

# 实验目的

下载并使用Wireshark，通过访问<http://www.zju.edu.cn> 抓取相关package，分析网络请求过程。

# 实验步骤

1. 下载并安装Wireshark程序
2. 启动程序，设置filter为 `host: www.zju.edu.cn`，只抓取与访问学校官网相关的网络包。
3. `curl http://www.zju.edu.cn`，加载完毕后导出抓取到的网络包。

# 实验结果

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.186.19.212	10.203.6.122	TCP	78	62949 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=18736122 TSecr=0 SACK_PERM=1
2	0.010591	10.203.6.122	10.186.19.212	TCP	74	443 → 62949 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=240282057 TSecr=1873
3	0.010745	10.186.19.212	10.203.6.122	TCP	66	62949 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18736133 TSecr=240282057
4	0.010941	10.186.19.212	10.203.6.122	TLSv1..	583	Client Hello
5	0.022753	10.203.6.122	10.186.19.212	TCP	66	443 → 62949 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=240282066 TSecr=18736133
6	0.022754	10.203.6.122	10.186.19.212	TLSv1..	1514	[TCP Previous segment not captured], Ignored Unknown Record
7	0.022755	10.203.6.122	10.186.19.212	TCP	1514	[TCP Out-Of-Order] 443 → 62949 [ACK] Seq=1 Ack=518 Win=30080 Len=1448 TSval=240282068 TSecr=187361
8	0.022756	10.203.6.122	10.186.19.212	TLSv1..	534	Ignored Unknown Record
9	0.022910	10.186.19.212	10.203.6.122	TCP	78	[TCP Dup ACK 3#1] 62949 → 443 [ACK] Seq=518 Ack=1 Win=131712 Len=0 TSval=18736145 TSecr=240282066
10	0.022965	10.186.19.212	10.203.6.122	TCP	66	62949 → 443 [ACK] Seq=518 Ack=2897 Win=128832 Len=0 TSval=18736145 TSecr=240282068
11	0.022988	10.186.19.212	10.203.6.122	TCP	66	62949 → 443 [ACK] Seq=518 Ack=3365 Win=128384 Len=0 TSval=18736145 TSecr=240282069
12	0.030189	10.186.19.212	10.203.6.122	TLSv1..	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
13	0.037698	10.203.6.122	10.186.19.212	TLSv1..	117	Change Cipher Spec, Encrypted Handshake Message
14	0.037771	10.186.19.212	10.203.6.122	TCP	66	62949 → 443 [ACK] Seq=611 Ack=3416 Win=131008 Len=0 TSval=18736160 TSecr=240282085
15	0.039169	10.186.19.212	10.203.6.122	TCP	1514	62949 → 443 [ACK] Seq=611 Ack=3416 Win=131072 Len=1448 TSval=18736161 TSecr=240282085 [TCP segment
16	0.039214	10.186.19.212	10.203.6.122	TCP	666	62949 → 443 [PSH, ACK] Seq=2059 Ack=3416 Win=131072 Len=600 TSval=18736161 TSecr=240282085 [TCP se
17	0.039263	10.186.19.212	10.203.6.122	TLSv1..	888	Application Data
18	0.060394	10.186.19.212	10.203.6.122	TCP	1514	[TCP Retransmission] 62949 → 443 [PSH, ACK] Seq=2033 Ack=3416 Win=131072 Len=1448 TSval=18736183 T
19	0.231890	10.203.6.122	10.186.19.212	TCP	66	443 → 62949 [ACK] Seq=3416 Ack=2659 Win=35840 Len=0 TSval=240282093 TSecr=18736161
20	0.231890	10.203.6.122	10.186.19.212	TLSv1..	1514	[TCP Previous segment not captured], Ignored Unknown Record
21	0.231891	10.203.6.122	10.186.19.212	TCP	1514	[TCP Out-Of-Order] 443 → 62949 [ACK] Seq=3416 Ack=3481 Win=38784 Len=1448 TSval=240282098 TSecr=18
22	0.231892	10.203.6.122	10.186.19.212	TLSv1..	1514	Ignored Unknown Record
23	0.231893	10.203.6.122	10.186.19.212	TLSv1..	1514	Ignored Unknown Record
24	0.231894	10.203.6.122	10.186.19.212	TLSv1..	1514	Ignored Unknown Record
25	0.231895	10.203.6.122	10.186.19.212	TLSv1..	1514	Ignored Unknown Record
26	0.231897	10.203.6.122	10.186.19.212	TLSv1..	1514	[TCP Previous segment not captured], Ignored Unknown Record
27	0.231898	10.203.6.122	10.186.19.212	TCP	1514	[TCP Out-Of-Order] 443 → 62949 [ACK] Seq=12104 Ack=3481 Win=38784 Len=1448 TSval=240282099 TSecr=1
28	0.231899	10.203.6.122	10.186.19.212	TLSv1..	1514	Ignored Unknown Record
29	0.231900	10.203.6.122	10.186.19.212	TLSv1..	681	Ignored Unknown Record
30	0.231900	10.203.6.122	10.186.19.212	TCP	681	[TCP Retransmission] 443 → 62949 [PSH, ACK] Seq=16448 Ack=3481 Win=38784 Len=615 TSval=240282115 T
31	0.232140	10.186.19.212	10.203.6.122	TCP	78	[TCP Dup ACK 14#1] 62949 → 443 [ACK] Seq=3481 Ack=3416 Win=131072 Len=0 TSval=18736354 TSecr=24028
32	0.232208	10.186.19.212	10.203.6.122	TCP	66	62949 → 443 [ACK] Seq=3481 Ack=6312 Win=128128 Len=0 TSval=18736354 TSecr=240282098
33	0.232241	10.186.19.212	10.203.6.122	TCP	66	62949 → 443 [ACK] Seq=3481 Ack=12104 Win=122368 Len=0 TSval=18736354 TSecr=240282098

> Frame 16: 666 bytes on wire (5328 bits), 666 bytes captured (5328 bits) on interface en0, id 0

> Ethernet II, Src: Apple\_af:cb:d1 (a0:78:17:af:cb:d1), Dst: JuniperN\_60:6f:c2 (2c:21:72:60:6f:c2)

> Internet Protocol Version 4, Src: 10.186.19.212, Dst: 10.203.6.122

> Transmission Control Protocol, Src Port: 62949, Dst Port: 443, Seq: 2059, Ack: 3416, Len: 600

0000 2c 21 72 60 6f c2 a0 78 17 af cb d1 08 00 45 00 , ! r ' o . x ..... E :  
ZJU.pcapng

Packets: 46 · Displayed: 46 (100.0%)

Profile: Default

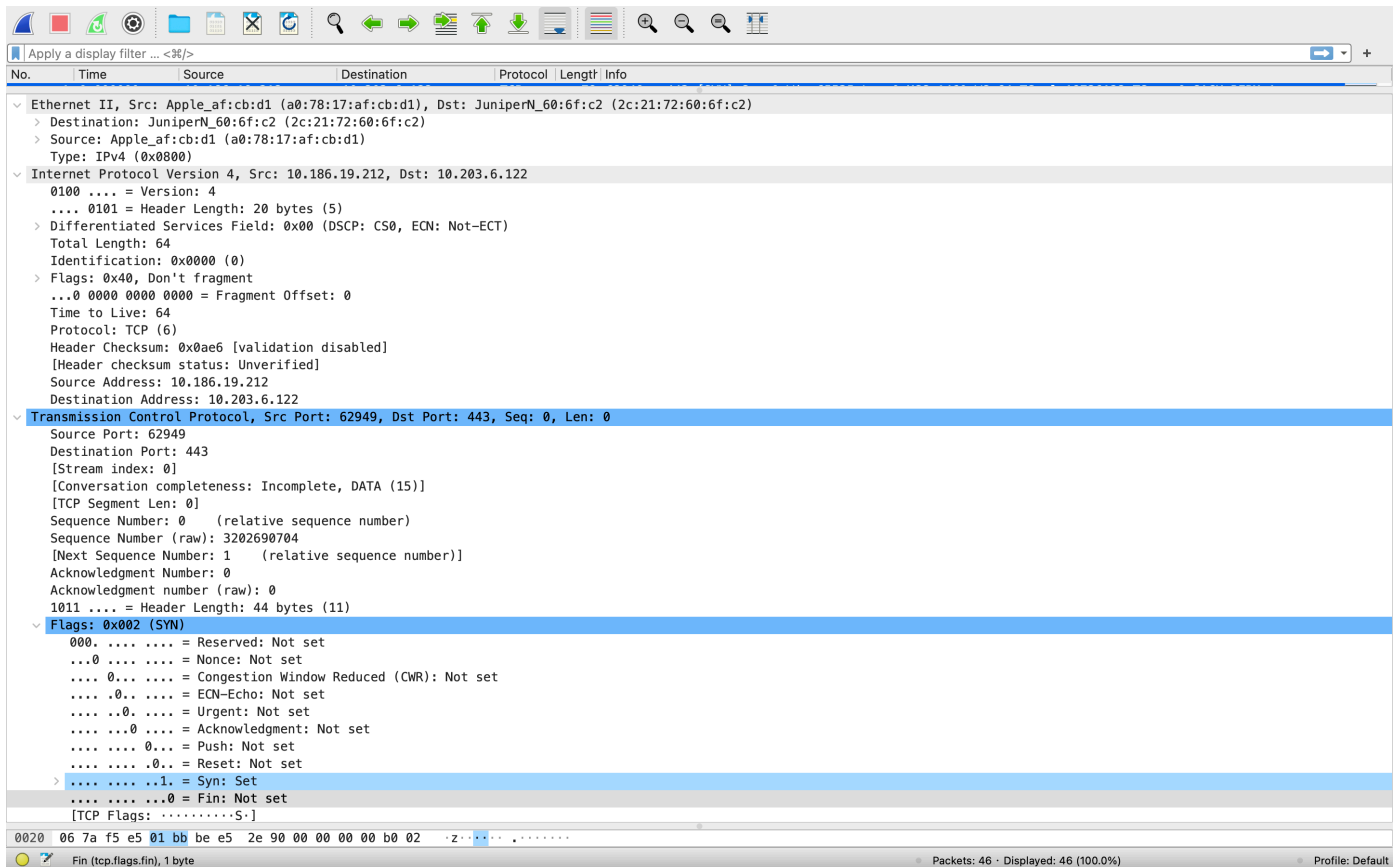
# 实验分析

## 1 TCP请求

三次握手主要发生在上图中的1-4个包中。

### 1.1 客户端向服务器发送请求

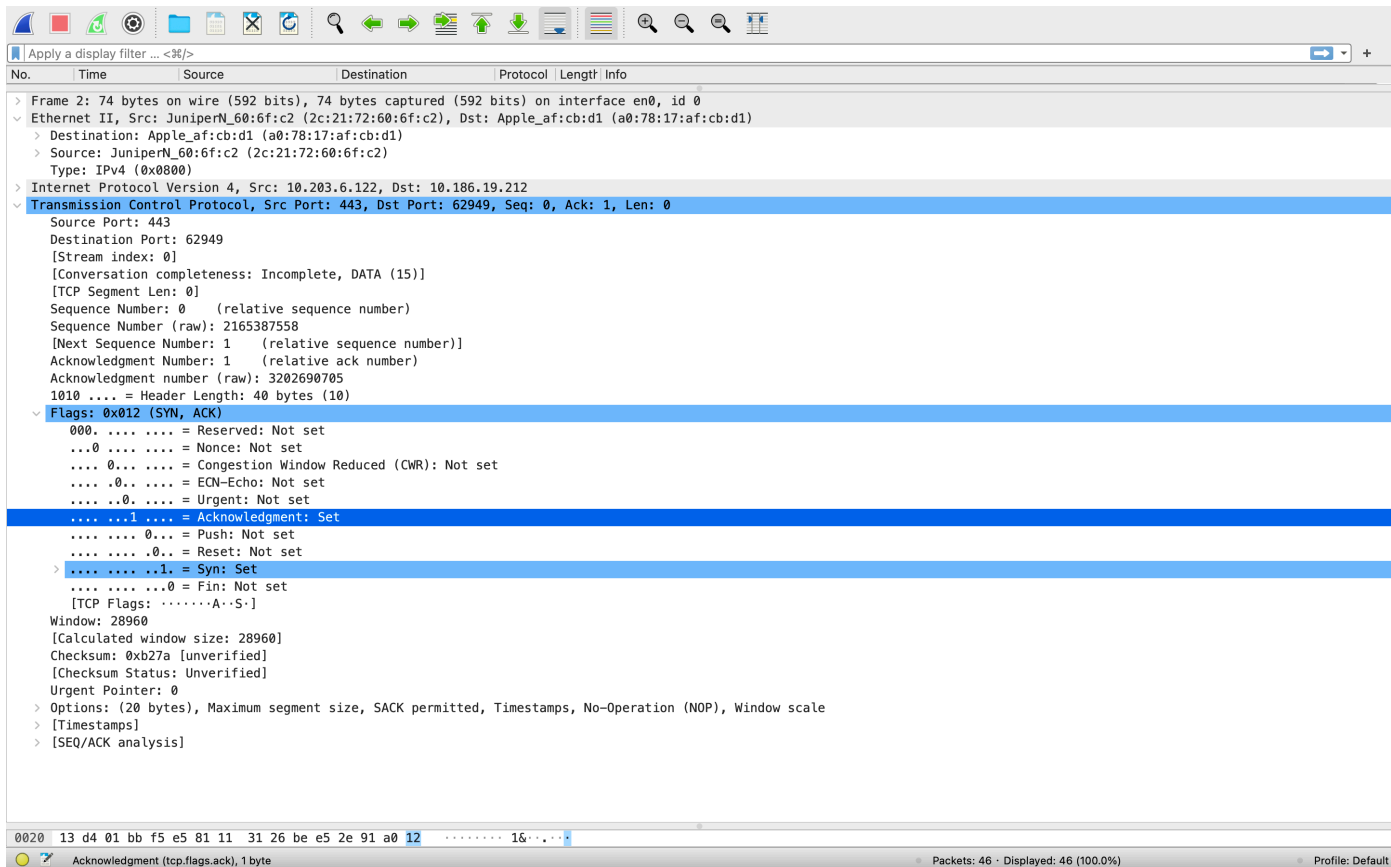
第一个包是客户端向服务器发出。



可以看到，包中包含了客户端的一些信息，例如Source, Post和所使用的传输协议等。在Flags中，Syn被设置为了Set。

## 1.2 服务器响应

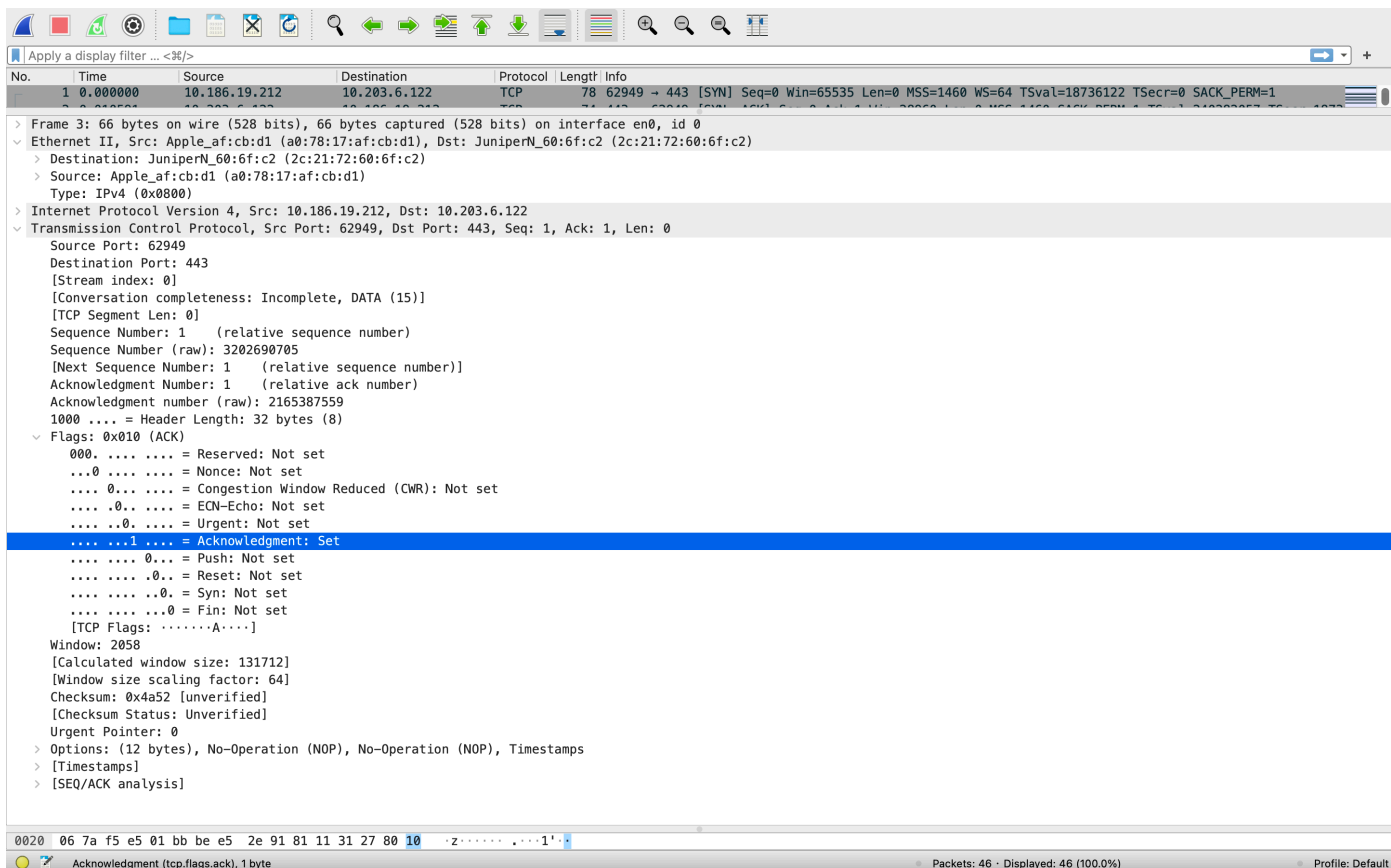
服务器返回客户端。



此时，Flags中的Acknowledgment和Syn都被设置为 Set

## 1.3 客户端再次发出请求

客户端向服务器发出ACK包。



## 2 HTTP请求

这里因为通过http协议访问，因此收到的状态码为 301 Moved Permanently。

Apply a display filter ... <3%>

Filter Buttons Preferences...

Label: Enter a description for the filter button

Filter: ip.addr== 10.203.6.122

Comment: Enter a comment for the filter button

Cancel

OK

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.186.114.94	10.203.6.122	TCP	78	49288 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=81474031 TSecr=0 SACK_PERM=1
2	0.012328	10.203.6.122	10.186.114.94	TCP	74	80 → 49288 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=666547083 TSecr=81474031
3	0.012447	10.186.114.94	10.203.6.122	TCP	66	49288 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=81474044 TSecr=666547083
4	0.012528	10.186.114.94	10.203.6.122	HTTP	144	GET / HTTP/1.1
5	0.018704	10.203.6.122	10.186.114.94	TCP	66	80 → 49288 [ACK] Seq=1 Ack=79 Win=29056 Len=0 TSval=666547091 TSecr=81474044
6	0.018705	10.203.6.122	10.186.114.94	HTTP	448	HTTP/1.1 301 Moved Permanently (text/html)
7	0.018800	10.186.114.94	10.203.6.122	TCP	66	49288 → 80 [ACK] Seq=79 Ack=303 Win=131328 Len=0 TSval=81474050 TSecr=666547091

(TCP Segment Len: 382)

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2866792621

[Next Sequence Number: 383 (relative sequence number)]

Acknowledgment Number: 79 (relative ack number)

Acknowledgment number (raw): 3218241111

1000 .... = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, 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

.... ....1... = Push: Set

.... .... .0.. = Reset: Not set

.... .... ..0. = Syn: Not set

.... .... ...0 = Fin: Not set

[TCP Flags: .....AP...]

Window: 227

[Calculated window size: 29056]

[Window size scaling factor: 128]

Checksum: 0x21e0 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

> [Timestamps]

> [SEQ/ACK analysis]

TCP payload (382 bytes)

Hypertext Transfer Protocol

HTTP/1.1 301 Moved Permanently\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]

0020 72 5e 00 50 c0 88 aa df c8 ad bf d2 76 57 80 18 r^P....vW..

Next Sequence Number (tcp.nextseq)

Packets: 30 · Displayed: 30 (100.0%)

Profile: Default