

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 3 班

姓 名 王栋

学 号 22920192204283

实验时间 2021 年 3 月 31 日

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

1 实验环境

Windows10

2 实验结果

```

Frame 22735: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on Interface \\Device\\NPF_{FF145840-255C-42C9-A7A8-E9C5762A7AC}, ID 0
  Interface id: 0 (\\Device\\NPF_{FF145840-255C-42C9-A7A8-E9C5762A7AC})
    Encapsulation type: Ethernet (1)
      Arrival Time: May 28, 2021 08:54:32.443647000 中国标准时间
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1622163272.443647000 seconds
      [Time delta from previous captured frame: 0.000125000 seconds]
      [Time delta from previous displayed frame: 0.000125000 seconds]
      [Time since reference or first frame: 1438.988215000 seconds]
      Frame Number: 22735
      Frame Length: 122 bytes (976 bits)
      Capture Length: 122 bytes (976 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp:data]
      [Coloring Rule Name: TCP]
      [Coloring Rule String: tcp]
  ✓ Ethernet II, Src: IntelCor_39:79:a7 (74:70:fd:39:79:a7), Dst: Hangzhou_3c:d7:5c (c4:ca:d9:3c:d7:5c)
    > Destination: Hangzhou_3c:d7:5c (c4:ca:d9:3c:d7:5c)
    > Source: IntelCor_39:79:a7 (74:70:fd:39:79:a7)
    Type: IPv4 (0x8000)
  ✓ Internet Protocol Version 4, Src: 10.30.58.142, Dst: 123.189.164.69
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 108
    Identification: 0x5431 (21315)
    > Flags: 0x00, Don't Fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.30.58.142
    Destination Address: 123.189.164.69
  ✓ Transmission Control Protocol, Src Port: 7816, Dst Port: 9010, Seq: 1, Ack: 1, Len: 68
    Source Port: 7816
    Destination Port: 9010
    [Stream index: 1052]
    [TCP Segment Len: 68]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 66621999
    [Raw Sequence Number: 60]
    [Relative Sequence Number: 1]

```

从上往下依次为物理层，数据链路层，网络层，传输层的相关信息

```

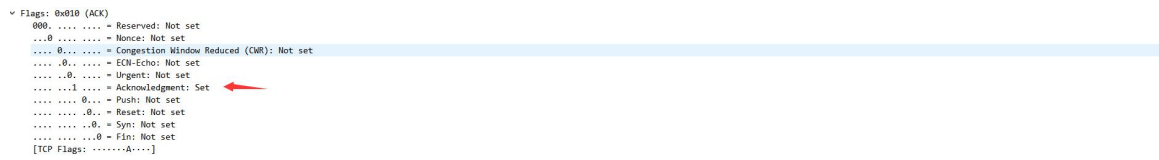
1000 ..... Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
000 ..... = Reserved: Not set
...0 ..... = Nonce: Not set
...0 ..... = Congestion Window Reduced (CWR): Not set
...0 ..... = ECH-Echo: Not set
...0 ..... = Urgent: Not set
...0 ..... = Acknowledgment: Not set
...0 ..... = Push: Not set
...0 ..... = Reset: Not set
> ...0...1... = Syn: Set
...0...0... = Fin: Not set

```

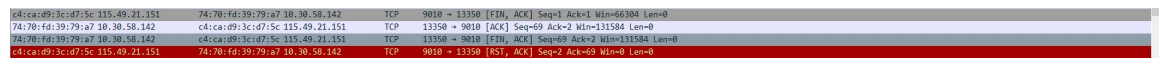
Tcp 第一次握手



第二次握手



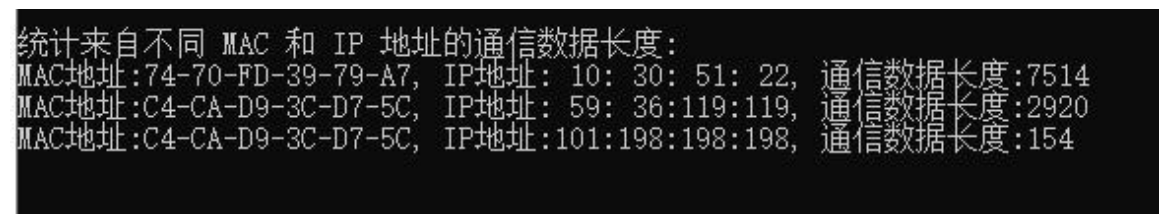
第三次握手



客户端断开链接，四次挥手

```
2021/03/31 16:09:24,C4-CA-D9-3C-D7-5C, 59: 36:119:119,74-70-FD-39-79-A7, 10: 30: 51: 22,129
2021/03/31 16:09:25,74-70-FD-39-79-A7, 10: 30: 51: 22,C4-CA-D9-3C-D7-5C,101:198:198:198,73
2021/03/31 16:09:25,74-70-FD-39-79-A7, 10: 30: 51: 22,C4-CA-D9-3C-D7-5C,101:198:198:198,73
2021/03/31 16:09:25,C4-CA-D9-3C-D7-5C,101:198:198:198,74-70-FD-39-79-A7, 10: 30: 51: 22,100
2021/03/31 16:09:25,C4-CA-D9-3C-D7-5C,101:198:198:198,74-70-FD-39-79-A7, 10: 30: 51: 22,132
2021/03/31 16:09:25,C4-CA-D9-3C-D7-5C, 59: 36:119:119,74-70-FD-39-79-A7, 10: 30: 51: 22,129
2021/03/31 16:09:26,C4-CA-D9-3C-D7-5C, 59: 36:119:119,74-70-FD-39-79-A7, 10: 30: 51: 22,129
```

文件输出日志



统计长度

74:70:fd:39:79:a7 10.30.51.22	c4:ca:d9:3c:d7:5c 121.192.180.66	FTP	Request: USER student
c4:ca:d9:3c:d7:5c 121.192.180.66	74:70:fd:39:79:a7 10.30.51.22	FTP	Response: 331 User name okay, need password.
74:70:fd:39:79:a7 10.30.51.22	c4:ca:d9:3c:d7:5c 121.192.180.66	FTP	Request: PASS 111
c4:ca:d9:3c:d7:5c 121.192.180.66	74:70:fd:39:79:a7 10.30.51.22	FTP	Response: 530 Not logged in.

检测 ftp，错误输入

74:70:fd:39:79:a7 10.30.51.22	c4:ca:d9:3c:d7:5c 121.192.180.66	FTP	Request: USER student
c4:ca:d9:3c:d7:5c 121.192.180.66	74:70:fd:39:79:a7 10.30.51.22	FTP	Response: 331 User name okay, need password.
74:70:fd:39:79:a7 10.30.51.22	c4:ca:d9:3c:d7:5c 121.192.180.66	FTP	Request: PASS software
c4:ca:d9:3c:d7:5c 121.192.180.66	74:70:fd:39:79:a7 10.30.51.22	FTP	Response: 230 User logged in, proceed.

检测 ftp，正确输入

3 实验代码

本次实验的代码已上传于以下代码仓库：<https://github.com/aLily11/cnii>

4 实验总结

通过这次实验学习用 WinPCAP 库监听网卡的数据流、统计流量、统计数据长度以及如何用 Wireshark 测试监听程序