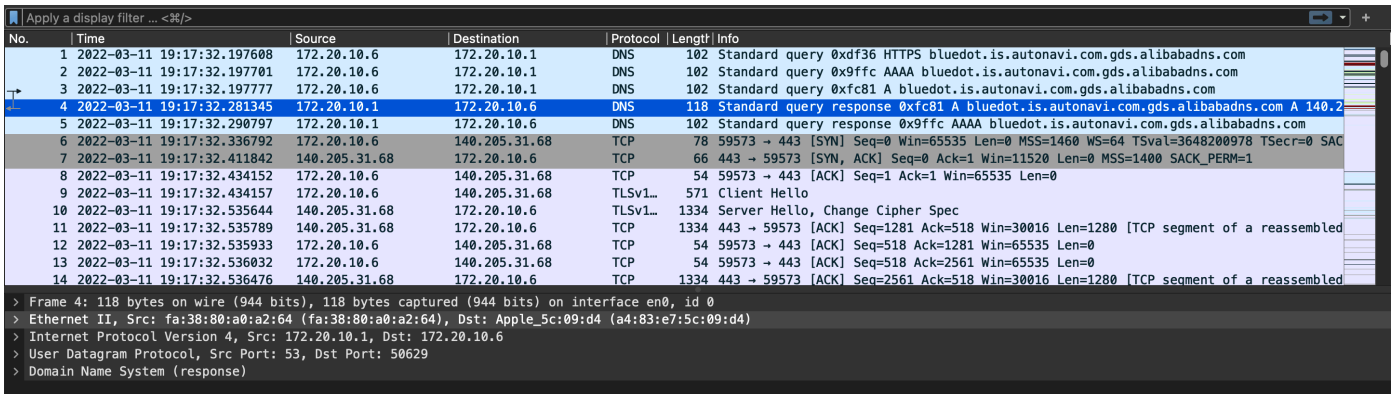
练习：用Wireshark分析HTTP

1. TCP/IP协议的5层结构

五层协议 （5层）：物理层、数据链路层、网络层、运输层、 应用层。

如图所示：



从上往下依次是：

- `Frame 4`：数据链路层
- `Ethernet II`：数据链路层
- `Internet Protocol Version 4`：网络层
- `User Datagram Protocol`：传输层
- `Domain Name System`：应用层

2. 分析哪些协议以及协议所占百分比

协议如下：

物理层：RJ45、CLOCK、IEEE802.3

数据链路：PPP、FR、VLAN、MAC

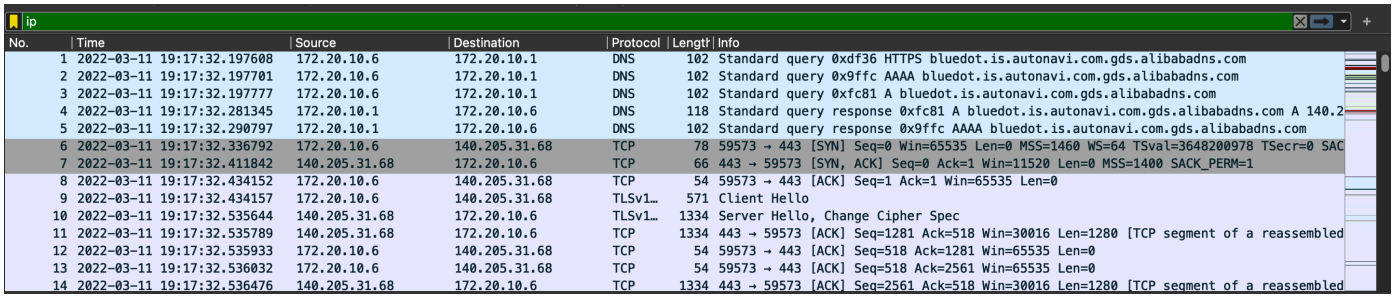
网络层：IP、ICMP、ARP、OSP、IPX、RIP、IGRP

传输层：TCP、UDP、SPX

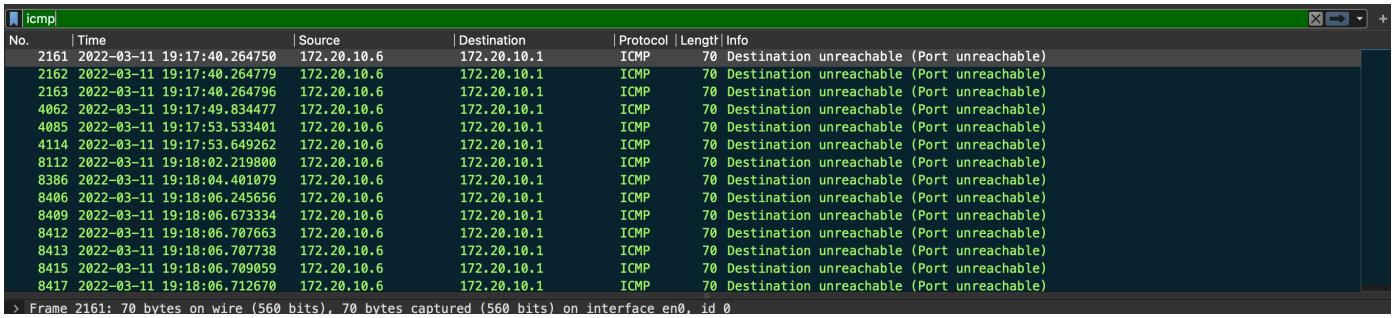
应用层：FTP、DNS、Telnet、SMTP、HTTP

物理层和数据链路层没有接受到协议。

网络层接受到了IP：

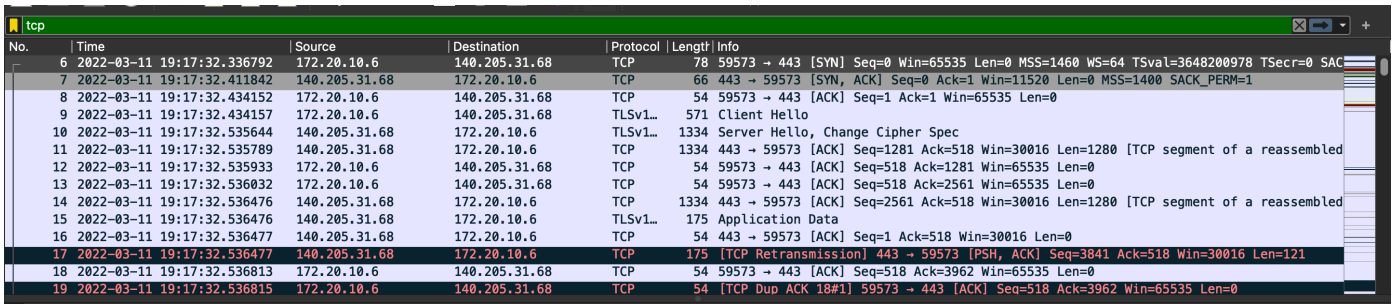


ICMP：

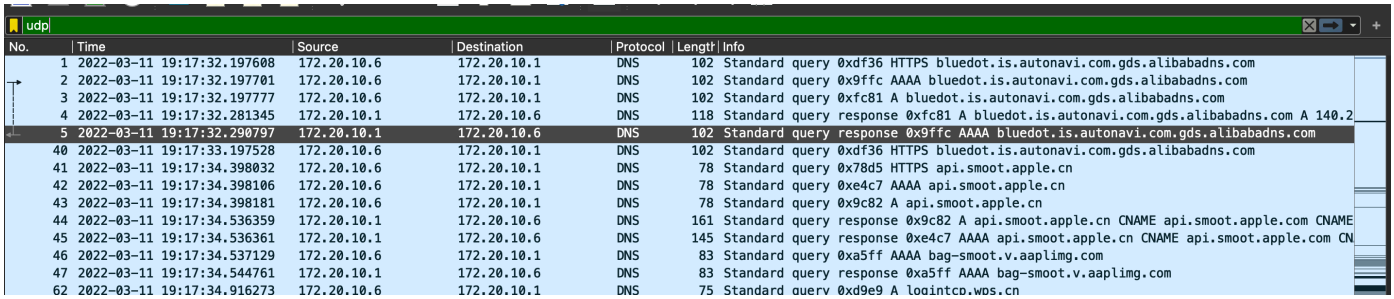


占比来说IP占绝大部分，ICMP较少。

传输层接受到了TCP：

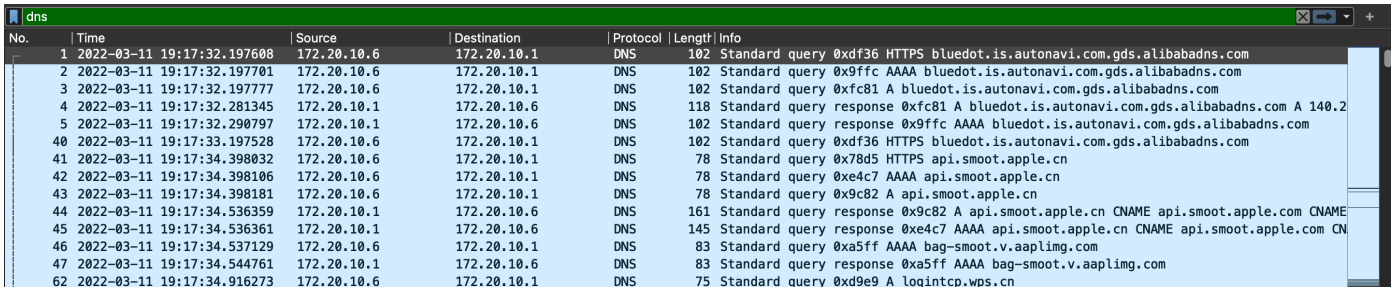


UDP：

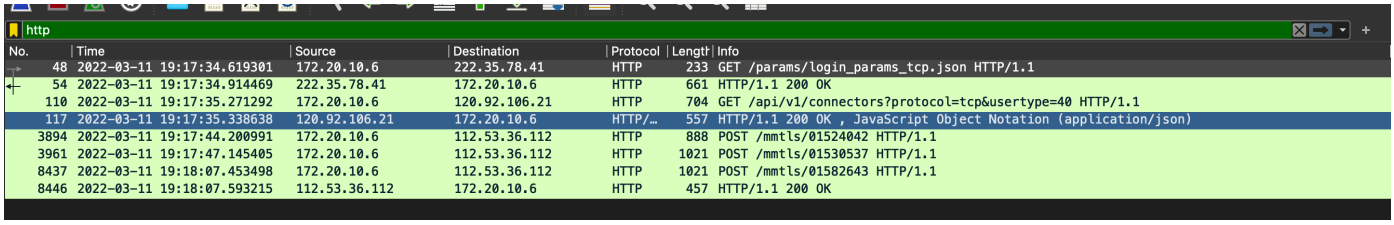


占比来说TCP占绝大部分，UDP较少。

应用层接受到了DNS：



HTTP：



占比来说DNS占绝大部分，HTTP较少。

3. 指出Web服务器的IP地址

本机的IP地址：172.20.10.6

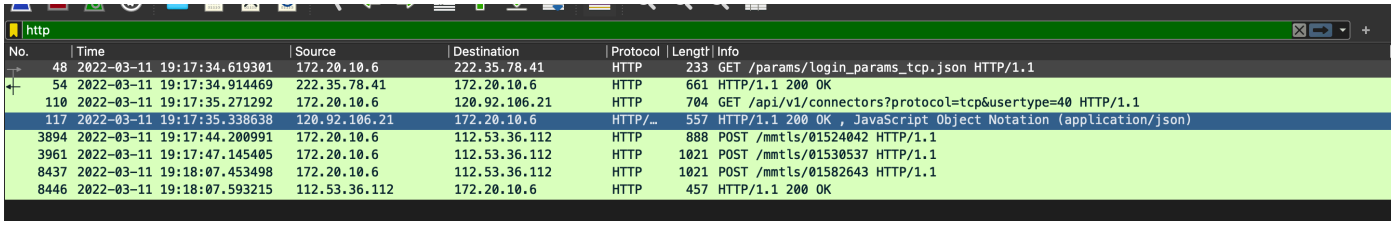
```
[wangxinhao@wangxinhaodeMacBook-Pro My_Personal_Blog % ifconfig | grep "inet " |
grep -v 127.0.0.1
        inet 172.20.10.6 netmask 0xfffffff0 broadcast 172.20.10.15
```

对端的：39.156.66.10

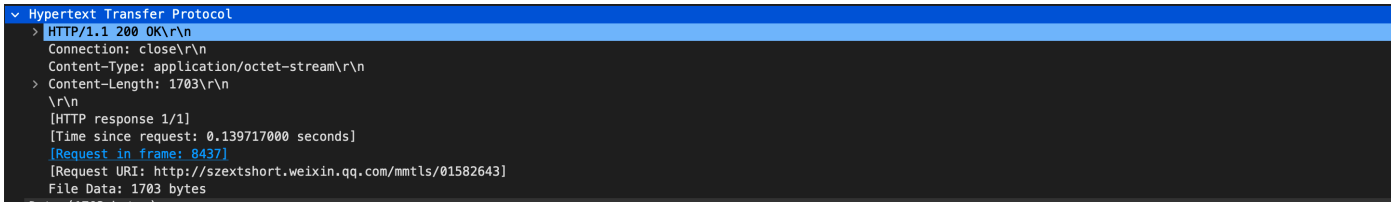
```
wangxinhao@wangxinhaodeMacBook-Pro My_Personal_Blog % ping baidu.cn
PING baidu.cn (39.156.66.10): 56 data bytes
```

4. 应用显示过滤器，分析你的主机与Web服务器之间HTTP协议

如图：



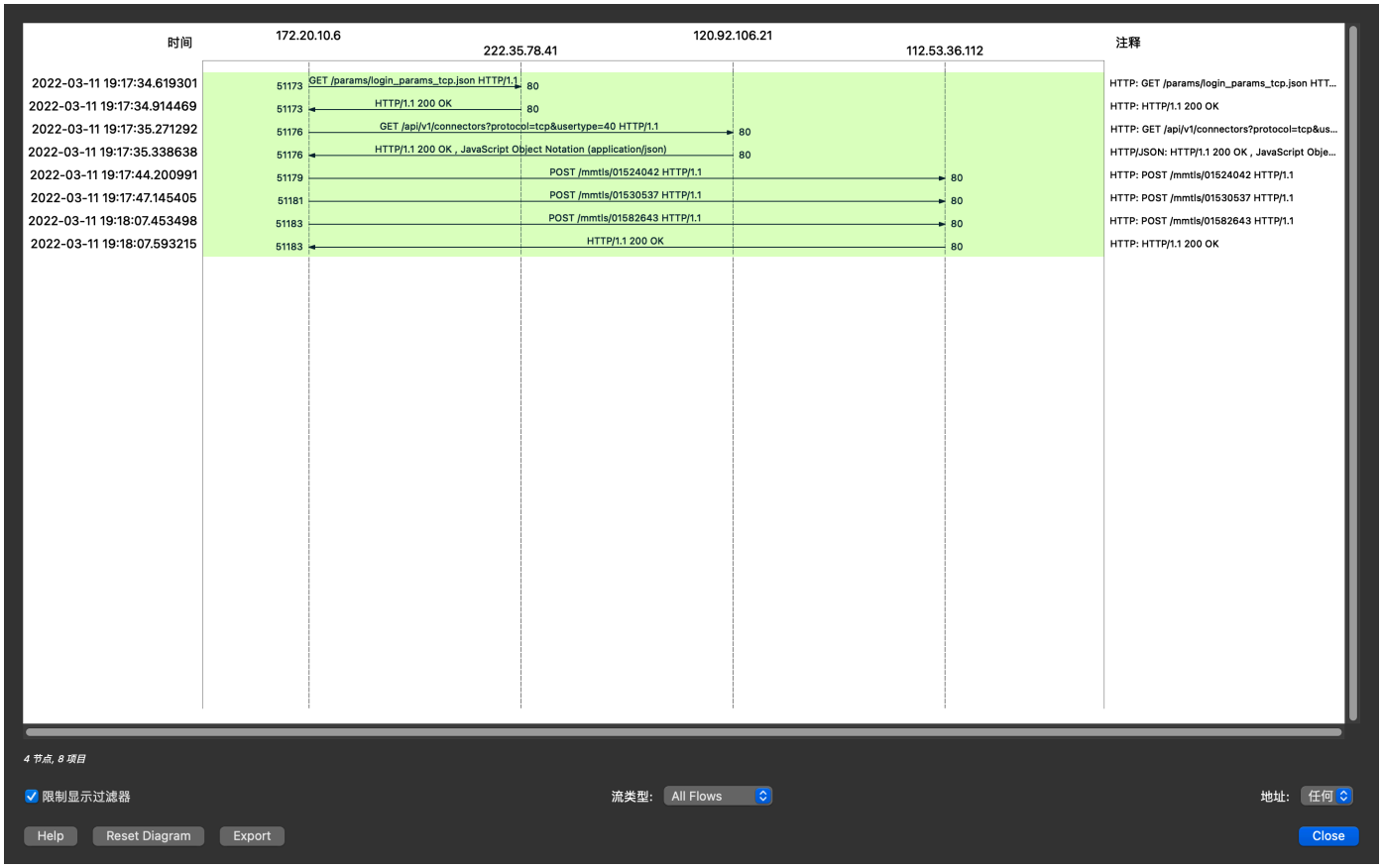
HTTP协议报文详细信息：



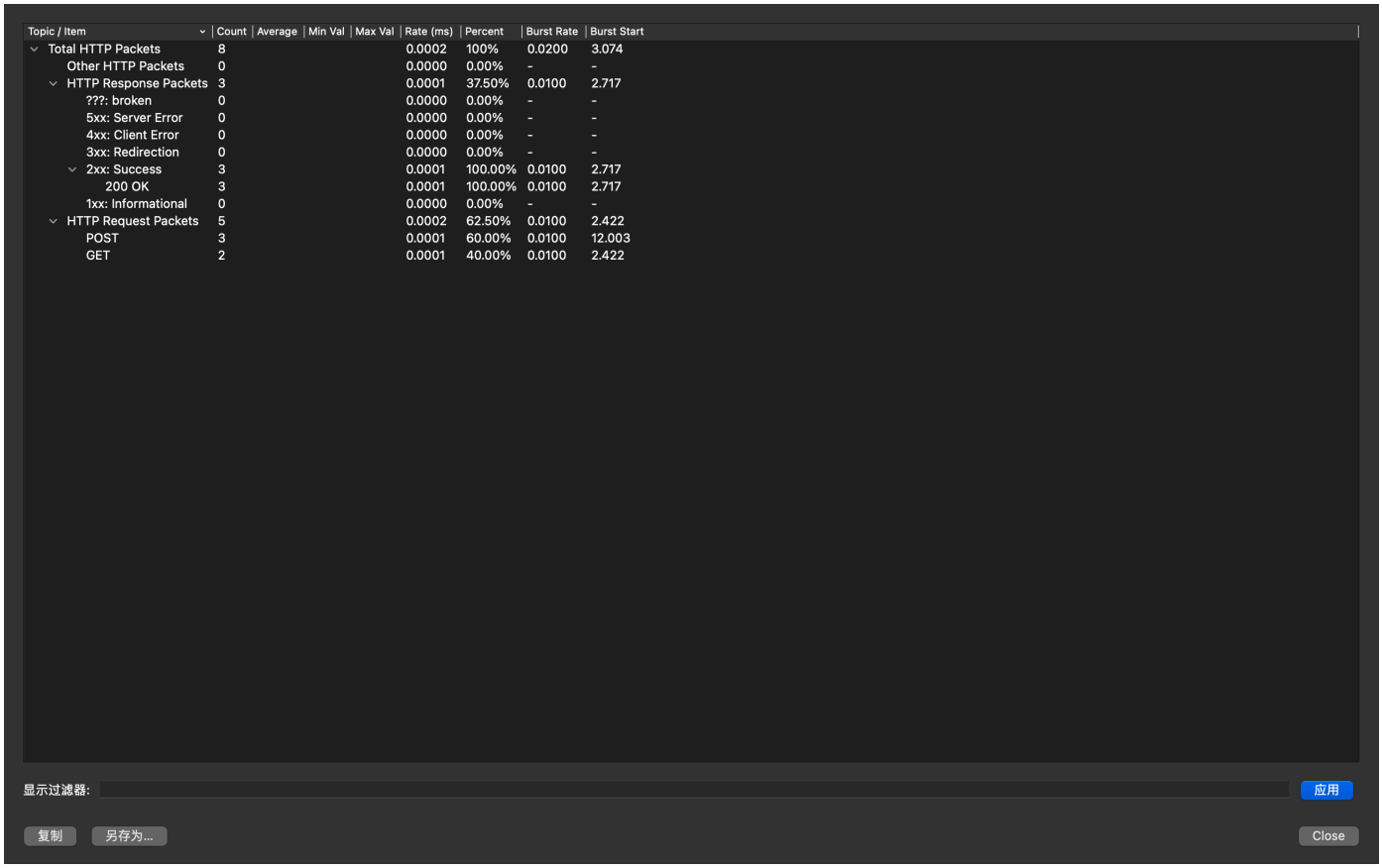
以下是 HTTP 请求/响应的步骤：

1. 客户端连接到Web服务器 一个HTTP客户端，通常是浏览器，与Web服务器的HTTP端口（默认为80）建立一个TCP套接字连接。例如，http://www.baidu.com。
2. 发送HTTP请求 通过TCP套接字，客户端向Web服务器发送一个文本的请求报文，一个请求报文由请求行、请求头部、空行和请求数据4部分组成。
3. 服务器接受请求并返回HTTP响应 Web服务器解析请求，定位请求资源。服务器将资源复本写到TCP套接字，由客户端读取。一个响应由状态行、响应头部、空行和响应数据4部分组成。
4. 释放连接TCP连接 若connection 模式为close，则服务器主动关闭TCP连接，客户端被动关闭连接，释放TCP连接;若connection 模式为keepalive，则该连接会保持一段时间，在该时间内可以继续接收请求;
5. 客户端浏览器解析HTML内容 客户端浏览器首先解析状态行，查看表明请求是否成功的状态代码。然后解析每一个响应头，响应头告知以下为若干字节的HTML文档和文档的字符集。客户端浏览器读取响应数据HTML，根据HTML的语法对其进行格式化，并在浏览器窗口中显示。

5. 执行 统计—>流量图，显示浏览器与HTTP服务器之间的HTTP协议过程



6. 执行 统计—>HTTP，显示浏览器与HTTP服务器之间请求与响应分组总数及占比



7. 其他问题及发现

我发现我捕获的信号中代表http协议的信号非常少，反而大部分是DNS协议的信号，不知道是什么原因。