ReVaulting

decryption and opportunities

whoami

Francesco Picasso

Reality Net System Solutions

@dfirfpi

https://github.com/dfirfpi

blog.digital-forensics.it

what and why

Reverse Engineering Vaults

where Windows puts users' credentials

Main goal is to decrypt them

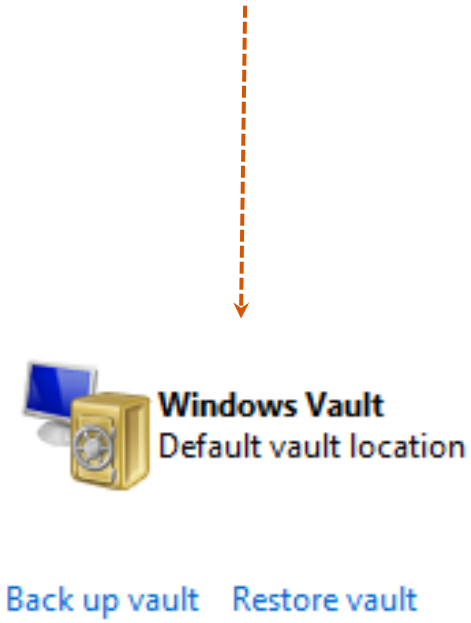
Offensive Digital Investigations

to access protected data/system

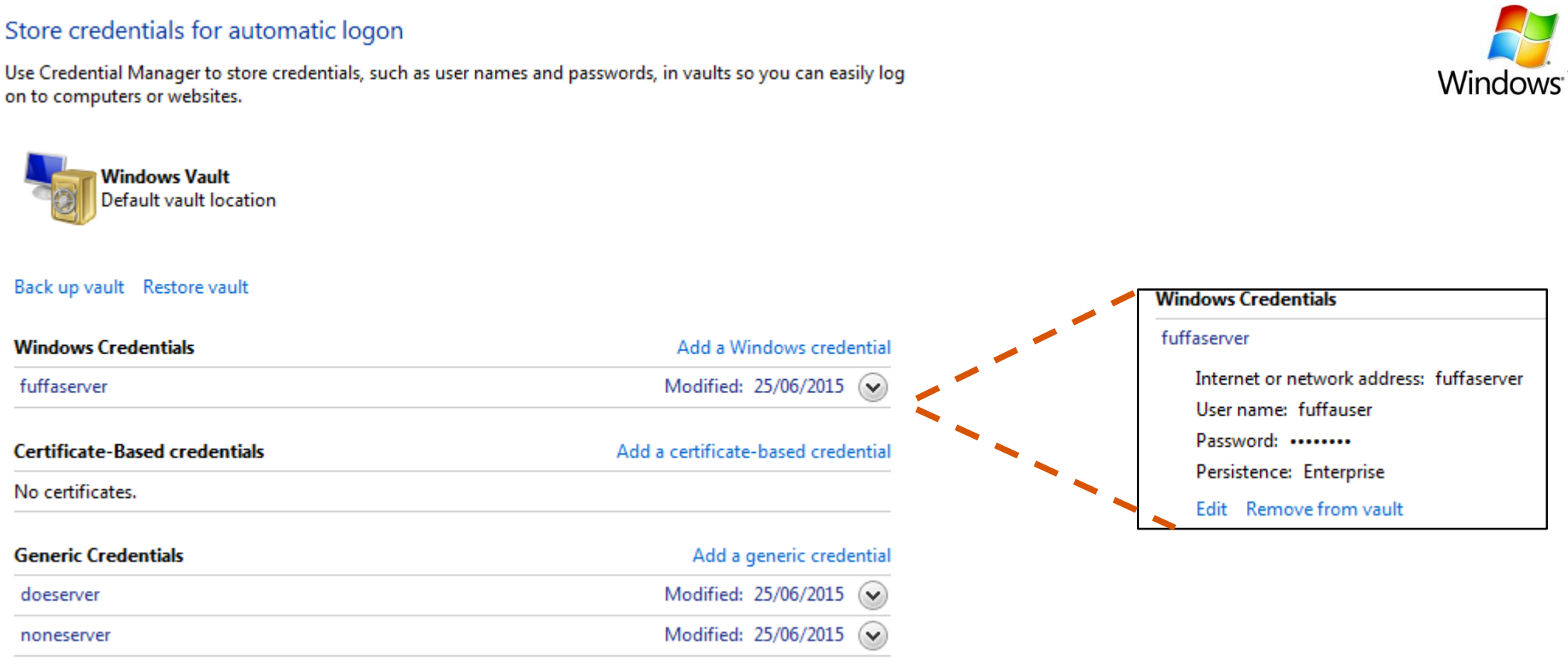
with proper legal authorizations

windows vaults

- User can manage his credentials with Credential Manager
  - create, delete, modify,
  - backup, restore: ***crd*** files
- Applications can manage credentials
  - user's one or their own
  - with or without user knowledge
- System can manage credentials
  - with or without user knowledge



credential manager



credentials? yes.. no.. yes again..

Windows 10

1

Web Credentials

Back up Credentials Restore Credentials

Windows Credentials Add a Windows credential

No Windows credentials.

Certificate-Based Credentials Add a certificate-based credential

No certificates.

Generic Credentials Add a generic credential

OneDrive Cached Credential Modified: 28/09/2015

virtualapp/didlogical Modified: 28/09/2015

yes

2

Windows Credentials

no

Web Credentials

Web Passwords

No web passwords.

no

```
C:\Users\dfirfpi>vaultcmd /listcreds:"Windows Credentials"
Credentials in vault: Windows Credentials
No credentials

C:\Users\dfirfpi>vaultcmd /listcreds:"Web Credentials"
Credentials in vault: Web Credentials

Credential schema: Windows Web Password Credential
Resource: https://login.microsoftonline.com/
Identity: [redacted].onmicrosoft.com
Saved By: Internet Explorer
Hidden: Yes
Roaming: No
Property (schema element id,value): (100,D[redacted])

Credential schema: Windows Web Password Credential
Resource: https://login.live.com/
Identity: [redacted]
Saved By: Internet Explorer
Hidden: Yes
Roaming: No
Property (schema element id,value): (100,[redacted])
```

yes

vaultcmd vs «Credential Manager»

credentials and vaults

from a *file system* point of view:

- **Credentials**
  - are files kept by the system in folders named "Credentials"
- **Vaults**
  - are files kept by the system in folders named "Vault"

- *<user-profile>*\AppData\(Local|Roaming)\Microsoft\
  - roaming for enterprise users
  - Vault folders contain sub-folders named based on the schema guid

- plus own **system**'s credentials/vaults

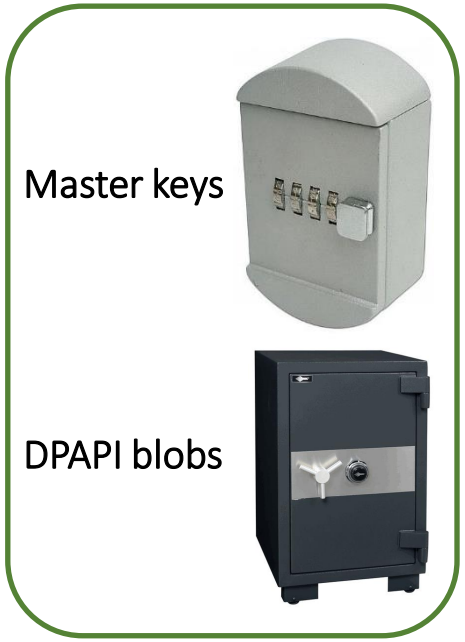
dpapi in a nutshell

well, a nutshell is not enough

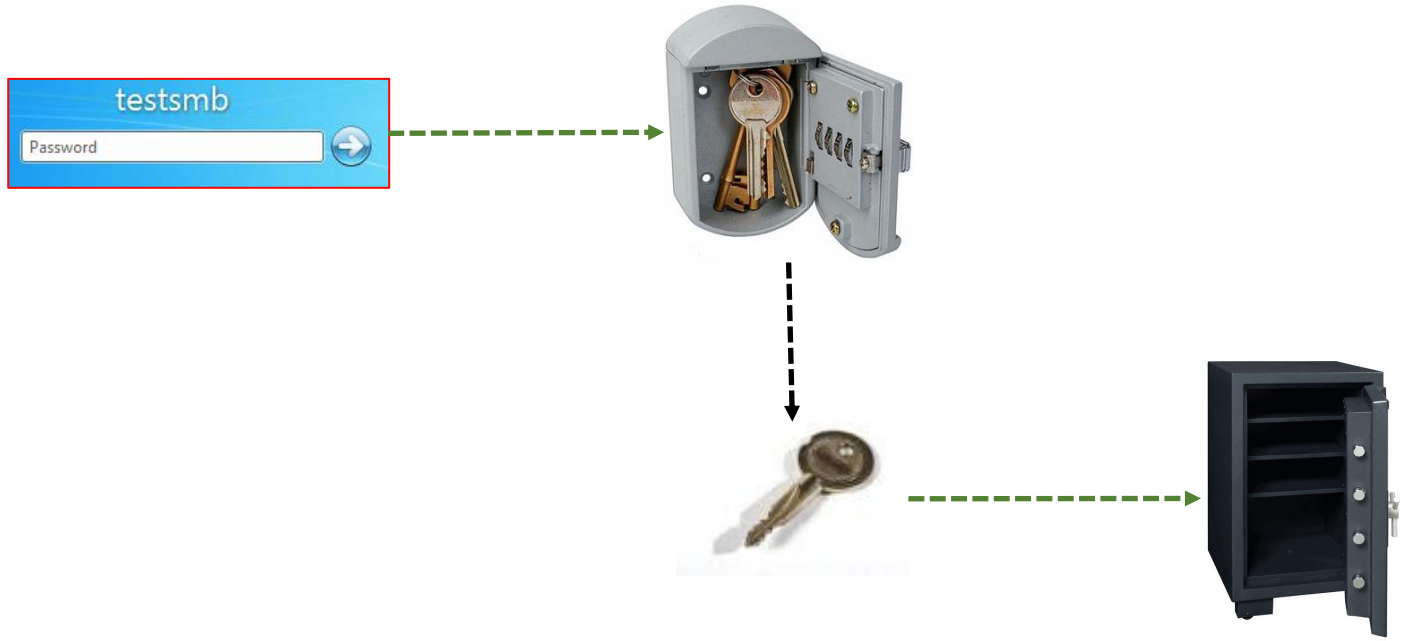
dpapi

- DPAPI: Data Protection API
  - first introduced with Windows 2000
  - http://msdn.microsoft.com/en-us/library/ms995355.aspx
- it receives plaintext and returns ciphertext
  - opaque, two methods: *CryptProctedData* and *CryptUnprotectData*
  - does not provide any storage facility
- It's the **key** technology used extensively by Windows

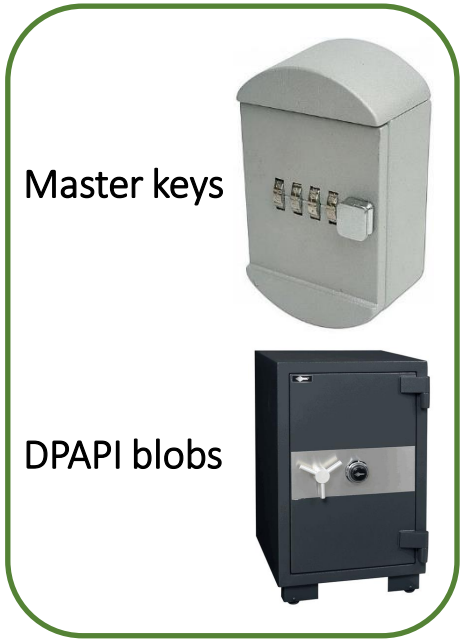
dpapi decryption



- user's password *unlocks* Master keys
- the proper master key *decrypts* the blob



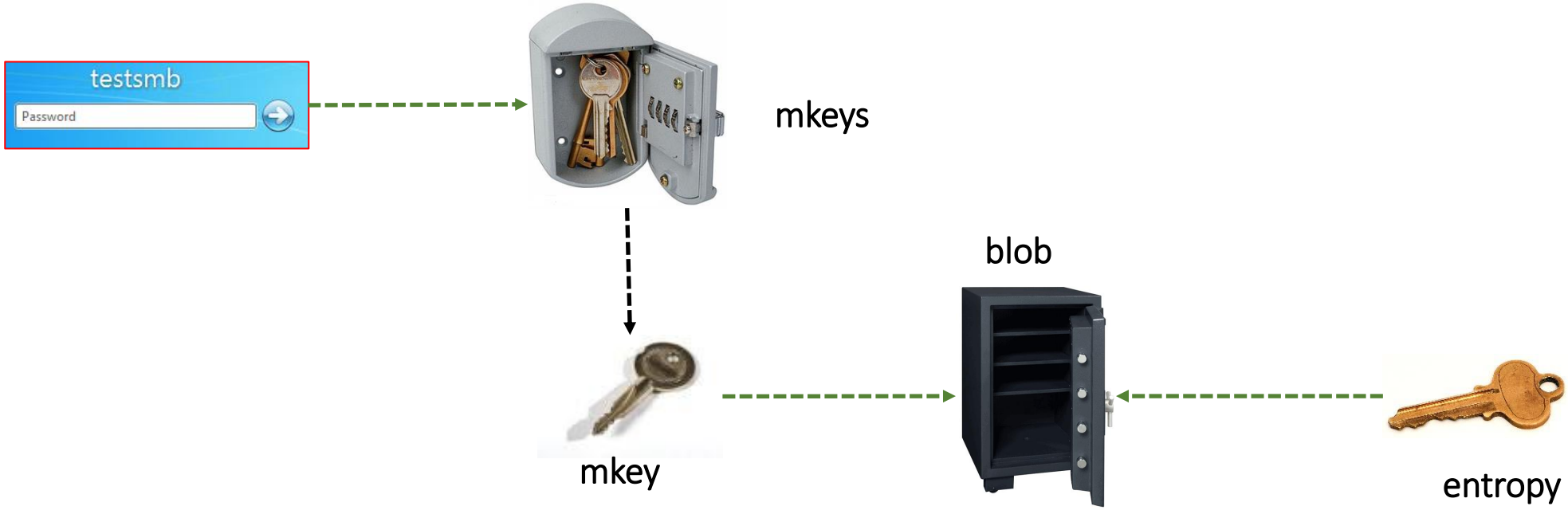
dpapi overview



- **password** should be only in user's brain
  - not always true…
  - the system has its key, which is stored in registry
- **mkeys** are files on disks
  - In proper directories
  - Each *mkey* has its own GUID
- **blobs** can be everywhere
  - DPAPI does not provide any storage facility

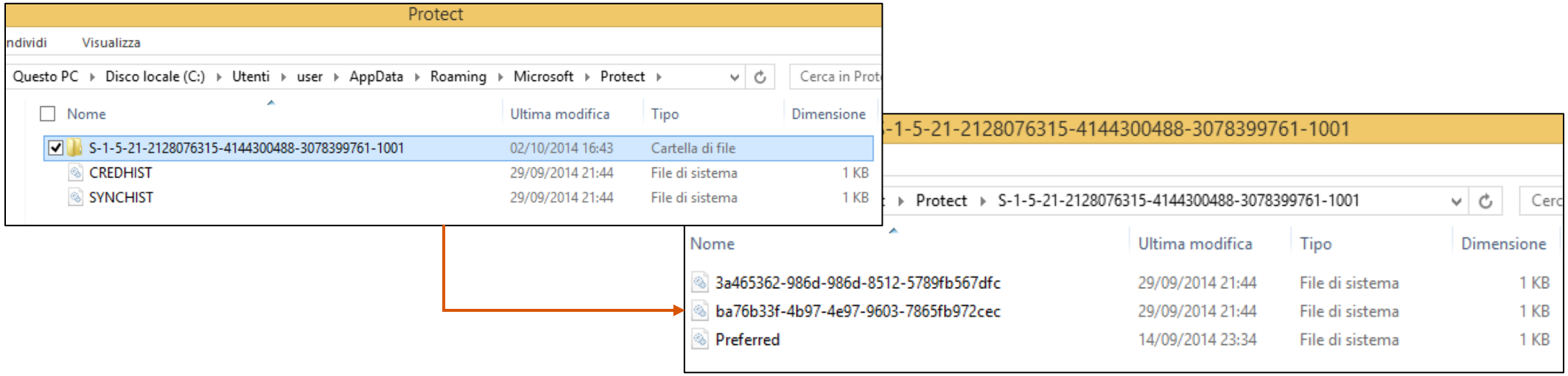
dpapi entropy

- user's password *unlocks* Master keys
- the proper master key **and** the proper **entropy** key *decrypt* the blob



dpapi locations

- User
  - <user profile dir>\AppData\Roaming\Microsoft\Protect
- Local System
  - <windir>\System32\Microsoft\Protect\S-1-5-18\User



dpapi blob

```
00000000: 01 00 00 00 D0 8C 9D DF - 01 15 D1 11 8C 7A 00 C0 |             z  |
00000010: 4F C2 97 EB 01 00 00 00 - B9 3B 02 F9 77 1D CF 4A |O        ;  w  J|
00000020: 9E 88 4E 35 38 31 A7 D4 - 00 00 00 20 3A 00 00 00 |  N581      :   |
00000030: 45 00 6E 00 74 00 65 00 - 72 00 70 00 72 00 69 00 |E n t e r p r i |
00000040: 73 00 65 00 20 00 43 00 - 72 00 65 00 64 00 65 00 |s e   C r e d e |
00000050: 6E 00 74 00 69 00 61 00 - 6C 00 20 00 44 00 61 00 |n t i a l   D a |
00000060: 74 00 61 00 0D 00 0A 00 - 00 00 10 66 00 00 00 01 |t a        f    |
00000070: 00 00 20 00 00 00 A6 0C - D5 B3 E4 F6 6F 0F EA C8 |            o   |
00000080: CC F2 A8 5B 4F C0 79 3F - 7D 80 73 16 90 C1 F8 13 |   [O y?} s     |
00000090: 78 24 50 CE 17 87 00 00 - 00 00 0E 80 00 00 00 02 |x$P             |
000000a0: 00 00 20 00 00 00 31 F4 - 01 B8 C3 D8 87 B3 A1 CA |      1         |
000000b0: 1E 6F 34 23 AB 8A DB 55 - C4 EB 58 4E 5D 9D 9A 07 | o4#   U  XN]   |
000000c0: 8F B9 D2 0E 6F 28 B0 00 - 00 00 AB B9 6A 18 B2 BF |    o(      j   |
000000d0: 07 CC 59 E9 80 2B 14 17 - 7D 4B 79 53 5A C6 B5 B0 |  Y  +  }KySZ   |
000000e0: 17 CC 5A BB 1A A7 8B 5C - B9 D1 6A 78 1C 25 B5 F1 |  Z    \  jx %  |
000000f0: 6B 87 23 17 2E 7F 29 41 - 4A 9F 41 B2 92 98 8E DE |k # . )AJ A     |
00000100: A0 F6 55 AF 82 FD B3 F3 - 03 A6 83 EE 81 38 71 DF |  U          8q |
00000110: 20 13 D7 96 4F 06 A6 43 - 0D 62 5F 7B 0C C4 51 1F |    O  C b_{  Q |
00000120: A1 F1 F5 4A E8 24 02 9F - 2A 76 FF 62 44 FD FD F1 |   J $  *v bD   |
00000130: 3A CB 83 0D 18 05 B2 14 - 9F 1B 04 45 BA DB E5 14 |:          E    |
00000140: 15 63 07 06 52 F0 3E 27 - 36 39 62 7B 50 CB 71 E0 | c  R >'69b{P q |
00000150: A9 E5 94 71 3D 56 3E 6B - 18 57 77 9E 78 E2 F5 35 |   q=V>k Ww x  5|
00000160: DD 6D 54 16 08 BE 0D 1F - 43 7A 0D 00 8C 47 D5 E8 | mT     Cz   G  |
00000170: 83 D7 72 9F 7D 2A 49 13 - DC BE 40 00 00 00 0C ED |  r }*I   @     |
00000180: D8 73 8A F6 50 D8 23 88 - AF 60 3E 41 C3 2A 67 CB | s  P #  `>A *g |
00000190: B9 A8 5B A1 EB 03 37 55 - 03 C5 F9 9D DE D1 37 79 |  [   7U      7y|
000001a0: 7B DF 1D 74 16 CB 55 09 - 16 7A CB 7D 0B 8D FF BD |{  t  U  z }    |
000001b0: 97 B3 DC FB 5D 87 06 E7 - CF 7F C0 2E 29 8F       |    ]      .) |
```

dpapi blob

```
00000000: 01 00 00 00 D0 8C 9D DF - 01 15 D1 11 8C 7A 00 C0 |           z  |
00000010: 4F C2 97 EB 01 00 00 00 - B9 3B 02 F9 77 1D CF 4A |O        ;  w  J|
00000020: 9E 88 4E 35 38 31 A7 D4 - 00 00 00 20 3A 00 00 00 |  N581      :   |
00000030: 45 00 6E 00 74 00 65 00 - 72 00 70 00 72 00 69 00 |E n t e r p r i |
00000040: 73 00 65 00 20 00 43 00 - 72 00 65 00 64 00 65 00 |s e   C r e d e |
00000050: 6E 00 74 00 69 00 61 00 - 6C 00 20 00 44 00 61 00 |n t i a l   D a |
00000060: 74 00 61 00 0D 00 0A 00 - 00 00 10 66 00 00 00 01 |t a        f    |
00000070: 00 00 20 00 00 00 A6 0C - D5 B3 E4 F6 6F 0F EA C8 |            o   |
00000080: CC F2 A8 5B 4F C0 79 3F - 7D 80 73 16 90 C1 F8 13 |   [O y?} s     |
00000090: 78 24 50 CE 17 87 00 00 - 00 00 0E 80 00 00 00 02 |x$P             |
000000a0: 00 00 20 00 00 00 31 F4 - 01 B8 C3 D8 87 B3 A1 CA |      1         |
000000b0: 1E 6F 34 23 AB 8A DB 55 - C4 EB 58 4E 5D 9D 9A 07 | o4#   U  XN]   |
000000c0: 8F B9 D2 0E 6F 28 B0 00 - 00 00 AB B9 6A 18 B2 BF |    o(      j   |
000000d0: 07 CC 59 E9 80 2B 14 17 - 7D 4B 79 53 5A C6 B5 B0 |  Y  +  }KySZ   |
000000e0: 17 CC 5A BB 1A A7 8B 5C - B9 D1 6A 78 1C 25 B5 F1 |  Z    \  jx %  |
000000f0: 6B 87 23 17 2E 7F 29 41 - 4A 9F 41 B2 92 98 8E DE |k # . )AJ A     |
00000100: A0 F6 55 AF 82 FD B3 F3 - 03 A6 83 EE 81 38 71 DF |  U          8q |
00000110: 20 13 D7 96 4F 06 A6 43 - 0D 62 5F 7B 0C C4 51 1F |    O  C b_{  Q |
00000120: A1 F1 F5 4A E8 24 02 9F - 2A 76 FF 62 44 FD FD F1 |   J $  *v bD   |
00000130: 3A CB 83 0D 18 05 B2 14 - 9F 1B 04 45 BA DB E5 14 |:          E    |
00000140: 15 63 07 06 52 F0 3E 27 - 36 39 62 7B 50 CB 71 E0 | c  R >'69b{P q |
00000150: A9 E5 94 71 3D 56 3E 6B - 18 57 77 9E 78 E2 F5 35 |   q=V>k Ww x  5|
00000160: DD 6D 54 16 08 BE 0D 1F - 43 7A 0D 00 8C 47 D5 E8 | mT     Cz   G  |
00000170: 83 D7 72 9F 7D 2A 49 13 - DC BE 40 00 00 00 0C ED |  r }*I   @     |
00000180: D8 73 8A F6 50 D8 23 88 - AF 60 3E 41 C3 2A 67 CB | s  P #  `>A *g |
00000190: B9 A8 5B A1 EB 03 37 55 - 03 C5 F9 9D DE D1 37 79 |  [   7U      7y|
000001a0: 7B DF 1D 74 16 CB 55 09 - 16 7A CB 7D 0B 8D FF BD |{  t  U  z }   |
000001b0: 97 B3 DC FB 5D 87 06 E7 - CF 7F C0 2E 29 8F       |    ]      .) |
```

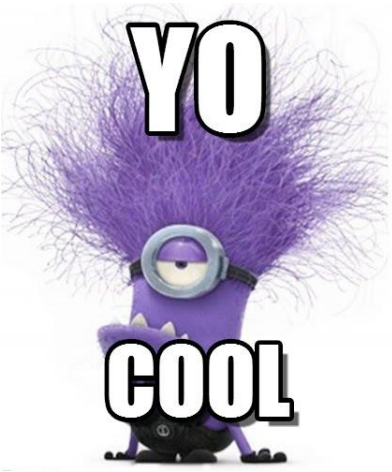
mkey guid

provider guid

Find your blobs!
hexadecimal signature search for provider guid.

blobinfo

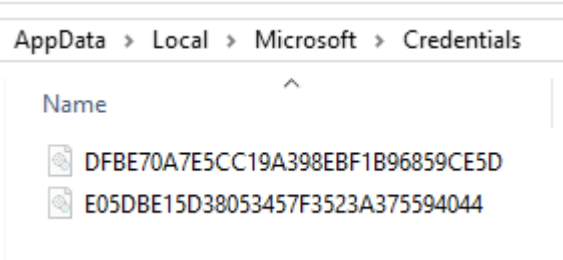
```
dpapilab> blobinfo.py "Enterprise Credential Data"

DPAPI BLOB
        version      = 1
        provider     = df9d8cd0-1501-11d1-8c7a-00c04fc297eb
        mkey         = f9023bb9-1d77-4acf-9e88-4e353831a7d4
        flags        = 0x20000000
        descr        = Enterprise Credential Data
        cipherAlgo   = AES-256 [0x6610]
        hashAlgo     = sha512 [0x800e]
        salt         = a60cd5b3e4f66f0feac8ccf2a85b4fc0793f7d80731690c1f813782450ce1787
        hmac         = 31f401b8c3d887b3a1ca1e6f3423ab8adb55c4eb584e5d9d9a078fb9d20e6f28
        cipher       = abb96a18b2bf07cc59e9802b14177d4b79535ac6b5b017cc5abb1aa78b5cb9d16a781C25b5f16b872
                       3172e7f29414a9f41b292988edea0f655af82fdb3f303a683ee813871df2013d7964f06a6430d625f7
                       b0cc4511fa1f1f54ae824029f2a76ff6244fdfdf13acb830d1805b2149f1b0445badbe514156307065
                       2f03e273639627b50cb71e0a9e594713d563e6b1857779e78e2f535dd6d541608be0d1f437a0d008c4
                       7d5e883d7729f7d2a4913dcbe
        sign         = 0cedd8738af650d82388af603e41c32a67cbb9a85ba1eb03375503c5f99dded137797bdf1d7416cb
                       5509167acb7d0b8dffbd97b3dcfb5d8706e7cf7fc02e298f
```



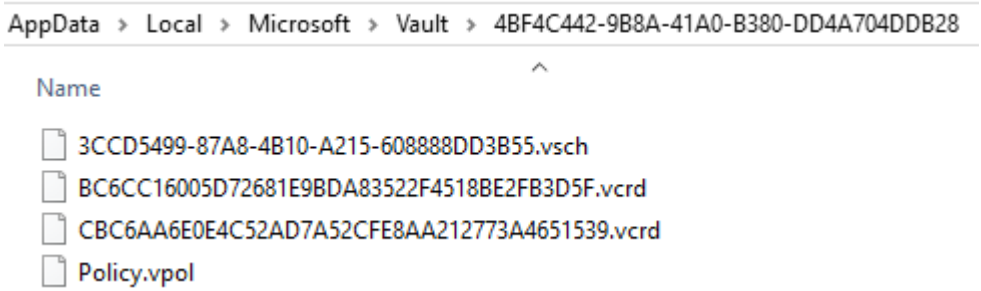
internals

just a bunch of reversing pills

- a **Credentials** folder can contain
  - [0-n] *guid* files



- a **Vault** folder can contain
  - [0-1] Policy.vpol files
  - [0-n] *schema_guid*.vsch files
  - [0-n] *guid*.vcrd files



credential file

```
00000000: 01 00 00 00 BE 01 00 00 - 00 00 00 00 01 00 00 00 |                |
00000010: D0 8C 9D DF 01 15 D1 11 - 8C 7A 00 C0 4F C2 97 EB |         z  O   |
00000020: 01 00 00 00 B9 3B 02 F9 - 77 1D CF 4A 9E 88 4E 35 |     ;  w  J  N5|
00000030: 38 31 A7 D4 00 00 00 20 - 3A 00 00 00 45 00 6E 00 |81      :   E n |
00000040: 74 00 65 00 72 00 70 00 - 72 00 69 00 73 00 65 00 |t e r p r i s e |
00000050: 20 00 43 00 72 00 65 00 - 64 00 65 00 6E 00 74 00 |  C r e d e n t |
00000060: 69 00 61 00 6C 00 20 00 - 44 00 61 00 74 00 61 00 |i a l   D a t a |
00000070: 0D 00 0A 00 00 00 10 66 - 00 00 00 01 00 00 20 00 |       f        |
00000080: 00 00 A6 0C D5 B3 E4 F6 - 6F 0F EA C8 CC F2 A8 5B |        o      [|
00000090: 4F C0 79 3F 7D 80 73 16 - 90 C1 F8 13 78 24 50 CE |O y?} s     x$P |
000000a0: 17 87 00 00 00 00 0E 80 - 00 00 00 02 00 00 20 00 |                |
000000b0: 00 00 31 F4 01 B8 C3 D8 - 87 B3 A1 CA 1E 6F 34 23 |  1          o4#|
000000c0: AB 8A DB 55 C4 EB 58 4E - 5D 9D 9A 07 8F B9 D2 0E |   U  XN]       |
000000d0: 6F 28 B0 00 00 00 AB B9 - 6A 18 B2 BF 07 CC 59 E9 |o(      j     Y |
000000e0: 80 2B 14 17 7D 4B 79 53 - 5A C6 B5 B0 17 CC 5A BB | +  }KySZ     Z |
000000f0: 1A A7 8B 5C B9 D1 6A 78 - 1C 25 B5 F1 6B 87 23 17 |   \  jx %  k # |
00000100: 2E 7F 29 41 4A 9F 41 B2 - 92 98 8E DE A0 F6 55 AF |. )AJ A       U |
00000110: 82 FD B3 F3 03 A6 83 EE - 81 38 71 DF 20 13 D7 96 |         8q     |
00000120: 4F 06 A6 43 0D 62 5F 7B - 0C C4 51 1F A1 F1 F5 4A |O  C b_{  Q    J|
00000130: E8 24 02 9F 2A 76 FF 62 - 44 FD FD F1 3A CB 83 0D | $  *v bD   :   |
00000140: 18 05 B2 14 9F 1B 04 45 - BA DB E5 14 15 63 07 06 |       E     c  |
00000150: 52 F0 3E 27 36 39 62 7B - 50 CB 71 E0 A9 E5 94 71 |R >'69b{P q    q|
00000160: 3D 56 3E 6B 18 57 77 9E - 78 E2 F5 35 DD 6D 54 16 |=V>k Ww x  5 mT |
00000170: 08 BE 0D 1F 43 7A 0D 00 - 8C 47 D5 E8 83 D7 72 9F |    Cz   G    r |
00000180: 7D 2A 49 13 DC BE 40 00 - 00 00 0C ED D8 73 8A F6 |}*I   @      s  |
00000190: 50 D8 23 88 AF 60 3E 41 - C3 2A 67 CB B9 A8 5B A1 |P #  `>A *g   [ |
000001a0: EB 03 37 55 03 C5 F9 9D - DE D1 37 79 7B DF 1D 74 |  7U      7y{  t|
000001b0: 16 CB 55 09 16 7A CB 7D - 0B 8D FF BD 97 B3 DC FB |  U  z }        |
000001c0: 5D 87 06 E7 CF 7F C0 2E - 29 8F                   |]      .) |
```

credential file

dpapi blob length

```
00000000: 01 00 00 00 BE 01 00 00 - 00 00 00 00 01 00 00 00 |            |
00000010: D0 8C 9D DF 01 15 D1 11 - 8C 7A 00 C0 4F C2 97 EB |         z  O   |
00000020: 01 00 00 00 B9 3B 02 F9 - 77 1D CF 4A 9E 88 4E 35 |     ;  w  J  N5|
00000030: 38 31 A7 D4 00 00 00 20 - 3A 00 00 00 45 00 6E 00 |81      :   E n |
00000040: 74 00 65 00 72 00 70 00 - 72 00 69 00 73 00 65 00 |t e r p r i s e |
00000050: 20 00 43 00 72 00 65 00 - 64 00 65 00 6E 00 74 00 |  C r e d e n t |
00000060: 69 00 61 00 6C 00 20 00 - 44 00 61 00 74 00 61 00 |i a l   D a t a |
00000070: 0D 00 0A 00 00 00 10 66 - 00 00 00 01 00 00 20 00 |       f        |
00000080: 00 00 A6 0C D5 B3 E4 F6 - 6F 0F EA C8 CC F2 A8 5B |        o      [|
00000090: 4F C0 79 3F 7D 80 73 16 - 90 C1 F8 13 78 24 50 CE |O y?} s     x$P |
000000a0: 17 87 00 00 00 00 0E 80 - 00 00 00 02 00 00 20 00 |                |
000000b0: 00 00 31 F4 01 B8 C3 D8 - 87 B3 A1 CA 1E 6F 34 23 |  1          o4#|
000000c0: AB 8A DB 55 C4 EB 58 4E - 5D 9D 9A 07 8F B9 D2 0E |   U  XN]       |
000000d0: 6F 28 B0 00 00 00 AB B9 - 6A 18 B2 BF 07 CC 59 E9 |o(      j     Y |
000000e0: 80 2B 14 17 7D 4B 79 53 - 5A C6 B5 B0 17 CC 5A BB | +  }KySZ     Z |
000000f0: 1A A7 8B 5C B9 D1 6A 78 - 1C 25 B5 F1 6B 87 23 17 |   \  jx %  k # |
00000100: 2E 7F 29 41 4A 9F 41 B2 - 92 98 8E DE A0 F6 55 AF |. )AJ A       U |
00000110: 82 FD B3 F3 03 A6 83 EE - 81 38 71 DF 20 13 D7 96 |         8q     |
00000120: 4F 06 A6 43 0D 62 5F 7B - 0C C4 51 1F A1 F1 F5 4A |O  C b_{  Q    J|
00000130: E8 24 02 9F 2A 76 FF 62 - 44 FD FD F1 3A CB 83 0D | $  *v bD   :   |
00000140: 18 05 B2 14 9F 1B 04 45 - BA DB E5 14 15 63 07 06 |       E     c  |
00000150: 52 F0 3E 27 36 39 62 7B - 50 CB 71 E0 A9 E5 94 71 |R >'69b{P q    q|
00000160: 3D 56 3E 6B 18 57 77 9E - 78 E2 F5 35 DD 6D 54 16 |=V>k Ww x  5 mT |
00000170: 08 BE 0D 1F 43 7A 0D 00 - 8C 47 D5 E8 83 D7 72 9F |    Cz   G    r |
00000180: 7D 2A 49 13 DC BE 40 00 - 00 00 0C ED D8 73 8A F6 |}*I   @      s  |
00000190: 50 D8 23 88 AF 60 3E 41 - C3 2A 67 CB B9 A8 5B A1 |P #  `>A *g   [ |
000001a0: EB 03 37 55 03 C5 F9 9D - DE D1 37 79 7B DF 1D 74 |  7U      7y{  t|
000001b0: 16 CB 55 09 16 7A CB 7D - 0B 8D FF BD 97 B3 DC FB |  U  z }        |
000001c0: 5D 87 06 E7 CF 7F C0 2E - 29 8F                   |]      .) |
```

dpapi blob

policy.vpol

```
00000000: 01 00 00 00 42 C4 F4 4B - 8A 9B A0 41 B3 80 DD 4A |    B  K   A   J|
00000010: 70 4D DB 28 20 00 00 00 - 57 00 65 00 62 00 20 00 |pM (    W e b   |
00000020: 43 00 72 00 65 00 64 00 - 65 00 6E 00 74 00 69 00 |C r e d e n t i |
00000030: 61 00 6C 00 73 00 00 00 - 01 00 00 00 00 00 00 00 |a l s           |
00000040: 01 00 00 00 68 01 00 00 - 0B DA 73 DD 83 FD 12 47 |    h     s    G|
00000050: AF 8B D1 53 C7 10 C6 B9 - 0B DA 73 DD 83 FD 12 47 |   S      s    G|
00000060: AF 8B D1 53 C7 10 C6 B9 - 44 01 00 00 01 00 00 00 |   S    D       |
00000070: D0 8C 9D DF 01 15 D1 11 - 8C 7A 00 C0 4F C2 97 EB |         z  O   |
00000080: 01 00 00 00 9E 5F CA 42 - 0B F4 29 41 BC 43 84 E5 |     _ B  )A C  |
00000090: 8D 82 4F 66 00 00 00 20 - 00 00 00 00 10 66 00 00 |  Of         f  |
000000a0: 00 01 00 00 20 00 00 00 - AD DE C4 5D BA C7 32 92 |           ]  2 |
000000b0: 58 E6 5D D4 6D 2C 27 63 - A6 C8 36 F3 7A 67 30 64 |X ] m,'c  6 zg0d|
000000c0: 69 78 2C 5B 1A 30 1E A5 - 00 00 00 00 0E 80 00 00 |ix,[ 0          |
000000d0: 00 02 00 00 20 00 00 00 - 5C 2E CF E4 E3 C4 74 76 |        \.    tv|
000000e0: 35 94 35 02 0B 53 37 C3 - 88 AC 3C 51 10 E7 A4 4B |5 5  S7   <Q   K|
000000f0: 05 03 67 B8 B9 5D 74 87 - 70 00 00 00 1D 86 E6 36 |  g  ]t p      6|
00000100: B0 A5 45 B2 24 32 15 D5 - EC BF D8 42 E7 C6 DC B3 |  E $2     B    |
00000110: C4 78 A4 9E 69 26 24 FC - E5 40 E5 BB E7 74 24 F8 | x  i&$  @   t$ |
00000120: E9 8E 50 44 5C 65 45 39 - 8A 55 B2 10 93 AD 12 8A |  PD\eE9 U      |
00000130: EC E9 CE D7 19 02 3E 94 - C4 F0 96 5C 71 2A 77 84 |      >    \q*w |
00000140: 37 CF 1C 41 10 50 E5 48 - BE C9 B7 AF BE C7 BA F3 |7  A P H        |
00000150: 79 D5 C2 E7 49 96 0B 09 - 1F 39 A0 5C 5E D7 B2 7D |y   I    9 \^  }|
00000160: C8 5D CA 08 A8 07 45 DD - 59 FA 11 6D 40 00 00 00 | ]    E Y  m@   |
00000170: 06 3C BF DE 52 E7 41 76 - E1 DB C9 ED BC 58 D1 1C | <  R Av     X  |
00000180: 5F 7D 85 00 5F A8 48 F2 - 45 93 73 CF 03 78 46 50 |_}  _ H E s  xFP|
00000190: 30 E5 D8 2E D9 1E D5 25 - 7C 72 3B 10 39 EA 03 EA |0  .   %|r; 9   |
000001a0: 88 00 40 49 C9 1D EB 19 - EC 6B 7F 7F 35 D1 99 A5 |  @I     k  5   |
000001b0: 00 00 00 00                                       |    |
```

policy.vpol

vault guid

description

dpapi blob

```
00000000: 01 00 00 00 42 C4 F4 4B - 8A 9B A0 41 B3 80 DD 4A |    B  K   A   J|
00000010: 70 4D DB 28 20 00 00 00 - 57 00 65 00 62 00 20 00 |pM (    W e b   |
00000020: 43 00 72 00 65 00 64 00 - 65 00 6E 00 74 00 69 00 |C r e d e n t i |
00000030: 61 00 6C 00 73 00 00 00 - 01 00 00 00 00 00 00 00 |a l s           |
00000040: 01 00 00 00 68 01 00 00 - 0B DA 73 DD 83 FD 12 47 |    h     s    G|
00000050: AF 8B D1 53 C7 10 C6 B9 - 0B DA 73 DD 83 FD 12 47 |   S      s    G|
00000060: AF 8B D1 53 C7 10 C6 B9 - 44 01 00 00 01 00 00 00 |   S    D        |
00000070: D0 8C 9D DF 01 15 D1 11 - 8C 7A 00 C0 4F C2 97 EB |         z  O   |
00000080: 01 00 00 00 9E 5F CA 42 - 0B F4 29 41 BC 43 84 E5 |      _ B  )A C  |
00000090: 8D 82 4F 66 00 00 00 20 - 00 00 00 00 10 66 00 00 |  Of         f  |
000000a0: 00 01 00 00 20 00 00 00 - AD DE C4 5D BA C7 32 92 |           ]  2 |
000000b0: 58 E6 5D D4 6D 2C 27 63 - A6 C8 36 F3 7A 67 30 64 |X ] m,'c  6 zg0d|
000000c0: 69 78 2C 5B 1A 30 1E A5 - 00 00 00 00 0E 80 00 00 |ix,[ 0          |
000000d0: 00 02 00 00 20 00 00 00 - 5C 2E CF E4 E3 C4 74 76 |        \.    tv|
000000e0: 35 94 35 02 0B 53 37 C3 - 88 AC 3C 51 10 E7 A4 4B |5 5  S7   <Q   K|
000000f0: 05 03 67 B8 B9 5D 74 87 - 70 00 00 00 1D 86 E6 36 |  g  ]t p      6|
00000100: B0 A5 45 B2 24 32 15 D5 - EC BF D8 42 E7 C6 DC B3 |  E $2     B    |
00000110: C4 78 A4 9E 69 26 24 FC - E5 40 E5 BB E7 74 24 F8 | x  i&$  @   t$ |
00000120: E9 8E 50 44 5C 65 45 39 - 8A 55 B2 10 93 AD 12 8A |  PD\eE9 U       |
00000130: EC E9 CE D7 19 02 3E 94 - C4 F0 96 5C 71 2A 77 84 |      >    \q*w  |
00000140: 37 CF 1C 41 10 50 E5 48 - BE C9 B7 AF BE C7 BA F3 |7  A P H         |
00000150: 79 D5 C2 E7 49 96 0B 09 - 1F 39 A0 5C 5E D7 B2 7D |y   I    9 \^   }|
00000160: C8 5D CA 08 A8 07 45 DD - 59 FA 11 6D 40 00 00 00 | ]    E Y  m@    |
00000170: 06 3C BF DE 52 E7 41 76 - E1 DB C9 ED BC 58 D1 1C | <  R Av     X  |
00000180: 5F 7D 85 00 5F A8 48 F2 - 45 93 73 CF 03 78 46 50 |_}  _ H E s  xFP|
00000190: 30 E5 D8 2E D9 1E D5 25 - 7C 72 3B 10 39 EA 03 EA |0  .   %|r; 9   |
000001a0: 88 00 40 49 C9 1D EB 19 - EC 6B 7F 7F 35 D1 99 A5 |  @I     k  5   |
000001b0: 00 00 00 00                                       |    |
```

policy.vpol decrypted

Bcrypt.h
#define BCRYPT_KEY_DATA_BLOB_MAGIC
0x4d42444b //Key Data Blob Magic (KDBM)

AES128 key

```
00000000: 24 00 00 00 01 00 00 00 - 02 00 00 00 4B 44 42 4D |$           KDBM|
00000010: 01 00 00 00 10 00 00 00 - 95 55 C5 D8 D7 33 C0 79 |         U   3 y|
00000020: 0E 39 8D EC FA 0F F7 3C - 34 00 00 00 01 00 00 00 | 9     <4       |
00000030: 01 00 00 00 4B 44 42 4D - 01 00 00 00 20 00 00 00 |    KDBM        |
00000040: 19 31 1B 75 C2 FB BF 97 - EB 84 35 ED 40 81 57 83 | 1 u      5 @ W |
00000050: B2 C4 04 B8 DE 9E 9C 32 - 3A D7 2F 4F E4 B3 88 06 |       2: /O    |
```

AES256 key

vcrd files

```
00000000: 99 54 CD 3C A8 87 10 4B - A2 15 60 88 88 DD 3B 55 |T <   K   `   ;U|
00000010: 04 00 00 00 2E 38 E5 FA - 4C 4D D0 01 FF FF FF FF |    .8  LM      |
00000020: 00 02 00 00 24 00 00 00 - 49 00 6E 00 74 00 65 00 |    $   I n t e |
00000030: 72 00 6E 00 65 00 74 00 - 20 00 45 00 78 00 70 00 |r n e t   E x p |
00000040: 6C 00 6F 00 72 00 65 00 - 72 00 00 00 30 00 00 00 |l o r e r   0   |
00000050: 01 00 00 00 80 00 00 00 - 00 00 00 00 02 00 00 00 |                |
00000060: B5 00 00 00 00 00 00 00 - 03 00 00 00 EA 00 00 00 |                |
00000070: 00 00 00 00 64 00 00 00 - 00 01 00 00 00 00 00 00 |    d           |
00000080: 01 00 00 00 02 00 00 00 - 07 00 00 00 0A 00 00 00 |                |
00000090: 21 00 00 00 00 52 ED E9 - 05 24 4A 05 DA 6F C4 C4 |!    R   $J  o  |
000000a0: DF 9A 81 EA 77 8E D6 35 - C2 FB 7F BD A3 AC C2 CD |    w  5        |
000000b0: F6 43 94 D6 97 02 00 00 - 00 02 00 00 00 07 00 00 | C              |
000000c0: 00 0A 00 00 00 21 00 00 - 00 00 03 CB 01 FD 50 02 |     !        P |
000000d0: AB 04 3F A4 07 64 6E DA - BC A4 E6 C5 C8 F9 DC AF |  ?  dn         |
000000e0: 1E D7 1B AB 41 4D 70 F8 - 10 39 03 00 00 00 00 00 |    AMp  9      |
000000f0: 00 00 07 00 00 00 0A 00 - 00 00 00 00 00 00 01 00 |                |
00000100: 64 00 00 00 00 00 00 00 - 08 00 00 00 0A 00 00 00 |d               |
00000110: 00 00 00 00 D5 00 00 00 - 01 10 00 00 00 3A 6F 91 |             :o |
00000120: 84 F4 4D E2 24 00 F3 66 - E8 62 1D 57 60 B6 C1 13 |  M $  f b W`   |
00000130: A6 F6 C3 11 E4 48 45 21 - 91 CA 05 0F 06 97 0C 81 |     HE!        |
00000140: 82 23 38 2C [.......................................................]| ...............................|
000001fd;
```

last update

«*description*»

schema (vsch) guid

attribute array length

attribute array
dword:id
dword:pointer
dword:unknown

vcrd files attributes' data

```
[…]
00000080: 01 00 00 00 02 00 00 00 - 07 00 00 00 0A 00 00 00 |                |
00000090: 21 00 00 00 00 52 ED E9 - 05 24 4A 05 DA 6F C4 C4 |!    R   $J  o  |
000000a0: DF 9A 81 EA 77 8E D6 35 - C2 FB 7F BD A3 AC C2 CD |    w  5        |
000000b0: F6 43 94 D6 97 02 00 00 - 00 02 00 00 00 07 00 00 | C              |
000000c0: 00 0A 00 00 00 21 00 00 - 00 00 03 CB 01 FD 50 02 |     !        P |
000000d0: AB 04 3F A4 07 64 6E DA - BC A4 E6 C5 C8 F9 DC AF |  ?  dn         |
000000e0: 1E D7 1B AB 41 4D 70 F8 - 10 39 03 00 00 00 00 00 |    AMp  9      |
000000f0: 00 00 07 00 00 00 0A 00 - 00 00 00 00 00 00 01 00 |                |
00000100: 64 00 00 00 00 00 00 00 - 08 00 00 00 0A 00 00 00 |d               |
00000110: 00 00 00 00 D5 00 00 00 - 01 10 00 00 00 3A 6F 91 |            :o  |
00000120: 84 F4 4D E2 24 00 F3 66 - E8 62 1D 57 60 B6 C1 13 |  M $  f b W`   |
00000130: A6 F6 C3 11 E4 48 45 21 - 91 CA 05 0F 06 97 0C 81 |     HE!        |
00000140: 82 23 38 2C 6A A3 52 D3 - 43 B9 74 04 C8 4E DB C0 | #8,j R C t  N  |
00000150: DB 8A CF 32 43 52 58 2E - 0F F3 32 40 98 F4 4C 97 |   2CRX.  2@  L |
00000160: D4 DA D8 FF 8C BB AE A7 - 5A F8 0A 24 52 C5 54 B9 |        Z  $R T |
00000170: 1F 98 EE 97 7D A4 FC 8E - 1A E2 09 FA BE BA 2A D4 |    }         * |
00000180: 61 F1 12 39 00 E2 32 5F - EE 21 51 78 D0 0C 6F 06 |a  9  2_ !Qx  o |
00000190: 92 1D 3F 20 05 5E 57 B2 - E7 BB FA 6D EC 41 C3 7B |  ?  ^W    m A {|
000001a0: 92 CC 41 6E 16 B1 52 F4 - 01 8F 8F 4B EF 82 BA AA |  An  R    K   |
000001b0: ED EC FF FE 4A 46 0F F1 - C1 16 A1 AC 29 68 45 AD |    JF      )hE |
000001c0: 7D 9A 41 66 C0 B9 9E BE - 0F BA 16 09 51 19 6F E8 |} Af        Q o |
000001d0: EC E2 3E 43 28 5E 5B AB - FB F8 69 B4 FD A2 18 5B |  >C(^[   i    [|
000001e0: F5 26 D2 01 21 A5 12 E8 - D2 25 D1 AA 19 01 00 00 | &  !    %      |
000001f0: 00 00 00 00 00 08 00 00 - 00 00 00 00 00         |              |
000001fd;
```

decrypt with AES128 key

IV length + IV

decrypt with AES256 key using the provided IV

vsch file

schema (vsch) guid

schema name

```
00000000: 01 00 00 00 99 54 CD 3C - A8 87 10 4B A2 15 60 88 |     T <   K  `  |
00000010: 88 DD 3B 55 00 00 00 00 - 0A 00 00 00 40 00 00 00 |  ;U        @    |
00000020: 57 00 69 00 6E 00 64 00 - 6F 00 77 00 73 00 20 00 |W i n d o w s    |
00000030: 57 00 65 00 62 00 20 00 - 50 00 61 00 73 00 73 00 |W e b   P a s s |
00000040: 77 00 6F 00 72 00 64 00 - 20 00 43 00 72 00 65 00 |w o r d   C r e |
00000050: 64 00 65 00 6E 00 74 00 - 69 00 61 00 6C 00 00 00 |d e n t i a l    |
00000060: 01 00 00 00 07 00 00 00 - 04 00 00 00 00 00 00 00 |                 |
00000070: 02 00 00 00 07 00 00 00 - 04 00 00 00 00 00 00 00 |                 |
00000080: 03 00 00 00 07 00 00 00 - 00 00 00 00 00 00 00 00 |                 |
00000090: 07 00 64 00 00 00 08 00 - 00 00 08 00 00 00 00 00 |  d              |
000000a0: 00 00 65 00 00 00 08 00 - 00 00 08 00 00 00 00 00 |  e              |
000000b0: 00 00 66 00 00 00 08 00 - 00 00 08 00 00 00 00 00 |  f              |
000000c0: 00 00 67 00 00 00 08 00 - 00 00 08 00 00 00 00 00 |  g              |
000000d0: 00 00 68 00 00 00 08 00 - 00 00 08 00 00 00 00 00 |  h              |
000000e0: 00 00 69 00 00 00 08 00 - 00 00 08 00 00 00 00 00 |  i              |
000000f0: 00 00 6A 00 00 00 08 00 - 00 00 08 00 00 00 00 00 |  j              |
00000100: 00 00 00 00 00 00       -                         |      |
```

```
vaultcmd /listschema

Global Schemas

Credential schema: Windows Secure Note
Schema guid: 2F1A6504-0641-44CF-8BB5-3612D865F2E5

Credential schema: Windows Web Password Credential
Schema guid: 3CCD5499-87A8-4B10-A215-608888DD3B55

Credential schema: Windows Credential Picker Protector
Schema guid: 154E23D0-C644-4E6F-8CE6-5069272F999F

Currently loaded credentials schemas:

Vault: Web Credentials
Vault Guid:4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Credential schema: Windows Web Password Credential
Schema guid: 3CCD5499-87A8-4B10-A215-608888DD3B55

Vault: Windows Credentials
Vault Guid:77BC582B-F0A6-4E15-4E80-61736B6F3B29

Credential schema:
Windows Domain Certificate Credential
Schema guid: E69D7838-91B5-4FC9-89D5-230D4D4CC2BC

Credential schema: Windows Domain Password Credential
Schema guid: 3E0E35BE-1B77-43E7-B873-AED901B6275B

Credential schema: Windows Extended Credential
Schema guid: 3C886FF3-2669-4AA2-A8FB-3F6759A77548
```

internals conclusions

- **credentials** file are simple dpapi blobs
  - they can be nested…
- **vaults** files (aka **vcrd** ones)
  - decrypt **policy.vpol** to obtain AES keys
    - policy.vpol are dpapi blobs
  - decrypt **attributes** inside **vcrd** files
    - using the proper AES key
  - print out using **vsch** schema files
    - …

arsenal

open source power

dpapi and vaults

dpapi level

- MK and BLOBs decryption

Vault level

- Credentials and Vaults decryption

dpapick

- simply <u>the</u> open source tool for DPAPI decryption
  - Python, can be installed by *pip*

- written by **Jean-Michel Picod**
  - ***Reversing DPAPI and Stealing Windows Secrets Offline***
    by Jean-Michel Picod and Elie Bursztein, BlackHat 2010

    - last year Jean-Michel integrated my patches for **Windows7 – 8.1** support
    - **Windows 10** is supported too
    - **live ID** will be added soon…

https://bitbucket.org/jmichel/dpapick

dpapilab

- my own *dpapi-oriented* **lab**

- you can find there
  - **Credentials** decryption with **creddec.py**
  - **Vaults** decryption with **vaultdec.py**
  - some un-ordered dpapi utilities

- Python source code
  - dpapick as “kernel”
  - Python **construct** to describe and declare structure used

https://github.com/dfirfpi/dpapilab

we need a password…

- **not an easy task**
- user's password is **the key**
- dictionary and rainbow tables attacks on ntlm
- hybrid attack
- anyway, there is something to do before…

the password

the stronghold

the trivial leak

- well-known since years
  - almost 7 years…
- The LSA Secret ***DefaultPassword*** OldVal keeps the Windows installation password
  - *"uh ok, I must insert my new Windows password, let me choose the best unbreakable one…"*

the trivial leak exposed

```
dpapilab> lsasecrets.py --security=SECURITY --system=SYSTEM --hex

NL$KM            CurrVal    1f8fe9331af… […]
…
DPAPI_SYSTEM     CurrVal    01000000ebf6828452f6ca25ba362fcd6c763688707087cd1c14651723bfeb3a0e96
                            2531368adf9544ded978
…
DefaultPassword  CurrVal
DefaultPassword  CupdTime   2012-09-11 09:49:36
DefaultPassword  OldVal     74006800690073004F006E006500490073005400 6F006F0047006F006F0064003400
                            75004200750074004400 6F006E002700740043006800650061007400 2100
DefaultPassword  OupdTime   2012-09-11 09:41:00
```

the trivial leak exposed

```
dpapilab> lsasecrets.py --security=SECURITY --system=SYSTEM
                        --secret=DefaultPassword

t h i s O n e I s T o o G o o d 4 u B u t D o n ' t C h e a t !
```

Windows 7

Windows 8

Windows 10

2013-07-11
Xavier de Carné de Carnavalet.

VENDOR CONTACT TIMELINE
2013-05-20: Bug found
2013-06-14: Contacted Microsoft Security Response Center
2013-06-14: Reply from Microsoft SRC: "*the behavior you are reporting is not something that we consider a security vulnerability*"

https://madiba.encs.concordia.ca/~x_decarn/docs/bug_report_password_caching.pdf

lovely logon picture (or pin)

Windows 8

- Windows introduced the possibility to login with
  - a pincode
  - a picture shape
- Windows 8-8.1 has a major issue
  - the mandatory “real” password is kept in a **system vault**
  - %WINDIR%\system32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
- Credits to Passcape for having discovered it
  - http://www.passcape.com/index.php?section=blog&cmd=details&id=27

logon picture/pin exposed

```
dpapilab> vaultdec.py

          --security=X:\Windows\System32\config\SECURITY
                                                          System DPAPI key
          --system=X:\Windows\System32\config\SYSTEM

          --masterkey=X:\Windows\System32\Microsoft\Protect\S-1-5-18\User   System mkeys

          X:\Windows\System32\config\systemprofile\AppData\Local\Microsof
          t\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28                      System Vault
```

logon picture/pin exposed

Windows 8

```
dpapilab> vaultdec.py […]

--------------------------------------------------------------------------------
Working on: 025AA2D2228C0DA34CAE4A82455024C169D7FF0C.vcrd

Attribute: 1 (vault_schema_simple) […]
Attribute: 2 (vault_schema_simple) […]
Attribute: 3 (vault_schema_simple) […]

Attribute: 64 (vault_schema_pin)
sid: S-1-5-21-2128076315-4144300488-3078399761-1001
resource: PIN Logon Vault Resource
password: fuffa
pin: 1357

Attribute: dead0001 (vault_schema_simple) […]
```

mimikatz

The most complete solution for memory dumps

mimikatz plugin

- wdigest
- Windows Vista, Windows [x86 – x64]

mimikatz plugin

- wdigest, livessp
- primary credentials, dpapi
- Windows XP up to Windows 8.1 [x86 – x64]

Benjamin Delpy aka **gentil_kiwi** first discovered the presence of users' **passwords** in the **lsass** process.

his open source tool has **tons** of features every *infosec* guy should know.

mimikatz can decrypt **Credentials** and **Vaults** too, besided showing memory cached values.

https://github.com/gentilkiwi/mimikatz

mimilib vs Windows 8.1

Windows 8 **live account**

```
Authentication Id : 0 ; 149932 (00000000:000249ac)
Session           : Interactive from 1
User Name         : mr
Domain            : WIN-FAOEGS8OE65
SID               : S-1-5-21-2128076315-4144300488-3078399761-100
        msv :
         [00000003] Primary
         * Username : mr[redacted]@gmail.com
         * Domain   : MicrosoftAccount
         * NTLM     : 07162731aca7[redacted]
         * SHA1     : 643658b7f815[redacted]5a4209a98
        tspkg : KO
        wdigest :
         * Username : mr[redacted]@gmail.com
         * Domain   : MicrosoftAccount
         * Password : (null)
        livessp :
         * Username : mr.[redacted]@gmail.com
         * Domain   : ps:password
         * Password : Fuffa123
        kerberos :
         * Username : mr.[redacted]@gmail.com
         * Domain   : MicrosoftAccount
         * Password : (null)
        ssp :
        masterkey :
         [00000000]
         * GUID :   {f82650c8-92d5-4d08-8473-90f86895dd4d}
         * Time :   03/10/2014 08:30:27
         * Key :    034a2654fa14dac6ebfcc5532fb5b2968b1df1d0586694d
        credman :
```

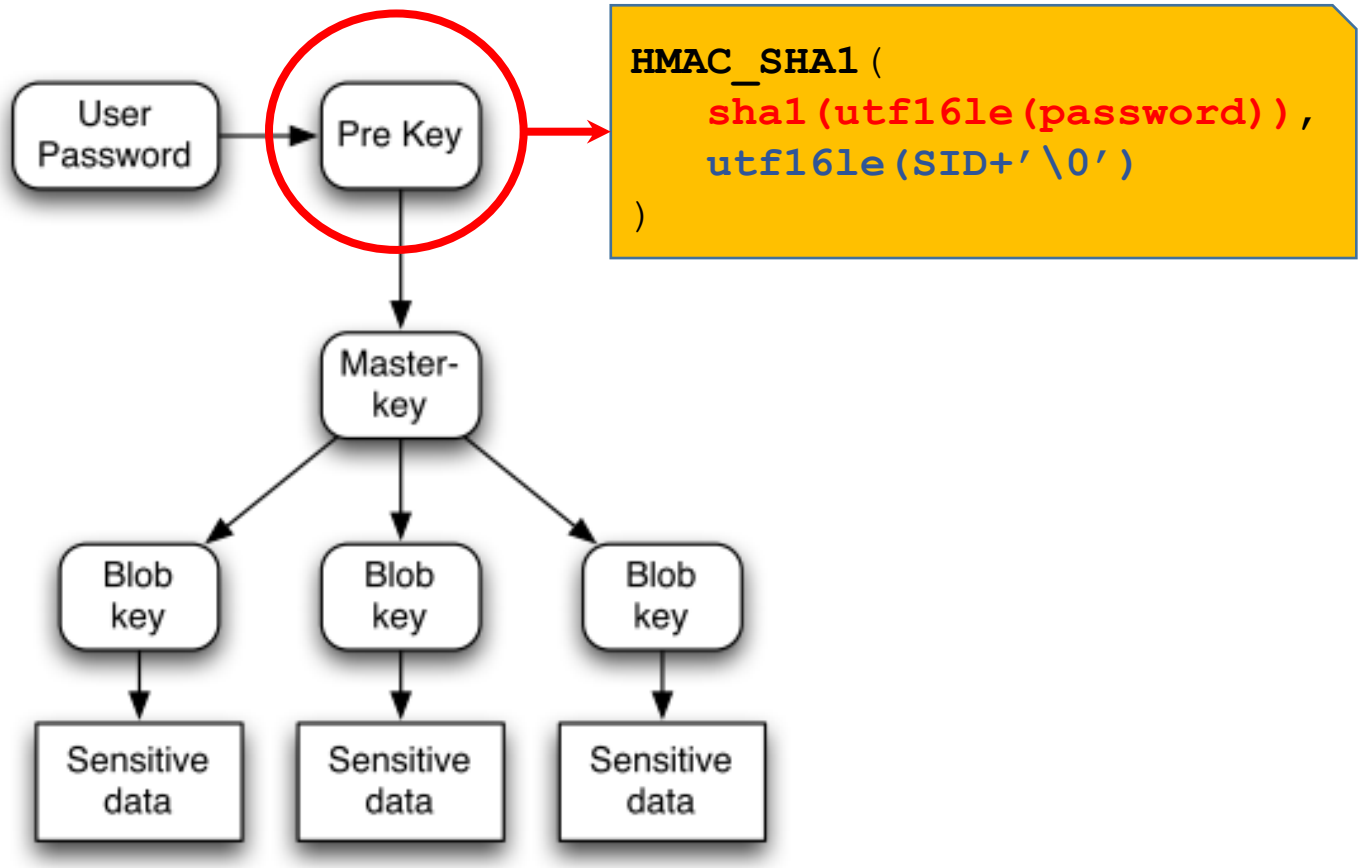
Windows 8 **local account**

```
Authentication Id : 0 ; 144828 (00000000:000235bc)
Session           : Interactive from 1
User Name         : user
Domain            : WIN-FAOEGS8OE65
SID               : S-1-5-21-2128076315-4144300488-3078399761-1001
        msv :
         [00000003] Primary
         * Username : user
         * Domain   : WIN-FAOEGS8OE65
         * NTLM     : 3b13f1ba6f8e68ab82c83eb6702e6d40
         * SHA1     : 74b87ba1e12734f71fe4737990e2c420bd145bf4
         [00010000] CredentialKeys
         * NTLM     : 3b13f1ba6f8e68ab82c83eb6702e6d40
         * SHA1     : 74b87ba1e12734f71fe4737990e2c420bd145bf4
        tspkg : KO
        wdigest :
         * Username : user
         * Domain   : WIN-FAOEGS8OE65
         * Password : (null)
        livessp : KO
        kerberos :
         * Username : user
         * Domain   : WIN-FAOEGS8OE65
         * Password : (null)
        ssp :
        masterkey :
        credman :
```

rekall mimikatz

```
        LUID              Type       Sess        SID          Module   Info        Domain           User         SType                Secret
-------------------- ---------------  --  -------------------- ------- ------- --------------- --------------- --------- --------------------------------
00000000:00047e22    Interactive      1    S-1-5-21-2421538757- msv     Primary win7cf          cf              NTLM      3b13f1ba6f8e68ab82c83eb6702e6d40
                                           1605280464-234451782
                                           0-1000
00000000:00047e22    Interactive      1    S-1-5-21-2421538757- msv     Primary win7cf          cf              SHA1      74b87ba1e12734f71fe4737990e2c420
                                           1605280464-234451782                                                   bd145bf4
                                           0-1000
00000000:00047e22    Interactive      1    S-1-5-21-2421538757- msv     Credent                                 NTLM      3b13f1ba6f8e68ab82c83eb6702e6d40
                                           1605280464-234451782         ialKeys
                                           0-1000
00000000:00047e22    Interactive      1    S-1-5-21-2421538757- msv     Credent                                 SHA1      74b87ba1e12734f71fe4737990e2c420
                                           1605280464-234451782         ialKeys                                            bd145bf4
                                           0-1000
00000000:00047df2    Interactive      1    S-1-5-21-2421538757- msv     Credent                                 NTLM      3b13f1ba6f8e68ab82c83eb6702e6d40
                                           1605280464-234451782         ialKeys
                                           0-1000
00000000:00047df2    Interactive      1    S-1-5-21-2421538757- msv     Credent                                 SHA1      74b87ba1e12734f71fe4737990e2c420
                                           1605280464-234451782         ialKeys                                            bd145bf4
                                           0-1000
00000000:00047df2    Interactive      1    S-1-5-21-2421538757- msv     Primary win7cf          cf              NTLM      3b13f1ba6f8e68ab82c83eb6702e6d40
                                           1605280464-234451782
                                           0-1000
00000000:00047df2    Interactive      1    S-1-5-21-2421538757- msv     Primary win7cf          cf              SHA1      74b87ba1e12734f71fe4737990e2c420
                                           1605280464-234451782                                                   bd145bf4
                                           0-1000
00000000:00047e22    Interactive      1    S-1-5-21-2421538757- wdigest         win7cf          cf              password  f u f f a
                                           1605280464-234451782
                                           0-1000
00000000:00047df2    Interactive      1    S-1-5-21-2421538757- wdigest         win7cf          cf              password  f u f f a
                                           1605280464-234451782
                                           0-1000
00000000:000003e5    Service          0    S-1-5-19             wdigest                                         password  -
00000000:000003e4    Service          0    S-1-5-20             wdigest         WORKGROUP       WIN7CF$         password  -
00000000:000003e7    UNKNOWN (0)      0    S-1-5-18             wdigest         WORKGROUP       WIN7CF$         password  -
WARNING:root:livessp not initialized, skipping it.
00000000:000003e7    UNKNOWN (0)      0    S-1-5-18             lsasrv                                          masterkey eda6f7b253017470d990bf6ae19ae1f4
                                                                                                                           1789bd2f4d6bc5c18431cc407a05598d
                                                                                                                           f32ce8e0aff9c1ebdaa0903b1b8de558
                                                                                                                           eac67087610533826e5b48e0f250241e
00000000:000003e7    UNKNOWN (0)      0    S-1-5-18             lsasrv                                          masterkey 3e9d7f32f2e57933ead318d075efc823
                                                                                                                           25697d87d992b626a20abb5f0ffba6f0
                                                                                                                           73d282a837b6fa058ecff36039aa944e
                                                                                                                           04b3dfb666ebace44aad6bff8789ca43
00000000:00047e22    Interactive      1    S-1-5-21-2421538757- lsasrv                                          masterkey f2f4d48b37042284310abfd62be9ab88
                                           1605280464-234451782                                                           97b7426622690e9cf5114ccadd4ff024
                                           0-1000                                                                         f7197267ee8b2d60bc68a405e5dce0d2
                                                                                                                           4a042f610bcd6903f46d49750644668f
```

sha1, at least




```
HMAC_SHA1(
    sha1(utf16le(password)),
    utf16le(SID+'\0')
)
```

1click cracking

- If attacking target fails…
- attack anything that can be outright decrypted
  - *1click cracking*
- backups, VMs, system *secrets*, etc
  - whatever can provide a password or a clue
- For example, WiFi password are SYSTEM DPAPI BLOBs
  - XML files in \ProgramData\Microsoft\WwanSvc\Profiles

Windows 7

Windows 8

Windows 10

wifi exposed

```
dpapilab> winwifidec.py --security=SECURITY --system=SYSTEM
                        --wdir=[DATA]\ProgramData\MICROSOFT\Wlansvc\Profiles\Interfaces\{C03B6CCB-…20}\
```

```
{3219475E-D1C2-11E3-9C44-00A0C6000001}
Wifi:WFD_GROUP_OWNER_PROFILE Password: f0rZaGenoa!

{A028DED4-860D-11E2-9BCF-00A0C6000000}
Wifi:rnsys Password: OMG-NoSecurity@Work:(
Wifi:iperboleguest Password: hackinbo01
Wifi:NETGEAR-NEW Password:Bu3n0sD1asAT0d0s
Wifi:FPIW Password: ThisIs*Not*MyHomeWifiPassword…
```

```
[redacted]_img_>icat -o 4194304 Dump4.bin 10769
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>rnsys</name>
        <SSIDConfig>
                <SSID>
                        <hex>726E737973</hex>
                        <name>rnsys</name>
                </SSID>
                <nonBroadcast>true</nonBroadcast>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>manual</connectionMode>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPA2PSK</authentication>
                                <encryption>AES</encryption>
                                <useOneX>false</useOneX>
                        </authEncryption>
                        <sharedKey>
                                <keyType>passPhrase</keyType>
                                <protected>true</protected>
                                <keyMaterial>01000000D08C9DDF0115D1118C7A00C04FC297EB010000002F27E01
C6BBE5A49ACD47F8D3FC433730000000020000000000010660000001000020000000602D260939050D136AF6E4ECE150696
BCC215240DDB497581458ED840174BA2500000000E8000000002000020000009421F74CE119752FA9AA000E2A5581747A3
6AC7A0495BA6D670A57128FFE67692000000A4BC7341ACE198CD6F010B0235B6F31C5C11960AE5AA67FFFEF1E1814AEF4FD
F400000009AD945C05C0B97F4551777FE68B5D8E40A1D30BDEF7AB4A0FB9E0885B48B3CE63F5728E460F7E37F58A2EEE3C53
DCCB483BAB644B031B2D0921617C504E532A2</keyMaterial>
                        </sharedKey>
                </security>
        </MSM>
</WLANProfile>
```

credential activity

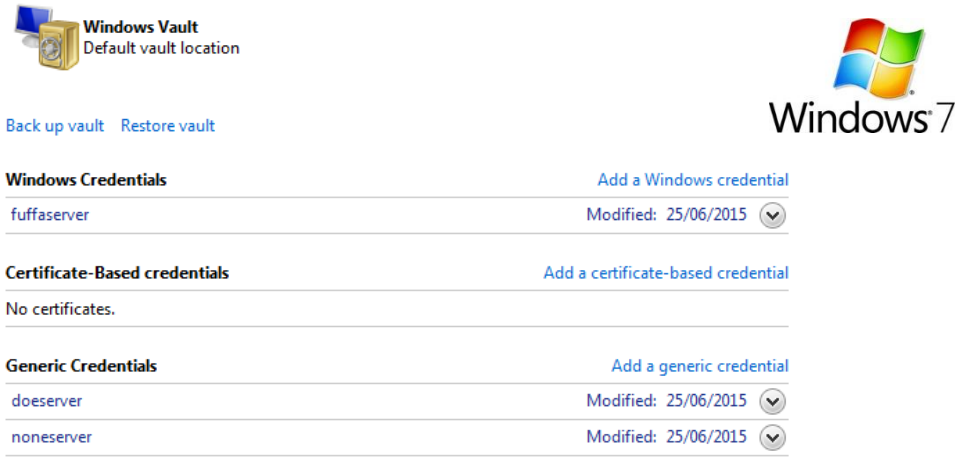
just a couple of examples

windows credentials

```
dpapilab> creddec.py

    --sid=S-1-5-21-2421538757-1605280464-2344517820-1000

    --masterkey=c:\Users\cf\AppData\Roaming\Microsoft\Protect\S-1-5-21-2421538757-1605280464-
                                                                    2344517820-1000

    --password=fuffa

      c:\Users\cf\AppData\Local\Microsoft\Credentials\2D080F6A5F429AB28A285E65B2CAB26A

      c:\Users\cf\AppData\Local\Microsoft\Credentials\833C2EF1F037027E409C9B8DBD908DF2

      c:\Users\cf\AppData\Local\Microsoft\Credentials\A199FA18351CD904F5210DFD7C18CE02
```

windows credentials exposed

```
2D080F6A5F429AB28A285E65B2CAB26A
last_update = '2015-06-25T17:47:03+00:00'
domain = u'Domain:target=fuffaserver'
unk_string1 = u''
unk_string2 u''
unk_string3 u''
username = u`fuffauser'
password = u`fuffapassword'
```




```
9CEE7E22AED680E028CB97193B5860E9
last_update = '2015-06-25T17:47:59+00:00'
domain = u'LegacyGeneric:target=doeserver'
unk_string1 = u''
unk_string2 u''
unk_string3 u''
username = u`doeuser'
password = u`doepassword'
```

```
A199FA18351CD904F5210DFD7C18CE02
last_update = '2015-06-25T18:23:12+00:00'
domain = u'Domain:target=credentials.FOO.gov'
unk_string1 = u''
unk_string2 u''
unk_string3 u''
username = u'WIN7CF\\username'
password = u`******************`
```

double cheeseburger credential

Windows 10

```
dpapilab> creddec.py

    --sid=S-1-5-21-1648103230-915194270-5828639865-1001

    --masterkey=c:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-1648103230-915194270-5828639865-1001

    --pwdhash=a0273792cb879a4ea0c2fd719dc15fe259a385e3

    --sysmkdir=C:\Windows\System32\Microsoft\Protect\S-1-5-18\User

    --security=sysreg\SECURITY

    --system=sysreg\SYSTEM

      c:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
```

you too curious… fake data there

double cheeseburger credential exposed

```
Container:
    domain = u'WindowsLive:target=virtualapp/didlogical'
    unk_string1 = u''
    unk_string2 u'PersistedCredential'
    unk_string3 u''
    username = u'02mrsvuptceu'
    password = u''

----------------------------------------

('<AuthInfo><UserName>02mrsvuptceu</UserName>
<UserPUID>00275EFE2EC418C0</UserPUID>
…
```

double cheeseburger credential

```
('<AuthInfo>
<UserName>02mrsvuptceu</UserName>
<UserPUID>00275EFE2EC418C0</UserPUID>
<CredProperties>
    <keypurposes><ps:KeyPurposes
xmlns:ps="http://schemas.microsoft.com/Passport/SoapServices/PPCRL"></ps:KeyPurposes></keypurposes>
<ip>94.36.56.146</ip>
    <authmembername>02mrsvuptceu@passport.com</authmembername>
</CredProperties>
<AuthToken>
    <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#" Id="devicesoftware" Type=[…]>
        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"></EncryptionMethod>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>http://Passport.NET/STS</ds:KeyName></ds:KeyInfo>
        <CipherData><CipherValue>Cm9aG1+DmmquOs8a0GD[...]</CipherValue></CipherData></EncryptedData>
</AuthToken>
<SessionKey>AgAAAJf5l4Mnb6E7 [...] AAAAAAAAAA==</SessionKey>
<SessionKeyType>3</SessionKeyType>
<CreatedTime>2015-10-01T19:37:56</CreatedTime>
<ExpiredTime>2015-10-15T19:37:55</ExpiredTime>
</AuthInfo>', 0)
```

winphone

decrypting «mobile» vaults

winphone test scenario

- Windows Phone OS is… just **Windows**
- so we can do the same, as decrypting **vaults**
- Test scenario with Windows 8.1
  - phone reset
  - Windows Live account
  - added some **email** account syncs
  - …
  - **physical acquisition** after every step

Windows 8

In need of kernel debugging

«*Kernel-mode debugging is supported only when the target phone is running a non-retail version of Windows. To create and install non-retail images of Windows Phone, you need the Windows Phone Kit, which is available only to registered partners. For information about becoming a partner, see Register to be a Windows Phone OEM.*»

many users… many vaults

- *email-related* vaults were created into **WPCOMMSSERVICES** profile
- one of the «*system-users*»
- for time reasons we'll face only it
- question: **password**?
  - PIN code protection == screensaver

Name	Size	Type	Date Modified
ACCESSLIB_SVC	1	Directory	03/08/2015 10.56...
CAPTURESVCGRP	1	Directory	03/08/2015 10.54...
DefApps	1	Directory	03/08/2015 10.54...
Default	1	Directory	03/08/2015 10.54...
FEEDBACKSVC	1	Directory	03/08/2015 10.56...
IPOVERUSBGROUP	1	Directory	03/08/2015 10.54...
NCSDSVC	1	Directory	03/08/2015 10.54...
NGPSVC	1	Directory	03/08/2015 10.54...
NOKIARCSESVC	1	Directory	03/08/2015 10.56...
NSGEXTUTI	1	Directory	03/08/2015 10.56...
OEMSVCGROUP	1	Directory	03/08/2015 10.54...
OEMSVCHOST	1	Directory	03/08/2015 10.56...
PSREGSERVICE	1	Directory	03/08/2015 10.56...
Public	1	Directory	03/08/2015 10.53...
QCSHUTDOWNSVC	1	Directory	03/08/2015 10.54...
SENSOR_SERVICE	1	Directory	03/08/2015 10.56...
System	1	Directory	03/08/2015 10.54...
TELREPSVC	1	Directory	03/08/2015 10.56...
WLANCOUNTRYSVC	1	Directory	03/08/2015 10.54...
WPCOMMSSERVICES	1	Directory	03/08/2015 10.54...
WPCRITICAL	1	Directory	03/08/2015 10.54...
WPNETWORK	1	Directory	03/08/2015 10.54...
WPNETWORKDRM	1	Directory	03/08/2015 10.56...
WPNETWORKPII	1	Directory	03/08/2015 10.56...
WPNONETWORK	1	Directory	03/08/2015 10.54...

many users… many passwords

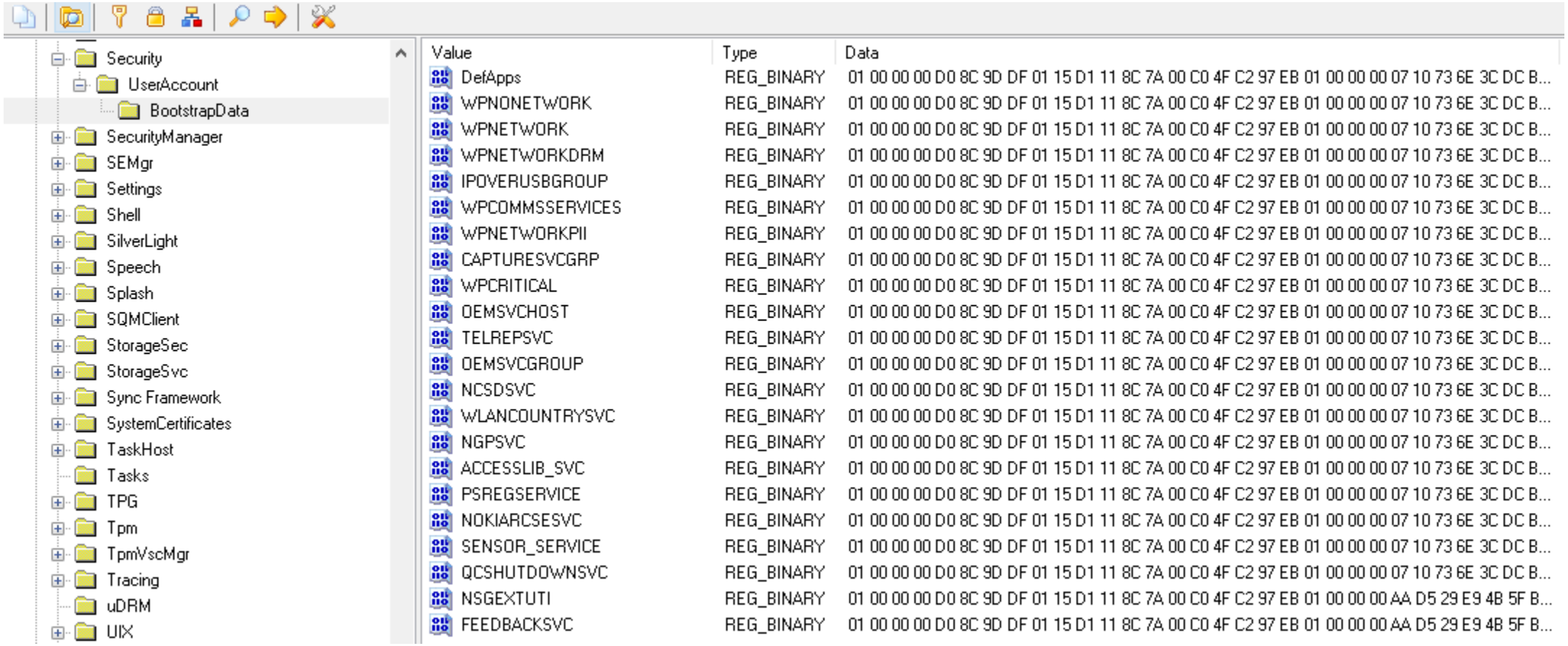
just_a_shell> pycreddump\pwdump.py SYSTEM SAM

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f194e99a9050a026b9445425b4e72c44:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:30f60b1fe0fd69e1eb179d480d54f0d9:::
DefApps:2781:aad3b435b51404eeaad3b435b51404ee:a33a6392a476adfe34294b2029f14708:::
WPNONETWORK:2782:aad3b435b51404eeaad3b435b51404ee:67c041a3ddcc8eeaca176b32a068d97e:::
WPNETWORK:2783:aad3b435b51404eeaad3b435b51404ee:83106e7f2e2921e35197328d8e11eea8:::
WPNETWORKDRM:2784:aad3b435b51404eeaad3b435b51404ee:9fae0b63cd1ba7a85ab0365df786f49a:::
IPOVERUSBGROUP:2786:aad3b435b51404eeaad3b435b51404ee:e0b0fac51f921e5127e12776bee0197e:::
WPCOMMSSERVICES:2788:aad3b435b51404eeaad3b435b51404ee:daa06a338359eed6fc28ddb773369e9f:::
WPNETWORKPII:2790:aad3b435b51404eeaad3b435b51404ee:68981b3c606c20b092366c2c34a8685d:::
CAPTURESVCGRP:2791:aad3b435b51404eeaad3b435b51404ee:ee0cab2b8d7316cc1d109bcc6511533c:::
WPCRITICAL:2792:aad3b435b51404eeaad3b435b51404ee:5fce1c3e7e5b1803a424b514521e1ccb:::
OEMSVCHOST:2793:aad3b435b51404eeaad3b435b51404ee:e6d325755d21dcaab124a9bd4957676e:::
TELREPSVC:2794:aad3b435b51404eeaad3b435b51404ee:dcbcde33eda70369566bf2b021497631:::
OEMSVCGROUP:2795:aad3b435b51404eeaad3b435b51404ee:7550da005cceb21c5ba5c8ecad2ed377:::
NCSDSVC:2796:aad3b435b51404eeaad3b435b51404ee:58686d487dd2ca7503cfe6fd17233d88:::
WLANCOUNTRYSVC:2797:aad3b435b51404eeaad3b435b51404ee:7c72dd4bf4f75fb9570c2058e97f3b4b:::
NGPSVC:2798:aad3b435b51404eeaad3b435b51404ee:1b739d6d3f099293b434c52e193d86b5:::
ACCESSLIB_SVC:2799:aad3b435b51404eeaad3b435b51404ee:23145899db9c5a665fc00f3c3cdf636f:::
PSREGSERVICE:2800:aad3b435b51404eeaad3b435b51404ee:8f88aebc4bfd2b6a59ed7406dd41094a:::
NOKIARCSESVC:2801:aad3b435b51404eeaad3b435b51404ee:076d30c9b00c86ab93e761b0d96070ff:::
SENSOR_SERVICE:2802:aad3b435b51404eeaad3b435b51404ee:c182e91ca1361bd390630676ff25e02a:::
QCSHUTDOWNSVC:2804:aad3b435b51404eeaad3b435b51404ee:35007aa28a7b5a86ff38aa485491a272:::
NSGEXTUTI:2805:aad3b435b51404eeaad3b435b51404ee:deb3282673fbb24ec84fbee636a52450:::
FEEDBACKSVC:2806:aad3b435b51404eeaad3b435b51404ee:27da8da6e58d6fde3de258182f96f2d8:::
```

cracking?

follow the white rabbit

SOFTWARE\Microsoft\Security\UserAccount\BootstrapData



- Security
  - UserAccount
    - BootstrapData
  - SecurityManager
  - SEMgr
  - Settings
  - Shell
  - SilverLight
  - Speech
  - Splash
  - SQMClient
  - StorageSec
  - StorageSvc
  - Sync Framework
  - SystemCertificates
  - TaskHost
  - Tasks
  - TPG
  - Tpm
  - TpmVscMgr
  - Tracing
  - uDRM
  - UIX

Value	Type	Data
DefApps	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
WPNONETWORK	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
WPNETWORK	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
WPNETWORKDRM	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
IPOVERUSBGROUP	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
WPCOMMSSERVICES	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
WPNETWORKPII	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
CAPTURESVCGRP	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
WPCRITICAL	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
OEMSVCHOST	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
TELREPSVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
OEMSVCGROUP	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
NCSDSVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
WLANCOUNTRYSVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
NGPSVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
ACCESSLIB_SVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
PSREGSERVICE	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
NOKIARCSESVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
SENSOR_SERVICE	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
QCSHUTDOWNSVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 07 10 73 6E 3C DC B...
NSGEXTUTI	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 AA D5 29 E9 4B 5F B...
FEEDBACKSVC	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 AA D5 29 E9 4B 5F B...

DefApps… blob

```
00000000: 01 00 00 00 D0 8C 9D DF - 01 15 D1 11 8C 7A 00 C0 |           z  |
00000010: 4F C2 97 EB 01 00 00 00 - 07 10 73 6E 3C DC BE 45 |O         sn<  E|
00000020: B3 41 88 ED EF A5 EE 16 - 00 00 00 00 02 00 00 00 | A            |
00000030: 00 00 10 66 00 00 00 01 - 00 00 20 00 00 00 64 AD |   f          d |
00000040: 7E FA F8 21 12 90 20 F7 - A2 BA A1 65 D7 12 F3 22 |~  !       e   "|
00000050: 0F EA 15 54 A7 12 00 9E - D2 4D 0C CB D4 2A 00 00 |   T     M   *  |
00000060: 00 00 0E 80 00 00 00 02 - 00 00 20 00 00 00 B2 A7 |                |
00000070: BE 9A 00 88 47 68 92 98 - 9C D2 45 B2 B3 90 A4 EA |    Gh    E     |
00000080: 6F 71 63 1E 2E FD 18 18 - 9F 82 53 3C 0B B7 10 02 |oqc .     S<    |
00000090: 00 00 F6 89 1B DB 4C 9B - EF 96 87 97 57 8F 76 4A |      L     W vJ|
000000a0: FD E5 A0 85 E2 D7 1F 57 - 25 A3 CF 0A 40 3C 3C 03 |       W%   @<< |
000000b0: 4A 04 DC C7 2D F4 7B E8 - 9B A8 76 BE 76 28 E8 A2 |J   - {   v v(  |
000000c0: 86 45 7A 99 B2 6B DC 5C - 8A 77 B8 C4 05 5C 5D 43 | Ez  k \ w   \]C|
000000d0: 94 65 AD 45 5D 8B D5 78 - CE 20 E9 62 0B 7E BF 83 | e E]  x   b ~  |
000000e0: BB E2 FD FD 05 97 94 5B - 0B 32 59 30 93 DF 4B 8A |       [ 2Y0  K |
000000f0: ED 04 6E EC 5F 3A 61 E6 - 21 05 B6 8D EB E7 8A 88 |  n _:a !       |
00000100: F4 9A BC 3A CF 41 1A A1 - 7A A1 E3 F6 4D 4A 60 0F |   : A  z   MJ` |
00000110: 03 EC 99 87 F8 43 50 F5 - 1B DA DD 09 B0 61 6C 84 |     CP      al |
00000120: CF 85 FF E8 B0 1B BB 30 - 23 A5 2F 09 3F D7 FE F4 |       0# / ?   |
00000130: 47 3A 98 04 15 6E 1D ED - 0C 41 35 49 F2 62 33 9D |G:   n   A5I b3 |
00000140: 98 D1 54 84 A8 DF BA 70 - 4C E0 8B 68 E9 75 7D 42 |  T    pL  h u}B|
00000150: 63 D4 32 C9 E3 E2 F5 DA - BE DC 34 DB 07 6B D1 69 |c 2       4  k i|
00000160: 33 D6 00 70 0B 05 C7 4C - C1 57 67 77 BD B9 19 ED |3  p   L Wgw    |
00000170: 60 32 BB 2B 77 6A 8A 84 - BC E7 06 66 D7 6D 98 3B |`2 +wj     f m ;|
00000180: 5D CC 0A FA F2 32 26 17 - 87 5A 37 8C 8C 73 EB 77 |]    2&  Z7  s w|
00000190: 7D 84 E2 53 A7 BD 6F FD - FC 4D 24 A5 E0 3F 79 3A |}  S  o  M$  ?y:|
000001a0: 20 B6 F9 70 90 B0 BF 8C - 02 6C CF 49 5D 41 7F D0 |   p     l I]A  |
```

mkey guid

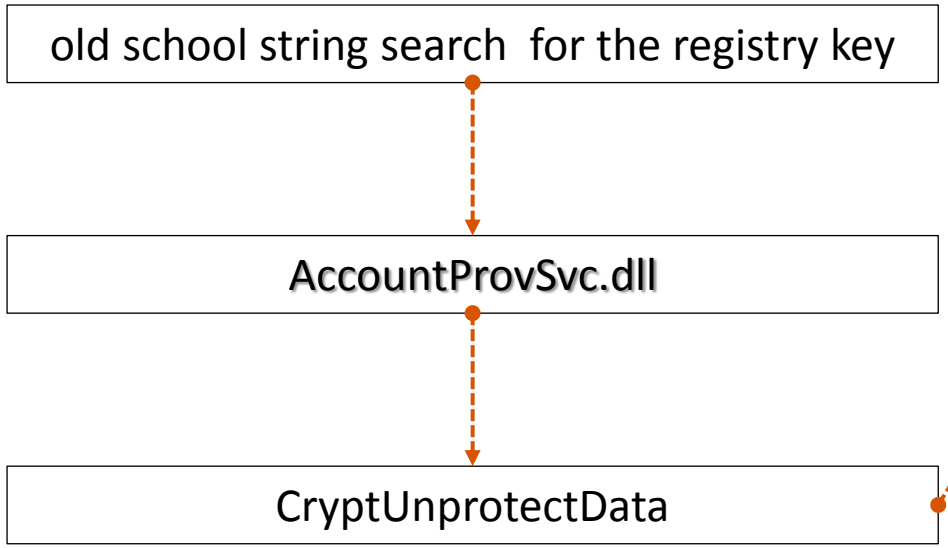
provider guid

trying to decrypt user's blob…

```
dpapilab> blobdec.py
                    --security=SECURITY --system=SYSTEM --masterkey=sysmk

                    bootstrap_DefApps.blob
```

FAIL!

entropy?




```
.data:1001C054 unk_1001C054    DCB 0x62 ; b
.data:1001C054
.data:1001C055                 DCB 0x6B ; k
.data:1001C056                 DCB 0xED ; Ý
.data:1001C057                 DCB 0xCB ; -
.data:1001C058                 DCB 0xCA ; -
.data:1001C059                 DCB    2
.data:1001C05A                 DCB 0x5E ; ^
.data:1001C05B                 DCB 0x41 ; A
.data:1001C05C                 DCB 0x84 ; ä
.data:1001C05D                 DCB 0x7E ; ~
.data:1001C05E                 DCB 0x33 ; 3
.data:1001C05F                 DCB 0x93 ; ô
.data:1001C060                 DCB 0x36 ; 6
.data:1001C061                 DCB 0x9C ; £
.data:1001C062                 DCB 0x2E ; .
.data:1001C063                 DCB 0x5E ; ^
```

decrypting user's blob

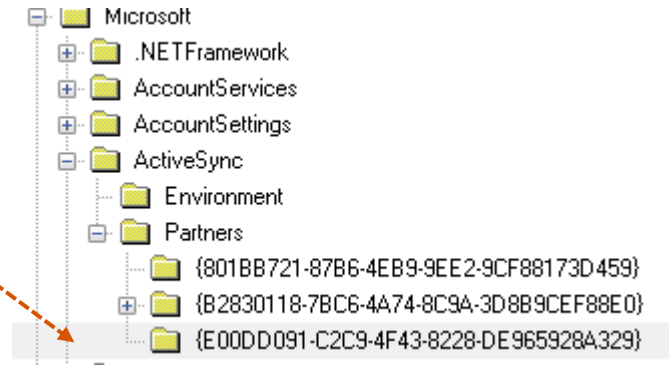
```
dpapilab> blobdec.py
                    --security=SECURITY --system=SYSTEM --masterkey=sysmk

                    --entropy_hex=626BEDCBCA025E41847E3393369C2E5E

                    bootstrap_DefApps.blob


DefApps password
----------------
E6056E45B3425B7BAB7E328971D8570DC0215D6821657AE0C3F6DD6F8059E3C283838A5CFAA30A2F7547EE12F766ADDFE
3F03D22FAE3DCDA36BA37ECED8807B7C5015E02FB4EF6160754C5ADEB1D1B4E292FED8419D986C3EE8A08901C85A34ABB
35F40A770CB31493383602C898B9352884195021BBDFD026F452CBA22B2E6F
```

going for vaults

```
dpapilab> vaultdec.py

    --sid=S-1-5-21-2702878673-795188819-444038987-2788

    --masterkey=\Users\WPCOMMSSERVICES\AppData\Roaming\Microsoft\Protect\S-1-5-21-2421538757-
                1605280464-2344517820-1000

    --password=E91889F98E8A68703ABFC68464B16A1373BB6501192F9D68A5C87C41CF43561852502650735EF84ED
               27AF308AAD9E08C031B5FC21C3DDC9C978222D83FC3308498C2AE0528A38EB086841E2743DE1BCEC18
               FCEDB0775DEA869BF98DEFCE6B5B58A58B58275F42BDA15049DCD9AA3953782E4CD4109CB22795311
               ADBF8E2ABAD1

      \Users\WPCOMMSSERVICES\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
```

mail vaults exposed (1)

```
Working on: 2DAF2FE224AF306A198BA169B1534ADCC618B47B.vcrd

Attribute: 1 […]
Attribute: 2 […]

Attribute: 3 (vault_schema_activesync)
identity: ActiveSyncCredentialDefaultUser
resource: SyncPassword{E00DD091-C2C9-4F43-8228-DE965928A329}MailIncoming
authenticator: WhatCouldPossiblyGoWrong?
```



mail vaults exposed (2)

resource: SyncPassword
{**E00DD091-C2C9-4F43-8228-E965928A329**}
MailIncoming

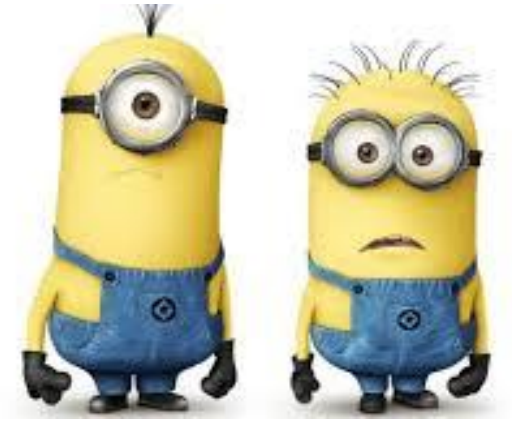
SOFTWARE HIVE
Microsoft**ActiveSync**\Partners

Value	Type	Data
AccountAutoConfig	REG_DWORD	0x00000001
AccountCreateTime	REG_BINARY	AB B8 06 EE E8 CD D0 01
AccountSettingsChanged	REG_DWORD	0x00000001
AccountType	REG_SZ	Email
AccountVersion	REG_DWORD	0x00000012
AttemptedSyncCount	REG_DWORD	0x00000002
AttentionRequiredToastSent	REG_DWORD	0x00000000
Email	REG_SZ	[redacted]@icloud.com
Engine	REG_SZ	{D277DF13-EB33-47E1-A3B9-0AC04B1F24F4}
Icon	REG_SZ	res://UIXMobileAssets{ScreenResolution}!%s.genericmail.png
InServerSettingsVerified	REG_DWORD	0x00000001
InteractiveSyncCount	REG_DWORD	0x00000002
IsPushImapSupported	REG_DWORD	0x00000000
IsSMTPError	REG_DWORD	0x00000001
LastInboundSyncAttempt	REG_BINARY	00 88 DD 06 E9 CD D0 01
LastInboundSyncResult	REG_DWORD	0x00000000
LastInboundSyncSuccess	REG_BINARY	00 88 DD 06 E9 CD D0 01
LastSMTPSyncAttempt	REG_BINARY	80 E3 1D FF E8 CD D0 01
LastSMTPSyncResult	REG_DWORD	0x00000000
LastSMTPSyncSuccess	REG_BINARY	80 E3 1D FF E8 CD D0 01
LastSyncAttempt	REG_BINARY	00 88 DD 06 E9 CD D0 01
LastSyncResult	REG_DWORD	0x00000000
LastSyncSuccess	REG_BINARY	00 88 DD 06 E9 CD D0 01
Name	REG_SZ	Icloud
OtherMailSyncPeriod	REG_DWORD	0x0000001E
ScheduledSyncPeriod	REG_DWORD	0x80000078
Server	REG_SZ	imap.mail.me.com:993:1
StoreId	REG_DWORD	0x0000000A
StoreType	REG_DWORD	0x00000006
SuccessfulSyncCount	REG_DWORD	0x00000002
UserInputServerSettings	REG_DWORD	0x00000000

mail vaults exposed (3)

```
Working on: DB580D5ADA46907C4D7218A754491C55CF9C3342.vcrd

Attribute: 3 (vault_schema_activesync)
identity: ActiveSyncCredentialDefaultUser
resource: OAuthRefreshToken{801BB721-87B6-4EB9-9EE2-9CF88173D459}OAuth
authenticator: 1/UyGV1eG2Q7FfabcdEF6nb3dFgr354htJ6K-mgaj2gw

--------------

Working on: FE912C0BD34AD8BC6C00C8E879B2490495AF937E.vcrd

Attribute: 3 (vault_schema_activesync)
identity: ActiveSyncCredentialDefaultUser
resource: SyncPassword{801BB721-87B6-4EB9-9EE2-9CF88173D459}MailIncoming
authenticator: ya29.xBFGoPazVskbtY_HqmExc3PXmVbYhXrYLd3ldzfryQcP65p4CerTGTEVLe_BjqnGHe_
```

Value	Type	Data
AccountAutoConfig	REG_DWORD	0x00000001
AccountCreateTime	REG_BINARY	0D CC 16 22 E8 CD D0 01
AccountSettingsChanged	REG_DWORD	0x00000001
AccountType	REG_SZ	Gmail
AccountVersion	REG_DWORD	0x00000012
AttemptedSyncCount	REG_DWORD	0x00000004
AttentionRequiredToastSent	REG_DWORD	0x00000000
AuthenticationType	REG_DWORD	0x00000001
Email	REG_SZ	[redacted]@gmail.com



ReVaulted

suddenly… conclusions!

Thank you!