



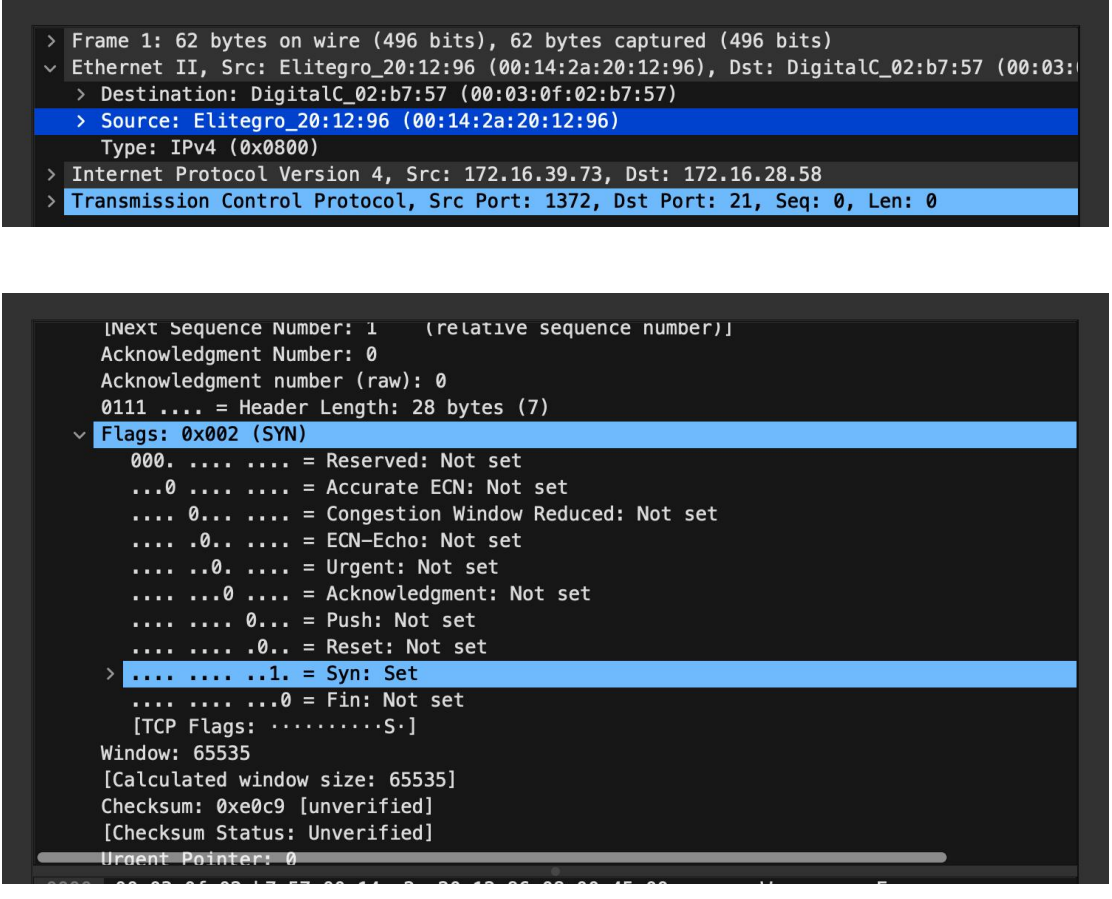
警

- 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	计算机学院	班 级	计科五班	组长	刘森元
学号	21307289	21307355	21307357		
学生	刘森元	黄梓宏	刘思昊		

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)

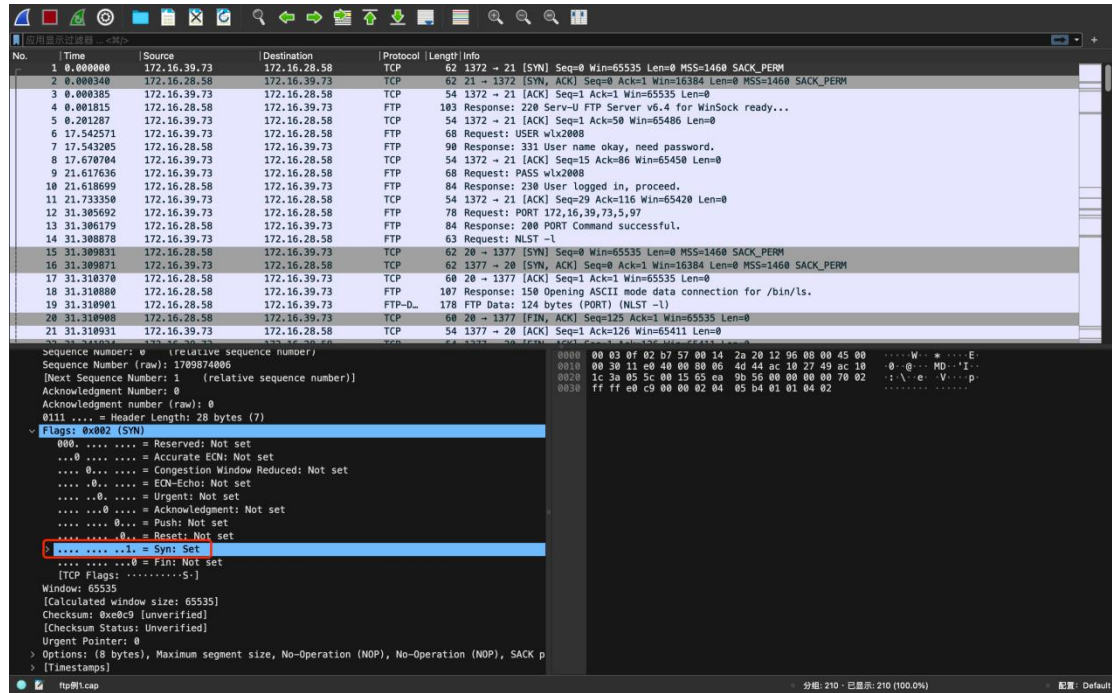
题号	
1	FTP 客户端的 mac 地址是多少?
答案	Source: Elitegro_20:12:96 (00:14:2a:20:12:96)
截图	
分析	该报文为 Client 到 Server 的第一次挥手报文，报文 Source 为 Client，Wireshark 中对应位置显示了 Client MAC 地址。
2	第 1、2、3 号报文的作用是什么?



答案

1. 第一个报文是客户端向服务器发送的 **SYN**（同步）报文。这个报文用于请求建立一个 **TCP** 连接。它包含了客户端的初始序列号和一些其他的控制信息。
2. 第二个报文是服务器向客户端发送的 **SYN-ACK**（同步-确认）报文。这个报文用于确认客户端的请求，并同意建立 **TCP** 连接。它包含了服务器的初始序列号、确认号以及一些其他的控制信息。
3. 第三个报文是客户端向服务器发送的 **ACK**（确认）报文。这个报文用于确认服务器的同意，并建立 **TCP** 连接。它包含了客户端的确认号和一些其他的控制信息。

截图





Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2854781995
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 1709874007
0111 = Header Length: 28 bytes (7)
Flags: 0x012 [SYN, ACK]
...0 = Reserved: Not set
...0 = Accurate ECN: Not set
...0 = Congestion Window Reduced: Not set
...0 = ECN-Echo: Not set
...0 = Urgent: Not set
...1 = Acknowledgment: Set
...0 = Push: Not set
...0 = Reset: Not set
...1 = Syn: Set
...0 = Fin: Not set
[TCP Flags:A..S]
Window: 16384
[Calculated window size: 16384]
Checksum: 0xe294 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (0 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK p
> [Timestamps]

Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1709874007
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 2854781995
0101 = Header Length: 28 bytes (5)
Flags: 0x010 (ACK)
...0 = Reserved: Not set
...0 = Accurate ECN: Not set
...0 = Congestion Window Reduced: Not set
...0 = ECN-Echo: Not set
...0 = Urgent: Not set
...1 = Acknowledgment: Set
...0 = Push: Not set
...0 = Reset: Not set
...0 = Syn: Not set
...0 = Fin: Not set
[TCP Flags:A....]
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x4f50 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]

分析

上述截图中使用红色方框标注出了各条报文的关键信息，其中 Sequence number / Acknowledgement number 的变化符合三次报文建立握手的变化。

3

该数据包中共有多少个 TCP 流？

答案

5 个。



截图

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.39.73	172.16.28.58	TCP	62	1372 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
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
15	31.308031	172.16.28.58	172.16.39.73	TCP	62	20 → 1377 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
16	31.308071	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
38	104.700804	172.16.28.58	172.16.39.73	TCP	62	20 → 1380 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
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
110	111.708415	172.16.28.58	172.16.39.73	TCP	62	20 → 1381 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
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
130	149.974062	172.16.28.58	172.16.39.73	TCP	62	20 → 1384 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
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

分析

通过过滤器规则“tcp.flags.syn == 1”可筛选出 TCP 三次握手报文的前两个，上图总共 10 个，即建立了 5 个 TCP 流。

4

用什么用户和密码登录成功？

答案

wlx2008; wlx2008

截图

No.	Time	Source	Destination	Protocol	Length	Info
4	0.001015	172.16.28.58	172.16.39.73	FTP	103	Response: 220 Serv-U FTP Server v6.4 for WinSock ready...
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.
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 Serv-U FTP Server v6.4 for WinSock ready...
12	31.305692	172.16.39.73	172.16.28.58	FTP	78	Request: PORT 172,16,39,73,5,97
13	31.306379	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
14	31.308870	172.16.39.73	172.16.28.58	FTP	63	Request: NLST -l
18	31.310800	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/l.
25	31.484083	172.16.28.58	172.16.39.73	FTP	182	Response: 226-Maximum disk quota limited to 307200 kBytes
27	42.200128	172.16.39.73	172.16.28.58	FTP	64	Request: MKD jji
28	42.201260	172.16.28.58	172.16.39.73	FTP	85	Response: 257 "/jji" directory created.
30	54.715458	172.16.39.73	172.16.28.58	FTP	64	Request: RNFR jji
31	54.716541	172.16.28.58	172.16.39.73	FTP	112	Response: 350 File or directory exists, ready for destination name
32	54.720019	172.16.39.73	172.16.28.58	FTP	64	Request: RNTO ppp
33	54.723253	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNTO command successful.
35	104.695575	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,100
36	104.696037	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
37	104.698520	172.16.39.73	172.16.28.58	FTP	73	Request: STOR xs2009-9.xls
41	104.701805	172.16.28.58	172.16.39.73	FTP	112	Response: 150 Opening ASCII mode data connection for xs2009-9.xls.
105	104.814922	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
107	111.703852	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,101
108	111.704411	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
109	111.707423	172.16.39.73	172.16.28.58	FTP	63	Request: NLST -l
113	111.709282	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/l.
120	111.822991	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
122	131.649709	172.16.39.73	172.16.28.58	FTP	73	Request: RNFR xs2009-9.xls
123	131.650613	172.16.28.58	172.16.39.73	FTP	112	Response: 350 File or directory exists, ready for destination name
124	131.654130	172.16.39.73	172.16.28.58	FTP	68	Request: RNTO 888.xls
125	131.657140	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNTO command successful.
127	149.968452	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,104
128	149.968908	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.

分析

通过过滤器规则“ftp”筛选出所有 FTP 报文，可见用户名和密码。

5

该 FTP 的命令连接和数据连接分别是什么样的连接？

答案

控制连接是持续连接，而数据连接是非持续连接。



计算机网络实验报告

截图

```
220 Serv-U FTP Server v6.4 for WinSock ready...
USER wlx2000
331 User name okay, need password.
PASS wlx2000
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 jji
257 "/jji" directory created.
RNFR jji
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!
```

No.	Time	Source	Destination	Protocol	Length	Info
35	104.695575	172.16.39.73	172.16.39.73	TCP	79	Request: PORT 172,16,39,73,5,100
36	104.696037	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
37	104.698520	172.16.39.73	172.16.28.58	FTP	73	Request: STOR xs2009-9.xls
41	104.701805	172.16.28.58	172.16.39.73	FTP	112	Response: 150 Opening ASCII mode data connection for xs2009-9.xls.
104	104.814541	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [ACK] Seq=136 Ack=534 Win=55002 Len=0
105	104.814922	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
106	105.017679	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [ACK] Seq=136 Ack=663 Win=64873 Len=0
107	111.703852	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,101
108	111.704411	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
109	111.704223	172.16.39.73	172.16.28.58	FTP	63	Request: NLST -l
113	111.709262	172.16.28.58	172.16.39.73	FTP	187	Response: 150 Opening ASCII mode data connection for /bin/ls.
119	111.822609	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [ACK] Seq=170 Ack=746 Win=64790 Len=0
120	111.822991	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
121	112.025742	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [ACK] Seq=170 Ack=875 Win=64661 Len=0
122	131.649709	172.16.39.73	172.16.28.58	FTP	73	Request: RNFR xs2009-9.xls
123	131.650613	172.16.28.58	172.16.39.73	FTP	112	Response: 350 File or directory exists, ready for destination name
124	131.654130	172.16.39.73	172.16.28.58	FTP	68	Request: RNTD 888.xls
125	131.657140	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNTD command successful.
126	131.831171	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [ACK] Seq=203 Ack=963 Win=64573 Len=0
127	149.968452	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,104
128	149.968988	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
129	149.972714	172.16.39.73	172.16.28.58	FTP	68	Request: RETR 888.xls
133	149.975126	172.16.28.58	172.16.39.73	TCP	121	Response: 150 Opening ASCII mode data connection for 888.xls (57856 Bytes).
202	150.113091	172.16.39.73	172.16.28.58	FTP	54	1372 -> 21 [ACK] Seq=242 Ack=1060 Win=64476 Len=0
203	150.113474	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
204	150.316222	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [ACK] Seq=242 Ack=1189 Win=64347 Len=0
205	160.024267	172.16.39.73	172.16.28.58	FTP	68	Request: QUIT
206	160.024673	172.16.28.58	172.16.39.73	FTP	68	Response: 221 Goodbye!
207	160.026301	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [FIN, ACK] Seq=248 Ack=1203 Win=64333 Len=0
208	160.026708	172.16.28.58	172.16.39.73	TCP	60	21 -> 1372 [ACK] Seq=1203 Ack=249 Win=65288 Len=0
209	160.026762	172.16.28.58	172.16.39.73	TCP	60	21 -> 1372 [FIN, ACK] Seq=1203 Ack=249 Win=65288 Len=0
210	160.026800	172.16.39.73	172.16.28.58	TCP	54	1372 -> 21 [ACK] Seq=249 Ack=1204 Win=64333 Len=0

Frame 41: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)

Ethernet II, Src: DigitalC_02:b7:57 (00:03:0f:02:b7:57), Dst: Elitegro_20:12:96 (00:14:2a:20:12:96)

Internet Protocol Version 4, Src: 172.16.28.58, Dst: 172.16.39.73

Transmission Control Protocol, Src Port: 21, Dst Port: 1372, Seq: 476, Ack: 136, Len: 58

Source Port: 21

Destination Port: 1372

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 58]

Sequence Number: 476 (relative sequence number)

Sequence Number (raw): 2054702471

[Next Sequence Number: 534 (relative sequence number)]

Acknowledgment Number: 136 (relative ack number)

Acknowledgment number (raw): 1709874142

分帧: 210 - 已显示: 08 (27%)

配置: Default



No.	Time	Source	Destination	Protocol	Length	Info
12	104.727934	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=23501 Win=65535 Len=0
73	104.727985	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
74	104.727990	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
75	104.727996	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
76	104.728215	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=26281 Win=65535 Len=0
77	104.728243	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
78	104.728249	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
79	104.728252	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
80	104.728497	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=29281 Win=65535 Len=0
81	104.728527	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
82	104.728533	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
83	104.728539	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
84	104.728777	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=32121 Win=65535 Len=0
85	104.728805	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
86	104.728811	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
87	104.728818	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
88	104.729859	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=35041 Win=65535 Len=0
89	104.729111	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
90	104.729117	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
91	104.729123	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
92	104.729341	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=37961 Win=65535 Len=0
93	104.729381	172.16.39.73	172.16.28.58	FTP-Data	1514	FTP Data: 1460 bytes (PORT) (STOR xs2009-9.xls)
94	104.729388	172.16.39.73	172.16.28.58	FTP-Data	970	FTP Data: 916 bytes (PORT) (STOR xs2009-9.xls)
95	104.729625	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=48881 Win=65535 Len=0
96	104.729987	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=43881 Win=65535 Len=0
97	104.730189	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=46721 Win=65535 Len=0
98	104.730466	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=49641 Win=65535 Len=0
99	104.730752	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=52561 Win=65535 Len=0
100	104.731037	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=55481 Win=65535 Len=0
101	104.731190	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [ACK] Seq=1 Ack=57858 Win=65535 Len=0
102	104.741612	172.16.28.58	172.16.39.73	TCP	60	20 → 1380 [FIN, ACK] Seq=1 Ack=57858 Win=65535 Len=0
103	104.741670	172.16.39.73	172.16.28.58	TCP	54	1380 → 20 [ACK] Seq=57858 Ack=2 Win=65535 Len=0

Frame 103: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Elliptigo_20:12:96 (00:14:2a:20:12:96), Dst: DigitalC_02:b7:57 (00:03:0f:02:02:b7:57)
Internet Protocol Version 4, Src: 172.16.39.73, Dst: 172.16.28.58
Transmission Control Protocol, Src Port: 1380, Dst Port: 20, Seq: 57858, Ack: 2, Len: 0
Source Port: 1380
Destination Port: 20
[Stream index: 2]
[Conversation completeness: Incomplete (30)]
[TCP Segment Len: 0]
Sequence Number: 57858 (relative sequence number)
Sequence Number (raw): 4238752345
[Next Sequence Number: 57858 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 4123825198

分析

通过过滤器规则“tcp.stream eq xx”筛选以及追踪流功能，可以分别得到命令链接和数据链接的报文，可见命令链接从服务开始到服务结束一直保持，而数据链接仅在传输任务时保持。

6

该 FTP 的连接模式是那种？为什么？

答案

主动模式，客户端向服务器发送 IP 地址和端口号，服务器主动连接客户端进行数据传输

No.	Time	Source	Destination	Protocol	Length	Info
4	0.001815	172.16.28.58	172.16.39.73	FTP	103	Response: 220 Serv-U FTP Server v6.4 for WinSock ready...
6	17.542571	172.16.39.73	172.16.28.58	FTP	68	Request: USER wlx2008
7	17.543285	172.16.28.58	172.16.39.73	FTP	90	Response: 331 User name okay, need password.
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	64	Response: 230 User logged in, proceed.
12	31.305692	172.16.39.73	172.16.28.58	FTP	78	Request: PORT 172,16,39,73,5,97
13	31.306179	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
14	31.308078	172.16.39.73	172.16.28.58	FTP	63	Request: NLST -l
18	31.318880	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
25	31.484083	172.16.28.58	172.16.39.73	FTP	182	Response: 226-Maximum disk quota limited to 307200 kBytes
27	42.200128	172.16.39.73	172.16.28.58	FTP	64	Request: MKD jjj
28	42.201268	172.16.28.58	172.16.39.73	FTP	85	Response: 257 "/jjj" directory created.
30	54.715458	172.16.39.73	172.16.28.58	FTP	64	Request: RNFR jjj
31	54.716541	172.16.28.58	172.16.39.73	FTP	112	Response: 350 File or directory exists, ready for destination name
32	54.720019	172.16.39.73	172.16.28.58	FTP	64	Request: RNTO ppp
33	54.723253	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNTO command successful.
35	104.695575	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,100
36	104.696037	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
37	104.698520	172.16.39.73	172.16.28.58	FTP	73	Request: STOR xs2009-9.xls
41	104.701885	172.16.28.58	172.16.39.73	FTP	112	Response: 150 Opening ASCII mode data connection for xs2009-9.xls.
105	104.814922	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
107	111.703852	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,101
108	111.704411	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
109	111.707423	172.16.39.73	172.16.28.58	FTP	63	Request: NLST -l
113	111.709282	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
120	111.822991	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
122	131.649709	172.16.39.73	172.16.28.58	FTP	73	Request: RNFR xs2009-9.xls
123	131.650613	172.16.28.58	172.16.39.73	FTP	112	Response: 350 File or directory exists, ready for destination name
124	131.654130	172.16.39.73	172.16.28.58	FTP	68	Request: RNTO 888.xls
125	131.657140	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNTO command successful.
127	149.968452	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,104
128	149.968900	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.

截图

分析

见途中选中条目 Info

7

最后四个报文的作用是什么？

答案

最后四个报文称为四次挥手。这四个报文的作用如下：

1. 第一个报文：主动关闭方发送的 FIN 报文（FIN = 1，ACK = 0）。这个报文表示主动关



闭方已经完成了数据的发送，并请求关闭连接。

2. 第二个报文：被动关闭方发送的 ACK 报文 (FIN = 0, ACK = 1)。这个报文是对第一个报文的确认，表示被动关闭方已经收到了关闭请求。

3. 第三个报文：被动关闭方发送的 FIN 报文 (FIN = 1, ACK = 0)。这个报文表示被动关闭方也已经完成了数据的发送，并请求关闭连接。

4. 第四个报文：主动关闭方发送的 ACK 报文 (FIN = 0, ACK = 1)。这个报文是对第三个报文的确认，表示主动关闭方已经收到了被动关闭方的关闭请求。

截图

No.	Time	Source	Destination	Protocol	Length	Info
179	149.981898	172.16.39.73	172.16.39.73	TCP	54	1384 → 20 [ACK] Seq=1 Ack=48881 Win=65535 Len=0
180	149.981882	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
181	149.982016	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=42341 Win=65535 Len=0
182	149.982185	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
183	149.982240	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
184	149.982283	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=45261 Win=65535 Len=0
185	149.982371	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
186	149.982511	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
187	149.982550	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=48181 Win=65535 Len=0
188	149.982625	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
189	149.982674	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=49641 Win=65535 Len=0
190	149.982750	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
191	149.982876	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
192	149.982913	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=52561 Win=65535 Len=0
193	149.982997	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
194	149.983033	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=54021 Win=65535 Len=0
195	149.983121	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
196	149.983246	172.16.28.58	172.16.39.73	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR 888.xls)
197	149.983277	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=56941 Win=65535 Len=0
198	149.983318	172.16.28.58	172.16.39.73	FTP-DATA	978	FTP Data: 916 bytes (PORT) (RETR 888.xls)
199	149.983346	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [ACK] Seq=1 Ack=57858 Win=64619 Len=0
200	150.016832	172.16.39.73	172.16.28.58	TCP	54	1384 → 20 [FIN, ACK] Seq=1 Ack=57858 Win=64619 Len=0
201	150.017147	172.16.28.58	172.16.39.73	TCP	60	20 → 1384 [ACK] Seq=57858 Ack=2 Win=65535 Len=0
202	150.113891	172.16.39.73	172.16.28.58	TCP	54	1372 → 21 [ACK] Seq=242 Ack=1060 Win=64476 Len=0
203	150.113474	172.16.28.58	172.16.39.73	FTP	183	Response: 228-Maximum disk quota limited to 307200 kBytes
204	150.316222	172.16.39.73	172.16.28.58	TCP	54	1372 → 21 [ACK] Seq=242 Ack=1189 Win=64347 Len=0
205	168.024267	172.16.39.73	172.16.28.58	FTP	60	Request: QUIT
206	168.024673	172.16.28.58	172.16.39.73	FTP	68	Response: 221 Goodbye!
207	168.026381	172.16.39.73	172.16.28.58	TCP	54	1372 → 21 [FIN, ACK] Seq=248 Ack=1203 Win=64333 Len=0
208	168.026708	172.16.28.58	172.16.39.73	TCP	60	21 → 1372 [ACK] Seq=1203 Ack=249 Win=65288 Len=0
209	168.026762	172.16.28.58	172.16.39.73	TCP	60	21 → 1372 [FIN, ACK] Seq=1203 Ack=249 Win=65288 Len=0
210	168.026800	172.16.39.73	172.16.28.58	TCP	54	1372 → 21 [ACK] Seq=249 Ack=1204 Win=64333 Len=0

分析

上述截图中使用红色方框标注出了各条报文的关键信息，其中 FIN / ACK 的变化符合四次报文挥手的变化。

8

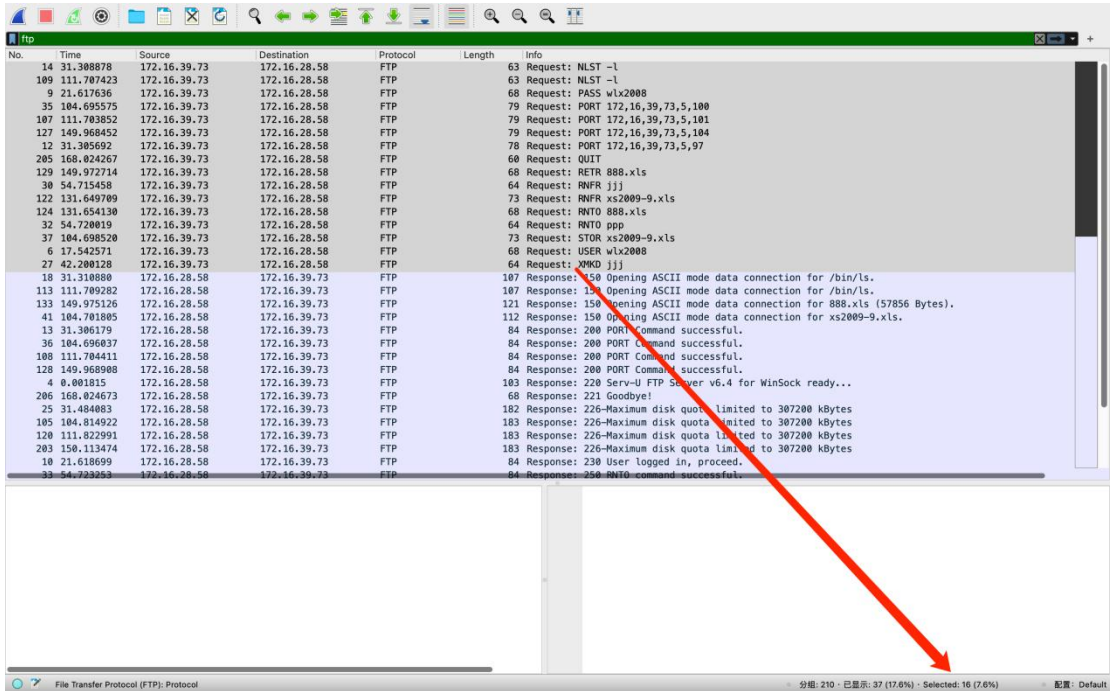
该数据包中有多少个 ftp 的命令及应答，其含义分别是什么？

答案

16 条 Request, 21 条 Response

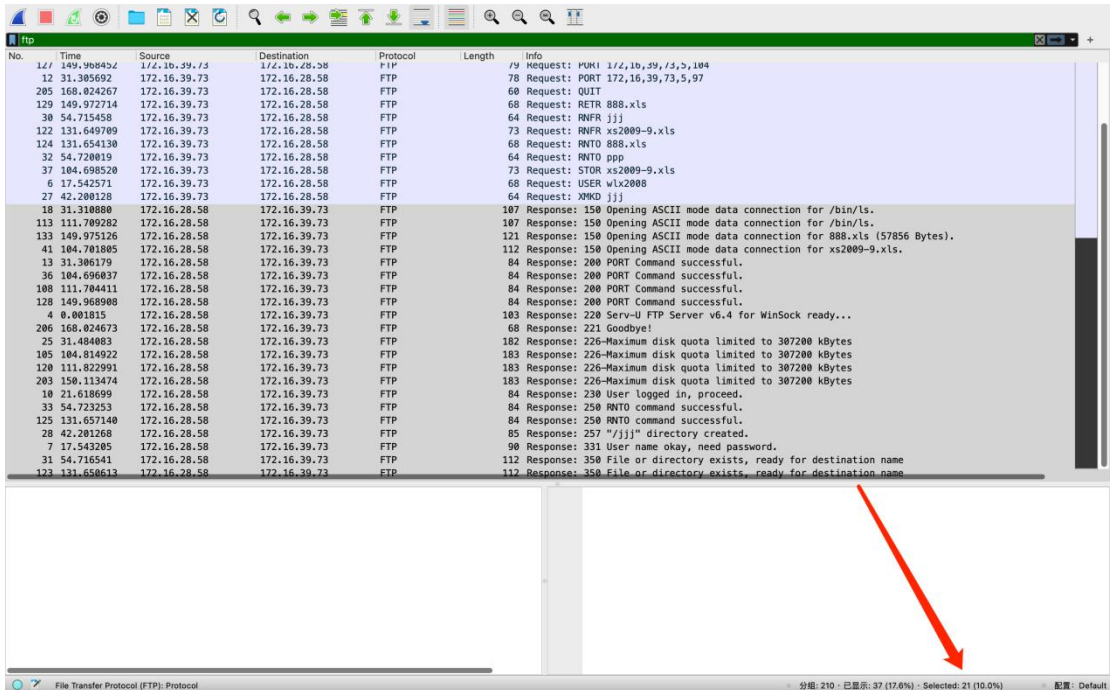


计算机网络实验报告



No.	Time	Source	Destination	Protocol	Length	Info
14	31.308878	172.16.39.73	172.16.28.58	FTP	63	Request: NLST -l
109	111.707423	172.16.39.73	172.16.28.58	FTP	63	Request: NLST -l
9	21.617636	172.16.39.73	172.16.28.58	FTP	68	Request: PASS wlx2008
35	104.695575	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,100
107	111.703852	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,101
127	149.968452	172.16.39.73	172.16.28.58	FTP	79	Request: PORT 172,16,39,73,5,104
12	31.305692	172.16.39.73	172.16.28.58	FTP	78	Request: PORT 172,16,39,73,5,97
205	168.024267	172.16.39.73	172.16.28.58	FTP	60	Request: QUIT
129	149.972714	172.16.39.73	172.16.28.58	FTP	68	Request: RETR 888.xls
38	54.715458	172.16.39.73	172.16.28.58	FTP	64	Request: RNFR jjj
122	131.649709	172.16.39.73	172.16.28.58	FTP	73	Request: RNFR xs2009-9.xls
124	131.654130	172.16.39.73	172.16.28.58	FTP	68	Request: RETR 888.xls
32	54.720019	172.16.39.73	172.16.28.58	FTP	64	Request: RNT0 ppp
37	104.698520	172.16.39.73	172.16.28.58	FTP	73	Request: STOR xs2009-9.xls
6	17.542571	172.16.39.73	172.16.28.58	FTP	68	Request: USER wlx2008
27	42.200128	172.16.39.73	172.16.28.58	FTP	64	Request: XMKD jjj
18	31.310880	172.16.39.73	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
113	111.709282	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
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).
41	104.701805	172.16.28.58	172.16.39.73	FTP	112	Response: 150 Opening ASCII mode data connection for xs2009-9.xls.
13	31.306179	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
36	104.696837	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
108	111.704411	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
128	149.968908	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
4	0.001815	172.16.28.58	172.16.39.73	FTP	103	Response: 220 Serv-U FTP Server v6.4 for WinSock ready...
206	168.024673	172.16.28.58	172.16.39.73	FTP	68	Response: 221 Goodbye!
25	31.484083	172.16.28.58	172.16.39.73	FTP	182	Response: 226-Maximum disk quota limited to 307200 kBytes
105	104.814922	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
120	111.822991	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
203	150.113474	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
10	21.618699	172.16.28.58	172.16.39.73	FTP	84	Response: 230 User logged in, proceed.
33	54.723253	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNT0 command successful.

截图



No.	Time	Source	Destination	Protocol	Length	Info
147	149.968452	172.16.39.73	172.16.28.58	FTP	79	Request: PUKI 172,16,39,73,5,104
12	31.305692	172.16.39.73	172.16.28.58	FTP	78	Request: PORT 172,16,39,73,5,97
205	168.024267	172.16.39.73	172.16.28.58	FTP	60	Request: QUIT
129	149.972714	172.16.39.73	172.16.28.58	FTP	68	Request: RETR 888.xls
38	54.715458	172.16.39.73	172.16.28.58	FTP	64	Request: RNFR jjj
122	131.649709	172.16.39.73	172.16.28.58	FTP	73	Request: RNFR xs2009-9.xls
124	131.654130	172.16.39.73	172.16.28.58	FTP	68	Request: RETR 888.xls
32	54.720019	172.16.39.73	172.16.28.58	FTP	64	Request: RNT0 ppp
37	104.698520	172.16.39.73	172.16.28.58	FTP	73	Request: STOR xs2009-9.xls
6	17.542571	172.16.39.73	172.16.28.58	FTP	68	Request: USER wlx2008
27	42.200128	172.16.39.73	172.16.28.58	FTP	64	Request: XMKD jjj
18	31.310880	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
113	111.709282	172.16.28.58	172.16.39.73	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
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).
41	104.701805	172.16.28.58	172.16.39.73	FTP	112	Response: 150 Opening ASCII mode data connection for xs2009-9.xls.
13	31.306179	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
36	104.696837	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
108	111.704411	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
128	149.968908	172.16.28.58	172.16.39.73	FTP	84	Response: 200 PORT Command successful.
4	0.001815	172.16.28.58	172.16.39.73	FTP	103	Response: 220 Serv-U FTP Server v6.4 for WinSock ready...
206	168.024673	172.16.28.58	172.16.39.73	FTP	68	Response: 221 Goodbye!
25	31.484083	172.16.28.58	172.16.39.73	FTP	182	Response: 226-Maximum disk quota limited to 307200 kBytes
105	104.814922	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
120	111.822991	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
203	150.113474	172.16.28.58	172.16.39.73	FTP	183	Response: 226-Maximum disk quota limited to 307200 kBytes
10	21.618699	172.16.28.58	172.16.39.73	FTP	84	Response: 230 User logged in, proceed.
33	54.723253	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNT0 command successful.
125	131.657140	172.16.28.58	172.16.39.73	FTP	84	Response: 250 RNT0 command successful.
28	42.201268	172.16.28.58	172.16.39.73	FTP	85	Response: 257 "/jjj" directory created.
7	17.543205	172.16.28.58	172.16.39.73	FTP	90	Response: 331 User name okay, need password.
31	54.716541	172.16.28.58	172.16.39.73	FTP	112	Response: 350 File or directory exists, ready for destination name
123	131.650613	172.16.28.58	172.16.39.73	FTP	112	Response: 350 File or directory exists, ready for destination name



分析	
	<p>USER: 提交登录用户名</p> <p>PASS: 提交登录密码</p> <p>PORT: 请求传输端口</p> <p>NLST: 获取指定目录下的文件列表</p> <p>XMKD: 在 FTP 服务器上创建指定的目录</p> <p>RNFR: 指定要重命名的文件或目录的原始名称</p> <p>RNTO: 指定要重命名的文件或目录的新名称</p> <p>STOR: 指定要上传到服务器的文件</p> <p>RETR: 指定要从服务器下载的文件</p> <p>Response 含义与 Info 中具体内容相同。</p>

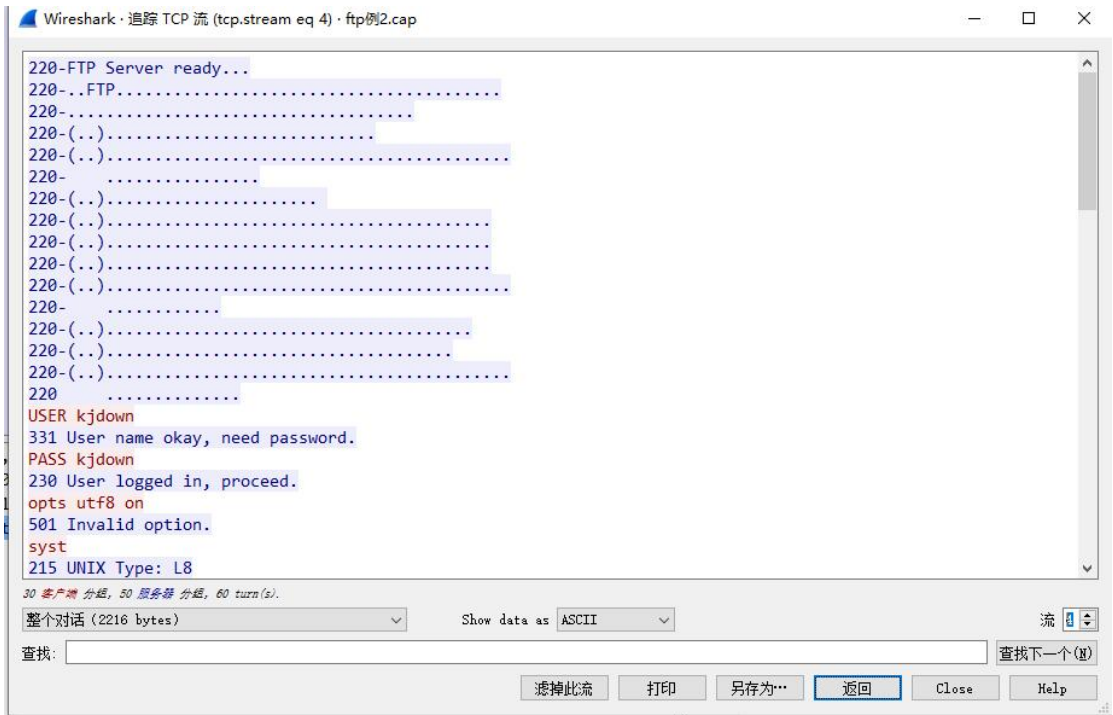
二、打开“FTP 数据包”的“ftp 例 2.cap”文件，进行观察分析，回答以下问题

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	服务器的 ip 地址: 172.16.3.240



	客户端的 mac 地址: 00:03:0f:02:b7:57
截图	<div><div><div>3 0.006731172.16.39.93172.16.3.240TCP62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM</div><div>4 0.009137172.16.3.240172.16.39.93TCP62 21 → 3995 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM</div><div>5 0.009192172.16.39.93172.16.3.240TCP54 3995 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0</div></div><div>Ethernet II, Src: Elitegro_20:12:96 (00:14:2a:20:12:96), Dst: DigitalC_02:b7:57 (00:03:0f:02:b7:57) > Destination: DigitalC_02:b7:57 (00:03:0f:02:b7:57) v Source: Elitegro_20:12:96 (00:14:2a:20:12:96) Address: Elitegro_20:12:96 (00:14:2a:20:12:96) 0. = LG bit: Globally unique address (factory default) 0 = IG bit: Individual address (unicast) Type: IPv4 (0x0800)</div></div>
分析	根据 TCP 协议三次握手的规律，对应的就是第 3，4，5 号报文。以第 3 号报文为例，source 即为客户端，destination 即为服务器端，对应查询 ip 地址或者 mac 地址即可。
2	该数据包中共有多少个 TCP 流？
答案	9 个
截图	<div><div>Wireshark · 追踪 TCP 流 (tcp.stream eq 8) · ftp例2.cap</div><div><div>.Q.~...R.~...^.....f.~S.H.A.P.E.~...~.~.~.M.E.R.G.E.F.O.R.M.A.T.~..... ..1.....B1..... ...1... ~.</div></div></div>

截图



分析

在工具中查找出来的最后的尝试登陆信息存在于 TCP 流 4 中，对应的用户名和密码如上。

4

该 FTP 的命令连接和数据连接分别是什么?

答案

命令连接是长连接，数据连接是短连接。

截图

[illegible]

图 4.1



计算机网络实验报告

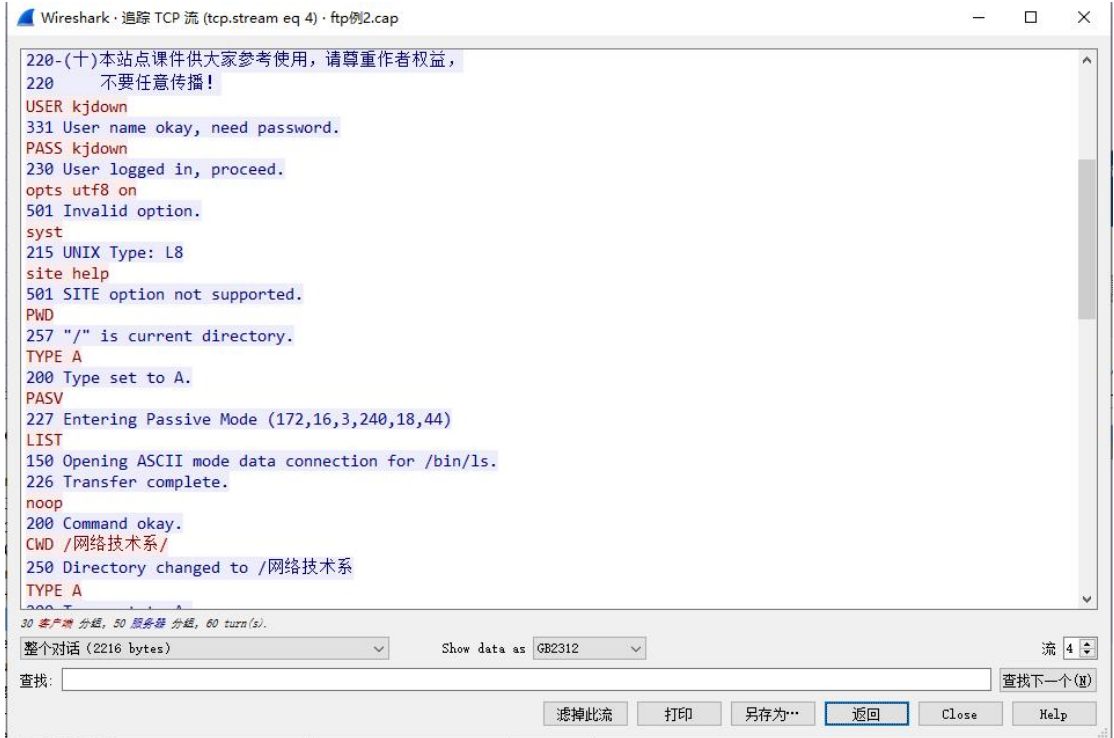


图 4.2

628	535.247202	172.16.39.93	172.16.3.240	TCP	54 1454 → 21 [ACK] Seq=375 Ack=1843 Win=65161 Len=0
629	565.983884	172.16.39.93	172.16.3.240	TCP	54 1454 → 21 [FIN, ACK] Seq=375 Ack=1843 Win=65161 Len=0
630	565.988017	172.16.3.240	172.16.39.93	TCP	60 21 → 1454 [ACK] Seq=1843 Ack=376 Win=65161 Len=0
631	566.203149	172.16.3.240	172.16.39.93	TCP	60 21 → 1454 [FIN, ACK] Seq=1843 Ack=376 Win=65161 Len=0
632	566.203215	172.16.39.93	172.16.3.240	TCP	54 1454 → 21 [ACK] Seq=376 Ack=1844 Win=65161 Len=0

图 4.3

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
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
230	403.312346	172.16.39.93	172.16.3.240	TCP	54 1654 → 4652 [ACK] Seq=1 Ack=1 Win=65535 Len=0
234	403.660506	172.16.3.240	172.16.39.93	FTP-DATA	1514 FTP Data: 1460 bytes (PASV) (LIST)
235	403.660543	172.16.3.240	172.16.39.93	FTP-DATA	110 FTP Data: 56 bytes (PASV) (LIST)
236	403.660592	172.16.39.93	172.16.3.240	TCP	54 1654 → 4652 [ACK] Seq=1 Ack=1517 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

图 4.4

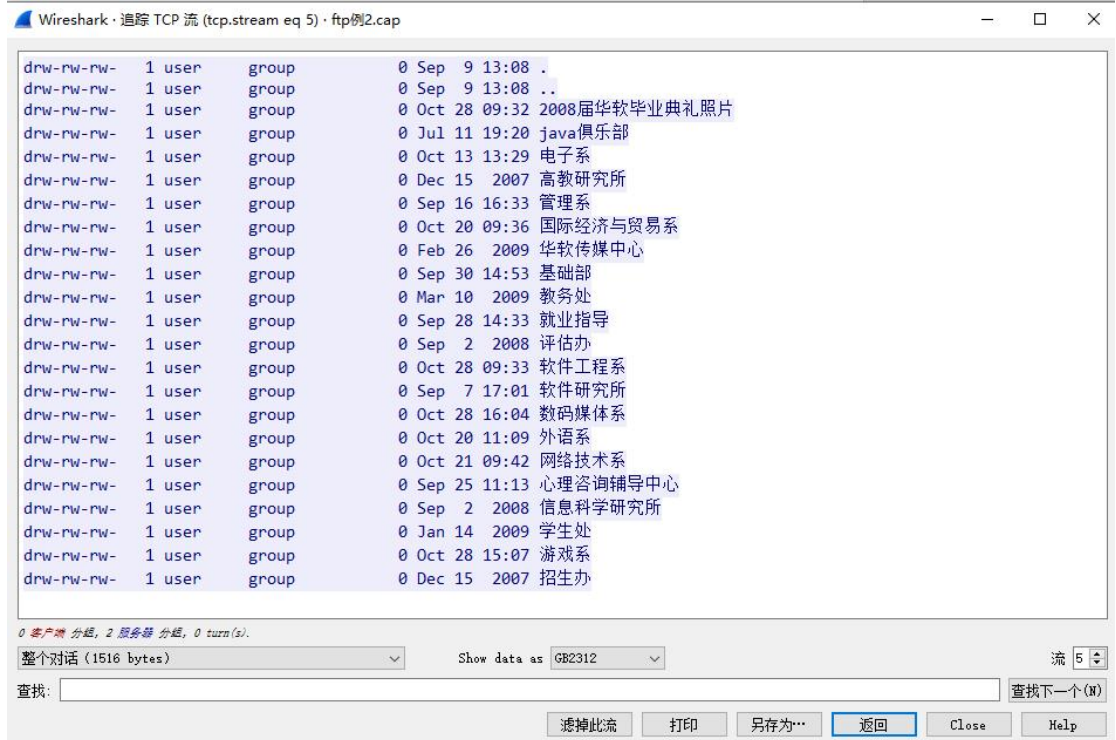


图 4.5

分析

命令连接用于传输控制指令，不涉及数据传输，通常由客户端随机端口向服务器 21 号端口发起连接请求，如下图 4.1 和图 4.2。可以看到控制指令包括验证 ftp 客户端身份的 USER 和 PASS 命令；指定文件传输类型的 TYPE 命令——此处将传输的文件说明为 ASCII 类型；进入被动连接的 PASV 命令。最后，参见图 4.3，该 TCP 控制连接在第 629-632 号报文终止。从该 TCP 连接的开始到结束，包含了 TCP 流（数据连接）5-8，所以命令连接是一个长连接。

数据连接用于传输数据。如果建立的是主动 FTP，那么数据连接应该是由服务器端使用 20 号端口主动向客户端随机端口发起数据连接的请求，然后开始上传和下载文件；如果建立的是被动 FTP，那么数据连接是由客户端发起的，而且客户端和服务端所使用的端口号都是随机选定的，服务器端不再指定 20 号端口。

以 TCP 流 5（图 4.4）为例，过程为简单的三次握手，建立连接，然后传输一个文件（见图 4.5），最后进行四次挥手，断开连接。TCP 流 6，7，8 均类似，被包括在 TCP 流 4 的报文中间，所以说数据连接是短连接。

5 哪几个报文是 FTP 数据连接的三次握手报文？

答案

5: 228-230

6: 256-258

7: 286-288

8: 324-326



计算机网络实验报告

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
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
230 403.312346	172.16.39.93	172.16.3.240	TCP	54 1654 → 4652 [ACK] Seq=1 Ack=1 Win=65535 Len=0

图 5.1

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
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
258 439.360876	172.16.39.93	172.16.3.240	TCP	54 1791 → 1137 [ACK] Seq=1 Ack=1 Win=65535 Len=0

图 5.2

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
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
288 476.228669	172.16.39.93	172.16.3.240	TCP	54 1934 → 1587 [ACK] Seq=1 Ack=1 Win=65535 Len=0

图 5.3

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
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
326 519.353959	172.16.39.93	172.16.3.240	TCP	54 2097 → 2118 [ACK] Seq=1 Ack=1 Win=65535 Len=0

图 5.4

分析

三次握手分别是[SYN], [SYN, ACK], [ACK]。

数据连接为 5-8 号 TCP 流，对应查找即可。

6

哪几个报文是 FTP 数据连接的挥手报文（结束报文）？

答案

5: 237-240

6: 270-273

7: 293-297

8: 620-623

截图

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

图 6.1

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

图 6.2

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
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

图 6.3



	<table><tr><td>620</td><td>534.787848</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60</td><td>2118 → 2097 [FIN, ACK] Seq=239105 Ack=1 Win=65535 Len=0</td></tr><tr><td>621</td><td>534.787917</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54</td><td>2097 → 2118 [ACK] Seq=1 Ack=239106 Win=65535 Len=0</td></tr><tr><td>622</td><td>534.788371</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54</td><td>2097 → 2118 [FIN, ACK] Seq=1 Ack=239106 Win=65535 Len=0</td></tr><tr><td>623</td><td>534.789817</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60</td><td>2118 → 2097 [ACK] Seq=239106 Ack=2 Win=65535 Len=0</td></tr></table>	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
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																							
	图 6.4																												
分析	四次挥手分别是[FIN, ACK], [ACK], [FIN, ACK]和[ACK], 对应在数据连接的 TCP 流中查询即可。																												
7	该 FTP 的连接模式是那种? 为什么?																												
答案	被动连接。因为在数据连接中, 服务器端的端口号并不指定为 20, 而是随机分配的端口号; 而且在控制连接中, 也有显示进入被动模式的 PASV 命令。																												
截图	<table><tr><td>324</td><td>519.351289</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>62</td><td>2097 → 2118 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM</td></tr><tr><td>325</td><td>519.353919</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>62</td><td>2118 → 2097 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM</td></tr><tr><td>326</td><td>519.353959</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54</td><td>2097 → 2118 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td></tr></table> <p>图 7.1</p>	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	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	326	519.353959	172.16.39.93	172.16.3.240	TCP	54	2097 → 2118 [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																							
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																							
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	以图 7.1 为例, 可以发现客户端和服务器端的端口号都是随机分配的。 以图 7.2 为例, 有 PASV 命令。																												

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。

实验步骤

(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。这时捕获的数据量有多少?

答: 片刻的时间内, 1s 内大概捕获了十几个包, 每个包的均值大概在 100bytes 左右。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::32cf:516d:b738:77ec	ff02::2	ICMPv6	70	Router Solicitation from 10:82:d7:dc:f5:66
2	0.005278	172.26.124.138	123.206.4.34	TLSv1.2	251	Application Data
3	0.067550	123.206.4.34	172.26.124.138	TLSv1.2	235	Application Data
4	0.067553	123.206.4.34	172.26.124.138	TLSv1.2	92	Application Data
5	0.067760	172.26.124.138	123.206.4.34	TCP	54	57164 → 443 [ACK] Seq=198 Ack=220 Win=4092 Len=0
6	0.200564	172.26.97.14	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
7	0.309899	c2:76:f6:89:80:b8	Broadcast	ARP	56	Who has 172.26.127.254? Tell 172.26.102.228
8	0.615302	92:54:11:db:d1:c4	Broadcast	ARP	56	Who has 172.26.127.254? Tell 172.26.113.173
9	0.711840	b2:6e:60:f2:13:90	Broadcast	ARP	56	Who has 172.26.127.254? Tell 172.26.28.204
10	0.848887	172.26.124.138	120.233.47.193	TCP	54	65451 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
11	0.874113	120.233.47.193	172.26.124.138	TCP	60	[TCP ACKed unseen segment] 443 → 65451 [ACK] Seq=1 Ack=2 Win=565
12	0.903709	172.26.124.138	120.226.166.151	TCP	54	65189 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
13	0.929698	120.226.166.151	172.26.124.138	TCP	60	[TCP ACKed unseen segment] 443 → 65189 [ACK] Seq=1 Ack=2 Win=501
14	1.019799	IntelCor_54:9d:e5	Broadcast	ARP	56	Who has 172.26.39.123? Tell 172.26.106.42
15	1.122139	172.26.97.14	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16	1.299012	172.26.124.138	120.233.184.160	TCP	54	65028 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
17	1.316996	120.233.184.160	172.26.124.138	TCP	60	[TCP ACKed unseen segment] 443 → 65028 [ACK] Seq=1 Ack=2 Win=72
18	1.327877	22:c9:24:2b:e4:86	Broadcast	ARP	56	Who has 172.26.127.254? Tell 172.26.53.151
19	1.429364	Guangdon_df:66:c3	Broadcast	ARP	56	Who has 172.26.127.254? Tell 172.26.39.189
20	1.429365	c2:40:31:c9:3c:3d	Broadcast	ARP	56	Who has 172.26.127.254? Tell 172.26.8.187
21	1.841207	IntelCor_f2:0c:4c	Broadcast	ARP	56	Who has 172.26.34.149? (ARP Probe)
22	1.841208	::	ff02::1:ff37:79c4	ICMPv6	78	Neighbor Solicitation for fe80::2e:158e:5c37:79c4



计算机网络实验报告

(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](http://www.ip138.com) 查询这些 IP 地址的地理位置。

答： 源 IP 地址是 172.26.124.138 目的 ip 地址是 123.206.4.34,是发送过去， 通过网站 www. ip138.com 可查询到 172.26.124.138 的地理位置在广东省广州市，也就是本机的网络 ip 地址，而 123.206.4.34 的地理位置位于天津市。

ipshudi.com

IP地址	123.206.4.34
归属地	中国 天津市
运营商	腾讯云
IP类型	数据中心

(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,在命令窗口运行

ping-+6-1a.b.c.d 和 ping-s 4 -1a. b.c.d 命令并捕获数据包。

```
lsh@lshdeMacBook-Air ~ % ping -s 100 172.26.127.254
PING 172.26.127.254 (172.26.127.254): 100 data bytes
108 bytes from 172.26.127.254: icmp_seq=0 ttl=64 time=5.548 ms
108 bytes from 172.26.127.254: icmp_seq=1 ttl=64 time=8.738 ms
108 bytes from 172.26.127.254: icmp_seq=2 ttl=64 time=5.098 ms
108 bytes from 172.26.127.254: icmp_seq=3 ttl=64 time=14.301 ms
108 bytes from 172.26.127.254: icmp_seq=4 ttl=64 time=12.187 ms
108 bytes from 172.26.127.254: icmp_seq=5 ttl=64 time=4.298 ms
108 bytes from 172.26.127.254: icmp_seq=6 ttl=64 time=10.437 ms
108 bytes from 172.26.127.254: icmp_seq=7 ttl=64 time=9.235 ms
108 bytes from 172.26.127.254: icmp_seq=8 ttl=64 time=4.826 ms
108 bytes from 172.26.127.254: icmp_seq=9 ttl=64 time=14.885 ms
108 bytes from 172.26.127.254: icmp_seq=10 ttl=64 time=12.968 ms
108 bytes from 172.26.127.254: icmp_seq=11 ttl=64 time=11.087 ms
108 bytes from 172.26.127.254: icmp_seq=12 ttl=64 time=9.976 ms
108 bytes from 172.26.127.254: icmp_seq=13 ttl=64 time=11.388 ms
108 bytes from 172.26.127.254: icmp_seq=14 ttl=64 time=4.925 ms
108 bytes from 172.26.127.254: icmp_seq=15 ttl=64 time=9.767 ms
108 bytes from 172.26.127.254: icmp_seq=16 ttl=64 time=5.302 ms
108 bytes from 172.26.127.254: icmp_seq=17 ttl=64 time=4.995 ms
108 bytes from 172.26.127.254: icmp_seq=18 ttl=64 time=5.203 ms
108 bytes from 172.26.127.254: icmp_seq=19 ttl=64 time=10.842 ms
^C
--- 172.26.127.254 ping statistics ---
20 packets transmitted, 20 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.298/8.800/14.885/3.409 ms
```

答:



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

答:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.26.124.138	172.26.127.254	ICMP	142	Echo (ping) request id=0x7b24, seq=10/2560, ttl=64 (reply in 2)
2	0.004014	172.26.127.254	172.26.124.138	ICMP	142	Echo (ping) reply id=0x7b24, seq=10/2560, ttl=64 (request in 1)
9	0.691656	172.26.124.138	223.6.6.6	TCP	54	54232 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
10	0.710686	223.6.6.6	172.26.124.138	TCP	66	[TCP ACKed unseen segment] 443 → 54232 [ACK] Seq=1 Ack=2 Win=23 Len=0
11	0.731698	223.6.6.6	172.26.124.138	TCP	66	[TCP Keep-Alive] 443 → 54232 [ACK] Seq=0 Ack=2 Win=23 Len=0 TSval=
12	0.731882	172.26.124.138	223.6.6.6	TCP	66	[TCP Previous segment not captured] 54232 → 443 [ACK] Seq=2 Ack=1
13	0.796916	172.26.124.138	120.53.53.53	TCP	54	59452 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
15	0.839328	120.53.53.53	172.26.124.138	TCP	60	[TCP ACKed unseen segment] 443 → 59452 [ACK] Seq=1 Ack=2 Win=501 Len=0
18	0.941211	183.240.222.156	172.26.124.138	TCP	66	50003 → 59563 [ACK] Seq=1 Ack=1 Win=32 Len=0 TSval=1304706000 TSe
19	0.941414	172.26.124.138	183.240.222.156	TCP	66	[TCP ACKed unseen segment] 59563 → 50003 [ACK] Seq=1 Ack=2 Win=20
20	1.005182	172.26.124.138	172.26.127.254	ICMP	142	Echo (ping) request id=0x7b24, seq=11/2816, ttl=64 (reply in 21)
21	1.009683	172.26.127.254	172.26.124.138	ICMP	142	Echo (ping) reply id=0x7b24, seq=11/2816, ttl=64 (request in 2)
24	1.430703	172.26.124.138	112.53.48.195	TCP	78	54719 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=49229
28	1.453987	112.53.48.195	172.26.124.138	TCP	66	80 → 54719 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1424 SACK_P
29	1.454204	172.26.124.138	112.53.48.195	TCP	54	54719 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
30	1.455312	172.26.124.138	112.53.48.195	HTTP	810	POST /mmtls/1497ad89 HTTP/1.1
31	1.470587	112.53.48.195	172.26.124.138	TCP	60	80 → 54719 [ACK] Seq=1 Ack=757 Win=64128 Len=0
32	1.521630	112.53.48.195	172.26.124.138	HTTP	367	HTTP/1.1 200 OK
33	1.521631	112.53.48.195	172.26.124.138	TCP	60	80 → 54719 [FIN, ACK] Seq=314 Ack=757 Win=64128 Len=0
34	1.521749	172.26.124.138	112.53.48.195	TCP	54	54719 → 80 [ACK] Seq=757 Ack=314 Win=261824 Len=0
35	1.521813	172.26.124.138	112.53.48.195	TCP	54	54719 → 80 [ACK] Seq=757 Ack=315 Win=261824 Len=0
36	1.522844	172.26.124.138	112.53.48.195	TCP	54	54719 → 80 [FIN, ACK] Seq=757 Ack=315 Win=262144 Len=0
37	1.538918	112.53.48.195	172.26.124.138	TCP	60	80 → 54719 [ACK] Seq=315 Ack=758 Win=64128 Len=0
44	2.008015	172.26.124.138	172.26.127.254	ICMP	142	Echo (ping) request id=0x7b24, seq=12/3072, ttl=64 (reply in 45)
45	2.018155	172.26.127.254	172.26.124.138	ICMP	142	Echo (ping) reply id=0x7b24, seq=12/3072, ttl=64 (request in 4)
58	3.010972	172.26.124.138	172.26.127.254	ICMP	142	Echo (ping) request id=0x7b24, seq=13/3328, ttl=64 (reply in 59)
59	3.018709	172.26.127.254	172.26.124.138	ICMP	142	Echo (ping) reply id=0x7b24, seq=13/3328, ttl=64 (request in 5)
85	4.014679	172.26.124.138	172.26.127.254	ICMP	142	Echo (ping) request id=0x7b24, seq=14/3584, ttl=64 (reply in 86)
86	4.025909	172.26.127.254	172.26.124.138	ICMP	142	Echo (ping) reply id=0x7b24, seq=14/3584, ttl=64 (request in 8)
101	4.771782	172.26.124.138	120.232.130.46	SSL	171	Continuation Data
102	4.803351	120.232.130.46	172.26.124.138	SSL	134	Continuation Data

(5) 捕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，分析此数据主要字段的含义。

答：捕获的数据中有 icmp tcp http ssl 协议。

ICMP Echo 请求和响应分组 (Ping)：

请求分组 (Ping 请求)：

Type (类型)：8 位字段，8，表示这是一个 ICMP Echo 请求消息。

Code (代码)：8 位字段，0，表示这是一个标准的 Echo 请求。

Checksum (校验和)：16 位字段，用于检测数据包的完整性。

Identifier (标识符)：16 位字段，用于将请求与响应配对。

Sequence Number (序列号)：16 位字段，用于将请求与响应配对。

Data (数据)：包含一些数据，用零填充。

响应分组 (Ping 响应)：

Type (类型)：8 位字段，0，表示这是一个 ICMP Echo 响应消息。

Code (代码)：8 位字段，0，表示这是一个标准的 Echo 响应。



计算机网络实验报告

Checksum (校验和) : 16 位字段, 用于检测数据包的完整性。

Identifier (标识符) : 16 位字段, 与请求中的标识符匹配, 用于配对请求和响应。

Sequence Number (序列号) : 16 位字段, 与请求中的序列号匹配, 用于配对请求和响应。

Data (数据) : 通常包含与请求相同的数据。

Time Stamp 请求分组 (Time Stamp 请求) :

Type (类型) : 8 位字段, 13, 表示这是一个 ICMP Time Stamp 请求消息。

Code (代码) : 8 位字段, 0, 表示这是一个标准的 Time Stamp 请求。

Checksum (校验和) : 16 位字段, 用于检测数据包的完整性。

Identifier (标识符) : 16 位字段, 用于将请求与响应配对。

Sequence Number (序列号) : 16 位字段, 用于将请求与响应配对。

Originate Timestamp (发起时间戳) : 64 位字段, 表示发送请求的时间戳。

Receive Timestamp (接收时间戳) : 64 位字段, 为 0 (在请求中), 接收响应时由接收端填充。

Transmit Timestamp (传输时间戳) : 64 位字段, 为 0 (在请求中), 接收响应时由接收端填充。

Time Stamp 响应分组 (Time Stamp 响应) :

Type (类型) : 8 位字段, 通常为 14, 表示这是一个 ICMP Time Stamp 响应消息。

Code (代码) : 8 位字段, 通常为 0, 表示这是一个标准的 Time Stamp 响应。

Checksum (校验和) : 16 位字段, 用于检测数据包的完整性。

Identifier (标识符) : 16 位字段, 与请求中的标识符匹配, 用于配对请求和响应。

Sequence Number (序列号) : 16 位字段, 与请求中的序列号匹配, 用于配对请求和响应。

Originate Timestamp (发起时间戳) : 64 位字段, 与请求中的时间戳相同。

Receive Timestamp (接收时间戳) : 64 位字段, 由接收端填充, 表示接收到请求的时间。

Transmit Timestamp (传输时间戳) : 64 位字段, 由接收端填充, 表示响应的时间。++

```
> Frame 14: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface en0, id 0
> Ethernet II, Src: Apple_15:73:72 (3c:a6:f6:15:73:72), Dst: RuijieNe_9f:46:87 (00:74:9c:9f:46:87)
> Internet Protocol Version 4, Src: 172.26.124.138, Dst: 172.26.127.254
> Internet Control Message Protocol
```

```
> Frame 15: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface en0, id 0
> Ethernet II, Src: RuijieNe_9f:46:87 (00:74:9c:9f:46:87), Dst: Apple_15:73:72 (3c:a6:f6:15:73:72)
> Internet Protocol Version 4, Src: 172.26.127.254, Dst: 172.26.124.138
> Internet Control Message Protocol
```

思考题:

(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?

2) 如何防范被嗅探?



答:

发现网络中的嗅探行为:

使用加密传输协议: 使用加密传输协议 (如 HTTPS、SSH、TLS 等) 来保护数据通信, 使得网络嗅探者难以直接获取敏感信息。这会使拦截的数据变得无用。

网络流量监控: 使用网络流量监控工具来监视网络活动, 检测异常流量或嗅探尝试。这些工具可以识别不寻常的流量模式或数据截取。

入侵检测系统 (IDS): 部署 IDS 来监测潜在的入侵行为, 包括嗅探攻击。IDS 可以检测到嗅探工具的活动和异常网络行为。

审计日志: 启用网络设备和服务器的审计日志, 以便跟踪和分析网络活动。审计日志可以用于检测潜在的嗅探行为。

流量分析: 使用流量分析工具, 如 Wireshark, 检查网络流量以查找异常或可疑的数据截取活动。

防范被嗅探:

使用加密通信: 始终使用加密协议来传输敏感数据, 以确保即使数据被截取, 也难以解密。

虚拟专用网络 (VPN): 使用 VPN 来加密整个网络连接, 以保护数据免受嗅探。VPN 将流量隧道化, 使其不容易被拦截。

防火墙和入侵检测系统: 使用防火墙和 IDS 来检测和阻止嗅探尝试。这些设备可以识别并应对潜在的攻击行为。

安全配置: 定期更新和加固网络设备和操作系统, 以减少潜在的嗅探漏洞。

物理安全: 确保物理访问控制, 防止未经授权的人员访问网络设备和数据线缆。

教育和培训: 培训员工和用户, 教育他们有关网络安全最佳实践, 以避免不慎泄露敏感信息。

总之, 发现网络中的嗅探行为需要监控和分析网络流量, 而防范被嗅探则需要使用加密、安全设备和最佳实践来保护数据免受嗅探攻击。网络安全是一个持续的努力, 需要综合的方法来确保网络的安全性和隐私保护。

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
21307289	刘森元	95
21307355	黄梓宏	97
21307357	刘思晏	96

【交实验报告】

上传实验报告: <ftp://172.26.49.141> 截止日期 (不迟于): 1 周之内

邮件标题格式: 组长学号_组员学号_组员姓名_Ftp 协议分析实验

文件格式: pdf (不要压缩包) 上传包括两个文件:



计算机网络实验报告

- (1) 小组实验报告。文件名格式：组长学号_Ftp 协议分析实验.pdf （由组长负责发送）
例如：文件名“20111001_Ftp 协议分析实验.pdf”表示 20111001 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。
文件名格式：组长学号_组员学号_组员姓名_Ftp 协议分析实验.pdf （由组员自行发送）
例如：文件名“20111001_05373092_张三_Ftp 协议分析实验.pdf”表示 20111001 组的 Ftp 协议分析实验报告。