



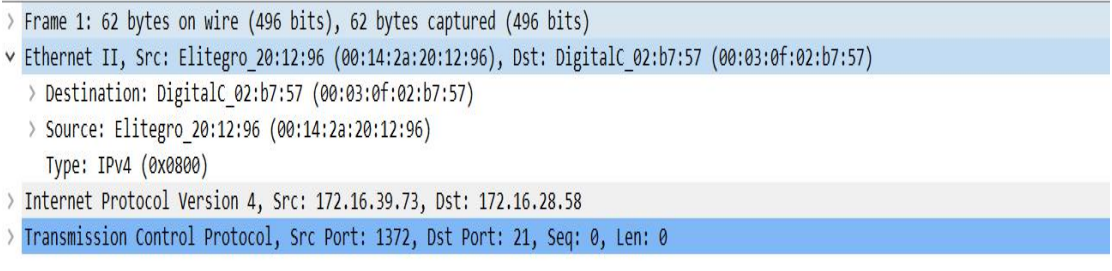
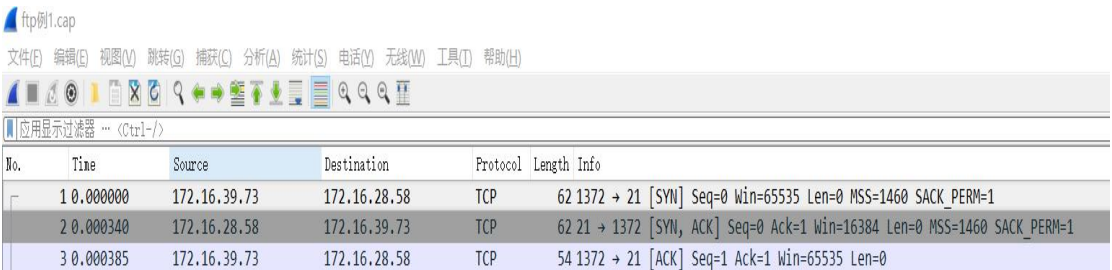
警示

- 1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
- 2.当次小组成员成绩只计学号、姓名登录在下表中的。
- 3.在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
- 4.实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院	班 级	15-1 班	组长	李佳
学号	15331151	15331150	15331143		
学生	李佳	李辉旭	黎皓斌		

Ftp 协议分析实验

一、打开“FTP 数据包”的“ftp 例 1.cap”文件，进行观察分析，回答以下问题(见附件)

题号	
1	FTP 客户端的 mac 地址是多少？
答案	00:14:2a:20:12:96
截图	
分析	由第一条抓包数据的协议树可以看到源的 MAC 地址，即客户端的 MAC 地址；
2	第 1、2、3 号报文的作用是什么？
答案	客户端与服务器之间的三次握手机制，建立 TCP 连接；
截图	
分析	1 号报文是客户端发送给服务器请求建立连接，2 号报文是服务器发送给客户端确认连接，3 号报文是客户端发送给服务器确认包，完毕后客户端与服务器进入 ESTABLISHED 状态，完成握手；
3	该数据包中共有多少个 TCP 流？
答案	5 个 TCP 流



截图

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000340	172.16.28.58	172.16.39.73	TCP	62	21 → 1372 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
16	31.309871	172.16.39.73	172.16.28.58	TCP	62	1377 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
39	104.700924	172.16.39.73	172.16.28.58	TCP	62	1380 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
111	111.708455	172.16.39.73	172.16.28.58	TCP	62	1381 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
131	149.974102	172.16.39.73	172.16.28.58	TCP	62	1384 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1

分析

每一个 TCP 流都会有三次握手过程，而三次握手中的第二次握手是由服务器发送给客户端确认连接，此时标志位 SYN 和 ACK 都是 1，而其他任何时候这两个标志位不同时为 1，因此使用过滤规则 `tcp.flags.syn==1 and tcp.flags.ack==1` 可以得到一共有多少个第二次握手，即有多少个 TCP 流；

4

用什么用户和密码登录成功？

答案

用户和密码都是 **wlx2008**

截图

68 Request: USER wlx2008
90 Response: 331 User name okay, need password.
54 1372 → 21 [ACK] Seq=15 Ack=86 Win=65450 Len=0
68 Request: PASS wlx2008
84 Response: 230 User logged in, proceed.

分析

由 6 号和 9 号报文的具体信息可以看到登陆的用用户名和密码都是 **wlx2008**；

5

该 FTP 的命令连接和数据连接分别是什么样的连接？

答案

命令连接：1372-21，用户名密码的命令连接；

数据连接：1377-20、1380-20、1381-20、1384-20，PORT 的数据连接；

截图

4	0.001815	172.16.28.58	172.16.39.73	FTP	104	Response: 220 Serv-U FTP Server V6.4 for Winsock ready...
5	0.201287	172.16.39.73	172.16.28.58	TCP	54	1372 → 21 [ACK] Seq=1 Ack=50 Win=65486 Len=0
6	17.542571	172.16.39.73	172.16.28.58	FTP	68	Request: USER wlx2008
7	17.543205	172.16.28.58	172.16.39.73	FTP	90	Response: 331 User name okay, need password.
8	17.678704	172.16.39.73	172.16.28.58	TCP	54	1372 → 21 [ACK] Seq=15 Ack=86 Win=65450 Len=0
9	21.617636	172.16.39.73	172.16.28.58	FTP	68	Request: PASS wlx2008
10	21.618699	172.16.28.58	172.16.39.73	FTP	84	Response: 230 User logged in, proceed.
15	31.309831	172.16.28.58	172.16.39.73	TCP	62	20 → 1377 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
16	31.309871	172.16.39.73	172.16.28.58	TCP	62	1377 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
17	31.310370	172.16.28.58	172.16.39.73	TCP	60	20 → 1377 [ACK] Seq=1 Ack=1 Win=65535 Len=0
18	31.310880	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
19	31.310901	172.16.28.58	172.16.39.73	FTP-DA	178	FTP Data: 124 bytes
20	31.310908	172.16.28.58	172.16.39.73	TCP	60	20 → 1377 [FIN, ACK] Seq=125 Ack=1 Win=65535 Len=0
21	31.310931	172.16.39.73	172.16.28.58	TCP	54	1377 → 20 [ACK] Seq=1 Ack=126 Win=65411 Len=0
22	31.343834	172.16.39.73	172.16.28.58	TCP	54	1377 → 20 [FIN, ACK] Seq=1 Ack=126 Win=65411 Len=0
23	31.342522	172.16.28.58	172.16.39.73	TCP	60	20 → 1377 [ACK] Seq=126 Ack=2 Win=65535 Len=0
39	104.700924	172.16.39.73	172.16.28.58	TCP	62	1380 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
40	104.701226	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=1 Win=65535 Len=0
41	104.701805	172.16.28.58	172.16.39.73	FTP	112	Response: 150 Opening ASCII mode data connection for xs2009-9.xls.
42	104.721779	172.16.39.73	172.16.28.58	FTP-DA	1514	FTP Data: 1460 bytes
43	104.731400	172.16.39.73	172.16.28.58	FTP-DA	1514	FTP Data: 1460 bytes
111	111.708455	172.16.39.73	172.16.28.58	TCP	62	1381 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
112	111.708976	172.16.28.58	172.16.39.73	TCP	60	20 → 1381 [ACK] Seq=1 Ack=1 Win=65535 Len=0
113	111.709282	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
114	111.709494	172.16.28.58	172.16.39.73	FTP-DA	367	FTP Data: 313 bytes
131	149.974102	172.16.39.73	172.16.28.58	TCP	62	1384 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
132	149.974406	172.16.28.58	172.16.39.73	TCP	60	20 → 1384 [ACK] Seq=1 Ack=1 Win=65535 Len=0
133	149.975126	172.16.28.58	172.16.39.73	FTP	121	Response: 150 Opening ASCII mode data connection for 888.xls (57856 Bytes).
134	149.976040	172.16.28.58	172.16.39.73	FTP-DA	1514	FTP Data: 1460 bytes



分析	1372-21 的控制连接贯穿于整个 FTP 会话中，用于保持用户登录；会话中 PORT 的数据连接用来传送文件或目录；
6	该 FTP 的连接模式是那种？为什么？
答案	主动模式(PORT 命令)
截图	
分析	从 12 号报文看出客户端向服务器发送 PORT 请求，指定端口进行数据传输；
7	最后四个报文的作用是什么？
答案	四次挥手，结束 TCP 连接并确认中断信息传输。
截图	
分析	<p>(1) TCP 客户端发送一个 FIN，关闭到服务器的数据传送；</p> <p>(2) 服务器收到 FIN 后发回 ACK，确认序号为收到的序号加 1。</p> <p>(3) 服务器关闭客户端连接，发送一个 FIN 给客户端；</p> <p>(4) 客户端发回 ACK 报文确认，并将确认序号设置为收到序号加 1；</p>
8	该数据包中有多少个 ftp 的命令及应答，其含义分别是什么？
答案	<p>有十次命令和十次应答：</p> <p>■命令：</p> <ol style="list-style-type: none"> 1. USER：登陆的用户名 2. PASS：用户登录口令 3. PORT：采用主动模式连接客户端 4. NLST：返回指定路径下的目录列表 5. XMKD：创建新目录 6. RNFR：重命名文件夹 7. RNTD：和 RNFR 命令共同完成对文件的重命名，紧跟在 RNFR 命令后 8. STOR：上传一个指定的文件并存储在指定的位置 9. RETR：请求服务器将指定路径内的文件复制到客户端 10. QUIT：关闭与服务器的连接



■ 应答:

1. 220: 表示新用户已准备好
2. 331: 用户名正确, 需要口令
3. 230: 用户登录
4. 200: 命令成功
5. 150: 文件状态良好, 打开数据连接
6. 226: 关闭数据连接, 请求的文件操作成功
7. 257: 创建 "PATHNAME"
8. 350: 请求的文件操作需要进一步命令
9. 250: 请求的文件操作完成
10. 221: 服务器关闭控制连接, 准备退出登录

截图

```
220 Serv-U FTP Server v6.4 for WinSock ready...
USER wlx2008
331 User name okay, need password.
PASS wlx2008
230 User logged in, proceed.
PORT 172,16,39,73,5,97
200 PORT Command successful.
NLST -l
150 Opening ASCII mode data connection for /bin/ls.
226-Maximum disk quota limited to 307200 kBytes
    Used disk quota 0 kBytes, available 307200 kBytes
226 Transfer complete.
XMKD jjj
257 "/jjj" directory created.
RNFR jjj
350 File or directory exists, ready for destination name
RNTD ppp
250 RNTD command successful.
PORT 172,16,39,73,5,100
200 PORT Command successful.
STOR xs2009-9.xls
150 Opening ASCII mode data connection for xs2009-9.xls.
226-Maximum disk quota limited to 307200 kBytes
    Used disk quota 56 kBytes, available 307143 kBytes
226 Transfer complete.
PORT 172,16,39,73,5,101
200 PORT Command successful.
NLST -l
150 Opening ASCII mode data connection for /bin/ls.
226-Maximum disk quota limited to 307200 kBytes
    Used disk quota 56 kBytes, available 307143 kBytes
226 Transfer complete.
RNFR xs2009-9.xls

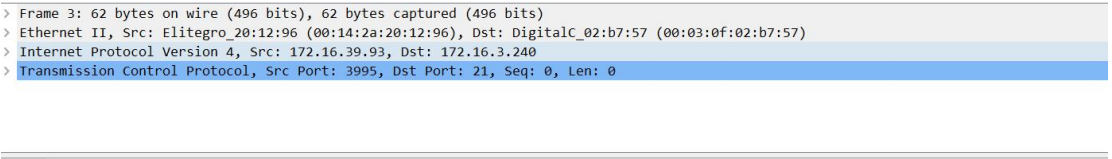
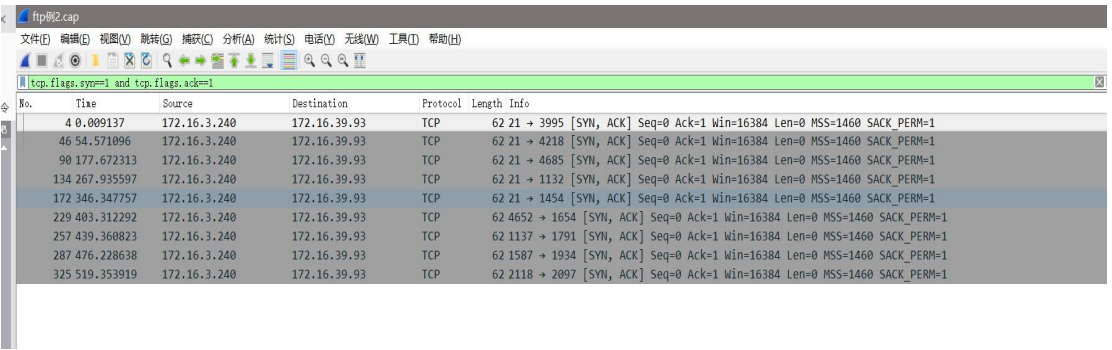
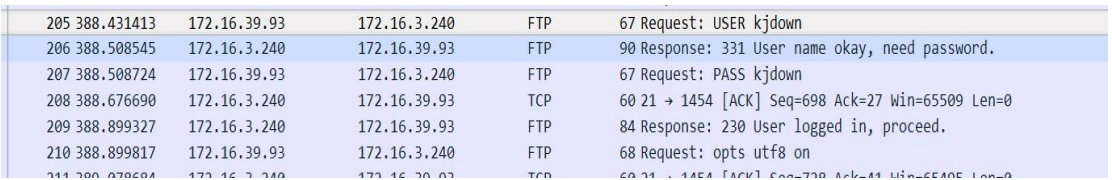
350 File or directory exists, ready for destination name
RNTD 888.xls
250 RNTD command successful.
PORT 172,16,39,73,5,104
200 PORT Command successful.
RETR 888.xls
150 Opening ASCII mode data connection for 888.xls (57856 Bytes).
226-Maximum disk quota limited to 307200 kBytes
    Used disk quota 56 kBytes, available 307143 kBytes
226 Transfer complete.
QUIT
221 Goodbye!
```




分析

选择菜单中的：分析->追踪流->TCP 流，追踪 TCP 流，即可看到 ftp 的命令及应答的具体内容，分析内容已体现在答案中；

二、打开“FTP 数据包”的“ftp 例 2.cap”文件，进行观察分析，回答以下问题

题号	
1	FTP 服务器的 ip 是多少？FTP 客户端的 mac 地址是多少？
答案	服务器 IP: 172.16.3.240 客户端 MAC 地址: 00:14:2a:20:12:96
截图	
分析	由客户端发送到服务器的 3 号报文协议树可以看到源以及目的地址的 IP 地址和 MAC 地址。源是客户端，目的地址是服务器地址。
2	该数据包中共有多少个 TCP 流？
答案	9 个 TCP 流
截图	
分析	每一个 TCP 流都会有三次握手过程，而三次握手中的第二次握手是由服务器发送给客户端确认连接，此时标志位 SYN 和 ACK 都是 1，而其他任何时候这两个标志位不同时为 1，因此使用过滤规则 tcp.flags.syn==1 and tcp.flags.ack==1 可以得到一共有多少个第二次握手，即有多少个 TCP 流；
3	最后用什么用户和密码登录成功？
答案	用户和密码都是 kjdown
截图	
分析	该 ftp 连接中前几次尝试登录失败，在 205 号-209 号报文中可以看到登录成功，账号密码都是 kjdown；
4	该 FTP 的命令连接和数据连接分别是什么？



计算机网络实验报告

答案

命令连接：3995-21、4218-21、4685-21、1132-21、1454-21,用户名密码登录的命令连接；

数据连接：4652-1654、1791-1137、1934-1587、2118-2097 ,4 个 PASV 的数据连接；

截图

17	22.945884	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=235	Win=65301	Len=0
19	23.250506	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=268	Win=65268	Len=0
21	26.207502	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=318	Win=65218	Len=0
23	27.008573	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=368	Win=65168	Len=0
25	29.344540	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=418	Win=65118	Len=0
27	31.102584	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=478	Win=65068	Len=0
31	36.454298	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=548	Win=64996	Len=0
33	39.208106	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=586	Win=64950	Len=0
35	44.579627	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=1	Ack=638	Win=64898	Len=0
37	52.281410	172.16.39.93	172.16.3.240	FTP	62	1654	→	4652	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460 SACK_PERM=1
41	54.422035	172.16.39.93	172.16.3.240	TCP	54	4218	→	21	[ACK]	Seq=1	Ack=1	Win=65310	Len=0
45	54.561498	172.16.39.93	172.16.3.240	TCP	54	4218	→	21	[ACK]	Seq=1	Ack=1	Win=65310	Len=0
49	55.532843	172.16.39.93	172.16.3.240	TCP	54	3995	→	21	[ACK]	Seq=32	Ack=761	Win=64776	Len=0
51	58.007863	172.16.39.93	172.16.3.240	TCP	54	4218	→	21	[ACK]	Seq=1	Ack=26	Win=65510	Len=0
53	60.423950	172.16.39.93	172.16.3.240	TCP	54	4218	→	21	[ACK]	Seq=1	Ack=77	Win=65459	Len=0
55	63.166166	172.16.39.93	172.16.3.240	TCP	54	4218	→	21	[ACK]	Seq=1	Ack=119	Win=65417	Len=0
57	65.400686	172.16.39.93	172.16.3.240	TCP	54	4218	→	21	[ACK]	Seq=1	Ack=157	Win=65379	Len=0

113	207.750790	172.16.39.93	172.16.3.240	TCP	54	4685	→	21	[ACK]	Seq=1	Ack=448	Win=65148	Len=0
115	209.929770	172.16.39.93	172.16.3.240	TCP	54	4685	→	21	[ACK]	Seq=1	Ack=492	Win=65044	Len=0
117	210.437503	172.16.39.93	172.16.3.240	TCP	54	4685	→	21	[ACK]	Seq=1	Ack=540	Win=64996	Len=0
119	212.570477	172.16.39.93	172.16.3.240	TCP	54	4685	→	21	[ACK]	Seq=1	Ack=586	Win=64950	Len=0
121	213.281453	172.16.39.93	172.16.3.240	TCP	54	4685	→	21	[ACK]	Seq=1	Ack=638	Win=64898	Len=0
123	216.269943	172.16.39.93	172.16.3.240	FTP	62	1654	→	4652	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460 SACK_PERM=1
125	219.672114	172.16.39.93	172.16.3.240	FTP	62	1654	→	4652	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460 SACK_PERM=1
127	223.838438	172.16.39.93	172.16.3.240	TCP	54	4685	→	21	[ACK]	Seq=23	Ack=718	Win=64818	Len=0
129	224.069364	172.16.39.93	172.16.3.240	TCP	54	4685	→	21	[ACK]	Seq=24	Ack=719	Win=64818	Len=0
131	267.033845	172.16.39.93	172.16.3.240	TCP	62	1132	→	21	[ACK]	Seq=0	Win=65535	Len=0	MSS=1460 SACK_PERM=1
133	267.935655	172.16.39.93	172.16.3.240	TCP	54	1132	→	21	[ACK]	Seq=1	Ack=1	Win=65535	Len=0
137	270.803642	172.16.39.93	172.16.3.240	TCP	54	1132	→	21	[ACK]	Seq=1	Ack=26	Win=65510	Len=0
139	273.104108	172.16.39.93	172.16.3.240	TCP	54	1132	→	21	[ACK]	Seq=1	Ack=77	Win=65459	Len=0
141	275.237019	172.16.39.93	172.16.3.240	TCP	54	1132	→	21	[ACK]	Seq=1	Ack=119	Win=65417	Len=0
143	277.572948	172.16.39.93	172.16.3.240	TCP	54	1132	→	21	[ACK]	Seq=1	Ack=157	Win=65379	Len=0
145	280.010608	172.16.39.93	172.16.3.240	TCP	54	1132	→	21	[ACK]	Seq=1	Ack=209	Win=65327	Len=0

179	349.786760	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=119	Win=65417	Len=0
181	353.341592	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=157	Win=65379	Len=0
183	353.544771	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=209	Win=65327	Len=0
185	354.966641	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=235	Win=65301	Len=0
187	355.169849	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=268	Win=65268	Len=0
189	356.998037	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=318	Win=65218	Len=0
191	359.232438	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=368	Win=65168	Len=0
193	364.310813	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=418	Win=65118	Len=0
195	369.692270	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=470	Win=65066	Len=0
197	371.623585	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=492	Win=65044	Len=0
199	372.029815	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=540	Win=64996	Len=0
201	384.217815	172.16.39.93	172.16.3.240	TCP	54	1454	→	21	[ACK]	Seq=1	Ack=586	Win=64950	Len=0

分析

3995-21、4218-21、4685-21、1132-21、1454-21 的控制连接贯穿于 FTP 流，用于用户登录；会话中 4652-1654、1791-1137、1934-1587、2118-2097 PASV 的数据连接用来传送文件或目录；

5

哪几个报文是 FTP 数据连接的三次握手报文？

答案

有四次数据连接：1. 228-230

2. 256-258

3. 286-288

4. 324-326

截图

228	403.311489	172.16.39.93	172.16.3.240	TCP	62	1654	→	4652	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	SACK_PERM=1	
229	403.312292	172.16.3.240	172.16.39.93	TCP	62	4652	→	1654	[SYN, ACK]	Seq=0	Ack=1	Win=16384	Len=0	MSS=1460	SACK_PERM=1
230	403.312346	172.16.39.93	172.16.3.240	TCP	54	1654	→	4652	[ACK]	Seq=1	Ack=1	Win=65535	Len=0		

256	439.360533	172.16.39.93	172.16.3.240	TCP	62	1791	→	1137	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	SACK_PERM=1	
257	439.360823	172.16.3.240	172.16.39.93	TCP	62	1137	→	1791	[SYN, ACK]	Seq=0	Ack=1	Win=16384	Len=0	MSS=1460	SACK_PERM=1
258	439.360876	172.16.39.93	172.16.3.240	TCP	54	1791	→	1137	[ACK]	Seq=1	Ack=1	Win=65535	Len=0		

286	476.228404	172.16.39.93	172.16.3.240	TCP	62	1934 → 1587	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	SACK_PERM=1	
287	476.228638	172.16.3.240	172.16.39.93	TCP	62	1587 → 1934	[SYN, ACK]	Seq=0	Ack=1	Win=16384	Len=0	MSS=1460	SACK_PERM=1
288	476.228669	172.16.39.93	172.16.3.240	TCP	54	1934 → 1587	[ACK]	Seq=1	Ack=1	Win=65535	Len=0		

324	519.351289	172.16.39.93	172.16.3.240	TCP	62	2097 → 2118	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	SACK_PERM=1	
325	519.353919	172.16.3.240	172.16.39.93	TCP	62	2118 → 2097	[SYN, ACK]	Seq=0	Ack=1	Win=16384	Len=0	MSS=1460	SACK_PERM=1
326	519.353959	172.16.39.93	172.16.3.240	TCP	54	2097 → 2118	[ACK]	Seq=1	Ack=1	Win=65535	Len=0		

分析

FTP 有 9 个 TCP 流，其中五次控制连接，四次数据连接的握手报文 228-230、256-258、286-288、324-326；

6

哪几个报文是 FTP 数据连接的挥手报文（结束报文）？



	有四次断开数据连接的挥手，其挥手报文号如下：																																																																																					
答案	<div>1. 237-240</div> <div>2. 270-273</div> <div>3. 293-297</div> <div>4. 620-623</div>																																																																																					
截图	<table><tr><td>237 403.735946</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 4652 → 1654 [FIN, ACK] Seq=1517 Ack=1 Win=65535 Len=0</td></tr><tr><td>238 403.736017</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1654 → 4652 [ACK] Seq=1 Ack=1518 Win=65535 Len=0</td></tr><tr><td>239 403.736121</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1654 → 4652 [FIN, ACK] Seq=1 Ack=1518 Win=65535 Len=0</td></tr><tr><td>240 403.741744</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 4652 → 1654 [ACK] Seq=1518 Ack=2 Win=65535 Len=0</td></tr></table> <table><tr><td>270 447.419304</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1137 → 1791 [FIN, ACK] Seq=2992 Ack=1 Win=65535 Len=0</td></tr><tr><td>271 447.419373</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1791 → 1137 [ACK] Seq=1 Ack=2993 Win=65464 Len=0</td></tr><tr><td>272 447.419475</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1791 → 1137 [FIN, ACK] Seq=1 Ack=2993 Win=65464 Len=0</td></tr><tr><td>273 447.419643</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1137 → 1791 [ACK] Seq=2993 Ack=2 Win=65535 Len=0</td></tr></table> <table><tr><td>293 476.501474</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1587 → 1934 [FIN, ACK] Seq=1131 Ack=1 Win=65535 Len=0</td></tr><tr><td>294 476.501536</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1934 → 1587 [ACK] Seq=1 Ack=1132 Win=64405 Len=0</td></tr><tr><td>295 476.541711</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1454 → 21 [ACK] Seq=178 Ack=1362 Win=64174 Len=0</td></tr><tr><td>296 476.561030</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1934 → 1587 [FIN, ACK] Seq=1 Ack=1132 Win=64405 Len=0</td></tr><tr><td>297 476.561201</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1587 → 1934 [ACK] Seq=1132 Ack=2 Win=65535 Len=0</td></tr></table> <table><tr><td>620 534.787848</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 2118 → 2097 [FIN, ACK] Seq=239105 Ack=1 Win=65535 Len=0</td></tr><tr><td>621 534.787917</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 2097 → 2118 [ACK] Seq=1 Ack=239106 Win=65535 Len=0</td></tr><tr><td>622 534.788371</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 2097 → 2118 [FIN, ACK] Seq=1 Ack=239106 Win=65535 Len=0</td></tr><tr><td>623 534.789817</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 2118 → 2097 [ACK] Seq=239106 Ack=2 Win=65535 Len=0</td></tr></table>	237 403.735946	172.16.3.240	172.16.39.93	TCP	60 4652 → 1654 [FIN, ACK] Seq=1517 Ack=1 Win=65535 Len=0	238 403.736017	172.16.39.93	172.16.3.240	TCP	54 1654 → 4652 [ACK] Seq=1 Ack=1518 Win=65535 Len=0	239 403.736121	172.16.39.93	172.16.3.240	TCP	54 1654 → 4652 [FIN, ACK] Seq=1 Ack=1518 Win=65535 Len=0	240 403.741744	172.16.3.240	172.16.39.93	TCP	60 4652 → 1654 [ACK] Seq=1518 Ack=2 Win=65535 Len=0	270 447.419304	172.16.3.240	172.16.39.93	TCP	60 1137 → 1791 [FIN, ACK] Seq=2992 Ack=1 Win=65535 Len=0	271 447.419373	172.16.39.93	172.16.3.240	TCP	54 1791 → 1137 [ACK] Seq=1 Ack=2993 Win=65464 Len=0	272 447.419475	172.16.39.93	172.16.3.240	TCP	54 1791 → 1137 [FIN, ACK] Seq=1 Ack=2993 Win=65464 Len=0	273 447.419643	172.16.3.240	172.16.39.93	TCP	60 1137 → 1791 [ACK] Seq=2993 Ack=2 Win=65535 Len=0	293 476.501474	172.16.3.240	172.16.39.93	TCP	60 1587 → 1934 [FIN, ACK] Seq=1131 Ack=1 Win=65535 Len=0	294 476.501536	172.16.39.93	172.16.3.240	TCP	54 1934 → 1587 [ACK] Seq=1 Ack=1132 Win=64405 Len=0	295 476.541711	172.16.39.93	172.16.3.240	TCP	54 1454 → 21 [ACK] Seq=178 Ack=1362 Win=64174 Len=0	296 476.561030	172.16.39.93	172.16.3.240	TCP	54 1934 → 1587 [FIN, ACK] Seq=1 Ack=1132 Win=64405 Len=0	297 476.561201	172.16.3.240	172.16.39.93	TCP	60 1587 → 1934 [ACK] Seq=1132 Ack=2 Win=65535 Len=0	620 534.787848	172.16.3.240	172.16.39.93	TCP	60 2118 → 2097 [FIN, ACK] Seq=239105 Ack=1 Win=65535 Len=0	621 534.787917	172.16.39.93	172.16.3.240	TCP	54 2097 → 2118 [ACK] Seq=1 Ack=239106 Win=65535 Len=0	622 534.788371	172.16.39.93	172.16.3.240	TCP	54 2097 → 2118 [FIN, ACK] Seq=1 Ack=239106 Win=65535 Len=0	623 534.789817	172.16.3.240	172.16.39.93	TCP	60 2118 → 2097 [ACK] Seq=239106 Ack=2 Win=65535 Len=0
237 403.735946	172.16.3.240	172.16.39.93	TCP	60 4652 → 1654 [FIN, ACK] Seq=1517 Ack=1 Win=65535 Len=0																																																																																		
238 403.736017	172.16.39.93	172.16.3.240	TCP	54 1654 → 4652 [ACK] Seq=1 Ack=1518 Win=65535 Len=0																																																																																		
239 403.736121	172.16.39.93	172.16.3.240	TCP	54 1654 → 4652 [FIN, ACK] Seq=1 Ack=1518 Win=65535 Len=0																																																																																		
240 403.741744	172.16.3.240	172.16.39.93	TCP	60 4652 → 1654 [ACK] Seq=1518 Ack=2 Win=65535 Len=0																																																																																		
270 447.419304	172.16.3.240	172.16.39.93	TCP	60 1137 → 1791 [FIN, ACK] Seq=2992 Ack=1 Win=65535 Len=0																																																																																		
271 447.419373	172.16.39.93	172.16.3.240	TCP	54 1791 → 1137 [ACK] Seq=1 Ack=2993 Win=65464 Len=0																																																																																		
272 447.419475	172.16.39.93	172.16.3.240	TCP	54 1791 → 1137 [FIN, ACK] Seq=1 Ack=2993 Win=65464 Len=0																																																																																		
273 447.419643	172.16.3.240	172.16.39.93	TCP	60 1137 → 1791 [ACK] Seq=2993 Ack=2 Win=65535 Len=0																																																																																		
293 476.501474	172.16.3.240	172.16.39.93	TCP	60 1587 → 1934 [FIN, ACK] Seq=1131 Ack=1 Win=65535 Len=0																																																																																		
294 476.501536	172.16.39.93	172.16.3.240	TCP	54 1934 → 1587 [ACK] Seq=1 Ack=1132 Win=64405 Len=0																																																																																		
295 476.541711	172.16.39.93	172.16.3.240	TCP	54 1454 → 21 [ACK] Seq=178 Ack=1362 Win=64174 Len=0																																																																																		
296 476.561030	172.16.39.93	172.16.3.240	TCP	54 1934 → 1587 [FIN, ACK] Seq=1 Ack=1132 Win=64405 Len=0																																																																																		
297 476.561201	172.16.3.240	172.16.39.93	TCP	60 1587 → 1934 [ACK] Seq=1132 Ack=2 Win=65535 Len=0																																																																																		
620 534.787848	172.16.3.240	172.16.39.93	TCP	60 2118 → 2097 [FIN, ACK] Seq=239105 Ack=1 Win=65535 Len=0																																																																																		
621 534.787917	172.16.39.93	172.16.3.240	TCP	54 2097 → 2118 [ACK] Seq=1 Ack=239106 Win=65535 Len=0																																																																																		
622 534.788371	172.16.39.93	172.16.3.240	TCP	54 2097 → 2118 [FIN, ACK] Seq=1 Ack=239106 Win=65535 Len=0																																																																																		
623 534.789817	172.16.3.240	172.16.39.93	TCP	60 2118 → 2097 [ACK] Seq=239106 Ack=2 Win=65535 Len=0																																																																																		
分析	FTP 的数据连接为非持久连接，数据传输完成即关闭，FTP 有 4 个数据连接，故有相对应的 4 个挥手断开连接；																																																																																					
7	该 FTP 的连接模式是那种？为什么？																																																																																					
答案	连接模式是被动模式。客户端的命令为 PASV，因此连接模式为被动模式。																																																																																					
截图	<pre>220 USER kjdown 331 User name okay, need password. PASS kjdown 230 User logged in, proceed. opts utf8 on 501 Invalid option. syst 215 UNIX Type: L8 site help 501 SITE option not supported. PWD 257 "/" is current directory. TYPE A 200 Type set to A. PASV 227 Entering Passive Mode (172,16,3,240,18,44) LIST 150 Opening ASCII mode data connection for /bin/ls. 226 Transfer complete. noop 200 Command okay. CWD /...../ 250 Directory changed to /...../ TYPE A 200 Type set to A. PASV 227 Entering Passive Mode (172,16,3,240,18,44)</pre>																																																																																					
分析	建立数据连接时，客户端发送给服务器 PASV 命令，服务器打开一个高端端口传送数据；																																																																																					

三、在线捕获数据包实验



1. 阅读教材 P64-69 内容，熟悉 FTP 协议。
2. 完成 P51 的实例 2-1。

[实验目的]

1. 了解网络数据类型。
2. 了解网络工作原理。
3. 了解工具 Wireshark 的使用。

[实验原理]

Wireshark 是一款开源网络协议分析器，它可以实时检测网络通信数据，检测其网络通信数据，然后通过图形界面浏览这些数据，查看网络通信数据包中每层的详细内容。

Wireshark 包含有强大的显示过滤器语言和查看 TCP 会话重构流的能力，支持上百种协议和媒体类型。

Wireshark 使用 Tcpdump 和 Linux 下的 libpcap 库直接同硬件驱动接触，可以不经过操作系统，保证了抓包速率和抓包的精确性。

关于 Wireshark 的详细使用可以参考本书第 1 章的相关内容。

[实验内容]

(1) 单击 Wireshark 工具栏左起第一个图标在接口上开始侦听，片刻后停止侦听。这时截获的数据量有多少？

14.408948s 内捕获的数据量有 4486 条。如下图所示：

The screenshot displays the Wireshark interface with a packet capture list on the left, a packet details pane in the middle, and a packet bytes pane on the right. The packet list shows a series of packets captured on interface 0, including DNS queries and responses, TCP SYN and ACK packets, and TLSv1.2 client and server hello messages. The packet details pane for the selected packet (Frame 1) shows the structure of the frame, Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

(2) 观察捕获数据的源 IP 地址和目的 IP 地址，这些数据是发出的还是发过来的？选择几个 IP 地址，通过网站 www.ip138.com 查询这些 IP 地址的地理位置。



23 6.186182 192.168.199.208 112.80.248.251 TCP 66 52504 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

192.168.199.208 (本机 IP) → 112.80.248.251(江苏省南京市联通) 发送数据

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:112.80.248.251

- 本站数据: 江苏省南京市 联通
- 参考数据1: 江苏南京 联通
- 参考数据2: 江苏省南京市 联通

[idc公司大全](#) | [ip查询接口](#)

如果您发现查询结果不详细或不正确, 请使用[IP数据库自助添加](#)功能进行修正

87 7.915538 111.13.29.202 192.168.199.208 TCP 1514 443 → 52506 [ACK] Seq=3569 Ack=1585 Win=17920 Len=1460 [TCP segment of a reassembled PDU]

111.13.29.202 (北京市移动) → 192.168.199.208 (本机 IP) 接收数据

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:111.13.29.202

- 本站数据: 北京市北京市 移动
- 参考数据1: 北京北京 移动
- 参考数据2: 中国 移动

[idc公司大全](#) | [ip查询接口](#)

(3) 查看所在网络的网关 IP 地址,假设查到的 IP 地址是 a.b.c.d,在命令行窗口运行 ping -r 6 -l a.b.c.d 和

ping -s 4 -l a.b.c.d 命令并截获数据包。

无线局域网适配器 本地连接* 2:

```
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . : 
描述 . . . . . : Microsoft Wi-Fi Direct 虚拟适配器
物理地址. . . . . : 34-E6-AD-C2-4D-F5
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
```

无线局域网适配器 WLAN:

```
连接特定的 DNS 后缀 . . . . . : lan
描述 . . . . . : Intel(R) Dual Band Wireless-AC 3160
物理地址. . . . . : 34-E6-AD-C2-4D-F4
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::f577:f2f3:8812:3a83%13(首选)
IPv4 地址 . . . . . : 192.168.199.208(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2017年10月20日 12:24:07
租约过期的时间 . . . . . : 2017年10月21日 9:02:33
默认网关 . . . . . : 192.168.199.1
DHCP 服务器 . . . . . : 192.168.199.1
DHCPv6 IAID . . . . . : 137684653
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-1C-E7-E2-5D-F0-76-1C-B3-C0-1B
DNS 服务器 . . . . . : 192.168.199.1
TCP/IP 上的 NetBIOS . . . . . : 已启用
```



```
C:\Users\lee>ping -r 6 -l 192.168.199.1
必须指定 IP 地址。

C:\Users\lee>ping -r 6 -l 200 192.168.199.1

正在 Ping 192.168.199.1 具有 200 字节的数据:
来自 192.168.199.1 的回复: 字节=200 时间=6ms TTL=64
    路由: 192.168.199.1 ->
            192.168.199.1
来自 192.168.199.1 的回复: 字节=200 时间=14ms TTL=64
    路由: 192.168.199.1 ->
            192.168.199.1
来自 192.168.199.1 的回复: 字节=200 时间=1ms TTL=64
    路由: 192.168.199.1 ->
            192.168.199.1
来自 192.168.199.1 的回复: 字节=200 时间=7ms TTL=64
    路由: 192.168.199.1 ->
            192.168.199.1

192.168.199.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 14ms, 平均 = 7ms
```

```
C:\Users\lee>ping -s 4 -l 192.168.199.1
必须指定 IP 地址。

C:\Users\lee>ping -s 4 -l 200 192.168.199.1

正在 Ping 192.168.199.1 具有 200 字节的数据:
来自 192.168.199.1 的回复: 字节=200 时间=1ms TTL=64
    时间戳: 192.168.199.1 : 51279813 ->
            192.168.199.1 : 51279814 ->
            192.168.199.208 : 51279675
来自 192.168.199.1 的回复: 字节=200 时间=3ms TTL=64
    时间戳: 192.168.199.1 : 51280828 ->
            192.168.199.1 : 51280828 ->
            192.168.199.208 : 51280689
来自 192.168.199.1 的回复: 字节=200 时间=2ms TTL=64
    时间戳: 192.168.199.1 : 51281834 ->
            192.168.199.1 : 51281835 ->
            192.168.199.208 : 51281696
来自 192.168.199.1 的回复: 字节=200 时间=1ms TTL=64
    时间戳: 192.168.199.1 : 51282844 ->
            192.168.199.1 : 51282844 ->
            192.168.199.208 : 51282705

192.168.199.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 3ms, 平均 = 1ms
```



(4) 执行 filter : ip.addr == a.b.c.d 命令查看, 截屏运行结果。

235	12.247631	192.168.199.208	192.168.199.1	ICMP	74 Echo (ping) request	id=0x0001, seq=688/45058, ttl=64 (reply in 236)
236	12.248731	192.168.199.1	192.168.199.208	ICMP	74 Echo (ping) reply	id=0x0001, seq=688/45058, ttl=64 (request in 235)
246	13.249569	192.168.199.208	192.168.199.1	ICMP	74 Echo (ping) request	id=0x0001, seq=689/45314, ttl=64 (reply in 247)
247	13.251666	192.168.199.1	192.168.199.208	ICMP	74 Echo (ping) reply	id=0x0001, seq=689/45314, ttl=64 (request in 246)
263	14.251289	192.168.199.208	192.168.199.1	ICMP	74 Echo (ping) request	id=0x0001, seq=690/45570, ttl=64 (reply in 264)
264	14.255380	192.168.199.1	192.168.199.208	ICMP	74 Echo (ping) reply	id=0x0001, seq=690/45570, ttl=64 (request in 263)
276	15.252947	192.168.199.208	192.168.199.1	ICMP	74 Echo (ping) request	id=0x0001, seq=691/45826, ttl=64 (reply in 277)
277	15.255386	192.168.199.1	192.168.199.208	ICMP	74 Echo (ping) reply	id=0x0001, seq=691/45826, ttl=64 (request in 276)

(5) 截获的数据中都有哪些协议? 分别找出 Echo 和 Stamp 的请求和响应分组, 分析这些数据主要字段的含义。

有 DHCP 协议 (Dynamic Host Configuration Protocol, 动态主机配置协议)、SSDP 协议 (Simple Service Discovery Protocol, 简单服务发现协议)、ICMP 协议 (Internet Control Message Protocol, Internet 控制报文协议)。

Echo 和 Stamp 的请求和响应分组数据主要字段含义是:

Type: 类型字段(8 bits)

Code: 代码字段(8 bits)

Checksum: 校验和字段(16 bits)

Identifier: 用于标志本 ICMP 进程(16 bits)

Sequence number: 用于判断回显应答数据报(16 bits)

```
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4aa9 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 690 (0x02b2)
  Sequence number (LE): 45570 (0xb202)
  [Response frame: 264]
  > Data (32 bytes)
```

【实验思考】

(1) 捕获网络上的数据可谓轻而易举, 网络嗅探可以说无处不在, 如何发现网络中的嗅探行为?

可以开启本机进程, 查看进程状态来发现: 如果存在嗅探, 数据报无法每次都顺畅地流到目的地, 网络通信丢包率会反常高; 还可以查看网络带宽, 如果发现某台及其长时间的占用该网络较大的带宽, 其有可能在监听; 监视自己网络中的主机, 查看主机中的硬盘空间是否增长过快, CPU 资源是否消耗过多, 以及系统是否经常莫名其妙地



断网等等；这些措施都可以发现嗅探行为，当然还可以监视 DNS Reverse Lookups。

(2) 如何防范被嗅探？

在网络中布置入侵检测系统 (IDS) 或入侵防御系统 (IPS)，网络防火墙等安全设备；采取屏蔽无线信号方法，将超出使用范围的无线信号屏蔽；不管是局域网内部还是互联网传输都应该对传输的数据进行加密 (SSL、SSH、IPSEC、OPENVPN 等)，网络嗅探器对这些加密的数据无法进行正确的解码；尽量在网络中使用交换机和路由器；还可以在交换机中使用静态 MAC 地址与端口绑定功能，来防止 MAC 地址欺骗；使用 MAC 地址过滤，强制访问控制；

本次实验完成后，请根据组员在实验中的贡献，请实事求是，自评在实验中应得的分数。（按百分制）

学号	学生	自评分
15331151	李佳	100
15331150	李辉旭	98
15331143	黎皓斌	98

【交实验报告】

上传实验报告：<ftp://222.200.180.109/>

截止日期（不迟于）：1 周之内

上传包括两个文件：

(1) 小组实验报告。上传文件名格式：小组号_Ftp 协议分析实验.pdf （由组长负责上传）

例如：文件名“10_Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告

(2) 小组成员实验体会。每个同学单独交一份只填写了实验体会的实验报告。只需填写自己的学号和姓名。

文件名格式：小组号_学号_姓名_Ftp 协议分析实验.pdf （由组员自行上传）

例如：文件名“10_05373092_张三_Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告。

注意：不要打包上传！