

## New Tool: cs-extract-key.py

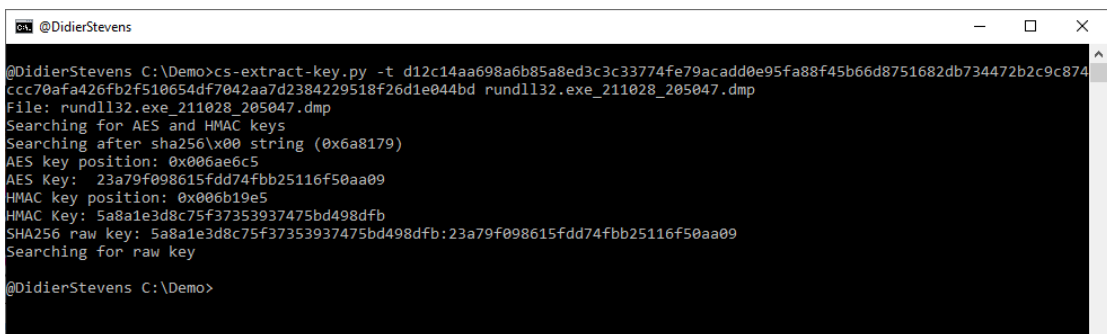
Published: 2021-11-03 · Archived: 2026-04-05 20:16:25 UTC

### New Tool: cs-extract-key.py

cs-extract-key.py is a tool designed to extract cryptographic keys from Cobalt Strike beacon process memory dumps.

This tool was already available in my [beta repository](#).

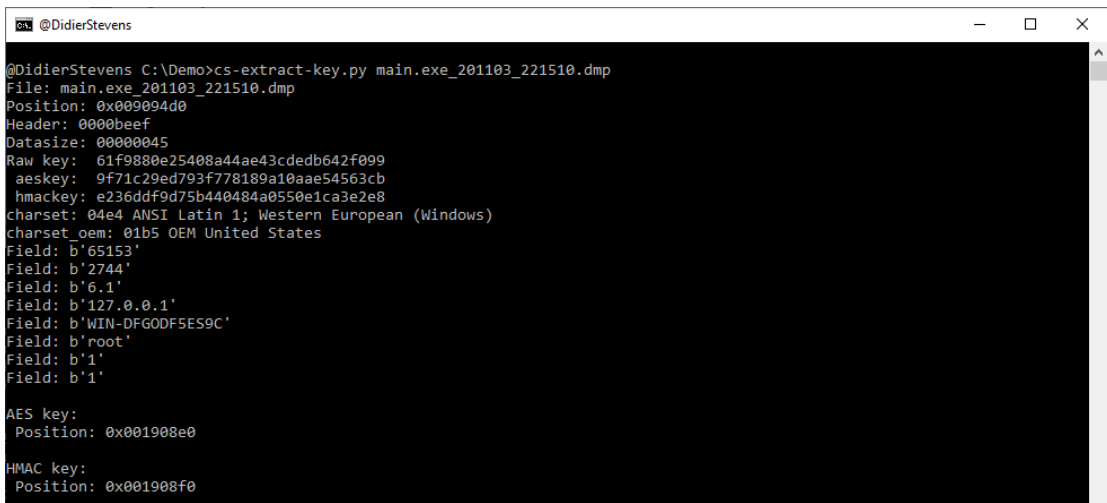
This tool can extract cryptographic keys from process memory dumps of a version 3.x beacon directly:



```
@DidierStevens C:\Demo>cs-extract-key.py -t d12c14aa698a6b85a8ed3c3c33774fe79acadd0e95fa88f45b66d8751682db734472bc9c874ccc70afa426fb2f510654df7042aa7d2384229518f26d1e044bd rundll32.exe_211028_205047.dmp
File: rundll32.exe_211028_205047.dmp
Searching for AES and HMAC keys
Searching after sha256\x00 string (0x6a8179)
AES key position: 0x006ae6c5
AES Key: 23a79f098615fdd74fbb25116f50aa09
HMAC key position: 0x006b19e5
HMAC Key: 5a8a1e3d8c75f37353937475bd498dfb
SHA256 raw key: 5a8a1e3d8c75f37353937475bd498dfb:23a79f098615fdd74fbb25116f50aa09
Searching for raw key

@DidierStevens C:\Demo>
```

And from version 4.x together with encrypted data extracted from network capture:



```
@DidierStevens C:\Demo>cs-extract-key.py main.exe_201103_221510.dmp
File: main.exe_201103_221510.dmp
Position: 0x009094d0
Header: 0000beef
Datatype: 00000045
Raw key: 61f9880e25408a44ae43cdebd642f099
aeskey: 9f71c29ed793f778189a10aae54563cb
hmackey: e236ddf9d75b440484a0550e1ca3e2e8
charset: 04e4 ANSI Latin 1; Western European (Windows)
charset_oem: 01b5 OEM United States
Field: b'65153'
Field: b'2744'
Field: b'6.1'
Field: b'127.0.0.1'
Field: b'WIN-DFG0DF5E59C'
Field: b'root'
Field: b'1'
Field: b'1'

AES key:
Position: 0x001908e0

HMAC key:
Position: 0x001908f0
```

More details can be found in the man page, and in and upcoming blog post.

[cs-extract-key\\_V0\\_0\\_1.zip](#) ([https](#))

MD5: 4102A5A5BFD4D432DA4A721D43F568F5

SHA256: BBEDF6CBFFF51669187694F463C32A49F53420BEDF8B76508D06850643DE334F

Source: <https://blog.didierstevens.com/2021/11/03/new-tool-cs-extract-key-py/>