misc

三重隐写

题目已经提示了3重隐写
首先可以看到一个文件名字是You know LSB,用silenteye得到key

> uFSARLVNwVIewCY5

然后用mp3stego decode

解压发现里面的文件还decrypt
最后一个音频文件是一个二维码，扫码得到key
解密得到flag

> hgame{i35k#zIewynLC0zfQur!*H9V$JiMVWmL}

re

oooollvm

考的是llvm的流程平坦化，网上有去平坦化的脚本，但不知道咋回事脚本运行的时候总是报错，只好硬着头皮看了。
看了很久发现了规律，大致就是if + break组成了多重while里面的判断，如果是false就跳出一层循环，最后来到switch语句。

```
if ( (((y < 10) ^ (((x - 1) * x & 1) == 0)) | (y < 10 && ((x - 1) * x & 1) ==
0)) & 1 )
```

其中这里纠结了很久，x和y既没有定义也没有赋值，然后双击看了看，发现这两个变量都在bss里面，就盲猜两个的值都是0
最后发现主要这个判断是false，对应输入的字符就是正确的

```
if ( table2[v15] != (~s[v15] & (v15 + table1[v15]) | ~(v15 + table1[v15]) &
s[v15]) )
```

exp：

```
table1 = [0x9c, 0x70, 0x43, 0x0bc, 0x3d, 0x8b, 0x6d, 0x15, 0x26, 0x9c, 0xb8,
0x43, 0x48, 0xb4, 0x6f, 0xa1, 0xb1, 0x5b, 0xb5,
0x6, 0x4b, 0x15, 0x84, 0x70, 0x2d, 0x55, 0x56, 0xc1, 0x1a, 0xc7, 0x58, 0x8f,
0x70, 0x70]
table1 += [0] * 14
```

```
table2 = [0xf4, 0x16, 0x24, 0xd2, 0x24, 0xeb, 0x43, 0x50, 0x62, 0xf3, 0x8f,
0x11, 0x65, 0x92, 0x50, 0xd3, 0xf1, 0x1, 0xb7, 0x55,
0x1a, 0x72, 0xb7, 0xc5, 0x30, 0x1a, 0x0e, 0xe9, 0x17, 0x89, 0x6, 0xe2, 0xf5,
0xec]

s = ''
for v15 in range(len(table2)):
    for j in range(33, 128):
        a = table2[v15] != (~j & (v15 + table1[v15]) | ~(v15 + table1[v15]) & j)
        if a == False:
            s += chr(j)
print(s)
```

> hgame{0LLVM_1S-c0mpLEX-But~5!mpLe}