



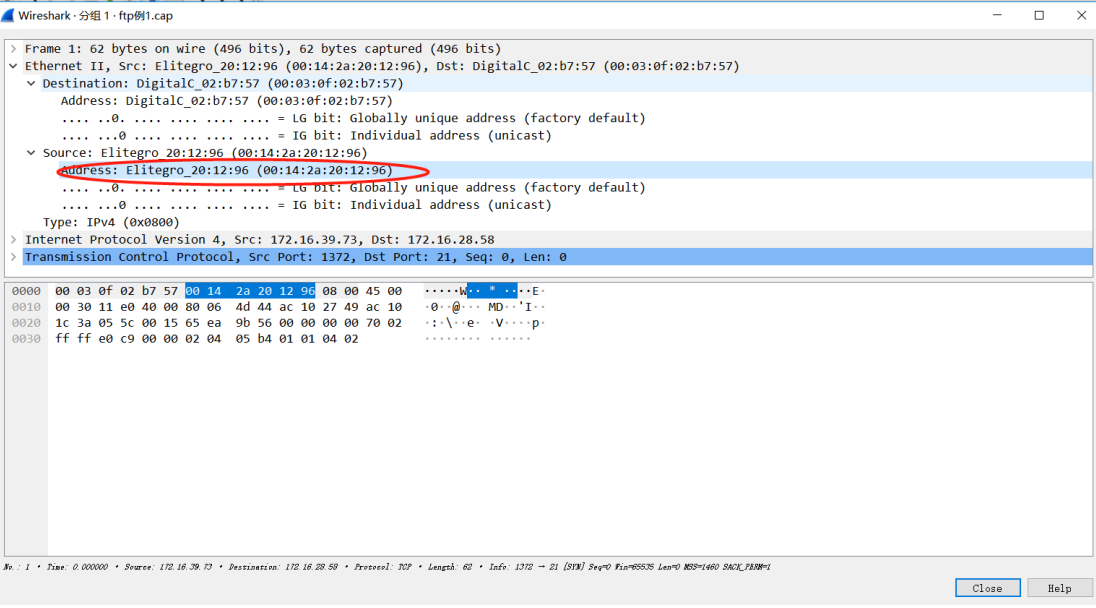
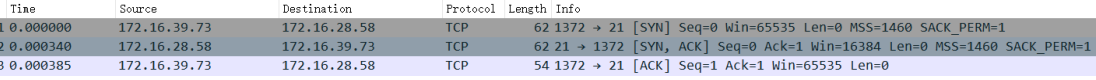
警示

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

院系	数据科学与计算机	班 级	周二_5-6_节	组长	蔡湘国
学号	16340007	16340305	16340074		
学生	蔡湘国	郑先淇	何自强		

Ftp 协议分析实验

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

题号	
1	FTP 客户端的 mac 地址是多少？
答案	00:14:2a:20:12:96
截图	
分析	选取的第一条报文，由 Info 可知由 621372->21 端口，可知是由客户端到服务端（FTP 服务器使用的端口号是 21），所以只需双击查看详情查找其 Source address 即可。
2	第 1、2、3 号报文的作用是什么？
答案	三次握手，建立连接
截图	



Wireshark · 分组 1 · ftp例1.cap

```
Transmission Control Protocol, Src Port: 1372, Dst Port: 21, Seq: 0, Len: 0
  Source Port: 1372
  Destination Port: 21
  [Stream index: 0]
  [TCP Segment Len: 0]
  sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
  Acknowledgment number: 0
  0111 .... = Header Length: 28 bytes (7)
  Flags: 0x002 (SYN)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
    ....0... = ECN-Echo: Not set
    ....0... = Urgent: Not set
    ....0... = Acknowledgment: Not set
    ....0... = Push: Not set
    ....0... = Reset: Not set
    ....0... = Syn: Set
    ....0... = Fin: Not set
  [TCP Flags: .....S.]
```

Wireshark · 分组 2 · ftp例1.cap

```
Transmission Control Protocol, Src Port: 21, Dst Port: 1372, Seq: 0, Ack: 1, Len: 0
  Source Port: 21
  Destination Port: 1372
  [Stream index: 0]
  [TCP Segment Len: 0]
  sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  0111 .... = Header Length: 28 bytes (7)
  Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
    ....0... = ECN-Echo: Not set
    ....0... = Urgent: Not set
    ....1... = Acknowledgment: Set
    ....0... = Push: Not set
    ....0... = Reset: Not set
    ....1... = Syn: Set
    ....0... = Fin: Not set
  [TCP Flags: .....A..S.]
```

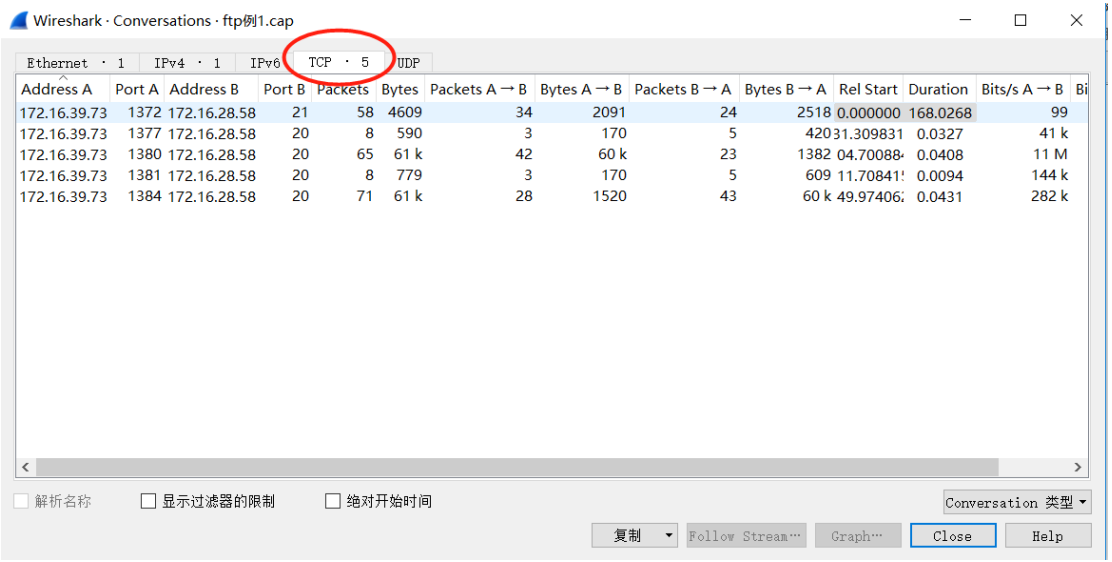
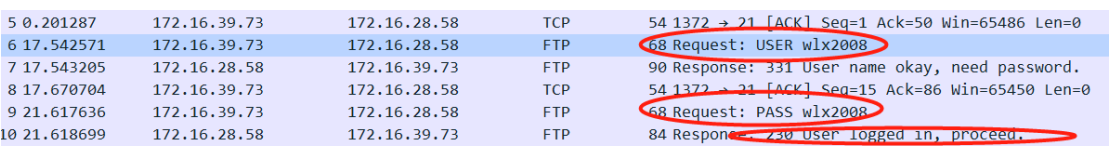
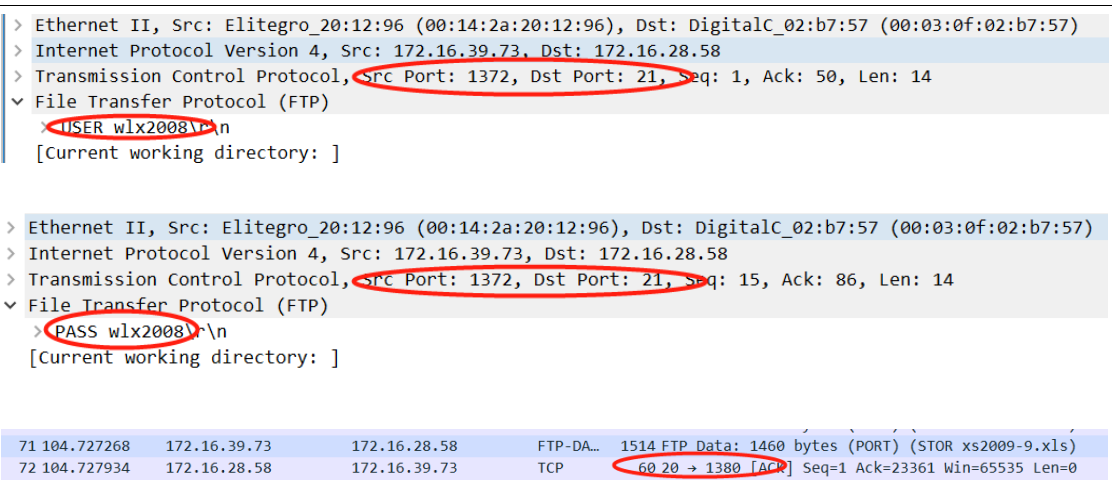
Wireshark · 分组 3 · ftp例1.cap

```
> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 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)
> Internet Protocol Version 4, Src: 172.16.39.73, Dst: 172.16.28.58
Transmission Control Protocol, Src Port: 1372, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
  Source Port: 1372
  Destination Port: 21
  [Stream index: 0]
  [TCP Segment Len: 0]
  sequence number: 1 (relative sequence number)
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
    ....0... = ECN-Echo: Not set
    ....0... = Urgent: Not set
    ....1... = Acknowledgment: Set
    ....0... = Push: Not set
    ....0... = Reset: Not set
    ....0... = Syn: Not set
    ....0... = Fin: Not set
  [TCP Flags: .....A....]
```

分析

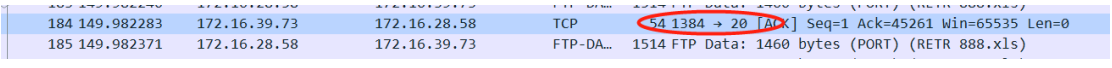
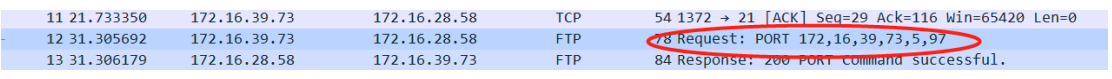
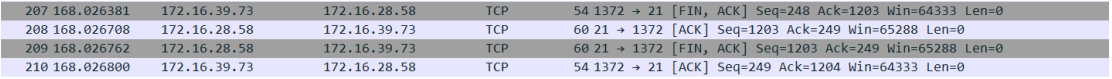
第一次握手数据包，客户端发送一个 TCP，标志位为 SYN，序列号为 0，代表客户端请求建立连接；第二次握手的数据包，服务器发回确认包，标志位为 SYN,ACK。将确认序号(Acknowledgement Number)设置为客户的 ISN 加 1 以,即 $0+1=1$ ；第三次握手的数据包，客户端再



	次发送确认包(ACK) SYN 标志位为0,ACK 标志位为 1.并且把服务器发来 ACK 的序号字段+1,放在确定字段中发送给对方.并且在数据段放写 ISN 的+1
3	该数据包中共有多少个 TCP 流?
答案	该数据包中共有 5 个 TCP 流。
截图	
分析	通过菜单栏中的统计 (Statistic) ->对话可以统计 TCP 流数量
4	用什么用户和密码登录成功?
答案	用户: wlx2008, 密码: wlx2008
截图	
分析	由图可知登录 FTP 服务器时,使用的控制命令是 USER 和 PASS。根据这两个命令,可以看到登录的账号为 wlx2008,密码为 wlx2008,最后显示登陆成功
5	该 FTP 的命令连接和数据连接分别是什么样的连接?
答案	控制连接是持久连接,数据连接是非持久连接
截图	



计算机网络实验报告

	
分析	当用户主机与远程主机开始一个 FTP 会话前，FTP 的客户机首先在 21 号端口上发起一个用于控制的与服务器的 TCP 连接。FTP 的客户机通过该控制连接发送用户的标识和口令，也发送改变远程目录的命令。当 FTP 的服务端从该连接上收到一个文件传输的命令后，就发起一个到客户机的数据连接。FTP 在该数据连接上准确地传送一个文件并关闭该连接。同一会话期间，如果用户还需要传输另一个文件，FTP 则打开另一个数据连接。截图中截了两个命令的例子用的都是同一个 TCP 连接（本例中的其他命令也一样）。而不同的数据传输则是经由不同的 TCP 连接。
6	该 FTP 的连接模式是那种？为什么？
答案	主动模式，使用的是 PORT 命令
截图	
分析	客户端向服务器的 FTP 端口（默认是 21）发送连接请求，服务器接受连接，建立一条命令链路。 当需要传送数据时，客户端在命令链路上用 PORT 命令告诉服务器：“我打开了 1372 端口，你过来连接我”。于是服务器从 20 端口向客户端的 1372 端口发送连接请求，建立一条数据链路来传送数据。
7	最后四个报文的作用是什么？
答案	四次握手断开客户端和服务器的连接
截图	
分析	TCP/IP 协议断开连接的时候需要有四次“分手”的过程，需要 4 个 TCP 报文段。
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 个；USER：认证用户名，PASS：认证密码，PORT：主动模式，指定服务器要连接的地址和端；NLST：返回指定目录的文件名列表，XMKD：新建目录，RNFR：从...重命名，RNT0：重命名到...，STOR：接收数据并且在服务器站点保存为文件，RETR：传输文件副本，QUIT：断开连接

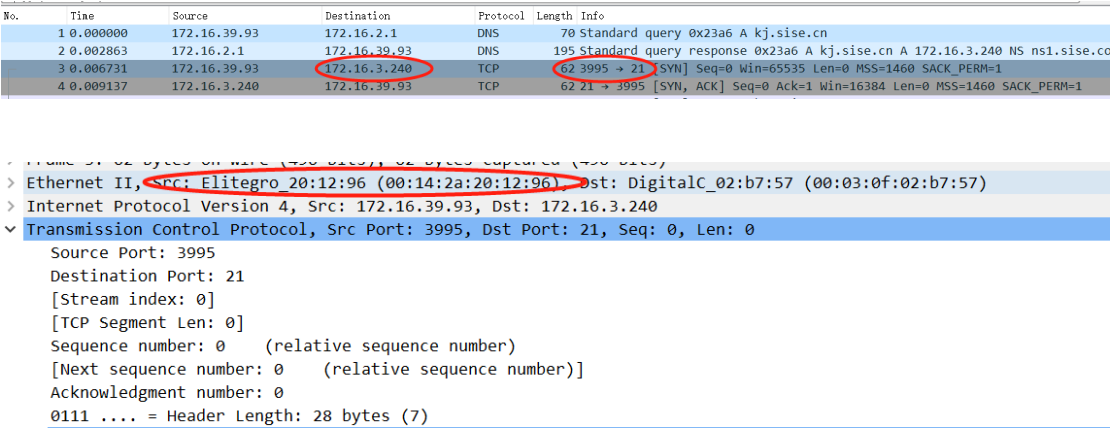
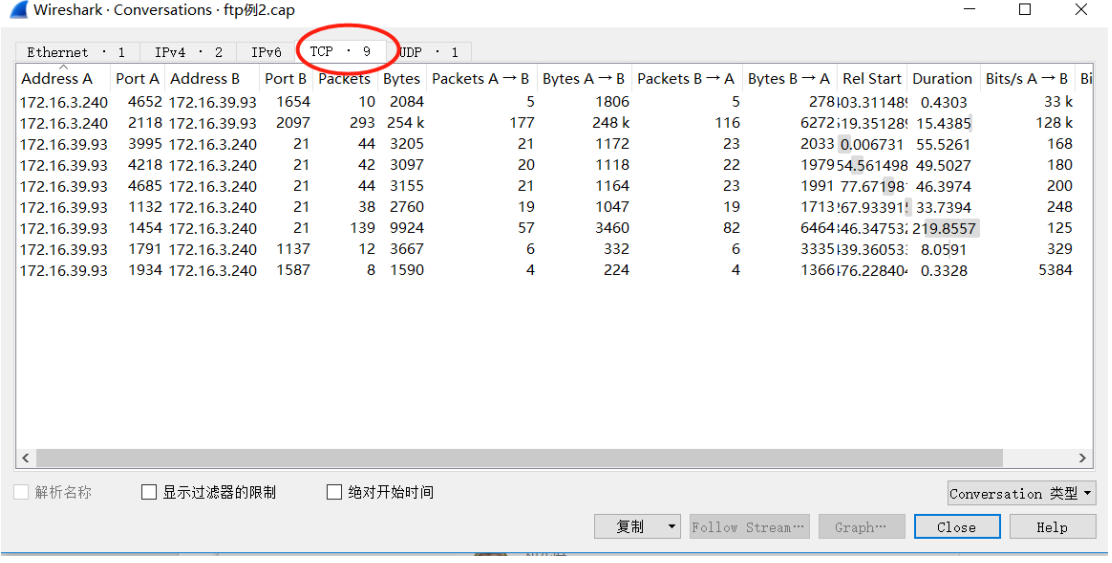
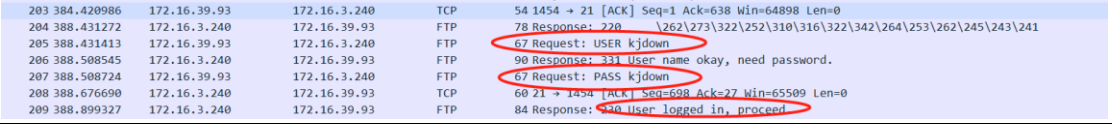


截图	<pre>220 Serv-U FTP Server v6.4 for WinSock ready... USER wlx2008 331 User name okay, need password. PASS wlx2008 230 User logged in, proceed. PORT 172,16,39,73,5,97 200 PORT Command successful. NLST -l 150 Opening ASCII mode data connection for /bin/ls. 226-Maximum disk quota limited to 307200 kBytes Used disk quota 0 kBytes, available 307200 kBytes 226 Transfer complete. XMKD jjj 257 "/jjj" directory created. RNFR jjj 350 File or directory exists, ready for destination name RNT0 ppp 250 RNT0 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 RNT0 888.xls 250 RNT0 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!</pre>
分析	<p>分析->追踪流->TCP 流，两种不同的颜色分别代表命令和响应，查看 Request，查找对应命令含义。命令含义可参照以下链接：https://zh.wikipedia.org/wiki/FTP%E5%91%BD%E4%BB%A4%E5%88%97%E8%A1%A8</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 ip:172.16.3.240; 客户端 mac 地址: 00: 14: 2a:20:12:96
截图	
分析	由 Info 可知由 4685->21 端口, 可知是由客户端到服务端 (FTP 服务器使用的端口号是 21), 则目的 ip 即为服务器 ip.源地址即为客户端地址, 所以只需双击查看详情查找其 Source address 即可查看客户端 MAC 地址。
2	该数据包中共有多少个 TCP 流?
答案	9
截图	
分析	通过菜单栏中的统计 (Statistic) -> 对话可以统计 TCP 流数量
3	最后用什么用户和密码登录成功?
答案	用户: kjdown 密码: kjdown
截图	
分析	由图 (第三个圈处) 可知用上述用户和密码登陆成功
4	该 FTP 的命令连接和数据连接分别是什么?
答案	控制连接是持久连接, 数据连接是非持久连接



截图	<pre>> Ethernet II, Src: Elitegro_20:12:96 (00:14:2a:20:12:96), Dst: DigitalC_02:b7:57 (00:03:0f:02:b7:57) > Internet Protocol Version 4, Src: 172.16.39.93, Dst: 172.16.3.240 > Transmission Control Protocol, Src Port: 4685, Dst Port: 21, Seq: 1, Ack: 662, Len: 11 v File Transfer Protocol (FTP) > USER xxxx\r\n [Current working directory:] > Ethernet II, Src: Elitegro_20:12:96 (00:14:2a:20:12:96), Dst: DigitalC_02:b7:57 (00:03:0f:02:b7:57) > Internet Protocol Version 4, Src: 172.16.39.93, Dst: 172.16.3.240 > Transmission Control Protocol, Src Port: 4685, Dst Port: 21, Seq: 12, Ack: 698, Len: 11 v File Transfer Protocol (FTP) PASS yyyy\r\n [Current working directory:]</pre>																				
分析	截图中截了两个命令的例子用的都是同一个 TCP 连接（本例中的其他命令也一样）。而不同的数据传输则是经由不同的 TCP 连接。																				
5	哪几个报文是 FTP 数据连接的三次握手报文？																				
答案	3 到 5																				
截图	<table><tr><td>3 0.006731</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>4 0.009137</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>62 21 → 3995 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>5 0.009192</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 3995 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td></tr></table>	3 0.006731	172.16.39.93	172.16.3.240	TCP	62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1	4 0.009137	172.16.3.240	172.16.39.93	TCP	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					
3 0.006731	172.16.39.93	172.16.3.240	TCP	62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1																	
4 0.009137	172.16.3.240	172.16.39.93	TCP	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																	
分析	第一次握手数据包，客户端发送一个 TCP，标志位为 SYN，序列号为 0，代表客户端请求建立连接；第二次握手的数据包，服务器发回确认包，标志位为 SYN,ACK。将确认序号(Acknowledgement Number)设置为客户的 ISN 加 1 以.即 0+1=1；第三次握手的数据包，客户端再次发送确认包(ACK) SYN 标志位为 0,ACK 标志位为 1.并且把服务器发来 ACK 的序号字段+1,放在确定字段中发送给对方.并且在数据段放写 ISN 的+1																				
6	哪几个报文是 FTP 数据连接的挥手报文（结束报文）？																				
答案	数据包的最后四个 TCP 报文是 ftp 数据连接的挥手报文。																				
截图	<table><tr><td>629 565.983884</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1454 → 21 [FIN, ACK] Seq=375 Ack=1843 Win=65161 Len=0</td></tr><tr><td>630 565.988017</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 21 → 1454 [ACK] Seq=1843 Ack=376 Win=65161 Len=0</td></tr><tr><td>631 566.203149</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 21 → 1454 [FIN, ACK] Seq=1843 Ack=376 Win=65161 Len=0</td></tr><tr><td>632 566.203215</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1454 → 21 [ACK] Seq=376 Ack=1844 Win=65161 Len=0</td></tr></table>	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
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																	
分析	TCP/IP 协议断开连接的时候需要有四次“分手”的过程，需要 4 个 TCP 报文段。由截图的标志位的状态可以看出。																				
7	该 FTP 的连接模式是那种？为什么？																				
答案	被动模式，使用的是 PASV 命令																				
截图	<pre>PASV 227 Entering Passive Mode (172,16,3,240,18,44) PASV 227 Entering Passive Mode (172,16,3,240,4,113) PASV 227 Entering Passive Mode (172,16,3,240,6,51) PASV 227 Entering Passive Mode (172,16,3,240,8,70)</pre>																				
分析	通过分析->追踪流->TCP 流查看对应命令和应答，如上截图使用 PASV 命令为被动模式																				



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。

(1) 5s 后捕获数据量为 102 个。截图如下：

No.	Time	Source	Destination	Protocol	Length	Info
2	0.004043	2001:250:3002:4410:...	2404:6800:4005:809:...	TCP	86	12826 → 443 [S...
6	0.124804	2001:250:3002:4410:...	2404:6800:4005:809:...	TCP	86	12827 → 443 [S...
50	2.130895	172.18.34.156	66.220.158.32	TCP	66	12843 → 443 [S...
51	2.131237	172.18.34.156	66.220.158.32	TCP	66	12844 → 443 [S...
52	2.296005	2001:250:3002:4410:...	2404:6800:4005:809:...	TCP	86	12828 → 443 [S...
62	3.131444	172.18.34.156	66.220.158.32	TCP	66	[TCP Retransmi...
63	3.131444	172.18.34.156	66.220.158.32	TCP	66	[TCP Retransmi...
86	3.958619	209.197.3.15	172.18.34.156	TLSv1.2	85	Encrypted Alert
87	3.958627	209.197.3.15	172.18.34.156	TCP	60	443 → 12832 [F...
88	3.958808	172.18.34.156	209.197.3.15	TCP	54	12832 → 443 [A...
99	4.638046	209.197.3.15	172.18.34.156	TLSv1.2	85	Encrypted Alert
100	4.638061	209.197.3.15	172.18.34.156	TCP	60	443 → 12831 [F...
101	4.638403	172.18.34.156	209.197.3.15	TCP	54	12831 → 443 [A...

> Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: HewlettP_58:b9:51 (48:ba:4e:58:b9:51), Dst: Hangzhou_e5:b2:d4 (38:22:d6:e5:
> Internet Protocol Version 6, Src: 2001:250:3002:4410:cdde:2fc8:872:8e92, Dst: 2404:6800:4005:
> Transmission Control Protocol, Src Port: 12826, Dst Port: 443, Seq: 0, Len: 0

0000 38 22 d6 e5 b2 d4 48 ba 4e 58 b9 51 86 dd 60 0d 8"....H·NX·Q·`·
0010 f5 8c 00 20 06 40 20 01 02 50 30 02 44 10 cd de ...@·.P0·D·...

wireshark_94782EEF-D623-4831...20181006120748_a33508.pcapng 分组: 102 · 已显示: 13 (12.7%) Profile: Default

(2) 查看本电脑的 ip:

以太网适配器 以太网 2:

连接特定的 DNS 后缀	: sysu.edu.cn
IPv6 地址	: 2001:250:3002:4410:527:a39b:ad22:51e2
临时 IPv6 地址.	: 2001:250:3002:4410:2496:bca3:741f:dccf
临时 IPv6 地址.	: 2001:250:3002:4410:3da5:5477:fe86:4e1
临时 IPv6 地址.	: 2001:250:3002:4410:cc27:3176:43c0:23a3
临时 IPv6 地址.	: 2001:250:3002:4410:cdde:2fc8:872:8e92
临时 IPv6 地址.	: 2001:250:3002:4410:d02f:a023:5981:5b5f
临时 IPv6 地址.	: 2001:250:3002:4410:e011:cc9:4884:39fd
本地链接 IPv6 地址.	: fe80::527:a39b:ad22:51e2%12
IPv4 地址	: 172.18.34.156
子网掩码	: 255.255.252.0
默认网关.	: fe80::3a22:d6ff:fee5:b2d4%12
	: 172.18.35.254

由上图可知 IP 地址为 172.18.34.156。再分析 wireshark 抓到的一些数据包（数据包详情见下图），



*以太网 2						
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(U) 无线(W) 工具(I) 帮助(H)						
tcp						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.004043	2001:250:3002:4410:...	2404:6800:4005:809:...	TCP	86	12826 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256...
6	0.124804	2001:250:3002:4410:...	2404:6800:4005:809:...	TCP	86	12827 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256...
50	2.130895	172.18.34.156	66.220.158.32	TCP	66	12843 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256...
51	2.131237	172.18.34.156	66.220.158.32	TCP	66	12844 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256...
52	2.296005	2001:250:3002:4410:...	2404:6800:4005:809:...	TCP	86	12828 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256...
62	3.131444	172.18.34.156	66.220.158.32	TCP	66	[TCP Retransmission] 12844 → 443 [SYN] Seq=0 Win=65535 ...
63	3.131444	172.18.34.156	66.220.158.32	TCP	66	[TCP Retransmission] 12843 → 443 [SYN] Seq=0 Win=65535 ...
86	3.958619	209.197.3.15	172.18.34.156	TLSv1.2	85	Encrypted Alert
87	3.958627	209.197.3.15	172.18.34.156	TCP	60	443 → 12832 [FIN, ACK] Seq=32 Ack=1 Win=60 Len=0
88	3.958808	172.18.34.156	209.197.3.15	TCP	54	12832 → 443 [ACK] Seq=1 Ack=33 Win=1023 Len=0
99	4.638046	209.197.3.15	172.18.34.156	TLSv1.2	85	Encrypted Alert
100	4.638061	209.197.3.15	172.18.34.156	TCP	60	443 → 12831 [FIN, ACK] Seq=32 Ack=1 Win=62 Len=0
101	4.638403	172.18.34.156	209.197.3.15	TCP	54	12831 → 443 [ACK] Seq=1 Ack=33 Win=1022 Len=0

由图可知，当源 IP 地址为 172.18.34.156 时，数据包为发出的，当目的 IP 地址为 192.168.3.191 时，数据包为发过来的。

通过网站 www.ip138.com 查询 IP 地址的地理位置：

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:172.18.34.156

- 本站数据：本地局域网
- 参考数据1：局域网局域网
- 参考数据2：本地局域网
- 兼容IPv6地址：::AC12:229C
- 映射IPv6地址：::FFFF:AC12:229C

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:66.220.158.32

- 本站数据：美国
- 参考数据1：美国弗吉尼亚州阿什本 facebook.com
- 参考数据2：美国
- 兼容IPv6地址：::42DC:9E20
- 映射IPv6地址：::FFFF:42DC:9E20

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:209.197.3.15

- 本站数据：美国
- 参考数据1：HIGHWINDS.COMHIGHWINDS.COM
highwinds.com
- 参考数据2：美国
- 兼容IPv6地址：::D1C5:030F
- 映射IPv6地址：::FFFF:D1C5:030F

(3) 默认网关：



以太网适配器 以太网 2:

```
连接特定的 DNS 后缀 . . . . . : sysu.edu.cn
IPv6 地址 . . . . . : 2001:250:3002:4410:527:a39b:ad22:51e2
临时 IPv6 地址. . . . . : 2001:250:3002:4410:2496:bca3:741f:dcf
临时 IPv6 地址. . . . . : 2001:250:3002:4410:3da5:5477:fe86:4e1
临时 IPv6 地址. . . . . : 2001:250:3002:4410:cc27:3176:43c0:23a3
临时 IPv6 地址. . . . . : 2001:250:3002:4410:cdde:2fc8:872:8e92
临时 IPv6 地址. . . . . : 2001:250:3002:4410:d02f:a023:5981:5b5f
临时 IPv6 地址. . . . . : 2001:250:3002:4410:e011:cc9:4884:39fd
本地链接 IPv6 地址. . . . . : fe80::527:a39b:ad22:51e2%12
IPv4 地址 . . . . . : 172.18.34.156
子网掩码 . . . . . : 255.255.252.0
默认网关. . . . . : fe80::3a22:d6ff:fee5:b2d4%12
                      172.18.35.254
```

由图可知所在的网关 IP 地址为: 172.18.35.254

执行 ping -r 6 -l 172.18.35.254

```
PS C:\Users\cxg> ping -r 6 172.18.35.254

正在 Ping 172.18.35.254 具有 32 字节的数据:
来自 172.18.35.254 的回复: 字节=32 时间<1ms TTL=255
    路由: 172.18.35.254
来自 172.18.35.254 的回复: 字节=32 时间=1ms TTL=255
    路由: 172.18.35.254
来自 172.18.35.254 的回复: 字节=32 时间=1ms TTL=255
    路由: 172.18.35.254
来自 172.18.35.254 的回复: 字节=32 时间=1ms TTL=255
    路由: 172.18.35.254

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

捕获的数据包:



*以太网 2

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

Apply a display filter ... <Ctrl-/> 表达式...

No.	Time	Source	Destination	Protocol	Length	Info
6551	2.505980	172.18.34.156	202.116.81.74	TCP	66	64158 → 80 [ACK] Seq=1 Ack=2609297 Win=1057 Len=0 ...
6552	2.505997	172.18.34.156	202.116.81.74	TCP	66	64158 → 80 [ACK] Seq=1 Ack=2612193 Win=1035 Len=0 ...
6553	2.506014	172.18.34.156	202.116.81.74	TCP	66	64158 → 80 [ACK] Seq=1 Ack=2615089 Win=1012 Len=0 ...
6554	2.506030	172.18.34.156	202.116.81.74	TCP	66	64158 → 80 [ACK] Seq=1 Ack=2616537 Win=1125 Len=0 ...
6555	2.506046	172.18.34.156	202.116.81.74	TCP	66	64158 → 80 [ACK] Seq=1 Ack=2619433 Win=1103 Len=0 ...
6556	2.506065	172.18.34.156	117.149.197.202	TCP	66	64156 → 80 [ACK] Seq=1 Ack=893417 Win=3450 Len=0 T...
6557	2.506082	172.18.34.156	202.116.81.74	TCP	66	64158 → 80 [ACK] Seq=1 Ack=2620881 Win=1125 Len=0 ...
6558	2.506100	172.18.34.156	120.198.248.42	TCP	54	64164 → 80 [ACK] Seq=1 Ack=2336001 Win=16372 Len=0 ...
6559	2.506116	172.18.34.156	117.149.197.202	TCP	66	64156 → 80 [ACK] Seq=1 Ack=894865 Win=3461 Len=0 T...
6560	2.506134	172.18.34.156	120.198.248.42	TCP	54	64164 → 80 [ACK] Seq=1 Ack=2337461 Win=16384 Len=0 ...
6561	2.506166	172.18.34.156	117.149.197.202	TCP	66	64156 → 80 [ACK] Seq=1 Ack=897761 Win=3439 Len=0 T...
6562	2.506185	172.18.34.156	117.149.197.202	TCP	66	[TCP Window Update] 64156 → 80 [ACK] Seq=1 Ack=897...
6563	2.506203	172.18.34.156	120.198.248.42	TCP	54	64164 → 80 [ACK] Seq=1 Ack=2340381 Win=16372 Len=0 ...
6564	2.506221	172.18.34.156	117.149.197.202	TCP	66	64156 → 80 [ACK] Seq=1 Ack=900657 Win=3439 Len=0 T...
6565	2.506265	172.18.34.156	120.198.248.42	TCP	54	64164 → 80 [ACK] Seq=1 Ack=2341841 Win=16384 Len=0 ...
6566	2.506316	172.18.34.156	117.149.197.202	TCP	66	64156 → 80 [ACK] Seq=1 Ack=902105 Win=3461 Len=0 T...
6567	2.506333	172.18.34.156	117.149.197.202	TCP	66	64156 → 80 [ACK] Seq=1 Ack=905001 Win=3439 Len=0 T...
6568	2.506349	172.18.34.156	117.149.197.202	TCP	66	64156 → 80 [ACK] Seq=1 Ack=907897 Win=3416 Len=0 T...

> Frame 6868: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: HewlettP_58:b9:51 (48:ba:4e:58:b9:51), Dst: Hangzhou_e5:b2:d4 (38:22:d6:e5:b2:d4)
> Internet Protocol Version 4, Src: 172.18.34.156, Dst: 172.18.35.254
> Internet Control Message Protocol

0000 38 22 d6 e5 b2 d4 48 ba 4e 58 b9 51 08 00 4c 00 8"....H NX Q...L.
0010 00 58 46 2f 00 00 80 01 00 00 ac 12 22 9c ac 12 XF/...."....

Internet Protocol Version 4 (ip), 48 bytes 分组: 53444 · 已显示: 53444 (100.0%) · 已丢弃: 0 (0.0%) Profile: Default

执行 ping -s 4 -l 172.18.35.254

```
PS C:\Users\cxg> ping -s 4 172.18.35.254

正在 Ping 172.18.35.254 具有 32 字节的数据:
来自 172.18.35.254 的回复: 字节=32 时间=1ms TTL=255
    时间戳: 172.18.35.254 : 45258631 ->
        172.18.34.156 : 16457173 ->
        172.18.34.156 : 16457173
来自 172.18.35.254 的回复: 字节=32 时间=1ms TTL=255
    时间戳: 172.18.35.254 : 45259637 ->
        172.18.34.156 : 16458181 ->
        172.18.34.156 : 16458181
来自 172.18.35.254 的回复: 字节=32 时间=2ms TTL=255
    时间戳: 172.18.35.254 : 45260647 ->
        172.18.34.156 : 16459191 ->
        172.18.34.156 : 16459191
来自 172.18.35.254 的回复: 字节=32 时间=1ms TTL=255
    时间戳: 172.18.35.254 : 45261657 ->
        172.18.34.156 : 16460199 ->
        172.18.34.156 : 16460199

172.18.35.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 2ms, 平均 = 1ms
PS C:\Users\cxg>
```

捕获的数据包:



计算机网络实验报告

正在捕获 以太网 2

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4	0.204284	172.18.32.64	172.18.35.255	NBNS	92	Name query NB WPAD<00>
5	0.218355	fe80::6dc7:6bf7:674...	ff02::c	UDP	718	51045 → 3702 Len=656
6	0.221420	2001:250:3002:4410::...	ff05::1:3	DHCPv6	166	Relay-forw L: 2001:250:3002:4410:a3e:8eff:fe79:c11d I...
7	0.293817	2001:250:3002:4410::...	ff02::1:2	DHCPv6	194	Solicit XID: 0xa8a94f CID: 00030001d4ee07473e19
8	0.300456	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.32.234? Tell 172.18.35.254
9	0.301354	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.32.235? Tell 172.18.35.254
10	0.301360	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.32.236? Tell 172.18.35.254
11	0.301361	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.32.237? Tell 172.18.35.254
12	0.301362	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.35.163? Tell 172.18.35.254
13	0.301363	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.35.7? Tell 172.18.35.254
14	0.302208	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.32.239? Tell 172.18.35.254
15	0.302215	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.35.101? Tell 172.18.35.254
16	0.302216	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.32.240? Tell 172.18.35.254
17	0.302217	Hangzhou_e5:b2:d4	Broadcast	ARP	60	Who has 172.18.32.241? Tell 172.18.35.254
18	0.346932	172.18.34.185	172.18.35.255	NBNS	92	Name query NB NPI51C891<00>
19	0.347874	172.18.34.185	224.0.0.251	MDNS	75	Standard query 0x0000 AAAA npi51c891.local, "QM" ques...
20	0.347881	fe80::4469:757d:393...	ff02::fb	MDNS	95	Standard query 0x0000 AAAA npi51c891.local, "QM" ques...
21	0.348705	172.18.35.70	224.0.0.251	MDNS	60	Standard query response 0x0000

> Frame 1: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface 0
> Ethernet II, Src: AsustekC_b7:84:a8 (08:62:66:b7:84:a8), Dst: IPv4mcast_de (01:00:5e:00:00:de)
> Internet Protocol Version 4, Src: 172.18.34.87, Dst: 225.0.0.222
> User Datagram Protocol, Src Port: 59278, Dst Port: 54997
> Data (164 bytes)

0000 01 00 5e 00 00 de 08 62 66 b7 84 a8 08 00 45 00 ..^...b f.....E.
0010 00 c0 10 12 00 00 1f 11 da d3 ac 12 22 57 e1 00W..

Internet Protocol Version 4 (ip), 20 bytes

(4) 执行 filter: ip.addr == 192.168.3.253,截屏运行结果:

ping -r 6 -l 172.18.35.254

No.	Time	Source	Destination	Protocol	Length	Info
62	1.705596	172.18.34.156	172.18.35.254	ICMP	102	Echo (ping) request id=0x0100, seq=21/5376, ttl=128 (r...
63	1.706941	172.18.35.254	172.18.34.156	ICMP	102	Echo (ping) reply id=0x0100, seq=21/5376, ttl=255 (r...
99	2.708995	172.18.34.156	172.18.35.254	ICMP	102	Echo (ping) request id=0x0100, seq=22/5632, ttl=128 (r...
100	2.709965	172.18.35.254	172.18.34.156	ICMP	102	Echo (ping) reply id=0x0100, seq=22/5632, ttl=255 (r...
153	3.712275	172.18.34.156	172.18.35.254	ICMP	102	Echo (ping) request id=0x0100, seq=23/5888, ttl=128 (r...
154	3.713104	172.18.35.254	172.18.34.156	ICMP	102	Echo (ping) reply id=0x0100, seq=23/5888, ttl=255 (r...
238	4.716022	172.18.34.156	172.18.35.254	ICMP	102	Echo (ping) request id=0x0100, seq=24/6144, ttl=128 (r...
239	4.718493	172.18.35.254	172.18.34.156	ICMP	102	Echo (ping) reply id=0x0100, seq=24/6144, ttl=255 (r...

> Frame 62: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: HewlettP_58:b9:51 (48:ba:4e:58:b9:51), Dst: Hangzhou_e5:b2:d4 (38:22:d6:e5:b2:d4)
> Internet Protocol Version 4, Src: 172.18.34.156, Dst: 172.18.35.254
> Internet Control Message Protocol

0000 38 22 d6 e5 b2 d4 48 ba 4e 58 b9 51 08 00 4c 00 8"....H NX.Q..L.
0010 00 58 46 3d 00 00 80 01 00 00 ac 12 22 9c ac 12 .XF=.....

Internet Protocol Version 4 (ip), 48 bytes

分组: 1393 · 已显示: 8 (0.6%)

Profile: Default



ping -s 4 -l 172.18.35.254

Wireshark packet capture analysis of a ping command. The capture shows ICMP Echo (ping) requests and replies between 172.18.34.156 and 172.18.35.254. The interface is *以太网 2.

No.	Time	Source	Destination	Protocol	Length	Info
27	1.073994	172.18.34.156	172.18.35.254	ICMP	114	Echo (ping) request id=0x0100, seq=25/6400, ttl=128 (r...
28	1.074925	172.18.35.254	172.18.34.156	ICMP	110	Echo (ping) reply id=0x0100, seq=25/6400, ttl=255 (r...
59	2.082041	172.18.34.156	172.18.35.254	ICMP	114	Echo (ping) request id=0x0100, seq=26/6656, ttl=128 (r...
60	2.083083	172.18.35.254	172.18.34.156	ICMP	110	Echo (ping) reply id=0x0100, seq=26/6656, ttl=255 (r...
96	3.088412	172.18.34.156	172.18.35.254	ICMP	114	Echo (ping) request id=0x0100, seq=27/6912, ttl=128 (r...
97	3.089331	172.18.35.254	172.18.34.156	ICMP	110	Echo (ping) reply id=0x0100, seq=27/6912, ttl=255 (r...
113	4.097838	172.18.34.156	172.18.35.254	ICMP	114	Echo (ping) request id=0x0100, seq=28/7168, ttl=128 (r...
114	4.098718	172.18.35.254	172.18.34.156	ICMP	110	Echo (ping) reply id=0x0100, seq=28/7168, ttl=255 (r...

Frame 27: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
> Ethernet II, Src: HewlettP_58:b9:51 (48:ba:4e:58:b9:51), Dst: Hangzhou_e5:b2:d4 (38:22:d6:e5:b2:d4)
> Internet Protocol Version 4, Src: 172.18.34.156, Dst: 172.18.35.254
> Internet Control Message Protocol

0000 38 22 d6 e5 b2 d4 48 ba 4e 58 b9 51 08 00 4f 00 8"....H..NX.Q...0.
0010 00 64 46 41 00 00 80 01 00 00 ac 12 22 9c ac 12 .dFA....

Internet Protocol Version 4 (ip), 60 bytes | 分组: 545 · 已显示: 8 (1.5%) | Profile: Default

(5) 捕获的数据中为 ICMP 协议。

Echo(ping)request: ICMP 创建一个回应请求数据包；

Echo(ping)reply: 回显应答。

组内自评：

学号	学生	自评分
16340007	蔡湘国	100
16340305	郑先洪	100
16340074	何自强	100