



- 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	<u> 计科 1 班</u>		组长	郝裕玮
学号	<u>18329015</u>	18325071		<u>19335153</u>		
学生	<u>郝裕玮</u>	<u>张闯</u>		马淙升		

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	<pre>Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) ✓ 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) ➤ Source: Elitegro_20:12:96 (00:14:2a:20:12:96) Type: IPv4 (0x0800) ➤ Internet Protocol Version 4, Src: 172.16.39.73, Dst: 172.16.28.58 ➤ Transmission Control Protocol, Src Port: 1372, Dst Port: 21, Seq: 0, Len: 0</pre>								
分析	根据框中划线信息即可确定 FTP 客户端(即 source)的 mac 地址								
2	第 1、2、3 号报文的作用是什么?								
答案	1-3 号报文代表 3 次握手,使得客户端和服务端建立连接。 1-3 号报文的作用见分析。								
截图	No. Time Source Destination Protocol Length Info								
分析	3 0.000385 172.16.39.73 172.16.28.58 TCP 54 1372 + 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0								



中山大學 い 以AT-SEN UNIVERSITY 计算机网络实验报告

3	该数据包中共有多少个 TCP 流?
答案	共有 5 个 TCP 流
截图	Mark/Utomark Packet(s)
分析	利用追踪流中的 TCP 流选项即可统计出共多少条 TCP 流,同时利用 tcp.stream eq 指令也可验证 TCP 流的序号为 0-4.没有 5,即共 5 条 TCP 流(同时该文件中也正好只有 5 次握手,与TCP 流数量相等)
4	用什么用户和密码登录成功?
答案	用户:wlx2008 密码:wlx2008
截图	Length Info 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	根据 Info 即可确认用户和密码
5	该 FTP 的命令连接和数据连接分别是什么样的连接?
答案	命令连接: 传输用户名和密码的连接(服务器端口为 21 的连接)



中山大學 计算机网络实验报告
数据连接: 传输用户名和密码的连接之后 (即用户 wlx2008 登陆成功之后) 的连接都是数据连

	接(客户端端	台口为 20 的连接)		
	(tcp. flags. syn ==	1 or tcp.ack == 1)and tcp.f	flags.fin==0 and tcp and !ftp an	d !ftp-data	X → v
	No. Time	Source	Destination	Protocol Le	ngth Info
	1 0.000000 2 0.000340	172.16.39.73 172.16.28.58	172.16.28.58 172.16.39.73	TCP TCP	62 1372 + 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 21 + 1372 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
	3 0.000385	172.16.39.73	172.16.28.58	TCP	54 1372 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0
	15 31.309831 16 31.309871	172.16.28.58 172.16.39.73	172.16.39.73 172.16.28.58	TCP TCP	62 20 → 1377 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 1377 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PER
截图	17 31.310370	172.16.28.58 172.16.28.58	172.16.39.73	TCP	60 20 → 1377 [ACK] Seq=1 Ack=1 Win=65535 Len=0
	38 104.700884 39 104.700924	172.16.39.73	172.16.39.73 172.16.28.58	TCP TCP	62 20 → 1380 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 1380 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PER
	40 104.701226 110 111.708415	172.16.28.58 172.16.28.58	172.16.39.73 172.16.39.73	TCP TCP	60 20 → 1380 [ACK] Seq=1 Ack=1 Win=65535 Len=0 62 20 → 1381 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK PERM=1
	111 111.708455 112 111.708976	172.16.39.73 172.16.28.58	172.16.28.58 172.16.39.73	TCP	62 1381 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PER
	130 149.974062	172.16.28.58	172.16.39.73	TCP TCP	60 20 + 1381 [ACK] Seq=1 Ack=1 Win=65535 Len=0 62 20 + 1384 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
	131 149.974102 132 149.974406	172.16.39.73 172.16.28.58	172.16.28.58 172.16.39.73	TCP TCP	62 1384 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERI 60 20 → 1384 [ACK] Seq=1 Ack=1 Win=65535 Len=0
	通过过滤器可			条件可翻译为	
					E确认值 ACK) 并且同时 FIN==(
		_			手的数据包。并根据用户 wlx20
			连接和数据连接。	12 1 113 1/1/12	2 1 H 3 3 V H C 3 7 IV W H / II / V W C 3
分析	00 豆木成为	即加水区为明マ	全 该种数加定该。		
	命令连接: N	o.1-3;			
	数据连接: N	o.15-17,No.38	3-40,No.110-112	,No.130-13	32;
6	该 FTP 的连拉	接模式是哪种? ラ	为什么?		
答案	主动模式,因	为使用了 PORT	命令和固定端口 2	1.	
截图	11 21.733350	172.16.39.73	172.16.28.58	TCP	54 1372 → 21 [ACK] Seq=29 Ack=116 Win=65420 Len=
	12 31.305692	172.16.39.73	172.16.28.58	FTP	78 Request: PORT 172,16,39,73,5,97
分析	每次客户端需	言要接收数据时,	都会向服务器端的	21 端口发送	PORT 命令。
7	最后四个报文	工的作用是什么?			
	四次挥手, 使	[客户端与服务端	尚断开连接。		
答案					
	作用详见分析	Ī.			
	207 168.026381	172.16.39.73	172.16.28.58	TCP	54 1372 + 21 [FIN, ACK] Seq=248 Ack=1203 Win=64333 Len=
截图	208 168.026708 209 168.026762	172.16.28.58 172.16.28.58	172.16.39.73 172.16.39.73	TCP TCP	60 21 → 1372 [ACK] Seq=1203 Ack=249 Win=65288 Len=0 60 21 → 1372 [FIN, ACK] Seq=1203 Ack=249 Win=65288 Len=
	210 168.026800	172.16.39.73	172.16.28.58	TCP	54 1372 + 21 [ACK] Seq=249 Ack=1204 Win=64333 Len=0
	第一次挥手,	家户端发出连接			返回 FIN+ACK。
	N1 D(1+ 1:				ZH III MEN
	第二次挥手:	服务端收到 FIN	J 之后,会发送 AC	〈报文,此时	服务端处于 CLOSE_WAIT 状态
	210 2001 4	74674 114 12624	, , , , , , , , , , , , , , , , , , ,	- 4////	74654 1495 4 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -
分析	第三次挥手:	若服务端没有要	向客户端发出的数据	居,则服务端分	发出连接释放报文段(FIN+ACK)
24 1/1			后确认)状态,等待		
	7472 74 - Ind XT / X		中心性をおく 医が思り (社長)	· Ho - indeption (y • -
	第四次挥手:	客户端收到服务	端的连接释放报文	段后,对此发	t出确认报文段(ACK=1),客户



中山大學 SUN YAT-SEN UNIVERSITY 计算机网络实验报告

0011	时间 2MSL 后,客户端才进入 CLOSED 状态。
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	表数据包甲有多少个Ttp 的命令及应答、具含义分别是什么? 共 15 条命令及共应答: (1) NLST -l:返回指定路径下的目录列表,省略<路径>时,返回当前目录: (2) PASS wlx2008:向服务器发送密码 wlx2008; (3) PORT 172,16,39,73,5,100:主动模式,包含了客户端用什么端口接收数据; (4) PORT 172,16,39,73,5,101:与(3)相同; (5) PORT 172,16,39,73,5,104:与(3)相同; (6) PORT 172,16,39,73,5,97:与(3)相同; (7) QUIT:与服务端断开连接; (8) RETR 888.xls:下载文件(888.xls); (9) RNFR jjj;准备对文件名为jjj的文件进行重命名(只是指定需要改名的文件,但尚未修改,修改名字需要 RNTO命令来实现); (10) RNFR xs2009-9.xls:同(9); (11) RNTO 888.xls:和(10)相配对,将文件名改为888.xls; (12) RNTO ppp:和(9)相配对,将文件名改为ppp; (13) STOR xs2009-9.xls:上传文件xs2009-9.xls: (14) USER wlx2008:向服务器发送用户名 wlx2008; (15) XMKD jjj;在当前目录下建立"/jjj"文件夹
截图	母条命令的含义。 Request: USER wlx2008 Response: 331 User name okay, need password. Request: PORT 172,16,39,73,5,97 Response: 200 PORT Command successful. Request: PASS wlx2008 Response: 230 User logged in, proceed. Request: NLST -1 Response: 150 Opening ASCII mode data connection for /bin/ls. Response: 226-Maximum disk quota limited to 307200 kBytes



Request: XMKD jjj

Response: 257 "/jjj" directory created.

Request: RNTO ppp

Response: 250 RNTO command successful.

Request: STOR xs2009-9.xls

Response: 150 Opening ASCII mode data connection for xs2009-9.xls.

Response: 226-Maximum disk quota limited to 307200 kBytes

Request: NLST -1

Response: 150 Opening ASCII mode data connection for /bin/ls.

Response: 226-Maximum disk quota limited to 307200 kBytes

Request: RNTO 888.xls

Response: 250 RNTO command successful.

Request: RETR 888.xls

分析

Response: 150 Opening ASCII mode data connection for 888.xls (57856 Bytes).

Response: 226-Maximum disk quota limited to 307200 kBytes

Request: RNFR jjj

Response: 350 File or directory exists, ready for destination name

Request: PORT 172,16,39,73,5,100

Response: 200 PORT Command successful.

Request: PORT 172,16,39,73,5,101

Response: 200 PORT Command successful.

Request: RNFR xs2009-9.xls

Response: 350 File or directory exists, ready for destination name

Request: PORT 172,16,39,73,5,104

Response: 200 PORT Command successful.

Request: QUIT

Response: 221 Goodbye!

根据每条命令本身内容和对应的回应内容即可分析出其含义

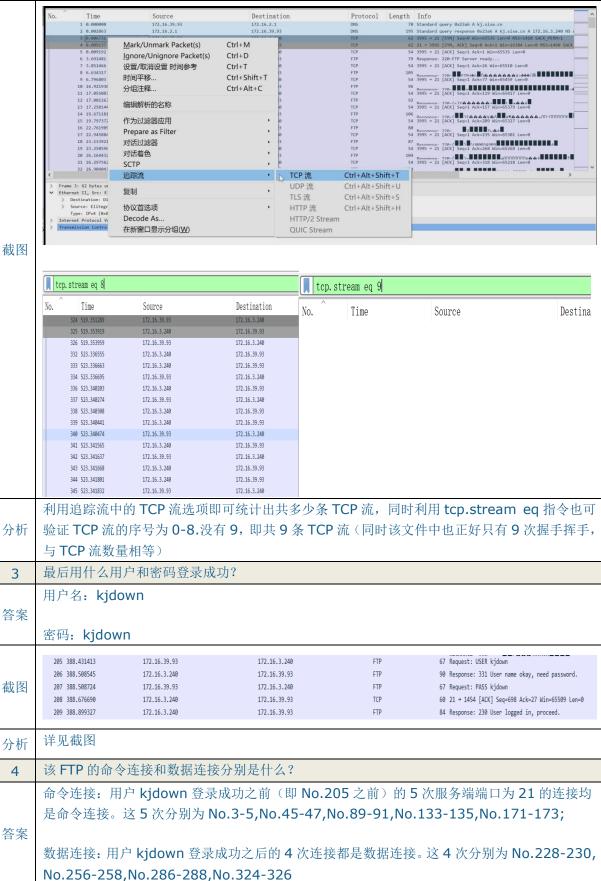
二、打开 "FTP 数据包"的 "ftp 例 2.cap"文件,进行观察分析,回答以下问题

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	<pre>> Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) V 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) > Source: Elitegro_20:12:96 (00:14:2a:20:12:96) Type: IPv4 (0x0800) > Internet Protocol Version 4, Src: 172.16.39.93, Dst: 172.16.3.240 > Transmission Control Protocol, Src Port: 3995, Dst Port: 21, Seq: 0, Len: 0</pre>
分析	详见截图
2	该数据包中共有多少个 TCP 流?
答案	共有 9 个 TCP 流



3

计算机网络实验报告





中山大學 SUN YAT-SEN UNIVERSITY 计算机网络实验报告

' I										
	205 388.431413 206 388.508545	172.16.39.93 172.16.3.240	172.16.3.240 172.16.39.93	FTP FTP	67 Request: USER kjdown 90 Response: 331 User name okay, need password.					
	207 388.508724	172.16.39.93	172.16.3.240	FTP	67 Request: PASS kjdown					
	208 388.676690 209 388.899327	172.16.3.240 172.16.3.240	172.16.39.93 172.16.39.93	TCP FTP	60 21 → 1454 [ACK] Seq=698 Ack=27 Win=65509 Len=0 84 Response: 230 User logged in, proceed.					
	(tep. flags. syn == 1 or tep. ack == 1) and tep. flags. fin == 0 and tep and !ftp and !ftp-data									
	No. Time	Source	Destination	Protocol Lengt	h Info					
	3 0.006731 4 0.009137	172.16.39.93 172.16.3.240	172.16.3.240 172.16.39.93	TCP TCP	62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 21 → 3995 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1					
	5 0.009192	172.16.39.93	172.16.3.240	TCP	54 3995 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
	45 54.561498 46 54.571096	172.16.39.93 172.16.3.240	172.16.3.240 172.16.39.93	TCP TCP	62 4218 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 21 → 4218 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1					
+1/1151	47 54.571162 89 177.671981	172.16.39.93 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP	54 4218 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0 62 4685 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1					
截图	90 177.672313 91 177.672367	172.16.3.240 172.16.39.93	172.16.39.93 172.16.3.240	TCP TCP	62 21 → 4685 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 54 4685 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
	133 267.933915 134 267.935597	172.16.39.93 172.16.3.240	172.16.3.240 172.16.39.93	TCP TCP	62 1132 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 21 → 1132 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1					
	135 267.935655 171 346.347532	172.16.39.93 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP	54 1132 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
	172 346.347757	172.16.3.240	172.16.39.93	TCP	62 1454 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 21 → 1454 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1					
	173 346.347811 228 403.311489	172.16.39.93 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP	54 1454 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0 62 1654 → 4652 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1					
	229 403.312292 230 403.312346	172.16.3.240 172.16.39.93	172.16.39.93 172.16.3.240	TCP TCP	62 4652 → 1654 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 54 1654 → 4652 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
	256 439.360533 257 439.360823	172.16.39.93 172.16.3.240	172.16.3.240 172.16.39.93	TCP TCP	62 1791 → 1137 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 62 1137 → 1791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1					
	258 439.360876 286 476.228404	172.16.39.93 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP	54 1791 → 1137 [ACK] Seq=1 Ack=1 Win=65535 Len=0 62 1934 → 1587 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1					
	287 476.228638 288 476.228669	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					
	324 519.351289	172.16.39.93 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP	54 1934 → 1587 [ACK] Seq=1 Ack=1 Win=65535 Len=0 62 2097 → 2118 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1					
	325 519.353919 326 519.353959	172.16.3.240 172.16.39.93	172.16.39.93 172.16.3.240	TCP TCP	62 2118 → 2097 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 54 2097 → 2118 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
	7岁7年7年6年11年11	计粉把与进行效	2.14. # 图 由 40.14.14.	夕 (中三) 新江文小	進山 TCD 社 沙中 CVN1 書					
	地 过过滤箱可	N	1. 越图中的过滤:	宋什り鮒 中八:	选出 TCP 协议中 SYN==1 或					
41 1-	者 Ack==1(Acknowledge	ment Number 确:	认编号,而非征	确认值 ACK) 并且同时 FIN==0					
分析		_								
	的数据也。这个	牛的数据包别走	找们而安的母伙连续	安中的二次维-	手的数据包。并根据用户 kjdown					
	登录成功前后	来区分命令连接	5和数据连接。							
_										
5	哪儿个报义是	FIP 剱据连接	的三次握手报文?							
答案	No.228-230	No.256-258,	No.286-288, No.3	324-326;						
H M				/						
	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 230 403.312346	172.16.3.240 172.16.39.93	172.16.39.93 172.16.3.240	TCP TCP TCP	62 4652 → 1654 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 54 1654 → 4652 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
	229 403.312292 230 403.312346 256 439.360533 257 439.360823	172.16.3.240 172.16.39.93 172.16.39.93 172.16.3.240	172.16.39.93 172.16.3.240 172.16.3.240 172.16.39.93	TCP TCP TCP	62 4652 + 1654 [SYM, ACK] Seq+0 Ack=1 Min-16384 Len+0 MSS=1460 SACK_PERM=1 54 1654 + 4652 [ACK] Seq=1 Ack=1 Min-55535 Len+0 62 1791 + 1137 [SYM] Seq=0 Min-55535 Len+0 MSS=1460 SACK_PERM=1 62 1137 + 1791 [SYM, ACK] Seq+0 Ack=1 Min-16384 Len+0 MSS=1460 SACK_PERM=1					
截图	229 403.312292 230 403.312346 256 439.360533 257 439.360823 258 439.360876 286 476.228404	172.16.3.240 172.16.39.93 172.16.39.93 172.16.3.240 172.16.39.93	172,16,39,93 172,16,32,40 172,16,3,240 172,16,39,93 172,16,3,240 172,16,3,240	TCP TCP TCP TCP TCP	82 4652 - 1654 [SYII, ACK] Sequé Acksi Niimi-16384 Lenné MSS-1466 SACK_PERH-1 54 1654 - 4652 [ACK] Sequé Acksi Niimi-65535 Lenné MSS-1466 SACK_PERH-1 62 1379 - 1137 [SYII] Sequé Niimi-65535 Lenné MSS-1466 SACK_PERH-1 62 1379 - 1379 [SYII, ACK] Sequé Acksi Niimi-16384 Lenné MSS-1466 SACK_PERH-1 62 1934 - 1387 [SYII] Sequé Niimi-65535 Lenné MSS-1466 SACK_PERH-1 62 1934 - 1387 [SYII] Sequé Niimi-65535 Lenné MSS-1466 SACK_PERH-1					
截图	229 483,312292 230 483,312346 256 439,366833 257 439,366823 258 439,366876 286 476,228404 287 476,22863 288 476,228669	172.16.3, 240 172.16.39.93 172.16.39.93 172.16.39.93 172.16.33.240 172.16.39.93 172.16.33.240 172.16.39.93	172.16.3, 249 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240	TCP TCP TCP TCP TCP TCP TCP TCP	82 4652 - 1654 (SYN, ACK) Sequé Acksi Nimin-16384 Lenné MSS-1460 SACK_PERHol 62 1791 + 1137 (SYN) Sequé Nimin-65355 Lenné 62 1791 + 1137 (SYN) Sequé Nimin-65355 Lenné MSS-1460 SACK_PERHol 62 1137 + 1791 (SYN, ACK) Sequé Acksi Nimin-16384 Lenné MSS-1460 SACK_PERHol 62 1137 + 1791 (TAK) Sequé Acksi Nimin-65356 Lenné MSS-1460 SACK_PERHol 62 1537 + 1537 (SYN) Sequé Nimin-65356 Lenné MSS-1460 SACK_PERHol 62 1537 + 1537 (ACK) Sequé Acksi Nimin-65386 Lenné MSS-1460 SACK_PERHol 63 1534 + 1537 (ACK) Sequé Acksi Nimin-65386 Lenné MSS-1460 SACK_PERHol 63 1534 + 1537 (ACK) Sequé Acksi Nimin-65386 Lenné MSS-1460 SACK_PERHol					
截图	229. 480, 312292 230. 483, 312246 256. 439, 36823 257. 439, 36823 258. 439, 36823 258. 439, 36823 288. 476, 228494 287. 476, 228699 324. 519, 351289 325. 519, 353129	172,16,3,246 172,16,39,93 172,16,39,93 172,16,33,246 172,16,39,93 172,16,39,93 172,16,39,93 172,16,39,93 172,16,39,93 172,16,39,93 172,16,34,46	172.16.3, 248 172.16.3, 248 172.16.3, 248 172.16.3, 248 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240	TCP	\$2. 4652 - 1654 (SYI), ACK Sequê Acks I Min-16384 Lenné MSS-1460 SACK_PERH-1 \$6. 1054 - 4652 (AKK) Sequê Acks I Min-16384 Lenné MSS-1460 SACK_PERH-1 \$62 1179 - 1137 (SYII) Sequê Min-16535 Lennê MSS-1460 SACK_PERH-1 \$62 1137 - 1137 (SYII) Sequê Acks I Min-16384 Lennê MSS-1460 SACK_PERH-1 \$61 1791 - 1137 (ACK) Sequê Acks I Min-16353 Lennê MSS-1460 SACK_PERH-1 \$62 1537 - 1934 (SYII) Sequê Min-16535 Lennê MSS-1460 SACK_PERH-1 \$63 1537 - 1934 (SYII) Sequê Min-16535 Lennê MSS-1460 SACK_PERH-1 \$62 1537 - 1934 (SYII) Sequê Min-16535 Lennê MSS-1460 SACK_PERH-1 \$62 2637 - 2138 (SYII) Sequê Min-16535 Lennê MSS-1460 SACK_PERH-1 \$62 2637 - 2138 (SYII) Sequê Min-16535 Lennê MSS-1460 SACK_PERH-1					
截图	229 483,312292 239 483,312246 256 489,369533 257 439,369823 258 439,369826 286 476,2228494 287 476,228638 288 476,228659 324 519,351289	172.16.3,240 172.16.39.93 172.16.39.93 172.16.3,240 172.16.3,240 172.16.3,240 172.16.3,240 172.16.3,240 172.16.39.93 172.16.39.93	172.16.3, 249 172.16.3, 240 172.16.3, 240 172.16.39.93 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240	TCP TCP TCP TCP TCP TCP TCP TCP TCP	\$2. 4652 - 1654 (SYI), ACK Sequê Acks Min-16384 Lenné MSS-1460 SACK_PERH-1 \$4. 1654 - 4652 (ACK Sequi Acks Min-16354 Lenné MSS-1460 SACK_PERH-1 \$4. 1374 (SYI) Sequê Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1379 - 1791 SYIN, ACK Sequê Acks Min-16355 Lenné MSS-1460 SACK_PERH-1 \$4. 1791 - 1137 (ACK) Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 SYIN Sequê Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 SYIN, ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK Sequê Acks Min-65535 Lenné MSS-1460 SACK_PERH-1 \$4. 1597 ACK					
截图	229 481,312292 239 481,312246 256 489,169513 257 439,360875 258 439,360876 268 476,224444 287 476,226583 288 476,226583 285 476,226583 225 519,353919 326 519,353959 326 519,353959	172.16.3.246 172.16.39.93 172.16.39.93 172.16.3.246 172.16.3.246 172.16.39.93 172.16.32.93 172.16.32.93 172.16.32.93 172.16.32.93	172.16.3, 249 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240 172.16.3, 240	TCP	82 4052 - 1654 (SVI), ACK J Sequé Acks I Min-16384 Level MSS-1460 SACK_PERN-1 54 1054 - 4652 (ACK Sequi Acks I Min-65535 Level 00 00 00 00 00 00 00 00 00 00 00 00 00					
	29. 403.312392 230 403.312346 256 439.360533 257 439.36023 258 439.360276 286 476.228844 287 476.228843 288 476.228638 288 476.228638 328 519.353129 325 519.353129 326 519.353919	172.16.3.248 172.16.39.93 172.16.39.93 172.16.13.248 172.16.13.9.93 172.16.13.249 172.16.32.99 172.16.32.90 172.16.32.93 172.16.32.93 172.16.32.93 172.16.32.93	172.16.3,249 172.16.3,249 172.16.3,248 172.16.3,248 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249	TOP TOP TOP TOP TOP TOP TOP TOP	102 4052 - 1654 (SM), ACC J Sept Acks J Min-16384 Lend MSS-1406 SACK_PERHS 5 1654 + 4652 (AK) Segt Acks J Min-16535 Lenne MSS-1406 SACK_PERHS 62 1379 - 1791 (SM) Sept Him-05535 Lenne MSS-1406 SACK_PERHS 54 1379 - 1791 (SM), ACC Sept Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 1791 + 1137 (ACK) Segt Acks J Min-05535 Lenne MSS-1406 SACK_PERHS 62 1384 - 1587 (SM) Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1587 - 1934 (SM), ACC J Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (SM) Segt Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) SEGT ACKS J MIN-16555					
截图	29. 403.312392 230 403.312346 256 439.360533 257 439.36023 258 439.360276 286 476.228844 287 476.228843 288 476.228638 288 476.228638 328 519.353129 325 519.353129 326 519.353919	172.16.3.248 172.16.39.93 172.16.39.93 172.16.13.248 172.16.13.9.93 172.16.13.249 172.16.32.99 172.16.32.90 172.16.32.93 172.16.32.93 172.16.32.93 172.16.32.93	172.16.3,249 172.16.3,249 172.16.3,248 172.16.3,248 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249	TOP TOP TOP TOP TOP TOP TOP TOP	82 4052 - 1654 (SVI), ACK J Sequé Acks I Min-16384 Level MSS-1460 SACK_PERN-1 54 1054 - 4652 (ACK Sequi Acks I Min-65535 Level 00 00 00 00 00 00 00 00 00 00 00 00 00					
分析	29. 483.33292 286 489.33236 287 489.366933 287 489.366923 284 489.366926 284 476.228688 282 476.228689 284 519.351289 385 519.351289 385 519.351999 利用 4 的过滤 是数据连接。	172.16.3.288 172.16.19.93 172.16.3.288 172.16.3.288 172.16.3.9.93 172.16.39.93 172.16.39.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 条件和截图结号	122.16.3.249 122.16.3.249 122.16.3.249 122.16.3.9.93 172.16.3.249 122.16.3.9.93 172.16.3.249 122.16.3.249 121.16.3.249 121.16.3.249	TO T	102 4052 - 1654 (SM), ACC J Sept Acks J Min-16384 Lend MSS-1406 SACK_PERHS 5 1654 + 4652 (AK) Segt Acks J Min-16535 Lenne MSS-1406 SACK_PERHS 62 1379 - 1791 (SM) Sept Him-05535 Lenne MSS-1406 SACK_PERHS 54 1379 - 1791 (SM), ACC Sept Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 1791 + 1137 (ACK) Segt Acks J Min-05535 Lenne MSS-1406 SACK_PERHS 62 1384 - 1587 (SM) Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1587 - 1934 (SM), ACC J Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (SM) Segt Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) SEGT ACKS J MIN-16555					
	29. 403.32296 29. 403.32246 29. 409.369533 257 403.360876 28. 439.360876 28. 476.228648 28. 476.228689 325 513.553919 326 519.553959 利用 4 的过滤 是数据连接。 哪几个报文是	172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.3248 172.16.39.93 172.16.3248 172.16.32.93 172.16.32.88 172.16.32.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93	172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 早即可得到本题答案 No.228-230,No.2	(即用户 kjdo 56-258,No.2 文)?	102 4052 - 1654 (SM), ACC J Sept Acks J Min-16384 Lend MSS-1406 SACK_PERHS 5 1654 + 4652 (AK) Segt Acks J Min-16535 Lenne MSS-1406 SACK_PERHS 62 1379 - 1791 (SM) Sept Him-05535 Lenne MSS-1406 SACK_PERHS 54 1379 - 1791 (SM), ACC Sept Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 1791 + 1137 (ACK) Segt Acks J Min-05535 Lenne MSS-1406 SACK_PERHS 62 1384 - 1587 (SM) Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1587 - 1934 (SM), ACC J Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (SM) Segt Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) SEGT ACKS J MIN-16555					
分析	29. 403.32296 29. 403.32246 29. 409.369533 257 403.360876 28. 439.360876 28. 476.228648 28. 476.228689 325 513.553919 326 519.553959 利用 4 的过滤 是数据连接。 哪几个报文是	172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.3248 172.16.39.93 172.16.3248 172.16.32.93 172.16.32.88 172.16.32.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93	122.16.3.249 122.16.3.249 122.16.3.249 122.16.3.9.93 172.16.3.249 122.16.3.9.93 172.16.3.249 122.16.3.249 121.16.3.249 121.16.3.249	(即用户 kjdo 56-258,No.2 文)?	102 4052 - 1654 (SM), ACC J Sept Acks J Min-16384 Lend MSS-1406 SACK_PERHS 5 1654 + 4652 (AK) Segt Acks J Min-16535 Lenne MSS-1406 SACK_PERHS 62 1379 - 1791 (SM) Sept Him-05535 Lenne MSS-1406 SACK_PERHS 54 1379 - 1791 (SM), ACC Sept Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 1791 + 1137 (ACK) Segt Acks J Min-05535 Lenne MSS-1406 SACK_PERHS 62 1384 - 1587 (SM) Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1587 - 1934 (SM), ACC J Sept Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 62 1034 - 1587 (ACK) Segt Acks J Min-16384 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (SM) Segt Acks J Min-16355 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2097 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) Segt Acks J Min-16555 Lenne MSS-1406 SACK_PERHS 54 2007 + 2118 (ACK) SEGT ACKS J MIN-16555					
分析	29. 403.32296 29. 403.32296 29. 403.32296 29. 403.360875 25. 439.360876 28. 476.22668 28. 476.22668 28. 476.22668 28. 476.22668 28. 476.22668 328 513.553919 326 513.553919 326 513.553919 326 513.553919 326 513.553919 326 513.553919 326 513.553919 326 513.553919 326 513.553919 326 513.553919	172.16.3.288 172.16.39.93 172.16.39.93 172.16.3.288 177.16.39.93 177.16.32.88 177.	172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 No.228-230,No.2 约挥手报文(结束报 No.293-297,No.6	(即用户 kjdo 56-258,No.2 文)?	122 4052 1554 (SM), ACK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1554 - 4652 (AKK) Sequé Acksi Minn-16351 Lemé) 162 1794 + 1137 (SM) Sequé Minn-6551 Lemé MSS-1460 SACK_PERN-1 SE 1379 + 1731 (SM) Sequé Minn-6551 Lemé MSS-1460 SACK_PERN-1 SE 1794 + 1137 (AKK) Sequé Acksi Minn-16358 Lemé MSS-1460 SACK_PERN-1 SE 1384 + 1587 (AKK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1384 + 1587 (AKK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1384 + 1587 (AKK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1394 - 1587 (AKK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1394 - 1587 (AKK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1394 - 1587 (AKK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (SM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (SM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (AKK) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1397 + 2118 (XM) Sequé Acksi Minn-16384 Lemé MSS-1460 SACK_P					
分析	29. 403.32296 29. 403.32246 29. 409.369533 257 403.360876 28. 439.360876 28. 476.228648 28. 476.228689 325 513.553919 326 519.553959 利用 4 的过滤 是数据连接。 哪几个报文是	172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.3248 172.16.39.93 172.16.3248 172.16.32.93 172.16.32.88 172.16.32.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93	172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 172.16.3,249 早即可得到本题答案 No.228-230,No.2	(即用户 kjdo 56-258,No.2 文)?	12 4622 - 1654 (SM), ACC J Sept Acks J Min-16384 Lend MSS-1466 SACK_PEBR-1 St 1654 + 6452 (AK) Segt Acks J Min-16535 Lenne MSS-1466 SACK_PEBR-1 St 1797 - 1137 (SM) Sept Him-65535 Lenne MSS-1466 SACK_PEBR-1 St 1797 + 1137 (AK) Segt Acks J Min-65535 Lenne MSS-1466 SACK_PEBR-1 St 1794 - 1137 (AK) Segt Acks J Min-65535 Lenne MSS-1466 SACK_PEBR-1 SQ 1384 - 1587 (SM) Sept Acks J Min-16384 Lenne MSS-1466 SACK_PEBR-1 SQ 1587 - 1934 (SM), ACC J Sept Acks J Min-16384 Lenne MSS-1466 SACK_PEBR-1 SQ 1384 - 1587 (AK) Segt Acks J Min-16384 Lenne MSS-1466 SACK_PEBR-1 SQ 1384 - 1587 (SM) Segt Acks J Min-16384 Lenne MSS-1466 SACK_PEBR-1 SQ 1384 - 1587 (SM), ACC Sept Acks J Min-16384 Lenne MSS-1466 SACK_PEBR-1 S4 2097 + 2118 (ACK) Segt Acks J Min-65535 Lenne MSS-1466 SACK_PEBR-1 S4 2097 + 2118 (ACK) Segt Acks J Min-65535 Lenne MSS-1466 SACK_PEBR-1					
分析	29. 403.33292 29. 403.33296 29. 403.3296 29. 403.300376 28. 439.360376 28. 476.22864 28. 476.22868 28. 476.22869 325 513.55393 326 513.55393 326 513.55393 326 513.55393 326 513.55393 326 513.55395 利用 4 的过滤 是数据连接。 哪几个报文是 No.237-240	172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.93 172.16.32.93 172.16.32.93	172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.240 No.228-230,No.2 内挥手报文(结束报 No.293-297,No.6	(即用户 kjdo 56-258,No.2 文)?	12 4652 + 1654 (SM), ACC) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$1654 - 4652 (AIK) Sequé Acks I limin-5353 Lemé MSS-1466 SACK_PERNAS \$2 1379 - 1791 (SM) Sequé Him-65535 Lemé MSS-1466 SACK_PERNAS \$4 1791 + 1137 (AIK) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$4 1791 + 1137 (AIK) Sequé Acks I limin-63535 Lemé MSS-1466 SACK_PERNAS \$2 1934 - 1587 (SM) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$1 1934 - 1587 (AIK) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$1 1934 - 1587 (AIK) Sequé Acks I limin-6353 Lemé MSS-1466 SACK_PERNAS \$4 1934 - 1587 (SM) Sequé Him-65535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé \$4 2865 LEMÉ ALKS ALKS BININ-65535 Lemé \$4 15654 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 Acks 1518 Nimin-6553					
分析	29. 403.332992 29. 403.33236 29. 409.36033 27. 409.360023 25. 409.360026 29. 475.228649 20. 475.228649 20. 519.353919 310. 519.353919 310. 519.353919 310. 519.353919 310. 519.353919 310. 519.353919 310. 519.353919 310. 519.353919	172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 条件和截图结身 这4次分别为【 FTP数据连接自 ,No.270-273,	172.16.3.9.93 172.16.3.240 172.16.3.240 172.16.3.93 172.16.3.93 172.16.3.99 172.16.3.99 172.16.3.99 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 No.228-230,No.2 的挥手报文(结束报 No.293-297,No.6	でで TOP TOP TOP TOP TOP TOP TOP TOP	122 4052 + 1654 (SM), ACK) Sequé Acks Minn-16384 Lemé MSS-1460 SACK_PERNAS \$1654 - 4652 (ACK) Sequé Acks Minn-16535 Lemé BC 1791 + 1137 (SM) Sequé Minn-65535 Lemé MSS-1460 SACK_PERNAS \$12379 + 1737 (SM) Sequé Minn-65536 Lemé MSS-1460 SACK_PERNAS \$1592 + 1137 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1582 1934 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$15934 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16535 Lemé \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé MSS-1460 SACK_PERNAS \$1034 + 1587 (ACK) Sequé Acks Minn-16536 Lemé \$1034 + 4652 (ACK) Sequé Acks Minn-16535 Lemé \$1034 + 4652 (ACK) Sequé Acks Minn-16535 Lemé \$1034 + 4652 (ACK) Sequé Acks Minn-16535 Lemé \$1034 + 4652 (ACK) Sequé Acks Minn-16536 Lemé \$1034 + 4652 (ACK) Sequé Ac					
分析	29. 403.33292 29. 403.33296 29. 403.3296 29. 403.300376 29. 439.300376 29. 476.22864 28. 476.22869 32. 513.55393 32. 513.5539 32. 513.553	172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.88 172.16.32.93 172.16.32.93 172.16.32.93	172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.240 No.228-230,No.2 内挥手报文(结束报 No.293-297,No.6	(即用户 kjdo 56-258,No.2 文)?	12 4652 + 1654 (SM), ACC) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$1654 - 4652 (AIK) Sequé Acks I limin-5353 Lemé MSS-1466 SACK_PERNAS \$2 1379 - 1791 (SM) Sequé Him-65535 Lemé MSS-1466 SACK_PERNAS \$4 1791 + 1137 (AIK) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$4 1791 + 1137 (AIK) Sequé Acks I limin-63535 Lemé MSS-1466 SACK_PERNAS \$2 1934 - 1587 (SM) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$1 1934 - 1587 (AIK) Sequé Acks I limin-16384 Lemé MSS-1466 SACK_PERNAS \$1 1934 - 1587 (AIK) Sequé Acks I limin-6353 Lemé MSS-1466 SACK_PERNAS \$4 1934 - 1587 (SM) Sequé Him-65535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé MSS-1466 SACK_PERNAS \$4 2997 + 2118 (AIK) Sequé Acks I limin-6535 Lemé \$4 2865 LEMÉ ALKS ALKS BININ-65535 Lemé \$4 15654 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 4 4652 [AIK], ACK] Sequé Acks 1518 Nimin-65535 Lemé \$4 1564 Acks 1518 Nimin-6553					
分析	29. 403.33299. 29. 403.33296. 29. 403.33296. 29. 409.36933. 25. 409.36923. 25. 409.36926. 28. 476.22658. 28. 476.22658. 28. 476.22658. 28. 25. 25. 25. 25. 25. 25. 25. 25. 25. 25	172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.30.88 172.16.30.88 172.16.30.88 172.16.30.88 172.16.30.93 172.16.30.88 172.16.30.93 172.16.30.93 172.16.30.93 172.16.30.93	172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249	でで TCP TCP TCP TCP TCP TCP (即用户 kjdc 56-258,No.2 文)? 520-623;	122 41622 + 1654 (SM), ACK) Sequé Acks Minn-16384 Lemél MSS-1460 SACK_PERNAT SE 1654 - 4652 (ACK) Sequé Acks Minn-5535 Lemél BC 1794 + 1137 (SM) Sequé Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1379 + 1217 (SM) Sequé Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1794 + 1137 (ACK) Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 1587 (ACK) Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 1587 (ACK) Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 1587 (ACK) Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 1587 (ACK) Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 1587 (ACK) Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 1587 (ACK) Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 2097 (SM), ACK] Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 2097 (SM), ACK] Sequé Acks Minn-5535 Lemél MSS-1460 SACK_PERNAT SE 1384 + 4652 (ACK) Sequé Acks Minn-5535 Lemél SE 1564 + 4652 (ACK) Sequé Acks Minn-5535 Lemél SE 1564 + 4652 (ACK) Sequé Acks Minn-5535 Lemél Ge 4652 + 1654 (ACK) Sequé Acks Minn-5535 Lemél Ge 4652 + 1654 (ACK) Sequé Acks Minn-55535 Lemél Ge 4652 + 1654 (ACK) Sequé Acks Minn-55535 Lemél Ge 4652 + 1654 (ACK) Sequé Acks Minn-55535 Lemél Ge 4652 + 1654 (ACK) Sequé Acks Minn-55535 Lemél Ge 4137 + 1791 [FIN, ACK] Seq-2992 Acks Minn-55535 Lemél Ge 1137 + 1791 [FIN, ACK] Seq-2992 Acks Minn-55535 Lemél					
分析	29. 403.33292 29. 403.33236 29. 403.33236 29. 403.06033 29. 403.260276 29. 475.226648 20. 475.226649 20. 513.35289 20. 513.35289 20. 513.353939 20. 513.353939 20. 513.353939 20. 513.353939 20. 513.353939 20. 513.353939 21. 403.746017 237. 403.735946 238. 403.736017 239. 403.736017 239. 403.736121 240. 403.741744	172.16.3.248 172.16.39.93 172.16.19.93 172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93	172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.293 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 No.228-230,No.2 的挥手报文(结束报 No.293-297,No.6	(即用户 kjdo 56-258,No.2 文)? 520-623;	12. 4652 ± 1654 (SM), ACK) Sequé Ackst Minn-16384 Lemé MSS-1460 SACK_PERN-1 SE 1054 ± 680.2 (AK) Sequé Ackst Minn-6353 Lemé (BSS-1460 SACK_PERN-1 SE 12137 ± 1217 (SM) Sequé Ninn-6553 Lemé MSS-1460 SACK_PERN-1 SE 12137 ± 1217 (JM), ACK) Sequé Ackst Minn-6353 Lemé MSS-1460 SACK_PERN-1 SE 12134 ± 1387 (JAK) Sequé Ackst Minn-6553 Lemé MSS-1460 SACK_PERN-1 SE 12134 ± 1387 (AK) Sequé Ackst Minn-6553 Lemé MSS-1460 SACK_PERN-1 SE 1234 ± 1387 (AK) Sequé Ackst Minn-6553 Lemé MSS-1460 SACK_PERN-1 SE 1234 ± 1387 (AK) Sequé Ackst Minn-6553 Lemé MSS-1460 SACK_PERN-1 SE 1234 ± 1387 (AK) Sequé Ackst Minn-6553 Lemé MSS-1460 SACK_PERN-1 SE 1234 ± 1387 (AK) Sequé Ackst Minn-6553 Lemé MSS-1460 SACK_PERN-1 SE 1234 ± 1287 (SM) Sequé NienéS535 Lemé MSS-1460 SACK_PERN-1 SE 1234 ± 1287 (AK) Sequé Ackst Minn-65535 Lemé MSS-1460 SACK_PERN-1 SE 1234 5 ± 1287 (AK) Sequé Ackst Minn-65535 Lemé MSS-1460 SACK_PERN-1 SE 1234 5 ± 1287 (AK) Sequé Ackst Minn-65535 Lemé MSS-1460 SACK_PERN-1 SE 1234 5 ± 1287 (AK) Sequé Ackst Minn-65535 Lemé MSS-1460 SACK_PERN-1 SE 1234 5 ± 1287 (AK) Sequé Ackst Minn-65535 Lemé SE 1464 4 4652 (AK) Sequé Ackst Minn-65535 Lemé Sequé Ackst Minn-65535 Lemé GØ 4652 ± 1654 (AK) Sequé Ackst Minn-65535 Lemé GØ 4652 ± 1654 (AK) Sequé Ackst Minn-65535 Lemé GØ 4652 ± 1654 (AK) Sequé Ackst Minn-65535 Lemé					
分析	29. 403.312392 29. 403.31236 256. 409.106933 257. 439.360823 258. 439.360826 288. 476.228648 288. 476.228648 288. 476.228649 326. 519.351299 326. 519.351299 326. 519.351299 326. 519.351299 326. 519.351299 326. 519.351299 326. 219.351299 327. 403.735946 238. 403.736017 239. 403.736017 239. 403.736017 239. 403.736121 240. 403.741744	172.16.3.248 172.16.39.93 172.16.19.93 172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.3.248 172.16.39.93 172.16.3.248	172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.293 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 No.228-230,No.2 内挥手报文(结束报 No.293-297,No.6 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240	(即用户 kjdd 56-258,No.2 文)? 520-623;	12 4052 + 1654 (SM), ACC Sequê Acks Minn-16384 Lemê (MSS-1466 SACC, PERN-1 SE 1654 - 4652 (ACK) Sequê Acks Minn-6353 Lemê (BU 1794 - 1137 (SM) Sequê Minn-6553 Lemê (BU 1794 - 1137 (SM) Sequê Minn-6553 Lemê (MSS-1466 SACC, PERN-1 SE 1794 - 1137 (ACK) Sequê Acks Minn-6353 Lemê (MSS-1466 SACC, PERN-1 SE 1934 - 1387 (ACK) Sequê Acks Minn-6553 Lemê (MSS-1466 SACC, PERN-1 SE 1934 - 1387 (ACK) Sequê Acks Minn-6553 Lemê (MSS-1466 SACC, PERN-1 SE 1934 - 1387 (ACK) Sequê Acks Minn-6558 Lemê (MSS-1466 SACC, PERN-1 SE 1934 - 1387 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1934 - 1387 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1934 - 1387 (SM) Sequê Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6555 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6556 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6556 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6566 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6566 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6566 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6566 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6566 Lemê (MSS-1466 SACC, PERN-1 SE 1937 - 2118 (ACK) Sequê Acks Minn-6566 SACC					
分析	29. 403.33292 29. 403.33236 29. 403.33236 29. 403.06033 29. 403.260276 29. 475.226648 20. 475.226649 20. 513.35289 20. 513.35289 20. 513.353939 20. 513.353939 20. 513.353939 20. 513.353939 20. 513.353939 20. 513.353939 21. 403.746017 237. 403.735946 238. 403.736017 239. 403.736017 239. 403.736121 240. 403.741744	172.16.3.248 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.1.3.93 172.16.1.3.93 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248	172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 No.228-230,No.2 内挥手报文(结束报 No.293-297,No.6 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240 172.16.3.240	でで TOP TOP TOP TOP TOP TOP TOP TOP	122 41622 + 1654 (SM), ACC) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1654 - 4652 (ACK) Sequê Acks Jimin-65351 Lemê (B. 1791 - 1137 (SM) Sequê Jimin-65531 Lemê HSS-1460 SACK_PERN-1 SE 1379 - 1791 (SM) Sequê Jimin-65531 Lemê HSS-1460 SACK_PERN-1 SE 1792 + 1137 (ACK) Sequê Acks Jimin-65364 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1934 (SM), ACK) Sequê Acks Jimin-65361 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1934 (SM), ACK) Sequê Acks Jimin-65361 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1937 (ACK) Sequê Acks Jimin-65361 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1937 (SM), ACK) Sequê Acks Jimin-65361 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1937 (SM), ACK) Sequê Acks Jimin-65361 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1937 (SM), ACK) Sequê Acks Jimin-65361 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1793 (ACK) Sequê Acks Jimin-65362 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1793 (ACK) Sequê Acks Jimin-65365 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1793 (ACK) Sequê Acks Jimin-65355 Lemê Gê 4652 + 1654 (ACK) Sequê Acks Jimin-65365 Lemê Gê 4652 + 1654 (ACK) Sequê Acks Jimin-65355 Lemê Gê 4652 + 1654 (ACK) Sequê Acks Zimin-65355 Lemê Gê 41791 + 1137 (ETN, ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137 (ACK) Sequê Acks 2933 Niin-65464 Lemê Se 14791 + 1137					
分析 6 答案	29. 403.33292 29. 403.33296 29. 403.33296 29. 403.36033 25. 403.360276 29. 475.226649 20. 475.226649 20. 513.35289 20. 513.35289 20. 513.35299 20. 513.35299 20. 513.35299 20. 513.35299 20. 513.35299 20. 513.35299 20. 513.35299 21. 403.756017 23. 403.736017 23. 403.736017 23. 403.736121 240 403.741744	172.16.3.248 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.248 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248	172.16.3.240 172.16.3.240	でで TCP TCP TCP TCP TCP TCP TCP TCP	122 41622 + 1654 (SM), ACC) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1654 - 4652 (ACK) Sequê Acks Jimin-6553 Lemê BC 1791 + 1137 (SM) Sequê Jimin-6553 Lemê HSS-1460 SACK_PERN-1 SE 1379 + 1791 (SM), ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1137 (ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1934 (SM), ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1934 (SM), ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1934 (SM), ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1937 (SM), ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1937 (SM), ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1934 (SM), ACK) Sequê Acks Jimin-16384 Lemê MSS-1460 SACK_PERN-1 SE 1793 + 1793 ACK JIMIN SE 1793 + 1793 ACK JIMIN SE 1793 + 1793 ACK JIMIN SE 1793 ACK JIMIN					
分析 6 答案	29. 403.312392 29. 403.31236 256. 409.106933 257. 439.360823 258. 439.360826 288. 476.228648 288. 476.228648 288. 476.228649 326. 519.351299 326. 519.351299 326. 519.351299 326. 519.351299 326. 519.351299 326. 519.351299 326. 219.351299 327. 403.735946 238. 403.736017 239. 403.736017	172.16.3.248 172.16.39.93 172.16.39.93 172.16.3.248 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.39.93 172.16.3.248 172.16.39.93 172.16.3.248	172.16.3.240 172.16.3.240	で で で で で で で で で で で で で で	12 4162 ± 1654 (SM), ACK) Sequé Acks I Min-16384 (Lende MSS-1466 SACK_PERN-1 St 1654 ÷ 4652 (ACK) Sequé Acks I Min-6553 Lenne 12 179 ± 1137 (SM) Sequé Nin-6553 Lenne MSS-1466 SACK_PERN-1 St 179 ± 1137 (ACK) Sequé Nick-1853 Lenne MSS-1466 SACK_PERN-1 St 179 ± 1137 (ACK) Sequé Acks I Min-1635 Lenné MSS-1466 SACK_PERN-1 SE 1394 ± 1387 (ACK) Sequé Acks I Min-1635 Lenné MSS-1466 SACK_PERN-1 SE 1394 ± 1387 (ACK) Sequé Acks I Min-1638 Lenné MSS-1466 SACK_PERN-1 SE 1394 ± 1387 (ACK) Sequé Acks I Min-1638 Lenné MSS-1466 SACK_PERN-1 SE 1394 ± 1387 (ACK) Sequé Acks I Min-1635 Lenné MSS-1466 SACK_PERN-1 SE 1394 ± 1387 (ACK) Sequé Acks I Min-1635 Lenné MSS-1466 SACK_PERN-1 SE 1394 ± 1387 (SM) Sequé Nin-65535 Lenné Acks I Min-1638 Lenné MSS-1460 SACK_PERN-1 SE 1397 ± 2118 2007 (SM), ACK) Sequé Acks I Min-1635 Lenné MSS-1466 SACK_PERN-1 SE 1397 ± 2118 2007 (SM), ACK) Sequé Acks I Min-1635 Lenné MSS-1466 SACK_PERN-1 SE 1454 ± 4652 [EIN, ACK] Sequé 1517 Acks 1 Min-65535 Lenné SE 1454 ± 4652 [EIN, ACK] Sequé 1518 Acks 1518 Min-65535 Lenné G0 4652 ± 1654 [ACK] Sequé 1518 Acks 1518 Min-65535 Lenné SE 1479 ± 1137 [ACK] Sequé Acks 2 Min-65535 Lenné SE 1791 ± 1137 [ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [EIN, ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [EIN, ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [EIN, ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [EIN, ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [EIN, ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [ACK] Sequé Acks 2 Min-65535 Lenné G0 1137 ± 1791 [ACK] Sequé Acks 2 Min-65535 Lenné					
分析 6 答案	29. 403.312392 29. 403.31236 256. 419.160513 257. 439.360823 258. 439.360876 286. 476.228648 288. 476.228648 288. 476.228648 288. 476.228649 325. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 327. 437.439394 237. 463.735946 238. 403.736017 239. 463.735017 240. 403.741744 257. 447.419393 272. 447.419343 273. 447.419343 274. 447.419343 275. 447.419343 276. 447.419343 277. 447.419343 278. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343	172.16.3.248 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4622 + 1654 (SM), ACC) Sequé Acks I Min-16384 Lemé MSS-1466 SACK_PERN-1 Set 1654 - 6452 (AK) Sequé Acks I Min-6553 Lemé BC 1791 + 1137 (SM) Sequé Hin-6553 Lemé MSS-1466 SACK_PERN-1 St 1791 + 1137 (AK) Sequé Hin-6553 Lemé MSS-1466 SACK_PERN-1 St 1791 + 1137 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 St 1791 + 1137 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (TM), ACC Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 S4 2097 + 2118 (AK) Sequé I Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 S4 2097 + 2118 (AK) Sequé I Acks I Min-6553 Lemé DSS Lemé MSS-1466 SACK_PERN-1 S4 2097 + 2118 (AK) Sequé I Acks I Min-6553 Lemé DSS Lemé DSS LEMÉ SACK SEQUÉ ACKS I MIN-6553 Lemé DSS LEMÉ SACK SEQUÉ ACKS I MIN-6553 LEMÉ SACK SEQUÉ ACKS SEQ					
分析 6 答案	29. 403.312392 29. 403.31236 25. 409.36033 25. 409.360876 28. 476.2226484 282 476.2226489 282 476.222649 324 519.351399 325 519.351399 326 519.351399 326 519.351399 326 519.351399 327 407.422649 24 407.422649 25 408.735146 27 408.735946 238 403.736017 239 403.736012 240 403.741744	172.16.3.248 172.16.3.9.93 172.16.3.9.93 172.16.3.248 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.248 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249 172.16.3.249	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4162 ± 1654 (SM), ACK Sequê Acks Min-16384 Lemê MSS-1460 SACK_PERN-1					
分析 6 答案	29. 403.312392 29. 403.31236 256. 419.160513 257. 439.360823 258. 439.360876 286. 476.228648 288. 476.228648 288. 476.228648 288. 476.228649 325. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 327. 437.439394 237. 463.735946 238. 403.736017 239. 463.735017 240. 403.741744 257. 447.419393 272. 447.419343 273. 447.419343 274. 447.419343 275. 447.419343 276. 447.419343 277. 447.419343 278. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343	172.16.3.248 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4622 + 1654 (SM), ACC) Sequé Acks I Min-16384 Lemé MSS-1466 SACK_PERN-1 Set 1654 - 6452 (AK) Sequé Acks I Min-6553 Lemé BC 1791 + 1137 (SM) Sequé Hin-6553 Lemé MSS-1466 SACK_PERN-1 St 1791 + 1137 (AK) Sequé Hin-6553 Lemé MSS-1466 SACK_PERN-1 St 1791 + 1137 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 St 1791 + 1137 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (AK) Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 SU 1934 - 1587 (TM), ACC Sequé Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 S4 2097 + 2118 (AK) Sequé I Acks I Min-6553 Lemé MSS-1466 SACK_PERN-1 S4 2097 + 2118 (AK) Sequé I Acks I Min-6553 Lemé DSS Lemé MSS-1466 SACK_PERN-1 S4 2097 + 2118 (AK) Sequé I Acks I Min-6553 Lemé DSS Lemé DSS LEMÉ SACK SEQUÉ ACKS I MIN-6553 Lemé DSS LEMÉ SACK SEQUÉ ACKS I MIN-6553 LEMÉ SACK SEQUÉ ACKS SEQ					
分析 6 答案	29. 403.312392 29. 403.31236 256. 419.160513 257. 439.360823 258. 439.360876 286. 476.228648 288. 476.228648 288. 476.228648 288. 476.228649 325. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 327. 437.439394 237. 463.735946 238. 403.736017 239. 463.735017 240. 403.741744 257. 447.419393 272. 447.419343 273. 447.419343 274. 447.419343 275. 447.419343 276. 447.419343 277. 447.419343 278. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343 279. 447.419343	172.16.3.248 172.16.39.93	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4852 + 1854 (SM), ACC) Sequé Acks I Min-16384 Lemé MSS-1466 SACK_PERN-1 SE 1654 + 6852 (AIK) Sequé Acks I Min-6535 Lemé BC 1791 + 1137 (SM) Sequé Nin-6555 Lemé HSS-1466 SACK_PERN-1 SE 1791 + 1137 (SM) Sequé Nin-6555 Lemé HSS-1466 SACK_PERN-1 SE 1791 + 1137 (AIK) Sequé Acks I Min-6555 Lemé MSS-1466 SACK_PERN-1 SE 1793 + 1897 (SM), ACC Sequé Acks I Min-6555 Lemé MSS-1466 SACK_PERN-1 SE 1793 + 1934 (SM), ACC Sequé Acks I Min-6555 Lemé MSS-1466 SACK_PERN-1 SE 1793 + 1934 (SM), ACC Sequé Acks I Min-6555 Lemé MSS-1466 SACK_PERN-1 SE 1793 + 1934 (SM), ACC Sequé Acks I Min-6555 Lemé MSS-1466 SACK_PERN-1 SE 1793 + 1934 (SM), ACC Sequé Acks I Min-6555 Lemé MSS-1466 SACK_PERN-1 SE 1793 + 1934 (SM), ACC Sequé Acks I Min-6555 Lemé MSS-1466 SACK_PERN-1 SE 1793 + 1934 (AIK) Sequé Acks I Min-6555 Lemé DS 1 ACC SE 1793 + 1934 (SM), ACC Sequé Acks I Min-6555 Lemé DS 1 ACC SE 1793 + 4652 (AIK), ACK Sequé Acks 138 Min-6555 Lemé G6 4652 + 1654 (AIK) Sequé 1518 Acks 2 Min-65555 Lemé G6 4552 + 1654 (AIK) Sequé 1518 Acks 2 Min-65555 Lemé G6 4137 + 1791 (FIN, ACK) Sequé Acks 2 Min-65555 Lemé G6 1137 + 1791 (AIK) Sequé Acks 2 Min-65555 Lemé G6 1137 + 1791 (AIK) Sequé Acks 2 Min-65555 Lemé G6 1587 + 1934 (FIN, ACK) Sequé Acks 2 Min-65555 Lemé G6 1587 + 1934 (FIN, ACK) Sequé Acks 2 Min-65555 Lemé G6 1587 + 1934 (FIN, ACK) Sequé Acks 2 Min-65555 Lemé G6 1587 + 1934 (AIK) Sequé Acks 1322 Min-64405 Lemé G6 1587 + 1934 (AIK) Sequé Acks 1322 Min-64405 Lemé G6 1587 + 1934 (AIK) Sequé Acks 1322 Min-64405 Lemé G6 1587 + 1934 (AIK) Sequé Acks 1322 Min-64405 Lemé G6 1587 + 1934 (AIK) Sequé 132 Acks 2 Min-65535 Lemé G6 1587 + 1934 (AIK) Sequé Acks 1322 Min-64405 Lemé G6 1587 + 1934 (AIK) Sequé 133 Acks 2 Min-65535 Lemé G6 1587 + 1934 (AIK) Sequé 133 Acks 2 Min-65535 Lemé G6 1587 + 1934 (AIK) Sequé 133 Acks 2 Min-65535 Lemé G6 1587 + 1934 (AIK) Sequé 133 Acks 2 Min-65535 Lemé G6 1587 + 1934 (AIK) Sequé 133 Acks 2 Min-65535 Lemé G6 1587 + 1934 (AIK) Sequé 133 Acks 2 Min-65535 Lemé G6 1587 + 1934 (AIK) Sequé 133 Acks 2 Min-65535 Lemé					
分析 6 答案	29. 403.312392 29. 403.31236 256. 419.160513 257. 439.360823 258. 439.360823 258. 439.360826 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 289. 476.551299 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 327. 403.735946 238. 403.736017 239. 403.736017 240. 403.736017 259. 407.6361300 297. 476.561201	172.16.3.248 172.16.3.248	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4622 + 1654 (SM), ACC) Sequê Acks I Min-16384 Lemê MSS-1460 SACC, PERN-1 SE 1654 + 652 (AK) Sequê Acks I Min-6535 Lemê (BL 179 + 1137 (SM) Sequê Hin-6535 Lemê HSS-1460 SACC, PERN-1 SE 1791 + 1137 (SM) Sequê Hin-6535 Lemê HSS-1460 SACC, PERN-1 SE 1791 + 1137 (ACX) Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1791 + 1137 (ACX) Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Hin-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê SE 1654 (SM), ACX Sequê Acks I Min-6535 Lemê SE 1654 + 4652 (ACX), ACX Sequê 1518 Acks 2 Min-65535 Lemê Gê 4552 + 1654 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê SE 1794 + 1137 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê Gê 1137 + 1791 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê Gê 1137 + 1791 (ACX) Sequê Acks 2 Min-65535 Lemê SE 1794 + 1537 (ACX) Sequê Acks 2 Min-65535 Lemê SE 1794 + 1537 (ACX) Sequê Acks 2 Min-65535 Lemê Gê 1587 + 1934 (EIN, ACX) Sequê Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1218 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1218 (ACX) Sequê 132 Acks 2 Min-6553					
分析 6 答案	29. 403.312392 29. 403.31236 25. 409. 136933 25. 409. 136937 25. 409. 1369276 28. 476. 228648 28. 476. 228648 28. 476. 228649 32. 519. 155199 32. 483. 736017 239. 403. 736017 239. 403. 736017 239. 403. 736123 240. 403. 741744	172.16.3.248 172.16.3.9.93 172.16.3.9.93 172.16.3.248	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4162 4 1654 (SM), ACK Sequê Acks Minn-16384 Lemê (MSS-1466 SACK_PERN-1					
分析 6 答案 截图	29. 403.312392 29. 403.31236 256. 419.160513 257. 439.360823 258. 439.360823 258. 439.360826 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 288. 476.228638 289. 476.551299 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 326. 519.353999 327. 403.735946 238. 403.736017 239. 403.736017 240. 403.736017 259. 407.6361300 297. 476.561201	172.16.3.248 172.16.3.268 172.16.3.9.93 172.16.3.9.93 172.16.3.268 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.268 177.16.9.93 172.16.3.268 177.16.9.93 172.16.3.268 172.16.3.268 172.16.3.268 172.16.3.268 172.16.3.268 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4622 + 1654 (SM), ACC) Sequê Acks I Min-16384 Lemê MSS-1460 SACC, PERN-1 SE 1654 + 652 (AK) Sequê Acks I Min-6535 Lemê (BL 179 + 1137 (SM) Sequê Hin-6535 Lemê HSS-1460 SACC, PERN-1 SE 1791 + 1137 (SM) Sequê Hin-6535 Lemê HSS-1460 SACC, PERN-1 SE 1791 + 1137 (ACX) Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1791 + 1137 (ACX) Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Hin-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê SE 1654 (SM), ACX Sequê Acks I Min-6535 Lemê SE 1654 + 4652 (ACX), ACX Sequê 1518 Acks 2 Min-65535 Lemê Gê 4552 + 1654 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê SE 1794 + 1137 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê Gê 1137 + 1791 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê Gê 1137 + 1791 (ACX) Sequê Acks 2 Min-65535 Lemê SE 1794 + 1537 (ACX) Sequê Acks 2 Min-65535 Lemê SE 1794 + 1537 (ACX) Sequê Acks 2 Min-65535 Lemê Gê 1587 + 1934 (EIN, ACX) Sequê Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1218 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1218 (ACX) Sequê 132 Acks 2 Min-6553					
分析 6 答案	29. 403.312392 29. 403.31236 25. 419.160513 25. 419.360876 28. 476.228618 28. 476.228618 28. 476.228618 28. 476.228618 28. 476.228618 28. 476.228618 28. 476.228618 28. 476.228619 325 519.353999 326 519.353999 326 519.353999 326 519.353999 327 403.735946 218. 403.736017 229. 403.736017 229. 403.736121 240. 403.741744 271. 447.419373 272. 447.419475 273. 447.419643 274.47.419643 275.477.4786189 276. 476.581281 277. 476.581281	172.16.3.248 172.16.3.268 172.16.3.9.93 172.16.3.9.93 172.16.3.268 172.16.3.9.93 172.16.3.9.93 172.16.3.9.93 172.16.3.268 177.16.9.93 172.16.3.268 177.16.9.93 172.16.3.268 172.16.3.268 172.16.3.268 172.16.3.268 172.16.3.268 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248 172.16.3.248	172.16.3.240 172.16.3.240	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	12 4622 + 1654 (SM), ACC) Sequê Acks I Min-16384 Lemê MSS-1460 SACC, PERN-1 SE 1654 + 652 (AK) Sequê Acks I Min-6535 Lemê (BL 179 + 1137 (SM) Sequê Hin-6535 Lemê HSS-1460 SACC, PERN-1 SE 1791 + 1137 (SM) Sequê Hin-6535 Lemê HSS-1460 SACC, PERN-1 SE 1791 + 1137 (ACX) Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1791 + 1137 (ACX) Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Hin-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê MSS-1460 SACC, PERN-1 SE 1794 + 1934 (SM), ACX Sequê Acks I Min-6535 Lemê SE 1654 (SM), ACX Sequê Acks I Min-6535 Lemê SE 1654 + 4652 (ACX), ACX Sequê 1518 Acks 2 Min-65535 Lemê Gê 4552 + 1654 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê SE 1794 + 1137 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê Gê 1137 + 1791 (ACX) Sequê 1518 Acks 2 Min-65535 Lemê Gê 1137 + 1791 (ACX) Sequê Acks 2 Min-65535 Lemê SE 1794 + 1537 (ACX) Sequê Acks 2 Min-65535 Lemê SE 1794 + 1537 (ACX) Sequê Acks 2 Min-65535 Lemê Gê 1587 + 1934 (EIN, ACX) Sequê Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1934 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1218 (ACX) Sequê 132 Acks 2 Min-65535 Lemê Gê 1587 + 1218 (ACX) Sequê 132 Acks 2 Min-6553					



答案	被动模式,	因为使用了 PAS\	/命令		
截图	225 400.933248 226 401.048537 227 403.308826	172.16.39.93 172.16.3.240 172.16.3.240	172.16.3.240 172.16.39.93 172.16.39.93	FTP TCP FTP	60 Request: PASV 60 21 + 1454 [ACK] Seq=851 Ack=77 Win=65459 Len=0 102 Response: 227 Entering Passive Mode (172,16,3,240,18,44)
分析	主动模式使	使用 PORT 命令和国	固定的 21 端口,	被动模式使用P	PASV 命令和随机端口。

三、在线捕获数据包实验

1. 阅读教材 P64-69 内容,熟悉 FTP 协议。

答:已阅读

- 2. 完成 P51 的实例 2-1。
- (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: 捕获的数据包的数量可以通过 Wireshark 捕获的数据包的行数看出,本次实验中捕获了数据包有 30444 个。

- 1					
	30438 24.032336	172.18.53.63	112.47.9.208	TCP	54 49650 → 443 [ACK] Seq=1 Ack=19025261 Win=3102 Len=0
ı	30439 24.032338	172.18.53.63	112.47.9.208	TCP	54 [TCP Dup ACK 30438#1] 49650 → 443 [ACK] Seq=1 Ack=19025261 Win=3102 Len=0
	30440 24.034335	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19025261 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30441 24.036254	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19026721 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30442 24.036268	172.18.53.63	112.47.9.208	TCP	54 49650 → 443 [ACK] Seq=1 Ack=19028181 Win=3102 Len=0
	30443 24.036272	172.18.53.63	112.47.9.208	TCP	54 [TCP Dup ACK 30442#1] 49650 → 443 [ACK] Seq=1 Ack=19028181 Win=3102 Len=0
	30444 24.036917	183.232.171.189	172.18.53.63	TCP	1514 80 → 59922 [ACK] Seq=1320890 Ack=12923 Win=4074 Len=1460 [TCP segment of a reassembled PDU]

(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。

答:判断数据是发出还是发来方法:通过查找本机的 IP 地址,若在一个数据包中本机的 IP 地址为源 IP 地址,则该数据包为发出的数据包,若本机的 IP 地址为目的 IP 地址,则为发入本机的数据包。

如在以下截图中第 30423 个数据包中源 IP 地址为本机 IP 地址,故该数据包为发出数据包。第 30424 个数据包目的 IP 地址为本机 IP 地址,故该数据包为发入数据包。

	30420 24.018357	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19010661 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30421 24.020302	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19012121 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30422 24.020320	172.18.53.63	112.47.9.208	TCP	54 49650 → 443 [ACK] Seq=1 Ack=19013581 Win=3102 Len=0
	30423 24.020323	172.18.53.63	112.47.9.208		54 [TCP Dup ACK 30422#1] 49650 → 443 [ACK] Seq=1 Ack=19013581 Win=3102 Len=0
	30424 24.020424	112.47.9.208	172.18.53.63	SSLv2	1514 Encrypted Data [TCP segment of a reassembled PDU]
	30425 24.022324	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19015041 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30426 24.022339	172.18.53.63	112.47.9.208	TCP	54 49650 → 443 [ACK] Seq=1 Ack=19016501 Win=3102 Len=0
- 1	30427 24.022342	172.18.53.63	112.47.9.208	TCP	54 [TCP Dup ACK 30426#1] 49650 → 443 [ACK] Seq=1 Ack=19016501 Win=3102 Len=0
	30428 24.024267	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19016501 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30429 24.026374	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19017961 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30430 24.026392	172.18.53.63	112.47.9.208	TCP	54 49650 → 443 [ACK] Seq=1 Ack=19019421 Win=3102 Len=0
	30431 24.026396	172.18.53.63	112.47.9.208	TCP	54 [TCP Dup ACK 30430#1] 49650 → 443 [ACK] Seq=1 Ack=19019421 Win=3102 Len=0
	30432 24.028408	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19019421 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30433 24.029039	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19020881 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30434 24.029059	172.18.53.63	112.47.9.208	TCP	54 49650 → 443 [ACK] Seq=1 Ack=19022341 Win=3102 Len=0
- 1	30435 24.029064	172.18.53.63	112.47.9.208	TCP	54 [TCP Dup ACK 30434#1] 49650 → 443 [ACK] Seq=1 Ack=19022341 Win=3102 Len=0
	30436 24.030336	112.47.9.208	172.18.53.63	TCP	1514 443 → 49650 [ACK] Seq=19022341 Ack=1 Win=1859 Len=1460 [TCP segment of a reassembled PDU]
	30437 24.032323	112.47.9.208	172.18.53.63	SSLv2	1514 Encrypted Data [TCP segment of a reassembled PDU]
	30438 24.032336	172.18.53.63	112.47.9.208	TCP	54 49650 → 443 [ACK] Seq=1 Ack=19025261 Win=3102 Len=0

查询 IP 地址的物理位置: 登陆 www.ip138.com ,输入我们捕获数据包的一些 IP 地址,如第 30419 个数据包的目的 IP 地址 112.47.9.208,查询结果如下:

iP段起始	iP段结束	归属地	网络	Windows子网掩码	Linux子网掩码
112.47.0.0	112.47.35.255	中国 福建省 泉州市	移动	255.255.192.0	112.47.0.0/18



再如第 30374 个数据包的源 IP 地址 183.232.171.189 的查询结果如下:

iP段起始	iP段结束	归属地	网络	Windows子网掩码	Linux子网掩码
183.232.162.0	183.232.199.255	中国广东省佛山市	移动	255.255.128.0	183.232.128.0/17

- (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 -r 6 -l a.b.c.d 和 ping -s 4 -l a.b.c.d 命令并捕获数据包。
 - 答: 在终端中输入 ipconfig 显示如下:

```
### C:\Users\Administrator.DES#TOP-6FNA37L>ipconfig
#### Windows IP 配置

以太网活配器 以太网:

- 连接特定的 DNS 后缀 ...

- 1Pv6 地址 ...

- 2001:250:3002:4460:15a4:abf4:42d5:dd5
- 临时 IPv6 地址 ...

- 2001:250:3002:4460:15a4:abf4:42d5:dd5
- 临时 IPv6 地址 ...

- 2001:250:3002:4460:15a4:abf4:42d5:dd5
- 临时 IPv6 地址 ...

- 2001:250:3002:4460:adid:aeld:d44d
- 临时 IPv6 地址 ...

- 2001:250:3002:4460:adid:aeld:d4d4
- 临时 IPv6 地址 ...

- 1Pv4 地址 ...

- 255. 255. 255. 0.0

- 数认网关...

| 以太网活配器 VMware Network Adapter VMnet1:

- 255. 255. 255. 0.0

- 数认网关...

- 255. 255. 0.0

- 数认网关...

- 1Pv6 地址 ...

- 1Pv6 上 ...

- 1Pv6 上
```

所以网关的 IP 地址为 172.18.55.254。(见默认网关那一行)

在终端中运行 ping -r 6 -l 32 172.18.55.254 和 ping -s 4 -l 32 172.18.55.254。

```
正在 Ping 172.18.55.254 具有 32 字节的数据:
来自 172.18.55.254 的回复; 字节=32 时间=lms TTL=255
第由: 172.18.55.254
来自 172.18.55.254
お自 172.18.55.254
```



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

ip	. addr==172, 18, 55, 254				
No.	Time	Source	Destination	Protocol	Length Info
Г	40 2.359985	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12126/24111, ttl=128 (no response found!)
	41 2.359993	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12126/24111, ttl=128 (reply in 42)
	42 2.360891	172.18.55.254	172.18.53.63	ICMP	102 Echo (ping) reply id=0x0001, seq=12126/24111, ttl=255 (request in 41)
	54 3.361788	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12127/24367, ttl=128 (no response found!)
	55 3.361794	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12127/24367, ttl=128 (reply in 56)
	56 3.362753	172.18.55.254	172.18.53.63	ICMP	102 Echo (ping) reply id=0x0001, seq=12127/24367, ttl=255 (request in 55)
	82 4.364799	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12128/24623, ttl=128 (no response found!)
	83 4.364804	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12128/24623, ttl=128 (reply in 84)
	84 4.365648	172.18.55.254	172.18.53.63	ICMP	102 Echo (ping) reply id=0x0001, seq=12128/24623, ttl=255 (request in 83)
	102 5.368513	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12129/24879, ttl=128 (no response found!)
-	103 5.368519	172.18.53.63	172.18.55.254	ICMP	102 Echo (ping) request id=0x0001, seq=12129/24879, ttl=128 (reply in 104)
4-	104 5.369396	172.18.55.254	172.18.53.63	ICMP	102 Echo (ping) reply id=0x0001, seq=12129/24879, ttl=255 (request in 103)
	221 11.424450	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12130/25135, ttl=128 (no response found!)
	222 11.424456	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12130/25135, ttl=128 (reply in 223)
	223 11.425352	172.18.55.254	172.18.53.63	ICMP	110 Echo (ping) reply id=0x0001, seq=12130/25135, ttl=255 (request in 222)
	237 12.428565	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12131/25391, ttl=128 (no response found!)
	238 12.428572	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12131/25391, ttl=128 (reply in 239)
	239 12.429365	172.18.55.254	172.18.53.63	ICMP	110 Echo (ping) reply id=0x0001, seq=12131/25391, ttl=255 (request in 238)
	254 13.434450	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12132/25647, ttl=128 (no response found!)
	255 13.434455	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12132/25647, ttl=128 (reply in 256)
	256 13.435254	172.18.55.254	172.18.53.63	ICMP	110 Echo (ping) reply id=0x0001, seq=12132/25647, ttl=255 (request in 255)
	284 14.439219	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12133/25903, ttl=128 (no response found!)
	285 14.439224	172.18.53.63	172.18.55.254	ICMP	114 Echo (ping) request id=0x0001, seq=12133/25903, ttl=128 (reply in 286)
L	286 14.440135	172.18.55.254	172.18.53.63	ICMP	110 Echo (ping) reply id=0x0001, seq=12133/25903, ttl=255 (request in 285)

- (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,分析这些数据主要字段的含义。
- 答: 捕获的数据中有如下协议: 0x9001, ARP, DHCPV6, EAP, ICMP, ICMPv6, IPv6, LLDP, LLMNR, MDNS, SSDP, TCP, UDP。

Echo 和 Stamp 请求和响应分组如(4)中图片所示(其中所选行上方为 Echo 请求和响应分组,所选行及其下方为 Stamp 请求和响应分组):

以下分析他们的主要字段:

```
> Frame 42: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{02C11E35-75E6-4428-8E0E-3F98D62BBDBD}, id 0
> Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: Micro-St_8e:f0:57 (2c:f0:5d:8e:f0:57)
> Internet Protocol Version 4, Src: 172.18.55.254, Dst: 172.18.53.63
> Internet Control Message Protocol
```

上图第一行主要包括物理层的数据帧概况,第二行主要包括数据链路层以太网帧头部信息,第三行是互联网层 IP 包头部信息,第四行是网络层 ICMP 包头部信息。其中第一、二、四行内容在 Echo 和 Stamp 分组中差别不大,以下主要分析第三行内容:

Echo 分组:

```
> Frame 41: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{02C11E35-75E6-4428-8E0E-3F98D62BBDBD}, id 0
> Ethernet II, Src: Micro-St_8e:f0:57 (2c:f0:Sd:8e:f0:57), Dst: Hangzhou_69:ce:55 (74:25:8a:69:ce:55)

Vinternet Protocol Version 4, Src: 172.18.53.63, Dst: 172.18.55.254
0100 .... = Version: 4
.... 1100 = Header Length: 48 bytes (12)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 88
Identification: 0xb951 (47441)
> Flags: 0x00
Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.18.53.63
Destination Address: 172.18.55.254
> Options: (28 bytes), Record Route
> Internet Control Message Protocol
```

从上图中可以看到数据帧的总长度 Total Length,首部校验 Identification,TTL,源地址 Source Address,目的主机地址 Destination Address

查看 Options 中内容可以看到路径中的路由信息:



```
v Options: (28 bytes), Record Route

∨ Options: (28 bytes), Record Route

  IP Option - Record Route (27 bytes)

✓ IP Option - Record Route (27 bytes)
     > Type: 7
                                                 > Type: 7
       Length: 27
                                                   Length: 27
       Pointer: 4
                                                   Pointer: 8
       Empty Route: 0.0.0.0 <- (next)
                                                   Recorded Route: 172.18.55.254
       Empty Route: 0.0.0.0
                                                   Empty Route: 0.0.0.0 <- (next)
       Empty Route: 0.0.0.0
                                                   Empty Route: 0.0.0.0
       Empty Route: 0.0.0.0
                                                   Empty Route: 0.0.0.0
       Empty Route: 0.0.0.0
                                                   Empty Route: 0.0.0.0
                                                   Empty Route: 0.0.0.0
       Empty Route: 0.0.0.0

▼ IP Option - End of Options List (EOL)
  IP Option - End of Options List (EOL)
     > Type: 0
                                                 > Type: 0
```

其中左图为请求分组的路由信息, 右图为响应分组的路由信息

Stamp 分组:

```
> Frame 223: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{02C11E35-75E6-4428-8E0E-3F98D628BDBD}, id 0
> Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: Micro-St_8e:f0:57 (2c:f0:5d:8e:f0:57)
> Internet Protocol Version 4, Src: 172.18.55.254, Dst: 172.18.53.63
0100 ... = Version: 4
.... 1110 = Header Length: 56 bytes (14)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 96
    Identification: 0xda5a (55898)
> Flags: 0x00
Fragment Offset: 0
    Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x70a5 [validation disabled]
[Header Checksum status: Unverified]
Source Address: 172.18.53.63
> Options: (36 bytes), Time Stamp
> IP Option - Time Stamp (36 bytes)
> Internet Control Message Protocol
```

Stamp 分组其余内容与 Echo 分组中相同, Options 中存储的是时间戳信息:

```
Options: (36 bytes), Time Stamp
v Options: (40 bytes), Time Stamp

▼ IP Option - Time Stamp (36 bytes)
                                                      IP Option - Time Stamp (36 bytes)
    > Type: 68
                                                         > Type: 68
      Length: 36
                                                           Length: 36
      Pointer: 5
                                                           Pointer: 13
      0000 .... = Overflow: 0
                                                           0000 .... = Overflow: 0
      .... 0001 = Flag: Time stamp and address (0x1)
                                                           .... 0001 = Flag: Time stamp and address (0x1)
      Address:
                                                           Address: 172.18.55.254
      Time stamp: 0
      Address:
                                                           Time stamp: 18901988
      Time stamp: 0
                                                           Address: -
      Address:
                                                           Time stamp: 0
      Time stamp: 0
                                                           Address:
      Address:
                                                           Time stamp: 0
      Time stamp: 0
                                                           Address:

▼ IP Option - End of Options List (EOL)
                                                           Time stamp: 0
     > Type: 0
```

左图为请求分组时间戳信息,右图为响应分组时间戳信息,且时间戳信息与命令行输出内容相对应。

【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?
- 答: (1)注意网速;
 - ②搜索主机相关进程;
 - ③ 使用相关软件进行监测;
- (2) 如何防范被嗅探?
- 答: ① 网络分段: 一个网络段包括一组共享低层设备和线路的机器,如交换机,动态集线器和网桥等设



- 备,可以对数据流进行限制,从而达到防止嗅探的目的。
- ②加密:一方面可以对数据流中的部分重要信息进行加密,另一方面也可只对应用层加密,然而后者将使大部分与网络和操作系统有关的敏感信息失去保护。选择何种加密方式这就取决于信息的安全级别及网络的安全程度。
- ③一次性口令设置:口令并不在网络上传输而是在两端进行字符串匹配,客户端利用从服务器上得到的 Challenge 和自身的口令计算出一个新字符串并将之返回给服务器。在服务器上利用比较算法进行匹配,如果 匹配,连接就允许建立,所有的 Challenge 和字符串都只使用一次。
 - ④禁用杂错节点: 安装不支持杂错的网卡,通常可以防止 IBM 兼容机进行嗅探。

学号	学生	<u>自评分</u>
<u>18329015</u>	郝裕玮	<u>100</u>
<u>18325071</u>	<u>张</u> 闯	<u>100</u>
<u>19335153</u>	马淙升	<u>100</u>