取证

介绍

何为取证?

电子取证是指利用计算机软硬件技术，以符合法律规范的方式对计算机入侵、破坏、欺诈、攻击等犯罪行为进行证据获取、保存、分析和出示的过程。从技术方面看，计算机犯罪取证是一个对受侵计算机系统进行扫描和破解，对入侵事件进行重建的过程。具体而言，是指把计算机看作犯罪现场，运用先进的辨析技术，对计算机犯罪行为进行解剖，搜寻罪犯及其犯罪证据。

接下来我们从常用的取证工具入手，来讲解取证的常见内容。

之所以从工具入手，是因为取证过程中如果不依靠现有的强大工具，就需要取证的人自己对相关数据文件的数据存储格式有详细的了解乃至是掌握。 取证工具的本质其实就是对已知存储格式的数据从格式上进行自动化地解析使得使用者可以轻松提取相应的数据资料。如果以手工的方式的话则需要大篇幅的内容来讲解各种诸如硬盘系统数据文件、内存镜像数据文件一类的相关数据存储的格式。

内存取证——Volatility

Volatility是开源的Windows，Linux，MaC，Android的内存取证分析工具，由python编写成，命令行操作，支持各种操作系统。

并且该工具属于框架类工具。即其本身除却官方自己实现的功能插件外，用户可以根据自己需要来制作自定义插件。

通过-h参数可以列举出本地工具已经集成了的功能插件以及相关描述。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.raw -h
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
```

这里介绍一个叫dumpIt的工具，它可以把当前运行的系统的内存数据导出为静态镜像文件。

imageinfo

对于内存取证，不同版本的系统运行时的内存数据格式是不一样的，利用这一点，可以先行分析出目标内存镜像对应的系统版本。然后再根据系统版本进行下一步的分析。

功能插件为imageinfo，

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000,
 Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/study/2020/hxb/misc/1.r
aw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x83f61c28L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x83f62c00L
                KPCR for CPU 1 : 0x807ca000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-09-27 15:20:52 UTC+0000
     Image local date and time : 2019-09-27 23:20:52 +0800
```

pstree|pslist|psscan|psxview

ps插件全家桶。它们的功能如图： 对内存数据进行分析显然不能错过系统运行时的进程信息分析。而这四个命令则类似Linux系统中的ps命令，可以列举系统运行中的进程。 根据列举出的进程可以初步猜测是否受到了进程注入类的攻击。

```
pslist          Print all running processes by following the EPROCESS lists
psscan          Pool scanner for process objects
pstree          Print process list as a tree
psxview         Find hidden processes with various process listings
```

三者的详细区别：

- pslist。不仅显示了所有正在运行的进程，而且给出了有价值的信息，比如PID、PPID、启动的时间。
- pstree。pslist的改进版，可以识别子进程以及父进程
- psscan。可以显示出被恶意软件比如rootkit为了躲避用户或杀毒软件而隐藏的进程
- psxview。psscan的改进版。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.raw --profile=Win7SP0x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0x8634b7e0 System                    4      0     91      472 ------      0 2019-09-27 15:19:00 UTC+0000
0x86f4b280 smss.exe                252      4      2       30 ------      0 2019-09-27 15:19:00 UTC+0000
0x875d4030 csrss.exe               336    320     10      486      0      0 2019-09-27 15:19:03 UTC+0000
0x87786390 csrss.exe               388    380     10      218      1      0 2019-09-27 15:19:04 UTC+0000
0x8778e030 wininit.exe             396    320      4       82      0      0 2019-09-27 15:19:04 UTC+0000
0x877ae3e0 winlogon.exe            448    380      6      120      1      0 2019-09-27 15:19:04 UTC+0000
0x877ec300 services.exe            496    396     15      224      0      0 2019-09-27 15:19:05 UTC+0000
0x877f77a8 lsass.exe               504    396     10      579      0      0 2019-09-27 15:19:05 UTC+0000
0x877f8b70 lsm.exe                 512    396     11      151      0      0 2019-09-27 15:19:05 UTC+0000
0x87896530 svchost.exe             608    496     13      372      0      0 2019-09-27 15:19:07 UTC+0000
0x8659a030 vmacthlp.exe            676    496      3       55      0      0 2019-09-27 15:19:07 UTC+0000
0x878bc030 svchost.exe             720    496      8      280      0      0 2019-09-27 15:19:08 UTC+0000
0x878e94b8 svchost.exe             820    496     20      401      0      0 2019-09-27 15:19:08 UTC+0000
0x878f2a00 svchost.exe             852    496     21      395      0      0 2019-09-27 15:19:08 UTC+0000
0x878f7b08 svchost.exe             884    496     44      877      0      0 2019-09-27 15:19:08 UTC+0000
0x879110b0 audiodg.exe             964    820      7      131      0      0 2019-09-27 15:19:09 UTC+0000
0x87927d40 svchost.exe            1036    496     14      556      0      0 2019-09-27 15:19:09 UTC+0000
0x87946030 svchost.exe            1124    496     17      365      0      0 2019-09-27 15:19:09 UTC+0000
0x8783b030 spoolsv.exe            1284    496     16      316      0      0 2019-09-27 15:19:11 UTC+0000
0x87853030 svchost.exe            1312    496     22      319      0      0 2019-09-27 15:19:11 UTC+0000
0x879db820 VGAuthService.         1480    496      3       84      0      0 2019-09-27 15:19:12 UTC+0000
0x879c4aa0 vmtoolsd.exe           1520    496     10      271      0      0 2019-09-27 15:19:13 UTC+0000
0x870e6838 svchost.exe            1740    496      7       94      0      0 2019-09-27 15:19:15 UTC+0000
0x87156398 dllhost.exe            1984    496     22      200      0      0 2019-09-27 15:19:17 UTC+0000
```

memdump

memdump可以提取出内存中的进程数据。许多进程在运行时，原始数据都是在进程中存储的，比较经典的例子就是画图程序。memdump导出的画图程序内存数据导入图像处理程序调整长宽后可以直接恢复图像内容。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 memdump -p 2440 -D ./
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing notepad.exe [  2440] to 2440.dmp
root@xibai-kali:~/桌面/study/2020/hxb/misc#
```

procdump

提取进程的可执行文件。通过导出可疑进程的可执行文件来对其进行逆向分析，挖掘可能存在的后面病毒木马之类的程序。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 procdump -p 2440 -D ./
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x87e37958 0x01000000 notepad.exe          OK: executable.2440.exe
```

timeliner

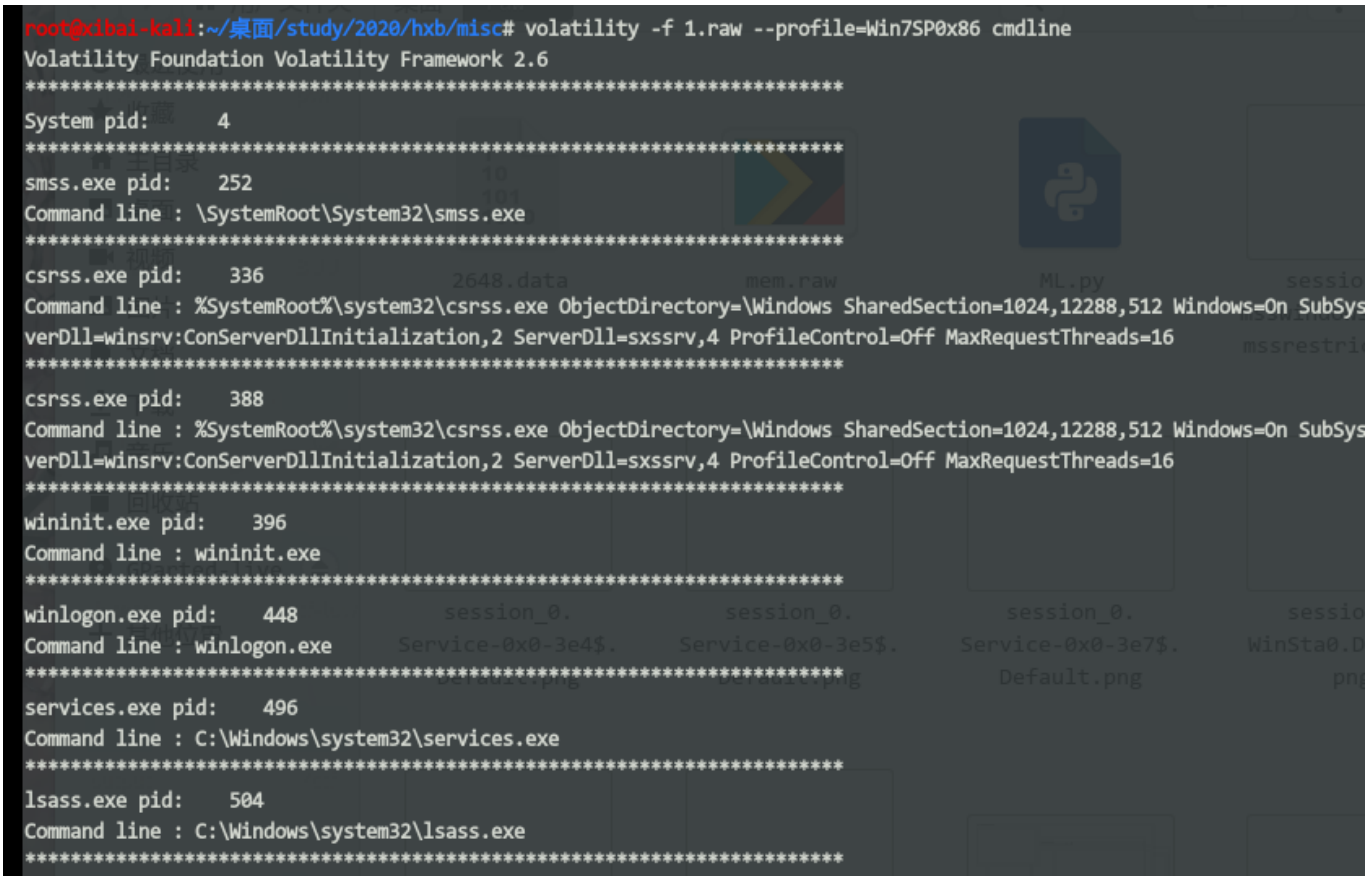
根据时间线列举系统行为。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x
86 timeliner
Volatility Foundation Volatility Framework 2.6
2019-12-20 15:42:24 UTC+0000|[LIVE RESPONSE]| (System time)|
2019-09-20 13:40:35 UTC+0000|[IEHISTORY]| explorer.exe->Visited: Administrator@about:H
ome| PID: 2028/Cache type "URL " at 0xb25100 End: 2019-09-20 13:40:35 UTC+0000
2019-12-20 15:41:43 UTC+0000|[IEHISTORY]| explorer.exe->Visited: Administrator@file://
/C:/Documents%20and%20Settings/Administrator/????/file.txt| PID: 2028/Cache type "URL
" at 0xb25200 End: 2019-12-20 15:41:43 UTC+0000
2019-12-20 22:12:07 UTC+0000|[IEHISTORY]| explorer.exe->:2019122020191221: Administrat
or@:Host: ????????| PID: 2028/Cache type "URL " at 0xbd5100 End: 2019-12-20 14:12:07 U
TC+0000
2019-12-20 23:41:43 UTC+0000|[IEHISTORY]| explorer.exe->:2019122020191221: Administrat
or@file:///C:/Documents%20and%20Settings/Administrator/????/file.txt| PID: 2028/Cache
type "URL " at 0xbd5200 End: 2019-12-20 15:41:43 UTC+0000
```

cmdline|cmdscan|consoles

这三个功能插件可以列举系统运行时由cmd执行过的命令

```
cmdline         Display process command-line arguments
cmdscan         Extract command history by scanning for _COMMAND_HISTORY
```



iehistory

此插件可以查看系统运行时的浏览缓存历史。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 iehistory
Volatility Foundation Volatility Framework 2.6
**************************************************
Process: 2028 explorer.exe
Cache type "DEST" at 0x14389d
Last modified: 2019-12-20 23:41:43 UTC+0000
Last accessed: 2019-12-20 15:41:44 UTC+0000
URL: Administrator@file:///C:/Documents%20and%20Settings/Administrator/Lhb/file.txt
**************************************************
Process: 2028 explorer.exe
Cache type "DEST" at 0x143b15
Last modified: 2019-12-20 23:41:43 UTC+0000
Last accessed: 2019-12-20 15:41:44 UTC+0000
URL: Administrator@file:///C:/Documents%20and%20Settings/Administrator/Lhb/file.txt
**************************************************
Process: 2028 explorer.exe
Cache type "URL " at 0xb25100
Record length: 0x100
Location: Visited: Administrator@about:Home
Last modified: 2019-09-20 13:40:35 UTC+0000
Last accessed: 2019-09-20 13:40:35 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x8c
**************************************************
Process: 2028 explorer.exe
Cache type "URL " at 0xb25200
Record length: 0x100
Location: Visited: Administrator@file:///C:/Documents%20and%20Settings/Administrator/????/file.txt
Last modified: 2019-12-20 15:41:43 UTC+0000
Last accessed: 2019-12-20 15:41:43 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xc4
**************************************************
Process: 2028 explorer.exe
Cache type "URL " at 0xbd5100
Record length: 0x100
Location: :2019122020191221: Administrator@:Host: ????????
```

connections|connscan

这两个插件则可以列举系统当时的网络连接情况

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x04d2d820 192.168.202.136:135      192.168.202.136:1027      828
0x04d2da08 192.168.202.136:1027     192.168.202.136:135       1240
```

notepad|editbox

这两个插件可以找出正在编辑中的文本数据。editbox比notepad适用性广一点。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 notepad
Volatility Foundation Volatility Framework 2.6
Process: 2440
Text:
?

Text:
d

Text:

Text:
?

Text:
??????????????????????????????????????????????????????????????flag????????????md5??

???md5(???:??)

root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 editbox
Volatility Foundation Volatility Framework 2.6
******************************
Wnd Context       : 0\WinSta0\Default
Process ID        : 2440
ImageFileName     : notepad.exe
IsWow64           : No
atom_class        : 6.0.3790.1830!Edit
value-of WndExtra : -
```

filescan|dumpfiles

`filescan`可以输出系统文件列表。`dumpfiles`可以提取被加载进内存的文件数据。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 filescan | grep txt
Volatility Foundation Volatility Framework 2.6
0x0000000000412cde0      1      0 RW-r-- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\file.txt
0x000000000426b890      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\win7gadgets.txt
0x000000000426ba90      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
0x000000000426bc90      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
0x000000000426be90      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\vistasidebar.txt
0x000000000479d4a8      4      2 -W-rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware VGAuth\logfile.txt.0
0x00000000049e1cf0      1      0 R--rw- \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\vmacthlp.txt
0x00000000049e6228      1      0 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Recent\file.txt.lnk
0x0000000004a511a0      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
0x0000000004a513a0      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\googledesktop.txt
0x0000000004a51770      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt
0x0000000004c05370      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\manifest.txt
0x0000000004c70ae8      1      0 RW---- \Device\HarddiskVolume1\WINDOWS\system32\CatRoot2\dberr.txt
0x0000000004d44028      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 dumpfiles -Q 0x0000000000412cde0 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x0412cde0   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\file.txt
```

hashdump

该工具可以抓取当前系统中的用户名及其密码对应的NTML哈希值

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x
86 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:8d9221b8e70124641a83291d3d21f7e
0:::
9w3a6J0$:1003:e761601f5cf981c136077a718ccdf409:ec9dc7d0895ad3dae1feba8ffdeacffd:::
4hiU9ZK$:1004:de5eea9d3fd12c34aad3b435b51404ee:2f2d544c53b3031f24d63402ea7fb4f9:::
A4W7iKb$:1005:61339c1be342167eaad3b435b51404ee:b6e6f6a85f90219d619aca4706f354fc:::
oeTQczq$:1006:b4d2cf4a862f6fcaaad3b435b51404ee:3fbc1f9dc4416f6fb3666de834185cb4:::
CAlrXyU$:1007:8ea6fb8594a1b952aad3b435b51404ee:51d603c77a884df049f7ed4dabed4fd4:::
AVqKsvQ$:1008:939e0f8990e68047aad3b435b51404ee:1796c2db94ce6276744f88b740152154:::
scdTbYy$:1009:792677ee54a26732891c5133c13673e8:138393419f9b418eb735d36e1da50a5e:::
```

hivelist|hivescan|hivedump

hivescan插件显示了可用的注册表配置单元的物理地址

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x
86 hivescan
Volatility Foundation Volatility Framework 2.6
Offset(P)
----------
0x0d7eb008
0x0d95b008
0x0da280b0
0x0da35a80
0x0e0dda80
0x12d41008
0x12d8e860
0x12df8200
0x12eab008
0x1776ea80
0x17851260
0x17b28008
0x17b31008
```

更加详细的信息可以通过hivelist命令查看，这条命令会显示虚拟地址、物理地址的细节以及更容易识别的路径等

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x
86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe174a008 0x12eab008 \Device\HarddiskVolume1\Documents and Settings\Administrator\Loc
al Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1013008 0x17b28008 [no name]
0xe101d008 0x17b31008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe12fb260 0x17851260 [no name]
0xe1756200 0x12df8200 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1763008 0x12d41008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe13c9a80 0x1776ea80 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1757860 0x12d8e860 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe24560b0 0x0da280b0 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NT
USER.DAT
0xe2460a80 0x0da35a80 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Lo
cal Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe247c008 0x0d95b008 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUS
ER.DAT
0xe2484008 0x0d7eb008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Loca
l Settings\Application Data\Microsoft\Windows\UsrClass.dat
```

hivedump则可以导出注册表信息

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 dumpregistry -o 0xe1757
860 -D ./
Volatility Foundation Volatility Framework 2.6
**********************************************
Writing out registry: registry.0xe1757860.SAM.reg

**********************************************
```

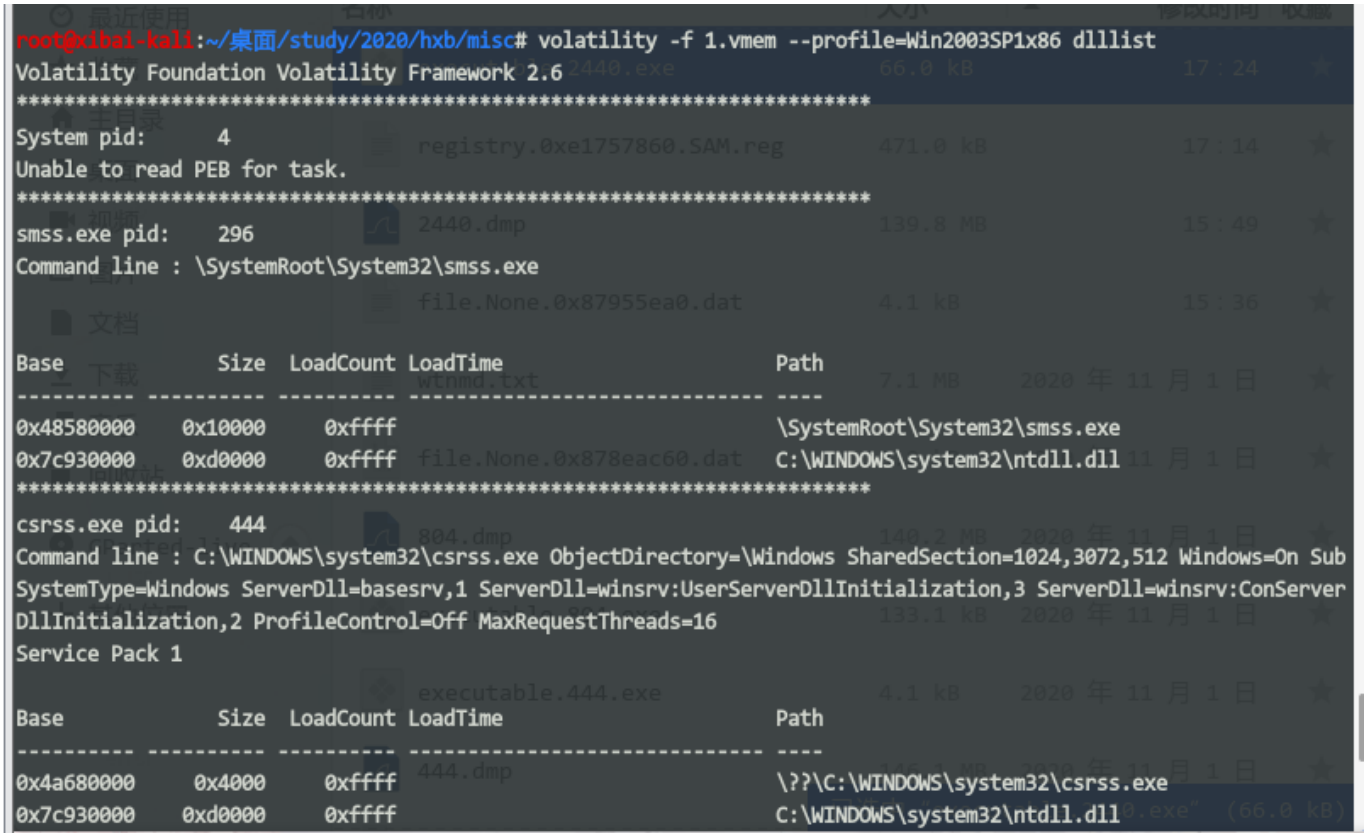
printkey

查看内存加载的注册表中的键值

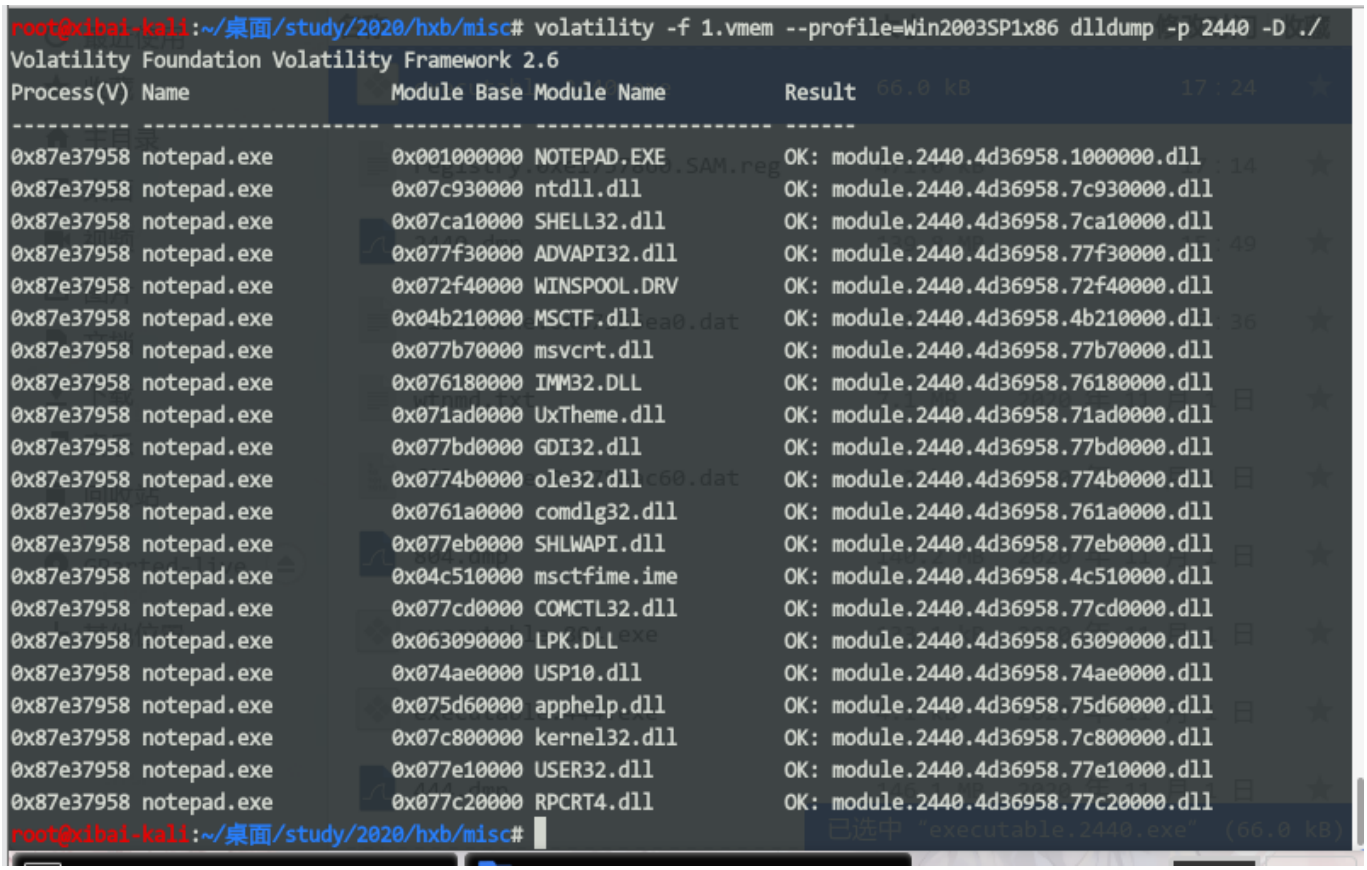
```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 printkey -K "SAM"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
Key name: SAM (V)
Last updated: 2019-12-20 14:18:07 UTC+0000

Subkeys:

Values:
REG_LINK      SymbolicLinkValue : (V) \Registry\Machine\SAM\SAM
----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
Key name: SAM (S)
Last updated: 2019-12-20 14:02:09 UTC+0000

Subkeys:
  (S) Domains
  (S) RXACT
```

dlllist|dlldump

dlllist可以看到每个进程运行需要的dll，dlldump可以导出进程运行中加载的dll



```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 dlllist
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    296
Command line : \SystemRoot\System32\smss.exe

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x48580000    0x10000     0xffff                                \SystemRoot\System32\smss.exe
0x7c930000    0xd0000     0xffff                                C:\WINDOWS\system32\ntdll.dll
************************************************************************
csrss.exe pid:    444
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On Sub
SystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServer
DllInitialization,2 ProfileControl=Off MaxRequestThreads=16
Service Pack 1

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x4a680000     0x4000     0xffff                                \??\C:\WINDOWS\system32\csrss.exe
0x7c930000    0xd0000     0xffff                                C:\WINDOWS\system32\ntdll.dll
```



```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 dlldump -p 2440 -D ./
Volatility Foundation Volatility Framework 2.6
Process(V) Name              Module Base Module Name          Result
---------- ----------------- ----------- ------------------ ------
0x87e37958 notepad.exe       0x001000000 NOTEPAD.EXE        OK: module.2440.4d36958.1000000.dll
0x87e37958 notepad.exe       0x07c930000 ntdll.dll          OK: module.2440.4d36958.7c930000.dll
0x87e37958 notepad.exe       0x07ca10000 SHELL32.dll        OK: module.2440.4d36958.7ca10000.dll
0x87e37958 notepad.exe       0x077f30000 ADVAPI32.dll       OK: module.2440.4d36958.77f30000.dll
0x87e37958 notepad.exe       0x072f40000 WINSPOOL.DRV       OK: module.2440.4d36958.72f40000.dll
0x87e37958 notepad.exe       0x04b210000 MSCTF.dll          OK: module.2440.4d36958.4b210000.dll
0x87e37958 notepad.exe       0x077b70000 msvcrt.dll         OK: module.2440.4d36958.77b70000.dll
0x87e37958 notepad.exe       0x076180000 IMM32.DLL          OK: module.2440.4d36958.76180000.dll
0x87e37958 notepad.exe       0x071ad0000 UxTheme.dll        OK: module.2440.4d36958.71ad0000.dll
0x87e37958 notepad.exe       0x077bd0000 GDI32.dll          OK: module.2440.4d36958.77bd0000.dll
0x87e37958 notepad.exe       0x0774b0000 ole32.dll          OK: module.2440.4d36958.774b0000.dll
0x87e37958 notepad.exe       0x0761a0000 comdlg32.dll       OK: module.2440.4d36958.761a0000.dll
0x87e37958 notepad.exe       0x077eb0000 SHLWAPI.dll        OK: module.2440.4d36958.77eb0000.dll
0x87e37958 notepad.exe       0x04c510000 msctfime.ime       OK: module.2440.4d36958.4c510000.dll
0x87e37958 notepad.exe       0x077cd0000 COMCTL32.dll       OK: module.2440.4d36958.77cd0000.dll
0x87e37958 notepad.exe       0x063090000 LPK.DLL            OK: module.2440.4d36958.63090000.dll
0x87e37958 notepad.exe       0x074ae0000 USP10.dll          OK: module.2440.4d36958.74ae0000.dll
0x87e37958 notepad.exe       0x075d60000 apphelp.dll        OK: module.2440.4d36958.75d60000.dll
0x87e37958 notepad.exe       0x07c800000 kernel32.dll       OK: module.2440.4d36958.7c800000.dll
0x87e37958 notepad.exe       0x077e10000 USER32.dll         OK: module.2440.4d36958.77e10000.dll
0x87e37958 notepad.exe       0x077c20000 RPCRT4.dll         OK: module.2440.4d36958.77c20000.dll
root@xibai-kali:~/桌面/study/2020/hxb/misc#
```

svcscan（限windwos）

查看开启的windows服务。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 svcscan
Volatility Foundation Volatility Framework 2.6
Offset: 0x621e90
Order: 1
Start: SERVICE_DISABLED
Process ID: -
Service Name: Abiosdsk
Display Name: Abiosdsk
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -
Offset: 0x621f28
Order: 2
Start: SERVICE_BOOT_START
Process ID: -
Service Name: ACPI
Display Name: Microsoft ACPI Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
```

modules|modscan|driverscan

查看系统内核驱动。隐藏的用modscan或者driverscan

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 modules
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                Base             Size File
---------- ------------------- ---------- ---------- ----
0x8823a308 ntoskrnl.exe        0x80800000   0x247000 \WINDOWS\system32\ntkrnlpa.exe
0x8823a2a0 hal.dll             0x80a47000    0x2c000 \WINDOWS\system32\hal.dll
0x8823a238 kdcom.dll           0xf7707000     0x8000 \WINDOWS\system32\KDCOM.DLL
0x8823a1c8 BOOTVID.dll         0xf770f000     0x8000 \WINDOWS\system32\BOOTVID.dll
0x8823a160 ACPI.sys            0xf7352000    0x34000 ACPI.sys
0x8823a0f0 WMILIB.SYS          0xf7487000     0x9000 \WINDOWS\system32\DRIVERS\WMILIB.SYS
0x8823a088 pci.sys             0xf733d000    0x15000 pci.sys
0x881f7008 isapnp.sys          0xf7497000     0xf000 isapnp.sys
0x881f7f98 compbatt.sys        0xf7897000     0x3000 compbatt.sys
0x881f7f30 BATTC.SYS           0xf7717000     0x5000 \WINDOWS\system32\DRIVERS\BATTC.SYS
0x881f7ec0 intelide.sys        0xf771f000     0x7000 intelide.sys
0x881f7e50 PCIIDEX.SYS         0xf74a7000     0xd000 \WINDOWS\system32\DRIVERS\PCIIDEX.SYS
0x881f7de0 MountMgr.sys        0xf74b7000    0x10000 MountMgr.sys
0x881f7d70 ftdisk.sys          0xf7317000    0x26000 ftdisk.sys
0x881f7d00 dmload.sys          0xf7727000     0x7000 dmload.sys
0x881f7c98 dmio.sys            0xf72ec000    0x2b000 dmio.sys
0x881f7c28 volsnap.sys         0xf72c3000    0x29000 volsnap.sys
```

screenshot

查看当前屏幕每个窗口中内容的轮廓线。

```
root@xibai-kali:~/桌面/study/2020/hxb/misc# volatility -f 1.vmem --profile=Win2003SP1x86 screenshot -D ./
Volatility Foundation Volatility Framework 2.6
Wrote ./session_0.SAWinSta.SADesktop.png
Wrote ./session_0.Service-0x0-3e7$.Default.png
Wrote ./session_0.Service-0x0-3e4$.Default.png
Wrote ./session_0.Service-0x0-3e5$.Default.png
Wrote ./session_0.WinSta0.Default.png
Wrote ./session_0.WinSta0.Disconnect.png
Wrote ./session_0.WinSta0.Winlogon.png
```

session_0.
SAWinSta.
SADesktop.png

session_0.
Service-0x0-3e4$.
Default.png

session_0.
Service-0x0-3e5$.
Default.png

session_0.
Service-0x0-3e7$.
Default.png

session_0.
WinSta0.Default.
png

session_0.
WinSta0.
Disconnect.png