




# 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

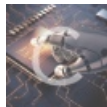
末初  于 2021-10-19 18:00:17 发布  373  收藏 1

分类专栏: [CTF\\_MISC\\_Writeup](#) 文章标签: [2021江西工业互联网安全决赛](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

246 篇文章 46 订阅

订阅专栏

### 文章目录

[智能制造](#)

[风力发电](#)

[火力发电厂](#)

[智慧城市](#)

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"
```

zhizao.pcapng

文件(F) 编辑(E) 视图(V) 网络(N) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(O) 帮助(H)

http contains "flag"

No.	Port	Time	Source	Destination	Protocol	Length	Frame	Identification	Info
12732	80	702.145376	192.168.1.121	192.168.1.54	HTTP/XML	92	✓	0xb685 (46725)	PUT /P20840_4.xml HTTP/1.1
13572	80	742.556564	192.168.1.121	192.168.1.54	HTTP/XML	92	✓	0xb73c (46908)	PUT /P20840_4.xml HTTP/1.1
865	1429	13.600083	192.168.1.54	192.168.1.121	HTTP	246	✓	0xf0fe (61694)	HTTP/1.0 200 OK (text/html)
1014	1435	13.809777	192.168.1.54	192.168.1.121	HTTP	698	✓	0xf125 (61733)	HTTP/1.0 200 OK (text/javascript)

> Frame 13572: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF\_{F6769163-D94C-4725-B5C2-A0586FD3F50D}, id 0  
 > Ethernet II, Src: LCFChEFe\_79:6c:81 (e8:6a:64:79:6c:81), Dst: DeltaEle\_76:18:3c (00:18:23:76:18:3c)  
 > Internet Protocol Version 4, Src: 192.168.1.121, Dst: 192.168.1.54  
 > Transmission Control Protocol, Src Port: 1726, Dst Port: 80, Seq: 513, Ack: 1, Len: 38  
 > [2 Reassembled TCP Segments (550 bytes): #13569(512), #13572(38)]  
 > Hypertext Transfer Protocol  
 > eXtensible Markup Language

```

0000 00 18 23 76 18 3c e8 6a 64 79 6c 81 08 00 45 00  ..#v<-j dyl...E-
0010 00 4e b7 3c 40 00 80 06 bf 6d c0 a8 01 79 c0 a8  ..N<@...m...y..
0020 01 36 06 be 00 50 62 ab 58 bd 79 ff 08 01 50 18  ..6...Pb..X.y...P-
0030 fa f0 27 fb 00 00 50 3e 3c 50 3e 3c 56 3e 66 6e  ...'...P> <P><V>fj
0040 61 67 7b 6a 78 32 30 32 31 7d 3c 2f 56 3e 3c 2f  ag{jx202 1}<V><f
0050 50 3e 3c 2f 43 41 54 41 4c 4f 47 3e                P><<CAIA LOG
  
```

CSDN @未初

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

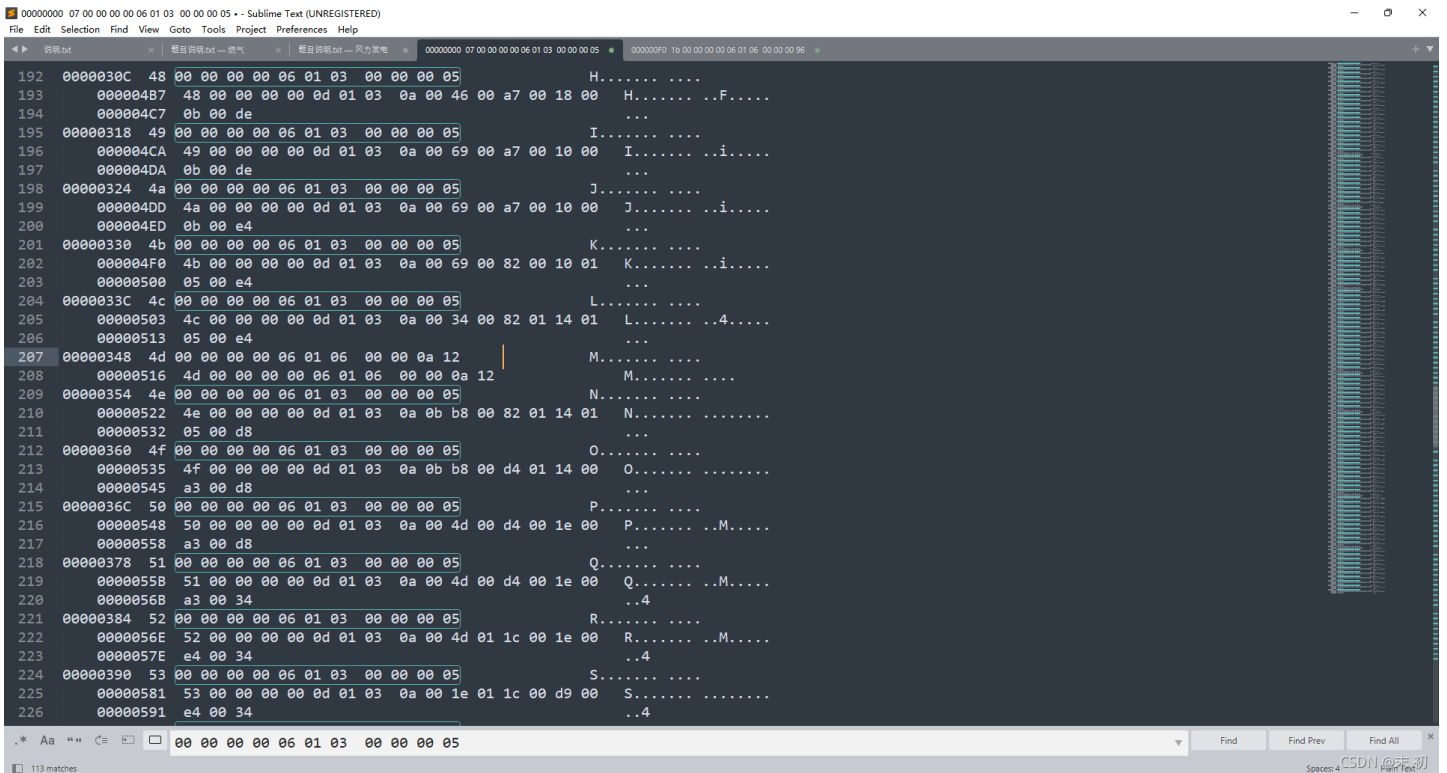
Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · 风力发电CTF.cap

```

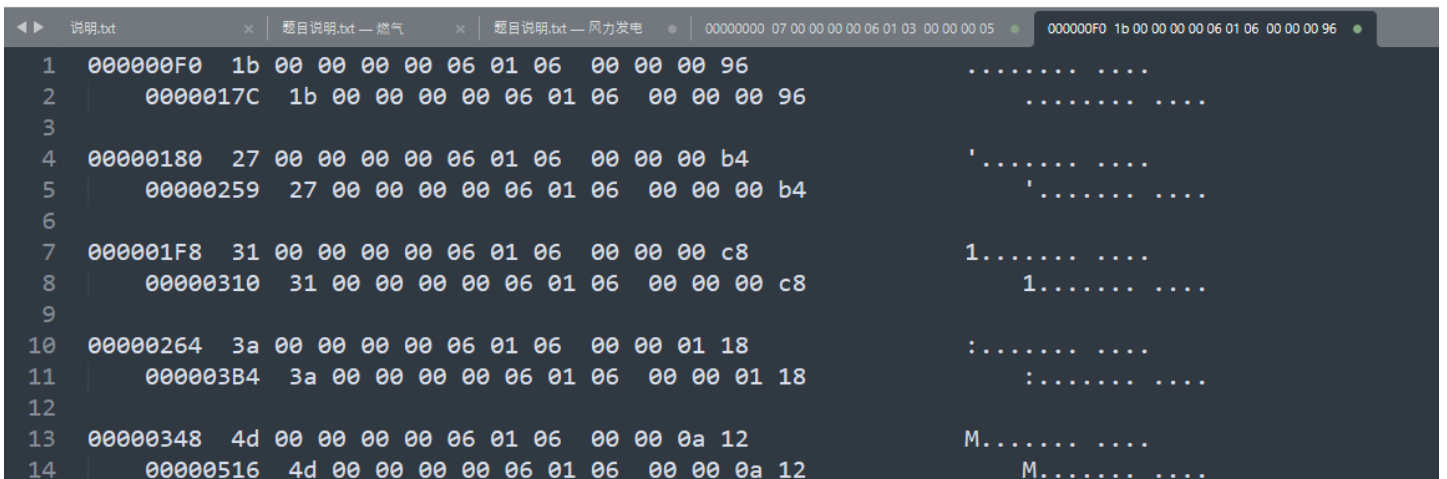
00000000 07 00 00 00 00 06 01 03 00 00 00 05 .....
00000000 07 00 00 00 00 0d 01 03 0a 00 14 00 f7 01 29 00 .....).
00000010 e8 00 b4 ...
0000000c 08 00 00 00 00 06 01 03 00 00 00 05 .....
00000013 08 00 00 00 00 0d 01 03 0a 00 14 00 d9 01 29 00 .....).
00000023 db 00 b4 ...
00000018 09 00 00 00 00 06 01 03 00 00 00 05 .....
00000026 09 00 00 00 00 0d 01 03 0a 00 72 00 d9 00 a6 00 .....r....
00000036 db 00 b4 ...
00000024 0a 00 00 00 00 06 01 03 00 00 00 05 .....
00000039 0a 00 00 00 00 0d 01 03 0a 00 72 00 d9 00 a6 00 .....r....
00000049 db 00 e4 ...
00000030 0b 00 00 00 00 06 01 03 00 00 00 05 .....
0000004c 0b 00 00 00 00 0d 01 03 0a 00 72 00 3d 00 a6 00 .....r.=...
0000005c 74 00 e4 t..
0000003c 0c 00 00 00 00 06 01 03 00 00 00 05 .....
0000005f 0c 00 00 00 00 0d 01 03 0a 00 c4 00 3d 01 06 00 .....=...
0000006f 74 00 e4 t..
00000048 0d 00 00 00 00 06 01 03 00 00 00 05 .....
00000072 0d 00 00 00 00 0d 01 03 0a 00 c4 00 3d 01 06 00 .....=...
00000082 74 00 5f t._
00000054 0e 00 00 00 00 06 01 03 00 00 00 05 .....
00000085 0e 00 00 00 00 0d 01 03 0a 00 c4 00 d1 01 06 01 .....
00000095 05 00 5f .._
00000060 0f 00 00 00 00 06 01 03 00 00 00 05 .....
00000098 0f 00 00 00 00 0d 01 03 0a 00 b2 00 d1 00 bb 01 .....
000000a8 05 00 5f .._
0000006c 10 00 00 00 00 06 01 03 00 00 00 05 .....
000000ab 10 00 00 00 00 0d 01 03 0a 00 b2 00 d1 00 bb 01 .....
000000bb 05 00 bf ...
  
```



Wireshark 不方便做查找，复制到 Sublime 发现绝大多数数据都是以 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 ...

```

CSDN @未初

```

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.?

```

CSDN @未初

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

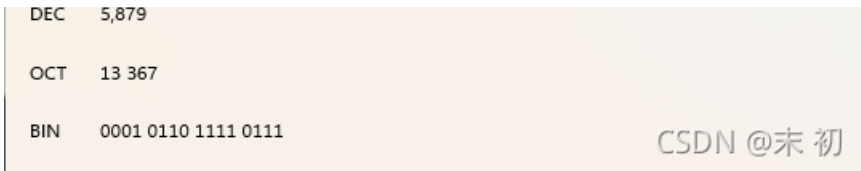
```

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 x 题目说明.txt — 燃气 x 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.....

```

CSDN @未初





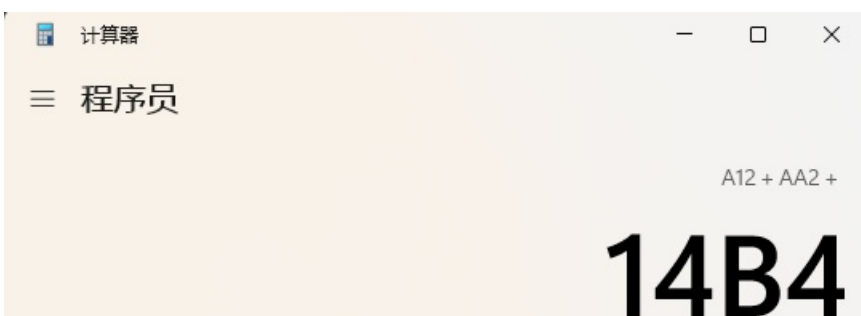
这样加起来转速 5879 也不对，继续分析，每分钟2500转



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

CSDN @末初

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

The image shows a Wireshark capture of a TCP stream. The left pane displays a list of packets, with packet 175 selected. The middle pane shows the details of the selected packet, including the S7 Communication header and the raw data. The right pane shows the raw data in hexadecimal and ASCII. A red arrow points to the Base64 encoded string '3tkalMz' in the raw data pane, which corresponds to the flag '3tkalMz'.

No.	Port	Time	Source	Destination
232	49158	0.040894382	192.168.1.151	192.168.1.111
114	102	0.040252268	192.168.1.111	192.168.1.151
42	102	0.022873429	192.168.1.111	192.168.1.151
101	102	0.040190111	192.168.1.111	192.168.1.151
146	102	0.040439910	192.168.1.111	192.168.1.151
174	102	0.040580412	192.168.1.111	192.168.1.151
216	102	0.040813986	192.168.1.111	192.168.1.151
225	102	0.040861348	192.168.1.111	192.168.1.151
43	49158	0.022876092	192.168.1.151	192.168.1.111
102	49158	0.040192333	192.168.1.151	192.168.1.111
147	49158	0.040441852	192.168.1.151	192.168.1.111
226	49158	0.040863518	192.168.1.151	192.168.1.111
175	49158	0.040582429	192.168.1.151	192.168.1.111
131	49158	0.040348287	192.168.1.151	192.168.1.111
115	49158	0.040254173	192.168.1.151	192.168.1.111
160	49158	0.040504274	192.168.1.151	192.168.1.111
203	102	0.040752982	192.168.1.111	192.168.1.151

Transmission Control Protocol, Src Port: 102, Dst Port: 49158, Seq: 2117, Ack: 1364  
 TPKT, Version: 3, Length: 51  
 ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  
 S7 Communication  
 Header: (Ack\_Data)  
 Protocol Id: 0x32  
 ROSCTR: Ack\_Data (3)  
 Redundancy Identification (Reserved): 0x0000

```

0000 00 0c 29 d8 6f 87 e0 dc a0 df 37 04 08 00 45 00 --)o--- --7---E-
0010 00 5b 00 d0 00 00 1e 06 17 77 c0 a8 01 97 c0 a8 [-.....-w-----
0020 01 6f 00 66 c0 06 00 03 03 69 17 00 3a 0d 50 18 -o-f-----i---:P-
0030 20 00 fc 36 00 00 03 00 00 33 02 f0 80 32 03 00 --6-----3---2--
0040 00 00 19 00 02 00 1e 00 00 04 02 01 04 00 80 43 ---.....-C-----
0050 50 55 20 53 52 32 30 20 20 20 20 20 20 20 ff PU SR20
0060 04 00 30 5a 6d 78 68 5a 33 74 6b 61 48 4d 7a --0ZmxhZ 3tkalMz
  
```

后面还发现一串，都是以0开头的，容易辨识

Wireshark - 捕获 TCP 流 (tcp.stream eq 0) - 火力发电CTF.cap

No.	Port	Time	Source	Destination
232	49158	0.040894382	192.168.1.151	192.168.1.111
114	102	0.040252268	192.168.1.111	192.168.1.151
42	102	0.022873429	192.168.1.111	192.168.1.151
101	102	0.040190111	192.168.1.111	192.168.1.151
146	102	0.040439910	192.168.1.111	192.168.1.151
174	102	0.040580412	192.168.1.111	192.168.1.151
216	102	0.040813986	192.168.1.111	192.168.1.151
225	102	0.040861348	192.168.1.111	192.168.1.151
43	49158	0.022876092	192.168.1.151	192.168.1.111
102	49158	0.040192333	192.168.1.151	192.168.1.111
147	49158	0.040441852	192.168.1.151	192.168.1.111
226	49158	0.040863518	192.168.1.151	192.168.1.111
175	49158	0.040582429	192.168.1.151	192.168.1.111
131	49158	0.040348287	192.168.1.151	192.168.1.111
115	49158	0.040254173	192.168.1.151	192.168.1.111
160	49158	0.040504247	192.168.1.151	192.168.1.111
203	102	0.040752982	192.168.1.111	192.168.1.151

Transmission Control Protocol, Src Port: 102, Dst Port: 49158, Seq: 4086, Ack: 2058  
TPKT, Version: 3, Length: 51  
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  
S7 Communication  
Header: (Ack\_Data)  
Protocol Id: 0x32  
ROSCTR: AckData (3)  
Redundancy Identification (Reserved): 0x0000

```
0000 00 0c 29 d8 6f 87 e0 dc a0 df 37 04 08 00 45 00  ..)o...-7...E-  
0010 00 5b 00 e3 00 00 1e 06 17 64 c0 a8 01 97 c0 a8  [.....d....  
0020 01 6f 00 66 c0 06 00 03 0b 1a 17 00 3c c3 50 18  o.f.....<P-  
0030 20 00 83 0b 00 00 03 00 00 33 02 f0 80 32 03 00  ..#...-3...2-  
0040 00 00 23 00 02 00 1e 00 00 04 02 01 04 00 80 43  ..#.....C  
0050 50 55 20 53 52 32 30 20 20 20 20 20 20 20 ff  PU SR20  
0060 04 00 30 4d 7a 56 79 4d 7a 4e 39                --0MzVyM zN9'
```

拼接起来

```
>>> from base64 import *  
>>> b64decode('ZmxhZ3Z3tkHmZmZyMzN9')  
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

The screenshot shows the Wireshark interface with a list of Modbus/TCP packets. Packet 16987 is selected. The details pane shows the following information:

- Frame 16987: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF\_{0944A1C5-F9B5-414D-B87E-12B01C8BEF54}, id 0
- Ethernet II, Src: VMware\_52:f4:5d (00:0c:29:52:f4:5d), Dst: Telemech\_1d:dc:54 (00:80:f4:1d:dc:54)
- Internet Protocol Version 4, Src: 172.16.28.17, Dst: 172.16.28.143
- Transmission Control Protocol, Src Port: 1207, Dst Port: 502, Seq: 1, Ack: 1, Len: 41
- Modbus/TCP
- Modbus

The hex dump shows the raw data of the packet, with a red arrow pointing to the end of the data: 21jc0Bzc mFvIQ==

CSDN @未初

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

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