CTF——MISC习题讲解（流量分析winshark系列~四）

原创

TJA小傲 于 2022-03-17 14:59:09 发布 1391 收藏 1

分类专栏： CTF-Misc 文章标签： web安全

本文链接：https://blog.csdn.net/tlovejr/article/details/123541872

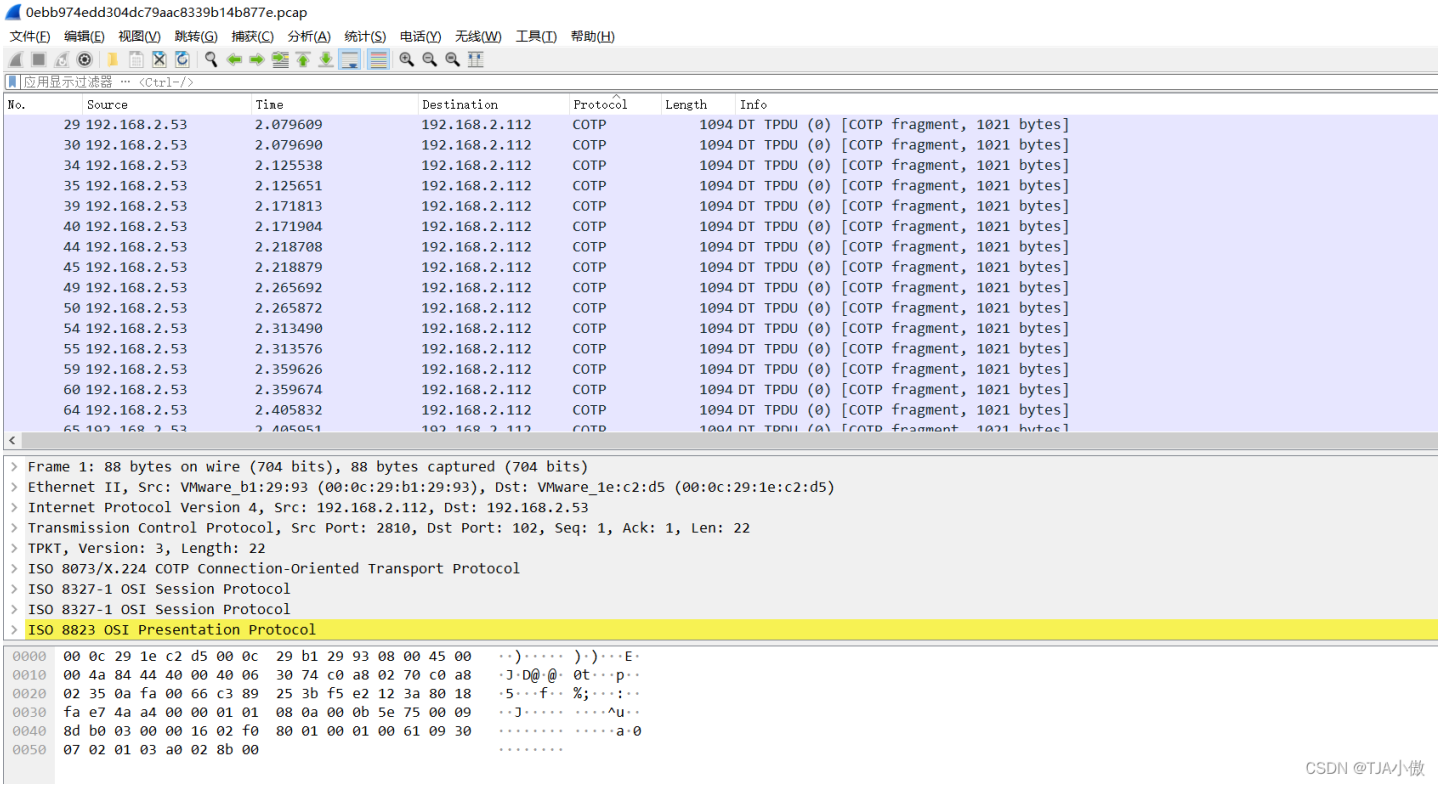
CTF——MISC习题讲解（流量分析winshark系列~四）

前言

上一章节我们已经做完一场流量分析杂项题目，接下来继续给大家讲解流量分析系列四。

一、工控协议分析

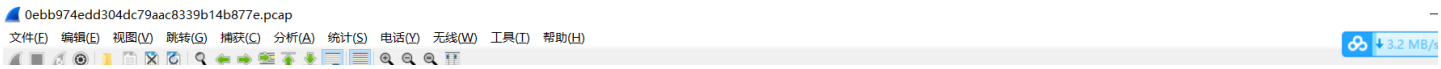
首先打开题目如下

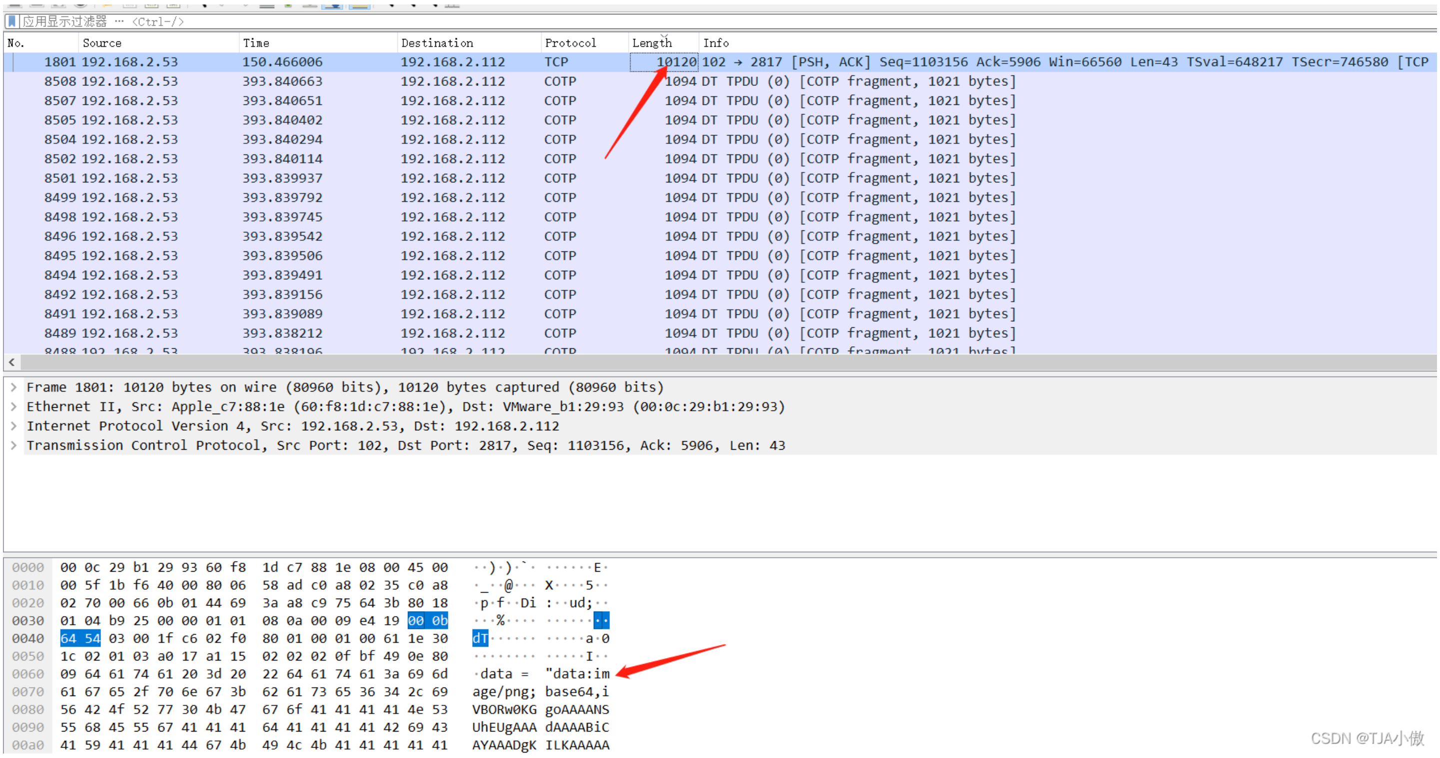


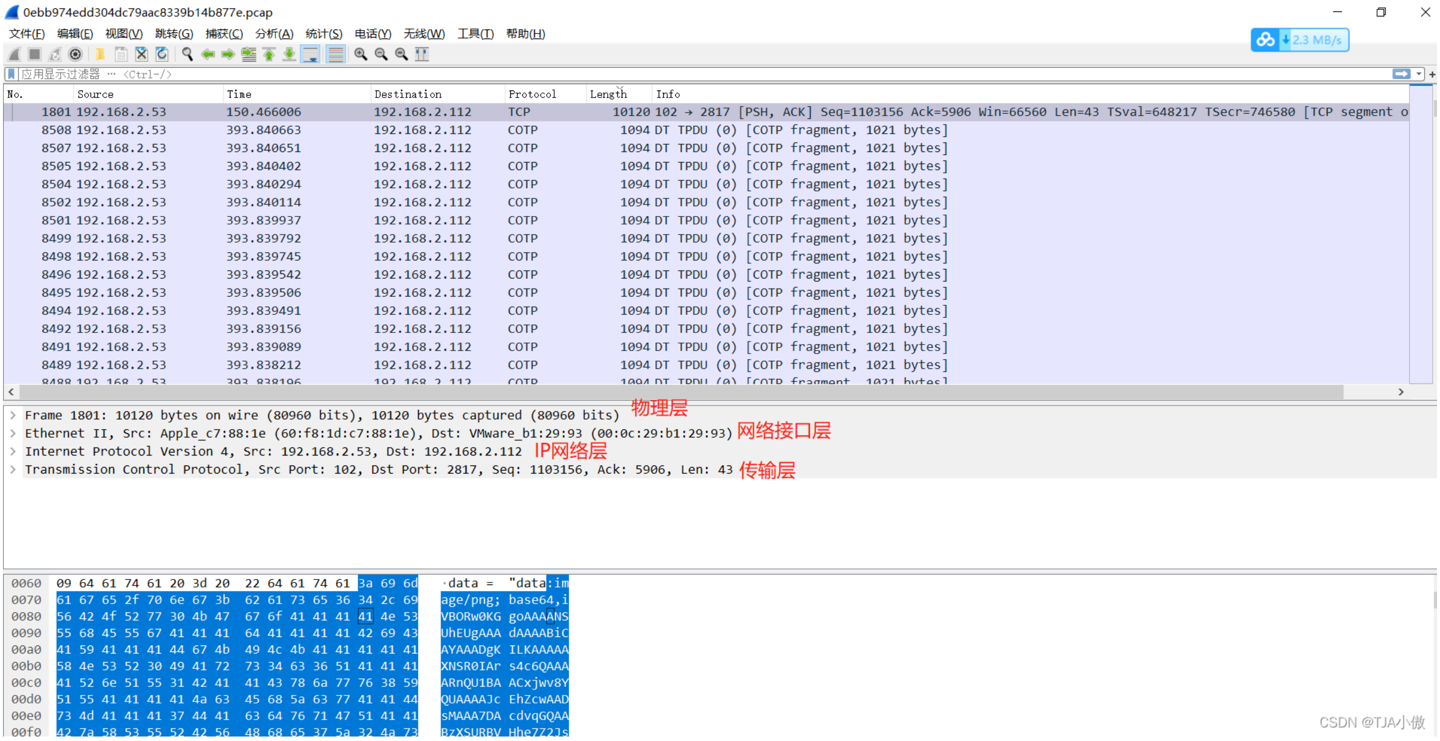
搜索flag发现也没有什么有用的东西

其实在做流分题中还是有一个小技巧，就是看一下长度

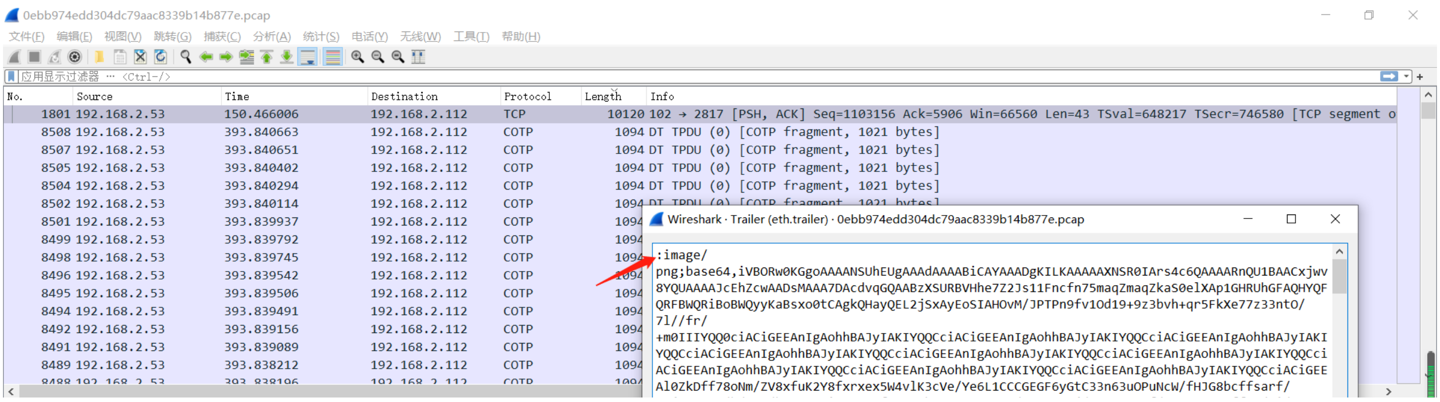
排序看到确实有一个长度过于长，而且在下面也有base编码

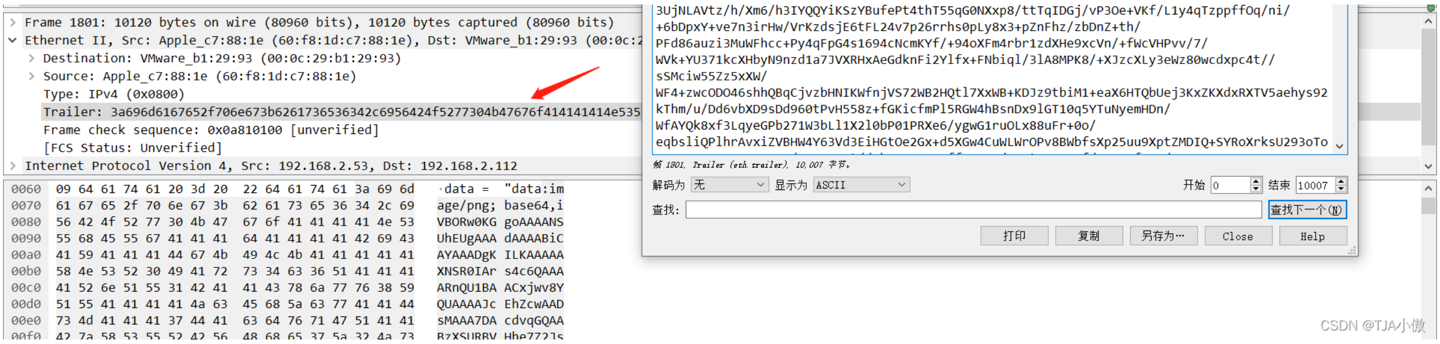



Frame 1801: 10120 bytes on wire (80960 bits), 10120 bytes captured (80960 bits)
Ethernet II, Src: Apple_c7:88:1e (60:f8:1d:c7:88:1e), Dst: VMware_b1:29:93 (00:0c:29:b1:29:93)
Internet Protocol Version 4, Src: 192.168.2.53, Dst: 192.168.2.112
Transmission Control Protocol, Src Port: 102, Dst Port: 2817, Seq: 1103156, Ack: 5906, Len: 43
CSDN @TJA小傲

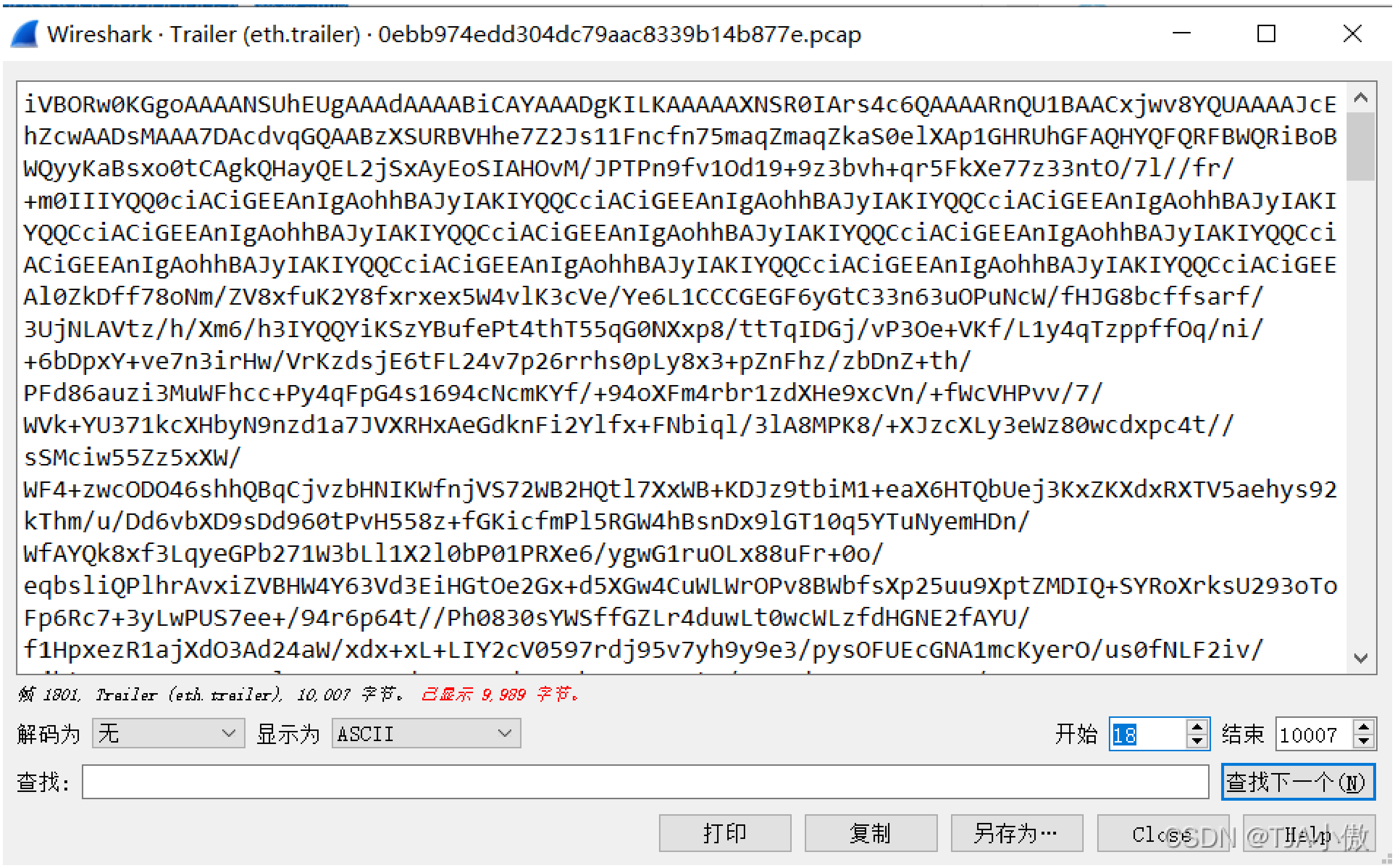

0ebb974edd304dc79aac8339b14b877e.pcap
物理层
网络接口层
IP网络层
传输层
CSDN @TJA小傲

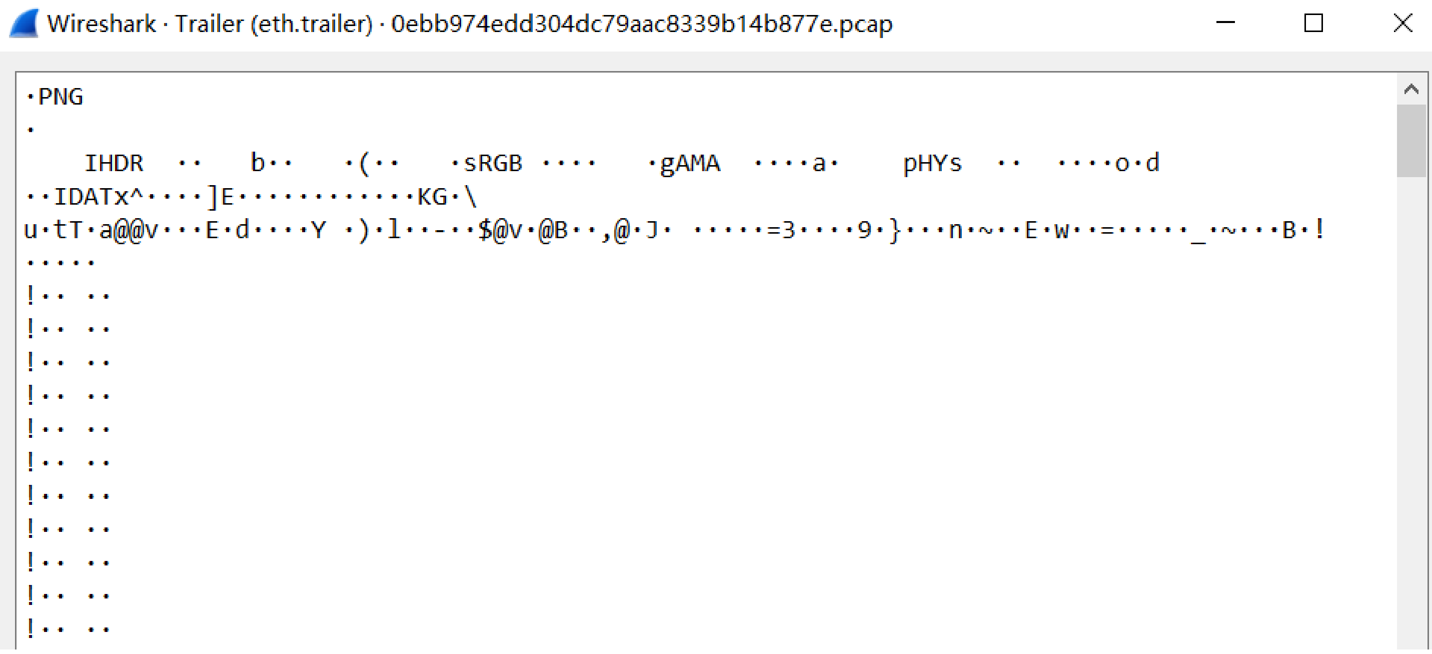
然后导出分组字节流

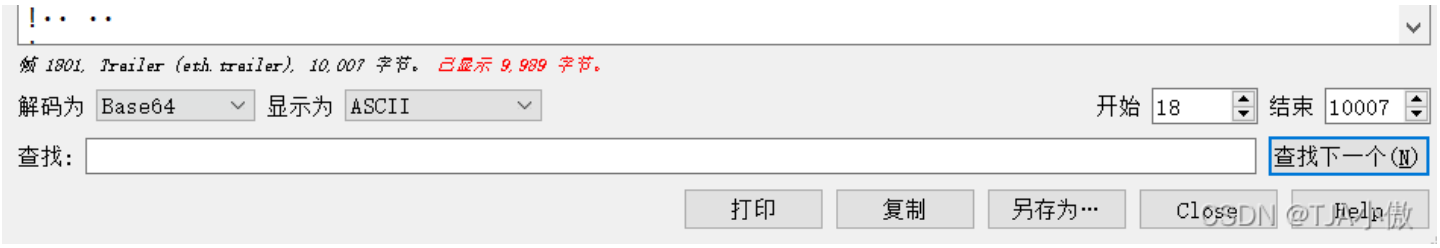

Wireshark · Trailer (eth.trailer) · 0ebb974edd304dc79aac8339b14b877e.pcap
:image/
png;base64,iVBORw0KGgoAAAANSUhEUgAAAdAAAABiCAYAAADgKILKAAAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv



这样的话先把对于的东西给去除，然后进行base64解码







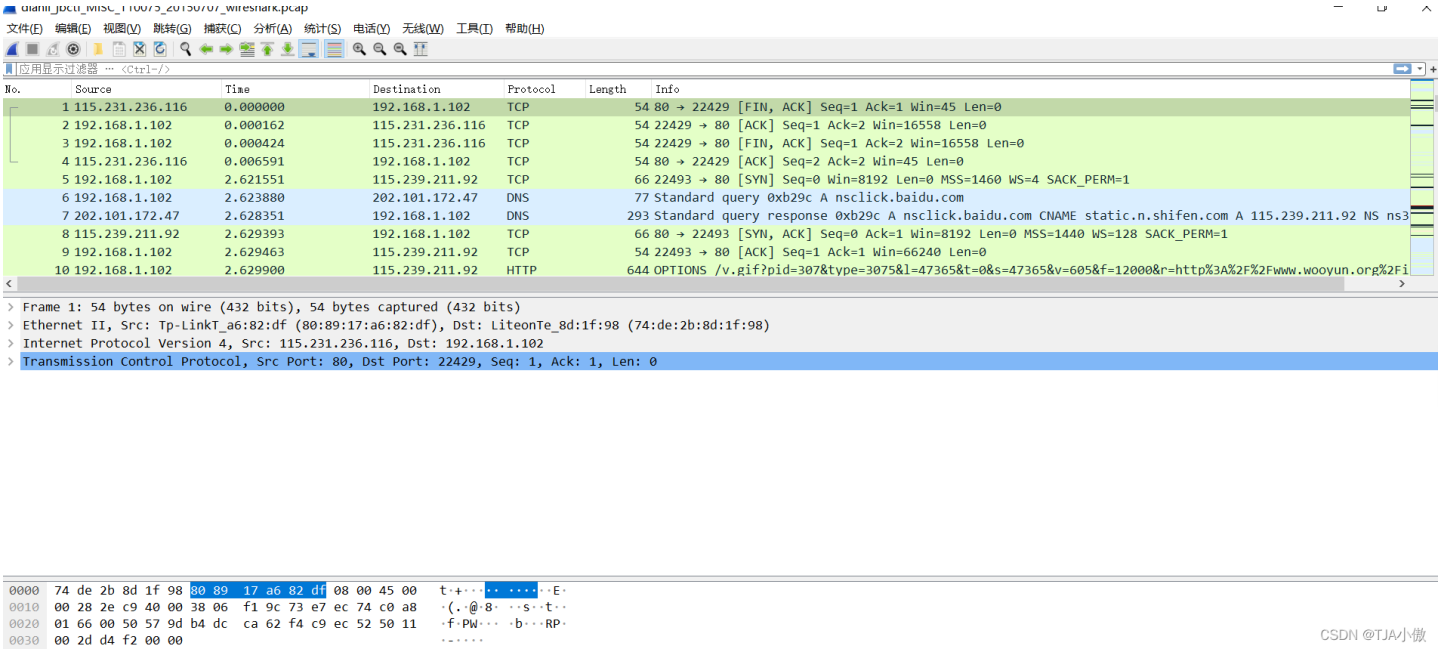
发现是个图片，那就直接在这里转换为图片

得到flag{ICS-mms104}

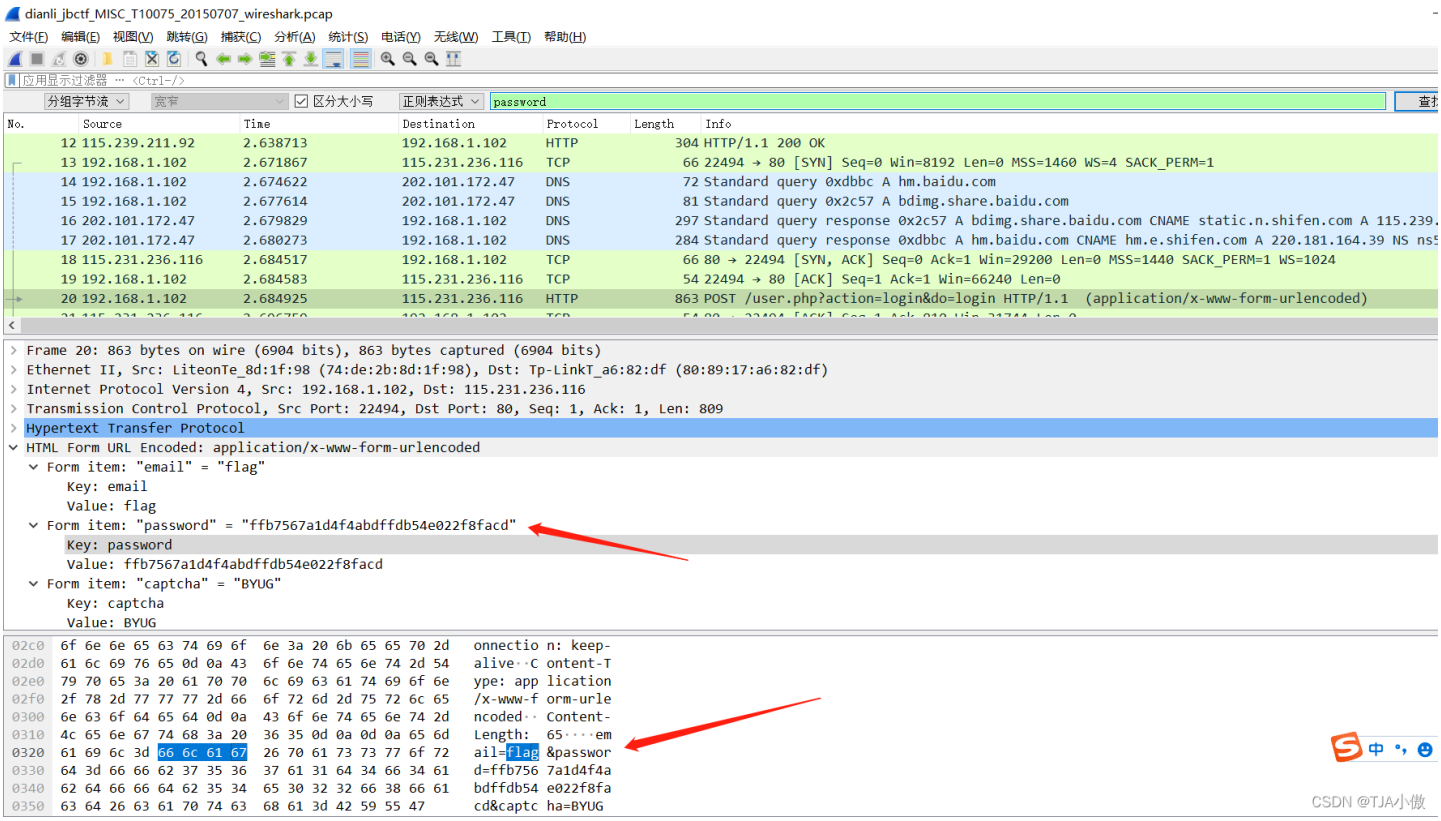
二、管理员的密码就是flag啊

这个只要读懂题，其实没有什么好讲的

首先打开题目发现以下界面



管理员密码，那就直接搜索一下flag看看就行

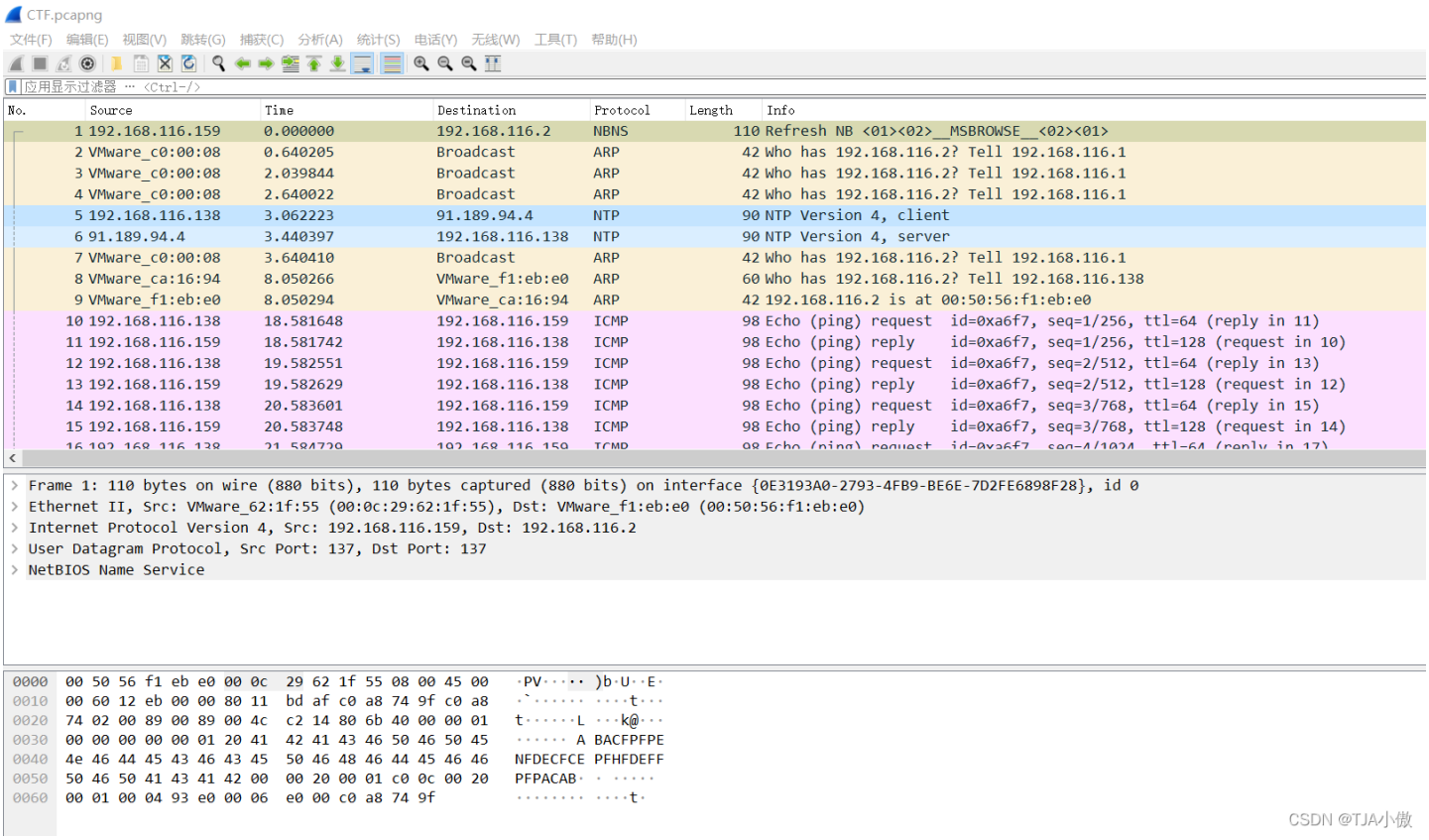


就很简单的得到了flag

flag{ffb7567a1d4f4abdffdb54e022f8facd}

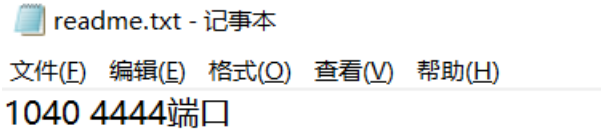
三、getshell

首先打开题目如下



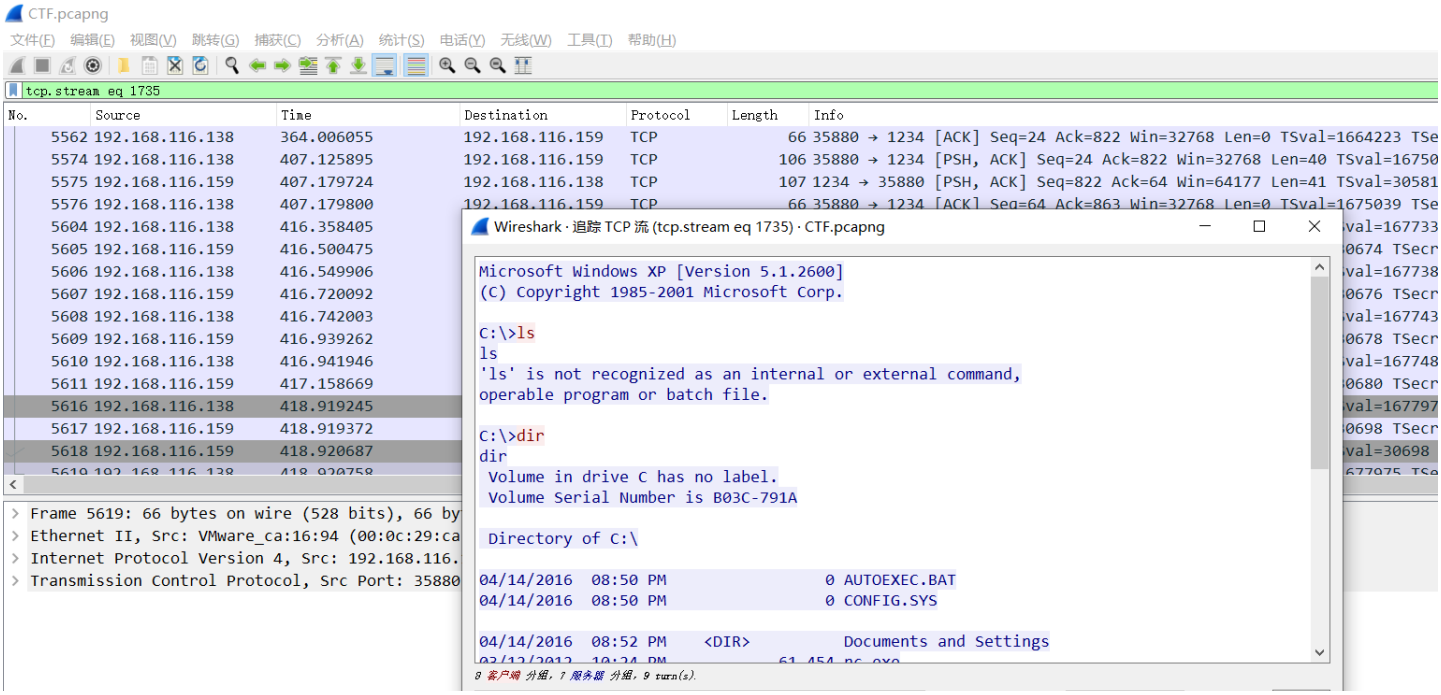
CSDN @TJA小傲

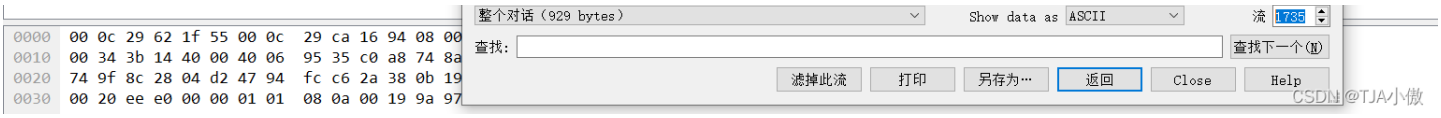
搜索flag都没有什么用，但是在压缩包里发现了还有一个txt文档



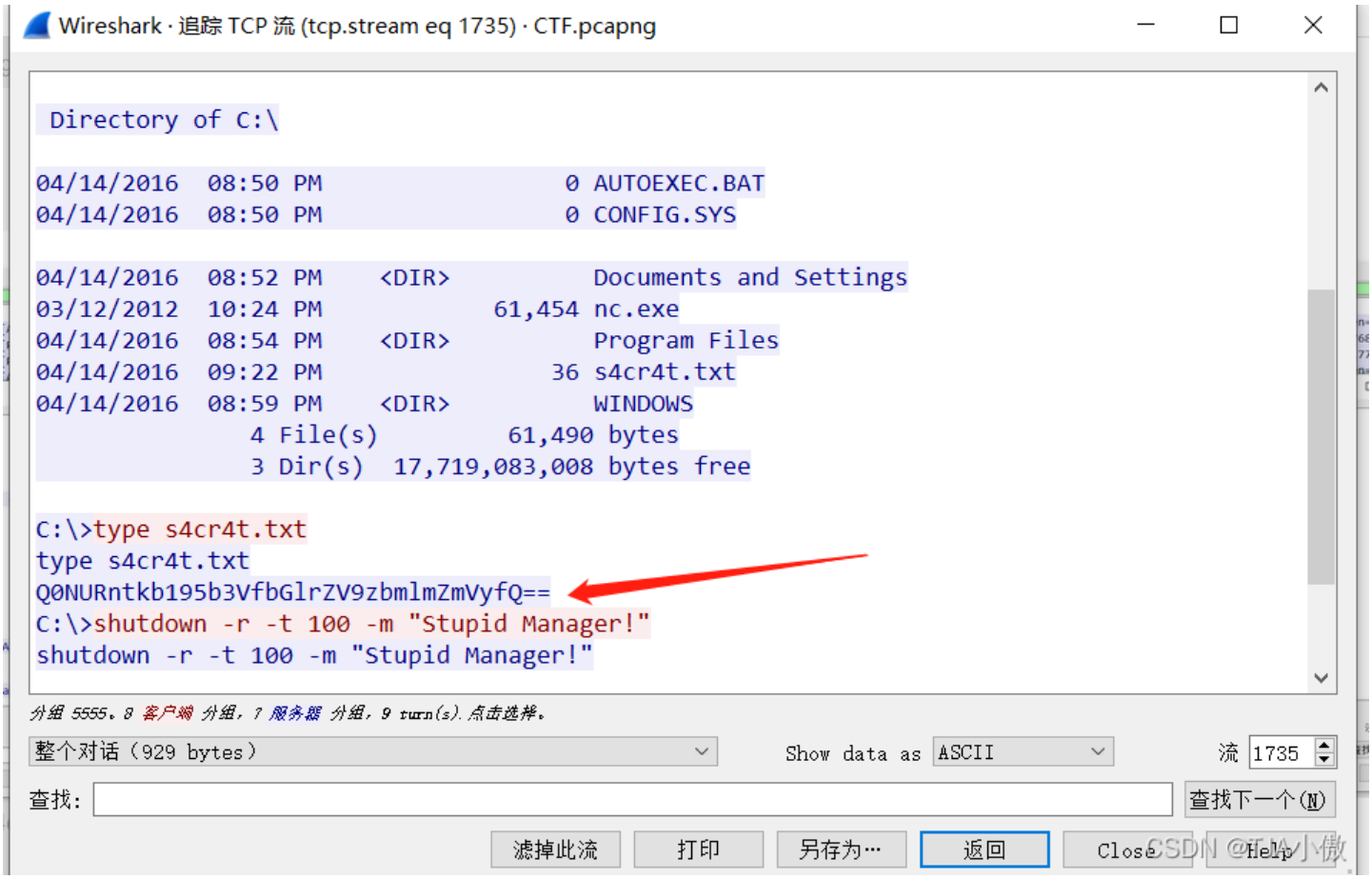
主要是用来反弹shell的

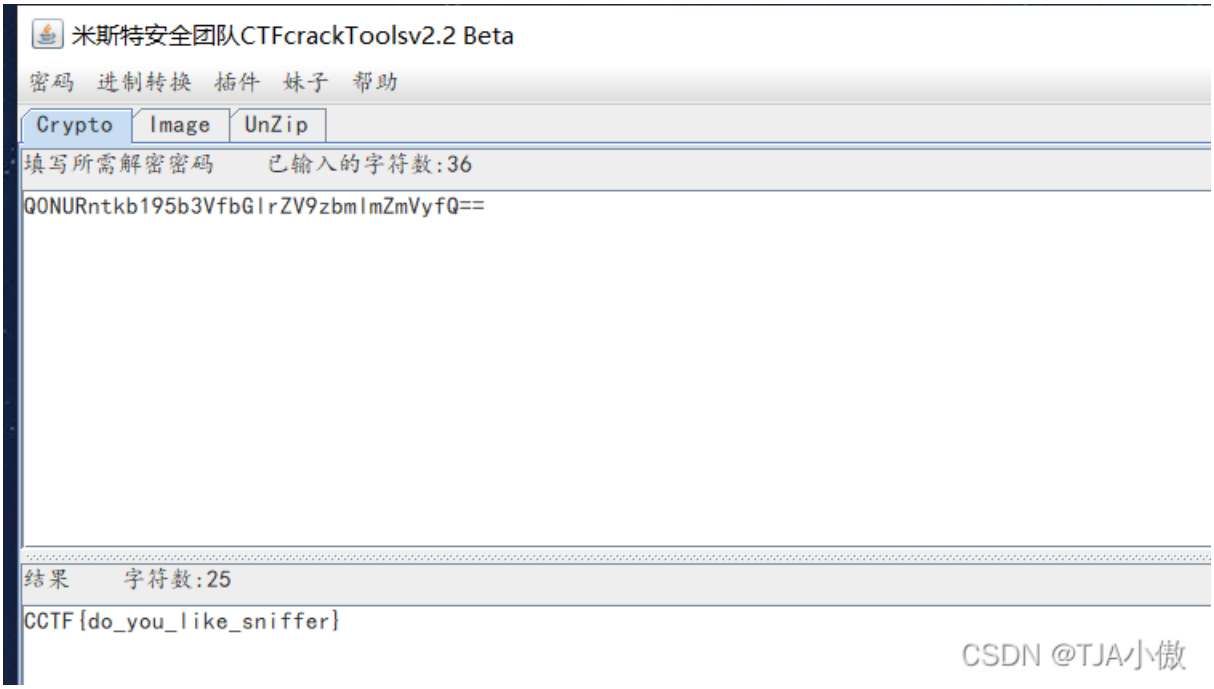
看下tcp流量





发现这是个winxp的系统，在下面发现了base64编码的





最终得到flag

CCTF{do_you_like_sniffer}

目前流量分析的题就到这里结束了，后续有时间也会给大家陆续更新一些杂项其他题目~
估计近几天就开始做靶场了，也会陆续给大家更新的