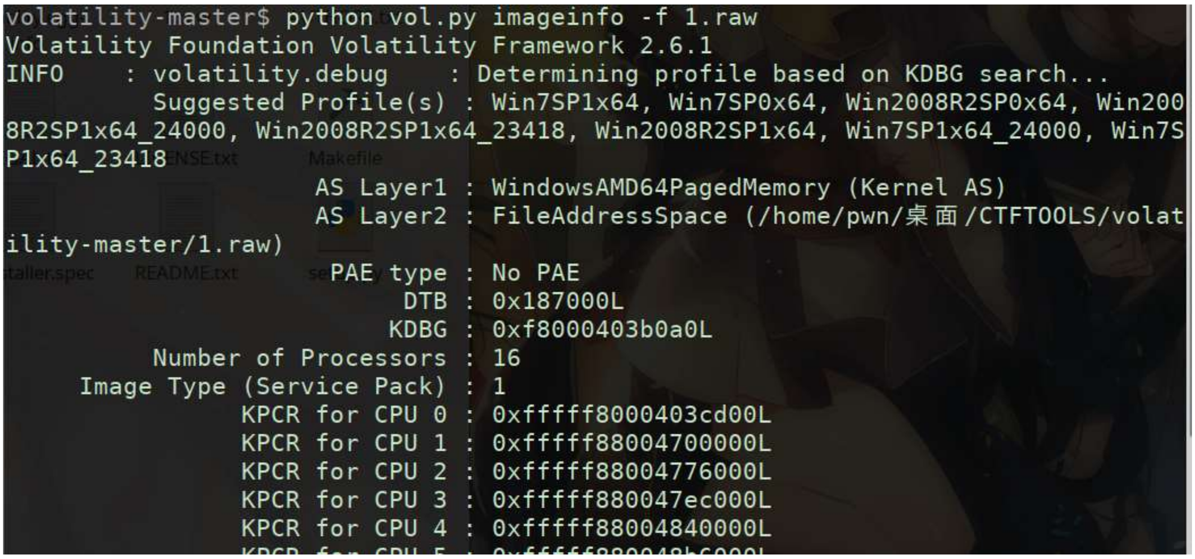
HGAME 2021 Week4 Writeup

MISC

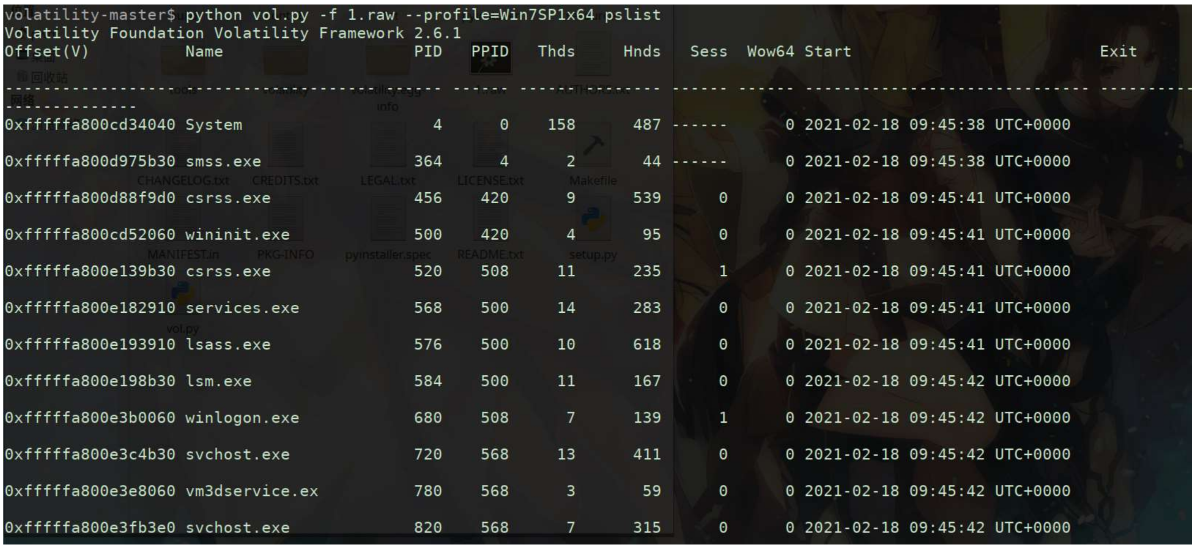
Akira之瞳-1

内存题，先用用`volatility`看下信息



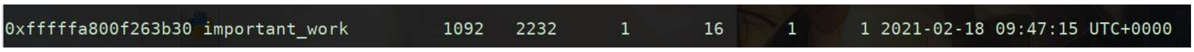
```
volatility-master$ python vol.py imageinfo -f 1.raw
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7S
P1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/pwn/桌面/CTFTOOLS/volat
ility-master/1.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf8000403b0a0L
          Number of Processors : 16
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff8000403cd00L
                KPCR for CPU 1 : 0xfffff88004700000L
                KPCR for CPU 2 : 0xfffff88004776000L
                KPCR for CPU 3 : 0xfffff880047ec000L
                KPCR for CPU 4 : 0xfffff88004840000L
                KPCR for CPU 5 : 0xfffff880048bc000L
```

确定是`Win7SP1x64`再从进程入手看看



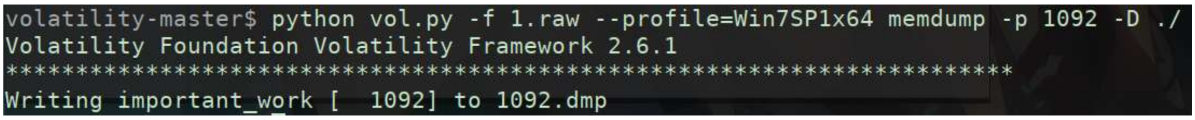
```
volatility-master$ python vol.py -f 1.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ---------
---------------
0xfffffa800cd34040 System                    4      0    158      487 ------      0 2021-02-18 09:45:38 UTC+0000

0xfffffa800d975b30 smss.exe                364      4      2       44 ------      0 2021-02-18 09:45:38 UTC+0000

0xfffffa800d88f9d0 csrss.exe               456    420      9      539      0      0 2021-02-18 09:45:41 UTC+0000

0xfffffa800cd52060 wininit.exe             500    420      4       95      0      0 2021-02-18 09:45:41 UTC+0000

0xfffffa800e139b30 csrss.exe               520    508     11      235      1      0 2021-02-18 09:45:41 UTC+0000

0xfffffa800e182910 services.exe            568    500     14      283      0      0 2021-02-18 09:45:41 UTC+0000

0xfffffa800e193910 lsass.exe               576    500     10      618      0      0 2021-02-18 09:45:41 UTC+0000

0xfffffa800e198b30 lsm.exe                 584    500     11      167      0      0 2021-02-18 09:45:42 UTC+0000

0xfffffa800e3b0060 winlogon.exe            680    508      7      139      1      0 2021-02-18 09:45:42 UTC+0000

0xfffffa800e3c4b30 svchost.exe             720    568     13      411      0      0 2021-02-18 09:45:42 UTC+0000

0xfffffa800e3e8060 vm3dservice.ex          780    568      3       59      0      0 2021-02-18 09:45:42 UTC+0000

0xfffffa800e3fb3e0 svchost.exe             820    568      7      315      0      0 2021-02-18 09:45:42 UTC+0000
```

感觉这个进程可能有关键信息



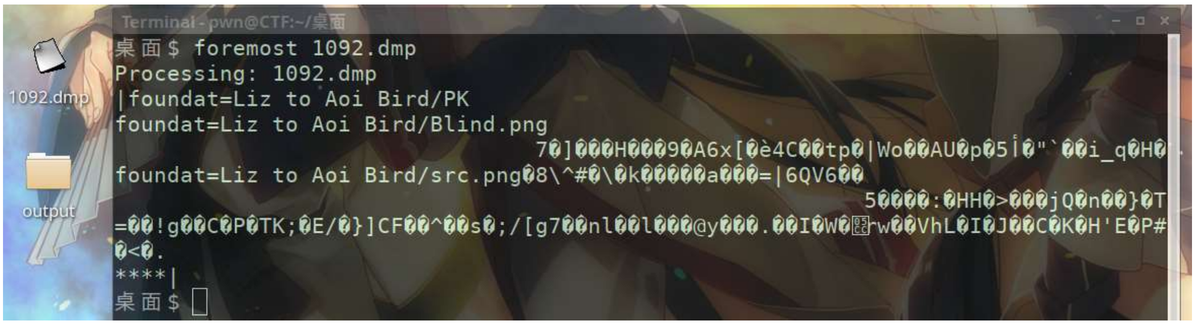
```
0xfffffa800f263b30 important_work         1092   2232      1       16      1      1 2021-02-18 09:47:15 UTC+0000
```

单独取出来看看



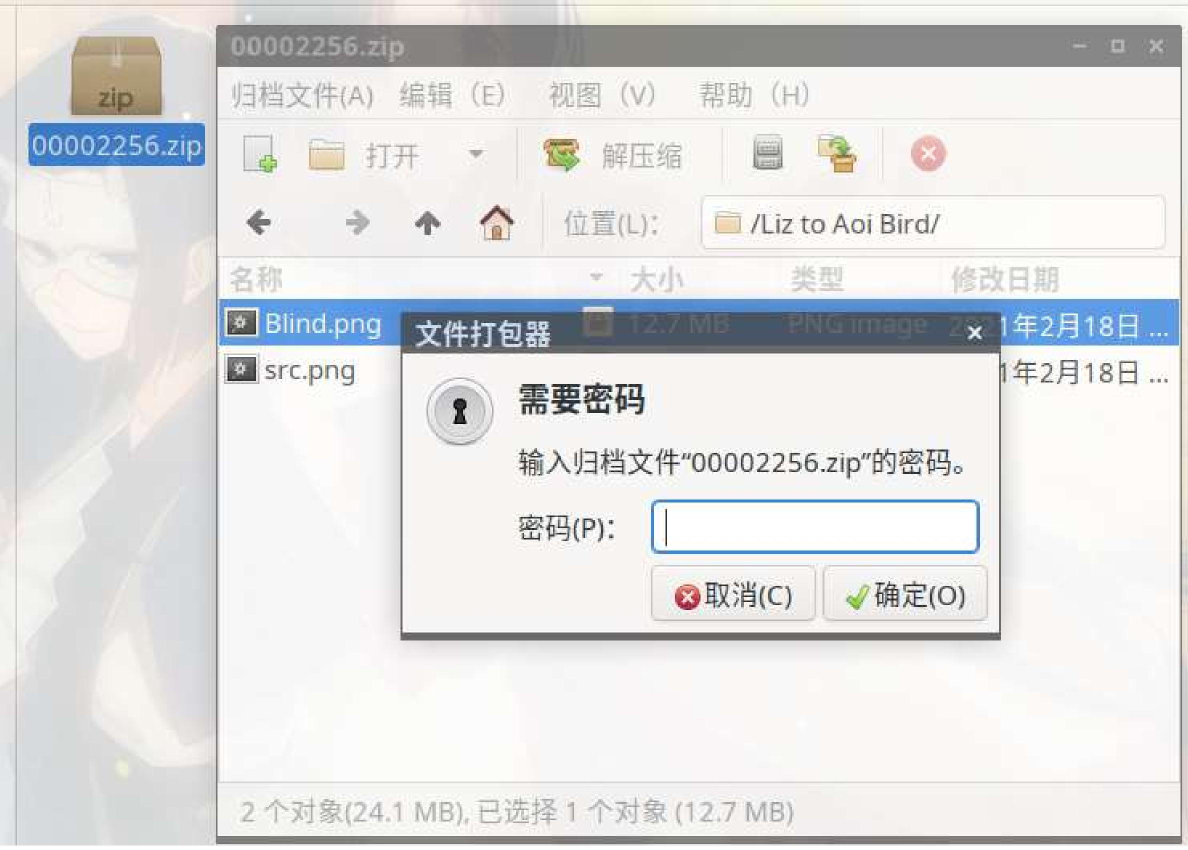
```
volatility-master$ python vol.py -f 1.raw --profile=Win7SP1x64 memdump -p 1092 -D ./
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing important_work [  1092] to 1092.dmp
```

使用foremost分离



```
桌面$ foremost 1092.dmp
Processing: 1092.dmp
|foundat=Liz to Aoi Bird/PK
foundat=Liz to Aoi Bird/Blind.png
                                7�]���H���9�A6x[�è4C��tp�|Wo��AU�p�5Ì�"`��i_q�H�
foundat=Liz to Aoi Bird/src.png�8\^#�\�k�����a���=|6QV6��
                                                         5����:�HH�>���jQ�n��}�T
=��!g��C�P�TK;�E/�}]CF��^��s�;/[g7��nl��l���@y���.��I�W�␅rw��VhL�I�J��C�K�H'E�P#
�<�.
****|
桌面$ 
```

发现zip，但需要密码



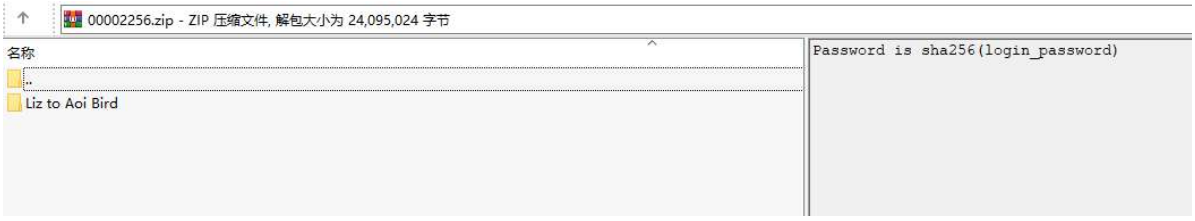
需要密码

输入归档文件“00002256.zip”的密码。

密码(P)：

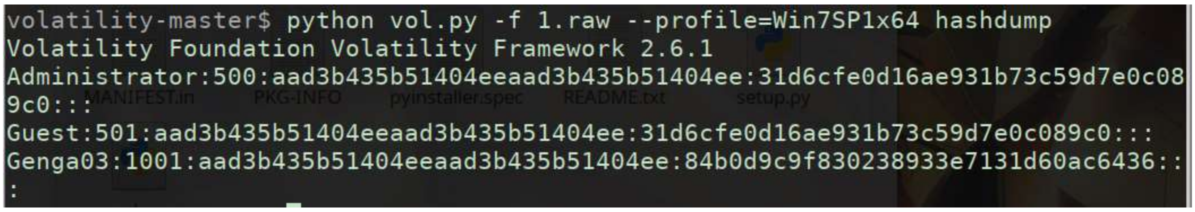
2 个对象(24.1 MB), 已选择 1 个对象 (12.7 MB)

在Windows环境中查看得到提示为登录密码的sha256形式



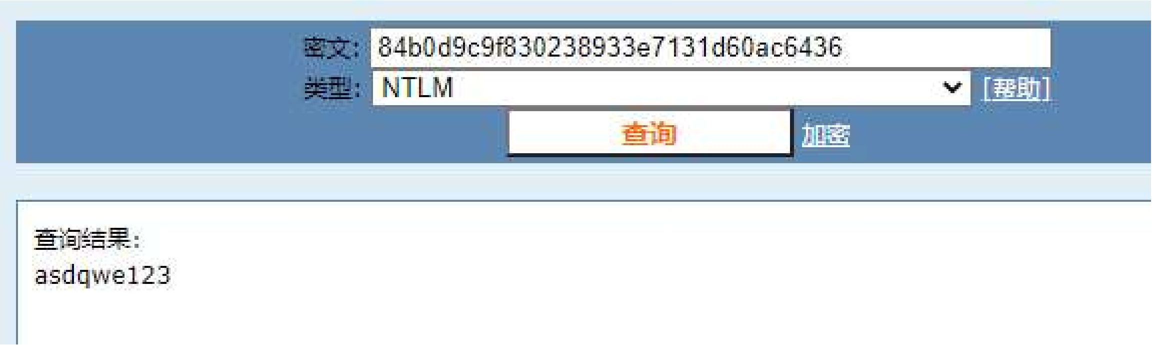
```
Password is sha256(login_password)
```

再用volatility获取登录用户密码的NTLM，其中Genga03后半就是



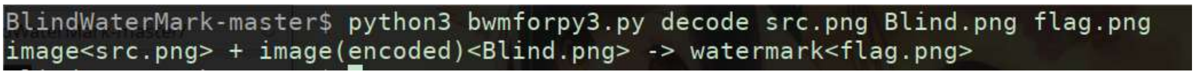
```
volatility-master$ python vol.py -f 1.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
```

尝试网页解出，发现弱密码



查询结果：
asdqwe123

转为sha256解压出两幅图片，看似一样看文件名，很明显是盲水印，用脚本解，起初一直失败死机，后来查了下发现Github上脚本原作者更新了python3版本且与python2不兼容，我用的是之前的python2版本，估计是这个原因，折腾一会用python3版本解出得到flag：



```
BlindWaterMark-master$ python3 bwmforpy3.py decode src.png Blind.png flag.png
image<src.png> + image(encoded)<Blind.png> -> watermark<flag.png>
```