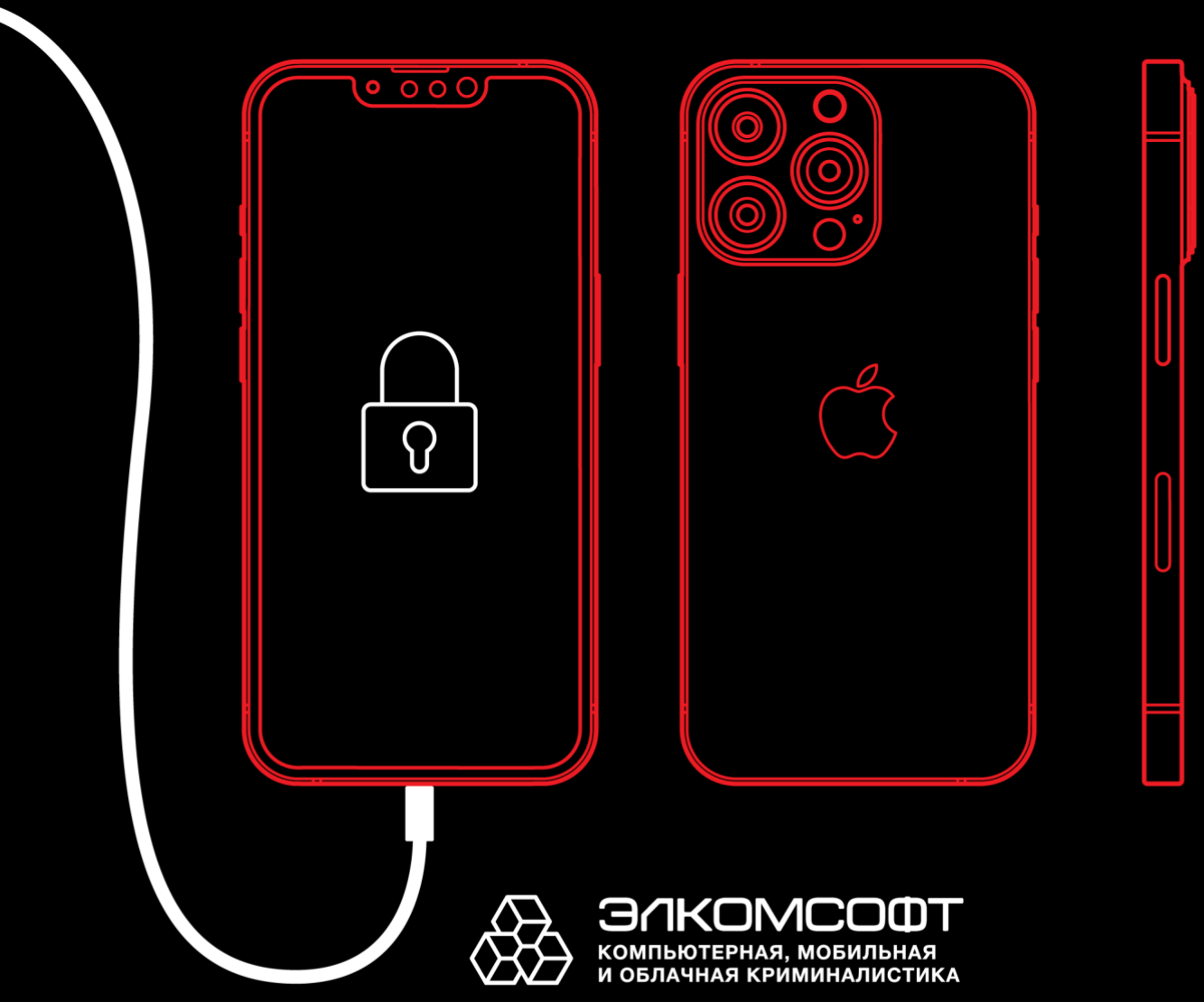
О. Д. Афонин, В. Ю. Каталов

Методическое руководство

по извлечению данных из iPhone и других устройств Apple



ЭЛКОМСОФТ
КОМПЬЮТЕРНАЯ, МОБИЛЬНАЯ
И ОБЛАЧНАЯ КРИМИНАЛИСТИКА

АПРЕЛЬ 2025

Москва

Содержание

1. Введение

В данном руководстве систематизирована информация по извлечению данных из iPhone и некоторых других устройств Apple, описаны подходы, стратегии и особенности разных методов, а также типичные ошибки.

В современном мире с повсеместным распространением носимой электроники устройства, операционные системы и облачные сервисы Apple занимают существенную часть рынка. Важные улики могут встретиться как в мобильном устройстве, так и в облаке или на компьютере злоумышленника. Всё это означает, что эксперту-криминалисту критически важно уметь извлекать и анализировать данные из различных источников. Мы хотим поделиться с вами набором методик, который не только поможет вам разобраться в современной мобильной экосистеме, но и позволит извлечь ценную информацию для анализа.

Важно отметить, что сама методика бесплатна и доступна каждому, однако упоминаемое в ней программное обеспечение, в том числе производства нашей компании, может распространяться на коммерческой основе. Извлечённые с помощью нашей методики данные можно далее использовать и анализировать как в других коммерческих программах, так и при помощи бесплатных скриптов и утилит, ссылки на которые приводятся в дополнительных материалах[1].

Настоящее методическое пособие – вовсе не о программах в чистом виде, однако без использования специализированного ПО в современной криминалистики обойтись невозможно. В пособии мы подробно расскажем о ряде продуктов, включая:

– **Elcomsoft Phone Breaker**, использующийся для извлечения данных из облака и расшифровке резервных копий iOS, защищённых паролем. Этот продукт – мультиплатформенный, с версиями для Windows и macOS.

– **Elcomsoft Phone Viewer**, в котором можно быстро просмотреть извлечённые другими нашими продуктами данные.

– **iOS Forensic Toolkit** – ещё один мультиплатформенный продукт, использующийся для извлечения данных из физических устройств iOS несколькими различными способами. Версия для Windows поддерживает расширенное логическое извлечение и низкоуровневый доступ посредством агента-экстрактора, а в версии для macOS к этим возможностям добавляется поддержка криминалистически чистого извлечения через эксплойт загрузчика.

Максимально возможный результат можно получить с использованием компьютера с macOS, но не стоит чрезмерно беспокоиться об ограничениях ПО для Windows: какую-то часть из них можно обойти тем или иным способом, и все эти способы описаны в настоящем пособии. Более того, многие возможности, которые мы рассмотрим в этой статье, доступны как пользователям macOS, так и Windows.

[1] Бесплатные утилиты, Наборы скриптов

2. С чего начать?

Исследование мобильного устройства начинается с его изъятия и транспортировки в лабораторию; возможно, до попадания на стенд устройство придётся какое-то время хранить. Правильное обращение с устройством в процессе его изъятия, хранения и транспортировки в лабораторию может упростить последующее извлечение и анализ данных. Неверный подход может привести к таким последствиям, как блокировка устройства или удалённое уничтожение улик.

При изъятии устройства необходимо оформить изъятие по действующим правилам, указав точное время и состояние устройство. Коротким нажатием на кнопку питания рекомендуем проверить, заблокирован ли экран устройства (см. ниже о предосторожностях, связанных с биометрическими датчиками).

Если устройство разблокировано, не допускайте блокировки экрана!

Для того, чтобы не допустить блокировки экрана, отключите таймер автоблокировки в настройках устройства: Настройки – Экран и яркость – Автоблокировка, установив значение «Никогда». Обратите внимание: в ряде случаев эта настройка может быть недоступной (например, при использовании внешних политик безопасности Exchange или MDM). В этом случае можно установить максимально доступное значение, после чего имитировать активность, периодически касаясь экрана устройства в процессе транспортировки.

2.1. Определение модели устройства

Успешный криминалистический анализ iPhone требует точной информации о том, какое именно устройство исследуется, каким процессором оборудовано и под управлением какой версии iOS оно работает. Рассмотрим несколько вариантов, которые помогут узнать, какой iPhone вы держите в руках, начиная с внешних признаков и нанесённых на корпус идентификаторов и заканчивая информацией, доступной исключительно программным способом.

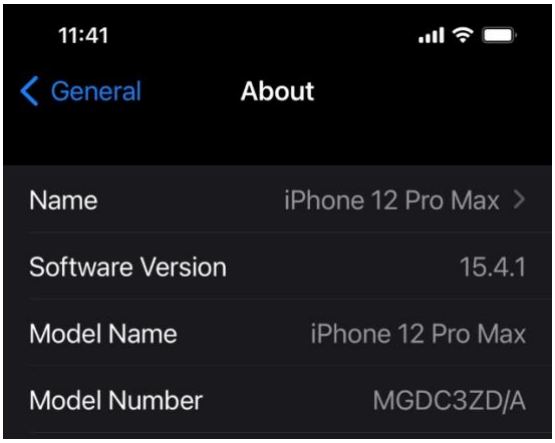
2.1.1. Программный способ (рекомендуемый)

С уверенностью определить номер модели устройства можно только программным способом. Информация о номере модели прошита в устройстве и не может быть изменена пользователем. В то же время внешние признаки (такие, как нанесённый на корпус номер) не являются стопроцентно надёжными: устройство могло побывать в ремонте с заменой корпуса; данные могут быть случайно или неслучайно затёрты; наконец, повреждения и следы использования могут сделать эту информацию нечитаемой. В некоторых ситуациях для доступа к нанесённому на корпус идентификатору модели необходимо извлечь лоток с SIM-картой, что может привести к нежелательным последствиям. Тем не менее, в ряде случаев приходится полагаться именно на те данные, которые нанесены на корпус устройства.

Самый надёжный способ определения модели – программный. Если устройство выключено, то узнать номер модели можно через режим диагностики[2]. Если включено и разблокировано – посмотреть в настройках устройства.

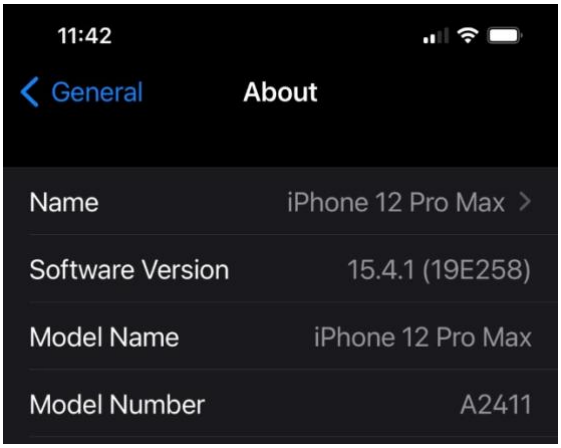
Устройство включено и разблокировано

Если устройство разблокировано, то будет достаточно открыть [Настройки] | [Об устройстве], где и будет указан номер модели.



В поле Model Number приводится полный идентификатор модели, позволяющий определить регион, для которого предназначено устройство (в показанном выше скриншоте – EMEA), объём встроенной памяти (256ГБ) и цвет (графит). Для получения этой информации попробуйте запустить поиск по идентификатору: MGDC3ZD/A.

Чтобы узнать простой идентификатор модели в формате Axxxx, достаточно коснуться строки Model Number. Кроме того, вы можете узнать подробную информацию о номере сборки iOS, коснувшись строки Software Version.



Устройство выключено или заблокировано

Для выключенных и/или заблокированных устройств можно воспользоваться одним из специальных режимов (см. следующий раздел, **Способ 1: режим диагностики**).

[2] Режим диагностики

2.1.2. Идентификация модели по внешнему виду

Однозначно определить модель устройства только по его внешнему виду не всегда представляется возможным в силу сходства дизайна разных моделей. Тем не менее, многие модели обладают характерными признаками, наличие которых помогает установить поколение устройства и его положение в линейке. На сайте Apple доступны инструкции с фотографиями устройств:

– Определение моделей iPhone[3]
– Определение моделей iPad[4]
– Определение моделей iPod[5]
– Определение моделей Apple TV[6]
– Определение модели часов Apple Watch[7]

Определить номер модели устройства только по внешнему не всегда удастся, особенно при наличии повреждений или заметных следов использования. С большей (но не абсолютной) точностью модель устройства можно определить по нанесённой на него маркировке.

2.1.3. Поиск номера модели устройства по маркировке

С некоторой вероятностью номер модели устройства можно определить по маркировке, нанесённой на корпус устройства. О том, как это сделать, на сайте Apple есть соответствующая статья:

– Поиск номера модели iPhone, iPad или iPod touch[8]

Инструкция на сайте Apple содержит информацию о том, что номер модели устройства наносится на обратную сторону устройства, если речь идёт об устройствах iPhone 7 и более ранних версиях, а также всех моделях iPad и iPod touch. В то же время на более новых моделях iPhone, начиная с линейки iPhone 8, 8 Plus и iPhone X, задняя крышка устройства лишена идентифицирующих надписей. Номер модели таких устройств можно определить после извлечения лотка для SIM-карты; соответствующий номер будет доступен в следующем виде:

[3] https://support.apple.com/ru-ru/HT201296
[4] https://support.apple.com/ru-ru/HT201471
[5] https://support.apple.com/ru-ru/HT204217
[6] https://support.apple.com/ru-ru/HT200008
[7] https://support.apple.com/ru-ru/HT204507
[8] https://support.apple.com/ru-ru/HT208200

Обратите внимание: извлечение из телефона SIM-карты из работающего телефона может привести к нежелательным последствиям! В современных версиях iOS извлечение SIM-карты приводит к эффекту, сравнимому с активацией режима S.O.S., в котором, в частности, блокируется передача данных через порт USB и отключаются биометрические датчики (для их повторной активации потребуется разблокировать телефон при помощи кода блокировки).

Номер модели указывается в формате Axxxx, где «xxxx» – это четыре цифры. По этому номеру можно в точности определить как саму модель телефона (например, iPhone 8 Plus), так и поколение процессора (SoC). В то же время номер модели не включает в себя информации о регионе, для которого предназначено устройство, о его цвете или объёме встроенной памяти. Вся эта информация закодирована в другом, более длинном идентификаторе, который доступен программным способом.

Помимо идентификатора модели, который нанесён на корпус устройства, на самом лотке для SIM-карты может присутствовать идентификатор IMEI. Рекомендуем отнестись к этой информации с осторожностью, т. к. оригинальный лоток для SIM-карты может быть заменён пользователем.

Почему этот способ ненадёжен: во время ремонта в неавторизованных сервисах задняя крышка заменяется на крышку от другой модели или неоригинальную, что ведёт к изменению видимого идентификатора модели.

2.2. Специальные режимы: Diagnostic, Recovery и DFU

В статье «Роль специальных режимов iOS в мобильной криминалистике: DFU, Recovery и SOS»[9] описан способ, помогающий определить модель устройства из специальных режимов Recovery и DFU, а в статье «Доступ к серийному номеру, MAC, MEID и IMEI заблокированного iPhone»[10] рассказывается о том, как получить доступ к режиму диагностики и получить из него данные об устройстве.

Этот способ имеет смысл использовать, если определить модель устройства по внешним признакам не удаётся, а само устройство находится в выключенном состоянии. Код блокировки экрана для проверки идентификатора модели в режимах диагностики, восстановления и DFU не требуется.

2.2.1. Способ 1: режим диагностики

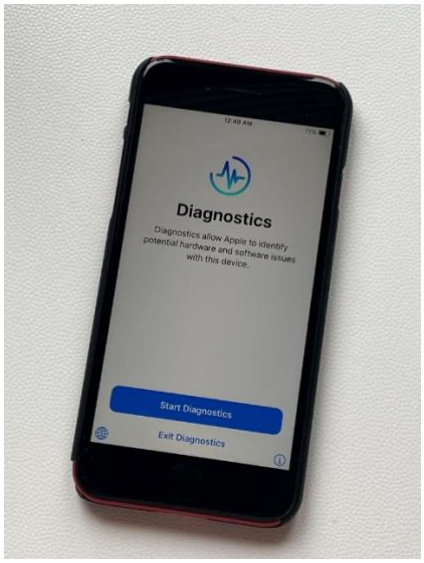
В режиме диагностики iPhone прямо на экране устройства доступны такие данные, как серийный номер устройства, идентификаторы IMEI и MEID. С использованием iOS Forensic Toolkit можно получить дополнительную информацию – точный идентификатор модели и цвет устройства, версию и номер сборки iOS, а также MAC-адрес адаптера Wi-Fi. Режим диагностики доступен даже тогда, когда iPhone заблокирован, а код блокировки экрана неизвестен.

Для ввода устройства в режим диагностики проделайте следующие шаги.

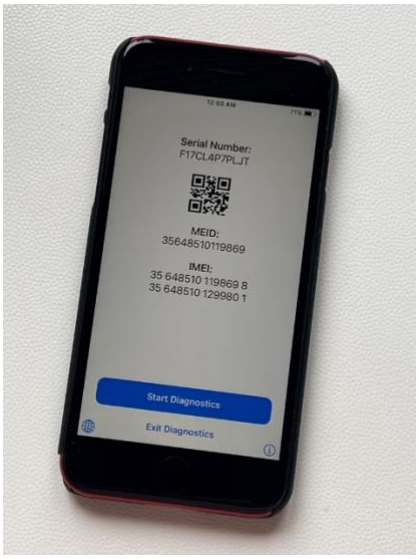
[9] https://blog.elcomsoft.ru/2020/02/rol-speczialnyh-rezhimov-ios-v-mobilnoj-kriminalistike-dfu-recovery-i-sos/

[10] https://blog.elcomsoft.ru/2023/03/dostup-k-serijnomu-nomeru-mac-meid-i-imei-zablokirovannogo-iphone/

1. Нажмите и удерживайте кнопки увеличения и уменьшения громкости.
2. Удерживая обе кнопки, подключите кабель Lightning к iPhone, после чего подключите его к компьютеру или адаптеру питания.
3. Дождитесь появления логотипа Apple, затем отпустите кнопки.



На следующем экране будут отображены серийный номер устройства и его идентификаторы MEID и IMEI.



В режиме диагностики доступна дополнительная информация об устройстве, получить доступ к которой можно при помощи iOS Forensic Toolkit. Сюда входят:

- Номер модели и цвет устройства;
- MAC-адрес сетевого адаптера Wi-Fi;
- Номер версии и номер сборки iOS;
- Идентификаторы некоторых аппаратных устройств;
- Дополнительная информация, которую можно экспортировать в файл XML.

2.2.2. Способ 2: режим Recovery

Режим восстановления (в англоязычных источниках – iOS recovery mode) используется для восстановления доступа к устройству через компьютер (имеется в виду приложение iTunes) в случае, когда что-то пошло не так. Режим восстановления доступен в том числе для заблокированных устройств и устройств с неизвестным кодом блокировки.

В сравнении с режимом диагностики, режим восстановления возвращает заметно меньшее количество данных. Проще всего устройство переводится в режим Recovery по инструкции в статье Не удается выполнить обновление или восстановление iPhone или iPod touch[11] (раздел «Перевод устройства в режим восстановления и повторная настройка»).

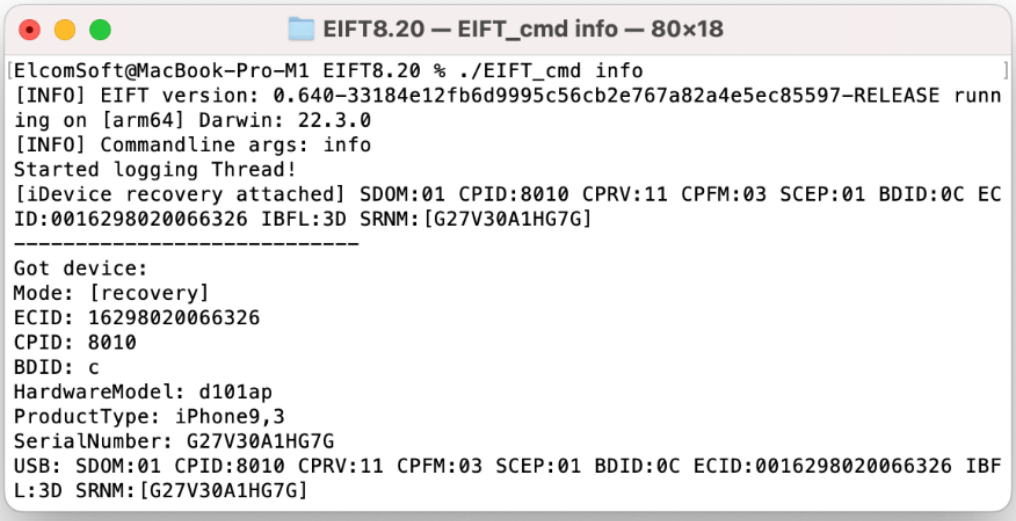
В режиме Recovery доступна следующая информация:

- Device model и Model: идентификация модели устройства в двух разных представлениях. К примеру, iPhone7,2 (n61ap), iPhone10,6 (d221ap) и т. п.
- ECID (UCID). Идентификатор ECID (Exclusive Chip Identification) или Unique Chip ID (UCID) уникален для каждого конкретного устройства (а точнее, установленного в нём процессора).
- Serial number: серийный номер устройства.

[11] Не удается выполнить обновление или восстановление iPhone или iPod touch: https://support.apple.com/ru-ru/HT201263

Дополнительная информация о режиме восстановления:

Роль специальных режимов iOS в мобильной криминалистике: DFU, Recovery и SOS[12]



2.2.3. Способ 3: режим DFU

В отличие от режима Recovery, режим DFU не предназначен для широкого использования. Он плохо документирован, а для его использования необходимо точно соблюдать тайминги. Перевод в этот режим может быть затруднён, если одна или несколько аппаратных кнопок на устройстве отказали[13].

В режиме DFU доступно ещё меньше данных, чем в режиме Recovery, и намного меньше по сравнению с режимом диагностики.

– Device model: идентификация модели устройства в двух разных представлениях.

– Идентификатор ECID (Exclusive Chip Identification) или Unique Chip ID (UCID) уникален для каждого конкретного устройства (а точнее, установленного в нём процессора).

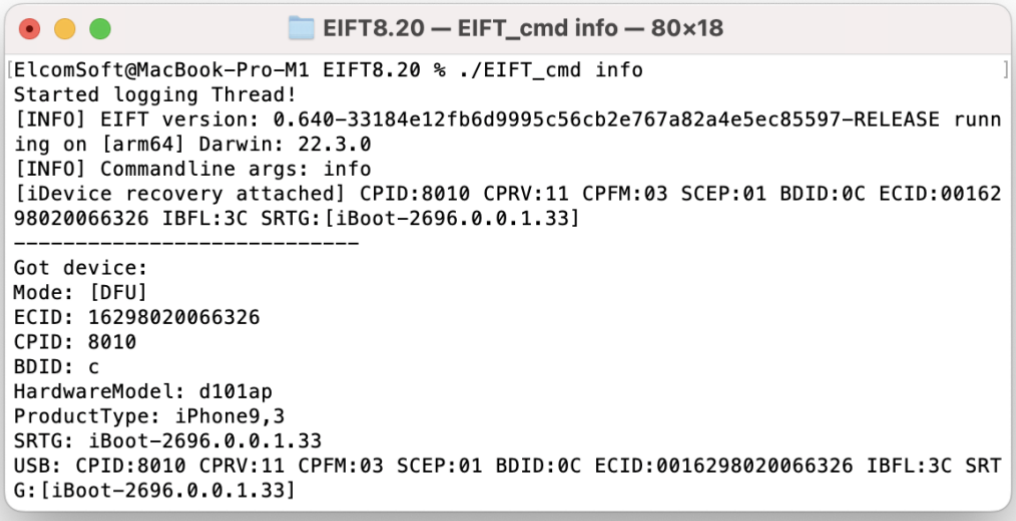
Серийный номер и IMEI недоступны. В режиме DFU недоступен номер версии iOS, однако доступна версия **iBoot**, по которой можно с большей или меньшей точностью угадать номер сборки iOS.

Дополнительная информация о режиме DFU и о том, как ввести в него[10] различные устройства Apple:

[12] https://blog.elcomsoft.ru/2020/02/rol-speczialnyh-rezhimov-ios-v-mobilnoj-kriminalistike-dfu-recovery-i-sos/

[13] https://blog.elcomsoft.ru/2021/09/apparatnyj-sposob-perevoda-iphone-v-rezhim-dfu-kogda-ne-rabotayut-knopki/

Роль специальных режимов iOS в мобильной криминалистике: DFU, Recovery и SOS



Существуют сервисы, позволяющие по серийному номеру устройства узнать дополнительную информацию о нём.

2.3. Блокировка экрана и биометрические датчики

В этом разделе описаны риски, которые приводят к необходимости дополнительных мер по защите данных.

Первый риск возникает непосредственно в момент изъятия устройства. Современные модели iPhone и планшетов iPad оборудованы биометрическими датчиками, позволяющими разблокировать экран устройства без ввода пароля (кода блокировки экрана).

Уровень безопасности биометрических датчиков (сканера отпечатков пальцев Touch ID и сканера лица Face ID) ниже уровня безопасности, обеспечиваемого кодом блокировки экрана. По этой причине их использование блокируется операционной системой как при возникновении признаков угрозы, так и по истечении определённого времени, которое исчисляется по достаточно сложным правилам.

Угрозой с точки зрения операционной системы считаются такие действия, как попытка разблокировки устройства не зарегистрированным ранее отпечатком пальца или образом лица. До момента блокировки биометрических датчиков, после которого разблокировать устройство можно лишь посредством пароля – пять попыток.

- Биометрические датчики блокируются после 5 неудачных попыток;
- Или через 48 часов с момента последней разблокировки;
- Или через 8 часов, если код блокировки экрана не вводился 6 дней подряд.

Блокировка биометрических датчиков приведёт к невозможности разблокировать устройство посредством датчиков Touch ID или Face ID. Вместо этого для разблокировки устройства придётся использовать только код-пароль (код блокировки экрана), который может быть неизвестен.

Обратите внимание: при изъятии устройства нельзя касаться кнопки Touch ID (для проверки устройства допустимо использовать короткое нажатие на кнопку питания). Для современных iPhone, оборудованных системой Face ID, недопустимо попадание «в кадр» посторонних лиц; в противном случае будет использована одна из пяти доступных попыток разблокировки. (Именно такая ситуация возникла во время презентации со сцены первого iPhone X, оборудованного системой разблокировки по лицу).

– **Не прикасайтесь** к датчику Touch ID. Используйте короткое нажатие на кнопку питания.

– **Обращайтесь с оборудованными системой Face ID устройствами с особой осторожностью.** Не допускайте попадания «в кадр» посторонних лиц, чтобы не использовать одну из 5 попыток биометрической разблокировки. Возможный вариант – заклеить датчики Face ID непрозрачной лентой.

2.4. «Защита украденного устройства»

В обсуждении кода блокировки экрана и биометрического способа аутентификации нельзя не рассказать об относительно новом (появился в iOS 17.3) способе дополнительной защиты, комбинирующем оба способа.

До выхода iOS 17.3 (а точнее, iOS 17.3 Developer Preview, в которой впервые появился прототип рассматриваемой функции) для подключения iPhone к компьютеру и подтверждения доверия к устройству требовался только код блокировки экрана. Теперь же у пользователя появилась возможность включить дополнительный уровень защиты. После его активации как для сопряжения с компьютером, так и для совершения целого ряда других действий, затрагивающих чувствительную информацию, кода блокировки уже недостаточно; теперь для сопряжения с новым компьютером нужен и код блокировки экрана, и дополнительная аутентификация с помощью Face ID или Touch ID.

Обратите внимание: в официальном описании функции «Защита украденного устройства» на сайте Apple[14] требование биометрической аутентификации для сопряжения iPhone с компьютером не упоминается; тем не менее, защита срабатывает.

«Защита украденного устройства» значительно затрудняет логическое извлечение данных. Если до появления этой функции для привязки было достаточно разблокировать устройство и ввести код блокировки экрана, то теперь необходимо подтвердить личность владельца биометрией. В случае, если владелец устройства отсутствует или биометрические данные предоставить невозможно, логический анализ смартфона становится практически невозможным.

[14] https://support.apple.com/ru-ru/120340

При включении этой функции, вероятно, единственным оставшимся методом анализа будет ручной, механический просмотр содержимого устройства с фото-видео фиксацией и созданием скриншотов. Такой способ доступа к данным считается самым инвазивным из возможных; при его проведении нужно тщательно соблюдать все предосторожности по работе с устройством и вести тщательное документирование каждого шага процесса.

2.4.1. Отключение защиты

Можно попробовать отключить функцию защиты украденного устройства, однако здесь присутствует сразу ряд моментов, усложняющих процесс.

Во-первых, для отключения «защиты украденного устройства» вам всё равно понадобится биометрическая аутентификация. Во-вторых, если пользователь не изменял настройки по умолчанию, при попытке отключить защиту система установит дополнительную задержку в течение часа, если устройство не находится в «знакомом месте». Это означает, что для отключения защиты потребуется два подтверждения с помощью Face ID или Touch ID: первое - при начале процесса изменения настроек, второе - после завершения тайм-аута.

2.4.2. «Знакомые места» и их значение

В рамках функций «Защиты украденного устройства» Apple предоставляет пользователю выбор: ряд функций безопасности (в частности - часовая задержка при отключении дополнительной защиты) может срабатывать каждый раз или только тогда, когда попытка делается вдали от «знакомых мест» (настройка называется "Away from Familiar Locations"). По умолчанию, если пользователь не изменит настройку вручную, многие дополнительные меры безопасности функции «Защита украденного устройства» применяются только тогда, когда iPhone находится вдали от знакомых мест.

Практическое следствие: отключать защиту либо проводить ручной осмотр имеет смысл по возможности в одном из «знакомых мест», каковыми являются, как правило, такие места, где пользователь проводит больше всего времени (дом, работа). Деталей работы этой функции Apple не раскрывает.

2.4.3. Дополнительная защита и резервные копии

В документации Apple указано: «При восстановлении из резервной копии iCloud или переносе непосредственно с предыдущего iPhone на новый также восстанавливаются настройки вашего устройства, включая функцию «Защита украденного устройства». После небольшой задержки, чтобы синхронизировать привычные места из iCloud, на новом устройстве автоматически возобновляются меры безопасности для защиты украденного устройства.»

Кроме того, отметим, что перенести данные на новое устройство с включённой дополнительной защитой также не удастся: в документации упомянуто «Использование iPhone для настройки нового устройства (например, с помощью функции «Быстрое начало»)».

Таким образом, отметим, что, несмотря на свою пользу для рядовых владельцев iPhone, функция защиты украденного устройства создаёт значительные препятствия для

экспертов по цифровой криминалистике, осложняя легальное извлечение данных из смартфонов, изъятых у преступников.

2.5. Режимы S.O.S. и защитный режим USB

Режим блокировки USB, также известный как защитный режим USB, появился в iOS 12.4.1. Этот режим предназначен для защиты устройств от несанкционированного доступа при подключении устройства к компьютеру или цифровому аксессуару через порт Lightning или USB Type-C.

Один из способов ручной активации защитного режима USB, также блокирующий и биометрические датчики – вызов режима Emergency / S.O.S. Этот режим вызывается нажатием той же комбинации кнопок, которая используется для выключения устройства. При его активации происходит блокировка передачи данных через порт USB и биометрических датчиков; для разблокировки устройства теперь можно использовать исключительно пароль (код блокировки экрана). Узнать о том, что данный режим был специально активирован, невозможно.

Если защитный режим USB будет активирован, то устройство невозможно будет ни сопрячь с новым компьютером, ни подключить к уже сопряжённому. Защитный режим USB активируется по любому из признаков:

– По таймеру: 1 час после блокировки экрана, если не был подключён цифровой аксессуар;

– Мгновенно, если активирован режим S.O.S.;

– Мгновенно, если подключить к заблокированному устройству новый цифровой аксессуар или подключить заблокированное устройство к новому компьютеру.

В настройках устройства пользователь может отключить активацию защитного режима USB. По умолчанию защитный режим USB активируется согласно описанным выше правилам. Дополнительная информация:

Разрешение подключения аксессуаров USB и других аксессуаров к iPhone, iPad или iPod touch - Служба поддержки Apple (RU)[15]

2.6. Риск удалённой блокировки устройства и уничтожения улик

Риск, которому подвергается устройство в процессе транспортировки и хранения – это риск удалённой блокировки и/или уничтожения данных. Для этого требуется войти в учётную запись пользователя на сайте https://www.icloud.com/find[16] (достаточно только логина и пароля, проходить двухфакторную аутентификацию не нужно), после чего устройство можно локализовать, заблокировать или сбросить к заводским настройкам с удалением всех данных.

Все эти действия с устройством можно проделать только в том случае, если устройство подключено к сети передачи данных посредством мобильной связи или Wi-Fi (локализация устройств, оборудованных чипом U1, возможна даже без подключения

[15] https://support.apple.com/ru-ru/HT208857
[16] https://www.icloud.com/find

устройства к сети). Соответственно, одна из задач при транспортировке устройства – изолировать его от беспроводных сетей.

2.7. Криминалистическая чистота извлечения

Перед тем, как приступить к анализу устройства и извлечению данных, необходимо определить цель извлечения. В контексте мобильной криминалистики полученная из устройства или из облачного сервиса информация обретает статус «цифровых улик». Необработанные данные, какими бы они ни были, крайне редко являются уликами или, тем более, доказательствами. Извлечённые данные необходимо анализировать, трактовать, часто связывать между собой (иногда из разных источников). В настоящем пособии речь идёт о самом первом этапе, извлечении. Анализ данных – отдельная необъятная тема.

Сам термин «улика» имеет как юридическое, так и следственное применение. Далеко не всегда найденные улики, которые использовались в процессе следственных действий, могут быть предъявлены в суде; это полностью справедливо и для цифровых улик.

Во избежание путаницы, цифровые улики, которые могут быть предъявлены в суде, назовём «цифровыми доказательствами». На сегодняшний день требования к юридической допустимости цифровых улик слабо закреплены законодательно, поэтому допустимость использования цифровых улик в качестве доказательств устанавливается в процессуальном порядке.

Подытожим:

– Термин «цифровые улики» используется в следственном контексте

– Термин «цифровые доказательства» – в юридическом

– «Цифровые доказательства» — это «цифровые улики», которые можно представить в суде

– Обеспечение криминалистической чистоты процесса обработки данных позволяет использовать цифровые улики в качестве цифровых доказательств

– Для того, чтобы извлечённые из iPhone данные имели шанс получить статус «цифровых доказательств», необходимо точно выполнять все этапы процесса криминалистически чистого извлечения.

2.7.1. Что такое «криминалистически чистое» извлечение?

Криминалистически чистой считается такая **методика сбора информации, которая позволяет предъявлять цифровые улики в качестве доказательств в суде.** Для этого необходимо, чтобы вся цепочка обработки цифровых данных была непрерывной и криминалистически чистой, что достигается точным следованием плану обработки цифровых доказательств с защитой цифровых улик. Защита цифровых улик гарантирует целостность и неизменность цифровых данных, которые, в свою очередь, обеспечиваются грамотным использованием специальных средств.

Криминалистическая чистота извлечения необходима именно для того, чтобы «цифровые улики» стали полноценными «цифровыми доказательствами», которые можно представить в суде. Фактически, криминалистическая чистота состоит из двух

моментов: криминалистической чистоты самого извлечения и гарантии неизменности (проверяемой на всех этапах) данных по пути от эксперта в суд.

На сегодняшний день не существует формальных юридических требований, относящихся к допустимости в качестве улик цифровых данных, полученных при анализе данных, полученных путём извлечения любых цифровых носителей информации, включая компьютеры, смартфоны, камеры наблюдения и т.п. Возможность использовать собранные улики в качестве доказательств как в нашей стране, так и во многих других, определяется в суде в рамках состязательного процесса. Демонстрация соблюдения криминалистической чистоты извлечения – важный и зачастую определяющий фактор, влияющий на то, будут ли допущены в качестве доказательств те или иные цифровые улики.

С технической точки зрения криминалистически чистое извлечение должно отвечать следующим условиям:

1. **Неизменность**: информация на устройстве не должна модифицироваться в процессе извлечения.
2. **Верифицируемость**: должна быть возможность подтвердить подлинность извлечённых данных. Как правило, для этого используется сверка цифровой подписи, в роли которой часто используется контрольная сумма, вычисленная посредством стойкого алгоритма (SHA-1, SHA-256 и т. п.)
3. **Повторяемость**: повторное извлечение данных из того же устройства должно выдавать в точности тот же результат (для проверки идентичности производится сверка контрольных сумм).

В современных устройствах реально достижим второй пункт; с первым и третьим возникают проблемы. Для ограниченного набора устройств предыдущих поколений возможна реализация всего набора.

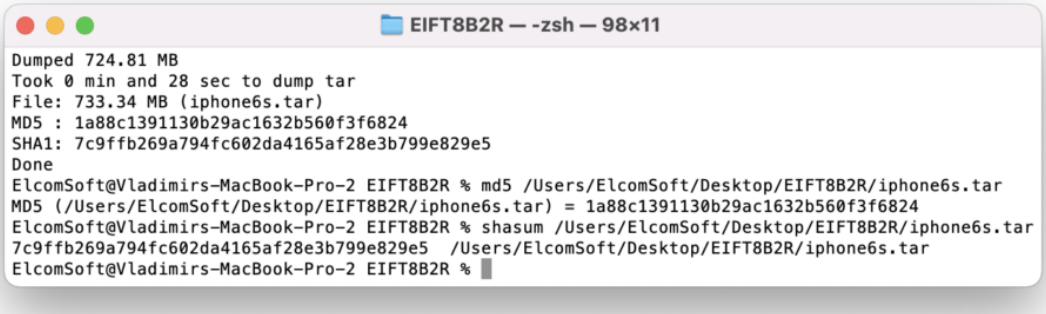
2.7.2. Целостность и неизменность пользовательских данных

Контроль целостности и неизменности извлечённых из устройства цифровых улик – важнейшая часть криминалистической чистоты процесса анализа. Контроль целостности позволяет проверить, не были ли извлечённые из устройства данные каким-либо образом изменены уже после того, как произошло извлечение. Обратите внимание: в этой части процесса никак не проверяется аутентичность самих цифровых улик, а только соответствие того набора данных, который был изначально извлечён из устройства тому, который был представлен в качестве цифровых доказательств.

В цифровой криминалистике в целом и мобильной криминалистике в частности целостность и неизменность цифровых улик проверяется вычислением контрольных сумм, в качестве которых используются значения криптографических хэш-функций. Важное свойство криптографических хэш-функций в том, что изменение даже единственного бита в оригинальном наборе данных приведёт к тому, что результирующее значение контрольной суммы будет кардинально отличаться от оригинала.

Для вычисления контрольных сумм в цифровой криминалистике традиционно используются функции **MD5** (считается устаревшей) и **SHA1**, в последние годы наблюдается переход к **SHA256**.

При создании образа файловой системы Elcomsoft iOS Forensic Toolkit[17] автоматически подсчитывает контрольные суммы в форматах MD5 и SHA1. Делается это для того, чтобы эксперт мог сохранить или распечатать контрольные суммы, которые впоследствии можно проверить для контроля целостности образа и доказательства неизменности извлечённых из устройства улик с момента извлечения. Несмотря на то, что функция MD5 считается устаревшей, совпадение обеих контрольных сумм гарантирует соответствие проверяемого набора данных оригиналу. Контрольные суммы выводятся в программе в следующем виде:



2.7.3. Проверка целостности данных

Для проверки контрольной суммы рекомендуем использовать утилиту командной строки certutil в следующем формате:

```
certutil -hashfile FILENAME md5|sha1|sha256
```

При успешном прохождении проверки выводится следующий результат:

```
MD5 hash of disk.e01: 0d8a7ca3d87bf6c202c26dc363983836

CertUtil: -hashfile command completed successfully
```

Более подробно о контрольных суммах – в нашей статье Данные Шредингера[18].

Применимость: целостность *уже извлечённых из устройства данных* можно и нужно контролировать независимо от метода, посредством которого данные были извлечены. В то же время *повторяемость результатов извлечения* способен обеспечить лишь один метод, основанный на эксплойте загрузчика и доступный только для устаревших устройств Apple.

[17] https://www.elcomsoft.ru/eift.html
[18] https://blog.elcomsoft.ru/2021/11/dannye-shredingera/

2.7.4. Повторяемость результата

Верифицируемость извлечённых данных вовсе не обязательно означает повторяемость результата извлечения данных. Повторяемым считается такое извлечение, в результате которого повторное каждое последующее метода выдаст такой же результат, что и самое первое извлечение. Проверить совпадение данных проще всего сравнением контрольных сумм, о которых было рассказано выше.

В отличие от контроля целостности и неизменности данных, которые *уже были извлечены*, повторяемость результата гарантирует, что из устройства были извлечены *именно те данные*, которые были представлены в качестве цифровых доказательств. В свою очередь, контроль целостности и неизменности гарантирует, что цифровые доказательства дошли до суда именно в таком виде, в каком они были извлечены из устройства.

Если целостность уже извлечённых данных проконтролировать просто (для этого достаточно подсчитать и сравнить контрольные суммы), то обеспечить повторяемость результата – чрезвычайно тяжело, а в ряде случаев – невозможно даже в теории. В Elcomsoft iOS Forensic Toolkit повторяемость извлечения обеспечивается при точном следовании инструкциям в процессе использования единственного метода – извлечения посредством эксплойта загрузчика.

Применимость: повторяемость результата достижима при использовании метода извлечения на основе эксплойта загрузчика в Elcomsoft iOS Forensic Toolkit. К сожалению, этот метод совместим с устройствами старых поколений (вплоть до iPhone 7/7 Plus, и весьма условно – с iPhone 8, 8 Plus и iPhone X). Для более новых устройств обеспечить повторяемый результат извлечения в настоящий момент не представляется возможным.

Вывод: с технической точки зрения, обеспечить повторяемость результата возможно не всегда. По этой причине эксперт должен сразу запросить у следствия разрешение на внесение изменений в содержимое устройства, дождаться его получения, и только после этого приступать к извлечению и исследованию содержимого устройства.

Отметим также, что само по себе использование checkm8 гарантии повторяемости не даёт. Важна как правильная реализация метода, так и чёткое следование инструкциям. Мы постарались упростить этот процесс, уменьшив вероятность ошибки в процессе повторных сессий по извлечению данных.

2.7.5. Достижима ли криминалистическая чистота извлечения в современных устройствах?

В ряде случаев идеальную криминалистическую чистоту в её формальном определении обеспечить невозможно, поскольку данные извлекаются из работающего устройства или системы. Этот процесс невозможно проконтролировать полностью, и часть данных на устройстве неизбежно меняется в процессе извлечения.

В то же время для ряда моделей криминалистическая чистота достижима. Это относится ко всем моделям iPhone из диапазона iPhone 4 – iPhone 7, а также другим устройствам Apple, для которых доступен эксплойт checkm8 или другой эксплойт загрузчика (для устаревших моделей). Для моделей iPhone 8 iPhone 8 Plus и iPhone X возможно верифицируемое и повторяемое извлечение, но лишь при определённых условиях. Так, если такое устройство работает под управлением iOS 15, для извлечения данных потребуется удаление кода блокировки, что приводит к ряду последствий; соответственно, такой процесс не является криминалистически чистым в классическом смысле слова, являясь, тем не менее, повторяемым и верифицируемым.

2.7.6. Краткий обзор методов извлечения данных

Для современных моделей iPhone существует несколько разных способов извлечения данных. Основные из них:

– расширенное логическое извлечение: из телефона извлекается резервная копия данных, медиа-файлы и некоторые другие данные. Этот метод доступен для всех устройств iPhone и iPad независимо от версии iOS;

– облачный анализ: данные скачиваются из облака (в данном случае – из iCloud);

– запрос у производителя: правоохранительные органы могут запросить копию данных из облака непосредственно у Apple. Компания предоставляет не все данные (а при использовании Advanced Data Protection – предоставляет минимальный набор информации), зато цифровые улики юридически грамотно оформляются;

– низкоуровневый анализ: на работающем устройстве эксперт пытается получить права суперпользователя для доступа к файловой системе;

– эксплойт загрузчика: единственный способ, которым можно получить полностью повторяемый, криминалистически чистый результат. Он доступен только для старых моделей – до iPhone 7/7s Plus включительно (с оговорками – для iPhone 8/8 Plus/iPhone X).

2.7.7. Криминалистическая чистота логического анализа

Каким образом нужно действовать для того, чтобы данные, извлечённые из устройства, можно было использовать не только в качестве улик, использующихся в процессе следственных действий, но и в качестве доказательств, которые можно представить в суде?

Метод расширенного логического извлечения – самый простой, универсальный и оттого распространённый способ извлечения цифровых улик. В рамках расширенного логического анализа создаётся резервная копия данных, извлекаются фотографии с сопутствующими метаданными (включая данные о местоположении), копируются некоторые системные журналы и данные приложений, доступные штатным образом.

В то же время **логический анализ** – это всегда извлечение из работающего устройства. Более того, в терминах компьютерной криминалистики логический анализ iPhone является, по сути, исследованием работающего устройства с авторизованной

пользовательской сессией. На устройстве загружена операционная система, работают приложения. Если устройство подключится к беспроводной сети, то существует риск блокировки или удаления данных по команде извне.

С технической точки зрения о криминалистической чистоте извлечения в процессе логического анализа не может быть и речи: две последовательно созданных резервных копии будут отличаться; их контрольные суммы не совпадут.

Несмотря на это, судебная практика говорит об обратном: данные из резервных копий iPhone и извлечённые из устройств фотографии довольно часто используются в суде в качестве доказательств несмотря на известные недостатки процесса. Для того, чтобы собранные данные можно было представить в суде, необходимо придерживаться чётких правил во время всего процесса взаимодействия с устройством:

– изолировать устройство от беспроводных сетей и задокументировать время и способ, которым это было сделано;

– документировать, документировать и ещё раз документировать! Каждый этап взаимодействия с устройством должен быть подробно описан, начиная с детального описания самого устройства;

– при извлечении данных создавать и сохранять контрольные суммы для каждого файла или образа. Повторное извлечение логическим способом выдаст другой результат, но ряд файлов (например, фотографии) не изменится независимо от числа попыток.

Правильно извлечённая, документированная и подписанная копия данных зачастую может быть представлена в суде в качестве цифровых доказательств.

2.7.8. Криминалистическая чистота облачного анализа

В процессе облачного анализа данные извлекаются из удалённого сервера, контролируемого сторонней компанией. Более того, за тот временной промежуток, который проходит между изъятием устройства и доступом в облако, данные могут быть неоднократно изменены, удалены или дополнены любым авторизованным пользователем. Единственный способ предотвратить такое развитие событий – выдача предписания владельцам облачного сервиса либо получение данных по запросу.

В случае с Apple данные в облаке хранятся в одном виде, а возвращаются по запросу в другом. Из облака скачиваются блоки (в случае с резервными копиями), файлы (фотографии, файлы из iCloud Drive) или отдельные записи (в остальных случаях). Для доступа к данным в процессе скачивания из облака необходимо сохранить их в формате, доступном для анализа.

Обеспечить криминалистическую чистоту полученных в результате облачного анализа данных с использованием сторонних инструментов невозможно; судебная практика в достаточном объёме не наработана. В то же время данные, полученные в процессе облачного анализа, могут оказаться ценными уликами, которые помогут в расследовании.

Рекомендуем придерживаться установленной процедуры, соблюдая правила документирования и сохраняя контрольные суммы извлечённых данных.

2.7.9. Запрос облачных данных у производителя

Компании, работающие в российском правовом поле, несут обязанность предоставлять информацию по запросам государственных структур, имея в то же время право отчитываться о таких запросах перед своими пользователями. Детализация таких отчётов, как правило, ограничивается законодательно. Тем не менее, многие компании регулярно публикуют отчёты о прозрачности (от англ. transparency report), основанные на статистических данных, связанных с запросами персональных данных или контента со стороны государственных органов. На их основе можно сделать выводы о том, какие именно данные выдавали компании в разных регионах, какое количество запросов поступило и какой процент заявок удовлетворяется.

В ряде случаев данные можно запросить у производителя ОС устройства (Apple, Google, Microsoft). На соответствующим образом оформленный запрос производитель возвращает юридически грамотно оформленные данные, криминалистическую чистоту которых гарантирует владелец облачного сервиса.

Если у вас есть возможность запросить данные у производителя – обязательно воспользуйтесь ей. Следуйте установленной процедуре, соблюдая правила документирования, при получении данных сверяйте (если есть) или создавайте (если нет) цифровые подписи предоставленных файлов.

Обратите внимание: Apple не предоставляет некоторые типы данных из облака, ссылаясь на защиту методом сквозного шифрования. Сюда входят пароли пользователя из облачной связки ключей, данные приложения «Здоровье», история браузера Safari и многие другие. Данные можно извлечь из облака при помощи Elcomsoft Phone Breaker[19], указав логин и пароль от учётной записи, пройдя двухфакторную аутентификацию и указав код блокировки одного из устройств пользователя, привязанных к той же учётной записи.

В Российской Федерации получение данных о пользователях у сервисов, где эти данные хранятся, регулируется рядом законов. Самые известные из них:

– **Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму»** и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»

– **Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»**

Аналогичные законы существуют практически во всех странах, и провайдеры облачных сервисов должны им подчиняться. Компания Apple сотрудничает с правоохранительными органами всех стран, предоставляет достаточно много данных, и

[19] https://www.elcomsoft.ru/eppb.html

регулярно публикует отчёты о количестве поступивших запросов (и сколько из них были удовлетворены).

Отчёты о прозрачности:

- https://www.apple.com/legal/transparency/

Политика конфиденциальности (применительно к запросам):

- https://www.apple.com/ru/privacy/government-information-requests/

Доступна специальная Программа поддержки правоохранительных органов[20], учебный курс, доступный сотрудникам соответствующих организаций.

Есть и подробные Правила Apple по работе с запросами правоохранительных органов[21]; в них описано, какие данные хранятся, какие могут быть переданы, и что для этого надо сделать (есть и ссылка на форму запроса).

Информация, предоставляемая Apple достаточно обширна. В приведённом выше документе указаны следующие категории данных:

- Device Registration
- Customer Service Records
- Apple Media Services
- Apple Store Transactions
- Apple Online Store Purchases
- Gift Cards
- Apple Pay
- iCloud
- Find My
- AirTag and Find My Network Accessory Program
- Extracting Data from Passcode Locked iOS Devices
- Other Available Device Information
- Requests for Apple Store CCTV Data
- Game Center
- iOS Device Activation
- Connection Logs
- My Apple ID and iForgot Logs
- FaceTime
- iMessage
- Apple TV app
- Sign in with Apple

Обратите внимание на Connection Logs: даже если владелец учётной записи не использует сервисы iCloud, его устройства постоянно связываются с серверами Apple для обеспечения полноценного функционирования системы. Apple даёт следующие пояснении по этому пункту:

Connection activity for a customer or a device to Apple services such as Apple Music, Apple TV app, Apple Podcasts, Apple Books, iCloud, My Apple ID, and Apple Discussions,

[20] https://essentials.applesurveys.com/jfe/form/SV_bBnTUv96wDVuDLT
[21] https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf

when available, may be obtained from Apple. These connection logs with IP addresses, if available, may be obtained with the appropriate legally valid request for the requestor's country.

Надо отметить, что данные возвращаются в виде, крайне неудобном для анализа; однако, многие производители криминалистического ПО давно добавили в свои продукты поддержку этого формата, как и многих других (не только того, что возвращает Apple). Единого стандарта не существует: данные слишком разнородны.

Отметим, что в Apple начали применять или расширили применение технологий «сквозного шифрования», что позволяет компании утверждать о невозможности выдачи таких данных по запросу и, соответственно, отказывать в выдаче таких данных. Для извлечения и расшифровки таких данных необходимо использовать специализированное ПО, производимое в том числе и нашей компанией (продукт Elcomsoft Phone Breaker[22]). Кроме того, включение пользователем расширенной защиты (опции Advanced Data Protection) защитит сквозным шифрованием и те данные, которые ранее к защищаемым категориям не относились – например, облачные резервные копии и фотографии. Извлечь защищённые таким образом данные в настоящий момент невозможно.

2.7.10. Криминалистическая чистота при низкоуровневом извлечении

Современные устройства iPhone оборудованы аппаратным сопроцессором безопасности, отвечающим за шифрование большей части содержимого хранилища устройства. Таким образом, любые методики низкоуровневого извлечения из iPhone (начиная с модели iPhone 5s) являются, по сути, извлечением из работающего устройства. Более того, все методы низкоуровневого анализа, кроме способа, использующего уязвимость загрузчика, являются также анализом авторизованной пользовательской сессии; о юридических последствиях мы уже рассказали в разделе, посвящённом логическому анализу.

Существует несколько принципиально различных способов низкоуровневого анализа iPhone.

С использованием джейлбрейка: эскалация привилегий с применением публично доступного джейлбрейка. Наименее «чистый» подход, при использовании которого обеспечить криминалистическую чистоту невозможно. Помимо вопросов к целостности данных, само устройство после установки джейлбрейка будет невозможно вернуть в оригинальное состояние; его нормальное функционирование будет под вопросом. Мы не рекомендуем пользоваться этим способом.

С использованием агента-экстрактора: эскалация привилегий посредством приложения-агента из состава Elcomsoft iOS Forensic Toolkit[23]. Достаточно «чистый» способ извлечения, оставляющий на устройстве минимум следов использования и оказывающий минимальное влияние на извлекаемые данные. Устройство возвращается

[22] https://www.elcomsoft.ru/eppb.html
[23] https://www.elcomsoft.ru/eift.html

в оригинальное состояние; при правильном документировании всего процесса извлечённые цифровые улики могут быть приняты судом в качестве доказательств.

С использованием эксплойта загрузчика (Elcomsoft iOS Forensic Toolkit): гарантированная криминалистическая чистота и гарантия неизменности данных; загрузка оригинальной ОС не требуется; никакие данные на устройстве не модифицируются. После применения этого способа устройство находится в оригинальном состоянии. Этот способ, использующий Elcomsoft iOS Forensic Toolkit – единственный, после использования которого можно провести повторное извлечение и получить полностью идентичный результат (при условии, что устройство не загружалось после первого извлечения, а было сразу выключено и оставалось выключенным до момента следующего извлечения).

2.7.11. Как превратить улики в доказательства

Завершая раздел о криминалистической чистоте, ещё раз напомним о важности тщательного документирования каждого шага цепочки извлечения. Подробно опишите как само устройство, так и используемые в процессе работы инструменты. **Обязательно сохраняйте журналы извлечения**, создаваемые используемым программным обеспечением.

Если используется Elcomsoft iOS Forensic Toolkit, то контрольные суммы извлекаемых данных вычисляются и сохраняются автоматически. Не забывайте включать эти контрольные суммы в отчёт об извлечении. Точное следование установленным процедурам увеличит вероятность того, что извлечённые данные будут приняты судом в качестве доказательств.

2.8. Транспортировка: изолирование устройства от беспроводных сетей

Изолировать устройство от нежелательного подключения к беспроводным сетям можно несколькими способами: поместив его в клетку Фарадея, активировав полётный режим и отключив беспроводные сети, либо выключив питание.

Общие рекомендации по транспортировке устройства:

– коротким нажатием кнопки блокировки экрана проверьте, включено ли устройство. Если устройство выключено, достаточно разместить его в клетке Фарадея. Если включено, см. ниже;

– по возможности разместите устройство в клетке Фарадея. Рекомендуем подключить внешний источник питания, расположенный внутри клетки Фарадея рядом с устройством;

– во избежание быстрой разрядки устройства активируйте полётный режим, проверьте и отключите сети Wi-Fi и Bluetooth;

– в отсутствие клетки Фарадея переведите устройство в «полётный» режим, после чего проверьте состояние переключателей беспроводных сетей Wi-Fi и Bluetooth, при необходимости отключив эти сети вручную.

Рекомендуем избегать следующих действий:

– не выключайте питание устройства. Это приведёт к необходимости разблокировать его паролем (кодом блокировки), который может быть неизвестен;

– не извлекайте SIM-карту. Это заблокирует биометрические датчики. Вы не сможете разблокировать устройство отпечатком пальца или сканом лица. Для разблокировки придётся использовать пароль (код блокировки).

2.8.1. Клетка Фарадея

Клетка Фарадея – устоявшееся название для класса устройств, предназначенных для экранирования аппаратуры от внешних электромагнитных волн. В целях транспортировки мобильных устройств часто выполняется в виде мягкого пакета, сделанного из токопроводящего материала или армированного токопроводящей сеткой. При отсутствии клетки Фарадея в её роли иногда используют обычные пакеты от картофельных чипсов с алюминиевой подложкой. Существуют разновидности клеток Фарадея как с возможностью подключения источника питания (портативного аккумулятора), так и без неё.

Допустимо использовать одноразовые клетки Фарадея, выполненные в виде металлизированных пакетов из полиэтилена.

Обратите внимание: извлечение SIM-карты в качестве меры по изолированию устройства от сотовых сетей приводит к немедленной блокировке биометрических датчиков; разблокировать такое устройство впоследствии можно будет только паролем.

2.8.2. Клетка Фарадея и полётный режим

Если устройство поместить в клетку Фарадея «как есть», со включённым радиомодулем, то телефон будет очень расходовать заряд аккумулятора в ускоренном режиме в попытках сканирования радиочастот. Это может привести к полному разряду устройства и его отключению, что нежелательно: разблокировать отключённое устройство после зарядки придётся исключительно паролем (кодом блокировки экрана).

Чтобы избежать ускоренного разряда аккумулятора рекомендуем подключить устройство к внешнему источнику питания (их рекомендуется размещать внутри клетки Фарадея, чтобы зарядный провод не послужил в качестве внешней антенны). Альтернатива – перевод устройства в полётный режим.

2.9. Хранение устройства

Пассивное хранение изъятого устройства также сопряжено с определёнными рисками, даже если оно изолировано от беспроводных сетей и подключено к внешнему источнику питания.

Основной риск связан с блокировкой биометрических датчиков устройства, после которой разблокировка устройства возможна лишь посредством пароля. При хранении устройства биометрические датчики Face ID или Touch ID будут заблокированы после:

– 48 часов с момента последней разблокировки;

– 8 часов, если код блокировки экрана не вводился 6 дней подряд;

– Если есть возможность разблокировать устройство посредством биометрических данных (приложив палец или отсканировав лицо владельца), **проделайте это до того, как датчики будут заблокированы.**

Кроме того, длительное хранение не подключённого к внешнему источнику питания устройства может привести к глубокому разряду встроенного аккумулятора, что, в свою очередь, может привести к сбросу даты и времени. Неправильные дата и время могут помешать анализу; в частности, вероятно возникновение проблем на этапе подписи агента-экстрактора (см. раздел «Агент-экстрактор»).

2.10. Удастся ли извлечь данные?

Принципиальная возможность доступа к информации зависит как от того, в каком состоянии (включено, выключено, заблокировано или нет) находится устройство, а также от того, известен ли код блокировки экрана. В последующих разделах будет рассказано о том, какие способы доступа к данным можно применить к конкретному устройству и в какой последовательности.

Для извлечения в большинстве случаев потребуется знание кода блокировки экрана. Набор доступных методов извлечение зависит как от модели устройства и установленной на нём версии iOS, так и от того, какая информация известна эксперту.

2.11. Документирование

Необходимо задокументировать максимум информации об устройстве, включая:

– точное время изъятия;

– точное местоположение во время изъятия;

– было ли устройство включено или выключено?

– был ли экран устройства включён или выключен? Что отображалось на экране в момент изъятия?

– детальное состояние устройства;

– ответственное лицо;

– максимально подробные спецификации устройства: производитель, идентификатор модели, серийный номер устройства;

– меры, предпринятые для изоляции устройства (укажите, что из следующего использовалось: клетка Фарадея, использовался ли внешний источник питания; режим «в самолёте»; отключение беспроводных сетей через пользовательский интерфейс).

3. Последующие шаги

Следующим шагом в процессе анализа устройства является извлечение данных. Доступ к данным можно получить различными способами (например, путём создания резервной копии), при этом набор и полнота полученной информации будет различаться.

3.1. Для чего нужен и почему важен код блокировки экрана

Начиная с iOS 8 код блокировки экрана используется для шифрования файлов в устройстве. Если устройство выключено, то расшифровать пользовательские данные будет невозможно. При включении устройства или после его перезагрузки система запрашивает код блокировки экрана. На его основе сопроцессор безопасности Secure Enclave вычисляет ключ, посредством которого расшифровываются ключи шифрования пользовательских файлов.

Без знания кода блокировки экрана анализ устройств в режиме BFU (Before First Unlock, до первой разблокировки) вернёт лишь ограниченный объём информации об устройстве: модель, серийный номер, аппаратный идентификатор и в редких случаях – IMEI. Для некоторых моделей устройств, подверженных эксплойту загрузчика, можно провести частичное извлечение.

В режиме повседневного использования пользователь разблокирует iPhone при помощи биометрических датчиков – сканера отпечатков пальцев или сканера лица. Несмотря на то, что биометрические данные можно использовать для разблокировки устройства, биометрическая разблокировка недоступна в режиме BFU – до первой разблокировки, которая всегда требует введения пароля. Кроме того, в ряде случаев (см.

ниже) потребуется ввести код блокировки экрана, даже если экран устройства был успешно разблокирован биометрикой.

Код блокировки экрана потребуется в следующих случаях:

– после включения или перезагрузки устройства – для его разблокировки.

– для сопряжения устройства с компьютером.

– для сброса пароля на резервную копию.

– для доступа к данным в iCloud, зашифрованным сквозным шифрованием.

– для сброса пароля к учётной записи Apple ID/iCloud.

– для низкоуровневого извлечения любым из способов.

– если система заблокировала биометрические датчики по тайм-ауту или в результате действий пользователя или эксперта.

Обход кода блокировки экрана практически бесполезен: к.од блокировки используется в качестве элемента ключа шифрования большей части пользовательских данных; его обход не даст возможности расшифровать эти файлы. Ту часть пользовательских данных, которая не зашифрована таким ключом, можно извлечь в режиме BFU через эксплойт загрузчика (для подверженных эксплойту устройств).

3.2. Взлом пароля (кода блокировки экрана)

Для ряда моделей iPhone доступны решения от сторонних производителей, целью которых является восстановление (взлом) кода блокировки экрана и/или извлечение из устройства данных. В частности, такие решения предоставляют компании Cellebrite и GrayShift.

В Elcomsoft iOS Forensic Toolkit доступен перебор для ограниченного набора моделей, в число которых входят устройства iPhone 4, 4s (требуется дополнительный аппаратный микроконтроллер), iPhone 5 и 5c, а также ряд моделей iPad, использующих аналогичные версии процессоров.

3.3. Методы извлечения и порядок их использования

В наших продуктах поддерживаются следующие варианты извлечения данных:

– анализ в ручном режиме: просмотр информации на экране устройства, документирование снимками экрана либо отправка нужных данных на другое устройство посредством AirDrop;

– логический анализ: резервные копии в формате iTunes, медиафайлы, данные приложений, некоторые системные журналы;

– облачное извлечение: резервные копии iCloud, синхронизированные данные, файлы iCloud Drive и данные, зашифрованные сквозным шифрованием;

– низкоуровневый анализ: использование агента-экстрактора или эксплойта загрузчика;

– для старых моделей (iPhone 4, 4s, 5, 5c): взлом кода блокировки экрана и полноценное физическое извлечение.

3.4. Зависимость методов извлечения от аппаратной платформы и версии iOS

Аппаратная платформа является одним из решающих факторов, влияющих на доступные способы извлечения данных. Поколение SoC не менее важно, чем установленная на устройство версия iOS/watchOS/iPadOS. Рассмотрим доступные для каждой комбинации платформ/версий ОС возможности извлечения данных. Актуальная матрица совместимости выглядит следующим образом:

Таблица 1: Матрица совместимости

	iPhone	iPod	iPad				TV	Agent	checkm8
		Touch		*Mini*	*Air*	*Pro*			
A4	iPhone 4	4	1				2		
A5/A5X	iPhone 4s	5	2, 3	1			3		+
A6/A6X	iPhone 5/5c		4						+
A7	iPhone 5s			2, 3	1			12.0-12.5.7	+
A8/A8X	iPhone 6	6		4	2		4 (HD)	12.0-12.5.7	+
A9/A9X	iPhone 6s, SE		5			1		12.0-14.3	+
A10/A10X	iPhone 7	7	6, 7			2	4K	12.0-14.3	+
A11	iPhone 8/X							12.0-16.6.1	*
A12/A12X/A12Z	iPhone Xr/Xs		8	5	3	3, 4	4K 2nd	12.0-16.6.1	
A13	iPhone 11, SE2		9					13.0-16.6.1	
A14	iPhone 12		10		4			14.0-16.6.1	
A15	iPhone 13, SE3, 14			6			4K 3rd	15.0-16.6.1	
A16	iPhone 14 Pro							16.0-16.6.1	
M1					5	5		14.6-16.6.1	
M2						6		16.1-16.6.1	

* Для iOS 14 до iOS 16 совместимость checkm8 с A11 ограничена

Внимание: версии iOS младше, чем 12.0, в актуальных сборках агента-экстрактора в iOS Forensic Toolkit не поддерживаются. Если вам необходимо установить агент-экстрактор на устройство под управлением более старой версии iOS, воспользуйтесь iOS Forensic Toolkit 8.23 или 7.81, в которых поддерживаются сборки iOS начиная с версии 9.0.

Внимание: для извлечения посредством checkm8 для устройств на основе Apple A11 (iPhone 8, 8 Plus, iPhone X) на iOS 14 и 15 необходимо, чтобы код блокировки на устройстве не был установлен.

Внимание: для работы checkm8 на моделях iPhone 8, 8 Plus, iPhone X, работающих под управлением iOS 16.x, необходимо, чтобы код блокировки на этих устройствах не был установлен ни разу после начальной настройки устройства. Просто удалить код блокировки экрана недостаточно; если код блокировки был установлен, то извлечь данные из устройства не удастся.

Значения цветов

Зелёный: доступны все возможности, включая взлом кода блокировки.

Синий: устройства, уязвимые для эксплойта загрузчика. Это означает, что вы сможете использовать как ограниченное извлечение для устройств с неизвестным кодом блокировки экрана, так и полноценное для устройств с известным или пустым кодом блокировки.

Красный: извлечение из заблокированных с неизвестным кодом блокировки экрана устройств недоступно. Для разблокированных устройств связка ключей и образ файловой системы могут быть извлечены для перечисленных версий iOS.

Серый: на данный момент доступны только логические методы и облачный анализ через iCloud.

Извлечение на основе эксплойта загрузчика поддерживается для устройств iPhone модельного ряда от iPhone 5s до iPhone X включительно. Обратите внимание на следующие особенности и ограничения:

– iPhone 4s. Несмотря на возраст этого устройства, работать с ним довольно сложно; надёжная реализация эксплойта требует использования дополнительного аппаратного обеспечения – программируемой платы-микроконтроллера. Наше решение также использует плату-микроконтроллер с разработанной нами специальной прошивкой для установки эксплойта;

– iPad (все модели). Обратите внимание на литеру «X» в названиях SoC! Такие процессоры, как A12X и A12Z, имеют минимальные отличия от A12, но требуют альтернативной реализации checkm8;

– Apple TV. Модель третьего поколения основана на SoC от iPhone 4s (см. выше); с новыми моделями 4 и 4K есть свои сложности. Модели 2021 года и более новые не поддерживаются.

Также доступна поддержка часов Apple Watch Series 3. Они не указаны в таблице, однако модель S3 совместима с эксплойтом checkm8, и из часов можно извлечь связку ключей и файловую систему независимо от версии watchOS.

3.5. Методы, которые не работают

В мобильной криминалистике традиционно использовался ряд методов извлечения данных, которые не будут работать для мобильных устройств Apple из-за шифрования пользовательских данных. Проблема, соответственно, лежит не только и не столько в плоскости снятия информации, сколько в её последующей расшифровке. Таким образом, в число неработоспособных методов входят:

– анализ JTAG: недоступен обычными методами на стандартных устройствах, доступных конечному потребителю;

– выпаивание микросхем памяти: данные зашифрованы, анализ микросхем памяти бесполезен.

4. Методы извлечения данных

Доступные методы извлечения данных могут зависеть от множества факторов, не все из которых очевидны. Пропустим механический анализ устройства с просмотром информации на экране устройства и **перейдём к техническим методам извлечения данных.**

4.1. Осмотр вручную

В ряде случаев осмотр вручную может стать единственным доступным методом анализа. В рамках этого метода предпринимается ручной, механический просмотр содержимого устройства с фото-видео фиксацией и созданием скриншотов. Такой способ доступа к данным считается самым инвазивным из возможных; при его проведении нужно тщательно соблюдать все предосторожности по работе с устройством и вести тщательное документирование каждого шага процесса.

4.1.1. Как это работает?

– доступ к отдельным файлам и их передача через AirDrop или облачные сервисы;

– создание скриншотов, фото- и видеофиксация данных, отображаемых на экране устройства.

4.1.2. Достоинства метода

– быстро и просто;

– можно проделать с любыми устройствами (если они разблокированы).

4.1.3. Недостатки ручного анализа

– не является криминалистически чистым (а часто - даже допустимым);

– множество изменений в данных;

– достоверность полученных таким образом цифровых улик сомнительна, а возможность их представления в качестве цифровых доказательств требует тщательной фиксации и подробного документирования каждого шага;

– доступен лишь ограниченный объем данных. Чувствительные данные (например, пароли) по-прежнему будут защищены функцией "защиты украденного устройства", и получить к ним доступ, скорее всего не удастся (в некоторых случаях это возможно, если осмотр происходит в одном из "знакомых мест"; см. ниже).

Ручной осмотр лучше использовать лишь в крайних случаях, когда того требует обстановка, а другие подходы недоступны. Однако следует учитывать его ограничения, особенно если требуется юридическая чистота процесса.

4.2. Расширенное логическое извлечение

Расширенное логическое извлечение доступно для всех устройств Apple в работоспособном состоянии, которые могут быть сопряжены или подключены к компьютеру. Если известен код блокировки экрана устройства, то извлечение может быть достаточно несложным; в иных случаях возможность проведения логического извлечения будет зависеть от возможности сопряжения устройства с компьютером и установленного на резервную копию пароля.

Логический анализ — самый известный способ получить доступ к основному массиву данных. Метод логического анализа работает для всех устройств под управлением iOS и её производных iPadOS, WatchOS и tvOS. Всё, что нужно для работы

— это само устройство, кабель Lightning (для часов Apple Watch — адаптер iBUS, для Apple TV 4K – также специальный адаптер) и в большинстве случаев — код блокировки экрана для того, чтобы установить сопряжение устройства с компьютером.

4.2.1. Ограничения метода

Одна из сильных сторон логического анализа — возможность доступа к данным даже тогда, когда экран устройства заблокирован (с рядом оговорок). В то же время логическое извлечение имеет следующие ограничения:

- работа только в режиме AFU (After First Unlock);
- требуется код блокировки экрана, если необходимо сопрячь устройство с компьютером;
- на резервную копию может быть установлен пароль (варианты решения: сброс через настройки устройства; восстановление методом перебора);
- количество извлекаемых данных ограничено;
- связку ключей можно извлечь только из резервных копий с паролем (вариант решения: установка временного пароля на резервную копию в процессе извлечения).

4.2.2. Достоинства метода

- прост в использовании;
- совершенно безопасен, если используется специализированное программное обеспечение;
- совместим со всеми версиями iOS;
- может работать с заблокированными устройствами (если есть доступ к ранее сопряжённому компьютеру);
- может извлекать журналы устройства и данные приложений;
- медиафайлы (с EXIF) доступны, даже если установлен пароль на резервную копию.

4.3. Облачное извлечение

Метод извлечения через iCloud не требует наличия самого устройства. В то же время для доступа к данным потребуются учётные данные пользователя (логин и пароль от Apple ID, доступ ко второму фактору аутентификации). Для расшифровки некоторых типов данных дополнительно потребуется код блокировки экрана доверенного устройства.

Посредством облачного извлечения можно получить доступ к резервным копиям всех привязанных к учётной записи устройств, синхронизированным данным, файлам iCloud Drive, а также к некоторым типам данных, защищённых сквозным шифрованием.

Важность синхронизированных данных трудно переоценить: они хранятся и извлекаются отдельно от резервных копий, а синхронизируется максимум данных: от контактов до фотографий и сообщений.

В контейнере iCloud Drive доступны множество файлов и документов, часто включая папки Documents и Desktop с компьютеров Mac.

В контейнере, защищённом сквозным шифрованием, доступны такие данные, как связка ключей с паролями, которая может содержать и маркеры аутентификации;

данные приложения «Здоровье», сообщения SMS и iMessage, пароль Экранного времени, история браузера Safari и другие данные.

Все эти данные собираются не только с исследуемого iPhone, но и со всех остальных устройств пользователя, подключённых к данной учётной записи.

4.3.1. Ограничения метода

– требуются учётные данные для входа в iCloud (включая второй фактор аутентификации);

– код блокировки или пароль одного из доверенных устройств: требуются для доступа к данным, защищённых сквозным шифрованием;

– устройства могут не использовать iCloud, поэтому иногда данные отсутствуют.

4.3.2. Достоинства метода

– совместим со всеми версиями iOS;
– само устройство не требуется;
– извлекаются даже те данные, которые не возвращает Apple по запросу;
– доступны данные всех устройств, подключённых к учётной записи;
– извлекается облачная Связка ключей;
– файлы в iCloud Drive;
– данные доступны в реальном времени;
– могут быть доступны старые резервные копии.

4.4. Низкоуровневое извлечение

В резервной копии, даже защищённой паролем, содержится намного меньше информации, чем хранится в устройстве. В устройстве содержатся базы данных с детальной историей местоположений, данные всех приложений, включая историю переписки в безопасных мессенджерах; WAL-файлы SQLite, в которых могут содержаться удалённые записи, временные файлы, данные WebKit, транзакции ApplePay, уведомления приложений и многое другое, что может стать важными уликами.

Доступ к файловой системе достаточно сложен, и начинается с вопроса о выборе метода, который будет для этого использоваться. Для разных моделей iPhone могут быть доступны извлечение через эксплойт загрузчика и/или доступ посредством программы-агента. Для того, чтобы понять, с какими именно версиями iOS и моделями iPhone совместим каждый из способов, нужно ознакомиться с матрицей совместимости (**Error! Reference source not found.**).

Общие для всех методов низкоуровневого доступа преимущества включают:

– извлекается максимально полный набор данных;

– пароль на резервные копии игнорируется; при желании извлекается из связки ключей;

– извлекается полная связка ключей.

Помимо описанных ниже способов, доступ к файловой системе может быть осуществлён посредством джейлбрейка. Установка джейлбрейка не является криминалистически чистым методом анализа, оставляя следы работы на устройстве, большая часть которых не документирована. Мы не рекомендуем пользоваться джейлбрейками за исключением случаев, когда использование агента-экстрактора по какой-либо причине невозможно.

4.4.1. Агент-экстрактор

Использование агента-экстрактора – самый простой и достаточно чистый с точки зрения криминалистики способ низкоуровневого извлечения. При использовании агента-экстрактора на устройство будет установлено приложение, которое самостоятельно получит необходимые для работы привилегии и установит соединение с компьютером.

Для получения привилегий для низкоуровневого доступа к файловой системе требуется эксплуатация уязвимости в iOS, которую агент-экстрактор производит строго в оперативной памяти устройства, не модифицируя данных в хранилище. Ограничение этого способа – требования к совместимости: поддерживаются только те версии iOS, для которых мы подобрали соответствующий эксплойт. Список поддерживаемых агентом версий iOS – в таблице **Error! Reference source not found.**.

4.4.2. Эксплойт загрузчика

Использование эксплойта загрузчика (для большинства совместимых устройств это checkm8, но для устаревших устройств могут использоваться другие подобные эксплойты) в целях мобильной криминалистики позволяет извлечь образ файловой системы и расшифровать связку ключей из совместимых модификаций iPhone, подверженных эксплойту checkm8, и соответствующих моделей iPad, Apple TV, Apple Watch и iPod Touch. Полный список поддерживаемых устройств - в таблице **Error! Reference source not found.**.

В отличие от аналогичных решений, наш продукт не использует заимствований из джейлбрейка checkra1n и не включает проприетарного кода Apple. В процессе работы эксперту необходимо будет скачать образ прошивки iPhone с сайта Apple (ссылка на скачивание выдаётся в процессе анализа устройства). iOS Forensic Toolkit использует скачанный образ прошивки для того, чтобы загрузить устройство, минуя установленную на смартфоне операционную систему и избежав таким образом любых модификаций в разделе данных или системном разделе iPhone.

Наша реализация метода обладает следующими преимуществами в сравнении с аналогами:

- гарантированная целостность и неизменность всех разделов устройства;
- любые модификации происходят только в оперативной памяти устройства;
- поддержка большинства совместимых версий iOS за единичными исключениями.

4.5. Сравнение доступных данных

Используя и комбинируя различные методы извлечения, эксперт сможет получить максимально возможный объём информации как из самого устройства, так и из облачных сервисов.

Таблица 2: Данные, доступные посредством различных методов извлечения

	Резервные копии (iTunes)	Резервные копии (iCloud)	Синхронизация iCloud	Образ файловой системы
Данные приложений	ограниченно	ограниченно	ограниченно	+
Apple Pay	—	—	—	+
Книги	—	+	+	+
Календари	+	+	только iCloud	+
Звонки	+	+	-	+
Контакты	+	+	только iCloud	+
Настройки устройства	+	+	—	+
Здоровье	только зашифрованные	—	Сквозное шифрование	+
Связка ключей	только зашифрованные	—	Сквозное шифрование	+
Почта	—	—	только iCloud	+
Карты	только зашифрованные	—	+	+
Медиа	+	только если не синхронизируется	+	+
Сообщения	+	только если не синхронизируется	Сквозное шифрование	+
Заметки	+	+	только iCloud	+
Уведомления	ограниченно	+	—	+
Экранное время	—	—	ограниченно	+
Диктофон	+	iOS<12	iOS 12+	+
Wallet	+	+	+	+
Web — закладки	+	+	Сквозное шифрование	+
Web — история	только зашифрованные	+	Сквозное шифрование	+

Web — поиск	только зашифрованные	+	Сквозное шифрование	+

5. Извлечение данных: логическое извлечение

Логический анализ или метод логического извлечения – самый распространённый способ извлечения данных, который доступен на всех поколениях iPhone, iPad и iPod Touch. Под логическим анализом часто подразумевается создание локальной резервной копии в формате iTunes, однако метод не ограничен только резервными копиями.

5.1. Что входит в состав расширенного логического извлечения

Логический анализ предоставляет доступ к следующим типам данных:

- расширенная информация об устройстве;
- резервная копия в формате iTunes (может оказаться зашифрованной паролем);
- медиафайлы (фото и видео) и некоторые базы данных, которые могут содержать записи об удалённых файлах;
- диагностические и crash-логи;
- данные некоторых приложений.

5.2. Сопряжение устройства с компьютером

В документации Apple[24] описан механизм сопряжения (привязки или, в терминах компании, «установки доверия») между iPhone, iPad или iPod Touch и компьютером. При первом подключении устройства к компьютеру отображается предупреждение с запросом, следует ли доверять данному компьютеру; в современных версиях iOS запрос требуется подтвердить кодом блокировки экрана.

Доверенные компьютеры могут синхронизироваться с устройством iOS, создавать резервные копии и получать доступ к фотографиям, видеороликам, контактам и другому контенту на устройстве. Эти компьютеры остаются доверенными, пока пользователь не изменит список доверенных компьютеров или не сотрёт данные с устройства iOS. Кроме того, переустановить привязку может потребоваться, если между подключениями проходит достаточное время.

Компьютер, удалённый из списка доверенных, теряет доступ к содержимому устройства.

5.2.1. Действия по сопряжению устройства с компьютером

Перед тем, как устройство сможет обмениваться информацией с компьютером, необходимо установить сопряжение между устройством и компьютером. В процессе сопряжения будет создана пара ключей, один из которых будет сохранён на устройстве, а второй – сохранён на компьютере в виде файла lockdown. Обмениваться данными устройство будет только с сопряжённым компьютером.

[24] https://support.apple.com/ru-ru/HT202778

Чтобы сопрячь устройство с компьютером, подключите его к компьютеру кабелем Lightning и подтвердите запрос «Trust this computer?» («Доверять этому компьютеру?») на устройстве. В момент подключения устройство должно быть включено и разблокировано (в противном случае порт USB может быть в защитном режиме). Далее необходимо подтвердить запрос вводом кода блокировки экрана на устройстве.

5.3. Депонированные ключи (файлы lockdown)

В процессе сопряжения на компьютере пользователя создаётся запись - файл, в котором содержится депонированный ключ (lockdown-файл или pairing record). В устройстве сохраняется вторая часть пары ключей; при её удалении (в результате сброса телефона к фабричным настройкам или из меню настроек) депонированный на компьютере ключ станет бесполезным.

Благодаря депонированным ключам пользователю не нужно каждый раз разблокировать телефон при подключении его к компьютеру для синхронизации или создания резервной копии. Теоретически депонированные ключи можно использовать с целью логического анализа, извлекая из устройства с заблокированным экраном резервную копию, медиа-файлы и прочие доступные данные. С практической точки зрения такое использование возможно в исключительно редких случаях и в основном с устройствами, работающими под управлением старых версий iOS.

5.3.1. Ограничения депонированных ключей

В настоящий момент депонированные ключи малопригодны для целей криминалистического анализа. Это связано с двумя факторами:

- Блокировка передачи данных защитным режимом USB (начиная с iOS 12.4.1).
- Депонированные ключи не могут быть использованы до первой разблокировки устройства.

Подробно о защитном режиме USB можно прочесть в разделе «Защита украденного устройства»

В обсуждении кода блокировки экрана и биометрического способа аутентификации нельзя не рассказать об относительно новом (появился в iOS 17.3) способе дополнительной защиты, комбинирующем оба способа.

До выхода iOS 17.3 (а точнее, iOS 17.3 Developer Preview, в которой впервые появился прототип рассматриваемой функции) для подключения iPhone к компьютеру и подтверждения доверия к устройству требовался только код блокировки экрана. Теперь же у пользователя появилась возможность включить дополнительный уровень защиты. После его активации как для сопряжения с компьютером, так и для совершения целого ряда других действий, затрагивающих чувствительную информацию, кода блокировки уже недостаточно; теперь для сопряжения с новым компьютером нужен и код блокировки экрана, и дополнительная аутентификация с помощью Face ID или Touch ID.

Обратите внимание: в официальном описании функции «Защита украденного устройства» на сайте Apple требование биометрической аутентификации для сопряжения iPhone с компьютером не упоминается; тем не менее, защита срабатывает.

«Защита украденного устройства» значительно затрудняет логическое извлечение данных. Если до появления этой функции для привязки было достаточно разблокировать устройство и ввести код блокировки экрана, то теперь необходимо подтвердить личность владельца биометрией. В случае, если владелец устройства отсутствует или биометрические данные предоставить невозможно, логический анализ смартфона становится практически невозможным.

При включении этой функции, вероятно, единственным оставшимся методом анализа будет ручной, механический просмотр содержимого устройства с фото-видео фиксацией и созданием скриншотов. Такой способ доступа к данным считается самым инвазивным из возможных; при его проведении нужно тщательно соблюдать все предосторожности по работе с устройством и вести тщательное документирование каждого шага процесса.

5.3.2. Отключение защиты

Можно попробовать отключить функцию защиты украденного устройства, однако здесь присутствует сразу ряд моментов, усложняющих процесс.

Во-первых, для отключения «защиты украденного устройства» вам всё равно понадобится биометрическая аутентификация. Во-вторых, если пользователь не изменял настройки по умолчанию, при попытке отключить защиту система установит дополнительную задержку в течение часа, если устройство не находится в «знакомом месте». Это означает, что для отключения защиты потребуется два подтверждения с помощью Face ID или Touch ID: первое - при начале процесса изменения настроек, второе - после завершения тайм-аута.

5.3.3. «Знакомые места» и их значение

В рамках функций «Защиты украденного устройства» Apple предоставляет пользователю выбор: ряд функций безопасности (в частности - часовая задержка при отключении дополнительной защиты) может срабатывать каждый раз или только тогда, когда попытка делается вдали от «знакомых мест» (настройка называется "Away from Familiar Locations"). По умолчанию, если пользователь не изменит настройку вручную, многие дополнительные меры безопасности функции «Защита украденного устройства» применяются только тогда, когда iPhone находится вдали от знакомых мест.

Практическое следствие: отключать защиту либо проводить ручной осмотр имеет смысл по возможности в одном из «знакомых мест», каковыми являются, как правило, такие места, где пользователь проводит больше всего времени (дом, работа). Деталей работы этой функции Apple не раскрывает.

5.3.4. Дополнительная защита и резервные копии

В документации Apple указано: «При восстановлении из резервной копии iCloud или переносе непосредственно с предыдущего iPhone на новый также восстанавливаются настройки вашего устройства, включая функцию «Защита украденного устройства». После небольшой задержки, чтобы синхронизировать привычные места из iCloud, на новом устройстве автоматически возобновляются меры безопасности для защиты украденного устройства.»

Кроме того, отметим, что перенести данные на новое устройство с включённой дополнительной защитой также не удастся: в документации упомянуто «Использование iPhone для настройки нового устройства (например, с помощью функции «Быстрое начало»)».

Таким образом, отметим, что, несмотря на свою пользу для рядовых владельцев iPhone, функция защиты украденного устройства создаёт значительные препятствия для экспертов по цифровой криминалистике, осложняя легальное извлечение данных из смартфонов, изъятых у преступников.

Режимы S.O.S. и защитный режим USB.

5.3.5. Пути к депонированным ключам

Расположение депонированных ключей зависит от версии операционной системы на компьютере пользователя. Ниже приводятся точные пути к депонированным ключам:

Windows Vista, 7, 8, 8.1, Windows 10:

```
%ProgramData%\Apple\Lockdown
```

Windows XP:

```
%AllUsersProfile%\Application Data\Apple\Lockdown
```

macOS:

```
/var/db/lockdown
```

В файловой системе iOS (папка доступна только в процессе низкоуровневого анализа):

```
/private/var/root/Library/Lockdown
```

В macOS Sierra папка с депонированными ключами доступна только с правами суперпользователя (для их извлечения потребуется ввести пароль). Права доступа можно получить следующей командой, выполненной в окне терминала:

```
sudo chmod 755 /private/var/db/lockdown
```

Это ограничение легко обходится при анализе образа диска. В более новых версиях macOS защита была усилена:

Теперь для доступа к депонированным ключам потребуется проделать дополнительные манипуляции, связанные с необходимостью отключения SIP (System Integrity Protection). Для этого нужно загрузить компьютер с macOS в режим Recovery (⌘+R во время загрузки системы), после чего выполнить в терминале следующую команду:

```
csrutil disable
```

Далее компьютер нужно перезагрузить, после чего выполнить указанную ранее команду для выдачи прав доступа. Ещё раз напомним, что всего этого можно избежать, если анализируется образ диска.

В указанных выше папках содержатся файлы, названия которых соответствуют идентификатору устройства в формате UUID. Файлы имеют расширение .plist. Если UUID телефона неизвестен, определить его можно с помощью команды “I” в приложении Elcomsoft iOS forensic Toolkit. UUID будет сохранён в XML файле в следующем виде:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<...>
<key>UniqueDeviceID</key>
<string>0a226c3b263e004a76e6199c43c4072ca7c64a59</string>
</dict>
</plist>
```

Рекомендуем заранее скопировать депонированные ключи в рабочий каталог; для простоты ввода можно использовать более короткие имена файлов. В macOS необходимости в этом не возникает: файл можно перетащить в окно терминала мышкой, после чего система автоматически подставит в командной строке полный путь к файлу.

5.3.6. Использование депонированных ключей в Elcomsoft iOS Forensic Toolkit

С помощью депонированного ключа, который был скопирован с доверенного компьютера, появится возможность установить сопряжение (доверенные отношения) с

компьютером в лаборатории. С помощью Elcomsoft iOS Forensic Toolkit можно использовать файл с депонированным ключом для того, чтобы создать резервную копию данных подключённого iPhone и дополнительно извлечь такие данные, как фотографии, системные журналы и файлы приложений.

Использовать депонированные ключи для разблокировки экрана невозможно; ключи используются исключительно для синхронизации данных и создания резервных копий устройства.

В Elcomsoft iOS Forensic Toolkit 8 депонированный ключ указывается в качестве параметра командной строки. Для установления доверенных отношений с устройством с использованием депонированного ключа воспользуйтесь следующей инструкцией.

1. Подключите к компьютеру iPhone.
2. Используйте депонированный ключ (lockdown file) для установления доверенных отношений между устройством и компьютером. Для этого необходимо добавлять параметр -r record.plist ко всем командам, выполняемым в процессе логического извлечения, где “record.plist” – путь к файлу с депонированным ключом. Обратите внимание на совпадение идентификаторов UDID устройства и соответствующего ключа.
3. В случае, если разблокировать устройство с помощью указанного депонированного ключа не удалось, попробуйте использовать другие депонированные ключи (например, извлечённые из других компьютеров).

ВНИМАНИЕ: при использовании депонированного ключа необходимо добавлять параметр *-r record.plist* ко всем командам, выполняемым в процессе логического извлечения.

5.4. Локальные резервные копии

Локальные резервные копии в формате iTunes содержат максимальный набор данных, который можно получить из устройства в пределах логического извлечения. Ознакомительная информация о системе резервного копирования опубликована на сайте Apple: Сведения о резервных копиях устройств[25]. Несмотря на то, что в резервную копию входит большое количество данных, часть информации в них не попадает. Согласно Apple:

В резервные копии iTunes не включаются следующие компоненты:

– содержимое из магазинов iTunes Store и App Store или файлы PDF, загруженные непосредственно в программу Apple Books;

– содержимое, синхронизированное с iTunes (например, импортированные файлы в формате MP3 или компакт-диски, видеоролики, книги и фотографии);

– данные, которые уже хранятся в iCloud, например «Фото iCloud», сообщения iMessage, текстовые (SMS) и мультимедийные (MMS) сообщения;

– настройки Face ID и Touch ID;

– информация и настройки Apple Pay;

– данные почты Apple;

[25] https://support.apple.com/ru-ru/HT204136

– данные из программ «Активность», «Здоровье» и «Связка ключей» (для создания резервной копии этих данных необходимо использовать функцию *шифрования резервных копий*[26] в iTunes).

Существуют и другие недокументированные отличия в плане контента между зашифрованными и нешифрованными резервными копиями.

В базе знаний Apple доступны следующие статьи по резервному копированию iOS:

- Восстановление данных устройства iPhone, iPad или iPod touch из резервной копии[27]
- Поиск резервных копий данных устройств iPhone, iPad и iPod touch[28]
- Резервное копирование данных на устройствах iPhone, iPad и iPod touch[29]

5.4.1. Как создаются резервные копии iOS

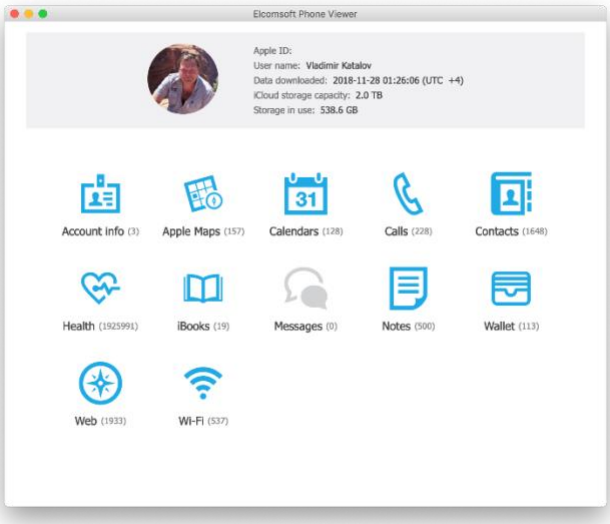
С компьютера, к которому подключается iPhone, нельзя получить доступ к файловой системе устройства: с компьютера будут доступны только медиафайлы и файлы некоторых приложений. Такой вариант позволяет усилить целостность и безопасность данных на устройствах Apple. Отметим, что при копировании по протоколу AFC (используется в iOS Forensic Toolkit в процессе извлечения медиа-данных) помимо фото и видео извлекаются метаданные, в которых могут содержаться ценные улики, которые невозможно получить стандартными средствами доступа.

За создание резервной копии отвечает сервис, работающий на самом устройстве iPhone или iPad. Работающее на компьютере приложение (им может быть как iTunes, так и iOS Forensic Toolkit или один из альтернативных продуктов) получает уже сформированный поток данных, который остаётся лишь сохранить на компьютере в виде файлов.

Необычность резервных копий в формате iTunes в том, что в ней нет привычных имён файлов и папок. Вместо этого используются хэши имён (включая путь к файлу или папке), индекс и дополнительные метаданные.

Apple не предоставляет пользователям и разработчикам инструментов для работы с резервными копиями iOS. Единственный официально поддерживаемый сценарий — восстановление резервной копии на новое или сброшенное устройство Apple. В то же время формат резервных копий хорошо изучен, и на рынке присутствует ряд продуктов для просмотра и анализа резервных копий iOS, включая Elcomsoft Phone Viewer[30] .

[26] https://support.apple.com/ru-ru/HT205220
[27] https://support.apple.com/ru-ru/HT204184
[28] https://support.apple.com/ru-ru/HT204215
[29] https://support.apple.com/ru-ru/HT203977
[30] https://www.elcomsoft.ru/epv.html



5.4.2. Пароли к резервным копиям

Резервные копии iTunes могут быть защищены паролем; подробности в статье Зашифрованные резервные копии в программе iTunes[31]. Пароли к резервным копиям iOS чрезвычайно стойкие; их перебор очень медленный, порядка единиц или десятков паролей в секунду даже с использованием графических ускорителей. В то же время резервные копии с паролем содержат значительно больше доступных данных в сравнении с незашифрованными резервными копиями (в частности — связка ключей, в которой хранятся все пароли пользователя).

Пароль на резервную копию — свойство того устройства (iPhone или iPad), из которого она извлечена. После того, как пароль был единожды установлен, он сохраняется на устройстве и используется для шифрования всех вновь созданных резервных копий независимо от того, с какого компьютера и каким приложением они будут создаваться.

В iOS 11 появилась возможность сбросить пароль к резервной копии через настройки устройства. У этого действия есть ряд негативных последствий (см. раздел «Сброс пароля к резервной копии: что для этого нужно, как проделать, последствия»).

5.4.3. С паролем или без?

Необычный аспект защиты резервных копий iOS — шифрование связки ключей, в которой доступны сохранённые пользователем пароли. Связка ключей шифруется по-разному в зависимости от того, установлен ли пароль на резервную копию. По информации от Apple:

Функция шифрования резервной копии в iTunes блокирует и шифрует данные. Зашифрованные резервные копии, созданные с помощью iTunes, могут включать в себя элементы, которые отсутствуют в незашифрованных резервных копиях iTunes:

- сохранённые пароли;
- настройки Wi-Fi;

[31] https://support.apple.com/ru-ru/HT205220

– история посещения веб-сайтов;
– медицинские данные.

Первый пункт наиболее важен. Однако нужно отметить, что утверждение Apple о том, что в резервные копии без защиты не попадают сохранённые пароли, технически некорректно. Содержимое связки ключей попадает как в резервные копии с паролем, так и без него. Разница в том, что если пароль на резервную копию установлен, то и содержимое связки ключей будет зашифровано тем же паролем. Если же пароля на резервную копию нет, то связка ключей будет зашифрована аппаратным ключом, уникальным для каждого устройства, в результате чего восстановить пароли из резервной копии можно будет только на то физическое устройство, с которого была сделана резервная копия. Расшифровать или перенести на новое устройство связку ключей не удастся.

– **практический вывод:** для максимально полного извлечения задайте временный пароль на резервную копию, если он не установлен. Многие криминалистические пакеты делают это автоматически, в том числе iOS Forensic Toolkit: если пароль на резервную копию пустой, то перед извлечением резервной копии будет установлен временный пароль ‘123’, а после её извлечения – сброшен.

– **обратите внимание,** что для установки и сброса пароля потребуется ввести код блокировки на экране устройства. Поскольку время, в течение которого на устройстве отображается запрос на ввод кода блокировки, ограничено, этот запрос легко пропустить. Если это происходит, на резервные копии на устройстве остаётся установленным пароль. При использовании iOS Forensic Toolkit рекомендуем проверить, не забыли ли вы удалить пароль на резервную копию после извлечения данных.

– **если из устройства была попытка извлечения данных сторонним криминалистическим пакетом,** на резервную копию может быть установлен неизвестный пароль. Если вы получили такое устройство, рекомендуем опробовать пароли из следующего списка:

- Elcomsoft iOS Forensic Toolkit: **123**
- Cellebrite UFED: **1234**
- MSAB XRY: **1234**
- Belkasoft Evidence Center: **12345**
- Oxygen Forensic Detective: **oxygen** or **123456**
- Magnet AXIOM: **mag123**
- MOBILedit Forensic: **123**

5.4.4. Что делать, если пароль к резервной копии неизвестен

В некоторых случаях пароль на резервную копию допустимо игнорировать. Даже если пароль неизвестен, но устройство удалось подключить к сопряжённому компьютеру, то будет доступен архив фотографий и видеороликов, системные журналы и некоторые данные приложений.

Для доступа к фотографиям используется независимый протокол, не связанный с протоколом создания резервных копий и паролем от них. Соответственно, фото и видео

можно извлечь независимо от того, установлен пароль на резервную копию или нет. В доступных метаданных хранятся в том числе и данные о локации, в которой был сделан снимок (если сервисы геолокации были активны в момент съёмки).

Кроме того, для некоторых моделей iPhone и версий iOS доступны методы низкоуровневого доступа, позволяющие извлечь значительно больше данных, чем попадает в резервные копии. В этом случае сбрасывать пароль резервного копирования не потребуется, т. к. данные извлекаются непосредственно из файловой системы устройства, а не в формате резервной копии.

Наконец, **исходный пароль от резервной копии можно извлечь из самого устройства (из связки ключей) в дополнение к образу файловой системы.** Трудно сказать, есть ли в этом какая-то дополнительная ценность по сравнению с извлечением собственно файловой системы, в которой в любом случае содержится значительно больше данных. Иногда такой пароль можно попробовать использовать для расшифровки более старой резервной копии, которая может содержать впоследствии удалённые данные.

5.4.5. Сброс пароля к резервной копии: что для этого нужно, как проделать, последствия

С выходом iOS 11 появилась возможность сброса пароля резервного копирования непосредственно с устройства iPhone; код блокировки экрана должен быть известен. Эта опция по-прежнему доступна в последних версиях iOS, и, вероятно, останется в будущем. Последовательность действий:

1. На устройстве перейдите в меню «Настройки» > «Основные» > «Сбросить».
2. Нажмите «Сбросить все настройки» и введите код блокировки устройства.
3. Следуйте инструкциям по сбросу настроек. Это не затронет данные или пароли пользователей, но приведёт к сбросу таких настроек, как уровень яркости дисплея, позиции программ на экране «Домой» и обои. Пароль для шифрования резервных копий также будет удалён.

Обратите внимание: после сброса настроек отключается режим «В полёте», что позволит устройству подключиться к сети интернет с соответствующими рисками и последствиями. Рекомендуем проводить сброс, предварительно поместив устройство в клетку Фарадея.

Внимание: на устройстве с iOS 10 или более ранней версии сброс пароля невозможен.

Сброс пароля к резервной копии по описанному выше сценарию приводит также к удалению кода блокировки экрана устройства, что приведёт к уничтожению части данных:

- транзакции Apple Pay;
- скачанные сообщения Exchange;
- некоторые другие данные, защищённые кодом блокировки экрана.

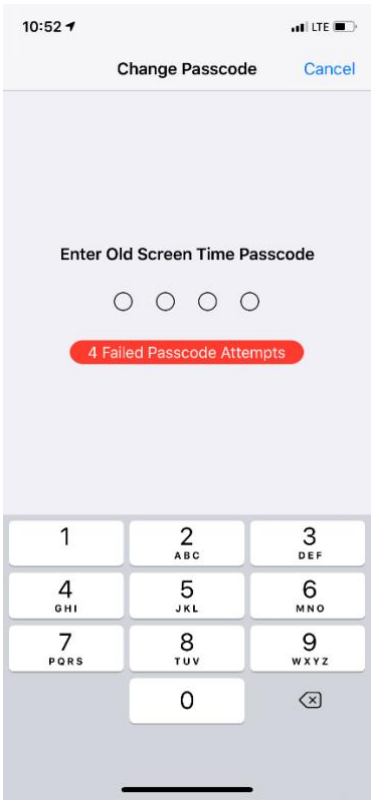
Кроме того, сброс кода блокировки исключает iPhone из доверенного круга устройств, которые могут синхронизировать в iCloud облачную связку ключей, данные «Здоровья», сообщения и некоторые другие данные. Также утрачивается возможность

сброса пароля к iCloud без знания старого, с использованием только кода блокировки устройства. Наконец, теряется большая часть данных, для хранения которых в принципе требуется наличия пасскода – например, данные банковских приложений.

5.4.6. Проблемы в процессе сброса пароля к резервной копии

Начиная с iOS 7, в системе могут быть настроены ограничения, которые защищают некоторые настройки телефона. В iOS 12 ограничения заменили на расширенный функционал, предоставляемый функцией Экранного времени.

Если пользователь установил защиту посредством ограничений или Экранного времени, при попытке сбросить настройки iOS запросит дополнительный пароль Экранного времени. Несмотря на то, что длина пароля ограничена всего 4 цифрами, перебрать все варианты быстро не удастся: после 6 неудачных попыток ввода система будет добавлять прогрессирующие задержки. Спустя 10 неудачных попыток время ожидания очередной попытки ввода составит час.



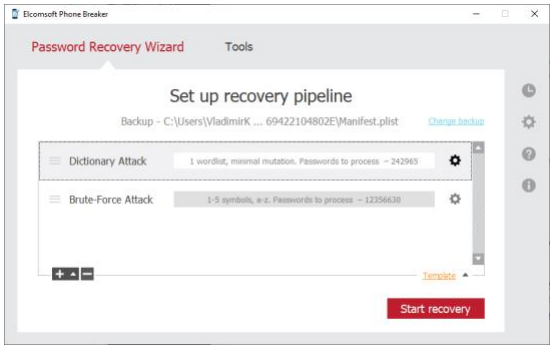
Пароль Экранного времени можно извлечь из облака при помощи Elcomsoft Phone Breaker, если известны логин и пароль от Apple ID пользователя, есть доступ ко второму фактору аутентификации и известен код блокировки или пароль от одного из доверенных устройств пользователя, зарегистрированных в той же учётной записи. Подробности – в разделе «Облачное извлечение».

5.4.7. Восстановление оригинального пароля в Elcomsoft Phone Breaker

Восстановление оригинального пароля методом перебора на современных версиях iOS работает крайне медленно. Начиная с iOS 10.2, скорость перебора с

использованием аппаратных ускорителей и мощных видеокарт не превышает нескольких десятков (в лучшем случае — сотен) паролей в секунду. С такой скоростью можно взломать лишь самые слабые пароли, которые встречаются крайне редко. Ещё один вариант — использование словаря, составленного из известных паролей того же пользователя.

Для атаки на пароль используйте Elcomsoft Phone Breaker. Подробности атак описаны в руководстве пользователя к продукту.



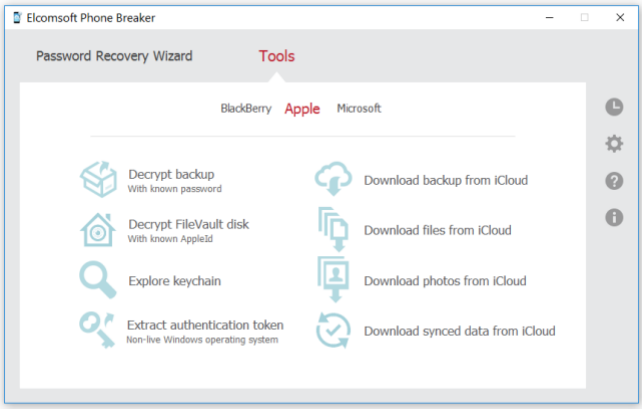
Обратите внимание: для восстановления паролей можно использовать только версию Elcomsoft Phone Breaker для Windows, т.к. только в этой редакции программы поддерживается перебор паролей, в том числе с использованием графических ускорителей.

В Elcomsoft Phone Breaker доступны фильтры, позволяющие ограничить количество вариантов паролей, которые будут использоваться для перебора. Можно указать минимальную и максимальную длину пароля, а также указать, какие наборы символов будут использоваться. Так, если заведомо известно, что пароль состоит только из цифр и латинских букв в нижнем регистре, имеет смысл так настроить атаку, чтобы программа не использовала для перебора специальные символы и заглавные буквы.

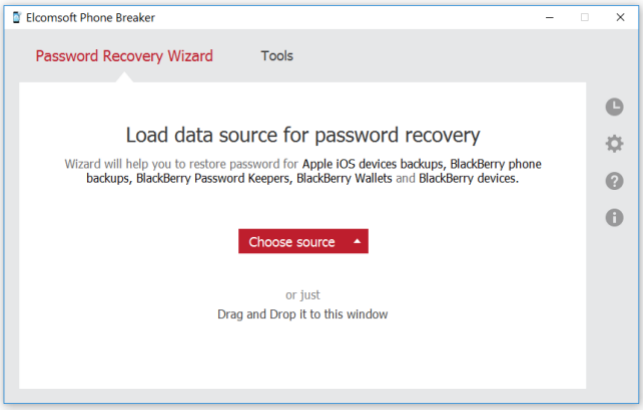
Обратите внимание: Использование одних и тех же паролей для защиты разных ресурсов – весьма распространённая практика. Попробуйте извлечь список паролей пользователя из альтернативных источников и использовать их для создания словаря. Кроме того, пароли пользователя могут помочь в создании шаблона, который ограничит число доступных комбинаций и существенно сократит время работы программы.

Инструкция по восстановлению пароля к резервной копии в формате iTunes с использованием Elcomsoft Phone Breaker:

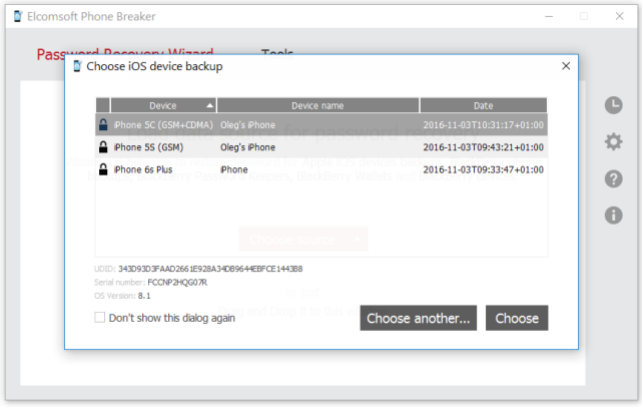
1. Запустите Elcomsoft Phone Breaker и откройте Password Recovery Wizard.



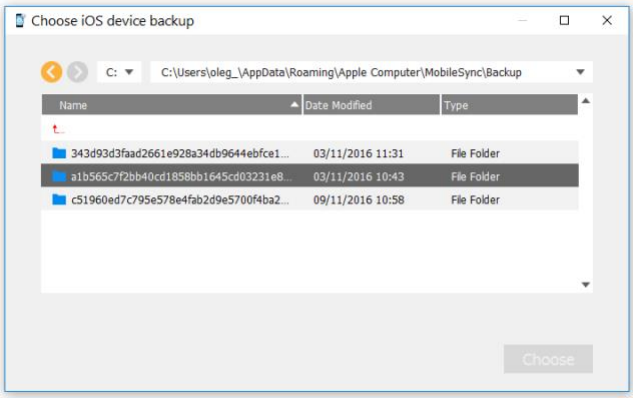
2. В окне Password Recovery Wizard выберите “Choose source” или перенесите файл Manifest.plist в окно программы.



3. Если программа запущена на компьютере пользователя из-под его учётной записи, в следующем окне будут перечислены все доступные резервные копии.



4. Если проводится анализ образа диска, путь к резервной копии нужно будет указать вручную через “Choose another”.



Если для создания резервной копии использовалось приложение iTunes, файлы доступны по следующим путям:

Windows XP:

– \Documents and Settings\(username)\Application Data\Apple Computer\MobileSync\Backup\

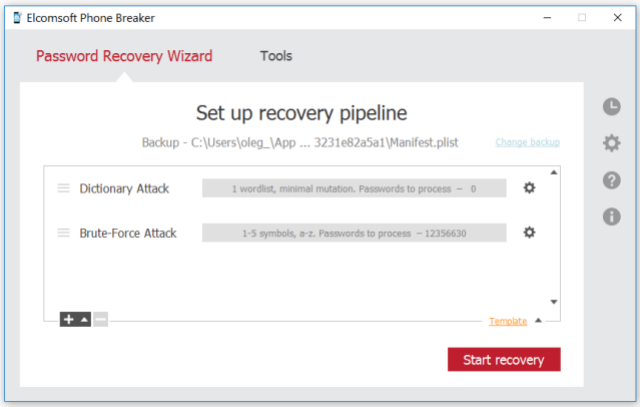
– Windows Vista, 7, 8, а также Windows 10 и 11 (автономная версия iTunes): \Users\username\AppData\Roaming\Apple Computer\MobileSync\Backup\

– При установке iTunes из Microsoft Store (Windows 10 и 11): \Users\username\Apple\MobileSync\Backup\

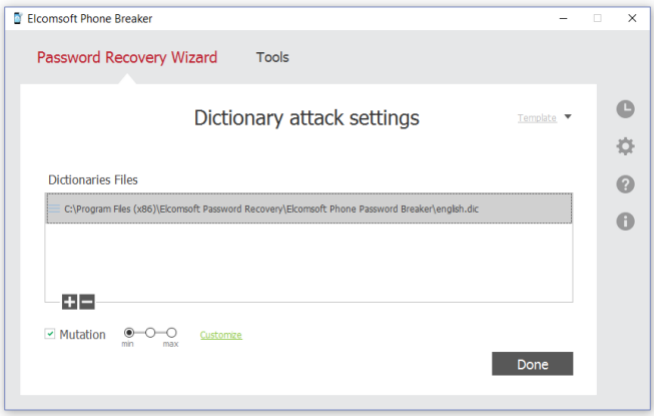
macOS:

– ~/Library/Application Support/MobileSync/Backup/

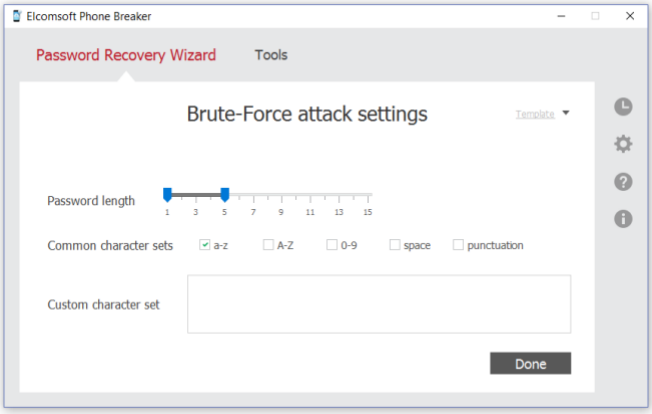
5. На следующем шаге настраиваются как сами атаки, так и последовательность, в которой они будут использоваться. Мы рекомендуем в первую очередь запускать словарные атаки (известные пароли пользователя, пароли из утечек, словари английских и русских слов, включая транслитерации и мутации). Во вторую очередь рекомендуем использовать полный перебор, также с ограниченными мутациями.



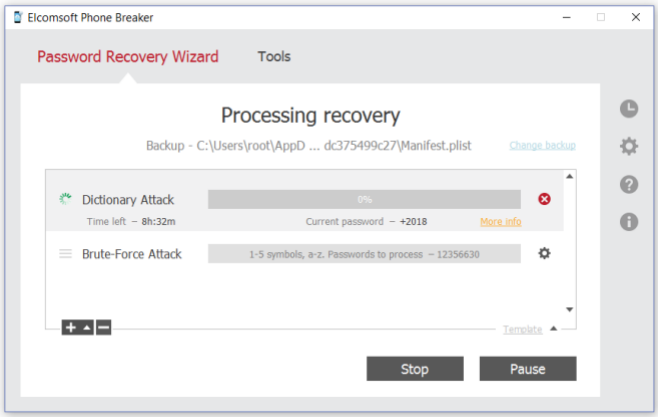
6. Настройки атак доступны кликом по иконке с изображением шестерёнки.



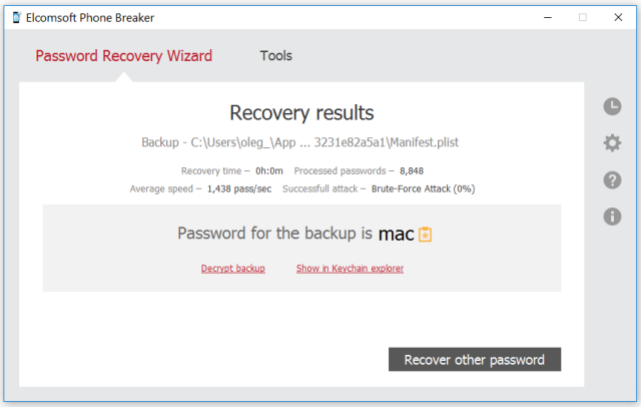
В атаке с использованием полного перебора можно ограничить как длину пароля (сверху и снизу), так и возможные наборы символов и уровни мутаций.



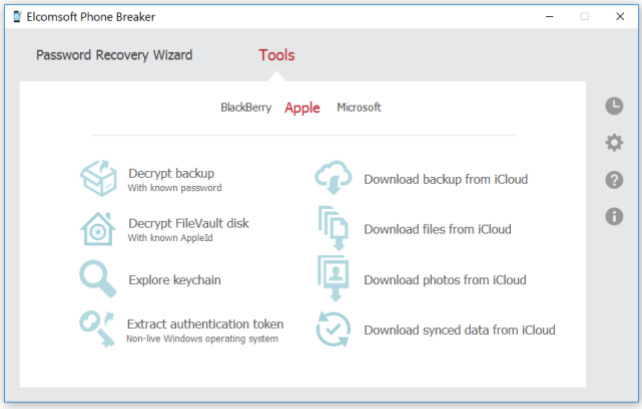
7. После настройки атак нажмите Start recovery. Будет запущен перебор паролей. Время до окончания атаки и текущий статус отображаются в окне “Processing recovery”. Более подробная информация доступна по нажатию “More info”.



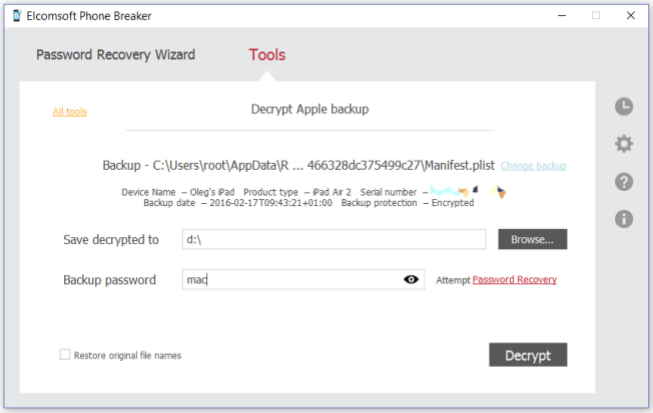
8. При успехе атаки пароль будет показан в соответствующем окне.



Восстановленный пароль может быть использован для расшифровки содержимого резервной копии, в том числе данных из связки ключей. Для расшифровки резервной копии нужно выйти в главное окно программы, после чего использовать команду “Decrypt backup with known password”.



Выберите резервную копию для расшифровки, укажите путь, куда будет сохранена расшифрованная копия, и введите пароль:



Обратите внимание на опцию **Restore original file names**. При использовании этого режима программа восстановит пути и названия файлов, максимально соответствующие тому, как данные хранились внутри устройства. Используйте этот режим для анализа содержимого вручную. При использовании для просмотра специализированных инструментов (Elcomsoft Phone Viewer в том числе) рекомендуем

не использовать эту опцию. Тогда расшифрованная резервная копия будет сохранена в стандартном формате iTunes.

Обратите внимание: Elcomsoft Phone Viewer способен работать с зашифрованными данными напрямую, если известен пароль. При использовании этого инструмента необходимости в предварительной расшифровке нет.

5.5. Медиафайлы

Логический анализ не ограничивается резервными копиями. В рамках процесса логического анализа можно также извлечь медиафайлы, в состав которых входят базы данных и уменьшенные копии изображений. Обратите внимание, что в метаданных EXIF хранятся в том числе и географические координаты, в которых был сделан снимок. Извлечение медиафайлов работает независимо от того, установлен ли пароль на резервную копию.

При извлечении медиафайлов по протоколу AFC создаётся tar-файл со следующей структурой папок:

```
AFC
│   com.apple.itunes.lock_sync
│
├────AirFair
│   └────sync
├────Books
│   │   .Books.plist.lock
│   │
│   ├────Managed
│   │       .Managed.plist.lock
│   │
│   ├────Purchases
│   │       .Purchases.plist.lock
│   │
│   └────Sync
│       ├────Artwork
│       └────Database
├────DCIM
│   ├────.MISC
│   │   └────Incoming
│   └────100APPLE
│           IMG_0001.PNG
│           IMG_0002.PNG
│           IMG_0003.PNG
│           IMG_0004.PNG
│
├────Downloads
│   │   downloads.28.sqlitedb
│   │   downloads.28.sqlitedb-shm
```

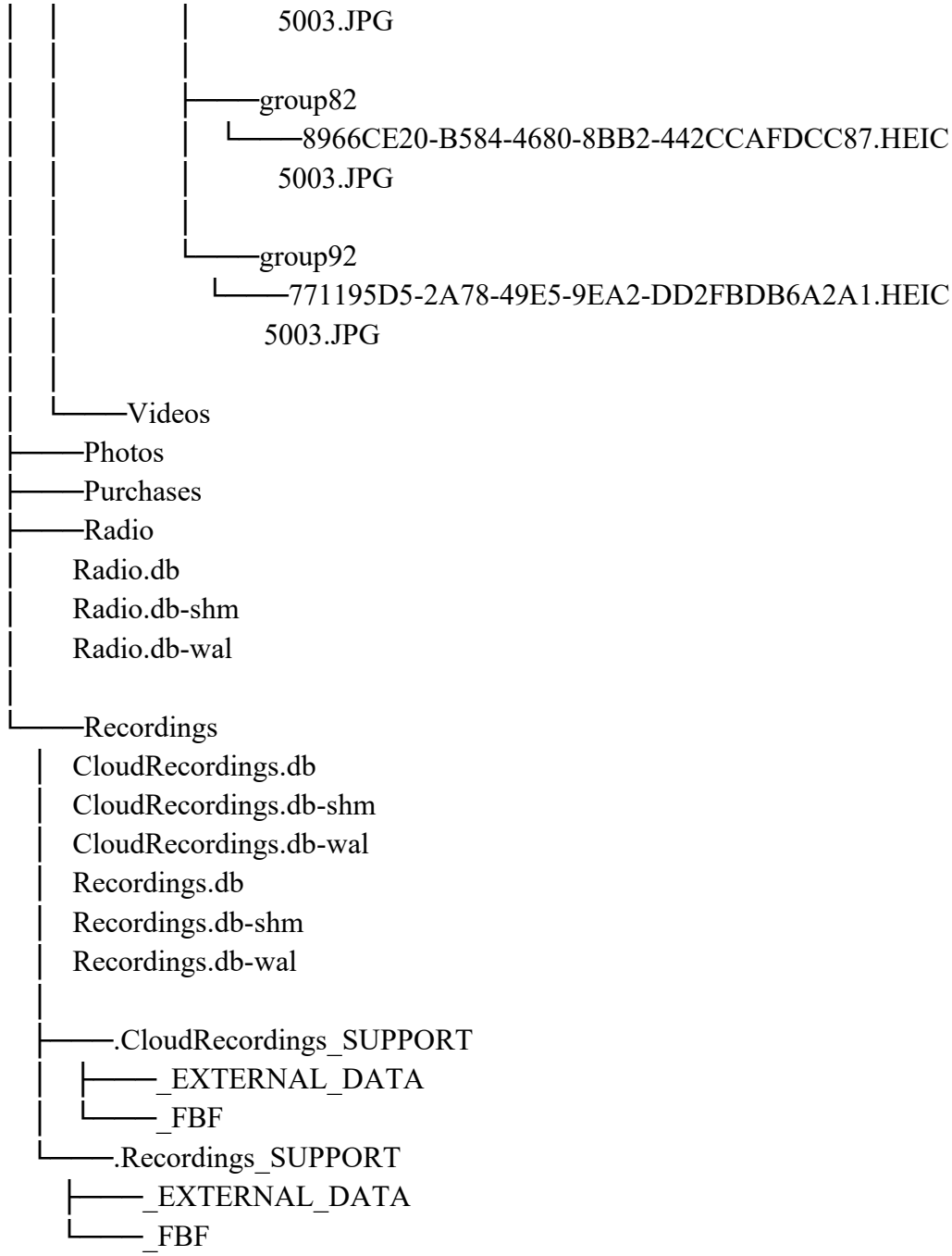
```
│   │   downloads.28.sqlitedb-wal
│   │
│   └───com.apple.UserManagedAssets
├───EnhancedAudioSharedKeys
│       ic-key-11711224381910920077d.dat
│
├───iTunes_Control
│   ├───Artwork
│   │       ArtworkDB
│   │
│   ├───iTunes
│   │       1624666015872072328 1-ContentTastePendingChanges.plist
│   │       IC-Info.sidv
│   │       iTunesCDB
│   │       iTunesControl
│   │       iTunesPrefs
│   │       iTunesPrefs.plist
│   │       iTunesSyncDeletes.plist
│   │       MediaLibrary.sqlitedb
│   │       MediaLibrary.sqlitedb-shm
│   │       MediaLibrary.sqlitedb-wal
│   │       PlayCounts.plist.cig
│   │       VoiceMemos.plist
│   │
│   ├───Music
│   └───Sync
│       └───Media
├───MediaAnalysis
│   │   mediaanalysis.db
│   │   mediaanalysis.db-shm
│   │   mediaanalysis.db-wal
│   │
│   └───.backup
│           mediaanalysis.backup
│
├───PhotoData
│   │   Photos.sqlite
│   │   Photos.sqlite-shm
│   │   Photos.sqlite-wal
│   │   protection
│   │   PXPlacesAlbumImageCached.jpg
│   │   PXPlacesAlbumImageCached_Dark.jpg
│   │
│   ├───.Photos_SUPPORT
```

```
│   │   └──── _EXTERNAL_DATA
│   ├──── AlbumsMetadata
│   │     E0AED833-8C8D-4C48-8694-15A896772A65.foldermetadata
│   │
│   ├──── Caches
│   │   │ CreateDatabase_20210517-145045-07
│   │   │ libraryavailable
│   │   │ PLDataMigrationInfo.plist
│   │   │ RebuildThumbnails_20210517-145053-07
│   │   │
│   │   ├──── Analytics
│   │   │     CPAnalyticsPropertiesCache.plist
│   │   │
│   │   ├──── ClientServerTransactions
│   │   ├──── GraphService
│   │   │   │ changetoken.plist
│   │   │   │ CLSBusinessCategoryCache.AOI.sqlite
│   │   │   │ CLSBusinessCategoryCache.AOI.sqlite-shm
│   │   │   │ CLSBusinessCategoryCache.AOI.sqlite-wal
│   │   │   │ CLSBusinessCategoryCache.Nature.sqlite
│   │   │   │ CLSBusinessCategoryCache.Nature.sqlite-shm
│   │   │   │ CLSBusinessCategoryCache.Nature.sqlite-wal
│   │   │   │ CLSBusinessCategoryCache.POI.sqlite
│   │   │   │ CLSBusinessCategoryCache.POI.sqlite-shm
│   │   │   │ CLSBusinessCategoryCache.POI.sqlite-wal
│   │   │   │ CLSBusinessCategoryCache.ROI.sqlite
│   │   │   │ CLSBusinessCategoryCache.ROI.sqlite-shm
│   │   │   │ CLSBusinessCategoryCache.ROI.sqlite-wal
│   │   │   │ CLSContactCache.sqlite
│   │   │   │ CLSContactCache.sqlite-shm
│   │   │   │ CLSContactCache.sqlite-wal
│   │   │   │ CLSLocationCache.sqlite
│   │   │   │ CLSLocationCache.sqlite-shm
│   │   │   │ CLSLocationCache.sqlite-wal
│   │   │   │ CLSPublicEventCache.sqlite
│   │   │   │ CLSPublicEventCache.sqlite-shm
│   │   │   │ CLSPublicEventCache.sqlite-wal
│   │   │   │ ftemetrics
│   │   │   │ PGCurationCache.sqlite.sqlite
│   │   │   │ PGCurationCache.sqlite.sqlite-shm
│   │   │   │ PGCurationCache.sqlite.sqlite-wal
│   │   │   │ PGSearchComputationCache.plist
│   │   │   │ PGSharingFeatureExtractorRecords.plist
│   │   │   │ PhotoAnalysisServiceFeaturesAnalytics.plist
```

```
│   │   │   │   PhotoAnalysisServicePreferences.plist
│   │   │   │   revgeoprovider.plist
│   │   │   │
│   │   │   └──PhotosGraph
│   │   │       construction-photosgraph.kgdb
│   │   │       construction-photosgraph.kgdb-shm
│   │   │       construction-photosgraph.kgdb-wal
│   │   │       photosgraph-tmp.kgdb
│   │   │       photosgraph-tmp.kgdb-shm
│   │   │       photosgraph-tmp.kgdb-wal
│   │   │       photosgraph.kgdb
│   │   │       photosgraph.kgdb-shm
│   │   │       photosgraph.kgdb-wal
│   │   │
│   │   ├──search
│   │   │   graphDataProgress.plist
│   │   │   psi.sqlite
│   │   │   psi.sqlite-shm
│   │   │   psi.sqlite-wal
│   │   │   searchMetadata.plist
│   │   │   searchProgress.plist
│   │   │   searchSystemInfo.plist
│   │   │   spotlightProgress.plist
│   │   │   synonymsProcess.plist
│   │   │   zeroKeywords.data
│   │   │
│   │   ├──VariationCache
│   │   └──VisionService
│   │       AlgoFaceClusterCache.data
│   │       clustererState.plist
│   │       faceWorkerState.plist
│   │       mediaAnalysisVersionState.plist
│   │       PhotoAnalysisServicePreferences.plist
│   │
│   ├──CPL
│   ├──CPLAssets
│   │   ├──group113
│   │   │   204AEA3D-D441-4FCB-BBD3-252FAD6D3023.PNG
│   │   │
│   │   ├──group133
│   │   │   CA492218-F4CA-4504-A781-0623B706AC27.PNG
│   │   │
│   │   ├──group153
│   │   │   C43C40AE-3589-4101-A170-616928967E12.PNG
```

```
│   │   │
│   │   └──group92
│   │       771195D5-2A78-49E5-9EA2-DD2FBDB6A2A1.HEIC
│   │
│   ├──FacesMetadata
│   ├──Journals
│   │   MigrationHistory-change.plj
│   │   MigrationHistory.plist
│   │
│   ├──Metadata
│   │   └──PhotoData
│   │       └──CPLAssets
│   │           ├──group113
│   │           │   204AEA3D-D441-4FCB-BBD3-252FAD6D3023.JPG
│   │           │
│   │           ├──group133
│   │           │   CA492218-F4CA-4504-A781-0623B706AC27.JPG
│   │           │
│   │           ├──group385
│   │           │   7D964629-43FC-4389-968B-2F099E8F8349.JPG
│   │           │
│   │           └──group82
│   │               8966CE20-B584-4680-8BB2-442CCAFDCC87.JPG
│   │
│   ├──MISC
│   │   DCIM_APPLE.plist
│   │   PreviewWellImage.tiff
│   │
│   ├──Mutations
│   │   └──PhotoData
│   │       └──CPLAssets
│   │           └──group92
│   │               └──771195D5-2A78-49E5-9EA2-DD2FBDB6A2A1
│   │                   └──Adjustments
│   │                       Adjustments.plist
│   │                       FullSizeRender.jpg
│   │
│   ├──OutgoingTemp
│   ├──PhotoCloudSharingData
│   │   │   personID
│   │   │   serverconfiguration
│   │   │
│   │   ├──Caches
│   │   │   diskcacherepository.plist
```

```
│   │   │       sharedAssetsPrefetchCount.plist
│   │   │
│   │   └──────INFLIGHT_JOBS
│   ├──────private
│   │   ├──────com.apple.accountsd
│   │   │       cloudServiceEnableLog.plist
│   │   │
│   │   └──────com.apple.assetsd
│   │           appPrivateData.plist
│   │           cloudServiceEnableLog.plist
│   │
│   ├──────Thumbnails
│   │   │   3334.ithmb
│   │   │   3350.ithmb
│   │   │   4531.ithmb
│   │   │   thumbnailConfiguration
│   │   │
│   │   └──────V2
│   │       ├──────DCIM
│   │       │   └──────100APPLE
│   │       │       ├──────IMG_0001.PNG
│   │       │       │       5003.JPG
│   │       │       │
│   │       │       ├──────IMG_0002.PNG
│   │       │       │       5003.JPG
│   │       │       │
│   │       │       ├──────IMG_0003.PNG
│   │       │       │       5003.JPG
│   │       │       │
│   │       │       └──────IMG_0004.PNG
│   │       │               5003.JPG
│   │       │
│   │       └──────PhotoData
│   │           └──────CPLAssets
│   │               ├──────group113
│   │               │   └──────204AEA3D-D441-4FCB-BBD3-252FAD6D3023.PNG
│   │               │           5003.JPG
│   │               │
│   │               ├──────group133
│   │               │   └──────CA492218-F4CA-4504-A781-0623B706AC27.PNG
│   │               │           5003.JPG
│   │               │
│   │               ├──────group67
│   │               │   └──────3B0F1669-2610-4E24-883D-98FC2CE9415D.PNG
```



Стандартными средствами (при использовании Explorer или Finder, если подключить устройство напрямую к компьютеру или синхронизировать через iTunes) извлекается только папка DCIM, в которой содержатся подкаталоги 100APPLE, 101APPLE и т.д., в которых хранятся фотографии. Через протокол AFC, в свою очередь, извлекается полная копия следующей папки файловой системы:

```
/private/var/mobile/Media
```

В состав резервных копий эта папка попадает не полностью, а только следующие каталоги:

- DCIM (сами фото/видео);

– PhotoData (инфа о редактировании, уменьшенные изображения и прочее);
– Recordings (записи встроенного диктофона).

Остальные данные или не сохраняются вовсе, или сохраняются не полностью. Кроме того, при создании резервной копии, вероятно, выполняется процедура VACUUM или ей подобная на все многочисленные базы данных в формате SQLite. В процессе выполнения этой процедуры происходит слияние файлов WAL с основным содержимым баз данных, и если в WAL содержались команды на удаление, то соответствующие записи будут безвозвратно удалены.

Таким образом, извлечение медиафайлов посредством AFC (и соответствующей функции iOS Forensic Toolkit) имеет следующие преимущества:

– можно полностью извлечь содержимое папки, даже если пароль на резервную копию установлен и неизвестен;
– извлекается значительно больше метаданных по сравнению с любыми другими способами, доступными в рамках логического анализа;
– могут быть найдены удалённые записи.

Для просмотра фотогалереи, включая данные EXIF, можно использовать любой совместимый инструмент, включая Elcomsoft Phone Viewer. Анализ метаданных проводится вручную.

5.6. Системные журналы

В рамках расширенного логического извлечения доступны некоторые системные журналы, включая журнал диагностики и crash-лог, а также файлы, доступ к которым через iTunes открывают некоторые приложения.

В извлекаемых журналах содержится масса ценной информации, в том числе такой, которая не попадает в резервные копии. В них входит информация о том, какие приложения и когда именно устанавливались и запускались пользователем, информация по сетям Wi-Fi, а также многочисленные системные события. Особенную ценность может журналы могут иметь для ответа на вопрос, что именно происходило в определённый период времени, а также для детектирования наличия специализированного ПО для слежки за пользователем (см. отчёт Amnesty International касательно NSO). В то же время ряд файлов сохраняется в неизвестном двоичном формате; их анализ невозможен.

Внимание: для того, чтобы подготовить устройство для извлечения максимально подробных системных журналов, устройство нужно подготовить. Для iPhone и iPad используйте комбинацию клавиш (см. ниже). Для часов Apple Watch требуется установка отладочного профиля sysdiagnose по ссылке[32].

Для других платформ установка отдельного профиля не требуется; достаточно нажать определённую комбинацию клавиш и выждать некоторое время, в течение которого создаются журналы. В процессе создания журнала sysdiagnose системой

[32] https://developer.apple.com/bug-reporting/profiles-and-logs/

копируются файлы из разных папок файловой системы, после чего упаковываются в один архив, который и извлекается iOS Forensic Toolkit.

Инструкции по подготовке устройства и анализу журналов

1. Обязательно ознакомьтесь с инструкциями и подготовьте устройство. Если журналы извлечь из неподготовленного устройства, то возвращается минимум информации – только crash logs и системная аналитика, большая часть из которой представляет интерес только для компании Apple. Для генерации журналов диагностики (diagnostic logs) необходимо сначала нажать комбинацию клавиш, которая различается в зависимости от типа устройства.

Для iPhone нужно одновременно нажать кнопки Volume Up, Volume Down и Power и удерживать их в течение одной-полутора секунд. Если кнопки удерживать дольше, ничего не произойдёт; о том, что логи успешно сгенерировались, сообщит лёгкая вибрация устройства и появившийся скриншот (бесполезный с точки зрения экспертизы). После этого подождите несколько минут, пока файл sysdiagnose_timestamp.tar.gz не появится среди прочего в следующем списке:

Settings | Privacy | Analytics & Improvements | Analytics Data

2. При анализе Apple Watch необходимо установить профиль по указанной выше ссылке (внимание: в остальных устройствах механизм встроен).

3. Только после этого можно приступать к извлечению с iOS Forensic Toolkit.

4. Анализ извлечённых журналов требует квалифицированного подхода. Рекомендуем ознакомиться с инструкциями за авторством Mattia Epifani по следующей ссылке:

https://www.for585.com/sysdiagnose[33]

В кратком изложении об анализе системных журналов можно прочитать в презентации Heather Mahalik:

https://www.osdfcon.org/presentations/2019/Heather-Mahalik_Using-Apple-Bug-Reporting-for-Forensic-Purposes.pdf[34]

Для обработки некоторых типов журналов потребуются специализированные скрипты. Их можно скачать по следующей ссылке:

https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts[35]

Для анализа Mobile Installation Logs используйте следующее ПО:

https://github.com/abrignoni/iOS-Mobile-Installation-Logs-Parser[36]

5.7. Данные приложений (shared files)

Некоторые приложения используют API, позволяющий пользователю передавать файлы через iTunes. Например, видеоплееры позволяют использовать iTunes, чтобы создать фильмотеку, аудиоплееры позволяют закачать с компьютера аудиофайлы и т.д.

В iOS Forensic Toolkit предусмотрен механизм для извлечения таких файлов из приложений.

---

[33] https://www.for585.com/sysdiagnose

[34] https://www.osdfcon.org/presentations/2019/Heather-Mahalik_Using-Apple-Bug-Reporting-for-Forensic-Purposes.pdf

[35] https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts

[36] https://github.com/abrignoni/iOS-Mobile-Installation-Logs-Parser

5.8. Шаги для логического извлечения данных

Для расширенного логического извлечения используйте Elcomsoft iOS Forensic Toolkit. Продукт поможет создать резервную копию с максимальным количеством информации, извлечёт медиафайлы, журналы диагностики и файлы приложений.

Обратите внимание: если пароль на резервную копию не установлен, то при создании резервной копии в iOS Forensic Toolkit будет автоматически установлен временный пароль ‘123’ (для этого нужно подтверждение на исследуемом устройстве – на экране появится запрос кода блокировки, не пропустите его). После окончания работы пароль будет сброшен в начальное (пустое) состояние. При открытии созданной продуктом резервной копии введите пароль 123 для её расшифровки.

Внимание: в процессе как установки, так и удаления временного пароля к резервной копии на экране устройства может возникнуть запрос кода блокировки экрана. Введите его в окне запроса. Запрос автоматически пропадает через некоторое время; если вовремя не ввести код блокировки в начале работы, то резервная копия будет создана без пароля, а если этого не сделать в конце – на устройстве останется установленным временный пароль 123, который впоследствии можно будет удалить специальной командой.

Последовательность шагов

Внимание: при использовании компьютера с macOS крайне рекомендуется использовать кабель USB-C несмотря на то, что на всех устройствах до iPhone 15 Pro используется старый стандарт USB.

1. Подключите iPhone к компьютеру
2. При подключении устройства к компьютеру автоматически выводится запрос на привязку устройства. Для привязки устройства к компьютеру на устройстве потребуется подтвердить запрос и ввести код блокировки экрана. Если по какой-либо причине привязки не произошло или она не сработала, привязать устройство к компьютеру можно вручную, выполнив команду:

```
./EIFT_cmd normal pair
```

3. Далее подтвердите запрос «Trust this computer?» на телефоне. Для подтверждения запроса нужно ввести код блокировки; если код блокировки не установлен, то система не станет его запрашивать.
4. Если используется запись pairing record (и только в этом случае), после каждой команды необходимо указывать путь к этой записи в параметре командной строки. В дальнейшем мы будем опускать этот момент, но не забывайте использовать параметр -r и путь к файлу pairing record, если используется данный способ авторизацииы:

```
./EIFT_cmd info -r record.plist
```

5. Извлеките основную или расширенную информацию об устройстве. Для извлечения только основной информации используйте следующую команду:

```
./EIFT_cmd info
```

Расширенную информацию можно извлечь следующей командой:

```
./EIFT_cmd info -a
```

В состав расширенной информации входят листинги в формате XML, в которых содержатся многочисленные записи о настройках устройства, а также список установленных на устройстве приложений с детализацией по дате и времени установки, путям к файлам и прочим данным. Для сохранения в файл используйте переадресацию вывода. Если это сделать, то работу команды через какое-то время придётся прервать вручную комбинацией клавиш Ctrl-C:

```
./EIFT_cmd info > info.txt
```

6. Проверьте, установлен ли пароль на резервную копию. Для этого выполните следующую команду:

```
./EIFT_cmd normal backuppwcheck
```

Далее ознакомьтесь со следующим листингом:

```
   Started logging Thread!
Got device:
Mode: [normal]
BuildVersion: 16H50
DeviceName: iPhone
HardwareModel: N53AP
Paired: YES
PasswordProtected: NO
ProductName: iPhone OS
ProductType: iPhone6,2
ProductVersion: 5.4
SerialNumber: <serial number> udid: <udid>
Loading custom record from=record.plist
Checking backup password...
Backup password is DISABLED
Done
```

7. Если пароль на резервную копию установлен, рекомендуем прежде создать резервную копию «как есть», после чего извлечь все последующие данные (медиафайлы, файлы приложений и системные журналы). Только после этого на устройствах, работающих на iOS 11 и более новых версиях, вы можете попытаться сбросить пароль резервной копии (обратите внимание на связанные с этим риски).
8. [**опционально**] Если пароль на резервную копию пуст, вы можете самостоятельно установить временный пароль на резервную копию. Данный шаг опционален: если вы этого не сделаете, iOS Forensic Toolkit автоматически установит временный пароль "123", который будет снят автоматически по

окончании создания резервной копии. В любом случае на устройстве будет запрошен код блокировки экрана; обязательно введите его, т.к. запрос будет убран с экрана спустя короткое время. Пароль можно задать следующей командой:

```
./EIFT_cmd normal backuppwset -p "123"
```

9. Далее создайте резервную копию (последний параметр указывает текущий каталог в качестве папки для сохранения резервной копии). Обратите внимание: если пароль на резервную копию пуст, инструментарий попытается установить временный пароль "123", в результате чего на устройстве будет запрошен код блокировки экрана; обязательно введите его, т.к. запрос пропадает с экрана спустя короткое время:

```
./EIFT_cmd normal backup -o ./
```

Отметим, что процесс резервного копирования начинается не сразу. На iOS 15+ может пройти до минуты, пока не начнётся прогресс. Точная причина нам неизвестна; возможно, сервис резервного копирования на телефоне подготавливает список файлов для копирования, обрабатывает WAL, удаляет временные файлы и т.д.

10. Если на шаге 7 вы самостоятельно установили временный пароль к резервной копии или пропустили запрос кода блокировки экрана в момент, когда утилита попыталась сбросить ранее установленный временный пароль, его нужно будет удалить вручную. Для этого в командной строке передаётся ранее установленный временный пароль (в данном случае – 123):

```
./EIFT_cmd normal backuppwunset -p "123"
```

11. Извлеките медиафайлы по протоколу afc. В отличие от резервных копий, данный протокол работает и для Apple TV и Apple Watch; он не может быть защищён паролем, т. к. медиа хранятся в папке, которая доступна всегда. Кроме того, помимо самих фото и видео, по протоколу afc извлекается ряд ценных метаданных.

```
./EIFT_cmd normal dumpafc -o afcdump.tar
```

12. На iPhone сгенерируйте журнал системной диагностики (sysdiagnose), одновременно зажав кнопки Vol+, Vol- и кнопку питания. Удерживайте кнопки примерно 1.25с, после чего подождите некоторое время (до 5 минут).

13. Копирование системных журналов об ошибках:

```
./EIFT_cmd normal dumpcrash -o crashlogs.tar
```

14. Следующая команда сохранит все совместно-используемые файлы приложений в файле container.tar:

```
./EIFT_cmd normal dumpshared -o container.tar
```

15. Расшифруйте резервную копию (напоминаем, используйте временный пароль) или откройте её в приложении для анализа Elcomsoft Phone Viewer, указав временный пароль (в данном примере – 123).

6. Извлечение данных: облачный анализ

Цель облачного анализа – дополнить извлекаемые из физического устройства данные или получить доступ к данным заблокированных, повреждённых и отсутствующих устройств. В облаке часто можно найти информацию, которой нет на самом устройстве. Такими данными могут быть фотографии, которые могут быть выгружены в облако с автоматическим удалением из памяти устройства, а также данные, которые были удалены на самом устройстве, но сохранились в облаке.

В облако попадают данные со всех устройств пользователя, зарегистрированных в учётной записи Apple, а не только с того или тех устройств, к которым есть физический доступ.

Второй составляющей облачной криминалистики является доступность данных. Облачный анализ может оказаться единственным доступным способом для извлечения данных в следующих ситуациях:

- Код блокировки устройства неизвестен; устройство не подвержено известным уязвимостям
- Устройство неработоспособно или заблокировано
- Нет физического доступа к устройству

Таким образом, облачный анализ является дополнением, а в ряде случаев — заменой анализа физического устройства, позволяя получить доступ к массиву данных, не уступающему тому, который доступен при логическом анализе iPhone.

6.1. Роль специализированного ПО в облачной криминалистике

Компания Apple не предоставляет инструментов для скачивания большинства типов данных, включая облачные резервные копии. Даже по запросу от правоохранительных органов Apple не предоставляет данных, защищённых сквозным шифрованием. Компания последовательно затрудняет доступ к таким данным для сторонних программ и сервисов. Шифрование, аппаратные идентификаторы, временная блокировка учётных записей и многие другие меры предназначены для защиты резервных копий от любых попыток доступа, кроме восстановления на «чистый» iPhone.

Таким образом, единственный способ получить доступ к данным из облака без специализированного ПО – восстановление недавно сброшенного iPhone из «облачной» резервной копии с последующим извлечением полученных данных уже из физического устройства. Недостатки этого способа очевидны: теряется криминологическая чистота исследования; требуется устройство, работающее под управлением конкретной версии iOS; скорость восстановления — низкая, а трудоёмкость процесса с учётом последующего извлечения — высокая. Специализированное ПО позволяет извлечь как синхронизированные данные, так и данные из резервной копии, а также данные, защищённые «сквозным шифрованием», без использования физических устройств.

6.2. Запрос данных у Apple

В ряде случаев сотрудники правоохранительных органов могут получить часть данных из «облака», оформив официальный запрос к компании Apple согласно протоколу:

https://www.apple.com/ru/privacy/government-information-requests/[37]

На странице содержится актуальная информация о том, что именно выдаёт Apple, каким образом оформляется запрос и куда его отправлять. Подробности и руководство по составлению запроса доступны на русском языке в файле https://www.apple.com/ru/privacy/docs/legal-process-guidelines-emeia.pdf[38]

Согласно официальному руководству, **Apple предоставляет по запросу следующие данные:**

Информация, которую предоставляет Apple (выдержка из документа):

A. Регистрация устройств
B. Записи об обслуживании пользователей
C. iTunes
D. Транзакции в розничных магазинах Apple
E. Покупки в интернет-магазине Apple Online Store
F. Подарочные карты iTunes
G. iCloud
    I. Данные подписчика
    II. Журналы электронной почты
    III. Контент из электронной почты и другой контент iCloud. Фотопоток,
    IV. документы, контакты, календари, закладки, резервные копии устройств iOS
H. Найти iPhone
I. Извлечение данных с устройств iOS, защищённых паролем
    I. С устройств под управлением iOS 8.0 и более новых версий Apple не извлекает данные iOS, поскольку инструменты извлечения данных больше не функционируют. Извлекаемые файлы защищены ключом шифрования, привязанным к коду-паролю пользователя, которым Apple не владеет.
    II. С устройств под управлением более ранних версий, чем iOS 8.0, защищённых кодом-паролем, Apple Inc. может извлекать определённые категории активных данных после получения ордера на обыск, выданного в соответствии с процедурами MLAT.
J. Прочая предоставляемая информация об устройствах:
    I. Запросы на предоставление записей с камер видеонаблюдения в розничных магазинах Apple
    II. Game Center

[37] https://www.apple.com/ru/privacy/government-information-requests/
[38] https://www.apple.com/ru/privacy/docs/legal-process-guidelines-emeia.pdf

III. Активация устройств iOS
IV. Журналы входа в систему
V. Журналы «Мой Apple ID» и iForgot
VI. FaceTime

Подробности о каждом из типов данных

Официальное руководство не охватывает всех ситуаций, которые могут возникнуть. Поэтому любые дополнительные вопросы направляйте в компанию Apple на адрес электронной почты law.enf.emeia@apple.com. Этот адрес предназначен только для представителей правоохранительных и государственных органов. Если вы хотите написать на этот адрес электронной почты, отправляйте письмо с действующего адреса правоохранительного/государственного органа. Запросы можно отправлять через форму https://www.apple.com/ru/privacy/contact/[39]

Для особо срочных и важных запросов у Apple есть выделенный адрес: exigent@apple.com

Вы можете использовать его, если речь идёт о:

– жизни/безопасности людей;

– безопасности государства;

– причинении существенного вреда жизненно важной инфраструктуре или сооружениям.

У этого способа доступа к данным есть как преимущества, так и недостатки в сравнении с использованием ПО для «облачной» криминалистики.

Преимуществом является то, что знать пароль от учётной записи (а в ряде случаев — и идентификатор учётной записи) пользователя не обязательно; запрос можно оформить как по идентификатору Apple ID, так и по серийному номеру устройства или персональной информации пользователя.

К недостаткам относится сложность оформления соответствующего запроса и сопутствующих документов, длительное время ожидания ответа и неполный объём данных, возвращаемый компанией. Apple не возвращает данные, для защиты которых использовалось «сквозное шифрование». Такие данные можно извлечь лишь посредством Elcomsoft Phone Breaker при соблюдении ряда условий.

Apple возвращает данные в «сыром» виде — то есть, зашифрованными в комплекте с ключами шифрования. Инструментарий для расшифровки или просмотра данных компания не предоставляет, поэтому для расшифровки и анализа эксперту так или иначе придётся воспользоваться одним из сторонних решений.

6.3. Преимущества и недостатки облачного анализа

Облачный анализ обладает рядом преимуществ и недостатков в сравнении с расширенным логическим извлечением. Эти отличия позволяют рекомендовать облачный анализ в качестве дополнения другим типам извлечения данных.

К преимуществам облачного анализа относятся следующие факторы:

[39] https://www.apple.com/ru/privacy/contact/

– в облаке iCloud хранятся данные, синхронизированные или сохранённые со всех зарегистрированных в учётной записи устройств пользователя, а не только с того устройства, к которому есть физический доступ;

– в облаке может храниться несколько старых резервных копий для каждого устройства, что позволяет извлечь и те данные, которые были удалены с самого устройства;

– облачный анализ позволяет получить данные даже в случаях, когда само устройство заблокировано, повреждено или отсутствует;

К недостаткам облачного анализа отнесём следующее:

– в облачные резервные копии попадает меньше данных, чем в локальные резервные копии с паролем;

– для доступа к ряду категорий данных требуется не только пароль и код двухфакторной аутентификации, но и код блокировки или системный пароль устройства;

– пароль от учётной записи может быть неизвестен;

– сложности юридического характера.

6.3.1. Роль двухфакторной аутентификации

Согласно Apple, двухфакторная аутентификация является дополнительным уровнем защиты Apple ID, который гарантирует, что посторонний человек не сможет получить доступ к учётной записи пользователя, даже зная пароль (за исключением службы Find My, доступ к которой предоставляется без прохождения проверки двухфакторной аутентификации).

Проверочный код можно получить одним из следующих способов:

– **получить push-сообщение на доверенное устройство Apple** (требуется разблокировать экран устройства кодом блокировки экрана или при помощи биометрики). Обратите внимание на рискованность этого способа: для его использования устройству потребуется предоставить доступ в сеть;

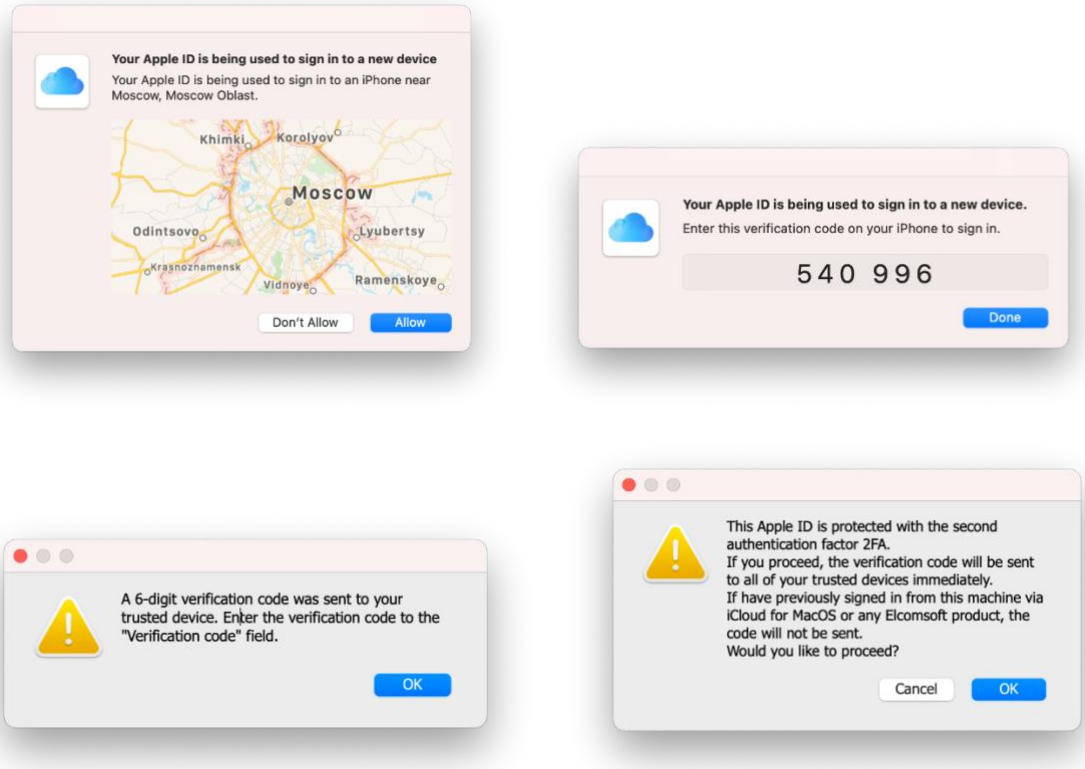
– **получить сообщение на доверенный телефонный номер.** Этот способ можно использовать, если само устройство заблокировано, но SIM-карта не защищена PIN-кодом. Если при настройке двухфакторной аутентификации пользователь выбрал опцию получения кода звонком автоответчика, то на доверенный телефонный номер поступит автоматизированный голосовой звонок; по умолчанию используется доставка в виде сообщения SMS;

– **сгенерировать на самом устройстве в режиме оффлайн.** Этот способ оптимален, если экран устройства удалось разблокировать, а устройство находится в полётном режиме.

Чтобы получить код в режиме офлайн, проделайте следующие действия:

1. На доверенном устройстве iPhone, iPad или iPod touch **выберите** «Настройки» > [Ваше имя] > «Пароль и безопасность», затем **коснитесь** «Получить код проверки».
2. На доверенном компьютере Mac с macOS 10.15 или новее **перейдите в меню** «Apple» > «Системные настройки» > «Apple ID» > «Пароль и безопасность», затем **нажмите** «Получить код проверки».

3. На доверенном компьютере Mac с macOS 10.14 или более ранней версии **перейдите в меню** «Apple» > «Системные настройки» > «iCloud» > «Учетная запись» > «Безопасность», затем **нажмите** «Получить код проверки». *Apple* [40]



Дополнительная информация на сайте Apple:

- Двухфакторная аутентификация на iPhone[41]
- Двухфакторная аутентификация для идентификатора Apple ID[42]
- Доступность двухфакторной аутентификации для идентификатора Apple ID[43]

6.4. Доступные данные: типы контейнеров

Данные в облаке хранятся в разных типах контейнеров, и доступ к ним осуществляется разными способами. Доступные в каждом из контейнеров данные будут перечислены в соответствующих разделах, однако нужно принять во внимание тот факт, что содержимое каждого из контейнеров может отличаться у разных пользователей в зависимости от настроек устройства и версии iOS, под управлением которого работает конкретное устройство.

6.4.1. Контейнер 1: резервные копии

В состав резервных копий в iCloud входят следующие типы данных:

– контакты, журнал звонков, сообщения SMS и iMessage*;

[40] https://support.apple.com/ru-ru/guide/ipod-touch/iphd709a3c46/ios
[41] https://support.apple.com/ru-ru/guide/iphone/iphd709a3c46/ios
[42] https://support.apple.com/ru-ru/HT204915
[43] https://support.apple.com/ru-ru/HT205075

– фотографии* и видеоролики;

– данные тех приложений, авторы которых разрешили резервное копирование;

– связка ключей (в составе облачных резервных копий — зашифрована аппаратным ключом и может быть восстановлена исключительно на то устройство, с которого была сделана резервная копия);

– настройки системы, список установленных приложений и многое другое.

В состав резервных копий в «облаке» могут не входить те данные, для которых пользователь включил синхронизацию с iCloud. При включении опции iCloud Photos фотографии пользователя попадают в отдельный сервис в iCloud и становятся доступными как часть синхронизированных данных, исчезая при этом из резервных копий (однако существует настройка, позволяющая включать и исключать фотографии из резервных копий и синхронизации по отдельности). Такие данные, как контакты, календари и заметки попадают и в синхронизированные данные, и в резервную копию.

На физическом уровне резервные копии в iCloud хранятся в распределённом виде на множестве серверов, которые принадлежат разным компаниям — Amazon, Google, Microsoft, AT&T и другим провайдерам. Ключи шифрования хранятся на серверах Apple в Купертино. Такая защита в состоянии эффективно противостоять угрозам физического или удалённого доступа к серверам, однако не защищает от доступа сотрудниками Apple или от удалённого доступа из авторизованной учётной записи.

Доступ к данным из резервных копий (за исключением паролей из Связки ключей, которые шифруются аппаратным ключом) могут иметь сотрудники Apple, а, следовательно, и сотрудники правоохранительных органов по запросу. Наконец, данные можно извлечь и расшифровать при помощи нашего продукта Elcomsoft Phone Breaker, если известны логин и пароль пользователя iCloud, а также есть доступ ко второму фактору аутентификации.

С учётом количества информации, которая хранится в резервных копиях, а также в той роли, которую они традиционно играли в облачной криминалистике, разработчики Apple постоянно усиливают защиту данных этого типа. На сегодняшний день с резервными копиями в облаке корректно работает ограниченное число продуктов, включая Elcomsoft Phone Breaker. Для доступа к облачным резервным копиям всегда требуется полный цикл аутентификации.

6.4.2. Контейнер 2: синхронизированные данные

В Apple последовательно расширяют список категорий данных, которые могут синхронизироваться между устройствами, а не статично храниться в резервной копии. Для некоторых категорий данных пользователю необходимо включить синхронизацию, другие синхронизируются в облако по умолчанию. Для некоторых типов данных включение их синхронизации приводит к исчезновению их из состава резервных копий. В то же время достаточно и таких категорий, которые могут и синхронизироваться в облако, и сохраняться в составе резервных копий.

Синхронизированные данные хранятся отдельно от резервных копий, доступны по отдельному протоколу и защищены менее стойкой защитой в сравнении с резервными копиями.

В состав синхронизированных данных входят следующие категории:

- Safari: история*, вкладки, закладки;
- Контакты, заметки, календари;
- Фотографии;
- История звонков**;
- Данные Apple Wallet;
- Информация об учётной записи;
- Почта iCloud;
- Книги Books, в том числе документы PDF и книги, полученные из сторонних источников;
- Погода, курсы;
- Shortcuts;
- Данные iMovie, Clips

* Начиная с iOS 14, история браузера Safari защищается сквозным шифрованием (см. ниже).

** История звонков синхронизируется нестабильно; явной зависимости от версий iOS не выявлено.

Получить доступ к синхронизированным данным проще, чем к облачным резервным копиям; допустимо использовать как полную процедуру аутентификации, так и токены macOS (на том же компьютере). В то же время нет полного совпадения между синхронизированными данными и данными, извлечёнными из облачной резервной копии. Для извлечения максимально полного набора рекомендуем скачать и резервную копию, и копию синхронизированных данных.

6.4.3. Контейнер 3: данные в iCloud Drive

В контейнере iCloud Drive могут содержаться некоторые данные приложений, которые не входят в состав облачных резервных копий (например, в iCloud Drive создаются автономные резервные копии мессенджера WhatsApp). Кроме того, в iCloud Drive могут содержаться скачанные пользователем в браузере Safari файлы, данные приложений Pages, Numbers, Keynote и, разумеется, документы с компьютеров Mac.

Поскольку **iCloud Drive** — общее хранилище данных, к которым должен быть доступ как у сторонних приложений, так и у самого пользователя, доступ к содержимому этого контейнера защищается слабее прочих. Для извлечения файлов достаточно авторизовать сессию логином и паролем (с прохождением проверки двухфакторной аутентификации); допустимо использовать маркеры аутентификации macOS (на том же компьютере).

6.4.4. Контейнер 4: сквозное шифрование

Некоторые типы данных в облаке могут быть дополнительно зашифрованы способом, известным как «сквозное шифрование». Сквозным

шифрованием защищаются такие данные, как связка ключей —пароли пользователя, которые он сохраняет в браузере Safari и приложениях. Данные приложения Здоровье, сообщения в iCloud (SMS и iMessage), данные Экранного времени, приложения Home, голосовые заметки, данные Карт Apple (поисковые запросы, маршруты и регулярные местоположения) также используют для защиты сквозное шифрование. Наконец, в iOS 14 появилась защита и таких данных, как история открытых в браузере Safari страниц.

Ниже перечислены известные категории данных, которые использует «сквозное шифрование»:

– облачная связка ключей (iCloud keychain), в которой содержатся пароли пользователя, ключи, токены, сертификаты и т.п.;
– облачные сообщения (SMS и iMessage);
– данные приложения Здоровье;
– данные Home;
– экранное время*;
– важные геопозиции*;
– голосовые заметки;
– Apple Maps (поисковые запросы, маршруты);
– история браузера Safari (начиная с iOS 14);
– данные, обозначенные знаком *, используют альтернативный механизм синхронизации и относятся к классу неизвлекаемых (см. ниже).

Помимо перечисленных, в документации Apple **указан ряд дополнительных категорий, для которых включено сквозное шифрование:**

– операции с использованием карты Apple Card (требуется iOS 12.4 или более поздняя версия);
– Memoji (требуется iOS 12.1 или более поздняя версия);
– платежная информация;
– набранный словарный запас клавиатуры QuickType (требуется iOS 11 или более поздней версии);
– информация Siri;
– пароли Wi-Fi;
– клавиши Bluetooth W1 и H1 (требуется iOS 13 или более поздняя версия).

Извлечение данных из этих категорий приложением Elcomsoft Phone Breaker не поддерживается.

Данные, защищённые сквозным шифрованием, дополнительно шифруются ключом, который генерируется на основе кода блокировки экрана iPhone или iPad. У пользователей компьютеров Mac в таком качестве выступает системный пароль. Не зная кода или пароля, данные расшифровать невозможно. По запросу от правоохранительных органов данные, защищённые сквозным шифрованием, предоставлены компанией Apple не будут.

Для извлечения данных, защищённых сквозным шифрованием, потребуется максимум информации, включая следующее:

– логин и пароль от учётной записи Apple ID
– прохождение проверки по методу двухфакторной аутентификации

– код блокировки или пароль одного из доверенных устройств, зарегистрированных в учётной записи пользователя.

6.4.4.1. Пароль Экранного времени

В категории «сквозного шифрования» хранится пароль Экранного времени. Этот пароль, если он установлен, будет запрошен системой при попытке сбросить пароль шифрования локальных резервных копий. Кроме того, пользователь может настроить ограничение на установку приложений, что сделает невозможной установку агента-экстрактора и последующий низкоуровневый анализ. Снять ограничение можно вводом пароля Экранного времени.

Начиная с iOS 12 данные Экранного времени синхронизируются в iCloud. Синхронизация происходит при выполнении двух условий. Во-первых, пользователь должен включить функцию «Учёт на всех устройствах» в настройках. Во-вторых, в учётной записи должна быть включена двухфакторная аутентификация.

Пароль Экранного времени в облаке iCloud хранится в зашифрованном виде. Для его расшифровки необходим код блокировки одного из доверенных устройств. Обратите внимание, что для синхронизации паролей Экранного времени в iCloud необходимо, чтобы функция «Учёт на всех устройствах» была уже активирована на устройстве. Функция доступна только в учётных записях с двухфакторной аутентификацией, поэтому дополнительный одноразовый код обязательно потребуется ввести в процессе работы.

Пароль Экранного времени отображается в приложении Elcomsoft Phone Viewer после того, как будут скачаны синхронизированные данные, защищённые сквозным шифрованием (при условии, что в процессе скачивания была отмечена категория Screen Time).

6.4.5. Контейнер 5: неизвлекаемые данные

Небольшую часть данных, защищённых сквозным шифрованием, извлечь из облака невозможно; ключи шифрования к таким данным не хранятся в облаке, а генерируются непосредственно на самом устройстве.

Таким образом, обмен такими данными осуществляется непосредственно между устройствами по принципу точка-точка. В частности, к таким данным относится статистика Экранного времени.

6.4.6. Advanced Data Protection в iCloud

В iOS 16.2 появился новый тип защиты облачных данных – Advanced Data Protection[44] в iCloud. При включении этой опции в настройках технология сквозного шифрования применяется и для таких данных, как резервные копии, фотографии в iCloud и другие:

- Device backup

[44] https://support.apple.com/guide/security/advanced-data-protection-for-icloud-sec973254c5f/web

- Messages backup
- iCloud Drive
- Notes
- Photos
- Reminders
- Safari bookmarks
- Siri Shortcuts
- Voice Memos
- Wallet passes

На сегодня Elcomsoft Phone Breaker не поддерживает извлечение и расшифровку таких данных. Работа над их поддержкой ведётся.

6.5. Что нужно для извлечения через облако

Требования к аутентификации учётной записи различаются в зависимости от типа контейнера.

– **резервные копии**: логин в Apple ID, пароль, второй фактор аутентификации (для учётных записей с 2FA);

– **синхронизированные данные**: логин в Apple ID, пароль, второй фактор аутентификации (для учётных записей с 2FA), **либо** маркер аутентификации macOS, использующийся на том же физическом компьютере;

– **iCloud Drive**: логин в Apple ID, пароль, второй фактор аутентификации (для учётных записей с 2FA), **либо** маркер аутентификации (только macOS, тот же физический компьютер);

– **сквозное шифрование**: логин в Apple ID, пароль, второй фактор аутентификации (всегда), код блокировки или пароль одного из доверенных устройств, зарегистрированных в учётной записи пользователя.

6.6. Получение пароля к Apple ID и кода двухфакторной аутентификации

Пароли к Apple ID можно извлечь из следующих источников:

– сохранённые пароли на компьютере пользователя в браузерах Chrome, Edge, Firefox, Opera: приложением Elcomsoft Internet Phone Breaker;

– сохранённые пароли на мобильных устройствах;

– сохранённые пароли в связке ключей macOS приложением Elcomsoft Password Digger;

– сохранённые пароли из iPhone: резервная копия с паролем либо низкоуровневый доступ;

Вторым фактором аутентификации является сам iPhone. Одноразовый код можно сгенерировать в настройках устройства без выхода в интернет:

– выберите «Настройки» > [имя пользователя];

– нажмите «Пароль и безопасность»;

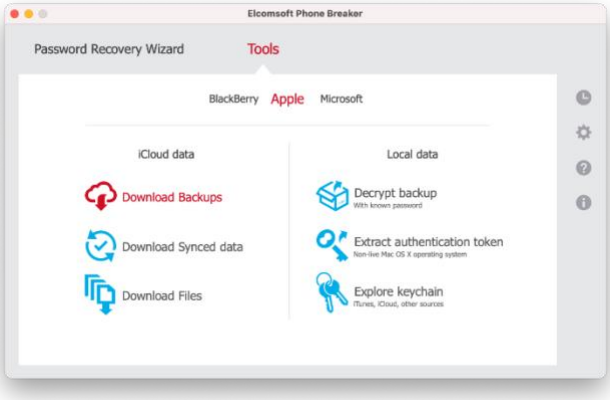
– появится сообщение «Информация об учетной записи недоступна». Нажмите «Получить код проверки».

Альтернативный способ получение проверочного кода – использование SIM-карты, соответствующей телефонному номеру, привязанному к учётной записи, для получения SMS.

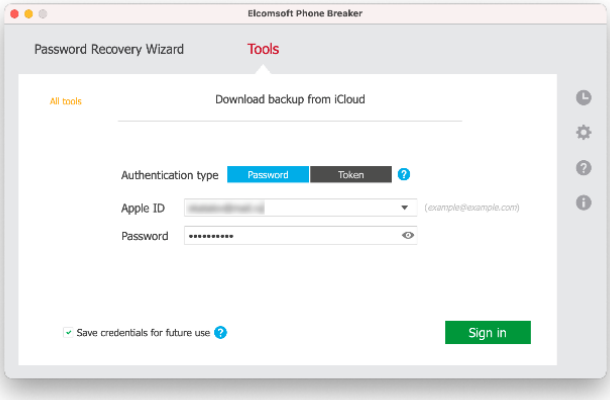
6.7. Облачное извлечение: пошаговая инструкция

Для извлечения данных из облака запустите Elcomsoft Phone Breaker и нажмите Apple. Из вкладки Download from iCloud выберите тип извлекаемых данных – резервные копии (Backups), файлы из iCloud Drive (Files), фотографии (Photos), облачную связку ключей (Keychain) или синхронизированные данные (Synced data), куда включены обычные данные и категории, защищённые сквозным шифрованием.

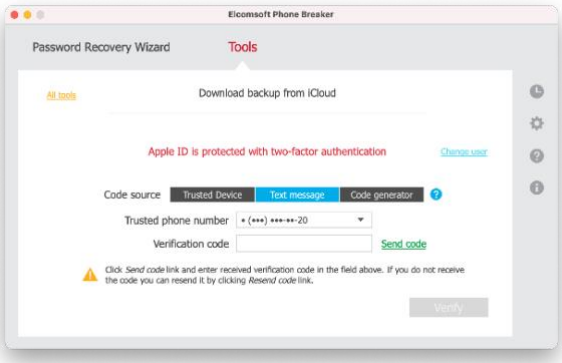
Пункт FileVault Recovery token позволяет извлечь депонированные ключи для разблокировки зашифрованных томов FileVault на компьютерах под управлением macOS.

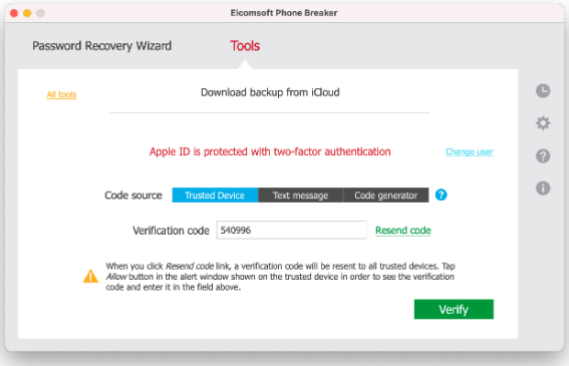


Авторизуйтесь в учётной записи пользователя.

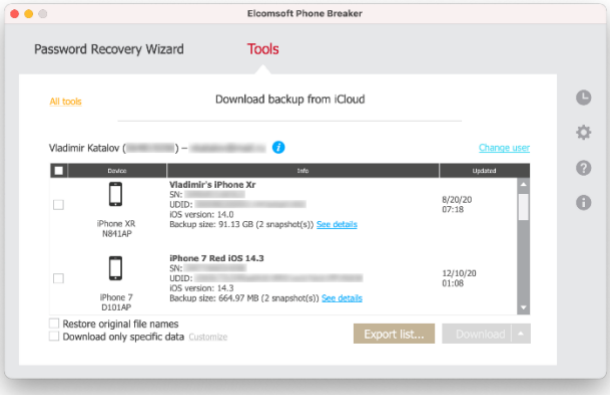


Пройдите проверку двухфакторной аутентификации.





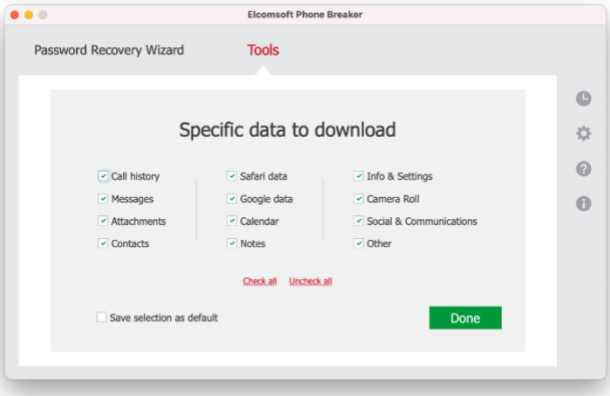
При скачивании облачных резервных копий будет выведен список доступных резервных копий. В список могут включаться до трёх последних резервных копий всех устройств пользователя.



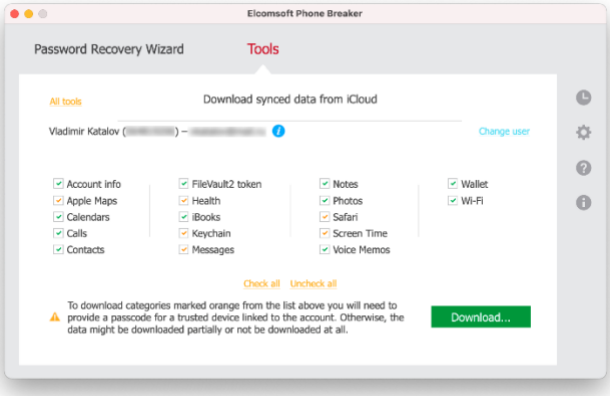
Опция Restore original file names декодирует оригинальные имена файлов, что повышает удобство анализа вручную. Если оставить эту опцию не выбранной, то резервная копия будет сохранена в стандартном формате iTunes; такие резервные копии могут быть открыты в множестве криминалистических продуктов, включая Elcomsoft Phone Viewer.

При необходимости вы можете отметить опцию частичного скачивания данных Download only specific data. В этом случае на следующем шаге вам будет предложено выбрать категории данных, которые будут скачаны. Эта опция позволяет сэкономить время, быстро извлекая самые важные данные. Обратите внимание, что при этом опция

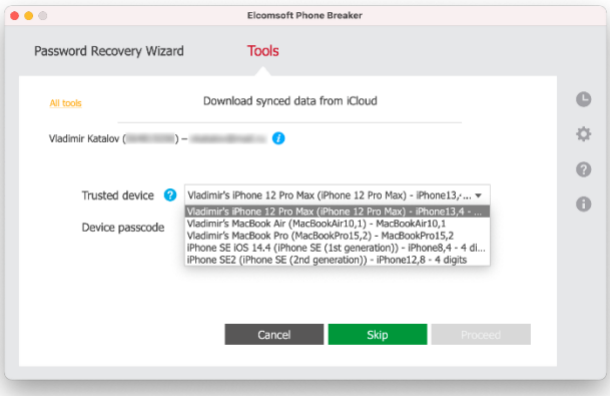
«Restore original file names» включится автоматически и не может быть выключена для частичного скачивания.



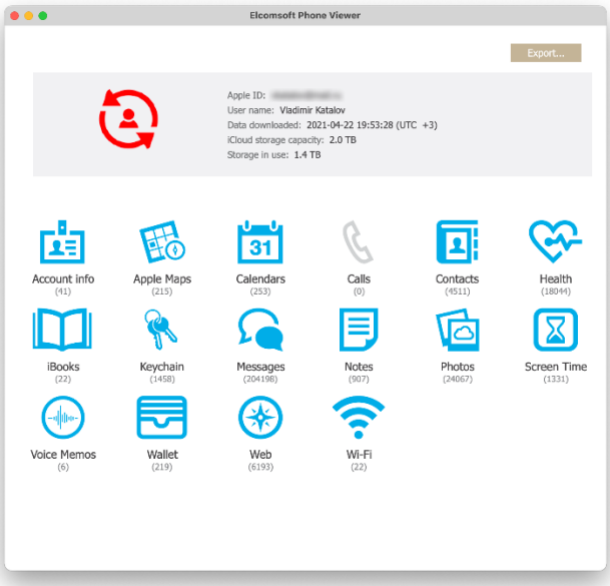
При скачивании синхронизированных данных отметьте категории, которые будут извлекаться.



Оранжевым цветом выделены данные, зашифрованные сквозным шифрованием; для доступа к этим данным потребуется пройти дополнительный шаг – ввод пароля или кода блокировки экрана одного из доверенных устройств пользователя.



После скачивания данные можно открыть для анализа в Elcomsoft Phone Viewer:



6.8. Маркеры аутентификации

Маркеры аутентификации используются для удобства повторного входа в учётную запись без ввода логина и пароля. Файлы с маркерами (токенами) аутентификации сохраняются на Mac или PC в виде файлов. Использование таких файлов теоретически может позволить обойти аутентификацию по логину/паролю и дополнительную проверку 2FA.

6.8.1. Ограничения

Практическая ценность маркеров аутентификации в настоящее время сильно ограничена. Если в прошлом можно было использовать для доступа к резервным копиям и другим категориям данных актуальные маркеры, извлечённые из компьютеров с Windows или macOS, то сегодня ограниченной ценностью обладают лишь маркеры, извлечённые из macOS, причём использовать их необходимо на том же самом физическом компьютере, из которого они были извлечены. С их помощью можно получить доступ к синхронизированным данным и данным iCloud Drive. Резервные копии и зашифрованные контейнеры доступны исключительно с полным циклом аутентификации.

Важно:

– маркеры аутентификации можно использовать только для доступа к синхронизированным данным и iCloud Drive;

– только при извлечении из компьютера с macOS;

– только на том же самом физическом компьютере (не виртуальной машине и не другом компьютере с macOS.

6.8.2. Извлечение

Если у пользователя был изъят компьютер под управлением macOS с аутентифицированной пользовательской сессией либо с известным паролем root, вы сможете извлечь и использовать (на том же компьютере) маркеры аутентификации.

Подробно об извлечении маркеров аутентификации можно прочитать в руководстве пользователя для Elcomsoft Phone Breaker.

Для извлечения маркера из системы с активной пользовательской сессией используйте утилиту командной строки Elcomsoft Apple Token Extractor (atex.dmg). Этот инструмент поставляется вместе с EPB (файл **atex.dmg**). Вы можете найти его в папке установки EPB.

Чтобы извлечь маркер аутентификации для текущего пользователя iCloud, выполните следующие действия:

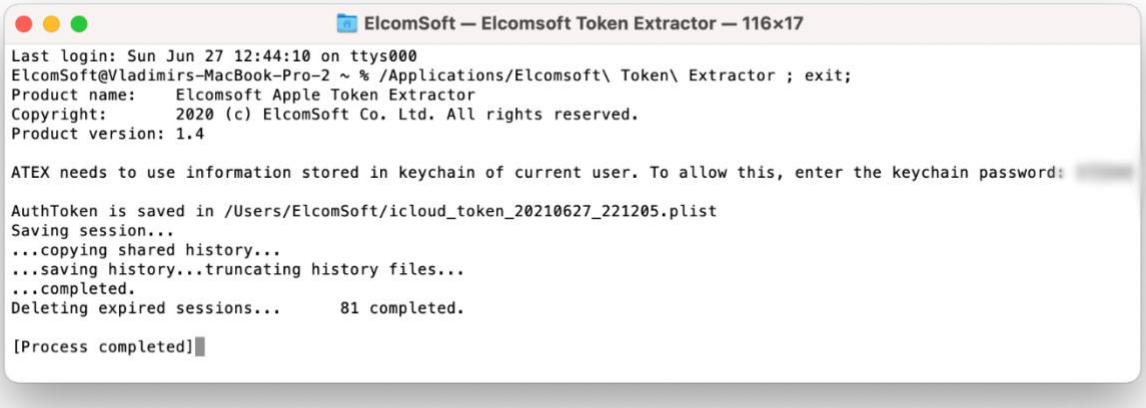
1. Запустите файл atex.dmg.

2. Скопируйте файл atex из смонтированного образа в папку, в которой вы хотите сохранить файл с токеном аутентификации.

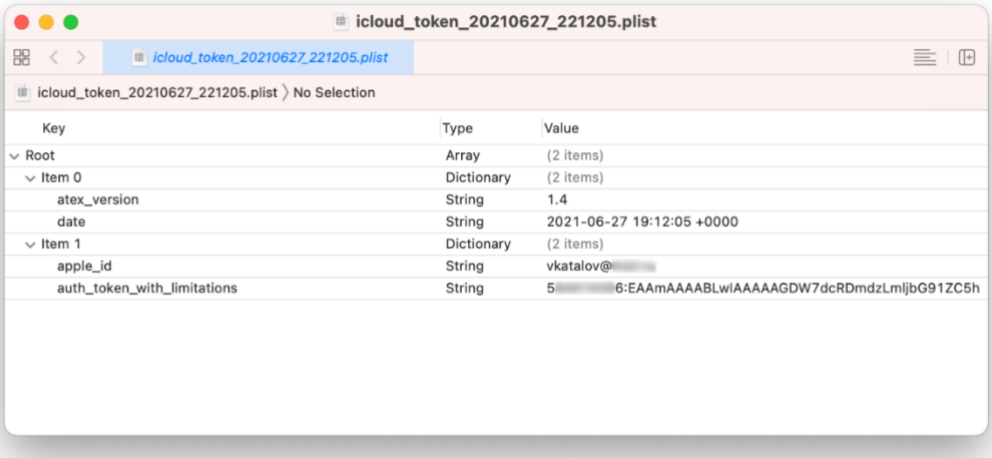
3. Откройте папку с файлом atex.

4. Запустите файл atex. Будет создан файл "icloud_token_<timestamp>.plist", который сохраняется в папке Users/<имя_текущего_пользователя>.

В открывшемся терминальном окне вы увидите полный путь к созданному файлу.



5. Файл "icloud_token_<timestamp>.plist" содержит маркер аутентификации текущего пользователя iCloud.



Чтобы извлечь маркер аутентификации для другого пользователя iCloud, выполните следующие действия:

1. Запустите atex.dmg.

2. Скопируйте файл atex из смонтированного образа в папку, в которую будет сохранён маркер аутентификации.

3. Откройте окно терминала.

4. Перейдите в папку с файлом atex.

5. Просмотреть список всех пользователей iCloud можно командой sudo atex -l or sudo atex --iCloudUserList

6. sudo используется для эскалации привилегий до root пользователя.

7. Введите пароль пользователя root.

8. Будет выведен список пользователей iCloud.

9. Для извлечения маркера запустите команду sudo atex --getToken -u <username> -p <password>

10. Пример: sudo atex --getToken -u mary -p 1234

11. Будет создан файл "icloud_token_<timestamp>.plist", сохраняемый в том же каталоге, откуда был запущен atex.
В открывшемся окне Терминала вы увидите полный путь к созданному файлу.

12. Файл "icloud_token_<timestamp>.plist" содержит маркер аутентификации текущего пользователя iCloud.

Параметры командной строки утилиты atex:

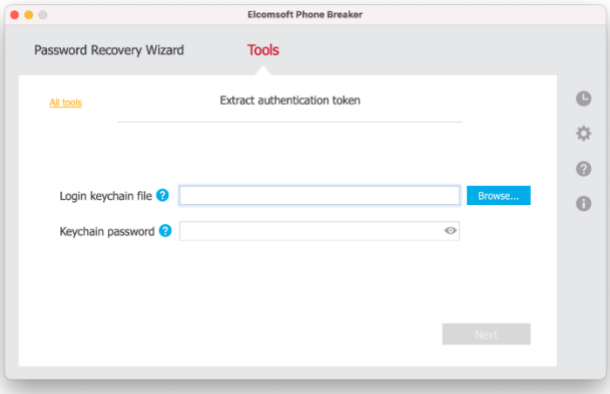
Параметр	Значение
-h или [--help]	Отображает справочное сообщение
-l или [--iCloudUserList]	Отображает список пользователей iCloud
--getToken -u <username> -p <password>	Извлекает маркер аутентификации для указанного пользователя. Имя пользователя и пароль следует вводить без скобок.
-u или [--username]	Имя пользователя. Имя пользователя следует вводить без скобок.

-p или [--password]	Пароль пользователя. Пароль следует вводить без скобок.

Альтернативный способ извлечения маркера аутентификации – через пользовательский интерфейс Elcomsoft Phone Breaker. Этот способ доступен только для извлечения маркеров из неактивной копии macOS, например, путём монтирования образа диска операционной системы, в которой хранится маркер.

Чтобы извлечь маркер аутентификации iCloud, сделайте следующее:

1. Смонтируйте образ диска, содержащий маркер аутентификации.
2. Запустите Elcomsoft Phone Breaker.
3. В меню **Tools** выберите вкладку **Apple**.
4. Нажмите Extract authentication token.



5. Укажите путь и пароль к файлу, содержащему маркер аутентификации:

a. **Login keychain file**: Введите путь к файлу login.keychain пользователя, маркер которого вы расшифровываете. По умолчанию он хранится в */Users/<user name>/Library/Keychains/login.keychain*.

b. **Keychain password**: Пароль к выбранному login.keychain.

6. Нажмите **Next**.
7. На следующей странице укажите путь к файлу, содержащему маркер аутентификации. По умолчанию **/Users/<имя пользователя>/Library/Application Support/iCloud/Accounts/**. Имя этого файла представляет собой числовое представление Apple ID пользователя в виде 6-10 цифр.
8. Apple ID пользователя отображается в верхней части экрана.
9. Нажмите **Extract**.
10. Маркер аутентификации извлекается.
11. Нажмите **Save token** для сохранения строки в файл в формате *.plist.

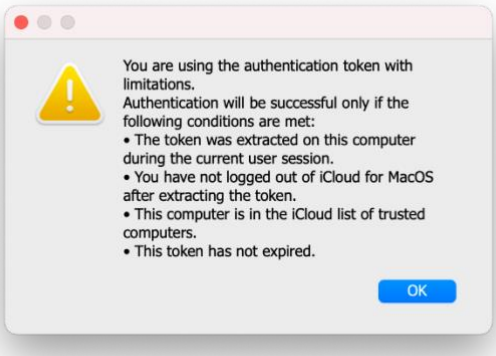
Извлечённый маркер можно использовать для аутентификации в iCloud.

6.8.3. Авторизация с использованием маркеров аутентификации

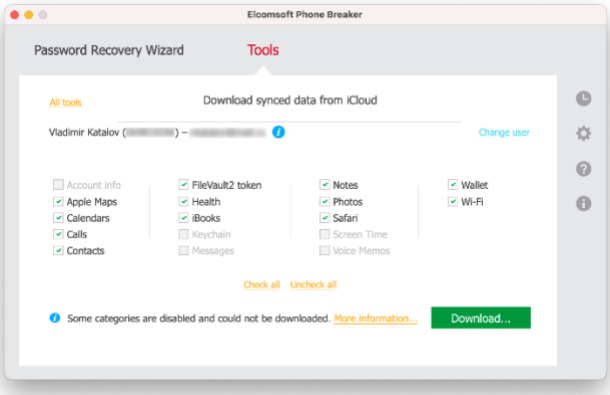
Использовать маркеры аутентификации так же просто, как и стандартную аутентификацию по логину и паролю. Для этого в окне скачивания синхронизированных

данных выберите аутентификацию по маркеру (Token) вместо логина и пароля. Укажите путь к файлу маркера.

Программа отобразит предупреждение, в котором перечислены описанные ранее ограничения в использовании маркеров:



При использовании маркеров аутентификации к некоторым категориям данных доступ получить невозможно. Недоступные для скачивания категории будут отображены серым цветом, а соответствующие пункты будут неактивны.



7. Извлечение данных: низкоуровневый анализ

Для всех устройств Apple, оборудованных 64-разрядным процессором и подсистемой безопасности Secure Enclave, низкоуровневый доступ позволяет извлечь полный образ файловой системы и расшифровать связку ключей. Для сравнения: методы физического извлечения, которые использовались в устаревших 32-разрядных устройствах, позволяли извлечь и расшифровать образ раздела данных целиком. При этом расшифровать содержимое блоков данных, в которых хранились удалённые файлы, как было невозможно для 32-разрядных устройств, так и осталось невозможным для современных.

7.1. Способы низкоуровневого анализа и различия между ними

Можно выделить **три основных способа** низкоуровневого анализа:

– агент-экстрактор;

– джейлбрейк (в том числе джейлбрейк checkra1n);
– уязвимость загрузчика.

7.1.1. Агент-экстрактор

Использование агента-экстрактора позволяет извлекать данные из iPhone без джейлбрейка. Агент-экстрактор не модифицирует пользовательские данные и демонстрирует высокую скорость, надёжность и совместимость, сводя к нулю риск приведения устройства в неработоспособное состояние.

– **агент-экстрактор** – самый простой, безопасный и достаточно чистый с криминалистической точки зрения способ.

Достоинства:

– прост в использовании;
– безопасен;
– достаточно чист с криминологической точки зрения;
– поддерживает все поколения устройств.

Недостатки:

– требуется подключение устройства к интернету (за исключением старых учётных записей разработчиков);
– ограниченная поддержка версий iOS (требуется наличие эксплойта уровня ядра).

7.1.2. Джейлбрейк

Установка джейлбрейка – достаточно рискованный процесс. После выхода агента-экстрактора в использовании публичных джейлбрейков практически не осталось смысла. Джейлбрейк модифицирует системный раздел и раздел данных; полностью удалить установленный джейлбрейк возможно не всегда. Даже после удаления джейлбрейка устройство может сбоить, а системные обновления могут не устанавливаться. Джейлбрейк может оставаться единственным способом низкоуровневого доступа в единичных случаях.

Джейлбрейк – рискованный и способ доступа, который стоит использовать только в ситуациях, когда другие методы недоступны.

Достоинства:

– Иногда является единственным доступным способом.

Недостатки:

– Риск выхода устройства из строя;
– Модифицируется системный раздел и раздел данных;
– Невозможно бесследное удаление;
– Возможны перебои с функционированием устройства после удаления джейлбрейка.

7.1.3. Уязвимость загрузчика

Извлечение с использованием уязвимости загрузчика **checkm8** – в реализации «Элкомсофт» единственный идеально чистый с криминалистической точки зрения

метод. Извлечение посредством эксплойта загрузчика использует уязвимость в коде загрузчика ряда устройств Apple. Apple удалось усложнить работу эксплойта на моделях iPhone 8/8 Plus/iPhone X под управлением iOS 14 и 15, сделав невозможным извлечение в режиме BFU. Кроме того, для этих моделей и версий iOS невозможно начать извлечение, если на устройстве установлен непустой код блокировки экрана, а в случае с iOS 16 извлечение через эксплойт загрузчика для iPhone 8/8 Plus/iPhone X и вовсе сработает лишь в исключительных случаях, когда на устройстве с момента начальной настройки ни разу не был установлен код блокировки экрана.

Метод доступен для устройств поколений iPhone 5s, 6, 6 Plus, 6s, 6s Plus, iPhone SE, iPhone 7 и 7 Plus, а также и совместимых моделей iPad, для которых была обнаружена уязвимость в коде загрузчика. Через уязвимость загрузчика можно получить доступ к данным и для более старых устройств – iPhone 4, 4s, 5 и 5c, для которых можно в том числе подобрать код блокировки экрана (для более современных моделей эта функция недоступна).

Прямое извлечение с использованием **checkm8** – идеально чистый с криминалистической точки зрения способ с ограниченной совместимостью, технически сложный в использовании

Достоинства:

- безопасен;
- идеально чист с криминологической точки зрения;
- не оставляет никаких следов использования;
- не загружает установленную на устройстве копию iOS;
- поддерживает все версии iOS.

Недостатки:

- потребуется скачать файл прошивки, соответствующей установленной версии iOS
- ограниченная поддержка устройств: современные модели не подвержены уязвимости

7.2. Для чего нужен код блокировки экрана

Большая часть пользовательских данных хранится в устройствах с iOS в зашифрованном виде, а ключи шифрования защищены. При включении устройства запрашивается код блокировки экрана. Введённый пользователем код используется сопроцессором безопасности Secure Enclave для генерации ключа, при помощи которого расшифровываются ключи, которыми зашифрованы файлы в устройстве. Данные отпечатков пальцев и сканера Face ID не могут быть использованы для генерации ключей шифрования; при включении или после перезагрузки устройства разблокировать его можно исключительно кодом блокировки.

Для использования всех перечисленных способов низкоуровневого доступа потребуется ввести код блокировки экрана, если он не пуст.

7.3. Способ 1: использование агента-экстрактора

Доступ к файловой системе и Связке ключей на iPhone невозможен без эскалации привилегий, для чего в ранних версиях iOS Forensic Toolkit использовался джейлбрейк.

В сравнении с другими методами агент-экстрактор демонстрирует высокую скорость, надёжность и совместимость.

Агент-экстрактор использует уязвимости на уровне ядра iOS, позволяющие организовать прямой доступ к файловой системе, извлечь и расшифровать записи из связки ключей. По объёму и детализации полученных данных этот способ не отличается от других низкоуровневых методов анализа, но, в отличие от них, не модифицирует системный раздел устройства и не имеет сопутствующих рисков, которые могли бы привести к отказу устройства. На пользовательском разделе привносимые изменения минимальны и не затрагивают реальные пользовательские данные. После работы агента-экстрактора добавятся только записи в некоторых системных журналах, отражающие события установки, запуска и удаления агента.

7.3.1. Совместимость и требования

Для загрузки агента-экстрактора на устройство необходима учётная запись Apple ID:

– обычная учётная запись (устройству потребуется предоставить доступ в интернет) с привязанным к ней доверенным устройством (для прохождения двухфакторной аутентификации);

– код блокировки экрана должен быть известен или не установлен;

– при работе с устройствами под управлением iOS 16 необходимо после установки агента включить режим разработчика Settings > Privacy & Security > Developer Mode, после чего перезагрузить устройство.

Использование обычной учётной записи требует подтверждения сертификата на самом устройстве, для чего потребуется подключение к сети, связанное с рядом сопутствующих рисков.

Список поддерживаемых агентом-экстрактором моделей устройств не ограничен; ограничения связаны с версиями iOS. На странице продукта[45] доступен актуальный список совместимых систем.

7.3.2. Учётная запись Apple ID для установки сторонних приложений

Каждое приложение, которое устанавливается на устройство под управлением iOS, iPadOS или TvOS, должно быть подписано. В отличие от других операционных систем, в iOS цифровая подпись уникальна для каждого устройства. Для того, чтобы установить на iPhone агент-экстрактор, его понадобится подписать.

Для подписи используются учётные записи Apple ID. С этой целью можно использовать как обычную учётную запись, так и учётную запись разработчика. После установки приложения под обычной учётной записью (не участвующей в программе для разработчиков), нужно дополнительно зайти в Settings > General > Device Management и подтвердить сертификат установленного приложения. Верификация происходит на сервере ppq.apple.com. Этот дополнительный шаг нужен для того, чтобы система могла

[45] https://www.elcomsoft.ru/eift.html

запустить приложение. Обратная сторона — устройству нужен будет доступ в сеть, что может привести к нежелательным последствиям.

7.3.3. Установка iOS Forensic Toolkit

Установка EIFT на компьютеры под управлением Windows не требуется: приложение доступно в виде портативной версии, и может запускаться из любой папки как со встроенного, так и с внешнего накопителя.

Установка редакции для Linux отличается от процедуры для компьютеров с Windows или macOS. Для установки с инструментария на компьютер с Linux нужно распаковать архив с паролем, ссылка на который предоставляется зарегистрированным пользователям, и перейти в папку с продуктом. После чего из папки, в которую установлен EIFT, нужно выполнить следующую команду, которая скачает и установит необходимых библиотеки:

```
sudo apt install ./com.elcomsoft.eift-dependency.deb
```

Обратите внимание: для скачивания библиотек компьютер должен быть подключён к интернету.

Установка версии для macOS прозрачна, однако для macOS потребуется выдача дополнительных прав. Если этого не сделать, при попытке запустить EIFT на компьютере возникают ошибки «недостаточно прав доступа».

Причин возникновения этой ошибки может быть несколько:

– не выполнена команда xattr, как это описано в документации;
– зайти в терминал;
– перейти в папку со скриптом установленного файрволла;
– выполнить команду (точка в конце обязательна): sudo xattr -d com.apple.quarantine;
– исполняемый код находится на рабочем столе;
– перенести EIFT в другое место, например, в локальный applications;
– не выданы права полного доступа shell к диску;

Выдать права доступа следующим образом:

– выбрать System Preferences->Security & Privacy->Full Disk Access;
– кликнуть на иконку «замок», чтобы разблокировать возможность изменений;
– нажать ‘+’;
– нажать комбинацию кнопок ‘cmd + Shift + .’ для отображения скрытых файлов;
– выбрать путь /bin/sh.

7.3.4. Установка агента-экстрактора

Если уже установлен агент предыдущей версии, перед началом работа его необходимо удалить. Это можно сделать непосредственно с домашнего экрана iPhone.

Во время установки агента аппарат должен быть разблокирован, а доверенные отношения с компьютером должны быть установлены (для этого потребуется подтвердить на устройстве код блокировки экрана). В процессе извлечения рекомендуется использовать порт USB 3.0, особенно для новых устройств.

При установке агента будет запрошен Apple ID и пароль; также нужно будет пройти двухфакторную аутентификацию, для чего крайне рекомендуется использовать доверенное устройство, привязанное к используемой учётной записи.

Внимание: при работе с устройствами под управлением iOS 16 необходимо после установки агента включить режим разработчика Settings > Privacy & Security > Developer Mode, после чего перезагрузить устройство.

Внимание: перед установкой агента необходимо установить отношение доверия между устройством и компьютером.

Перед началом работы **убедитесь в выполнении следующих требований:**

- **Дата и время на компьютере, выход в интернет:** убедитесь, что дата и время на вашем компьютере соответствуют актуальным. Кроме того, убедитесь, что компьютер имеет выход в интернет.
- **Привязка до установки агента:** убедитесь, что доверенные отношения (привязка устройства к компьютеру) установлены до установки агента.
- **Кабель USB-C:** рекомендуем использовать кабель с коннектором USB Type-C. Тип кабеля не особо критичен в процессе установки и подписи агента, но важен для последующего извлечения.

Подготовка устройства

Перед тем, как приступить к установке агента, убедитесь, что устройство имеет достаточный уровень заряда и корректные настройки даты и времени.

- **Проверьте дату и время на телефоне**: дата и время на телефоне должны совпадать с актуальными. Если это не так, измените дату и время вручную в настройках устройства. Это необходимо для корректной установки агента и проверки цифровой подписи.

На следующем шаге установите приложение агента на устройство - **но пока не запускайте его.**

- **Установите агент-экстрактор** (не запускайте его)

Для установки агента вызовите следующую команду:

./EIFT_cmd agent install

Вам потребуется ввести e-mail и пароль от Apple ID. Если ваш аккаунт привязан к организации, то EIFT попросит уточнить, какой именно аккаунт использовать: индивидуальный или корпоративный. Если у вас есть доступ к платному аккаунту разработчика, то для установки агента предпочтительнее использовать его, так как при этом не потребуется интернет-соединения.

В случае с бесплатным аккаунтом для проверки сертификата потребуется интернет-соединение, что является нежелательным при извлечении данных с устройства.

Если для учётной записи включена двухфакторная аутентификация, то вам также может потребоваться ввести одноразовый код, полученный либо через SMS, либо через доверенное устройство.

Пароль от учётной записи будет отличаться в зависимости от того, какая операционная система установлена на вашем компьютере. На компьютере с Windows

вам потребуется указать так называемый пароль приложений, который нужно предварительно создать в учётной записи Apple ID. В macOS всегда указывается обычный пароль от Apple ID, после чего необходимо пройти двухфакторную авторизацию через доверенное устройство или SMS.

- **Перезагрузите телефон:** осуществите штатную перезагрузку телефона (штатное отключение и перезагрузка).

Для чего нужна перезагрузка: если вы установите и запустите приложение агента-экстрактора, не перезагрузив предварительно телефон, то в случае возникновения ситуации kernel panic и спонтанной перезагрузки устройства могут возникнуть повреждения файловой системы, после чего операционная система откатит файловую систему в "чистое" состояние. В результате отката могут пропасть записи сопряжения телефона и/или повредиться уже установленное приложение агента-экстрактора, что, в свою очередь, потребует его переустановки.

Настройки и файрволл

В зависимости от типа учётной записи Apple ID, которая используется для подписи приложения агента, перед запуском агента может понадобиться верифицировать цифровую подпись приложения. Для этого устройству необходимо связаться с сертифицирующим сервером Apple, для чего, в свою очередь, устройству потребуется доступ в интернет. Выход в интернет несёт сопутствующие риски, которые желательно уменьшить, использовав аппаратный или программный файрволл.

Внимание: этот раздел относится к ситуации, когда для запуска агента требуется подтвердить цифровую подпись. При использовании некоторых видов учётных записей разработчика проверка не нужна; в таком случае пропустите этот раздел.

– **Подключите устройство к программному или аппаратному файерволлу**

  - Физически подключите устройство к программному или аппаратному (Raspberry Pi or Orange Pi) файрволлу.

– **Проверьте цифровую подпись приложения агента**

  - Откройте настройки и перейдите в пункт "Настройки -> Основные -> VPN и управление устройством."
  - Проверьте цифровую подпись агента. Не запускайте приложение агента-экстрактора; на этом шаге проверяется подпись приложения.

– **Перезапустите телефон (второй раз): снова перезапустите телефон штатным образом.**

– **Запустите приложение агента на телефоне**

  - Коснитесь иконки установленного на телефон приложения агента-экстрактора, чтобы запустить его. Если появится запрос на включение режима разработчика, см. следующие шаги.

– **Включите режим разработчика (если он будет запрошен)**

  - Перейдите "Настройки -> Конфиденциальность и безопасность -> Режим разработчика."

- Включите режим разработчика (может потребоваться очередная перезагрузка телефона).

– **Убедитесь, что режим разработчика активирован (если он был запрошен):**

- После перезагрузки, снова перейдите в настройки режима разработчика и убедитесь, что этот режим активирован.

На этом этапе приложение **агента можно запустить.**

– запустите приложение агента, коснувшись его иконки на телефоне.

– отключите устройство от файрволла (если он использовался) и подключите к компьютеру.

– если вы использовали аппаратный файрволл, отключите от него телефон и подключите к компьютеру.

– запустите EIFT и следуйте инструкциям из руководства по эксплуатации.

– на компьютере запустите iOS Forensic Toolkit.

7.3.5. Особенности установки агента-экстрактора

При использовании обычных учётных записей и учётных записей разработчика, зарегистрированных в программе Apple Developer после 6 июля 2021, необходимо подтвердить цифровую подпись агента извлечения на исследуемом iPhone, для чего требуется подключить телефон к Интернету.

При работе с устройствами под управлением iOS 16 необходимо перед установкой агента включить режим разработчика Settings > Privacy & Security > Developer Mode. Будет запрошен код блокировки экрана, который необходимо будет ввести.

Влияние спонтанных перезагрузок на целостность файловой системы

Нештатные перезагрузки (ошибка device panic) могут привести к повреждениям файловой системы. Чтобы восстановить её целостность, операционная система может откатить файловую систему к предыдущему состоянию.

Влияние отката файловой системы на работу агента-экстрактора

Результатом отката файловой системы может стать неработоспособность агента и/или исчезновение ранее установленной привязки к компьютеру. Избежать этой ситуации помогут промежуточные штатные перезагрузки устройства.

Переустановка агента

Если ситуация с откатом файловой системы всё же возникла, вам может потребоваться заново привязать устройство к компьютеру и/или переустановить агента.

7.3.5.1. Риски при установке агента-экстрактора

При использовании обычной учётной записи Apple ID, не зарегистрированной в программе Apple для разработчиков или зарегистрированной после 6 июля 2021, процесс установки агента-экстрактора требует подтверждения цифрового сертификата, которым подписано устанавливаемое приложение. Для подтверждения сертификата, в свою очередь, исследуемому устройству необходимо подключиться к серверу Apple.

Упомянем очевидные вещи – автоматическую синхронизацию данных на устройстве (нарушается неизменность улик) и ненулевой риск дистанционной

блокировки и/или стирания устройства через приложение Локатор. Риск можно свести к допустимому минимуму, ограничив подключение на устройстве набором адресов, который требуется для проверки сертификата.

При помощи обычных Apple ID можно загружать приложения (в том числе агента-экстрактора) только с компьютеров с macOS, при этом в учётной записи обязательно должно присутствовать ранее зарегистрированное доверенное устройство. Это — не единственное ограничение: вам потребуется верифицировать цифровую подпись загруженного приложения в режиме онлайн. Риски очевидны: удалённая блокировка или сброс устройства, нежелательная синхронизация данных.

Наконец, последнее ограничение: обычные учётные записи можно использовать для подписи не более трёх устройств в неделю. Обойти это ограничение легко: достаточно создать новый Apple ID (не забывайте о требовании привязки к доверенному устройству!)

7.3.5.2. Программа Apple для разработчиков

Зарегистрированным разработчикам доступен штатный способ установки приложений, минующий App Store. Для того, чтобы считаться разработчиком, нужно зарегистрироваться в программе Apple для разработчиков по следующей ссылке: Enrollment – Support – Apple Developer[46]

Альтернативный способ регистрации – через приложение Apple Developer на iPhone или iPad: Enrolling and Managing your Account in the Apple Developer App – Support – Apple Developer[47]

Заявка подаётся либо от лица индивидуального разработчика, либо от лица организации. В прошлом персональные учётные записи и учётные записи организаций были функционально идентичны, однако в последнее время Apple ограничила индивидуальных разработчиков таким образом, что они могут загружать на iPhone приложения только с компьютеров Mac. Учётные записи организаций не имеют таких ограничений и могут использоваться для загрузки приложений с компьютеров macOS или Windows.

Ещё раз отметим, что в настоящий момент регистрация в программе Apple для разработчиков более не несёт преимуществ для установки агента-экстрактора.

7.3.5.3. Ограничение на количество устройств

Оба типа учётных записей позволяют регистрировать в программе по сто устройств каждого типа в год (например, сто iPhone, сотню iPad, ещё сто Apple TV и т.д.). Удаление ранее зарегистрированного устройства не сбрасывает счёт; лимит сбрасывается автоматически на ежегодной основе. В результате этого ограничения вы сможете загружать агент не более чем на сто устройств в год для каждого Apple ID, зарегистрированного в программе разработчика. После первых десяти устройств возникнет задержка, и регистрация каждого нового устройства будет обрабатываться до 72 часов. Причины этого нам неизвестны; вряд ли дело в том, что Apple хотят помешать работы криминалистов.

[46] https://developer.apple.com/support/enrollment/
[47] https://developer.apple.com/support/app-account/

7.3.5.4. Снижение рисков при использовании обычных учётных записей

Как упоминалось выше, при использовании Apple ID, не зарегистрированного в программе для разработчиков, при установке агента-экстрактора необходимо верифицировать цифровой сертификат подписи на телефоне. Это, в свою очередь, требует выхода телефона в Интернет со всеми сопутствующими последствиями. Для снижения сопутствующих рисков необходимо ограничить подключение; в идеале iPhone должен иметь возможность подключаться только к узлу проверки сертификатов и ни к чему больше. Более того; выход в сеть потребуется при первом запуске агента-экстрактора даже в случаях, когда использовалась учётная запись разработчика, зарегистрированная позднее 6 июля 2021 года.

7.3.5.4.1. Способ 1: программный

Внимательно ознакомьтесь с инструкциями ниже и в точности следуйте им. Не забывайте использовать дополнительное устройство и обязательно отключайте USB Sharing на исследуемом устройстве перед тем, как продолжить работу.

Перед началом работы скачайте и распакуйте скрипт по ссылке. Вам предварительно понадобится дать скрипту права на выполнение (команда *chmod +x {пусть к скрипту}*) и снять карантин (*xattr -d com.apple.quarantine {пусть к скрипту}*).

Этап 1. Подготовка целевого аппарата

1. Отключить на целевом аппарате все сетевые подключения.
2. (mac os) Проверить, что USB Sharing отключён.
3. Подключить целевой аппарат и провести установку агента.
4. Отключить целевой аппарат.

Этап 2. Подпись агента на целевом аппарате

1. Отключить на тестовом аппарате и целевом аппарате все сетевые подключения
2. (mac os) Настроить и включить USB Sharing
3. Запустить *sudo ./install_firewall.sh* из консоли, предварительно перейдя в папку со скриптом
4. Подключить тестовый аппарат кабелем к компьютеру
5. Дойти до режима проверки аппарата в скрипте, чтобы один хост открывался, другой нет
6. Подтвердить успешность блокировки хостов
7. Проверить "окно" времени изменения IP адреса, желательно дождаться момента, когда это окно станет в диапазоне 200-300 секунд
8. Отключить тестовый аппарат
9. Подключить целевой аппарат
10. На целевом аппарате пройти проверку подписи уже установленного агента
11. Отключить целевой аппарат
12. Выйти из скрипта кнопкой Q
13. На компьютере (mac os) выключить USB Sharing

Рассмотрим процесс в деталях.

Во-первых, скачайте скрипт по ссылке:

https://www.elcomsoft.com/download/firewall.zip

Важно: убедитесь в точности установки времени и даты на телефоне! Если время на аппарате не соответствует реальному, цифровая подпись не будет верифицирована!

Далее следуйте инструкции.

НЕ ГАРАНТИРУЕТСЯ, что Apple не изменит работу учётных записей и ваша учётная запись не будет заблокирована в дальнейшем. Скрипт блокирует только TCP пакеты. В любой момент разработчики Apple могут внести изменения, которые могут привести к любым отклонениям в работе скрипта. Мы настоятельно рекомендуем использовать Apple Developer Account как единственно безопасный способ!

Скрипт не поможет, если на телефоне включена функция Private Relay. Отключите её в настройках. Также убедитесь, что на телефоне не включены VPN-сервисы.

Результат исполнения зависит от того, насколько вы внимательны в процессе работы со скриптом. Скрипт должен быть запущен все время, пока вы работаете с устройствами.

Вам понадобится одно дополнительное устройство, для настройки этого скрипта.

Ни в коем случае нельзя использовать скрипт без дополнительного устройства, это может привести к Remote Device Lock/Wipe, поскольку на момент инсталляции файрвола устройство будет выпущено в интернет без ограничений!

Инструкция по использованию:

1. Настраиваем USB Internet Sharing для нужного порта (обычно это USB iPhone или USB iPad, в зависимости от устройства)

2. Запускаем скрипт:

sudo ./install_firewall.sh

У вас попросят подключить **тестовое устройство**, поскольку это необходимо для того, чтобы в системе появился необходимый интерфейс.

3. Подключаем **тестовое устройство**. На устройстве должны быть отключены все сетевые интерфейсы (BlueTooth, WiFi, Cell) и подтверждаем нажатием любой клавиши (например пробел).

После чего скрипт анализирует окружение системы, находит нужные для вас IP адреса (они могут быть разными и различаться каждый раз от запуска к запуску!), формирует правила файрвола и реконфигурирует его.

Результатом работы должен быть такой вывод данных:

```
No ALTQ support in kernel
ALTQ related functions disabled
No ALTQ support in kernel
ALTQ related functions disabled
pf enabled
```

Это означает, что правила файрвола инсталлировались успешно.

4. После этого вам будет предложено проверить, что на вашем аппарате все работает. Запустите Safari и проверьте:

Попытайтесь открыть хост www.elcomsoft.com, должны получить результат о неудаче – хост недоступен.

Попробуйте открыть хост ppq.apple.com, хост должен быть доступен и ответить Ok.

5. Подтверждаем запрос, что у нас все прошло ОК

6. С этого момента у нас будет выведено, какой IP адрес критичный обнаружен, и сколько у нас есть времени до того момента, когда он изменится

```
      IP detected as 17.171.47.86/32,
IP will be valid for 59 sec.
press [Q] key to interrupt firewall
```

Если это значение находится в рамках менее 30 секунд, то рекомендуется подождать, пока это время истечет, скрипт обнаружит другой IP адрес и время на операцию станет равным 300 или чуть меньше.

7. Можно подключать **исследуемый аппарат** и проходить проверку подписи. За один раз это может не получиться, аппарат может ругнуться, что это не удалось. Не страшно, пробуем еще раз – и вуаля, все прошло на ура.

8. Обязательно отключите исследуемый аппарат и нажимаем кнопку Q. Скрипт автоматически восстановит предыдущие настройки файрвола и завершится.

Если же вы его прервали по нажатию кнопок Ctrl+C, то восстановить предыдущие значения файрвола можно запуском скрипта:

```
sudo ./uninstall_firewall.sh
```

Помните, что всё, что вы делаете, вы делаете на свой страх и риск. Мы не знаем, какие изменения может привнести Apple в любой момент времени.

9. Перед тем, как продолжить работу, обязательно зайдите в настройки и **отключите USB Sharing**.

7.3.5.4.2. Способ 2: с использованием Raspberry Pi

Ещё один способ обезопасить соединение – использовать специальную прошивку для Raspberry Pi 4 или подобного одноплатного микрокомпьютера (см. раздел Дополнительные материалы), превращающую устройство в функциональный файрволл, который позволяет верифицировать цифровую подпись агента, блокируя попытки доступа подключённого iPhone к интернету.

С целью упростить и обезопасить процесс мы разработали прошивку, которая превращает микрокомпьютер Raspberry Pi 4 в функциональный файрволл. Его использование максимально просто: одним проводом Pi подключается к роутеру, другим — к телефону, после чего на iPhone возникает защищённое соединение.

Прошивку можно найти в нашем репозитории на github (проект eiftpi[48]).

Дополнительное оборудование

Для настройки файрволла и подключения к нему iPhone вам потребуется дополнительное оборудование:

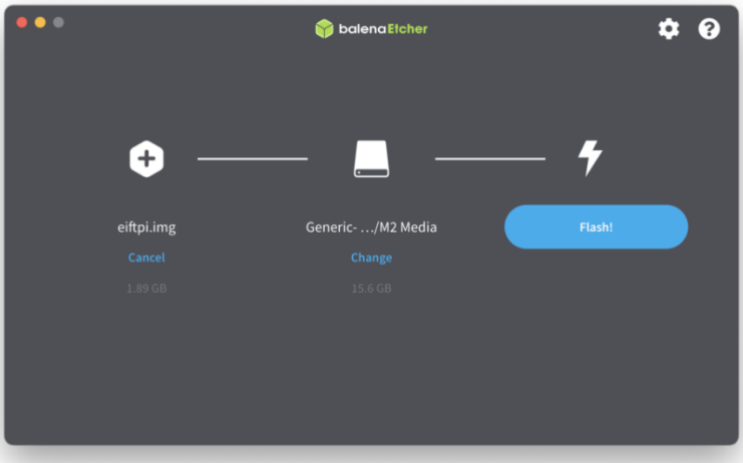
– Raspberry Pi 4 или более новая модель (например, Raspberry Pi 4 Model B);
– Карта microSD;
– Адаптер Lightning to Ethernet;
– Адаптер USB to Ethernet.

Инструкции по установке прошивки на Raspberry Pi

Скачайте образ прошивки из GitHub — Elcomsoft/eiftpi и запишите его на SD-карту с помощью программы, например, balenaEtcher. Вы можете скачать balenaEtcher по следующей ссылке: https://etcher.balena.io/.

– Вставьте SD-карту в компьютер.
– Запустите balenaEtcher и выберите скачанный образ прошивки.
– Выберите SD-карту как целевой носитель.
– Нажмите кнопку «Записать», чтобы записать образ прошивки на SD-карту.
– По завершении процесса извлеките SD-карту из компьютера.

[48] https://github.com/Elcomsoft/eiftpi



На Raspberry Pi вам понадобятся два сетевых интерфейса. Один интерфейс должен быть подключён к интернету, а другой будет использоваться для подключения iPhone. Для подключения iPhone вам понадобится адаптер Lightning to Ethernet. Доступно два варианта подключения:

1. Вы можете подключить Raspberry Pi к интернету через Wi-Fi, а iPhone подключить через порт Ethernet.
2. Либо используйте встроенный Ethernet-порт на Raspberry Pi для подключения к интернет, организовав второй интерфейс с помощью адаптера USB-A to Ethernet.

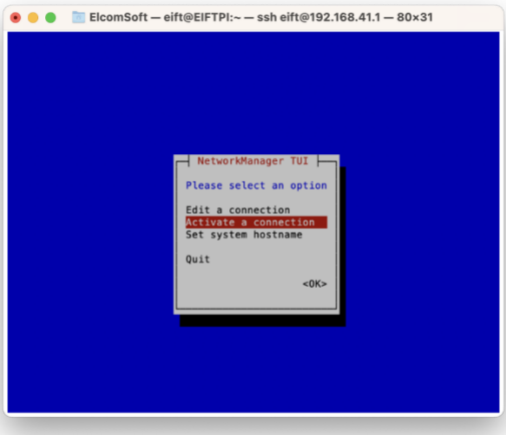
Важно: телефон необходимо подключать к встроенному в плату Ethernet, а сам Pi к интернету — либо по Wi-Fi, либо через USB-адаптер.

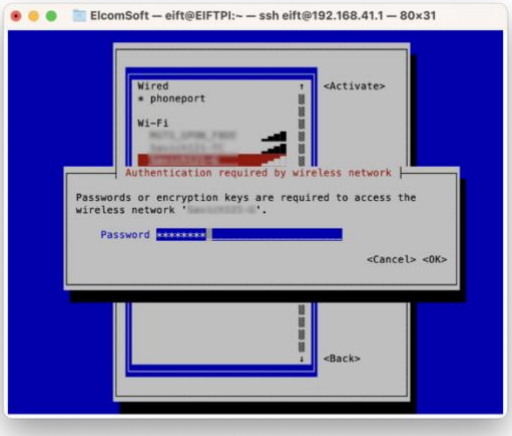
Примечание: Мы не рекомендуем прямое подключение Raspberry Pi к маршрутизатору и настройку беспроводной точки доступа на Pi, так как это в результате iPhone может подключиться к другой сети. Кроме того, этот метод требует дополнительных настроек.

- Для более простой и надёжной установки используйте два проводных подключения. Для этого вам потребуется адаптер USB to Ethernet.

Если вы предпочитаете подключить Raspberry Pi через Wi-Fi, выполните следующие шаги:

- Подключите Raspberry Pi к компьютеру Mac с помощью Ethernet. (Если у вашего MacBook нет Ethernet-порта, вам понадобится дополнительный адаптер USB-C to Ethernet или USB-A to Ethernet.)
- Откройте терминал на компьютере Mac и введите следующую команду:
  ssh eift@192.168.41.1
- Пароль — «Elcomsoft» (без кавычек).
- После входа выполните следующую команду для настройки Wi-Fi:
  sudo nmtui
- В интерфейсе nmtui вы сможете легко подключиться к Wi-Fi сети.





На этом всё! Вы успешно установили прошивку на Raspberry Pi. Подключите Pi к сети (через Ethernet или Wi-Fi), после чего подключите iPhone к Pi с помощью кабеля. Рекомендуем для начала подключить таким образом тестовый iPhone, чтобы убедиться, что доступ к интернету ограничен: на iPhone должны быть доступны только адреса ppq.apple.com и humb.apple.com.

7.3.6. Использование агента

Использование агента-экстрактора в EIFT позволяет извлечь образ файловой системы устройства. Для большинства устройств поддерживается возможность копирования и расшифровки связки ключей (см. таблицу совместимости в примечаниях).

Запустите установленное приложение агента на iPhone (коснитесь соответствующей иконки на экране устройства) и не сворачивайте его в течение всей работы. Не переключайтесь на другие приложения.

При выполнении последующих команд будет запущен процесс эскалации привилегий. В редких случаях процедура может приводить к спонтанной перезагрузке устройства. Если это случилось, просто попробуйте ещё раз (EIFT при этом рекомендуется перезапустить); переустанавливать приложение агента-экстрактора не нужно.

Предварительные шаги

Важно правильно подготовить устройство, проделав все необходимые предварительные шаги.

Проверить дату и время на целевом устройстве

Недостаточно проверить только текущее время; обязательно убедитесь, что не только время, но и день/месяц/год соответствуют текущему значению. Почему это

важно: операционная система устройства должна корректно верифицировать сертификат цифровой подписи, который будет передан с сервера Apple; верификация включает проверку срока действия сертификата. Если время/дата не совпадают, то проверка не будет пройдена.

Не забудьте отключить раздачу интернета после подписи агента!

Если вы забудете отключить раздачу интернета с компьютера после подписи агента на целевом устройстве, возможна потеря данных в результате получения команды на удалённую блокировку или удалённый сброс устройства в процессе работы.

Не используйте VPN или прокси-сервер в процессе подписи агента

В процессе цифровой подписи агента-экстрактора на компьютере не должно быть активных VPN соединений или прокси.

Используйте кабели USB Type-C — Lightning

В отличие от извлечения посредством checkm8, для которого нужен кабель USB-A — Lightning, извлечение посредством агента-экстрактора может работать быстрее и надёжнее при использовании сертифицированного кабеля USB-C — Lightning.

Проделав все необходимые предварительные шаги, можно двигаться дальше.

Убедитесь, что устройство успешно сопряжено с компьютером

Для этого достаточно выполнить следующую пару команд:

```
./EIFT_cmd normal unpair

./EIFT_cmd normal pair
```

Указание выходного пути

Ключ ***-o*** используется для передачи имени папки, в которой будут создаваться выходные файлы (имена файлов назначаются автоматически). Этот ключ используется как при извлечении образа файловой системы tar, так и связки ключей и метаданных файловой системы (имена и размеры файлов, дата и время); указывать его обязательно.

Сохранение связки ключей

Следующая команда сохранит связку ключей в папку /Users/ElcomSoft/Desktop/data/:

```
./EIFT_cmd agent keychain -o
/Users/ElcomSoft/Desktop/data/
```

Создание образа файловой системы

Образ файловой системы, извлекаемый из устройства, сохраняется в архив в формате tar. Перед созданием tar-архива убедитесь, что приложение агента открыто и работает. Держите приложение открытым в течение всего процесса извлечения, в том числе и между различными операциями (копированием связки ключей, созданием tar-архива или образа диска).

Следующая команда создаст tar-архив, содержащий все файлы пользовательского раздела. Архив будет создан в папке /Users/ElcomSoft/Desktop/data/.

```
./EIFT_cmd agent tar -o /Users/ElcomSoft/Desktop/data/
```

В случаях, когда есть подозрение на наличие в устройстве зловредного или шпионского программного обеспечения, вы можете извлечь копию системного раздела для его последующего анализа. Для архивирования системного раздела воспользуйтесь немного другой командой (архив будет сохранён в папке -o /Users/ElcomSoft/Desktop/data/):

```
./EIFT_cmd agent tar --system -o
/Users/ElcomSoft/Desktop/data/
```

Обратите внимание: в обычных ситуациях в архивировании системного раздела необходимости нет.

Извлечение отдельных папок и метаданных файловой системы

В процессе низкоуровневого извлечения посредством агента-экстрактора в дополнение к полному образу файловой системы появилась возможность извлекать как отдельные папки, так и только метаданные файловой системы (имена и размеры файлов, дата и время).

С технической точки зрения новый функционал реализован двумя дополнительными командами: extract и metadata. Ключ -o указывает на папку, в которой будут сохраняться извлечённые данные, и добавлен опциональный параметр -p, который указывает на исходную папку или конкретный файл в файловой системе iOS, который нужно извлечь. Если ключ -p не указан, используется путь "/private/var/" (то есть, корень пользовательских данных).

Примеры запуска

Извлечение только метаданных папки Media:

```
EIFT_cmd agent metadata -p /private/var/mobile/Media/ -
o /Users/ElcomSoft/Desktop/metadata/
```

Извлечение папки Media целиком:

```
EIFT_cmd agent extract -p /private/var/mobile/Media/ -o
/Users/ElcomSoft/Desktop/data/
```

Извлечение полного образа файловой системы:

```
EIFT_cmd agent extract -o
/Users/ElcomSoft/Desktop/data/
```

Извлечение только файла Photo.jpg из фотоальбома:

```
EIFT_cmd agent extract -p
/private/var/mobile/Media/DCIM/Photo.jpg -o
/Users/ElcomSoft/Desktop/data/
```

Последний шаг – удаление агента-экстрактора. Для этого либо введите команду **./EIFT_cmd agent uninstall**, либо удалите значок приложения с экрана стандартным способом.

7.3.7. Последовательность шагов

В этом разделе кратко описана вся последовательность шагов при использовании агента. Обратите внимание: при анализе iPhone с использованием обычного Apple ID настройте ограничения на доступ в сеть согласно ранее приведённой инструкции. При использовании Apple ID разработчика iPhone может быть изолирован от беспроводных сетей.

– Скачайте и установите последнюю сборку Elcomsoft iOS Forensic Toolkit.

– Проделайте предварительные шаги, описанные в предыдущем разделе.

– Командой **./EIFT_cmd normal pair** создайте привязку устройства к компьютеру.

– Введите команду **./EIFT_cmd agent install** для установки агента-экстрактора на телефон. Введите логин и пароль используемого Apple ID, после чего введите одноразовый код двухфакторной аутентификации (код доставляется на доверенное устройство — iPhone, iPad или Mac).

– **После установки агента, iOS 16**: в настройках устройства включите режим разработчика Settings > Privacy & Security > Developer Mode. Будет запрошен код блокировки экрана, который необходимо будет ввести.

– Если был использован обычный Apple ID, верифицируйте сертификат цифровой подписи на iPhone. Для этого устройству понадобится доступ к сети. После подтверждения сертификата запустите приложение-агента, коснувшись его иконки.

– Если был использован Apple ID разработчика, просто запустите приложение-агента, коснувшись его иконки.

– Введите команду **./EIFT_cmd agent keychain -o /Users/ElcomSoft/Desktop/data/** для извлечения и расшифровки связки ключей

– Введите команду **./EIFT_cmd agent tar -o /Users/ElcomSoft/Desktop/data/** для извлечения образа только пользовательского раздела (рекомендуется)

– При подозрении на наличие шпионского или зловредного ПО, введите команду **./EIFT_cmd agent tar --system -o /Users/ElcomSoft/Desktop/data/** для извлечения образа системного раздела. Опционально используйте извлечение отдельных папок, файлов или метаданных.

– Введите команду **./EIFT_cmd agent uninstall** для удаления агента-экстрактора с телефона либо просто либо удалите значок приложения с экрана стандартным способом.

Настоятельно рекомендуем извлечь как связку ключей, так и файловую систему, так как содержимое связки ключей может использоваться для расшифровки данных некоторых приложений (например, облачных резервных копий WhatsApp, данных Signal и т.д.). Образ файловой системы можно проанализировать в программе Elcomsoft Phone Viewer или аналогичном продукте.

7.4. Способ 2: эксплойт загрузчика для iPhone

Прямой доступ через эксплойт загрузчика – самый чистый с криминологической точки зрения способ низкоуровневого доступа.

Для процессоров Apple A5 и более поздних моделей используется метод эксплойта под названием checkm8 («чекмейт», в переводе - «шах и мат»), который позволяет получить доступ к устройству и извлечь из него данные. Для более старых устройств применялся другой метод, также основанный на эксплойте загрузчика, однако принцип работы checkm8 и старых эксплойтов схож. Основное отличие в том, что в более старых версиях iOS, младше четвёртой, отсутствовала функция шифрования данных на устройстве.

Внимание: для ввода iPhone в режим DFU и установки эксплойта используйте только кабели Lightning с разъёмом USB-A. При необходимости можно использовать переходник с Type-C на Type-A. Для подключения некоторых моделей iPhone к компьютерам на Apple Silicon (процессоры M1 и более поздние) использование USB хаба рекомендуется для повышения стабильности работы; см. **Error! Reference source not found.**).

7.4.1. Вводный раздел и теория

В данном разделе описаны принципы работы механизма извлечения данных через эксплойт загрузчика checkm8. Для практической работы этот раздел опционален.

Метод анализа, основанный на использовании эксплойта checkm8, использует уязвимость в загрузчике ряда моделей Apple. Для доступа к данным необходимо указать код блокировки экрана, если он установлен. iOS Forensic Toolkit не использует заимствований из джейлбрейка checkra1n и не включает проприетарного кода Apple. В процессе работы эксперту необходимо будет скачать образ прошивки iPhone с сайта Apple (ссылка на скачивание выдаётся в процессе анализа устройства). iOS Forensic Toolkit использует скачанный образ прошивки для того, чтобы загрузить устройство, минуя установленную на смартфоне операционную систему и избежав таким образом любых модификаций в разделе данных или системном разделе iPhone.

7.4.1.1. Определения

checkm8 — эксплойт уязвимости, найденной в ряде моделей iPhone и других устройств Apple, позволяющий исполнять произвольный код независимо от того, какая версия iOS установлена на устройстве. Уязвимость была обнаружена на аппаратном уровне в большом количестве моделей, которые выпускались на протяжении многих лет. Уязвимость кроется в загрузчике, который получает управление задолго до запуска операционной системы. Наше решение поддерживает устройства из списка, который приводится в **Error! Reference source not found.**.

checkra1n —джейлбрейк, созданный на основе эксплойта checkm8. В отличие от checkm8, который является эксплойтом уязвимости, джейлбрейк checkra1n для своей работы вносит определённые модификации и в системный раздел, и в раздел пользовательских данных. По этой причине использование джейлбрейка checkra1n в

целях криминалистического анализа является хоть и возможным, но не оптимальным способом.

Аппаратные платформы. Актуальный список поддерживаемых моделей приводится в **Error! Reference source not found.**.

7.4.1.2. Преимущества iOS Forensic Toolkit

– гарантированная целостность и неизменность всех разделов устройства.

– любые модификации происходят только в оперативной памяти устройства.

– интерактивные инструкции по установке эксплойта.

– поддержка версий iOS начиная с iOS 3.0 (актуальная информация – на странице продукта[49]).

– поддержка заблокированных устройств в режиме BFU, обход ограничений USB.

7.4.1.3. Принцип работы

Анализ iPhone с использованием уязвимости checkm8 требует точного соблюдения порядка действий. Во-первых, необходимо применить эксплойт, для чего нужно перевести iPhone в режим DFU и подключить его к компьютеру (напомним, поддерживаются только компьютеры Mac). Затем следует применить уязвимость, загрузив в оперативную память устройства модифицированный код. В реализации iOS Forensic Toolkit этот процесс выглядит следующим образом:

1. Из режима DFU в устройство производится загрузка нашего кода, которому затем передаётся управление.
2. Код iOS Forensic Toolkit получает версию загрузчика iBoot и на её основе определяет версию iOS, установленную на устройстве.
3. В консоли iOS Forensic Toolkit, которая запущена на компьютере Mac, выводится ссылка или ссылки на файл с прошивкой соответствующей версии. Прошивки всегда скачиваются непосредственно с сайта Apple.
4. Скачанный файл с прошивкой перетаскивается мышкой на окно EIFT. Если компьютер подключён к интернету, достаточно просто вставить ссылку; в этом случае инструментарий автоматически скачает только минимально необходимый для работы код, что будет существенно быстрее.
5. EIFT распаковывает прошивку, на лету модифицирует исполняемый код и пересылает его в оперативную память устройства.
    a. Обратите внимание: все модификации выполняются исключительно в оперативной памяти устройства; никаких изменений в область данных или системный раздел не вносится. Более того, способ никаким образом не использует копию операционной системы, установленную на самом устройстве. Весь процесс загрузки полностью контролируем, а управление получает только и исключительно тот код, который передаётся на устройство приложением.

[49] Elcomsoft iOS Forensic Toolkit: https://www.elcomsoft.ru/eift.html

6. Далее потребуется провести разблокировку диска, для чего потребуется ввести код-пароль блокировки экрана. Без него можно создать копию пользовательского раздела, но сами данные в большинстве своём останутся зашифрованными.
7. Если код блокировки пустой, то раздел данных будет разблокирован автоматически. Если же код блокировки неизвестен, то извлечение возможно только в BFU-режиме (режиме «до первой разблокировки»), в котором доступен лишь очень ограниченный объём информации.
8. После этого можно приступать к извлечению и расшифровке связки ключей и файловой структуры устройства. Извлекаются абсолютно все данные: базы данных приложений, журнал звонков, история переписки, включая сообщения и вложения, фотографии, скачанные на устройство файлы, данные местоположения и многое другое.

7.4.1.4. Возможные действия с заблокированными устройствами

В первую очередь требуется определить, в каком именно состоянии находится «заблокированный» iPhone. Если устройство выдаёт сообщение о необходимости подключения к iTunes — вероятно, был исчерпан лимит на число попыток разблокировки устройства (более 10 раз был введён неправильный код блокировки экрана). В этом случае аппаратный сопроцессор безопасности блокирует доступ к устройству; обойти эту блокировку не удалось. В этом случае будет запрошен код блокировки; если он неизвестен, нажмите ENTER, после чего EIFT перейдёт в режим извлечения данных BFU — «до первой разблокировки».

Альтернативная ситуация: устройство заблокировано защитным режимом USB, в котором отключается возможность передачи данных через порт Lightning. В этом случае переведите iPhone в режим DFU, и связь с телефоном будет установлена. В этом случае на запрос «известен ли код блокировки» укажите N/n. После этого EIFT перейдёт в режим извлечения данных BFU — «до первой разблокировки».

7.4.1.5. Поддержка iPhone 8, 8 Plus и iPhone X и iOS 16

В операционной системе iOS 14 и 15 для iPhone 8, 8 Plus и iPhone X были усилены меры безопасности, обозначенные термином “SEP hardening” (SEP – Secure Enclave Processor, аппаратный сопроцессор безопасности). Поддержка iPhone 8, 8Plus и iPhone X, работающих под управлением указанных версий iOS, возможна при условии предварительного удаления кода блокировки, что нарушает криминалистическую чистоту исследования. Если код блокировки экрана установлен и неизвестен, то для версий iOS до 15.x включительно поддерживается ограниченное извлечение в режиме BFU.

Модели iPhone 8, 8Plus и iPhone X получили обновление до iOS 16. В этой версии iOS защита SEP была дополнительно усилена. Теперь извлечение посредством checkm8 из указанных моделей стало невозможно, если на устройстве хотя бы раз после начальной настройки использовался код блокировки экрана, даже если код блокировки был впоследствии удалён. Извлечение в режиме BFU на указанных моделях, работающих под управлением iOS 16, не поддерживается.

Ряд моделей iPad на более старых процессорах также получил поддержку iOS 16. Для них может потребоваться предварительно удалить код блокировки экрана. Невозможно предсказать, потребуется ли это делать или нет; попробуйте применить эксплойт, и, если возникнет ошибка, загрузите устройство и удалите код блокировки. **Внимание:** удаление кода блокировки нарушит криминалистическую чистоту исследования!

7.4.1.6. Использование checkm8 для взлома кода блокировки

В текущей версии EIFT взломать код блокировки 64-разрядных моделей iPhone нельзя: аппаратный сопроцессор iPhone блокирует доступ к устройству после десяти неудачных попыток. Обойти это ограничение для 64-разрядных устройств не удалось.

7.4.2. Как добиться повторяемого результата при использовании checkm8

Само по себе использование checkm8 не даёт гарантии повторяемости результата. На результат извлечения могут повлиять несколько факторов.

1. Используемый инструментарий. В Elcomsoft iOS Forensic Toolkit 8 используется метод, в котором код эксплойта загружается только в оперативную память устройства; пользовательские данные на устройстве не модифицируются. В других продуктах методы могут отличаться и отличаются, в результате чего полученные наборы данных могут отличаться между сессиями.
2. Точное следование инструкциям. Очень важно не допустить загрузки устройства в установленную операционную систему, что может произойти, например, при неточном следовании инструкциям по вводу в режим DFU. Загрузка ОС неизбежно приводит к модификации содержимого. Даже если это несколько записей в системных журналах и изменение времени доступа к файлам, контрольные суммы извлекаемых данных не совпадут.
3. Правильное хранение устройства между сессиями. Если между двумя сессиями извлечения данных устройство хотя бы раз загружалось в iOS, данные будут модифицированы.

В обновлённой версии iOS Forensic Toolkit мы постарались максимально облегчить и обезопасить работу эксперта, сведя влияние второго и третьего факторов к минимуму. Нам удалось этого добиться изменением всего одного флага загрузки.

7.4.2.1. Флаг автозагрузки

Для устройств под управлением iOS доступна специальная функция, управляющая загрузкой устройства. При установке специального флага (в нашем продукте он называется "autoboot") в значение False устройство будет загружаться не в установленную операционную систему, а в режим восстановления (recovery). iOS Forensic Toolkit самостоятельно установит этот флаг в значение False в процессе применения эксплойта загрузчика; эксперт также может самостоятельно установить нужное значение автозагрузки следующей командой:

```
./EIFT_cmd tools autobootFalse
```

Значение флага автозагрузки сохраняется и после выключения или перезагрузки устройства. Предполагается, что устройство будет находиться в режиме с отключённой автозагрузкой в течение всего времени, пока оно находится в процессе исследования. Оригинальное значение флага ‘autobootTrue’ предполагается восстанавливать вручную непосредственно перед тем, как устройство будет возвращено владельцу. Для этого используется следующая команда:

```
./EIFT_cmd tools autobootTrue
```

Для чего нужен этот флаг?

1. Ошибка (например, неточное соблюдение таймингов) при переводе устройства в DFU не приведёт к загрузке ОС. Вместо этого устройство загрузится в безопасный режим Recovery, откуда можно повторить попытку.
2. Если находящееся на хранении устройство случайно будет включено, то и в этом случае загрузки ОС не произойдёт. Устройство загрузится в Recovery.
3. В то же время возвращать устройство его владельцу в таком виде нельзя: владелец не сможет пользоваться таким аппаратом. Перед возвратом устройства его нужно привести в оригинальный вид, установив флажок автозагрузки в значение True.

7.4.2.2. Нарушает ли изменение флага автозагрузки принцип криминалистической чистоты?

Нет, не нарушает. Во-первых, данные пользователя в любом случае не модифицируются, сколько бы ни изменялось значение флага автозагрузки. Во-вторых, не изменяется и содержимое системного раздела: значение флага хранится в NVRAM и не пересекается с содержимым системного раздела.

7.4.3. Глубокий разряд аккумулятора

Ещё одна опасность – глубокий разряд аккумулятора. Если устройство выключено, а аккумулятор разряжен ниже определённого минимума, то подключение его к зарядному устройству приведёт к началу загрузки. Чтобы сохранить данные в целости, нужно убедиться, что устройство загружается в режим восстановления (Recovery), а не загружает операционную систему.

Для этого нужно нажать и удерживать кнопку «Домой» (или боковую кнопку на iPhone 8, 8 Plus или iPhone X), затем подключить зарядное устройство и удерживать кнопку, пока устройство не переключится в режим восстановления.

Сложность возникает на полностью разряженных устройствах, которые не начнут загрузку ОС до тех пор, пока аккумулятор не будет заряжен до некоторого минимального уровня. В этом случае вы можете попытаться перевести устройство напрямую в режим DFU. Это достаточно сложно сделать для поколения iPhone 8, т. к. требует точного соблюдения таймингов (лучше всего использовать секундомер или таймер), но довольно просто на iPhone 7 и более старых моделях.

Загрузка DFU производится при любом уровне заряда аккумулятора. Оставьте устройство в DFU подключённым к ПК примерно на минуту. Этого должно быть более

чем достаточно для нормальной загрузки в режим восстановления (Recovery) с помощью iOS Forensic Toolkit. Оттуда, когда для автозагрузки установлено значение false, вы можете безопасно заряжать устройство без риска случайного запуска последовательности загрузки.

7.4.4. Подготовка к работе

Способ извлечения посредством эксплойта загрузчика — один из самых мощных инструментов в арсенале эксперта. В то же время использование этого метода обставлено многочисленными ограничениями и сопутствующими требованиями. Для работы понадобятся:

– **Компьютер на базе macOS.** Поддерживаются Mac на основе процессоров Intel и Apple Silicon. Виртуальные машины и системы Hackintosh не поддерживаются.

– **iOS Forensic Toolkit в совместимой редакции.**

– **Поддерживаемое устройство** (см. таблицу совместимости). Устройство должно быть достаточно работоспособным для того, чтобы ввести его в режим DFU. Если одна из кнопок устройства не функционирует, см. раздел **Аппаратный ввод в режим DFU: когда не работают кнопки** в дополнительных материалах. Устройства с неизвестным паролем или заблокированные после 10 неверных попыток поддерживаются в ограниченном режиме BFU; режим ограничений USB на работу эксплойта не влияет.

– **Код-пароль разблокировки устройства должен быть известен.** В противном случае будет возможно извлечь лишь очень ограниченный объём данных (режим BFU).

– **Поддерживаемая версия iOS.** Мы подавляющее большинство версий iOS, работающих на перечисленных устройствах, включая большинство бета-версий.

– **Кабель USB-A – Lightning. Кабели USB-C – Lightning не могут быть использованы для данного метода извлечения;** для компьютеров, где есть только USB-C, необходимо использовать переходник.

– Для подключения некоторых моделей iPhone к компьютерам на Apple Silicon (процессоры M1 и более поздние) использование USB хаба рекомендуется для повышения стабильности работы; см. таблицу совместимости **Использование USB хабов для повышения стабильности работы checkm8/checkra1n с компьютерами на Apple Silicon**.

– **Необходимо знать** (или определить во время использования уязвимости) **точную версию iOS**, установленную на устройстве.

– **Должна быть возможность скачать прошивку нужной версии** (соответствующую установленной); ссылка на скачивание будет показана в продукте во время использования.

7.4.5. Ввод в режим DFU

Этот шаг является обязательным вне зависимости от того, какие дальнейшие действия вы планируете совершить в рамках анализа. Процедура ввода в режим DFU

одинакова для всех поддерживаемых устройств вплоть до поколения A10 (iPhone 7/7 Plus).

Обратите внимание: поскольку процедура требует точного соблюдения таймингов и полностью работоспособных физических кнопок без «дребезга» контактов, иногда телефон не удаётся ввести в режим DFU с первой попытки. В стандартной конфигурации устройство будет перезагружено в iOS, что нарушит криминалистическую чистоту исследования. Чтобы этого не происходило, рекомендуем предварительно отключить автозагрузку. Для этого:

Отключите автоматическую загрузку устройства в iOS. Это делается для того, чтобы при неудачной попытке входа в DFU устройство не загрузилось в iOS. Для отключения автозагрузки проделайте следующие шаги.

1. Выключите устройство, если оно включено.
2. Переведите устройство в режим Recovery и подключите его к компьютеру. На устройстве должен появиться экран «connect to iTunes». Инструкции по вводу в режим Recovery см. далее по тексту.
3. На компьютере выполните команду:

```
./EIFT_cmd tools autobootFalse
```

В результате выполнения этой команды будет получено устройство, которое в случае неожиданной перезагрузки будет загружаться не в операционную систему, а в режим Recovery, что не нарушает криминалистической чистоты устройства.

Не забудьте отключить этот режим по окончании работы с устройством командой `./EIFT_cmd tools autobootTrue`

iPhone 7, 7 Plus и более старые устройства:

Шаг 1: ввод в Recovery

На iPhone 7, iPhone 7 Plus:

1) Убедитесь, что устройство выключено. Если это не так, выключите устройство штатным образом.
2) Нажмите и удерживайте кнопку уменьшения громкости.
3) Продолжая удерживать кнопку, подключите телефон к компьютеру.
4) Продолжайте удерживать кнопку, пока на устройстве не отобразится экран восстановления.

На iPhone 6s и более старых, включая iPhone SE (1-го поколения):

1) Убедитесь, что устройство выключено. Если это не так, выключите устройство штатным образом.
2) Нажмите и удерживайте **кнопку «Домой»**.
3) Продолжая удерживать кнопку, подключите телефон к компьютеру.
4) Продолжайте удерживать кнопку, пока на устройстве не отобразится экран восстановления.

Шаг 2: ввод в DFU

На iPhone 6s и более старых, включая iPhone SE (1-го поколения):

1. Одновременно зажмите кнопку питания (или боковую кнопку) и кнопку Home (с датчиком Touch ID) и удерживайте в течение 8 секунд

2. Отпустите кнопку питания, а кнопку Home продолжайте удерживать ещё 8 секунд

3. В случае успеха экран должен остаться чёрным. Если устройство перезагрузилось в обычном режиме или устройство показывает логотип iTunes, необходимо повторить процедуру.

4. На iPhone 7 и 7 Plus:

5. Одновременно зажмите боковую кнопку и кнопку Vol- и удерживайте в течение 8 секунд

6. Отпустите кнопку питания, а кнопку Vol- продолжайте удерживать ещё 8 секунд

7. iPhone 8, 8 Plus и iPhone X:

Для устройств на процессорах A11 существует два режима DFU, которые отличаются между собой. Критично важно ввести устройство в правильный режим DFU; в противном случае может не сработать эксплойт или возникнуть ошибки в процессе монтирования раздела данных. Для того, чтобы устройство перешло в нужный режим DFU, разработана и протестирована процедура перевода в этот режим через промежуточный режим Recovery. Используйте следующую последовательность шагов.

Шаг 1: ввод в Recovery

Вероятность успешного применения эксплойта загрузчика повышается, если смартфон ввести в режим DFU не непосредственно, а через промежуточный сервисный режим Recovery.

Для iPhone 8, 8 Plus и iPhone X используйте такие шаги:

1) Убедитесь, что устройство выключено. Если это не так, выключите устройство штатным образом.

2) Нажмите и удерживайте **боковую кнопку**.

3) Достаточно быстро, чтобы не успела начаться процедура загрузки iOS, подключите телефон к компьютеру, продолжая удерживать кнопку.

4) Продолжайте удерживать кнопку, пока на устройстве не отобразится экран восстановления:

Шаг 2: ввод iPhone 8, 8 Plus или iPhone X в DFU

Далее iPhone переводится из режима Recovery в режим DFU. Не отключая телефон от компьютера, запустите iOS Forensic Toolkit в режиме ожидания:

./EIFT boot -w

Далее на iPhone 8, 8 Plus или iPhone X:

1) Короткое нажатие Vol+
2) Короткое нажатие Vol-
3) Нажать и удерживать Power до появления сообщения "iPhone disconnected" в приложении iOS Forensic Toolkit на компьютере. Это сообщение означает, что iPhone отключился от компьютера.
4) Продолжая удерживать Power, зажать и удерживать Vol- в течение 4 секунд
5) cСустя 4 секунды отпустить Power (продолжая удерживать Vol-).
6) iOS Forensic Toolkit подключится и начнёт загрузку iPhone. Когда это произойдёт, отпустите кнопку Vol-.

Важно: если передержать кнопки дольше 4 секунд, вместо входа в DFU телефон перезагрузится. Перед началом работы с исследуемым устройством рекомендуем по возможности попрактиковаться на другом экземпляре iPhone той же модели.

7.4.6. Руководство по использованию iOS Forensic Toolkit 8.0

Ниже приводится полное руководство по использованию продукта в режиме эксплойта загрузчика.

7.4.6.1. Установка iOS Forensic Toolkit 8.0 для Mac

Для того, чтобы установить iOS Forensic Toolkit 8.0, используйте следующие шаги:

1. Смонтируйте образ DMG, соответствующий версии macOS; укажите пароль от образа (поставляется в электронном письме с подтверждением заказа).

2. Перетащите папку **EIFT8** (либо папку с соответствующим именем для более новых версий продукта) на рабочий стол

3. Откройте консоль

4. Запустите xattr, чтобы снять атрибут карантина:

xattr -r -d com.apple.quarantine <path to folder>

5. Можно также ввести часть команды (xattr -r -d com.apple.quarantine) с пробелом в конце, после чего перетащить папку в окно консоли. Команда будет дополнена автоматически.

6. Перейти в папку с установленным EIFT (командой cd Desktop/EIFT8.41 в зависимости от версии инструментария).

7. Приложение готово к запуску командой /EIFT_ cmd

8. Для разных версий macOS поставляются разные образы DMG:

9. iOS-Toolkit-8 -Mac-legacy.dmg для macOS Catalina и более старых

10. iOS-Toolkit-8-Mac.dmg для Big Sur, Monterey и Ventura

Имена образов DMG могут отличаться в более новых версиях продукта. Важным является наличие или отсутствие маркера “legacy”: сборки, маркированные таким образом, предназначены для установки на компьютеры, работающие под управлением macOS Catalina и более старых версий системы. Все компьютеры, собранные на

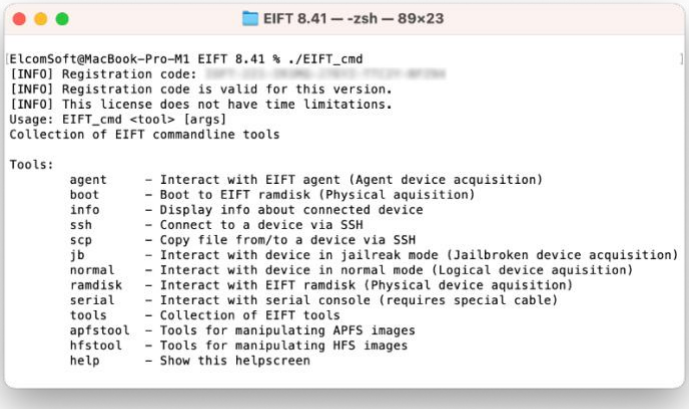
процессорах семейства Apple Silicon (все варианты Apple M1 и M2), работают под управлением свежих версий macOS, и для них используются стандартные (не “legacy”) сборки.

7.4.6.2. Параметры командной строки

В новой версии инструментария был полностью переработан пользовательский интерфейс. В силу ряда причин мы отказались от использования консольного меню, с которым пользователи программы знакомы по предыдущим версиям. Актуальная версия использует интерфейс командной строки.

Поддерживаемые команды:

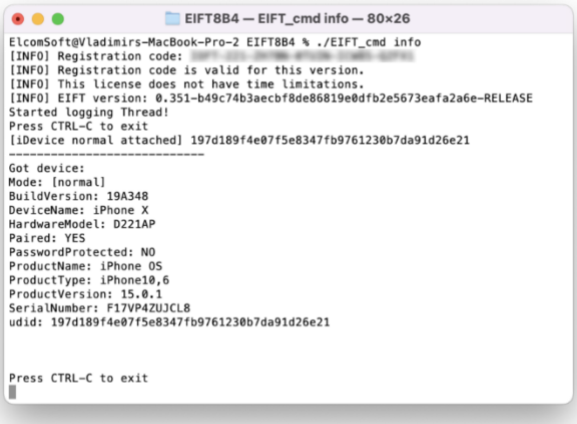
Основное окно.



Воздержитесь от использования следующих команд (за исключением случаев, описанных в инструкции):

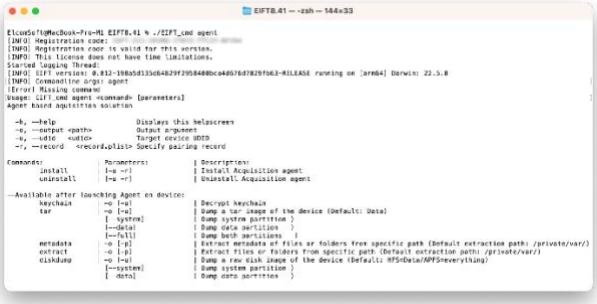
- ssh
- scp
- serial
- tools

Информация об устройстве

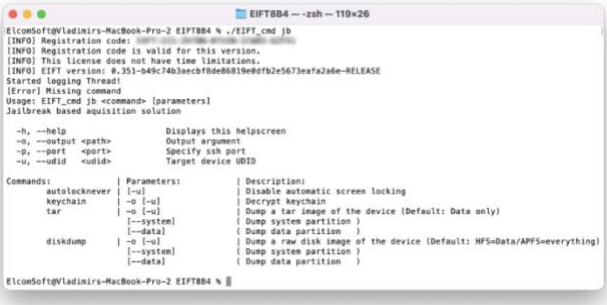


Логическое извлечение

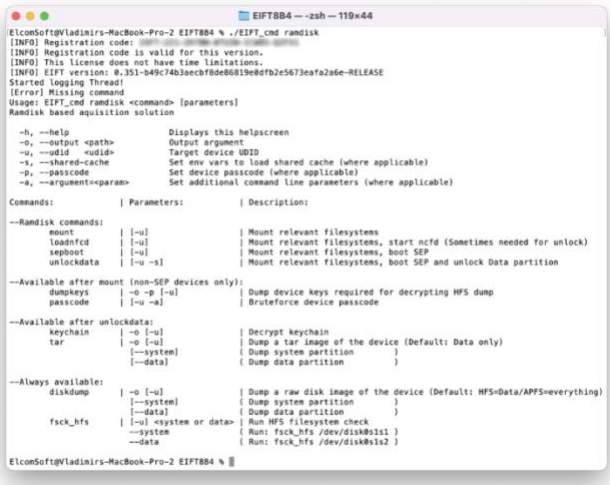
Извлечение посредством агента-экстрактора



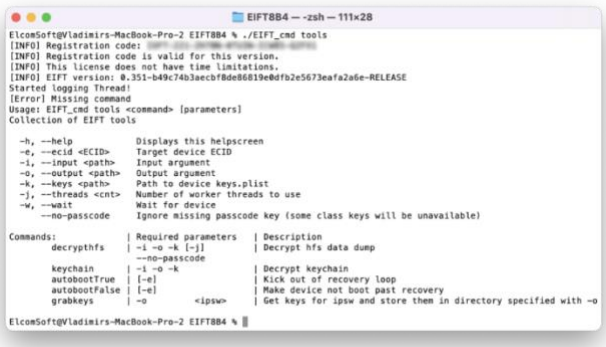
Извлечение через джейлбрейк



Работа с Ramdisk (в процессе извлечения через эксплойт загрузчика)



Tools (дополнительные инструменты)



7.4.7. Извлечение через эксплойт загрузчика: обзорные инструкции

Этот способ извлечения требует от эксперта некоторых специальных навыков и предварительной тренировки по переводу устройства в режим DFU. Неправильная последовательность перевода в DFU перезагрузит устройство в iOS, нарушив криминалистическую чистоту извлечения.

Попрактикуйтесь в переводе устройства в режим DFU. Используйте для этого другое устройство (не то, которое нужно анализировать).

Отключите автоматическую загрузку устройства в iOS:

1. Выключите устройство, если оно включено.
2. Переведите устройство в режим Recovery и подключите его к компьютеру. На устройстве должен появиться экран «connect to iTunes». Инструкции по вводу в режим Recovery: *Шаг 1: ввод в Recovery*
3. На компьютере выполните команду:

```
./EIFT_cmd tools autobootFalse
```

(Не забудьте отключить этот режим по окончании работы с устройством – перед его возвращением. Для этого перезагрузите устройство либо выключите его командой ssh halt, после чего снова включите. После того, как устройство попадёт в режим recovery, выполните команду `./EIFT_cmd tools autobootTrue`).

```
./EIFT_cmd boot -w
```

Переведите устройство в режим Recovery (если оно не находится в нём).

Из режима Recovery переведите устройство в режим DFU по инструкции выше.

Дальнейшие шаги отличаются в зависимости от модели устройства и наличия/отсутствия кода блокировки экрана.

Для устройств iPhone 5s, iPad Mini 1/2 и iPad Air (1st gen), а также для любых других устройств, на которых не установлен код блокировки экрана (или не был установлен изначально, или был сброшен), используйте следующие шаги.

```
./EIFT_cmd ramdisk unlockdata
```

Для всех остальных устройств

Сначала попробуйте действовать так же, как и в предыдущем случае:

```
./EIFT_cmd ramdisk unlockdata
```

В том и только в том случае, если в результате этой команды выводится ошибка “Failed to load necessary libraries. Is shared cache loaded?”, выполните следующие две команды:

```
./EIFT_cmd ramdisk loadnfcd
```

```
./EIFT_cmd ramdisk unlockdata -s
```

Далее – для всех устройств:

```
./EIFT_cmd ramdisk keychain -o {filename}
```

```
./EIFT_cmd ramdisk tar -o {filename}
```

Если не указывать полный путь к файлу, то образ файловой системы и связка ключей создадутся в текущей папке (то есть, в папке инструментария). Если нужно сохранить данные в другом месте, например, на внешнем диске, то нужно указать полный путь (macOS), например, так:

```
/Volumes/MyDisk/iPhone7/data.tar
```

Рекомендуем назначать имена с расширением .tar для образа файловой системы и .xml для связки ключей.

Если устройство остаётся в лаборатории и планируется его дальнейшее исследование, выключите устройство:

```
./EIFT_cmd ssh halt
```

Если работа с устройством завершена, и устройство требуется вернуть владельцу, отключите режим блокирования автозагрузки. Для этого перезагрузите устройство либо выключите его командой ssh halt, после чего снова включите. После того, как устройство попадёт в режим recovery, выполните указанную ниже команду. После этого устройство автоматически перезагрузится:

```
./EIFT_cmd tools autobootTrue
```

7.4.8. Извлечение через эксплойт загрузчика: подробные инструкции

В этом разделе приводится подробная расшифровка перечисленных выше команд. Обратите внимание: для поколения iPhone 8, 8 Plus и iPhone X требуется перевод в режим Recovery, из которого устройство затем переводится в режим DFU.

Отключите автоматическую загрузку устройства в iOS. Это делается для того, чтобы при неудачной попытке входа в DFU устройство не загрузилось в iOS. Для отключения автозагрузки проделайте следующие шаги.

1. Выключите устройство, если оно включено.
2. Переведите устройство в режим Recovery согласно инструкциям для конкретного устройства. В процессе перевода в режим Recovery устройство будет подключено к компьютеру. На устройстве должен появиться экран «connect to iTunes».
3. На компьютере выполните команду:

```
./EIFT_cmd tools autobootFalse
```

(Если работа с устройством завершена, и устройство требуется вернуть владельцу, отключите режим блокирования автозагрузки. Для этого перезагрузите устройство либо выключите его командой ssh halt, после чего снова включите. После того, как устройство попадёт в режим recovery, выполните команду `./EIFT_cmd tools autobootTrue`. После этого устройство автоматически перезагрузится).

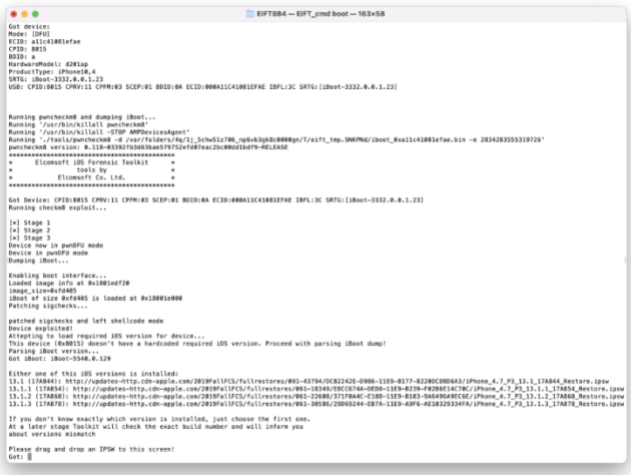
На первом шаге выполните команду:

```
./EIFT_cmd boot -w
```

После выполнения этой команды EIFT переходит в режим ожидания, осуществляя постоянный опрос подключённых устройств.

Переведите устройство в режим DFU по инструкции выше.

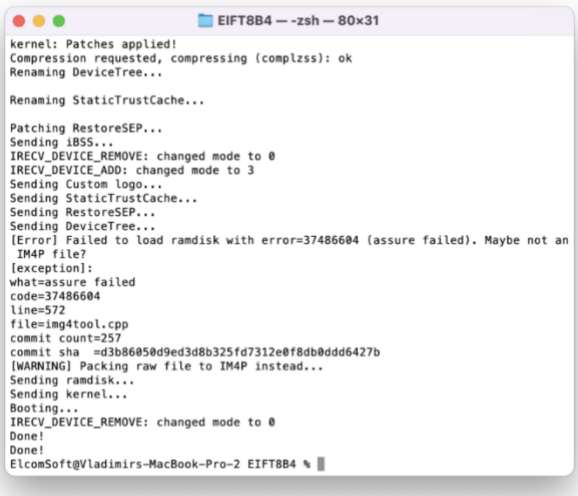
Как только к компьютеру будет подключено совместимое устройство, находящееся в режиме DFU, программа автоматически запускает эксплойт. Определяется версия iOS, установленная на устройстве, и предоставляется ссылка для скачивания. При наличии нескольких потенциальных совпадений будет выведено несколько ссылок для скачивания; рекомендуем использовать последнюю ссылку из списка. Загрузите файл по ссылке и перетащите файл ipsw в окно консоли.



Наше решение не использует операционную систему, установленную на iPhone. Вместо этого в ОЗУ устройства загружается модифицированная версия оригинальной прошивки Apple. Этот процесс требует копию оригинального образа прошивки Apple, соответствующей версии iOS устройства и номеру сборки.

Во многих случаях версия iOS будет автоматически определена EIFT на первом этапе эксплойта на основе версии iBoot и информации об аппаратном обеспечении устройства. Однако в некоторых случаях версия iBoot может соответствовать нескольким сборкам iOS, а в iOS 14 и 15 — и вовсе не определяться. Если использовать неправильный образ прошивки, у вас будет возможность либо повторить эксплойт с другой версией прошивки, либо продолжить с текущим образом (что в большинстве случаев сработает).

Если эксплойт успешно загрузит прошивку, вы увидите следующую информацию:



На экране iPhone появится следующая информация:

Дальнейшие шаги будут отличаться в зависимости от модели устройства и наличия или отсутствия на ней кода блокировки экрана.

Для устройств iPhone 5s, iPad Mini 1/2 и iPad Air (1st gen), а также для любых других устройств, на которых не установлен код блокировки экрана (или не был установлен изначально, или был сброшен), используйте единственную команду:

```
./EIFT_cmd ramdisk unlockdata
```

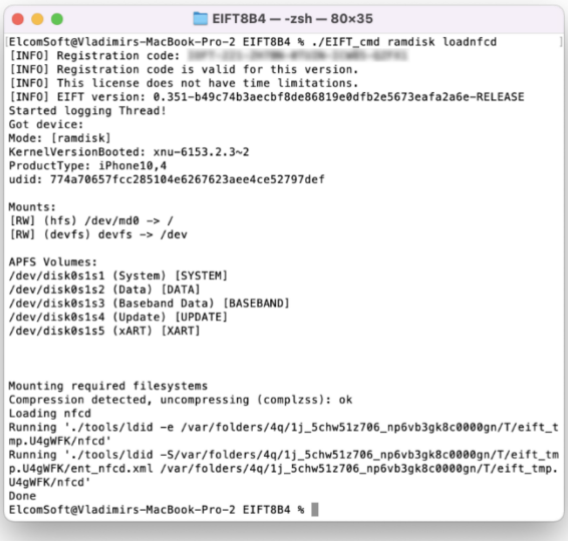
Для всех остальных устройств попытайтесь использовать ту же команду:

```
./EIFT_cmd ramdisk unlockdata
```

В том и только в том случае, если в результате этой команды выводится ошибка “Failed to load necessary libraries. Is shared cache loaded?”, выполните следующие две команды:

```
./EIFT_cmd ramdisk loadnfcd
./EIFT_cmd ramdisk unlockdata -s
```

Команда loadnfcd опциональна, и в большинстве случаев вы можете разблокировать пользовательский раздел (см. следующий пункт) и без неё. Однако иногда возникает ошибка, и придётся вернуться к этой команде. Если на устройстве отсутствует (был удалён или не был установлен изначально) код блокировки экрана, выполнять эту команду не нужно.



Команда unlockdata разблокирует раздел данных и монтирует его в режиме «только для чтения». Обратите внимание: команда unlockdata с ключом -s выполняется только после команды loadnfcd:

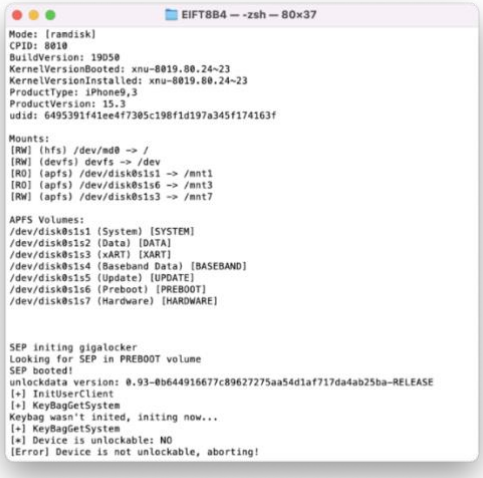
```
./EIFT_cmd ramdisk unlockdata -s
```

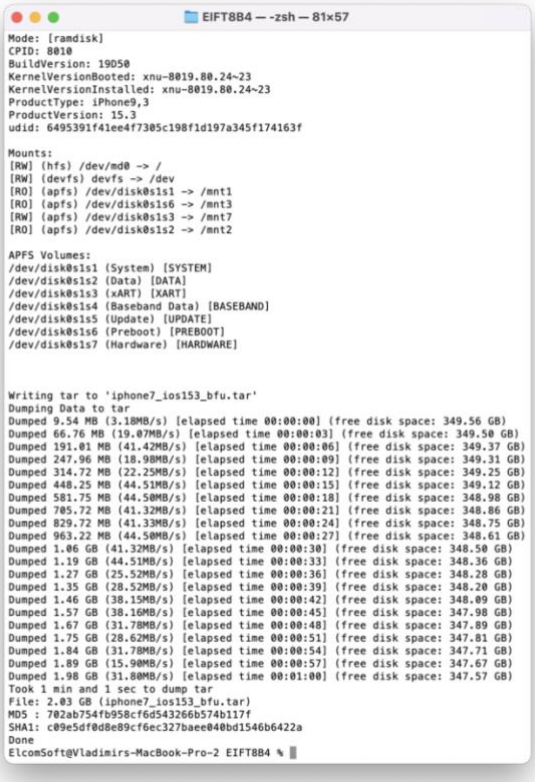
Во всех других случаях ключ -s использовать не нужно:

```
./EIFT_cmd ramdisk unlockdata
```

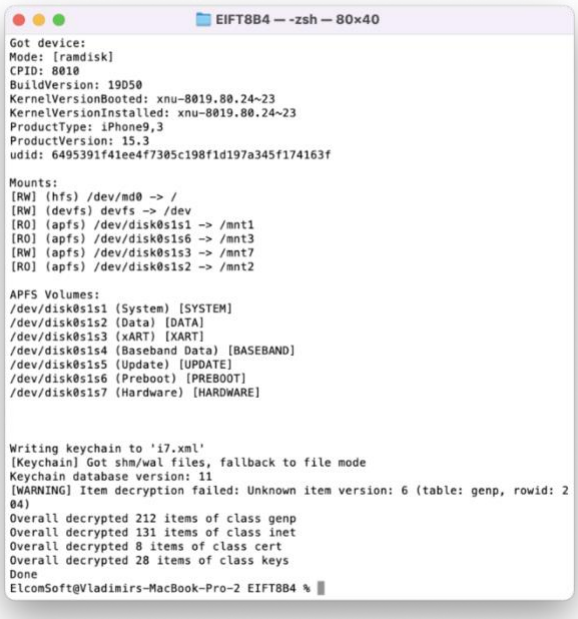
Если установлен пароль блокировки экрана, он будет запрошен:

При вводе неправильного кода блокировки экрана отобразится сообщение об ошибке. Ввод правильного пароля разблокирует раздел данных, и вы сможете продолжить извлечение. Если пароль неизвестен, просто нажмите ENTER. В этом случае будет возможно ограниченное извлечение в режиме BFU (несмотря на ошибку, что устройство не может быть разблокировано); при этом будет доступен только очень ограниченный набор данных.



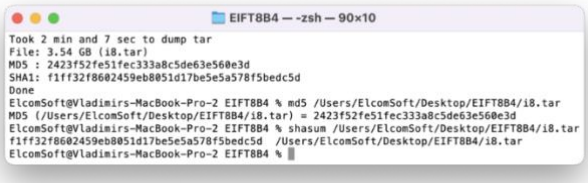



```
./EIFT_cmd ramdisk keychain -o {filename}
```



Извлекает и расшифровывает связку ключей. Если путь не указан, файл будет сохранён в текущую папку.

```
./EIFT_cmd ramdisk tar -o {filename}
```



Извлекает образ файловой системы с автоматическим подсчётом и сохранением контрольной суммы (посредством хэш-функции). Значение контрольной суммы сохраняется в той же папке, что и основной файл.

Если работа с устройством полностью закончена и его планируется вернуть владельцу, отключите режим блокирования автозагрузки по окончании работы с устройством (устройство после этого автоматически перезагрузится в iOS). Обратите внимание: эта команда срабатывает из режима recovery, так что устройство потребуется предварительно перезагрузить.

./EIFT_cmd tools autobootTrue

Если устройство планируется оставить в лаборатории для проведения дополнительных действий, команду отключения блокирования автозагрузки выполнять не нужно. Вместо этого выключите устройство:

./EIFT_cmd ssh halt

ВАЖНО: обязательно используйте эту команду после работы! Из режима DFU невозможно выключить iPhone с помощью кнопок. Если вы попытаетесь нажать и удерживать кнопку питания после отключения режима блокировки автозагрузки, iPhone

перезагрузится (если при этом активен режим блокирования автозагрузки – то в режим Recovery, в противном случае – в систему).

7.4.9. Удаление кода блокировки: когда нужно, а когда не нужно сбрасывать пасскод

Несмотря на то, что уязвимость кроется в жёстко прошитом коде загрузчика в большом количестве моделей, выпускавшихся на протяжение многих лет, в последних поколениях iPhone, в которых присутствует уязвимость, разработчикам Apple удалось в большой степени нивелировать её эффект.

С выходом iOS 14 разработчики Apple усложнили работу экспертов-криминалистов, усилив защиту сопроцессора Secure Enclave (SEP) для устройств на платформах A10 и A11 (это – модели от iPhone 7 и 7 Plus до iPhone 8, 8 Plus и iPhone X). На тот момент защиту можно было обойти, удалив с iPhone код блокировки экрана; впоследствии для процессоров A10 появился дополнительный эксплойт SEP, который позволил обойтись без удаления кода блокировки на iPhone 7 и 7 Plus, работавших под управлением iOS 14 и 15 (iOS 16 для этих моделей не вышла). В то же время для iPhone 8, 8 Plus и iPhone X такого эксплойта не появилось, и для извлечения данных из этих устройств, если на них установлена iOS 14 или 15, по-прежнему нужно удалять код блокировки экрана.

7.4.9.1. Почему удаление кода блокировки для iPhone с A11 на iOS 16 не помогает

С выходом iOS 16, доступной для iPhone 8, 8 Plus и iPhone X, доступ к разделу данных посредством эксплойта checkm8 стал невозможным, если на устройстве хотя бы раз с момента начальной настройки устанавливался код блокировки экрана. Важно понимать, что уязвимость загрузчика как такового не исправлена (исправить уязвимость самого загрузчика по-прежнему невозможно), но смонтировать раздел с пользовательскими данными уже не получится. Сопроцессор Secure Enclave Processor (SEP) отвечает за хранение ключей и шифрование данных, и получить доступ к зашифрованным данным не удастся, если на iPhone хоть раз с момента начальной настройки использовался код блокировки экрана. Если же iPhone 8, 8 Plus или iPhone X был настроен и использовался без кода блокировки (сценарий, далёкий от реальности), то доступ к данным по-прежнему возможен. Более старые устройства не получили ни патча, ни, собственно, iOS 16, поэтому на них это ограничение не распространяется. Нет его и на других устройствах, которые получили iOS 16, но работают на более старых процессорах — таких, как ряд моделей iPad.

Таким образом, для извлечения данных через эксплойт загрузчика **код блокировки экрана нужно сбрасывать в следующих случаях**:

- **iPhone 8, 8 Plus, iPhone X**: если установлена iOS 14 или 15 (для iOS 16 сброс бесполезен)

Однако не торопитесь сбрасывать код блокировки: сброс ведёт к целому ряду неприятных последствий, и в ряде случаев без него можно обойтись.

7.4.9.2. Как удалить код блокировки

Сброс кода блокировки можно осуществить несколькими способами. Во-первых, это можно сделать через настройки: Settings, Face ID & Passcode, Turn Passcode Off. На устройствах с Touch ID, соответственно, используйте последовательность Settings, Touch ID & Passcode, Turn Passcode Off. В любом случае, вам потребуется оригинальный код блокировки экрана.

Второй способ сбросить код блокировки экрана - через функцию Reset All Settings (потребуется ввести оригинальный код блокировки экрана), однако для наших целей он избыточен и используется, в основном, в случаях, когда необходимо сбросить пароль к резервной копии.

Вполне возможно, что код блокировки вам удалить не удастся, даже если вы точно знаете оригинальный пароль. Политики безопасности и политики MDM, "полётный" режим устройства, ограничения «Экранного времени» и некоторые другие настройки могут запрещать удаление кода блокировки экрана. И если с паролем «Экранного времени» можно попробовать удалить (см. статью «Сброс пароля экранного времени» в нашем блоге), то внешние политики безопасности могут быть вне вашего контроля. О возможных проблемах при сбросе кода блокировки экрана и способах их решения мы написали подробную статью - Удаление кода блокировки с iPhone: подводные камни и проблемы[50].

7.4.9.3. Последствия удаления кода блокировки

Удаление кода блокировки удалит и те данные, которые зависят от наличия на устройстве данной настройки безопасности. Сброс кода блокировки исключает iPhone из «доверенного круга устройств», которые могут синхронизировать в iCloud облачную связку ключей, данные «Здоровья», сообщения и некоторые другие данные. Кроме того, удаление кода блокировки приводит к тому, что с устройства удаляются скачанные сообщения Exchange (если они были) и обнуляется история транзакций Apple Pay. Наконец, после удаления пароля вы более не сможете сбросить или изменить с данного устройства пароль от Apple ID, если на вашей учётной записи активирована двухфакторная аутентификация (точнее, сможете это сделать через браузер, указав старый пароль и пройдя проверку двухфакторной аутентификацией).

По указанным причинам причине удаление пароля — крайняя мера, идти на которую стоит лишь после тщательной оценки всех «за» и «против». Если вы всё же вынуждены сбросить код блокировки экрана, убедитесь, что предварительно была сделана резервная копия устройства (даже если она защищена паролем), извлечены медиафайлы по протоколу AFC и сохранены журналы диагностики и файлы приложений.

7.4.9.4. Когда сбрасывать код блокировки не нужно

Итак, мы выяснили, что сброс кода блокировки может оказаться необходимым для извлечения данных через эксплойт загрузчика **только** для телефонов iPhone 8, 8 Plus и iPhone X на процессоре A11, работающих под управлением iOS 14 или 15 (поддержка

[50] https://blog.elcomsoft.ru/2020/12/udalenie-koda-blokirovki-s-iphone-podvodnye-kamni-i-problemy/

iOS 16 для этих моделей весьма условна, поэтому сброс кода блокировки при данных условиях будет бесполезен). В то же время для тех же устройств может быть доступен альтернативный способ низкоуровневого анализа, не требующий сброса кода блокировки экрана.

Если исследуемое устройство работает на iOS 14, 15 или даже ряда версий iOS 16 (см. таблицу совместимости), наиболее полным, эффективным и безопасным методом извлечения будет агент-экстрактор из комплекта iOS Forensic Toolkit. Агент-экстрактор не требует снятия кода блокировки.

Обратите внимание! Для следующих моделей iPad ранее требовалось сбрасывать код блокировки экрана, если они работали под управлением iOS 16:

- iPad Pro // A9X
- iPad Pro 2 // A10X
- iPad 5 // A9
- iPad 6 // A10
- iPad 7 // A10

С выходом iOS Forensic Toolkit 8.55 такой необходимости больше нет. Рекомендуем проверить версию iOS Forensic Toolkit и обновить её, если установлена более старая.

7.4.10. Проблемы и решения

В этом разделе описаны ограничения метода, а также известные нам проблемы и способы их решения.

7.4.10.1.После извлечения через checkm8 устройство перезагружается в режим Recovery

Так и должно быть. После успешного применения эксплойта iOS Forensic Toolkit сбрасывает флаг автозагрузки, после чего устройство всегда будет загружаться в режим восстановления (recovery). Сделано это для того, чтобы обезопасить данные на устройстве от модификации, которая неизбежно возникает при штатной загрузке ОС. Эта защита обеспечивает повторяемость результатов: в каждой последующая сессии извлечения данных эксперт получит тот же результат, что и в первый раз; контрольные суммы образов совпадут.

В то же время возвращать устройство владельцу в таком состоянии нельзя. Перед возвратом устройства необходимо вернуть флаг автозагрузки в изначальное состояние. Для этого переведите устройство в режим восстановления (recovery), подключите его к компьютеру с iOS Forensic Toolkit и выполните следующую команду:

```
./EIFT_cmd tools autobootTrue
```

После её выполнения устройство перезагрузится штатным образом.

Нарушает ли переключение флага автозагрузки криминалистическую чистоту процесса? Нет, не нарушает: значение флага хранится в NVRAM, а не на разделе данных

или в системном разделе. Его переключение не нарушает целостность данных. Подробнее - в статье Цифровые улики и повторяемость криминалистического анализа[51].

ВАЖНО: iOS Forensic Toolkit автоматически установит флаг автозагрузки только после успешного применения эксплойта загрузчика. В то же время и предварительный процесс перевода устройства в режим DFU сопряжён с риском случайной перезагрузки устройства в ОС. Соответственно, перед вводом устройства в режим DFU мы рекомендуем перевести устройство в режим восстановления (Recovery), после чего вручную установить флаг автозагрузки указанной ниже командой, :

```
./EIFT_cmd tools autobootFalse
```

7.4.10.2.Ошибка при попытке извлечения 32-разрядного устройства

Проблема: Не удаётся выполнить команду unlockdata при извлечении из 32-разрядных устройств.

Причина: Так и должно быть. Для 32-разрядных устройств используются другая процедура, в рамках которой извлекается не копия файловой системы, а образ раздела данных.

Решение: Используйте процесс по извлечению данных из 32-разрядных устройств, описанный в статье Perfect Acquisition Part 4: The Practical Part[52]

7.4.10.3.Сброс кода блокировки экрана: применимость и риски

В некоторых случаях на ранней стадии загрузки возникает ошибка, которая может выглядеть следующим образом (значения *code*, *line* и *commit* могут не совпадать):

```
      [ERROR] EIFT: failed with exception:
[exception]:
what=Failed to open connection to device
code=11993119
line=183
file=../../../ra1nsn0w/iOSDevice.cpp
commit count=191
commit sha  =1d674084639c73f1397535ee8aec50b35f1760d6
```

Если это происходит, на устройстве придётся удалить (сбросить) код блокировки экрана, после чего повторить попытку. Как правило, ситуация возникает в результате усиления мер безопасности на уровне SEP (Secure Enclave Processor) в поздних версиях iOS. Подробности – в разделе 7.4.9.

Проблема: не проходит команда unlockdata на устройствах с чипом A11 Bionic под управлением iOS 14 или 15 (всегда) или любые другие устройства под управлением iOS 16 (только при возникновении ошибки).

Решение: загрузите устройство штатным образом, разблокируйте его кодом блокировки экрана, после чего удалите код блокировки в настройках Settings - Face ID

[51] https://blog.elcomsoft.ru/2023/02/czifrovye-uliki-i-povtoryaemost-kriminalisticheskogo-analiza/
[52] https://blog.elcomsoft.com/2023/04/perfect-acquisition-part-4-the-practical-part/

& Passcode или Touch ID & Passcode - Turn Passcode Off (потребуется подтверждение вводом кода блокировки).

Возможные проблемы: обратите внимание на флаг автозагрузки (см. выше), который может предотвратить штатную загрузку ОС. При необходимости установите нужное значение флага из режима recovery.

Последствия: сброс кода блокировки экрана приводит к безвозвратному удалению некоторых категорий данных (например, переписку в Exchange, транзакции Apple Pay и т.д.), а также приводит к утрате устройством статуса доверенного (в контексте последующего доступа к данным, защищённым сквозным шифрованием в Apple ID/iCloud).

7.4.10.4.Невозможно перевести устройство в режим DFU

Существует несколько возможных ошибок при переводе в режим DFU.

Недостаточный уровень заряда. Часто встречается, если устройство долго хранилось обесточенным. Если подключить устройство к питанию, то по достижении определённого уровня заряда оно начнёт загрузку в ОС, чего желательно избежать. Мы рекомендуем сразу перевести устройство в режим восстановления (Recovery), что можно проделать даже при низком уровне заряда.

Неисправность или дребезг кнопок. Для перевода в DFU требуется точное соблюдение последовательности нажатия кнопок и таймингов. Неисправность кнопок или дребезг контактов могут нарушить последовательность, что приведёт к перезагрузке устройства. Рекомендуем воспользоваться одной из следующих инструкций: Аппаратный перевод в DFU: когда не работают кнопки (требуется разборка) либо Автоматический ввод в DFU с микроконтроллером Raspberry Pi Pico (только для устройств на чипах A11 Bionic, разборка не требуется).

Несоблюдение последовательности нажатий или таймингов также может привести к перезагрузке или переводу в режим восстановления. Чтобы исключить сценарий с неисправными кнопками или контактами, рекомендуем предварительно потренироваться на аналогичной заведомо исправной модели.

Общие рекомендации

В случае проблем с вводом в режим DFU (это требует некоторой сноровки) или применения уязвимости в первую очередь просто повторите попытку, затем попробуйте поменять кабель (желательно использовать оригинальный) и/или подключить устройство к другому USB-порту. Если же и это не помогает – использовать другой компьютер (разумеется, при наличии). Наконец, попробуйте ввести устройство в DFU другим способом.

7.4.10.5.Несовпадение версии прошивки, ошибка автоматического определения версии

Проблема: В iOS Forensic Toolkit отображается несколько ссылок на скачивание прошивки либо не отображается ни одной; при использовании ссылки или образа прошивки не удаётся разблокировать раздел данных.

Причина: В нашей реализации checkm8 используется образ оригинальной прошивки Apple, изменения в которую вносятся на лету в оперативной памяти. Версия

прошивки, установленной на устройстве, должна совпадать с той, модифицированный образ которой подгружается в память устройства. Если версии не совпадают, то извлечение может как сработать штатным образом, так и не сработать (не удастся смонтировать раздел данных) или привести к перезагрузке устройства.

Функция определения версии прошивки работает на основе версии загрузчика iBoot. В то же время одна и та же версия загрузчика может использоваться несколькими версиями iOS, что и приводит к выводу нескольких ссылок на прошивки.

Решение: доступно два варианта.

1. Определить точную версию ОС с использованием режима диагностики (это безопаснее полной загрузки устройства).
2. Последовательно перебрать все предложенные iOS Forensic Toolkit варианты прошивок начиная с самой свежей сборки. Убедитесь, что флаг автозагрузки установлен (при спонтанной перезагрузке устройство войдёт в режим восстановления, а не начнёт загрузку ОС).

В некоторых случаях корректную версию прошивки определить не удаётся (например, если новая версия iOS вышла позднее установленной у вас версии iOS Forensic Toolkit). В таких случаях попробуйте найти ссылку на нужный образ на сайте ipsw.me.

Если на устройстве установлена бета-версия iOS, свяжитесь с нашей службой поддержки. Как правило, Apple не публикует образов бета-версий ОС.

Для устройств **Apple TV** (часто), **Apple Watch** (всегда), **HomePod** (всегда) и **iPhone/iPad** (редко) полные образы прошивок .ipsw могут быть недоступны. Вместо этого может быть доступен образ обновления в формате OTA. Такие образы или ссылки на них поддерживаются iOS Forensic Toolkit; переименовывать или распаковывать такие файлы не нужно.

7.4.10.6.В выходных данных присутствует предупреждение 'Snapshot'

Проблема: В выходных данных присутствует предупреждение 'Snapshot':

```
    Mounts:
[RW] (hfs) /dev/md0 -> /
[RW] (devfs) devfs -> /dev
APFS Volumes:
/dev/disk0s1s1 (Whitetail14A403.D10D101OS) [NONE]
Snapshot: com.apple.os.update-
151D1F6F36C3D125B3424A627391C16BCF5FCDA55D4BAE35C3BE3D65720F
574C23EE3363F263A1A37DBF741A65C4CC73
Snapshot: com.apple.os.update-MSUPrepareUpdate
/dev/disk0s1s2 (Data) [NONE]
/dev/disk0s1s3 (Baseband Data) [NONE]
```

Причина: Если в выходных данных присутствует 'Snapshot', это означает, что устройство находится в одном из двух возможных состояний:

1. Обновление скачано, но не установлено: на устройстве скачан файл обновления ОС, который ещё не был установлен.

2. **Модифицированный системный раздел**: работа джейлбрейка, вредоносного или шпионского ПО.

Решение 1: Если на устройстве скачано обновление, его можно удалить из настроек.

Шаги:

1. В настройках Settings выберите General - iPhone Storage.
2. В списке приложений найдите пункт "iOS update" и коснитесь его.
3. Нажмите "Delete Update".

Если обновлений не обнаружено, а предупреждение "Snapshot" присутствует, свяжитесь с нашей службой поддержки.

Существует способ, позволяющий обойти предупреждение "Snapshot" без загрузки устройства и удаления обновления. Этот способ связан с сопутствующими рисками; если вы хотите его использовать, свяжитесь с нашей службой поддержки.

Внимание: Загрузка устройства в iOS несёт сопутствующие риски (нежелательный выход устройства в интернет, изменение временных меток некоторых баз данных и т.п.)

Решение 2: если системный раздел устройства модифицирован или есть подозрение на работу вредоносного/шпионского ПО, свяжитесь с нашей службой поддержки.

7.4.10.7.Повреждения файловой системы, проблемные файлы APFS 'copy-on-write'

Проблема: Некоторые файлы имеют анормально большие размеры.

Причина: Как правило, причина — повреждение файловой системы либо специфика реализации схемы APFS «copy-on-write». При использовании агента-экстрактора проблема решается автоматически, однако это решение неприменимо при использовании checkm8.

Решение: На данный момент универсального решения не существует.

Обходной путь: Проблему можно обойти, подключившись к устройству в режиме SSH (поддерживается в iOS Forensic Toolkit) и либо вручную скопировав только нужные файлы, либо, напротив, удалив повреждённые файлы. За подробными инструкциями обратитесь в нашу службу поддержки.

В будущих версиях: Решение ожидается в будущих версиях iOS Forensic Toolkit, в которых запланирована интеграция агента-экстрактора и нового агента для работы с checkm8. Новый агент, в частности, будет поддерживать частичное извлечение файловой системы и извлечение метаданных.

7.4.10.8.Неизвестный код блокировки экрана

Обратите внимание: разблокировка устройств с неизвестным кодом блокировки не реализована (на данный момент такой функционал доступен только для 32-разрядных моделей до iPhone 5c включительно). Если вы не знаете код блокировки экрана, максимум что можно сделать – это выполнить частичное извлечение файловой системы (только те файлы, которые не зашифрованы – к сожалению, их немного, но всё же иногда

они представляют некоторую ценность, поскольку там есть журнал звонков, некоторые данные геолокации, черновики сообщений и т. д.)

Сопроцессор безопасности iPhone заблокирует устройство после десяти попыток ввода неверного кода блокировки. После этого устройство можно будет проанализировать только в режиме BFU независимо от того, узнаете ли вы оригинальный код блокировки экрана или нет. Обойти это ограничение пока не удалось. В целях безопасности iOS Forensic Toolkit позволяет лишь 7 попыток ввода кода блокировки.

7.4.10.9.Индикация на экране устройства

Чтобы процесс загрузки, применения уязвимости и разблокировки данных был более понятным визуально, мы меняем заставку на устройстве при выполнении различных шагов – сначала показывается Booting, затем Exploited, наконец Unlocking, а в процессе копирования файловой системы – Copying data. На данный момент заставки реализованы не для всех устройств.

7.5. Способ 2.1: эксплойт загрузчика и часы Apple Watch S0-S3

iOS Forensic Toolkit 8 в некоторых редакциях позволяет извлекать данные из ряда моделей часов Apple Watch от оригинальной модели (“S0”) до Series 3 включительно. Извлечение осуществляется посредством эксплойта checkm8 с использованием адаптера USB.

Ниже приводится таблица совместимости моделей часов и методов извлечения. Зелёным отмечены модели, для которых доступно низкоуровневое извлечение через эксплойт загрузчика; красным - модели, для которых возможно логическое извлечение. Для моделей, которые отсутствуют в таблице, извлечение невозможно.

Series	Чип (SoC)	SEP	watchOS	Последняя доступная версия watchOS	Внутренний идентификатор модели
1st gen	S7002 (S1)	-	1.0	4.3.2	Watch1,1, Watch1,2
Series 1	T8002 (S1P)	+	3.0	6,3	Watch2,6, Watch2,7
Series 2	T8002 (S2)	+	3.0	6,3	Watch2,3, Watch2,4
Series 3	T8004 (S3)	+	4.0	8.7.1	Watch3,1, Watch3,2, Watch3,3, Watch3,4
Series 4	T8006 (S4)	+	5.0	10	Watch4,1, Watch4,2, Watch4,3, Watch4,4
Series 5	T8006 (S5)	+	6.0	10	Watch5,1, Watch5,2, Watch5,3, Watch5,4
SE	T8006 (S5)	+	7.0	10	Watch5,9, Watch5,10, Watch5,11, Watch5,12
Series 6	T8301 (S6)	+	7.0	10	Watch6,1, Watch6,2, Watch6,3, Watch6,4

7.5.1. Адаптеры USB для часов Apple Watch

Для подключения часов к компьютеру используется специальный адаптер – один из множества доступных на рынке. Существует несколько типов таких адаптеров, поддерживающих разные поколения часов Apple Watch. Некоторые из них на фотографии:

Мы использовали адаптер S-Dock, который изображён на фотографии в левом нижнем углу.

О разных типах адаптеров и различиях между ними мы писали в статье Apple Watch Forensics: The Adapters[53] . Обратите внимание: понадобится адаптер, поддерживающий исследуемую модель Apple Watch. Подключённые к адаптеру часы выглядят следующим образом:

7.5.2. Совместимость

Поддерживаются все модели часов Apple Watch S0 (первая модель часов), S1, S2 и S3 под управлением всех версий watchOS.

7.5.3. Подготовка к работе

Убедитесь, что у вас есть всё необходимое для работы с часами.

1. iOS Forensic Toolkit в совместимой редакции.

2. Совместимая модель часов Apple Watch. Часы должны быть достаточно работоспособны для перевода в режим DFU.

[53] https://blog.elcomsoft.com/2021/08/apple-watch-forensics-the-adapters/

3. Код блокировки от Apple Watch должен быть известен. В противном случае поддерживается ограниченное извлечение в режиме BFU.

4. Совместимый USB-адаптер для подключения часов к компьютеру.

5. Вы должны иметь возможность загрузить официальную прошивку Apple (ссылка для скачивания будет предоставлена во время извлечения), которая соответствует версии watchOS, установленной на устройстве.

Обратите внимание: разработчики Apple частично исправили уязвимость загрузчика в iOS 14 и 15, изменив порядок загрузки и разблокировки данных. Однако watchOS 7 и 8, основанные на этих версиях iOS, соответствующего патча не получили, в результате чего вам не нужно будет удалять код блокировки экрана часов.

7.5.4. Анализ данных

Про возможности анализа извлечённых из часов данных рассказано в статье Криминалистический анализ Apple Watch[54]. Кроме того, рекомендуем следующие статьи из нашего блога:

- Apple Watch Forensics 02: Analysis[55]
- Apple TV Forensics 03: Analysis [56]

7.5.5. Apple Watch: извлечение данных через checkm8

Для извлечения данных из часов используйте следующую последовательность действий:

1. Запустите iOS Forensic Toolkit 8.0 (Mac)

2. Подключите часы Apple Watch к компьютеру через адаптер USB (часы должны быть выключены)

3. Выполните команду ./EIFT_cmd boot -w

4. Переведите часы в режим DFU и дождитесь срабатывания эксплойта

5. Выполните команду ./EIFT_cmd unlockdata

6. При ошибке "Failed to load necessary libraries. Is shared cache loaded?" последовательно выполните команды ./EIFT_cmd ramdisk loadnfcd и ./EIFT_cmd unlockdata -s

7. Выполните команду ./EIFT_cmd ramdisk keychain -o {filename} для извлечения связки ключей

8. Выполните команду ./EIFT_cmd ramdisk tar -o {filename} для извлечения файловой системы

9. Выполните команду ./EIFT_cmd ssh halt для выключения Apple Watch

7.5.6. Пошаговое руководство

Разберём указанные выше команды подробнее.

---

[54]:https://blog.elcomsoft.ru/2022/02/kriminalisticheskij-analiz-apple-watch-3/
[55] https://blog.elcomsoft.com/2019/06/apple-watch-forensics-02-analysis/
[56] https://blog.elcomsoft.com/2019/09/apple-tv-forensics-03-analysis/

После запуска iOS Forensic Toolkit подключите Apple Watch к компьютеру через USB-адаптер. На момент подключения часы должны находиться в выключенном состоянии.

Перевод часов в режим DFU:

Нажмите и удерживайте колёсико часов и боковую кнопку в течение 10 секунд. Отпустите боковую кнопку, продолжая удерживать колёсико в зажатом положении в течение ещё 10 секунд.

Альтернативный способ перевода в DFU:

1. Запустить EIFT с ключом -w (режим ожидания).
2. Подключить часы к компьютеру через адаптер (привязка не нужна).
3. Зажать обе кнопки (основную кнопку и колёсико).
4. Дождаться пока экран погаснет, отсчитать 2 секунды.
5. Оставить зажатым колёсико, отпустив вторую кнопку.
6. EIFT автоматически обнаружит часы в режиме DFU.

При успешном входе в DFU экран часов останется чёрным. Если на часах появился логотип Apple, вы удерживали кнопки слишком долго; повторите попытку.

После того, как часы перешли в режим DFU, в iOS Forensic Toolkit выполните следующую команду:

```
./EIFT_cmd boot
```

Обратите внимание: если EIFT уже был запущен в режиме ожидания (-w), эту команду выполнять не нужно; эксплойт запустится автоматически.

Команда запускает эксплойт. Определяется версия iOS, установленная на устройстве, и предоставляется ссылка для скачивания. При наличии нескольких потенциальных совпадений будет выведено несколько ссылок для скачивания; рекомендуем использовать последнюю ссылку из списка. Загрузите файл по ссылке и перетащите его в окно консоли, после чего нажмите ENTER.

На экране часов отобразится сообщение “Booting”.

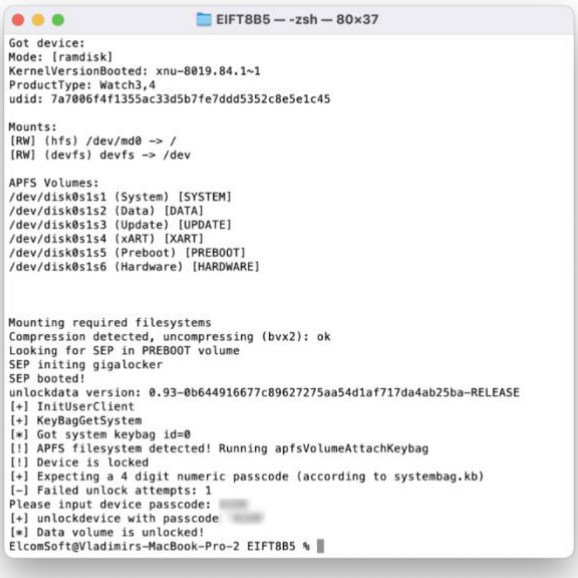
Во многих случаях версия watchOS будет автоматически определена EIFT на первом этапе эксплойта на основе версии iBoot и информации об аппаратном обеспечении устройства. Однако в некоторых случаях версия iBoot может соответствовать нескольким сборкам watchOS или и вовсе не определяться. Если использовать неправильный образ прошивки, у вас будет возможность либо повторить эксплойт с другой версией прошивки, либо продолжить с текущим образом (что в большинстве случаев сработает).

Если эксплойт успешно загрузит прошивку, вы увидите следующую индикацию:


```
./EIFT_cmd ramdisk unlockdata
```

Команда разблокирует раздел данных и монтирует его в режиме «только для чтения».

Если установлен пароль блокировки экрана, он будет запрошен. Если код блокировки часов неизвестен, нажмите ENTER (будет доступно ограниченное извлечение в режиме BFU).



При вводе неправильного кода блокировки экрана отобразится сообщение об ошибке. Ввод правильного пароля разблокирует раздел данных, и вы сможете продолжить извлечение. Если пароль неизвестен, просто нажмите ENTER. В этом случае будет возможно ограниченное извлечение в режиме BFU (несмотря на ошибку, что устройство не может быть разблокировано); при этом будет доступен только очень ограниченный набор данных.

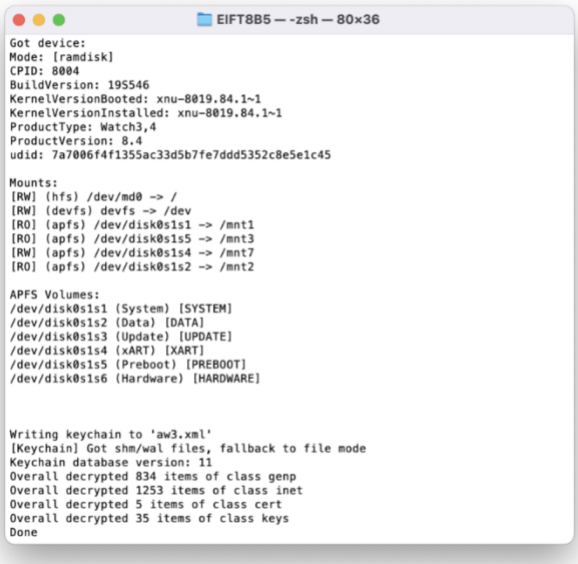
В том и только в том случае, если в результате предыдущей команды выводится ошибка "Failed to load necessary libraries. Is shared cache loaded?", последовательно выполните следующие две команды:

```
./EIFT_cmd ramdisk loadnfcd
```

```
./EIFT_cmd ramdisk unlockdata -s
```

Следующая команда извлекает и расшифровывает связку ключей.

```
./EIFT_cmd ramdisk keychain -o {filename}
```



Если путь не указан, файл будет будет сохранён в текущую папку.

```
./EIFT_cmd ramdisk tar -o {filename}
```

Извлекает образ файловой системы с автоматическим подсчётом и сохранением контрольной суммы (посредством хэш-функции). Значение контрольной суммы сохраняется в той же папке, что и основной файл.

Контроллер SoC и USB в Apple Watch значительно медленнее, чем в версии для iPhone, что приводит к сравнительно низкой скорости извлечения — примерно 3 МБ/с.

7.6. Способ 2.2: эксплойт загрузчика и приставки Apple TV 3, Apple TV 4 (HD), Apple TV 4K

В нескольких поколениях Apple TV, основанных на чипах A5, A8 и A10X, присутствует уязвимость загрузчика, позволяющая извлечь из этих устройств данные посредством эксплойта checkm8. Уязвимость присутствует в моделях Apple TV 3 (2012 и 2013), Apple TV 4 / Apple TV HD (2015 и 2021) и Apple TV 4K (2017). В более новых версиях приставки уязвимость загрузчика была исправлена.

7.6.1. Apple TV: извлечение данных через эксплойт загрузчика

Для извлечения данных из приставок Apple TV используйте **следующую последовательность действий:**

1. Запустите iOS Forensic Toolkit 8.0 (Mac)
2. Подключите приставку к компьютеру через порт USB (для приставки Apple TV 4K потребуется кабель-переходник)
3. Переведите приставку в режим DFU (см. инструкции ниже)
4. Выполните команду **./EIFT_cmd boot**
5. Выполните команду ./EIFT_cmd unlockdata

6. Выполните команду **./EIFT_cmd ramdisk keychain -o {filename}** для извлечения связки ключей

7. Выполните команду **./EIFT_cmd ramdisk tar -o {filename}** для извлечения файловой системы

8. Выполните команду **./EIFT_cmd ssh halt** для выключения приставки

Обратите внимание: для установки эксплойта checkm8 на приставках первой модели Apple TV 3 (A1427) 2021 года вам потребуется дополнительное оборудование – Raspberry Pico, как и для iPhone 4s. Более поздняя версия поддерживается на программном уровне.

7.6.2. Перевод приставок Apple TV в режим DFU

В этом разделе рассматриваются модели Apple TV, подверженные эксплойту загрузчика checkm8. Более новые модели Apple TV 4K, включая модель 2021 года (на чипе A12 Bionic) и 2022 (A15 Bionic), не подвержены уязвимости, используемой эксплойтом checkm8, и в настоящем руководстве ыне рассматриваются.

7.6.2.1. Apple TV 3 (2012 и 2013)

Существует две версии Apple TV 3 с немного различающимися вариантами чипа A5. В оригинальной версии 2012 года (модель A1427) устанавливался чип A5 от iPhone, в котором присутствовало два физических ядра, одно из которых было отключено. В 2013 году, в модели A1469, в приставки начали устанавливать обновлённую версию кристалла – с меньшей площадью и единственным физическим ядром. С точки зрения пользователя различий между этими версиями практически не было, если не считать незначительного уменьшения в новой версии приставки энергопотребления. Нет различий и в том, как эти устройства переводятся в режим DFU. Обе модели подвержены уязвимости, используемой в эксплойте checkm8, и совместимы со способом низкоуровневого анализа, предложенным в iOS Forensic Toolkit 8.

Для перевода Apple TV 3 в режим DFU вам понадобится совместимый с приставкой пульт дистанционного управления. **Итак, перевод в DFU:**

1. Убедитесь, что устройство подключено к источнику питания и включено

2. Убедитесь, что устройство подключено к компьютеру с помощью micro-USB кабеля

3. Нажмите и удерживайте кнопки Down (1) и Menu (2) до тех пор (около 6 секунд), пока LED-индикатор не начнет быстро мигать

4. Отпустите обе кнопки

5. Нажмите и удерживайте кнопки Play (3) и Menu (2) до тех пор (около 6 секунд), пока LED-индикатор не начнет быстро мигать

6. Отпустите обе кнопки

Примечание: важно именно отпустить обе кнопки. Если вы будете удерживать кнопку Menu, то перейти в DFU-режим не удастся.

Кнопки Down, Menu и Play отмечены на рисунке как (1), (2) и (3) соответственно.

Если вы корректно проделали эту последовательность, приставка перейдёт в режим DFU.

7.6.2.2. Apple TV HD (4 поколение)

Оригинальная версия приставки четвёртого поколения вышла в 2017 году под названием **Apple TV 4**. В данной версии появился новый пульт дистанционного управления с поддержкой Siri. В 2021 была выпущена обновлённая версия приставки, в комплектацию которой вошёл новый пульт ДУ. Приставку переименовали в **Apple TV HD**, но каких-либо аппаратных отличий от приставок первого поколения (помимо нового пульта ДУ) устройство не получило. В версии 2021 года также используется чип Apple A8, подверженный всё той же уязвимости, используемой в эксплойте checkm8.

Перевод приставки в режим DFU осуществляется при помощи пульта ДУ. При обычном использовании приставки пульт привязывается к устройству в настройках, однако для перевода устройства в режим DFU привязка пульта не требуется, т.к. для перевода используется инфракрасный канал. Мы протестировали версии как с оригинальным пультом, так и с его обновлённой версией.

В приставках Apple TV 4 и Apple TV HD присутствует выделенный порт USB-C, что упрощает их подключение к компьютеру.

Для перевода Apple TV 4 (Apple TV HD) в режим DFU воспользуйтесь следующей инструкцией.

1. Убедитесь, что устройство подключено к питанию и включено

2. Подключите устройство к компьютеру кабелем USB-C

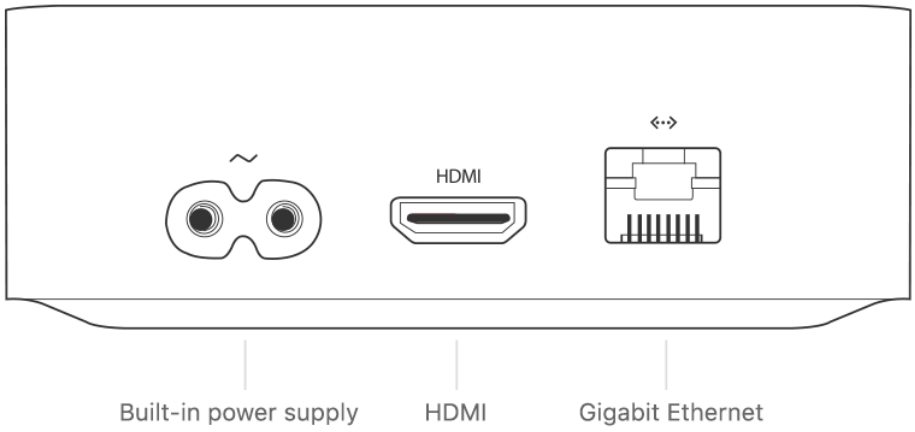
3. Нажмите и удерживайте кнопки Menu и Play до частого мигания светодиодного индикатора (6 секунд)

4. Отпустите обе кнопки

Кнопки Menu и Play на старом и новом пультах ДУ расположены и маркированы по-разному:

7.6.2.3. Apple TV 4K (2017)

Первое поколение телеприставки Apple TV, способной выводить изображение в разрешении 4K, вышло в 2017 году на базе чипа A10X. Этот чип подвержен эксплойту checkm8 и, соответственно, совместим с низкоуровневым методом извлечения данных в iOS Forensic Toolkit. В Apple TV 4K отсутствует встроенный порт USB, посредством которого можно было бы подключить устройство к компьютеру. Ввиду этого вам потребуется специальный адаптер для подключения приставки к компьютеру и ещё один адаптер – для перевода её в режим DFU.



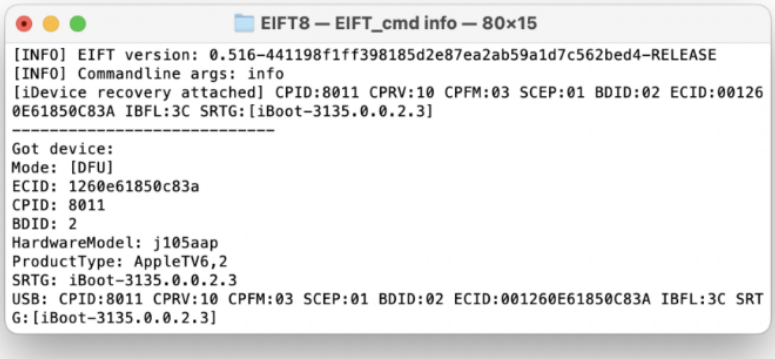
USB-порт кроется под разъёмом Ethernet (RJ45). Подключиться к нему можно при помощи специального адаптера *GoldenEye* (или Foxlink X892), который можно приобрести приблизительно за 40€. При помощи этого адаптера вы сможете подключить приставку к компьютеру и произвести логическое извлечение данных. В то же время одного этого адаптера недостаточно для работы checkm8, т.к. перевод приставки в режим DFU более не производится с пульта дистанционного управления.

Для перевода приставки в режим DFU рекомендуем воспользоваться простым и дешёвым кабелем DCSD (подробнее о нём – в статье The Mysterious Apple DCSD Cable Demystified). Приобрести этот кабель можно приблизительно за 20€.

Для перевода Apple TV 4K в режим DFU используйте следующие шаги.

1. Отключите приставку от питания
2. Подключите кабель DCSD к USB порту компьютера
3. Подключите к кабелю DCSD адаптер GoldenEye (с использованием Lightning)
4. Подключите GoldenEye к приставке Apple TV 4K
5. Включите Apple TV 4K в сеть электропитания

После этого приставка автоматически загрузится в режим DFU:



7.7. Способ 2.3: эксплойт загрузчика и колонки HomePod

Умные колонки Apple HomePod оборудованы скрытым диагностическим портом, который можно использовать для подключения к компьютеру с последующим извлечением данных. Для доступа к данным необходимо будет осуществить частичный разбор колонки с целью получения доступа к скрытому порту, после чего собрать и подключить адаптер для подключения колонки к компьютеру.

Первое поколение умных колонок HomePod было представлено Apple в 2018 году как высококачественная аудиосистема, предназначенная для прослушивания музыки с голосовым управлением посредством ассистента Siri. В колонках был использован достаточно мощный процессор Apple A8, который устанавливался в том числе в iPhone 6. Несмотря на то, что сам iPhone 6 не получил обновления даже до iOS 13, собранный на том же чипе HomePod продолжает обновляться до актуальных версий системы.

Будучи устройством, постоянно подключённым к сети, в колонках HomePod неизбежно должны накапливаться данные, а невозможность установки на устройства кода блокировки делает извлечение этих данных не только возможным, но и достаточно несложным процессом – при условии использования корректных инструментов.

7.7.1. Подготовка к работе

Чтобы получить **доступ к данным в колонках HomePod,** вам потребуются следующие вещи.

1. Колонка HomePod первого поколения, которая была настроена и какое-то время проработала у пользователя. Версия iOS, установленная в колонке, значения не имеет.

2. Специальный адаптер для подключения колонки к USB. Адаптер можно собрать самостоятельно, распечатав подложку на 3D-принтере; потребуется пайка.

3. Компьютер под управлением macOS. На сегодняшний день работа checkm8 поддерживается только на таких компьютерах.

4. Наш инструментарий Elcomsoft iOS Forensic Toolkit 8, чтобы применить эксплойт checkm8, расшифровать связку ключей и извлечь образ файловой системы HomePod. Напомним, вам потребуется компьютер с macOS.

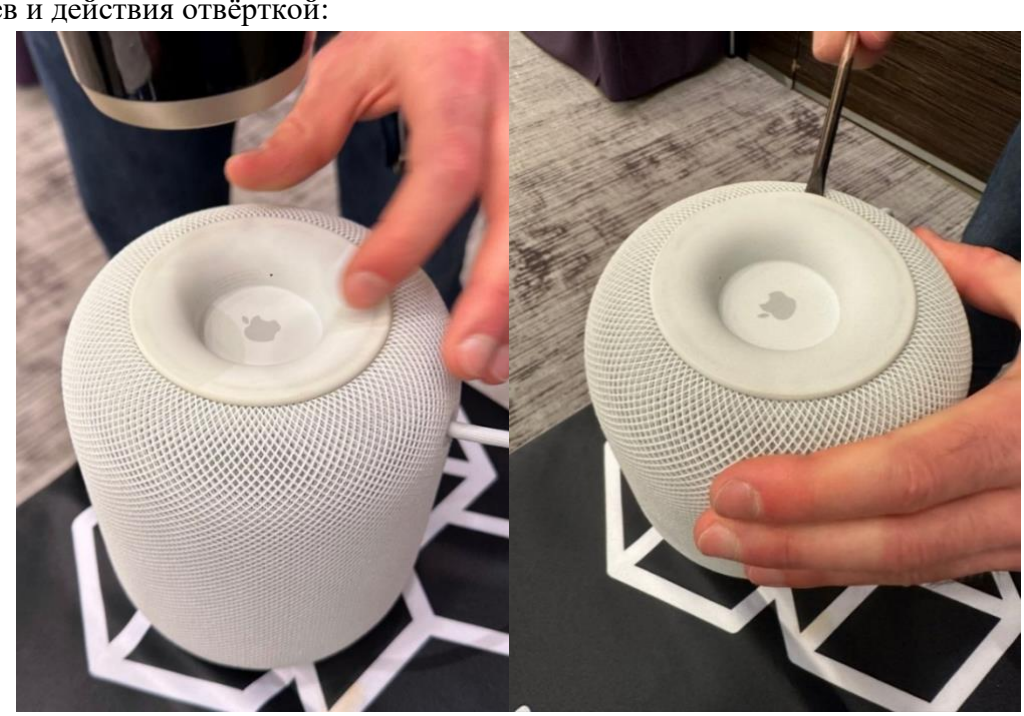
Обратите внимание: вскрытие колонки лишает гарантии.

7.7.2. Скрытый порт диагностики

Под нижней крышкой колонки расположена контактная площадка скрытого диагностического порта. Чтобы получить доступ к контактам, вам потребуется снять крышку (для этого её понадобится нагреть при помощи обычного фена), а для подключения к компьютеру нужно будет собрать адаптер USB.

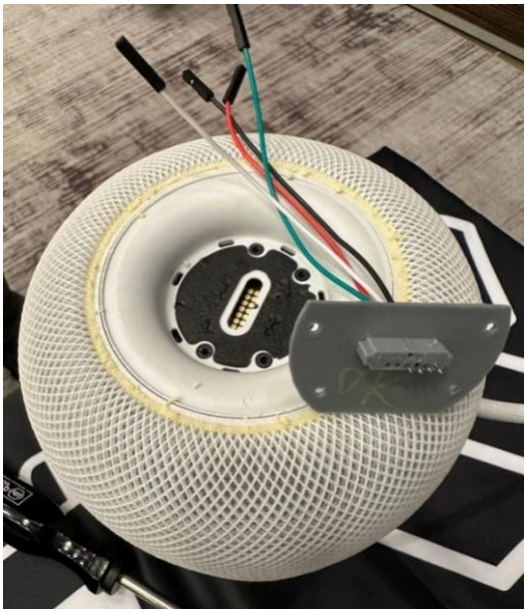
Перед тем, как приступить к работе, убедитесь, что колонка отключена от электросети. Переверните колонку, установив её на мягкое тканевое покрытие.

После этого вам потребуется снять крышку, которая закрывает диагностический порт. Крышка крепится к основанию при помощи клея. Чтобы размягчить клей, основание нужно нагреть при помощи обычного фена, после чего подцепить крышку шлицевой отвёрткой. Чтобы избежать плавления пластика, рекомендуем действовать короткими сессиями, чередуя 10–15 секунд нагрева и аккуратные действия отвёрткой. Нагрев и действия отвёрткой:



Снова нагрев и снова действия отвёрткой. Не торопитесь, и крышку удастся снять без каких-либо повреждений.

Под крышкой находится контактная площадка диагностического порта. Диагностический порт представляет из себя комбинацию USB и UART. Для наших целей доступ к UART не нужен, поэтому рекомендуемый простейший адаптер использует всего четыре провода. Основу адаптера можно распечатать на трёхмерном принтере (см. далее).



Для наших целей подходит самый простой адаптер, поддерживающий только USB. Его основание можно распечатать на 3D-принтере; инструкции и схема доступны в GitHub – Elcomsoft/homepwn[57]. Кроме того, вам понадобится набор винтов M2x6 и набор контактных штифтов Pogo pins. Мы использовали штифты следующего типа:

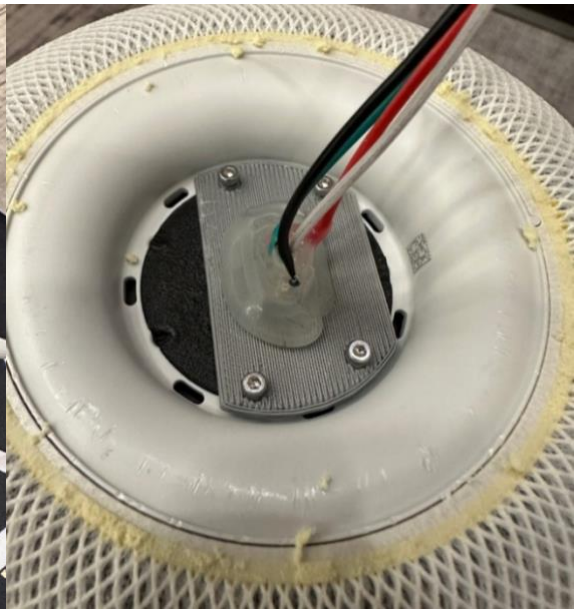
- Внешний диаметр 1.02 мм
- Общая длина 15.8 мм
- Длина штифта 1.4 мм (пример[58])

Печатайте так, чтобы сторона, входящая в HomePod, была обращена вверх. Рекомендуем печатать с опорой. Сначала припаяйте провода к штифтам, и только потом вставляйте их в переходник (иначе пластик, напечатанный на 3D-принтере, расплавится). Убедитесь, что качество пайки на высоком уровне; в противном случае USB-соединение будет очень нестабильным или не будет работать.

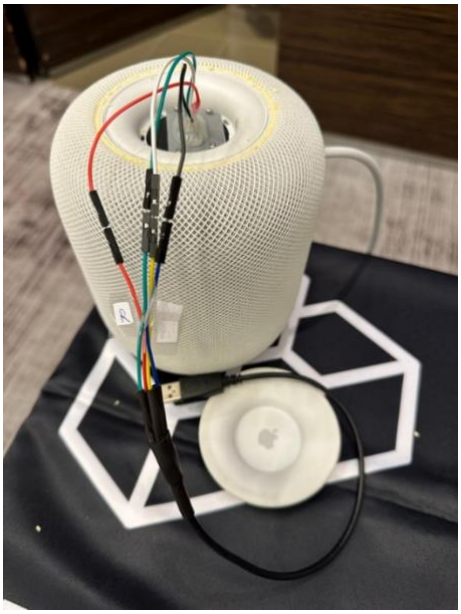
Если вам нужен доступ к UART, то вам потребуется два дополнительных штифта и адаптер 1.8V UART – USB, который мы не использовали за ненадобностью.

Прикрутите адаптер к площадке винтами:

[57] https://github.com/Elcomsoft/homepwn
[58] https://www.amazon.de/dp/B07SKD8Q42



Подключите контакты к коммутационному кабелю (USB breakout):



Наконец, подключите кабель к компьютеру. Если в компьютере есть только порты Type-C, вам понадобится ещё один адаптер с USB-A на USB-C.

7.7.3. Эксплуатация уязвимости checkm8

В умных колонках HomePod первого поколения, основанных на чипах Apple A8, присутствует уязвимость загрузчика, позволяющая извлечь из этих устройств данные посредством эксплойта checkm8. Мы разработали специальный адаптер, позволяющий подключить колонку к компьютеру. При помощи адаптера и инструментария iOS Forensic Toolkit для колонок HomePod первого поколения доступно полноценное извлечение данных, о чём и пойдёт речь в данной статье.

7.7.4. HomePod и checkm8: шпаргалка

Для извлечения данных из колонок HomePod первого поколения используйте следующую последовательность действий:

1. Запустите iOS Forensic Toolkit 8.0 (Mac)
2. Подключите приставку к компьютеру через порт USB (для HomePod потребуется адаптер-переходник)
3. Переведите приставку в режим DFU (см. инструкции ниже)
4. Выполните команду ./EIFT_cmd info
5. Выполните команду ./EIFT_cmd boot -w
6. Выполните команду ./EIFT_cmd unlockdata
7. Выполните команду ./EIFT_cmd ramdisk keychain -o {filename} для извлечения связки ключей
8. Выполните команду ./EIFT_cmd ramdisk tar -o {filename} для извлечения файловой системы
9. [опционально] Выполните команду ./EIFT_cmd ssh halt для выключения приставки

7.7.5. Перевод колонки HomePod в режим DFU

Ввод HomePod первого поколения в режим DFU реализован достаточно просто: нужно перевернуть колонку и включить её в сеть.

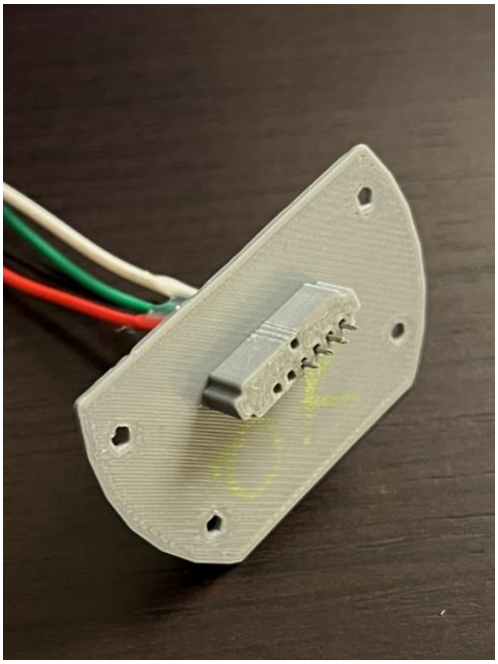
1. Отключите HomePod.
2. Переверните устройство (диагностический порт должен оказаться сверху).
3. Подключите колонку к компьютеру при помощи адаптера.
4. Включите колонку в сеть.

После этого HomePod загружается в режиме DFU.

7.7.6. Извлечение данных из HomePod: последовательность шагов

Рассмотрим процесс извлечения данных из колонок HomePod первого поколения в деталях.

В первую очередь устройство нужно подключить к компьютеру, для чего используется специальный адаптер.

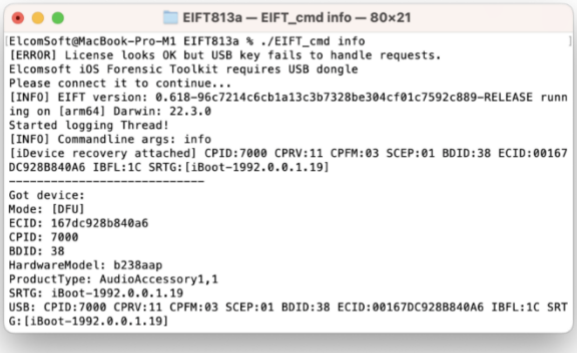


Далее колонка переводится в режим DFU (см. выше), после чего выполните следующую команду:

Следующая команда отобразит информацию об устройстве:

```
./EIFT_cmd ramdisk info
```

Команду имеет смысл запускать для того, чтобы убедиться, что колонка успешно перешла в режим DFU. В этом режиме доступен минимум информации; сюда входят аппаратный идентификатор и версия iBoot, по которой можно определить установленную версию ОС.



Строка "Mode: [DFU]" указывает, что колонка успешно переведена в режим DFU. Теперь выполните команду:

```
./EIFT_cmd boot -w
```

Как только инструментарий определит подключение колонки в режиме DFU, iOS Forensic Toolkit автоматически применит эксплойт. Определяется версия OS, установленная на устройстве, и предоставляется ссылка для скачивания. При наличии нескольких потенциальных совпадений будет выведено несколько ссылок для

скачивания; рекомендуем использовать последнюю ссылку из списка. Загрузите файл по ссылке и перетащите его в окно консоли либо скопируйте URL прошивки (рекомендуется, если компьютер подключён к сети интернет), после чего нажмите ENTER.

В отличие от прошивок для iPhone и iPad, которые доступны в виде полных образов в формате IPSW, прошивки для колонок HomePod труднодоступны и публикуются в виде OTA-обновлений. Для целей извлечения данных достаточно таких образов.

Во многих случаях версия ОС будет автоматически определена EIFT на первом этапе эксплойта на основе версии iBoot и информации об аппаратном обеспечении устройства. Однако в некоторых случаях версия iBoot может соответствовать нескольким сборкам системы или и вовсе не определяться. Если использовать неправильный образ прошивки, у вас будет возможность либо повторить эксплойт с другой версией прошивки, либо продолжить с текущим образом (что в большинстве случаев сработает).

После того, как эксплойт успешно загрузит прошивку, выполните следующую команду:

```
./EIFT_cmd ramdisk unlockdata
```

Команда разблокирует раздел данных и монтирует его в режиме «только для чтения». На колонках HomePod невозможно установить код блокировки, поэтому вводить его не придётся.

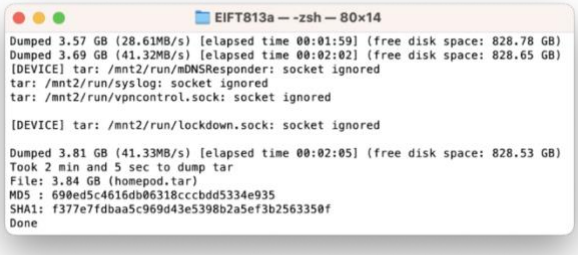
Следующая команда извлекает и расшифровывает связку ключей. Если путь не указан, файл будет сохранён в текущую папку.

```
./EIFT_cmd ramdisk keychain -o {filename}
```

Обратите внимание: в силу того, что на HomePod невозможно установить код блокировки, с них невозможно и получить доступ к облачным данным, защищённым сквозным шифрованием (для сквозного шифрования используется код блокировки экрана или системный пароль). Таким образом, количество записей связки ключей, извлечённых из приставки, будет заметно меньшим, чем можно получить при исследовании iPhone или iPad. В следующей статье мы рассмотрим, какие именно записи из связки ключей доступны в умных колонках.

Следующая команда извлекает образ файловой системы с автоматическим подсчётом и сохранением контрольной суммы (посредством хэш-функции). Значение контрольной суммы сохраняется в той же папке, что и основной файл.

```
./EIFT_cmd ramdisk tar -o {filename}
```



Как видим, из колонки HomePod было извлечено 3.81 ГБ данных файловой системы. В следующей статье мы внимательно проанализируем извлечённые данные и попытаемся определить, насколько эти данные могут представлять интерес для расследования.

Отключить колонку можно обычным образом, для чего можно вытащить шнур питания из розетки либо сделать то же самое, предварительно выполнить команду **./EIFT_cmd ssh halt**

7.8. Способ 3: использование джейлбрейка

Джейлбрейк – собирательное название класса приложений для операционной системы iOS, позволяющих путём эскалации привилегий получить на устройстве права суперпользователя. Эскалацию привилегий осуществляют с использованием

уязвимостей в системе безопасности iOS. С учётом того, что разработчики Apple оперативно исправляют ошибки с выходом обновлений iOS, выход новых и новых утилит для джейлбрейка – процесс непрерывный.

Важно: функционал подавляющего большинства джейлбрейков за единичными исключениями (описанными в следующем разделе) полностью перекрывается функционалом встроенного в EIFT агента-экстрактора, который обеспечивает существенно более безопасное и прозрачное с криминалистической точки зрения извлечение данных.

Важно отметить, что все джейлбрейки – небезопасны и не оптимальны для использования в рамках криминалистического анализа. Джейлбрейки разрабатываются в первую очередь для пользователей, которые хотят вмешаться в работу системы, модифицировать оболочку или установить на iPhone стороннее ПО, минуя процесс установки из App Store. Соответственно, в джейлбрейках предусмотрены механизмы, отключающие проверку цифровой подписи не только у самого приложения джейлбрейка, но и у сторонних приложений.

Другой и не менее важный недостаток классических джейлбрейков с точки зрения эксперта-криминалиста – глубокое и перманентное вмешательство в работу операционной системы. Самый простой способ запустить неподписанное приложение в iOS – это разместить его в системном разделе. Для этого джейлбрейк перемонтирует файловую систему и модифицирует системный раздел, в котором содержатся файлы самой операционной системы. Модификация системного раздела исключает возможность установки последующих обновлений устройства (за исключением полного восстановление прошивки из образа). Невозможно становится полностью и бесследно удалить джейлбрейк из системы – даже несмотря на слепок файловой системы, который создают многие такие утилиты. Фактически, единственным способом восстановить нормальный функционал устройства после использования джейлбрейка становится сброс к заводским настройкам и восстановление прошивки через iTunes.

7.8.1. Сопутствующие риски

Использование джейлбрейка может оказаться рискованным. Актуальные на сегодняшний день джейлбрейки не модифицируют ядро системы и не влияют на процесс загрузки; для получения прав суперпользователя приложение джейлбрейка пользователь должен сам запустить после загрузки.

Использование джейлбрейка в целях криминалистики связано со следующими рисками.

1. Нежелательный выход устройства в интернет в процессе установки джейлбрейка.
2. Изменяются данные на устройстве. Большая часть функционала джейлбрейков не несёт полезной для эксперта-криминалиста нагрузки; всё, что необходимо для анализа – это доступ к устройству и полный доступ к файловой системе. Остальной функционал джейлбрейка скорее вредит, т. к. для его функционирования разработчики идут на модификацию файлов, расположенных как в системном разделе устройства, так и в разделе данных. В худшем случае извлечённые после установки джейлбрейка данные могут оказаться неприменимыми в качестве доказательной базы.

3. Невозможность полноценного восстановления устройства в начальное состояние. Оставшиеся после удаления джейлбрейка следы могут сделать невозможным установку обновлений ОС и мешать нормальному повседневному использованию устройства.

Всех этих проблем можно избежать, если вместо джейлбрейка использовать входящее в состав iOS Forensic Toolkit приложение агента-экстрактора.

7.8.2. В каких случаях имеет смысл использовать джейлбрейк

С учётом рисков, связанных с установкой джейлбрейков, использовать их рекомендуется в ограниченных случаях:

1. Джейлбрейк оказался доступен для устройства, которое не поддерживается ни методом эксплойта загрузчика, ни агентом-экстрактором. Отметим, что такие комбинации достаточно экзотичны; как правило, если для устройства доступен джейлбрейк, то оно уже поддерживается в iOS Forensic Toolkit или одним, или другим методом.
2. Для извлечения данных из iPhone 4s, для которого существуют джейлбрейки, но метод прямого извлечения через эксплойт загрузчика слишком сложен, т. к. требует использования аппаратного микроконтроллера. Даже в этом случае рекомендуем воспользоваться методом, использующим эксплойт загрузчика.

Кроме того, джейлбрейки иногда используются, если у эксперта нет доступа к компьютеру под управлением macOS. Такой компьютер потребуется для использования прямого извлечения посредством эксплойта загрузчика, а также для подписи агента-экстрактора обычной учётной записью Apple ID, не зарегистрированной в программе для разработчиков.

7.8.3. Извлечение данных с использованием джейлбрейка

Способ извлечения через джейлбрейк возможен, если на устройстве установлен джейлбрейк и работает SSH-сервер. Для доступа по SSH необходимо также знать пароль пользователя root (по умолчанию этот пароль – “Alpine”, без кавычек и с большой буквы).

Данный метод обычно позволяет извлечь полный образ файловой системы и связку ключей. Тем не менее, объем доступных данных может различаться в зависимости от конкретного джейлбрейка. Для того, чтобы извлечь файловую систему и связку ключей, на устройство загружается специальный код, который после выполнения удаляется. Записи о доступе по SSH могут остаться в журналах системы; к сожалению, этого нельзя избежать, но и на целостность данных подобные записи особого влияния не окажут. Если физическое извлечение посредством эксплойта загрузчика или низкоуровневое извлечение агентом-экстрактором для исследуемого устройства недоступно, то извлечение на основе джейлбрейка может оказаться единственным доступным способом получить полный доступ к содержимому устройства.

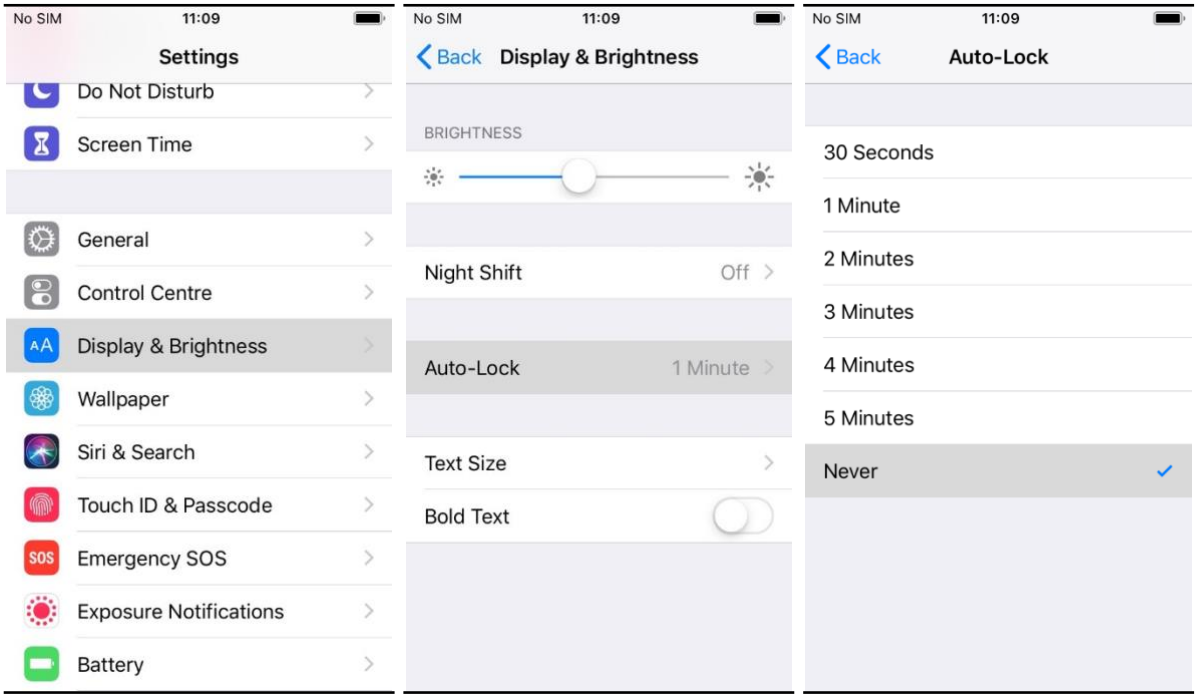
В основе метода лежит возможность подключиться к устройству через SSH. Для этого необходимо знать пароль пользователя root (если он отличается от стандартного “Alpine”). Набор команд ./EIFT_cmd jb предоставляет следующие опции:

- предотвращение блокировки экрана
- копирование связки ключей
- копирование системного/пользовательского раздела в виде tar-архива
- создание образа диска

Важно: в течение всего времени извлечения данных, устройство должно оставаться разблокированным. В противном случае некоторые файлы или записи связки ключей окажутся недоступными.

Чтобы предотвратить автоблокировку (включена по умолчанию), в настройках устройства перейдите в меню *Settings* → *Display & Brightness* → *Auto Lock* и выберите значение *Never*.

Отключение автоблокировки проиллюстрировано ниже:



Утилита autolocknever

Иногда отключить автоблокировку напрямую из настроек невозможно (например, когда на устройство установлен профиль управления).

В таких случаях поможет утилита autolocknever, которая изменит необходимые конфигурационные файлы напрямую:

```
./EIFT_cmd jb autolocknever
```

Копирование связки ключей

Перед копированием связки ключей устройство должно быть разблокировано. Проследите также, что экран устройства остаётся разблокированным во время всего процесса копирования.

Следующая команда сохранит связку ключей в файле *keychain.xml*:

```
./EIFT_cmd jb keychain -o keychain.xml
```

Создание TAR-архива

Перед созданием tar-архива устройство должно быть разблокировано. Проследите также, что экран устройства остаётся разблокированным во время всего процесса создания архива (см. выше).

Следующая команда создаст tar-архив *data.tar*, содержащий все файлы пользовательского раздела:

```
./EIFT_cmd jb tar -o data.tar
```

Если вам нужен tar-архив системного раздела (*system.tar*), то запустите такую команду:

```
./EIFT_cmd jb tar --system -o system.tar
```

Создание образа диска

Вы также можете создать полный образ диска для дальнейшего исследования. Самый простой способ – вызвать следующую команду:

```
./EIFT_cmd jb diskdump -o dump.dmg
```

При вызове *diskdump* без каких-либо параметров произойдёт одно из следующего:

1. Если формат файловой системы **HFS**, то создастся образ пользовательского раздела**/dev/disk0s1s2** (Data)
2. Если формат файловой системы **APFS**, то создастся образ всего диска **/dev/disk0s1** (Full storage)

Для устройств с файловой системой **HFS** возможно передать дополнительный параметр --system. В таком случае *diskdump* создаст образ системного раздела.

```
./EIFT_cmd jb diskdump --system -o dump.dmg
```

Для файловой системы **APFS** доступно только создание образа всего диска.

Вы можете также вручную передать параметры --system и --data и создать образ раздела **/dev/disk0s1**.

```
./EIFT_cmd jb diskdump --system --data -o dump.dmg
```

7.8.4. Возможные проблемы

При закрытии iOS Forensic Toolkit закройте оба окна программы, включая фоновый процесс Secure channel.

Если iOS Forensic Toolkit подключается к iPhone, но результат его работы не соответствует подключённому устройству, закройте оба окна программы и убедитесь, что на компьютере, на котором работает iOS Forensic Toolkit, выключен Wi-Fi. Если Wi-Fi выключен, но проблема не исчезает, отключите и проводное соединение компьютера с сетью: это может помочь, если в вашей локальной сети присутствуют другие устройства с iOS.

8. Устаревшие устройства: 32-разрядные модели без Secure Enclave

Для устаревших устройств, оборудованных 32-разрядными процессорами, доступен вариант полного физического анализа, включая взлом кода блокировки экрана. Обратите внимание: iPhone 4s поддерживается посредством дополнительного аппаратного модуля, использование которого описано в соответствующем разделе.

8.1. Шпаргалка: извлечение данных из 32-разрядных устройств

Переведите устройство в режим recovery и установите флаг автозагрузки:

```
./EIFT_cmd tools autobootFalse
```

После этого переведите устройство в режим DFU. После перехода устройства в режим DFU выполните следующую команду в iOS Forensic Toolkit:

```
./EIFT_cmd boot -w
```

Команда запустит EIFT в режиме ожидания. Как только программа определит, что к компьютеру подключено устройство в режиме DFU, она сразу запускает эксплойт.

Внимание: в некоторых случаях для установки эксплойта может потребоваться две-три попытки. Если на этом этапе возникает ошибка, повторно введите телефон в DFU и повторите попытку.

Код определяет версию ОС, установленную на iPhone, и предоставляет ссылку для скачивания. Наше решение для извлечения не использует операционную систему, установленную на iPhone, для загрузки устройства. Вместо этого в ОЗУ устройства загружается отдельная исправленная версия оригинальной прошивки Apple. Загрузите файл .ipsw по ссылке и перетащите его в окно консоли.

Далее используйте следующие команды:

Монтирование файловой системы:

```
./EIFT_cmd ramdisk mount
```

Может потребоваться проверка целостности файловой системы командой fsck (в случаях нештатного отключения телефона):

```
./EIFT_cmd ramdisk fsck_hfs –data
```

Разблокировка

Если iPhone заблокирован, а пароль неизвестен, выполните следующую команду, чтобы запустить перебор паролей:

```
./EIFT_cmd ramdisk passcode
```

Извлечение ключей:

```
./EIFT_cmd ramdisk dumpkeys -p <passcode> -o keys.plist
```

Извлечение раздела данных:

```
./EIFT_cmd ramdisk diskdump -o data.dmg
```

Расшифровка раздела данных ранее извлечёнными ключами:

```
./EIFT_cmd hfstool -i data.dmg -o data_dec.dmg -k
keys.plist -j 16 -d
```

Расшифровка связки ключей:

```
./EIFT_cmd tools keychain -i data.dmg -o keychain.xml -
k keys.plist
```

Для ускорения расшифровки вы можете добавить параметр -j для использования нескольких потоков. Например, "-j 10" будет использовать десять потоков для расшифровки.

Выключение устройства:

```
./EIFT_cmd ssh halt
```

Восстановление флага автозагрузки:

Если работа с устройством завершена, и устройство требуется вернуть владельцу, отключите режим блокирования автозагрузки. Для этого перезагрузите устройство либо выключите его командой ssh halt, после чего снова включите. После того, как устройство попадёт в режим recovery, выполните указанную ниже команду. После этого устройство автоматически перезагрузится:

```
./EIFT_cmd tools autobootTrue
```

Анализ данных: монтирование извлечённого образа HFS в формате DMG на компьютерах с Windows:

```
eift_cmd hfstool --mount -i data.dmg -k keys.plist
```

либо

```
eift_cmd hfstool --mount -i data_dec.dmg
```

Первая команда монтирует снятый, но ещё не расшифрованный образ с использованием соответствующего файла с ключами. Вторая – монтирует уже расшифрованный образ.

8.2. Извлечение данных и подбор кода блокировки

Для извлечения данных и подбора кода блокировки экрана используется метод полного извлечения. Этот метод – лучший способ извлечения данных с устройств, не оборудованных аппаратным сопроцессором безопасности Secure Enclave. Он идеально подходит для криминалистического анализа, так как гарантированно не вносит никаких

изменений в данные устройства и имеет ряд преимуществ по сравнению с другими методами.

Полный список устройств, которые поддерживаются данным методом:

- iPhone 3G/3GS/4/4s/5/5c
- iPod Touch 2/3/4/5
- iPad 1/2/3/4
- iPad Mini (1st gen)
- Apple TV 2/3

Процедура извлечения состоит из трех этапов: создание полного образа раздела данных, получение полного набора ключей шифрования и расшифровка образа диска. Если устройство защищено неизвестным кодом блокировки, его можно восстановить в процессе работы.

Процедура извлечения состоит из нескольких этапов:

1. ввод устройства в режим Recovery и сброс флага автозагрузки
2. ввод устройства в режим DFU
3. создание полного образа раздела данных
4. получение BFU ключей
5. подбор кода блокировки экрана, если он неизвестен
6. получение полного набора ключей шифрования
7. расшифровка образа диска
8. извлечение и расшифровка связки ключей

Рассмотрим каждый этап в подробностях.

8.2.1. Флаг автозагрузки

При исследовании устройства iOS Forensic Toolkit **первое, что необходимо сделать** — это установить в загрузчике специальный флаг, благодаря которому при случайной перезагрузке устройство не станет загружать iOS, а запустится в режиме восстановления. Это помогает сохранить криминалистическую чистоту исследования в случае ошибок при вводе в режим DFU. Для этого достаточно загрузить устройство в режиме Recovery, после чего выполнить в терминале iOS Forensic Toolkit со следующим параметром:

```
./EIFT_cmd tools autobootFalse
```

8.2.2. Ввод устройства в режим DFU

На первом шаге необходимо ввести устройство в режим DFU. Сделать это можно только вручную. Если одна из кнопок устройства не функционирует, см. раздел **Аппаратный ввод в режим DFU: когда не работают кнопки** в дополнительных материалах. Существует несколько вариантов, но мы рекомендуем такую последовательность:

1. Начальное состояние: телефон должен быть выключен и не подключён к компьютеру.

2. Нажмите кнопку *Home* (единственную/центральную на лицевой панели), и удерживая её, подключите кабель Lightning. Отпустите *Home*, когда на экране устройства появится картинка «Подключитесь к iTunes».

3. Одновременно нажмите *Home* и *Sleep/Power* (кнопка блокировки на верхнем торце устройства) и удерживайте их 8 секунд (на некоторое время на экране появится логотип Apple).

4. Отпустите кнопку *Sleep/Power*, но продолжайте удерживать *Home* ещё 8 секунд

Если всё сделано правильно, экран аппарата останется чёрным, а в iTunes или Finder (в зависимости от используемой версии macOS) телефон появится как *iPhone Recovery Mode (режим восстановления)*. Всё готово к следующим шагам, которые уже автоматизированы.

8.2.3. Создание образа пользовательского раздела

Следующая команда создаст побитовый образ пользовательского раздела:

```
./EIFT_cmd ramdisk diskdump -o data.dmg
```

Примечание: если устройство завершило работу некорректно, либо файловая система повреждена, возможна такая ошибка:

```
    [Error] [!] Data partition is in an unclean state,
please run fsck first to fix potential inconsistencies!

    Alternatively pass --unclean, to ignore this and
proceed with dumping anyways!
```

В таком случае к команде можно добавить флаг --unclean, чтобы проигнорировать ошибку и создать образ в любом случае.

```
./EIFT_cmd ramdisk diskdump --unclean -o data.dmg
```

Во время процедуры создания образа данные на устройстве никак не модифицируются.

Помимо пользовательского раздела можно опционально создать и образ системного диска. Системные разделы обычных устройств не содержат ничего интересного, однако установленные джейлбрейки и вредоносное программное обеспечение могут вносить значимые изменения в разделе, которые можно проанализировать.

```
./EIFT_cmd ramdisk diskdump --system -o system.dmg
```

Примечание: если устройство завершило работу некорректно, либо файловая система повреждена, возможна ошибка. В таком случае добавьте к команде флаг --unclean, как это было описано выше.

8.2.4. Получение BFU ключей

Ключи BFU извлекаются независимо от того, известен ли код блокировки экрана. С помощью этих ключей можно расшифровать ограниченное количество данных; они необходимы и для доступа к полному набору ключей шифрования, которые нужны для полной расшифровки данных (см. следующий раздел).

Для извлечения BFU ключей выполните следующую команду:

```
./EIFT_cmd ramdisk dumpkeys -n -o keys_bfu.plist
```

8.2.5. Получение полного набора ключей шифрования

Для доступа к пользовательским данным необходим полный набор ключей шифрования, без него будет расшифровано только ограниченное число данных (BFU).

Важно: следующие действия необходимо выполнять на том же устройстве, с которого был снят образ диска.

Примечание: извлечь набор ключей можно проводить, даже если на устройстве произошли какие-то изменения с момента снятия образа диска. Эти изменения никак не повлияют на целостность образа, созданного ранее.

8.2.5.1. Извлечение файла systembag.kb

Для извлечения системной сумки с ключами (systembag.kb) вам понадобится образ диска (data.dmg) и соответствующие ключи BFU (keys_bfu.plist).

Примечание: на этом этапе можно также использовать и полный набор ключей. Следующая команда извлечёт системную сумку с ключами:

```
./EIFT_cmd hfstool -i data.dmg -p /keybags/systembag.kb
-e -o systembag.kb -k keys_bfu.plist --no-passcode
```

Команда создаст новый файл под именем systembag.kb. Проверьте, что файл расшифрован корректно: он должен начинаться с bplist. На UNIX системах это можно проверить следующей командой:

```
head -c 6 systembag.kb | hexdump -C
```

Ожидаемый вывод:

```
00000000    62 70 6c 69 73 74  |bplist|

00000006
```

Как вариант, полученный файл можно попытаться открыть в любом plist-редакторе. Если файл открывается, то расшифровка прошла успешно.

8.2.5.2. Подбор кода блокировки экрана

Если код блокировки экрана неизвестен, на этом этапе его можно попробовать подобрать.

Для подбора кода блокировки экрана вам понадобится системная сумка с ключами (systembag.kb) и BFU ключи (keys_bfu.plist). Следующая команда запустит подбор пароля с параметрами по умолчанию:

```
./EIFT_cmd ramdisk passcode -b systembag.kb -k
keys_bfu.plist
```

Возможно также передать утилите passcode дополнительные аргументы, с помощью параметра --argument

```
./EIFT_cmd ramdisk passcode --argument='-y'
(проверяются только 4-значные варианты PIN)

./EIFT_cmd ramdisk passcode --argument='-z'
(проверяются только 4-значные варианты PIN)
```

Полный список аргументов утилиты passcode можно увидеть, передав ей параметр '-h'

```
./EIFT_cmd ramdisk passcode --argument='-h'
```

Утилита passcode поддерживает также атаку по словарю. Для этого передайте путь к файлу со словарём через параметр -i, как это показано ниже:

```
EIFT_cmd ramdisk passcode -i /path/to/dictionary
```

8.2.5.3. Получение полного набора ключей шифрования

Для получения полного набора ключей шифрования потребуется всё полученное на предыдущих этапах: системная сумка с ключами (systembag.kb), BFU ключи (keys_bfu.plist) и код блокировки экрана.

Следующая команда извлекает полный набор ключей шифрования:

```
./EIFT_cmd ramdisk dumpkeys -k keys_bfu.plist -b
systembag.kb -o keys.plist -p <PASSCODE>
```

Замените <PASSCODE> на код блокировки экрана. Например, если по блокировки 0000, то команда будет выглядеть следующим образом:

```
./EIFT_cmd ramdisk dumpkeys -k keys_bfu.plist -b
systembag.kb -o keys.plist -p 0000
```

Если пароля на устройстве нет, параметр -p можно опустить.

В результате создастся новый файл keys.plist, содержащий все ключи, необходимые для расшифровки пользовательских данных.

8.2.6. Расшифровка образа диска

Для расшифровки образа диска (data.dmg) потребуется полный набор ключей шифрования (keys.plist). О том, как получить ключи с того же устройства, рассказано в предыдущем разделе.

Чтобы расшифровать образ диска, запустите следующую команду:

./EIFT_cmd hfstool -i data.dmg -o data_dec.dmg -k keys.plist -j 16 -d

Примечание: параметр -j устанавливает количество потоков, используемых для расшифровки. На современных компьютерах рекомендуется использовать 16 потоков. Количество потоков можно увеличить или уменьшить в зависимости от вычислительной мощности компьютера.

По завершении расшифровки утилита выдаст отчёт об ошибках (если они есть) и статистику по расшифрованным файлам:

```
Summary

[.] Took    0 minutes and      0 seconds to unwrap 6107
filekeys [.] Took      0 minutes and      0 seconds to copy
dmg

[-] Took    0 minutes and      2 seconds to decrypt
files [*] Total files 6133

[*] Decryption succeded on 6107 files [*] Not decrypted
0 files

[*] Not encrypted files 26
```

8.2.7. Извлечение связки ключей

В связке ключей iOS хранит пароли пользователя. Каждая запись из связки ключей дополнительно зашифрована; для их расшифровки понадобится полный набор ключей шифрования, извлечённый ранее. Следующая команда извлечёт связку ключей из образа диска и расшифрует её содержимое:

```
./EIFT_cmd tools keychain -i data.dmg -k keys.plist -o
keychain.xml
```

Не имеет значения, зашифрованный или расшифрованный образ подаётся на вход команде. Если образ зашифрован, необходимые файлы будут расшифрованы на лету.

В результате работы команды создастся новый файл с именем keychain.xml.

8.2.8. Окончание работы с устройством

Если работа с устройством завершена, и устройство требуется вернуть владельцу, отключите режим блокирования автозагрузки. Для этого перезагрузите устройство либо выключите его командой ssh halt, после чего снова включите. После того, как устройство попадёт в режим recovery, выполните указанную ниже команду. После этого устройство автоматически перезагрузится:

```
./EIFT_cmd tools autobootTrue
```

8.2.9. Анализ данных

Извлечённый образ диска в формате DMG с файловой системой HFS можно смонтировать в виде диска на с Windows одной из двух команд:

```
eift_cmd hfstool --mount -i data.dmg -k keys.plist
```

либо

```
eift_cmd hfstool --mount -i data_dec.dmg
```

Первая команда монтирует снятый, но ещё не расшифрованный образ с использованием соответствующего файла с ключами. Вторая – монтирует уже расшифрованный образ.

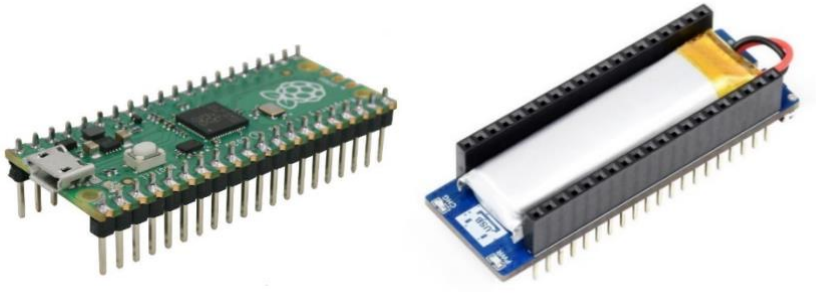
9. iPhone 4s

В iPhone 4s используется контроллер USB, требующий особого подхода. В этой модели присутствует уязвимость загрузчика, эксплуатация которой позволяет как разблокировать устройство, заблокированное неизвестным кодом блокировки, так и извлечь из него данные. Эксплуатация данной уязвимости технически сложна и требует использования дополнительного аппаратного обеспечения – устройства Raspberry Pi Pico с особой прошивкой, которая поставляется в составе восьмой версии iOS Forensic Toolkit.

9.1. Сборка микроконтроллера Pico

Для работы с iPhone 4s и подобными устройствами вам потребуется собрать устройство на основе микроконтроллера Raspberry Pi Pico. В силу того, что на плате установлен единственный порт USB, вам также потребуется источник питания, в качестве которого мы рекомендуем использовать аккумулятор. Вам потребуются:

Плата Raspberry Pi Pico в варианте с припаянными контактами, источник питания, включая аккумулятор:

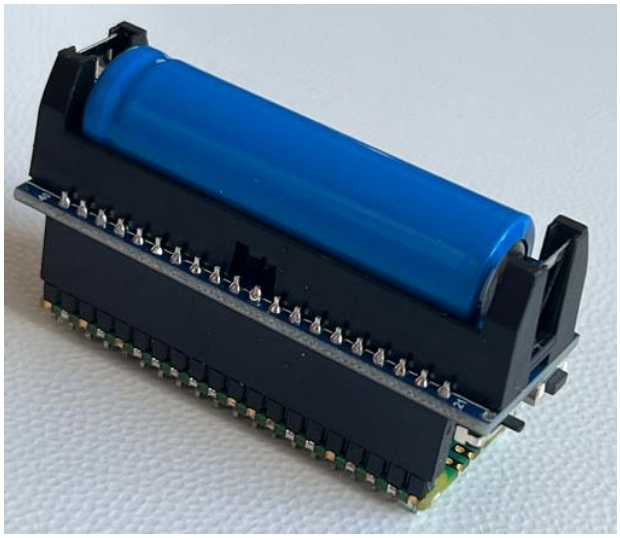


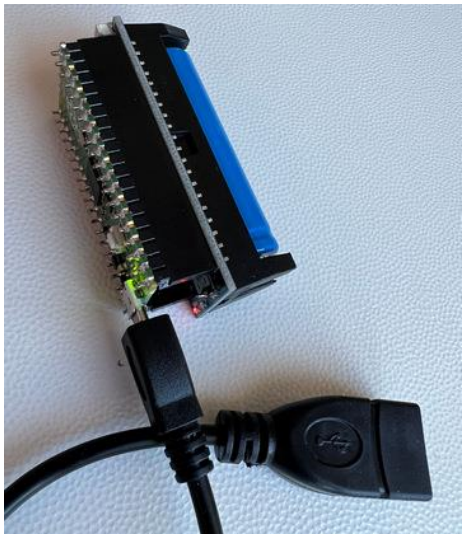
Можно использовать и такой источник питания (сайт производителя[59]):

Кабель micro-USB OTG:

Также потребуется обычный кабель micro-USB для прошивки платы.
Устройство в сборе выглядит следующим образом:

[59] https://www.waveshare.com/pico-ups-a.html





9.1.1. Подробнее об источнике питания

Показанное выше решение в виде аккумулятора для платы Pico на основе литиевого элемента питания 14500N обеспечивает напряжение в 3,7В, чего достаточно для применения эксплойта, но не хватает для перевода iPhone в DFU. Перевод в DFU осуществляется вручную, после чего iPhone подключается к плате Pico.

9.1.2. Прошивка микроконтроллера Pico

Прежде чем подключить iPhone к плате Pico, вам нужно будет прошить его специальной версией прошивки. Образ встроенного ПО предоставляется с iOS Forensic Toolkit.

Для прошивки Raspberry Pi Pico проделайте следующие шаги.

1. Убедитесь, что на компьютере установлен iOS Forensic Toolkit 8.0 более новой.

2. Зажмите кнопку на плате Pico.

3. Не отпуская кнопки, подключите плату к Mac при помощи обычного кабеля micro-USB.

4. Плата отобразится в виде внешнего накопителя.

5. Перенесите на этот накопитель файл “picom8.uf2” из корневой папки с установленным EIFT.

6. Прошивка будет установлена, а Pico перезагрузится.

7. После окончания загрузки микроконтроллер готов к работе.

9.1.3. Дальнейшие действия

На первом шаге необходимо подключить устройство к компьютеру, чтобы перевести его в режим DFU, затем отключить его от компьютера и подключить к плате Pico.

- Устройство не перейдёт в режим DFU, если напряжение менее 5В.
- Устройство не перейдёт в режим DFU, если оно вообще ни к чему не подключено.

Для перевода в DFU выполните следующие действия:

1. Подключите iPhone к компьютеру.

2. Выключите телефон.
3. Нажмите и удерживайте кнопку питания в течение 3 секунд.
4. Нажмите и удерживайте кнопку «Домой», не отпуская кнопку питания в течение 10 секунд.
5. Отпустите кнопку питания, но продолжайте удерживать кнопку «Домой».
6. Продолжайте удерживать кнопку «Домой», пока iTunes не предупредит вас о том, что он обнаружил устройство в режиме восстановления.

Экран телефона должен оставаться пустым. Если присутствует логотип iTunes, вы находитесь в Recovery, а не в DFU. Если это так, попробуйте перевести телефон в DFU ещё раз.

Когда iPhone находится в DFU, подключите его к плате Raspberry Pi Pico. Эксплойт применяется автоматически сразу после подключения. После успешного применения эксплойта на Pico будет выведена индикация в виде повторяющихся коротких миганий светодиода, чередующихся длинными паузами. Коды ошибок и дополнительную информацию о состоянии светодиодов см. в руководстве пользователя, поставляемом с EIFT.

После применения эксплойта отключите iPhone от Pico и подключите его к компьютеру. Далее используйте iOS Forensic Toolkit в обычном режиме, следуя процессу разблокировки и извлечения для 32-разрядных устройств (iPhone 4 и 5/5c).

9.1.4. Особенности установки эксплойта

В некоторых случаях для установки эксплойта может потребоваться две-три попытки. Если на Pico возникает ошибка, повторно введите телефон в DFU, снова подключите его к Pico и повторите попытку.

9.1.5. Дальнейшие действия

Дальнейшие действия совпадают с описанными в разделе Переведите устройство в режим recovery и установите флаг автозагрузки:

```
./EIFT_cmd tools autobootFalse
```

После этого переведите устройство в режим DFU. После перехода устройства в режим DFU выполните следующую команду в iOS Forensic Toolkit:

```
./EIFT_cmd boot -w
```

Команда запустит EIFT в режиме ожидания. Как только программа определит, что к компьютеру подключено устройство в режиме DFU, она сразу запускает эксплойт.

Внимание: в некоторых случаях для установки эксплойта может потребоваться две-три попытки. Если на этом этапе возникает ошибка, повторно введите телефон в DFU и повторите попытку.

Код определяет версию ОС, установленную на iPhone, и предоставляет ссылку для скачивания. Наше решение для извлечения не использует операционную систему, установленную на iPhone, для загрузки устройства. Вместо этого в ОЗУ устройства

загружается отдельная исправленная версия оригинальной прошивки Apple. Загрузите файл .ipsw по ссылке и перетащите его в окно консоли.

Далее используйте следующие команды:

Монтирование файловой системы:

```
./EIFT_cmd ramdisk mount
```

Может потребоваться проверка целостности файловой системы командой fsck (в случаях нештатного отключения телефона):

```
./EIFT_cmd ramdisk fsck_hfs -data
```

Разблокировка

Если iPhone заблокирован, а пароль неизвестен, выполните следующую команду, чтобы запустить перебор паролей:

```
./EIFT_cmd ramdisk passcode
```

Извлечение ключей:

```
./EIFT_cmd ramdisk dumpkeys -p <passcode> -o keys.plist
```

Извлечение раздела данных:

```
./EIFT_cmd ramdisk diskdump -o data.dmg
```

Расшифровка раздела данных ранее извлечёнными ключами:

```
./EIFT_cmd hfstool -i data.dmg -o data_dec.dmg -k
keys.plist -j 16 -d
```

Расшифровка связки ключей:

```
./EIFT_cmd tools keychain -i data.dmg -o keychain.xml -
k keys.plist
```

Для ускорения расшифровки вы можете добавить параметр -j для использования нескольких потоков. Например, "-j 10" будет использовать десять потоков для расшифровки.

Выключение устройства:

```
./EIFT_cmd ssh halt
```

Восстановление флага автозагрузки:

Если работа с устройством завершена, и устройство требуется вернуть владельцу, отключите режим блокирования автозагрузки. Для этого перезагрузите устройство либо выключите его командой ssh halt, после чего снова включите. После того, как устройство попадёт в режим recovery, выполните указанную ниже команду. После этого устройство автоматически перезагрузится:

```
./EIFT_cmd tools autobootTrue
```

Анализ данных: монтирование извлечённого образа HFS в формате DMG на компьютерах с Windows:

```
eift_cmd hfstool --mount -i data.dmg -k keys.plist
```

либо

```
eift_cmd hfstool --mount -i data_dec.dmg
```

Первая команда монтирует снятый, но ещё не расшифрованный образ с использованием соответствующего файла с ключами. Вторая – монтирует уже расшифрованный образ.

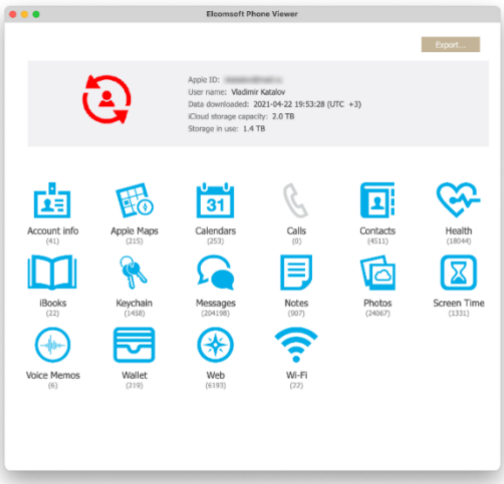
Извлечение данных и подбор кода блокировки.

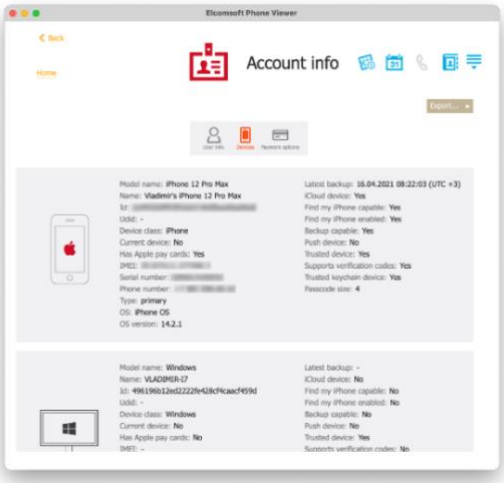
10. Просмотр и анализ данных

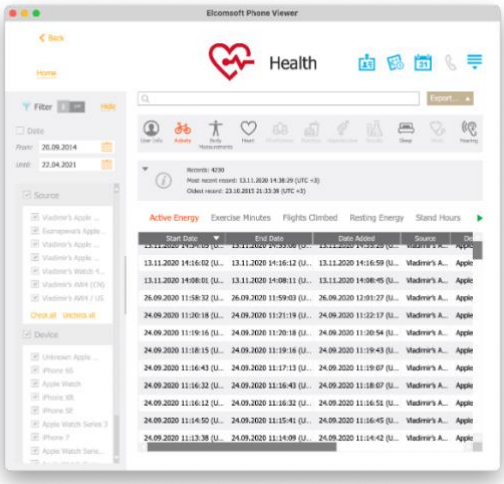
Анализу информации, извлечённой из устройств под управлением iOS, посвящены многочисленные работы. В данной публикации мы не будем подробно останавливаться на аналитике, ограничившись рассмотрением источников данных и инструментов, которые можно использовать для их анализа.

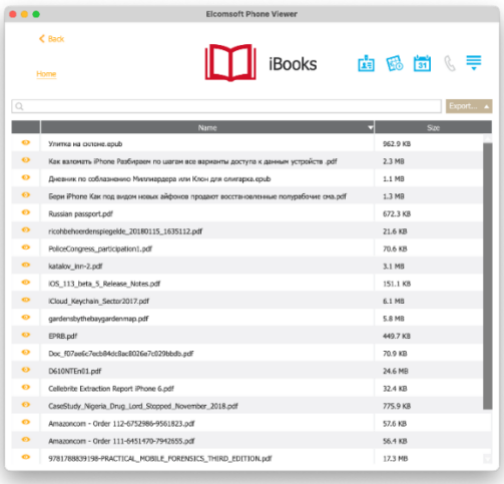
Для анализа данных, извлекаемых из разнообразных источников утилитами производства «Элкомсофт», рекомендуем воспользоваться программой Elcomsoft Phone Viewer, которая поддерживает большую часть соответствующих форматов данных. Приведённые ниже скриншоты дают представление о возможностях программы.

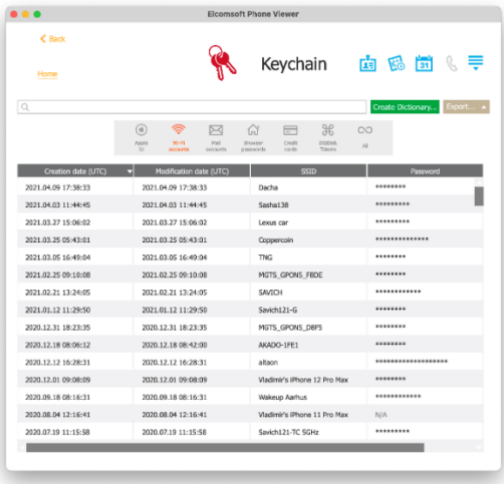
В приложении поддерживаются следующие категории данных:

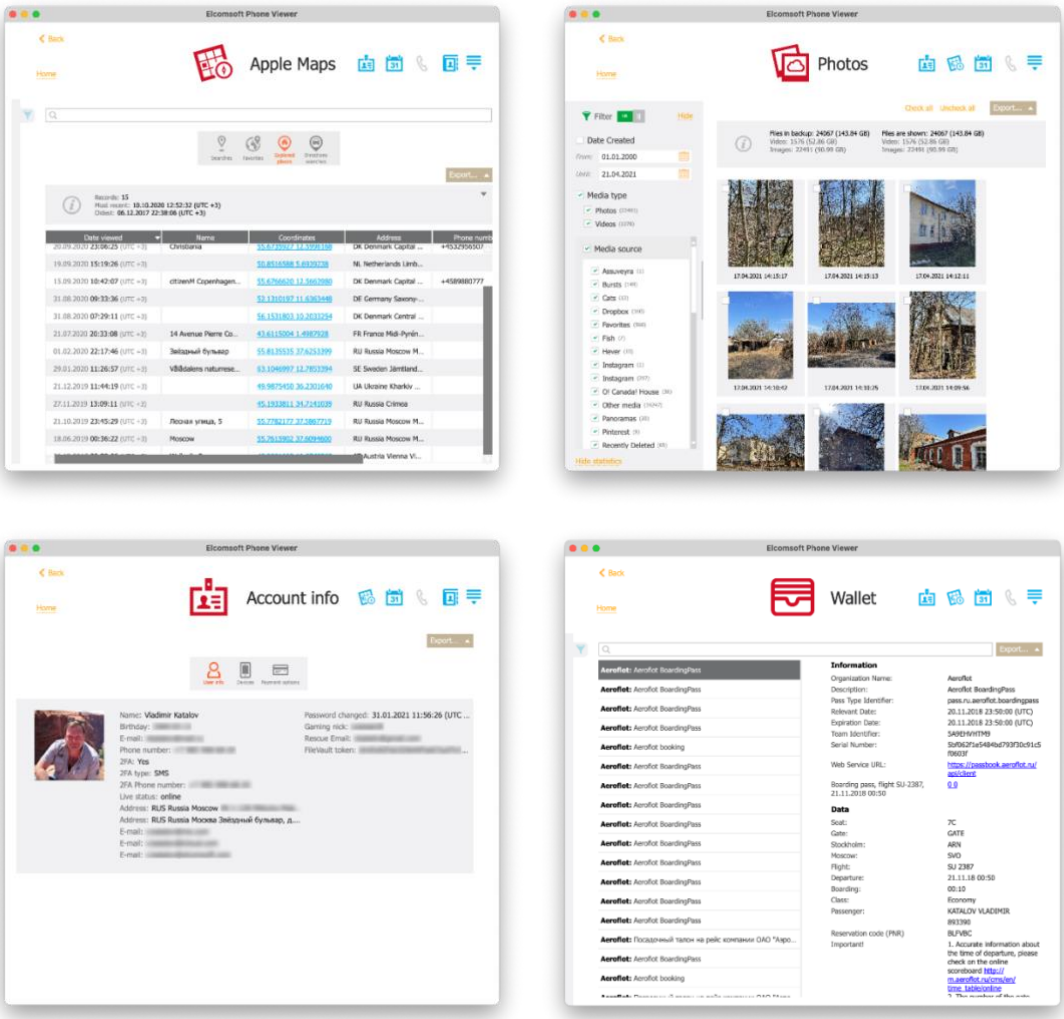

Elcomsoft Phone Viewer
Export...
Apple ID:
User name: Vladimir Katalov
Data downloaded: 2021-04-22 19:53:28 (UTC +3)
iCloud storage capacity: 2.0 TB
Storage in use: 1.4 TB
Account info
Apple Maps
Calendars
Calls
Contacts
Health
iBooks
Keychain
Messages
Notes
Photos
Screen Time
Voice Memos
Wallet
Web
Wi-Fi


Elcomsoft Phone Viewer
Account info


Elcomsoft Phone Viewer
Health


Elcomsoft Phone Viewer
iBooks


Elcomsoft Phone Viewer
Keychain



10.1.Источники данных

Инструменты для извлечения данных из устройств под управлением iOS производства «Элкомсофт» возвращают данные в нескольких различных форматах, называемых далее «источниками данных». Ниже перечислены доступные для анализа источники данных и методы их исследования.

Резервная копия в формате iTunes

Инструмент для создания: Elcomsoft iOS Forensic Toolkit; Elcomsoft Phone Breaker (при скачивании облачных резервных копий из iCloud с выключенными опциями восстановления оригинальной структуры каталогов).

Инструменты для анализа: Elcomsoft Phone Viewer, любые сторонние пакеты, воспринимающие формат резервных копий iTunes.

Заметки: при создании резервной копии посредством Elcomsoft iOS Forensic Toolkit и отсутствии пароля на резервной копии будет установлен пароль “123”. Этот пароль необходимо ввести при открытии резервной копии. Если резервная копия защищена неизвестным паролем, его необходимо будет восстановить в Elcomsoft Phone Breaker или Elcomsoft Distributed Password Recovery.

Резервная копия с восстановленной структурой каталогов

Инструмент для создания: Elcomsoft Phone Breaker (при скачивании облачных резервных копий из iCloud с опцией восстановления оригинальной структуры каталогов).

Инструменты для анализа: только ручной анализ.

Заметки: при создании резервной копии вы можете выбрать опцию «восстановить оригинальную структуру каталогов». Такие резервные копии удобно анализировать в ручном режиме, но исключают автоматизированный анализ в криминалистическом ПО.

Образ DMG (прямое извлечение 32-разрядных устройств)

Инструмент для создания: Elcomsoft iOS Forensic Toolkit при прямом извлечении 32-разрядных устройств.

Инструменты для анализа: Elcomsoft Phone Viewer, любые сторонние пакеты, воспринимающие формат DMG, вручную. Для монтирования образа DMG в Windows рекомендуем использовать утилиту Catacombae – HFSExplorer[60] .

Заметки: в режиме ручного анализа образ DMG можно смонтировать в macOS по инструкции с сайта Apple[61]:

Образ диска — это сжатая копия содержимого диска или папки. Имена файлов образов дисков имеют в своем окончании «.dmg». Чтобы увидеть содержимое образа диска, необходимо сначала открыть образ диска, чтобы он появился на рабочем столе или в окне Finder.

На Mac дважды нажмите образ, чтобы открыть его.

Дважды нажмите мышью открывшийся образ диска, чтобы получить доступ к его содержимому.

Облачная резервная копия из iCloud

Инструмент для создания: Elcomsoft Phone Breaker (при скачивании облачных резервных копий из iCloud).

Инструменты для анализа: Elcomsoft Phone Viewer.

Заметки: после скачивания резервной копии из облака утилитой Elcomsoft Phone Breaker будет автоматически предложено открыть данные в Elcomsoft Phone Viewer. Если при скачивании облачных резервных копий из iCloud опция восстановления оригинальной структуры каталогов не была включена, то резервная копия будет сохранена в формате локальных резервных копий iTunes, и вы сможете открыть её в любом пакете, совместимом с этим форматом.

Связка ключей (низкоуровневое извлечение)

Инструмент для создания: Elcomsoft iOS Forensic Toolkit.

Инструменты для анализа: Elcomsoft Phone Viewer, Elcomsoft Phone Breaker.

Заметки: для просмотра и анализа связки ключей, извлечённой из устройства методом низкоуровневого анализа, можно использовать как Elcomsoft Phone Viewer, так и Elcomsoft Phone Breaker (инструмент Keychain Explorer).

Связка ключей (расширенное логическое извлечение)

Инструмент для создания: Elcomsoft iOS Forensic Toolkit.

---

[60] https://www.catacombae.org/hfsexplorer/

[61] https://support.apple.com/ru-ru/guide/mac-help/mchlp1700/mac

Инструменты для анализа: Elcomsoft Phone Viewer, Elcomsoft Phone Breaker.

Заметки: для просмотра и анализа связки ключей, которая содержится в локальной резервной копии с паролем, можно использовать как Elcomsoft Phone Viewer, так и Elcomsoft Phone Breaker (инструмент Keychain Explorer).

Облачная связка ключей (извлечение из iCloud)

Инструмент для создания: Elcomsoft Phone Breaker.

Инструменты для анализа: Elcomsoft Phone Viewer, Elcomsoft Phone Breaker.

Заметки: для просмотра и анализа облачной связки ключей можно использовать как Elcomsoft Phone Viewer, так и Elcomsoft Phone Breaker (инструмент Keychain Explorer).

Журналы диагностики

Инструмент для создания: Elcomsoft iOS Forensic Toolkit (расширенное логическое извлечение).

Инструменты для анализа: ручной анализ, бесплатные утилиты, набор скриптов (см. ниже).

Заметки: для просмотра и анализа журналов диагностики можно использовать как простой текстовый редактор, так и специальные скрипты, разработанные для этой цели.

Медиафайлы

Инструмент для создания: Elcomsoft iOS Forensic Toolkit (расширенное логическое извлечение).

Инструменты для анализа: ручной анализ, Elcomsoft Phone Viewer.

Заметки: важно отметить, что медиафайлы, извлекаемые из iPhone в процессе расширенного логического извлечения, содержат не только фотографии и видео, но и набор метаданных. В состав метаданных может входить информация о распознанных лицах, местоположении, редактировании и т. п. Фотографии и видео можно просмотреть в любом приложении с поддержкой соответствующих форматов (обратите внимание: в свежих версиях iOS фотографии по умолчанию сохраняются в формате HEIC), но для просмотра и анализа метаданных необходимо воспользоваться утилитой Elcomsoft Phone Viewer.

10.2.Информация об устройстве, список установленных приложений

Инструмент для создания: Elcomsoft iOS Forensic Toolkit (расширенное логическое извлечение, извлечение в режимах Recovery и DFU).

Инструменты для анализа: ручной анализ, бесплатные утилиты, набор скриптов (см. ниже).

Заметки: информация об устройстве и список установленных приложений создаются в текстовом формате и дублируются в оригинальном для iOS формате PLIST. Файлы PLIST можно просматривать посредством бесплатных утилит или анализировать при помощи набора скриптов. Текстовые файлы можно просмотреть в любом текстовом редакторе.

10.3.Бесплатные утилиты

За прошедшие годы мы собрали небольшую, но крайне полезную коллекцию бесплатных инструментов, способных облегчить работу эксперта-криминалиста. В приведённый ниже список входят инструменты для работы с plist-файлами, в том числе с бинарными, базами данных SQLite, даунгрейдами iOS, и даже инструменты для расширенного логического анализа iPhone.

- plist Editor[62]
- DB Browser for SQLite[63]
- SQLite Expert[64]
- 3uTools[65]
- iMobileDevice[66]

10.4.Наборы скриптов

Существует огромное количество бесплатных инструментов, каждый из которых предназначен для выполнения какой-либо одной специфической функции. Большинство таких инструментов распространяются в виде платформенно-независимых скриптов, использование которых поможет произвести углублённый анализ устройства и составлять отчёт. Здесь мы приводим ссылки не на конкретные приложения, а на целые коллекции скриптов и утилит.

- APOLLO67
- iLEAPP68
- ArtEx69
- Sysdiagnose forensic scripts70
- ZPET71
- iOS Triage72
- iTunes Backup Reader73
- M.E.A.T.74

---

[62] https://www.icopybot.com/plist-editor.htm
[63] https://sqlitebrowser.org
[64] https://www.sqliteexpert.com
[65] https://www.3u.com
[66] http://docs.quamotion.mobi/docs/imobiledevice/
[67] https://github.com/mac4n6/APOLLO
[68] https://github.com/abrignoni/iLEAPP
[69] https://www.doubleblak.com
[70] https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts
[71] https://www.duffy.app/ZPET
[72] https://github.com/RealityNet/ios_triage
[73] https://github.com/jfarley248/iTunes_Backup_Reader
[74] https://github.com/jfarley248/MEAT

11. Вопросы и ответы

В этом разделе мы собрали ответы на вопросы, которые нам чаще всего задавали во время мероприятий.

Как пользоваться Recovery-режимом и что можно получить с его помощью

В устройствах Apple, работающих под управлением iOS, есть два специальных режима: Recovery и DFU. Использование режима Recovery позволяет узнать информацию об устройстве. Количество доступной в этом режиме информации ограничивается следующими данными: идентификация модели устройства; идентификатор ECID (Exclusive Chip Identification) или Unique Chip ID (UCID); версия загрузчика iBoot; серийный номер устройства; в редких случаях – IMEI. Подробные инструкции по использованию этого режима описаны в статье Роль специальных режимов iOS в мобильной криминалистике: DFU, Recovery и SOS[75] .

Как узнать версию iOS заблокированного телефона и что можно достать через DFU

Если iPhone заблокирован (например, удалённой блокировкой или после 10 неудачных попыток разблокировки), вы всё равно сможете перевести устройство в режим DFU. В этом режиме вы сможете узнать версию загрузчика iBoot, по которой можно попробовать угадать установленную на устройстве версию iOS. При использовании iOS Forensic Toolkit продукт выведет вилку возможных версий iOS, использующих данную версию загрузчика. Вы можете проделать это самостоятельно по данным из таблицы iBoot (Bootloader) – The iPhone Wiki[76]. Подробные инструкции по использованию режима DFU описаны в статье Режим восстановления iPhone: как узнать версию iOS[77].

Что можно извлечь после сброса настроек (сброса пароля к резервной копии)

Если вы вынуждены были сбросить настройки устройства командой Reset all settings с целью сброса пароля к резервной копии в формате iTunes, то с устройства будет также удалён код блокировки экрана. При удалении кода блокировки теряются следующие данные: список транзакций Apple Pay; скачанные сообщения Exchange и других почтовых учётных записей, для которых установлено внешнее управление через политику MDM; пароли к Wi-Fi и ряд системных настроек.

После сброса настроек удаляется и пароль на создание резервных копий в формате iTunes. Для максимально полного извлечения рекомендуем установить временный пароль на резервную копию (только в этом случае будет расшифрована Связка ключей). Если вы используете для извлечения данных наш продукт Elcomsoft iOS Forensic Toolkit, на резервные копии будет автоматически установлен временный пароль ‘123’, а по окончании извлечения – сброшен в исходное состояние.

---

[75] https://blog.elcomsoft.ru/2020/02/rol-speczialnyh-rezhimov-ios-v-mobilnoj-kriminalistike-dfu-recovery-i-sos/

[76] https://www.theiphonewiki.com/wiki/IBoot_(Bootloader)

[77] https://blog.elcomsoft.ru/2021/02/rezhim-vosstanovleniya-iphone-kak-uznat-versiyu-ios/

Наконец, сброс настроек выключает режим «в полёте», если он был активирован. По этой причине рекомендуем производить сброс настроек в условиях, когда устройство изолировано от беспроводных сетей.

Почему агент не работает с iOS x.y

Агент-экстрактор использует обнаруженные в iOS уязвимости для того, чтобы выбраться из «песочницы» и получить доступ к файловой системе. К примеру, одна из известных нам уязвимостей была обнаружена в iOS 14.8, а в iOS 14.8.1 – исправлена. Соответственно, после исправления уязвимости в iOS агент-экстрактор работать не будет – до тех пор, пока не будет обнаружена очередная уязвимость. Для актуальной информации о поддерживаемых агентом версиях iOS см. страницу Elcomsoft iOS Forensic Toolkit [78].

Рекомендуем воспользоваться расширенным логическим извлечением, скачать данные из iCloud или воспользоваться доступом через checkm8, если устройство совместимо с этим методом.

Работает ли EIFT в виртуальной машине или на хакинтоше

Нет. Для работы iOS Forensic Toolkit для Mac требуется оригинальный компьютер Mac, Mac mini или Macbook. В старых версиях инструментария поддерживались только системы с процессором Intel, но начиная с iOS Forensic Toolkit 8.0 поддерживаются и чипы архитектуры Apple Silicon (например, все редакции чипов M1 и M2).

Как зарегистрировать учётную запись разработчика

Пройдите по ссылке https://developer.apple.com/programs/enroll/ и нажмите Enroll. Войдите в свою учётную запись Apple ID и следуйте инструкциям. Участие в программе для индивидуальных разработчиков стоит $99 в год. Имейте в виду: Apple редко одобряет заявки, сделанные с недавно созданных Apple ID, и всегда верифицирует данные (имя, адрес и платёжную карту).

Максимальные шансы получить одобрение на регистрацию учётной записи в программе для разработчиков – при использовании ненового Apple ID, в котором указан адрес, совпадающий с тем, к которому привязана платёжная карта; регистрироваться лучше с компьютера Mac, а наличие истории покупок с той же учётной записи дополнительно повышает шансы.

Почему после подписи обычной учётной записью агент не запускается (где подтвердить сертификат)

Для того, чтобы запустить приложение, установленное не из App Store, вам потребуется вручную подтвердить цифровой сертификат, которым было подписано приложение. Этот шаг не требуется, если была использована старая учётная запись из программы для разработчиков (но нужен для недавно зарегистрированных учётных записей).

Для подтверждения сертификата необходимо открыть устройству доступ в интернет (внимание: обратите внимание на настройки файрволла!), после чего открыть приложение Settings и перейти в раздел “General” > “About” > “Certificate Trust Settings”. Найдите сертификат, которым был подписан агента-экстрактор, и коснитесь его, после

[78] https://www.elcomsoft.ru/eift.html

чего подтвердите запрос. iPhone подключится к удалённому серверу Apple для проверки сертификата. Обратите внимание: мы усиленно рекомендуем защитить соединение посредством файрволла (программного или аппаратного) по инструкциям, приведённым в соответствующем разделе.

Как настроить файрволл и для чего это нужно

При выполнении определённых операций вам может потребоваться предоставить устройству iOS ограниченный доступ в интернет. Чаще всего это требуется для подтверждения сертификата, которым был подписан агент-экстрактор.

Чтобы обеспечить сохранность данных, важно заблокировать доступ ко всем серверам, за исключением тех, которые необходимы для работы. В соответствующих разделах руководства приводятся подробные инструкции.

Как извлечь системные журналы

Некоторые системные журналы можно извлечь при помощи iOS Forensic Toolkit в процессе расширенного логического анализа. Для доступа к системным журналам установите отладочные профили и используйте команду EIFT для их извлечения (подробности – в соответствующем разделе данного руководства). В то же время многие журналы и логи остаются доступными исключительно посредством низкоуровневого анализа, который можно провести при помощи агента-экстрактора и других поддерживаемых способов.

Почему агент не подключается к устройству, на котором установлен джейлбрейк checkra1n

В состав checkra1n входит сервис SSH DropBear, который использует нестандартный порт 44. Для его использования необходимо поменять номер порта 22 на 44 в скрипте EIFT (строка IPORT). Возникает та же проблема и с AFU, если не устанавливать Cydia и OpenSSH, который использует стандартный порт 22.

Чем отличается расширенное логическое извлечение от резервных копий iTunes

Создавая резервную копию в iTunes, вы создаёте только резервную копию. Если пароль на резервную копию не задан, то часть данных из неё расшифровать не удастся.

В аналогичной ситуации iOS Forensic Toolkit автоматически установит (а после извлечения – снимет) временный пароль на резервную копию «123», что позволит расшифровать все сохранённые в ней данные. Кроме того, независимо от наличия или отсутствия пароля к резервной копии, по независимым протоколам EIFT дополнительно извлечёт медиафайлы (фотографии, видео и метаданные), системные журналы и файлы приложений.

Как установить доверенные отношения на Маке

В новых версиях macOS нет приложения iTunes, а при подключении iPhone к компьютеру всплывающее окно, которое требует установить связь между устройствами, не появляется. Соответственно, установить доверенные отношения между iPhone и компьютером Mac вам придётся непосредственно из Finder.

Чему и как мешает режим ограничений USB

Режим ограничений USB не позволяет устройству (iPhone, iPad) обмениваться информацией с компьютером или другими цифровыми устройствами через порт Lightning. Соответственно, если этот режим активирован (а он активируется

автоматически сразу после блокировки экрана устройства, если к нему не был подключён какой-либо проводной аксессуар), то вам не удастся провести расширенное логическое извлечение или создать резервную копию через iTunes, установить агент-экстрактор или джейлбрейк.

Деактивировать режим ограничений USB можно единственным способом – разблокировав экран устройства (биометрикой или кодом блокировки). Кроме того, этот режим не включается, если устройство перевести в один из режимов Recovery или DFU (возможности которых в целях извлечения данных сильно ограничены).

Как извлечь маркеры аутентификации iCloud и что с ними можно сделать

Роль маркеров аутентификации в настоящий момент сводится к возможности скачивания синхронизированных данных (без сквозного шифрования). Использовать можно только маркеры, извлечённые из компьютеров с macOS, и только непосредственно на том же физическом компьютере, из которого они были извлечены.

Насколько опасно сбрасывать пароль на резервную копию, что именно теряется

При сбросе пароля на резервную копию удаляются пароли Wi-Fi и код блокировки экрана, что в свою очередь приводит к удалению таких данных, как скачанные сообщения Exchange, транзакции Apple Pay и других типов данных из приложений, которые требуют наличия на устройстве кода блокировки. Кроме того, отключается режим «в полёте», если он был активирован, что несёт известные риски.

Почему в облачной резервной копии нет каких-либо данных

Причин, по которым в облачных резервных копиях могут отсутствовать те или иные данные, может быть несколько. Самая распространённая причина – включение пользователем облачной синхронизации для данного типа данных. Например, при включении синхронизации сообщений (SMS, iMessage) они перестанут сохраняться в составе резервных копий. При включении синхронизации фотографий (iCloud Photos) они также перестают попадать в резервную копию, но пользователь может самостоятельно включить или отключить как синхронизацию, так и сохранение в составе резервных копий по отдельности. В этом случае рекомендуем скачать из облака синхронизированные данные.

Вторая причина – отключение пользователем сохранение данных в облако для конкретной категории. Также могут влиять такие причины, как ограниченное место в облаке и нерегулярная зарядка устройства в присутствии сетей Wi-Fi, нарушающая расписание создания резервных копий. Наконец, резервные копии могут быть отключены в принципе.

С чего начать? (правильные шаги по изолированию iPhone)

Последовательность действий по изолированию устройств описана в разделе Транспортировка: изолирование устройства от беспроводных сетей.

Почему важно установить пароль на резервную копию?

Если резервная копия не защищена паролем, то отдельные категории данных (в частности – связка ключей, в которой хранятся все пароли пользователя) будут зашифрованы аппаратным ключом устройства, и расшифровать эти данные при анализе будет невозможно. Если же резервная копия защищена паролем, то и эти данные будут также зашифрованы при помощи пароля, после чего их можно успешно расшифровать.

Какие данные могут быть в iCloud и в каком порядке их извлекать?

В iCloud хранятся данные следующих категорий: синхронизированные данные; резервные копии; файлы iCloud Drive; данные, защищённые сквозным шифрованием.

Извлекать рекомендуем в следующем порядке:

1. Синхронизированные данные (если известен код блокировки экрана, то и данные, защищённые сквозным шифрованием)
2. Файлы iCloud Drive
3. Резервные копии

Резервные копии рекомендуется извлекать в последнюю очередь как по причине их большого объёма, так и потому, что Apple регулярно блокирует учётные записи, из которых были скачаны резервные копии с использованием сторонних инструментов.

Безопасно ли ставить джейлбрейк и зачем это может понадобиться?

В зависимости от версии iOS и типа джейлбрейка риск с точки зрения работоспособности устройства может быть небольшим, так и существенным (особенно для старых джейлбрейков). Основные риски джейлбрейка в том, что для их установки может потребоваться подключение устройства к сети интернет, а извлечённые с их помощью данные могут оказаться непригодными в качестве доказательств. Подробности в разделе **Сопутствующие риски**.

С учётом рисков, связанных с установкой джейлбрейков, **использовать их рекомендуется в ограниченных случаях:**

1. Джейлбрейк доступен для версии iOS, не поддерживаемой агентом-экстрактором.

2. Для извлечения данных из iPhone 4s, для которого существуют джейлбрейки, но метод прямого извлечения требует дополнительного аппаратного микроконтроллера, которого нет под рукой.

Кроме того, джейлбрейки иногда используются в целях экономии:

1. Экономия ежегодной абонентской платы, которая требуется при регистрации учётной записи Apple для разработчиков.

2. Экономия на приобретении компьютера под управлением macOS, который потребуется для использования прямого извлечения посредством checkm8 или для использования обычного (бесплатного) Apple ID для подписи агента-экстрактора вместо учётной записи разработчика.

Что можно извлечь из Apple Watch и как?

Непосредственно из часов Apple Watch можно извлечь ограниченное количество информации, куда входят системные журналы и журналы диагностики, настройки часов, иногда – фотографии уменьшенного раздела. Для анализа потребуется подключение через адаптер iBUS.

Подробная информация об анализе Apple Watch приводится в статьях Извлечение и анализ данных Apple Watch[79] и Анализ Apple TV и Apple Watch[80].

Что можно извлечь из Apple TV и как?

[79] https://blog.elcomsoft.ru/2020/06/izvlechenie-i-analiz-dannyh-apple-watch/
[80] https://blog.elcomsoft.ru/2019/06/analiz-apple-tv-i-apple-watch/

Извлечение данных из Apple TV похоже на аналогичный процесс с iPhone за исключением того, что служба резервного копирования на приставке отсутствует. Соответственно, в процессе логического анализа извлекаются только медиафайлы по протоколу afc. С учётом того, что Apple TV, как правило, зарегистрированы в iCloud Photos, может быть доступно достаточно большое количество фотографий и видеороликов.

На приставках Apple TV не может быть установлен ни код блокировки, ни ограничения Экранного времени. Более того, для подключения приставки к компьютеру не требуется процесс установления доверительных отношений. Наконец, операционная система tvOS основана на соответствующих версиях iOS, что облегчает разработку джейлбрейков для Apple TV и позволяет при их использовании получить доступ к файловой системе и связке ключей.

Подробная информация об анализе Apple TV приводится в статье Анализ Apple TV и Apple Watch[81].

Как расшифровать переписку Signal?

Переписку из мессенджера Signal можно извлечь исключительно из самого устройства путём извлечения рабочей базы данных. В отличие от других мессенджеров, Signal шифрует базы данных. Ключ шифрования создаётся при первом входе пользователя в Signal на устройстве. Затем ключ хранится в связке ключей, защищённой высоким классом защиты. Без этого ключа можно извлекать только вложения (изображения, документы, голосовые сообщения и т. д.)

Для расшифровки этой базы данных понадобится утилита Elcomsoft Phone Viewer, образ файловой системы и связка ключей, извлечённые из iPhone в процессе низкоуровневого анализа утилитой iOS Forensic Toolkit. Подробные инструкции приведены в статье Расшифровка базы данных Signal[82].

Можно ли сбросить пароль к iCloud, если он неизвестен?

Да, пароль к iCloud можно сбросить, даже если он неизвестен, если выполняются следующие условия:

1. Соответствующая учётная запись использует двухфакторную аутентификацию
2. У вас есть доступ к физическому устройству iPhone и известен код блокировки экрана, или
3. У вас есть доступ ко второму фактору аутентификации (например, SIM-карте или самому устройству, на которое можно получить одноразовый код).

Подробные инструкции – на сайте Apple Если вы забыли пароль для учетной записи Apple ID – Служба поддержки Apple[83].

Что и когда можно извлечь из заблокированного устройства?

Заблокированное устройство можно перевести в режим Recovery или DFU, после чего извлечь информацию об устройстве. Количество доступной в этих режимах информации ограничивается следующими данными: идентификация модели

[81] https://blog.elcomsoft.ru/2019/06/analiz-apple-tv-i-apple-watch/

[82] https://blog.elcomsoft.com/2019/08/how-to-extract-and-decrypt-signal-conversation-history-from-the-iphone/

[83] https://support.apple.com/ru-ru/HT201487

устройства; идентификатор ECID (Exclusive Chip Identification) или Unique Chip ID (UCID); версия загрузчика iBoot; серийный номер устройства; в редких случаях – IMEI. Подробные инструкции по использованию этого режима описаны в статье Роль специальных режимов iOS в мобильной криминалистике: DFU, Recovery и SOS[84].

Можно ли извлечь хоть что-то из устройства, сброшенного к заводским настройкам?

Из такого устройства можно извлечь информацию о самом устройстве и версии iOS, которая на нём установлена. После сброса к заводским настройкам никаких пользовательских данных или учётных записей на устройстве не останется. Вот подробный список данных, которые можно получить об устройстве после сброса: точная идентификация модели устройства; идентификатор ECID (Exclusive Chip Identification) или Unique Chip ID (UCID); версия загрузчика iBoot; серийный номер устройства; в редких случаях – IMEI. По идентификатору устройства или его серийному номеру можно запросить у Apple информацию о владельце устройства, после чего оформить запрос на получение имеющихся у компании данных о владельце.

Посредством крайне трудоёмких процедур из сброшенного устройства можно извлечь и такие данные, как точное время сброса (согласно показаниям встроенных RTC часов), а если iPhone был заново настроен после сброса – точное время (согласно показаниям встроенных RTC часов) и способ настройки (настроен как новое устройство, восстановлен из локальной или облачной резервной копии или данные переданы на устройство по кабелю). Эти процедуры исключительно сложны в использовании.

12.iOS Forensic Toolkit: полезные команды и примеры использования

В восьмой версии iOS Forensic Toolkit применяется интерфейс командной строки. Далеко не все команды, ключи и последовательность их использования очевидны. И если в предыдущих разделах приводятся готовые пошаговые алгоритмы, то в этой главе мы опишем как полезные, но редко упоминаемые команды, так и ситуации, в которых их стоит использовать.

12.1.Команды, выполняющиеся из режима восстановления (recovery)

Первоочередной командой, которую нужно запустить в режиме recovery при извлечении через эксплойт загрузчика, является модификация значения флага автозагрузки. Перед началом работы с устройством рекомендуем заблокировать автозагрузку следующей командой:

```
./EIFT_cmd tools autobootFalse
```

[84] https://blog.elcomsoft.ru/2020/02/rol-speczialnyh-rezhimov-ios-v-mobilnoj-kriminalistike-dfu-recovery-i-sos/

Эта команда используется для блокировки автоматической загрузки устройства в iOS. После её выполнения устройство больше не сможет случайно загрузиться в обычном режиме; все последующие перезагрузки будут переводить его в режим восстановления (recovery), что позволяет защитить данные от случайной модификации.

Если работа с устройством завершена, и устройство требуется вернуть владельцу, отключите режим блокирования автозагрузки. Для этого перезагрузите устройство либо выключите его командой ssh halt, после чего снова включите. После того, как устройство попадёт в режим recovery, выполните указанную ниже команду. После этого устройство автоматически перезагрузится:

```
./EIFT_cmd tools autobootTrue
```

Сразу после выполнения этой команды устройство будет перезагружено в iOS.

12.2.Команды, выполняющиеся из режима pwnedDFU

Для выключения устройства, которое находится в режиме pwnedDFU (то есть, после загрузки модифицированного Ramdisk-а командой boot) либо после процедуры извлечения посредством checkm8, необходима специальная команда. Требуется потому, что выключить устройство кнопками в этом режиме невозможно, т.к. вместо выключения устройство перезагрузится (в ОС либо в recovery в зависимости от значения флажка автозагрузки).

```
./EIFT_cmd ssh halt
```

Команды, описанные ниже, используются в процессе извлечения через эксплойт загрузчика. Они применимы только для 64-разрядных устройств (для 32-разрядных моделей используется другая процедура извлечения).

Следующая команда разблокирует раздел данных.

```
./EIFT_cmd ramdisk unlockdata
```

В некоторых ситуациях команда unlockdata не срабатывает, выдав ошибку “Failed to load necessary libraries. Is shared cache loaded?”. В таких случаях потребуется сначала выполнить команду “ramdisk loadnfcd”, которая произведёт операцию “seshat unlock”. Это процедура, выполняющая некоторые манипуляции с сопроцессором Secure Enclave (SEP), которая необходима в том случае, если Secure Enclave работает в «усиленном» режиме (устройства, которые находятся в этом режиме, некоторые производители называют “SE-bound devices”).

Отметим, что сразу после установки кода блокировки устройство находится в «слабом» режиме. Через какое-то время устройство переводится в «усиленный» режим, который появился, вероятно, в iPhone 6 (A8).

```
./EIFT_cmd ramdisk loadnfcd
```

Сразу после операции “seshat unlock” нужно снова выполнить команду unlockdata, добавив к ней ключ -s. Обратите внимание: с этим ключом unlockdata выполняется только после команды loadnfcd.

```
./EIFT_cmd ramdisk unlockdata -s
```

Две следующих команды используются для извлечения связки ключей (keychain) и образа файловой системы (tar) соответственно.

```
./EIFT_cmd ramdisk keychain -o {filename}
```

```
./EIFT_cmd ramdisk tar -o {filename}
```

12.3.Команды для устройств, загруженных в ОС

Быстро перевести устройство в режим восстановления (recovery) можно одной командой:

```
./EIFT_cmd tools recovery
```

Если устройство не привязано к компьютеру или привязка перестала работать, рекомендуем отвязать и заново привязать устройство следующими командами (потребуется разблокировать экран устройства и ввести код блокировки):

```
./EIFT_cmd normal unpair
```

```
./EIFT_cmd normal pair
```

Следующие команды нужны при использовании агента-экстрактора.

Установка агента-экстрактора осуществляется следующей командой:

```
./EIFT_cmd agent install
```

Извлечение связки ключей и образа раздела данных (ключ -o указывает путь для выходных файлов; имена файлов назначаются автоматически) осуществляется командами keychain и tar соответственно:

```
./EIFT_cmd agent keychain -o
/Users/ElcomSoft/Desktop/data/
```

```
./EIFT_cmd agent tar -o /Users/ElcomSoft/Desktop/data/
```

Системный раздел (например, при подозрении на наличие шпионского или зловредного ПО) можно извлечь следующей командой:

```
./EIFT_cmd agent tar --system -o
/Users/ElcomSoft/Desktop/data/
```

Также доступны команды extract и metadata. Команда extract извлечёт часть файловой системы (папку со всеми подкаталогами) или отдельный файл, путь к которым

передаётся посредством ключа -p. Если же этот ключ не указан, то будут извлечены все данные из каталога “/private/var/” (то есть, корень пользовательских данных) со всеми подкаталогами; то есть, извлекаются те же данные, что и командой tar.

Извлечение папки Media целиком:

```
   EIFT_cmd agent extract -p /private/var/mobile/Media/ -o
/Users/ElcomSoft/Desktop/data/
```

Извлечение только файла Photo.jpg из фотоальбома:

```
   EIFT_cmd agent extract -p
/private/var/mobile/Media/DCIM/Photo.jpg -o
/Users/ElcomSoft/Desktop/data/
```

Извлечение полного образа файловой системы (ключ -p не указан):

```
   EIFT_cmd agent extract -o
/Users/ElcomSoft/Desktop/data/
```

Наконец, команда metadata извлечёт только метаданные файловой системы, начиная с папки, указанной в параметре -p (при его отсутствии – корневой каталог раздела данных). К примеру, извлечь метаданные папки Media можно следующей командой:

```
   EIFT_cmd agent metadata -p /private/var/mobile/Media/ -
o /Users/ElcomSoft/Desktop/metadata/
```

Удалить агент можно командой:

```
   ./EIFT_cmd agent uninstall
```

13. Дополнительные материалы

В этом разделе находятся материалы, которые не нужны непосредственно для работы с устройствами, но могут представлять интерес в теоретическом аспекте.

13.1. Сравнение редакций iOS Forensic Toolkit: Windows, Linux, macOS

Между редакциями для Windows, Linux и macOS существуют важные различия. В редакции для Windows доступны функции логического и низкоуровневого извлечения посредством агента-экстрактора; извлечение через эксплойт загрузчика не поддерживается. В версиях для Linux и macOS дополнительно поддерживается извлечение через эксплойт загрузчика. Подробнее о различиях между версиями:

Функции	macOS	Windows	Linux*
Расширенная информация об устройстве	✓	✓	✓
Логическое извлечение (резервная копия)	✓	✓	✓
Извлечение медиафайлов и метаданных	✓	✓	✓
Извлечение диагностических логов	✓	✓	✓
Извлечение агентом с учётной записью разработчика	✓	✓	✓
Извлечение агентом с обычной учётной записью	✓	✓	✓
Извлечение через уязвимости загрузчика	✓	✗	✓
Дополнительные сервисные возможности	✓	✓	✓

Редакция для Linux поддерживает сборки Debian, Ubuntu, Kali Linux и Mint на компьютерах с архитектурой Intel.

13.2.Raspberry Pi 5 в качестве альтернативы компьютеру с macOS

В iOS Forensic Toolkit до сих пор есть небольшие различия в функционале между версиями для Windows, Linux и macOS. В частности, работа с эксплойтами загрузчика, в том числе checkm8, реализована только в версиях для macOS и Linux.

Если у эксперта уже установлена Windows, ставить на тот же компьютер параллельную сборку с Linux может оказаться невыполнимой задачей как с технической, так и с организационной точек зрения. Лучшим вариантом стала бы виртуальная машина с Linux; однако, к сожалению, их использование не поддерживается нашим продуктом, т. к. эксплойт checkm8 из виртуальной машины не сработает. Логичным вариантом было бы приобретение специализированного компьютера для низкоуровневого извлечения данных. Вместо покупки дешёвого ноутбука, который, скорее всего, подведёт, как только вы попробуете его использовать, было бы разумнее приобрести недорогой, но современный одноплатный микрокомпьютер класса Raspberry Pi 5. Raspberry Pi 5 оснащён четырёхъядерным процессором, 8 ГБ оперативной памяти и интерфейсом PCIe 2.0, который позволяет подключать SSD-накопители форм-фактора M.2 через соответствующий комплект от стороннего производителя.

13.2.1.1.Elcomsoft Forensic Acquisition System (EFAS)

Чтобы запустить iOS Forensic Toolkit на Raspberry Pi 5, мы создали специальный загрузочный образ, названный Elcomsoft Forensic Acquisition (Operating) System, сокращённо EFAS, доступный по ссылке https://github.com/Elcomsoft/EFAS. Он представляет собой минимальную среду на основе Arch Linux для архитектуры ARM с предустановленными и уже настроенными зависимостями. Для этой цели мы создали специальную сборку iOS Forensic Toolkit для платформы Linux arm64 и тщательно её протестировали, чтобы убедиться в отсутствии «подводных камней». EFAS уже имеет

все необходимые зависимости и библиотеки, заранее установленные и правильно настроенные, так что пользователь сможет сразу запустить EIFT и начать им пользоваться.

Примечание: теоретически возможно запустить сборку iOS Forensic Toolkit для Linux arm64 на других операционных системах, однако официально это не поддерживается, поскольку для корректной работы iOS Forensic Toolkit необходимо установить и настроить несколько зависимостей.

13.2.1.2.Возможности EFAS

EFAS поставляется с предустановленным и включённым SSH для удалённого доступа. Подключите Raspberry Pi к Ethernet, затем войдите в него по SSH с помощью команды `ssh eift@EFASpi5` и пароля `Elcomsoft`, после чего продолжите работу с обычного компьютера.

Примечание: если вы не планируете использовать SSH, рекомендуем отключить его с помощью команд `sudo systemctl disable sshd` и `sudo systemctl stop sshd`, чтобы избежать риска утечки данных через сеть. Если позже вы решите вновь включить SSH, используйте `команды sudo systemctl enable sshd` и `sudo systemctl start sshd`.

В качестве альтернативы вы можете подключить к Raspberry Pi монитор через порт HDMI, подключить мышь и клавиатуру через USB, превратив таким образом Raspberry Pi в компактный, но мощный десктоп. При запуске EFAS появится экран входа GDM, где можно выбрать пользователя `eift` и войти с паролем `Elcomsoft`. Далее загрузится рабочая среда KDE с полезными ярлыками, такими как эмулятор терминала Alacritty или просмотрщик файлов Nemo. Из-за слабой совместимости среды X11 с Raspberry Pi 5 мы решили использовать систему, полностью основанную на Wayland. Это работает для большинства базовых приложений, но, к сожалению, иногда возникают проблемы с устаревшими программами (например, GParted), требующими использования терминала для некоторых задач.

Примечание: мы настоятельно рекомендуем изменить пароль по умолчанию. Это можно сделать с помощью терминала и команды `passwd`.

13.2.1.3.Использование iOS Forensic Toolkit на Raspberry Pi 5

iOS Forensic Toolkit можно загрузить непосредственно на Raspberry Pi из браузера Firefox либо скачать его на компьютер и скопировать на RPI через USB-накопителя или командой `scp`.

Важно: не распаковывайте iOS Forensic Toolkit на USB-накопителе, т. к. это может вызвать проблемы при последующем запуске EIFT.

Вместо этого скопируйте zip-файл на RPI (например, на десктоп), после чего распакуйте EIFT уже там (например, с помощью терминала командой `unzip` EIFT.zip). После этого вы сможете запустить EIFT.

13.2.1.4.Использование NVME-накопителя

Raspberry Pi 5 поставляется с интерфейсом PCIe 2.0, который можно использовать для подключения SSD в форм-факторе M.2 с помощью соответствующего

адаптера от сторонних производителей. При первом подключении накопителя вам может потребоваться разбить его на разделы и отформатировать. Если вы планируете использовать этот накопитель для извлечения данных на Raspberry Pi, а затем отсоединить его и подключить к компьютеру через USB-адаптер для M.2, то лучше отформатировать накопитель в файловую систему, которую поддерживают как RPI, так и ваш компьютер - например, exFAT. Во всех остальных случаях мы рекомендуем форматировать накопитель в BTRFS, использование которой даст некоторые преимущества при работе с Perfect Acquisition и большими образами: BTRFS поддерживает функции COW (Copy On Write) и снапшоты, которые могут быть полезны (EIFT использует COW, если эта функция поддерживается файловой системой).

При использовании iOS Forensic Toolkit убедитесь, что корректно указан выходной путь `-o <путь>`, который должен указывать на накопитель M.2.

13.2.1.5.Форматирование накопителя M.2

Сначала убедитесь, что накопитель правильно обнаружен. Это можно сделать с помощью команды `lsblk`. Вывод должен выглядеть примерно так:

```
   [eift@EFASpi5 ~]$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
mmcblk0 179:0 0 119.1G 0 disk
└─mmcblk0p1 179:1 0 160M 0 part /boot
└─mmcblk0p2 179:2 0 118.9G 0 part /
nvme0n1 259:0 0 465.8G 0 disk
└─nvme0n1p1 259:1 0 465.8G 0 part
[eift@EFASpi5 ~]$
```

Здесь вы можете видеть, что M.2 обнаружен как `nvme0n1`.

Для разбиения накопителя используйте команду `sudo gdisk /dev/nvme0n1`. Используйте `o` для удаления существующих разделов (возможно, потребуется подтверждение `y`), затем используйте `n,1,<enter>,<enter>,<enter>`

Далее нажмите `w,y` , чтобы сохранить изменения на диске.

Далее отформатируйте раздел командой `sudo mkfs.btrfs /dev/nvme0n1p1`.

После этого можно смонтировать диск в GUI Nemo.

13.2.1.6.Где скачать EFAS

Elcomsoft Forensic Acquisition (Operating) System доступна с полностью открытым исходным кодом, а скрипты, используемые для создания образа, доступны в нашем репозитории GitHub по ссылке https://github.com/Elcomsoft/EFAS. Перейдите в раздел «Релизы» и загрузите последнюю сборку, сгенерированную нашим CI-каналом.

Доверие к операционной системе — это хорошо, но намного лучше, когда вы можете на самом деле проверить, что именно входит в её состав. В конце концов, в области криминалистики эксперты обращаются с чрезвычайно чувствительными данными. В нашей сборке вы можете видеть не только файлы, которые окажутся на образе, но и можете самостоятельно проверить скрипты, которые устанавливают и настраивают программное обеспечение. Кроме того, полный журнал работы CI-провайдера, создавшего образ, также доступен на GitHub, так что вы можете в деталях

исследовать, как именно был создан образ. Если и этого недостаточно, вы можете самостоятельно клонировать репозиторий и создать образ локально.

Примечание: для самостоятельного создания образа вам потребуется хост на Linux и несколько зависимостей, установленных и правильно настроенных, таких как `systemd-binfmt` и `qemu`.

EFAS активно развивается. Ждём вашей обратной связи и предложений – их можно писать непосредственно на GitHub или в нашу службу поддержки.

13.3.Дополнительное оборудование для iOS Forensic Toolkit

Чтобы максимально раскрыть возможности инструментария iOS Forensic Toolkit, вам потребуется набор дополнительных аксессуаров, начиная от кабелей и переходников и заканчивая одноплатными микроконтроллерами и микрокомпьютерами.

13.3.1. Программный продукт: Elcomsoft iOS Forensic Toolkit

В состав продукта входит лицензионный USB-ключ, который должен быть подключён к компьютеру в течение всего времени работы программы. Для новых пользователей ключ доставляется по почте, а обновить лицензию можно в режиме онлайн. Таким образом, для запуска EIFT вам потребуется:

- Программный продукт Elcomsoft iOS Forensic Toolkit;
- USB-ключ с лицензией.

13.3.2. Компьютер Mac

EIFT совместим с операционными системами Windows, Linux и macOS, но есть некоторые функции, доступные только на macOS:

- Агент-экстрактор и обычные учётные записи Apple ID: установить агент на исследуемое устройство будет гораздо проще с компьютера с macOS по сравнению с другими платформами;
- Функции последовательной отладки: в большинстве случаев вам это не потребуется, но вам может попасться уникальная комбинация устройств и версий iOS, которая потребует дополнительной отладки, и macOS поддерживает эту функцию;
- SSH-доступ: эта функция полезна, если вам нужно быстро извлечь какие-то конкретные данные, а не полный образ файловой системы (и во многих других случаях).

13.3.3. Raspberry Pi Pico

Raspberry Pi Pico — доступный по цене одноплатный микроконтроллер, который весьма полезен для выполнения ряда специфических задач. Его можно использовать для следующих целей:

- Эксплойт Apple A5/A5X: Pico можно использовать для загрузки эксплойта этих конкретных чипов Apple;
- Автоматические снимки экрана: Pico позволяет автоматизировать захват экрана для создания "длинных" скриншотов;

– Автоматический вход в режим DFU (A11+): Pico упрощает процесс входа в режим DFU для устройств с чипами A11 и более поздних.

Для выполнения этих задач потребуются дополнительные кабели и адаптеры, о которых рассказывается в следующих разделах.

13.3.4. Raspberry Pi 4 и 5.

Raspberry Pi 4 или 5 — полноценные одноплатные микрокомпьютеры с архитектурой ARM. Мы настоятельно рекомендуем использовать Raspberry 4 или 5 для установки и первого запуска агента-экстрактора. Это устройство помогает создать функциональный файрволл, чтобы обезопасить процесс установки и первого запуска агента. При использовании macOS можно обойтись и программным вариантом, но решение с использованием Raspberry Pi надёжнее и удобнее в использовании.

Кроме того, микрокомпьютер Raspberry Pi 5 можно использовать в качестве полноценной замены компьютеру Mac в контексте извлечения через эксплойт загрузчика. С этой целью мы разработали Elcomsoft Forensic Acquisition System (EFAS) для Raspberry Pi 5 – заранее сконфигурированный образ Linux для архитектуры arm64, который можно установить на Raspberry Pi 5 для последующей работы с checkm8. Подробно об этом рассказано в соответствующем разделе.

Помимо, собственно, микрокомпьютера вам понадобится источник питания USB-C с соответствующим кабелем для Raspberry Pi.

13.3.5. Кабели

В простых случаях можно обойтись и единственным кабелем Lightning от Apple, но за исключением простейших операций набор необходимых для работы кабелей увеличивается. Усиленно рекомендуем иметь под рукой как минимум следующие кабели:

– USB-C - Lightning
– USB-A - Lightning
– USB-A - Apple 30-контактный (для очень старых устройств)
– Кроме того, вам понадобятся дополнительные кабели:
– USB-C (M) - USB-A (F)
– Micro-USB - USB-A Female (OTG)
– USB-A - micro-USB
– Два кабеля Ethernet

13.3.6. Адаптеры

Также потребуются несколько адаптеров, особенно для устройств, отличных от iPhone или iPad:

– Адаптер GoldenEye (для Apple TV)
– Универсальный адаптер для Apple Watch
– Адаптер для Apple HomePod (его можно распечатать на 3D-принтере)
– Кроме того, вам могут понадобиться следующие адаптеры:

– Dupont-контакты с порта USB-A на 5V+заземление (для питания Raspberry Pi Pico)
– Адаптер камеры Apple
– Dupont-контакты с Lightning на 5V+заземление+данные
– USB-A - Ethernet
– Lightning - Ethernet

13.3.7. Дополнительные и необязательные аксессуары

Существуют и другие аксессуары, которые полезно иметь под рукой:

– SD-карта и картридер: понадобятся для загрузки Raspberry Pi.

– Хаб USB-C с USB-A портами: настоятельно рекомендуем, так как эксплойт checkm8 работает с его использованием более надёжно (вместо него можно использовать адаптер USB-C - USB-A). Кроме того, хаб будет полезен для подключения лицензионного USB-ключа EIFT, если в вашем компьютере недостаточно свободных портов USB-A.

– USB-мышь: будет полезна для того, чтобы функция снятия длинных скриншотов работала более надёжно.

– Адаптер DSCD для последовательной отладки: помогает решить проблемы с отдельными устройствами, работающими на определённых версиях ОС Apple.

– Внешний диск (желательно с интерфейсом USB-C): важный и неотъемлемый компонент для сохранения полученных данных. Рекомендуем использовать объёмные NVME-накопители в корпусе USB-C. Имейте в виду, что современные мобильные устройства могут иметь накопители объёмом до терабайта, а некоторые версии iPad Pro - и до двух терабайт.

13.4.Список соответствия идентификаторов моделей Apple

Многие утилиты идентифицируют модель устройства по её условному обозначению. К примеру, под идентификатором iPhone10,1 зашифрована модель, известная как iPhone 8. В приведённом ниже списке перечислены идентификаторы моделей и соответствующие им устройства.

– i386 : iPhone Simulator
– x86_64 : iPhone Simulator
– arm64 : iPhone Simulator
– iPhone1,1 : iPhone
– iPhone1,2 : iPhone 3G
– iPhone2,1 : iPhone 3GS
– iPhone3,1 : iPhone 4
– iPhone3,2 : iPhone 4 GSM Rev A
– iPhone3,3 : iPhone 4 CDMA
– iPhone4,1 : iPhone 4S
– iPhone5,1 : iPhone 5 (GSM)
– iPhone5,2 : iPhone 5 (GSM+CDMA)
– iPhone5,3 : iPhone 5C (GSM)

- iPhone5,4 : iPhone 5C (Global)
- iPhone6,1 : iPhone 5S (GSM)
- iPhone6,2 : iPhone 5S (Global)
- iPhone7,1 : iPhone 6 Plus
- iPhone7,2 : iPhone 6
- iPhone8,1 : iPhone 6s
- iPhone8,2 : iPhone 6s Plus
- iPhone8,4 : iPhone SE (GSM)
- iPhone9,1 : iPhone 7
- iPhone9,2 : iPhone 7 Plus
- iPhone9,3 : iPhone 7
- iPhone9,4 : iPhone 7 Plus
- iPhone10,1 : iPhone 8
- iPhone10,2 : iPhone 8 Plus
- iPhone10,3 : iPhone X Global
- iPhone10,4 : iPhone 8
- iPhone10,5 : iPhone 8 Plus
- iPhone10,6 : iPhone X GSM
- iPhone11,2 : iPhone XS
- iPhone11,4 : iPhone XS Max
- iPhone11,6 : iPhone XS Max Global
- iPhone11,8 : iPhone XR
- iPhone12,1 : iPhone 11
- iPhone12,3 : iPhone 11 Pro
- iPhone12,5 : iPhone 11 Pro Max
- iPhone12,8 : iPhone SE 2nd Gen
- iPhone13,1 : iPhone 12 Mini
- iPhone13,2 : iPhone 12
- iPhone13,3 : iPhone 12 Pro
- iPhone13,4 : iPhone 12 Pro Max
- iPhone14,2 : iPhone 13 Pro
- iPhone14,3 : iPhone 13 Pro Max
- iPhone14,4 : iPhone 13 Mini
- iPhone14,5 : iPhone 13
- iPhone14,6 : iPhone SE 3rd Gen
- iPhone14,7 : iPhone 14
- iPhone14,8 : iPhone 14 Plus
- iPhone15,2 : iPhone 14 Pro
- iPhone15,3 : iPhone 14 Pro Max
-
- iPod1,1 : 1st Gen iPod

- iPod2,1 : 2nd Gen iPod
- iPod3,1 : 3rd Gen iPod
- iPod4,1 : 4th Gen iPod
- iPod5,1 : 5th Gen iPod
- iPod7,1 : 6th Gen iPod
- iPod9,1 : 7th Gen iPod
-
- iPad1,1 : iPad
- iPad1,2 : iPad 3G
- iPad2,1 : 2nd Gen iPad
- iPad2,2 : 2nd Gen iPad GSM
- iPad2,3 : 2nd Gen iPad CDMA
- iPad2,4 : 2nd Gen iPad New Revision
- iPad3,1 : 3rd Gen iPad
- iPad3,2 : 3rd Gen iPad CDMA
- iPad3,3 : 3rd Gen iPad GSM
- iPad2,5 : iPad mini
- iPad2,6 : iPad mini GSM+LTE
- iPad2,7 : iPad mini CDMA+LTE
- iPad3,4 : 4th Gen iPad
- iPad3,5 : 4th Gen iPad GSM+LTE
- iPad3,6 : 4th Gen iPad CDMA+LTE
- iPad4,1 : iPad Air (WiFi)
- iPad4,2 : iPad Air (GSM+CDMA)
- iPad4,3 : 1st Gen iPad Air (China)
- iPad4,4 : iPad mini Retina (WiFi)
- iPad4,5 : iPad mini Retina (GSM+CDMA)
- iPad4,6 : iPad mini Retina (China)
- iPad4,7 : iPad mini 3 (WiFi)
- iPad4,8 : iPad mini 3 (GSM+CDMA)
- iPad4,9 : iPad Mini 3 (China)
- iPad5,1 : iPad mini 4 (WiFi)
- iPad5,2 : 4th Gen iPad mini (WiFi+Cellular)
- iPad5,3 : iPad Air 2 (WiFi)
- iPad5,4 : iPad Air 2 (Cellular)
- iPad6,3 : iPad Pro (9.7 inch, WiFi)
- iPad6,4 : iPad Pro (9.7 inch, WiFi+LTE)
- iPad6,7 : iPad Pro (12.9 inch, WiFi)
- iPad6,8 : iPad Pro (12.9 inch, WiFi+LTE)
- iPad6,11 : iPad (2017)
- iPad6,12 : iPad (2017)

- iPad7,1 : iPad Pro 2nd Gen (WiFi)
- iPad7,2 : iPad Pro 2nd Gen (WiFi+Cellular)
- iPad7,3 : iPad Pro 10.5-inch
- iPad7,4 : iPad Pro 10.5-inch
- iPad7,5 : iPad 6th Gen (WiFi)
- iPad7,6 : iPad 6th Gen (WiFi+Cellular)
- iPad7,11 : iPad 7th Gen 10.2-inch (WiFi)
- iPad7,12 : iPad 7th Gen 10.2-inch (WiFi+Cellular)
- iPad8,1 : iPad Pro 11 inch 3rd Gen (WiFi)
- iPad8,2 : iPad Pro 11 inch 3rd Gen (1TB, WiFi)
- iPad8,3 : iPad Pro 11 inch 3rd Gen (WiFi+Cellular)
- iPad8,4 : iPad Pro 11 inch 3rd Gen (1TB, WiFi+Cellular)
- iPad8,5 : iPad Pro 12.9 inch 3rd Gen (WiFi)
- iPad8,6 : iPad Pro 12.9 inch 3rd Gen (1TB, WiFi)
- iPad8,7 : iPad Pro 12.9 inch 3rd Gen (WiFi+Cellular)
- iPad8,8 : iPad Pro 12.9 inch 3rd Gen (1TB, WiFi+Cellular)
- iPad8,9 : iPad Pro 11 inch 4th Gen (WiFi)
- iPad8,10 : iPad Pro 11 inch 4th Gen (WiFi+Cellular)
- iPad8,11 : iPad Pro 12.9 inch 4th Gen (WiFi)
- iPad8,12 : iPad Pro 12.9 inch 4th Gen (WiFi+Cellular)
- iPad11,1 : iPad mini 5th Gen (WiFi)
- iPad11,2 : iPad mini 5th Gen
- iPad11,3 : iPad Air 3rd Gen (WiFi)
- iPad11,4 : iPad Air 3rd Gen
- iPad11,6 : iPad 8th Gen (WiFi)
- iPad11,7 : iPad 8th Gen (WiFi+Cellular)
- iPad13,1 : iPad air 4th Gen (WiFi)
- iPad13,2 : iPad air 4th Gen (WiFi+Cellular)
- iPad13,4 : iPad Pro 11 inch 3rd Gen
- iPad13,5 : iPad Pro 11 inch 3rd Gen
- iPad13,6 : iPad Pro 11 inch 3rd Gen
- iPad13,7 : iPad Pro 11 inch 3rd Gen
- iPad13,8 : iPad Pro 12.9 inch 5th Gen
- iPad13,9 : iPad Pro 12.9 inch 5th Gen
- iPad13,10 : iPad Pro 12.9 inch 5th Gen
- iPad13,11 : iPad Pro 12.9 inch 5th Gen
- iPad13,16 : iPad Air 5th Gen (WiFi)
- iPad13,17 : iPad Air 5th Gen (WiFi+Cellular)
- iPad13,18: iPad 10th Gen
- iPad13,19: iPad 10th Gen
- iPad14,3-A: iPad Pro 11 inch 4th Gen

- iPad14,3-B: iPad Pro 11 inch 4th Gen
- iPad14,4-A: iPad Pro 11 inch 4th Gen
- iPad14,4-B: iPad Pro 11 inch 4th Gen
- iPad14,5-A: iPad Pro 12.9 inch 6th Gen
- iPad14,5-B: iPad Pro 12.9 inch 6th Gen
- iPad14,6-A: iPad Pro 12.9 inch 6th Gen
- iPad14,6-B: iPad Pro 12.9 inch 6th Gen
-
- Watch1,1 : Apple Watch8mm case
- Watch1,2 : Apple Watch 42mm case
- Watch2,6 : Apple Watch Series 1 38mm case
- Watch2,7 : Apple Watch Series 1 42mm case
- Watch2,3 : Apple Watch Series 2 38mm case
- Watch2,4 : Apple Watch Series 2 42mm case
- Watch3,1 : Apple Watch Series 3 38mm case (GPS+Cellular)
- Watch3,2 : Apple Watch Series 3 42mm case (GPS+Cellular)
- Watch3,3 : Apple Watch Series 3 38mm case (GPS)
- Watch3,4 : Apple Watch Series 3 42mm case (GPS)
- Watch4,1 : Apple Watch Series 4 40mm case (GPS)
- Watch4,2 : Apple Watch Series 4 44mm case (GPS)
- Watch4,3 : Apple Watch Series 4 40mm case (GPS+Cellular)
- Watch4,4 : Apple Watch Series 4 44mm case (GPS+Cellular)
- Watch5,1 : Apple Watch Series 5 40mm case (GPS)
- Watch5,2 : Apple Watch Series 5 44mm case (GPS)
- Watch5,3 : Apple Watch Series 5 40mm case (GPS+Cellular)
- Watch5,4 : Apple Watch Series 5 44mm case (GPS+Cellular)
- Watch5,9 : Apple Watch SE 40mm case (GPS)
- Watch5,10 : Apple Watch SE 44mm case (GPS)
- Watch5,11 : Apple Watch SE 40mm case (GPS+Cellular)
- Watch5,12 : Apple Watch SE 44mm case (GPS+Cellular)
- Watch6,1 : Apple Watch Series 6 40mm case (GPS)
- Watch6,2 : Apple Watch Series 6 44mm case (GPS)
- Watch6,3 : Apple Watch Series 6 40mm case (GPS+Cellular)
- Watch6,4 : Apple Watch Series 6 44mm case (GPS+Cellular)
- Watch6,6 : Apple Watch Series 7 41mm case (GPS)
- Watch6,7 : Apple Watch Series 7 45mm case (GPS)
- Watch6,8 : Apple Watch Series 7 41mm case (GPS+Cellular)
- Watch6,9 : Apple Watch Series 7 45mm case (GPS+Cellular)
- Watch6,10 : Apple Watch SE 40mm case (GPS)
- Watch6,11 : Apple Watch SE 44mm case (GPS)
- Watch6,12 : Apple Watch SE 40mm case (GPS+Cellular)

– Watch6,13 : Apple Watch SE 44mm case (GPS+Cellular)
– Watch6,14 : Apple Watch Series 8 41mm case (GPS)
– Watch6,15 : Apple Watch Series 8 45mm case (GPS)
– Watch6,16 : Apple Watch Series 8 41mm case (GPS+Cellular)
– Watch6,17 : Apple Watch Series 8 45mm case (GPS+Cellular)
– Watch6,18 : Apple Watch Ultra

13.5.Эволюция системы безопасности в версиях iOS

Современный смартфон содержит огромное количество информации о пользователе, которая может превратиться в угрозу, оказавшись в чужих руках. В процессе постепенного расширения сценариев использования смартфонов усиливались и меры, предпринимаемые производителями по защите данных.

В этом разделе описана история того, как эволюционировали методы защиты данных, которые использовала Apple в своих устройствах.

iPhone OS 1–3

В первых версиях iOS (и, соответственно, в первых трёх моделях iPhone) защита данных была символической: PIN-код защищал информацию от любопытных глаз, но и только. Шифрования не было; данные можно было извлечь как из самого устройства, так и из микросхемы памяти. Впрочем, в первых поколениях iPhone не могло содержаться особо ценной информации, за исключением фотографий.

Модели устройств:

– iPhone OS 1.0 – iPhone
– iPhone OS 2.0 – iPhone 3G
– iPhone OS 3.0 – iPhone 3GS

iOS 4: шифрование файловой системы

До версии iOS 4 данные в iPhone хранились в открытом виде. Их извлечение было вопросом несложных манипуляций. Сама компания Apple активно сотрудничала с правоохранительными органами, соглашаясь извлечь данные из присланного iPhone (забегая вперёд, так продолжалось вплоть до выхода iOS 8). В iOS 4 впервые появилось шифрование. Впрочем, использование аппаратного идентификатора в качестве ключа шифрования позволило довольно быстро найти способ извлечь и расшифровать зашифрованные данные, даже если код блокировки экрана был неизвестен.

Модели устройств:

– iOS 4.0 – iPhone 4
– iOS 5.0 – iPhone 4s
– iOS 6.0 – iPhone 5

iOS 5: появился iCloud

В пятой версии iOS появился облачный сервис iCloud. Именно тогда было положено начало облачному извлечению данных: из iCloud стало возможным извлекать резервные копии. В те времена не было ни сквозного шифрования, ни двухфакторной аутентификации, ни защиты по аппаратному идентификатору, ни блокировки учётных записей после скачивания резервной копии сторонним ПО…

iOS 6: "Lost mode" в Find My iPhone

Служба Find My iPhone появилась в iOS 3, но возможность удалённо заблокировать смартфон посредством режима “lost mode” появилась намного позднее.

iOS 7: запрос при сопряжении с новым компьютером

Можно ли сегодня представить себе, что когда-то iPhone можно было просто подключить к компьютеру, и он сразу устанавливал соединение и начинал передачу данных? Тем не менее, до 7-й версии iOS было именно так. И только в iOS 7 появился привычный всплывающий запрос, требующий разблокировать экран устройства и подтвердить установление сопряжения с новым компьютером (последующие подключения обходились без этого благодаря файлам pairing/lockdown).

С точки зрения облачной криминалистики в iOS 7 появилось важное новшество: iCloud keychain, облачная связка ключей. С седьмой версии iOS пароли пользователя стали синхронизироваться между устройствами.

iOS 7 стала первой версией iOS, работавшей на первом 64-разрядном iPhone, оборудованном датчиком отпечатков пальцев и аппаратной подсистемой безопасности Secure Enclave.

Модели устройств:

- iOS 7.0 – iPhone 5s, первый 64-разрядный iPhone с Secure Enclave

Здиарски обнаружил уязвимость в устройствах iOS, см. Apple Confirms “Backdoors”; Downplays Their Severity. Некоторые из обнаруженных Здиарски служб по сей день используются в Elcomsoft iOS Forensic Toolkit.

iOS 8: шифрование на основе кода блокировки. Взлом паролей перестал работать

iOS 8 стала прорывом в области безопасности мобильных операционных систем. Именно в iOS 8 был заложен фундамент той модели безопасности, которая используется в iPhone по сегодняшний день. С точки зрения безопасности изменилось буквально всё. Двухэтапная проверка 2SV включена и для резервных копий. Срок действия маркеров аутентификации сокращён до одного часа.

Модели устройств:

- iOS 8.0 – iPhone 6 и 6 Plus

Начнём с простого — логического анализа.

До выхода iOS 8 Apple использовали следующую практику. При установлении сопряжения между iPhone и другим устройством (подразумевался компьютер пользователя) создавалась запись lockdown, которая сохранялась в виде файла. В старых версиях iOS эта запись была фиксированной; она не менялась никогда, даже после сброса устройства. Раз установив соединение с одним компьютером, пользователь мог подключать iPhone к любому другому устройству — если скопировал файл lockdown. Именно такой файл и создавался в процессе настройки iPhone на заводе. Файл сохранялся на сервере компании, что позволяло Apple добиться сразу двух целей. Во-первых, сотрудники компании могли помочь пользователю, который забыл код блокировки, извлечь из телефона данные. Второй, не декларируемой особенностью данной схемы было сотрудничество с полицией. Если в Apple присылали iPhone с сопроводительным ордером, то компания извлекала из него информацию. Это работало,

даже если код блокировки был неизвестен. При этом разорвать раз установленное соединение было невозможно даже сбросом телефона к заводским настройкам.

Добровольному сотрудничеству с полицией был положен конец с выходом iOS 8. Начиная с этой версии системы для установления с компьютером требуется не один фиксированный ключ, а пара уникальных ключей, которая генерируется при сопряжении нового устройства. Одна половинка ключа сохраняется в самом iPhone, а вторая — передаётся на компьютер пользователя, где и сохраняется в файл lockdown. Стоит удалить любую из половинок, и соединение не установится. Сброс телефона — уничтожаются все сохранённые в нём «половинки», соединение невозможно.

Комбинация шифрования файловой системы динамическим ключом на основе кода блокировки экрана и нового подхода к установлению соединения привела к тому, что ни сотрудники Apple, ни эксперты-криминалисты больше не могут извлечь данные из iPhone на основе заводских записей lockdown. Об этом же написано в официальной инструкции Apple для правоохранительных органов, доступной только на английском языке:

For all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key. All iPhone 6 and later device models are manufactured running iOS 8.0 or a later version of iOS. Apple’s guidelines for law enforcement requests

Для всех устройств, работающих под управлением iOS 8.0 и более поздних версий, Apple не может выполнить извлечение данных с устройства, поскольку данные, запрашиваемые правоохранительными органами, зашифрованы, а у Apple нет ключа шифрования. Все устройства iPhone 6 и более поздние модели производятся под управлением iOS 8.0 или более поздней версии iOS.

Кроме того, в iOS 8 появилась новая подсистема «Ограничения» (в современных версиях iOS – Экранное время), позволяющая установить 4-значный цифровой PIN-код для защиты от некоторых действий с устройством (например, защита от сброса или изменения кода блокировки экрана, установки или удаления приложений).

iOS 8.1: iCloud Photos

Фотографии пользователя теперь можно не только сохранять в облачной резервной копии, но и синхронизировать между устройствами, активировав сервис iCloud Photos. При его включении фотографии автоматически перестают сохраняться в составе облачных резервных копий, однако пользователь может включить эту функцию отдельно.

iOS 8.1: перестали работать IP-BOX, MFC Dongle и аналоги

С этой версии iOS перестали работать многочисленные недорогие устройства для подбора кода блокировки экрана. Для всех более новых версий iOS подбор кода блокировки возможен только с использованием решений Cellebrite или GrayShift с высокой стоимостью и ограниченным распространением.

iOS 9: длина кода блокировки увеличена до 6 цифр

В iOS 9 появилось единственное заметное новшество: длина кода блокировки экрана, которую предлагает система при настройке телефона по умолчанию, увеличена до 6 цифр. Пользователь по-прежнему может настроить 4-значный PIN, но от версии к версии сделать это становится всё сложнее.

В iOS 9 впервые появилось ограничение на время жизни записей о сопряжении (см. следующий раздел); в этой версии системы он составляет 6 месяцев с момента последнего использования. Срок жизни маркеров аутентификации вновь увеличен (ранее был сокращён до 1 часа). Наконец, на смену механизму двухэтапной проверки 2SV пришла привычная и намного более продвинутая двухфакторная аутентификация 2FA.

Модели устройств:

- iOS 9.0.1 – iPhone 6s и 6s Plus

iOS 10: ограничен срок действия записей о сопряжении

До iOS 10 записи о сопряжении (lockdown) действовали в течение длительного времени. В нашей лаборатории хранились записи, которым было несколько месяцев — и они продолжали работать. После того, как полиция начала активно пользоваться записями pairing record, извлекаемыми из компьютеров пользователей, в Apple решили ограничить срок действия этих записей. iOS 10 и более новые версии аннулируют записи о сопряжении через 30 дней с момента последнего использования.

iOS 10 стала и большим шагом назад в том, что касается защиты резервных копий. Начиная с iOS 5 (или iOS 4), Apple использовала один и тот же алгоритм для проверки паролей к резервным копиям iPhone. Для вычисления ключа шифрования вычислялось 20,000 итераций хеш-функции. Это было достаточно медленно и достаточно безопасно. В iOS 10 произошла неожиданность: в защите резервных копий обнаружилась забытая уязвимость, использующая единственную итерацию хеша. На основе этой уязвимости в нашей компании была создана атака со скоростью в десятки миллионов паролей в секунду.

Модели устройств:

- iOS 10.0.1 – iPhone 7 и 7 Plus

iOS 10.1: исправлена проблема с защитой резервных копий

Описанная выше уязвимость в защите резервных копий была исправлена в iOS 10.1; наша компания удостоилась благодарности в сопроводительной документации.

iOS 10.2: серьёзно усилена парольная защита резервных копий

В очередной версии iOS на несколько порядков увеличилось количество итераций хеш-функции, использующейся для проверки пароля. С этого момента перебор пароля к резервной копии стал чрезвычайно медленным: от единиц паролей в минуту с использованием ресурсов центрального процессора до нескольких десятков или сотен паролей в секунду при использовании одного или нескольких графических ускорителей.

iOS 10.3: переход на файловую систему APFS

В iOS 10.3 был осуществлён переход всех обновляемых устройств на новую файловую систему APFS. Сам по себе этот переход не сделал устройства более безопасными, но производителям ПО для анализа данных из iPhone пришлось обновлять пакеты программ. Наш продукт Elcomsoft iOS Forensic Toolkit новшество затронуло по касательной, лишь облегчив обработку ситуации нештатной перезагрузки устройства в процессе установки эксплойта checkm8 (для предыдущих версий системы приходилось обрабатывать ситуацию с флагом “file system dirty”, который был упразднён с переходом на APFS).

iOS 11: сопряжение с компьютером по паролю, пароль к резервной копии можно сбросить

В iOS 11 произошло два крупных изменения. Во-первых, установить сопряжение с новым компьютером теперь можно только в случае, если известен код блокировки: его потребуется ввести после разблокирования экрана (для самой разблокировки, кстати, можно по-прежнему использовать биометрику).

Вторым важным и неоднозначным новшеством стала возможность сброса пароля к резервной копии. Сбросить пароль можно в настройках системы вместе с некоторыми другими настройками (в частности, при сбросе пароля на резервную копию удаляется и код блокировки экрана, что автоматически приводит к удалению таких данных, как список транзакций Apple Pay).

Для сброса пароля к резервной копии потребуется ввести код блокировки экрана. Эта возможность радикально снижает безопасность iOS и упрощает логический анализ устройства, если код блокировки известен.

Модели устройств:

- iOS 11.0 – iPhone 8 и 8 Plus
- iOS 11.0.1 – iPhone X

Срок действия записей о сопряжении ограничен ещё сильнее. Теперь существующие записи о сопряжении (pairing records) остаются действительными в течение 30 дней с момента последнего использования (источник: iOS Security Guide May 2019 edition, iOS 12.3).

В iOS 11 был представлен «аварийный» режим S.O.S., при активации которого отключается возможность разблокировки iPhone биометрическими датчиками. Наконец, в локальные резервные копии перестали сохраняться уведомления.

iOS 11.4: текстовые сообщения в облаке

Текстовые сообщения SMS и iMessage теперь можно синхронизировать с iCloud. Если эта опция включена, то сообщения более не попадают в облачные резервные копии. Для синхронизации сообщений используются контейнеры сквозного шифрования, а для их извлечения необходимо пройти двухфакторную аутентификацию и указать код блокировки или системный пароль любого доверенного устройства, ранее зарегистрированного в учётной записи пользователя.

iOS 11.4.1: защитный режим USB

В iOS 11.4.1 впервые появился защитный режим USB, изначальным предназначением которого было противодействие инструментам для перебора кодов блокировки производства Cellerbrite и Grayshift. iOS 11.4.1 автоматически отключает передачу данных через USB (порт Lightning) через час после того, как экран устройства был заблокирован или отключён от компьютера или аксессуара USB. Кроме того, пользователь может активировать этот режим и вручную, просто запустив режим S.O.S.

iOS 12: расширен режим блокировки USB, Ограничения превратились в Экранное время, Здоровье в облаке

iOS 12 развивает и расширяет ограничения USB. Согласно новому руководству по безопасности iOS, опубликованному Apple после выпуска iOS 12, возможность передачи данных через порт USB блокируется сразу (а не через час, как это было раньше) после блокировки экрана устройства, если с момента последнего подключения

через USB прошло более трех дней или если устройство находится в состоянии, когда для его разблокировки требуется пароль. Кроме того, порт USB блокируется, если пользователь активирует режим S.O.S. В оригинале этот момент описан так:

“In addition, on iOS 12 if it’s been more than three days since a USB connection has been established, the device will disallow new USB connections immediately after it locks. This is to increase protection for users that don’t often make use of such connections. USB connections are also disabled whenever the device is in a state where it requires a passcode to re-enable biometric authentication.”

Кроме того, в iOS 12 на смену Ограничениям пришёл новый сервис — Экранное время. Спустя время настройки и статистика Экранного времени стали доступны для синхронизации через iCloud.

В этой версии iOS появилась синхронизация данных приложения Здоровье в iCloud, а чуть позже эти данные стали защищать посредством сквозного шифрования.

Модели устройств:

– iOS 12.0 – iPhone Xs и Xs Max
– iOS 12.0 – iPhone Xr

iOS 13: смена пароля к резервной копии через код блокировки; защитный режим USB снова расширен

В актуальной на сегодня ветке iOS 13, включающей в себя ответвление iPadOS, Apple отказалась от поддержки приложения iTunes на компьютерах Mac. Теперь резервные копии устройств с iOS/iPadOS создаются прямо из приложения Finder.

Модели устройств:

– iOS 13.0 – iPhone 11 Pro и 11 Pro Max
– iOS 13.0 – iPhone 11

При установке или изменении пароля, защищающего локальную резервную копию, пользователь должен ввести код блокировки экрана iPhone. Пароль необходимо ввести на самом iPhone. Таким образом, роль кода блокировки в iOS 13 окончательно возведена в абсолют; зная код блокировки экрана, с телефоном можно проделать практически всё, что угодно, от сброса пароля на резервную копию до смены пароля к Apple ID и отвязки устройства от iCloud.

Защитный режим USB также был расширен. В iOS 13 появилось своеобразное «сопряжение» аксессуаров. Чтобы подсоединиться к компьютеру, пользователю нужно будет ввести PIN-код на iPhone, после чего устройства обменяются криптографическими ключами. «Сопряжение» аксессуара не использует криптографических ключей; это односторонний процесс, для которого не требуется PIN-код. Аксессуар «сопрягается» с iPhone, когда пользователь впервые подключает его к устройство в момент, когда экран телефона разблокирован (или же разблокирует iPhone уже после подключения аксессуара). iPhone сохранит информацию о «сопряжённом» аксессуаре и присвоит этому аксессуару доверенный статус.

Ограничения USB в iOS 13 различны для ранее сопряжённых и ранее не сопряжённых аксессуаров. В iOS 13 возможность коммуникации через порт USB блокируется через час после того, как телефон был заблокирован или пользователь

отключил ранее сопряжённый аксессуар. При этом подключение аксессуара, которого нет в списке сопряжённых, вызывает мгновенное срабатывание блокировки порта USB.

Наконец, в незашифрованные резервные копии без пароля более не попадает журнал звонков и история браузера Safari.

Одновременно с iOS 13 вышла macOS 10.15.4, в которой необходимо снять флажок карантина для запуска приложений, скачанных не из App Store (как это сделать[85]).

iOS 14: всего понемногу

В iOS 14 появилась масса нововведений, касающихся защиты персональных данных пользователя. С точки зрения эксперта-криминалиста можно отметить изменение путей в файловой системе, по которым хранятся некоторые системные базы данных (подробности[86]).

В этой версии iOS разработчики Apple смогли частично усилить защиту SEP в моделях линеек iPhone 7, 8 и X, что привело к невозможности использования эксплойта checkm8 в режиме BFU (при неизвестном коде блокировки) на этих моделях. Кроме того, взлом устройств джейлбрейком checkra1n стал заметно сложнее; для ряда моделей (поколений A11 и более новых, т.е. iPhone 8, 8 Plus, iPhone X и соответствующих моделей iPad) для этого необходимо будет обнулить код блокировки экрана.

С точки зрения облачной криминалистики изменения минимальны и относятся к деталям технической реализации.

iOS 15: цифровая подпись разделов

В iOS 15 появились цифровые подписи разделов. По этой причине для этой версии ОС нет джейлбрейка checkra1n.

iOS 16: усилена защита ядра, Advanced Data Protection в облаке

В iOS 16.3 появилась поддержка Advanced Data Protection для iCloud, благодаря которой защиту методом сквозного шифрования получили данные, которые ранее были свободно доступны. В их число вошли облачные резервные копии, медиафайлы, многие синхронизированные данные.

Кроме того, в iOS 16 была заметно усилена защита ядра; приложениям стало труднее выбираться из песочницы.

Наконец, с выходом iOS 16 разработчики Apple эффективно закрыли возможность извлечения данных через эксплойт загрузчика для линейки iPhone 8, 8 Plus и iPhone X. Теперь извлечение возможно в том и только в том случае, если на устройстве ни разу с момента начальной настройки не был установлен код блокировки экрана; ситуация, которая в реальной жизни практически не встречается.

При работе с устройствами под управлением iOS 16 необходимо перед установкой агента включить режим разработчика Settings > Privacy & Security > Developer Mode.

[85]https://blog.elcomsoft.com/2020/04/macos-ios-and-icloud-updates-forensic-consequences/
[86] https://blog.d204n6.com/2020/09/ios-14-first-thoughts-and-analysis.html

13.6.Аппаратный ввод в режим DFU: когда не работают кнопки

В процессе анализа и извлечения данных из iPhone может потребоваться переключить устройство в режим DFU. Для старых устройств это даёт возможность доступа к данным через эксплойт checkm8. Переключение в режим DFU требует последовательности нажатий клавиш со строгим соблюдением таймингов. Если устройство повреждено и одна или несколько аппаратных кнопок вышли из строя, ввод в DFU может быть затруднён или невозможен. В данном разделе предлагается альтернативный способ.

Для чего нужен режим DFU

Основная цель перевода iPhone в режим DFU – использование для анализа устройства эксплойта загрузчика, позволяющего извлекать данные из устройств Apple нескольких поколений. Кроме того, режим DFU необходим для взлома кода блокировки на старых моделях iPhone посредством Elcomsoft iOS Forensic Toolkit. Ещё один вариант использования режима DFU — извлечение по методу «до первой разблокировки» (BFU). Наконец, DFU можно использовать для сброса заблокированного телефона (в этом случае данные с устройства будут безвозвратно удалены).

Причины, по которым перевод в DFU может оказаться невозможен

Штатный способ ввода в режим DFU – нажатие и удержание аппаратных клавиш в строгой последовательности. В случаях, когда одна или несколько клавиш повреждены или работают нестабильно (например, окислился контакт и образовался «дребезг»), перевести устройство в режим DFU штатным способом не удастся. В этом случае устройство придётся разобрать, а для перевода в режим DFU – использовать отладочные контакты на системной плате устройства.

Существует **три причины, по которым BootROM (загрузчик) устройства переведёт его в режим DFU.**

1. Последовательность нажатий на кнопки (см. выше)

2. Неудачный запуск LLB

3. Замыкание контакта DFU на системной плате

Рассмотрим сразу третий вариант, поскольку первый – хорошо изучен, а второй невозможно использовать в процессе криминалистического анализа.

В целях диагностики на материнской плате устройств iOS расположено несколько тестовых контактов. Один из них – контакт FORCE_DFU. При загрузке устройства состояние контакта проверяется загрузчиком, и если к нему приложено напряжение 3,3В, устройство переводится в режим DFU. Рассмотрим этот процесс на примере iPhone5.

Для подключения к контактам на материнской плате используем сигнальный кабель. Для других моделей iPhone процедура отличается только тем, какой именно контакт необходимо подключить к кабелю.

Вам потребуется следующее:

- iPhone (например, iPhone5, как в этом примере)
- Отвёртки и другие инструменты для разборки устройства
- Сигнальный кабель

– Кабель USB

Проще всего процедура выполняется командой из двух человек. При выполнении процедуры в одну пару рук вам потребуются дополнительные инструменты:

– Стандартное зарядное устройство, подключённое в розетке к сети питания

– Электророзетка с выключателем

Инструкции:

1. Убедитесь, что устройство заряжено. Выключите телефон.

2. Разберите устройство, чтобы обеспечить доступ к системной плате. Обратите внимание: возможно, вам придётся снять фольгу, выполняющую роль электромагнитного экрана. Подробные инструкции по разборке разных моделей iPhone доступны на сайте компания iFixit.

3. Подключите к телефону кабель USB. Пока не подключайте кабель к компьютеру.

4. Используйте сигнальный кабель, подключив его к соответствующим диагностическим разъёмам, обозначенных на схемах ниже (соответственно устройству). Затем, удерживая контакт, попросите ассистента подключить другой конец USB-кабеля к компьютеру. Удерживайте провод подключённым несколько секунд.

5. Экран телефона должен оставаться черным, а компьютер должен распознать устройство в режиме DFU.

В случае, когда процедура выполняется без ассистента:

1.1 Подключите другой конец USB-кабеля к зарядному устройству.

1.2 Подключите зарядное устройство к розетке с выключателем. (Пока не включайте зарядку!)

1.3 Соедините два контакта проводом.

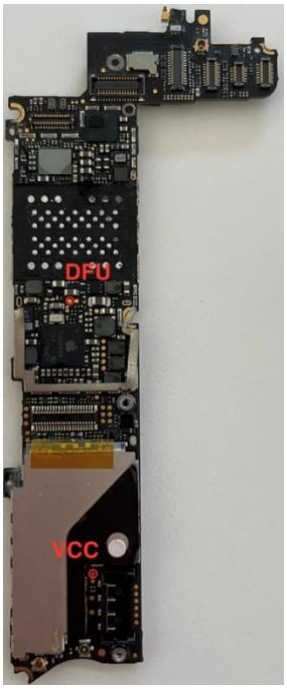
1.4 Ногой включите выключатель питания в розетке. Удерживайте соединение сигнального провода с тесовым контактом в течение нескольких секунд.

5.1 Экран должен оставаться черным. Если устройство загружается в штатном режиме, выключите его и повторите попытку.

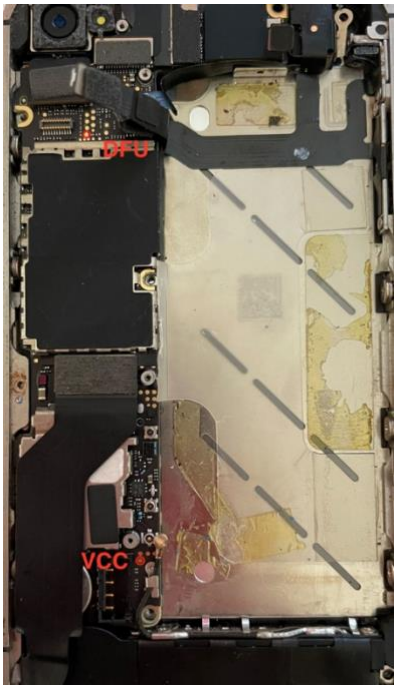
5.2 Если экран остаётся черным, можно отпустить провод.

Отсоедините USB-кабель от зарядного устройства и подключите его к компьютеру. Компьютер должен распознать устройство в режиме DFU.

В **iPhone 4** используются следующие контакты:



iPhone 4s:



В **iPhone 5** используются следующие контакты:


WARNING
Potential for fire or burning. Do not disassemble, puncture, crush, heat, or burn.
Li-ion Polymer Battery
3.8V ⎓ 5.45Whr
APN: 616-0613
VPN: LIS1491APPCS
1440mAh
Apple Japan
Li-ion
DFU
VCC

iPhone 5c:

iPhone 5s:

iPhone 6:

iPhone 6s Plus:

iPhone SE (первое поколение):

iPhone 7

13.7.Использование USB хабов для повышения стабильности работы checkm8/checkra1n с компьютерами на Apple Silicon

Процесс установки эксплойта *checkm8,* позволяющего провести криминалистически чистое извлечение данных из ряда моделей iPhone, может оказаться достаточно капризным и ненадёжным в зависимости от используемого оборудования.

Мы обнаружили, что при подключении iPhone к компьютерам Mac на платформе Apple Silicon использование промежуточного USB хаба может помочь в случаях проблем с установкой эксплойта.

iPhone подключается к **Intel Mac**: эксплойт устанавливается как с USB хабом, так и без него. В случае возникновения проблем попробуйте подключиться напрямую. Кабели с Type-C по-прежнему не поддерживаются.

M1, M2 (Apple Silicon) Mac: если вы используете **USB хаб**, то эксплойт будет уверенно устанавливаться на все совместимые модели iPhone.

M1, M2 (Apple Silicon) Mac без USB хаба: некоторые модели iPhone потребуют переподключения (reconnect) в процессе установки эксплойта. iOS Forensic Toolkit выдаст соответствующий запрос. Достаточно отключить кабель от iPhone и подключить его снова.

На некоторые модели iPhone эксплойт без хаба не установится. Список таких моделей приводится ниже.

	Intel	Apple Silicon	
		no hub	*w/hub*
iPhone 5	+	reconnect	+
iPhone 5s	+	reconnect	+
iPhone 6	+	-	+
iPhone 6s	+	-	+
iPhone SE	+	-	+
iPhone 7	+	reconnect	+

13.8. Использование обычной учётной записи для подписи агента-экстрактора

Использование обычной учётной записи Apple ID для подписи агента-экстрактора обладает некоторыми особенностями.

1. После установки агента-экстрактора необходимо подтвердить сертификат в настройках устройства. Для этого устройству потребуется доступ в интернет, что связано с рядом рисков.

2. Успешно подтвердить сертификат не удастся, если дата или время на устройстве не соответствуют действительному. Если возникает ошибка, убедитесь, что устройство показывает точные дату и время.

13.9.Raspberry Pi Pico: функции автоматизации

Одноплатный микроконтроллер Raspberry Pi Pico можно использовать для автоматизации нескольких рутинных операций.

13.9.1. Автоматический ввод в DFU

Перевод устройства в режим DFU – первый и необходимый шаг, предшествующий низкоуровневому извлечению данных посредством checkm8. Стандартная процедура перевода в режим DFU требует последовательного нажатия кнопок на устройстве и точного соблюдения таймингов; особую сложность

представляет перевод в DFU устройств с отказавшими кнопками. Новый способ перевода в DFU максимально прост, корректно переводя в режим DFU в том числе и частично неработоспособные устройства. Для того, чтобы воспользоваться новым способом, вам понадобится одноплатный микроконтроллер Raspberry Pi Pico с разработанной нами программой прошивки и дополнительными кабелями.

Ранее мы уже писали о том, как Raspberry Pi Pico помогает разблокировке и извлечению данных из iPhone 4s. Для нового процесса вам понадобится несколько другая сборка.

Совместимость:

– Процесс авто-DFU не поддерживает старые модели iPhone (iPhone 7 и старше)

– Совместимость с более новыми моделями iPhone (iPhone Xs/Xr и новее) возможна, но не гарантируется.

Вам понадобятся:

– Одноплатный микроконтроллер Raspberry Pi Pico с контактами.

– Адаптер USB-A – micro-USB (для прошивки Pico с компьютера Mac)

– Специальный кабель Lightning.

Подготовка специального кабеля Lightning

Сам по себе этот кабель предельно прост: на одном конце – коннектор Lightning без чипа, на другом – провода или 4 коннектора Dupont для подключения к Pico. От Lightning[87] нам потребуется всего четыре провода:

– GND (Black)

– 5V (Red)

– ID0 (Yellow)

– ID1 (Blue)

Внимание: на вашем экземпляре кабеля цвета проводов могут отличаться. Обязательно проверьте распиновку вольтметром!

Важно: требуется такой кабель, в котором нет встроенного чипа в коннекторе Lightning. В таком качестве идеально подходит удлинитель (Lightning male <> Lightning female), т.к. все остальные кабели оснащены чипом. Рекомендуем подобный кабель:

Средняя цена этих кабелей обычно составляет от 1,5 до 2 долларов. Рекомендуем запастись кабелями, так как кабель будет использоваться в качестве «донора»: его придётся разрезать и припаивать разъёмы к вышеупомянутым линиям/проводам.

Наконец, рекомендуем подобный набор соединительных кабелей для подключения к разъёмам Pico:

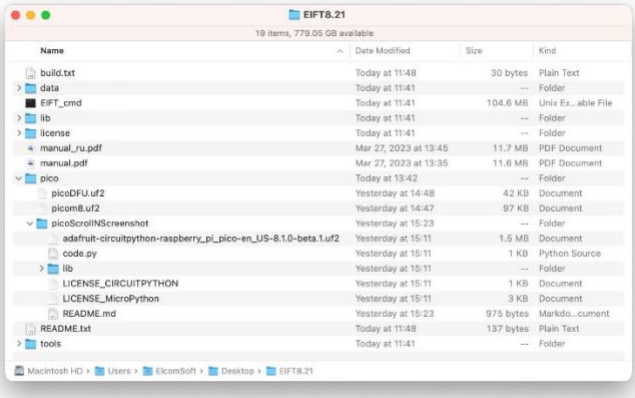
[87] https://en.wikipedia.org/wiki/Lightning_(connector)

В качестве альтернативы вы можете использовать кабели, продающиеся под названиями *Dupont Cable Female* (или “Hookup Wire for Arduino cable”), к которым можно просто подпаять провода, если внешний вид конструкции неважен.

13.9.1.1.Подготовка к работе

Единственное, что нужно сделать с платой Pico, это установить соответствующую прошивку. Для этого подключите плату Pico к Mac с помощью кабеля USB-micro-USB, одновременно зажав кнопку на плате Pico; он будет распознан как внешнее хранилище. Затем перетащите на него следующий файл из папки установки EIFT:

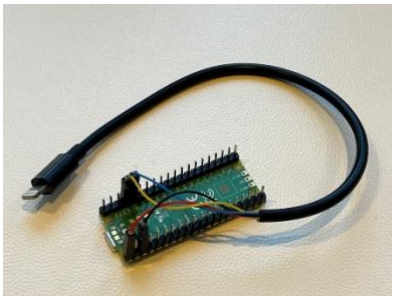
```
/pico/picoDFU.uf2
```



Светодиод на плате Pico будет мигать, после чего Pico отсоединится от компьютера. Эта часть подготовки завершена. Переподключите Pico к Mac (на плату будет подано питание), после чего подключите кабель к соответствующим разъёмам на плате:

```
5V (Red)      <-> VBUS
GND (Black)   <-> GND
ID0 (Yellow) <-> GP2
ID1 (Blue)    <-> GP3
```

Вы можете подключить два последних разъёма в обратном порядке: ID0 к GP3, ID1 к GP2.



13.9.1.2.Ввод в DFU

После того, как Pico собран и прошит, а специальный кабель Lightning подключён к разъёмам на Pico, остальной процесс не представляет сложности. Для перевода устройства в DFU проделайте следующие шаги.

1. Если устройство включено, выключите его

2. Введите устройство в режим Recovery mode: нажмите кнопку уменьшения громкости, после чего подключите его к компьютеру стандартным Lightning кабелем, и удерживайте кнопку до тех пор, пока устройство не перейдёт в Recovery

3. Используйте команду **./EIFT_cmd tools autobootFalse** для блокировки автозагрузки (чтобы устройство случайно не загрузилось в обычном режиме ни при каких обстоятельствах)

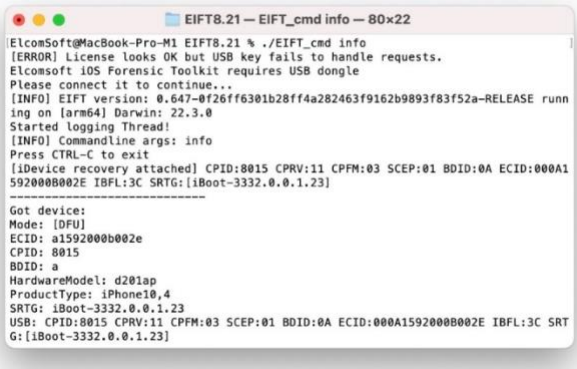
4. Подключите Pico к питанию через micro-USB

5. Подключите устройство к разъёму Lightning специального кабеля, который в свою очередь подключён к разъёмам на Pico

6. Устройство должно перейти в режим DFU

На этом процесс завершён. Вы можете подключить iPhone к Mac и использовать EIFT[88] для извлечения данных из iPhone посредством checkm8.

[88] https://www.elcomsoft.ru/eift.html



13.9.1.3. Информация об авторском праве

Код для picoDFU взят из проекта Tamarin firmware[89], который доступен под лицензией GPLv3. В соответствие с этой лицензией мы в скором времени опубликуем наш код.

13.9.2. Длинные скриншоты (скриншоты с прокруткой)

Автоматизацию снимков экрана можно рассматривать как новый способ доступа к данным, позволяющий извлечь информацию, недоступную в рамках расширенного логического анализа (например, историю переписки в защищённых программах мгновенного обмена сообщениями). Новый способ доступа дополняет возможности расширенного логического анализа и расширяет набор доступных для исследования данных.

Микроконтроллер Raspberry Pi Pico поможет частично автоматизировать процесс снятия «длинных» снимков экрана (скриншотов с прокруткой). Полуавтоматический режим снятия скриншотов доступен для всех моделей iPhone и версий iOS, но требует подключения исследуемого iPhone к Raspberry Pi под управлением нашей прошивки.

13.9.2.1. Настройка Raspberry Pi Pico

По сравнению с автоматическим вводом в режим DFU требования к процессу снятия скриншотов ниже. Помимо, собственно, iPhone или iPad, с которого будут сделаны снимки экрана, вам потребуются:

- Одноплатный микроконтроллер Raspberry Pi Pico
- Lightning to USB (официальный Apple Camera Adapter или его аналог)
- USB-A to micro-USB (как для прошивки, так и для подключения айфона к Pico через адаптер Lightning to USB)
- Проводная (USB) мышь с колесом прокрутки (опционально)

Далее необходимо подготовить Raspberry Pi Pico, установив на него требуемые файлы. Для этого:

- **Прошейте circuitpython на Raspberry Pi Pico**
  - Зажмите и удерживайте кнопку BOOTSEL

[89] https://github.com/stacksmashing/tamarin-firmware

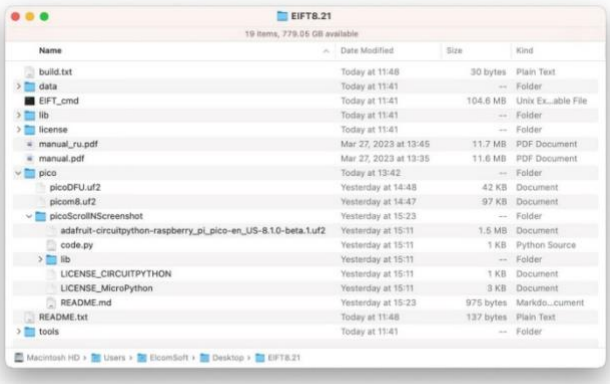
- Подключите к компьютеру USB-кабель
- Скопируйте файл **.uf2** на определившийся накопитель под названием RPI-RP2
- Накопитель будет подключён заново и получит новое имя CIRCUITPY

– **Установите код**
- На диске CIRCUITPY удалите все файлы
- Скопируйте каталог lib на диск CIRCUITPY
- Скопируйте файл code.py на диск CIRCUITPY

Путь к прошивке:

```
pico/picoScrollNScreenshot/adafruit-(...).uf2
```

Файлы, которые нужно скопировать на диск (code.py и папка lib) расположены по тому же пути.



После того, как все необходимые файлы будут переданы на Pico, проделайте следующие шаги:

1. Отключите Pico от компьютера

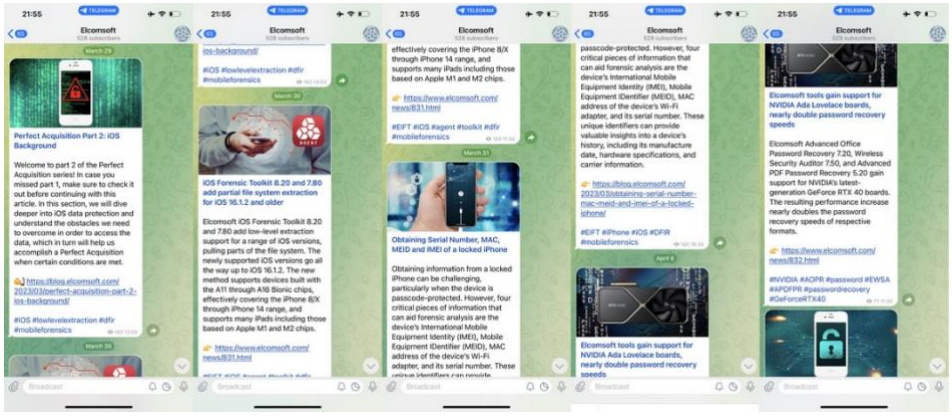
2. Подключите к iPhone адаптер USB

3. Соедините Pico (micro USB) с iPhone (точнее, с подключённым к телефону USB-адаптером)

4. Приблизительно через 15 секунд начнут создаваться скриншоты. Процесс будет продолжаться до тех пор, пока телефон не будет отключён от Pico.

Дополнительное питание не требуется, т.к. Pico получает напряжение 5В от разъёма USB. Если используется адаптер Apple Camera Adapter, вы можете использовать дополнительный порт Lightning для того, чтобы запитать от него iPhone (чтобы не допустить разрядки аккумулятора в процессе работы).

После того, как снимки экрана сделаны, скопируйте их на компьютер (извлечением медиа-файлов, используя полное логическое извлечение или через AirDrop). Возможно, вы захотите произвести склейку скриншотов, для чего можно воспользоваться одним из множества приложений для iOS, например – Tailor[90].



Наконец, вы сможете произвести распознавание текста на скриншотах для последующей индексации и анализа.

13.9.2.2.Особенности и решение проблем

Процесс не всегда срабатывает с первого раза, и проблема не в снимках экрана, которые успешно снимаются в любом случае, а в прокрутке. Увеличить вероятность успешной прокрутки можно, подключив кабелем USB обычную проводную мышь с колесом прокрутки и несколько раз прокрутив содержимое окна вверх-вниз упомянутым колесом.

Кроме того, мы не вполне уверены, что метод сработает с использованием сторонних адаптеров Lightning-USB. С адаптером от Apple проблем не возникает.

Вы можете отредактировать файл *code.py*, а именно – следующие опции:

```
SCROLL_WITH_MOUSE = 1
SCROLL_MOUSE_DISTANCE = 250
DELAY_AFTER_SCROLL = 1
```

SCROLL_WITH_MOUSE отвечает за то, эмулируется ли клавиатура (значение 0) или мышь (1). Первый режим более надёжен, но некоторые приложения его не поддерживают (например, Telegram).

[90] https://github.com/stacksmashing/tamarin-firmware

SCROLL_MOUSE_DISTANCE используется только при эмуляции мыши, и устанавливает дистанцию прокрутки. Мы экспериментально определили оптимальное значение этого параметра (250); рекомендуем использовать его, если скриншоты в дальнейшем планируется склеивать. Если на каком-то устройстве возникают проблемы с избыточным перекрытием или, наоборот, избыточной прокруткой скриншотов, измените значение этого параметра.

DELAY_AFTER_SCROLL контролирует задержку между тем, как осуществлена прокрутка, и снятием снимка экрана. По умолчанию задержка – 1 секунда. Этот интервал введён для того, чтобы на странице после прокрутки успели прогрузиться изображения и информация о ссылках.

Обратите внимание, что по умолчанию прокрутка ведётся сверху вниз. Соответственно, начинать работу нужно с верхней части страницы или чата.

Учтите, что скрипт начинает работать сразу после того, как Pico подключается к любому устройству, включая компьютер Mac. Из-за этого мы ввели 15-секундную задержку между подключением и началом работы скрипта. Это позволяет, например, отредактировать или удалить файл *code.py*.

Наконец, имейте в виду, что скрипт не может определить момент, когда экран прокручен до конца, и продолжает делать снимки экрана. Процесс необходимо остановить вручную, просто отключив кабель.

13.9.2.3. Экспериментальный статус

Новая возможность носит статус экспериментальной. Процесс далёк от совершенства; основная проблема в том, что скриншоты снимаются и сохраняются на самом устройстве, а не на компьютере. В то же время новый метод может оказаться единственным способом извлечения некоторых типов данных из ряда приложений, если устройство не имеет уязвимого к эксплойтам загрузчика, а установленная версия ОС не поддерживается агентом-экстрактором.

13.10. Raspberry Pi 3/4: функциональный файрволл для безопасной установки агента-экстрактора

Процесс низкоуровневого извлечения данных из iPhone и iPad требует установки на устройство специальной программы - агента-экстрактора. Агент чрезвычайно прост в использовании, но после последних изменений на стороне Apple его установка стала вызывать проблемы даже у опытных пользователей. В этом разделе мы описываем вариант решения - прошивку для Raspberry Pi 4, превращающую устройство в функциональный файрволл, который позволяет верифицировать цифровую подпись агента, блокируя попытки доступа подключённого iPhone к интернету.

13.10.1. Дополнительное оборудование

Для настройки файрволла и подключения к нему iPhone вам потребуется дополнительное оборудование:

- Raspberry Pi 4 или более новая модель (например, Raspberry Pi 4 Model B)
- Карта microSD
- Адаптер Lightning to Ethernet

– Адаптер USB to Ethernet

13.10.2. Инструкции по установке прошивки на Raspberry Pi

Скачайте образ прошивки из GitHub - Elcomsoft/eiftpi[91] и запишите его на SD-карту с помощью программы, например, balenaEtcher. Вы можете скачать balenaEtcher по следующей ссылке: https://etcher.balena.io/.

– Вставьте SD-карту в компьютер.
– Запустите balenaEtcher и выберите скачанный образ прошивки.
– Выберите SD-карту как целевой носитель.
– Нажмите кнопку "Записать", чтобы записать образ прошивки на SD-карту.
– По завершении процесса извлеките SD-карту из компьютера.

На Raspberry Pi вам понадобятся два сетевых интерфейса. Один интерфейс должен быть подключён к интернету, а другой будет использоваться для подключения iPhone. Для подключения iPhone вам понадобится адаптер Lightning to Ethernet. Доступно два варианта подключения:

1. Вы можете подключить Raspberry Pi к интернету через Wi-Fi, а iPhone подключить через порт Ethernet.

2. Либо используйте встроенный Ethernet-порт на Raspberry Pi для подключения к интернет, организовав второй интерфейс с помощью адаптера USB-A to Ethernet.

Важно: телефон необходимо подключать к встроенному в плату Ethernet, а сам Pi к интернету - либо по Wi-Fi, либо через USB-адаптер.

Примечание: Мы не рекомендуем прямое подключение Raspberry Pi к маршрутизатору и настройку беспроводной точки доступа на Pi, так как это в результате iPhone может подключиться к другой сети. Кроме того, этот метод требует дополнительных настроек.

• Для более простой и надёжной установки используйте два проводных подключения. Для этого вам потребуется адаптер USB to Ethernet.

Если в**ы предпочитаете подключить Raspberry Pi через Wi-Fi**, выполните следующие шаги:

[91] https://github.com/Elcomsoft/eiftpi

1. Подключите Raspberry Pi к компьютеру Mac с помощью Ethernet. (Если у вашего MacBook нет Ethernet-порта, вам понадобится дополнительный адаптер USB-C to Ethernet или USB-A to Ethernet.)

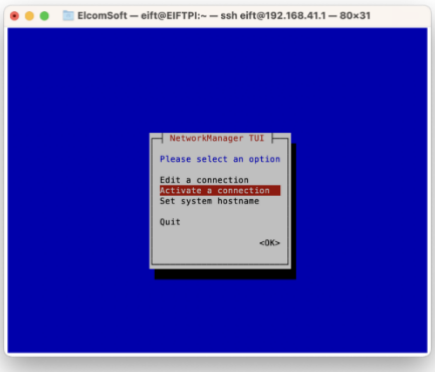
2. Откройте терминал на компьютере Mac и введите следующую команду:

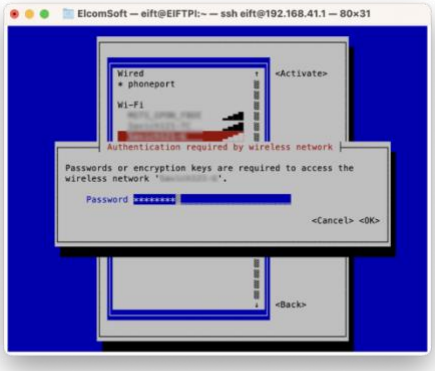
3. ssh eift@192.168.41.1

4. Пароль - "Elcomsoft" (без кавычек).

5. После входа выполните следующую команду для настройки Wi-Fi: sudo nmtui

6. В интерфейсе nmtui вы сможете легко подключиться к Wi-Fi сети.





На этом всё! Вы успешно установили прошивку на Raspberry Pi. Подключите Pi к сети (через Ethernet или Wi-Fi), после чего подключите iPhone к Pi с помощью кабеля. Рекомендуем для начала подключить таким образом тестовый iPhone, чтобы убедиться, что доступ к интернету ограничен: на iPhone должны быть доступны только адреса ppq.apple.com и humb.apple.com.

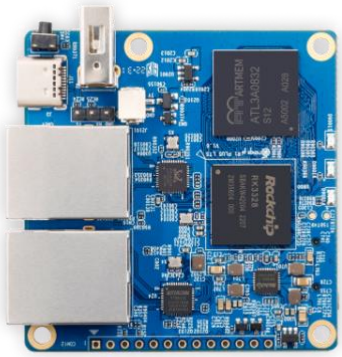
13.11. Orange Pi R1 Plus LTS: функциональный файрволл для безопасной установки агента-экстрактора

С той же целью, что и Raspberry Pi, можно использовать и одноплатный микрокомпьютер Orange Pi R1 Plus LTS, отличающийся в первую очередь наличием второго порта Ethernet. Raspberry Pi 4 мощнее и более универсален, но именно для работы в качестве файрволла Orange Pi R1 Plus LTS подходит лучше. Выделим его основные преимущества:

1. Доступность: Orange Pi R1 Plus LTS легко найти в свободной продаже. Наш же проект EIFTPI свободно распространяется на GitHub с открытым исходным кодом.

2. Дешевизна: Orange Pi R1 Plus LTS доступен за очень небольшие деньги; в сравнении с Raspberry Pi 4 он заметно дешевле. Наличие второго порта Ethernet позволит сэкономить и на покупке адаптера USB-Ethernet, который потребовался бы в случае с Raspberry Pi 4.

3. Два сетевых порта: в устройстве не один, а два физических сетевых интерфейса Ethernet: "LAN" (расположен рядом с портом USB-C) и "WAN." В нашем решении порт **LAN** используется для подключения платы к интернету, а порт **WAN** - для подключения к плате устройства iPhone или iPad через соответствующий переходник USB-C - Ethernet или Lightning - Ethernet).



13.11.1. Дополнительное оборудование

Для настройки файерволла и **подключения к нему iPhone** вам потребуется дополнительное оборудование:

– Карта microSD

– Блок питания или кабель Type-C для подключения Orange Pi R1 Plus LTS (энергопотребление платы настолько невелико, что вполне хватает питания, подаваемого с портов USB-C компьютера Mac или MacBook)

– Адаптер для подключения к порту Ethernet устройств iPhone или iPad (USB-C - Ethernet или Lightning - Ethernet)

– Два сетевых кабеля Ethernet: один для подключения платы к роутеру, второй - для подключения к плате iPhone или iPad

13.11.2. Инструкции по установке прошивки на Orange Pi R1 Plus LTS

Скачайте образ прошивки из GitHub - Elcoms[92]oft/eiftpi и запишите его на SD-карту:

1. Вставьте SD-карту в компьютер.

2. Запустите выбранное приложение для прошивки и выберите скачанный образ.

[92] https://github.com/Elcomsoft/eiftpi

3. Выберите SD-карту как целевой носитель.

4. Нажмите кнопку "Записать", чтобы записать образ прошивки на SD-карту.

5. По завершении процесса извлеките SD-карту из компьютера.

6. Далее всё просто:

7. Установите карту microSD с прошивкой в Orange Pi R1 Plus LTS и подключите плату к питанию

8. Подключите к плате iPhone при помощи адаптера Lightning - Ethernet. Внимание: на Orange Pi R1 Plus LTS используйте порт WAN

9. Подключите плату Orange Pi R1 Plus LTS к интернету. Используйте для этого порт LAN

Важно: при использовании Orange Pi R1 Plus LTS в качестве файрволла, всегда подключайте iPhone или iPad к порту, который расположен поблизости от коннектора GPIO (он помечен как "WAN"). Второй порт, который расположен поблизости от порта USB-C и помечен как "LAN", используется для подключения платы Orange Pi R1 Plus LTS к интернету.

Если вы предпочитаете беспроводное подключение через Wi-Fi (не рекомендуется) или хотите самостоятельно собрать образ прошивки, на сайте проекта GitHub - Elcomsoft/eiftpi[93] есть дополнительные инструкции.

14. Список литературы

1. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. Москва: Стандарт-информ, 2014.
2. ГОСТ Р ИСО/МЭК 27050-1:2019. Информационные технологии. Методы обеспечения безопасности. Выявление и раскрытие электронной информации. Часть 1. Обзор и концепции. Москва: Стандартинформ, 2019.
3. Типовая методика исследования информации в мобильных телефонах / Тушканова О. В. [и др.]. М.: ЭКЦ МВД России, 2014.

[93] https://github.com/Elcomsoft/eiftpi

4. Цифровые следы преступлений: монография / Багмет А.М. [и др.]. Москва: Проспект, 2021. 168 с. ISBN 978-5-392-32868-0
5. Электронные доказательства в уголовном судопроизводстве: учебное пособие для ВУЗов / Зуев С.В. [и др.]. Москва: Юрайт, 2020. 193 с. ISBN 978-5-534-13286-1
6. Цифровая криминалистика: учебник для вузов / В.Б. Вехов [и др.]. Москва: Юрайт, 2022. 417 с. ISBN 978-5-534-14600-4

О компании

Компания «ЭлкомСофт» основана в 1990 году в Москве. С 1997 года Элкомсофт специализируется на разработке решений в сфере информационной безопасности и цифровой криминалистики.

Решения для мобильной и цифровой криминалистики

В компании «ЭлкомСофт» разработана полноценная линейка продуктов для извлечения информации из ряда мобильных устройств и получения доступа к зашифрованной информации, хранящейся как в мобильных устройствах, так и на персональных компьютерах. С помощью продуктов компании криминалисты могут получить доступ к информации, хранящейся в мобильных устройствах. Помимо прочего, возможно извлечение и просмотр информации из учётных записей Apple, Google и Microsoft Account, что автоматически предоставляет доступ к массиву данных о пользователе, накопленному различными службами указанных компаний.

Продукты ЭлкомСофт зарегистрированы в Едином реестре российских программ для электронных вычислительных машин и баз данных с присвоением класса программного обеспечения, к которому относятся «Средства обеспечения информационной безопасности, Информационные системы для решения специфических отраслевых задач», «Программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий».

- Elcomsoft Premium Forensic Bundle, **№11766 от 18.10.2021**
- Elcomsoft Desktop Forensic Bundle, **№11768 от 18.10.2021**
- Elcomsoft Password Recovery Bundle, **№6446 от 07.04.2020**
- Elcomsoft Mobile Forensic Bundle, **№7320 от 30.11.2020**
- Elcomsoft iOS Forensic Toolkit, **№7361 от 30.11.2020**
- Elcomsoft Distributed Password Recovery, **№11632 от 28.09.2021**

Контакты

сайт: **www.elcomsoft.ru**
блог: **blog.elcomsoft.ru**
электронная почта: **info@elcomsoft.com**