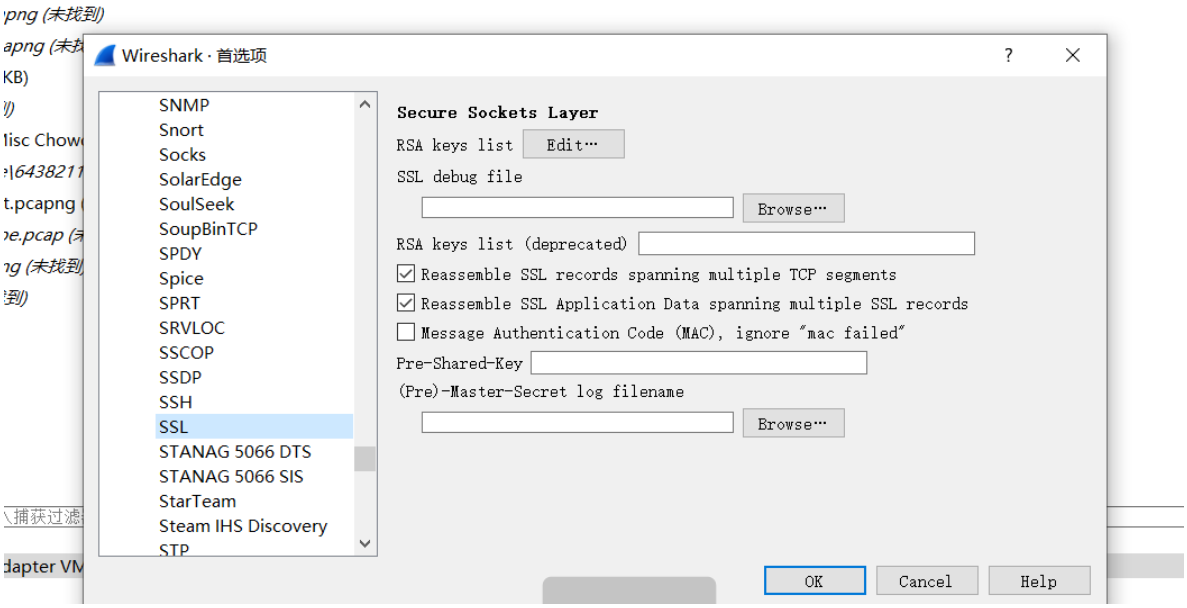
签到题目

lsb stegsolve拿到part2

图片最后拿出zip得到part1

简单流量

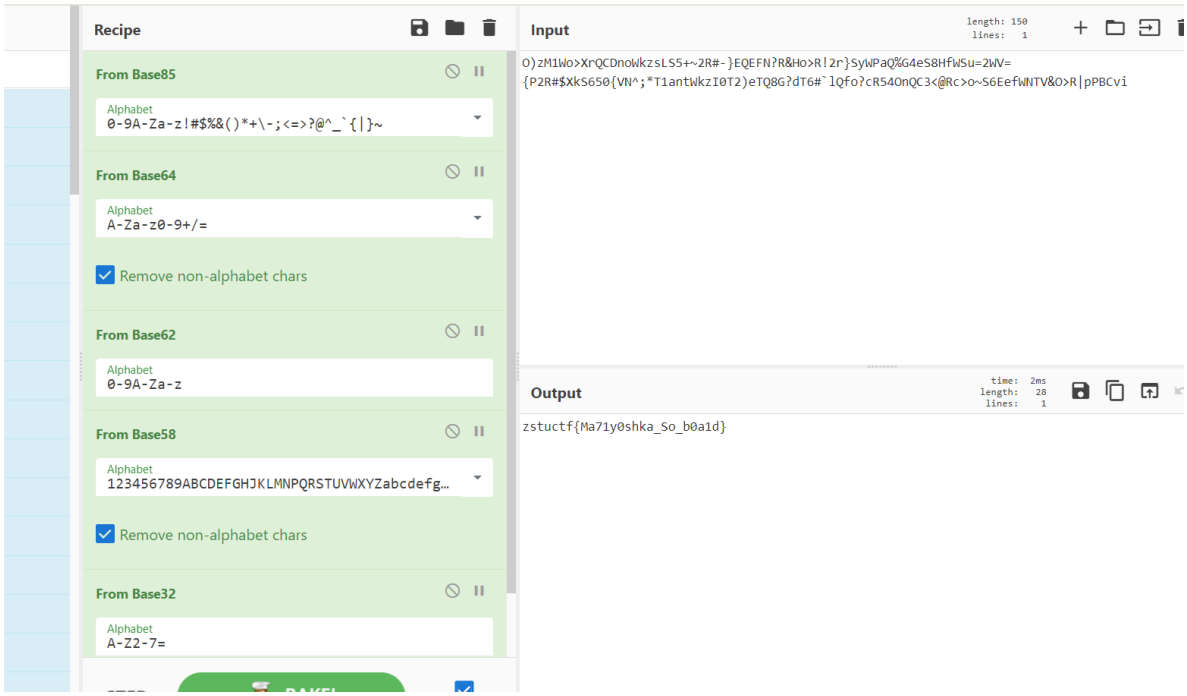
一个 sslkey.log 还有一个加密流量



流量好像是百度搜索 大部分urlencode的

直接搜索zstu就能找到

五层套娃



大音乐家

wav左右声道分开 01

```
import wave
song = wave.open("song_embedded.wav", mode='rb')
frame_bytes = bytearray(list(song.readframes(song.getnframes())))
extracted = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
dic = "0123456789ABCDEF"
out = ""
for i in range(0, len(extracted), 4):
    out +=
dic[8*extracted[i]+4*extracted[i+1]+2*extracted[i+2]+1*extracted[i+3]]
print(out)
with open("out.txt", "w") as f:
    f.write(out)
```

取出zip 伪加密 得到flag

监听消息

一个流量 一共就两个流 追踪直接贴出来一个png pngcheck crc不对 爆破得到原图 ps右边加上定位就能微信扫出来

替换密码

前面除去flag部分替换密码得到密码表 替换flag里的字母得到正确flag

哈希爆破

根据附件跑一下得到dic 然后爆破一下就行 范围不大跑起来快的

```
from hashlib import sha256
cipher = "b2ba5bea9136b5387c4482ba2a2bf068a524ef8986d13ab953b5a3e41e5ae266"
dic = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

def brute(cipher):
    #  success("cipher -> {}".format(cipher))
    #  print type(cipher)
    for a in dic:
        for b in dic:
            for c in dic:
                for d in dic:
                    x = (a + b + c + d + "1IAVP3RwDQbO3MCb").encode()
                    # print(sha256(x).hexdigest())
                    if sha256(x).hexdigest() == cipher:
                        return x


print(brute(cipher))
```

非对称的

rsa

记得不是很清楚 好像是给的 n e c吧

n因式分解得到p q

```
phi = (p-1) * (q-1)
d = gmpy2.invert(e, phi)
m = gmpy2.powmod(c, d, n)
print(m)
tmp = hex(m)
print tmp, tmp[2:].decode('hex')
```