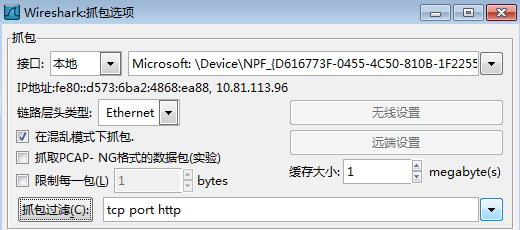
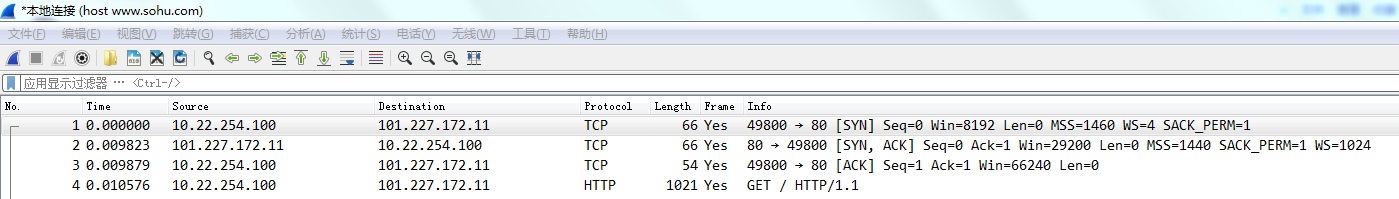
**三次握手实验**

课堂案例：

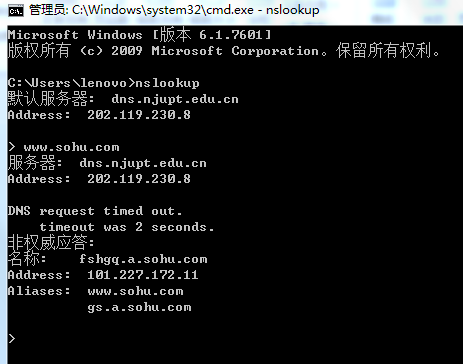
抓取源于或发往主机[www.sohu.com](http://www.sohu.com)的所有流量，抓包过滤器配置：在滤波器选项中选择http过滤





10.22.254.100是本机，101.227.172.11会是什么地址？

我们通过nslookup命令解析一下，发现确实是的，于是前三行就是传说中的“TCP三次握手”。

 在TCP/IP协议中，TCP协议提供可靠的连接服务，采用三次握手建立一个连接。

**第一次握手**：建立连接时，客户端发送syn包(syn=j)到服务器，并进入SYN\_SEND状态，等待服务器确认；

**第二次握手**：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送一个SYN包（syn=k），即SYN+ACK包，此时服务器进入SYN\_RECV状态；

**第三次握手**：客户端收到服务器的SYN＋ACK包，向服务器发送确认包ACK(ack=k+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。

完成三次握手，客户端与服务器开始传送数据.

**课堂任务：**

**设置过滤指令，抓取三个网站的流量，分析TCP中三次握手协议。**

**幕后原理**：根据主机名执行过滤，Wireshark会通过域名解析服务把用户输入的主机名转换为IP地址，并抓取与这一IP地址相对应的流量。

思考：

1.利用wireshark 抓获所有TCP源端口范围为5000-6000的telnet流量，抓波过滤器应如何设置？

2.用以下文字描述三个结构化抓包过程：

Host [www.mywebsite.com](http://www.mywebsite.com) and not port 80 or port 23

Host 192.168.0.25 and not tcp port 80

Host 10.0.0.1 and not host 10.0.0.2