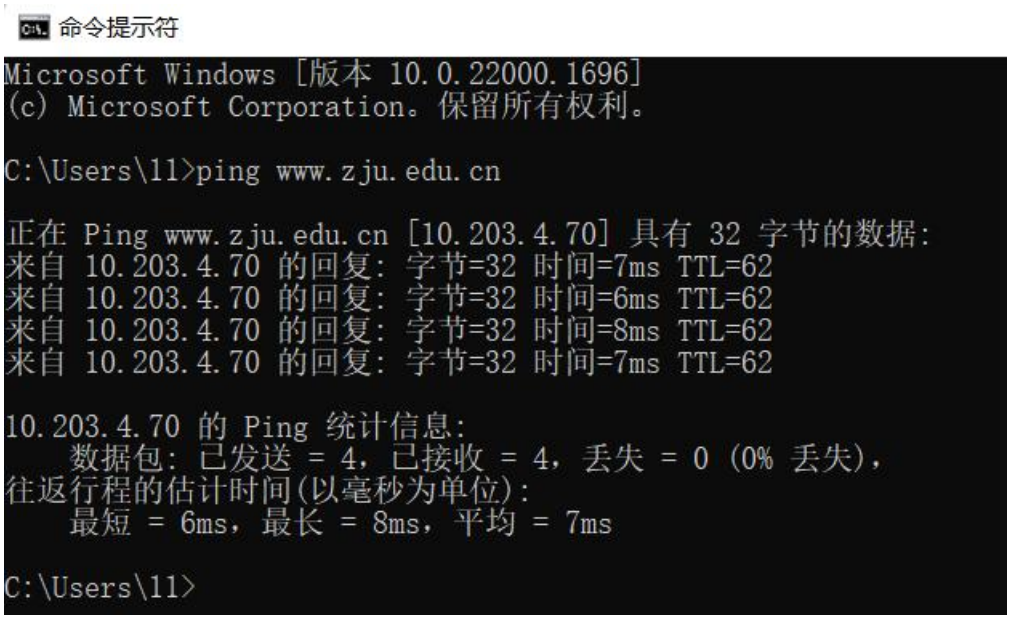
## HW4:Using Wireshark

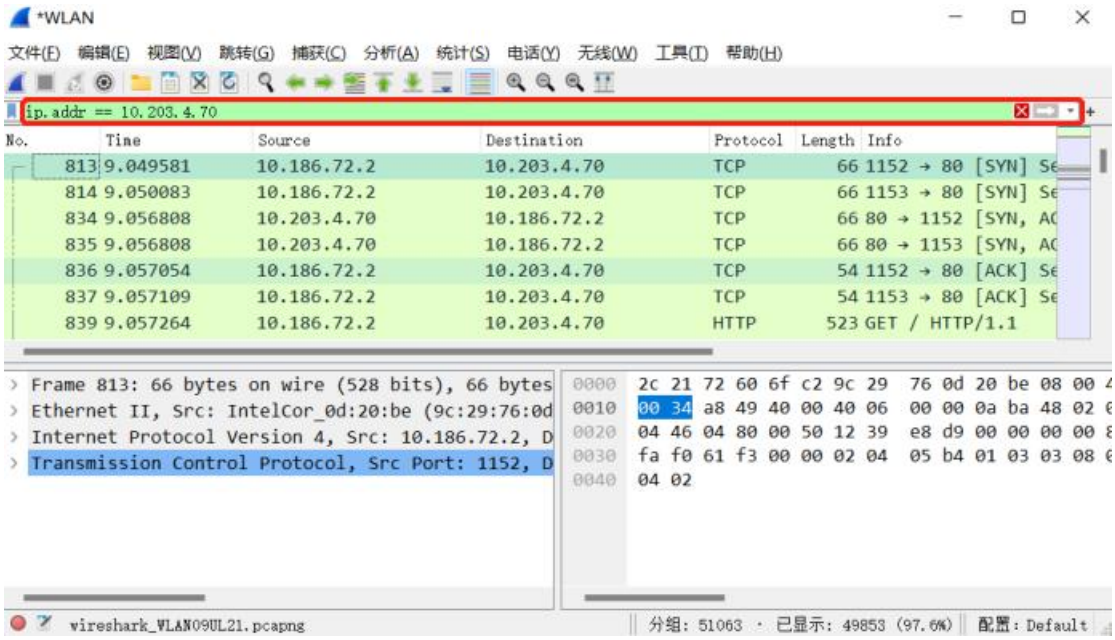
### 一、获取抓包网站的 IP 地址




### 二、清楚浏览器缓存

## 三、设置显示过滤器

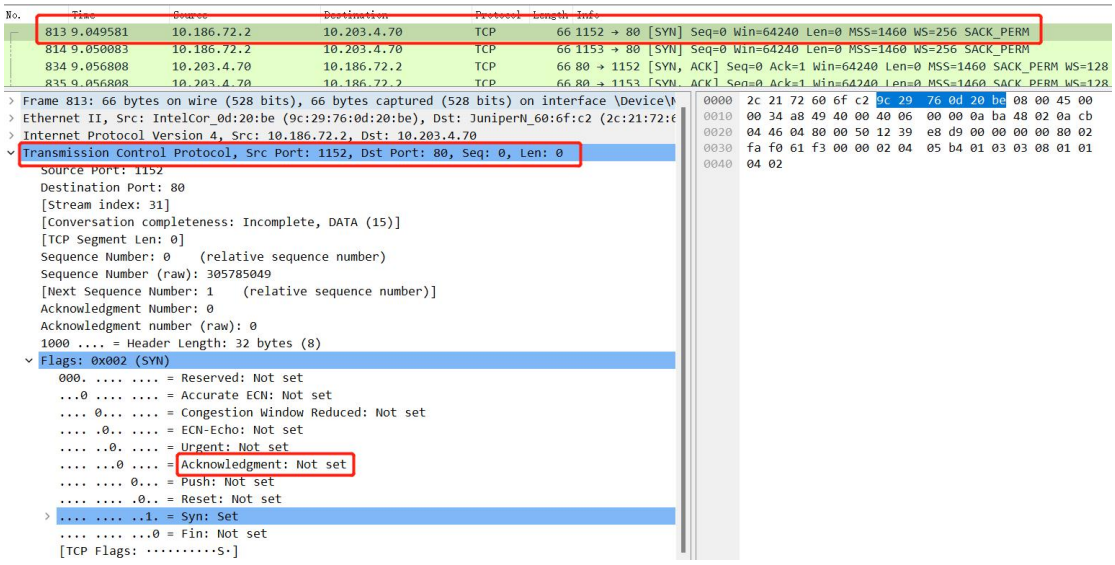
*在红框内输入 ip.addr == 10.203.4.70，使抓取的包只和 www.zju.edu.cn 有关*



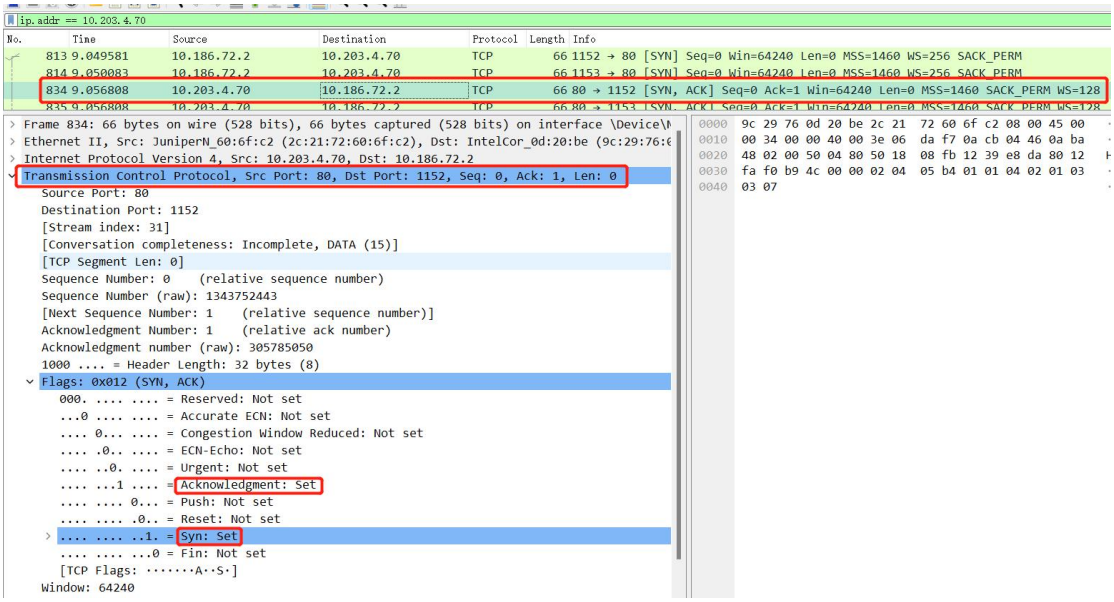

## 四、数据分析

### 1、TCP 的建立（三次握手协议）

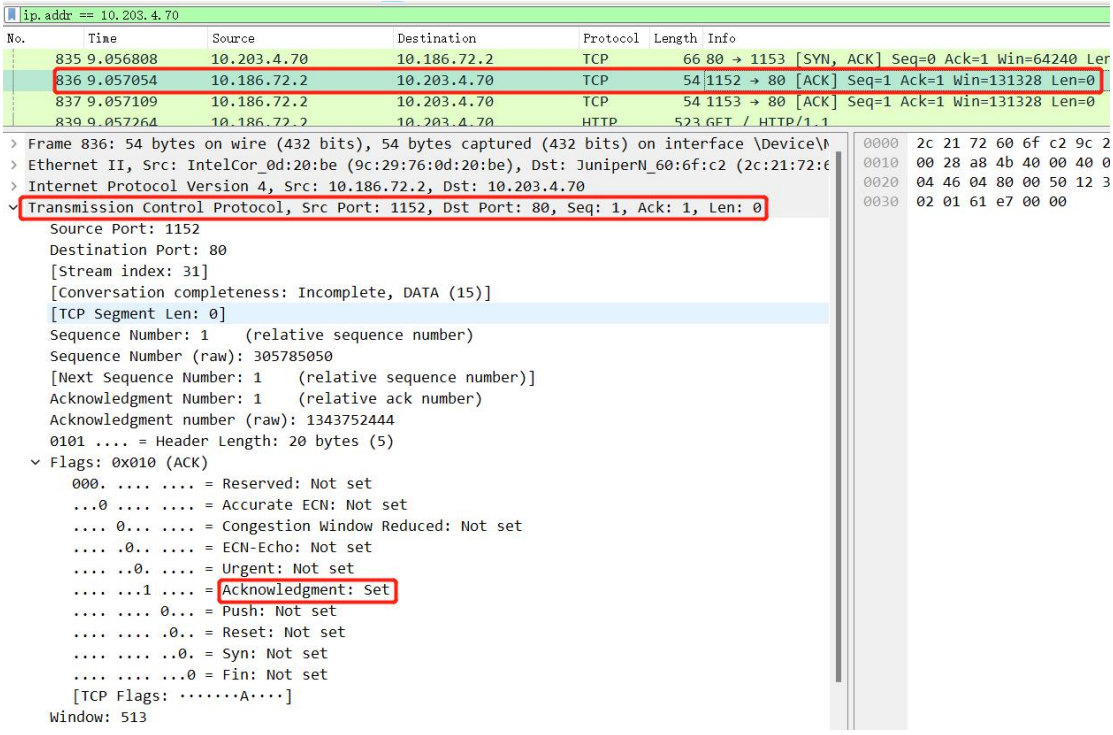
**阶段一：**客户端给服务器发送一个 SYN 段(在 TCP 标头中 SYN 位字段为 1 的 TCP/IP 数据包)，该段中也包含客户端的初始序列号，同时，该阶段的 ACK 为 Not set 状态，SYN 为 set 状态。



**阶段二：**服务器返回客户端 SYN +ACK 段(在 TCP 标头中 SYN 和 ACK 位字段都为 1 的 TCP/IP 数据包)， 该段中包含服务器的初始序列号；同时使 Acknowledgment 为 Set 状态来表示确认已收到客户端的 SYN 段。

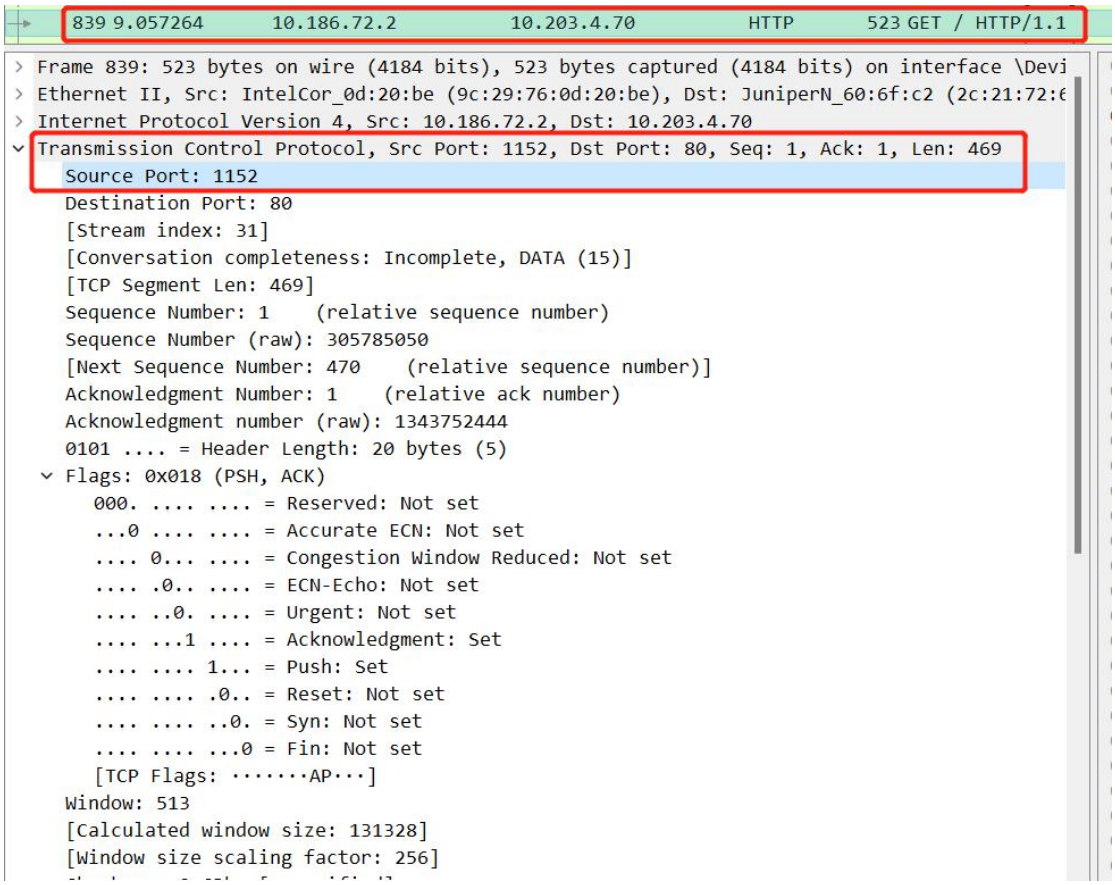


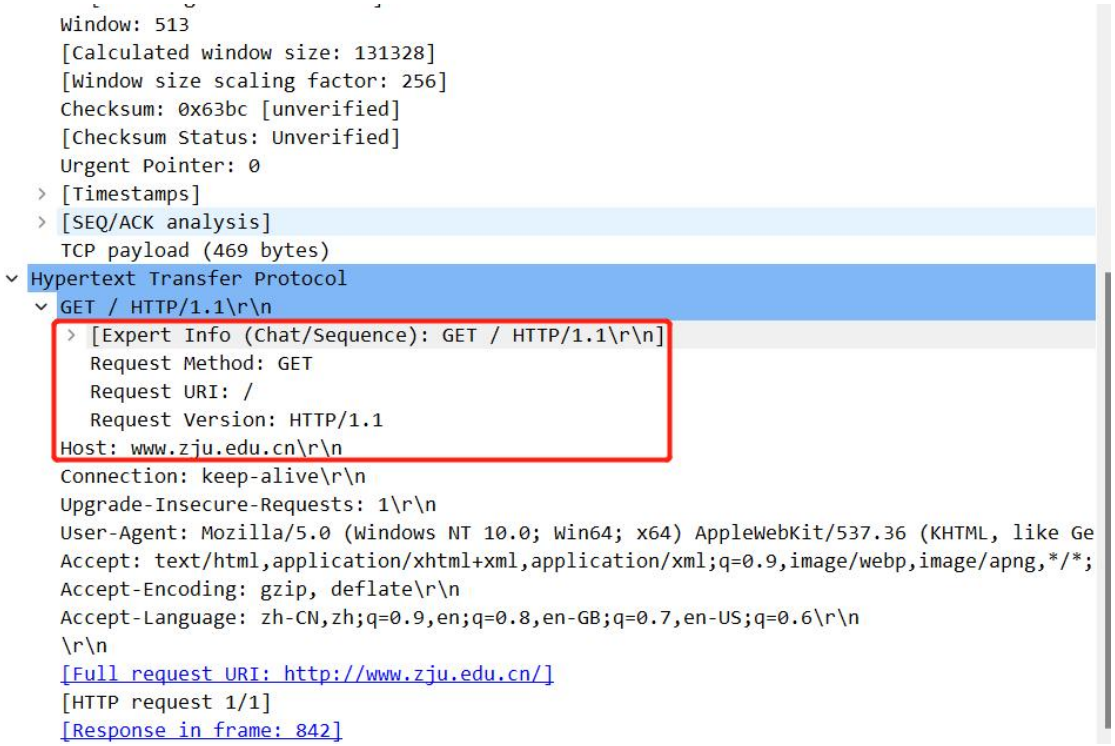

**阶段三：**客户端给服务器响应一个 ACK 段(在 TCP 标头中 ACK 位字段为 1 的 TCP/IP 数据包)，来表示确认已收到服务器的 SYN 段。



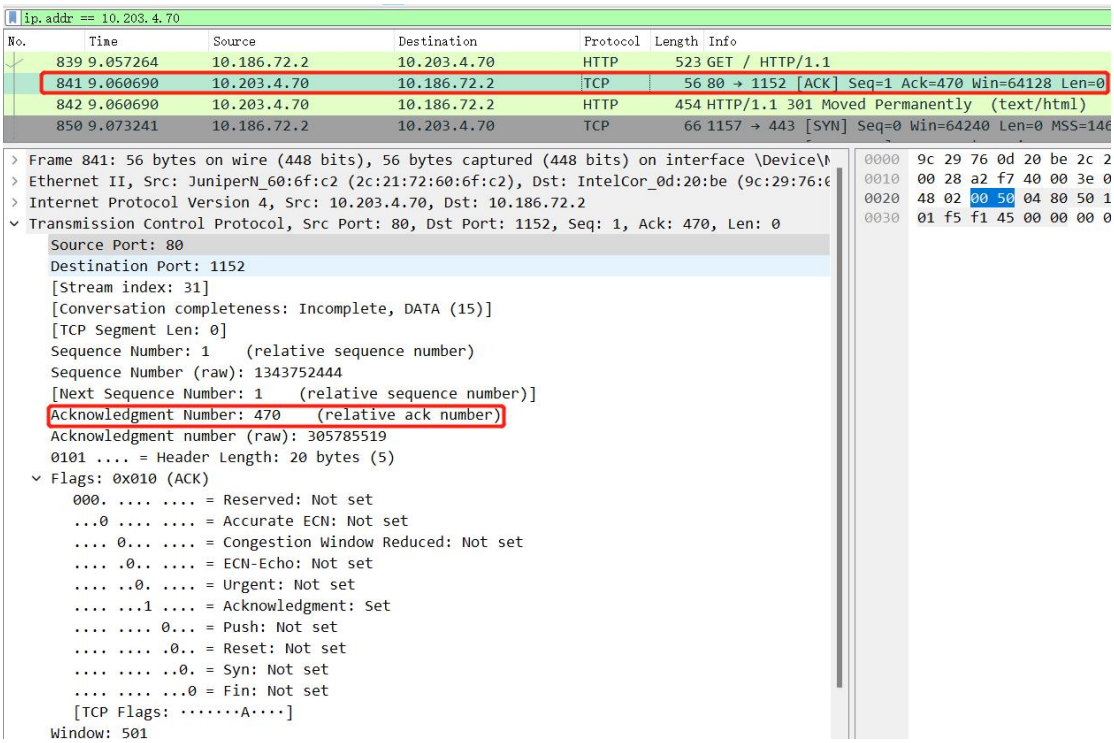
## 2、HTTP 请求

(1)客户发出 HTTP 请求之后，服务器收到请求发送 ACK



(2) 服务器发送应答报文


ip.addr == 10.203.4.70
No. Time Source Destination Protocol Length Info
839 9.057264 10.186.72.2 10.203.4.70 HTTP 523 GET / HTTP/1.1
841 9.060690 10.203.4.70 10.186.72.2 TCP 56 80 → 1152 [ACK] Seq=1 Ack=470 Win=64128 Len=0
842 9.060690 10.203.4.70 10.186.72.2 HTTP 454 HTTP/1.1 301 Moved Permanently (text/html)
850 9.073241 10.186.72.2 10.203.4.70 TCP 66 1157 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
Frame 841: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\N
Ethernet II, Src: JuniperN_60:6f:c2 (2c:21:72:60:6f:c2), Dst: IntelCor_0d:20:be (9c:29:76:6
Internet Protocol Version 4, Src: 10.203.4.70, Dst: 10.186.72.2
Transmission Control Protocol, Src Port: 80, Dst Port: 1152, Seq: 1, Ack: 470, Len: 0
Source Port: 80
Destination Port: 1152
[Stream index: 31]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1343752444
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 470 (relative ack number)
Acknowledgment number (raw): 305785519
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
000. .... .... = Reserved: Not set
...0 .... .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..0. = Syn: Not set
.... .... ...0 = Fin: Not set
[TCP Flags: ·····A····]
Window: 501
0000 9c 29 76 0d 20 be 2c 2
0010 00 28 a2 f7 40 00 3e 0
0020 48 02 00 50 04 80 50 1
0030 01 f5 f1 45 00 00 00 0