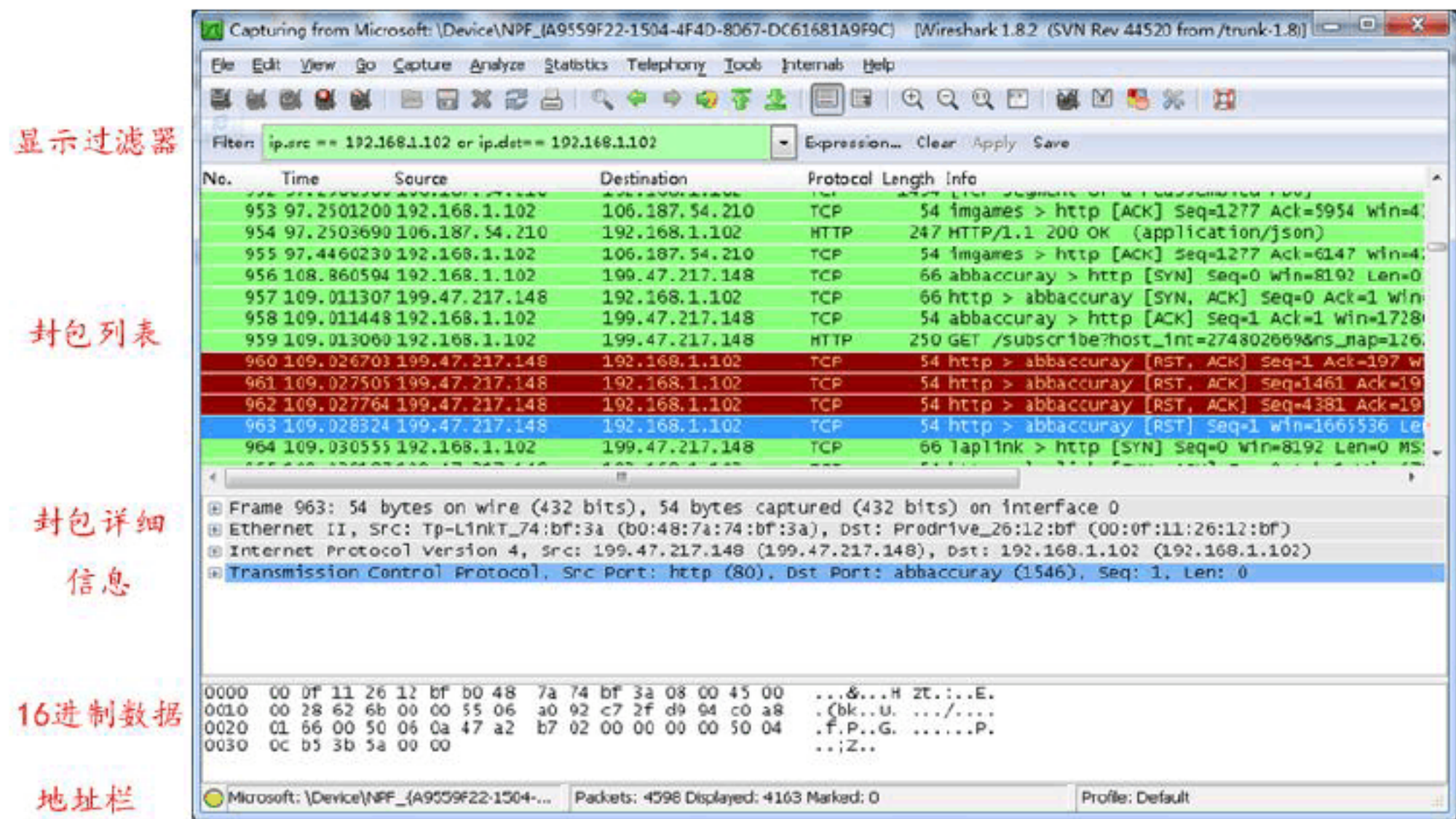


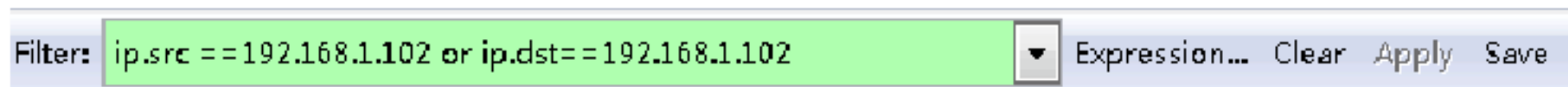
Wireshark 窗口介绍



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. Miscellaneous(地址栏, 杂项)

Wireshark 显示过滤



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。

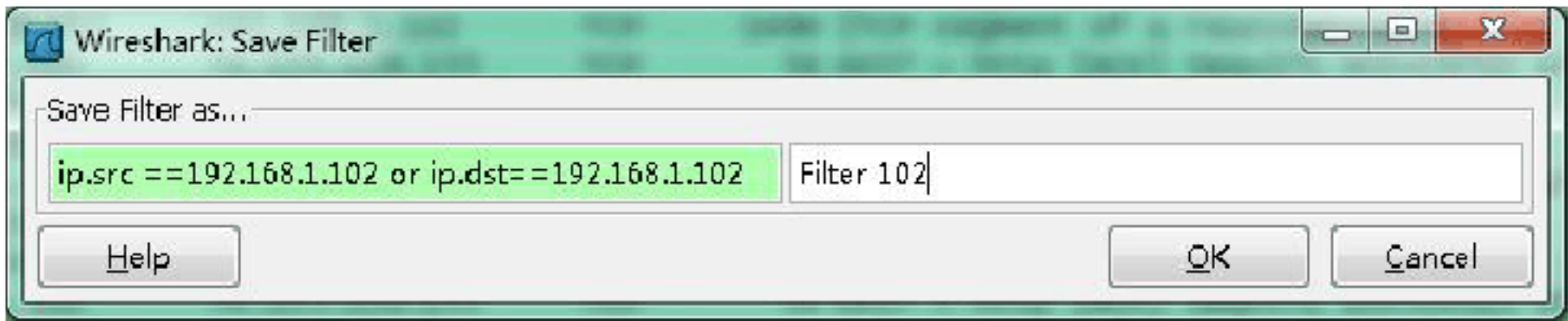
过滤器有两种,

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

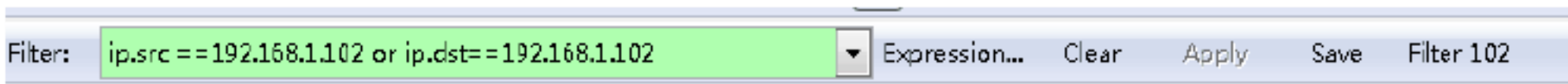
一种是捕获过滤器，用来过滤捕获的封包，以免捕获太多的记录。 在Capture -> Capture Filters 中设置

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 协议的源端口为 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 reassemb
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 reassemb
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 Modified
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

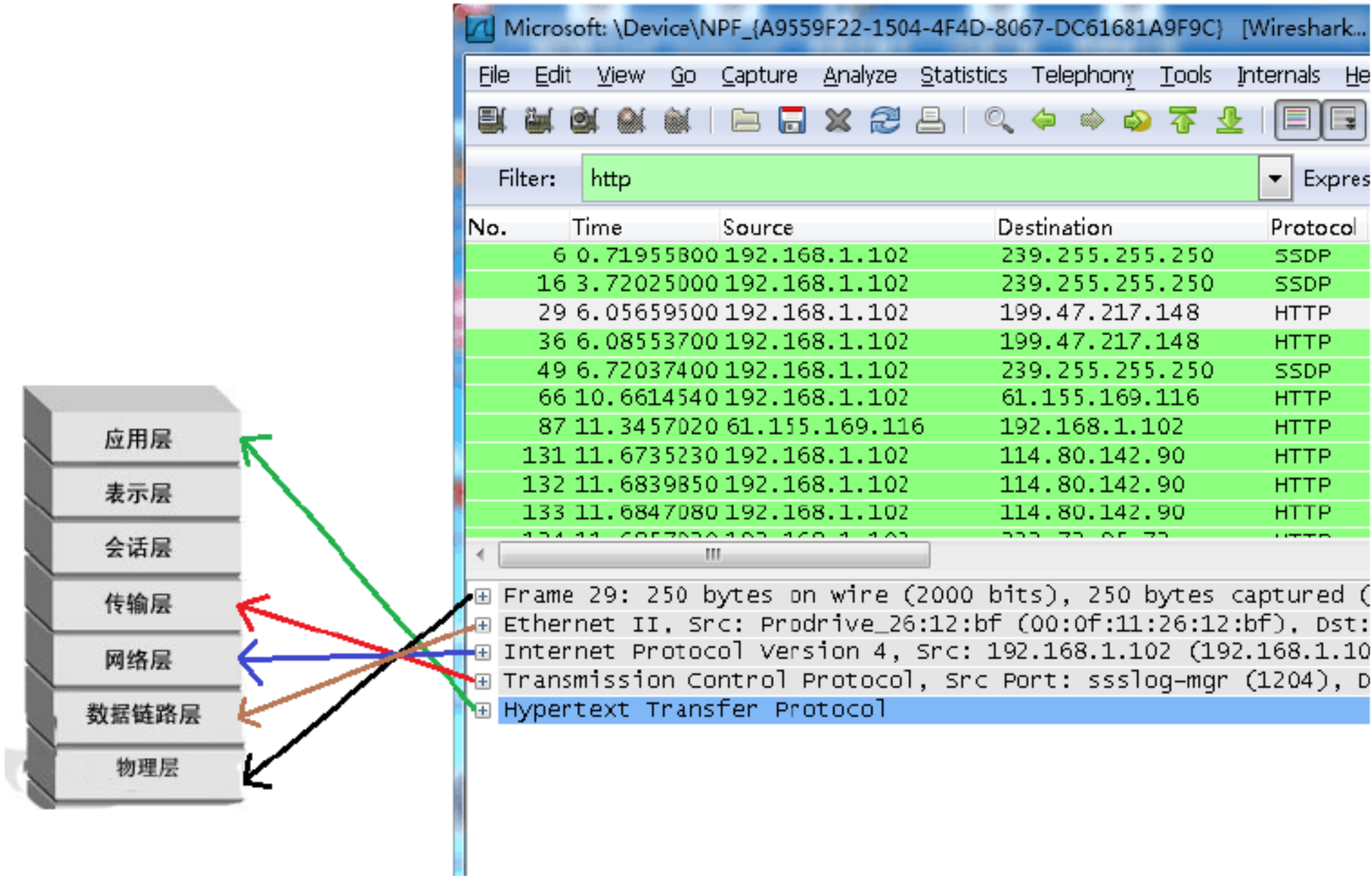
Ethernet II: 数据链路层以太网帧头部信息

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

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

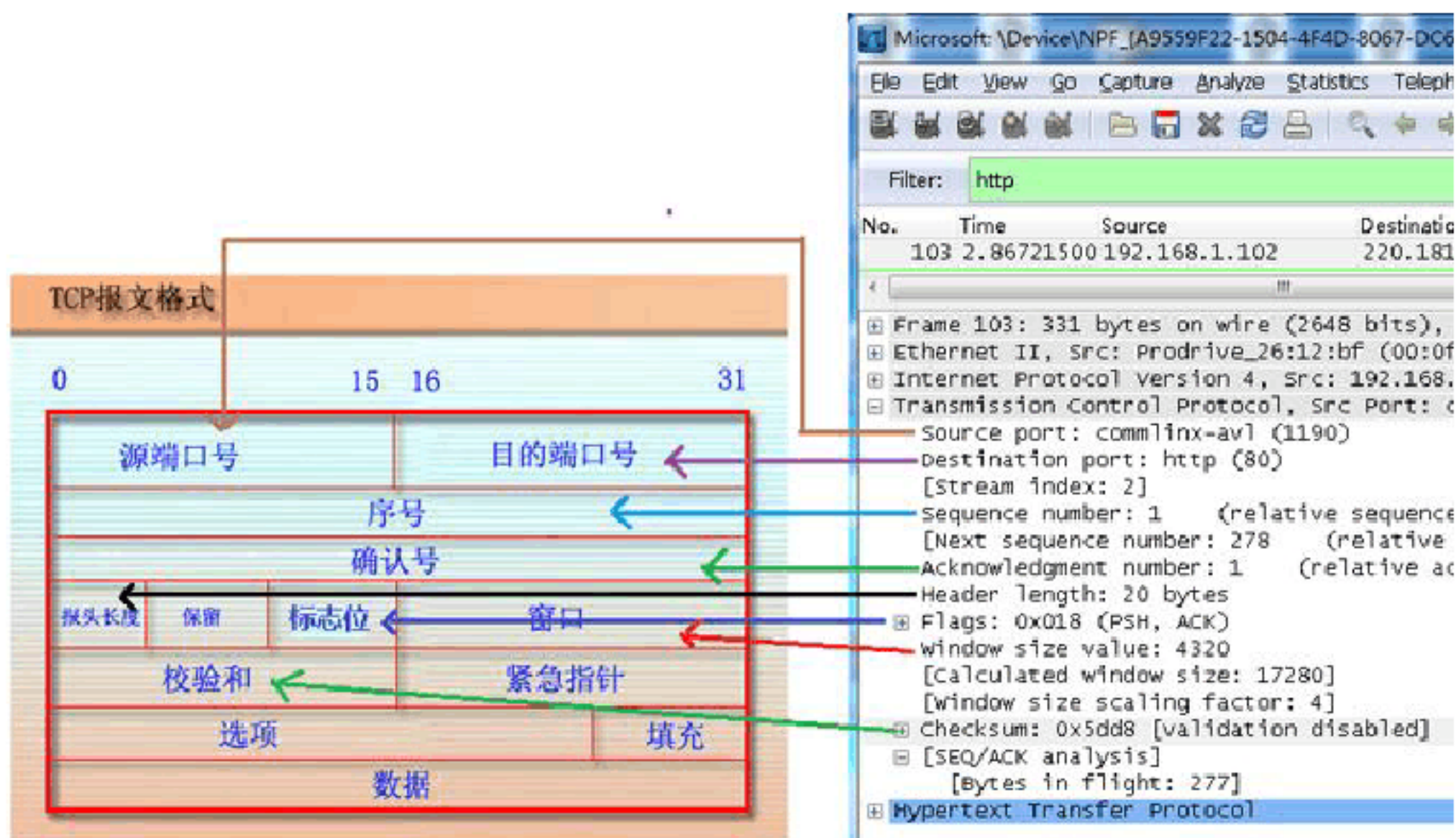
Hypertext Transfer Protocol: 应用层的信息，此处是 HTTP 协议

wireshark 与对应的 OSI 七层模型



TCP 包的具体内容

从下图可以看到wireshark 捕获到的TCP 包中的每个字段。

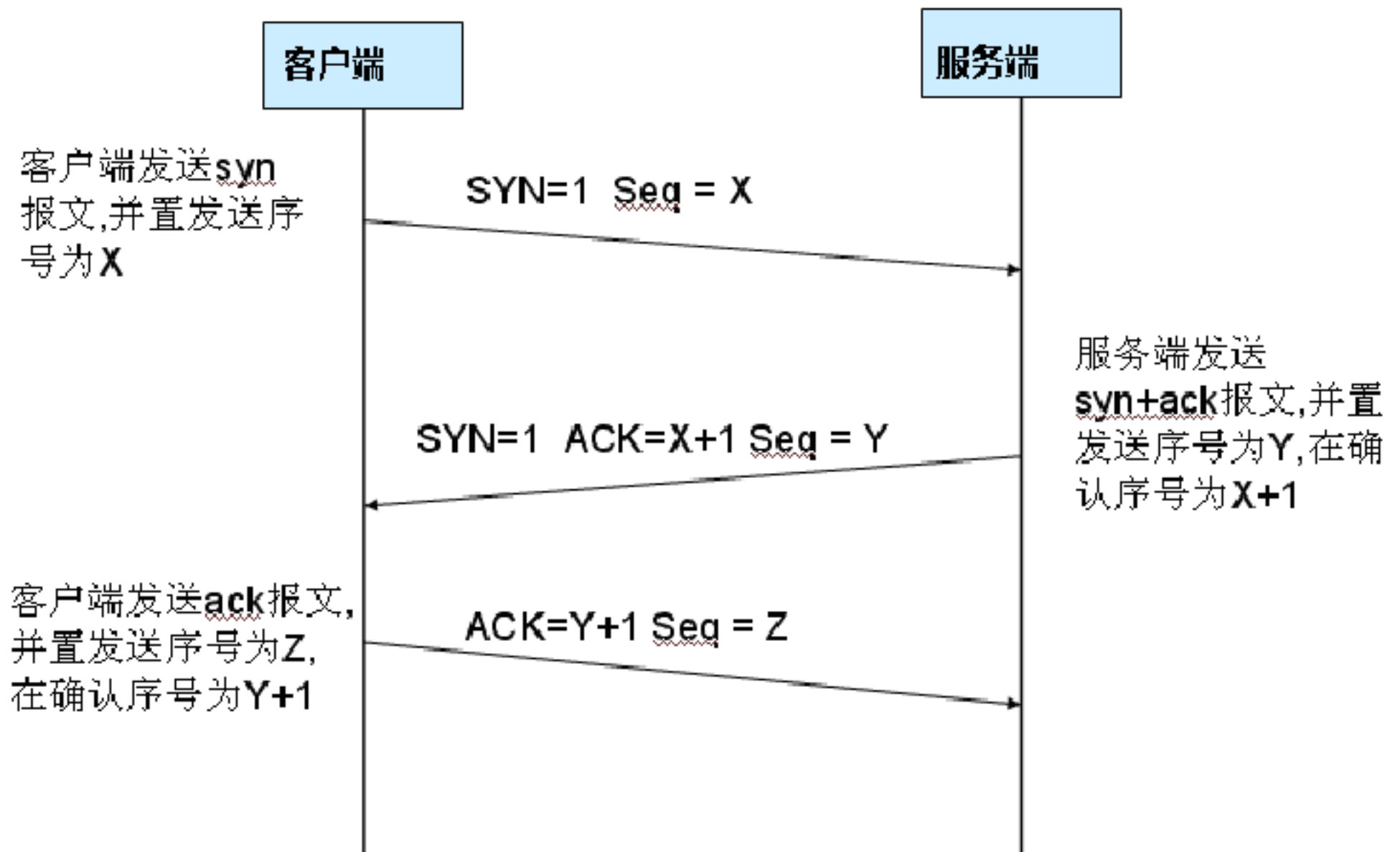


实例分析 TCP 三次握手过程

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

TCP 三次握手



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

Capturing from Microsoft: \Device\NPF_{A9559F22-1504-4F4D-8067-DC61681A9F9C} [Wireshark 1.8.2 (SVN)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 5 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
58	20.6015100	192.168.1.8	61.155.169.116	TCP	66	foliocorp > http [SYN]
59	20.6197360	61.155.169.116	192.168.1.8	TCP	66	http > foliocorp [SYN]
60	20.6199200	192.168.1.8	61.155.169.116	TCP	54	foliocorp > http [ACK]
61	20.6244780	192.168.1.8	61.155.169.116	HTTP	948	GET /tankxiao HTTP/1.1
62	20.6729870	61.155.169.116	192.168.1.8	TCP	1466	[TCP segment of a reass
63	20.6737650	61.155.169.116	192.168.1.8	TCP	1466	[TCP segment of a reass
64	20.6738460	192.168.1.8	61.155.169.116	TCP	54	foliocorp > http [ACK]

Frame 61: Ethernet II, Src: HuaweiDe_26:12:bf (00:0f:11:26:12:bf), Dst: HuaweiDe_65:bc:c6 (00:0f:11:26:12:bf), Length: 948, Protocol: Hypertext Transfer Protocol

三次握手过程

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

Capturing from Microsoft: \Device\NPF_{A9559F22-1504-4F4D-8067-DC61681A9F9C} [Wireshark 1.8.2 (SVN)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 5 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
58	20.6015100	192.168.1.8	61.155.169.116	TCP	66	foliocorp > http [SYN]
59	20.6197360	61.155.169.116	192.168.1.8	TCP	66	http > foliocorp [SYN,
60	20.6199200	192.168.1.8	61.155.169.116	TCP	54	foliocorp > http [ACK]
61	20.6244780	192.168.1.8	61.155.169.116	HTTP	948	GET /tankxiao HTTP/1.1

Frame 58: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface

Ethernet II, Src: Prodrive_26:12:bf (00:0f:11:26:12:bf), Dst: HuaweiDe_65:bc:c6

Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 61.155.169.116

Transmission Control Protocol, Src Port: foliocorp (2242), Dst Port: http (80),

Source port: foliocorp (2242)

Destination port: http (80)

[Stream index: 5]

Sequence number: 0 (relative sequence number)

Header length: 32 bytes

Flags: 0x002 (SYN)

Window size value: 8192

[Calculated window size: 8192]

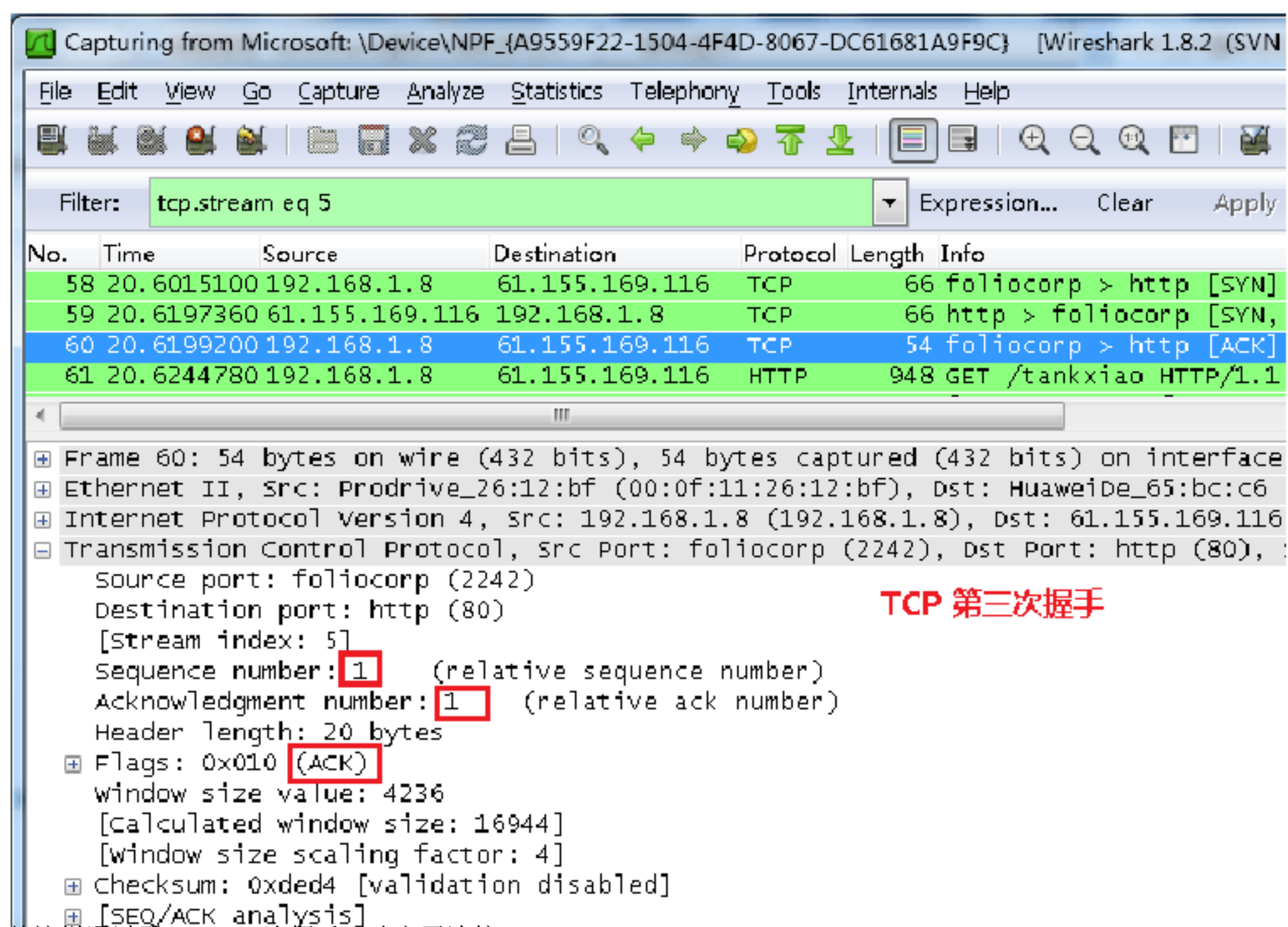
Checksum: 0x4bae [validation disabled]

Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, N

TCP第一次握手

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ISN 加 1 以.即 $0+1=1$, 如下图



TCP 第三次握手

就这样通过了 TCP 三次握手，建立了连接

<http://www.cnblogs.com/TankXiao/archive/2012/10/10/2711777.html>

1. 设置过滤条件

【1】 `http and ip.addr == 192.168.1.106 and tcp.port == 8080`

【a】 `http`: 指定网络协议

【b】 `ip.addr == 192.168.1.106`: 指定服务器 ip 地址，请根据实际情况替换。

【c】 `tcp.port == 8080`，指定端口号，请根据实际情况替换。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
<https://d.book118.com/556151144223010145>