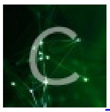
攻防世界misc新手区writeup

原创

^嘟_^ 于 2019-10-10 19:36:42 发布 574 收藏 3
分类专栏： ctf 文章标签： ctf 攻防世界 misc

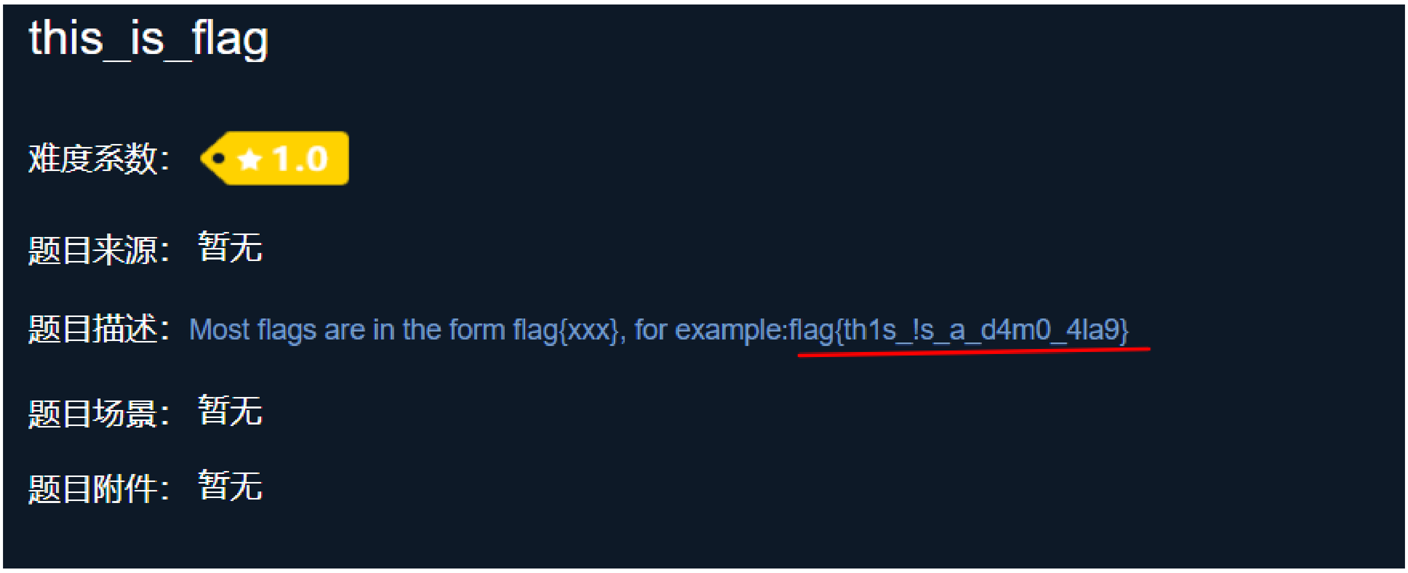
本文链接：https://blog.csdn.net/weixin_41217671/article/details/102489232
版权


ctf专栏收录该内容
2 篇文章 0 订阅
订阅专栏

```
title: 攻防世界misc新手区writeup
tags: ctf
categories: ctf
```

1.this_is_flag

标线即为flag值


this_is_flag

难度系数： ★1.0

题目来源： 暂无

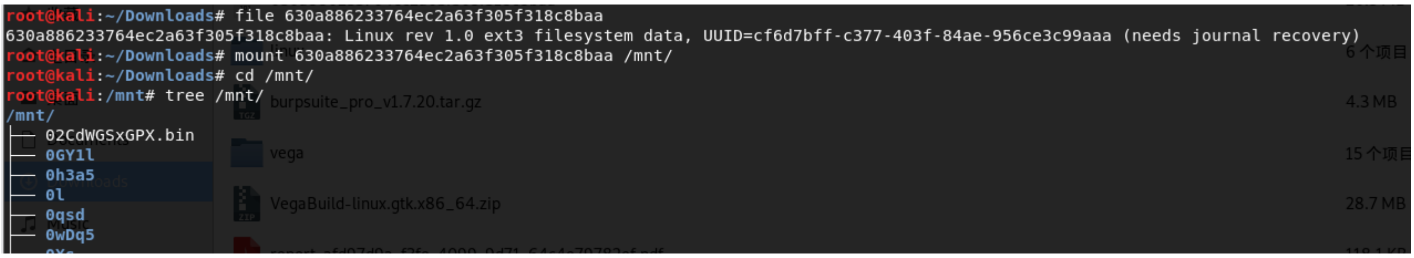
题目描述： Most flags are in the form flag{xxx}, for example:flag{th1s_!s_a_d4m0_4la9}

题目场景： 暂无

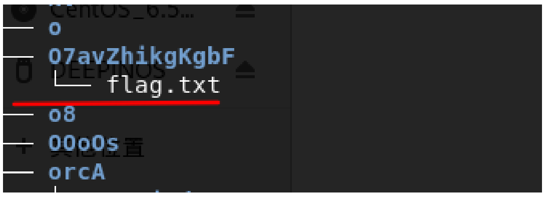
题目附件： 暂无

2.ext3

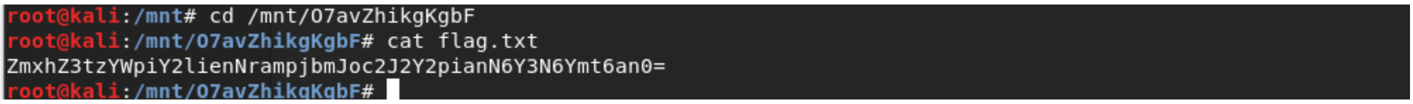
下载文件后放进linux，flie命令查看是什么文件，可以看到是磁盘文件，将其挂载


```
root@kali:~/Downloads# file 630a886233764ec2a63f305f318c8baa
630a886233764ec2a63f305f318c8baa: Linux rev 1.0 ext3 filesystem data, UUID=cf6d7bff-c377-403f-84ae-956ce3c99aaa (needs journal recovery)
root@kali:~/Downloads# mount 630a886233764ec2a63f305f318c8baa /mnt/
root@kali:~/Downloads# cd /mnt/
root@kali:/mnt# tree /mnt/
/mnt/
├── 02CdWGSxGPX.bin
├── 0GY1l
├── 0h3a5
├── 0l
├── 0qsd
├── 0wDq5
```

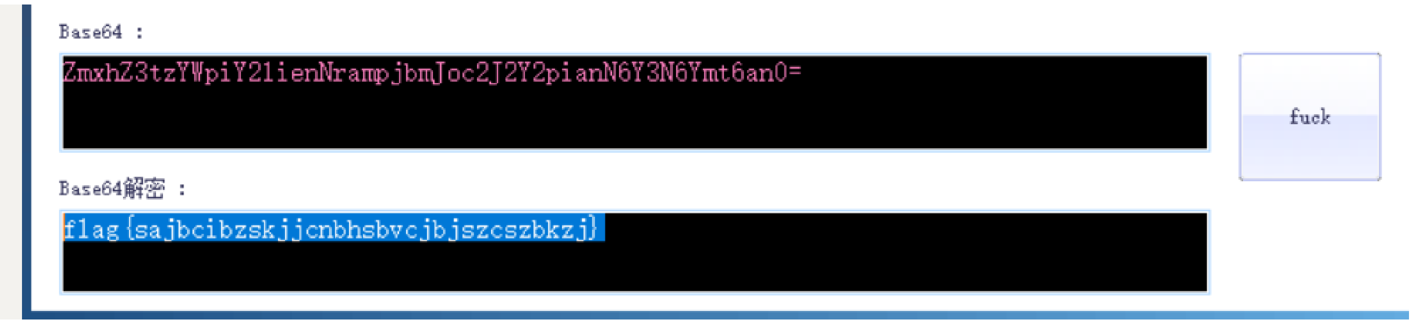
可以查看flag文本文件，cat查看得base64的编码，进行转换得flag值



```
├─ o
├─ 07avZhikgKgbF
│  └── flag.txt
├─ o8
├─ 0OoOs
└─ orcA
```



```
root@kali:/mnt# cd /mnt/07avZhikgKgbF
root@kali:/mnt/07avZhikgKgbF# cat flag.txt
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=
root@kali:/mnt/07avZhikgKgbF#
```



Base64 :

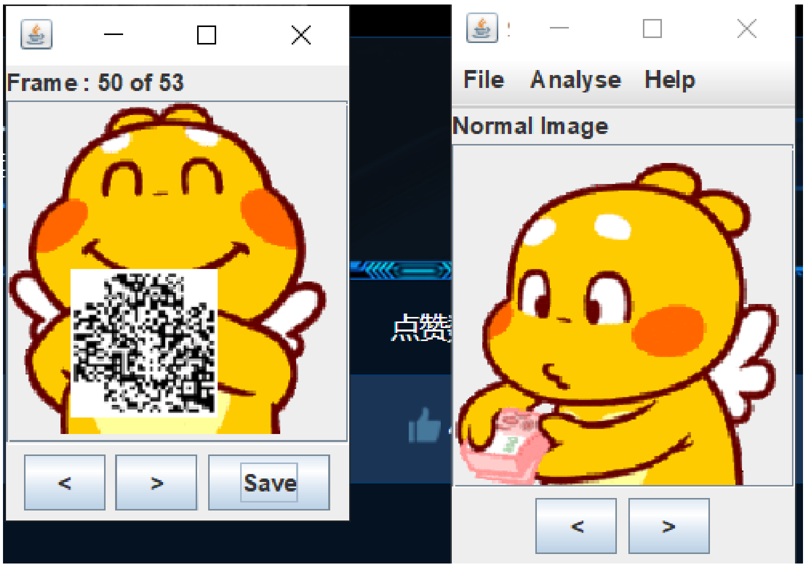
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

Base64解密 :

flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

3.give_you_flag

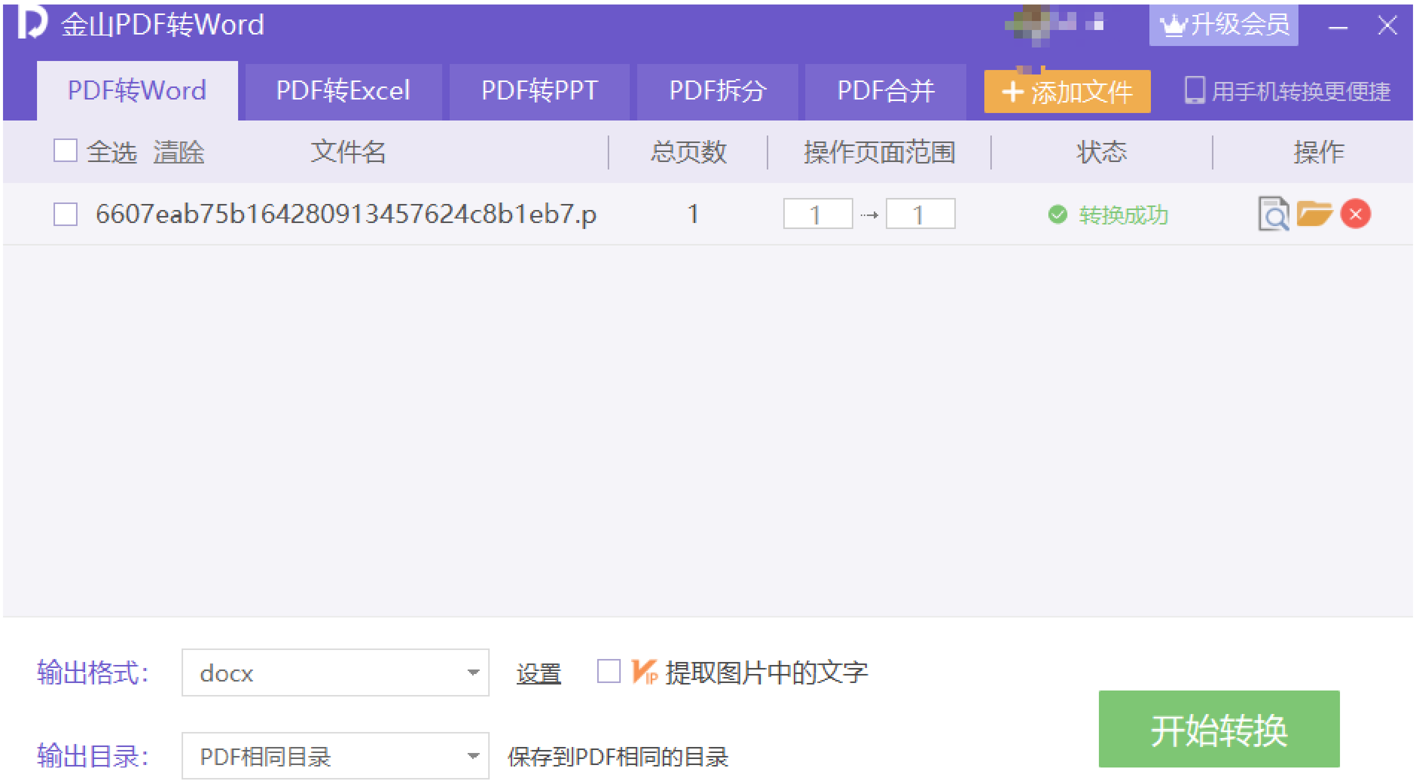
下载后是一张gif有一副二维码的图片，用Stegsolve保存二维码的图片



用ps软件修复二维码图片，二维码扫出来即为flag值

4.pdf

下载后是一个pdf文件，将pdf转换word文件，我这里用wps自带转换

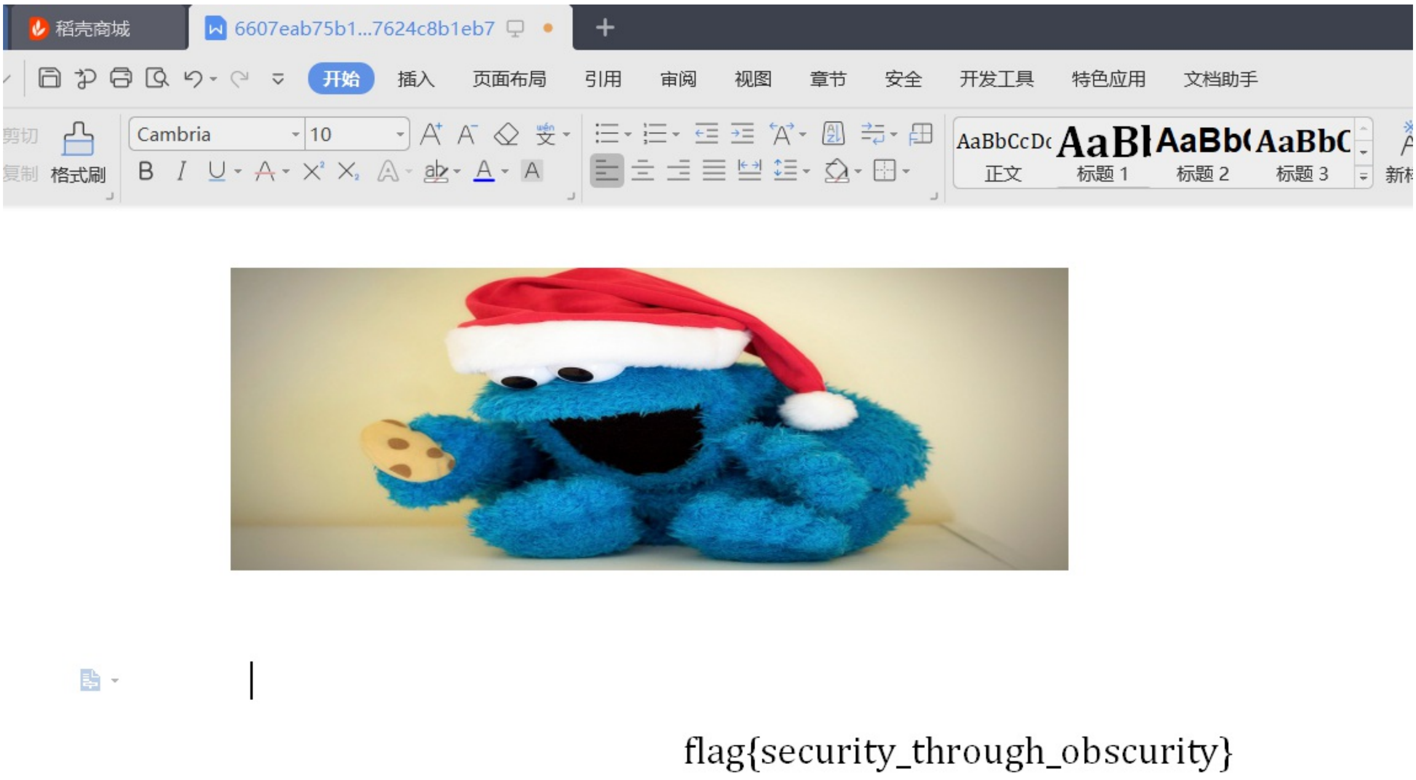


□ 全选 清除 文件名	总页数	操作页面范围	状态	操作
□ 6607eab75b164280913457624c8b1eb7.p	1	1 → 1	转换成功	

输出格式: docx 设置 □ 提取图片中的文字

输出目录: PDF相同目录 保存到PDF相同的目录

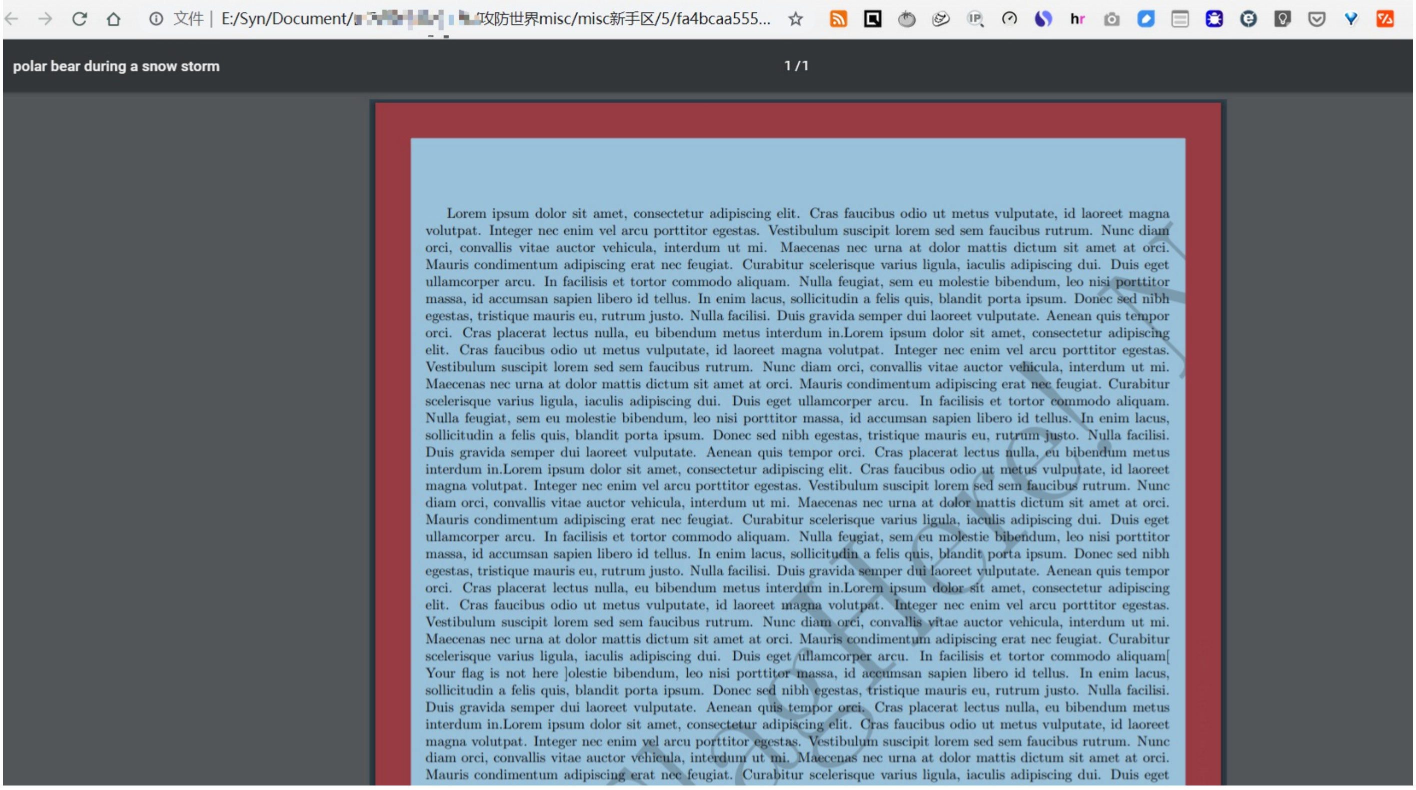
打开转换的word，删除图片或移动缩小图片，即可看见图片下藏着flag值



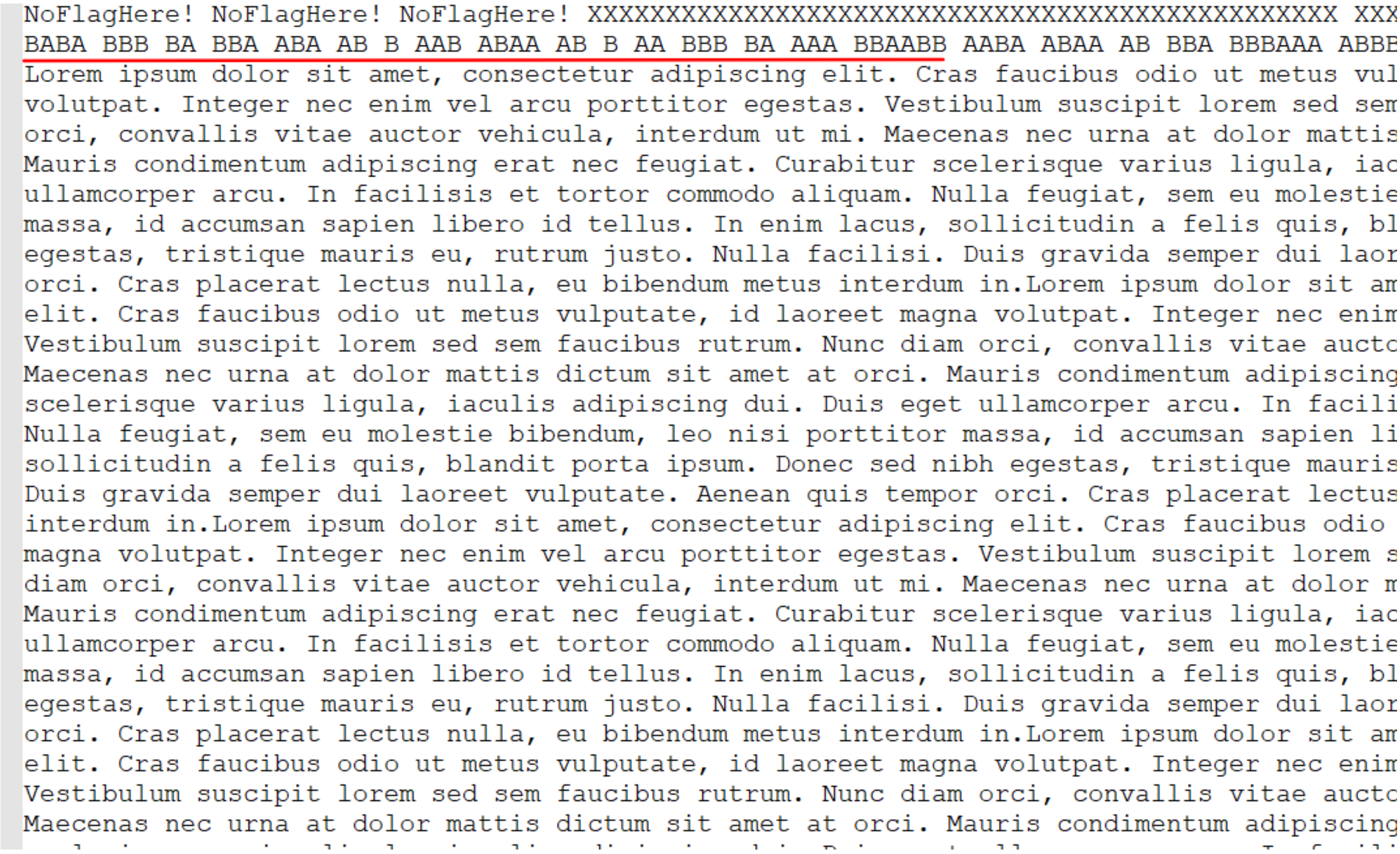
flag{security_through_obscurity}

5.stegano

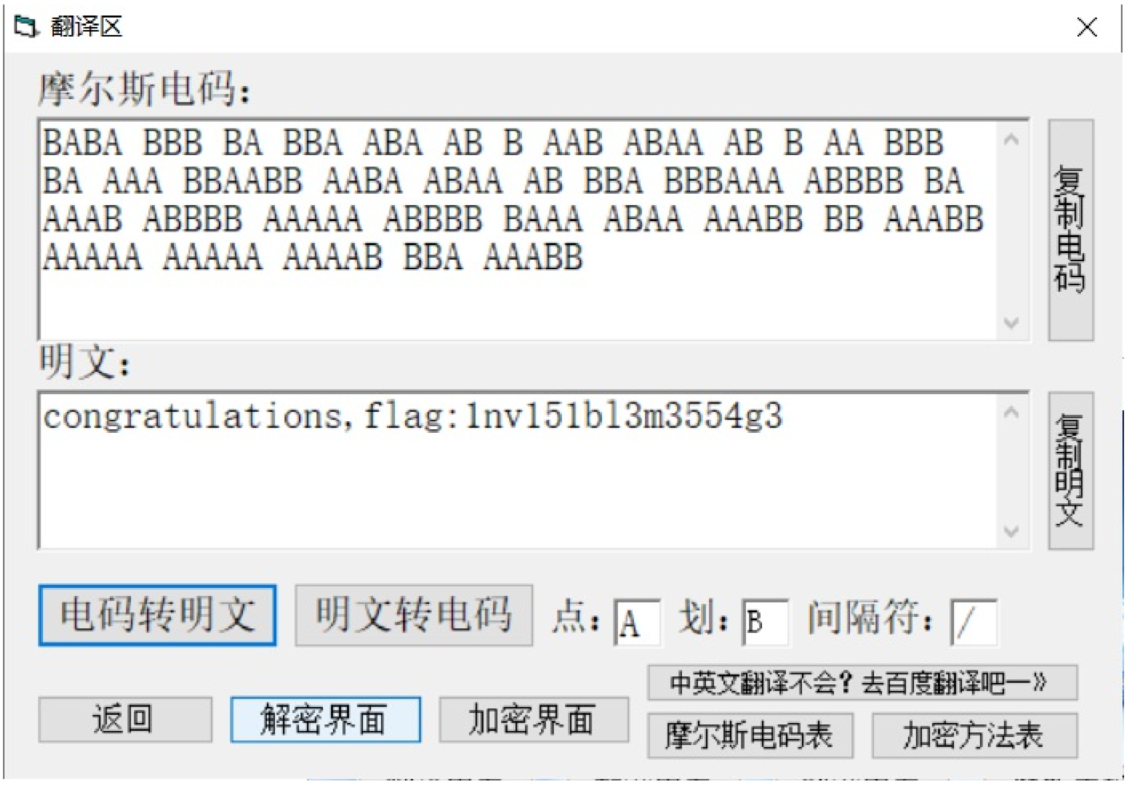
将pdf用浏览器打开选择全选，复制到记事本里去，可以发现AABB的一段文字，是摩斯电码，A是点，B是划 等到-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .---- -... .-.. ...-- -- ...-- ....- --. ...--转化成字母即为flag


文件 | E:/Syn/Document/[redacted]攻防世界misc/misc新手区/5/fa4bcaa555...
polar bear during a snow storm
1 / 1
Here!

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam[Your flag is not here]olestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget



```
NoFlagHere! NoFlagHere! NoFlagHere! XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXX
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBE
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vul
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iac
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, bl
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit am
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae aucto
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing
scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facili
Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien li
sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris
Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus
interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio
magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem s
diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor m
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iac
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, bl
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit am
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae aucto
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing
```



摩尔斯电码:

BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB

明文:

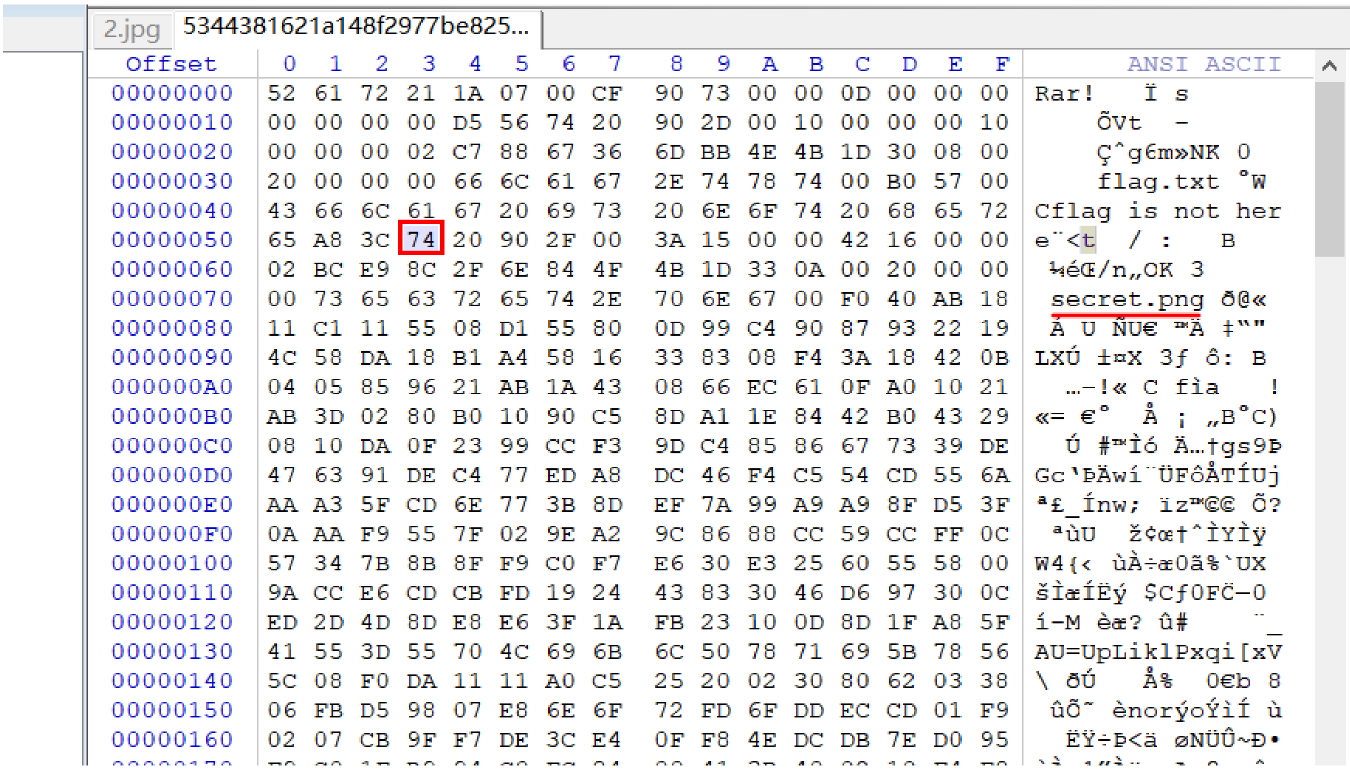
congratulations,flag:1nv151bl3m3554g3

点: A 划: B 间隔符: /

flag格式是flag{1nv151bl3m3554g3}

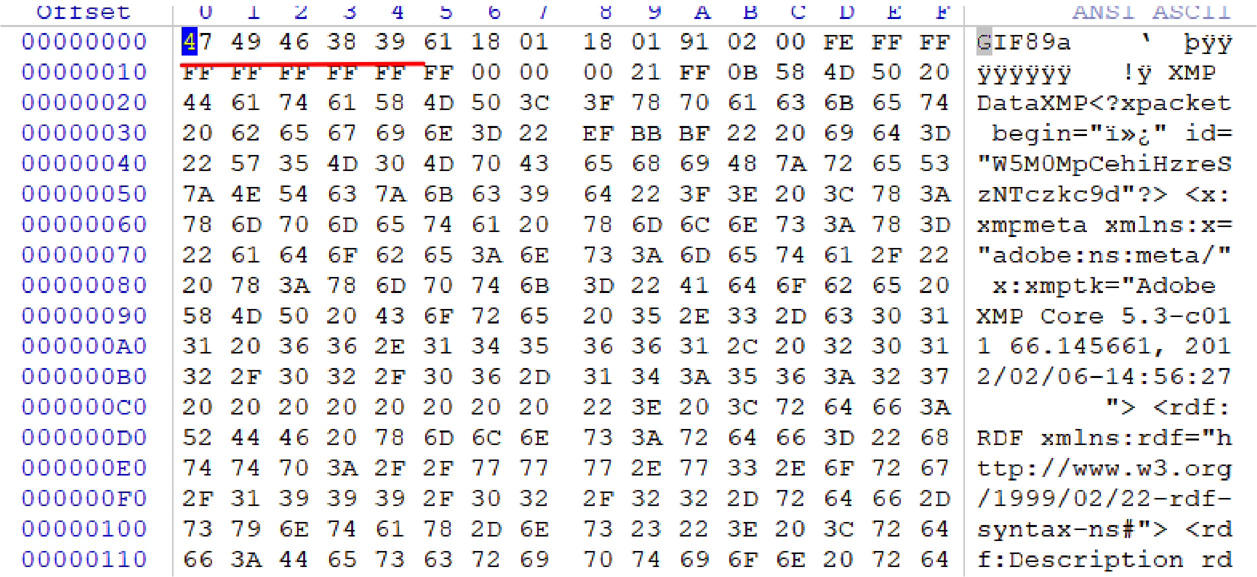
6.SimpleRAR

下载后是一个压缩包，用winhex查看一下，可以secret.png文件，把A8 3C 7A修改为A8 3C 74,这个是RAR对png文件头的编码.解压可以看到一张png图片，显示空白



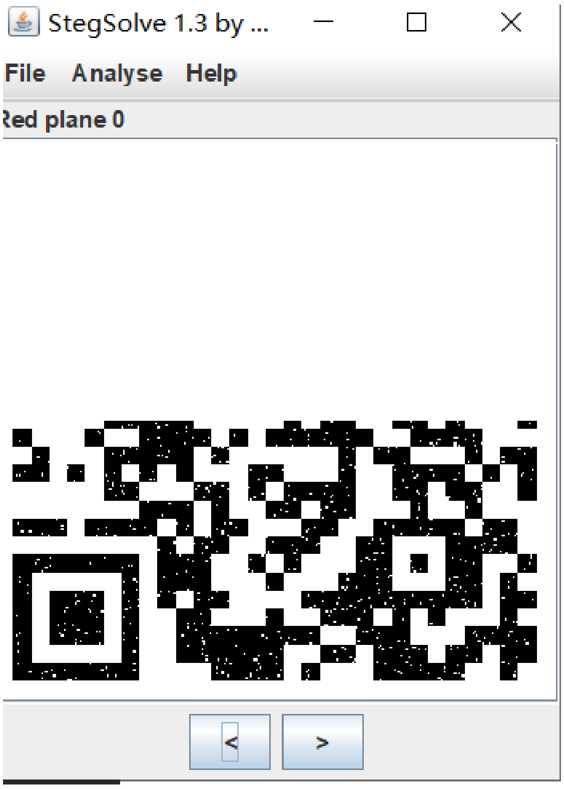
```
2.jpg   5344381621a148f2977be825...

  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   52 61 72 21 1A 07 00 CF  90 73 00 00 0D 00 00 00  Rar!   Ï s
00000010   00 00 00 00 D5 56 74 20  90 2D 00 10 00 00 00 10      ÕVt  -
00000020   00 00 00 02 C7 88 67 36  6D BB 4E 4B 1D 30 08 00      Çˆg6m»NK 0
00000030   20 00 00 00 66 6C 61 67  2E 74 78 74 00 B0 57 00      flag.txt °W
00000040   43 66 6C 61 67 20 69 73  20 6E 6F 74 20 68 65 72  Cflag is not her
00000050   65 A8 3C 74 20 90 2F 00  3A 15 00 00 42 16 00 00  e¨<t  / :   B
00000060   02 BC E9 8C 2F 6E 84 4F  4B 1D 33 0A 00 20 00 00   ¼éŒ/n„OK 3
00000070   00 73 65 63 72 65 74 2E  70 6E 67 00 F0 40 AB 18   secret.png ð@«
00000080   11 C1 11 55 08 D1 55 80  0D 99 C4 90 87 93 22 19   Á U ÑU€ ™Ä ‡“"
00000090   4C 58 DA 18 B1 A4 58 16  33 83 08 F4 3A 18 42 0B  LXÚ ±¤X 3ƒ ô: B
000000A0   04 05 85 96 21 AB 1A 43  08 66 EC 61 0F A0 10 21    …–!« C fìa    !
000000B0   AB 3D 02 80 B0 10 90 C5  8D A1 1E 84 42 B0 43 29  «= €°  Å ¡ „B°C)
000000C0   08 10 DA 0F 23 99 CC F3  9D C4 85 86 67 73 39 DE    Ú #™Ìó Ä…†gs9Þ
000000D0   47 63 91 DE C4 77 ED A8  DC 46 F4 C5 54 CD 55 6A  Gc‘ÞÄwí¨ÜFôÅTÍUj
000000E0   AA A3 5F CD 6E 77 3B 8D  EF 7A 99 A9 A9 8F D5 3F  ª£_Ínw; ïz™©© Õ?
000000F0   0A AA F9 55 7F 02 9E A2  9C 86 88 CC 59 CC FF 0C   ªùU  ž¢œ†ˆÌYÌÿ
00000100   57 34 7B 8B 8F F9 C0 F7  E6 30 E3 25 60 55 58 00  W4{‹ ùÀ÷æ0ã%`UX
00000110   9A CC E6 CD CB FD 19 24  43 83 30 46 D6 97 30 0C  šÌæÍËý $Cƒ0FÖ—0
00000120   ED 2D 4D 8D E8 E6 3F 1A  FB 23 10 0D 8D 1F A8 5F  í-M èæ? û#     ¨_
00000130   41 55 3D 55 70 4C 69 6B  6C 50 78 71 69 5B 78 56  AU=UpLiklPxqi[xV
00000140   5C 08 F0 DA 11 11 A0 C5  25 20 02 30 80 62 03 38  \ ðÚ   Å%  0€b 8
00000150   06 FB D5 98 07 E8 6E 6F  72 FD 6F DD EC CD 01 F9   ûÕ˜ ènorýoÝìÍ ù
00000160   02 07 CB 9F F7 DE 3C E4  0F F8 4E DC DB 7E D0 95    ËŸ÷Þ<ä øNÜÛ~Ð•
```

再用winhex打开png图片，可以看到GIF文件头，GIF (gif)，文件头：47494638，把png文件格式改为gif

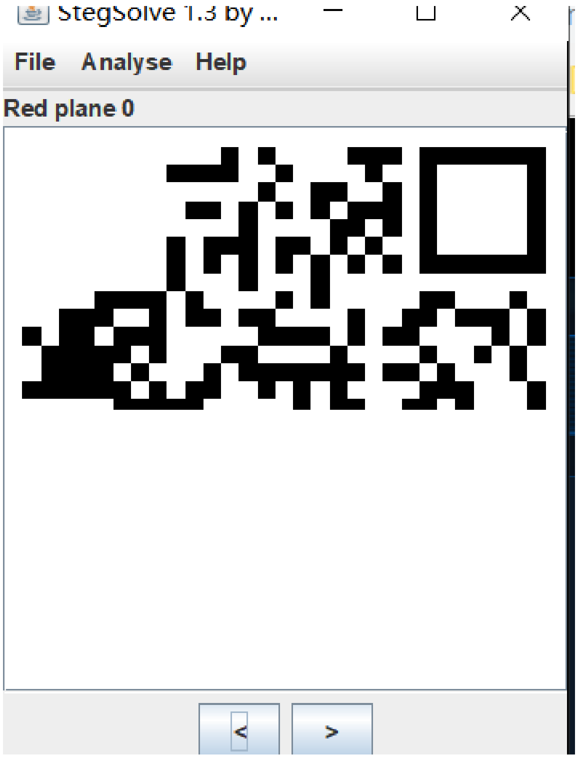


```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   47 49 46 38 39 61 18 01  18 01 91 02 00 FE FF FF  GIF89a  ‘  þÿÿ
00000010   FF FF FF FF FF FF 00 00  00 21 FF 0B 58 4D 50 20  ÿÿÿÿÿÿ   !ÿ XMP
00000020   44 61 74 61 58 4D 50 3C  3F 78 70 61 63 6B 65 74  DataXMP<?xpacket
00000030   20 62 65 67 69 6E 3D 22  EF BB BF 22 20 69 64 3D   begin="ï»¿" id=
00000040   22 57 35 4D 30 4D 70 43  65 68 69 48 7A 72 65 53  "W5M0MpCehiHzreS
00000050   7A 4E 54 63 7A 6B 63 39  64 22 3F 3E 20 3C 78 3A  zNTczkc9d"?> <x:
00000060   78 6D 70 6D 65 74 61 20  78 6D 6C 6E 73 3A 78 3D  xmpmeta xmlns:x=
00000070   22 61 64 6F 62 65 3A 6E  73 3A 6D 65 74 61 2F 22  "adobe:ns:meta/"
00000080   20 78 3A 78 6D 70 74 6B  3D 22 41 64 6F 62 65 20   x:xmptk="Adobe
00000090   58 4D 50 20 43 6F 72 65  20 35 2E 33 2D 63 30 31  XMP Core 5.3-c01
000000A0   31 20 36 36 2E 31 34 35  36 36 31 2C 20 32 30 31  1 66.145661, 201
000000B0   32 2F 30 32 2F 30 36 2D  31 34 3A 35 36 3A 32 37  2/02/06-14:56:27
000000C0   20 20 20 20 20 20 20 20  22 3E 20 3C 72 64 66 3A          "> <rdf:
000000D0   52 44 46 20 78 6D 6C 6E  73 3A 72 64 66 3D 22 68  RDF xmlns:rdf="h
000000E0   74 74 70 3A 2F 2F 77 77  77 2E 77 33 2E 6F 72 67  ttp://www.w3.org
000000F0   2F 31 39 39 39 2F 30 32  2F 32 32 2D 72 64 66 2D  /1999/02/22-rdf-
00000100   73 79 6E 74 61 78 2D 6E  73 23 22 3E 20 3C 72 64  syntax-ns#"> <rd
00000110   66 3A 44 65 73 63 72 69  70 74 69 6F 6E 20 72 64  f:Description rd
```

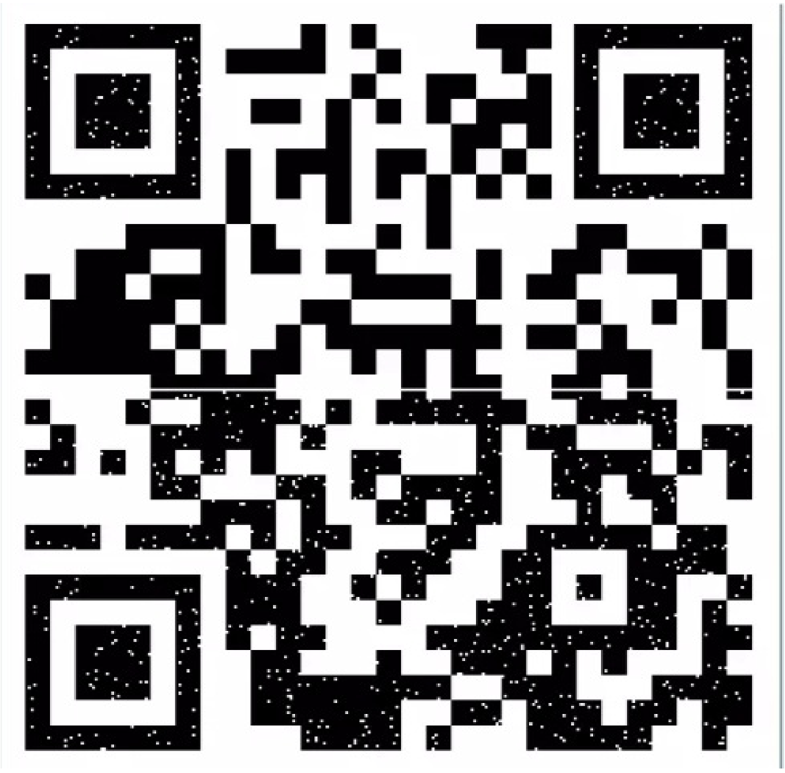
把gif发到stesolve跑一下，只弄出来一半。



再把gif丢进ps里，是两个图层的，导出另一图层的一张，再丢进stegsolve跑下，跑出二维码破碎的上部分

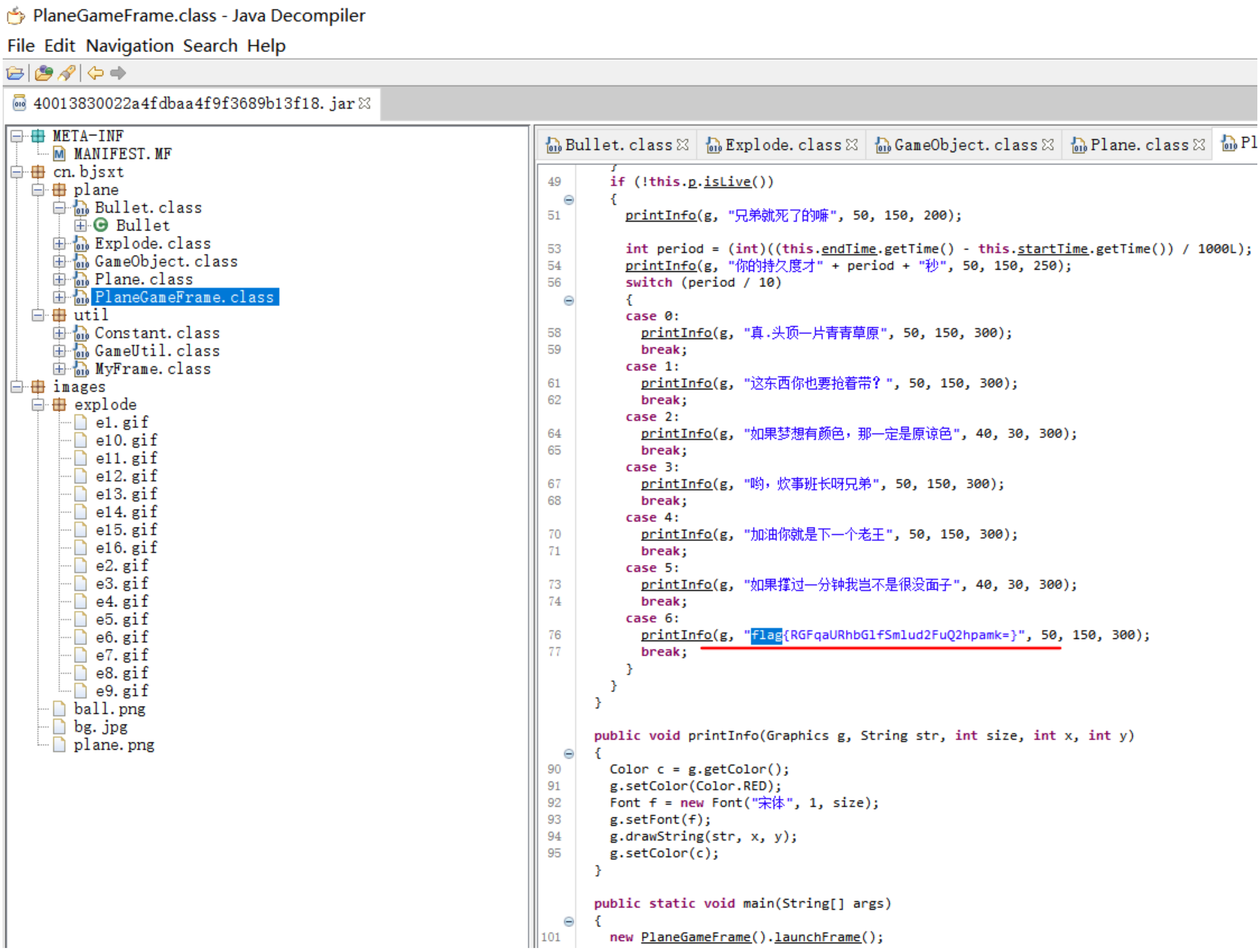


再报这两张图片丢进ps，ps修复一下，flag{yanji4n_bu_we1shi}



7.坚持60s

用jd-gui 打开下载的java程序，搜索关键字flag，得到是base64编码进行转化



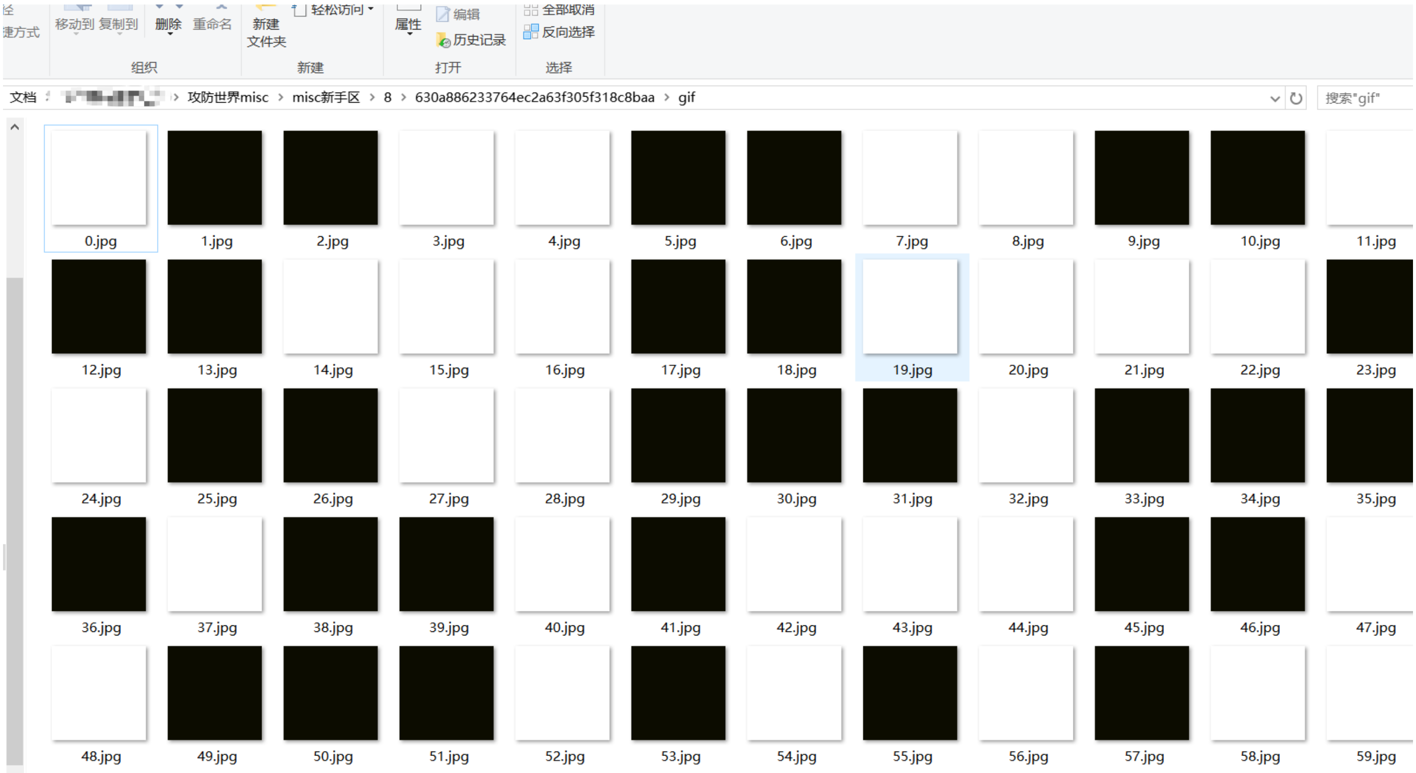
PlaneGameFrame.class - Java Decompiler
File Edit Navigation Search Help
40013830022a4fdbaa4f9f3689b13f18.jar
Bullet.class
Explode.class
GameObject.class
Plane.class
Pl

```
META-INF
  MANIFEST.MF
cn.bjsxt
  plane
    Bullet.class
      Bullet
    Explode.class
    GameObject.class
    Plane.class
    PlaneGameFrame.class
  util
    Constant.class
    GameUtil.class
    MyFrame.class
images
  explode
    e1.gif
    e10.gif
    e11.gif
    e12.gif
    e13.gif
    e14.gif
    e15.gif
    e16.gif
    e2.gif
    e3.gif
    e4.gif
    e5.gif
    e6.gif
    e7.gif
    e8.gif
    e9.gif
  ball.png
  bg.jpg
  plane.png
```

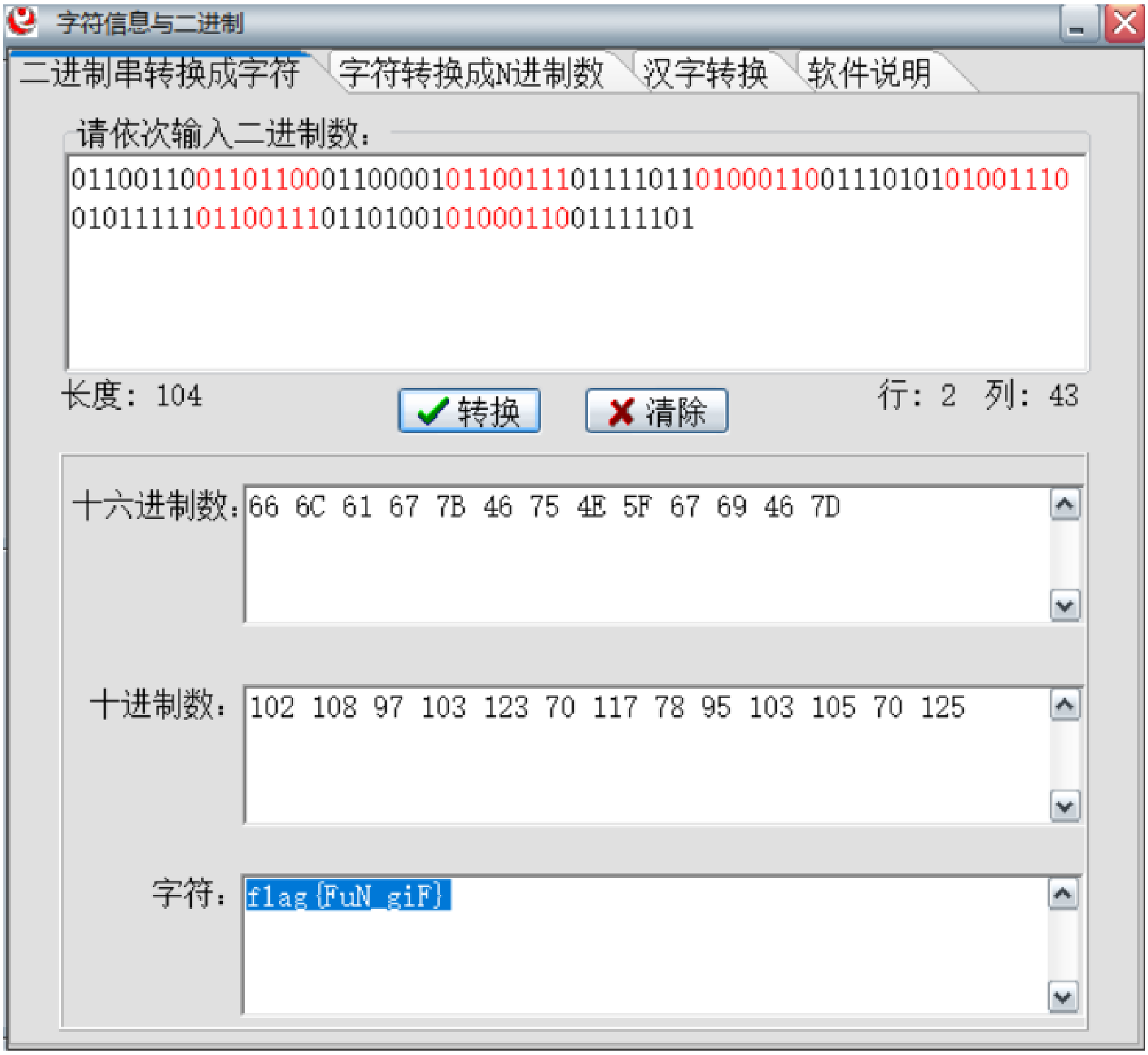
```
    if (!this.p.isLive())
    {
      printInfo(g, "兄弟就死了的嘛", 50, 150, 200);

      int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
      printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);
      switch (period / 10)
      {
      case 0:
        printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
        break;
      case 1:
        printInfo(g, "这东西你也要抢着带？", 50, 150, 300);
        break;
      case 2:
        printInfo(g, "如果梦想有颜色，那一定是原谅色", 40, 30, 300);
        break;
      case 3:
        printInfo(g, "哟，炊事班长呀兄弟", 50, 150, 300);
        break;
      case 4:
        printInfo(g, "加油你就是下一个老王", 50, 150, 300);
        break;
      case 5:
        printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
        break;
      case 6:
        printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
        break;
      }
    }
  }

  public void printInfo(Graphics g, String str, int size, int x, int y)
  {
    Color c = g.getColor();
    g.setColor(Color.RED);
    Font f = new Font("宋体", 1, size);
    g.setFont(f);
    g.drawString(str, x, y);
    g.setColor(c);
  }

  public static void main(String[] args)
  {
    new PlaneGameFrame().launchFrame();
```

8.gif

下载是个压缩包，进行解压时一堆黑白的图片，可以联想二进制，白是0，黑是1二进制转换成字符串，得flag值



文档 › [redacted] › 攻防世界misc › misc新手区 › 8 › 630a886233764ec2a63f305f318c8baa › gif



请依次输入二进制数：

```
0110011001101100011000010110011101111011010001100111010101001110
0101111101100111011010010100011001111101
```

长度：104

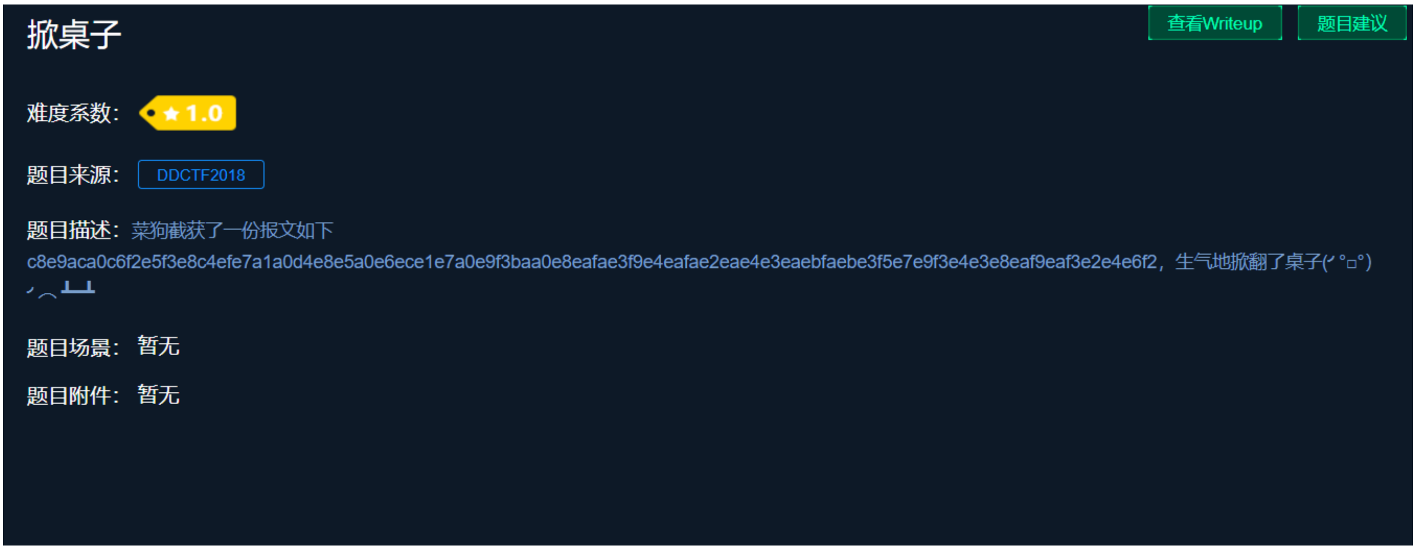
行：2　列：43

十六进制数：66 6C 61 67 7B 46 75 4E 5F 67 69 46 7D

十进制数：102 108 97 103 123 70 117 78 95 103 105 70 125

字符：flag{FuN_giF}

9.掀桌子



掀桌子

难度系数： ★ 1.0

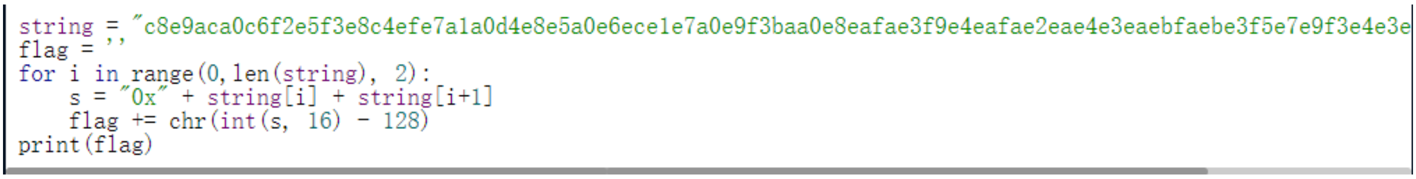
题目来源： DDCTF2018

题目描述：菜狗截获了一份报文如下
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2，生气地掀翻了桌子(╯°□°）╯︵ ┻━┻

题目场景： 暂无

题目附件： 暂无

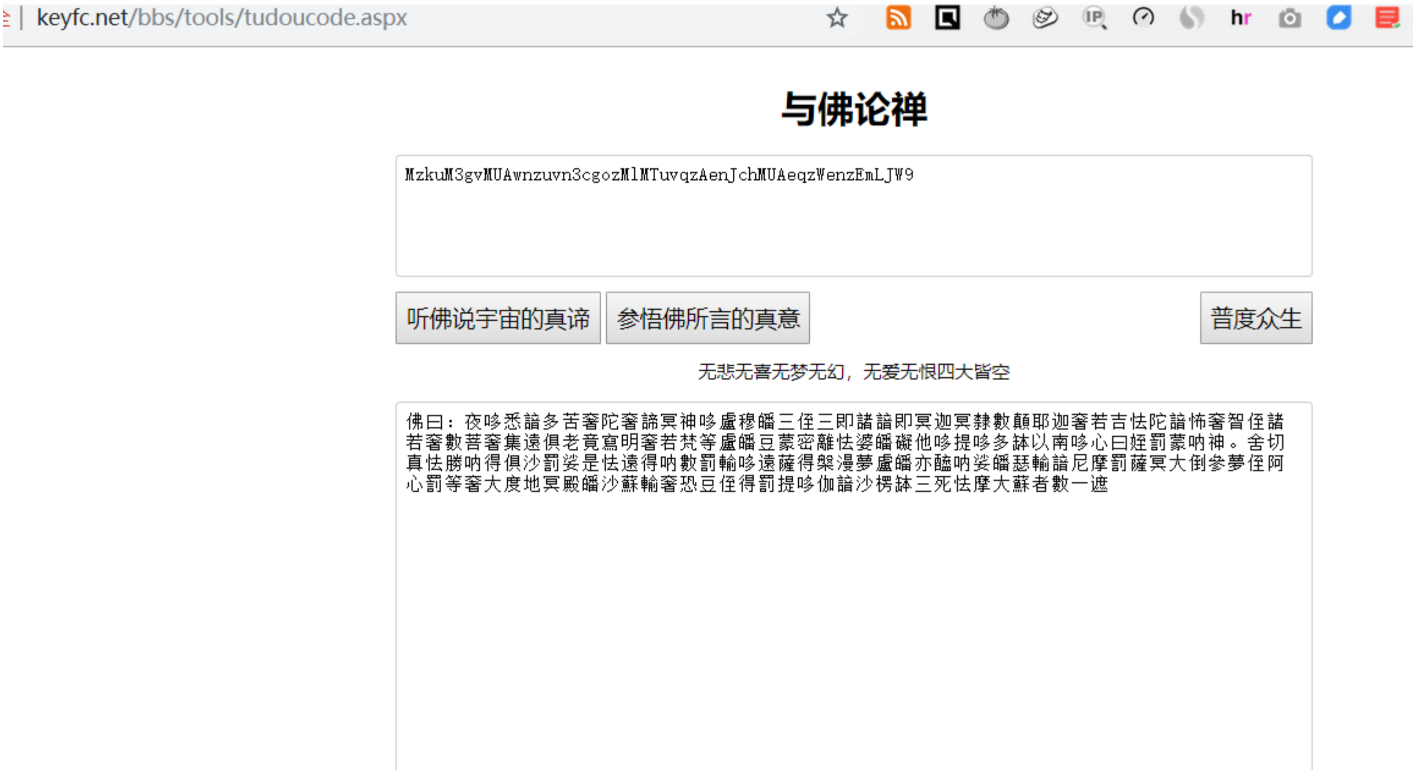
每两个一组，将16进制转换为10进制，减去128以后输出 ascii



```
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e
flag = ''
for i in range(0,len(string), 2):
    s = "0x" + string[i] + string[i+1]
    flag += chr(int(s, 16) - 128)
print(flag)
```

10.如来十三掌

打开是与佛论禅，到http://keyfc.net/bbs/tools/tudoucode.aspx解密，佛了。



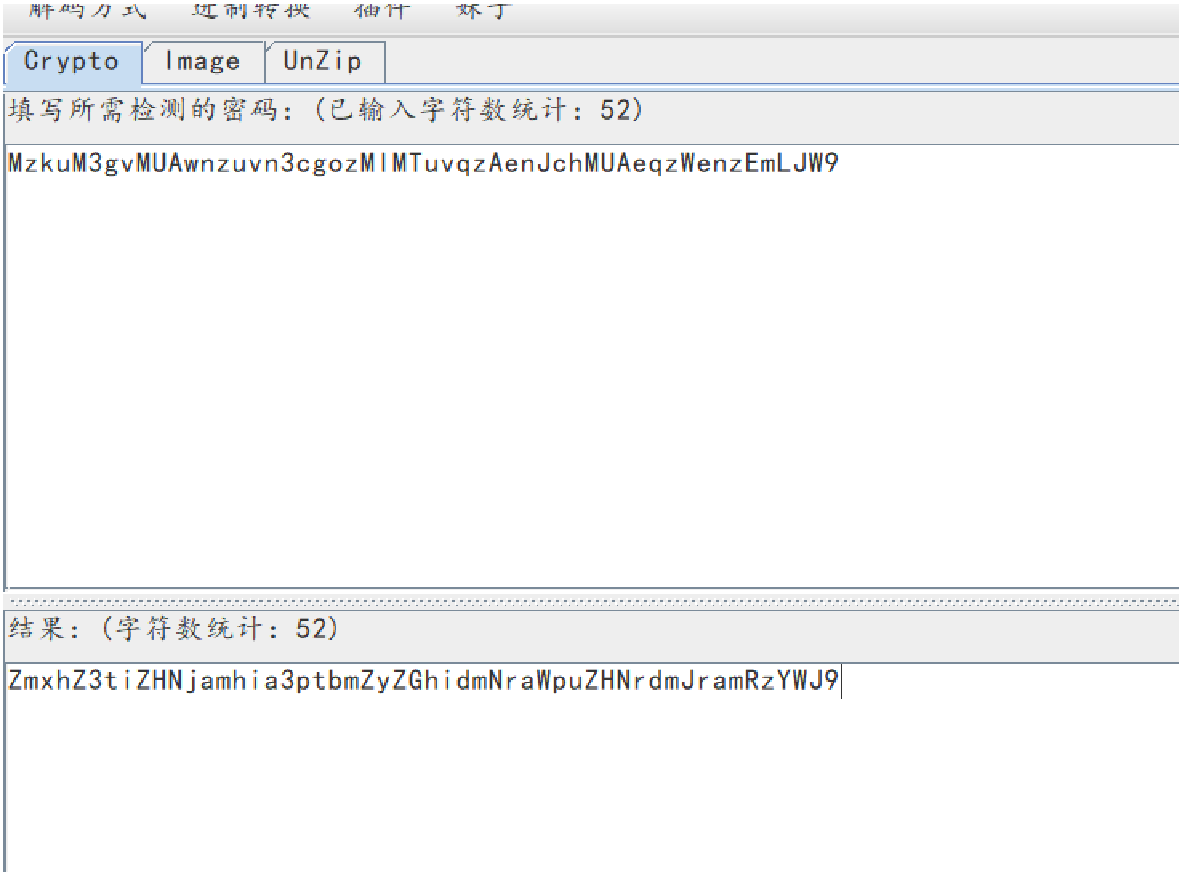
与佛论禅

MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

无悲无喜无梦无幻，无爱无恨四大皆空

佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

解 rot-13， 得到ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9 在base64解码
flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}



填写所需检测的密码：(已输入字符数统计：52)

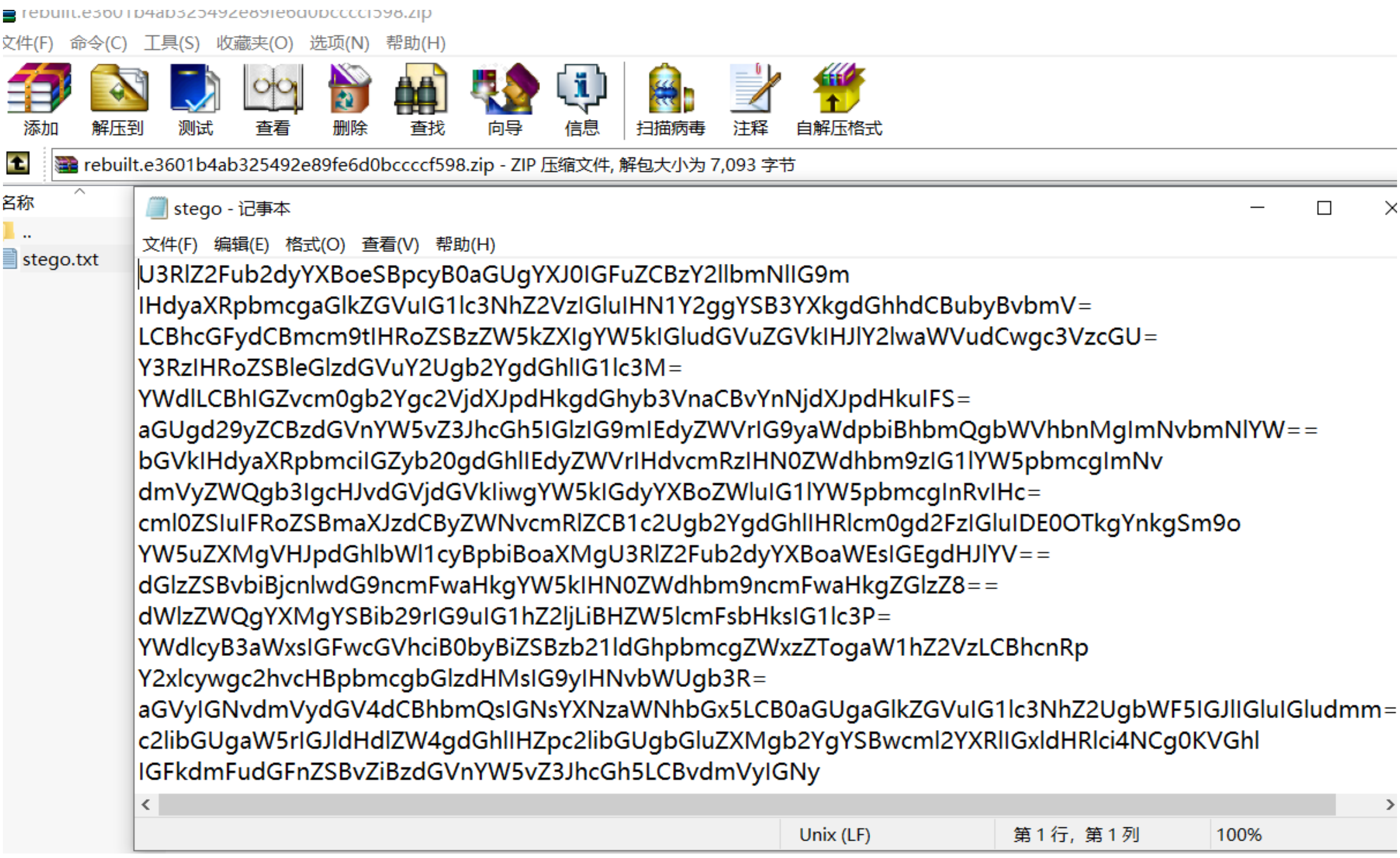
MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

结果：(字符数统计：52)

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

11.base64stego

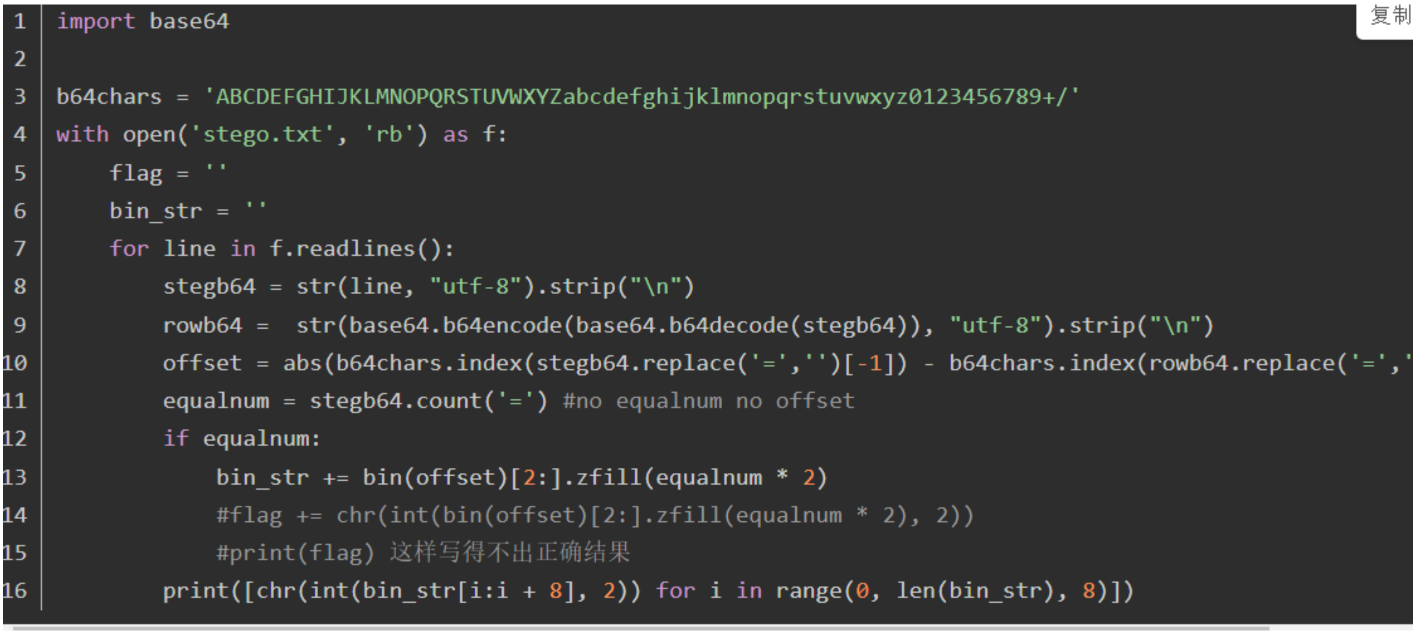
下载来一个解压包，需要密码，伪加密来着，用winrar修复功能修复一下就可以打开了，打开一大串base64，应该是吧，直接解解不出来


rebuilt.e3601b4ab325492e89fe6d0bcccf598.zip
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加
解压到
测试
查看
删除
查找
向导
信息
扫描病毒
注释
自解压格式
名称
..
stego.txt
stego - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Unix (LF)
第 1 行，第 1 列
100%

rebuilt.e3601b4ab325492e89fe6d0bcccf598.zip - ZIP 压缩文件, 解包大小为 7,093 字节

```
U3RlZ2Fub2dyYXBoeSBpcyB0aGUgYXJ0IGFuZCBzY2llbmNlIG9m
IHdyaXRpbmcgaGlkZGVuIG1lc3NhZ2VzIGluIHN1Y2ggYSB3YXkgdGhhdCBubyBvbmV=
LCBhcGFydCBmcm9tIHRoZSBzZW5kZXIgYW5kIGludGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
Y3RzIHRoZSBleGlzdGVuY2Ugb2YgdGhlIG1lc3M=
YWdlLCBhIGZvcm0gb2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpdHkuIFS=
aGUgd29yZCBzdGVnYW5vZ3JhcGh5IGlzIG9mIEdyZWVrIG9yaWdpbiBhbmQgbWVhbnMgImNvbmNlYW==
bGVkIHdyaXRpbmciIGZyb20gdGhlIEdyZWVrIHdvcmRzIHN0ZWdhbm9zIG1lYW5pbmcgImNv
dmVyZWQgb3IgcHJvdGVjdGVkIiwgYW5kIGdyYXBoZWluIG1lYW5pbmcgInRvIHc=
cml0ZSIuIFRoZSBmaXJzdCByZWNvcmRlZCB1c2Ugb2YgdGhlIHRlcm0gd2FzIGluIDE0OTkgYnkgSm9o
YW5uZXMgVHJpdGhlbWl1cyBpbiBoaXMgU3RlZ2Fub2dyYXBoaWEsIGEgdHJlYV==
dGlzZSBvbiBjcnlwdG9ncmFwaHkgYW5kIHN0ZWdhbm9ncmFwaHkgZGlzZ8==
dWlzZWQgYXMgYSBib29rIG9uIG1hZ2ljLiBHZW5lcmFsbHksIG1lc3P=
YWdlcyB3aWxsIGFwcGVhciB0byBiZSBzb21ldGhpbmcgZWxzZTogaW1hZ2VzLCBhcnRp
Y2xlcywgc2hvcHBpbmcgbGlzdHMsIG9yIHNvbWUgb3R=
aGVyIGNvdmVydGV4dCBhbmQsIGNsYXNzaWNhbGx5LCB0aGUgaGlkZGVuIG1lc3NhZ2UgbWF5IGJlIGluIGludmm=
c2libGUgaW5rIGJldHdlZW4gdGhlIHZpc2libGUgbGluZXMgb2YgYSBwcml2YXRlIGxldHRlci4NCg0KVGhl
IGFkdmFudGFnZSBvZiBzdGVnYW5vZ3JhcGh5LCBvdmVyIGNy
```

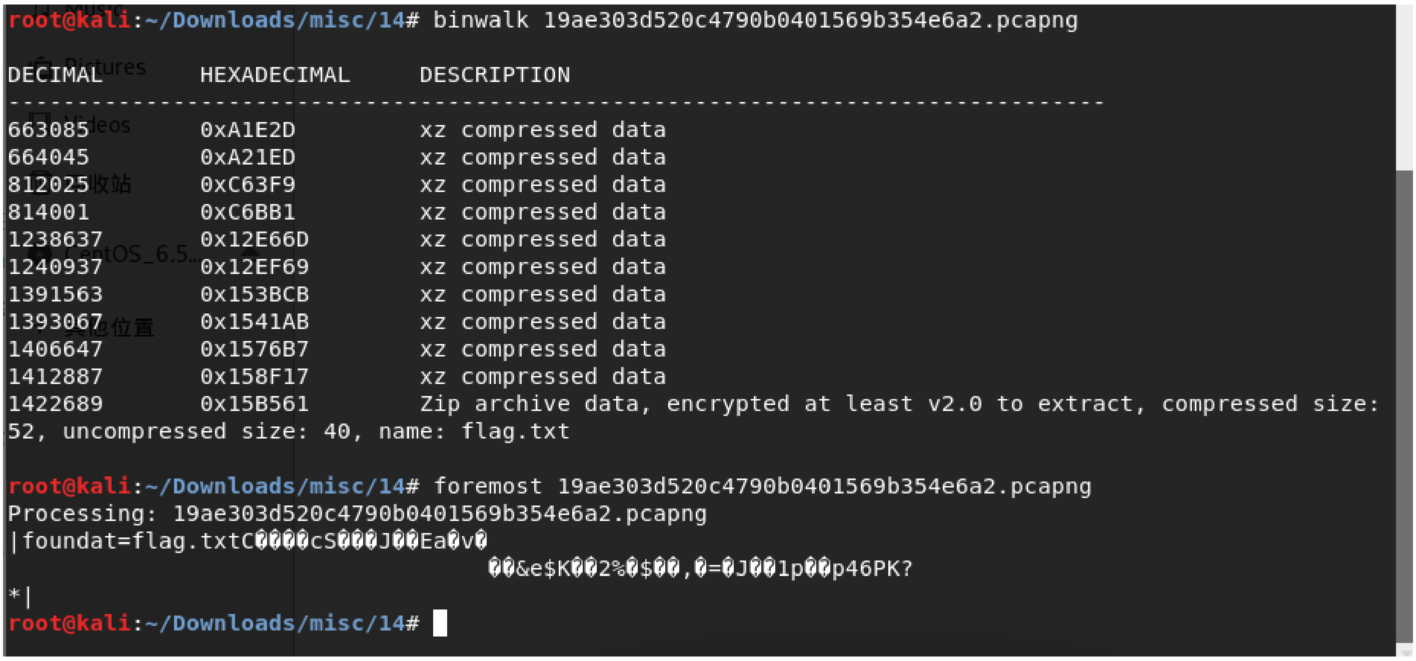
参考https://www.tr0y.wang/2017/06/14/Base64steg/使用脚本处理一下



```python
import base64

b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('stego.txt', 'rb') as f:
    flag = ''
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 =  str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=','')[-1]) - b64chars.index(rowb64.replace('=','
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
            #flag += chr(int(bin(offset)[2:].zfill(equalnum * 2), 2))
            #print(flag) 这样写得不出正确结果
        print([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)])
```

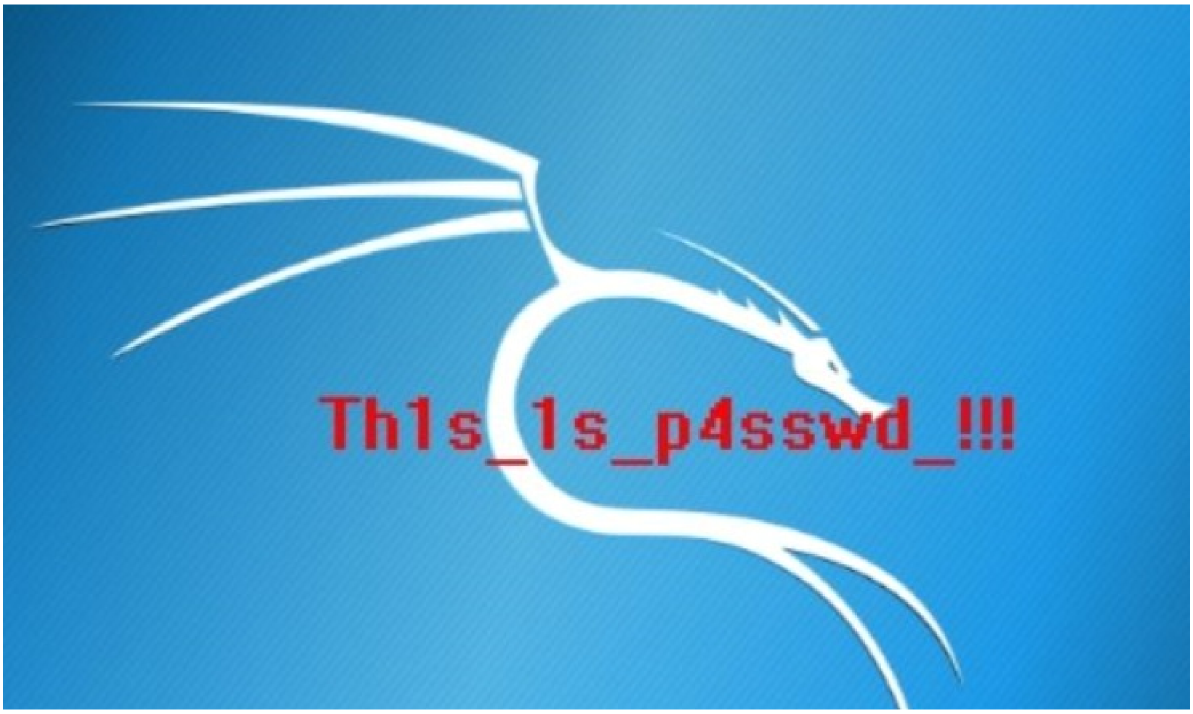
12.功夫再高也怕菜刀

下载下来是个流量包，binwalk跑一下，里面还包含一个zip，foremost分离文件 ，zip包需要密码，不是弱密码

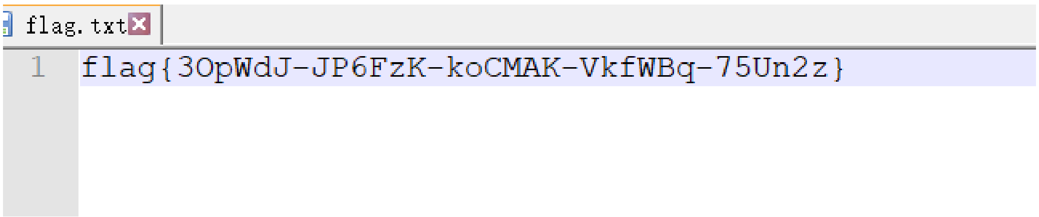


```
root@kali:~/Downloads/misc/14# binwalk 19ae303d520c4790b0401569b354e6a2.pcapng

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
663085        0xA1E2D         xz compressed data
664045        0xA21ED         xz compressed data
812025        0xC63F9         xz compressed data
814001        0xC6BB1         xz compressed data
1238637       0x12E66D        xz compressed data
1240937       0x12EF69        xz compressed data
1391563       0x153BCB        xz compressed data
1393067       0x1541AB        xz compressed data
1406647       0x1576B7        xz compressed data
1412887       0x158F17        xz compressed data
1422689       0x15B561        Zip archive data, encrypted at least v2.0 to extract, compressed size:
52, uncompressed size: 40, name: flag.txt

root@kali:~/Downloads/misc/14# foremost 19ae303d520c4790b0401569b354e6a2.pcapng
Processing: 19ae303d520c4790b0401569b354e6a2.pcapng
|foundat=flag.txtC����cS���J��Ea�v�
                                   ��&e$K��2%�$��,�=�J��1p��p46PK?

*|
root@kali:~/Downloads/misc/14# 
```

分析流量包，搜索flag.txt关键字，在1150行，追踪tcp流量流，发现jpg十六进制加密，还原jpg图片，图片文字即压缩包密码，



flag值为：



```
flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}
```