

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 软件工程 2019 级 1 班

姓 名 雷鸿宇

学 号 22920192204173

实验时间 2021 年 3 月 28 日

2021 年 3 月 28 日

填写说明

- 1、本文件为 Word 模板文件，建议使用 Microsoft Word 2019 打开，在可填写的区域中如实填写；
- 2、填表时，勿破坏排版，勿修改字体字号，打印成 PDF 文件提交；
- 3、文件总大小尽量控制在 1MB 以下，勿超过 5MB；
- 4、应将材料清单上传在代码托管平台上；
- 5、在学期最后一节课前按要求打包发送至 cni21@qq.com。

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。

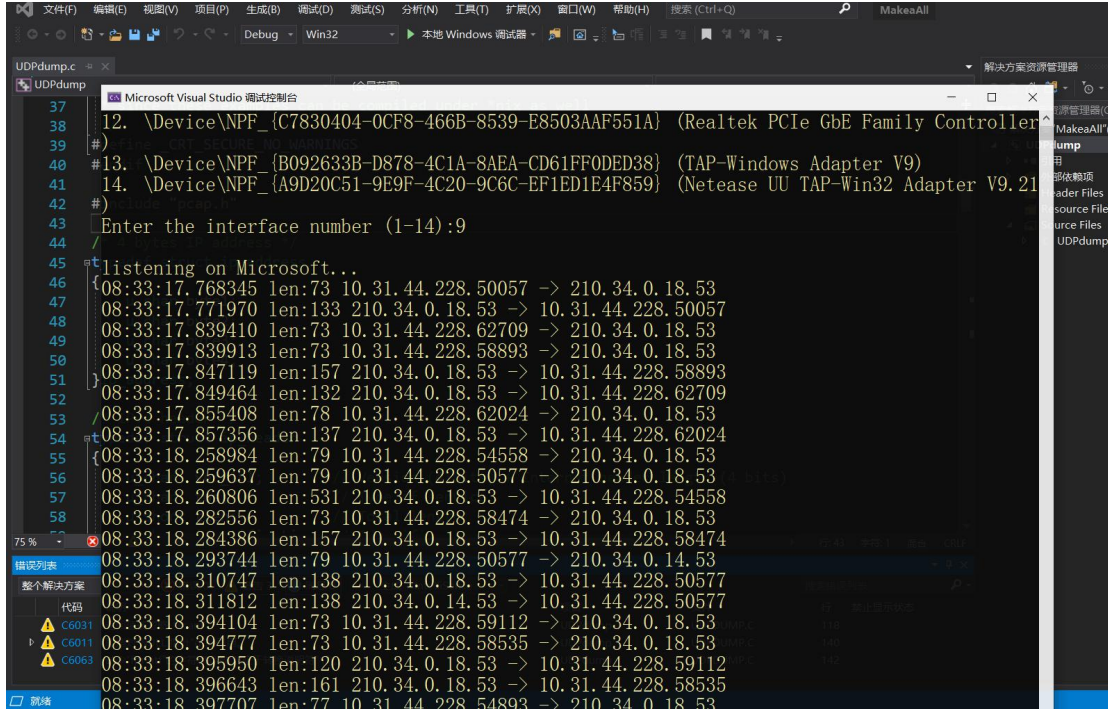
2 实验环境

Windows 10、Winpcap、Wireshark

编程语言：c

3 实验结果

下载并配置好 winpcap，运行源代码

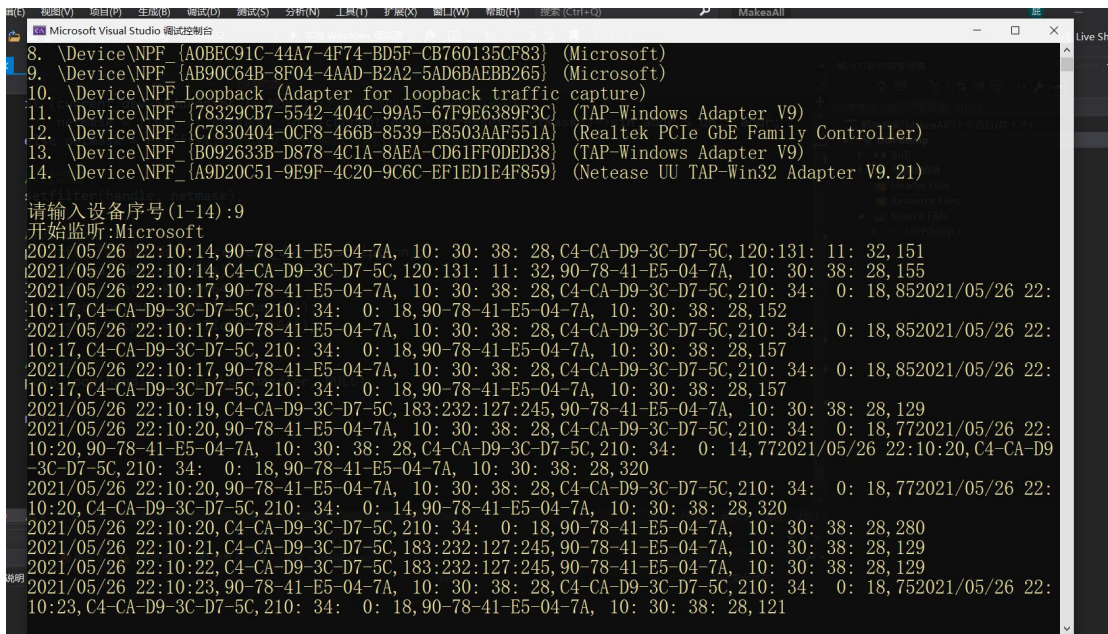


```

UDPdump.c
37
38 12. \Device\NPF_{C7830404-0CF8-466B-8539-E8503AAF551A} (Realtek PCIe GbE Family Controller)
39 #)
40 #13. \Device\NPF_{B092633B-D878-4C1A-8AEA-CD61FF0DED38} (TAP-Windows Adapter V9)
41 #14. \Device\NPF_{A9D20C51-9E9F-4C20-9C6C-EF1ED1E4F859} (Netease UU TAP-Win32 Adapter V9.21)
42 #)
43 Enter the interface number (1-14):9
44 /
45 listening on Microsoft...
46 {08:33:17.768345 len:73 10.31.44.228.50057 -> 210.34.0.18.53
47 08:33:17.771970 len:133 210.34.0.18.53 -> 10.31.44.228.50057
48 08:33:17.839410 len:73 10.31.44.228.62709 -> 210.34.0.18.53
49 08:33:17.839913 len:73 10.31.44.228.58893 -> 210.34.0.18.53
50 08:33:17.847119 len:157 210.34.0.18.53 -> 10.31.44.228.58893
51 08:33:17.849464 len:132 210.34.0.18.53 -> 10.31.44.228.62709
52 08:33:17.855408 len:78 10.31.44.228.62024 -> 210.34.0.18.53
53 08:33:17.857356 len:137 210.34.0.18.53 -> 10.31.44.228.62024
54 08:33:18.258984 len:79 10.31.44.228.54558 -> 210.34.0.18.53
55 08:33:18.259637 len:79 10.31.44.228.50577 -> 210.34.0.18.53
56 08:33:18.260806 len:531 210.34.0.18.53 -> 10.31.44.228.54558
57 08:33:18.282556 len:73 10.31.44.228.58474 -> 210.34.0.18.53
58 08:33:18.284386 len:157 210.34.0.18.53 -> 10.31.44.228.58474
08:33:18.293744 len:79 10.31.44.228.50577 -> 210.34.0.14.53
08:33:18.310747 len:138 210.34.0.18.53 -> 10.31.44.228.50577
08:33:18.311812 len:138 210.34.0.14.53 -> 10.31.44.228.50577
08:33:18.394104 len:73 10.31.44.228.59112 -> 210.34.0.18.53
08:33:18.394777 len:73 10.31.44.228.58535 -> 210.34.0.18.53
08:33:18.395950 len:120 210.34.0.18.53 -> 10.31.44.228.59112
08:33:18.396643 len:161 210.34.0.18.53 -> 10.31.44.228.58535
08:33:18.397707 len:77 10.31.44.228.54893 -> 210.34.0.18.53

```

修改代码，让其额外显示源 MAC、目的 MAC 以及帧长度等信息



```

8. \Device\NPF_{A0BEC91C-44A7-4F74-BD5F-CB760135CF83} (Microsoft)
9. \Device\NPF_{AB90C64B-8F04-4AAD-B2A2-5AD6BAEBB265} (Microsoft)
10. \Device\NPF_{Loopback (Adapter for loopback traffic capture)}
11. \Device\NPF_{78329CB7-5542-404C-99A5-67F9E6389F3C} (TAP-Windows Adapter V9)
12. \Device\NPF_{C7830404-0CF8-466B-8539-E8503AAF551A} (Realtek PCIe GbE Family Controller)
13. \Device\NPF_{B092633B-D878-4C1A-8AEA-CD61FF0DED38} (TAP-Windows Adapter V9)
14. \Device\NPF_{A9D20C51-9E9F-4C20-9C6C-EF1ED1E4F859} (Netease UU TAP-Win32 Adapter V9.21)

请输入设备序号 (1-14):9
开始监听:Microsoft
2021/05/26 22:10:14, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 120:131: 11: 32, 151
2021/05/26 22:10:14, C4-CA-D9-3C-D7-5C, 120:131: 11: 32, 90-78-41-E5-04-7A, 10: 30: 38: 28, 155
2021/05/26 22:10:17, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 852021/05/26 22:
10:17, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 90-78-41-E5-04-7A, 10: 30: 38: 28, 152
2021/05/26 22:10:17, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 852021/05/26 22:
10:17, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 90-78-41-E5-04-7A, 10: 30: 38: 28, 157
2021/05/26 22:10:17, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 852021/05/26 22:
10:17, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 90-78-41-E5-04-7A, 10: 30: 38: 28, 157
2021/05/26 22:10:19, C4-CA-D9-3C-D7-5C, 183:232:127:245, 90-78-41-E5-04-7A, 10: 30: 38: 28, 129
2021/05/26 22:10:20, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 772021/05/26 22:
10:20, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 210: 34: 0: 14, 772021/05/26 22:10:20, C4-CA-D9-
3C-D7-5C, 210: 34: 0: 18, 90-78-41-E5-04-7A, 10: 30: 38: 28, 320
2021/05/26 22:10:20, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 772021/05/26 22:
10:20, C4-CA-D9-3C-D7-5C, 210: 34: 0: 14, 90-78-41-E5-04-7A, 10: 30: 38: 28, 320
2021/05/26 22:10:20, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 90-78-41-E5-04-7A, 10: 30: 38: 28, 280
2021/05/26 22:10:21, C4-CA-D9-3C-D7-5C, 183:232:127:245, 90-78-41-E5-04-7A, 10: 30: 38: 28, 129
2021/05/26 22:10:22, C4-CA-D9-3C-D7-5C, 183:232:127:245, 90-78-41-E5-04-7A, 10: 30: 38: 28, 129
2021/05/26 22:10:23, 90-78-41-E5-04-7A, 10: 30: 38: 28, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 752021/05/26 22:
10:23, C4-CA-D9-3C-D7-5C, 210: 34: 0: 18, 90-78-41-E5-04-7A, 10: 30: 38: 28, 121

```

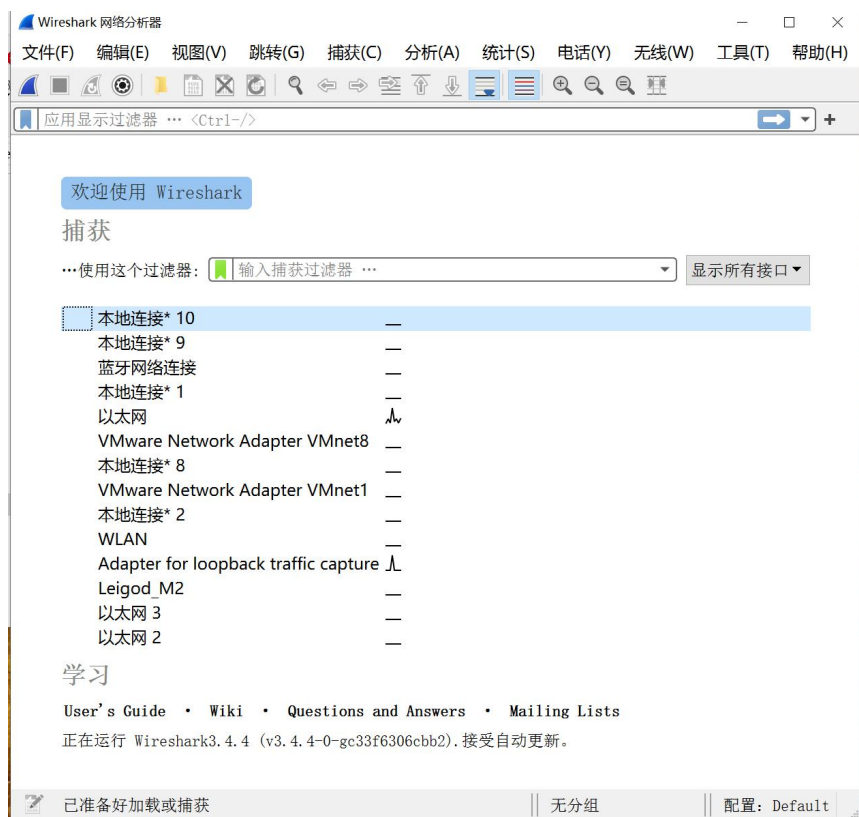
使用 wireshark 前，先 ipconfig 本机的网络信息

无线局域网适配器 WLAN:

```

连接特定的 DNS 后缀 . . . . . : xmu.edu.cn
描述. . . . . : Intel(R) Wireless-AC 9560 160MHz
物理地址. . . . . : 90-78-41-E5-04-7A
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
IPv6 地址 . . . . . : 2001:da8:e800:71e2:74a0:c4b8:8ff9:517c(首选)
临时 IPv6 地址. . . . . : 2001:da8:e800:71e2:c15d:7a32:2776:feel(首选)
本地链接 IPv6 地址. . . . . : fe80::74a0:c4b8:8ff9:517c%17(首选)
IPv4 地址 . . . . . : 10.31.44.228(首选)
子网掩码 . . . . . : 255.255.224.0
获得租约的时间 . . . . . : 2021年4月30日 7:55:17
租约过期的时间 . . . . . : 2021年4月30日 9:26:28
默认网关. . . . . : fe80::c6ca:d9ff:fe3c:d759%17
                      10.31.32.1
DHCP 服务器 . . . . . : 172.18.0.12
DHCPv6 IAID . . . . . : 143685697
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-24-C6-CB-72-98-FA-9B-61-CC-92
DNS 服务器 . . . . . : 210.34.0.18
                      210.34.0.14
TCP/IP 上的 NetBIOS . . . . . : 已启用
  
```

安装 wireshark，观察相关界面



观察到一个 TCP 连接的三次握手

1 0.000000	10.31.44.228	140.206.78.149	TCP	66 50538 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2 0.029976	140.206.78.149	10.31.44.228	TCP	62 80 → 50538 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1386 WS=128
3 0.030363	10.31.44.228	140.206.78.149	TCP	54 50538 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0

点击查看每一项的详细信息

第一次握手

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{AB90C648-8F04-4A4D-B2A2-5AD6BAEBB265}, id 0
> Ethernet II, Src: IntelCor_e5:04:7a (90:78:41:e5:04:7a), Dst: Hangzhou_3c:d7:59 (c4:ca:d9:3c:d7:59)
> Internet Protocol Version 4, Src: 10.31.44.228, Dst: 140.206.78.149
√ Transmission Control Protocol, Src Port: 50538, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 50538
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3418427460
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment Number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0xbff8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    > [Timestamps]
```

第二次握手

```
√ Transmission Control Protocol, Src Port: 80, Dst Port: 50538, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 50538
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2120237745
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3418427461
  0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0 .... = Congestion Window Reduced (CWR): Not set
    ....0 .... = ECH-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
```

第三次握手（flags 下可以看到个标记的值）

```
√ Transmission Control Protocol, Src Port: 50538, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 50538
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3418427461
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2120237746
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0 .... = Congestion Window Reduced (CWR): Not set
    ....0 .... = ECH-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
```

观察一个 ip 报文（可以看到版本、头长度、是否分片、源地址、目的地址等信息）


```

    Padding: 000000000000
  v Internet Protocol Version 4, Src: 140.206.78.149, Dst: 10.31.44.228
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x74 (DSCP: Unknown, ECN: Not-ECT)
    0111 01.. = Differentiated Services Codepoint: Unknown (29)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 40
    Identification: 0x87ad (34733)
  v Flags: 0x40, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 48
    Protocol: TCP (6)
    Header Checksum: 0xb048 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.206.78.149
    Destination Address: 10.31.44.228

```

帧分析器（60 字节）

```

  v Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{AB90C648-8F04-4A4D-B2A2-SAD6BAEBB265}, id 0
    v Interface id: 0 (\Device\NPF_{AB90C648-8F04-4A4D-B2A2-SAD6BAEBB265})
      Interface name: \Device\NPF_{AB90C648-8F04-4A4D-B2A2-SAD6BAEBB265}
      Interface description: WLAN
      Encapsulation type: Ethernet (1)
      Arrival Time: Apr 30, 2021 08:42:44.251636000 中国标准时间
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1619743364.251636000 seconds
      [Time delta from previous captured frame: 0.028711000 seconds]
      [Time delta from previous displayed frame: 0.028711000 seconds]
      [Time since reference or first frame: 0.071883000 seconds]
      Frame Number: 5
      Frame Length: 60 bytes (480 bits)
      Capture Length: 60 bytes (480 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp]
      [Coloring Rule Name: HTTP]
      [Coloring Rule String: http || tcp.port == 80 || http2]
    v Ethernet II, Src: Hangzhou_3c:d7:59 (c4:ca:d9:3c:d7:59), Dst: IntelCor_e5:04:7a (90:78:41:e5:04:7a)
      .. Destination: TotalLen: 480, 7a: 10b:70:41:e5:04:7a

```

查看具体内容（16 进制表示，winpacp 也可以进行类似操作）

```

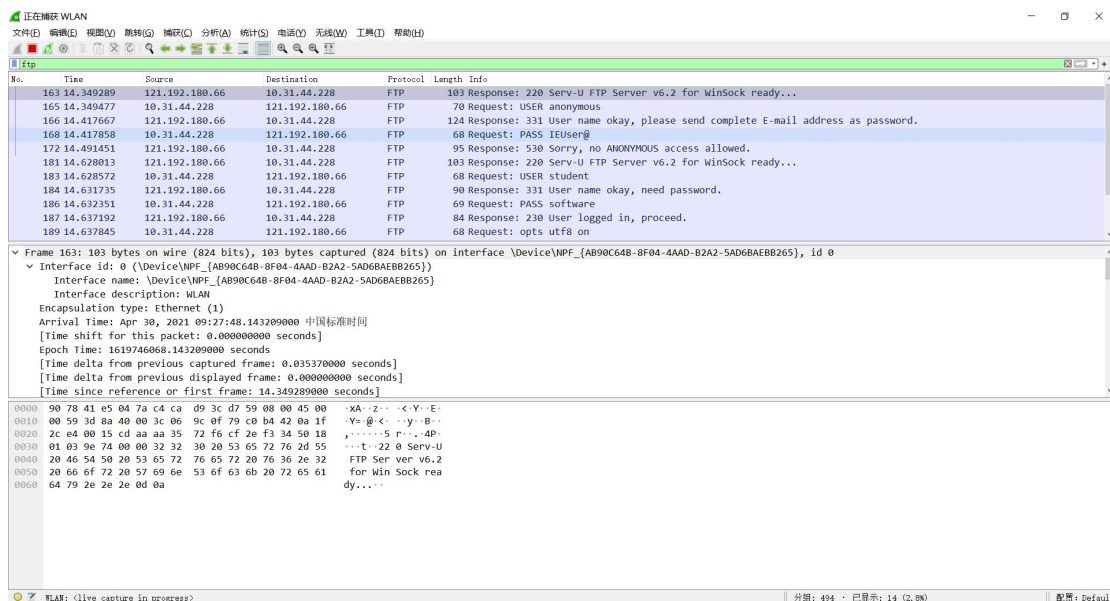
90 78 41 e5 04 7a c4 ca d9 3c d7 59 08 00 45 74  -X A - - - - - < - Y - - Et
00 28 87 ad 40 00 30 06 b0 48 8c ce 4e 95 0a 1f  - ( - - @ - - - H - - N - -
2c e4 00 50 c5 6a 7e 60 42 b2 cb c1 11 61 50 10  - , - - P - j - - B - - - - aP -
00 7b 39 03 00 00 00 00 00 00 00 00 00 00 00  - { 9 - - - - -

```

四次挥手

80.14.231280	180.163.222.207	10.31.44.228	TCP	60 80 → 50542 [ACK] Seq=1 Ack=965 Win=10640 Len=0
87.14.232182	180.163.222.207	10.31.44.228	HTTP	327 HTTP/1.1 200 OK
88.14.232364	10.31.44.228	180.163.222.207	TCP	54 50542 → 80 [FIN, ACK] Seq=965 Ack=274 Win=131328 Len=0
89.14.248129	10.31.44.228	180.163.222.207	TCP	66 50543 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
90.14.260306	180.163.222.207	10.31.44.228	TCP	60 80 → 50542 [FIN, ACK] Seq=274 Ack=966 Win=16640 Len=0
91.14.260408	10.31.44.228	180.163.222.207	TCP	54 50542 → 80 [ACK] Seq=966 Ack=275 Win=131328 Len=0
92.14.277255	180.163.222.207	10.31.44.228	TCP	62 80 → 50543 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1386 WS=128

进入 ftp（这里使用了学院的 ftp，很抱歉占用相关资源，可以看到 530、230 等回应）



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/leipipi>

5 实验总结

本次实验使用 wireshark 和 winpacp 配合，观察了网络流量，并加深了对以太网帧、IP 报文、TCP 段和 FTP 命令的格式的理解，真实看到了 TCP 三次握手和四次挥手的过程，以及登入 ftp 的整个传输过程，最后，初步了解了网络编程的一些相关操作。