WireShark 使用教程

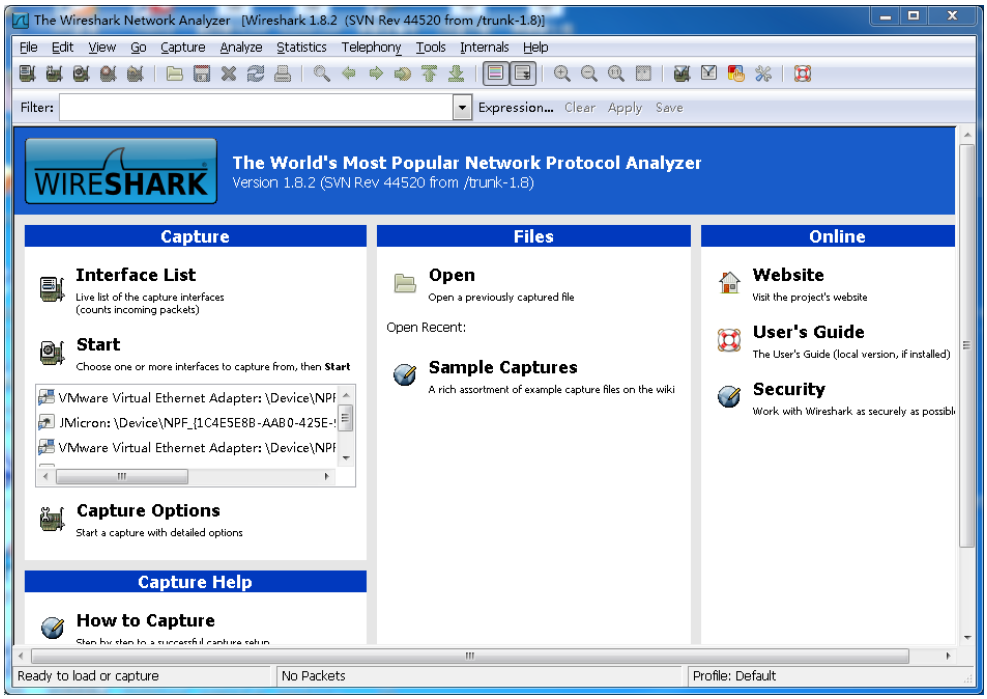
wireshark 是非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的详细信息。使用 wireshark 的人必须了解网络协议，否则就看不懂 wireshark 了。

为了安全考虑，wireshark 只能查看封包，而不能修改封包的容，或者发送封包。

wireshark 能获取 HTTP，也能获取 HTTPS，但是不能解密 HTTPS，所以 wireshark 看不懂 HTTPS 中的容，总结，如果是处理 HTTP,HTTPS 还是用 Fiddler，**其他协议比如 TCP,UDP 就用 wireshark.**

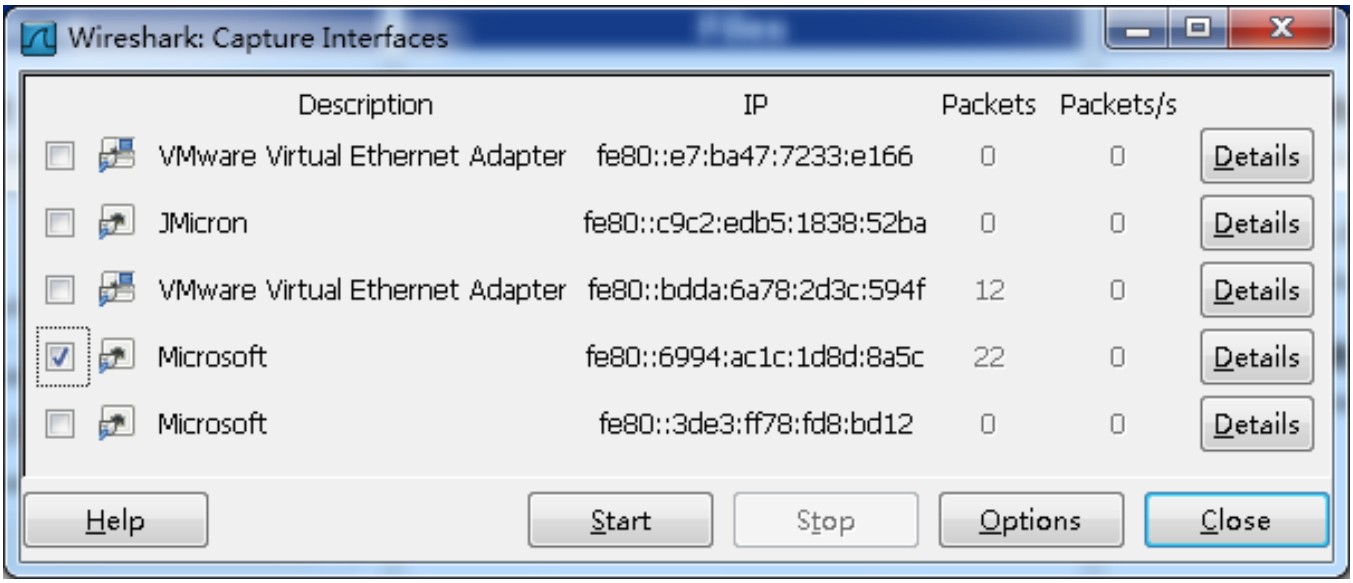
wireshark 开始抓包

开始界面

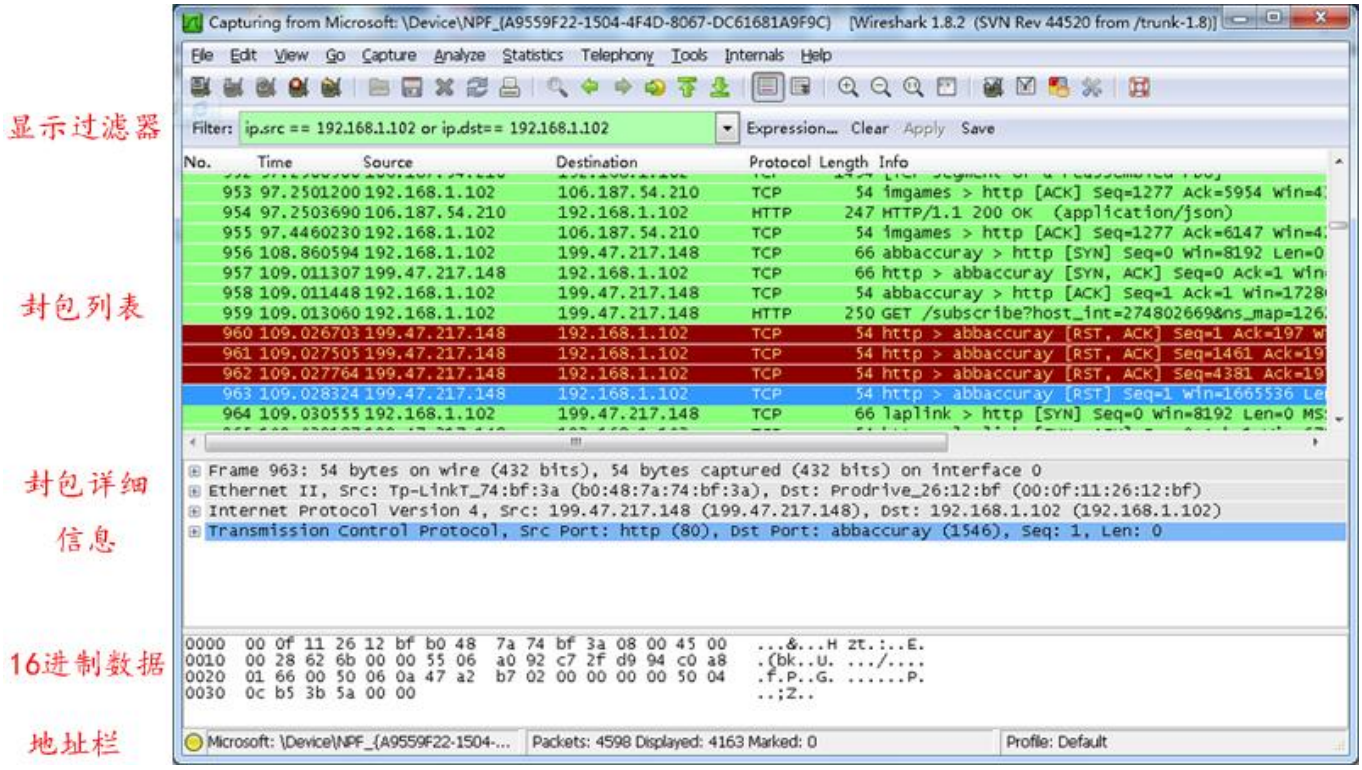


wireshark 是捕获机器上的某一块网卡的网络包，当你的机器上有多块网卡的时候，你需要选择一个网卡。

点击 Caputre->Interfaces.. 出现下面对话框，选择正确的网卡。然后点击"Start"按钮，开始抓包



Wireshark 窗口介绍



WireShark 主要分为这几个界面

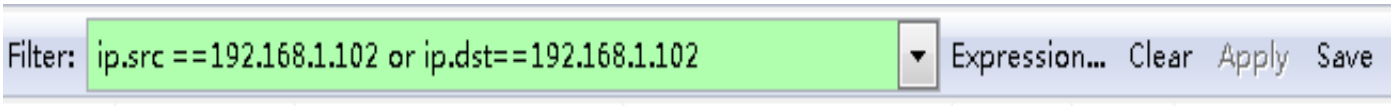
1. Display Filter(显示过滤器)， 用于过滤

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)



使用过滤是非常重要的， 初学者使用 wireshark 时，将会得到大量的冗余信息，在几千甚至几万条记录中，以至于很难找到自己需要的部分。搞得晕头转向。

过滤器会帮助我们在大量的数据中迅速找到我们需要的信息。

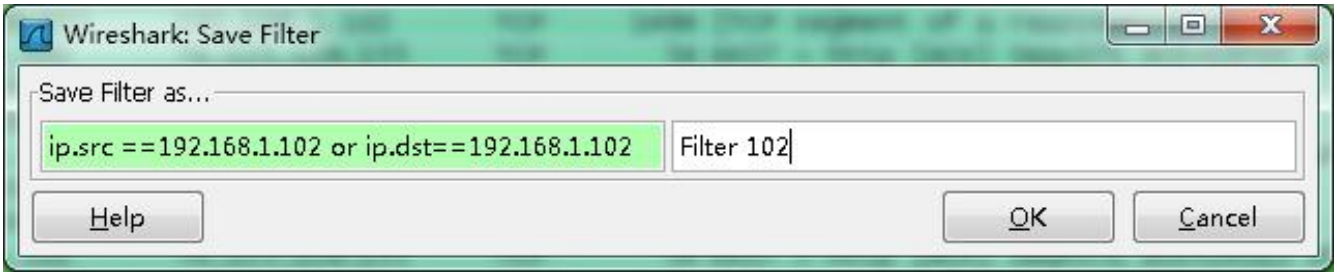
过滤器有两种，

一种是显示过滤器，就是主界面上那个，用来在捕获的记录中找到所需要的记录

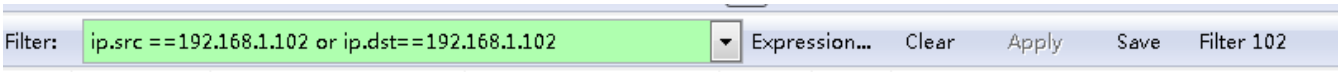
一种是捕获过滤器，用来过滤捕获的封包，以免捕获太多的记录。 在 Capture -> Capture Filters 中设置

保存过滤

在 Filter 栏上，填好 Filter 的表达式后，点击 Save 按钮， 取个名字。比如"Filter 102",



Filter 栏上就多了个"Filter 102" 的按钮。



过滤表达式的规则

表达式规则

1. 协议过滤

比如 TCP，只显示 TCP 协议。

2. IP 过滤

比如 ip.src ==192.168.1.102 显示源地址为 192.168.1.102，

ip.dst==192.168.1.102, 目标地址为 192.168.1.102

3. 端口过滤

tcp.port ==80, 端口为 80 的

tcp.srcport == 80, 只显示 TCP 协议的愿端口为 80 的。

4. Http 模式过滤

http.request.method=="GET", 只显示 HTTP GET 方法的。

5. 逻辑运算符为 AND/ OR

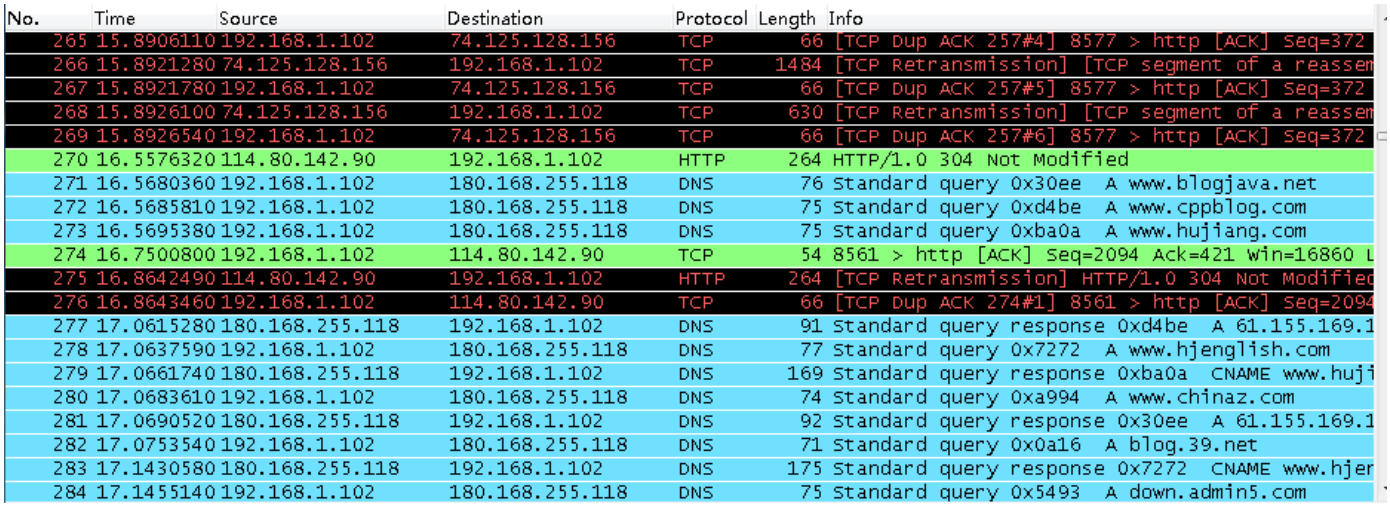
常用的过滤表达式

过滤表达式	用途
http	只查看 HTTP 协议的记录
ip.src ==192.168.1.102 or ip.dst==192.168.1.102	源地址或者目标地址是 192.168.1.102

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。 你可以看到不同的协议用了不同的颜色显示。

你也可以修改这些显示颜色的规则， View ->Coloring Rules.



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

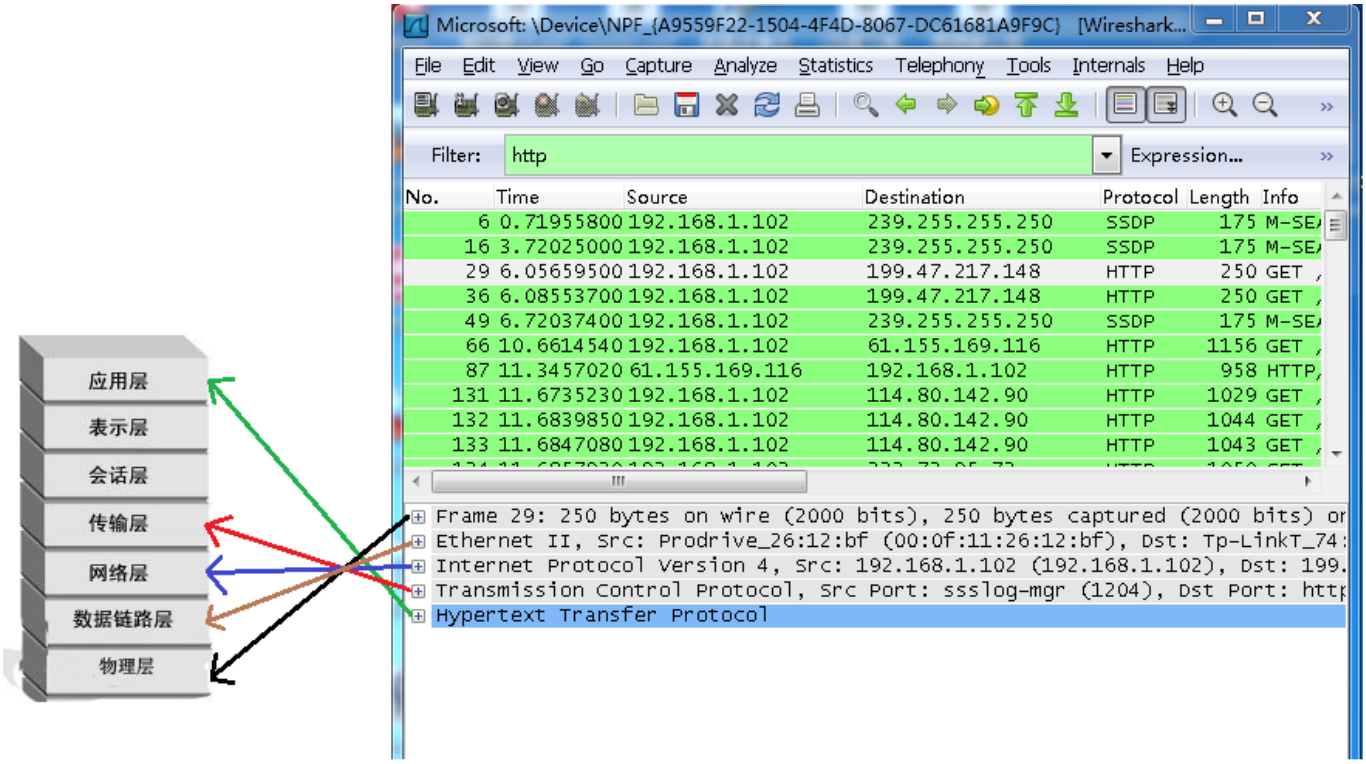
Frame: 物理层的数据帧概况

Ethernet II: 数据链路层以太网帧头部信息

Internet Protocol Version 4: 互联网层 IP 部信息

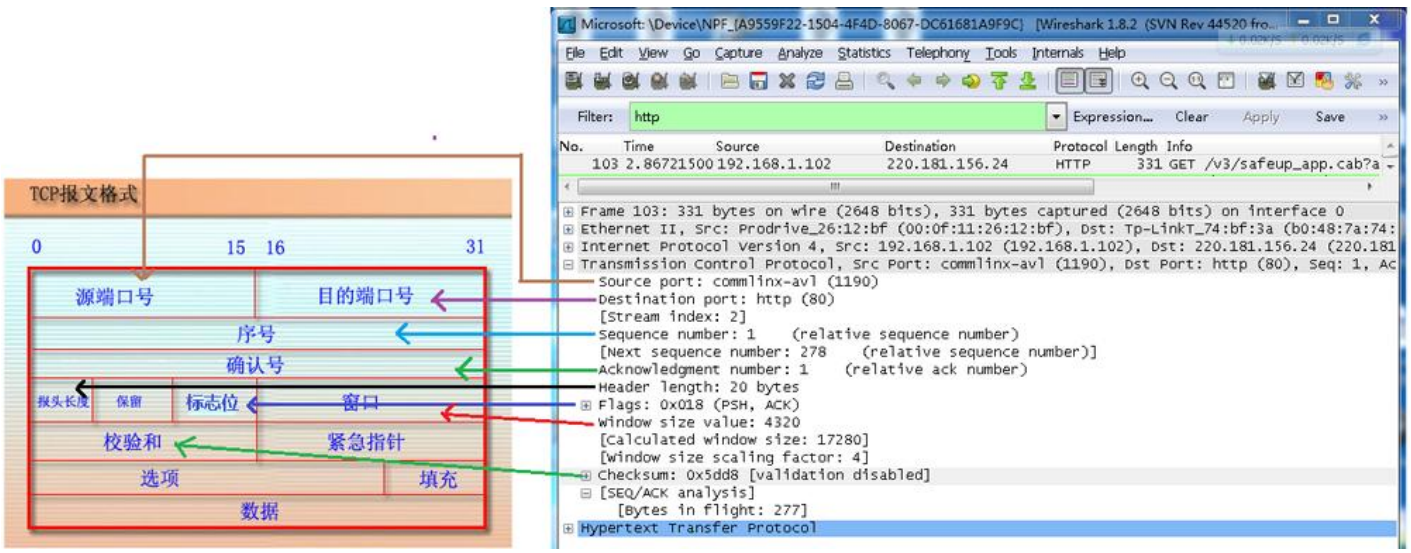
Transmission Control Protocol: 传输层 T 的数据段头部信息，此处是 TCP

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



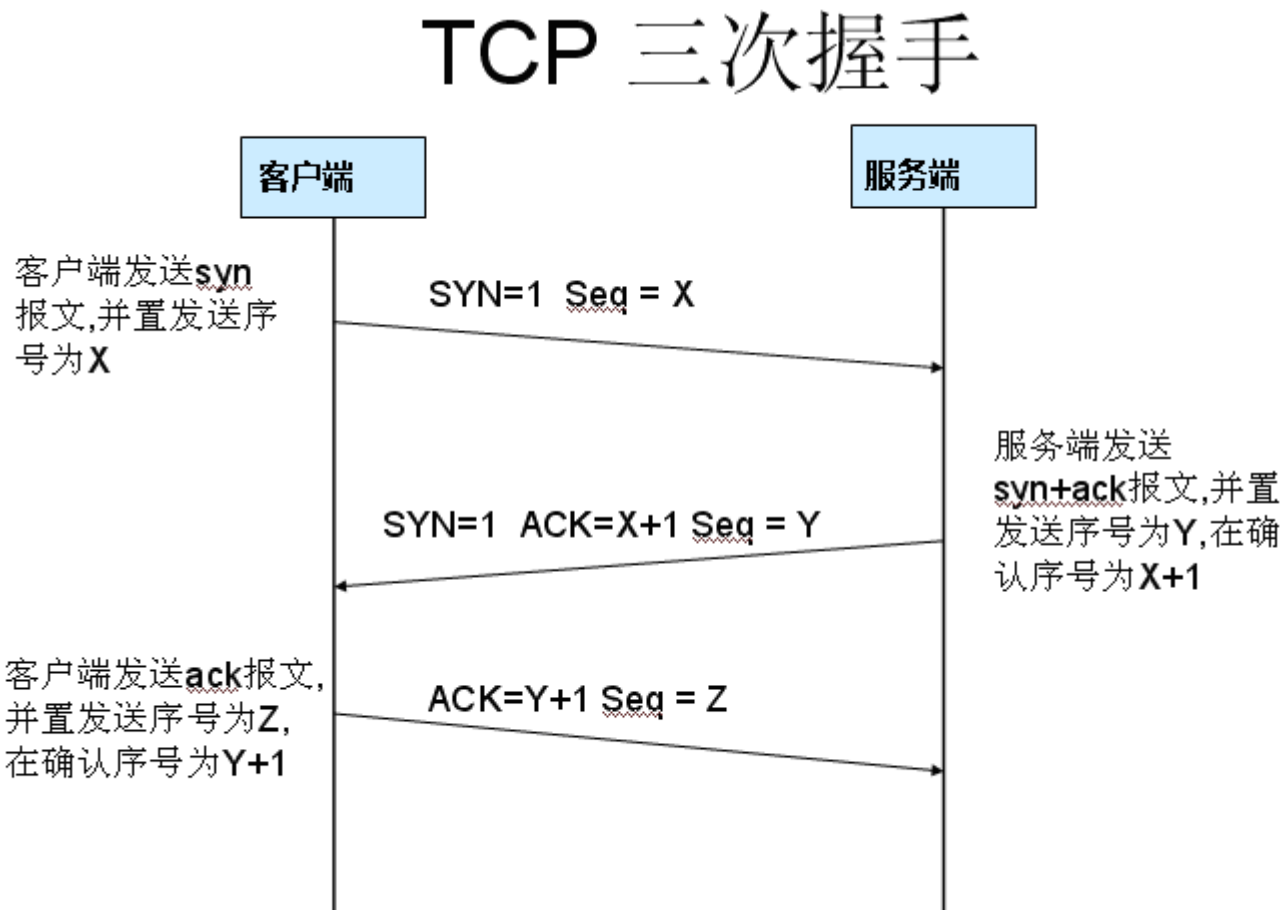
TCP 包的具体容

从下图可以看到 wireshark 捕获到的 TCP 包中的每个字段。



看到这， 基本上对 wireshak 有了初步了解， 现在我们看一个 TCP 三次握手的实例

三次握手过程为

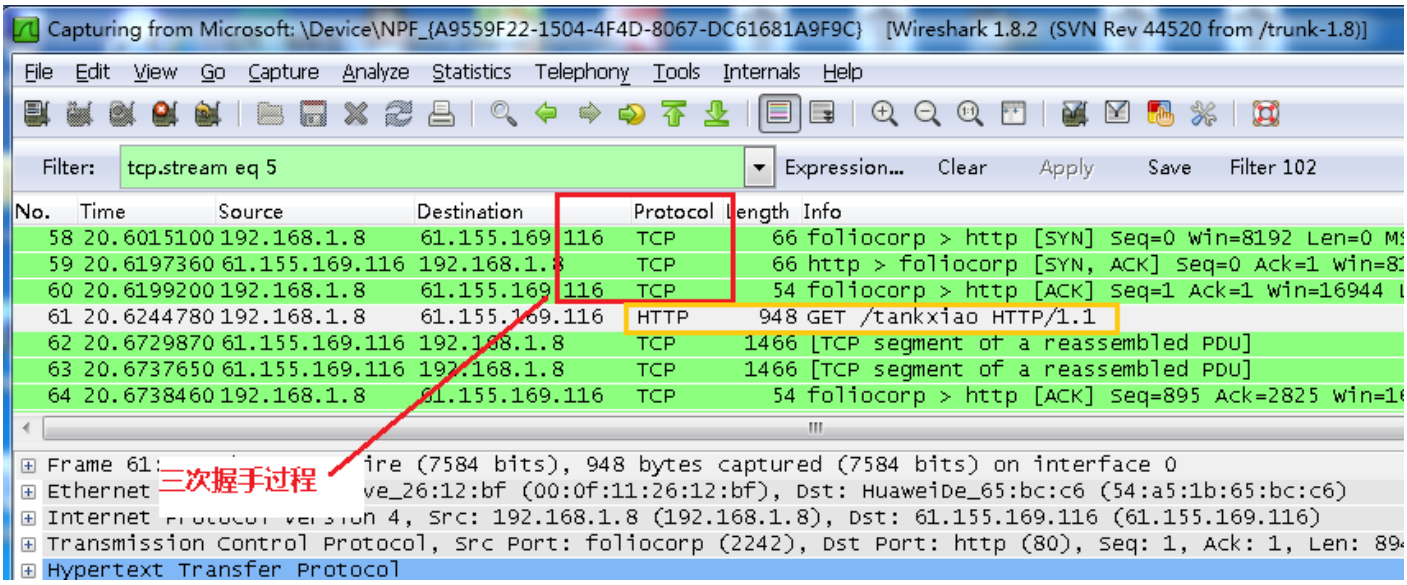


这图我都看过很多遍了， 这次我们用 wireshark 实际分析下三次握手的过程。

打开 wireshark，打开浏览器输入 .cr173.

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",

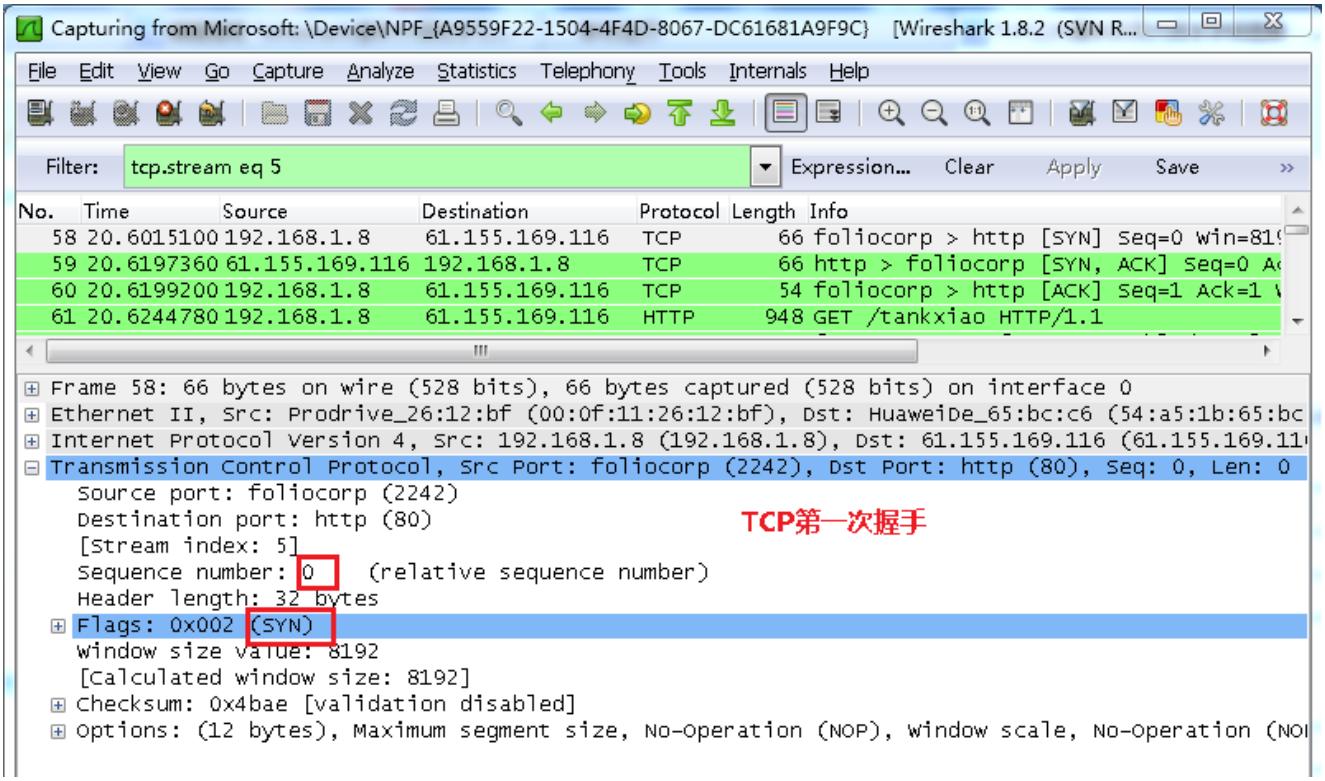
这样做的目的是为了得到与浏览器打开相关的数据包，将得到如下图



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。

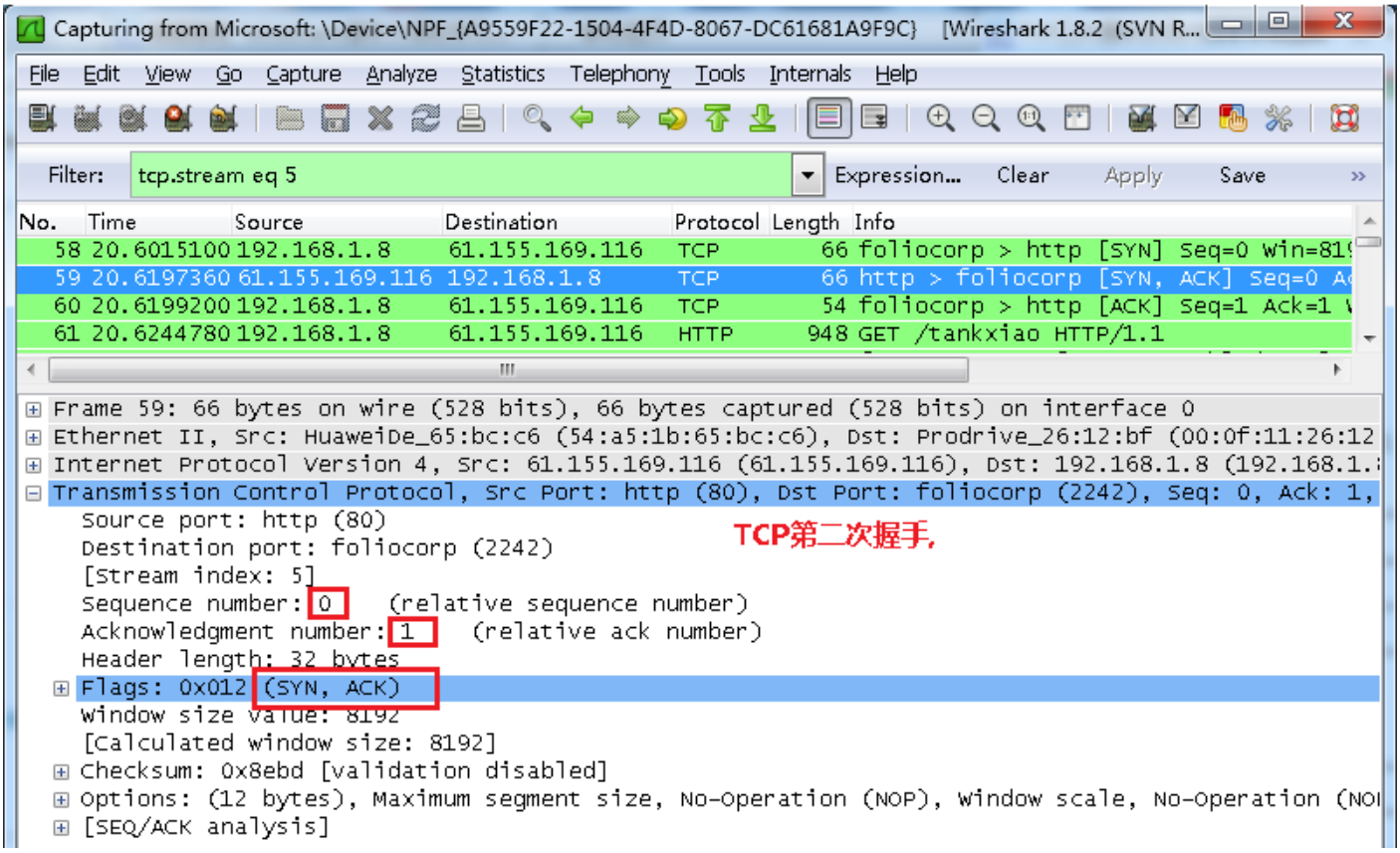
第一次握手数据包

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



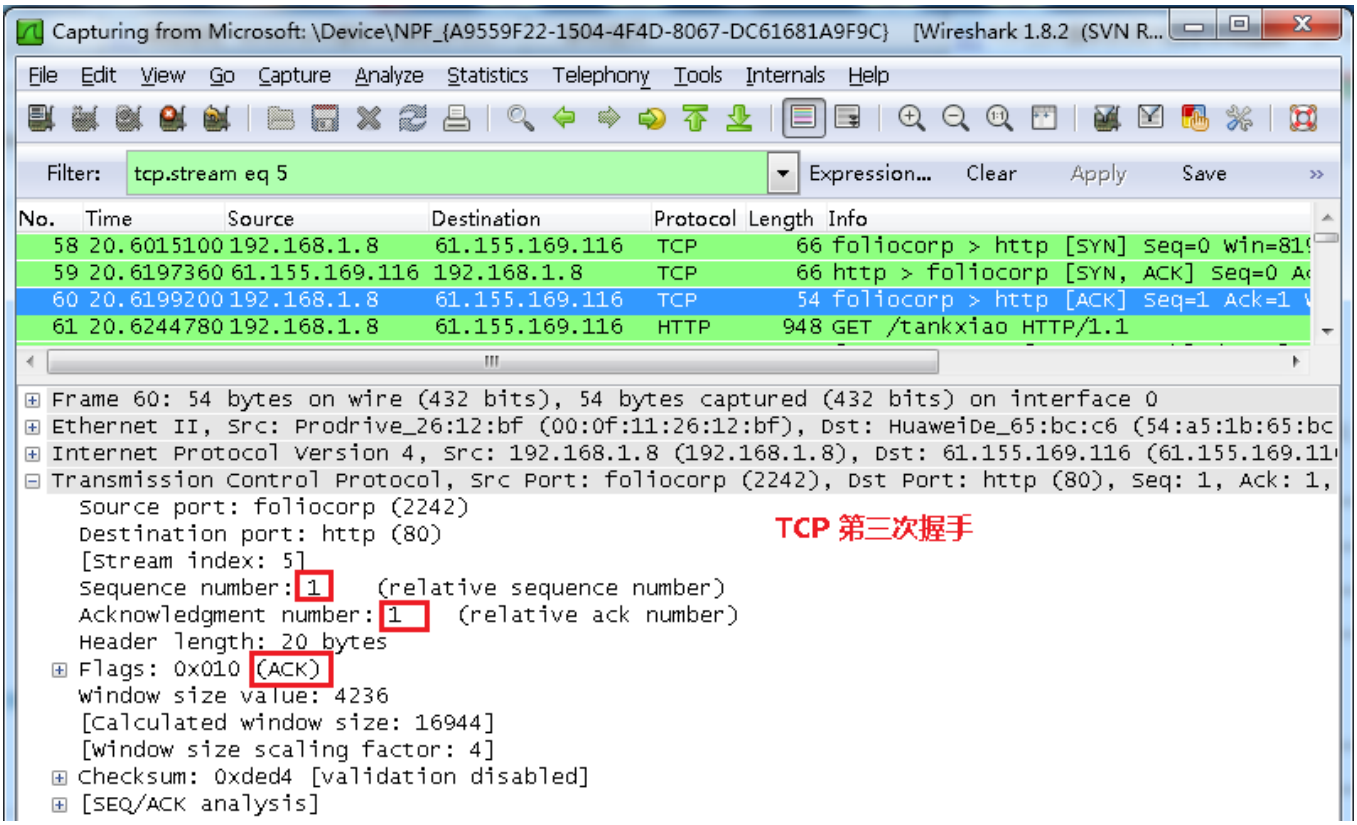
第二次握手的数据包

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