



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: 陈希典

学 院: 计算机学院

系:

专 业: 计算机科学与技术

学 号: 3210102362

指导教师: 郑扣根

2023 年 9 月 18 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。

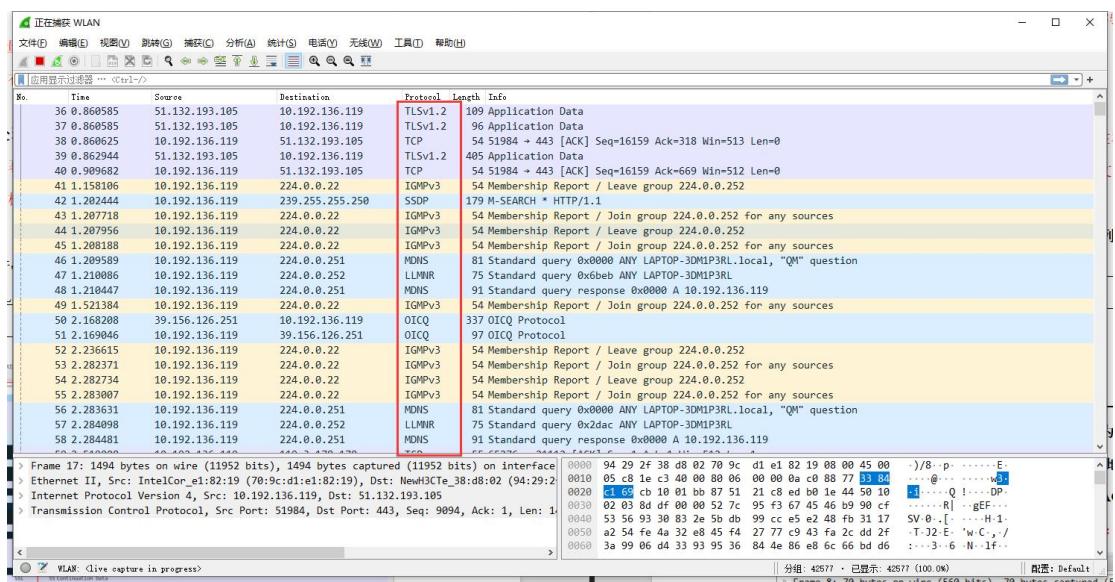
五、实验数据记录和处理

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： TLSv1.2 TCP IGMPv3 SSDP MDNS LLMNR

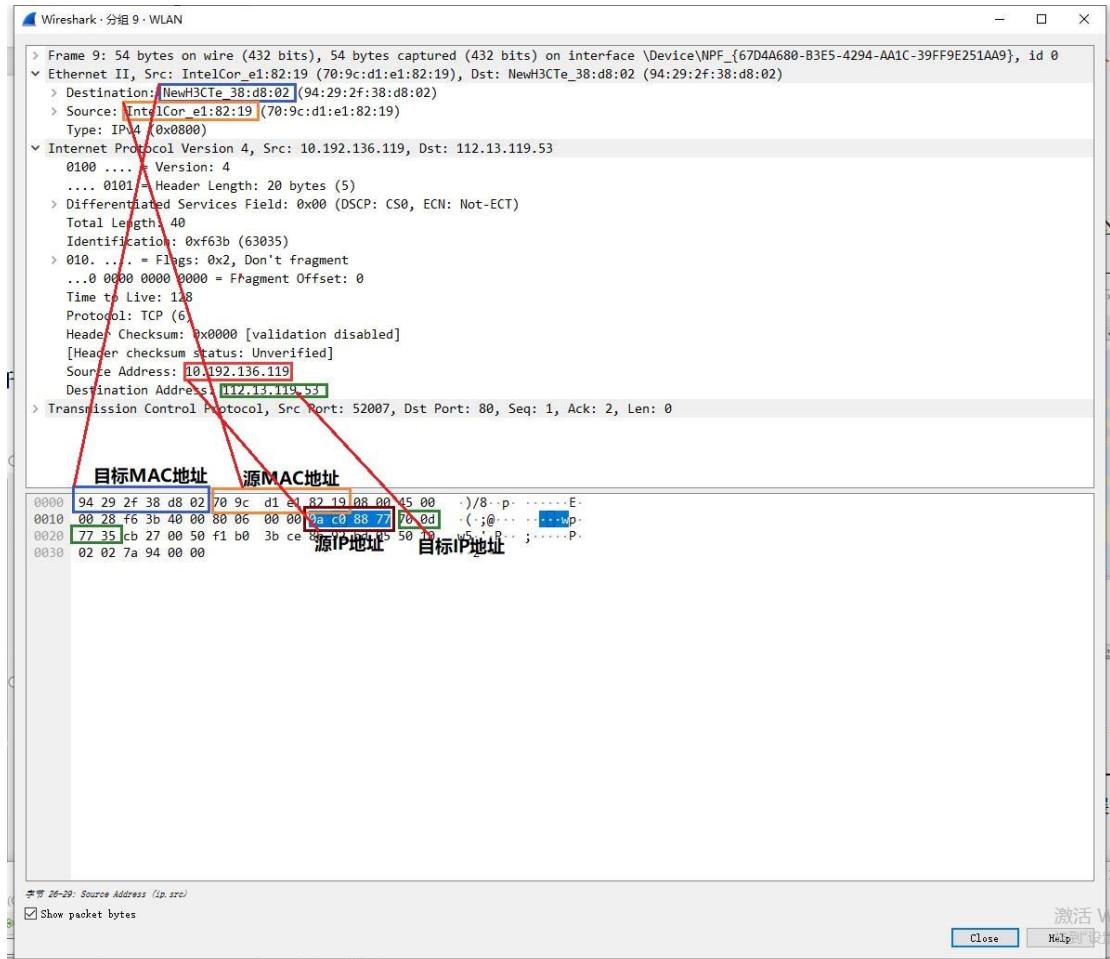


2. 找一个包含 IP 的数据包，这个数据包有 5 层？最高层协议是 HTTP，从 Ethernet 开始往上，各层协议的名字分别为：Internet Protocol Version 4，Transmission Control Protocol，Hypertextfer Protocol。

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）：

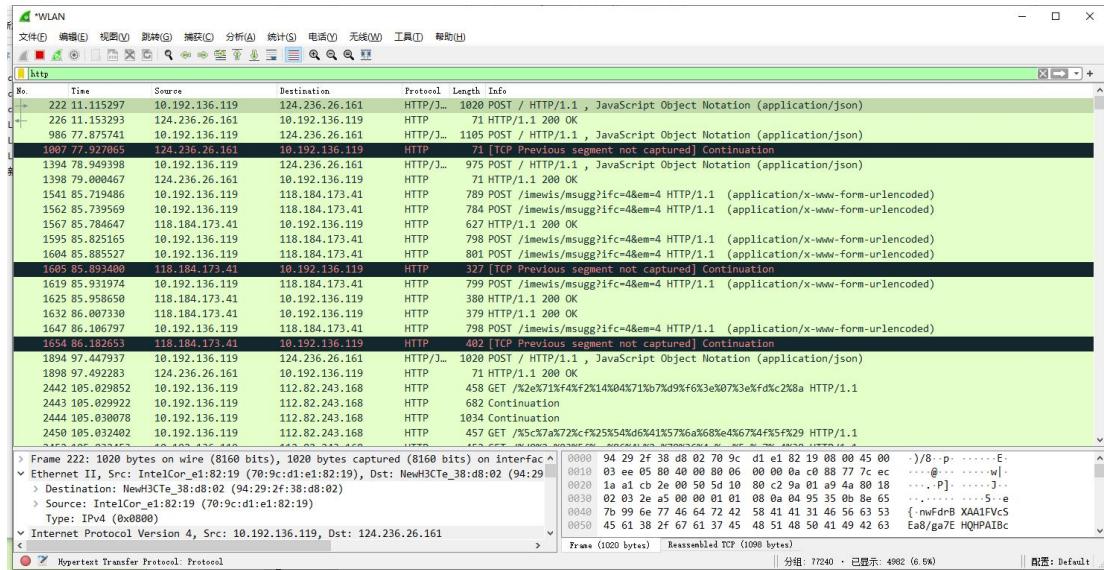


3. 配置应用显示过滤器，让界面只显示某一协议类型的数据包（输入协议名称）。

使用的过滤器：http，希望显示的协议类型：

HTTP。

截图：

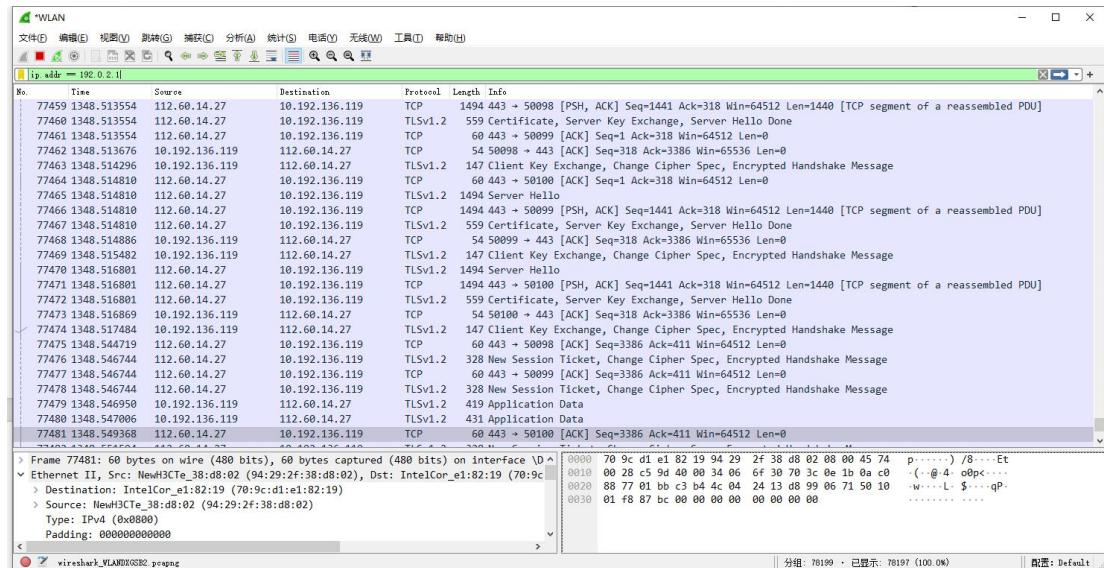


4. 配置应用显示过滤器，让界面只显示某个 IP 地址的数据包 (ip.addr==x.x.x.x)。

使用的过滤器: ip.addr == 192.0.2.1 , 希望显示的 IP 地址:

192.0.2.1。

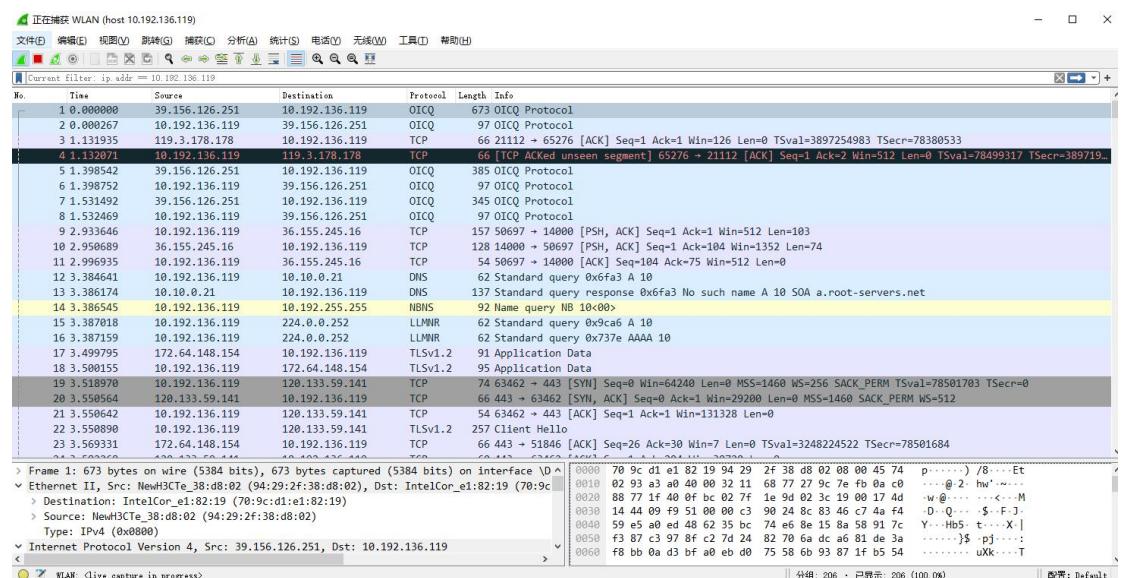
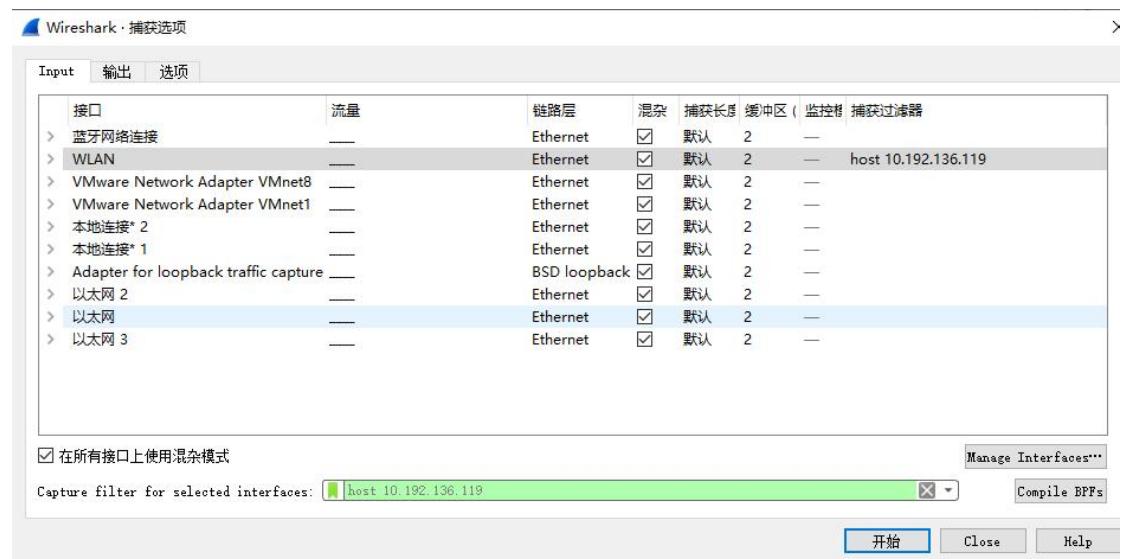
截图:



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 10.192.136.119 , 希望捕获的 IP 地址:
10.192.136.119。

截图:

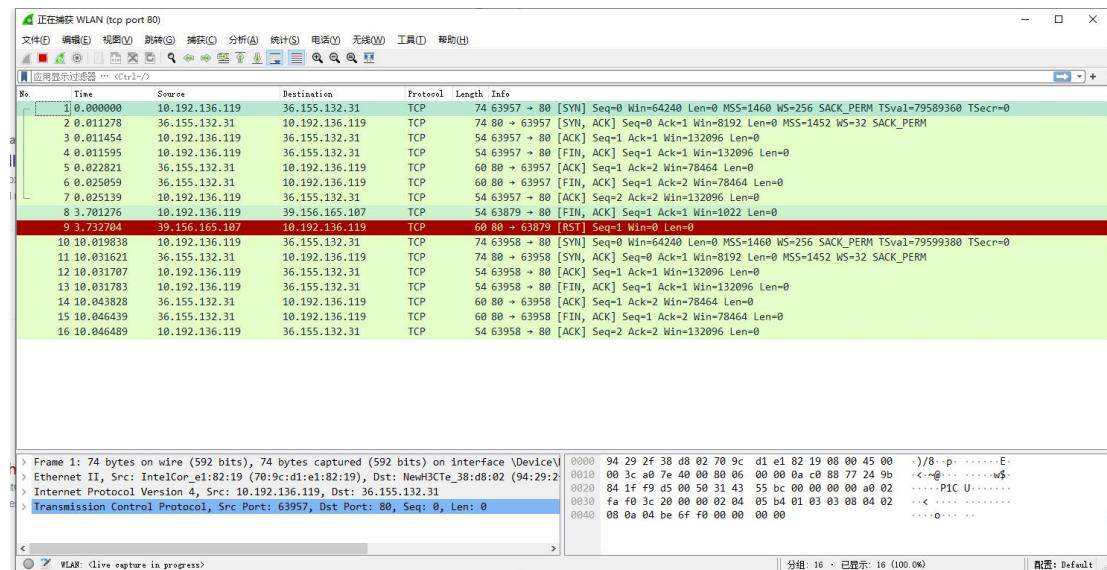
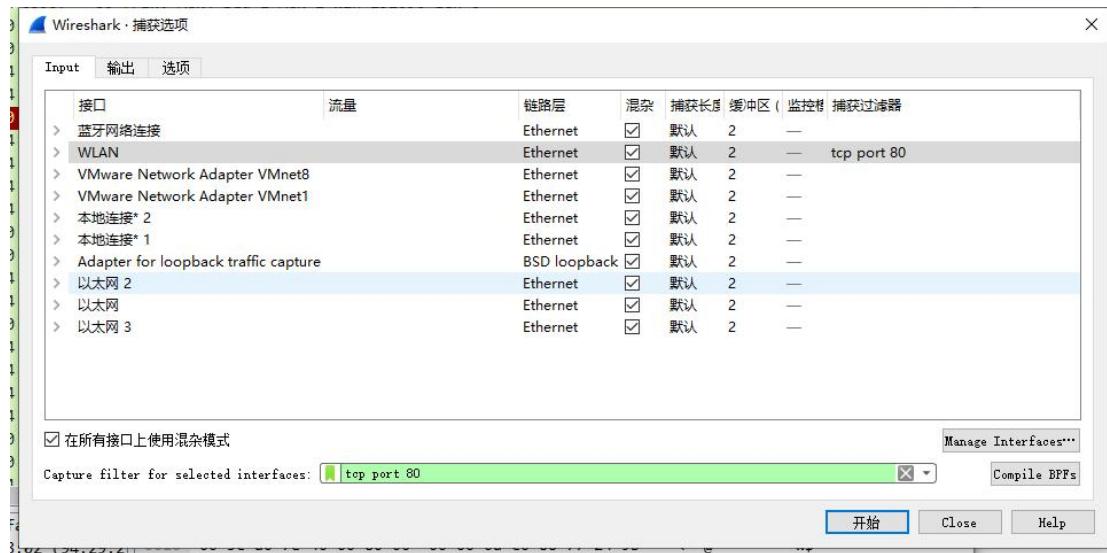


6. 配置捕获过滤器，只捕获某类协议的数据包（tcp port xx 或者 udp port xx）。

使用的过滤器：tcp port 80，希望捕获的协议类型：

TCP。

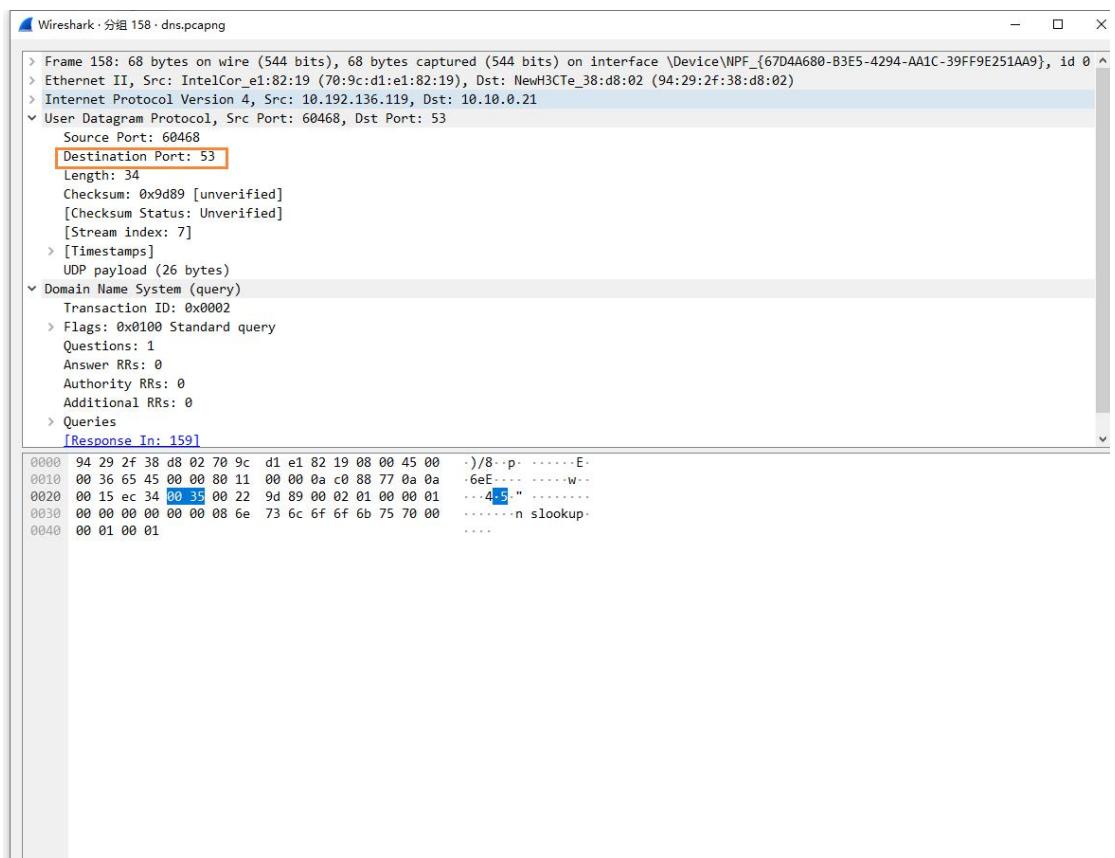
截图：



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）。

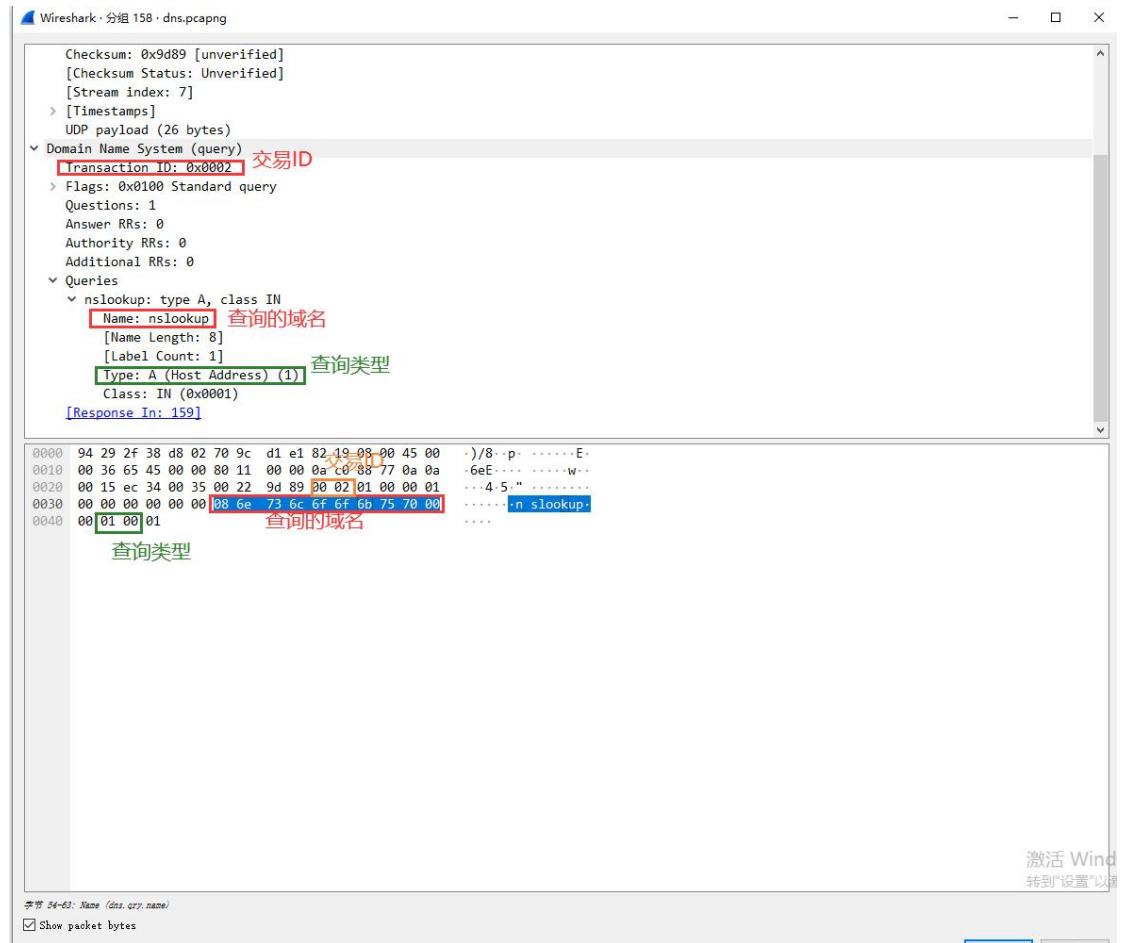
✧ Part Two

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？4 层：Frame, Ethernet II, Internet Protocol Version 4, User Datagram Protocol, Domain Name System。使用的服务方端口是：53。

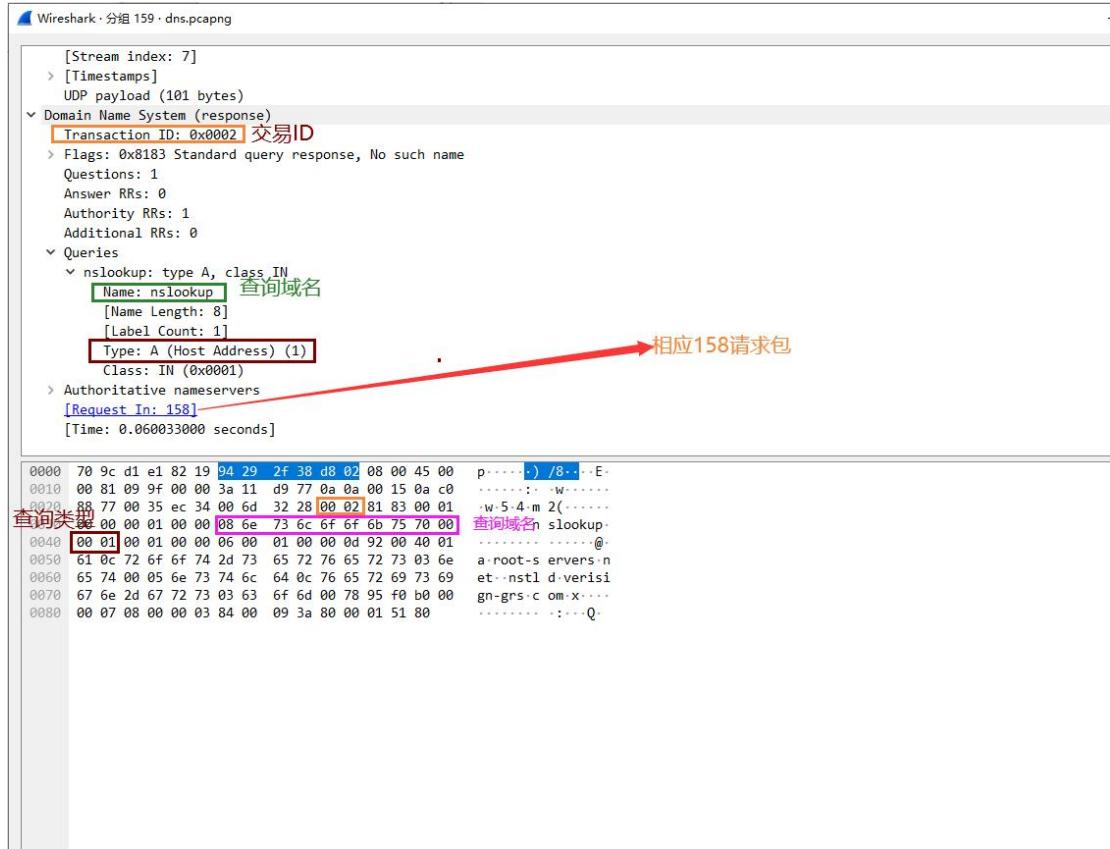


分别选择一个请求包和一个响应包，展开最高层协议的详细内容，标出交易 ID、查询类型、查询的域名内容以及查询结果。

请求包：



响应包:



响应信息

```
Data length: 64
Primary name server: a.root-servers.net
Responsible authority's mailbox: nstld.verisign-grs.com
Serial Number: 2023092400
0000 70 9c d1 e1 82 19 94 29 2f 38 d8 02 08 00 45 00 p..... ) /8...E.
0010 00 81 09 9f 00 00 3a 11 d9 77 0a 0a 00 15 0a c0 .....:..w.....  

0020 88 77 00 35 ec 34 00 6d 32 28 00 02 81 83 00 01 .w.5.4.m 2(.....  

0030 00 00 00 01 00 00 08 6e 73 6c 6f 6f 6b 75 70 00 .....n slookup.  

0040 00 01 00 01 00 00 06 00 01 00 00 0d 92 00 40 01 .....@.a.root-servers.n  

0050 61 0c 72 6f 74 2d 73 65 72 76 65 72 73 03 6e et..nstld.veris...  

0060 65 74 00 05 6e 73 74 6c 64 0c 76 65 72 69 73 69 gn-grs.c om.x...  

0070 67 6e 2d 67 72 73 03 63 6f 6d 00 78 95 f0 b0 00 .....Q.  

0080 00 07 08 00 00 03 84 00 09 3a 80 00 01 51 80 .....
```

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？

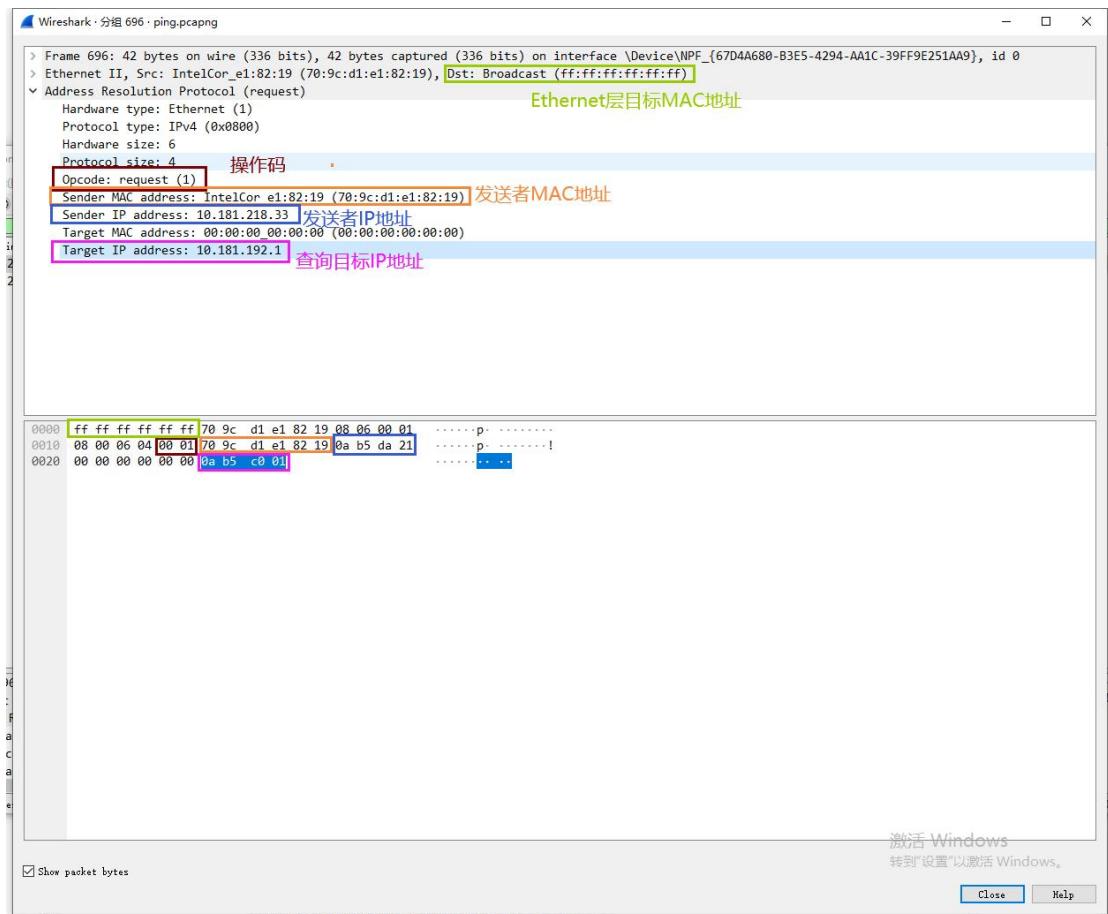
Ping IP 地址时： ICMP

Ping 域名时： ICMP DNS

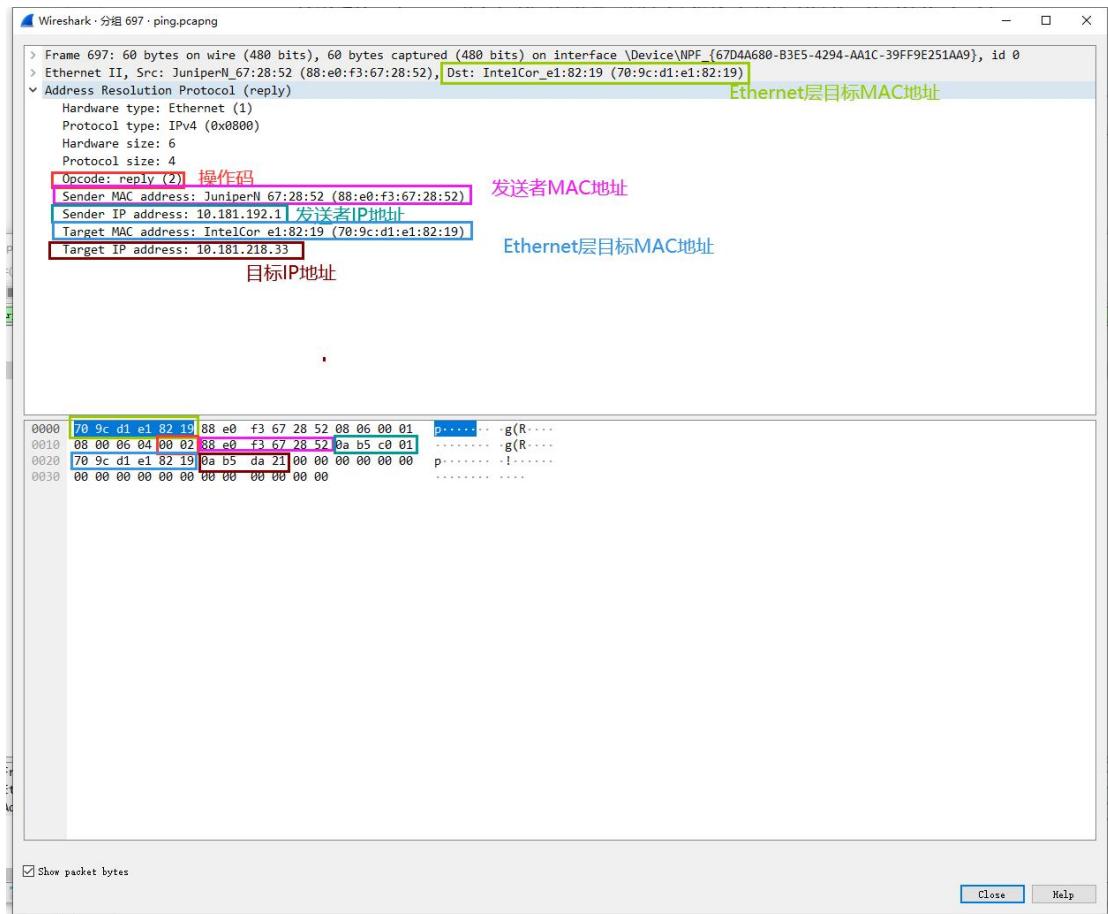
ICMP 数据包分别由哪几层协议构成？

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(使用 arp -d 捕获的)

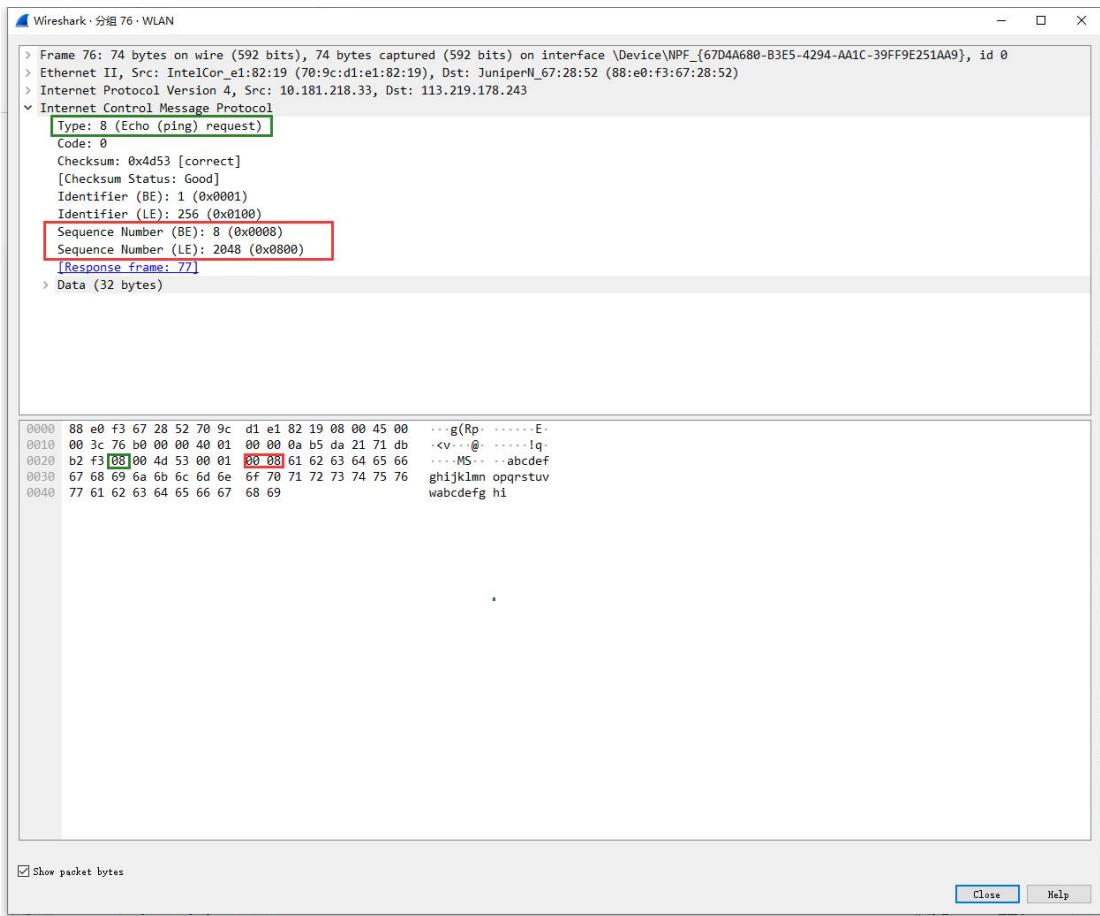


ARP 响应数据包

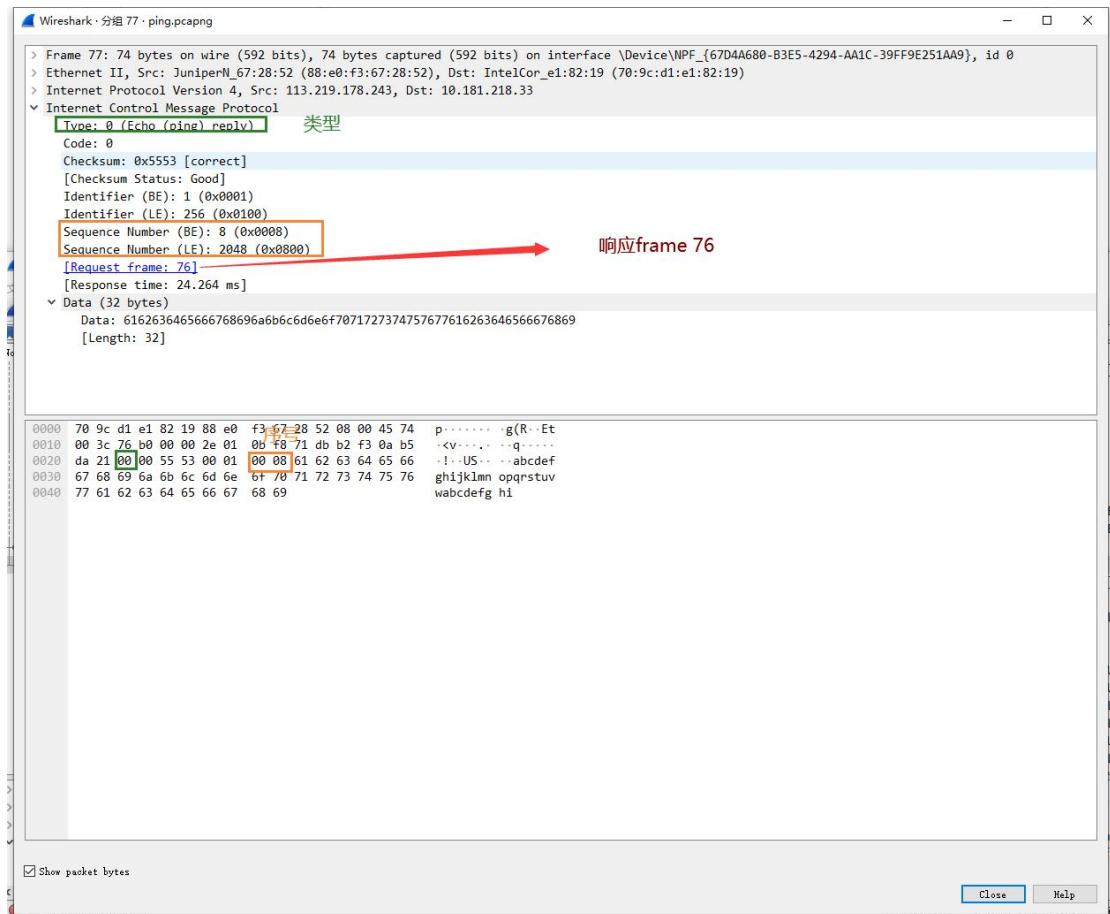


分别选择一个 ICMP 请求和响应数据包，展开最高层协议的详细内容，标出类型、序号。

请求包 frame 76,绿色为 Type 类型,红色表示序号,其中 BE 和 LE 是大端和小端的意思,表示的都是 00 08 红色标红的部分.

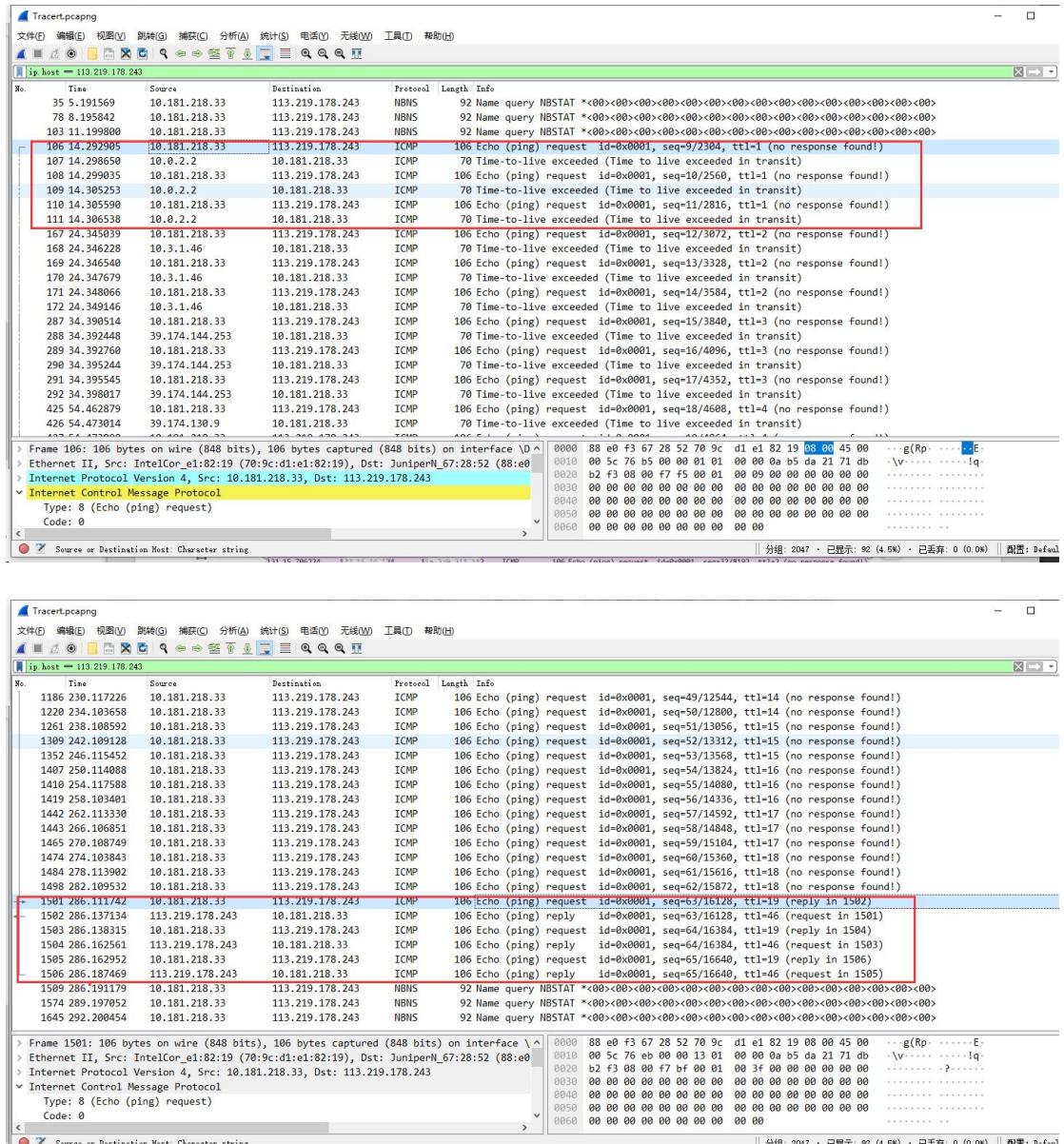


响应包 frame 77



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 层 :Ethernet II 协议 IPV4 协议 ICMP 协议。

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19。附上截图：

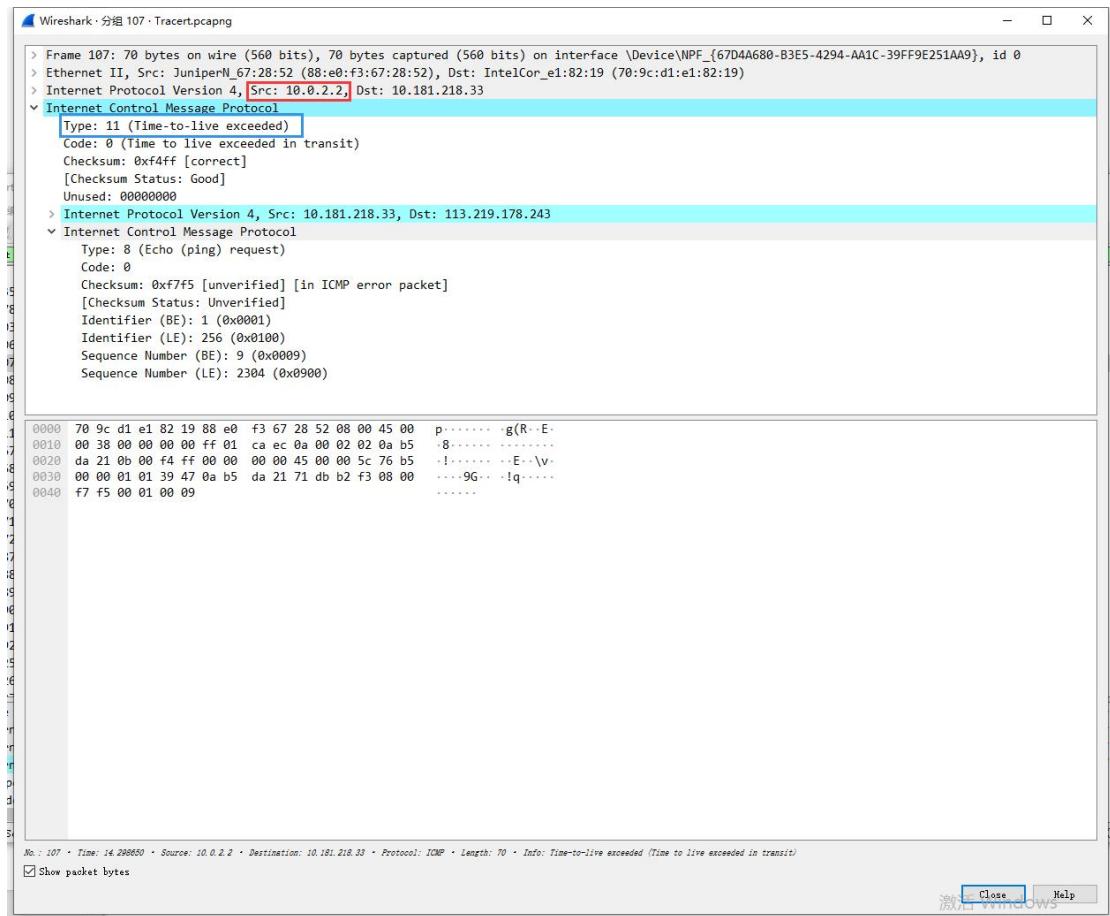


观察并记录响应包的信息，第一组响应包的发送者 IP 是： 10.0.2.2，

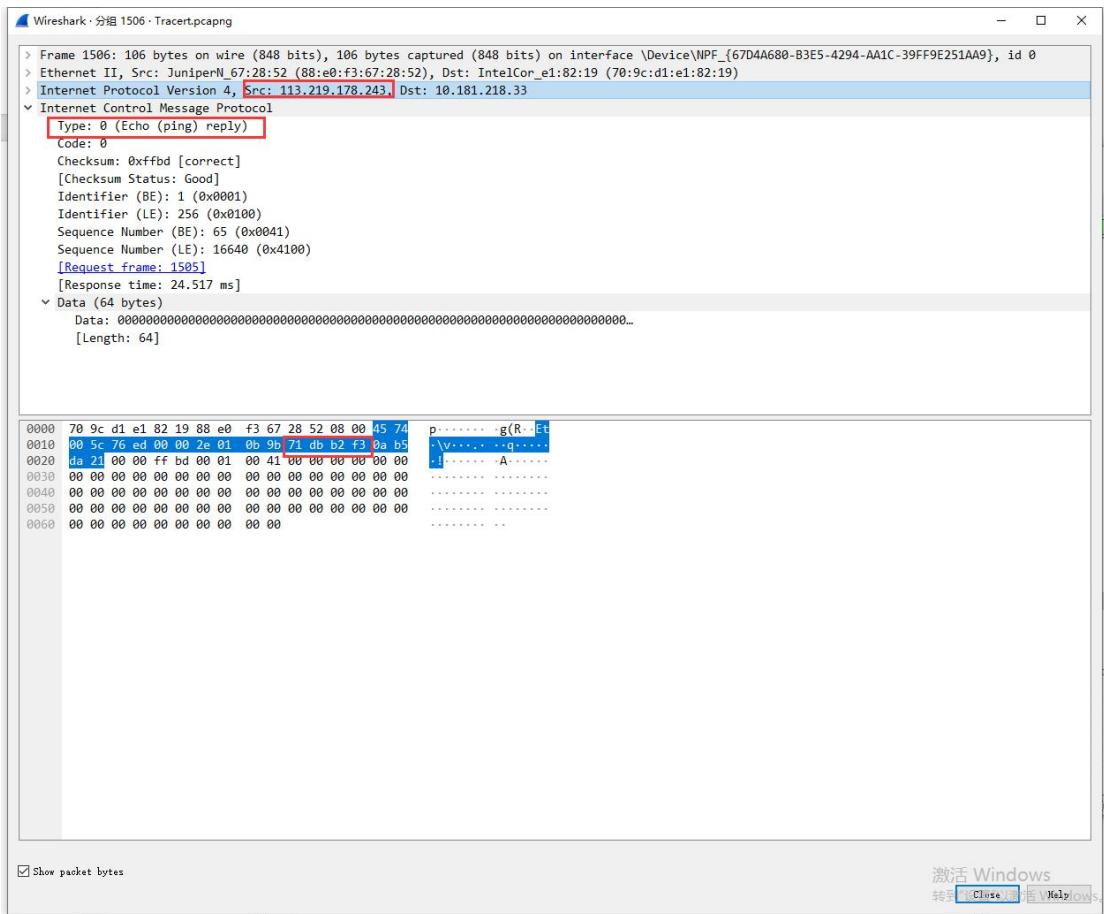
标记 ICMP 层的类型字段。最后一组响应包的发送者 IP 是：

113.219.178.243，标记 ICMP 层的类型字段。附上截图：

第一组响应包



最后一组相应包



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

- 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。

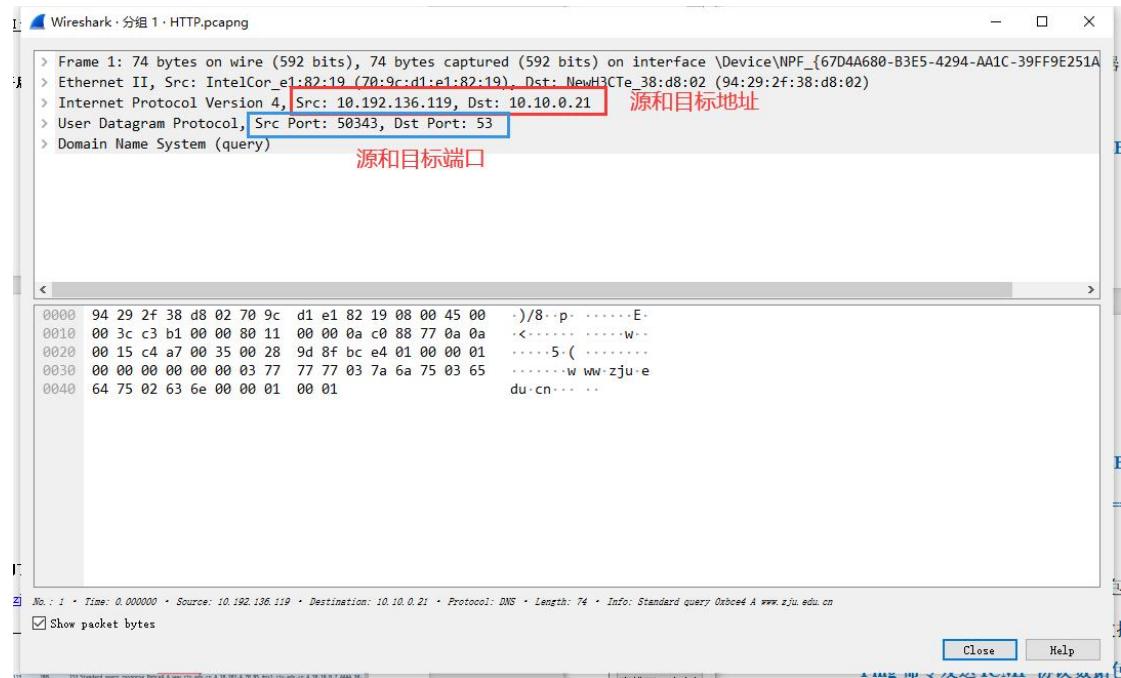
捕获到的这些最高层的协议数据包分别由哪几层协议构成？

DNS: Ethernet II 协议、IPV4 协议、UDP 协议、DNS 协议

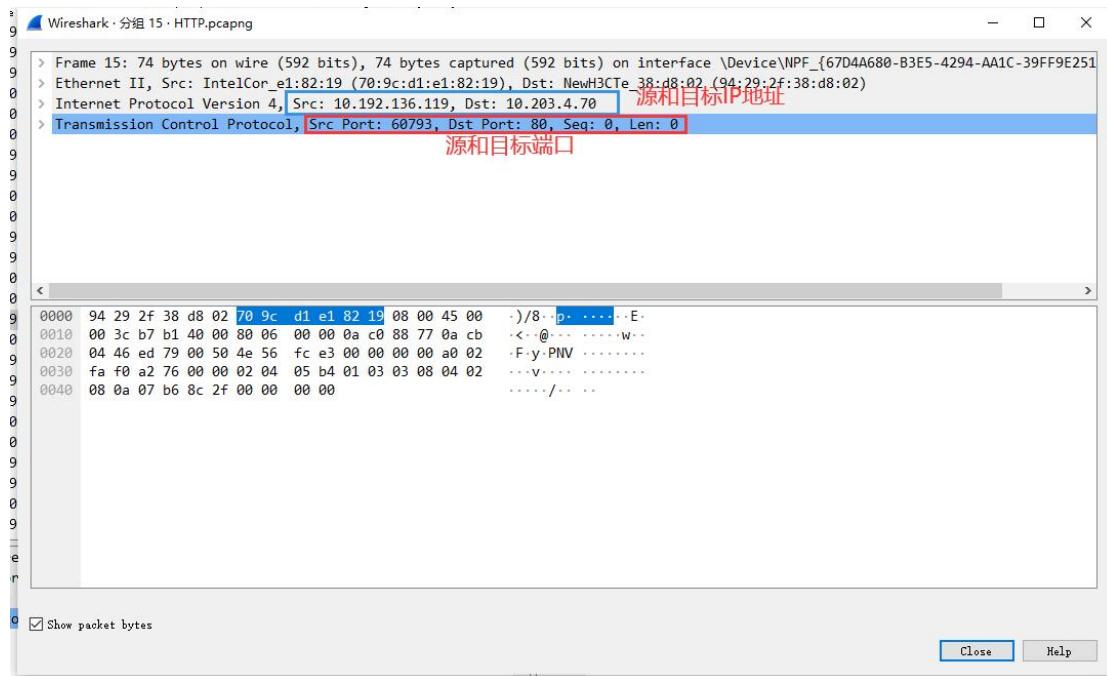
HTTP: Ethernet II 协议、IPV4 协议、TCP 协议、DNS 协议

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）

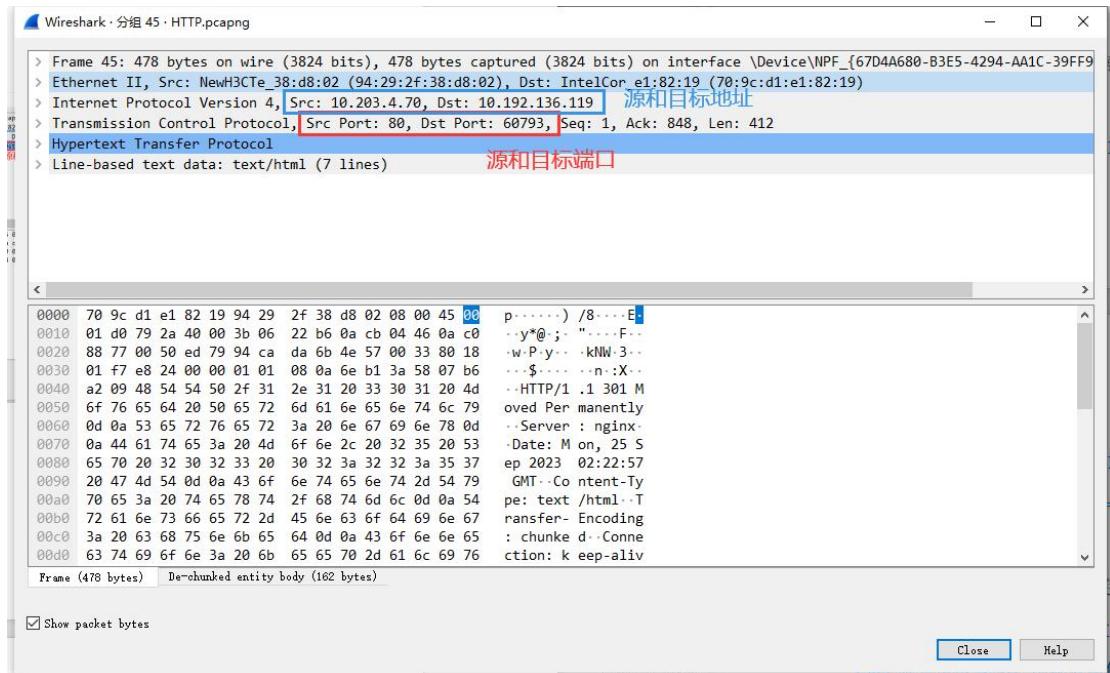
DNS 数据包



TCP 数据包



HTTP 数据包



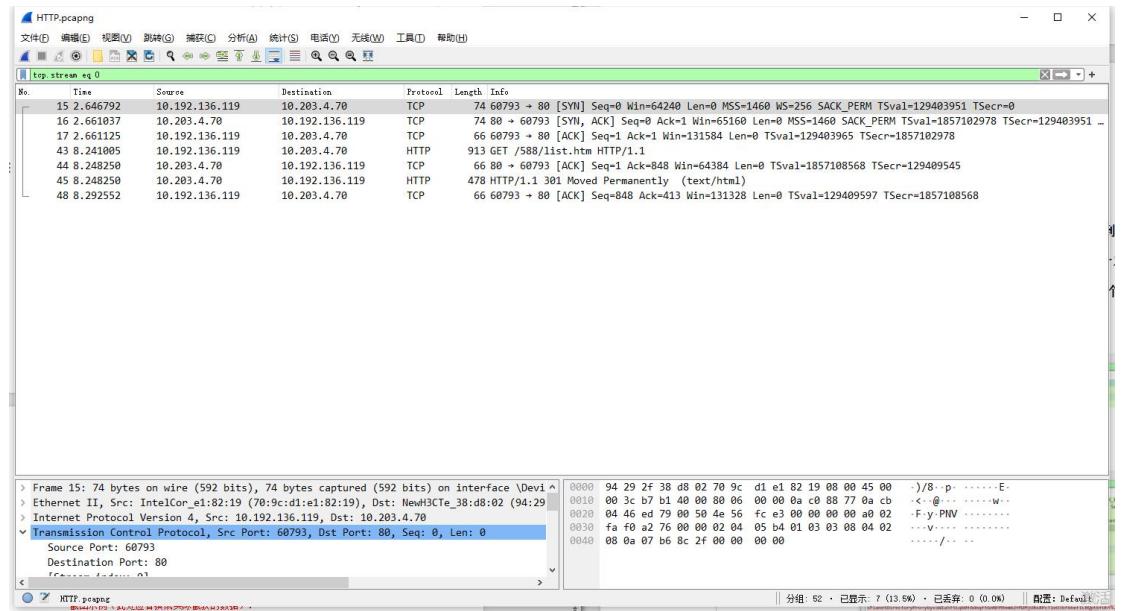
2. 为了打开网页，浏览器查询了哪些相关的域名？

域名列表： www.zju.edu.cn tel.zju.edu.cn

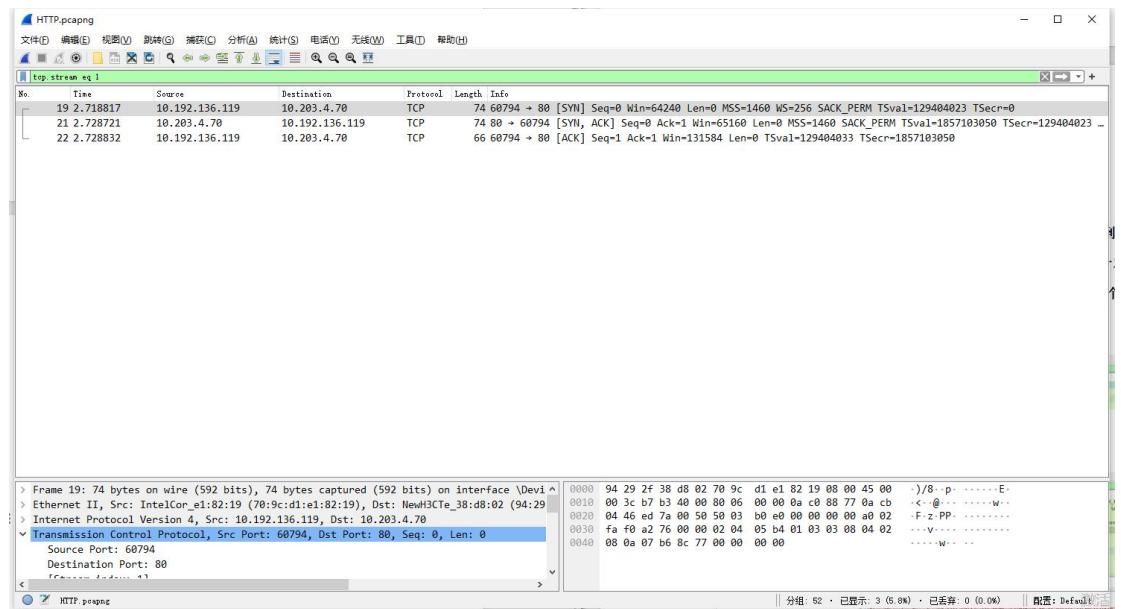
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.192.136.119	10.10.0.21	DNS	74	Standard query 0xbce4 A www.zju.edu.cn
2	0.005768	10.192.136.119	10.10.0.21	DNS	74	Standard query 0x36ca A www.zju.edu.cn
3	0.010679	10.192.136.119	10.10.0.21	DNS	74	Standard query 0x7af0 HTTPS www.zju.edu.cn
4	0.010802	10.10.0.21	10.192.136.119	DNS	153	Standard query response 0xbc4 A www.zju.edu.cn A 10.203.4.70 NS dns1.zju.edu.cn A 10.10.0.7 AAAA 20..
5	0.010802	10.10.0.21	10.192.136.119	DNS	153	Standard query response 0x36ca A www.zju.edu.cn A 10.203.4.70 NS dns1.zju.edu.cn A 10.10.0.7 AAAA 20..
6	0.010802	10.10.0.21	10.192.136.119	DNS	120	Standard query response 0x7af0 HTTPS www.zju.edu.cn SOA dns1.zju.edu.cn
7	0.232348	10.192.136.119	10.10.0.21	DNS	74	Standard query response 0x6383 A tel.zju.edu.cn
8	0.232596	10.192.136.119	10.10.0.21	DNS	74	Standard query 0x7e97 HTTPS tel.zju.edu.cn
9	0.240838	10.10.0.21	10.192.136.119	DNS	125	Standard query response 0x6383 A tel.zju.edu.cn A 10.203.9.35 NS dns1.zju.edu.cn A 10.10.0.8
10	0.240838	10.10.0.21	10.192.136.119	DNS	120	Standard query response 0x7e97 HTTPS tel.zju.edu.cn SOA dns1.zju.edu.cn
11	2.634331	10.192.136.119	10.10.0.21	DNS	74	Standard query 0x5837 A www.zju.edu.cn
12	2.634695	10.192.136.119	10.10.0.21	DNS	74	Standard query 0x4a5e HTTPS www.zju.edu.cn
13	2.646257	10.10.0.21	10.192.136.119	DNS	153	Standard query response 0x5837 A www.zju.edu.cn A 10.203.4.70 NS dns1.zju.edu.cn A 10.10.0.7 AAAA 20..
14	2.646257	10.10.0.21	10.192.136.119	DNS	120	Standard query response 0x4a5e HTTPS www.zju.edu.cn SOA dns1.zju.edu.cn
15	2.646792	10.192.136.119	10.203.4.70	TCP	74	60793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM Tsv1=129403951 TSecr=0
16	2.661037	10.203.4.70	10.192.136.119	TCP	74	60793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM Tsv1=129403951 TSecr=0
17	2.661125	10.192.136.119	10.203.4.70	TCP	66	60793 → 80 [ACK] Seq=1 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsv1=129403956 TSecr=1857102978
18	2.714938	10.192.136.119	10.10.0.21	DNS	74	Standard query 0x1cef A www.zju.edu.cn
19	2.718817	10.192.136.119	10.203.4.70	TCP	74	60794 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM Tsv1=129404023 TSecr=0
20	2.720843	10.10.0.21	10.192.136.119	DNS	125	Standard query response 0x1cef A www.zju.edu.cn A 10.203.4.70 NS dns1.zju.edu.cn A 10.10.0.9
21	2.728721	10.203.4.70	10.192.136.119	TCP	74	80 → 60794 [SYN, ACK] Seq=1 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsv1=1857103050 TSecr=12940402..
22	2.728832	10.192.136.119	10.203.4.70	TCP	66	60794 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 Tsv1=129404033 TSecr=1857103050
23	2.736669	10.192.136.119	10.10.0.21	DNS	74	Standard query 0xd040 A www.zju.edu.cn
24	2.741100	10.10.0.21	10.192.136.119	DNS	153	Standard query response 0xd040 A www.zju.edu.cn A 10.203.4.70 NS dns1.zju.edu.cn A 10.10.0.7 AAAA 20..
25	5.025555	10.192.136.119	10.10.0.21	DNS	74	Standard query 0xfc4 A www.zju.edu.cn

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： 2



tcp.stream eq 0

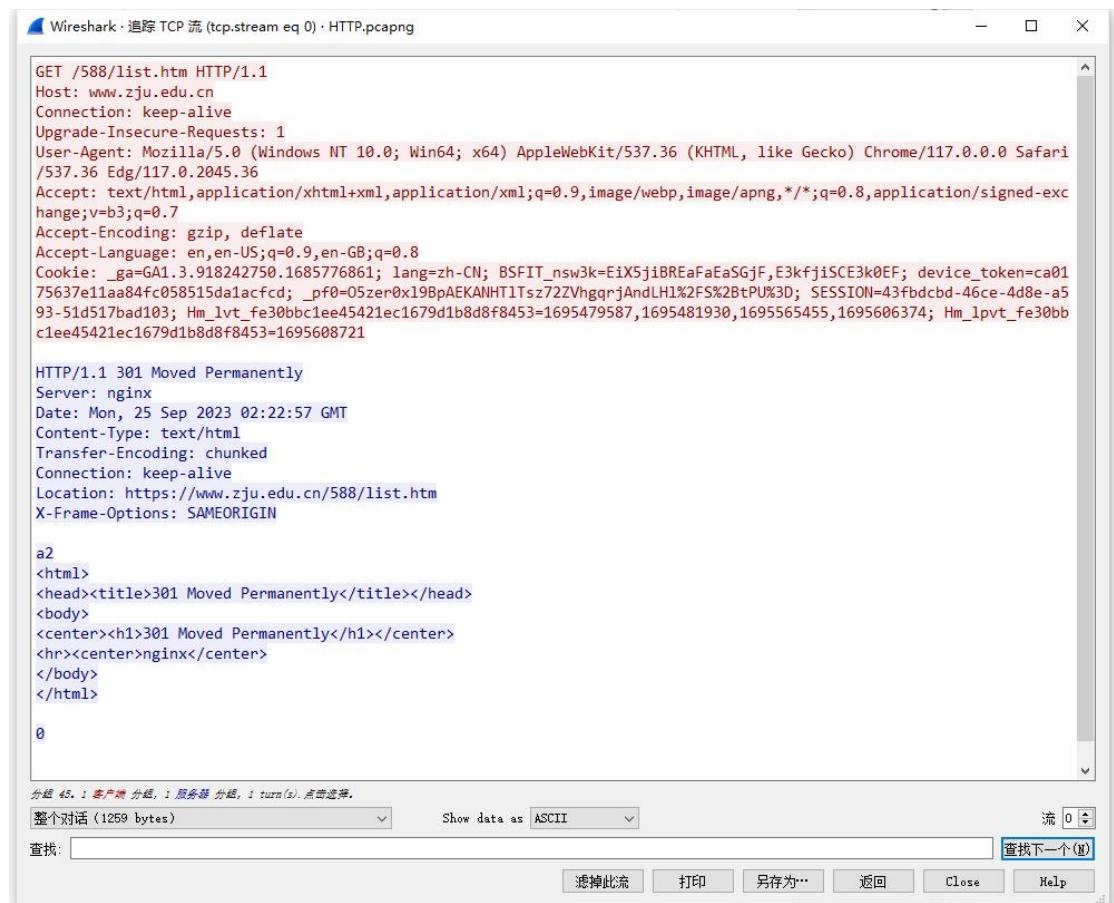
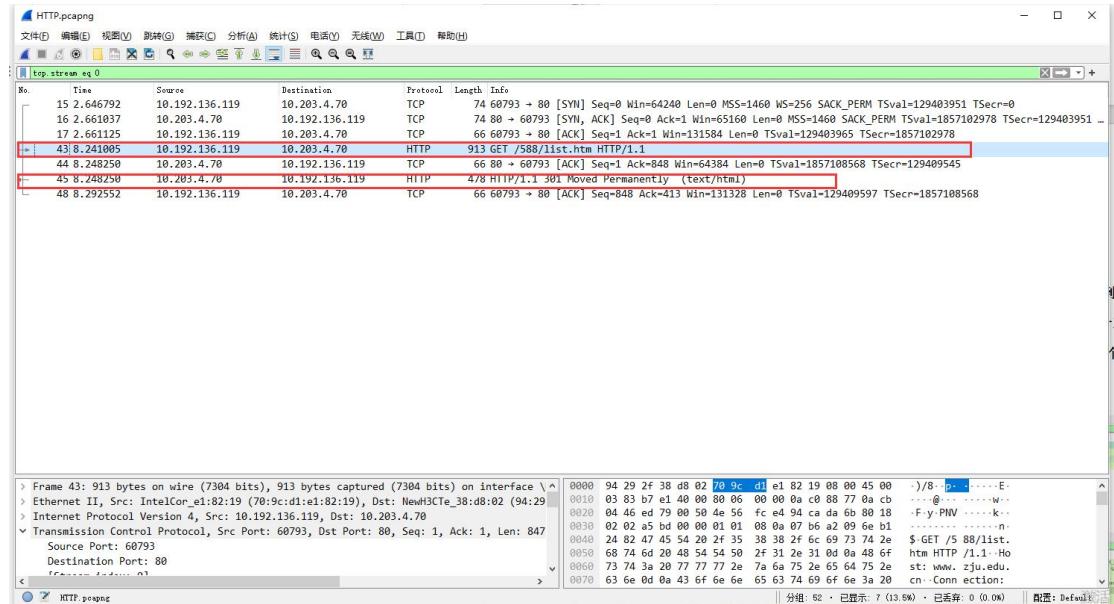


tcp.stream eq 1

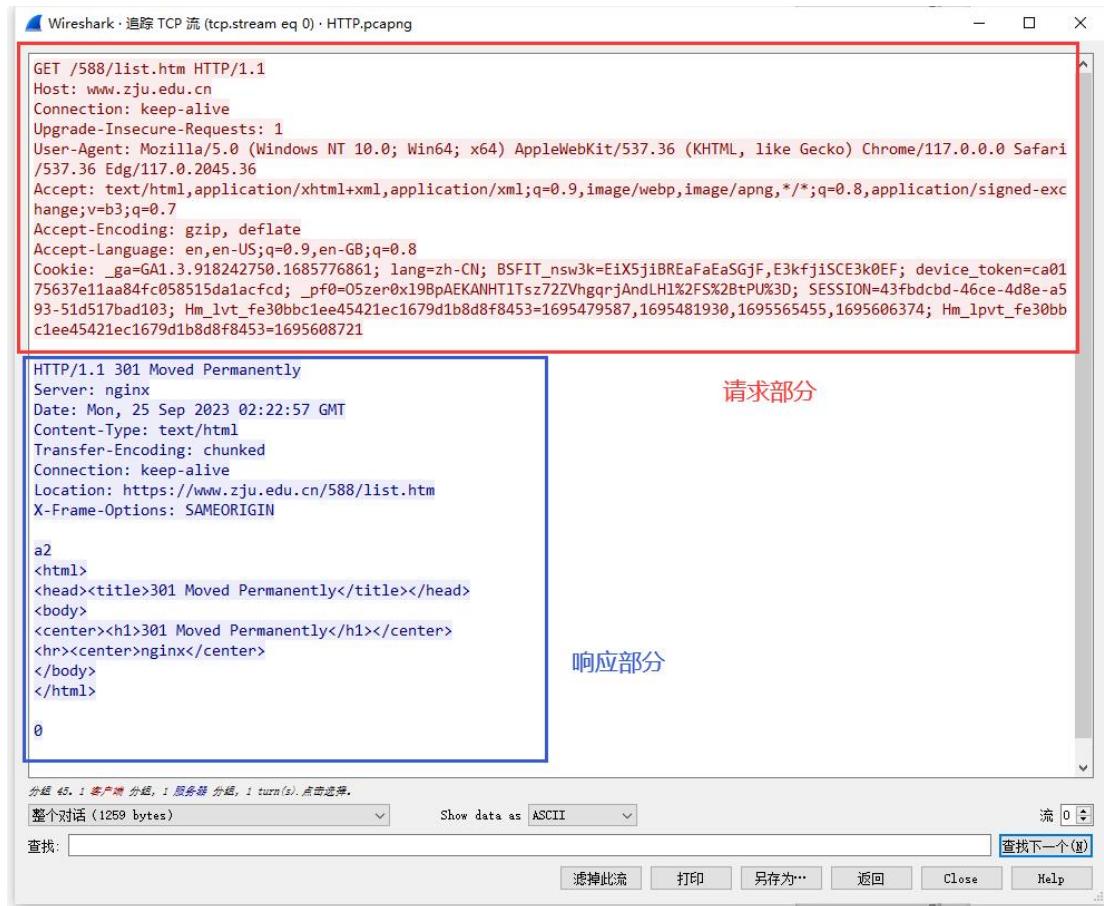
4. 右键点击某个 HTTP 数据包，选择跟踪 TCP 流，可以看到 HTTP 会话的数据。分析浏览器与 WEB 服务器之间进行了几次 HTTP 会话（一对 HTTP 请求和响应对）

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）：



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，捕获过滤器应该该怎么写？

设特定服务器 IP 为 X

捕获过滤器:

host == X and tcp port = 80 (也会带有 TCP 包)

或

host = X and tcp port http (只要 HTTP)

显示过滤器:

ip.addr = X and http

- 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 ICMP 协议数据包

当尝试 Ping 一个本机 ARP 缓存表中不存在的目标 IP 地址，而且目标主机的 IP 地址与自己不在同一子网（不在同一网络段）时，通常会向默认网关发送 Ping 请求。这是因为默认网关充当了不同子网之间的数据转发点。此时 Ping 会尝试将目标 IP 地址解析为 MAC 地址。如果本地 ARP 缓存中没有目标 IP 地址的对应 MAC 地址，它会首先发送 ARP 请求广播到本地网络，以尝试找到目标 IP 地址对应的 MAC 地址。如果目标主机与本机不在同一子网，那么 ARP 请求广播会发送到默认网关的 MAC 地址，因为默认网关是用来连接不同子网的设备。当默认网关收到 ARP 请求后，它将会响应并提供自己的 MAC 地址，以便本机可以将 Ping 请求发送给默认网关，由默认网关负责将请求路由到目标主机所在的子网。ARP 请求广播用于解析目标 IP 地址的 MAC 地址，并且默认网关扮演了重要的角色，帮助将 Ping 请求传递到目标主机所在的不同子网。

Ping IP 地址：Ping 会直接将 ICMP 数据包发送到该 IP 地址。

Ping 域名：Ping 首先需要将域名解析为 IP 地址。这会使用 DNS 来查询域名所对应的 IP 地址。如果目标计算机的 IP 地址不在本地 ARP 缓存中，系统可能会生成 ARP 请求来查找目标计算机的 MAC 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？

Tracert/Traceroute 发送 ICMP 协议数据包：

整个路由跟踪过程如下：

发送探测数据包：Tracert/Traceroute 工具向目标主机发送一系列的探测数据包。每个探测数据包都带有一个不同的 TTL（Time to Live）值，TTL 值从 1 开始递增，每次增加 1。

第一个路由器处理：当第一个探测数据包到达第一台路由器时，TTL 值为 1，这意味着它只能经过一个路由跳转。当路由器收到具有 TTL 为 1 的数据包时，它会将 TTL 减 1，并发现 TTL 值现在为 0，这时它会丢弃数据包，并向发送方返回 ICMP 超时消息。

超时消息返回：Tracert/Traceroute 工具捕获到 ICMP 超时消息后，记录了此路由器的 IP 地址和响应时间，并发送下一个 TTL 值的探测数据包。这个过程一直重复，TTL 值逐渐增加，直到探测数据包到达目标主机。

目标主机响应：当探测数据包到达目标主机时，目标主机会生成一个 ICMP 端口不可达消息，将其发送回 Tracert/Traceroute 工具。这个消息包含了目标主机的 IP 地址和响应时间。

绘制路由跟踪结果：Tracert/Traceroute 工具根据收到的响应数据包构建路由跟踪结果。它显示了从源主机到目标主机的路径中的每个路由器或中间节点的 IP 地址，

以及每个节点的响应时间。

- 如何理解 TCP 连接和 HTTP 会话？他们之间存在什么关系？

TCP

TCP 连接是指在两台计算机之间建立的可靠的、双向的、持久的通信通道。它确保数据的可靠传输，包括数据的分段、重新排序、丢失重传等机制。

TCP 连接是通过 IP 地址和端口号来标识的，这两者组合在一起形成了套接字（Socket）。在一个 TCP 连接中，数据可以双向流动，允许客户端和服务器之间的双向通信。

HTTP

HTTP 是一种应用层协议，用于在 Web 上传输超文本文档（如网页）和其他资源。

HTTP 会话是指在客户端和服务器之间建立的一系列 HTTP 请求和响应交换。通常，一个 HTTP 会话包含多个 HTTP 请求和响应，它们之间可以有一定的关联性。

在 HTTP 会话中，客户端发送 HTTP 请求到服务器，服务器处理请求并返回 HTTP 响应。这个过程可以包括多轮的请求和响应，例如，当浏览器加载一个网页时，可能会涉及多个 HTTP 请求来获取页面的不同资源（HTML、CSS、JavaScript、图像等）。

HTTP 会话通常是无状态的，这意味着每个 HTTP 请求之间没有直接关联，服务器不会保持关于客户端的状态信息。为了实现状态管理，通常会使用 HTTP Cookie 等机制。

关系：

HTTP 通常运行在 TCP 连接之上。当客户端要与服务器建立 HTTP 通信时，首先需要建立一个 TCP 连接，然后在该 TCP 连接上进行 HTTP 请求和响应的交互。

一个 TCP 连接可以承载多个 HTTP 会话。在一个 TCP 连接上，客户端可以发起多个 HTTP 请求，并且服务器可以按顺序响应这些请求。这有助于减少 TCP 连接的建立和断开开销，提高通信效率。

HTTP 会话通过 HTTP 协议来定义请求和响应的格式和规则，而 TCP 连接则提供了底层的数据传输和可靠性保证。HTTP 会话是为保持用户状态、为不同 TCP 连接建立联系的机制，一个 HTTP 会话可以包含若干次 TCP 连接的建立与断开。HTTP 建立在 TCP 连接的基础说进行。

- 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 协议的原因：

快速响应时间：DNS 旨在提供快速的域名解析服务。由于 UDP 是一种无连接协议，它的开销较小，不需要建立和维护连接，因此 DNS 查询通常能够更快地获得响应。这对于快速解析域名非常重要，因为延迟会直接影响用户体验。

较小的开销：UDP 是一种无连接协议，不需要像 TCP 那样进行三次握手等连接建立过程。这降低了网络和服务器资源的消耗，允许 DNS 服务器高效地处理大量查询请求。

不需要可靠性保证：DNS 查询通常涉及到短小的请求和响应，不像 HTTP 那样需要严格的可靠性保证。即使 DNS 查询中的某些响应丢失，客户端通常可以忍受，因为可以通过发起另一个查询来尝试解析域名。

容忍少量的丢包：DNS 查询通常是轻量级的，不涉及大量数据传输，所以如果某些 UDP 数据包在传输过程中丢失，它们通常会被忽略，而客户端可以根据需要重试查询。

HTTP 使用 TCP 协议的原因：

可靠性：HTTP 是一种应用层协议，通常用于传输 HTML 页面、图像、视频和其他 Web 资源，这些资源的可靠性非常重要。TCP 协议提供了可靠的数据传输，它通过序号、确认和重传机制确保数据按顺序到达目标，并且在发生丢失或损坏时能够进行恢复。

顺序性：HTTP 请求和响应的顺序很重要。TCP 协议通过序号来保证数据包的顺序传输，这对于确保网页和其他资源按正确的顺序加载非常关键。

流量控制和拥塞控制：TCP 协议提供了流量控制和拥塞控制机制，以防止过多的数据流入网络，从而避免网络拥塞。这对于互联网上大量的 HTTP 请求和响应非常重要，以保持网络的稳定性和可靠性。

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：

- 1.为什么捕获过滤器中只能指定端口而无法抓取特定的协议类型？
- 2.捕获过滤器和显示过滤器都是怎么运作的，它们为什么语法不一致
- 3.DNS 标准查询的响应都能看出哪些信息。
- 4.有关 ARP 和 DNS 的原理和联系

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：

捕获过滤器与显示过滤器语法存在些许不同

在做 Part3 需要获得 zju.edu.cn 下的 HTTP 数据包，这个时候 Wireshark 并不能抓取成功，需要点进主页在切换别的页(比如如下点击顺序)

The screenshot shows the Zhejiang University website homepage. The top navigation bar includes links for '信息公开' (Information Disclosure), '校网导航' (Campus Network Navigation), '浙大服务' (Zhejiang University Services), and a search bar labeled '浙大百事通搜索' (Search Zhejiang University). The main menu features categories like '校情总览' (University Overview), '求是新闻' (Qishiz News), '综合服务' (Comprehensive Services), '学校机构' (University Institutions), '教师队伍' (Teacher Team), '教育教学' (Teaching and Education), '科学研究' (Scientific Research), and '招生就业' (Admissions and Employment). A sidebar on the left lists links for '学校概况' (University Profile), '学校章程' (University Charter), '学校标识' (University Logo), '现任领导' (Current Leadership), '统计公报' (Statistical Report), '虚拟校园' (Virtual Campus), and '校史馆' (University History Museum). The central content area displays a large image of the university campus at night. Below it, a section titled '学校数据与统计公报' (School Data and Statistical Report) contains three sub-links: '毕业生就业质量公报' (Graduate Employment Quality Report) and '本科教学质量报告' (Undergraduate Teaching Quality Report). The main report page is titled '浙江大学2022年基本数据' (Zhejiang University 2022 Basic Data) and includes a table for student enrollment statistics.

学生情况 (单位: 人)	
在校全日制学生	65821
本科生	29117
其中: 国际学生	2496
硕士研究生	27098
其中: 非全日制硕士研究生	6544
国际学生	862
博士研究生	16893
其中: 非全日制博士研究生	743
国际学生	799
国际学生数	5123

注意输入过滤器字母不要大写，是有大小写区分的。

有时设置过滤器之后不会立即显示，或者切换过滤器会有卡顿，导致看上去什么包都没抓上，此时可以在此输入并多按几下 enter（空过滤器同理），就会发现抓到的包会刷新出来。

你对本实验安排有哪些更好的建议呢？欢迎献计献策：

建议不要再使用 www.zju.edu.cn 作为 Part3 的查询网址，做实验找不到 HTTP 协议，后来寻求学长帮助才知道原来目前大多数网页都采取了 HTTPS 协议，包括 www.zju.edu.cn，所以 Wireshark 无法抓取 HTTP 数据包。

本实验和教学课相差较大，需要很多协议相关的知识，以及工作原理介绍，不然抓包也不知道应该看什么，应该截取什么。