第二届网刃杯网络安全大赛 Writeup

原创

末 初 已于 2022-04-26 15:41:20 修改 2754 收藏 24

分类专栏： CTF_MISC_Writeup 文章标签： 2022第二届网刃杯

于 2022-04-25 17:37:34 首次发布

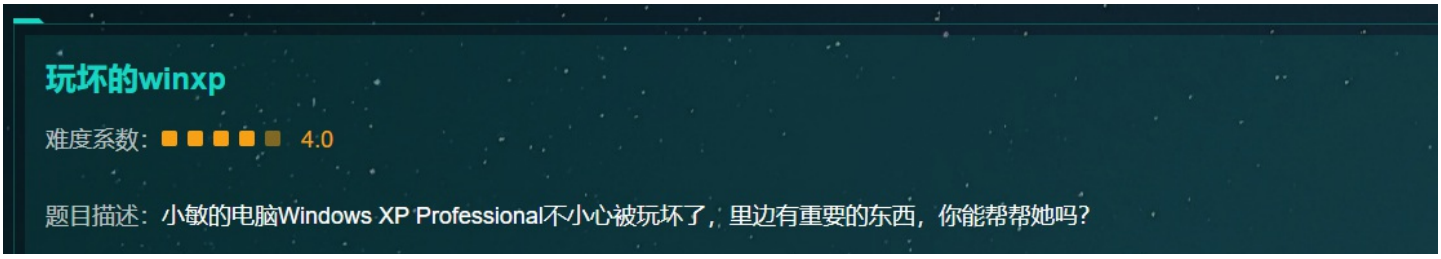
本文链接：https://blog.csdn.net/mochu7777777/article/details/124380608

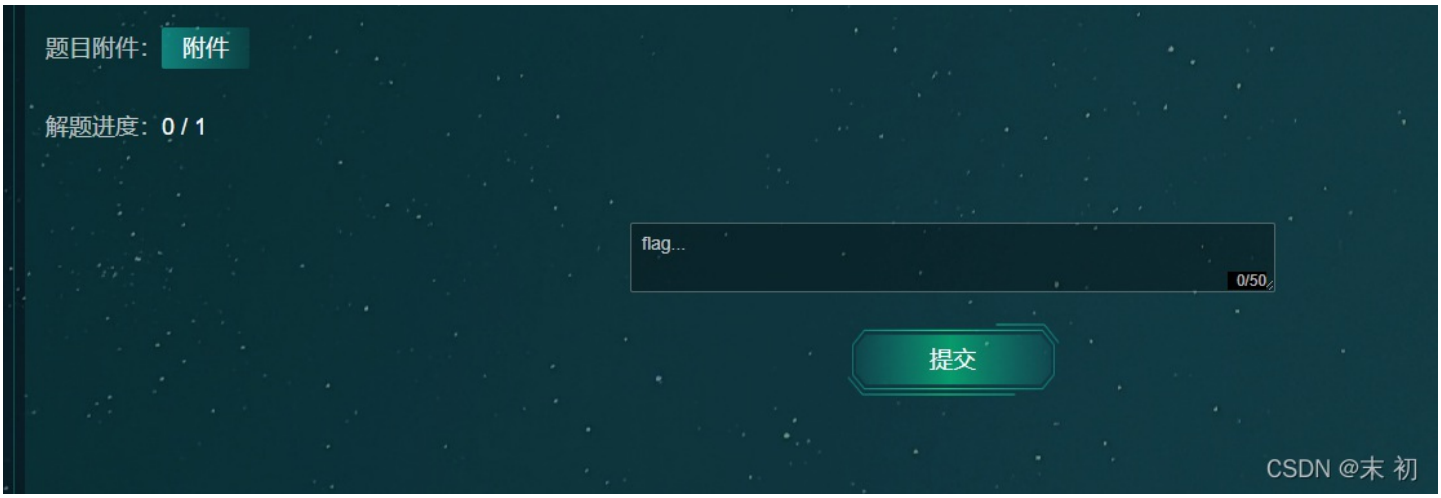
文章目录

```
题目附件：
链接：https://pan.baidu.com/s/1XlA0tSNwSFr7Lj7WTMT5cw
提取码：pteg
--------------------------------------------------
其中部分压缩包有加密密码是赛事官方设置
《玩坏的winxp》： bvis823HNas20cFKAJS2KF1Axasv
《不要相信你所看到的》： surn528WBC86Fj3da9QRscGW256f
```

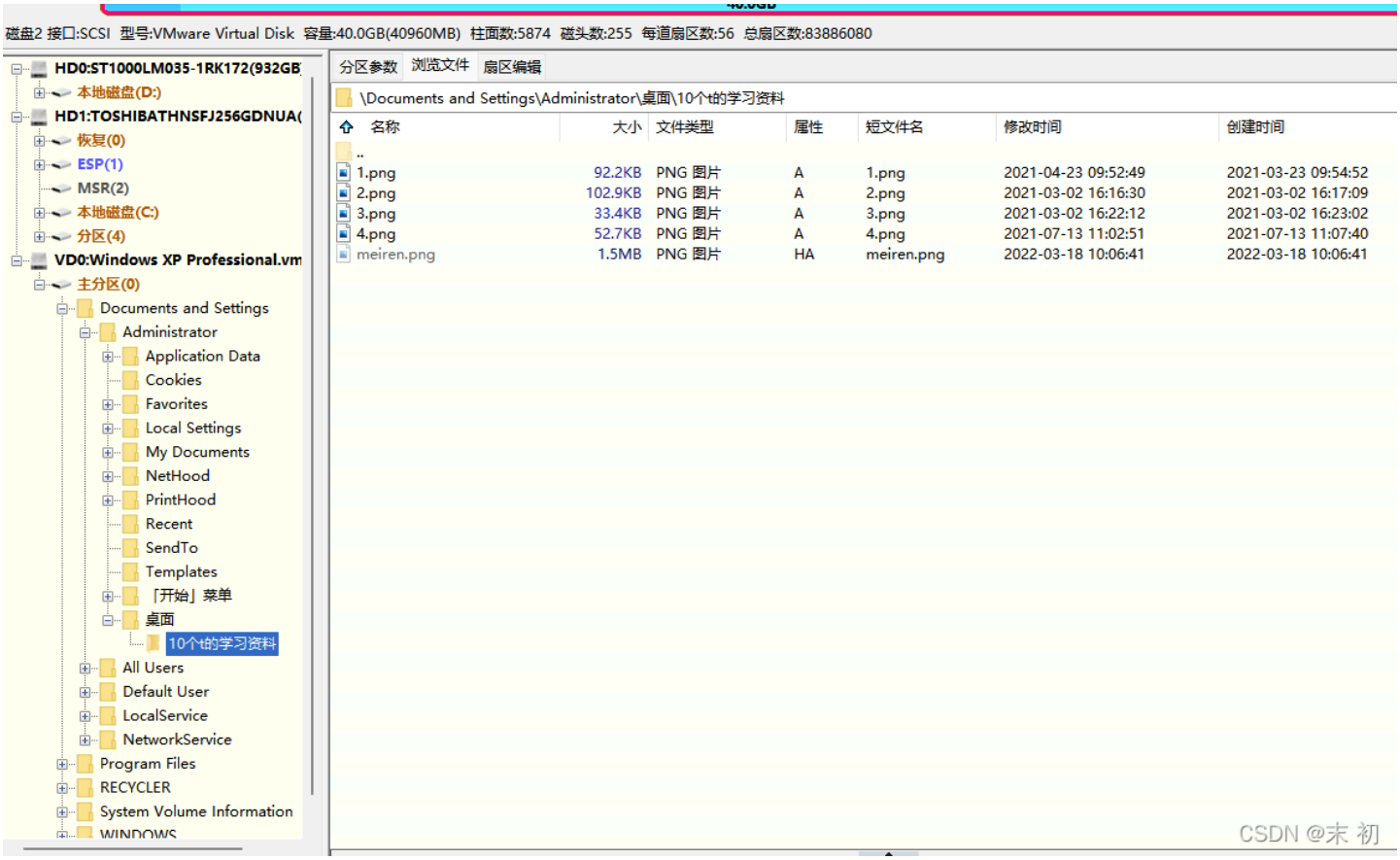
MISC

玩坏的winxp

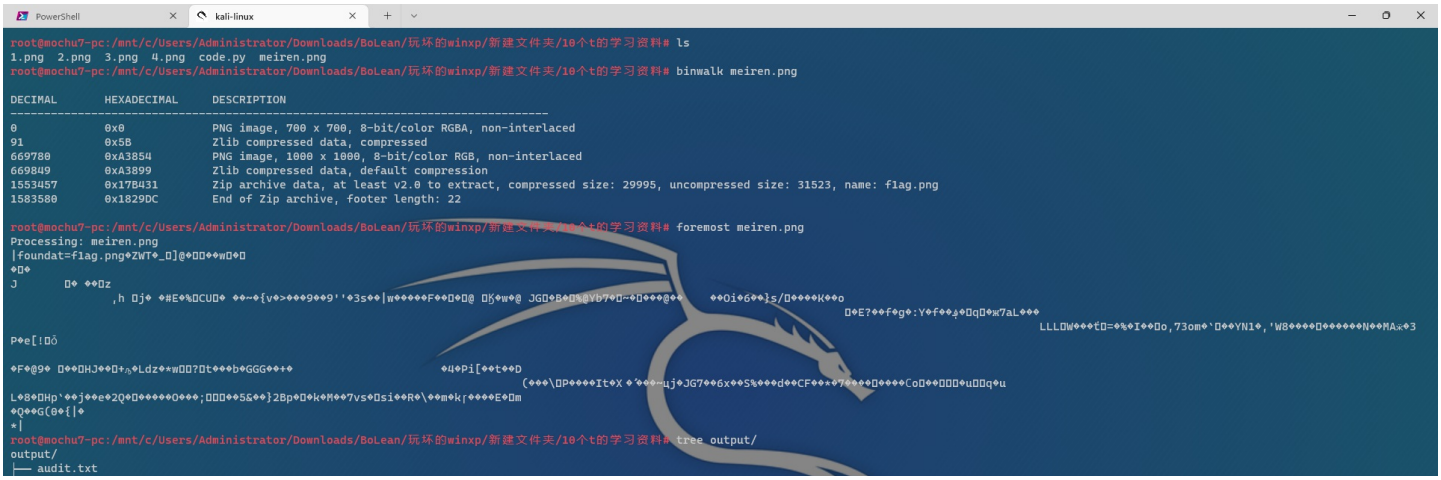




`vmdk` 文件，用 `DiskGenius` 打开，找到 `Administrator` 用户的桌面的学习资料



`binwalk` 分析 `meiren.png`， `foremost` 分离



```
├── png
│   ├── 00000000.png
│   └── 00001308.png
└── zip
    └── 00003034.zip

2 directories, 4 files
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/BoLean/玩坏的winxp/新建文件夹/10个t的学习资料#
```

CSDN @末 初

此电脑 › 下载 › BoLean › 玩坏的winxp › 新建文件夹 › 10个t的学习资料 › output › zip ›

00003034.zip

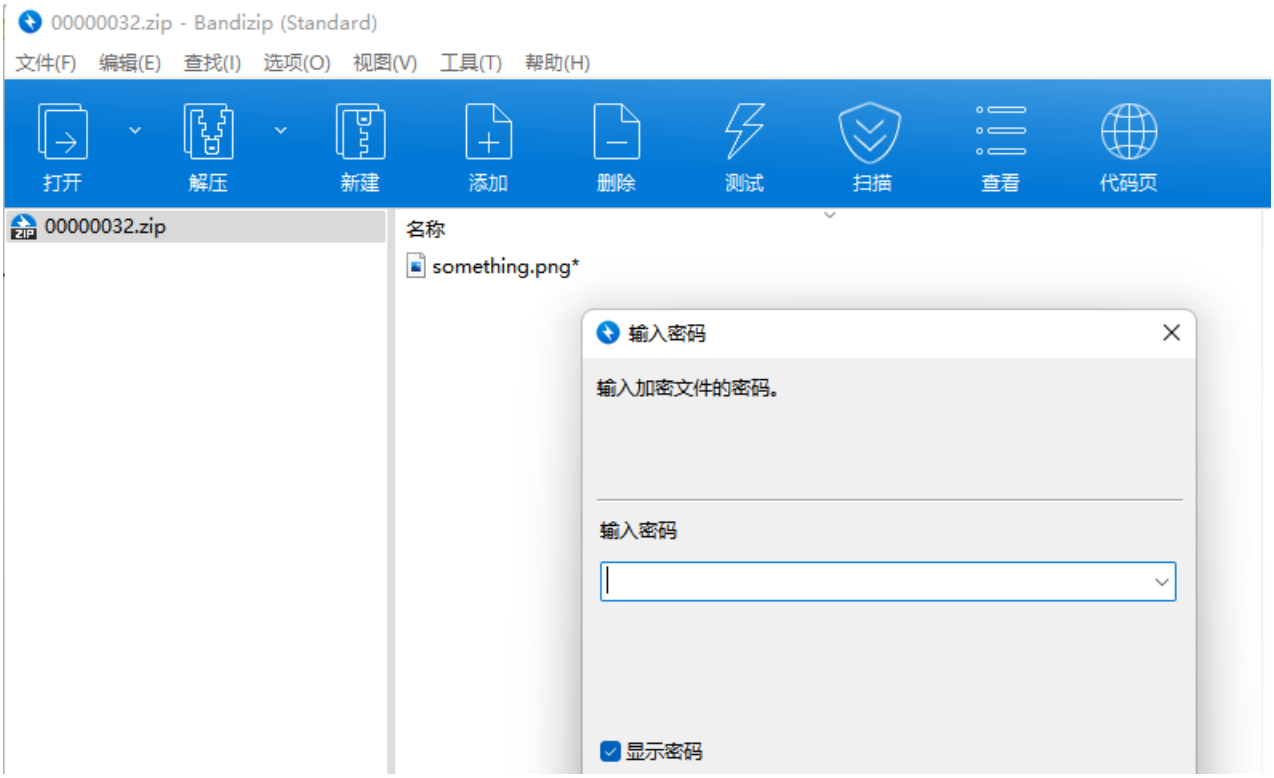
f1ag.png

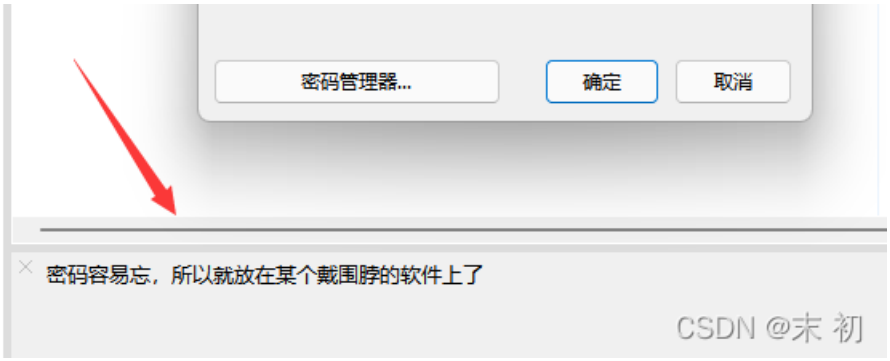
继续`binwalk`分析，`foremost`分离`f1ag.png`

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/BoLean/玩坏的winxp/新建文件夹/10个t的学习资料/output/zip# ls
00003034.zip  f1ag.png
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/BoLean/玩坏的winxp/新建文件夹/10个t的学习资料/output/zip# binwalk f1ag.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 617 x 333, 8-bit/color RGB, non-interlaced
78            0x4E            Zlib compressed data, compressed
16871         0x41E7          Zip archive data, encrypted at least v2.0 to extract, compressed size: 14449, uncompressed size: 16047, name: something.png

root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/BoLean/玩坏的winxp/新建文件夹/10个t的学习资料/output/zip# foremost f1ag.png
Processing: f1ag.png
◆□X◆◆L◆Ai□ ◆◆◆◆FY◆Ê◆zA◆◆\",◆◆/◆◆◆□$◆◆[◆hRp%◆qG.□◆◆3◆◆|◆□◆◆¿*#◆◆F'I=◆C~◆\:◆V◆z◆□◆◆@]◆G◆□◆◆gtC◆><ÿy3◆◆◆OG◆◆(□◆8&"=◆KV◆◆VQ◆□◆I◆L_◆□cE
□M◆'\◆◆;◆w=□◆v◆}L◆◆
tu◆Ce◆&◆,◆r

*|
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/BoLean/玩坏的winxp/新建文件夹/10个t的学习资料/output/zip# tree output/
output/
├── audit.txt
├── png
│   └── 00000000.png
└── zip
    └── 00000032.zip

2 directories, 3 files
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/BoLean/玩坏的winxp/新建文件夹/10个t的学习资料/output/zip#
```

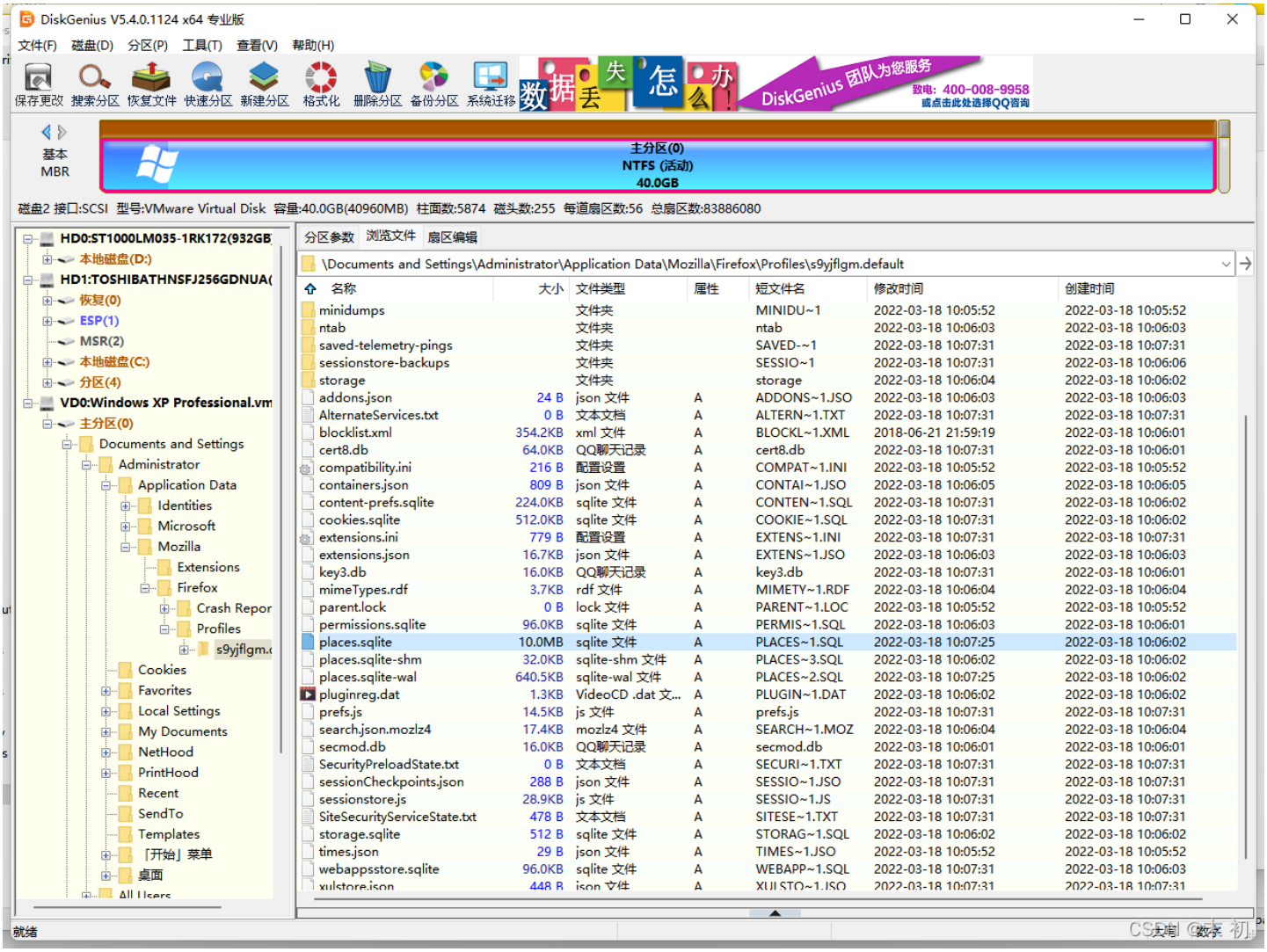
CSDN @末 初

分离出来的压缩包需要密码

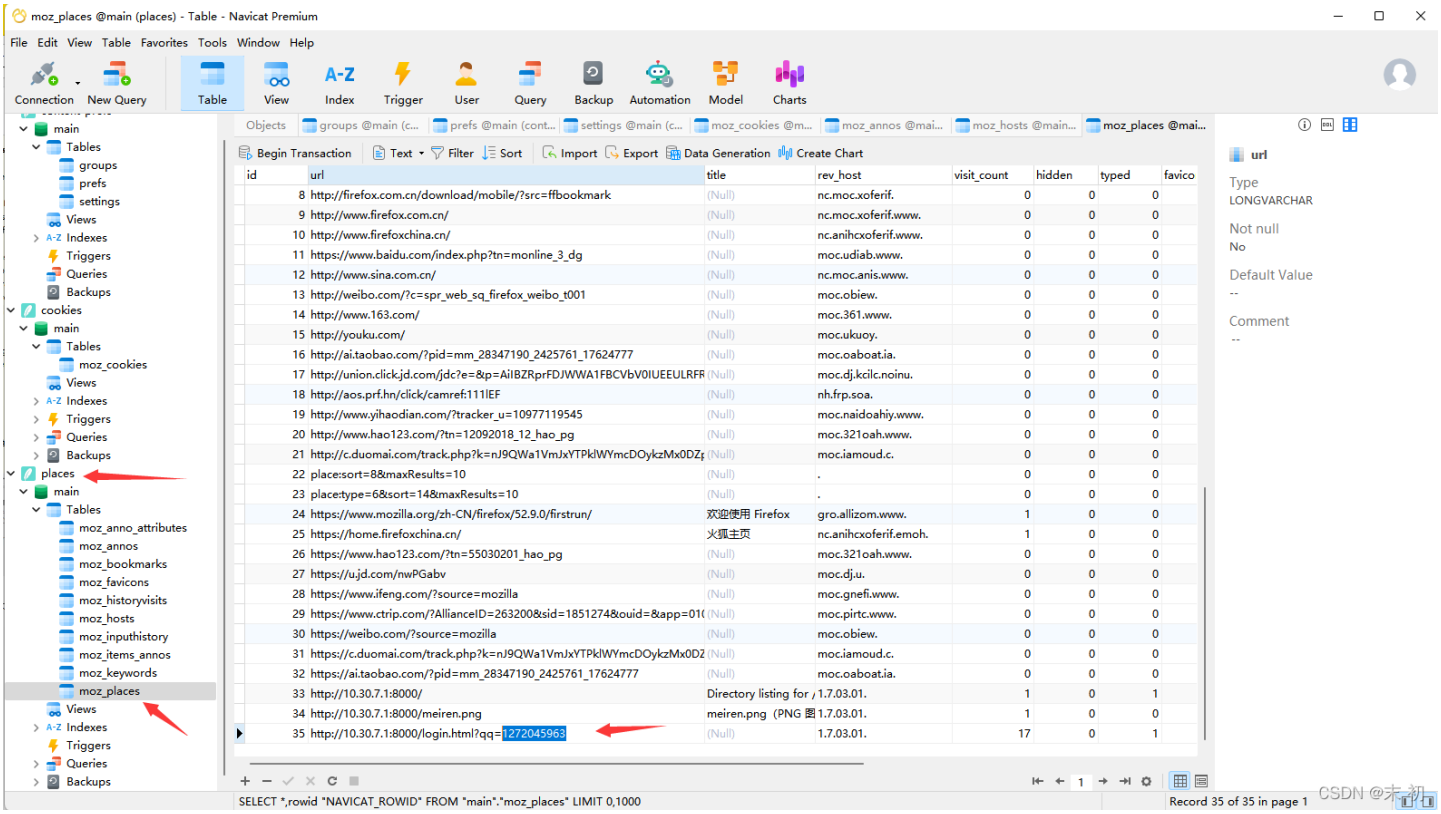




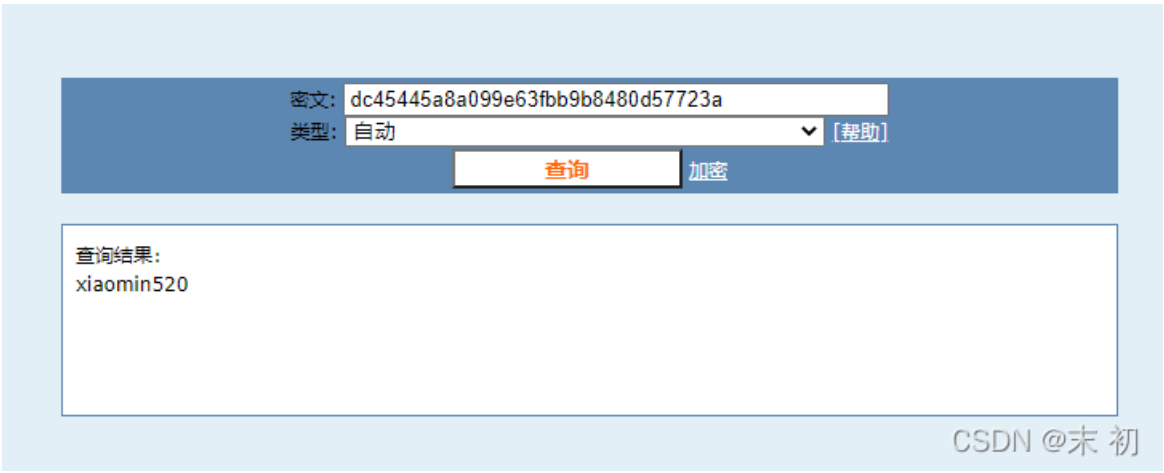
提示`QQ`有压缩包密码，但是在虚拟磁盘镜像中没有找到有安装过`QQ`这个软件，猜测可能在线登录过，所以就找唯一安装的浏览器`Firefox`的本地数据



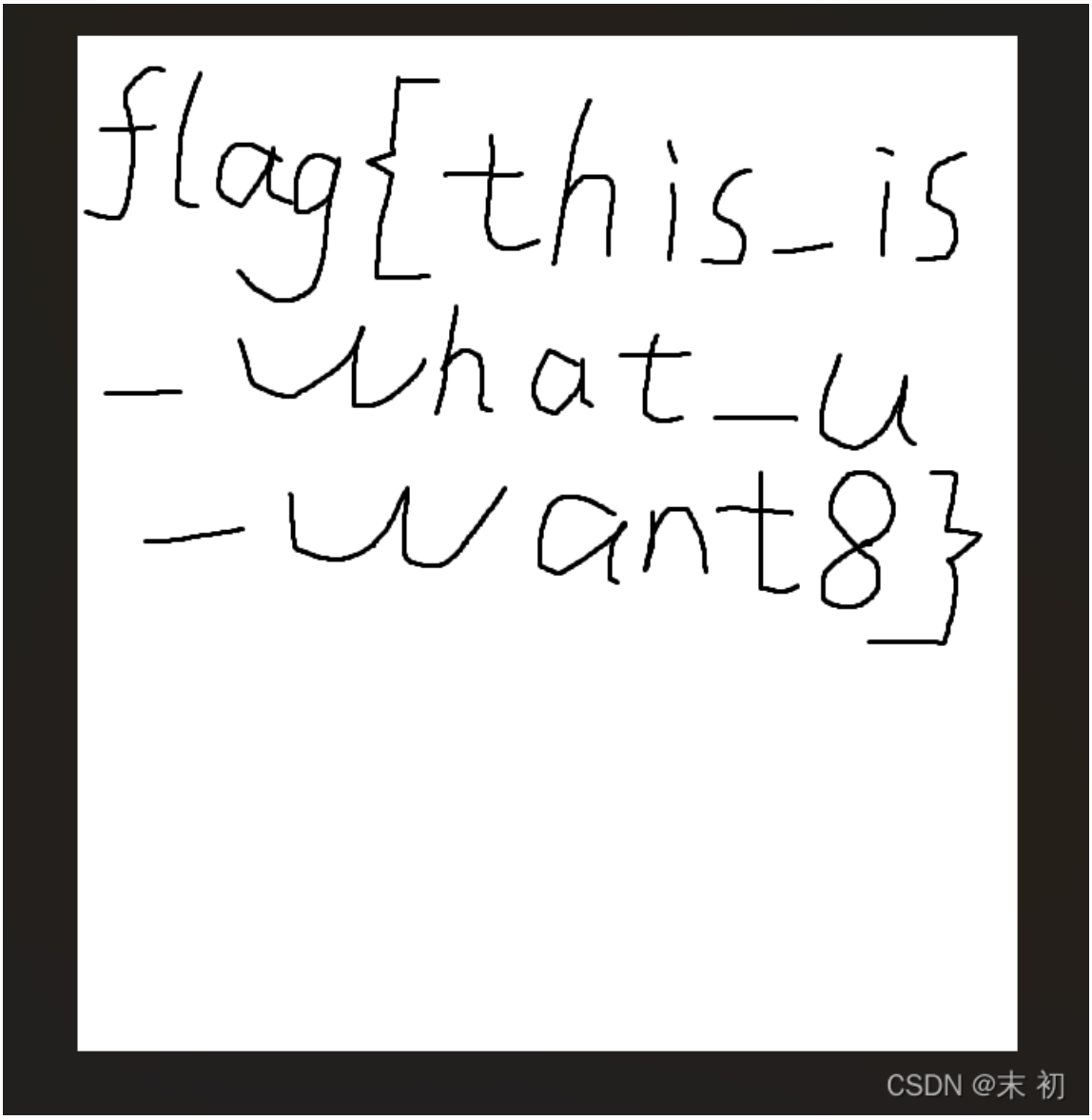
这里几个`.db`文件都不是`.db`文件，`Navicat`无法建立连接，几个`.sqlite`文件可以使用`Navicat`建立连接，找了好久最终在`places.sqlite`中找到qq账号



在开放的QQ空间中找到留言



得到解压密码：`xiaomin520`

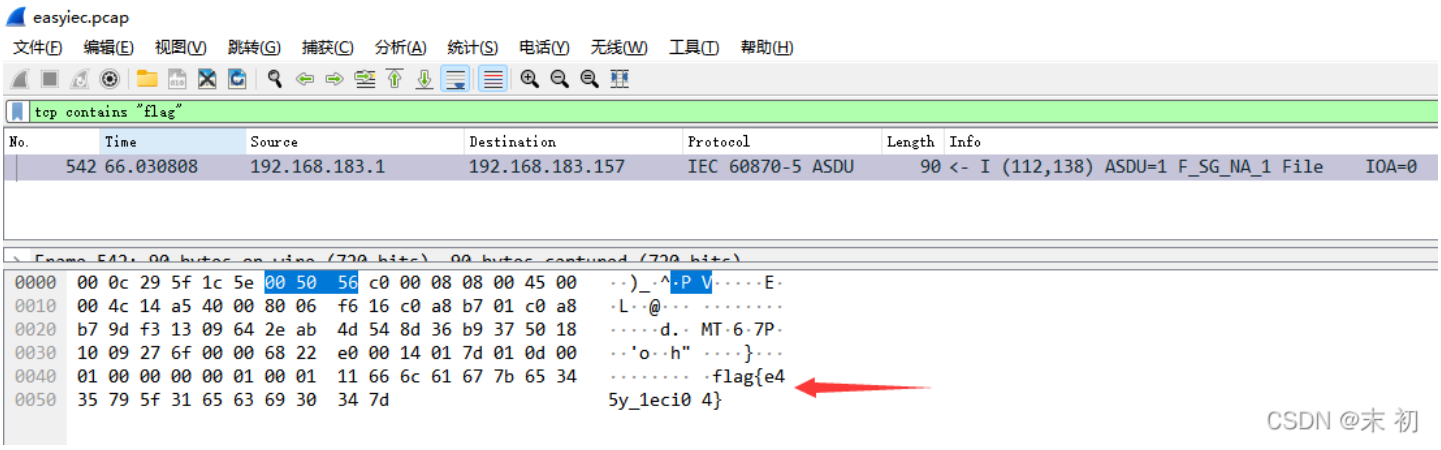



```
flag{this_is_what_u_want8}
```

ICS

easyiec

```
tcp contains "flag"
```

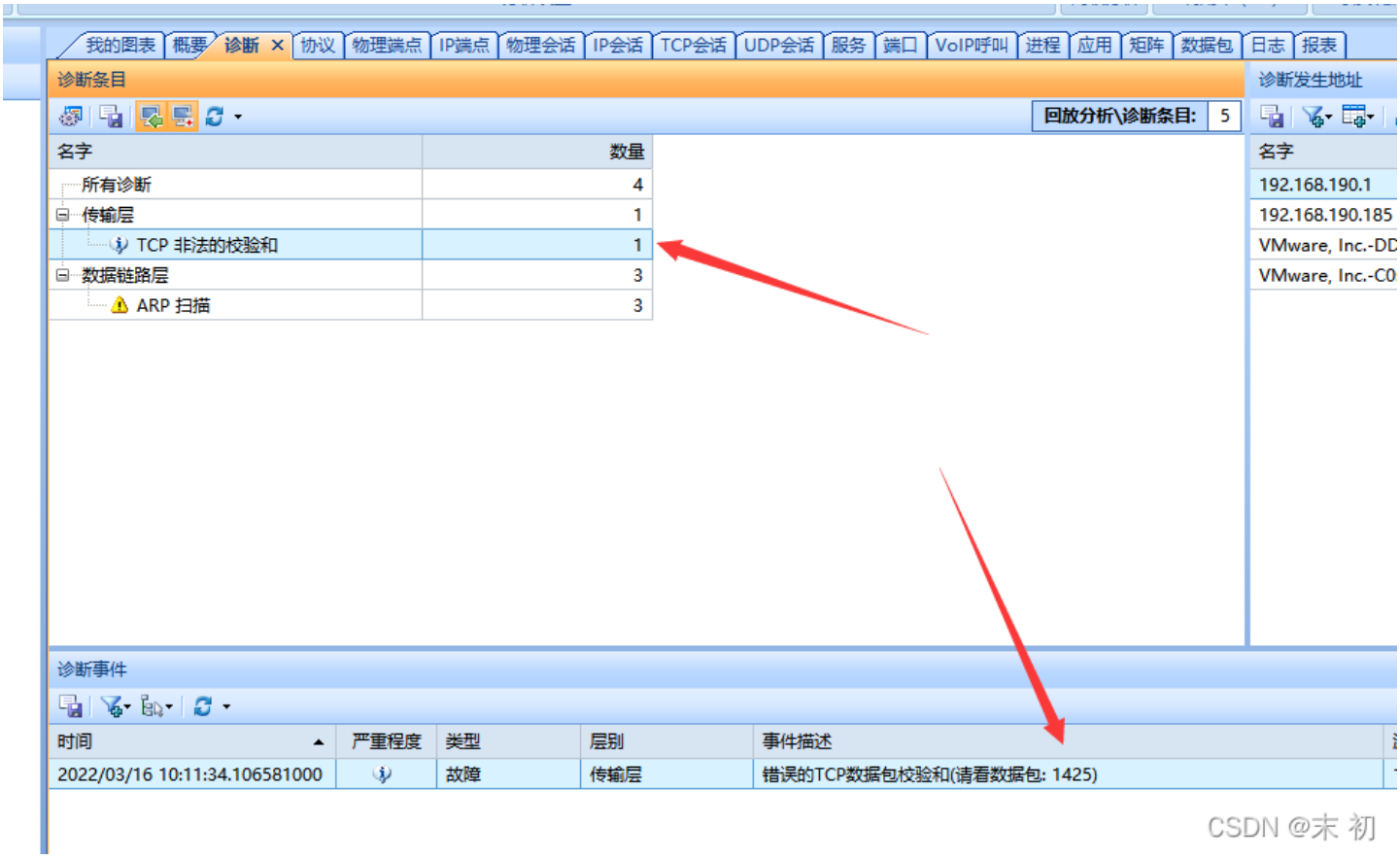


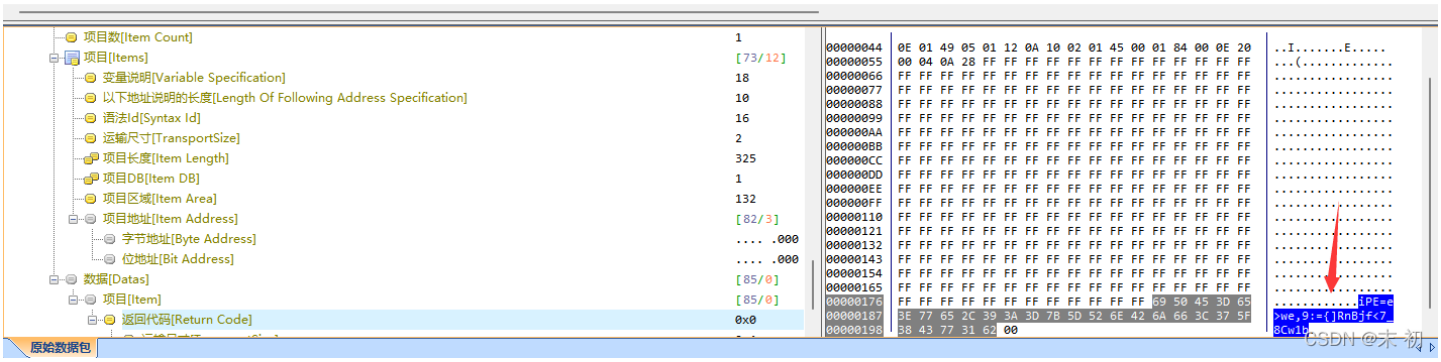

```
flag{e45y_1eci04}
```

xyp07

用科来网络分析系统打开

发现一个TCP非法校验，应该是修改了这里





Decode Any Base Encoding Scheme

Just paste any Base encoded string and BaseCrack will detect and decode it.

Supports multiline encoded strings of any scheme.

▶ Supported Encoding Schemes

▶ Try an example!

iPE=e>we,9:={]RnBjf<7_8Cw1b

DECODE

Decoded Results:

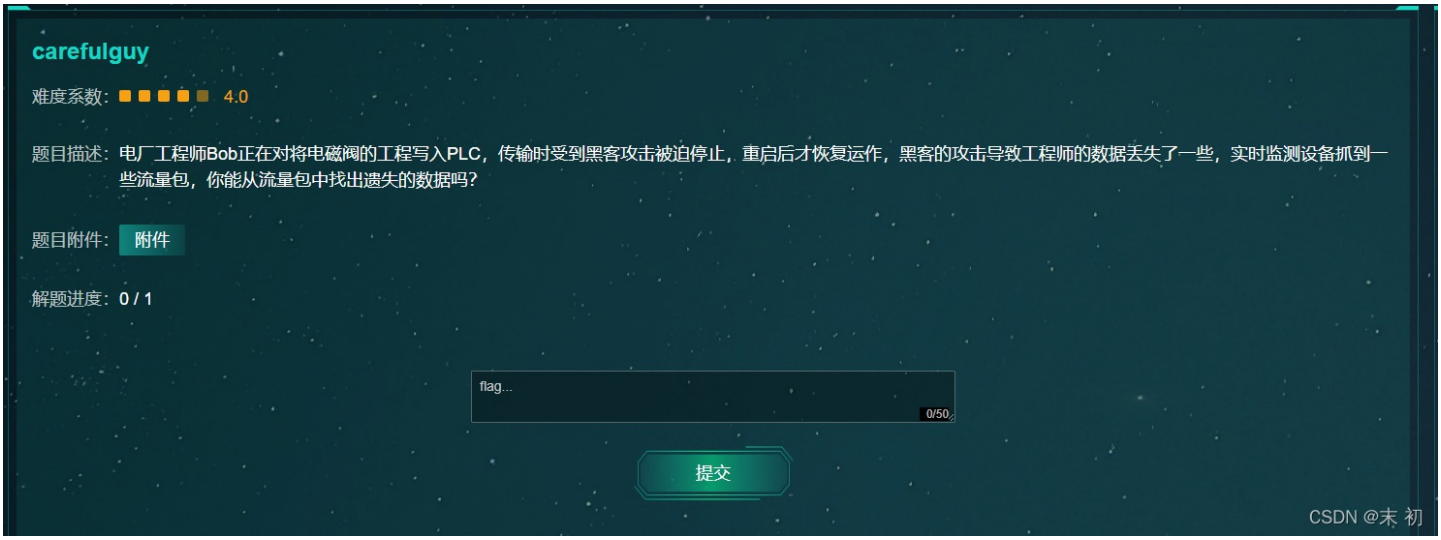
welcome_S7_world_xyp07 [Base91]

▶ Raw Results

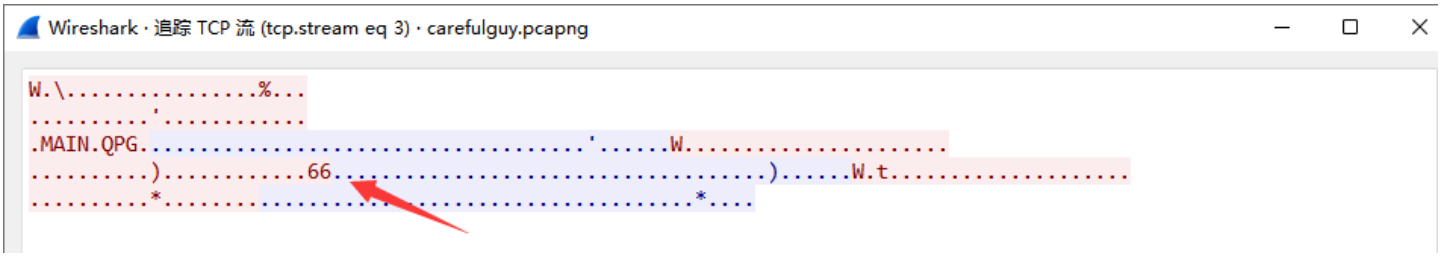
CSDN @末 初

```
flag{welcome_S7_world_xyp07}
```

carefulguy



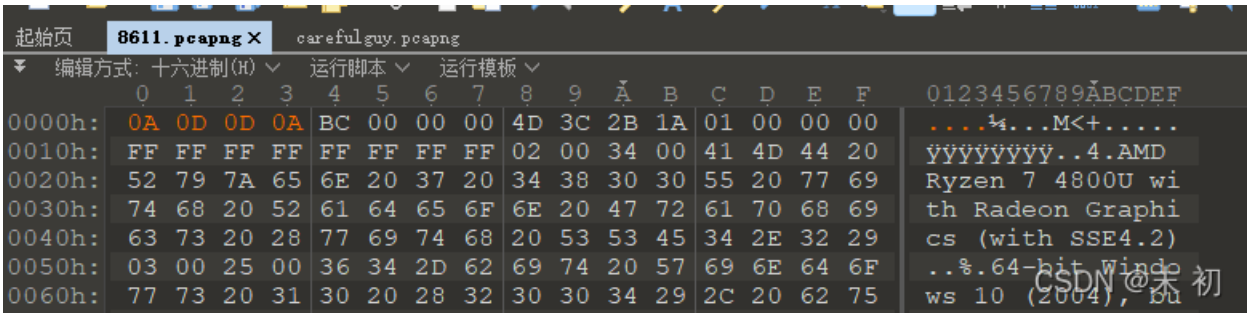
从`tcp.stream eq 3`开始往后有flag的十六进制



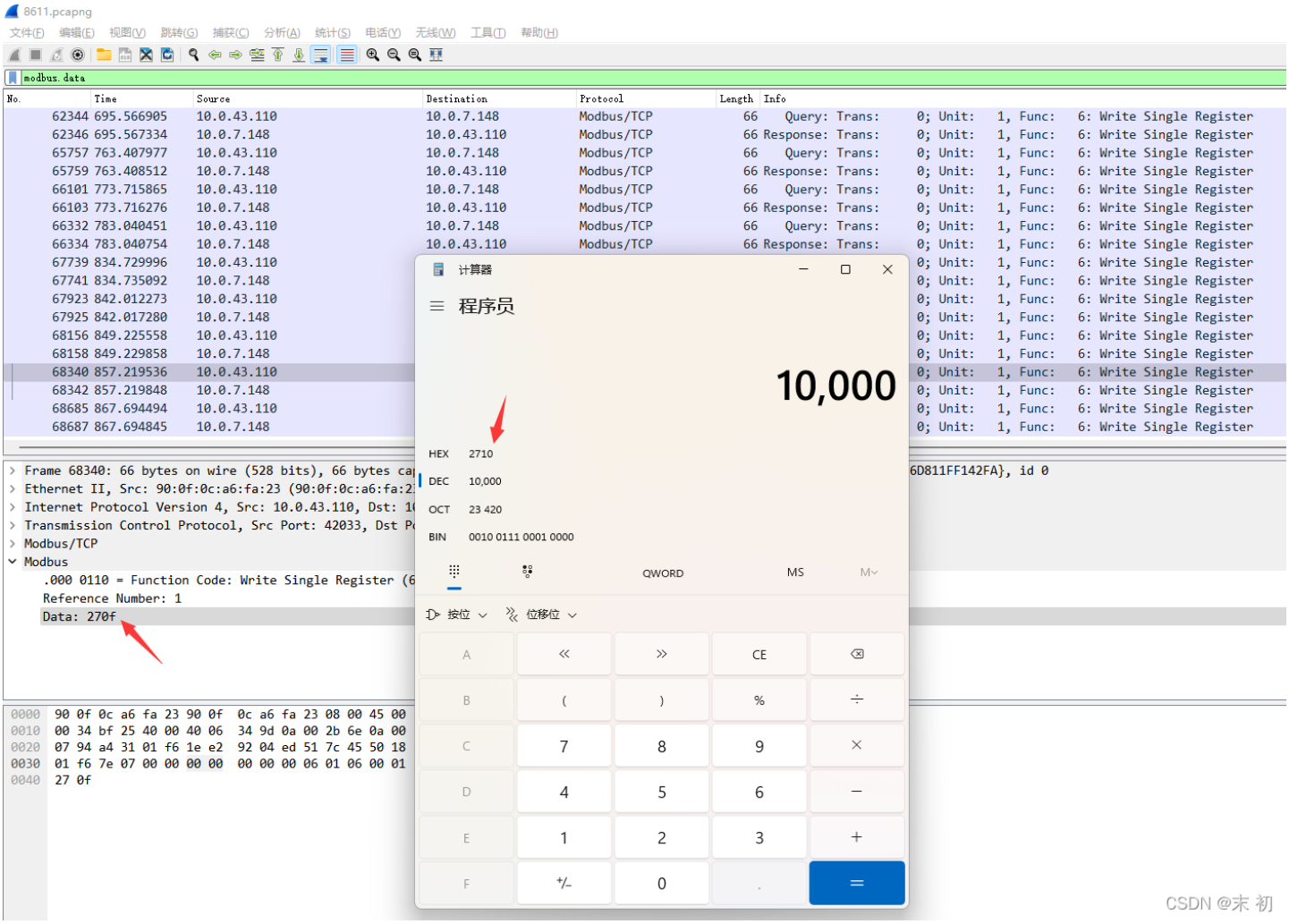

```
>>> from binascii import *
>>> flag='666c61677b703475733331357633727931 6e74337265737469633397d'
>>> unhexlify(flag)
b'flag{p4us315v3ry1nt3restic9}'
```

喜欢移动的黑客

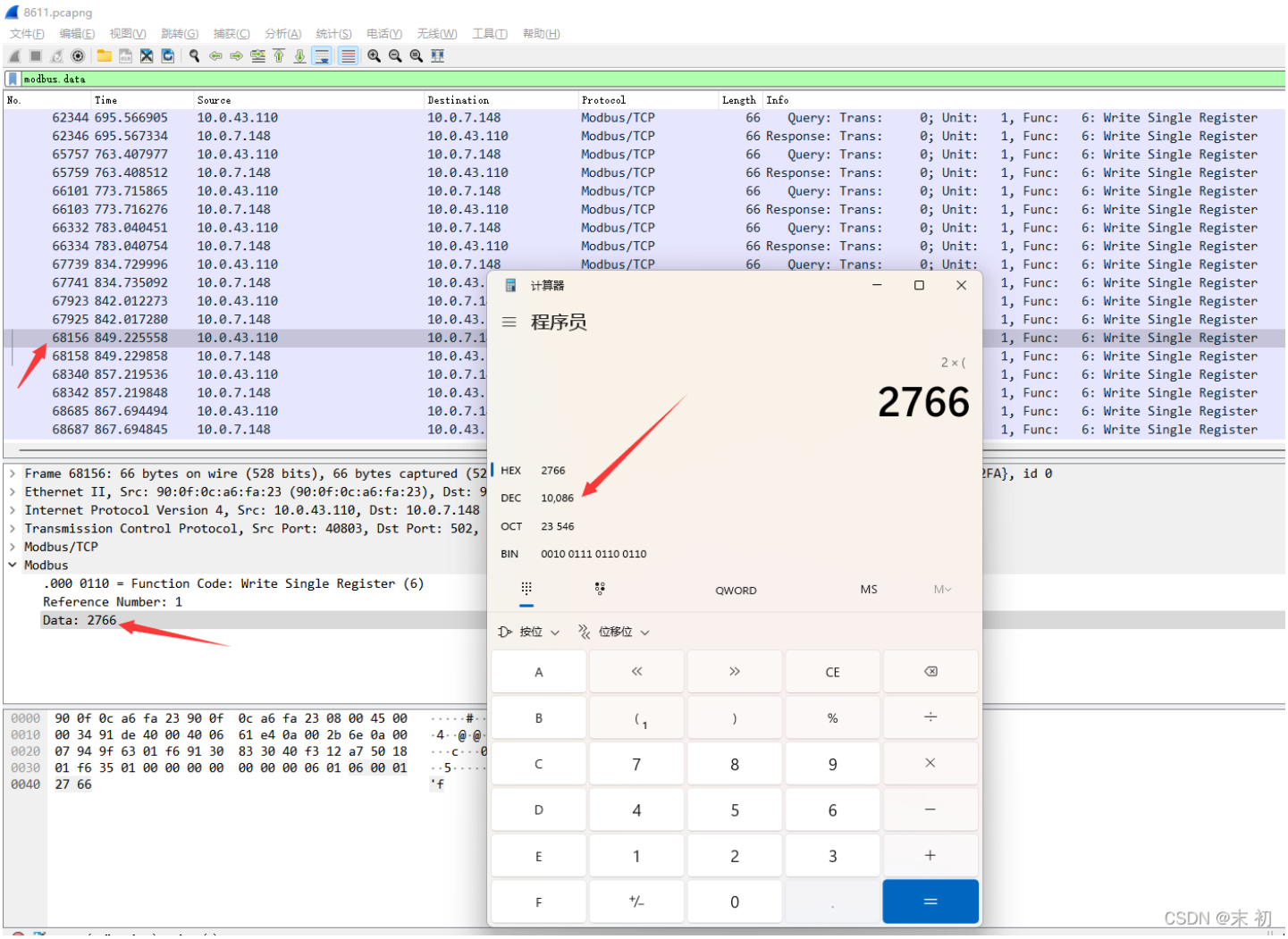
直接打开WireShark显示不是`pcapng`文件，修改文件头前四个字节



过滤器中输入`modbus.data`锁定转速数据的包



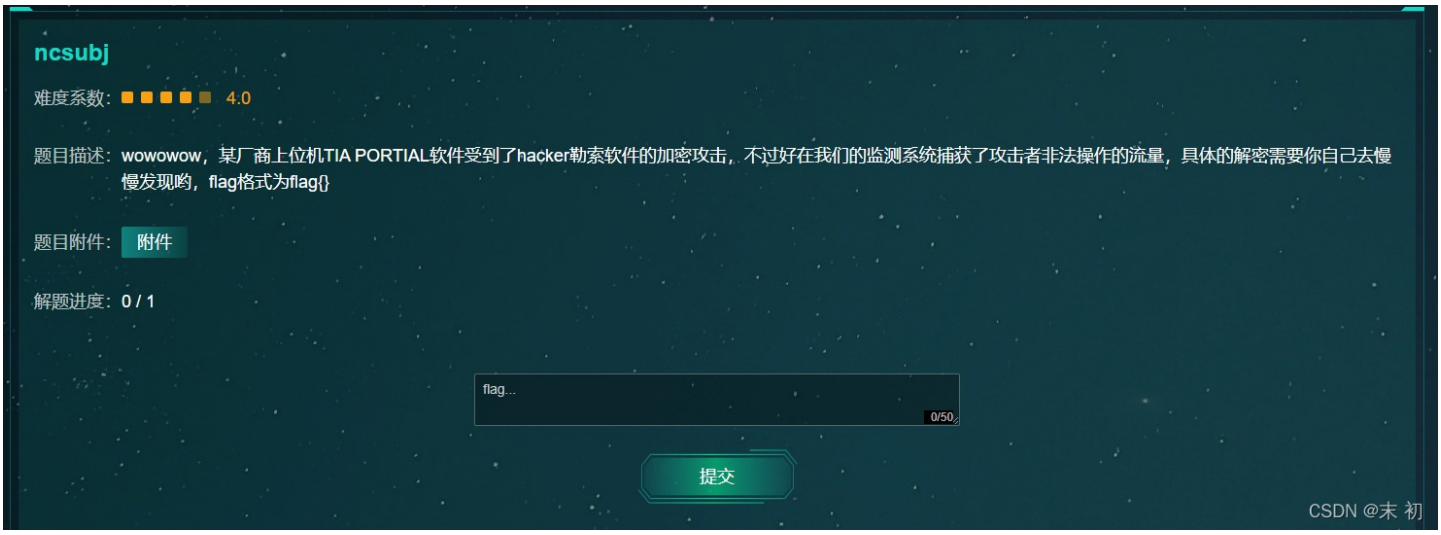
找到转速超过`10000`以上的数据包



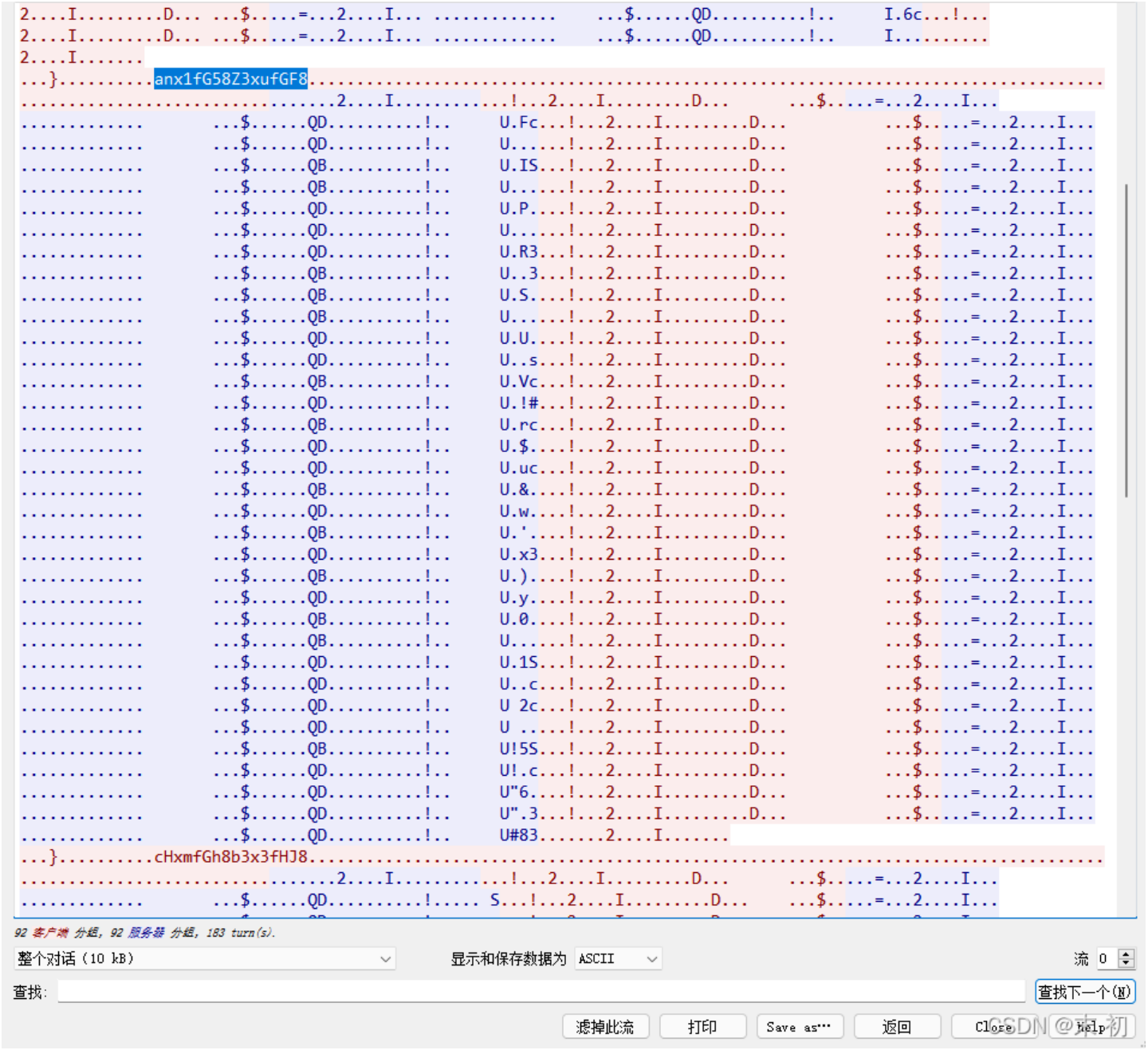
data是十六进制，转化一下十进制

```
flag{1008668156}
```

ncsubj

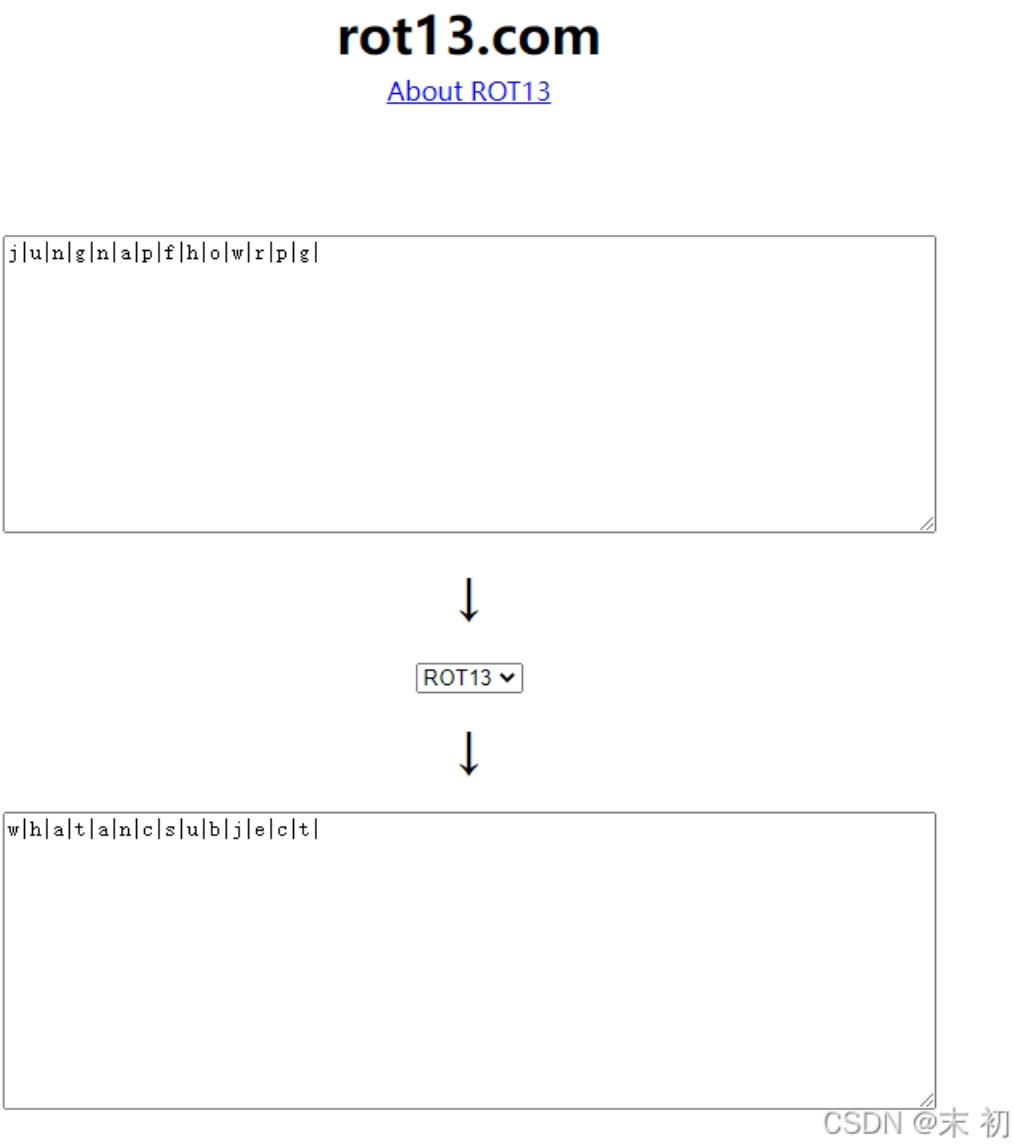


TCP追踪流，发现分成三段的base64



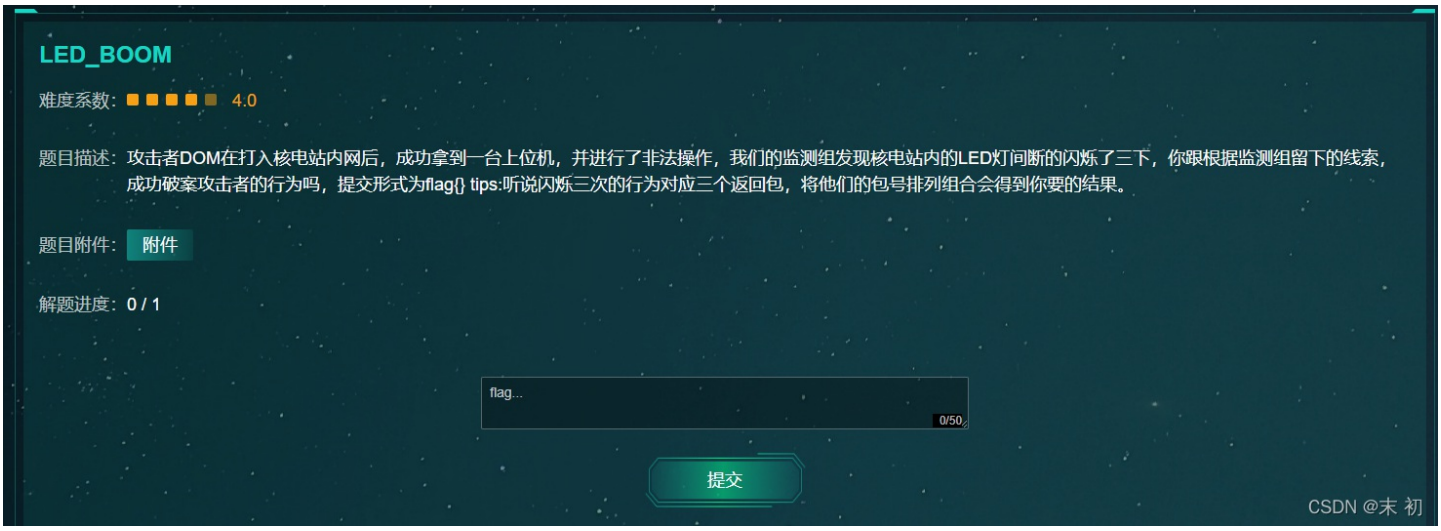

```
PS C:\Users\Administrator> php -r "var_dump(base64_decode('anx1fG58Z3xufGF8cHxmfGh8b3x3fHJ8cHxnfA=='));"
Command line code:1:
string(28) "j|u|n|g|n|a|p|f|h|o|w|r|p|g|"
```

rot13




```
flag{whatancsubject}
```

LED_BOOM



Base64 在线解码、编码

常规Base64 | CSS Base64 | DES加密/解密 | 3DES加密/解密 | AES加密/解密 | RSA加密/解密

U2FsdGVkX19c00V8qLVgcso8U4fse+7LirQKiHFkn9HU9BuwFAivH1siJXg/Rk6z

编码源格式：文本 Hex 解码结果： 自动检测 中文编码： UTF-8 编码 解码

```
00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
-----------------------------------------------
53 61 6C 74 65 64 5F 5F  5C D3 45 7C A8 B5 60 72
CA 3C 53 87 EC 7B EE CB  8A B4 0A 88 71 64 9F D1
D4 F4 1B B0 14 08 AF 1F  5B 22 25 78 3F 46 4E B3
```

插件【Salted】OpenSSL encrypted data

另存为：**salted文件**

附加信息：

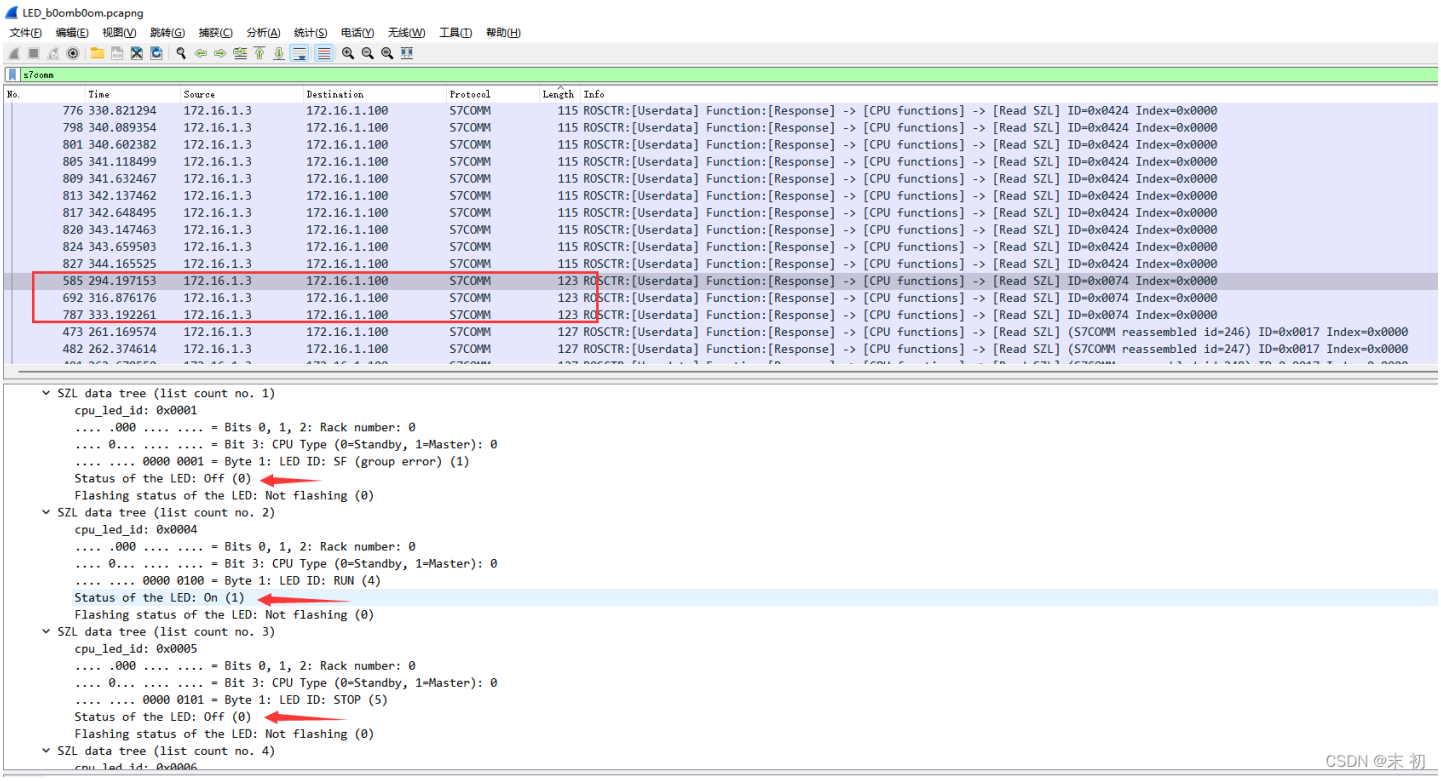
salte:5CD3457CA8B56072

当前编码：*[Hex]*

数据长度：*48 Bytes*

插件数：*18*，耗时：*0ms*

流量包过滤`s7comm`协议的包，按照提示寻找三个响应包，按长度排序很容易发现长度为`123`仅有的3个包，并且数据中有`LED On`或者`LED Off`



```
密文：U2FsdGVkX19cOOV8qLVgcso8U4fse+7LirQKiHFkn9HU9BuwFAivH1siJXg/Rk6z
密钥：585692787
```

AES解密：https://www.sojson.com/encrypt_aes.html


```
flag{tietie_tietie_tiet13}
```