



Elcomsoft iOS Forensic Toolkit

Версия 6.40

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 Elcomsoft iOS Forensic Toolkit 6.40 появилась возможность разблокировать смартфоны iPhone 5 и iPhone 5c с неизвестным кодом блокировки. Пользователи инструментария смогут быстро подобрать код блокировки экрана и разблокировать экран устройства. Наша реализация не требует разборки устройства или дополнительного аппаратного обеспечения. Для проведения атаки требуется компьютер под управлением macOS.

Важные изменения

Разблокировка iPhone 5 и iPhone 5c с неизвестным паролем

В экосистеме Apple на коде блокировки экрана основан ключ шифрования, посредством которого в хранилище устройства зашифрована подавляющая часть пользовательских данных. Защита на устройствах iPhone 5 и 5c реализована на программном уровне, что позволило нашим разработчикам её обойти программным же способом.



Скорость перебора паролей достигает максимально возможной цифры в 13.6 паролей в секунду (аппаратный предел платформы), что позволяет перебрать все возможные комбинации паролей из 4 цифр всего за 12 минут. Пароли, состоящие из 6 цифр, перебираются в течение 21 часа в полном объёме, однако реальное время разблокировки может быть значительно сокращено, благодаря предварительной атаке по самым распространённым паролям.

Список изменений в версии 6.40

- Экспериментальная поддержка восстановления кода блокировки экрана iPhone 5/5c (только в версии для macOS)
- Улучшена установка агента извлечения при использовании Apple ID, подключённого к нескольким учётным записям разработчика
- Улучшения производительности и исправления ошибок

```
ElcomSoft — Toolkit.command — tee - Toolkit.command — 76x43

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 6.40/Mac for 64bit devices

(c) 2011-2020 Elcomsoft Co. Ltd.

Device connected: Daddy's iPhone
Hardware model: N49AP
OS version: 10.3.3
Device ID: 8f8c0c04178595029ae176f077e0aa48586aa1c6

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 FILE SYSTEM (USER) - Acquire user files only (as TAR archive)
5 UNINSTALL - Uninstall acquisition agent from device

Experimental features
P BREAK PASSCODE - iPhone 5/5C only

X EXIT

>:
```

```
ElcomSoft — Toolkit.command — tee - Toolkit.command — 76x46

Please select an action
1 Put device in DFU mode
2 Exploit device
3 Break 4-digit passwords
4 Break 6-digit passwords
5 Reboot device
0 Back

>: 2

Detecting device type...
Connected to iPhone5,4, model n49ap, cpid 0x8950, bdid 0x0e
DFU device information
CPID:0x8950 CPRV:0x20 BDID:0x0E ECID:0x000001071A0DCD8B CPM:0x03 SCEP:0x10
IBFL:0x00
SRTG:[iBoot-1145.3]
Exploiting with checkm8
Device is now in pwned DFU mode!

Loading iBSS.n48ap on device...
Decrypted Img3 image
Uploading soft DFU

Loading iBEC.n48ap on device...
[=====] 100.0%

Loading DeviceTree.n48ap on device...
[=====] 100.0%

Loading ramdisk on device...
[=====] 100.0%

Loading DeviceTree.n48ap on device...
[=====] 100.0%

Loading kernelcache.n48ap on device...
[=====] 100.0%

Waiting for device to boot...

Mounting user partition...

Press 'Enter' to continue
```

Как обновить программу

1. Всем активным пользователям Elcomsoft iOS Forensic Toolkit предлагается загрузить новую версию 6.40 с сайта компании. Для этого необходимо ввести действующий регистрационный ключ в онлайн-форме <https://www.elcomsoft.com/key.html>.
2. 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

