**中国科学技术大学计算机学院**

**计算机网络实验报告**

**实验二**

**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10月20日**

1. **实验目的**

1、了解HTTP 协议的层次结构；

2、熟悉HTTP 协议中用于消息传输的数据结构；

3、掌握HTTP 协议数据传输的原理。

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。

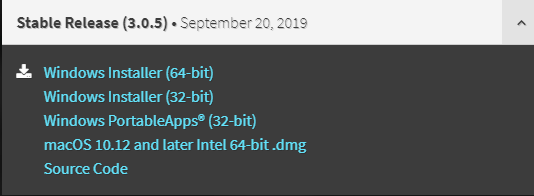
本实验使用Wireshark抓取Chrome浏览器的在访问网页时发送和接收的数据包，对其进行分析。

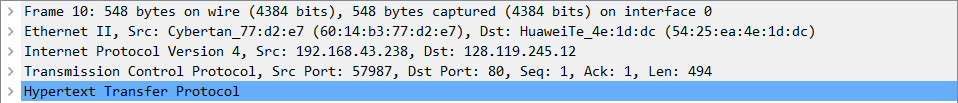
1. **实验环境**

软件：Windows10-64bit，Wireshark，Chrome.

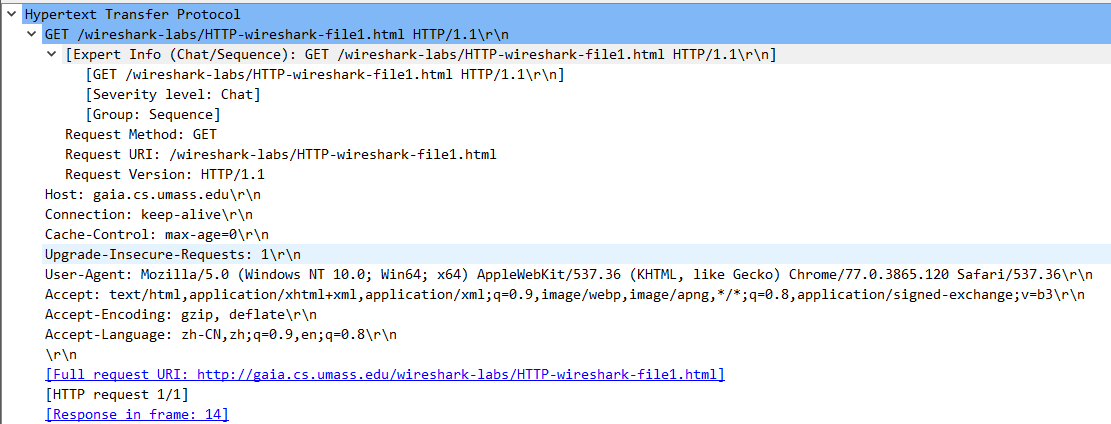
硬件：Intel Corei5-7300HQ，NVIDIA GTX1050Ti，16GiB RAM.

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



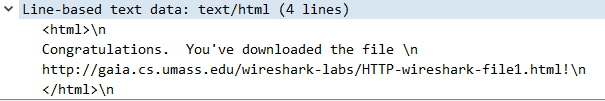
1. 双击打开wireshark安装包即可完成安装
2. 实验过程
3. 实验一
4. 用请求的报文为例，可以看到请求的报文被分为5层，

从下到上依次对应：应用层、传输层、网络层、链路层和物理层。



图中可以非常清楚的看到该报文格式与课本中给出的HTTP请求报文格式完全一致。

1. 在HTTP返回报文中，可以找到内容如图：



1. 我使用的HTTP版本为：



服务器使用的HTTP版本为：



1. 我的IP地址为192.168.43.238，服务器的IP地址为128.119.245.12
2. 上一次更改的时间为：



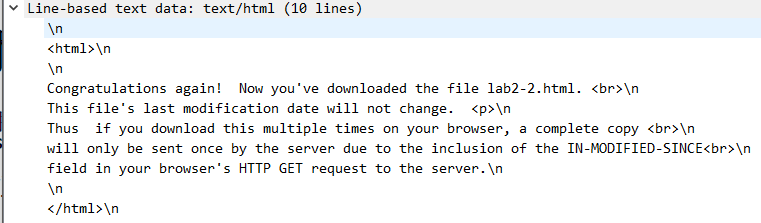
1. 长度为（单位Byte）：



1. 实验二
2. 找到的截图如下：



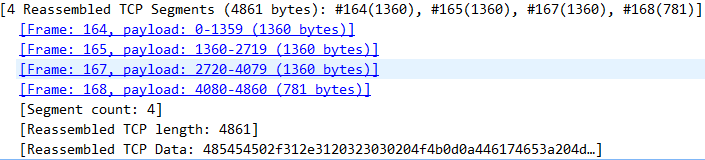
1. 第一次显式的返回了文件的内容，返回的报文中有：



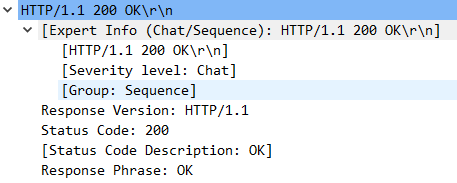
第二次没有返回，因为没有上面的条目。

原因：因为第一次请求得到的文件的上一次改动时间没有发生变化，所以当用户在多次请求这个文件的时候，HTTP的GET请求中会包含IF-MODIFIED-SINCE这个域，服务器若发现两个时间吻合则不会重新发送一次这个文件。

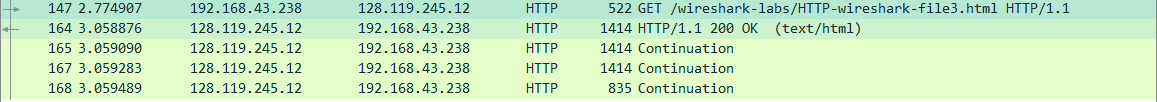
1. 实验三
2. 发送了1个GET。
3. 需要4个TCP信息段：



1. 如图：



1. 报文中的数据被分为4个连续的TCP信息段传输：



1. 实验四
2. 发送了3个请求信息，分别发送到了：







1. 连续的下载两个图片，两次请求的时间戳不同。
2. 实验五
3. 如图：

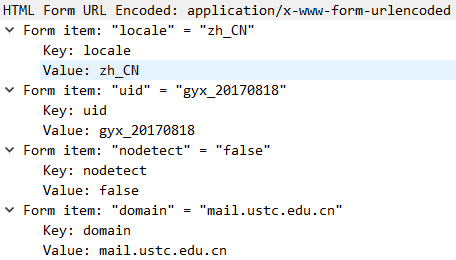


1. 如图：



1. 实验六
2. POST

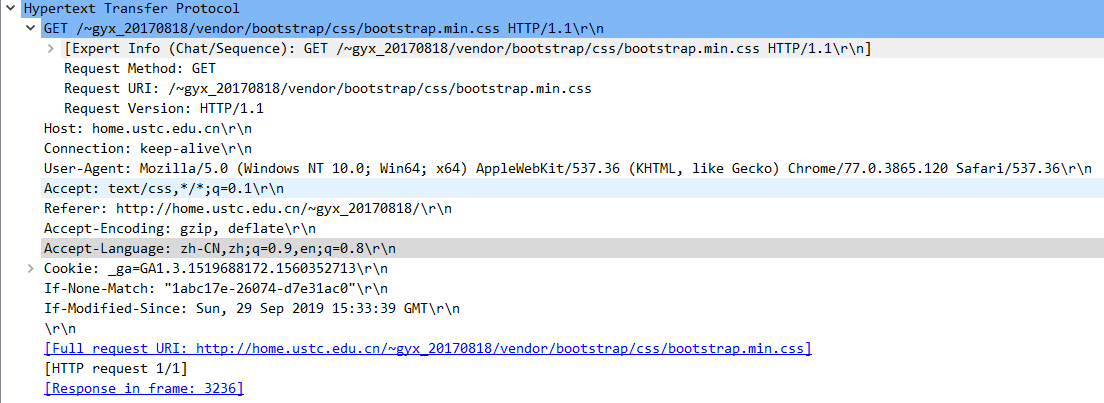
对于科大邮箱服务，在登录时就会使用POST请求，在POST向浏览器发送的数据中，有（略去密码部分未截图）：



以上内容，包含了我登录校内邮箱的所有信息。POST请求将我在浏览器中输入的用户名和密码等信息通过报文的形式传输给了邮箱的服务器。

1. GET

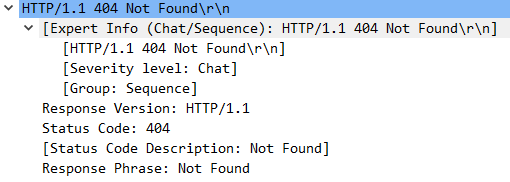
对于GET请求，以访问我的实验一搭建的个人主页为例。如图：



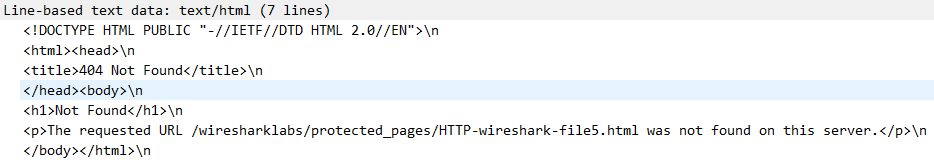
可以看到，GET请求将要向服务器发送的数据会附在URL之后，对于中文等字符则先进行base64再请求。

1. 实验七

故意将实验中给的网址输错一个字符，就会得到出错的网址。在返回的报文中，可以看到：



返回的状态码是404，要访问的文件不存在。而对于返回的html文本，则清楚的显示NOT FOUND：



1. **实验总结**
2. HTTP功能：Http协议是一个建立在TCP/IP协议上的应用层规范是一个应用层的协议。它定义了与服务器进行交互的几种不同方法，使得应用程序和服务器之间可以进行通信。
3. 实验收获：
   1. 我熟悉了Wireshark的使用，学会了通过Wireshark获得数据包。
   2. 通过阅读浏览器发送和接收的HTTP报文，并比对书上的HTTP报文结构，我对报文的每个条目代表的信息有了深刻的了解。
   3. 通过实验六对GET和POST两种方式的比较和搜集资料，我对这两种方法的差异有了深刻的了解，同时还对GET和POST的一些常见的误区有了认识。