Криминалистический анализ устройств с iOS 8: извлечение данных на физическом уровне из iPhone 5 и 5C, iPad и iPad Mini

Москва, Россия, 16 января 2015. Компания «Элкомсофт» обновляет линейку продуктов для криминалистического анализа мобильных устройств под управлением Apple iOS 8, оснащённых 32-битными процессорами. В новой версии Elcomsoft iOS Forensic Toolkit добавлена поддержка последней версии iOS 8, что делает возможным извлечение данных на физическом уровне из всех 32-разрядных устройств, включая iPhone 5, 5C, iPad, 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.

В новом релизе также добавлена возможность извлечения паролей Apple ID, что в свою очередь позволяет получить доступ к пользовательским данным, хранящимся в «облачном» сервисе Apple iCloud.

«С точки зрения информационной безопасности iOS 8 – это прорыв», комментирует Владимир Каталов, президент и CEO компании «Элкомсофт». «В отличие от предыдущих версий iOS, в восьмой версии шифруются практически все пользовательские данные. Новая модель безопасности отражена в официальной политике безопасности, опубликованной на сайте Apple. Отныне даже сам производитель устройств не может извлекать пользовательские данные из устройств под управлением iOS 8 по чисто техническим причинам. Наша компания предоставляет инструменты, позволяющие при определённых условиях обходить ограничения и извлекать пользовательские данные из устройств с последними версиями прошивки.»

iOS 8: Новая модель безопасности

В последней версии iOS Apple значительно усилила безопасность хранящихся на устройствах данных. Согласно официальному заявлению компании, данные, хранящиеся на устройствах под управлением iOS 8, технически не могут быть извлечены из защищённых паролем устройств и, соответственно, не могут быть переданы государственным структурам даже при наличии запроса от правоохранительных органов.

Согласно информации, опубликованной на официальном сайте компании, “На устройствах под управлением iOS 8 ваша персональная информация включая фотографии, сообщения (включая вложения), электронная почта, контакты, история звонков, содержимое iTunes, заметки и напоминания хранятся под защитой вашего индивидуального пароля. В отличие от конкурентов, Apple не может обойти этот пароль и не имеет доступа к пользовательским данным. Соответственно, выдача информации из устройств под управлением iOS 8 по запросу от правоохранительных органов невозможна по техническим причинам.»

Фактически, в устройствах под управлением iOS 8 практически вся пользовательская информация шифруется с использованием стойкого уникального ключа, привязанного как к аппаратному идентификатору, так и к паролю, установленному пользователем. Соответственно, расшифровать пользовательские данные, не зная пароля, не представляется возможным.

Кроме того, при наличии соответствующих настроек из хранилища могут извлекаться пароли, защищающие доступ к учётным записям Apple ID. Это позволяет криминалисту извлекать данные непосредственно из «облачного» сервиса Apple iCloud с помощью продукта Elcomsoft Phone Breaker. Кроме того, использование комбинации Apple ID и пароля позволяет 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 8 возможно только при наличии установленного «jailbreak» либо при возможности его установки криминалистом. Установить «jailbreak» возможно, 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 8

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. Некоторые типы данных могут быть извлечены из устройства исключительно при помощи физического метода доступа. Становятся доступными такие данные, как пароли к Apple ID, SMS, электронная почта, логины и пароли к приложениям и учётным записям.

При исследовании соответствующим образом настроенных устройств под управлением iOS 8 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 8. 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, 7 и 8 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 только устройства с 32-разрядными процессорами. Поддержка 64-битных устройств в стадии разработки.

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 8 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» 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