Mobile Forensics Day 2019

Извлечение данных из устройств под управлением iOS. Физический и логический методы

Извлечение данных из iPhone

Содержание

Как сохранить улики

- Действия при конфискации устройства
- Хранение конфискованных iPhone

Способы извлечения данных

- Логическое извлечение
- Физическое извлечение
- Достоинства и недостатки подходов

Извлечение данных из iPhone

Действия при конфискации устройства

Ошибочные действия:

- **Бездействие**
  Улики могут быть уничтожены дистанционной командой; фоновые процессы могут изменить данные
- **Выключение телефона**
  Отключается датчик отпечатков; разблокировка только PIN; не сработают Lockdown-файлы; отключается Wi-Fi
- **Контакт с датчиком отпечатков или Face ID**
  Датчик биометрической идентификации (Touch ID, Face ID) допускает лишь 5 попыток, после чего блокируется

Первые шаги

Как сохранить данные

Что нужно сделать, а чего ни в коем случае нельзя делать с iPhone после изъятия?

- **Нельзя выключать**
  - катастрофически затруднит доступ
- **Нельзя оставлять беспроводное подключение к сети**
  - возможность дистанционной блокировки устройства, уничтожение данных

Первые шаги

Как сохранить данные: руководство к действию

- Включите на iPhone режим «в самолёте»
- Перепроверьте положение переключателей Wi-Fi и Bluetooth
  - отключите эти сети вручную, если они включены
- Подключите iPhone к портативному источнику питания
- iOS 11.4.1: к порту Lightning можно подключить адаптер USB
  - Может помочь избежать включения режима ограничений USB
  - Только для iOS 11.4.1, вероятность её использования низкая
- Поместите iPhone, подключённый к источнику питания, в клетку Фарадея

Первые шаги

Клетка Фарадея

Используйте встроенное зарядное устройство!

- Изолирует радиочастоты
- Исключает возможность дистанционного влияния
- Устройство быстро разряжается, используйте встроенный аккумулятор

Первые шаги

Как сохранить данные: предосторожности

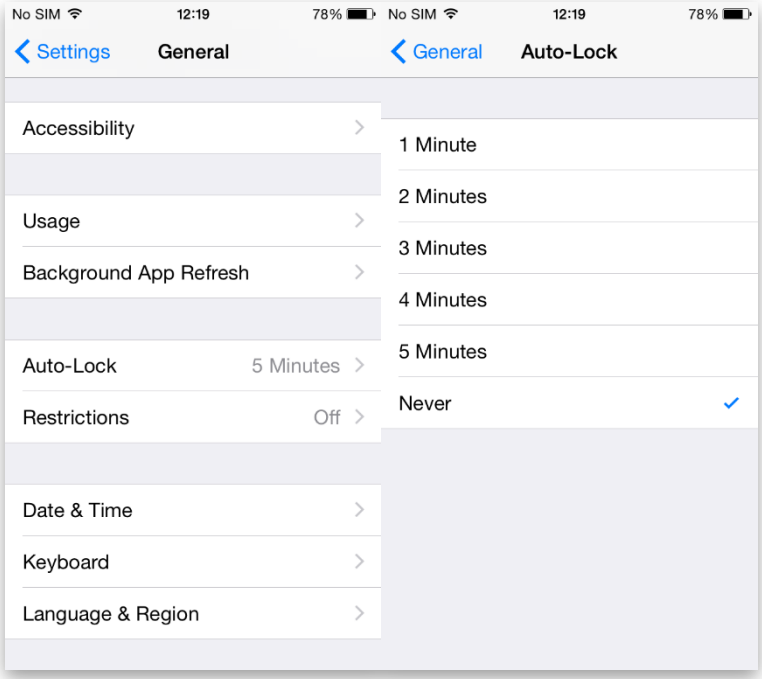
- Touch ID: не прикасайтесь к сканеру отпечатков
  - Иначе потеряете 1 из 5 попыток разблокировки по датчику отпечатков
- Face ID: взяв устройство в руки, убедитесь, что в поле зрения датчиков Face ID не попадает ни одно лицо
  - Если ваше лицо будет захвачено сканером Face ID, вы потеряете 1 из 5 попыток
- Ознакомьтесь с правилами работы биометрических методов разблокировки
- Ознакомьтесь с работой системы S.O.S. и её последствиями

Извлечение данных из iPhone

Запрет блокировки экрана

Отключение автоматической блокировки

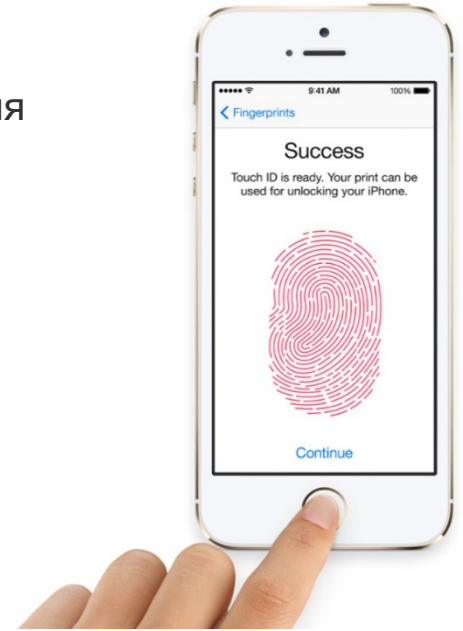
- Settings – General – Auto Lock – Never
  - Для устройств с политикой MDM/Exchange может быть невозможно
- Гораздо проще извлечь данные
- Возможность создания свежей резервной копии



Извлечение данных из iPhone

Датчик отпечатков пальцев

- Разблокировку датчиком отпечатков **нельзя использовать** для установки jailbreak
  - iOS 11, 12, 13: доверительные отношения с новым компьютером требуют ввода PIN-кода
- Датчик **можно использовать**:
  - iOS 8..10: установление доверительных отношений с компьютером
  - iOS 8..10: создание локальной резервной копии
  - Все версии: создание облачной резервной копии, просмотр данных на самом устройстве (включая Связку ключей)



Извлечение данных из iPhone

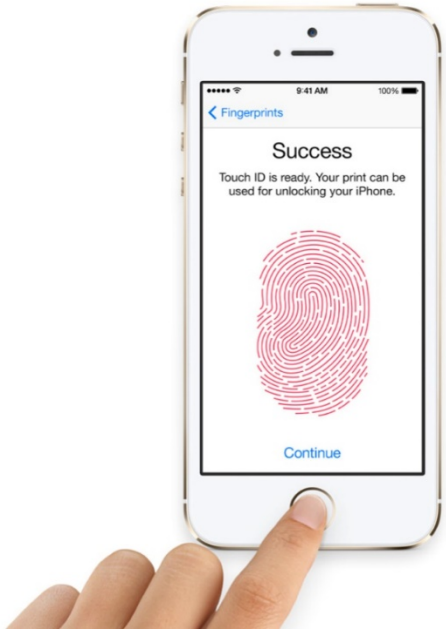
Если известен PIN или пароль блокировки

Зная пароль блокировки, можно:

- *Установить доверительные отношения*
- Создать локальную резервную копию, расшифровать keychain

iOS 11/12/13

- сбросить пароль на резервную копию
- сменить пароль к Apple ID
  - Создать и скачать облачную резервную копию
  - Скачать iCloud Keychain, iCloud Photos, синхр. данные
  - Отключить блокировку iCloud
  - Управлять другими устройствами на том же Apple ID



Извлечение данных из iPhone

Новое в iOS 13

- В облачные резервные копии в iCloud не попадают журнал звонков и история браузера Safari
- Маркеры аутентификации не могут быть использованы для:
  - Скачивания облачных резервных копий
  - Доступа к облачной Связке ключей
  - Доступа к сообщениям (SMS/iMessage) в iCloud
  - Доступа к данным Здоровье

Извлечение данных из iPhone

Новое в iOS 13

- Изменение или установка пароля на локальную резервную копию требует ввода кода блокировки (на самом устройстве)
  - Может помешать логическому извлечению, если код блокировки неизвестен
- Облачные резервные копии содержат ещё меньше информации

Извлечение данных из iPhone

Режим ограничений USB

- Режим ограничений USB (USB restricted mode)
- В iOS 12 и 13 активируется сразу после блокировки экрана
  - Если пользователь не подключал аксессуары в последние несколько дней
- Можно активировать вручную (режим SOS)
- Полностью блокирует USB-порт (возможна только зарядка)
  - Cellebrite, GrayKey обходят блокировку порта на некоторых моделях

Извлечение данных из iPhone

Методы извлечения данных

Облачное извлечение

- Apple ID/пароль (часть данных) или маркер аутентификации (только синхронизированные данные)
- Для доступа к некоторым видам данных необходим код блокировки устройства (Связка ключей, Здоровье, сообщения)
- Затребовать у Apple (ордер)

Извлечение данных из iPhone

Методы извлечения данных

- **Облачное извлечение**
  - Резервные копии
  - Синхронизированные данные
  - Зашифрованные данные (для доступа требуется PIN устройства)
- **Логический анализ**
  - Резервные копии (с паролем или без); в резервных копиях с паролем – часть содержимого Связки ключей
  - Медиа-файлы и открытые данные приложений
  - Журналы crash logs
- **Физическое извлечение**
  - Образ файловой системы
  - Полное содержимое Связки ключей (пароли, маркеры аутентификации)

Извлечение данных из iPhone

Методы извлечения данных

Логическое извлечение посредством резервных копий

- Резервная копия может быть зашифрована паролем
  - iOS 11/12/13 позволяет сбросить пароль (нужен PIN устройства)
  - Медленный перебор (100 п/с на GPU); результат не гарантирован
  - Для связи с устройством можно использовать lockdown-записи
  - Режим ограничений USB делает логическое извлечение невозможным
- Необходимо подключить iPhone к компьютеру
  - Это не всегда удаётся (ограничения USB, PIN для связи с компьютером)

Извлечение данных из iPhone

Методы извлечения данных

Физическое извлечение

- Требуется PIN/код блокировки экрана
- Известный код блокировки позволит обойти ограничения USB и установить связь с компьютером
- Требуется:
  - Джейлбрейк (многочисленные сложности) либо
  - ПО с прямой эксплуатацией цепочки уязвимостей (ограниченная поддержка устройств/версий iOS)

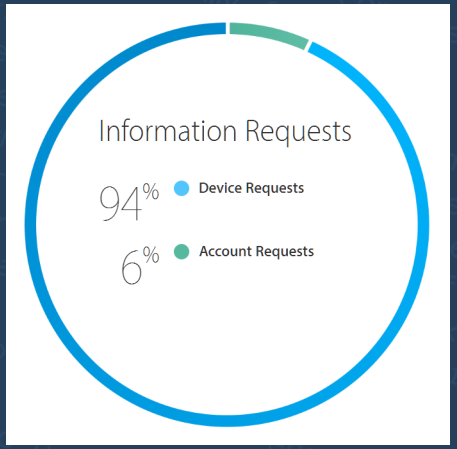
Извлечение данных из iPhone

Можно ли взломать PIN/пароль блокировки?

- Старые устройства не работают
- Доступны сторонние сервисы (Cellerbrite, GrayKey)
  - Ограничения по версиям iOS и моделям устройств
  - Результат не гарантирован, деньги не возвращаются

iOS Forensics

В первую очередь



Запросить данные напрямую у Apple

- Необходимо следовать определённым процедурам
- Много времени на ответ
- Неудобный формат данных
- Возможно, свежих данных в облаке нет
  - San-Bernardino case: последняя резервная копия была сделана несколько месяцев назад

Извлечение данных из iPhone

Предварительные шаги

Создать локальную резервную копию

- Даже если установлен пароль на резервную копию
- Использовать iOS Forensic Toolkit
- Разблокировать при помощи PIN, датчика отпечатков, lockdown-файла

Извлечение данных из iPhone

Проблемы мобильной криминалистики

- Как разблокировать устройство?
- Как извлечь данные из заблокированного устройства?
- Если устройство разблокировано, как извлечь максимальное количество информации?

Извлечение данных из iPhone

	Физический анализ	Логический анализ	Облачный анализ
Времязатраты	**35-180 минут** (в зависимости от модели)	**Минуты** (без пароля или пароль известен) **Неизвестно** (неизвестный пароль)	**0-4 часа** (в зависимости от скорости соединения и объёма данных)
Связка ключей	**Да**	**Нет** (резервная копия без пароля) **Да** (резервная копия с паролем)	**Да** * Отдельный сервис iCloud Keychain, требуется код блокировки
Удалённые файлы	**Нет**	**Нет**	**Для некоторых типов данных** (фото: до 30 дней)
Удалённые записи SQLite	**Да**	**Да**	**Да**
Возможные проблемы	Jailbreak; PIN/пароль блокировки	Неизвестный пароль, низкая скорость восстановления; требуется PIN/пароль блокировки устройства для связи с компьютером, сброса пароля на резервную копию; **iOS 13**: установка пароля на резервную копию требует ввода кода блокировки	Двухфакторная аутентификация; уведомление пользователя по email

Извлечение данных из iPhone

	Физический анализ	Логический анализ	Облачный анализ
Резервная копия устройства	**Да** (больше данных)	**Да** (количество доступных данных больше в резервных копиях с паролем)	**Да** (меньше данных в сравнении с локальной резервной копией)
Контакты, календари, заметки, звонки	**Да**	**Да**	**Да**
Сообщения (SMS, iMessage)	**Да**	**Да**	**Если включена 2FA, известен код блокировки**
История местоположения	**Да**	**Да**	**Да**
Сообщения Email	**Да**	**Нет**	**Нет**
Данные сторонних приложений	**Да**	**Некоторые**	**Некоторые**

Логическое извлечение данных

Достоинства метода

- Самый простой и надёжный метод
- Хорошо изучен, поддерживается большинством инструментов
- Доступна большая часть информации
- Можно расшифровать «связку ключей», в которой хранятся пароли пользователя
- В iOS 11/12/13 можно сбросить пароль к резервной копии (если известен PIN/пароль блокировки устройства)
- Предыдущие версии iOS можно обновить до iOS 12/13 (требуется PIN/пароль блокировки)

Логическое извлечение данных

Что попадает в резервную копию

- Локальная резервная копия содержит:
  - Историю браузера Safari, страницы, закладки
  - Контакты, учётные записи, заметки
  - Пароли в связке ключей keychain
  - Данные приложений, документы, книги
  - Данные Wallet
  - Историю местоположения
- Фото и видео (если не включен iCloud Photo Library)
- Текстовые сообщения (SMS, MMS, iMessage)
- Историю переписки для **некоторых** программ мгновенного обмена сообщениями
- Журнал звонков
- И многое другое

Логическое извлечение данных

Не только резервные копии!

- Логическое извлечение – это не только резервные копии
- Подробная информация об устройстве, пользователе, список установленных приложений
- Медиа-файлы: фото и видео (через отдельный механизм, даже если установлен пароль на резервную копию)
- Файлы приложений (книги, документы, БД менеджеров паролей и др.)
- Крэш-логи системы и приложений
- Старые версии iOS: практически полное содержимое смартфона

Логическое извлечение данных

Что НЕ попадает в резервную копию

- В локальную резервную копию не попадает:
  - Временные файлы и кэш браузера
  - Данные приложений, для которых запрещено резервное копирование
  - WAL (write-ahead logs) и freelists для приложений, использующих SQLite
  - Расширенная история местоположения
  - Электронная почта (сообщения, вложения)
  - История переписки для многих программ мгновенного обмена сообщениями
  - Данные Home и Screen Time

Логическое извлечение данных

Недостатки и ограничения

- Устройство нужно разблокировать (паролем, отпечатком пальца, при помощи lockdown-файла)
- **iOS 11/12/13: требуется пароль блокировки устройства!**
  - В некоторых случаях может использоваться lockdown-файл
- Резервная копия может быть зашифрована
  - При невозможности сброса пароля требуется длительный перебор
  - Скорость перебора чрезвычайно низкая
- Ограниченный набор данных

Логическое извлечение данных

Недостатки и ограничения

- **iOS 11**
  - Срок действия lockdown-файла ограничен (14 дней?)
- **iOS 11.4+**:
  - Срок действия lockdown-файла 7 суток
  - Порт доступа Lightning блокируется; дальнейшие действие невозможны без пароля блокировки

Логическое извлечение данных

Пароль на резервную копию

- Если задан пароль на резервную копию

Незашифрованные данные не покидают аппарат! *

- Всё шифрование происходит внутри устройства (iPhone, iPad)
- iTunes просто получает зашифрованный поток данных
- Нет способа перехвать незашифрованные данные, поскольку их просто нет
- Если пароль неизвестен, его невозможно просто «сбросить»

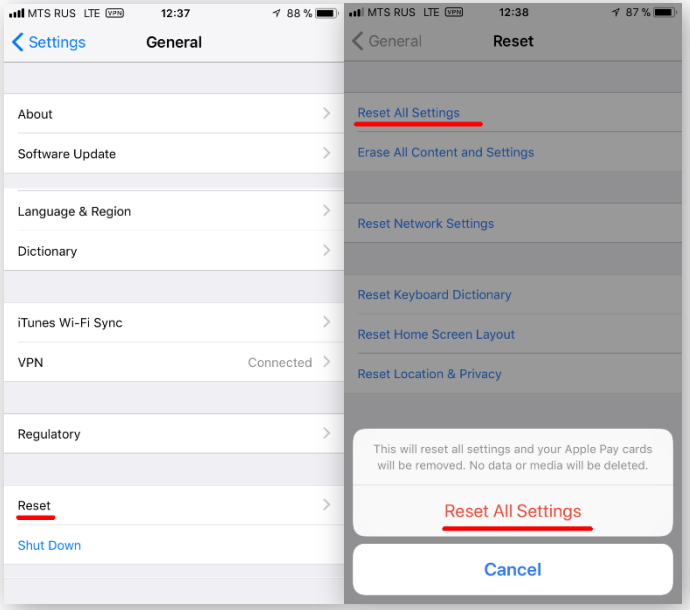
** Некоторая информация всё же доступна: серийный номер, версия iOS и т.д.*

Логическое извлечение данных

iOS 11/12/13: сброс пароля резервной копии

iOS 11/12/13 позволяет сбросить пароль на резервные копии

- Влияет только на вновь создаваемые резервные копии, но не на уже имеющиеся
- Разблокируйте iPhone
- **Settings** > **General**
- Нажмите **Reset**
- Нажмите **Reset All Settings**
- Введите пароль блокировки устройства
- Предыдущую версию iOS можно обновить до 12
- Невозможно, есть установлен пароль на Restrictions / Screen Time



Логическое извлечение данных

Lockdown-записи (файлы)

- iTunes использует pairing-записи для идентификации доверенного компьютера
- Доверенный компьютер может создать резервную копию
- Нет необходимости разблокировать устройство, но оно должно быть разблдокировано хотя бы раз после включения

iOS 4 до 8.2

- Сервисы *file_relay*, *afc*, *house_arrest*
- Можно достать практически всё, даже если ключено шифрование резервных копий

iOS 8.3 и более новые

- Резервные копии, медиа-файлы, документы, информация об устройстве

Логическое извлечение данных

Что если…?

Lockdown-запись уже не работает (срок действия истёк?)

- Lockdown-запись уже невозможно использовать для аутентификации
- Попробуйте разблокировать другим способом

Ситуация с «холодной загрузкой»

- Разблокируйте устройство хотя бы раз, чтобы оно могло принимать pairing-записи

Если опция *Encrypt iPhone backup* включена, но пароль вам неизвестен

- Пароль нельзя поменять, не зная старый
- Всё равно сделайте резервную копию, потом попытайтесь восстановить пароль

Логическое извлечение данных

Используемые инструменты

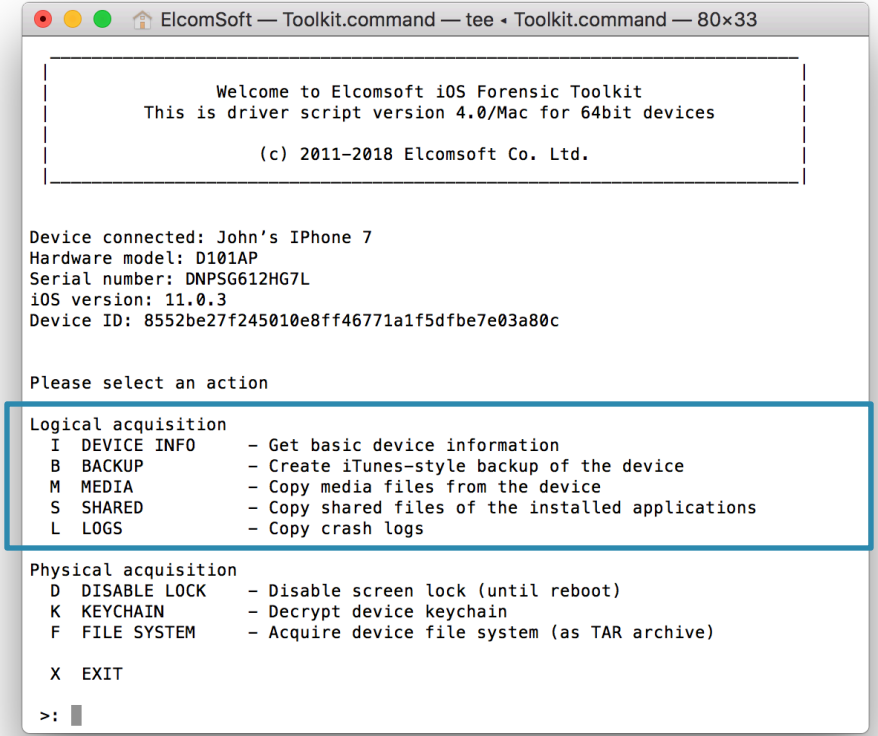
- **Apple iTunes** для установки драйверов для связи с устройством
- **Elcomsoft iOS Forensic Toolkit** для создания резервной копии
- **Elcomsoft Phone Breaker** для взлома пароля; для расшифровки резервной копии; для просмотра связки ключей keychain
- **Elcomsoft Phone Viewer** для просмотра данных из резервной копии

Демонстрация

Логическое извлечение

Последовательность шагов:

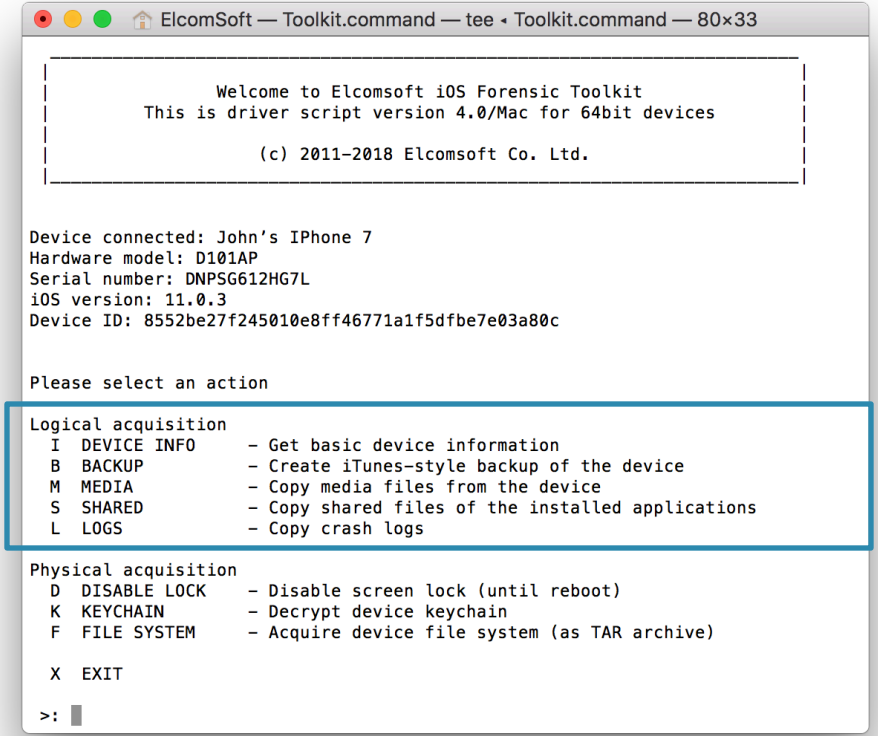
- Получение информации об устройстве
- Создание резервной копии
- Извлечение медиа-файлов и файлов приложений
- Извлечение журналов crash logs



Демонстрация

Информация об iPhone

- Степень детализации зависит от ситуации
- Множество вариантов:
- **BFU:** Устройство сразу после перезагрузки (при наличии или отсутствии lockdown)
- **AFU:** Устройство было разблокировано хотя бы раз (при наличии или отсутствии lockdown)



Демонстрация

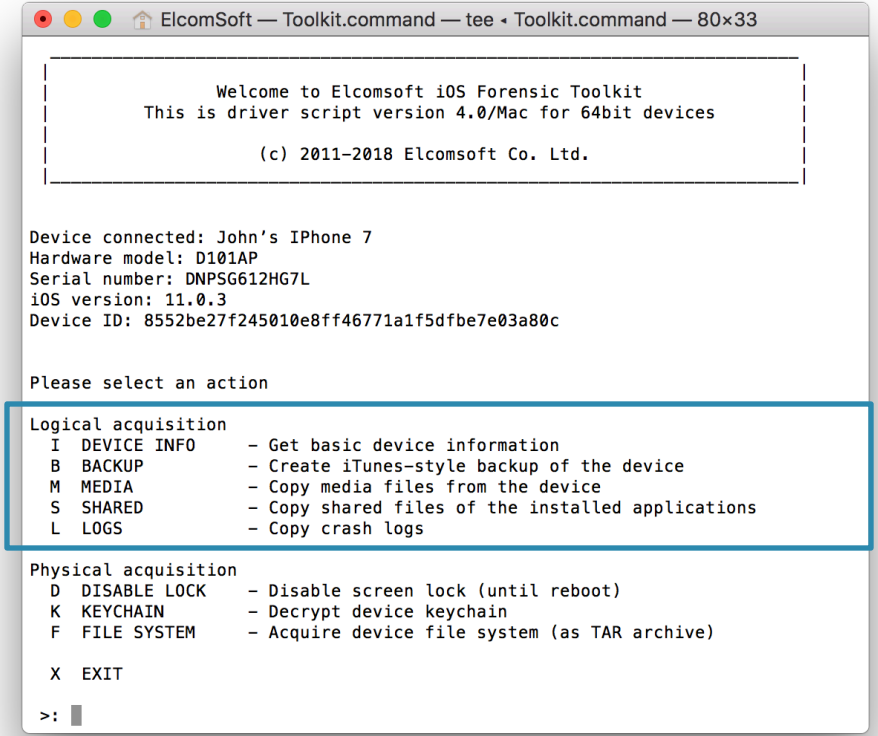
Device Info и Lockdown

Нет записи lockdown:

- BFU:
  базовая информация
- AFU:
  базовая информация

Есть запись lockdown :

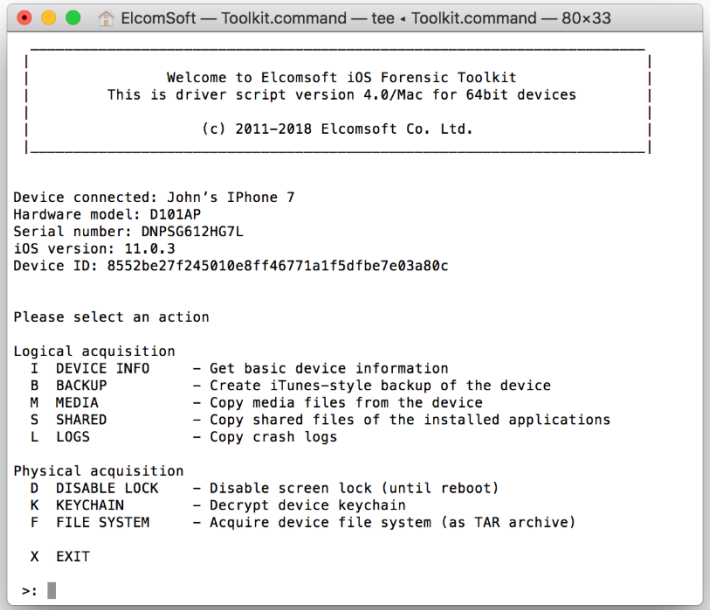
- BFU:
  расширенная информация
- AFU:
  расширенная информация и список установленных приложений



Логическое извлечение данных

Резервные копии и пароли

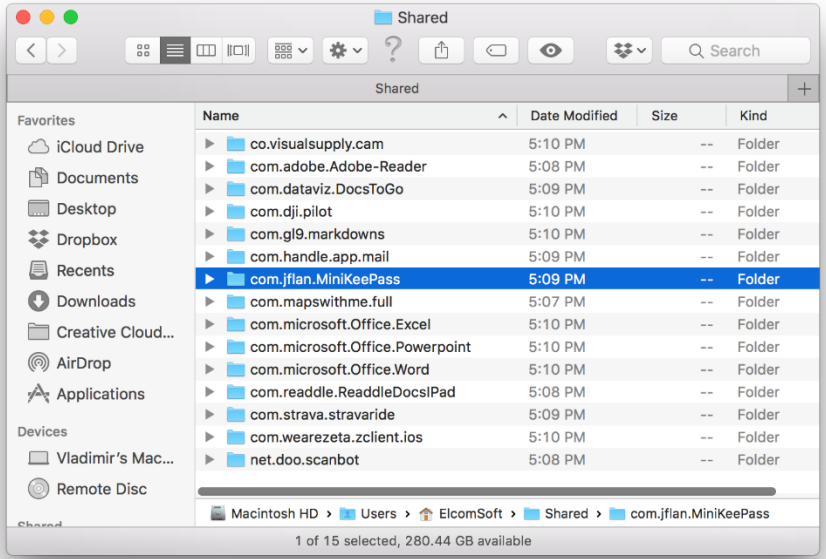
- В резервной копии с паролем доступно больше данных
- Установите пароль на резервную копию перед извлечением
- В iOS 13 для этого нужен код блокировки устройства
- В резервных копиях без пароля содержимое Связки ключей зашифровано аппаратным ключом
- iOS Forensic Toolkit установит пароль “123”



Логическое извлечение данных

Файлы приложений

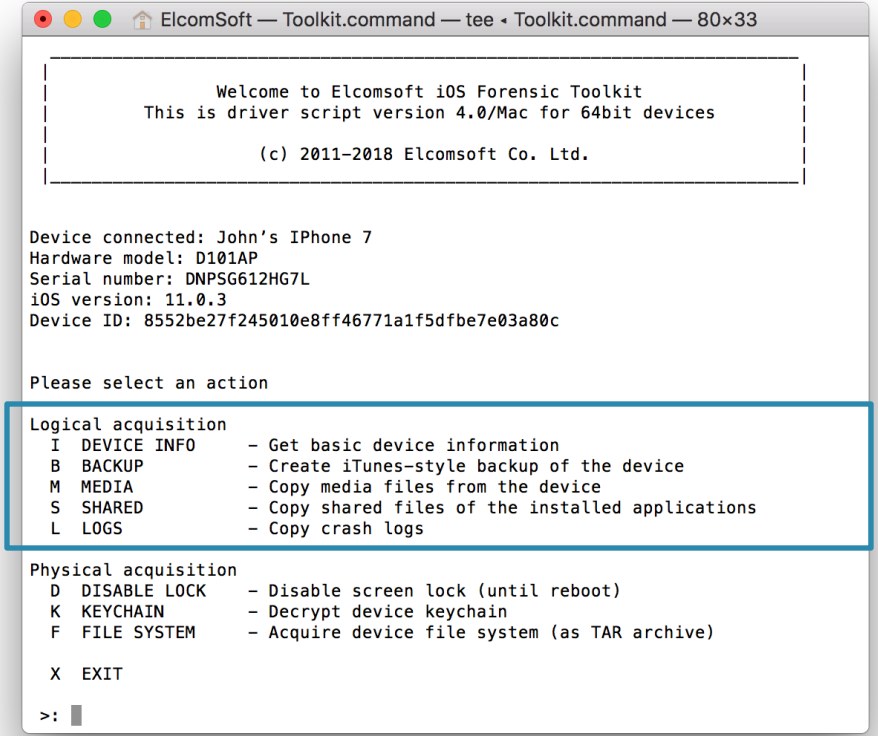
- Файлы, доступные через интерфейс iTunes File Sharing
- Могут содержать документы PDF (iBooks), БД с паролями
- Не защищаются паролем на резервную копию
- Другой механизм доступа в сравнении с резервными копиями
- **EIFT**: извлекает максимальное количество данных
- blog.elcomsoft.com/2018/02/get-ios-shared-files-without-a-jailbreak/



Демонстрация

Дальнейшие шаги

- Создание резервной копии
- Задание пароля, если пароль пустой
- Извлечение медиа-файлов, файлов приложений и журналов crash logs
- Просмотр в Elcomsoft Phone Viewer

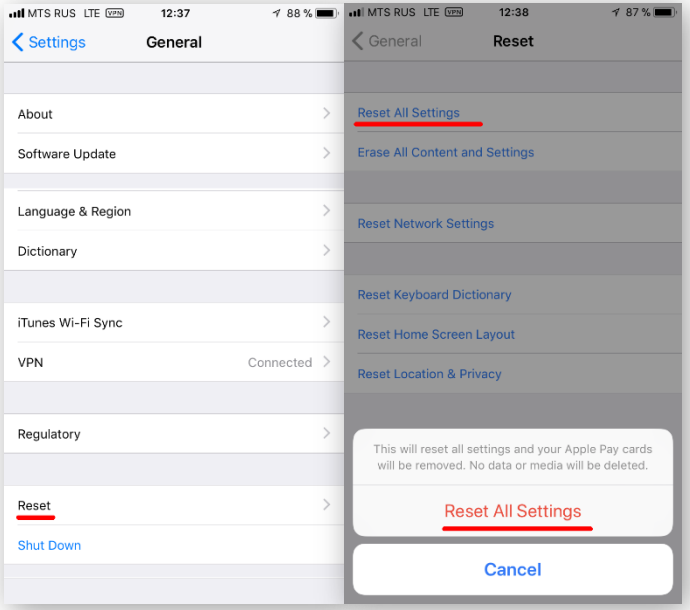


Логическое извлечение данных

Как сбросить пароль резервной копии

iOS 11/12/13 позволяют сбросить пароль к резервной копии

- Разблокируйте iPhone посредством Touch ID, Face ID или кода блокировки
- **Settings** > **General**
- Внизу экрана нажмите **Reset**
- Нажмите **Reset All Settings**
- Введите код блокировки устройства для подтверждения

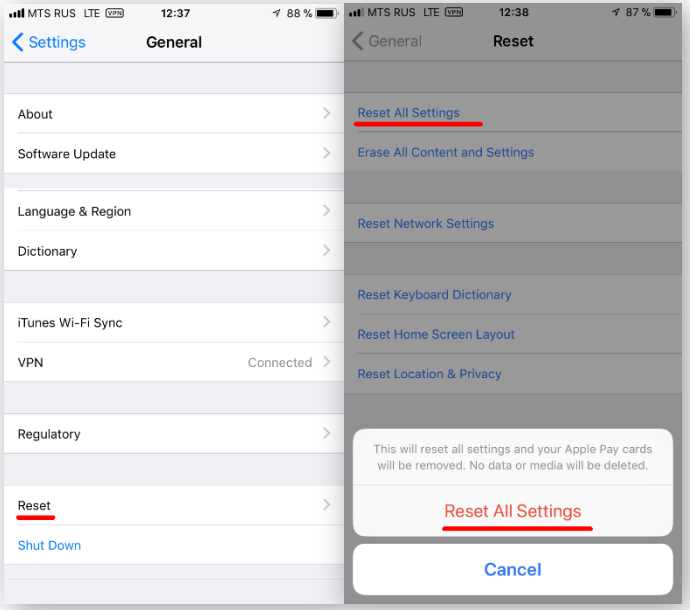


Логическое извлечение данных

Как сбросить пароль резервной копии

Использование сброса через “Reset All Settings” сбросит следующие данные:

- **Код блокировки устройства:**
  - **удаляются транзакции Apple Pay, почта Exchange, часть других данных**
- Некоторые настройки экрана
- Пароли Wi-Fi (но остальное содержимое Связки ключей не удаляется)
- com.apple.wifi.plist
- **Пароль на резервную копию в iTunes**

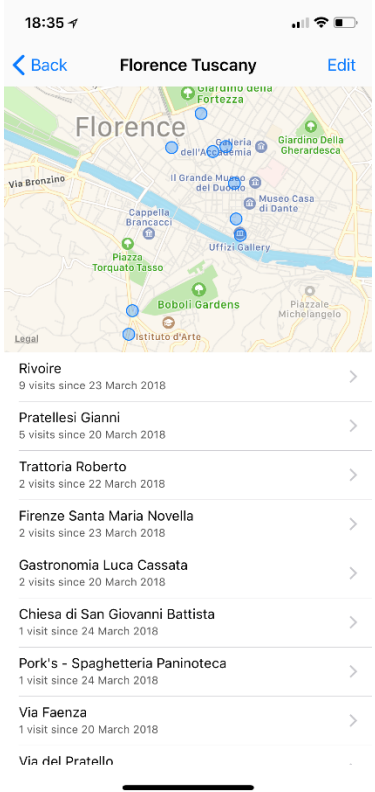


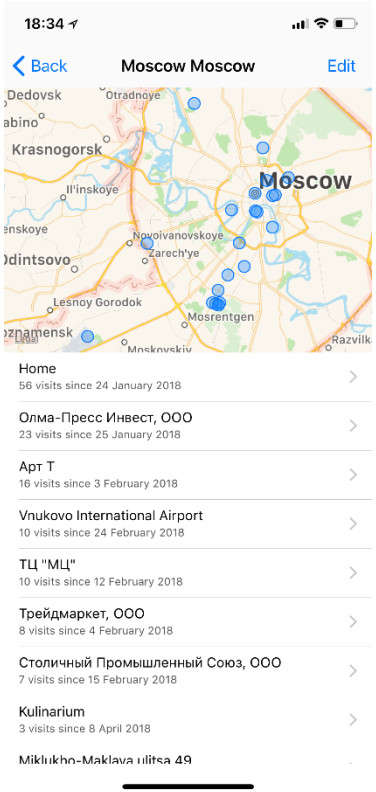
Физическое извлечение данных

Чего нет в резервных копиях

При помощи физического анализа можно извлечь дополнительную информацию

- История местоположения
- Почта
- Данные Здоровья
- Данные Home
- Данные Экранного времени
- Сохранённые Push-уведомления
- Данные Spotlight
- Кэш и сниппеты клавиатуры
- Список устройств Bluetooth
- Основные данные и кэш приложений





Физическое извлечение данных

Чего нет в резервных копиях

- Данные приложений, для которых запрещено резервное копирование
- Все записи Связки ключей, включая защищённые
- Статистика загрузки CPU
- Статистика использования аккумулятора
- Использование данных и сетевых ресурсов
- Многочисленные логи
- Лог активности приложений
- SHM и WAL для всех БД SQLite

Физическое извлечение данных

Достоинства метода

- Максимально полный доступ к данным, удобно монтировать и анализировать
- Почта, переписка во всех программах мгновенного обмена сообщениями
- Доступ к данным всех приложений
- Расширенная история местоположения
- Детальная история использования телефона
- **Можно полностью расшифровать Связку ключей (keychain)**

Физическое извлечение данных

Ограничения метода

- Требуется jailbreak
- Требуется PIN/пароль блокировки
- **Jailbreak доступен далеко не для всех платформ и версий iOS**
- iOS 11.4.1 – последняя версия с полноценным jailbreak
- iOS 12.0..12.4 – возможно получение root-прав (+ssh), достаточно для извлечения файловой системы
  - Для версий iOS 12.3, 12.3.1, 12.4.1 джейлбрейка нет

Физическое извлечение данных

Физическое извлечение: требования

Вы знаете пасскод

- Или пасскод не установлен
- Или устройство не заблокировано

Jailbreak может быть установлен

- Установка непростая и не всегда возможна
- Требуется пасскод

Достоинства

- На выходе – образ файловой системы, расшифрованная Связка ключей
- Расшифровываются *все* записи в Связке ключей
- Guaranteed (short) timeframe

Физическое извлечение данных

Требуется jailbreak

Необходим взлом устройства

- Jailbreak использует найденные уязвимости
- Установка jailbreak – комплексный процесс; **результат не гарантирован**
- Vодификация системного раздела и раздела данных
- Риск получения неработоспособного устройства
  - В iOS 10..12 риск минимален; в старых версиях iOS риск повышенный
- Для установки jailbreak требуется PIN/пароль блокировки
- При установке необходимо предоставить iPhone доступ к Интернет
  - Возможна удалённая блокировка устройства, удалённое уничтожение информации

Физическое извлечение данных

Особенности в 64-разрядных устройствах

- **Требуется jailbreak**
- **iOS 12/13**: порт Lightning может быть заблокирован сразу после блокировки экрана
- Экран устройства должен оставаться разблокированным в течение всего процесса извлечения данных
  - В противном случае часть данных будет недоступна
- Извлекается образ файловой системы
  - Папки и файлы в виде TAR архива
  - Данные приложений, почта, расширенные данные местоположения
- Расшифровать связку ключей можно **полностью**, включая записи ThisDeviceOnly
- **Метод оптимально работает в сочетании с логическим извлечением данных.**

Физическое извлечение данных

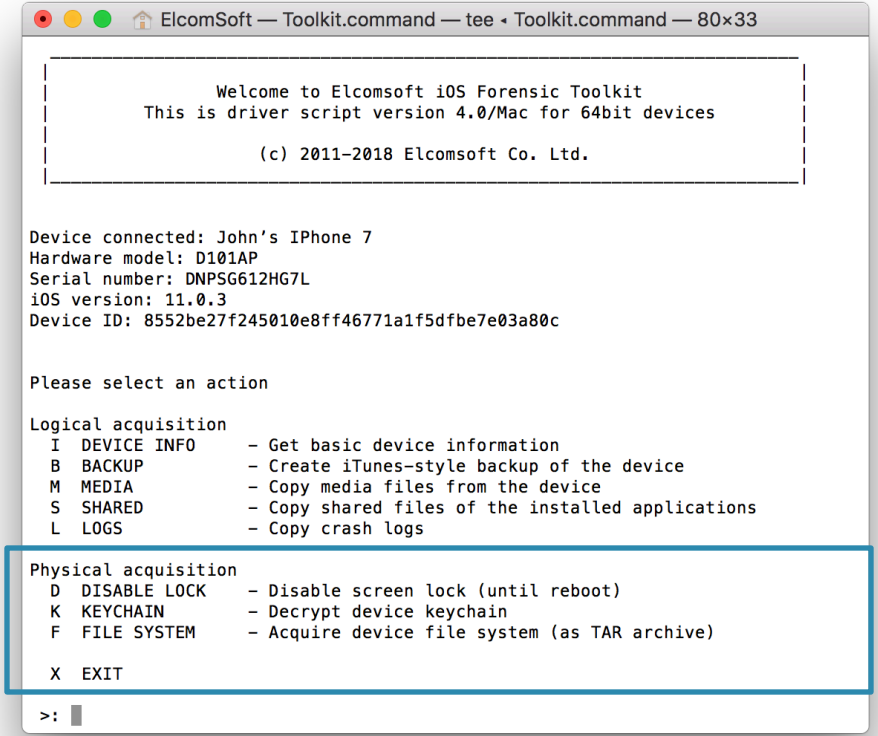
Используемые инструменты

- **Файл с jailbreak для версии устройства и iOS**
- Cydia Impactor для установки jailbreak
- Одноразовая учётная запись Apple ID для цифровой подписи jailbreak
- *(Альтернатива) https://ignition.fun*
- **Elcomsoft iOS Forensic Toolkit** для извлечения и расшифровки данных

Демонстрация

Последовательность шагов

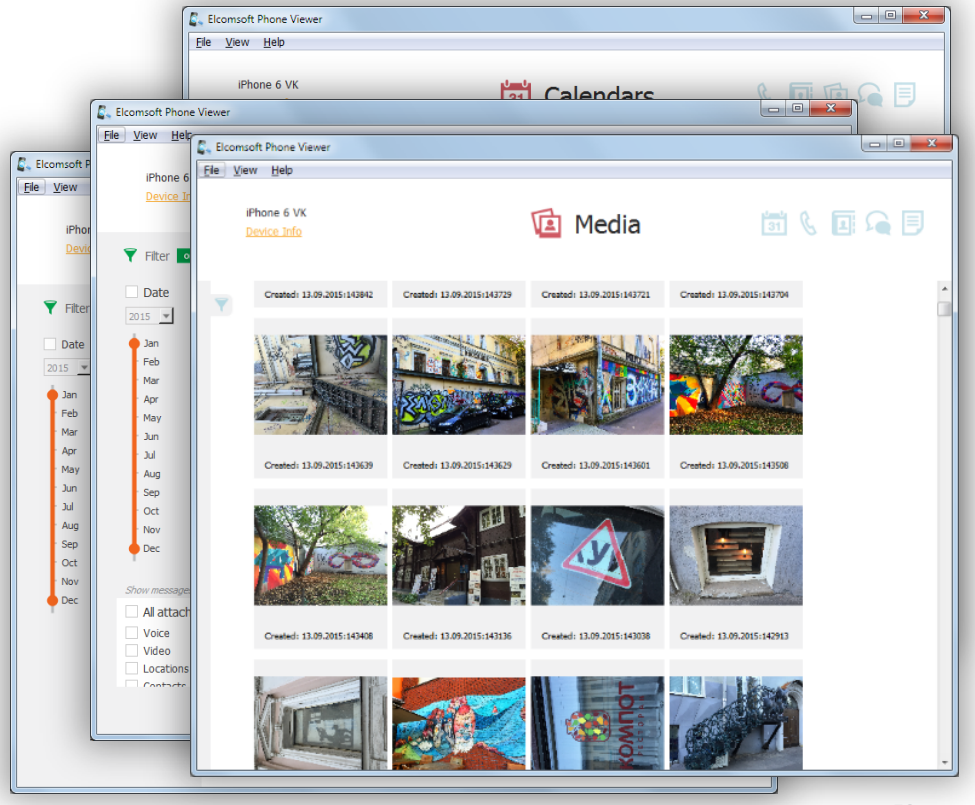
- D: Отключение блокировки экрана
- K: Извлечение Связки ключей
- F: Создание образа файловой системы



Демонстрация

Просмотр и анализ

- Просмотр паролей из Связки ключей: Elcomsoft Phone Breaker
- Анализ образа файловой системы: Elcomsoft Phone Viewer



Облачный анализ

Преимущества облачного анализа

- Нет необходимости в самом устройстве
  - iPhone может быть заблокирован, сломан или физически недоступен
- Из облака можно извлечь даже больше данных, чем из самого устройства благодаря синхронизации с другими устройствами пользователя
- В облаке в течение ограниченного времени могут храниться удалённые данные
- Облачный анализ достаточно быстрый и простой

Облачный анализ

Облачный анализ: что можно извлечь

- Резервные копии из iCloud backups (включая учётные записи с 2FA)
- Содержимое iCloud Drive (включая данные сторонних приложений, которые недоступны никаким другим способом)
- iCloud Photos
- Ключ восстановления доступа к FileVault2
- Связка ключей iCloud keychain
- Данные Здоровья (включая данные, зашифрованные кодом блокировки)
- Облачные сообщения (iMessage и SMS)
- Ведётся работа над доступом к данным *Экранное время* и *Home*

Облачный анализ

Проблема доступности данных аутентификации

- Основная проблема облачного анализа - доступность данных для аутентификации
  - логин и пароль от учётной записи
  - второй фактор аутентификации (разблокированное устройство из той же учётной записи; SIM-карта, на которую можно получить код в виде SMS)
  - для доступа к отдельным категориям - код блокировки экрана (iOS) или системный пароль (macOS) устройства из той же учётной записи

Облачный анализ

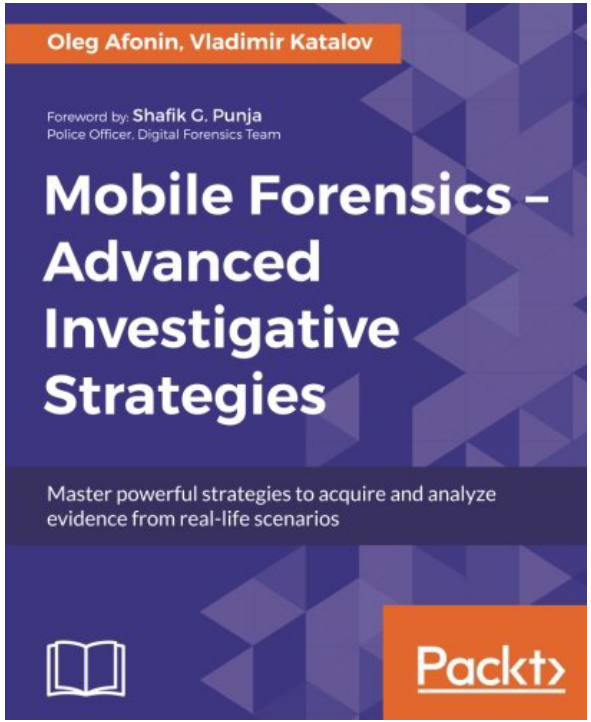
Логин и пароль в результате физического анализа

- Данные для аутентификации можно получить в результате физического анализа
  - логин и пароль от Apple ID/iCloud
  - маркер аутентификации
  - второй фактор аутентификации – не проблема (физический анализ предполагает разблокирование устройства, можно получить код в режиме офлайн в приложении Settings)
  - код блокировки экрана необходим для физического анализа, а следовательно, может быть использован и для доступа к защищённым категориям в облаке

Извлечение данных из iPhone

Инструменты

- iTunes
- Бесплатные и с открытым кодом
  - iLoot (https://github.com/hackappcom/iloot)
  - InflatableDonkey (https://github.com/horrorho/InflatableDonkey)
  - libmobiledevice (http://www.libimobiledevice.org)
  - iMobileDevice (http://quamotion.mobi/iMobileDevice)
- **Elcomsoft iOS Forensic Toolkit**
- **Elcomsoft Phone Breaker**
- **Elcomsoft Phone Viewer**



Логическое и физическое извлечение данных из iPhone: возможности и ограничения

Oleg Afonin, Vladimir Katalov ElcomSoft Co. Ltd.

http://www.elcomsoft.com
http://blog.crackpassword.com

Facebook: ElcomSoft
Twitter: @elcomsoft