

**本科实验报告**

|  |  |
| --- | --- |
| 课程名称： | 计算机网络基础 |
| 实验名称： | 网络协议分析 |
| 姓 名： | 姚熙源 |
| 学 院： | 计算机学院 |
| 系： | 计算机科学与技术 |
| 专 业： | 软件工程 |
| 学 号： | 3190300677 |
| 指导教师： | 董玮 |

2022年 5月 28日

**浙江大学实验报告**

实验名称： 网络协议分析 实验类型： 分析实验

同组学生： 实验地点： 计算机网络实验室

# 实验目的

* 进一步学习使用Wireshark抓包工具。
* 观察和理解常见网络协议的交互过程
* 理解数据包分层结构和格式。

# 实验内容

* 熟练掌握网络协议分析软件Wireshark的使用
* 观察所在网络出现的各类网络协议，了解其种类和分层结构
* 观察捕获到的数据包格式，理解各字段含义
* 根据要求配置Wireshark，捕获某一类协议的数据包，并分析解读

# 主要仪器设备

* 联网的PC机
* WireShark协议分析软件

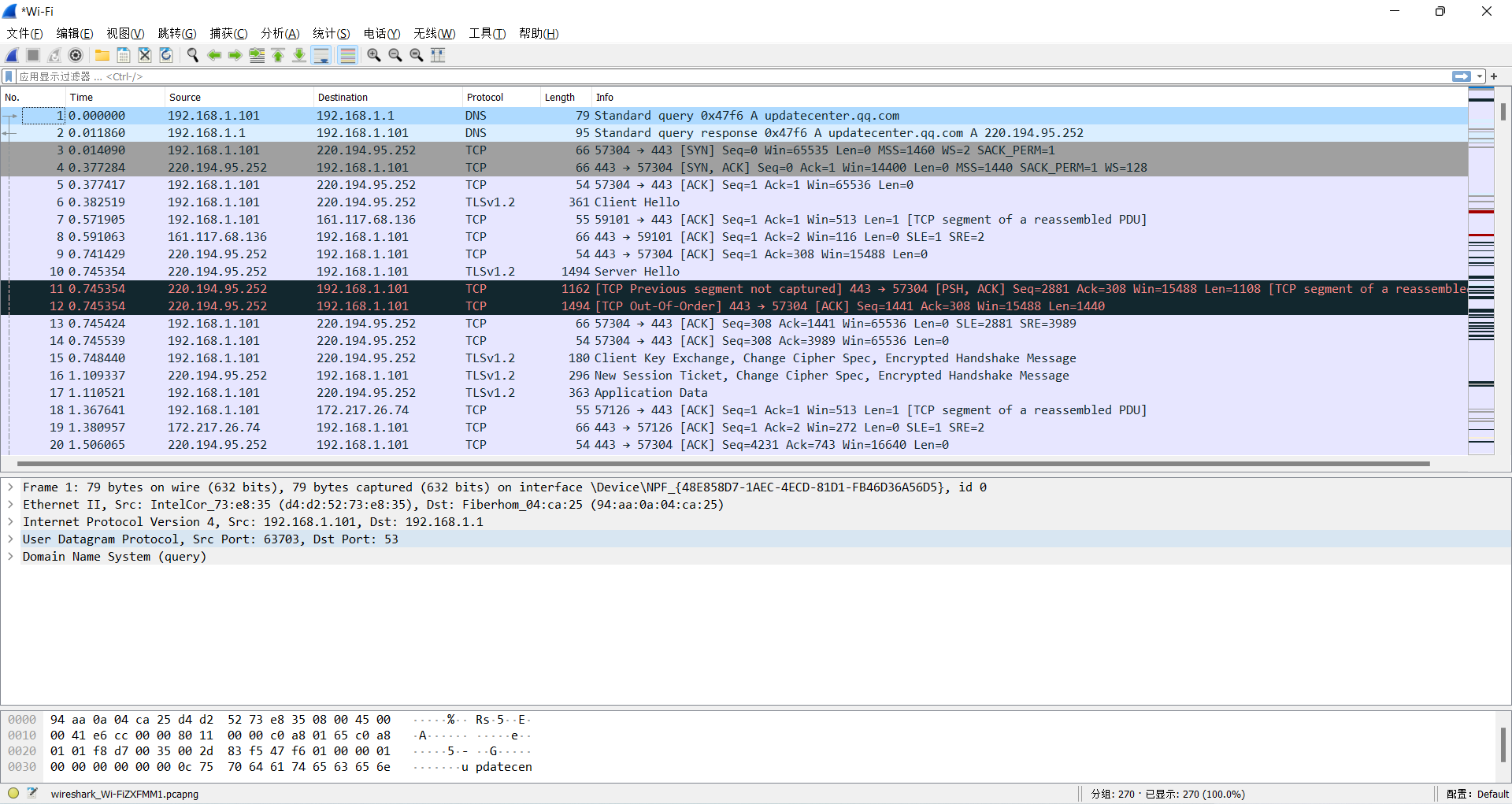
# 操作方法与实验步骤

* 配置网络包捕获软件，捕获所有机器的数据包
* 观察捕获到的数据包，并对照解析结果和原始数据包
* 配置网络包捕获软件，只捕获特定IP或特定类型的包
* 抓取以下通信协议数据包，观察通信过程和数据包格式
* PING：测试一个目标地址是否可达（在实验一基础上）
* TRACE ROUTE：跟踪一个目标地址的途经路由（在实验一基础上）
* NSLOOKUP：查询一个域名（在实验一基础上）
* HTTP：访问一个网页
* FTP：上传或下载一个文件
* SMTP：发送一封邮件
* POP3/IMAP：接收一封邮件
* RTP：抓取一段音频流

提醒：为了避免捕获到大量无关数据包，影响实验观察，建议关闭所有无关软件。

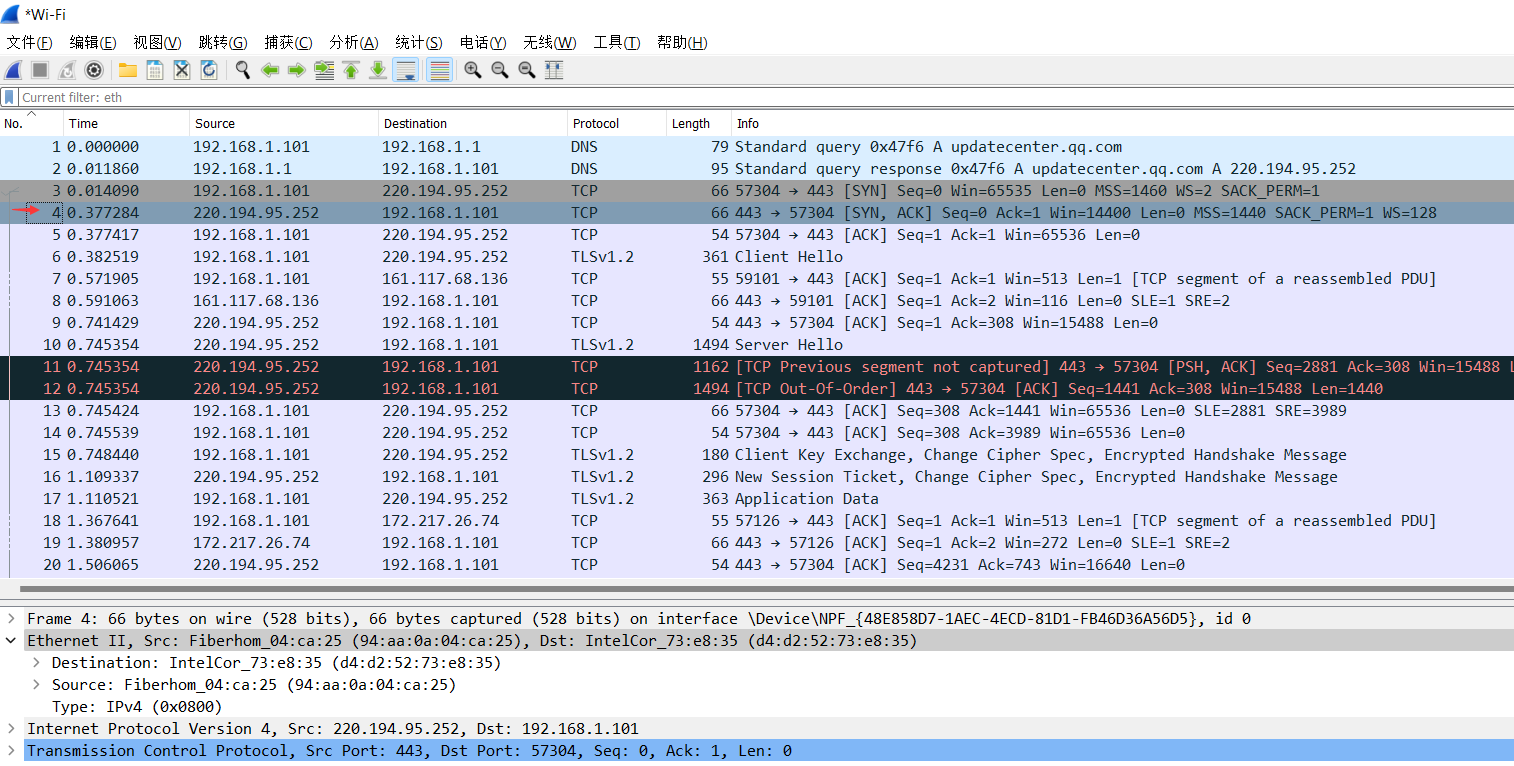
# 实验数据记录和处理

* Part One
* **打开WireShark，开始捕获网络数据包后，你看到了什么？有哪些协议？**



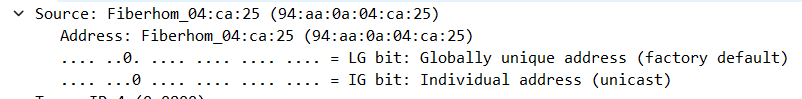
看到了很多的数据包不停地在发送和接收，可看到每个数据包的具体内容和解析。其中也包含很多种协议，有TCP、DNS、TLSv1.2、UDP、SSL、ARP、HTTP等协议。

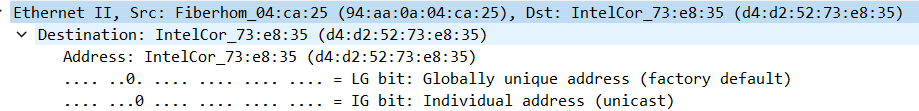
* **找一个包含Ethernet的数据包，这是什么协议？标出源和目标MAC地址。**



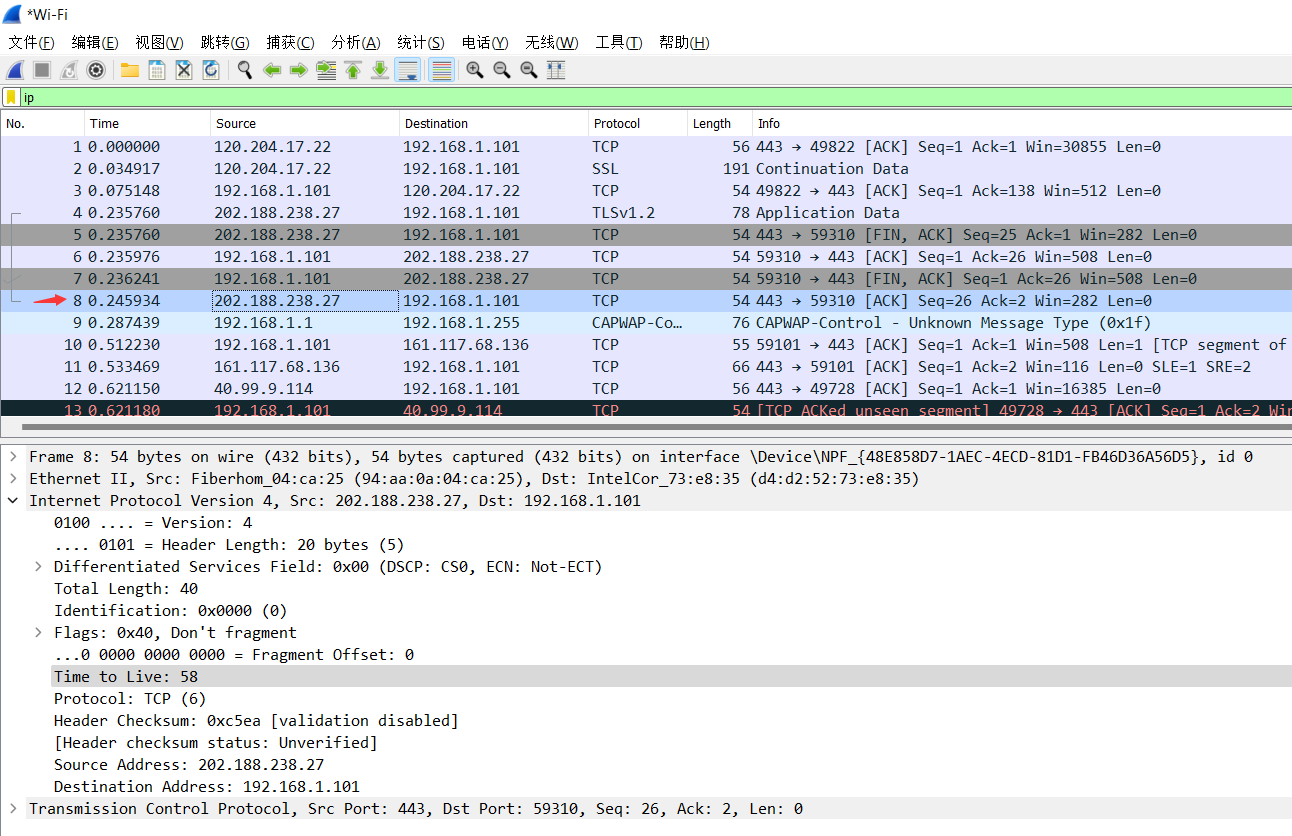
这是TCP协议。

源MAC地址：

 目标MAC地址：



* **找一个包含IP的数据包，这是什么协议？标出源IP地址、目标IP地址。**

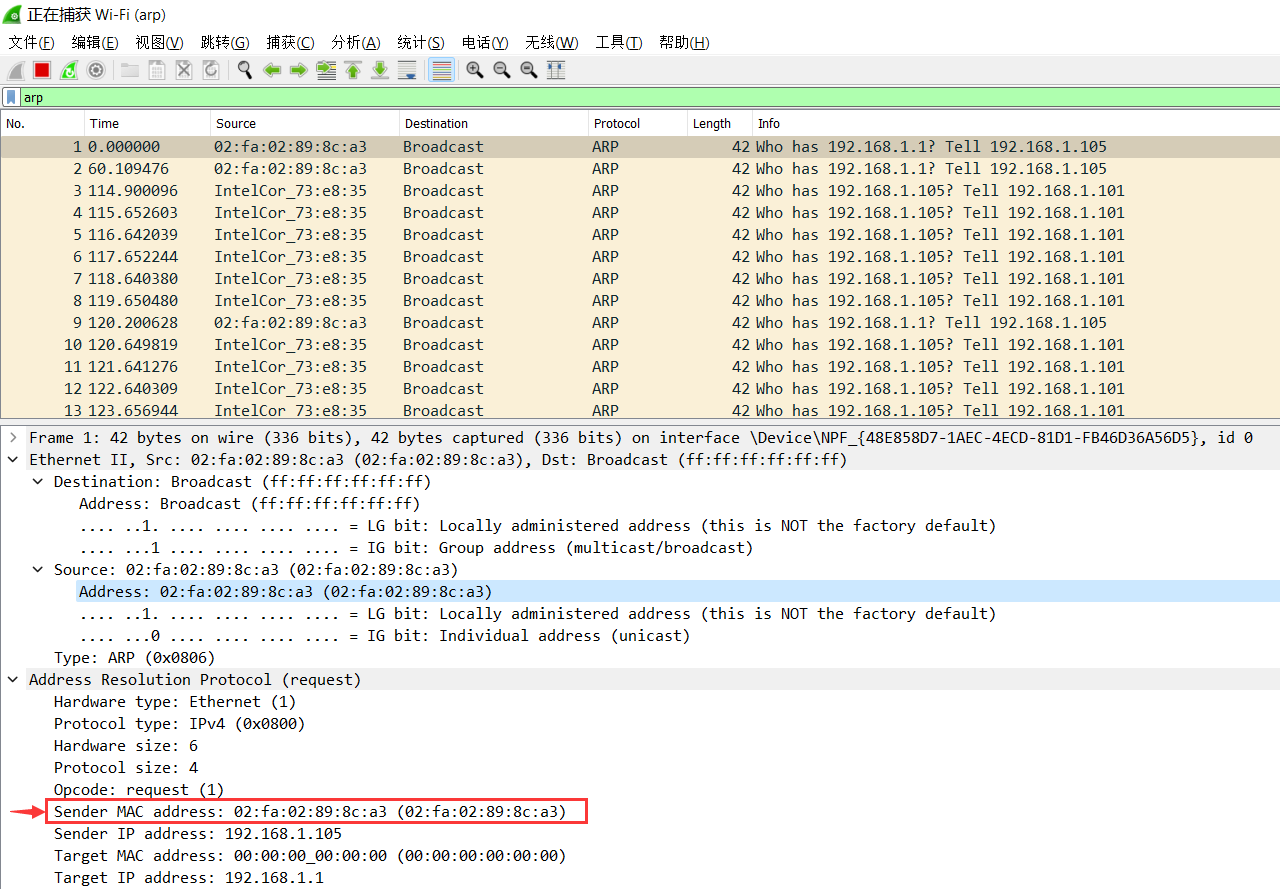


这是TCP协议

源IP地址：Source Address: 192.168.1.101

目标IP地址：Destination Address: 202.188.238.27

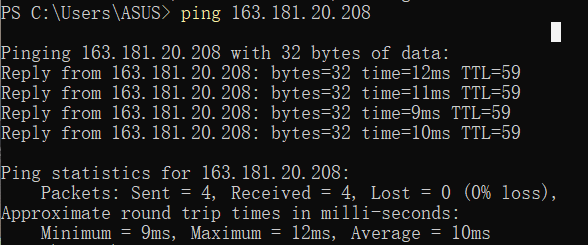
* **找一个ARP数据包，这是请求还是应答？标注发送者的MAC地址。**

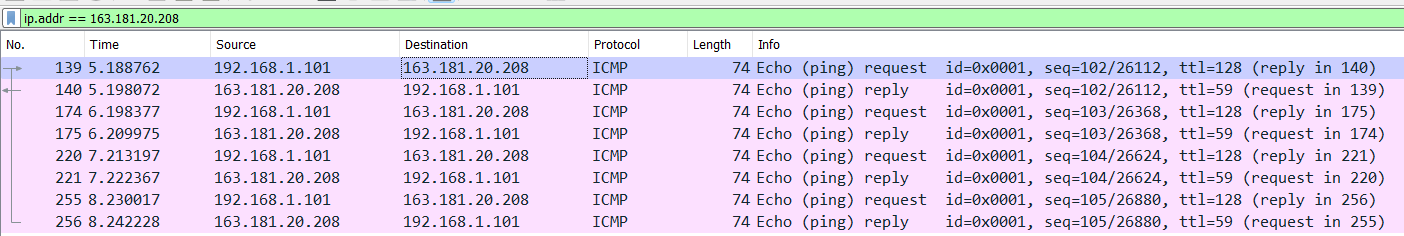


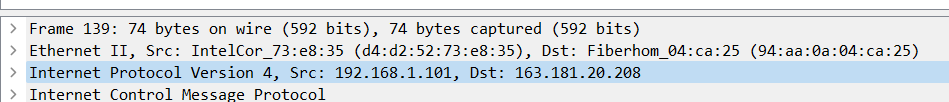
这是请求包，发送者的MAC地址已用红色框标注。

请在下面的每次捕获任务完成后，保存Wireshark抓包记录（.pcap格式），随报告一起提交。每一个协议一个单独文件，文件名请取得便于理解。

* Part Two
* **使用Ping命令，测试某个IP地址的连通性，并捕获这次的数据包。数据包由几层协议构成？分别是什么协议？选择一个请求包和一个响应包，展开最高层协议的详细内容，标出请求包和应答包、类型、序号。**

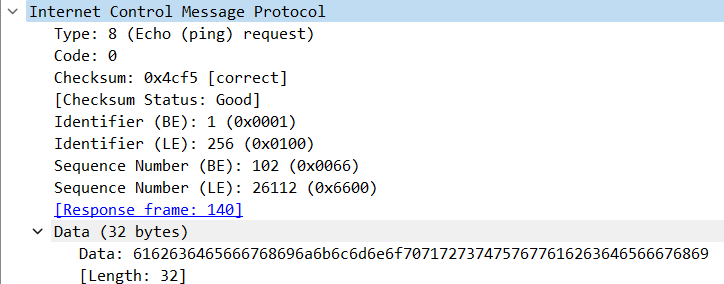




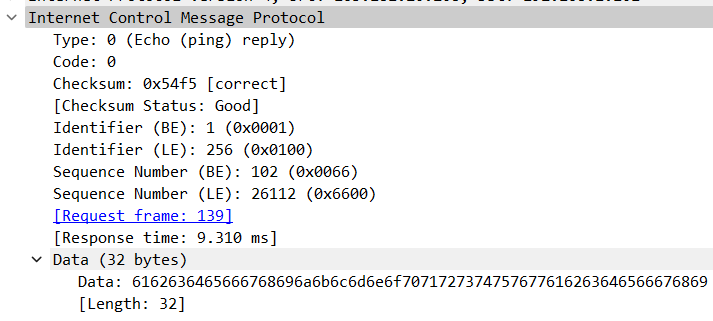


数据包由3层协议构成，分别是以太网协议、IPv4协议、ICMP协议

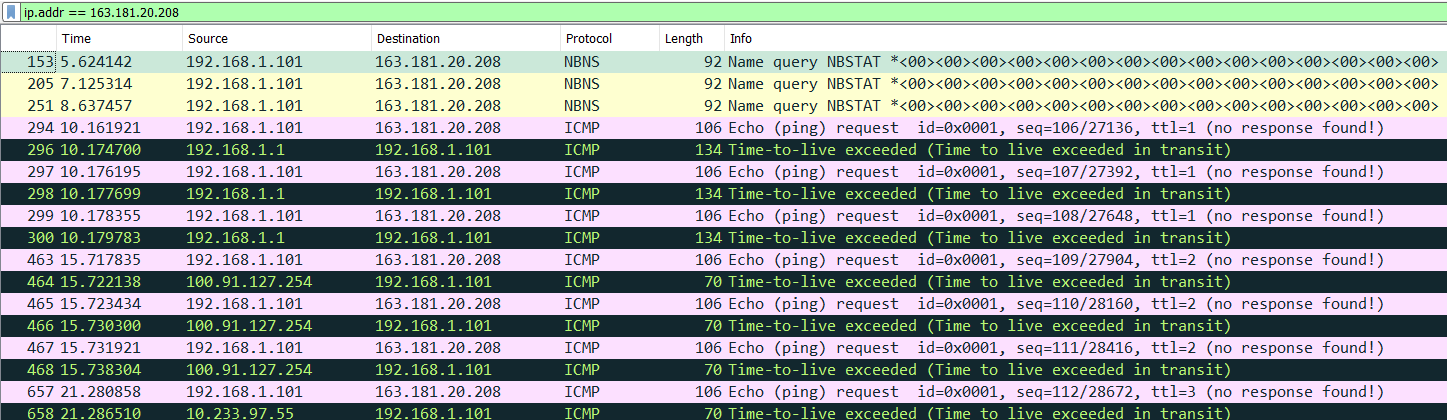
请求包，类型Type: 8(Echo (ping) request)，序号Sequence Number(BE): 102(0x0066)



响应包，类型Type: 0(Echo (ping) reply)，序号Sequence Number (BE): 102(0x0066)



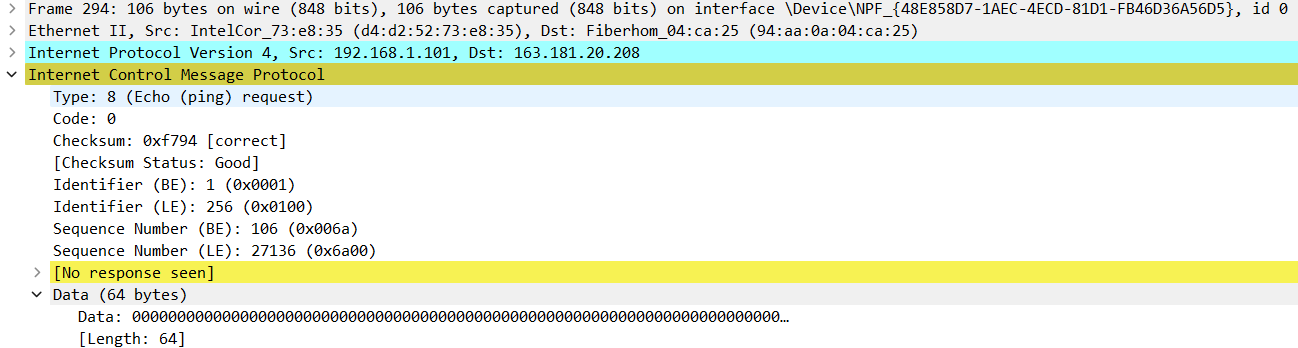
* **使用Tracert命令（Mac下使用Traceroute命令），跟踪某个外部IP地址的路由，并捕获这次的数据包。数据包由几层协议构成？分别是什么协议？查看并标记多个请求包的IP协议层的TTL字段，发现了什么规律？选择一个请求包和一个响应包，展开最高层协议的详细内容，标出类型、序号等关键字段。与Ping命令的数据包有什么不同？**



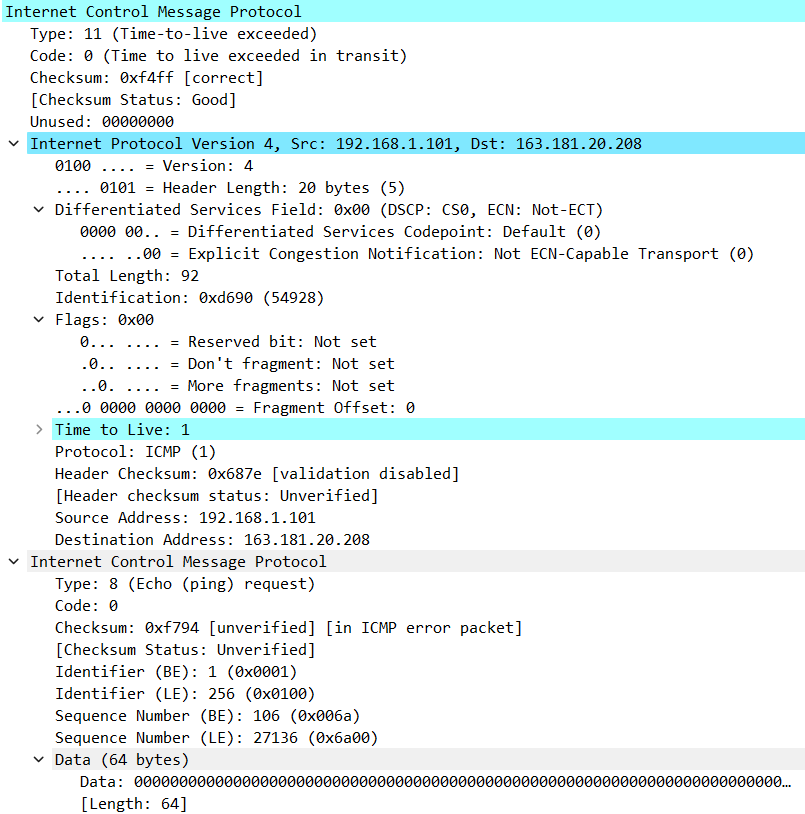
由3层协议构成，分别是以太网协议、IPv4协议和ICMP协议

TTL字段从1开始慢慢递增；

请求包，类型Type: 8 (Echo (ping) request)，序号Sequence Number (BE): 106(0x006a)

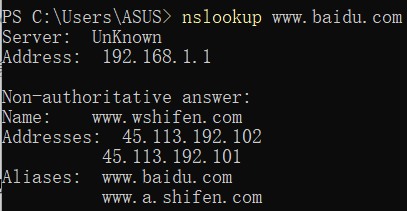


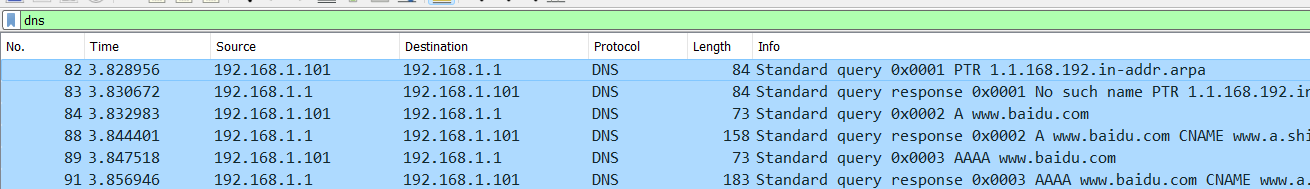
响应包，类型Type: 11 (Time-to-live exceeded)，序号Sequence Number(BE): 106(0x006a)



和ping命令的数据包相比，tracert命令的ICMP数据包data字段总是为0，响应包中包含了类型为11TTL降为0的超时信息。

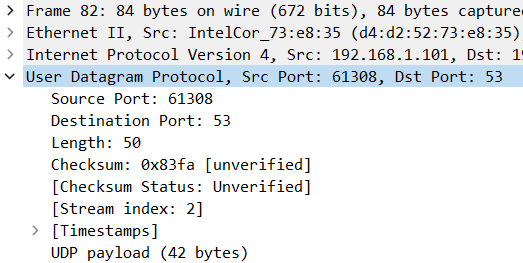
* **使用nslookup命令，查询某个域名，并捕获这次的数据包。数据包由几层协议构成？分别是什么协议？标记UDP协议层的端口字段。选择一个请求包和一个响应包，展开最高层协议的详细内容，标出类型、序号、域名信息。**



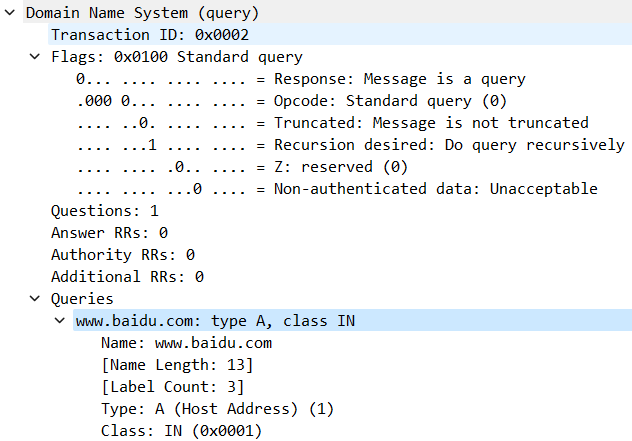


由4层协议构成，分别是以太网、IPv4、UDP、DN协议。

UDP协议层的端口字段



请求包

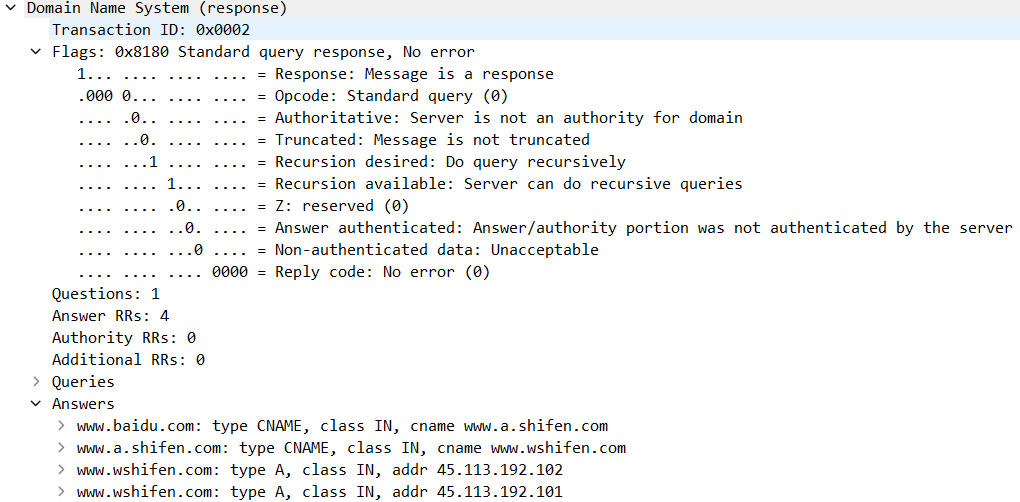


类型：Flags: 0x0100 Standard query

序号：Transaction ID: 0x0002

域名信息：www.baidu.com : type A, class IN

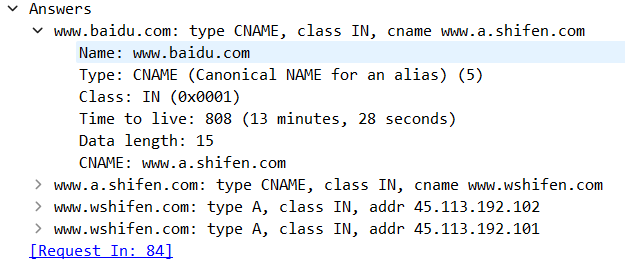
响应包



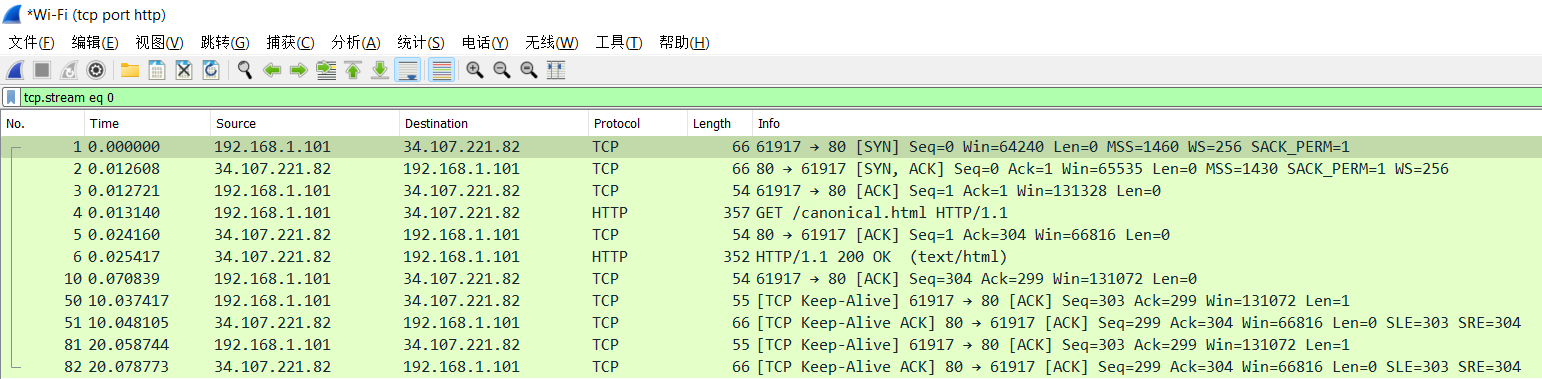
类型：Flags: 0x8180 Standard query response, No error

序号：Transaction ID: 0x0002

域名信息：



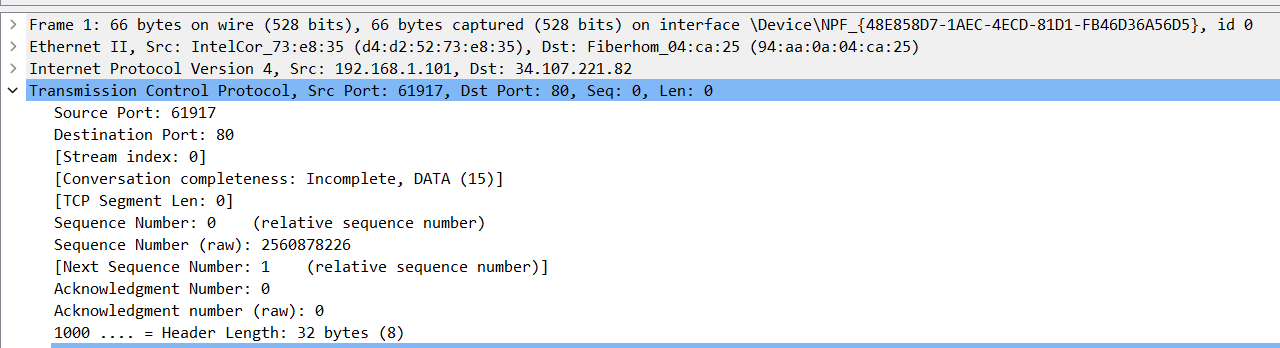
* Part Three
* **运行ipconfig /flushdns命令清空DNS缓存，然后打开浏览器，访问一个网页，并捕获这次的数据包（网页完全打开后，停止捕获）。数据包由几层协议构成？分别是什么协议？标出数据包的源和目标IP地址、源和目标端口。**



由4层协议构成，分别是以太网、IPv4、TCP、HTTP

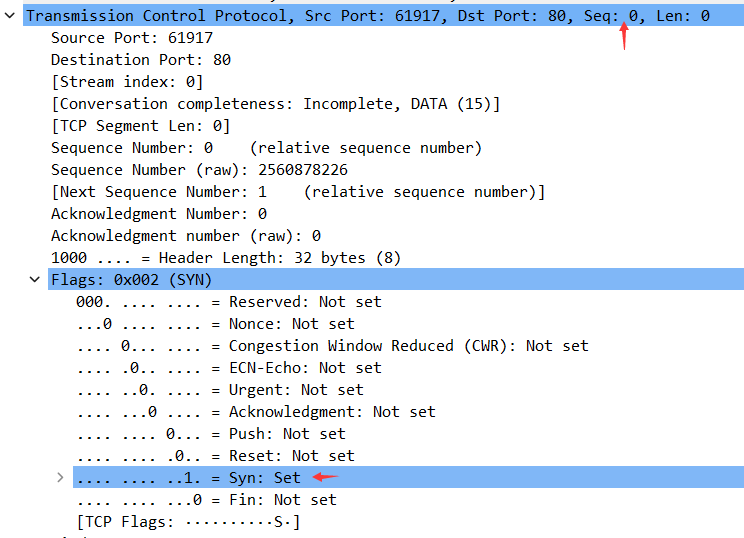
Source : 192.168.1.101 ; Port : 61917

Destination : 34.107.221.82 ; Port : 80

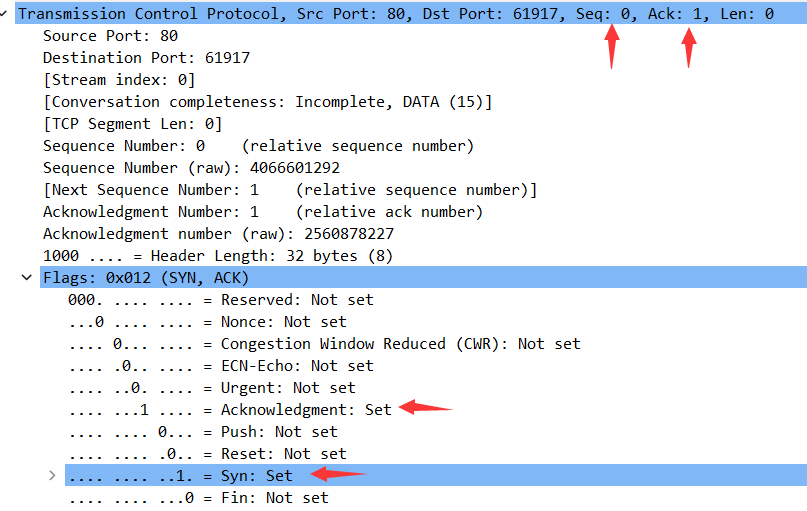


* **找到建立TCP连接的三个数据包（称为三次握手），展开TCP协议层的Flags字段，分别标记三个数据包的SYN标志位和ACK标志位。**

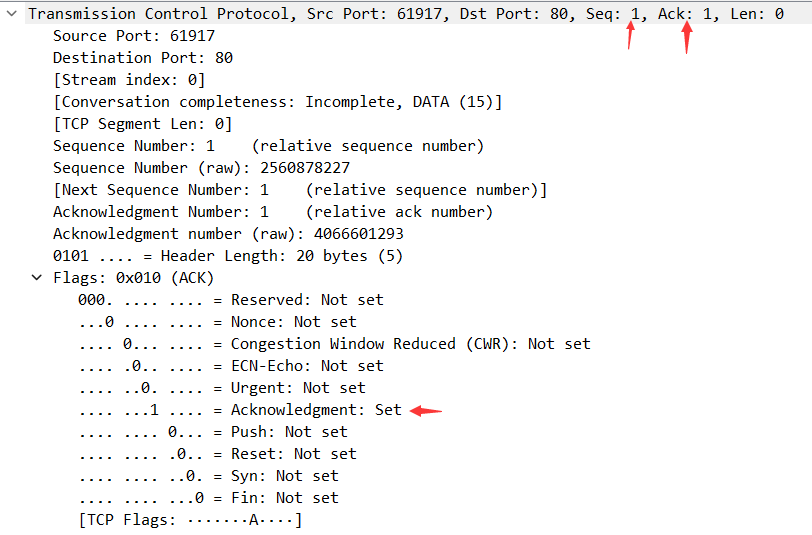
第一次握手，由port 61917向port 80发送第一个数据包，序号seq=0且syn标志位是Set状态。



第二次握手，由port 80向port 61917返回数据个数据包给我的ip，序号seq=0，ack=1(0+1)且ack和syn标志位是Set状态。



第三次握手，由port 61917向port 80返回数据包表示连接已建立，序号seq=1，ack=1(0+1)且Ack是Set状态表示双方的连接已经建立。



* **选择一个包，点击右键，选择跟踪一个TCP流，截取完整的HTTP请求消息和部分响应消息，标记HTTP请求头部的Method字段、URI字段和Host字段，标记HTTP响应头部的Status Code字段、Content-Type和Content-Length字段，以及区分响应头部和体部的标记（单独的回车换行符）。**

HTTP请求头部头部的Method字段、URI字段和Host字段：

GET /canonical.html HTTP/1.1

Host: detectportal.firefox.com

HTTP响应头部的Status Code字段、Content-Type和Content-Length字段

HTTP/1.1 200 OK

Content-Type: text/html

Content-Length: 90



* **使用过滤器tcp.stream eq X，让X从0开始变化，直到没有数据。观察总共捕获到了几个TCP连接（一个TCP流对应一个TCP连接）？存在几个HTTP会话（一对HTTP请求和响应对应一次HTTP会话）？注意：一个TCP流上可能存在多个HTTP会话。**

tcp.stream eq 0，9个TCP连接，1个HTTP请求和1个HTTP响应

tcp.stream eq 1，9个TCP连接，1个HTTP请求和1个HTTP响应

tcp.stream eq 2，9个TCP连接，1个OCSP请求和1个OCSP响应

tcp.stream eq 3，9个TCP连接，1个OCSP请求和1个OCSP响应

tcp.stream eq 4，9个TCP连接，1个OCSP请求和1个OCSP响应

tcp.stream eq 5，9个TCP连接，1个OCSP请求和1个OCSP响应

tcp.stream eq 6，7个TCP连接，1个OCSP请求和1个OCSP响应

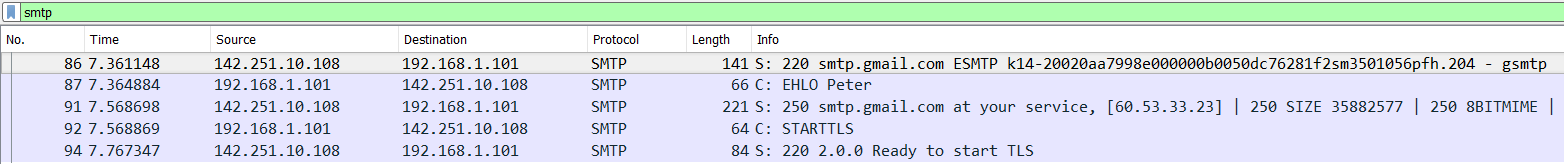
tcp.stream eq 7，9个TCP连接，2个OCSP请求和2个OCSP响应

tcp.stream eq 8，6个TCP连接

tcp.stream eq 9，6个TCP连接，1个HTTP请求和1个HTTP响应

总共捕获了82个TCP连接。

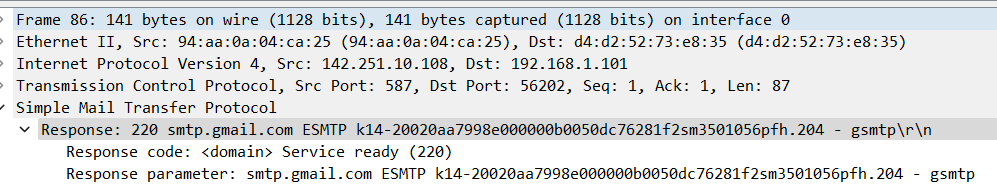
* Part Four
* **打开邮件客户端Foxmail或Outlook，写一封电子邮件（建议采用直接送达方式），并捕获这次的数据包。捕获到的数据包由几层协议构成？分别是什么协议？标出数据包的源和目标IP地址、源和目标端口。**



捕获到的数据包由4层协议构成，分别是以太网、IPv4、TCP、SMTP

Source : 142.251.10.108 ; Destination : 192.168.1.101

Source Port : 587 ; Destination Port : 56202



* **跟踪TCP流，查看SMTP握手消息采用的是什么（HELO还是EHLO）？标出SMTP协议层中的客户端机器名、发件人地址、收件人地址、认证的用户名和密码（如果是EHLO握手方式）、邮件正文（内容过长可截取关键部分）。**

由于我的ISP阻挡了port 25，所以捕获到的邮件是不允许不加密的，因此smtp服务器只能使用port587(TLS加密)，大部分的内容都是截图内容都是加密的。



SMTP握手消息采用的是EHLO。由于捕获到的数据包都是通过加密的，所以没办法看到发件人地址、收件人地址、认证的用户名和密码、邮件正文等，只能我手动添加这些内容了。

客户端机器名：Peter

发件人地址：[westcircle888@gmail.com、](mailto:westcircle888@gmail.com、)

收件人地址：[westcircle@163.com](mailto:westcircle@163.com)

认证用户名和密码：AUTH LOGIN

邮件正文：Lab6

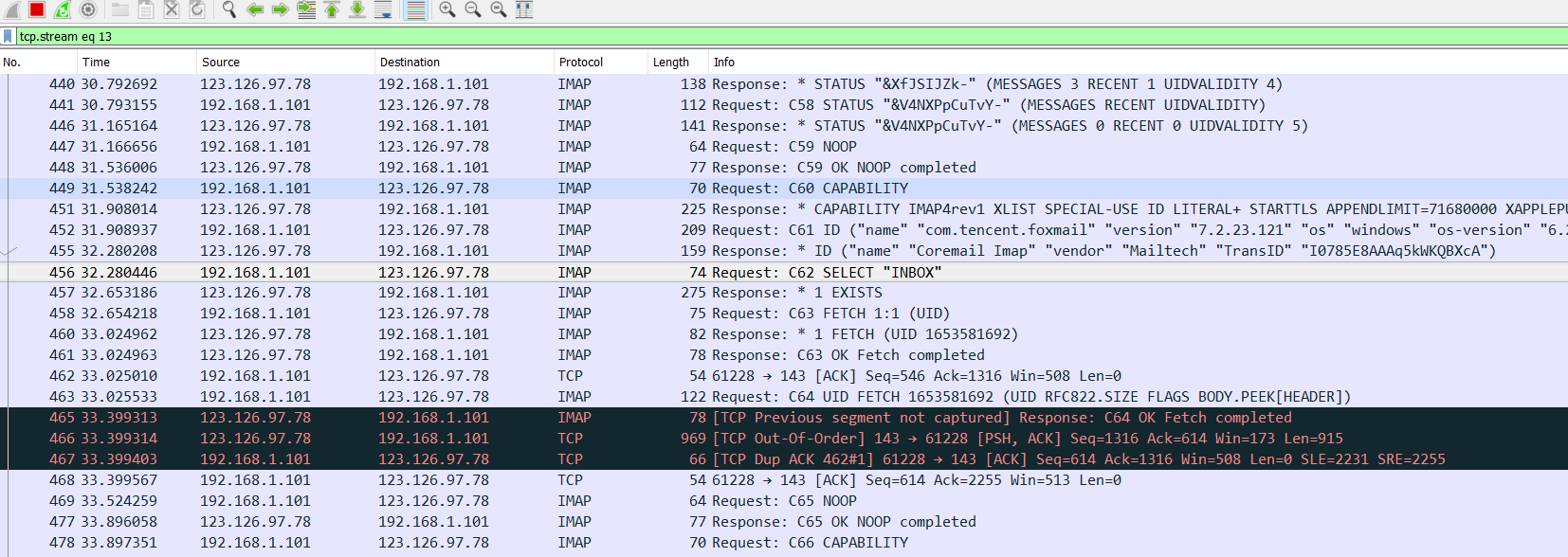


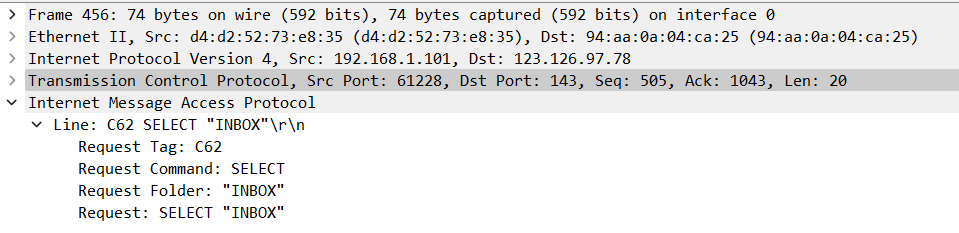
* **打开邮件客户端Foxmail或Outlook，收取自己邮箱中的邮件（请在邮件服务器中设置允许POP3或者IMAP），并捕获这次的数据包。捕获到的数据包由几层协议构成？分别是什么协议？标出数据包的源和目标IP地址、源和目标端口。**

在邮件服务器中设置了IMAP，使用其中一个邮箱发送邮件给另一个邮箱，并在另一个邮箱中收取邮件。捕获到的数据包是IMAP，由4层协议构成，分别是以太网、IPv4、TCP、IMAP

Source Port : 61228 ; Destination Port : 143

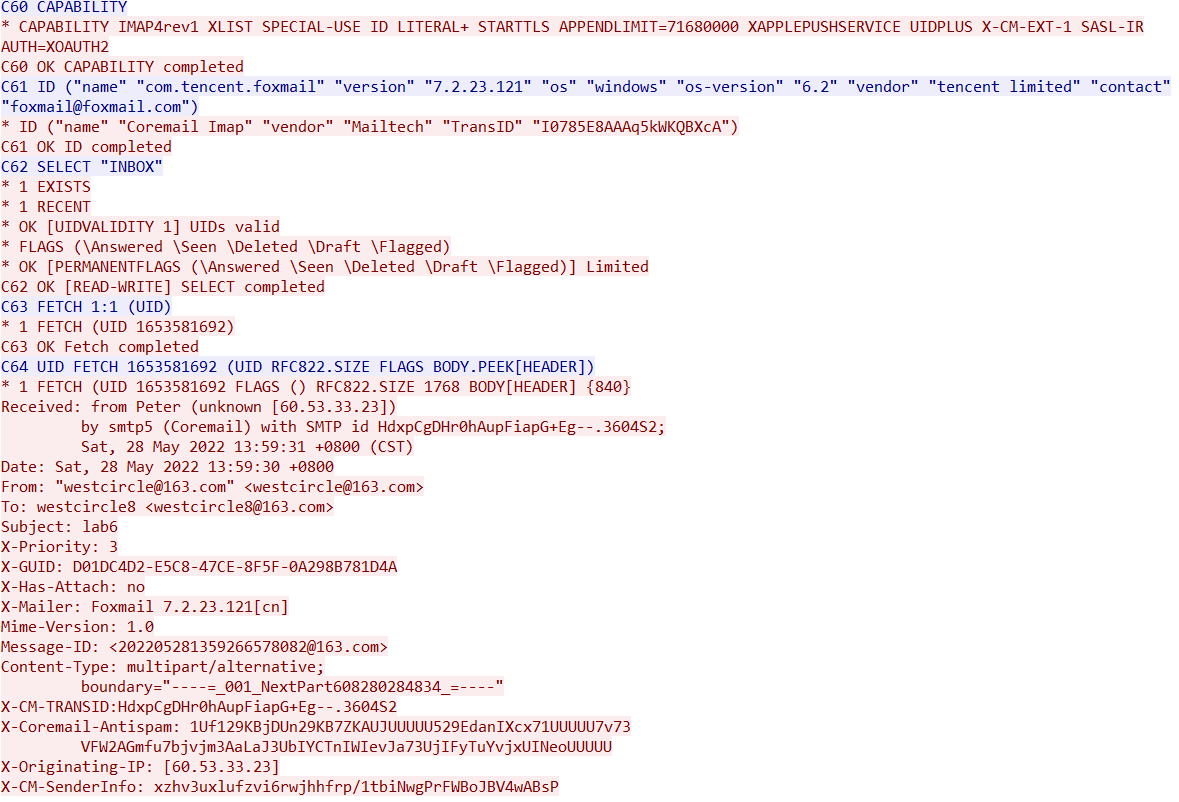
Source : 192.168.1.101 ; Destination : 123.126.97.78





* **跟踪TCP流，标出POP3或IMAP协议层中的认证用户名和密码、以及接收的邮件正文（内容过长可截取关键部分）。**

UID 1653581692，Received from : Peter(我的机器名)、From : [westcircle@163.com、To](mailto:westcircle@163.com、To) : [westcircle8@163.com](mailto:westcircle8@163.com)（收件人邮箱），邮件正文：lab6

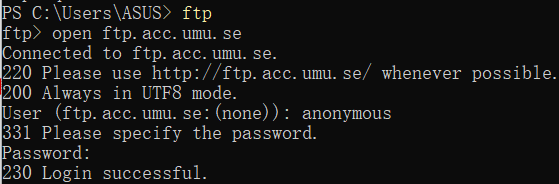


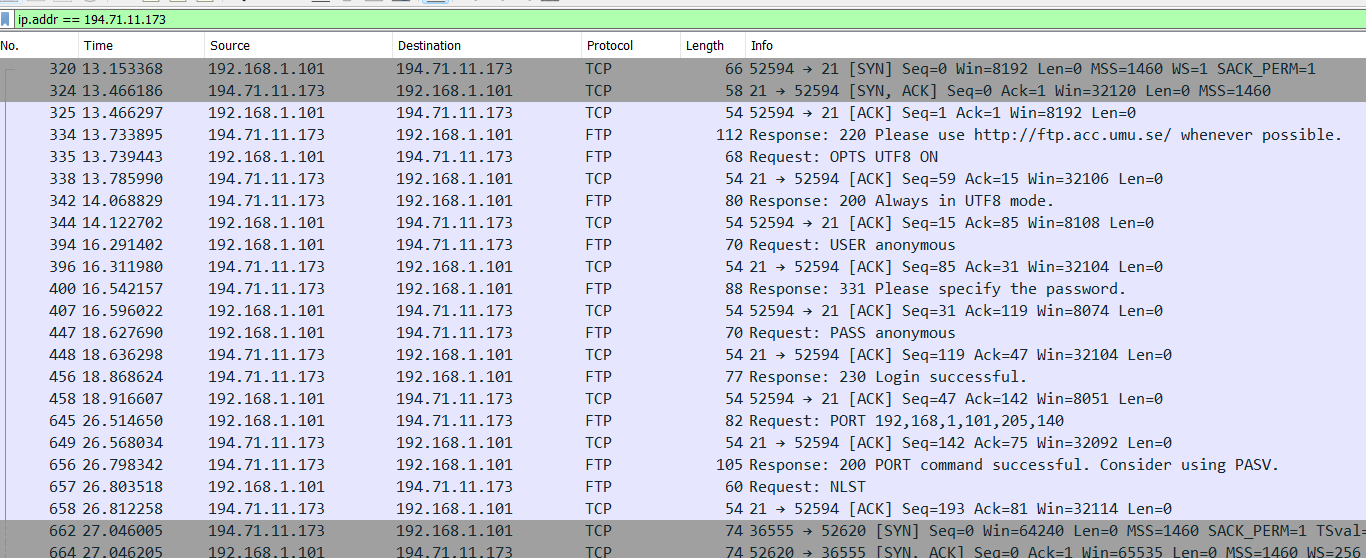
* Part Five

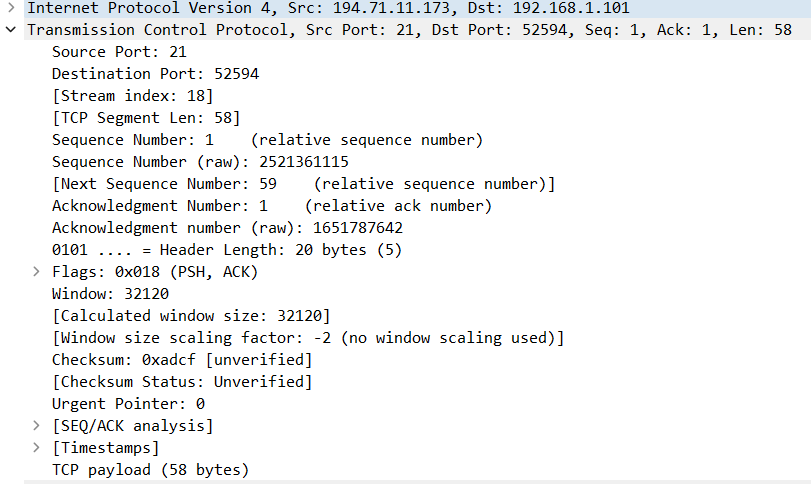
本部分需要边操作，边捕获，请在每次操作后暂停捕获，或者使用过滤器。建议通过FTP命令行进行实验，也可以使用FTP图形客户端。

* **运行FTP xxx.com命令，连接并登录服务器，输入用户名和帐号（如果是免费服务器，可以使用匿名帐号Anonymous，密码是任意的邮箱）。捕获到的数据包由几层协议构成？分别是什么协议？标出数据包的源和目标IP地址、源和目标端口。**

在网上找的公用的ftp服务器。





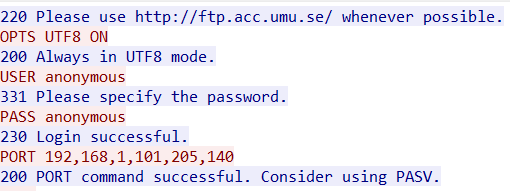


TCP3次握手后，与ftp服务器建立连接后，FTP服务器回应数据包，其中由4层协议构成，分别是以太网、IPv4、TCP、FTP。

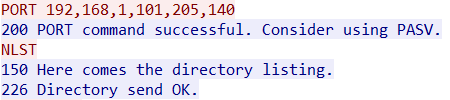
Source : 194.71.11.173 ; Destination : 192.168.1.101

Source Port : 21 ; Destionation Port : 52594

* **跟踪TCP流，标注客户端发出的登录命令、用户名、密码以及服务器的响应。**

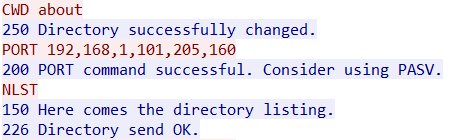


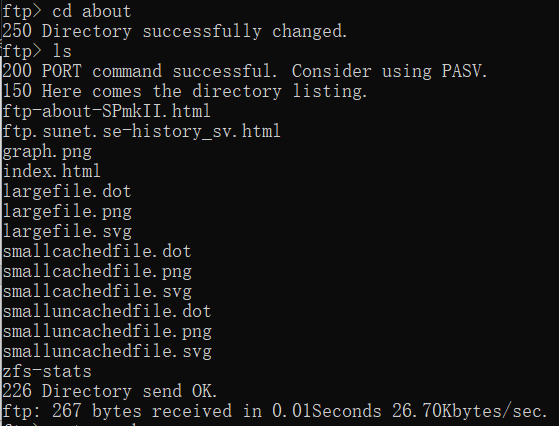
* **执行列目录操作（ls），在新捕获的数据包中跟踪TCP流，标注客户端发出的命令、以及服务器的响应。查看是否建立了一个新的TCP连接，跟踪该连接的TCP流。建议连接校内服务器，如果服务器在校外，可能需要先执行passive命令（下同）。**



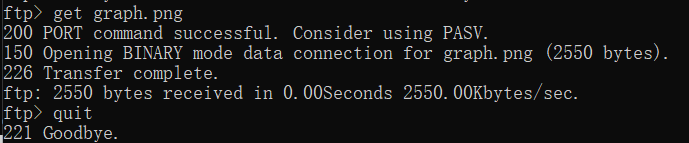
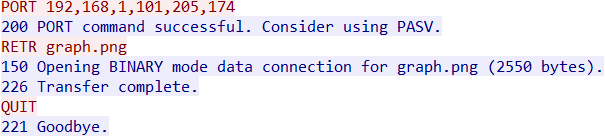


* **执行更换目录操作（cd），在新捕获的数据包中跟踪TCP流，标注客户端发出的命令、以及服务器的响应。**





* **执行下载文件操作（get filename），如果是二进制文件，先执行binary命令。在新捕获的数据包中跟踪TCP流，标注客户端发出的命令、以及服务器的响应。查看是否建立了一个新的TCP连接，跟踪该连接的TCP流（内容较长时截取部分关键内容）。**



# 实验结果与分析

根据你看到的数据包，分别解答以下协议的问题（看完请删除本句）：

* Ping发送的是什么类型的协议数据包？什么时候会出现ARP消息？Ping一个域名和Ping一个IP地址出现的数据包有什么不同？

答：Ping发送的是ICMP协议的数据包。当我们向一个IP地址发送数据的时候就需要用到ARP缓存表，这个表记录着IP地址与MAC地址的映射关系可查询M AC地址。但是当缓存表中没有这样的记录时，就会发送一个ARP请求给该IP所对应的MAC地址。Ping一个域名时还需要发送DNS协议请求数据来获得对应的IP地址。

* Tracert/Traceroute发送的是什么类型的协议数据包，整个路由跟踪过程是如何进行的？

答：ICMP类型的协议数据包。通过TTL字段递增来实现的，发送TTL字段为1的时候到达第一跳的路由器数据包超时时，本机就可以受到ICMP Error的信息知道路由器的地址，字段为2的第二跳也超时，同样收到错误信息，以此类推。

* 建立TCP连接的数据包由几个构成？各自的SYN和ACK标志字段是什么？

答：由三个数据包构成。第一次SYN=1(SET)，第二次SYN=1(SET)、ACK=1(SET)，第三次ACK=1(SET)

* 浏览器打开一个网页，可能会看到多个TCP连接，多次HTTP会话。一个TCP连接上是否会存在多个HTTP会话？什么情况下会出现DNS数据包？

答：会存在多个HTTP会话。当使用域名访问网页的时候，而本地又没有相关信息就会出现DNS数据包。

* 邮件客户端发送一封电子邮件，需要几次请求、响应消息的交互？消息的一般格式是什么？邮件正文结束的标记是什么？

使用smtp协议发送邮件给服务器时需要6次请求、响应消息的交互。

1. 使用EHLO命令与连接上的smtp服务器“打招呼”
2. 使用“AUTH LOGIN”登录到smtp服务器
3. 指明发件人和收件人mail from : xxx, rcpt to : xxx
4. 输入data命令，“data”命令表示准备开始输入邮件内容，其邮件格式为，邮件头包含from、to和subject（主题），邮件正文内容在下方，还有其他的内容。
5. 直遇到“.”告诉邮件服务器邮件内容已经写完
6. 输入quit命令断开与邮件服务器的连接。

* 邮件客户端接收一封电子邮件，需要几次请求、响应消息的交互？消息的一般格式是什么？用户名和密码是否经过了加密处理？

答：邮件客户端接收一封邮件大致过程：

1. Login
2. Select Inbox
3. Search New
4. Fetch
5. Logout

Received : from 机器名

by smtp5 (Coremail) with SMTP id HdxpCgDHr0hAupFiapG+Eg--.3604S2;

Sat, 28 May 2022 13:59:31 +0800 (CST)

Date: Sat, 28 May 2022 13:59:30 +0800

From: "xxx@163.com" <xxx@163.com>

To: xxxx<xxxx@163.com>

Subject: 正文内容

X-Priority: 3

X-GUID: 。。。

X-Has-Attach: no

X-Mailer: Foxmail 7.2.23.121[cn]

Mime-Version: 1.0

Message-ID: 。。。

Content-Type: multipart/alternative;

boundary="----=\_001\_NextPart608280284834\_=----"

X-CM-TRANSID:。。。

X-Coremail-Antispam: 。。。

X-Originating-IP: 。。。

X-CM-SenderInfo: 。。。

用户名和密码均经过了加密处理。

* 登录FTP服务器时，会产生几个TCP连接？列目录和上传或者下载文件时，会产生几个TCP连接？

答：登录时产生一个控制TCP连接，之后列目录又产生一次连接，下载文件时也产生一个连接。

# 讨论、心得

这次的实验对我来说算是相当困难因为一直在实验过程中遇到很多的麻烦，花费了2天的时间一直在找问题所在，尤其是Part4的部分，SMTP的数据包一直捕获不到，在Foxmail、Outlook、163等邮件服务器找了很多相关问题和解决方案都找不了，最后发现是SMTP协议是不能加密SSL的，如果加密了就不能捕获到了，但是不使用SSL的话，就只能使用port 25或587，而port 25又被我的ISP所阻挡了所以也不能用port 25发邮件，587则是使用TLS加密，虽然能被捕获到但是追踪TCP流的时候，内容都是加密的，导致我只能在网上找一些案列来看其流程。这次的实验真的耗费了我很多的精力和时间来完成，在这次的实验过程中也学到了很多的知识点，加深了我对计算机网络的认知，虽然过程很艰辛但是收获还是很多的。