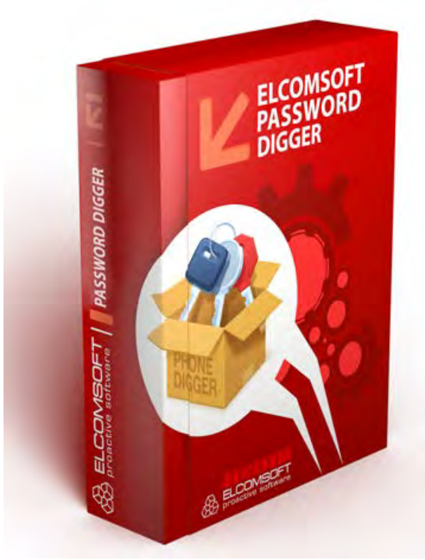
Elcomsoft Password Digger Decrypts Mac OS Keychains


ELCOMSOFT PASSWORD DIGGER
ELCOMSOFT | PASSWORD DIGGER
PHONE DIGGER
ELCOMSOFT proactive software

Moscow, Russia – September 16, 2015 - ElcomSoft Co. Ltd. announces the release of Elcomsoft Password Digger, a digital forensic tool for Windows to decrypt the content of Mac OS X keychains. The new tool can decrypt the content of system and all user keychains from a Mac OS computer, exporting complete information into an unencrypted XML file or building a plain text dictionary for using with password recovery tools.

About Mac OS X Keychain

Keychain was introduced with Mac OS 8.6 as means to provide secure storage for sensitive information. Mac OS X uses keychain to manage system-wide and user passwords. System passwords such passwords to Wi-Fi networks are stored in the system keychain, while pretty much everything else ends up in the user keychain.

User keychain can contain highly sensitive authentication information such as passwords to Web sites and accounts (including the user's Apple ID password), VPN, RDP, FTP and SSH passwords, passwords to mail accounts including Gmail and Microsoft Exchange, passwords to network shares, and iWork document passwords. Third-party applications can store sensitive information in the keychain. In addition, the keychain may contain private keys, certificates, authentication tokens, and secure notes. Particularly, extracting the user's Apple ID password is highly valuable as it enables investigators to pull backups created by user's iOS devices (iPhone, iPad) from Apple iCloud.

Information stored in the keychain is securely encrypted. System keychain uses a decryption key stored in a file, while user keychains are typically encrypted with keys derived from users' Mac OS account passwords.

For viewing items stored in the keychain, Apple offers a built-in utility named Keychain Access. However, using Keychain Access for forensic purposes is slow and inconvenient as the Apple tool requires the user has to re-enter the password for viewing each individual record.

Extracting Mac OS X Keychain

Elcomsoft Password Digger is designed to extract, decrypt and export the content of the system and all user keychains. The tool dumps information from the keychain into a plain, decrypted XML file containing all records complete with all fields such as the URL, creation and last access time, login, password, and other relevant fields. The resulting XML file can be imported into any XML-enabled tool including a wide range of forensic products and many generic tools such as Microsoft Excel.

In order to use Elcomsoft Password Digger, experts will need a Windows PC, keychain files extracted from Mac OS, as well as the user's authentication information (Mac OS login and password or keychain password, if it's different). For decrypting system keychains, the tool will require a decryption key that must be extracted from the Mac OS computer (administrative privileges are required to extract the file from a live system).

Building Custom Password Dictionaries

Attacking many types of passwords is impossible without a quality dictionary. Even with GPU acceleration, certain types of passwords (such as those protecting Microsoft Office 2010-2013 documents) are just too slow to brute force. A custom dictionary containing the user's other passwords is invaluable in assisting these types of attacks.

Elcomsoft Password Digger offers a tool to build highly relevant password dictionaries in one click. By extracting all passwords stored in the user's keychain and saving them into a plain, filtered text file that only contains the passwords, Elcomsoft Password Digger allows building a highly relevant custom dictionary for breaking strong passwords. The resulting file can be used for dictionary attacks with all password recovery tools that support custom dictionaries.

About Password Digger

Elcomsoft Password Digger is a Windows tool to extract and 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 offers the ability to dump all passwords from the keychain into a plain text file, producing a custom dictionary for password recovery tools. A custom dictionary containing all user passwords can be used to speed up password recovery when breaking encrypted documents or backups. The system and all user keychains can be decrypted.

Pricing and Availability

Elcomsoft Password Digger is available immediately. North American pricing starts from $199. Local pricing may vary.

Elcomsoft Password Digger requires a Windows PC with Windows Vista, Windows 7, 8, 8.1, Windows 10 or Windows 2003, 2008 or 2012 Server, and supports keychains produced by all versions of Mac OS including the latest Mac OS X 'El Capitan'.

About ElcomSoft Co. Ltd.

Founded in 1990, ElcomSoft Co. Ltd. develops state-of-the-art computer forensics tools, provides computer forensics training and computer evidence consulting services. Since 1997, ElcomSoft has been providing support to businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools are used by most of the Fortune 500 corporations, multiple branches of the military all over the world, foreign governments, and all major accounting firms. ElcomSoft is a Microsoft Partner (Gold Application Development and Gold Intelligent Systems), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.