2021年江西工业互联网安全技术技能大赛线下决赛部分Writeup

原创

末 初 于 2021-10-19 18:00:17 发布 373 收藏 1

分类专栏： CTF_MISC_Writeup 文章标签： 2021江西工业互联网安全决赛

本文链接：https://blog.csdn.net/mochu7777777/article/details/120782921

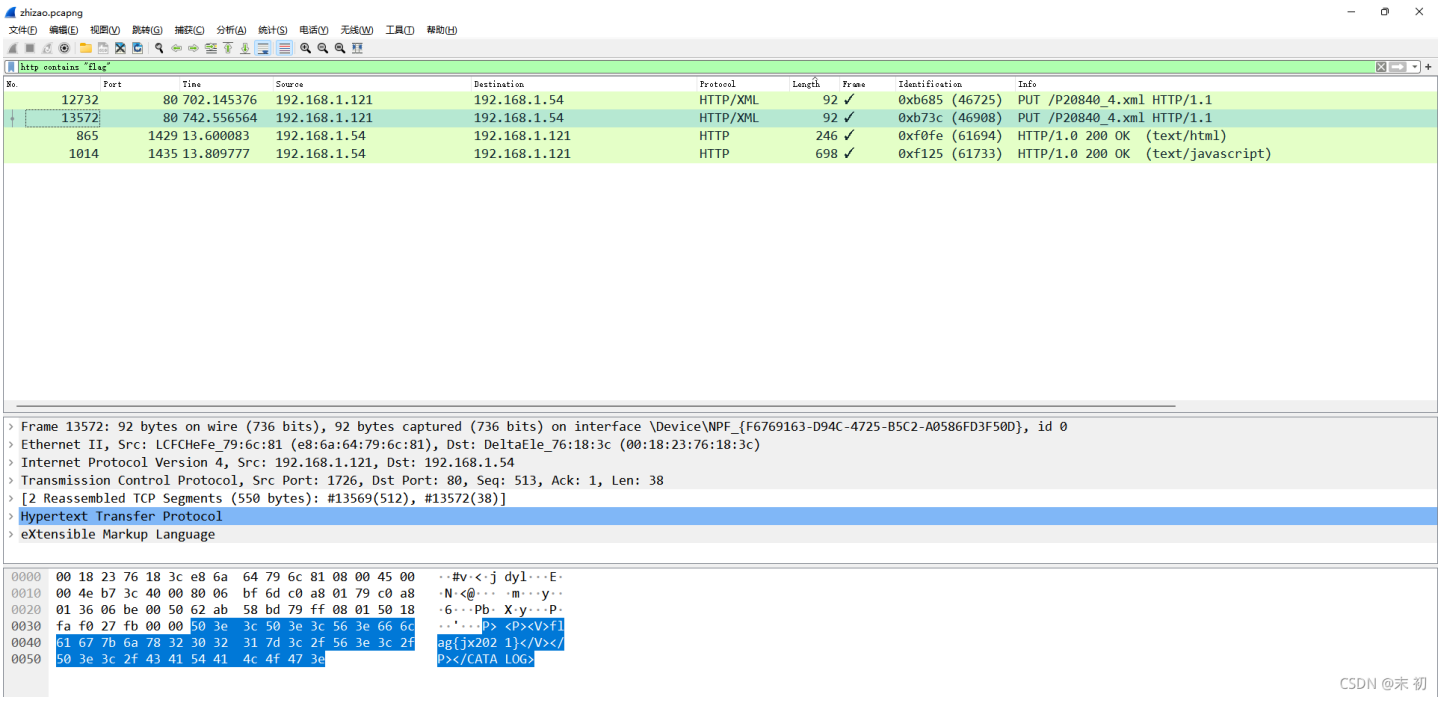
文章目录

```
题目附件自取
链接：https://pan.baidu.com/s/17TagYh6oxZhePWeh36g9YA
提取码：ky47
```

智能制造

签到题，直接查找http流量包中的关键字

```
http contains "flag"
```



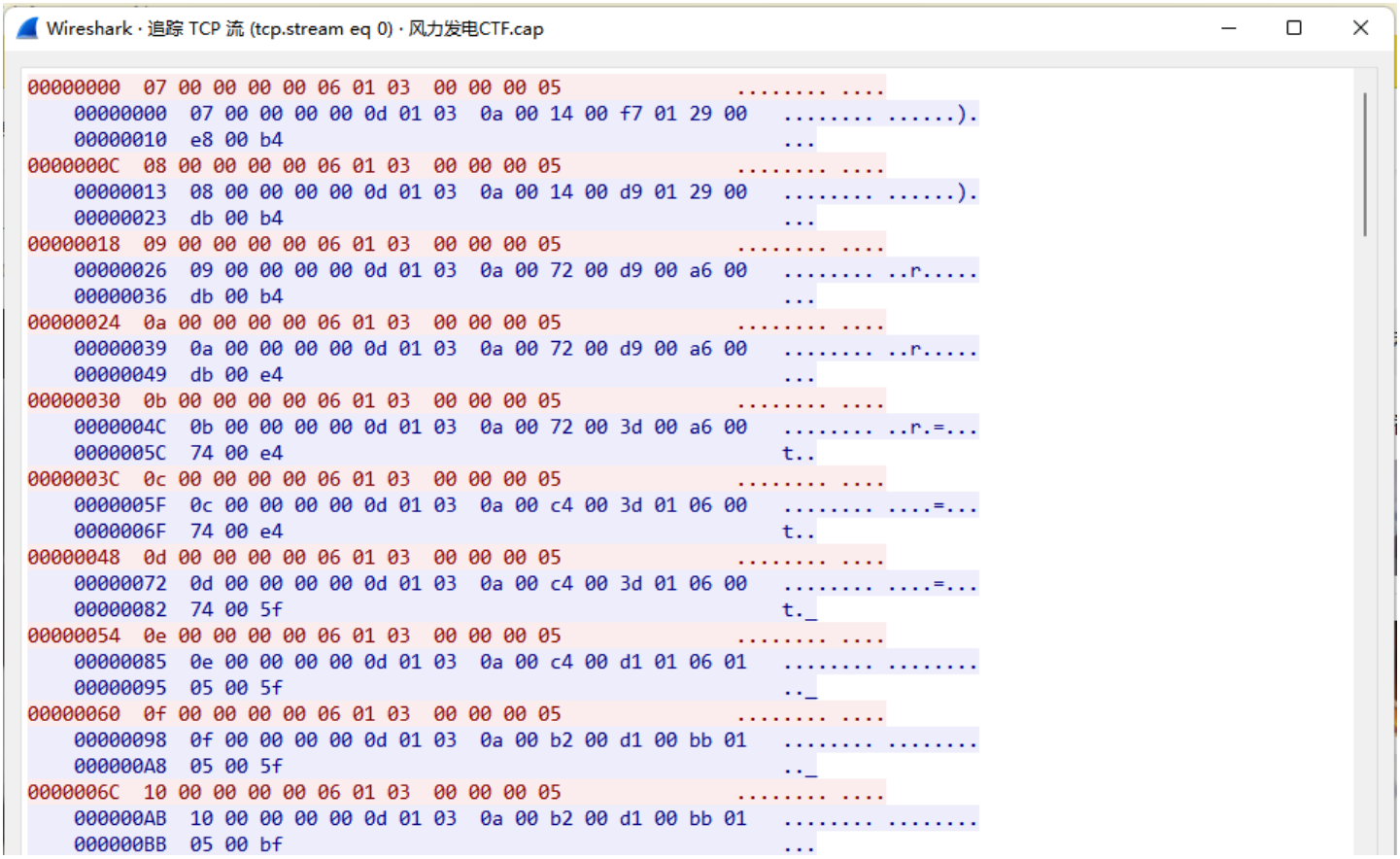

```
flag{jx2021}
```

风力发电

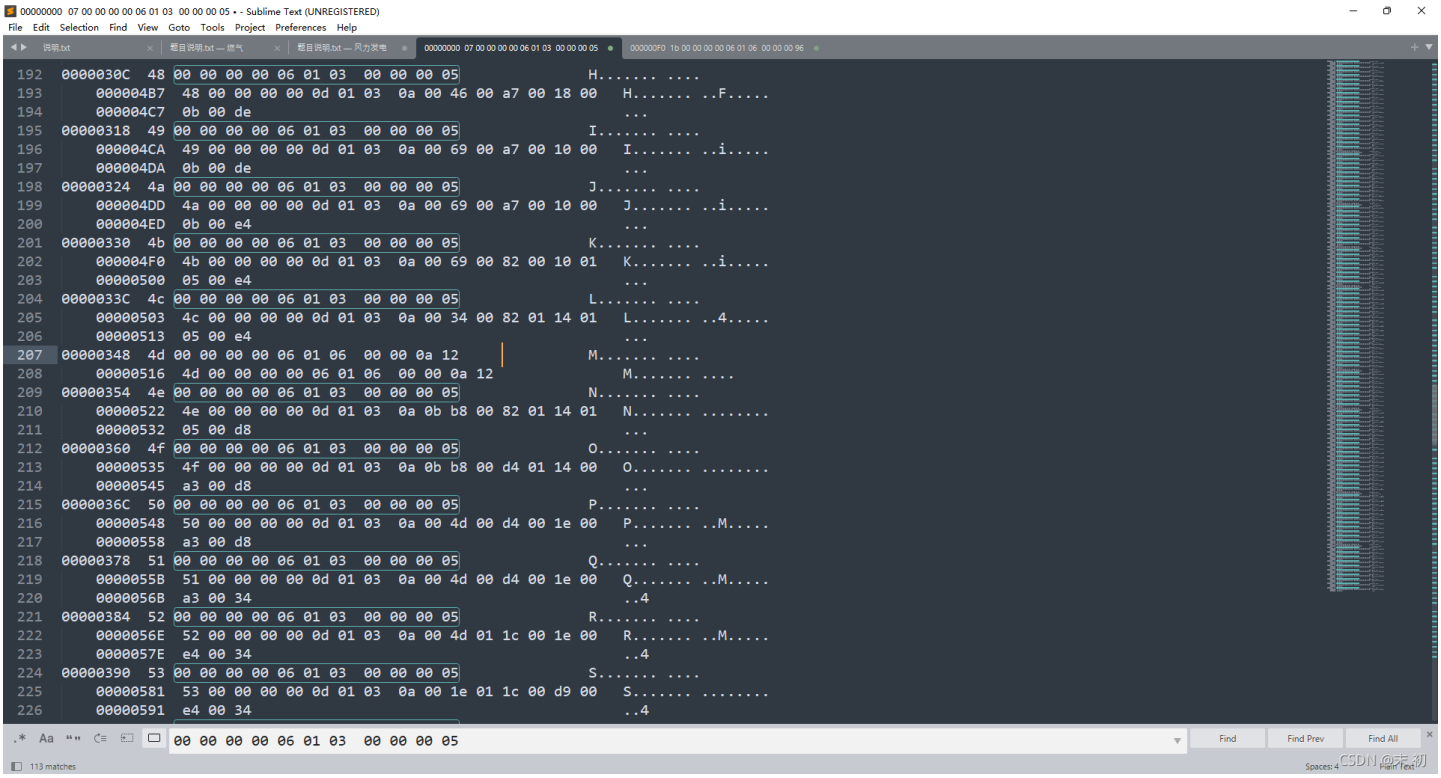
题目描述

```
风力发电机平时正常转速2500转每分钟，但有一天风力发电机转速异常，请从流量包中找出异常的转速流量之和。
```

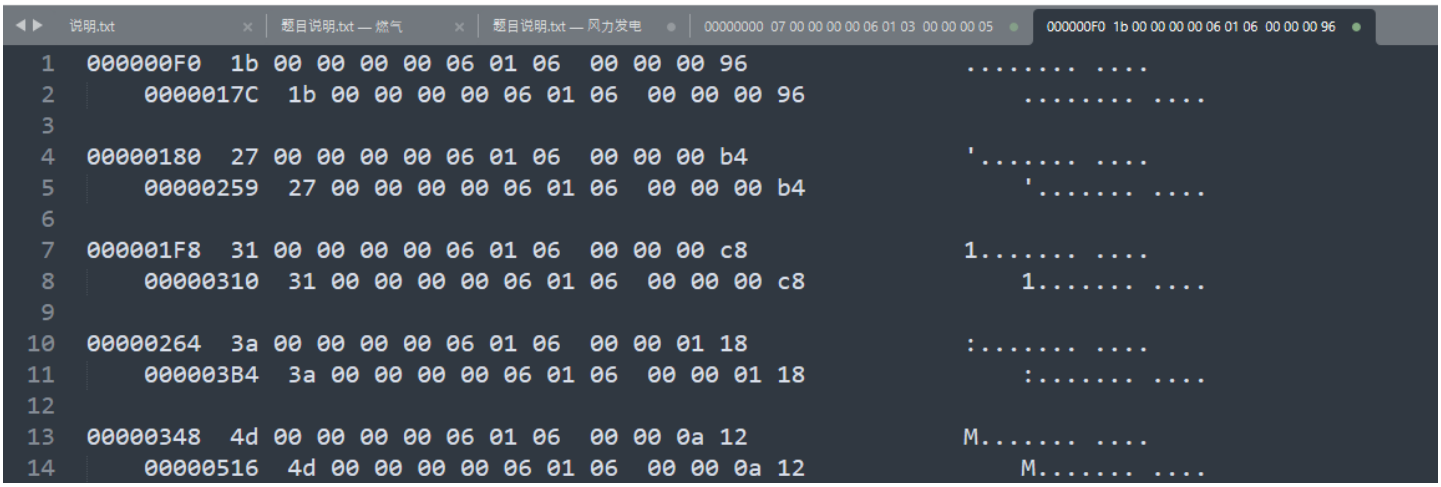
TCP总共14个流，其中有几个流有一些十六进制字符数据，转换字符没发现什么线索，也没发现什么规律，然后用`Hex 转储`发现第一个流的数据存在规律



WireShark 不方便做查找，复制到 Sublime 发现绝大多条数据都是以 00 00 00 00 06 01 03 00 00 00 05 开头



只有八组数据例外，并且长度也少了七个字节



```
15
16  000003B4  56 00 00 00 00 06 01 06  00 00 00 c8              V....... ....
17      000005BA  56 00 00 00 00 06 01 06  00 00 00 c8              V....... ....
18
19  00000498  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
20      0000071C  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
21
22  00000528  75 00 00 00 00 06 01 06  00 00 01 2b              u....... ...+
23      000007F9  75 00 00 00 00 06 01 06  00 00 01 2b              u....... ...+
```

CSDN @末 初

这八组数据除去开头的一些序号之外，都是以 `00 00 00 00 06 01 06 00 00` 开头的，只有末尾两个字节不同

```
1   000000F0  1b 00 00 00 00 06 01 06  00 00 00 96              ........ ....
2       0000017C  1b 00 00 00 00 06 01 06  00 00 00 96              ........ ....
3
4   00000180  27 00 00 00 00 06 01 06  00 00 00 b4              '....... ....
5       00000259  27 00 00 00 00 06 01 06  00 00 00 b4              '....... ....
6
7   000001F8  31 00 00 00 00 06 01 06  00 00 00 c8              1....... ....
8       00000310  31 00 00 00 00 06 01 06  00 00 00 c8              1....... ....
9
10  00000264  3a 00 00 00 00 06 01 06  00 00 01 18              :....... ....
11      000003B4  3a 00 00 00 00 06 01 06  00 00 01 18              :....... ....
12
13  00000348  4d 00 00 00 00 06 01 06  00 00 0a 12              M....... ....
14      00000516  4d 00 00 00 00 06 01 06  00 00 0a 12              M....... ....
15
16  000003B4  56 00 00 00 00 06 01 06  00 00 00 c8              V....... ....
17      000005BA  56 00 00 00 00 06 01 06  00 00 00 c8              V....... ....
18
19  00000498  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
20      0000071C  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
21
22  00000528  75 00 00 00 00 06 01 06  00 00 01 2b              u....... ...+
23      000007F9  75 00 00 00 00 06 01 06  00 00 01 2b              u....... ...+
```

CSDN @末 初

但是直接一起相加起来不对，继续分析

```
206     00000513  05 00 e4                                          ...
207 00000348  4d 00 00 00 00 06 01 06  00 00 0a 12              M....... ....
208     00000516  4d 00 00 00 00 06 01 06  00 00 0a 12              M....... ....
209 00000354  4e 00 00 00 00 06 01 03  00 00 00 05              N....... ....
210     00000522  4e 00 00 00 00 0d 01 03  0a 0b b8 00 82 01 14 01   N....... ........
211     00000532  05 00 d8                                          ...
212 00000360  4f 00 00 00 00 06 01 03  00 00 00 05              O....... ....
213     00000535  4f 00 00 00 00 0d 01 03  0a 0b b8 00 d4 01 14 00   O....... ........
214     00000545  a3 00 d8                                          ...
```

CSDN @末 初

```
233 000003B4  56 00 00 00 00 06 01 06  00 00 00 c8              V....... ....
234     000005BA  56 00 00 00 00 06 01 06  00 00 00 c8              V....... ....
235 000003C0  57 00 00 00 00 06 01 03  00 00 00 05              W....... ....
236     000005C6  57 00 00 00 00 0d 01 03  0a 00 c8 00 91 00 46 00   W....... ......F.
237     000005D6  5a 00 86                                          Z..
238 000003CC  58 00 00 00 00 06 01 03  00 00 00 05              X....... ....
239     000005D9  58 00 00 00 00 0d 01 03  0a 00 c8 00 91 00 46 00   X....... ......F.
240     000005E9  5a 00 2d                                          Z.-
```

CSDN @末 初

```
289  00000498  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
290      0000071C  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
291  000004A4  6a 00 00 00 00 06 01 03  00 00 00 05              j....... ....
292      00000728  6a 00 00 00 00 0d 01 03  0a 01 f4 00 5b 00 5a 00   j....... ....[.Z.
293      00000738  8b 00 b0                                          ...
294  000004B0  6b 00 00 00 00 06 01 03  00 00 00 05              k....... ....
295      0000073B  6b 00 00 00 00 0d 01 03  0a 01 f4 00 5b 00 5a 00   k....... ....[.Z.
296      0000074B  8b 00 0f                                          ...
297  000004BC  6c 00 00 00 00 06 01 03  00 00 00 05              l....... ....
298      0000074E  6c 00 00 00 00 0d 01 03  0a 01 f4 00 4e 00 5a 01   l....... ....N.Z.
299      0000075E  0e 00 0f                                          ...
```



```
61  000000F0  1b 00 00 00 00 06 01 06  00 00 00 96              ........ ....
62      0000017C  1b 00 00 00 00 06 01 06  00 00 00 96              ........ ....
63  000000FC  1c 00 00 00 00 06 01 03  00 00 00 05              ........ ....
64      00000188  1c 00 00 00 00 0d 01 03  0a 00 96 00 df 01 13 00   ........ ........
65      00000198  b4 00 31                                          ..1
66  00000108  1d 00 00 00 00 06 01 03  00 00 00 05              ........ ....
67      0000019B  1d 00 00 00 00 0d 01 03  0a 00 96 00 df 01 13 00   ........ ........
68      000001AB  b4 00 3f                                          ..?
69  00000114  1e 00 00 00 00 06 01 03  00 00 00 05              ........ ....
70      000001AE  1e 00 00 00 00 0d 01 03  0a 00 96 00 a5 01 13 00   ........ ........
71      000001BE  70 00 3f                                          p.?
```

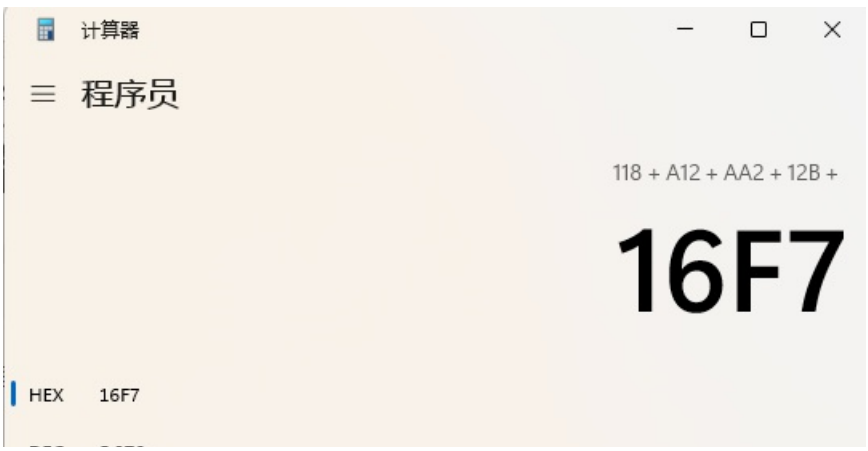

发现这八组数据有些数据之后的几条数据的后一段大部分为`0a 00`，少部分为`0a 01`或`0a 0b`，将后部分数据为`0a 00`的从八组里面去除，只剩下四组

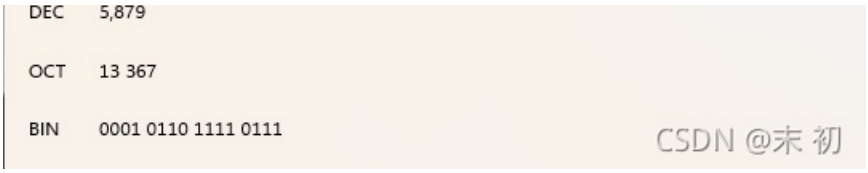
00000264 3a 00 00 00 00 06 01 06 00 00 01 18 • - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

说明.txt | 题目说明.txt — 燃气 | 题目说明.txt — 风力发电 | 00000000 07 00 00 00 00 06 01 03 00 00 00 05 | 00000264 3a 00 00 00 00 06 01 06 00 00 01 18

```
1   00000264  3a 00 00 00 00 06 01 06  00 00 01 18              :....... ....
2       000003B4  3a 00 00 00 00 06 01 06  00 00 01 18              :....... ....
3
4   00000348  4d 00 00 00 00 06 01 06  00 00 0a 12              M....... ....
5       00000516  4d 00 00 00 00 06 01 06  00 00 0a 12              M....... ....
6
7   00000498  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
8       0000071C  69 00 00 00 00 06 01 06  00 00 0a a2              i....... ....
9
10  00000528  75 00 00 00 00 06 01 06  00 00 01 2b              u....... ...+
11      000007F9  75 00 00 00 00 06 01 06  00 00 01 2b              u....... ...+
```

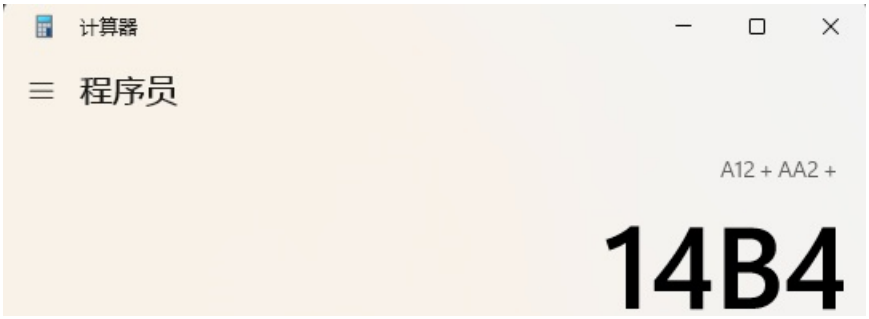





这样加起来转速`5879`也不对，继续分析，每分钟2500转

转换成十六进制就是`09 C4`，这里四组的后两位字节如果真是转速，那么根据转速可大致分为两类`0a xx`和`01 xx`，对比`09 C4`一快一慢；OK，那么根据快慢分两组加起来

得到每分钟转速：`579`



HEX	14B4
DEC	5,300
OCT	12 264
BIN	0001 0100 1011 0100

得到每分钟转速：`5300`
最终flag为

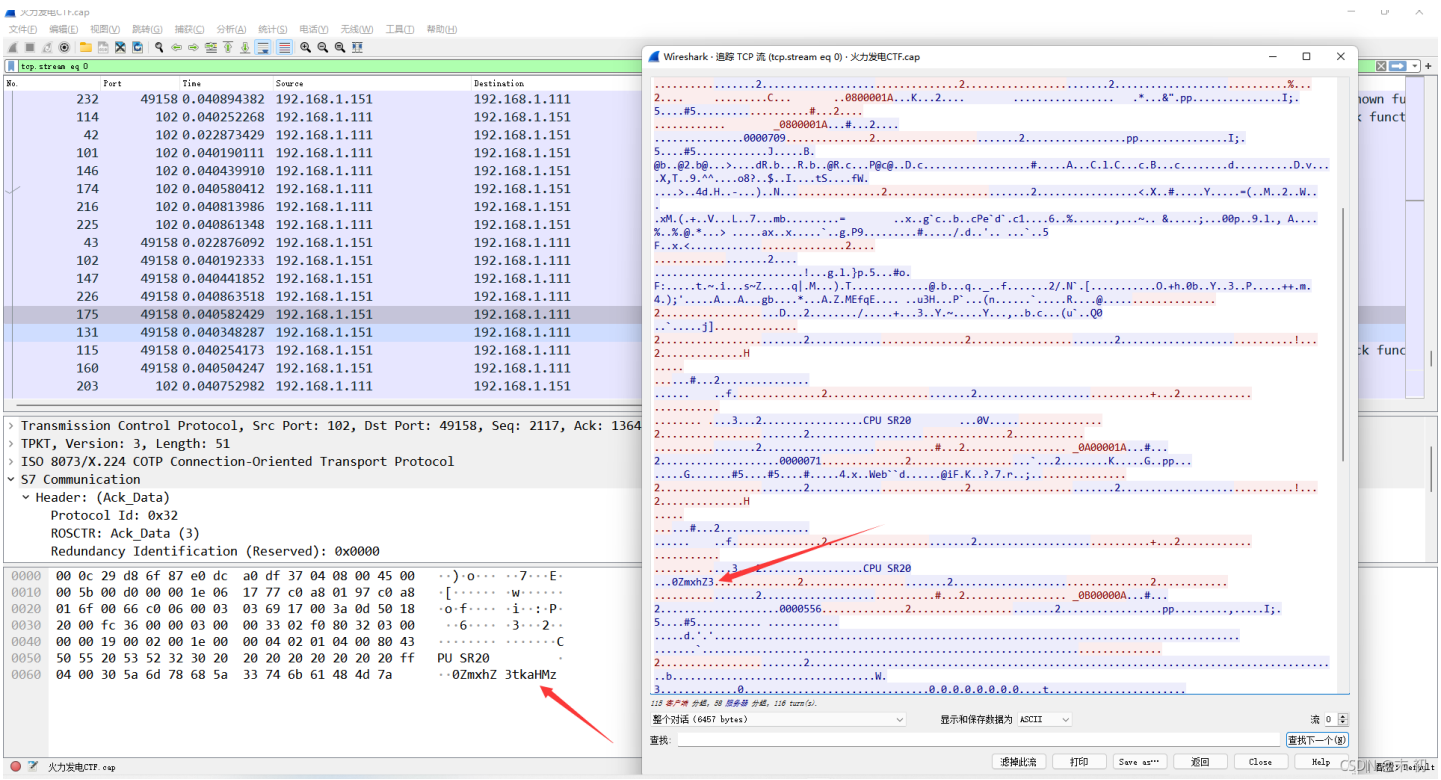
```
flag{5300}
```

火力发电厂

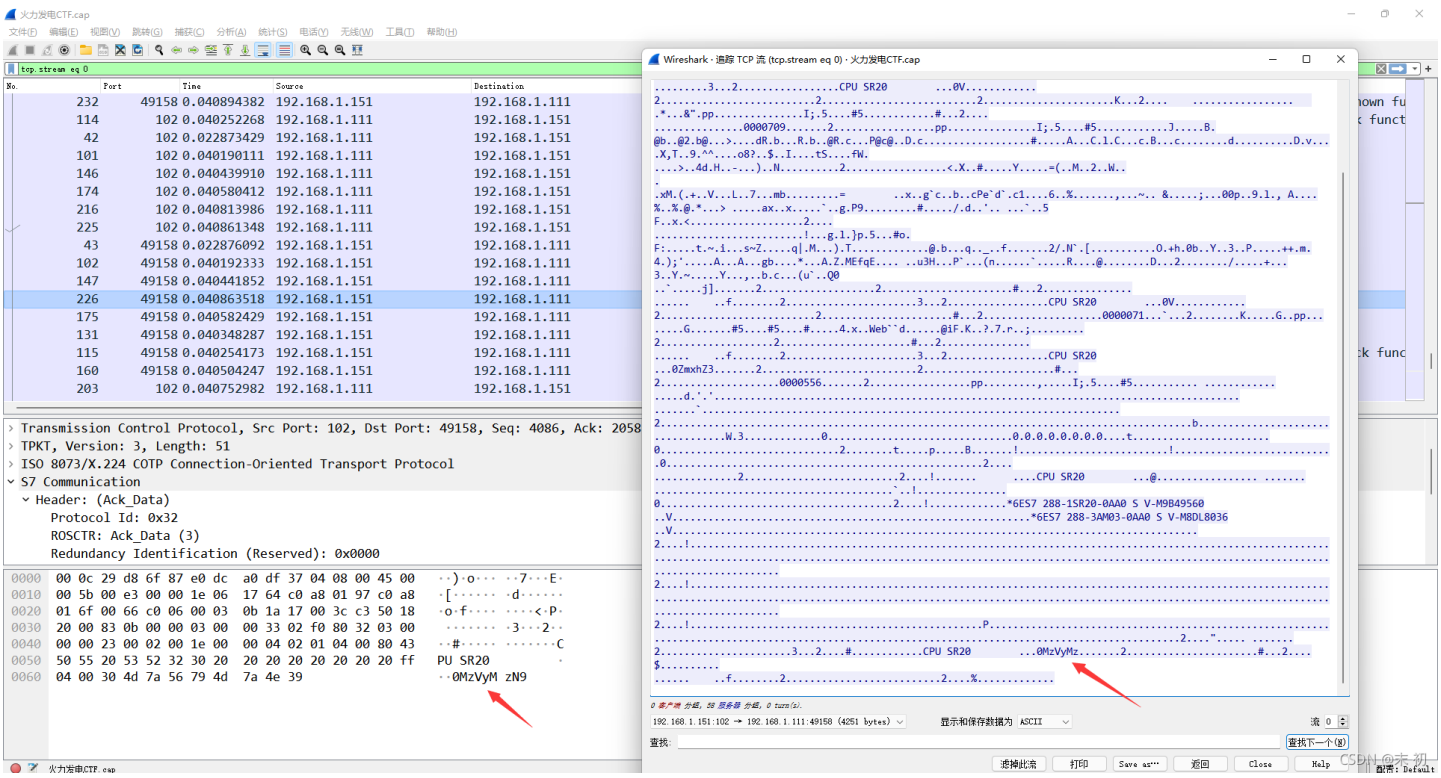
题目描述

```
找到流量中的flag数据
```

只有一个`TCP`流，在其中发现了很明显的flag字符的base64编码开头；鼠标点击到流中字符串的位置回跳转到该字符存在的包中



后面还发现一串，都是以0开头的，容易辨识



拼接起来

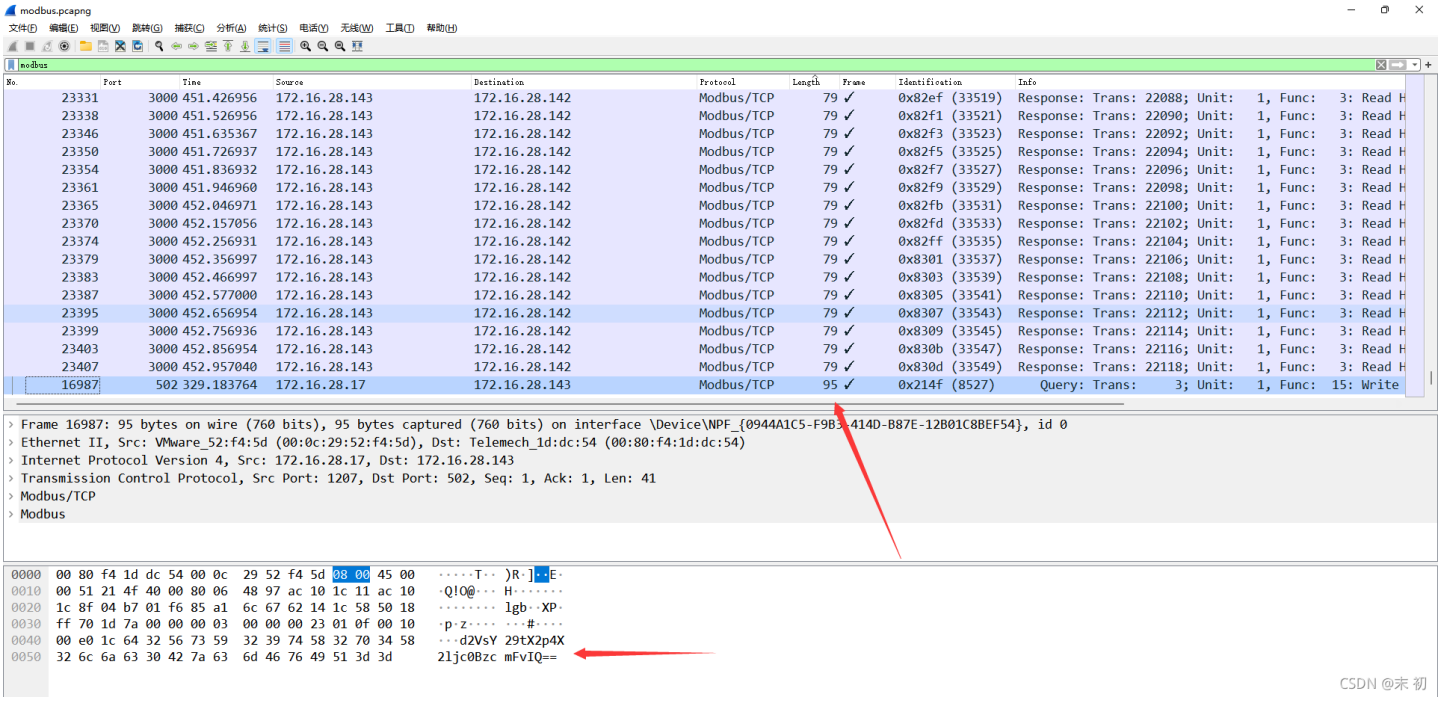
```
>>> from base64 import *
>>> b64decode('ZmxhZ3tkaHMzMzVyMzN9')
b'flag{dhs335r33}'
```

智慧城市

题目描述

```
找到流量中隐藏的flag
```

签到题，过滤出Modbus协议，按长度排序




```
>>> from base64 import *
>>> b64decode('d2VsY29tX2p4X2ljc0BzcmFvIQ==')
b'welcom_jx_ics@srao!'
```

```
flag{welcom_jx_ics@srao!}
```