浙江大学

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：　李秋宇

学　　院：　计算机学院

系：　计算机系

专　　业：　计算机科学与技术

学　　号：　3220103373

指导教师：　邱劲松

2024 年 9 月 11 日

浙江大学实验报告

一、 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。

二、 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

三、 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

四、 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。

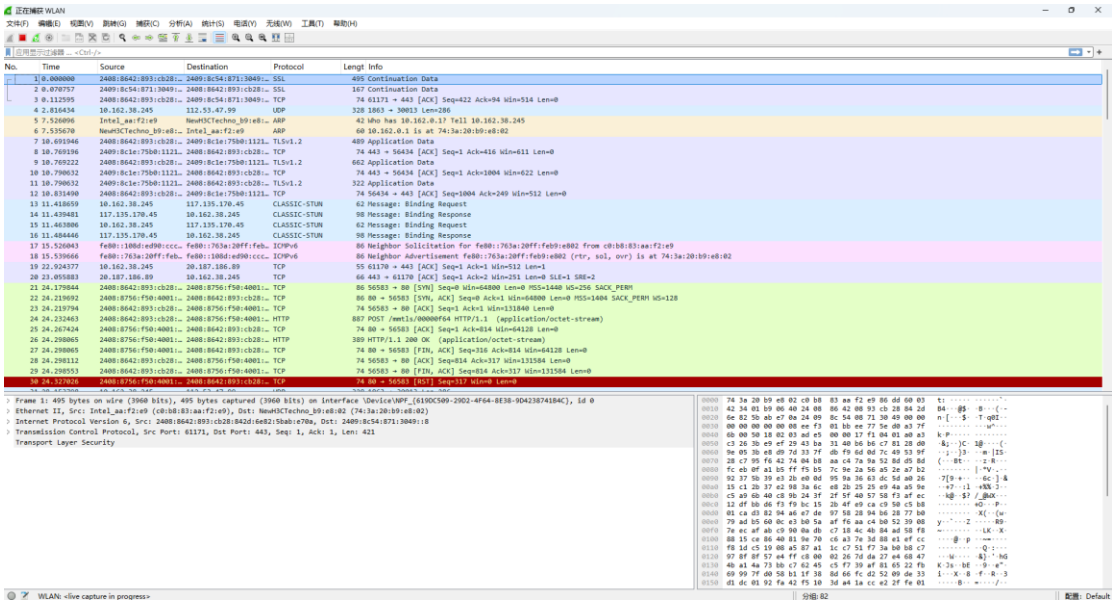
五、 实验数据记录和处理

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：SSL, TCP, UDP, ARP, TLSv1.2, CLASSIC-STUN, ICMPv6, HTTP

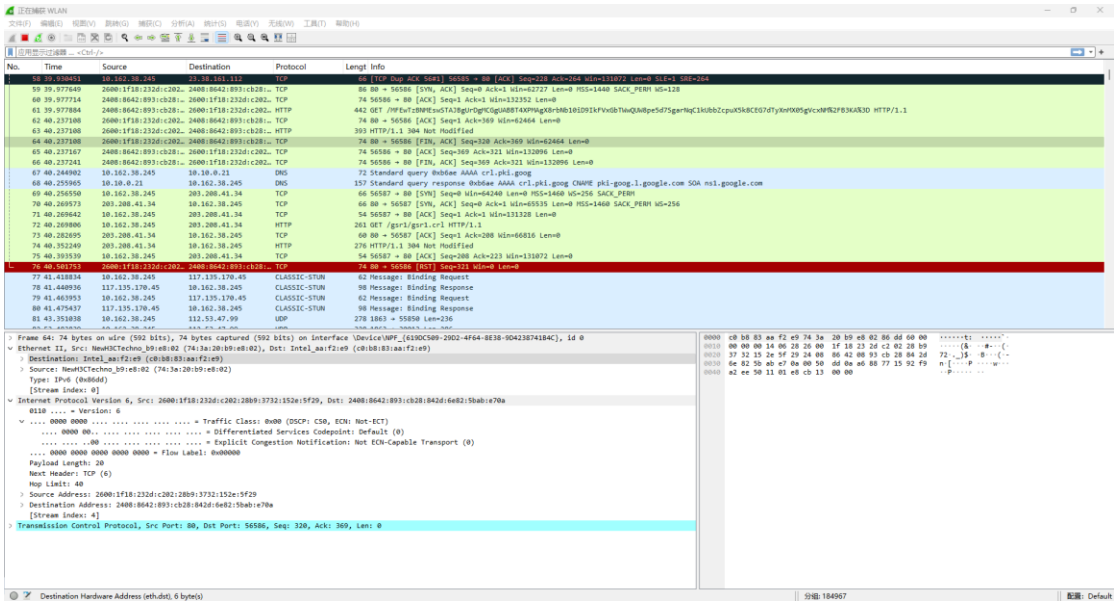


2. **找一个包含 IP 的数据包，这个数据包有 4 层？最高层协议是 TCP，从 Ethernet 开始往上，各层协议的名字分别为：Internet Protocol && Transmission Control Protocol。**

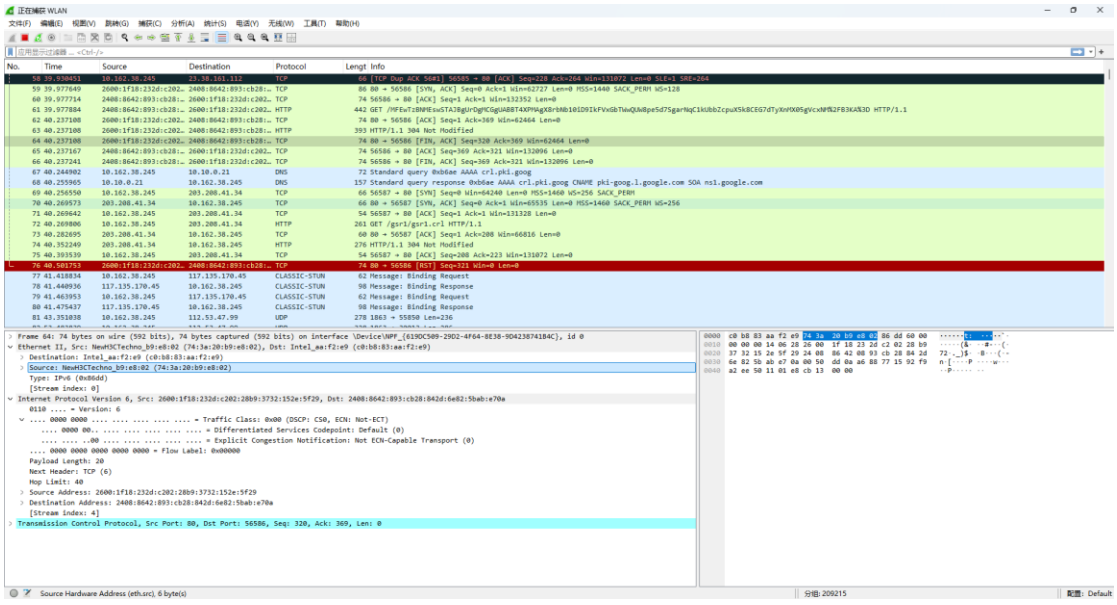
   展开 IP 层协议，标出源 IP 地址、目标 IP 地址及其在数据包中的具体位置，展开 Ethernet 层，标出源 MAC 地址和目标 MAC 地址及其在数据包中的具体位置。

   截图参考（此处应替换成实际截获的数据）：

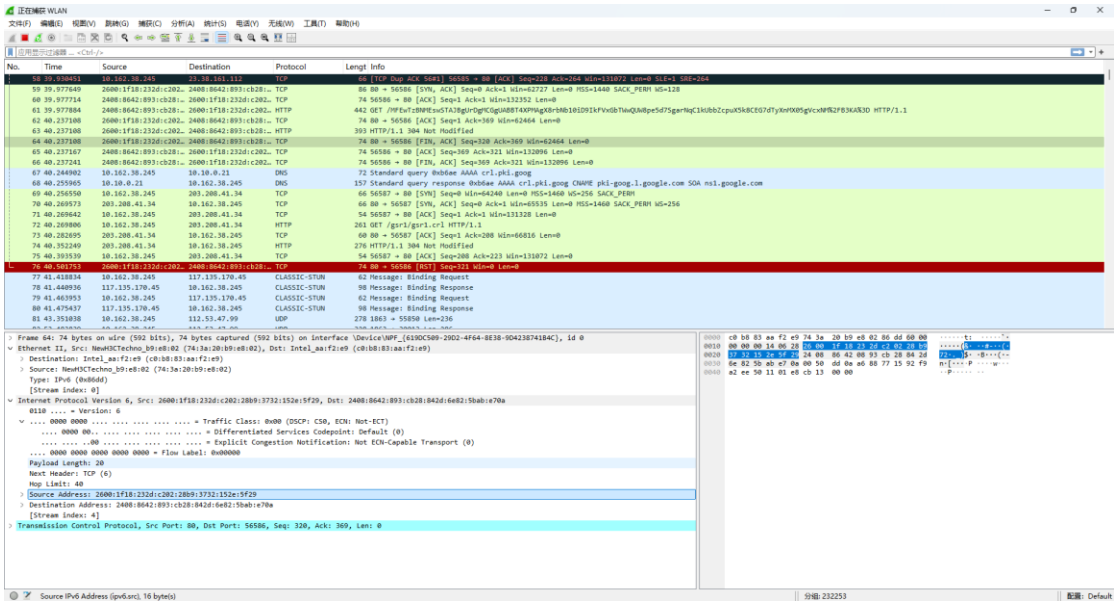
   目标 MAC 地址：



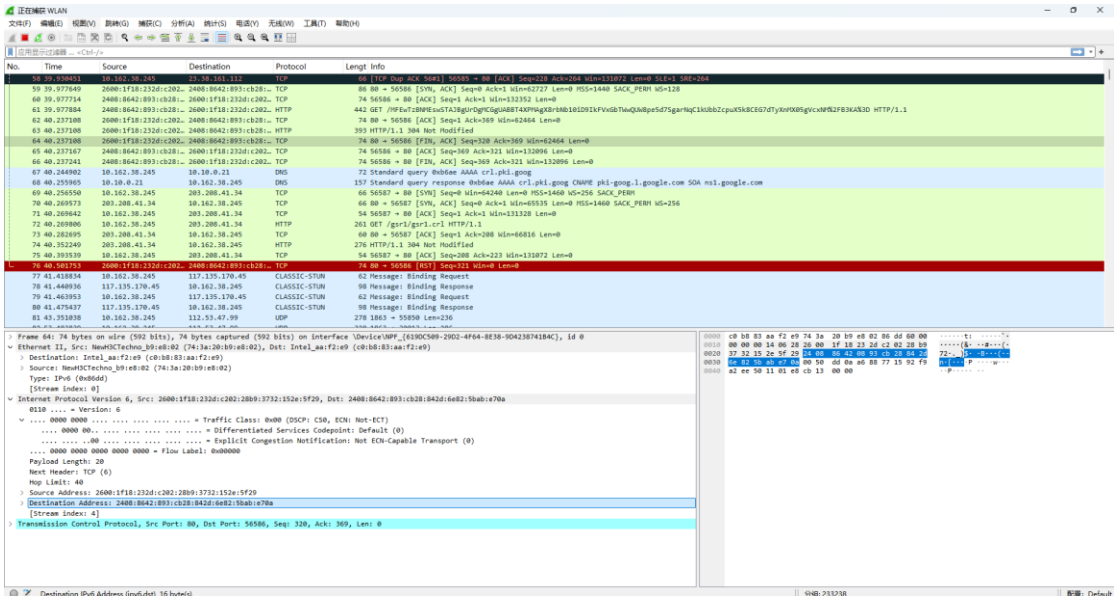
源 MAC 地址：



源 IP 地址：



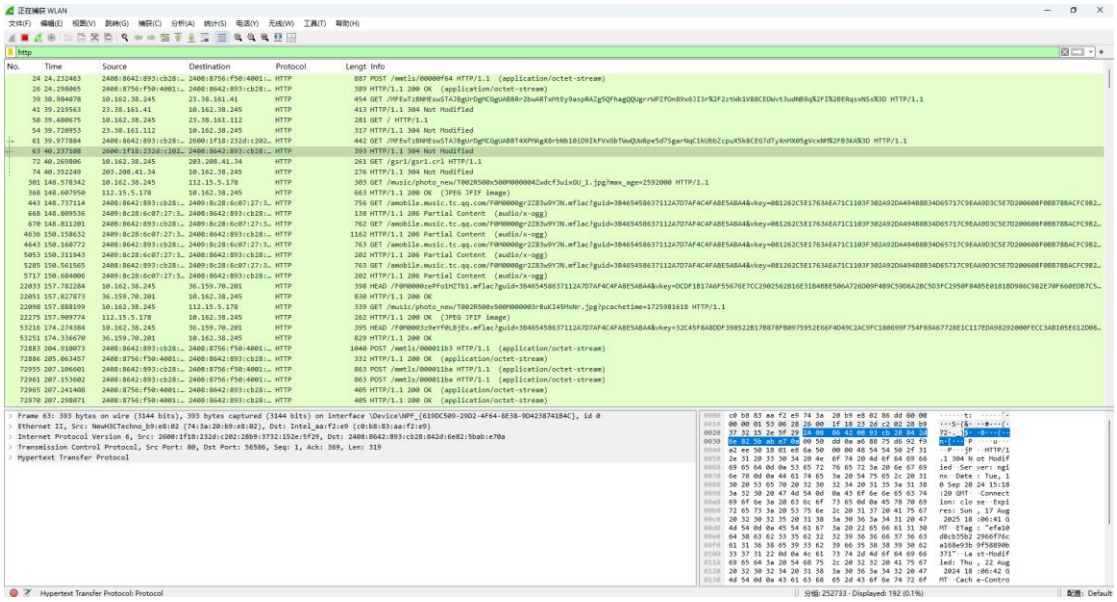
目标 IP 地址：



3. 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：____http____，希望显示的协议类型：_HTTP_____。

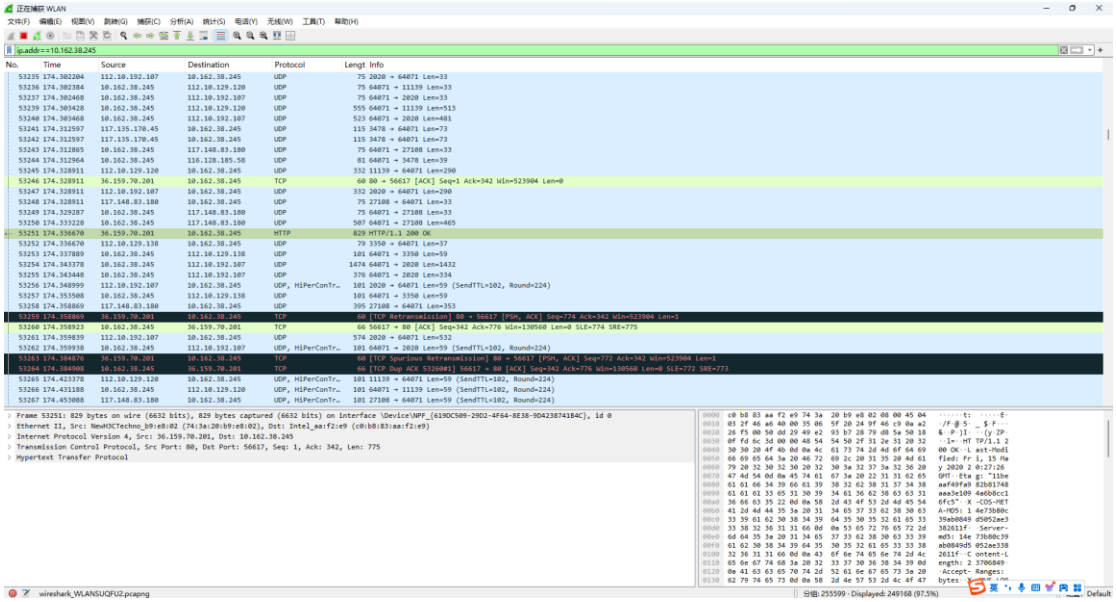
截图：



4. 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 == 10.162.38.245__ ，希望显示的 IP 地址：__10.162.38.245__ 。

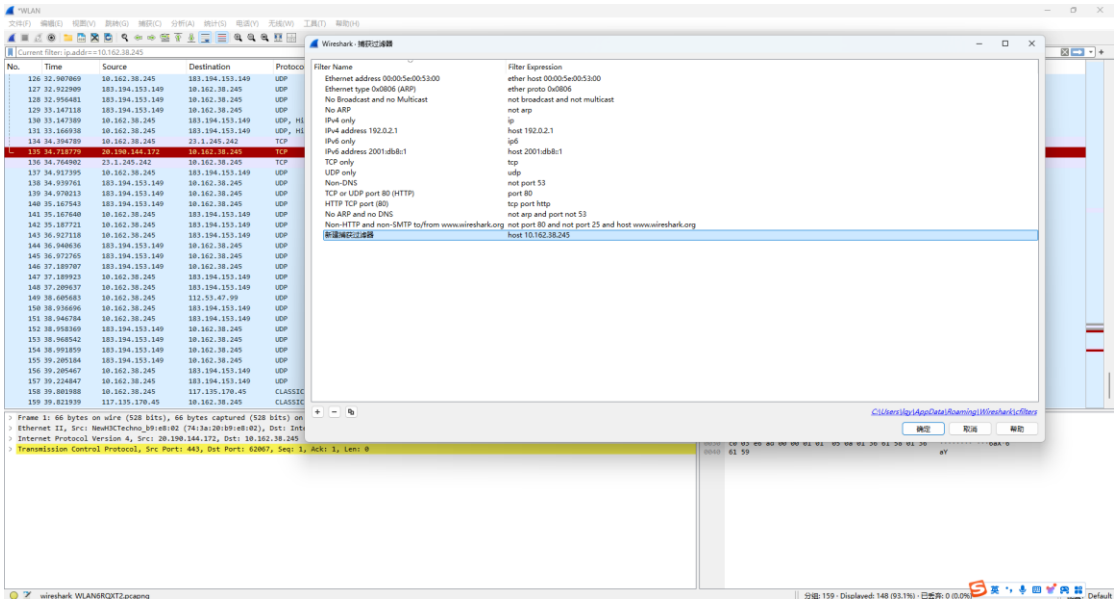
截图：



5. 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 10.162.38.245__ ，希望捕获的 IP 地址：__10.162.38.245__ 。

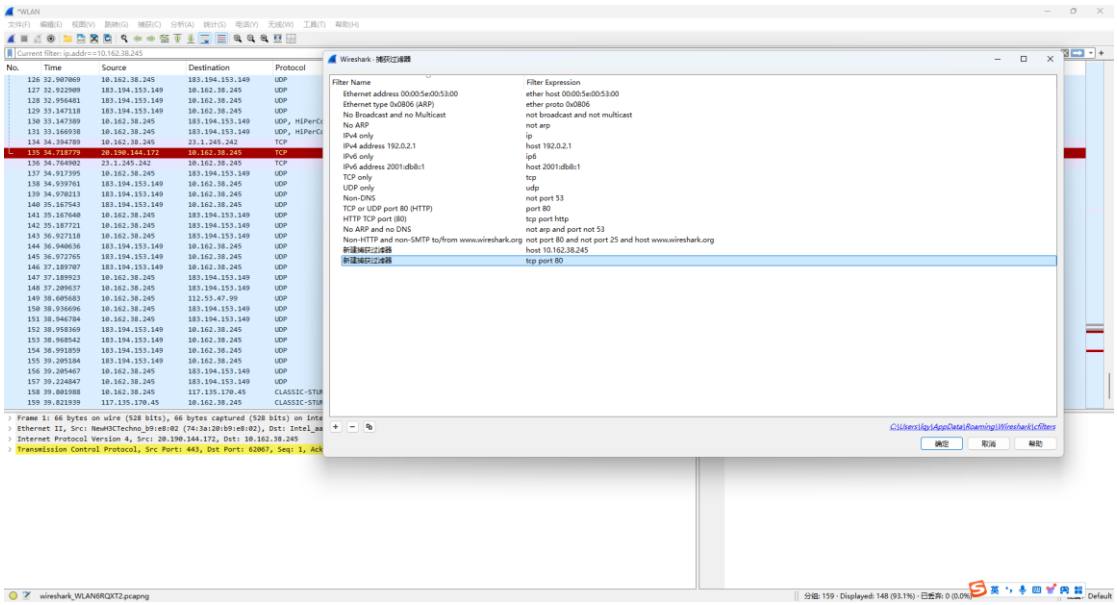
截图：



6. 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 port 80__ ，希望捕获的协议类型：__tcp__ 。

截图：



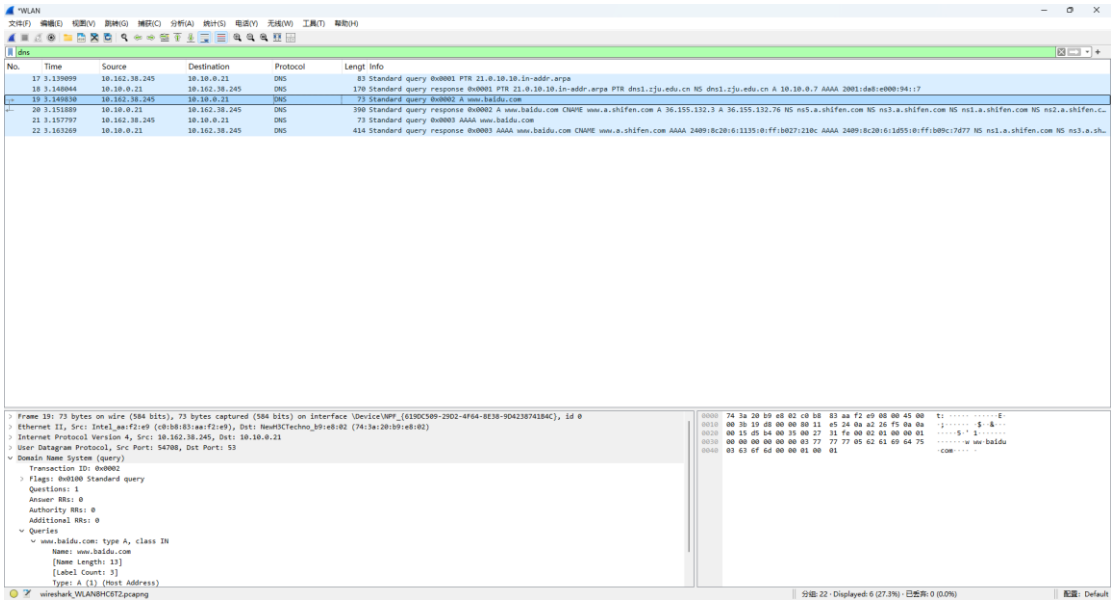
请在下面的每次捕获任务完成后，保存 Wireshark 抓包记录（.pcap 格式），随报告一起提交。每一个任务一个单独文件（如 dns.pcap、ping.pcap、tracert.pcap）。

✧ Part Two

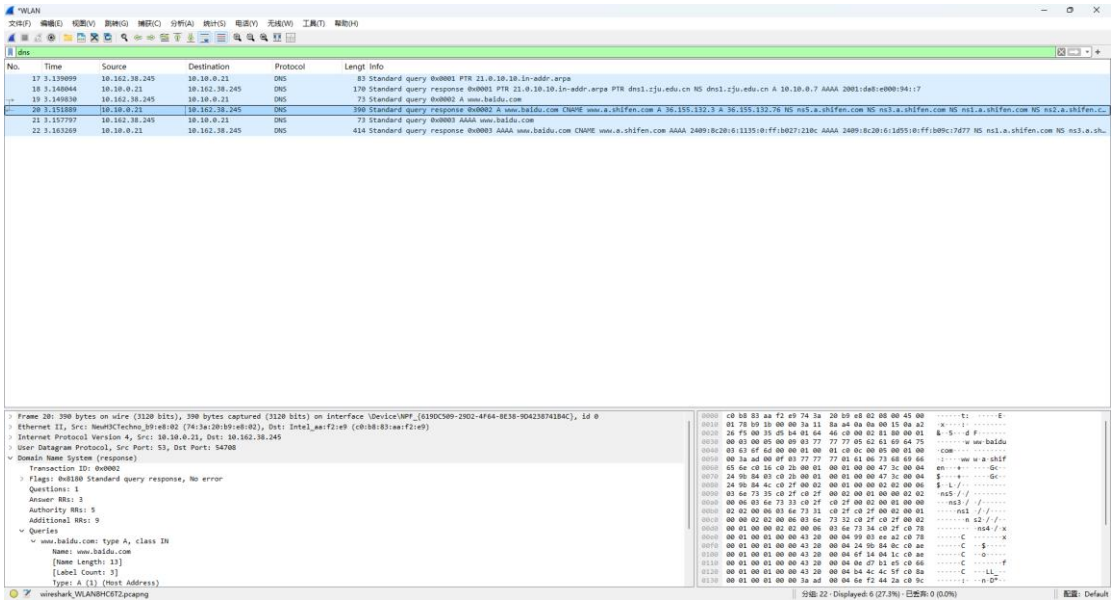
任务 1：使用 nslookup 命令，查询某个域名，并捕获这次的数据包。DNS 数据包由哪几层协议构成？ Ethernet II, Internet Protocol, User Datagram Protocol, Domain Name System 。 使用的服务方端口是： 53 。

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。

截图参考（此处应替换成实际截获的数据，请求和响应各一个）：



请求截图如上



响应截图如上

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：36.155.132.76

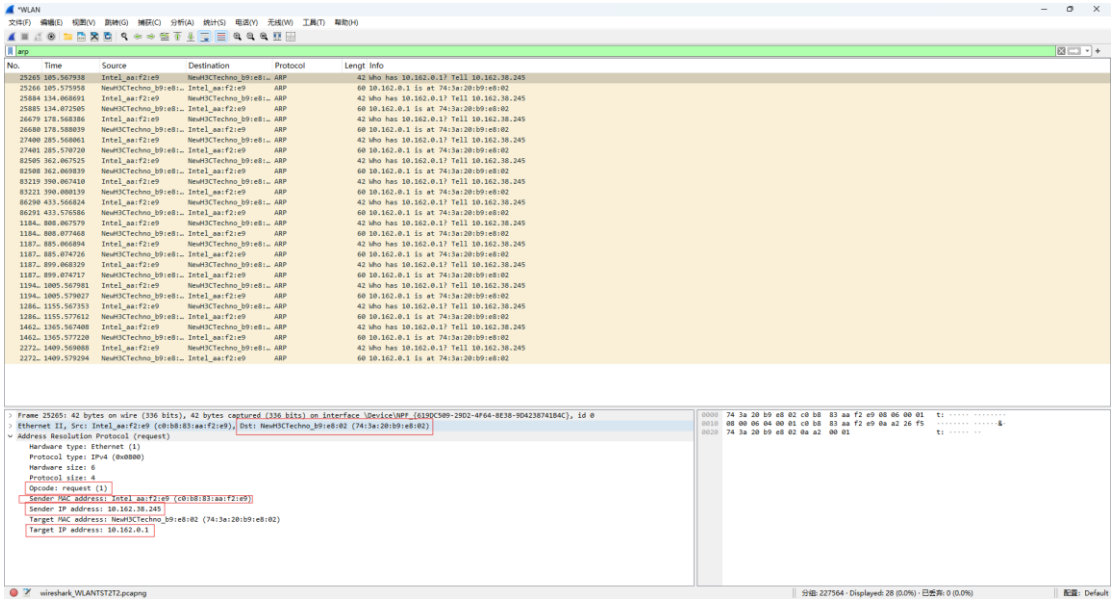
Ping 域名时：www.baidu.com

ICMP 数据包分别由哪几层协议构成？Ethernet II, Internet Protocol, Internet Control Message Protocol

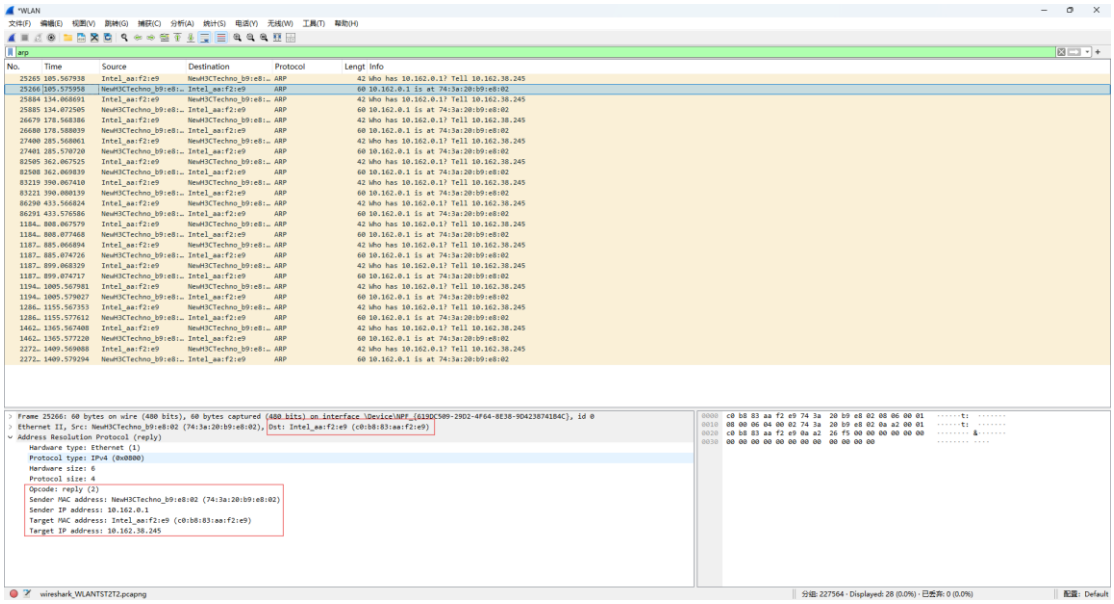
分别选择一个 ARP 请求和响应数据包，展开最高层协议的详细内容，标出操作码、发送者 IP 地址、发送者 MAC 地址、查询的目标 IP 地址、Ethernet 层的目标 MAC 地址以及查询结果。

截图参考（此处应替换成实际截获的数据，请求和响应各一）：

查询包：

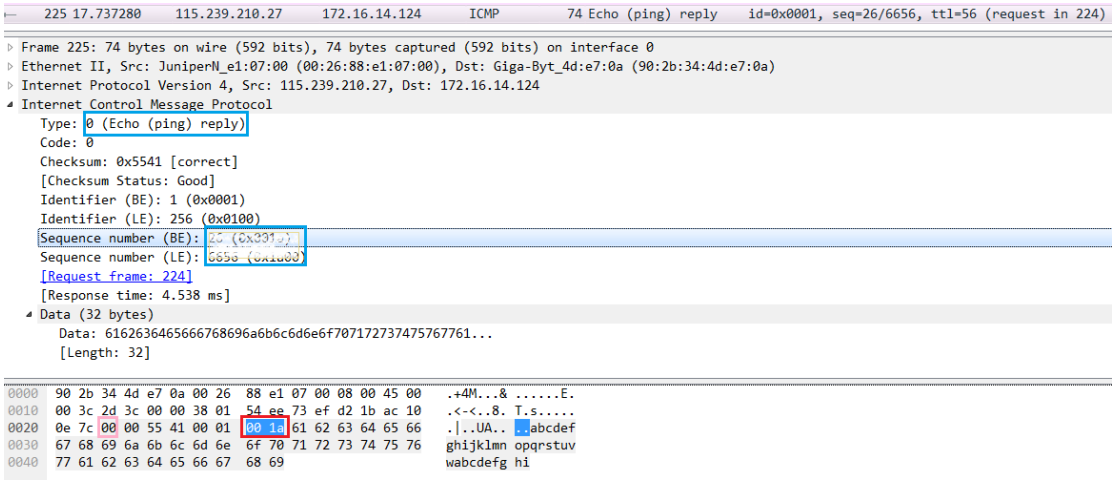


响应包：

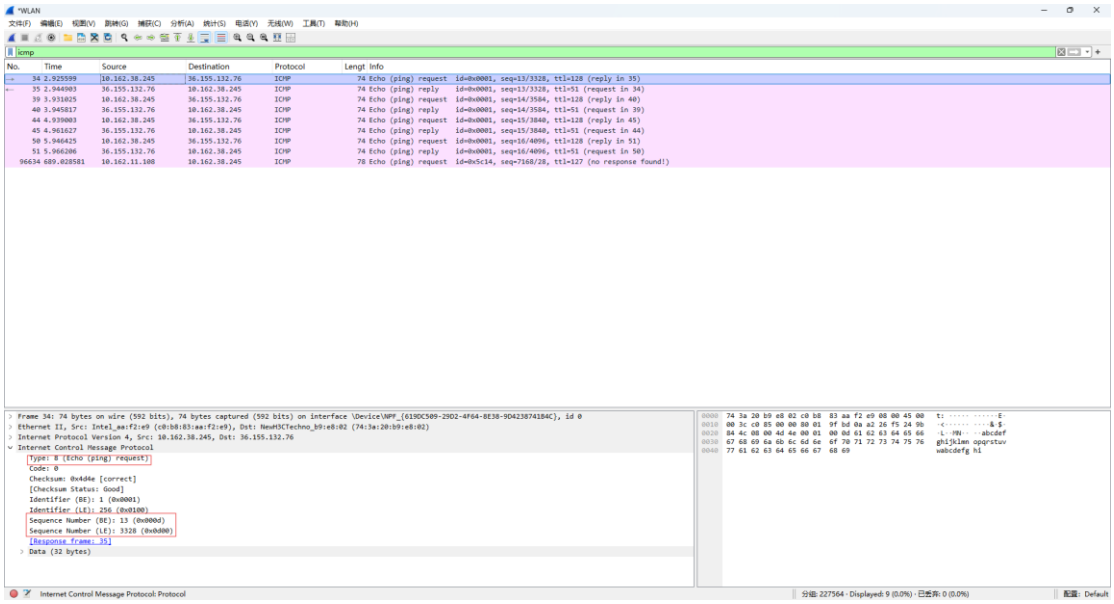


分别选择一个 ICMP 请求和响应数据包，展开最高层协议的详细内容，标出类型、序号。

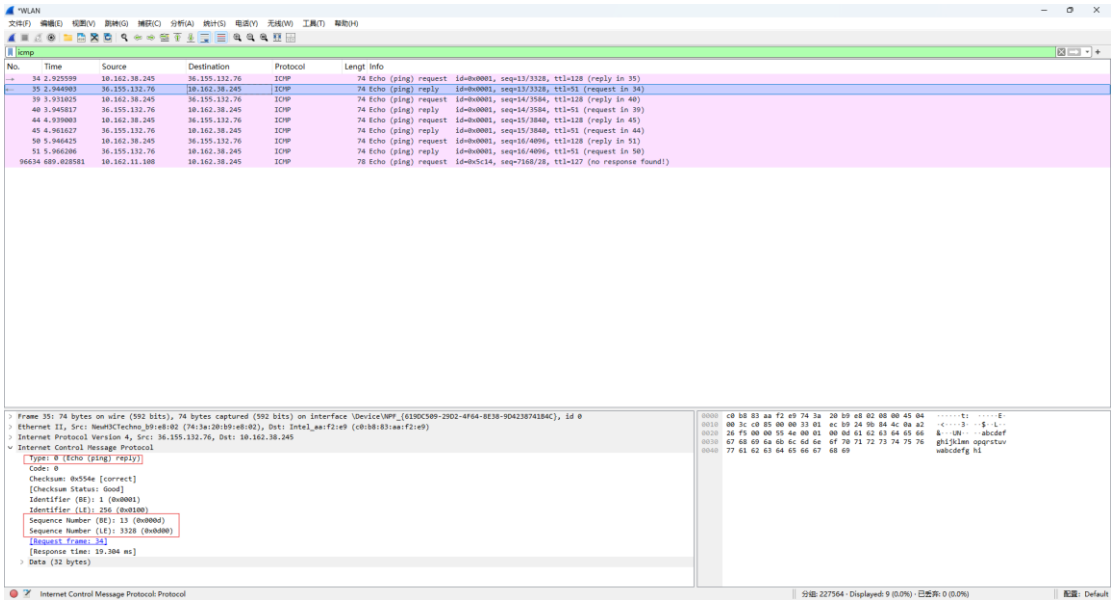
截图参考（此处应替换成实际截获的数据，请求和响应各一）：



请求：



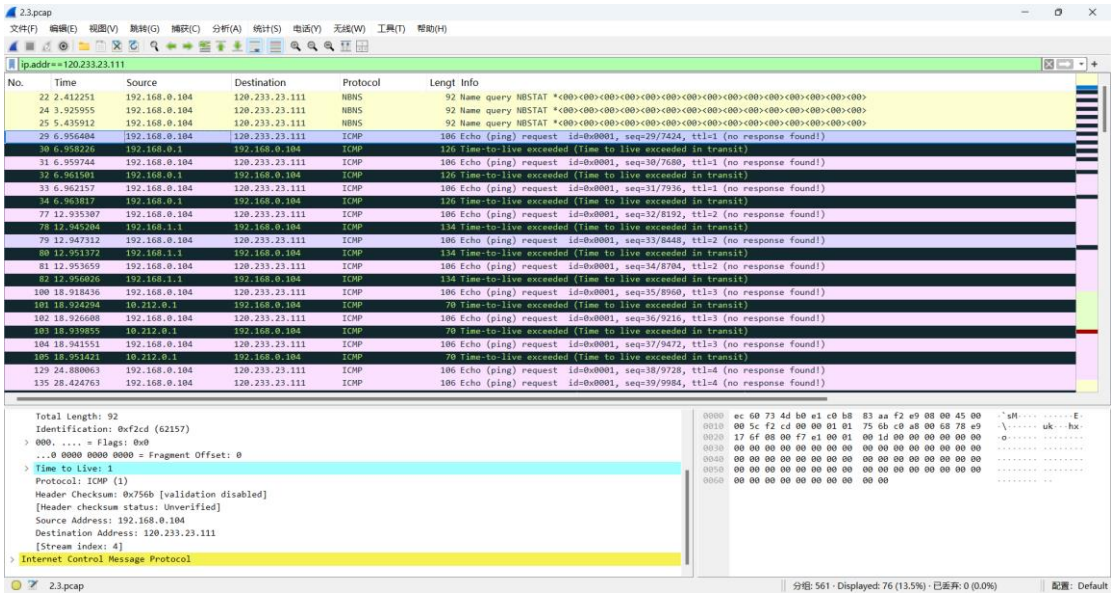
响应：



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？__4__。

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__13__。附上截图：

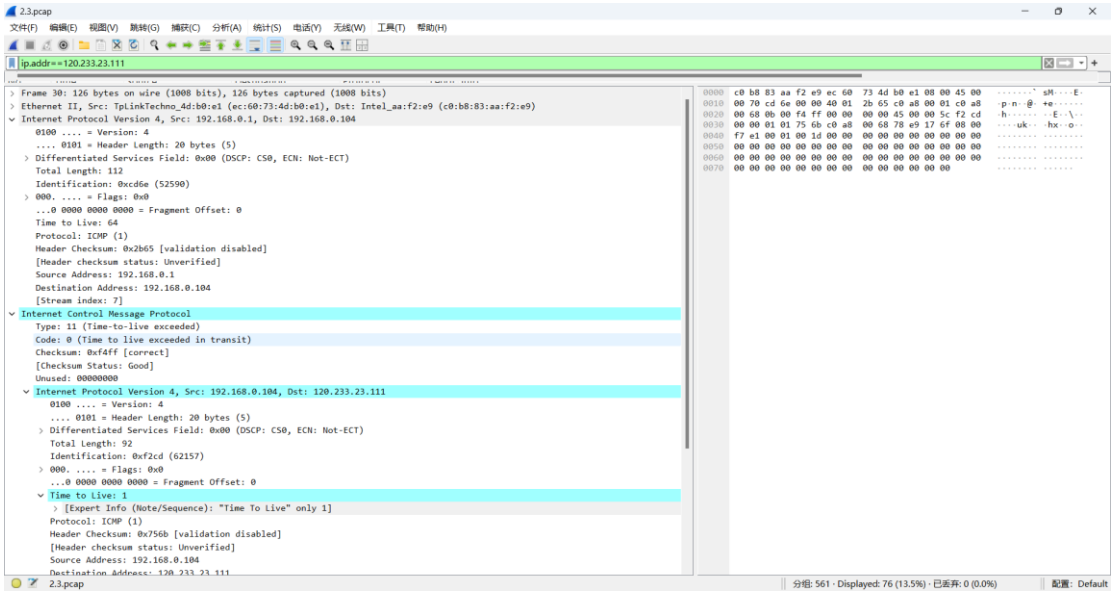
截图参考（此处应替换成实际截获的数据）：



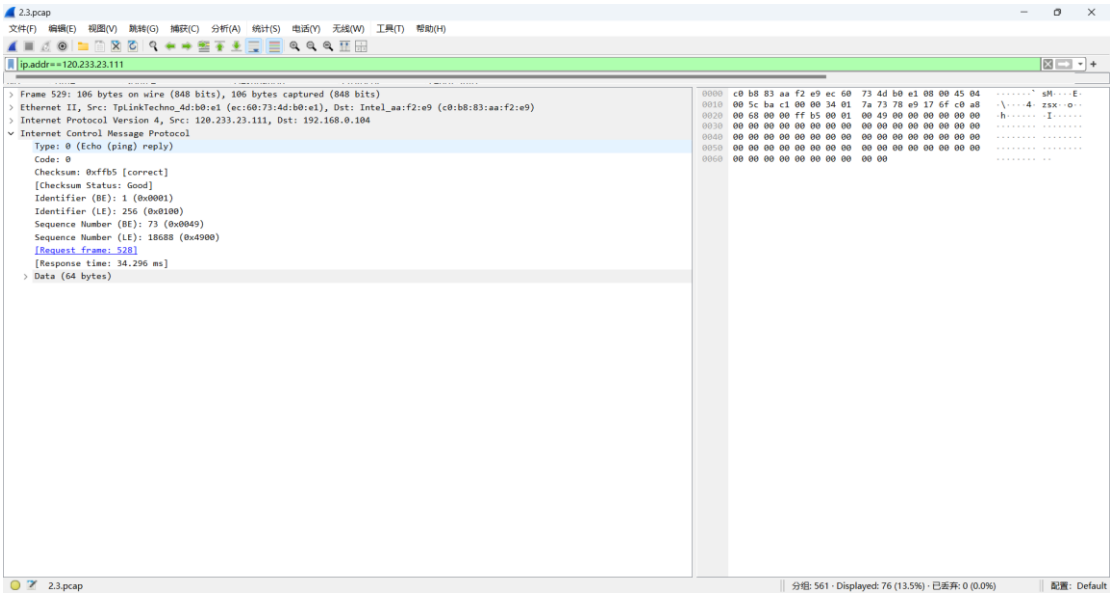
观察并记录响应包的信息，第一组响应包的发送者 IP 是：__192.168.0.1__，标记 ICMP 层的类型字段。最后一组响应包的发送者 IP 是：__120.233.23.111__，标记 ICMP 层的类型字段。附上截图：

截图参考（此处应替换成实际截获的数据）：

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。**

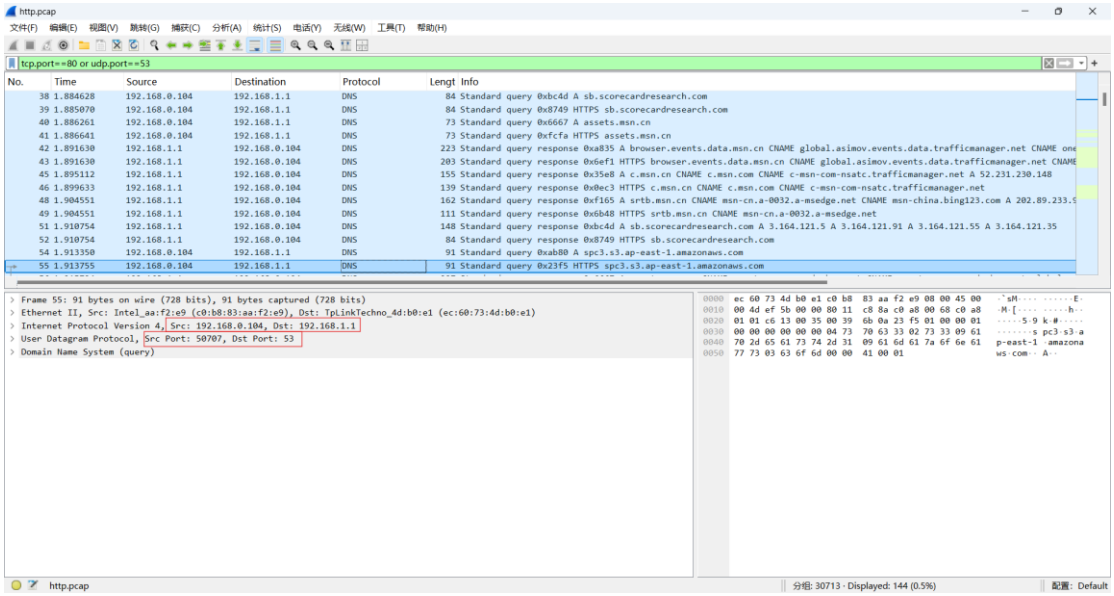
   捕获到的这些最高层的协议数据包分别由哪几层协议构成？

   DNS： Frame 32; Ethernet II; Internet Protocol; User Datagram Protocol; Domain Name System

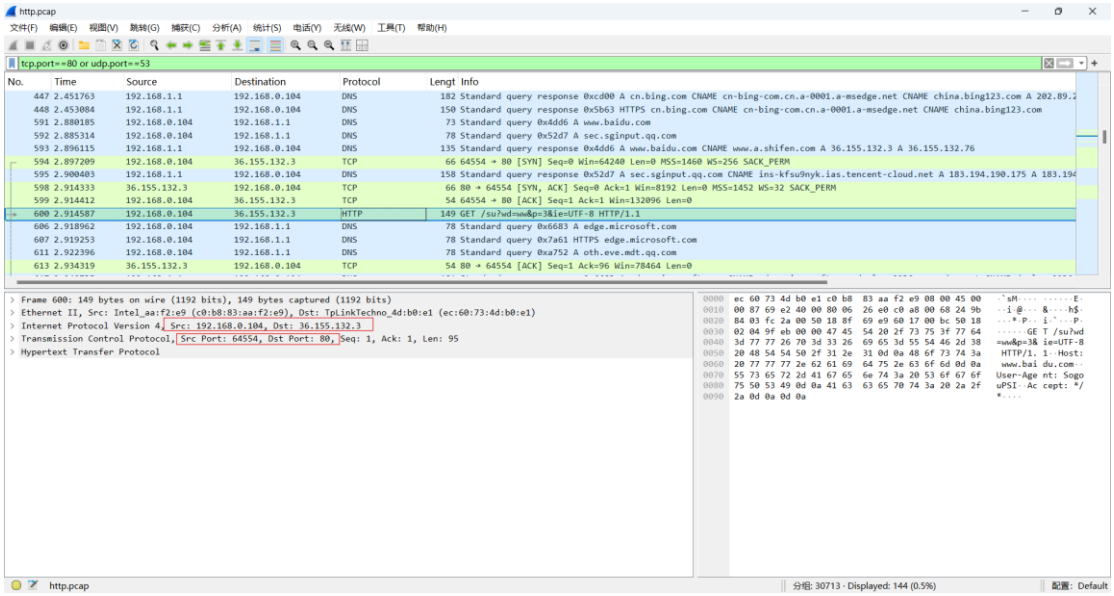
   HTTP: Frame 660; Ethernet II; Internet Protocol; Transmission Control Protocol; Hypertext Transfer Protocol

   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）

   DNS：



HTTP：



2. 为了打开网页，浏览器查询了哪些相关的域名？

域名列表：www.zju.edu.cn; www.zju.edu.cn.w.cdngslb.com

3. 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）

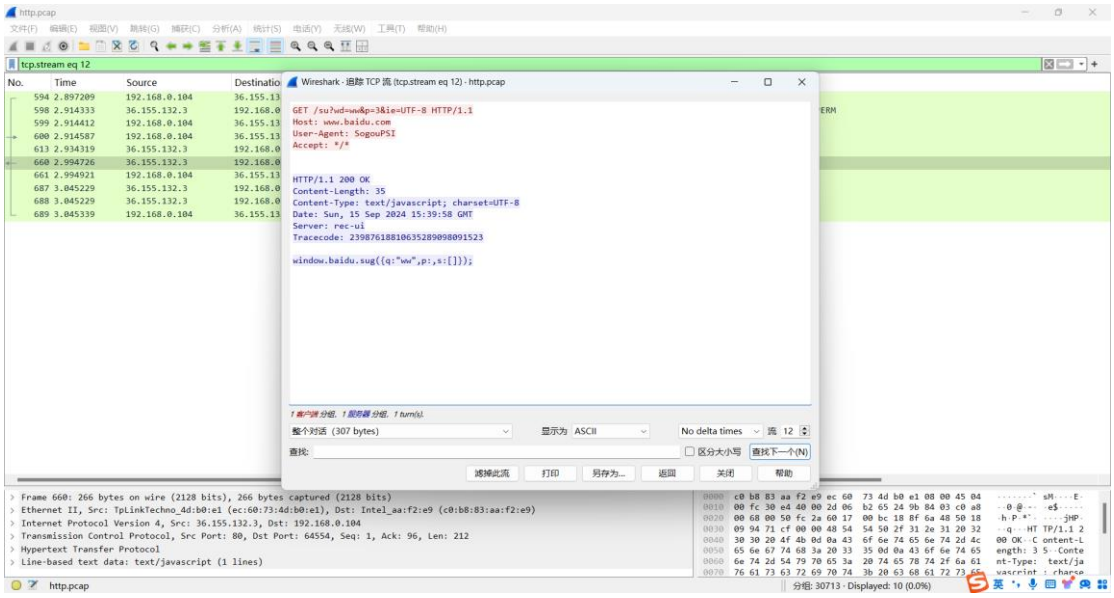
TCP 连接数： 37

4. **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__

5. **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）：**

截图示例（此处应替换成实际截获的数据）：



六、 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？**

http and ip.addr==xxxx

- **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？**

  1. Ping 发送的是 ICMP 数据包
  2. 同一子网内的主机通信时会出现 ARP 数据包
  3. Ping 一个域名是首先需要经过 DNS 查询域名对应的 ip 地址，然后才发送 ICMP 数据包，如果是直接 ping 一个 ip 地址则不需要 DNS 查询过程

- **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 发送的是一系列 ICMP 回显请求或 UDP 数据包到目标主机

1. 每个路由器节点在转发数据包之前，会记录下它的 IP 地址作为跃点
2. 当数据包到达目标主机时，目标主机会回复 ICMP 回显应答或 UDP 应答，这些应答会沿着相同的路径返回

- **如何理解 TCP 连接和 HTTP 会话？他们之间存在什么关系？**

  TCP 连接属于传输层的协议，而 http 属于应用层的协议，http 会话依赖于 TCP 连接的形成

  TCP 提供了一个可靠的传输层连接，而 HTTP 定义了如何在这些连接上进行数据交换和通信

- **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 使用 UDP 传输主要是其传输速度快消耗资源少，无需建立连接，且域名查询的数据量小，符合 UDP 的工作方式

  而 http 使用 tcp 是因为其可靠性、准确性、数据完整性等保障

七、 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：

Wireshark 的更多完整使用方法还有什么？

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：

课程就是计算机网络，虽然只是一个入门的 lab，有很多内容和知识还没有学习到，但是我们可以调用自身的方法，进行网上搜索相关内容，完成解惑

你对本实验安排有哪些更好的建议呢？欢迎献计献策：

暂无