



ELCOMSOFT

# Методы извлечения данных из устройств под управлением iOS

# Извлечение данных из iPhone

## Содержание

### Способы извлечения данных

- Логическое извлечение
- Извлечение посредством джейлбрейка
- Использование уязвимости в коде загрузчика
- Извлечение без джейлбрейка
- Достоинства и недостатки подходов



# Извлечение данных из iPhone

## Эти методы не работают

- JTAG: отладочный порт отсутствует (с технической точки зрения, его может заменить порт USB; практическая ценность низкая)
- Извлечение микросхемы памяти: шифрование делает извлечение микросхем памяти бесполезным



# Извлечение данных из iPhone

## Методы извлечения данных

- **Логический анализ**
  - Резервные копии (с паролем или без); в резервных копиях с паролем – часть содержимого Связки ключей
  - Медиа-файлы и открытые данные приложений
  - Журналы crash logs
- **Физическое извлечение**
  - Образ файловой системы
  - Полное содержимое Связки ключей (пароли и токены)

# Извлечение данных из iPhone

## Методы извлечения данных

### Логическое извлечение посредством резервных копий

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

# Извлечение данных из iPhone

## Особенности физического извлечения данных

- **Требуется низкоуровневый доступ к файловой системе**
  - Способ 1: установка джейлбрейка из публичных источников
  - Способ 2: использование аппаратной уязвимости в BootRom
  - Способ 3: использование программы-агента

# Извлечение данных из iPhone

## Особенности физического извлечения данных

- **Способ 1: установка джейлбрейка из публичных источников**
  - Несложная процедура
  - Требуется точное следование инструкциям
  - Есть риски (нежелательная модификация системного раздела, установка на устройство нежелательного ПО и т.п.)
  - После удаления остаются следы, а нормальная работа устройства может быть нарушена
  - Может потребоваться учётная запись разработчика
  - Возможна установка с enterprise-сертификатом или через AltStore
  - Может понадобиться установка ssh-клиента
  - **Административный запрет в ряде организаций**

# Извлечение данных из iPhone

## Особенности физического извлечения данных

- **Способ 2: использование аппаратной уязвимости в BootRom**
  - Аппаратная уязвимость существует в устройствах поколений A7-A11 (iPhone 5s...8/8Plus, iPhone X, соответствующие модели iPad, Apple TV)
  - Не зависит от версий iOS, не может быть исправлена
  - Эксплойт checkm8, джейлбрейк checkra1n
  - **Вариант 1:** прямая эксплуатация уязвимости для доступа к файловой системе и Связке ключей
  - **Вариант 2:** работа через джейлбрейк checkra1n с тем же результатом
  - Частичное извлечение файловой системы и Связки ключей из устройств с неизвестным паролем



# Извлечение данных из iPhone

## Особенности физического извлечения данных

- **Способ 3: использование программы-агента**
  - Не требует установки джейлбрейка
  - После удаления не оставляет явных следов и не нарушает работу устройства
  - Максимальная безопасность и скорость работы
  - Требуется использование учётной записи Apple ID, зарегистрированной в программе Apple для разработчиков
  - Совместимость ограничена: на данный момент iOS 11 и 12 (9-10 и 13 в процессе реализации)

	Физический анализ	Логический анализ
Времязатраты	<b>35-180 минут</b> (в зависимости от модели и объёма памяти)	<b>Минуты</b> (без пароля или пароль известен) <b>Неизвестно</b> (неизвестный пароль)
Связка ключей	<b>Да</b>	<b>Нет</b> (резервная копия без пароля) <b>Да</b> (резервная копия с паролем)
Удалённые файлы	<b>Нет</b>	<b>Нет</b>
Удалённые записи SQLite	<b>Да</b>	<b>Да</b>
Возможные проблемы	Jailbreak; PIN/пароль блокировки	Неизвестный пароль, низкая скорость восстановления; требуется PIN/пароль блокировки устройства для связи с компьютером, сброса пароля на резервную копию; <b>iOS 13:</b> установка пароля на резервную копию

	Физический анализ	Логический анализ
Резервная копия устройства	Да (больше данных)	Да (количество доступных данных больше в резервных копиях с паролем)
Контакты, календари, заметки, звонки	Да	Да
Сообщения (SMS, iMessage)	Да	Да
История местоположения	Да	Да
Сообщения Email	Да	Нет
Данные сторонних приложений	Да	Некоторые
Системные данные	Да	Некоторые

# Физическое извлечение данных

## Чего нет в резервных копиях

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



# Физическое извлечение данных

## Достоинства метода

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



# Физическое извлечение данных

## Ограничения метода

- Требуется прямой доступ к файловой системе, а следовательно – эскалация привилегий
- Требуется PIN/пароль блокировки
- **Эскалация привилегий доступна далеко не для всех платформ и версий iOS**
- Для некоторых комбинаций аппаратных платформ и версий iOS извлечение [пока] возможно только с установкой джейлбрейка



# Извлечение данных из iPhone

## Особенности физического извлечения данных

- Требуется низкоуровневый доступ к файловой системе
  - Способ 1: установка джейлбрейка из публичных источников
  - Способ 2: использование аппаратной уязвимости в BootRom
  - Способ 3: использование программы-агента

# Физическое извлечение данных

## Способ 1: с использованием джейлбрейка

Происходит взлом устройства

- Jailbreak использует найденные уязвимости
- Установка jailbreak – комплексный процесс; **результат не гарантирован**
- Модификация системного раздела (иногда возможен rootless) и раздела данных



# Физическое извлечение данных

## Общее для всех способов

- Извлекается образ файловой системы
  - Папки и файлы в виде TAR архива
  - iOS 13: для доступа к некоторым папкам необходимы специальные привилегии
  - iOS 13: данные Screen Time (возможно, что-то ещё) доступны только ядру
- Расшифровать связку ключей можно **полностью**, включая записи ThisDeviceOnly
- **Метод оптимально работает в сочетании с логическим извлечением данных**

# Физическое извлечение данных

## Способ 1: с использованием джейлбрейка

### Происходит взлом устройства

- Следы после удаления
  - Возможны проблемы с нормальной работой устройства
- Риск получения неработоспособного устройства
  - В iOS 11..13 риск минимален (но остаётся)
- Для установки jailbreak требуется PIN/пароль блокировки
- При установке часто необходимо предоставить iPhone доступ к Интернет
  - Возможна удалённая блокировка устройства, удалённое уничтожение информации

# Физическое извлечение данных

## Способ 1: особенности

- **iOS 12/13:** порт Lightning может быть заблокирован сразу после блокировки экрана
- Экран устройства должен оставаться разблокированным в течение всего процесса извлечения данных
  - В противном случае часть данных будет недоступна

# Физическое извлечение данных

## Способ 1: инструменты

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

# Физическое извлечение данных

## Способ 2: с использованием аппаратной уязвимости

- Использует аппаратную уязвимость в Bootrom (checkm8)
- Совместим с большинством версий iOS
- Извлечение с использованием джейлбрейка checkra1n или без него
- Использование аппаратной уязвимости через джейлбрейк checkra1n имеет те же последствия, что и использование других типов джейлбрейков
- Использование уязвимости без джейлбрейка checkra1n поддерживается в ограниченном числе продуктов

# Физическое извлечение данных

## Способ 2: с использованием аппаратной уязвимости

- Установка checkra1n через режим DFU
- В отличие от классических типов джейлбрейков, обходит режим ограничений USB (начиная с версии 0.9.6, наоборот, активизирует его)
- Возможно частичное извлечение файловой системы и Связки ключей из iPhone с неизвестным паролем
- Частичное извлечение даёт доступ к только ограниченному количеству данных

# Использование джейлбрейк

## Что делает джейлбрейк

- Эскалация привилегий, что позволяет:
  - Устанавливать и запускать любые приложения, включая неподписанные
  - Получать доступ к приватным данным приложений (песочницам)
  - Получать доступ к файловой системе, расшифровать Связку ключей



# Использование джейлбрейк

## Классические утилиты джейлбрейк

- Доступ к корневой файловой системе “/”
- Требуется перемонтирование файловой системы для доступа к корню
- Модифицирует системные файлы
- Обновления OTA невозможны даже после удаления
- Оставляет множество следов
- В отдельных случаях устройство нестабильно даже после восстановления через iTunes



# Использование джейлбрейк

## Джейлбрейк Rootless

- “Rootless” означает «без доступа к корню файловой системы»
- Возможна установка без связи с интернетом (использование учётной записи разработчика)
- Доступ к папке **/var**
- Все модифицированные файлы только в папке **/var**
- Оставляет минимум следов
- Более стабильная работа
- Джейлбрейк Rootless предпочтителен с точки зрения криминалистики



# Использование джейлбрейк

## Эксплойт Checkm8

- Опубликован в сентябре 2019
- Использует аппаратную уязвимость в Bootrom
- **Apple не сможет его исправить**
- Поддерживает процессоры A5 - A11
- Поддерживает все версии iOS
- iPhone 4S до iPhone X включительно



EPIC JAILBREAK: Introducing checkm8 (read "checkmate"), a permanent unpatchable bootrom exploit for hundreds of millions of iOS devices.

Most generations of iPhones and iPads are vulnerable: from iPhone 4S (A5 chip) to iPhone 8 and iPhone X (A11 chip).

# Использование джейлбрейк

## Джейлбрейк Checkra1n

- Джейлбрейк основан на эксплойте checkm8
- Устанавливается в режиме DFU
- Не требует Cydia Impactor
- **Порт USB в режиме DFU всегда доступен независимо от активации режима ограничений USB**
- Позволяет извлекать многие файлы и базы данных в режиме «холодной» загрузки (до первой разблокировки)
- **НЕ МОЖЕТ использоваться для взлома кода блокировки**
- Если код блокировки известен, позволяет извлечь образ файловой системы и расшифровать Связку ключей



# Использование джейлбрейк

## Джейлбрейк Checkra1n: проблемы

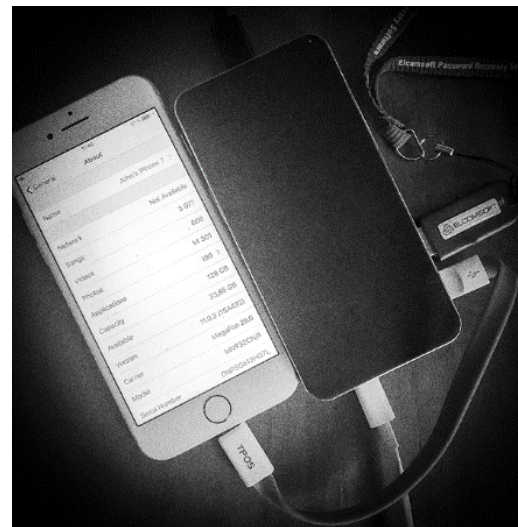
- Как и классические утилиты джейлбрейк, модифицирует системный раздел
- Многие модификации не нужны для извлечения файловой системы
- Некоторые версии переводят устройство в защитный режим USB
- Не работает с iOS ниже 12.3
- **Не работает с бета-версией iOS 13.4**



# Использование программы-агента

## Недостатки джейлбрейка

- Подавляющее большинство функций джейлбрейка не требуется для извлечения
- Ни один джейлбрейк не является инструментом криминалистического анализа
- Джейлбрейки потенциально опасны
- Остаются следы использования



# Физическое извлечение данных

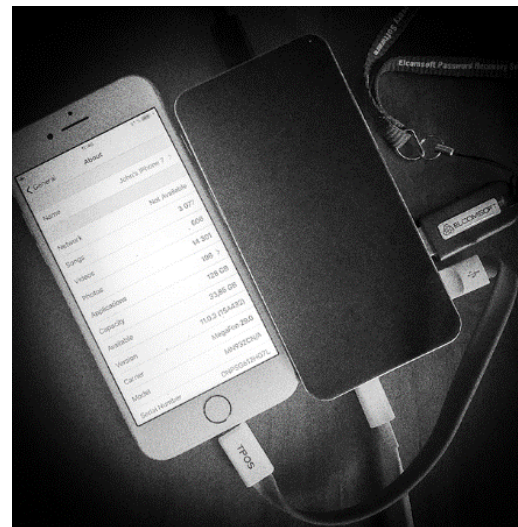
## Способ 3: с использованием программы-агента

- Использование агента собственной разработки позволяет избежать всех проблем, связанных с установкой джейлбрейка
- Максимальная надёжность работы, отсутствие рисков
- Минимальные следы использования (только записи в системных журналах)
- Работоспособность устройства не нарушается, обновления OTA устанавливаются в штатном режиме
- Для работы требуется код блокировки устройства
- Для установки требуется учётная запись Apple ID, зарегистрированная в программе Apple для разработчиков

# Использование программы-агента

## Извлечение данных без джейлбрейка

- Программа-агент собственной разработки Элкомсофт
- Агент (файл IPA) подписывается сертификатом разработчика и устанавливается на устройство
- Агент запускается на устройстве
- Агент использует известные уязвимости для эскалации привилегий
- С компьютера эксперта подаётся команда извлечения данных
- Не используется ssh (выше скорость и надёжность)



# Использование программы-агента

## Извлечение данных без джейлбрейка

- Файловая система упаковывается в архив TAR
- Извлекается и расшифровывается Связка ключей
- Агент удаляется с устройства
- Устройство функционирует в штатном режиме
- Единственный след от использования агента – записи в системных журналах





# Использование программы-агента

## Ограничения программы-агента

- Экран устройства необходимо разблокировать
- Код блокировки должен быть известен
- Отдельные версии iOS не поддерживаются
- Не поддерживаются некоторые устройства
- Совместимость: iPhone 5s..Xr/Xs/Xs Max под управлением iOS 11-12
- За исключением **iOS 12.3, 12.3.1, 12.4.1**
- Уязвимость для iOS 12.4 не слишком надёжна
- Поддержка iOS 9/10, 12.3, 12.4.1, 13.0-13.3 в процессе реализации

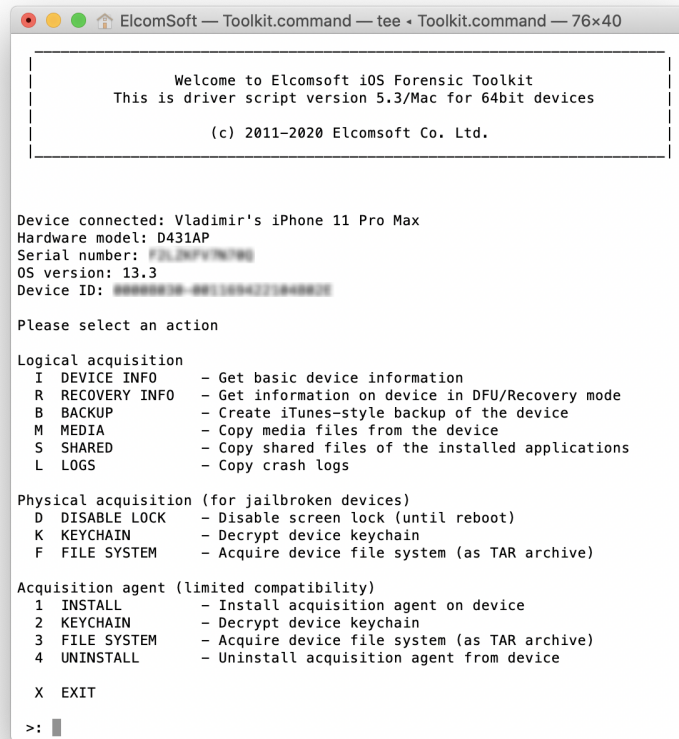
# Сравнение методов

Метод	Модели устройств	Версии iOS	Доступ к /	Следы и последствия работы	Надёжность работы
Классический JB	Все модели, для которых доступен джейлбрейк	До 12.4, 13.0 – 13.3 Кроме 12.3, 12.3.1, 12.4.1	Да	Множество следов. Возможность дальнейшей нормальной работы устройства сомнительна.	Требует тщательного следования инструкциям. Потенциально рискованный процесс.
Rootless	A7-A11 iPhone 5S – iPhone X	iOS 11-12	Нет	Небольшие следы. Работоспособность, как правило, не нарушается.	Надёжная работа, модификации только файлов в папке /var
Checkra1n	A7-A11 iPhone 5S – iPhone X	iOS 12.3 и выше	Да	См. классические JB	Достаточно надёжная работа, но были случаи выхода устройств из строя
Агент	A7-A12 iPhone 5S – iPhone Xr/Xs/Xs Max	iOS 11-12 Кроме 12.3, 12.3.1, 12.4.1	Да	Минимум следов (только записи в журналах). Работоспособность полностью сохраняется.	Высокая надёжность. Не модифицирует файлы, не перемонтирует файловую систему.

# Использование программы-агента

## До начала работы

- Убедитесь, что ваша учётная запись Apple ID зарегистрирована в программе Apple для разработчиков
- В учётных записях, участвующих в программе Apple для разработчиков, всегда активирована двухфакторная аутентификация
- Создайте уникальный пароль приложения на сайте [appleid.apple.com](https://appleid.apple.com)



```
ElcomSoft — Toolkit.command — tee - Toolkit.command — 76x40

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.3/Mac for 64bit devices

(c) 2011-2020 Elcomsoft Co. Ltd.

Device connected: Vladimir's iPhone 11 Pro Max
Hardware model: D431AP
Serial number: F1L20P7N7M
OS version: 13.3
Device ID: 00000000-00000000-00000000-00000000

Please select an action

Logical acquisition
I DEVICE INFO - Get basic device information
R RECOVERY INFO - Get information on device in DFU/Recovery mode
B BACKUP - Create iTunes-style backup of the device
M MEDIA - Copy media files from the device
S SHARED - Copy shared files of the installed applications
L LOGS - Copy crash logs

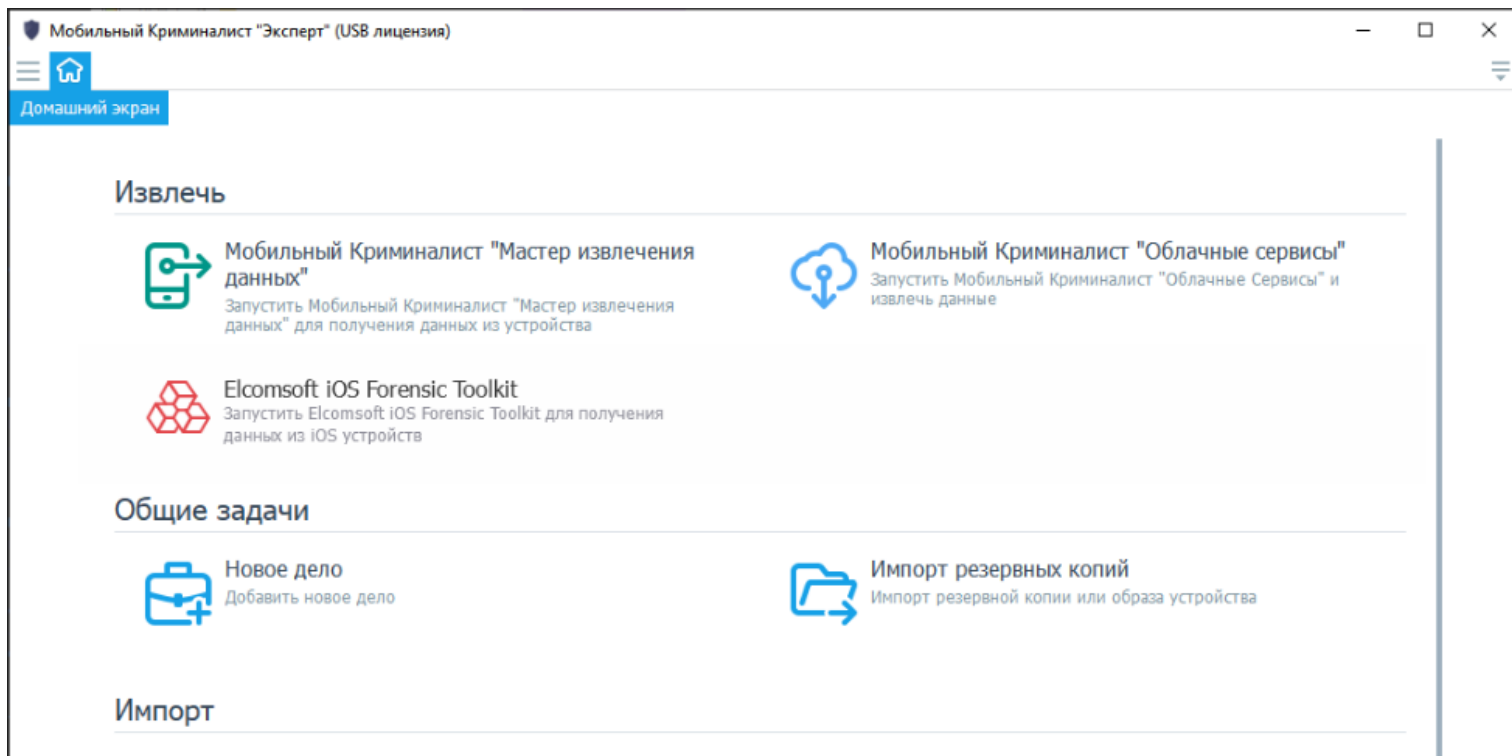
Physical acquisition (for jailbroken devices)
D DISABLE LOCK - Disable screen lock (until reboot)
K KEYCHAIN - Decrypt device keychain
F FILE SYSTEM - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
1 INSTALL - Install acquisition agent on device
2 KEYCHAIN - Decrypt device keychain
3 FILE SYSTEM - Acquire device file system (as TAR archive)
4 UNINSTALL - Uninstall acquisition agent from device

X EXIT

>: █
```

# Интеграция с МК: запуск



# Использование программы-агента

## Работа с агентом

- Подключите iPhone к компьютеру
- Разблокируйте экран и подтвердите запрос на установление связи с компьютером
- **Команда 1:** установка агента
- Введите уникальный пароль приложения, созданный на предыдущем шаге
- Агент будет установлен на устройстве

```
ElcomSoft — Toolkit.command — tee - Toolkit.command — 76x40

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.3/Mac for 64bit devices

(c) 2011-2020 Elcomsoft Co. Ltd.

Device connected: Vladimir's iPhone 11 Pro Max
Hardware model: D431AP
Serial number: F1L20P7N7W
OS version: 13.3
Device ID: 00000000-00000000-00000000-00000000

Please select an action

Logical acquisition
I DEVICE INFO - Get basic device information
R RECOVERY INFO - Get information on device in DFU/Recovery mode
B BACKUP - Create iTunes-style backup of the device
M MEDIA - Copy media files from the device
S SHARED - Copy shared files of the installed applications
L LOGS - Copy crash logs

Physical acquisition (for jailbroken devices)
D DISABLE LOCK - Disable screen lock (until reboot)
K KEYCHAIN - Decrypt device keychain
F FILE SYSTEM - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
1 INSTALL - Install acquisition agent on device
2 KEYCHAIN - Decrypt device keychain
3 FILE SYSTEM - Acquire device file system (as TAR archive)
4 UNINSTALL - Uninstall acquisition agent from device

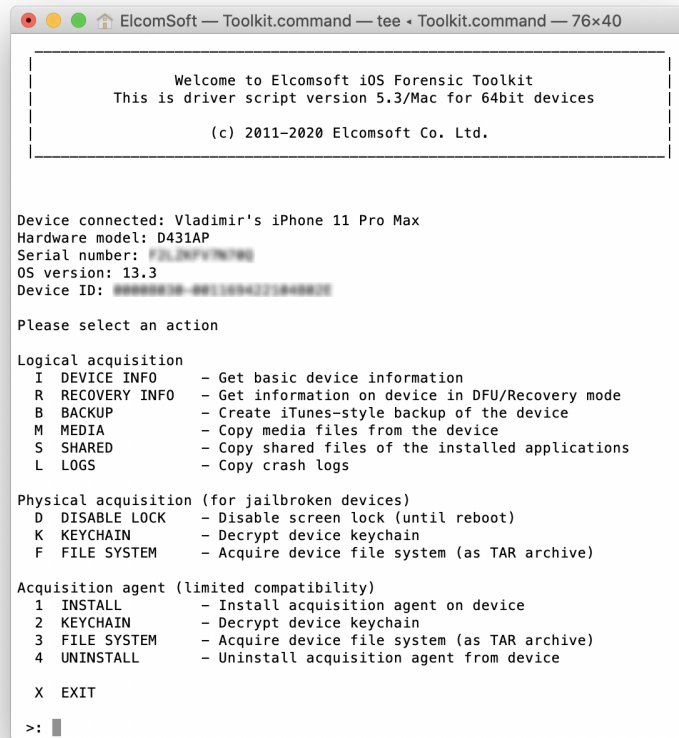
X EXIT

>: █
```

# Использование программы-агента

## Работа с агентом

- Запустите приложение-агент на iPhone
- Приложение должно оставаться активным в процессе работы



```
ElcomSoft — Toolkit.command — tee - Toolkit.command — 76x40

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.3/Mac for 64bit devices

(c) 2011-2020 Elcomsoft Co. Ltd.

Device connected: Vladimir's iPhone 11 Pro Max
Hardware model: D431AP
Serial number: F1L20P7N7W
OS version: 13.3
Device ID: 00000000-00000000-00000000-00000000

Please select an action

Logical acquisition
I DEVICE INFO - Get basic device information
R RECOVERY INFO - Get information on device in DFU/Recovery mode
B BACKUP - Create iTunes-style backup of the device
M MEDIA - Copy media files from the device
S SHARED - Copy shared files of the installed applications
L LOGS - Copy crash logs

Physical acquisition (for jailbroken devices)
D DISABLE LOCK - Disable screen lock (until reboot)
K KEYCHAIN - Decrypt device keychain
F FILE SYSTEM - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
1 INSTALL - Install acquisition agent on device
2 KEYCHAIN - Decrypt device keychain
3 FILE SYSTEM - Acquire device file system (as TAR archive)
4 UNINSTALL - Uninstall acquisition agent from device

X EXIT

>: █
```

# Использование программы-агента

## Работа с агентом

- **Команда 2:** извлечение и расшифровка Связки ключей

```
ElcomSoft — Toolkit.command — tee < Toolkit.command — 80x8
Created log file with name: keychaindumper_18.02.2020_15-27-29.log
Overall dumped 4932 items of class 'genp'
Overall dumped 1091 items of class 'inet'
Overall dumped 41 items of class 'cert'
Overall dumped 405 items of class 'keys'
Overall dumped 32 items of class 'idnt'

Cleaning up...
```

```
ElcomSoft — Toolkit.command — tee - Toolkit.command — 76x40

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.3/Mac for 64bit devices

(c) 2011-2020 Elcomsoft Co. Ltd.

Device connected: Vladimir's iPhone 11 Pro Max
Hardware model: D431AP
Serial number: F1L20P7N7M
OS version: 13.3
Device ID: 00000000-00000000-00000000-00000000

Please select an action

Local acquisition
DEVICE INFO - Get basic device information
RECOVERY INFO - Get information on device in DFU/Recovery mode
BACKUP - Create iTunes-style backup of the device
MEDIA - Copy media files from the device
SHARED - Copy shared files of the installed applications
LOGS - Copy crash logs

Local acquisition (for jailbroken devices)
DISABLE LOCK - Disable screen lock (until reboot)
KEYCHAIN - Decrypt device keychain
FILE SYSTEM - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
1 INSTALL - Install acquisition agent on device
2 KEYCHAIN - Decrypt device keychain
3 FILE SYSTEM - Acquire device file system (as TAR archive)
4 UNINSTALL - Uninstall acquisition agent from device

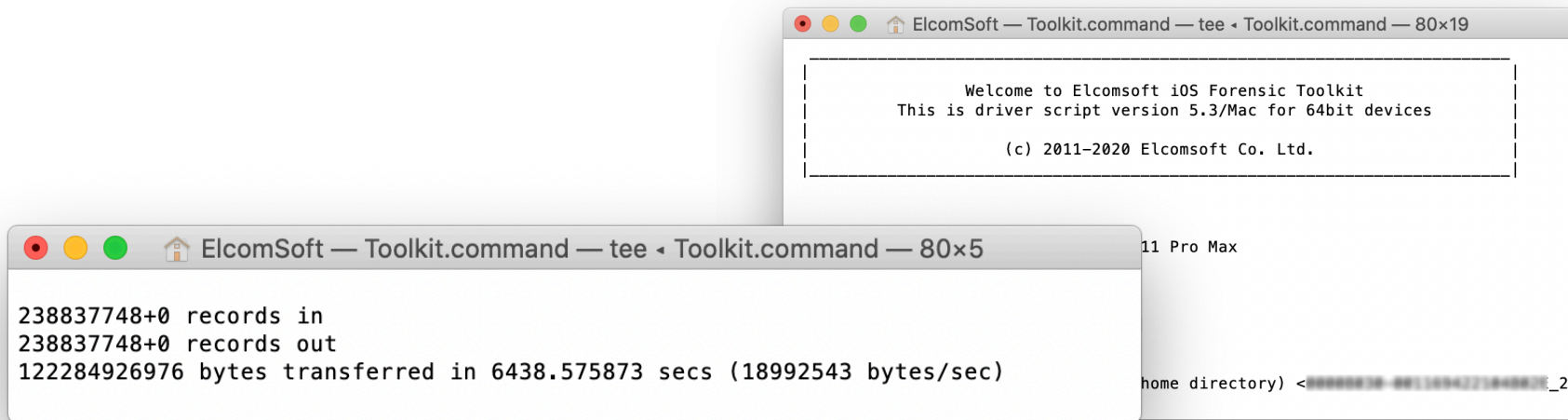
X EXIT

>: █
```

# Использование программы-агента

## Работа с агентом

- **Команда 3:** извлечение образа файловой системы



```
ElcomSoft — Toolkit.command — tee < Toolkit.command — 80x19
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.3/Mac for 64bit devices

(c) 2011-2020 Elcomsoft Co. Ltd.

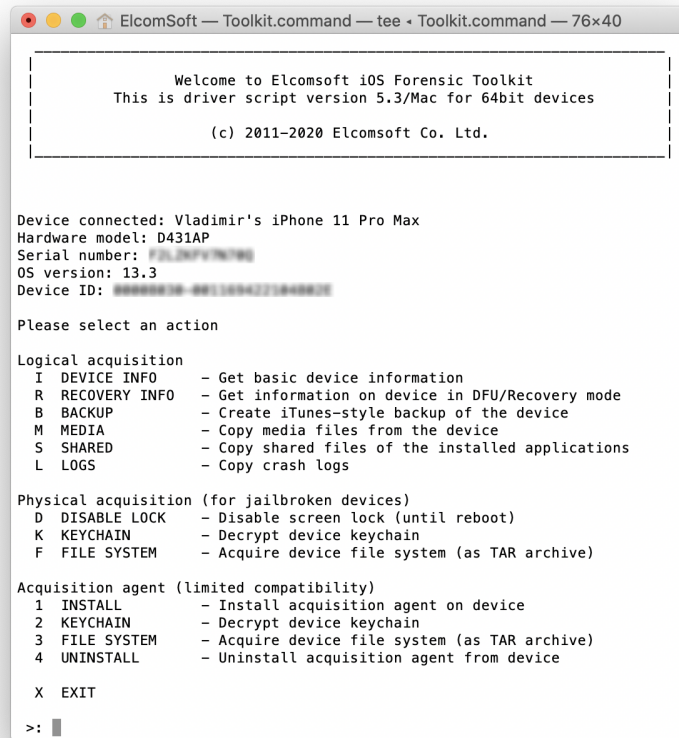
ElcomSoft — Toolkit.command — tee < Toolkit.command — 80x5
238837748+0 records in
238837748+0 records out
122284926976 bytes transferred in 6438.575873 secs (18992543 bytes/sec)
```



# Использование программы-агента

## Работа с агентом

- Команда 4: удаление агента с устройства



```
ElcomSoft — Toolkit.command — tee - Toolkit.command — 76x40

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.3/Mac for 64bit devices

(c) 2011-2020 Elcomsoft Co. Ltd.

Device connected: Vladimir's iPhone 11 Pro Max
Hardware model: D431AP
Serial number: F1L20PYN7M9
OS version: 13.3
Device ID: 88888888-8811884271888888

Please select an action

Logical acquisition
I DEVICE INFO - Get basic device information
R RECOVERY INFO - Get information on device in DFU/Recovery mode
B BACKUP - Create iTunes-style backup of the device
M MEDIA - Copy media files from the device
S SHARED - Copy shared files of the installed applications
L LOGS - Copy crash logs

Physical acquisition (for jailbroken devices)
D DISABLE LOCK - Disable screen lock (until reboot)
K KEYCHAIN - Decrypt device keychain
F FILE SYSTEM - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
1 INSTALL - Install acquisition agent on device
2 KEYCHAIN - Decrypt device keychain
3 FILE SYSTEM - Acquire device file system (as TAR archive)
4 UNINSTALL - Uninstall acquisition agent from device

X EXIT

>: █
```

# Интеграция с МК: загрузка данных

Мобильный Криминалист "Эксперт" (USB лицензия)

Домашний экран

### Извлечь

- Мобильный Криминалист "Мастер извлечения данных"**  
Запустить Мобильный Криминалист "Мастер извлечения данных" для получения данных из устройства
- Мобильный Криминалист "Облачные сервисы"**  
Запустить Мобильный Криминалист "Облачные Сервисы" и извлечь данные
- Elcomsoft iOS Forensic Toolkit**  
Запустить Elcomsoft iOS Forensic Toolkit для получения данных из iOS устройств

### Общие задачи

- Новое дело**  
Добавить новое дело
- Импорт резервных копий**  
Импорт резервной копии или образа устройства

### Импорт

- Apple**  
Резервная копия iTunes | Резервная копия tarball/zip
- Android**  
Физический образ Android | Файловая система tarball/zip | Резервная копия Android | Резервная копия CNWM | Резервная копия TWRP | Резервная копия Xiaomi | Резервная копия Huawei
- Оxygen**  
Резервная копия OCB | Резервная копия Oxygen | Резервная копия ПК | Образ Oxygen UICC | Извлечение Oxygen Agent
- Дроны**  
Журналы дронов DJI | Журналы приложения DJI GO | Резервная копия DJI Assistant | Физический образ дрона DJI | Логи дрона Parrot | Центр уведомлений
- Сторонние ИИ**  
Резервная копия | Резервная копия | Импорт файловой системы Apple tarball/zip | ... \bd4d4a22144463c9400844235fc31e8d319e83b8\_20200225\_164943Z... | Извлечение файлов... | Отмена
- KaiOS**  
Физический образ | Файловая система tarball/zip

Версия: 1.3.0.63

1 новое уведомление

# МК: информация об устройстве

Мобильный Криминалист "Эксперт" (USB лицензия)

Дела (24)

- tar + itunes
- iTunes backup (bd4d4a22144463c94008442...)
- Apple tarball (bd4d4a22144463c94008442...)**

Apple Заметки: 88  
WebKit Data: 18  
Аккаунты и пароли: 1 202  
Артефакты ОС: 9 841  
Беспроводные соединения: 2 499  
Звонки: 224  
Календарь: 455  
Контакты: 1 966  
Отчёты: 1  
Сообщения: 3 278  
Файлы: 295 218  
Важное: 17  
Граф связей: 1  
Лента событий: 91 073  
Поиск: 924  
Приложения: 42- Airbnb: 1
- Amazon shopping: 24
- Apple Maps: 2
- Apple Wallet: 204
- BlaBlaCar: 4
- Booking.com: 69
- Dropbox: 1
- Endomondo: 3
- Facebook: 1
- Facebook Messenger: 23
- Google Chrome: 81
- Google Home: 25
- Google Keep: 101
- Google Mail: 34
- Google photos: 1 397
- Google Translate: 33
- Health: 73 306
- и др.

Apple tarball (bd4d4a22144463c9400844235fc31e8d319e83b8\_20200225\_164943Z.tar)

Часовой пояс: (UTC+00:00) UTC  
ОС: iOS 12.4.3 (16G130)  
Номер инцидента: [Добавить номер инцидента](#)  
Номер вещдока: [Добавить номер вещдока](#)

Статистика | Извлечение | Владелец | Устройство | Заметка

### Топ 10 контактов

Номер	Процент	Имя
1609	57,14%	Yuriy Votyakov
427	15,16%	First name Last name
194	6,89%	+79264102930
168	5,97%	Andrey Oxygen
84	2,98%	Jesse Aaron
84	2,98%	Виктaлий Петров
82	2,91%	nxsms
61	2,17%	Jay Parkers
60	2,13%	2909288299
47	1,67%	beeline

[Перейти в Контакты](#)

### Топ 10 групп

Номер	Процент	Имя
44	18,64%	RT на русском
42	17,80%	ELLE мода
41	17,37%	ELLE красота
37	15,68%	Group chat theme
22	9,32%	e58cba2bb8abb05859ef229...
10	4,24%	Pet group
10	4,24%	Jay Parkers, Jesse Aaron
10	4,24%	Back To The Winter
10	4,24%	Jay_Parkers, BobPlant87, A...
10	4,24%	Jay_Parkers, BobPlant87, A...

[Перейти в Контакты](#)

### Общие разделы 12

Приложения: 42	Apple Заметки: 88	WebKit Data: 18	Аккаунты и пароли: 1 202	Артефакты ОС: 9 841
Беспроводные соедин...: 2 499	Звонки: 224	Календарь: 455	Контакты: 1 966	Отчёты
Сообщения: 3 278	Файлы: 295 218			

Найти текст...

Версия: 1.3.0.63 Всего извлечений: 94

# МК: связка ключей

The screenshot displays the 'Мобильный Криминалист Эксперт' (Mobile Criminalist Expert) software interface. The main window shows a list of cryptographic keys under the 'Keychain (1.123)' section. The interface includes a sidebar with filters, a main list of keys with columns for type, count, and details, and a right-hand pane showing details for the selected key.

**Filters:**

- Тип: 4
- Certificates: 21
- Keys: 103
- Интернет: 272
- Общее: 727

**Keychain (1.123) - Учетные данные (79)**

Иконка	Тип	Счетчик	Имя
🔑	Данные	397	IF07214373FB6674A48C0668F0581819185563AC893C79EBA0E389252FAF
🔑	Данные	3D	2288EE189D07F750B0871CAF2149F3E280B5197FD2A352050A9C14FDD81177
🔑	Данные	CB	7E29CAA6E08B7DBAA4180513780AEB0AB74CEAD7CB0C96A881A2871A1DB1ED
🔑	Данные	26	0FB164C6E9F8E901C52EEBC940D4D1B7AA428B860C68AE2644A85284F781A
🔑	Данные	10	392707761832244F78F3FCCE2888E36953CB716AC268305A250D58D67C4F7
🔑	Данные	99	494D4CC9AD7DA392D0B58004E5E08569A0BA60421ED2D122408403D80063F
🔑	Данные	4	3ED954037F96D68FF1CC9E9E4B47AC9DBDAF75FF0FCDFC04CDF998D3CFD6EB26
🔑	Данные	58	1EAA106A4BD89C36D70627AE244AE7E194E34C226F1F13209A05AC64D4370D
🔑	Данные	D8	7AA5C6ABE38472EBE8C5B8C78CE9A4553B475BE46FE4390DE2A39F833A0DA7
🔑	Данные	8	47894F90ECE58C9D42C2ADD0C74C873ACD781606929DA586744B70334B4C7E
🔑	Данные	5	8C8CE4B6DE517914411F48D15037CF33AB39787A68381227D51880D3DBE2B8
🔑	Данные	D	C067CD587A81CB301DAD5F689198515A6E5D29FA86624CB885243AFCE244C65
🔑	Данные	6	2A51386B2CB88C446FE0B2D8B25E9AA8EEF1A644337889553A18A1FCADAEC7
🔑	Данные	E	CA349D5444984FA6276AEFA99810B745C1F4ED72E9A8D6160C36AB1332A95E
🔑	Данные	1	E025B01588EE5E15D9FAEE1E40234C8876831337BF9F167E2DD85786ED06D59
🔑	Данные	D	684A11B3B3D0FF8CCE5387427169201DE054FA45A3D8278FA6D9911EF5E4E
🔑	Данные	7	CEB6E40D7C669A9421B8E7782178278FF1C23D766A54910CF0A0EA477C9D74F
🔑	Данные	4	E43043A059D1341C9032F2F819AED3A0CE478F2C894F11EE5F1E083796D7191
🔑	Данные	3	ADACFB09B17B6132AEF636186C5092EDC18C977DE343F96CEDED58370CC015
🔑	Данные	A	1DABAA5D91E6FED2934F9164DDC90EA69818EE338DD0F1C538A60242C7704B
🔑	Данные	CC	50F65554418835EE4AAB302BF8798EB31002900AFB3D14FB01479815871D1
🔑	Данные	7	3872193F00A7DEC8C550276CA38201F4777EF79E326E0AFA9D30694E70C8136
🔑	Данные	E	EFB730D9658FA6D51837B242ED9758E
🔑	Данные	0	97B2A25-2C38-44A1-8843-265B92AF393
🔑	Данные	3	081D50440FF598800909C58CEDEF906CECD0C6FFF583E5E989838AAD81FB1909D9E99971D...
🔑	Данные	3	082013E044FDD96E0893E23CE6672DC7C7032AE89E928D0F4452295EABE3002AF5FA09...
🔑	Данные	xdrj	6g4Uzo03g0KnicSpkVohdACHkZtpEn8QAaZxcsSNTDTAMwypkPI7F lokstg
🔑	Данные	bplist00N	Z8055544210N _ADClientDPIDRecordKey_JDPID-E3DD8E2-8BD7-4C50-B167-011... _ADClientDPIDStorageContainerKey
🔑	Данные	1	_pfo
🔑	Данные	1	_pfo
🔑	Данные	2	_pfo
🔑	Данные	1	_pfo
🔑	Данные	1	_pfo

**Details (Детали) for selected key:**

- Исходный раздел: 📁 файлы
- Исходный файл: bd4d4a22144463c9400844235f3c1e8d31...
- Учетная запись: \_ADClientDPIDStorageContainerKey
- Группа доступа: apple
- Служба: com.apple.iAdIDRecords
- Данные: bplist00N Z8055544210N \_ADClientDPIDRecordKey\_JDPID-E3DD8E2-8BD7-4C50-B167-0116... 1 }
- Атрибуты: \_ADClientDPIDStorageContainerKey
- Дата создания (UTC): 23.07.2018 08:45:05 (UTC + 0)
- Дата изменения (UTC): 23.07.2018 08:45:05 (UTC + 0)

Buttons: [🌟 Важное](#) [🔗 Добавить тег](#) [📌 Добавить заметку](#)

Bottom status bar: Найти текст... Версия: 1.3.0.63 Всего: 1.123 Отфильтровано: 1.123 Выбрано: 1

# МК: файловая система

Мобильный Криминалист "Эксперт" (USB лицензия)

Файлы - Apple tarball (bd4...)

Информация об извлечении | Экспорт | Сброс фильтров | Вид | Карты | Наборы хешей

Дерево папок | Все файлы | Изображения | Аудиофайлы | Видео | Изображения угроз | Фотоснимки | Базы данных | Документы | Найти текст...

Имя	Дата создания (UTC)	Дата изменения (UTC)	Дата доступа (UTC)	Тип
var	04.02.2020 13:51:48 (UTC+0)	04.02.2020 13:51:48 (UTC+0)	04.02.2020 12:48:08 (UTC+0)	Папка
.DocumentRevisions-V100	04.02.2020 13:48:52 (UTC+0)	04.02.2020 13:48:52 (UTC+0)	14.12.2019 13:28:00 (UTC+0)	Папка
binpack	04.02.2020 13:48:41 (UTC+0)	04.02.2020 13:48:41 (UTC+0)	20.11.2019 13:03:04 (UTC+0)	Папка
cache	04.02.2020 13:50:02 (UTC+0)	04.02.2020 13:50:02 (UTC+0)	04.02.2020 11:35:09 (UTC+0)	Папка
containers	04.02.2020 13:49:59 (UTC+0)	04.02.2020 13:49:59 (UTC+0)	03.02.2020 11:04:34 (UTC+0)	Папка
db	04.02.2020 13:48:53 (UTC+0)	04.02.2020 13:48:53 (UTC+0)	29.03.2019 18:21:24 (UTC+0)	Папка
install	04.02.2020 13:49:57 (UTC+0)	04.02.2020 13:49:57 (UTC+0)	04.02.2020 12:46:09 (UTC+0)	Папка
keybags	04.02.2020 13:51:48 (UTC+0)	04.02.2020 13:51:48 (UTC+0)	24.01.2020 17:50:13 (UTC+0)	Папка
lib	04.02.2020 13:49:59 (UTC+0)	04.02.2020 13:49:59 (UTC+0)	20.11.2019 13:03:04 (UTC+0)	Папка
log	04.02.2020 13:50:02 (UTC+0)	04.02.2020 13:50:02 (UTC+0)	04.02.2020 12:48:11 (UTC+0)	Папка
logs	04.02.2020 13:48:53 (UTC+0)	04.02.2020 13:48:53 (UTC+0)	29.01.2020 00:59:59 (UTC+0)	Папка
Managed Preferences	04.02.2020 13:51:48 (UTC+0)	04.02.2020 13:51:48 (UTC+0)	29.03.2019 18:19:26 (UTC+0)	Папка
mobile	04.02.2020 13:48:53 (UTC+0)	04.02.2020 13:48:53 (UTC+0)	20.11.2019 12:42:29 (UTC+0)	Папка
MobileAsset	04.02.2020 13:48:41 (UTC+0)	04.02.2020 13:48:41 (UTC+0)	20.11.2019 12:41:39 (UTC+0)	Папка
MobileDevice	04.02.2020 13:49:57 (UTC+0)	04.02.2020 13:49:57 (UTC+0)	29.03.2019 18:19:26 (UTC+0)	Папка
MobileSoftwareUpdate	04.02.2020 13:48:53 (UTC+0)	04.02.2020 13:48:53 (UTC+0)	04.02.2020 12:32:55 (UTC+0)	Папка
msgs	04.02.2020 13:48:53 (UTC+0)	04.02.2020 13:48:53 (UTC+0)	29.03.2019 18:19:29 (UTC+0)	Папка
networkd	04.02.2020 13:48:41 (UTC+0)	04.02.2020 13:48:41 (UTC+0)	29.03.2019 18:21:48 (UTC+0)	Папка
preferences	04.02.2020 13:48:41 (UTC+0)	04.02.2020 13:48:41 (UTC+0)	04.02.2020 12:38:39 (UTC+0)	Папка
root	04.02.2020 13:49:57 (UTC+0)	04.02.2020 13:49:57 (UTC+0)	04.02.2020 12:40:36 (UTC+0)	Папка
run	04.02.2020 13:51:48 (UTC+0)	04.02.2020 13:51:48 (UTC+0)	04.02.2020 11:35:10 (UTC+0)	Папка
tmp	04.02.2020 13:51:48 (UTC+0)	04.02.2020 13:51:48 (UTC+0)	04.02.2020 13:17:13 (UTC+0)	Папка
vm	04.02.2020 13:48:52 (UTC+0)	04.02.2020 13:48:52 (UTC+0)	04.02.2020 12:33:34 (UTC+0)	Папка
wireless	04.02.2020 13:49:57 (UTC+0)	04.02.2020 13:49:57 (UTC+0)	29.03.2019 18:21:39 (UTC+0)	Папка
checkra.in.dmg	04.02.2020 13:48:41 (UTC+0)	04.02.2020 13:48:41 (UTC+0)	18.12.2019 16:04:09 (UTC+0)	Архив
dropbear_rsa_host_key	04.02.2020 13:48:52 (UTC+0)	04.02.2020 13:48:52 (UTC+0)	20.11.2019 13:01:52 (UTC+0)	Файл

Имя var  
Дата создания (UTC) 04.02.2020 13:48:41 (UTC+0)  
Дата изменения 04.02.2020 13:48:41 (UTC+0) (UTC)  
Дата доступа (UTC) 18.12.2019 16:04:09 (UTC+0)  
Тип Папка  
Категория Папка  
Полный путь /private/var

Дубликаты

Нет дубликатов файлов

Версия: 1.3.0.63 Всего: 24 папок, 2 файлов (10,6 МБ) Отфильтровано: 24 папок, 2 файлов (10,6 МБ) Выбрано: 1 папка

# Учётная запись разработчика

- А зачем она вообще нужна?
- Подойдёт ли обычная учётную запись?
- Как зарегистрироваться, сколько стоит?
  - <https://developer.apple.com/programs/enroll/>
- Какие ограничения?

## ✓ Enrolling as an Individual

If you are an individual or sole proprietor/single person business, get started by signing in with your Apple ID with [two-factor authentication](#) turned on. You'll need to provide basic personal information, including your legal name and address.

## ✓ Enrolling as an Organization

If you're enrolling your organization, you'll need an Apple ID with [two-factor authentication](#) turned on, as well as the following to get started:

### A D-U-N-S® Number

Your organization must have a D-U-N-S Number so that we can verify your organization's identity and legal entity status. These unique nine-digit numbers are assigned by Dun & Bradstreet and are widely used as standard business identifiers. You can check to see if your organization already has a D-U-N-S Number and request one if necessary. They are free in most jurisdictions. [Learn more >](#)

### Legal Entity Status

Your organization must be a legal entity so that it can enter into contracts with Apple. We do not accept DBAs, fictitious businesses, trade names, or branches.



# Методы извлечения данных из устройств под управлением iOS

## Вопросы?

(c) ElcomSoft 2020  
Vladimir Katalov, ElcomSoft Co. Ltd.

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

Facebook: ElcomSoft  
Twitter: @elcomsoft