攻防世界 3-11

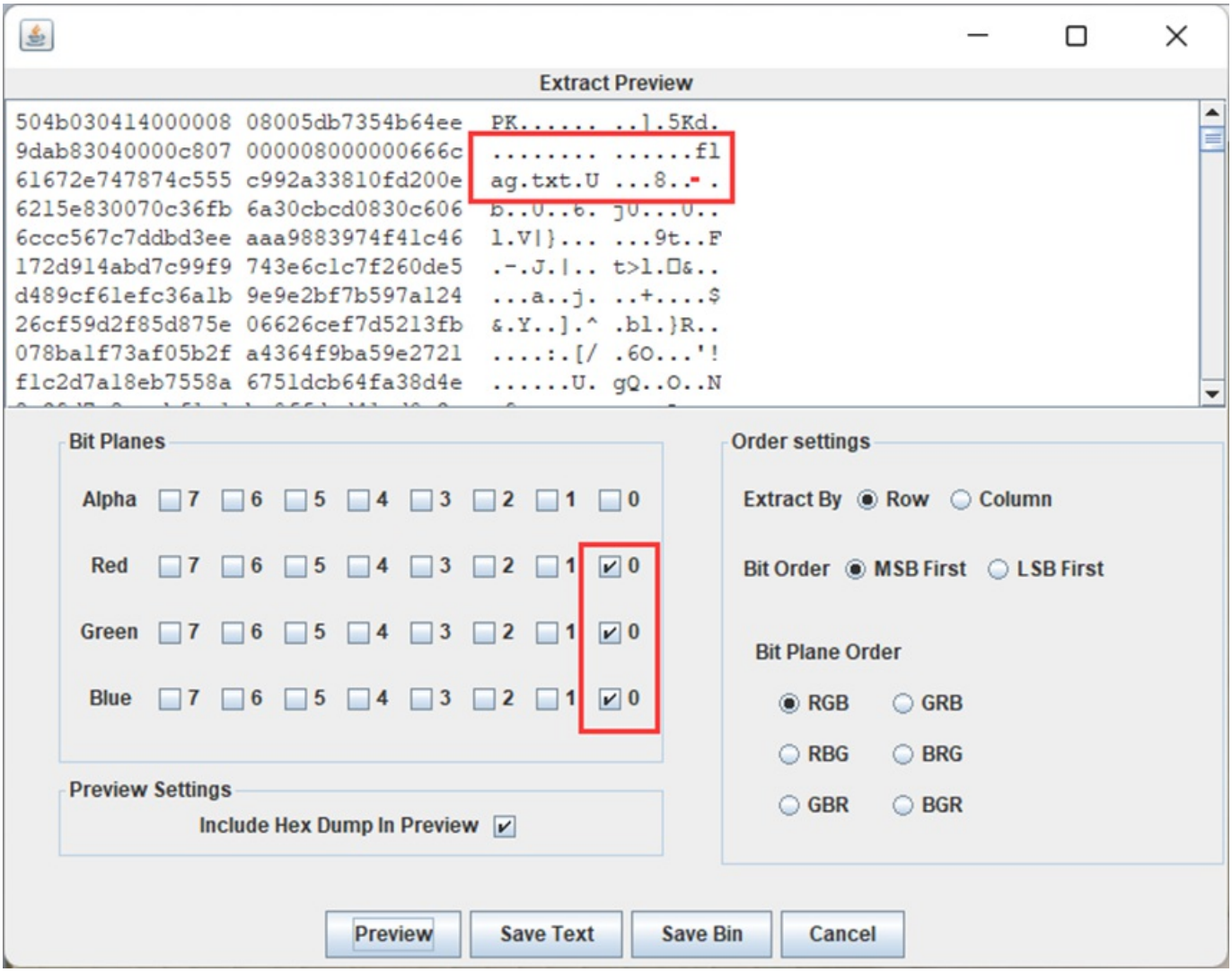
原创

方亭子 于 2022-02-24 20:58:30 发布 125 收藏

分类专栏： # 攻防世界MISC题目 文章标签： python

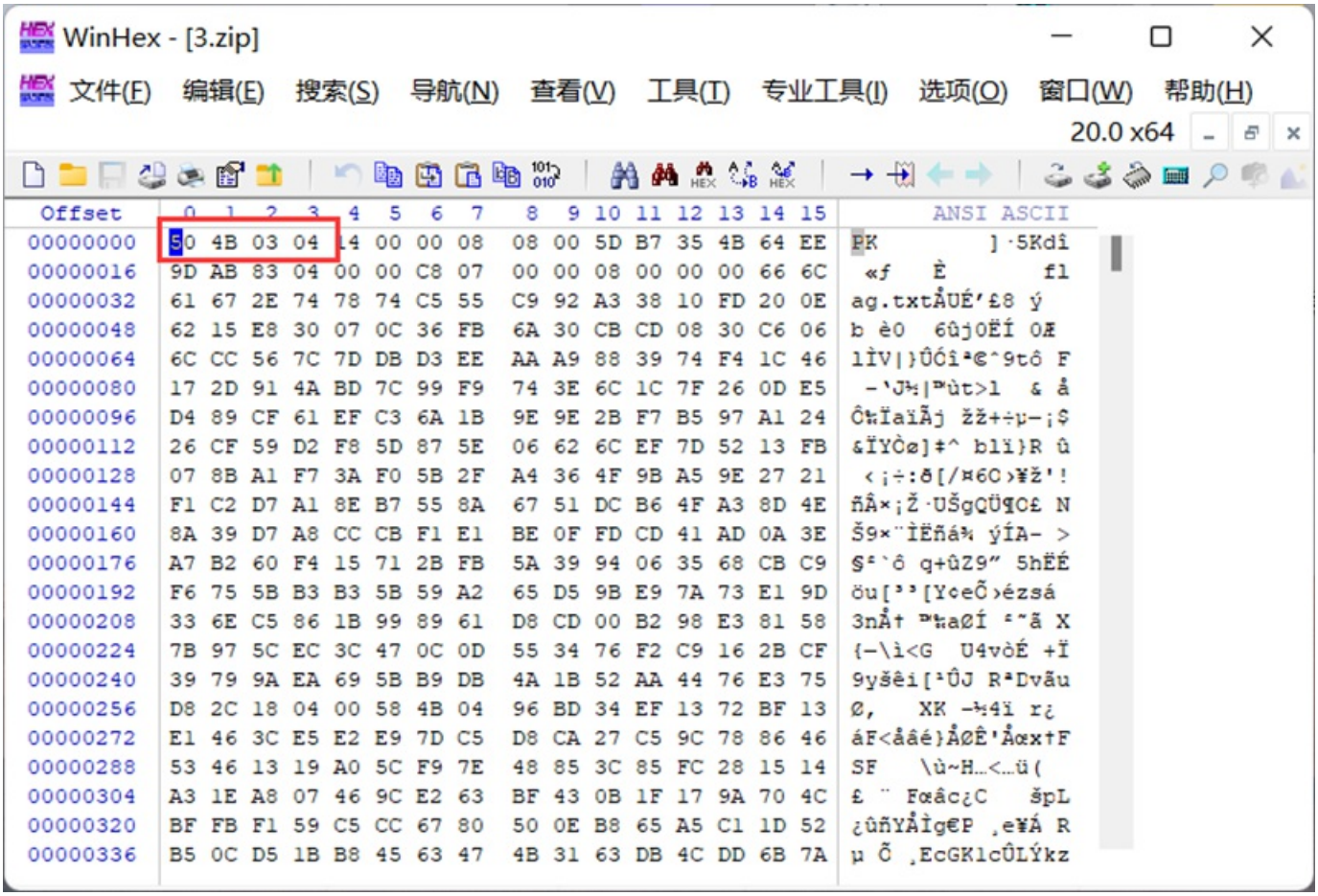
方莱莱出品

拿到题目，使用隐写工具Stegsolve看下，发现是lsb隐写



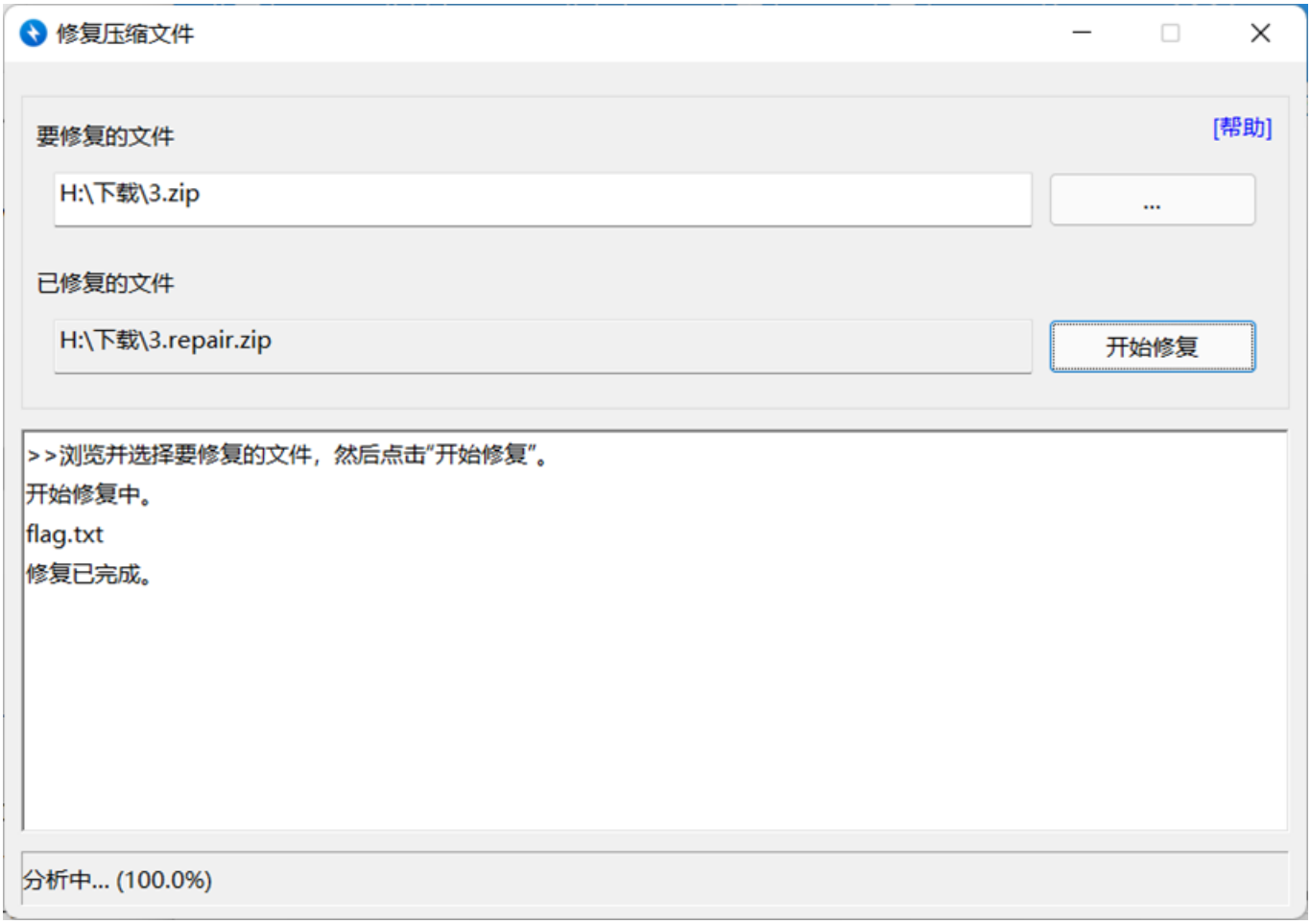
save bin保存文件

使用winhex打开发现文件头是zip文件的文件头



修改后缀名，然后解压文件，提示压缩包损坏

使用bandizip修复压缩包



打开后是一串base64代码，编写解码脚本

```
import base64
a = input("输入base64代码：")
b = base64.b64decode(a)
print(b)
```

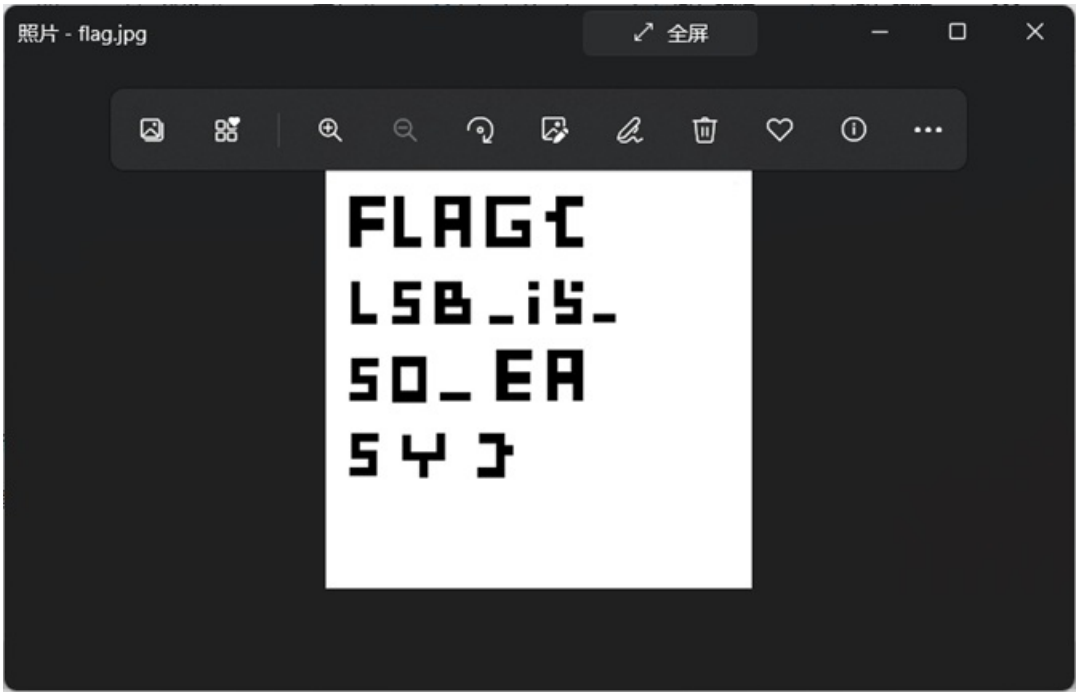
解码后看到了png开头的字符，判断是base64转图片

```
b"\x89PNG\r\n\x1a\n\x00\x00\x00\rIHDR\x00\x00\x00\xfa\x00\x00\x00\xfa\x08\x06\x00\x00\x00\x88\xecZ=\x00\x00\x00\x01sRGB\x00\xae\xce\x1c\xe9\x0
0\x00\x00\x04gAMA\x00\x00\xb1\x8f\x0b\xfca\x05\x00\x00\x00\tpHYs\x00\x00\x12t\x00\x00\x12t\x01\xdef\x1fx\x00\x00\x05jIDATx^\xed\xdd[N\xe4F\x00
@\xd1!\xfb_+[H\xc6\x03Q$\xd2\rn\x97\xdf\xf7\x1c\xc9\x9a\xf9i?\xaa\xb9*\x97\x81\xe6\xed\xef\xdf~\x01\xb7\xf6\xd7\xe7\xbf\xc0\x8d\t\x1d\x02\x84\
x0e\x01B\x87\x00\xa1C\x80\xd0!@\xe8\x10 t\x08\x10:\x04\x08\x1d\x02\x84\x0e\x01B\x87\x0b{\x7f\x7f\xff\xfc\xdf\xf7\xfcR\x0b\x04\x98\xd1!@\xe8\x1
0 t\x08\x10:\x04\x08\x1d\x02\x84\x0e\x01\x8b\xbf\xbd\xf6\xf6\xf6\xf6\xf9\xbf\xf5<:\x95g\xc7Y\xeb\xbb\x82{]\xc7W[\x1c\xf7\x91\x91q\x1a=\xc7\xb5
\xde#\xc6\x99\xd1!@\xe8\x10 t\x08\x10:\x04x\x18\xb7p\xff\xdf]\xff\x9cs\xdb\xfa\xba\xd60\xfa\x1e\x9f\xe9Z\xea6\t}\xcd7x\xeb \x96\xee\x7f\xf4\xf
a\xb7\xbe\xae5\\\xe1\x1c\x99\xc7\xad;\x04\x08\x1d\x02\x84\xce\x9f[\xf4G\x1b\xf7!t\x08\x10:\x04\x08\x1d\x02N\xf3}\xf4g\xa7\xf1\xec8k}\x8bg\x8b\
xb5\xe8\x9cs\xdb\xfa\xba^\xf1\xea\x18\x1cq\x8e\x8c1\xa3_\xd0\x14\xe6\xdc\r&B\xe7\xcf\x0c\xfdh\xe3>\x84\x0e\x01B\x87\x00\xa1C\x80\xd0!\xc0o\xaf
\r\xec\xff\xa8\xd7>\xf3h\x9fk\xefo\xb2\xd6\xd8\xb3\x1f3:\x04\x08\x1d\x02\x84\x0e\x01\x97]\xa3\xcf\xf5\xd3\xb9\x8c\xacC\xb7x\xed\xdaF\xde\x8b\x
ad\xc7\x9e\xfd\x98\xd1!@\xe8\x10 t\x08\x10:\x04\x08\x1d\x02\x16?u\x07\xae\xc3\x8c\x0e\x01B\x87\x00\xa1C\x80\xd0!@\xe8\x10 t\x08\x10:\x04\x08\x
1d\x02\x84\x0e\x01B\x87\x00\xa1C\x80\xd0!@\xe8\x10 t\x08\x10:\x04\x08\x1d\x02\x84\x0e\x01B\x87\x00\x1f%\xc5C#\x7f\x9c\x82\xf3\x19\n\xfd\xd1\x1
```

修改一下脚本，保存为图片格式，并且识图片字符，不过用的pytesseract模块没有识别好字符，需要自己在对照一下。
脚本：

```python
import pytesseract,base64
from PIL import Image
a = input("输入base64代码：")
b = base64.b64decode(a)
with open("flag.jpg","wb+") as c:#把解码后的内容，保存为flag.jpg
    c.write(b)
d = Image.open("flag.jpg")
f = pytesseract.image_to_string(d)
print(f)
```

脚本获得的图片



识别结果如下：

```
FLAG
LSB i4-
SO_EA
su
```

正确flag：FLAG{LSB_i5_SO_EASY}