Six Ways to Decrypt iPhone Passwords from the Keychain

By Vladimir Katalov

Published: 2018-12-18 · Archived: 2026-04-05 18:42:16 UTC

In Apple's world, the keychain is one of the core and most secure components of macOS, iOS and its derivatives such as watchOS and tvOS. The keychain is intended to keep the user's most valuable secrets securely protected. This includes protection for authentication tokens, encryption keys, credit card data and a lot more. End users are mostly familiar with one particular feature of the keychain: the ability to store all kinds of passwords. This includes passwords to Web sites (Safari and third-party Web browsers), mail accounts, social networks, instant messengers, bank accounts and just about everything else. Some records (such as Wi-Fi passwords) are "system-wide", while other records can be only accessed by their respective apps. iOS 12 further develops password auto-fill, allowing users to utilize passwords they stored in Safari in many third-party apps.

If one can access information saved in the keychain, one can then gain the keys to everything managed by the device owner from their online accounts to banking data, online shopping, social life and much more.

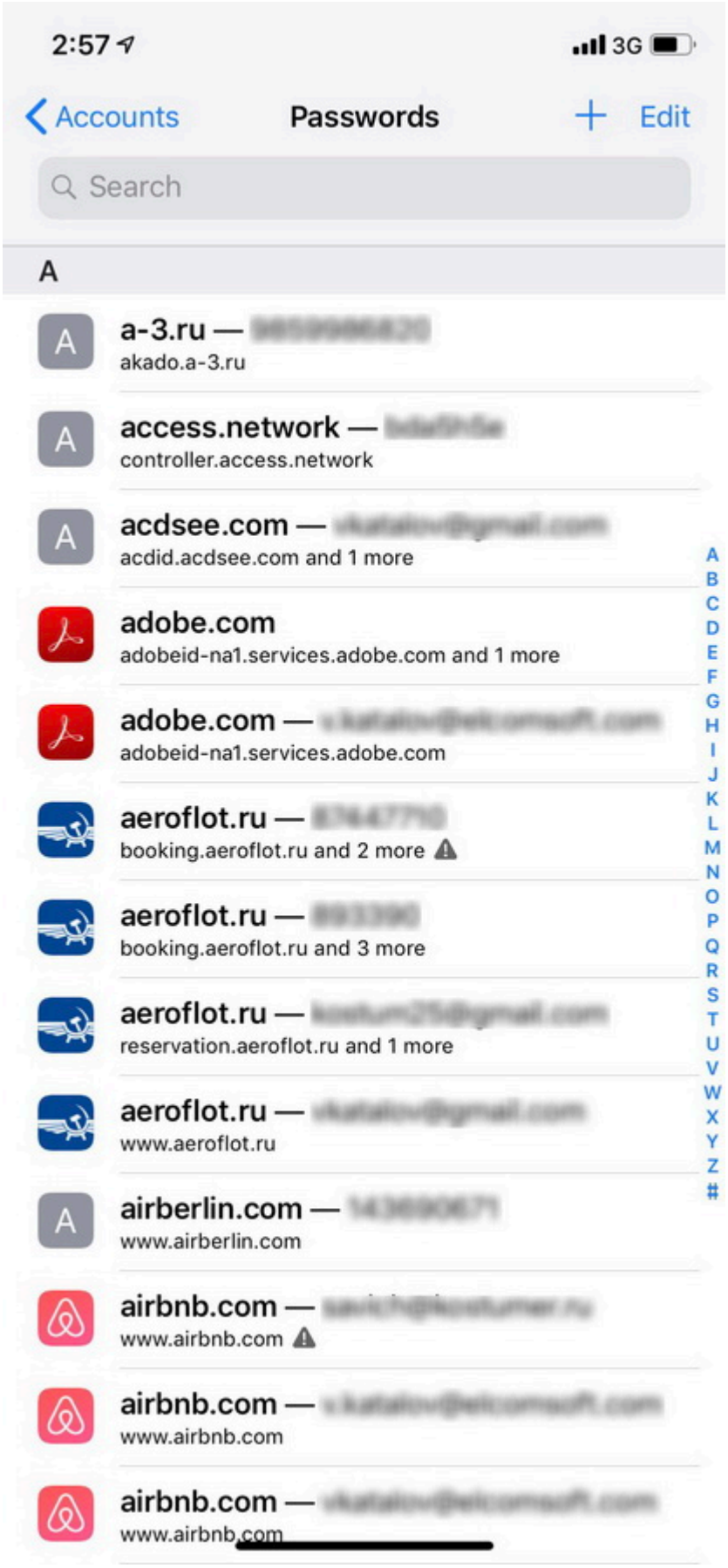
Apple offers comprehensive documentation for developers on keychain services, and provides additional information in iOS Security Guide.

In this article we assembled information about all existing methods for accessing and decrypting the keychain secrets.

Method 1: Interactive (iOS Settings)

Have you ever tried opening [Settings] | [Passwords & Accounts] | [Website & App Passwords]? In order to access that screen, you will have to enter your screen lock passcode (or authenticate via the Touch ID or Face ID) even if the device is unlocked. On this screen, you'll be able to interactively browse through the list of your stored passwords. The "interactive" part stands for the lack of proper exporting. In order to export a particular password, you'll have to copy it to the clipboard or send it via AirDrop. There is no way to export more than one password at once.

When browsing the passwords in iOS settings, you will quickly realize something is missing. Do you have Facebook or Twitter app installed on your iPhone? If you do, can you see your Facebook or Twitter password in the Settings? Unless you have used either password in Safari (e.g. for the purpose of single sign-on), you won't see those passwords in iOS settings. This is simply because those types of passwords are not saved by their respective apps. The apps are using authentication tokens instead.



Credit card data is saved at a different location:

[Settings] | [Safari] | [AutoFill] | [Saved Credit Cards]

For some reason, iOS does not allow viewing or editing Wi-Fi passwords. You can do that in macOS, though.

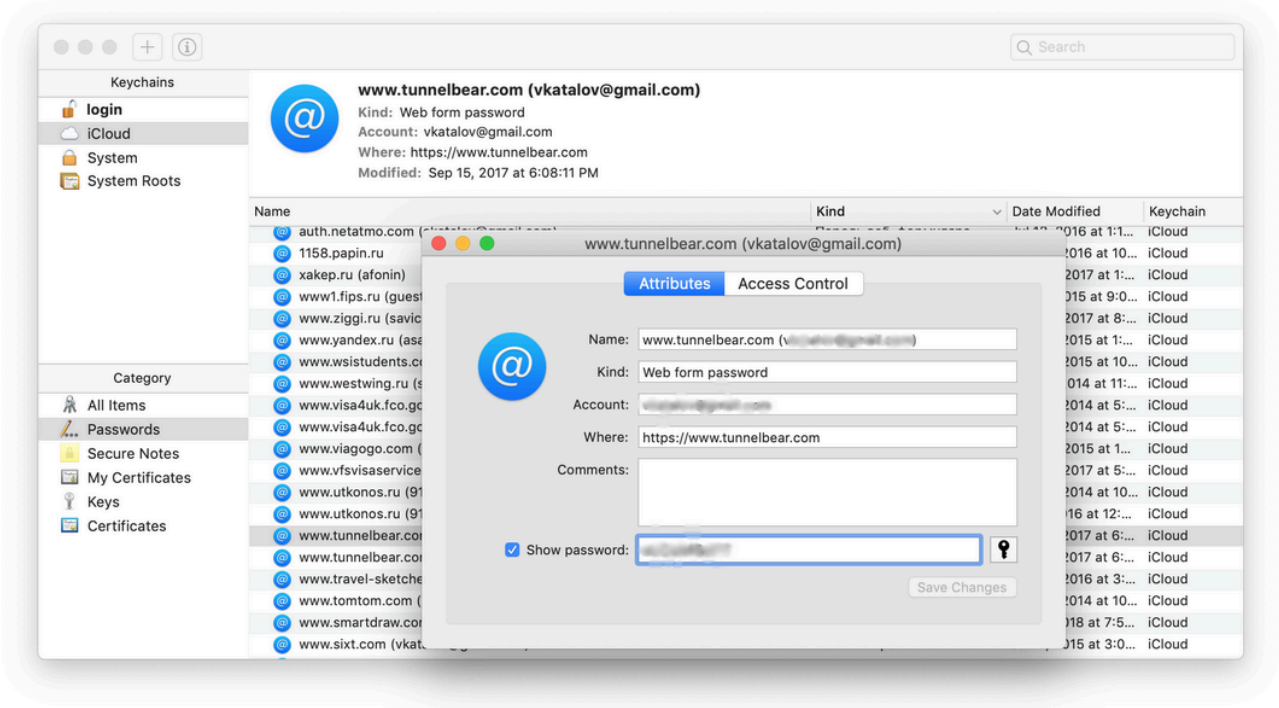
Complexity: easy

Pros: no need for additional software

Cons: need access to physical device (unlocked); one-by-one copy-paste (no export of all records at once); Web site passwords and credit cards only

Method 2: macOS Keychain Tool

If you have a Mac in addition to an iPhone and your passwords are synced through iCloud (more on that later), you can use the built-in Keychain Access tool on the Mac. This tool also displays one item at a time, and you will have to enter the keychain password every time. Thankfully, on newer Macbooks you can use Touch ID instead of the password.



Complexity: easy

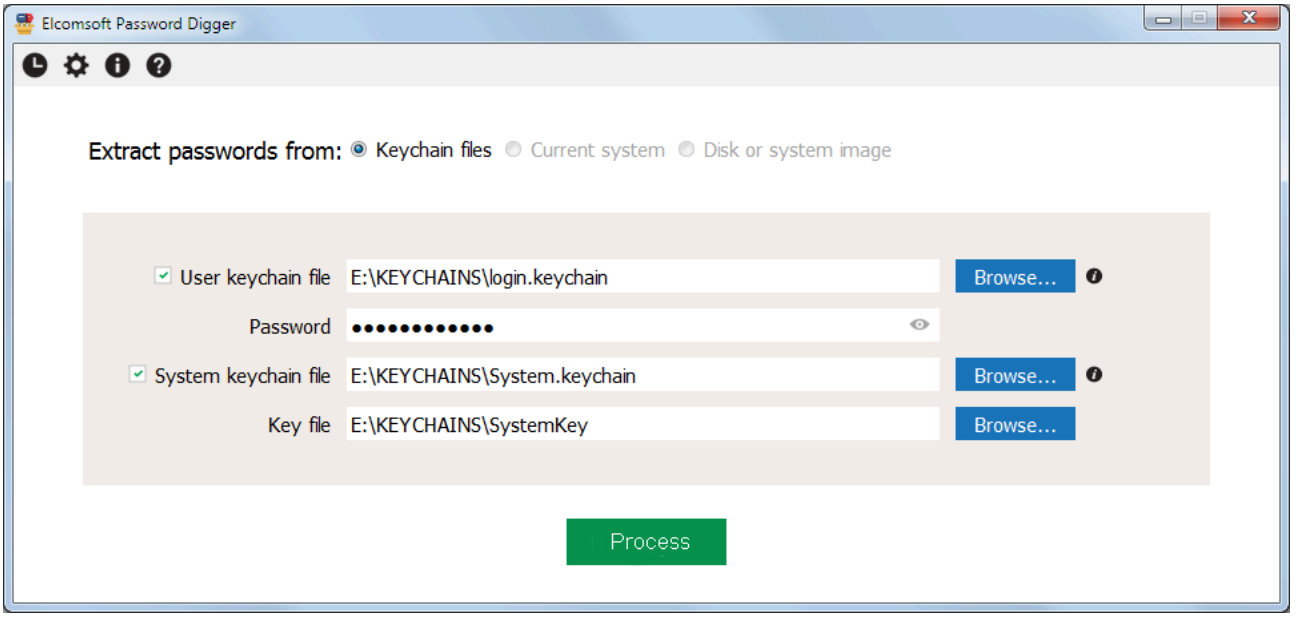
Pros: no need for additional software; all keychain data is available

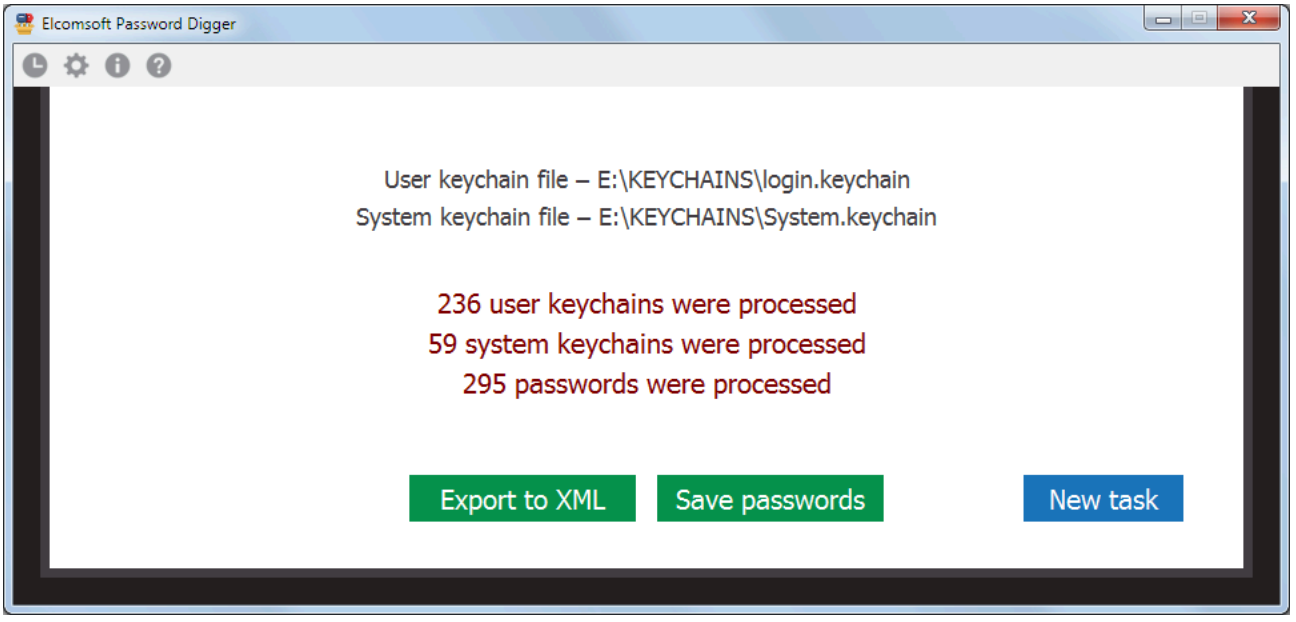
Cons: need access to iCloud-synced Mac; one-by-one copy-paste (entering keychain password every time)

Notes: keychain password is also needed

Method 3: Decrypting the Full macOS Keychain

Instead of manually browsing through the records and exporting passwords one by one, you can use Elcomsoft Phone Digger to extract all of them. You will need to copy the user's and system keychain files from the Mac being analyzed. In order to decrypt the user keychain, you will require the user's password. The system keychain is decrypted with a key file accessible with admin privileges.





Complexity: medium

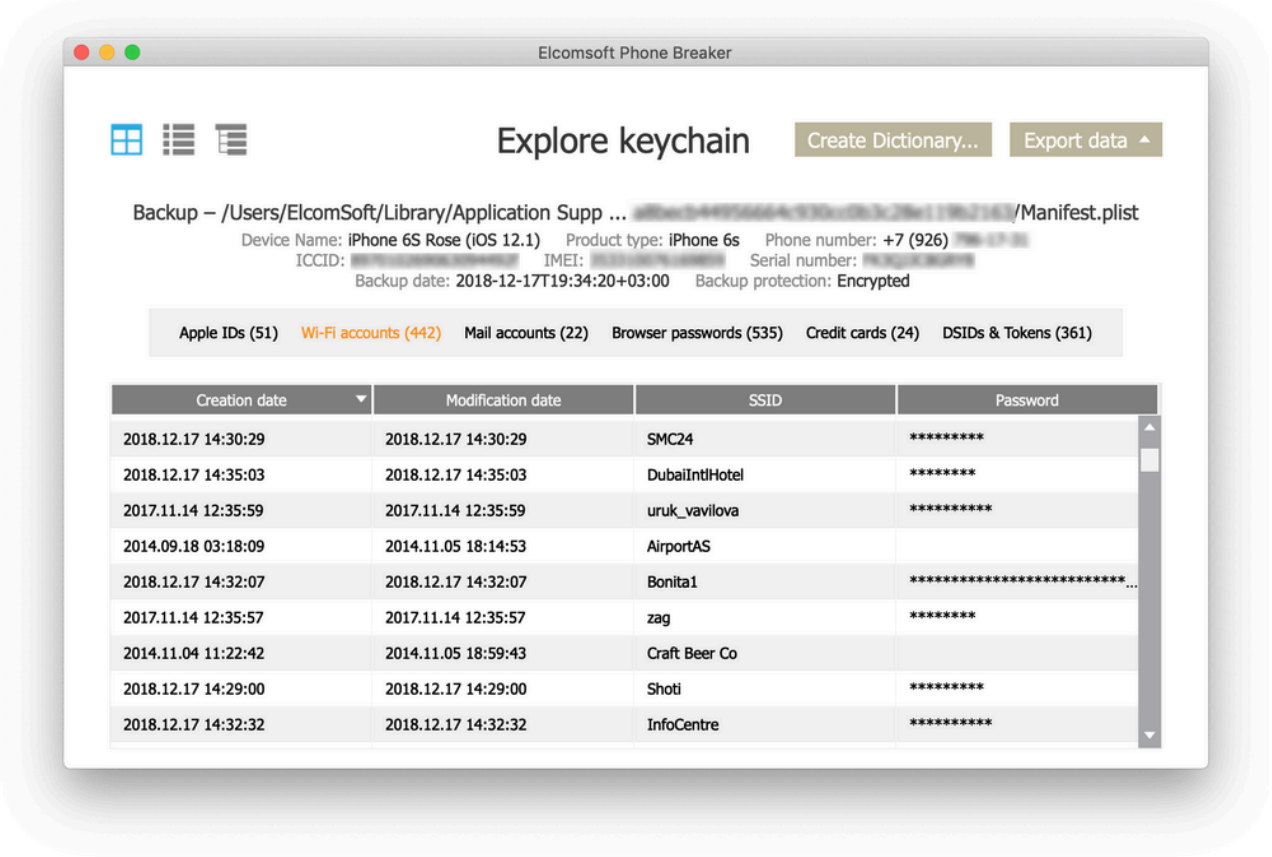
Pros: all keychain data (both user and system keychain) is available

Cons: need access to iCloud-synced Mac

Notes: user logon and keychain passwords are also needed

Method 4: Extract Keychain from Encrypted iTunes Backups

If you have access to the iPhone, you can create a password-protected iTunes backup. The “password-protected” part is absolutely mandatory. If you won’t set a password, or if you are analyzing an existing backup without a password, the keychain will not be accessible. In order to view the keychain, load the backup into Elcomsoft Phone Breaker and use the [Explore keychain] feature. You can notice that many of the keychain items are not decrypted. This is because those keychain records have a higher protection class, and can be accessed only by the device they were created on (a hardware specific key is required to decrypt).



This is not the only problem. If you don’t know the backup password for an existing backup, breaking it will not be easy. While we used to see recovery speeds of tens of thousands passwords per second for iOS 4-10.1, recent versions of iOS such as iOS 11 and 12 brought that number down to just about a hundred passwords per second with a powerful GPU. However, if you have the device itself and it is running iOS 11 or iOS 12, you can simply reset the backup password by using the “Reset All Settings” command. Note that this wipes Wi-Fi passwords but not the user’s passwords stored in the keychain.

Complexity: medium

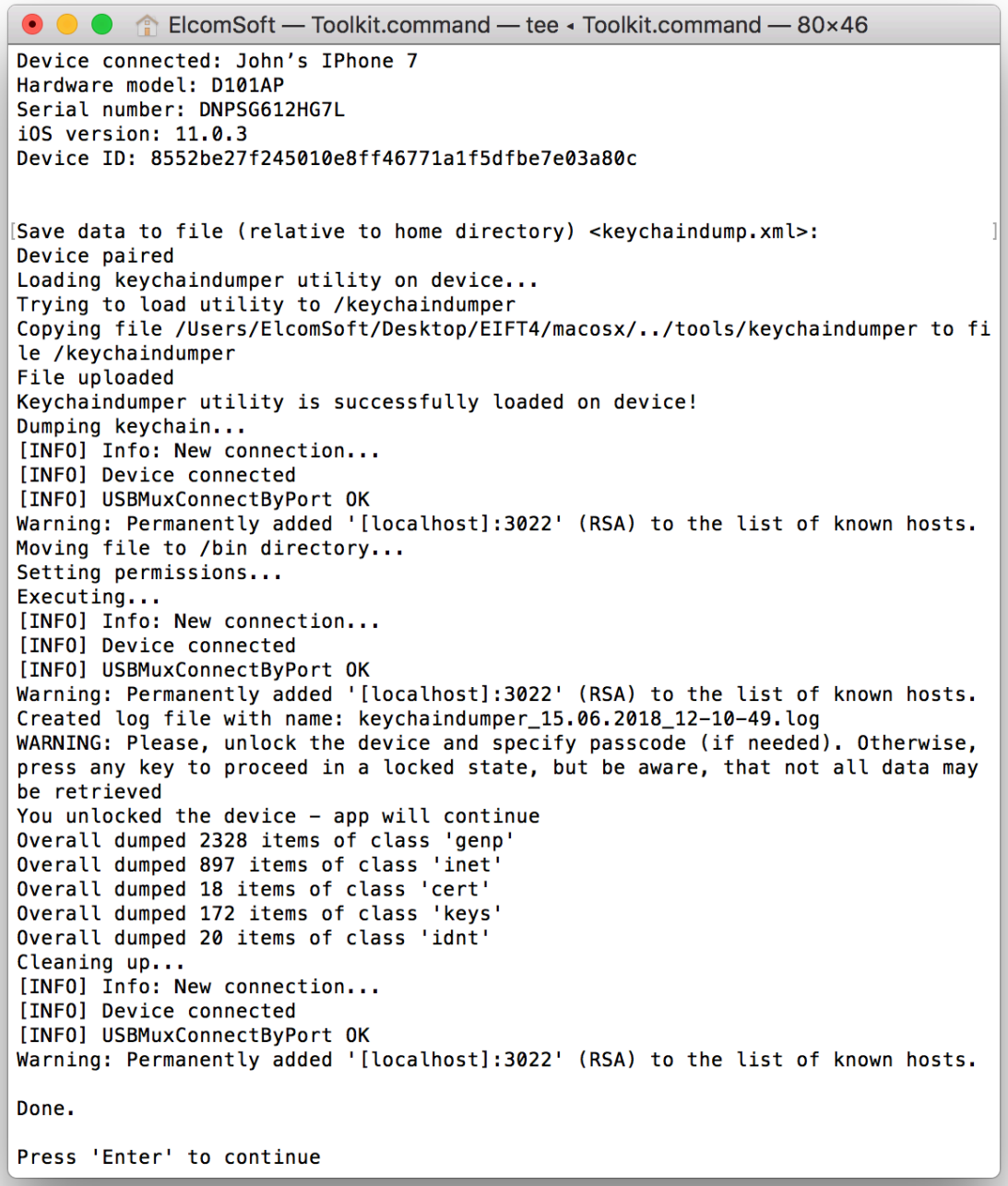
Pros: just iTunes backup (with known password) is needed, or device itself

Cons: breaking iOS 10.2+ password (if set) is virtually impossible; not all the records can be decrypted

Notes: for iOS 11+, backup password can be reset (but Wi-Fi passwords are lost then)

Method 5: Jailbreaking and Physical Acquisition

This is the dirtiest but the most powerful of all methods. If you have a device that can be jailbroken (at the time of this writing, jailbreaks exists for iOS versions up to and including iOS 11.3.1), you would be able to decrypt *all* keychain records including those with the highest protection class. Just use Elcomsoft iOS Forensic Toolkit. If you managed to install a jailbreak (this is not easy on some versions of iOS), the rest will be a matter of a few clicks.



The GrayKey device by GrayShift allows extracting the keychain (as well as the copy of the file system) from non-jailbroken iPhones, but it costs $15K and is available only to select agencies in select countries (US, Canada, UK, Australia and New Zealand for now). It also works for a limited number of iOS versions (the compatibility list is kept secret for some reason).

Complexity: hard

Pros: allows to get access to 100% keychain records

Cons: need access to the (unlocked) device; jailbreaking is required

Notes: GrayKey allows keychain extraction for iOS 11.4 as well and probably even some iOS 12 versions – without jailbreak, but available to Law Enforcement onlyt (in a limited number of countries); also, it is pricy

Method 6: iCloud Keychain

Since iOS 7, the keychain can be synced with other devices through iCloud. This is good news since iCloud extraction does not require access to the device itself. However, you will need the user's Apple ID and password, as well as the one-time code from the second authentication factor (unless you are performing the extraction on an already trusted device). In addition, you will need the screen lock passcode or system password to one of the iOS or macOS devices enrolled into the "trusted circle".

Many keychain items are not synced to iCloud. Apple's Set up iCloud Keychain article reads: "iCloud Keychain remembers things, so that you don't have to. It auto-fills your information—like your Safari usernames and passwords, credit cards, Wi-Fi networks, and social log-ins—on any device that you approve". Previous version of that article said that only the passwords are synced, which is not true; some applications (such as Facebook and LinkedIn at least) sync authentication tokens as well. The tokens are more difficult to use than passwords; you cannot use them manually to access the desired web site or application. However, they are somewhat superior to passwords as their use will allow you bypass the second authentication factor (if 2FA is used).

iCloud Keychain can be obtained with Elcomsoft Phone Breaker that you used to explore the local (iTunes) keychain. The downloaded keychain look just like the keychain from the iTunes backup. The number of records will be different as some records will be missing. In return, you may see a few extra records you did not see in the local backup.

Complexity: medium

Pros: does not require access to device; access keychain data from all synced devices

Cons: iCloud credentials (including second factor) and device passcode are needed, as well as iCloud Security Code for accounts without 2FA; many records are not available

Notes: if all requirements are met, you can also get access to iMessage in iCloud and iCloud-synced Health data

Conclusion: the Benefits of Keychain Decryption

There can be many situations when you may need access to keychain data even if you are not working for the law enforcement. If you do, you know better how important this data can be.

If you ever reset your device, this operation completely wipes the keychain without the chance of recovery. If you happened to have a single iTunes backup and forgot to set a password on it, you are out of luck. In this case, iCloud keychain may be your only hope if you had it enabled.

If you reset network settings on your device, this deletes the Wi-Fi passwords. If you have a lot of saved networks, just make sure to save them in advance.

It is worth adding a short note for our readers from the law enforcement. If you manage to extract the keychain, the next thing you may want to do is generating a wordlist/dictionary from the passwords discovered in the keychain. This wordlist will be *extremely* effective when attacking passwords to other data (documents, databases, or systems) of the device/account owner, especially if you use Distributed Password Recovery.

Apple, EDPR, EIFT, Elcomsoft Distributed Password Recovery, Elcomsoft iOS Forensic Toolkit, Elcomsoft Phone Breaker, Elcomsoft Phone Digger, Elcomsoft Phone Viewer, EPB, EPD, iCloud, iOS, iTunes, jailbreak, keychain, Keychain Access, macOS

Elcomsoft Distributed Password Recovery

Build high-performance clusters for breaking passwords faster. Elcomsoft Distributed Password Recovery offers zero-overhead scalability and supports GPU acceleration for faster recovery. Serving forensic experts and government agencies, data recovery services and corporations, Elcomsoft Distributed Password Recovery is here to break the most complex passwords and strong encryption keys within realistic timeframes.

Elcomsoft Distributed Password Recovery official web page & downloads »

Elcomsoft iOS Forensic Toolkit

Extract critical evidence from Apple iOS devices in real time. Gain access to phone secrets including passwords and encryption keys, and decrypt the file system image with or without the original passcode. Physical and logical acquisition options for all 64-bit devices running all versions of iOS.

Elcomsoft iOS Forensic Toolkit official web page & downloads »

Elcomsoft Phone Breaker

Gain full access to information stored in FileVault 2 containers, iOS, Apple iCloud and Windows Phone devices! Download device backups from Apple iCloud and Microsoft OneDrive servers. Use Apple ID and password or extract binary authentication tokens from computers, hard drives and forensic disk images to download iCloud data without a password. Decrypt iOS backups with GPU-accelerated password recovery.

Elcomsoft Phone Breaker official web page & downloads »

Elcomsoft Password Digger

Elcomsoft Password Digger is a Windows tool to decrypt information stored in Mac OS X keychain. The tool dumps the content of an encrypted keychain into a plain XML file for easy viewing and analysis. One-click dictionary building dumps all passwords from the keychain into a plain text file, producing a custom dictionary for password recovery tools. The custom dictionary helps breaking passwords to encrypted documents or backups faster.

Elcomsoft Password Digger official web page & downloads »

Source: https://blog.elcomsoft.com/2018/12/six-ways-to-decrypt-iphone-passwords-from-the-keychain/