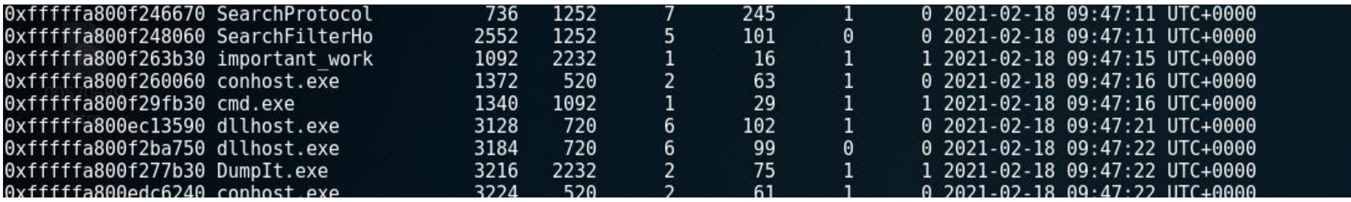
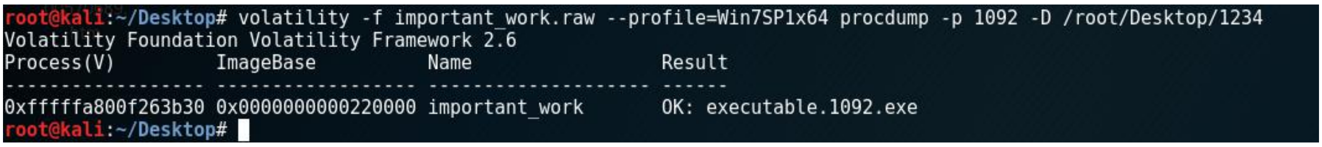
Misc1

拿到文件是 raw 形式，百度得知是内存读取，于是在 kali 上先用 volitity 命令获取相关信息



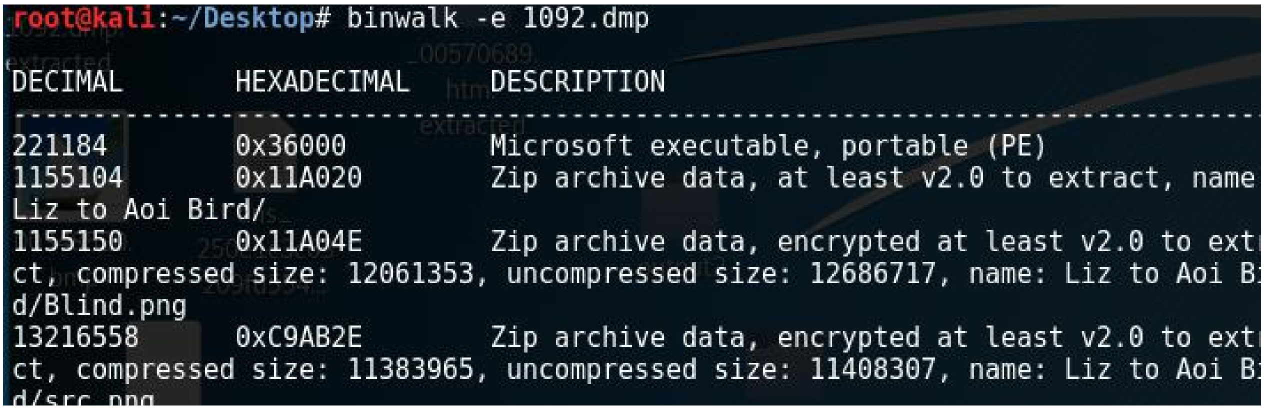
```
0xfffffa800f246670 SearchProtocol          736   1252      7      245      1      0 2021-02-18 09:47:11 UTC+0000
0xfffffa800f248060 SearchFilterHo         2552   1252      5      101      0      0 2021-02-18 09:47:11 UTC+0000
0xfffffa800f263b30 important_work         1092   2232      1       16      1      1 2021-02-18 09:47:15 UTC+0000
0xfffffa800f260060 conhost.exe            1372    520      2       63      1      0 2021-02-18 09:47:16 UTC+0000
0xfffffa800f29fb30 cmd.exe                1340   1092      1       29      1      1 2021-02-18 09:47:16 UTC+0000
0xfffffa800ec13590 dllhost.exe            3128    720      6      102      1      0 2021-02-18 09:47:21 UTC+0000
0xfffffa800f2ba750 dllhost.exe            3184    720      6       99      0      0 2021-02-18 09:47:22 UTC+0000
0xfffffa800f277b30 DumpIt.exe             3216   2232      2       75      1      1 2021-02-18 09:47:22 UTC+0000
0xfffffa800edc6240 conhost.exe            3224    520      2       61      1      0 2021-02-18 09:47:22 UTC+0000
```

看到一个关键进程，important work ，于是将他以 dmp 的形式读取出来（这里用 dumpfile 会出错）



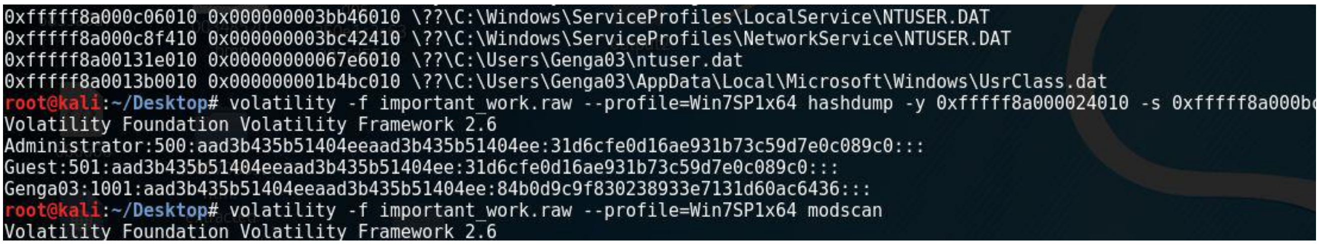
```
root@kali:~/Desktop# volatility -f important_work.raw --profile=Win7SP1x64 procdump -p 1092 -D /root/Desktop/1234
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa800f263b30 0x0000000000220000 important_work       OK: executable.1092.exe
root@kali:~/Desktop# 
```

再用 binwalk 分解得到一个关键的 zip 文件。



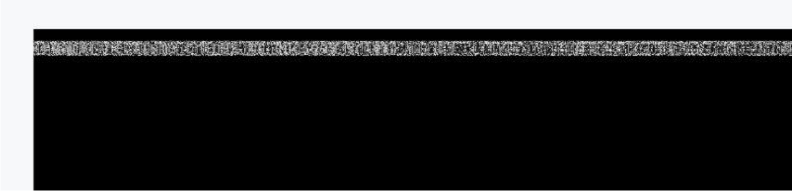
```
root@kali:~/Desktop# binwalk -e 1092.dmp

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
221184        0x36000         Microsoft executable, portable (PE)
1155104       0x11A020        Zip archive data, at least v2.0 to extract, name
Liz to Aoi Bird/
1155150       0x11A04E        Zip archive data, encrypted at least v2.0 to extr
ct, compressed size: 12061353, uncompressed size: 12686717, name: Liz to Aoi Bi
d/Blind.png
13216558      0xC9AB2E        Zip archive data, encrypted at least v2.0 to extr
ct, compressed size: 11383965, uncompressed size: 11408307, name: Liz to Aoi Bi
d/src.png
```

打开这个 zip 文件发现里面有两张图片，但是需要密码，看到 zip 附带的提示，sha256（login password），于是再返回内存读取用户登陆密码 hash 值，

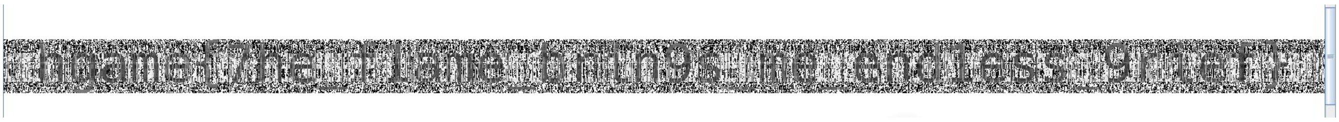


```
0xfffff8a000c06010 0x000000003bb46010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a000c8f410 0x000000003bc42410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a00131e010 0x0000000067e6010 \??\C:\Users\Genga03\ntuser.dat
0xfffff8a0013b0010 0x000000001b4bc010 \??\C:\Users\Genga03\AppData\Local\Microsoft\Windows\UsrClass.dat
root@kali:~/Desktop# volatility -f important_work.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a000b
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
root@kali:~/Desktop# volatility -f important_work.raw --profile=Win7SP1x64 modscan
Volatility Foundation Volatility Framework 2.6
```

再用 md5 解密得到明文 asdqwe123，再用 sha256 加密后就是压缩包密码，解压得到两张看上去一摸一样的图片，百度得知是盲水印攻击，于是下载盲水印脚本，这里因为 pyhton 问题搞了好久，感谢 akira 学长耐心解答我的问题。最后得到水印图片



再用 stegsolve 改变通道得到 flag



hgame{7he_f1ame_br1n9s_me_end1ess_9rief}