**暨南大学本科实验报告专用纸**

课程名称 计算机网络 成绩评定

实验项目名称 Internet应用与应用层协议分析 指导教师 潘冰

实验项目编号 3 实验地点 个人PC机

学生姓名 易雪 学号 2019054617

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 9 月 27 日～ 10 月 18 日

1. **实验目的**
2. 理解WWW、DNS服务、FTP服务、SMTP的作用和原理
3. 学会使用wireshark分析HTTP、FTP、SMTP和DNS协议的工作过程，加深对协议格式和工作原理的理解。
4. **实验内容**
5. 通过域名访问WWW、FTP服务器，分析DNS、WWW、FTP工作过程，并使用Wireshark分析相关协议格式
6. 在客户端访问SMTP服务器，使用wireshark分析SMTP、POP3协议的工作过程。（可以在客户端安装outlook或使用QQ邮件服务器或自己编程）
7. **实验步骤**
8. HTTP协议分析

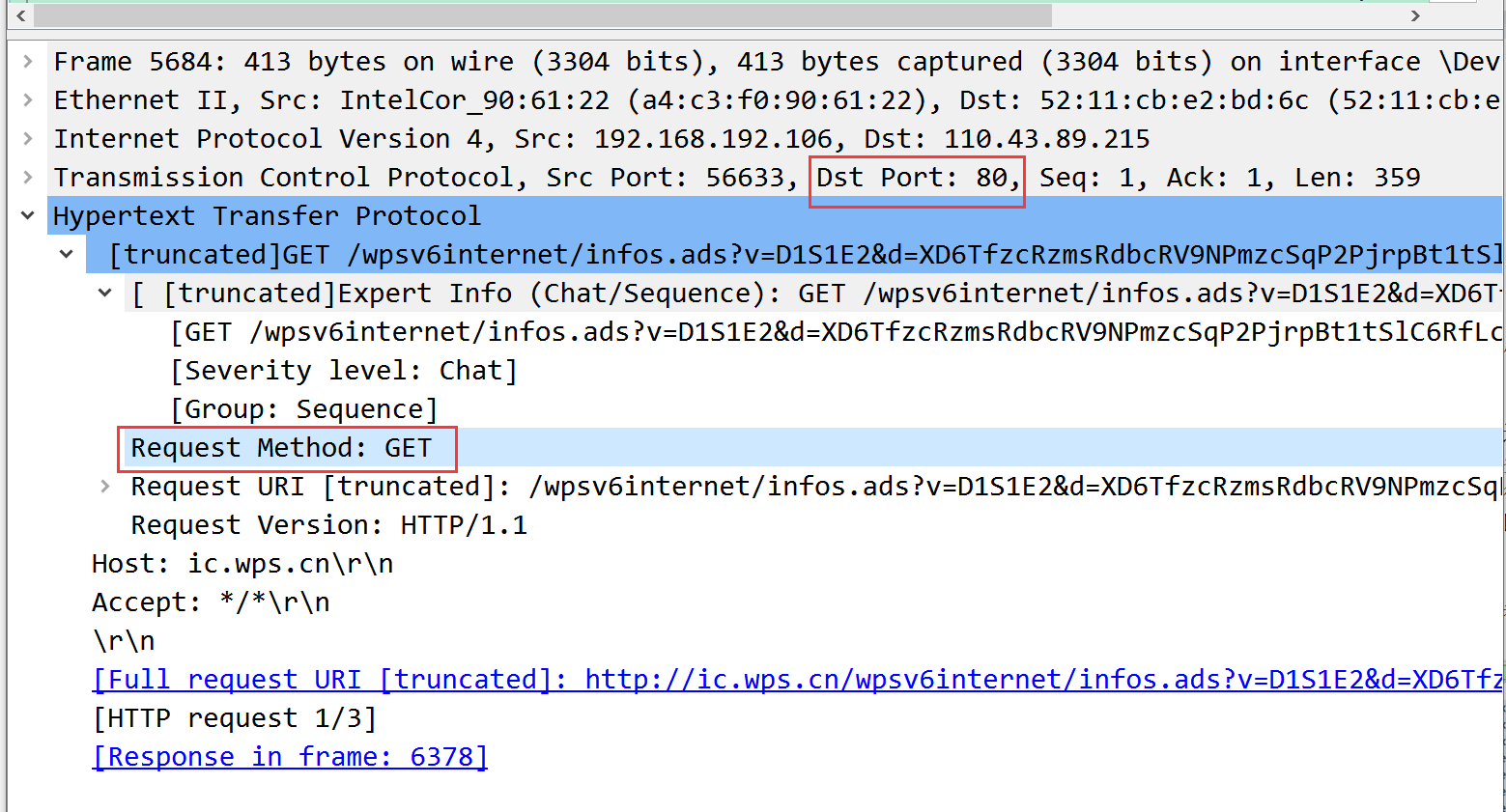
访问任意web站点，用wireshark分析HTTP协议的工作过程和HTTP协议格式。（协议首部含义需要查询了解）

注意：如果访问的网站信息量太大，可以利用windows自带组件（如IIS）或自行下载www服务器软件，建立并配置www站点，主页内容需要包含姓名、学号等个人信息，然后访问自己建立的网站。

HTTP工作流程：

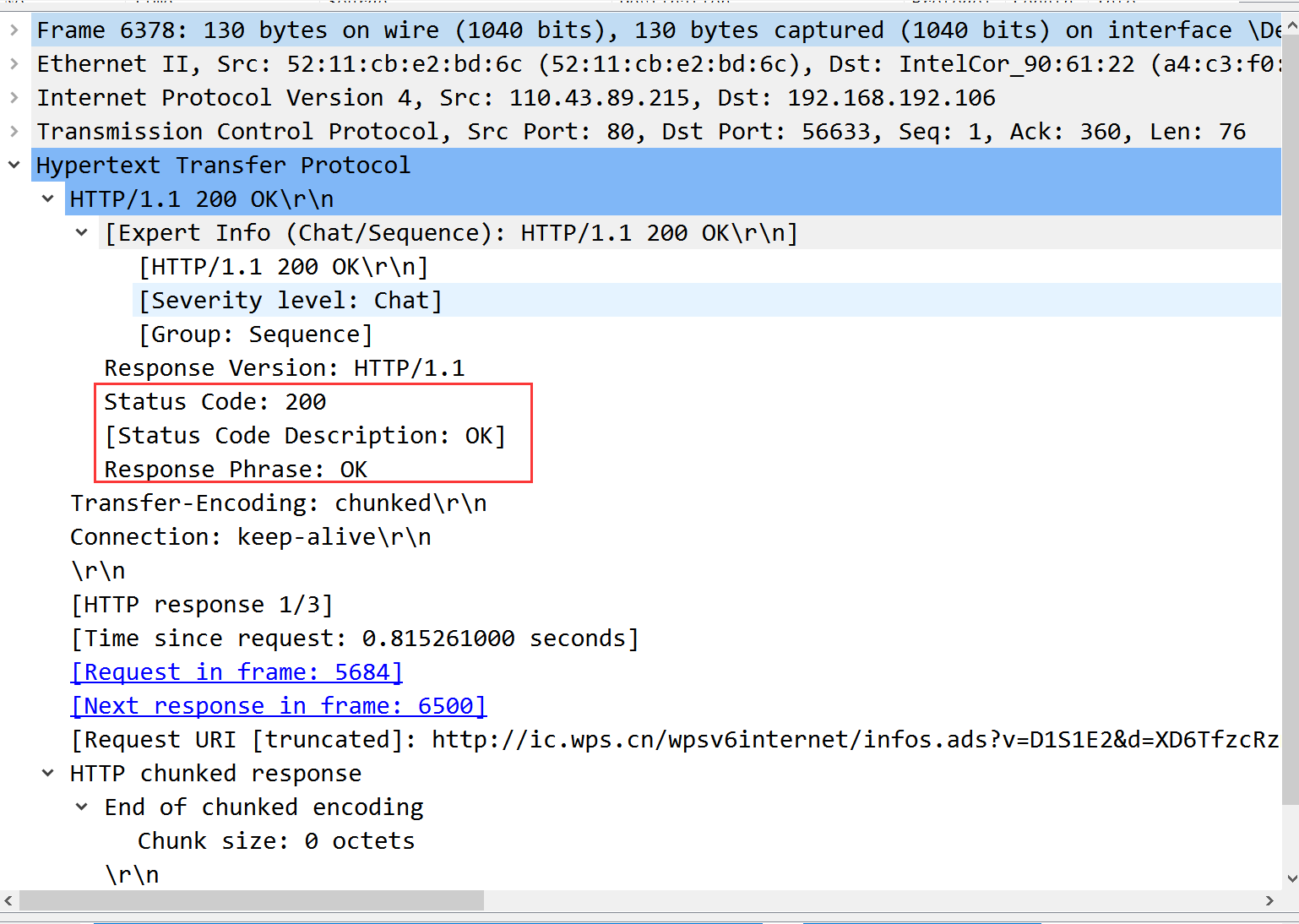
客户端通过TCP的三次握手建立与服务器的连接——客户端向服务器发送HTTP请求——服务器收到客户端请求后，将恢复响应数据包，并向客户端发送数据——客户端通过TCP四次握手，与服务器断开连接。

打开百度随便搜索，如何用wireshark抓取到：（此时校园网不稳定，连接了手机热点，所以ip地址不一样...）



HTTP数据包通过TCp被传输到服务器的80端口，也就是HTTP标准的通信端口（8080）

数据包请求的方法是GET，请求的版本是HTTP/1.1，表示客户端请求使用的HTTP1.1版本。



HTTP使用了一些预定义的响应码表示请求方法的结果。这里有一个带有200状态码的数据包，表示依次成功的请求方法。这个数据包里包含一个时间戳，以及一些关于web服务器内容编码和配置参数的额外信息。当客户端收到这个数据包后，这次的处理也就完成了。

1. DNS协议分析

通过域名访问某网站，用wireshark捕获DNS数据包，并分析DNS工作过程和DNS格式。

注意：

1. 有时候可能捕获不到DNS解析过程，为什么？要仔细分析。
2. 可以自己建立DNS服务器并使用它进行域名解析。

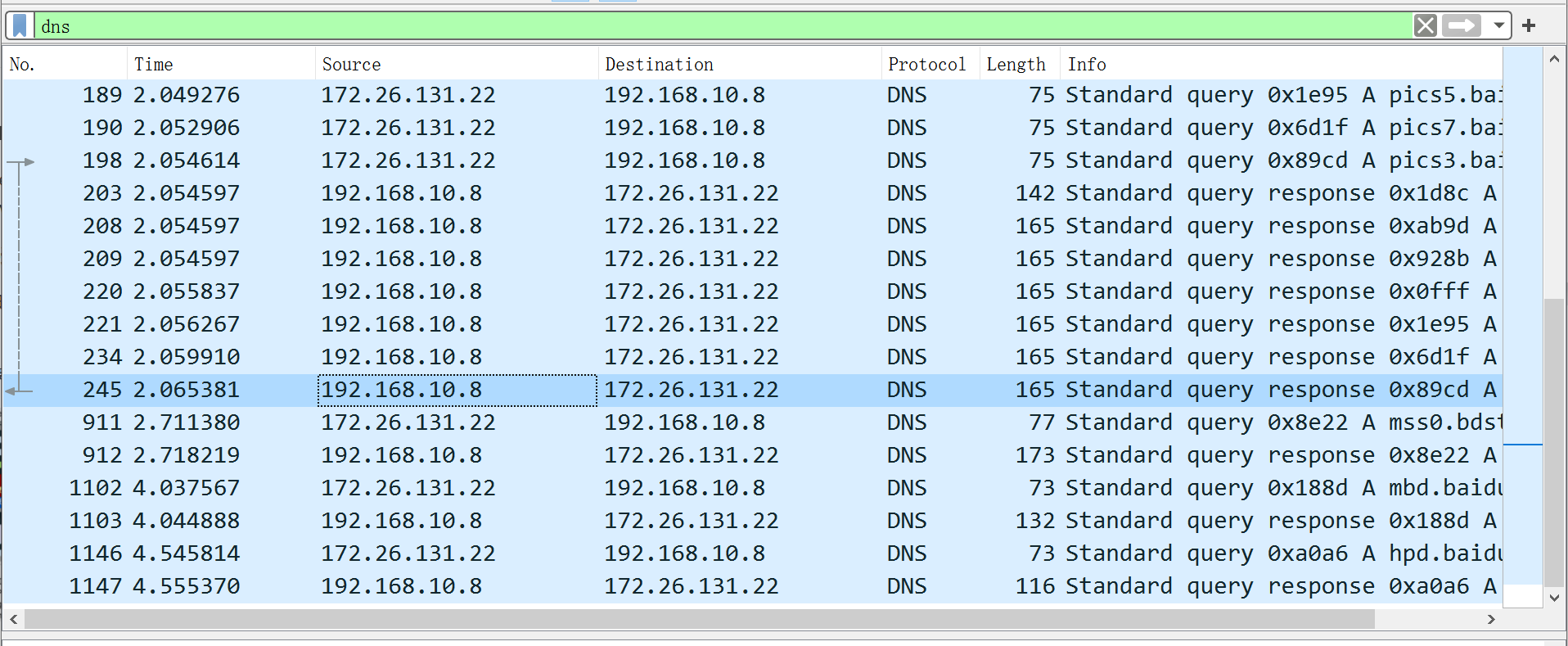
①建立DNS服务器

利用windows自带组件或下载DNS软件（如ntbind），建立DNS服务器，并对DNS服务器的配置（建立域名-IP地址的解析关系）

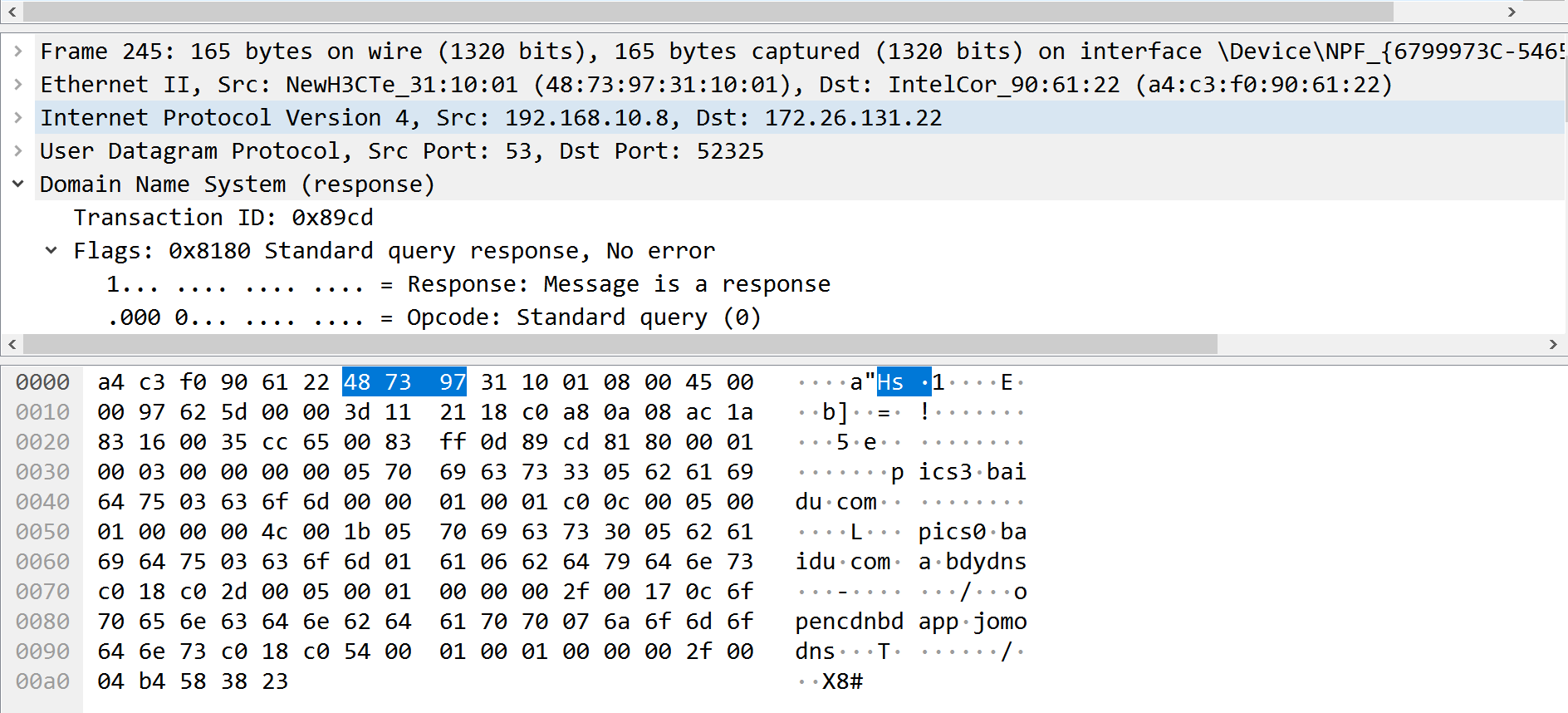
②使用DNS

在任意一台计算机上配置TCP/IP协议，将DNS服务器配置成上述DNS服务器（注意该DNS服务器的IP地址是静态的），用该DNS服务器中设置的器域名访问该WWW服务，并与用IP地址访问的结果进行比较。（注意该客户机的IP地址最好与DNS服务器地址同一个网段，即网络号相同）

打开wireshark，输入百度网址，到页面呈现，数据包传递的信息都被放在wireshark里。筛选DNS：



选择245号包，会出现以下内容，分别是每层里面的内容和头部的字节码：



这个数据包的165个字节里包含：数据链路层报文头（数据链路层），ip层头（网络层），upd头（传输层），dns头（应用层）。

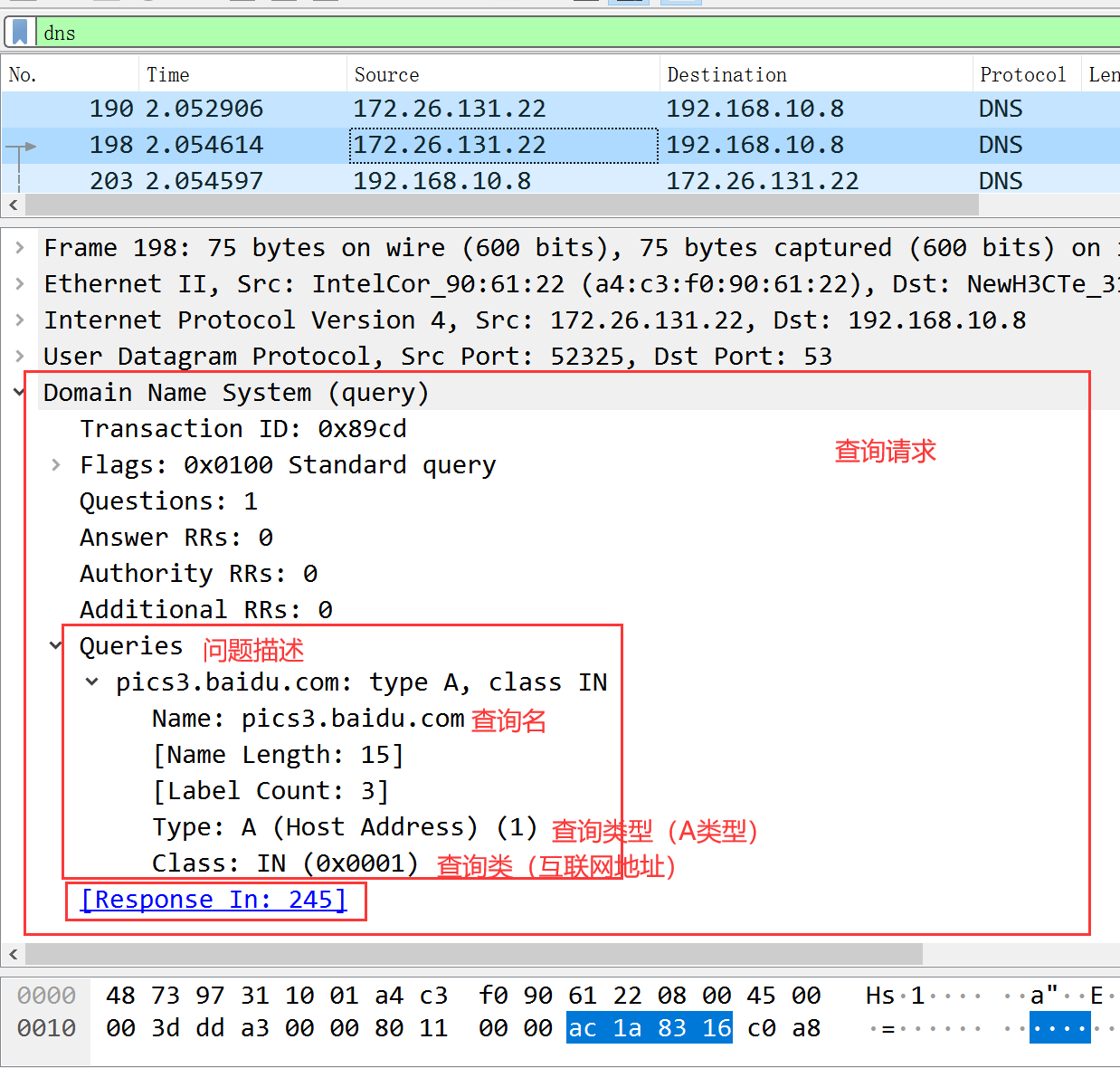
链路层的主要信息有两个mac地址，源地址和目的地址，主机的mac地址会被发送到路由器的mac地址，然后再由路由器进行转发。

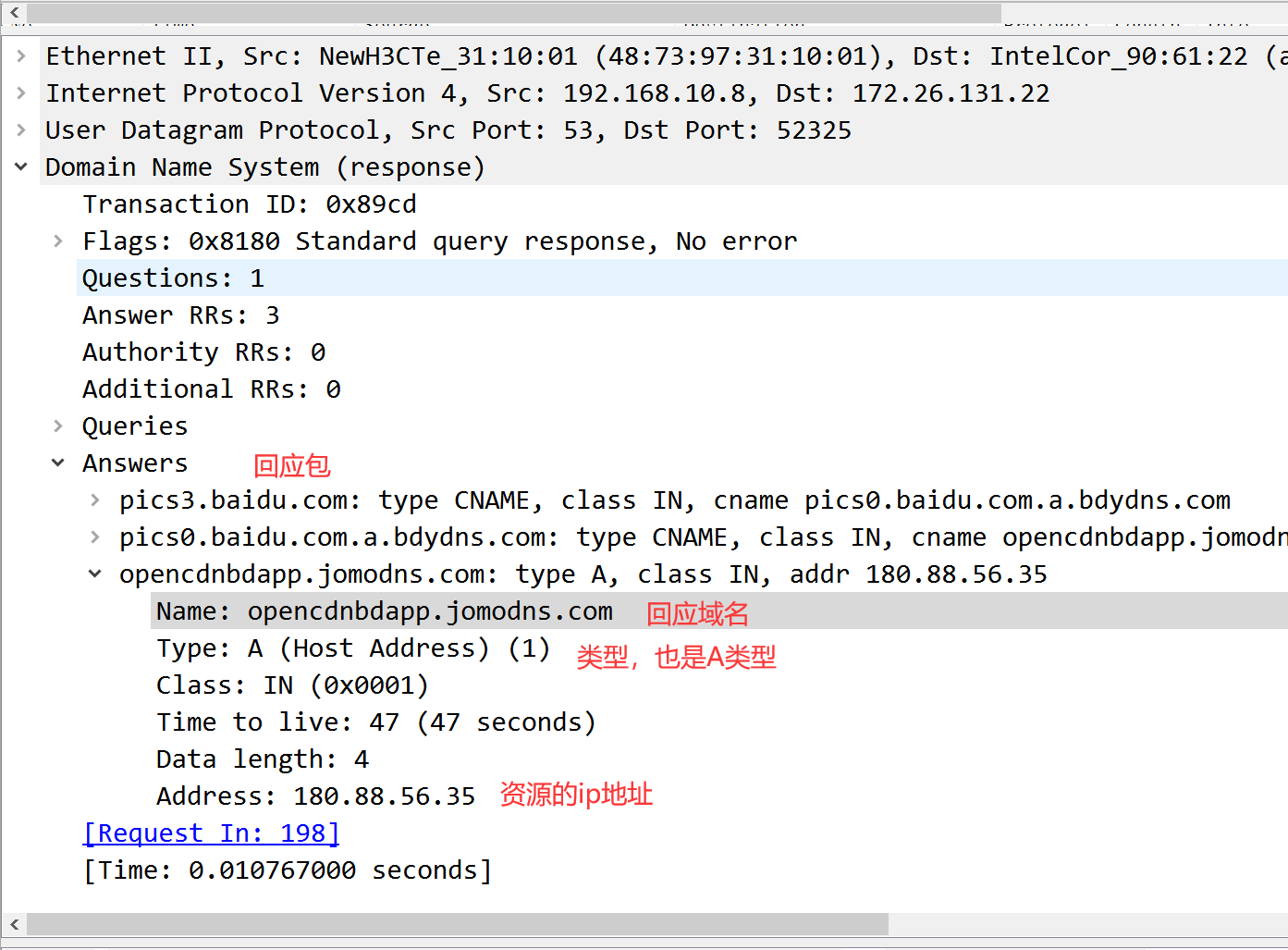
网络层有ip4，ip地址，目的ip地址等信息。

传输层主要负责端口的管理。

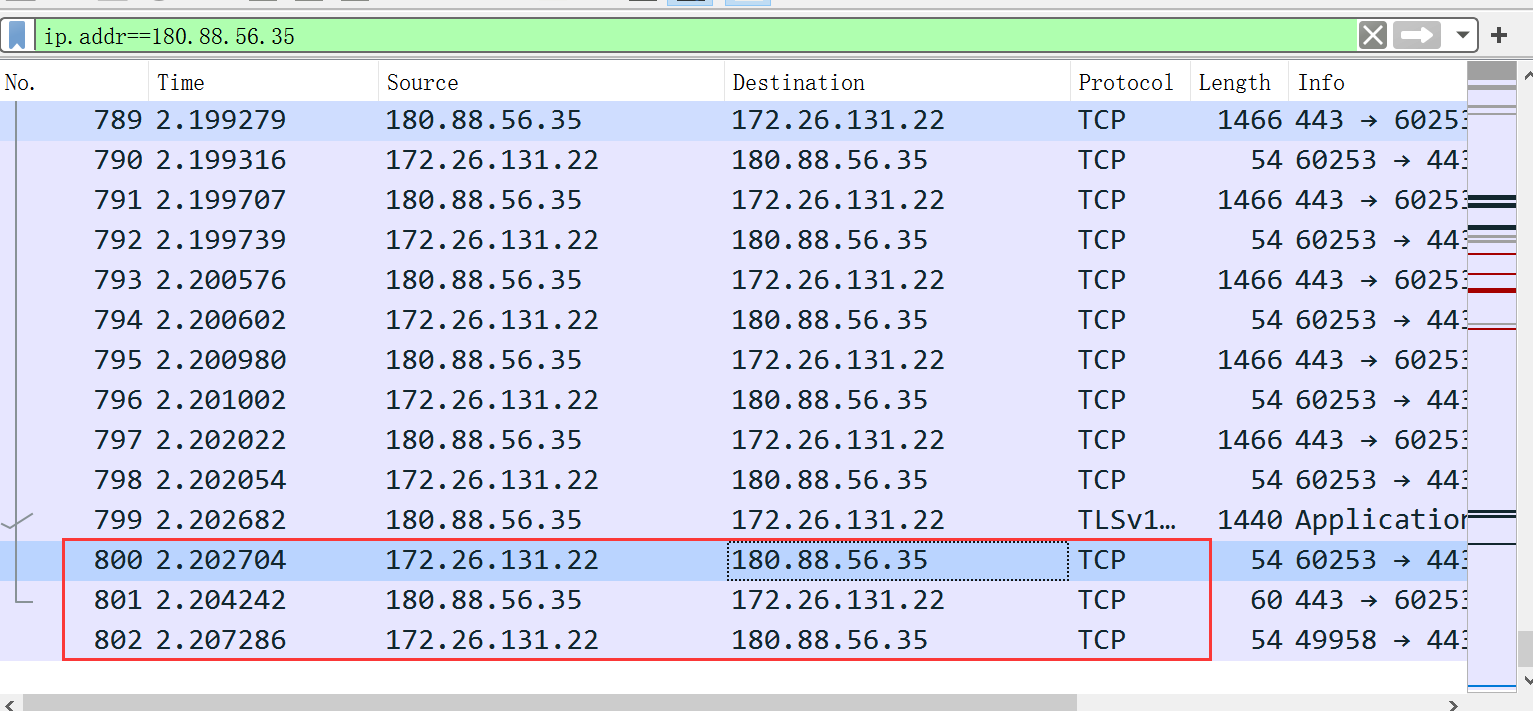
问题部分（报文格式中查询问题区域部分。显示DNS查询请求的问题）

此部分包含：查询名（一般是要查询的域名，有时也会是IP地址，用于反向查询），查询类型（DNS查询请求的资源类型，通常为A类型，表示由域名获取对应的IP地址），查询类：地址类型，通常为互联网地址，值为1。

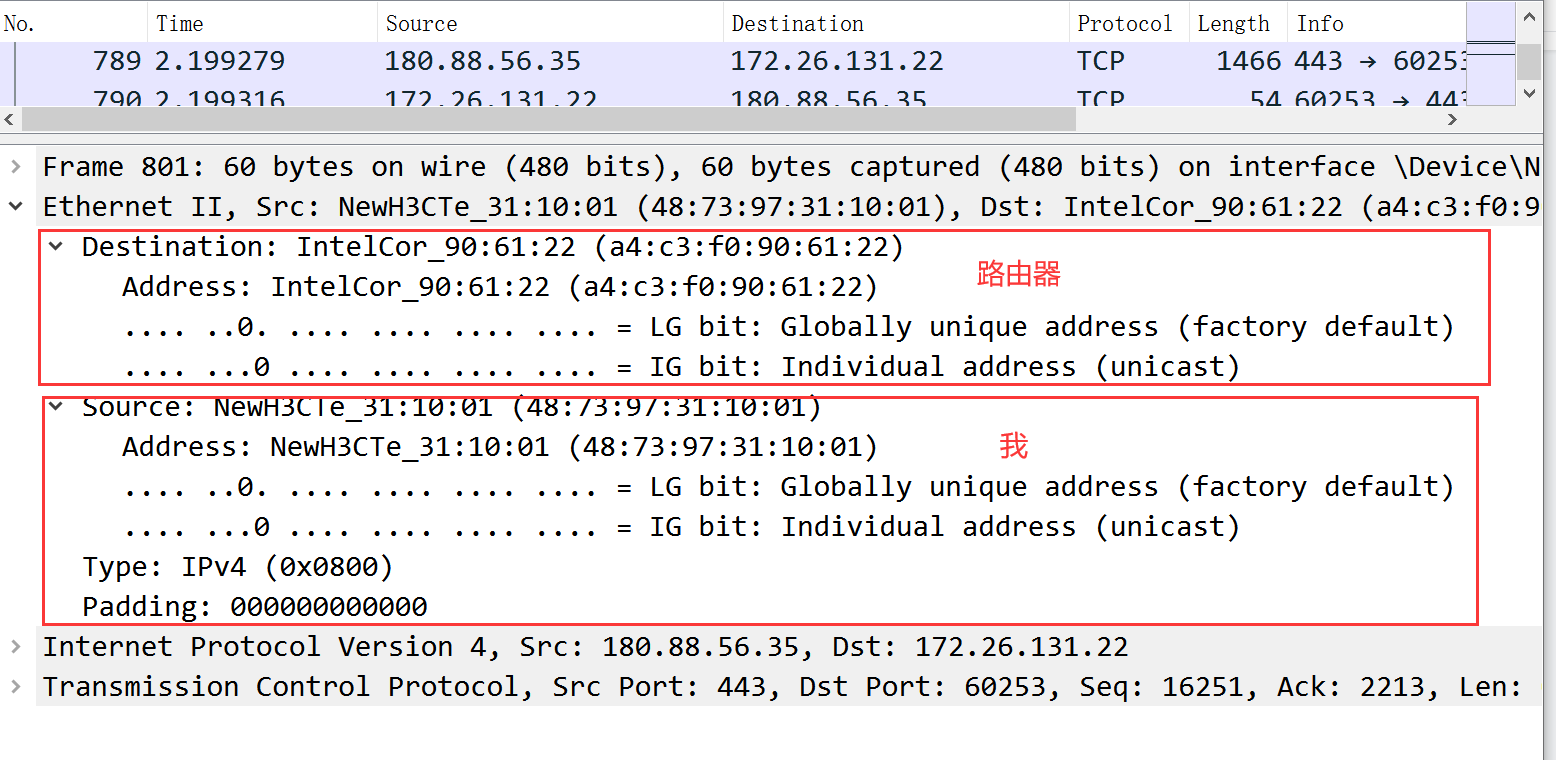




用接收到的资源ip地址过滤一下，可以看到TCP三次握手：

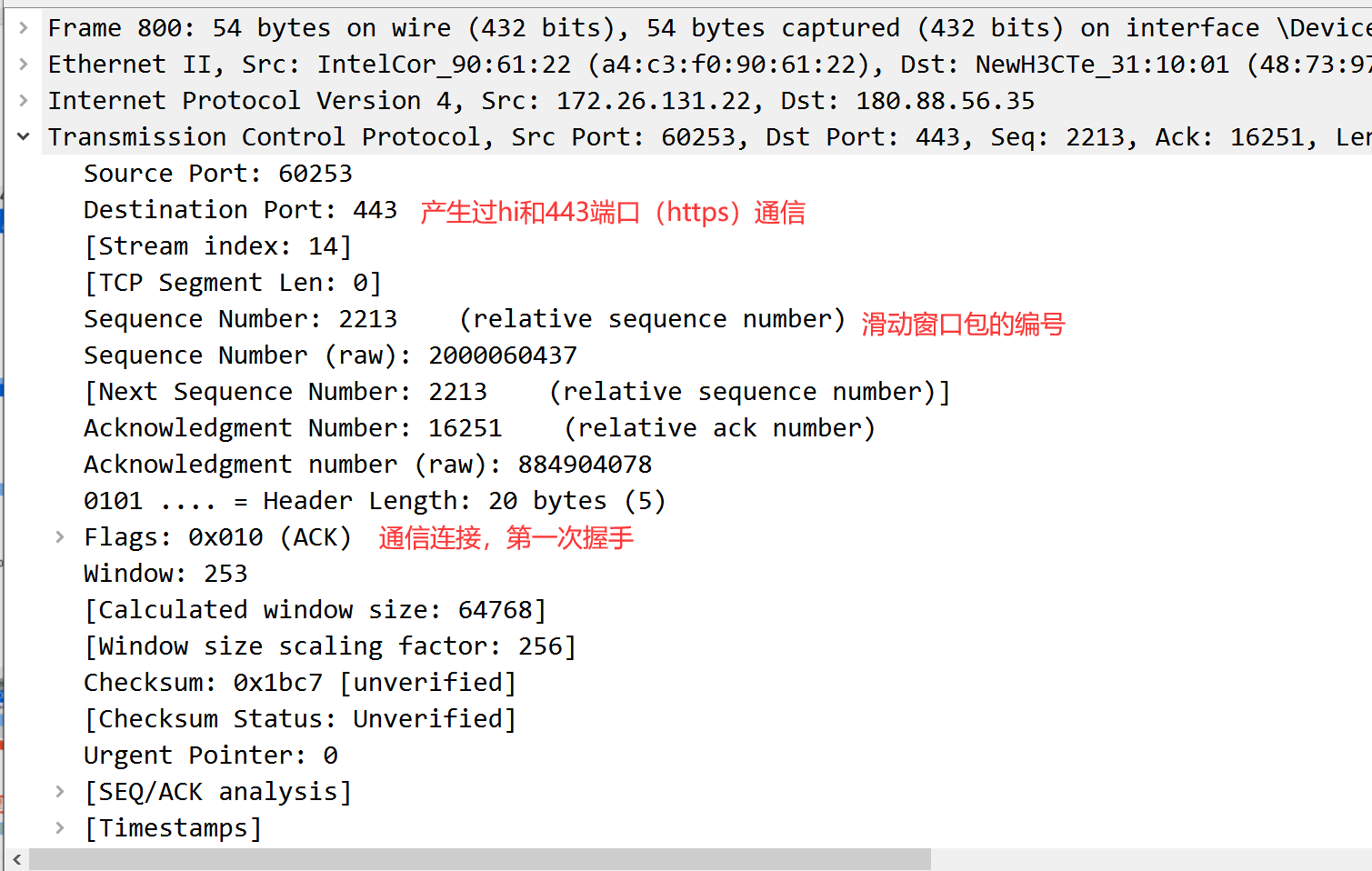


数据链路层依然发送给路由器：

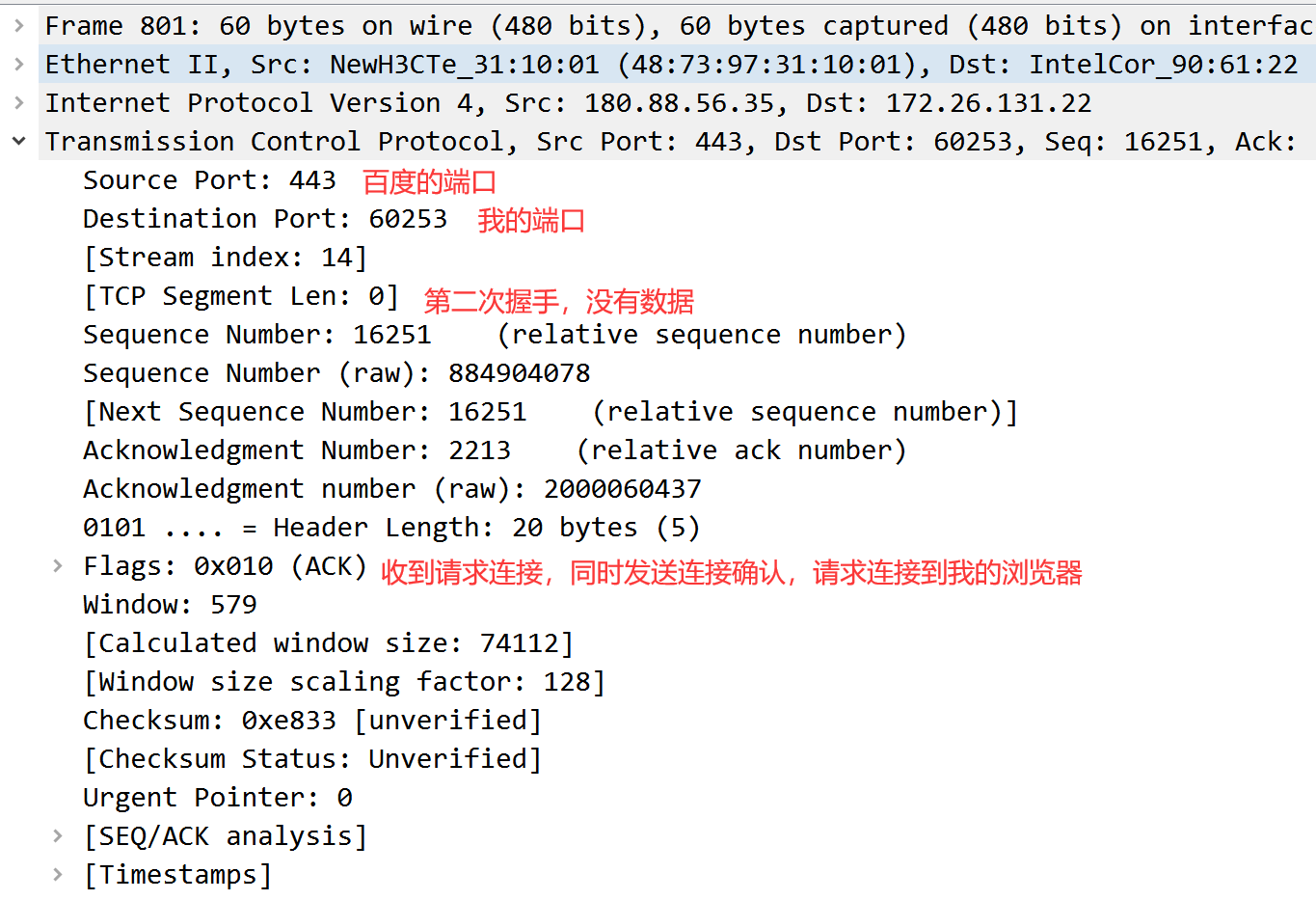


网络层是发给百度的ip，传输层把对应端口对应了起来。

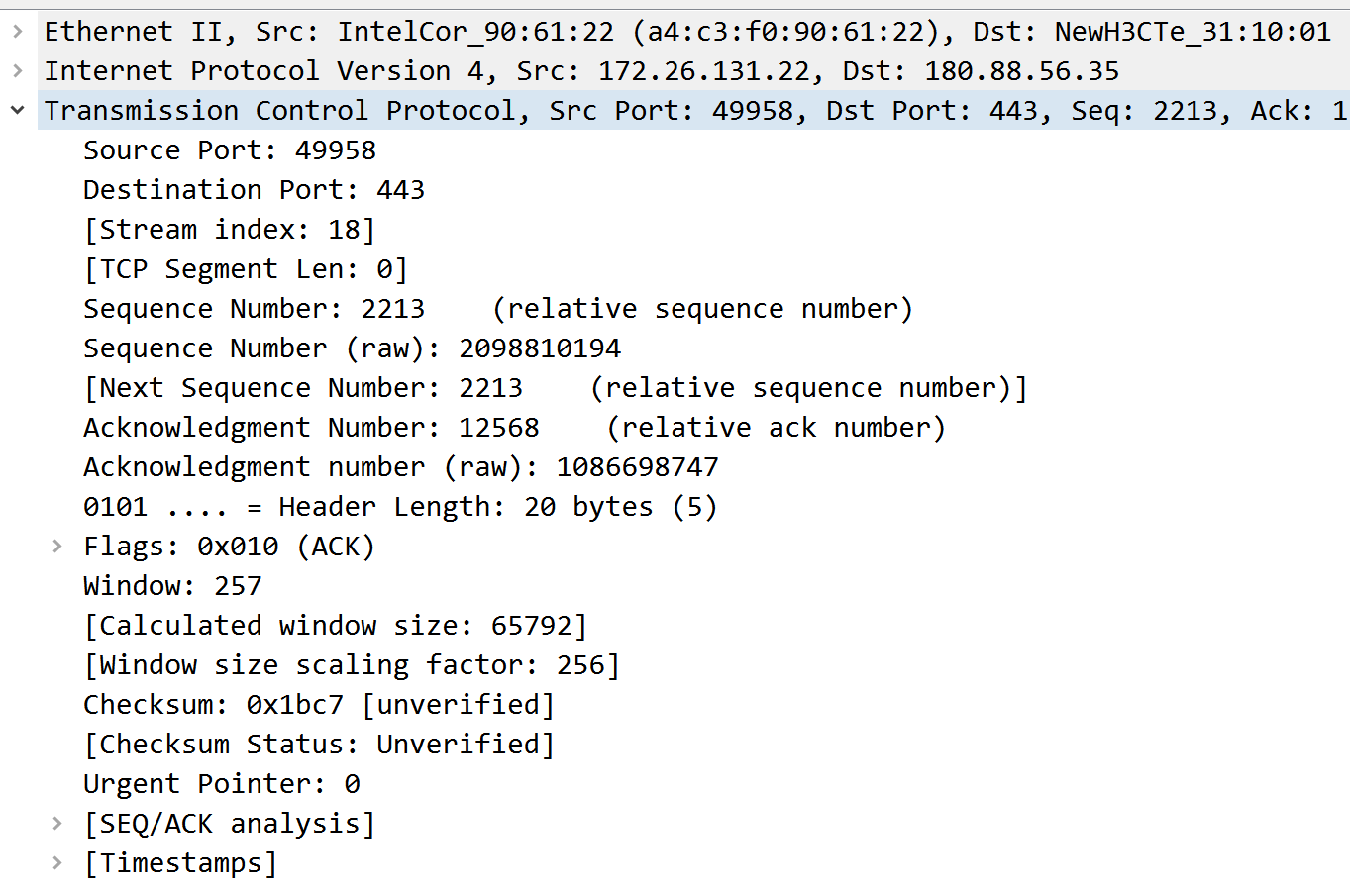
Tcp层第一个请求包：



第二个包：

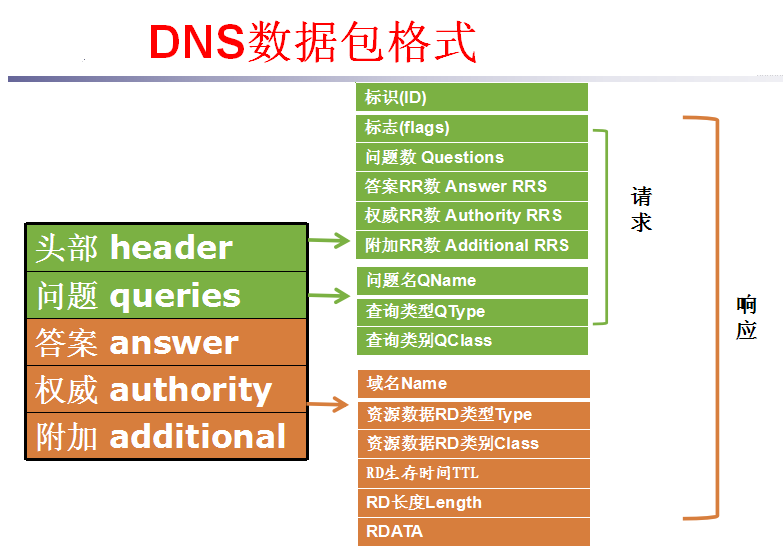


第三个包也类似



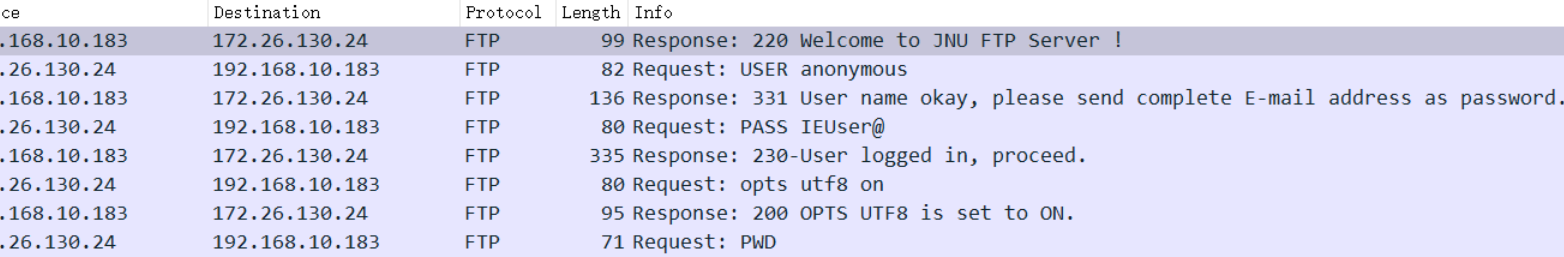
然后就可以开始通信了，http协议就开始相互发送数据包。

1. 附DNS数据包格式



1. FTP协议分析
2. 访问FTP服务器，如ftp://ftp.jnu.edu.cn
3. 用wireshark分析FTP的工作过程。注意观察FTP的工作模式，用于控制连接的端口和数据连接的端口。

注意：可以利用Windows自带的FTP组件或下载FTP软件，建立FTP服务器，并进行配置，并访问分析FTP协议



三次握手建立连接后，FTP服务器返回状态码220，表示服务就绪。登录过程先由终端向FTP发送用户名“anonymous”并等待验证。用户名验证通过以后，FTP服务器返回状态码331，表示用户名验证已通过并需要输入密码。终端将登陆密码IEUser@发送给FTP服务器，FTP服务器验证后返回状态码230，表示用户已登录。终端向FTP服务器发送OPTS UTF8 on，FTP服务器返回状态码200，表示命令执行成功。

1. SMTP和POP协议分析

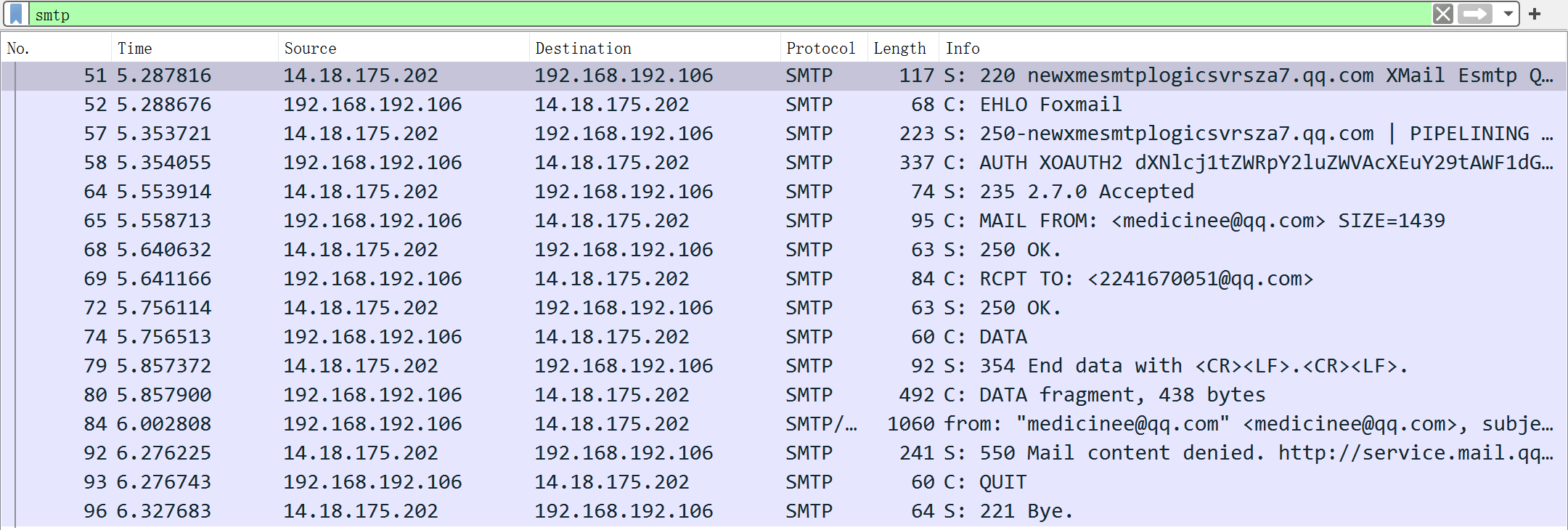
基于Web的邮件或客户端的邮件软件（如outlook）收发邮件，捕获数据报分析邮件收发过程和SMTP、POP3等协议格式和工作过程。

注意：①可以利用windows自带组件安装SMTP服务器，并配置邮件服务器，并访问。

②什么情况下可以捕获POP或SMTP数据包

收发邮件大致过程：发件人调用用户代利编辑要发的邮件——发件人点击“发送邮件”按钮，将发送邮件的工作交给用户代理来完成。用户代理通过SMTP协议将邮件发送给发送方的邮件服务器——服务器收到用户发来的邮件后，把收到的邮件临时存放在邮件缓存队列中，等待时间成熟后再发送到接收方的邮件服务器——时机成熟，邮件发送之前，发送方的邮件服务器的SMTP客户与接收方的邮件服务器的SMTP服务器需要实现建立TCP连接，之后再将队列中的邮件发送出去——接收方的邮件服务器中的SMTP服务器进程再收到邮件后，把邮件放入收件人的用户邮箱中，等待收件人进行读取——收件人打算收信时，就运行PC机中的用户代理，使用POP3协议读取发送给自己的邮件。

用Foxmail向自己的另一个邮箱发送邮件，捕获到如下信息：



51：表示建立好连接，服务器准备就绪

52：客户端向服务器发送主机名

57：服务器回复250，表示服务器能够就收邮件

58：SMTP邮件发送程序使用要求的官方认证进行回应

64：认证通过

65：开始发送邮件

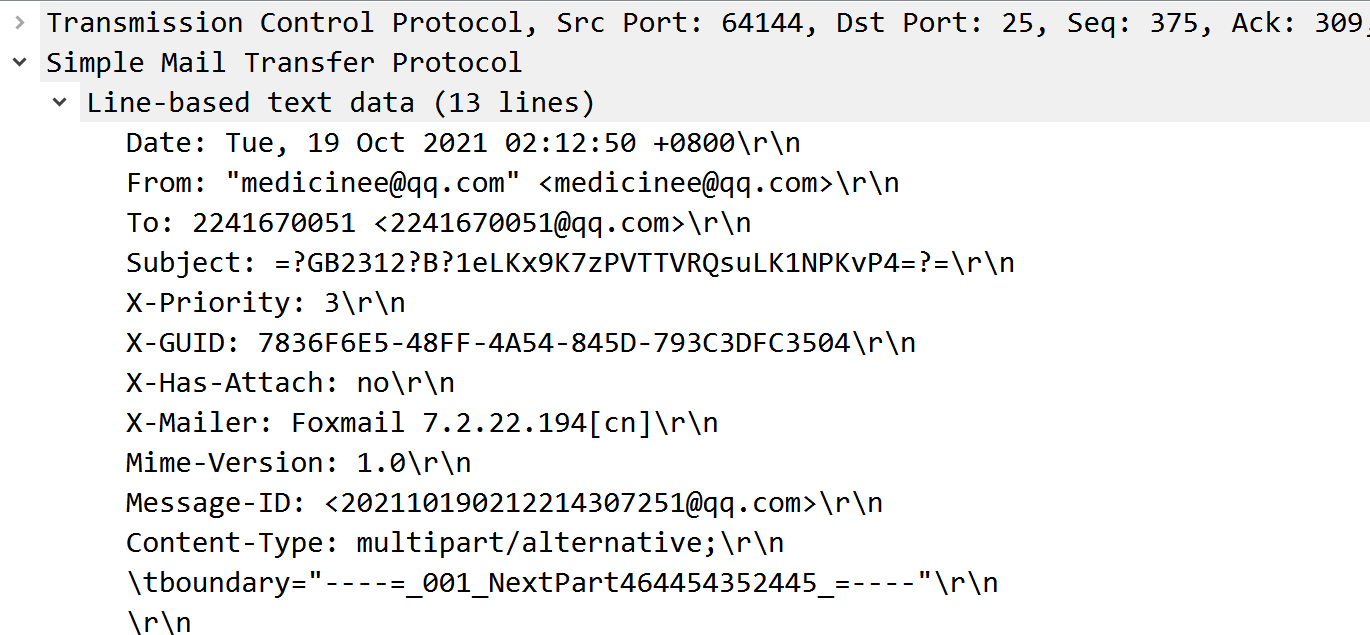
68：服务器响应OK

69：指出接收方的地址

72：服务器响应OK

74：表示即将开始发送邮件内容

75：354表示能接受文件，并提示data结束格式

80：发送邮件：

84：指出发送方地址

92：550表示收到邮件退回信息（具体理由或许是被qq邮箱当作垃圾邮件处理了，所以被退回）

93：结束，退出。