哈尔滨工业大学

**<<计算机网络>>**

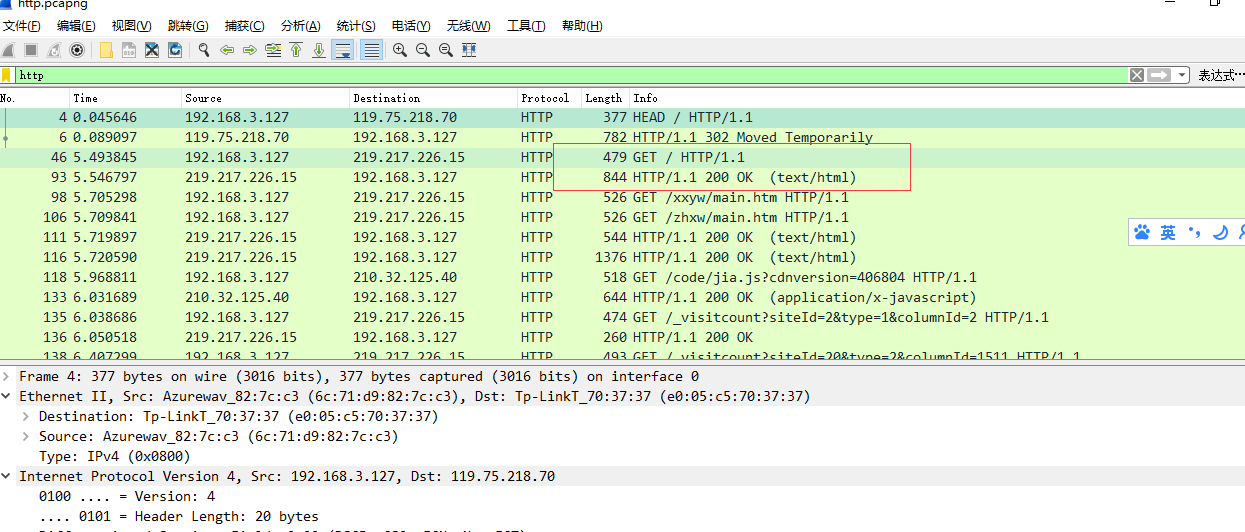
**实验报告**

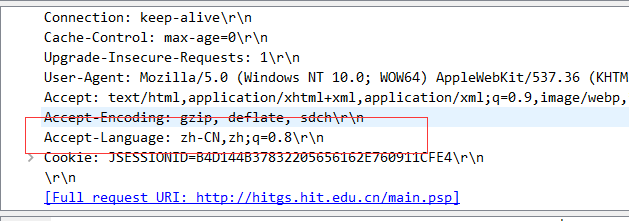
**(2016年度春季学期)**

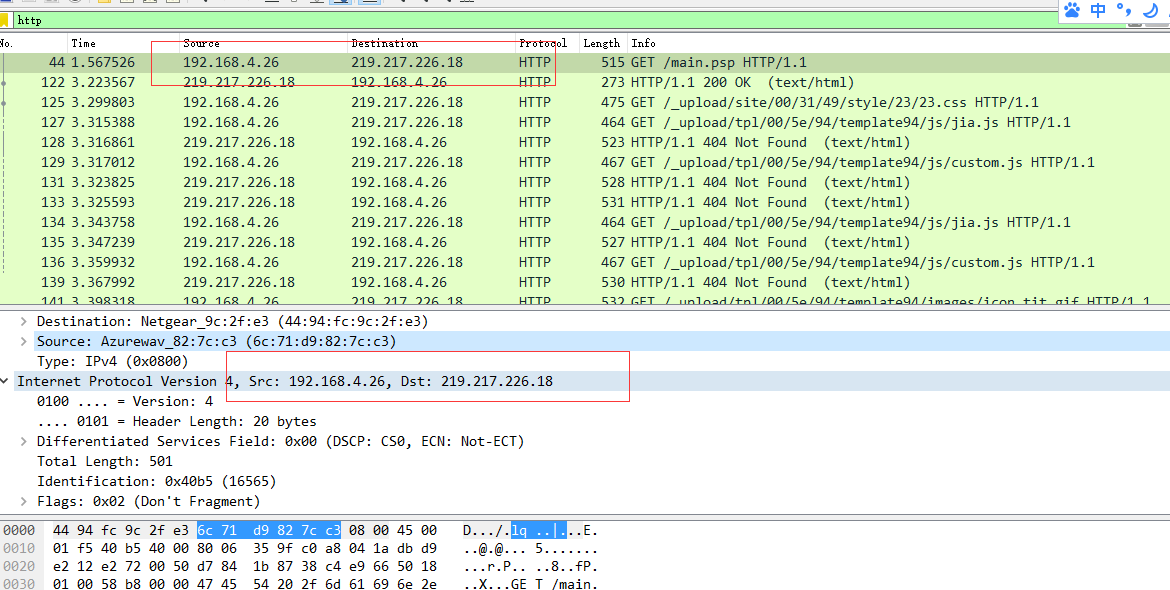
|  |  |
| --- | --- |
| **姓名：** | **马晶义** |
| **学号：** | **1130310723** |
| **学院：** | **计算机科学与技术学院** |
| **教师：** | **刘晓烽** |

**实验5 ：利用Wireshark进行协议分析**

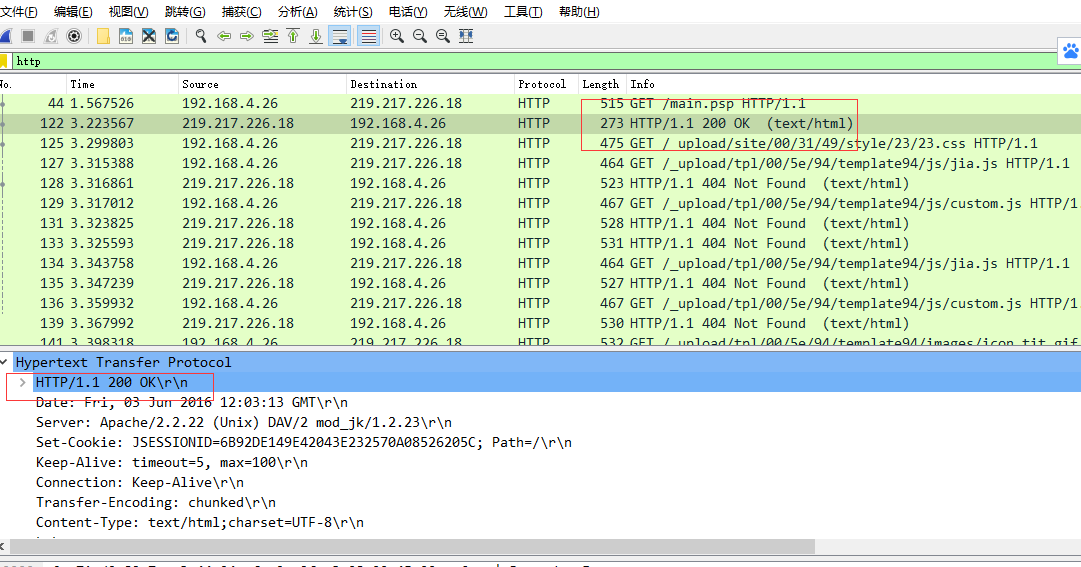
1. **实验目的**
2. **实验内容**
3. **实验过程**
   1. **HTTP分析**
4. **HTTP GET/response**
   1. 图中可以看出浏览器GET请求是HTTP 1.1，所访问的服务器的HTTP协议版本号是1.1（返回HTTP/1.1 200 ok）



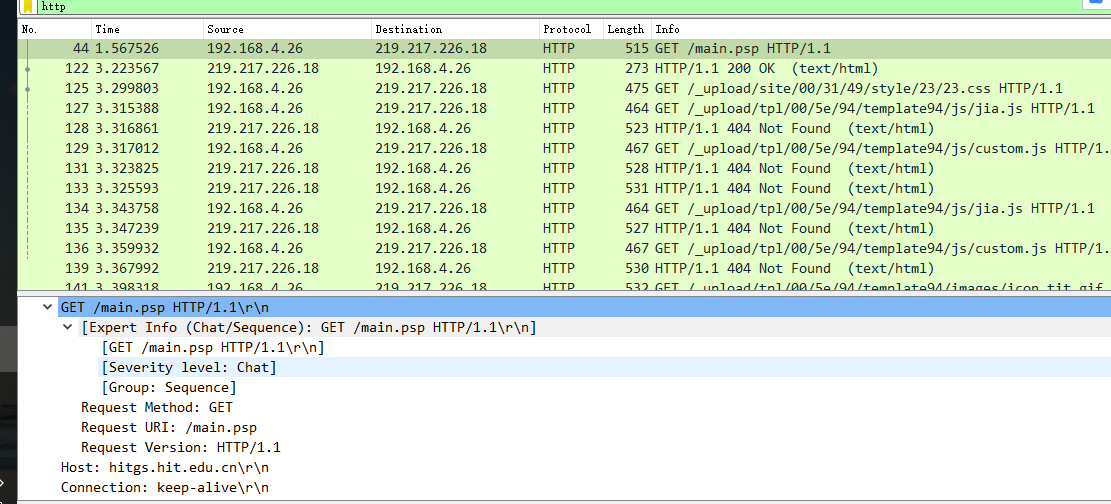
* 1. 浏览器指出接收的语言版本： zh-CN 简体中文
  2. 本机的IP地址是192.168.4.6，服务器http://hitgs.hit.edu.cn/main.psp的IP地址是 219.217.226.18



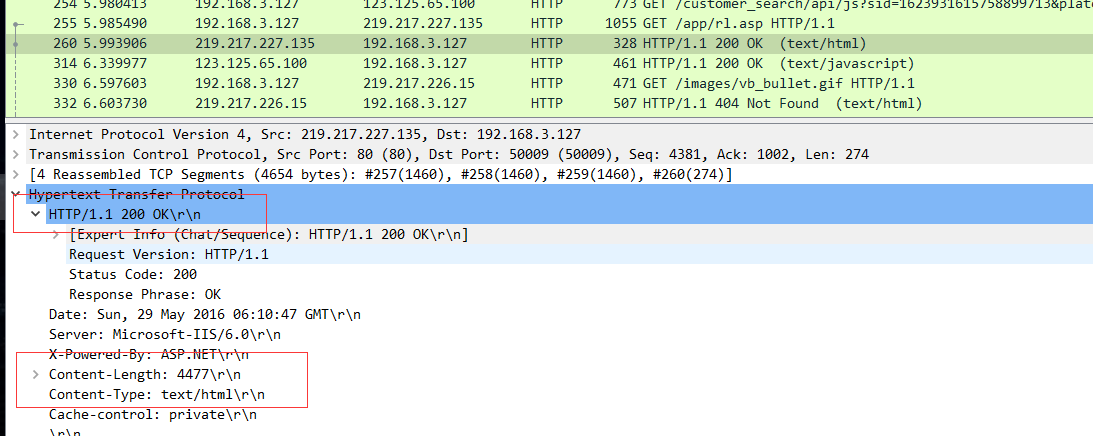
* 1. 从服务器向浏览器返回的状态码是200



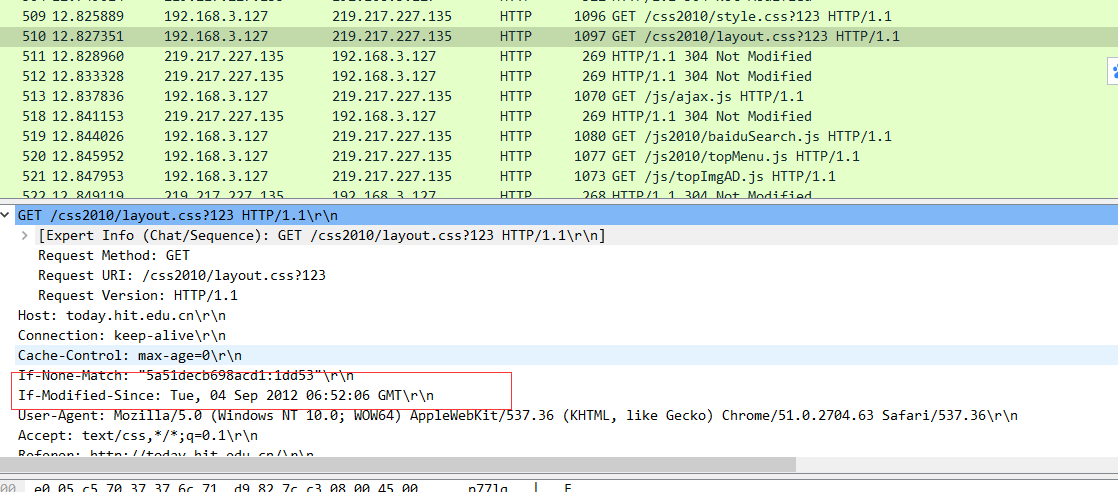
1. **HTTP 条件 GET/response交互**
2. 发出的第一个GET请求中，没有 IF-MODIFIED-SINCE



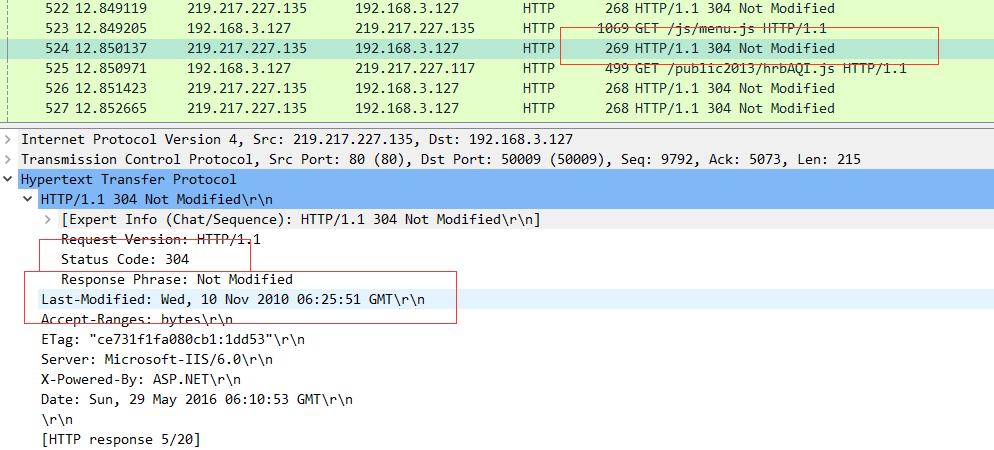
1. 明确了文件的内容，图中可以看出返回文件内容的大小及格式



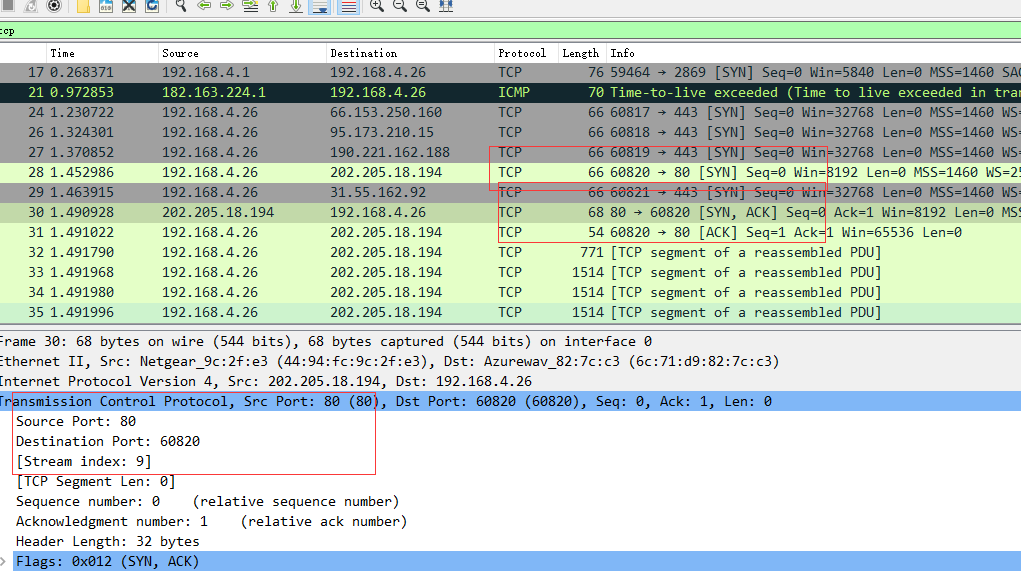
1. 较晚的HTTP GET请求中，有一行IF-MODIFIED-SINCE,后面跟着的是报文上次修改的时间



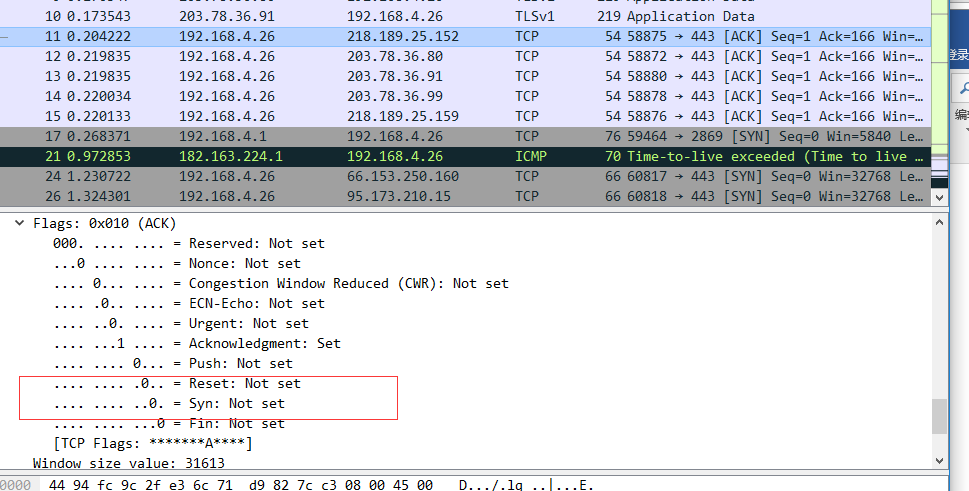
1. 状态码是 304，不明确返回文件的内容。因为返回的是304的报文，表示缓存的报文未被修改，是最新的。因此，不需要返回文件的内容，浏览器只需要从缓存中取得即可。



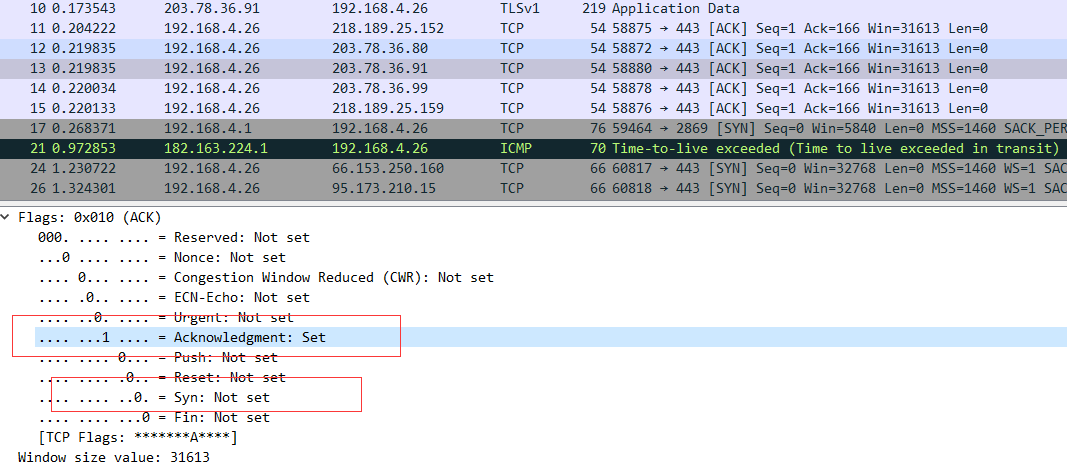
* 1. **TCP分析**
     1. 客户端主机的IP地址192.168.4.26 端口号是60820
     2. 服务器的IP地址是202.205.18.194 发送和接收的端口号是80



* + 1. 初始化TCP连接的TCP SYN报文段序号是0，用标志位1来标识SYN报文段

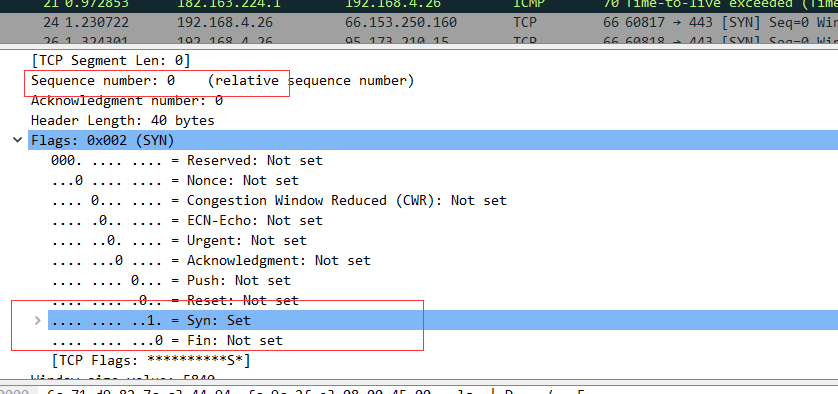


* + 1. 服务器向客户端发送的SYNACK报文段序号是 0，Acknowledgement字段的值是1, 用1来标示SYNACK

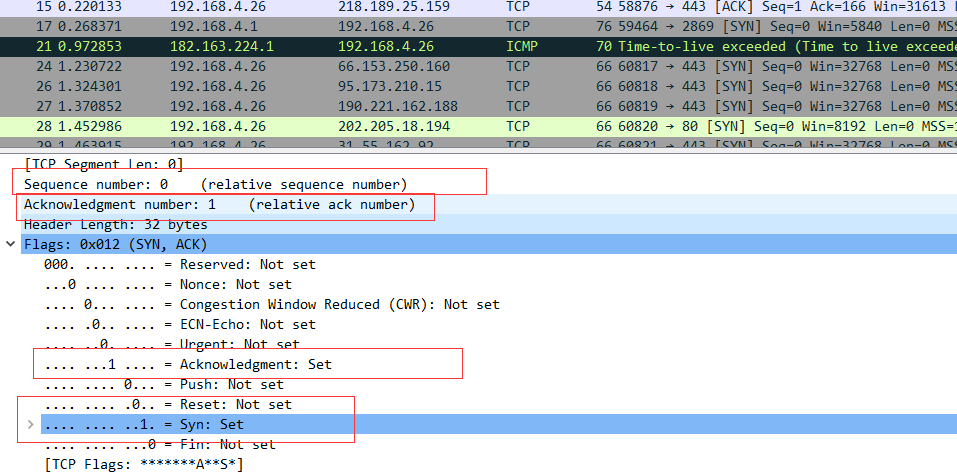


* + 1. Tcp三次握手过程：

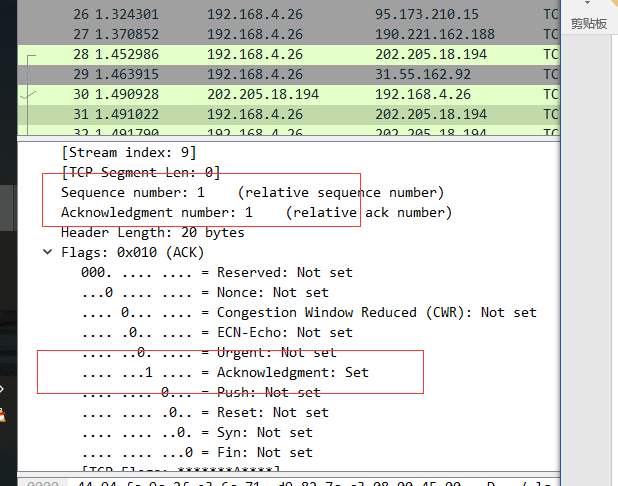
第一次握手：seq = 0 ,syn = 1



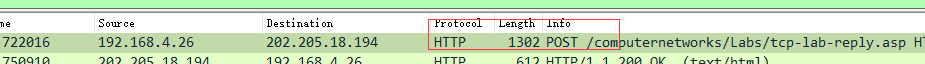
第二次握手：seq = 0,ack = 1,syn=1,ack标识为1

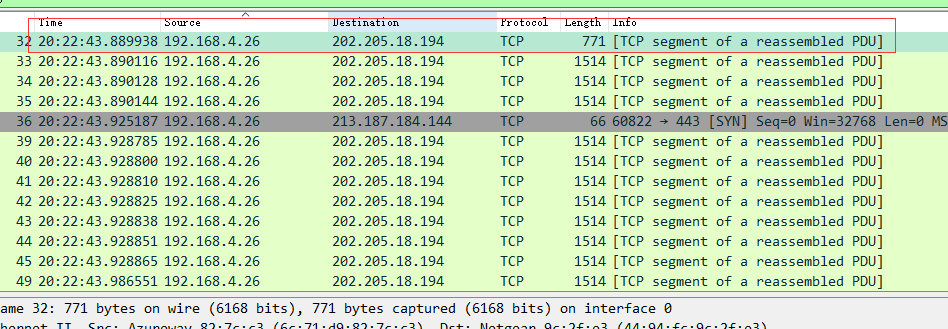


第三次握手 seq=1,ack=1,ack标志位是1



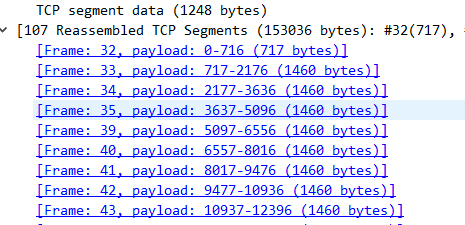
* + 1. 包含HTTP POST命令的TCP报文段序号是



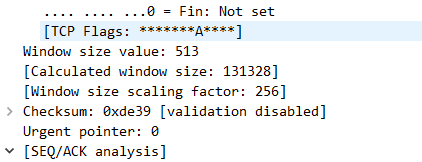
* + 1. TCP连接上的第六个报文段的序号是 32 发送时间 20:22:43.889938

RTT时间：接收时间：20:22:43.927974

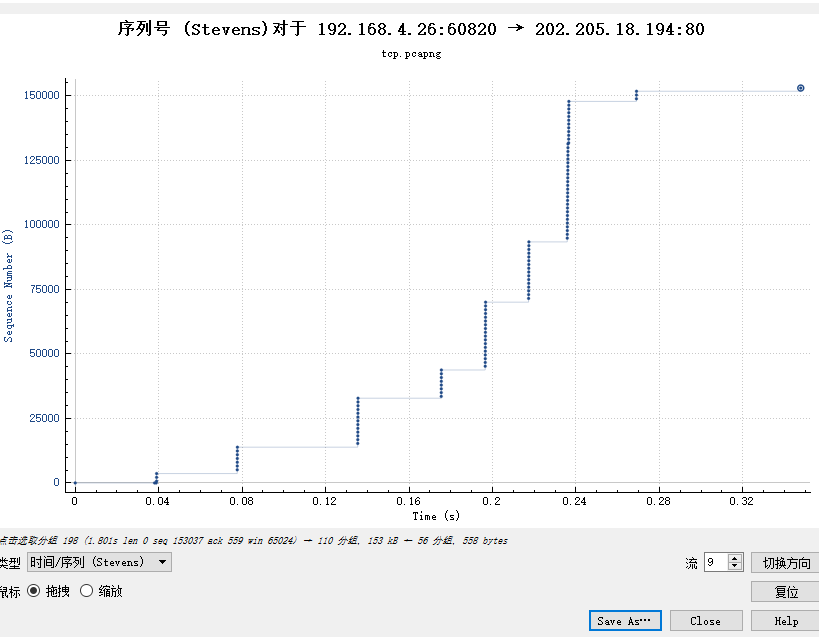
* + 1. 前6个TCP报文段长度分别是 :717,1460,1460,1460,1460,1460



* + 1. 接收端的可用缓存空间是 513，限制发送的传输后，接收端缓存仍然够用



* + 1. 无重传的报文段 根号序列号判断，没有重复

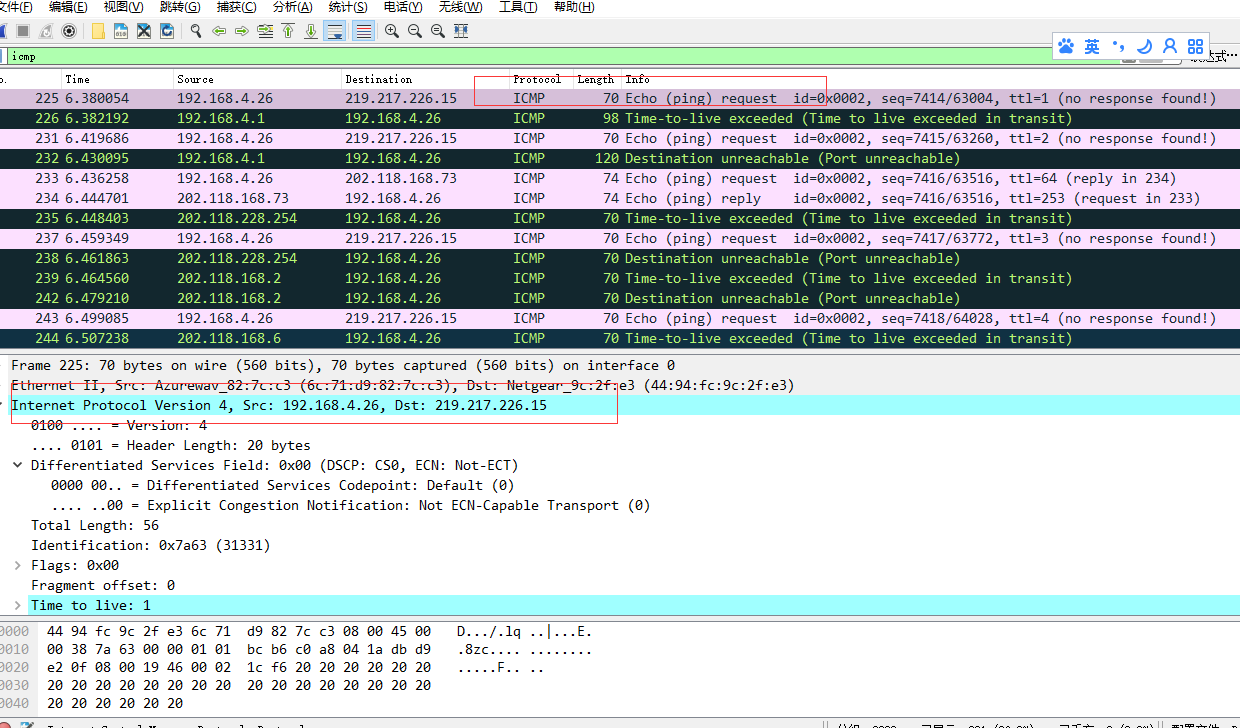


* + 1. 连接的Throughput是：

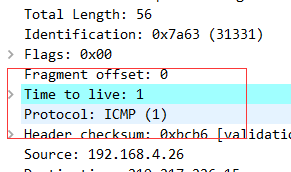
1496\*3/(2.488325-2.488311)/8=40071428.58 (bytes/s)

* 1. **IP分析**

**（1）**

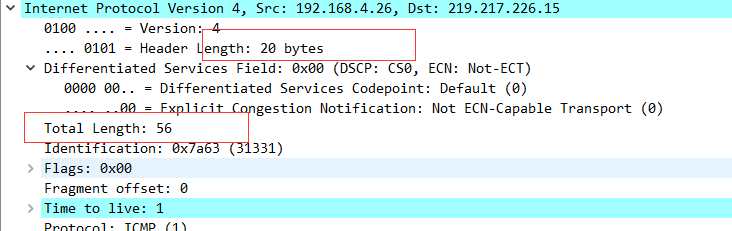


* + 1. 主机的IP地址是：192.168.4.26
    2. 上层协议字段的值是 ICMP(1)

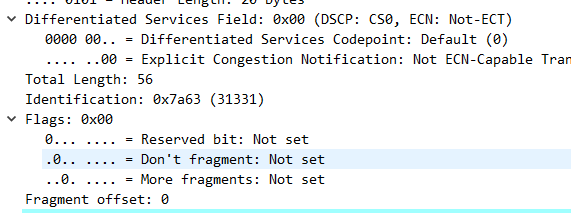


* + 1. IP头有20字节，净载为56-20=36字节

总长度是56去掉报文头20字节得到

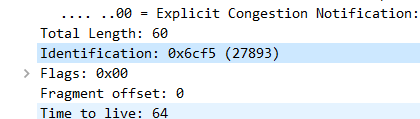


* + 1. 数据包净载大小 36字节
    2. 该IP数据包未分片，依据是DF=0,表示可以分片；但MF=0表示是最后一个分片，因此是未分片的。



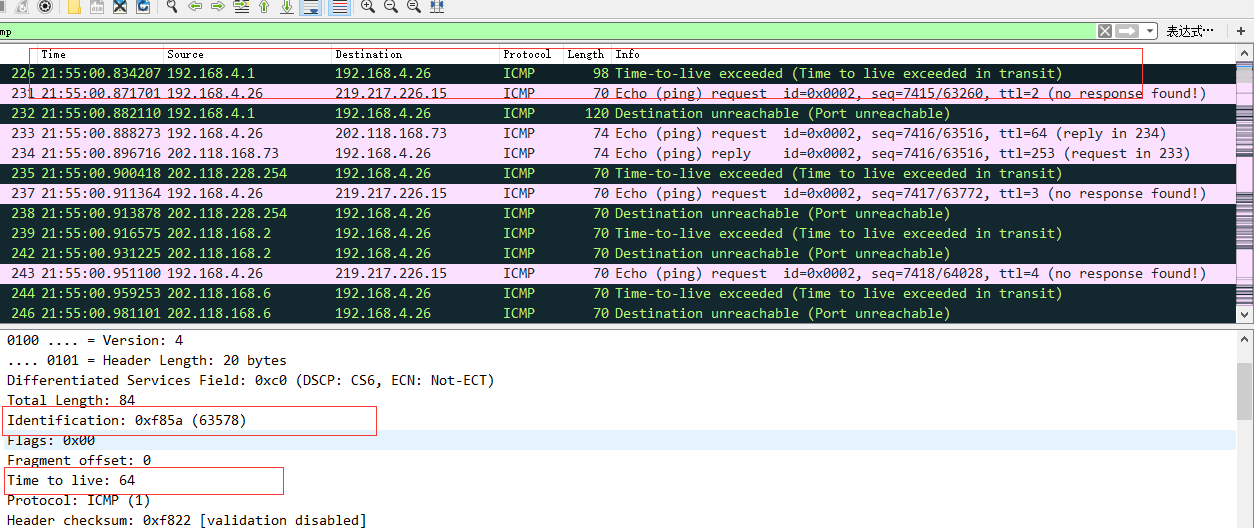
（2）

* + - 1. IP数据报中总是发生改变：id,ttl,头部检验和
      2. ID,TTL,头部段校验和字段会发生变化，目的IP地址和源IP地址不会发生变化。ID数据包ID；TTL在经过路由器的时候需要减一，头部发生变化，因此校验和不一样。源主机和目的主机未变化，因此源IP目的IP不发生变化。
      3. Identification字段值 0xbcf5



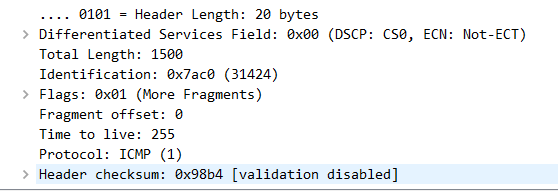
（3）最近路由器返回的ICMP Time-to-live-exceeded消息：

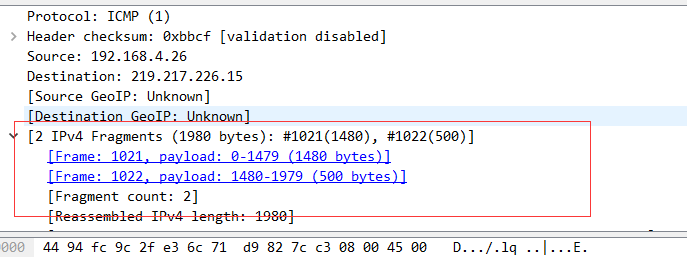
1、A. Identification字段值为：0xf85a(63578)，TTL值为：64



2、B. Identification根据计数器变化； TTL增长。

（4）包大小改为2000字节以后的发送ICMP Echo Request消息：





1、消息被分片了,上图中显示被分为2片了

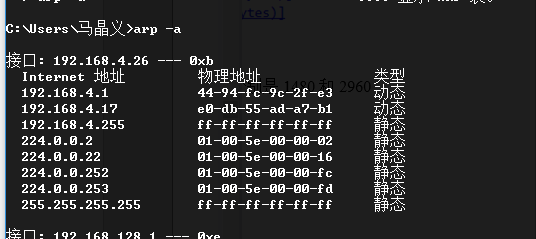
2、第一个IP报的头部段flag是1，表明它不是最后一个分片，该分组的分片长度是1500B，其中数据段是1480个字节，头部段20字节。

修改为3500字节后的发送的ICMP Echo Request:



1. 原始数据包分为3片
2. 前两个分片MF=1，后两个分片offset分别是1480和2960
   1. **ARP数据包**
      1. 利用MS-DOS命令查看arp缓存

列含义：Internet 地址 物理地址 类型



* + 1. 清除主机上ARP缓存的内容：

1. ARP数据包的格式：

如下图所示，ARP分为9个部分： Hardware type：2字节

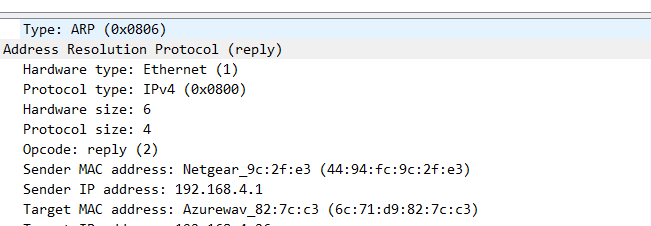
Protocol type：2字节 Hardware size：1字节

Protocol size：1字节 Opcode：2字节

Sender MAC address：6字节 Sender IP Address：4字节

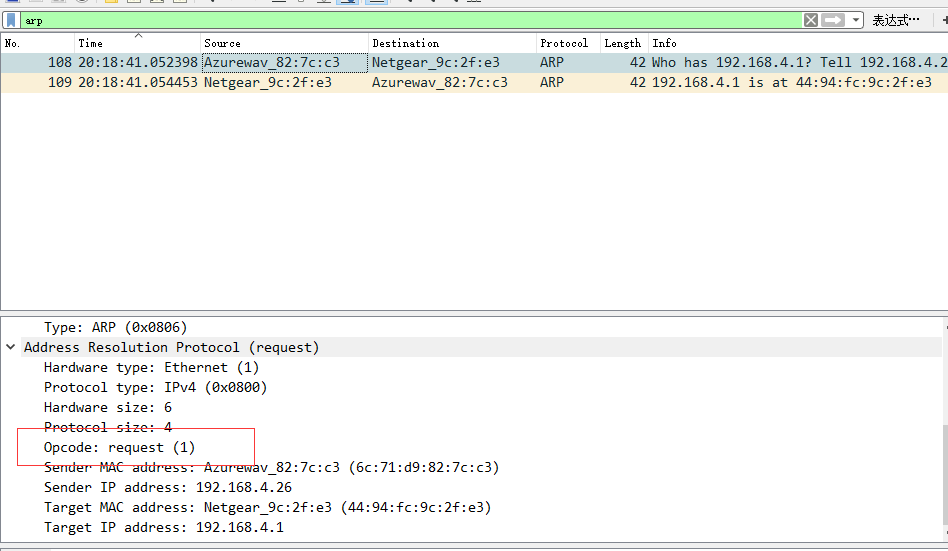
Target MAC Address：6字节 Target IP Address：4字节

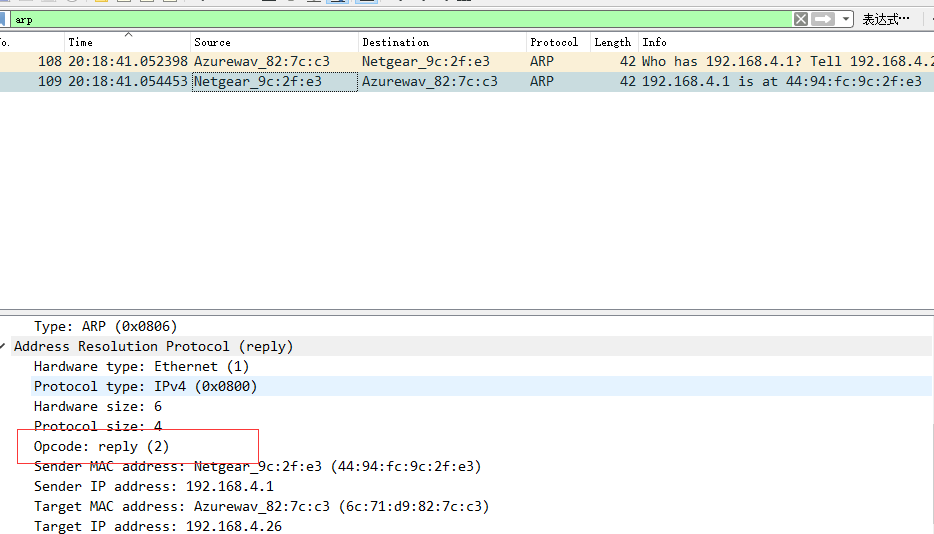




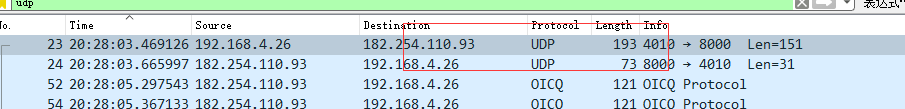
1. 判断ARP是请求和应答包：

如图所示，Opcode:request()中的值是1则是请求，是2则是应答

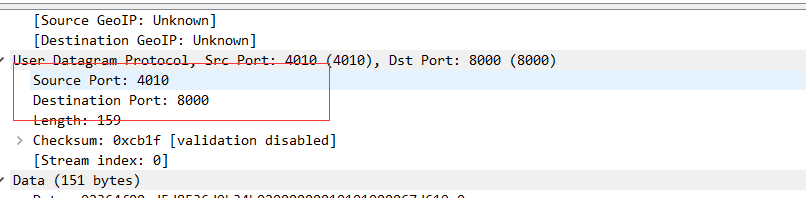




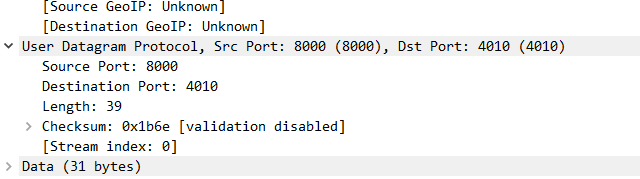
* + 1. 因为ARP进行查询工作时，主机并不知道哪个主机知道目的MAC地址，所以要通过广播的形式，向局域网中所有节点进行查询；但ARP响应时已经知道源MAC地址（就是发送广播帧的节点），所以要在一个有着明确目的局域网地址的帧中传送。
  1. **UDP数据包**



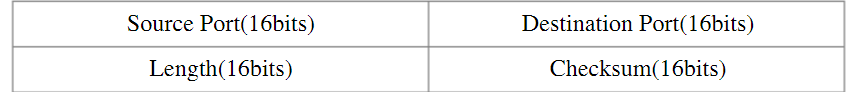
* + 1. 消息是基于UDP
    2. 主机IP是192.168.4.26目的IP地址 182.254.110.93
    3. 主机发送QQ消息的端口号是4010，QQ服务器的端口号是8000



* + 1. 数据报的格式：如图所示

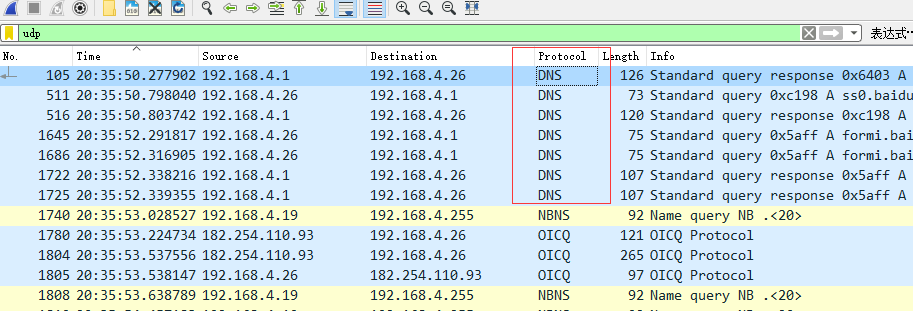


分别占字节数：

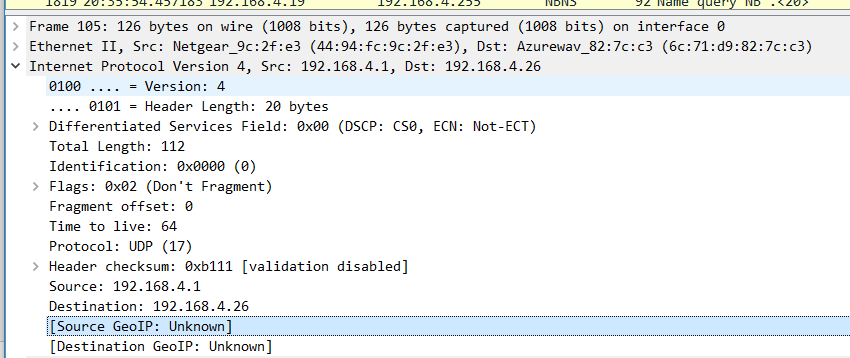


* + 1. 因为服务器要返回接收的结果发送给给客户端。 可以看出UDP的不可靠数据传输，因为只提供了⼀一次返回的基本ACK，没有保证数据一定能够被准确无误地送达。而且我们可以看到UDP数据包是没有序列号的，因此不能像TCP协议那样先进行握⼿，然后在发送数据，同时又发送ACK消息。
  1. **DNS协议分析**

打开[www.baidu.com](http://www.baidu.com)显示结果



报文详细：



1. **实验心得**

通过本次实验，熟悉了Wireshark的基本操作，了解对HTTP,TCP,IP,UDP,ARP,DNE各种协议的分析，验证了课程中所教授的课程知识，对协议中的报文的格式有了更深的认识，对其各个部分的作用有了一定的了解。对网络中，各个协议的工作方式，能够通过wirdshark进行分析，并得到各种报文的格式。深入理解了报文在网络中发送接受及转发的过程。对IPv4分组发送有了实践的检验，深入了解分片的过程。此次实验综合所学的协议，加深了对协议的认识。