Инструментарий “Элкомсофт” для цифровой криминалистики

Belka-day | 31.10.2019

Александр Талипов

Некоторые клиенты

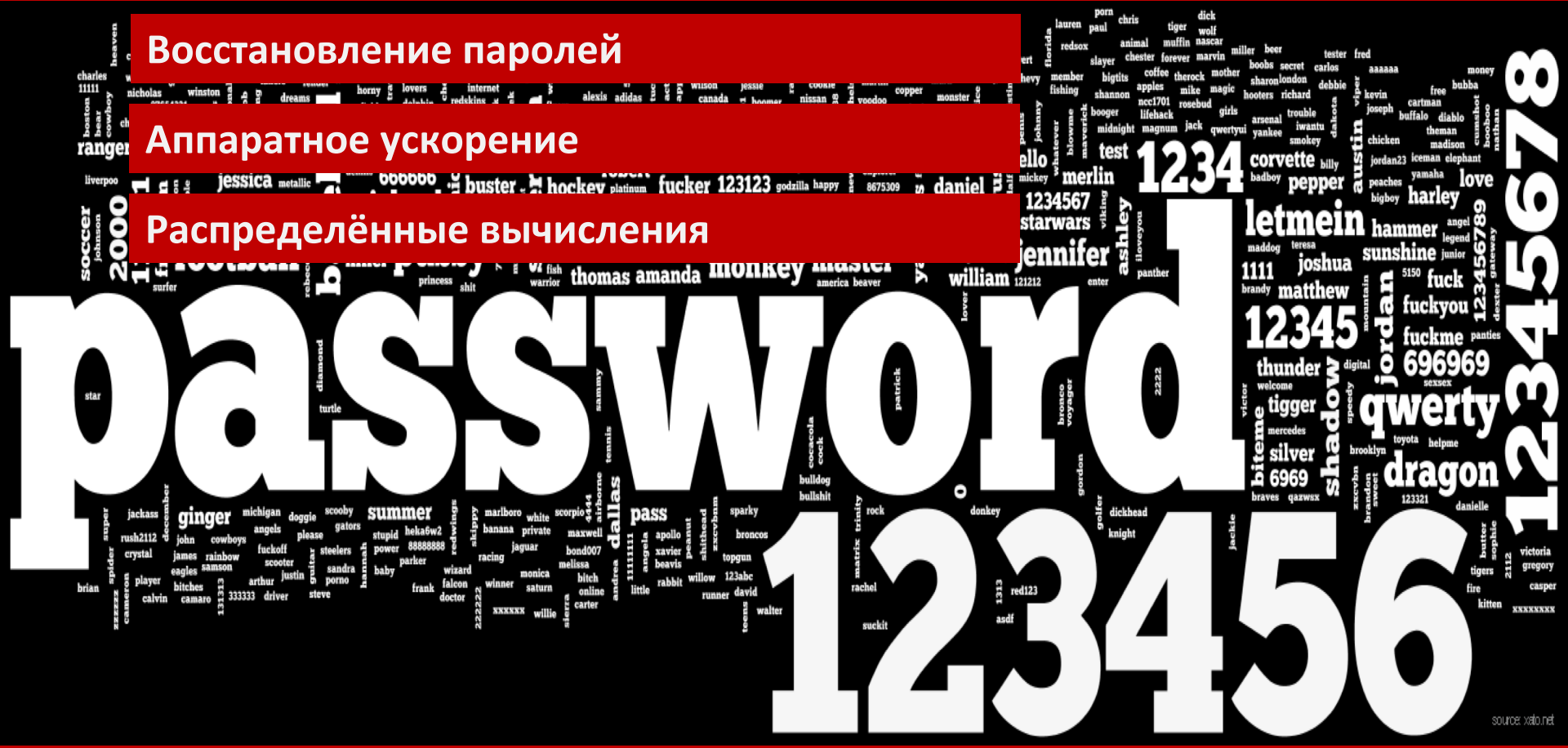






Компьютерно-техническая экспертиза

- Восстановление паролей
- Аппаратное ускорение
- Распределённые вычисления



Восстановление паролей

- **Пароли для ограничения доступа**
  - Обычно восстанавливаются моментально
- **Слабое шифрование**
  - Возможно моментальное восстановление с Thunder Tables
- **Сильное шифрование**: требуется перебор
  - Начальная атака по списку часто употребляемых паролей
  - Атака по словарю с использованием мутаций
  - Аппаратное ускорение
  - Распределённые вычисления без потерь

Часто употребляемые пароли

- **Всего 25 распространённых паролей используются в 2.2% случаев**
- **500 самых популярных паролей используются в 9.1% случаев**
- Компактный словарь на 10,000 популярных паролей срабатывает в 30% случаев
- 59% пользователей использует одинаковые или похожие пароли
- **Пароль зависит от языка пользователя**
  - Используйте **Proactive System Password Recovery** для моментального извлечения паролей и составления пользовательского словаря

Атака по словарю

- **Большая часть паролей основана на словарных фразах**
  - Иногда с добавлением цифр
- **Словарные пароли редко блокируются политиками безопасности**
  - Вместо этого, политики устанавливают требования к минимальной длине пароля, использованию цифр и специальных символов
- Стойкие пароли (например, Office 2010-2016) можно восстановить только словарной атакой
- По статистике, успешность словарных атак ~50%

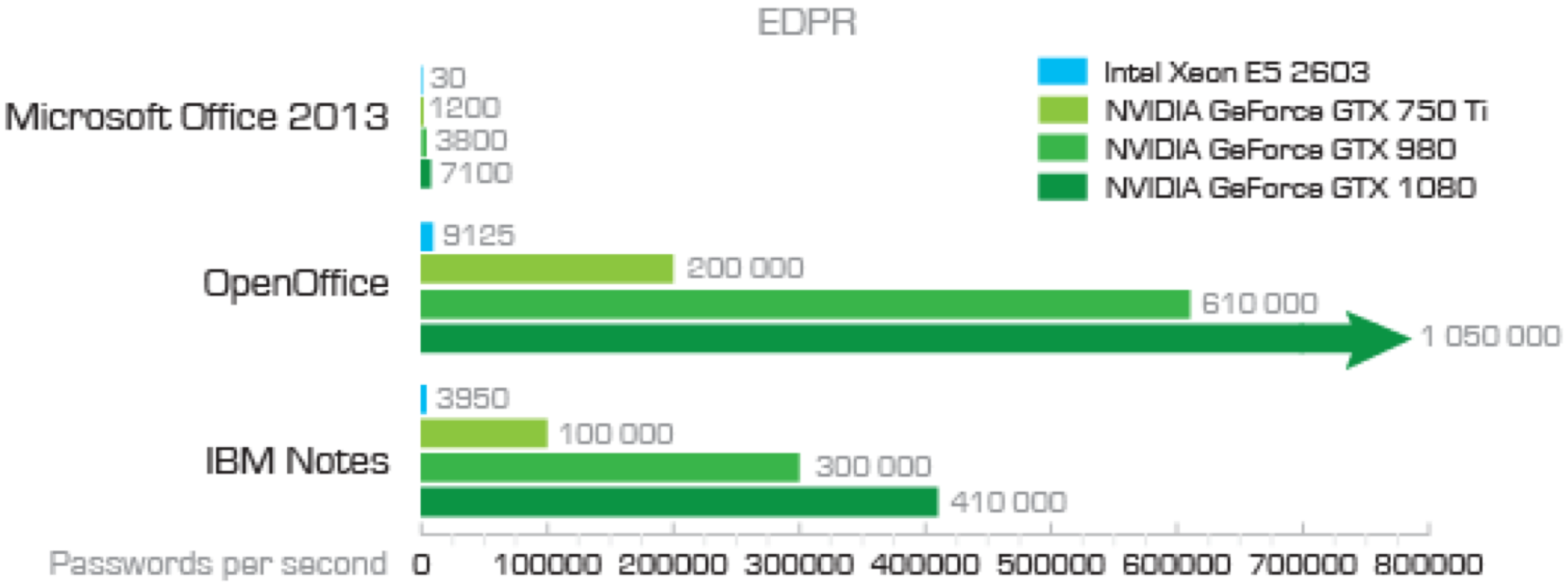
Атака по словарю

- **Подход к решению задачи:**
  - Используйте готовые словари, включая словари утечек паролей
  - Предварительные атаки с заранее сконфигурированными мутациями
  - Прямой перебор паролей в последнюю очередь
- **Наши рекомендации:**
  - Не тратьте слишком много времени на атаки по стандартным словарям общеупотребимых слов.
    Небольшой целенаправленный словарь сработает быстрее и более качественно.
  - Используйте слова как из английского языка, так и из родного языка пользователя.

Аппаратное ускорение

- **Подход к решению задачи:**
  - Обязательно используйте аппаратное ускорение
  - Устанавливайте максимальное число ускорителей
  - Экономия бюджетных средств: используйте существующий парк видеокарт (в продуктах Элкомсофт - асинхронная поддержка с одновременной работой карт AMD и NVIDIA)
- **Наши рекомендации:**
  - GPU (а не CPU) – лучшее вложение средств
  - Докупайте дополнительные видеокарты. Добавляйте, а не заменяйте: совместное использование даст максимальный прирост производительности при минимальных вложениях

Бенчмарки

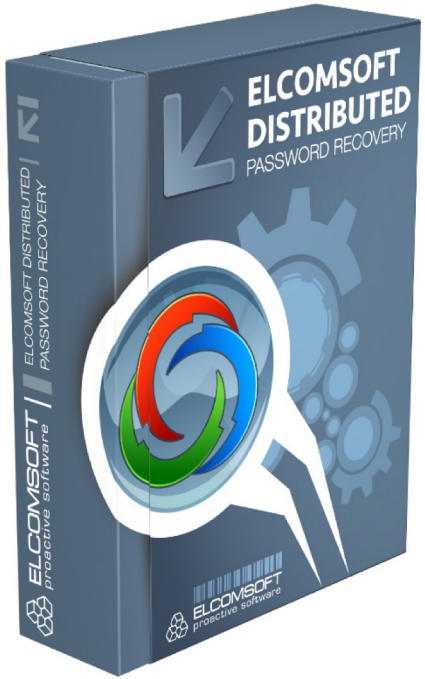

EDPR
Intel Xeon E5 2603
NVIDIA GeForce GTX 750 Ti
NVIDIA GeForce GTX 980
NVIDIA GeForce GTX 1080
Microsoft Office 2013
30
1200
3800
7100
OpenOffice
9125
200 000
610 000
1 050 000
IBM Notes
3950
100 000
300 000
410 000
Passwords per second
0
100000
200000
300000
400000
500000
600000
700000
800000

Распределённые вычисления

- **Подход к решению задачи:**
  - Используйте распределенные атаки
  - Масштабируемость без накладных расходов:
    10,000 компьютеров сработают ровно в 10,000 раз быстрее вне зависимости от пропускной способности сети
  - Подключайте дополнительные компьютеры через LAN и через Internet
- **Наши рекомендации:**
  - Единственный компьютер с видеокартой работает быстрее 50-ти компьютеров без видеокарт
  - Кластер компьютеров с видеокартами обеспечивает производительность порядка нескольких терафлоп

Elcomsoft Distributed Password Recovery

- Ускорение с использованием GPU на картах AMD и NVIDIA
- Распределённые вычисления с линейным масштабированием без накладных расходов
- Поддержка до 128 ядер CPU и до 12 GPU (Win10) на каждом компьютере
- Поддержка огромного числа форматов файлов

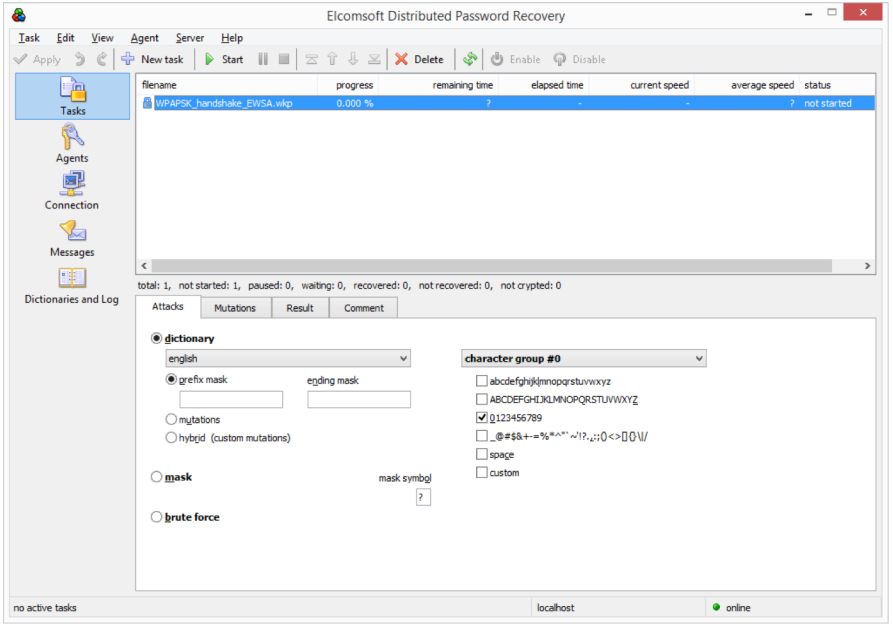


Elcomsoft Distributed Password Recovery

- Архивы ZIP, RAR, 7Zip
- Офисные приложения Microsoft Office 97 - 2019
- Open Office, Hangul Office
- PGP и OpenKey, IKE, TrueCrypt, BitLocker, FileVault
- Системные пароли (учётных записей, keychain и т.п.) Windows, UNIX, macOS
- Lotus(IBM) Notes, Oracle, The Bat!, Mozilla, FireFox, ThunderBird
- Apple iWork ‘09, 2013-2014
- Резервные копии BlackBerry (BB OS 6.0 – 7.1)

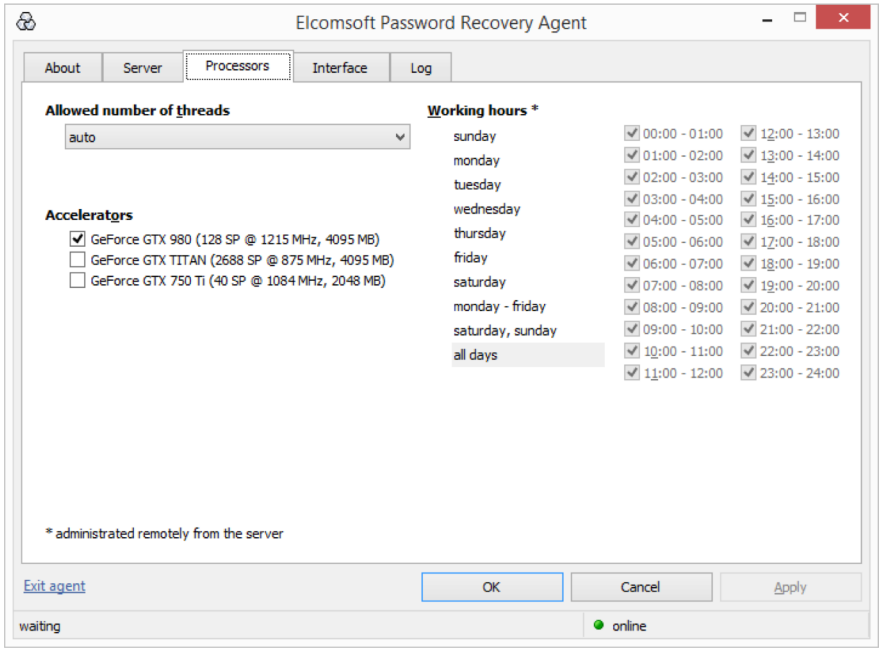
Elcomsoft Distributed Password Recovery

- Работа через LAN и/или Интернет
- Управление через консоль
- Минимальные требования к пропускной способности сети
- Агенты работают как системные службы
- Официальные сертификаты соответствия



Elcomsoft Distributed Password Recovery

- Удаленная установка и управление клиентами
- Гибкое управление задачами
- Контроль утилизации процессорного времени
- Расширяемость через плагины
- Найденные пароли автоматически сохраняются и используются в последующих задачах



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

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

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

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 ее использования низкая
- Поместите iPhone, подключенный к источнику питания, в клетку Фарадея

Клетка Фарадея

Используйте встроенное зарядное устройство!

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

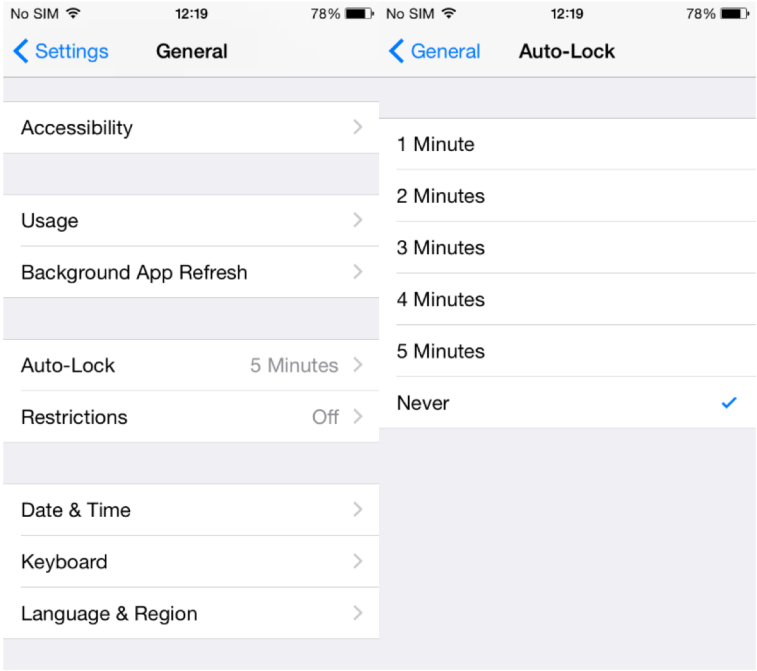
Как сохранить данные: предосторожности

- 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

Запрет блокировки экрана

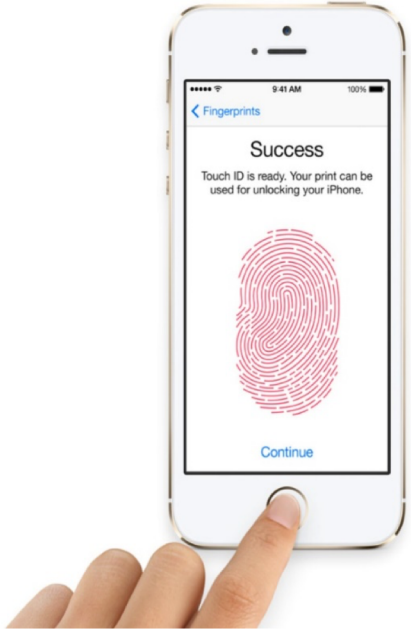
Отключение автоматической блокировки

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



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)



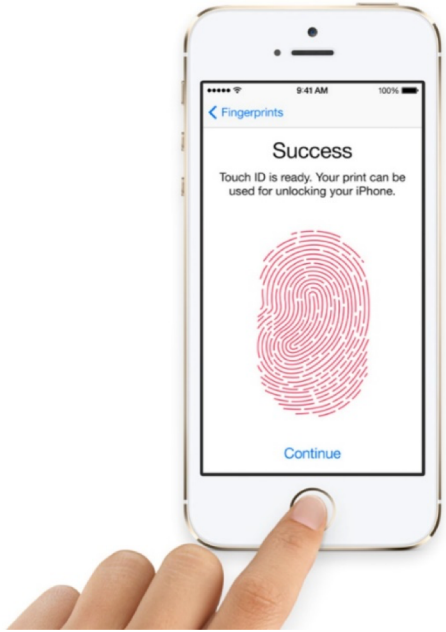
Если известен PIN или пароль блокировки

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



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

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 еще меньше информации

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

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)

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)

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)

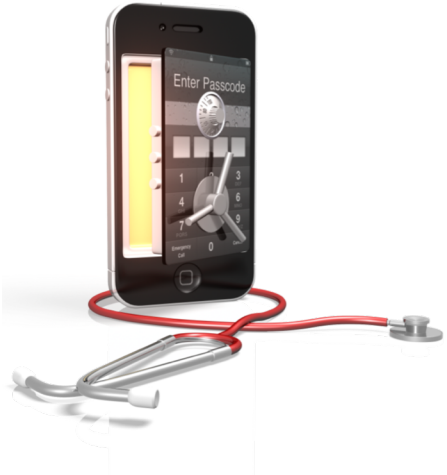
Методы извлечения данных

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)

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



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

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

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

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

Пароль на резервную копию

- Если задан пароль на резервную копию

Незашифрованные данные не покидают аппарат!*

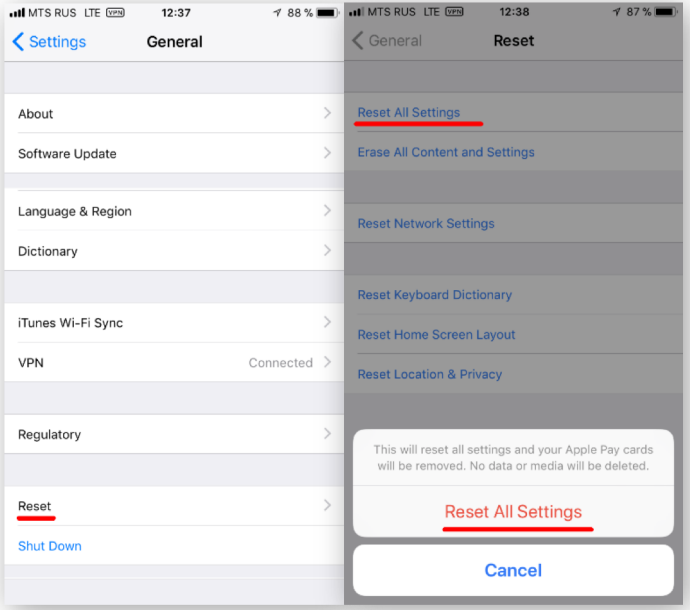
- Всё шифрование происходит внутри устройства (iPhone, iPad)
- iTunes просто получает зашифрованный поток данных
- Нет способа перехватить незашифрованные данные, поскольку их просто нет
- Если пароль неизвестен, его невозможно просто «сбросить»

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

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



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 разблокировано хотя бы раз после включения

iOS 4 до 8.2

- Можно достать практически всё, даже если включено шифрование резервных копий

iOS 8.3 и более новые

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

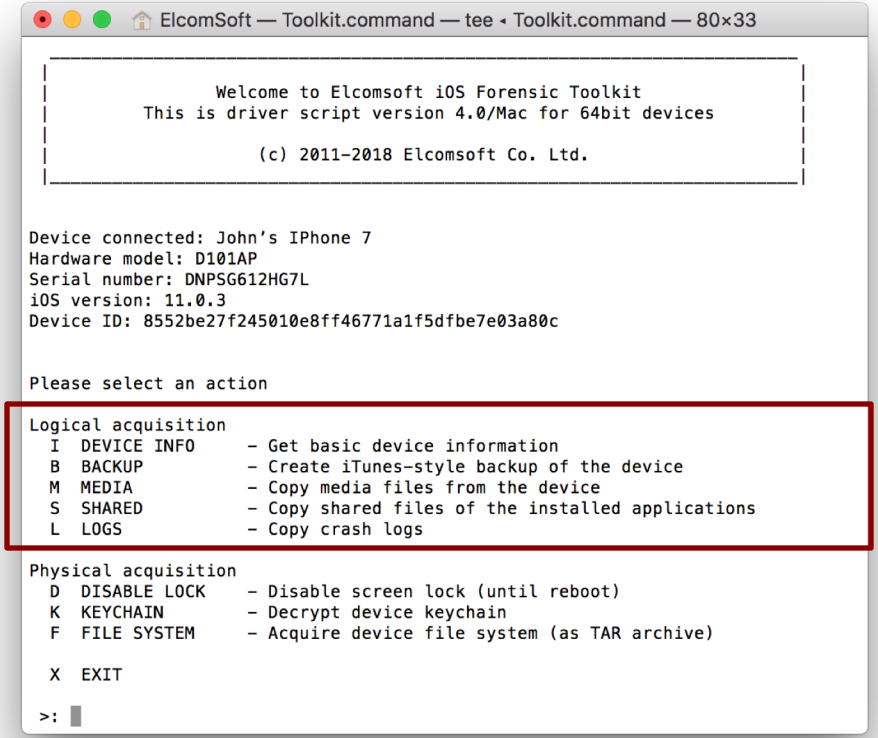
Используемые инструменты

- **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

Логическое извлечение

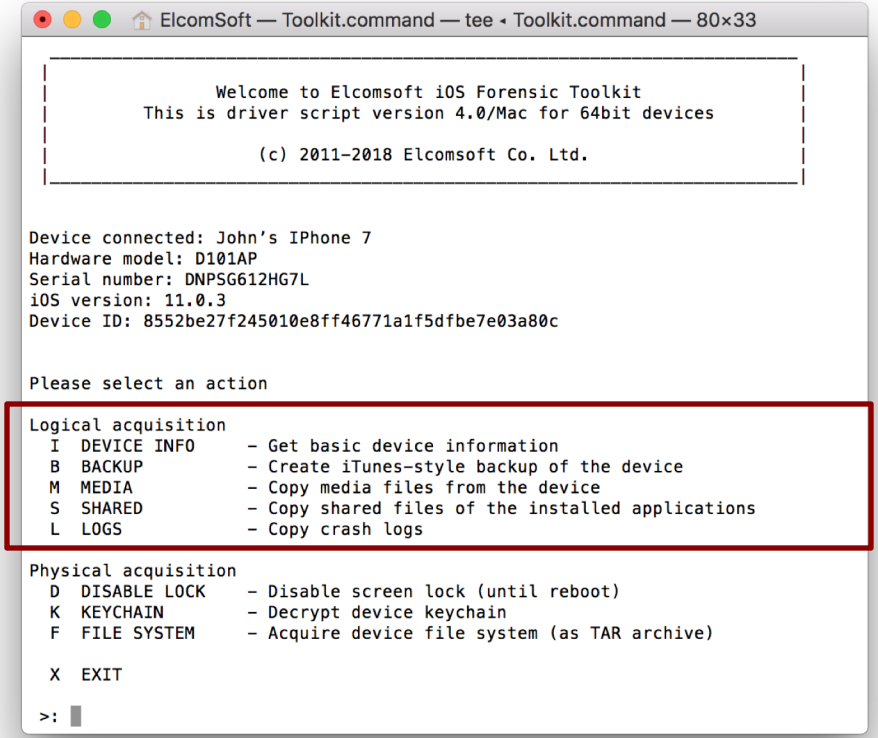
Последовательность шагов:

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



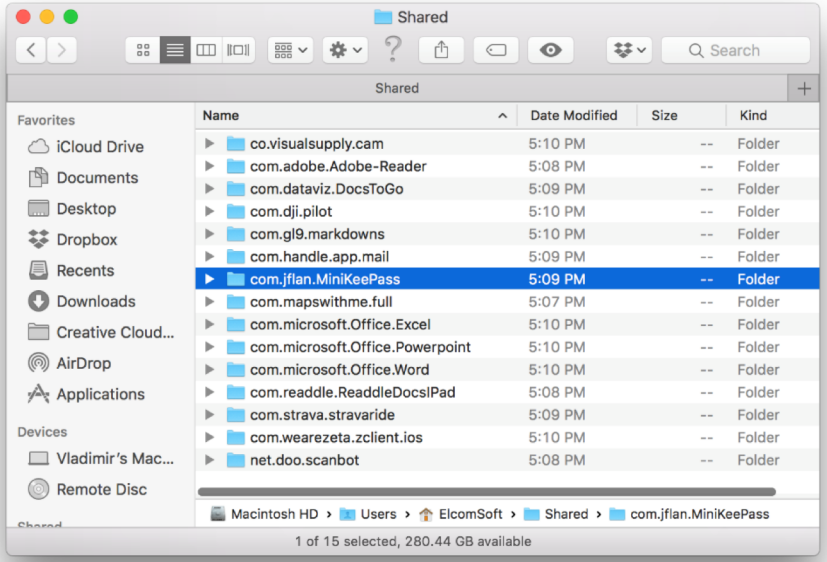
Информация об iPhone

- 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)



Файлы приложений

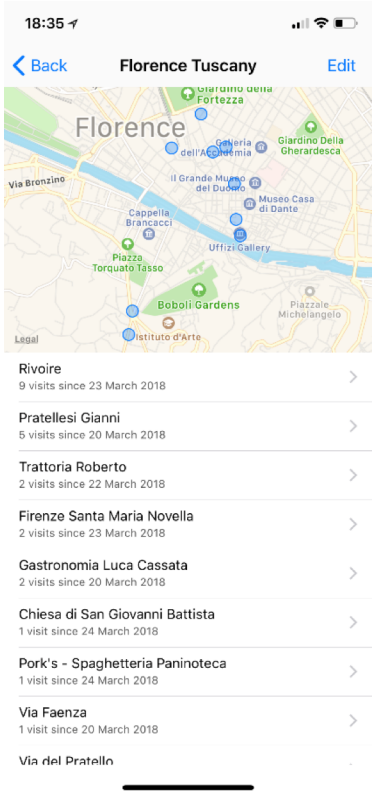
- Файлы, доступные через интерфейс iTunes File Sharing
- Могут содержать документы PDF (iBooks), БД с паролями
- Не защищаются паролем на резервную копию
- Другой механизм доступа в сравнении с резервными копиями
- **EIFT**: извлекает максимальное количество данных
-

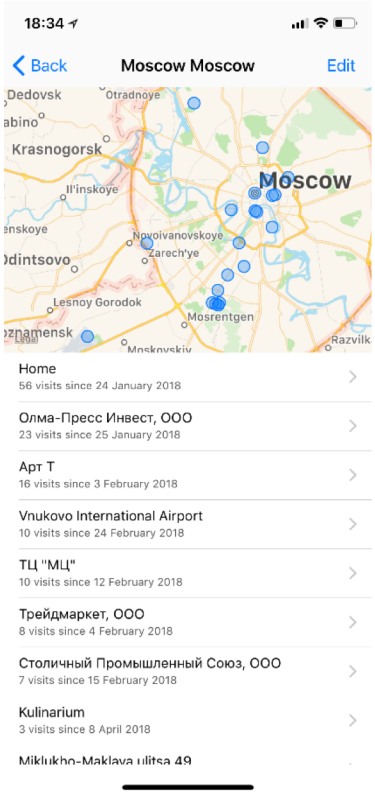


Чего нет в резервных копиях

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





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

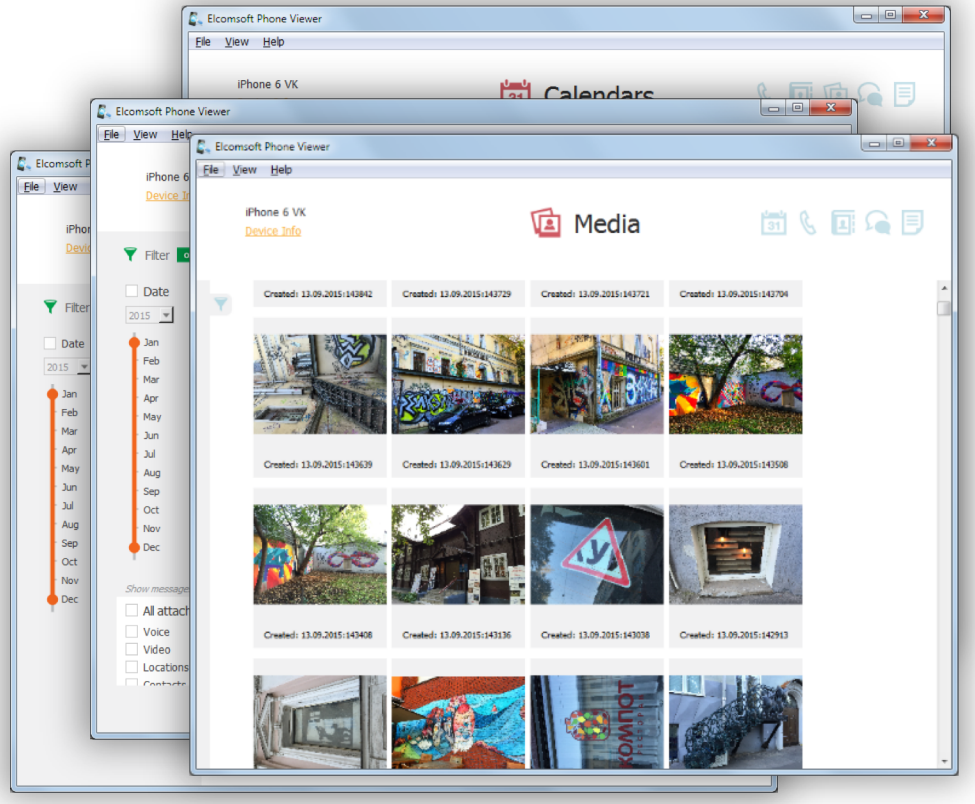
Используемые инструменты

- **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

Просмотр и анализ

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



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

Спасибо за внимание!

Александр Талипов ElcomSoft Co. Ltd.

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

Facebook: ElcomSoft
Twitter: @elcomsoft