计算机网络第二次实验报告

2211421 何禹姗

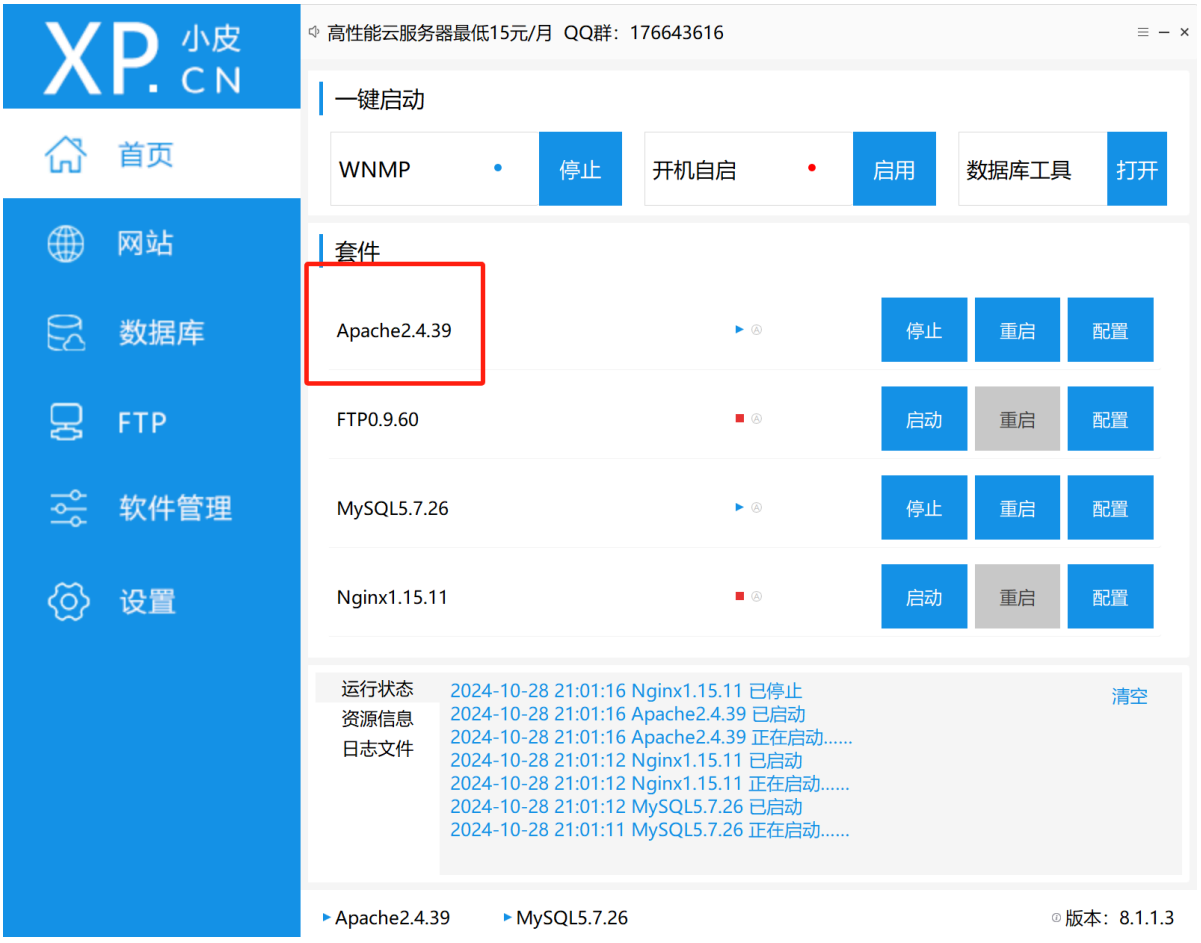
实验2：配置Web服务及分析HTTP交互过程

一、搭建Web服务器，并制作简单的Web页面

（一）搭建Web服务器

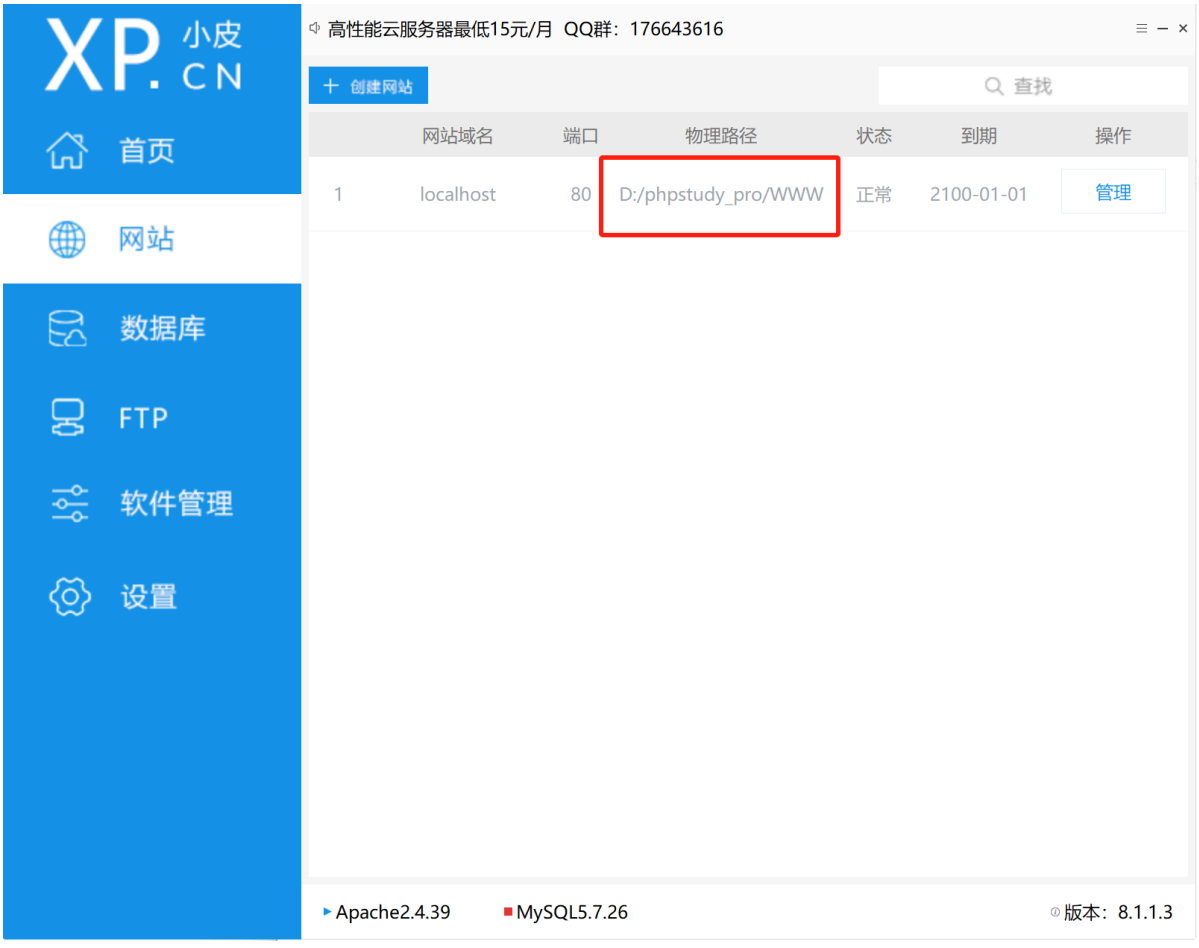
平台：phpstudy

（1）安装好phpstudy，启动Apache。



（2）打开浏览器，访问localhost，访问成功

（3）看到Web目录，将网站文件拖到该目录下，输入目录即可访问



（二）制作Web页面

编写main.html文件

```
<html>
    <head>
        <meta charset="utf-8">
        <title>computernetwork</title>
```

```
        <style>
            body {
                display: flex;
                flex-direction: column;
                align-items: center;
                justify-content: center;
                min-height: 100vh;
                margin: 0;
                padding: 20px;
                box-sizing: border-box;
            }
             h1 {
                font-size: 28px;
                color: #333;
                margin-bottom: 20px;
            }
            p {
                font-size: 16px;
                color: #666;
                line-height: 1.6;
            }
            img {
                width: 150px;
                height: auto;
                margin-top: 20px;
            }
        </style>
    </head>
    <body>
        <div class="content">
            <h1>个人信息</h1>
            <p>专业：计算机科学与技术</p>
            <p>学号：2211421</p>
            <p>姓名：何禹姗</p>
            <h1>个人LOGO</h1>
            <img src="头像.jpg" alt="个人头像"/>
            <h1>自我介绍音频</h1>
            <audio controls>
                <source src="自我介绍音频.m4a" type="audio/mpeg">
            </audio></div>
    </body>
</html>
```

包含文本信息（专业、学号、姓名）、自己的LOGO、自我介绍音频。

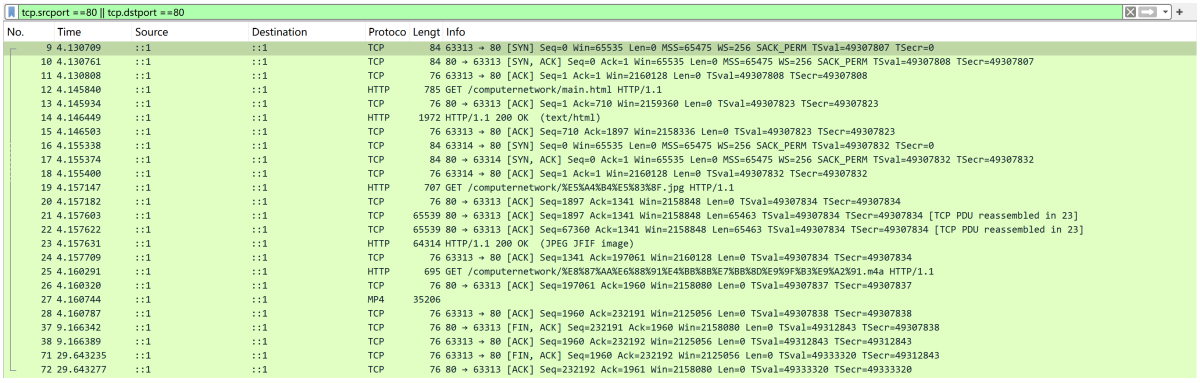
二、通过浏览器访问Web服务器，获取编写的HTML文档，并显示Web页面

输入http://localhost/computernetwork/main.html，即可显示Web页面

三、使用Wireshark捕获与Web服务器的交互过程

（一）Wireshark捕获过程

开启wireshark，选择 Adapter for lookback traffic capture，使用tcp.srcport ==80 || tcp.dstport ==80进行过滤，得到结果如图所示，图中”200 OK“说明抓包成功。

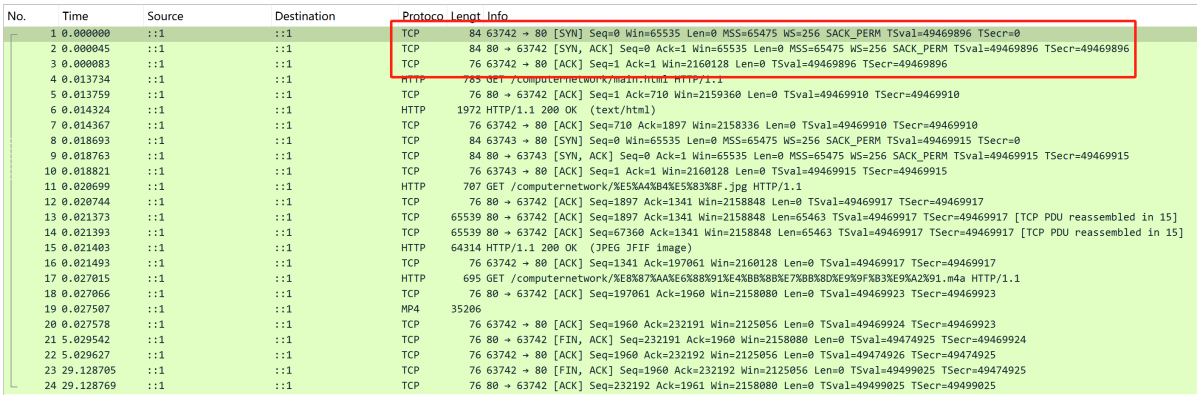


tcp.srcport ==80 || tcp.dstport ==80

No.	Time	Source	Destination	Protoco	Lengt	Info
9	4.130709	::1	::1	TCP	84	63313 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49307807 TSecr=0
10	4.130761	::1	::1	TCP	84	80 → 63313 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49307808 TSecr=49307807
11	4.130808	::1	::1	TCP	76	63313 → 80 [ACK] Seq=1 Ack=1 Win=2160128 Len=0 TSval=49307808 TSecr=49307808
12	4.145840	::1	::1	HTTP	785	GET /computernetwork/main.html HTTP/1.1
13	4.145934	::1	::1	TCP	76	80 → 63313 [ACK] Seq=1 Ack=710 Win=2159360 Len=0 TSval=49307823 TSecr=49307823
14	4.146449	::1	::1	HTTP	1972	HTTP/1.1 200 OK (text/html)
15	4.146503	::1	::1	TCP	76	63313 → 80 [ACK] Seq=710 Ack=1897 Win=2158336 Len=0 TSval=49307823 TSecr=49307823
16	4.155338	::1	::1	TCP	84	63314 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49307832 TSecr=0
17	4.155374	::1	::1	TCP	84	80 → 63314 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49307832 TSecr=49307832
18	4.155400	::1	::1	TCP	76	63314 → 80 [ACK] Seq=1 Ack=1 Win=2160128 Len=0 TSval=49307832 TSecr=49307832
19	4.157147	::1	::1	HTTP	707	GET /computernetwork/%E5%A4%B4%E5%83%8F.jpg HTTP/1.1
20	4.157182	::1	::1	TCP	76	80 → 63313 [ACK] Seq=1897 Ack=1341 Win=2158848 Len=0 TSval=49307834 TSecr=49307834
21	4.157603	::1	::1	TCP	65539	80 → 63313 [ACK] Seq=1897 Ack=1341 Win=2158848 Len=65463 TSval=49307834 TSecr=49307834 [TCP PDU reassembled in 23]
22	4.157622	::1	::1	TCP	65539	80 → 63313 [ACK] Seq=67360 Ack=1341 Win=2158848 Len=65463 TSval=49307834 TSecr=49307834 [TCP PDU reassembled in 23]
23	4.157631	::1	::1	HTTP	64314	HTTP/1.1 200 OK (JPEG JFIF image)
24	4.157709	::1	::1	TCP	76	63313 → 80 [ACK] Seq=1341 Ack=197061 Win=2160128 Len=0 TSval=49307834 TSecr=49307834
25	4.160291	::1	::1	HTTP	695	GET /computernetwork/%E8%87%AA%E6%88%91%E4%BB%8B%E7%BB%8D%E9%9F%B3%E9%A2%91.m4a HTTP/1.1
26	4.160320	::1	::1	TCP	76	80 → 63313 [ACK] Seq=197061 Ack=1960 Win=2158080 Len=0 TSval=49307837 TSecr=49307837
27	4.160744	::1	::1	MP4	35206	
28	4.160787	::1	::1	TCP	76	63313 → 80 [ACK] Seq=1960 Ack=232191 Win=2125056 Len=0 TSval=49307838 TSecr=49307838
37	9.166342	::1	::1	TCP	76	80 → 63313 [FIN, ACK] Seq=232191 Ack=1960 Win=2158080 Len=0 TSval=49312843 TSecr=49307838
38	9.166389	::1	::1	TCP	76	63313 → 80 [ACK] Seq=1960 Ack=232192 Win=2125056 Len=0 TSval=49312843 TSecr=49312843
71	29.643235	::1	::1	TCP	76	63313 → 80 [FIN, ACK] Seq=1960 Ack=232192 Win=2125056 Len=0 TSval=49333320 TSecr=49312843
72	29.643277	::1	::1	TCP	76	80 → 63313 [ACK] Seq=232192 Ack=1961 Win=2158080 Len=0 TSval=49333320 TSecr=49333320

（二）抓包分析

1、TCP三次握手连接建立过程



No.	Time	Source	Destination	Protoco	Lengt	Info
1	0.000000	::1	::1	TCP	84	63742 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49469896 TSecr=0
2	0.000045	::1	::1	TCP	84	80 → 63742 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49469896 TSecr=49469896
3	0.000083	::1	::1	TCP	76	63742 → 80 [ACK] Seq=1 Ack=1 Win=2160128 Len=0 TSval=49469896 TSecr=49469896
4	0.013734	::1	::1	HTTP	785	GET /computernetwork/main.html HTTP/1.1
5	0.013759	::1	::1	TCP	76	80 → 63742 [ACK] Seq=1 Ack=710 Win=2159360 Len=0 TSval=49469910 TSecr=49469910
6	0.014324	::1	::1	HTTP	1972	HTTP/1.1 200 OK (text/html)
7	0.014367	::1	::1	TCP	76	63742 → 80 [ACK] Seq=710 Ack=1897 Win=2158336 Len=0 TSval=49469910 TSecr=49469910
8	0.018693	::1	::1	TCP	84	63743 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49469915 TSecr=0
9	0.018763	::1	::1	TCP	84	80 → 63743 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM TSval=49469915 TSecr=49469915
10	0.018821	::1	::1	TCP	76	63743 → 80 [ACK] Seq=1 Ack=1 Win=2160128 Len=0 TSval=49469915 TSecr=49469915
11	0.020699	::1	::1	HTTP	707	GET /computernetwork/%E5%A4%B4%E5%83%8F.jpg HTTP/1.1
12	0.020744	::1	::1	TCP	76	80 → 63742 [ACK] Seq=1897 Ack=1341 Win=2158848 Len=0 TSval=49469917 TSecr=49469917
13	0.021373	::1	::1	TCP	65539	80 → 63742 [ACK] Seq=1897 Ack=1341 Win=2158848 Len=65463 TSval=49469917 TSecr=49469917 [TCP PDU reassembled in 15]
14	0.021393	::1	::1	TCP	65539	80 → 63742 [ACK] Seq=67360 Ack=1341 Win=2158848 Len=65463 TSval=49469917 TSecr=49469917 [TCP PDU reassembled in 15]
15	0.021403	::1	::1	HTTP	64314	HTTP/1.1 200 OK (JPEG JFIF image)
16	0.021493	::1	::1	TCP	76	63742 → 80 [ACK] Seq=1341 Ack=197061 Win=2160128 Len=0 TSval=49469917 TSecr=49469917
17	0.027015	::1	::1	HTTP	695	GET /computernetwork/%E8%87%AA%E6%88%91%E4%BB%8B%E7%BB%8D%E9%9F%B3%E9%A2%91.m4a HTTP/1.1
18	0.027066	::1	::1	TCP	76	80 → 63742 [ACK] Seq=197061 Ack=1960 Win=2158080 Len=0 TSval=49469923 TSecr=49469923
19	0.027507	::1	::1	MP4	35206	
20	0.027578	::1	::1	TCP	76	63742 → 80 [ACK] Seq=1960 Ack=232191 Win=2125056 Len=0 TSval=49469924 TSecr=49469923
21	5.029542	::1	::1	TCP	76	80 → 63742 [FIN, ACK] Seq=232191 Ack=1960 Win=2158080 Len=0 TSval=49474925 TSecr=49469924
22	5.029627	::1	::1	TCP	76	63742 → 80 [ACK] Seq=1960 Ack=232192 Win=2125056 Len=0 TSval=49474926 TSecr=49474925
23	29.128705	::1	::1	TCP	76	63742 → 80 [FIN, ACK] Seq=1960 Ack=232192 Win=2125056 Len=0 TSval=49499025 TSecr=49474925
24	29.128769	::1	::1	TCP	76	80 → 63742 [ACK] Seq=232192 Ack=1961 Win=2158080 Len=0 TSval=49499025 TSecr=49499025

（1）第一次握手：客户端发送一个SYN=1，ACK=0标志的数据包给客户端，请求进行连接。

第一次握手，客户端发送一个带有SYN标志位的TCP包给服务器，标志位SYN=1，意为请求连接，客户端进入SYN_SENT状态；ACK=0，表示当前没有接收到数据；SYN包的序列号Seq=0即初始建立连接值为0，数据包相对序列号从0开始，表示当前还没有发送数据。客户端发送SYN报文，并置发送序号Seq=x。

该数据包具体信息如下图所示：

```
> Frame 9: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_Loopback, id
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 63742, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 63742
    Destination Port: 80
    [Stream index: 2]
    [Stream Packet Number: 1]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3484585347
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x002 (SYN)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x1aae [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamp
  > [Timestamps]
```

Frame 9表示要发送的数据块为第9帧，在线路上的实际字节数为84字节，捕获的字节数也是84字节。

这条TCP数据包是在本地回环地址 (::1) 上发送的，源端口为63742，目的端口为80（HTTP端口）。

窗口大小为65535，头部长度为40字节，确认号ACK和序列号Seq均为0。

（2）第二次握手：服务端收到请求并且允许连接，发送一个SYN=1,ACK=1标志的数据包给发送端，表示可以通讯，并且客户端发送一个确认数据包。

服务器收到客户端的SYN包后，发送一个带有SYN和ACK标志位的TCP包作为相应，服务器进入SYN_RCVD状态。Seq=0表示初始建立值为0，表示当前还没有发送数据。服务端发送SYN+ACK报文，并置发送序号Seq=y，确认序号ACK=x+1。

该数据包具体信息如下图所示：

```
> Frame 10: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_Loopback, ic
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 80, Dst Port: 63742, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 63742
    [Stream index: 2]
    [Stream Packet Number: 2]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2683230820
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3484585348
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0xc38e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamp
  > [Timestamps]
  > [SEQ/ACK analysis]
```

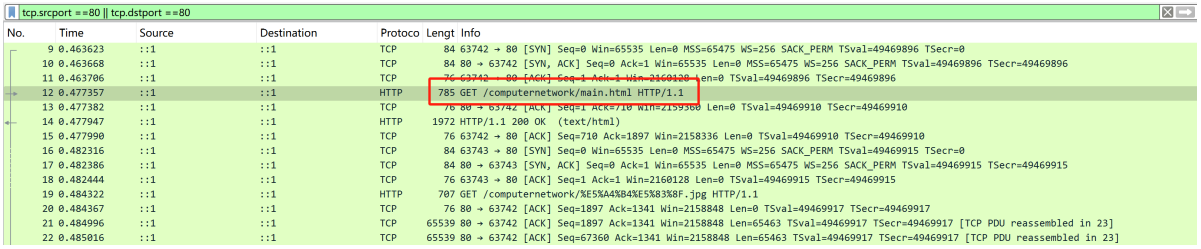
（3）第三次握手：服务端发送一个SYN=0,ACK=1的数据包给客户端，表示连接已被确认，此时TCP连接建立，开始通讯。

客户端收到服务器的SYN+ACK包后，发送一个带有ACK标志位的TCP包作为确认，ACK=1。此时客户端进入ESTABLISHED状态，服务器收到客户端的ACK包后，也进入ESTABLISHED状态。Seq=1，表示当前已经发送了1个数据。客户端发送ACK报文，并置发送序号Seq=z，确认序号ACK=y+1。

该数据包具体信息如下图所示：

```
> Frame 11: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_Loopback,
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 63742, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 63742
    Destination Port: 80
    [Stream index: 2]
    [Stream Packet Number: 3]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3484585348
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2683230821
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 8438
    [Calculated window size: 2160128]
    [Window size scaling factor: 256]
    Checksum: 0xcb75 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
```

2、三次握手后，浏览器和目的主机开始传输数据并进行http访问。浏览器向域名发出GET请求报文



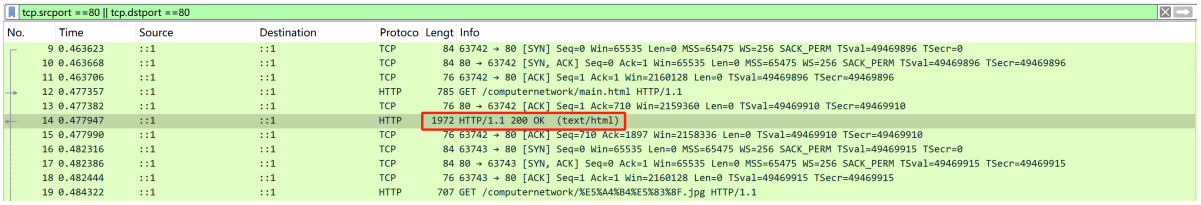
此时，使用的协议为HTTP/1.1，请求访问界面为main.html，请求访问方式为GET。

GET请求的包具体内容如下：

```
> Frame 4: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface \Device\NPF_Loopba
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 63742, Dst Port: 80, Seq: 1, Ack: 1, Len: 709
v Hypertext Transfer Protocol
  v GET /computernetwork/main.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /computernetwork/main.html
      Request Version: HTTP/1.1
    Host: localhost\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126", "Google Chrome";v="126"\r\n
    sec-ch-ua-mobile: ?0\r\n
    sec-ch-ua-platform: "Windows"\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/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
    Sec-Fetch-Site: none\r\n
    Sec-Fetch-Mode: navigate\r\n
    Sec-Fetch-User: ?1\r\n
    Sec-Fetch-Dest: document\r\n
    Accept-Encoding: gzip, deflate, br, zstd\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
    \r\n
```

GET / HTTP/1.1\r\n称为请求行，由三个部分组成：请求方法、URL、HTTP协议版本。这条TCP数据包包含了HTTP请求的部分，请求方法为GET，目标URL为 /computernetwork /main.html，HTTP协议版本为1.1。

3、请求被目的主机通过后，回应其封装好的HTML形式数据，即响应报文，200 OK表示客户端请求成功

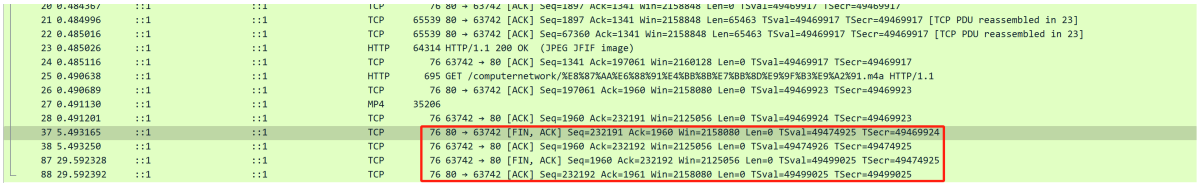


具体数据内容如下：

```
> Frame 6: 1972 bytes on wire (15776 bits), 1972 bytes captured (15776 bits) on interface \Device\NPF_Lo
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 80, Dst Port: 63742, Seq: 1, Ack: 710, Len: 1896
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 29 Oct 2024 02:17:25 GMT\r\n
    Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02\r\n
    Last-Modified: Tue, 29 Oct 2024 02:14:05 GMT\r\n
    ETag: "617-6259423c7283b"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 1559\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n
    [Request in frame: 4]
    [Time since request: 0.000590000 seconds]
    [Request URI: /computernetwork/main.html]
    [Full request URI: http://localhost/computernetwork/main.html]
    File Data: 1559 bytes
```

响应报文由状态行、响应头部、空行和响应体四部分组成。状态行给出响应HTTP协议的版本号，响应返回状态码，响应描述；响应头部返回服务器的基本信息，响应体为请求的数据。

4、TCP的四次挥手



（1）第一次挥手

服务器发送一个请求结束的报文【FIN,ACK】给客户端以关闭数据传送，服务器进入FIN_WAIT1状态，置seq=x，ack=y。

```
> Frame 21: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_Loopback, i
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 80, Dst Port: 63742, Seq: 232191, Ack: 1960, Len: 0
    Source Port: 80
    Destination Port: 63742
    [Stream index: 0]
    [Stream Packet Number: 18]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 232191    (relative sequence number)
    Sequence Number (raw): 2683463011
    [Next Sequence Number: 232192    (relative sequence number)]
    Acknowledgment Number: 1960    (relative ack number)
    Acknowledgment number (raw): 3484587307
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x011 (FIN, ACK)
    Window: 8430
    [Calculated window size: 2158080]
    [Window size scaling factor: 256]
    Checksum: 0x2513 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
```

(2) 第二次挥手

客户端接收到服务器发送的【FIN,ACK】并发送【ACK】表示确认，此时客户端进入CLOSE_WAIT状态，服务器收到客户端的【ACK】后，进入FIN_WAIT2状态，置seq=y，ack=x+1。

```
> Frame 22: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_Loopback,
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 63742, Dst Port: 80, Seq: 1960, Ack: 232192, Len: 0
    Source Port: 63742
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 19]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1960    (relative sequence number)
    Sequence Number (raw): 3484587307
    [Next Sequence Number: 1960    (relative sequence number)]
    Acknowledgment Number: 232192    (relative ack number)
    Acknowledgment number (raw): 2683463012
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 8301
    [Calculated window size: 2125056]
    [Window size scaling factor: 256]
    Checksum: 0x120a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
```

(3) 第三次挥手

客户端发送一个【FIN,ACK】以关闭服务器到服务器的数据传送，进入LAST_ACK状态，置seq=y，ack=x+1。

```
> Frame 23: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_Loopback, id
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 63742, Dst Port: 80, Seq: 1960, Ack: 232192, Len: 0
    Source Port: 63742
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 20]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1960    (relative sequence number)
    Sequence Number (raw): 3484587307
    [Next Sequence Number: 1961    (relative sequence number)]
    Acknowledgment Number: 232192    (relative ack number)
    Acknowledgment number (raw): 2683463012
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x011 (FIN, ACK)
    Window: 8301
    [Calculated window size: 2125056]
    [Window size scaling factor: 256]
    Checksum: 0xb3e5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
```

(4) 第四次挥手

服务器收到客户端发送的【FIN,ACK】并发送【ACK】，此时服务器进入TIME_WAIT状态，关闭连接，客户端收到服务器的【ACK】，关闭连接，置seq=x+1，ack=y+1。

```
> Frame 24: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_Loopback,
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 80, Dst Port: 63742, Seq: 232192, Ack: 1961, Len: 0
    Source Port: 80
    Destination Port: 63742
    [Stream index: 0]
    [Stream Packet Number: 21]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 232192    (relative sequence number)
    Sequence Number (raw): 2683463012
    [Next Sequence Number: 232192    (relative sequence number)]
    Acknowledgment Number: 1961    (relative ack number)
    Acknowledgment number (raw): 3484587308
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 8430
    [Calculated window size: 2158080]
    [Window size scaling factor: 256]
    Checksum: 0x5540 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
```

至此，HTTP交互完成。