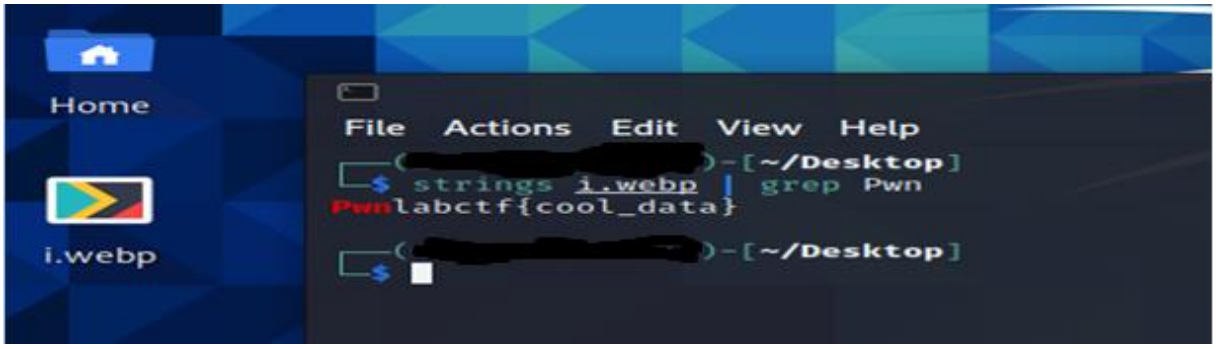
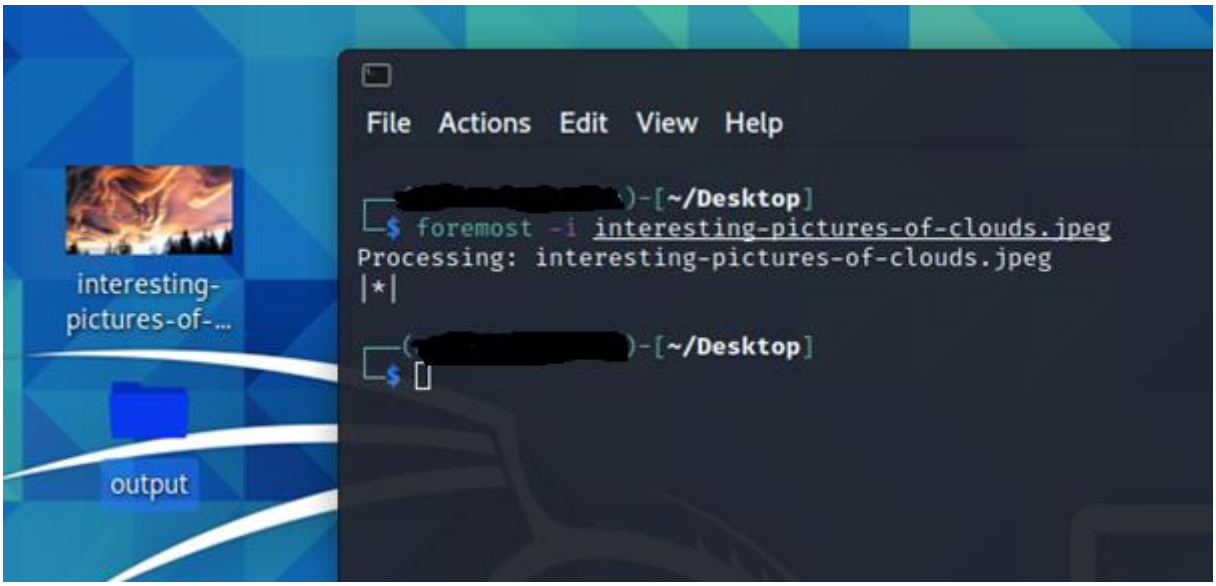
Strings are Important

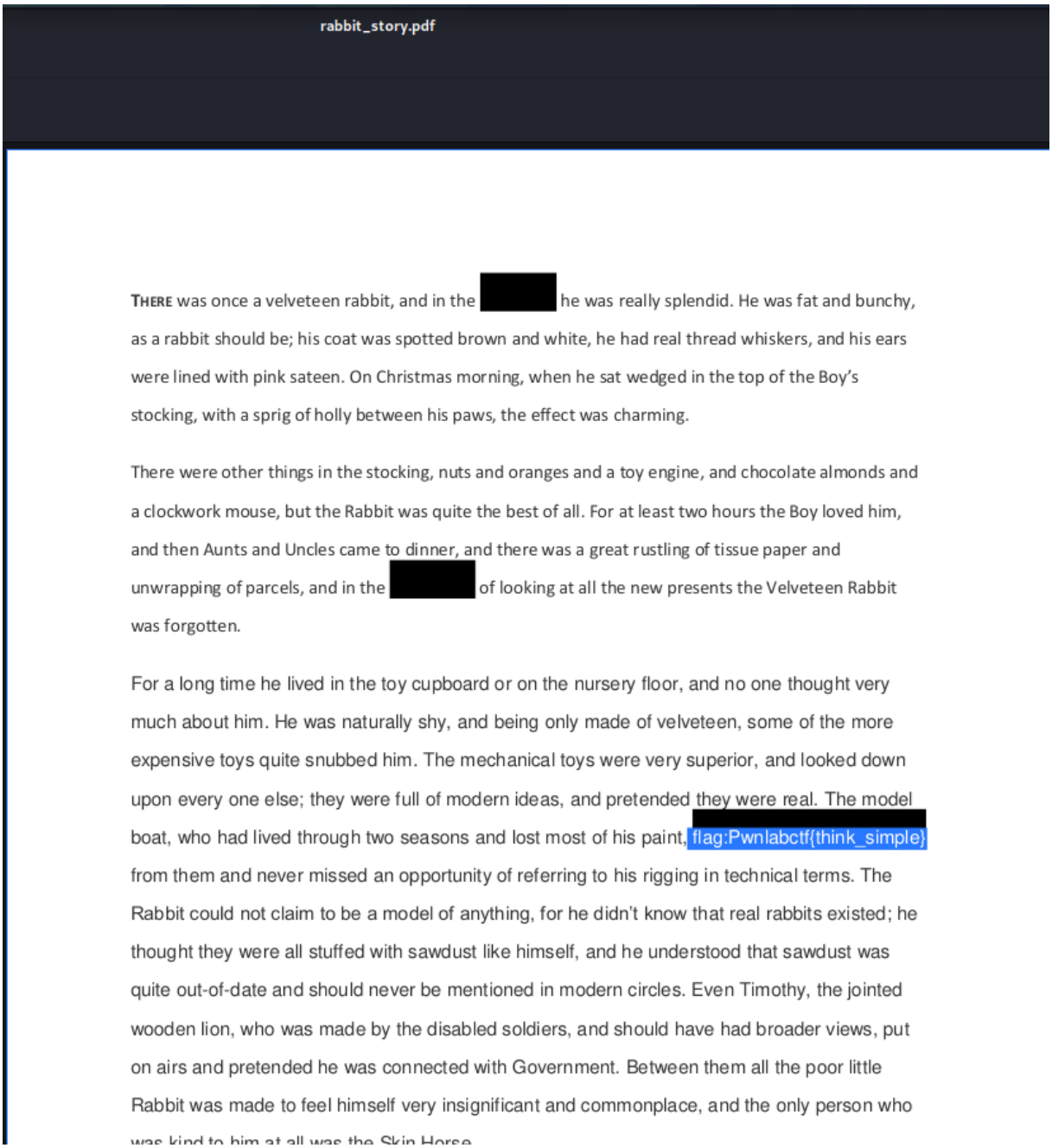
Bu soruyu açıklamaya gerek bile duymuyorum :D



Binwalk

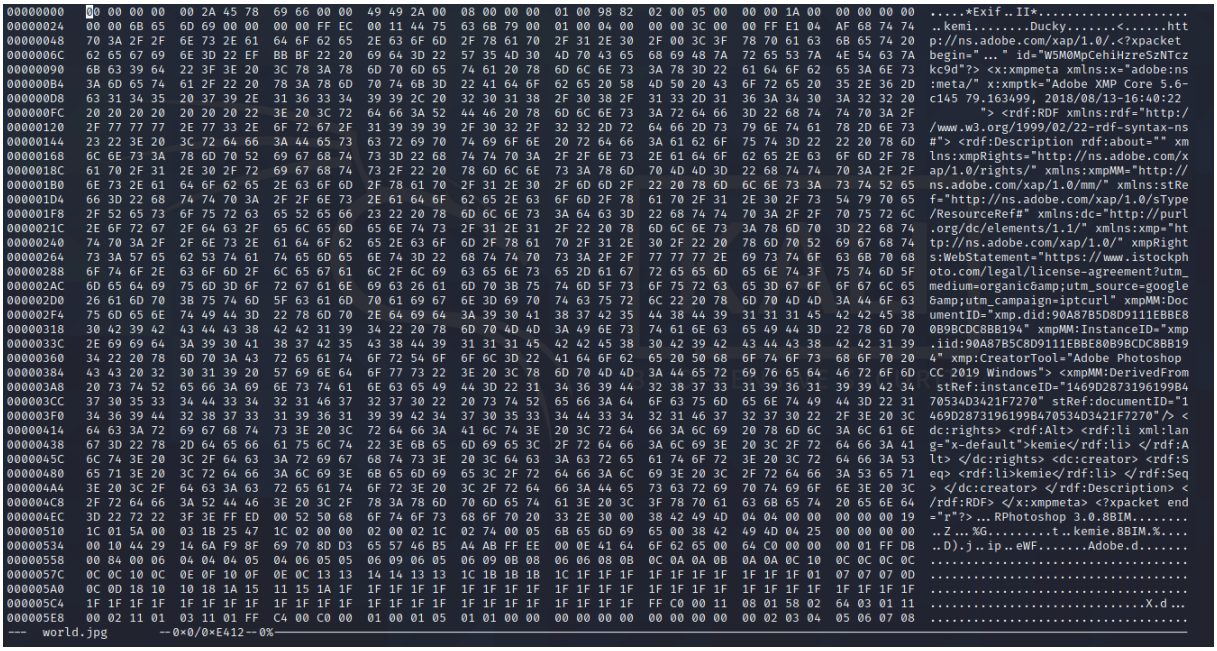


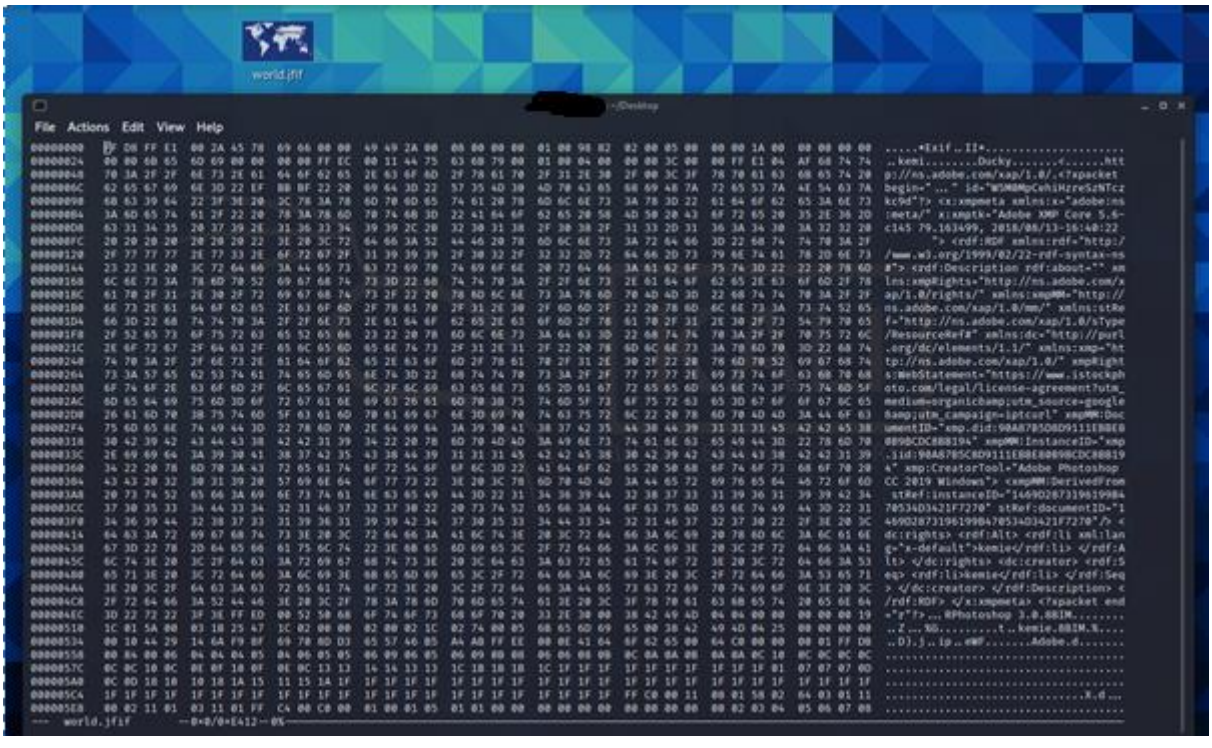
I love rabbit story



World’s Hex

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

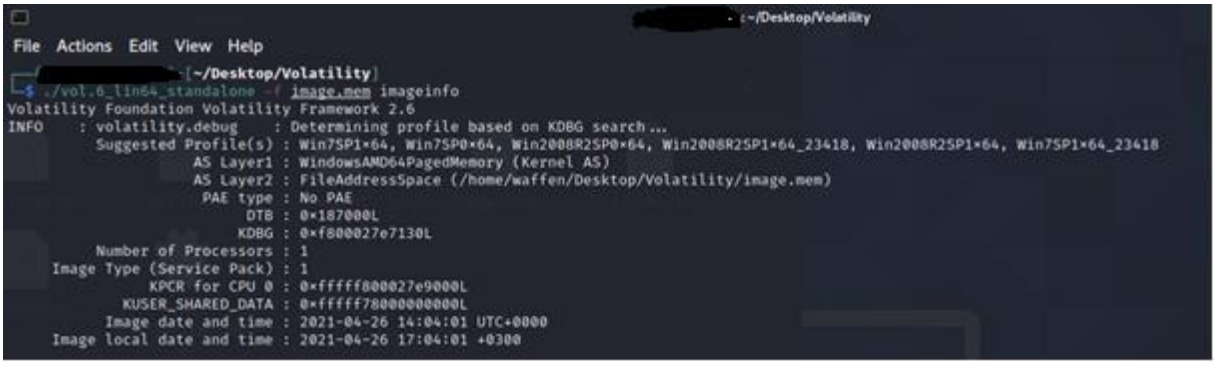




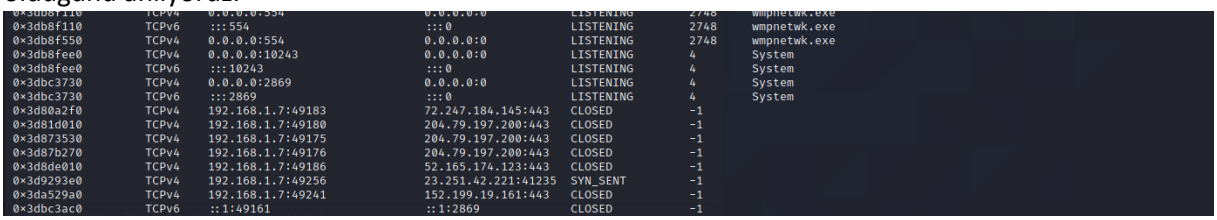
I hope you can find me

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.



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

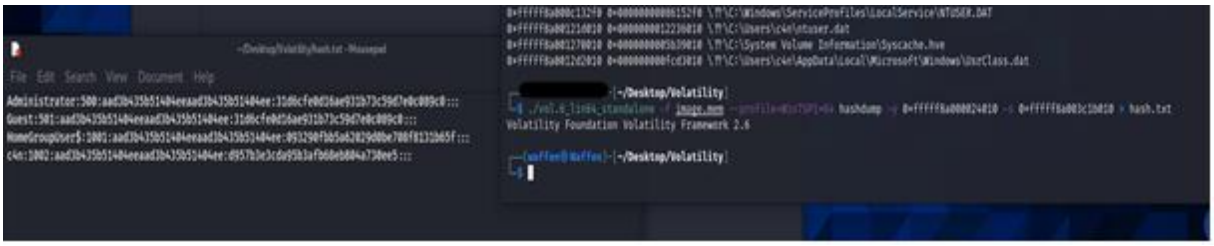


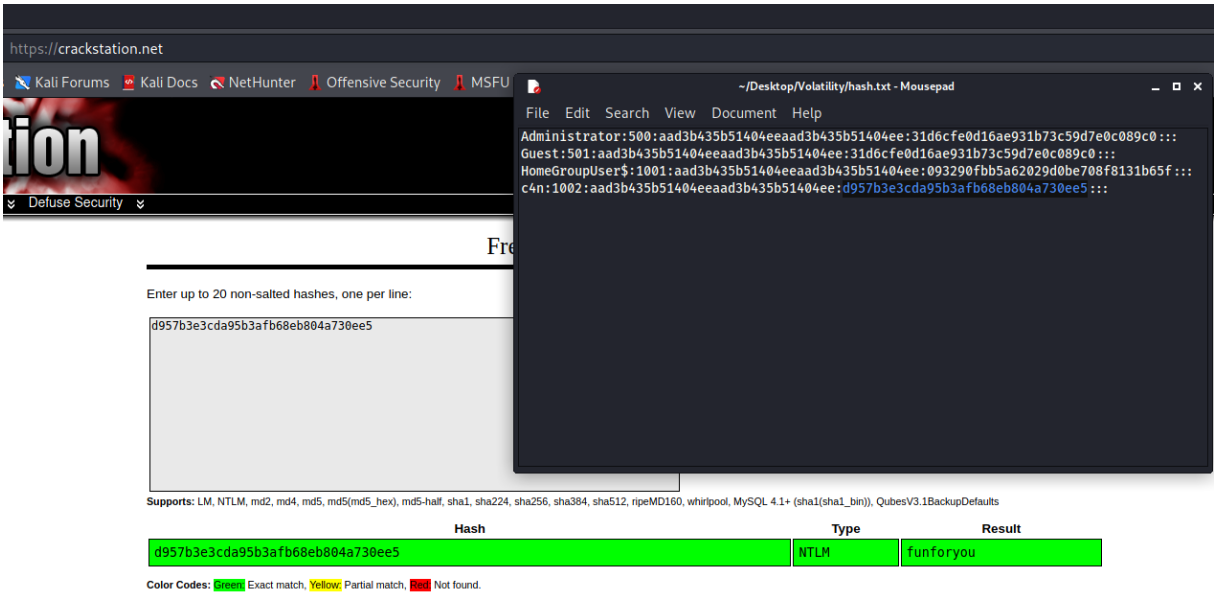
0x3db8f110	TCPv6	:::554	:::0	LISTENING	2748	wmpnetwk.exe
0x3db8f550	TCPv4	0.0.0.0:554	0.0.0.0:0	LISTENING	2748	wmpnetwk.exe
0x3db8fee0	TCPv4	0.0.0.0:10243	0.0.0.0:0	LISTENING	4	System
0x3db8fee0	TCPv6	:::10243	:::0	LISTENING	4	System
0x3dbc3730	TCPv4	0.0.0.0:2869	0.0.0.0:0	LISTENING	4	System
0x3dbc3730	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	::1:49161	::1:2869	CLOSED	-1	

3)

Username ve Password'u plain text elde etmek için registery 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.

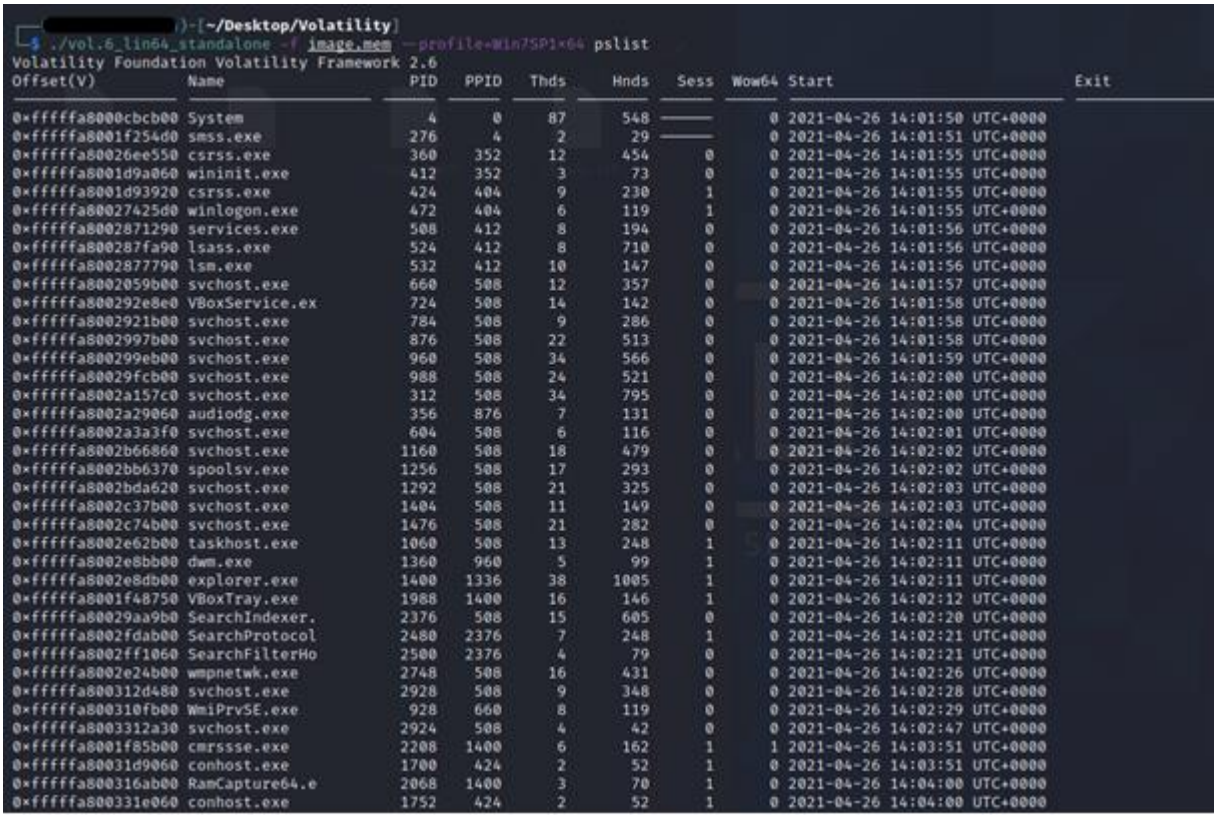
```
└─$ ./vol.6_lin64_standalone -f image.mem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----

0xfffff8a003c0b010 0x000000001aa81010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a003c1b010 0x000000000a6f8010 \SystemRoot\System32\Config\SAM
0xfffff8a00000f010 0x000000000276cc010 [no name]
0xfffff8a000024010 0x0000000027657010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004f410 0x000000000274c2410 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0000f5010 0x000000000275b1010 \SystemRoot\System32\Config\SECURITY
0xfffff8a00046d010 0x000000002637e010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a0004e8010 0x000000000b24a010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000be0410 0x000000000085d3410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000c132f0 0x000000000086152f0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00121d010 0x0000000012236010 \??\C:\Users\c4n\ntuser.dat
0xfffff8a001270010 0x0000000005b39010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a0012d2010 0x000000000fcd3010 \??\C:\Users\c4n\AppData\Local\Microsoft\Windows\UsrClass.dat
```





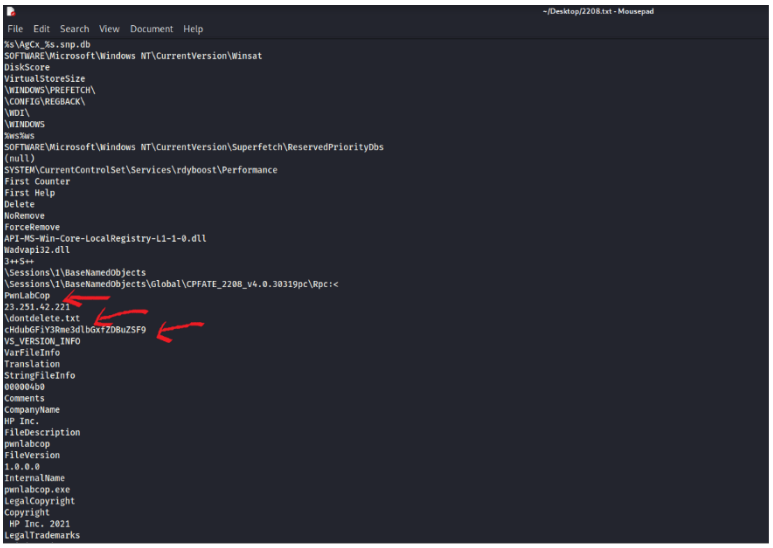
4-5)

Elimizdeki dump'ın pslist'ine baktığımızda cmrssse.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 metini bulabiliyoruz. Şifreli metinimiz bir base64, decode edince flagi elde ediyoruz.



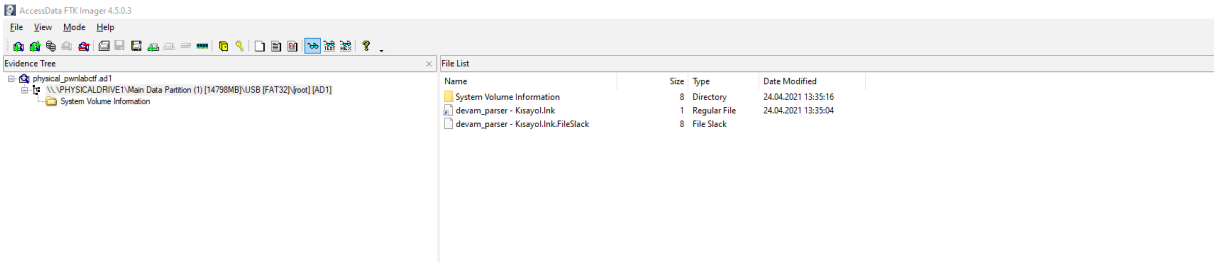
```
┌──([redacted])-[~/Desktop/Volatility]
└─$ ./vol.6_lin64_standalone -f image.mem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000cbcb00 System                    4      0     87      548 ------      0 2021-04-26 14:01:50 UTC+0000
0xfffffa8001f254d0 smss.exe                276      4      2       29 ------      0 2021-04-26 14:01:51 UTC+0000
0xfffffa80026ee550 csrss.exe               360    352     12      454      0      0 2021-04-26 14:01:55 UTC+0000
0xfffffa8001d9a060 wininit.exe             412    352      3       73      0      0 2021-04-26 14:01:55 UTC+0000
0xfffffa8001d93920 csrss.exe               424    404      9      230      1      0 2021-04-26 14:01:55 UTC+0000
0xfffffa80027425d0 winlogon.exe            472    404      6      119      1      0 2021-04-26 14:01:55 UTC+0000
0xfffffa8002871290 services.exe            508    412      8      194      0      0 2021-04-26 14:01:56 UTC+0000
0xfffffa800287fa90 lsass.exe               524    412      8      710      0      0 2021-04-26 14:01:56 UTC+0000
0xfffffa8002877790 lsm.exe                 532    412     10      147      0      0 2021-04-26 14:01:56 UTC+0000
0xfffffa8002059b00 svchost.exe             660    508     12      357      0      0 2021-04-26 14:01:57 UTC+0000
0xfffffa800292e8e0 VBoxService.ex          724    508     14      142      0      0 2021-04-26 14:01:58 UTC+0000
0xfffffa8002921b00 svchost.exe             784    508      9      286      0      0 2021-04-26 14:01:58 UTC+0000
0xfffffa8002997b00 svchost.exe             876    508     22      513      0      0 2021-04-26 14:01:58 UTC+0000
0xfffffa800299eb00 svchost.exe             960    508     34      566      0      0 2021-04-26 14:01:59 UTC+0000
0xfffffa80029fcb00 svchost.exe             988    508     24      521      0      0 2021-04-26 14:02:00 UTC+0000
0xfffffa8002a157c0 svchost.exe             312    508     34      795      0      0 2021-04-26 14:02:00 UTC+0000
0xfffffa8002a29060 audiodg.exe             356    876      7      131      0      0 2021-04-26 14:02:00 UTC+0000
0xfffffa8002a3a3f0 svchost.exe             604    508      6      116      0      0 2021-04-26 14:02:01 UTC+0000
0xfffffa8002b66860 svchost.exe            1160    508     18      479      0      0 2021-04-26 14:02:02 UTC+0000
0xfffffa8002bb6370 spoolsv.exe            1256    508     17      293      0      0 2021-04-26 14:02:02 UTC+0000
0xfffffa8002bda620 svchost.exe            1292    508     21      325      0      0 2021-04-26 14:02:03 UTC+0000
0xfffffa8002c37b00 svchost.exe            1404    508     11      149      0      0 2021-04-26 14:02:03 UTC+0000
0xfffffa8002c74b00 svchost.exe            1476    508     21      282      0      0 2021-04-26 14:02:04 UTC+0000
0xfffffa8002e62b00 taskhost.exe           1060    508     13      248      1      0 2021-04-26 14:02:11 UTC+0000
0xfffffa8002e8bb00 dwm.exe                1360    960      5       99      1      0 2021-04-26 14:02:11 UTC+0000
0xfffffa8002e8db00 explorer.exe           1400   1336     38     1005      1      0 2021-04-26 14:02:11 UTC+0000
0xfffffa8001f48750 VBoxTray.exe           1988   1400     16      146      1      0 2021-04-26 14:02:12 UTC+0000
0xfffffa80029aa9b0 SearchIndexer.         2376    508     15      605      0      0 2021-04-26 14:02:20 UTC+0000
0xfffffa8002fdab00 SearchProtocol         2480   2376      7      248      1      0 2021-04-26 14:02:21 UTC+0000
0xfffffa8002ff1060 SearchFilterHo         2500   2376      4       79      0      0 2021-04-26 14:02:21 UTC+0000
0xfffffa8002e24b00 wmpnetwk.exe           2748    508     16      431      0      0 2021-04-26 14:02:26 UTC+0000
0xfffffa800312d480 svchost.exe            2928    508      9      348      0      0 2021-04-26 14:02:28 UTC+0000
0xfffffa800310fb00 WmiPrvSE.exe            928    660      8      119      0      0 2021-04-26 14:02:29 UTC+0000
0xfffffa8003312a30 svchost.exe            2924    508      4       42      0      0 2021-04-26 14:02:47 UTC+0000
0xfffffa8001f85b00 cmrssse.exe            2208   1400      6      162      1      1 2021-04-26 14:03:51 UTC+0000
0xfffffa80031d9060 conhost.exe            1700    424      2       52      1      0 2021-04-26 14:03:51 UTC+0000
0xfffffa800316ab00 RamCapture64.e         2068   1400      3       70      1      0 2021-04-26 14:04:00 UTC+0000
0xfffffa800331e060 conhost.exe            1752    424      2       52      1      0 2021-04-26 14:04:00 UTC+0000
```

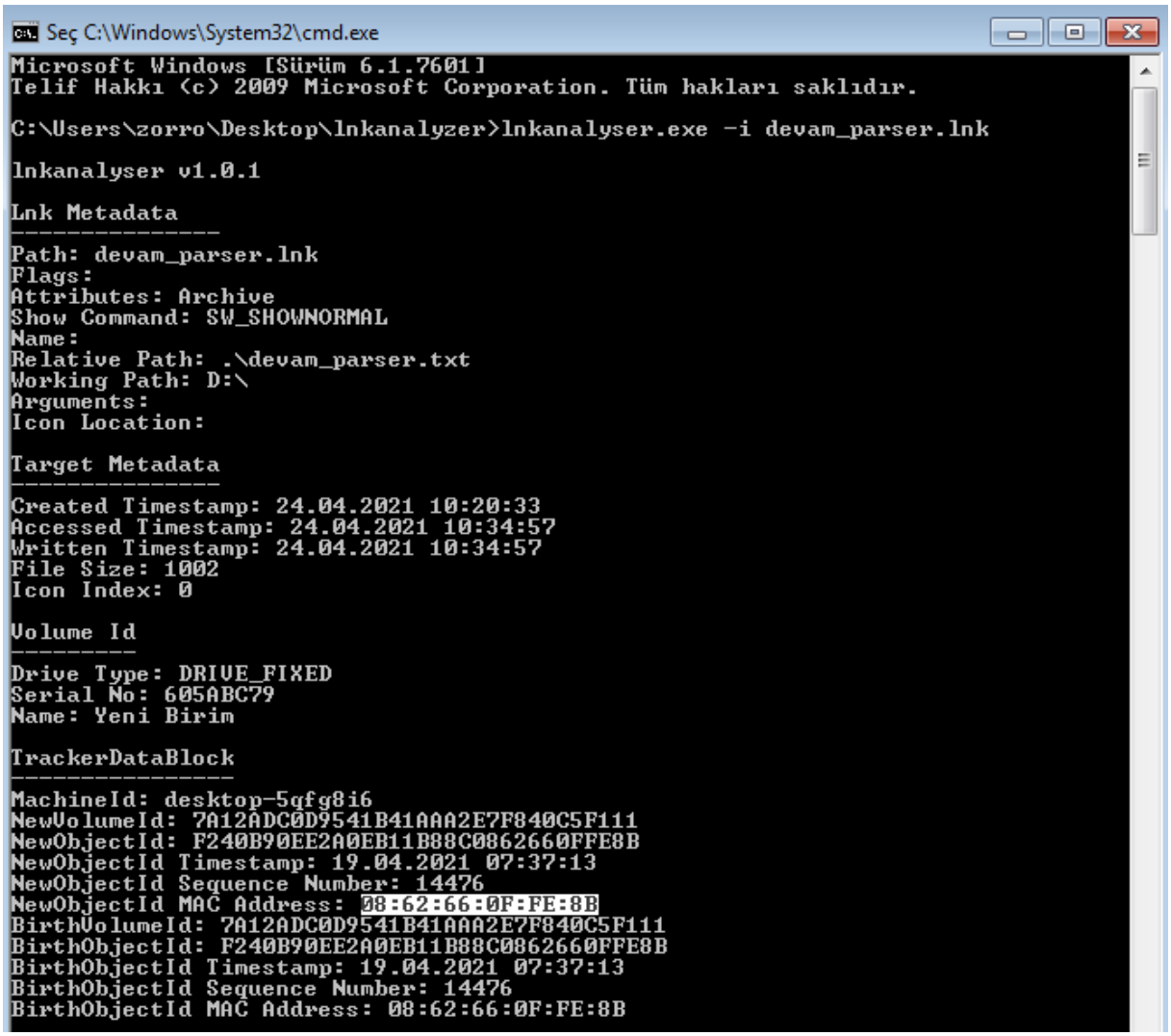
```
└─$ ./vol.6_lin64_standalone -f image.mem --profile=Win7SP1x64 memdump -p 2208 --dump-dir /home/[redacted]/Desktop
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing cmrssse.exe [  2208] to 2208.dmp
```


~/Desktop/2208.txt - Mousepad
File Edit Search View Document Help
%s\AgCx_%s.snp.db
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winsat
DiskScore
VirtualStoreSize
\WINDOWS\PREFETCH\
\CONFIG\REGBACK\
\WDI\
\WINDOWS
%ws%ws
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Superfetch\ReservedPriorityDbs
(null)
SYSTEM\CurrentControlSet\Services\rdyboost\Performance
First Counter
First Help
Delete
NoRemove
ForceRemove
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
Wadvapi32.dll
3++S++
\Sessions\1\BaseNamedObjects
\Sessions\1\BaseNamedObjects\Global\CPFATE_2208_v4.0.30319pc\Rpc:<
PwnLabCop
23.251.42.221
\dontdelete.txt
cHdubGFiY3Rme3dlbGxfZDBuZSF9
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
000004b0
Comments
CompanyName
HP Inc.
FileDescription
pwnlabcop
FileVersion
1.0.0.0
InternalName
pwnlabcop.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 lnkanalyser https://github.com/woanware/woanware.github.io/blob/master/downloads/lnkanalyser.v.1.0.1.zip kullanarak elimizdeki ".lnk" dosyasını inceliyoruz ve MAC adresini elde ediyoruz.



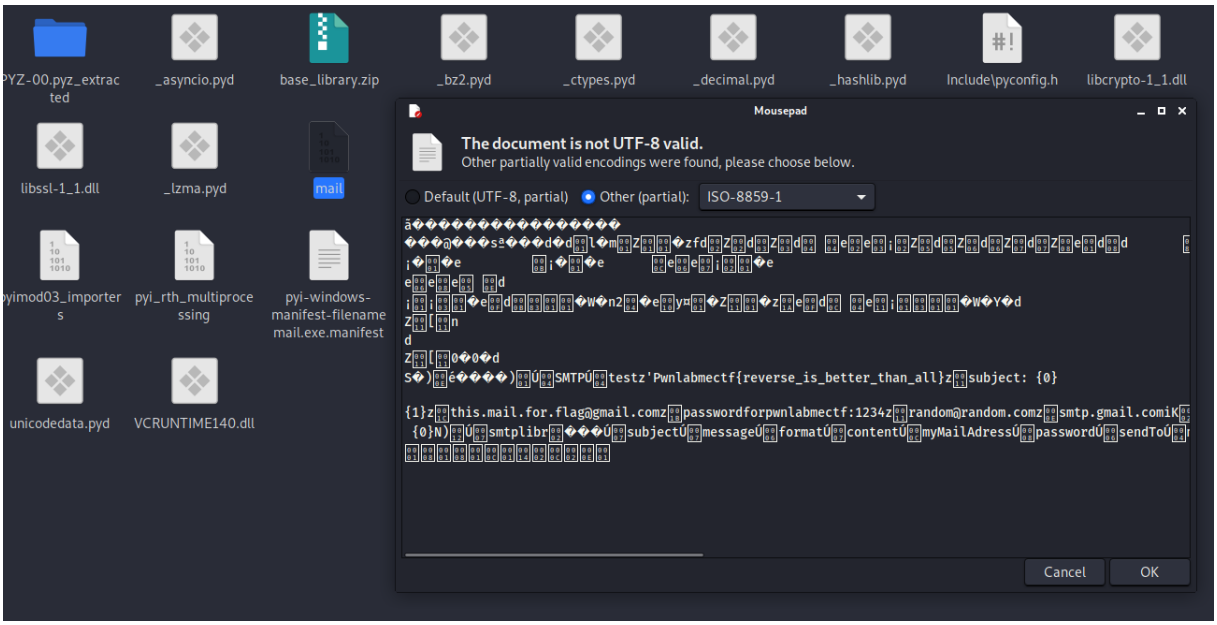


Silly Challange

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.

```
└─# 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

-AtesSuToprakTahta-