哈爾濱工業大學
Harbin Institute of Technology

计算机网络
课程实验报告

实验名称	利用 Wireshark 进行协议分析				
姓名	石翔宇		院系	计算学部	
班级	1903103		学号	1190200523	
任课教师	刘亚维		指导教师	刘亚维	
实验地点	格物 207		实验时间	2021.11.21	
实验课表现	出勤、表现得分(10)		实验报告得分(40)		实验总分	
	操作结果得分(50)				
教师评语					

计算机科学与技术学院 SINCE 1956...
School of Computer Science and Technology

实验目的：

熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间进行交互以及报文交换的情况。

实验内容：

1) 学习 Wireshark 的使用
2) 利用 Wireshark 分析 HTTP 协议
3) 利用 Wireshark 分析 TCP 协议
4) 利用 Wireshark 分析 IP 协议
5) 利用 Wireshark 分析 Ethernet 数据帧

选做内容：

a) 利用 Wireshark 分析 DNS 协议
b) 利用 Wireshark 分析 UDP 协议
c) 利用 Wireshark 分析 ARP 协议

实验过程：

（一）Wireshark的使用

1. 选择无线网卡WLAN进行分组捕获，访问http://www.hit.edu.cn/ ；
2. 在完整的页面加载完成后，结束分组捕获。

（二）HTTP分析

1）HTTP GET/response 交互

1. 在Wireshark窗口的显示过滤说明处输入“http”，分组列表子窗口中将只显示所捕获到的HTTP报文；
2. 开始Wireshark分组捕获；
3. 访问http://news.hit.edu.cn/，在加载完全部页面后停止分组捕获。

2）HTTP 条件 GET/response 交互

1. 启动浏览器，清空浏览器的缓存；
2. 启动Wireshark分组捕获，访问http://news.hit.edu.cn/ ，在加载完全部页面后，重新刷新页面；
3. 停止Wireshark分组捕获，在显示过滤筛选说明处输入“http”，分组列表子窗口中将只显示所俘获到的HTTP报文。

（三）TCP分析

1. 访问http://gaia.cs.umass.edu/wireshark-labs/alice.txt ，得到ALICE'S ADVENTURES IN WONDERLAND文本，将该文件保存到主机上；
2. 打开 http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html ，选择好本地alice.txt文件的位置，开始Wireshark分组捕获后，点击“Upload alice.txt file”按钮，将文件上传到gaia.cs.umass.edu服务器；
3. 停止Wireshark分组捕获；
4. 在显示筛选规则中输入“tcp”，进行分析。

（四）IP分析

1. 启动Wireshark开始分组捕获；

2. 启动 pingplotter 并“Address to Trace Window”域中输入目的地址。在“# of times to Trace”域中输入“3”，这样就不过采集过多的数据。Edit->Options->Packet，将Packet Size(in bytes,default=56)域设为56，这样将发送一系列大小为56字节的包。然后按下“Trace”按钮。
3. Edit->Options->Packet，然后将Packet Size(in bytes,default=56)域改为2000，这样将发送一系列大小为 2000 字节的包。然后按下“Resume”按钮；
4. 最后，将 Packet Size(in bytes,default=56)域改为3500，发送一系列大小为3500字节的包。然后按下“Resume”按钮；
5. 停止 Wireshark 的分组捕获。

（五）抓取ARP数据包

1. 利用命令arp查看主机上ARP缓存的内容；
2. 启动Wireshark开始分组俘获，在命令行模式下输入：ping 172.20.113.111；
3. 停止Wireshark捕获。

（六）抓取UDP数据包

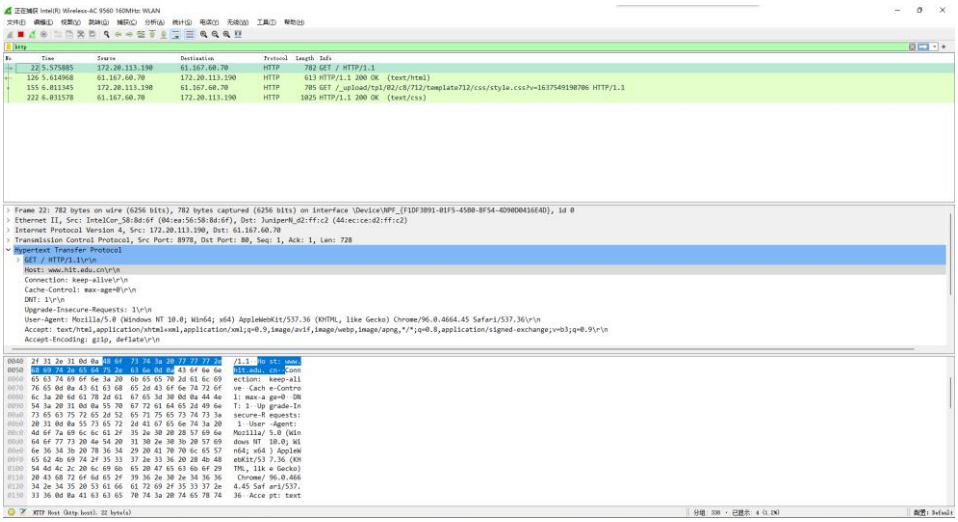
1. 启动Wireshark，开始分组捕获；
2. 发送QQ消息给好友；
3. 停止Wireshark 组捕获；
4. 在显示筛选规则中输入“udp”并展开数据包的细节。

（七）利用WireShark进行DNS协议分析

1. 在浏览器中访问www.baidu.com ；
2. 打开Wireshark，启动抓包。在控制台回车执行完毕后停止抓包。

实验结果：

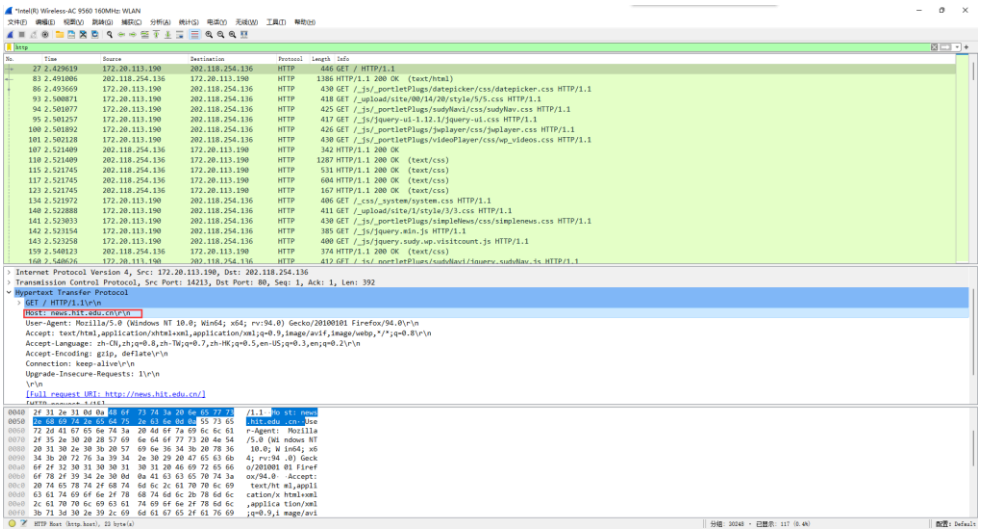
（一）Wireshark的使用



访问http://www.hit.edu.cn/，可以看到经过过滤后的第一条HTTP报文即为发向http://www.hit.edu.cn/服务器的HTTP GET报文。

（二）HTTP分析

1）HTTP GET/response交互



访问http://news.hit.edu.cn/分组捕获结果如上。第一条报文即是HTTP GET，第二条则是服务器返回的response。

思考问题：

1. 你的浏览器运行的是HTTP1.0，还是HTTP1.1？你所访问的服务器所运行HTTP协议的版本号是多少？

   浏览器运行的是HTTP1.1；访问的服务器运行的HTTP协议版本号为HTTP/1.1。

2. 你的浏览器向服务器指出它能接收何种语言版本的对象？

   Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

3. 你的计算机的IP地址是多少？服务器http://news.hit.edu.cn/ 的IP地址是多少？

   本机IP地址：172.20.113.190；服务器的IP地址：202.118.254.136。

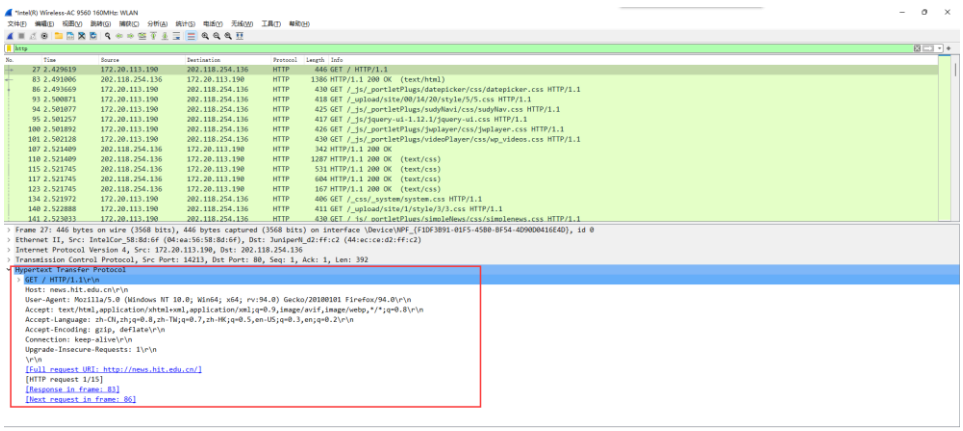
4. 从服务器向你的浏览器返回的状态代码是多少？

   返回的状态码为200。

2）HTTP条件GET/response交互

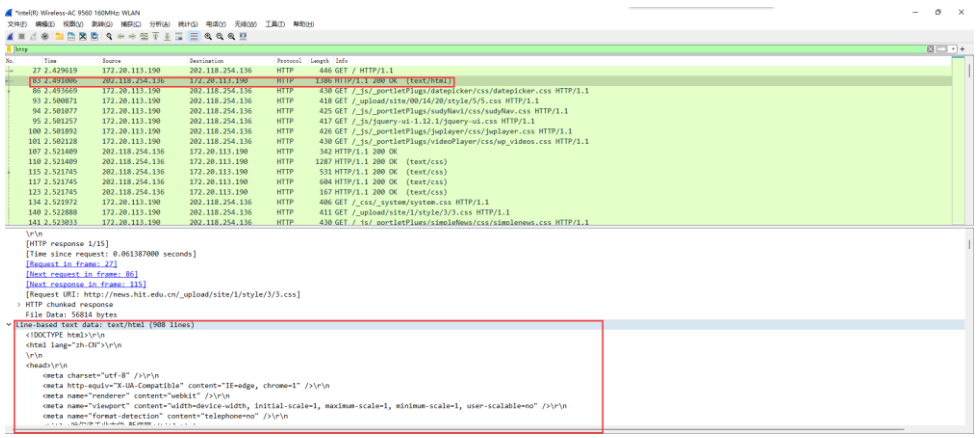
思考问题：

1. 分析你的浏览器向服务器发出的第一个HTTP GET请求的内容，在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？



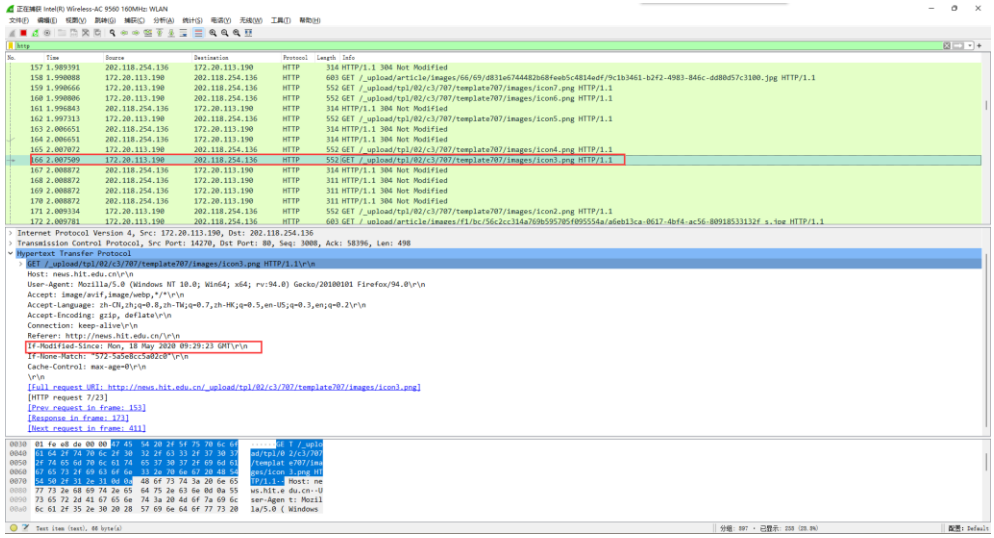
   向服务器发出的第一个HTTP GET请求中没有IF-MODIFIED-SINCE。

2. 分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？



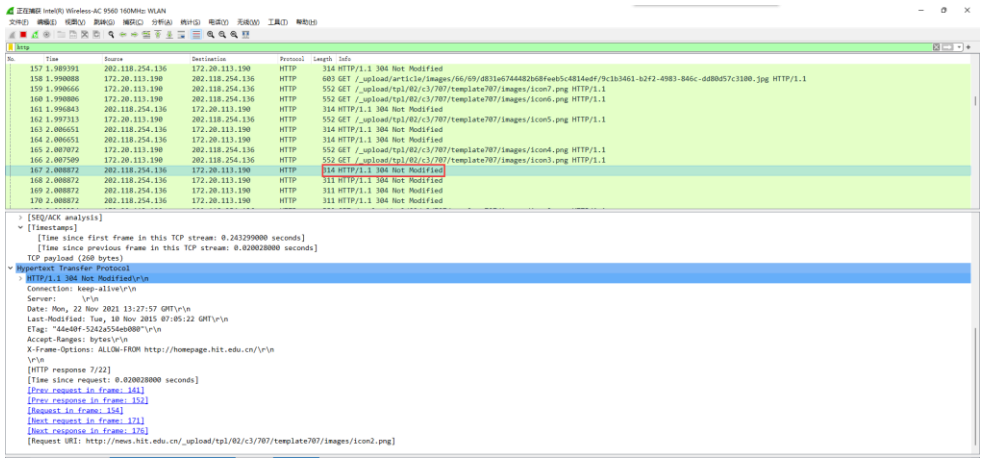
由图中红框中的内容可以看出，服务器明确返回了文件的内容。

3. 分析你的浏览器向服务器发出的较晚的“HTTP GET”请求，在该请求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？



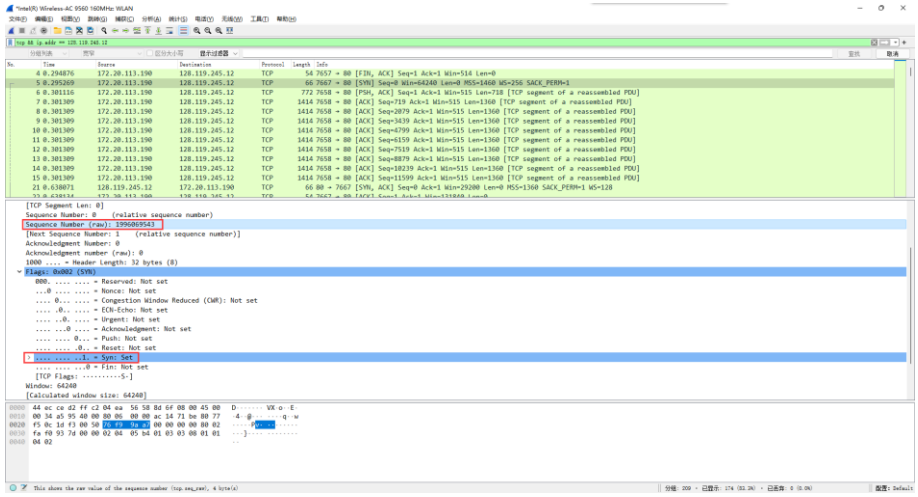
请求报文中有一行是IF-MODIFIED-SINCE；信息为缓存文件上次修改的时间。

4. 服务器对较晚的HTTP GET请求的响应中的HTTP状态代码是多少？服务器是否明确返回了文件的内容？请解释。



服务器对于较晚的HTTP GET请求会的的状态代码为304；由上图可以得知最近请求服务器回复消息的长度仅有314字节，远远小于之前回复信息的长度，从而服务器未明确返回文件的内容。

（三）TCP分析

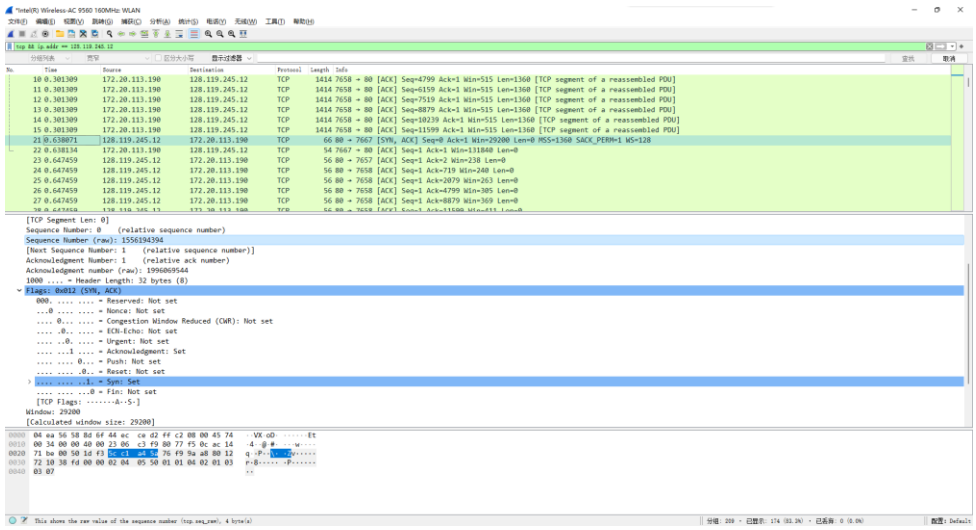


思考问题：

1. 客户服务器之间用于初始化TCP连接的TCP SYN报文段的序号（sequence number）是多少？在该报文段中，是用什么来标示该报文段是 SYN 报文段的？

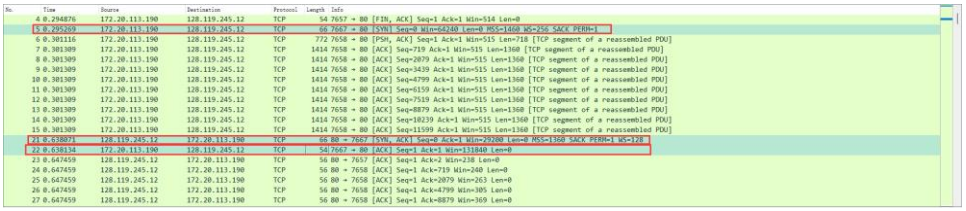
   初始化TCP连接的TCP SYN报文段的序号是1996069543；将SYN标志位设置为1来标示。

2. 服务器向客户端发送的SYNACK报文段序号是多少？该报文段中，Acknowledgement字段的值是多少？Gaia.cs.umass.edu服务器是如何决定此值的？在该报文段中，是用什么来标示该报文段是SYNACK报文段的？



服务器向客户端发送的SYNACK报文段序号是1556194394；Acknowledgement字段的值是1996069544；服务器通过SYN请求报文段的序号加1确定的；使用Flags部分的Ack和SYN标志位置为1来标示该报文段是SYNACK报文段。

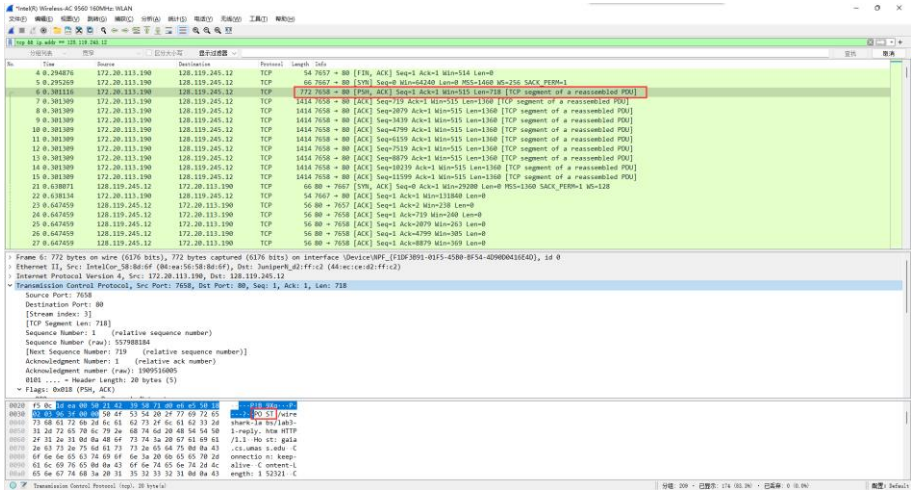
3. 你能从捕获的数据包中分析出tcp三次握手过程吗？



上图三个红框部分就是tcp三次握手过程。分别是客户机向服务器端发送SYN请求报文、

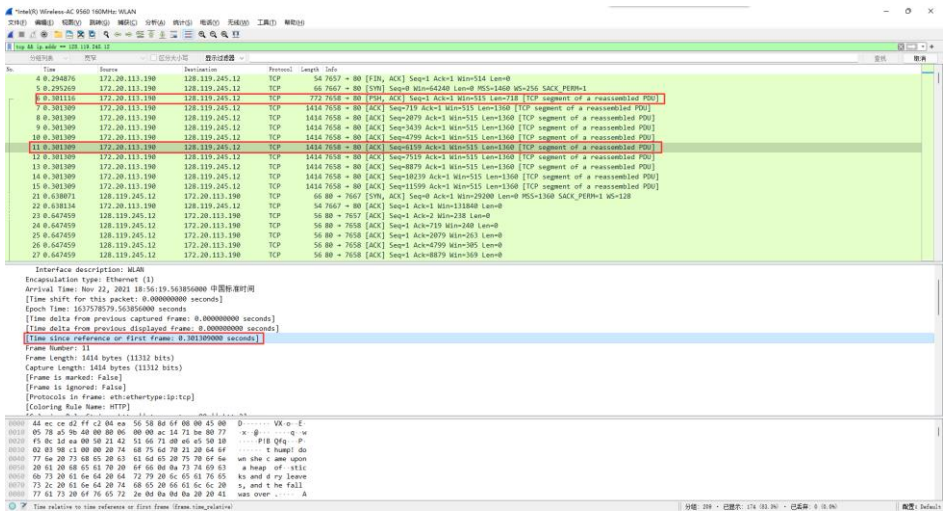
服务器向客户机回复SYNACK报文以及客户机向服务器回复Ack报文段。

4. 包含HTTP POST命令的TCP报文段的序号是多少？

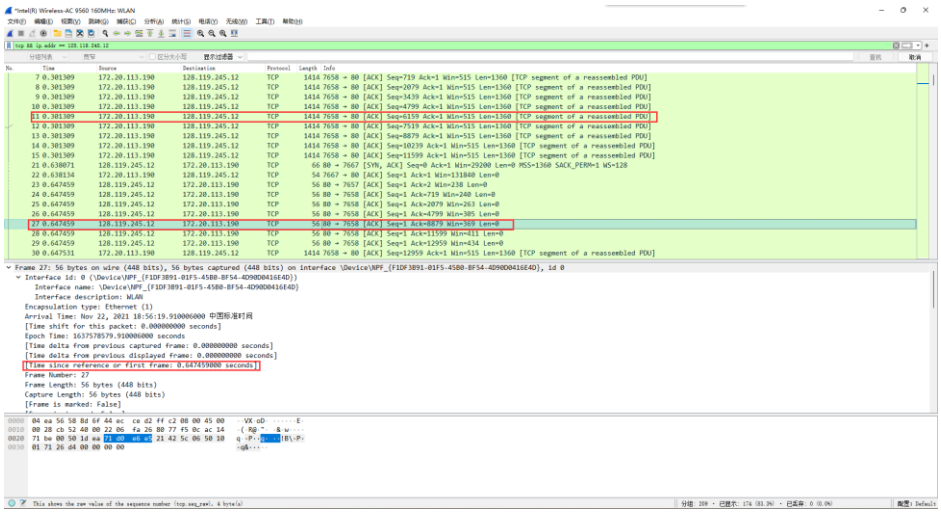


包含HTTP POST命令的TCP报文段的序号是1。

5. 如果将包含HTTP POST命令的TCP报文段看作是 TCP 连接上的第一个报文段，那么该TCP连接上的第六个报文段的序号是多少？是何时发送的？该报文段所对应的ACK是何时接收的？

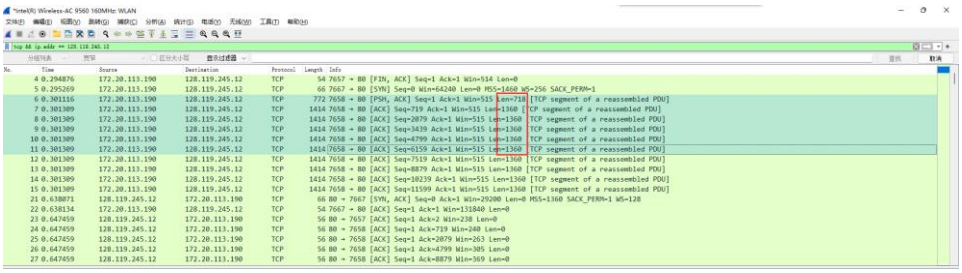


TCP连接上的第六个报文段的序号是557994342（第一个为557988184）；在第一个发送后0.3013秒发送。



该报文段所对应的ACK是在第一个发送后0.6475秒接收的。

6. 前六个TCP报文段的长度各是多少？



第一个报文段长度为718，其余五个均为1360。

7. 在整个跟踪过程中，接收端公示的最小的可用缓存空间是多少？限制发送端的传输以后，接收端的缓存是否仍然不够用？

接收端公示最小可用的缓存空间为515；没有出现限制发送端发送的情况。

8. 在跟踪文件中是否有重传的报文段？进行判断的依据是什么？

没有重传的片段；依据为发送端的报文段序号始终在增加，没有出现重复发送某一个序号的报文段的情况。

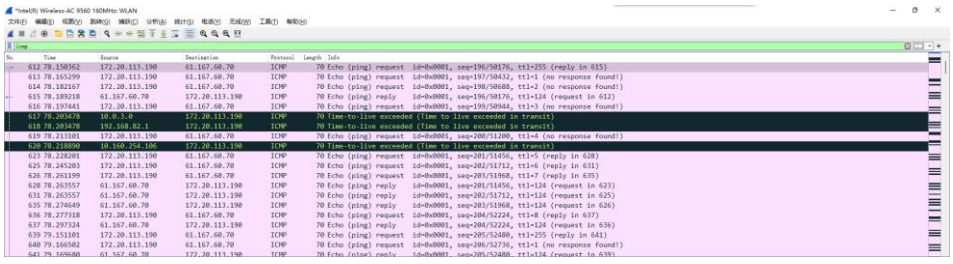
9. TCP 连接的throughput (bytes transferred per unit time)是多少？请写出你的计算过程。

184 1.702177 128.119.245.12 172.20.113.190 TCP 56 80 → 7658 [ACK] Seq=1 Ack=153040 Win=1485 Len=0

计算公式为：

$$\text{Throughput} = \frac{153040 * 8\ bits}{1.70 - 0.30s} = 0.82\ Mbps$$

（四）IP分析

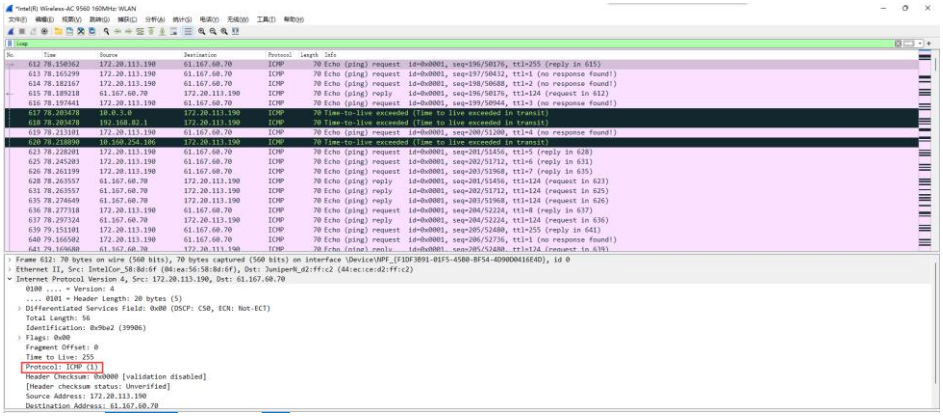


思考问题：

1. 你主机的IP地址是什么？

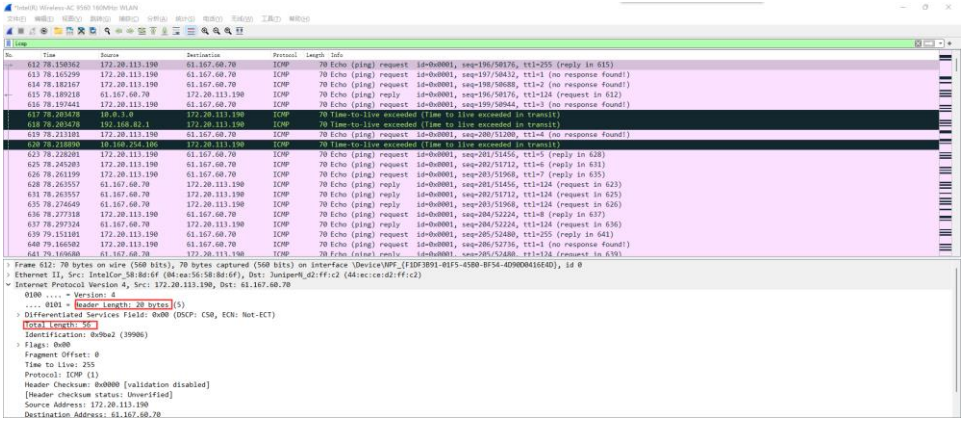
   本机IP地址为172.20.113.190。

2. 在IP数据包头中，上层协议（upper layer）字段的值是什么？



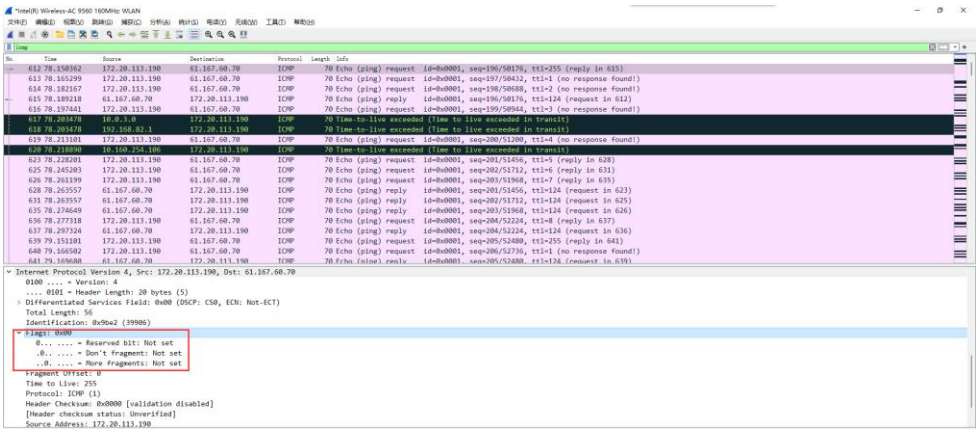
   上层协议字段的值是ICMP (1)。

3. IP头有多少字节？该IP数据包的净载为多少字节？并解释你是怎样确定该IP数据包的净载大小的？



   由上图红框部分得知，IP头有20字节；IP数据包的净载为$56-20=36$字节。

4. 该IP数据包分片了吗？解释你是如何确定该IP数据包是否进行了分片。



   由上图画红框Flags部分得知，IP数据包没有分片。

5. 你主机发出的一系列ICMP消息中IP数据报中哪些字段总是发生改变？

IP数据报中TTL、Checksum和Sequence Number总是发生改变。

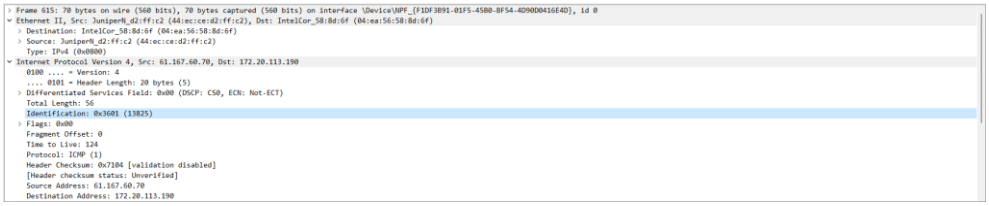
6. 哪些字段必须保持常量？哪些字段必须改变？为什么？

   版本号、首部长度、区分服务以及协议必须保持常量；TTL、Checksum和Sequence Number必须改变；TTL每次转发必然改变，由于TTL改变，Checksum也会改变，Sequence Number区分不同的ICMP报文也会改变。

7. 描述你看到的IP数据包Identification字段值的形式。

   Identification字段值为2个字节，从前向后依次递增。

8. Identification字段和TTL字段的值是什么？

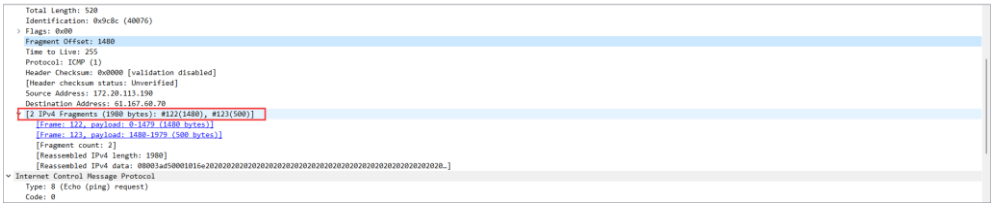


Identification字段为0x3601，TTL字段为124。

9. 最近的路由器（第一跳）返回给你主机的ICMP Time-to-live exceeded消息中这些值是否保持不变？为什么？

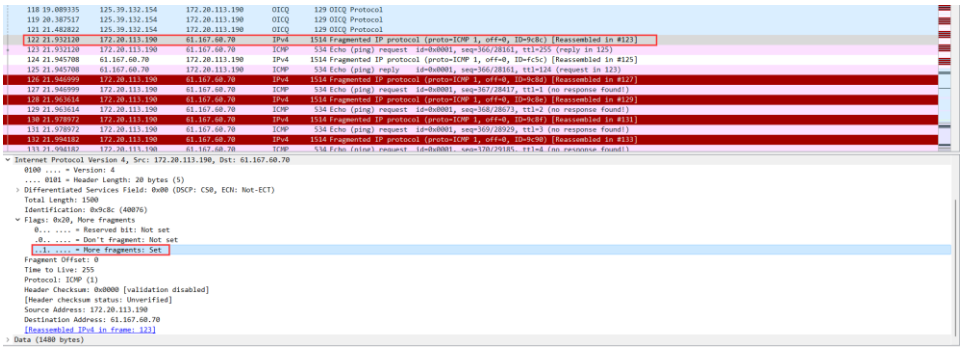
   Identification字段变化，用来区分不同的ICMP消息；TTL保持不变，均进行了一次转发。

10. 该消息是否被分解成不止一个IP数据报？



由上图画红框部分可看出消息被分成2个数据报。

11. 观察第一个IP分片，IP头部的哪些信息表明数据包被进行了分片？IP头部的哪些信息表明数据包是第一个而不是最后一个分片？该分片的长度是多少？



IP头部的Flags中More fragments表明数据包被进行了分片，同时数据包是第一个而不是最后一个分片；长度为1500。

12. 原始数据包被分成了多少片？

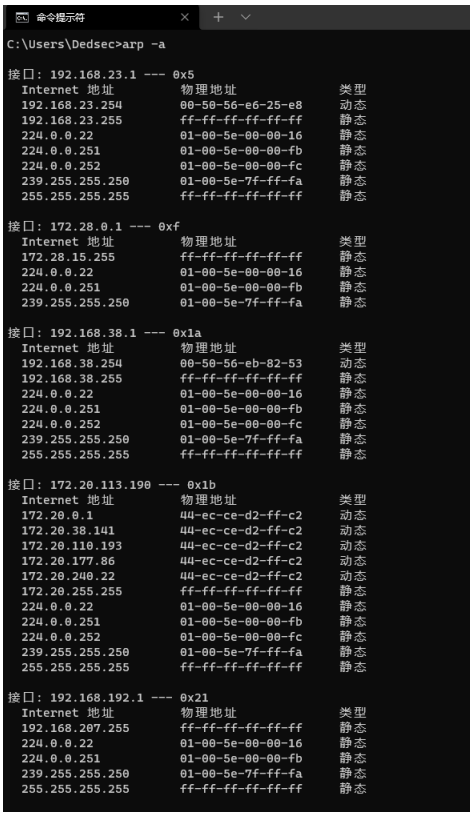
由上图画红框部分可以看出原始数据包被分成了三片。

13. 这些分片中IP数据报头部哪些字段发生了变化？

标志位字段部分和Checksum字段部分发生了变化。

（五）抓取ARP数据包

利用命令arp查看主机上ARP 缓存的内容如下：



思考问题：

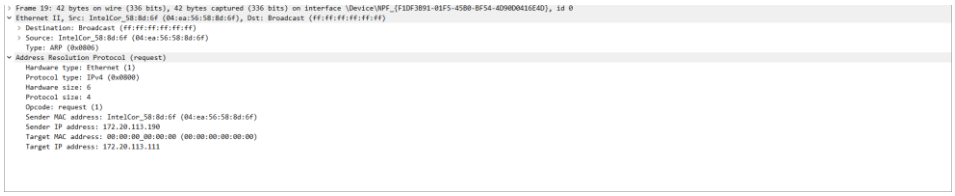
1. 说明ARP缓存中每一列的含义是什么?

每一列的含义均由其表头表示，上图中含义分别为Internet 地址、物理地址和类型。

2. ARP数据包的格式是怎样的？由几部分构成，各个部分所占的字节数是多少？

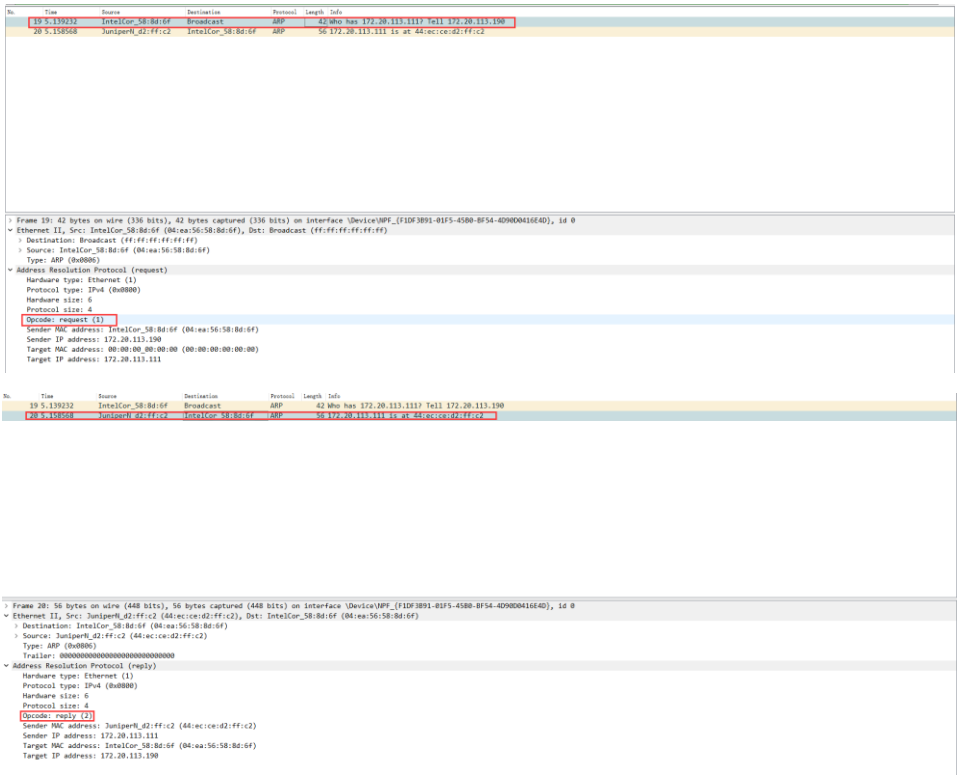
ARP数据包的格式如下图所示；总共有9部分组成，各个部分所占的字节数如下图所示。

实验中ARP数据包内容如下。



3. 如何判断一个ARP数据是请求包还是应答包？

判断Opcode部分，当其值为1时为请求，2时为应答，如下面两张图所示：

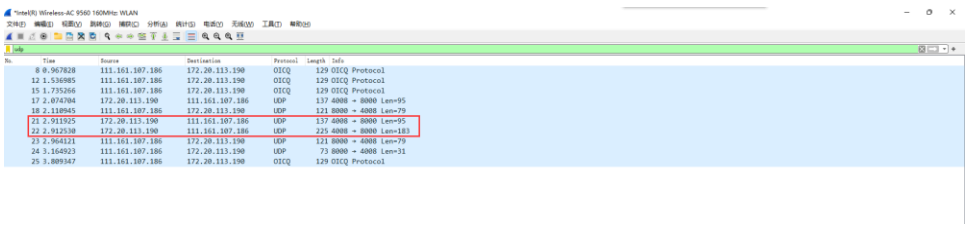


4. 为什么ARP查询要在广播帧中传送，而ARP响应要在一个有着明确目的局域网地址的帧中传送？

由于查询方不知道被查询方的MAC地址（这也正是为何要进行ARP查询的原因），而所有结点都要处理广播帧，因此通过广播发送给被查询方。而被查询方通过接收到的广播帧的源地址知道查询方的MAC地址了，因此可以用该地址进行响应，这样局域网中的除查询方外其它主机就不会接收和处理该ARP响应了，避免浪费带宽和其它主机的计算资源。

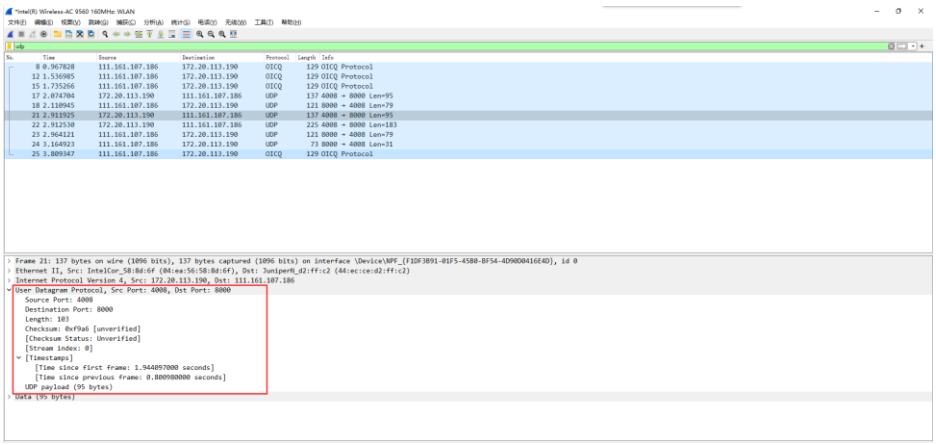
（六）抓取UDP数据包

UDP数据包如下：



思考问题：

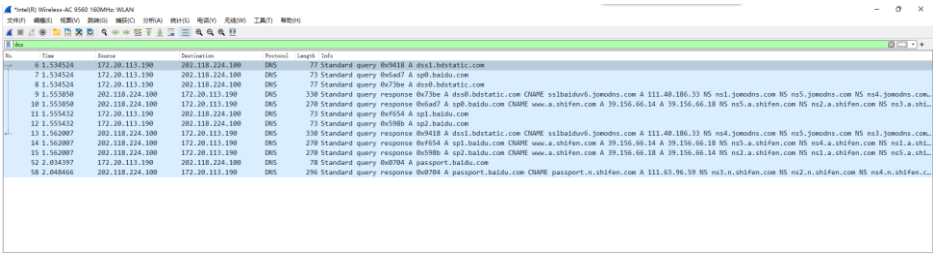
1. 消息是基于UDP的还是TCP的？
   消息是基于UDP的。
2. 你的主机ip地址是什么？目的主机ip地址是什么？
   主机ip地址是172.20.113.190；目的主机ip地址是111.161.107.186。
3. 你的主机发送QQ消息的端口号和QQ服务器的端口号分别是多少？
   主机发送QQ消息的端口号是4008；QQ服务器的端口号是8000。
4. 数据报的格式是什么样的？都包含哪些字段，分别占多少字节？



   数据报的格式如上图所示；包含源端口号、目的端口号、长度和Checksum；各占2个字节。
5. 为什么你发送一个ICQ数据包后，服务器又返回给你的主机一个ICQ数据包？这UDP的不可靠数据传输有什么联系？对比前面的TCP协议分析，你能看出UDP是无连接的吗？
   因为UDP是不可靠的数据传输，需要ICQ实现可靠数据传输；发送数据之前没有连接的建立过程，UDP是无连接的。

（七）利用WireShark进行DNS协议分析

DNS抓包结果如下：



可以看到DNS服务器为202.118.224.100。

经IP地址查询这是哈工大的DNS服务器。

问题讨论：

（二）HTTP分析中的思考问题
（三）TCP分析中的思考问题
（四）IP分析中的思考问题
（五）抓取ARP数据包中的思考问题
（六）抓取UDP数据包中的思考问题

心得体会：

此次实验中，通过利用WireShark工具，各种网络协议进行了深入的跟踪与分析，更加深入地了解了每层的功能和不同协议的报文格式，加深了对于各种协议交互过程的理解，同时也增加了对计算机网络研究的兴趣。