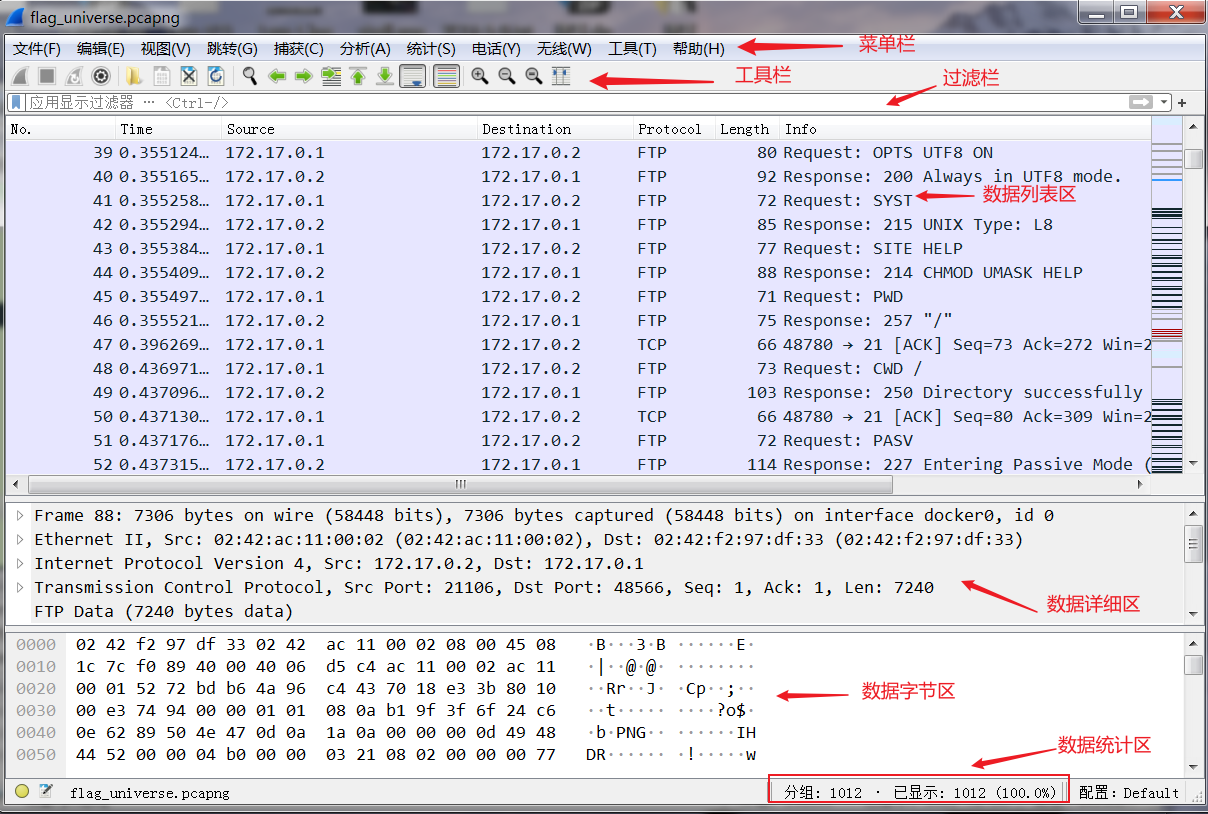
# 流量分析

网络流量分析是指捕捉网络中流动的数据包，并通过查看包内部数据以及进行相关的协议、流量分析、统计等来发现网络运行过程中出现的问题。

## 一：wireshark的基本使用方法

**0. 软件的认识：**

0.1 软件界面认识



0.2 部分字段意思

（1）Frame: 物理层的数据帧概况

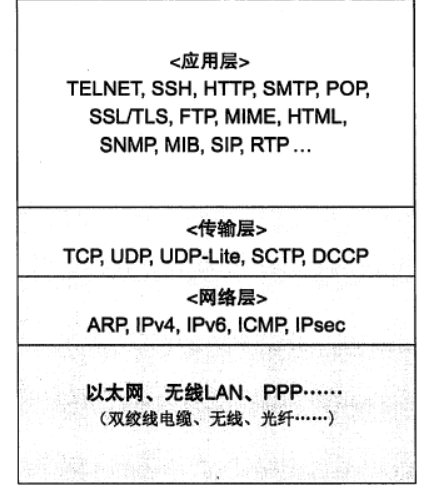
（2）Ethernet II: 数据链路层以太网帧头部信息

（3）Internet Protocol Version 4: 互联网层IP包头部信息

（4）Transmission Control Protocol: 传输层T的数据段头部信息，此处是TCP

（5）Hypertext Transfer Protocol: 应用层的信息，此处是HTTP协议

（tips：tcp/ip协议模型图）

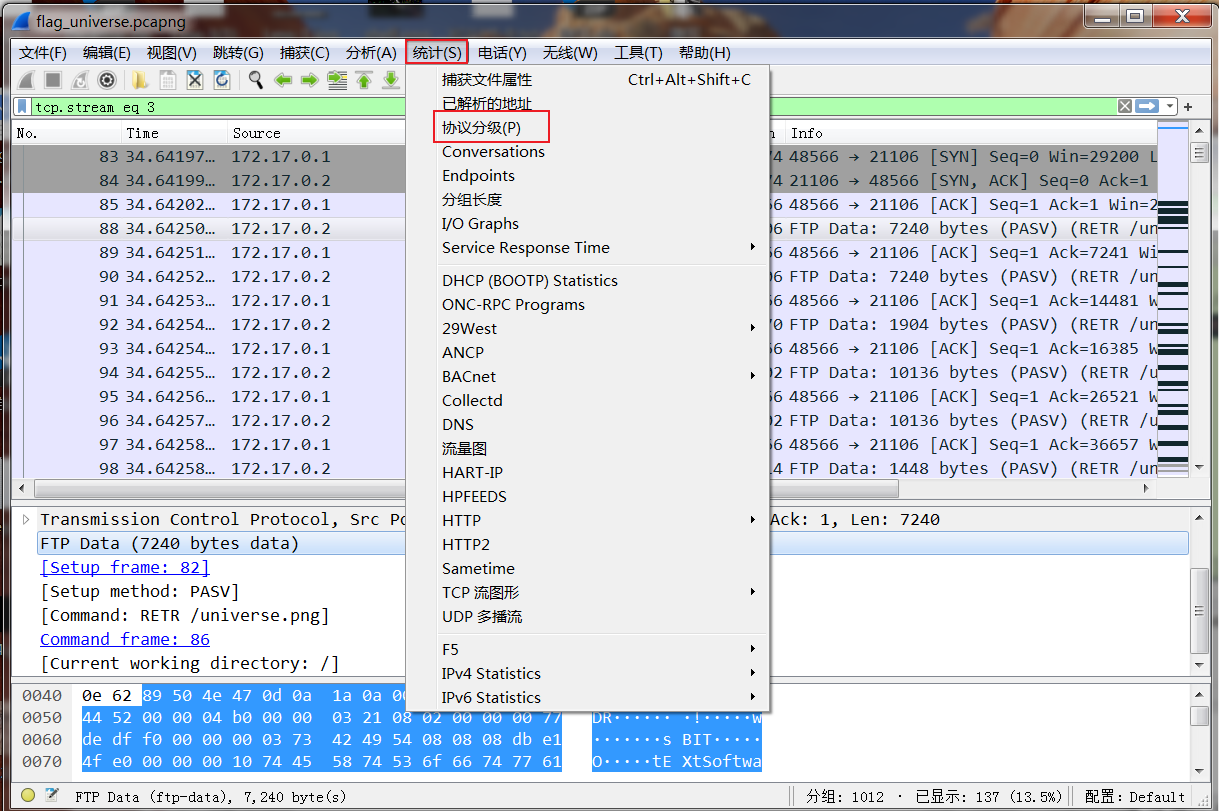


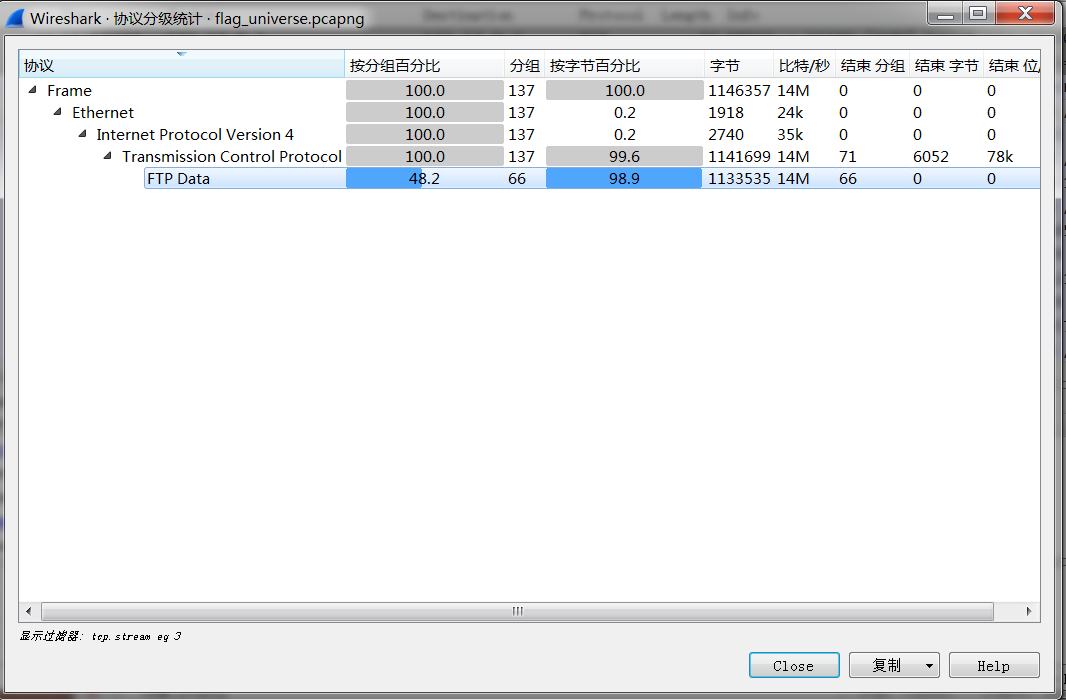
**1. 数据包的统计（部分）：**

数据包的统计可以使你对该数据包有基本认识，如该数据包主要含有哪些协议，端点，ip等，从而进行分析，得出一些关键信息。

1.1 协议分级统计：

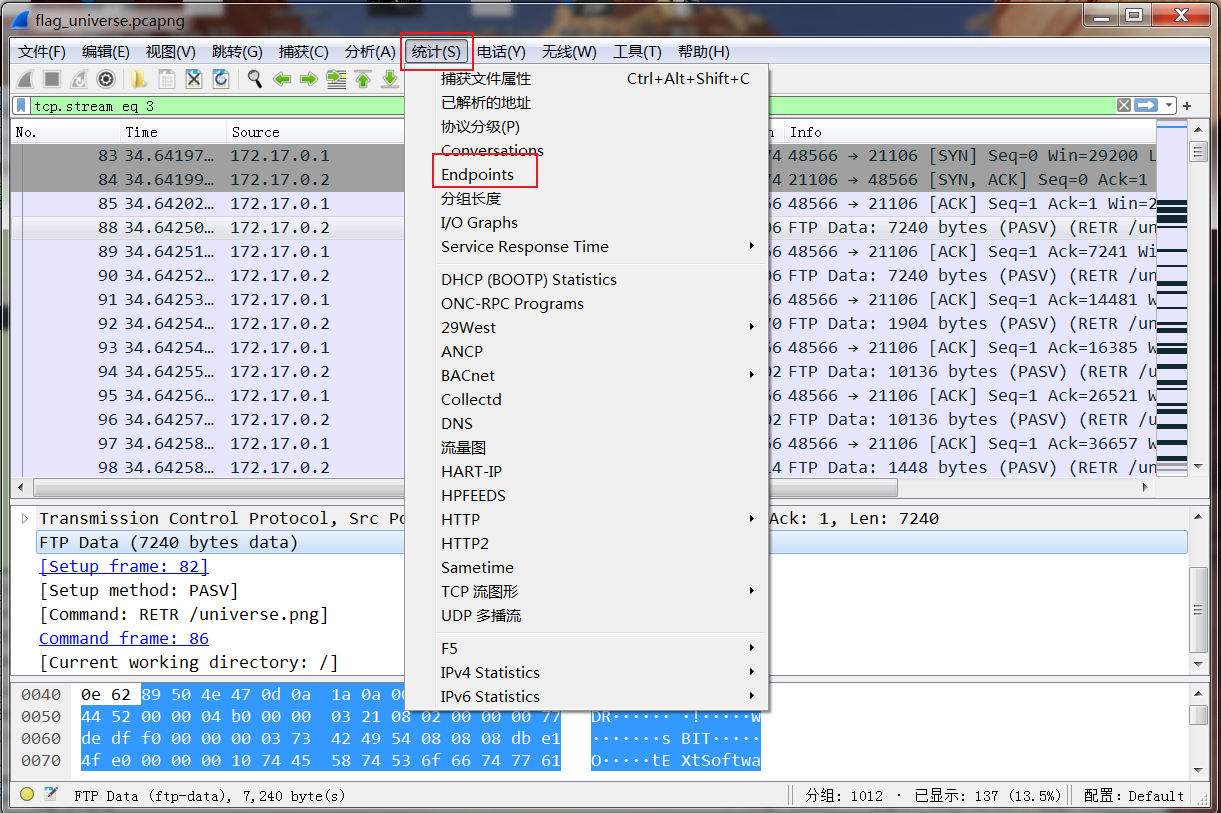
⚫使用【统计】-【协议分级】，便可获得该数据包的所有协议信息，从中可以分析出该数据包主要为什么协议的数据包，如该例中为ftp数据包。

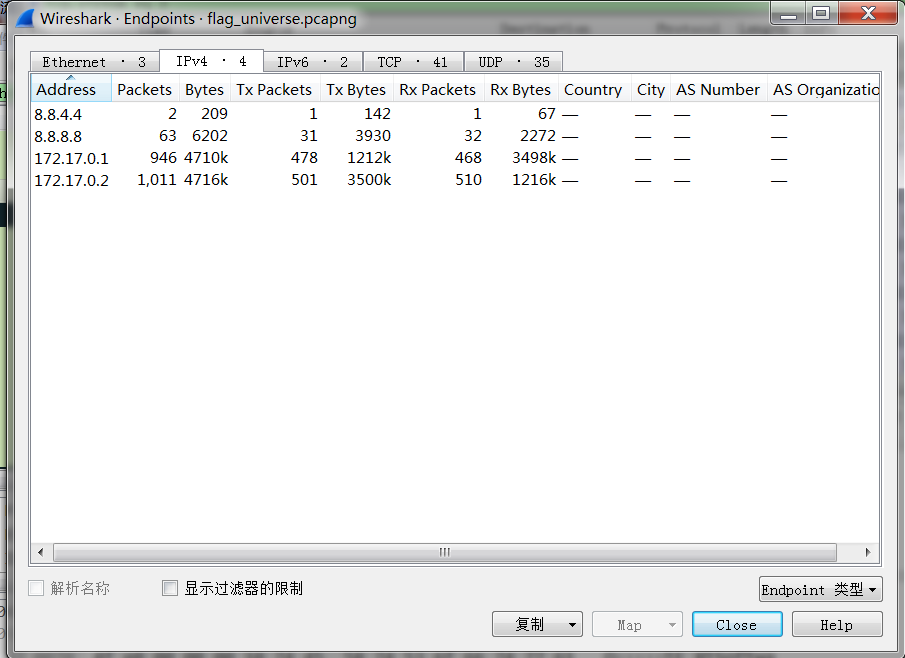




1.2 端点的统计

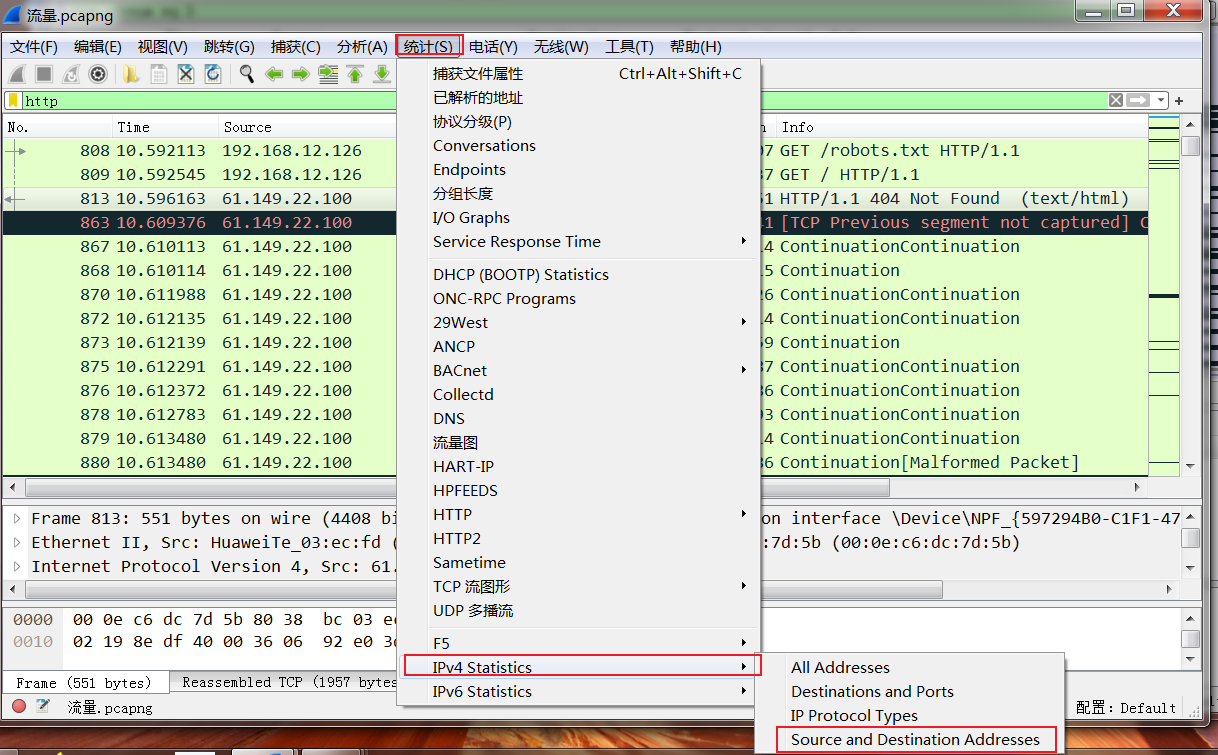
⚫使用【统计】-【Endpoints】，即可获取所有在此处指网络上能够发送或者接收数据的一台设备，以及其相关信息。

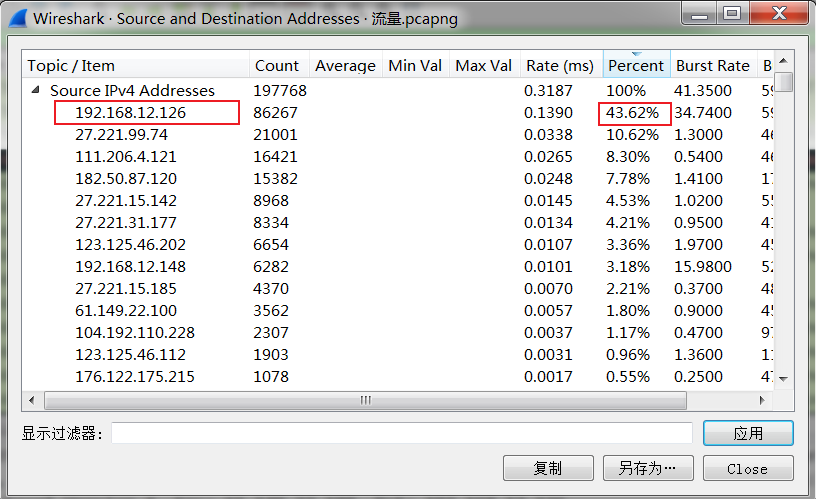




1.3 ip的统计

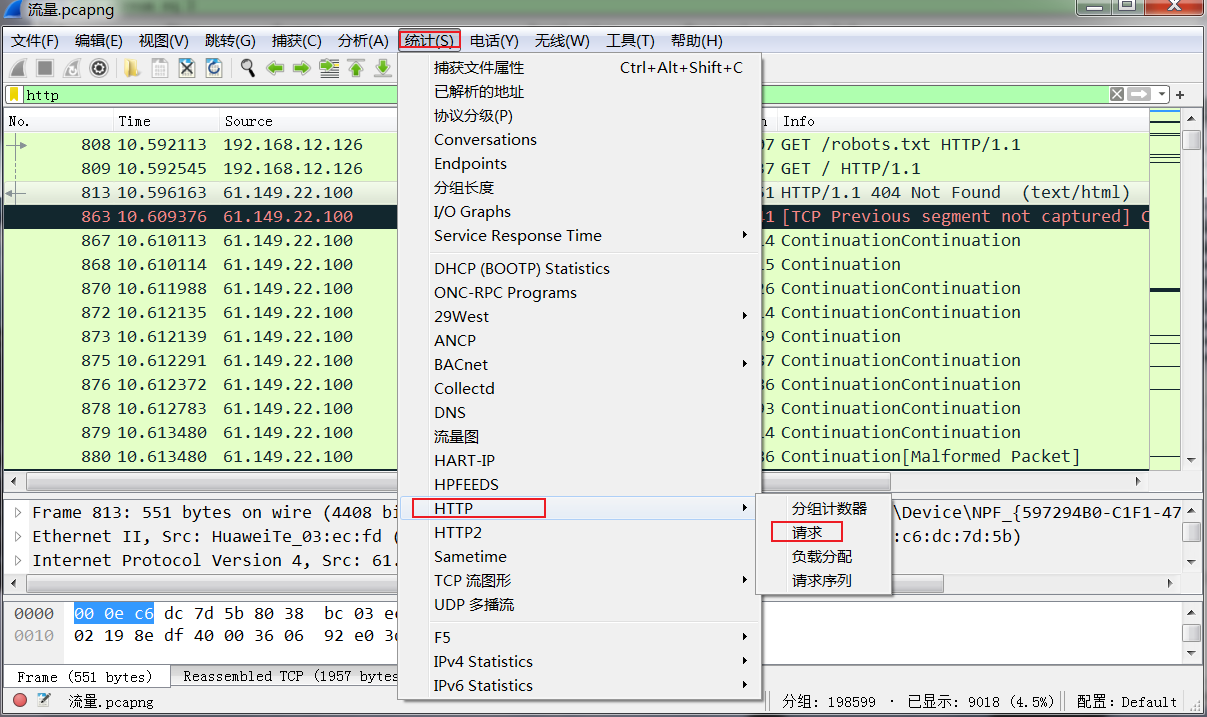
⚫使用【统计】-【Ipv4 Statistics】-【Source and Destination Addresses】，即可获取该数据包的全部ip，如图分析得源地址中最多的为192.168.12.126，因此可以确定该地址为该包的ip。

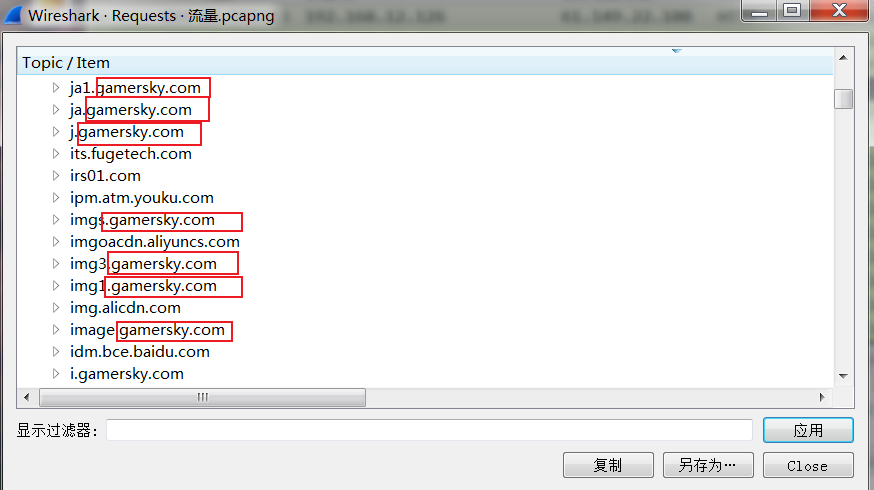




1.4 http请求统计

⚫使用【统计】-【HTTP】-【请求】，即可获取全部http请求内容，在这之中可以分析得出最频繁访问的网站。如图，在该包中最频繁访问的网站时gamersky.com



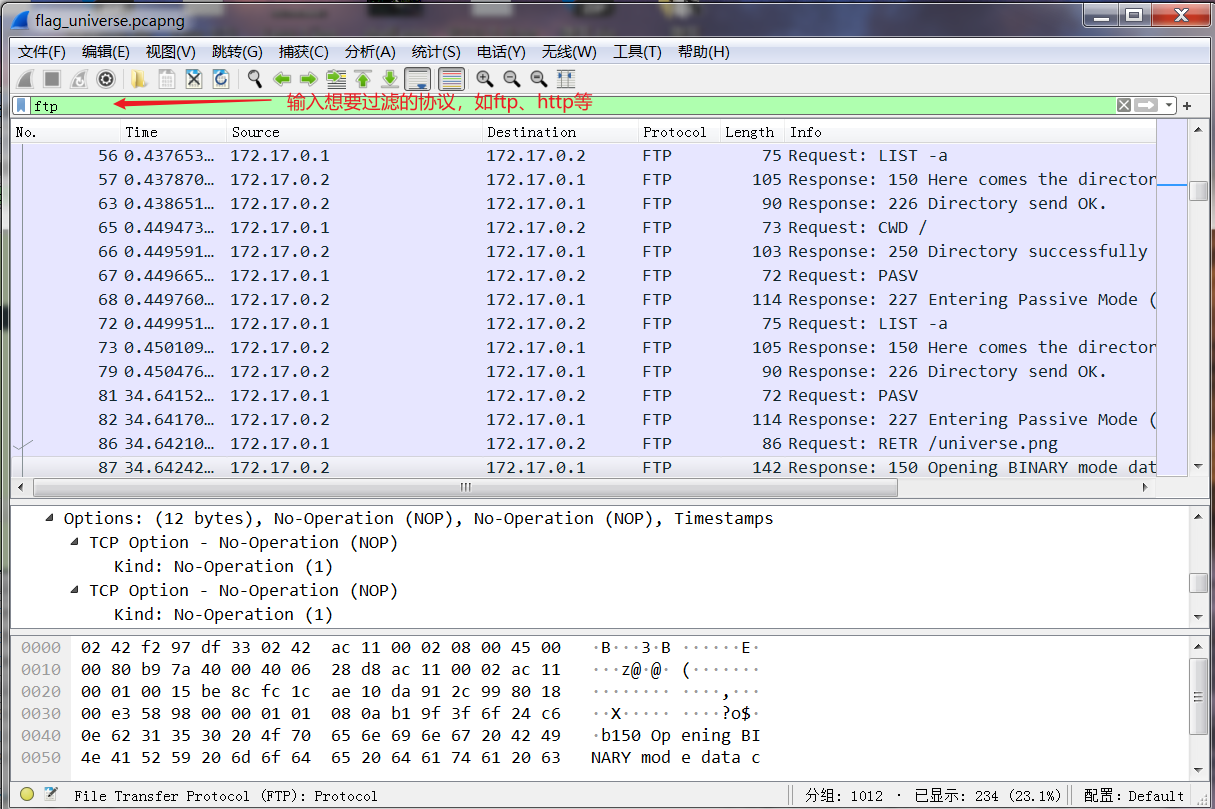


**2. 数据包的过滤**

数据包筛选功能是wireshark的核心功能，比如需要筛选出特定的协议如HTTP，Telnet等，也可能需要筛选出ip地址，端口等。

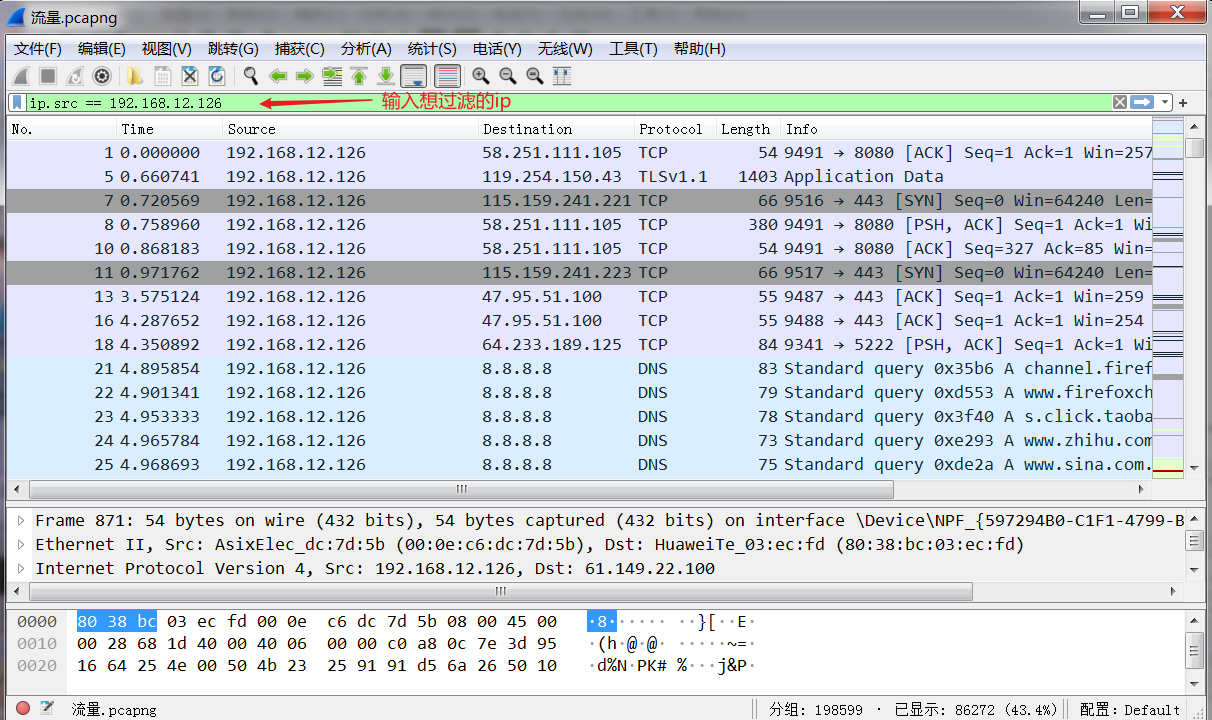
1.1 筛选协议

⚫过滤框中直接输入协议名即可。

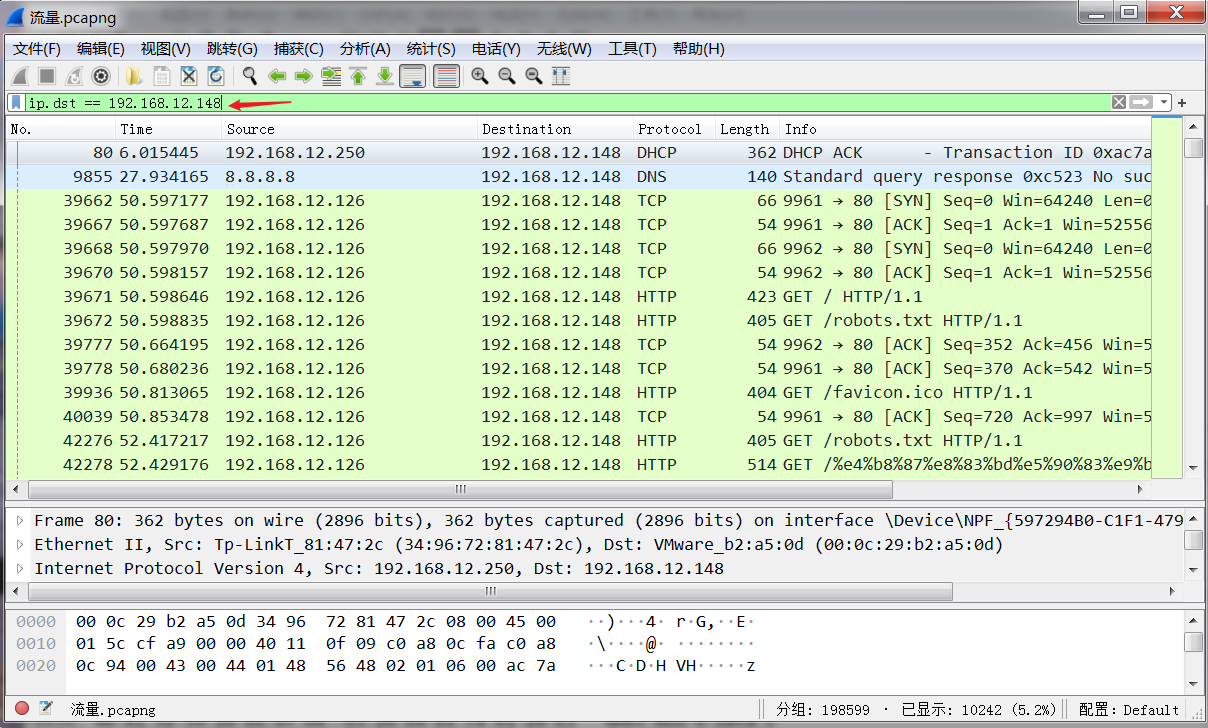


1.2 IP过滤

⚫源ip过滤，输入命令：ip.src == 地址



⚫目的ip的过滤，ip.dst == 地址

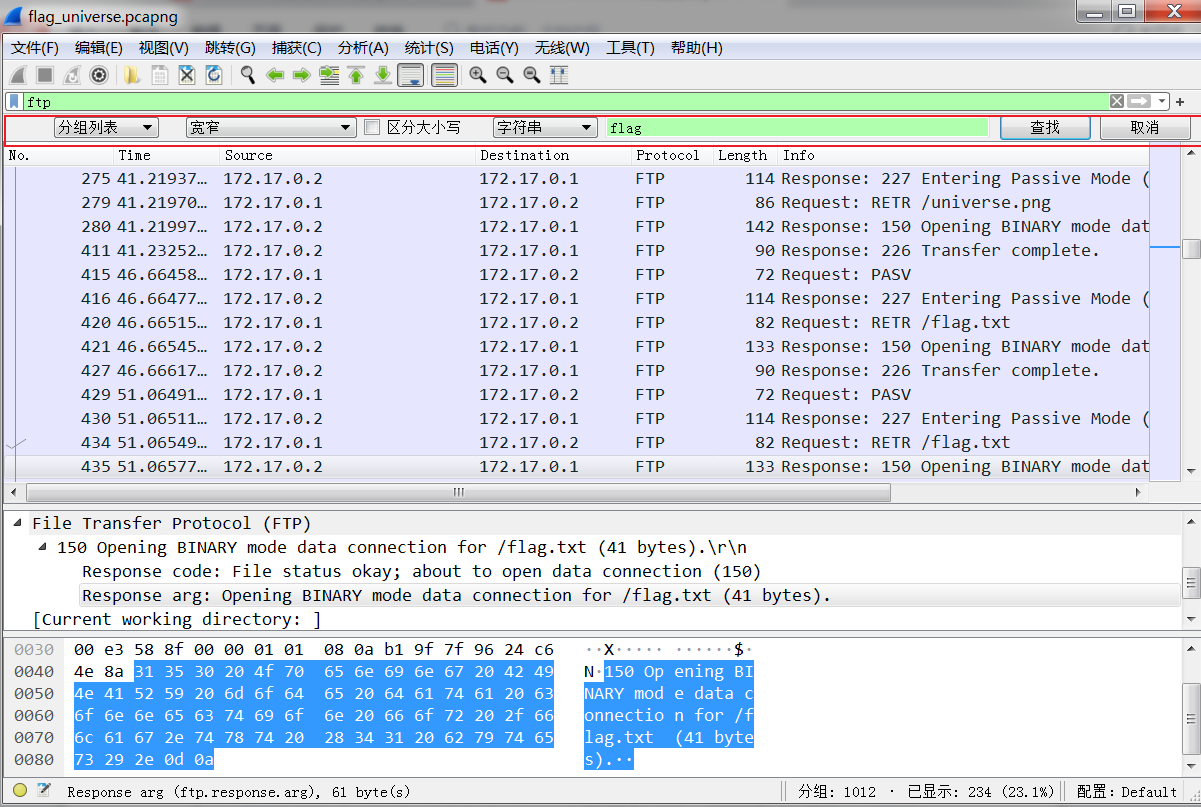


1.3 其他常见过滤

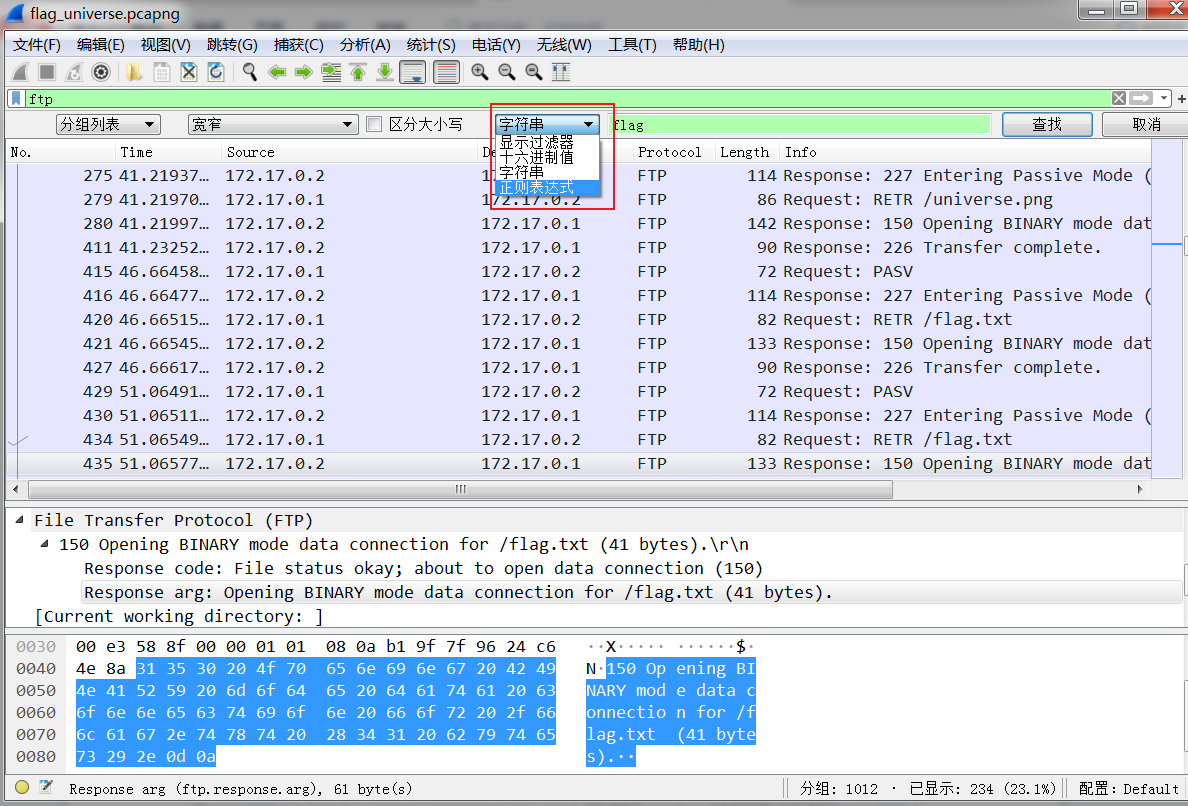
⚫ mac地址筛选:  
   eth.dst ==A0:00:00:04:C5:84 筛选目标mac地址  
   eth.addr==A0:00:00:04:C5:84 筛选MAC地址  
  ⚫ 端口筛选：  
   tcp.dstport == 80  筛选tcp协议的目标端口为80 的流量包  
   tcp.srcport == 80  筛选tcp协议的源端口为80 的流量包  
   udp.srcport == 80  筛选udp协议的源端口为80 的流量包  
⚫ 协议筛选：  
   tcp  筛选协议为tcp的流量包  
   udp 筛选协议为udp的流量包  
   arp/icmp/http/ftp/dns/ip  筛选协议为arp/icmp/http/ftp/dns/ip的流量包  
 ⚫包长度筛选：  
    udp.length ==20   筛选长度为20的udp流量包  
    tcp.len >=20  筛选长度大于20的tcp流量包  
    ip.len ==20  筛选长度为20的IP流量包  
    frame.len ==20 筛选长度为20的整个流量包  
⚫  http请求筛选  
    请求方法为GET：http.request.method==“GET”筛选HTTP请求方法为GET的  流量包  
    请求方法为POST：http.request.method==“POST”筛选HTTP请求方法为POST的流量包  
    指定URI：http.request.uri==“/img/logo-edu.gif”筛选HTTP请求的URL为/img/logo- du.gif的流量包  
    请求或相应中包含特定内容：http contains “FLAG” 筛选HTTP内容为/FLAG的流量包

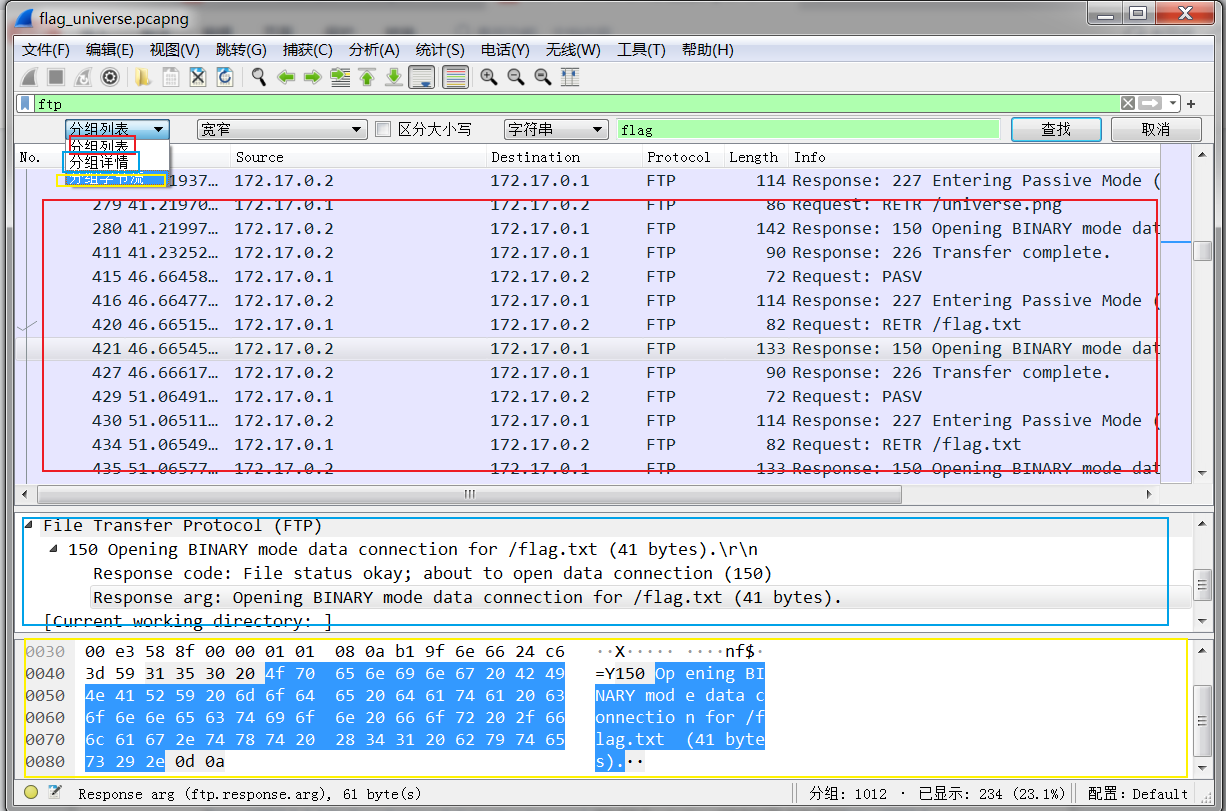
**3. 数据包的搜索**

⚫在wireshark界面按“Ctrl+F”，可以进行关键字搜索：



Wireshark的搜索功能支持正则表达式、字符串、十六进制等方式进行搜索，通常情况下直接使用字符串方式进行搜索。

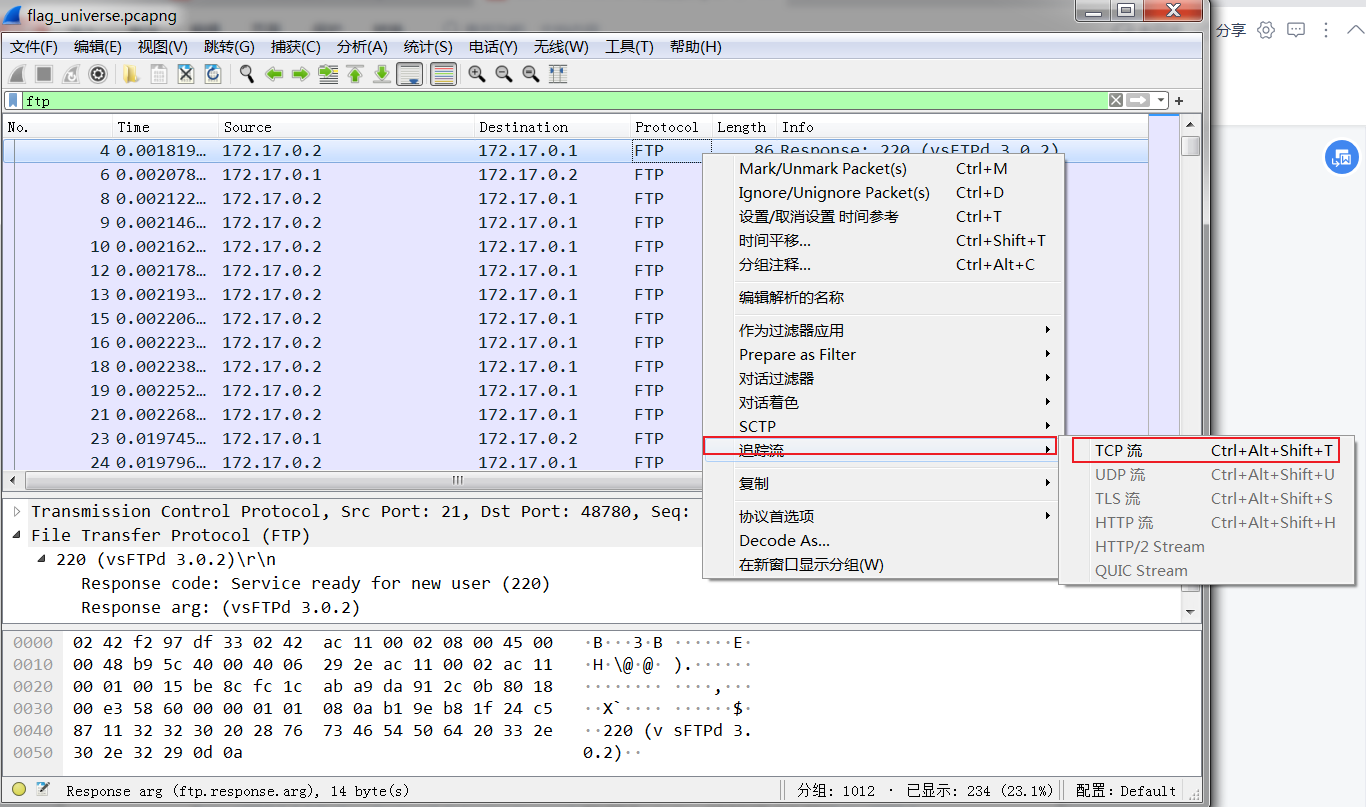
搜索栏的左边下拉，有分组列表、分组详情、分组字节流三个选项，分别对应wireshark界面的三个部分，搜索时选择不同的选项以指定搜索区域：



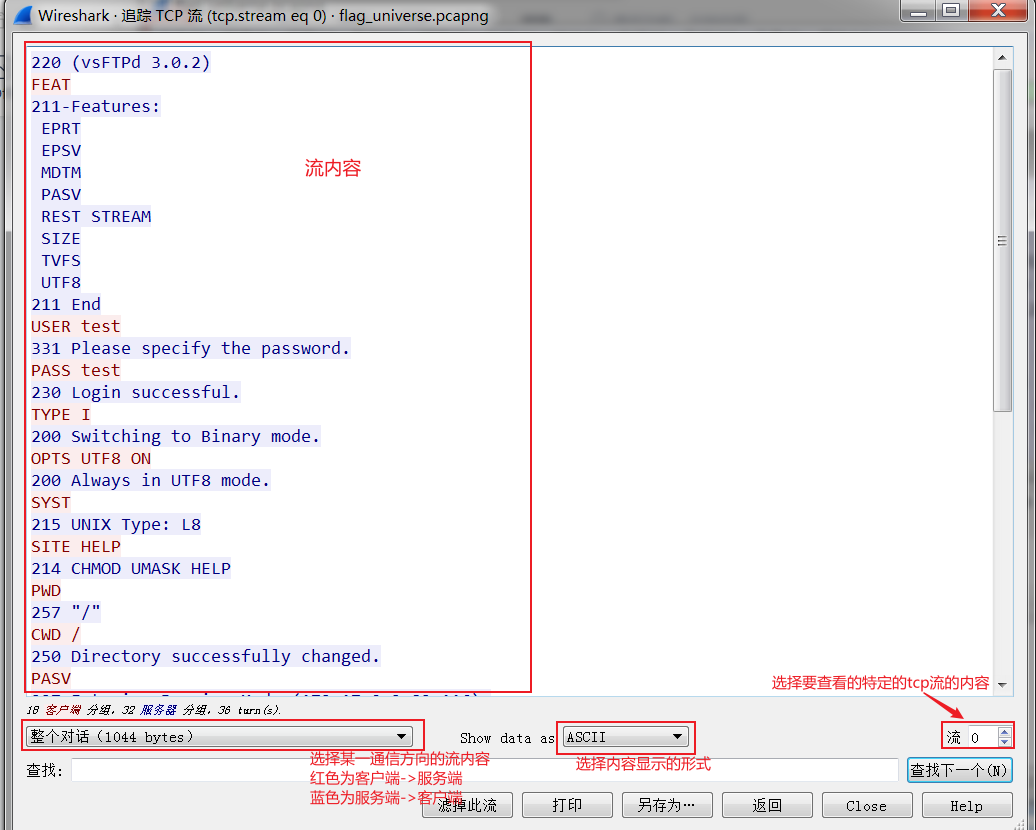
**4. 数据包的还原**

⚫在wireshark中，存在一个交追踪流的功能，可以将HTTP或TCP流量集合在一起并还原成原始数据，具体操作方式如下：

选中想要还原的流量包，右键选中，选择追踪流 – TCP流/UPD流/SSL流/HTTP流。

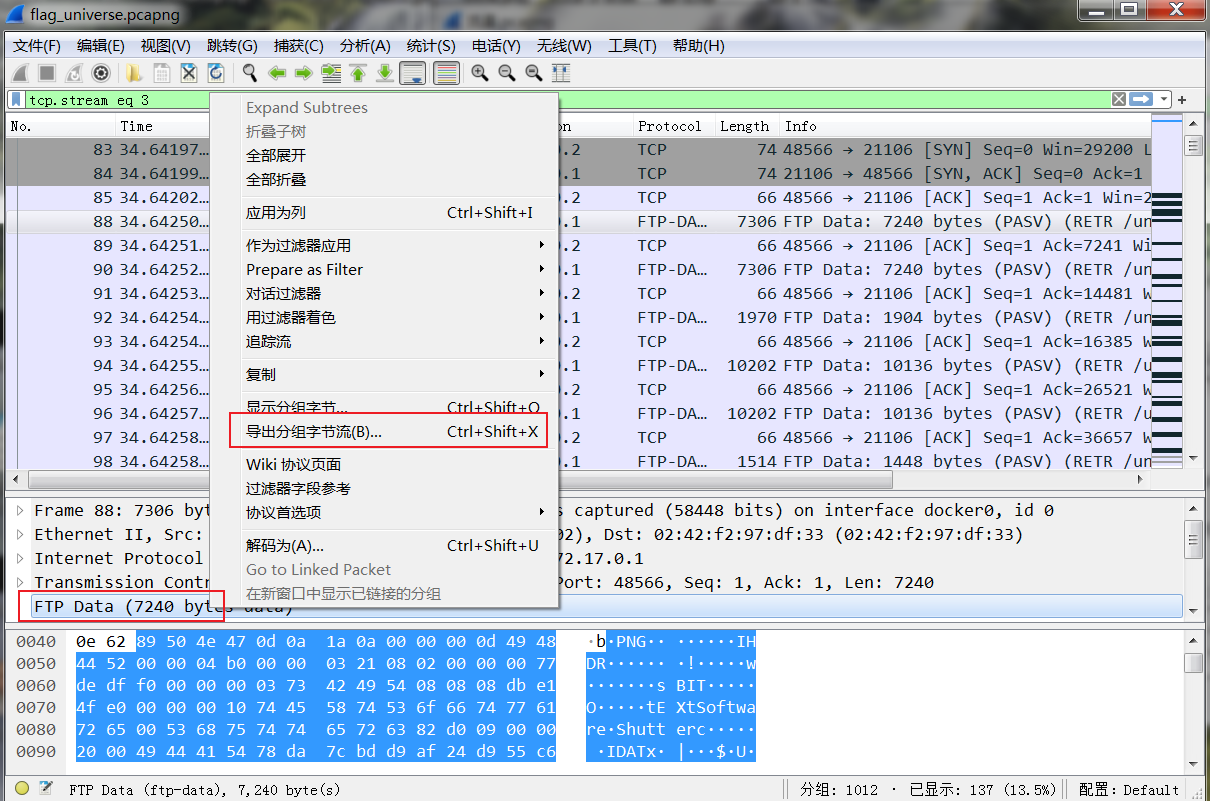


可在弹出的窗口中看到被还原的流量信息：

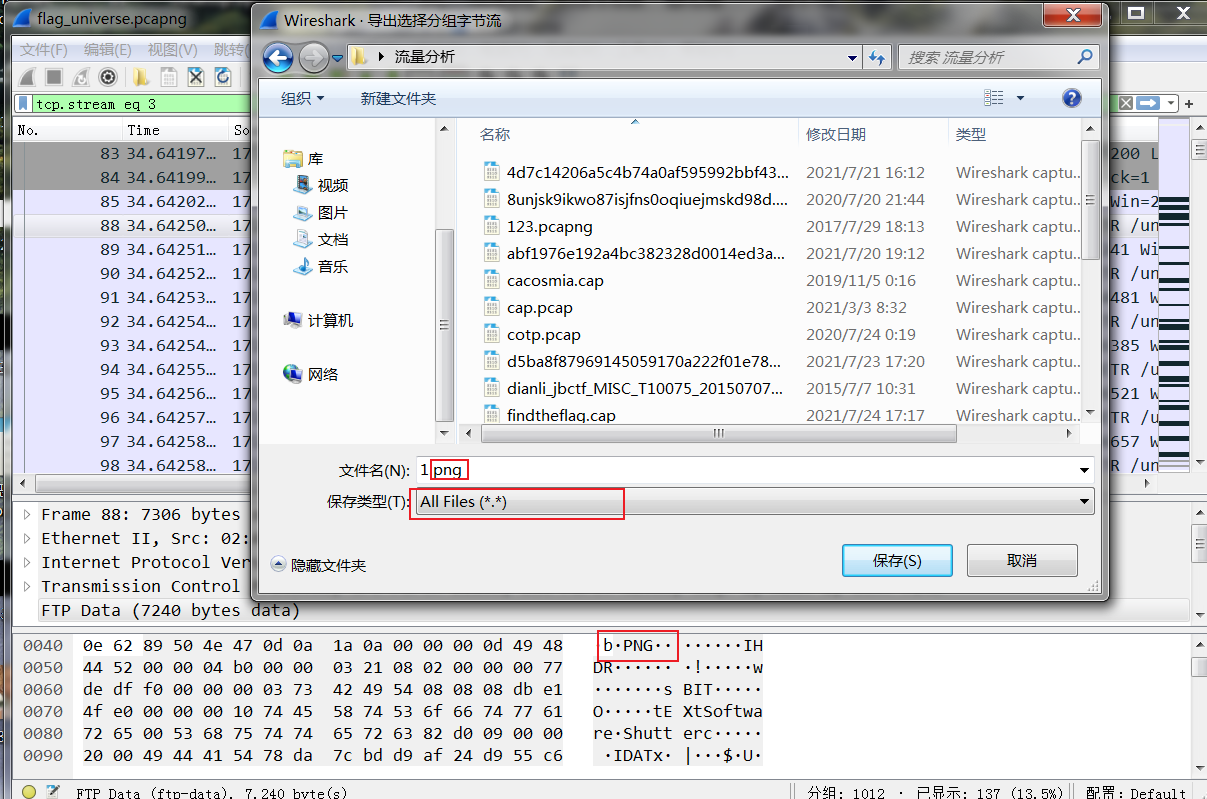


**5. 数据的提取**

⚫数据详细区内寻找到文件数据后点击右键-【导出分组字节流】



保存为相应的文件，保存类型选择全部文件



## 二. 例题分析

#### 一、题目描述

题目链接：（若是使用互联网上已有的CTF靶场题目请附上对应题目的链接，若是本地搭建的CTF题目请附上相关本地题目复现材料的百度网盘永久连接）

题目来源平台：攻防世界 [题目 (xctf.org.cn)](https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=5458&page=2)

题目名称：flag\_universe

题目描述：please find the flag in our universe!

题目场景： 暂无

题目类型：MISC

题目附件：（若有请附上附件，若无可忽略）

FLAG： flag{Plate\_err\_klaus\_Mail\_Life}

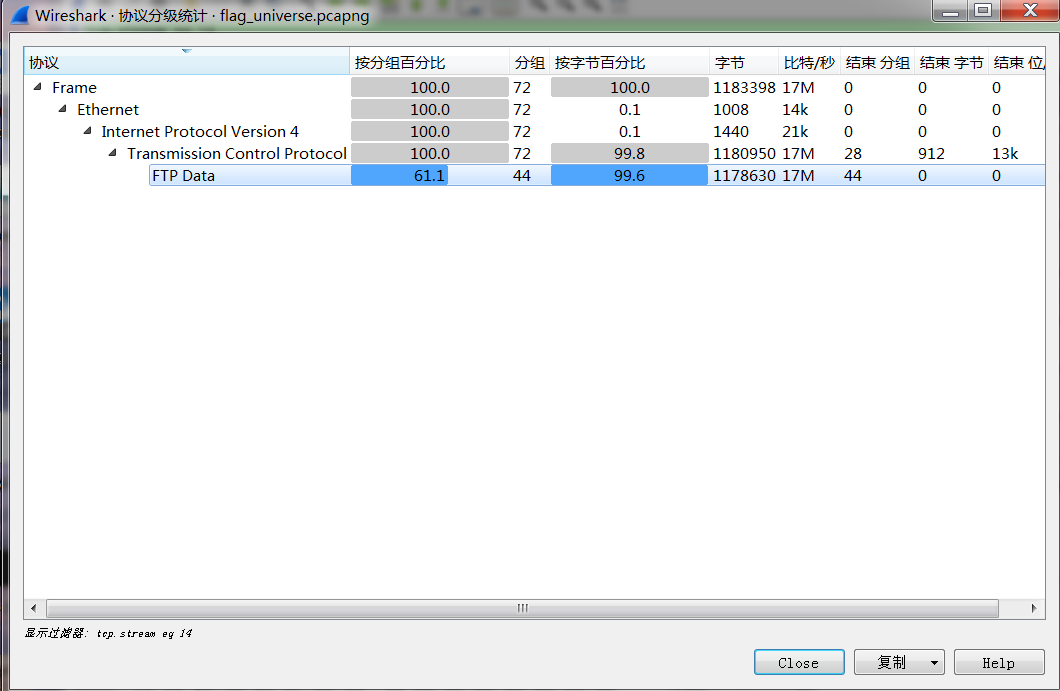
#### 二、解题工具

|  |  |  |  |
| --- | --- | --- | --- |
| 工具类型 | 工具名称 | 版本 | 备注 |
| 基础环境 |  |  |  |
| Windows system | 10.0.18363 |  |
| 工具 | Wireshark | 2.2.1 |  |
|  |  |  |
| 脚本 |  |  |  |
|  |  |  |
|  |  |  |

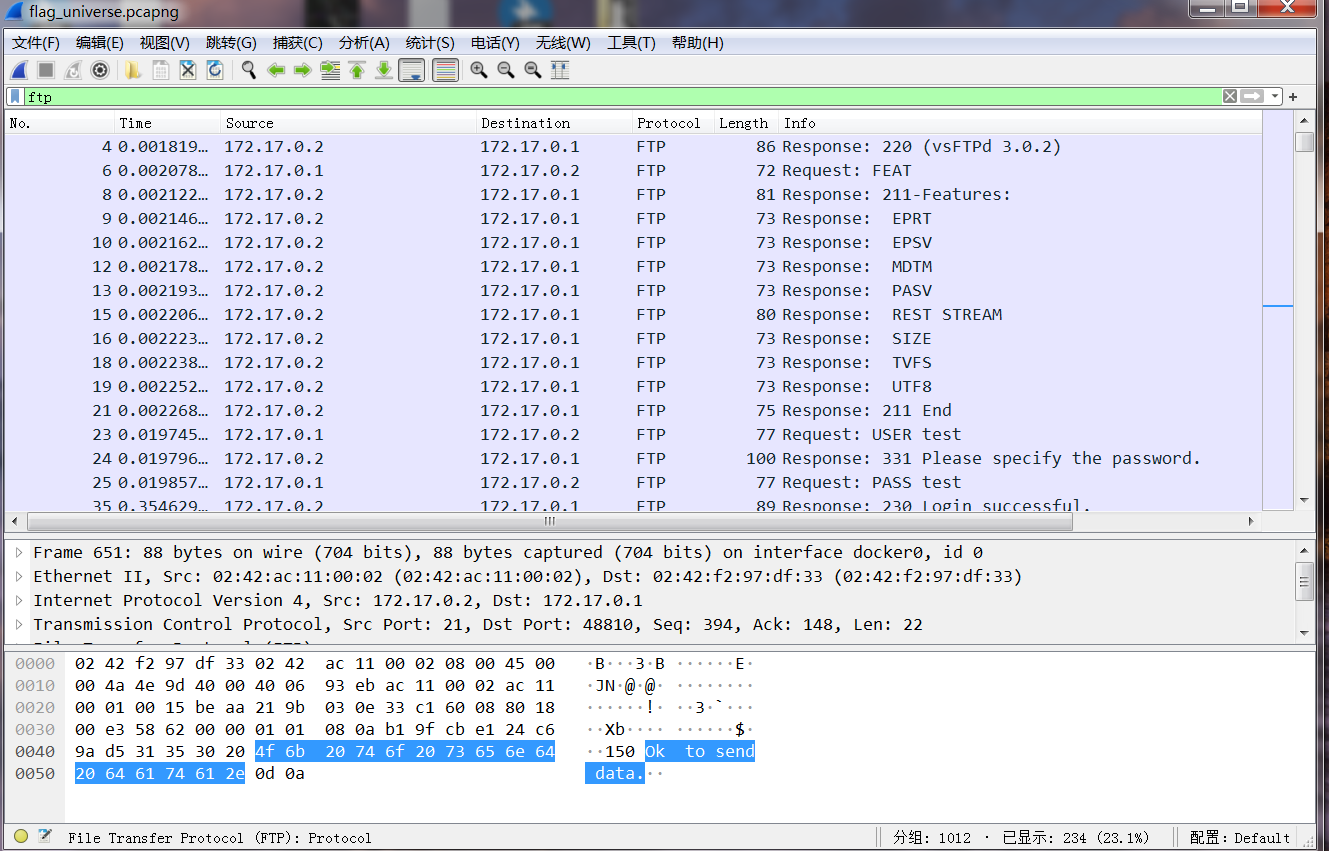
#### 三、解题过程

（详细说明CTF赛题的解题过程，分步骤说明）

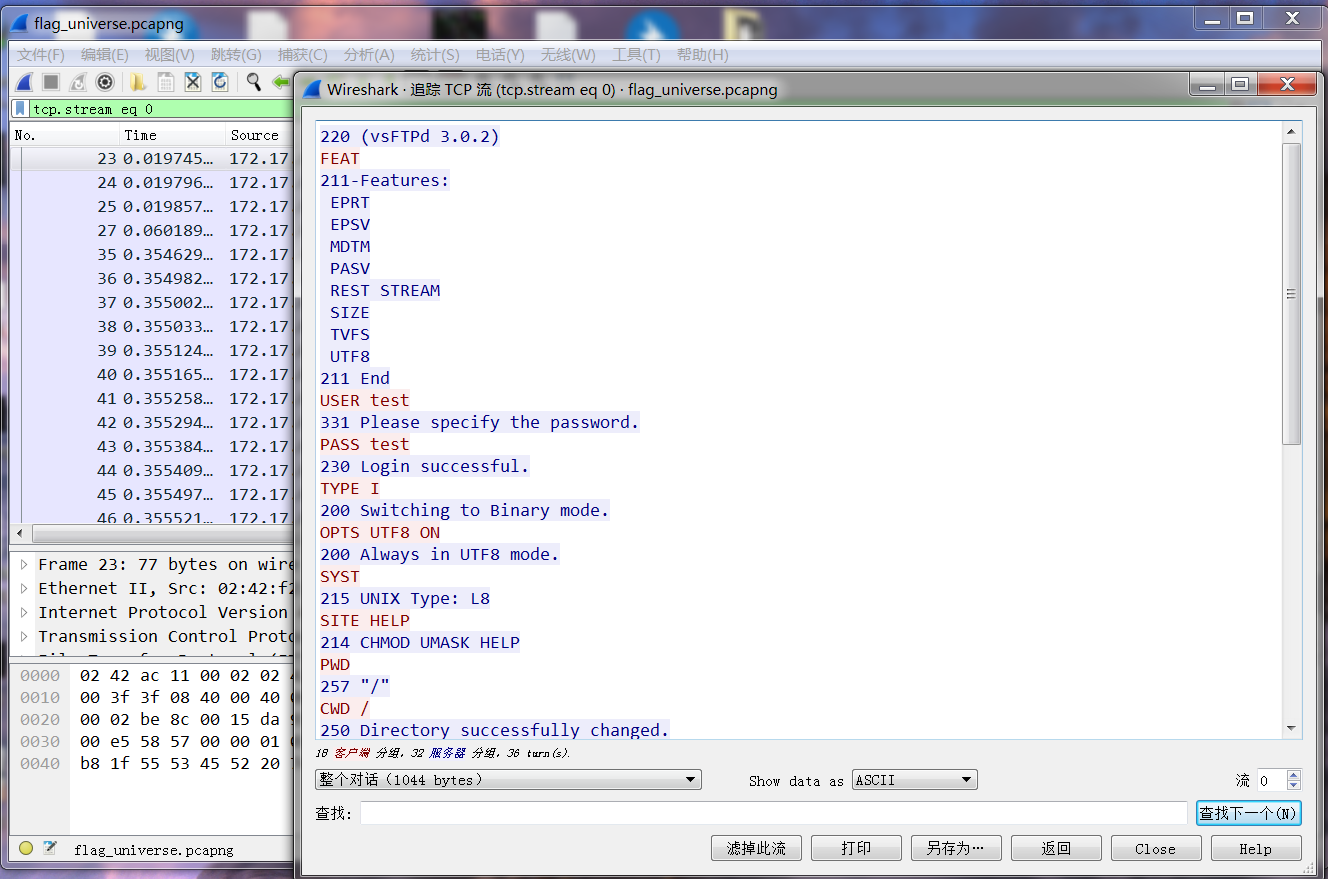
### 步骤1： 协议分级，发现是ftp流量数据包



### 步骤2： 过滤ftp流量

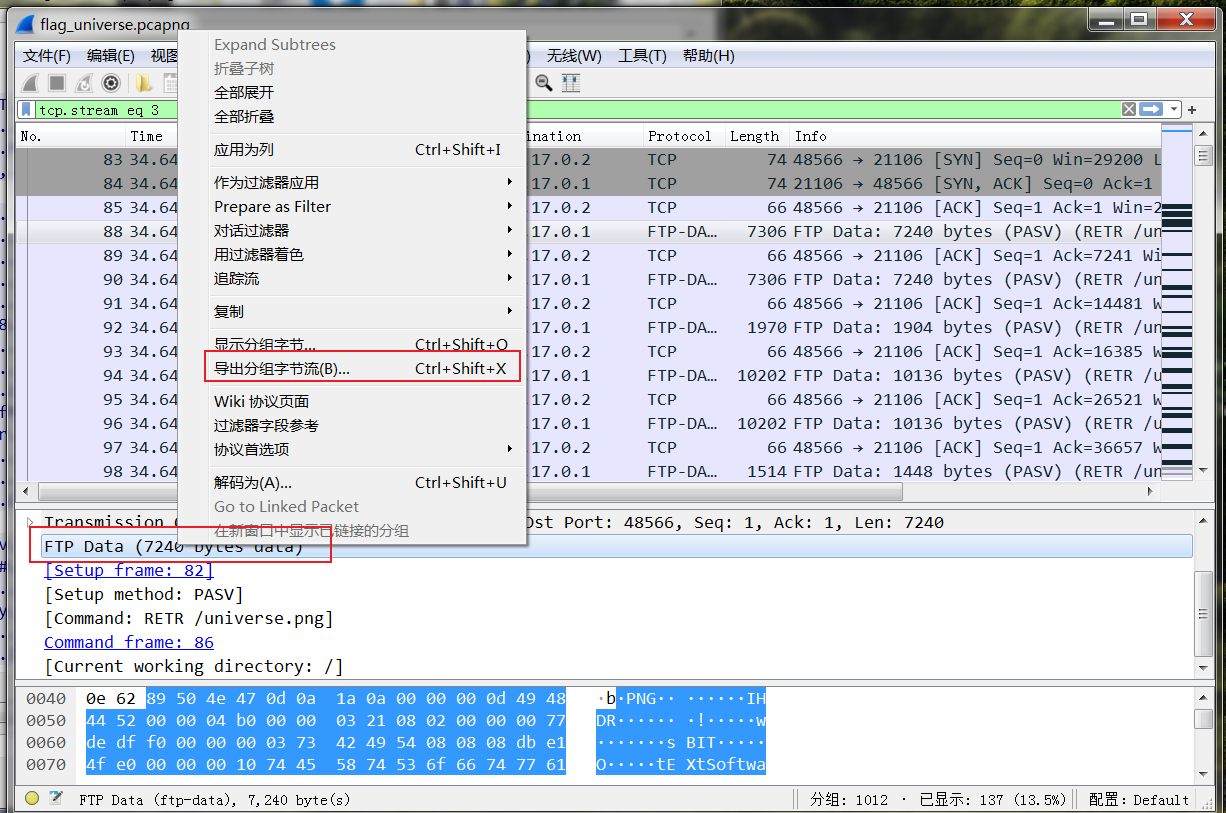


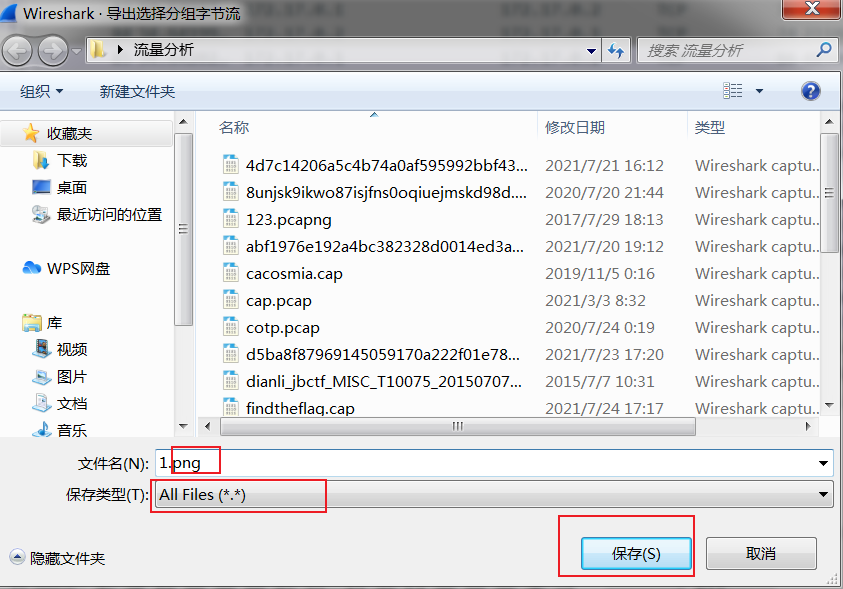
### 步骤3：因为流量不多，逐一进行tcp流追踪发现3，4，6，11，13，14为png图片，逐一导出



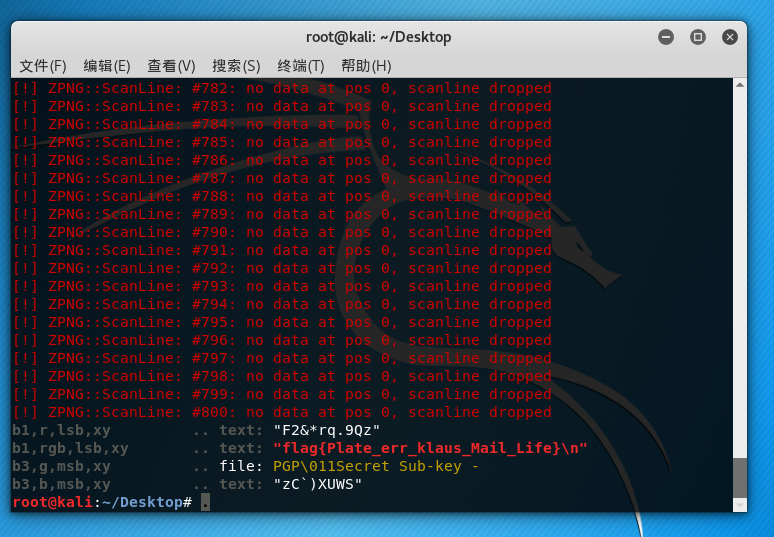
图片导出方式：

在该流下导出分组字流组，保存为png格式，保存类型选择全部文件





### 步骤5：保存图像发现都为黑色，在010editoer中打开发现缺少png的文件尾，补上后发现仍为黑色，对其全都进行zsteg在第14张图片发现flag



## 三. 思路总结

3.1. 常见题型

（流量分析题目主要在于对数据包的分析与wireshark工具的使用，因此只列了部分类型，详情可以参考网上资料[CTF流量分析之题型深度解析(ichunqiu.com)](https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=51302&highlight=%E6%B5%81%E9%87%8F%E5%88%86%E6%9E%90)，[CTF——MISC——流量分析\_ctf流量分析](https://blog.csdn.net/vhkjhwbs/article/details/100847221?ops_request_misc=%257B%2522request%255Fid%2522%253A%2522162727924616780265489389%2522%252C%2522scm%2522%253A%252220140713.130102334.pc%255Fall.%2522%257D&request_id=162727924616780265489389&biz_id=0&utm_medium=distribute.pc_search_result.none-task-blog-2~all~first_rank_v2~rank_v29-16-100847221.pc_search_result_before_js&utm_term=%E6%B5%81%E9%87%8F%E5%88%86%E6%9E%90&spm=1018.2226.3001.4187)）

⚫流量包修复  
⚫协议分析  
⚫数据提取

3.2. 思路分析

⚫流量分析重在分析因此首先要对数据包有个总体感受

1. 第一先进行协议分级与端点统计

2. 第二在之前分析的基础上进行选择性过滤并注意数据列表是否有特殊字符等3. 第三发现特殊的异常，进行判断是特殊的字符串或特殊数据文件等

4. 第四对数据进行提取，如特殊的字符串或文件数据

5. 对提取的数据文件进行处理，如图片隐写，压缩包解码等。

3.3. 总结

⚫流量分析是一类综合性很强的题目，会结合其他misc类型的题目，但其难点与重点大多在于对数据包的流量分析，因此对wireshark的熟练使用非常重要，以及明白一些相关的工控协议等知识，然后在实践中慢慢学习如何进行分析。

（个人能力有限在这中说得并不全面和正确，因此附上一些参考资料以供大家参考和补充[CTF流量分析之wireshark使用(ichunqiu.com)](https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=50836&highlight=%E6%B5%81%E9%87%8F%E5%88%86%E6%9E%90)，[流量分析基础篇-CSDN博客](https://blog.csdn.net/weixin_30333885/article/details/97581077)，[网络分析工具——WireShark的使用（超详细）\_CSDN博客](https://blog.csdn.net/zzwwhhpp/article/details/113077747?ops_request_misc=%257B%2522request%255Fid%2522%253A%2522162727963716780357258139%2522%252C%2522scm%2522%253A%252220140713.130102334..%2522%257D&request_id=162727963716780357258139&biz_id=0&utm_medium=distribute.pc_search_result.none-task-blog-2~all~top_positive~default-1-113077747.pc_search_result_before_js&utm_term=wireshark&spm=1018.2226.3001.4187)，[CTF-MISC-CSDN博客\_ctf流量分析](https://blog.csdn.net/vhkjhwbs/article/details/100847221?ops_request_misc=%257B%2522request%255Fid%2522%253A%2522162727924616780265489389%2522%252C%2522scm%2522%253A%252220140713.130102334.pc%255Fall.%2522%257D&request_id=162727924616780265489389&biz_id=0&utm_medium=distribute.pc_search_result.none-task-blog-2~all~first_rank_v2~rank_v29-16-100847221.pc_search_result_before_js&utm_term=%E6%B5%81%E9%87%8F%E5%88%86%E6%9E%90&spm=1018.2226.3001.4187)）

1.基础知识（+工具使用）  
2.常见题型  
3.解题思路  
4.例题分析