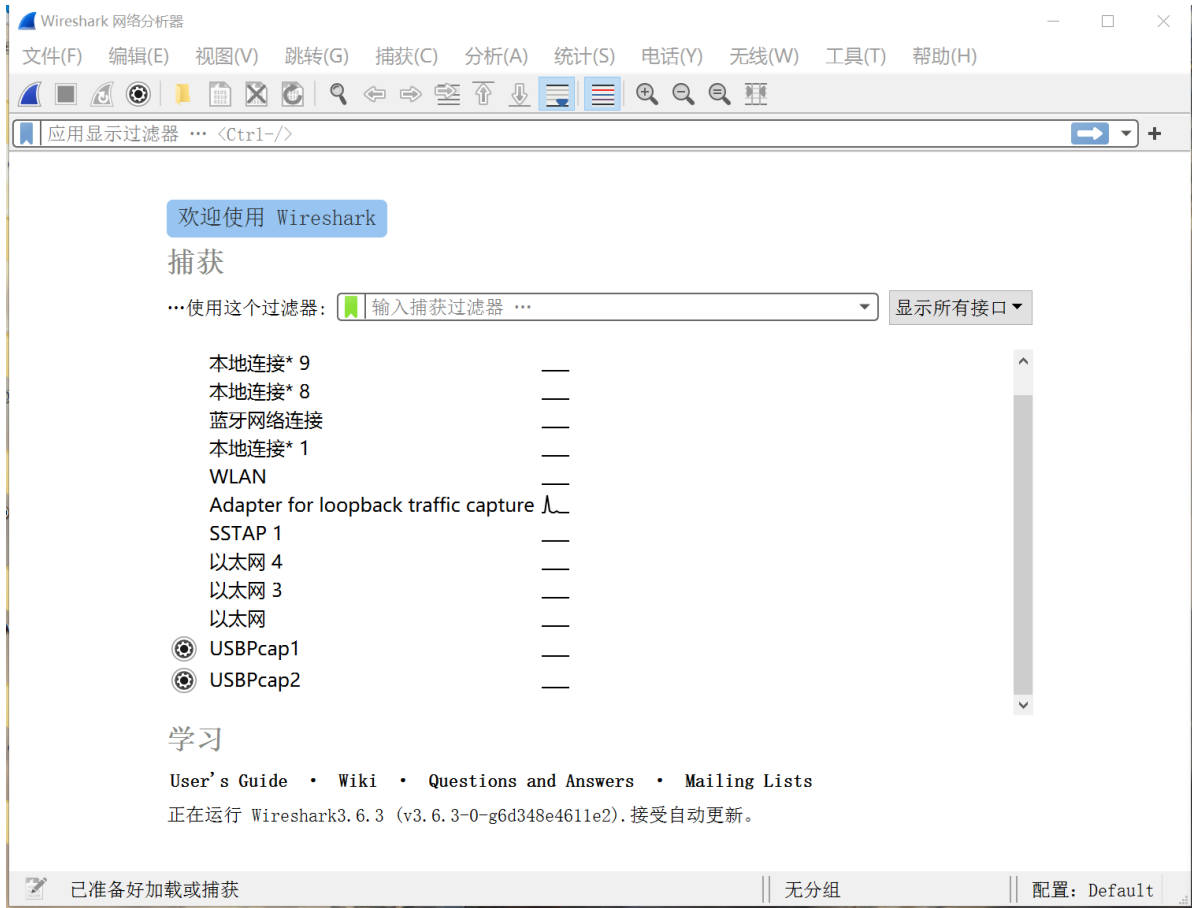


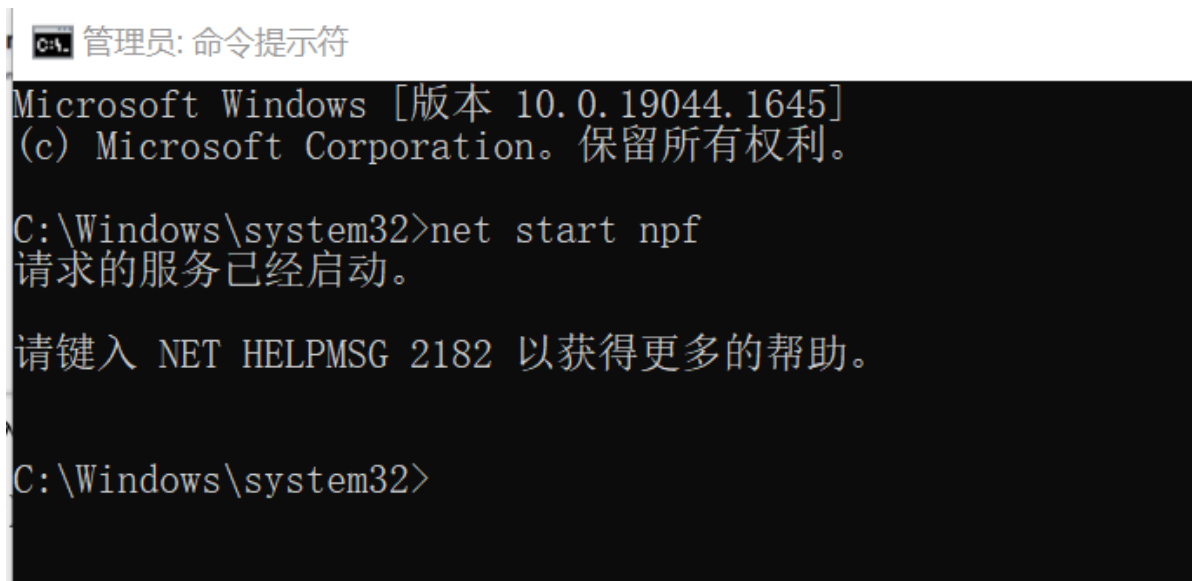
HW4:Using Wireshark

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。



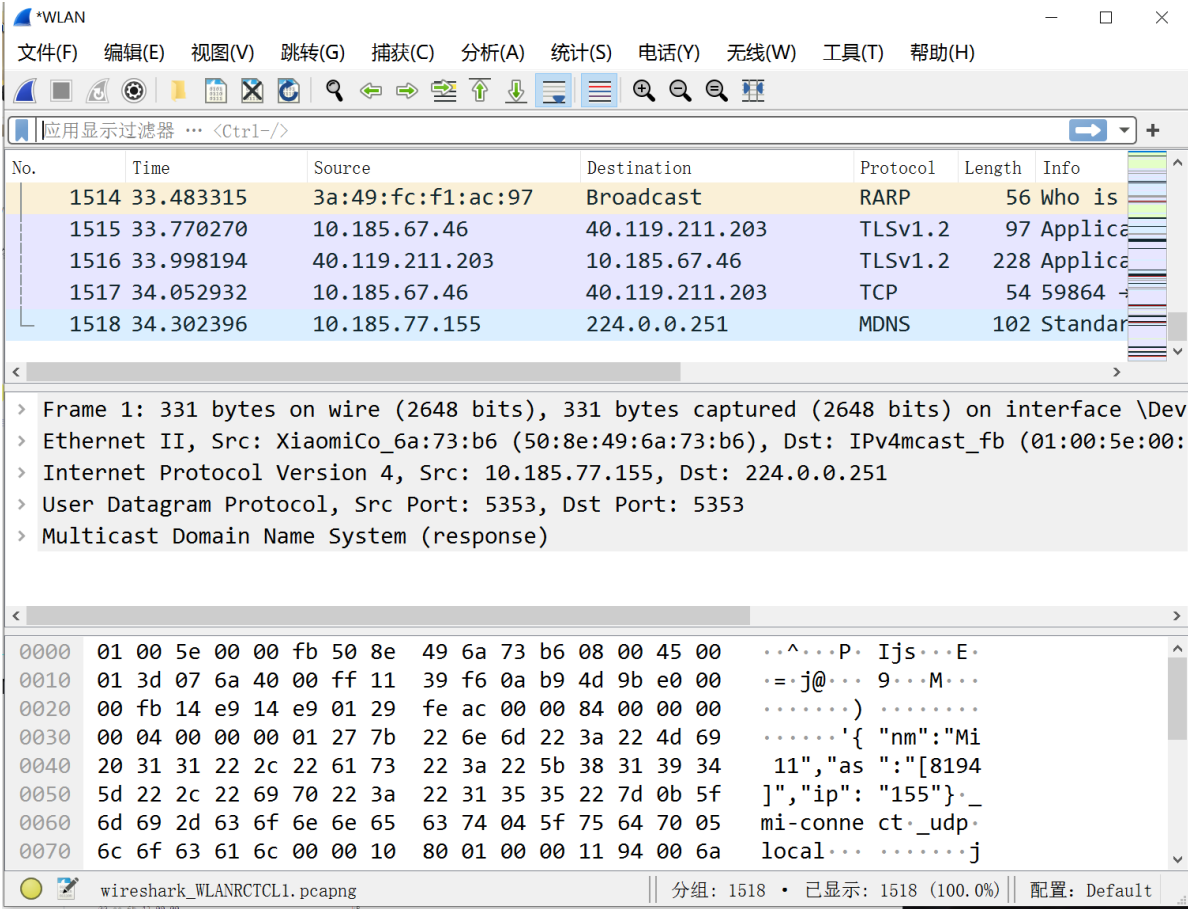
3.在cmd中输入 ping www.cs.zju.edu.cn 获得的抓包网站服务器为10.203.4.16

```
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

正在捕获 WLAN (host 10.203.4.16)

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)

Current filter: ip.addr==10.203.4.16

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.185.67.46	10.203.4.16	TCP	74	59990 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSva...
2	0.000877	10.185.67.46	10.203.4.16	TCP	74	59991 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSva...
3	0.009379	10.203.4.16	10.185.67.46	TCP	74	80 → 59990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 ...
4	0.009452	10.185.67.46	10.203.4.16	TCP	66	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1757258 TSecr=33172...
5	0.009728	10.185.67.46	10.203.4.16	TCP	1514	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSval=1757258 TSecr=33...
6	0.009728	10.185.67.46	10.203.4.16	HTTP	1076	GET / HTTP/1.1
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=1 ...
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=33172...
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 TSecr=...
10	0.013773	10.203.4.16	10.185.67.46	TCP	66	80 → 59990 [ACK] Seq=1 Ack=2459 Win=34816 Len=0 TSval=3317289308 TSecr=...
11	0.015200	10.203.4.16	10.185.67.46	HTTP	1071	HTTP/1.1 200 OK (text/html)
12	0.015200	10.203.4.16	10.185.67.46	TCP	66	80 → 59990 [FIN, ACK] Seq=1006 Ack=2459 Win=34816 Len=0 TSval=331728930...
13	0.015255	10.185.67.46	10.203.4.16	TCP	66	59990 → 80 [ACK] Seq=2459 Ack=1007 Win=130560 Len=0 TSval=1757263 TSecr=...
14	0.015675	10.185.67.46	10.203.4.16	TCP	66	59990 → 80 [FIN, ACK] Seq=2459 Ack=1007 Win=130560 Len=0 TSval=1757264 ...
15	0.019137	10.203.4.16	10.185.67.46	TCP	66	80 → 59990 [ACK] Seq=1007 Ack=2460 Win=34816 Len=0 TSval=3317289312 TSe...
16	0.038371	10.185.67.46	10.203.4.16	TCP	1514	59991 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSval=1757287 TSecr=33...
17	0.038371	10.185.67.46	10.203.4.16	HTTP	1052	GET /_visitcount?siteId=24&type=1&columnId=520 HTTP/1.1
18	0.041616	10.203.4.16	10.185.67.46	TCP	66	80 → 59991 [ACK] Seq=1 Ack=1449 Win=31872 Len=0 TSval=3317289336 TSecr=...
19	0.041616	10.203.4.16	10.185.67.46	TCP	66	80 → 59991 [ACK] Seq=1 Ack=2435 Win=34816 Len=0 TSval=3317289336 TSecr=...

> Frame 16: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{552716C5-2987-4A70-88F2-058E645FE20F}, id 0

> Ethernet II, Src: IntelCor_ba:1a:3f (64:bc:58:ba:1a:3f), Dst: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e)

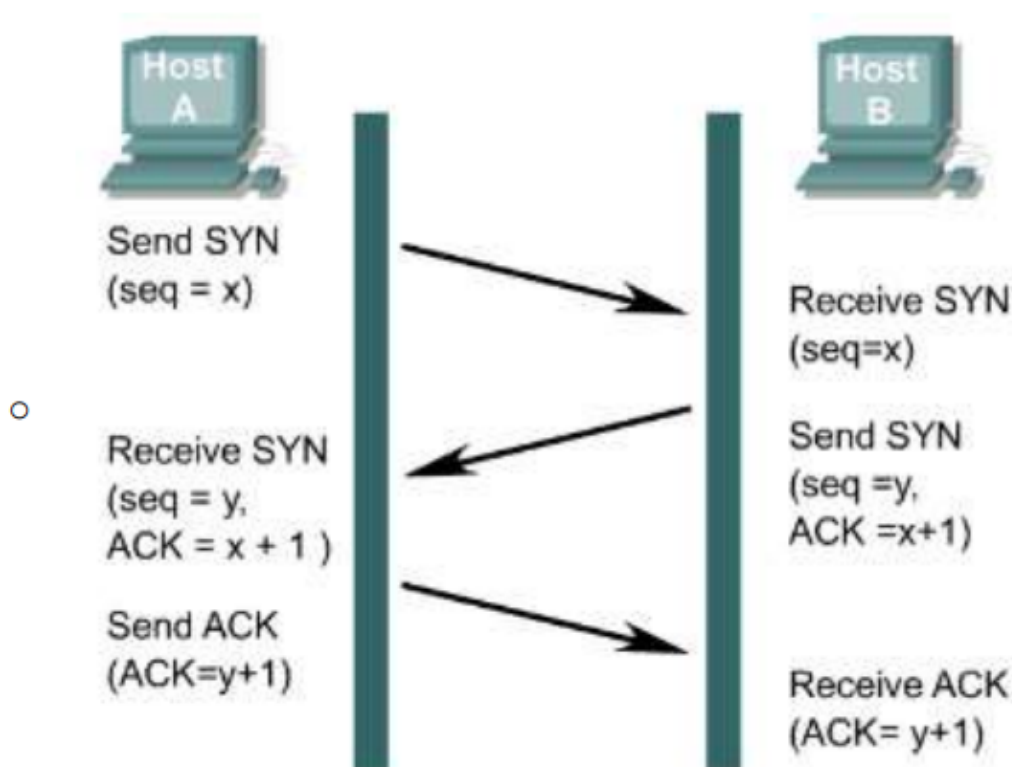
> Internet Protocol Version 4, Src: 10.185.67.46, Dst: 10.203.4.16

> Transmission Control Protocol, Src Port: 59991, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448

0000 84 46 fe 26 2f 2e 64 bc 58 ba 1a 3f 08 00 45 00 ·F·&/·d·X···?··E·
0010 05 dc 17 6a 40 00 80 00 00 00 0a b9 43 2e 0a cb ···j@····C···
0020 04 10 ea 57 00 50 ca 34 80 dd 7b d9 4c 12 80 10 ···W·P·4··{·L···

Ethernet (eth), 14 byte(s) 分组: 24 · 已显示: 24 (100.0%) 配置: Default

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。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.185.67.46	10.203.4.16	TCP	74	59990 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSva...
2	0.000877	10.185.67.46	10.203.4.16	TCP	74	59991 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSva...
3	0.009379	10.203.4.16	10.185.67.46	TCP	74	80 → 59990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 ...
4	0.009452	10.185.67.46	10.203.4.16	TCP	66	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1757258 TSecr=33172...
5	0.009728	10.185.67.46	10.203.4.16	TCP	1514	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSval=1757258 TSecr=33...
6	0.009728	10.185.67.46	10.203.4.16	HTTP	1076	GET / HTTP/1.1

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。

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
1	0.000000	10.185.67.46	10.203.4.16	TCP	74	59990 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=1757258 TSecr=3317258
2	0.000877	10.185.67.46	10.203.4.16	TCP	74	59991 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=1757258 TSecr=3317258

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{552716C5-2987-4A70-88F2-058E645FE} on Ethernet II, Src: IntelCor_ba:1a:3f (64:bc:58:ba:1a:3f), Dst: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e)

> Internet Protocol Version 4, Src: 10.185.67.46, Dst: 10.203.4.16

▼ Transmission Control Protocol, Src Port: 59990, Dst Port: 80, Seq: 0, Len: 0

Source Port: 59990

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 1217582828

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1010 = Header Length: 40 bytes (10)

> Flags: 0x002 (SYN)

Window: 64240

[Calculated window size: 64240]

Checksum: 0x5cf0 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamps

[Timestamps]

▼ 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

- 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

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
1	0.000000	10.185.67.46	10.203.4.16	TCP	74	59990 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000877	10.185.67.46	10.203.4.16	TCP	74	59991 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.009379	10.203.4.16	10.185.67.46	TCP	74	80 → 59990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
4	0.009452	10.185.67.46	10.203.4.16	TCP	66	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0

> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{552716C5-2987-4A70-88F2-058E645FE20F} Ethernet II, Src: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e), Dst: IntelCor_ba:1a:3f (64:bc:58:ba:1a:3f)

> Internet Protocol Version 4, Src: 10.203.4.16, Dst: 10.185.67.46

> Transmission Control Protocol, Src Port: 80, Dst Port: 59990, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 59990

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 2277652795

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1217582829

1010 = Header Length: 40 bytes (10)

> Flags: 0x012 (SYN, ACK)

Window: 28960

[Calculated window size: 28960]

Checksum: 0x477e [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

> [Timestamps]

> [SEQ/ACK analysis]

- > 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
- [TCP Flags:A..S.]

- 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。

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
1	0.000000	10.185.67.46	10.203.4.16	TCP	74	59990 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000877	10.185.67.46	10.203.4.16	TCP	74	59991 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.009379	10.203.4.16	10.185.67.46	TCP	74	80 → 59990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1
4	0.009452	10.185.67.46	10.203.4.16	TCP	66	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1757258 TSecr=33...
5	0.009728	10.185.67.46	10.203.4.16	TCP	1514	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSval=1757258 TSecr=33...
6	0.009728	10.185.67.46	10.203.4.16	HTTP	1076	GET / HTTP/1.1
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=1

> Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{552716C5-2987-4A70-88F2-058E645FE20F}, id 0

> Ethernet II, Src: IntelCor_ba:1a:3f (64:bc:58:ba:1a:3f), Dst: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e)

> Internet Protocol Version 4, Src: 10.185.67.46, Dst: 10.203.4.16

> Transmission Control Protocol, Src Port: 59990, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 59990

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1217582829

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2277652796

1000 = Header Length: 32 bytes (8)

> 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

0020 04 10 ea 56 00 50 48 92 d6 ed 87 c2 39 3c 80 10 ..V..PH..9<..

0030 02 02 5c e8 00 00 01 01 08 0a 00 1a d0 4a c5 b9 ..J.....J..

Acknowledgment Number (tcp.ack), 4 byte(s)

分组: 32 • 已显示: 32 (100.0%)

配置: Default

```

  ▾ 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
    .... .... = Push: Not set
    .... .... = Reset: Not set
    .... .... = Syn: Not set
    .... .... = 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.

The image displays a Wireshark packet capture analysis. The top pane shows a list of packets. Packet 6 is selected, showing an HTTP GET request from 10.185.67.46 to 10.203.4.16. The bottom pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol (TCP) header. The TCP header shows the source port as 59990 and the destination port as 80. The sequence number is 1449, and the acknowledgment number is 1. The bottom pane also shows the Hypertext Transfer Protocol (HTTP) details, including the request method (GET), request URI (/), and various headers like Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language. The response is shown in frame 11.

应用显示过滤器: * <Ctrl>- />

No.	Time	Source	Destination	Protocol	Length	Info
5	0.009728	10.185.67.46	10.203.4.16	TCP	1514	59990 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSval=1757258 TSecr...
6	0.009728	10.185.67.46	10.203.4.16	HTTP	1076	GET / HTTP/1.1
7	0.010775	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...

> Frame 6: 1076 bytes on wire (8608 bits), 1076 bytes captured (8608 bits) on interface \Device\NPF_{552716C5-2987-4A70-88F2-058E645FE20F}, id 0

> Ethernet II, Src: IntelCor_ba:1a:3f (64:bc:58:ba:1a:3f), Dst: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e)

> Internet Protocol Version 4, Src: 10.185.67.46, Dst: 10.203.4.16

0100 ... = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1062

Identification: 0x1766 (5990)

> Flags: 0x40, Don't fragment

... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.185.67.46

Destination Address: 10.203.4.16

> Transmission Control Protocol, Src Port: 59990, Dst Port: 80, Seq: 1449, Ack: 1, Len: 1010

Source Port: 59990

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 1010]

Sequence Number: 1449 (relative sequence number)

Sequence Number (raw): 1217584277

[Next Sequence Number: 2459 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

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

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Host: www.cs.zju.edu.cn\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: zh-CN,zh;q=0.9\r\n

> [truncated]Cookie: _ga=GA1.3.648237072.1618061684; Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1634523961,1635745146; BSFIT_52q/y=hKo0HKT3H/txz/yZHN,h...

\r\n

[Full request URI: http://www.cs.zju.edu.cn/]

[HTTP request 1/1]

[Response in frame: 11]

在此处可以看到具体的URI

'''

[Full request URI: <http://www.cs.zju.edu.cn/>]

[HTTP request 1/1]

[Response in frame: 11]

- 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)
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