



Elcomsoft iOS Forensic Toolkit

Версия 6.0

Elcomsoft iOS Forensic Toolkit помогает экспертам-криминалистам осуществлять физическое и логическое извлечение данных из устройств под управлением Apple iOS путем создания и дешифрования образа файловой системы устройства и извлечения секретов устройства (паролей, ключей шифрования и защищённых данных).

Краткий обзор

В обновлении iOS Forensic Toolkit 6.0 появилась возможность извлекать данные без джейлбрейка из актуального поколения устройств iPhone, работающих на самых свежих версиях iOS. В обновлении EIFT 6.0 расширен список версий iOS, для которых доступно извлечение образа файловой системы без джейлбрейка. Извлечение посредством агента-экстрактора теперь доступно для большинства устройств iPhone и iPad под управлением последних версий iOS от 13.3.1 до iOS 13.4.1 включительно.

Важные изменения

Поддерживаемые версии iOS

В новой версии Elcomsoft iOS Forensic Toolkit 6.0 расширен список версий iOS, для которых доступно извлечение образа файловой системы без джейлбрейка, посредством агента-экстрактора. Снятие данных стало доступно для устройств, работающих под управлением последних версий iOS 13, включая сборки iOS 13.3.1, 13.4 и 13.4.1.



Поддерживаемые модели устройств



Извлечение посредством агента-экстрактора не требует установки джейлбрейка и работает на всех совместимых устройствах вплоть до актуальных моделей iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max и SE 2020, а также iPad, основанные на аналогичных процессорах. Джейлбрейк checkra1n недоступен для устройств поколений A12-A13, что делает агент-экстрактор единственным доступным способом извлечения данных.

Безопасное извлечение данных

Метод низкоуровневого извлечения данных посредством агента-экстрактора позволяет экспертам быстро и максимально безопасно извлечь полный образ файловой системы, а для версий iOS до 13.3 включительно — и расшифровать Связку ключей. Данный метод извлечения не модифицирует системный раздел и пользовательские данные, не влияет на работоспособность устройства и не оставляет следов работы (за исключением нескольких записей в системном журнале).





Учётная запись разработчика

Агент-экстрактор устанавливается на устройство в режиме офлайн, без связи с интернетом, при условии использования учётной записи Apple ID, зарегистрированной в программе Apple для разработчиков. Подробнее об учётных записях и регистрации в программе Apple для разработчиков – в статье «Мобильная криминалистика: учётные записи Apple для разработчиков».

Список изменений в версии 6.0

- Добавлена поддержка iOS 13.3.1 до iOS 13.4.1 для извлечения файловой системы из iPhone и iPad посредством агента-экстрактора (модели iPhone 6s – iPhone 11, 11 Pro, 11 Pro Max и SE).

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

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 6.0/Mac for 64bit devices
(c) 2011-2020 Elcomsoft Co. Ltd.

Device connected: Vladimir's iPhone SE 2020
Hardware model: D79AP
Serial number: 0000000000000000
OS version: 13.4.1
Device ID: 0000000000000000

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

>: |
```

```
ElcomSoft - Toolkit.command - tee - Toolkit.command - 76x34

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 6.0/Mac for 64bit devices
(c) 2011-2020 Elcomsoft Co. Ltd.

Device with udid 0000000000000000 has been detected.
Device Name: Vladimir's iPhone SE 2020
Device Model: iPhone12,8
OS Version: iPhone OS 13.4.1
Serial Number: 0000000000000000
Build Version: 17E8258

Device will be enrolled in the Apple Developer Program.
Install: CreatingStagingDirectory (5%)
Install: ExtractingPackage (15%)
Install: InspectingPackage (20%)
Install: TakingInstallLock (20%)
Install: PreflightingApplication (30%)
Install: InstallingEmbeddedProfile (30%)
Install: VerifyingApplication (40%)
Install: CreatingContainer (50%)
Install: InstallingApplication (60%)
Install: PostflightingApplication (70%)
Install: SandboxingApplication (80%)
Install: GeneratingApplicationMap (90%)
Process has been completed.
Please launch the Acquisition agent on the iOS device now and keep it running in the foreground.
Press 'Enter' to continue
```

Дальнейшие действия

- Всем активным пользователям Elcomsoft iOS Forensic Toolkit предлагается загрузить новую версию 6.0 с сайта компании. Для этого необходимо ввести действующий регистрационный ключ в онлайн-форме <https://www.elcomsoft.com/key.html>.
- Пользователи, у которых истёк срок действия лицензии Elcomsoft iOS Forensic Toolkit, могут продлить свою лицензию по соответствующей цене, которую можно узнать на сайте, введя регистрационный ключ в онлайн-форме (<https://www.elcomsoft.com/key.html>).

Свяжитесь с нами по электронной почте sales@elcomsoft.com для получения более подробной информации по обновлению или продлению лицензии.



ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

www.elcomsoft.ru
blog.elcomsoft.ru
sales@elcomsoft.com

