

# 计算机网络第二次编程作业

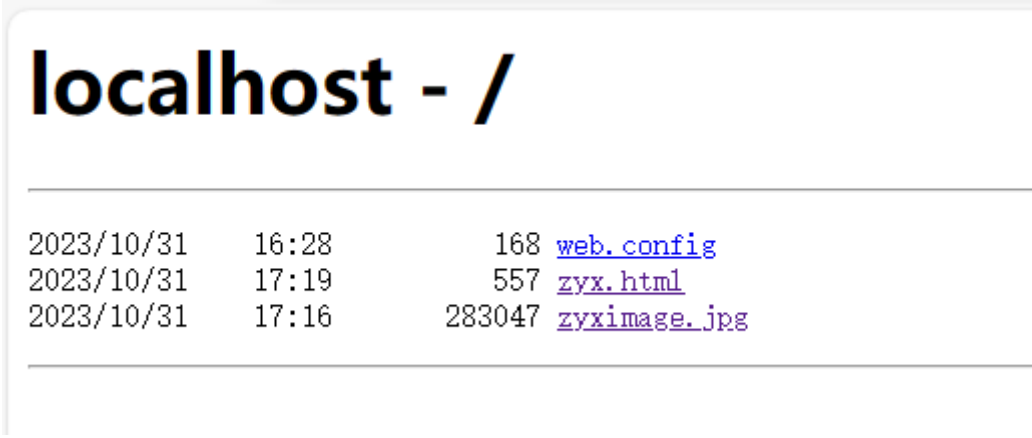
2112079 朱奕翔 计算机科学与技术

## 实验要求

- (1) 搭建Web服务器（自由选择系统），并制作简单的Web页面，包含简单文本信息（至少包含专业、学号、姓名）、自己的LOGO、自我介绍的音频信息。页面不要太复杂，包含要求的基本信息即可。
- (2) 通过浏览器获取自己编写的Web页面，使用Wireshark捕获浏览器与Web服务器的交互过程，并进行简单的分析说明。
- (3) 使用HTTP，不要使用HTTPS。
- (4) 提交实验报告。

## 一、搭建Web服务器

在本机上搭建Web服务器，设置的端口为8080，搭建好之后访问http://localhost:8080/出现如下界面表明搭建



## 二、制作简单的Web页面并通过浏览器浏览

利用vscode和相关插件能够快速制定html框架，在body部分填入自己的个人信息，照片，自我介绍的音频信息等。html文件存在搭建服务器时设定的文件夹内，这样在访问上述网站时就能选择访问该网页。一个简单的Web页面制作完成，并如图所示成功通过浏览器进行浏览。

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>zyx</title>
</head>
<body>
  <h1>个人信息</h1>
  
  <br>
```

朱奕翔

<br>

2112079

<br>

计算机科学与技术

<br>

<audio controls="controls" loop="loop">

<source src="./media/自我介绍.mp3" type="audio/mp3">

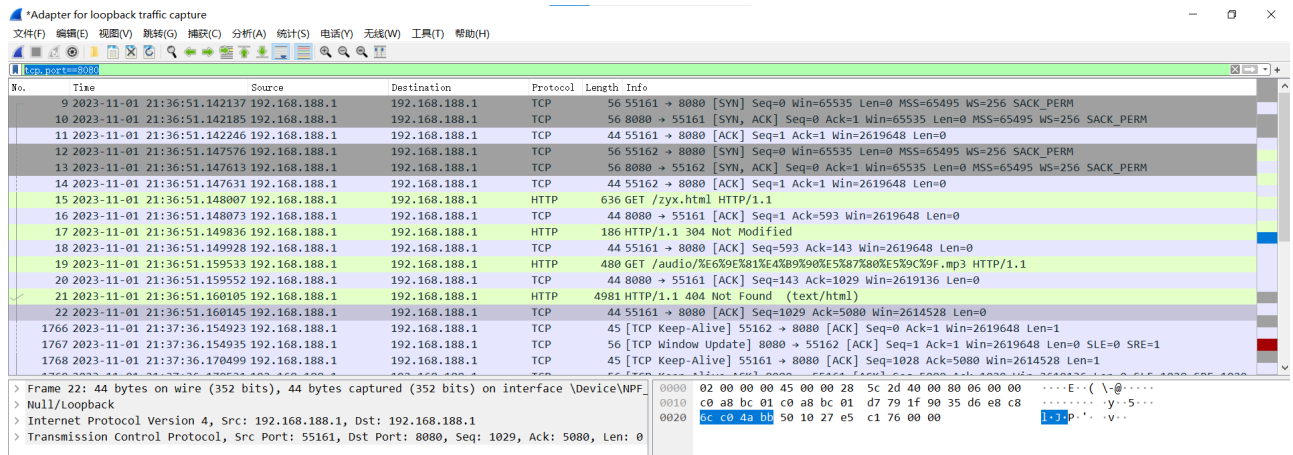
</audio>

</body>

</html>

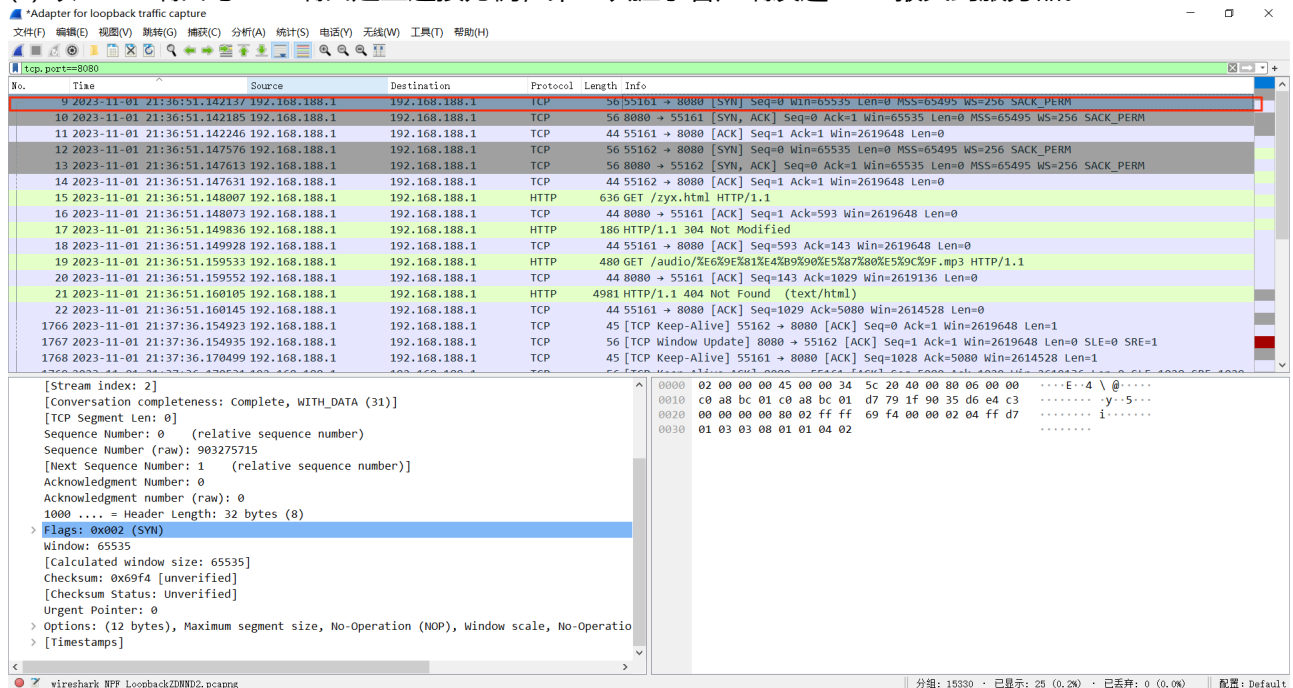
### 三、Wireshark捕获Web浏览器和服务器的交互过程

1. 由于是在本机搭建的服务器，通过本机主机的内部通信，而不经物理网络，因此通过Adapter for loopback traffic capture网络适配器来进行抓包。通过加入过滤条件tcp.port==8080能够清晰地看到与8080端口有关的交互过程。



2. 建立连接的过程称为“三次握手”

(1) 以55161端口与8080端口建立连接为例，第一次握手客户端发送 SYN 报文到服务器。



## (2) 第二次，服务器接收到 客户端的SYN 报文，回复 SYN + ACK 报文。

\*Adapter for loopback traffic capture

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

tcp.port==8080

No.	Time	Source	Destination	Protocol	Length	Info
9	2023-11-01 21:36:51.142137	192.168.188.1	192.168.188.1	TCP	56	55161 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
10	2023-11-01 21:36:51.142185	192.168.188.1	192.168.188.1	TCP	56	8080 → 55161 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
11	2023-11-01 21:36:51.142246	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
12	2023-11-01 21:36:51.147576	192.168.188.1	192.168.188.1	TCP	56	55162 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
13	2023-11-01 21:36:51.147613	192.168.188.1	192.168.188.1	TCP	56	8080 → 55162 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
14	2023-11-01 21:36:51.147631	192.168.188.1	192.168.188.1	TCP	44	55162 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
15	2023-11-01 21:36:51.148007	192.168.188.1	192.168.188.1	HTTP	636	GET /zyx.html HTTP/1.1
16	2023-11-01 21:36:51.148073	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=1 Ack=593 Win=2619648 Len=0
17	2023-11-01 21:36:51.149836	192.168.188.1	192.168.188.1	HTTP	186	HTTP/1.1 304 Not Modified
18	2023-11-01 21:36:51.149928	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=593 Ack=143 Win=2619648 Len=0
19	2023-11-01 21:36:51.159533	192.168.188.1	192.168.188.1	HTTP	480	GET /audio/2E6%9E%81%E4%B9%90%E5%87%80%E5%9C%9F.mp3 HTTP/1.1
20	2023-11-01 21:36:51.159552	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=143 Ack=1029 Win=2619136 Len=0
21	2023-11-01 21:36:51.160105	192.168.188.1	192.168.188.1	HTTP	4981	HTTP/1.1 404 Not Found (text/html)
22	2023-11-01 21:36:51.160145	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1029 Ack=5080 Win=2614528 Len=0
1766	2023-11-01 21:37:36.154923	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55162 → 8080 [ACK] Seq=0 Ack=1 Win=2619648 Len=1
1767	2023-11-01 21:37:36.154935	192.168.188.1	192.168.188.1	TCP	56	[TCP Window Update] 8080 → 55162 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 SLE=0 SRE=1
1768	2023-11-01 21:37:36.170499	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55161 → 8080 [ACK] Seq=1028 Ack=5080 Win=2614528 Len=1

[Stream index: 2]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 1824536291  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 903275716  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x012 (SYN, ACK)  
Window: 65535  
[Calculated window size: 65535]  
Checksum: 0xc63f [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation  
[Timestamps]  
[csum/ack analysis]

0000 02 00 00 00 45 00 00 34 5c 21 40 00 80 06 00 00 .....E...4\l@.....  
0010 c0 a8 bc 01 c0 a8 bc 01 1f 90 d7 79 6c c0 36 e3 .....y1-6-  
0020 35 d6 e4 c4 80 12 ff ff c6 3f 00 00 02 04 ff d7 .....5.....?  
0030 01 03 03 08 01 01 04 02 .....1.....

## (3) 第三次，客户端接收到服务端的 SYN+ACK 报文后，回复 ACK 报文

\*Adapter for loopback traffic capture

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

tcp.port==8080

No.	Time	Source	Destination	Protocol	Length	Info
9	2023-11-01 21:36:51.142137	192.168.188.1	192.168.188.1	TCP	56	55161 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
10	2023-11-01 21:36:51.142185	192.168.188.1	192.168.188.1	TCP	56	8080 → 55161 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
11	2023-11-01 21:36:51.142246	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
12	2023-11-01 21:36:51.147576	192.168.188.1	192.168.188.1	TCP	56	55162 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
13	2023-11-01 21:36:51.147613	192.168.188.1	192.168.188.1	TCP	56	8080 → 55162 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
14	2023-11-01 21:36:51.147631	192.168.188.1	192.168.188.1	TCP	44	55162 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
15	2023-11-01 21:36:51.148007	192.168.188.1	192.168.188.1	HTTP	636	GET /zyx.html HTTP/1.1
16	2023-11-01 21:36:51.148073	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=1 Ack=593 Win=2619648 Len=0
17	2023-11-01 21:36:51.149836	192.168.188.1	192.168.188.1	HTTP	186	HTTP/1.1 304 Not Modified
18	2023-11-01 21:36:51.149928	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=593 Ack=143 Win=2619648 Len=0
19	2023-11-01 21:36:51.159533	192.168.188.1	192.168.188.1	HTTP	480	GET /audio/2E6%9E%81%E4%B9%90%E5%87%80%E5%9C%9F.mp3 HTTP/1.1
20	2023-11-01 21:36:51.159552	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=143 Ack=1029 Win=2619136 Len=0
21	2023-11-01 21:36:51.160105	192.168.188.1	192.168.188.1	HTTP	4981	HTTP/1.1 404 Not Found (text/html)
22	2023-11-01 21:36:51.160145	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1029 Ack=5080 Win=2614528 Len=0
1766	2023-11-01 21:37:36.154923	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55162 → 8080 [ACK] Seq=0 Ack=1 Win=2619648 Len=1
1767	2023-11-01 21:37:36.154935	192.168.188.1	192.168.188.1	TCP	56	[TCP Window Update] 8080 → 55162 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 SLE=0 SRE=1
1768	2023-11-01 21:37:36.170499	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55161 → 8080 [ACK] Seq=1028 Ack=5080 Win=2614528 Len=1

[Stream index: 2]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 903275716  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 1824536292  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window: 10233  
[Calculated window size: 2619648]  
[Window size scaling factor: 256]  
Checksum: 0xd93d [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options:  
[Timestamps]  
[csum/ack analysis]

0000 02 00 00 00 45 00 00 28 5c 22 40 00 80 06 00 00 .....E...(\@.....  
0010 c0 a8 bc 01 c0 a8 bc 01 d7 79 1f 90 35 d6 e4 c4 .....y..5...  
0020 6c c0 36 e4 50 10 27 f9 d9 3d 00 00 .....1.6.....

## 3. 断开连接的过程称为“四次挥手”

### (1)客户端A发送一个FIN，用来关闭客户A到服务器B的数据传送。

The screenshot shows a Wireshark packet capture of a TCP connection. The packet list on the left shows a sequence of packets. Packet 2341, at time 2023-11-01 21:38:19.181168, is a TCP packet from 192.168.188.1 to 192.168.188.1. The packet details pane shows the following information:

- Stream index: 2
- Conversation completeness: Complete, WITH\_DATA (31)
- TCP Segment Len: 0
- Sequence Number: 1029 (relative sequence number)
- Sequence Number (raw): 903276744
- Next Sequence Number: 1030 (relative sequence number)
- Acknowledgment Number: 5080 (relative ack number)
- Acknowledgment number (raw): 1824541371
- 0101 ... = Header Length: 20 bytes (5)
- Flags: 0x011 (FIN, ACK)
- Window: 10213
- [Calculated window size: 2614528]
- [Window size scaling factor: 256]
- Checksum: 0xc175 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]

The packet bytes pane shows the raw data of the packet, including the header and the body.

### (2)服务器B收到这个FIN，它发回一个ACK，确认序号为收到的序号加1。和SYN一样，一个FIN将占用一个序号。

The screenshot shows a Wireshark packet capture of a TCP connection. The packet list on the left shows a sequence of packets. Packet 2341, at time 2023-11-01 21:38:19.181168, is a TCP packet from 192.168.188.1 to 192.168.188.1. The packet details pane shows the following information:

- Stream index: 2
- Conversation completeness: Complete, WITH\_DATA (31)
- TCP Segment Len: 0
- Sequence Number: 5080 (relative sequence number)
- Sequence Number (raw): 1824541371
- Next Sequence Number: 5080 (relative sequence number)
- Acknowledgment Number: 1030 (relative ack number)
- Acknowledgment number (raw): 903276745
- 0101 ... = Header Length: 20 bytes (5)
- Flags: 0x010 (ACK)
- Window: 10231
- [Calculated window size: 2619136]
- [Window size scaling factor: 256]
- Checksum: 0xc163 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [Seq/ACK analysis]

The packet bytes pane shows the raw data of the packet, including the header and the body.

### (3)服务器B关闭与客户端A的连接，发送一个FIN给客户端A。

Adapter for loopback traffic capture

文件(F) 编辑(E) 视图(V) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

tcp.port==8080

No.	Time	Source	Destination	Protocol	Length	Info
17	2023-11-01 21:36:51.149836	192.168.188.1	192.168.188.1	HTTP	186	HTTP/1.1 304 Not Modified
18	2023-11-01 21:36:51.149928	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=593 Ack=143 Win=2619648 Len=0
19	2023-11-01 21:36:51.159533	192.168.188.1	192.168.188.1	HTTP	480	GET /audio/EE6X9E81E4X89%00%E5%87%80%E5%9C%9F.mp3 HTTP/1.1
20	2023-11-01 21:36:51.159552	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=143 Ack=1029 Win=2619136 Len=0
21	2023-11-01 21:36:51.160105	192.168.188.1	192.168.188.1	HTTP	4981	HTTP/1.1 404 Not Found (text/html)
22	2023-11-01 21:36:51.160145	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1029 Ack=5080 Win=2614528 Len=0
1766	2023-11-01 21:37:36.154923	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55162 → 8080 [ACK] Seq=0 Ack=1 Win=2619648 Len=1
1767	2023-11-01 21:37:36.154935	192.168.188.1	192.168.188.1	TCP	56	[TCP Window Update] 8080 → 55162 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 SLE=0 SRE=1
1768	2023-11-01 21:37:36.170499	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55161 → 8080 [ACK] Seq=1028 Ack=5080 Win=2614528 Len=1
1769	2023-11-01 21:37:36.170531	192.168.188.1	192.168.188.1	TCP	56	[TCP Keep-Alive ACK] 8080 → 55161 [ACK] Seq=5080 Ack=1029 Win=2619136 Len=0 SLE=1028 SRE=1029
2333	2023-11-01 21:38:19.180377	192.168.188.1	192.168.188.1	TCP	44	55162 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=2619648 Len=0
2334	2023-11-01 21:38:19.180435	192.168.188.1	192.168.188.1	TCP	44	8080 → 55162 [ACK] Seq=1 Ack=2 Win=2619648 Len=0
2335	2023-11-01 21:38:19.180512	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [FIN, ACK] Seq=1029 Ack=5080 Win=2614528 Len=0
2336	2023-11-01 21:38:19.180536	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=5080 Ack=1030 Win=2619136 Len=0
2341	2023-11-01 21:38:19.181168	192.168.188.1	192.168.188.1	TCP	44	8080 → 55162 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
2342	2023-11-01 21:38:19.181196	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [FIN, ACK] Seq=5080 Ack=1030 Win=2619136 Len=0
2343	2023-11-01 21:38:19.181209	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1030 Ack=5081 Win=2614528 Len=0

[Stream index: 2]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 5080 (relative sequence number)  
Sequence Number (raw): 1824541371  
[Next Sequence Number: 5081 (relative sequence number)]  
Acknowledgment Number: 1030 (relative ack number)  
Acknowledgment number (raw): 903276745  
0101 ... = Header Length: 20 bytes (5)  
Flags: 0x011 (FIN, ACK)  
Window: 10231  
[Calculated window size: 2619136]  
[Window size scaling factor: 256]  
Checksum: 0xc162 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]

0000 02 00 00 00 45 00 00 28 5c 37 40 00 80 06 00 00 .....E..(\7@.....  
0010 c0 a8 bc 01 c0 a8 bc 01 1f 90 d7 79 6c c0 4a bb .....y..J..  
0020 35 d6 e8 c9 50 11 27 f7 c1 62 00 00 .....5...b..

Flags (12 bits) (tcp.flags), 2 byte(s) 分组: 15330 · 已显示: 25 (0.2%) · 已丢弃: 0 (0.0%) 配置: Default

(4)客户端A发回ACK报文确认，并将确认序号设置为收到序号加1。

tcp.port==8080

No.	Time	Source	Destination	Protocol	Length	Info
17	2023-11-01 21:36:51.149836	192.168.188.1	192.168.188.1	HTTP	186	HTTP/1.1 304 Not Modified
18	2023-11-01 21:36:51.149928	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=593 Ack=143 Win=2619648 Len=0
19	2023-11-01 21:36:51.159533	192.168.188.1	192.168.188.1	HTTP	480	GET /audio/EE6X9E81E4X89%00%E5%87%80%E5%9C%9F.mp3 HTTP/1.1
20	2023-11-01 21:36:51.159552	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=143 Ack=1029 Win=2619136 Len=0
21	2023-11-01 21:36:51.160105	192.168.188.1	192.168.188.1	HTTP	4981	HTTP/1.1 404 Not Found (text/html)
22	2023-11-01 21:36:51.160145	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1029 Ack=5080 Win=2614528 Len=0
1766	2023-11-01 21:37:36.154923	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55162 → 8080 [ACK] Seq=0 Ack=1 Win=2619648 Len=1
1767	2023-11-01 21:37:36.154935	192.168.188.1	192.168.188.1	TCP	56	[TCP Window Update] 8080 → 55162 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 SLE=0 SRE=1
1768	2023-11-01 21:37:36.170499	192.168.188.1	192.168.188.1	TCP	45	[TCP Keep-Alive] 55161 → 8080 [ACK] Seq=1028 Ack=5080 Win=2614528 Len=1
1769	2023-11-01 21:37:36.170531	192.168.188.1	192.168.188.1	TCP	56	[TCP Keep-Alive ACK] 8080 → 55161 [ACK] Seq=5080 Ack=1029 Win=2619136 Len=0 SLE=1028 SRE=1029
2333	2023-11-01 21:38:19.180377	192.168.188.1	192.168.188.1	TCP	44	55162 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=2619648 Len=0
2334	2023-11-01 21:38:19.180435	192.168.188.1	192.168.188.1	TCP	44	8080 → 55162 [ACK] Seq=1 Ack=2 Win=2619648 Len=0
2335	2023-11-01 21:38:19.180512	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [FIN, ACK] Seq=1029 Ack=5080 Win=2614528 Len=0
2336	2023-11-01 21:38:19.180536	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [ACK] Seq=5080 Ack=1030 Win=2619136 Len=0
2341	2023-11-01 21:38:19.181168	192.168.188.1	192.168.188.1	TCP	44	8080 → 55162 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
2342	2023-11-01 21:38:19.181196	192.168.188.1	192.168.188.1	TCP	44	8080 → 55161 [FIN, ACK] Seq=5080 Ack=1030 Win=2619136 Len=0
2343	2023-11-01 21:38:19.181209	192.168.188.1	192.168.188.1	TCP	44	55161 → 8080 [ACK] Seq=1030 Ack=5081 Win=2614528 Len=0

[Stream index: 2]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 1030 (relative sequence number)  
Sequence Number (raw): 903276745  
[Next Sequence Number: 1030 (relative sequence number)]  
Acknowledgment Number: 5081 (relative ack number)  
Acknowledgment number (raw): 1824541372  
0101 ... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window: 10213  
[Calculated window size: 2614528]  
[Window size scaling factor: 256]  
Checksum: 0xc174 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[seq/ack analysis]

0000 02 00 00 00 45 00 00 28 5c 38 40 00 80 06 00 00 .....E..(\8@.....  
0010 c0 a8 bc 01 c0 a8 bc 01 d7 79 1f 90 35 d6 e8 c9 .....y..5...  
0020 6c c0 4a bc 50 10 27 e5 c1 74 00 00 .....l.J...t..

Flags (12 bits) (tcp.flags), 2 byte(s) 分组: 15330 · 已显示: 25 (0.2%) · 已丢弃: 0 (0.0%) 配置: Default

#### 4. “三次握手”和“四次挥手”总结

由于TCP是全双工的，为了确保建立连接和断开连接成功，分别需要“三次握手”和“四次挥手”使得客户端和服务端都能够得知对方已与自己建立或断开连接。

#### 5. 获取html文本

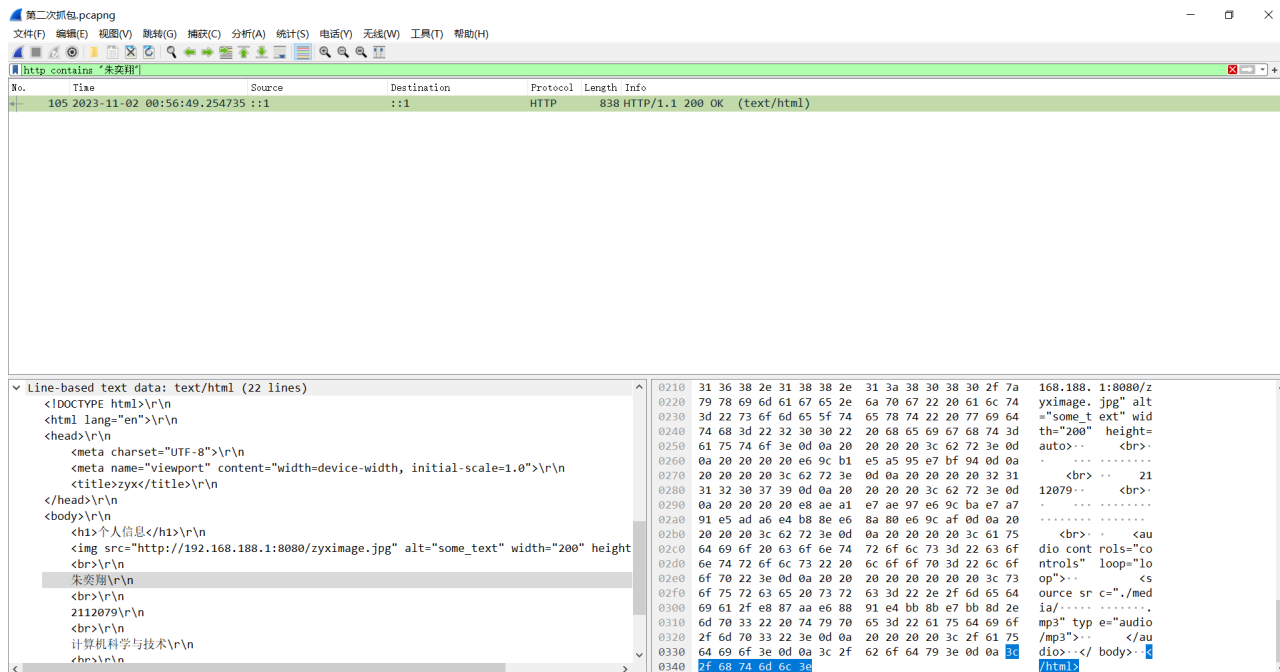
通过加入过滤条件http contains "朱奕翔"可以快速定位到成功从服务器发送到客户端的html数据包，将过滤条件改为http就能看到客户端向服务器发送的请求，如图所示是客户端先向客户端发送的请求，之后客户端返回文本形式html内容，200 OK表示成功返回。

103	2023-11-02 00:56:49.254352	:::1	HTTP	770	GET /zyx.html HTTP/1.1
105	2023-11-02 00:56:49.254735	:::1	HTTP	838	HTTP/1.1 200 OK (text/html)

这张图的左下角可以看到数据可以看到返回的text正是编写的html文件中的内容，进一步验证了返回成



功。

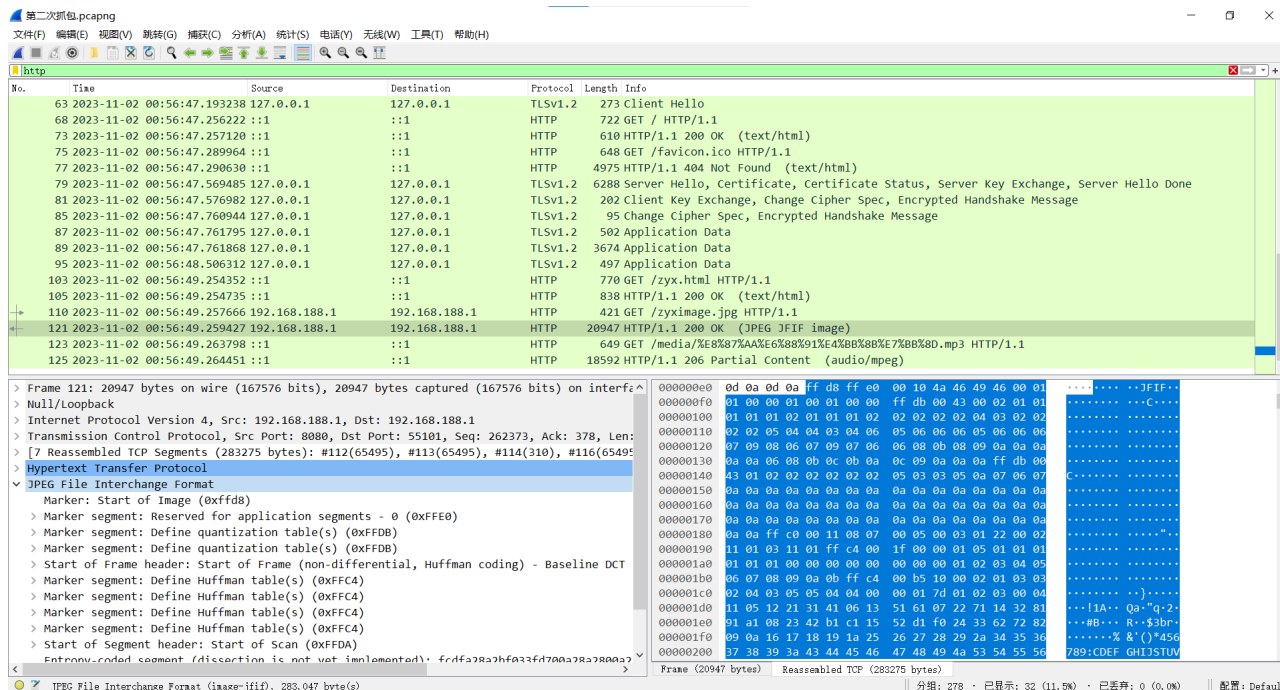


## 6. 获取图片

同理，客户端也请求了图片，也成功得到了回应

No.	Time	Source	Destination	Protocol	Length	Info
110	2023-11-02 00:56:49.257666	192.168.188.1	192.168.188.1	HTTP	421	GET /zyximage.jpg HTTP/1.1
121	2023-11-02 00:56:49.259427	192.168.188.1	192.168.188.1	HTTP	20947	HTTP/1.1 200 OK (JPEG JFIF image)

能够清楚地看到图片的十六进制数据。

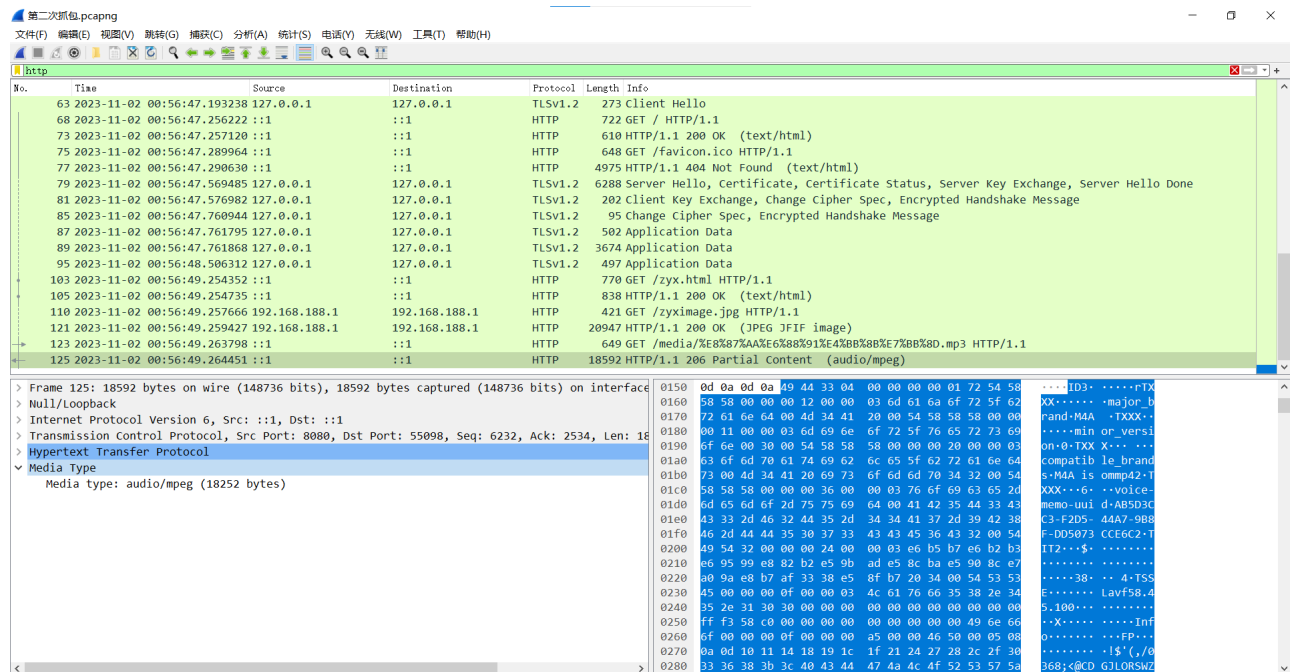


## 7. 获取流媒体

随着获取得到文本和图片之后，紧接着就请求了其中的流媒体文件，在这个网页中是音频，可以看到206 partial content代表的是部分资源请求成功，常用于流媒体，在这里说明流媒体返回成功。

No.	Time	Source	Destination	Protocol	Length	Info
103	2023-11-02 00:56:49.254352	:::1	:::1	HTTP	770	GET /zyx.html HTTP/1.1
105	2023-11-02 00:56:49.254735	:::1	:::1	HTTP	838	HTTP/1.1 200 OK (text/html)
110	2023-11-02 00:56:49.257666	192.168.188.1	192.168.188.1	HTTP	421	GET /zyximage.jpg HTTP/1.1
121	2023-11-02 00:56:49.259427	192.168.188.1	192.168.188.1	HTTP	20947	HTTP/1.1 200 OK (JPEG JFIF image)
123	2023-11-02 00:56:49.263798	:::1	:::1	HTTP	649	GET /media/%E8%87%AA%E6%80%91%E4%B8%8E%7%B8%8D.mp3 HTTP/1.1
125	2023-11-02 00:56:49.264451	:::1	:::1	HTTP	18592	HTTP/1.1 206 Partial Content (audio/mpeg)

## 返回的十六进制内容如下所示



## 总结

1. 搭建服务器和制作简单的文件在搜索相关资料学习后比较简单，但是也只是浅尝辄止，html可以制作出精美的网页。
2. wireshark抓包初次使用有些困难，但通过不断摸索，熟悉里面的各种功能，尤其是过滤条件的语法可以快速找到想要获取的捕获的内容。
3. 在使用时遇到了搜索不到html文本内容的包的情况，只能找到http 304 not modified这种响应，最终得知是为了提高性能和减少带宽消耗采用的缓存的机制，当服务器内容未发生变化时不需要重新发送资源内容。所以清空缓存重新抓包就得到了http 200 OK的响应，也能通过http contains "朱奕翔"这个过滤条件直接找到返回的报文。