

**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： | 颜晗 |
| 学 院： | 计算机学院 |
| 系： |  |
| 专 业： | 计算机科学与技术 |
| 学 号： | 3200105515 |
| 指导教师： | 张泉方，杨樾人 |

2022年 10 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

# 实验数据记录和处理

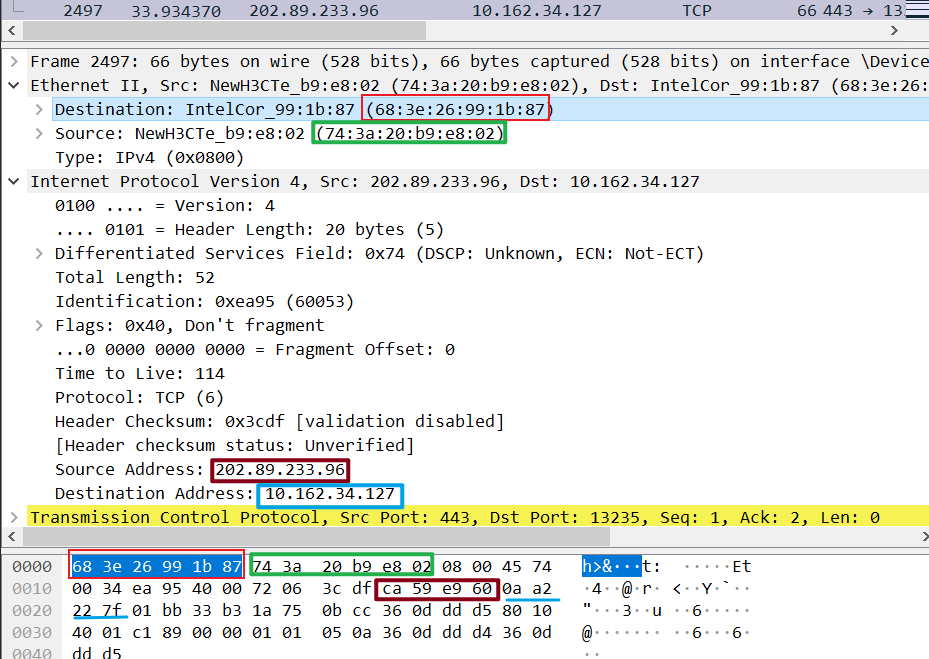
* Part One

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, TLSv1.2, UDP, DNS, DHCPv6, TLSv1.3, HTTP

1. **找一个包含IP的数据包，这个数据包有 4 层？最高层协议是 Transmission Control Protocol ，从Ethernet开始往上，各层协议的名字分别为 Internet protocol , Transmission Control Protocol 。**

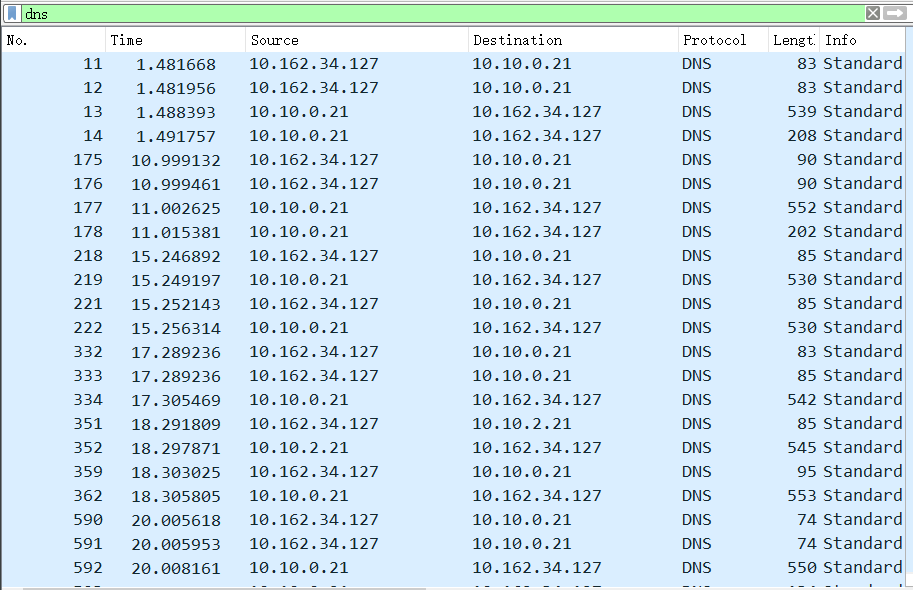
**展开IP层协议，标出源IP地址、目标IP地址及其在数据包中的具体位置，展开Ethernet层，标出源MAC地址和目标MAC地址及其在数据包中的具体位置。**



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 。

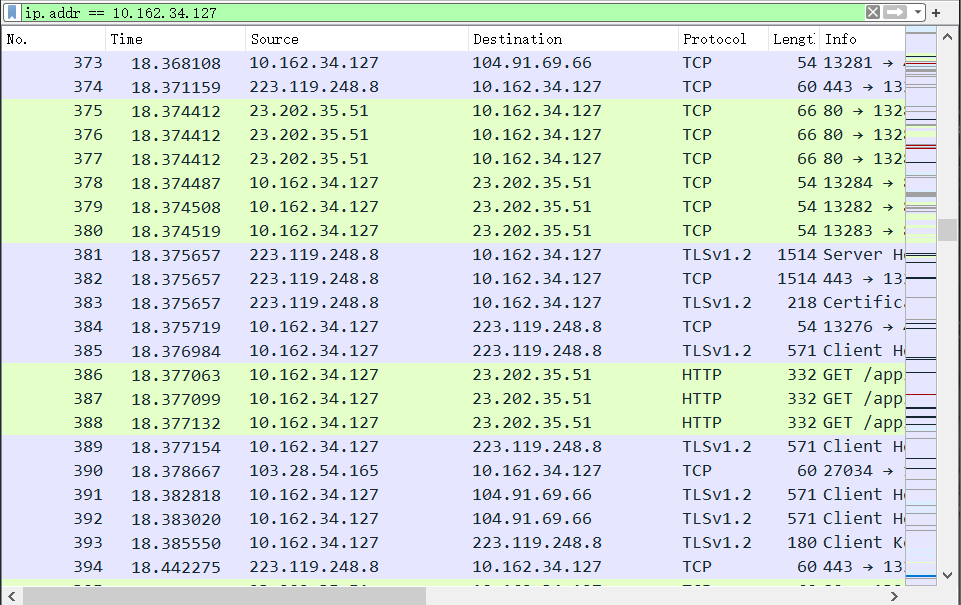
截图：



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 == 10.162.34.127 ，希望显示的IP地址： 10.162.34.127 。

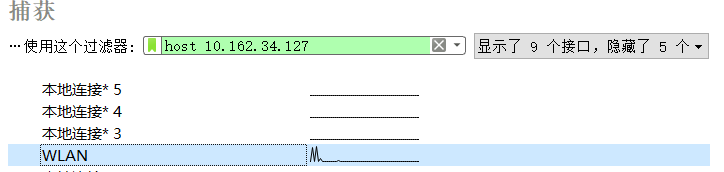
截图：

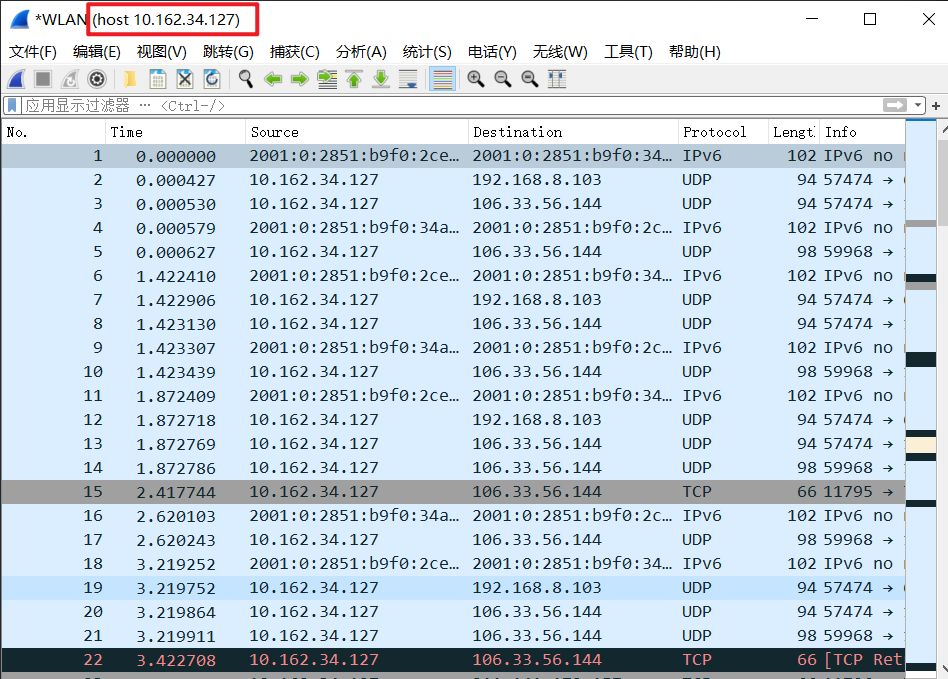


1. **配置捕获过滤器，只捕获某个IP地址的数据包（host x.x.x.x）。**

使用的过滤器： host 10.162.34.127 ，希望捕获的IP地址： 10.162.34.127 。

截图：

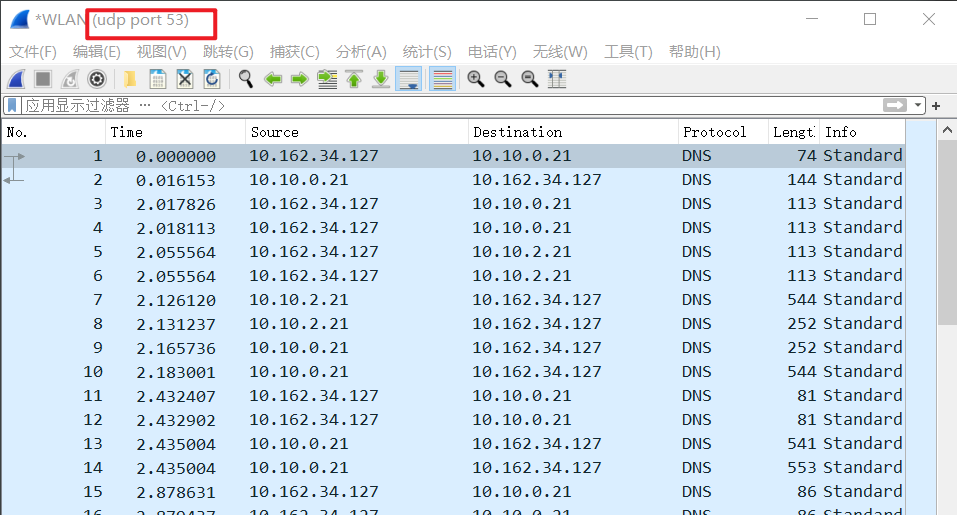




1. **配置捕获过滤器，只捕获某类协议的数据包（tcp port xx 或者udp port xx）。**

使用的过滤器： udp.port == 53 ，希望捕获的协议类型： UDP 。

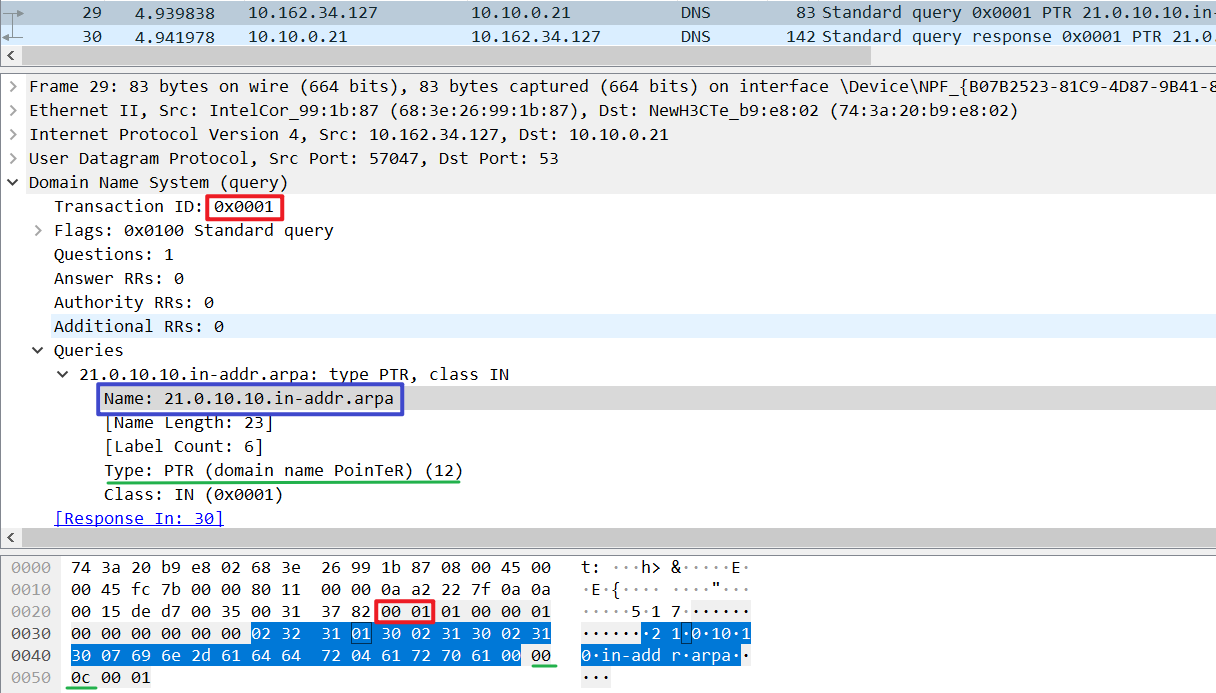
截图：

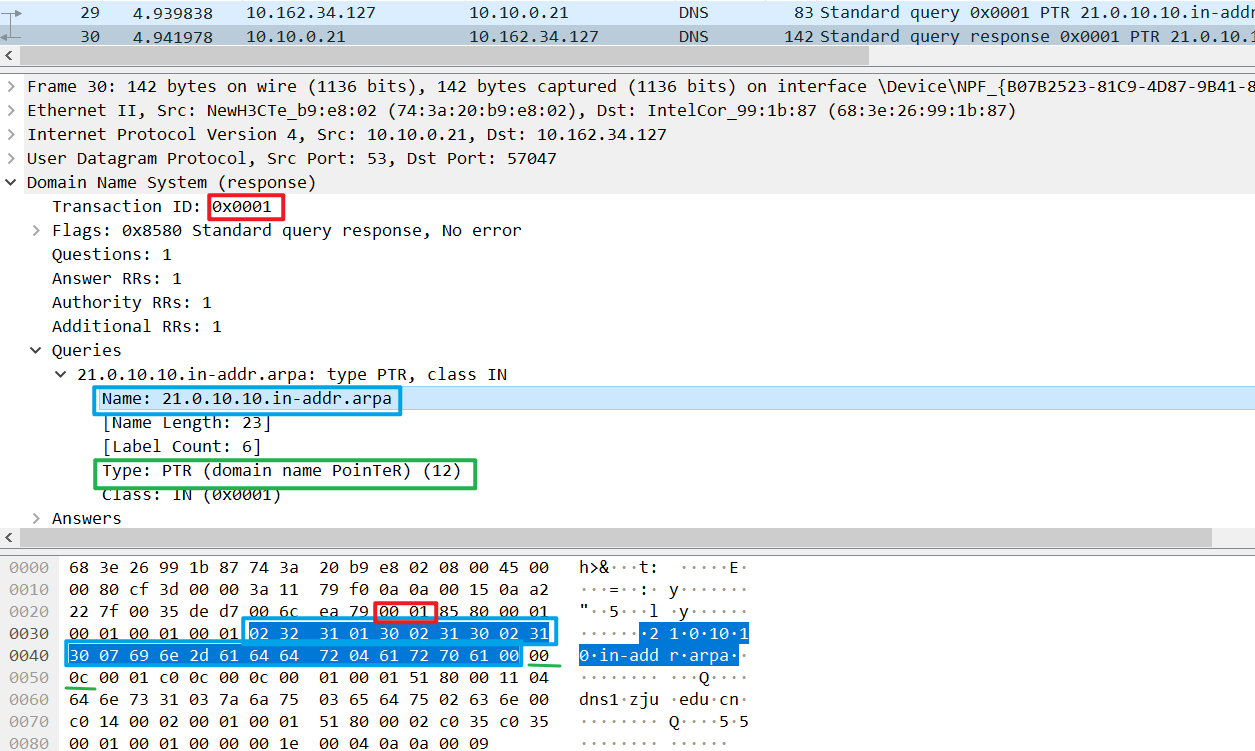


* Part Two

**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？ Frame, Ethernet, Ipv4, UDP, DNS 共五层 。 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。**





**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？**

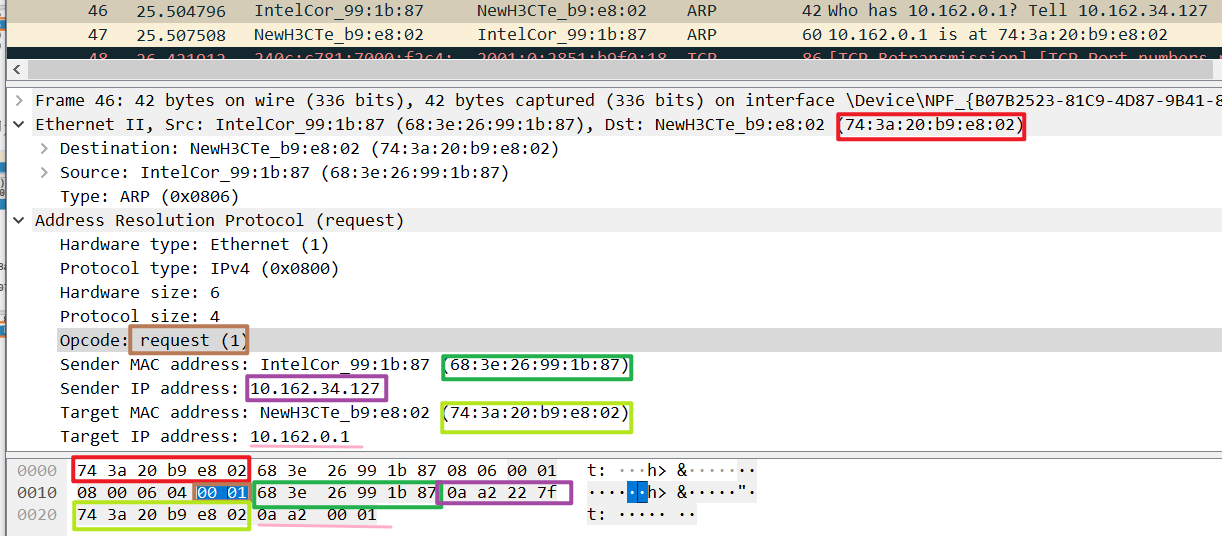
Ping IP地址时： ICMP

Ping域名时： DNS, ICMP

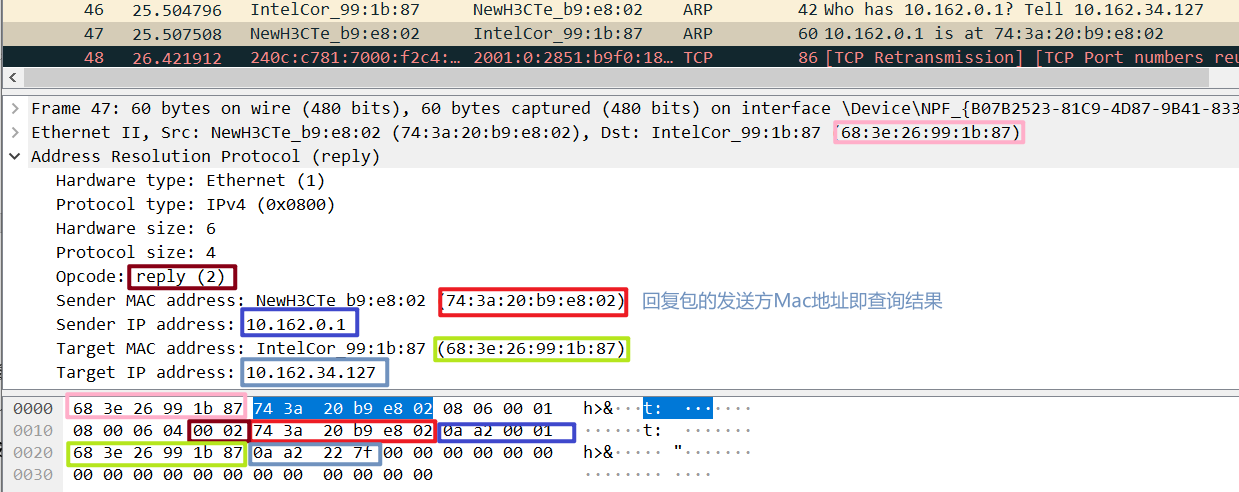
ICMP数据包分别由哪几层协议构成？ Frame, Ethernet, Ipv4, ICMP

**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。**

**ARP请求包：**

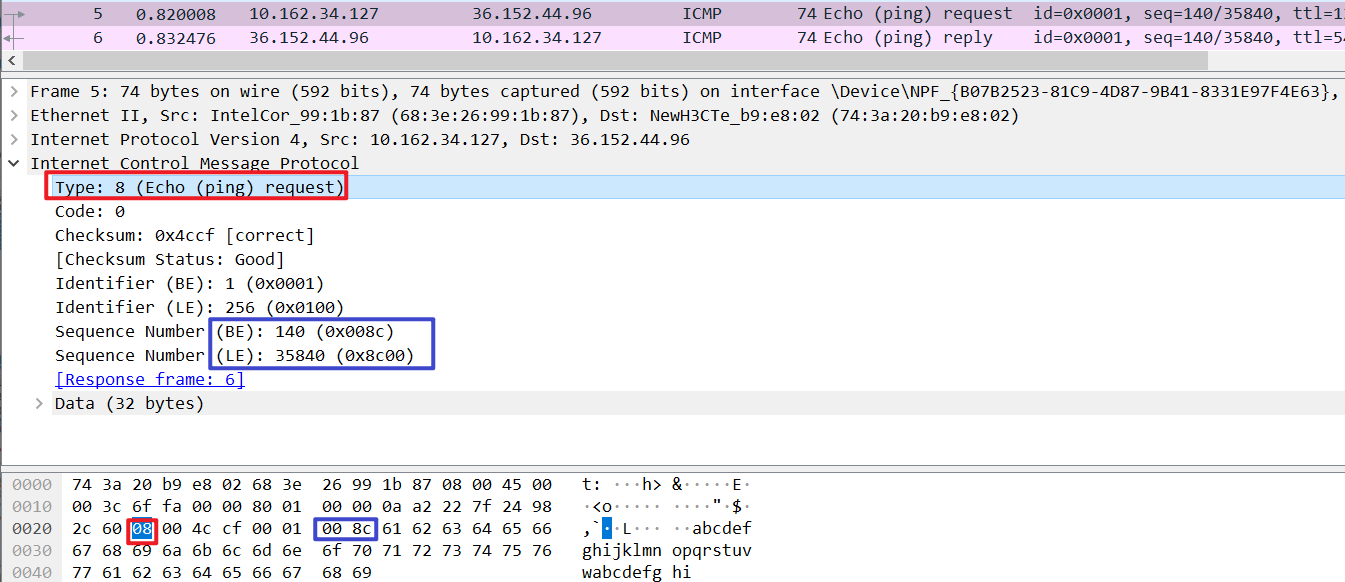


**ARP响应包：**

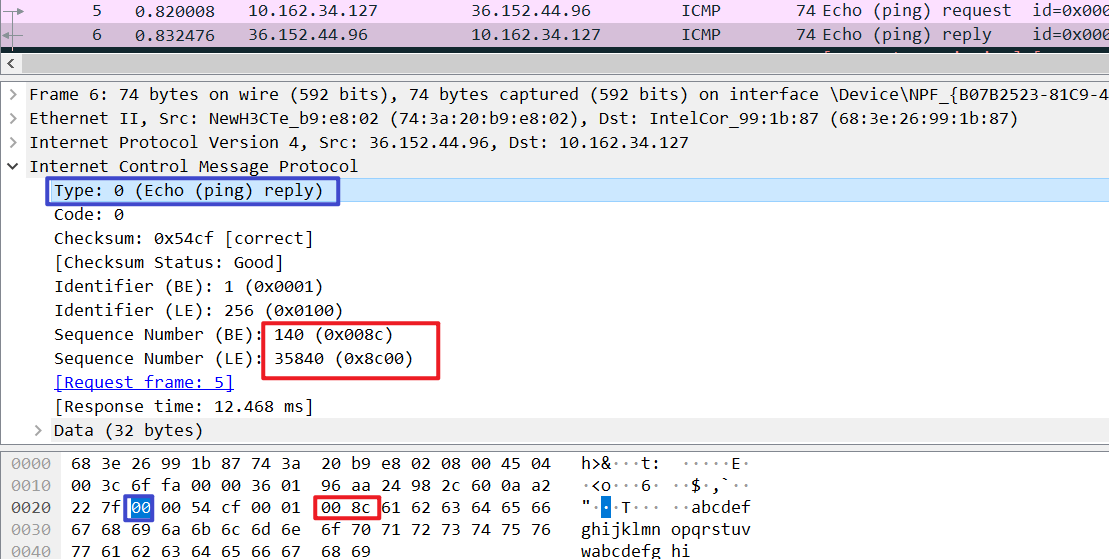


**分别选择一个ICMP请求和响应数据包，展开最高层协议的详细内容，标出类型、序号。**

ICMP请求数据包：

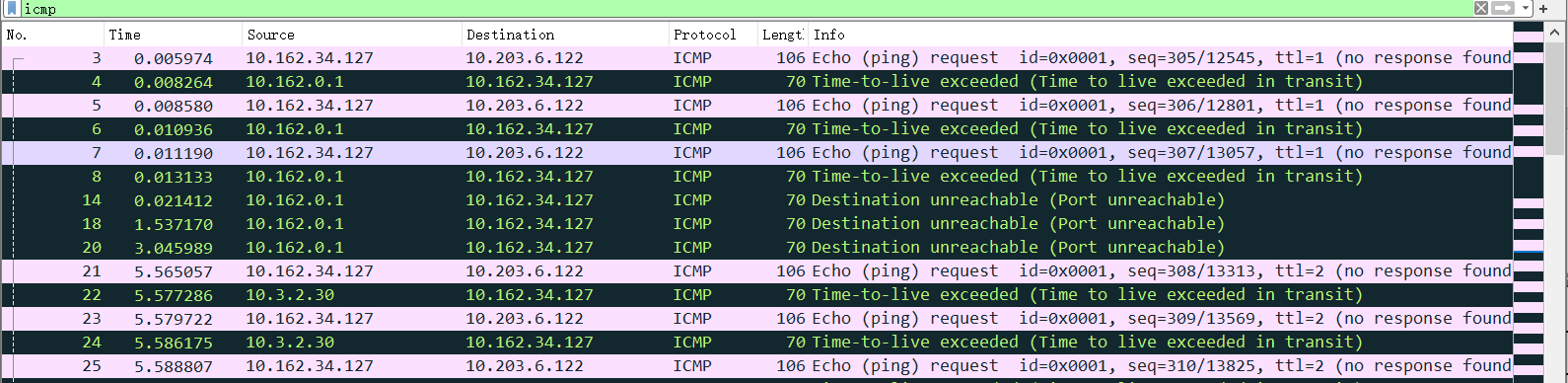


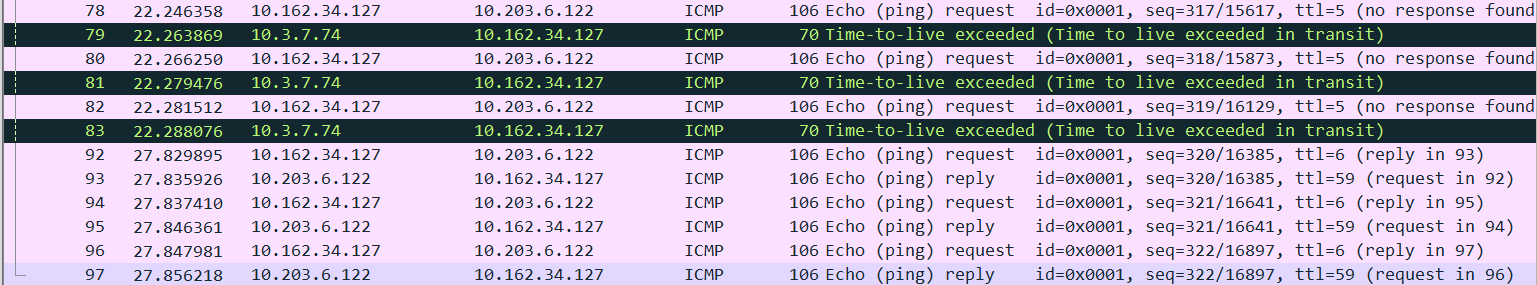
ICMP响应数据包：



**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？ 4层，Frame,Ethernet, Ipv4,ICMP 。**

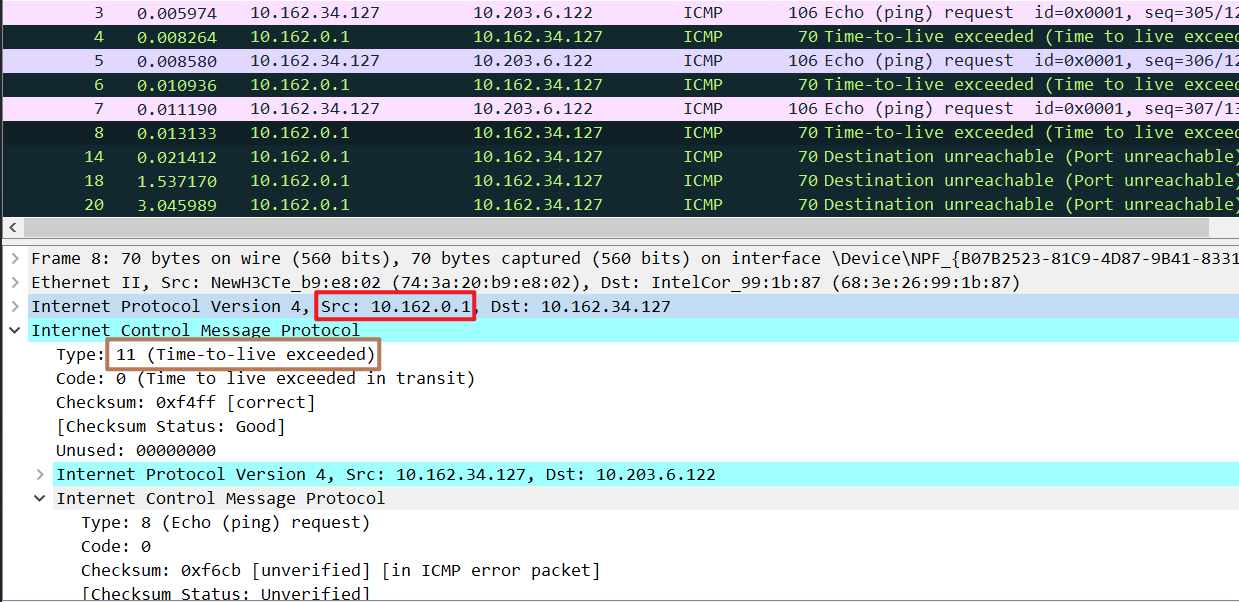
**观察并记录请求包中IP协议层的TTL字段变化规律，第一个请求的TTL等于 1 ，同样TTL的请求连续发送了 3 个，然后每次TTL增加了 1 ，最后一个请求的TTL等于 6 。附上截图：**



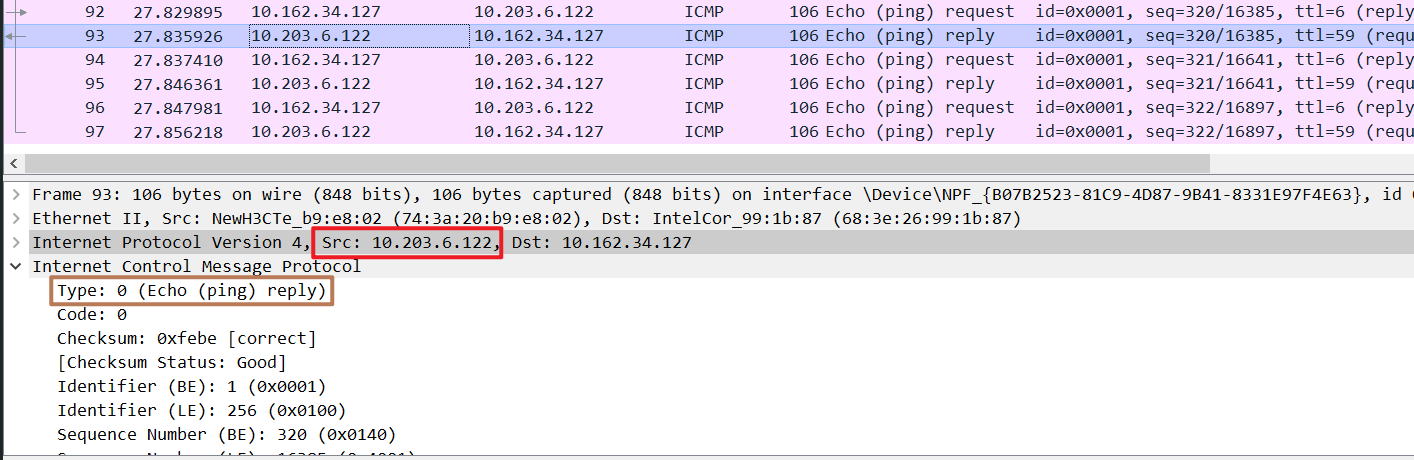


**观察并记录响应包的信息，第一组响应包的发送者IP是： 10.162.0.1 ，标记ICMP层的类型字段。最后一组响应包的发送者IP是： 10.203.6.122 ，标记ICMP层的类型字段。附上截图：**

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。**

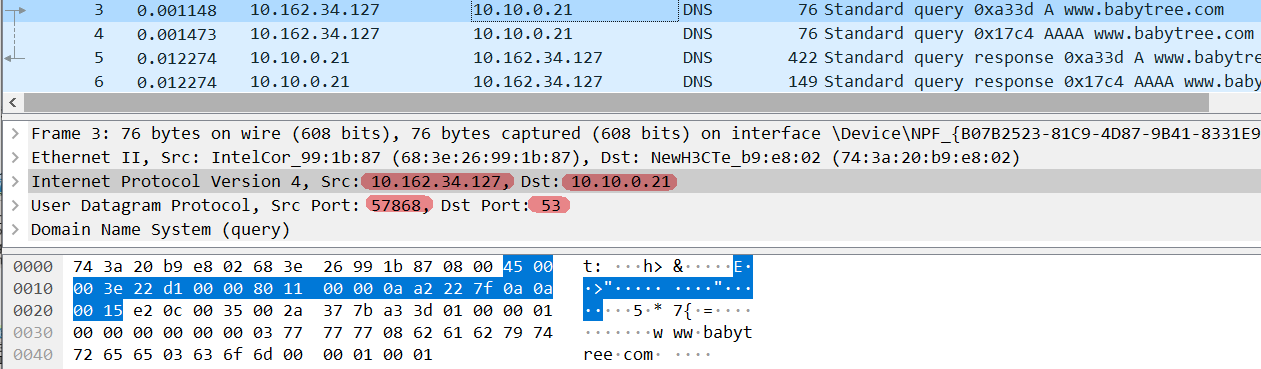
**由于原网站难以捕获到http数据包，访问网站更改为** [**www.babytree.com**](http://www.babytree.com)

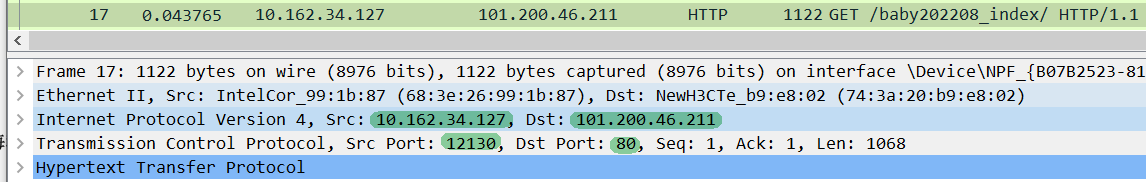
**捕获到的这些最高层的协议数据包分别由哪几层协议构成？**

DNS： 5层： Frame, Ethernet, Ipv4, UDP, DNS

HTTP: 5层： Frame, Ethernet, Ipv4, TCP, HTTP

**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： go.microsoft.com [www.babytree.com](http://www.babytree.com), log.babytree.com, babytree-inc.zhiye.com, beian.miit.gov.cn, hm.baidu.com, cms.babytreeimg.com, pic07.babytreeimg.com, open.babytree.com, r.babytree.com, pic08.babytreeimg.com等非常多域名

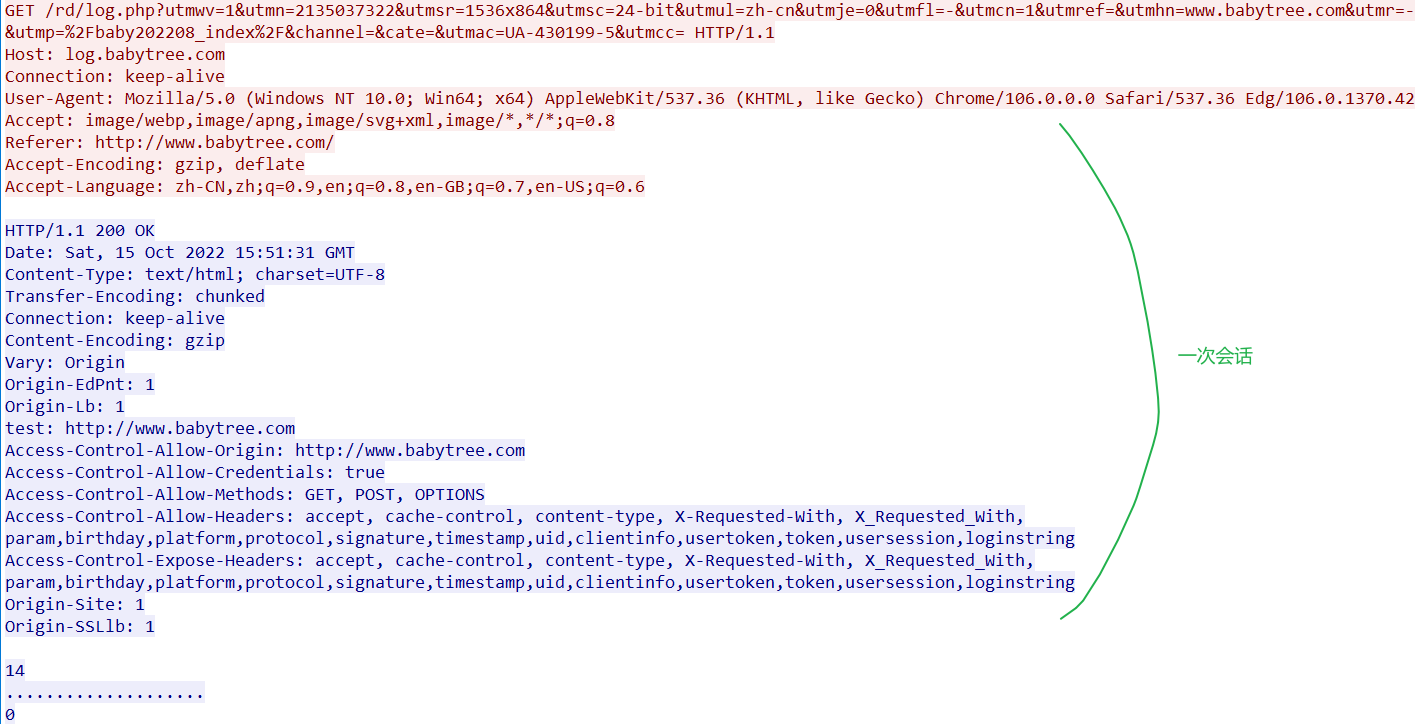
1. **使用显示过滤器tcp.stream eq X，让X从0开始变化，直到没有数据。分析浏览器为了获取网页数据，总共建立了几个连接？（一个TCP流对应一个TCP连接）**

TCP连接数： 5 (0~4)

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： 2

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？

捕获过滤器：tcp port 80 and host [ip]

http数据包默认使用tcp 80端口，在host后填充想捕获的ip地址。

* 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？

Ping 发送的是 ICMP 类型的协议数据包。

当计算机没有缓存所请求的 IP 地址的物理地址时会请求地址解析，出现 ARP 数据包。（正常情况下本机也在一直与默认网关发送arp包）

如果当前计算机内不存在所ping域名对应的IP地址时会先进行域名解析，此时ping一个域名会额外出现DNS数据包。

* 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？

Tracert/Traceroute发送的是ICMP类型的协议数据包，路由追踪过程如下：

由源地址向目标发送不同TTL值的数据包，要求路径上的每个路由器在转发数据包时将TTL减一，当TTL减为0时有，路由器应该将该数据包超时的消息发回源地址，同时包含这一跳路由信息。最开始TTL为1，每次发送时的初始TTL加1，直至最终抵达目的地。

* 如何理解TCP连接和HTTP会话？他们之间存在什么关系？

HTTP是应用层协议，主要解决如何包装数据；而TCP是传输层协议，主要解决数据如何在网络中传输。HTTP 和 TCP 共同帮助信息在网络中正确传达，计算机遵照 HTTP 协议建立会话，封装数据，再通过 TCP 协议进行连接以传输这些数据。缺少任何一个都会使数据传输变得困难。

* 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？

UDP协议只需要一次请求与应答，而TCP有三次握手与四次挥手等多项开销，显然UDP协议有更低的开销与较高的效率。

DNS数据包一般比较小，不用额外分成许多包，丢包重新再发就行，使用UDP协议可提升效率。而HTTP数据包一般比较大，需要分成多次传输，此时TCP的额外开销影响就较小了，且此时TCP可以保证数据传输的稳定可靠性。

因此 DNS 更适合 UDP 协议，而 HTTP 更适合 TCP 协议

# 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：

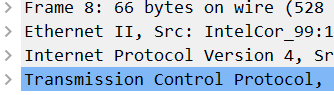
各种网络协议到底是怎么分类的，有什么包含并列关系？frame是协议吗？

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：

关掉了大部分软件依旧有许多无关数据包，混杂其中，对于初学者来说很难分辨那些是实验相关的，那些是无关的。

对网络协议一窍不通，对于lab中的各种名词难明其意，开始问协议究竟问那个也没搞清





你对本实验安排有哪些更好的建议呢？欢迎献计献策：

希望实验提供一些网络协议参考资料，不然懵懂地做完实验其实作用也不大，完全不知道它们在干什么。