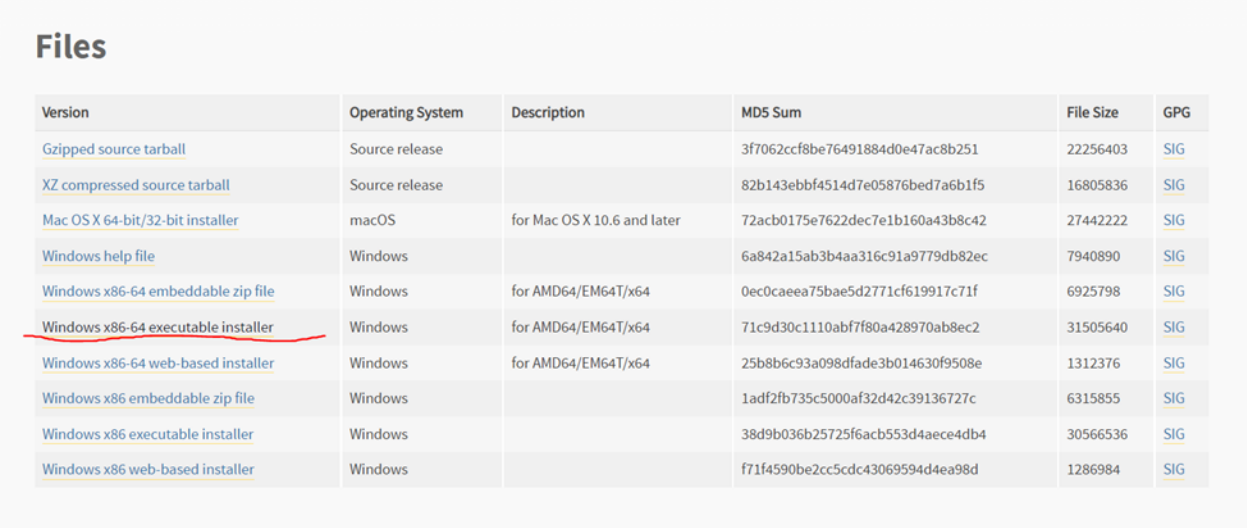
Malware Analysis Report

Introduction

In this course we are tasked to install Rekall, an advanced forensic and incident response framework, to safely study malicious malware from Virus Share (Where we will get most of our source code to Malware that I will study).

Installing Rekall

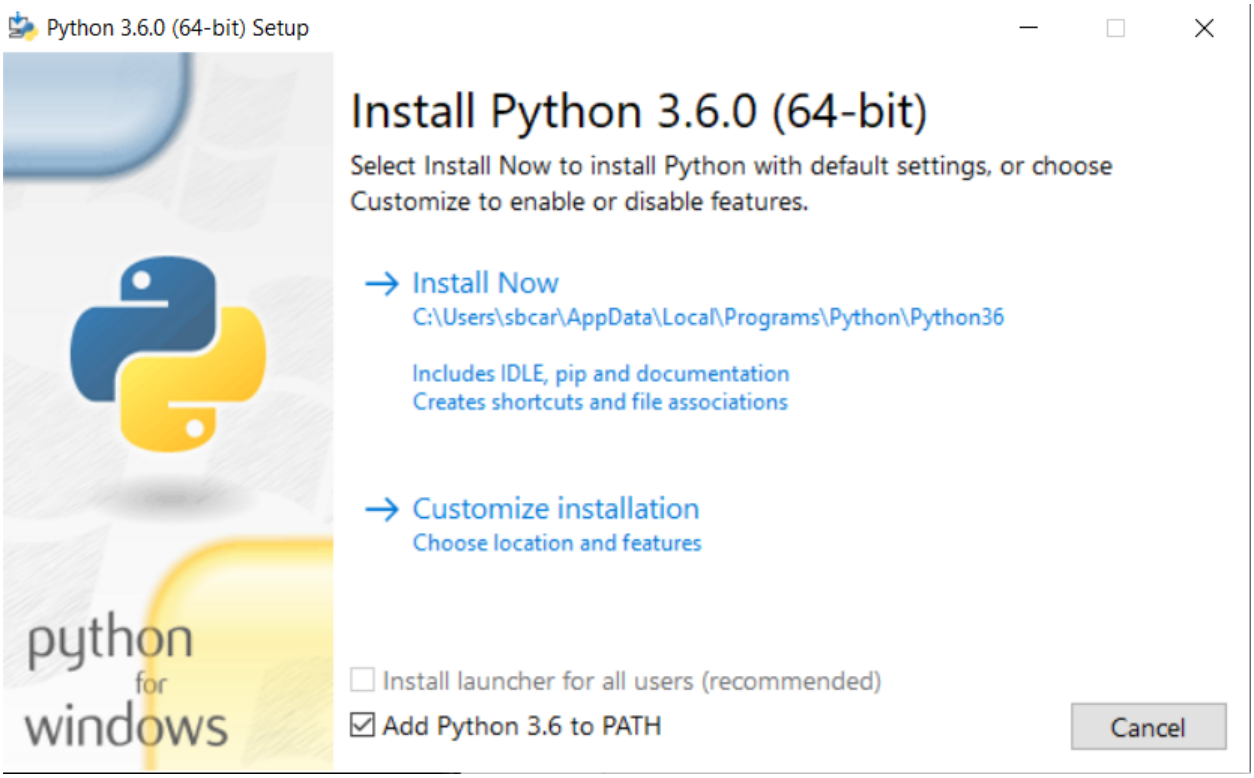
First, you'll need to install python 3.6 to help run Rekall. Click the link https://www.python.org/downloads/release/python-360/ and scroll until you see, "Windows x86-64 executable installer" and follow the installation process along with check marking



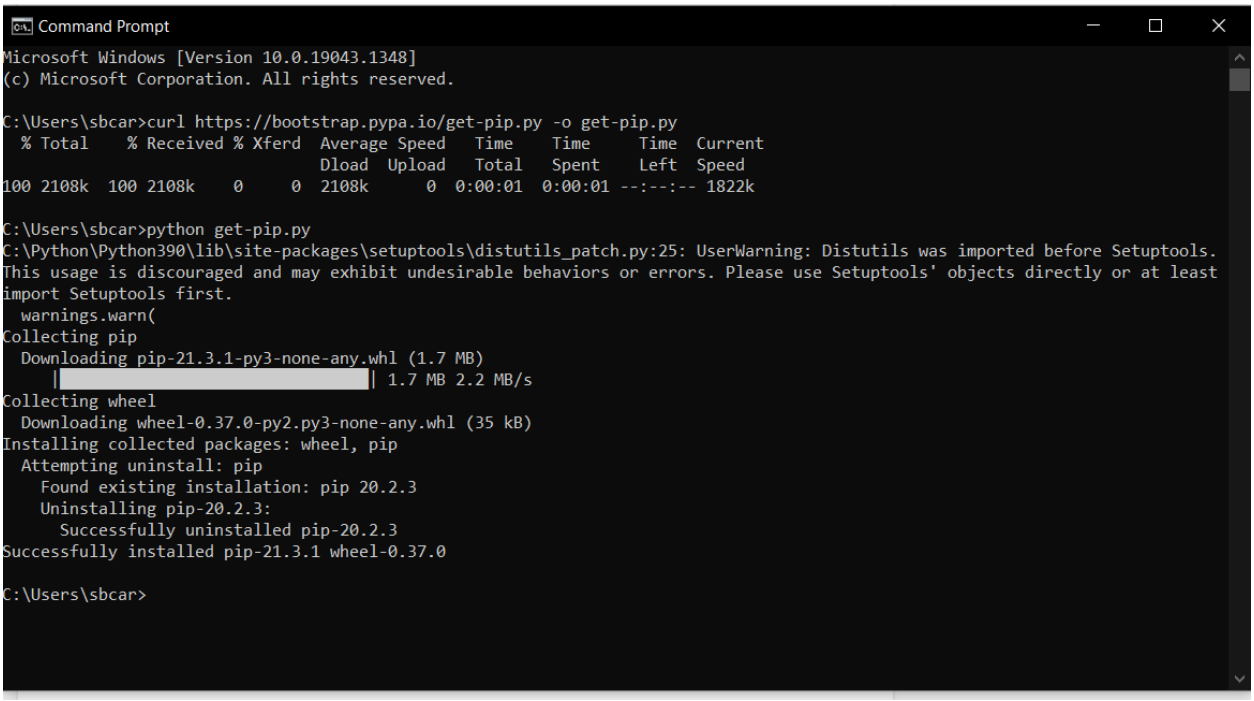
Files

Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		3f7062ccf8be76491884d0e47ac8b251	22256403	SIG
XZ compressed source tarball	Source release		82b143ebbf4514d7e05876bed7a6b1f5	16805836	SIG
Mac OS X 64-bit/32-bit installer	macOS	for Mac OS X 10.6 and later	72acb0175e7622dec7e1b160a43b8c42	27442222	SIG
Windows help file	Windows		6a842a15ab3b4aa316c91a9779db82ec	7940890	SIG
Windows x86-64 embeddable zip file	Windows	for AMD64/EM64T/x64	0ec0caeea75bae5d2771cf619917c71f	6925798	SIG
Windows x86-64 executable installer	Windows	for AMD64/EM64T/x64	71c9d30c1110abf7f80a428970ab8ec2	31505640	SIG
Windows x86-64 web-based installer	Windows	for AMD64/EM64T/x64	25b8b6c93a098dfade3b014630f9508e	1312376	SIG
Windows x86 embeddable zip file	Windows		1adf2fb735c5000af32d42c39136727c	6315855	SIG
Windows x86 executable installer	Windows		38d9b036b25725f6acb553d4aece4db4	30566536	SIG
Windows x86 web-based installer	Windows		f71f4590be2cc5cdc43069594d4ea98d	1286984	SIG

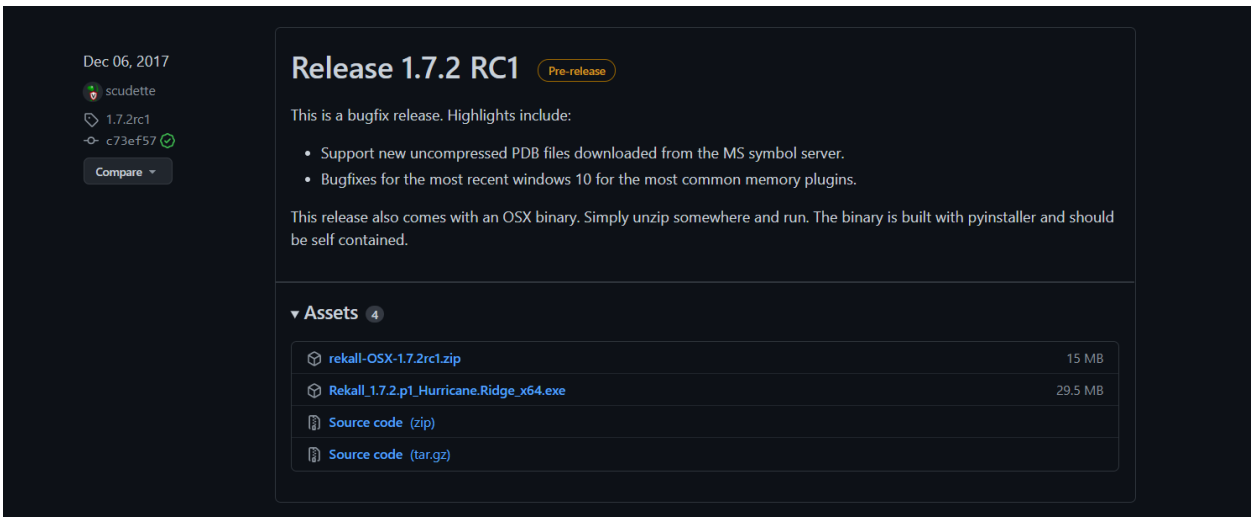
, “ADD TO PAT H”.



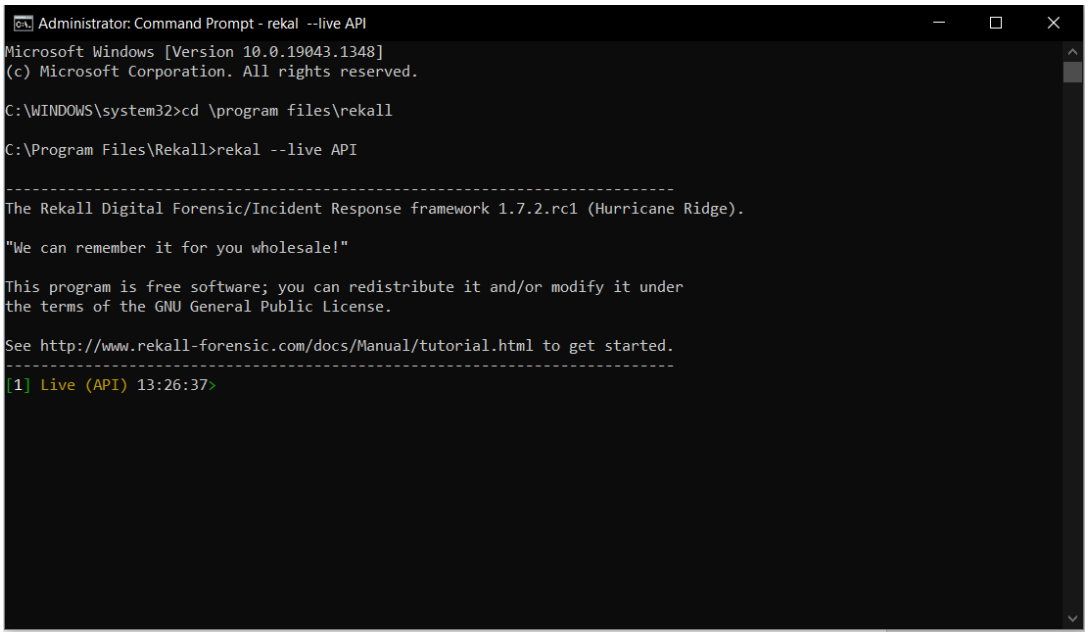
Then pull command prompt and type, “curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py” Results should like as the picture below.



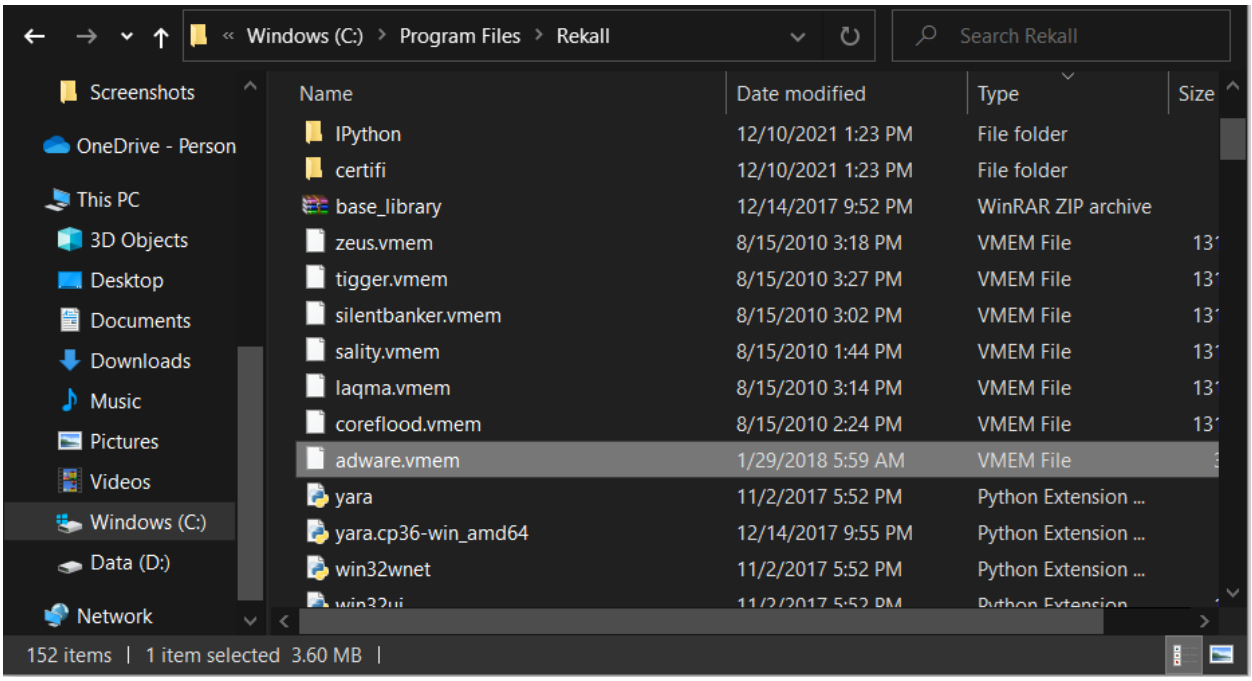
Then, go to this Github page https://github.com/google/rekall/releases and download the file, “Rekall_1.7.2.p1_Hurricane.Ridge_x64.exe” and follow it’s directions. For simplicity if prompt on where to put folder put it under C:\\Program Files and make a folder called Rekall and install there.



Then pull up the command prompt on that C:\\Program File\ and type in, “cd \program files\rekall” and type in another line, “rekal --live API” Then your Rekall set and ready to analyze malware.



Note: When you have your downloaded malware, be sure to place them under the same Rekall folder that you made in your C drive.



Key Commands:

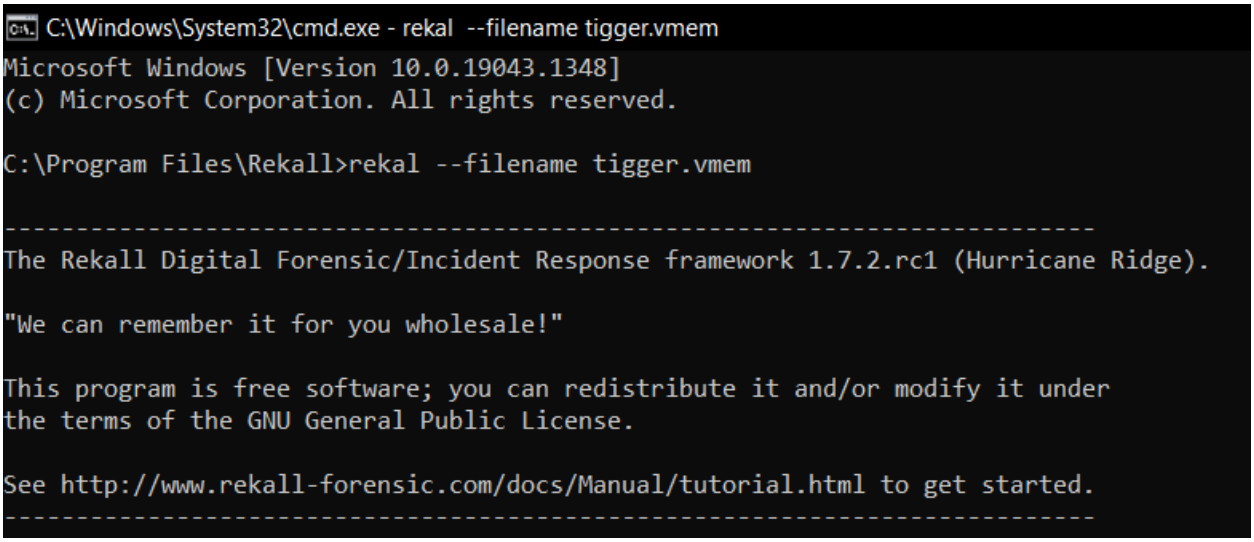
These will the key commands that we will be using to observe and analyze our Malware.

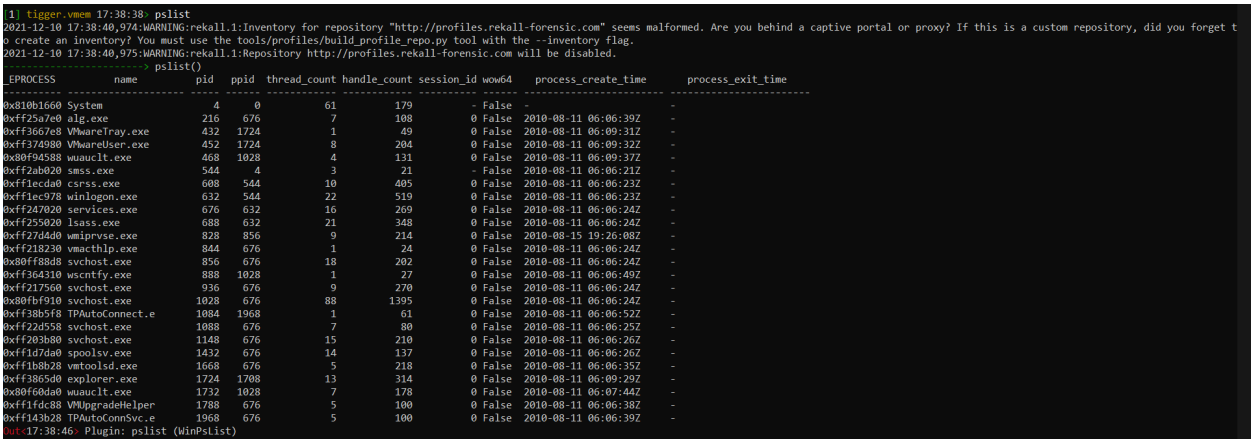
- Pslist
- Psxview
- Pstree
- Memdump
- Connscan
- Sockets
- Cmdscan
- Malfind
- Hooks_inline ####
- Netstat
- Netscan
- Procinfo
- Moddump

Malware Analyst 1: Tigger Trojan

Background: Is a Trojan that installs a rootkit to gain access to a computer for their admin privileges. It can disable windows security and steal crucial and valuable

information that is stored on the computer like web cookies, log keystrokes, and could install spy code to stalk a user's browser activity.





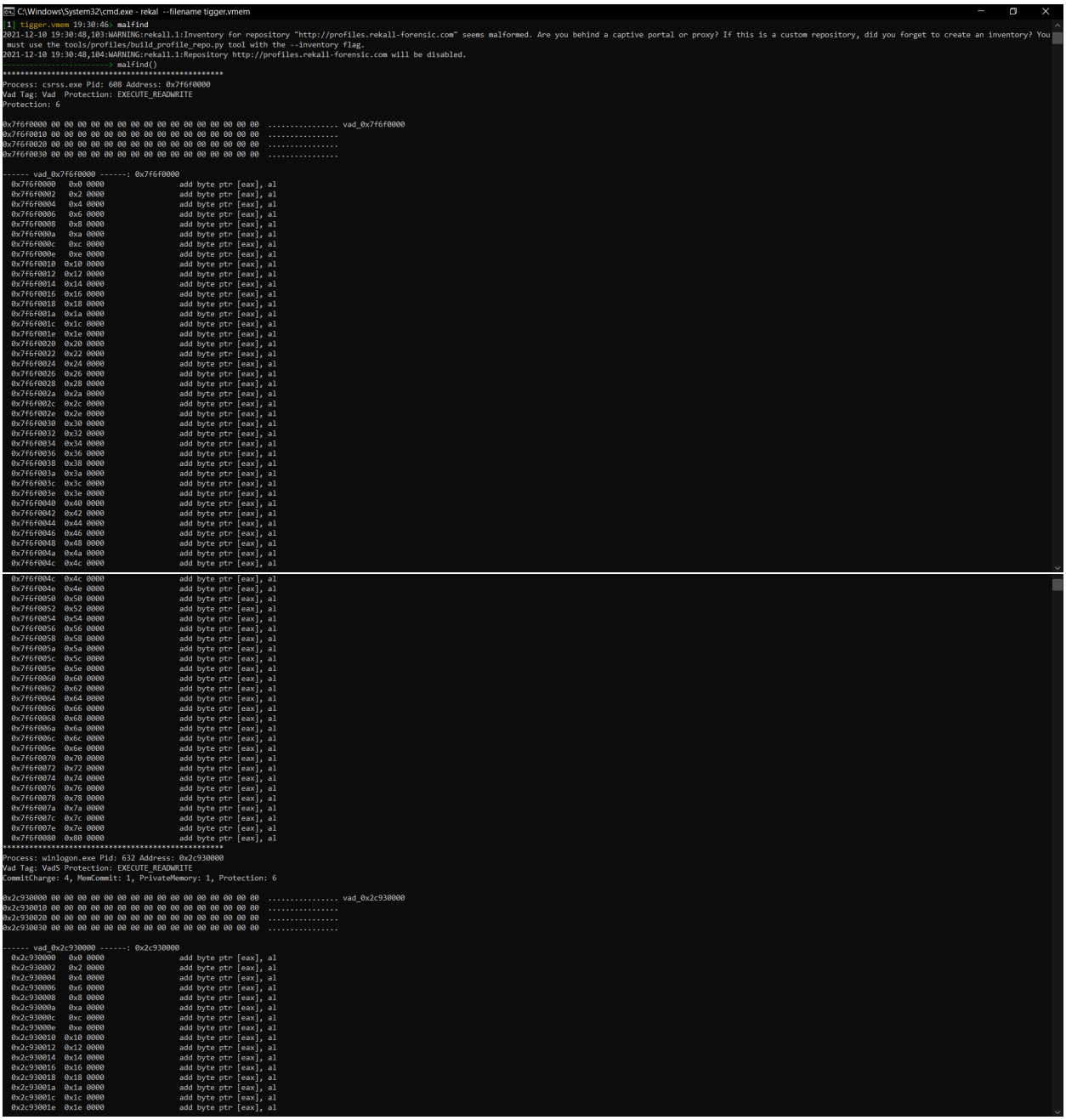
```
[1] tigger.vmem 17:44:06> connscan
----------------------> connscan()
 tcpip/GUID/9546A8399BAC4717BC41758594EF0D9C2 matched offset 0x4562+0xf3ba9000=0 offset_p      local_net_address       remote_net_address       pid
---------- ------------------------ ---------------------- ----------
 0x2214988 172.16.176.143:1034       131.107.115.254:80            1260
 0x6015ab0 172.16.176.143:1037       131.107.115.254:443           1260
Out<17:44:09> Plugin: connscan (ConnScan)
```

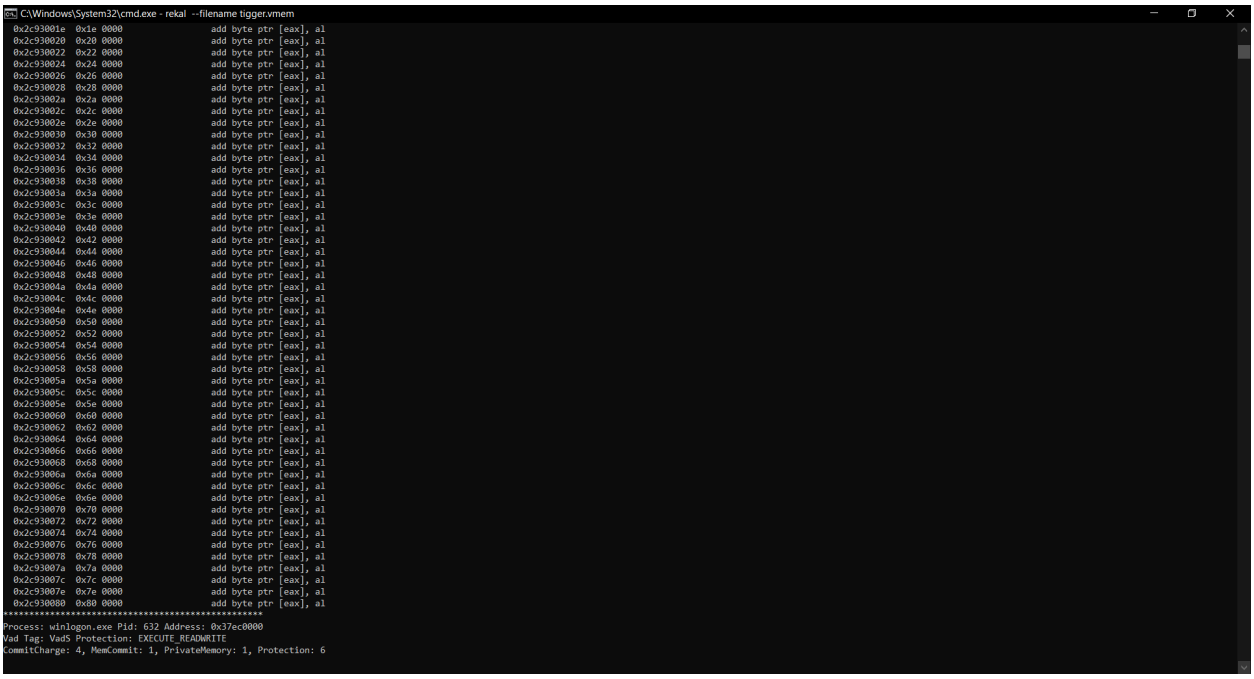
```
[1] tigger.vmem 18:02:55> pstree
------------------------> pstree()
_EPROCESS                              ppid  thd_count hnd_count       create_time
-------------------------------------- ------ --------- --------- -----------------------
  0x810b1660 System (4)                   0        61       179 -
. 0xff2ab020 smss.exe (544)               4         3        21 2010-08-11 06:06:21Z
.. 0xff1ecda0 csrss.exe (608)           544        10       405 2010-08-11 06:06:23Z
.. 0xff1ec978 winlogon.exe (632)        544        22       519 2010-08-11 06:06:23Z
... 0xff247020 services.exe (676)       632        16       269 2010-08-11 06:06:24Z
.... 0xff25a7e0 alg.exe (216)           676         7       108 2010-08-11 06:06:39Z
.... 0xff218230 vmacthlp.exe (844)      676         1        24 2010-08-11 06:06:24Z
.... 0x80ff88d8 svchost.exe (856)       676        18       202 2010-08-11 06:06:24Z
..... 0xff27d4d0 wmiprvse.exe (828)     856         9       214 2010-08-15 19:26:08Z
.... 0xff217560 svchost.exe (936)       676         9       270 2010-08-11 06:06:24Z
.... 0x80fbf910 svchost.exe (1028)      676        88      1395 2010-08-11 06:06:24Z
..... 0x80f94588 wuauclt.exe (468)     1028         4       131 2010-08-11 06:09:37Z
..... 0xff364310 wscntfy.exe (888)     1028         1        27 2010-08-11 06:06:49Z
..... 0x80f60da0 wuauclt.exe (1732)    1028         7       178 2010-08-11 06:07:44Z
.... 0xff22d558 svchost.exe (1088)      676         7        80 2010-08-11 06:06:25Z
.... 0xff203b80 svchost.exe (1148)      676        15       210 2010-08-11 06:06:26Z
.... 0xff1d7da0 spoolsv.exe (1432)      676        14       137 2010-08-11 06:06:26Z
.... 0xff1b8b28 vmtoolsd.exe (1668)     676         5       218 2010-08-11 06:06:35Z
.... 0xff1fdc88 VMUpgradeHelper (1788)  676         5       100 2010-08-11 06:06:38Z
.... 0xff143b28 TPAutoConnSvc.e (1968)  676         5       100 2010-08-11 06:06:39Z
..... 0xff38b5f8 TPAutoConnect.e (1084) 1968        1        61 2010-08-11 06:06:52Z
... 0xff255020 lsass.exe (688)          632        21       348 2010-08-11 06:06:24Z
  0xff3865d0 explorer.exe (1724)       1708        13       314 2010-08-11 06:09:29Z
. 0xff3667e8 VMwareTray.exe (432)      1724         1        49 2010-08-11 06:09:31Z
. 0xff374980 VMwareUser.exe (452)      1724         8       204 2010-08-11 06:09:32Z
Out<18:02:56> Plugin: pstree (PSTree)
[1] tigger.vmem 18:02:56>
```

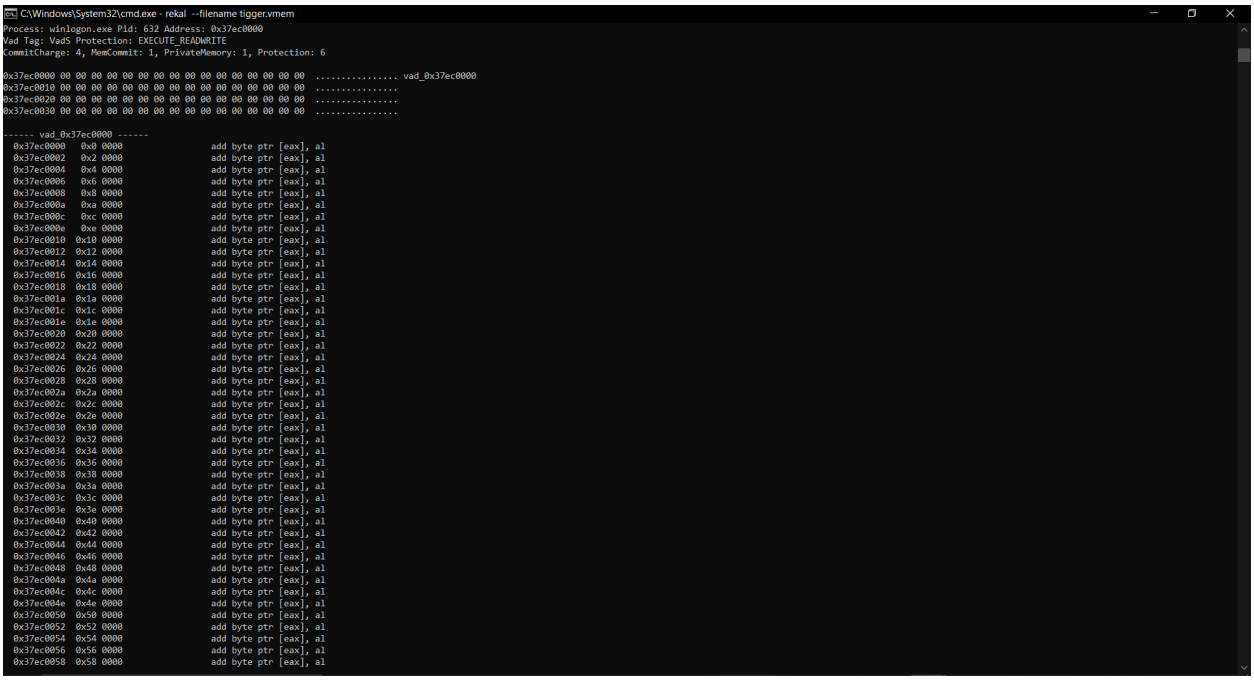
```
[1] tigger.vmem 17:47:28> sockets
------------------------> sockets()
 offset_v   pid    port  proto   protocol      address      create_time
---------- ------ ------ ------ ---------- --------------- -----------
0x80fd1008      4      0     47 GRE        0.0.0.0         2010-08-11 06:08:00Z
0xff258008    688    500     17 UDP        0.0.0.0         2010-08-11 06:06:35Z
0xff367008      4    445      6 TCP        0.0.0.0         2010-08-11 06:06:17Z
0x80ffc128    936    135      6 TCP        0.0.0.0         2010-08-11 06:06:24Z
0x80f62e98   1028   1053     17 UDP        127.0.0.1       2010-08-15 19:26:50Z
0xff225b70    688      0    255 Reserved   0.0.0.0         2010-08-11 06:06:35Z
0xff254008   1028    123     17 UDP        127.0.0.1       2010-08-15 19:26:50Z
0x80fce930   1088   1025     17 UDP        0.0.0.0         2010-08-11 06:06:38Z
0xff127d28    216   1026      6 TCP        127.0.0.1       2010-08-11 06:06:39Z
0xff12b580   1148   1900     17 UDP        127.0.0.1       2010-08-15 19:26:50Z
0xff1b8250    688   4500     17 UDP        0.0.0.0         2010-08-11 06:06:35Z
0xff382e98      4   1033      6 TCP        0.0.0.0         2010-08-11 06:08:00Z
0x80fbdc40      4    445     17 UDP        0.0.0.0         2010-08-11 06:06:17Z
Out<17:47:29> Plugin: sockets (Sockets)
```

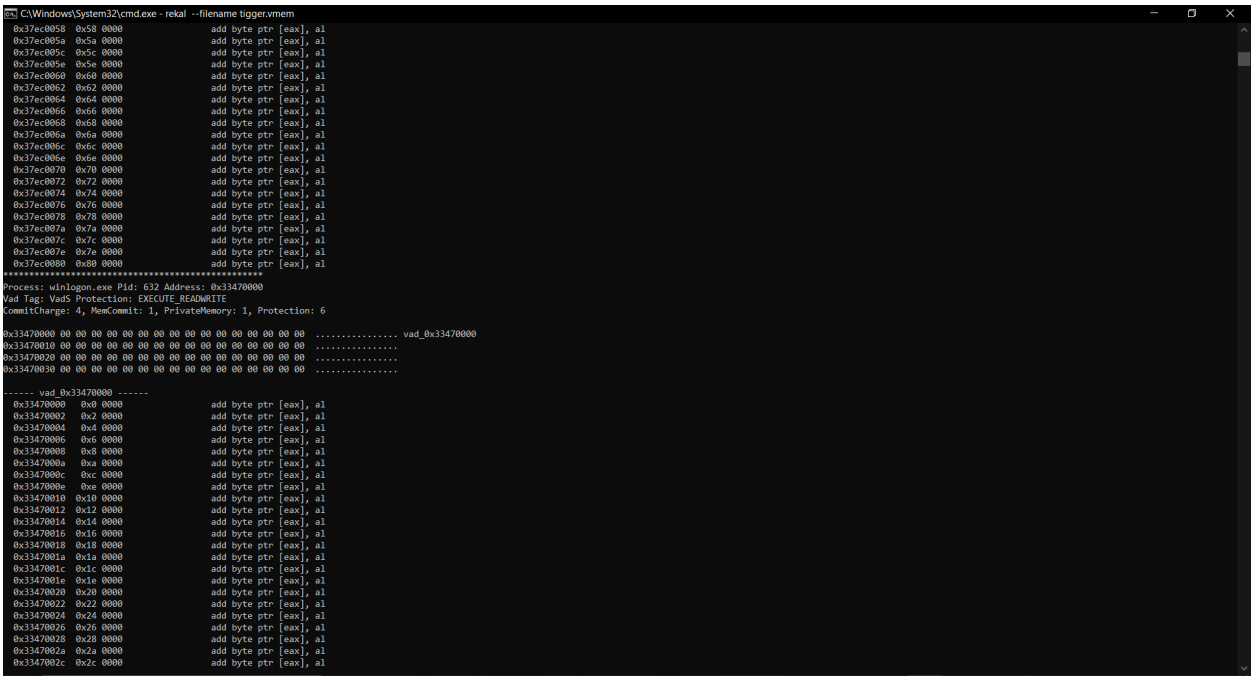
```
[1] tigger.vmem 18:05:53> psxview
----------------------> psxview()
_EPROCESS          name          pid  PsActiveProcessHead CSRSS PspCidTable Sessions Handles PSScan Thrdproc
---------- -------------------- ----- ------------------- ----- ----------- -------- ------- ------ --------
0x810b1660 System                   4 True                False True        False    False   True   True
0xff25a7e0 alg.exe                216 True                True  True        True     True    True   True
0xff3667e8 VMwareTray.exe         432 True                True  True        True     True    True   True
0xff374980 VMwareUser.exe         452 True                True  True        True     True    True   True
0x80f94588 wuauclt.exe            468 True                True  True        True     True    True   True
0xff3802c8 cmd.exe                532 False               False False       False    False   True   False
0xff2ab020 smss.exe               544 True                False True        False    True    True   True
0xff1ecda0 csrss.exe              608 True                False True        True     True    True   True
0xff1ec978 winlogon.exe           632 True                True  True        True     True    True   True
0xff247020 services.exe           676 True                True  True        True     True    True   True
0xff255020 lsass.exe              688 True                True  True        True     True    True   True
0xff27d4d0 wmiprvse.exe           828 True                True  True        True     True    True   True
0xff218230 vmacthlp.exe           844 True                True  True        True     True    True   True
0x80ff88d8 svchost.exe            856 True                True  True        True     True    True   True
0xff364310 wscntfy.exe            888 True                True  True        True     True    True   True
0xff217560 svchost.exe            936 True                True  True        True     True    True   True
0x80fbf910 svchost.exe           1028 True                True  True        True     True    True   True
0xff38b5f8 TPAutoConnect.e       1084 True                True  True        True     True    True   True
0xff22d558 svchost.exe           1088 True                True  True        True     True    True   True
0xff203b80 svchost.exe           1148 True                True  True        True     True    True   True
0xff1ebc08 logonui.exe           1168 False               False False       False    False   True   False
0xff1d7da0 spoolsv.exe           1432 True                True  True        True     True    True   True
0xff1b8b28 vmtoolsd.exe          1668 True                True  True        True     True    True   True
0xff3865d0 explorer.exe          1724 True                True  True        True     True    True   True
0x80f60da0 wuauclt.exe           1732 True                True  True        True     True    True   True
0xff1fdc88 VMUpgradeHelper       1788 True                True  True        True     True    True   True
0xff143b28 TPAutoConnSvc.e       1968 True                True  True        True     True    True   True
Out<18:05:58> Plugin: psxview (WindowsPsxView)
[1] tigger.vmem 18:05:58>
```

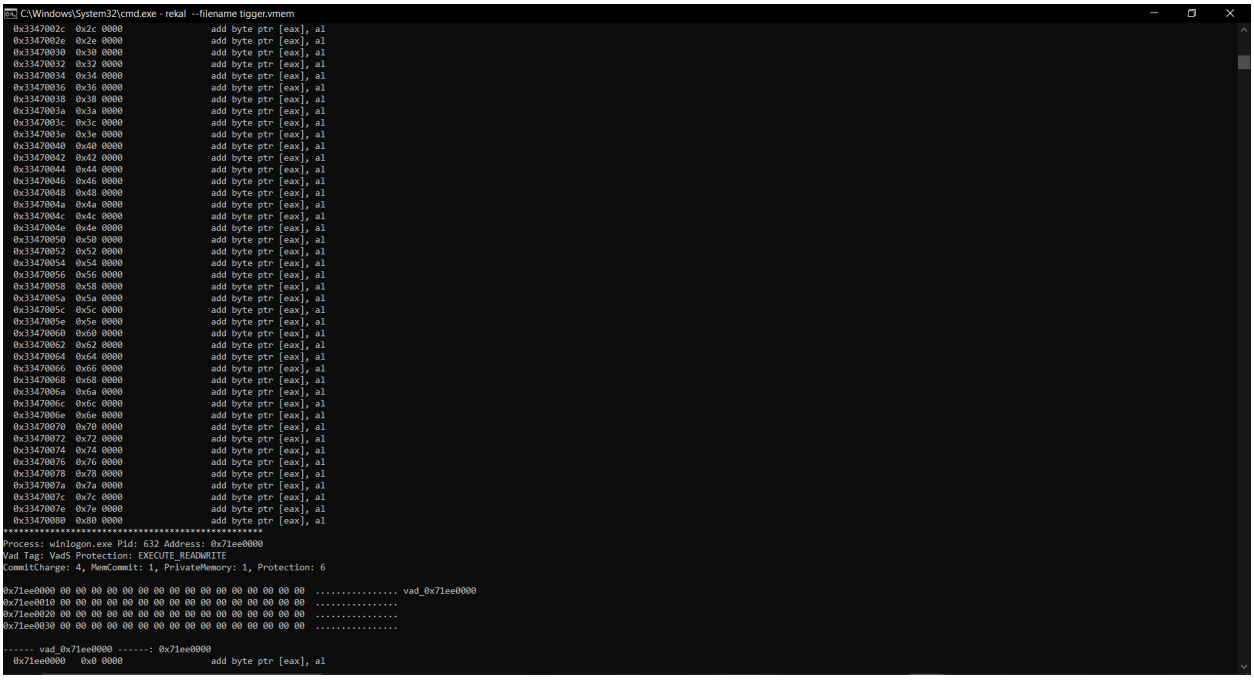
```
[1] tigger.vmem 19:40:45> hooks_iat 1028
----------------------> hooks_iat(1028)
         source                target        target_func
  -------------------- -------------------- -----------
--------------------------
Process svchost.exe (1028)
--------------------------
Out<19:40:46> Plugin: hooks_iat (IATHooks)
[1] tigger.vmem 19:40:46>
```

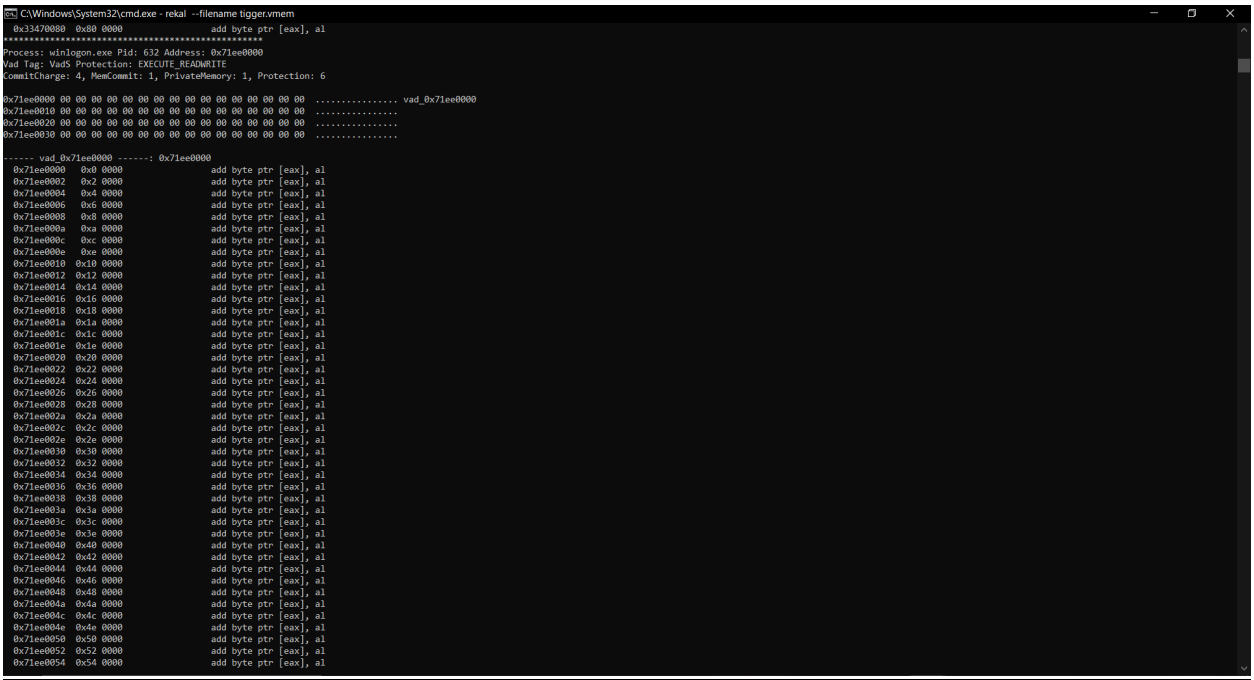

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
[1] tigger.vmem 19:30:46> malfind
2021-12-10 19:30:48,103:WARNING:rekall.1:Inventory for repository "http://profiles.rekall-forensic.com" seems malformed. Are you behind a captive portal or proxy? If this is a custom repository, did you forget to create an inventory? You must use the tools/profiles/build_profile_repo.py tool with the --inventory flag.
2021-12-10 19:30:48,104:WARNING:rekall.1:Repository http://profiles.rekall-forensic.com will be disabled.
[1] tigger.vmem 19:30:48> malfind()
****
Process: csrss.exe Pid: 608 Address: 0x7f6f0000
Vad Tag: Vad Protection: EXECUTE_READWRITE
Protection: 6
0x7f6f0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... vad_0x7f6f0000
0x7f6f0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x7f6f0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x7f6f0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
------ vad_0x7f6f0000 ------: 0x7f6f0000
0x7f6f0000 0x0 0000 add byte ptr [eax], al
0x7f6f0002 0x2 0000 add byte ptr [eax], al
0x7f6f0004 0x4 0000 add byte ptr [eax], al
0x7f6f0006 0x6 0000 add byte ptr [eax], al
0x7f6f0008 0x8 0000 add byte ptr [eax], al
0x7f6f000a 0xa 0000 add byte ptr [eax], al
0x7f6f000c 0xc 0000 add byte ptr [eax], al
0x7f6f000e 0xe 0000 add byte ptr [eax], al
0x7f6f0010 0x10 0000 add byte ptr [eax], al
0x7f6f0012 0x12 0000 add byte ptr [eax], al
0x7f6f0014 0x14 0000 add byte ptr [eax], al
0x7f6f0016 0x16 0000 add byte ptr [eax], al
0x7f6f0018 0x18 0000 add byte ptr [eax], al
0x7f6f001a 0x1a 0000 add byte ptr [eax], al
0x7f6f001c 0x1c 0000 add byte ptr [eax], al
0x7f6f001e 0x1e 0000 add byte ptr [eax], al
0x7f6f0020 0x20 0000 add byte ptr [eax], al
0x7f6f0022 0x22 0000 add byte ptr [eax], al
0x7f6f0024 0x24 0000 add byte ptr [eax], al
0x7f6f0026 0x26 0000 add byte ptr [eax], al
0x7f6f0028 0x28 0000 add byte ptr [eax], al
0x7f6f002a 0x2a 0000 add byte ptr [eax], al
0x7f6f002c 0x2c 0000 add byte ptr [eax], al
0x7f6f002e 0x2e 0000 add byte ptr [eax], al
0x7f6f0030 0x30 0000 add byte ptr [eax], al
0x7f6f0032 0x32 0000 add byte ptr [eax], al
0x7f6f0034 0x34 0000 add byte ptr [eax], al
0x7f6f0036 0x36 0000 add byte ptr [eax], al
0x7f6f0038 0x38 0000 add byte ptr [eax], al
0x7f6f003a 0x3a 0000 add byte ptr [eax], al
0x7f6f003c 0x3c 0000 add byte ptr [eax], al
0x7f6f003e 0x3e 0000 add byte ptr [eax], al
0x7f6f0040 0x40 0000 add byte ptr [eax], al
0x7f6f0042 0x42 0000 add byte ptr [eax], al
0x7f6f0044 0x44 0000 add byte ptr [eax], al
0x7f6f0046 0x46 0000 add byte ptr [eax], al
0x7f6f0048 0x48 0000 add byte ptr [eax], al
0x7f6f004a 0x4a 0000 add byte ptr [eax], al
0x7f6f004c 0x4c 0000 add byte ptr [eax], al
0x7f6f004c 0x4c 0000 add byte ptr [eax], al
0x7f6f004e 0x4e 0000 add byte ptr [eax], al
0x7f6f0050 0x50 0000 add byte ptr [eax], al
0x7f6f0052 0x52 0000 add byte ptr [eax], al
0x7f6f0054 0x54 0000 add byte ptr [eax], al
0x7f6f0056 0x56 0000 add byte ptr [eax], al
0x7f6f0058 0x58 0000 add byte ptr [eax], al
0x7f6f005a 0x5a 0000 add byte ptr [eax], al
0x7f6f005c 0x5c 0000 add byte ptr [eax], al
0x7f6f005e 0x5e 0000 add byte ptr [eax], al
0x7f6f0060 0x60 0000 add byte ptr [eax], al
0x7f6f0062 0x62 0000 add byte ptr [eax], al
0x7f6f0064 0x64 0000 add byte ptr [eax], al
0x7f6f0066 0x66 0000 add byte ptr [eax], al
0x7f6f0068 0x68 0000 add byte ptr [eax], al
0x7f6f006a 0x6a 0000 add byte ptr [eax], al
0x7f6f006c 0x6c 0000 add byte ptr [eax], al
0x7f6f006e 0x6e 0000 add byte ptr [eax], al
0x7f6f0070 0x70 0000 add byte ptr [eax], al
0x7f6f0072 0x72 0000 add byte ptr [eax], al
0x7f6f0074 0x74 0000 add byte ptr [eax], al
0x7f6f0076 0x76 0000 add byte ptr [eax], al
0x7f6f0078 0x78 0000 add byte ptr [eax], al
0x7f6f007a 0x7a 0000 add byte ptr [eax], al
0x7f6f007c 0x7c 0000 add byte ptr [eax], al
0x7f6f007e 0x7e 0000 add byte ptr [eax], al
0x7f6f0080 0x80 0000 add byte ptr [eax], al
****
Process: winlogon.exe Pid: 632 Address: 0x2c930000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x2c930000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... vad_0x2c930000
0x2c930010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x2c930020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x2c930030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
------ vad_0x2c930000 ------: 0x2c930000
0x2c930000 0x0 0000 add byte ptr [eax], al
0x2c930002 0x2 0000 add byte ptr [eax], al
0x2c930004 0x4 0000 add byte ptr [eax], al
0x2c930006 0x6 0000 add byte ptr [eax], al
0x2c930008 0x8 0000 add byte ptr [eax], al
0x2c93000a 0xa 0000 add byte ptr [eax], al
0x2c93000c 0xc 0000 add byte ptr [eax], al
0x2c93000e 0xe 0000 add byte ptr [eax], al
0x2c930010 0x10 0000 add byte ptr [eax], al
0x2c930012 0x12 0000 add byte ptr [eax], al
0x2c930014 0x14 0000 add byte ptr [eax], al
0x2c930016 0x16 0000 add byte ptr [eax], al
0x2c930018 0x18 0000 add byte ptr [eax], al
0x2c93001a 0x1a 0000 add byte ptr [eax], al
0x2c93001c 0x1c 0000 add byte ptr [eax], al
0x2c93001e 0x1e 0000 add byte ptr [eax], al

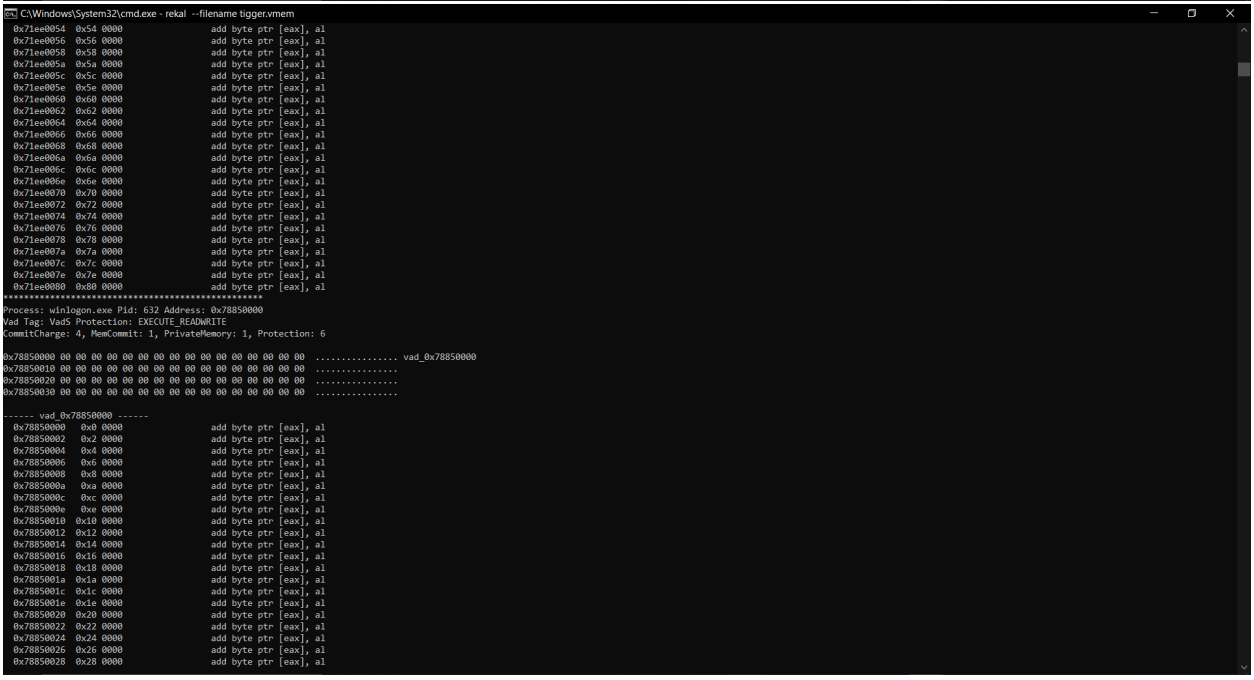

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x2c93001e 0x1e 0000 add byte ptr [eax], al
0x2c930020 0x20 0000 add byte ptr [eax], al
0x2c930022 0x22 0000 add byte ptr [eax], al
0x2c930024 0x24 0000 add byte ptr [eax], al
0x2c930026 0x26 0000 add byte ptr [eax], al
0x2c930028 0x28 0000 add byte ptr [eax], al
0x2c93002a 0x2a 0000 add byte ptr [eax], al
0x2c93002c 0x2c 0000 add byte ptr [eax], al
0x2c93002e 0x2e 0000 add byte ptr [eax], al
0x2c930030 0x30 0000 add byte ptr [eax], al
0x2c930032 0x32 0000 add byte ptr [eax], al
0x2c930034 0x34 0000 add byte ptr [eax], al
0x2c930036 0x36 0000 add byte ptr [eax], al
0x2c930038 0x38 0000 add byte ptr [eax], al
0x2c93003a 0x3a 0000 add byte ptr [eax], al
0x2c93003c 0x3c 0000 add byte ptr [eax], al
0x2c93003e 0x3e 0000 add byte ptr [eax], al
0x2c930040 0x40 0000 add byte ptr [eax], al
0x2c930042 0x42 0000 add byte ptr [eax], al
0x2c930044 0x44 0000 add byte ptr [eax], al
0x2c930046 0x46 0000 add byte ptr [eax], al
0x2c930048 0x48 0000 add byte ptr [eax], al
0x2c93004a 0x4a 0000 add byte ptr [eax], al
0x2c93004c 0x4c 0000 add byte ptr [eax], al
0x2c93004e 0x4e 0000 add byte ptr [eax], al
0x2c930050 0x50 0000 add byte ptr [eax], al
0x2c930052 0x52 0000 add byte ptr [eax], al
0x2c930054 0x54 0000 add byte ptr [eax], al
0x2c930056 0x56 0000 add byte ptr [eax], al
0x2c930058 0x58 0000 add byte ptr [eax], al
0x2c93005a 0x5a 0000 add byte ptr [eax], al
0x2c93005c 0x5c 0000 add byte ptr [eax], al
0x2c93005e 0x5e 0000 add byte ptr [eax], al
0x2c930060 0x60 0000 add byte ptr [eax], al
0x2c930062 0x62 0000 add byte ptr [eax], al
0x2c930064 0x64 0000 add byte ptr [eax], al
0x2c930066 0x66 0000 add byte ptr [eax], al
0x2c930068 0x68 0000 add byte ptr [eax], al
0x2c93006a 0x6a 0000 add byte ptr [eax], al
0x2c93006c 0x6c 0000 add byte ptr [eax], al
0x2c93006e 0x6e 0000 add byte ptr [eax], al
0x2c930070 0x70 0000 add byte ptr [eax], al
0x2c930072 0x72 0000 add byte ptr [eax], al
0x2c930074 0x74 0000 add byte ptr [eax], al
0x2c930076 0x76 0000 add byte ptr [eax], al
0x2c930078 0x78 0000 add byte ptr [eax], al
0x2c93007a 0x7a 0000 add byte ptr [eax], al
0x2c93007c 0x7c 0000 add byte ptr [eax], al
0x2c93007e 0x7e 0000 add byte ptr [eax], al
0x2c930080 0x80 0000 add byte ptr [eax], al
****
Process: winlogon.exe Pid: 632 Address: 0x37ec0000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6

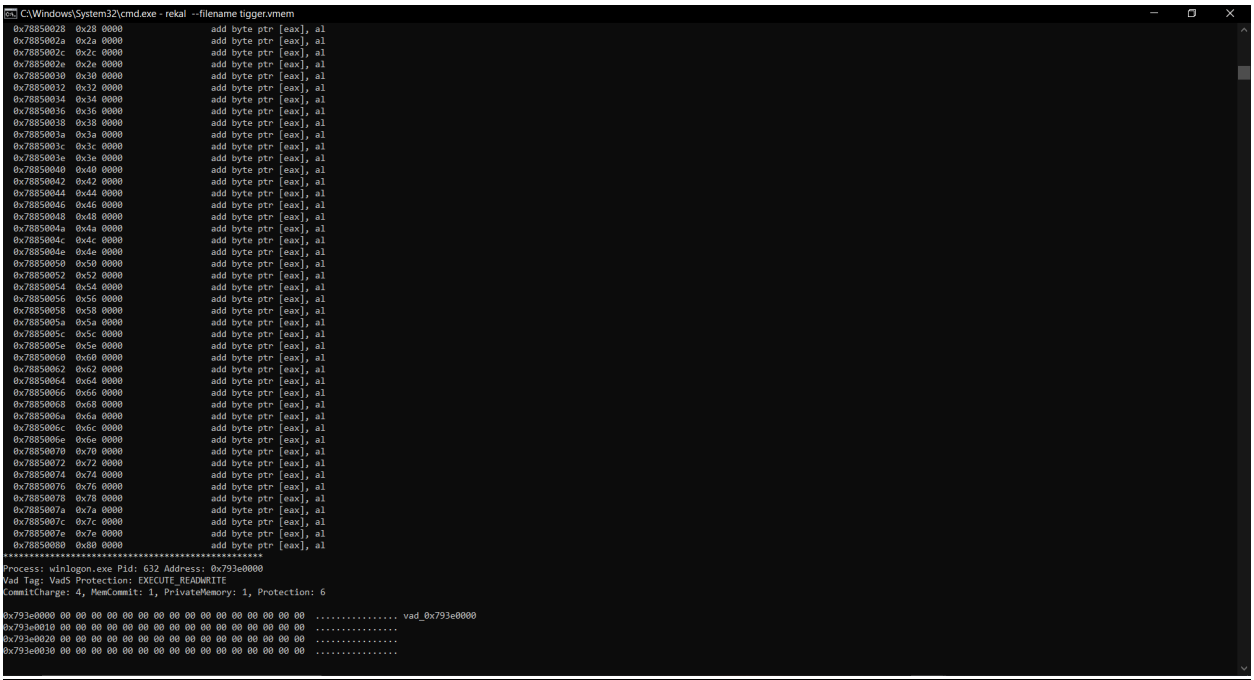

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
Process: winlogon.exe Pid: 632 Address: 0x37ec0000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x37ec0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... vad_0x37ec0000
0x37ec0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x37ec0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x37ec0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
----- vad_0x37ec0000 -----
0x37ec0000 0x0 0000 add byte ptr [eax], al
0x37ec0002 0x2 0000 add byte ptr [eax], al
0x37ec0004 0x4 0000 add byte ptr [eax], al
0x37ec0006 0x6 0000 add byte ptr [eax], al
0x37ec0008 0x8 0000 add byte ptr [eax], al
0x37ec000a 0xa 0000 add byte ptr [eax], al
0x37ec000c 0xc 0000 add byte ptr [eax], al
0x37ec000e 0xe 0000 add byte ptr [eax], al
0x37ec0010 0x10 0000 add byte ptr [eax], al
0x37ec0012 0x12 0000 add byte ptr [eax], al
0x37ec0014 0x14 0000 add byte ptr [eax], al
0x37ec0016 0x16 0000 add byte ptr [eax], al
0x37ec0018 0x18 0000 add byte ptr [eax], al
0x37ec001a 0x1a 0000 add byte ptr [eax], al
0x37ec001c 0x1c 0000 add byte ptr [eax], al
0x37ec001e 0x1e 0000 add byte ptr [eax], al
0x37ec0020 0x20 0000 add byte ptr [eax], al
0x37ec0022 0x22 0000 add byte ptr [eax], al
0x37ec0024 0x24 0000 add byte ptr [eax], al
0x37ec0026 0x26 0000 add byte ptr [eax], al
0x37ec0028 0x28 0000 add byte ptr [eax], al
0x37ec002a 0x2a 0000 add byte ptr [eax], al
0x37ec002c 0x2c 0000 add byte ptr [eax], al
0x37ec002e 0x2e 0000 add byte ptr [eax], al
0x37ec0030 0x30 0000 add byte ptr [eax], al
0x37ec0032 0x32 0000 add byte ptr [eax], al
0x37ec0034 0x34 0000 add byte ptr [eax], al
0x37ec0036 0x36 0000 add byte ptr [eax], al
0x37ec0038 0x38 0000 add byte ptr [eax], al
0x37ec003a 0x3a 0000 add byte ptr [eax], al
0x37ec003c 0x3c 0000 add byte ptr [eax], al
0x37ec003e 0x3e 0000 add byte ptr [eax], al
0x37ec0040 0x40 0000 add byte ptr [eax], al
0x37ec0042 0x42 0000 add byte ptr [eax], al
0x37ec0044 0x44 0000 add byte ptr [eax], al
0x37ec0046 0x46 0000 add byte ptr [eax], al
0x37ec0048 0x48 0000 add byte ptr [eax], al
0x37ec004a 0x4a 0000 add byte ptr [eax], al
0x37ec004c 0x4c 0000 add byte ptr [eax], al
0x37ec004e 0x4e 0000 add byte ptr [eax], al
0x37ec0050 0x50 0000 add byte ptr [eax], al
0x37ec0052 0x52 0000 add byte ptr [eax], al
0x37ec0054 0x54 0000 add byte ptr [eax], al
0x37ec0056 0x56 0000 add byte ptr [eax], al
0x37ec0058 0x58 0000 add byte ptr [eax], al

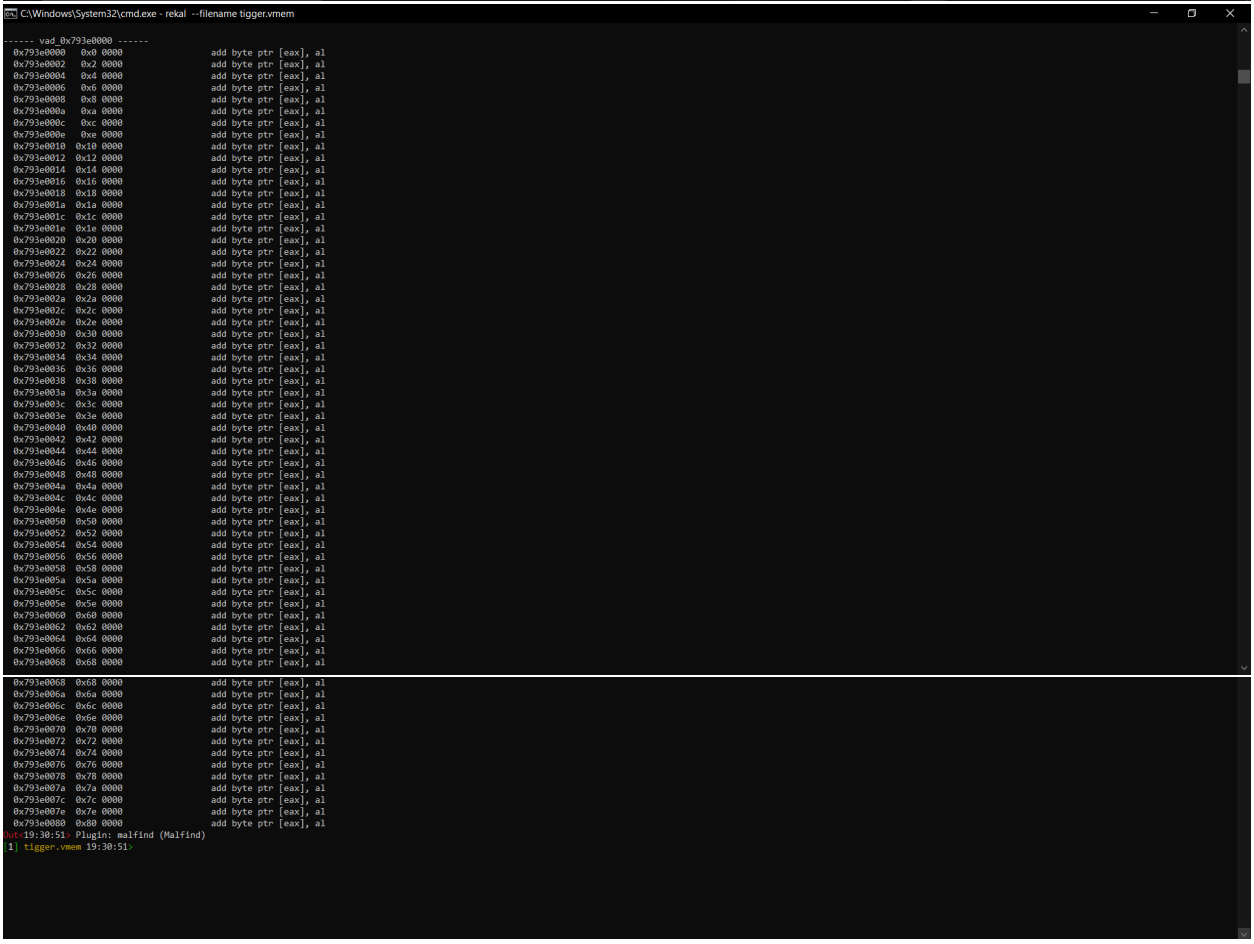

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x37ec0058 0x58 0000 add byte ptr [eax], al
0x37ec005a 0x5a 0000 add byte ptr [eax], al
0x37ec005c 0x5c 0000 add byte ptr [eax], al
0x37ec005e 0x5e 0000 add byte ptr [eax], al
0x37ec0060 0x60 0000 add byte ptr [eax], al
0x37ec0062 0x62 0000 add byte ptr [eax], al
0x37ec0064 0x64 0000 add byte ptr [eax], al
0x37ec0066 0x66 0000 add byte ptr [eax], al
0x37ec0068 0x68 0000 add byte ptr [eax], al
0x37ec006a 0x6a 0000 add byte ptr [eax], al
0x37ec006c 0x6c 0000 add byte ptr [eax], al
0x37ec006e 0x6e 0000 add byte ptr [eax], al
0x37ec0070 0x70 0000 add byte ptr [eax], al
0x37ec0072 0x72 0000 add byte ptr [eax], al
0x37ec0074 0x74 0000 add byte ptr [eax], al
0x37ec0076 0x76 0000 add byte ptr [eax], al
0x37ec0078 0x78 0000 add byte ptr [eax], al
0x37ec007a 0x7a 0000 add byte ptr [eax], al
0x37ec007c 0x7c 0000 add byte ptr [eax], al
0x37ec007e 0x7e 0000 add byte ptr [eax], al
0x37ec0080 0x80 0000 add byte ptr [eax], al
****
Process: winlogon.exe Pid: 632 Address: 0x33470000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x33470000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... vad_0x33470000
0x33470010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x33470020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x33470030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
----- vad_0x33470000 -----
0x33470000 0x0 0000 add byte ptr [eax], al
0x33470002 0x2 0000 add byte ptr [eax], al
0x33470004 0x4 0000 add byte ptr [eax], al
0x33470006 0x6 0000 add byte ptr [eax], al
0x33470008 0x8 0000 add byte ptr [eax], al
0x3347000a 0xa 0000 add byte ptr [eax], al
0x3347000c 0xc 0000 add byte ptr [eax], al
0x3347000e 0xe 0000 add byte ptr [eax], al
0x33470010 0x10 0000 add byte ptr [eax], al
0x33470012 0x12 0000 add byte ptr [eax], al
0x33470014 0x14 0000 add byte ptr [eax], al
0x33470016 0x16 0000 add byte ptr [eax], al
0x33470018 0x18 0000 add byte ptr [eax], al
0x3347001a 0x1a 0000 add byte ptr [eax], al
0x3347001c 0x1c 0000 add byte ptr [eax], al
0x3347001e 0x1e 0000 add byte ptr [eax], al
0x33470020 0x20 0000 add byte ptr [eax], al
0x33470022 0x22 0000 add byte ptr [eax], al
0x33470024 0x24 0000 add byte ptr [eax], al
0x33470026 0x26 0000 add byte ptr [eax], al
0x33470028 0x28 0000 add byte ptr [eax], al
0x3347002a 0x2a 0000 add byte ptr [eax], al
0x3347002c 0x2c 0000 add byte ptr [eax], al


C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x3347002c 0x2c 0000 add byte ptr [eax], al
0x3347002e 0x2e 0000 add byte ptr [eax], al
0x33470030 0x30 0000 add byte ptr [eax], al
0x33470032 0x32 0000 add byte ptr [eax], al
0x33470034 0x34 0000 add byte ptr [eax], al
0x33470036 0x36 0000 add byte ptr [eax], al
0x33470038 0x38 0000 add byte ptr [eax], al
0x3347003a 0x3a 0000 add byte ptr [eax], al
0x3347003c 0x3c 0000 add byte ptr [eax], al
0x3347003e 0x3e 0000 add byte ptr [eax], al
0x33470040 0x40 0000 add byte ptr [eax], al
0x33470042 0x42 0000 add byte ptr [eax], al
0x33470044 0x44 0000 add byte ptr [eax], al
0x33470046 0x46 0000 add byte ptr [eax], al
0x33470048 0x48 0000 add byte ptr [eax], al
0x3347004a 0x4a 0000 add byte ptr [eax], al
0x3347004c 0x4c 0000 add byte ptr [eax], al
0x3347004e 0x4e 0000 add byte ptr [eax], al
0x33470050 0x50 0000 add byte ptr [eax], al
0x33470052 0x52 0000 add byte ptr [eax], al
0x33470054 0x54 0000 add byte ptr [eax], al
0x33470056 0x56 0000 add byte ptr [eax], al
0x33470058 0x58 0000 add byte ptr [eax], al
0x3347005a 0x5a 0000 add byte ptr [eax], al
0x3347005c 0x5c 0000 add byte ptr [eax], al
0x3347005e 0x5e 0000 add byte ptr [eax], al
0x33470060 0x60 0000 add byte ptr [eax], al
0x33470062 0x62 0000 add byte ptr [eax], al
0x33470064 0x64 0000 add byte ptr [eax], al
0x33470066 0x66 0000 add byte ptr [eax], al
0x33470068 0x68 0000 add byte ptr [eax], al
0x3347006a 0x6a 0000 add byte ptr [eax], al
0x3347006c 0x6c 0000 add byte ptr [eax], al
0x3347006e 0x6e 0000 add byte ptr [eax], al
0x33470070 0x70 0000 add byte ptr [eax], al
0x33470072 0x72 0000 add byte ptr [eax], al
0x33470074 0x74 0000 add byte ptr [eax], al
0x33470076 0x76 0000 add byte ptr [eax], al
0x33470078 0x78 0000 add byte ptr [eax], al
0x3347007a 0x7a 0000 add byte ptr [eax], al
0x3347007c 0x7c 0000 add byte ptr [eax], al
0x3347007e 0x7e 0000 add byte ptr [eax], al
0x33470080 0x80 0000 add byte ptr [eax], al
****
Process: winlogon.exe Pid: 632 Address: 0x71ee0000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x71ee0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... vad_0x71ee0000
0x71ee0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x71ee0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x71ee0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
----- vad_0x71ee0000 ------: 0x71ee0000
0x71ee0000 0x0 0000 add byte ptr [eax], al


C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x33470080 0x80 0000 add byte ptr [eax], al
****
Process: winlogon.exe Pid: 632 Address: 0x71ee0000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x71ee0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x71ee0000
0x71ee0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x71ee0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x71ee0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
----- vad_0x71ee0000 -----: 0x71ee0000
0x71ee0000 0x0 0000 add byte ptr [eax], al
0x71ee0002 0x2 0000 add byte ptr [eax], al
0x71ee0004 0x4 0000 add byte ptr [eax], al
0x71ee0006 0x6 0000 add byte ptr [eax], al
0x71ee0008 0x8 0000 add byte ptr [eax], al
0x71ee000a 0xa 0000 add byte ptr [eax], al
0x71ee000c 0xc 0000 add byte ptr [eax], al
0x71ee000e 0xe 0000 add byte ptr [eax], al
0x71ee0010 0x10 0000 add byte ptr [eax], al
0x71ee0012 0x12 0000 add byte ptr [eax], al
0x71ee0014 0x14 0000 add byte ptr [eax], al
0x71ee0016 0x16 0000 add byte ptr [eax], al
0x71ee0018 0x18 0000 add byte ptr [eax], al
0x71ee001a 0x1a 0000 add byte ptr [eax], al
0x71ee001c 0x1c 0000 add byte ptr [eax], al
0x71ee001e 0x1e 0000 add byte ptr [eax], al
0x71ee0020 0x20 0000 add byte ptr [eax], al
0x71ee0022 0x22 0000 add byte ptr [eax], al
0x71ee0024 0x24 0000 add byte ptr [eax], al
0x71ee0026 0x26 0000 add byte ptr [eax], al
0x71ee0028 0x28 0000 add byte ptr [eax], al
0x71ee002a 0x2a 0000 add byte ptr [eax], al
0x71ee002c 0x2c 0000 add byte ptr [eax], al
0x71ee002e 0x2e 0000 add byte ptr [eax], al
0x71ee0030 0x30 0000 add byte ptr [eax], al
0x71ee0032 0x32 0000 add byte ptr [eax], al
0x71ee0034 0x34 0000 add byte ptr [eax], al
0x71ee0036 0x36 0000 add byte ptr [eax], al
0x71ee0038 0x38 0000 add byte ptr [eax], al
0x71ee003a 0x3a 0000 add byte ptr [eax], al
0x71ee003c 0x3c 0000 add byte ptr [eax], al
0x71ee003e 0x3e 0000 add byte ptr [eax], al
0x71ee0040 0x40 0000 add byte ptr [eax], al
0x71ee0042 0x42 0000 add byte ptr [eax], al
0x71ee0044 0x44 0000 add byte ptr [eax], al
0x71ee0046 0x46 0000 add byte ptr [eax], al
0x71ee0048 0x48 0000 add byte ptr [eax], al
0x71ee004a 0x4a 0000 add byte ptr [eax], al
0x71ee004c 0x4c 0000 add byte ptr [eax], al
0x71ee004e 0x4e 0000 add byte ptr [eax], al
0x71ee0050 0x50 0000 add byte ptr [eax], al
0x71ee0052 0x52 0000 add byte ptr [eax], al
0x71ee0054 0x54 0000 add byte ptr [eax], al


C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x71ee0054 0x54 0000 add byte ptr [eax], al
0x71ee0056 0x56 0000 add byte ptr [eax], al
0x71ee0058 0x58 0000 add byte ptr [eax], al
0x71ee005a 0x5a 0000 add byte ptr [eax], al
0x71ee005c 0x5c 0000 add byte ptr [eax], al
0x71ee005e 0x5e 0000 add byte ptr [eax], al
0x71ee0060 0x60 0000 add byte ptr [eax], al
0x71ee0062 0x62 0000 add byte ptr [eax], al
0x71ee0064 0x64 0000 add byte ptr [eax], al
0x71ee0066 0x66 0000 add byte ptr [eax], al
0x71ee0068 0x68 0000 add byte ptr [eax], al
0x71ee006a 0x6a 0000 add byte ptr [eax], al
0x71ee006c 0x6c 0000 add byte ptr [eax], al
0x71ee006e 0x6e 0000 add byte ptr [eax], al
0x71ee0070 0x70 0000 add byte ptr [eax], al
0x71ee0072 0x72 0000 add byte ptr [eax], al
0x71ee0074 0x74 0000 add byte ptr [eax], al
0x71ee0076 0x76 0000 add byte ptr [eax], al
0x71ee0078 0x78 0000 add byte ptr [eax], al
0x71ee007a 0x7a 0000 add byte ptr [eax], al
0x71ee007c 0x7c 0000 add byte ptr [eax], al
0x71ee007e 0x7e 0000 add byte ptr [eax], al
0x71ee0080 0x80 0000 add byte ptr [eax], al
****
Process: winlogon.exe Pid: 632 Address: 0x78850000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x78850000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x78850000
0x78850010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x78850020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x78850030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
----- vad_0x78850000 -----
0x78850000 0x0 0000 add byte ptr [eax], al
0x78850002 0x2 0000 add byte ptr [eax], al
0x78850004 0x4 0000 add byte ptr [eax], al
0x78850006 0x6 0000 add byte ptr [eax], al
0x78850008 0x8 0000 add byte ptr [eax], al
0x7885000a 0xa 0000 add byte ptr [eax], al
0x7885000c 0xc 0000 add byte ptr [eax], al
0x7885000e 0xe 0000 add byte ptr [eax], al
0x78850010 0x10 0000 add byte ptr [eax], al
0x78850012 0x12 0000 add byte ptr [eax], al
0x78850014 0x14 0000 add byte ptr [eax], al
0x78850016 0x16 0000 add byte ptr [eax], al
0x78850018 0x18 0000 add byte ptr [eax], al
0x7885001a 0x1a 0000 add byte ptr [eax], al
0x7885001c 0x1c 0000 add byte ptr [eax], al
0x7885001e 0x1e 0000 add byte ptr [eax], al
0x78850020 0x20 0000 add byte ptr [eax], al
0x78850022 0x22 0000 add byte ptr [eax], al
0x78850024 0x24 0000 add byte ptr [eax], al
0x78850026 0x26 0000 add byte ptr [eax], al
0x78850028 0x28 0000 add byte ptr [eax], al


C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x78850028 0x28 0000 add byte ptr [eax], al
0x7885002a 0x2a 0000 add byte ptr [eax], al
0x7885002c 0x2c 0000 add byte ptr [eax], al
0x7885002e 0x2e 0000 add byte ptr [eax], al
0x78850030 0x30 0000 add byte ptr [eax], al
0x78850032 0x32 0000 add byte ptr [eax], al
0x78850034 0x34 0000 add byte ptr [eax], al
0x78850036 0x36 0000 add byte ptr [eax], al
0x78850038 0x38 0000 add byte ptr [eax], al
0x7885003a 0x3a 0000 add byte ptr [eax], al
0x7885003c 0x3c 0000 add byte ptr [eax], al
0x7885003e 0x3e 0000 add byte ptr [eax], al
0x78850040 0x40 0000 add byte ptr [eax], al
0x78850042 0x42 0000 add byte ptr [eax], al
0x78850044 0x44 0000 add byte ptr [eax], al
0x78850046 0x46 0000 add byte ptr [eax], al
0x78850048 0x48 0000 add byte ptr [eax], al
0x7885004a 0x4a 0000 add byte ptr [eax], al
0x7885004c 0x4c 0000 add byte ptr [eax], al
0x7885004e 0x4e 0000 add byte ptr [eax], al
0x78850050 0x50 0000 add byte ptr [eax], al
0x78850052 0x52 0000 add byte ptr [eax], al
0x78850054 0x54 0000 add byte ptr [eax], al
0x78850056 0x56 0000 add byte ptr [eax], al
0x78850058 0x58 0000 add byte ptr [eax], al
0x7885005a 0x5a 0000 add byte ptr [eax], al
0x7885005c 0x5c 0000 add byte ptr [eax], al
0x7885005e 0x5e 0000 add byte ptr [eax], al
0x78850060 0x60 0000 add byte ptr [eax], al
0x78850062 0x62 0000 add byte ptr [eax], al
0x78850064 0x64 0000 add byte ptr [eax], al
0x78850066 0x66 0000 add byte ptr [eax], al
0x78850068 0x68 0000 add byte ptr [eax], al
0x7885006a 0x6a 0000 add byte ptr [eax], al
0x7885006c 0x6c 0000 add byte ptr [eax], al
0x7885006e 0x6e 0000 add byte ptr [eax], al
0x78850070 0x70 0000 add byte ptr [eax], al
0x78850072 0x72 0000 add byte ptr [eax], al
0x78850074 0x74 0000 add byte ptr [eax], al
0x78850076 0x76 0000 add byte ptr [eax], al
0x78850078 0x78 0000 add byte ptr [eax], al
0x7885007a 0x7a 0000 add byte ptr [eax], al
0x7885007c 0x7c 0000 add byte ptr [eax], al
0x7885007e 0x7e 0000 add byte ptr [eax], al
0x78850080 0x80 0000 add byte ptr [eax], al
****
Process: winlogon.exe Pid: 632 Address: 0x793e0000
Vad Tag: Vad5 Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x793e0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... vad_0x793e0000
0x793e0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x793e0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x793e0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....


C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
------ vad_0x793e0000 ------
0x793e0000 0x0 0000 add byte ptr [eax], al
0x793e0002 0x2 0000 add byte ptr [eax], al
0x793e0004 0x4 0000 add byte ptr [eax], al
0x793e0006 0x6 0000 add byte ptr [eax], al
0x793e0008 0x8 0000 add byte ptr [eax], al
0x793e000a 0xa 0000 add byte ptr [eax], al
0x793e000c 0xc 0000 add byte ptr [eax], al
0x793e000e 0xe 0000 add byte ptr [eax], al
0x793e0010 0x10 0000 add byte ptr [eax], al
0x793e0012 0x12 0000 add byte ptr [eax], al
0x793e0014 0x14 0000 add byte ptr [eax], al
0x793e0016 0x16 0000 add byte ptr [eax], al
0x793e0018 0x18 0000 add byte ptr [eax], al
0x793e001a 0x1a 0000 add byte ptr [eax], al
0x793e001c 0x1c 0000 add byte ptr [eax], al
0x793e001e 0x1e 0000 add byte ptr [eax], al
0x793e0020 0x20 0000 add byte ptr [eax], al
0x793e0022 0x22 0000 add byte ptr [eax], al
0x793e0024 0x24 0000 add byte ptr [eax], al
0x793e0026 0x26 0000 add byte ptr [eax], al
0x793e0028 0x28 0000 add byte ptr [eax], al
0x793e002a 0x2a 0000 add byte ptr [eax], al
0x793e002c 0x2c 0000 add byte ptr [eax], al
0x793e002e 0x2e 0000 add byte ptr [eax], al
0x793e0030 0x30 0000 add byte ptr [eax], al
0x793e0032 0x32 0000 add byte ptr [eax], al
0x793e0034 0x34 0000 add byte ptr [eax], al
0x793e0036 0x36 0000 add byte ptr [eax], al
0x793e0038 0x38 0000 add byte ptr [eax], al
0x793e003a 0x3a 0000 add byte ptr [eax], al
0x793e003c 0x3c 0000 add byte ptr [eax], al
0x793e003e 0x3e 0000 add byte ptr [eax], al
0x793e0040 0x40 0000 add byte ptr [eax], al
0x793e0042 0x42 0000 add byte ptr [eax], al
0x793e0044 0x44 0000 add byte ptr [eax], al
0x793e0046 0x46 0000 add byte ptr [eax], al
0x793e0048 0x48 0000 add byte ptr [eax], al
0x793e004a 0x4a 0000 add byte ptr [eax], al
0x793e004c 0x4c 0000 add byte ptr [eax], al
0x793e004e 0x4e 0000 add byte ptr [eax], al
0x793e0050 0x50 0000 add byte ptr [eax], al
0x793e0052 0x52 0000 add byte ptr [eax], al
0x793e0054 0x54 0000 add byte ptr [eax], al
0x793e0056 0x56 0000 add byte ptr [eax], al
0x793e0058 0x58 0000 add byte ptr [eax], al
0x793e005a 0x5a 0000 add byte ptr [eax], al
0x793e005c 0x5c 0000 add byte ptr [eax], al
0x793e005e 0x5e 0000 add byte ptr [eax], al
0x793e0060 0x60 0000 add byte ptr [eax], al
0x793e0062 0x62 0000 add byte ptr [eax], al
0x793e0064 0x64 0000 add byte ptr [eax], al
0x793e0066 0x66 0000 add byte ptr [eax], al
0x793e0068 0x68 0000 add byte ptr [eax], al
0x793e0068 0x68 0000 add byte ptr [eax], al
0x793e006a 0x6a 0000 add byte ptr [eax], al
0x793e006c 0x6c 0000 add byte ptr [eax], al
0x793e006e 0x6e 0000 add byte ptr [eax], al
0x793e0070 0x70 0000 add byte ptr [eax], al
0x793e0072 0x72 0000 add byte ptr [eax], al
0x793e0074 0x74 0000 add byte ptr [eax], al
0x793e0076 0x76 0000 add byte ptr [eax], al
0x793e0078 0x78 0000 add byte ptr [eax], al
0x793e007a 0x7a 0000 add byte ptr [eax], al
0x793e007c 0x7c 0000 add byte ptr [eax], al
0x793e007e 0x7e 0000 add byte ptr [eax], al
0x793e0080 0x80 0000 add byte ptr [eax], al
Out:19:30:51> Plugin: malfind (Malfind)
[1] tigger.vmem 19:30:51>

```
[1] tigger.vmem 20:08:38> threads
----------------------> threads()
 _ETHREAD   pid    tid     start            start_symbol              Process      win32_start win32_start_symb
---------- ------ ------ ---------- ------------------------------ --------------- ----------- ----------------
0x810b13e8      4      8 0x80683528 nt!Phase1Initialization        System                  0x0  0x0
0x810b0020      4     12 0x804edb6c nt!InbvRotateGuiBootDisplay    System                  0x0  0x0
0x810b0d20      4     16 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810b0aa8      4     20 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810b0830      4     24 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810b05b8      4     28 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810b0340      4     32 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810af020      4     36 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810afda8      4     40 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810afb30      4     44 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810af8b8      4     48 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810af640      4     52 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810af3c8      4     56 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810ae020      4     60 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810aeda8      4     64 0x80533cd0 nt!ExpWorkerThread             System                  0x0  0x0
0x810aeb30      4     68 0x806091a8 nt!ExpWorkerThreadBalanceManag System                  0x0  0x0
                                    er
0x810ad2c8      4     72 0x80508898 nt!MiDereferenceSegmentThread  System                  0x0  0x0
0x810aa020      4     76 0x8064226e nt!MiModifiedPageWriter        System                  0x0  0x0
0x810aada8      4     80 0x8053b3e8 nt!KeBalanceSetManager         System                  0x0  0x0
0x810aab30      4     84 0x8053b6de nt!KeSwapProcessOrStack        System                  0x0  0x0
0x810d5020      4     88 0x804ec6e8 nt!FsRtlWorkerThread           System                  0x0  0x0
0x810d5da8      4     92 0x804ec6e8 nt!FsRtlWorkerThread           System                  0x0  0x0
0x810d0870      4     96 0xfc37cb10 acpi+0x10b10                   System                  0x0  0x0
0x8102f020      4    100 0x8050ac2a nt!MiMappedPageWriter          System                  0x0  0x0
0x80fc6890      4    104 0xfc32091e dmio+0xa91e                   System                  0x0  0x0
0x8102db98      4    108 0xfc1eab85 ndis+0x6b85                   System                  0x0  0x0
0x80fa51a8      4    116 0xfc580f90 redbook+0x5f90                System                  0x0  0x0
0xff3c8020      4    136 0xfbfa881a rdpdr+0x2681a                 System                  0x0  0x0
0xff3c7748      4    140 0xfbfa881a rdpdr+0x2681a                 System                  0x0  0x0
0x80f4b020      4    144 0xfbfa881a rdpdr+0x2681a                 System                  0x0  0x0
0x80feeda8      4    148 0xfbf91cfa rdpdr+0xfcfa                  System                  0x0  0x0
0xff35d620      4    172 0xfc5eb92d raspptp+0x92d                 System                  0x0  0x0
0xff35d3a8      4    176 0xfc5ec103 raspptp+0x1103                System                  0x0  0x0
0x80fa8b10      4    280 0xfc0cce96 usbport+0x5e96                System                  0x0  0x0
0xff351b38      4    284 0xfc58eefe vmci+0x3efe                   System                  0x0  0x0
0xff353da8      4    288 0xfc58ef6c vmci+0x3f6c                   System                  0x0  0x0
0x80f4db48      4    292 0xfc0cce96 usbport+0x5e96                System                  0x0  0x0
0xff3bfda8      4    336 0xfc1256d0 parport+0x46d0                System                  0x0  0x0
0xff36dda8      4    352 0xfc175038 rasacd+0x1038                 System                  0x0  0x0
0x80fae390      4    356 0xf3b2da99 rdbss+0x18a99                 System                  0x0  0x0
0x80fae118      4    360 0xf3b2da99 rdbss+0x18a99                 System                  0x0  0x0
0xff39b738      4    364 0xf3b2da99 rdbss+0x18a99                 System                  0x0  0x0
0xff39b4c0      4    368 0xf3b158af rdbss+0x8af                   System                  0x0  0x0
0x80fcd020      4    540 0x805ee5b8 nt!SepRmCommandServerThread   System                  0x0  0x0
0xff257230      4   1516 0xf35f97d8 mrxdav+0x217d8                System                  0x0  0x0
0xff257658      4   1520 0xf35f97d8 mrxdav+0x217d8                System                  0x0  0x0
0xff3682d0      4   1524 0xf35f97d8 mrxdav+0x217d8                System                  0x0  0x0
0xff251658      4   1528 0xf35db82c mrxdav+0x382c                 System                  0x0  0x0
0xff24a560      4   1536 0xf35d8d18 mrxdav+0xd18                  System                  0x0  0x0
```

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem

```
0xff257658      4   1520 0xf35f97d8 mrxdav+0x217d8              System               0x0  0x0
0xff3682d0      4   1524 0xf35f97d8 mrxdav+0x217d8              System               0x0  0x0
0xff251658      4   1528 0xf35db82c mrxdav+0x382c               System               0x0  0x0
0xff24a560      4   1536 0xf35d8d18 mrxdav+0xd18                System               0x0  0x0
0xff242c28      4   1552 0xfc9f7cda vmmemctl+0xcda              System               0x0  0x0
0xff24fc10      4   1612 0xf356eb32 srv+0x11b32                 System               0x0  0x0
0xff24a998      4   1636 0xf356eb32 srv+0x11b32                 System               0x0  0x0
0xff12e5d0      4    276 0xf32ce7b6 http+0x327b6                System               0x0  0x0
0xff12e310      4    296 0xf32ce7b6 http+0x327b6                System               0x0  0x0
0xff12d020      4    300 0xf32ce7b6 http+0x327b6                System               0x0  0x0
0xff12dda8      4    304 0xf32ce7b6 http+0x327b6                System               0x0  0x0
0xff12db30      4    312 0xf32cbdda http+0x2fdda                System               0x0  0x0
0xff1f92b0      4   1648 0xf2edd150 0xf2edd150                  System               0x0  0x0
0xff2674a0      4   1720 0xf2edc54e 0xf2edc54e                  System               0x0  0x0
0x80f334a8      4   1992 0xf2edba46 0xf2edba46                  System               0x0  0x0
0x80f1b020      4   1916 0xfc7ae0ae flpydisk+0x30ae             System               0x0  0x0
0xff3bd370      4   1696 0xfc1eab85 ndis+0x6b85                 System               0x0  0x0
0xff134da8    216    236 0x7c810867 kernel32+0x10867           alg.exe           0x1005bc6  alg+0x5bc6
0xff131580    216    256 0x7c810856 kernel32+0x10856           alg.exe          0x77deb479  advapi32+0x1b479
0xff130da8    216    260 0x7c810856 kernel32+0x10856           alg.exe                0x0  0x0
0xff128718    216    436 0x7c810856 kernel32+0x10856           alg.exe                0x0  0x0
0xff1283e8    216    440 0x7c810856 kernel32+0x10856           alg.exe          0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
0xff127020    216    444 0x7c810856 kernel32+0x10856           alg.exe          0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff37d490    216   1948 0x7c810856 kernel32+0x10856           alg.exe              0x9068  0x9068
0xff3623c8    432    448 0x7c810867 kernel32+0x10867           VMwareTray.exe      0x40246a  vmwaretray+0x246a
0xff3762b0    452    456 0x7c810867 kernel32+0x10867           VMwareUser.exe      0x49fcbb  vmwareuser+0x9fcbb
0xff36cda8    452   1868 0x7c810856 kernel32+0x10856           VMwareUser.exe      0x407130  vmwareuser+0x7130
0xff384530    452    568 0x7c810856 kernel32+0x10856           VMwareUser.exe      0x412ea0  vmwareuser+0x12ea0
0xff3a5718    452   1264 0x7c810856 kernel32+0x10856           VMwareUser.exe    0x781329e1  msvcr80+0x29e1
0xff1e3648    452   1356 0x7c810856 kernel32+0x10856           VMwareUser.exe    0x781329e1  msvcr80+0x29e1
0x81025318    452   1368 0x7c810856 kernel32+0x10856           VMwareUser.exe           0x0  0x0
0x80f95da8    452   1360 0x7c810856 kernel32+0x10856           VMwareUser.exe    0x774f319a  ole32+0x1319a
0xff392da8    452   1372 0x7c810856 kernel32+0x10856           VMwareUser.exe       0x905b  0x905b
0xff214248    452   1884 0x7c810856 kernel32+0x10856           VMwareUser.exe       0x9067  0x9067
0x80f18408    468    988 0x7c810867 kernel32+0x10867           wuauclt.exe         0x40bad5  wuauclt+0xbad5
0x80fd9da8    468    992 0x7c810856 kernel32+0x10856           wuauclt.exe          0x9057  0x9057
0x80f94a68    468   1784 0x7c810856 kernel32+0x10856           wuauclt.exe          0x8771  0x8771
0x80fda518    468   1000 0x7c810856 kernel32+0x10856           wuauclt.exe         0x4077e2  wuauclt+0x77e2
0xff29b020    544    548 0x4858a4c8 smss+0xa4c8                 smss.exe                0x0  vad_0x0
0xff27c980    544    556 0x485893b2 smss+0x93b2                 smss.exe                0x0  vad_0x0
0xff1fbda8    544    560 0x485893b2 smss+0x93b2                 smss.exe               0x66ae  vad_0x0+0x66ae
0xff1e0650    608    616 0x75b6b329 winsrv+0xb329               csrss.exe               0x0  vad_0x0
0xff1f1da8    608    620 0x75b654a4 winsrv+0x54a4               csrss.exe               0x0  vad_0x0
0xff1ec558    608    624 0x75b44616 csrsrv+0x4616               csrss.exe               0x0  vad_0x0
0xff1f1980    608    628 0x75b43b3a csrsrv+0x3b3a               csrss.exe               0x0  vad_0x0
0xff20f7e8    608    640 0x75b44616 csrsrv+0x4616               csrss.exe               0x0  vad_0x0
0xff1d6228    608    644 0x75b6b0f7 winsrv+0xb0f7               csrss.exe               0x0  vad_0x0
0x80f02410    608    648 0x75b6b0f7 winsrv+0xb0f7               csrss.exe               0x0  vad_0x0
0xff24f130    608    696 0x75b6b0f7 winsrv+0xb0f7               csrss.exe               0x0  vad_0x0
0xff1587e0    608   1824 0x75b62272 winsrv+0x2272               csrss.exe               0x0  vad_0x0
0xff395298    608    812 0x75b6b59c winsrv+0xb59c               csrss.exe               0x0  vad_0x0
0xff20fc10    632    636  0x103d353 winlogon+0x3d353            winlogon.exe            0x0  0x0
0xff230130    632    656 0x7c810856 kernel32+0x10856           winlogon.exe            0x0  0x0
0xff224020    632    660 0x7c810856 kernel32+0x10856           winlogon.exe     0x77e76bf0  rpcrt4+0x6bf0
0xff23b130    632    664 0x7c810856 kernel32+0x10856           winlogon.exe     0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
```

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem

```
0xff217da8    632    920 0x7c810856 kernel32+0x10856              winlogon.exe         0x6db1  0x6db1
0xff213da8    632    924 0x7c810856 kernel32+0x10856              winlogon.exe     0x76c6c86b  sfc_os+0xc86b
0x80f529f0    632    928 0x7c810856 kernel32+0x10856              winlogon.exe     0x76c6c5ae  sfc_os+0xc5ae
0xff299620    632    932 0x7c810856 kernel32+0x10856              winlogon.exe     0x76c6c5ae  sfc_os+0xc5ae
0xff2a5b08    632   1220 0x7c810856 kernel32+0x10856              winlogon.exe      0x1039156  winlogon+0x39156
0xff200760    632   1252 0x7c810856 kernel32+0x10856              winlogon.exe     0x76602dc9  cscdll+0x2dc9
0xff1e33c8    632   1684 0x7c810856 kernel32+0x10856              winlogon.exe     0x769c8831  userenv+0x8831
0xff1dbda8    632   1688 0x7c810856 kernel32+0x10856              winlogon.exe     0x769d3cf1  userenv+0x13cf1
0xff22e330    632    480 0x7c810856 kernel32+0x10856              winlogon.exe      0x102b585  winlogon+0x2b585
0xff3b7880    632    112 0x7c810856 kernel32+0x10856              winlogon.exe     0x769d3cf1  userenv+0x13cf1
0xff1359c0    632    652 0x7c810856 kernel32+0x10856              winlogon.exe     0x759514de  wlnotify+0x14de
0xff3b5610    632   1008 0x7c810856 kernel32+0x10856              winlogon.exe     0x72d230e8  wdmaud+0x30e8
0xff37b188    632   1012 0x7c810856 kernel32+0x10856              winlogon.exe     0x76b44dd6  winmm+0x4dd6
0xff3608e0    632   1856 0x7c810856 kernel32+0x10856              winlogon.exe     0x77e76bf0  rpcrt4+0x6bf0
0xff37ada8    632   1480 0x7c810856 kernel32+0x10856              winlogon.exe     0x77e76bf0  rpcrt4+0x6bf0
0xff134020    632   1660 0x7c810856 kernel32+0x10856              winlogon.exe     0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff22a468    632   1216 0x7c810856 kernel32+0x10856              winlogon.exe     0x77e76bf0  rpcrt4+0x6bf0
0xff136688    632   1072 0x7c810856 kernel32+0x10856              winlogon.exe     0x77e76bf0  rpcrt4+0x6bf0
0xff277020    676    700 0x7c810856 kernel32+0x10856              services.exe     0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
0x80f03558    676    752 0x7c810856 kernel32+0x10856              services.exe     0x7c910aca  ntdll!RtlReleaseActivationContext+0x73
0x80f5f020    676    756 0x7c810856 kernel32+0x10856              services.exe     0x7c929fae  ntdll!RtlAdjustPrivilege+0x122
0xff25c020    676    816 0x7c810856 kernel32+0x10856              services.exe     0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff243568    676    820 0x7c810856 kernel32+0x10856              services.exe            0x0  0x0
0xff244660    676    824 0x7c810856 kernel32+0x10856              services.exe     0x77e76bf0  rpcrt4+0x6bf0
0xff244a88    676    832 0x7c810856 kernel32+0x10856              services.exe     0x776c39c0  authz+0x39c0
0xff244240    676    840 0x7c810856 kernel32+0x10856              services.exe     0x5f773bfb  ncobjapi+0x3bfb
0xff219da8    676    872 0x7c810856 kernel32+0x10856              services.exe      0x100963b  services+0x963b
0xff214660    676    916 0x7c810856 kernel32+0x10856              services.exe         0x6686  0x6686
0xff207b88    676   1112 0x7c810856 kernel32+0x10856              services.exe     0x758c349f  umpnpmgr+0x349f
0xff2a4620    676   1116 0x7c810856 kernel32+0x10856              services.exe     0x758c5df7  umpnpmgr+0x5df7
0xff1ef700    676   1280 0x7c810856 kernel32+0x10856              services.exe            0x0  0x0
0xff1dfda8    676   1576 0x7c810856 kernel32+0x10856              services.exe            0x0  0x0
0xff13a020    676   2020 0x7c810856 kernel32+0x10856              services.exe     0x5f771c49  ncobjapi+0x1c49
0xff25a558    676    224 0x7c810856 kernel32+0x10856              services.exe     0x5f773e24  ncobjapi+0x3e24
0xff240478    676    228 0x7c810856 kernel32+0x10856              services.exe     0x5f771d97  ncobjapi+0x1d97
0x80f2eda8    676    980 0x7c810856 kernel32+0x10856              services.exe     0x77e76bf0  rpcrt4+0x6bf0
0xff281020    688    704 0x7c810856 kernel32+0x10856              lsass.exe        0x75746767  lsasrv+0x16767
0xff250020    688    708 0x7c810856 kernel32+0x10856              lsass.exe        0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
0xff27f1d0    688    712 0x7c810856 kernel32+0x10856              lsass.exe        0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff369230    688    716 0x7c810856 kernel32+0x10856              lsass.exe        0x7c929fae  ntdll!RtlAdjustPrivilege+0x122
0x80fba218    688    720 0x7c810856 kernel32+0x10856              lsass.exe        0x75743381  lsasrv+0x13381
0x80efe248    688    736 0x7c810856 kernel32+0x10856              lsass.exe        0x7c910aca  ntdll!RtlReleaseActivationContext+0x73
0xff2a6930    688    760 0x7c810856 kernel32+0x10856              lsass.exe        0x77e76bf0  rpcrt4+0x6bf0
0xff1fac90    688    764 0x7c810856 kernel32+0x10856              lsass.exe               0x0  0x0
0xff1fa868    688    768 0x7c810856 kernel32+0x10856              lsass.exe            0x8fcd  0x8fcd
0xff1f96d0    688    780 0x7c810856 kernel32+0x10856              lsass.exe        0x75738e06  lsasrv+0x8e06
0x80faada8    688    784 0x7c810856 kernel32+0x10856              lsass.exe            0x7e34  0x7e34
0xff243990    688    804 0x7c810856 kernel32+0x10856              lsass.exe        0x75738e06  lsasrv+0x8e06
0xff252c20    688    836 0x7c810856 kernel32+0x10856              lsass.exe               0x0  0x0
0xff1efda8    688   1296 0x7c810856 kernel32+0x10856              lsass.exe               0x0  0x0
0xff1df3c8    688   1596 0x7c810856 kernel32+0x10856              lsass.exe        0x77deb479  advapi32+0x1b479
0xff2594c0    688   1740 0x7c810856 kernel32+0x10856              lsass.exe        0x662e085b  hnetcfg+0x3085b
0xff2587f0    688   1744 0x7c810856 kernel32+0x10856              lsass.exe        0x77c3a341  msvcrt+0x2a341
0xff26a568    688   1748 0x7c810856 kernel32+0x10856              lsass.exe        0x77c3a341  msvcrt+0x2a341
0xff225660    688   1752 0x7c810856 kernel32+0x10856              lsass.exe        0x77c3a341  msvcrt+0x2a341
```

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem

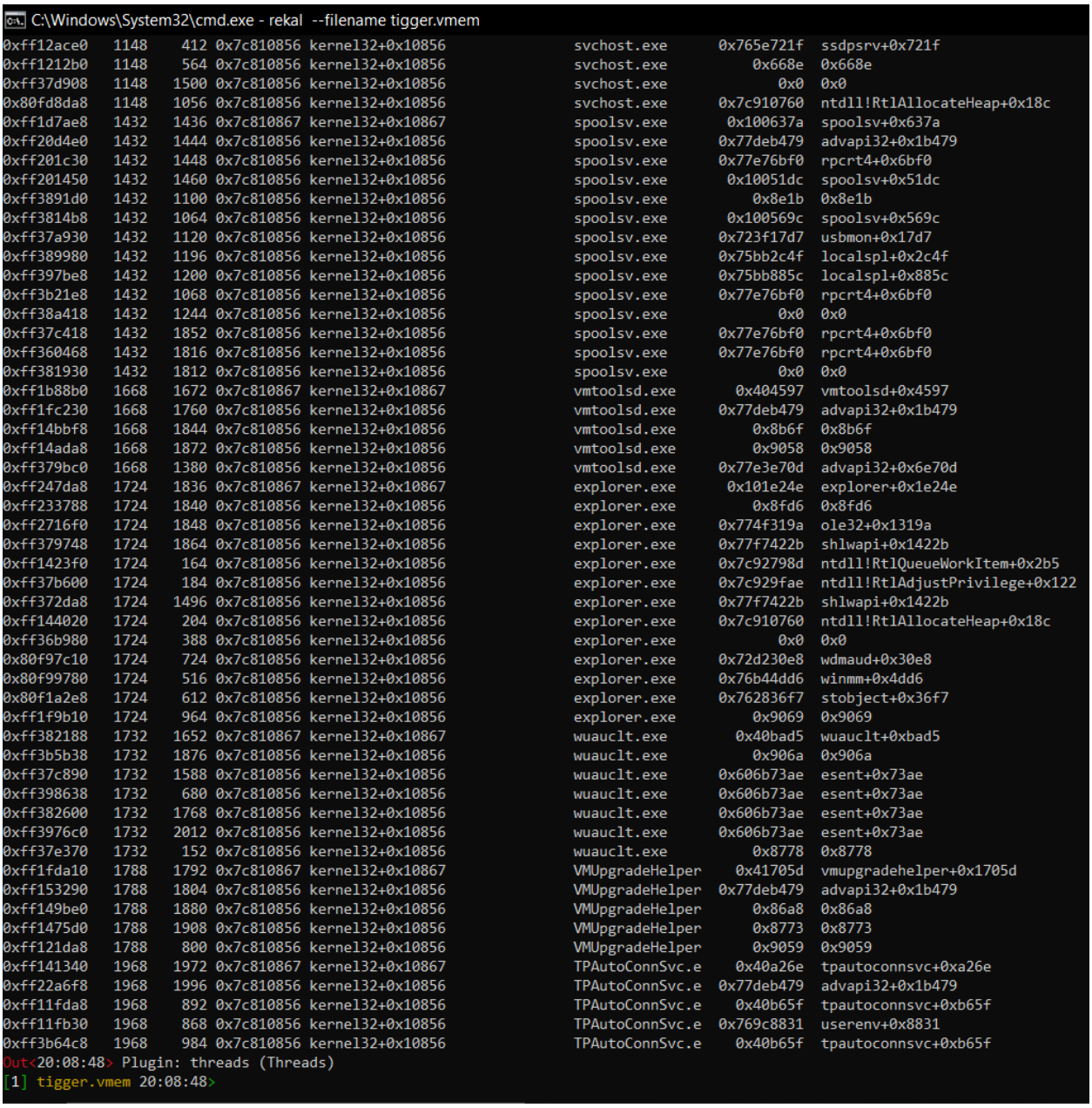
```
0xff225660    688   1752 0x7c810856 kernel32+0x10856              lsass.exe       0x77c3a341  msvcrt+0x2a341
0xff142bf0    688   1232 0x7c810856 kernel32+0x10856              lsass.exe       0x769c8831  userenv+0x8831
0xff36c1f0    688   1604 0x7c810856 kernel32+0x10856              lsass.exe       0x75738e06  lsasrv+0x8e06
0xff20c428    688    392 0x7c810856 kernel32+0x10856              lsass.exe       0x77e76bf0  rpcrt4+0x6bf0
0x80f32da8    828   1336 0x7c810867 kernel32+0x10867              wmiprvse.exe     0x1024636  wmiprvse+0x24636
0x80f5c3b8    828   1592 0x7c810856 kernel32+0x10856              wmiprvse.exe    0x5f771c49  ncobjapi+0x1c49
0xff298bc0    828   1708 0x7c810856 kernel32+0x10856              wmiprvse.exe        0x906b  0x906b
0xff2683d0    828    496 0x7c810856 kernel32+0x10856              wmiprvse.exe    0x774f319a  ole32+0x1319a
0xff3751d0    828   1016 0x7c810856 kernel32+0x10856              wmiprvse.exe     0x100ce42  wmiprvse+0xce42
0x80f16da8    828   1464 0x7c810856 kernel32+0x10856              wmiprvse.exe        0x9075  0x9075
0xff3a7368    828   2044 0x7c810856 kernel32+0x10856              wmiprvse.exe           0x0  0x0
0xff237470    828   1176 0x7c810856 kernel32+0x10856              wmiprvse.exe    0x716df2be  cimwin32+0xcf2be
0x80f17478    828   1608 0x7c810856 kernel32+0x10856              wmiprvse.exe    0x77e3e70d  advapi32+0x6e70d
0xff213578    844    848 0x7c810867 kernel32+0x10867              vmacthlp.exe      0x42aad1  vmacthlp+0x2aad1
0xff1e9da8    856    860 0x7c810867 kernel32+0x10867              svchost.exe      0x1002509  svchost+0x2509
0xff231020    856    896 0x7c810856 kernel32+0x10856              svchost.exe     0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
0xff287c10    856    904 0x7c810856 kernel32+0x10856              svchost.exe     0x7c929fae  ntdll!RtlAdjustPrivilege+0x122
0xff1b9b98    856    908 0x7c810856 kernel32+0x10856              svchost.exe           0x0  0x0
0xff1f2da8    856   1036 0x7c810856 kernel32+0x10856              svchost.exe           0x0  0x0
0xff3792d0    856    528 0x7c810856 kernel32+0x10856              svchost.exe    0x7610fe60  termsrv+0x1fe60
0xff3b8978    856   1928 0x7c810856 kernel32+0x10856              svchost.exe        0x7d12  0x7d12
0xff3bada8    856    572 0x7c810856 kernel32+0x10856              svchost.exe        0x77d1  0x77d1
0xff3ba358    856    580 0x7c810856 kernel32+0x10856              svchost.exe    0x760fe99c  termsrv+0xe99c
0xff3b8450    856    576 0x7c810856 kernel32+0x10856              svchost.exe    0x760fe894  termsrv+0xe894
0xff3b93d0    856    584 0x7c810856 kernel32+0x10856              svchost.exe    0x760fa72e  termsrv+0xa72e
0xff364838    856    604 0x7c810856 kernel32+0x10856              svchost.exe    0x769c8831  userenv+0x8831
0xff36da48    856    588 0x7c810856 kernel32+0x10856              svchost.exe           0x0  0x0
0xff3bb2f8    856    596 0x7c810856 kernel32+0x10856              svchost.exe    0x77e76bf0  rpcrt4+0x6bf0
0xff37fda8    856    592 0x7c810856 kernel32+0x10856              svchost.exe           0x0  0x0
0xff235da8    856    808 0x7c810856 kernel32+0x10856              svchost.exe           0x0  0x0
0xff3ae9a0    856   1488 0x7c810856 kernel32+0x10856              svchost.exe    0x77e76bf0  rpcrt4+0x6bf0
0x80efeab0    856    728 0x7c810856 kernel32+0x10856              svchost.exe    0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff3ba880    888    912 0x7c810867 kernel32+0x10867              wscntfy.exe      0x10027f2  wscntfy+0x27f2
0xff2167f8    936    940 0x7c810867 kernel32+0x10867              svchost.exe      0x1002509  svchost+0x2509
0x80fb6020    936    944 0x7c810856 kernel32+0x10856              svchost.exe    0x77deb479  advapi32+0x1b479
0xff200228    936    948 0x7c810856 kernel32+0x10856              svchost.exe    0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
0x80ffc2b0    936    952 0x7c810856 kernel32+0x10856              svchost.exe    0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff2843c0    936    956 0x7c810856 kernel32+0x10856              svchost.exe    0x7c929fae  ntdll!RtlAdjustPrivilege+0x122
0xff22f3c0    936    960 0x7c810856 kernel32+0x10856              svchost.exe           0x0  0x0
0xff1f1558    936    968 0x7c810856 kernel32+0x10856              svchost.exe           0x0  0x0
0xff14b210    936   1860 0x7c810856 kernel32+0x10856              svchost.exe        0x9070  0x9070
0xff13d330    936    512 0x7c810856 kernel32+0x10856              svchost.exe    0x77e76bf0  rpcrt4+0x6bf0
0x80fbf698   1028   1032 0x7c810867 kernel32+0x10867              svchost.exe      0x1002509  svchost+0x2509
0xff291da8   1028   1040 0x7c810856 kernel32+0x10856              svchost.exe        0x8b96  0x8b96
0xff291b30   1028   1044 0x7c810856 kernel32+0x10856              svchost.exe    0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
0x80f524e8   1028   1048 0x7c810856 kernel32+0x10856              svchost.exe    0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff1f7320   1028   1076 0x7c810856 kernel32+0x10856              svchost.exe    0x77deb479  advapi32+0x1b479
0x80f0d4b8   1028   1104 0x7c810856 kernel32+0x10856              svchost.exe        0x9093  0x9093
0xff1f2020   1028   1128 0x7c810856 kernel32+0x10856              svchost.exe    0x76d8ae19  dhcpcsvc+0xae19
0xff203818   1028   1140 0x7c810856 kernel32+0x10856              svchost.exe        0x9084  0x9084
0xff1e8448   1028   1364 0x7c810856 kernel32+0x10856              svchost.exe    0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff205da8   1028   1384 0x7c810856 kernel32+0x10856              svchost.exe    0x77df9981  advapi32+0x29981
0xff1ff7f0   1028   1388 0x7c810856 kernel32+0x10856              svchost.exe    0x77e76bf0  rpcrt4+0x6bf0
0xff1ff3d0   1028   1392 0x7c810856 kernel32+0x10856              svchost.exe    0x77666bb2  wzcsvc+0x46bb2
0xff29b8c8   1028   1396 0x7c810856 kernel32+0x10856              svchost.exe    0x77deb479  advapi32+0x1b479
```

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem

```
0xff205da8   1028   1384 0x7c810856 kernel32+0x10856              svchost.exe      0x77df9981  advapi32+0x29981
0xff1ff7f0   1028   1388 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff1ff3d0   1028   1392 0x7c810856 kernel32+0x10856              svchost.exe      0x77666bb2  wzcsvc+0x46bb2
0xff29b8c8   1028   1396 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff227c20   1028   1404 0x7c810856 kernel32+0x10856              svchost.exe      0x774f319a  ole32+0x1319a
0xff205570   1028   1408 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff2277f8   1028   1412 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff2283d8   1028   1416 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff202830   1028   1420 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff22c818   1028   1424 0x7c810856 kernel32+0x10856              svchost.exe      0x7730b153  schedsvc+0xb153
0xff22c5a0   1028   1428 0x7c810856 kernel32+0x10856              svchost.exe      0x7730a89a  schedsvc+0xa89a
0xff1e7428   1028   1440 0x7c810856 kernel32+0x10856              svchost.exe      0x7731709d  schedsvc+0x1709d
0xff1fe840   1028   1468 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff1fe4a0   1028   1472 0x7c810856 kernel32+0x10856              svchost.exe      0x7730a597  schedsvc+0xa597
0x80fce020   1028   1476 0x7c810856 kernel32+0x10856              svchost.exe          0x8b63  0x8b63
0xff24c468   1028   1512 0x7c810856 kernel32+0x10856              svchost.exe      0x7c910aca  ntdll!RtlReleaseActivationContext+0x73
0xff242800   1028   1564 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff24b230   1028   1568 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff1dfb30   1028   1580 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff1df8b8   1028   1584 0x7c810856 kernel32+0x10856              svchost.exe           0x492  0x492
0xff257a80   1028   1640 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff160020   1028   1728 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff1fd6f0   1028   1756 0x7c810856 kernel32+0x10856              svchost.exe          0x84b8  0x84b8
0xff1fc658   1028   1764 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff1fca88   1028   1772 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff2083d0   1028   1776 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff24f7f8   1028   1780 0x7c810856 kernel32+0x10856              svchost.exe      0x769c8831  userenv+0x8831
0xff15a668   1028   1796 0x7c810856 kernel32+0x10856              svchost.exe      0x767c28de  w32time+0x28de
0xff154888   1028   1800 0x7c810856 kernel32+0x10856              svchost.exe      0x662e085b  hnetcfg+0x3085b
0xff159020   1028   1808 0x7c810856 kernel32+0x10856              svchost.exe      0x77738ff5  es+0x28ff5
0xff1490c0   1028   1888 0x7c810856 kernel32+0x10856              svchost.exe      0x75219a1e  repdrvfs+0x19a1e
0xff148020   1028   1896 0x7c810856 kernel32+0x10856              svchost.exe      0x5f773bfb  ncobjapi+0x3bfb
0xff147da8   1028   1900 0x7c810856 kernel32+0x10856              svchost.exe      0x5f773bfb  ncobjapi+0x3bfb
0xff144360   1028   1924 0x7c810856 kernel32+0x10856              svchost.exe          0x8e3a  0x8e3a
0xff143da8   1028   1932 0x7c810856 kernel32+0x10856              svchost.exe      0x776c39c0  authz+0x39c0
0xff154b20   1028   2016 0x7c810856 kernel32+0x10856              svchost.exe      0x5f743c44  ncprov+0x3c44
0xff13ada8   1028   2024 0x7c810856 kernel32+0x10856              svchost.exe      0x5f771c49  ncobjapi+0x1c49
0xff13ab30   1028   2028 0x7c810856 kernel32+0x10856              svchost.exe      0x5f771c49  ncobjapi+0x1c49
0xff139b48   1028   2036 0x7c810856 kernel32+0x10856              svchost.exe      0x4c0a82cf  wscsvc+0x82cf
0xff2406f0   1028   2040 0x7c810856 kernel32+0x10856              svchost.exe      0x4c0a4c28  wscsvc+0x4c28
0xff134600   1028    244 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff1301e8   1028    272 0x7c810856 kernel32+0x10856              svchost.exe      0x774f319a  ole32+0x1319a
0xff12a408   1028    416 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff125020   1028    472 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff122810   1028    484 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff121020   1028    488 0x7c810856 kernel32+0x10856              svchost.exe      0x7c929fae  ntdll!RtlAdjustPrivilege+0x122
0xff122020   1028    492 0x7c810856 kernel32+0x10856              svchost.exe      0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff122360   1028    504 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff25cda8   1028    500 0x7c810856 kernel32+0x10856              svchost.exe      0x74f02555  ssdpapi+0x2555
0xff376980   1028    520 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff3b7da8   1028    692 0x7c810856 kernel32+0x10856              svchost.exe      0x776f6207  shsvcs+0x16207
0xff3ae480   1028   1304 0x7c810856 kernel32+0x10856              svchost.exe      0x73405033  tapisrv+0x25033
0xff3ae710   1028   1308 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff360d58   1028   1312 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff3655b0   1028   1316 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
```

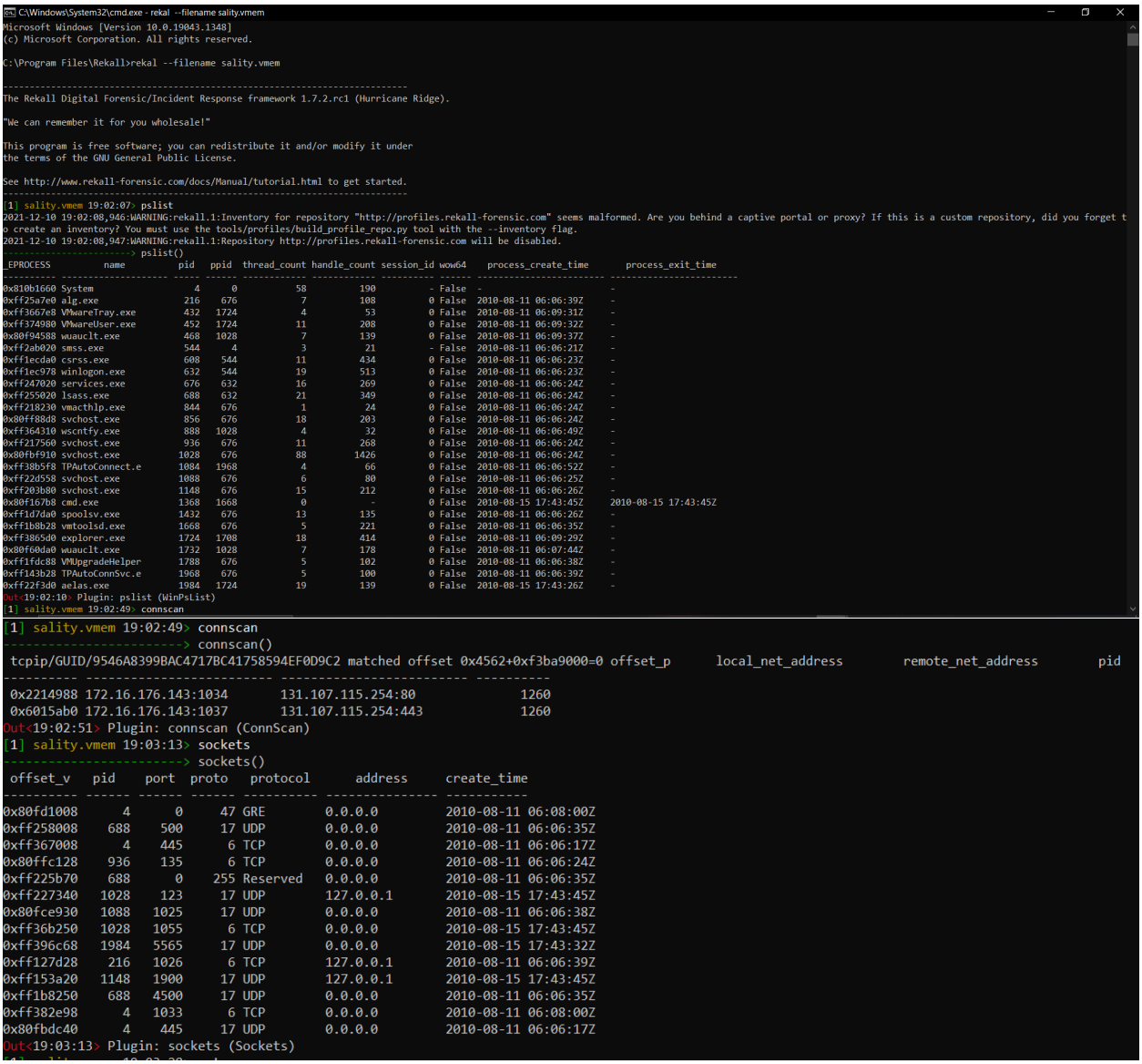
C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem

```
0xff3655b0   1028   1316 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff37a4b8   1028   1320 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff37dd80   1028   1324 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff380bc0   1028   1248 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff3b2710   1028   1504 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff3b1d80   1028   1292 0x7c810856 kernel32+0x10856              svchost.exe          0x905a  0x905a
0xff38dda8   1028    208 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff38e1d8   1028    220 0x7c810856 kernel32+0x10856              svchost.exe      0x75887b5e  rastapi+0x7b5e
0xff39fda8   1028   1964 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff38c348   1028   1940 0x7c810856 kernel32+0x10856              svchost.exe      0x57cde2a8  unimdm+0x1e2a8
0xff3b7358   1028    232 0x7c810856 kernel32+0x10856              svchost.exe      0x72001a18  uniplat+0x1a18
0xff381da8   1028    864 0x7c810856 kernel32+0x10856              svchost.exe      0x57d46dd4  kmddsp+0x6dd4
0xff39ada8   1028    340 0x7c810856 kernel32+0x10856              svchost.exe      0x57d29bc0  ndptsp+0x9bc0
0xff3b1330   1028    344 0x7c810856 kernel32+0x10856              svchost.exe      0x57d91f91  h323+0x21f91
0xff3b0da8   1028    348 0x7c810856 kernel32+0x10856              svchost.exe      0x57d63f47  hidphone+0x3f47
0xff390da8   1028    376 0x7c810856 kernel32+0x10856              svchost.exe      0x76ebe104  tapi32+0xe104
0xff3bc3d0   1028    464 0x7c810856 kernel32+0x10856              svchost.exe      0x7225bb4d  rasppp+0x1bb4d
0x80fbb610   1028    268 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff13c360   1028    792 0x7c810856 kernel32+0x10856              svchost.exe      0x7c910760  ntdll!RtlAllocateHeap+0x18c
0x80f2e2a0   1028   1912 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff148970   1028   1692 0x7c810856 kernel32+0x10856              svchost.exe      0x7773802f  es+0x2802f
0xff154da8   1028    536 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff282b70   1028   1712 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0x80f65020   1028    384 0x7c810856 kernel32+0x10856              svchost.exe      0x762cf010  wbemcore+0xf010
0xff1eb4c0   1028   1268 0x7c810856 kernel32+0x10856              svchost.exe      0x762cf0a3  wbemcore+0xf0a3
0x80ff3020   1028   1452 0x7c810856 kernel32+0x10856              svchost.exe      0x7509b647  srvsvc+0xb647
0x80fdc378   1028   1820 0x7c810856 kernel32+0x10856              svchost.exe      0x7509b647  srvsvc+0xb647
0xff1f6da8   1028    200 0x7c810856 kernel32+0x10856              svchost.exe      0x774f319a  ole32+0x1319a
0xff388da8   1028   1508 0x7c810856 kernel32+0x10856              svchost.exe      0x74f0742e  ssdpapi+0x742e
0xff36f5f8   1028    124 0x7c810856 kernel32+0x10856              svchost.exe      0x74f0742e  ssdpapi+0x742e
0xff397248   1084   1096 0x7c810867 kernel32+0x10867              TPAutoConnect.e    0x42462c  tpautoconnect+0x2462c
0xff21a868   1088   1092 0x7c810867 kernel32+0x10867              svchost.exe       0x1002509  svchost+0x2509
0xff1e58c8   1088   1184 0x7c810856 kernel32+0x10856              svchost.exe      0x767756a3  dnsrslvr+0x56a3
0xff1e55a8   1088   1188 0x7c810856 kernel32+0x10856              svchost.exe      0x7677464b  dnsrslvr+0x464b
0xff212c18   1088   1192 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff14f720   1088   1828 0x7c810856 kernel32+0x10856              svchost.exe          0x8bab  0x8bab
0xff14ebf8   1088   1936 0x7c810856 kernel32+0x10856              svchost.exe      0x662e085b  hnetcfg+0x3085b
0xff3af4b8   1088   1904 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff38a890   1088   1204 0x7c810856 kernel32+0x10856              svchost.exe      0x77df9981  advapi32+0x29981
0xff1eab18   1148   1152 0x7c810867 kernel32+0x10867              svchost.exe       0x1002509  svchost+0x2509
0xff1fa020   1148   1224 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff1ef2d0   1148   1276 0x7c810856 kernel32+0x10856              svchost.exe      0x74c41b04  lmhsvc+0x1b04
0xff251a80   1148   1540 0x7c810856 kernel32+0x10856              svchost.exe      0x5a6e57c5  webclnt+0x57c5
0xff24b658   1148   1544 0x7c810856 kernel32+0x10856              svchost.exe      0x5a6e57c5  webclnt+0x57c5
0xff253658   1148   1548 0x7c810856 kernel32+0x10856              svchost.exe      0x77e76bf0  rpcrt4+0x6bf0
0xff12d428   1148    316 0x7c810856 kernel32+0x10856              svchost.exe      0x77deb479  advapi32+0x1b479
0xff12f020   1148    320 0x7c810856 kernel32+0x10856              svchost.exe      0x7c92798d  ntdll!RtlQueueWorkItem+0x2b5
0xff12fd40   1148    328 0x7c810856 kernel32+0x10856              svchost.exe      0x7c910760  ntdll!RtlAllocateHeap+0x18c
0xff12f998   1148    332 0x7c810856 kernel32+0x10856              svchost.exe      0x7c929fae  ntdll!RtlAdjustPrivilege+0x122
0xff12b318   1148    396 0x7c810856 kernel32+0x10856              svchost.exe      0x662e085b  hnetcfg+0x3085b
0xff12a8b8   1148    408 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0xff12ace0   1148    412 0x7c810856 kernel32+0x10856              svchost.exe      0x765e721f  ssdpsrv+0x721f
0xff1212b0   1148    564 0x7c810856 kernel32+0x10856              svchost.exe          0x668e  0x668e
0xff37d908   1148   1500 0x7c810856 kernel32+0x10856              svchost.exe             0x0  0x0
0x80fd8da8   1148   1056 0x7c810856 kernel32+0x10856              svchost.exe      0x7c910760  ntdll!RtlAllocateHeap+0x18c
```



Malware Analyst 2: Sality

Background: A malware that aims to lower your security and delete important files related to Windows system while also replacing and spreading itself to other files. This virus can not only affect computer's files, but it can also possibly delete antivirus security to further spread itself.


C:\Windows\System32\cmd.exe - rekal --filename sality.vmem
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.
C:\Program Files\Rekall>rekal --filename sality.vmem
The Rekall Digital Forensic/Incident Response framework 1.7.2.rc1 (Hurricane Ridge).
"We can remember it for you wholesale!"
This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.
See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.
[1] sality.vmem 19:02:07> pslist
2021-12-10 19:02:08,946:WARNING:rekall.1:Inventory for repository "http://profiles.rekall-forensic.com" seems malformed. Are you behind a captive portal or proxy? If this is a custom repository, did you forget t
o create an inventory? You must use the tools/profiles/build_profile_repo.py tool with the --inventory flag.
2021-12-10 19:02:08,947:WARNING:rekall.1:Repository http://profiles.rekall-forensic.com will be disabled.
----------------------> pslist()
_EPROCESS name pid ppid thread_count handle_count session_id wow64 process_create_time process_exit_time
0x810b1660 System 4 0 58 190 - False -
0xff25a7e0 alg.exe 216 676 7 108 0 False 2010-08-11 06:06:39Z -
0xff3667e8 VMwareTray.exe 432 1724 4 53 0 False 2010-08-11 06:09:31Z -
0xff374980 VMwareUser.exe 452 1724 11 208 0 False 2010-08-11 06:09:32Z -
0x80f94588 wuauclt.exe 468 1028 7 139 0 False 2010-08-11 06:09:37Z -
0xff2ab020 smss.exe 544 4 3 21 - False 2010-08-11 06:06:21Z -
0xff1ecda0 csrss.exe 608 544 11 434 0 False 2010-08-11 06:06:23Z -
0xff1ec978 winlogon.exe 632 544 19 513 0 False 2010-08-11 06:06:23Z -
0xff247020 services.exe 676 632 16 269 0 False 2010-08-11 06:06:24Z -
0xff255020 lsass.exe 688 632 21 349 0 False 2010-08-11 06:06:24Z -
0xff218230 vmacthlp.exe 844 676 1 24 0 False 2010-08-11 06:06:24Z -
0x80ff88d8 svchost.exe 856 676 18 203 0 False 2010-08-11 06:06:24Z -
0xff364310 wscntfy.exe 888 1028 4 32 0 False 2010-08-11 06:06:49Z -
0xff217560 svchost.exe 936 676 11 268 0 False 2010-08-11 06:06:24Z -
0x80fbf910 svchost.exe 1028 676 88 1426 0 False 2010-08-11 06:06:24Z -
0xff30b5f0 TPAutoConnect.e 1084 1968 4 66 0 False 2010-08-11 06:06:52Z -
0xff22d558 svchost.exe 1088 676 6 80 0 False 2010-08-11 06:06:25Z -
0xff203b80 svchost.exe 1148 676 15 212 0 False 2010-08-11 06:06:26Z -
0x80f167b8 cmd.exe 1368 1668 0 - 0 False 2010-08-15 17:43:45Z 2010-08-15 17:43:45Z
0xff1d7da0 spoolsv.exe 1432 676 13 135 0 False 2010-08-11 06:06:26Z -
0xff1b8b28 vmtoolsd.exe 1668 676 5 221 0 False 2010-08-11 06:06:35Z -
0xff3865d0 explorer.exe 1724 1708 18 414 0 False 2010-08-11 06:09:29Z -
0x80f60da0 wuauclt.exe 1732 1028 7 178 0 False 2010-08-11 06:07:44Z -
0xff1fdc88 VMUpgradeHelper 1788 676 5 102 0 False 2010-08-11 06:06:38Z -
0xff143b28 TPAutoConnSvc.e 1968 676 5 100 0 False 2010-08-11 06:06:39Z -
0xff22f3d0 aelas.exe 1984 1724 19 139 0 False 2010-08-15 17:43:26Z -
Out<19:02:10> Plugin: pslist (WinPsList)
[1] sality.vmem 19:02:49> connscan
[1] sality.vmem 19:02:49> connscan
----------------------> connscan()
tcpip/GUID/9546A8399BAC4717BC41758594EF0D9C2 matched offset 0x4562+0xf3ba9000=0 offset_p local_net_address remote_net_address pid
0x2214988 172.16.176.143:1034 131.107.115.254:80 1260
0x6015ab0 172.16.176.143:1037 131.107.115.254:443 1260
Out<19:02:51> Plugin: connscan (ConnScan)
[1] sality.vmem 19:03:13> sockets
----------------------> sockets()
offset_v pid port proto protocol address create_time
0x80fd1008 4 0 47 GRE 0.0.0.0 2010-08-11 06:08:00Z
0xff258008 688 500 17 UDP 0.0.0.0 2010-08-11 06:06:35Z
0xff367008 4 445 6 TCP 0.0.0.0 2010-08-11 06:06:17Z
0x80ffc128 936 135 6 TCP 0.0.0.0 2010-08-11 06:06:24Z
0xff225b70 688 0 255 Reserved 0.0.0.0 2010-08-11 06:06:35Z
0xff227340 1028 123 17 UDP 127.0.0.1 2010-08-15 17:43:45Z
0x80fce930 1088 1025 17 UDP 0.0.0.0 2010-08-11 06:06:38Z
0xff36b250 1028 1055 6 TCP 0.0.0.0 2010-08-15 17:43:45Z
0xff396c68 1984 5565 17 UDP 0.0.0.0 2010-08-15 17:43:32Z
0xff127d28 216 1026 6 TCP 127.0.0.1 2010-08-11 06:06:39Z
0xff153a20 1148 1900 17 UDP 127.0.0.1 2010-08-15 17:43:45Z
0xff1b8250 688 4500 17 UDP 0.0.0.0 2010-08-11 06:06:35Z
0xff382e98 4 1033 6 TCP 0.0.0.0 2010-08-11 06:08:00Z
0x80fbdc40 4 445 17 UDP 0.0.0.0 2010-08-11 06:06:17Z
Out<19:03:13> Plugin: sockets (Sockets)

```
[1] sality.vmem 19:03:28> pstree
------------------------> pstree()
_EPROCESS                                ppid  thd_count hnd_count       create_time
---------------------------------------- ------ --------- --------- -----------------------
  0x810b1660 System (4)                     0        58       190 -
. 0xff2ab020 smss.exe (544)                 4         3        21 2010-08-11 06:06:21Z
.. 0xff1ecda0 csrss.exe (608)             544        11       434 2010-08-11 06:06:23Z
.. 0xff1ec978 winlogon.exe (632)          544        19       513 2010-08-11 06:06:23Z
... 0xff247020 services.exe (676)         632        16       269 2010-08-11 06:06:24Z
.... 0xff25a7e0 alg.exe (216)             676         7       108 2010-08-11 06:06:39Z
.... 0xff218230 vmacthlp.exe (844)        676         1        24 2010-08-11 06:06:24Z
.... 0x80ff88d8 svchost.exe (856)         676        18       203 2010-08-11 06:06:24Z
.... 0xff217560 svchost.exe (936)         676        11       268 2010-08-11 06:06:24Z
.... 0x80fbf910 svchost.exe (1028)        676        88      1426 2010-08-11 06:06:24Z
..... 0x80f94588 wuauclt.exe (468)       1028         7       139 2010-08-11 06:09:37Z
..... 0xff364310 wscntfy.exe (888)       1028         4        32 2010-08-11 06:06:49Z
..... 0x80f60da0 wuauclt.exe (1732)      1028         7       178 2010-08-11 06:07:44Z
.... 0xff22d558 svchost.exe (1088)        676         6        80 2010-08-11 06:06:25Z
.... 0xff203b80 svchost.exe (1148)        676        15       212 2010-08-11 06:06:26Z
.... 0xff1d7da0 spoolsv.exe (1432)        676        13       135 2010-08-11 06:06:26Z
.... 0xff1b8b28 vmtoolsd.exe (1668)       676         5       221 2010-08-11 06:06:35Z
..... 0x80f167b8 cmd.exe (1368)          1668         0         - 2010-08-15 17:43:45Z
.... 0xff1fdc88 VMUpgradeHelper (1788)    676         5       102 2010-08-11 06:06:38Z
.... 0xff143b28 TPAutoConnSvc.e (1968)    676         5       100 2010-08-11 06:06:39Z
..... 0xff38b5f8 TPAutoConnect.e (1084)  1968         4        66 2010-08-11 06:06:52Z
... 0xff255020 lsass.exe (688)            632        21       349 2010-08-11 06:06:24Z
  0xff3865d0 explorer.exe (1724)         1708        18       414 2010-08-11 06:09:29Z
. 0xff3667e8 VMwareTray.exe (432)        1724         4        53 2010-08-11 06:09:31Z
. 0xff374980 VMwareUser.exe (452)        1724        11       208 2010-08-11 06:09:32Z
. 0xff22f3d0 aelas.exe (1984)            1724        19       139 2010-08-15 17:43:26Z
Out<19:03:29> Plugin: pstree (PSTree)
[1] sality.vmem 19:03:55> psxview
```

```
[1] sality.vmem 19:03:55> psxview
----------------------> psxview()
_EPROCESS         name          pid  PsActiveProcessHead CSRSS PspCidTable Sessions Handles PSScan Thrdproc
--------- ------------------- ----- ------------------- ----- ----------- -------- ------- ------ --------
0x810b1660 System                  4 True                False True        False    False   True   True
0xff25a7e0 alg.exe               216 True                True  True        True     True    True   True
0xff3667e8 VMwareTray.exe        432 True                True  True        True     True    True   True
0xff374980 VMwareUser.exe        452 True                True  True        True     True    True   True
0x80f94588 wuauclt.exe           468 True                True  True        True     True    True   True
0xff2ab020 smss.exe              544 True                False True        False    True    True   True
0xff1ecda0 csrss.exe             608 True                False True        True     True    True   True
0xff1ec978 winlogon.exe          632 True                True  True        True     True    True   True
0xff247020 services.exe          676 True                True  True        True     True    True   True
0xff255020 lsass.exe             688 True                True  True        True     True    True   True
0xff218230 vmacthlp.exe          844 True                True  True        True     True    True   True
0x80ff88d8 svchost.exe           856 True                True  True        True     True    True   True
0xff364310 wscntfy.exe           888 True                True  True        True     True    True   True
0xff217560 svchost.exe           936 True                True  True        True     True    True   True
0x80fbf910 svchost.exe          1028 True                True  True        True     True    True   True
0xff38b5f8 TPAutoConnect.e      1084 True                True  True        True     True    True   True
0xff22d558 svchost.exe          1088 True                True  True        True     True    True   True
0xff203b80 svchost.exe          1148 True                True  True        True     True    True   True
0x80f167b8 cmd.exe              1368 True                False True        False    False   True   False
0xff1d7da0 spoolsv.exe          1432 True                True  True        True     True    True   True
0xff1b8b28 vmtoolsd.exe         1668 True                True  True        True     True    True   True
0xff3865d0 explorer.exe         1724 True                True  True        True     True    True   True
0x80f60da0 wuauclt.exe          1732 True                True  True        True     True    True   True
0xff1fdc88 VMUpgradeHelper      1788 True                True  True        True     True    True   True
0xff143b28 TPAutoConnSvc.e      1968 True                True  True        True     True    True   True
0xff22f3d0 aelas.exe            1984 True                True  True        True     True    True   True
Out<19:03:59> Plugin: psxview (WindowsPsxView)
[1] sality.vmem 19:03:59>
```

```
[1] sality.vmem 21:25:11> hooks_iat 1368
------------------------> hooks_iat(1368)
         source                target        target_func
  -------------------- -------------------- -----------
----------------------
Process cmd.exe (1368)
----------------------
Out<21:25:11> Plugin: hooks_iat (IATHooks)
[1] sality.vmem 21:25:11>
```

```
[1] sality.vmem 21:28:17> cmdscan
------------------------> cmdscan()
**************************************************
CommandProcess: csrss.exe Pid: 608
CommandHistory: 0xf786f8 Application: TPAutoConnect.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x448
Cmd  Address   Text
--- ---------- ----
Out<21:28:17> Plugin: cmdscan (CmdScan)
```

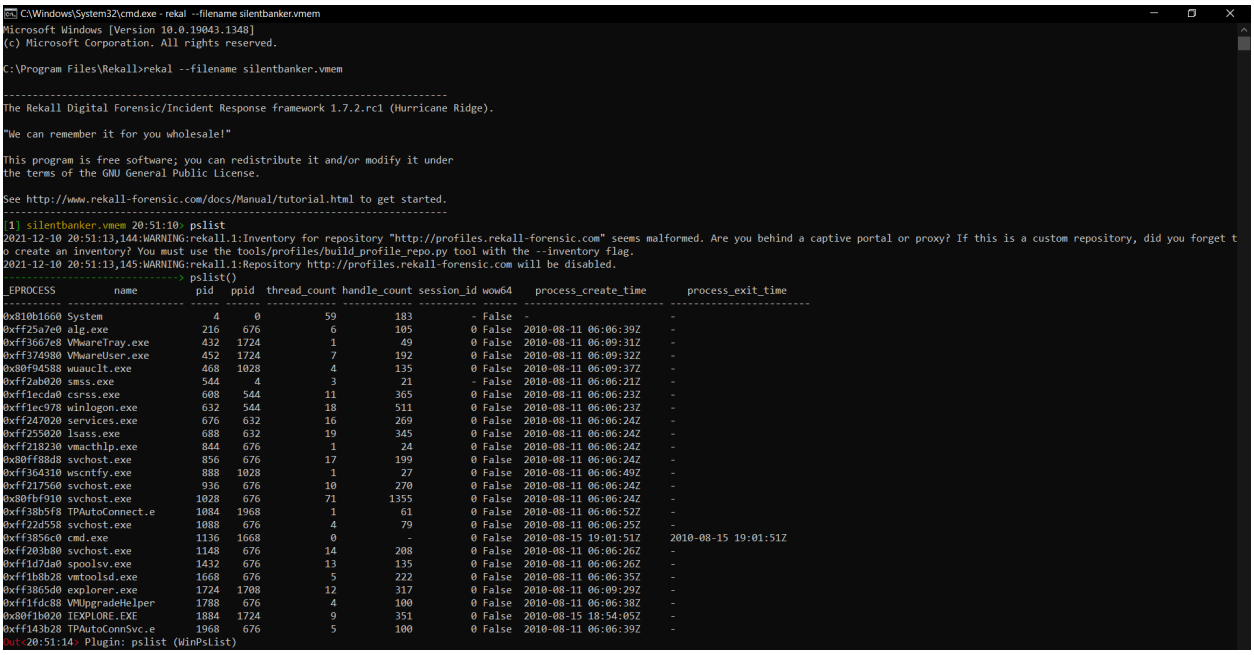
Procinfo

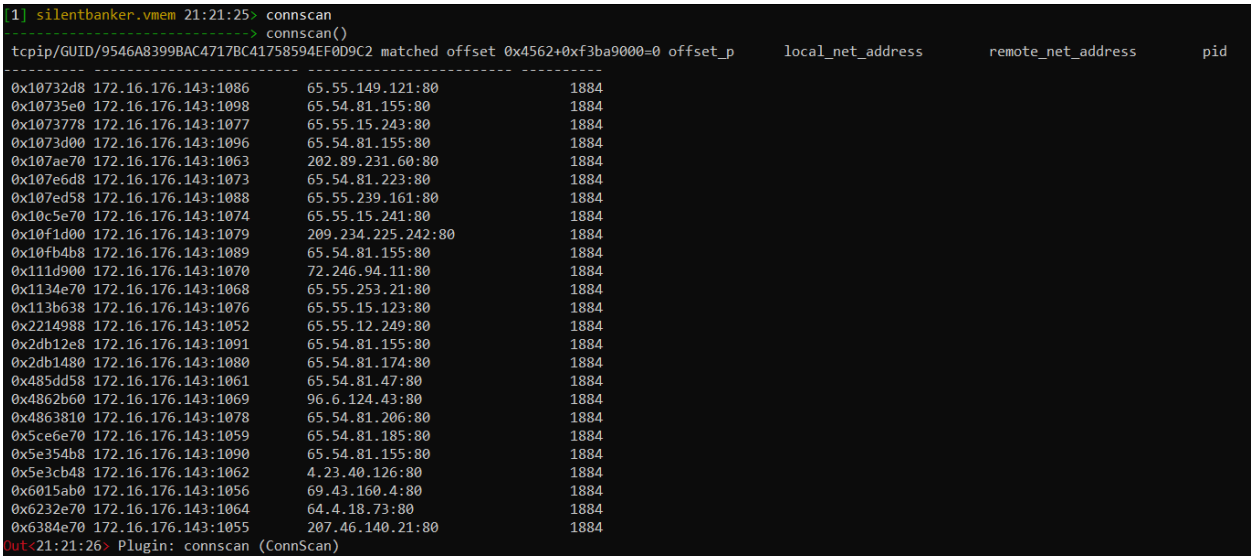
```
************************************************
Pid: 1724 explorer.exe

Process Environment
   =::=::\
   ALLUSERSPROFILE=C:\Documents and Settings\All Users
   APPDATA=C:\Documents and Settings\Administrator\Application Data
   CLIENTNAME=Console
   CommonProgramFiles=C:\Program Files\Common Files
   COMPUTERNAME=BILLY-DB5B96DD3
   ComSpec=C:\WINDOWS\system32\cmd.exe
   FP_NO_HOST_CHECK=NO
   HOMEDRIVE=C:
   HOMEPATH=\Documents and Settings\Administrator
   LOGONSERVER=\\BILLY-DB5B96DD3
   NUMBER_OF_PROCESSORS=1
   OS=Windows_NT
   Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
   PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
   PROCESSOR_ARCHITECTURE=x86
   PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
   PROCESSOR_LEVEL=6
   PROCESSOR_REVISION=170a
   ProgramFiles=C:\Program Files
   SESSIONNAME=Console
   SystemDrive=C:
   SystemRoot=C:\WINDOWS
   TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   USERDOMAIN=BILLY-DB5B96DD3
   USERNAME=Administrator
   USERPROFILE=C:\Documents and Settings\Administrator
   windir=C:\WINDOWS

PE Information
```

```
************************************************
Pid: 1984 aelas.exe

Process Environment
   =::=::\
   ALLUSERSPROFILE=C:\Documents and Settings\All Users
   APPDATA=C:\Documents and Settings\Administrator\Application Data
   CLIENTNAME=Console
   CommonProgramFiles=C:\Program Files\Common Files
   COMPUTERNAME=BILLY-DB5B96DD3
   ComSpec=C:\WINDOWS\system32\cmd.exe
   FP_NO_HOST_CHECK=NO
   HOMEDRIVE=C:
   HOMEPATH=\Documents and Settings\Administrator
   LOGONSERVER=\\BILLY-DB5B96DD3
   NUMBER_OF_PROCESSORS=1
   OS=Windows_NT
   Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
   PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
   PROCESSOR_ARCHITECTURE=x86
   PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
   PROCESSOR_LEVEL=6
   PROCESSOR_REVISION=170a
   ProgramFiles=C:\Program Files
   SESSIONNAME=Console
   SystemDrive=C:
   SystemRoot=C:\WINDOWS
   TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   USERDOMAIN=BILLY-DB5B96DD3
   USERNAME=Administrator
   USERPROFILE=C:\Documents and Settings\Administrator
   windir=C:\WINDOWS
```

Malware Analyst 3: Silent Banker

Background: Is a Trojan Banker that is known to steal your information like keystrokes, screenshots, etc. Except is most notably know to steal information that includes your finances. Mostly this can be done with using a misleading spoof website to scam you (thinking that it's the real official website) for any of your important finical information, and it can backdoor by installing virus with access to your email.





```
[1] silentbanker.vmem 21:21:34> pstree
------------------------------> pstree()
_EPROCESS                              ppid  thd_count hnd_count       create_time
-------------------------------------- ------ --------- --------- -----------------------
  0x810b1660 System (4)                   0        59       183 -
. 0xff2ab020 smss.exe (544)               4         3        21 2010-08-11 06:06:21Z
.. 0xff1ecda0 csrss.exe (608)           544        11       365 2010-08-11 06:06:23Z
.. 0xff1ec978 winlogon.exe (632)        544        18       511 2010-08-11 06:06:23Z
... 0xff247020 services.exe (676)       632        16       269 2010-08-11 06:06:24Z
.... 0xff25a7e0 alg.exe (216)           676         6       105 2010-08-11 06:06:39Z
.... 0xff218230 vmacthlp.exe (844)      676         1        24 2010-08-11 06:06:24Z
.... 0x80ff88d8 svchost.exe (856)       676        17       199 2010-08-11 06:06:24Z
.... 0xff217560 svchost.exe (936)       676        10       270 2010-08-11 06:06:24Z
.... 0x80fbf910 svchost.exe (1028)      676        71      1355 2010-08-11 06:06:24Z
..... 0x80f94588 wuauclt.exe (468)     1028         4       135 2010-08-11 06:09:37Z
..... 0xff364310 wscntfy.exe (888)     1028         1        27 2010-08-11 06:06:49Z
.... 0xff22d558 svchost.exe (1088)      676         4        79 2010-08-11 06:06:25Z
.... 0xff203b80 svchost.exe (1148)      676        14       208 2010-08-11 06:06:26Z
.... 0xff1d7da0 spoolsv.exe (1432)      676        13       135 2010-08-11 06:06:26Z
.... 0xff1b8b28 vmtoolsd.exe (1668)     676         5       222 2010-08-11 06:06:35Z
..... 0xff3856c0 cmd.exe (1136)        1668         0         - 2010-08-15 19:01:51Z
.... 0xff1fdc88 VMUpgradeHelper (1788)  676         4       100 2010-08-11 06:06:38Z
.... 0xff143b28 TPAutoConnSvc.e (1968)  676         5       100 2010-08-11 06:06:39Z
..... 0xff38b5f8 TPAutoConnect.e (1084) 1968        1        61 2010-08-11 06:06:52Z
... 0xff255020 lsass.exe (688)          632        19       345 2010-08-11 06:06:24Z
  0xff3865d0 explorer.exe (1724)        1708        12       317 2010-08-11 06:09:29Z
. 0xff3667e8 VMwareTray.exe (432)       1724         1        49 2010-08-11 06:09:31Z
. 0xff374980 VMwareUser.exe (452)       1724         7       192 2010-08-11 06:09:32Z
. 0x80f1b020 IEXPLORE.EXE (1884)        1724         9       351 2010-08-15 18:54:05Z
Out<21:21:34> Plugin: pstree (PSTree)
```

```
[1] silentbanker.vmem 21:21:43> psxview
----------------------------> psxview()
_EPROCESS         name          pid  PsActiveProcessHead CSRSS PspCidTable Sessions Handles PSScan Thrdproc
--------- ------------------- ----- ------------------- ----- ----------- -------- ------- ------ --------
0x810b1660 System                  4 True                False True        False    False   True   True
0xff25a7e0 alg.exe               216 True                True  True        True     True    True   True
0xff3667e8 VMwareTray.exe        432 True                True  True        True     True    True   True
0xff374980 VMwareUser.exe        452 True                True  True        True     True    True   True
0x80f94588 wuauclt.exe           468 True                True  True        True     True    True   True
0xff2ab020 smss.exe              544 True                False True        False    True    True   True
0xff1ecda0 csrss.exe             608 True                False True        True     True    True   True
0xff1ec978 winlogon.exe          632 True                True  True        True     True    True   True
0xff247020 services.exe          676 True                True  True        True     True    True   True
0xff255020 lsass.exe             688 True                True  True        True     True    True   True
0xff218230 vmacthlp.exe          844 True                True  True        True     True    True   True
0x80ff88d8 svchost.exe           856 True                True  True        True     True    True   True
0xff364310 wscntfy.exe           888 True                True  True        True     True    True   True
0xff217560 svchost.exe           936 True                True  True        True     True    True   True
0x80fbf910 svchost.exe          1028 True                True  True        True     True    True   True
0xff38b5f8 TPAutoConnect.e      1084 True                True  True        True     True    True   True
0xff22d558 svchost.exe          1088 True                True  True        True     True    True   True
0xff3856c0 cmd.exe              1136 True                False True        False    False   True   False
0xff203b80 svchost.exe          1148 True                True  True        True     True    True   True
0xff1d7da0 spoolsv.exe          1432 True                True  True        True     True    True   True
0xff1b8b28 vmtoolsd.exe         1668 True                True  True        True     True    True   True
0xff3865d0 explorer.exe         1724 True                True  True        True     True    True   True
0x80f60da0 wuauclt.exe          1732 False               False False       False    False   True   False
0xff1fdc88 VMUpgradeHelper      1788 True                True  True        True     True    True   True
0x80f1b020 IEXPLORE.EXE         1884 True                True  True        True     True    True   True
0xff143b28 TPAutoConnSvc.e      1968 True                True  True        True     True    True   True
Out<21:21:46> Plugin: psxview (WindowsPsxView)
[1] silentbanker.vmem 21:21:46>
```

```
[1] silentbanker.vmem 21:26:05> hooks_iat 1136
------------------------------> hooks_iat(1136)
         source                target        target_func
  -------------------- -------------------- -----------
----------------------
Process cmd.exe (1136)
----------------------
Out<21:26:05> Plugin: hooks_iat (IATHooks)
```

```
[1] silentbanker.vmem 21:29:07> cmdscan
------------------------------> cmdscan()
**************************************************
CommandProcess: csrss.exe Pid: 608
CommandHistory: 0xf786f8 Application: TPAutoConnect.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x448
Cmd  Address   Text
--- ---------- ----
Out<21:29:07> Plugin: cmdscan (CmdScan)
```

ProcInfo

```
************************************************
Pid: 432 VMwareTray.exe

Process Environment
   =::=::\
   ALLUSERSPROFILE=C:\Documents and Settings\All Users
   APPDATA=C:\Documents and Settings\Administrator\Application Data
   CLIENTNAME=Console
   CommonProgramFiles=C:\Program Files\Common Files
   COMPUTERNAME=BILLY-DB5B96DD3
   ComSpec=C:\WINDOWS\system32\cmd.exe
   FP_NO_HOST_CHECK=NO
   HOMEDRIVE=C:
   HOMEPATH=\Documents and Settings\Administrator
   LOGONSERVER=\\BILLY-DB5B96DD3
   NUMBER_OF_PROCESSORS=1
   OS=Windows_NT
   Path=C:\Program Files\VMware\VMware Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
   PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
   PROCESSOR_ARCHITECTURE=x86
   PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
   PROCESSOR_LEVEL=6
   PROCESSOR_REVISION=170a
   ProgramFiles=C:\Program Files
   SESSIONNAME=Console
   SystemDrive=C:
   SystemRoot=C:\WINDOWS
   TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   USERDOMAIN=BILLY-DB5B96DD3
   USERNAME=Administrator
   USERPROFILE=C:\Documents and Settings\Administrator
   windir=C:\WINDOWS

PE Infomation
         Attribute                                    Value
------------------------------------------------------------------------------
```

```
************************************************
Pid: 452 VMwareUser.exe

Process Environment
   =::=::\
   ALLUSERSPROFILE=C:\Documents and Settings\All Users
   APPDATA=C:\Documents and Settings\Administrator\Application Data
   CLIENTNAME=Console
   CommonProgramFiles=C:\Program Files\Common Files
   COMPUTERNAME=BILLY-DB5B96DD3
   ComSpec=C:\WINDOWS\system32\cmd.exe
   FP_NO_HOST_CHECK=NO
   HOMEDRIVE=C:
   HOMEPATH=\Documents and Settings\Administrator
   LOGONSERVER=\\BILLY-DB5B96DD3
   NUMBER_OF_PROCESSORS=1
   OS=Windows_NT
   Path=C:\Program Files\VMware\VMware Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
   PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
   PROCESSOR_ARCHITECTURE=x86
   PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
   PROCESSOR_LEVEL=6
   PROCESSOR_REVISION=170a
   ProgramFiles=C:\Program Files
   SESSIONNAME=Console
   SystemDrive=C:
   SystemRoot=C:\WINDOWS
   TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
   USERDOMAIN=BILLY-DB5B96DD3
   USERNAME=Administrator
   USERPROFILE=C:\Documents and Settings\Administrator
   windir=C:\WINDOWS
```

References:

Tutorial Links

https://www.youtube.com/watch?v=verKqNVshS4

http://www.rekall-forensic.com/documentation-1/rekall-documentation/tutorial

https://stariix.blogspot.com/2018/05/zeus-trojan-memory-forensics-with.html

https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1

Source Codes Links

https://virusshare.com/file?364040375650bf968b7503de130ecf17b8194f47825847e98149446acd741e50

https://github.com/google/rekall

https://github.com/google/rekall/releases

https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples

https://github.com/InQuest/malware-samples

https://www.python.org/downloads/release/python-360/

Note Information Links about the Analyzed Malware

https://www.darkreading.com/attacks-breaches/-tigger-trojan-keeps-security-researchers-hopping

https://en.wikipedia.org/wiki/Sality

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/sality

https://www.eclipseaviation.com/is-silent-banker-a-trojan-horse-2/

Malaware Database Links

https://virusshare.com/

https://bazaar.abuse.ch/browse/

https://reverseengineering.stackexchange.com/questions/206/where-can-i-as-an-individual-get-malware-samples-to-analyze

https://zeltser.com/malware-sample-sources/

Miscellaneous Links to Helpful information

https://evild3ad.com/1136/volatility-memory-forensics-federal-trojan-aka-r2d2/

https://sensorstechforum.com/popular-windows-file-types-used-malware-2018/

https://rioasmara.com/2019/09/28/basic-extracting-malware-from-memory/

https://github.com/InQuest/malware-samples

https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

https://github.com/ganboing/malwarecookbook