

廈門大學



信息学院软件工程系

《计算机网络》实验报告

题 目 实验三 基于 PCAP 库侦听并分析网络流量

班 级 数字媒体技术 2020 级

姓 名 庞天骏

学 号 22920202202910

实验时间 2022 年 11 月 14 日

1 实验目的

通过完成实验，理解数据链路层、网络层、传输层和应用层的基本原理。掌握用 Wireshark 观察网络流量并辅助网络侦听相关的编程；掌握用 Libpcap 或 WinPcap 库侦听并处理以太网帧和 IP 报文的方法；熟悉以太网帧、IP 报文、TCP 段和 FTP 命令的格式概念，掌握 TCP 协议的基本机制；熟悉帧头部或 IP 报文头部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念，熟悉段头部各字段和 FTP 控制命令的指令和数据的含义。

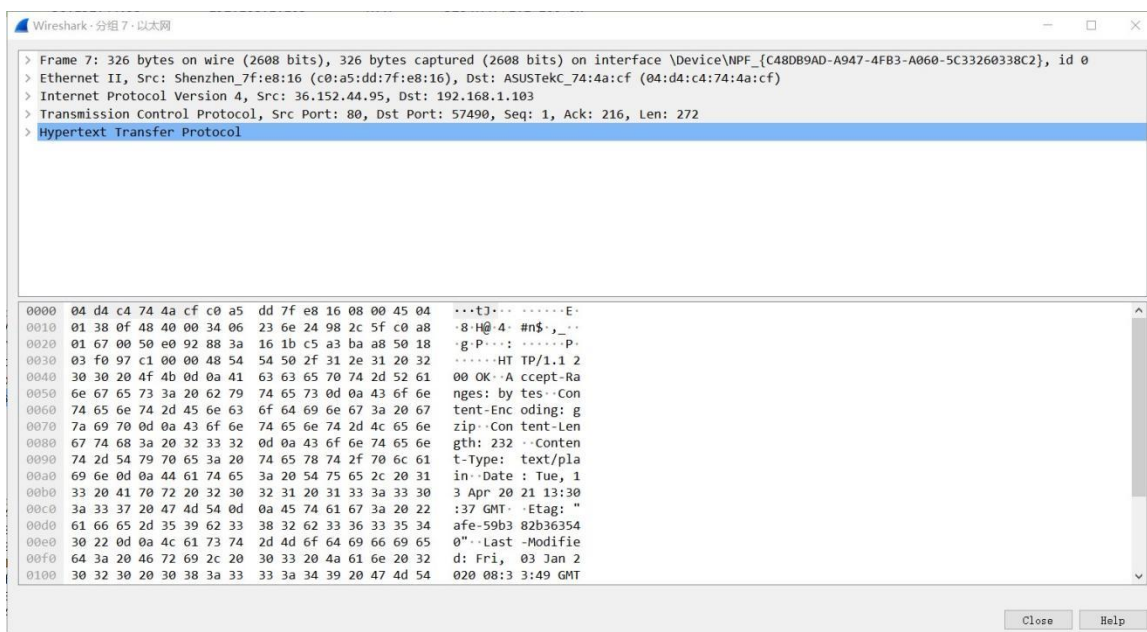
2 实验环境

操作系统：Windows10

3 实验结果

1. 用侦听解析软件观察数据格式

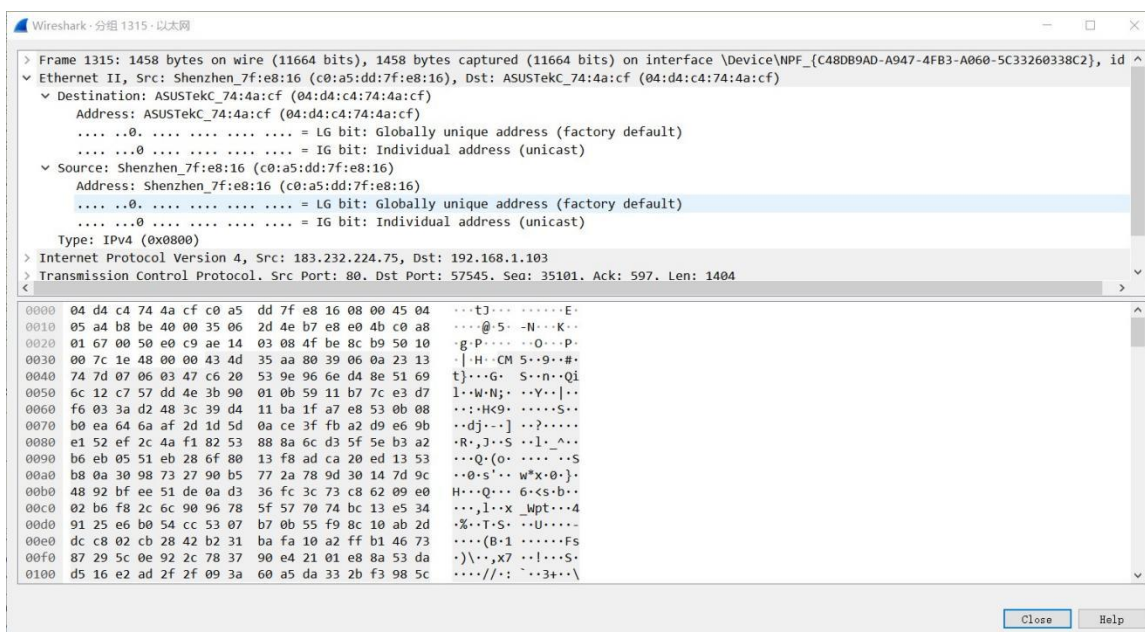
(1) 网络协议层次嵌套



- Frame: 物理层的数据帧概况。

- Ethernet II: 数据链路层以太网头部帧。
- Internet Protocol Version 4: 互联网层 IP 报头的信息。
- Transmission Control Protocol: 传输层的数据段头部信息, 此处是 TCP 协议。
- Hypertext Transfer Protocol: 应用层的信息, 此处是 HTTP 协议。

(2) 以太网帧格式

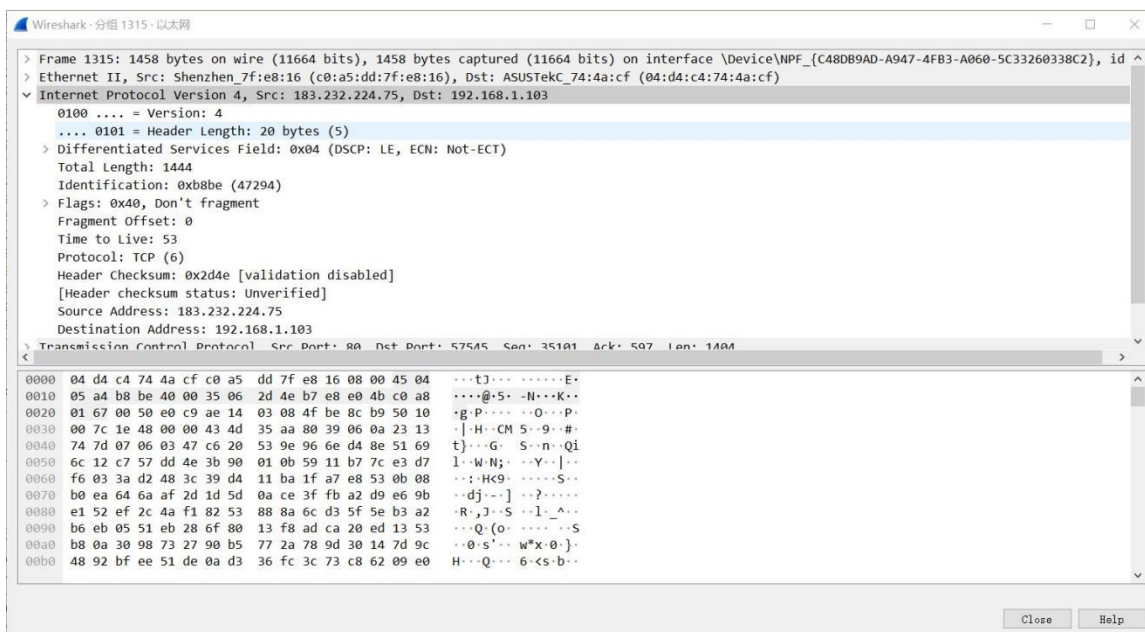


Destination Address: 目的地址

Source Address: 源地址

Type: 类型

(3) IP 报文格式



Version: 版本

Header Length: 首部长度

Differentiated Services Field: 区分服务

Total Length: 总长度

Identification: 标识

Flags: 标志

Fragment Offset: 片位移

Time to Live: 生存时间

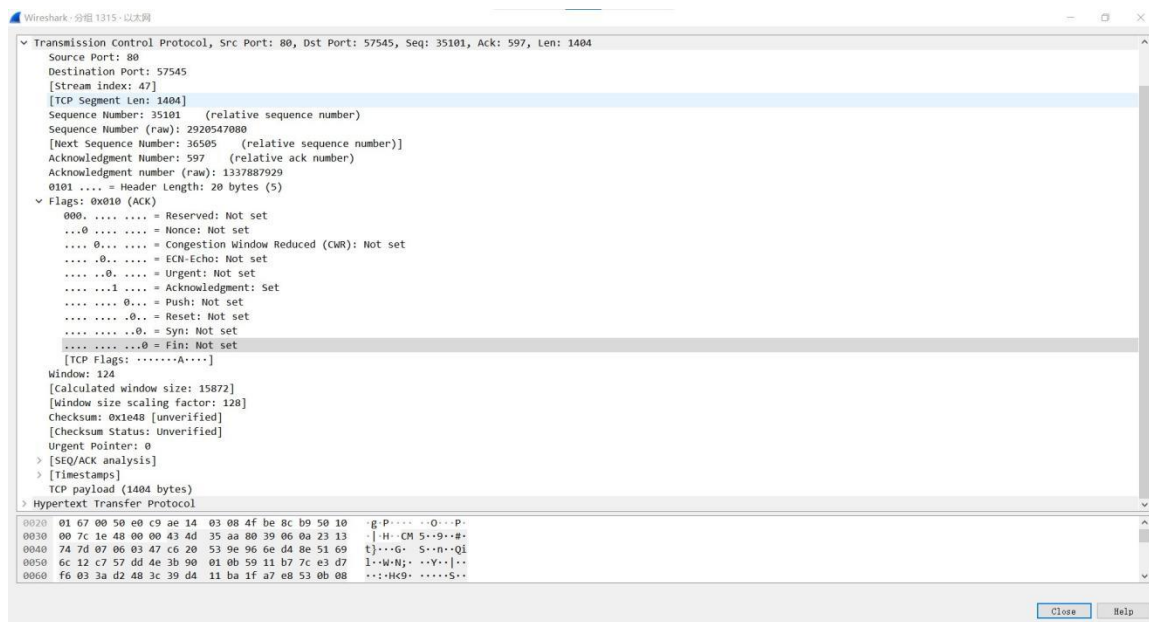
Protocol: 协议

Header Checksum: 首部校验和

Source Address: 源地址

Destination Address: 目的地址

(4) TCP 段格式



Source Port: 源端口

Destination Port: 目的端口

Sequence Number: 序号

Acknowledgment Number: 确认号

Header Length: 首部长度

Reserved: 保留

Urgent: URG 紧急控制位

Acknowledgment: ACK 确认控制位

Push: PSH 推送控制位

Reset: RST 复位控制位

Syn: SYN 同步控制位

Fin: FIN 终止控制位

Window: 窗口

Checksum: 校验和

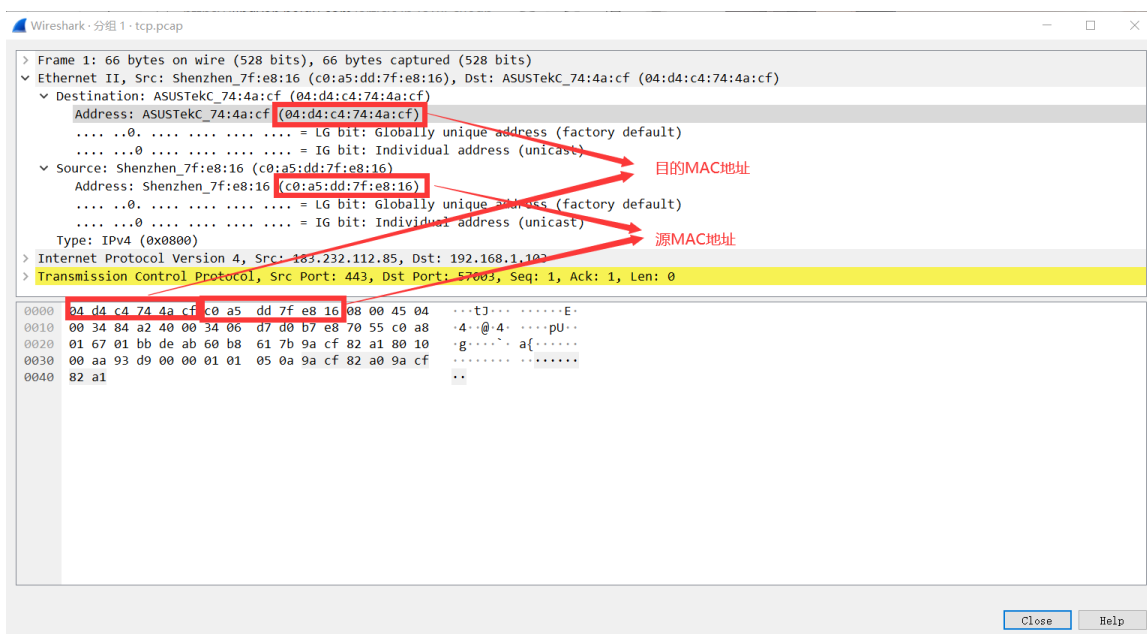
Urgent Pointer: 紧急指针

Timestamps: 时间戳选项

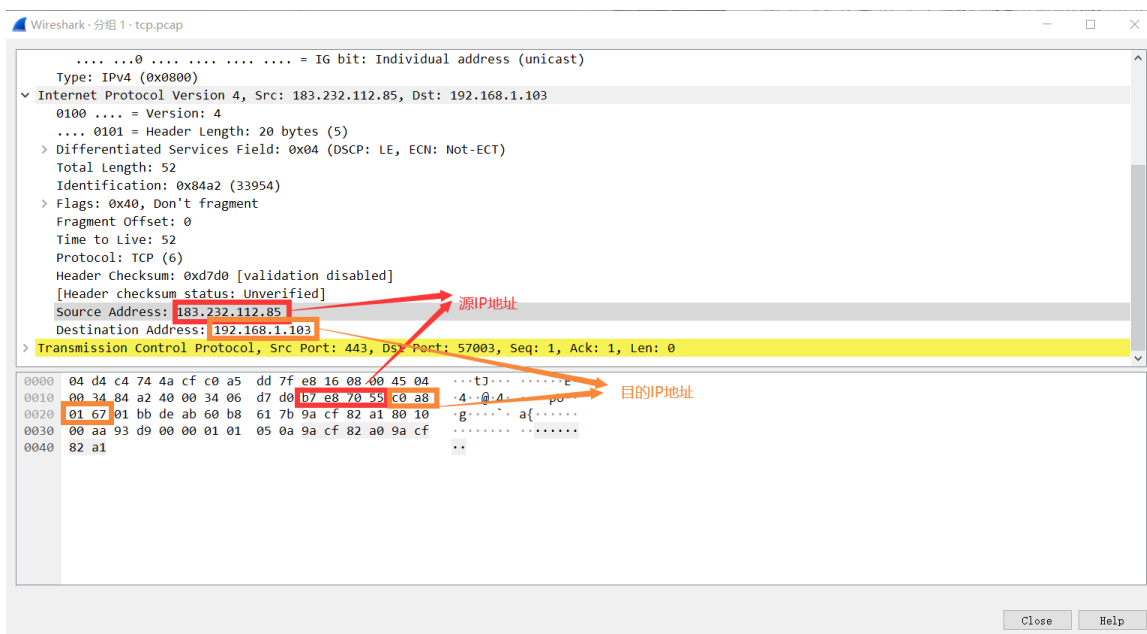
TCP payload: TCP 有效载荷

(5) FTP 协议命令和相应的格式

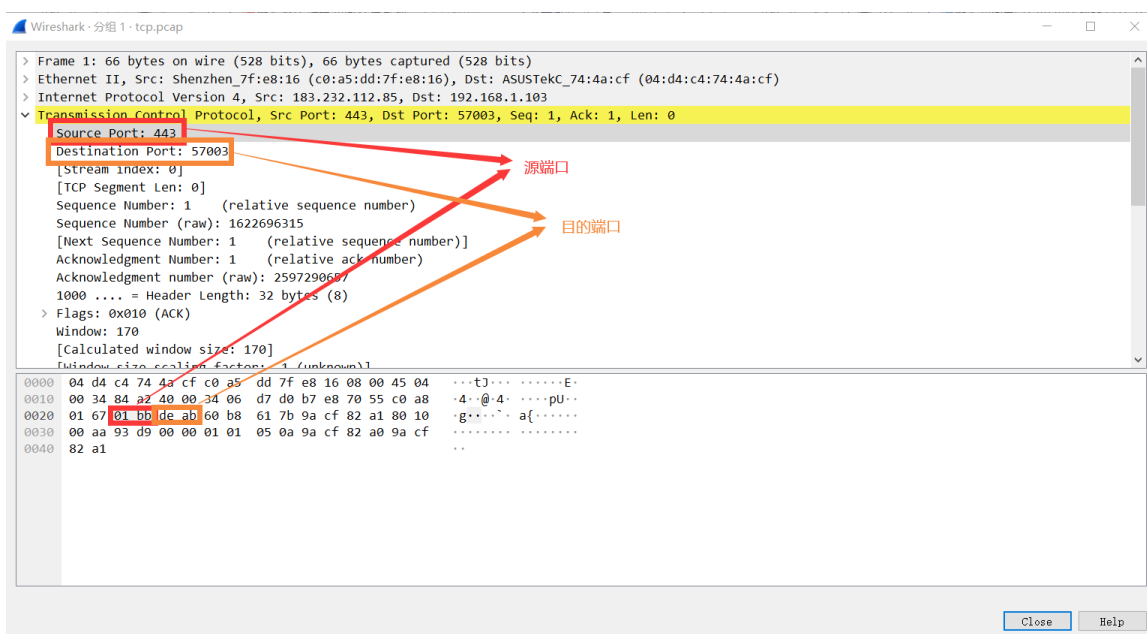
(6) MAC 地址



(7) IP 地址



(8) TCP 端口



2. 用侦听解析软件观察 TCP 机制

(1) TCP 建立的三次握手连接

1.140825	192.168.1.103	36.158.197.35	TCP	66 53310 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1.166476	36.158.197.35	192.168.1.103	TCP	66 443 → 53310 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 WS=128
1.166522	192.168.1.103	36.158.197.35	TCP	54 53310 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0

(i) 第一个握手数据包：客户端发送一个 TCP，标志位为 SYN，序列号为 0，代表客户端请求建立连接。

```
> Frame 188: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF{...}
> Ethernet II, Src: ASUSTekC_74:4a:cf (04:d4:c4:74:4a:cf), Dst: Shenzhen_7f:e8:16 (c0:a5:d0:7f:e8:16)
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 36.158.197.35
v Transmission Control Protocol, Src Port: 53310, Dst Port: 443, Seq: 0, Len: 0
  Source Port: 53310
  Destination Port: 443
  [Stream index: 5]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2981193389
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
v Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): 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
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....S.]
  ...
```

(ii) 第二个握手数据包：服务器接收到客户端的 SYN 报文，回复 SYN+ACK 报文。报文标志 SYN，ACK，ACK number=接收到的 Seq+1=1，自己的 Seq=0。


```

> Frame 195: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device^
> Ethernet II, Src: Shenzhen_7f:e8:16 (c0:a5:dd:7f:e8:16), Dst: ASUSTekC_74:4a:cf (04:d4:c
> Internet Protocol Version 4, Src: 36.158.197.35, Dst: 192.168.1.103
v Transmission Control Protocol, Src Port: 443, Dst Port: 53310, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 53310
  [Stream index: 5]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2385539129
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2981193390
  1000 .... = Header Length: 32 bytes (8)
v 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
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....A..S.]

```

(iii) 第三个握手数据包：客户端接收到服务端的 SYN+ACK 报文后，回复 ACK 报文。报文标志 ACK，Seq=1，ACK=接收到的 Seq+1=1。

```

> Frame 196: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device^
> Ethernet II, Src: ASUSTekC_74:4a:cf (04:d4:c4:74:4a:cf), Dst: Shenzhen_7f:e8:16 (c0:a5:d
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 36.158.197.35
v Transmission Control Protocol, Src Port: 53310, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 53310
    Destination Port: 443
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 2981193390
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 2385539130
    0101 .... = Header Length: 20 bytes (5)
v 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
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A....]
    Window: 543

```

(2) TCP 撤除连接的四次挥手操作

1.960788	192.168.1.103	36.158.197.35	TCP	54 53310 → 443 [FIN, ACK] Seq=1940 Ack=27393 Win=131072 Len=0
1.985899	36.158.197.35	192.168.1.103	TCP	60 443 → 53310 [ACK] Seq=27393 Ack=1941 Win=74112 Len=0
1.986622	36.158.197.35	192.168.1.103	TCP	60 443 → 53310 [FIN, ACK] Seq=27393 Ack=1941 Win=74112 Len=0
1.986650	192.168.1.103	36.158.197.35	TCP	54 53310 → 443 [ACK] Seq=1941 Ack=27394 Win=131072 Len=0

(i) 第一次挥手：FIN+ACK。客户端发送一个 FIN，用来关闭客户到服务器的数据传送。

```

> Frame 440: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device^
> Ethernet II, Src: ASUSTekC_74:4a:cf (04:d4:c4:74:4a:cf), Dst: Shenzhen_7f:e8:16 (c0:a5:d
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 36.158.197.35
v Transmission Control Protocol, Src Port: 53310, Dst Port: 443, Seq: 1940, Ack: 27393, Le
    Source Port: 53310
    Destination Port: 443
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence Number: 1940 (relative sequence number)
    Sequence Number (raw): 2981195329
    [Next Sequence Number: 1941 (relative sequence number)]
    Acknowledgment Number: 27393 (relative ack number)
    Acknowledgment number (raw): 2385566522
    0101 .... = Header length: 20 bytes (5)
v Flags: 0x011 (FIN, 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
    .... .... ..0. = Syn: Not set
    .... .... ...1 = Fin: Set
    [TCP Flags: .....A...F]
    Window: 512

```

(ii) 第二次挥手：ACK。服务器收到这个 FIN，它发回一个 ACK，确认序号为收到的序号加 1。

```
> Frame 461: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device^
> Ethernet II, Src: Shenzhen_7f:e8:16 (c0:a5:dd:7f:e8:16), Dst: ASUSTekC_74:4a:cf (04:d4:c
> Internet Protocol Version 4, Src: 36.158.197.35, Dst: 192.168.1.103
v Transmission Control Protocol, Src Port: 443, Dst Port: 53310, Seq: 27393, Ack: 1941, Le
  Source Port: 443
  Destination Port: 53310
  [Stream index: 5]
  [TCP Segment Len: 0]
  Sequence Number: 27393 (relative sequence number)
  Sequence Number (raw): 2385566522
  [Next Sequence Number: 27393 (relative sequence number)]
  Acknowledgment Number: 1941 (relative ack number)
  Acknowledgment number (raw): 2981195330
  0101 .... = Header Length: 20 bytes (5)
v 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
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = FIN: Not set
  [TCP Flags: .....A....]
  Window: 570
```

(iii) 第三次挥手：FIN+ACK。服务器关闭与客户端的连接，发送一个 FIN 给客户端。

```

> Frame 463: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device^
> Ethernet II, Src: Shenzhen_7f:e8:16 (c0:a5:dd:7f:e8:16), Dst: ASUSTekC_74:4a:cf (04:d4:c
> Internet Protocol Version 4, Src: 36.158.197.35, Dst: 192.168.1.103
v Transmission Control Protocol, Src Port: 443, Dst Port: 53310, Seq: 27393, Ack: 1941, Le
    Source Port: 443
    Destination Port: 53310
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence Number: 27393 (relative sequence number)
    Sequence Number (raw): 2385566522
    [Next Sequence Number: 27394 (relative sequence number)]
    Acknowledgment Number: 1941 (relative ack number)
    Acknowledgment number (raw): 2981195330
    0101 .... = Header Length: 20 bytes (5)
v Flags: 0x011 (FIN, 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
    .... .... ..0. = Syn: Not set
    > .... .... ...1 = Fin: Set
    [TCP Flags: .....A...F]
    Window: 570

```

(iv) 第四次挥手：ACK。客户端发回 ACK 报文确认，并将确认序号设置为收到序号加 1。

```
> Frame 464: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device^
> Ethernet II, Src: ASUSTekC_74:4a:cf (04:d4:c4:74:4a:cf), Dst: Shenzhen_7f:e8:16 (c0:a5:d
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 36.158.197.35
v Transmission Control Protocol, Src Port: 53310, Dst Port: 443, Seq: 1941, Ack: 27394, Le
    Source Port: 53310
    Destination Port: 443
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence Number: 1941 (relative sequence number)
    Sequence Number (raw): 2981195330
    [Next Sequence Number: 1941 (relative sequence number)]
    Acknowledgment Number: 27394 (relative ack number)
    Acknowledgment number (raw): 2385566523
    0101 .... = Header Length: 20 bytes (5)
v 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
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A....]
    Window: 512
```

(3) 用 Libpcap 或 WinPcap 库侦听网络数据

	A	B	C	D	E	F	G
1	Time	Source MAC	Source IP	Dst MAC	Dst IP	Length	
2	2021/5/14 8:13:14	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	80	
3	2021/5/14 8:13:14	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	80	
4	2021/5/14 8:13:14	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	228	
5	2021/5/14 8:13:14	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	244	
6	2021/5/14 8:13:14	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	80	
7	2021/5/14 8:13:14	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	228	
8	2021/5/14 8:13:16	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	94	
9	2021/5/14 8:13:16	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	173	
10	2021/5/14 8:13:16	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	94	
11	2021/5/14 8:13:16	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	173	
12	2021/5/14 8:13:17	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	103	
13	2021/5/14 8:13:17	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	272	
14	2021/5/14 8:13:17	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	103	
15	2021/5/14 8:13:17	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	272	
16	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	66	
17	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	66	
18	2021/5/14 8:13:18	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	82	
19	2021/5/14 8:13:18	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	66	
20	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	117	
21	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	117	
22	2021/5/14 8:13:18	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	176	
23	2021/5/14 8:13:19	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	160	
24	2021/5/14 8:13:19	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	117	
25	2021/5/14 8:13:19	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	160	
26	2021/5/14 8:13:20	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	95	
27	2021/5/14 8:13:20	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	95	
28	2021/5/14 8:13:20	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	197	
29	2021/5/14 8:13:20	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	213	
30	2021/5/14 8:13:20	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	95	

```

D:\Program Files (x86)\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
1. \Device\NPF_{03ACEB66-0DD6-4B07-8225-4B6E32B5482A} (Microsoft)
2. \Device\NPF_{6EF0A426-0AAF-4F7B-986F-F2E7E3AB6C9A} (Microsoft)
3. \Device\NPF_{43A5353B-483C-498E-B12B-4EF2C8135683} (Microsoft)
4. \Device\NPF_{C48DB9AD-A947-4FB3-A060-5C33260338C2} (Realtek PCIe GbE Family Controller)
Enter the interface number (1-4):2

listening on Microsoft...
-----60s after-----
Length of message sent from MAC(3C-F0-11-52-63-04) and IP(10.30.46.75) is total 12351.
Length of message sent from MAC(C4-CA-D9-3C-D7-5C) and IP(210.34.0.18) is total 22643.
Length of message sent to MAC(C4-CA-D9-3C-D7-5C) and IP(10.30.46.75) is total 11706.
Length of message sent to MAC(3C-F0-11-52-63-04) and IP(210.34.0.18) is total 22643.
Length of message sent to MAC(01-00-5E-7F-FF-FA) and IP(10.30.46.75) is total 645.
-----60s after-----
Length of message sent from MAC(3C-F0-11-52-63-04) and IP(10.30.46.75) is total 7820.
Length of message sent to MAC(C4-CA-D9-3C-D7-5C) and IP(10.30.46.75) is total 7820.
-----60s after-----
Length of message sent from MAC(3C-F0-11-52-63-04) and IP(10.30.46.75) is total 878.
Length of message sent to MAC(C4-CA-D9-3C-D7-5C) and IP(10.30.46.75) is total 635.
Length of message sent to MAC(FF-FF-FF-FF-FF-FF) and IP(10.30.46.75) is total 243.
-----60s after-----
Length of message sent from MAC(C4-CA-D9-3C-D7-5C) and IP(120.232.18.31) is total 5724.
Length of message sent from MAC(3C-F0-11-52-63-04) and IP(10.30.46.75) is total 2555.
Length of message sent to MAC(3C-F0-11-52-63-04) and IP(120.232.18.31) is total 5724.
Length of message sent to MAC(C4-CA-D9-3C-D7-5C) and IP(10.30.46.75) is total 2555.

```

(4) 解析侦听到的网络数据

	A	B	C	D	E	F	G	H	I	J	K
2021/5/22 17:46:58	E8-6F-38-3E-88-D1	192.168.1.109	3C-F0-11-52-63-04	192.168.1.102	anonymous	1137004652@qq.com	FAILED				
2021/5/22 17:47:01	E8-6F-38-3E-88-D1	192.168.1.109	3C-F0-11-52-63-04	192.168.1.102	user	123456	SUCCEED				

4 实验代码

本次实验的代码已上传于以下代码仓库：

<https://github.com/0maple-syrup0/EX3.git>

5 实验总结

通过此次实验，理解了数据链路层、网络层、传输层和应用层的基本原理。掌握了用 Wireshark 观察网络流量并辅助网络侦听相关的编程；熟悉了以太网帧、IP 报文、TCP 段和 FTP 命令的格式概念，掌握了 TCP 协议的基本机制；熟悉了帧头部或 IP 报文头部各字段的含义。熟悉了 TCP 段和 FTP 数据协议的概念，熟悉了段头部各字段和 FTP 控制命令的指令和数据的含义。