GovTools

User Manual
v1.0
Stand: 05.04.2024

GovCracker & GovTools
by Decrypta Technologies

GovTools

GovTools ist ein Open-Source Tool, für die Entschlüsselung von Passwörtern in der kriminalistischen IT-Forensik.

GovTools wurde in erster Linie für den Einsatz in internationalen Strafverfolgungs-behörden, Universitäten und für IT-Forensik-Unternehmen entwickelt.

Weitere Informationen unter www.govcracker.com oder Github.

Hinweise:

1. Alle Urheberrechte dieses Programms liegen ausschließlich beim Autor, außer es wurde schriftlich darauf verzichtet.

2. Diese Software dürfen Sie nicht zum Entschlüsseln von Passwörtern missbrauchen, für die Sie keine Befugnis haben (vgl. § 202 a ff. StGB).

3. Es wird keine Garantie oder Haftung jeglicher Art übernommen. Sie verwenden die Software auf eigene Gefahr. Der Autor haftet nicht für Datenverlust, Schäden, Gewinnverlust oder jeglicher andere Arten von Verlust oder Beschädigung.

Inhaltsverzeichnis

1 GovTools │ Hash-Extraktion

1.1 Standard-Verfahren

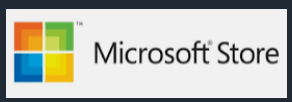
1. Wählen Sie den passenden Eintrag in der Extraktionsliste aus.

2. Wählen Sie die verschlüsselte Datei oder Image aus und folgen den Anweisungen.

3. Images dürfen bei der Erstellung **nicht** gesplittet werden.

4. Das Ergebnis der Extraktion wird in den GovTools Ordner „_Hashout“ exportiert.

5. Für manche Funktionen müssen Sie „Linux for Windows“ (Ubuntu 20.04 oder 22.04 LTS) installieren. Dieses Software-Paket können Sie kostenlos im Microsoft-Store herunterladen.



1.2 7zip

Dateiformat: *.7z
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.3 APFS (Apple MacBook)

Dateiformat: RAW-Format, wie bspw. *.dd, *.001, usw.
Extraktion: siehe Standard-Verfahren.
Besonderheiten: Linux for Windows (Ubuntu 20.04 oder 22.04. LTS) installieren

Image (richtig) erstellen:

- Booten Sie das MacBook (ohne T2 oder M1 Chip) mit einer portablen Linux-Distribution, wie bspw. Paladin, Caine, Digital Collector oder Kali.
- Erstellen Sie ein Raw-Image (.dmg oder .001) der gesamten Apple-Fest-platte (**ohne** Datei-Splitting).
- Wenn es sich um ein iMac mit Fusion-Drive handelt, nehmen Sie bitte mit uns Kontakt auf. Hierfür gibt es besondere Vorgehensweisen.
- Kopieren Sie das Image auf eine **interne** Festplatte, bspw. C:\ oder D:\ des GovCracker-PCs (**nicht** externe Festplatte).
- Wählen Sie die Image-Datei aus.
- Es ist möglich, dass mehrere Hashes extrahiert werden, da das System mehrere UUIDs enthalten kann.
- Normalerweise ist der erste angezeigte Hash der richtige (der lokale Open-Directory-Benutzer).
- Das Ziel von apfs2hashcat ist es den Hash aus einem verschlüsselten MacBook-Image zu extrahieren. Die Filevault Verschlüsselung kann GovCracker im Hash-Typ 18300 entschlüsseln.

1.4 Bitcoin-Wallet (Bitcoin Core)

Dateiformat: wallet.dat (Standarddatei)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.5 Bitlocker

Dateiformat: Bitlocker-Datei oder Image
Extraktion: siehe Standard-Verfahren
Besonderheiten: Die Extraktion eines 16GB USB-Sticks dauert ca. eine Stunde.

1.6 DASH-Wallet (DASH Core)

Dateiformat: wallet.dat (Standarddatei)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.7 DogeCoin-Wallet (DogeCoin Core)

Dateiformat: wallet.dat (Standarddatei)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.8 eCryptfs

Dateiformat: wrapped-passphrase (Standarddatei)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.9 Electrum-Wallet

Dateiformat: default_wallet (Standarddatei)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.10 Ethereum (MyEtherWallet.com / Keystore-File)

Dateiformat: UTC + Erstellungsdatum + Walletadresse (bspw. UTC--2021-01-12T19-30-43.061A—a505557bafe221b889a1f9f11d7d659895edd979)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.11 Exodus Wallet

Besonderheiten: siehe Anleitung in GovTools

1.12 iTunes Backup (Apple)

Datei: manifest.plist (Standarddatei)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.13 KeePass

Dateiformat: *.kdbx
Extraktion: siehe Standard-Verfahren
Besonderheiten: Keyfile optional

1.14 LibreOffice / OpenOffice

Dateiformat: *.ods, *.odt, usw.
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.15 Linux Login Password

Dateipfad: etc/shadow in Linux
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.16 Litecoin-Wallet (Litecoin Core)

Dateiformat: Wallet.dat (Standarddatei)
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.17 LUKS (Linux Unified Key System)

Dateiformat: frei wählbare Dateiendung
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.18 MetaMask Wallet

Besonderheiten: siehe beschriebene Anleitung in GovTools

1.19 Mozilla Firefox

Besonderheiten: siehe beschriebene Anleitung in GovTools

1.20 MultiBit Wallet

Besonderheiten: siehe beschriebene Anleitung in GovTools

1.21 Office (Word, Excel, etc.)

Dateiformat: *.doc*, *.xl*, usw.
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.22 PDF

Dateiformat: *.pdf
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.23 RAR

Dateiformat: *.rar
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

1.24 VeraCrypt / TrueCrypt (File)

Dateiformat: frei wählbare Dateiendung
Extraktion: siehe Standard-Verfahren
Besonderheiten: Es wird autom. immer ein zweiter Hash für ein mögliches Hidden-Volumen extrahiert. Dieser kann bei Bedarf gelöscht werden (letzter Hash in der Hash Datei).

1.25 VeraCrypt / TrueCrypt (Partition)

Dateiformat: frei wählbare Dateiendung
Extraktion: siehe Standard-Verfahren
Besonderheiten: Es wird autom. immer ein zweiter Hash für ein mögliches Hidden-Volumen extrahiert. Dieser kann bei Bedarf gelöscht werden (letzter Hash in der Hash Datei).

1.26 VeraCrypt / TrueVrypt (Boot-Partition)

Dateiformat: frei wählbare Dateiendung
Extraktion: siehe Standard-Verfahren
Besonderheiten: Es wird autom. immer ein zweiter Hash für ein mögliches Hidden-Volumen extrahiert. Dieser kann bei Bedarf gelöscht werden (letzter Hash in der Hash Datei).

1.27 Windows Login Password

Extraktion: siehe Hinweise im GovTools

1.28 Windows Hello PIN

Extraktion: siehe Hinweise im GovTools

1.29 ZIP

Dateiformat: *.zip
Extraktion: siehe Standard-Verfahren
Besonderheiten: nein

2 Weitere Tools

1.30 Combinator

Combinator kann bis zu drei Wordlists miteinander verbinden. Jedes Wort der zweiten und dritten Wordlist wird an jedes Wort der ersten Wordlist angehangen.

1.31 Len

Mit "Len" können Sie Wordlist-Einträge mit einer bestimmten Länge in eine neue Wordlist extrahieren. Damit könnten Sie bspw. alle GovCracker_Wordlist.txt Einträge mit einer mind. Länge von 6 und einer max. Länge von 10 extrahiert werden.

1.32 DupCleaner

DupCleaner entfernt alle Duplikate aus einer Wordlist.

1.33 Hash Generator

Für Testzwecke können hier Test-Hashes erstellt werden. Der Hashwert wird automatisch im Ordner „_Hashout“ abgelegt.

1.34 Bulk-Extractor

Bulk-Extractor ist ein sehr leistungsstarkes Extraktions-Werkzeug. Es durchsucht RAW-Imagedateien (*.dd, *.mem, usw.) von Datenträgerabbildern nach IP-, E-Mail-Adressen, Telefonnummern, usw.
Des Weiteren werden umfangreiche Wordlists aus der Imagedatei erstellt. Sollte das gesuchte Passwort irgendwo abgespeichert worden sein, wird Bulk-Extraktor es finden und extrahieren. Die Extraktionsprozesse können eigene Zeit in Anspruch nehmen.