Memory Analysis

Dr. Ferhat Özgür Çatak Mehmet Can DÖŞLÜ

Content

- ➢Basic Memory Analysis
- ➢Examining Files with Volatility
- ➢Example

Basic Memory Analysis

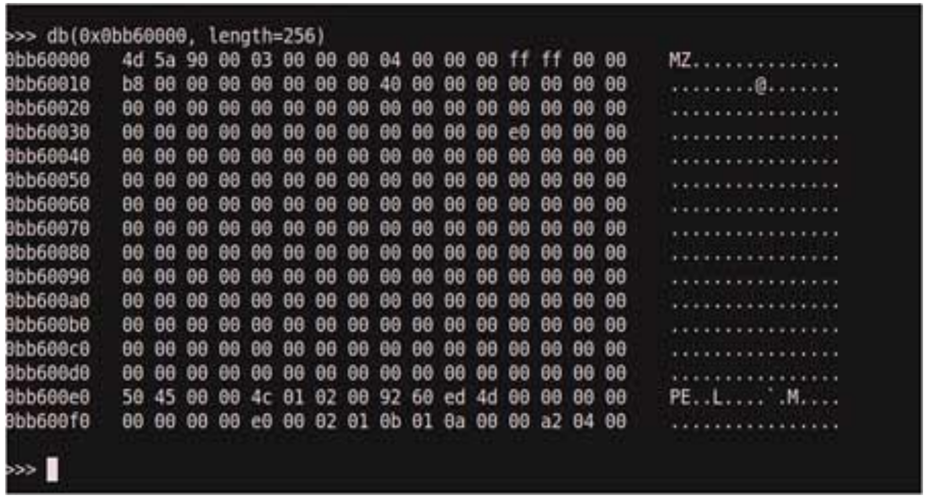
- Memory analysis is based on taking screen shots from a physical, virtual device or process and examine images manually or analysis tools.
- This process provides informations about
  - Processes
  - Network Connections
  - Loaded modules

Basic Memory Analysis

- Meantime with basic memory analysis analyst can do
  - Unpacking
  - Detection of rootkits
  - Reverse engineering analysis

Basic Memory Analysis

- Memory analysis is based on taking screen shots from a physical, virtual device or process and examine images manually or analysis tools.
- This process provides informations about
  - Processes
  - Network Connections
  - Opened Files
  - Loaded modules
  - Unpacked versions of packed files



```
>>> db(0x0bb60000, length=256)
0bb60000   4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    MZ..............
0bb60010   b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00    ........@.......
0bb60020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb60030   00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00    ................
0bb60040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb60050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb60060   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb60070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb60080   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb60090   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb600a0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb600b0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb600c0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb600d0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0bb600e0   50 45 00 00 4c 01 02 00 92 60 ed 4d 00 00 00 00    PE..L....`.M....
0bb600f0   00 00 00 00 e0 00 02 01 0b 01 0a 00 00 a2 04 00    ................

>>>
```

Basic Memory Analysis

- Memory analysis is consisting of two basic concepts

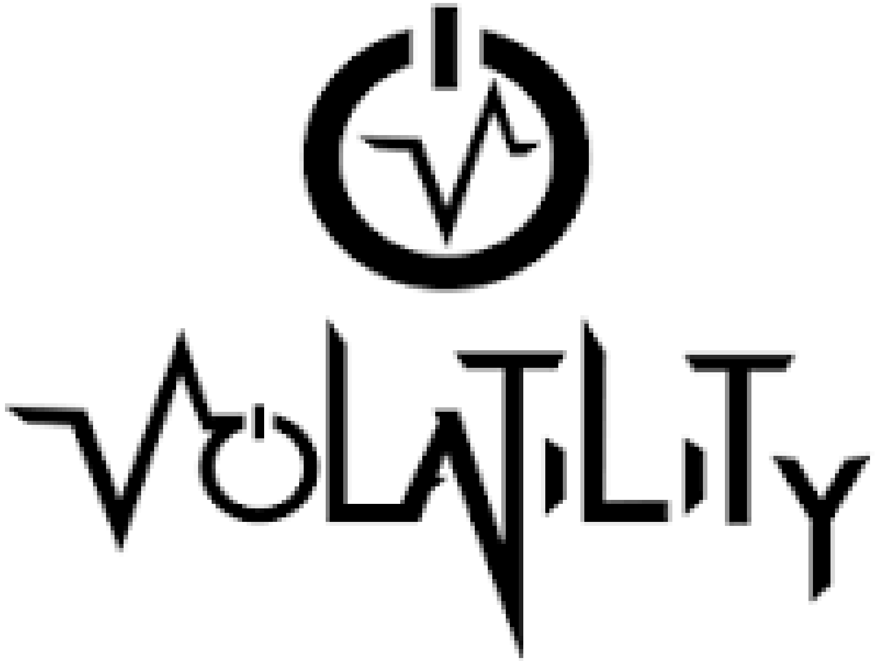
  I. Memory Acquisition
  II. Memory Analysis

Basic Memory Analysis

- In terms of memory acquisition of physical devices, below tools can be used. For virtual environments copying ‘.vmem’ memory file to an analysis tool is enough.
    - Win32dd/Win64dd
    - dd
    - Memoryze
    - Dumply,
    - Fastdump
- For process dumps LordPE, Process Hacker and Ollydump can be used.

Basic Memory Analysis

- After obtaining memory, memory can be implemented. In this case Volatility tool will be examined.



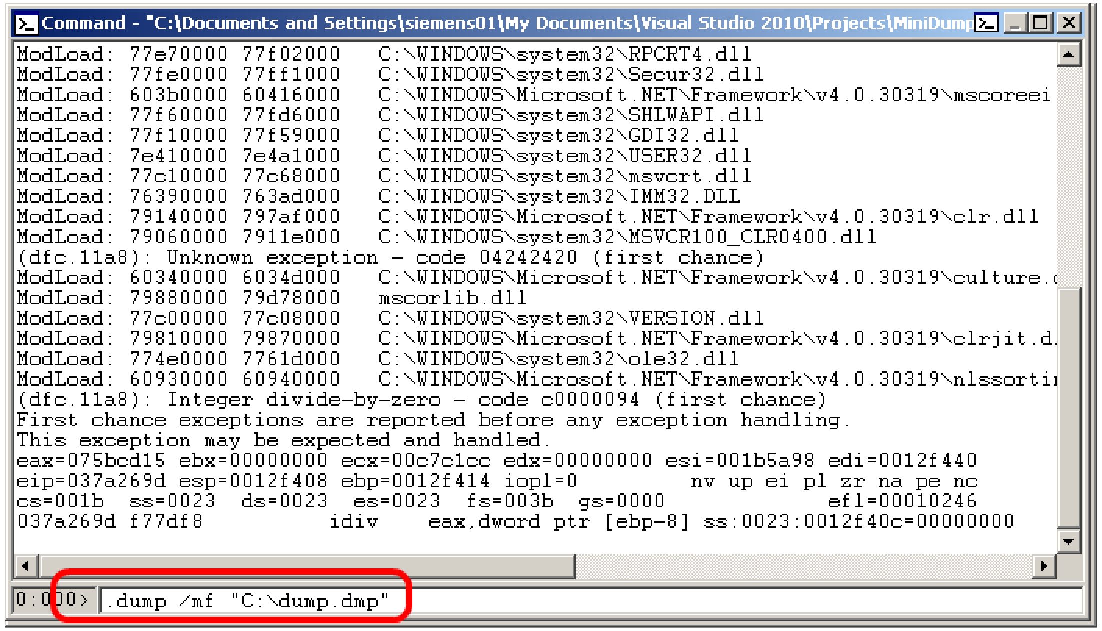
Basic Memory Analysis

- Inspection of a malware with memory analysis has some benefits. These are :
  - Rootkits can hide theirselves from classical detection approaches. Memory analysis can detect rootkits.
  - If a malware deleted , memory analysis process may gather information about it.
  - Memory forensics can provide clues for static and dynamic analysis.

ROOT
KIT
ROOT/ADMIN ACCESS
SET OF TOOLS

Basic Memory Analysis

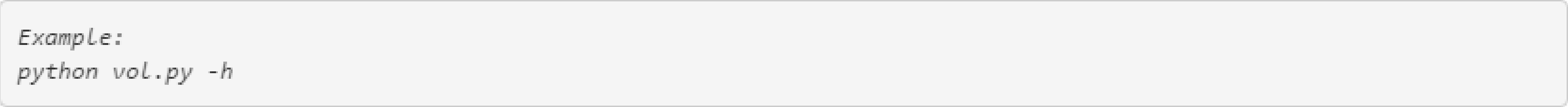
- Inspection of a malware with memory analysis has also some disadvantages. These are :
  - Memory maps are different for OS
  - Just for a limited time for analysis
  - Big memory, long time to analyze


Command - "C:\Documents and Settings\siemens01\My Documents\Visual Studio 2010\Projects\MiniDump

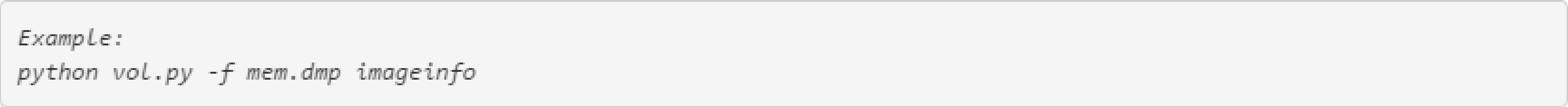
```
ModLoad: 77e70000 77f02000   C:\WINDOWS\system32\RPCRT4.dll
ModLoad: 77fe0000 77ff1000   C:\WINDOWS\system32\Secur32.dll
ModLoad: 603b0000 60416000   C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscoreei
ModLoad: 77f60000 77fd6000   C:\WINDOWS\system32\SHLWAPI.dll
ModLoad: 77f10000 77f59000   C:\WINDOWS\system32\GDI32.dll
ModLoad: 7e410000 7e4a1000   C:\WINDOWS\system32\USER32.dll
ModLoad: 77c10000 77c68000   C:\WINDOWS\system32\msvcrt.dll
ModLoad: 76390000 763ad000   C:\WINDOWS\system32\IMM32.DLL
ModLoad: 79140000 797af000   C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\clr.dll
ModLoad: 79060000 7911e000   C:\WINDOWS\system32\MSVCR100_CLR0400.dll
(dfc.11a8): Unknown exception - code 04242420 (first chance)
ModLoad: 60340000 6034d000   C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\culture.
ModLoad: 79880000 79d78000   mscorlib.dll
ModLoad: 77c00000 77c08000   C:\WINDOWS\system32\VERSION.dll
ModLoad: 79810000 79870000   C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\clrjit.d
ModLoad: 774e0000 7761d000   C:\WINDOWS\system32\ole32.dll
ModLoad: 60930000 60940000   C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\nlssorti
(dfc.11a8): Integer divide-by-zero - code c0000094 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=075bcd15 ebx=00000000 ecx=00c7c1cc edx=00000000 esi=001b5a98 edi=0012f440
eip=037a269d esp=0012f408 ebp=0012f414 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
037a269d f77df8          idiv    eax,dword ptr [ebp-8] ss:0023:0012f40c=00000000

0:000> .dump /mf "C:\dump.dmp"
```

Examining Files with Volatility

- Volatility is Python based memory forensics tool.
- OS Independent
- Open source Project
- Clarifies memory
- Can implement plugins



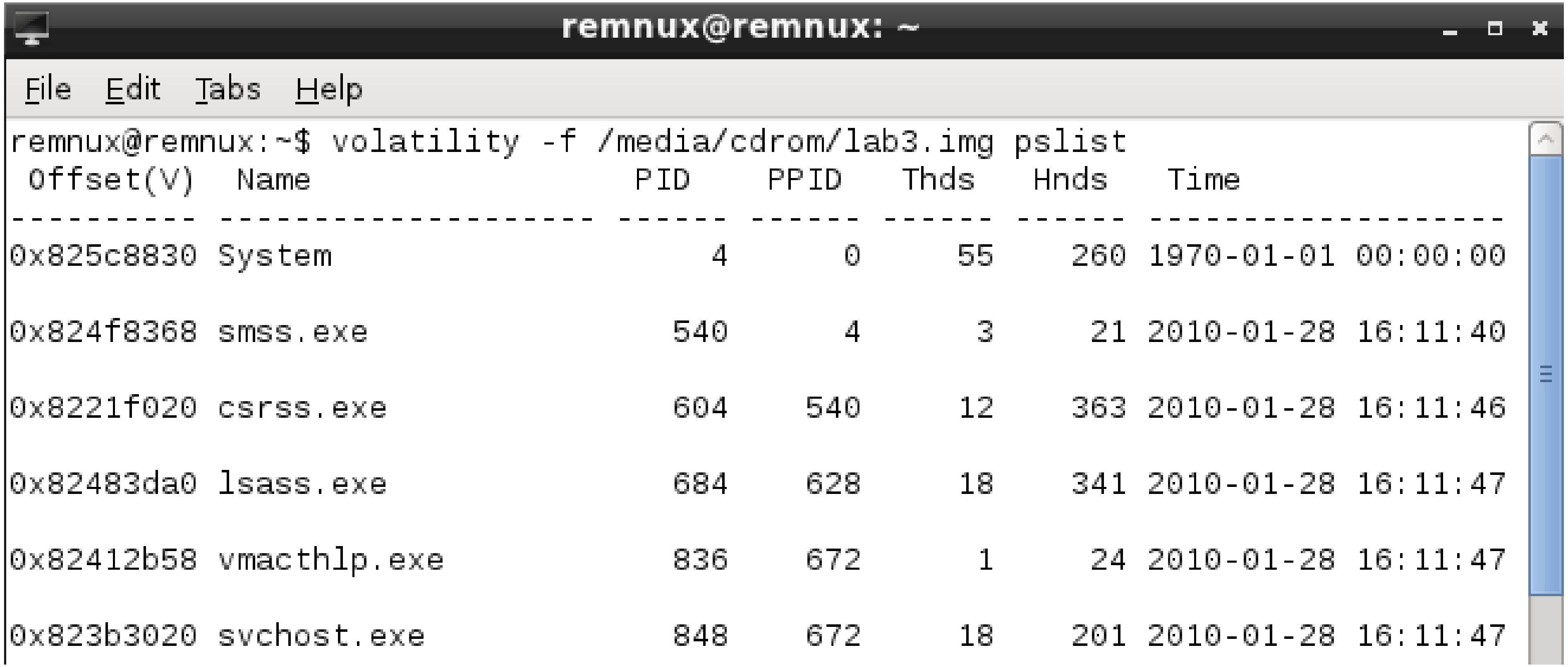
```
Example:
python vol.py -h
```



```
Example:
python vol.py -f mem.dmp imageinfo
```

Examining Files with Volatility

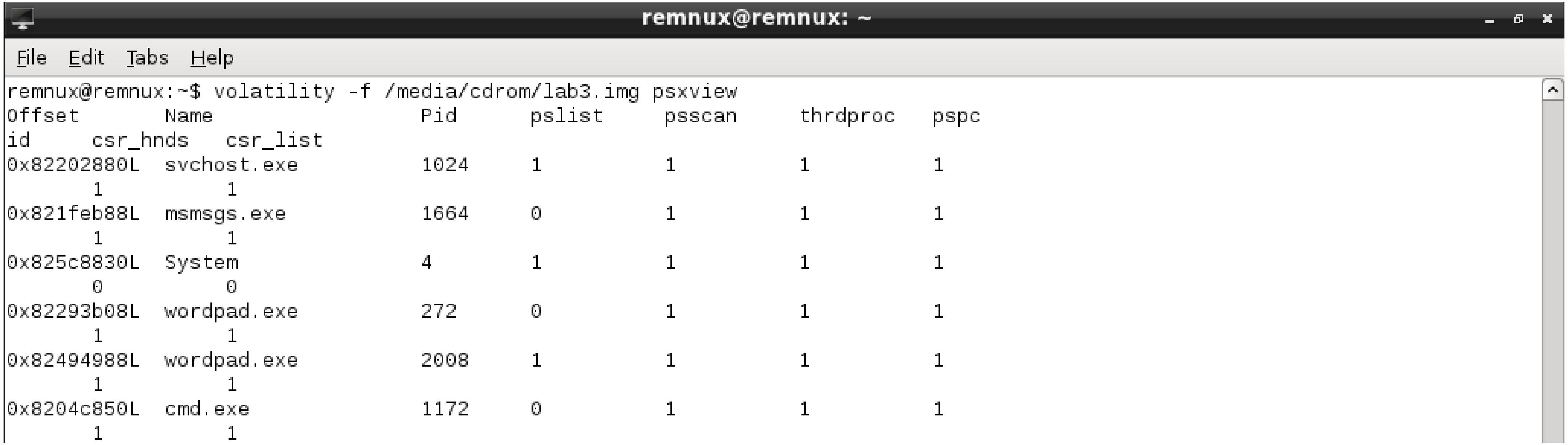
- Pslist : List all processes



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img pslist
 Offset(V)  Name                    PID    PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ -------------------
0x825c8830 System                    4      0     55    260 1970-01-01 00:00:00

0x824f8368 smss.exe                540      4      3     21 2010-01-28 16:11:40

0x8221f020 csrss.exe               604    540     12    363 2010-01-28 16:11:46

0x82483da0 lsass.exe               684    628     18    341 2010-01-28 16:11:47

0x82412b58 vmacthlp.exe            836    672      1     24 2010-01-28 16:11:47

0x823b3020 svchost.exe             848    672     18    201 2010-01-28 16:11:47
```

Examining Files with Volatility

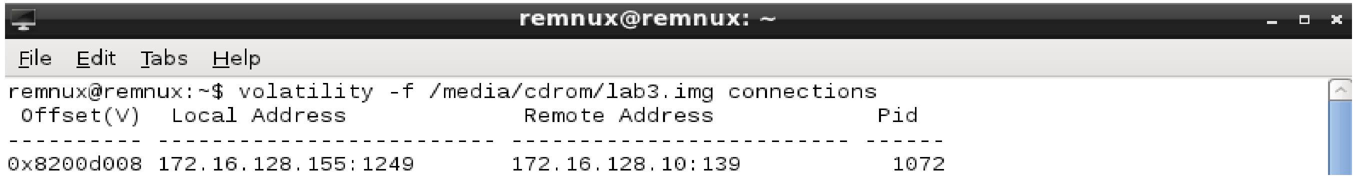
- Psxview : List all processes including hidden ones



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img psxview
Offset       Name                Pid      pslist     psscan     thrdproc   pspc
id      csr_hnds   csr_list
0x82202880L  svchost.exe         1024     1          1          1          1
       1          1
0x821feb88L  msmsgs.exe          1664     0          1          1          1
       1          1
0x825c8830L  System              4        1          1          1          1
       0          0
0x82293b08L  wordpad.exe         272      0          1          1          1
       1          1
0x82494988L  wordpad.exe         2008     1          1          1          1
       1          1
0x8204c850L  cmd.exe             1172     0          1          1          1
       1          1
```

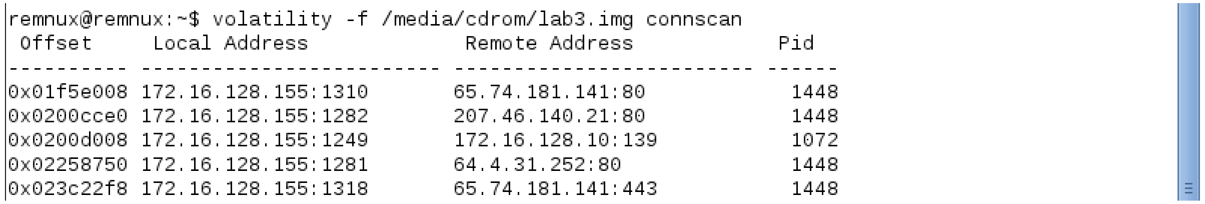
Examining Files with Volatility

- Connection : List network connections



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img connections
 Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ------
0x8200d008 172.16.128.155:1249       172.16.128.10:139           1072
```

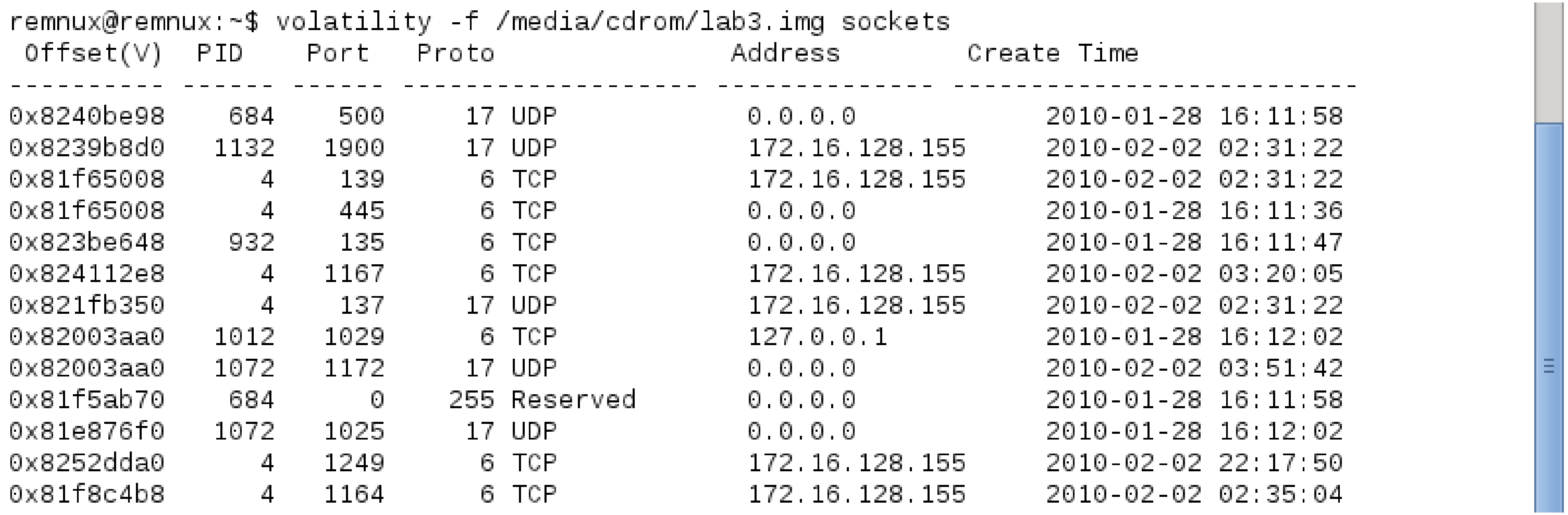
- Connscan : List all closed connections that remains in memory



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img connscan
 Offset     Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ------
0x01f5e008 172.16.128.155:1310       65.74.181.141:80            1448
0x0200cce0 172.16.128.155:1282       207.46.140.21:80            1448
0x0200d008 172.16.128.155:1249       172.16.128.10:139           1072
0x02258750 172.16.128.155:1281       64.4.31.252:80              1448
0x023c22f8 172.16.128.155:1318       65.74.181.141:443           1448
```

Examining Files with Volatility

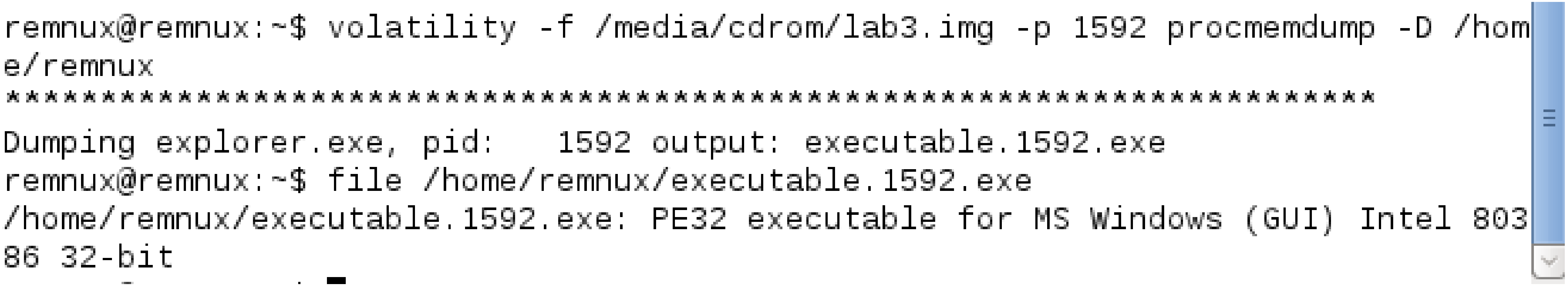
- Sockets and sockscan : List all the sockets and related processes



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img sockets
 Offset(V)  PID    Port   Proto               Address        Create Time
---------- ------ ------ ------------------- -------------- -------------------------
0x8240be98    684    500     17 UDP            0.0.0.0            2010-01-28 16:11:58
0x8239b8d0   1132   1900     17 UDP            172.16.128.155     2010-02-02 02:31:22
0x81f65008      4    139      6 TCP            172.16.128.155     2010-02-02 02:31:22
0x81f65008      4    445      6 TCP            0.0.0.0            2010-01-28 16:11:36
0x823be648    932    135      6 TCP            0.0.0.0            2010-01-28 16:11:47
0x824112e8      4   1167      6 TCP            172.16.128.155     2010-02-02 03:20:05
0x821fb350      4    137     17 UDP            172.16.128.155     2010-02-02 02:31:22
0x82003aa0   1012   1029      6 TCP            127.0.0.1          2010-01-28 16:12:02
0x82003aa0   1072   1172     17 UDP            0.0.0.0            2010-02-02 03:51:42
0x81f5ab70    684      0    255 Reserved       0.0.0.0            2010-01-28 16:11:58
0x81e876f0   1072   1025     17 UDP            0.0.0.0            2010-01-28 16:12:02
0x8252dda0      4   1249      6 TCP            172.16.128.155     2010-02-02 22:17:50
0x81f8c4b8      4   1164      6 TCP            172.16.128.155     2010-02-02 02:35:04
```

Examining Files with Volatility

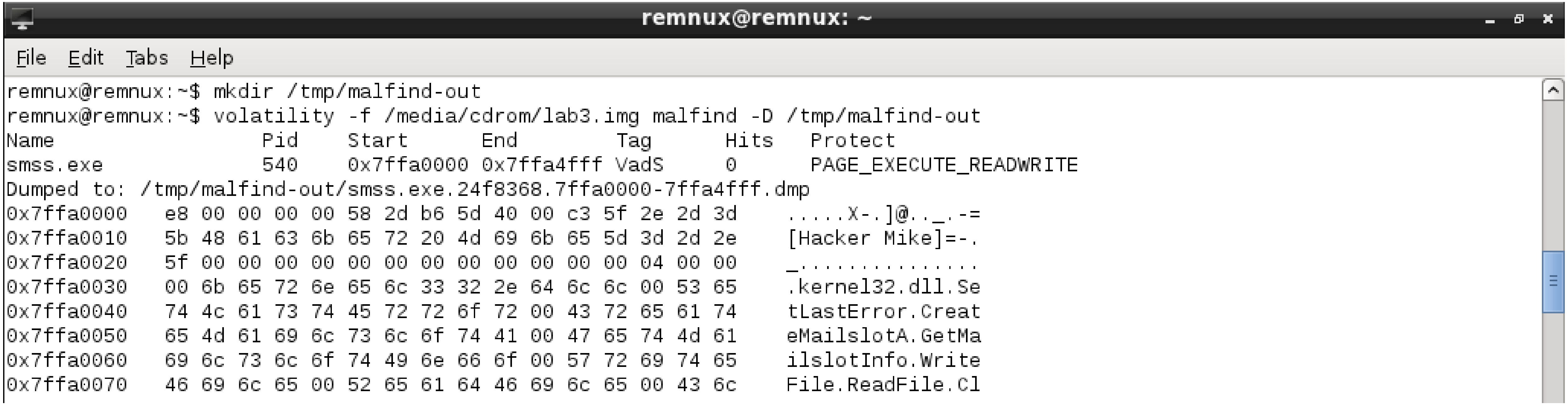
- Procmemdump : Disassembler and debugger provider for memory analysis



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img -p 1592 procmemdump -D /hom
e/remnux
************************************************************************
Dumping explorer.exe, pid:   1592 output: executable.1592.exe
remnux@remnux:~$ file /home/remnux/executable.1592.exe
/home/remnux/executable.1592.exe: PE32 executable for MS Windows (GUI) Intel 803
86 32-bit
```

Examining Files with Volatility

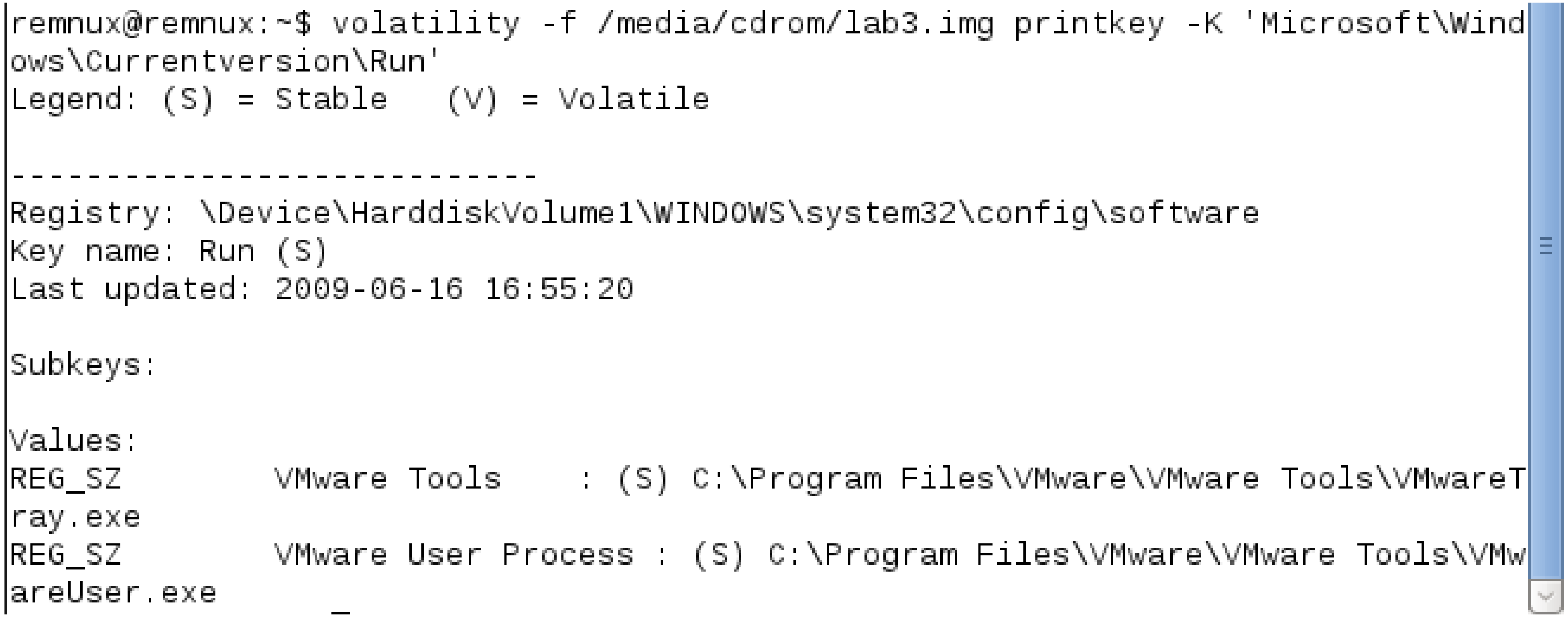
- Malfind : Provides to find malicious code parts in memory



```
remnux@remnux:~$ mkdir /tmp/malfind-out
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img malfind -D /tmp/malfind-out
Name                 Pid    Start      End        Tag      Hits   Protect
smss.exe             540    0x7ffa0000 0x7ffa4fff VadS     0      PAGE_EXECUTE_READWRITE
Dumped to: /tmp/malfind-out/smss.exe.24f8368.7ffa0000-7ffa4fff.dmp
0x7ffa0000   e8 00 00 00 00 58 2d b6 5d 40 00 c3 5f 2e 2d 3d    .....X-.]@.._.-=
0x7ffa0010   5b 48 61 63 6b 65 72 20 4d 69 6b 65 5d 3d 2d 2e    [Hacker Mike]=-.
0x7ffa0020   5f 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00    _...............
0x7ffa0030   00 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 53 65    .kernel32.dll.Se
0x7ffa0040   74 4c 61 73 74 45 72 72 6f 72 00 43 72 65 61 74    tLastError.Creat
0x7ffa0050   65 4d 61 69 6c 73 6c 6f 74 41 00 47 65 74 4d 61    eMailslotA.GetMa
0x7ffa0060   69 6c 73 6c 6f 74 49 6e 66 6f 00 57 72 69 74 65    ilslotInfo.Write
0x7ffa0070   46 69 6c 65 00 52 65 61 64 46 69 6c 65 00 43 6c    File.ReadFile.Cl
```

Examining Files with Volatility

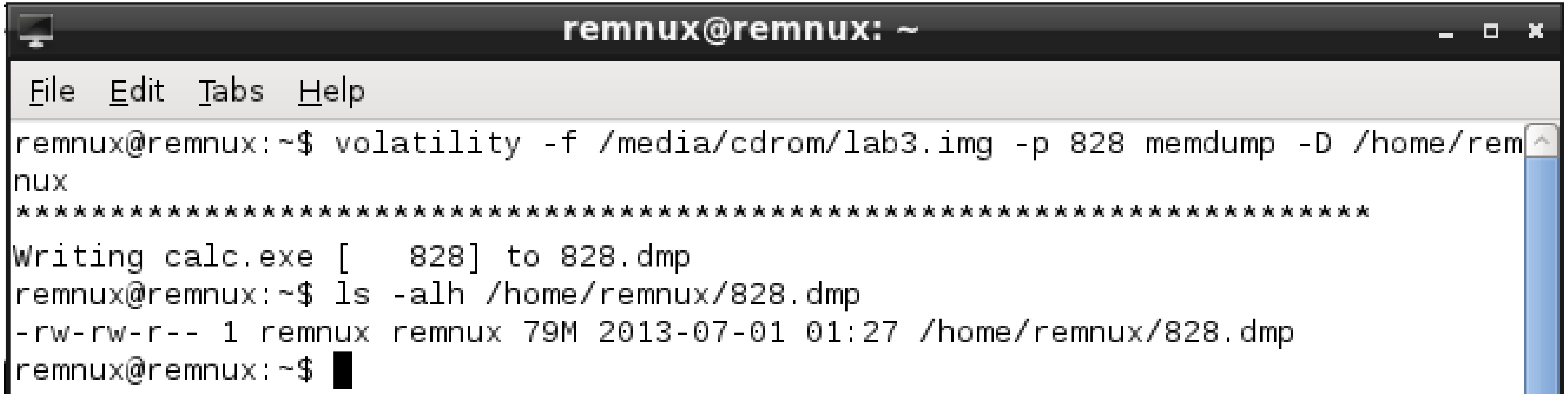
- Printkey : Informs registry operations in memory



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img printkey -K 'Microsoft\Wind
ows\Currentversion\Run'
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Run (S)
Last updated: 2009-06-16 16:55:20

Subkeys:

Values:
REG_SZ        VMware Tools     : (S) C:\Program Files\VMware\VMware Tools\VMwareT
ray.exe
REG_SZ        VMware User Process : (S) C:\Program Files\VMware\VMware Tools\VMw
areUser.exe      _
```

Examining Files with Volatility

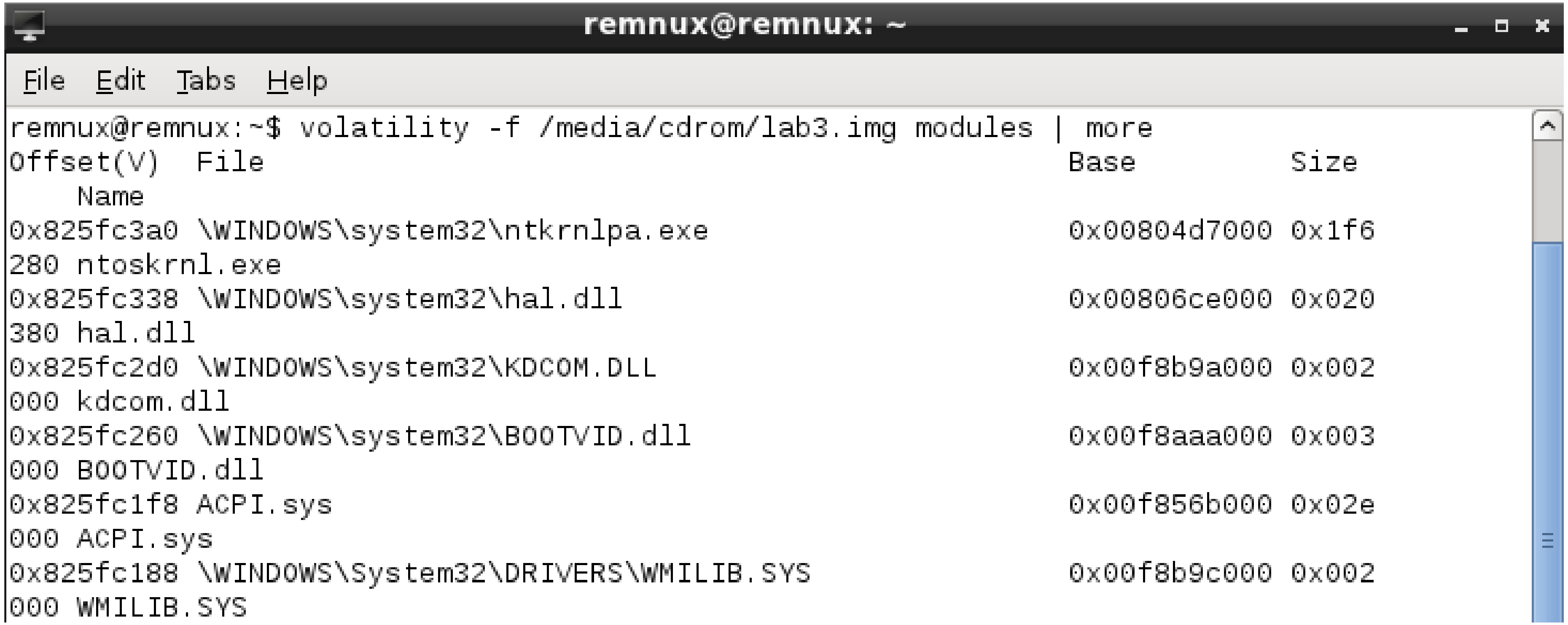
- Memdump : Provides memory image of a process



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img -p 828 memdump -D /home/rem
nux
************************************************************************
Writing calc.exe [   828] to 828.dmp
remnux@remnux:~$ ls -alh /home/remnux/828.dmp
-rw-rw-r-- 1 remnux remnux 79M 2013-07-01 01:27 /home/remnux/828.dmp
remnux@remnux:~$ 
```

Examining Files with Volatility

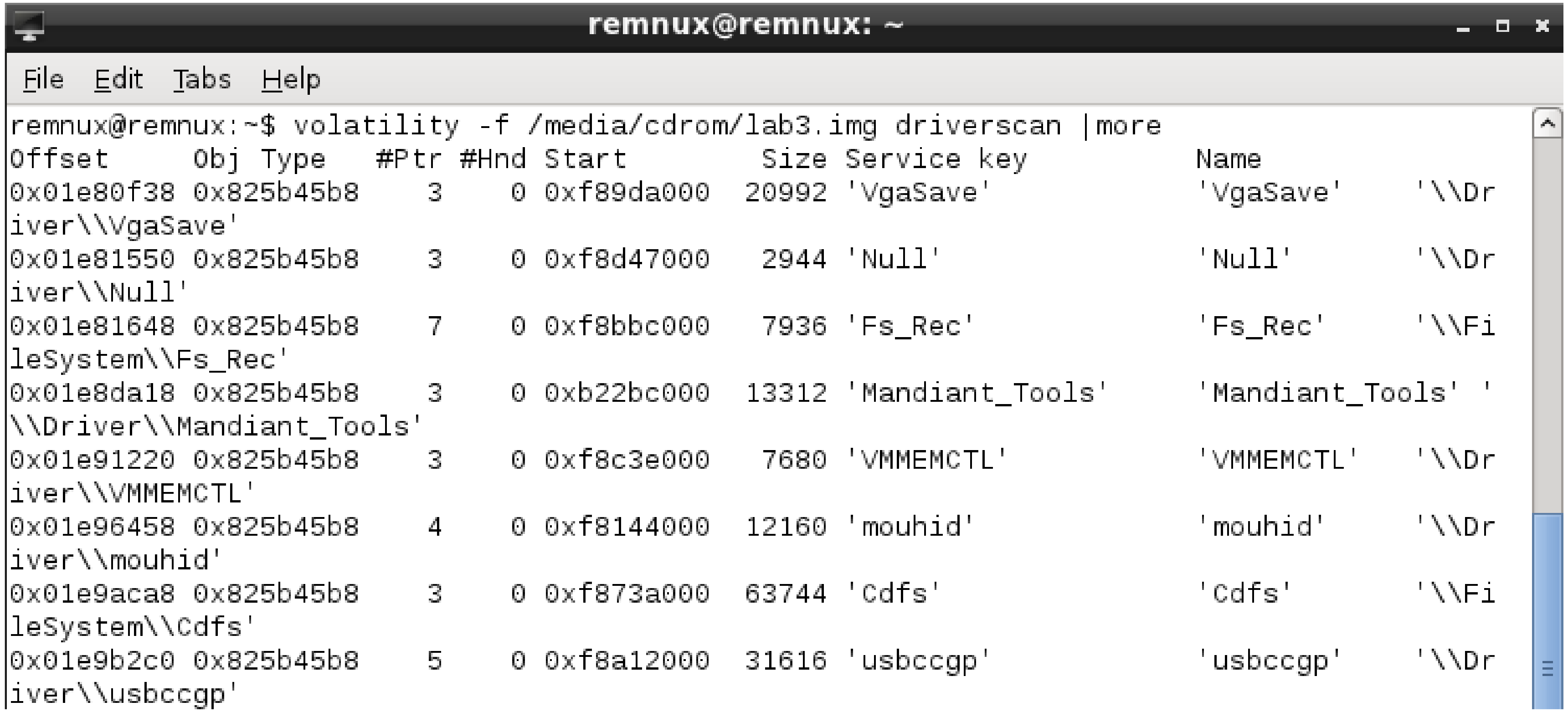
- Modules : Shows uploaded library modules in kernel



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img modules | more
Offset(V)  File                                                Base         Size
    Name
0x825fc3a0 \WINDOWS\system32\ntkrnlpa.exe                      0x00804d7000 0x1f6
280 ntoskrnl.exe
0x825fc338 \WINDOWS\system32\hal.dll                           0x00806ce000 0x020
380 hal.dll
0x825fc2d0 \WINDOWS\system32\KDCOM.DLL                         0x00f8b9a000 0x002
000 kdcom.dll
0x825fc260 \WINDOWS\system32\BOOTVID.dll                       0x00f8aaa000 0x003
000 BOOTVID.dll
0x825fc1f8 ACPI.sys                                            0x00f856b000 0x02e
000 ACPI.sys
0x825fc188 \WINDOWS\System32\DRIVERS\WMILIB.SYS                0x00f8b9c000 0x002
000 WMILIB.SYS
```

Examining Files with Volatility

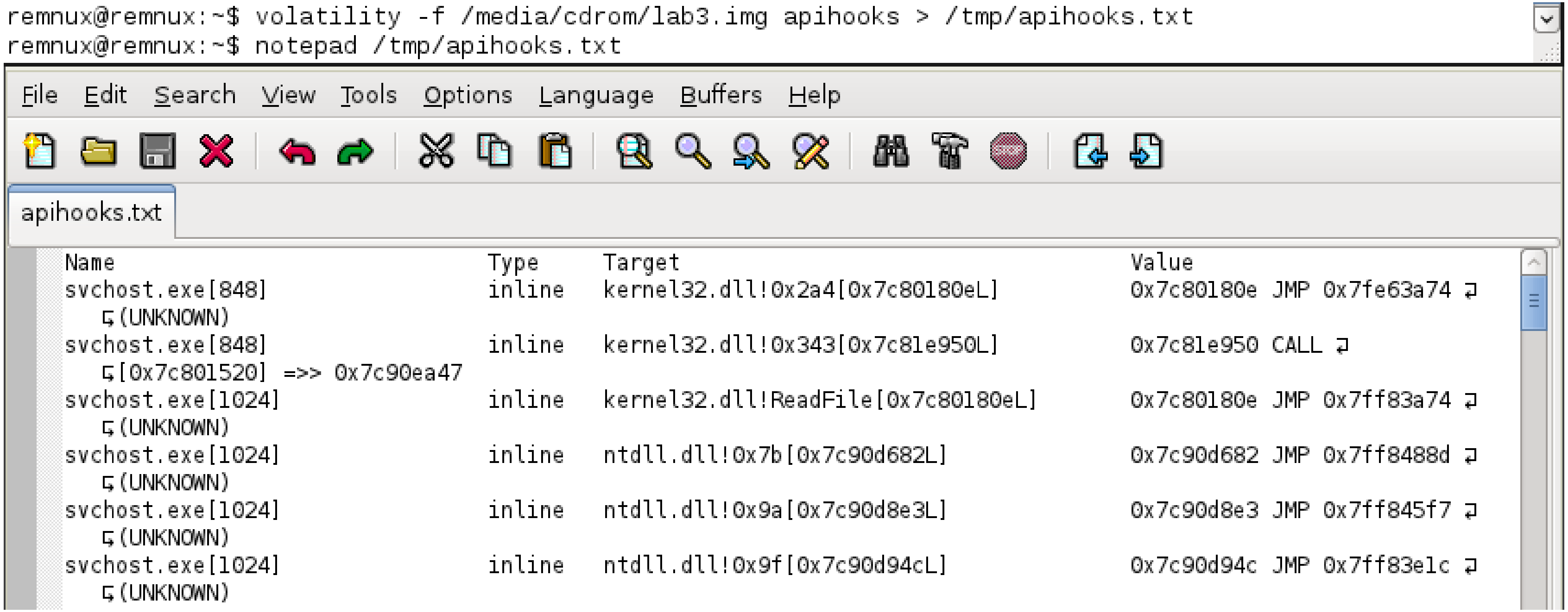
- Driverscan : Shows installed drivers for memory



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img driverscan |more
Offset     Obj Type   #Ptr #Hnd Start        Size Service key          Name
0x01e80f38 0x825b45b8    3    0 0xf89da000  20992 'VgaSave'            'VgaSave'     '\\Dr
iver\\VgaSave'
0x01e81550 0x825b45b8    3    0 0xf8d47000   2944 'Null'               'Null'        '\\Dr
iver\\Null'
0x01e81648 0x825b45b8    7    0 0xf8bbc000   7936 'Fs_Rec'             'Fs_Rec'      '\\Fi
leSystem\\Fs_Rec'
0x01e8da18 0x825b45b8    3    0 0xb22bc000  13312 'Mandiant_Tools'     'Mandiant_Tools' '
\\Driver\\Mandiant_Tools'
0x01e91220 0x825b45b8    3    0 0xf8c3e000   7680 'VMMEMCTL'           'VMMEMCTL'    '\\Dr
iver\\VMMEMCTL'
0x01e96458 0x825b45b8    4    0 0xf8144000  12160 'mouhid'             'mouhid'      '\\Dr
iver\\mouhid'
0x01e9aca8 0x825b45b8    3    0 0xf873a000  63744 'Cdfs'               'Cdfs'        '\\Fi
leSystem\\Cdfs'
0x01e9b2c0 0x825b45b8    5    0 0xf8a12000  31616 'usbccgp'            'usbccgp'     '\\Dr
iver\\usbccgp'
```

Examining Files with Volatility

- Apihooks : Shows possible hooked processes

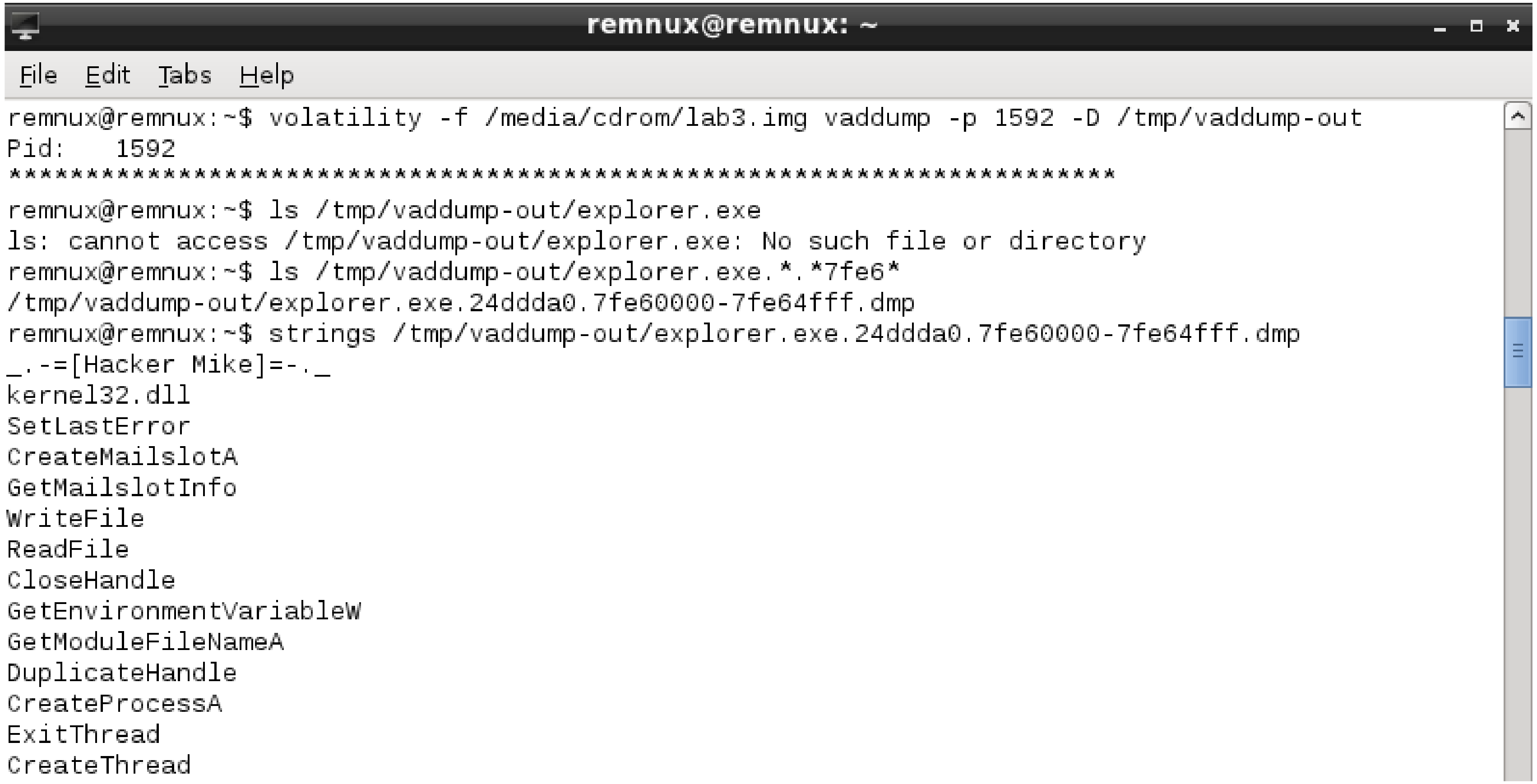


```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img apihooks > /tmp/apihooks.txt
remnux@remnux:~$ notepad /tmp/apihooks.txt
```

```
Name                        Type     Target                                 Value
svchost.exe[848]            inline   kernel32.dll!0x2a4[0x7c80180eL]        0x7c80180e JMP 0x7fe63a74 ↲
   ↳(UNKNOWN)
svchost.exe[848]            inline   kernel32.dll!0x343[0x7c81e950L]        0x7c81e950 CALL ↲
   ↳[0x7c801520] =>> 0x7c90ea47
svchost.exe[1024]           inline   kernel32.dll!ReadFile[0x7c80180eL]     0x7c80180e JMP 0x7ff83a74 ↲
   ↳(UNKNOWN)
svchost.exe[1024]           inline   ntdll.dll!0x7b[0x7c90d682L]            0x7c90d682 JMP 0x7ff8488d ↲
   ↳(UNKNOWN)
svchost.exe[1024]           inline   ntdll.dll!0x9a[0x7c90d8e3L]            0x7c90d8e3 JMP 0x7ff845f7 ↲
   ↳(UNKNOWN)
svchost.exe[1024]           inline   ntdll.dll!0x9f[0x7c90d94cL]            0x7c90d94c JMP 0x7ff83e1c ↲
   ↳(UNKNOWN)
```

Examining Files with Volatility

- Vaddump : Acquisition of particular memory dump



```
remnux@remnux:~$ volatility -f /media/cdrom/lab3.img vaddump -p 1592 -D /tmp/vaddump-out
Pid:   1592
************************************************************************
remnux@remnux:~$ ls /tmp/vaddump-out/explorer.exe
ls: cannot access /tmp/vaddump-out/explorer.exe: No such file or directory
remnux@remnux:~$ ls /tmp/vaddump-out/explorer.exe.*.*7fe6*
/tmp/vaddump-out/explorer.exe.24ddda0.7fe60000-7fe64fff.dmp
remnux@remnux:~$ strings /tmp/vaddump-out/explorer.exe.24ddda0.7fe60000-7fe64fff.dmp
_.-=[Hacker Mike]=-._
kernel32.dll
SetLastError
CreateMailslotA
GetMailslotInfo
WriteFile
ReadFile
CloseHandle
GetEnvironmentVariableW
GetModuleFileNameA
DuplicateHandle
CreateProcessA
ExitThread
CreateThread
```

Example

- Zeus.vmem