



警示

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

| | | | | | |
|----|------------|----------|-------------|----|-----|
| 院系 | 数据科学与计算机学院 | 班 级 | 16 级信息与计算科学 | 组长 | 回煜淼 |
| 学号 | 16339021 | 16339049 | 16343065 | | |
| 学生 | 回煜淼 | 辛依繁 | 桑娜 | | |

Ftp 协议分析实验

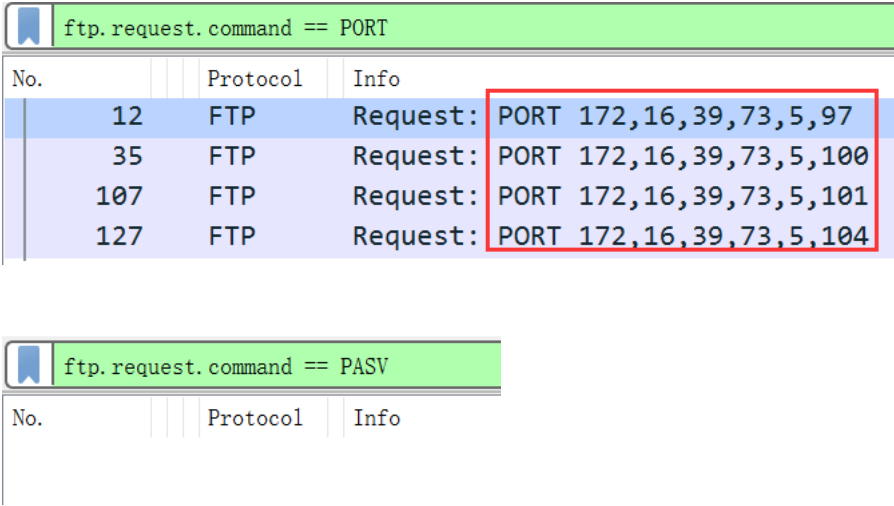
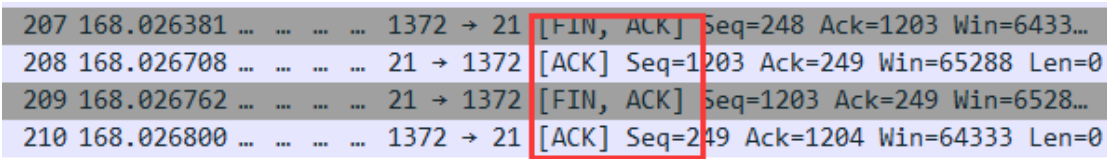
一、打开“FTP 数据包”的“ftp 例 1.cap”文件，进行观察分析，回答以下问题(见附件)

| | |
|----|---|
| 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 | 展开第 1 号报文的详细信息，可以看到 Src 后的地址，即为客户端的 mac 地址。 |
| 2 | 第 1、2、3 号报文的作用是什么？ |
| 答案 | ftp 客户端和 ftp 服务端进行三次握手，从而建立连接。 |
| 截图 | |
| 分析 | <p>SYN 是建立连接标志，ACK 是确认标志。</p> <p>1 号报文：客户端发出建立连接的请求；</p> <p>2 号报文：服务端确认收到信息，并同意建立连接；</p> <p>3 号报文：客户端确认收到信息，建立连接。</p> |
| 3 | 该数据包中共有多少个 TCP 流？ |
| 答案 | 5 个 |



| | | | | | | | |
|--------------|--|--|--------------|----------|---------|---------|---------|
| 截图 | Wireshark · Conversations · ftp例1 | | | | | | |
| | Ethernet • 1 | | IPv4 • 1 | | IPv6 | TCP • 5 | UDP |
| | Address A | Port A | Address B | Port B | Packets | Bytes | |
| | 172.16.39.73 | 1372 | 172.16.28.58 | 21 | 58 | 4609 | |
| | 172.16.39.73 | 1377 | 172.16.28.58 | 20 | 8 | 590 | |
| | 172.16.39.73 | 1380 | 172.16.28.58 | 20 | 65 | 61 k | |
| | 172.16.39.73 | 1381 | 172.16.28.58 | 20 | 8 | 779 | |
| | 172.16.39.73 | 1384 | 172.16.28.58 | 20 | 71 | 61 k | |
| | 在 wireshark 上方的工具栏中选择“统计”，再选择“对话”，在弹出的页面上方选择“TCP”标签，即可得知共有 5 个 TCP 流。 | | | | | | |
| | 4 | 用什么用户和密码登录成功？ | | | | | |
| | 答案 | wlx2008, wlx2008 | | | | | |
| 截图 | <div>6 17.542571 Request: USER wlx2008</div> <div>7 17.543205 Response: 331 User name okay, need password.</div> <div>8 17.670704 1372 → 21 [ACK] Seq=15 Ack=86 Win=65450 Len=0</div> <div>9 21.617636 Request: PASS wlx2008</div> <div>10 21.618699 Response: 230 User logged in, proceed.</div> | | | | | | |
| | 分析 | USER 是发送用户名的命令，PASS 是发送密码的命令。第 10 号报文表示登录成功。 | | | | | |
| | 5 | 该 FTP 的命令连接和数据连接分别是什么样的连接？ | | | | | |
| | 答案 | 命令连接：1372-21 | | | | | |
| | | 数据连接：1377-20 1380-20 1381-20 1384-20 | | | | | |
| | 截图 | Ethernet • 1 | | IPv4 • 1 | | IPv6 | TCP • 5 |
| Address A | | Port A | Address B | Port B | Packets | Bytes | P |
| 172.16.39.73 | | 1372 | 172.16.28.58 | 21 | 58 | 4609 | |
| 172.16.39.73 | | 1377 | 172.16.28.58 | 20 | 8 | 590 | |
| 172.16.39.73 | | 1380 | 172.16.28.58 | 20 | 65 | 61 k | |
| 172.16.39.73 | | 1381 | 172.16.28.58 | 20 | 8 | 779 | |
| 172.16.39.73 | | 1384 | 172.16.28.58 | 20 | 71 | 61 k | |
| 分析 | 控制连接：客户端希望与 ftp 服务器建立上传下载的数据传输时，它首先向服务器的 TCP 21 端口发起一个建立连接的请求，ftp 服务器接受来自客户端的请求，完成连接的建立过程。 | | | | | | |
| | 数据连接： | | | | | | |
| | PORT 方式的连接过程是： | | | | | | |
| | 客户端向服务器的 ftp 端口发送的数据传送请求，服务器主动与客户建立连接。 | | | | | | |
| | 客户端通过控制连接利用 PORT 命令将端口号通告给服务器。服务器从自己的 TCP 20 端口连 | | | | | | |



| | |
|----|--|
| | <p>接至客户的指定端口发送数据。</p> <p>在 wireshark 上方的工具栏中选择“统计”，再选择“对话”，在弹出的页面上方选择“TCP”标签，即可看到每次所用端口。</p> |
| 6 | 该 FTP 的连接模式是那种？为什么？ |
| 答案 | 主动模式。因为客户端用的是 PORT，没有找到 PASV。 |
| 截图 |  |
| 分析 | <p>PORT 方式的连接过程是：</p> <p>客户端向服务器的 ftp 端口发送的数据传送请求，服务器主动与客户建立连接。</p> <p>客户端通过控制连接利用 PORT 命令将端口号通告给服务器。服务器从自己的 TCP 20 端口连接至客户的指定端口发送数据。</p> |
| 7 | 最后四个报文的作用是什么？ |
| 答案 | 断开连接 |
| 截图 |  |
| 分析 | <p>FIN 是结束标志，ACK 是确认标志。</p> <p>207 号报文：首先客户端向服务端发出断开连接的请求；</p> <p>208 号报文：服务端回应确认收到了；</p> <p>209 号报文：再次，服务端发出 FIN 同意结束；</p> <p>210 号报文：客户端回应确认收到，连接断开。</p> |
| 8 | 该数据包中有多少个 ftp 的命令及应答，其含义分别是什么？ |



计算机网络实验报告

答案

| | | | |
|-------|----------------|------|--------------------|
| USER | 认证用户名 | RNFR | 从...重命名 |
| PASS | 认证密码 | RNTO | 重命名到... |
| PORT | 指定服务器要连接的地址和端口 | STOR | 存放文件，文件从客户端传送到服务器端 |
| NLIST | 返回指定目录的文件名列表 | RETR | 读取文件，文件从服务器端传送到客户端 |
| XMKD | 创建目录 | QUIT | 断开连接 |

ftp 命令：10 个

| | | | |
|-----|------------------|-----|------------|
| 150 | 打开数据连接 | 230 | 用户登录 |
| 200 | 命令被成功执行 | 257 | 创建“目录名” |
| 220 | 新用户服务准备好了 | 331 | 用户名正确，需要口令 |
| 221 | 服务关闭控制连接，可以退出登录 | 250 | 请求的文件操作完成 |
| 226 | 关闭数据连接，请求的文件操作成功 | 350 | 下一步命令 |

ftp 应答：10 个

截图

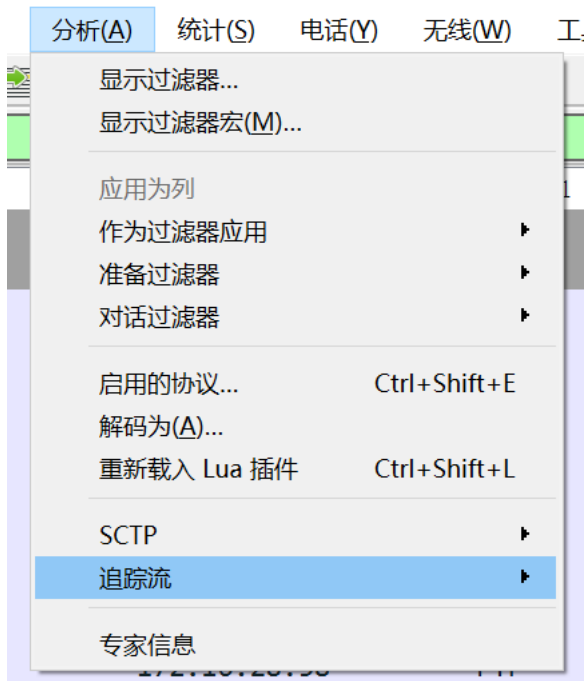
```
USER wlx2008
PASS wlx2008
PORT 172,16,39,73,5,97
NLST -l
XMKD jjj
RNFR jjj
RNT0 ppp
PORT 172,16,39,73,5,100
STOR xs2009-9.xls
PORT 172,16,39,73,5,101
NLST -l
RNFR xs2009-9.xls
RNT0 888.xls
PORT 172,16,39,73,5,104
RETR 888.xls
QUIT
```



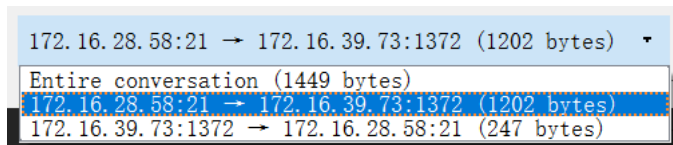
```
220 Serv-U FTP Server v6.4 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
226-Maximum disk quota limited to 307200 kBytes
    Used disk quota 0 kBytes, available 307200 kBytes
226 Transfer complete.
257 "/jjj" directory created.
350 File or directory exists, ready for destination name
250 RNT0 command successful.
200 PORT Command successful.
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.
200 PORT Command successful.
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.
350 File or directory exists, ready for destination name
250 RNT0 command successful.
200 PORT Command successful.
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.
221 Goodbye!
```



分析



在 wireshark 中选择工具栏里的“分析”，在“追踪流”中选择“TCP”，即可看到所有的 tcp 命令和应答。



在打开的窗口左下方可以选择是客户发送到服务器的，还是服务器发送到客户的。

统计出所有的命令和应答，查阅相关资料即可得出它们的含义。

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 | FTP 服务器 ip: 172.16.3.240 FTP 客户端 mac 地址: 00:14:2a:20:12:96 |
| 截图 | |



| | |
|----|--|
| 分析 | 1. 首先打开文件，观察第一个 TCP 标识所在行，即为其 ip 地址 2. 同上个实验，展开报文观察 mac 地址。 |
| 2 | 该数据包中共有多少个 TCP 流？ |
| 答案 | 该数据包中共有 9 个 TCP 流。 |
| 截图 | |
| 分析 | 利用工具栏列表中“统计”快捷键中的“对话”按钮，选择“TCP”选项卡，即可得到当前数据包的 TCP 流数目，观察可知此数据包的 TCP 流数目为 9。 |
| 3 | 最后用什么用户和密码登录成功？ |
| 答案 | 用户名: kjdown 密码: kjdown |
| 截图 | |
| 分析 | 首先在过滤控制窗口采用过滤协议中的 ftp 过滤，过滤后很容易找到用户名和密码的相关信息。 |
| 4 | 该 FTP 的命令连接和数据连接分别是什么？ |
| 答案 | 该 FTP 的命令连接有：3395-21、4218-21、4685-21、1454-21。 该 FTP 的数据连接有：4652-1654、1791-1137、1934-1587、2118-2097。 |
| 截图 | |
| 分析 | 如图所示，找到命令连接和数据连接的端口号，即客户端-服务端的端口号即可。 |
| 5 | 哪几个报文是 FTP 数据连接的三次握手报文？ |
| 答案 | 1.228-230 2.256-258 |



| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------|---|----------------|--------------|--|-----|---|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|---|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|---|----------------|--------------|--------------|-----|---|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|---|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|---|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|---|----------------|--------------|--------------|-----|--|----------------|--------------|--------------|-----|---|
| | 3.286-288 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 4.324-326 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 截图 | <table><tr><td>228 403.311489</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>62 1654 → 4652 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>229 403.312292</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>62 4652 → 1654 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>230 403.312346</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1654 → 4652 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td></tr><tr><td>256 439.360533</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>62 1791 → 1137 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>257 439.360823</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>62 1137 → 1791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>258 439.360876</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1791 → 1137 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td></tr><tr><td>286 476.228404</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>62 1934 → 1587 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>287 476.228638</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>62 1587 → 1934 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>288 476.228669</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1934 → 1587 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td></tr><tr><td>324 519.351289</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>62 2097 → 2118 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>325 519.353919</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>62 2118 → 2097 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>326 519.353959</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 2097 → 2118 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td></tr></table> | 228 403.311489 | 172.16.39.93 | 172.16.3.240 | TCP | 62 1654 → 4652 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | 229 403.312292 | 172.16.3.240 | 172.16.39.93 | TCP | 62 4652 → 1654 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | 230 403.312346 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1654 → 4652 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | 256 439.360533 | 172.16.39.93 | 172.16.3.240 | TCP | 62 1791 → 1137 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | 257 439.360823 | 172.16.3.240 | 172.16.39.93 | TCP | 62 1137 → 1791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | 258 439.360876 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1791 → 1137 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | 286 476.228404 | 172.16.39.93 | 172.16.3.240 | TCP | 62 1934 → 1587 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | 287 476.228638 | 172.16.3.240 | 172.16.39.93 | TCP | 62 1587 → 1934 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | 288 476.228669 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1934 → 1587 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | 324 519.351289 | 172.16.39.93 | 172.16.3.240 | TCP | 62 2097 → 2118 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | 325 519.353919 | 172.16.3.240 | 172.16.39.93 | TCP | 62 2118 → 2097 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | 326 519.353959 | 172.16.39.93 | 172.16.3.240 | TCP | 54 2097 → 2118 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | |
| 228 403.311489 | 172.16.39.93 | 172.16.3.240 | TCP | 62 1654 → 4652 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 229 403.312292 | 172.16.3.240 | 172.16.39.93 | TCP | 62 4652 → 1654 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 230 403.312346 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1654 → 4652 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 256 439.360533 | 172.16.39.93 | 172.16.3.240 | TCP | 62 1791 → 1137 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 257 439.360823 | 172.16.3.240 | 172.16.39.93 | TCP | 62 1137 → 1791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 258 439.360876 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1791 → 1137 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 286 476.228404 | 172.16.39.93 | 172.16.3.240 | TCP | 62 1934 → 1587 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 287 476.228638 | 172.16.3.240 | 172.16.39.93 | TCP | 62 1587 → 1934 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 288 476.228669 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1934 → 1587 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 324 519.351289 | 172.16.39.93 | 172.16.3.240 | TCP | 62 2097 → 2118 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 325 519.353919 | 172.16.3.240 | 172.16.39.93 | TCP | 62 2118 → 2097 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 326 519.353959 | 172.16.39.93 | 172.16.3.240 | TCP | 54 2097 → 2118 [ACK] Seq=1 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 分析 | 找到 ftp 数据连接发出的命令，根据握手报文的原则性质统计，共计四次。 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | 哪几个报文是 FTP 数据连接的挥手报文（结束报文）？ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 答案 | 1.237-240 2.270-273 3.293-297 4.620-623 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 截图 | <table><tr><td>237 403.735946</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 4652 → 1654 [FIN, ACK] Seq=1517 Ack=1 Win=65535 Len=0</td></tr><tr><td>238 403.736017</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1654 → 4652 [ACK] Seq=1 Ack=1518 Win=65535 Len=0</td></tr><tr><td>239 403.736121</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1654 → 4652 [FIN, ACK] Seq=1 Ack=1518 Win=65535 Len=0</td></tr><tr><td>240 403.741744</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 4652 → 1654 [ACK] Seq=1518 Ack=2 Win=65535 Len=0</td></tr><tr><td>270 447.419304</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1137 → 1791 [FIN, ACK] Seq=2992 Ack=1 Win=65535 Len=0</td></tr><tr><td>271 447.419373</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1791 → 1137 [ACK] Seq=1 Ack=2993 Win=65464 Len=0</td></tr><tr><td>272 447.419475</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1791 → 1137 [FIN, ACK] Seq=1 Ack=2993 Win=65464 Len=0</td></tr><tr><td>273 447.419643</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1137 → 1791 [ACK] Seq=2993 Ack=2 Win=65535 Len=0</td></tr><tr><td>293 476.501474</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1587 → 1934 [FIN, ACK] Seq=1131 Ack=1 Win=65535 Len=0</td></tr><tr><td>294 476.501536</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1934 → 1587 [ACK] Seq=1 Ack=1132 Win=64405 Len=0</td></tr><tr><td>295 476.541711</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1454 → 21 [ACK] Seq=173 Ack=1362 Win=64174 Len=0</td></tr><tr><td>296 476.561030</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 1934 → 1587 [FIN, ACK] Seq=1 Ack=1132 Win=64405 Len=0</td></tr><tr><td>297 476.561201</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 1587 → 1934 [ACK] Seq=1132 Ack=2 Win=65535 Len=0</td></tr><tr><td>620 534.787848</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 2118 → 2097 [FIN, ACK] Seq=239105 Ack=1 Win=65535 Len=0</td></tr><tr><td>621 534.787917</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 2097 → 2118 [ACK] Seq=1 Ack=239106 Win=65535 Len=0</td></tr><tr><td>622 534.788371</td><td>172.16.39.93</td><td>172.16.3.240</td><td>TCP</td><td>54 2097 → 2118 [FIN, ACK] Seq=1 Ack=239106 Win=65535 Len=0</td></tr><tr><td>623 534.789817</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 2118 → 2097 [ACK] Seq=239106 Ack=2 Win=65535 Len=0</td></tr></table> | 237 403.735946 | 172.16.3.240 | 172.16.39.93 | TCP | 60 4652 → 1654 [FIN, ACK] Seq=1517 Ack=1 Win=65535 Len=0 | 238 403.736017 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1654 → 4652 [ACK] Seq=1 Ack=1518 Win=65535 Len=0 | 239 403.736121 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1654 → 4652 [FIN, ACK] Seq=1 Ack=1518 Win=65535 Len=0 | 240 403.741744 | 172.16.3.240 | 172.16.39.93 | TCP | 60 4652 → 1654 [ACK] Seq=1518 Ack=2 Win=65535 Len=0 | 270 447.419304 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1137 → 1791 [FIN, ACK] Seq=2992 Ack=1 Win=65535 Len=0 | 271 447.419373 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1791 → 1137 [ACK] Seq=1 Ack=2993 Win=65464 Len=0 | 272 447.419475 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1791 → 1137 [FIN, ACK] Seq=1 Ack=2993 Win=65464 Len=0 | 273 447.419643 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1137 → 1791 [ACK] Seq=2993 Ack=2 Win=65535 Len=0 | 293 476.501474 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1587 → 1934 [FIN, ACK] Seq=1131 Ack=1 Win=65535 Len=0 | 294 476.501536 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1934 → 1587 [ACK] Seq=1 Ack=1132 Win=64405 Len=0 | 295 476.541711 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1454 → 21 [ACK] Seq=173 Ack=1362 Win=64174 Len=0 | 296 476.561030 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1934 → 1587 [FIN, ACK] Seq=1 Ack=1132 Win=64405 Len=0 | 297 476.561201 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1587 → 1934 [ACK] Seq=1132 Ack=2 Win=65535 Len=0 | 620 534.787848 | 172.16.3.240 | 172.16.39.93 | TCP | 60 2118 → 2097 [FIN, ACK] Seq=239105 Ack=1 Win=65535 Len=0 | 621 534.787917 | 172.16.39.93 | 172.16.3.240 | TCP | 54 2097 → 2118 [ACK] Seq=1 Ack=239106 Win=65535 Len=0 | 622 534.788371 | 172.16.39.93 | 172.16.3.240 | TCP | 54 2097 → 2118 [FIN, ACK] Seq=1 Ack=239106 Win=65535 Len=0 | 623 534.789817 | 172.16.3.240 | 172.16.39.93 | TCP | 60 2118 → 2097 [ACK] Seq=239106 Ack=2 Win=65535 Len=0 |
| 237 403.735946 | 172.16.3.240 | 172.16.39.93 | TCP | 60 4652 → 1654 [FIN, ACK] Seq=1517 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 238 403.736017 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1654 → 4652 [ACK] Seq=1 Ack=1518 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 239 403.736121 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1654 → 4652 [FIN, ACK] Seq=1 Ack=1518 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 240 403.741744 | 172.16.3.240 | 172.16.39.93 | TCP | 60 4652 → 1654 [ACK] Seq=1518 Ack=2 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 270 447.419304 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1137 → 1791 [FIN, ACK] Seq=2992 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 271 447.419373 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1791 → 1137 [ACK] Seq=1 Ack=2993 Win=65464 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 272 447.419475 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1791 → 1137 [FIN, ACK] Seq=1 Ack=2993 Win=65464 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 273 447.419643 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1137 → 1791 [ACK] Seq=2993 Ack=2 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 293 476.501474 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1587 → 1934 [FIN, ACK] Seq=1131 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 294 476.501536 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1934 → 1587 [ACK] Seq=1 Ack=1132 Win=64405 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 295 476.541711 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1454 → 21 [ACK] Seq=173 Ack=1362 Win=64174 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 296 476.561030 | 172.16.39.93 | 172.16.3.240 | TCP | 54 1934 → 1587 [FIN, ACK] Seq=1 Ack=1132 Win=64405 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 297 476.561201 | 172.16.3.240 | 172.16.39.93 | TCP | 60 1587 → 1934 [ACK] Seq=1132 Ack=2 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 620 534.787848 | 172.16.3.240 | 172.16.39.93 | TCP | 60 2118 → 2097 [FIN, ACK] Seq=239105 Ack=1 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 621 534.787917 | 172.16.39.93 | 172.16.3.240 | TCP | 54 2097 → 2118 [ACK] Seq=1 Ack=239106 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 622 534.788371 | 172.16.39.93 | 172.16.3.240 | TCP | 54 2097 → 2118 [FIN, ACK] Seq=1 Ack=239106 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 623 534.789817 | 172.16.3.240 | 172.16.39.93 | TCP | 60 2118 → 2097 [ACK] Seq=239106 Ack=2 Win=65535 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 分析 | 找到数据连接的命令，根据挥手报文的原则性质统计，共计四次。 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | 该 FTP 的连接模式是那种？为什么？ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 答案 | 该 FTP 的连接方式是 PASV 被动传输。 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 截图 | <table><tr><td>224 400.851141</td><td>172.16.3.240</td><td>172.16.39.93</td><td>FTP</td><td>74 Response: 200 Type set to A.</td></tr><tr><td>225 400.933248</td><td>172.16.39.93</td><td>172.16.3.240</td><td>FTP</td><td>60 Request: PASV</td></tr><tr><td>226 401.048537</td><td>172.16.3.240</td><td>172.16.39.93</td><td>TCP</td><td>60 21 → 1454 [ACK] Seq=851 Ack=77 Win=65459 Len=0</td></tr></table> | 224 400.851141 | 172.16.3.240 | 172.16.39.93 | FTP | 74 Response: 200 Type set to A. | 225 400.933248 | 172.16.39.93 | 172.16.3.240 | FTP | 60 Request: PASV | 226 401.048537 | 172.16.3.240 | 172.16.39.93 | TCP | 60 21 → 1454 [ACK] Seq=851 Ack=77 Win=65459 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 224 400.851141 | 172.16.3.240 | 172.16.39.93 | FTP | 74 Response: 200 Type set to A. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 225 400.933248 | 172.16.39.93 | 172.16.3.240 | FTP | 60 Request: PASV | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 226 401.048537 | 172.16.3.240 | 172.16.39.93 | TCP | 60 21 → 1454 [ACK] Seq=851 Ack=77 Win=65459 Len=0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 分析 | 根据截图我们可以看到，客户端命令为 PASV，故该 FTP 的连接方式是 PASV 被动传输。 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

三、在线捕获数据包实验

1. 阅读教材 P64-69 内容，熟悉 FTP 协议。



2. 完成 P51 的实例 2-1。

【实验内容】

1. 单击 Wireshark 工具栏左起第一个图标，在接口上开始侦听，片刻后停止侦听。

这时捕获的数据量有多少？

答：按照要求，结果如下图所示，从数据帧列表以及状态栏可知，总共共获取 1855 个数据包。

| | | | | | | |
|------|----------|---------------|---------------|-------|------|--------------------------------|
| 1848 | 7.734829 | fe80::54d0... | fe80::bc70... | SSDP | 456 | HTTP/1.1 200 OK |
| 1849 | 7.761439 | fe80::f872... | ff02::1:3 | LLMNR | 86 | Standard query 0x1804 A isatap |
| 1850 | 7.761510 | 172.18.152... | 224.0.0.252 | LLMNR | 66 | Standard query 0x1804 A isatap |
| 1851 | 7.793461 | 223.73.54.9 | 172.18.154... | UDP | 89 | 38015 → 12345 Len=47 |
| 1852 | 7.801438 | 172.18.154... | 223.73.54.9 | UDP | 1492 | 12345 → 38015 Len=1450 |
| 1853 | 7.801613 | 172.18.154... | 223.73.54.9 | UDP | 1492 | 12345 → 38015 Len=1450 |
| 1854 | 7.801748 | 172.18.154... | 223.73.54.9 | UDP | 1492 | 12345 → 38015 Len=1450 |
| 1855 | 7.830058 | fe80::e16c... | ff02::c | UDP | 1249 | 53344 → 3702 Len=1187 |

| | |
|----------|--------------------|
| 分组: 1855 | 已显示: 1855 (100.0%) |
|----------|--------------------|

2. 观察捕获数据的源 IP 地址和目的 IP 地址，这些数据是发出还是发过来的？选

择几个 IP 地址，查询这些 IP 地址的地理位置。

答：以下随机截选几个 IP 地址进行查询及分析：

例子 1：

| No. | Time | Source 源地址 | Destination 目的地址 | Protocol | Length | Info |
|-----|----------|---------------|------------------|----------|--------|------------------------|
| 537 | 4.750133 | 172.18.154.95 | 120.239.40.247 | UDP | 1491 | 12345 → 19525 Len=1449 |
| 538 | 4.750245 | 172.18.154.95 | 120.239.40.247 | UDP | 1494 | 12345 → 19525 Len=1452 |
| 542 | 4.750919 | 172.18.154.95 | 120.239.40.247 | UDP | 1494 | 12345 → 19525 Len=1452 |
| 543 | 4.750982 | 172.18.154.95 | 120.239.40.247 | UDP | 1494 | 12345 → 19525 Len=1452 |
| 544 | 4.751040 | 172.18.154.95 | 120.239.40.247 | UDP | 1493 | 12345 → 19525 Len=1451 |
| 545 | 4.751091 | 172.18.154.95 | 120.239.40.247 | UDP | 1494 | 12345 → 19525 Len=1452 |
| 546 | 4.751242 | 172.18.154.95 | 120.239.40.247 | UDP | 1491 | 12345 → 19525 Len=1449 |
| 547 | 4.751306 | 172.18.154.95 | 120.239.40.247 | UDP | 1492 | 12345 → 19525 Len=1450 |
| 550 | 4.751422 | 172.18.154.95 | 120.239.40.247 | UDP | 1491 | 12345 → 19525 Len=1449 |

分析：源地址为 172.18.154.95 目的地址为 120.239.40.247，由于源地址为本机地址，因此此时在发送数据。

经 www.ip138.com 查询结果如下：



ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:172.18.154.95

- 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

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:120.239.40.247

- 本站数据：广东省茂名市 移动
- 参考数据1：广东茂名 移动
- 参考数据2：中国 移动

例子2:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|----------------|----------|--------|-----------------------------|
| 590 | 4.788563 | 172.18.154.95 | 120.239.40.247 | UDP | | 89 12345 → 19525 Len=47 |
| 597 | 4.801592 | 172.18.154.95 | 223.73.54.9 | UDP | | 1491 12345 → 38015 Len=1449 |
| 598 | 4.801650 | 172.18.154.95 | 223.73.54.9 | UDP | | 1494 12345 → 38015 Len=1452 |
| 599 | 4.801695 | 172.18.154.95 | 223.73.54.9 | UDP | | 1494 12345 → 38015 Len=1452 |
| 601 | 4.855749 | 172.18.154.95 | 120.239.40.247 | UDP | | 1492 12345 → 19525 Len=1450 |
| 602 | 4.855827 | 172.18.154.95 | 120.239.40.247 | UDP | | 1494 12345 → 19525 Len=1452 |
| 603 | 4.855896 | 172.18.154.95 | 120.239.40.247 | UDP | | 1492 12345 → 19525 Len=1450 |
| 612 | 4.929871 | 172.18.154.95 | 223.73.54.9 | UDP | | 1491 12345 → 38015 Len=1449 |
| 613 | 4.930030 | 172.18.154.95 | 223.73.54.9 | UDP | | 1493 12345 → 38015 Len=1451 |

分析：源地址为 172.18.154.95 目的地址为 223.73.54.9，由于源地址为本机地址，因此此时在发送数据。

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:223.73.54.9

- 本站数据：广东省广州市 移动
- 参考数据1：广东广州 移动
- 参考数据2：中国 移动

例子3:



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|---------------|----------|--------|-------|
| 559 | 4.773290 | 120.239.40.247 | 172.18.154.95 | UDP | 91 | 19525 |
| 560 | 4.773334 | 120.239.40.247 | 172.18.154.95 | UDP | 90 | 19525 |
| 569 | 4.773971 | 120.239.40.247 | 172.18.154.95 | UDP | 141 | 19525 |
| 570 | 4.774004 | 120.239.40.247 | 172.18.154.95 | UDP | 91 | 19525 |
| 575 | 4.774297 | 120.239.40.247 | 172.18.154.95 | UDP | 91 | 19525 |

分析：源地址为 120.239.40.247，目的地址为 172.18.154.95，由于目的地址为本机地址，因此此时在接收数据。

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,在命令窗口进行运行

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：使用 ipconfig 指令，查询到所在网络网关地址为：172.18.155.254

以太网适配器 本地连接:

```
连接特定的 DNS 后缀 . . . . . : sysu.edu.cn
IPv6 地址 . . . . . : 2001:250:3002:4600:bc70:7ad5:6439:f61b
临时 IPv6 地址. . . . . : 2001:250:3002:4600:7d1d:d652:57b1:aa16
本地链接 IPv6 地址. . . . . : fe80::bc70:7ad5:6439:f61b%15
IPv4 地址 . . . . . : 172.18.154.95
子网掩码 . . . . . : 255.255.252.0
默认网关. . . . . : fe80::eda:41ff:fe1b:a263%15
                    172.18.155.254
```

执行 ping -r 6 -l 172.18.155.254，结果如下：

```
C:\Users\Administrator>ping -r 6 -l 200 172.18.155.254
```

```
正在 Ping 172.18.155.254 具有 200 字节的数据:
来自 172.18.155.254 的回复: 字节=200 时间=1ms TTL=255
    路由: 172.18.155.254
来自 172.18.155.254 的回复: 字节=200 时间=9ms TTL=255
    路由: 172.18.155.254
来自 172.18.155.254 的回复: 字节=200 时间=1ms TTL=255
    路由: 172.18.155.254
来自 172.18.155.254 的回复: 字节=200 时间=1ms TTL=255
    路由: 172.18.155.254
```

```
172.18.155.254 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 = 9ms, 平均 = 3ms
```

捕获数据包为：



| ip.addr == 172.18.155.254 | | | | | | | |
|---------------------------|-------------|----------------|----------------|----------|--------|---------------------|---|
| No. | Time | Source | Destination | Protocol | Length | Info | |
| 765518 | 4973.679947 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request | id=0x0001, seq=173/44288, ttl=64 (reply in 765519) |
| 765519 | 4973.681095 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply | id=0x0001, seq=173/44288, ttl=255 (request in 765518) |
| 765558 | 4974.681315 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request | id=0x0001, seq=174/44544, ttl=64 (reply in 765560) |
| 765560 | 4974.690965 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply | id=0x0001, seq=174/44544, ttl=255 (request in 765558) |
| 765636 | 4975.684429 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request | id=0x0001, seq=175/44800, ttl=64 (reply in 765637) |
| 765637 | 4975.685442 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply | id=0x0001, seq=175/44800, ttl=255 (request in 765636) |
| 765661 | 4976.686379 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request | id=0x0001, seq=176/45056, ttl=64 (reply in 765662) |
| 765662 | 4976.687438 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply | id=0x0001, seq=176/45056, ttl=255 (request in 765661) |
| 725106 | 4667.094570 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply | id=0x0001, seq=169/43264, ttl=255 (request in 725105) |

执行 ping -s 4 -l 172.18.155.254，结果如下：

```
C:\Users\Administrator>ping -s 4 -l 200 172.18.155.254

正在 Ping 172.18.155.254 具有 200 字节的数据:
来自 172.18.155.254 的回复: 字节=200 时间=1ms TTL=255
    时间戳: 172.18.155.254 : 47452575 ->
                172.18.154.95 : 18673331
来自 172.18.155.254 的回复: 字节=200 时间=1ms TTL=255
    时间戳: 172.18.155.254 : 47453580 ->
                172.18.154.95 : 18674335
来自 172.18.155.254 的回复: 字节=200 时间=1ms TTL=255
    时间戳: 172.18.155.254 : 47454585 ->
                172.18.154.95 : 18675340
来自 172.18.155.254 的回复: 字节=200 时间=1ms TTL=255
    时间戳: 172.18.155.254 : 47455587 ->
                172.18.154.95 : 18676342

172.18.155.254 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 = 1ms, 平均 = 1ms
```

捕获数据包为：

| ip.addr == 172.18.155.254 | | | | | | | |
|---------------------------|-------------|----------------|----------------|----------|--------|---------------------|---|
| No. | Time | Source | Destination | Protocol | Length | Info | |
| 846114 | 5557.411873 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request | id=0x0001, seq=177/45312, ttl=64 (reply in 846115) |
| 846115 | 5557.412798 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply | id=0x0001, seq=177/45312, ttl=255 (request in 846114) |
| 846209 | 5558.415973 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request | id=0x0001, seq=178/45568, ttl=64 (reply in 846210) |
| 846210 | 5558.417089 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply | id=0x0001, seq=178/45568, ttl=255 (request in 846209) |
| 846257 | 5559.420972 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request | id=0x0001, seq=179/45824, ttl=64 (reply in 846258) |
| 846258 | 5559.422000 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply | id=0x0001, seq=179/45824, ttl=255 (request in 846257) |
| 846332 | 5560.423001 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request | id=0x0001, seq=180/46080, ttl=64 (reply in 846333) |
| 846333 | 5560.424122 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply | id=0x0001, seq=180/46080, ttl=255 (request in 846332) |

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

答：



| ip.addr == 172.18.155.254 | | | | | | |
|---------------------------|-------------|----------------|----------------|----------|--------|---|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 765518 | 4973.679947 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request id=0x0001, seq=173/44288, ttl=64 (reply in 765519) |
| 765519 | 4973.681095 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply id=0x0001, seq=173/44288, ttl=255 (request in 765518) |
| 765558 | 4974.681315 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request id=0x0001, seq=174/44544, ttl=64 (reply in 765560) |
| 765560 | 4974.690965 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply id=0x0001, seq=174/44544, ttl=255 (request in 765558) |
| 765636 | 4975.684429 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request id=0x0001, seq=175/44800, ttl=64 (reply in 765637) |
| 765637 | 4975.685442 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply id=0x0001, seq=175/44800, ttl=255 (request in 765636) |
| 765661 | 4976.686379 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request id=0x0001, seq=176/45056, ttl=64 (reply in 765662) |
| 765662 | 4976.687438 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply id=0x0001, seq=176/45056, ttl=255 (request in 765661) |
| 725106 | 4667.094570 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply id=0x0001, seq=169/43264, ttl=255 (request in 725105) |

| ip.addr == 172.18.155.254 | | | | | | |
|---------------------------|-------------|----------------|----------------|----------|--------|---|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 846114 | 5557.411873 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request id=0x0001, seq=177/45312, ttl=64 (reply in 846115) |
| 846115 | 5557.412798 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply id=0x0001, seq=177/45312, ttl=255 (request in 846114) |
| 846209 | 5558.415973 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request id=0x0001, seq=178/45568, ttl=64 (reply in 846210) |
| 846210 | 5558.417089 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply id=0x0001, seq=178/45568, ttl=255 (request in 846209) |
| 846257 | 5559.420972 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request id=0x0001, seq=179/45824, ttl=64 (reply in 846258) |
| 846258 | 5559.422000 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply id=0x0001, seq=179/45824, ttl=255 (request in 846257) |
| 846332 | 5560.423001 | 172.18.154.95 | 172.18.155.254 | ICMP | 282 | Echo (ping) request id=0x0001, seq=180/46080, ttl=64 (reply in 846333) |
| 846333 | 5560.424122 | 172.18.155.254 | 172.18.154.95 | ICMP | 278 | Echo (ping) reply id=0x0001, seq=180/46080, ttl=255 (request in 846332) |

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。

协议有：ARP,TCP,UDP,IGMPv3,WSP,TLSv1, TLSv1.2, IGMPv2,MDNS,EAP,LLMNR,IPv6,ICMPv6,NBNS,HTTP/XML, SSDP,QUIC,DHCPv6,DB-LSP-DISC,ICMP 等。

在所截取的数据包中，没有发现 Stamp，只有 Echo。我们随机截取一组 Echo 请求和响应分组：

| No. | Time | Source | Destination | Protocol | Length | Info |
|--------|-------------|----------------|----------------|----------|--------|---|
| 765518 | 4973.679947 | 172.18.154.95 | 172.18.155.254 | ICMP | 270 | Echo (ping) request id=0x0001, seq=173/44288, ttl=64 (reply in 765519) |
| 765519 | 4973.681095 | 172.18.155.254 | 172.18.154.95 | ICMP | 270 | Echo (ping) reply id=0x0001, seq=173/44288, ttl=255 (request in 765518) |

从左到右的意思依次为：No 是指数据帧编号，Time 是指时间戳，Source 是指源地址，Destination 是指目标地址，Protocol 是指协议类型，Length 是指数据捕获长度。Info 里面的主要内容是表明该操作是响应还是请求，序列号，而 TTL 指定数据包被路由器丢弃之前允许通过的最大网段数量，是 IP 数据包在网络中可以转发的最大跳数(跃点数)，TTL 的最大值是 255，推荐值是 64。

如上图，其中编号为 765518 的为 Echo 的请求分组，编号为 765519 的为响应分组，找出它们的分组主干树状图如下所示：

| Wireshark · 分组 765518 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212 | |
|---|--|
| ▶ Frame 765518: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface 0 | |
| ▶ Ethernet II, Src: LcfcHefe_2a:57:c3 (68:f7:28:2a:57:c3), Dst: Hangzhou_1b:a2:63 (0c:da:41:1b:a2:63) | |
| ▶ Internet Protocol Version 4, Src: 172.18.154.95, Dst: 172.18.155.254 | |
| ▶ Internet Control Message Protocol | |



计算机网络实验报告

Wireshark · 分组 765519 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

- ▶ Frame 765519: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface 0
- ▶ Ethernet II, Src: Hangzhou_1b:a2:63 (0c:da:41:1b:a2:63), Dst: LcfcHefe_2a:57:c3 (68:f7:28:2a:57:c3)
- ▶ Internet Protocol Version 4, Src: 172.18.155.254, Dst: 172.18.154.95
- ▶ Internet Control Message Protocol

主要字段分析（彩色标记）：

Wireshark · 分组 765518 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

- Frame 765518 数据帧编号 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface 0
 - Interface id: 0 (\Device\NPF_{A53E4F33-8232-47F2-A2E7-8E71F5FA1207})
Interface name: \Device\NPF_{A53E4F33-8232-47F2-A2E7-8E71F5FA1207}
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Mar 27, 2018 13:01:29.543256000 中国标准时间
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1522126889.543256000 seconds
 - [Time delta from previous captured frame: 0.009209000 seconds]
 - [Time delta from previous displayed frame: 50.489958000 seconds]
 - [Time since reference or first frame: 4973.679947000 seconds] 时间戳

Wireshark · 分组 765518 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

- Frame 765518: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface 0
 - Interface id: 0 (\Device\NPF_{A53E4F33-8232-47F2-A2E7-8E71F5FA1207})
Interface name: \Device\NPF_{A53E4F33-8232-47F2-A2E7-8E71F5FA1207}
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Mar 27, 2018 13:01:29.543256000 中国标准时间
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1522126889.543256000 seconds 与上一包间隔时间
 - [Time delta from previous captured frame: 0.009209000 seconds]
 - [Time delta from previous displayed frame: 50.489958000 seconds]
 - [Time since reference or first frame: 4973.679947000 seconds]

Wireshark · 分组 765519 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

Arrival Time: Mar 27, 2018 13:01:29.544404000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1522126889.544404000 seconds
[Time delta from previous captured frame: 0.001148000 seconds]
[Time delta from previous displayed frame: 0.001148000 seconds]
[Time since reference or first frame: 4973.681095000 seconds]
Frame Number: 765519
Frame Length: 270 bytes (2160 bits)
Capture Length: 270 bytes (2160 bits) 捕获长度



计算机网络实验报告

Wireshark · 分组 765518 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

- ▶ Frame 765518: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface
- ▶ Ethernet II, Src: LcfcHefe_2a:57:c3 (68:f7:28:2a:57:c3), Dst: Hangzhou_1b:a2:63 (08:00:27:1b:a2:63)
 - ▶ Destination: Hangzhou_1b:a2:63 (08:00:27:1b:a2:63)
 - ▶ Source: LcfcHefe_2a:57:c3 (68:f7:28:2a:57:c3)
 - Type: IPv4 (0x0800)
- ▶ Internet Protocol Version 4, Src: 172.18.154.95, Dst: 172.18.155.254

源地址

目的地址

Wireshark · 分组 765518 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

- ▶ Flags: 0x00
 - 0... = Reserved bit: Not set
 - .0... = Don't fragment: Not set
 - ..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: ICMP (1) 协议类型

Wireshark · 分组 765518 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

- ▶ IP Option - End of Options List (EOL)
 - Type: 0

- ▶ Internet Control Message Protocol

Type: 8 (Echo (ping) request) 请求分组

Wireshark · 分组 765519 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

- ▶ IP Option - End of Options List (EOL)

- ▶ Internet Control Message Protocol

Type: 0 (Echo (ping) reply) 响应分组

Wireshark · 分组 765518 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xbd0f [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 173 (0x00ad)

Sequence number (LE): 44288 (0xad00)

序列号

Wireshark · 分组 765519 · wireshark_A53E4F33-8232-47F2-A2E7-8E71F5FA1207_20180327113835_a12212

Code: 0

Checksum: 0xc50f [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 173 (0x00ad)

Sequence number (LE): 44288 (0xad00)

[Request frame: 765518]

[Response time: 1.148 ms]

响应时间



【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？

用户可以通过查看系统进程，或者通过检查网络接口卡的工作模式是否为混杂模式来判断是否已经被嗅探。

2. 如何防范被嗅探？

1. 进行网络分段，尽量在网络中使用交换机和路由器。
2. 对在网络中传输的数据进行加密，在内部关键位置布置防火墙和 IDS，防止来自内部的嗅探。
3. 一次性口令设置。
4. 禁用杂错节点。

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

| 学号 | 学生 | 自评分 |
|----------|-----|-----|
| 16339021 | 回煜森 | 100 |
| 16339049 | 辛依繁 | 100 |
| 16343065 | 桑娜 | 100 |