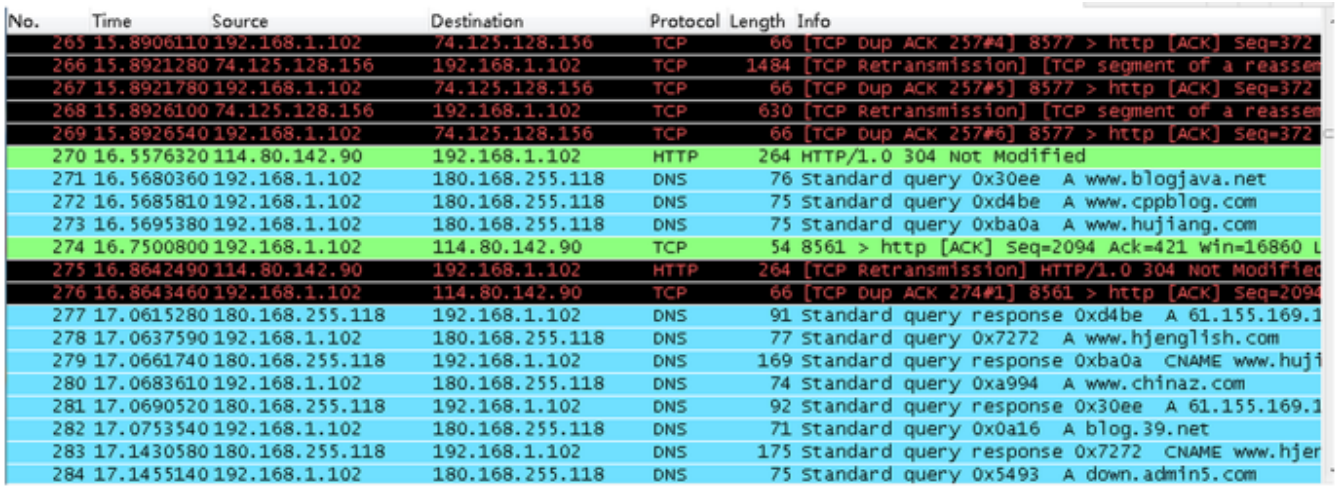
http.request.method == "GET" && http contains "User-Agent: "
http.request.method == "POST" && http contains "Host: "
http.request.method == "POST" && http contains "User-Agent: "
http contains "HTTP/1.1 200 OK" && http contains "Content-Type: "
http contains "HTTP/1.0 200 OK" && http contains "Content-Type: "

以下内容摘抄
自： http://www.cnblogs.com/TankXiao/archive/2012/10/10/2711777.html

封包列表(Packet List Pane)

封包列表的面板中显示： 编号、时间戳、源地址、目标地址、协议、长度、以及封包信息，不同的协议用了不同的颜色显示，也可以自己修改这些显示的颜色规则， view->coloring Rules。封标列表如下图所示



No.	Time	Source	Destination	Protocol	Length	Info
265	15.8906110	192.168.1.102	74.125.128.156	TCP	66	[TCP Dup ACK 257#4] 8577 > http [ACK] Seq=372
266	15.8921280	74.125.128.156	192.168.1.102	TCP	1484	[TCP Retransmission] [TCP segment of a reassem
267	15.8921780	192.168.1.102	74.125.128.156	TCP	66	[TCP Dup ACK 257#5] 8577 > http [ACK] Seq=372
268	15.8926100	74.125.128.156	192.168.1.102	TCP	630	[TCP Retransmission] [TCP segment of a reassem
269	15.8926540	192.168.1.102	74.125.128.156	TCP	66	[TCP Dup ACK 257#6] 8577 > http [ACK] Seq=372
270	16.5576320	114.80.142.90	192.168.1.102	HTTP	264	HTTP/1.0 304 Not Modified
271	16.5680360	192.168.1.102	180.168.255.118	DNS	76	Standard query 0x30ee A www.blogjava.net
272	16.5685810	192.168.1.102	180.168.255.118	DNS	75	Standard query 0xd4be A www.cppblog.com
273	16.5695380	192.168.1.102	180.168.255.118	DNS	75	Standard query 0xba0a A www.hujiang.com
274	16.7500800	192.168.1.102	114.80.142.90	TCP	54	8561 > http [ACK] Seq=2094 Ack=421 Win=16860 L
275	16.8642490	114.80.142.90	192.168.1.102	HTTP	264	[TCP Retransmission] HTTP/1.0 304 Not Modifie
276	16.8643460	192.168.1.102	114.80.142.90	TCP	66	[TCP Dup ACK 274#1] 8561 > http [ACK] Seq=2094
277	17.0615280	180.168.255.118	192.168.1.102	DNS	91	Standard query response 0xd4be A 61.155.169.1
278	17.0637590	192.168.1.102	180.168.255.118	DNS	77	Standard query 0x7272 A www.hjenglish.com
279	17.0661740	180.168.255.118	192.168.1.102	DNS	169	Standard query response 0xba0a CNAME www.huji
280	17.0683610	192.168.1.102	180.168.255.118	DNS	74	Standard query 0xa994 A www.chinaz.com
281	17.0690520	180.168.255.118	192.168.1.102	DNS	92	Standard query response 0x30ee A 61.155.169.1
282	17.0753540	192.168.1.102	180.168.255.118	DNS	71	Standard query 0x0a16 A blog.39.net
283	17.1430580	180.168.255.118	192.168.1.102	DNS	175	Standard query response 0x7272 CNAME www.hjer
284	17.1455140	192.168.1.102	180.168.255.118	DNS	75	Standard query 0x5493 A down.admin5.com

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，各行信息如下

Frame: 物理层的数据帧概括

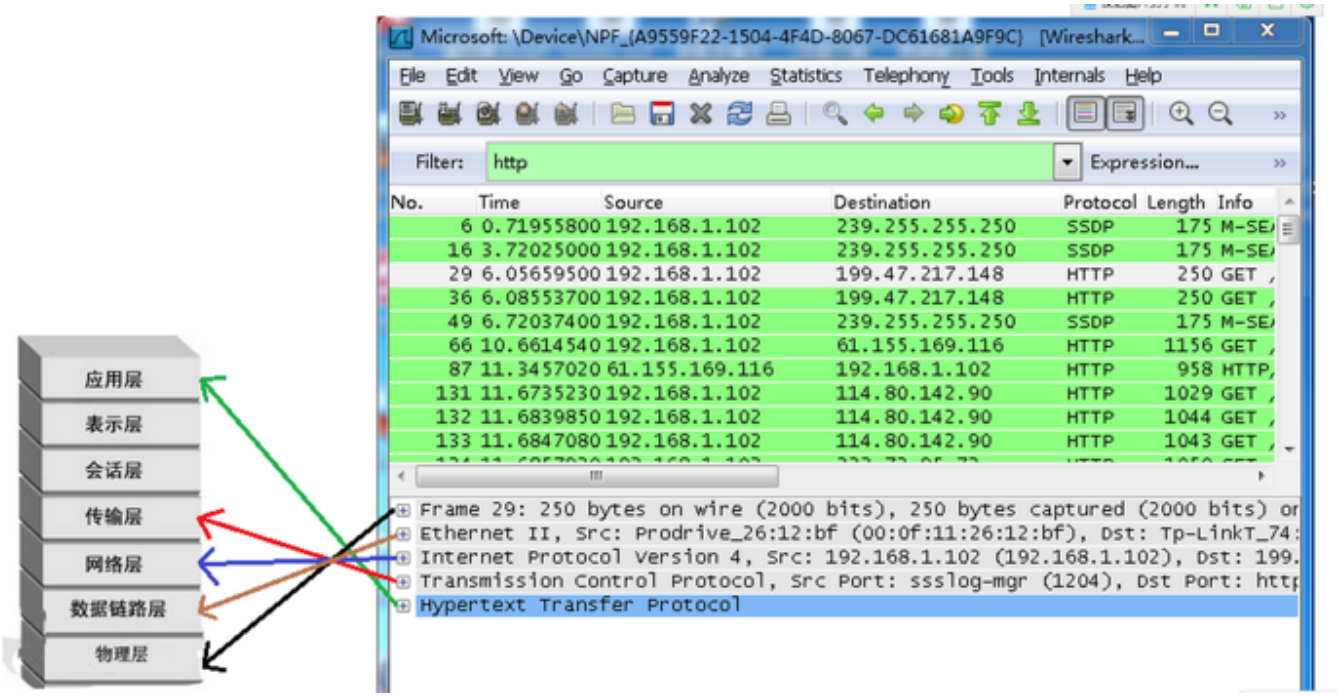
Ethernet II : 数据链路层以太网帧头部信息

Internet Protocol Version 4 : 互联网层IP包头部信息

Transmission Control protocol： 传输层T的数据头部信息，此处是TCP

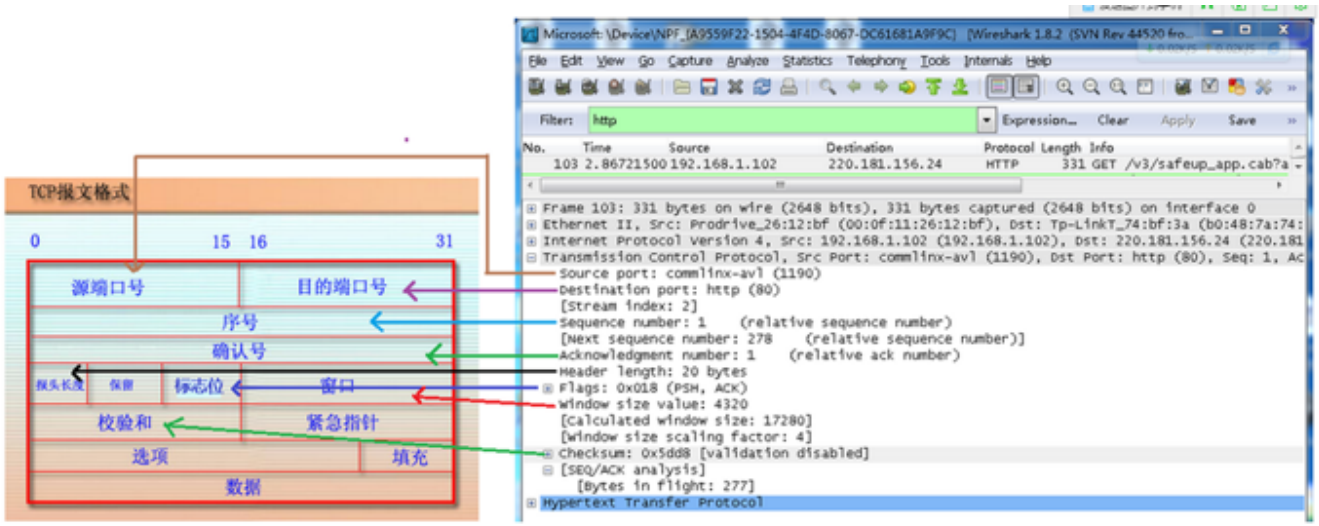
Hypertext Transfer Protocol: 应用层的信息，此处是HTTP协议

Wireshark与对应的OSI七层模型



TCP包具体内容

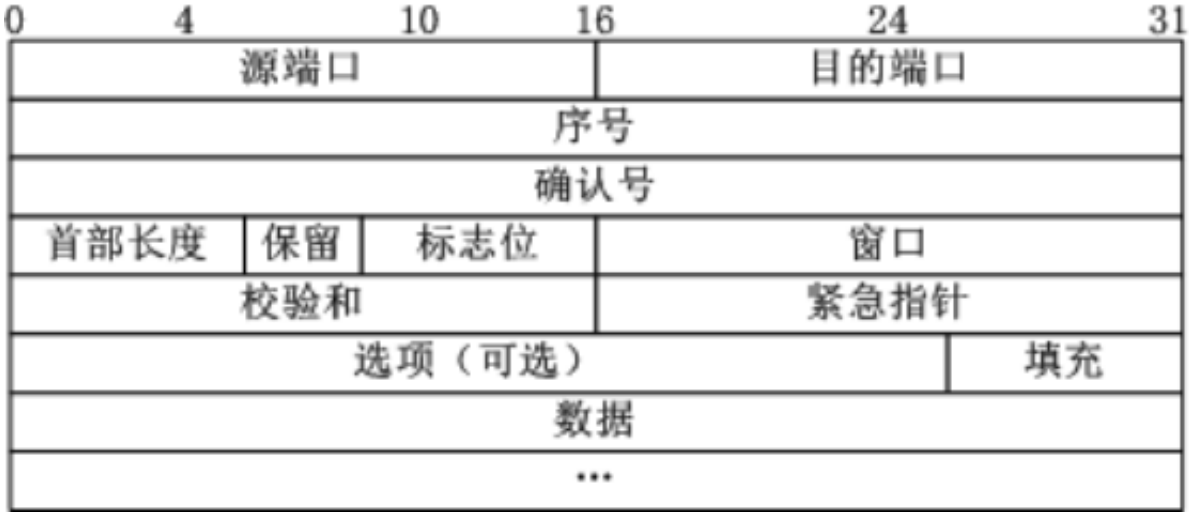
从下图可以看到wireshark捕获到的TCP包中的每个字段。



实例分析TCP三次握手过程

TCP报文格式

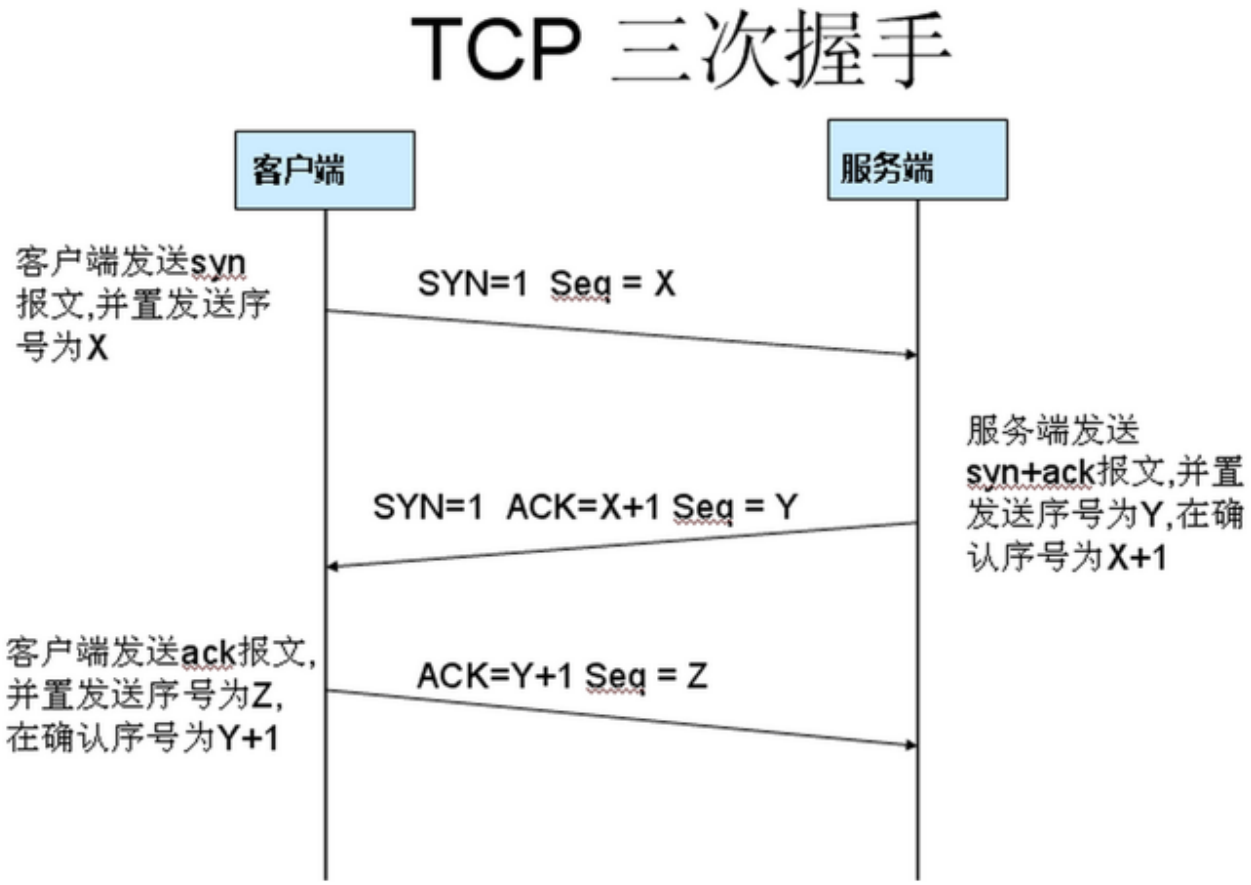
下面是TCP报文格式图



上图中有几个字段需要重点介绍下：

1、序号：Seq序号，占32位，用来标识从TCP源端向目的端发送的字节流，发起方发送数据时对此进行标记。
2、确认序号：Ack序号，占32位，只有ACK标志位为1时，确认序号字段才有效（Ack=Seq+1）。
3、标志位：共6个，即URG、ACK、PSH、RST、SYN、FIN等，具体含义如下：
（A）URG：紧急指针（urgent pointer）有效。
（B）ACK：确认序号有效。
（C）PSH：接收方应该尽快将这个报文交给应用层。
（D）RST：重置连接。
（E）SYN：发起一个新连接。
（F）FIN：释放一个连接。
需要注意的是：
（A）不要将确认序号Ack与标志位中的ACK搞混了。
（B）确认方的Ack=发起方的Seq+1，两端配对。

三次握手过程为

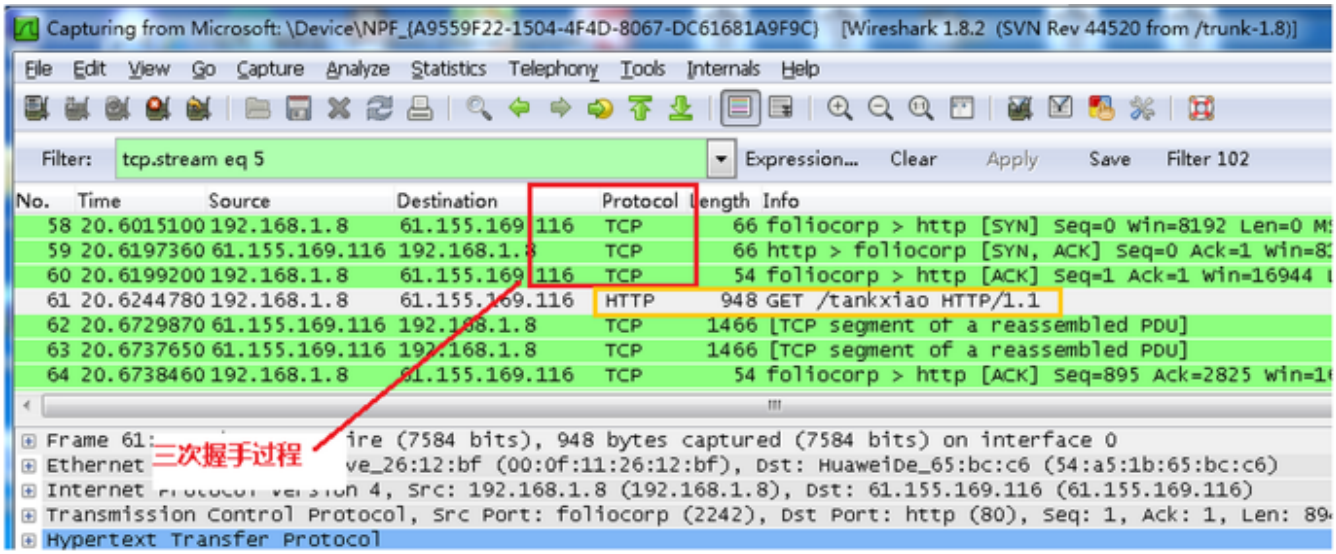


这图我都看过很多遍了， 这次我们用wireshark实际分析下三次握手的过程。

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

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",

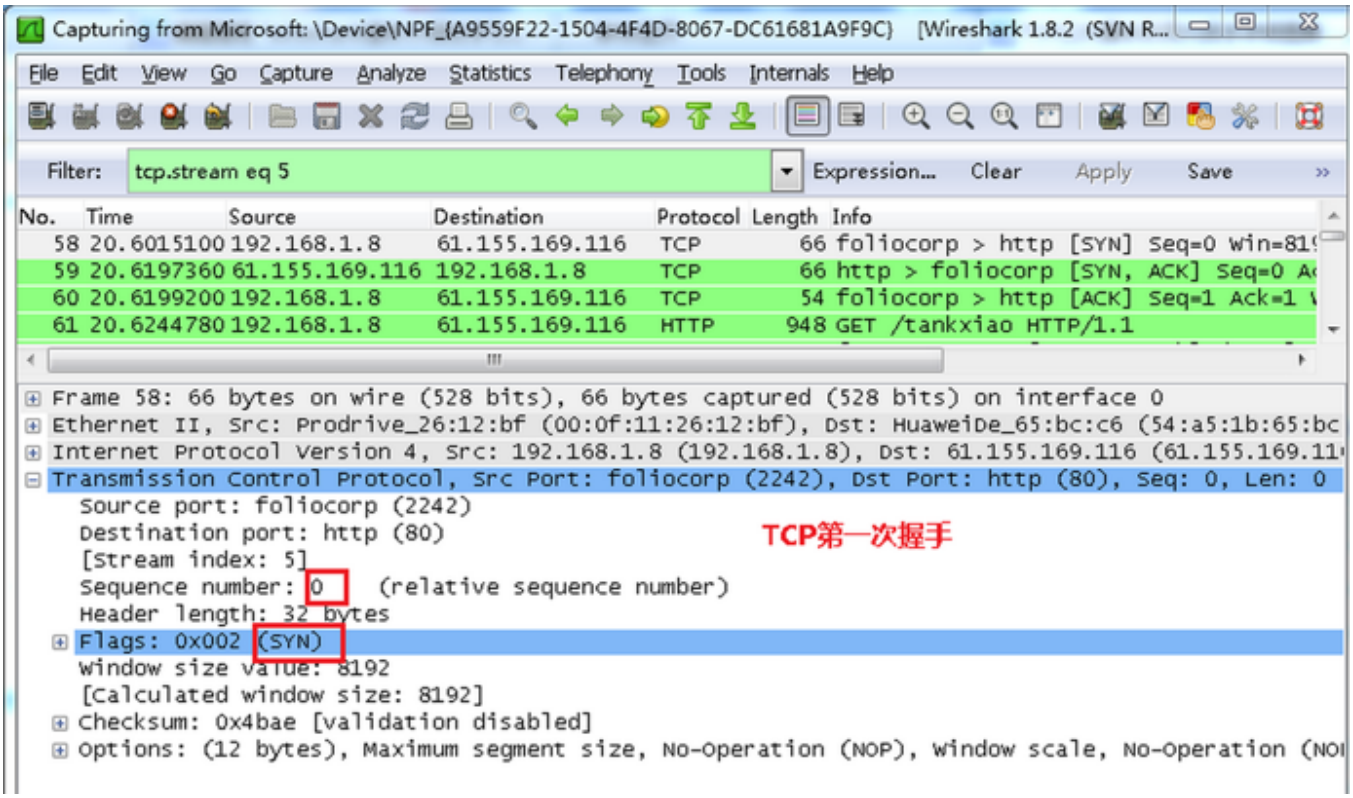
这样做的目的是为了得到与浏览器打开网站相关的数据包，将得到如下图



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

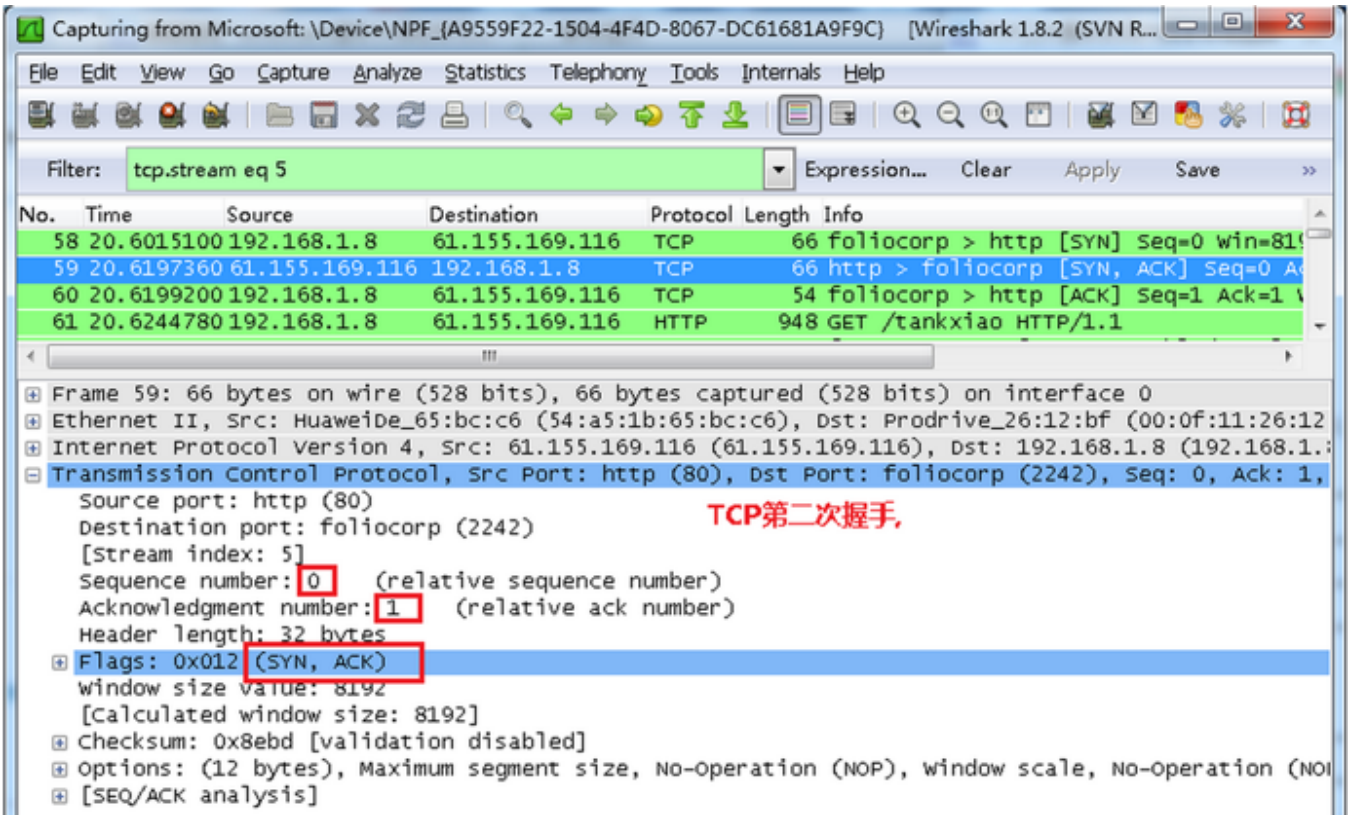
第一次握手数据包

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



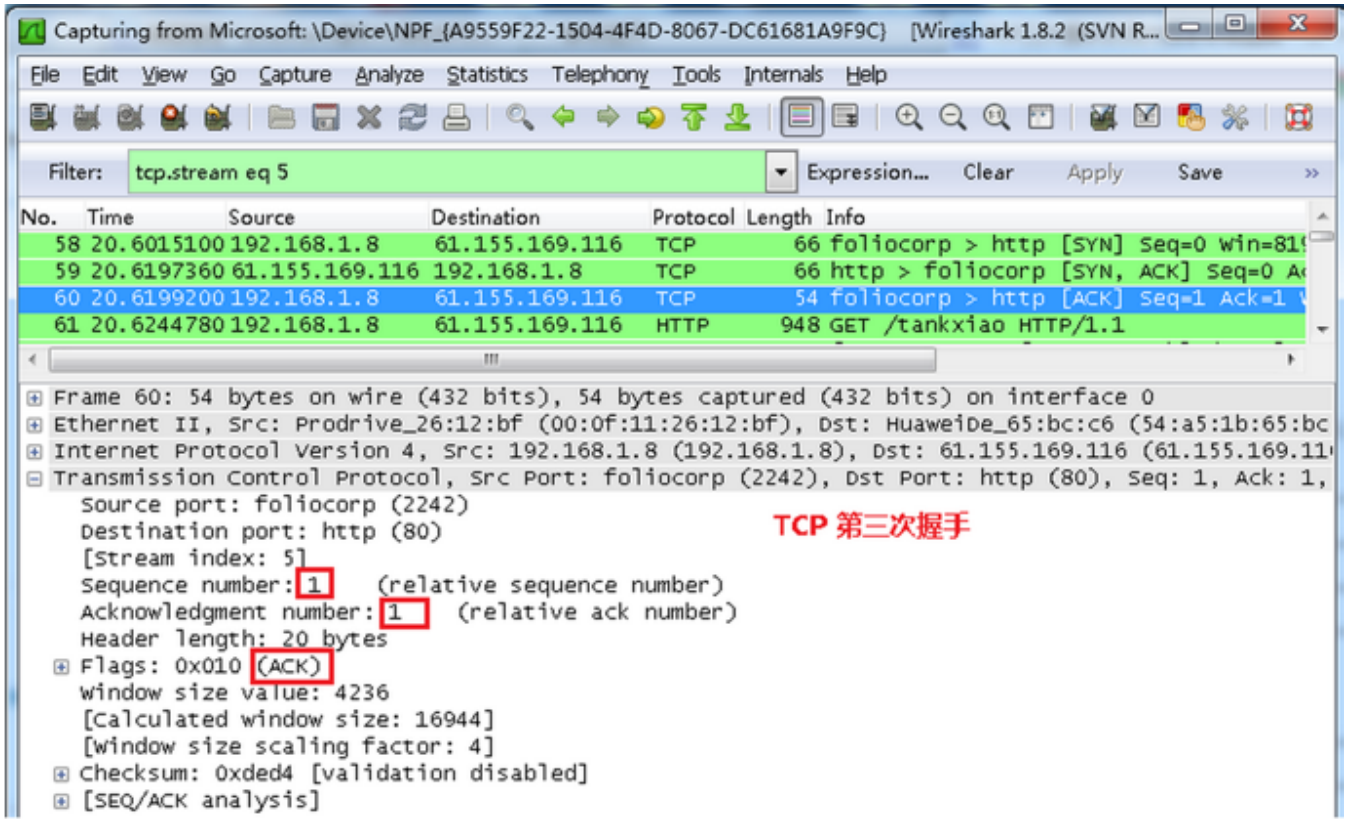
第二次握手的数据包

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:


Capturing from Microsoft: \Device\NPF_{A9559F22-1504-4F4D-8067-DC61681A9F9C} [Wireshark 1.8.2 (SVN R...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 5
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
58 20.6015100 192.168.1.8 61.155.169.116 TCP 66 foliocorp > http [SYN] Seq=0 Win=81
59 20.6197360 61.155.169.116 192.168.1.8 TCP 66 http > foliocorp [SYN, ACK] Seq=0 A
60 20.6199200 192.168.1.8 61.155.169.116 TCP 54 foliocorp > http [ACK] Seq=1 Ack=1
61 20.6244780 192.168.1.8 61.155.169.116 HTTP 948 GET /tankxiao HTTP/1.1
Frame 60: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Prodrive_26:12:bf (00:0f:11:26:12:bf), Dst: HuaweiDe_65:bc:c6 (54:a5:1b:65:bc
Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 61.155.169.116 (61.155.169.11
Transmission Control Protocol, Src Port: foliocorp (2242), Dst Port: http (80), Seq: 1, Ack: 1,
Source port: foliocorp (2242)
Destination port: http (80)
[Stream index: 5]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x010 (ACK)
Window size value: 4236
[Calculated window size: 16944]
[Window size scaling factor: 4]
Checksum: 0xded4 [validation disabled]
[SEQ/ACK analysis]
TCP 第三次握手