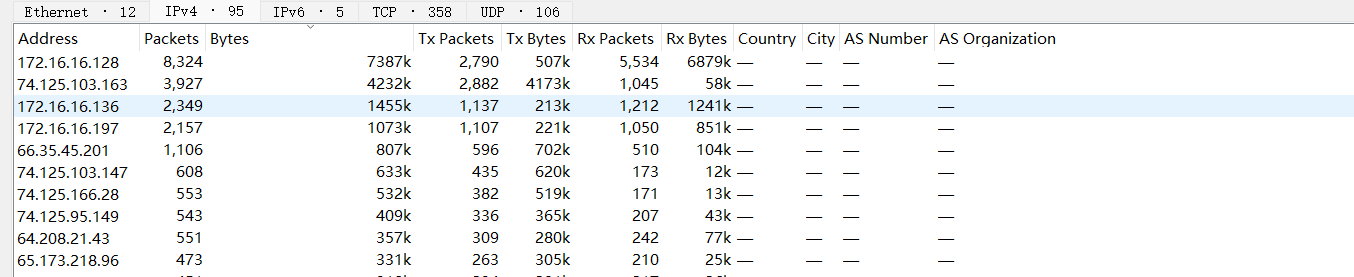
网络流量分析（一）实验

【验证实验 1】

当发现网络中出现异常增加的流量之后，管理员使用Wireshark进行了数据包嗅探捕获， lotsofweb.pcapng 就是数据包捕获文件，请对该数据包捕获文件进行分析，并回答下列问题：

1）捕获文件反映出来的通信量最大、最活跃的端点有哪些？请提供关键分析证据截图。

**答：**



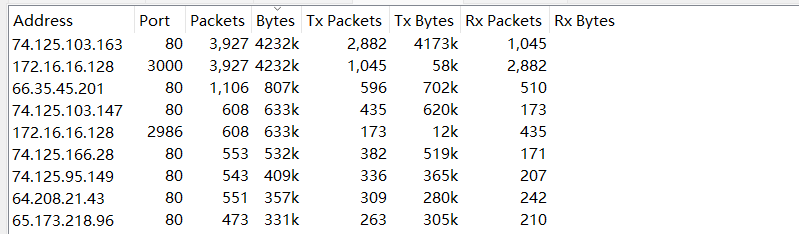


图1-活跃节点

通信量最大、最活跃的端点有172.16.16.128

2）最大的数据通信量来自于哪些节点的通信？请提供关键分析证据截图。

**答：**

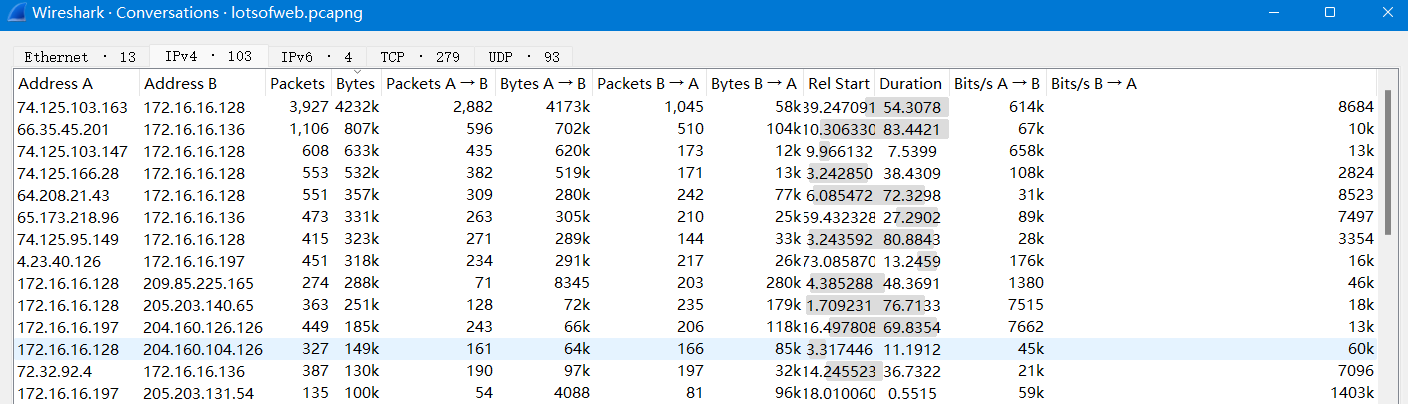
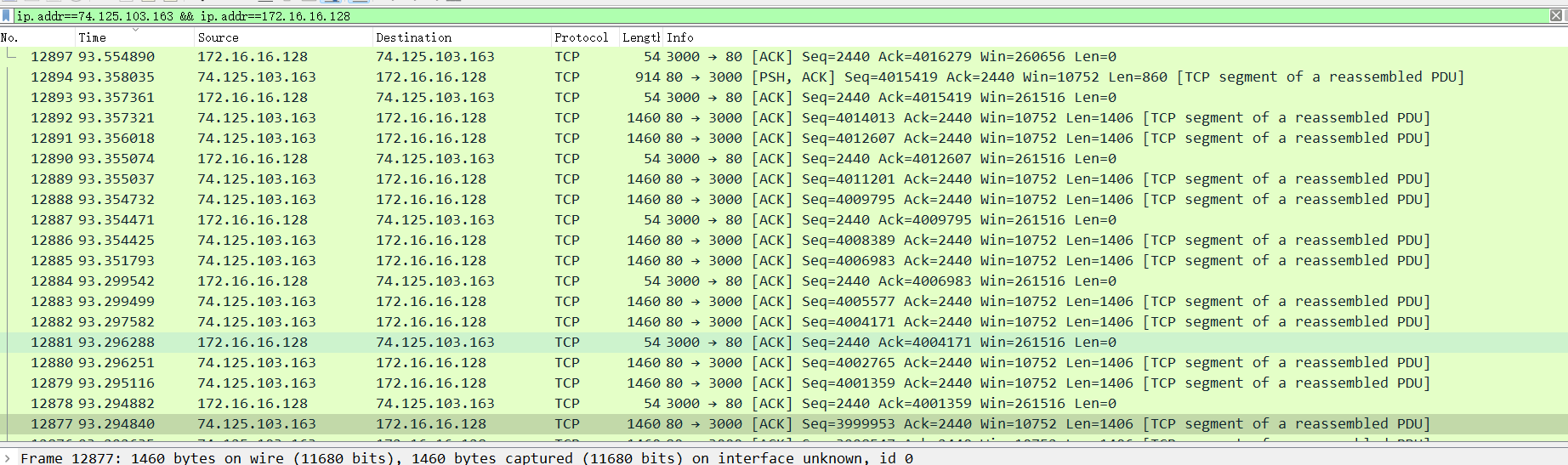


图2 最大的数据通信量

来自于172.16.16.128与74.125.103.163

3）对通信量最大的端点之间的会话进行分析，通信数据又什么特点呢？请提供关键分析 证据截图

**答：**



172.16.16.128给74.125.103.163发送长度为54的一个包， 74.125.103.163发送长度为1460的两个包。

【验证实验 2】

我们通过 Wireshark 的协议分层结构统计功能发现某一段时间内 ARP 数据包的数量大 增，利用过滤器将这一段时间内的arp 数据包过滤出来，保存在捕获文件lotsofarp.pcapng 中， 请你对该捕获文件进行分析，你有什么猜测或者结论呢？请给出你的理由并提供证据截图。

**答**：

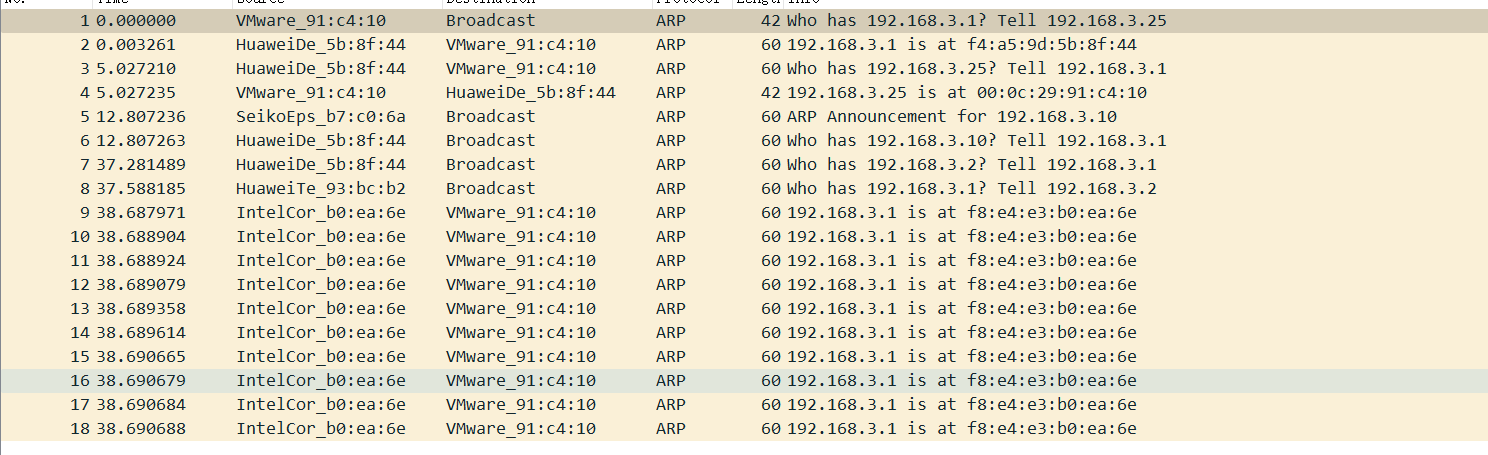


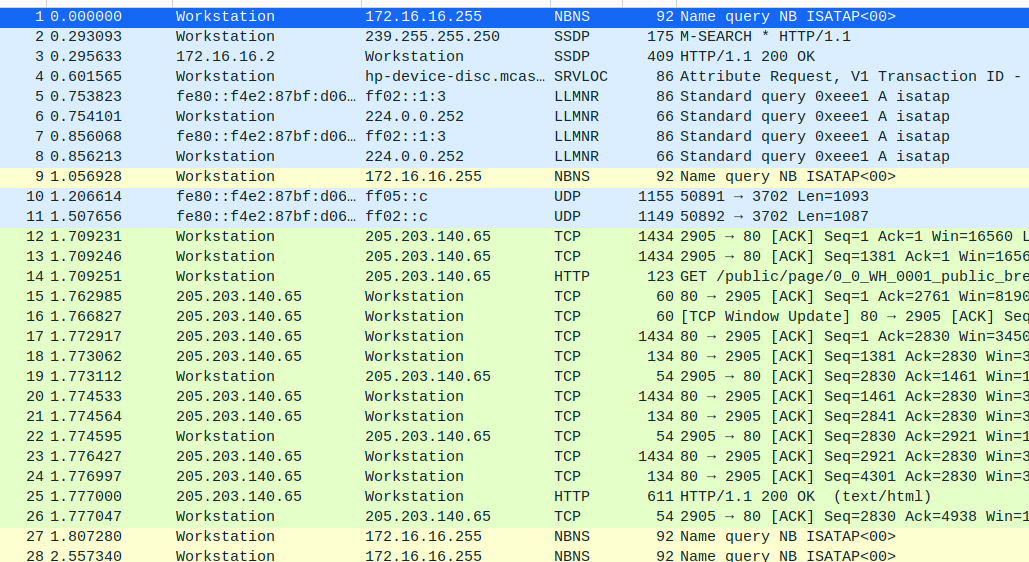
图4-异常的arp欺骗

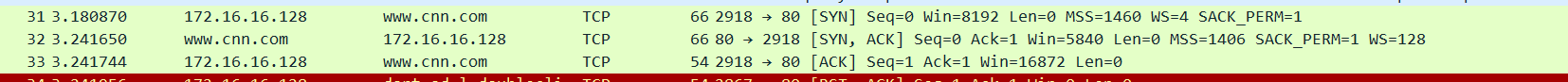
IntelCor\_b0:ea:6e在短时间内发送了多条arp数据包，对192.168.3.1进行了arp欺骗，伪装为192.168.3.25，防止目的主机刷新缓存区。

【验证实验 3】

用 Wireshark 打开捕获文件 lotsofweb.pcapng，通过设置名字解析的相关选项和参数，使 8 得数据包列表面板中的 source 或者 destination 列中出现与 IP 地址对应的名字，并提供截图。

答：



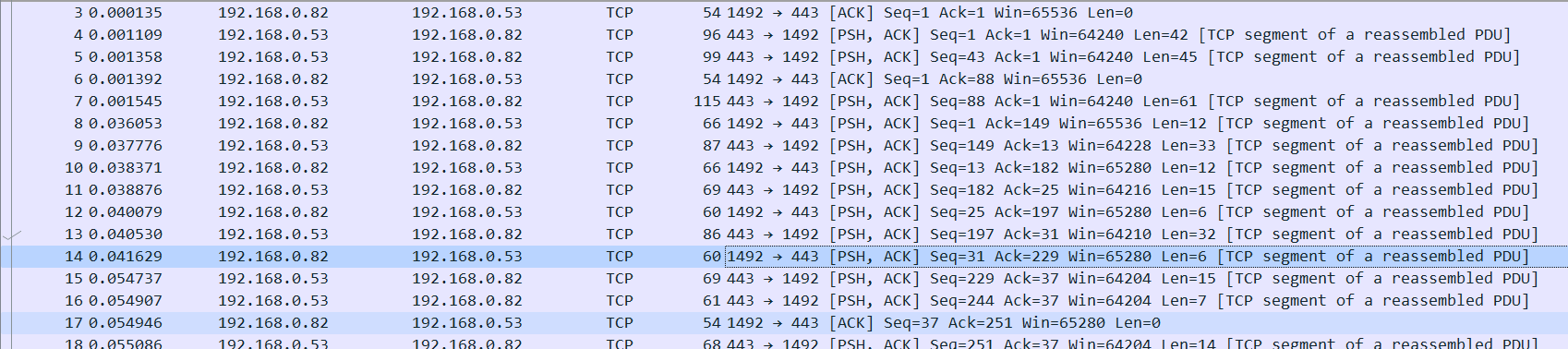


【验证实验 4】

使用 Wireshark 打开捕获文件 wrongdissector.pcapng，对数据包进行分析，并回答下列问 题：

1）Wireshark 是否选择了错误的协议解析器，为什么？请提供截图证据；

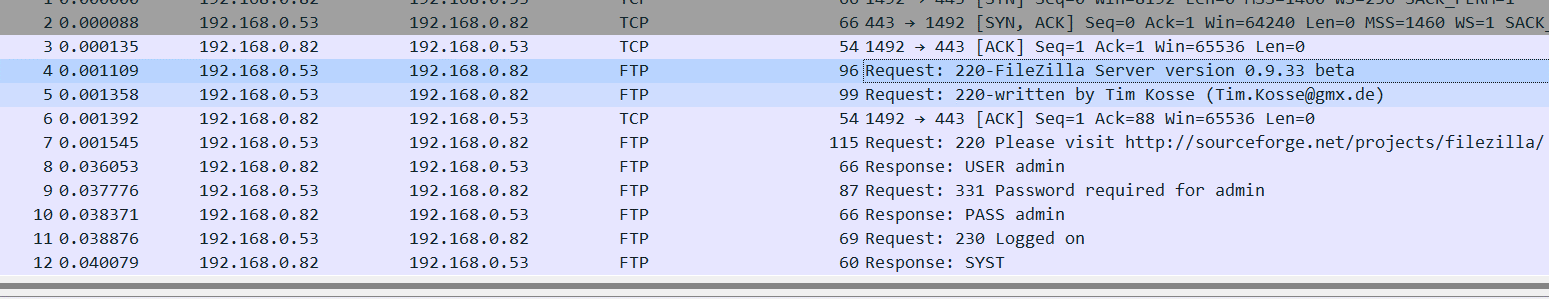
**答：**是，无法对包文进行正确解析。



2）你认为正确的协议解析器应该是什么？为什么？

**答：**FTP，因为开始时有FileZilla Server version 0.9.33 beta，是ftp服务器

3）请为 Wireshark 的更换正确的协议解析器，并提供截图证据。



4）你认为本案例中 Wireshark 错误选择协议解析器的原因时什么？

**答：**本案例中使用的端口为443，常用的协议是https故wireshark默认使用TCP解析。

【验证实验 5】

使用 Wireshark 打开捕获文件 http\_google.pcapng，对数据包进行分析，完成下面的操作：

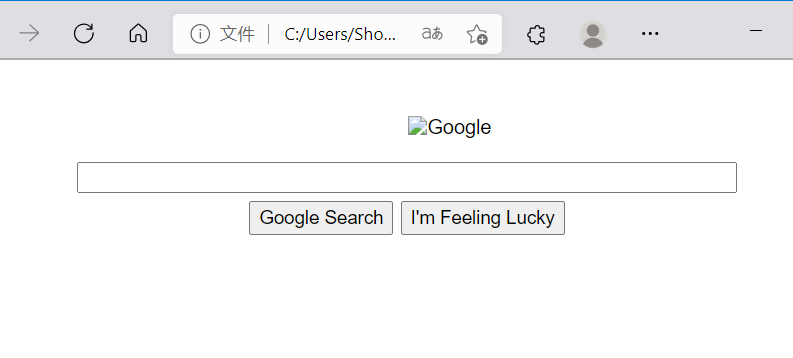
1）在 Wireshark 的数据包列表面板中找到第一个 http 请求数据包；

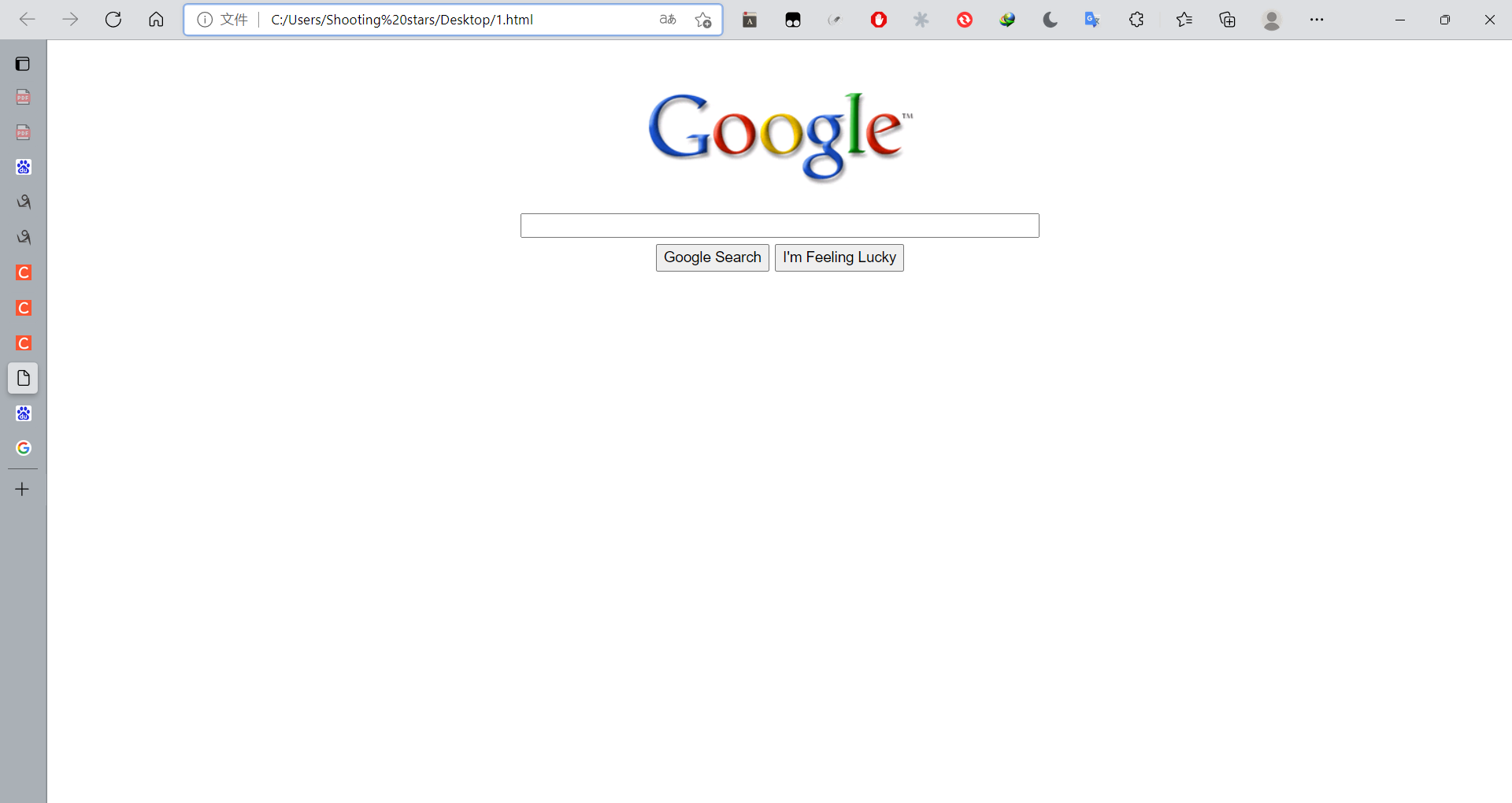


2）跟踪该 http 流，找到第一个 http 请求数据包的响应数据包；



3）该响应数据包响应了一个什么样的内容呢，从 http 的响应数据包提取服务器响应的 对象，并使用浏览器查看之？并请提交截图

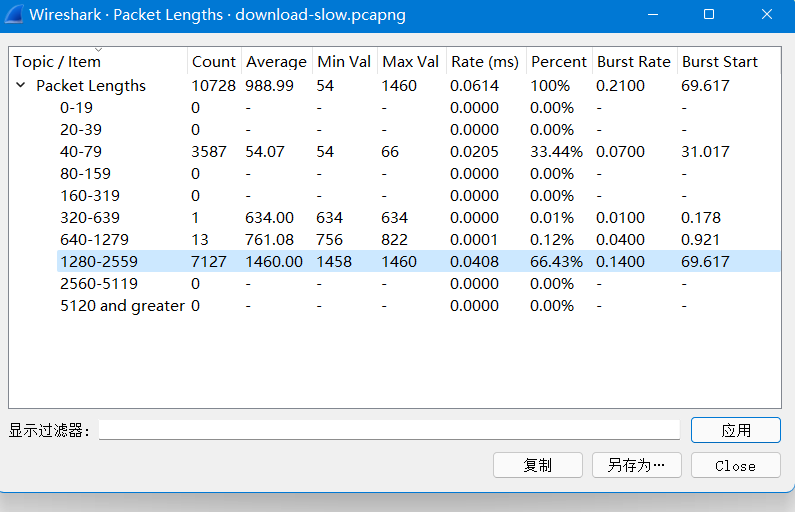




【验证实验 6】

使用 Wireshark 打开捕获文件 download\_slow.pcapng，对其数据包长度进行统计分析。 这些网络流量中是否存在大规模的数据传输呢？请说明你的理由并提供证据截图。

**答：**



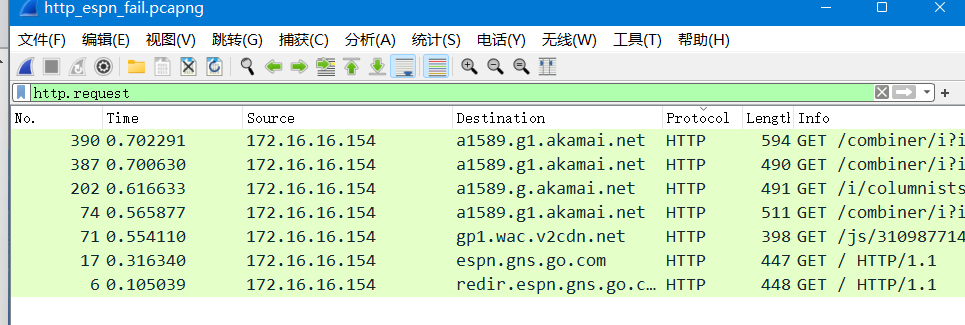
存在很多较大的数据包，在包长度为1280-2559之间有7127个包传输，网络正在进行大量的数据传输。

【综合分析实验 7】

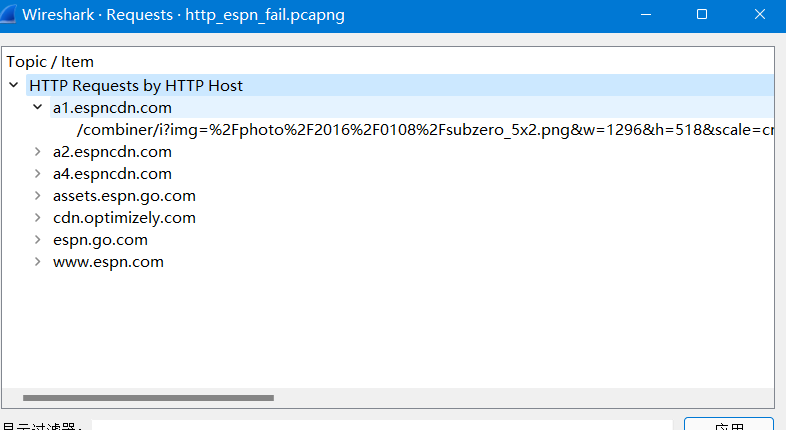
在这个场景中，我们的用户是 Peter，一位从不熬夜导致经常错过球赛的大学生球迷。 每天上午，他都要打开计算机访问网站，查看前一天晚上的最终比赛成绩。 这个上午，当 Peter 和 往常一样打开网站 ESPN 查看比赛成绩的时候，他发现加载网页 耗费了很长的时间，而当加载过程终于完成时，页面丢失了大部分图片和内容。这是怎么回 事儿呢？我们一块儿来帮 Peter 分析下。 首先需要明确的是，这个问题只在 Peter 一个人的计算机上发生，并没有影响到其他 人，因此我们在他的计算机上进行数据包嗅探工作，获取了 http\_espn\_fail.pcapng 捕获文 件。 从何入手呢？ HTTP。 【分析过程】：

实验 7-1：请提供两种方法过滤 http 请求数据包的截图

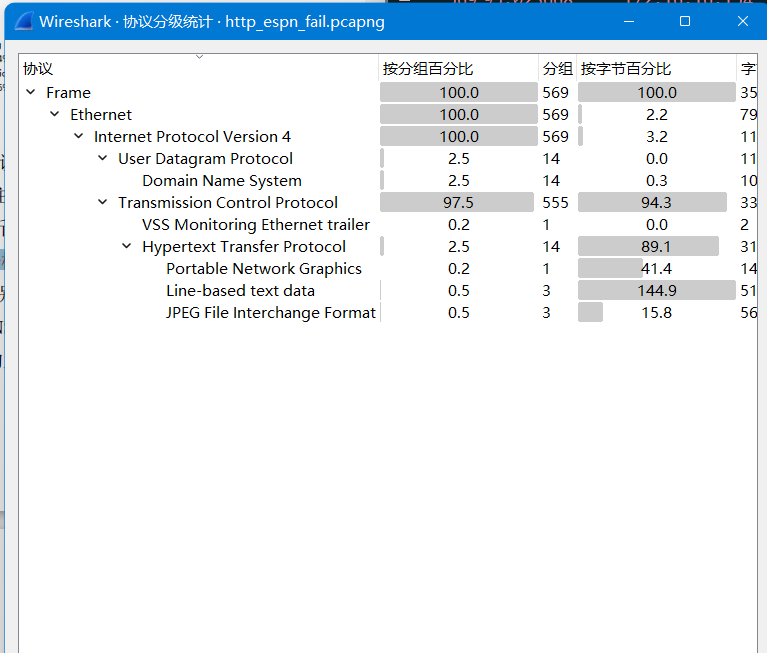
**答**：1、通过过滤器：



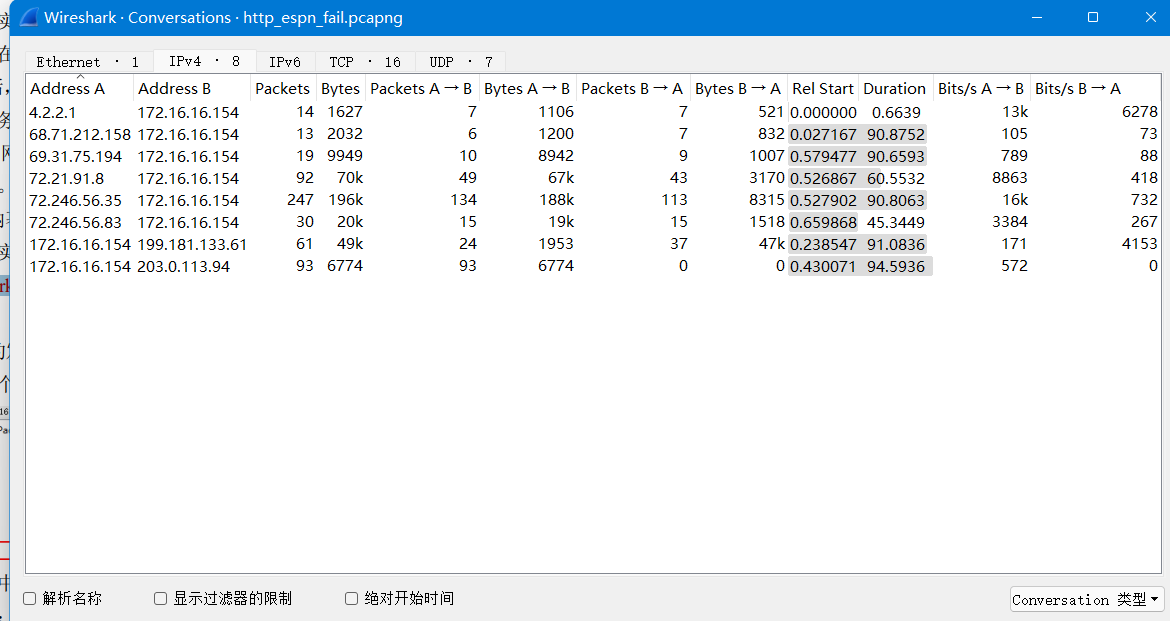
2、通过统计功能：



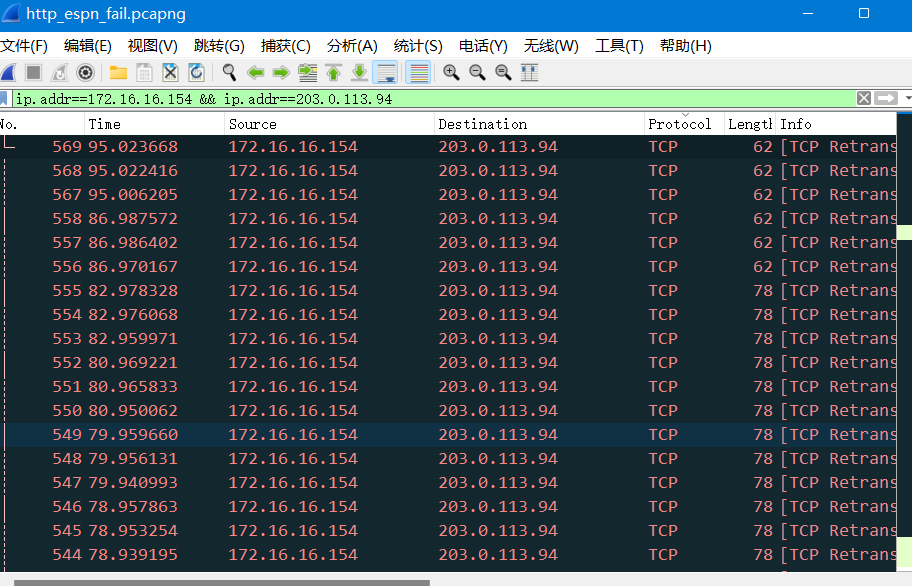
实验 7-2：请提供对整个报文的协议分层统计分析的截图



实验 7-3：请使用 Wireshark 统计会话功能列出本案例捕获数据包中的所有会话，并提交 截图



实验 7-4：请在 Wireshark 数据包列表面板中展示异常会话，并 提交截图



【本次实验的心得、体会和建议】

在本次实验中，我学会了如何使用wireshark抓包，并对所抓取的数据包进行分析，尝试了wireshark中自带的许多高效实用的功能，同时能够对报文进行分析，对不同的数据片段进行辨识。同时我还学习到了许多关于计算机网络的知识，对于计算机网络的相关知识点有了一个大概的了解。

体会：在学习过程中，一上来就开始实验有些困难，对于基本知识点没有一个了解，建议开课前进行一个先导课程或开放资料，对于实验中的协议，端口，ip地址等内容有一个比较好的认识将更加有利于实验的进行。