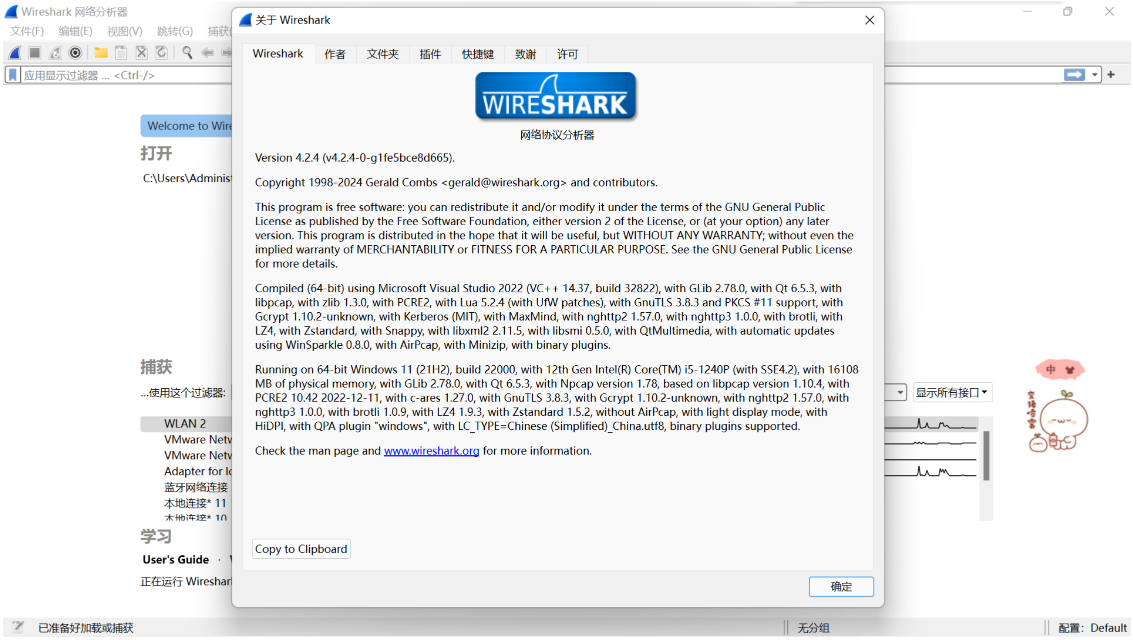
homework4

实验步骤

1. 下载安装Wireshark软件

   这里已经安装完毕



Version 4.2.4 (v4.2.4-0-g1fe5bce8d665).

Copyright 1998-2024 Gerald Combs <gerald@wireshark.org> and contributors.

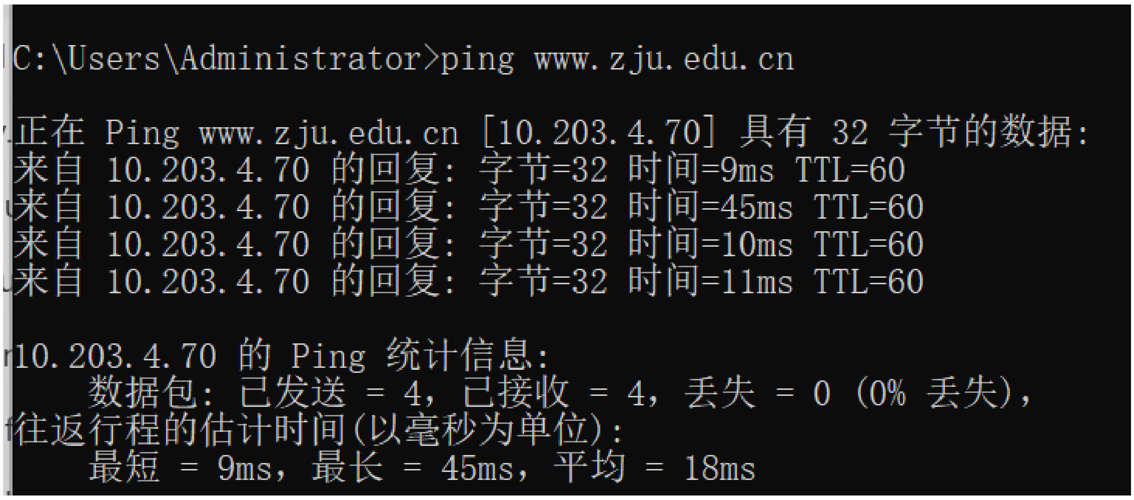
This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

Compiled (64-bit) using Microsoft Visual Studio 2022 (VC++ 14.37, build 32822), with GLib 2.78.0, with Qt 6.5.3, with libpcap, with zlib 1.3.0, with PCRE2, with Lua 5.2.4 (with UfW patches), with GnuTLS 3.8.3 and PKCS #11 support, with Gcrypt 1.10.2-unknown, with Kerberos (MIT), with MaxMind, with nghttp2 1.57.0, with nghttp3 1.0.0, with brotli, with LZ4, with Zstandard, with Snappy, with libxml2 2.11.5, with libsmi 0.5.0, with QtMultimedia, with automatic updates using WinSparkle 0.8.0, with AirPcap, with Minizip, with binary plugins.

Running on 64-bit Windows 11 (21H2), build 22000, with 12th Gen Intel(R) Core(TM) i5-1240P (with SSE4.2), with 16108 MB of physical memory, with GLib 2.78.0, with Qt 6.5.3, with Npcap version 1.78, based on libpcap version 1.10.4, with PCRE2 10.42 2022-12-11, with c-ares 1.27.0, with GnuTLS 3.8.3, with Gcrypt 1.10.2-unknown, with nghttp2 1.57.0, with nghttp3 1.0.0, with brotli 1.0.9, with LZ4 1.9.3, with Zstandard 1.5.2, without AirPcap, with light display mode, with HiDPI, with QPA plugin "windows", with LC_TYPE=Chinese (Simplified)_China.utf8, binary plugins supported.

Check the man page and www.wireshark.org for more information.

2. 在cmd中输入`ping www.zju.edu.cn`，获得需要进行抓包的网站的服务器 10.203.4.70

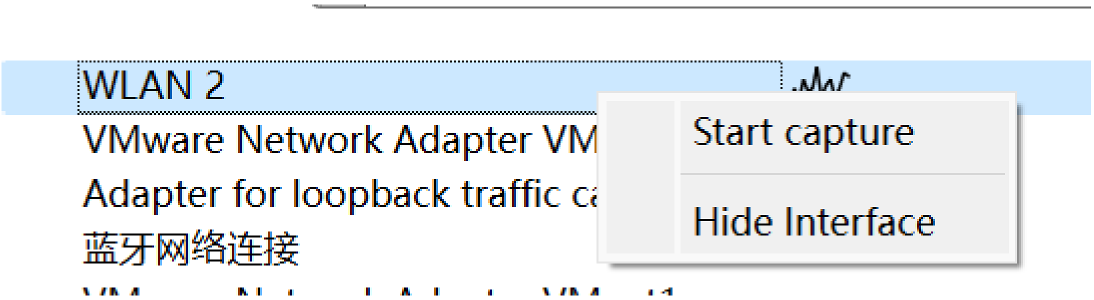


```
C:\Users\Administrator>ping www.zju.edu.cn

正在 Ping www.zju.edu.cn [10.203.4.70] 具有 32 字节的数据:
来自 10.203.4.70 的回复: 字节=32 时间=9ms TTL=60
来自 10.203.4.70 的回复: 字节=32 时间=45ms TTL=60
来自 10.203.4.70 的回复: 字节=32 时间=10ms TTL=60
来自 10.203.4.70 的回复: 字节=32 时间=11ms TTL=60

10.203.4.70 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 = 9ms，最长 = 45ms，平均 = 18ms
```

3. 在网页中打开`http://zju.edu.cn`

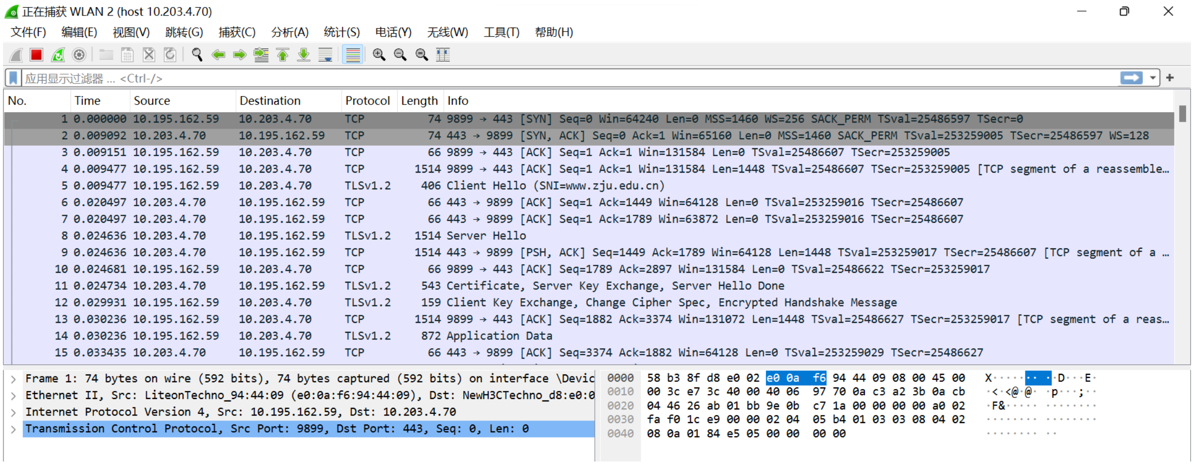
4. 打开Wireshark，添加过滤器`host 10.203.4.70`，选择连接的网络，点击capture开始抓包

5.



6. 可以利用显示过滤器查看结果，或者不使用

实验结果



```
No.    Time     Source         Destination    Protocol Length Info
     1 0.000000 10.195.162.59  10.203.4.70    TCP        74 9899 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM TSval=25486597 TSecr=0
     2 0.009092 10.203.4.70    10.195.162.59  TCP        74 443 → 9899 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=253259005 TSecr=25486597 WS=128
     3 0.009151 10.195.162.59  10.203.4.70    TCP        66 9899 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=25486607 TSecr=253259005
     4 0.009477 10.195.162.59  10.203.4.70    TCP      1514 9899 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSval=25486607 TSecr=253259005 [TCP segment of a reassemble…
     5 0.009477 10.195.162.59  10.203.4.70    TLSv1.2   406 Client Hello (SNI=www.zju.edu.cn)
     6 0.020497 10.203.4.70    10.195.162.59  TCP        66 443 → 9899 [ACK] Seq=1 Ack=1449 Win=64128 Len=0 TSval=253259016 TSecr=25486607
     7 0.020497 10.203.4.70    10.195.162.59  TCP        66 443 → 9899 [ACK] Seq=1 Ack=1789 Win=63872 Len=0 TSval=253259016 TSecr=25486607
     8 0.024636 10.203.4.70    10.195.162.59  TLSv1.2  1514 Server Hello
     9 0.024636 10.203.4.70    10.195.162.59  TCP      1514 443 → 9899 [PSH, ACK] Seq=1449 Ack=1789 Win=64128 Len=1448 TSval=253259017 TSecr=25486607 [TCP segment of a …
    10 0.024681 10.195.162.59  10.203.4.70    TCP        66 9899 → 443 [ACK] Seq=1789 Ack=2897 Win=131584 Len=0 TSval=25486622 TSecr=253259017
    11 0.024734 10.203.4.70    10.195.162.59  TLSv1.2   543 Certificate, Server Key Exchange, Server Hello Done
    12 0.029931 10.195.162.59  10.203.4.70    TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    13 0.030236 10.195.162.59  10.203.4.70    TCP      1514 9899 → 443 [ACK] Seq=1882 Ack=3374 Win=131072 Len=1448 TSval=25486627 TSecr=253259017 [TCP segment of a reas…
    14 0.030236 10.195.162.59  10.203.4.70    TLSv1.2   872 Application Data
    15 0.033435 10.203.4.70    10.195.162.59  TCP        66 443 → 9899 [ACK] Seq=3374 Ack=1882 Win=64128 Len=0 TSval=253259029 TSecr=25486627
```

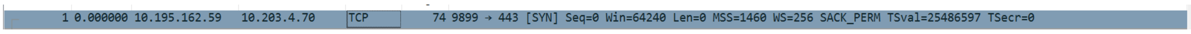
```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Devic
> Ethernet II, Src: LiteonTechno_94:44:09 (e0:0a:f6:94:44:09), Dst: NewH3CTechno_d8:e0:0
> Internet Protocol Version 4, Src: 10.195.162.59, Dst: 10.203.4.70
> Transmission Control Protocol, Src Port: 9899, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  58 b3 8f d8 e0 02 e0 0a  f6 94 44 09 08 00 45 00   X·····  ··D···E·
0010  00 3c e7 3c 40 00 40 06  97 70 0a c3 a2 3b 0a cb   ·<·<@·@·  p···;··
0020  04 46 26 ab 01 bb 9e 0b  c7 1a 00 00 00 00 a0 02   ·F&·····  ········
0030  fa f0 1c e9 00 00 02 04  05 b4 01 03 03 08 04 02   ········  ········
0040  08 0a 01 84 e5 05 00 00  00 00                     ········  ··
```

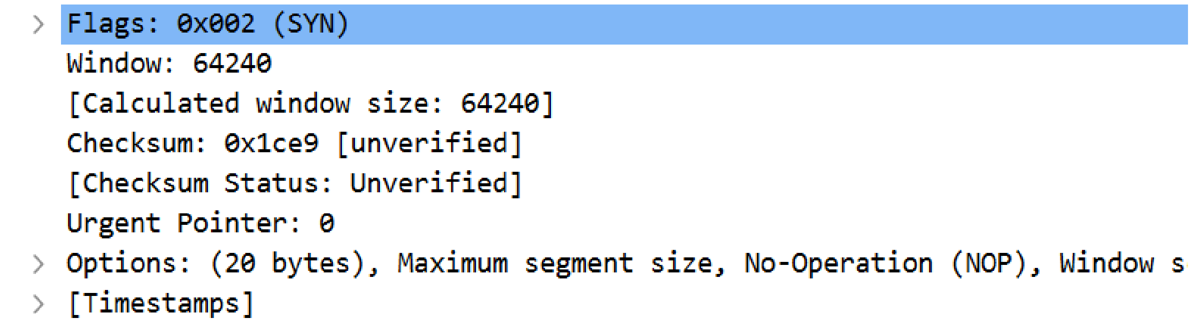
得到了如图所示的结果

数据分析

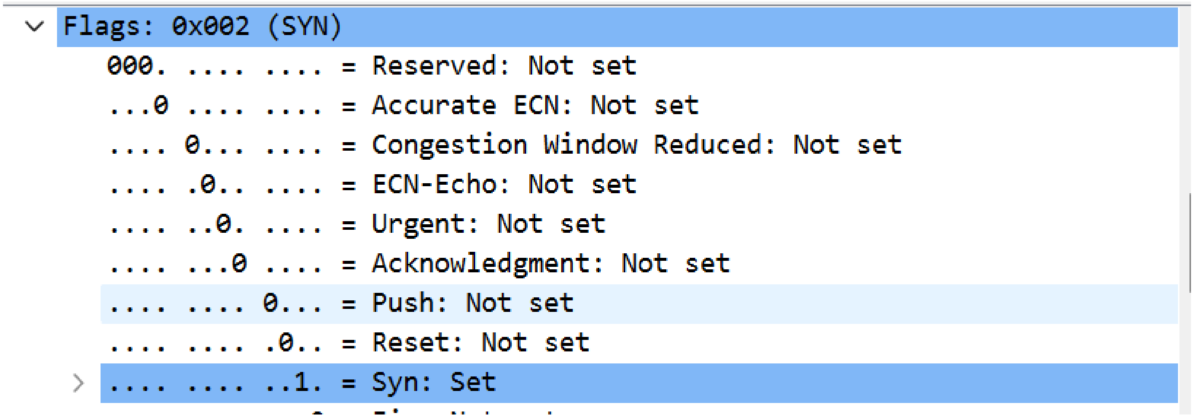
TCP的建立



```
1 0.000000 10.195.162.59  10.203.4.70  TCP  74 9899 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM TSval=25486597 TSecr=0
```

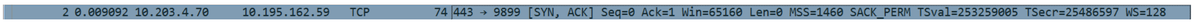


```
> Flags: 0x002 (SYN)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x1ce9 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window s
> [Timestamps]
```

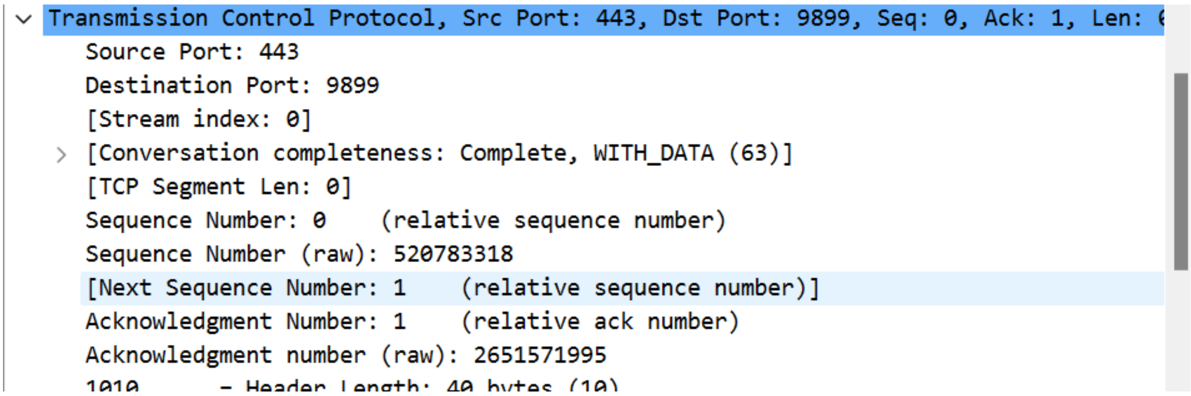


```
v Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
```

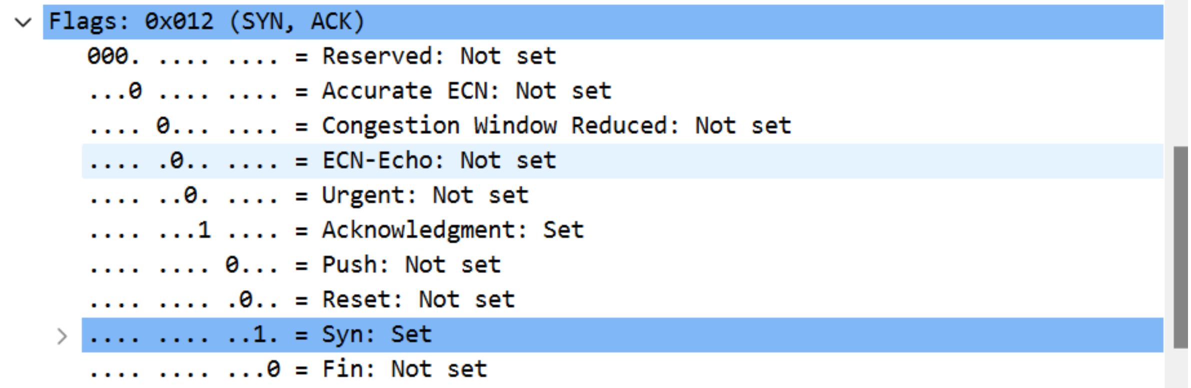
三次握手的第一次连接是客户端主动要连接服务端的，9899端口给443端口数据，可以看到Seq=0（序列号），代表初次连接。Ack=0（确认码），初次连接为0。还要给标志位，就是flags=初次连接需要给SYN=1的标志位建立连接。



```
2 0.009092 10.203.4.70  10.195.162.59  TCP  74 443 → 9899 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=253259005 TSecr=25486597 WS=128
```

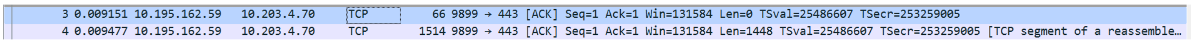


```
Transmission Control Protocol, Src Port: 443, Dst Port: 9899, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 9899
    [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 520783318
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2651571995
    1010 .... = Header Length: 40 bytes (10)
```



```
Flags: 0x012 (SYN, 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
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
```

三次握手的第二次是服务端的回馈，443端口给9899端口数据，初次连接所以Seq=0，Ack=上一次客户端的序列号+1，标志位是SYN=1和ACK=1，代表这是一个确认的回馈连接

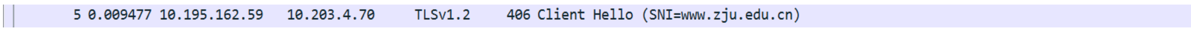


```
3 0.009151 10.195.162.59   10.203.4.70   TCP     66 9899 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=25486607 TSecr=253259005
4 0.009477 10.195.162.59   10.203.4.70   TCP   1514 9899 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSval=25486607 TSecr=253259005 [TCP segment of a reassemble…
```

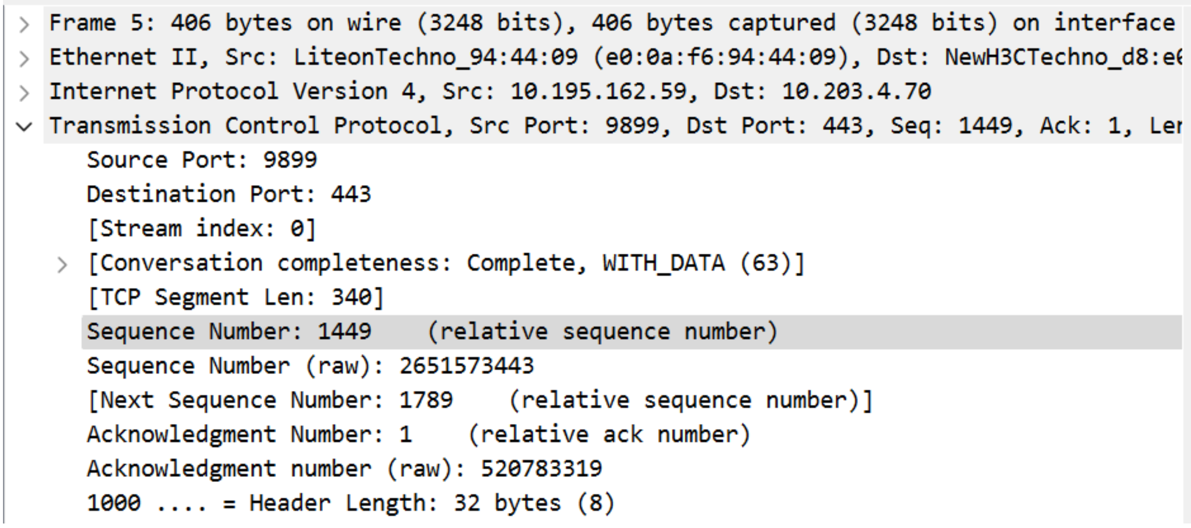
第三次握手详情点击，是客户端9899给443的反馈，Seq=1，因为这是客户端的第二次交互了，Ack=上一次服务端连接的序列号+1

握手过程中传送的包里不包含数据，三次握手完毕后，客户端与服务器才正式开始传送数据。理想状态下，TCP连接一旦建立，在通信双方中的任何一方主动关闭连接之前，TCP 连接都将被一直保持下去。断开连接时服务器和客户端均可以主动发起断开TCP连接的请求，断开过程需要经过“四次挥手”（过程就不细写 了，就是服务器和客户端交互，最终确定断开）

得到TLS协议



```
5 0.009477 10.195.162.59   10.203.4.70     TLSv1.2     406 Client Hello (SNI=www.zju.edu.cn)
```



```
> Frame 5: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface
> Ethernet II, Src: LiteonTechno_94:44:09 (e0:0a:f6:94:44:09), Dst: NewH3CTechno_d8:e
> Internet Protocol Version 4, Src: 10.195.162.59, Dst: 10.203.4.70
v Transmission Control Protocol, Src Port: 9899, Dst Port: 443, Seq: 1449, Ack: 1, Len
      Source Port: 9899
      Destination Port: 443
      [Stream index: 0]
    > [Conversation completeness: Complete, WITH_DATA (63)]
      [TCP Segment Len: 340]
      Sequence Number: 1449    (relative sequence number)
      Sequence Number (raw): 2651573443
      [Next Sequence Number: 1789    (relative sequence number)]
      Acknowledgment Number: 1    (relative ack number)
      Acknowledgment number (raw): 520783319
      1000 .... = Header Length: 32 bytes (8)
```