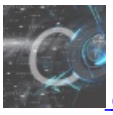
长安杯杂项writeup

原创

~VAS~ 已于 2022-04-23 03:47:02 修改 747 收藏

分类专栏： ctf 文章标签： 网络安全

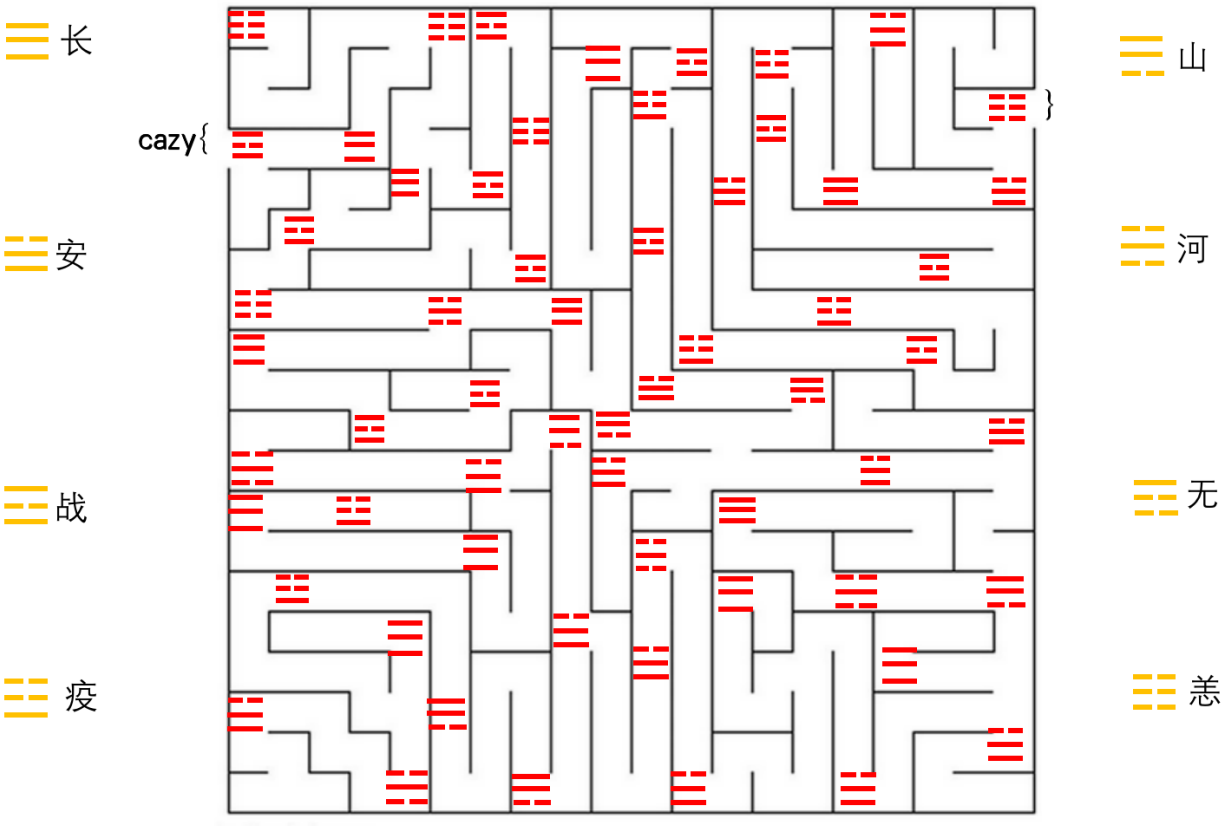
于 2022-01-08 22:17:13 首次发布

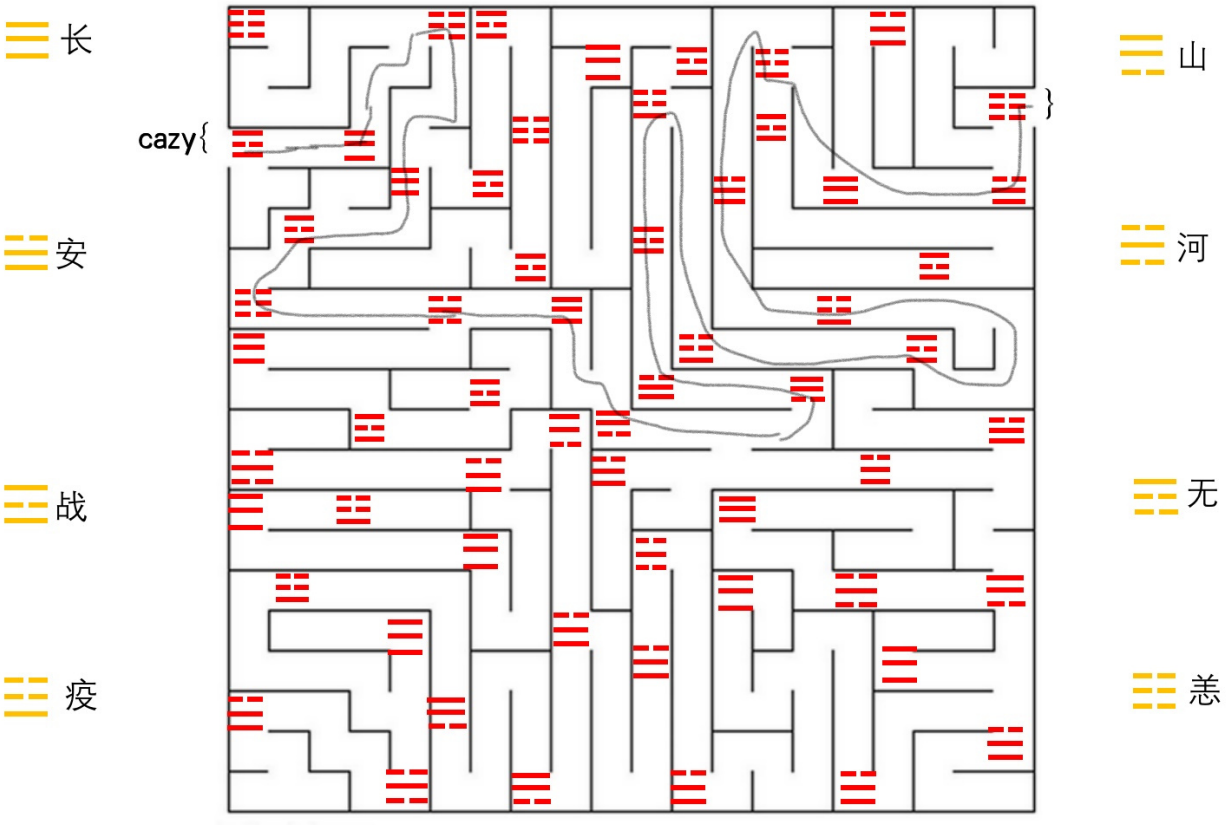


文章目录

八卦迷宫

这题是签到题





```
cazy{zhanchangyangchangzhanyanghechangshanshananzhanyiyizhanyianyichanganyang}
```

朴实无华的取证

先看一下版本WinXPSP2x86

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell https://aka.ms/pscore6

PS D:\TOOLS\数字取证\volatility-master\volatility-master> .\vol.exe -f .\xp_sp3.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\TOOLS\数字取证\volatility-master\volatility-master\xp_sp3.raw)
                      PAE type : PAE
                           DTB : 0x764000L
                          KDBG : 0x8054e2e0L
          Number of Processors : 2
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
                KPCR for CPU 1 : 0xf8757000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-12-27 02:37:41 UTC+0000
     Image local date and time : 2021-12-27 10:37:41 +0800
PS D:\TOOLS\数字取证\volatility-master\volatility-master>
```

CSDN @~VAS~

然后看一下进程

```
0x81fd27e8 softupnotify.ex        2936    916      0 --------      0      0 2021-12-27 01:40:40 UTC+0000   2021-12-27 01
:40:40 UTC+0000
0x819b0970 mspaint.exe            3888   1904      9      258      0      0 2021-12-27 01:44:37 UTC+0000

0x81a08da0 conime.exe             3260   2124      9      183      0      0 2021-12-27 01:44:47 UTC+0000

0x81d68a50 IEXPLORE.EXE           3748   1904     21      578      0      0 2021-12-27 01:44:52 UTC+0000

0x819d6a18 wdswfsafe.exe          2136    916      4       70      0      0 2021-12-27 01:44:52 UTC+0000

0x819c98a0 softupnotify.ex         884    916      0 --------      0      0 2021-12-27 01:44:52 UTC+0000   2021-12-27 01
:44:52 UTC+0000
0x81c2b2f0 IEXPLORE.EXE           3976   3748     37     1374      0      0 2021-12-27 01:44:52 UTC+0000

0x819b23b0 softupnotify.ex        1916    916      0 --------      0      0 2021-12-27 02:00:18 UTC+0000   2021-12-27 02
:00:18 UTC+0000
0x81c33630 softupnotify.ex         972    916      0 --------      0      0 2021-12-27 02:03:28 UTC+0000   2021-12-27 02
:03:28 UTC+0000
0x81f2c7e0 notepad.exe            2976   1904      6      180      0      0 2021-12-27 02:27:06 UTC+0000

0x81c7f630 360zip.exe             3388   1904     10      366      0      0 2021-12-27 02:28:39 UTC+0000

0x81d4d020 2345PicViewer.e        3812   1904     23      378      0      0 2021-12-27 02:36:41 UTC+0000

0x81923020 taskmgr.exe            3628    668      9      188      0      0 2021-12-27 02:37:11 UTC+0000

0x81c30da0 DumpIt.exe             3300   1904      1       16      0      0 2021-12-27 02:37:38 UTC+0000

PS D:\TOOLS\数字取证\volatility-master\volatility-master>
```

CSDN @~VAS~

notepad看一下,发现一个encrypt的东西 加密吗???

```
PS D:\TOOLS\数字取证\volatility-master\volatility-master> .\vol.exe -f .\xp_sp3.raw --profile=WinXPSP2x86 notepad
Volatility Foundation Volatility Framework 2.6
Process: 2976
Text:
?

Text:
?□

Text:
□

Text:
?
```

```
Text:
?????????????
20211209(encrypt)
??????????????????????
????!?????
????!???
```

CSDN @~VAS~

换kali,Windows vol有毒

```
root@kali: ~/桌面/volatility_2.6_lin64_standalone
文件  动作  编辑  查看  帮助

Text:
?

Text:
?????????????
20211209(encrypt)
??????????????????????
????!?????
????!???


┌──(root💀kali)-[~/桌面/volatility_2.6_lin64_standalone]
└─# ./volatility_2.6_lin64_standalone -f ../ctf/xp_sp3.raw filescan | grep fl
ag
Volatility Foundation Volatility Framework 2.6
0x00000000017ad6a8      2      0 R--rw- \Device\HarddiskVolume1\Documents and
 Settings\Administrator\桌面\flag.zip
0x00000000018efcb8      1      0 RW-rw- \Device\HarddiskVolume1\Documents and
 Settings\Administrator\Recent\flag.lnk
0x0000000001b34f90      1      1 R--r-- \Device\HarddiskVolume1\Documents and
 Settings\Administrator\桌面\flag.zip
0x0000000001e65028      1      0 R--rw- \Device\HarddiskVolume1\Documents and
 Settings\Administrator\桌面\flag.png

┌──(root💀kali)-[~/桌面/volatility_2.6_lin64_standalone]
└─# sS
```

CSDN @~VAS~

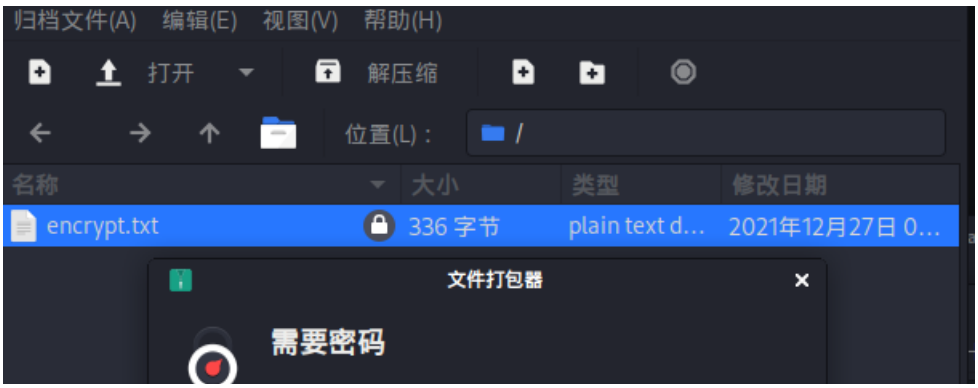
导出文件

```
┌──(root💀kali)-[~/桌面/volatility_2.6_lin64_standalone]
└─# ./volatility_2.6_lin64_standalone -f ../ctf/xp_sp3.raw dumpfiles -Q 0x000
0000001b34f90 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x01b34f90   None   \Device\HarddiskVolume1\Documents and S
ettings\Administrator\桌面\flag.zip
SharedCacheMap 0x01b34f90   None   \Device\HarddiskVolume1\Documents and Sett
ings\Administrator\桌面\flag.zip

┌──(root💀kali)-[~/桌面/volatility_2.6_lin64_standalone]
└─# sSsS
```

CSDN @~VAS~

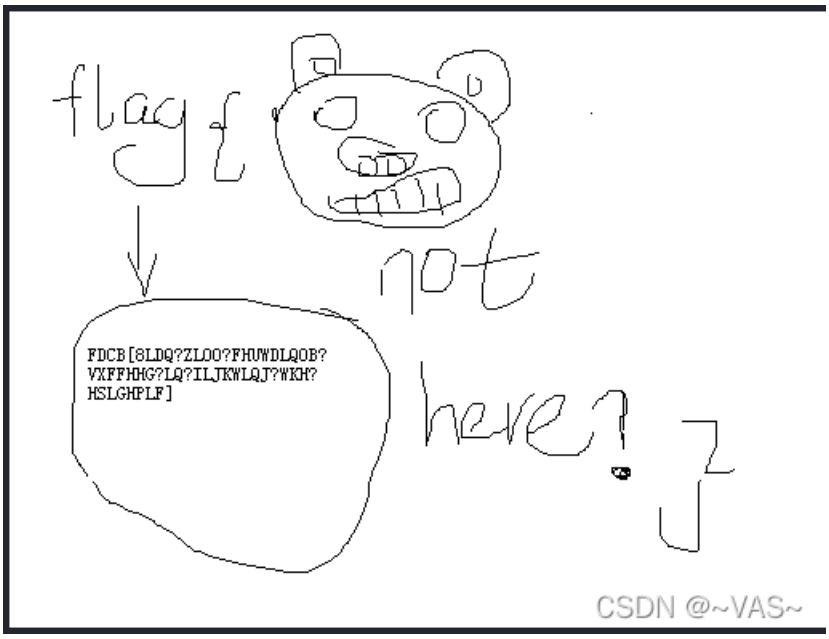
发现有密码输入之前看到的东西试试



得到一个脚本

```
//Ó×¶ùÔ°Ë®Æ¼µÄ¾ÓÃÜ£¨²¿·Ö£©
void Encrypt(string& str)
{
 for(int i = 0; i < str.length(); i++)
 {
  if(str[i] >='a'&& str[i]<='w')
   str[i]+=3;
  else if(str[i]=='x')
   str[i]='a';
  else if(str[i]=='y')
   str[i]='b';
  else if(str[i]=='z')
   str[i]='c';
  else if(str[i]=='_')
   str[i]='|';
  str[i] -= 32;
 }
}
```

flag.png还有东西,看来是用上面那个脚本反推解密



借用了套神的脚本改了一下

```python
s = 'fdcb[8ldq?zloo?fhuwdlqob?vxffhhg?lq?iljkwlqj?wkh?hslghplf]'
for i in s:

    if(ord(i)-3>=ord('a') and ord(i)-3<=ord('w')):

        print(chr(ord(i)-3),end='')
    elif(i == 'a'):
        print('x',end='')
    elif(i == 'b'):
        print('y',end='')
    elif(i == 'c'):
        print('z',end='')
    elif(i == "|"):

        print('_')
    else:

        print(chr(ord(i)+32),end='')
```

```
test1
D:\Python_project\venv\Scripts\python.exe D:/Python_project/test1.py
cazy{Xian_will_certainly_succeed_in_fighting_the_epidemic}
Process finished with exit code 0
```

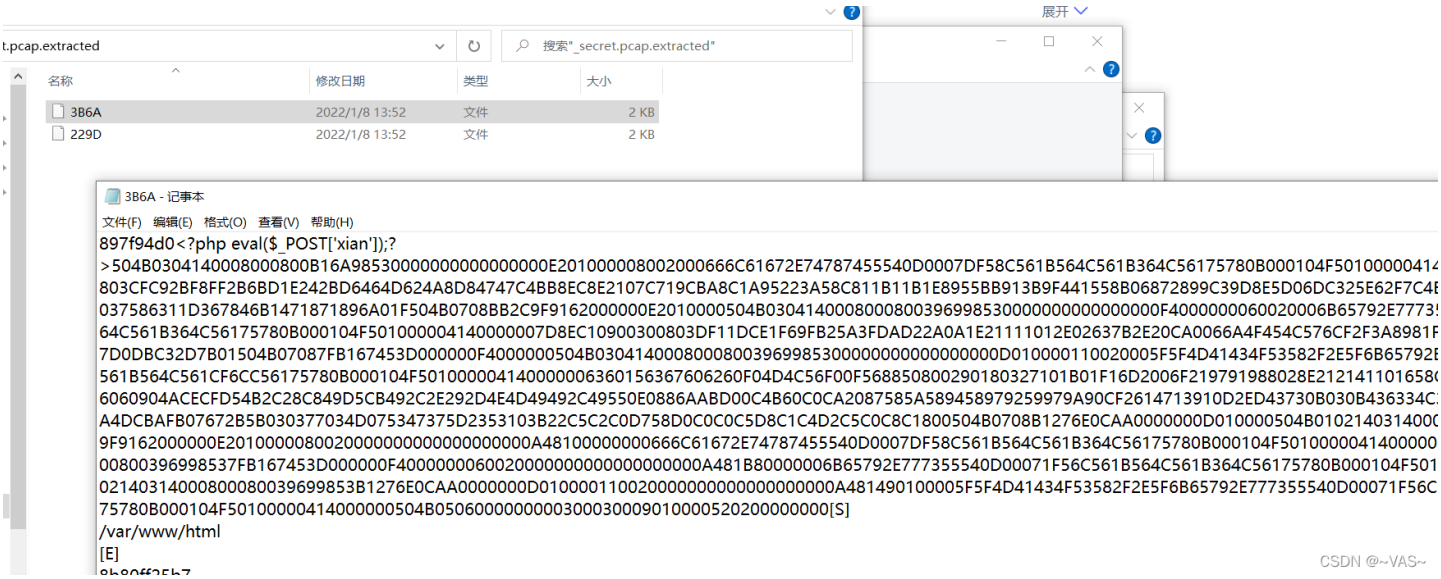
无字天书

secret.pcap用binwalk分解,出了两个文件

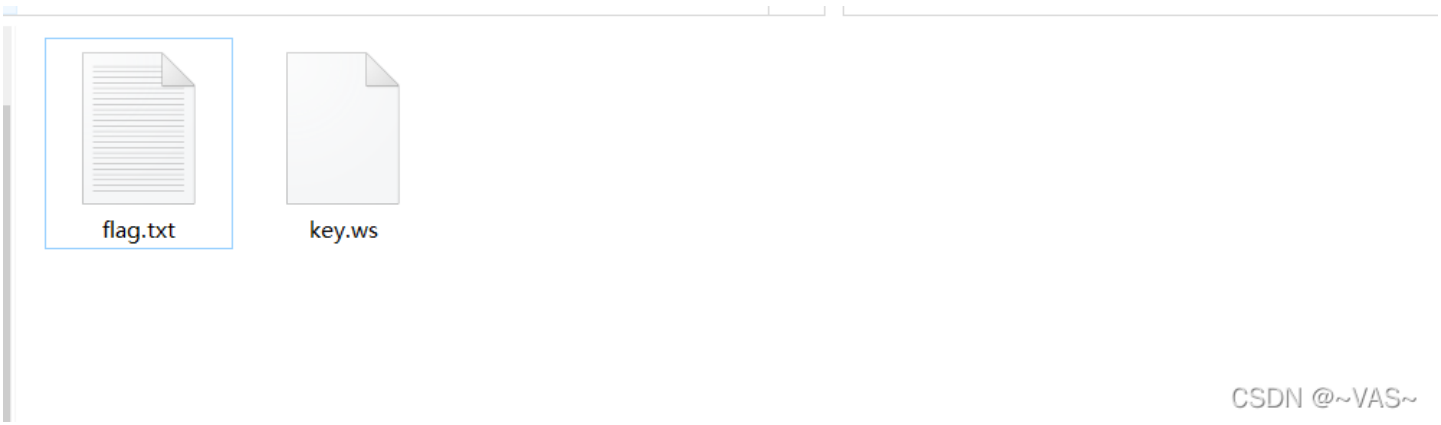
```
┌──(root💀DESKTOP-F82I2BJ)-[/mnt/c/Users/mzq/Downloads]
└─# binwalk secret.pcap -e

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Libpcap capture file, little-endian, version 2.4, No link-layer encapsulation, s
naplen: 524288
5358          0x14EE          Unix path: /var/www/html
8861          0x229D          gzip compressed data, from Unix, last modified: 1970-01-01 00:00:00 (null date)
15210         0x3B6A          gzip compressed data, from Unix, last modified: 1970-01-01 00:00:00 (null date)
```

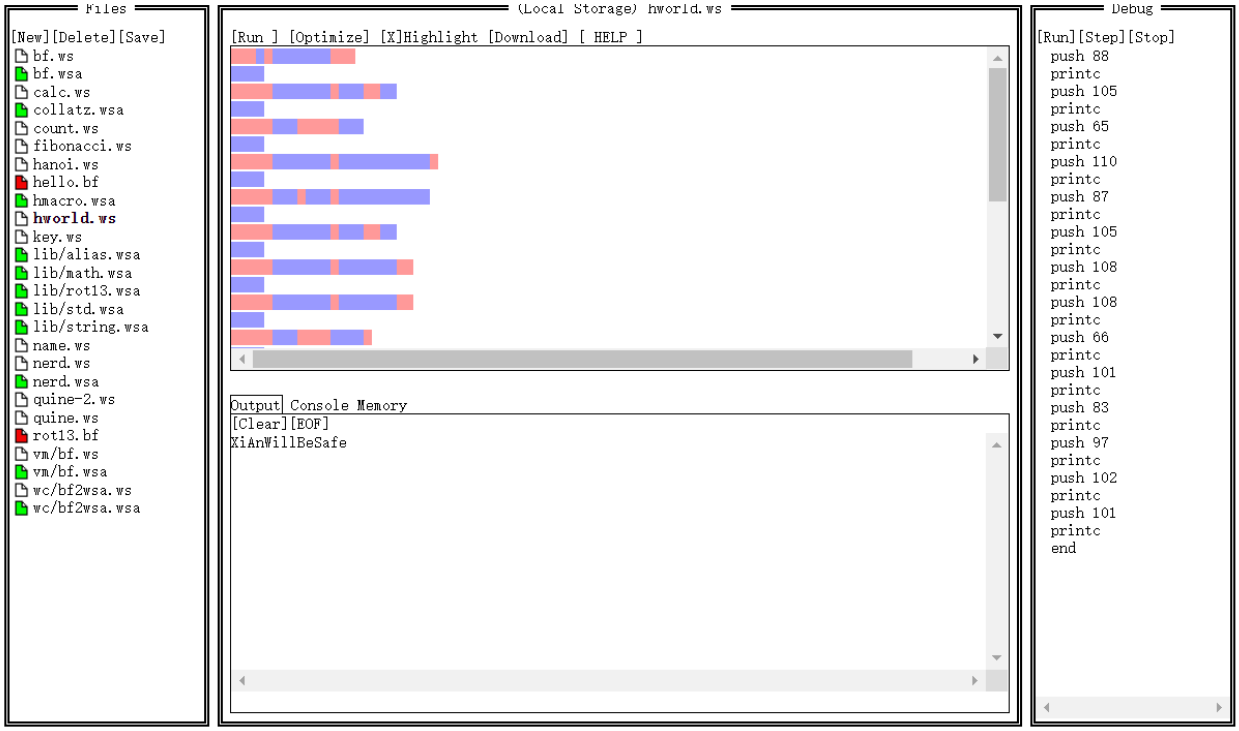
其中一个文件里数据明显是一个压缩包504b是zip



转1.zip,解压后是一个flag.txt和key.ws



key.ws是whitespace https://vii5ard.github.io/whitespace/

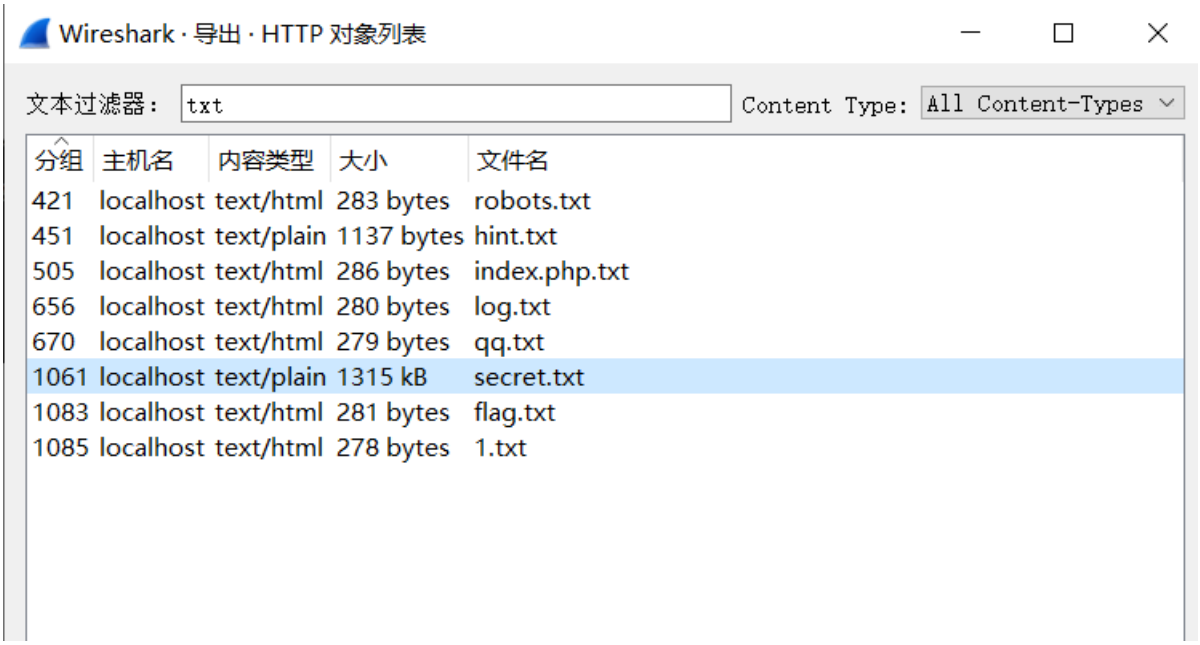


flag.txt是snow加密,密码是whitespace解出的

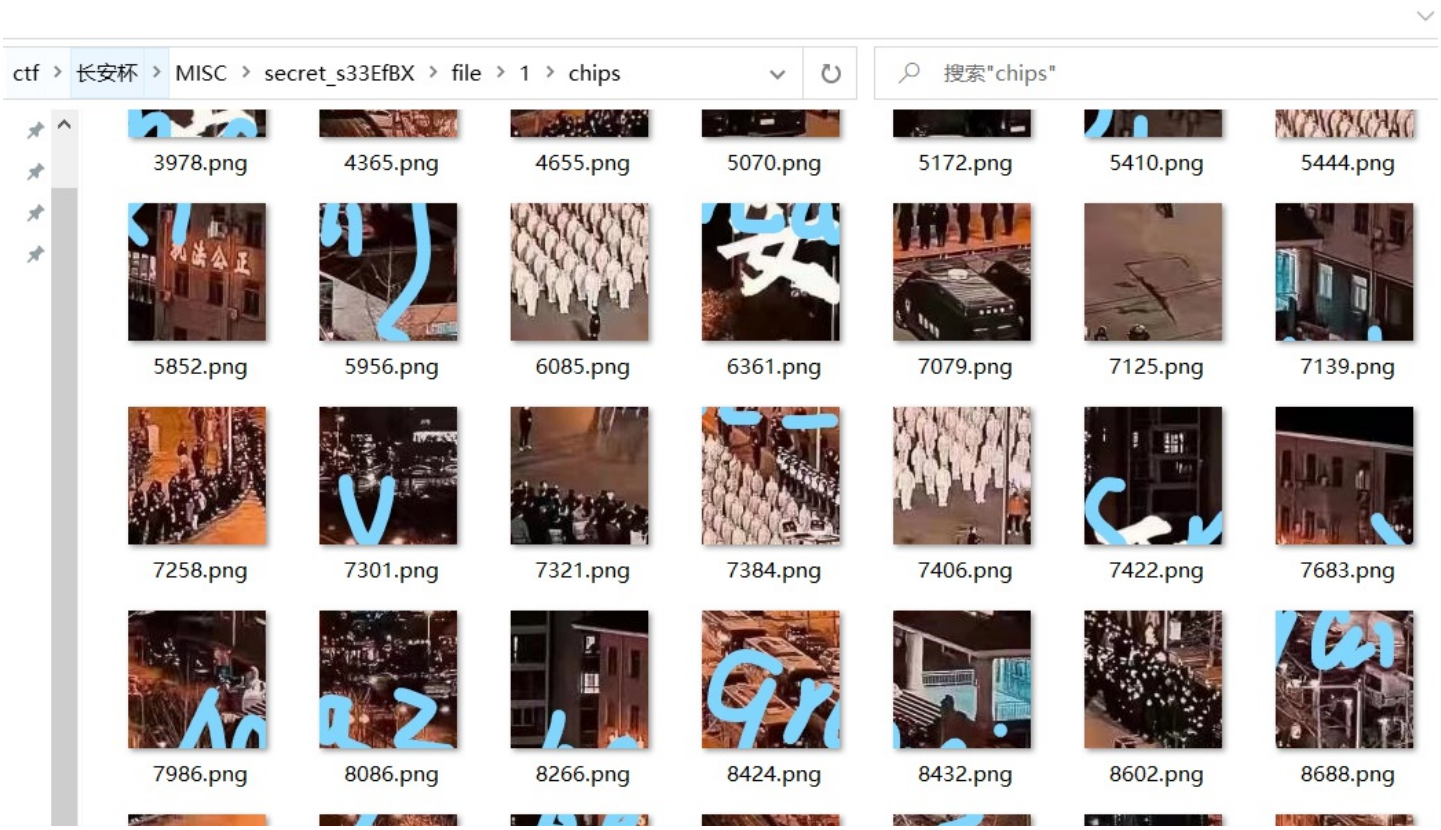
```
D:\TOOLS\密码学工具\snow>SNOW.EXE -p XiAnWillBeSafe -C flag.txt
cazy{C4n_yOu_underSt4nd_th3_bOoK_WithOut_Strlng}
D:\TOOLS\密码学工具\snow>
```

西安加油

查看http流文件,找txt文件,发现一个flag.txt进去后啥也没有,然后在secret,txt找到base64编码的zip文件



保存为压缩包后解压发现全是图片,看来又要拼图了



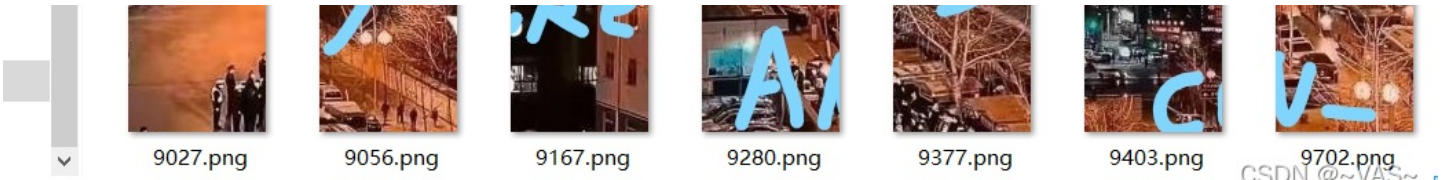

9027.png
9056.png
9167.png
9280.png
9377.png
9403.png
9702.png


Figure 1
Solution
Crazy_Snake_Xi_An_Great_Again
Analyzing image:
26.1%
28.3%
30.4%
32.6%
34.8%
37.0%
39.1%
41.3%
43.5%
encrypt.txt
1650.png
4365.png
7139.png
8432.png
CSDN @~VAS~