厦門大學

信息学院软件工程系

《计算机网络》实验报告

题　　目 ___实验四 观察 TCP 报文段并侦听分析 FTP 协议

班　　级 　　软件工程 2018 级 1 班

姓　　名 　　林坚

学　　号 　　24320182203232

实验时间 　　2020 年 3 月 26 日

2020 年　　3 月　　26 日

1　实验目的

本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第二部分。

用 Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程，观察段ID、
窗口机制和拥塞控制机制等。将该过程截图在报告中。
用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征，
再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网
络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。
最终在文件上输出形如下列 CSV 格式的日志：
时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否

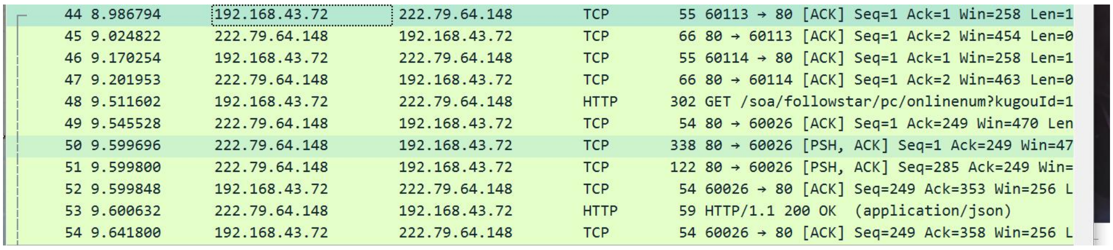
```
2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D
D5-72,192.168.33.2,student,software,SUCCEED
```

2　实验环境

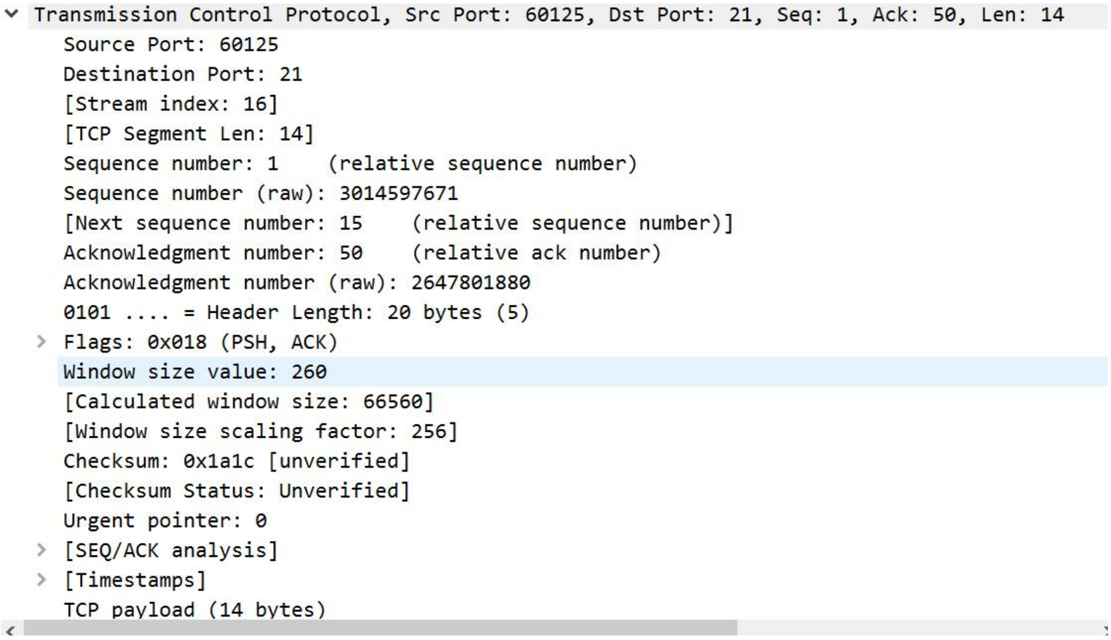
VS2017 ，C++,Winpcap 库

3　实验结果

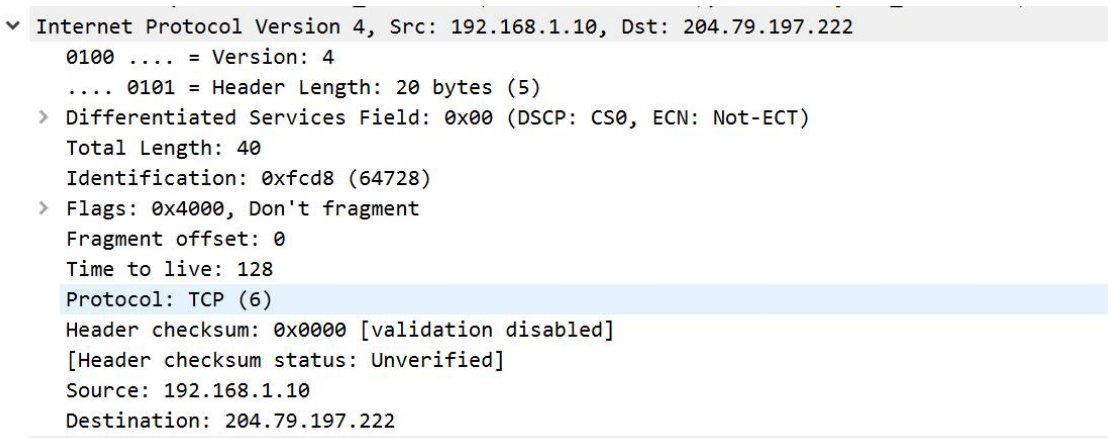
用 Wireshark 侦听并观察 TCP 数据段。观察三次挥手和四次挥手过程



```
44 8.986794   192.168.43.72   222.79.64.148   TCP    55 60113 → 80 [ACK] Seq=1 Ack=1 Win=258 Len=1
45 9.024822   222.79.64.148   192.168.43.72   TCP    66 80 → 60113 [ACK] Seq=1 Ack=2 Win=454 Len=0
46 9.170254   192.168.43.72   222.79.64.148   TCP    55 60114 → 80 [ACK] Seq=1 Ack=1 Win=258 Len=1
47 9.201953   222.79.64.148   192.168.43.72   TCP    66 80 → 60114 [ACK] Seq=1 Ack=2 Win=463 Len=0
48 9.511602   192.168.43.72   222.79.64.148   HTTP  302 GET /soa/followstar/pc/onlinenum?kugouId=1
49 9.545528   222.79.64.148   192.168.43.72   TCP    54 80 → 60026 [ACK] Seq=1 Ack=249 Win=470 Len
50 9.599696   222.79.64.148   192.168.43.72   TCP   338 80 → 60026 [PSH, ACK] Seq=1 Ack=249 Win=47
51 9.599800   222.79.64.148   192.168.43.72   TCP   122 80 → 60026 [PSH, ACK] Seq=285 Ack=249 Win=
52 9.599848   192.168.43.72   222.79.64.148   TCP    54 60026 → 80 [ACK] Seq=249 Ack=353 Win=256 L
53 9.600632   222.79.64.148   192.168.43.72   HTTP   59 HTTP/1.1 200 OK  (application/json)
54 9.641800   192.168.43.72   222.79.64.148   TCP    54 60026 → 80 [ACK] Seq=249 Ack=358 Win=256 L
```

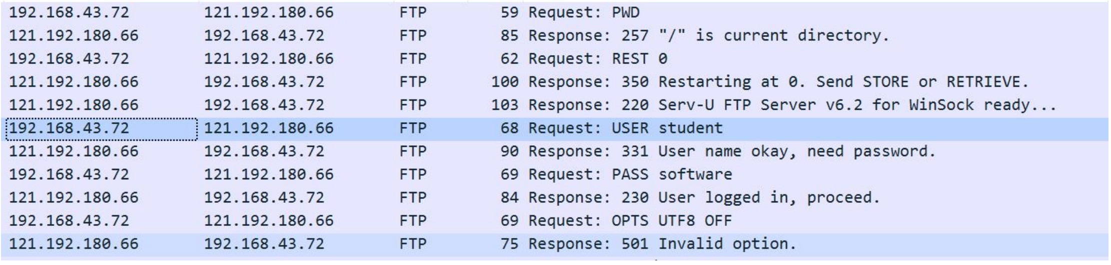


```
Transmission Control Protocol, Src Port: 60125, Dst Port: 21, Seq: 1, Ack: 50, Len: 14
  Source Port: 60125
  Destination Port: 21
  [Stream index: 16]
  [TCP Segment Len: 14]
  Sequence number: 1    (relative sequence number)
  Sequence number (raw): 3014597671
  [Next sequence number: 15    (relative sequence number)]
  Acknowledgment number: 50    (relative ack number)
  Acknowledgment number (raw): 2647801880
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
  Window size value: 260
  [Calculated window size: 66560]
  [Window size scaling factor: 256]
  Checksum: 0x1a1c [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
  TCP payload (14 bytes)
```

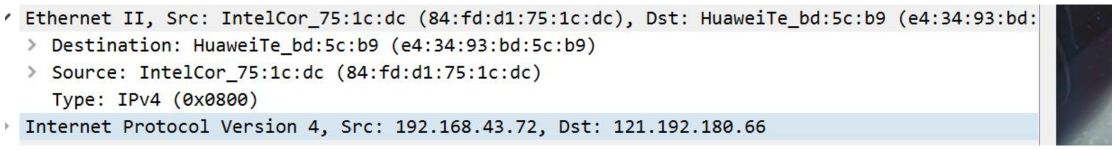


```
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 204.79.197.222
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0xfcd8 (64728)
> Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.10
  Destination: 204.79.197.222
```

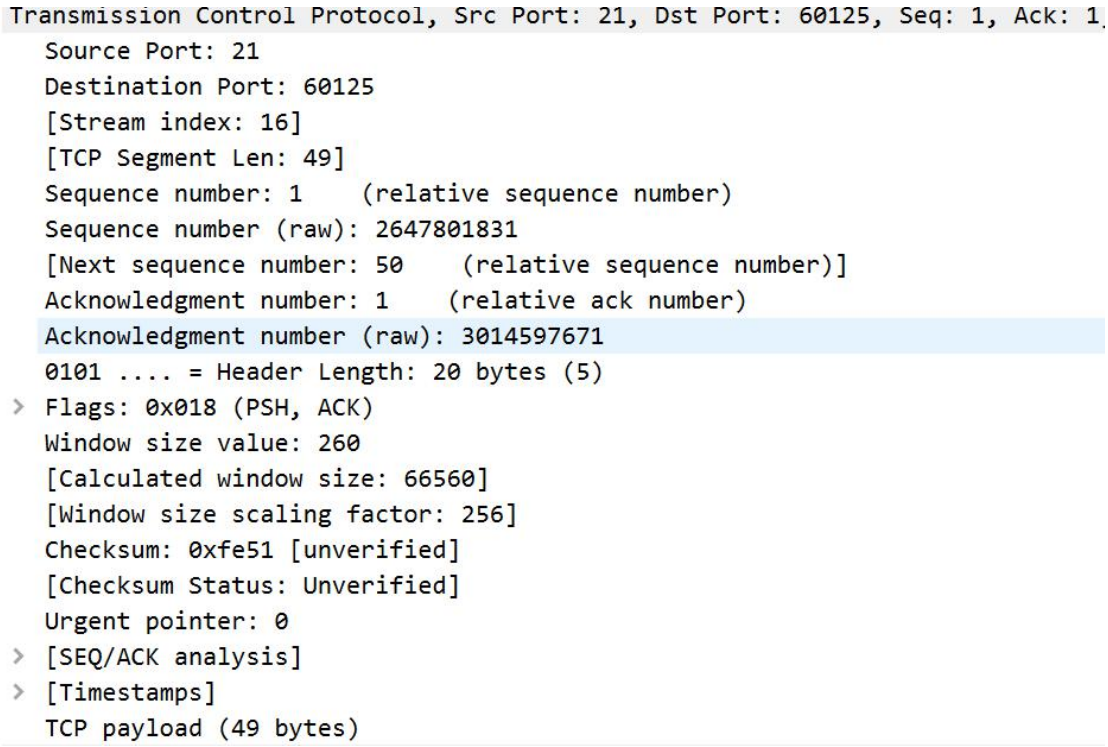
用 Wireshark 侦听并观察 FTP 数据



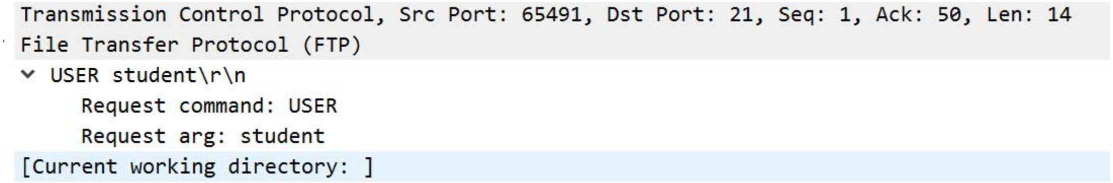
```
192.168.43.72     121.192.180.66    FTP     59 Request: PWD
121.192.180.66    192.168.43.72     FTP     85 Response: 257 "/" is current directory.
192.168.43.72     121.192.180.66    FTP     62 Request: REST 0
121.192.180.66    192.168.43.72     FTP    100 Response: 350 Restarting at 0. Send STORE or RETRIEVE.
121.192.180.66    192.168.43.72     FTP    103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
192.168.43.72     121.192.180.66    FTP     68 Request: USER student
121.192.180.66    192.168.43.72     FTP     90 Response: 331 User name okay, need password.
192.168.43.72     121.192.180.66    FTP     69 Request: PASS software
121.192.180.66    192.168.43.72     FTP     84 Response: 230 User logged in, proceed.
192.168.43.72     121.192.180.66    FTP     69 Request: OPTS UTF8 OFF
121.192.180.66    192.168.43.72     FTP     75 Response: 501 Invalid option.
```



```
Ethernet II, Src: IntelCor_75:1c:dc (84:fd:d1:75:1c:dc), Dst: HuaweiTe_bd:5c:b9 (e4:34:93:bd:
  > Destination: HuaweiTe_bd:5c:b9 (e4:34:93:bd:5c:b9)
  > Source: IntelCor_75:1c:dc (84:fd:d1:75:1c:dc)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.72, Dst: 121.192.180.66
```

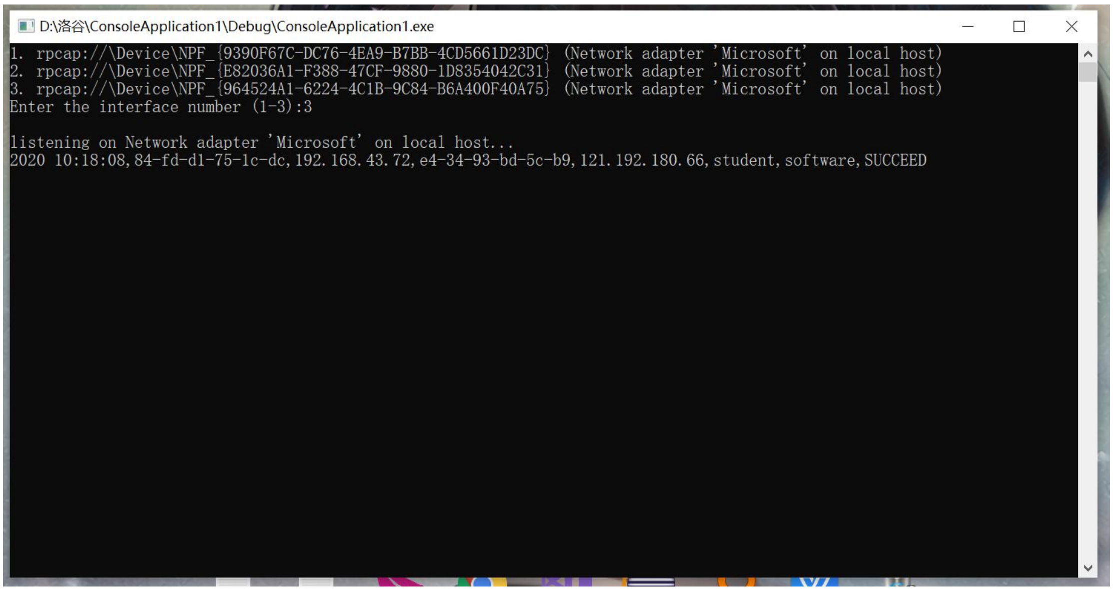


```
Transmission Control Protocol, Src Port: 21, Dst Port: 60125, Seq: 1, Ack: 1,
    Source Port: 21
    Destination Port: 60125
    [Stream index: 16]
    [TCP Segment Len: 49]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 2647801831
    [Next sequence number: 50    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 3014597671
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0xfe51 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (49 bytes)
```



```
Transmission Control Protocol, Src Port: 65491, Dst Port: 21, Seq: 1, Ack: 50, Len: 14
File Transfer Protocol (FTP)
  v USER student\r\n
        Request command: USER
        Request arg: student
[Current working directory: ]
```

基于 WinPCAP 工具包制作程序，实现监听网
络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

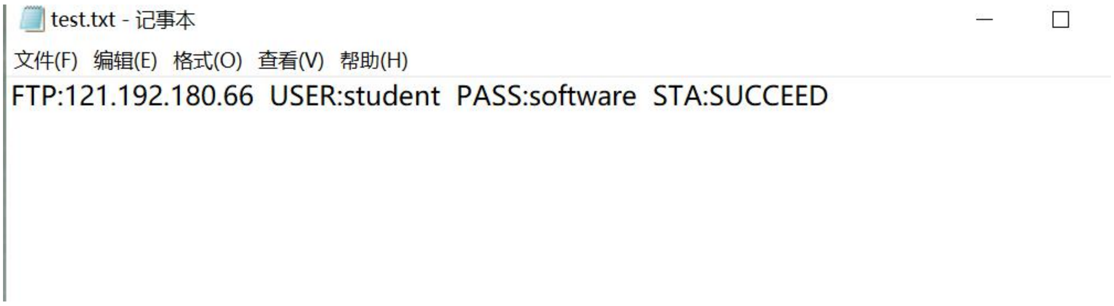


D:\洛谷\ConsoleApplication1\Debug\ConsoleApplication1.exe

```
1. rpcap://\Device\NPF_{9390F67C-DC76-4EA9-B7BB-4CD5661D23DC} (Network adapter 'Microsoft' on local host)
2. rpcap://\Device\NPF_{E82036A1-F388-47CF-9880-1D8354042C31} (Network adapter 'Microsoft' on local host)
3. rpcap://\Device\NPF_{964524A1-6224-4C1B-9C84-B6A400F40A75} (Network adapter 'Microsoft' on local host)
Enter the interface number (1-3):3

listening on Network adapter 'Microsoft' on local host...
2020 10:18:08,84-fd-d1-75-1c-dc,192.168.43.72,e4-34-93-bd-5c-b9,121.192.180.66,student,software,SUCCEED
```

保存到当地 txt 文件里，格式如下



FTP:121.192.180.66 USER:student PASS:software STA:SUCCEED

4 实验总结

通过实验的收获，真实总结，勿长篇大论。

总结：对于 FTP 的运作原理有了更深入的认识，对于 TCP 报文握手挥手过程从不了解到大概了解，对于 FTP 登录环节的通信过程有了大概的认识。