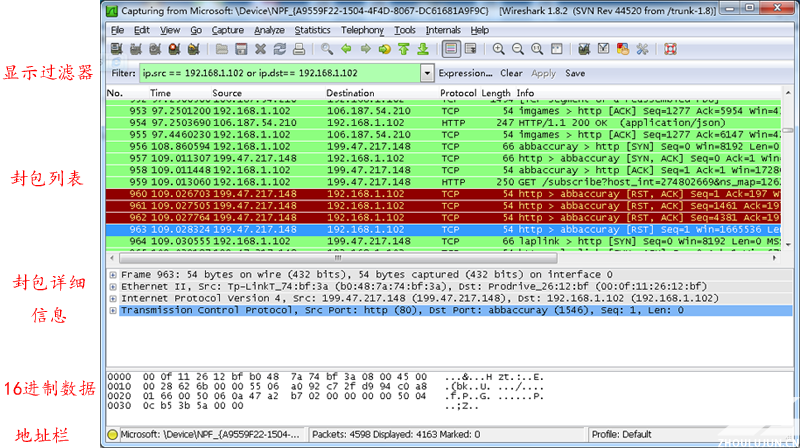
# wireshark窗口介绍



WireShark 主要分为这几个界面

1. Display Filter(显示过滤器)，  用于过滤

2. Packet List Pane(封包列表)， 显示捕获到的封包， 有源地址和目标地址，端口号。 颜色不同，代表

3. Packet Details Pane(封包详细信息), 显示封包中的字段

4. Dissector Pane(16进制数据)

5. Miscellanous(地址栏，杂项)

## 封包详细信息 (Packet Details Pane)

这个面板是我们最重要的，用来查看协议中的每一个字段。

各行信息分别为

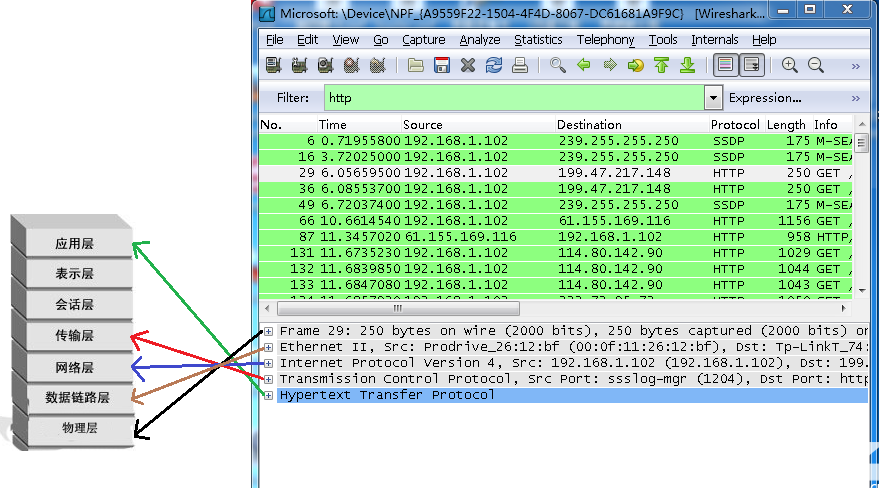
Frame:   物理层的数据帧概况

Ethernet II: 数据链路层以太网帧头部信息

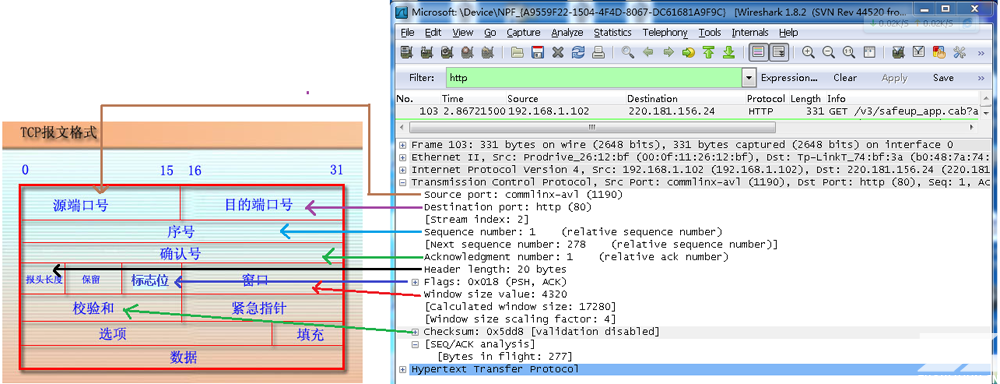
Internet Protocol Version 4: 网络层IP包头部信息

Transmission Control Protocol:  传输层T的数据段头部信息，此处是TCP

Hypertext Transfer Protocol:  应用层的信息，此处是HTTP协议



## TCP包的具体内容



## 实例分析TCP三次握手过程

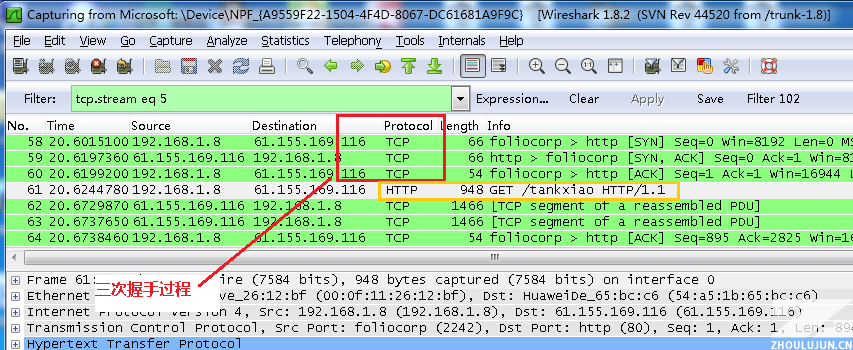
## IMG_256

这图我都看过很多遍了， 这次我们用wireshark实际分析下三次握手的过程。

1.打开wireshark, 打开浏览器输入 http://www.cnblogs.com/tankxiao

2.在wireshark中输入http过滤， 然后选中GET /tankxiao HTTP/1.1的那条记录，右键然后点击"Follow TCP Stream",

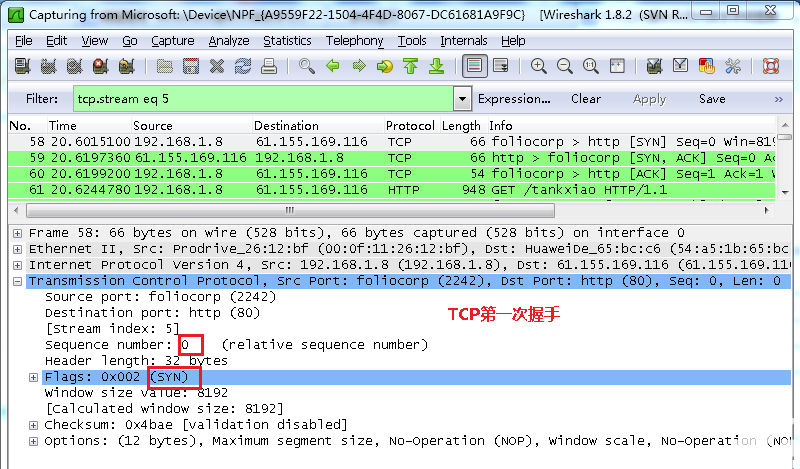
这样做的目的是为了得到与浏览器打开网站相关的数据包，将得到如下图



图中可以看到wireshark截获到了三次握手的三个数据包。第四个包才是HTTP的， 这说明HTTP的确是使用TCP建立连接的。

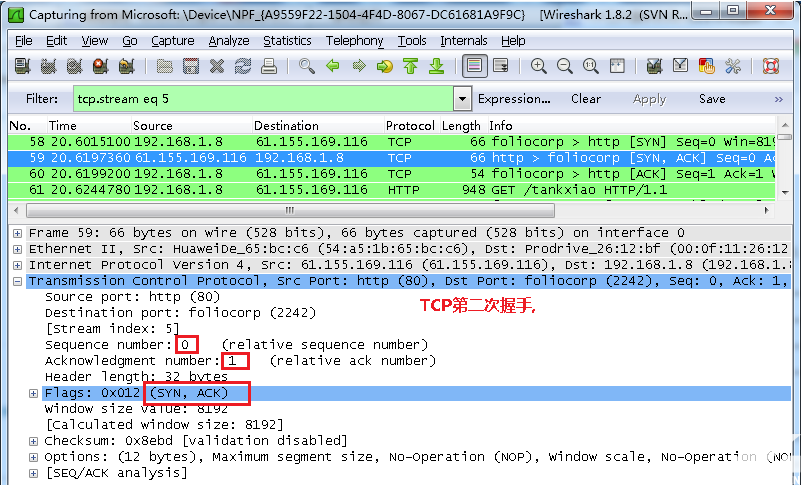
第一次握手数据包

客户端发送一个TCP，标志位为SYN，序列号为0， 代表客户端请求建立连接。 如下图



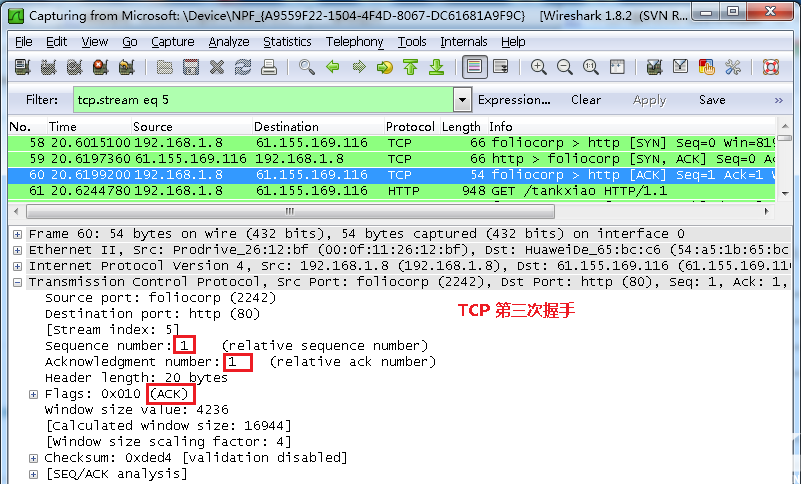
第二次握手的数据包

服务器发回确认包, 标志位为 SYN,ACK. 将确认序号(Acknowledgement Number)设置为客户的I S N加1以.即0+1=1, 如下图



第三次握手的数据包

客户端再次发送确认包(ACK) SYN标志位为0,ACK标志位为1.并且把服务器发来ACK的序号字段+1,放在确定字段中发送给对方.并且在数据段放写ISN的+1, 如下图:



 就这样通过了TCP三次握手，建立了连接。