# 华东师范大学软件工程学院实验报告

|  |  |  |
| --- | --- | --- |
| **实验课程**：计算机网络实验 | **年级**：2023级 | **实验成绩**： |
| **实验名称**：IP v4 | **姓名**：陆尚辰 |  |
| **实验编号**：Lab3 | **学号**：10235101545 | **实验日期**：2024.12.6 |
| **指导教师**：刘献忠 | **组号**： | **实验时间**： |

**一、实验目的**

1. 学会通过Wireshark分析ip协议

2. 了解IP数据报的组成

3. 了解IP各部分的含义

**二、实验内容与实验步骤**

1.获取IP packets

（1）启动Wireshark，在菜单栏的捕获->选项中进行设置，选择已连接的以太网，设置捕获过滤器为“tcp port 80”，将混杂模式设为关闭,勾选 enable network name resolution.然后开始捕获。

（2）打开windows的命令行，在里面输入wget www.sina.com

（3）打开Wireshark， 停止捕获。

2.分析和绘制

根据你对IP报文的理解，画出IP报文的结构。需要显示出IP报头字段的位置和大小（字节为单位）。

3.Internet Path

（1）在DOS命令行下使用tracert命令:

（2）tracert www.sina.com

（3）保存输出

（4）根据输出画出网络路径。\*号可能是因为某些路由不会为TTL超时发送“已超时”信息。

4.计算校验和

（1）IP报头的校验和可以用来验证一个数据包是否正确。

（2）选择一个IP报文，计算它的checksum。

**三、实验环境**

1. Wireshark v2.0.2

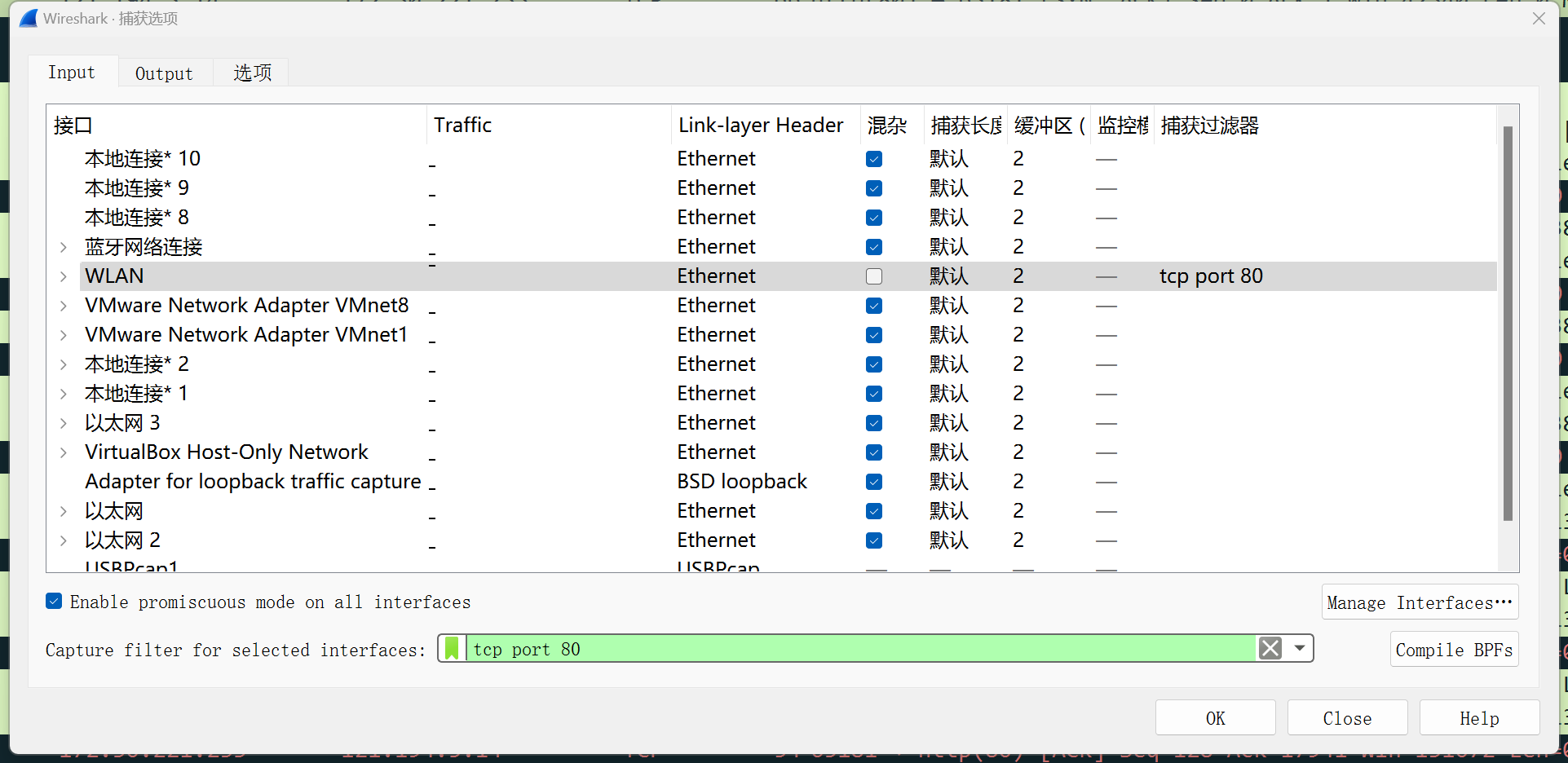
2. Windows操作系统

3. wget

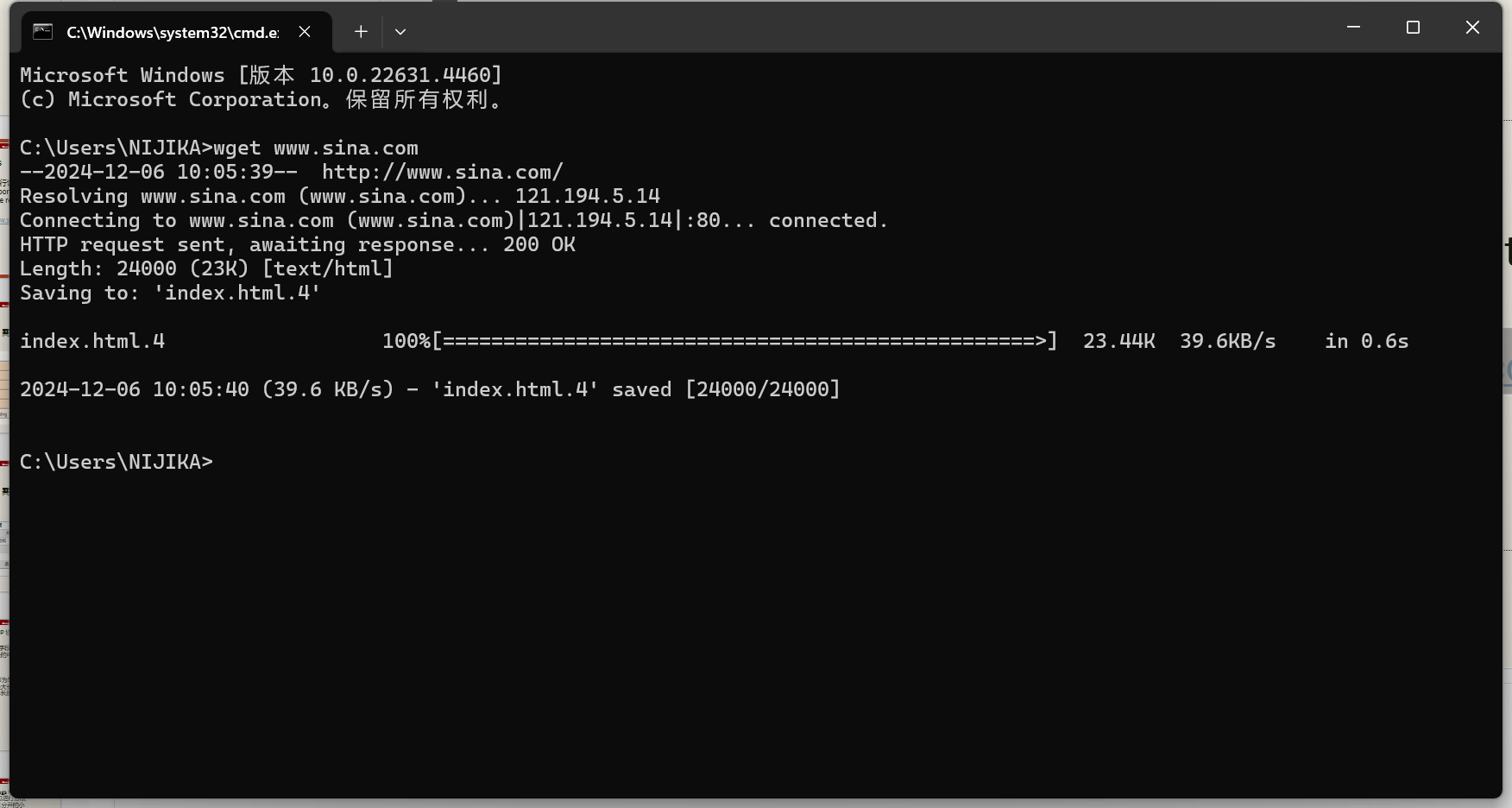
**四、实验过程与分析**

**4.1获取IP Packets**

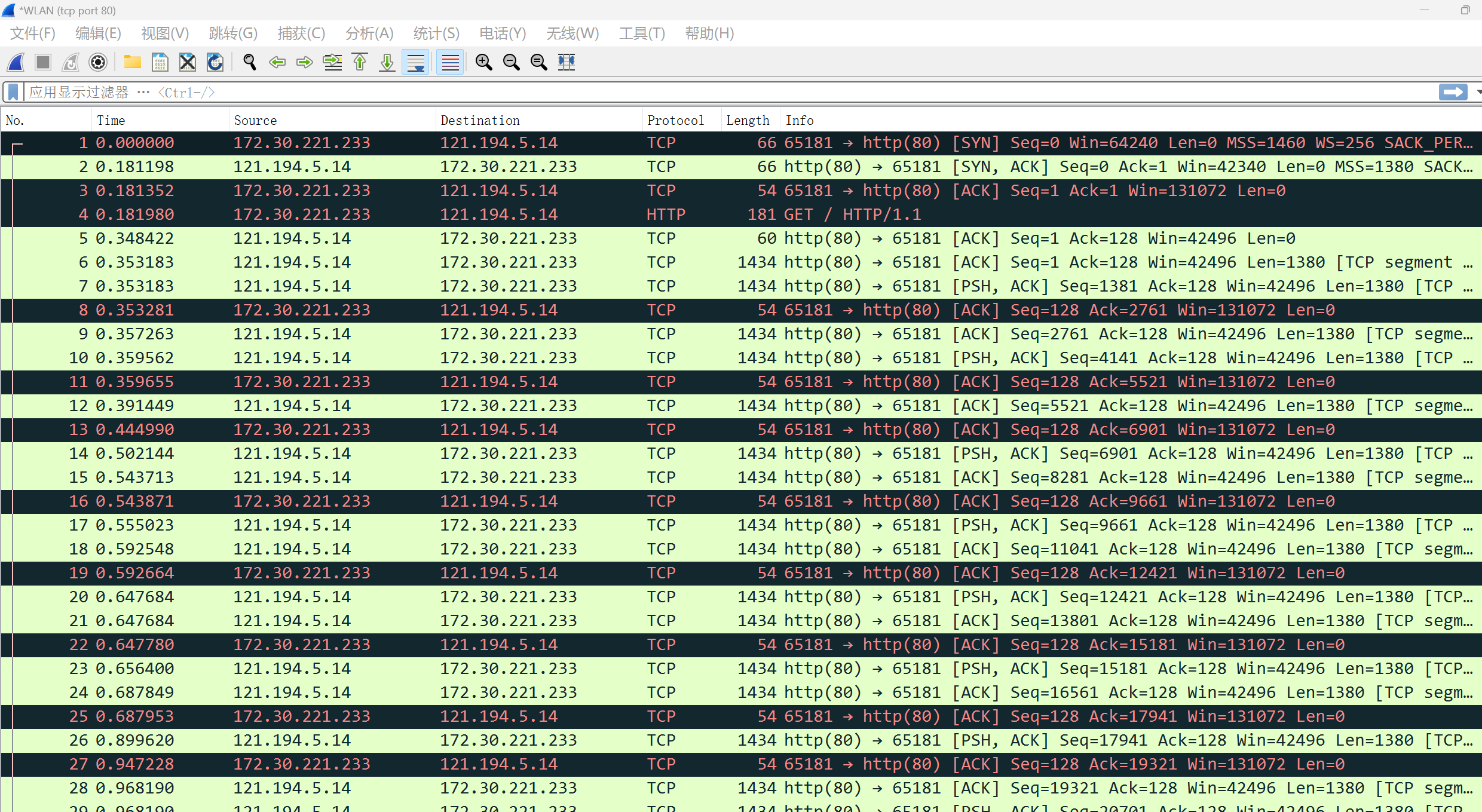
（1） 启动Wireshark，在菜单栏的捕获->选项中进行设置，选择已连接的以太网，设置捕获过滤器为“tcp port 80”，将混杂模式设为关闭,勾选 enable network name resolution.然后开始捕获。



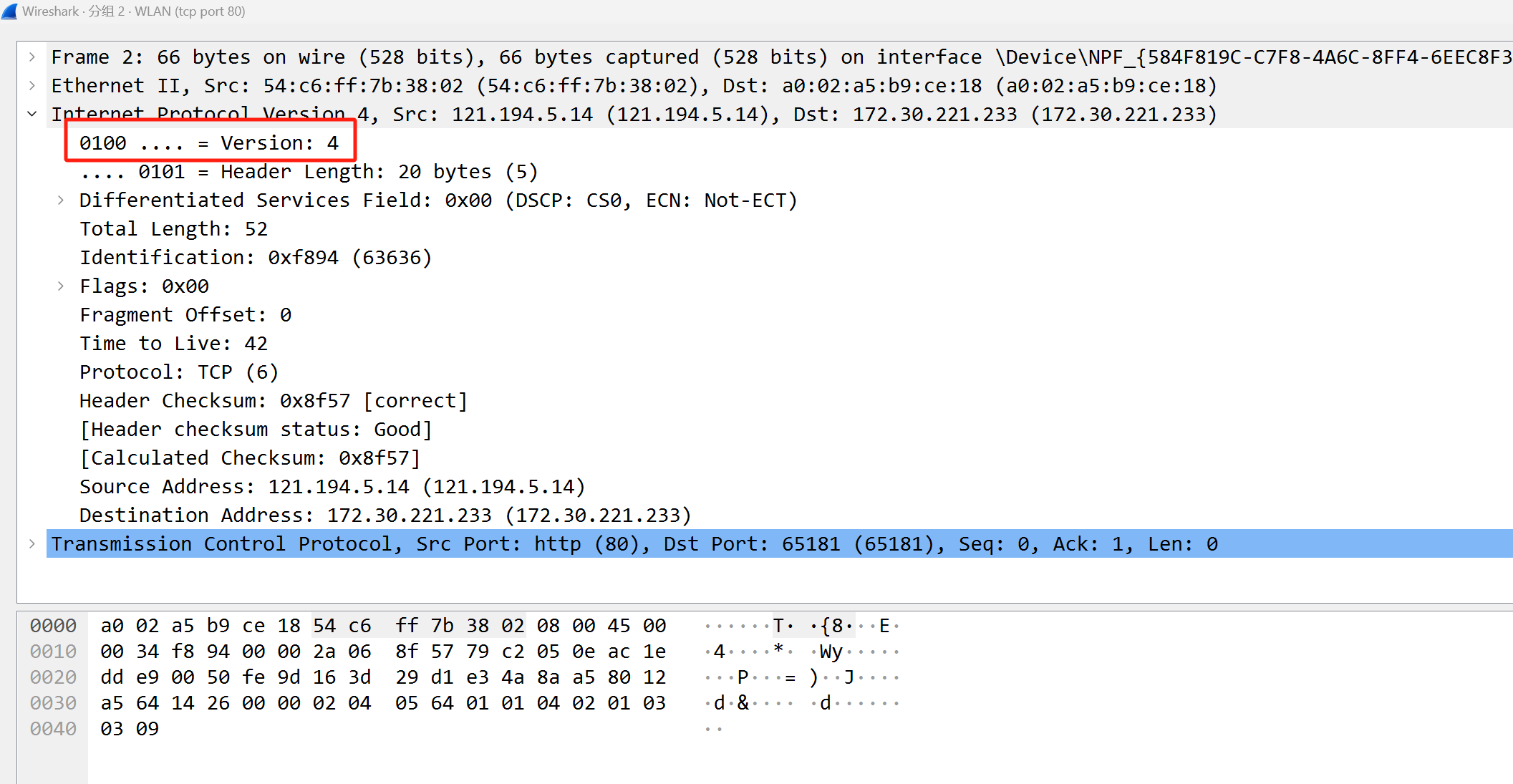
（2）打开windows的命令行，在里面输入wget [www.sina.com](http://www.sina.com)



（3）停止捕获，得到如下结果：



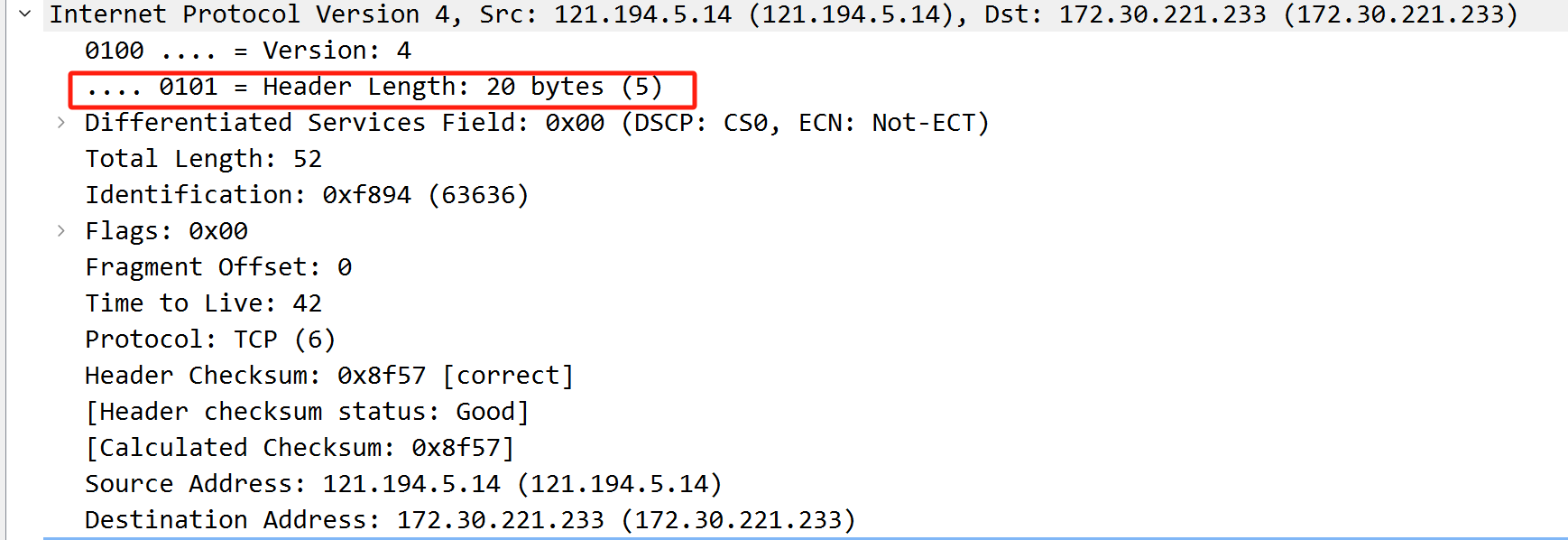
**4.2分析 IPV4 包并绘制报文结构**



（1）第一个字段表示版本号，长度为4位，表示目前采用的IP协议的版本号。为0100表示版本为4。

（2）第二个字段表示首部长度，长度为4位，表示IP报头的长度。

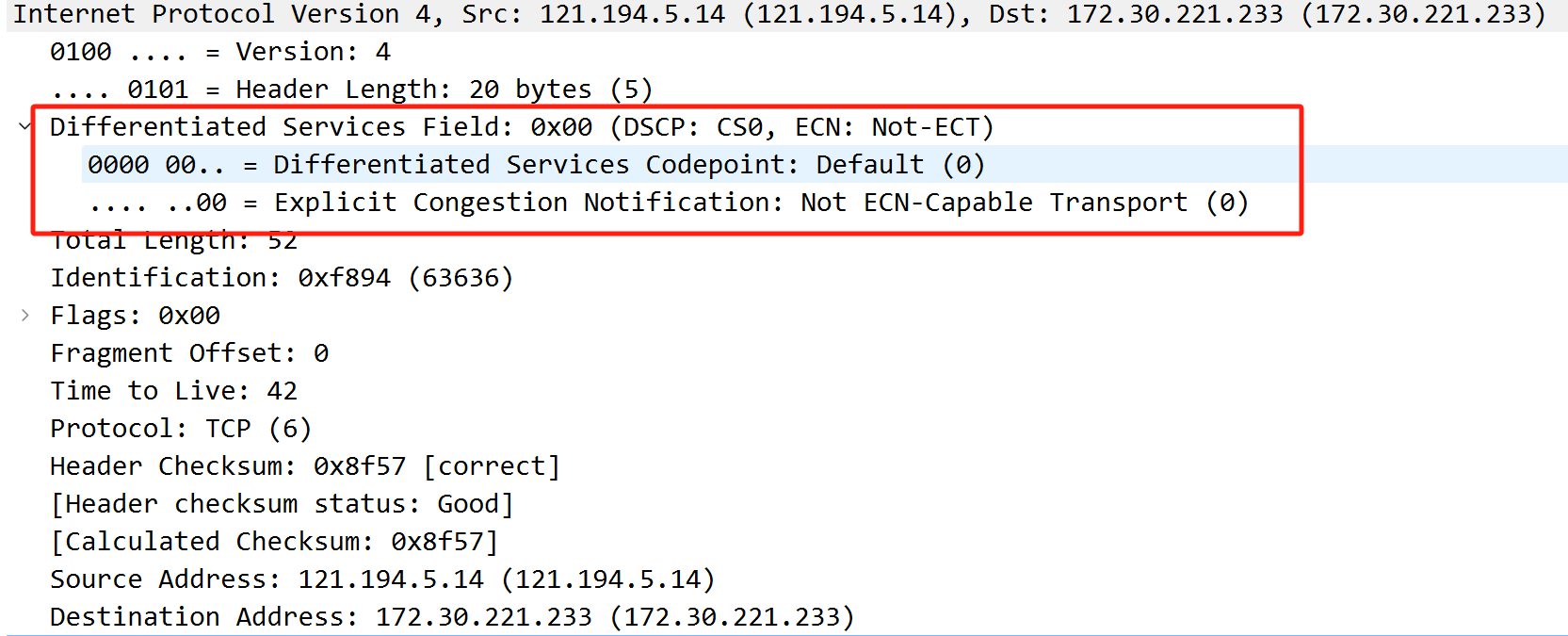
这里，首部长度为 20 bytes。



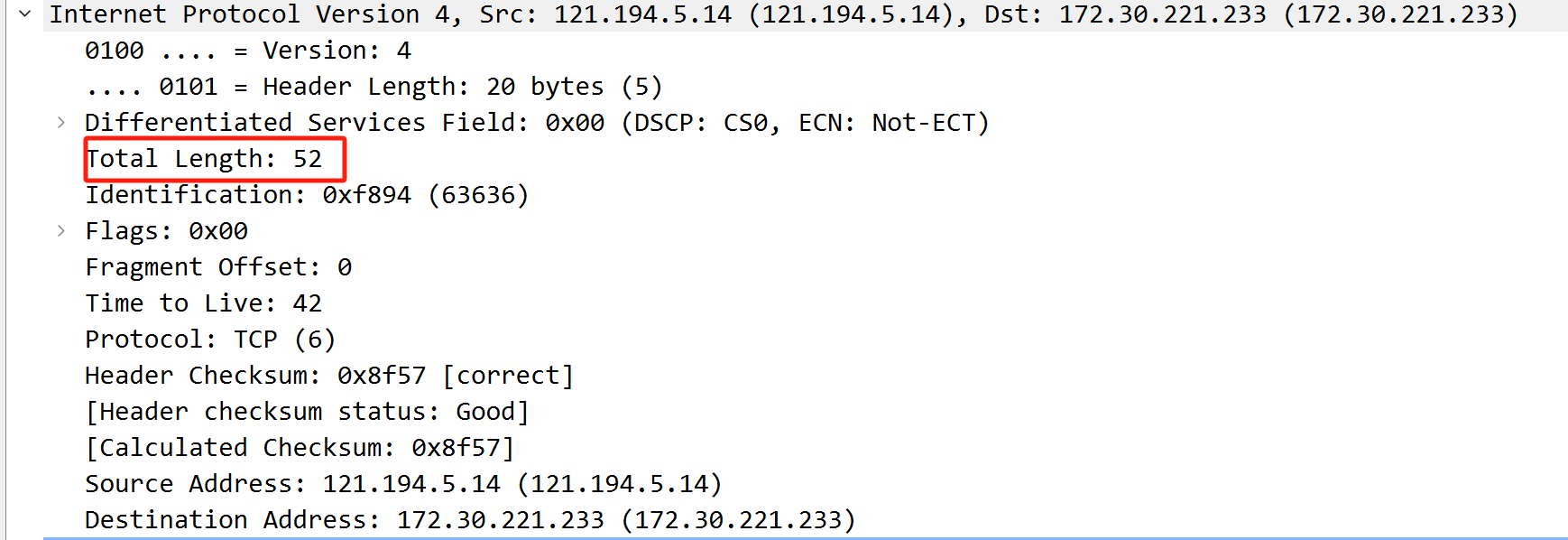
（3）第三个字段服务类型，长度为8位，指定数据报的优先级和服务类型。第一个部分是DSCP，长度为6位，表示区分服务代码点，用于区分不同的服务质量。

第二个部分是ECN，长度为2bit，表示显式拥塞通知，用于指示网络拥塞。

在这个数据报中DSCP的值为0000 00表示默认服务，ECN 的值为 00，表示没有拥塞。

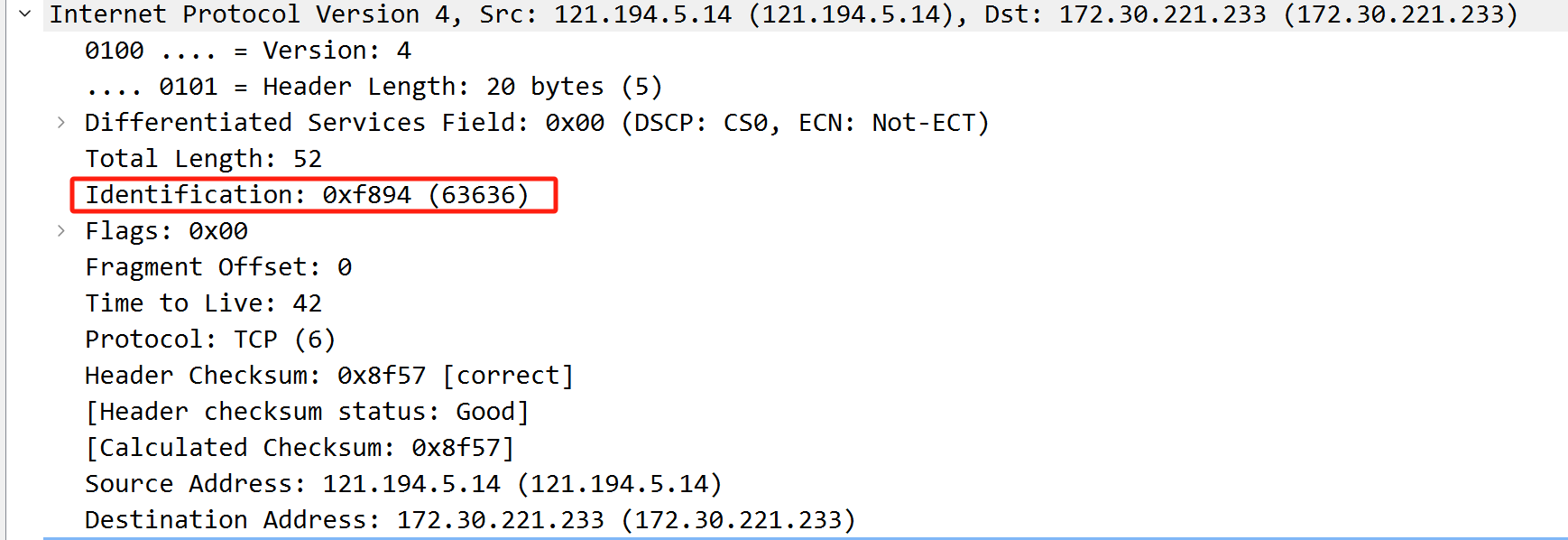


（4）总长度，长度为16位，表示整个IP数据报的长度，包括首部和数据部分，单位为1字节。这里表示的长度为52字节。



（5）标识符，占16位，用于标识每一个IP数据报，该字段和为Flags 和 Fragment Offest字段结合，对较大的数据报进行分片操作。当数据报需要分片时，所有分片具有相同的标识符。

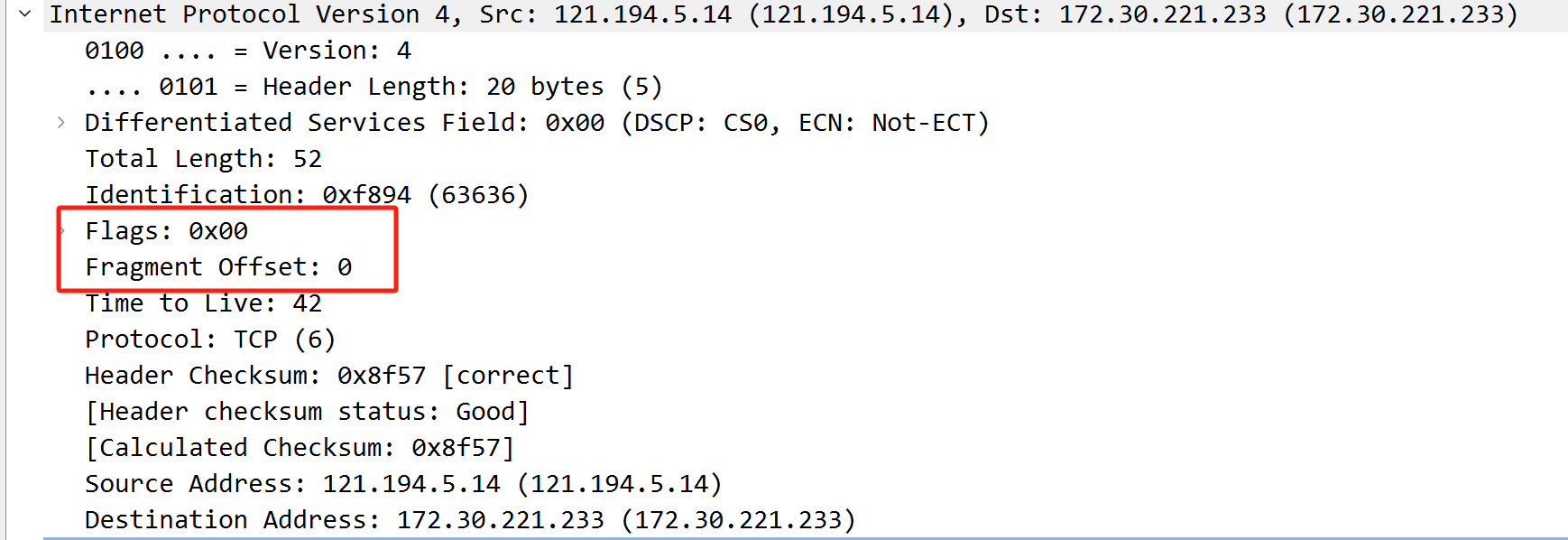
这里，标识符为：0xf894(63636)



(6) 标志：占3位，与分片有关，用于控制和标识数据报是否可以分片及是否为最后一个分片。第一位不使用。第二位是 DF位，DF = 1时表明路由器不能对该数据报分段。如果一个上层数据报无法在不分段的情况下进行转发，则路由器会丢弃该上层数据包并返回一个错误信息。第三位是 MF位，MF=1 表示后面还有分片的数据报，MF=0表示这已经是若干数据报片中的最后一个。

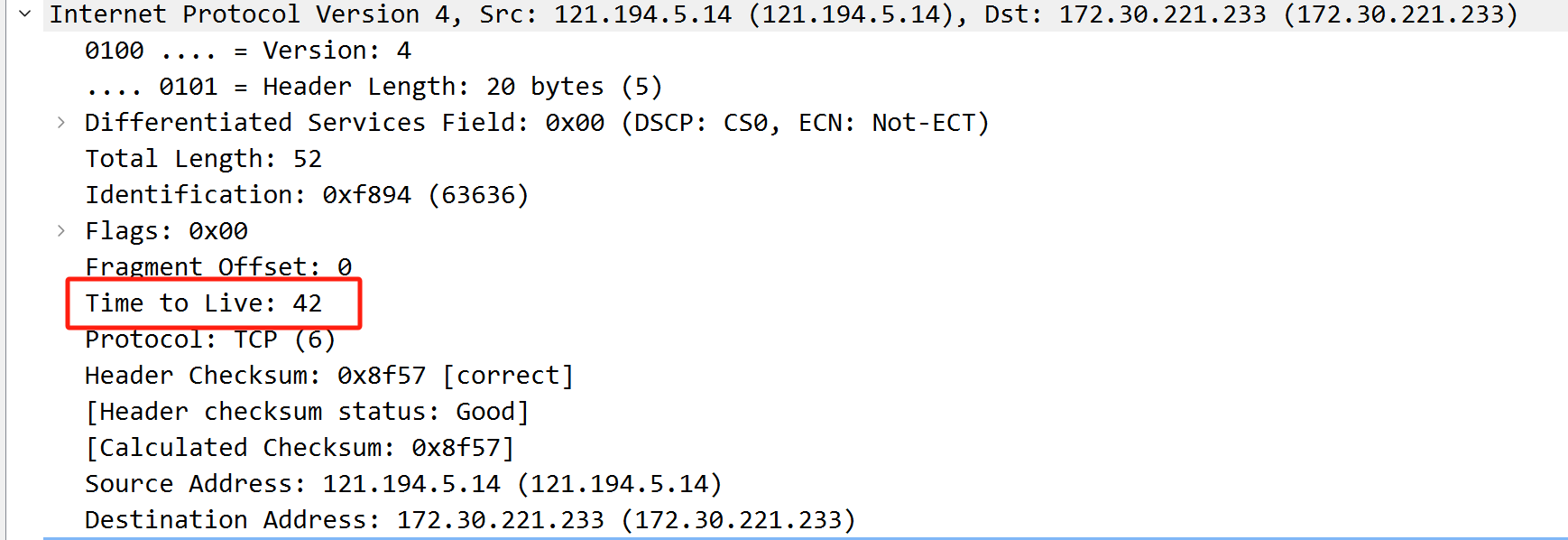
在这里DF为0，MF为0，表示可分段，并且这是最后一个数据片。

(7)片偏移：占13位，用于指示分片在原始数据报中的相对位置，相对于原数据报的数据部分，该分片从何处开始，是开始还是中间，以便于进行重组还原IP包。在这个数据报中，片偏移为0。



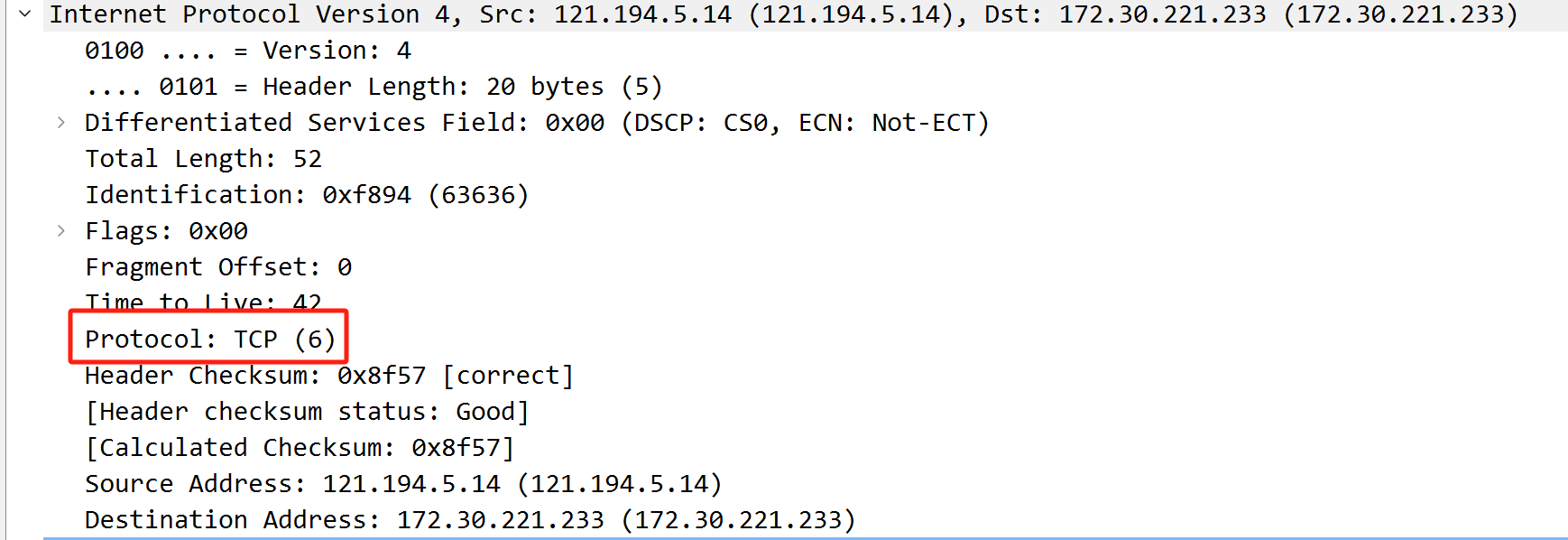
(8)生存时间TTL：占8位，定义数据报在网络中的最大存活时间，每经过一个路由器TTL减1，为0时数据报被丢弃。

这里TTL为42。



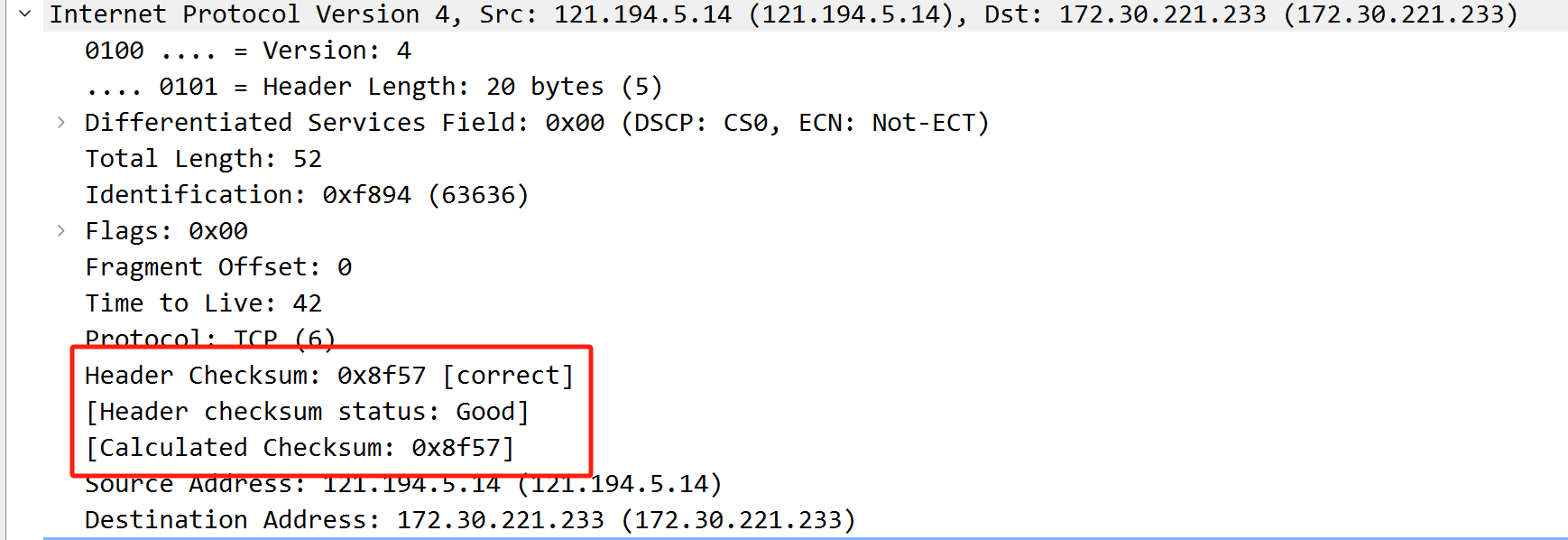
(9)协议占8位，指出数据部分使用的上层协议， 例如TCP（6）UDP（17）

这里协议为TCP（6）。



(10)头部校验和:占16位，用于校验首部是否有错误。

可以看到这里校验和为0x8f57，未发生错误。



(11)源IP地址：占32位（IPv4）或128位（IPv6），标识发送方的IP地址。这里源地址为121.194.5.14

(12)目的IP地址：占32位（IPv4）或128位（IPv6），标识接收方的IP地址。这里目的地址为172.30.221.233

由此，我们可以得到如下报文结构：



**4.3回答问题**

（**1）你的计算机和远程服务器的IP地址是多少？**

我的计算机IP地址：121.194.5.14

远程服务器IP地址：172.30.221.233

**（2）总长度字段是否包括IP头加IP有效载荷，或只是IP有效载荷？**

Total Length包括了IP的头和有效载荷，指的是总长度。

**（3）在不同的数据包中标识字段的值如何更改或保持相同的值？例如，在同一个TCP连接中的数据包中标识字段的值是否相同，还是每个都不同？不同传输方向上会相同吗？如果标识字段的值有变化，你能从中找出规律吗？**

标识字段的值在不同的数据包中不同。在同一个TCP 连接中，标识字段的值不同。TCP序列号和确认号在同一个传输方向上根据字节流的发送和接收情况依次递增，在不同传输方向上分别由两端独立维护，它们的值是相互对应的，用于确保数据的可靠传输和按序接收。在这个数据报中，标识字段的值为 0xf894。

**（4）从计算机发送的报文的TTL字段初始值是什么？它是最大可能的值，还是一些较低的值？**

TTL字段是IPv4 包头的一个8bit字段，其最大值是 255。TTL 字段初始值因操作系统而异，Windows系统TTL的初始值通常为128。

**（5）如何判断一个数据包是否被分片？（普通操作下的大多数的IP数据包不会被分片的。但是接收者需要有办法去确定。）**

可以根据IP 报头中的标志位（MF 和 DF）和片偏移字段进行判断

如果 DF 位被设置为 1，表示这个数据包不允许被分片传输。

如果 MF 位为 1，表示这个数据包是一个分片，且后面还有更多的分片；如果 MF 位为 0，则表示这个分片是原数据包的最后一个分片。

如果一个数据包没有被分段，那么它的标志字段的 DF 位为 1，且标志字段的 MF 位为 0。

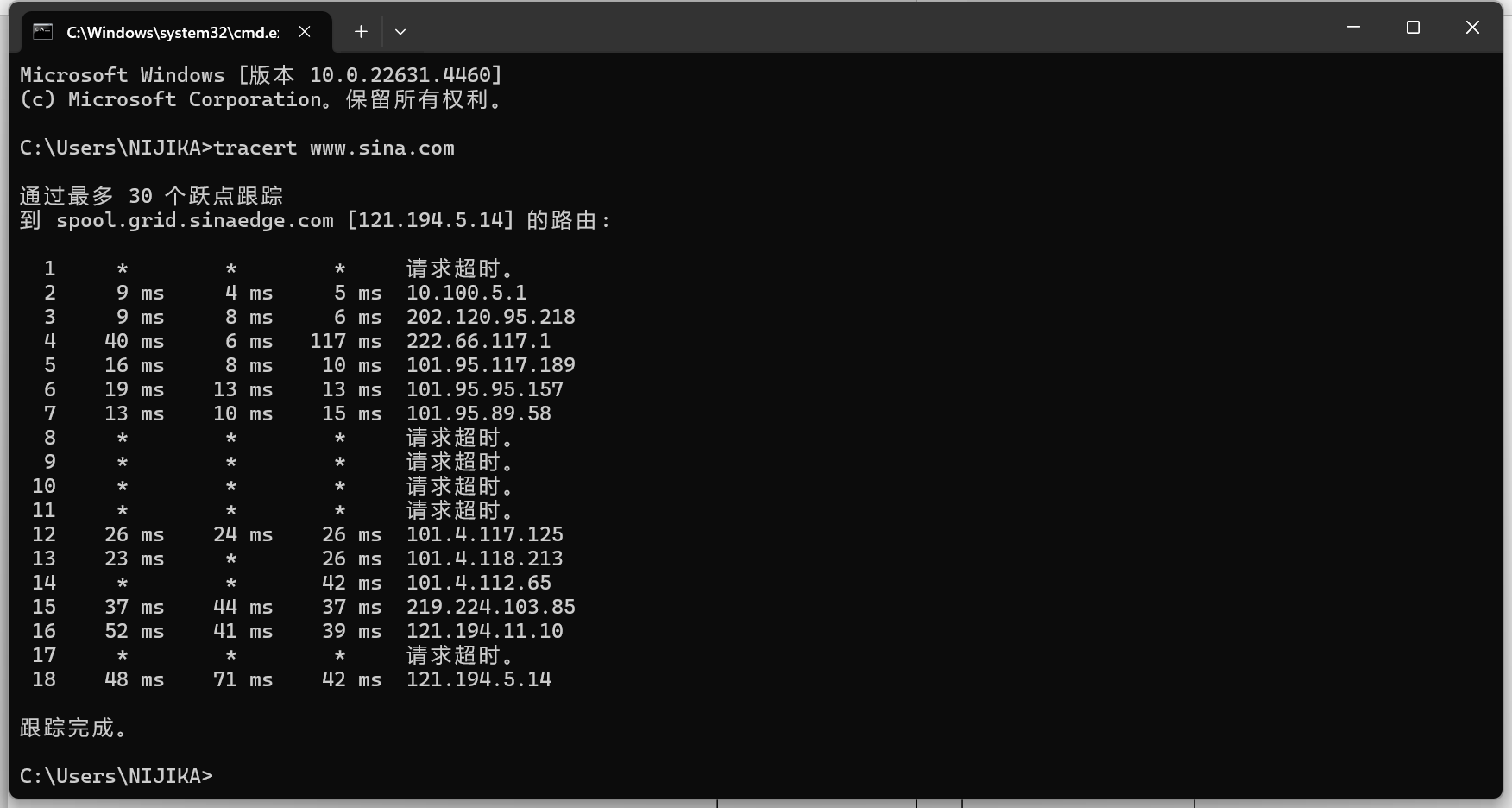
**（6）IP报头的长度是多少，它是如何被编码进报头长度域的？**

IP报头的长度为20bytes，版本号和首部长度字段共占8位，其中版本号占4位，首部长度占4位。

**4.4 Internet Path**

在DOS命令行下使用tracert命令:tracert www.sina.com

如图所示：

****

由此可以画出网络路径图：

本机

121.194.5.14

\*

10.100.5.1

\*

219.224.103.85

202.120.95.218

222.66.117.1

101.4.112.65

101.4.118.213

101.95.117.189

101.95.89.58

101.4.117.125

\*

\*

\*

\*

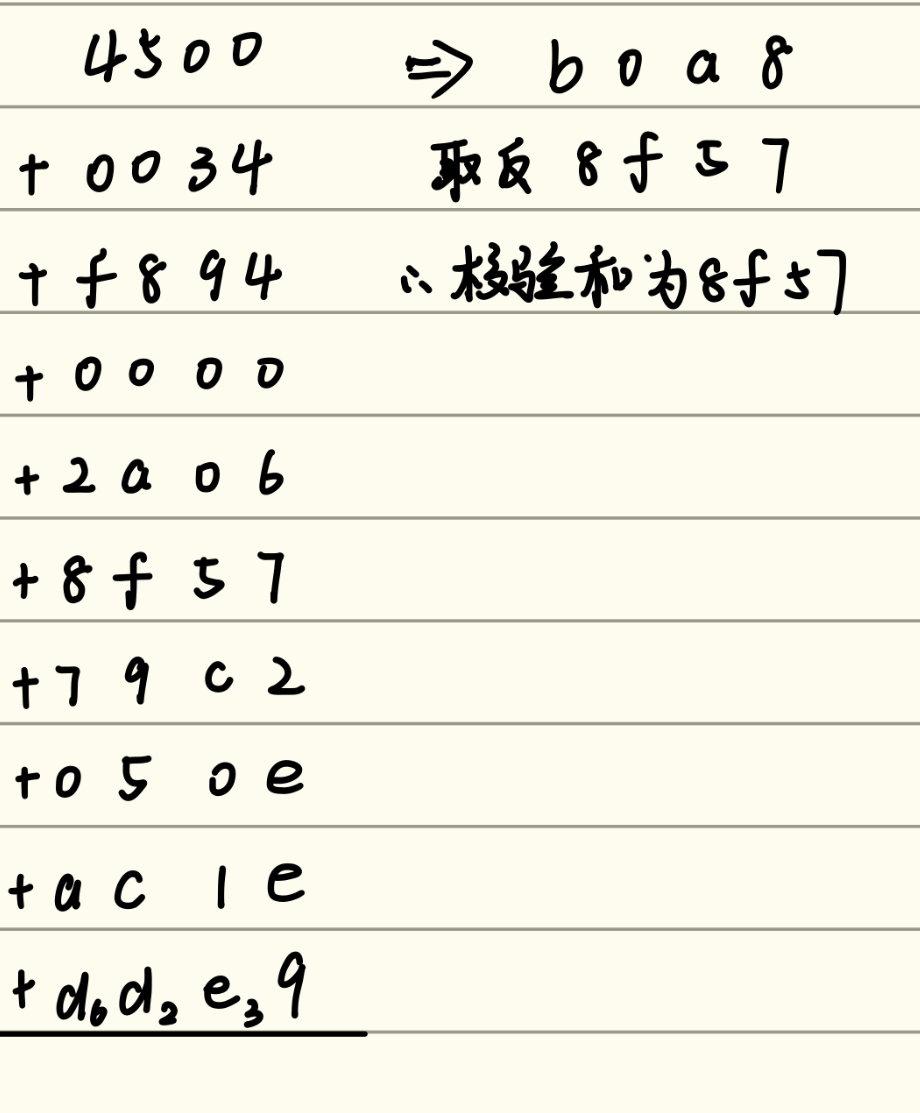
**4.5 校验和**

IP报头的校验和可以用来验证一个数据包是否正确。

选择前文的IP报文，计算它的checksum。

得到的数据为：

45 00 00 34 f8 94 00 00 2a 06 8f 57 79 c2 05 0e ac 1e dd e9



得到校验和为0x8f57，与ip报内checksum一致。

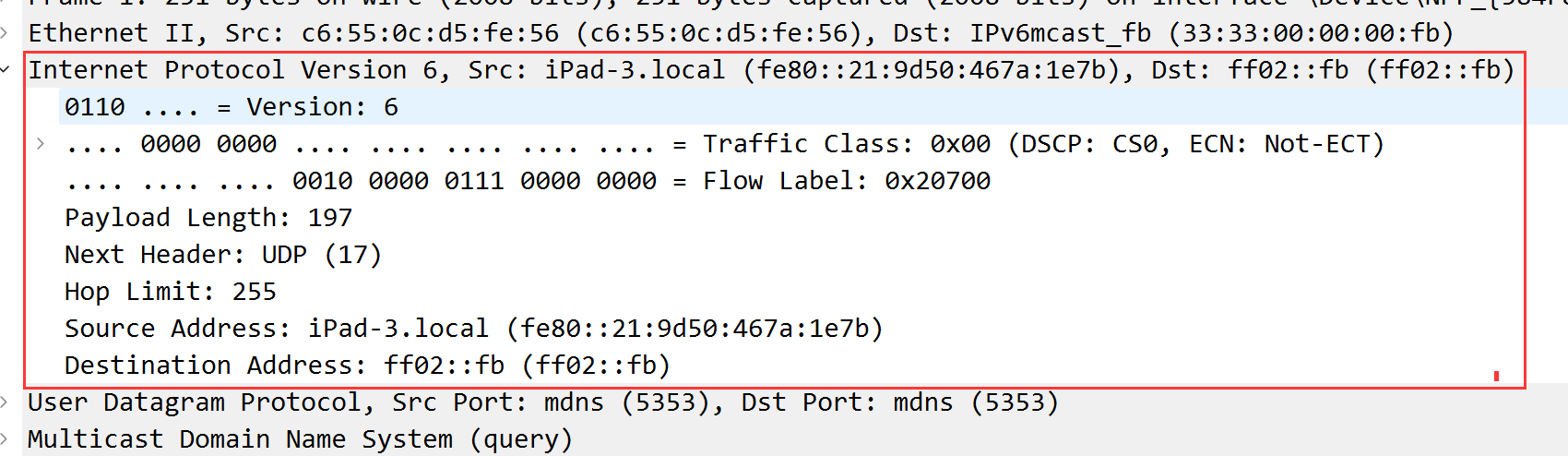
**五、实验结果总结**

1.问题思考：

（1）Read about and experiment with IPv6. Modern operating systems already include support for IPv6, so you may be able to capture IPv6 traffic on your network. You can also “join the IPv6” backbone by tunneling to an IPv6 provider.

可以利用网络分析工具Wireshark，在相应的网络接口上进行数据包捕获设置，选择捕获 IPv6 相关协议的流量，就能获取到网络中传输的 IPv6 流量信息了。在 Wireshark 中，启动捕获后，通过筛选条件（如 “ip.version == 6”）来筛选出 IPv6 数据包进行查看和分析。

如下图所示：



IPv6 数据包的结构与 IPv4 数据包的结构有所不同。

可以看到校验和字段被取消。增加了 Hop Limit 字段，用于替代 IPv4 中的 TTL字段。

IPv6 具有多方面的特点。它拥有巨大的地址空间，128 位的地址数量庞大。报头结构简化，固定为 40 字节，相比 IPv4 更利于路由器高效处理数据包。支持自动配置，包括无状态和有状态两种方式，方便设备快速接入网络。安全性良好，集成了 IPsec，强制使用加密和认证手段保障数据传输安全。对移动性支持增强，使移动设备在不同网络间切换时能高效处理地址变更和保持通信。还具备任播功能，能将数据发送到一组接口中距离发送者最近的接口，像在 CDN 中有很好的应用，可提升访问速度。

（2）Learn about tunnels, which wrap an IP packet within another IP header.

关于隧道：它能够实现在一种网络协议之上传输另一种网络协议的数据包，使得不同网络协议环境之间可以互通。

隧道可以用于将 IPv6 数据包封装在 IPv4数据包中，也可以用于将 IPv4 数据包封装在 IPv6 数据包中。

可以跨越不同 IP 协议的网络环境实现通信。

（3）Read about IP geolocation. It is the process of assigning a geographical location to an IP address using measurements or clues from its name administrative databases. Try a geolocation service.

IP 地理定位是一种通过多种线索来确定 IP 地址地理位置的技术。它主要利用 IP 地址分配机构的数据库信息，这些数据库在分配 IP 段时会关联一定的地理区域范围；同时也会分析 IP 数据包在网络中的路由路径，借助网络节点的已知地理位置来推断；还会综合互联网服务提供商所掌握的用户接入位置线索。不过，IP 地理定位的准确性会受到多种因素的限制，例如动态 IP 分配会使位置信息发生变化，代理服务器和 VPN 等工具也会干扰定位，使其结果往往只是一个大致的参考范围。

（4）Learn about IPsec or IP security. It provides confidentiality and authentication for IP packets, and is often used as part of VPNs.

IPsec（IP 安全协议）是一种用于保障 IP 数据包安全的网络协议。IPsec VPN 的隧道模式下，会对整个原始 IP 数据包进行封装处理，添加新报头用于公网传输，到达后再解封装，以此确保数据在公网传输过程中的保密性、完整性和来源可靠性。

**六、附录**

无