

2024Tangping Cup-冷鸢

博客: <http://www.miaoaixuan.cn/>

Misc

非常好忽悠混合

flag1

通过下载视频发现flag1藏在视频文件名称里



flag2

在视频的第二帧中发现有flag2



心中无码，自然高清

通过枚举分别可打印字符的马赛克图，然后将马赛克flag切片进行脚本比对，可得最终flag

```

1  from PIL import Image, ImageDraw, ImageFont
2  import os
3  import string
4
5  # Ensure the output directory exists
6  output_dir = './mosaic_chars'
7  if not os.path.exists(output_dir):
8      os.makedirs(output_dir)
9
10 flag = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890'
11
12 H = 68
13 W = 30
14
15 canvas = Image.new('RGB', (W * len(flag), H), (255, 255, 255))
16 # Ensure the font path is correct for your system
17 font = ImageFont.truetype('C:/Users/miaoaixuan/Desktop/JetBrainsMono-Regular.ttf', 50, encoding='utf-8')
18 pen = ImageDraw.Draw(canvas)
19 pen.text((0, 0), flag, 'black', font)
20
21 def mosaic_img(img: Image.Image, L, H, R, D):
22     w, h = R - L, D - H
23     a = [0, 0, 0]
24     cnt = 0
25     for x in range(w):
26         for y in range(h):
27             j = img.getpixel((L+x, H+y))
28             for ch in range(len(a)):
29                 a[ch] += j[ch]
30             cnt += 1
31     b = [k//cnt for k in a]
32     mosaic = Image.new('RGB', (w, h), tuple(b))
33     img.paste(mosaic, (L, H, R, D))
34
35 for i in range(len(flag)):
36     char = canvas.crop((W * i, 0, W * (i+1), H))
37     if 0 <= i < len(flag) : # Apply mosaic to specified characters
38         mosaic_img(canvas, W*i, 0, W*i+W, H//2)
39         mosaic_img(canvas, W*i, H//2, W*i+W, H)
40     # Save the character image after potentially applying mosaic
41     char = canvas.crop((W * i, 0, W * (i+1), H)) # Recrop to get the updated character
42     char.save(f'{output_dir}/{flag[i]}_{char.tobytes().__len__().png}')
43

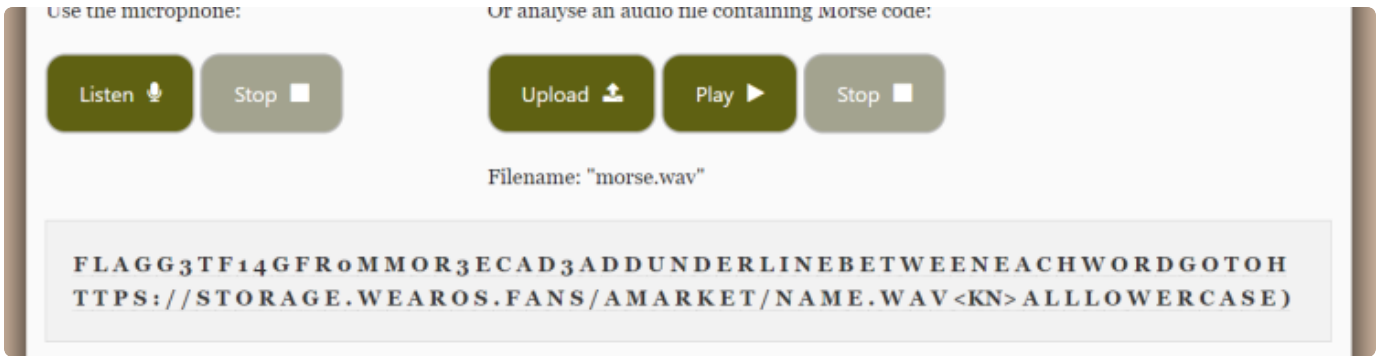
```

```
44 canvas.save('flag_censored.png', format='png')
```

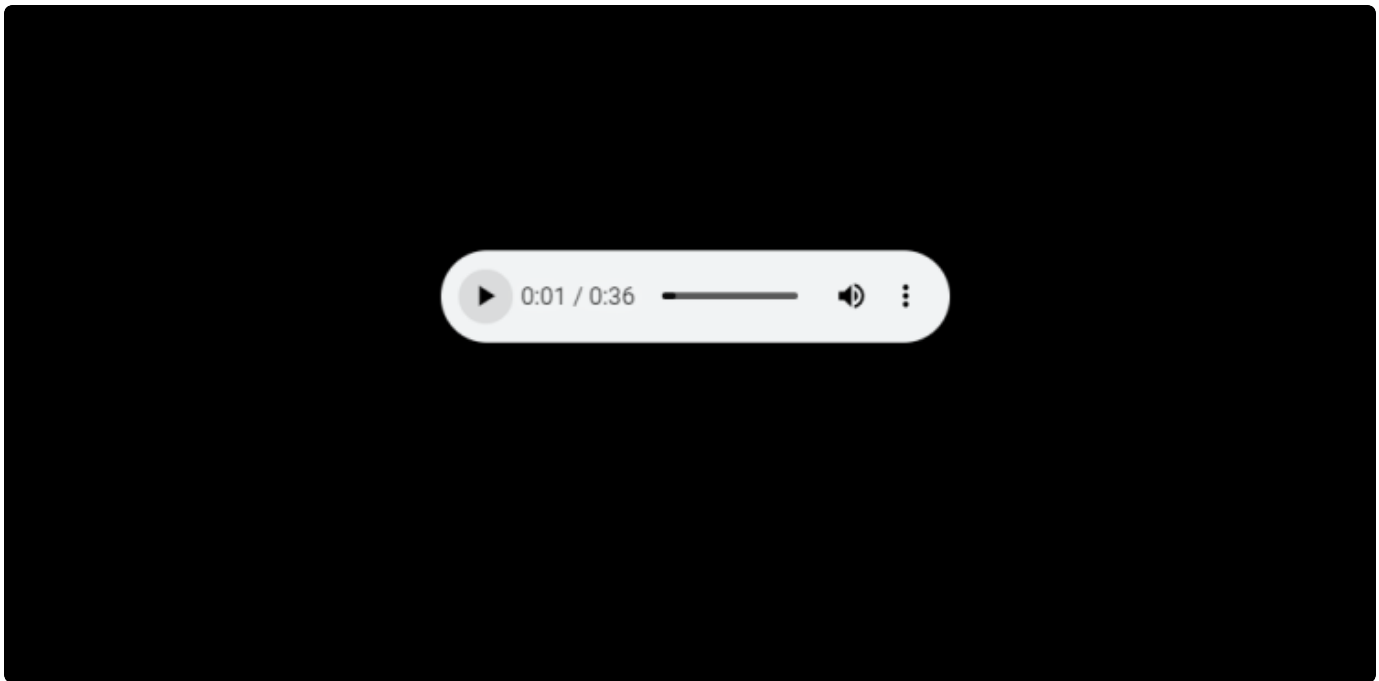
```
1  import os
2
3
4  def files_are_identical(file1_path, file2_path):
5      """逐字节比较两个文件，检查它们是否完全相同"""
6      with open(file1_path, 'rb') as file1, open(file2_path, 'rb') as file2:
7          while True:
8              chunk1 = file1.read(4096)
9              chunk2 = file2.read(4096)
10
11             if chunk1 != chunk2:
12                 return False
13
14             if not chunk1: # 如果chunk1为空，意味着文件已到末尾
15                 break
16
17         return True
18
19  def compare_file_with_folder(target_file_path, folder_path):
20      """比较指定文件与文件夹内所有文件，找出内容完全相同的文件"""
21      identical_files = []
22
23      for root, _, files in os.walk(folder_path):
24          for filename in files:
25              file_path = os.path.join(root, filename)
26              if files_are_identical(target_file_path, file_path):
27                  identical_files.append(file_path)
28
29      return identical_files
30
31  def print_identical_files(identical_files):
32      """打印所有相同文件的路径"""
33      if identical_files:
34          print("找到以下相同的文件：")
35          for file_path in identical_files:
36              print(file_path)
37      else:
38          print("在文件夹中没有找到相同的文件。")
39
40  target_file_path = 'C:/Users/miaoaixuan/Desktop/1/char_23.png'
41  folder_path = 'C:/Users/miaoaixuan/mosaic_chars'
42  identical_files = compare_file_with_folder(target_file_path, folder_path)
43  print_identical_files(identical_files)
```

bepbep

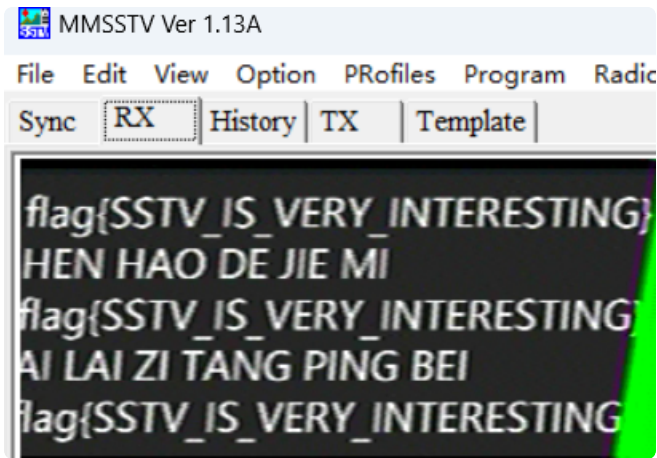
通过摩斯自动网站解密摩斯电码[Morse Code Adaptive Audio Decoder | Morse Code World](#)根据要求需要转小写，还要加下划线，得到flag1



Flag1末尾有一网址可得第二段音频,易得sstv解密



sstv解密得flag2



我朝，大盒

通过这几条信息可判断列车的行驶轨迹和旁边高速，再通过路路通程序查询可得车次号

- 1月25日12:50中国电信 中国沙棘之乡、中国蚕豆之乡、中国绿色名县——“天下贵清康养漳县”欢迎您!微信搜索畅游漳县小程序，了解更多旅游资讯。[漳县文体广电和旅游局]
- 1月25日13:40中国电信 “畅游生态陇南乐享康养胜地热情好客的陇南人民欢迎您!更多旅游资讯，请关注“陇南文旅”微信公众号获取。
- 1月25日16:39中国电信 [广元市农民工暨返乡下乡创业工作领导小组办公室]乡亲们朋友们您好!为传递省委省政府对全川返乡乡亲们的关心关爱，省农民工办公室牵头首届“天府情动，向川籍老乡送上新春福利。请通过微信关注“四川农民工服务平台”领取，或登录网址【数据删除】领取，并到就近农民工服务站兑换!。



D206 动车 共15站						
车站名称	车次	到点	开点	停时	里程	
兰州	D206	--:--	11:35	0分	0	
岷县	D206	13:19	13:21	2分	216	1
哈达铺	D206	13:38	13:40	2分	241	1
陇南	D206	14:37	14:41	4分	28分钟 370公里	1
广元	D206	15:42	15:48	6分	509	1
阆中	D206	16:42	16:44	2分	615	1
南部	D206	16:57	16:59	2分	636	1
南充北	D206	17:29	17:31	2分	697	1
武胜	D206	18:00	18:02	2分	754	1
重庆西	D207	19:01	19:12	11分	867	1
綦江东	D207	19:42	19:44	2分	928	1
赶水东	D207	20:02	20:04	2分	959	1
桐梓东	D207	20:43	20:45	2分	1035	1
遵义	D207	21:13	21:15	2分	1088	1
贵阳北	D207	22:20	--:--	0分	1214	1

图片exif中有iso信息

照相机制造商	OnePlus
照相机型号	PJA110
光圈值	f/1.8
曝光时间	1/172 秒
ISO 速度	ISO-138
曝光补偿	0 档光圈
焦距	6 毫米
最大光圈	1.7
测光模式	偏中心平均
目标距离	200 米
闪光灯模式	无闪光, 强制
闪光灯能量	
35mm 焦距	24
高级照片	

可得答案

Flag1

问题1: 图片中的位置附近有一条高速公路 请给出高速公路编号[G+两位数字]

G75

问题2: 图片所在位置最近的市是哪个[XX(X)市]

阆中市

问题3: 图片采用的ISO感光度是多少

138

提交答题区1

Flag2

问题4: 出题人所乘车的的车次号是

D206

提交答题区2

这是flag2flag{A1_lA1_zl_gU0_Tie}

躺平问答

通过百度等搜索引擎搜索易得 (bushi

上周，身为2024届英才计划培养对象的出题人ZianTT参加了一次冬令营，请问他的活动大致地点是？（七个汉字）

哈尔滨工业大学

在2023年，Cloudflare因为机房停电导致大量服务不可用，Cloudflare官方博客记载此时的英文版链接是：

<https://blog.cloudflare.com/post-mortem-on-cloudflare-control-plane-and-analytics-outage>

QQ上线了新春活动，但糟糕的体验显然引发了一些用户的困扰，关闭该功能的链接是？（一个由https://开始的链接）

<https://docs.qq.com/form/page/DUWI2cXN2WktZVWlB>

HTCPCP是一种类似HTTP的协议，用于控制咖啡壶，其中，当发送了BREW请求来冲泡的时候，如果服务认为请求的添加项组合违背了饮酒者对所述种类的共识，返回的状态码是：

403

OpenAI在2024年1月发生了多少运行事件(以公示数据为准)：

11

比赛平台域名tpcup.org的Registry Domain ID 是：

6de68c6722e84ac0a541745e94b7dca0-LROR

本次比赛计算服务提供商所在主体纳税人识别号是：（18位由数字和大写字母组成的字符串）

91440403MACK9P7J40

Web

躺平论坛

easy的F12

1 / 1 条

看不到的Flag

Lyscf

14 天前

登录 回复并刷新后可见

回复

说点什么吧...

</> 元素

<!DOCTYPE html>
<html dir="ltr" lang="zh-Hans">
 <head>
 <meta charset="utf-8">
 <title>看不到的Flag - 躺平论坛</title>
 <link rel="stylesheet" href="https://forum.tpcup.org/assets/forum.css?v=c0c03a38">
 <link rel="canonical" href="https://forum.tpcup.org/d/1-kan-bu-dao-de-flag">
 <link rel="preload" href="https://forum.tpcup.org/assets/forum.css?v=c0c03a38" as="style">
 <link rel="preload" href="https://forum.tpcup.org/assets/forum.js?v=8b038f4c" as="script">
 <link rel="preload" href="https://forum.tpcup.org/assets/forum-zh-Hans.js?v=c42b4028" as="script">
 <link rel="preload" href="https://forum.tpcup.org/assets/fonts/fa-solid-900.woff2" as="font">
 <link rel="preload" href="https://forum.tpcup.org/assets/fonts/fa-regular-400.woff2" as="font">
 <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, minimum-scale=1">
 <meta name="description" content="flag{we1cc0m3_t0_taN6P4ng_f0Rum}" == \$0
 <meta name="theme-color" content="#4D698E">
 <meta name="application-name" content="躺平论坛">
 <meta name="robots" content="index, follow">
 <meta name="twitter:card" content="summary_large_image">
 <meta name="twitter:title" content="看不到的Flag">
 <meta name="article:published_time" content="2024-02-03T04:22:31+00:00">
 <meta name="twitter:description" content="flag{we1cc0m3_t0_taN6P4ng_f0Rum}">
 <meta name="twitter:url" content="https://forum.tpcup.org/d/1-kan-bu-dao-de-flag">
 <meta property="og:site_name" content="躺平论坛">
 <meta property="og:type" content="article">
 <meta property="og:title" content="看不到的Flag">
 <meta property="og:description" content="flag{we1cc0m3_t0_taN6P4ng_f0Rum}">
 <meta property="og:url" content="https://forum.tpcup.org/d/1-kan-bu-dao-de-flag">
 <script type="application/ld+json"><script type="application/ld+json"></script>
 </head>
 <body class="no-touch">
 <div id="app" class="App affix App--discussion" aria-hidden="false">
 <div id="modal"></div>
 <div id="alerts"></div>
 <script></script>
 <script src="https://forum.tpcup.org/assets/forum.js?v=8b038f4c"></script>
 <script src="https://forum.tpcup.org/assets/forum-zh-Hans.js?v=c42b4028"></script>

Crypto

主唱太拼命了

看题目的意思，估计是要爆破p+q的后60位，刚好在网上找到一篇文章：

https://blog.csdn.net/weixin_52640415/article/details/130415368

直接拿里边的脚本来改了下

```

1  from Crypto.Util.number import *
2  from gmpy2 import *
3  ct = 184408724864033236225108070129785071805299414261066431154569808379562
    95325764192595485820729772845428753953590301713705078399201869365193708057
    32784889990407467183280759666536755061491905511950907381249931601944707007
    74724197391162379524862601796129845824968624416098490356038421618390694071
    15218245681423369
4  n = 9904357718211844437843964228564004795839497131210203530098363400218484
    96582243738732680608868337286124945651708032263596414682715371553854580290
    52632983980837449378159671374748926031921883773305189594299358694724069728
    79351916463222895099854550580764060495625083269234422638257312101484295327
    5020353743587393
5  gift = 1990829629715426119360378447663893112351624070402530624456193093583
    34639717991281104899674484609133115805473897433672609025228650732008259177
    23058108366848
6
7
8  PR.<x> = PolynomialRing(Zmod(n))
9  ok = False
10 p = 0
11 def pq_add(tp,tq,tgift,idx, kbit):
12     global ok
13     global p
14     if ok:
15         return
16     if tp*tq>n:
17         #print('>')
18         return
19
20     if (tp+(2<<idx))*(tq+(2<<idx))<n:
21         #print('<', hex((tp+(1<<(idx+2))))[:20], hex(tq+(2<<idx))[:20], he
x(N)[:20])
22         return
23
24     if idx<=kbit:
25         try:
26             f = tp + x
27             rr = f.monic().small_roots(X=2^kbit, beta=0.44)
28             if rr != []:
29                 """print(rr)
30                 print(tp)
31                 print('p = ',f(rr[0]))"""
32                 p = int(f(rr[0]))
33                 ok = True
34                 return

```

```

35         except:
36             pass
37
38         return
39
40     idx -= 1
41     b = tgift >> idx
42     one = 1 << idx
43
44     #print(hex(tp)[:20], hex(tq)[:20], hex(tgift)[:20], idx, b)
45
46     if b == 0 or b == 1:
47         pq_add(tp, tq, tgift, idx, kbit)
48     if b == 1 or b == 2:
49         pq_add(tp + one, tq, tgift - one, idx, kbit)
50         pq_add(tp, tq + one, tgift - one, idx, kbit)
51     if b == 2 or b == 3:
52         pq_add(tp + one, tq + one, tgift - (one << 1), idx, kbit)
53
54     tp = 1 << 511
55     tq = 1 << 511
56     tgift = gift - tp - tq
57     kbit = 60
58     pq_add(tp, tq, tgift, 511, kbit)
59     print(p)
60     q = n // p
61     e = bytes_to_long(b"too desperate!")
62     phi = (p - 1) * (q - 1)
63     d = invert(e, phi)
64     print(long_to_bytes(int(pow(ct, d, n))))

```

Reverse

HIT! 准入认证!

IDA打开搜索即得

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Function name	Segment	Start	Len
__init_proc	.init	0000000000001000	0000
sub_1020	.plt	0000000000001020	0000
__puts	.plt	0000000000001030	0000
__printf	.plt	0000000000001040	0000
__strcpy	.plt	0000000000001050	0000
__isoc99_scanf	.plt	0000000000001060	0000
__cxa_finalize	.plt.got	0000000000001070	0000
start	.text	0000000000001080	0000
sub_1080	.text	0000000000001080	0000
sub_1080	.text	0000000000001080	0000
sub_1120	.text	0000000000001120	0000
sub_1160	.text	0000000000001160	0000
sub_1165	.text	0000000000001165	0000
sub_11C0	.text	00000000000011C0	0000
sub_125E	.text	000000000000125E	0000
sub_1405	.text	0000000000001405	0000
main	.text	000000000000150E	0000
__init	.text	0000000000001640	0000
__fini	.text	00000000000016A0	0000
__term_proc	.fini	00000000000016A4	0000
__puts	extern	00000000000040F0	0000
__printf	extern	00000000000040F8	0000
__libc_start_main	extern	0000000000004100	0000
__strcpy	extern	0000000000004108	0000
__isoc99_scanf	extern	0000000000004110	0000
__cxa_finalize	extern	0000000000004118	0000
__bion_start	extern	0000000000004128	0000

IDA View-A

```

.rodata:0000000000002010 db 0
.rodata:0000000000002011 db 0
.rodata:0000000000002012 db 0
.rodata:0000000000002013 db 0
.rodata:0000000000002014 db 0
.rodata:0000000000002015 db 0
.rodata:0000000000002016 db 0
.rodata:0000000000002017 db 0
.rodata:0000000000002018 db 0
.rodata:0000000000002019 db 0
.rodata:000000000000201A db 0
.rodata:000000000000201B db 0
.rodata:000000000000201C db 0
.rodata:000000000000201D db 0
.rodata:000000000000201E db 0
.rodata:000000000000201F db 0
.rodata:0000000000002020 afIagZi4n7tA7t3 db 'flag{Zi4n7t_a7t3nd_YCjh_WinT3r_c4mp_in_h1t}',0
.rodata:0000000000002020 ; DATA XREF: .data:s140
.rodata:000000000000204C align 10h
.rodata:0000000000002050 aXvDlclabqmaxn db 'Xkvsv^DlclABQMaxHF^IamEOX*~$?v-AJoJczCos.',0
.rodata:0000000000002050 ; DATA XREF: .data:s240
.rodata:0000000000002070 align 20h
.rodata:0000000000002080 aAsdfghjklqwert db 'asdfghjklqwertyuiopzxcvbnmQWERTYUIOPZXCVBNMASDFGHJKL$%<~!@#&(-?H'
.rodata:0000000000002080 ; DATA XREF: sub_125E+4Efo
.rodata:0000000000002080 ; sub_125E+BAfo ...
.rodata:0000000000002081 db 'IT Login System v0.0.1 by ZianTT',0
.rodata:00000000000020E2 ; const char format[]
.rodata:00000000000020E2 format db 'Username: ',0 ; DATA XREF: main+9Dfo
.rodata:00000000000020ED a32s db 'X32s',0 ; DATA XREF: main+B5fo
.rodata:00000000000020ED ; main+E1fo
.rodata:00000000000020F2 ; const char aRegisterCode[]
.rodata:00000000000020F2 aRegisterCode db 'Register Code: ',0 ; DATA XREF: main+C6fo
.rodata:0000000000002102 ; const char s[]
.rodata:0000000000002102 s db 'Verification successful',0
.rodata:0000000000002102 ; DATA XREF: main+111fo
.rodata:000000000000211B ; const char aVerificationFa[]
.rodata:000000000000211B aVerificationFa db 'Verification failed!',0
.rodata:000000000000211B ; DATA XREF: main:loc_162Afo
.rodata:000000000000211B _rodata ends
.rodata:000000000000211B
.rodata:0000000000002130 ; =====
.eh_frame_hdr:0000000000002130 ;
.eh_frame_hdr:0000000000002130 ; Segment type: Pure data
.eh_frame_hdr:0000000000002130 ; Segment permissions: Read
.eh_frame_hdr:0000000000002130 _eh_frame_hdr segment dword public 'CONST' use64
.eh_frame_hdr:0000000000002130 assume cs:_eh_frame_hdr

```