

A Deep Dive into Apple Keychain Decryption

Published: 2025-01-20 · Archived: 2026-04-05 13:13:37 UTC

When it comes to the forensic investigation of Apple devices, a Keychain analysis is of particular importance. Not only does Keychain contain passwords from websites and applications, but it can also provide computer forensics with access to the same user's other Apple devices. Let's take a closer look.

- [Types of Keychains](#)
- [Use Cases](#)
- [Summary](#)

Types of Keychains

Keychain or [Keychain Services](#) is the password management system in macOS and iOS. It stores account names, passwords, private keys, certificates, sensitive application data, payment data, and secure notes. These records are dynamically linked to users' particular login passwords so that, when they log on to a Mac device, all of their various accounts and passwords are made available to the operating system and select applications.

The Keychain storage is located in:

- `~/Library/Keychains/` (and subfolders)
- `/Library/Keychains/`
- `/Network/Library/Keychains.`

There are three types of Mac Keychains: **Login Keychain**, **System Keychain**, and **Local Items (iCloud) Keychain**. They can be decrypted in Passware Kit within the **Password Managers | MacOS Keychain** section.

The Keychain files are viewed and edited through an application called Keychain Access. There is also a command-line equivalent to Keychain Access: `/usr/bin/security`. While there is no Keychain Access utility for iOS, passwords are synchronized across all of the Apple devices tied to a given iCloud account provided that the user has enabled the iCloud Keychain option. When this option is enabled, synchronization of the data occurs partially, as some applications and services may set a special flag in a Keychain to prevent the transmission of the corresponding data to iCloud.

Login Keychain

The Login Keychain is the default Keychain file that stores most of the passwords, secure notes, and other data. The data is stored in a file named **login.keychain-db** (or **login.keychain** in macOS prior to 10.12 Sierra) located in `/Users/<UserName>/Library/Keychains`.

By default, the Login Keychain password is the same as the Mac user password.

The password recovery process for this Keychain is time-consuming, but it can be accelerated by using GPU, reaching speeds of up to 1,200,000 passwords per second on an AMD 6900 XT.

🏠 < >
Tools Help ☺ - □ ×

Recover File Password

Files
Passwords Found
Resources
Performance
Attacks
Log

login.keychain-db

Folder: E:\Passware\Evidence\Keychain\login.keychain
 File Type: Keychain — Open Password, Hardware acceleration possible
 Complexity: ●●●● Brute-force - Slow
 MDS: 75825295F19323B2650CEDF738136D7A

Password: File-Open Ghost007

Accounts' passwords

11334056061	J3gkjjpRc3OcHKjXY71EsBi/BKczOgmgrVcvWBnsUPU=
JohnDoe	Ater9874nFd
JohnInCharge	Bdhey668a2
Window Bitmap Encryption	34ABF33DCE8E7AA0C57891871B1F730A
com.apple.scopedbookmarksgent.xpc	AwIAAAEBAAH70AAAAABiFL0J2sBE1kRPovu7InbcQN/gCP+26K0= pr:y*S1AKge#6zmk)f/g

Keychain Secure Note File: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted Keychain Access records\kumar.davletov@icloud.com-securenote.KSN

Keychain Secure Note File: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted Keychain Access records\securenote.KSN

Some keychain records (35 of 41) have been skipped as they exceed 128 symbols.

Extracted data: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted Keychain Access records

MDS hashes for files: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted Keychain Access records\Md5Hashes.txt

PASSWORDS FOUND 7	TIME ELAPSED 8 minutes, 7 seconds
PASSWORDS ANALYZED 21,205,699	

🖨️ Print
💾 Save Job ▾
⏪ RESUME ATTACKS
⬇️ SAVE REPORT
✅ DONE


System Keychain

The System Keychain stores items that are accessed by the OS, such as Wi-Fi passwords, and shared among users. The file, which is usually located in */Library/Keychains/*, can be decrypted instantly if a “Master Key” file is available (usually located in */private/var/db/SystemKey*).

🏠 < >
Tools Help ☺ - □ ×

Recover File Password

Files
Passwords Found
Resources
Performance
Attacks
Log



System.keychain

Folder: E:\Passware\Evidence\Keychain\system.keychains
 File Type: Keychain
 Complexity: ●●●● Instant Unprotection
 MD5: 4826C6F661B623CF74BABA1B770E8E07

Accounts' passwords	Password
DoeFR	kskujen99x
Netcom_536_5G	Che\$klL1
FR_GPON5_25AB	VWjBKgLXp5r95Cm45
GTS_GPON5_B47A	FKdxGGeX5f078
The-Clu 5GHz	oZBejNoc
JohnDoe	engahL2d

Extracted data: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted Keychain Access records

MD5 hashes for files: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted Keychain Access records\Md5Hashes.txt

PASSWORDS FOUND: **6**

TIME ELAPSED: **0 seconds**

🖨️ Print
💾 Save Job ▾
⏪ RESUME ATTACKS
⬇️ SAVE REPORT
✅ DONE

Local Items (iCloud) Keychain

The Local Items Keychain is used for keychain items that can be synced with iCloud Keychain. It contains encryption keys, applications data, webform entries, and some iOS data synced with iCloud. It presents two files: a keybag (**user.kb** file) and an SQLite database with encrypted records (**keychain-2.db**). If the iCloud synchronization is turned on, the **keychain-2.db** may contain passwords from other devices as well. Passware Kit recovers a password for the **user.kb** file and then decrypts the **keychain-2.db** database. By default, the user.kb password is the same as the macOS user password.

To recover the **user.kb** password on a Mac without a T2 chip, Passware Kit requires the 128-bit universally unique identifier number (UUID), which is the same as the name of the Keychain folder. Unfortunately, the password recovery for Local Items Keychain cannot be accelerated on GPU. After the successful recovery of a password, Passware Kit extracts all records that appear readable and saves the rest of the data in a file. Strings shorter than 128 symbols are considered passwords and saved to a **Passwords.txt** file, while **json** and **bplist** binary files are extracted as-is. Passware Kit also creates an **extracted-records.json** file with the complete extracted data.

Recover File Password

user.kb

Folder: E:\Passware\Evidence\Keychain\local_items.keychain\8C235FE7-184E-58FA-BF08-744A4453311F
File Type: MacOS Keychain file — Open Password
Complexity: ●●●● Brute-force - Slow
MD5: E5B210EB3B56D1E6AC87B1F0F3B3093B

Passwords:

File-Open	Ghost007
Extracted	000280-08-6dffd34c-8bd6-4557-9d45-616b95c55f078
Extracted	/X3YWmLYW081Dgho0wi09w==
Extracted	1027158E-99F4-45FF-BDA9-3C44516906DC
Extracted	127171FA-0206-4452-B3C6-7500B97FA39D
Extracted	133
Extracted	14FA1CD6-3AC3-4C56-86A1-D177EE806C68
Extracted	153C6835-ECD1-49AD-870F-4905228783F8
Extracted	19H1806
Extracted	25BB7C7F-049C-4B2C-BEAE-4CB26AD1557A
Extracted	sjkk^277sSLks9

Extracted data: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted keychain records\8C235FE7184E58FABF08744A4453311F

MD5 hashes for files: C:\Users\PasswareUser\AppData\Roaming\Passware\Passware Kit\CurrentUnprotected\Extracted keychain records\8C235FE7184E58FABF08744A4453311F\Md5Hashes.txt

PASSWORDS FOUND: **40** TIME ELAPSED: **1 minute, 7 seconds**

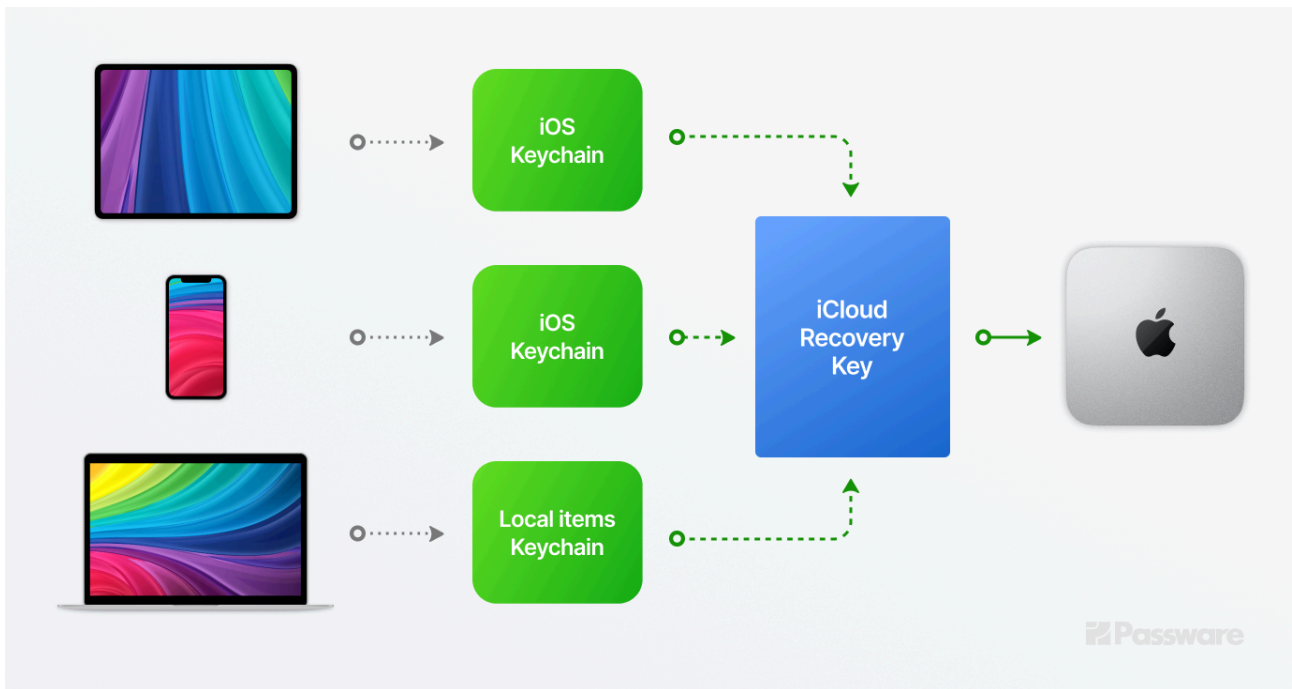
PASSWORDS ANALYZED: **22**

Print Save Job RESUME ATTACKS SAVE REPORT DONE

Use Cases

It is extremely important to analyze as many Apple devices linked to the same iCloud account as possible. A decrypted Keychain from one device can gain entry into a device with stronger encryption, such as a Mac with a T2 chip. The following are some examples of cases in which Passware Kit facilitates the extraction of data from locked devices. Note that instant decryption is possible only if iCloud was selected as the backup option while the encryption was enabled.

If there are no additional devices to extract the Keychain from, Passware offers a [T2 Decryption Add-on](#) to decrypt APFS disks from Mac computers protected with an Apple T2 security chip.



Case 1

A Macbook Air 2017 and a Mac Pro 2019 with a T2 chip of the same iCloud account

For the MacBook Air without a T2 chip, Passware Kit decrypts or recovers a password for an APFS disk using the **Full Disk Encryption | FileVault/APFS** option. Having gained access to the Keychain folder, Passware Kit recovers the Keychain password from a **user.kb** file by means of the **Password Managers | MacOS Keychain | Local Items Keychain** option and then extracts the data from the Local Items Keychain. The extracted data includes a **decrypted-keychain.plist** file that can serve to unlock an APFS disk on the Mac Pro with a T2 chip instantly with the **Full Disk Encryption | APFS/Mac T2** option.

Tools Help

Unlock an APFS Volume on Mac with T2 chip

YOU WILL NEED THE FOLLOWING

iCloud credentials or iOS backup
The unlock is possible only if iCloud was selected as the backup option while the encryption was enabled

Target Mac
The Mac with T2 chip to unlock

Thunderbolt 3 cable
to connect to the target Mac

This Mac
Thunderbolt 3 port is required

iCloud credentials

iCloud Login

IOS Backup

Decrypted Keychain

Decrypted Keychain

Users > agent > Desktop > Wor... > decrypted-keychain.plist

Browse...

NEXT

The screenshot shows the 'Recover File Password' interface. At the top, there are navigation icons (home, back, forward) and 'Tools' and 'Help' links. Below the title, there are tabs for 'Files', 'Passwords Found', 'Resources', 'Performance', 'Attacks', and 'Log'. The main content area displays the following information:

- Disk Name:** disk8s5
- File Type:** APFS local disk
- Complexity:** ●●●● Instant Unprotection
- Password:** FNOU-A63L-MEE9-EEF3-EY6OP-DWF3
- GUID:** EC1C2AD9-B618-4ED6-BD8D-BD8361C27507
- Mounted Volume:** Volumes > Macintosh HD 1

At the bottom of the interface, there is a summary bar showing 'PASSWORDS FOUND: 1' and 'TIME ELAPSED: 36 seconds'. Below this are buttons for 'Print', 'Save Job', 'RESUME ATTACKS', 'SAVE REPORT', and 'DONE'.

Case 2

An iPhone 7 Plus disabled with time-lock and a Mac Mini 2018 with a T2 chip of the same iCloud account

[Passware Kit Mobile](#) recovers a passcode for the iPhone 7 and extracts the data from the device, including an iOS Keychain, saving a **decrypted-keychain.plist** file. With the **Full Disk Encryption | APFS/Mac T2** option, Passware Kit Forensic for Mac uses the decrypted keychain to unlock an APFS disk on the Mac Mini equipped with a T2 chip.

Case 3

An iPhone 13 and a decrypted APFS image of a Macbook Pro 2017 of the same iCloud account

Password recovery for a Login Keychain, unlike the recovery of a Local Items Keychain password, can be accelerated on GPU. Therefore, the first step is to recover a **login.keychain** file password from the APFS image using the **Password Managers | MacOS Keychain | Keychain** option. On an AMD 6900 XT, the speed is up to 1,200,000 passwords per second. By default, the password for the Login Keychain and Local Items Keychain is the same, so there is high chance that recovering the Login Keychain password also provides access to the Local Items (iCloud) Keychain database and, thus, to the records in the iPhone, such as mobile Safari passwords.

Case 4


An iPhone 6 and a Macbook Pro 2017 without a T2 chip of the same iCloud account

[Passware Kit Mobile](#) recovers the passcode for the iPhone 6 and extracts its data, including an iOS Keychain, saving a **decrypted-keychain.plist** file. Passware Kit Forensic uses the decrypted keychain to instantly decrypt the Macbook's APFS image with the **Full Disk Encryption | APFS / Mac T2** option. This approach avoids the need to perform a time-consuming brute-force password recovery process.

Summary

The table below summarizes the decryption and password recovery options for different types of Keychain.

Type of Keychain	Location	Input files/folders	Decryption Recovery Options	GPU Acceleration
Login Keychain	/Users/<UserName>/Library/Keychains	login.keychain	Brute-force - Slow	Yes
System Keychain	/Library/Keychains/ Master Key: /private/var/db/SystemKey	System.keychain SystemKey	Instant Decryption	N/A
Local Items Keychain	~/Library/Keychains/<UUID>	user.kb UUID	Brute-force - Slow	No



A comprehensive forensic investigation involves the analysis of multiple devices and artifacts. Starting from the least-secure devices (e.g., memory images, iTunes backups, and Macs without T2/M1 chip), Passware Kit extracts and decrypts a Keychain that can then be used to access data from other devices.

Learn more about [Passware Kit Forensic capabilities](#) and the best practices on the [Passware Knowledge Base](#).

Source: <https://support.passware.com/hc/en-us/articles/4573379868567-A-Deep-Dive-into-Apple-Keychain-Decryption>