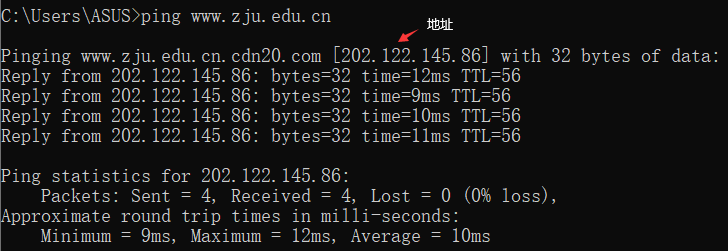
**信息安全原理HW4**

**姓名：姚熙源 学号：3190300677**

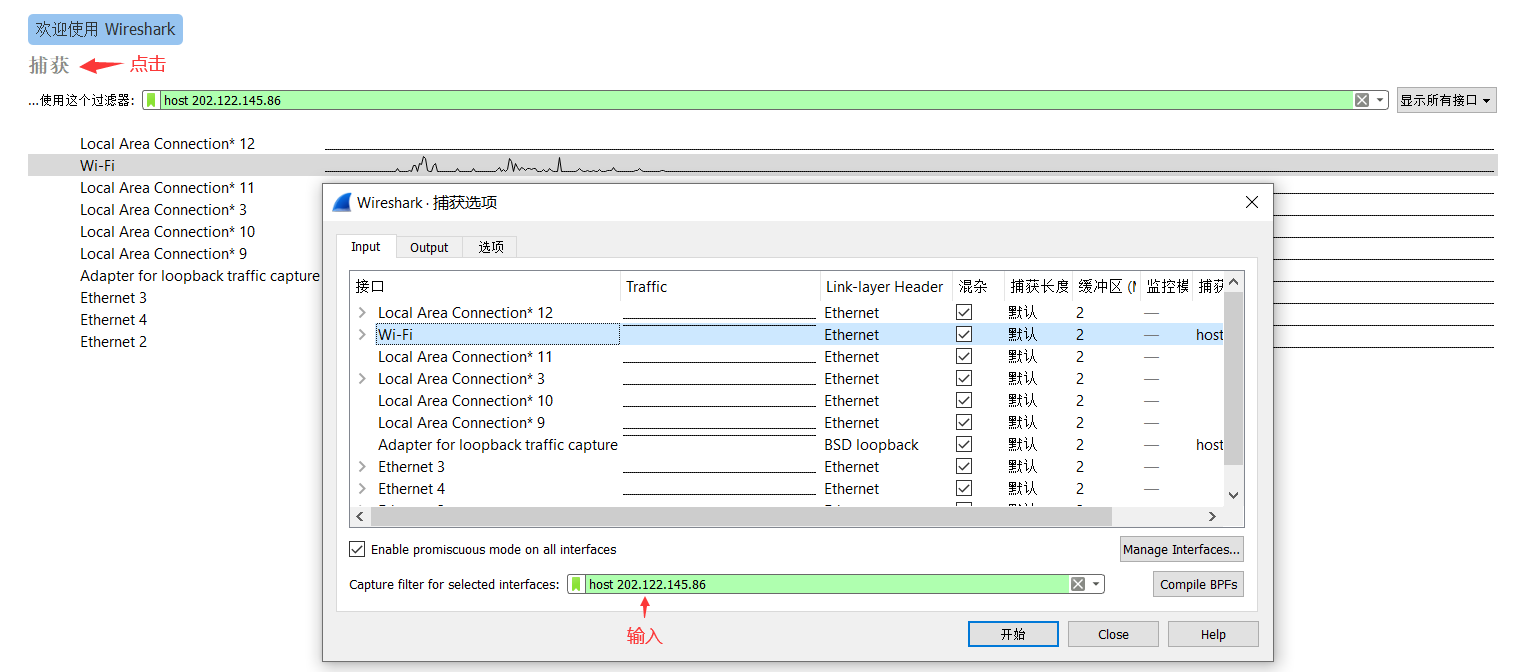
**实验过程与结果分析**

1. 下载并安装Wireshark
2. 获取[www.zju.edu.cn](http://www.zju.edu.cn)网站的服务器地址，在cmd中ping这个网址即可

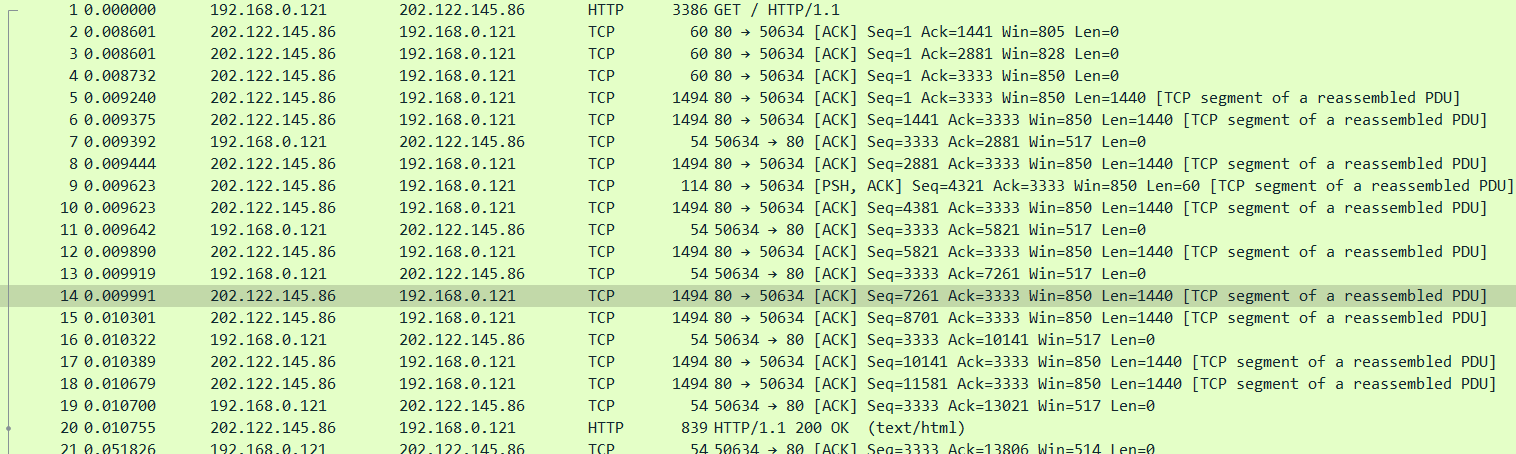


该网站([www.zju.edu.cn)的地址为202.122.145.86](http://www.zju.edu.cn)的地址为202.122.145.86)

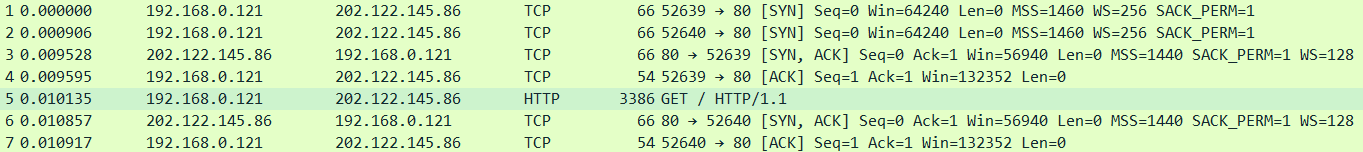
1. 打开Wireshark，在界面中点击捕获，然后在下方的过滤器中输入host 202.122.145.86，点击开始来抓取该网站的包。



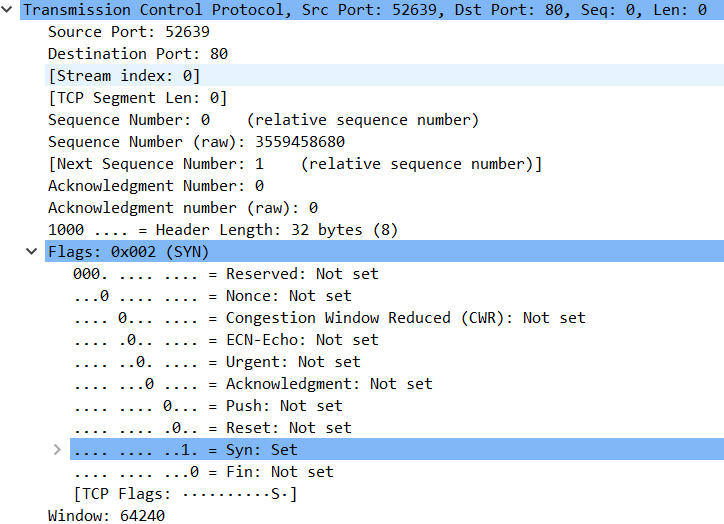
开始抓包后的界面：

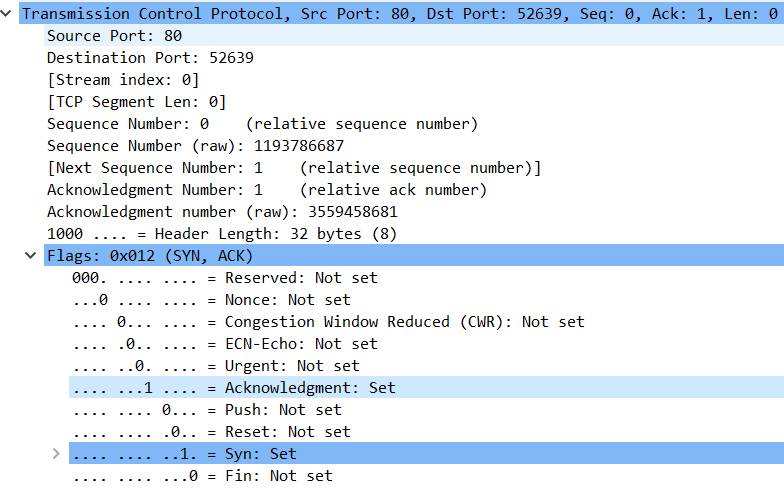


1. 对包进行分析
   1. 建立TCP（三次握手）

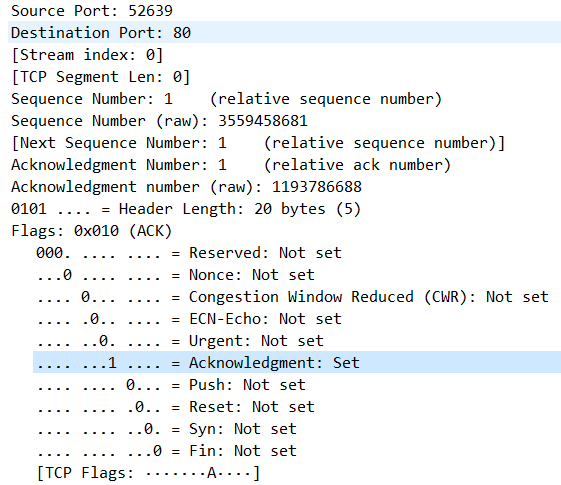


由上图可知道本机有两个端口分别为52639和52640都对网站的端口(80)建立了连接，我们以其中一个端口(52639)来分析与说明。由本机的52639端口发送请求到网站，我们可在下方的框架得到一些信息比如source,destination,port等信息，下面为line1的信息

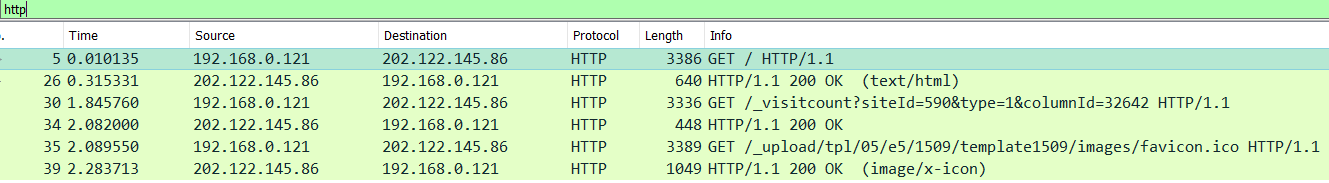


其Syn已设置为Set，表示建立新连接，发送sequence(x）给服务器，然后再看看服务器对本机回复的这个ACK包(line3)和Syn(sequence(y))来让本机确认序号有效(x+1)，其Syn和Acknowledgment都设置为Set

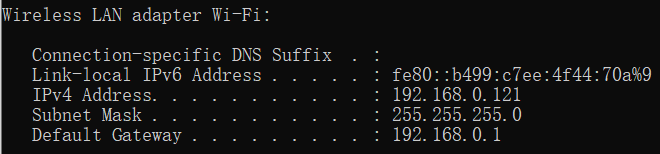
最后再进行最后一次的连接，由本机端口52639发送ACK包(y+1）到服务器端口来让服务器确认序号(y+1），其中Acknowledgment设置为Set，然后TCP连接成功。



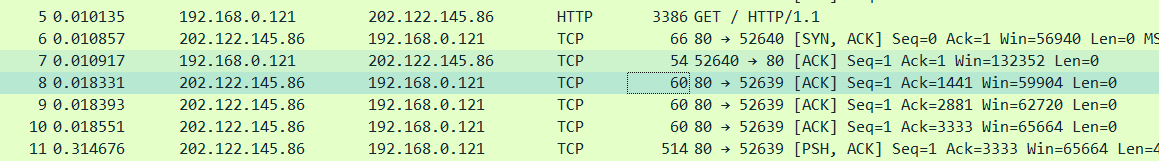
* 1. HTTP请求的连接，在上方的过滤器输入http可查看

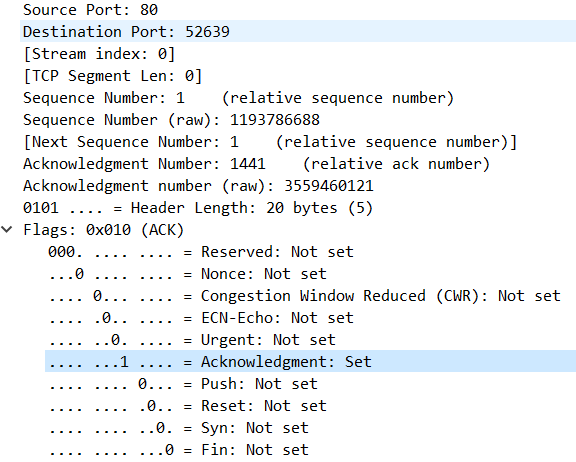


一个是GET请求，一个是RESPONSE发送回我的ip地址，在line5中可知道source是我的ip地址（在cmd中输入ipconfig便可查看自己的ip地址），而destination是网站的服务器地址。在line26，由服务器地址发送RESPONSE信息回给我的地址显示“OK”。

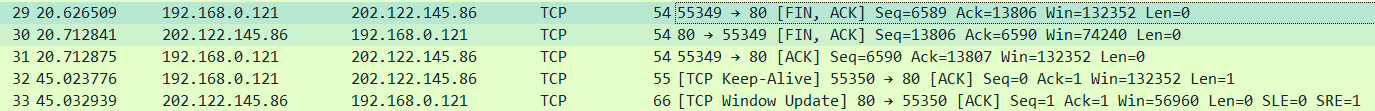


由本机发送GET请求，网站服务器端口在接收到请求后便会发送一个ACK包回给本机



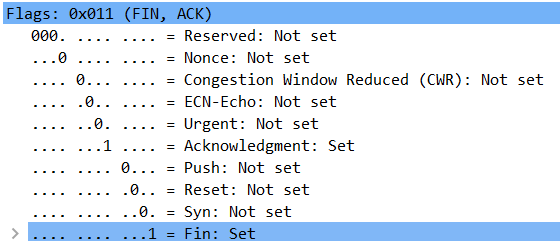
本机接收到的信息：

* 1. 断开连接

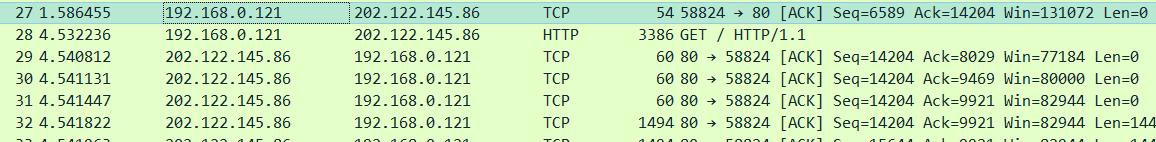


（由于我不小心点到了刷新网页所以图中的端口可能与之前的不同）

当我关掉[www.zju.edu.cn](http://www.zju.edu.cn)网站时，本机的端口向服务器断开连接，随后服务器端口也断开了连接。Fin设置为Set，表示断开连接。

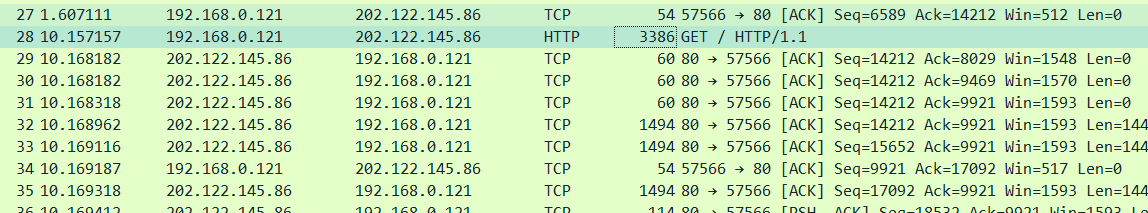


1. 刷新页面并重新抓包(hw4\_Refresh.pcapng)



Line28是刷新后所得到的新包，说明了刷新页面并不会再重新对TCP进行连接，而是直接发送HTTP的GET请求到服务器上。

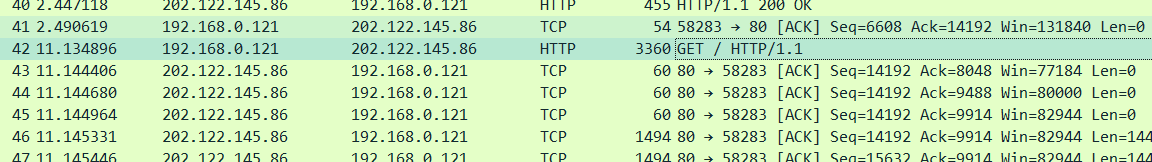
1. 在文本框重新输入网址(hw4\_EnterAgain.pcapng)



Line28是重新输入网址后得到的新包，说明了重新输入网址也不会断开端口的连接，而是又再发送HTTP的GET请求，与刷新界面一样。

重新输入该网址会将本机的端口断开连接并连接上新的断开然后再重新与TCP进行连接。

1. 在已有此网页的情况下，再新建一个标签页输入相同的网址（hw4\_EnterAnotherTab.pcapng）



Line42是重新输入该网址后得到的新包，可以看到的是并没有端口的断开连接而是直接发送HTTP请求到服务器上。