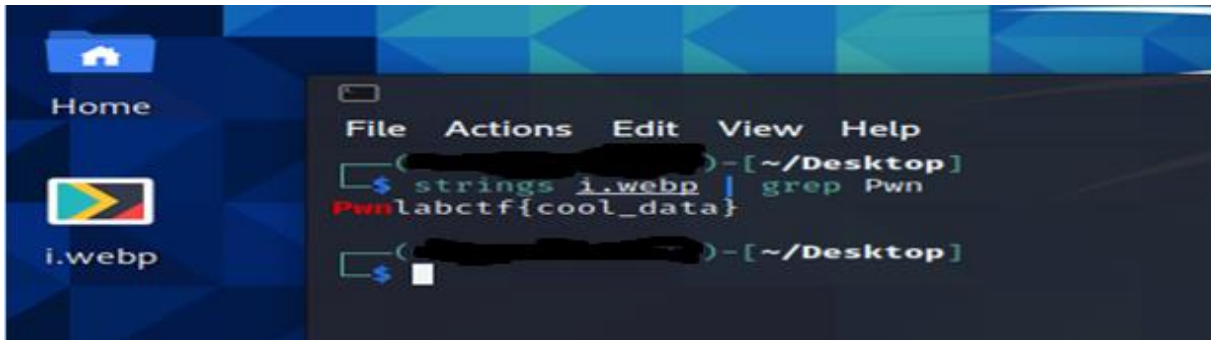
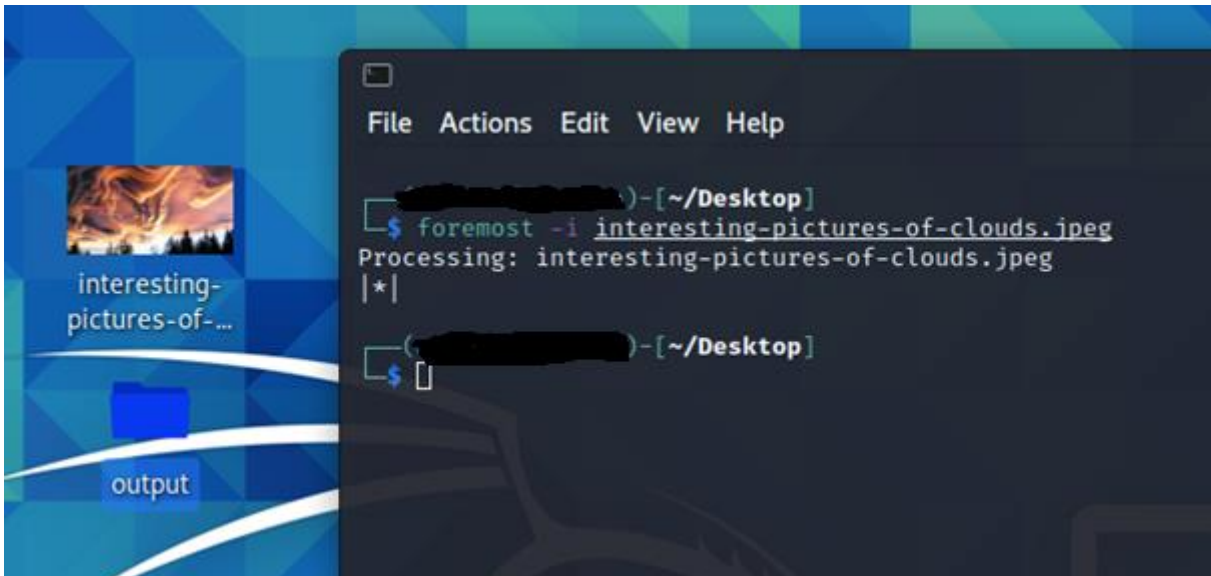


Strings are Important

Bu soruyu açıklamaya gerek bile duymuyorum :D



Binwalk



I love rabbit story

rabbit_story.pdf

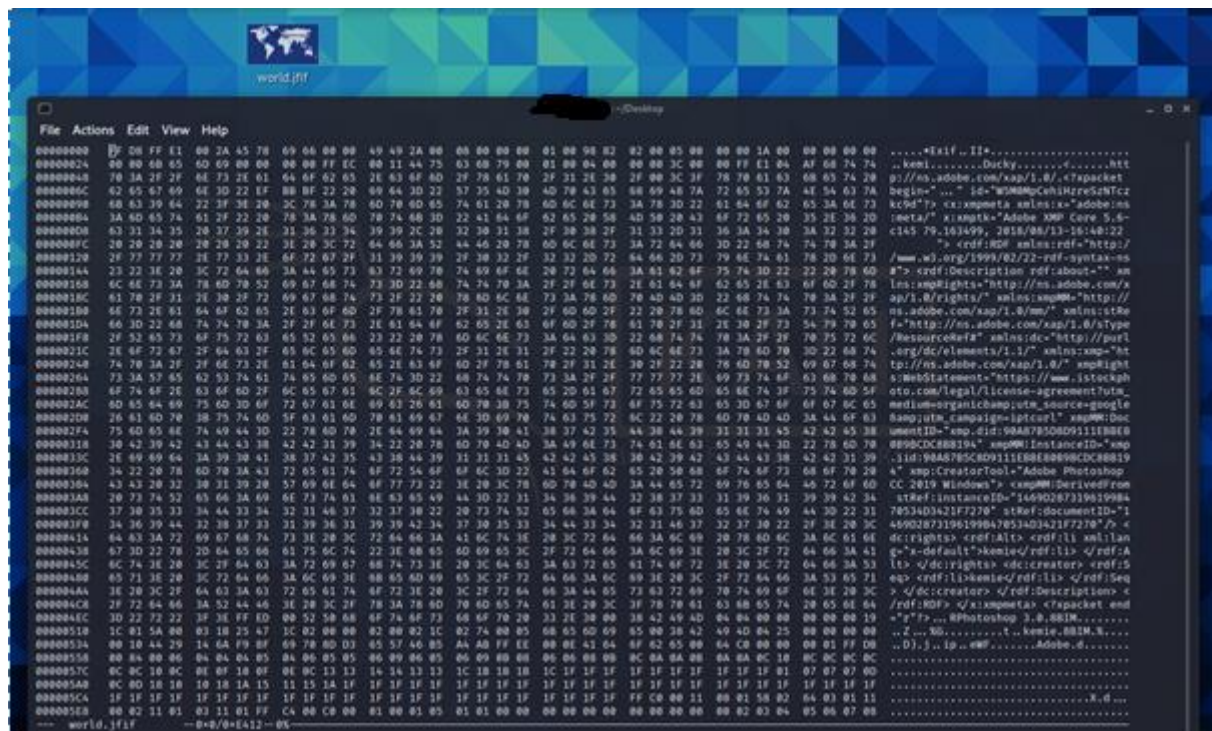
THERE was once a velveteen rabbit, and in the [REDACTED] he was really splendid. He was fat and bunchy, as a rabbit should be; his coat was spotted brown and white, he had real thread whiskers, and his ears were lined with pink sateen. On Christmas morning, when he sat wedged in the top of the Boy's stocking, with a sprig of holly between his paws, the effect was charming.

There were other things in the stocking, nuts and oranges and a toy engine, and chocolate almonds and a clockwork mouse, but the Rabbit was quite the best of all. For at least two hours the Boy loved him, and then Aunts and Uncles came to dinner, and there was a great rustling of tissue paper and unwrapping of parcels, and in the [REDACTED] of looking at all the new presents the Velveteen Rabbit was forgotten.

For a long time he lived in the toy cupboard or on the nursery floor, and no one thought very much about him. He was naturally shy, and being only made of velveteen, some of the more expensive toys quite snubbed him. The mechanical toys were very superior, and looked down upon every one else; they were full of modern ideas, and pretended they were real. The model boat, who had lived through two seasons and lost most of his paint, [REDACTED] flag:Pwnlabctf{think_simple} from them and never missed an opportunity of referring to his rigging in technical terms. The Rabbit could not claim to be a model of anything, for he didn't know that real rabbits existed; he thought they were all stuffed with sawdust like himself, and he understood that sawdust was quite out-of-date and should never be mentioned in modern circles. Even Timothy, the jointed wooden lion, who was made by the disabled soldiers, and should have had broader views, put on airs and pretended he was connected with Government. Between them all the poor little Rabbit was made to feel himself very insignificant and commonplace, and the only person who was kind to him at all was the Skin Horse.

World's Hex

Dosyanın hex headerlarına baktığımızda boş olduğunu görüyoruz, Exif olduğu için JFIF headerı olan “FF 08 FF E1” yapıyoruz ve dosyanın uzantısını “.jif” olarak değiştirip açıyoruz.

[illegible]

I hope you can find me

1)

Elimizdeki bir dump dosyası olduğu için volatility tool'unu kullanabiliriz. Öncelikle imageinfo'suna bakıyoruz. Profilleri bulduktan sonra bilgisayar ismi için özel sorgumuzu yapıyoruz ve plain text şeklinde bilgisayar ismine erişiyoruz.

```
File Actions Edit View Help
[~/Desktop/Volatility]
$ ./vol.6.linux_standalone -f image.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1*64, Win7SP0*64, Win2008R2SP0*64, Win2008R2SP1*64_23418, Win2008R2SP1*64, Win7SP1*64_23418
      AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/waffen/Desktop/Volatility/image.mem)
      PAE type : No PAE
      DTB : 0x187000L
      KDBG : 0xf800027e7130L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0xfffff800027e9000L
      KUSER_SHARED_DATA : 0xfffff80000000000L
      Image date and time : 2021-04-26 14:04:01 UTC+0000
      Image local date and time : 2021-04-26 17:04:01 +0300
```

```
[~/Desktop/Volatility]
$ ./vol.6.linux_standalone -f image.mem --profile=Win7SP1*64 -s "ControlSet001\Control\ComputerName\ComputerName" -- 0xfffff80000024010 printkey
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2021-04-25 20:46:06 UTC+0000

Subkeys:

Values:
REG_SZ ComputerName : (S) mmmsrvc
REG_SZ ComputerName : (S) CTFLAND
```

2)

Yolladığı isteklere bakmak için netscan komutunu kullanarak kayıtlara bakıyoruz ve SENT olan IP olduğunu anlıyoruz.

| | | | | | | |
|------------|-------|-------------------|---------------------|-----------|------|--------------|
| 0x3db8f10 | TCPv4 | 0.0.0.0:554 | 0.0.0.0 | LISTENING | 2748 | wmpnetwk.exe |
| 0x3db8f10 | TCPv6 | :::554 | :::0 | LISTENING | 2748 | wmpnetwk.exe |
| 0x3db8f50 | TCPv4 | 0.0.0.0:554 | 0.0.0.0 | LISTENING | 2748 | wmpnetwk.exe |
| 0x3db8fee0 | TCPv4 | 0.0.0.0:10243 | 0.0.0.0 | LISTENING | 4 | System |
| 0x3db8fee0 | TCPv6 | :::10243 | :::0 | LISTENING | 4 | System |
| 0x3dbc3730 | TCPv4 | 0.0.0.0:2869 | 0.0.0.0 | LISTENING | 4 | System |
| 0x3dbc3730 | TCPv6 | :::2869 | :::0 | LISTENING | 4 | System |
| 0x3d80a2f0 | TCPv4 | 192.168.1.7:49183 | 72.247.184.145:443 | CLOSED | -1 | |
| 0x3d81d010 | TCPv4 | 192.168.1.7:49180 | 204.79.197.200:443 | CLOSED | -1 | |
| 0x3d873530 | TCPv4 | 192.168.1.7:49175 | 204.79.197.200:443 | CLOSED | -1 | |
| 0x3d87b270 | TCPv4 | 192.168.1.7:49176 | 204.79.197.200:443 | CLOSED | -1 | |
| 0x3d8de010 | TCPv4 | 192.168.1.7:49186 | 52.165.174.123:443 | CLOSED | -1 | |
| 0x3d9293e0 | TCPv4 | 192.168.1.7:49256 | 23.251.42.221:41235 | SYN_SENT | -1 | |
| 0x3da529a0 | TCPv4 | 192.168.1.7:49241 | 152.199.19.161:443 | CLOSED | -1 | |
| 0x3dbc3ac0 | TCPv6 | :::149161 | :::12869 | CLOSED | -1 | |

3)

Username ve Password'u plain text elde etmek için registry key taraması yapıyoruz. SYSTEM ve SAM registerlarının virtual adreslerini alıp "vol image.mem -profile hashdump -y SYSTEMv -s SAM" yapıp username password hashlerini alıyoruz. Aldığımız hash'i crackstation'dan kırmayı deniyoruz ve flagimizi elde ediyoruz.

```
L$ ./vol.6_lin64_standalone -f image.mem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
-----
0xfffff8a003c0b010 0x000000001aa81010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a003c1b010 0x000000000a6f8010 \SystemRoot\System32\Config\SAM
0xfffff8a00000f010 0x00000000276cc010 [no name]
0xfffff8a000024010 0x0000000027657010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004f410 0x00000000274c2410 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0000f5010 0x00000000275b1010 \SystemRoot\System32\Config\SECURITY
0xfffff8a00046d010 0x000000002637e010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a0004e8010 0x00000000b24a010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000be0410 0x00000000085d3410 ??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000c132f0 0x00000000086152f0 ??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00121d010 0x0000000012236010 ??\C:\Users\c4n\ntuser.dat
0xfffff8a001270010 0x0000000005b39010 ??\C:\System Volume Information\Syscache.hve
0xfffff8a0012d2010 0x00000000fcd3010 ??\C:\Users\c4n\AppData\Local\Microsoft\Windows\UsrClass.dat
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1001:aad3b435b51404eeaad3b435b51404ee:093290fbb5a62029d0be708f8131b65f:::
c4n:1002:aad3b435b51404eeaad3b435b51404ee:d957b3e3cda95b3afb68eb804a730ee5:::

~/Desktop/Volatility
./vol.6_lin64_standalone -f image.mem --profile=Win7SP1x64 hashdump -y 0xfffff8a000c132f0 -s 0xfffff8a000be0410 > hash.txt
Volatility Foundation Volatility Framework 2.6

~/Desktop/Volatility
```

https://crackstation.net

Kali Forums Kali Docs NetHunter Offensive Security MSFU

tion

Defuse Security

Fre

Enter up to 20 non-salted hashes, one per line:

d957b3e3cda95b3afb68eb804a730ee5

Supports: LM, NTLM, md2, md4, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1/sha1_bin), QubesV3.1BackupDefaults

| Hash | Type | Result |
|----------------------------------|------|-----------|
| d957b3e3cda95b3afb68eb804a730ee5 | NTLM | funforyou |

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

~/Desktop/Volatility/hash.txt - Mousepad

File Edit Search View Document Help

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser\$:1001:aad3b435b51404eeaad3b435b51404ee:093290fbb5a62029d0be708f8131b65f:::
c4n:1002:aad3b435b51404eeaad3b435b51404ee:d957b3e3cda95b3afb68eb804a730ee5:::

4-5)

Elimizdeki dump'ın pslist'ine baktığımızda cmrssi.exe'yi görüyoruz ve bu process'in dump'ını alıyoruz. Aldığımız memdump'a strings atıp filtreli bir şekilde inceliyoruz. Soruda bir txt dosyası ve içinde şifreli veri olduğunu söylüyor. Buradan yola çıkarak hem company name'i hem de şifreli metni bulabiliyoruz. Şifreli metnimiz bir base64, decode edince flagi elde ediyoruz.

```

C:\Users\user> cd ~/Desktop/Volatility
$ ./vol.6_lin64_standalone -f image.mem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name  PID  PPID  Thds  Hnds  Sess  Wow64  Start  Exit
0xfffffa8000c00000 System  4  0  87  548  0  0  0  2021-04-26 14:01:50 UTC+0000
0xfffffa80001f2540 smss.exe 276 4 2 29 0 0 0 2021-04-26 14:01:51 UTC+0000
0xfffffa800026ee550 csrss.exe 360 352 12 454 0 0 0 2021-04-26 14:01:55 UTC+0000
0xfffffa80001d9a060 wininit.exe 412 352 3 73 0 0 0 2021-04-26 14:01:55 UTC+0000
0xfffffa80001d93920 csrss.exe 424 404 9 230 1 0 0 2021-04-26 14:01:55 UTC+0000
0xfffffa800027425d0 winlogon.exe 472 404 6 119 1 0 0 2021-04-26 14:01:55 UTC+0000
0xfffffa80002871290 services.exe 508 412 8 194 0 0 0 2021-04-26 14:01:56 UTC+0000
0xfffffa8000287fa90 lsass.exe 524 412 8 710 0 0 0 2021-04-26 14:01:56 UTC+0000
0xfffffa80002877790 lsm.exe 532 412 10 147 0 0 0 2021-04-26 14:01:56 UTC+0000
0xfffffa80002059b00 svchost.exe 660 508 12 357 0 0 0 2021-04-26 14:01:57 UTC+0000
0xfffffa8000292e8e0 VBoxService.exe 724 508 14 142 0 0 0 2021-04-26 14:01:58 UTC+0000
0xfffffa80002921b00 svchost.exe 784 508 9 286 0 0 0 2021-04-26 14:01:58 UTC+0000
0xfffffa80002997b00 svchost.exe 876 508 22 513 0 0 0 2021-04-26 14:01:58 UTC+0000
0xfffffa8000299eb00 svchost.exe 960 508 34 566 0 0 0 2021-04-26 14:01:59 UTC+0000
0xfffffa800029fcb00 svchost.exe 988 508 24 521 0 0 0 2021-04-26 14:02:00 UTC+0000
0xfffffa80002a157c0 svchost.exe 312 508 34 795 0 0 0 2021-04-26 14:02:00 UTC+0000
0xfffffa80002a29060 audiodg.exe 356 876 7 131 0 0 0 2021-04-26 14:02:00 UTC+0000
0xfffffa80002a3a3f0 svchost.exe 604 508 6 116 0 0 0 2021-04-26 14:02:01 UTC+0000
0xfffffa80002b66860 svchost.exe 1160 508 18 479 0 0 0 2021-04-26 14:02:02 UTC+0000
0xfffffa80002bb6370 spoolsv.exe 1256 508 17 293 0 0 0 2021-04-26 14:02:02 UTC+0000
0xfffffa80002bda620 svchost.exe 1292 508 21 325 0 0 0 2021-04-26 14:02:03 UTC+0000
0xfffffa80002c37b00 svchost.exe 1404 508 11 149 0 0 0 2021-04-26 14:02:03 UTC+0000
0xfffffa80002c74b00 svchost.exe 1476 508 21 282 0 0 0 2021-04-26 14:02:04 UTC+0000
0xfffffa80002e62b00 taskhost.exe 1060 508 13 248 1 0 0 2021-04-26 14:02:11 UTC+0000
0xfffffa80002e8bb00 dwm.exe 1360 960 5 99 1 0 0 2021-04-26 14:02:11 UTC+0000
0xfffffa80002e8db00 explorer.exe 1400 1336 38 1005 1 0 0 2021-04-26 14:02:11 UTC+0000
0xfffffa80001f48750 VBoxTray.exe 1988 1400 16 146 1 0 0 2021-04-26 14:02:12 UTC+0000
0xfffffa800029aa9b0 SearchIndexer.exe 2376 508 15 605 0 0 0 2021-04-26 14:02:20 UTC+0000
0xfffffa80002fdab00 SearchProtocolHost.exe 2480 2376 7 248 1 0 0 2021-04-26 14:02:21 UTC+0000
0xfffffa80002ff1060 SearchFilterHost.exe 2500 2376 4 79 0 0 0 2021-04-26 14:02:21 UTC+0000
0xfffffa80002e24b00 wmpnetwk.exe 2748 508 16 431 0 0 0 2021-04-26 14:02:26 UTC+0000
0xfffffa8000312d480 svchost.exe 2928 508 9 348 0 0 0 2021-04-26 14:02:28 UTC+0000
0xfffffa8000310fb00 WmiPrvSE.exe 928 660 8 119 0 0 0 2021-04-26 14:02:29 UTC+0000
0xfffffa80003312a30 svchost.exe 2924 508 4 42 0 0 0 2021-04-26 14:02:47 UTC+0000
0xfffffa80001f85b00 cmrssi.exe 2208 1400 6 162 1 1 0 2021-04-26 14:03:51 UTC+0000
0xfffffa800031d9060 conhost.exe 1700 424 2 52 1 0 0 2021-04-26 14:03:51 UTC+0000
0xfffffa8000316ab00 RamCapture64.exe 2068 1400 3 70 1 0 0 2021-04-26 14:04:00 UTC+0000
0xfffffa8000331e060 conhost.exe 1752 424 2 52 1 0 0 2021-04-26 14:04:00 UTC+0000

```

```

$ ./vol.6_lin64_standalone -f image.mem --profile=Win7SP1x64 memdump -p 2208 --dump-dir /home/ /Desktop
Volatility Foundation Volatility Framework 2.6
*****
Writing cmrssi.exe [ 2208] to 2208.dmp

```

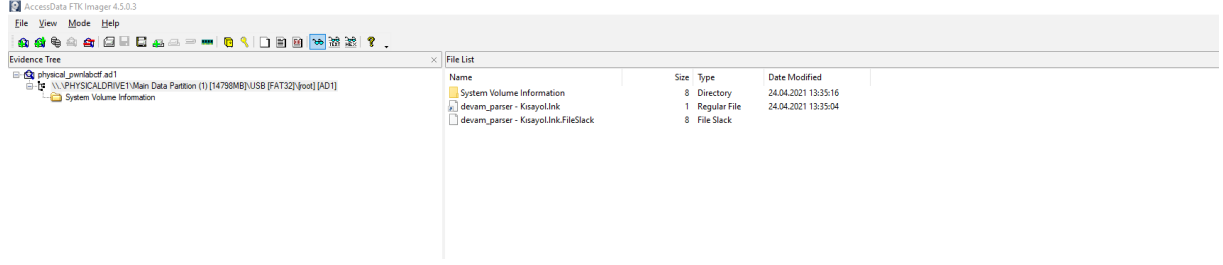
```
File Edit Search View Document Help
--Desktop\2208.txt - Mousepad

ssAGC_36.snp.db
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winsat
DiskScore
VirtualStoreSize
\WINDOWS\Prefetch\
\CONFIG\VF0BACK\
\WDI\
\WINDOWS
Watches
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Superfetch\ReservedPriorityObs
(null)
SYSTEM\CurrentControlSet\Services\rdyboost\Performance
First Counter
First Help
Delete
NoRemove
ForceRemove
API-HS-Win-Core-LocalRegistry-L1-1-0.dll
Hedup132.dll
3+3+
\Sessions\1\BaseNamedObjects
\Sessions\1\BaseNamedObjects\Global\CPFATE_2208_v4.0.30319pc\Rpc<
Pmlabcop
23.251.42.221
\dontdelete.txt
\Hedup132.dll\bx720bu25f9
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
00000409
Comments
CompanyName
HP Inc.
FileDescription
pmlabcop
FileVersion
1.0.0.0
InternalName
pmlabcop.exe
LegalCopyright
Copyright
HP Inc. 2021
LegalTrademarks
```

Where is My MAC

Ad1 uzantılı dosyaları FTK Imager ile inceliyoruz. Elimizdeki ad1 uzantılı dosyayı import ettiğimizde “.lnk” uzantılı dosya olduğunu görüyoruz, bu dosyanın hashlerini export ediyoruz. Windows için bir tool olan Inkanalyser

<https://github.com/woanware/woanware.github.io/blob/master/downloads/Inkanalyser.v1.0.1.zip> kullanarak elimizdeki “.lnk” dosyasını inceliyoruz ve MAC adresini elde ediyoruz.



```
C:\> Seç C:\Windows\System32\cmd.exe
Microsoft Windows [Sürüm 6.1.7601]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\zorro\Desktop\Inkanalyzer>Inkanalyser.exe -i devam_parser.lnk

Inkanalyser v1.0.1

Lnk Metadata
-----
Path: devam_parser.lnk
Flags:
Attributes: Archive
Show Command: SW_SHOWNORMAL
Name:
Relative Path: .\devam_parser.txt
Working Path: D:\
Arguments:
Icon Location:

Target Metadata
-----
Created Timestamp: 24.04.2021 10:20:33
Accessed Timestamp: 24.04.2021 10:34:57
Written Timestamp: 24.04.2021 10:34:57
File Size: 1002
Icon Index: 0

Volume Id
-----
Drive Type: DRIVE_FIXED
Serial No: 605ABC79
Name: Yeni Birim

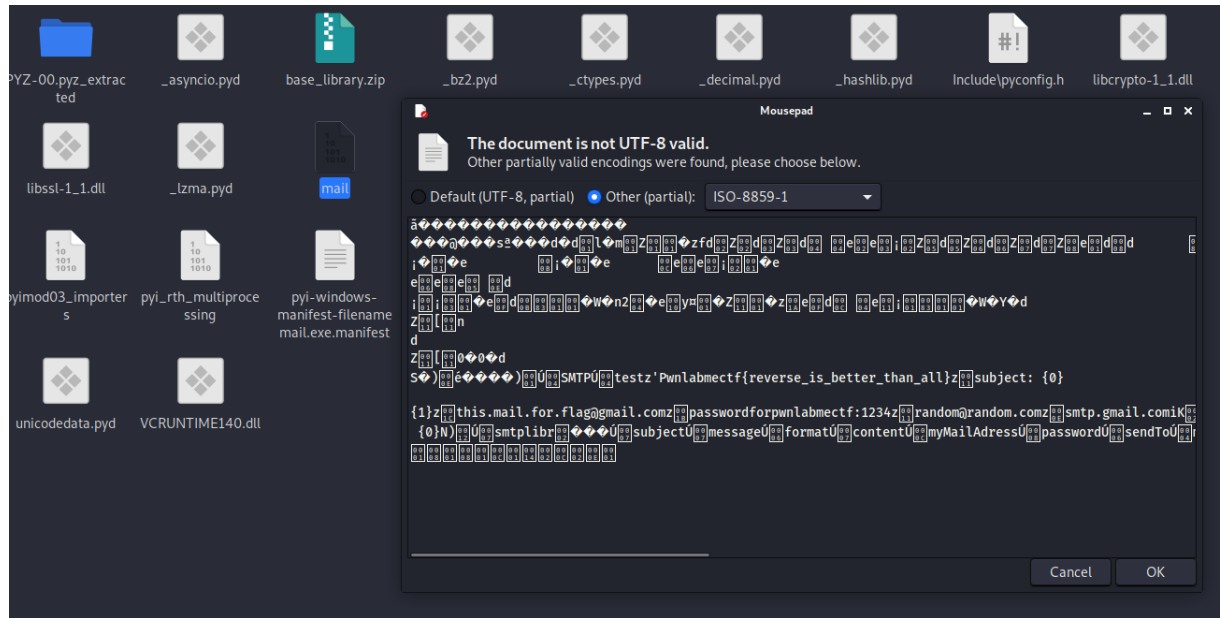
TrackerDataBlock
-----
MachineId: desktop-5qfg8i6
NewVolumeId: 7A12ADC0D9541B41AAA2E7F840C5F111
NewObjectId: F240B90EE2A0EB11B88C0862660FFE8B
NewObjectId Timestamp: 19.04.2021 07:37:13
NewObjectId Sequence Number: 14476
NewObjectId MAC Address: 08:62:66:0F:FE:8B
BirthVolumeId: 7A12ADC0D9541B41AAA2E7F840C5F111
BirthObjectId: F240B90EE2A0EB11B88C0862660FFE8B
BirthObjectId Timestamp: 19.04.2021 07:37:13
BirthObjectId Sequence Number: 14476
BirthObjectId MAC Address: 08:62:66:0F:FE:8B
```


Silly Challenge

Elimizdeki sample'ın python'dan exe'ye çevirilmiş bir executable olduğunu görüyoruz bu yüzden "python exe unpack" toolunu kullanıyoruz "<https://github.com/countercept/python-exe-unpacker>

". Gerekli parametreleri verdiğimizde bize executable'ın python'a dönüştürülmüş halini unpack ediyor. İçerisinde mail isminde bir binary görüyoruz, mousepad ile açtığımızda flagi elde ediyoruz.

```
L# python3 python exe unpack.py -i mail.exe -o unpacked
[*] On Python 3.9
[*] Processing mail.exe
[*] Pyinstaller version: 2.1+
[*] This exe is packed using pyinstaller
[*] Unpacking the binary now
[*] Python version: 39
[*] Length of package: 6598005 bytes
[*] Found 31 files in CArchive
[*] Beginning extraction ... please standby
[*] Found 229 files in PYZ archive
[*] Successfully extracted pyinstaller exe.
```



Fatih YILMAZ

-AteSuToprakTahta-