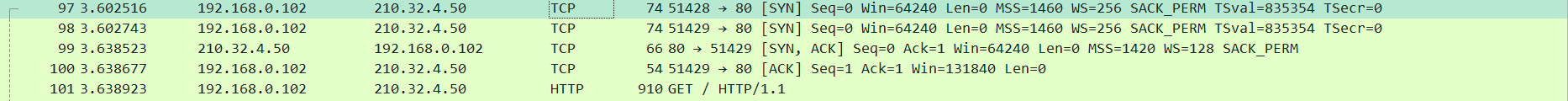
# HW4

实验内容：

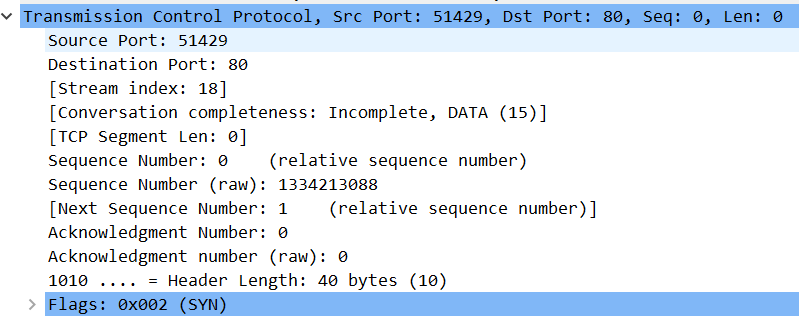
使用wireshark抓捕访问 <http://www.cs.zju.edu.cn> 网站时网络数据包。

1. 下载wireshark 软件并进行安装。
2. 在cmd命令行使用ping [www.cs.zju.edu.cn](http://www.cs.zju.edu.cn) （偷懒）  获得IP值（因为我在校外运行，所以尝试了在使用rvpn与不使用的两种情况，发现两者ip地址相去甚远，实验最后选用ip为210.32.4.50）。
3. 运行wireshark程序，访问网站，进行抓包。
4. 对抓包进行处理分析（每一分析前括号内内容为包序号）。

处理分析结果如下：

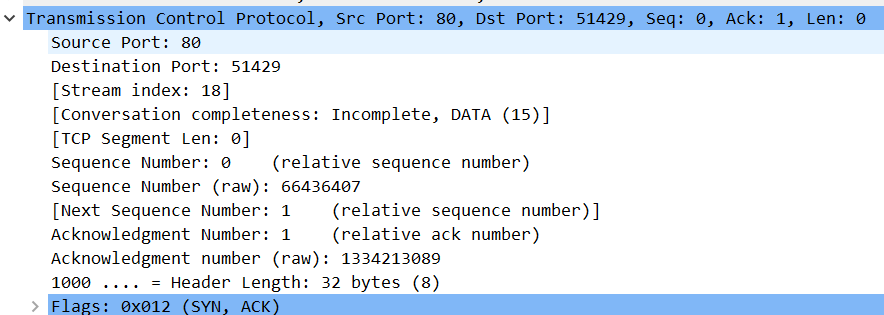
由上图看出推测，192.168.0.102应该为我的电脑客户端的ip地址，在访问上述网站时，不断发出包以请求；在发出第二个包时，收到了目标服务器ip的回复，从而二次发送数据包确认以完成TCP协议的三次握手。

（97-100）三次握手的具体内容如下：

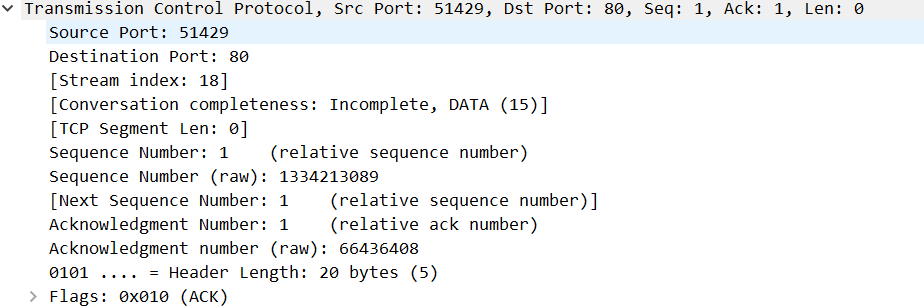


第一次握手数据包

客户端发送一个TCP连接请求  
 源端口：51429  
 目的端口：80  
 序列号：0  
 确认号：初始为0  
 标志位：SYN



第二次握手的数据包  
 服务器发回确认包  
 源端口：80  
 目的端口：51429  
 序列号：0  
 确认号：1  
 标志位：SYN+ACK



第三次握手的数据包  
 客户端发送确认包  
 源端口：51429  
 目的端口：80  
 序列号：1  
 确认号：1  
 标志位：ACK

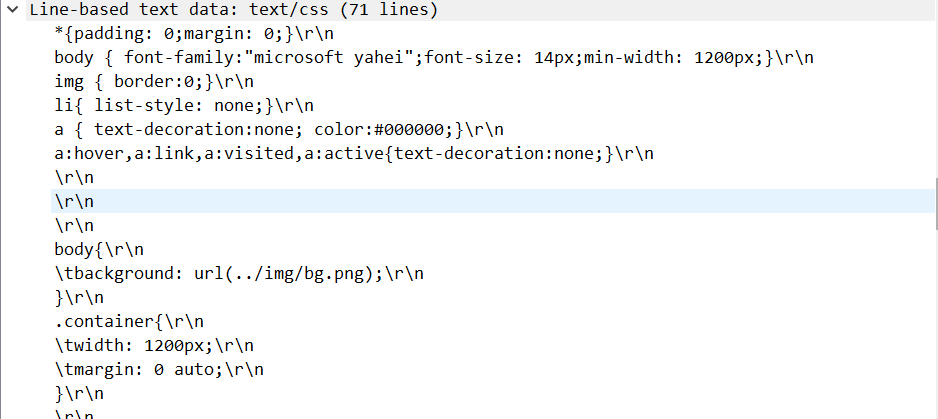
此上，三次握手结束，紧接着服务器发送了http协议数据包。

（107）然后根据我仅有的一些知识，尝试分析了一下我都抓到了什么东东。

a7df6ffb51de81e8f61e7b4c9a793b3

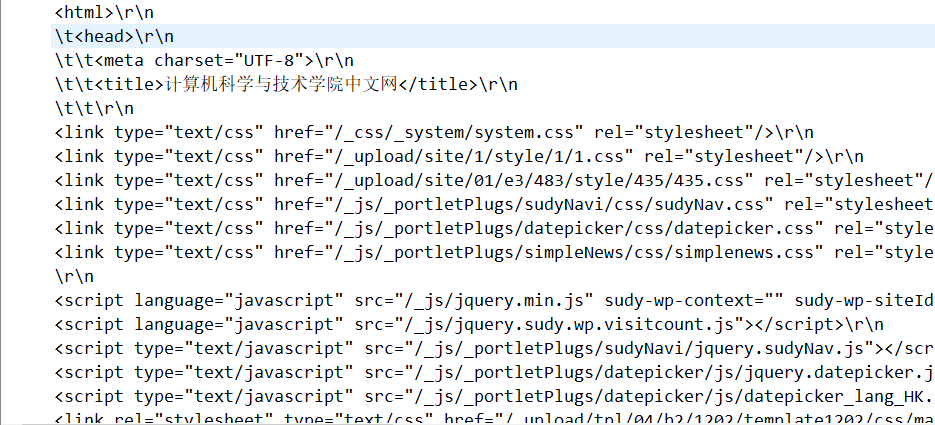
这感觉是一个html语言文本文件，主要内容（局部）为：

应该是用html语言写的网站的基本排布内容。

（114）接着找到一个css文件，主要内容（局部）：

应该是网页编写时一些美观性的层叠性设计吧。

（12258）在目标网站，选择点击中文网后，也出先了相似的html文件包，页面逐渐丰富，因而html文件中的代码信息也丰富了不少，这里只成列部分结果：



当然还有最熟悉的404 not found环节：

