Wireshark—分析HTTP协议

一、实验目的

1）利用 wireshark 软件分析 HTTP 及其下层协议（TCP 协议）；

2）了解网络中数据封装的概念；

3）掌握 HTTP 及 TCP 协议的工作过程。

二、实验内容

1）启动 wireshark 软件，进行报文截获；

2）在浏览器访问 www.xjtu.edu.cn 页面（打开网页，浏览并关闭页面）；

3）停止报文截获，将截获命名为“http—学号”；

4）分析截获报文。

三、实验步骤

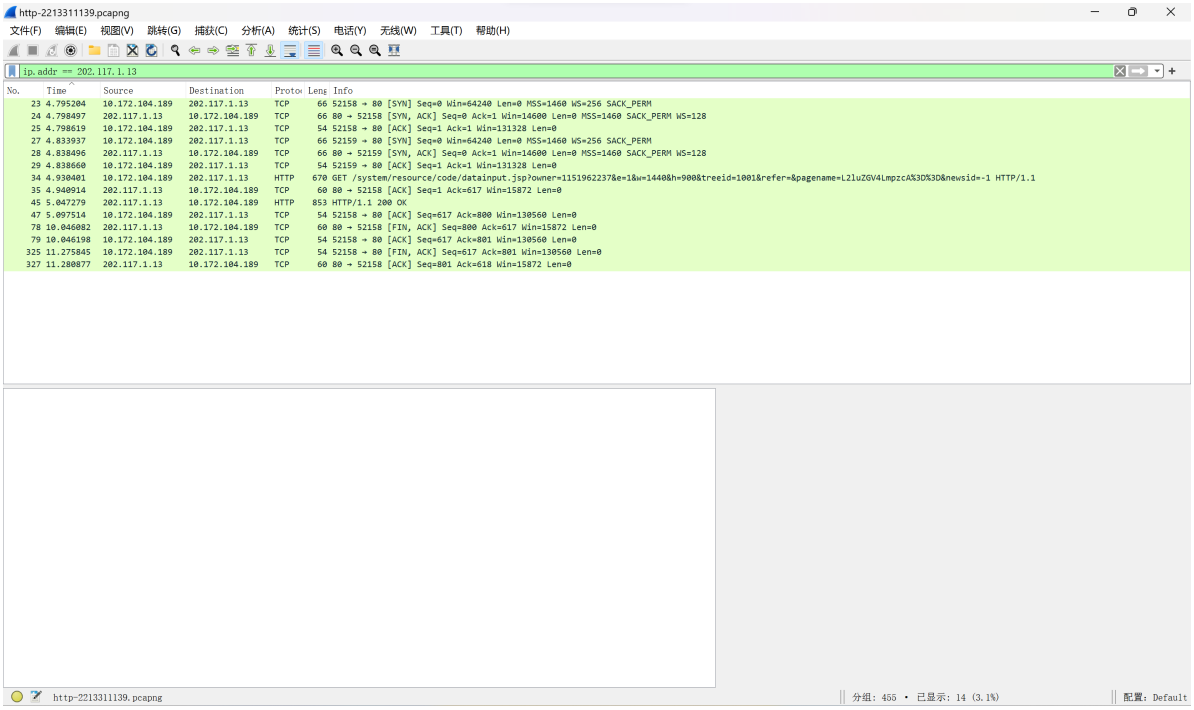
1）从截获的报文中选择 HTTP 请求报文（即 get 报文）和 HTTP 应答报文，并分析各字段的 值；

2）综合分析截获的报文，概括 HTTP 协议的工作过程；

3）从截获报文中选择 TCP 建立连接和释放连接的报文，分析各个字段的值并概括 TCP 协议 的工作过程。

四、实验过程及结果

总览：



TCP握手：

```
    23 4.795204   10.172.104.189   202.117.1.13      TCP      66 52158 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    24 4.798497   202.117.1.13     10.172.104.189    TCP      66 80 → 52158 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
    25 4.798619   10.172.104.189   202.117.1.13      TCP      54 52158 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    27 4.833937   10.172.104.189   202.117.1.13      TCP      66 52159 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    28 4.838496   202.117.1.13     10.172.104.189    TCP      66 80 → 52159 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
    29 4.838660   10.172.104.189   202.117.1.13      TCP      54 52159 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

HTTP:

```
  34 4.930401   10.172.104.189   202.117.1.13      HTTP     670 GET /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1440&h=900&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1 HTTP/1.1
  35 4.940914   202.117.1.13     10.172.104.189    TCP       60 80 → 52158 [ACK] Seq=1 Ack=617 Win=15872 Len=0
  45 5.047279   202.117.1.13     10.172.104.189    HTTP     853 HTTP/1.1 200 OK
  47 5.097514   10.172.104.189   202.117.1.13      TCP       54 52158 → 80 [ACK] Seq=617 Ack=800 Win=130560 Len=0
```

TCP挥手：

```
    78 10.046082   202.117.1.13      10.172.104.189    TCP      60 80 → 52158 [FIN, ACK] Seq=800 Ack=617 Win=15872 Len=0
    79 10.046198   10.172.104.189    202.117.1.13      TCP      54 52158 → 80 [ACK] Seq=617 Ack=801 Win=130560 Len=0
   325 11.275845   10.172.104.189    202.117.1.13      TCP      54 52158 → 80 [FIN, ACK] Seq=617 Ack=801 Win=130560 Len=0
   327 11.280877   202.117.1.13      10.172.104.189    TCP      60 80 → 52158 [ACK] Seq=801 Ack=618 Win=15872 Len=0
```

两遍三次握手出现的原因：在使用Wireshark抓包时，当建立TCP连接时，会出现两遍三次握手的情况。这是因为Wireshark在抓包时，会在本地计算机和目标服务器之间建立一个虚拟的网络接口，称为“Loopback”接口，用于捕获本地计算机与目标服务器之间的通信。因此，当Wireshark抓包时，本地计算机和目标服务器之间的通信实际上是通过Loopback接口进行的，而不是通过物理网络接口。

在进行TCP连接时，会进行三次握手来确保连接的可靠性。在Wireshark抓包时，由于本地计算机和目标服务器之间的通信是通过Loopback接口进行的，因此会出现两遍三次握手的情况。一遍是本地计算机和Loopback接口之间的三次握手，另一遍是Loopback接口和目标服务器之间的三次握手。

HTTP如何使用TCP：

域名解析 → TCP 三次握手建立连接 → 客户端发起 http 请求 → 服务器响应 http 请 求并发送 Web 页面文件 → 浏览器解析 Web 页面文件并请求其中的资源（如 js、css、图 片等） → 浏览器对页面进行渲染呈现给用户 → TCP 四次挥手释放连接

HTTP 协议如何使用 TCP 协议：当 HTTP 要传送一条报文时，会以流的形式将报文数据 的内容通过一条打开的 TCP 连接按序传输。TCP 收到数据流之后，会将数据流分成被称作 段的小数据块，并将段封装在 IP 分组中，通过因特网进行传输。

1. TCP连接建立：在HTTP协议中，客户端通过发送一个SYN包来请求建立TCP连接。服务器收到SYN包后，发送一个带有SYN和ACK标志的包作为响应。最后，客户端发送一个带有ACK标志的包来确认连接建立。
2. HTTP请求：一旦TCP连接建立，客户端发送一个HTTP请求给服务器。这个请求通常包含一个请求行、请求头和请求体。请求行包含请求方法（GET、POST等）、URL和HTTP协议版本。请求头包含一些元数据，如Host、User-Agent、Content-Type等。请求体包含一些附加的数据，如表单数据或上传的文件。
3. 服务器响应：服务器收到HTTP请求后，根据请求的内容和服务器的处理逻辑，生成一个HTTP响应。响应通常包含一个响应行、响应头和响应体。响应行包含HTTP协议版本、状态码和状态信息。
4. 数据传输：HTTP协议使用TCP协议来传输数据。TCP协议提供可靠的、面向连接的数据传输。它将HTTP请求和响应分割成多个小的数据包，并通过TCP连接逐个发送。TCP协议还提供流量控制和拥塞控制，以确保数据的可靠传输。
5. 连接关闭：一旦HTTP响应发送完毕，服务器关闭TCP连接。客户端收到响应后，也可以选择关闭TCP连接。如果客户端需要发送更多的HTTP请求，它可以继续使用现有的TCP连接，或者建立一个新的TCP连接。

TCP三次握手

```
 23 4.795204    10.172.104.189   202.117.1.13     TCP      66 52158 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 24 4.798497    202.117.1.13     10.172.104.189   TCP      66 80 → 52158 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
 25 4.798619    10.172.104.189   202.117.1.13     TCP      54 52158 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

第一次：

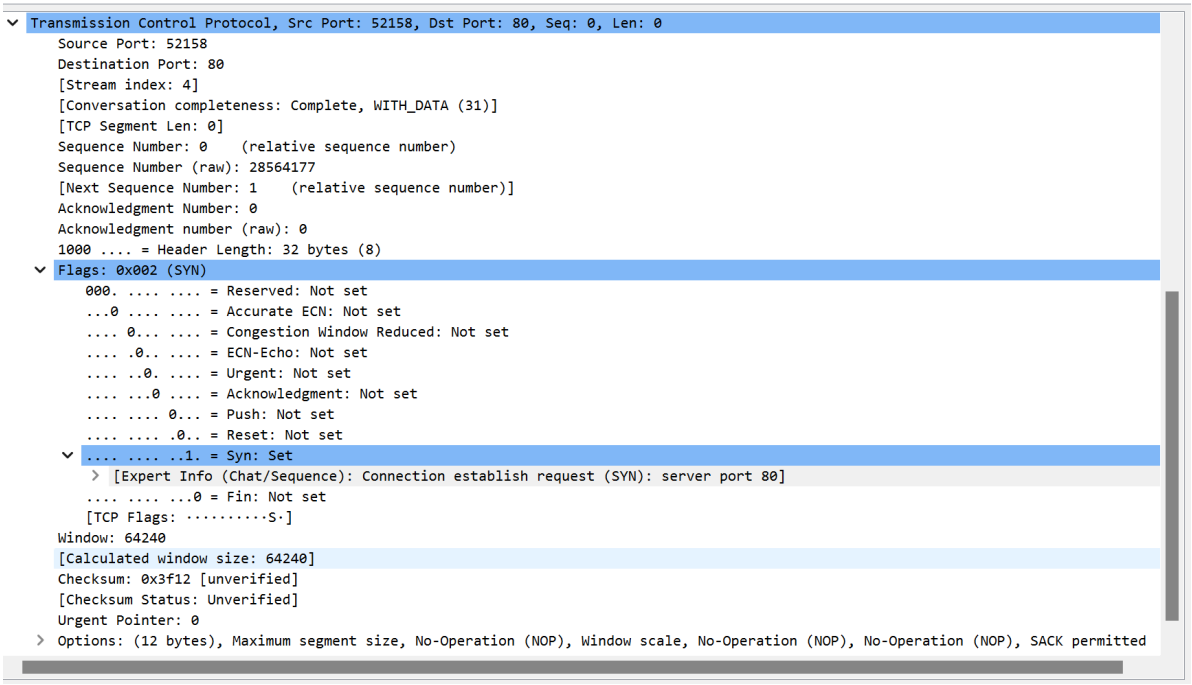
```
23 4.795204    10.172.104.189   202.117.1.13     TCP      66 52158 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

Frame，Ethernet and IPv4：

```
> Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{C57448F0-5278-4340-ABF3-D9F68FED7FE2}, id
v Ethernet II, Src: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5), Dst: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  > Destination: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  > Source: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.172.104.189, Dst: 202.117.1.13
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0xdb2b (56107)
  v 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...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: 10.172.104.189
    Destination Address: 202.117.1.13
```

表明在网络层的源地址是客户机的IP:10.172.104.189;目标地址是www.xjtu.edu.cn域名代表的IP：202.117.1.13；

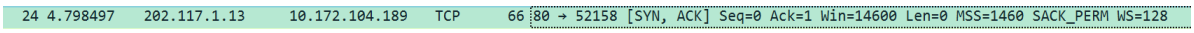
TCP：



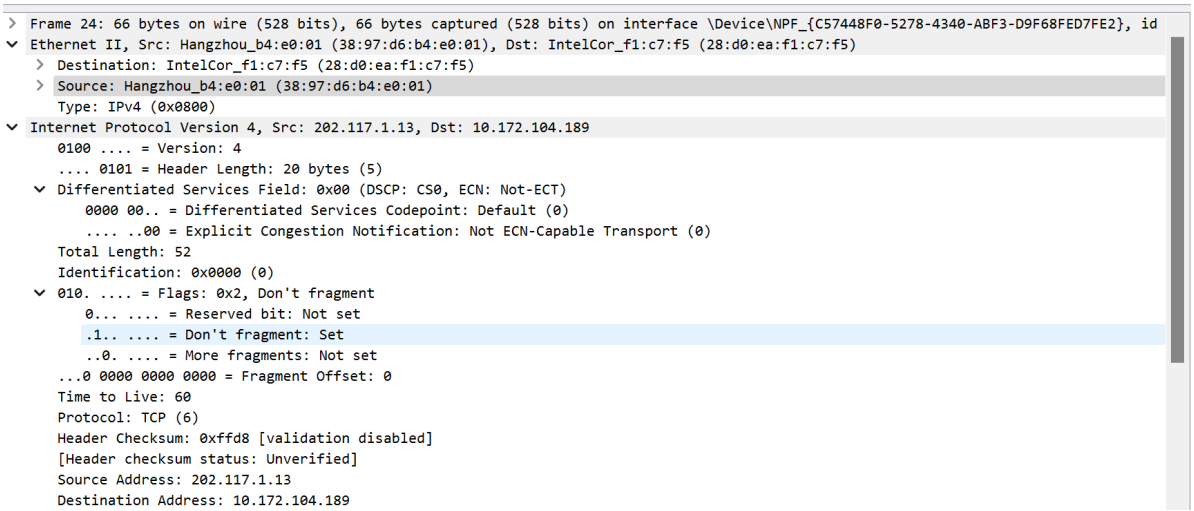
第一次握手，源端口是客户机端口52158，目标端口是http的80端口，表示客户机向www.xjtu.edu.cn服务器的（http）80端口发起请求。相对序列号relative sequence number为0.

标志位中只有SYN同步信号处被置为1，表示有效，表明这是一条申请建立TCP连接的请求。

第二次：



Frame，Ethernet and IPv4：



消息传递时网络层的源地址IP：202.117.1.13，表明是www.xjtu.edu.cn的主机地址，而目标地址IP：

10.172.104.189，表明客户机地址。

TCP:

```
Transmission Control Protocol, Src Port: 80, Dst Port: 52158, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 52158
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2355874376
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 28564178
    1000 .... = Header Length: 32 bytes (8)
  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
      [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····A··S·]
    Window: 14600
    [Calculated window size: 14600]
    Checksum: 0xf7c4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
```

第二次握手时，源端口是服务器主机的http80端口，而目标端口则是客户机的52158端口；

标志位处SYN和ACK置为1，表明这是一条服务器发回给客户机的确认包消息。

相对序列号relative sequence number仍是0，而相对确认号则为第一次握手中消息的相对序列号加1，所以是1。

这是服务器对客户机申请的应答请求。

第三次：

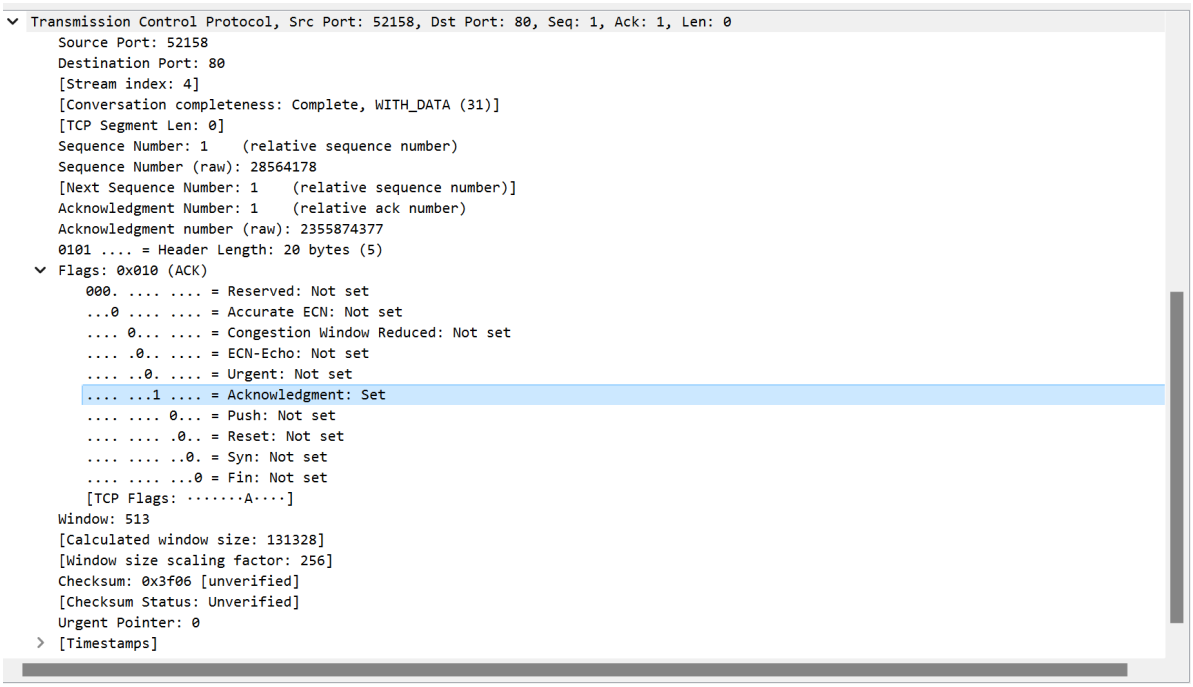
```
 25 4.798619    10.172.104.189    202.117.1.13      TCP      54 52158 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

Frame，Ethernet and IPv4：

```
Frame 25: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C57448F0-5278-4340-ABF3-D9F68FED7FE2}, id
Ethernet II, Src: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5), Dst: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  Destination: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  Source: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.172.104.189, Dst: 202.117.1.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 40
  Identification: 0xdb2c (56108)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...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: 10.172.104.189
  Destination Address: 202.117.1.13
```

本条消息传输时的网络层源地址IP又是客户机：10.172.104.189；而目标地址为IP：202.117.1.13，表明是www.xjtu.edu.cn的主机地址。表明此消息是客户机向服务器发送的。

TCP：



第三次握手时源端口又是客户机52158；而目标端口是服务器的80端口；

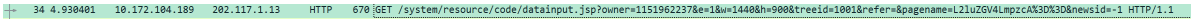
标志位只有ACK处置为1；表明这是客户机向服务器的确认消息。

相对确认号relative ACK number为第二次握手中的相对序列号加1，为1；

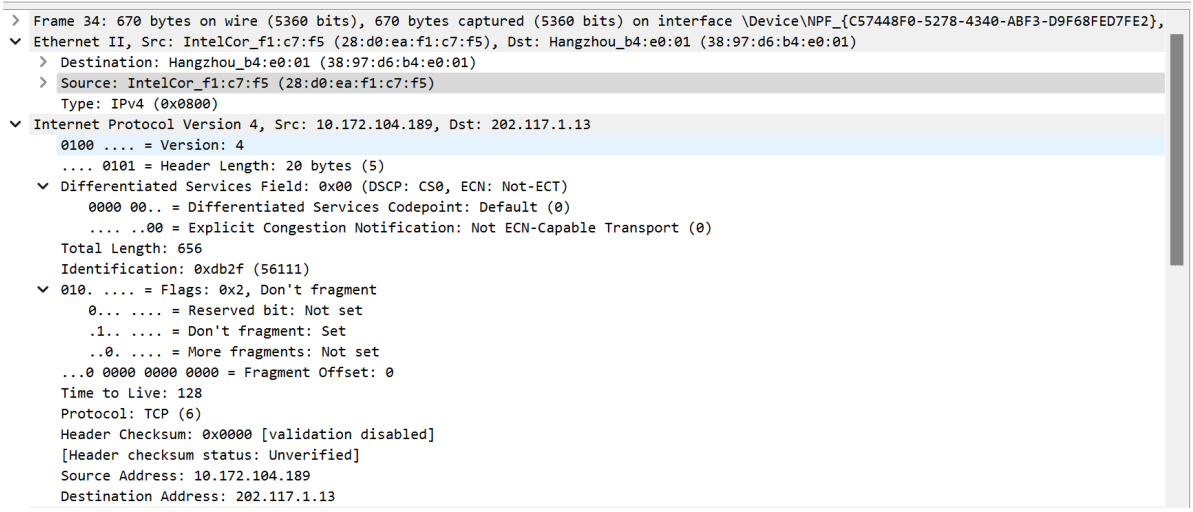
经历三次握手后，客户机和服务器的TCP连接正式建立。

HTTP

http请求：



Frame，Ethernet and IPv4：



传输时的网络层源地址IP又是客户机：10.172.104.189；而目标地址为IP：202.117.1.13，表明是www.xjtu.edu.cn的主机地址。表明此消息是客户机向服务器发送的。

TCP：

```
Transmission Control Protocol, Src Port: 52158, Dst Port: 80, Seq: 1, Ack: 1, Len: 616
    Source Port: 52158
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 616]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 28564178
    [Next Sequence Number: 617    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2355874377
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, 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
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····AP···]
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x416e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
```

此时的TCP部分说明了源端口端口号52158，和目标端口号80，表明消息是客户端发出到服务器的请求；

此消息的长度为616，确认号的标志位置为1；

这表明客户机向服务器发送HTTP请求时，TCP协议向服务器发送了确认消息，确认服务器是否收到了客户机发送的http建立请求。

HTTP:

```
Hypertext Transfer Protocol
  GET /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1440&h=900&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1440&h=900&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1 HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1440&h=900&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1
      Request URI Path: /system/resource/code/datainput.jsp
      Request URI Query: owner=1151962237&e=1&w=1440&h=900&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1
        Request URI Query Parameter: owner=1151962237
        Request URI Query Parameter: e=1
        Request URI Query Parameter: w=1440
        Request URI Query Parameter: h=900
        Request URI Query Parameter: treeid=1001
        Request URI Query Parameter: refer=
        Request URI Query Parameter: pagename=L2luZGV4LmpzcA%3D%3D
        Request URI Query Parameter: newsid=-1
    Request Version: HTTP/1.1
  Host: www.xjtu.edu.cn\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 Edg/118.0.2088.46\r\n
  Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
  Referer: http://www.xjtu.edu.cn/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  Cookie: _ga=GA1.3.1569066176.1676197486; JSESSIONID=D0D8329894F493D800AAF745C4A1A5D9\r\n
  \r\n
  [Full request URI: http://www.xjtu.edu.cn/system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1440&h=900&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1]
  [HTTP request 1/1]
  [Response in frame: 45]
```

Reset (tcp.flags.reset), 1 byte(s)　　分组: 455 · 已显示: 14 (3.1%)

http请求报答的格式：

```
GET(sapce)URL(space)HTTPversion\r\n
头部字段名：content\r\n
.
.
.
\r\n
```

URL：

```
/system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1440&h=900&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1
```

HTTP version：

```
HTTP/1.1\r\n
```

头部字段+\r\n：Host,Connection,User-Agent,Accept,Referer,Accept-Encoding,Accept-Language,Cookie

```
Host: www.xjtu.edu.cn\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 Edg/118.0.2088.46\r\n
Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
Referer: http://www.xjtu.edu.cn/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
Cookie: _ga=GA1.3.1569066176.1676197486; JSESSIONID=D0D8329894F493D800AAF745C4A1A5D9\r\n
\r\n
```

http应答：

```
45 5.047279    202.117.1.13      10.172.104.189    HTTP    853 HTTP/1.1 200 OK
```

Frame，Ethernet and IPv4：

```
> Frame 45: 853 bytes on wire (6824 bits), 853 bytes captured (6824 bits) on interface \Device\NPF_{C57448F0-5278-4340-ABF3-D9F68FED7FE2}, id 0
v Ethernet II, Src: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01), Dst: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
    > Destination: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
    > Source: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
      Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 202.117.1.13, Dst: 10.172.104.189
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
          0000 00.. = Differentiated Services Codepoint: Default (0)
          .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
      Total Length: 839
      Identification: 0xe847 (59463)
    v 010. .... = Flags: 0x2, Don't fragment
          0... .... = Reserved bit: Not set
          .1.. .... = Don't fragment: Set
          ..0. .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 60
      Protocol: TCP (6)
      Header Checksum: 0x147e [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 202.117.1.13
      Destination Address: 10.172.104.189
```

TCP：

```
v Transmission Control Protocol, Src Port: 80, Dst Port: 52158, Seq: 1, Ack: 617, Len: 799
      Source Port: 80
      Destination Port: 52158
      [Stream index: 4]
      [Conversation completeness: Complete, WITH_DATA (31)]
      [TCP Segment Len: 799]
      Sequence Number: 1    (relative sequence number)
      Sequence Number (raw): 2355874377
      [Next Sequence Number: 800    (relative sequence number)]
      Acknowledgment Number: 617    (relative ack number)
      Acknowledgment number (raw): 28564794
      0101 .... = Header Length: 20 bytes (5)
    v Flags: 0x018 (PSH, 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
          .... .... 1... = Push: Set
          .... .... .0.. = Reset: Not set
          .... .... ..0. = Syn: Not set
          .... .... ...0 = Fin: Not set
          [TCP Flags: ·····AP···]
      Window: 124
      [Calculated window size: 15872]
      [Window size scaling factor: 128]
      Checksum: 0x0f9e [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    > [Timestamps]
```

HTTP：

http应答报文格式：

```
HTTPversion(space)状态码(space)状态信息\r\n
头部字段名：content\r\n
.
.
.
\r\n
```

状态行：

```
HTTP/1.1 200 OK\r\n
```

200表示客户端请求成功；

头部段：

```
Date: Mon, 23 Oct 2023 01:11:01 GMT\r\n
Server: China Webber /1.1\r\n
X-Frame-Options: SAMEORIGIN\r\n
X-XSS-Protection: 1; mode=block\r\n
X-Content-Type-Options: nosniff\r\n
Referer-Policy: no-referer-when-downgrade\r\n
X-Download-Options: noopen\r\n
X-Permitted-Cross-Domain-Policies: master-only\r\n
 [truncated]Content-Security-Policy: default-src 'self' data:
Cache-Control: no-store\r\n
Pragma: no-cache\r\n
Expires: Thu, 01 Jan 1970 00:00:00 GMT\r\n
Content-Type: image/gif;charset=UTF-8\r\n
Content-Length: 0\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Language: zh-CN\r\n
\r\n
```

TCP四次挥手

```
 78 10.046082   202.117.1.13      10.172.104.189   TCP      60 80 → 52158 [FIN, ACK] Seq=800 Ack=617 Win=15872 Len=0
 79 10.046198   10.172.104.189    202.117.1.13     TCP      54 52158 → 80 [ACK] Seq=617 Ack=801 Win=130560 Len=0
325 11.275845   10.172.104.189    202.117.1.13     TCP      54 52158 → 80 [FIN, ACK] Seq=617 Ack=801 Win=130560 Len=0
327 11.280877   202.117.1.13      10.172.104.189   TCP      60 80 → 52158 [ACK] Seq=801 Ack=618 Win=15872 Len=0
```

1. FIN/ACK包：TCP连接的一方发送一个FIN（finish）标志的TCP包，表示它已经完成了数据传输，并且希望关闭连接。
2. ACK包：接收到FIN包的一方发送一个ACK（acknowledge）标志的TCP包，表示它已经收到了FIN包，并且同意关闭连接。
3. FIN/ACK包：接收到ACK包的一方发送一个带有FIN/ACK标志的TCP包，表示它也同意关闭连接。
4. ACK包：发送FIN/ACK包的一方接收到ACK包后，确认对方已同意关闭连接，然后发送一个ACK标志的TCP包，表示连接已经关闭。

第一次挥手：

```
 78 10.046082   202.117.1.13      10.172.104.189   TCP      60 80 → 52158 [FIN, ACK] Seq=800 Ack=617 Win=15872 Len=0
```

Frame，Ethernet and IPv4：

```
> Frame 78: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{C57448F0-5278-4340-ABF3-D9F68FED7FE2}, id 0
v Ethernet II, Src: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01), Dst: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
    > Destination: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
    > Source: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
      Type: IPv4 (0x0800)
      Padding: 000000000000
v Internet Protocol Version 4, Src: 202.117.1.13, Dst: 10.172.104.189
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
          0000 00.. = Differentiated Services Codepoint: Default (0)
          .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
      Total Length: 40
      Identification: 0xe848 (59464)
    v 010. .... = Flags: 0x2, Don't fragment
          0... .... = Reserved bit: Not set
          .1.. .... = Don't fragment: Set
          ..0. .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 60
      Protocol: TCP (6)
      Header Checksum: 0x179c [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 202.117.1.13
      Destination Address: 10.172.104.189
```

TCP：

```
Transmission Control Protocol, Src Port: 80, Dst Port: 52158, Seq: 800, Ack: 617, Len: 0
    Source Port: 80
    Destination Port: 52158
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 800    (relative sequence number)
    Sequence Number (raw): 2355875176
    [Next Sequence Number: 801    (relative sequence number)]
    Acknowledgment Number: 617    (relative ack number)
    Acknowledgment number (raw): 28564794
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x011 (FIN, 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
    .... .... ...1 = Fin: Set
      [Expert Info (Chat/Sequence): Connection finish (FIN)]
    [TCP Flags: ·····A···F]
    Window: 124
    [Calculated window size: 15872]
    [Window size scaling factor: 128]
    Checksum: 0x6b9b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
```

```
Source Address (ip.src), 4 byte(s)
```

源端口号是服务器端的80；而目的端口号为客户机端口号52128；

标志位的ACK和FIN置为1，说明这是一条服务器端向客户机发送的断开连接的请求。

相对确认号为617；

第二次挥手：

```
 79 10.046198   10.172.104.189   202.117.1.13      TCP      54 52158 → 80 [ACK] Seq=617 Ack=801 Win=130560 Len=0
```

Frame，Ethernet and IPv4：

```
Frame 79: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C57448F0-5278-4340-ABF3-D9F68FED7FE2}, id 0
Ethernet II, Src: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5), Dst: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  Destination: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  Source: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.172.104.189, Dst: 202.117.1.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 40
  Identification: 0xdb31 (56113)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...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: 10.172.104.189
  Destination Address: 202.117.1.13
```

TCP：

```
Transmission Control Protocol, Src Port: 52158, Dst Port: 80, Seq: 617, Ack: 801, Len: 0
    Source Port: 52158
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 617    (relative sequence number)
    Sequence Number (raw): 28564794
    [Next Sequence Number: 617    (relative sequence number)]
    Acknowledgment Number: 801    (relative ack number)
    Acknowledgment number (raw): 2355875177
    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: 510
    [Calculated window size: 130560]
    [Window size scaling factor: 256]
    Checksum: 0x3f06 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
```

源端口号为客户机的52128；而目的端口号为服务器端的80端口；

标志位的ACK置为1；

第一次挥手服务器向客户机发出断开连接的请求后，第二次挥手时客户机向服务器端发送确认消息，表明服务器到客户机的连接已经断开；

第三次挥手：

```
325 11.275845   10.172.104.189   202.117.1.13     TCP      54 52158 → 80 [FIN, ACK] Seq=617 Ack=801 Win=130560 Len=0
```

Frame，Ethernet and IPv4：

```
Frame 325: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C57448F0-5278-4340-ABF3-D9F68FED7FE2}, id 0
Ethernet II, Src: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5), Dst: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  Destination: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
  Source: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.172.104.189, Dst: 202.117.1.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 40
  Identification: 0xdb32 (56114)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...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: 10.172.104.189
  Destination Address: 202.117.1.13
```

TCP：

```
Transmission Control Protocol, Src Port: 52158, Dst Port: 80, Seq: 617, Ack: 801, Len: 0
    Source Port: 52158
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 617    (relative sequence number)
    Sequence Number (raw): 28564794
    [Next Sequence Number: 618    (relative sequence number)]
    Acknowledgment Number: 801    (relative ack number)
    Acknowledgment number (raw): 2355875177
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x011 (FIN, 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
    > .... .... ...1 = Fin: Set
    > [TCP Flags: ·····A···F]
    Window: 510
    [Calculated window size: 130560]
    [Window size scaling factor: 256]
    Checksum: 0x3f06 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

源端口号为客户机的52128端口；而目的端口号为服务器端的80端口；

标志位的ACK和FIN置为1；

说明第三次挥手即是客户机向服务器端发出了断开连接的请求；

第四次挥手：

```
327 11.280877   202.117.1.13     10.172.104.189    TCP      60 80 → 52158 [ACK] Seq=801 Ack=618 Win=15872 Len=0
```

Frame，Ethernet and IPv4：

```
> Frame 327: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{C57448F0-5278-4340-ABF3-D9F68FED7FE2}, id 0
Ethernet II, Src: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01), Dst: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
  > Destination: IntelCor_f1:c7:f5 (28:d0:ea:f1:c7:f5)
  > Source: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
    Type: IPv4 (0x0800)
    Padding: 000000000000
Internet Protocol Version 4, Src: 202.117.1.13, Dst: 10.172.104.189
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 40
    Identification: 0xe849 (59465)
  010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 60
    Protocol: TCP (6)
    Header Checksum: 0x179b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 202.117.1.13
    Destination Address: 10.172.104.189
```

TCP：

```
Transmission Control Protocol, Src Port: 80, Dst Port: 52158, Seq: 801, Ack: 618, Len: 0
    Source Port: 80
    Destination Port: 52158
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 801    (relative sequence number)
    Sequence Number (raw): 2355875177
    [Next Sequence Number: 801    (relative sequence number)]
    Acknowledgment Number: 618    (relative ack number)
    Acknowledgment number (raw): 28564795
    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: 124
    [Calculated window size: 15872]
    [Window size scaling factor: 128]
    Checksum: 0x6b9a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
```

源端口号是服务器端的80；而目的端口号为客户机端口号52128端口；

第三次挥手是客户机向服务器端发出了断开连接的请求；服务器端收到这个请求后第四次挥手即是服务器端向客户机发出了ACK确认消息，断开了客户机到服务器的连接；

四次挥手之后，从服务器到客户机和从客户机到服务器端的两边连接都断开了。

五、心得体会

通过本次实验，我掌握了使用 wireshark 进行抓包的方法，并通过抓包学习了 HTTP 请 求与响应报文的格式，以及 TCP 协议建立连接时的三次握手过程和释放连接时的四次挥手过程，HTTP如何使用TCP的过程。