

# 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

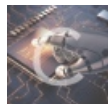
分类专栏: [CTF\\_MISC\\_Writeup](#) 文章标签: [2022第二届网刃杯](#)

于 2022-04-25 17:37:34 首次发布

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/124380608>

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

### MISC

[玩坏的winxp](#)

### ICS

[easyiec](#)

[xyp07](#)

[carefulguy](#)

[喜欢移动的黑客](#)

[ncsubj](#)

[LED\\_BOOM](#)

题目附件:

链接: <https://pan.baidu.com/s/1X1A0tSNwSFr7Lj7WTMT5cw>

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》: `bvis823HNas20cFKAJJS2KF1Ahasv`

《不要相信你所看到的》: `sur528WBC86Fj3da9QRscGW256f`

## MISC

### 玩坏的winxp

#### 玩坏的winxp

难度系数:  4.0

题目描述: 小敏的电脑Windows XP Professional不小心被玩坏了, 里边有重要的东西, 你能帮帮她吗?

题目附件: 附件

解题进度: 0 / 1

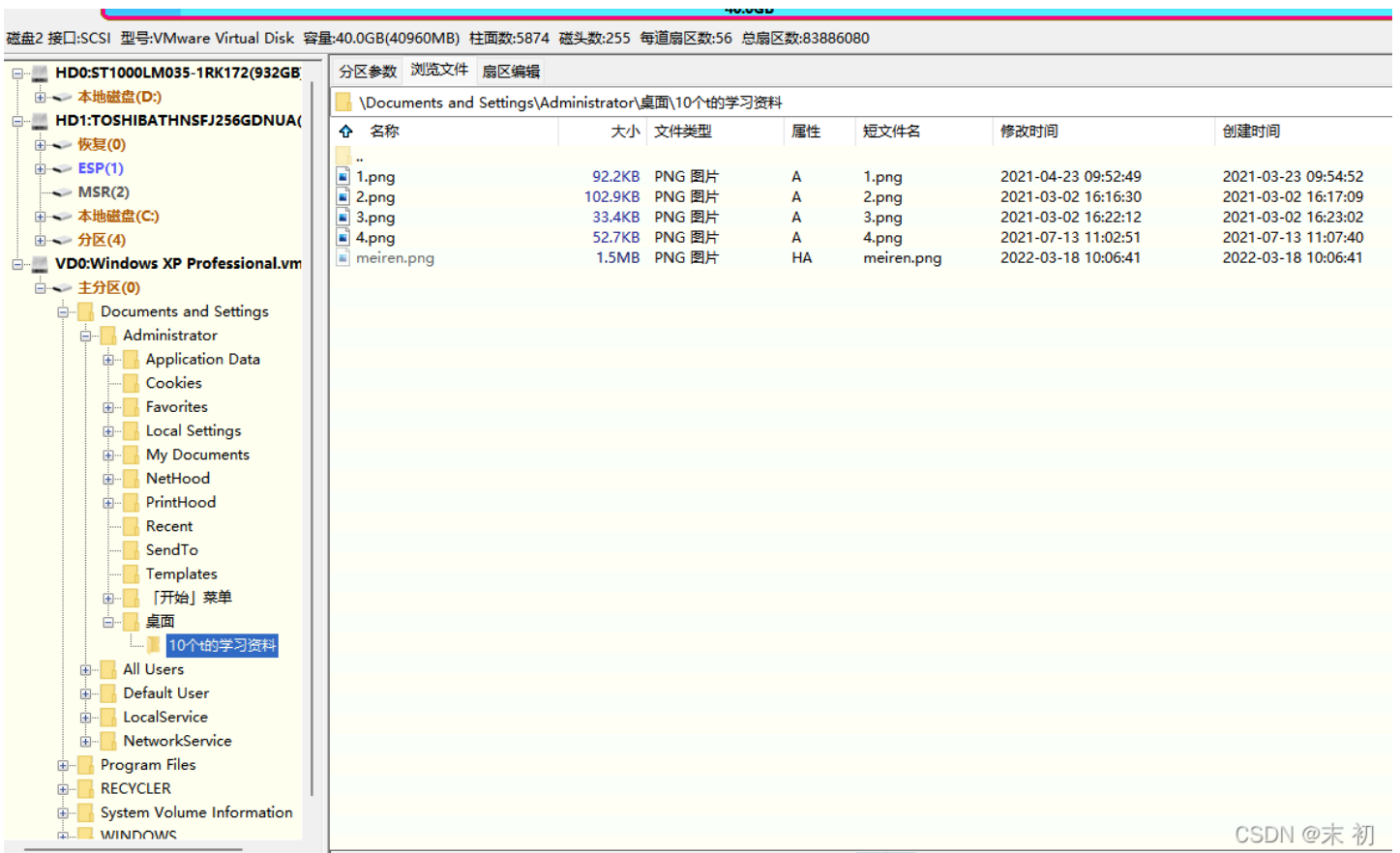
flag...

0/50

提交

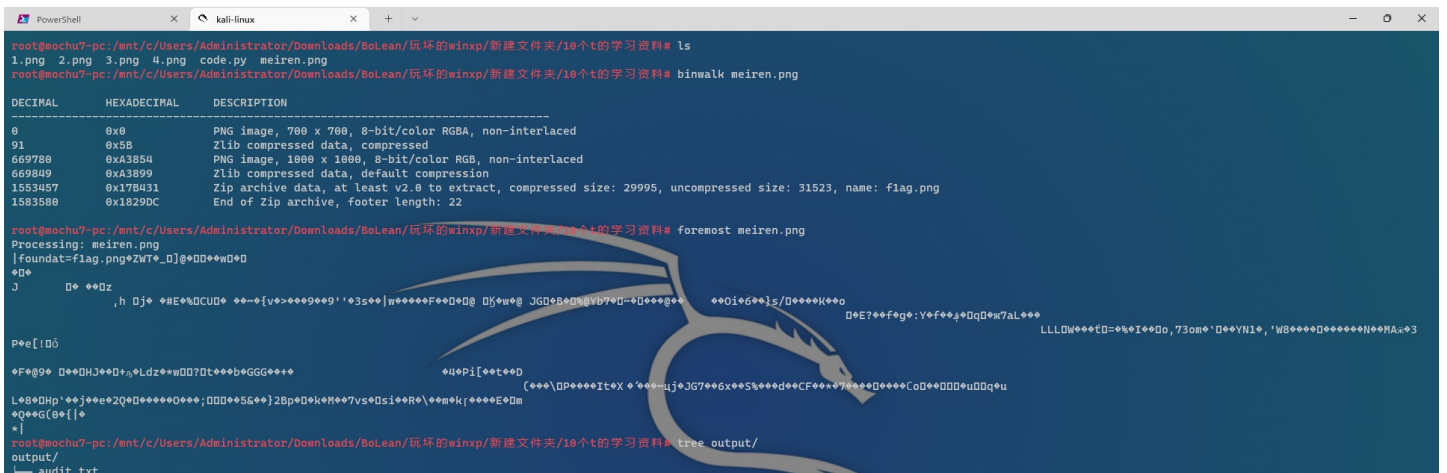
CSDN @末初

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



CSDN @末初

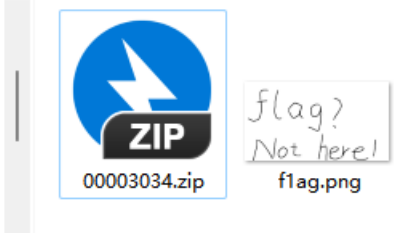
binwalk 分析 meiren.png, foremost 分离



```
├── png
│   ├── 00000000.png
│   └── 00001300.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# |
```

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 >



继续 binwalk 分析， foremost 分离 flag.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  flag.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 flag.png

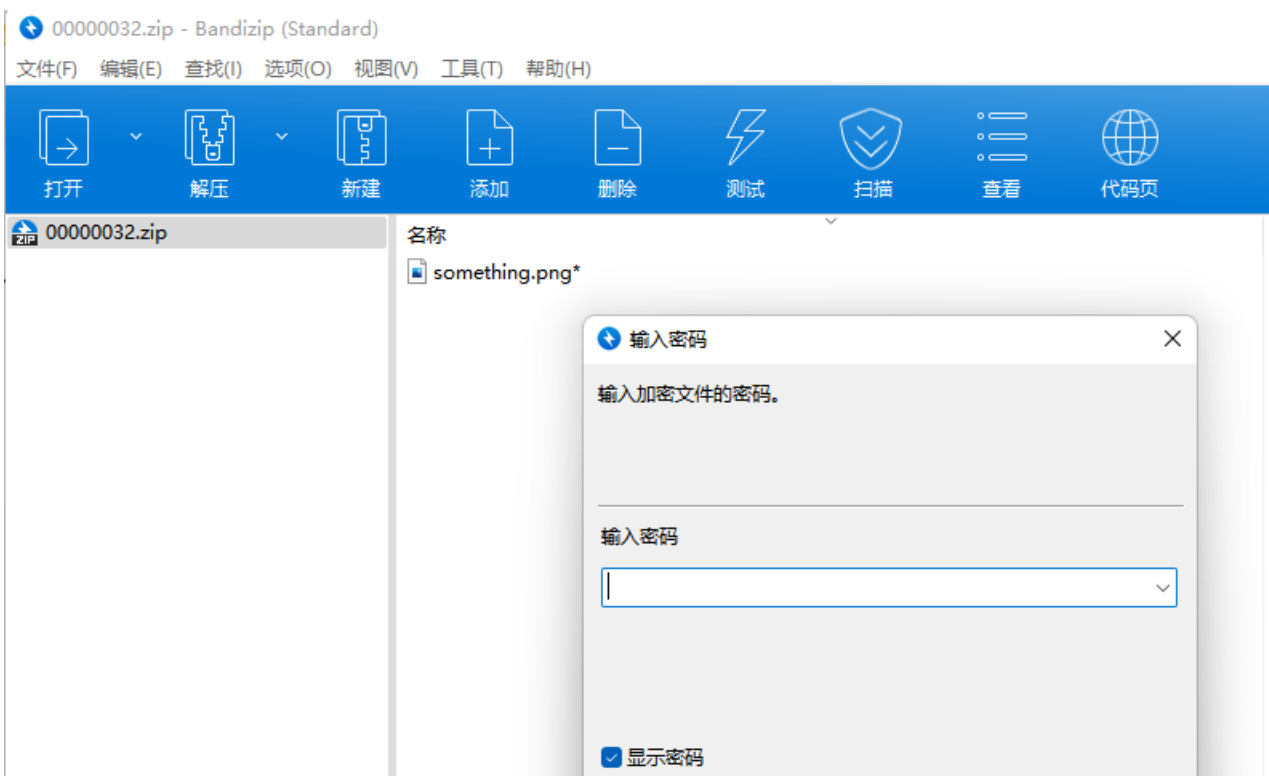
DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0             0x0             PNG image, 617 x 333, 8-bit/color RGB, non-interlaced
78           0x4E           Zlib compressed data, compressed
16871        0x41E7         Zip archive data, encrypted at least v2.0 to extract, compressed size: 14449, uncompressed 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 flag.png
Processing: flag.png
0[X0+L+Ai0 +000FY+E0zA00", 00/000P$0+[0hRp0+qG.00+300|00+0+0#00F'I=0C~0\;0V0z0000@]0G00+0gtC0><y3000G00(0080"=0KV00VQ000I0L_00c0
0M0'\00;00w=00v0}L00
tu0Ce000,0r

*|
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

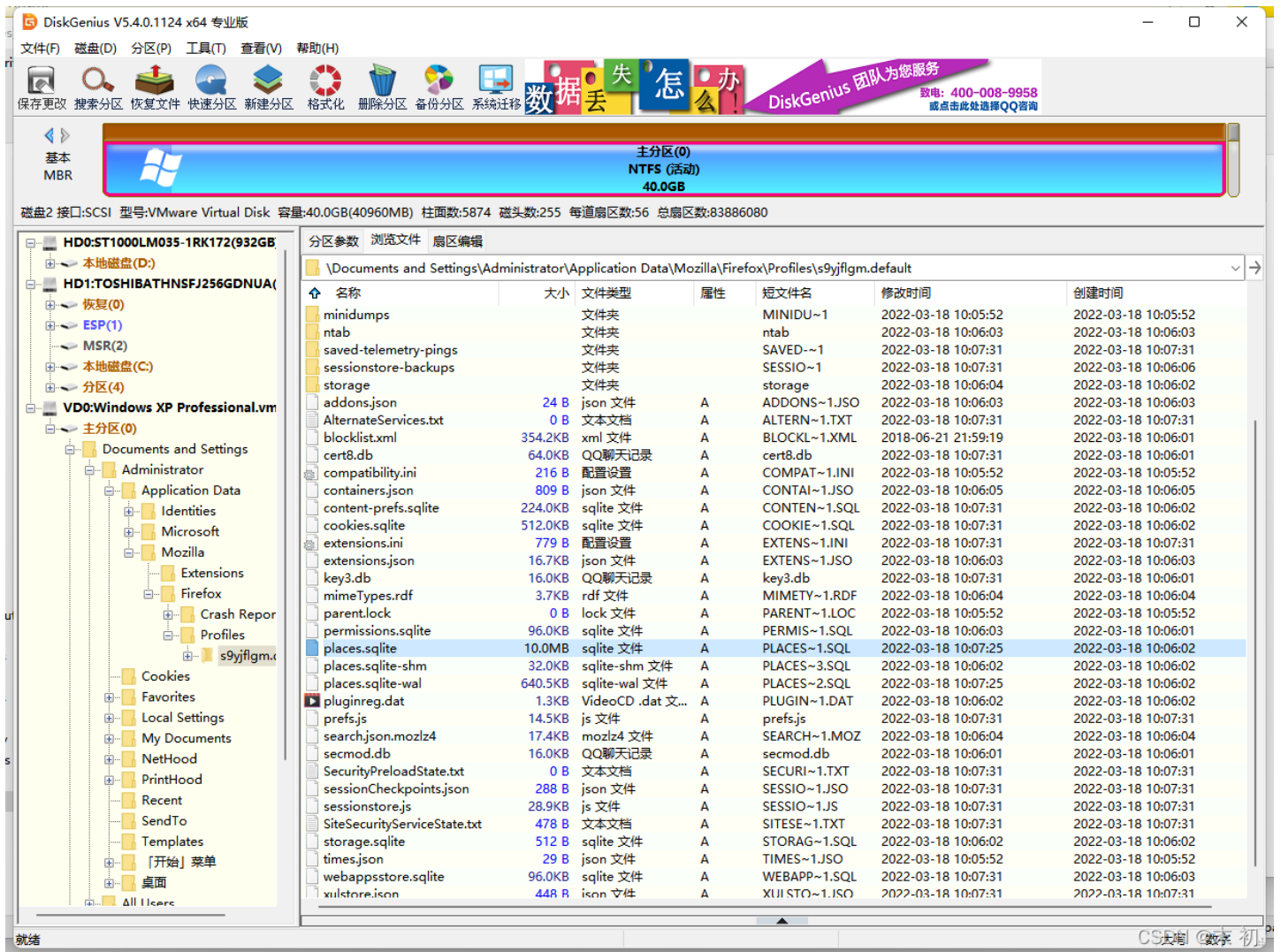
2 directories, 3 files
root@mochu7-pc: /mnt/c/Users/Administrator/Downloads/BoLean/玩坏的winxp/新建文件夹/10个t的学习资料/output/zip# |
```

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

moz\_places @main (places) - Table - Navicat Premium

File Edit View Table Favorites Tools Window Help

Connection New Query Table View Index Trigger User Query Backup Automation Model Charts

Objects groups @main (c... prefs @main (cont... settings @main (c... moz\_cookies @m... moz\_annos @mai... moz\_hosts @main... moz\_places @mai...

Begin Transaction Text Filter Sort Import Export Data Generation Create Chart

id	url	title	rev_host	visit_count	hidden	typed	favico
8	http://firefox.com.cn/download/mobile/?src=ffbookmark	(Null)	nc.moc.xoferif.	0	0	0	0
9	http://www.firefox.com.cn/	(Null)	nc.moc.xoferif.www.	0	0	0	0
10	http://www.firefoxchina.cn/	(Null)	nc.anihxoferif.www.	0	0	0	0
11	https://www.baidu.com/index.php?tn=monline_3_dg	(Null)	moc.udiab.www.	0	0	0	0
12	http://www.sina.com.cn/	(Null)	nc.moc.anis.www.	0	0	0	0
13	http://weibo.com/?c=spr_web_sq_firefox_weibo_t001	(Null)	moc.obiew.	0	0	0	0
14	http://www.163.com/	(Null)	moc.361.www.	0	0	0	0
15	http://youku.com/	(Null)	moc.ukooy.	0	0	0	0
16	http://ai.taobao.com/?pid=mm_28347190_2425761_17624777	(Null)	moc.oaboat.ia.	0	0	0	0
17	http://union.click.jd.com/jdc?e=&p=AilBZRprFDJWWA1FBCVbV0IUEULRFR	(Null)	moc.dj.kcil.noinu.	0	0	0	0
18	http://aos.pr.fh.click/camref:111IEF	(Null)	nh.frp.soa.	0	0	0	0
19	http://www.yihaodian.com/?tracker_u=10977119545	(Null)	moc.naidoahiy.www.	0	0	0	0
20	http://www.hao123.com/?tn=12092018_12_hao_pg	(Null)	moc.321oah.www.	0	0	0	0
21	http://c.duomai.com/track.php?k=nJ9QWa1VmJxYTPkIWYmcDOykzMx0DZj	(Null)	moc.iamoud.c.	0	0	0	0
22	placesort=8&maxResults=10	(Null)	.	0	0	0	0
23	placetype=6&sort=14&maxResults=10	(Null)	.	0	0	0	0
24	https://www.mozilla.org/zh-CN/firefox/52.9.0/firstrun/	欢迎使用 Firefox	gro.allizom.www.	1	0	0	0
25	https://home.firefoxchina.cn/	火狐主页	nc.anihxoferif.emoh.	1	0	0	0
26	https://www.hao123.com/?tn=55030201_hao_pg	(Null)	moc.321oah.www.	0	0	0	0
27	https://u.jd.com/nwPGabv	(Null)	moc.dju.	0	0	0	0
28	https://www.ifeng.com/?source=mozilla	(Null)	moc.gnefi.www.	0	0	0	0
29	https://www.ctrip.com/?AllianceID=263200&sid=1851274&couid=&app=01	(Null)	moc.pirtc.www.	0	0	0	0
30	https://weibo.com/?source=mozilla	(Null)	moc.obiew.	0	0	0	0
31	https://c.duomai.com/track.php?k=nJ9QWa1VmJxYTPkIWYmcDOykzMx0DZj	(Null)	moc.iamoud.c.	0	0	0	0
32	https://ai.taobao.com/?pid=mm_28347190_2425761_17624777	(Null)	moc.oaboat.ia.	0	0	0	0
33	http://10.30.7.1:8000/	Directory listing for /	1.7.03.01.	1	0	0	1
34	http://10.30.7.1:8000/meiren.png	meiren.png (PNG 图)	1.7.03.01.	1	0	0	0
35	http://10.30.7.1:8000/login.html?qq=1272045963	(Null)	1.7.03.01.	17	0	0	1

url  
Type  
LONGVARCHAR  
Not null  
No  
Default Value  
Comment

SELECT \*,rowid "NAVICAT\_ROWID" FROM "main"."moz\_places" LIMIT 0,1000

Record 35 of 35 in page 1

在开放的QQ空间中找到留言



留个言吧...



Harry

03-17 10:49

dc45445a8a099e63fbb9b8480d57723a

CSDN @末 初

密文: dc45445a8a099e63fbb9b8480d57723a

类型: 自动 [帮助]

查询

加密

查询结果:

xiaomin520

CSDN @末 初

得到解压密码: [xiaomin520](#)

flag{this\_is  
-what\_u  
-want8}

CSDN @末初

```
flag{this_is_what_u_want8}
```

ICS

easyiee

```
tcp contains "flag"
```

easyiec.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

top contains "flag"

No.	Time	Source	Destination	Protocol	Length	Info
542	66.030808	192.168.183.1	192.168.183.157	IEC 60870-5 ASDU	90	<- I (112,138) ASDU=1 F_SG_NA_1 File IOA=0

Frame 542: 90 bytes on wire (720 bits) 90 bytes captured (720 bits)

```

0000  00 0c 29 5f 1c 5e 00 50 56 c0 00 08 08 00 45 00  ..)_.^P.V.....E.
0010  00 4c 14 a5 40 00 80 06 f6 16 c0 a8 b7 01 c0 a8  .L.@.....
0020  b7 9d f3 13 09 64 2e ab 4d 54 8d 36 b9 37 50 18  ....d..MT.6.7P.
0030  10 09 27 6f 00 00 68 22 e0 00 14 01 7d 01 0d 00  ..'o..h"....}...
0040  01 00 00 00 00 01 00 01 11 66 6c 61 67 7b 65 34  ....flag{e4
0050  35 79 5f 31 65 63 69 30 34 7d                    5y_1eci0 4}
  
```

CSDN @末初

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

我的图表 概要 诊断 x 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 服务 端口 VoIP呼叫 进程 应用 矩阵 数据包 日志 报表

诊断条目

回放分析\诊断条目: 5

名字	数量
所有诊断	4
传输层	1
TCP 非法的校验和	1
数据链路层	3
ARP 扫描	3

诊断发生地址

名字
192.168.190.1
192.168.190.185
VMware, Inc.-DC
VMware, Inc.-CO

诊断事件

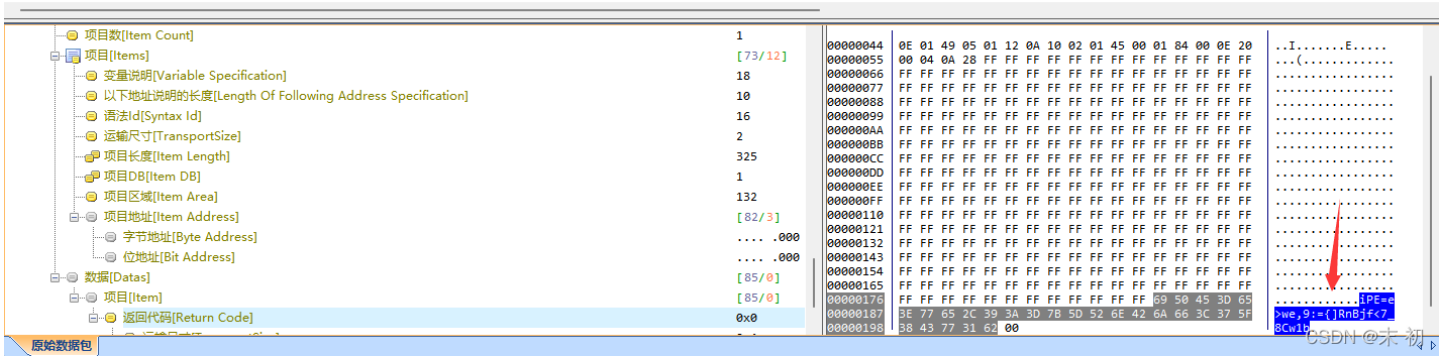
时间	严重程度	类型	层别	事件描述
2022/03/16 10:11:34.106581000	故障	故障	传输层	错误的TCP数据包校验和(请看数据包: 1425)

CSDN @末初

数据包 - 诊断事件 - 分析工程 1

编号	日期	绝对时间	源	源端口	源地地理位置	目标	目标端口	目标地理位置	协议	应用
1425	2022/03/16	10:11:34.106581000	192.168.190.1	54066	本地	192.168.190.185	102	本地	S7	





# 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**

难度系数: ■■■■■ 4.0

题目描述: 电厂工程师Bob正在将对电磁阀的工程写入PLC, 传输时受到黑客攻击被迫停止, 重启后才恢复运作, 黑客的攻击导致工程师的数据丢失了一些, 实时监测设备抓到一些流量包, 你能从流量包中找出丢失的数据吗?

题目附件: [附件](#)

解题进度: 0 / 1

flag...

提交

CSDN @末初

从 `tcp.stream eq 3` 开始往后有flag的十六进制

Wireshark · 追踪 TCP 流 (tcp.stream eq 3) · carefulguy.pcapng

The image shows a Wireshark packet capture window. The title bar reads "Wireshark · 追踪 TCP 流 (tcp.stream eq 3) · carefulguy.pcapng". The main display area shows a list of packets. The selected packet (packet 66) is highlighted in blue. A red arrow points to the hex value "66" in the packet's payload. The packet details pane shows the following structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The payload is shown in hex and ASCII: "W. \. .... .%. ...".

```
>>> from binascii import *
>>> flag='666c616777b7034757333313576337279316e74333726573746963397d'
>>> unhexlify(flag)
b'flag{p4us315v3ry1nt3restic9}'
```

## 喜欢移动的黑客

**喜欢移动的黑客**

难度系数: ■■■■■ 3.0

题目描述: Monkey是一家汽修厂的老板, 日常喜欢改装车, 但由于发动机的转速有上限, 发动机最多能接受10000转/分钟的转速, Monkey在最新一次对发动机转速进行测试时发生了故障, 机械师阿张排查时测试期间, 有一些异常的流量, 请根据阿张捕获的流量包分析发动机的转速达到了多少转才出现的故障, flag为flag(data+包号)

题目附件: [附件](#)

解题进度: 0 / 1

flag...

提交

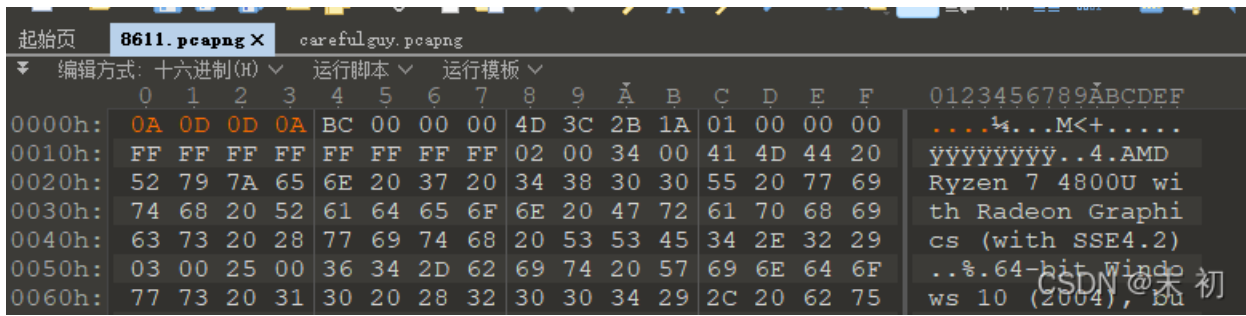
CSDN @末初

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

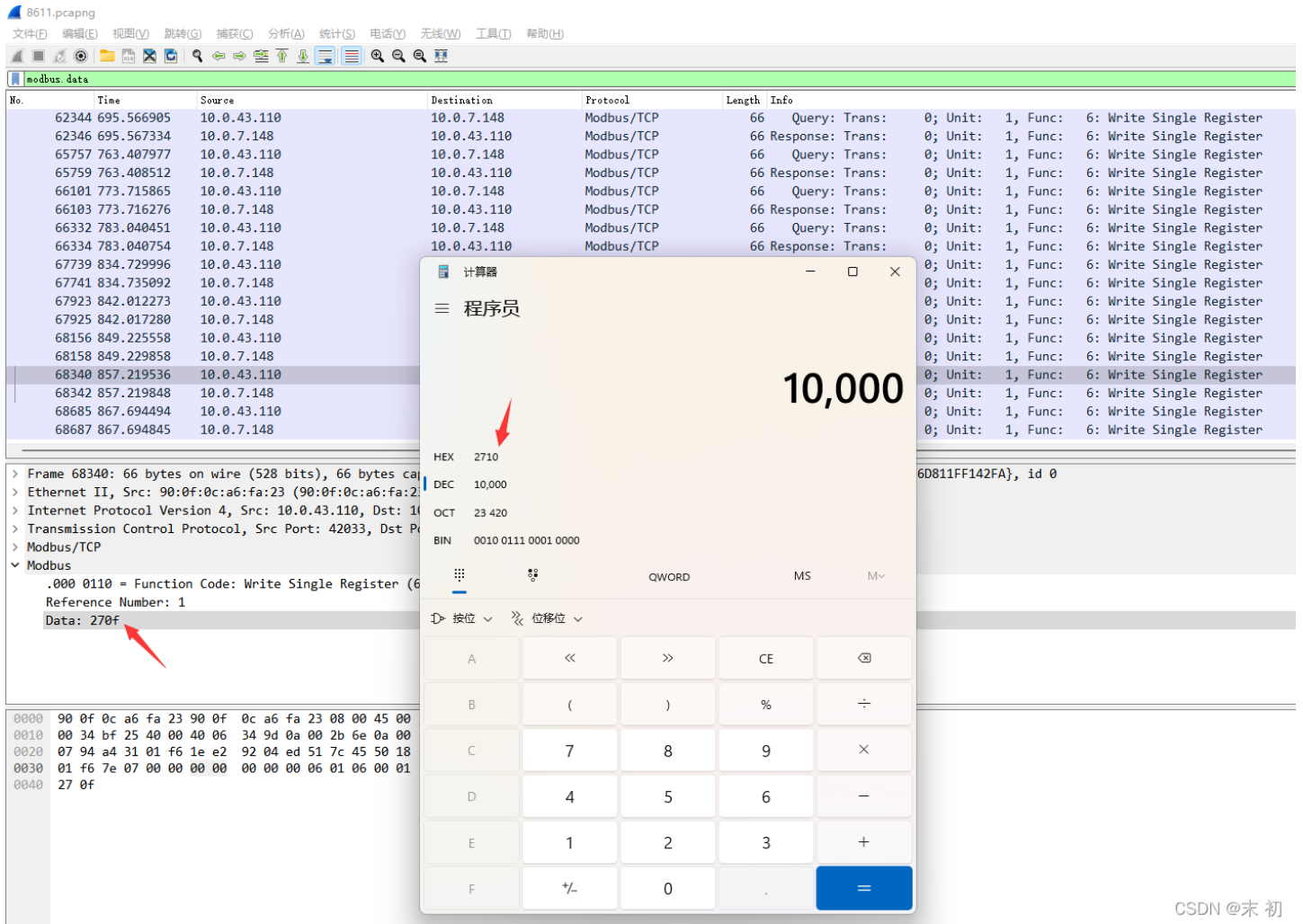
010 Editor - C:\Users\Administrator\Downloads\BoLean\喜欢移动的黑客\8611.pcapng

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)

The image shows the 010 Editor interface. The title bar reads "010 Editor - C:\Users\Administrator\Downloads\BoLean\喜欢移动的黑客\8611.pcapng". The menu bar includes "文件(F)", "编辑(E)", "搜索(S)", "视图(V)", "格式(O)", "脚本(I)", "模板(L)", "调试(D)", "工具(T)", "窗口(W)", and "帮助(H)". The main display area shows the file header of the pcapng file, with the first four bytes highlighted in blue. The header is shown in hex and ASCII: "0x00000000".



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

8611.pcapng

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

No.	Time	Source	Destination	Protocol	Length	Info
62344	695.566905	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
62346	695.567334	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
65757	763.407977	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
65759	763.408512	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
66101	773.715865	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
66103	773.716276	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
66332	783.040451	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
66334	783.040754	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
67739	834.729996	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
67741	834.735092	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
67923	842.012273	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
67925	842.017280	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
68156	849.225558	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
68158	849.229858	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
68340	857.219536	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
68342	857.219848	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
68685	867.694494	10.0.43.110	10.0.7.148	Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
68687	867.694845	10.0.7.148	10.0.43.110	Modbus/TCP	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register

> Frame 68156: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: 90:0f:0c:a6:fa:23 (90:0f:0c:a6:fa:23), Dst: 90:0f:0c:a6:fa:23

> Internet Protocol Version 4, Src: 10.0.43.110, Dst: 10.0.7.148

> Transmission Control Protocol, Src Port: 40803, Dst Port: 502, Seq: 10086, Win: 0, Len: 0

> Modbus/TCP

Modbus

.000 0110 = Function Code: Write Single Register (6)

Reference Number: 1

Data: 2766

HEX 2766

DEC 10,086

OCT 23 546

BIN 0010 0111 0110 0110

计算器

程序员

2766

0000 90 0f 0c a6 fa 23 90 0f 0c a6 fa 23 08 00 45 00

0010 00 34 91 de 40 00 40 06 61 e4 0a 00 2b 6e 0a 00

0020 07 94 9f 63 01 f6 91 30 83 30 40 f3 12 a7 50 18

0030 01 f6 35 01 00 00 00 00 00 00 00 06 01 06 00 01

0040 27 66

CSDN @末初

data 是十六进制，转化一下十进制

flag{10086668156}

## ncsubj

ncsubj

难度系数: 4.0

题目描述: wowowow, 某厂商上位机TIA PORTIAL软件受到了hacker勒索软件的加密攻击, 不过好在我们的监测系统捕获了攻击者非法操作的流量, 具体的解密需要你自己去慢慢发现哟, flag格式为flag{}

题目附件: 附件

解题进度: 0 / 1

flag...

提交

CSDN @末初

TCP追踪流，发现分成三段的base64

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · ncsubj.pcapng

```

2...I.....D...$....=.2...I.....$....QD.....!.. I.6c...!...
2...I.....D...$....=.2...I.....$....QD.....!.. I.....
2...I.....
...}.....anx1fG58Z3xufGF8.....
.....2...I.....!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.Fc...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.....!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.IS...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.....!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.P...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.....!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.R3...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U..3...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.S...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.....!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.U...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U..s...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.Vc...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.!#...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.rc...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.$...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.uc...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.&...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.w...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.'...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.x3...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.)...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.y...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.0...!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U.....!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U.15...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U..c...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U 2c...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U .....!..2...I.....D...$....=.2...I...
.....$....QB.....!.. U!55...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U!.c...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U"6...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U".3...!..2...I.....D...$....=.2...I...
.....$....QD.....!.. U#83...!..2...I.....
...}.....cHxmfGh8b3x3fHJ8.....
.....2...I.....!..2...I.....D...$....=.2...I...
.....$....QD.....!.. S...!..2...I.....D...$....=.2...I...

```

92 客户端 分組, 92 服务器 分組, 183 turn(s).

整个对话 (10 kB) 显示和保存数据为 ASCII 流 0

查找:  查找下一个(N)

滤掉此流 打印 Save as... 返回 Close @ 初

```

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.com

[About ROT13](#)

```
j|u|n|g|n|a|p|f|h|o|w|r|p|g|
```



ROT13 ▾



```
w|h|a|t|a|n|c|s|u|b|j|e|c|t|
```

CSDN @末初

```
flag{whatancsubject}
```

## LED\_BOOM

### LED\_BOOM

难度系数: ■ ■ ■ ■ ■ 4.0

题目描述: 攻击者DOM在打入核电站内网后, 成功拿到一台上位机, 并进行了非法操作, 我们的监测组发现核电站内的LED灯间断的闪烁了三次, 你跟根据监测组留下的线索, 成功破案攻击者的行为吗, 提交形式为flag{} tips:听说闪烁三次的行为对应三个返回包, 将他们的包号排列组合会得到你要的结果。

题目附件: [附件](#)

解题进度: 0 / 1

flag... 0/50

提交

CSDN @末初

# 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

U2FsdGVkX19c0V08qLVgcs08U4fse+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

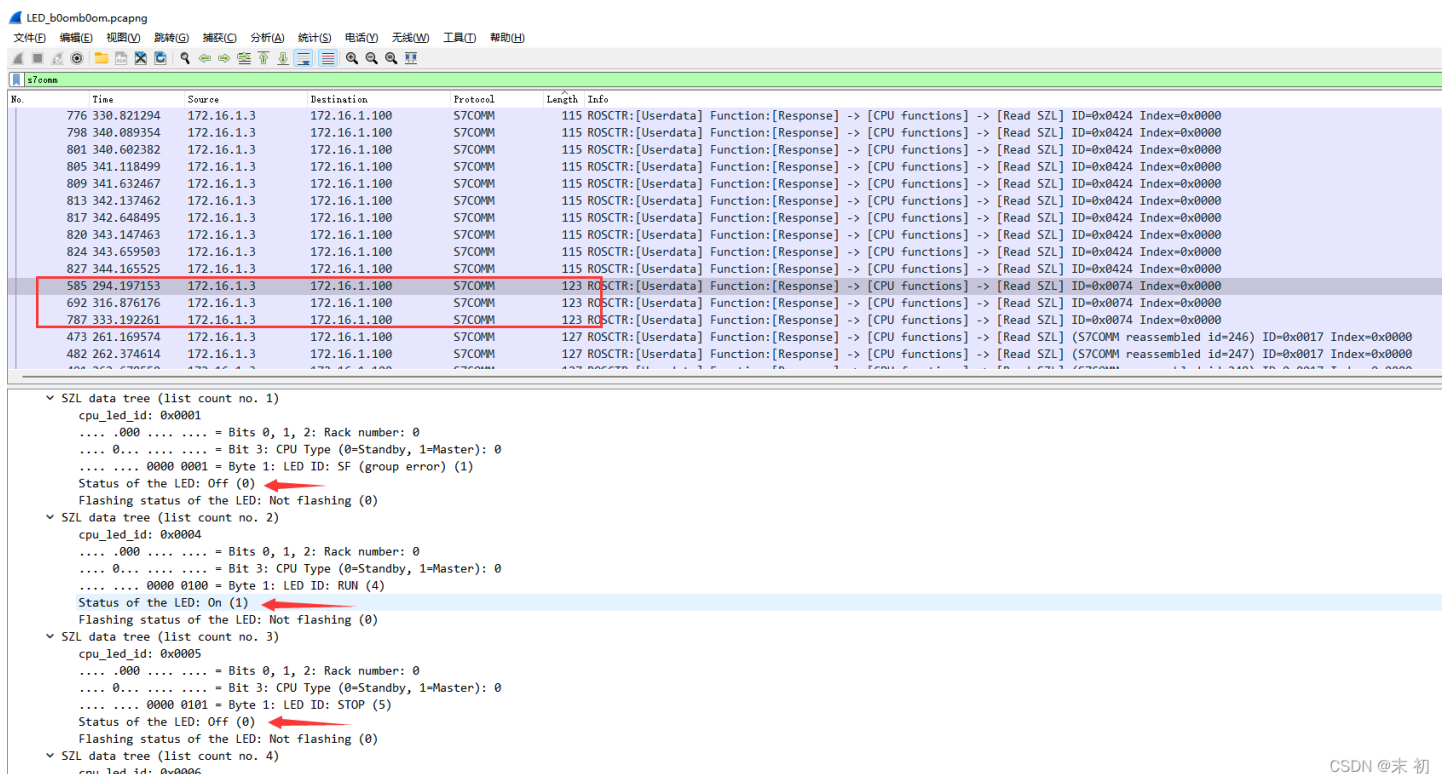
当前编码: [Hex]

数据长度: 48 Bytes

插件数: 18, 耗时: 0ms

CSDN @末初

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



LED\_b0omb0om.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

No.	Time	Source	Destination	Protocol	Length	Info
776	330.821294	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
798	340.089354	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
801	340.602382	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
805	341.118499	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
809	341.632467	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
813	342.137462	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
817	342.648495	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
820	343.147463	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
824	343.659503	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
827	344.165525	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0424 Index=0x0000
585	294.197153	172.16.1.3	172.16.1.100	S7COMM	123	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0074 Index=0x0000
692	316.876176	172.16.1.3	172.16.1.100	S7COMM	123	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0074 Index=0x0000
787	333.192261	172.16.1.3	172.16.1.100	S7COMM	123	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0074 Index=0x0000
473	261.169574	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] (S7COMM reassembled id=246) ID=0x0017 Index=0x0000
482	262.374614	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] (S7COMM reassembled id=247) ID=0x0017 Index=0x0000

▼ SZL data tree (list count no. 1)  
cpu\_led\_id: 0x0001  
....000 .... = Bits 0, 1, 2: Rack number: 0  
....0... .... = Bit 3: CPU Type (0=Standby, 1=Master): 0  
.... .... 0000 0001 = Byte 1: LED ID: SF (group error) (1)  
Status of the LED: Off (0)  
Flashing status of the LED: Not flashing (0)

▼ SZL data tree (list count no. 2)  
cpu\_led\_id: 0x0004  
....000 .... = Bits 0, 1, 2: Rack number: 0  
....0... .... = Bit 3: CPU Type (0=Standby, 1=Master): 0  
.... .... 0000 0100 = Byte 1: LED ID: RUN (4)  
Status of the LED: On (1)  
Flashing status of the LED: Not flashing (0)

▼ SZL data tree (list count no. 3)  
cpu\_led\_id: 0x0005  
....000 .... = Bits 0, 1, 2: Rack number: 0  
....0... .... = Bit 3: CPU Type (0=Standby, 1=Master): 0  
.... .... 0000 0101 = Byte 1: LED ID: STOP (5)  
Status of the LED: Off (0)  
Flashing status of the LED: Not flashing (0)

▼ SZL data tree (list count no. 4)  
cpu\_led\_id: 0x0006

CSDN @末初

密文: U2FsdGVkX19c0OV8qLVgcso8U4fse+7LirQKiHFkn9HU9BuwFAivH1siJXg/Rk6z  
密钥: 585692787

AES解密: [https://www.sojson.com/encrypt\\_aes.html](https://www.sojson.com/encrypt_aes.html)

首页 / 加密 & 解密 / AES加密 / 解密

加密/解密   AES加密/解密   DES加密/解密   RC4加密/解密   Rabbit加密/解密   TripleDes加密/解密   MD5加密   Base64加密   Hash加密   JS 加密   JS 解密

flag(tietie\_tietie\_tiet13)

585692787

U2FsdGVkX19c0OV8qLVgcso8U4fse+7LirQKiHFkn9HU9BuwFAivH1siJXg/Rk6z

密码是可选项，也就是可以不填。

< 解密

加密 >

解密成功

CSDN @末初

flag{tietie\_tietie\_tiet13}