кода “jailbreak” либо возможности установки такого кода.

Физический метод извлечения данных из устройств iOS 7

Метод физического извлечения данных открывает доступ ко всей информации, хранящейся в устройствах iPhone, iPad и iPod Touch. С помощью снятия физического образа устройства обеспечивается доступ к гораздо более широкому спектру данных по сравнению с другими методами. Становятся доступной такая информация, как пароли к сайтам и учётным записям Apple ID, SMS, электронная почта, логины и пароли к программам.

Некоторые типы данных могут быть извлечены из устройства исключительно при помощи физического метода доступа. Такие данные включают:

1. Скачанная на устройство электронная почта вне зависимости от типа почтового аккаунта. Данные и содержимое скачанных сообщений не сохраняются в резервных копиях данных, и доступны только методом прямого физического извлечения.
2. Географические координаты. Резервные копии, создаваемые iTunes на локальном диске компьютера либо сохраняемые устройством в «облако» iCloud, содержат только самые базовые, обрывочные данные о местоположении пользователя. В то же время, физический анализ устройства позволяет восстановить точное местоположение пользователя буквально по минутам. Извлекаются данные, инициированные любыми событиями и сгенерированные всеми приложениями, запущенными на устройстве. Информация о местоположении регулярно запрашивается устройством при таких событиях, как калибровка компаса, отслеживание рекламы, при поиске сотовых и беспроводных сетей передачи данных Wi-Fi, для диагностики, установки временной зоны, для отображения траффика и многого другого.
3. Системный журнал и журнал ошибок, позволяющие отследить запуск и установку приложений.
4. Данные кэша приложений. В то время как данные программ (к примеру, список контактов в программе мгновенного обмена сообщениями) сохраняются в резервных копиях, кэш приложений в резервные копии данных не попадает. В эту категорию данных входят HTML-страницы, к которым обращались приложения, а также их адреса. С учётом того, что большинство приложений iOS в том или ином виде обращается к Интернет, количество доступных для анализа данных бывает весьма заметным. Данные кэша приложений есть только в полном образе, полученном методом физического доступа.

При исследовании соответствующим образом настроенных устройств под управлением iOS 7 может открыться доступ к «облачному» хранилищу iCloud, что позволяет не только извлекать резервные копии данных, сохранённые всеми устройствами, привязанными к исследуемой учётной записи, но и отслеживать местоположение пользователя в реальном времени.

Огромным преимуществом метода физического извлечения данных остаётся скорость работы. В отличие от методов, требующих перебора пароля, физическое извлечение данных занимает ограниченное время, зависящее от версии и

объёма памяти обрабатываемого устройства. Типичное время извлечения данных из 32-гигабайтного iPhone 5 не превышает 25 минут, в то время как аналогичного объёма iPhone 4 обрабатывается за 40 минут.

Альтернативные методы извлечения данных

При невозможности извлечения данных физическим методом возможно извлечь информацию из резервной копии данных, создаваемых устройствами под управлением iOS на компьютере пользователя. Для работы с резервными копиями данных служит продукт Elcomsoft Phone Password Breaker.

Альтернативный способ извлечения данных появился в последней версии продукта, открыв доступ к резервным копиям пользовательской информации через онлайновый «облачный» сервис. Для получения доступа к данным требуется знать Apple ID и пароль пользователя, доступные при физическом извлечении данных из устройств под управлением iOS 7. Доступ к самим устройствам при этом не требуется, а данные поступают непосредственно на компьютер следователя (Mac или Windows PC).

Продукт Elcomsoft Phone Password Breaker доступен по адресу http://www.elcomsoft.ru/eppb.html

Поддерживаемые устройства

Elcomsoft iOS Forensic Toolkit работает на компьютерах под управлением Windows и Mac OS X. Возможность извлечения данных из устройств под управлением iOS зависит от типа устройства и установленной версии iOS.

Многие устройства поддерживаются без каких-либо ограничений. Данные могут быть извлечены независимо от версии операционной системы, наличия или отсутствия “jailbreak”, вне зависимости от установленного пароля. Неограниченная поддержка доступна для следующих устройств:

- Первые версии iPhone вплоть до iPhone 4, включая все модели GSM и CDMA
- Первая версия iPad
- iPod Touch 1-4

Последние поколения устройств под управлением iOS 5, iOS 6 и iOS 7 требуют наличия или возможности установки кода “jailbreak”:

- iPhone 4S, 4C, 5, 5C
- iPad 2, 3 и 4, iPad Mini
- iPod Touch 5

В текущей версии продукта поддерживаются версии iOS до версии 7 включительно.

О продукте Elcomsoft iOS Forensic Toolkit

iOS Forensic Toolkit – удобный инструмент криминалистического анализа. 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 7 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.

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» находятся в Москве. Для получения более подробной информации посетите http://www.elcomsoft.ru