电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221302009

姓 名 陆圣珩

（实验） 课程名称 计算机网络

理论教师 刘梦娟

实验教师 刘梦娟

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陆圣珩 学号：2017221302009 指导教师：刘梦娟**

**实验地点：信软楼西303 实验时间：2019.4.26**

**一、实验名称：运输层协议验证实验**

**二、实验学时：2学时**

**三、实验目的：**

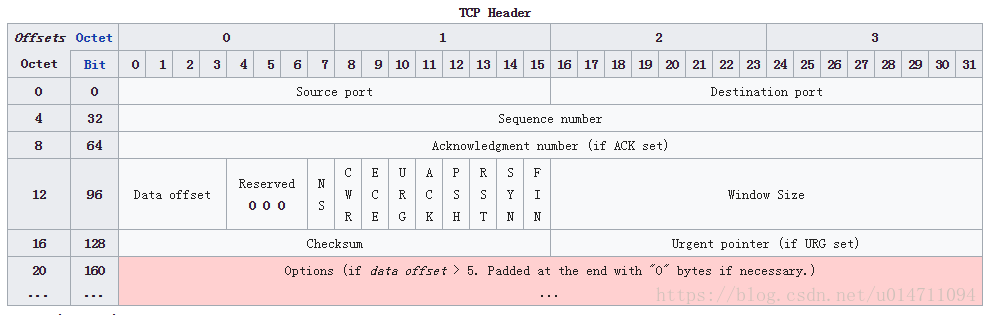
掌握Wireshark工具的基本用法；

掌握TCP协议的可靠传输机制、TCP的三次握手机制、以及TCP连接终止机制和流量控制机制；

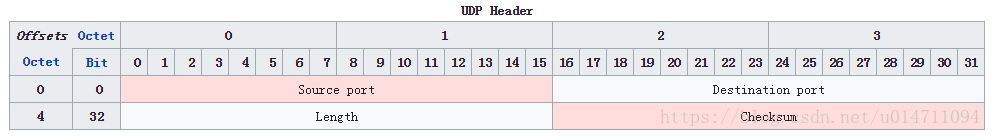
掌握UDP协议的报文格式，以及基本字段的含义。

**四、实验原理：**

**TCP协议的报文格式**



**UDP协议的报文格式**

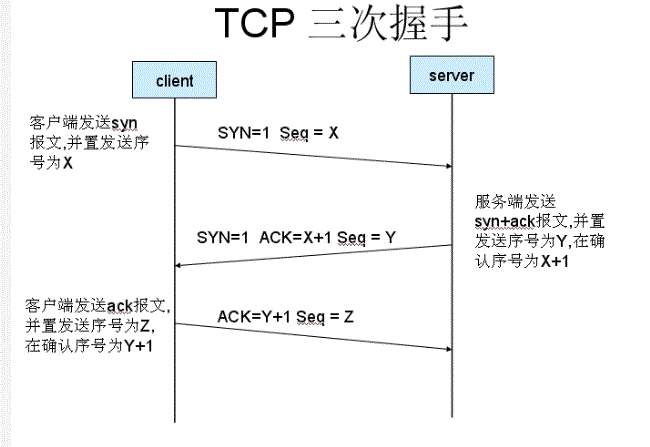


**TCP的序号和确认号机制（待补充）**

TCP会话的每一端都包含一个32位（bit）的序列号，该序列号被用来跟踪该端发送的数据量。每一个包中都包含序列号，在接收端则通过确认号用来通知发送端数据成功接收

当某个主机开启一个TCP会话时，他的初始序列号是随机的，可能是0和4,294,967,295之间的任意值，然而，像Wireshark这种工具，通常显示的都是相对序列号/确认号，而不是实际序列号/确认号，相对序列号/确认号是和TCP会话的初始序列号相关联的。这是很方便的，因为比起真实序列号/确认号，跟踪更小的相对序列号/确认号会相对容易一些

**TCP的连接建立过程**



**五、实验内容：**

实验内容主要包括两个部分：第一个部分是关于TCP协议的验证实验，第二个部分是UDP协议的验证实验。

在TCP部分，实验包括：

(1)分析TCP连接的建立过程，相关标志位字段的值，以及序号和确认号的值；

(2)分析TCP连接的结束过程，相关标志位字段的值，以及序号和确认号的值；

(3)计算RTT估计值。

在UDP部分：根据捕获的UDP发送和响应报文，分析主要字段的含义。

**六、实验器材（设备、元器件）：**

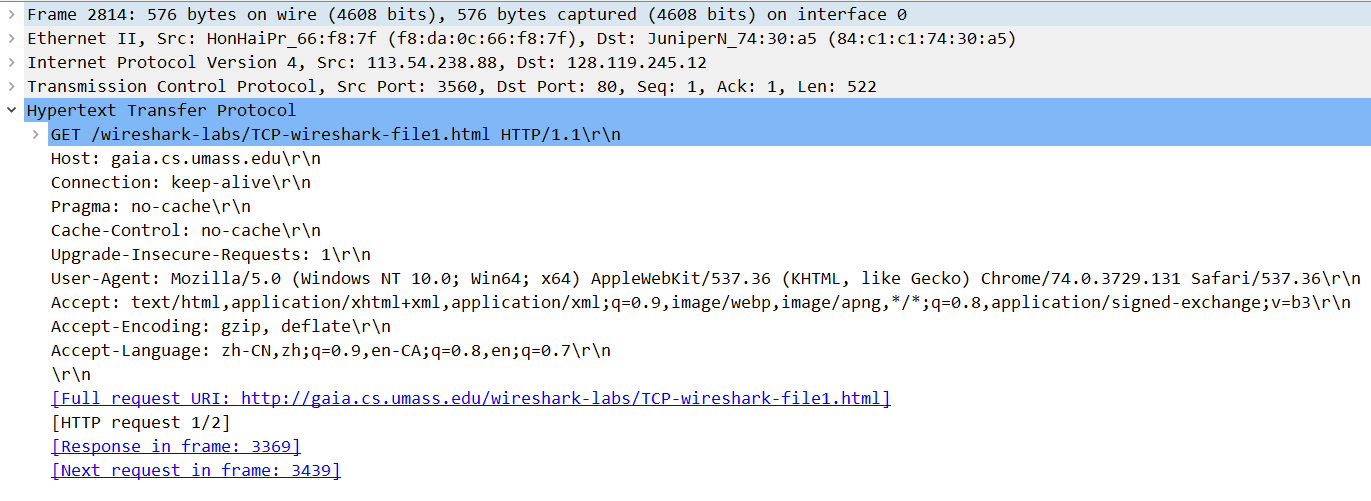
台式机，软件Wireshark

**七、实验步骤：**

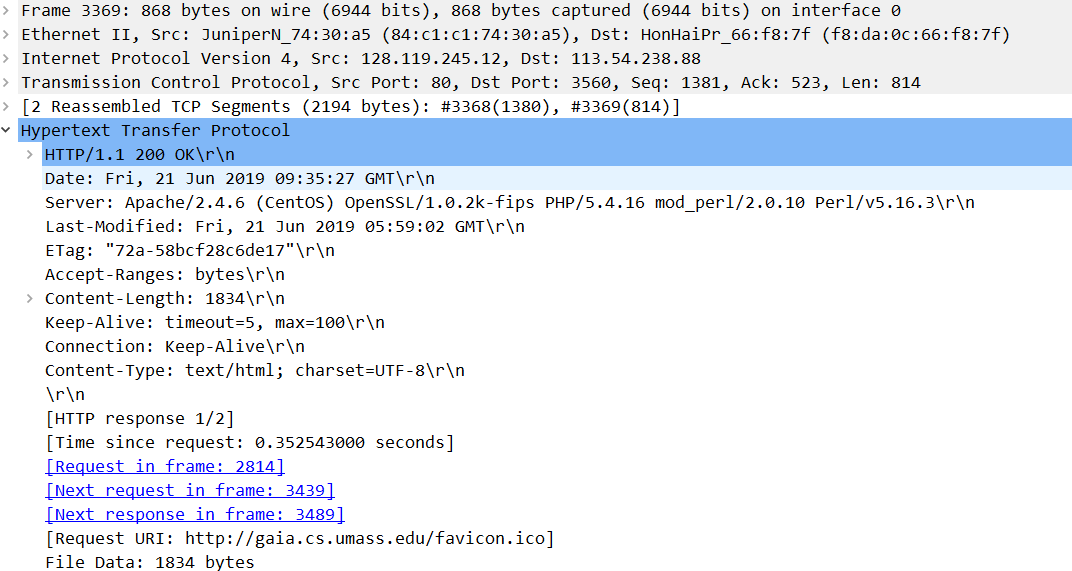
**步骤1：在浏览器中打开上传网页，捕获相关的请求消息和响应消息的报文段；**

具体步骤可参考英文指南

**打开网站：http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html**



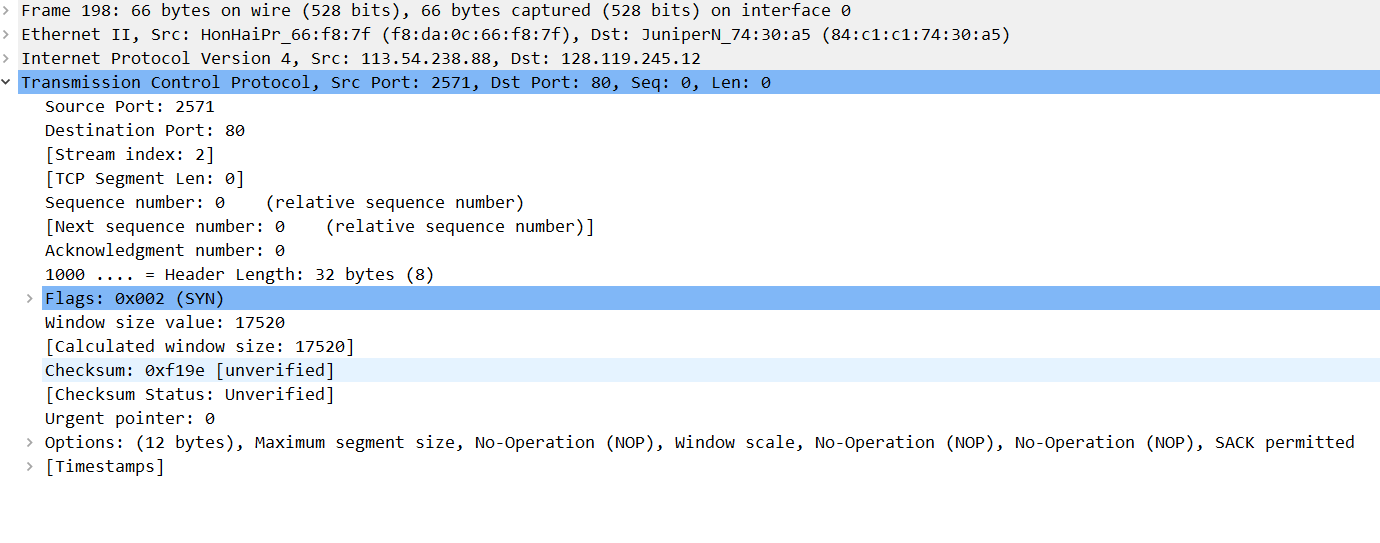
（打开上传网页的GET请求）



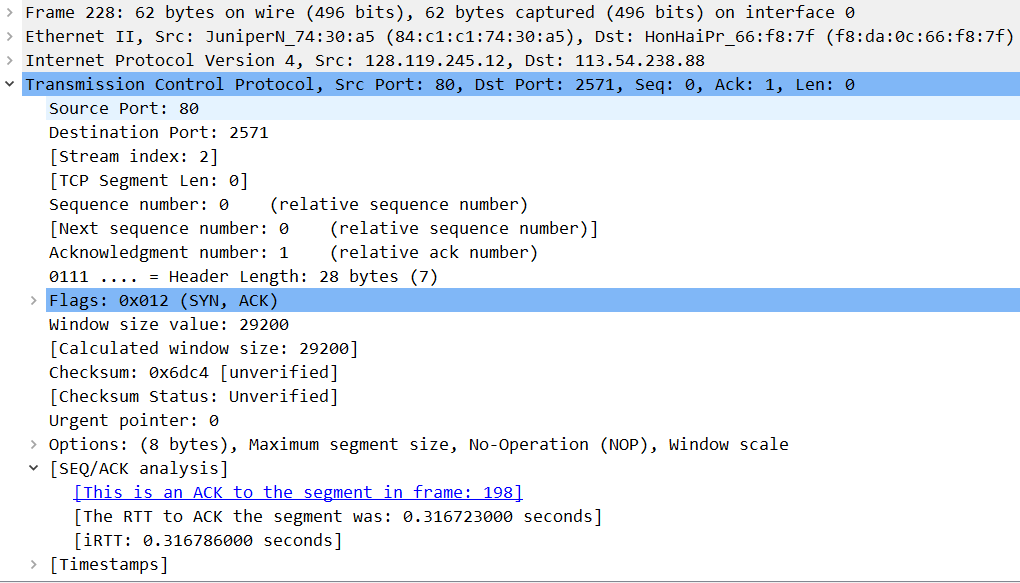
（服务器的响应报文）

**步骤2：从捕获的分组中分析出与服务器建立三次握手的过程，并给出三次握手的报文段的截图；(可以给出GET页面的TCP连接的/也可以给出POST文件的TCP连接的截图)**

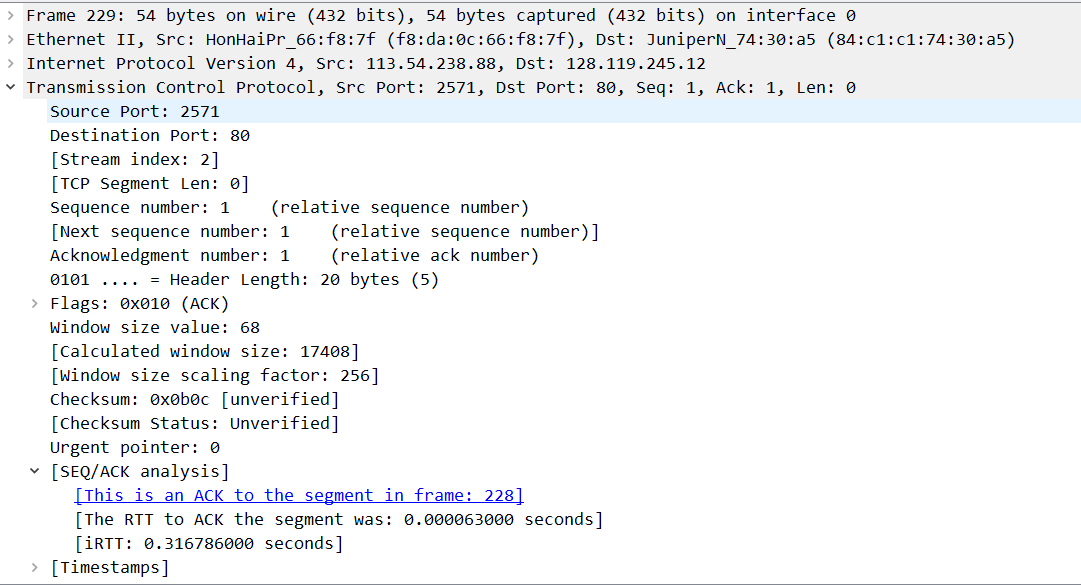
**帮助：**在GET请求报文发送之前需要先建立TCP连接：



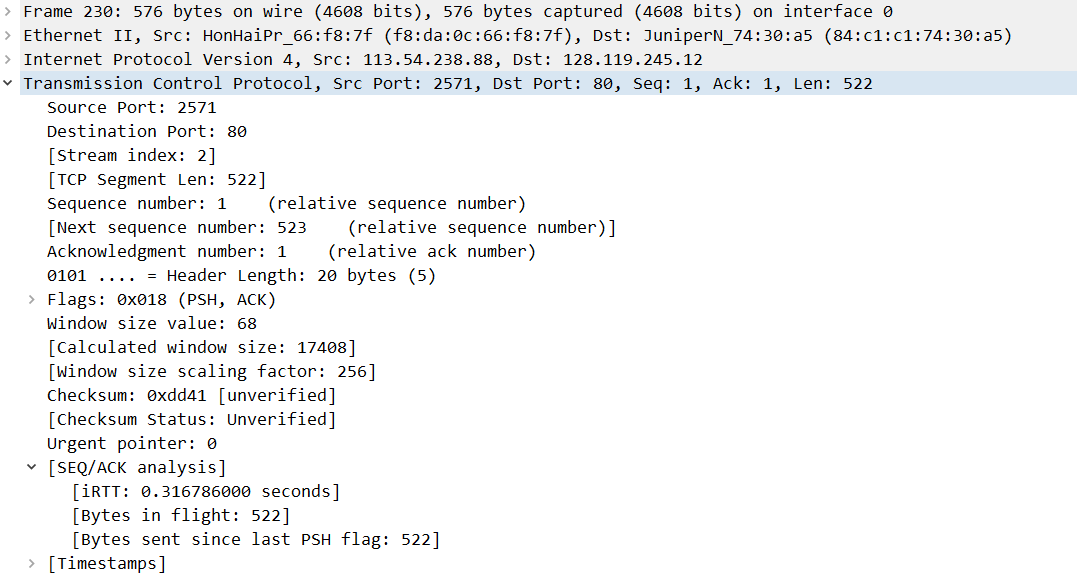
（首先由客户方发起SYN报文）不携带数据，序列号初始为0；



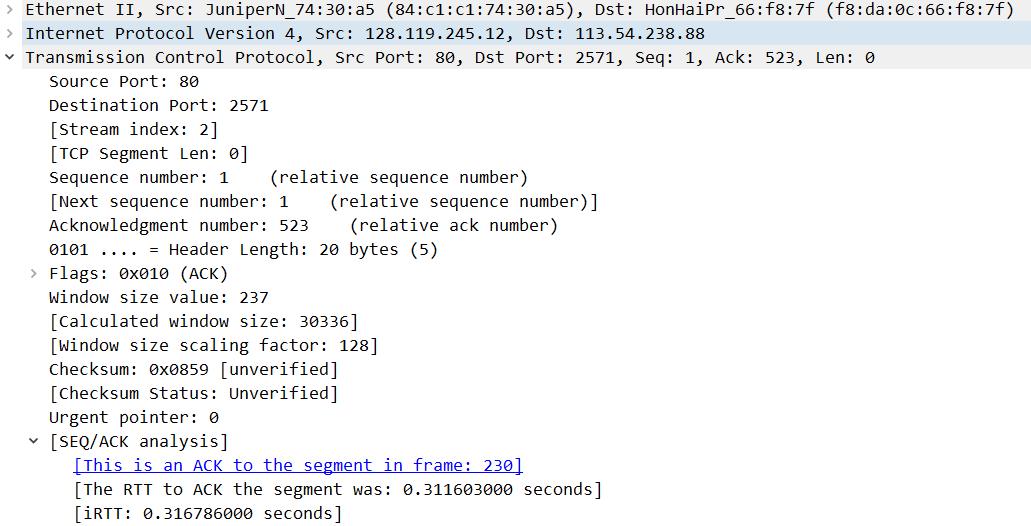
（由服务器返回SYNACK报文）不携带数据，序列号为0，应答号为1；

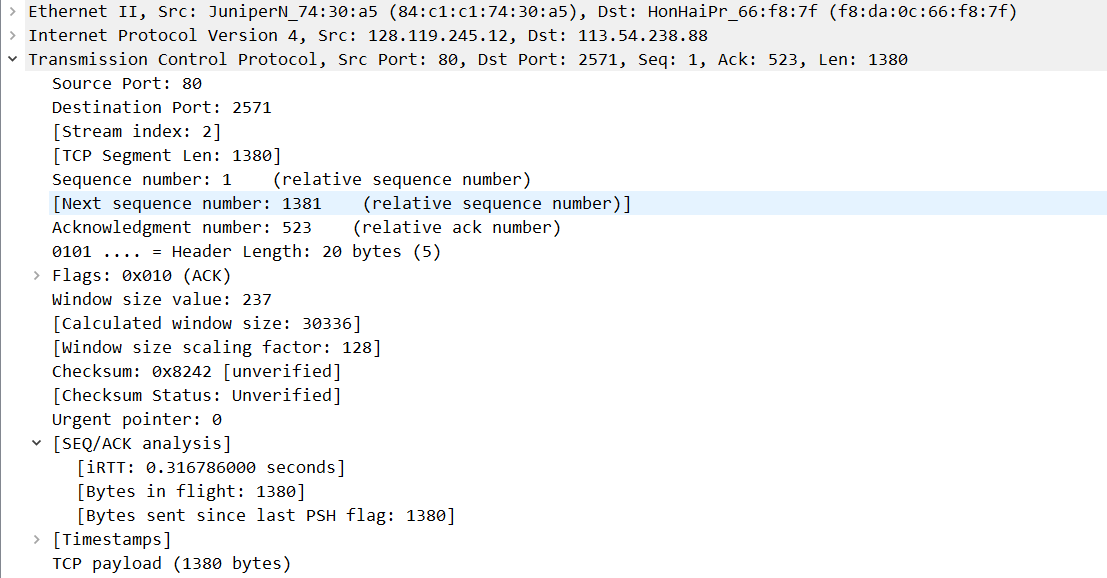
（由客户端发送ACK应答报文，通知服务器已知对方的序列号,序列号为1，确认号为1）

TCP连接建立完成，客户方才可以发送GET请求消息；



服务器方返回请求的数据，分为了两个报文段

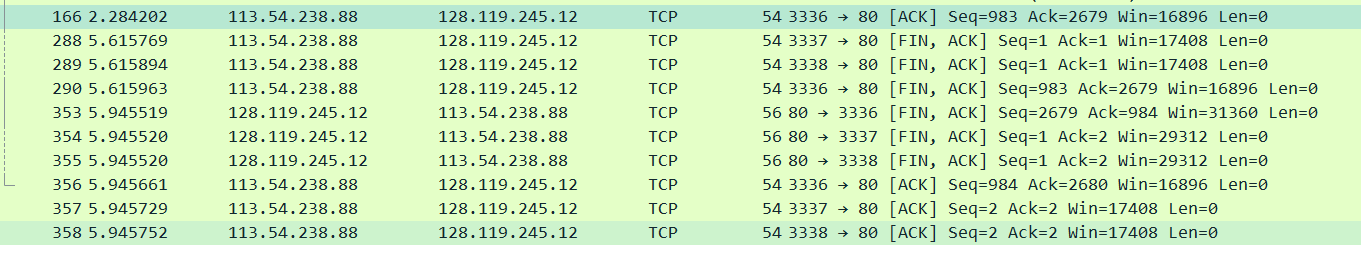




（两个报文段的数据合并为一个HTTP响应对象）

贴截图并简单说明

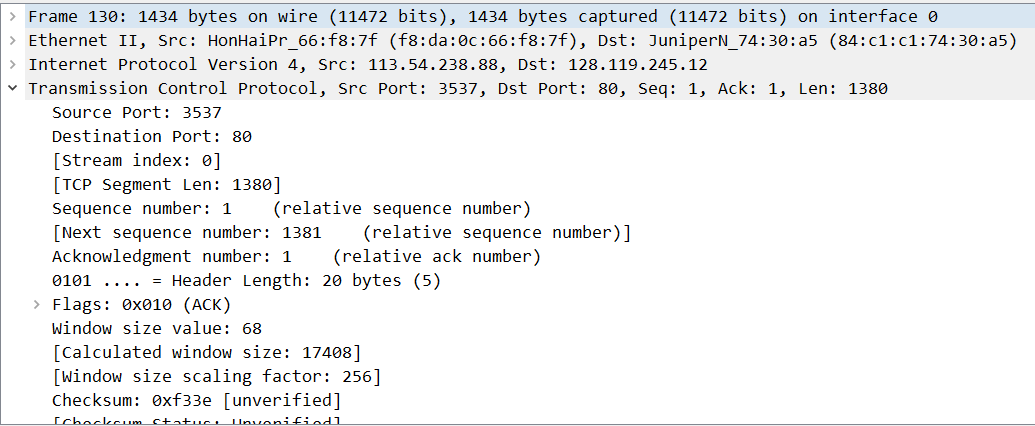
**步骤3：从捕获的分组中分析出TCP连接结束的过程，并截图，这里以上传页面获取的连接的结束为例**

TCP连接终止四次握手的截图

**步骤4：上传《爱丽丝漫游奇幻世界》文件到步骤2中GET的服务器页面；需要点击上传按钮；**

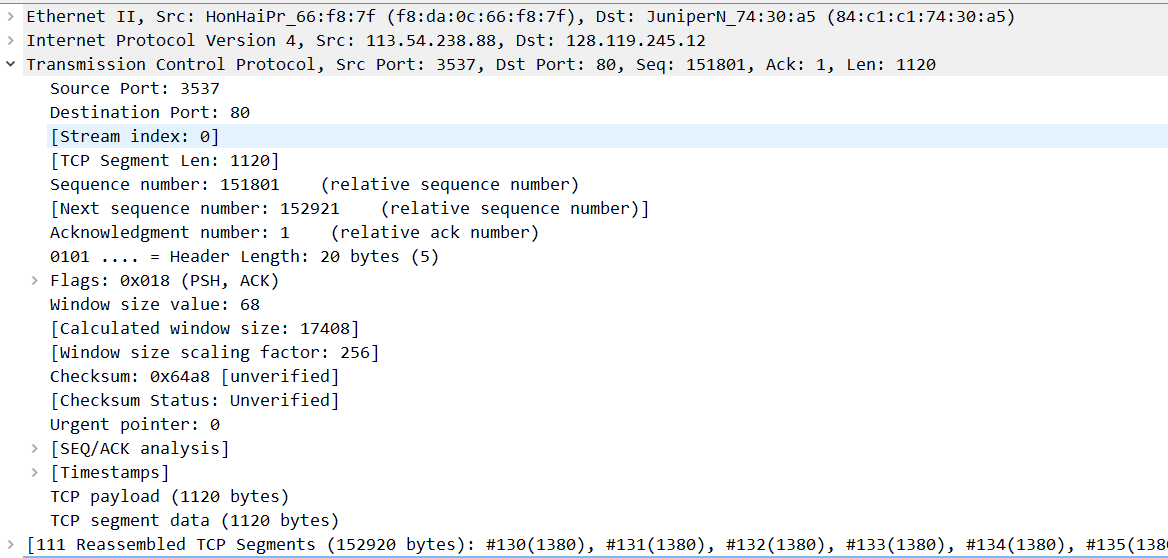
**爱丽丝漫游奇幻世界的文件来源：**http://gaia.cs.umass.edu/wireshark­labs/alice.txt

**注意：这里上传文件使用的是另一个TCP连接（客户端口49716），这个连接也是在最初建立TCP连接的阶段建立的；本步骤只关注上传文件到服务器的数据报文情况。**



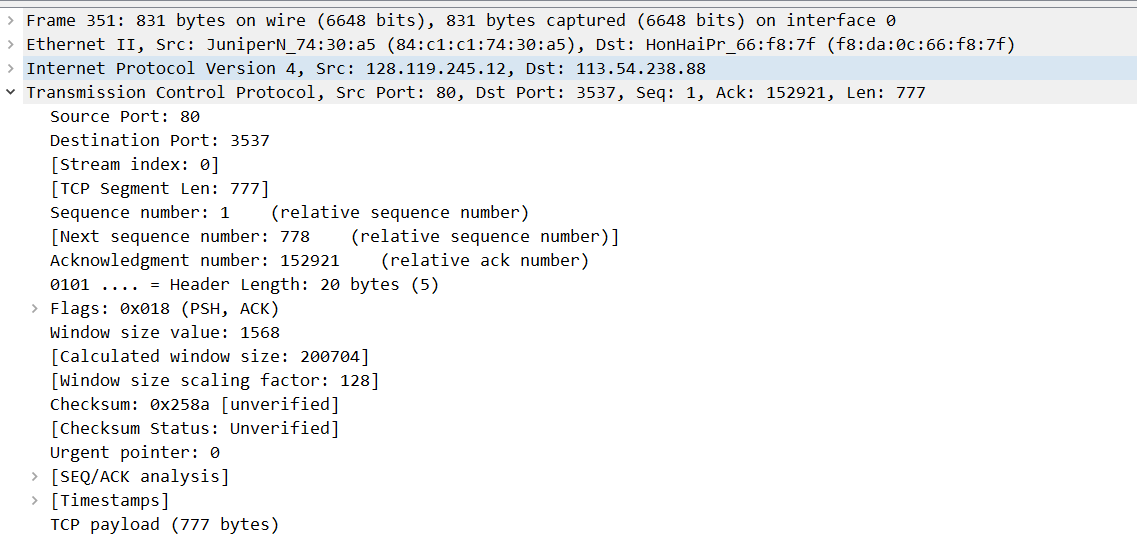
（第一个TCP报文段）

该文件上传总共分成了111个TCP报文段

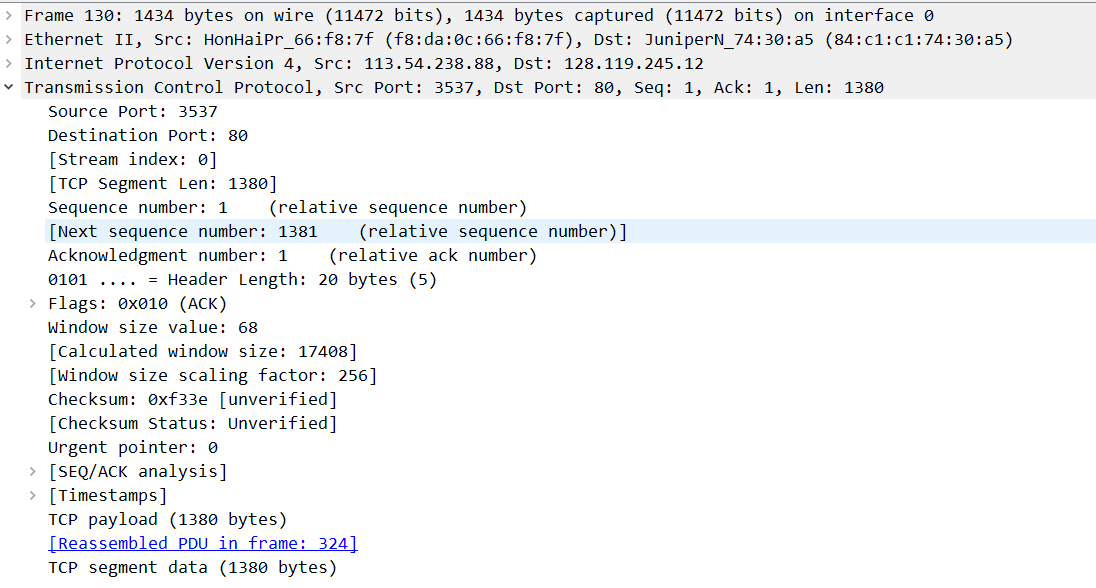


最后重组的POST消息；

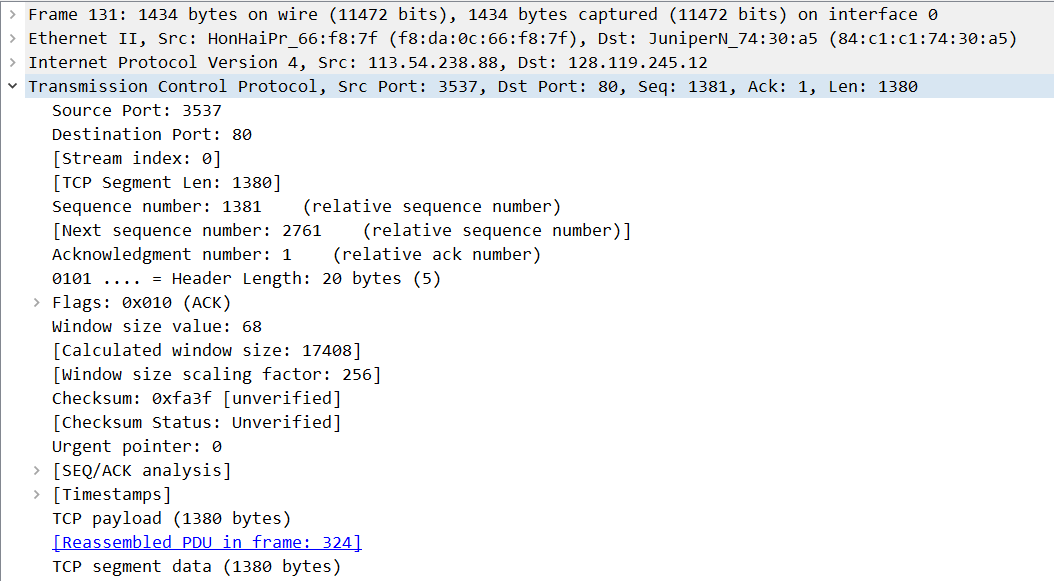
文件成功上传后的确认:



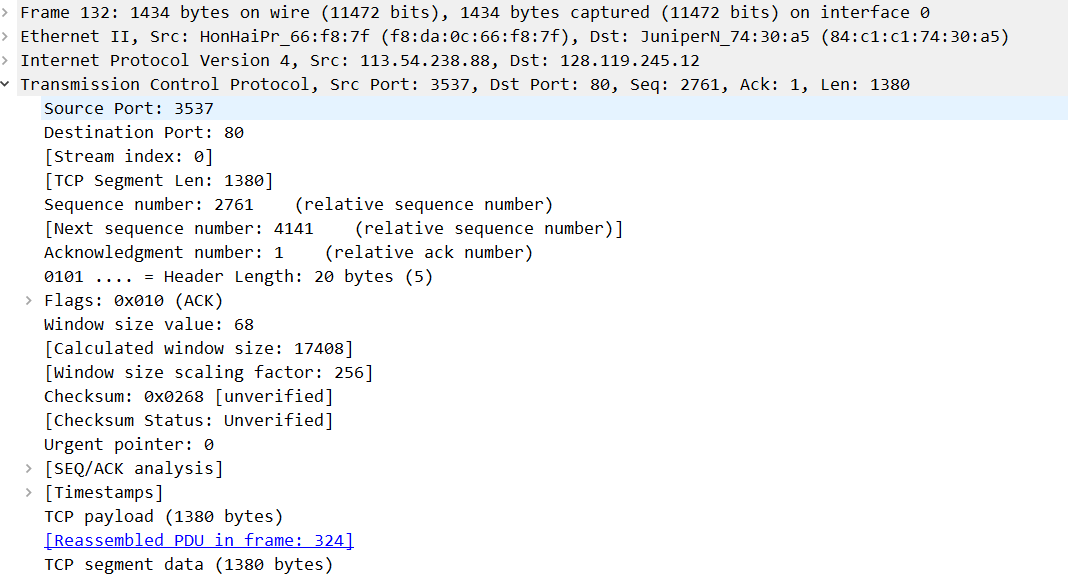
**步骤5：观察HTTP POST消息中包含的前6个TCP报文段，截图，分析这6个报文段的序列号和确认号的情况；**



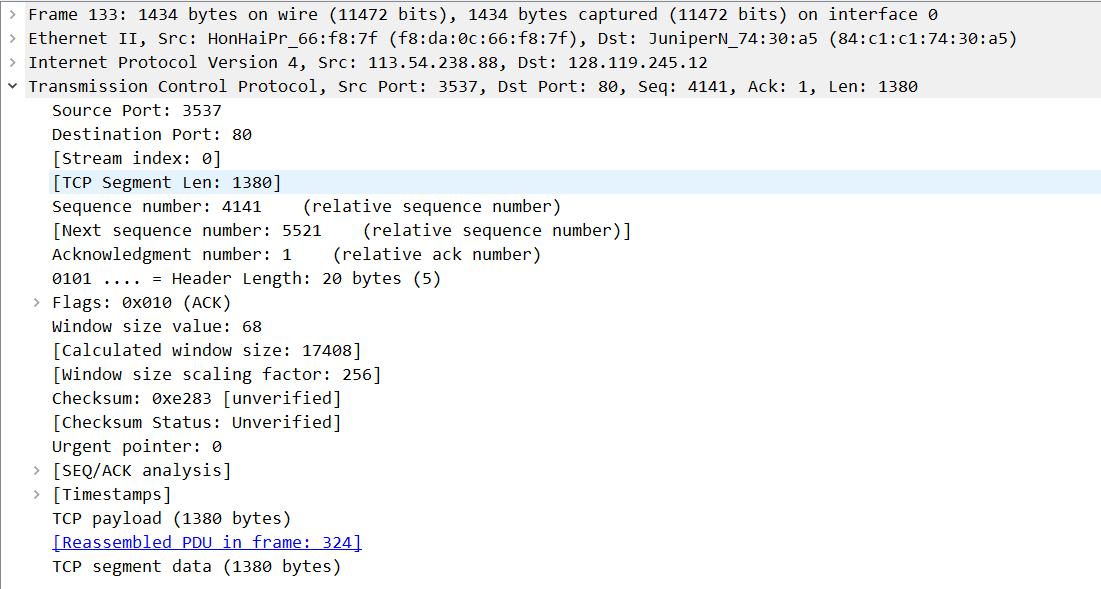
（第1个TCP报文段）



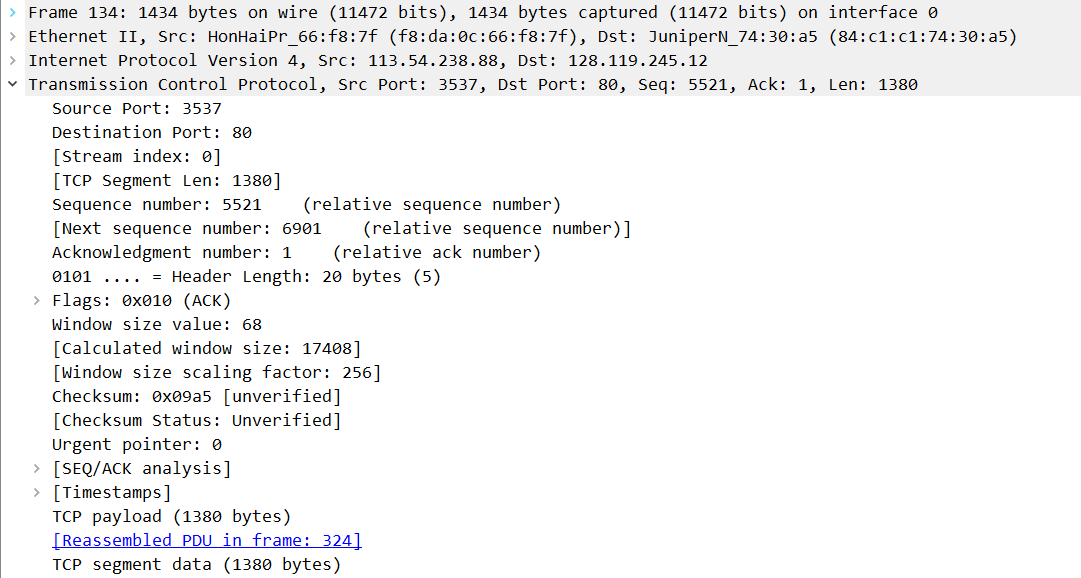
（第2个TCP报文段）



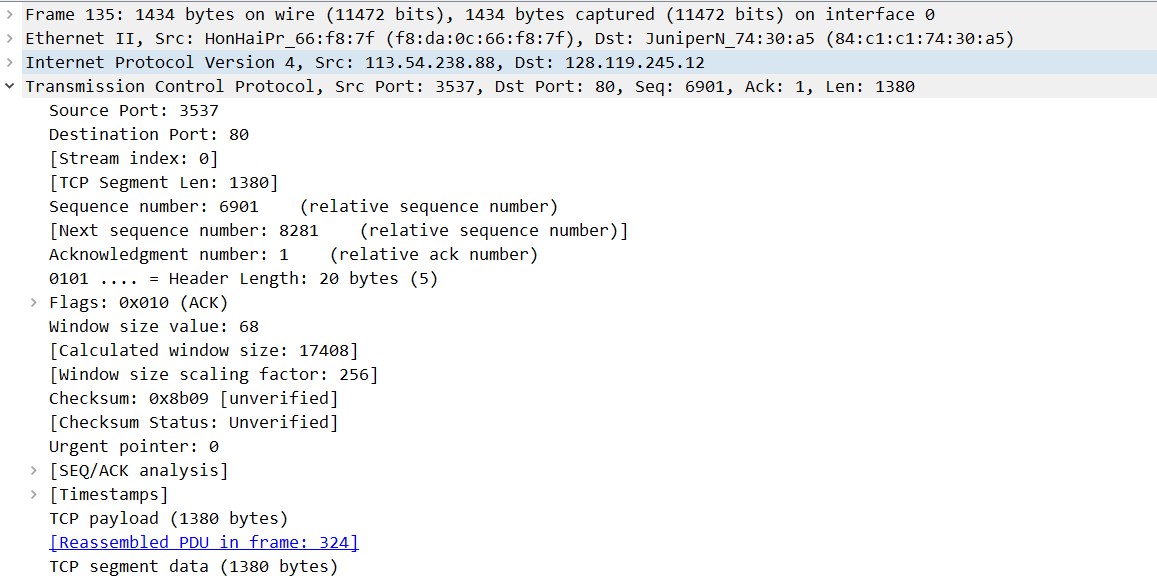
（第3个TCP报文段）



（第4个TCP报文段）

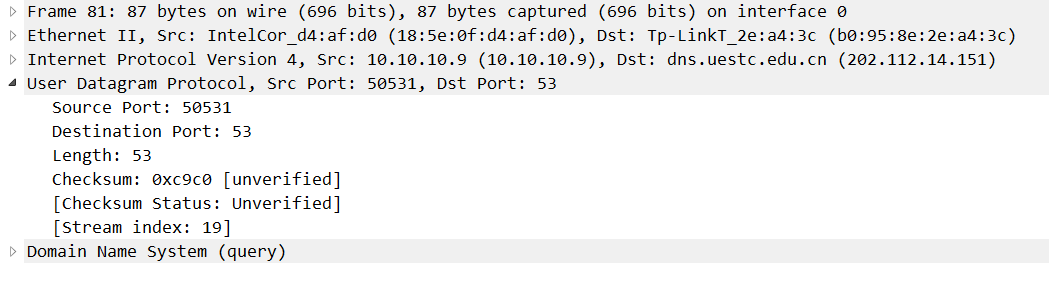


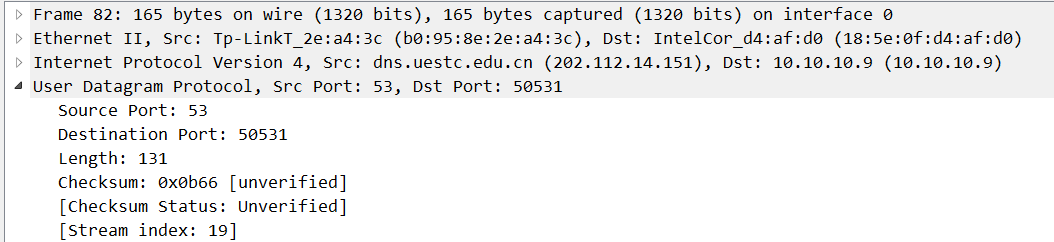
（第5个TCP报文段）



（第6个TCP报文段）

**步骤6：利用第一个实验中学习的nslookup工具，捕获基于UDP的DNS请求报文和响应报文；**





**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

针对步骤1的结果，回答以下问题：

* What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

回答：这个问题是客户机上传文件到服务器使用的IP地址和TCP端口号，分别是：49716和192.168.1.101（区别于获取上传页面使用的TCP端口号：49716）。

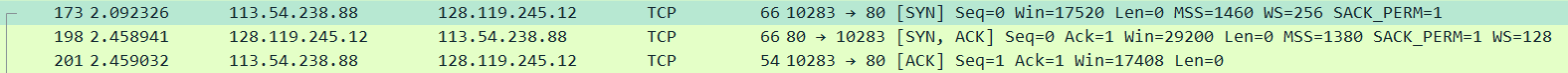
* What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

回答： IP：128.119.245.12 PORT：80

针对步骤2的结果，回答以下问题：

* What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

回答：





* 服务器gaia.cs.umass.edu发送给客户主机的作为SYN报文响应的SYNACK报文段的序列号是多少？在SYNACK报文段中确认号字段的值是多少？gaia.cs.umass.edu是怎么产生这个值的？TCP是通过在哪些字段进行设置来标识一个SYNACK报文的？

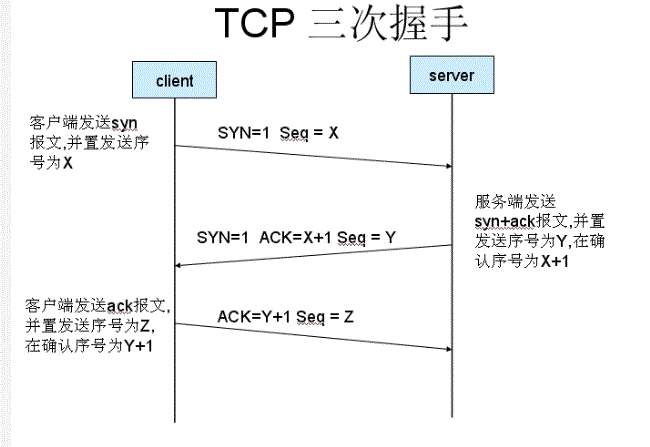
回答：



在收到SYN后产生

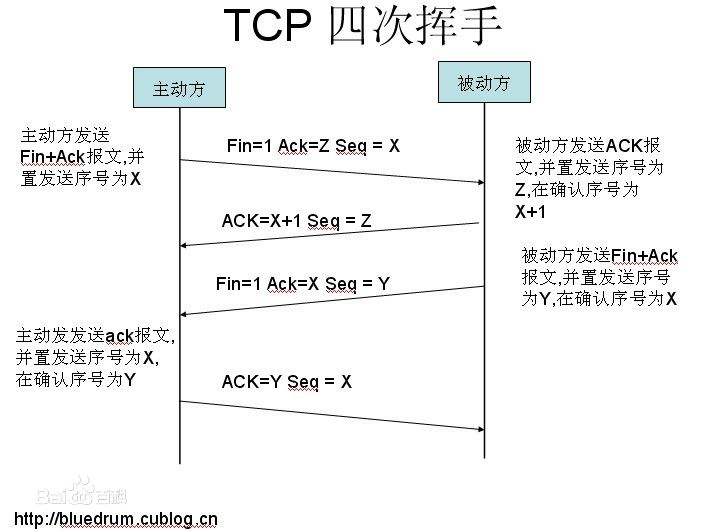


* 画出TCP三次握手的示意图。包括：标志位、序列号和确认号。



针对步骤3的结果，回答以下问题：

* 画出TCP连接结束的示意图。包括：标志位、序列号和确认号。



针对步骤4的结果，回答以下问题：

* 包含the HTTP POST命令的TCP报文段的序列号是多少？注意为了找到POST命令，你需要挖掘分组的内容字段，以寻找一个在DATA field携带了“POST”的报文段。

回答：包含the HTTP POST命令的TCP报文段的序列号是130，即第一个报文段的data field携带了“POST”的报文段。

针对步骤5的结果，回答以下问题：

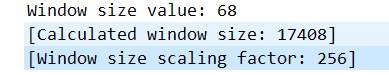
* 考虑将包含HTTP POST的TCP报文段作为TCP连接的第一个报文段。在TCP连接中的前6个报文段的序号分别是多少(including the segment containing the HTTP POST)？每个报文段的发送时间是多少？在什么时候收到每个报文段的ACK确认消息？假设每个报文段发送的时间是有差异的，当收到确认消息时，这6个报文段的RTT值？

回答：130,131,132,133,134,135。

* What is the length of each of the first six TCP segments？

1380bytes

* What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

回答：

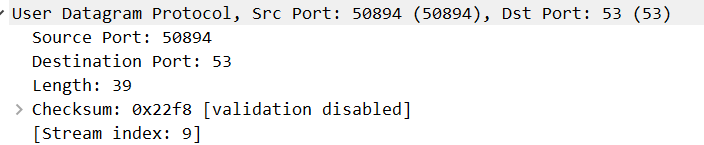
* Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
* How much data does the receiver typically acknowledge in an ACK?

回答：1460字节

针对步骤6的结果，回答以下问题：

* 从trace文件中选择一个UDP分组。从这个分组中，确定在UDP头部中有多少个字段。（不应该看书，请直接从你的分组trace文件中分析），介绍每个字段的作用。

回答：头部包括了以下域：源端口、目标端口、校验和、长度

确定每个UDP头部字段的长度为16字节

* 长度字段的值表示了什么的长度？（用你捕捉到的UDP分组来验证你的说法）

回答：长度字段的值表示了UDP头部的长度加上携带的数据的长度。

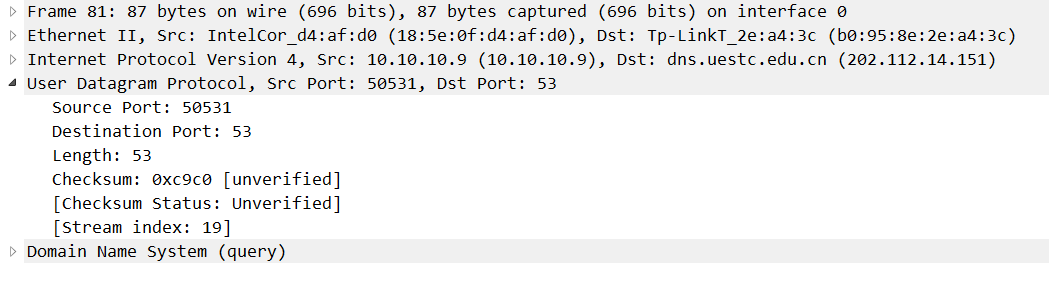
* 在一个UDP载荷中最多能携带的字节数？

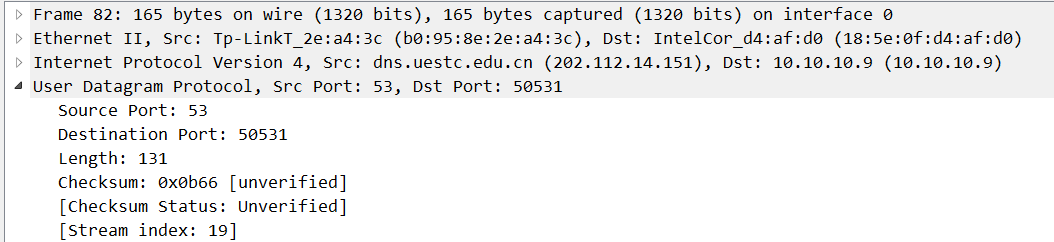
回答：2^16-1-(udp length - data)=65527

* 最大可能的源端口号是多少？

回答：源端口号为两位字节，也就是16bit，

* UDP的协议号是多少？用16进制和10进制给出答案。为了回答这个问题，你将需要查看IP包的协议字段。
* 检查一对UDP包，其中你的主机发送的是第一个UDP包，第二个UDP包是对这个第一个UDP包的应答。（暗示：对于响应第一个分组的第二个分组，第一个分组的发送方应该是第二个分组的目的主机，描述端口号之间的关系）





主机：50531，DNS服务器：53

**九、总结及心得体会：**

本次实验对于wireshark的使用基本与第一次实验一致，即经过两次实验已经可以较为熟练的使用wireshark并运用其解决问题。相比上一次实验的HTTP与DNS，本次实验的TCP与UDP在难度上有了稍许提升，主要在于有了一次连接会有更多符合条件的包去筛选和理解。经过本次使用也能更直观的了解到一般网页是如何通过tcpudp进行基本的交互，对计算机网络运输层的内容也有了更加直观和形象的理解。

**十、对本实验过程及方法、手段的改进建议：**

**无**

**报告评分：**

**指导教师签字：**