[工控CTF]2021工业信息安全技能大赛（江西站）-WP

原创

3tefanie丶zhou 于 2021-09-30 14:43:14 发布 1711 收藏 5

文章标签： 网络安全

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/luochen2436/article/details/120561075

版权

文章目录

西门子S7协议

文件分析

异常流量分析

应急恢复

恶意app分析

工控流量分析

丢失的密码

工业固件分析

opc流量分析

西门子S7协议

0300002402f0803201000000003000e00050501120a100200010000830000000004000801。请解读以上协议内容，并准确的拿到此报文返回值，flag即为返回值。提交格式：flag{xxx}。

查找西门子S7协议资料，发现是一个写操作，根据其报文格式，获拼接出回复报文

写demo3：

1200 写 入：output0=4

PC发出报文分析：

(A[3]~A[4]=0x0024=36=读取报文总长度, A[12]A[13]=0x0008=序列号，A[16]A[17]=0x05=写入byte个数(1)+4 ,A[23]=0x02=写入方式为byte,A[24]~A[25]=0x0001=1=写入个数count; A[26]A[27]=0x0001=DB1(因为是output,所以DB块编号无所谓),A[28]=0x82=写入的数据类型为output，A[29]A[31]=0x000000=读取偏移量offset(bit为单位)A[32]~A[33]=0x0004=写入方式为byte , A[34]~A[35]=0x0008=1*8=写入byte的个数 ,A[36]= 写入数据)

```
03 00 00 24 02 F0 80 32 01 00 00 00 08 00 0E 00 05 05 01 12 0A 10 02 00 01 00 01 82 00 00 00 00 04 00 08 04
```

PLC回复报文分析：

(B[12]~B[13]=0x0565=序列号，最后一个B[14]=0xFF表示写入)

```
03 00 00 16 02 F0 80 32 03 00 00 00 08 00 02 00 01 00 00 05 01 FF
```

写报文：

```
03 00 00 24 02 F0 80 32 01 00 00 00 03 00 0e 00 05 05 01 12 0a 10 02 00 01 00 00 83 00 00 00 00 04 00 08 01
```

回复报文：

```
03 00 00 16 02 F0 80 32 03 00 00 00 03 00 02 00 01 00 00 05 01 FF
```

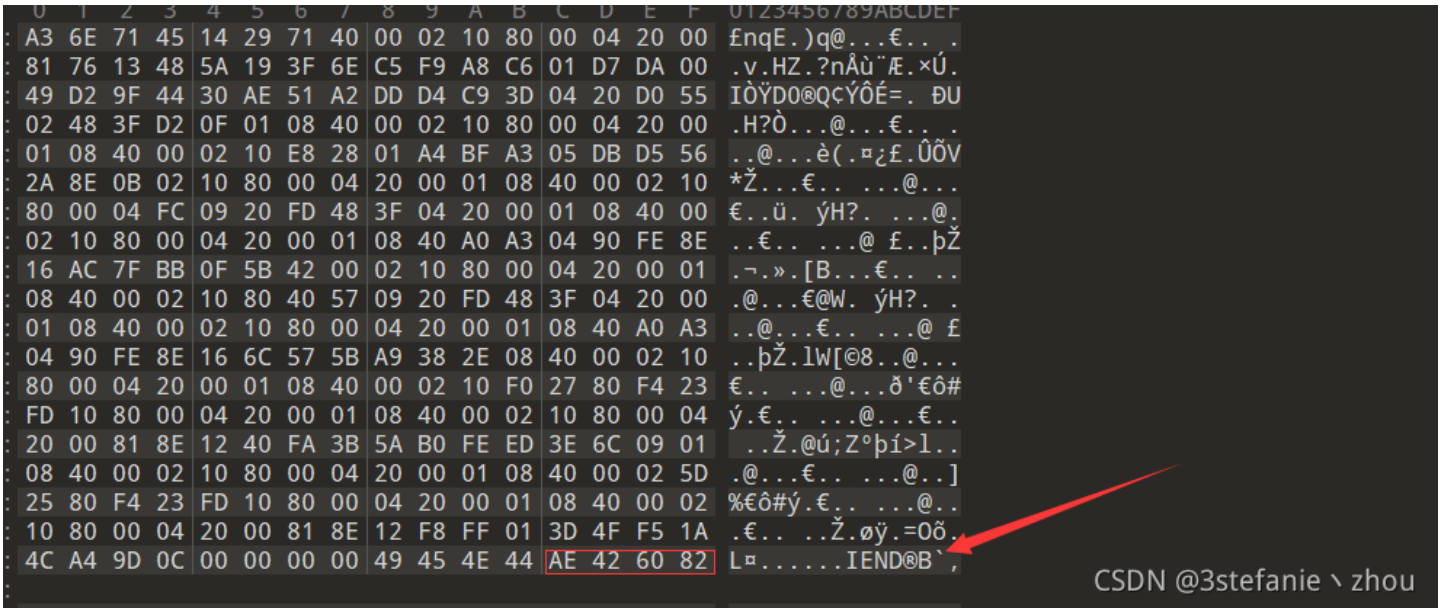
根据题目要求，回复报文作为flag

```
flag{0300001602f0803203000000030002000100000501ff}
```

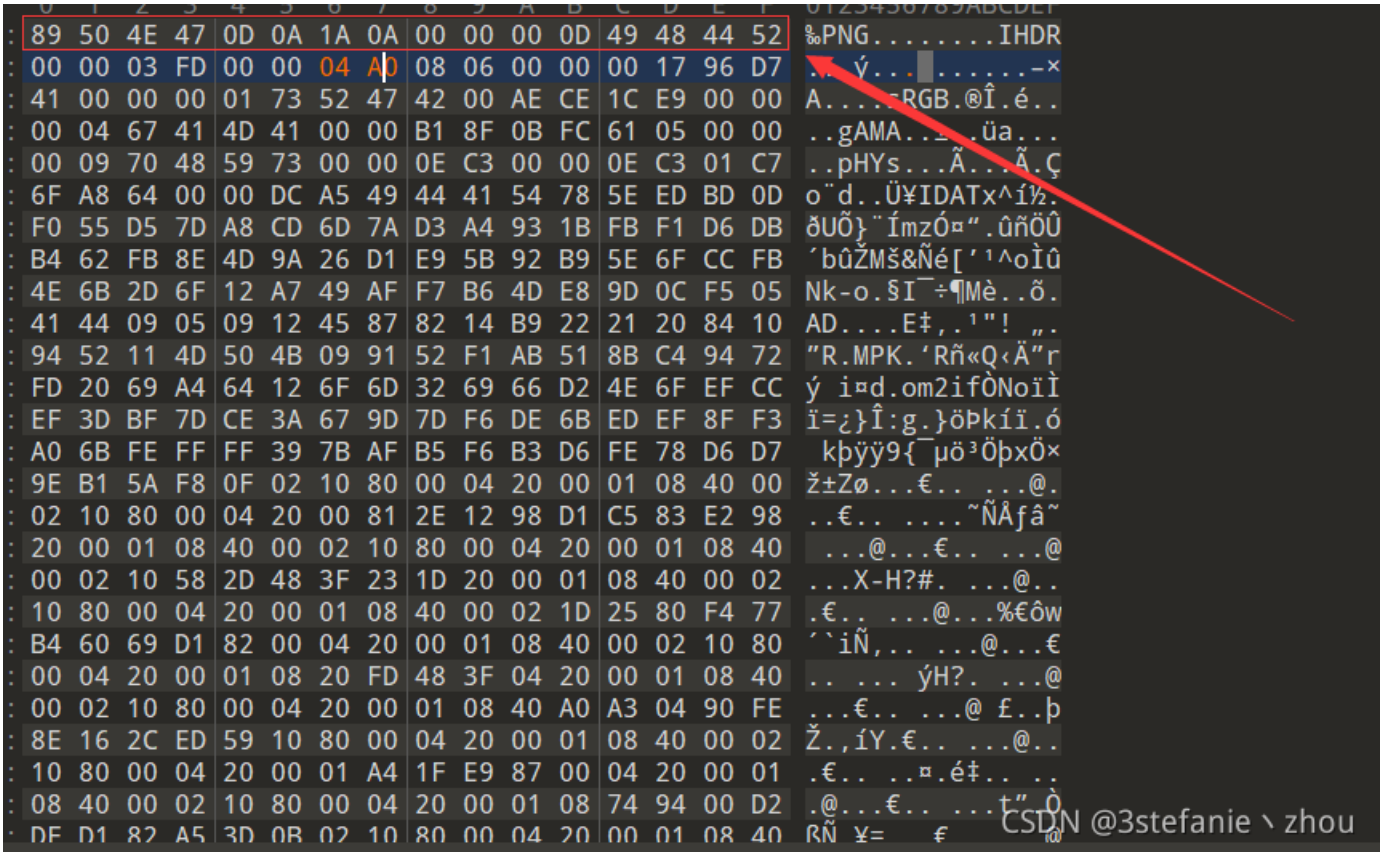
文件分析

hint:这是工艺监控流程文件被人破坏，写入了某些特别的内容，请根据文件，找出其中的flag。提交格式：flag{xxx}。

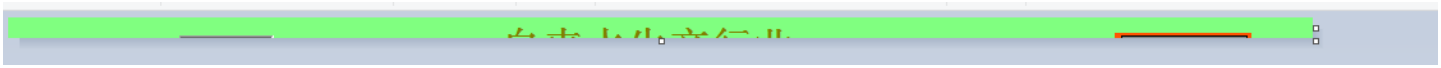
解压文件，得到一个没有后缀名的文件，丢进 010 editor中查看



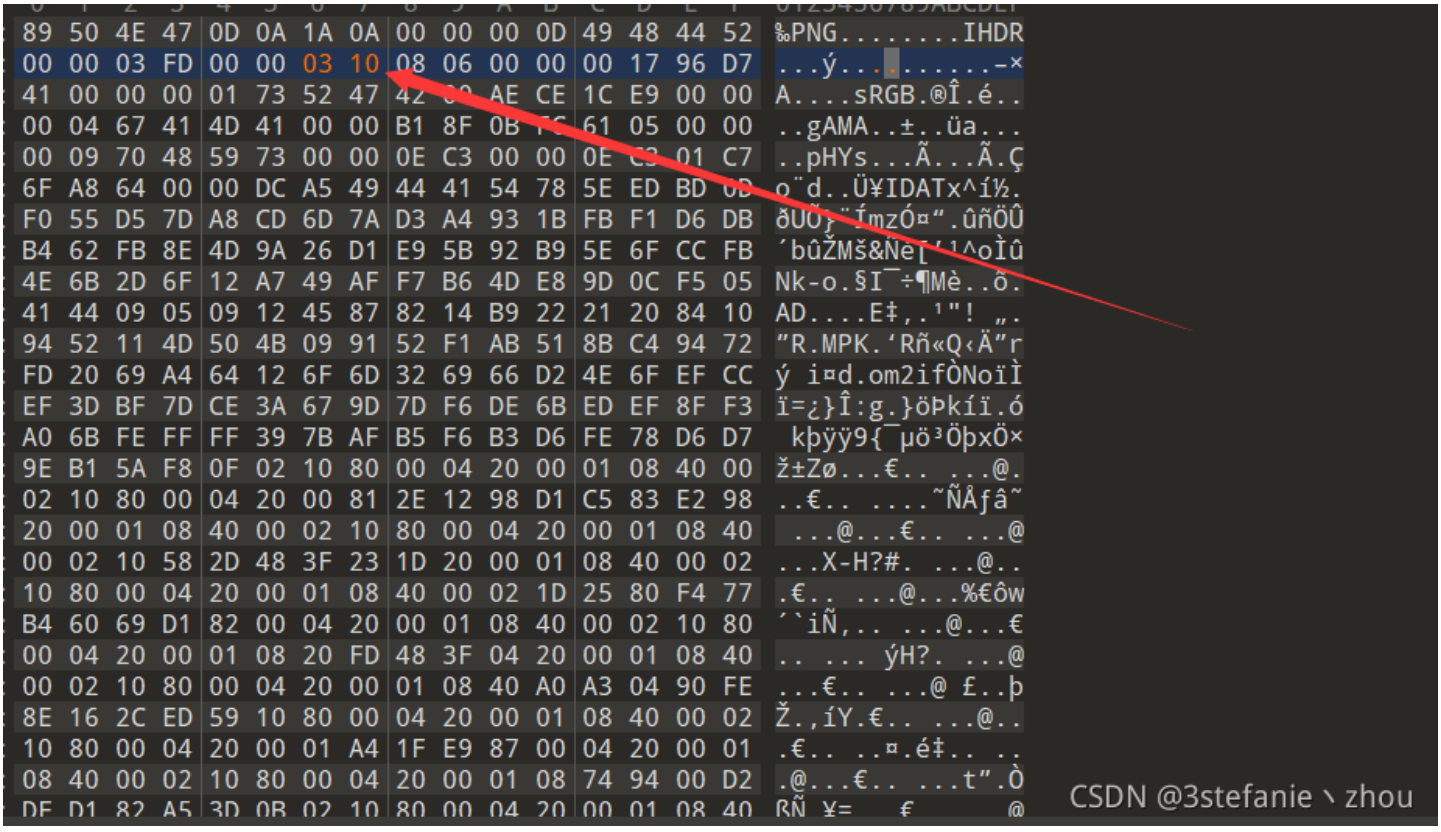
在文件尾出发现 AE 42 60 82,得知是一张图片，这是png的文件尾格式
但是缺失文件头，补上



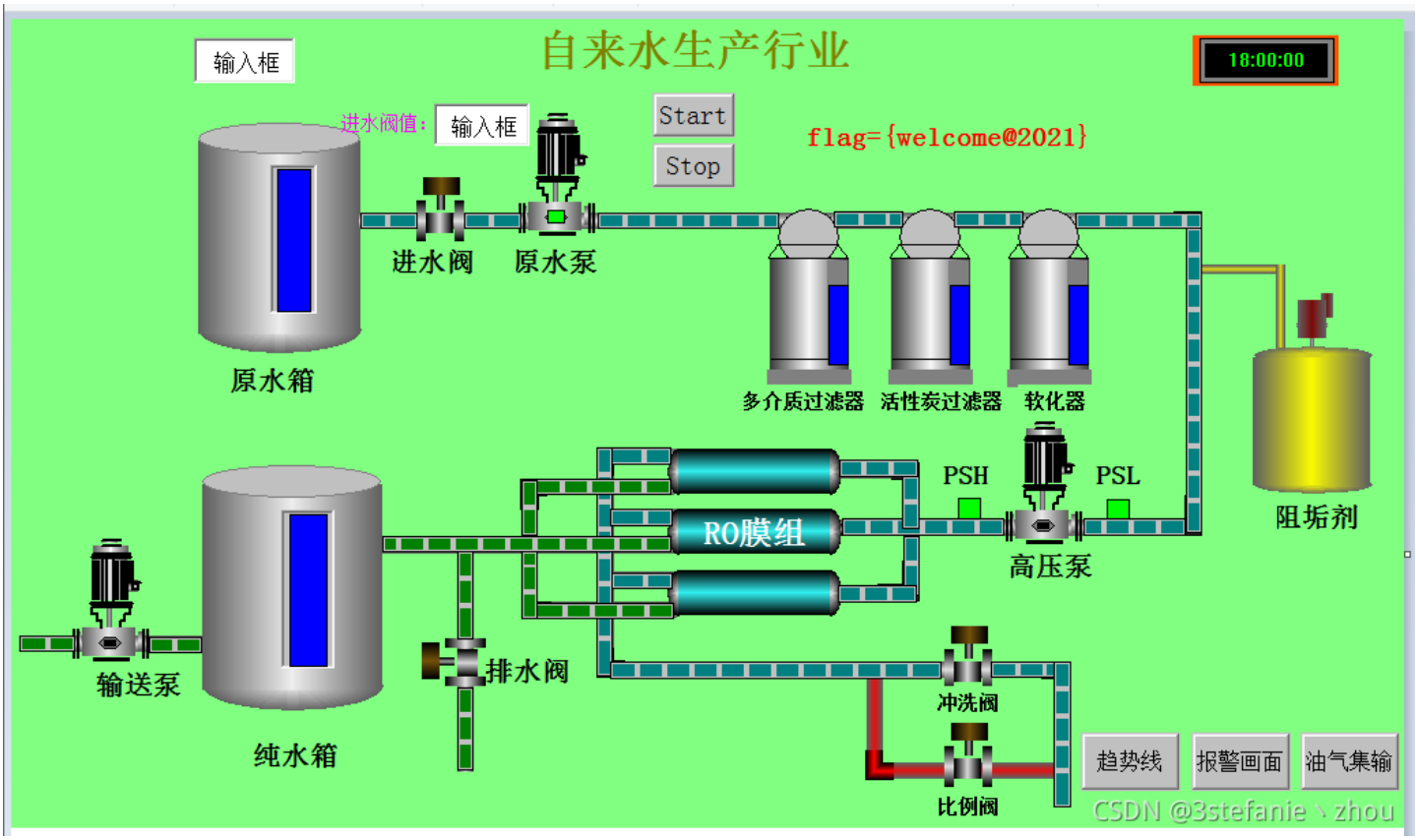
打开图片



高度很小，修改高度为03 10



打开图片，发现flag




```
flag{welcome@2021}
```

异常流量分析

hint:某企业的运维工程师发现网络中出现流量异常，于是从场内一交换机抓取了数据包，请协助找出流量中针对正常的业务的异常数据内容，flag提交形式为flag{xxxx}。

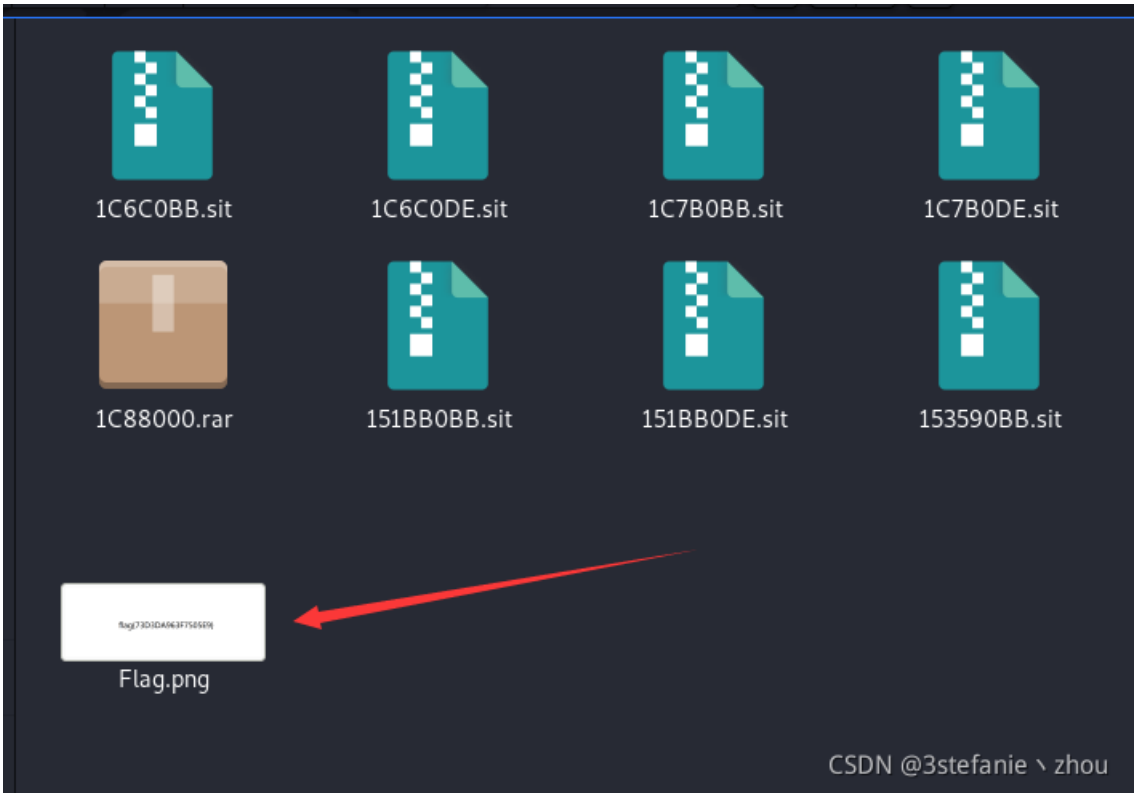
使用wireshark打开流量包，追踪tcp流

在流41发现一串字符串，syntvfguvfZbqohffffff

synt开头，显然这是flag经过rot13编码，直接解码,得到flag

应急恢复

得到一个data.img的光盘映像文件
丢进kali，binwalk分析一下
发现压缩包文件，文件分离一下
发现flag.png



flag{73D3DA963F7505E9}

CSDN @3stefanie丶zhou

```
flag{73D3DA963F750E9}
```

恶意app分析

hint:在某工控人员手机中发现一个疑似远控木马样本，请分析该样本，请找到回传数据的目标邮箱地址，为后续的攻击溯源提供帮助，flag提交格式为：flag{邮箱地址}。

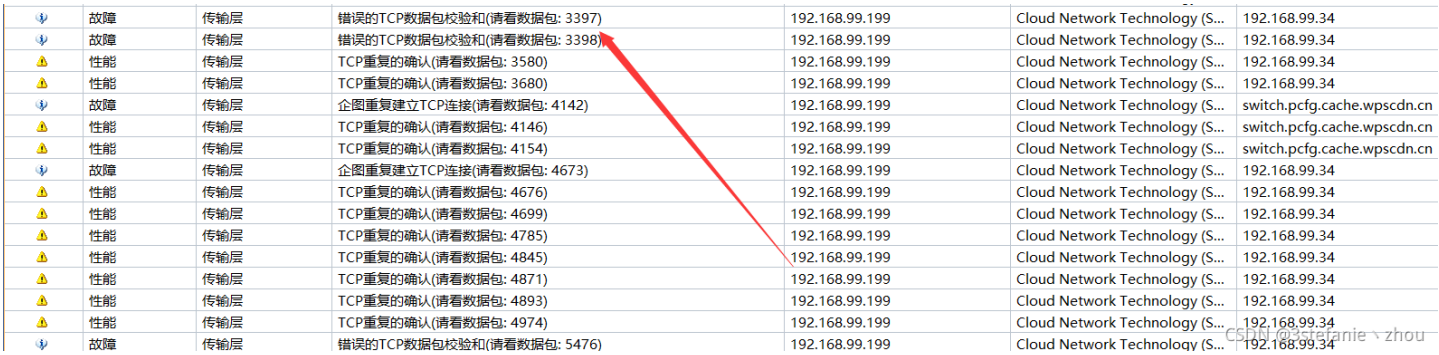
解压文件，得到一个apk文件
直接丢进jadx反编译，全局搜索email

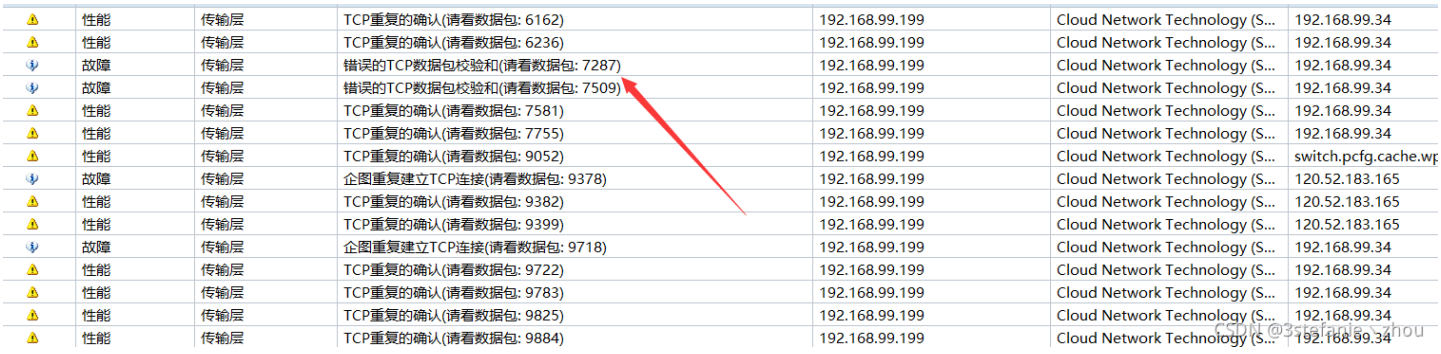

```
flag{hahaha_wtf@163.com}
```

工控流量分析

hint:某企业车间PLC运行异常，造成生产线无法正常运行。请您帮助改企业车间分析出PLC遭到异常的原因。flag格式为:flag{}。

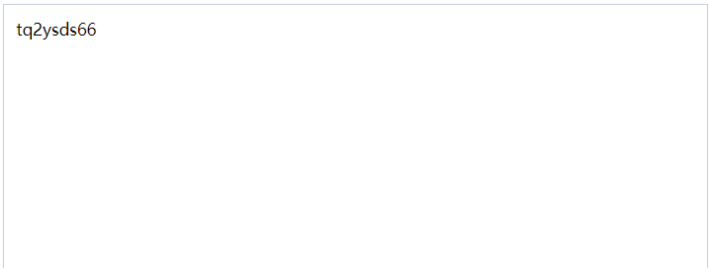
PLC运行异常，将数据包丢进科来分析数据包
发现3397，3398，7287，7509这四个数据包TCP数据包错误

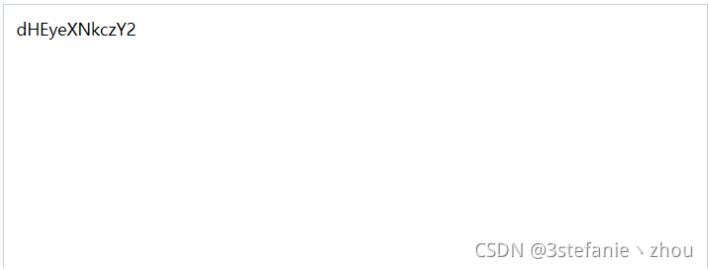




使用wireshark来继续分析

对3397，3398，7287，7509周围几个数据包分析
在3399发现一个可疑信息，dHEyeXNkczY2
对其进行解码尝试，发现base64解码得到内容比较可靠



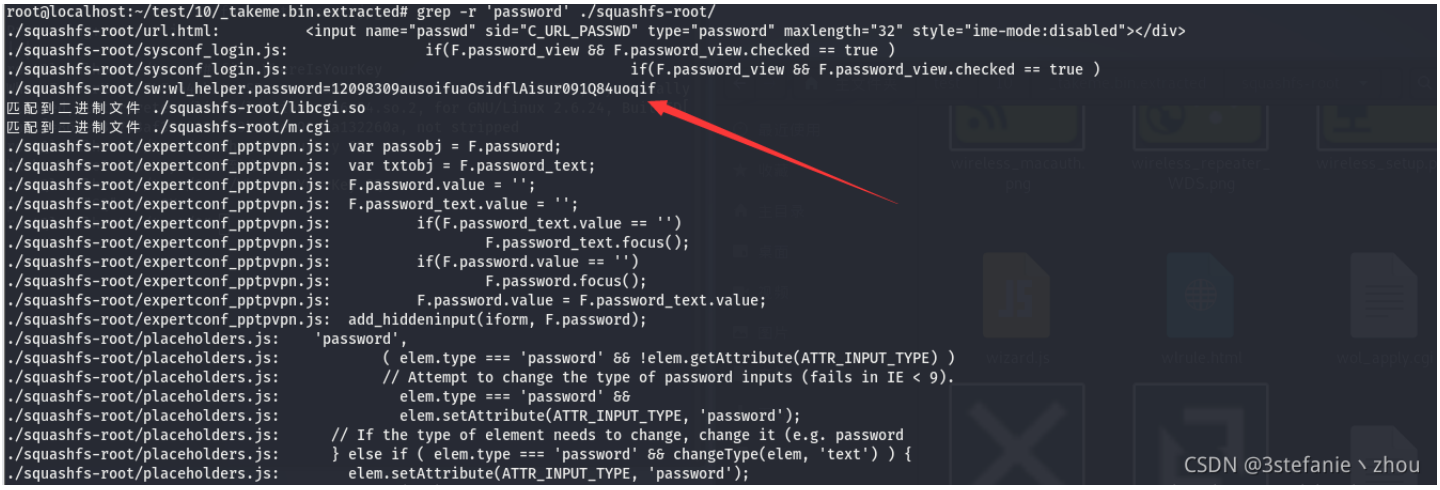


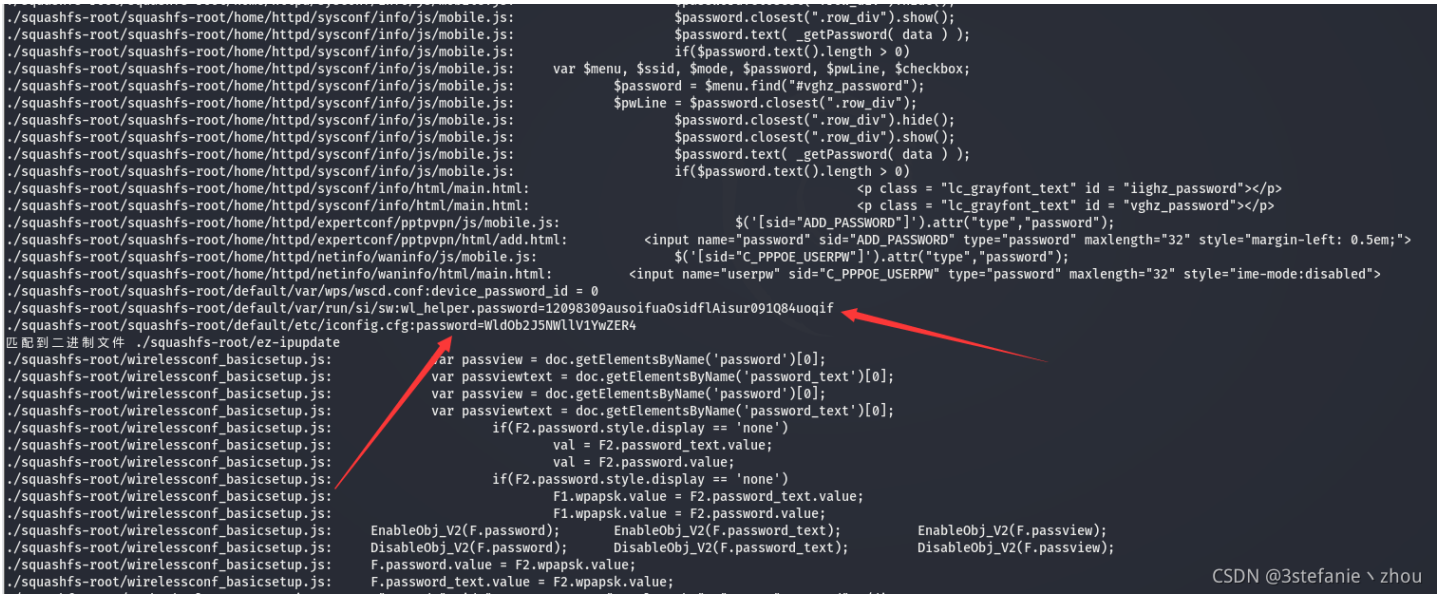

```
flag{tq2ysds66}
```

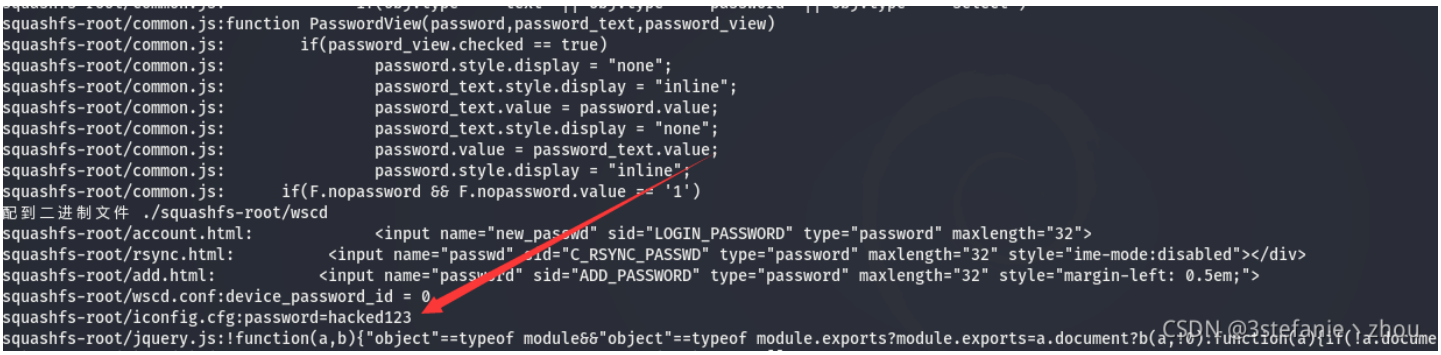
丢失的密码

hint:小明作为工厂运维人员，对路由器固件进行升级操作。升级后尝试使用默认帐户信息以admin / admin身份登录以设置路由器，但无法连接。分析原因并获取帐户信息。密码即为flag。

使用binwalk - e ，分离文件，根据提示，密码为flag
在分离的目录下，全局搜索password
得到如下密码







逐一作为flag尝试

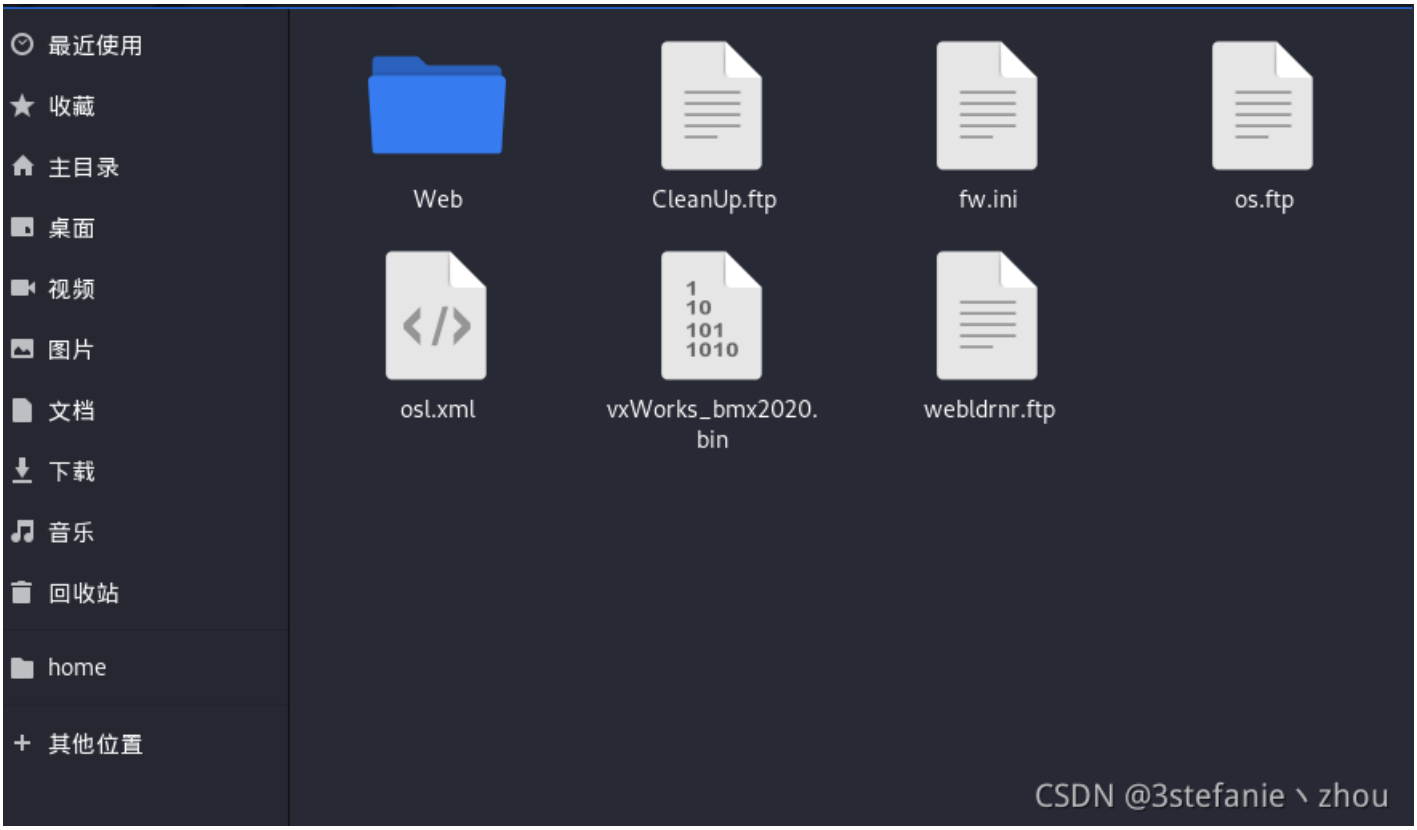
正确flag为

```
flag{WldOb2J5NWllV1YwZER4}
```

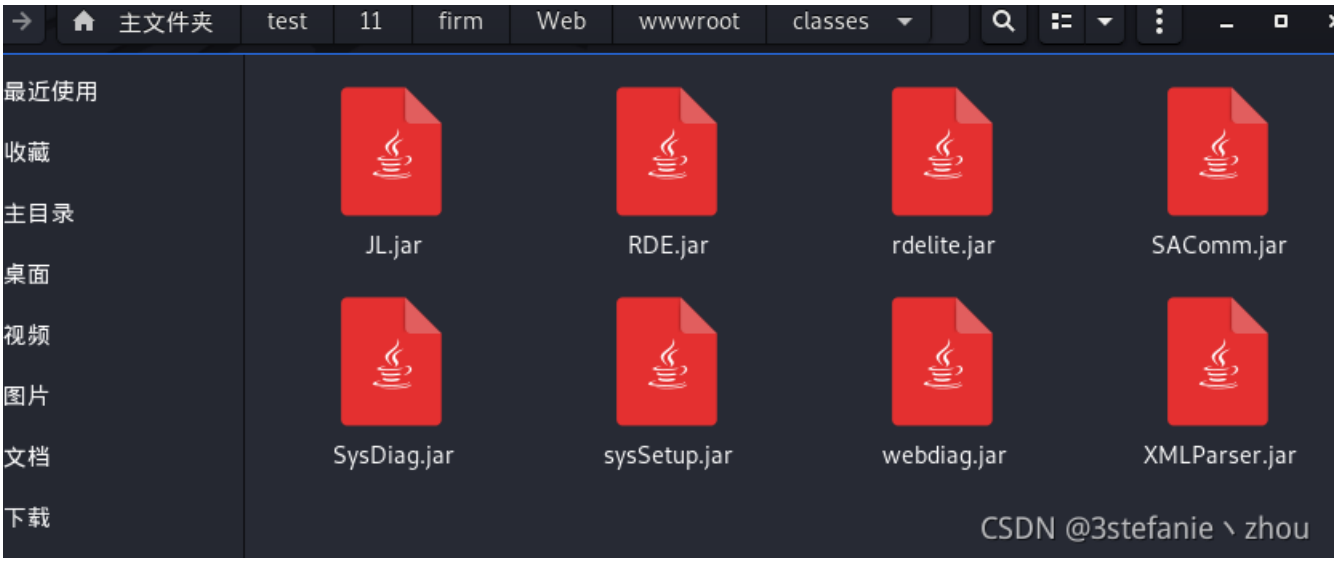
工业固件分析

hint:某PLC设备的固件已被攻击者提取并打包，请对固件进行分析，获取固件中被硬编码的ftp账户用户名密码信息。flag格式为：flag{ftp username+ftp password}，例如，用户名为admin，密码为123，则flag为flag{admin+123}。

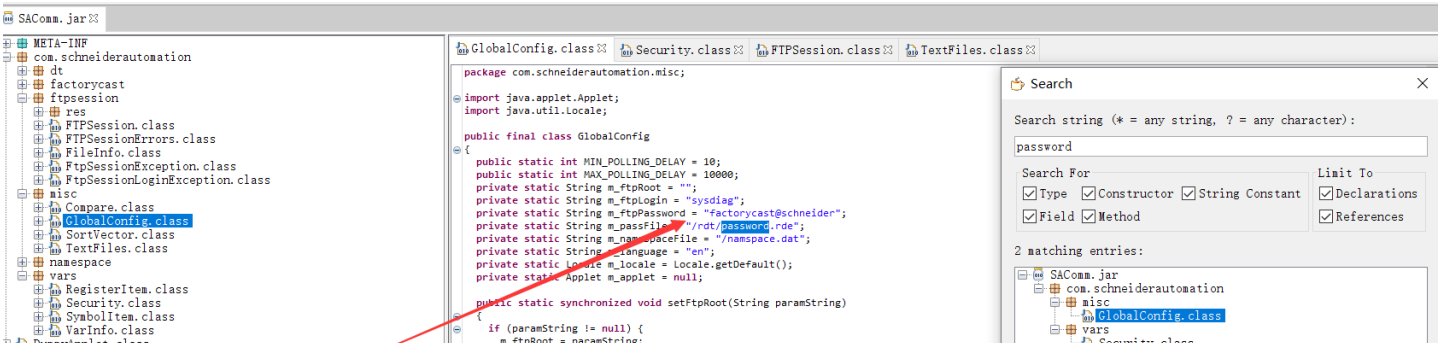
根据提示信息，解压压缩包，得到如下文件

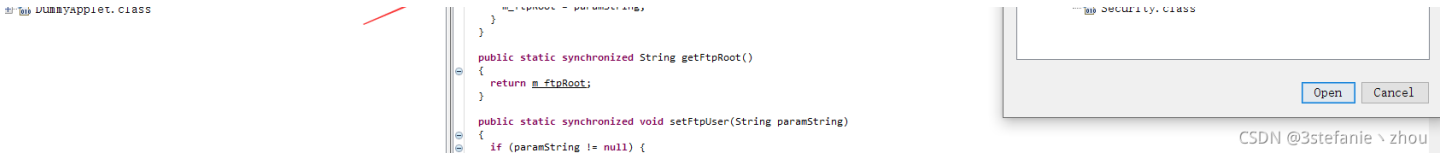


由于ftp账户用户名密码信息被硬编码在代码中，所以找到如下jar包



逐一丢进jd里面反编译，然后全局搜索password
最终在SAComm.jar这个Jar包中发现ftp的账户密码信息



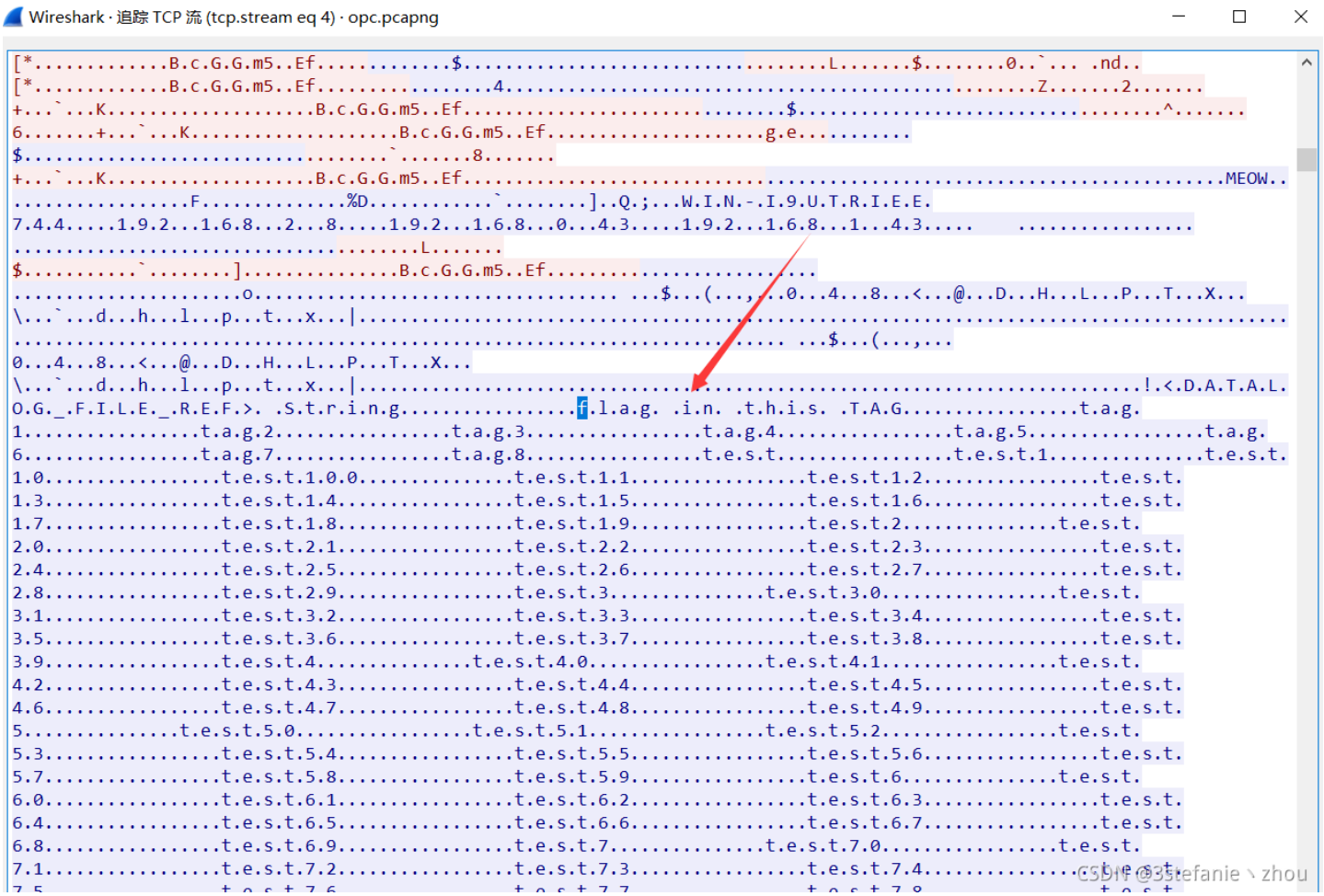



```
flag{sysdiag+factorycast@schneider}
```

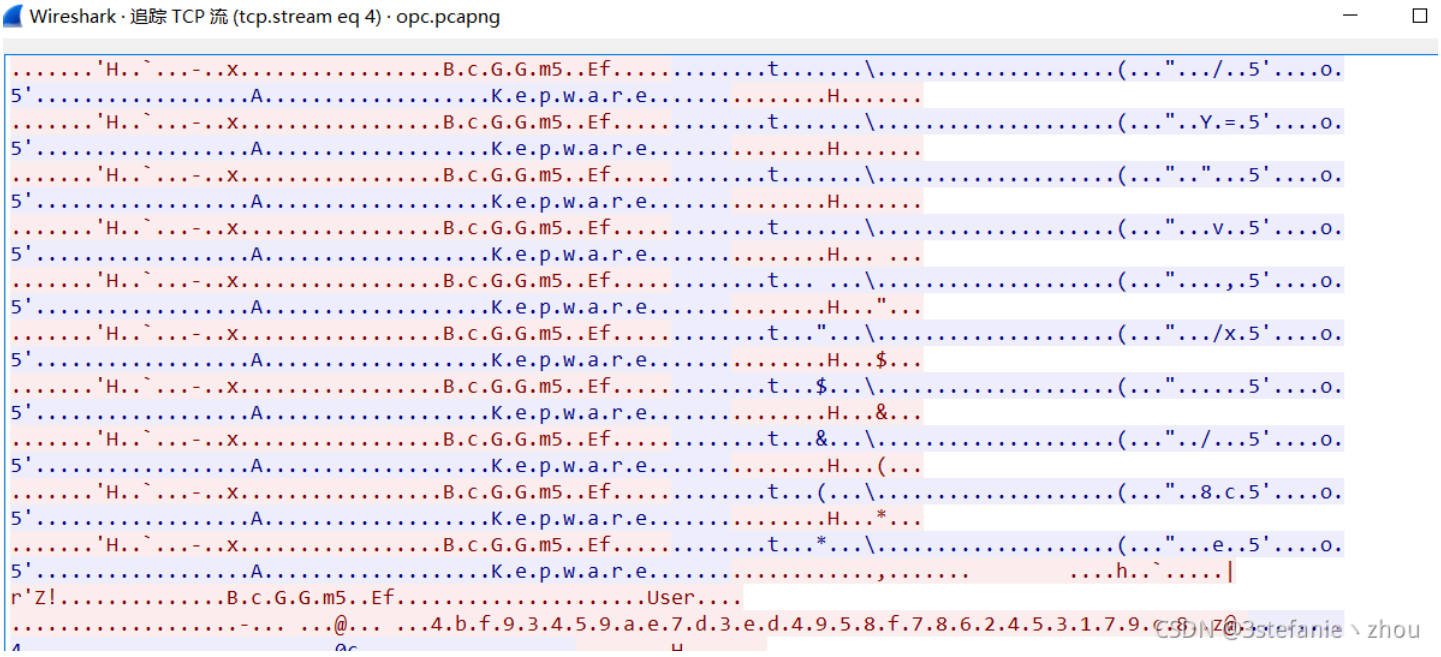
opc流量分析

hint:OPC是微软公司的对象连接和嵌入技术在过程控制方面的应用，OPC标准定义了在基于PC的客户机之间进行自动化数据实时交换的方法，因此OPC协议在工业控制现场使用非常多。请对提供的OPC通信流量进行分析，尝试找出流量中的flag。

追踪tcp流数据，在流4发现flag相关信息，string flag in this tag



分析附近数据包，得到如下可疑信息



4.b.f.9.3.4.5.9.a.e.7.d.3.e.d.4.9.5.8.f.7.8.6.2.4.5.3.1.7.9.c.8
5.3.5.5.4.E.5.4.6.1.6.E.6.8.4.1.4.D.6.A.4.1.7.9.4.D.5.1.3.d.3.d
7.a.5.d.8.a.4.b.4.9.5.8.a.4.b.f.9.3.4.5.9.a.e.7.d.3.e.d.4.9.5.8
9.a.9.e.4.d.6.f.2.a.4.b.3.c.4.a.4.f.6.e.7.c.8.b.9.d.6.f.4.a.6.f
8.a.9.b.7.e.1.f.7.8.6.2.4.5.3.1.7.9.c.8.9.a.1.4.5.4.6.9.4.7.1.6
a.4.b.3.c.4.9.5.8.f.7.8.4.d.6.f.2.a.4.b.3.c.4.9.5.8.f.7.4.5.3.1
1.7.9.c.8.9.a.1.4.5.4.6.9.4.7.1.6.f.9.3.4.5.9.a.e.7.d.3.e.4.7.9

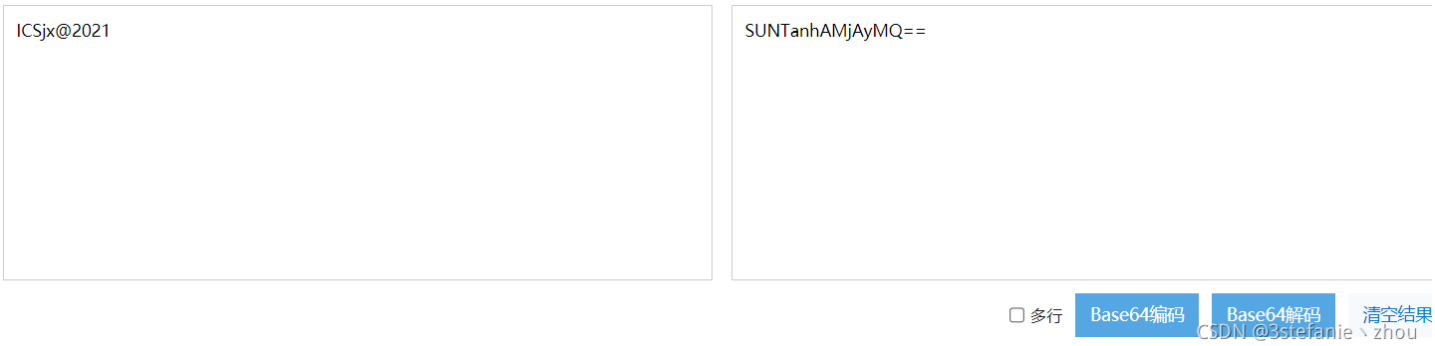
去除小数点,得到16进制数据

4bf93459ae7d3ed4958f7862453179c8
53554E54616E68414D6A41794D513d3d
7a5d8a4b4958a4bf93459ae7d3ed4958
9a9e4d6f2a4b3c4a4f6e7c8b9d6f4a6f
8a9b7e1f7862453179c89a1454694716
a4b3c4958f784d6f2a4b3c4958f74531
179c89a1454694716f93459ae7d3e479

转成字符串

Kù4Y®}>Ô•xbE1yÈ
SUNTanhAMjAyMQ==
z]ŠKIX¤¿“EšçÓílX
šžMo*K<JOn|‹oJo*
Š›~xbE1yÈšTiG
¤³Ä•*xMo*K<lX÷E1
œ‰¡EF”qo“EšçÓäy

将唯一的正常字符串进行base64解码



得到flag

```
flag{ICSjx@2021}
```

【吾有所思人，隔在远远乡】