

**本科实验报告**

|  |  |
| --- | --- |
| 课程名称： | 计算机网络 |
| 实验名称： | 网络协议分析 |
| 姓 名： | 汪辉 |
| 学 院： | 计算机学院 |
| 系： |  |
| 专 业： | 计算机科学与技术 |
| 学 号： | 3190105609 |
| 指导教师： | 陆系群 |

2021年 9月 15日

**浙江大学实验报告**

# 实验目的

* 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

* Wireshark是PC上使用最广泛的免费抓包工具，可以分析大多数常见的协议数据包。有Windows版本和Mac版本，可以免费从网上下载。
* 掌握网络协议分析软件Wireshark的使用，学会配置过滤器
* 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、Windows、Linux或Mac操作系统、浏览器软件
* WireShark协议分析软件

# 操作方法与实验步骤

* 安装网络包捕获软件Wireshark
* 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
* TRACE ROUTE：跟踪一个目标地址的途经路由
* NSLOOKUP：查询一个域名
* HTTP：访问一个网页

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。实验之前可以提前了解下第六部分有哪些问题。

# 实验数据记录和处理

以下实验记录均需结合屏幕截图，进行文字标注和描述，图片应大小合适、关键部分清晰可见，可直接在图片上进行标注，也可以单独用文本进行描述。

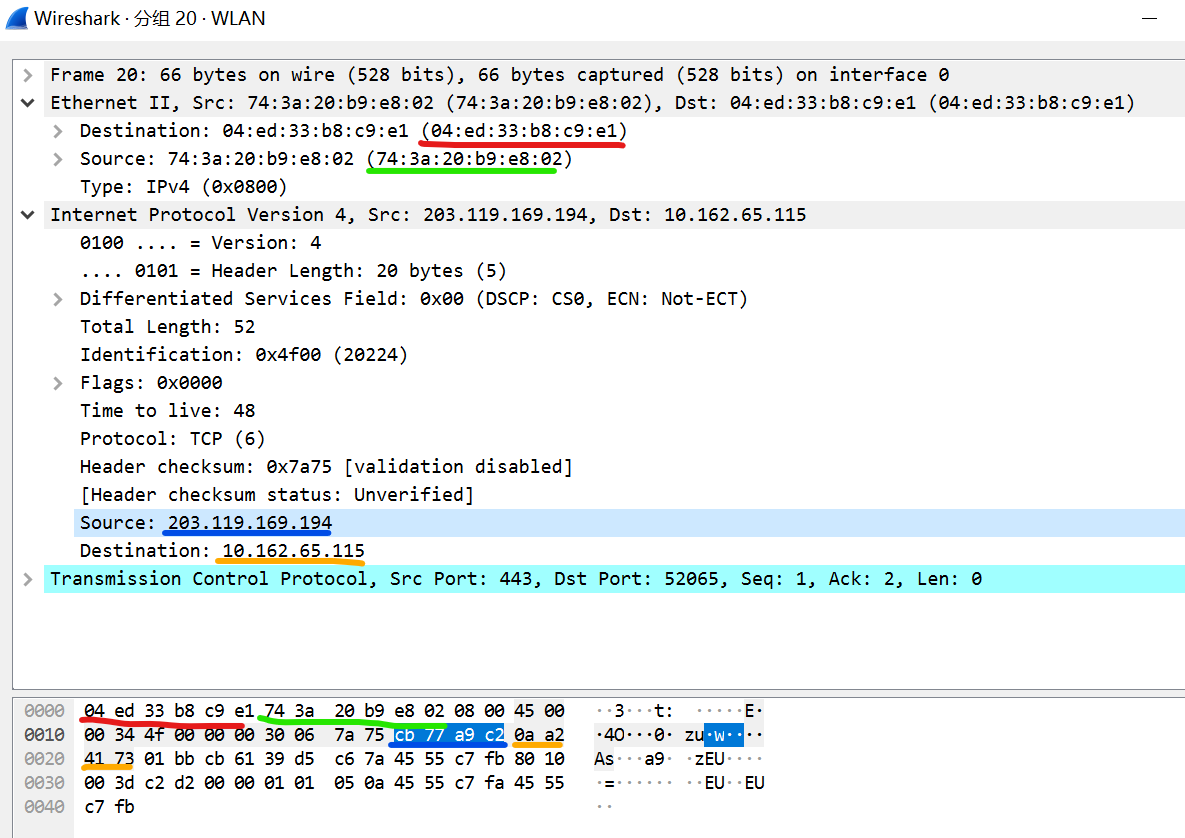
* Part One

1. **运行Wireshark软件，开始捕获数据包，列出你看到的协议名字（至少5个）。**

协议名：TCP、DNS、SSL、TLSv1.2、SSDP

1. **找一个包含IP的数据包，这个数据包有 5 层？最高层协议是 TCP ，从Ethernet开始往上，各层协议的名字分别为： IPv4，TCP 。**

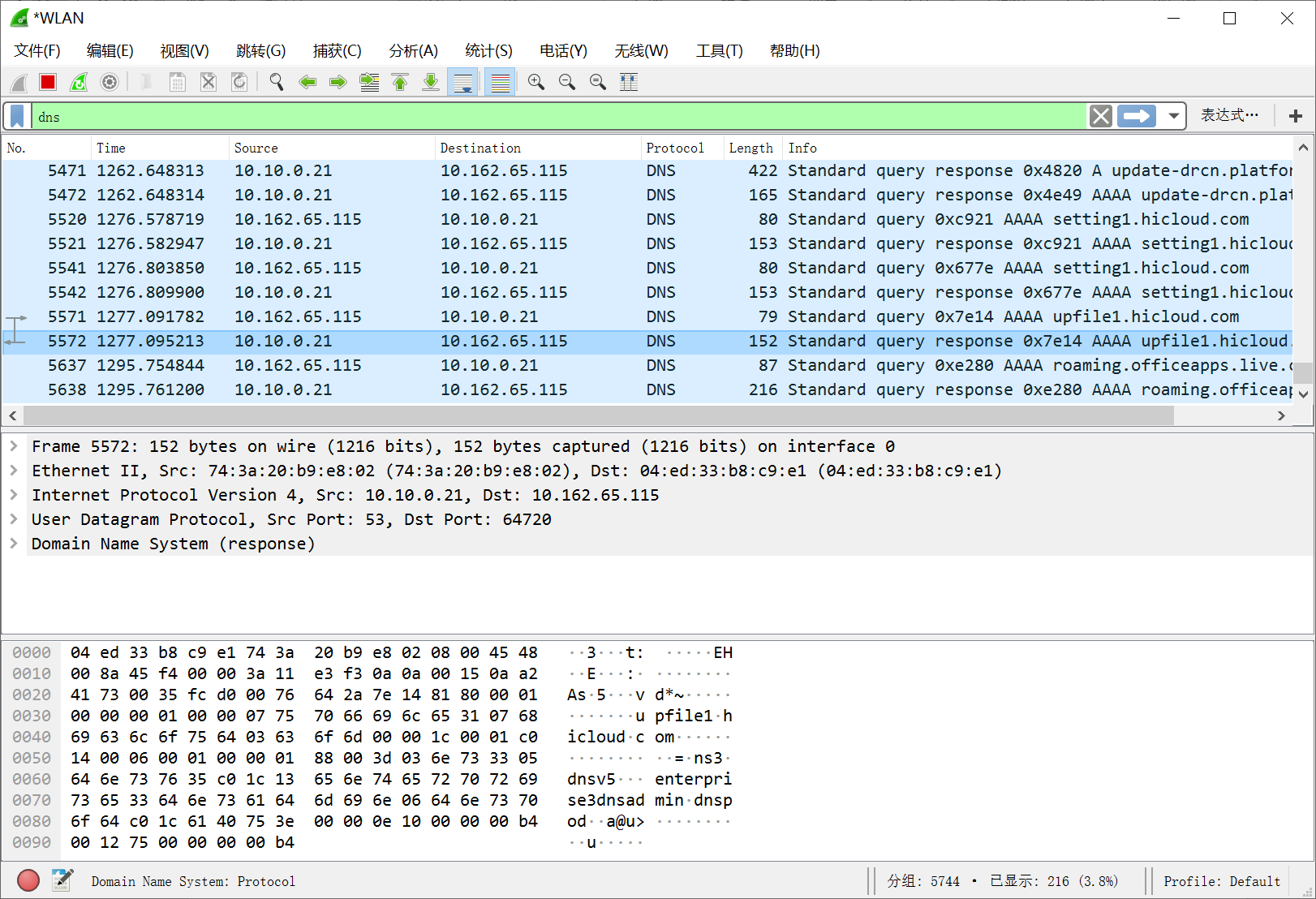
**展开IP层协议，标出源IP地址、目标IP地址及其在数据包中的具体位置，展开Ethernet层，标出源MAC地址和目标MAC地址及其在数据包中的具体位置。**



1. **配置应用显示过滤器，让界面只显示某一协议类型的数据包（输入协议名称）。**

使用的过滤器： dns ，希望显示的协议类型： DNS 。

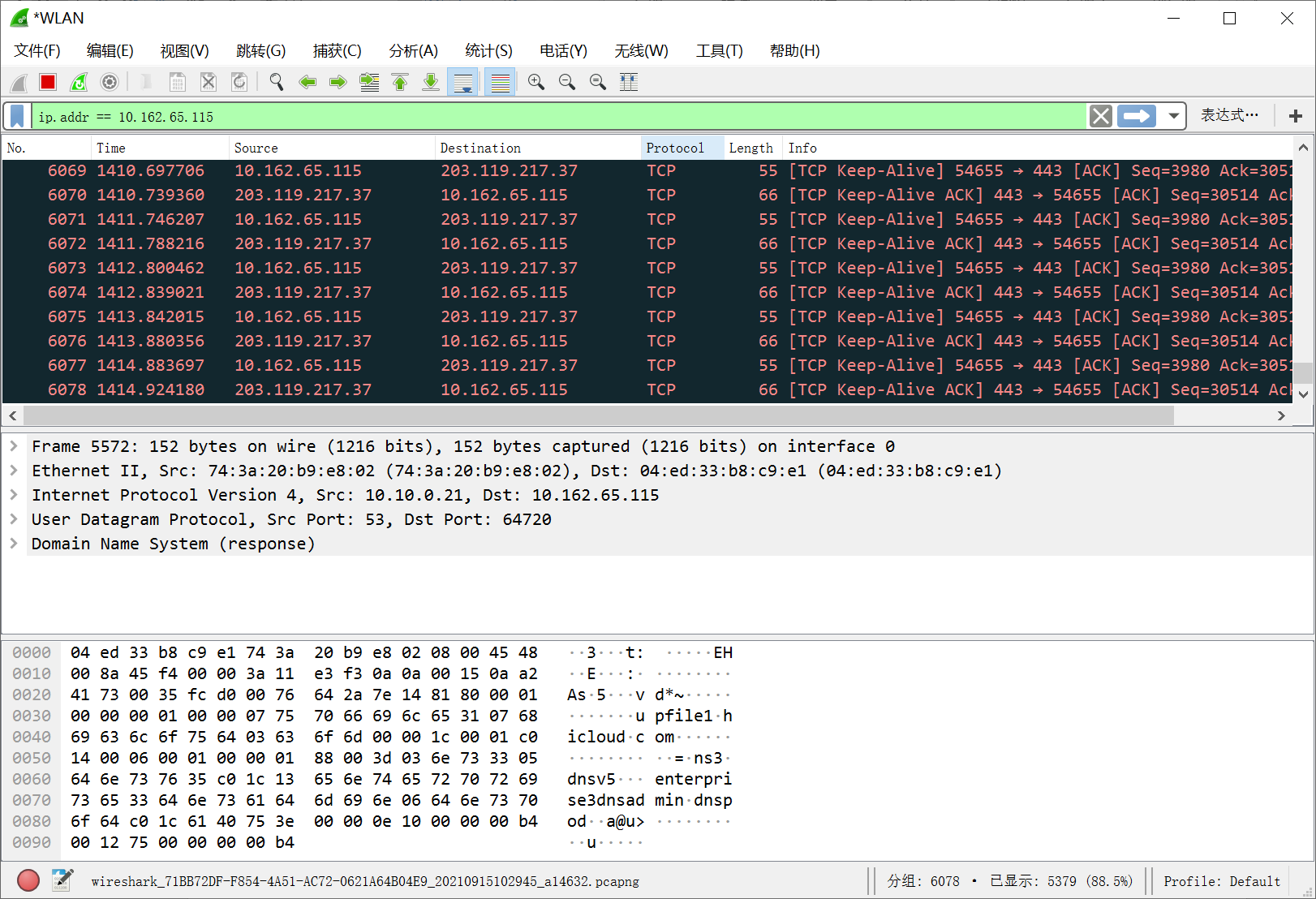
截图：



1. **配置应用显示过滤器，让界面只显示某个IP地址的数据包（ip.addr==x.x.x.x）。**

使用的过滤器：ip.addr==10.162.65.115 ，希望显示的IP地址： 10.162.65.115 。

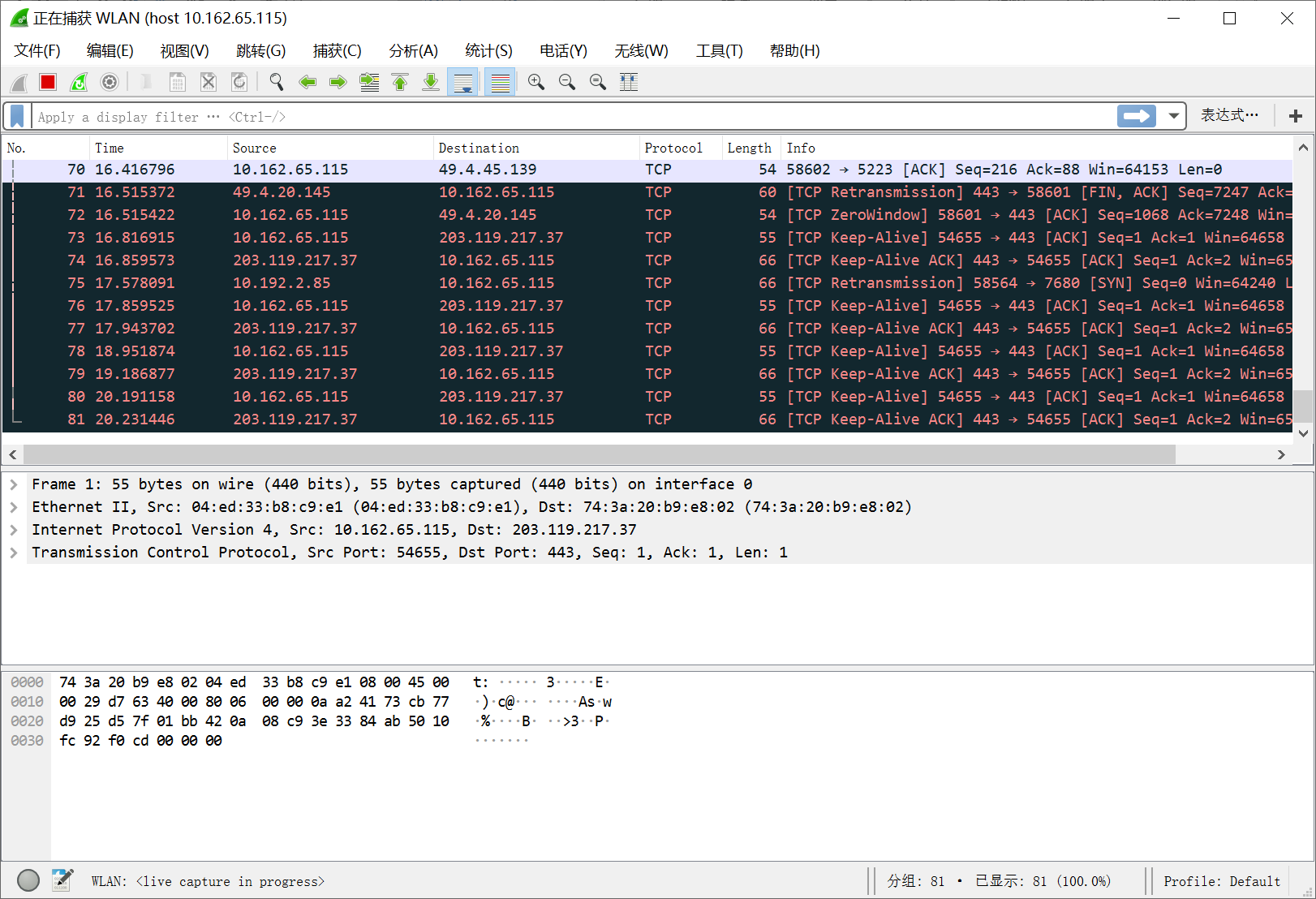
截图：



1. **配置捕获过滤器，只捕获某个IP地址的数据包（host x.x.x.x）。**

使用的过滤器： host 10.162.65.115 ，希望捕获的IP地址： 10.162.65.115 。

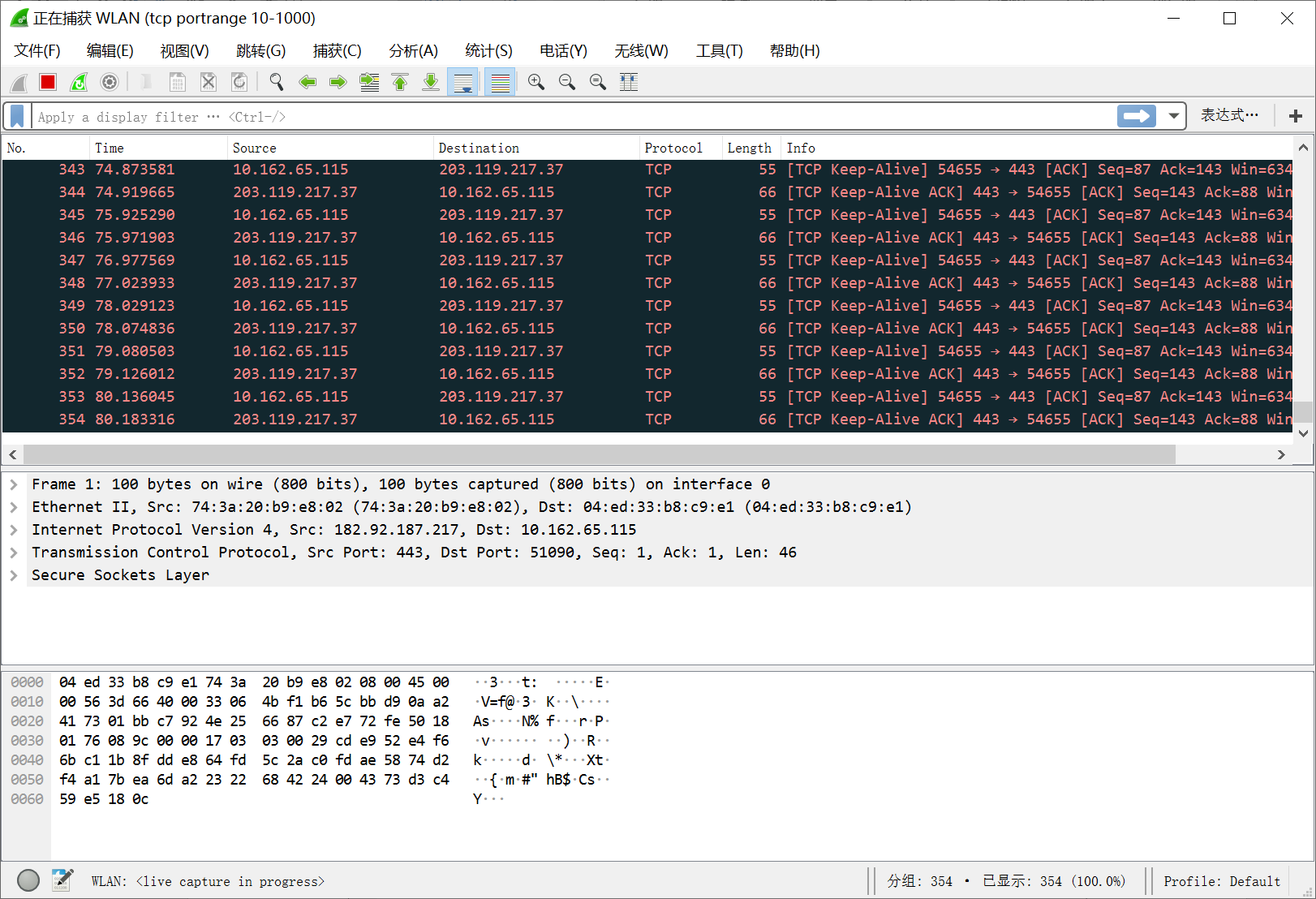
截图：



1. **配置捕获过滤器，只捕获某类协议的数据包（tcp port xx 或者udp port xx）。**

使用的过滤器： tcp portrange 10-1000 ，希望捕获的协议类型： TCP 。

截图：



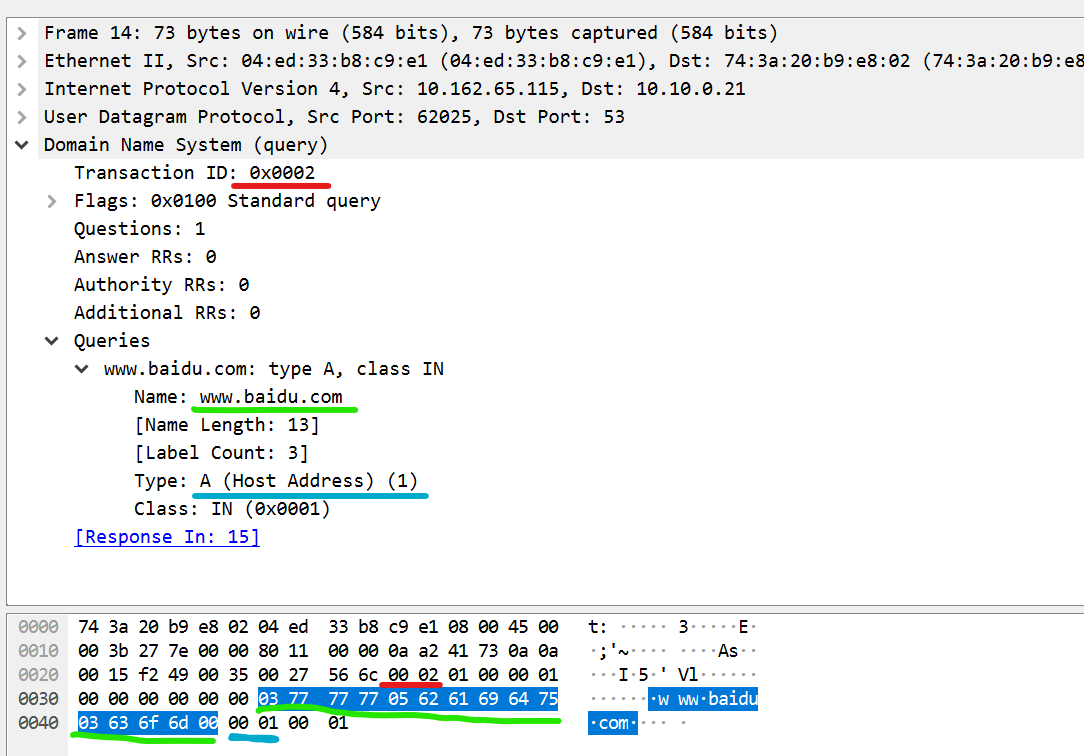
请在下面的每次捕获任务完成后，保存Wireshark抓包记录（.pcap格式），随报告一起提交。每一个任务一个单独文件（如dns.pcap、ping.pcap、tracert.pcap）。

* Part Two

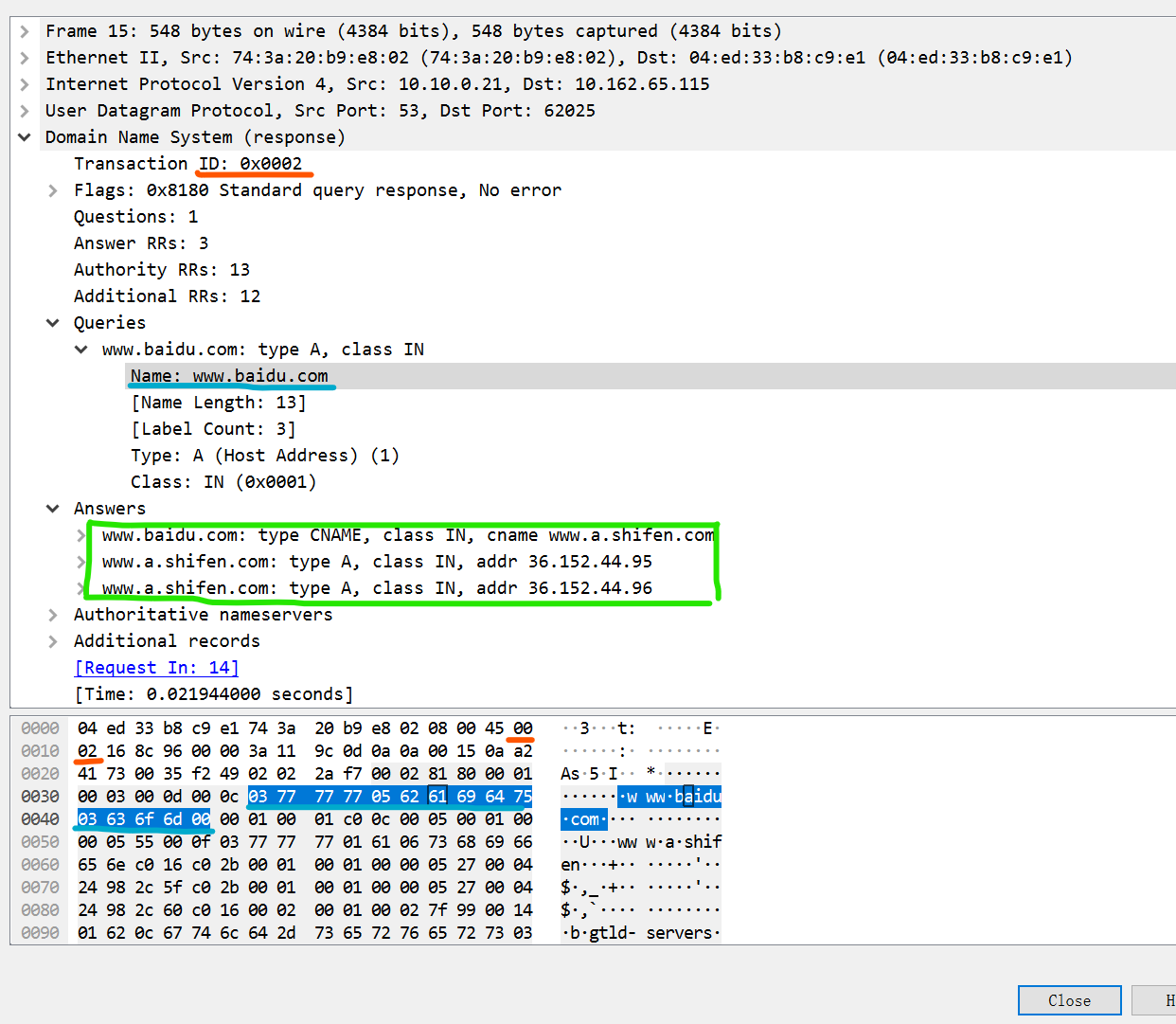
**任务1：使用nslookup命令，查询某个域名，并捕获这次的数据包。DNS数据包由哪几层协议构成？ Ethernet,Ipv4,UDP,DNS 。 使用的服务方端口是： 53 。**

**分别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，标出交易ID、查询类型、查询的域名内容以及查询结果。**

请求：



响应：



**任务2：使用Ping命令，分别测试某个IP地址和某个域名的连通性，并捕获数据包。捕获到了哪些相关协议数据包？**

Ping IP地址时： ICMP

Ping域名时： ICMP

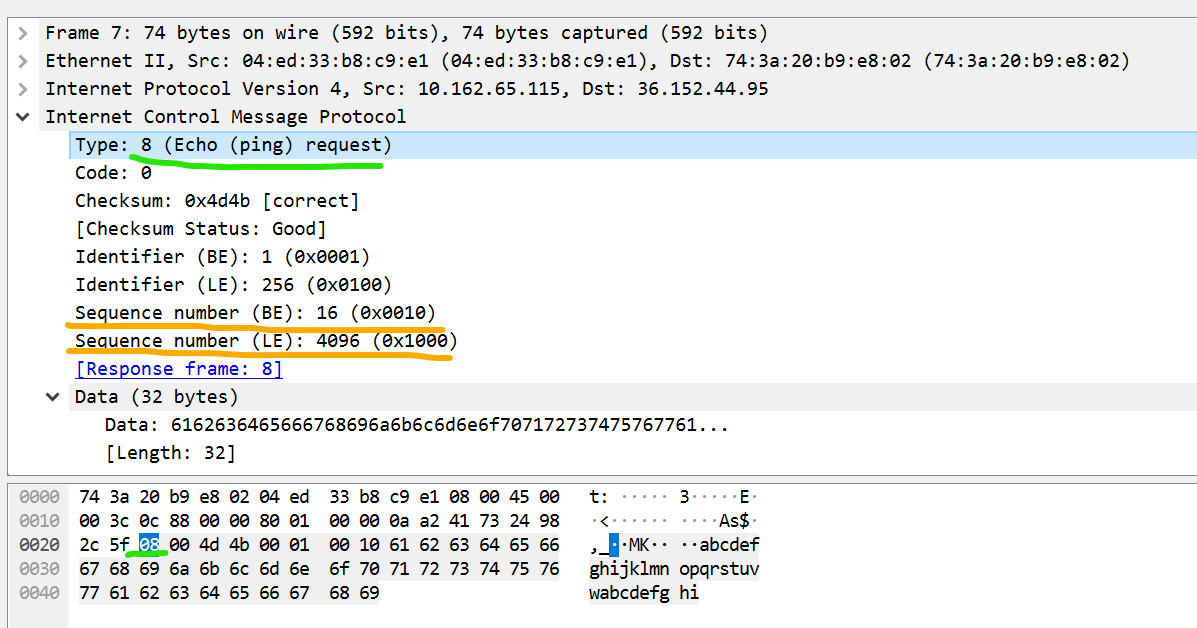
ICMP数据包分别由哪几层协议构成？ Ethernet,IPv4,ICMP

**分别选择一个ARP请求和响应数据包，展开最高层协议的详细内容，标出操作码、发送者IP地址、发送者MAC地址、查询的目标IP地址、Ethernet层的目标MAC地址以及查询结果。**

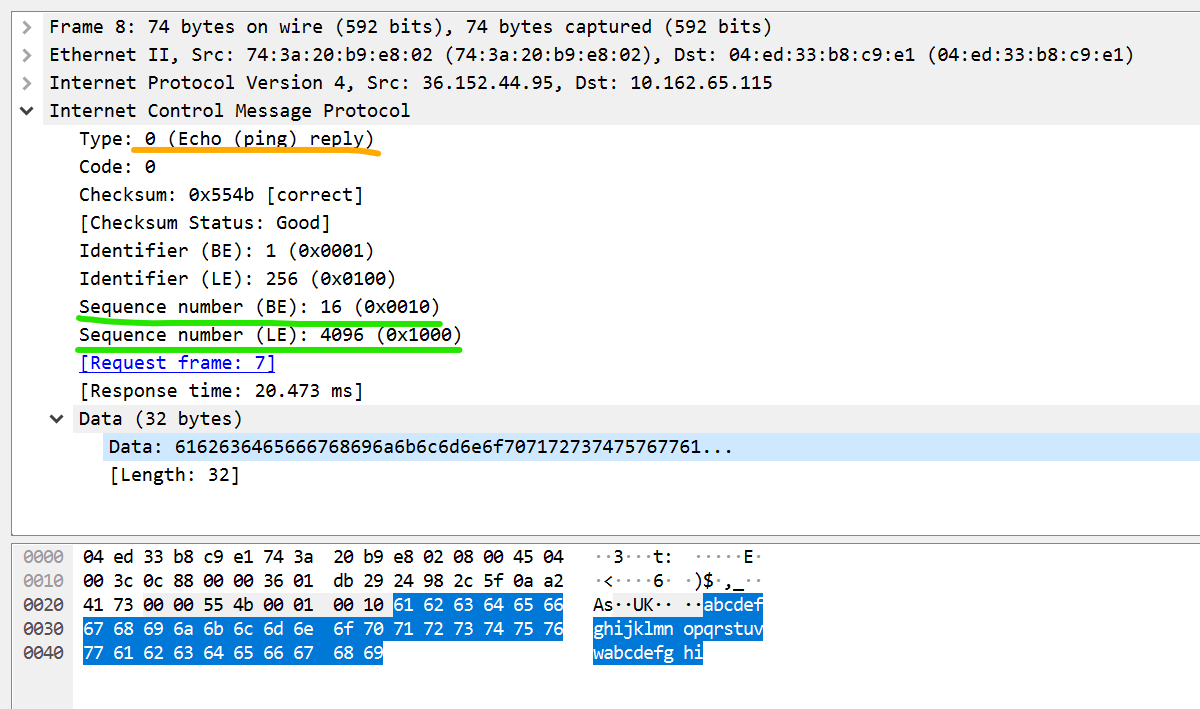
**无ARP协议的数据包。**

**分别选择一个ICMP请求和响应数据包，展开最高层协议的详细内容，标出类型、序号。**

请求：

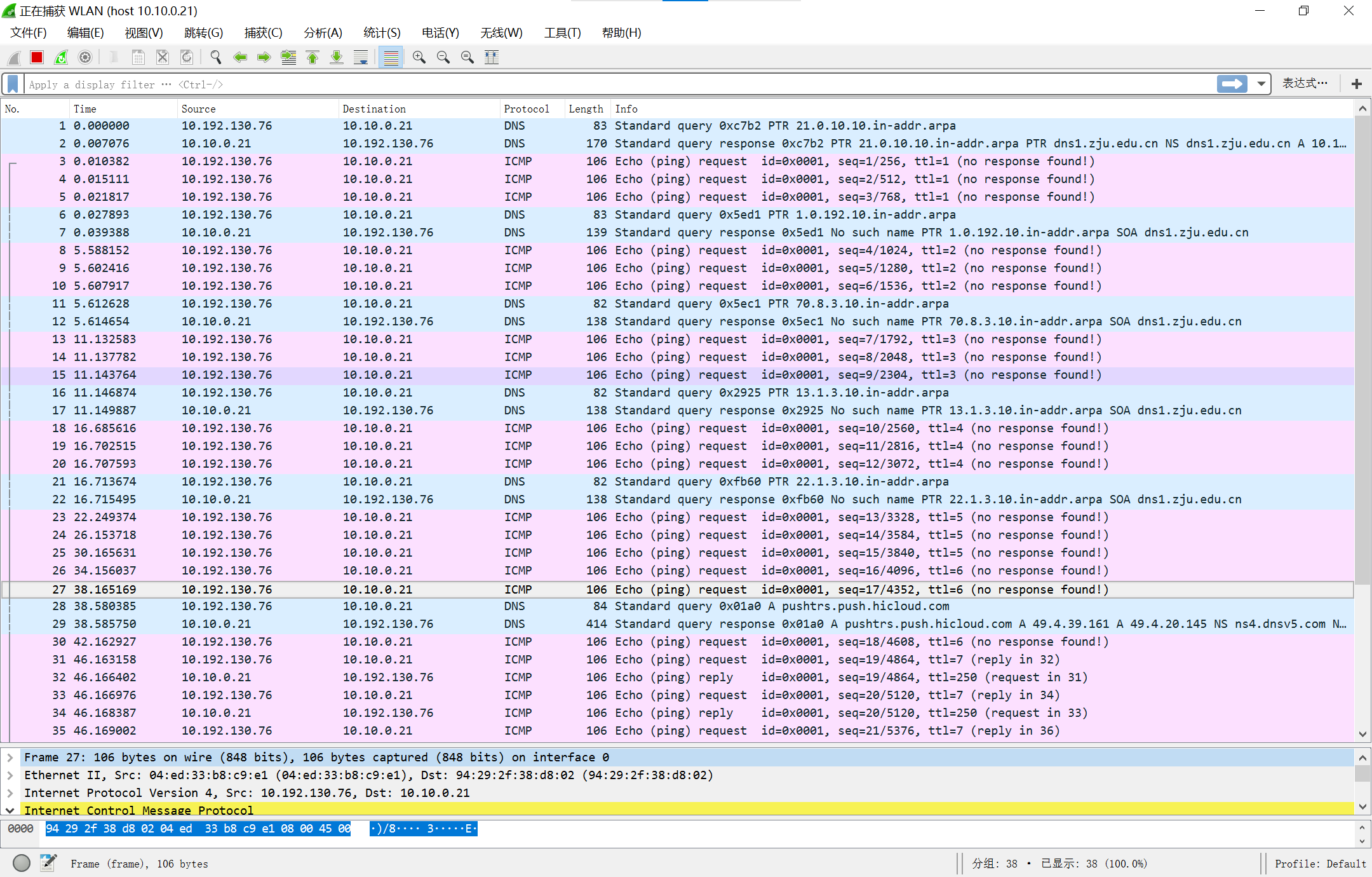


响应：



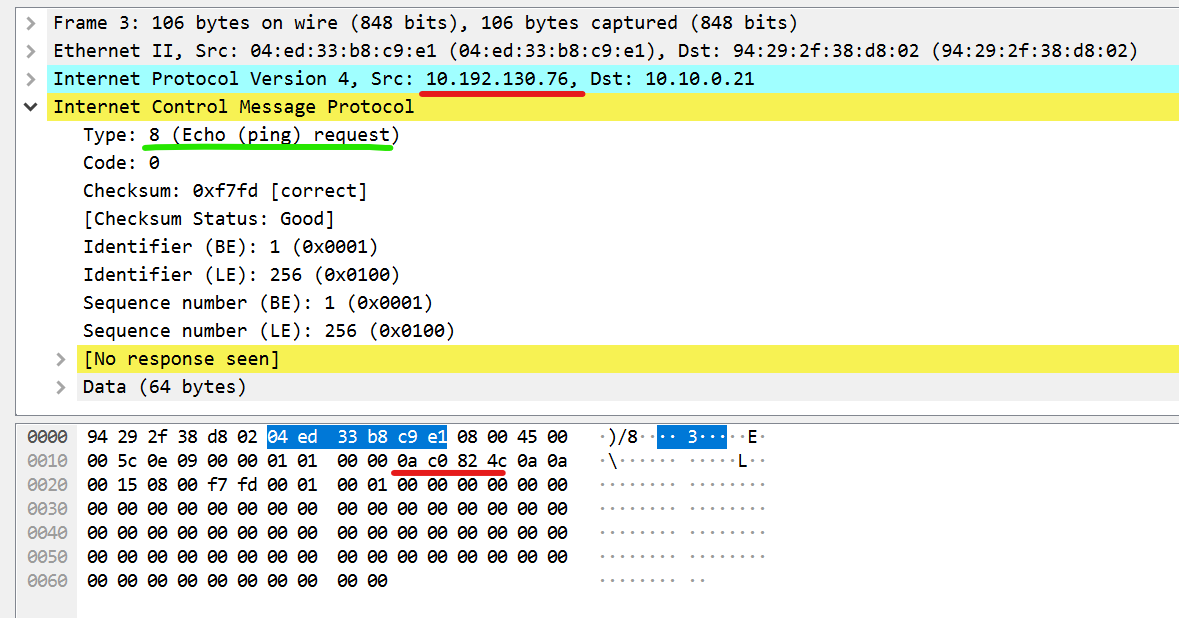
**任务3：使用Tracert命令（Mac下使用Traceroute命令），跟踪某个外部IP地址的路由，并捕获这次的数据包。跟踪路由使用的数据包协议类型是： ICMP ，数据包由几层协议构成？ 3 。**

**观察并记录请求包中IP协议层的TTL字段变化规律，第一个请求的TTL等于 1 ，同样TTL的请求连续发送了 3 个，然后每次TTL增加了 1 ，最后一个请求的TTL等于 7 。附上截图：**

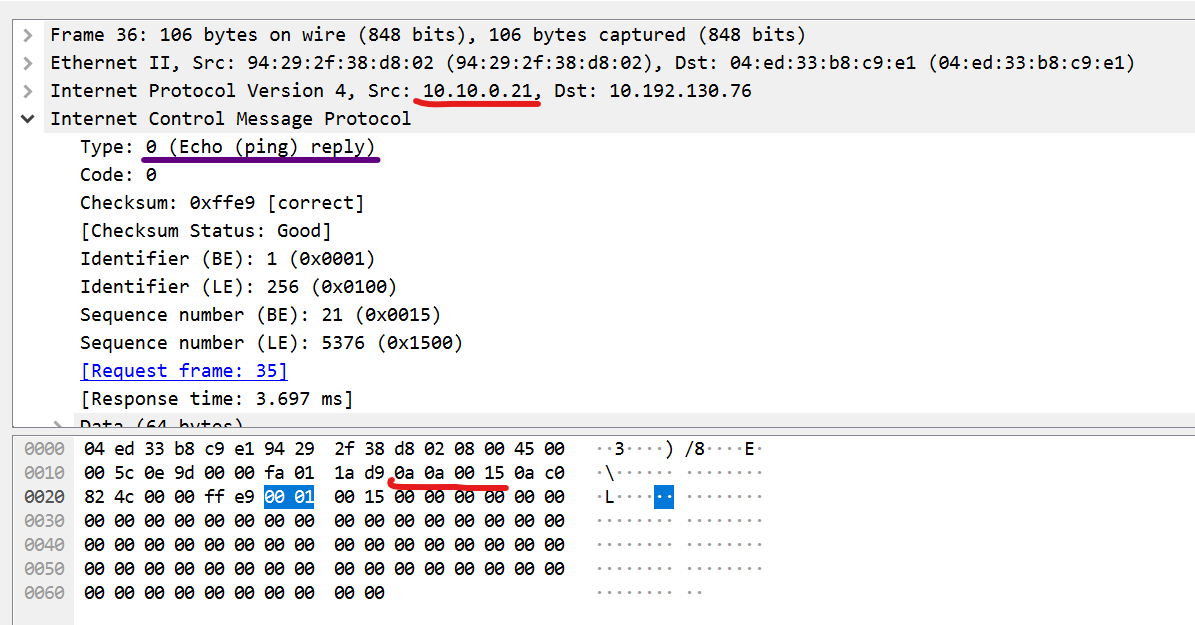
****

**观察并记录响应包的信息，第一组响应包的发送者IP是： 10.192.130.76 ，标记ICMP层的类型字段。最后一组响应包的发送者IP是： 10.10.0.21 ，标记ICMP层的类型字段。附上截图：**

第一组：



最后一组：



请在下面的捕获任务完成后，保存Wireshark抓包记录（.pcap格式），随报告一起提交。文件名http.pcap。

* Part Three

1. **运行ipconfig /flushdns命令清空DNS缓存，然后打开浏览器，访问www.zju.edu.cn，并使用捕获过滤器只捕获访问该网站的数据（过滤器设置：tcp port 80 or udp port 53），网页完全打开后，停止捕获。**

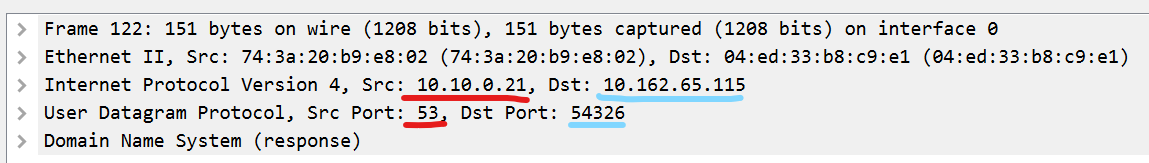
**捕获到的这些最高层的协议数据包分别由哪几层协议构成？**

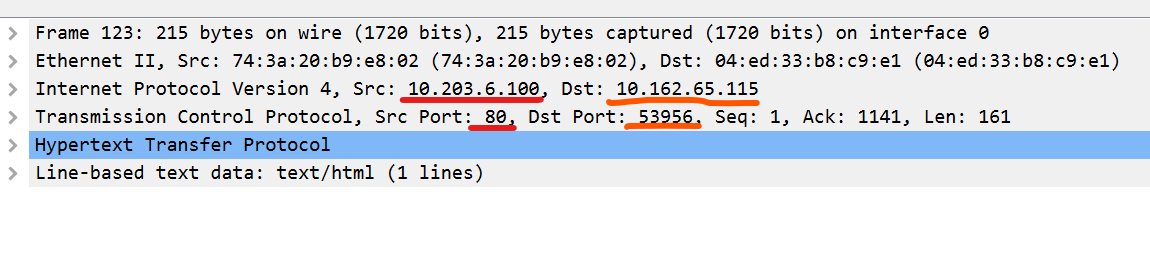
**备注：以访问**[**www.news.zju.edu.cn**](http://www.news.zju.edu.cn)**代替。**

DNS： Ethernet，IP v4，UDP，DNS

HTTP: Ethernet，IP v4，TCP，HTP

**每种协议选取一个代表展开后截图，并标出源和目标IP地址、源和目标端口）**



****

1. **为了打开网页，浏览器查询了哪些相关的域名？**

域名列表： lp.open.weixin.qq.com ， deff.nelreports.net ，www.news.zju.edu.cn ，

www.zju.edu.cn ，zdxb.ihwrm.com ，digi-hzrb.hangzhou.com.cn ，gb.cri.cn ， pic.zju.edu.cn ，www.cctv.com ，www.cyol.net ，www.cnr.cn ，[www.gmw.cn](http://www.gmw.cn) ， www.jyb.com.cn ，[www.news365.com.cn](http://www.news365.com.cn)，[www.peopledaily.com.cn](http://www.peopledaily.com.cn)， [www.sciencenet.cn](http://www.sciencenet.cn) ，[www.wokeji.com](http://www.wokeji.com) ，[www.xinhua.org](http://www.xinhua.org) ，[www.zjdaily.com.cn](http://www.zjdaily.com.cn) ，[www.zjol.com.cn](http://www.zjol.com.cn) ，zhfw.zju.edu.cn

1. **使用显示过滤器tcp.stream eq X，让X从0开始变化，直到没有数据。分析浏览器为了获取网页数据，总共建立了几个连接？（一个TCP流对应一个TCP连接）**

TCP连接数： 5

1. **右键点击某个HTTP数据包，选择跟踪TCP流，可以看到HTTP会话的数据。分析浏览器与WEB服务器之间进行了几次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。**

HTTP会话数： 1

1. **选择一个HTTP的TCP流进行截图，标出请求和响应部分（最好有多个HTTP会话的）：**

****

# 实验结果分析与思考

* 如果只想捕获某个特定WEB服务器IP地址相关的HTTP数据包，捕获过滤器应该怎么写？

tcp port http and host x.x.x.x

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

ICMP请求类型的数据包。

如果在本地 ARP 映射表中查找出 IP 地址 192.168.1.2 所对应的 MAC地址，则可以直接使用；如果没有，则需要发送 ARP 协议查询 MAC 地址。

Ping域名可能得到域名的多个ip。

* 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？

ICMP。

客户端依次发送TTL递增的ICMP请求数据包，得到下一次跳转的地址，直到发送到目标地址并得到目标主机发送的应答数据。

* 如何理解TCP连接和HTTP会话？他们之间存在什么关系？

TCP建立连接需要经过三次握手，HTTP每次传输数据都需要服务器响应客户端的请求。

TCP是传输层协议，HTTP是应用层协议，HTTP是基于TCP连接的基础进行的，在完成TCP连接以后，应用层就以HTTP协议开始数据的收发。

* DNS为什么选择使用UDP协议进行传输？而HTTP为什么选择使用TCP协议？

DNS通常只进行一次会话，即只有一次请求和对应的应答，而通过TCP协议建立连接即需要三次握手，是一种对资源的浪费，使用UDP协议更加高效。

HTTP选择TCP协议因为HTTP需要一直保持连接发生连续的请求和应答，这样一来三次握手的资源占用就无足轻重而TCP使得传输服务更可靠。

# 讨论、心得

在完成本实验后，你可能会有很多待解答的问题，你可以把它们记在这里，接下来的学习中，你也许会逐渐得到答案的，同时也可以让老师了解到你有哪些困惑，老师在课堂可以安排针对性地解惑。等到课程结束后，你再回头看看这些问题时你或许会有不同的见解：

·浏览器能不能直接通过ip地址访问网页？

·如果一个域名对应的有不止一个ip地址，怎么决定哪一个被连接？

·日常使用的网页链接和域名有什么区别？

在实验过程中你可能会遇到的困难，并得到了宝贵的经验教训，请把它们记录下来，提供给其他人参考吧：

·wireshark捕获和过滤的语法格式不尽相同。

·了解终端的命令的大致含义有助于理解抓取的数据包。

你对本实验安排有哪些更好的建议呢？欢迎献计献策：