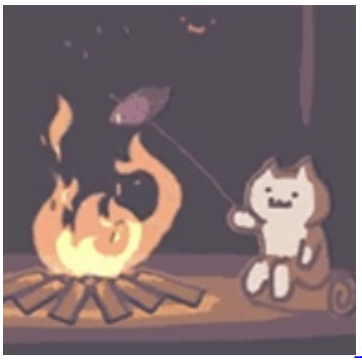
[西湖论剑2021中国杭州网络安全技能大赛]Yusa的秘密 writeup

原创

shu天 于 2021-11-21 13:00:00 发布 4552 收藏 1

分类专栏： ctf 文章标签： 西湖论剑 内存取证 Windows

本文链接：https://blog.csdn.net/weixin_46081055/article/details/121447445



[西湖论剑2021]Yusa的秘密

Sakura组织即将进攻地球，此时你意外得到了该组织内某个成员的电脑文件，你能从中发现本次阴谋所用的关键道具吗。

（注：题目中包含了五个彩蛋，且彩蛋对解题本身没有任何影响，快去发现吧！）

> 附件：Who_am_I.zip，Yusa-PC.raw

Yusa-PC.raw是内存镜像

首先pslist

```
.\volatility_2.6_win64_standalone.exe -f D:\download\Yusa的秘密\Yusa-PC.raw --profile=Win7SP1x64 pslist

Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
   Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ----------------------------
-- ------------------------------
0xfffffa80024bdae0 System                    4      0     97      598 ------      0 2021-10-28 03:46:58 UTC+0000

0xfffffa8002ecdb30 smss.exe                244      4      2       29 ------      0 2021-10-28 03:46:58 UTC+0000

0xfffffa8003950340 csrss.exe               336    320      9      483      0      0 2021-10-28 03:46:59 UTC+0000

0xfffffa8003adfb30 wininit.exe             388    320      3       77      0      0 2021-10-28 03:46:59 UTC+0000

0xfffffa8003ae15d0 csrss.exe               396    380     10      328      1      0 2021-10-28 03:46:59 UTC+0000

0xfffffa8003b008f0 winlogon.exe            432    380      5      118      1      0 2021-10-28 03:46:59 UTC+0000

0xfffffa8003b6e1d0 services.exe            488    388      7      212      0      0 2021-10-28 03:46:59 UTC+0000
```

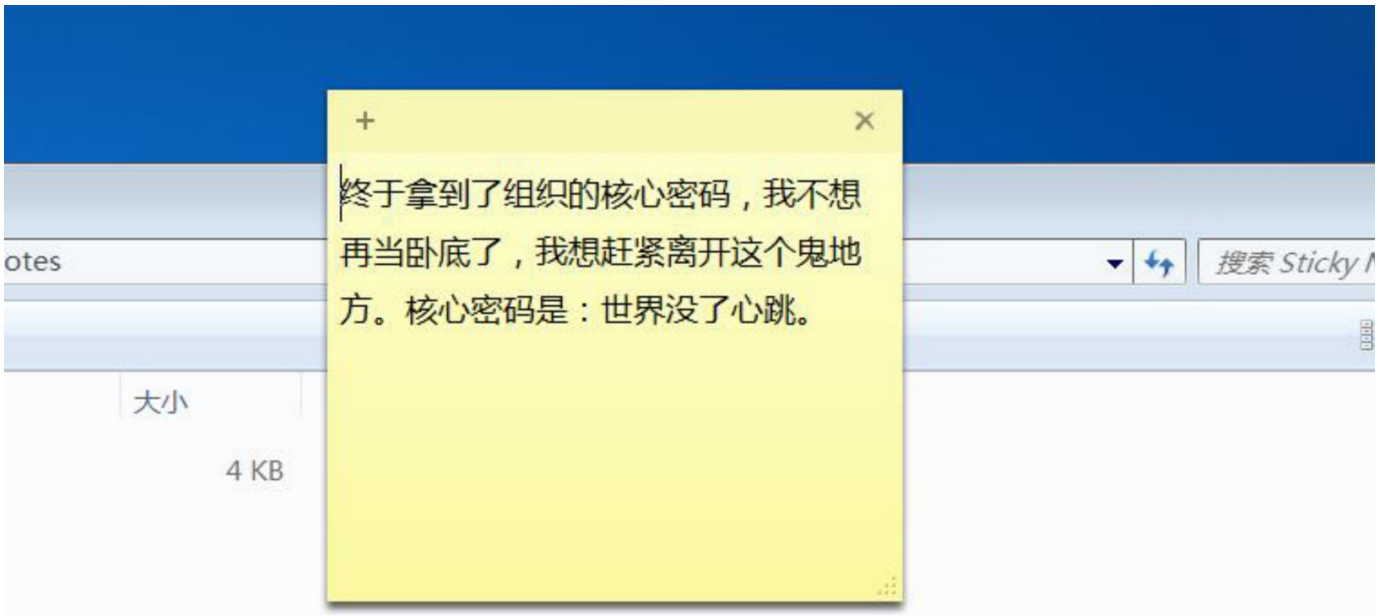
```
0xfffffa8003b04b30 lsass.exe              504    388      6      596      0      0 2021-10-28 03:46:59 UTC+0000
0xfffffa8003b03a10 lsm.exe                512    388     10      142      0      0 2021-10-28 03:46:59 UTC+0000
0xfffffa8003bfe9f0 svchost.exe            620    488     10      360      0      0 2021-10-28 03:47:00 UTC+0000
0xfffffa8003c1ab30 vmacthlp.exe           680    488      3       53      0      0 2021-10-28 03:47:00 UTC+0000
0xfffffa8003c46b30 svchost.exe            712    488      9      270      0      0 2021-10-28 03:47:00 UTC+0000
0xfffffa8003c763e0 svchost.exe            772    488     21      502      0      0 2021-10-28 03:47:00 UTC+0000
0xfffffa8003ca4b30 svchost.exe            856    488     16      375      0      0 2021-10-28 03:47:00 UTC+0000
0xfffffa8003cb5830 svchost.exe            884    488     41     1024      0      0 2021-10-28 03:47:00 UTC+0000
0xfffffa8003d703a0 svchost.exe            348    488     13      343      0      0 2021-10-28 03:47:01 UTC+0000
0xfffffa8003d9a6e0 svchost.exe            984    488     13      382      0      0 2021-10-28 03:47:01 UTC+0000
0xfffffa8003e34910 spoolsv.exe           1212    488     12      275      0      0 2021-10-28 03:47:01 UTC+0000
0xfffffa8003e49470 taskhost.exe          1244    488      9      227      1      0 2021-10-28 03:47:01 UTC+0000
0xfffffa8003e64b30 svchost.exe           1272    488     17      332      0      0 2021-10-28 03:47:01 UTC+0000
0xfffffa8003f16630 svchost.exe           1408    488     15      239      0      0 2021-10-28 03:47:02 UTC+0000
0xfffffa8003f57b30 VGAuthService.        1468    488      3       86      0      0 2021-10-28 03:47:02 UTC+0000
0xfffffa8003f8f060 vmtoolsd.exe          1520    488     10      269      0      0 2021-10-28 03:47:02 UTC+0000
0xfffffa8004077b30 sppsvc.exe            1736    488      4      157      0      0 2021-10-28 03:47:02 UTC+0000
0xfffffa80040af890 svchost.exe           1836    488      6       93      0      0 2021-10-28 03:47:03 UTC+0000
0xfffffa80040b3560 WmiPrvSE.exe          1908    620     10      214      0      0 2021-10-28 03:47:03 UTC+0000
0xfffffa8004112520 msdtc.exe              308    488     12      144      0      0 2021-10-28 03:47:05 UTC+0000
0xfffffa8003e55810 dwm.exe               2260    856      5      243      1      0 2021-10-28 03:47:08 UTC+0000
0xfffffa8003ddeb30 explorer.exe          2276   2252     45     1400      1      0 2021-10-28 03:47:08 UTC+0000
0xfffffa80042804b0 vmtoolsd.exe          2380   2276      8      220      1      0 2021-10-28 03:47:09 UTC+0000
0xfffffa8004322890 SearchIndexer.        2552    488     13      796      0      0 2021-10-28 03:47:13 UTC+0000
0xfffffa8002954b30 svchost.exe           1232    488     13      323      0      0 2021-10-28 03:49:04 UTC+0000
0xfffffa80030cb260 wmpnetwk.exe          2792    488      9      221      0      0 2021-10-28 03:49:04 UTC+0000
0xfffffa8003c8b460 StikyNot.exe          2228   2276      8      210      1      0 2021-10-28 10:37:08 UTC+0000
0xfffffa8003ad2b30 taskhost.exe          2160    488      5      101      1      0 2021-10-29 04:10:23 UTC+0000
0xfffffa8003cca750 cmd.exe               2536   2276      1       19      1      0 2021-10-29 04:15:14 UTC+0000
0xfffffa8003b1d920 conhost.exe           1344    396      2       58      1      0 2021-10-29 04:15:14 UTC+0000
```

```
0xfffffa8002b49060 audiodg.exe            2744    772      6      141      0      0 2021-10-29 05:42:04 UTC+0000
0xfffffa800282e590 dllhost.exe            1168    620     28      354      1      0 2021-10-29 05:42:32 UTC+0000
0xfffffa8002d0a920 wab.exe                2448    820      8      154      1      0 2021-10-29 05:43:20 UTC+0000
0xfffffa80028b2b30 DumpIt.exe              820   2276      1       25      1      1 2021-10-29 05:43:42 UTC+0000
0xfffffa8003042b30 conhost.exe            1356    396      2       59      1      0 2021-10-29 05:43:42 UTC+0000
0xfffffa8002841060 dllhost.exe            1000    620      6  7536754      1      0 2021-10-29 05:44:04 UTC+0000
```

可疑进程有 wab.exe （Windows联系人），StikyNot.exe（便笺）
filescan+filedump导出

StikyNot.exe–导出便笺数据库（StickyNotes.snt），在自己虚拟机上恢复

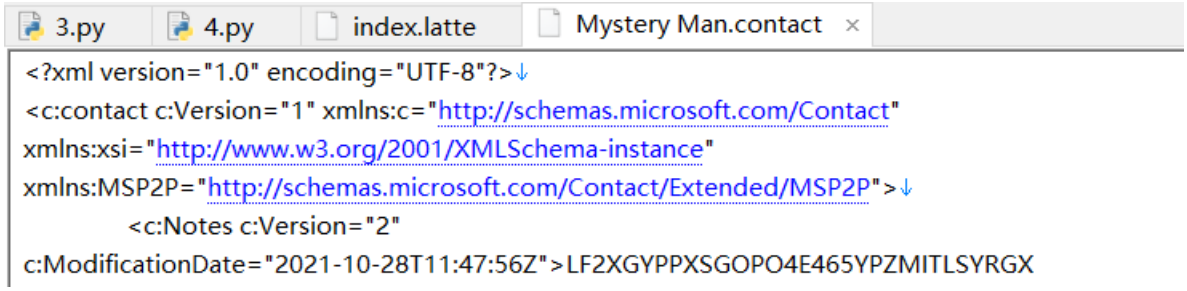
```
0x000000003fb306e0     16      1 RW-r-- \Device\HarddiskVolume2\Users\Yusa\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt
```



CSDN @shu天

得到密码–世界没了心跳

wab.exe–导出联系人数据库（有两个Mystery Man.contact、yusa.contact）
Mystery Man.contact里面有东西
我直接打开失败了，所以解密data



GWS7OJOEL42O2LZFYQDSLRKXEXO56LCVB566IZ2FPW7S37K7HQK46LLUM42EJB354RT
SL3IHFR6VONHEJ4S4ITZNEVHTJPNXJS62OHAECGZGCWWRVOBUXMNKMGJTTKTDZME
2TKU3PGVMWS5ZVGVYUKYJSKY2TON3ZJU2VSK3WGVGHK3BVGVJW6NLBGZCDK33NK
Q2WE6KBGU3XKRJVG52UQNJXOVNDKTBSM42TK4KFGVRGK3BVLFLTGNBUINBTKYTFNQ
2VSVZTGVNEOOJVLJBU4NKMGZSDKNCXNY2UY4KHGVGHSZZVG52WMNSLMVCTKWLJL
I2DIQ2DMEZFMNJXG54WCT2EJF3VSV2NGVGW2SJVLJVFKNCNKRIXSWLNJJUVS6SJGNM
TERLZJ5KFM3KNK5HG2TSEM46Q====</c:Notes><c:CreationDate>2021-10-28T05:56:
31Z</c:CreationDate><c:Extended xsi:nil="true"/>↓
<c:ContactIDCollection><c:ContactID
c:ElementID="c81482a1-44bc-43bf-bfc0-159ab6a43962"><c:Value>176e8955-bc8e-48
8a-9cb2-b4fbffa547b3</c:Value></c:ContactID></c:ContactIDCollection><c:NameColl
ection><c:Name c:ElementID="86ef8fab-e13d-4b52-9cf5-ec0601898181"><c:Title>保
持神秘</c:Title><c:FormattedName>Mystery
Man</c:FormattedName><c:GivenName>Mystery
Man</c:GivenName></c:Name></c:NameCollection><c:PhotoCollection><c:Photo
c:ElementID="fdfaef8f-b334-4c80-813c-83d391488eb4"><c:Url c:Version="1"
c:ModificationDate="2021-10-28T06:06:09Z">C:\Users\Yusa\Desktop\QQ图片
20211028140534.jpg</c:Url><c:LabelCollection><c:Label>UserTile</c:Label></c:Labe
lCollection></c:Photo></c:PhotoCollection><c:PositionCollection c:Version="1"
c:ModificationDate="2021-10-28T06:21:33Z"><c:Position

<c:Notes c:Version="2" c:ModificationDate="2021-10-28T11:47:56Z">LF2XGYPPXSGOPO4E465YPZMITLSYRGXGWS7OJOEL42O2LZF
YQDSLRKXEXO56LCVB566IZ2FPW7S37K7HQK46LLUM42EJB354RTSL3IHFR6VONHEJ4S4ITZNEVHTJPNXJS62OHAECGZGCWWRVOBUXMNKMGJTTKTD
ZME2TKU3PGVMWS5ZVGVYUKYJSKY2TON3ZJU2VSK3WGVGHK3BVGVJW6NLBGZCDK33NKQ2WE6KBGU3XKRJVG52UQNJXOVNDKTBSM42TK4KFGVRGK3B
VLFLTGNBUINBTKYTFNQ2VSVZTGVNEOOJVLJBU4NKMGZSDKNCXNY2UY4KHGVGHSZZVG52WMNSLMVCTKWLJLI2DIQ2DMEZFMNJXG54WCT2EJF3VSV2
NGVGW2SJVLJVFKNCNKRIXSWLNJJUVS6SJGNMTERLZJ5KFM3KNK5HG2TSEM46Q====</c:Notes><c:CreationDate>2021-10-28T05:56:31Z<
/c:CreationDate><c:Extended xsi:nil="true"/>
<c:ContactIDCollection>

base36解密

LF2XGYPPXSGOPO4E465YPZMITLSYRGXGWS7OJOEL4202LZFYQDSLRKXEXO56LCVB566IZ2FPW7S37K7HQK46LLUM42EJB354RTSL3IHFR6VONHEJ4S4ITZN
EVHTJPNXJS62OHAECGZGCWWRVOBUXMNKMGJTTKTDZME2TKU3PGVMWS5ZVGVYUKYJSKY2TON3ZJU2VSK3WGVGHK3BVGVJW6NLBGZCDK33NKQ2WE6KBGU3XKR
JVG52UQNJXOVNDKTBSM42TK4KFGVRGK3BVLFLTGNBUINBTKYTFNQ2VSVZTGVNEOOJVLJBU4NKMGZSDKNCXNY2UY4KHGVGHSZZVG52WMNSLMVCTKWLJLI2DI
Q2DMEZFMNJXG54WCT2EJF3VSV2NGVGW2SJVLJVFKNCNKRIXSWLNJJUVS6SJGNMTERLZJ5KFM3KNK5HG2TSEM46Q====

编码 解码 清空

Yusa，组织刚刚派下来一个任务，请快点完成，你只有三天时间。
6L+Z5piv5L2g5Lya55So5Yiw55qEa2V577yM5Y+v5Lul55So5a6D5omT5byA57uE57uH57uZ5L2g55qE5bel5YW344CC5bel5YW3
5ZG95ZCN5L6d54Wn5LqG5Lyg57uf6KeE5YiZ44CCa2V577yaODIwYWM5MmI5ZjU4MTQyYmJiYzI3Y2EyOTVmMWNmNDg=

base64

请输入要进行 Base64 编码或解码的字符

6L+Z5piv5L2g5Lya55So5Yiw55qEa2V577yM5Y+v5Lul55So5a6D5omT5byA57uE57uH57uZ5L2g55qE5bel5YW344CC5bel5YW35ZG95ZC
N5L6d54Wn5LqG5Lyg57uf6KeE5YiZ44CCa2V577yaODIwYWM5MmI5ZjU4MTQyYmJiYzI3Y2EyOTVmMWNmNDg=

编码 (Encode) 解码 (Decode) ↕交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果: 编/解码后自动全选

这是你会用到的key，可以用它打开组织给你的工具。工具命名依照了传统规则。key：820ac92b9f58142bbbc27ca295f1cf48

key：820ac92b9f58142bbbc27ca295f1cf48

再看看filescan出来什么可疑文件

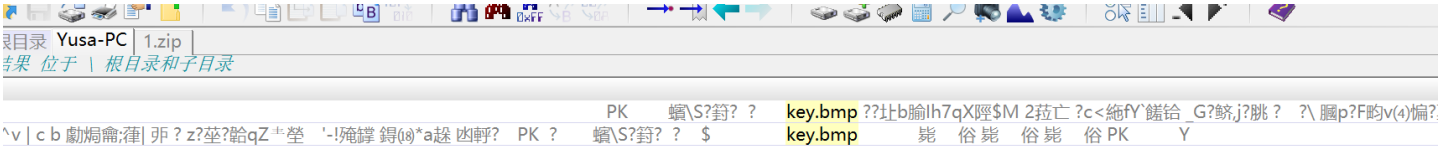
```
0x000000003f335070    15      0 R--r-- \Device\HarddiskVolume2\Program Files\Common Files\VMware\Drivers\video_wddm\\
0x000000003f3356f0    1       0 R--rw- \Device\HarddiskVolume2\PROGRA~1\MSBuild\MICROS~1\WINDOW~1\key.zip
```

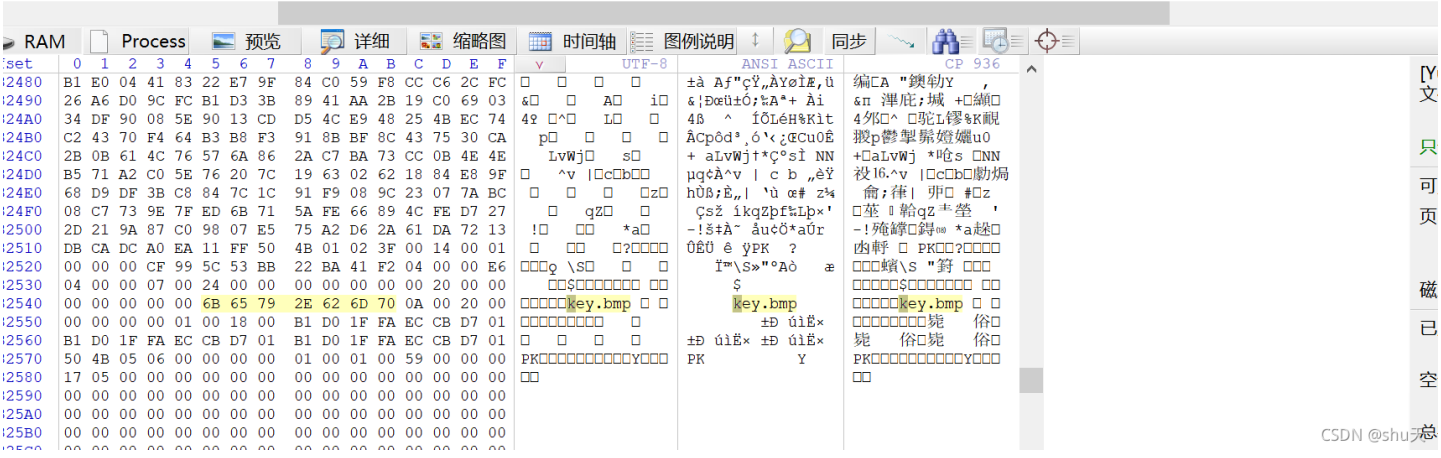
导出key.zip，用之前得到的密码**世界没了心跳**解密，得到一个exp

```python
from PIL import Image
import struct
pic = Image.open('key.bmp')
fp = open('flag', 'rb')
fs = open('Who_am_I', 'wb')

a, b = pic.size
list1 = []
for y in range(b):
    for x in range(a):
        pixel = pic.getpixel((x, y))
        list1.extend([pixel[1], pixel[0], pixel[2], pixel[2], pixel[1], pixel[0]])

data = fp.read()
for i in range(0, len(data)):
    fs.write(struct.pack('B', data[i] ^ list1[i % a*b*6]))
fp.close()
fs.close()
```

Who_am_I自然是联想到本机用户，密码：YusaYusa520，解密最开始附件里的压缩包，得到whoami

最后差一个key.bmp，filescan找不到，全盘搜索，发现是在压缩包里面，导出





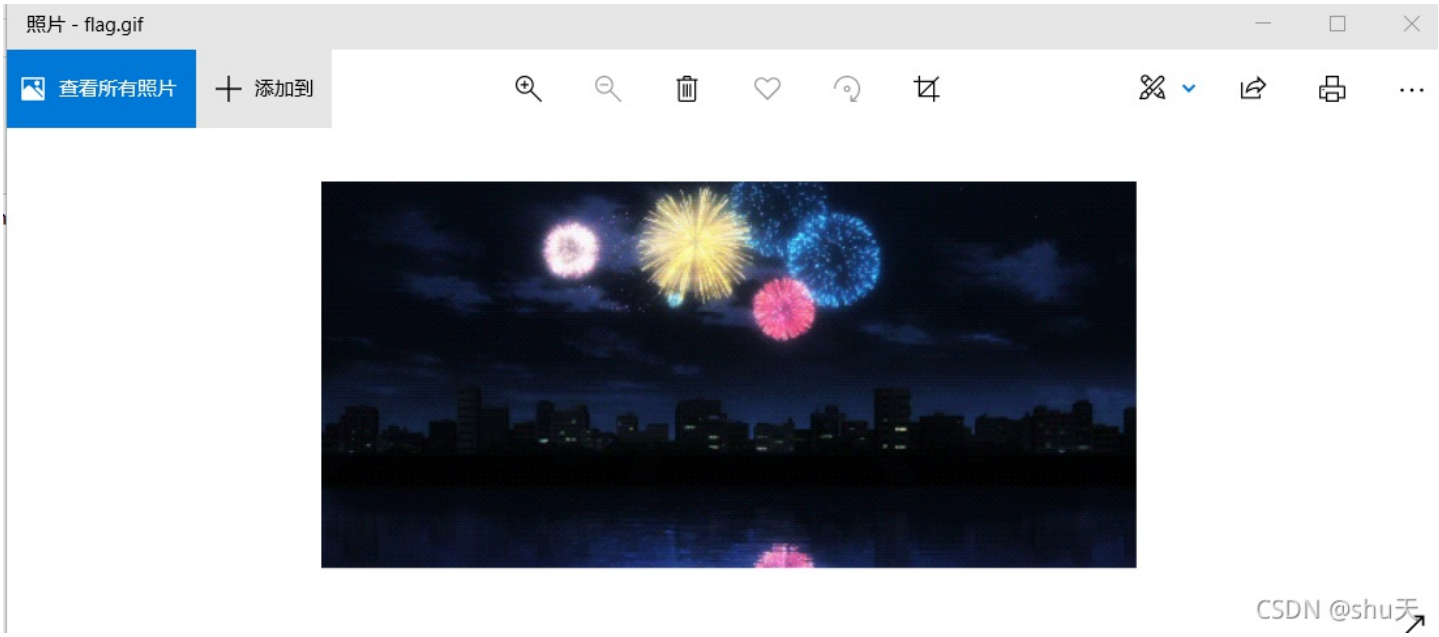
用key：820ac92b9f58142bbbc27ca295f1cf48，解压缩得到key.bmp

改一下脚本，异或得到flag.gif

```python
from PIL import Image
import struct
pic = Image.open('key.bmp')
fp = open('Who_am_I', 'rb')
fs = open('flag', 'wb')

a, b = pic.size
list1 = []
for y in range(b):
    for x in range(a):
        pixel = pic.getpixel((x, y))
        list1.extend([pixel[1], pixel[0], pixel[2], pixel[2], pixel[1], pixel[0]])

data = fp.read()
for i in range(0, len(data)):
    fs.write(struct.pack('B', data[i] ^ list1[i % a*b*6]))
fp.close()
fs.close()
```

flag是个gif

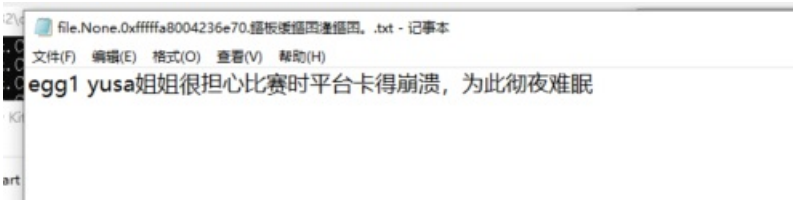
```
shen@DESKTOP-4R7ESOT:/mnt/d/download/Yusa的秘密$ file flag
flag: GIF image data, version 89a, 500 x 237
```



一帧一帧看，得到flag

eggs

egg1



egg4 cmdscan