```
week2 0yster's writeup
```

> 这周做得很水，好多题都是一路做到最后就是卡住没出结果。菜是原罪不多说，不过端正态度想想题目虽然没做出来，但是期间学到了许多姿势和知识，至少也不是一无所获。

re

Pro的Python教室(二)

下下来的pyc拿去在线反编译得到代码：

```
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
        continue
    enc1.append(chr(ord(enc[i]) + 2))

s1 = []
for x in range(3):
    for i in range(len):
        if (i + x) % 3 == 0:
            s1.append(enc1[i])
            continue

enc2 = enc2.join(s1)
if enc2 in aaa:
    print "You 're Right!"
else:
    print "You're Wrong!"
```

分析代码可知：输入流奇数位的字符的ASCII码加1，偶数位的加2。然后隔了3位重组字符串。
那对应写解密脚本，就是先三位三位取出然后重组得到字符ASCII码改变的字符串，然后字符串每个字符按奇偶位对ASCII码进行操作反推出flag。

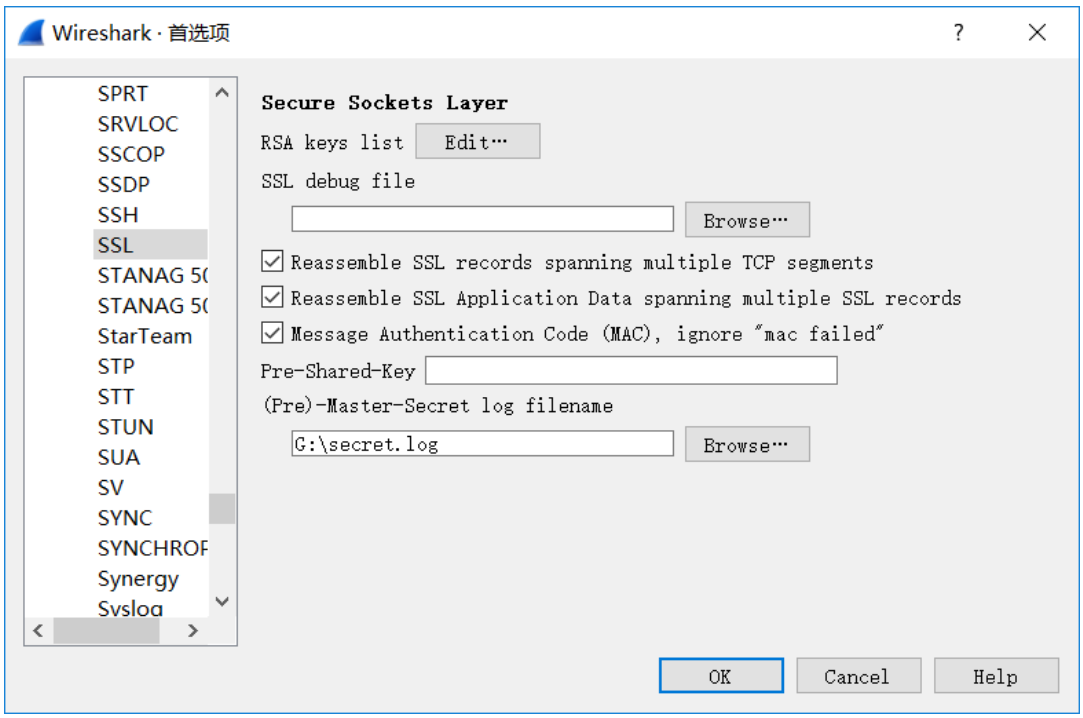
```
#coding=utf-8
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
enc1=[]
flag=[]

for i in range(9):
    enc1.append(aaa[i])
    enc1.append(aaa[i+18])
    enc1.append(aaa[i + 9])

for j in range(len(enc1)):
    if j % 2 == 0:
        flag.append(chr(ord(enc1[j])-1))
        continue
    flag.append(chr(ord(enc1[j]) - 2))
print ''.join(flag)
```

跑出来结果hgame{Now_Y0u_got_th3_PYC!}

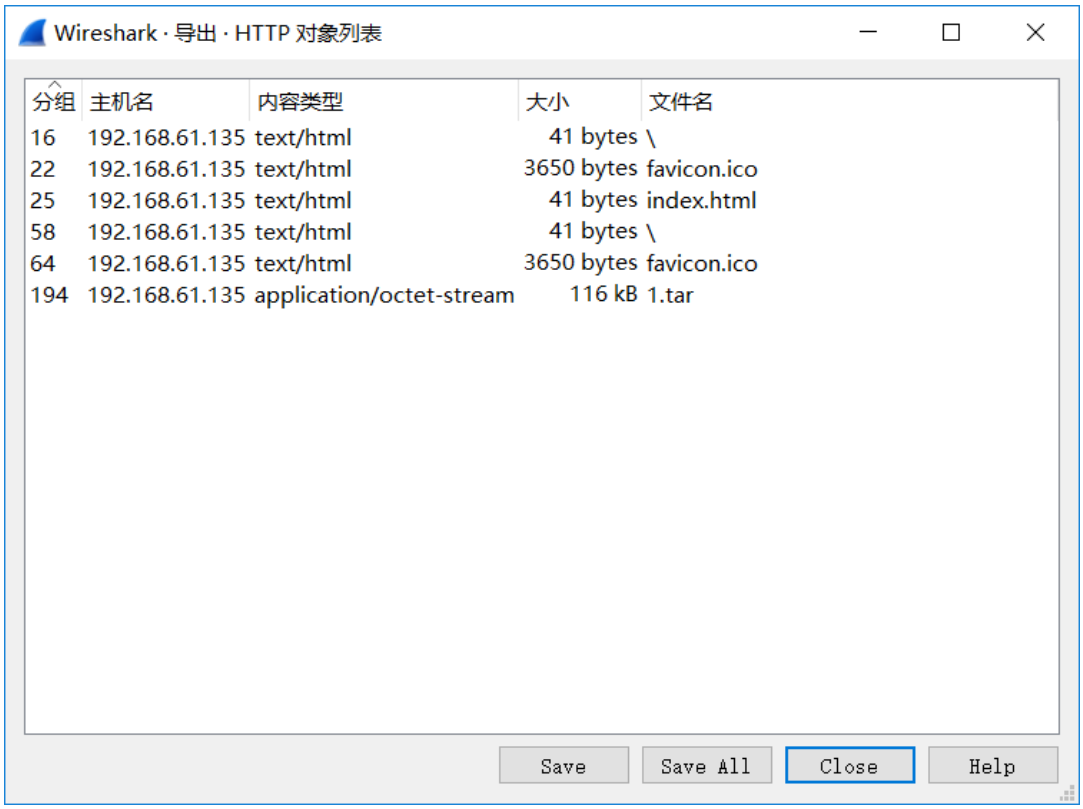
misc

找得到我嘛？小火汁

下载得到的流量包打开，先导出对象无果。于是按16进制搜索zip特征头，找到一个压缩包。提取出来，里面的文件是secret.log。经谷歌，猜测是解密https的密钥。
编辑首选项，在ssl协议出将secret.log导入



此时尝试导出对象，发现多出1.tar这个文件



里面的文件在winhex下打开找到flag

crypto

Vigener~

打开复制，直接找个解密网站
这里真的是没有比较，没有伤害。vigener在线无密钥解密的网站，百度找死没找到，谷歌一查就出。
https://www.kidclark.com/vigener/