



[~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

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zip471642048/article/details/122386678>

版权



[ctf 专栏收录该内容](#)

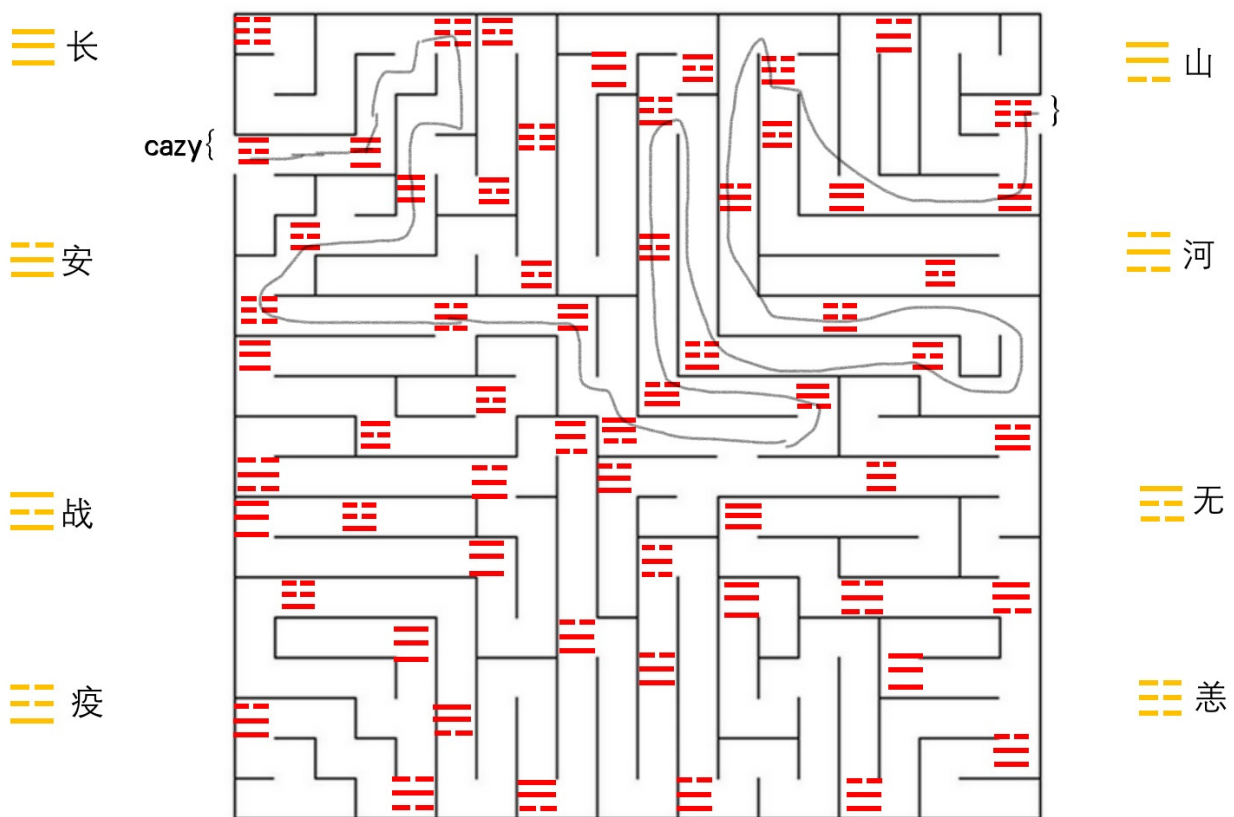
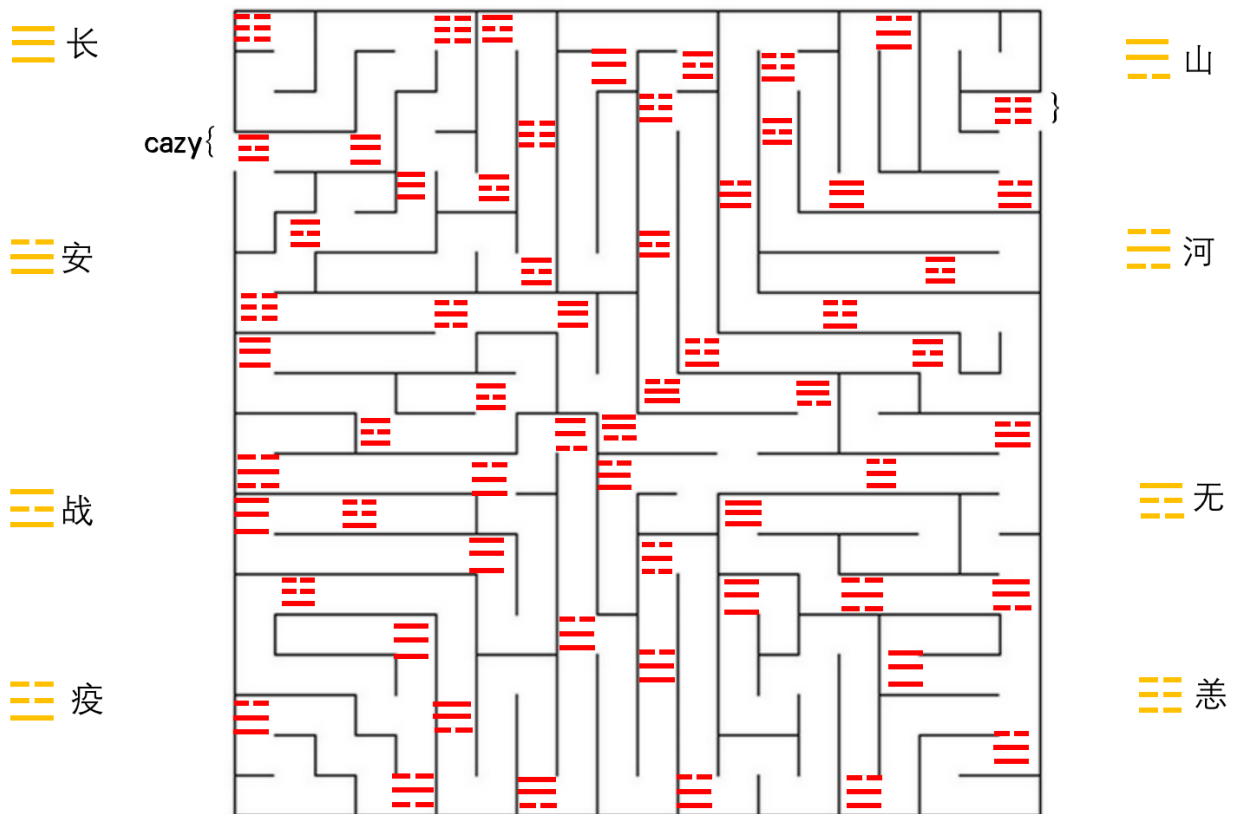
50 篇文章 1 订阅

订阅专栏

文章目录

- [八卦迷宫](#)
- [朴实无华的取证](#)
- [无字天书](#)
- [西安加油](#)

[八卦迷宫](#)



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 : 0xfffff000L
      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 wdsfwfsafe.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
0x0000000017ad6a8      2      0 R--rw- \Device\HarddiskVolume1\Documents and
Settings\Administrator\桌面\flag.zip
0x0000000018efcb8      1      0 RW-rw- \Device\HarddiskVolume1\Documents and
Settings\Administrator\Recent\flag.lnk
0x000000001b34f90      1      1 R--r-- \Device\HarddiskVolume1\Documents and
Settings\Administrator\桌面\flag.zip
0x000000001e65028      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~

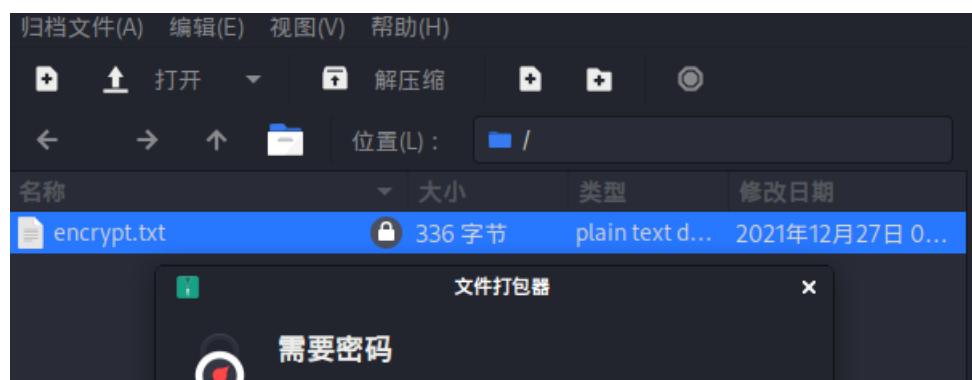
导出文件

```
(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]
# sss
```

CSDN @~VAS~

发现有密码输入之前看到的東西试试

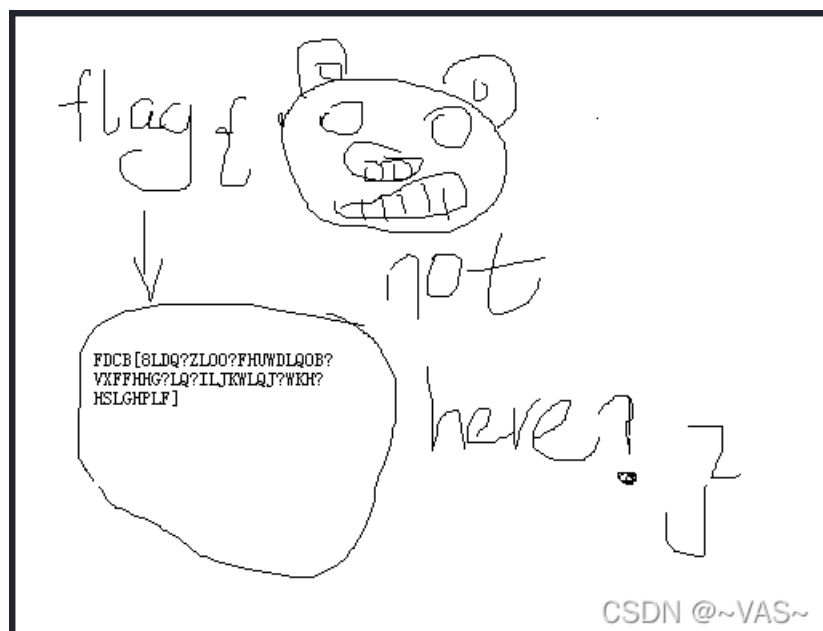




得到一个脚本

```
//Ó×ŸùÔ°Ë®Æ¼μÃ%ÓÄÜE""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

```

s = 'fdcb[8ldq?zloo?fhuwdlqob?vxffhbg?lq?iljkw1qj?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 x
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-F82128J) ~/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, snaplen: 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)

CSDN @~VAS~

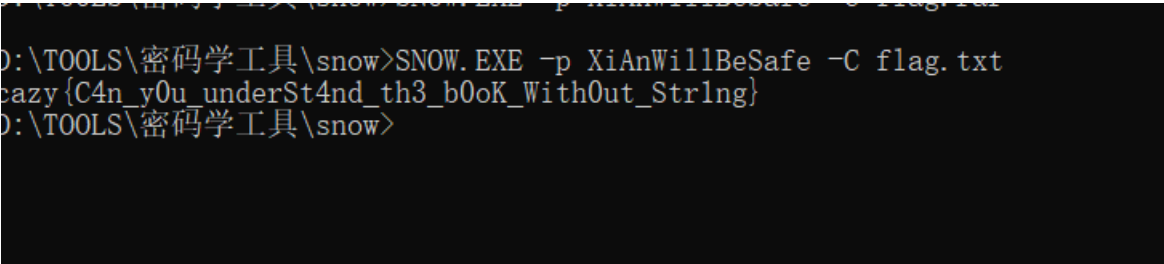
转1.zip,解压后是一个flag.txt和key.ws

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



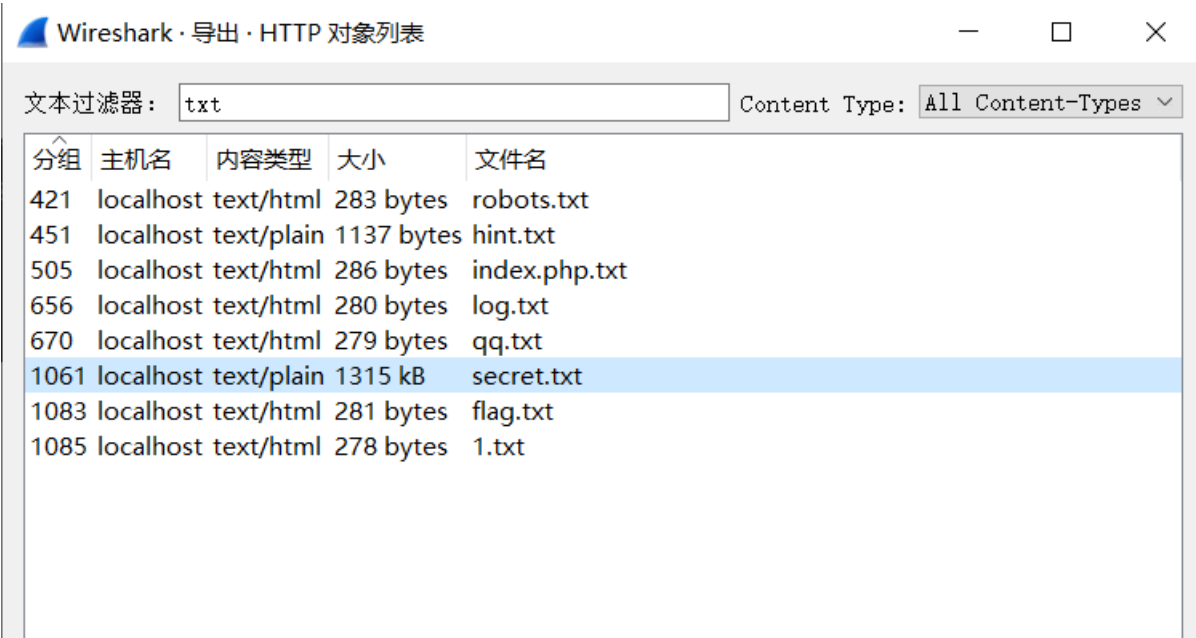
CSDN @~VAS~

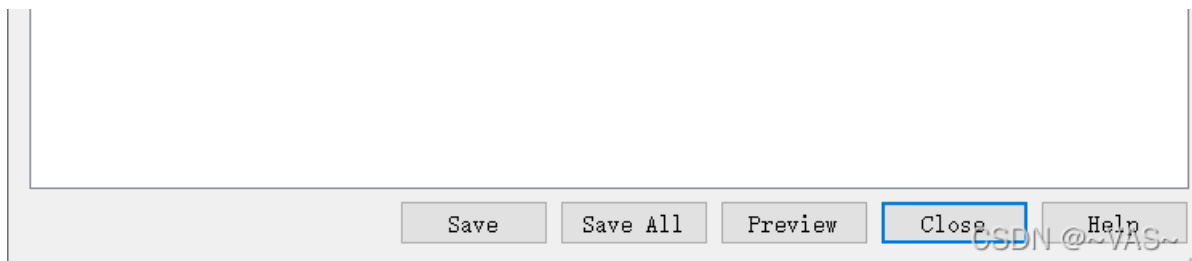
flag.txt是snow加密,密码是whitespace解出的



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



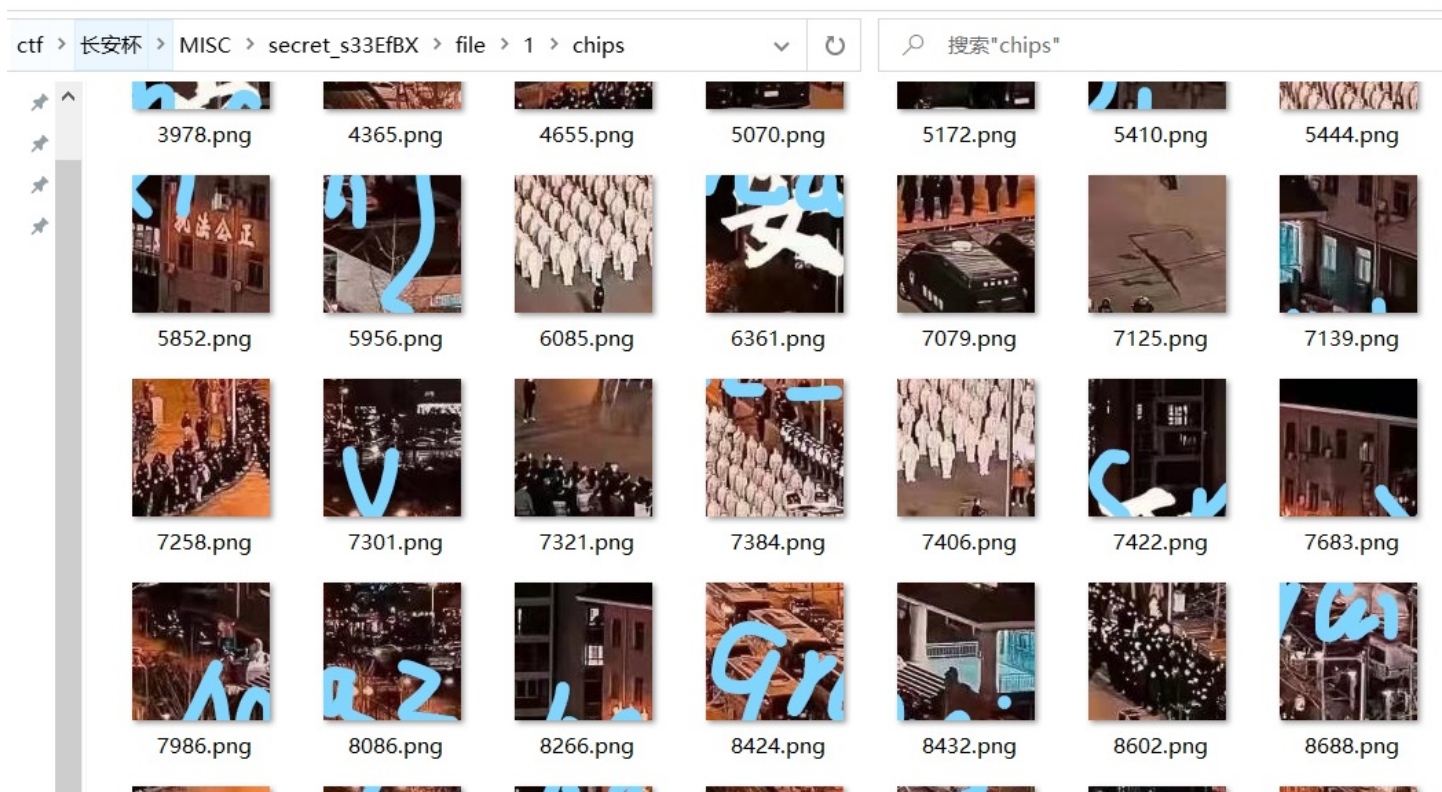


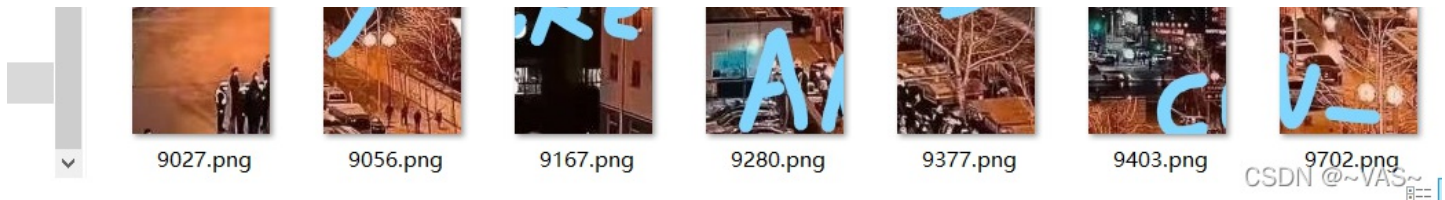
secret.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

UESDBBQAAAAAAAtlmVMAAAAAAAGACAAAY2hpcHMVVVQNAa3oMZhxqDGYcagxmF1eAsAAQT1AQAAABQAAABQSwMEFAAIAAgAC2WZUwAAAAAAGAAABAAIAbf
TWC8uX2NoaXBzVWQNAa3oMZhxqDGYcagxmF1eAsAAQT1AQAAABQAAABQSwMEFAAIAAgAC2WZUwAAAAAAGAAABAAIAbf
Wf7eviWZKaG1qcWhSsmF7MwBUKJNZXGJgslADagAjkknlG8MAUEsHCBjbeAqhtAAAA0gAAAFBLAwQAAUgACADUy5ITAIAAAAAAAB8aAAADAgAGN0aXBzLzkyODAwG5nVQNAAdw
GYRygmF1eAsAAQT1AQAAABQAAADst/VbVN8bNrqBAYYQhpCQGNDoDiWVcKqRiRgBQSSKQ1q6u7tTgRGRFgZEOiSkQUKQUKkGyQGDt/3h/P+cv6D87mva
+31rLX3Xteq537uJ1pbU/0U06T1SAADUqKvBkbe1xf8KGP/2eROETWAAKE+WBUpWz54BfLddYAA/0hYA3Vp4tw2xTWaA+LYmv21z3RaAefP/fPMf/sNj+/A/4T/8h/
+/gJCIAPiJfK9C1RBBsAd/105LSf4/NoGICACkpPxf+/+qCbD7/wb4T038h//wH/7Df/gP//
+GmliYqlyomlyOPTWeCApLy71/9kHAPHfVokAQD9eHa6o65X3AudZj/75li1qp3VU2qTfDfZqYvXoAf6jummypQIASILMkS0GFFpMht4m3sBQfNtg/i5OxRp14Z0vdQNHL3h7PoOM3UksRIq
msfLvpZ/4m/zOXH9lu2/EbYj7/ig5Hzax37hNp7yXP38eU2juyyO/UuGwBRAfMRm0FAyhmaXDQNDcbVqsGFHzbcbxaiUJOxP7NcrGLVHAqcE6B/uuUv0pEsehY2elKzoYw
+EjZqrSpcWcD946FVWCi189j39WaE1aOAYcDJSpmr+V2cqV7UsoZD7uK7YVY0XveGBN27jXYYqQNNqalHT1YBWY4+KF3UWuqSh3a07TiffCh8HnmXMMWmtmrCBMlj5dyM3OhfF33g
+hyxZPt55Z6lW5MRRfd+E7bAd385eO9S69GJLsYwX4NLWWdodHSp2XPvcummDRLSqalDS6dW6nH5teOR6n4vwwk6lQT6t1EWZU0OVWxu1vK1ZTXGKMRRNT3z
+PDwDxgF3n75nbpWlfiKerNrxYmqQlUpFTRagjbnxqx+Iz3FCGZg0pg/SyYepf10NEvW5eVeqFQnvrT2zmy
+e6eN281ckYL5Ac478wdpJYKmbTsd8bnoj7lVp73zsWkuUrklidg6auisfvVoe7sBDjes/dSn9uxsefLI4H74VD4e2SeZqLsoRZtt55iqjRwUBFfuOTjT7fl34olCO00JdKOQsbGxjY4Lmyc
+03PjNu7bs7WfN+eFS7Ozs/Pzsr672+vr615yGUGpGRYrR4ktRcgPPkt7DvlyfEv/UeUTr+McuZZbxdj64Xt9JZseBZjHJDFoAgnhiOZ8+XRszEgYkCuhGHwqvA5D
+7hs//6jvMrJ20XWcdDEIXHNe0FwXbFub2D0vSgoWN/Q6+eVi3z7CEBYhsUyaEhlavpaewsW6zspOqB0jHvllw3rJYcywh2DhT56PWNn//ljnHpi/KMJ6OUxd+mMBX94q/A7KTmaJcpn26Uwc
+VaOLZw+LODxD0WZubt3V001VbNs9WB1JXfYIafSqvbaZfJr4K8AsMNLHPX/OGGNIrIjd/awzLBISENLhSfzvbxFNFuTAXSgW0zo
+2XF9smVwWy8v4XhjlS0RyJHYpJChQOJFVei9C3yRXgX6fOkTEphN5D0JABR1sHobdWLR/m2YWWDD1MWEtjXPmj82nLoflSHwCNv/f2uxufNm0pkmcHUONS380edXVZVIGq4pdWz8M8d
s18mtPUenF3YnTXqpU0rtqr/Nej07XPeY27PME2zhscRDafoX4v9RQR759zpi9bu7JrYvB7ZrWz29KSk6BK5XXK8SvCzjknSUWq+ULM0Mjly8vLSlVZscm1tzX6mqrKiQkCwEma7621cgM0PqJ7f
+J5+ID56atMvmjKx3JndNOTdv7R/o/W50iN54YCMr8RNE8wetu/PVUe2YlUmdaB2FQYkrKD1MvSPumVYwzfLFYeUPVkmGlsNFUI/dOfOqS79pWz
+RqcoVPezhMjZtVkyGOcHuBN9/RZGSVTSerTGKzlkXoRZSjz0P3XlImONLwcr111dLujcgvSshN9M0hkScDzlrS8mFvFO8fjs3O3Ds3zn9y1BUOp
+YsdYuvexpV6KTD2ogGLFGxTaqhQwCFGvj8uK
+6lUzHWH8ZESzjDrOnXvOzG8XetD5sSqpRbv6+2fpQveefnNR78FB6RY4/FH2QyKwZSUIPbpnxWqEu0mpK0R78ILFRPdgIHkYjBWVrxoGAiwj8N4SDEj1Cc33EWOYyJEe2IWB6H8R8M7IVNral
2wmpk92XWavpLtn3zfs90XfOmYncw4zGWE8U1kaHdaol/dT4eHllkykLVup9CPs5SuoT6PpzXjJCj/7mDjZkrdGX7TsL69IV6qxc2p3drKzd0/Hh1Qzxpdk42hllFLYvt3d1flT8GwT0rrhAQFF/
2m7C7i62B60PZRTZeb3RjCv1PUeZD19fXoZdng1N8EE1u9ZwPWkZf3p+peXf02vPovbByKytgYwdWwx3zcBQL4P5sb88GJ/jtX2WtwgDXleWKBjR6+cYemd4iGj2lW6lcJwvvrK7bvV/4swxJjId
kuTkgNiKcCw8/PH9ksi78W/ZzbX/iHldB7PZn/18Axm
+FuV3mBfeEuI03QfT09vYeeFzqRfGaKa/Fci5C0krCSWTm5gX70EhdvnTEgNfmualR36hYaxqSl6mvFnLYFU6213oZeO7cjArXYq5E7K82HrihHWSwkZ0/zaV0fhsWzrpBiDKUrm1RgSH9nZ3E4hi
rJ+76hPlx7OivV+W2GhH96oyc+O+/OxJdJl7B3MNdod0LDRVCSCemyDvE4gRlhxXhUs90rThvikActEmw4rJX1D9gaVctiKK
+5GtOqVzUR0K7YvEQFZJg6OklnDjCROlZqq8q35bpKvVsudN7f26xTfRPNer11F3hYKwb0cugv
+VaXnZ4gRtaD1kg9/esNNTRqEo35winfrGj3K5EHhy6dQaWNxU88vYFF22wAp3Q1Vj0YFCR5fTbj6VzV9+qcc+VTBhvFepRXEa6fclh
+hJ3sOBONKie2eyBawgHbJtryZ8c3L43IQKqCqV76fBTa5JWu8Jp27ZyRU9UcZkoSv5Y2Uso7hcHNI41ZT0LHAGP7NyyT3VZdJLUDrF5rug0ZWVvyh/oBVum2NddhByexRkG8nVMqHX04u7
BKVZrhk1Gcb6h17iTk+mrP9IH20bQTMexsulNbq180u4xhkm7H6y/2s+WF/O/qTww/YiKVgrWpi1NYBH07YJQ7jii+Lrc5LmHTaDTyhtWPHH1t/Y96458ebNtqtqqlHjKsqRPaXim0IUv35xYj/b
+ip8AssdovMjXs0H2WQR/W57BCdRntBmieoahk8od9pL/YZduixFvs8c03cyhOnt22uGHVAn
+mkBzb9dS5ZLxLdunFxcXnZ3J5E5pnRy1tDAYNR4VD2eWP0eKmtu31EZQllavPv3rCFZiZWWSVlc6BctHhZeUvITVqriwWb4+EKAMKnS3X8UG8TV7cbVP7qRszkvbc5k2o5HTb7KbVImfGXL52l
nXuRfX06KmpX7/8sXXE97p5ZupNPENJ97ExvtoWmN5H533TOD/FistjV+cmyfaLWwk7GiR8uGnY60+48i3eJ8CmLD/rfpOZC7G1dbSRZ30ah+Xu3S

保存为压缩包后解压发现全是图片,看来又要拼图了





CSDN @~VAS~

