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	郑旭然		院系	软件工程	
班级	2037102		学号	120L020719	
任课教师	李全龙		指导教师	李全龙	
实验地点	格物楼 207		实验时间	2022.10.24	
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
6) 利用 Wireshark 分析 DNS 协议
7) 利用 Wireshark 分析 UDP 协议
8) 利用 Wireshark 分析 ARP 协议

实验过程：

1) 利用 Wireshark 分析 HTTP 协议

按照实验指导书上流程进行操作：

启动 Web browser，然后启动 Wireshark 分组嗅探器。在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俘获到的HTTP 报文。

开始 Wireshark 分组俘获。

在打开的Web browser窗口中输入以下地址: http://hitgs.hit.edu.cn/。

停止分组俘获。

启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单中的“Internet 选项”命令，在出现的对话框中，选择“删除文件”）。

启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。

在浏览器的地址栏中输入以下 URL: http://hitgs.hit.edu.cn/ ,在你的浏览器中重新输入相同的 URL 或单击浏览器中的“刷新”按钮。

停止 Wireshark 分组俘获，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。

实验结果见下一节。

2) 利用 Wireshark 分析 TCP 协议

A. 俘获大量的由本地主机到远程服务器的 TCP 分组

（1） 启动浏览器，打开 http://gaia.cs.umass.edu/wireshark-labs/alice.txt 网页，得到ALICE'S ADVENTURES IN WONDERLAND文本，将该文件保存到你的主机上。

（2）打开http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html ，在 Browse 按钮旁的文本框中输入保存在你的主机上的文件 ALICE'S ADVENTURES INWONDERLAND的全名（含路径），此时不要按“Upload alice.txt file”按钮。

（3） 启动Wireshark，开始分组俘获。

（4） 在浏览器中，单击“Upload alice.txt file”按钮，将文件上传到gaia.cs.umass.edu服务器，一旦文件上传完毕，一个简短的贺词信息将显示在你的浏览器窗口中。

（5） 停止俘获。

B. 浏览追踪信息

在显示筛选规则中输入“tcp”,可以看到在本地主机和服务器之间传输的一系列 tcp 和 http 报文，你应该能看到包含 SYN 报文的三次握手。也可以看到有主机向服务器发送的一个 HTTP POST 报文和一系列的“http continuation”报文。

C. TCP 基础

3) 利用 Wireshark 分析 IP 协议

A. 通过执行 traceroute 执行捕获数据包

（1）启动 Wireshark 并开始数据包捕获

（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。

B. 对捕获的数据包进行分析

（1）在你的捕获窗口中，应该能看到由你的主机发出的一系列ICMPEcho Request包 和中间路由器返回的一系列ICMP TTL-exceeded消息。选择第一个你的主机发出的ICMP Echo Request消息，在packet details窗口展开数据包的Internet Protocol部分。

C. 找到在将包大小改为3500字节后你的主机发送的第一个ICMP Echo Request消息

4) 抓取ARP数据包

（1）利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的 内容。

（2）在命令行模式下输入：ping 192.168.1.82（或其他 IP 地址）

（3）启动 Wireshark，开始分组俘获。

5) 抓取UDP数据包

（1）启动 Wireshark，开始分组捕获；

（2）发送 QQ 消息给你的好友；

（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。

6) 利用 Wireshark 进行 DNS 协议分析

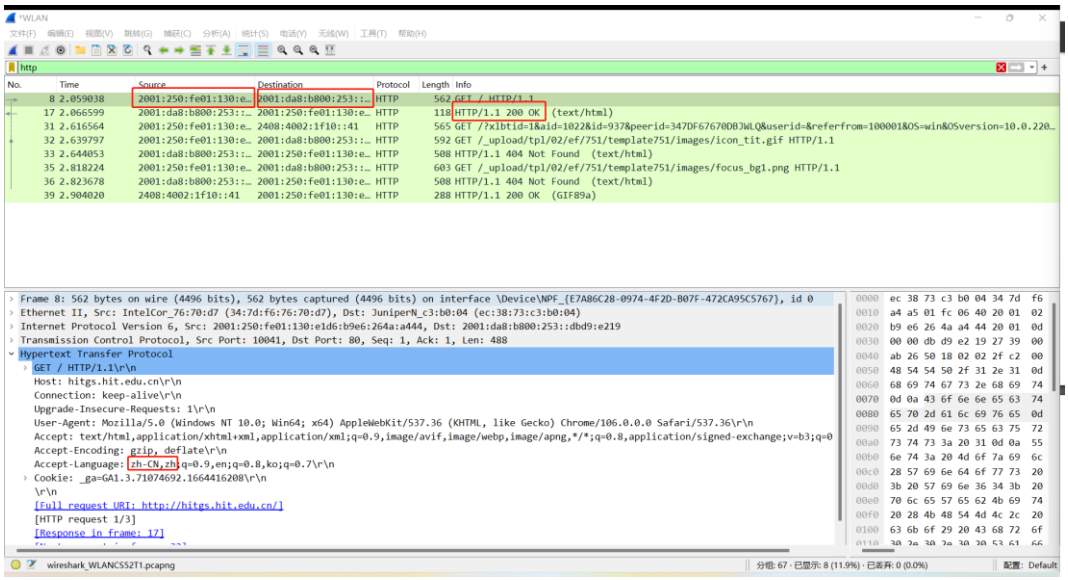
（1）打开浏览器键入:www.baidu.com。

（2）打开Wireshark，启动抓包。

（3）在控制台回车执行完毕后停止抓包。

实验结果：

1) 利用 Wireshark 分析 HTTP 协议



✧ 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？

HTTP 1.1

✧ 你的浏览器向服务器指出它能接收何种语言版本的对象？

zh-CN, zh

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

Source Address: 2001:250:fe01:130:e1d6:b9e6:264a:a444

Destination Address: 2001:da8:b800:253::dbd9:e219

✧ 从服务器向你的浏览器返回的状态代码是多少？

200 OK

✧ 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？

没有

✧ 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？

服务器明确返回了文件内容。返回的状态码是200，代表明确返回了文件；若返回状态码为404，不返回文件。

✧ 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？

有：Mon, 17 Oct 2022 09:15:49 GMT\r\n，为缓存最后更新的时间。

✧ 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。

304 Not Modified。服务器不会明确返回文件内容，因为服务器判断为 Not Modified，客户端可以使用本地仍为最新版本的缓存。

2) 利用 Wireshark 分析 TCP 协议

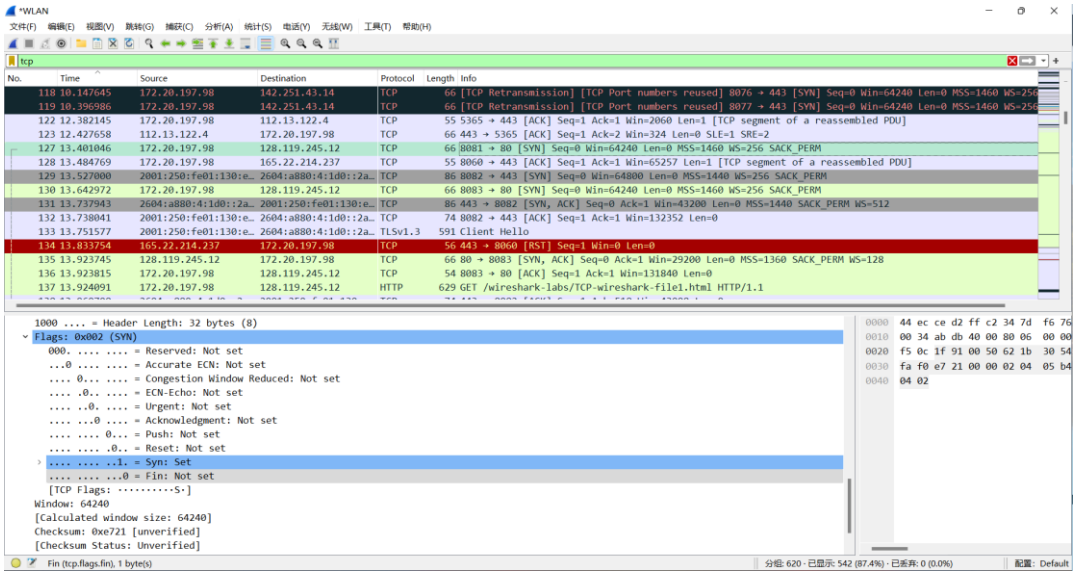
✧ 向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址和TCP 端

口号是多少？

客户端主机的 IP 地址：172.20.197.98，TCP 端口号：8081

✧ Gaia.cs.umass.edu 服务器的 IP 地址是多少？对这一连接，它用来发送和接收 TCP 报文的端口号是多少？

服务器的 IP 地址：128.119.245.12，用来收发 TCP 报文的端口号：80



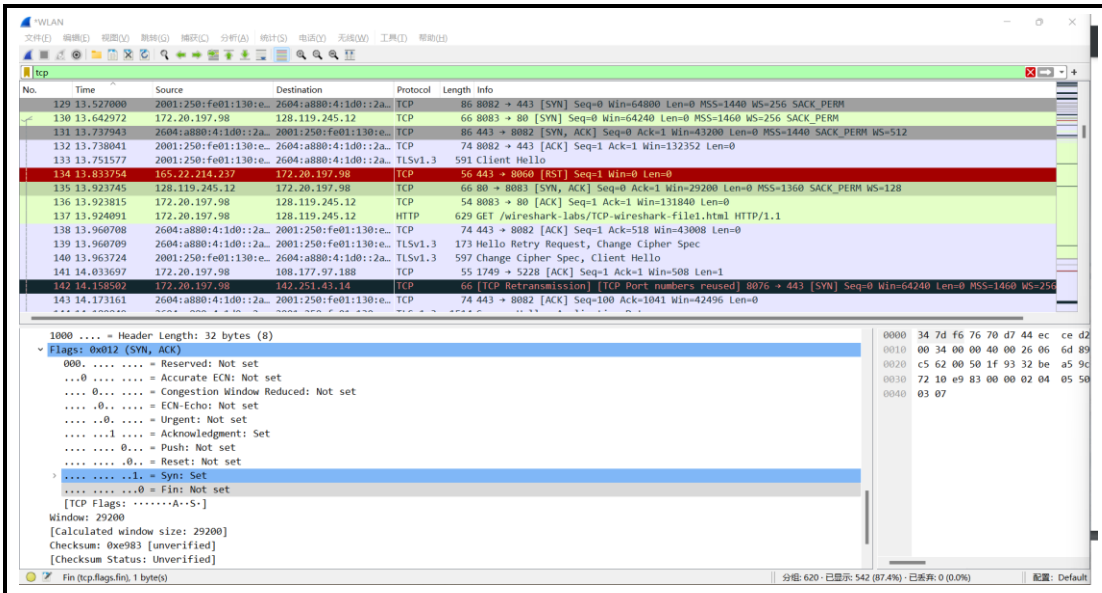
✧ 客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号（sequence number）是多少？在该报文段中，是用什么来标示该报文段是 SYN 报文段的？

初始化tcp连接的tcp syn报文段的序号为0（随机值）；该报文段将SYN标志位置为1，表示该报文段为SYN段用于tcp建立连接。

✧ 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？

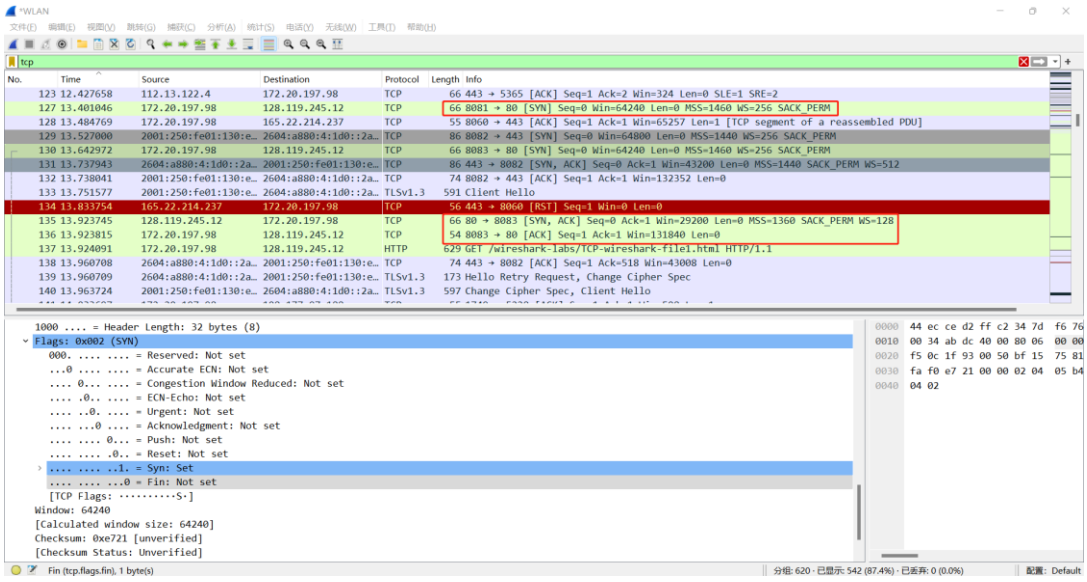
SYNACK 报文段序号是0；Acknowledgement 字段的值是1；

Gaia.cs.umass.edu 服务器根据上一次客户端发给服务器的 seq+1 得到该字段；在该报文段中，通过Flags位中SYN与ACK均为1来标示该报文段是SYNACK。



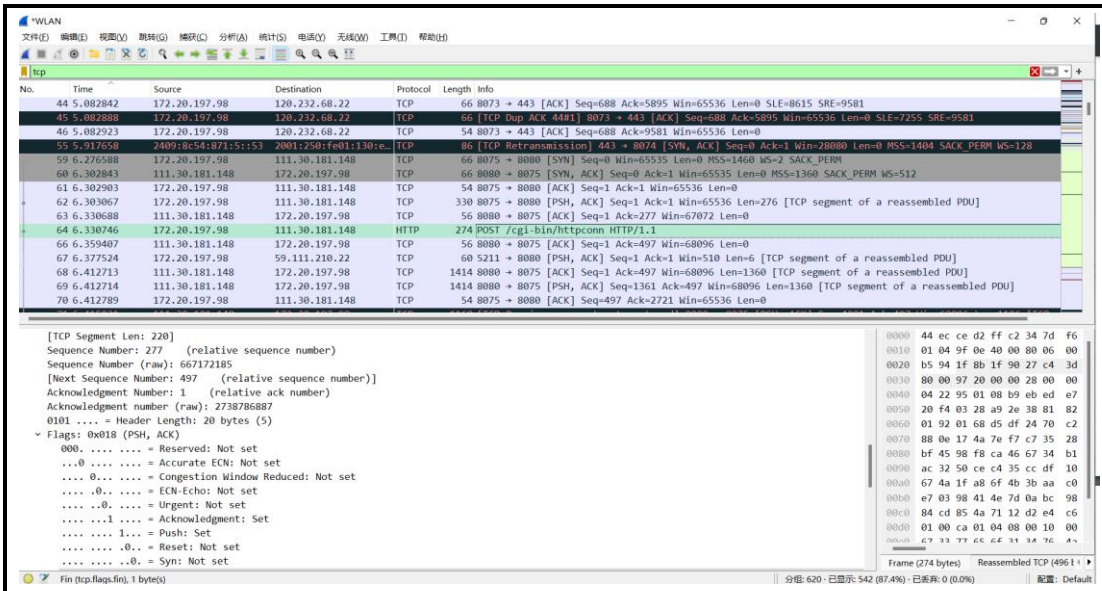
✧ 你能从捕获的数据包中分析出tcp三次握手过程吗？

客户端先向服务器发送一个seq = 0的建立连接请求，然后服务器向客户端返回seq = 0, ack = 1的响应,最后客户端seq=1,ack=1的确认报文，连接建立。



✧ 包含 HTTP POST 命令的 TCP 报文段的序号是多少？

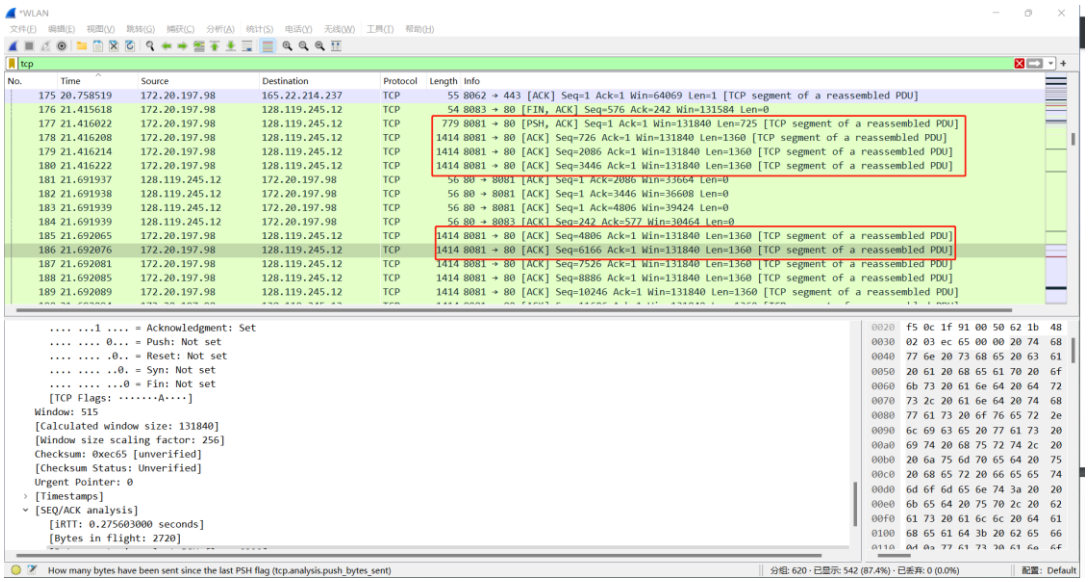
277.



✧ 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？

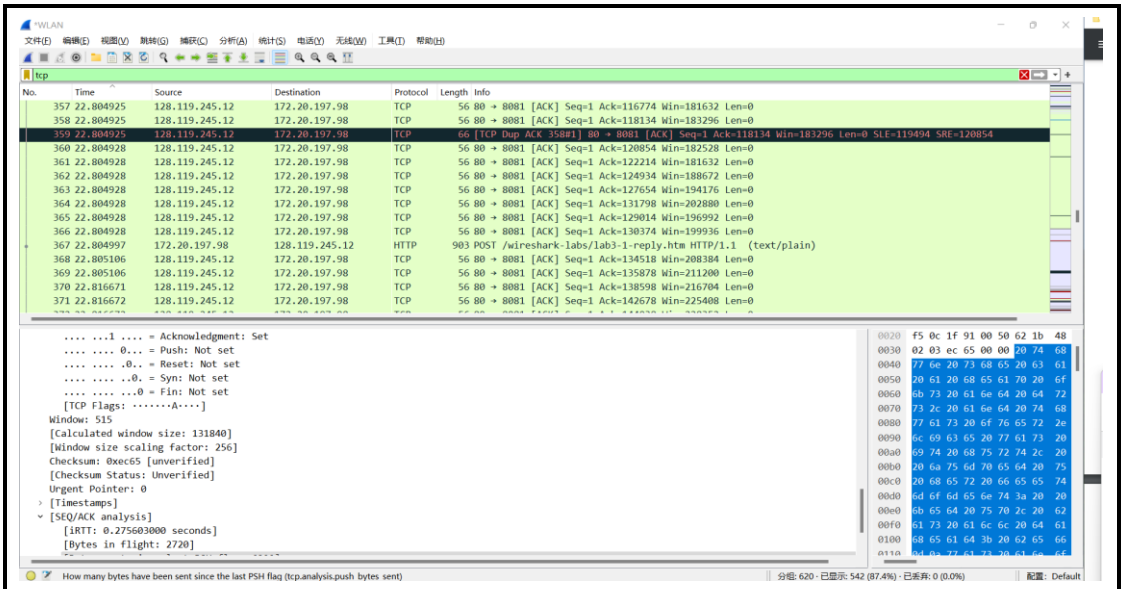
第六个报文段为23，在 HTTP POST 发送之前，TCP连接建立之后发送。对应的 ACK 即为服务器返回的第六个 ACK。

✧ 前六个 TCP 报文段的长度各是多少？



779,1414,1414,1414,1414,1414

✧ 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？

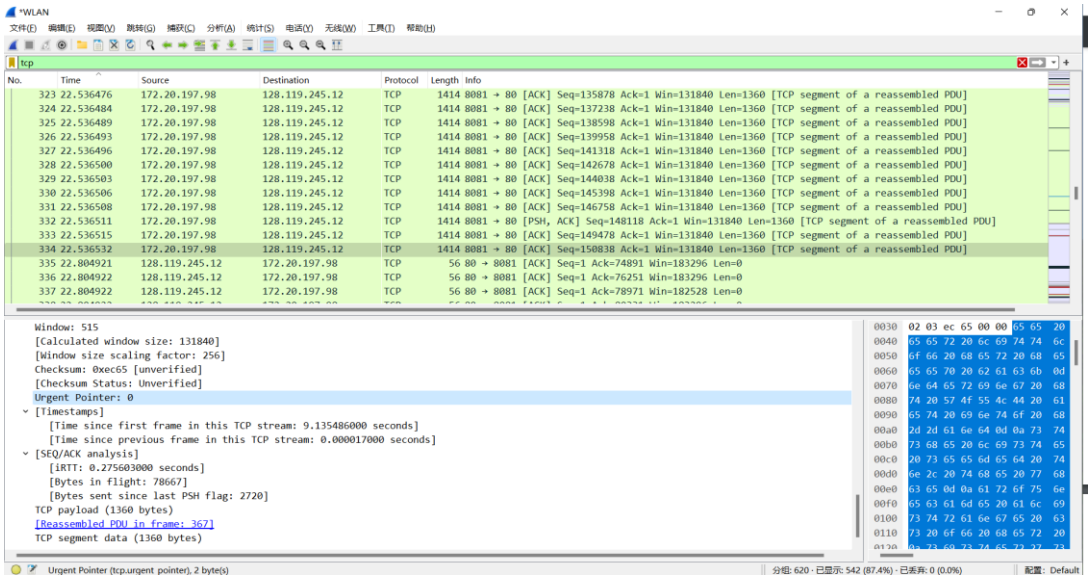


接收端公示的最小的可用缓存空间是131840，且窗口大小递增，缓存够用。

✧ 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？

没有出现重传，客户端发送的报文Seq没有出现重复的情况。

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



答： 发送数据总的长度为152198B + 108 * 54B = 158030B

发送时间共9.135486000s

因此吞吐量为158030B / 9.135486000s = 17298.4776 Bps.

3) 利用 Wireshark 分析 IP 协议

➢ 你主机的IP地址是什么？

172.20.230.140

➢ 在IP数据包头中，上层协议（upper layer）字段的值是什么？

01

```
Internet Protocol Version 4, Src: 172.20.77.246, Dst: 61.167.60.70
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 56
   Identification: 0x2d5c (11612)
 > Flags: 0x0000
   ...0 0000 0000 0000 = Fragment offset: 0
   Time to live: 255
   Protocol: ICMP (1)
   Header checksum: 0x1a71 [validation disabled]
   [Header checksum status: Unverified]
   Source: 172.20.77.246
   Destination: 61.167.60.70
Internet Control Message Protocol
```

- 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？

  如上图所示，IP头有20字节，数据报净载Total Length-Header Length=56B-20B = 36B.

- 该IP数据包分片了吗？解释你是如何确定该P数据包是否进行了分片？

```
Flags: 0x0000
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not set
   ..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
```

  未分片，offset=0，MF=0.

- 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？

  TTL、ID、Header Checksum

- 哪些字段必须保持常量？哪些字段必须改变？为什么？

  ID 区分不同的数据包，必须改变；TTL经过一个路由器后减一，必须改变；Header Checksum 由前面的部分计算而得，因此也必须改变；除此之外，其他字段如IP版本号等保持常量。

- 描述你看到的IP数据包Identification字段值的形式。

  16位，每次递增1。

- Identification字段和TTL字段的值是什么？

  Identification：0x0000　TTL：254

- 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？

  不变，对于Identification标识来说，相同的标识是为了分段后组装成同一段，不会变；它们都是由第一跳路由器返回的数据报，所以TTL也不变。

- （第一个ICMP Echo Request消息）该消息是否被分解成不止一个IP数据报？

  共分成2片。

- 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？

offset=0，MF=1，表示其为第一个分片，不是最后一个分片。分片长度为1500.

- 将包大小改为3500字节后，原始数据包被分成了多少片？

  3片。

- 这些分片中IP数据报头部哪些字段发生了变化？

  前两片MF均为1，而最后一片为0； 另外，第二片的 offset=1480，最后一片offset=2960。

4) 抓取ARP数据包

（1）利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的内容。说明 ARP 缓存中每一列的含义是什么?

```
C:\Users\zxr>arp -a

Interface: 172.20.230.140 --- 0x12
  Internet Address      Physical Address      Type
  169.254.169.254       44-ec-ce-d2-ff-c2     dynamic
  172.20.0.1            44-ec-ce-d2-ff-c2     dynamic
  172.20.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ARP缓存中每一列表示IP地址所对应的物理地址和类型（动态配置或静态配置）。

（2）清除主机上 ARP 缓存的内容,抓取 ping 命令时的数据包。分析数据包,回答下面的问题：

- 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？

共26字节，由9部分构成，依次是：硬件类型（2字节），协议类型（2字节），硬件地址长度（1字节），协议地址长度（1字节），OP（2字节），发送端MAC地址（6字节），发送端IP地址（4字节），目的MAC地址（6字节），目的IP地址（4字节）。

- 如何判断一个ARP数据是请求包还是应答包？

  通过OP字段查看。OP=1为请求包， OP=2时表明是应答包。

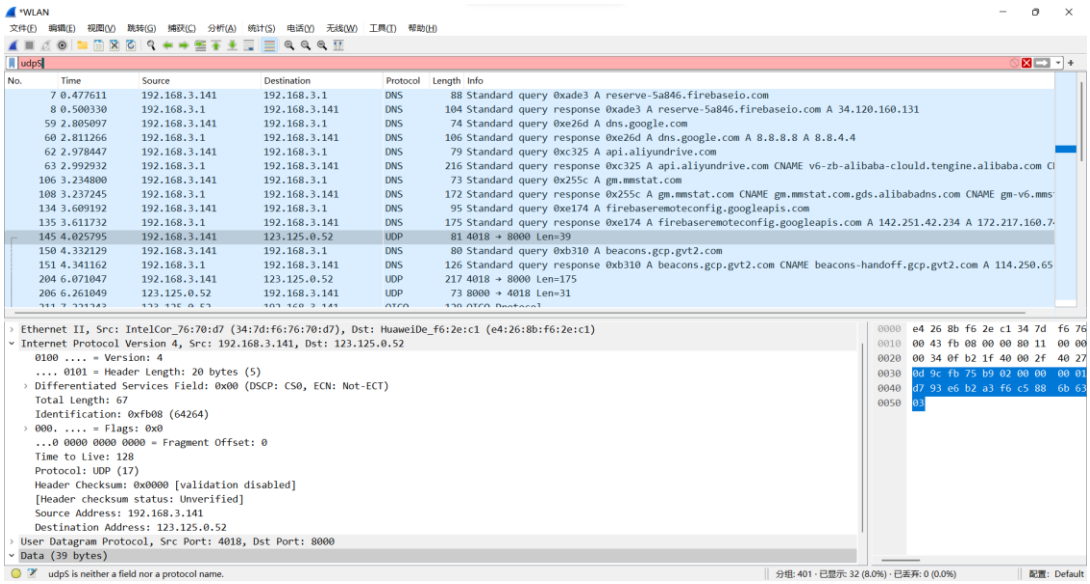
- 为什么ARP查询要在广播帧中传送，而ARP响应要在一个有着明确目的局域网地址的帧中传送？

ARP查询时，发送主机并不知道目的IP对应的MAC地址，所以需要进行广播查询。但ARP响应已经可以知道查询主机的MAC地址，因此ARP响应会在一个有着明确目的的局域网地址的帧中传送。

5) 抓取UDP数据包

- 消息是基于UDP的还是TCP的？

  基于UDP。



- 你的主机ip地址是什么？目的主机ip地址是什么？

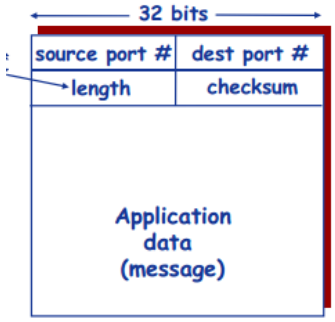
  主机IP：192.168.3.141（非校园网） 目的主机IP：123.125.0.52

- 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：4018，QQ服务器的端口号：8000

- 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？

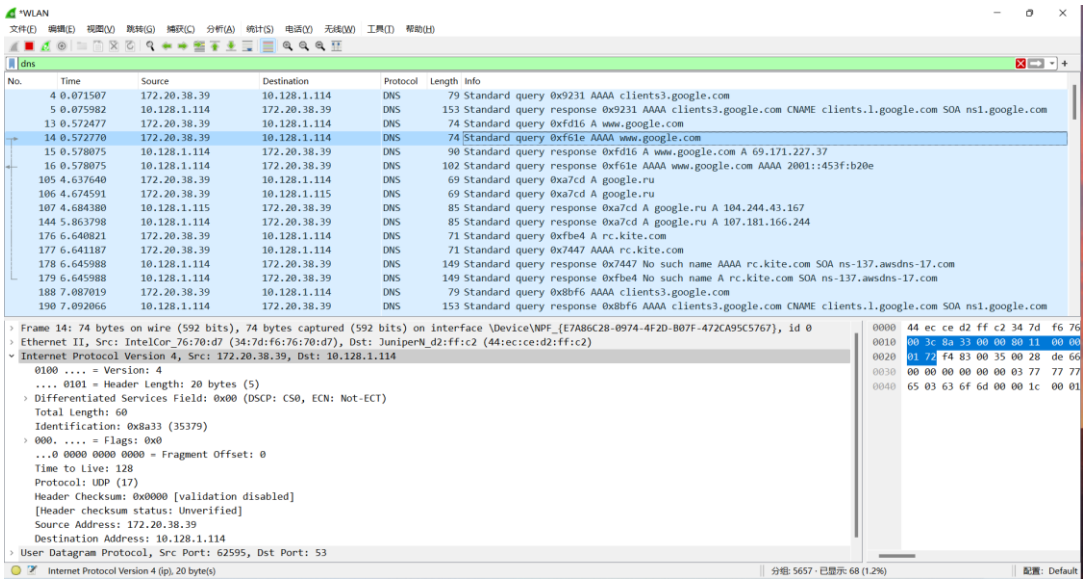
  UDP数据报格式如图所示：UDP数据报由5部分构成，分别是源端口号（4字节），目的端口号（4字节），长度（4字节），校验和（4字节）和其上附加的应用层数据。



- 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？

  发送端发送一个ICQ数据包，服务器需要返回一个接收结果给发送端。UDP也是类似，UDP是不可靠无连接的数据传输，仅返回一个接收状态，无重传；数据包没有序列号，因此是乱序无连接的。

6) 利用 WireShark 进行 DNS 协议分析



问题讨论：

见实验结果部分思考问题。

心得体会：

本次实验让我充分了解了网络中各种协议，学会了使用WireShark进行协议分析，深入理解了各个协议的实现，对计算机网络有了进一步的理解。