GovTools

User Manual
v1.0
Stand: 05.04.2024

GovCracker & GovTools
by Decrypta Technologies

GovTools

GovTools is an open source tool for the decryption of passwords in criminal IT forensics.

GovTools was primarily developed for use in international law enforcement agencies, universities and IT forensics companies.

Further information can be found at www.govcracker.com or Github.

Notes:

1. all copyrights of this program belong exclusively to the author, unless waived in writing.

2. you may not misuse this software to decrypt passwords for which you have no authorization.

3. no guarantee or liability of any kind is assumed. You use the software at your own risk. The author is not liable for loss of data, damage, loss of profit or any other type of loss or damage.

Table of contents

1 GovTools | Hash-Extraction

1.1 Standard procedure

1. Select the appropriate entry in the extraction list.

2. Then select the encrypted file or image and follow the instructions.

3 Images must not be split during creation.

4. The result of the extraction is exported to the GovTools folder "_Hashout".

5. For some functions you need to install "Linux for Windows" (Ubuntu 20.04 or 22.04 LTS). You can download this software package free of charge from the Microsoft Store.

1.2 7zip

File format: *.7z

Extraction: see standard procedure

Special features: no

1.3 APFS (Apple MacBook)

File format: RAW format, such as *.dd, *.001, etc.

Extraction: see standard procedure.

Special features: Install Linux for Windows (Ubuntu 20.04 or 22.04. LTS)

Create image (correctly):

- Boot the MacBook (without T2 or M1 chip) with a portable Linux distribution, such as Paladin, Caine, Digital Collector or Kali.

- Create a raw image (.dmg or .001) of the entire Apple hard disk (without file splitting).

- If it is an iMac with a Fusion drive, please contact us. There are special procedures for this.

- Copy the image to an internal hard disk, e.g. C:\ or D:\ of the GovCracker PC (not an external hard disk).

- Select the image file.

- It is possible that several hashes are extracted, as the system may contain several UUIDs.

- Normally the first hash displayed is the correct one (the local Open Directory user).

- The goal of apfs2hashcat is to extract the hash from an encrypted Mac book image. The Filevault encryption can decrypt GovCracker in hash type 18300.

1.4 Bitcoin wallet (Bitcoin Core)

File format: wallet.dat (standard file)

Extraction: see standard procedure

Special features: no

1.5 Bitlocker

File format: Bitlocker file or image

Extraction: see standard procedure

Special features: Extraction of a 16GB USB stick takes approx. one hour.

1.6 DASH wallet (DASH Core)

File format: wallet.dat (standard file)

Extraction: see standard procedure

Special features: no

1.7 DogeCoin wallet (DogeCoin Core)

File format: wallet.dat (standard file)

Extraction: see standard procedure

Special features: no

1.8 eCryptfs

File format: wrapped-passphrase (standard file)

Extraction: see standard procedure

Special features: no

1.9 Electrum wallet

File format: default_wallet (standard file)

Extraction: see standard procedure

Special features: no

1.10 Ethereum (MyEtherWallet.com / keystore file)

File format: UTC + creation date + wallet address

(bspw. UTC--2021-01-12T19-30-43.061A—
a505557bafe221b889a1f9f11d7d659895edd979)

Extraction: see standard procedure

Special features: no

1.11 Exodus Wallet

Special features: see instructions in GovTools

1.12 iTunes Backup (Apple)

File: manifest.plist (standard file)

Extraction: see standard procedure

Special features: no

1.13 KeePass

File format: *.kdbx

Extraction: see standard procedure

Special features: Keyfile optional

1.14 LibreOffice / OpenOffice

File format: *.ods, *.odt, etc.

Extraction: see standard procedure

Special features: no

1.15 Linux Login Password

File path: etc/shadow in Linux

Extraction: see standard procedure

Special features: no

1.16 Litecoin Wallet (Litecoin Core)

File format: Wallet.dat (standard file)

Extraction: see standard procedure

Special features: no

1.17 LUKS (Linux Unified Key System)

File format: freely selectable file extension

Extraction: see standard procedure

Special features: no

1.18 MetaMask Wallet

Special features: see instructions described in GovTools

1.19 Mozilla Firefox

Special features: see described instructions in GovTools

1.20 MultiBit Wallet

Special features: see described instructions in GovTools

1.21 Office (Word, Excel, etc.)

File format: *.doc*, *.xl*, etc.

Extraction: see standard procedure

Special features: no

1.22 PDF

File format: *.pdf

Extraction: see standard procedure

Special features: You can extract hashes from several PDF files at the same time.

1.23 RAR

File format: *.rar

Extraction: see standard procedure

Special features: no

1.24 VeraCrypt / TrueCrypt (File)

File format: freely selectable file extension

Extraction: see standard procedure

Special features: A second hash is always automatically extracted for a possible hidden volume. This can be deleted if required (last hash in the hash file).

1.25 VeraCrypt / TrueCrypt (Partition)

File format: freely selectable file extension

Extraction: see standard procedure

Special features: A second hash is always automatically extracted for a possible hidden volume. This can be deleted if required (last hash in the hash file).

1.26 VeraCrypt / TrueVrypt (boot partition)

File format: freely selectable file extension

Extraction: see standard procedure

Special features: A second hash is always automatically extracted for a possible hidden volume. This can be deleted if required (last hash in the hash file).

1.27 Windows Login Password

Extraction: see notes in GovTools

1.28 Windows Hello PIN

Extraction: see notes in GovTools

1.29 ZIP

File format: *.zip

Extraction: see standard procedure

Special features: no

2 Further tools

2.1 Cominator

Combinator can combine up to three wordlists. Each word in the

second and third wordlist is appended to each word in the first wordlist.

2.2 Len

With "Len" you can extract wordlist entries of a certain length into a new wordlist. For example, all GovCracker_Wordlist.txt entries with a minimum length of 6 and a maximum length of 10 can be extracted.

2.3 DupCleaner

DupCleaner removes all duplicates from a wordlist.

2.4 Hash Generator

Test hashes can be created here for test purposes. The hash value is automatically stored in the "_Hashout" folder.

2.5 Bulk Extractor

Bulk-Extractor is a very powerful extraction tool. It searches RAW image files (*.dd, *.mem, etc.) from disk images for IP, e-mail addresses, telephone numbers, etc.

Furthermore, extensive word lists are created from the image file. If the password you are looking for has been saved somewhere, Bulk-Extraktor will find it and extract it. The extraction processes can take some time.