

# 廈門大學



## 信息学院软件工程系

### 《计算机网络》实验报告

题    目 实验四  观察 TCP 报文段并监听分析 FTP 协议

班    级 软件工程 2018 级 3 班

姓    名 沈黄隽

学    号 24320182203260

实验时间 2020 年 3 月 23 日

2020 年 4 月 7 日

## 1 实验目的

先用 Omnipcap 或 Wireshark 侦听并观察 TCP 报文段。观察其建立和撤除连接的过程，观察其报文段 ID、窗口机制和拥塞控制机制等。将其过程截图在报告中。

用 Omnipcap 或 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

操作环境：Visual Studio 2019、WpdPack、Wireshark

编程语言：C 语言

### 3 实验结果

1、观察 TCP 数据段，观察 Wireshark 对数据的分组形式，观察建立及撤除连接的过程。具体截图如下：

The first screenshot shows the initial TCP connection establishment. The second screenshot shows the continuation of the connection with data exchange and a FIN/ACK sequence.

No.	Time	Source	Destination	Protocol	Length	Info
67	3.261732	192.168.43.182	40.90.10.66	TCP	54	12646 → 443 [ACK] Seq=1 Ack=219 Win=1023 Len=0
79	3.936378	192.168.43.182	121.192.180.66	TCP	66	14432 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM...
80	4.033766	121.192.180.66	192.168.43.182	TCP	66	21 → 14432 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1360 WS=256...
81	4.033948	192.168.43.182	121.192.180.66	TCP	54	14432 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
82	4.110252	121.192.180.66	192.168.43.182	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
83	4.110374	192.168.43.182	121.192.180.66	TCP	54	14432 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
84	4.110560	192.168.43.182	121.192.180.66	FTP	70	Request: USER anonymous
85	4.118990	121.192.180.66	192.168.43.182	FTP	124	Response: 331 User name okay, please send complete E-mail address...
86	4.189147	192.168.43.182	121.192.180.66	TCP	54	14432 → 21 [ACK] Seq=17 Ack=120 Win=261888 Len=0
87	4.189349	192.168.43.182	121.192.180.66	FTP	68	Request: PASS IEUser@
88	4.223780	192.168.43.182	203.119.129.64	TCP	55	[TCP Keep-Alive] 12110 → 443 [ACK] Seq=0 Ack=1 Win=64725 Len=1
89	4.264490	121.192.180.66	192.168.43.182	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
90	4.264597	192.168.43.182	121.192.180.66	TCP	54	14432 → 21 [ACK] Seq=31 Ack=161 Win=261888 Len=0
91	4.264659	192.168.43.182	121.192.180.66	TCP	54	14432 → 21 [FIN, ACK] Seq=31 Ack=161 Win=261888 Len=0
92	4.267411	192.168.43.182	121.192.180.66	TCP	66	14433 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM...

  

No.	Time	Source	Destination	Protocol	Length	Info
110	4.407709	121.192.180.66	192.168.43.182	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
111	4.407806	192.168.43.182	121.192.180.66	TCP	54	14433 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
112	4.407884	192.168.43.182	121.192.180.66	FTP	68	Request: USER student
113	4.466303	192.168.43.182	121.192.180.66	TCP	66	14434 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM...
115	4.491642	121.192.180.66	192.168.43.182	FTP	90	Response: 331 User name okay, need password.
116	4.491744	192.168.43.182	121.192.180.66	TCP	54	14433 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
117	4.491809	192.168.43.182	121.192.180.66	FTP	69	Request: PASS software
118	4.544080	121.192.180.66	192.168.43.182	TCP	66	21 → 14434 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1360 WS=256...
119	4.544218	192.168.43.182	121.192.180.66	TCP	54	14434 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
120	4.562964	121.192.180.66	192.168.43.182	FTP	84	Response: 230 User logged in, proceed.
121	4.563054	192.168.43.182	121.192.180.66	TCP	54	14433 → 21 [ACK] Seq=30 Ack=116 Win=261888 Len=0
122	4.563140	192.168.43.182	121.192.180.66	FTP	68	Request: opts utf8 on
123	4.567178	192.168.43.182	117.184.242.159	TLSv1.2	92	Application Data
124	4.620641	121.192.180.66	192.168.43.182	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
125	4.620763	192.168.43.182	121.192.180.66	TCP	54	14434 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
126	4.620837	192.168.43.182	121.192.180.66	FTP	70	Request: USER anonymous
127	4.632416	121.192.180.66	192.168.43.182	FTP	75	Response: 501 Invalid option.

2.观察端口参数，了解 TCP 握手与挥手过程

> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)

▼ Ethernet II, Src: HuaweiTe\_21:a1:65 (d0:16:b4:21:a1:65), Dst: IntelCor\_cc:97:78 (a0:c5:89:cc:97:78)

> Destination: IntelCor\_cc:97:78 (a0:c5:89:cc:97:78)

> Source: HuaweiTe\_21:a1:65 (d0:16:b4:21:a1:65)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 121.192.180.66, Dst: 192.168.3.9

▼ Transmission Control Protocol, Src Port: 21, Dst Port: 64331, Seq: 1, Ack: 1, Len: 49

Source Port: 21

Destination Port: 64331

[Stream index: 0]

[TCP Segment Len: 49]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 3030692600

[Next sequence number: 50 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 558041827

v Flags: 0x4000, Don't fragment  
 0... .. = Reserved bit: Not set  
 .1... .. = Don't fragment: Set  
 ..0... .. = More fragments: Not set  
 Fragment offset: 0  
 Time to live: 46  
 Protocol: TCP (6)  
 Header checksum: 0x2886 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 121.192.180.66

0000	a0 c5 89 cc 97 78 d0 16	b4 21 a1 65 08 00 45 a0	.....x... !.e..E..
0010	00 59 31 c5 40 00 2e 06	28 86 79 c0 b4 42 c0 a8	..Y1..@... (.y..B..
0020	03 09 00 15 fb 4b b4 a4	b2 f8 21 43 0a e3 50 18	.....K... !C..P..
0030	01 02 2f f2 00 00 32 32	30 20 53 65 72 76 2d 55	.. /...22 0 Serv-U
0040	20 46 54 50 20 53 65 72	76 65 72 20 76 36 2e 32	FTP Ser ver v6.2
0050	20 66 6f 72 20 57 69 6e	53 6f 63 6b 20 72 65 61	for Win Sock rea
0060	64 79 2e 2e 2e 0d 0a		dy.....

Acknowledgment number: 1 (relative ack number)  
 Acknowledgment number (raw): 558041827  
 0101 .... = Header Length: 20 bytes (5)  
 v Flags: 0x018 (PSH, 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  
 ....1... .. = Push: Set  
 ....0... .. = Reset: Not set  
 ....0... .. = Syn: Not set  
 ....0... .. = Fin: Not set  
 [TCP Flags: .....AP...]  
 Window size value: 258  
 [Calculated window size: 258]  
 [Window size scaling factor: -1 (unknown)]  
 Checksum: 0x2ff2 [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 v [SEQ/ACK analysis]

0000	a0 c5 89 cc 97 78 d0 16	b4 21 a1 65 08 00 45 a0	.....x... !.e..E..
0010	00 59 31 c5 40 00 2e 06	28 86 79 c0 b4 42 c0 a8	..Y1..@... (.y..B..
0020	03 09 00 15 fb 4b b4 a4	b2 f8 21 43 0a e3 50 18	.....K... !C..P..
0030	01 02 2f f2 00 00 32 32	30 20 53 65 72 76 2d 55	.. /...22 0 Serv-U
0040	20 46 54 50 20 53 65 72	76 65 72 20 76 36 2e 32	FTP Ser ver v6.2
0050	20 66 6f 72 20 57 69 6e	53 6f 63 6b 20 72 65 61	for Win Sock rea
0060	64 79 2e 2e 2e 0d 0a		dy.....

v Transmission Control Protocol, Src Port: 21, Dst Port: 64331, Seq: 1, Ack: 1, Len: 49  
 Source Port: 21  
 Destination Port: 64331  
 [Stream index: 0]  
 [TCP Segment Len: 49]  
 Sequence number: 1 (relative sequence number)  
 Sequence number (raw): 3030692600  
 [Next sequence number: 50 (relative sequence number)]  
 Acknowledgment number: 1 (relative ack number)  
 Acknowledgment number (raw): 558041827

0000	a0 c5 89 cc 97 78 d0 16	b4 21 a1 65 08 00 45 a0	.....x... !.e..E..
0010	00 59 31 c5 40 00 2e 06	28 86 79 c0 b4 42 c0 a8	..Y1..@... (.y..B..
0020	03 09 00 15 fb 4b b4 a4	b2 f8 21 43 0a e3 50 18	.....K... !C..P..
0030	01 02 2f f2 00 00 32 32	30 20 53 65 72 76 2d 55	.. /...22 0 Serv-U
0040	20 46 54 50 20 53 65 72	76 65 72 20 76 36 2e 32	FTP Ser ver v6.2
0050	20 66 6f 72 20 57 69 6e	53 6f 63 6b 20 72 65 61	for Win Sock rea
0060	64 79 2e 2e 2e 0d 0a		dy.....



3、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

	A	B	C	D	E	F	G	H
1	2020/4/7 19:47	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	anonymous	IEUser@	FAILED
2	2020/4/7 19:47	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	anonymous	IEUser@	FAILED
3	2020/4/7 19:47	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	anonymous	IEUser@	FAILED
4	2020/4/7 19:47	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	student	software	SUCCEED
5	2020/4/7 19:57	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	anonymous	IEUser@	FAILED
6	2020/4/7 19:57	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	student	software	SUCCEED
7	2020/4/7 19:57	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	anonymous	IEUser@	FAILED
8	2020/4/7 19:57	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	student	IEUser@	FAILED
9	2020/4/7 19:57	00-E1-8C-BF-44-47	192.168.0.102	74-C3-30-B5-1E-0C	121.192.180.66	student	software	SUCCEED
10								

表格输出到硬盘的形式如下：

	A	B	C	D	E
1	FTP:121.192.180.66	USR:anonymous	PAS:IEUser@	STA:FAILED	
2	FTP:121.192.180.66	USR:anonymous	PAS:IEUser@	STA:FAILED	
3	FTP:121.192.180.66	USR:anonymous	PAS:IEUser@	STA:FAILED	
4	FTP:121.192.180.66	USR:student	PAS:software	STA:OK	
5	FTP:121.192.180.66	USR:anonymous	PAS:IEUser@	STA:FAILED	
6	FTP:121.192.180.66	USR:student	PAS:software	STA:OK	
7	FTP:121.192.180.66	USR:anonymous	PAS:IEUser@	STA:FAILED	
8	FTP:121.192.180.66	USR:student	PAS:IEUser@	STA:FAILED	
9	FTP:121.192.180.66	USR:student	PAS:software	STA:OK	
10					

## 4 实验总结

用 Wireshark 软件对 FTP 通信时的网络分组进行了侦听操作，观察了解 TCP 握手和挥手的过程。对 FTP 的通信协议的过程有了更为深入的理解，且在此基础编程能力得到提升。