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 王薪蕾

学　　号 **24320182203285**

实验时间 **2020** 年 **3** 月 **25** 日

2020 年　**3** 月　**25** 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 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
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,software1,FAILED
```

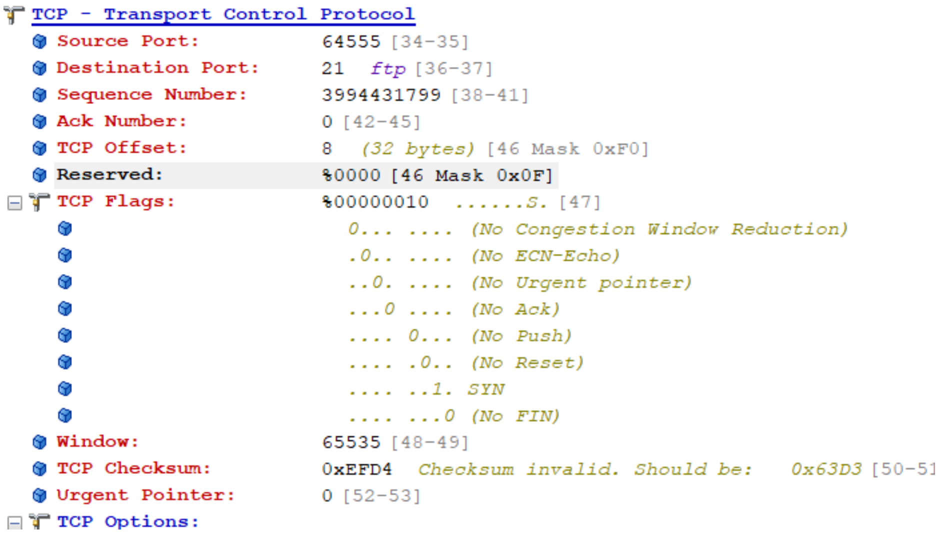
2 实验环境

操作系统：windows，编程语言：C++

3 实验结果

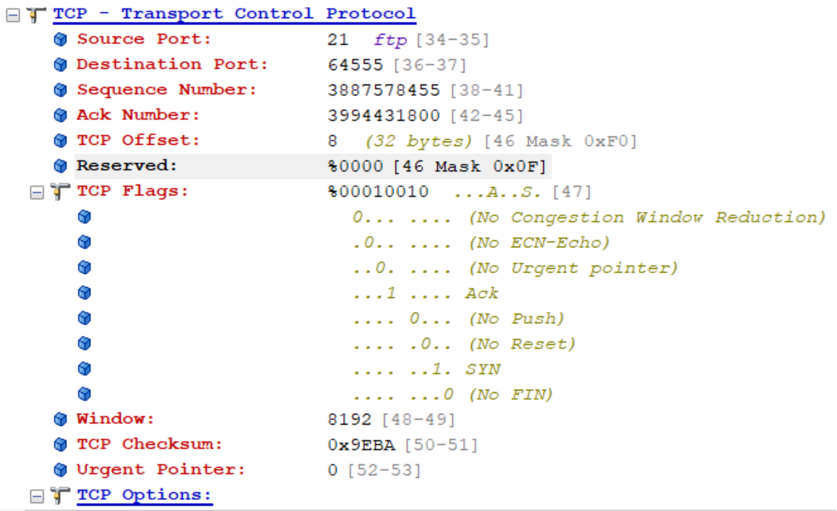
建立时三次握手

Syn 建立→ftp



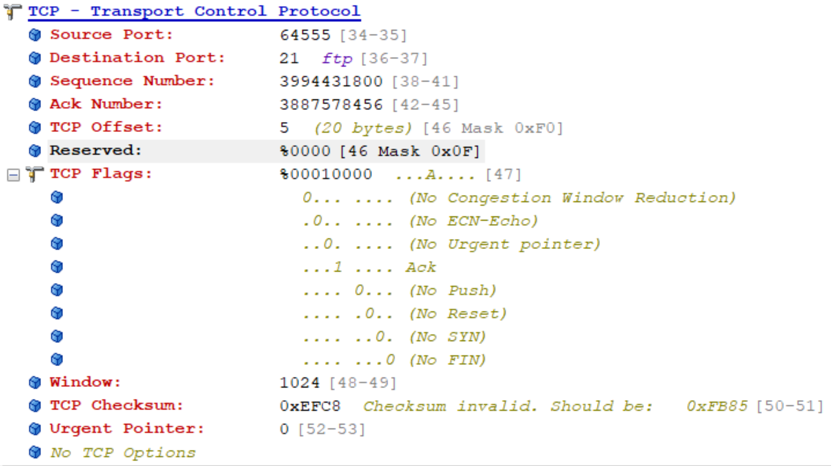
```
TCP - Transport Control Protocol
  Source Port:            64555 [34-35]
  Destination Port:       21   ftp [36-37]
  Sequence Number:        3994431799 [38-41]
  Ack Number:             0 [42-45]
  TCP Offset:             8   (32 bytes) [46 Mask 0xF0]
  Reserved:               %0000 [46 Mask 0x0F]
  TCP Flags:              %00000010   ......S. [47]
                            0... .... (No Congestion Window Reduction)
                            .0.. .... (No ECN-Echo)
                            ..0. .... (No Urgent pointer)
                            ...0 .... (No Ack)
                            .... 0... (No Push)
                            .... .0.. (No Reset)
                            .... ..1. SYN
                            .... ...0 (No FIN)
  Window:                 65535 [48-49]
  TCP Checksum:           0xEFD4  Checksum invalid. Should be:   0x63D3 [50-51
  Urgent Pointer:         0 [52-53]
  TCP Options:
```

ftp→Ack 有效 syn 建立

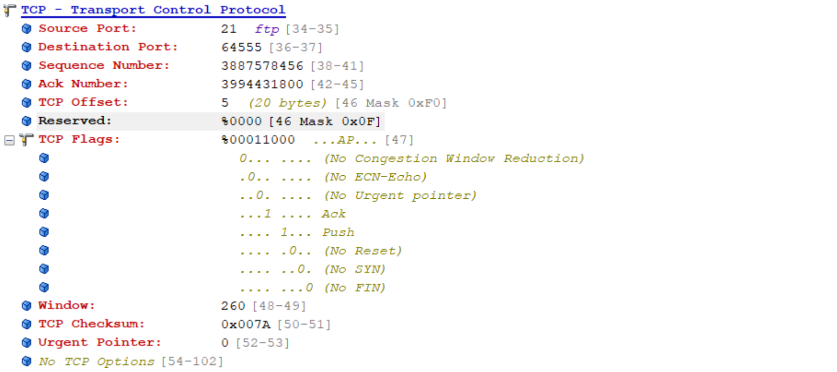


```
⊟ TCP - Transport Control Protocol
     Source Port:              21   ftp [34-35]
     Destination Port:         64555 [36-37]
     Sequence Number:          3887578455 [38-41]
     Ack Number:               3994431800 [42-45]
     TCP Offset:               8   (32 bytes) [46 Mask 0xF0]
     Reserved:                 %0000 [46 Mask 0x0F]
  ⊟ TCP Flags:                 %00010010   ...A..S. [47]
                                 0... ....  (No Congestion Window Reduction)
                                 .0.. ....  (No ECN-Echo)
                                 ..0. ....  (No Urgent pointer)
                                 ...1 ....  Ack
                                 .... 0...  (No Push)
                                 .... .0..  (No Reset)
                                 .... ..1.  SYN
                                 .... ...0  (No FIN)
     Window:                   8192 [48-49]
     TCP Checksum:             0x9EBA [50-51]
     Urgent Pointer:           0 [52-53]
  ⊟ TCP Options:
```

Ack 有效→ftp



```
TCP - Transport Control Protocol
   Source Port:              64555 [34-35]
   Destination Port:         21   ftp [36-37]
   Sequence Number:          3994431800 [38-41]
   Ack Number:               3887578456 [42-45]
   TCP Offset:               5   (20 bytes) [46 Mask 0xF0]
   Reserved:                 %0000 [46 Mask 0x0F]
⊟ TCP Flags:                 %00010000   ...A.... [47]
                               0... ....  (No Congestion Window Reduction)
                               .0.. ....  (No ECN-Echo)
                               ..0. ....  (No Urgent pointer)
                               ...1 ....  Ack
                               .... 0...  (No Push)
                               .... .0..  (No Reset)
                               .... ..0.  (No SYN)
                               .... ...0  (No FIN)
   Window:                   1024 [48-49]
   TCP Checksum:             0xEFC8   Checksum invalid. Should be:   0xFB85 [50-51]
   Urgent Pointer:           0 [52-53]
   No TCP Options
```



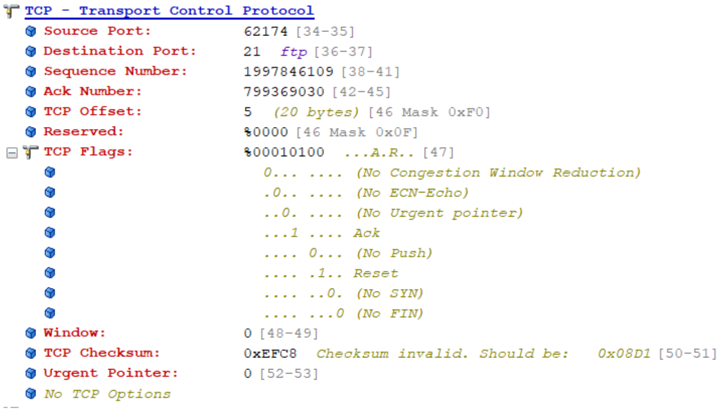
```
TCP - Transport Control Protocol
   Source Port:              21   ftp [34-35]
   Destination Port:         64555 [36-37]
   Sequence Number:          3887578456 [38-41]
   Ack Number:               3994431800 [42-45]
   TCP Offset:               5   (20 bytes) [46 Mask 0xF0]
   Reserved:                 %0000 [46 Mask 0x0F]
⊟ TCP Flags:                 %00011000   ...AP... [47]
                               0... ....  (No Congestion Window Reduction)
                               .0.. ....  (No ECN-Echo)
                               ..0. ....  (No Urgent pointer)
                               ...1 ....  Ack
                               .... 1...  Push
                               .... .0..  (No Reset)
                               .... ..0.  (No SYN)
                               .... ...0  (No FIN)
   Window:                   260 [48-49]
   TCP Checksum:             0x007A [50-51]
   Urgent Pointer:           0 [52-53]
   No TCP Options [54-102]
```

断开时如果直接关闭窗口，WinPcap 无法捕捉到包

用命令行连接时出现‘远程主机关闭连接’的错误

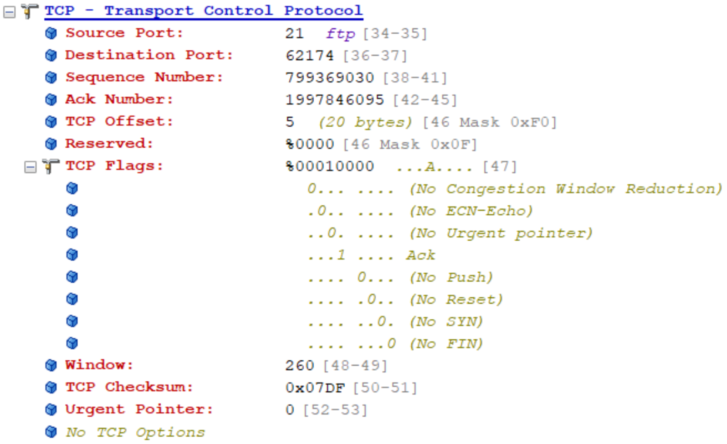
此时抓到这样的包

RST 复位 TCP 连接→ftp



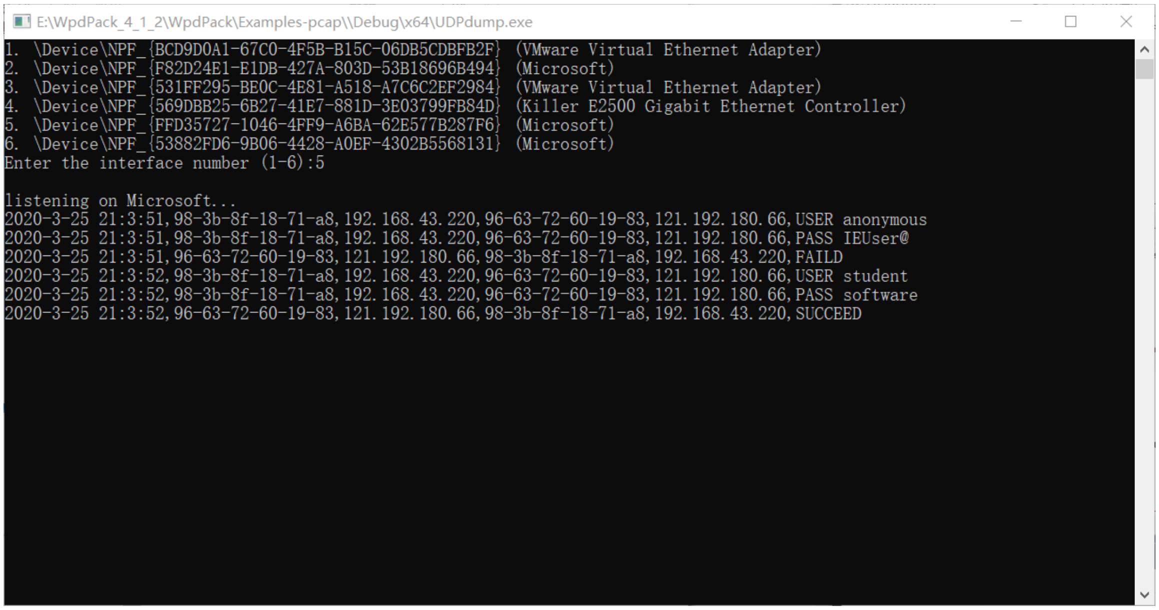
```
TCP - Transport Control Protocol
    Source Port:              62174 [34-35]
    Destination Port:         21   ftp [36-37]
    Sequence Number:          1997846109 [38-41]
    Ack Number:               799369030 [42-45]
    TCP Offset:               5   (20 bytes) [46 Mask 0xF0]
    Reserved:                 %0000 [46 Mask 0x0F]
  TCP Flags:                  %00010100   ...A.R.. [47]
                                0... .... (No Congestion Window Reduction)
                                .0.. .... (No ECN-Echo)
                                ..0. .... (No Urgent pointer)
                                ...1 .... Ack
                                .... 0... (No Push)
                                .... .1.. Reset
                                .... ..0. (No SYN)
                                .... ...0 (No FIN)
    Window:                   0 [48-49]
    TCP Checksum:             0xEFC8  Checksum invalid. Should be:   0x08D1 [50-51]
    Urgent Pointer:           0 [52-53]
    No TCP Options
```

ftp→ACK



```
TCP - Transport Control Protocol
    Source Port:              21   ftp [34-35]
    Destination Port:         62174 [36-37]
    Sequence Number:          799369030 [38-41]
    Ack Number:               1997846095 [42-45]
    TCP Offset:               5   (20 bytes) [46 Mask 0xF0]
    Reserved:                 %0000 [46 Mask 0x0F]
  TCP Flags:                  %00010000   ...A.... [47]
                                0... .... (No Congestion Window Reduction)
                                .0.. .... (No ECN-Echo)
                                ..0. .... (No Urgent pointer)
                                ...1 .... Ack
                                .... 0... (No Push)
                                .... .0.. (No Reset)
                                .... ..0. (No SYN)
                                .... ...0 (No FIN)
    Window:                   260 [48-49]
    TCP Checksum:             0x07DF [50-51]
    Urgent Pointer:           0 [52-53]
    No TCP Options
```

编程的输出图：


E:\WpdPack_4_1_2\WpdPack\Examples-pcap\\Debug\x64\UDPdump.exe

```
1.  \Device\NPF_{BCD9D0A1-67C0-4F5B-B15C-06DB5CDBFB2F}  (VMware Virtual Ethernet Adapter)
2.  \Device\NPF_{F82D24E1-E1DB-427A-803D-53B18696B494}  (Microsoft)
3.  \Device\NPF_{531FF295-BE0C-4E81-A518-A7C6C2EF2984}  (VMware Virtual Ethernet Adapter)
4.  \Device\NPF_{569DBB25-6B27-41E7-881D-3E03799FB84D}  (Killer E2500 Gigabit Ethernet Controller)
5.  \Device\NPF_{FFD35727-1046-4FF9-A6BA-62E577B287F6}  (Microsoft)
6.  \Device\NPF_{53882FD6-9B06-4428-A0EF-4302B5568131}  (Microsoft)
Enter the interface number (1-6):5

listening on Microsoft...
2020-3-25 21:3:51,98-3b-8f-18-71-a8,192.168.43.220,96-63-72-60-19-83,121.192.180.66,USER anonymous
2020-3-25 21:3:51,98-3b-8f-18-71-a8,192.168.43.220,96-63-72-60-19-83,121.192.180.66,PASS IEUser@
2020-3-25 21:3:51,96-63-72-60-19-83,121.192.180.66,98-3b-8f-18-71-a8,192.168.43.220,FAILD
2020-3-25 21:3:52,98-3b-8f-18-71-a8,192.168.43.220,96-63-72-60-19-83,121.192.180.66,USER student
2020-3-25 21:3:52,98-3b-8f-18-71-a8,192.168.43.220,96-63-72-60-19-83,121.192.180.66,PASS software
2020-3-25 21:3:52,96-63-72-60-19-83,121.192.180.66,98-3b-8f-18-71-a8,192.168.43.220,SUCCEED
```

4 实验总结

学习了 ftp 的 TCP 握手协议，其连接、终止

怎么从包中分析出用户名、密码和是否成功连接