**中国科学技术大学计算机学院**

**计算机网络实验报告**

**实验三**

**利用Wireshark 观察http报文**

学 号：PB17111568

姓 名：郭雨轩

专 业：计算机科学与技术

指导老师：张信明

**中国科学技术大学计算机学院**

**2019年11月30日**

1. **实验目的**

1、捕获从计算机到远程服务器的大量TCP传输；

2、根据获得的跟踪结果对TCP传输机制作一些必要的分析，加深对TCP协议的理解；

1. **实验原理**

Wireshark（前称Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是抓取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换，监听共享网络上传送的数据包，并不能对其进行修改或者控制。

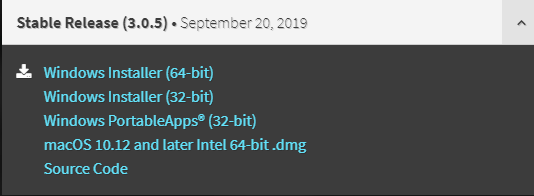
本实验使用Wireshark抓取Chrome浏览器的在访问网页时发送和接收的数据包，对其进行分析。

1. **实验环境**

软件：Windows10-64bit，Wireshark，Chrome.

硬件：Intel Corei5-7300HQ，NVIDIA GTX1050Ti，16GiB RAM.

1. **实验过程**
2. Wireshark安装
3. 访问wireshark.org得到了wireshark安装包



1. 双击打开wireshark安装包即可完成安装
2. 实验过程
3. 问题一：

客户端IP：

客户端端口号：

1. 问题二：

服务器IP：

服务器端口号：

1. 问题三：

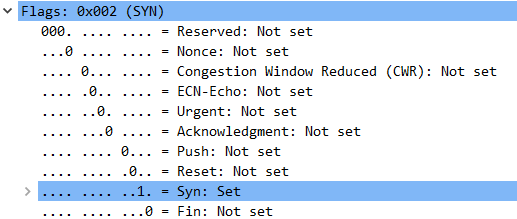
客户端IP：

客户端端口号：

1. 问题四：

初始化连接的序列号：

哪部分决定是SYN：

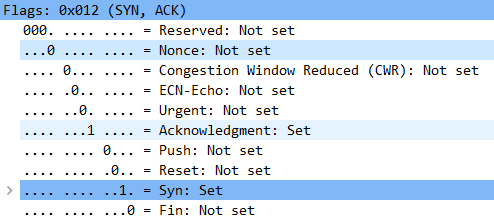


1. 问题五：

序列号：

ACK：，根据客户端的序列号加1确定

哪部分决定是SYN：



1. 问题六

POST序列号：

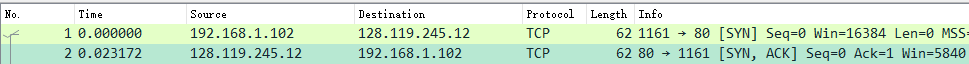
1. 问题七

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO. | SEQ | Send time | ACK time | RTT | E-RTT |
| 1 | 1 | 0.026477 | 0.053937 | 0.02746 | 0.02746 |
| 2 | 566 | 0.041737 | 0.077294 | 0.035557 | 0.0285 |
| 3 | 2026 | 0.054026 | 0.124085 | 0.070059 | 0.0337 |
| 4 | 3486 | 0.054690 | 0.169118 | 0.11443 | 0.0438 |
| 5 | 4946 | 0.077405 | 0.217299 | 0.13989 | 0.0558 |
| 6 | 6406 | 0.078157 | 0.267802 | 0.18964 | 0.0725 |

1. 问题八

|  |  |
| --- | --- |
| NO | Length |
| 1 | 565 |
| 2 | 1460 |
| 3 | 1460 |
| 4 | 1460 |
| 5 | 1460 |
| 6 | 1460 |

1. 问题九



在整个发送过程中，只有在No.2报文时的Win最小为5480

1. 问题十

没有，因为ACK单调递增

1. 问题十一

一个ACK通常确认1460的数据，

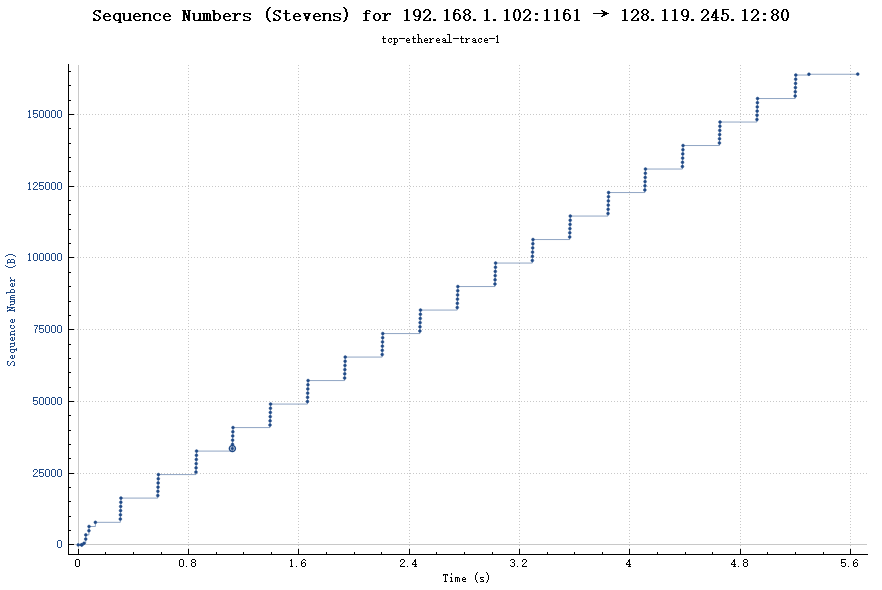


ACK跨度为2920，正在压缩其他段。

1. 问题十二

吞吐量 = (164091-1)/(5.45583- 0.026477) = 30.222 (kB/s)

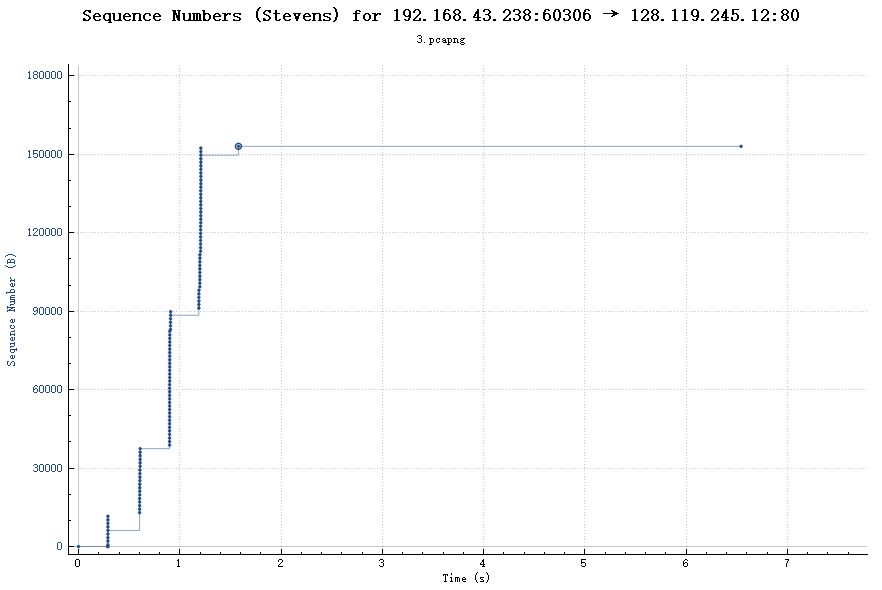
1. 问题十三



只在最开始的一小部分时慢启动，之后进入拥塞避免状态，发送速度一直平稳不变，与课本上讲的有较大出入。

这个图与课本的出入在于，当结束慢启动之后，就一直维持恒定的发送速率进行发送，不会有每过一个周期加1这个操作。

1. 问题十四



在我的发送过程中，一直进行慢启动直到文件发送完成也没有结束慢启动。至少这个过程与课本上讲得慢启动基本一致，至于拥塞避免状态的行为和快速重传的行为则不确定。

1. **实验总结**
2. 实验收获：
   1. 我熟悉了Wireshark的使用，学会了通过Wireshark的统计数据获得数据包发送的情况。
   2. 通过阅读TCP报文，我对连接建立和拆除的行为有了更加直观的认识，同时根据得到的统计图，我对真实的TCP的行为也有了了解。