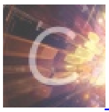
volatility安装、内存取证常见知识点及例题讲解(已进行2.1次更新)

原创

置顶 是Mumuzi 已于 2022-04-11 22:02:33 修改 3045 收藏 52
分类专栏： 笔记 ctf 文章标签： linux
于 2021-05-26 22:35:29 首次发布

本文链接：https://blog.csdn.net/qq_42880719/article/details/117304586
版权

笔记 同时被 2 个专栏收录
23 篇文章 6 订阅
订阅专栏


ctf
75 篇文章 28 订阅
订阅专栏

最近的CTF比赛有关内存取证、机器学习、流量分析的题越来越多，自己又没怎么下来学过，基本都混在简单基础的图片隐写上面，所以开坑整理内存取证的知识点，并选取两道例题来实操。之后也准备对机器学习开坑。

常见的内存镜像文件有raw、vmem、dmp、img等，这里就需要用到内存取证工具volatility(例题讲解使用版本为2.6)，当然如果看见有个叫DumpIt的进程，不用去理会，他就是生成内存文件的程序。

指令讲解及从零安装

从0开始安装volatility(2021/11/4)

因为我常用的kali坏掉了，每次只能靠快照存活那么几分钟，正好买的Samsung SSD T7到了，就重新在kali里面安装一下volatility吧。

基操部分

1.安装vmware tools
点击上方虚拟机—安装Vmware tools，桌面出现光盘的图标后双击打开，解压VMware tools到桌面，然后进入文件夹，输入命令

```
sudo ./vmware-install.pl
```

然后一路回车，有yes的就输入yes
直到最后出现enjoy表明安装成功
然后建议重启一下

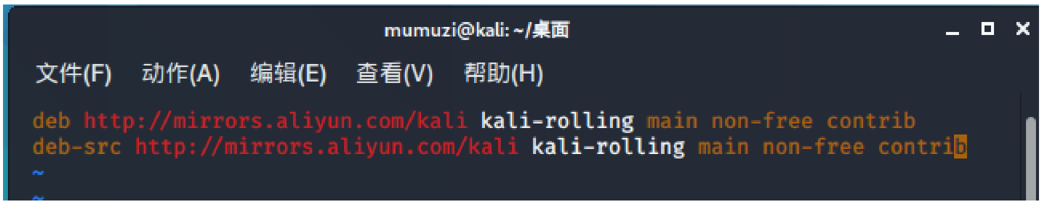
2.换源

输入以下指令

sudo vim /etc/apt/sources.list

将原有的源注释掉然后更换国内源

```
中科大源
deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
阿里云源
deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
清华大学源
deb http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free
deb-src https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free

三选一即可
```



```
deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
~
~
```

然后输入

```
sudo apt-get update
sudo apt-get upgrade
```

然后装个中文输入法吧

```
sudo apt-get install fcitx
sudo apt-get install fcitx-googlepinyin
重启即可
```

3.安装pip

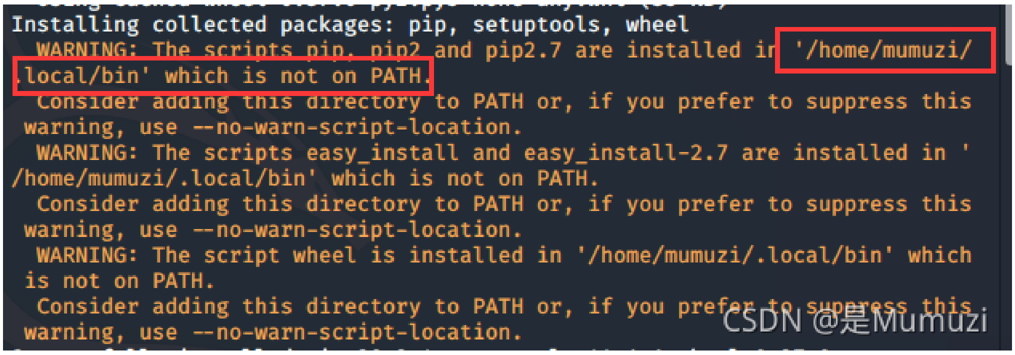
我使用的2020.2的kali，只安装了python2.7.18和python3.8.2，但没有pip。

请务必先安装python3再安装python2。如果先安装2再安装3会出现pip和pip3都指向的python3,也不用担心，再次执行python2 get-pip.py即可

对于python2.7:

```
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py

python get-pip.py
```

如果安装之后输入pip仍然出现找不到pip的情况
说明没有写入PATH，请根据他的提示输入以下命令，如图



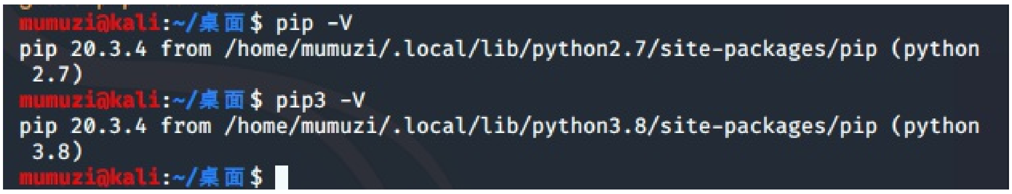
```
Installing collected packages: pip, setuptools, wheel
  WARNING: The scripts pip, pip2 and pip2.7 are installed in '/home/mumuzi/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
  WARNING: The scripts easy_install and easy_install-2.7 are installed in '/home/mumuzi/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
  WARNING: The script wheel is installed in '/home/mumuzi/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
```

请输入

```
echo 'export PATH=/home/mumuzi/.local/bin:$PATH' >>~/.bashrc
source ~/.bashrc
注：/home/mumuzi/.local/bin根据自己的WARNING提示来修改
```

对于python3:

```
我也是用的wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
然后python3 get-pip.py
(虽然我印象中python2和3的get-pip是独立的
```



```
mumuzi@kali:~/桌面$ pip -V
pip 20.3.4 from /home/mumuzi/.local/lib/python2.7/site-packages/pip (python 2.7)
mumuzi@kali:~/桌面$ pip3 -V
pip 20.3.4 from /home/mumuzi/.local/lib/python3.8/site-packages/pip (python 3.8)
mumuzi@kali:~/桌面$
```

安装volatility

建议害怕安装出问题之前，拍点快照
推荐方法(方便安装插件)
1.下载volatility
https://github.com/volatilityfoundation/volatility
或者git clone https://github.com/volatilityfoundation/volatility.git
进入文件夹后，输入

```
python setup.py install
```

2.然后运行，你会发现缺少很多库，于是安装这些库，一个个安装

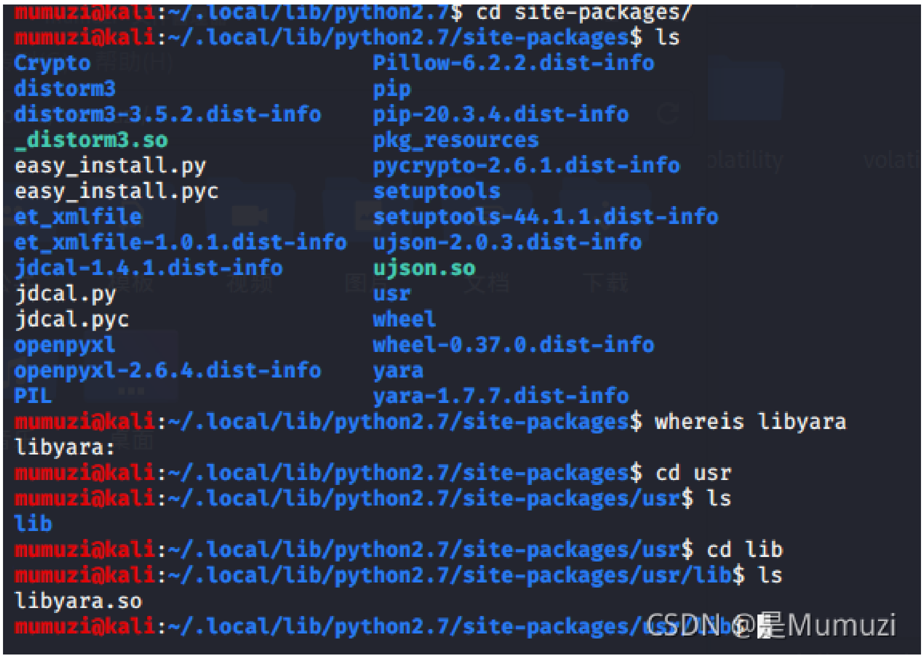
```
pip install yara
pip install pycrypto
如果在安装的时候报python.h的错，请执行下面一条
sudo apt-get install python2-dev
pip install pillow
pip install distorm3
pip install openpyxl
```

然后直接运行python vol.py即可

以下问题可能只是我个人出现的，如果你们也出现了可以看一看

虽然运行发现出现错误，发现是yara的原因，重新安装一次，发现在
Requirement already satisfied: yara in /home/mumuzi/.local/lib/python2.7/site-packages (1.7.7)
而报错原因是

```
Failed to import '/usr/lib/libyara.so'
PATH = /home/mumuzi/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games;/usr/lib
*** Failed to import volatility.plugins.linux.malfind (OSError: /usr/lib/libyara.so: cannot open shared object f
ile: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/mumuzi/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games;/usr/lib;/usr/lib
......
```

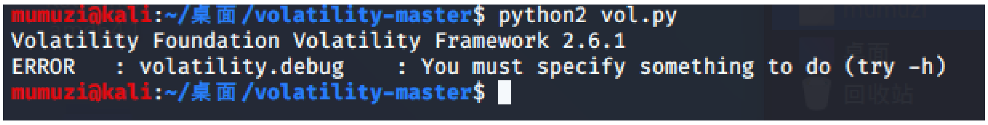


```
mumuzi@kali:~/.local/lib/python2.7$ cd site-packages/
mumuzi@kali:~/.local/lib/python2.7/site-packages$ ls
Crypto                          Pillow-6.2.2.dist-info
distorm3                        pip
distorm3-3.5.2.dist-info        pip-20.3.4.dist-info
_distorm3.so                    pkg_resources
easy_install.py                 pycrypto-2.6.1.dist-info
easy_install.pyc                setuptools
et_xmlfile                      setuptools-44.1.1.dist-info
et_xmlfile-1.0.1.dist-info      ujson-2.0.3.dist-info
jdcal-1.4.1.dist-info           ujson.so
jdcal.py                        usr
jdcal.pyc                       wheel
openpyxl                        wheel-0.37.0.dist-info
openpyxl-2.6.4.dist-info        yara
PIL                             yara-1.7.7.dist-info
mumuzi@kali:~/.local/lib/python2.7/site-packages$ whereis libyara
libyara:
mumuzi@kali:~/.local/lib/python2.7/site-packages$ cd usr
mumuzi@kali:~/.local/lib/python2.7/site-packages/usr$ ls
lib
mumuzi@kali:~/.local/lib/python2.7/site-packages/usr$ cd lib
mumuzi@kali:~/.local/lib/python2.7/site-packages/usr/lib$ ls
libyara.so
mumuzi@kali:~/.local/lib/python2.7/site-packages/usr/lib$
```

于是想到利用软连接来解决问题

```
ln -s /home/mumuzi/.local/lib/python2.7/site-packages/usr/lib/libyara.so /usr/lib/libyara.so
```

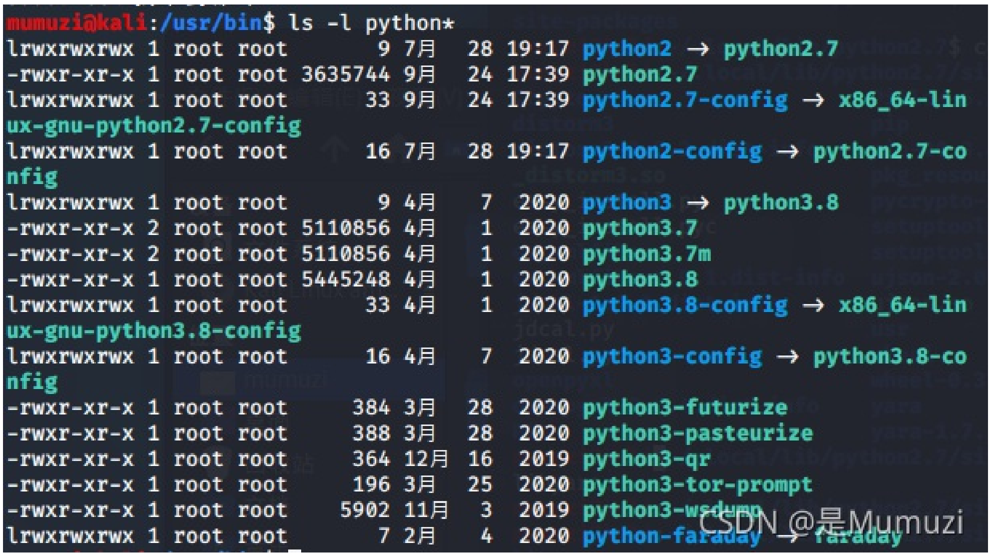
问题就被解决啦



```
mumuzi@kali:~/桌面/volatility-master$ python2 vol.py
Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug    : You must specify something to do (try -h)
mumuzi@kali:~/桌面/volatility-master$ 
```

还可能出现下面的问题

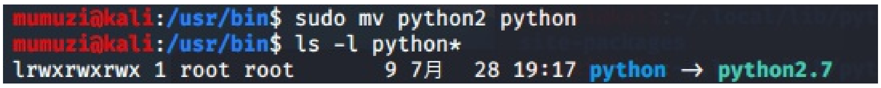
bash: /usr/local/bin/vol.py：/usr/bin/python：解释器错误: 没有那个文件或目录
然后在测试发现，将python改成python2才能使用。
于是进入bin目录，查看一下链接



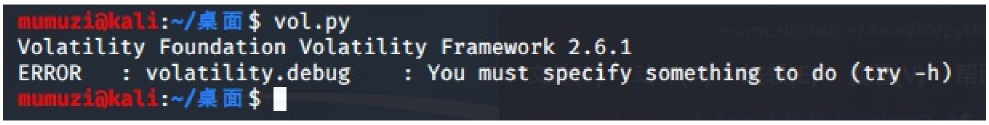
```
mumuzi@kali:/usr/bin$ ls -l python*
lrwxrwxrwx 1 root root       9 7月   28 19:17 python2 → python2.7
-rwxr-xr-x 1 root root 3635744 9月   24 17:39 python2.7
lrwxrwxrwx 1 root root      33 9月   24 17:39 python2.7-config → x86_64-lin
ux-gnu-python2.7-config
lrwxrwxrwx 1 root root      16 7月   28 19:17 python2-config → python2.7-co
nfig
lrwxrwxrwx 1 root root       9 4月    7  2020 python3 → python3.8
-rwxr-xr-x 2 root root 5110856 4月    1  2020 python3.7
-rwxr-xr-x 2 root root 5110856 4月    1  2020 python3.7m
-rwxr-xr-x 1 root root 5445248 4月    1  2020 python3.8
lrwxrwxrwx 1 root root      33 4月    1  2020 python3.8-config → x86_64-lin
ux-gnu-python3.8-config
lrwxrwxrwx 1 root root      16 4月    7  2020 python3-config → python3.8-co
nfig
-rwxr-xr-x 1 root root     384 3月   28  2020 python3-futurize
-rwxr-xr-x 1 root root     388 3月   28  2020 python3-pasteurize
-rwxr-xr-x 1 root root     364 12月  16  2019 python3-qr
-rwxr-xr-x 1 root root     196 3月   25  2020 python3-tor-prompt
-rwxr-xr-x 1 root root    5902 11月   3  2019 python3-wsdump
lrwxrwxrwx 1 root root       7 2月    4  2020 python-faraday → faraday
```

CSDN @是Mumuzi

发现bin下，是python2指向的python2.7，所以使用python的时候是找不到python2.7的，于是将bin下的python2改名python



```
mumuzi@kali:/usr/bin$ sudo mv python2 python
mumuzi@kali:/usr/bin$ ls -l python*
lrwxrwxrwx 1 root root       9 7月   28 19:17 python → python2.7
```



```
mumuzi@kali:~/桌面$ vol.py
Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug    : You must specify something to do (try -h)
mumuzi@kali:~/桌面$ 
```

插件的安装可以看后面

独立volatility安装方法

1.下载volatility
https://www.volatilityfoundation.org/26
选择下载Linux系统的，下载下来之后解压
然后把解压出来的文件夹改名为volatility，使用指令移动到/usr/local
顺便把那个可执行文件的文件名也改成volatility

```
sudo mv volatility/ /usr/local/
```

2.然后添加环境变量，通过修改profile

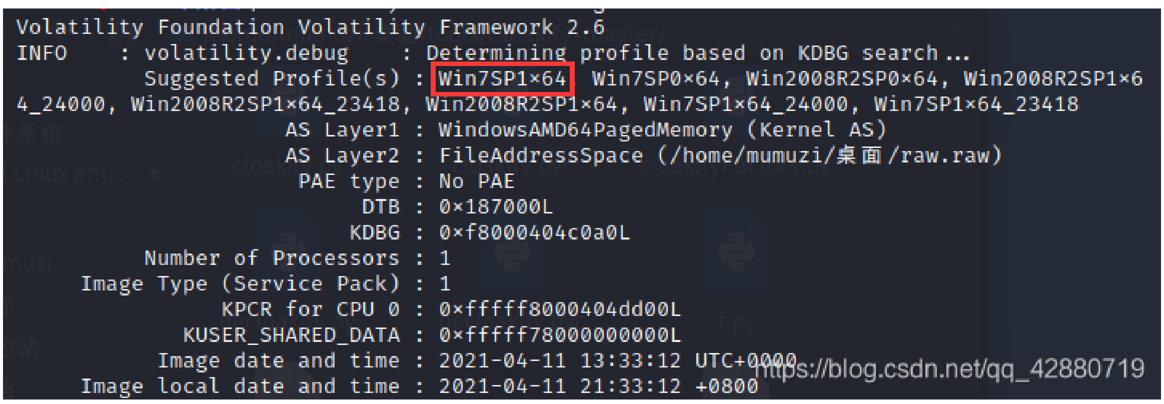
```
sudo vim /etc/profile
然后在最后，换行添加一句
export PATH=/usr/local/volatility:$PATH
重启即可
```

之后直接输入volatility，即可发现已经成功安装

imageinfo

分析获取内存镜像的基本信息

```
volatility -f raw.raw imageinfo
```



```
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x6
4_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/mumuzi/桌面/raw.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf8000404c0a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff8000404dd00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2021-04-11 13:33:12 UTC+0000
     Image local date and time : 2021-04-11 21:33:12 +0800
```

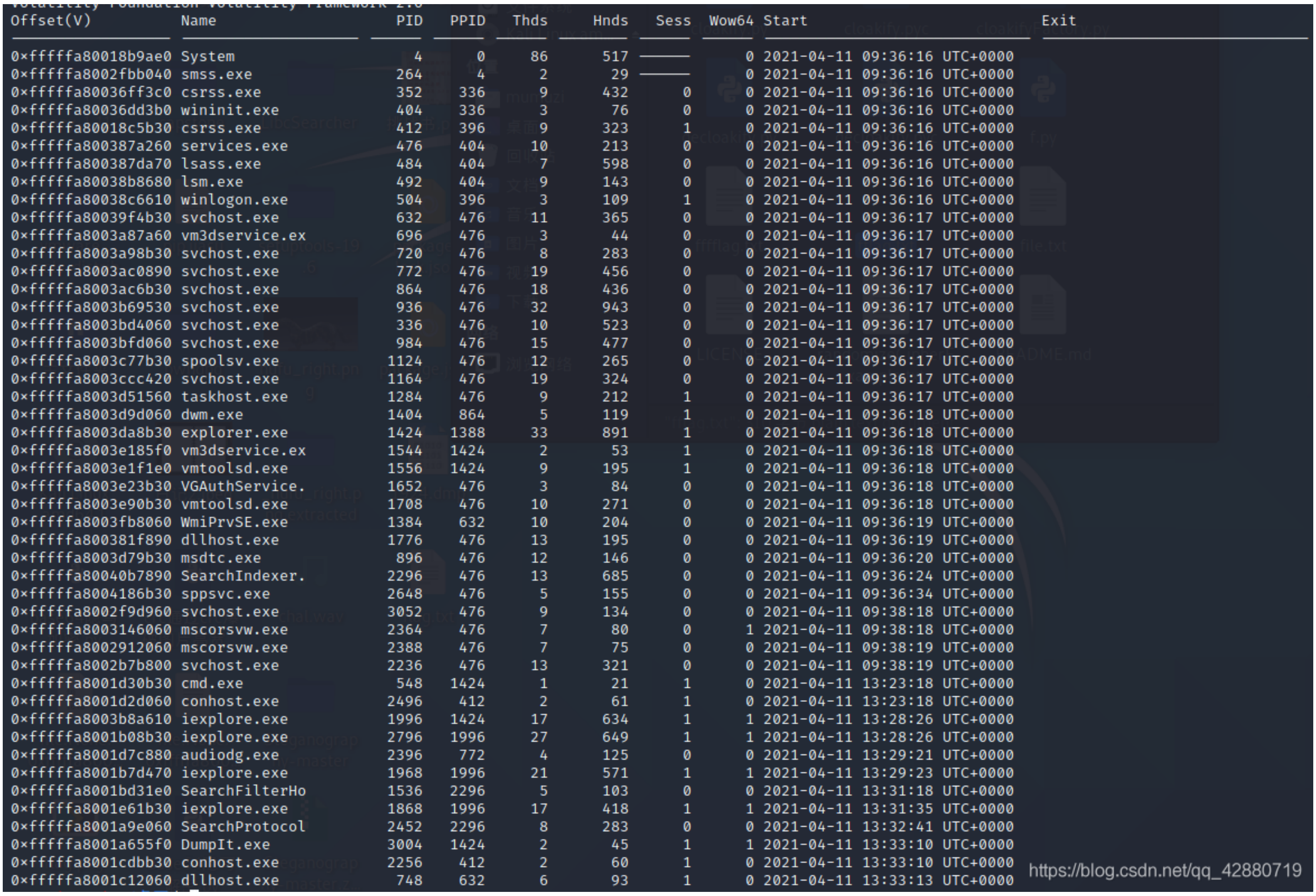
volatility 建议当做 Win7SP1x64 的镜像，后面的参数使用–profile(两根横杠)

pslist

知道镜像信息后，一般就会pslist
pslist：查看镜像中正在运行的进程

```
volatility -f raw.raw --profile=Win7SP1x64 pslist
```

当然，也可以用psxview，psxview可查看一些隐藏进程

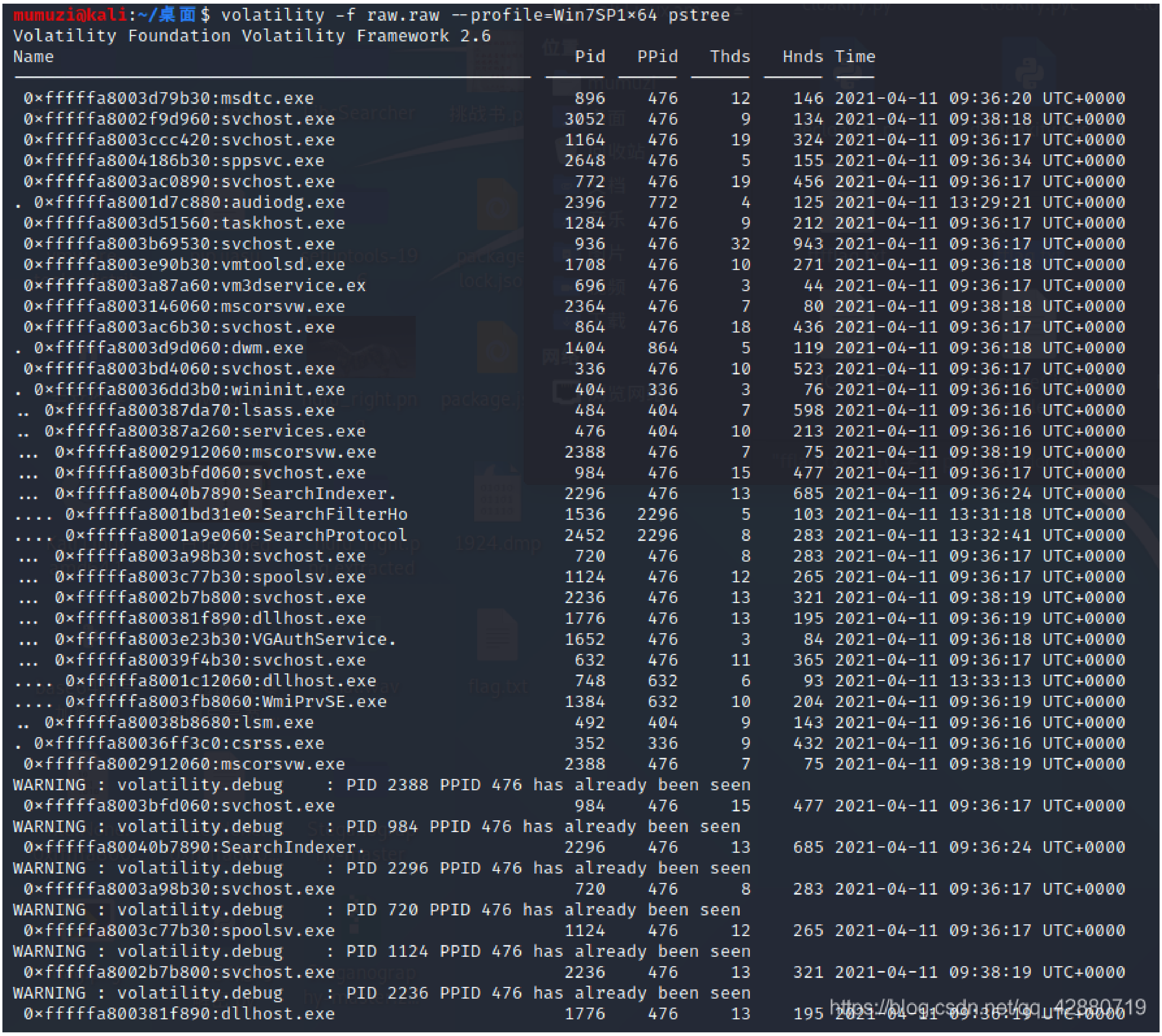


```
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa80018b9ae0 System                    4      0     86      517 ------      0 2021-04-11 09:36:16 UTC+0000
0xfffffa8002fbb040 smss.exe                264      4      2       29 ------      0 2021-04-11 09:36:16 UTC+0000
0xfffffa80036ff3c0 csrss.exe               352    336      9      432      0      0 2021-04-11 09:36:16 UTC+0000
0xfffffa80036dd3b0 wininit.exe             404    336      3       76      0      0 2021-04-11 09:36:16 UTC+0000
0xfffffa80018c5b30 csrss.exe               412    396      9      323      1      0 2021-04-11 09:36:16 UTC+0000
0xfffffa800387a260 services.exe            476    404     10      213      0      0 2021-04-11 09:36:16 UTC+0000
0xfffffa800387da70 lsass.exe               484    404      7      598      0      0 2021-04-11 09:36:16 UTC+0000
0xfffffa80038b8680 lsm.exe                 492    404      9      143      0      0 2021-04-11 09:36:16 UTC+0000
0xfffffa80038c6610 winlogon.exe            504    396      3      109      1      0 2021-04-11 09:36:16 UTC+0000
0xfffffa80039f4b30 svchost.exe             632    476     11      365      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003a87a60 vm3dservice.ex          696    476      3       44      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003a98b30 svchost.exe             720    476      8      283      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003ac0890 svchost.exe             772    476     19      456      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003ac6b30 svchost.exe             864    476     18      436      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003b69530 svchost.exe             936    476     32      943      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003bd4060 svchost.exe             336    476     10      523      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003bfd060 svchost.exe             984    476     15      477      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003c77b30 spoolsv.exe            1124    476     12      265      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003ccc420 svchost.exe            1164    476     19      324      0      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003d51560 taskhost.exe           1284    476      9      212      1      0 2021-04-11 09:36:17 UTC+0000
0xfffffa8003d9d060 dwm.exe                1404    864      5      119      1      0 2021-04-11 09:36:18 UTC+0000
0xfffffa8003da8b30 explorer.exe           1424   1388     33      891      1      0 2021-04-11 09:36:18 UTC+0000
0xfffffa8003e185f0 vm3dservice.ex         1544   1424      2       53      1      0 2021-04-11 09:36:18 UTC+0000
0xfffffa8003e1f1e0 vmtoolsd.exe           1556   1424      9      195      1      0 2021-04-11 09:36:18 UTC+0000
0xfffffa8003e23b30 VGAuthService.         1652    476      3       84      0      0 2021-04-11 09:36:18 UTC+0000
0xfffffa8003e90b30 vmtoolsd.exe           1708    476     10      271      0      0 2021-04-11 09:36:18 UTC+0000
0xfffffa8003fb8060 WmiPrvSE.exe           1384    632     10      204      0      0 2021-04-11 09:36:19 UTC+0000
0xfffffa800381f890 dllhost.exe            1776    476     13      195      0      0 2021-04-11 09:36:19 UTC+0000
0xfffffa8003d79b30 msdtc.exe               896    476     12      146      0      0 2021-04-11 09:36:20 UTC+0000
0xfffffa80040b7890 SearchIndexer.         2296    476     13      685      0      0 2021-04-11 09:36:24 UTC+0000
0xfffffa8004186b30 sppsvc.exe             2648    476      5      155      0      0 2021-04-11 09:36:34 UTC+0000
0xfffffa8002f9d960 svchost.exe            3052    476      9      134      0      0 2021-04-11 09:38:18 UTC+0000
0xfffffa8003146060 mscorsvw.exe           2364    476      7       80      0      1 2021-04-11 09:38:18 UTC+0000
0xfffffa8002912060 mscorsvw.exe           2388    476      7       75      0      0 2021-04-11 09:38:19 UTC+0000
0xfffffa8002b7b800 svchost.exe            2236    476     13      321      0      0 2021-04-11 09:38:19 UTC+0000
0xfffffa8001d30b30 cmd.exe                 548   1424      1       21      1      0 2021-04-11 13:23:18 UTC+0000
0xfffffa8001d2d060 conhost.exe            2496    412      2       61      1      0 2021-04-11 13:23:18 UTC+0000
0xfffffa8003b8a610 iexplore.exe           1996   1424     17      634      1      1 2021-04-11 13:28:26 UTC+0000
0xfffffa8001b08b30 iexplore.exe           2796   1996     27      649      1      1 2021-04-11 13:28:26 UTC+0000
0xfffffa8001d7c880 audiodg.exe            2396    772      4      125      0      0 2021-04-11 13:29:21 UTC+0000
0xfffffa8001b7d470 iexplore.exe           1968   1996     21      571      1      1 2021-04-11 13:29:23 UTC+0000
0xfffffa8001bd31e0 SearchFilterHo         1536   2296      5      103      0      0 2021-04-11 13:31:18 UTC+0000
0xfffffa8001e61b30 iexplore.exe           1868   1996     17      418      1      1 2021-04-11 13:31:35 UTC+0000
0xfffffa8001a9e060 SearchProtocol         2452   2296      8      283      0      0 2021-04-11 13:32:41 UTC+0000
0xfffffa8001a655f0 DumpIt.exe             3004   1424      2       45      1      1 2021-04-11 13:33:10 UTC+0000
0xfffffa8001cdbb30 conhost.exe            2256    412      2       60      1      0 2021-04-11 13:33:10 UTC+0000
0xfffffa8001c12060 dllhost.exe             748    632      6       93      1      0 2021-04-11 13:33:13 UTC+0000
```

pstree

以树的形式来列出正在进行的进程，当然pstree也不会显示出隐藏或未链接的进程

> volatility -f raw.raw --profile=Win7SP1x64 pslist



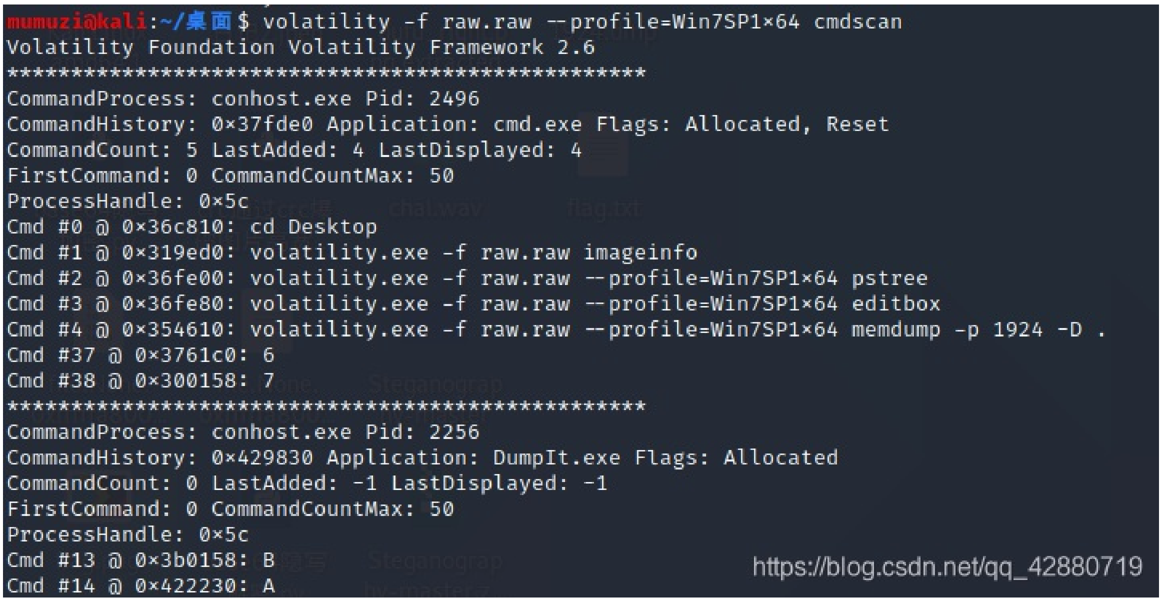
```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8003d79b30:msdtc.exe                         896    476     12    146 2021-04-11 09:36:20 UTC+0000
 0xfffffa8002f9d960:svchost.exe                      3052    476      9    134 2021-04-11 09:38:18 UTC+0000
 0xfffffa8003ccc420:svchost.exe                      1164    476     19    324 2021-04-11 09:36:17 UTC+0000
 0xfffffa8004186b30:sppsvc.exe                       2648    476      5    155 2021-04-11 09:36:34 UTC+0000
 0xfffffa8003ac0890:svchost.exe                       772    476     19    456 2021-04-11 09:36:17 UTC+0000
. 0xfffffa8001d7c880:audiodg.exe                     2396    772      4    125 2021-04-11 13:29:21 UTC+0000
 0xfffffa8003d51560:taskhost.exe                     1284    476      9    212 2021-04-11 09:36:17 UTC+0000
 0xfffffa8003b69530:svchost.exe                       936    476     32    943 2021-04-11 09:36:17 UTC+0000
 0xfffffa8003e90b30:vmtoolsd.exe                     1708    476     10    271 2021-04-11 09:36:18 UTC+0000
 0xfffffa8003a87a60:vm3dservice.ex                    696    476      3     44 2021-04-11 09:36:17 UTC+0000
 0xfffffa8003146060:mscorsvw.exe                     2364    476      7     80 2021-04-11 09:38:18 UTC+0000
 0xfffffa8003ac6b30:svchost.exe                       864    476     18    436 2021-04-11 09:36:17 UTC+0000
. 0xfffffa8003d9d060:dwm.exe                         1404    864      5    119 2021-04-11 09:36:18 UTC+0000
 0xfffffa8003bd4060:svchost.exe                       336    476     10    523 2021-04-11 09:36:17 UTC+0000
. 0xfffffa80036dd3b0:wininit.exe                      404    336      3     76 2021-04-11 09:36:16 UTC+0000
.. 0xfffffa800387da70:lsass.exe                       484    404      7    598 2021-04-11 09:36:16 UTC+0000
.. 0xfffffa800387a260:services.exe                    476    404     10    213 2021-04-11 09:36:16 UTC+0000
... 0xfffffa8002912060:mscorsvw.exe                  2388    476      7     75 2021-04-11 09:38:19 UTC+0000
... 0xfffffa8003bfd060:svchost.exe                    984    476     15    477 2021-04-11 09:36:17 UTC+0000
... 0xfffffa80040b7890:SearchIndexer.                2296    476     13    685 2021-04-11 09:36:24 UTC+0000
.... 0xfffffa8001bd31e0:SearchFilterHo               1536   2296      5    103 2021-04-11 13:31:18 UTC+0000
.... 0xfffffa8001a9e060:SearchProtocol               2452   2296      8    283 2021-04-11 13:32:41 UTC+0000
... 0xfffffa8003a98b30:svchost.exe                    720    476      8    283 2021-04-11 09:36:17 UTC+0000
... 0xfffffa8003c77b30:spoolsv.exe                   1124    476     12    265 2021-04-11 09:36:17 UTC+0000
... 0xfffffa8002b7b800:svchost.exe                   2236    476     13    321 2021-04-11 09:38:19 UTC+0000
... 0xfffffa800381f890:dllhost.exe                   1776    476     13    195 2021-04-11 09:36:19 UTC+0000
... 0xfffffa8003e23b30:VGAuthService.                1652    476      3     84 2021-04-11 09:36:18 UTC+0000
... 0xfffffa80039f4b30:svchost.exe                    632    476     11    365 2021-04-11 09:36:17 UTC+0000
.... 0xfffffa8001c12060:dllhost.exe                   748    632      6     93 2021-04-11 13:33:13 UTC+0000
.... 0xfffffa8003fb8060:WmiPrvSE.exe                 1384    632     10    204 2021-04-11 09:36:19 UTC+0000
.. 0xfffffa80038b8680:lsm.exe                         492    404      9    143 2021-04-11 09:36:16 UTC+0000
. 0xfffffa80036ff3c0:csrss.exe                        352    336      9    432 2021-04-11 09:36:16 UTC+0000
 0xfffffa8002912060:mscorsvw.exe                     2388    476      7     75 2021-04-11 09:38:19 UTC+0000
WARNING : volatility.debug    : PID 2388 PPID 476 has already been seen
 0xfffffa8003bfd060:svchost.exe                       984    476     15    477 2021-04-11 09:36:17 UTC+0000
WARNING : volatility.debug    : PID 984 PPID 476 has already been seen
 0xfffffa80040b7890:SearchIndexer.                   2296    476     13    685 2021-04-11 09:36:24 UTC+0000
WARNING : volatility.debug    : PID 2296 PPID 476 has already been seen
 0xfffffa8003a98b30:svchost.exe                       720    476      8    283 2021-04-11 09:36:17 UTC+0000
WARNING : volatility.debug    : PID 720 PPID 476 has already been seen
 0xfffffa8003c77b30:spoolsv.exe                      1124    476     12    265 2021-04-11 09:36:17 UTC+0000
WARNING : volatility.debug    : PID 1124 PPID 476 has already been seen
 0xfffffa8002b7b800:svchost.exe                      2236    476     13    321 2021-04-11 09:38:19 UTC+0000
WARNING : volatility.debug    : PID 2236 PPID 476 has already been seen
 0xfffffa800381f890:dllhost.exe                      1776    476     13    195 2021-04-11 09:36:19 UTC+0000
```

还有psscan指令，它是以pool tag来扫描，很少用；还有psdispscan、dlllist、dlldump、handles、getsids，这里不做描述

cmdscan

cmdscan是搜索XP / 2003 / Vista / 2008和conhost.exe上搜索csrss.exe的内存，对于win7是搜索cmd.exe。是搜索命令行的输入历史记录

```
volatility -f raw.raw --profile=Win7SP1x64 cmdscan
```

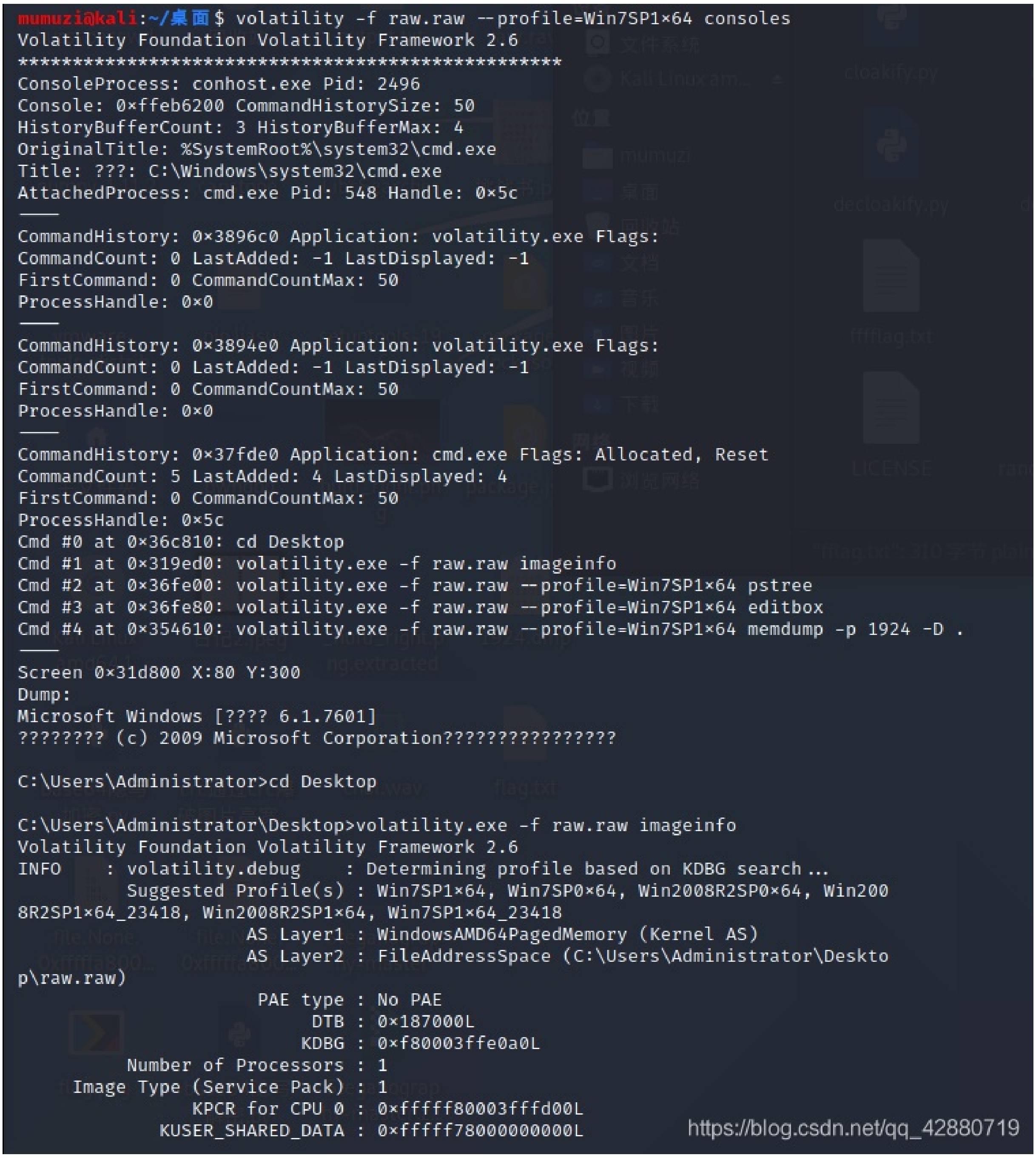


```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1×64 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 2496
CommandHistory: 0×37fde0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×5c
Cmd #0 @ 0×36c810: cd Desktop
Cmd #1 @ 0×319ed0: volatility.exe -f raw.raw imageinfo
Cmd #2 @ 0×36fe00: volatility.exe -f raw.raw --profile=Win7SP1×64 pstree
Cmd #3 @ 0×36fe80: volatility.exe -f raw.raw --profile=Win7SP1×64 editbox
Cmd #4 @ 0×354610: volatility.exe -f raw.raw --profile=Win7SP1×64 memdump -p 1924 -D .
Cmd #37 @ 0×3761c0: 6
Cmd #38 @ 0×300158: 7
**************************************************
CommandProcess: conhost.exe Pid: 2256
CommandHistory: 0×429830 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×5c
Cmd #13 @ 0×3b0158: B
Cmd #14 @ 0×422230: A
```

consoles

相似与cmdscan，但是他扫描的不是COMMAND_HISTORY，而是CONSOLE_INFORMATION，而且还有个显著的优点是cmdscan只能查看到输入的指令，而consoles能查看到输入的指令以及缓冲区的输出(即键入和键出)

```
volatility -f raw.raw --profile=Win7SP1x64 consoles
```

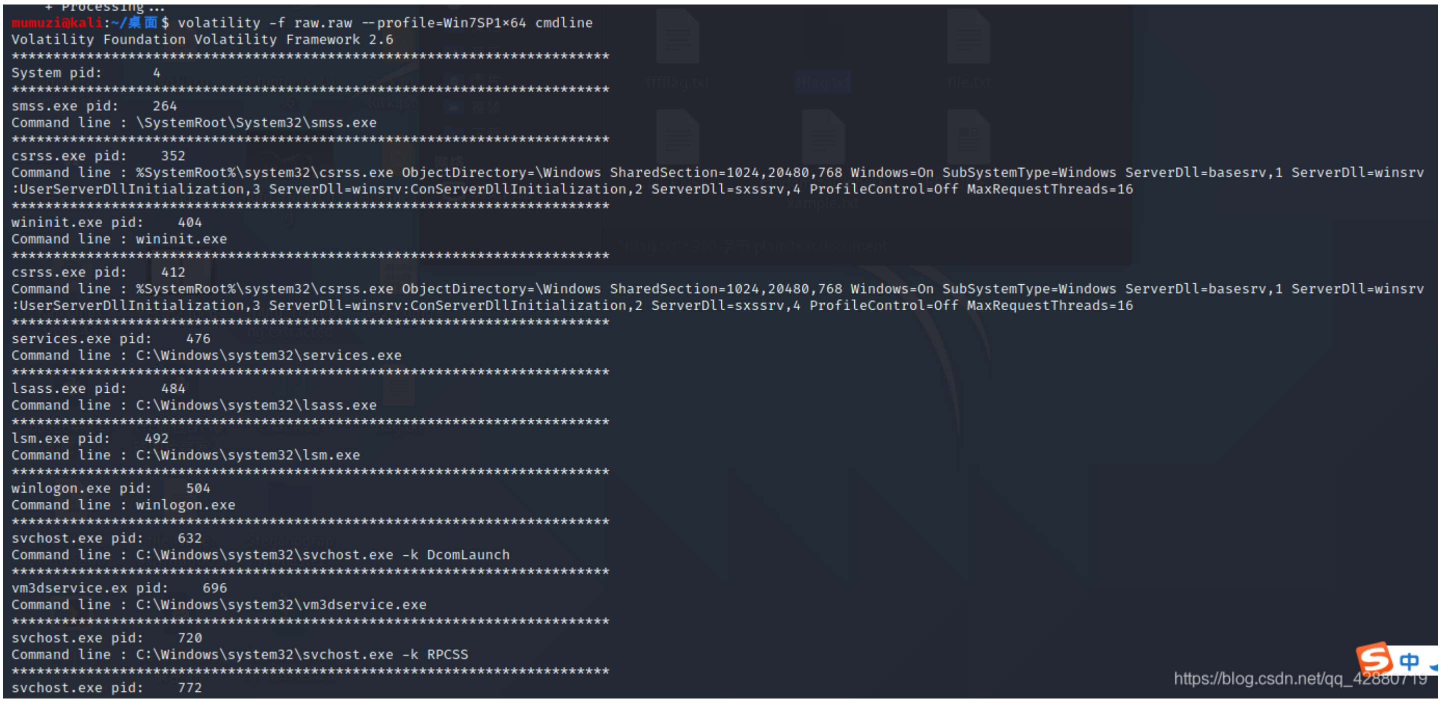


```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 2496
Console: 0xffeb6200 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: ???: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 548 Handle: 0x5c
----
CommandHistory: 0x3896c0 Application: volatility.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x3894e0 Application: volatility.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x37fde0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 at 0x36c810: cd Desktop
Cmd #1 at 0x319ed0: volatility.exe -f raw.raw imageinfo
Cmd #2 at 0x36fe00: volatility.exe -f raw.raw --profile=Win7SP1x64 pstree
Cmd #3 at 0x36fe80: volatility.exe -f raw.raw --profile=Win7SP1x64 editbox
Cmd #4 at 0x354610: volatility.exe -f raw.raw --profile=Win7SP1x64 memdump -p 1924 -D .
----
Screen 0x31d800 X:80 Y:300
Dump:
Microsoft Windows [???? 6.1.7601]
???????? (c) 2009 Microsoft Corporation????????????????

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>volatility.exe -f raw.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search ...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\Administrator\Deskto
p\raw.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80003ffe0a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80003fffd00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
```

cmdline

此指令将会列出所有命令行下运行的程序

> volatility -f raw.raw --profile=Win7SP1x64 cmdline



```
    + Processing ...
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1×64 cmdline
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
************************************************************************
smss.exe pid:    264
Command line : \SystemRoot\System32\smss.exe
************************************************************************
csrss.exe pid:    352
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv
:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
************************************************************************
wininit.exe pid:    404
Command line : wininit.exe
************************************************************************
csrss.exe pid:    412
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv
:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
************************************************************************
services.exe pid:    476
Command line : C:\Windows\system32\services.exe
************************************************************************
lsass.exe pid:    484
Command line : C:\Windows\system32\lsass.exe
************************************************************************
lsm.exe pid:    492
Command line : C:\Windows\system32\lsm.exe
************************************************************************
winlogon.exe pid:    504
Command line : winlogon.exe
************************************************************************
svchost.exe pid:    632
Command line : C:\Windows\system32\svchost.exe -k DcomLaunch
************************************************************************
vm3dservice.ex pid:    696
Command line : C:\Windows\system32\vm3dservice.exe
************************************************************************
svchost.exe pid:    720
Command line : C:\Windows\system32\svchost.exe -k RPCSS
************************************************************************
svchost.exe pid:    772
```

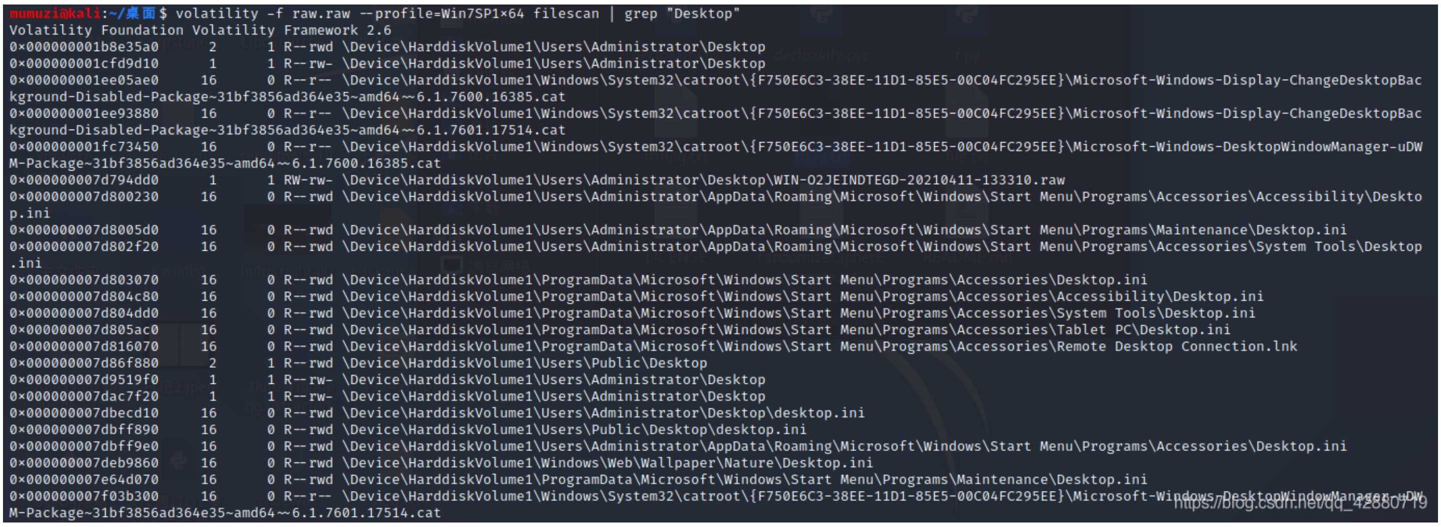
除此之外，简单讲一些不常见的指令

> privs:显示进程权限
> envars：显示进程环境变量
> verinfo：显示PE文件中嵌入的版本信息
> enumfunc：列出进程，dll和内核驱动程序导入和导出

filescan

扫描文件指令,一般呢会根据正在进行的进程来定向扫描，也常常会扫描桌面文件。

> volatility -f raw.raw --profile=Win7SP1x64 filescan
> volatility -f raw.raw --profile=Win7SP1x64 filescan | grep “flag”
> volatility -f raw.raw --profile=Win7SP1x64 filescan | grep “Desktop”（有的可能是中文把Desktop改成桌面即可）
> volatility -f raw.raw --profile=Win7SP1x64 filescan | grep -E “png”（查找png后缀文件）

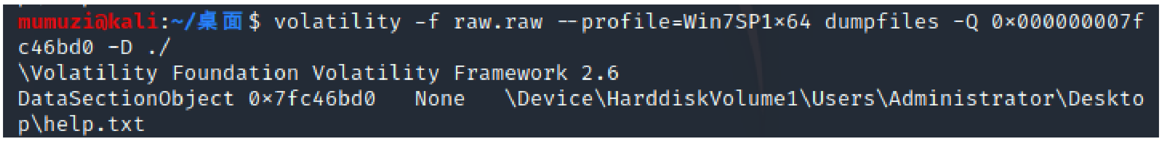


```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1×64 filescan | grep "Desktop"
Volatility Foundation Volatility Framework 2.6
0×000000001b8e35a0      2      1 R--rwd \Device\HarddiskVolume1\Users\Administrator\Desktop
0×000000001cfd9d10      1      1 R--rw- \Device\HarddiskVolume1\Users\Administrator\Desktop
0×000000001ee05ae0     16      0 R--r-- \Device\HarddiskVolume1\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Display-ChangeDesktopBac
kground-Disabled-Package~31bf3856ad364e35~amd64~~6.1.7600.16385.cat
0×000000001ee93880     16      0 R--r-- \Device\HarddiskVolume1\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Display-ChangeDesktopBac
kground-Disabled-Package~31bf3856ad364e35~amd64~~6.1.7601.17514.cat
0×000000001fc73450     16      0 R--r-- \Device\HarddiskVolume1\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-DesktopWindowManager-uDW
M-Package~31bf3856ad364e35~amd64~~6.1.7600.16385.cat
0×000000007d794dd0      1      1 RW-rw- \Device\HarddiskVolume1\Users\Administrator\Desktop\WIN-O2JEINDTEGD-20210411-133310.raw
0×000000007d800230     16      0 R--rwd \Device\HarddiskVolume1\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Deskto
p.ini
0×000000007d8005d0     16      0 R--rwd \Device\HarddiskVolume1\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini
0×000000007d802f20     16      0 R--rwd \Device\HarddiskVolume1\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop
.ini
0×000000007d803070     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
0×000000007d804c80     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini
0×000000007d804dd0     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop.ini
0×000000007d805ac0     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Tablet PC\Desktop.ini
0×000000007d816070     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk
0×000000007d86f880      2      1 R--rwd \Device\HarddiskVolume1\Users\Public\Desktop
0×000000007d9519f0      1      1 R--rw- \Device\HarddiskVolume1\Users\Administrator\Desktop
0×000000007dac7f20      1      1 R--rw- \Device\HarddiskVolume1\Users\Administrator\Desktop
0×000000007dbecd10     16      0 R--rwd \Device\HarddiskVolume1\Users\Administrator\Desktop\desktop.ini
0×000000007dbff890     16      0 R--rwd \Device\HarddiskVolume1\Users\Public\Desktop\desktop.ini
0×000000007dbff9e0     16      0 R--rwd \Device\HarddiskVolume1\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
0×000000007deb9860     16      0 R--rwd \Device\HarddiskVolume1\Windows\Web\Wallpaper\Nature\Desktop.ini
0×000000007e64d070     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini
0×000000007f03b300     16      0 R--r-- \Device\HarddiskVolume1\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-DesktopWindowManager-uDW
M-Package~31bf3856ad364e35~amd64~~6.1.7601.17514.cat
```

dumpfiles

dump出指定PID的文件，一般只要是做内存题都会用到的指令。

> volatility -f raw.raw --profile=Win7SP1x64 dumpfiles -Q [PID] -D ./
> 将PID的文件保存在当前目录



```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1×64 dumpfiles -Q 0×000000007f
c46bd0 -D ./
\Volatility Foundation Volatility Framework 2.6
DataSectionObject 0×7fc46bd0   None   \Device\HarddiskVolume1\Users\Administrator\Deskto
p\help.txt
```

procdump

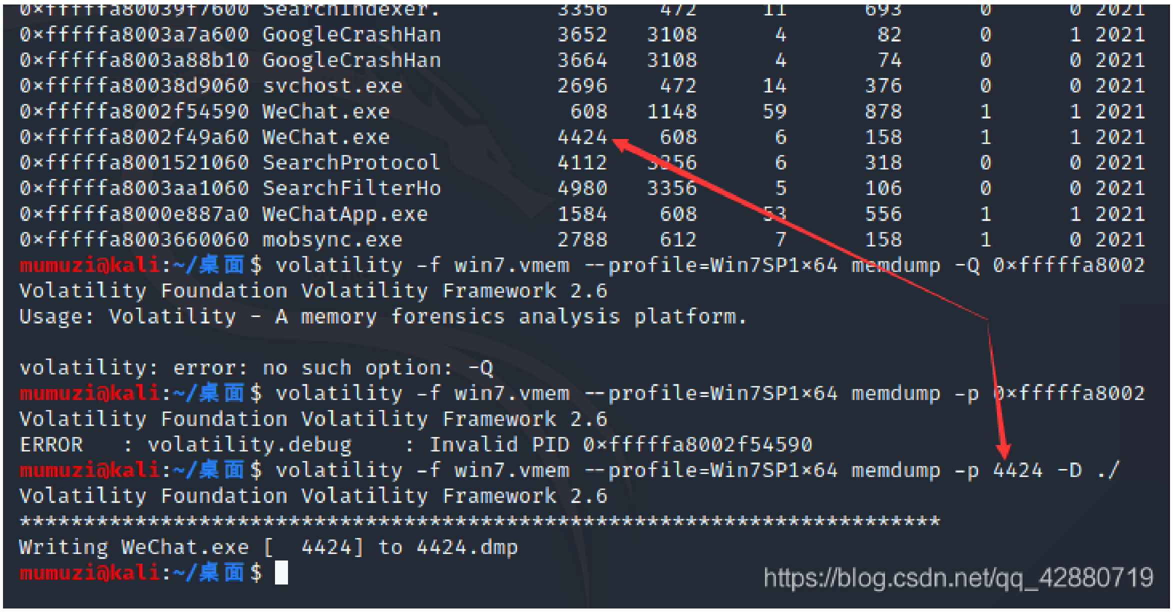
转储进程的可执行文件，后跟PID

> volatility -f mal.raw --profile=Win7SP1x64 procdump -p 3468 -D ./

memdump

可以将内存中的某个进程保存出来

> volatility -f win7.vmem --profile=Win7SP1x64 memdump -p [PID] -D ./



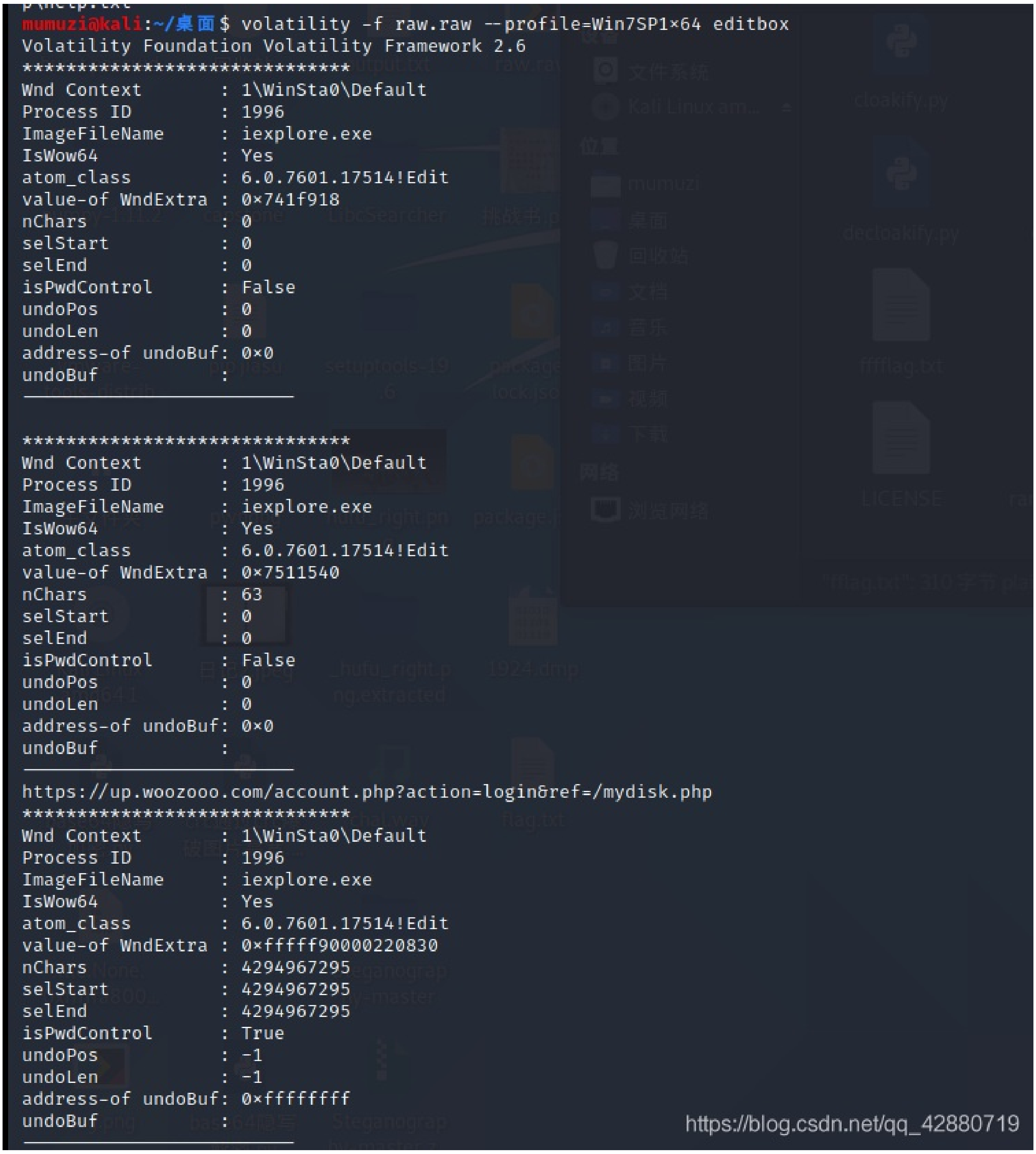
```
0×fffffa80039f7600 SearchIndexer.         3356   472    11      693      0      0 2021
0×fffffa8003a7a600 GoogleCrashHan         3652  3108     4       82      0      1 2021
0×fffffa8003a88b10 GoogleCrashHan         3664  3108     4       74      0      0 2021
0×fffffa80038d9060 svchost.exe            2696   472    14      376      0      0 2021
0×fffffa8002f54590 WeChat.exe              608  1148    59      878      1      1 2021
0×fffffa8002f49a60 WeChat.exe             4424   608     6      158      1      1 2021
0×fffffa8001521060 SearchProtocol         4112  3356     6      318      0      0 2021
0×fffffa8003aa1060 SearchFilterHo         4980  3356     5      106      0      0 2021
0×fffffa8000e887a0 WeChatApp.exe          1584   608    53      556      1      1 2021
0×fffffa8003660060 mobsync.exe            2788   612     7      158      1      0 2021
mumuzi@kali:~/桌面$ volatility -f win7.vmem --profile=Win7SP1×64 memdump -Q 0×fffffa8002
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

volatility: error: no such option: -Q
mumuzi@kali:~/桌面$ volatility -f win7.vmem --profile=Win7SP1×64 memdump -p 0×fffffa8002
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Invalid PID 0×fffffa8002f54590
mumuzi@kali:~/桌面$ volatility -f win7.vmem --profile=Win7SP1×64 memdump -p 4424 -D ./
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing WeChat.exe [  4424] to 4424.dmp
mumuzi@kali:~/桌面$
```

https://blog.csdn.net/qq_42880719

editbox/notepad

显示出有关编辑控件的信息
在XP中，正在运行的notepad程序，使用notepad指令就可以看到notepad.exe的内容，而在win7中，将不支持notepad，只能使用editbox，这里举例editbox

```
volatility -f raw.raw --profile=Win7SP1x64 editbox
```

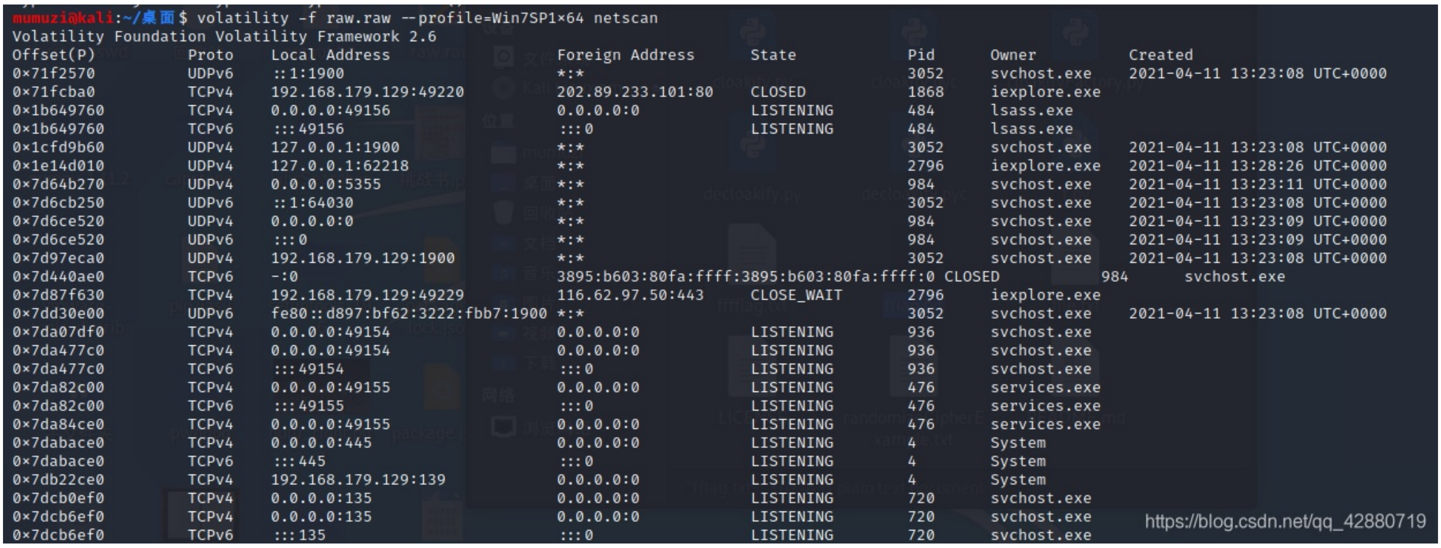


```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 editbox
Volatility Foundation Volatility Framework 2.6
******************************
Wnd Context       : 1\WinSta0\Default
Process ID        : 1996
ImageFileName     : iexplore.exe
IsWow64           : Yes
atom_class        : 6.0.7601.17514!Edit
value-of WndExtra : 0x741f918
nChars            : 0
selStart          : 0
selEnd            : 0
isPwdControl      : False
undoPos           : 0
undoLen           : 0
address-of undoBuf: 0x0
undoBuf           :
_________________________

******************************
Wnd Context       : 1\WinSta0\Default
Process ID        : 1996
ImageFileName     : iexplore.exe
IsWow64           : Yes
atom_class        : 6.0.7601.17514!Edit
value-of WndExtra : 0x7511540
nChars            : 63
selStart          : 0
selEnd            : 0
isPwdControl      : False
undoPos           : 0
undoLen           : 0
address-of undoBuf: 0x0
undoBuf           :
_________________________
https://up.woozooo.com/account.php?action=login&ref=/mydisk.php
******************************
Wnd Context       : 1\WinSta0\Default
Process ID        : 1996
ImageFileName     : iexplore.exe
IsWow64           : Yes
atom_class        : 6.0.7601.17514!Edit
value-of WndExtra : 0xfffff90000220830
nChars            : 4294967295
selStart          : 4294967295
selEnd            : 4294967295
isPwdControl      : True
undoPos           : -1
undoLen           : -1
address-of undoBuf: 0xffffffff
undoBuf           :
_________________________
```

netscan

查看网络连接的连接情况

```
volatility -f raw.raw --profile=Win7SP1x64 netscan
```

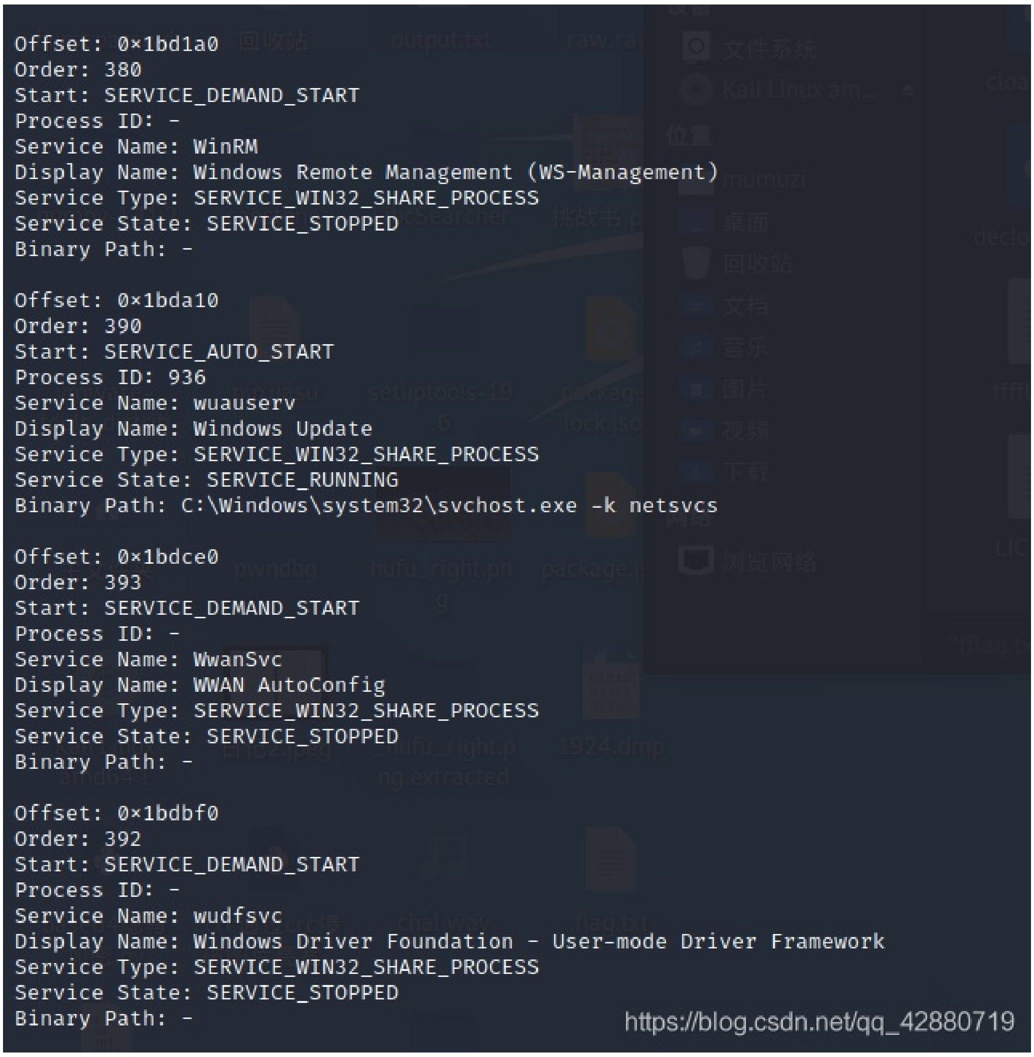


```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1×64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0×71f2570          UDPv6    ::1:1900                       *:*                                   3052     svchost.exe    2021-04-11 13:23:08 UTC+0000
0×71fcba0          TCPv4    192.168.179.129:49220          202.89.233.101:80    CLOSED           1868     iexplore.exe
0×1b649760         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        484      lsass.exe
0×1b649760         TCPv6    :::49156                       :::0                 LISTENING        484      lsass.exe
0×1cfd9b60         UDPv4    127.0.0.1:1900                 *:*                                   3052     svchost.exe    2021-04-11 13:23:08 UTC+0000
0×1e14d010         UDPv4    127.0.0.1:62218                *:*                                   2796     iexplore.exe   2021-04-11 13:28:26 UTC+0000
0×7d64b270         UDPv4    0.0.0.0:5355                   *:*                                   984      svchost.exe    2021-04-11 13:23:11 UTC+0000
0×7d6cb250         UDPv6    ::1:64030                      *:*                                   3052     svchost.exe    2021-04-11 13:23:08 UTC+0000
0×7d6ce520         UDPv4    0.0.0.0:0                      *:*                                   984      svchost.exe    2021-04-11 13:23:09 UTC+0000
0×7d6ce520         UDPv6    :::0                           *:*                                   984      svchost.exe    2021-04-11 13:23:09 UTC+0000
0×7d97eca0         UDPv4    192.168.179.129:1900           *:*                                   3052     svchost.exe    2021-04-11 13:23:08 UTC+0000
0×7d440ae0         TCPv6    -:0                            3895:b603:80fa:ffff:3895:b603:80fa:ffff:0 CLOSED          984      svchost.exe
0×7d87f630         TCPv4    192.168.179.129:49229          116.62.97.50:443     CLOSE_WAIT       2796     iexplore.exe
0×7dd30e00         UDPv6    fe80::d897:bf62:3222:fbb7:1900 *:*                                   3052     svchost.exe    2021-04-11 13:23:08 UTC+0000
0×7da07df0         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        936      svchost.exe
0×7da477c0         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        936      svchost.exe
0×7da477c0         TCPv6    :::49154                       :::0                 LISTENING        936      svchost.exe
0×7da82c00         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        476      services.exe
0×7da82c00         TCPv6    :::49155                       :::0                 LISTENING        476      services.exe
0×7da84ce0         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        476      services.exe
0×7dabace0         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0×7dabace0         TCPv6    :::445                         :::0                 LISTENING        4        System
0×7db22ce0         TCPv4    192.168.179.129:139            0.0.0.0:0            LISTENING        4        System
0×7dcb0ef0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        720      svchost.exe
0×7dcb6ef0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        720      svchost.exe
0×7dcb6ef0         TCPv6    :::135                         :::0                 LISTENING        720      svchost.exe
```

svcscan

扫描windows服务列表

> volatility -f raw.raw --profile=Win7SP1x64 svcscan

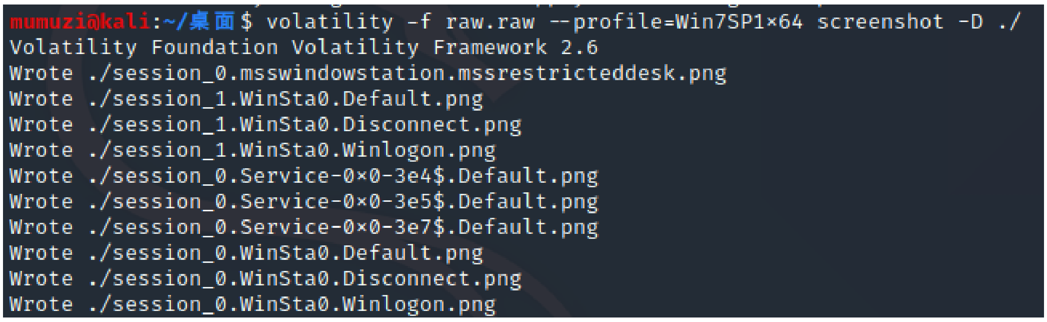


```
Offset: 0×1bd1a0
Order: 380
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: WinRM
Display Name: Windows Remote Management (WS-Management)
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0×1bda10
Order: 390
Start: SERVICE_AUTO_START
Process ID: 936
Service Name: wuauserv
Display Name: Windows Update
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\Windows\system32\svchost.exe -k netsvcs

Offset: 0×1bdce0
Order: 393
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: WwanSvc
Display Name: WWAN AutoConfig
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0×1bdbf0
Order: 392
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: wudfsvc
Display Name: Windows Driver Foundation - User-mode Driver Framework
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -
```

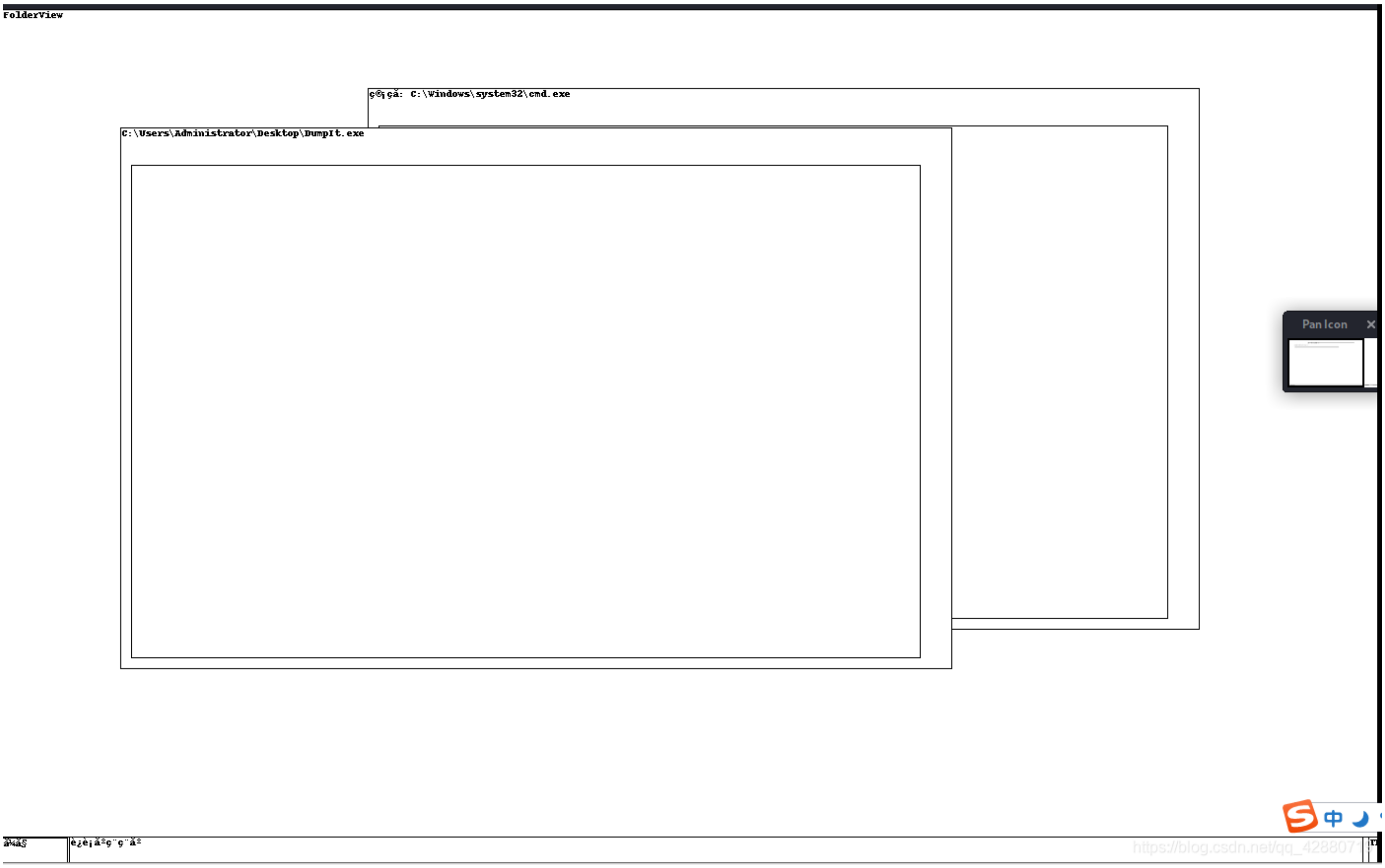
screenshot

显示GDI样式的截屏

```
volatility -f raw.raw --profile=Win7SP1x64 screenshot -D ./
```



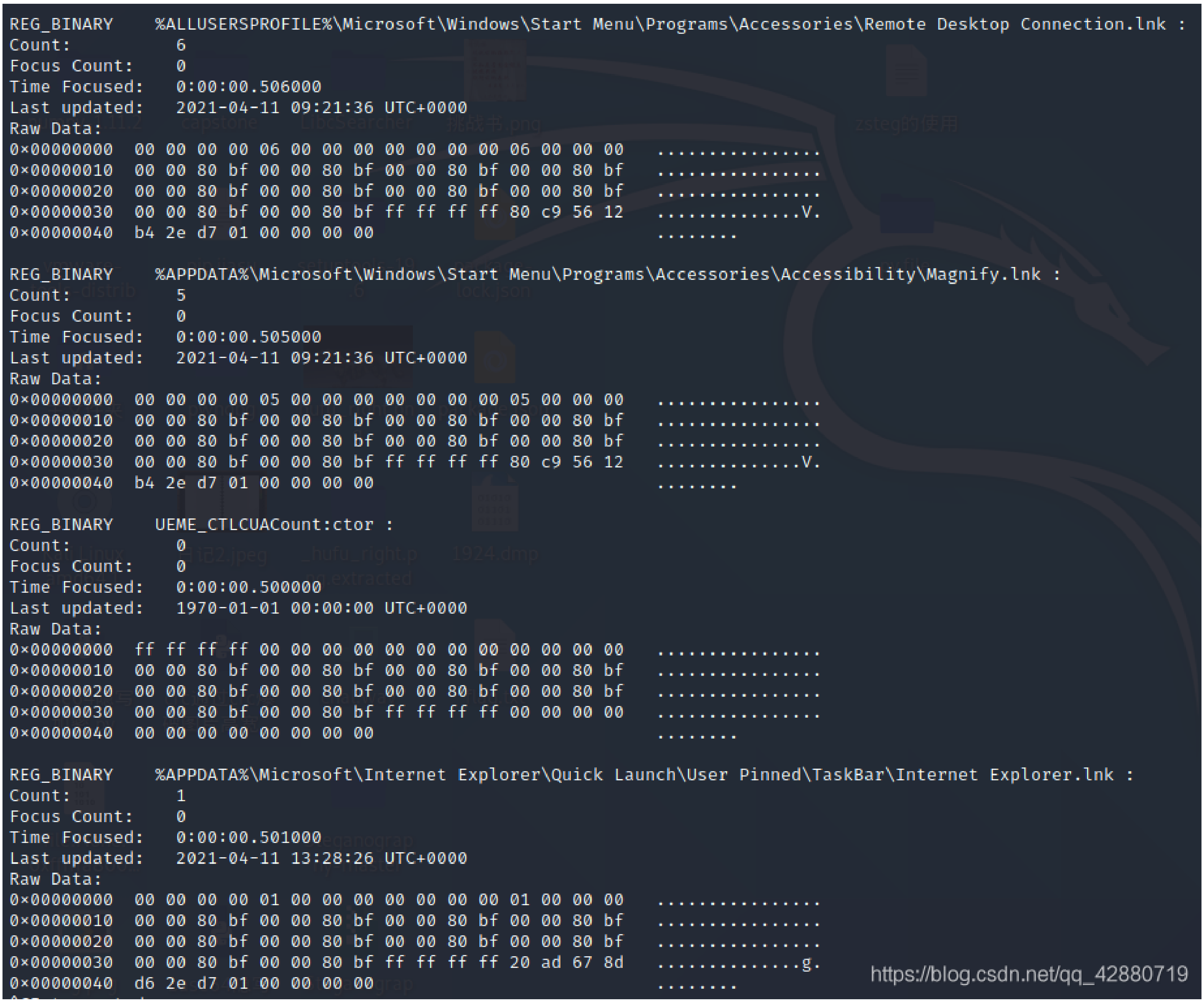
```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 screenshot -D ./
Volatility Foundation Volatility Framework 2.6
Wrote ./session_0.msswindowstation.mssrestricteddesk.png
Wrote ./session_1.WinSta0.Default.png
Wrote ./session_1.WinSta0.Disconnect.png
Wrote ./session_1.WinSta0.Winlogon.png
Wrote ./session_0.Service-0x0-3e4$.Default.png
Wrote ./session_0.Service-0x0-3e5$.Default.png
Wrote ./session_0.Service-0x0-3e7$.Default.png
Wrote ./session_0.WinSta0.Default.png
Wrote ./session_0.WinSta0.Disconnect.png
Wrote ./session_0.WinSta0.Winlogon.png
```


FolderView
ç®¡çã: C:\Windows\system32\cmd.exe
C:\Users\Administrator\Desktop\DumpIt.exe
Pan Icon
中

userassist

查看运行的进程和次数

```
volatility -f raw.raw --profile=Win7SP1x64 userassist
```

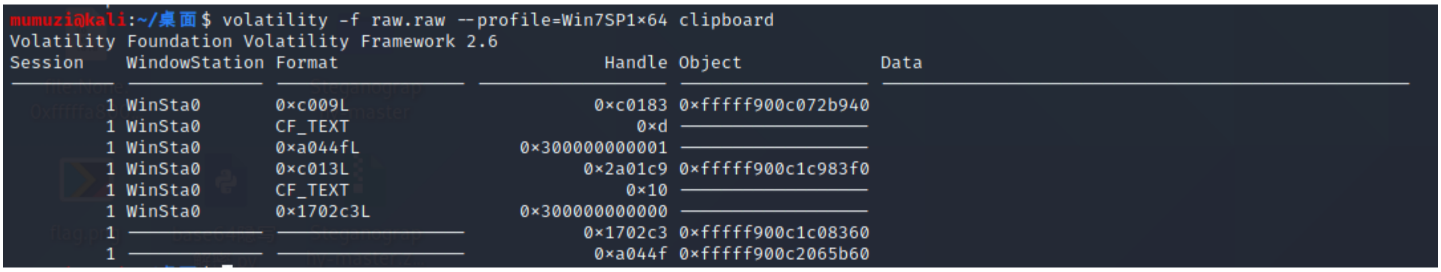


```
REG_BINARY    %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk :
Count:          6
Focus Count:    0
Time Focused:   0:00:00.506000
Last updated:   2021-04-11 09:21:36 UTC+0000
Raw Data:
0x00000000  00 00 00 00 06 00 00 00 00 00 00 00 06 00 00 00   ................
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 80 c9 56 12   ..............V.
0x00000040  b4 2e d7 01 00 00 00 00                           ........

REG_BINARY    %APPDATA%\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Magnify.lnk :
Count:          5
Focus Count:    0
Time Focused:   0:00:00.505000
Last updated:   2021-04-11 09:21:36 UTC+0000
Raw Data:
0x00000000  00 00 00 00 05 00 00 00 00 00 00 00 05 00 00 00   ................
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 80 c9 56 12   ..............V.
0x00000040  b4 2e d7 01 00 00 00 00                           ........

REG_BINARY    UEME_CTLCUACount:ctor :
Count:          0
Focus Count:    0
Time Focused:   0:00:00.500000
Last updated:   1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000  ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 00 00 00 00   ................
0x00000040  00 00 00 00 00 00 00 00                           ........

REG_BINARY    %APPDATA%\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk :
Count:          1
Focus Count:    0
Time Focused:   0:00:00.501000
Last updated:   2021-04-11 13:28:26 UTC+0000
Raw Data:
0x00000000  00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00   ................
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 20 ad 67 8d   ..............g.
0x00000040  d6 2e d7 01 00 00 00 00                           ........
```

clipboard

剪贴板数据，加参数-v可以导出

> volatility -f raw.raw --profile=Win7SP1x64 clipboard
> volatility -f raw.raw --profile=Win7SP1x64 clipboard -v >clip.txt

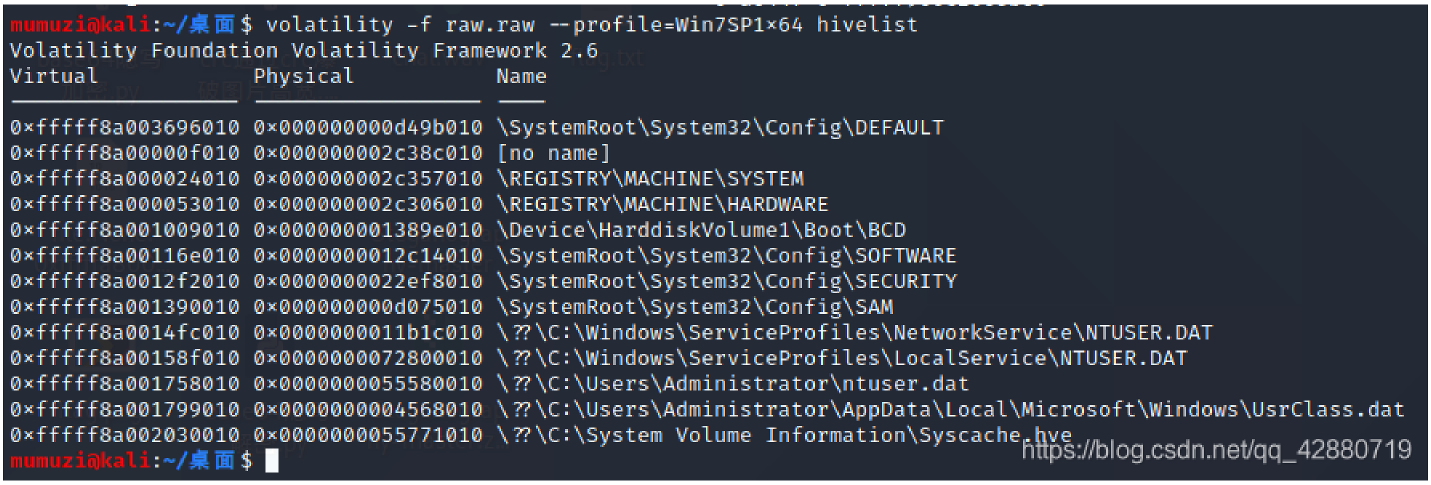


```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6
Session    WindowStation Format                         Handle Object             Data
---------- ------------- ------------------ ------------------ ------------------ --------------------------------------------------
         1 WinSta0       0xc009L                       0xc0183 0xfffff900c072b940
         1 WinSta0       CF_TEXT                           0xd ------------------
         1 WinSta0       0xa044fL               0x300000000001 ------------------
         1 WinSta0       0xc013L                       0x2a01c9 0xfffff900c1c983f0
         1 WinSta0       CF_TEXT                          0x10 ------------------
         1 WinSta0       0x1702c3L              0x300000000000 ------------------
         1 ------------- ------------------            0x1702c3 0xfffff900c1c08360
         1 ------------- ------------------            0xa044f 0xfffff900c2065b60
```

hivelist

列出注册表

```
volatility -f raw.raw --profile=Win7SP1x64 hivelist
dumpregistry -o virtual地址可以导出，如volatility -f raw.raw --profile=Win7SP1x64 dumpregistry -o 0xfffff8a003696010
```



```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a003696010 0x000000000d49b010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a00000f010 0x000000002c38c010 [no name]
0xfffff8a000024010 0x000000002c357010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000053010 0x000000002c306010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a001009010 0x000000001389e010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a00116e010 0x0000000012c14010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a0012f2010 0x0000000022ef8010 \SystemRoot\System32\Config\SECURITY
0xfffff8a001390010 0x000000000d075010 \SystemRoot\System32\Config\SAM
0xfffff8a0014fc010 0x0000000011b1c010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a00158f010 0x0000000072800010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001758010 0x0000000055580010 \??\C:\Users\Administrator\ntuser.dat
0xfffff8a001799010 0x0000000004568010 \??\C:\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002030010 0x0000000055771010 \??\C:\System Volume Information\Syscache.hve
mumuzi@kali:~/桌面$
```

malfind

malfind 查找隐藏或注入的代码/ DLL

```
volatility -f raw.raw --profile=Win7SP1x64 malfind
```

可以查找出存在异常的进程

handles

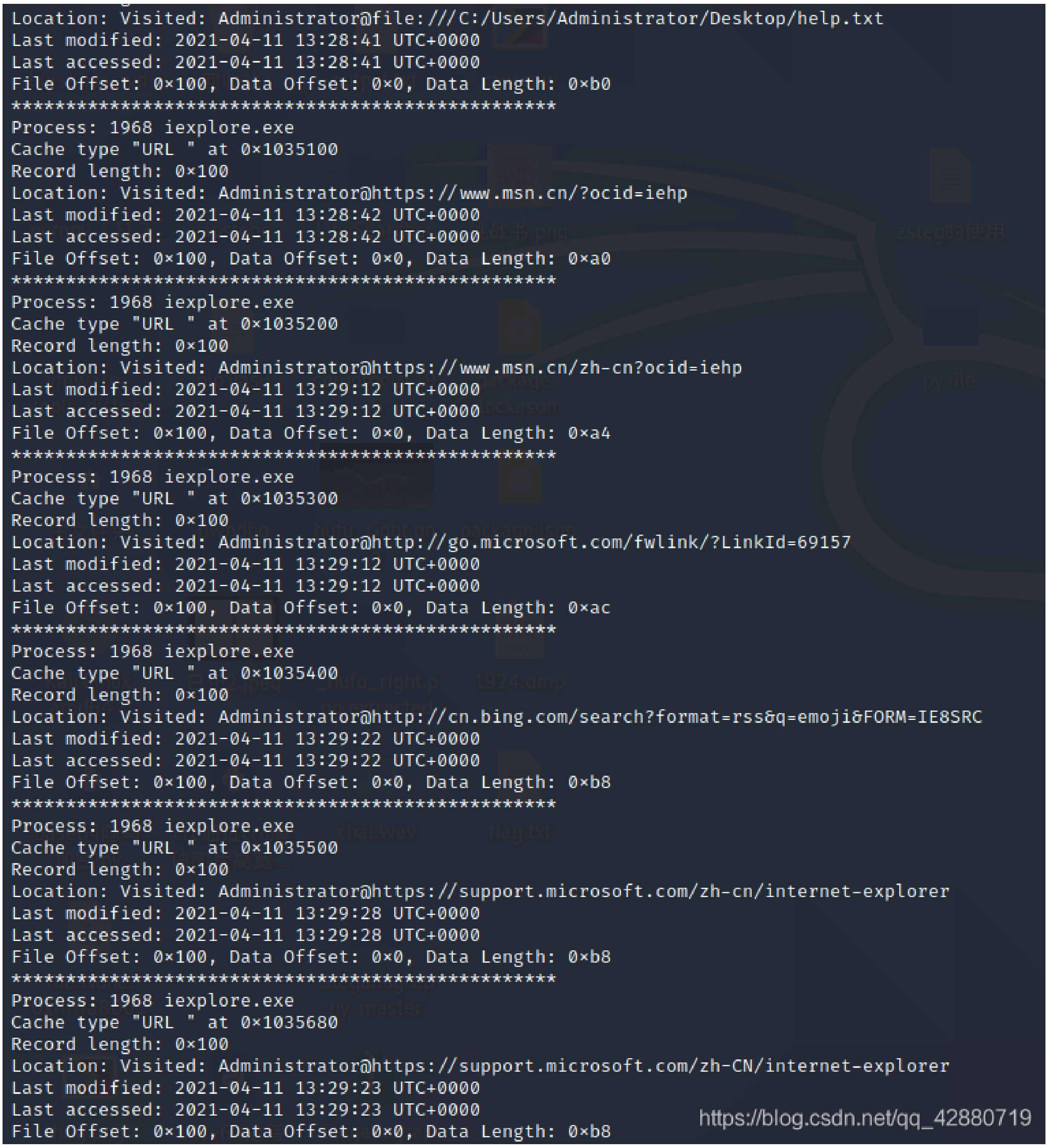
查看文件句柄，如上面malfind发现PID为2233

```
volatility -f raw.raw --profile=Win7SP1x64 handles -p 620 -t file
```

iehistory

获取浏览器的浏览历史，这个指令也经常用到。

```
volatility -f raw.raw --profile=Win7SP1x64 iehistory
```

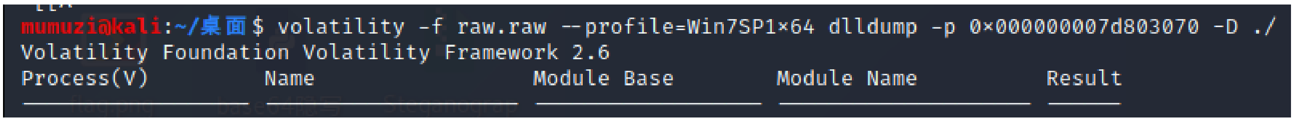


```
Location: Visited: Administrator@file:///C:/Users/Administrator/Desktop/help.txt
Last modified: 2021-04-11 13:28:41 UTC+0000
Last accessed: 2021-04-11 13:28:41 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xb0
**************************************************
Process: 1968 iexplore.exe
Cache type "URL " at 0x1035100
Record length: 0x100
Location: Visited: Administrator@https://www.msn.cn/?ocid=iehp
Last modified: 2021-04-11 13:28:42 UTC+0000
Last accessed: 2021-04-11 13:28:42 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa0
**************************************************
Process: 1968 iexplore.exe
Cache type "URL " at 0x1035200
Record length: 0x100
Location: Visited: Administrator@https://www.msn.cn/zh-cn?ocid=iehp
Last modified: 2021-04-11 13:29:12 UTC+0000
Last accessed: 2021-04-11 13:29:12 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 1968 iexplore.exe
Cache type "URL " at 0x1035300
Record length: 0x100
Location: Visited: Administrator@http://go.microsoft.com/fwlink/?LinkId=69157
Last modified: 2021-04-11 13:29:12 UTC+0000
Last accessed: 2021-04-11 13:29:12 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xac
**************************************************
Process: 1968 iexplore.exe
Cache type "URL " at 0x1035400
Record length: 0x100
Location: Visited: Administrator@http://cn.bing.com/search?format=rss&q=emoji&FORM=IE8SRC
Last modified: 2021-04-11 13:29:22 UTC+0000
Last accessed: 2021-04-11 13:29:22 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xb8
**************************************************
Process: 1968 iexplore.exe
Cache type "URL " at 0x1035500
Record length: 0x100
Location: Visited: Administrator@https://support.microsoft.com/zh-cn/internet-explorer
Last modified: 2021-04-11 13:29:28 UTC+0000
Last accessed: 2021-04-11 13:29:28 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xb8
**************************************************
Process: 1968 iexplore.exe
Cache type "URL " at 0x1035680
Record length: 0x100
Location: Visited: Administrator@https://support.microsoft.com/zh-CN/internet-explorer
Last modified: 2021-04-11 13:29:23 UTC+0000
Last accessed: 2021-04-11 13:29:23 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xb8
```

dlldump

将指定PID的进程的所有DLL导出

```
volatility -f raw.raw --profile=Win7SP1x64 dlldump -p [PID] -D ./
```



```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 dlldump -p 0x000000007d803070 -D ./
Volatility Foundation Volatility Framework 2.6
Process(V)         Name                 Module Base         Module Name          Result
------------------ -------------------- ------------------ -------------------- ------
```

使用插件找到密码

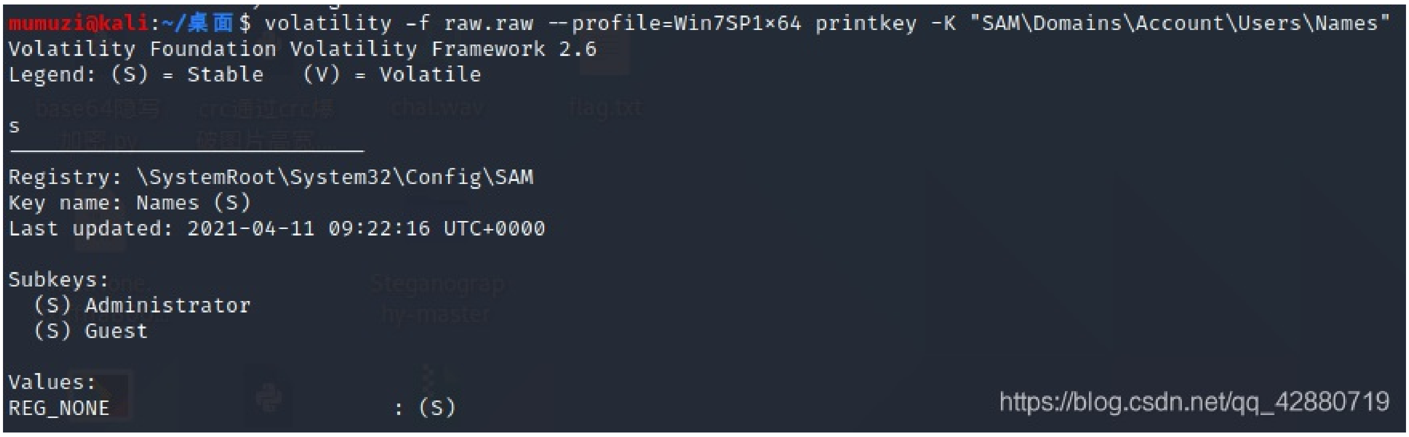
不像printkey一样，用hash来获取密码，这里可以直接使用mimikatz.py插件来获取内存中的密码，无论多复杂都彳亍。当然也可以用最新版的passware kit来获取密码，原理同样是从内存中直接获取密码。
插件地址
https://github.com/ruokeqx/tool-for-CTF/tree/master/volatility_plugins
若不会装插件，可看这篇文章
命令也很简单，直接在后面加个mimikatz即可，如：

> volatility -f raw.raw --profile=Win7SP1x64 mimikatz

printkey

常常是用来列举用户及密码、查看获取最后登陆系统的用户。

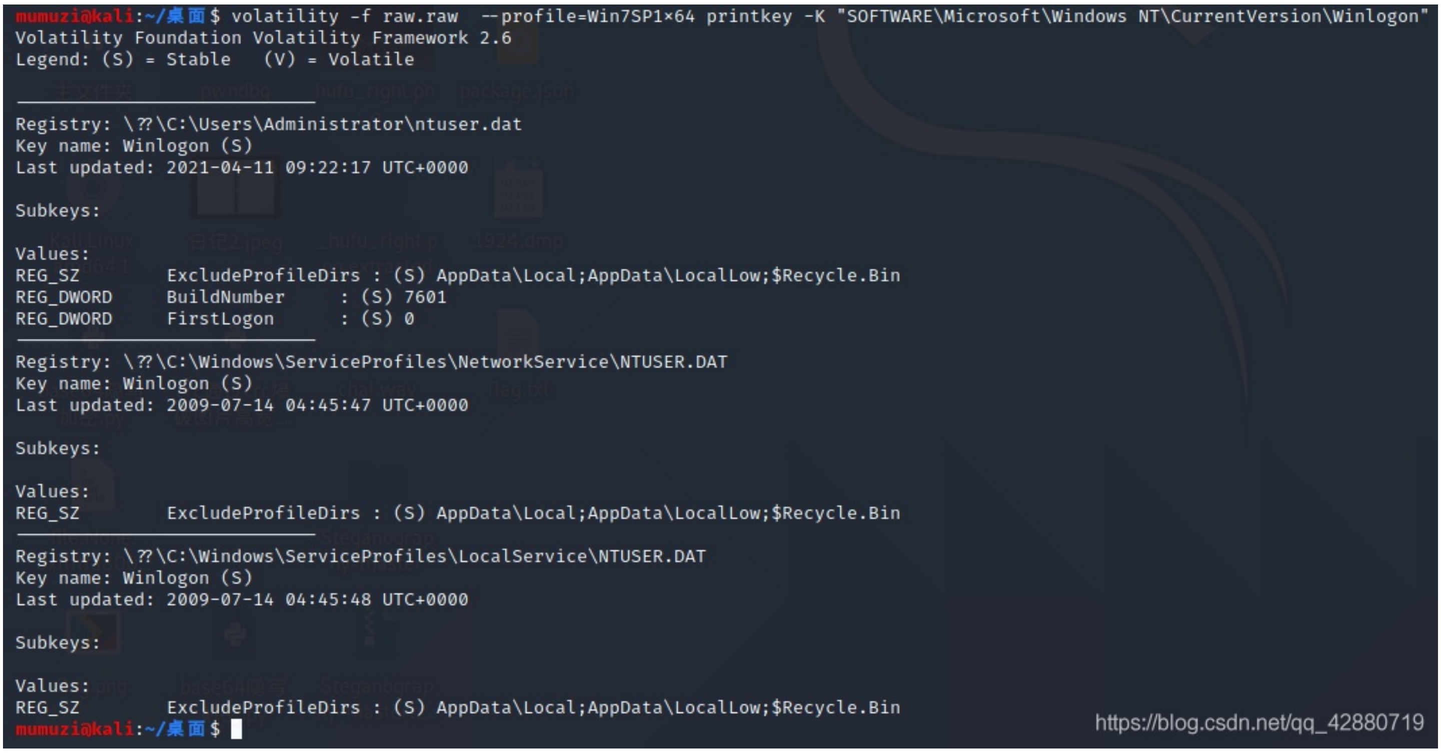
> 获取用户：volatility -f raw.raw --profile=Win7SP1x64 printkey -K “SAM\Domains\Account\Users\Names”



```
mumuzi@kali:~/桌面$ volatility -f raw.raw --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

s
____________________________
Registry: \SystemRoot\System32\Config\SAM
Key name: Names (S)
Last updated: 2021-04-11 09:22:16 UTC+0000

Subkeys:
  (S) Administrator
  (S) Guest

Values:
REG_NONE                      : (S)
```

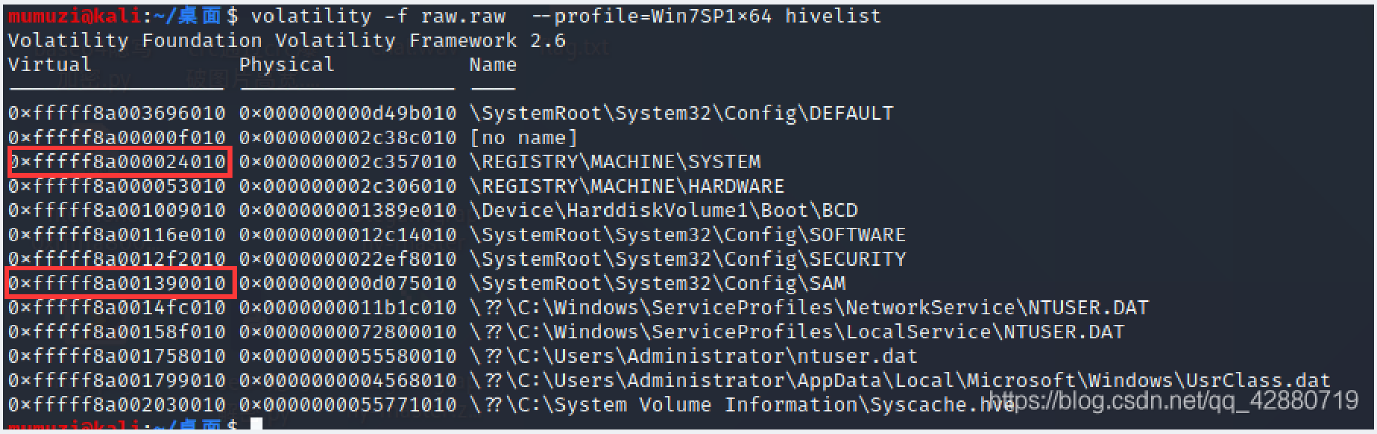
https://blog.csdn.net/qq_42880719

> 获取最后登陆系统的用户：volatility -f raw.raw --profile=Win7SP1x64 printkey -K “SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon”



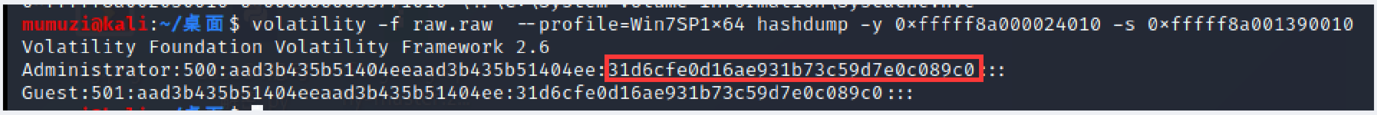
```
mumuzi@kali:~/桌面$ volatility -f raw.raw  --profile=Win7SP1x64 printkey -K "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \??\C:\Users\Administrator\ntuser.dat
Key name: Winlogon (S)
Last updated: 2021-04-11 09:22:17 UTC+0000

Subkeys:

Values:
REG_SZ        ExcludeProfileDirs : (S) AppData\Local;AppData\LocalLow;$Recycle.Bin
REG_DWORD     BuildNumber       : (S) 7601
REG_DWORD     FirstLogon        : (S) 0
----------------------------
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: Winlogon (S)
Last updated: 2009-07-14 04:45:47 UTC+0000

Subkeys:

Values:
REG_SZ        ExcludeProfileDirs : (S) AppData\Local;AppData\LocalLow;$Recycle.Bin
----------------------------
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: Winlogon (S)
Last updated: 2009-07-14 04:45:48 UTC+0000

Subkeys:

Values:
REG_SZ        ExcludeProfileDirs : (S) AppData\Local;AppData\LocalLow;$Recycle.Bin
mumuzi@kali:~/桌面$ 
```

获取密码哈希：
1.获取system 的 virtual 地址，SAM 的 virtual 地址：
volatility -f raw.raw --profile=Win7SP1x64 hivelist



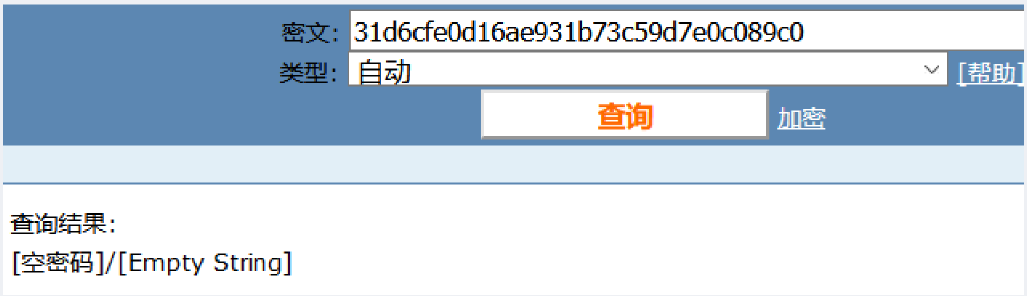
```
mumuzi@kali:~/桌面$ volatility -f raw.raw  --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a003696010 0x000000000d49b010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a00000f010 0x000000002c38c010 [no name]
0xfffff8a000024010 0x000000002c357010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000053010 0x000000002c306010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a001009010 0x000000001389e010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a00116e010 0x0000000012c14010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a0012f2010 0x0000000022ef8010 \SystemRoot\System32\Config\SECURITY
0xfffff8a001390010 0x000000000d075010 \SystemRoot\System32\Config\SAM
0xfffff8a0014fc010 0x0000000011b1c010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a00158f010 0x0000000072800010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001758010 0x0000000055580010 \??\C:\Users\Administrator\ntuser.dat
0xfffff8a001799010 0x0000000004568010 \??\C:\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002030010 0x0000000055771010 \??\C:\System Volume Information\Syscache.hve
mumuzi@kali:~/桌面$
```

2.hashdump:
volatility -f raw.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a001390010



```
mumuzi@kali:~/桌面$ volatility -f raw.raw  --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a001390010
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

>3.碰运气解hash(一般题都是能用cmd5、somd5解出来的)



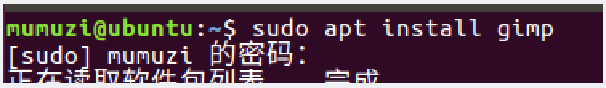
密文：31d6cfe0d16ae931b73c59d7e0c089c0
类型：自动 [帮助]

查询结果：
[空密码]/[Empty String]

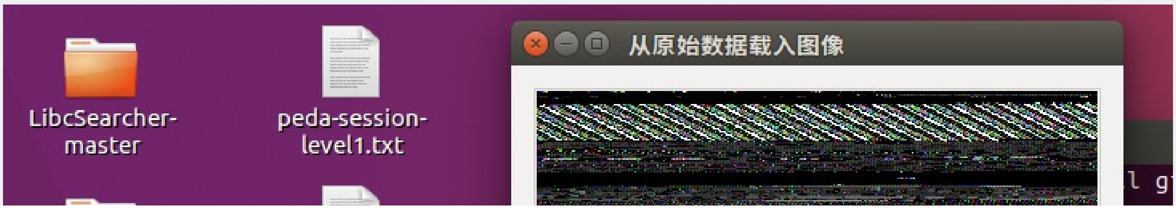
配合Gimp

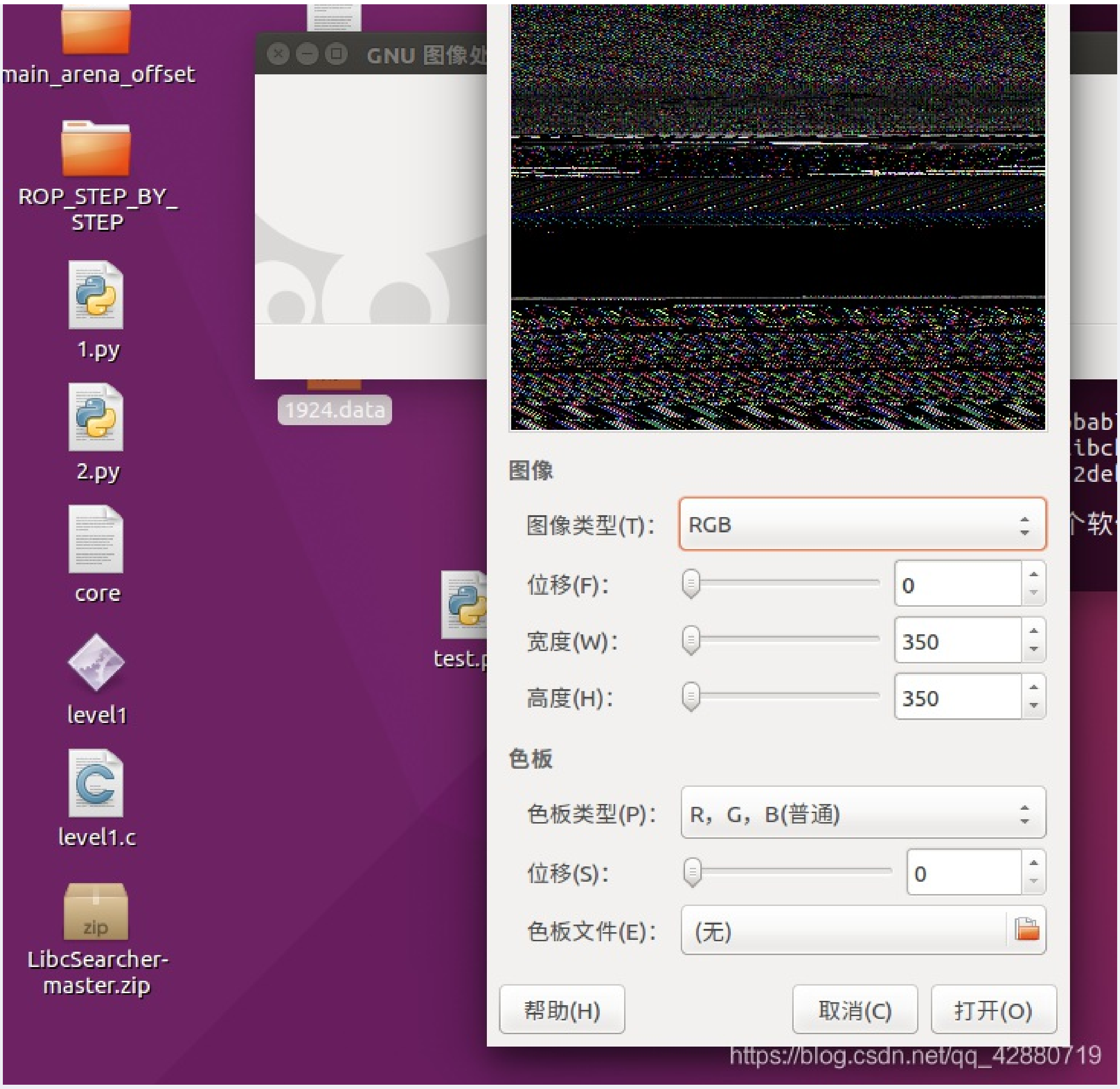
dump出正在运行的内存，然后配合Gimp

1.dump出正在运行的程序，随便dump都行
volatility -f raw.raw --profile=Win7SP1x64 memdump -p [PID] -D ./
2.将dump出来的文件(如1234.dmp)重命名为.data拓展名(即1234.data)
3.使用Gimp打开(ubuntu)



```
mumuzi@ubuntu:~$ sudo apt install gimp
[sudo] mumuzi 的密码：
正在读取软件包列表... 完成
```





图像

图像类型(T)：RGB

位移(F)：0

宽度(W)：350

高度(H)：350

色板

色板类型(P)：R，G，B(普通)

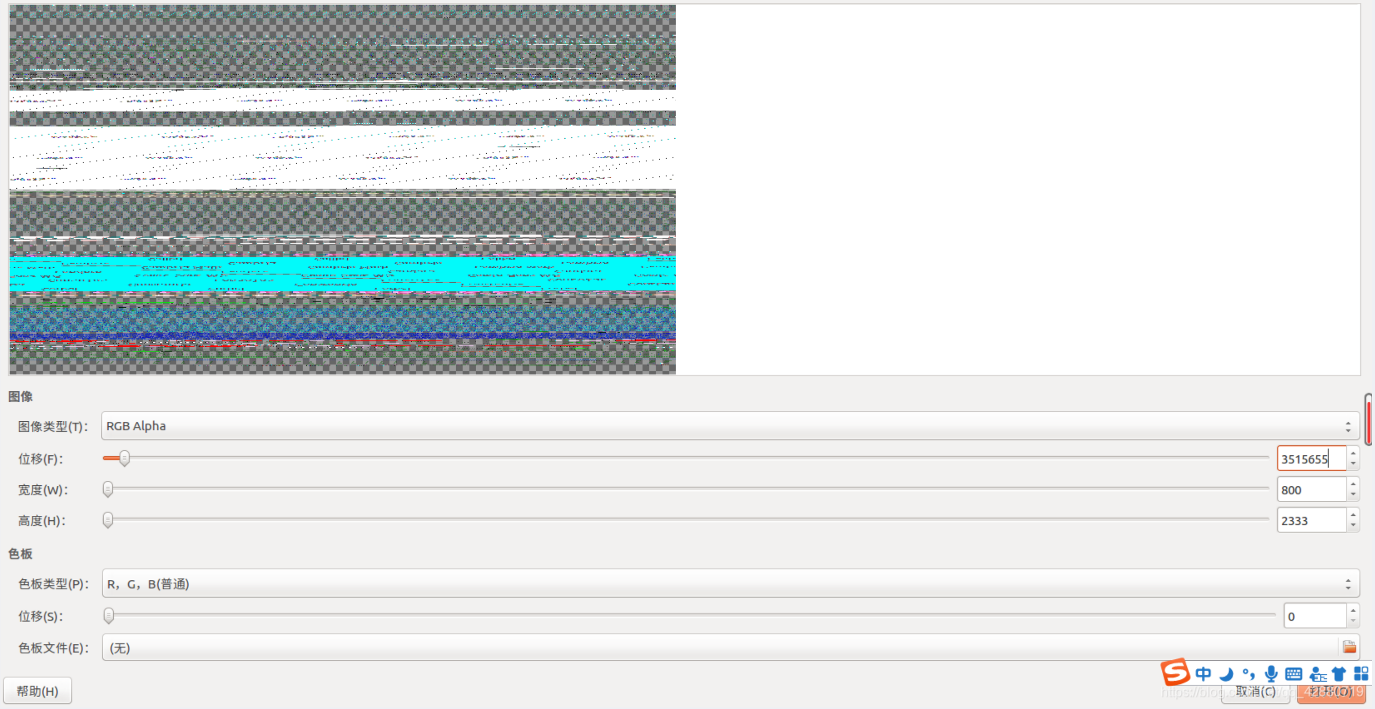
位移(S)：0

色板文件(E)：(无)

>4.这里请放大，进行如下操作

(1).将图像类型RGB修改为RGB Alpha

(2).调整高度(建议调稍微高一点)、确定一个看着合适的宽度、调整位移，可以使用鼠标滑轮和键盘来快速调整，也可以拖动调整



图像

图像类型(T)：RGB Alpha

位移(F)：3515655

宽度(W)：800

高度(H)：2333

色板

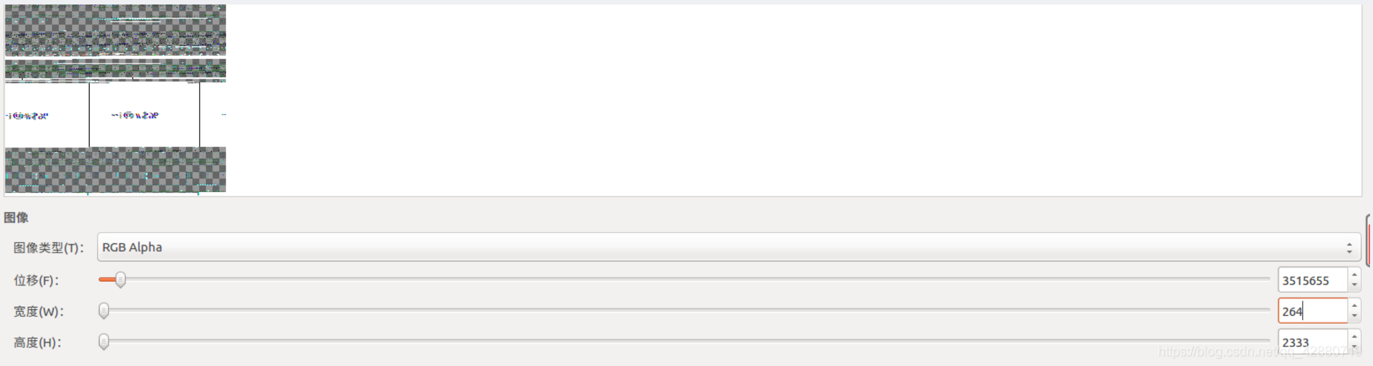
色板类型(P)：R，G，B(普通)

位移(S)：0

色板文件(E)：(无)

>例如这里我就找到文字信息(请注意，在宽度和位移下，可能会出现不同的界面)

>例如这里我就找到文字信息(请注意，在宽度和偏移下，可能会出现不同的界面)
经过调整，当宽度为264的时候，就会出现我想要的信息



图像

图像类型(T): RGB Alpha

位移(F): 3515655

宽度(W): 264

高度(H): 2333

当然，这里是倒过来的，脑补一下就行了。

例题

我真的是懒啊新题就不写了这里直接放我写的其他内存的WP
蓝帽2021 初赛
强网杯2021 初赛
第二届祥云杯
WMCTF2021
四川省大学生信息安全技术大赛
第一届网刃杯
Securinets CTF Quals 2022 Forensics Writeup