|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院系 | 计算机学院 | 班 级 | 计算科学与技术（系统结构） | | 组长 | 喻一峰 |
| 学号 | 22336287 | 22336018 | |  |  |  |
| 学生 | 喻一峰 | 蔡可豪 | |  |  |  |

1. **实验报告如有雷同，雷同各方当次实验成绩均以0分计。**

**警示**

1. **当次小组成员成绩只计学号、姓名登录在下表中的。**
2. **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。**
3. **实验报告文件以PDF格式提交。**

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 | 该处标明了FTP Source即客户端的MAC地址，是00:14:2a:20:12:96 |
| 2 | 第1、2、3号报文的作用是什么？ |
| 答案 | 1号报文是客户端向服务器发送连接请求。  2号报文是服务器确认收到连接请求，并向客户端发送连接请求。  3号报文是客户端确认收到连接请求。 |
| 截图 |  |
| 分析 | SYN是建立连接标志，ACK是确认标志。这三条报文是经典的三次握手 |
| 3 | 该数据包中共有多少个TCP流？ |
| 答案 | 一共有91个TCP流 |
| 截图 |  |
| 分析 | 应用TCP过滤后，显示有91个TCP流。 |
| 4 | 用什么用户和密码登录成功？ |
| 答案 | 用户和密码都是wlx2008 |
| 截图 |  |
| 分析 | 从图中可以看出使用wlx2008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 | 命令连接是用来传输FTP命令的，由客户端向FTP服务器TCP的21端口发起。  数据连接是用来传输FTP数据的，由FTP服务器TCP的20端口向客户端发起。 |
| 截图 |  |
| 分析 | 从图中可以看出命令连接是客户端向FTP服务器TCP的21端口发起的，数据连接是FTP服务器TCP的20端口向客户端发起。 |
| 6 | 该FTP的连接模式是那种？为什么？ |
| 答案 | 是主动连接，因为是客户端提出数据传输请求，服务器主动与客户端建立了连接。 |
| 截图 |  |
| 分析 | 客户端发送了命令：PORT 172,16,39,73,5,97，随后服务器通过20端口连接到了1377端口发送数据。 |
| 7 | 最后四个报文的作用是什么？ |
| 答案 | 最后四个报文是TCP四次挥手的过程，作用是安全可靠地断开客户端与服务器的连接，并且确保所有数据已经安全传输并确认 |
| 截图 |  |
| 分析 | 客户端首先请求关闭（报文 207），服务器确认并随后请求关闭（报文 208 和 209），最后客户端确认（报文 210），连接成功关闭。 |
| 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 | 命令有16条（不含重复的则有10条）： USER：客户端向服务器提供用户名，用于登录。 PASS：客户端向服务器提供密码，用于验证用户的身份。 PORT：客户端向服务器提供用于数据连接的 IP 地址和端口号。 NLST：客户端请求服务器发送当前目录或指定目录下的文件名列表。 XMKD：客户端请求服务器创建一个新的目录。 RNFR：客户端指定一个准备重命名的文件。 RNTO：客户端将指定文件重命名为新的文件名。 STOR：客户端请求将文件上传到服务器。 RETR：客户端请求从服务器下载指定的文件。 QUIT：客户端请求结束 FTP 会话并断开连接。  应答有21条（不含重复的则有10条）： 220：服务器准备好，欢迎新的客户端连接。 331：用户名正确，需要密码以继续登录。 230：用户成功登录。 200：命令成功执行。 150：服务器准备好开始传输文件数据。 226：文件传输完成。 257：新目录已成功创建。 350：命令部分成功，需进一步操作。 250：请求的操作成功完成。 221：会话结束，服务器关闭控制连接。 |
| 截图 |  |
| 分析 | 通过过滤ftp，可以看到有图中这些ftp的命令及应答。 |

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

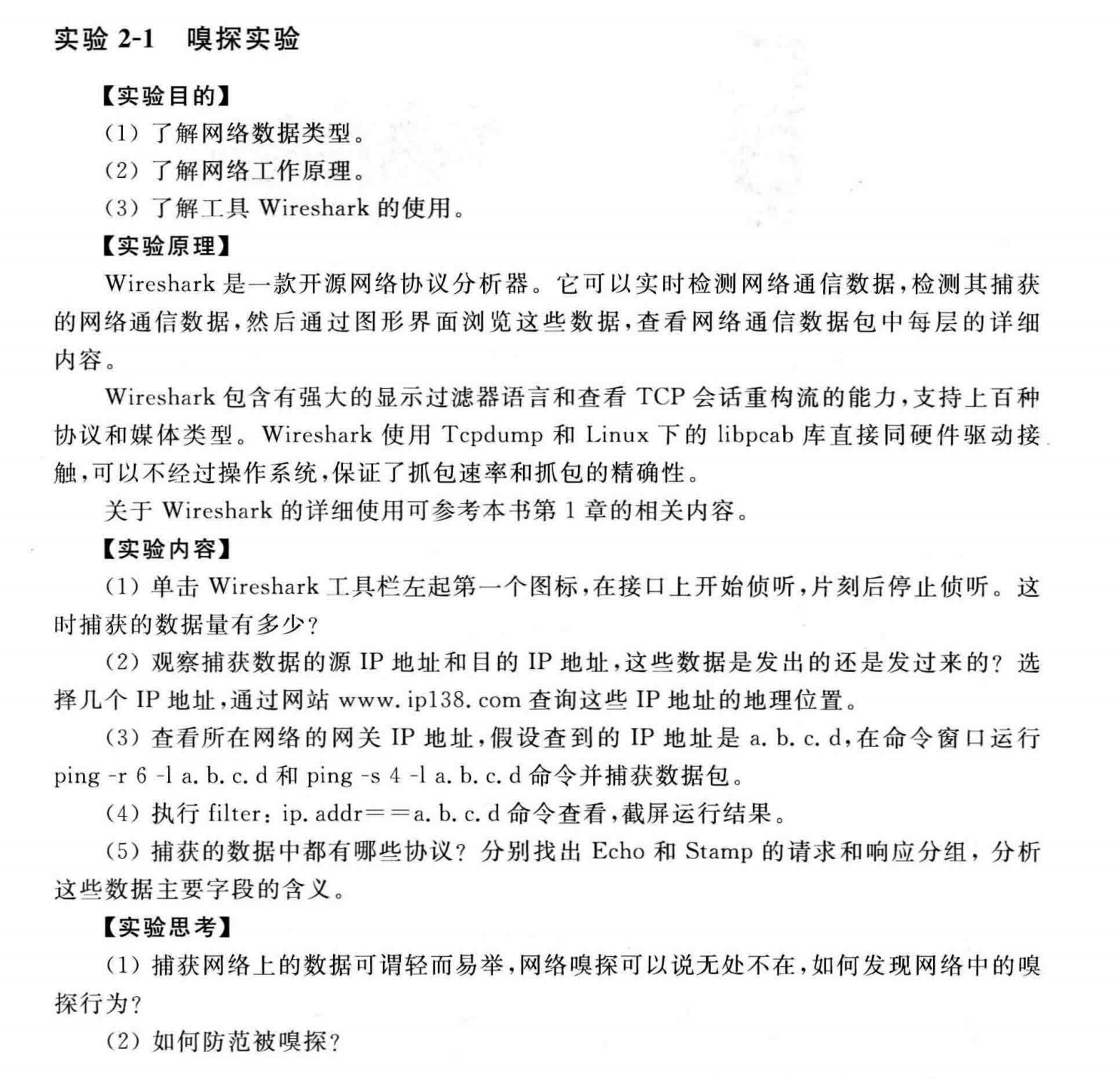
|  |  |
| --- | --- |
| 题号 |  |
| 1 | FTP服务器的ip是多少？FTP客户端的mac地址是多少？ |
| 答案 | FTP服务器的ip是172.16.3.240，FTP客户端的mac地址是00:14:2a:20:12:96 |
| 截图 |  |
| 分析 | 从图中可以看出服务器即Dst的ip，客户端即Source的mac地址。 |
| 2 | 该数据包中共有多少个TCP流？ |
| 答案 | 295 |
| 截图 |  |
| 分析 | 通过过滤TCP，可以看出一共有295个TCP流 |
| 3 | 最后用什么用户和密码登录成功？ |
| 答案 | 用户和密码都是kjdown |
| 截图 |  |
| 分析 | 从图中可看出，只有这个用户和密码，服务器端才显示登录成功，其他都是显示无法登录。 |
| 4 | 该FTP的命令连接和数据连接分别是什么？ |
| 答案 | 命令连接：客户端先向服务器的TCP 21端口发起建立连接标志，FTP服务器收到请求后，完成连接。  数据连接：FTP的命令连接建立之后，便可以开始进行文件处理或者数据传输。 |
| 截图 |  |
| 分析 | 从图中可以看到，进行了PASV的被动模式连接，进行了命令连接后对文件进行操作。 |
| 5 | 哪几个报文是FTP数据连接的三次握手报文？ |
| 答案 | 1、228、229、230号报文 2、256、257、258号报文 3、286、287、288号报文 4、324、325、326号报文 |
| 截图 |  |
| 分析 | 从四张截图中可以看到进行了经典的三次握手。 |
| 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、238、239、240号报文 2、270、271、272、273号报文 3、293、294、296、297号报文 4、620、621、622、623号报文 |
| 截图 |  |
| 分析 | 从四张截图可以看到有四次FPT数据连接的挥手报文，最后还有629、630、631、632号报文也是挥手报文，但不是数据连接的。 |
| 7 | 该FTP的连接模式是那种？为什么？ |
| 答案 | 是被动模式。因为客户端向服务器发送了PASV命令，随后服务器向客户端回复了进入被动模式。 |
| 截图 |  |
| 分析 | 图中可以看出是被动模式连接，并且打开了一个高级端口1454. |

**三、**在线捕获数据包实验

1. 阅读教材P64-69内容，熟悉FTP协议。

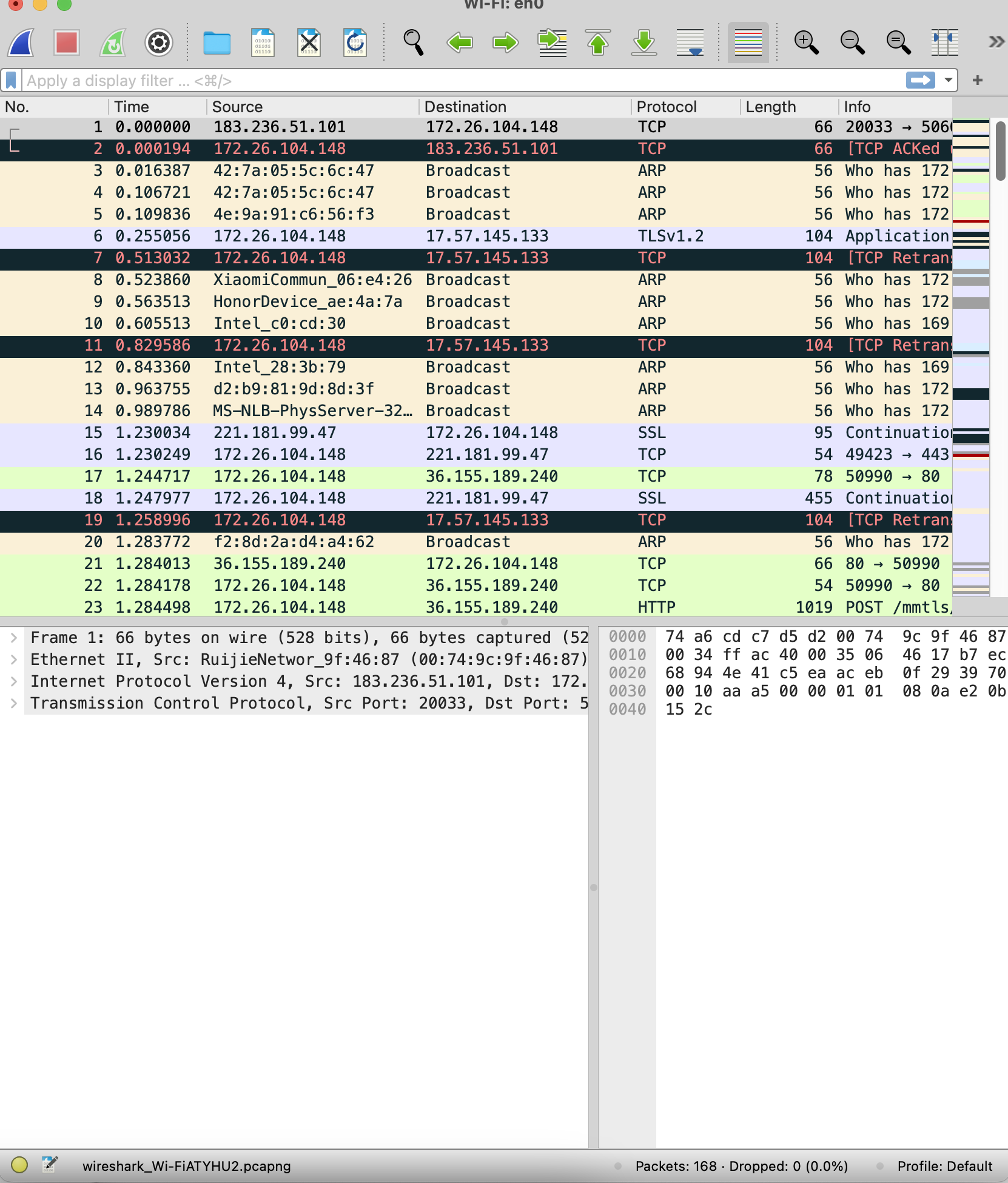
2. 完成P51的实例2-1。

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）

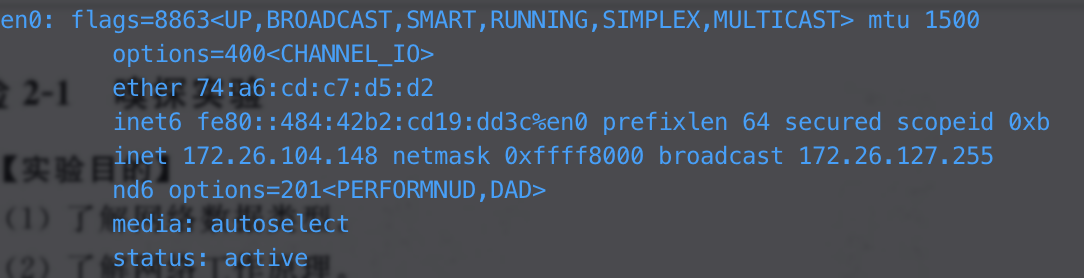
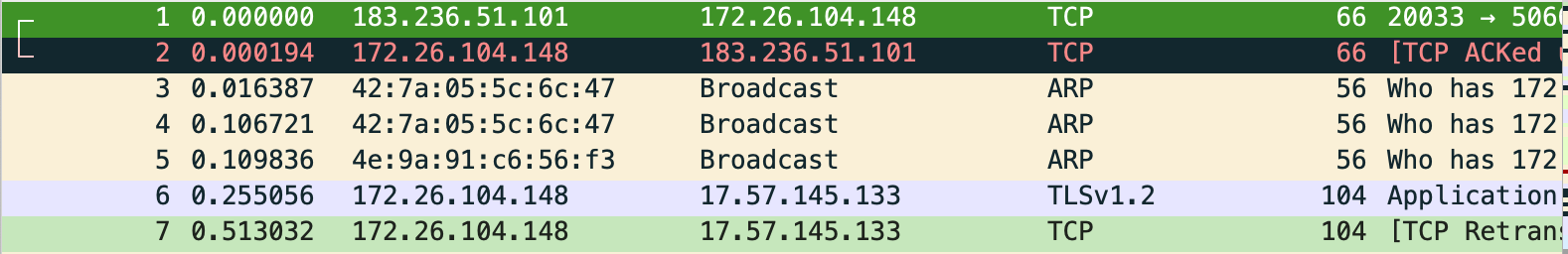


实验过程：

（1）168 个 packets。可以从下图的左下角获取到。



（2）查询 1、2、6、7 号 Packets，并且在使用 ifconfig 查询到主机的 ip 地址是 172.26.104.148。因此对于packet1，数据是接受的；对于 packet2，数据是发出的；对于 packet6 和 packet7，数据都是发出的。



172.26.104.148: 本地局域网 IP，广东移动

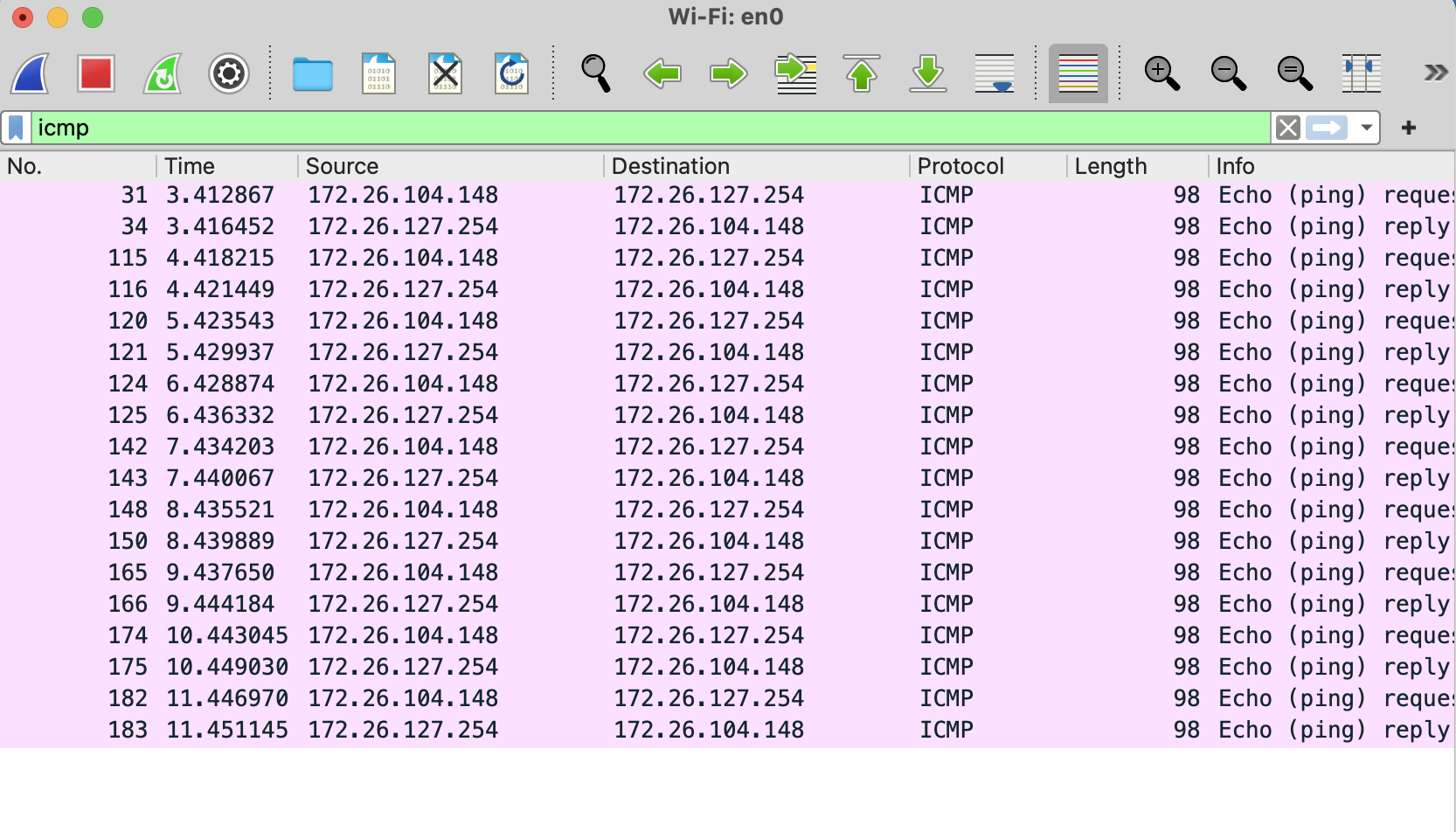
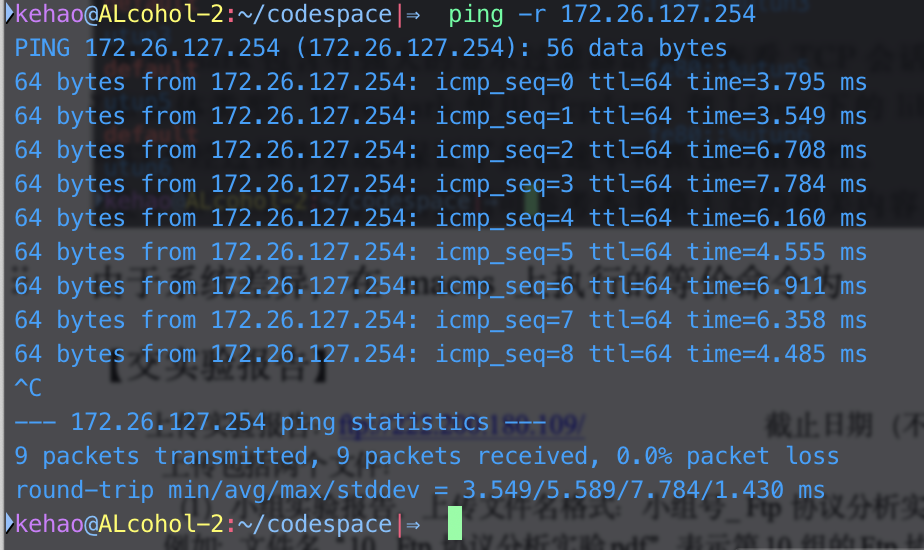
183.261.51.101：中国 广东省 广州市 移动

17.57.145.133：中国 台湾省 台北市 Apple

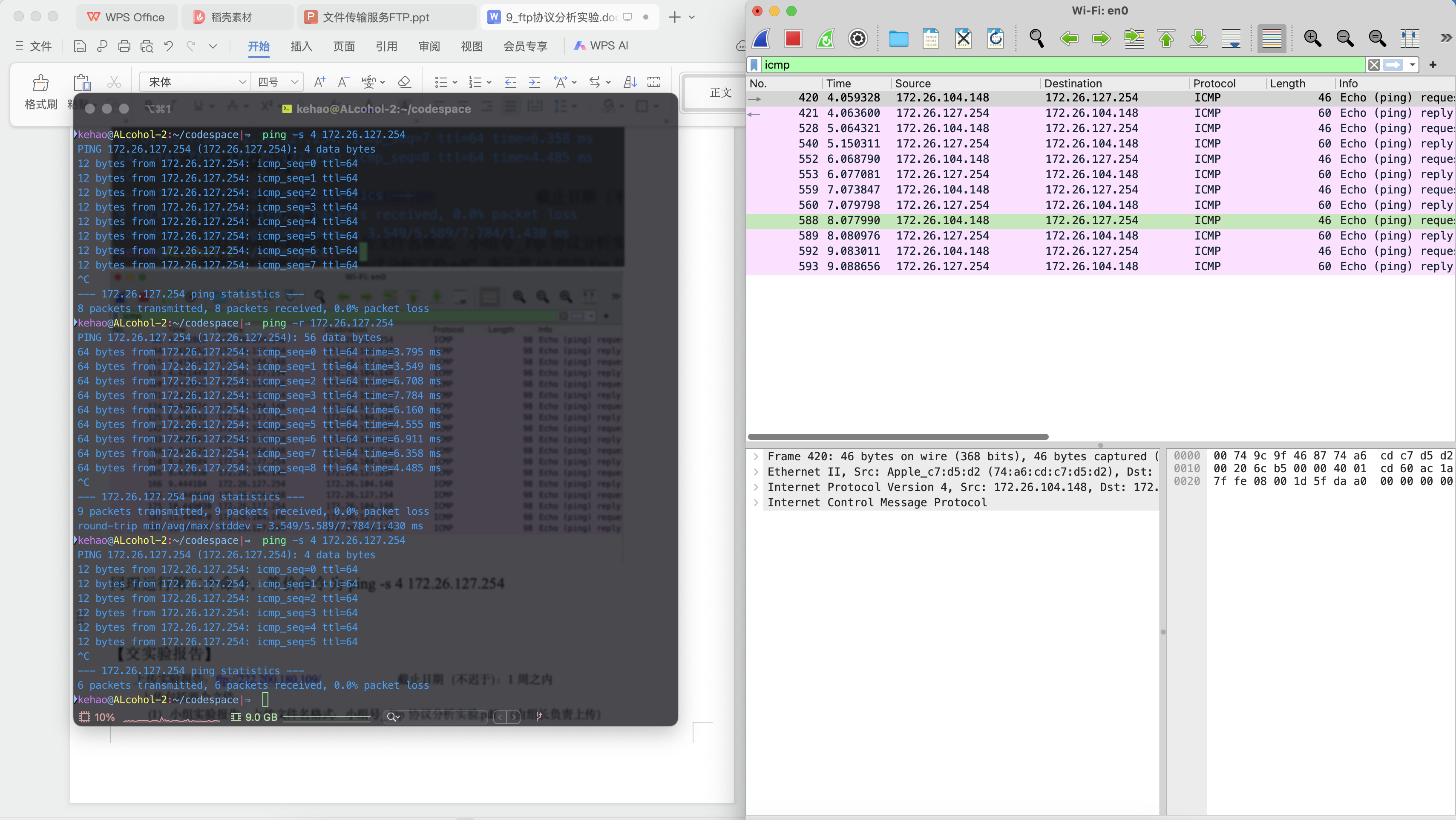
1. 使用命令查询并过滤信息，得到网关地址为 172.26.127.254



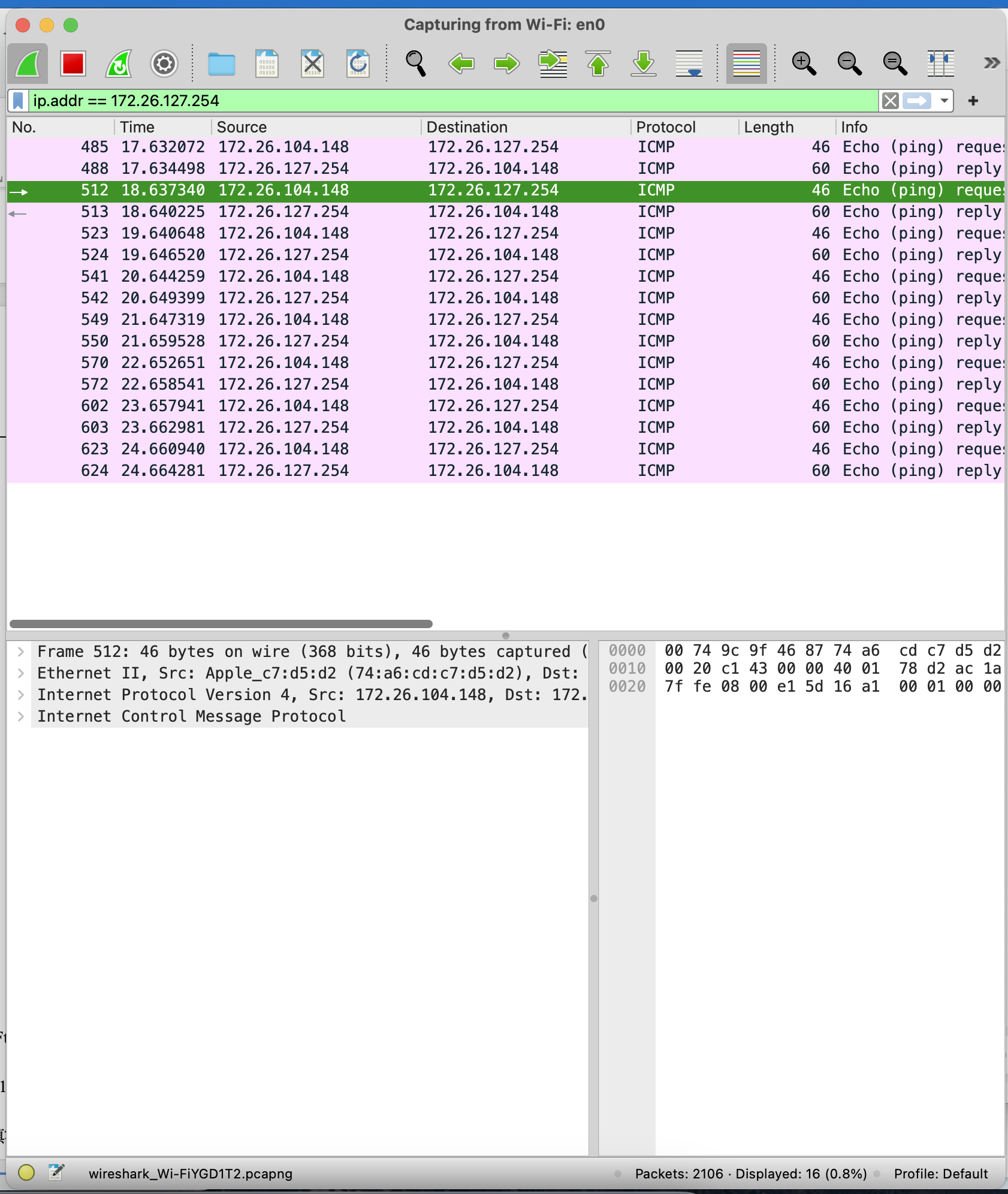
由于系统差异，在 macos 上执行的等价命令为ping -r a.b.c.d，后在 wireshark 中进行筛选捕获，关键词为icmp，即为 ping 所协议。



同理运行第二个命令，等价命令为ping -s 4 172.26.127.254，捕获结果如下。



1. 使用ip.addr == 172.26.127.254筛选结果如下



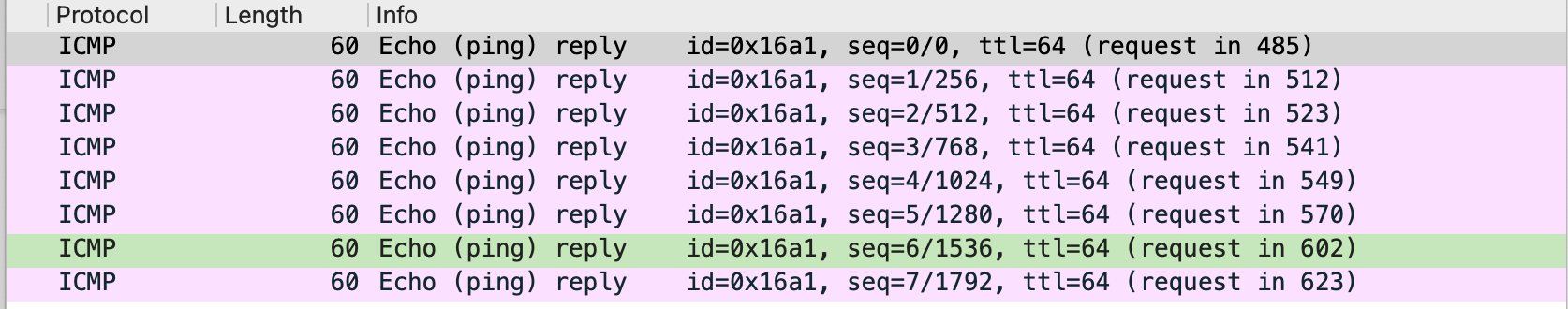
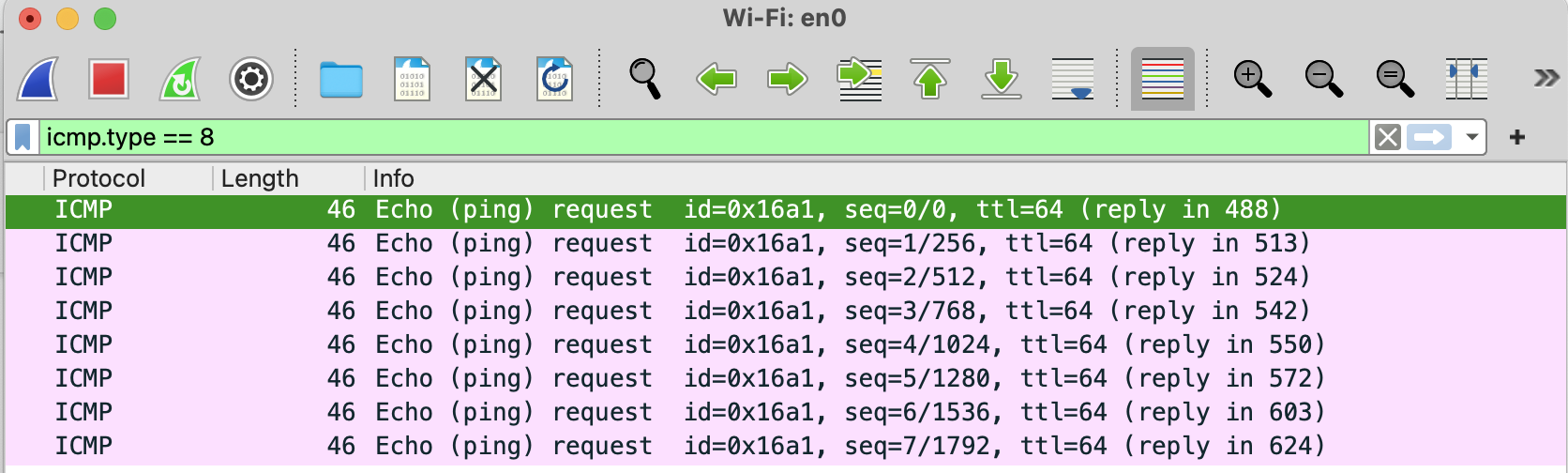
1. 所示协议均为 ICMP，因此可以使用如下四个命令来进行分组过滤  
   icmp.type == 8 // 用于查看 Echo Request

icmp.type == 0 // 用于查看 Echo Reply

icmp.type == 13 // 用于查看 Timestamp Request

icmp.type == 14 // 用于查看 Timestamp Reply

如下贴出过滤结果



后两个命令不存在数据。上网查询了一下，macos 部分发行版不支持发送 Timestamp Request and Reply，采取了更加安全的时间测量。而对于 Echo 组的字段解释如下

Echo Request 向目标设备发送请求数据包，等待其回应。帮助验证两者之间的网络连通性。

而 Echo Reply 是对 Echo Request 的应答，设备收到 Echo Request 之后，会返回一个 Echo Reply 消息。告知发送 Echo Request 的设备网络连接有效。

常规字段 source 和 destination 表示了发送 Request 的设备和接受连通性检验的设备IP 地址。

【实验思考】

1. 如何发现网络中的嗅探行为？

存在嗅探的时候，秀叹气一般会把网络接口卡设置为混杂模式-PROMISC，可以通过 ifconfig -a 来检查网卡的工作模式。

也可以查看系统日志，查看异常活频繁访问敏感端口的 IP 地址。

现成工具可以选择 Nmap 对服务器类设备进行扫描。

1. 如何防止被嗅探？

使用加密协议 https 或者 ssl/tls 技术保证信息安全。或者建立加密隧道 VPN，即虚拟专用网络，在公共网络上建立安全的通信通道，防止数据被嗅探。

更加常见的做法是配置防火墙。过滤非法流量且限制敏感访问。如有需要还可以自定义防火墙规则。

【交实验报告】

上传实验报告：<ftp://222.200.180.109/> 截止日期（不迟于）：1周之内

上传包括两个文件：

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

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

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

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

例如: 文件名“10\_05373092\_张三\_ Ftp协议分析实验.pdf”表示第10组的Ftp协议分析实验报告。

|  |  |  |
| --- | --- | --- |
| 学号 | 学生 | 自评分 |
| 22336287 | 喻一峰 | 100 |
| 22336018 | 蔡可豪 | 100 |
|  |  |  |
|  |  |  |
|  |  |  |

**注意：不要打包上传！**