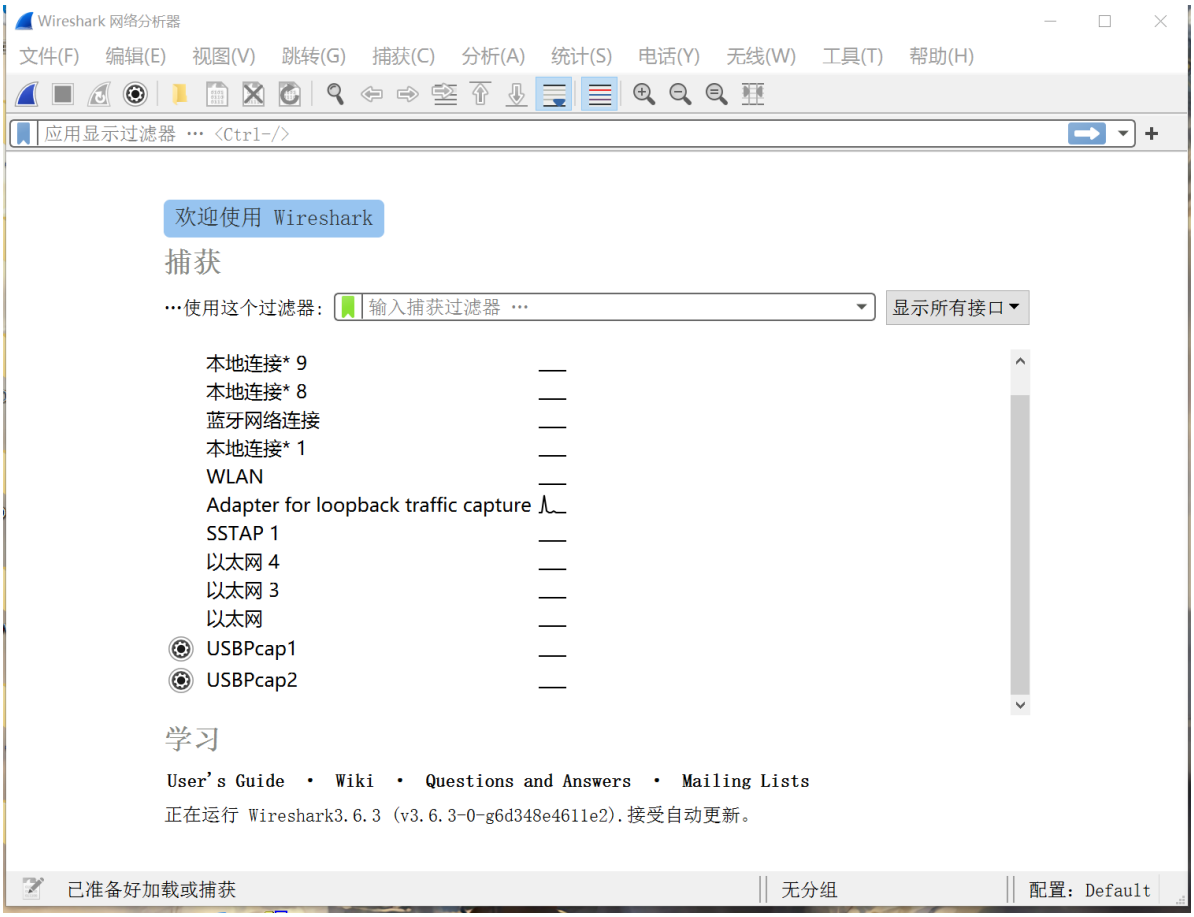
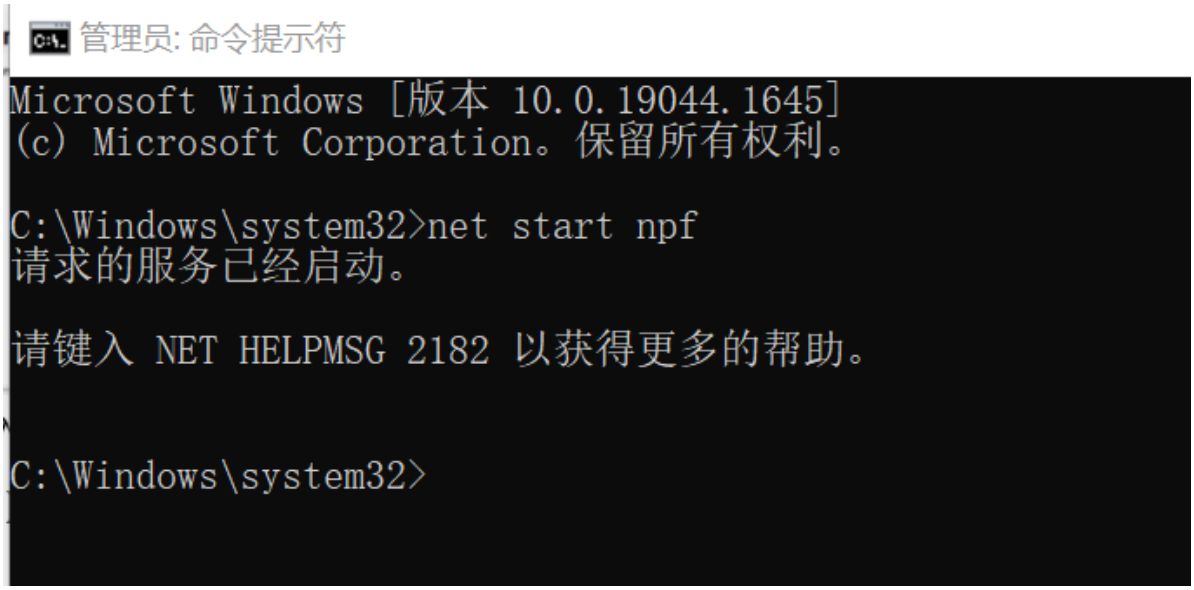
HW4:Using Wireshark

一.实验步骤

1.安装wireshark工具

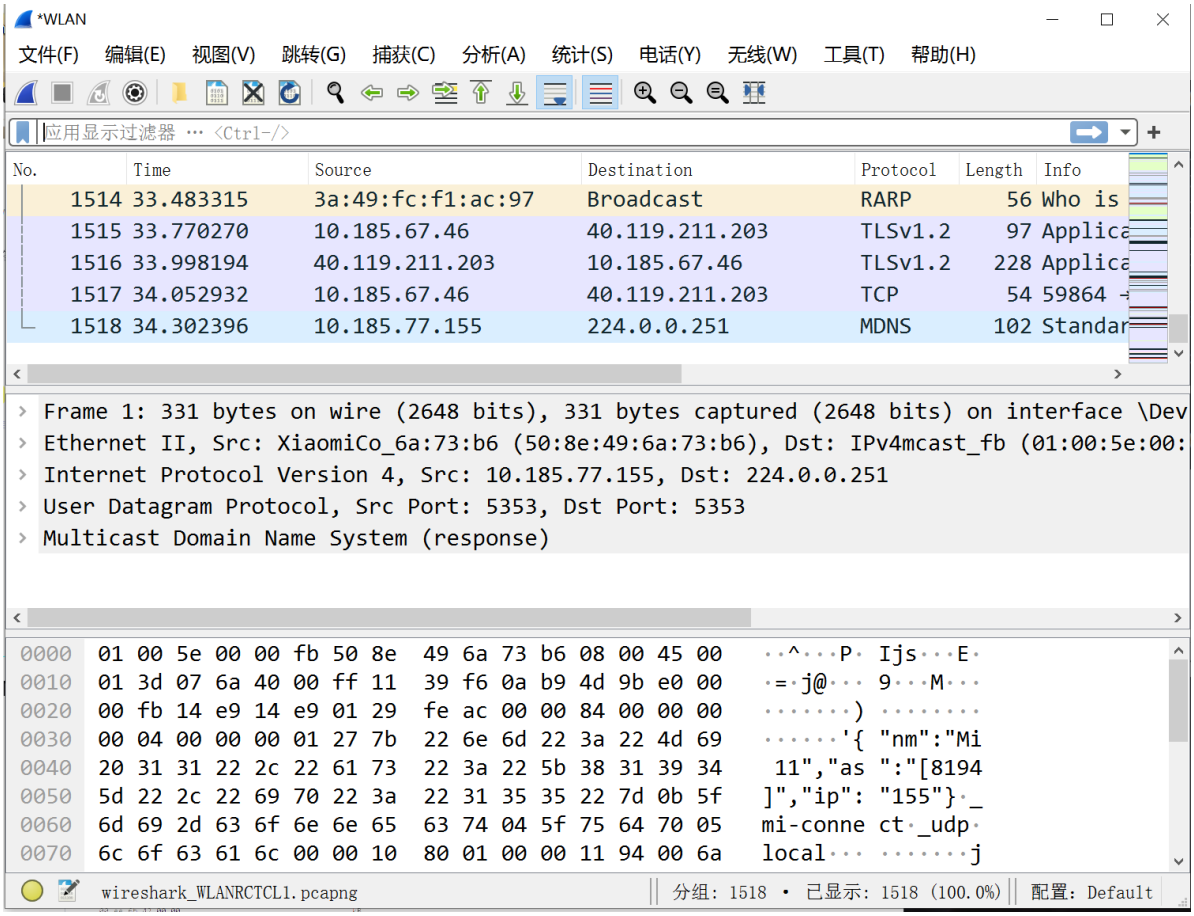


2.重启电脑并重启网卡服务，管理员模式下运行cmd，输入net start npf。

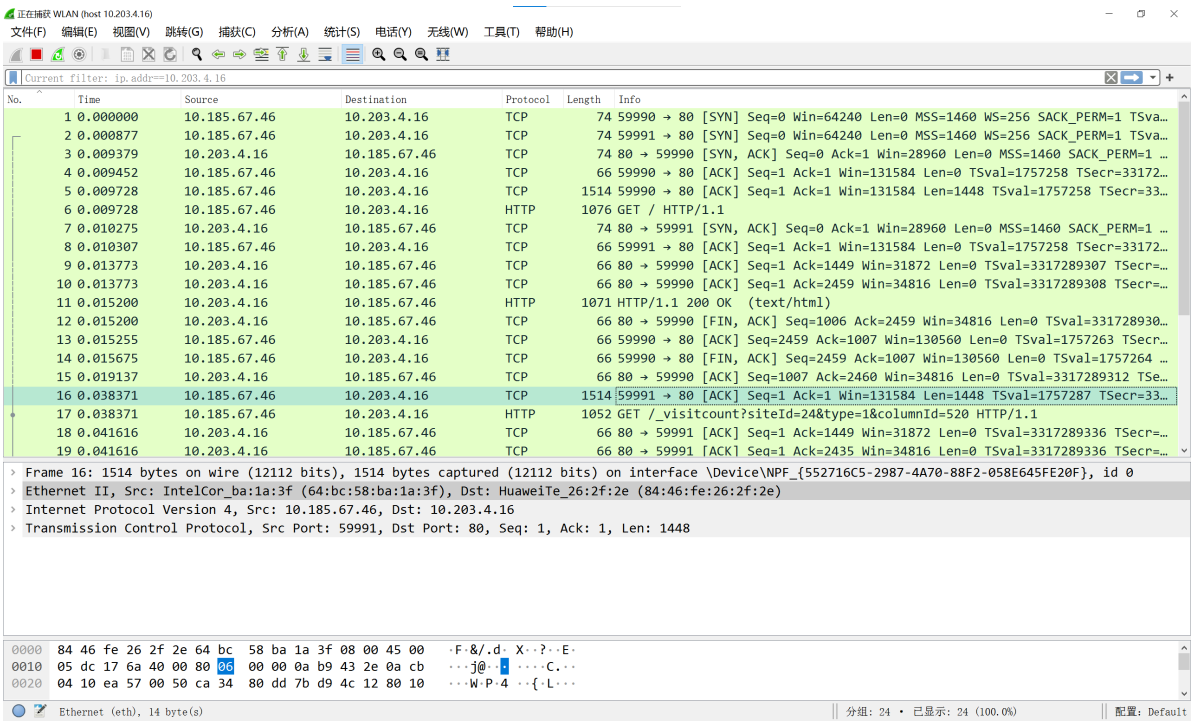


3.在cmd中输入 ping www.cs.zju.edu.cn 获得的抓包网站服务器为10.203.4.16

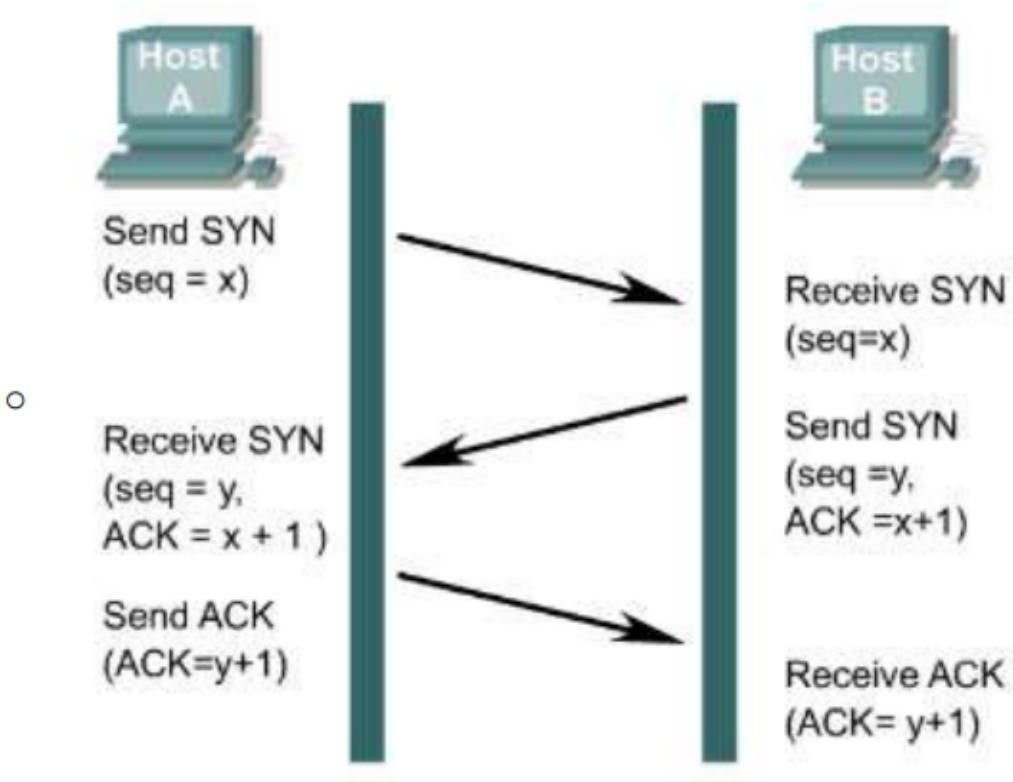
```
C:\Windows\system32>ping www.cs.zju.edu.cn

正在 Ping www.cs.zju.edu.cn [10.203.4.16] 具有 32 字节的数据:
来自 10.203.4.16 的回复: 字节=32 时间=7ms TTL=60
来自 10.203.4.16 的回复: 字节=32 时间=11ms TTL=60
来自 10.203.4.16 的回复: 字节=32 时间=7ms TTL=60
来自 10.203.4.16 的回复: 字节=32 时间=8ms TTL=60

10.203.4.16 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 7ms, 最长 = 11ms, 平均 = 8ms

C:\Windows\system32>
```



4.在捕获筛选器之中输入host 10.203.4.16便可以筛选出该ip下的信息 具体信息如下

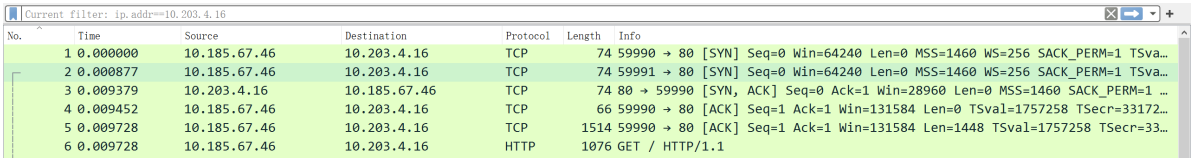


二.数据分析



1. www.cs.zju.edu.cn 的链接需要经历TCP过程，tcp的建立需要三次握手

   为什么这里的http连接之前有五次tcp?
   因为这里不是第一次连接的过程，tcp连接传输数据的时候有自己的滑动窗口和拥塞控制，这里存在一些中间传递信息的帧。

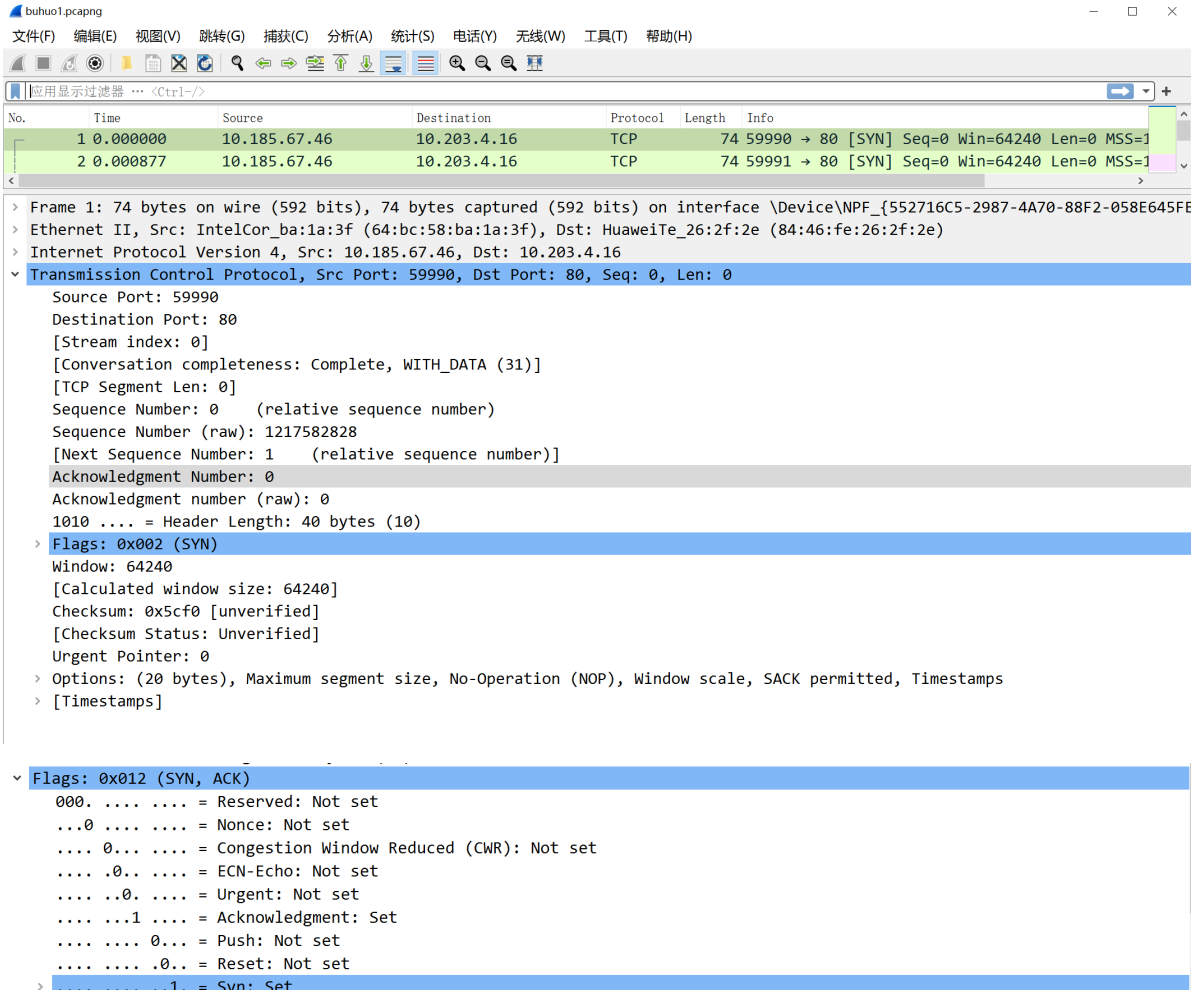


2. TCP的建立

- 第一阶段：客户发送同步请求，发送一个TCP，标志位为SYN,序列号为0，获得src，dst，port等信息，此时的ack 为not set的状态。

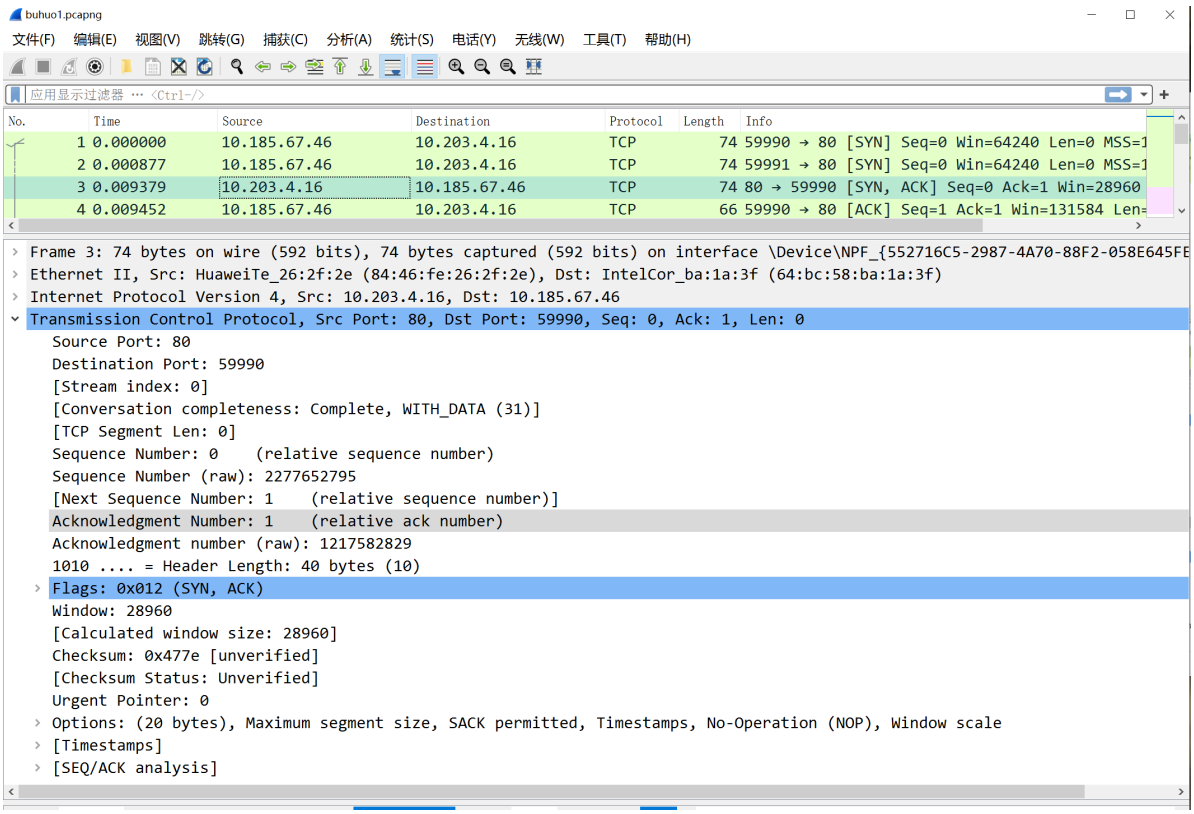
  Seq = 0 ： 初始建立连接值为0，数据包的相对序列号从0开始，表示当前还没有发送数据。

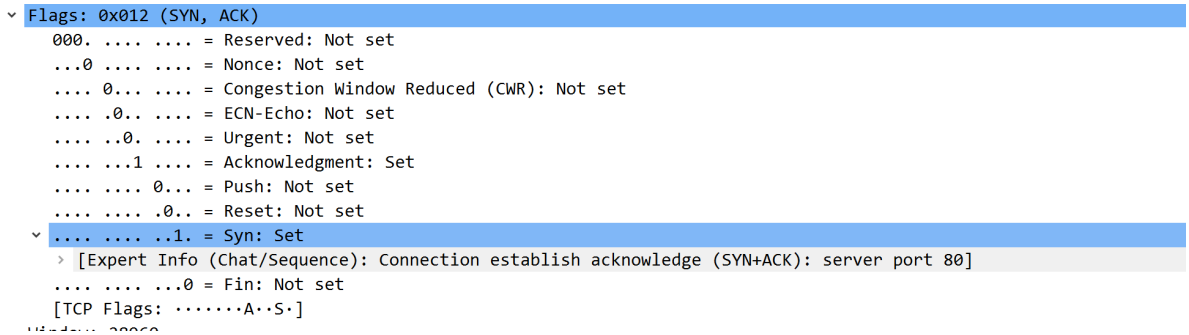
  Ack =0：初始建立连接值为0，已经收到包的数量，表示当前没有接收到数据。



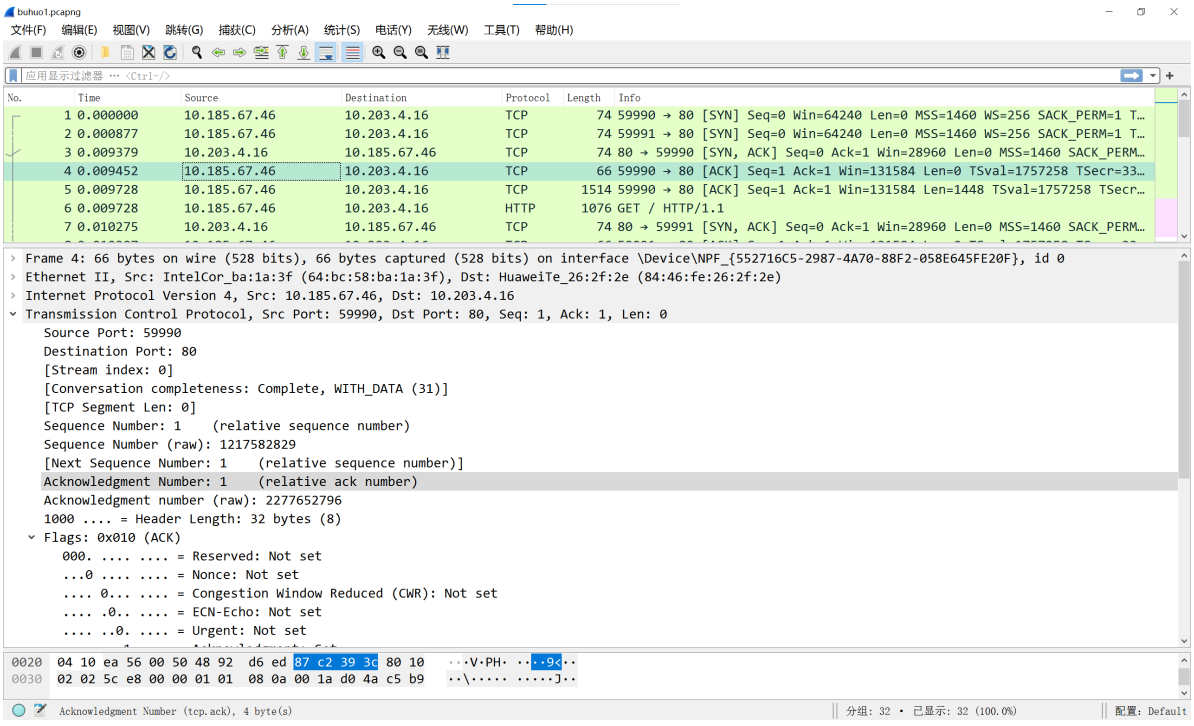
- 第二阶段：服务器向客户回复一个ACK包，此时flag，syn都设置为set。

  此数据包标志位为 SYN,ACK. 将确认序号(Acknowledgement Number)设置为1, 如下图





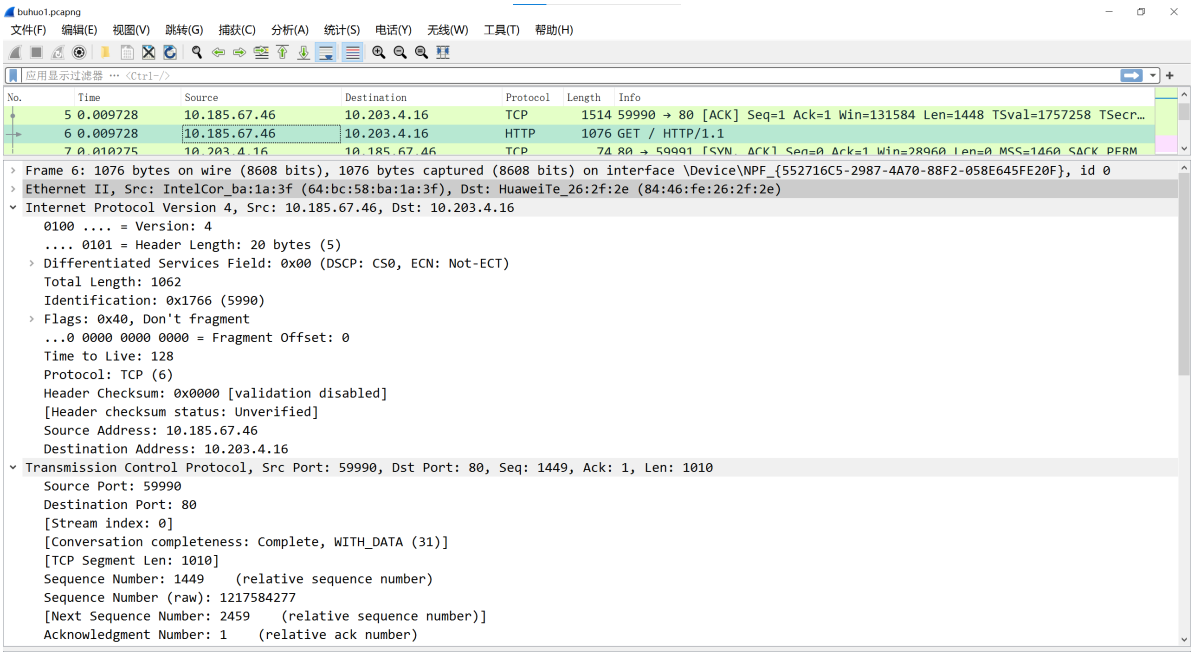
- 第三阶段：客户再向服务器发送ACK包(不是syn)，SYN标志位为0,ACK标志位为1。



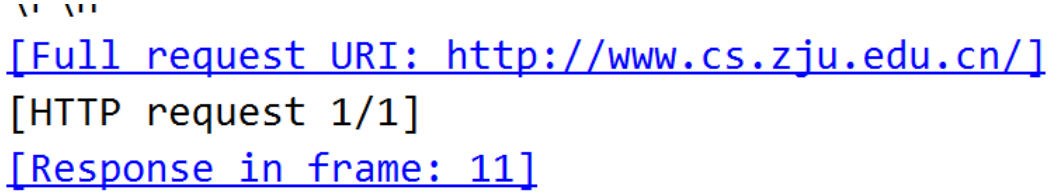
```
Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····A····]
```

3. HTTP请求

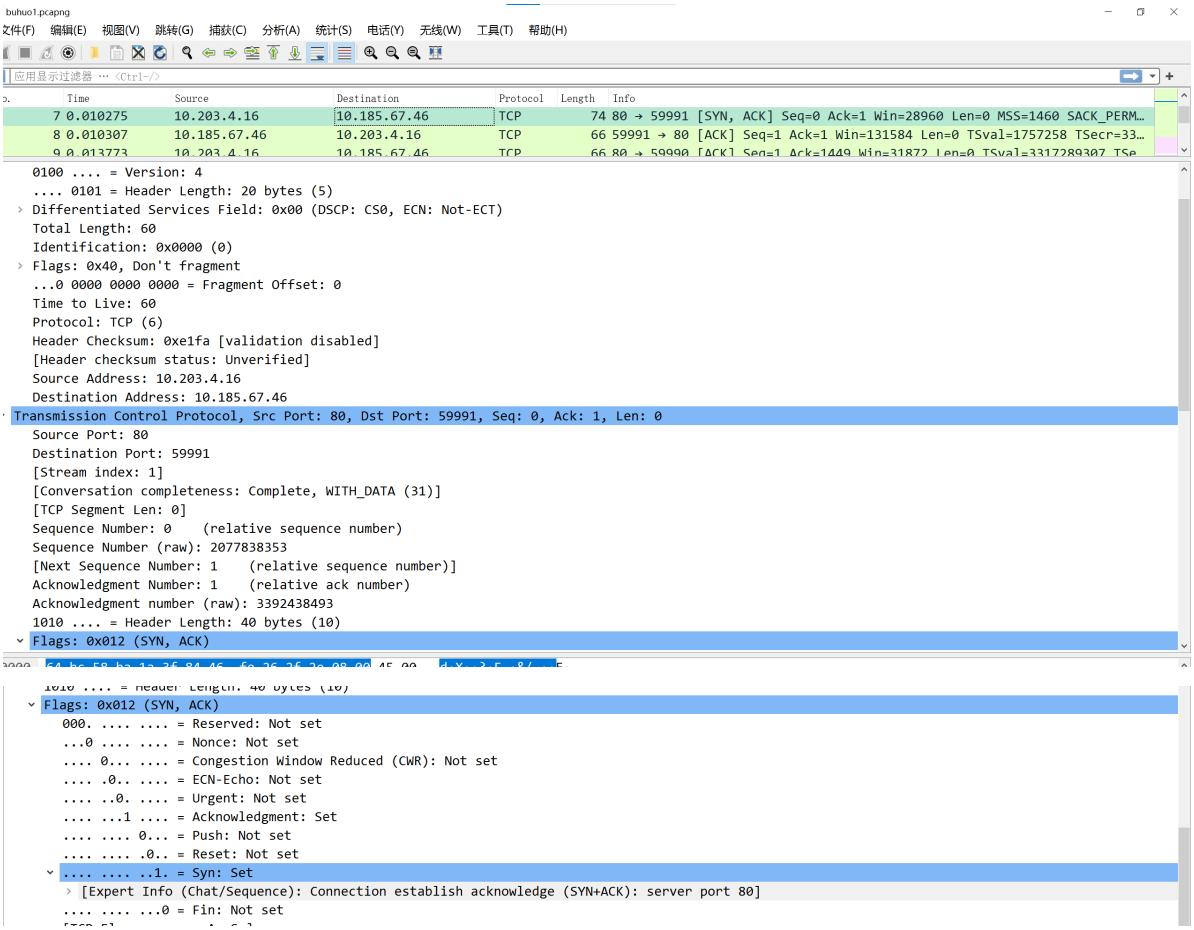
- 客户发出请求，服务器接收并发送ACK.



在此处可以看到具体的URI



- 服务器应答


buhuo1.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
No. Time Source Destination Protocol Length Info
7 0.010275 10.203.4.16 10.185.67.46 TCP 74 80 → 59991 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM…
8 0.010307 10.185.67.46 10.203.4.16 TCP 66 59991 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1757258 TSecr=33…
9 0.013773 10.203.4.16 10.185.67.46 TCP 66 80 → 59990 [ACK] Seq=1 Ack=1449 Win=31872 Len=0 TSval=3317289307 TSe…
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x0000 (0)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 60
Protocol: TCP (6)
Header Checksum: 0xe1fa [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.203.4.16
Destination Address: 10.185.67.46
Transmission Control Protocol, Src Port: 80, Dst Port: 59991, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 59991
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2077838353
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3392438493
1010 .... = Header Length: 40 bytes (10)
Flags: 0x012 (SYN, ACK)
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
....0 = Fin: Not set