**《计算机网络》课程实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **实验**  **名称** | 实验二 IP 和 TCP 数据分组的捕获和解析 | | **学 院** | 计算机学院 | **授课教师** | 张冬梅 |
| **班 级** | **班内序号** | **学 号** | | **学生姓名** | **成绩** | |
| **2020211314** | **19** | **2020211502** | | **王小龙** |  | |
| **实**  **验**  **内**  **容** | 本次实验内容：  （1）捕获在使用网络过程中产生的分组（packet）： IP 数据包、ICMP 报文、DHCP 报文、TCP 报文 段。  （2）分析各种分组的格式，说明各种分组在建立网络连接和通信过程中的作用。  （3）分析 IP 数据报分片的结构：理解长度大于 1500 字节 IP 数据报分片传输的结构  （4）分析 TCP 建立连接、拆除连接和数据通信的过程。 | | | | | |
| **学生实验报告** | 详见“实验报告和源程序”部分 | | | | | |
| **实**  **验**  **成**  **绩**  **评**  **定** | **评语**:  **成绩**:  指导教师签名：  年 月 日 | | | | | |

注：评语要体现每个学生的工作情况，可以加页。

实验报告和源程序

**一.实验内容**

1） 捕获在连接Internet过程中产生的网络层分组：DHCP分组，ARP分组，IP数据分组，ICMP分组；

2） 分析各种分组的格式，说明各种分组在建立网络连接过程中的作用；

3） 分析IP数据分组分片的结构；

4）分析TCP建立连接，拆除连接和数据通信的流程。

**二.实验目的**

通过本次实验了解计算机上网的工作过程，学习各种网络层分组的格式及其作用。

**三.实验环境**

1 台装有 Windows 操作系统的 PC 机，要求能够连接到 Internet，并安装 Wireshark 软件。

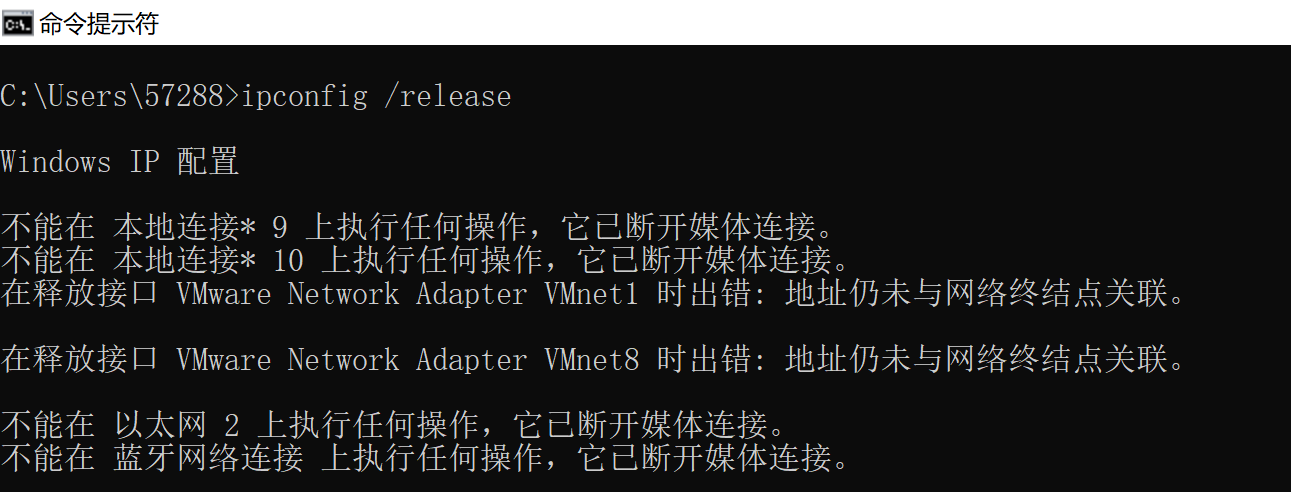
**四.实验步骤和协议分析**

**1. 捕获和分析 DHCP 报文**

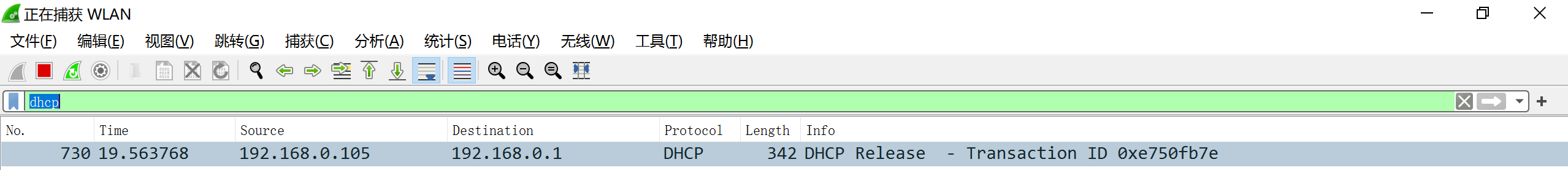
DHCP动态主机设置协议（Dynamic Host Configuration Protocol）是一个局域网的网络协议，使用UDP协议工作，主要有两个用途：给内部网络或网络服务供应商自动分配IP地址、给内部网络管理员作为对所有计算机作中央管理的手段。

DHCP数据报的捕获（申请IP地址时）：

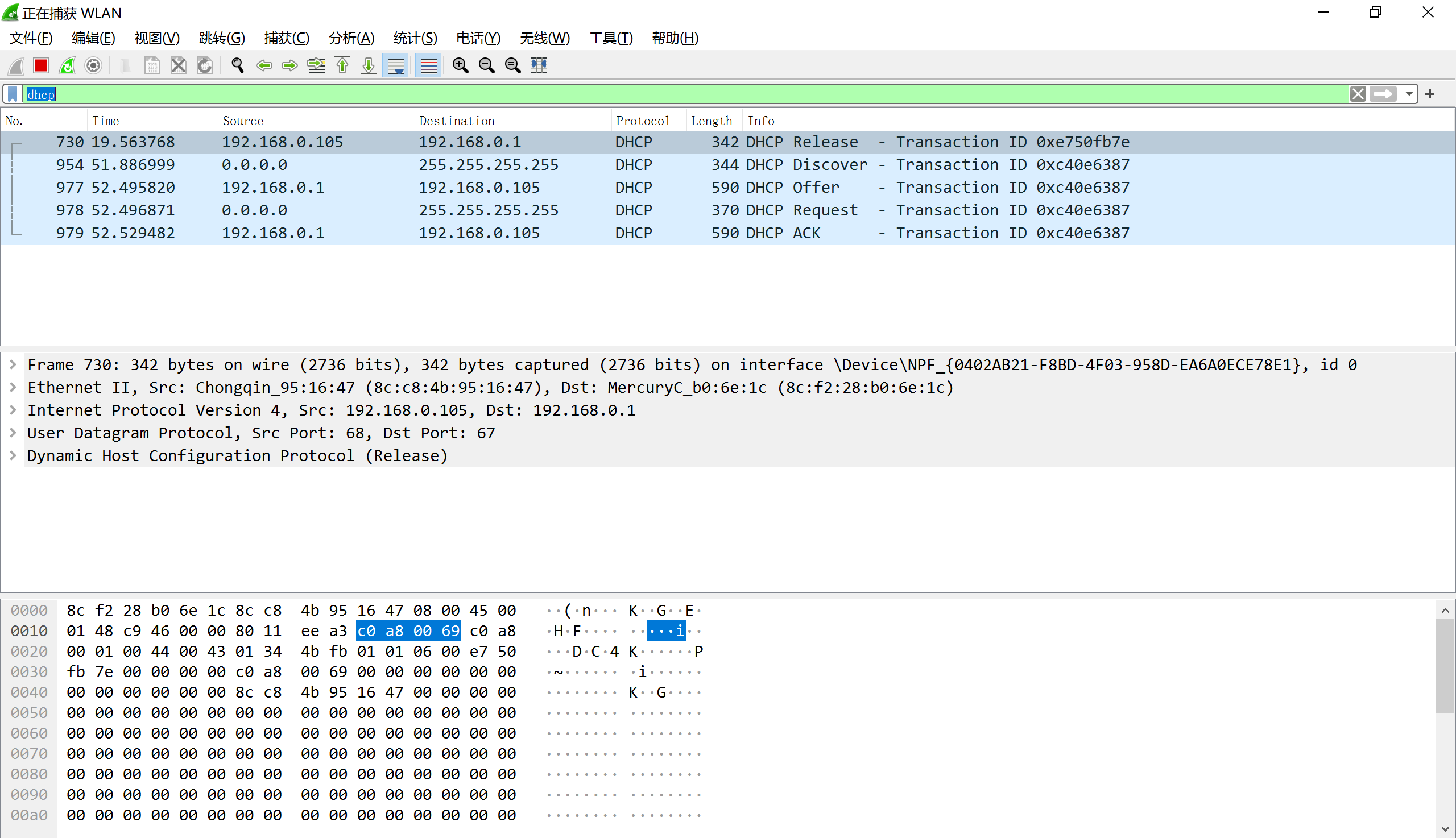
（1）在命令提示符窗口中输入ipconfig /release，释放已获取的IP地址：



在应用显示过滤器中输入dhcp，在Wireshark中看到了DHCP release的报文如下：



（2）在cmd继续输入ipconfig /renew，过滤出 DHCP 报文：

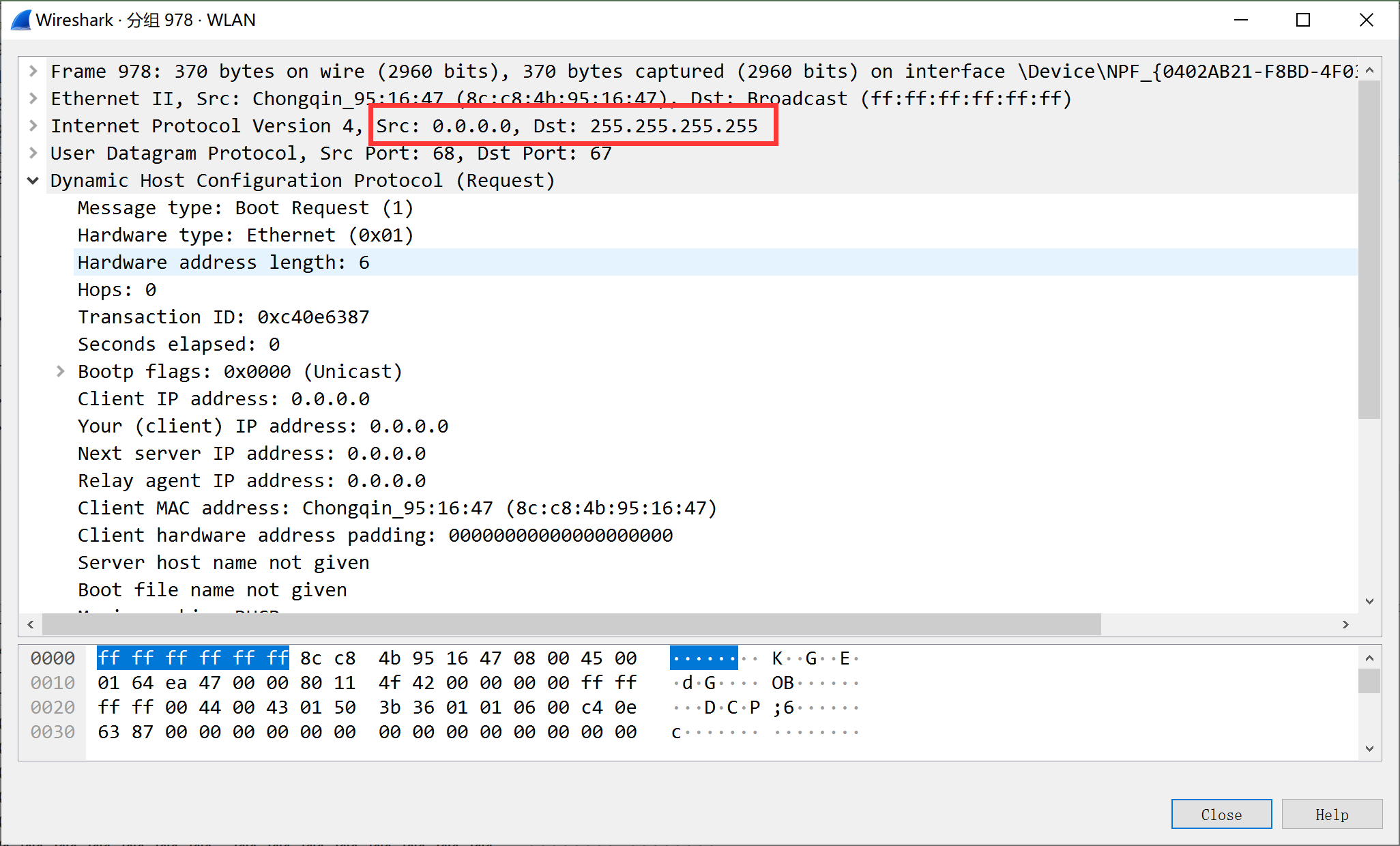


可以看到在连接过程中产生了DHCP Discover, DHCP Offer, DHCP Request和DHCP ACK数据报。

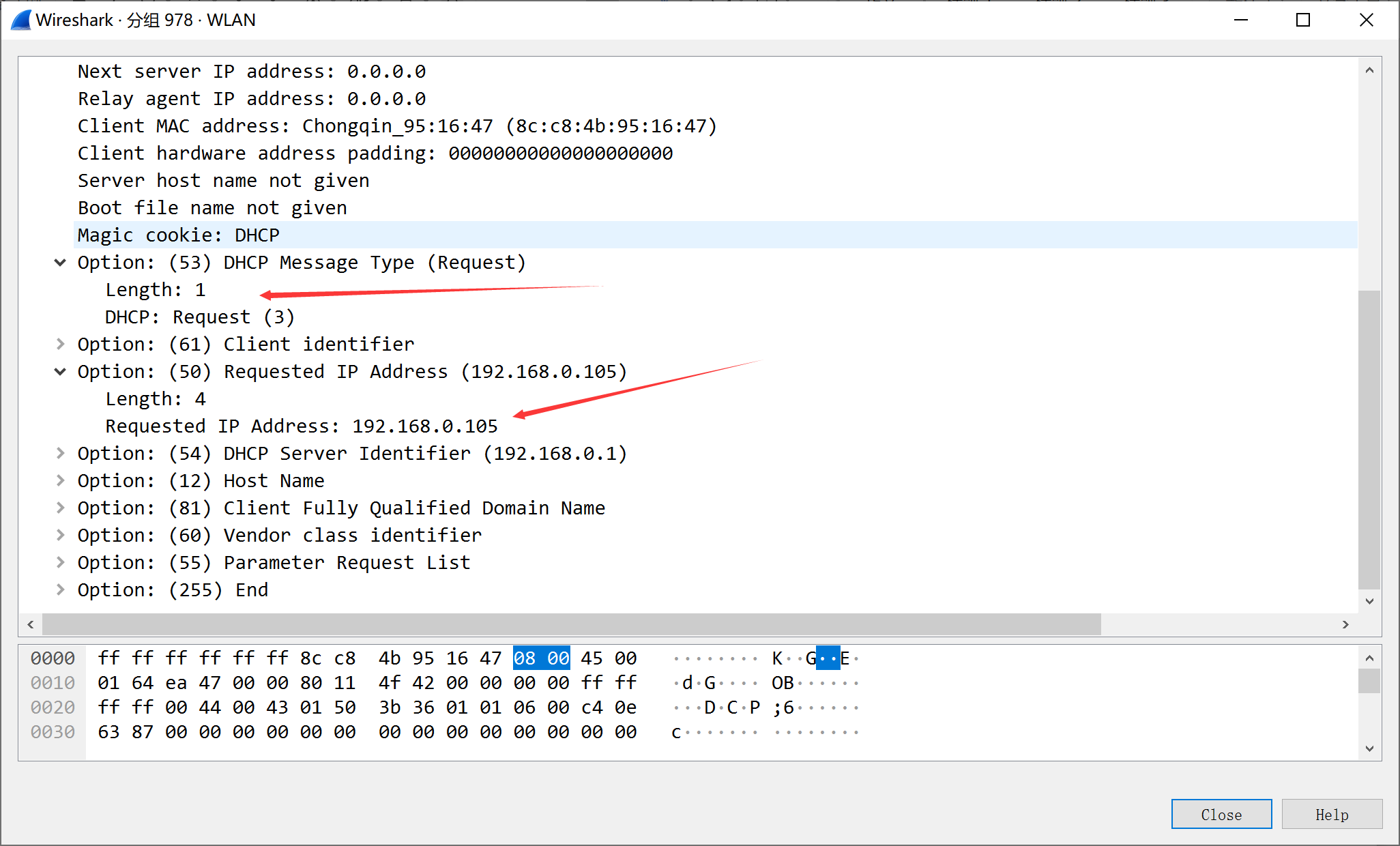
**DHCP分组：**

DHCP动态主机设置协议（Dynamic Host Configuration Protocol）是一个局域网的网络协议，使用UDP协议工作，主要有两个用途：给内部网络或网络服务供应商自动分配IP地址、给内部网络管理员作为对所有计算机作中央管理的手段。

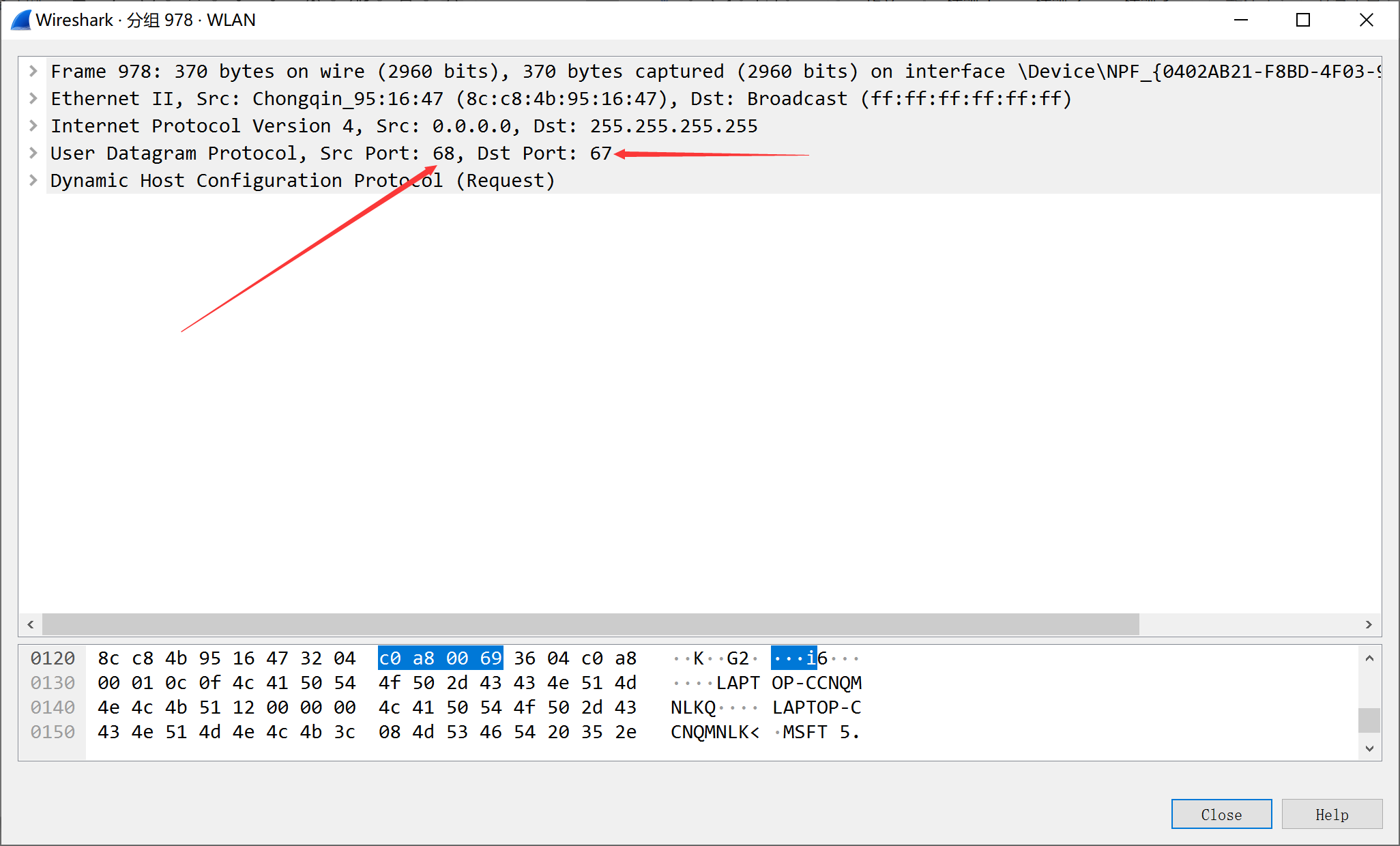
由捕获的数据包可见，其IP头部的目标地址为255.255.255.255，表明该包为一个广播包，同时可以看到其源地址为00 00 00 00。



由DHCP的数据包部分译码，可以发现DHCP Message Type域为1，说明是申请IP地址，以及其他信息，并且最终申请的IP地址为192.168.0.105。



此外，可以看到DHCP服务使用了UDP的67与68端口。其中客户端向68端口广播请求配置，而服务器向67端口广播回应请求。



多次对DHCP数据包的查看与分析后，可以发现DHCP服务动态申请IP地址的步骤：

（1）客户机请求IP（DHCP DISCOVER广播包）；

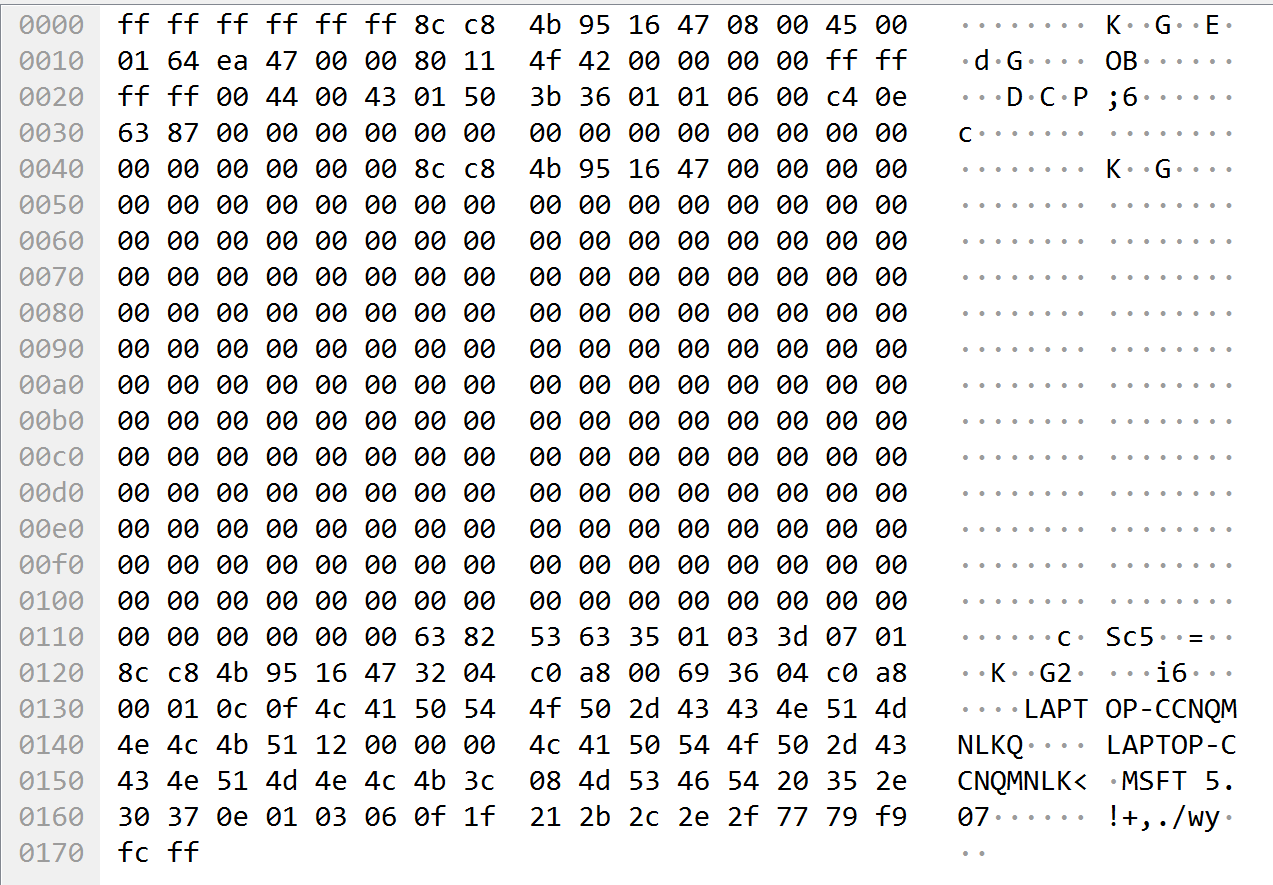
（2）Server响应（DHCP OFFER广播包）；

（3）客户机选择IP（DHCP REQUEST广播包）；

（4）Server确定租约（DHCP ACK/DHCP NAK广播包）。

**解析DHCP报文(分析request)**

本次实验捕获的一个IP数据分组如下所示：



IPv4协议下分组的首部各字段如下所示：



1.IP 报头

|  |  |  |
| --- | --- | --- |
| 单元的字节数 | **报文（16进制）** | 说明分析 |
| 14 | 略 | 以太网报头 |
| 1 | 45 | IP报头的开始  版本：0100，表示IPv4  首部长度：0101，表示首部共20字节（单位4 Byte） |
| 1 | 00 | 服务类型：未被使用 |
| 2 | 01 64 | 总长度，单位为字节,这里为 356 字节 |
| 2 | ea 47 | 标识，是一个计数器，用来产生数据报的标识 |
| 2 | 00 00 | 标志：前2比特有意义，这里为000；  低字段MF=0表示最后一片；中间段DF=0允许分片  片偏移：分片后在原分组中相对位置，8 Byte为单位，等于0无偏移 |
| 1 | 80 | 生存时间(TTL) |
| 1 | 11 | 数据报使用的UDP协议 |
| 2 | 4f 42 | 首部检验和 |
| 4 | 00 00 00 00 | 源地址：00.00.00.00 |
| 4 | ff ff ff ff | 目的地址：ff.ff.ff.ff |

2.UDP 数据报头

|  |  |  |
| --- | --- | --- |
| 单元的字节数 | **报文（16进制）** | 说明分析 |
| 2 | 00 44 | UDP报头的开始。 |
| 2 | 00 43 | 接收端计算机上 UDP 软件使用的端口,此处为67. |
| 2 | 01 50 | UDP 报头和数据的总长度 |
| 2 | 3b 36 | 校验和 |

3.UDP 数据报

|  |  |  |
| --- | --- | --- |
| 单元的字节数 | **报文（16进制）** | 说明分析 |
| 1 | 01 | 报文的操作类型,此处为1，表示请求报文。 |
| 1 | 01 | 通常为1，表示以太网的MAC地址。 |
| 1 | 06 | DHCP客户端的MAC地址长度 |
| 1 | 00 | 为0，表示没有经过中继 |
| 4 | c4 0e 63 87 | 请求标识：标识一次IP地址请求过程 |
| 2 | 00 00 | DHCP客户端从获取到IP地址或续约过程开始到现在的耗时,单位为秒，为0，表示未获得IP地址。 |
| 2 | 00 00 | 广播应答标识位，标识DHCP服务器应答报文是单播还是广播，此处首位为0，表示单播 |
| 4 | 00 00 00 00 | DHCP客户端的IP地址。仅在DHCP服务器发送的ACK报文中显示，其他报文中均显示0。 |
| 4 | 00 00 00 00 | DHCP服务器分配给客户端的IP地址，仅在DHCP服务器发送的Offer和 ACK报文中显示，其他报文中显示为0。 |
| 4 | 00 00 00 00 | 下个为DHCP客户端分配IP地址等信息的DHCP服务器IP地址，仅在 DHCP Offer、DHCP ACK报文中显示，其他报文中显示为0。 |
| 4 | 00 00 00 00 | DHCP客户端发出请求报文后经过的第一个DHCP中继的IP地址，若没经过DHCP中继，则显示为0。 |
| 16 | 8c c8 4b 95 16 47 后续均为零 | DHCP客户端的MAC地址，在每个报文中都会显示对应DHCP客户端的 MAC地址。后跟10字节的填充位，全部为0. |
| 64 | 均为0 | 为DHCP客户端分配IP地址的DHCP服务器名称（DNS域名格式），在 Offer和ACK报文中显示发送报文的DHCP服务器名称，其他报文显示为 0。 |
| 128 | 均为0 | DHCP服务器为DHCP客户端指定的启动配置文件名称及路径信息，仅在 DHCP Offer报文中显示，其他报文中显示为空。 |
| 4 | 63 82 53 63 | 后续可选字段的格式。 此处为为固定值0x63825363，表示DHCP格式。 |
| 略 | 略 | 可选字段 |

**2.捕获和分析 ICMP 报文**

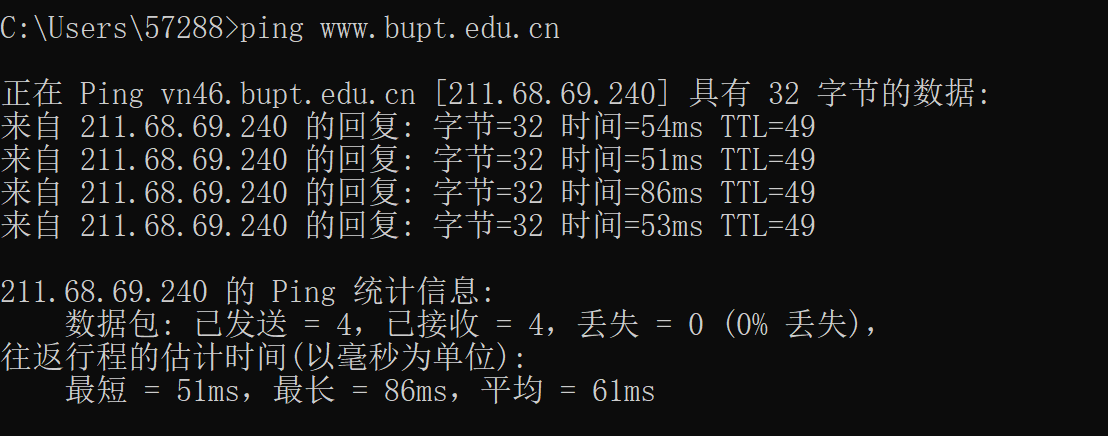
ICMP（Internet Control Message Protocol）是Internet控制报文协议。它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

ICMP数据报的捕获：

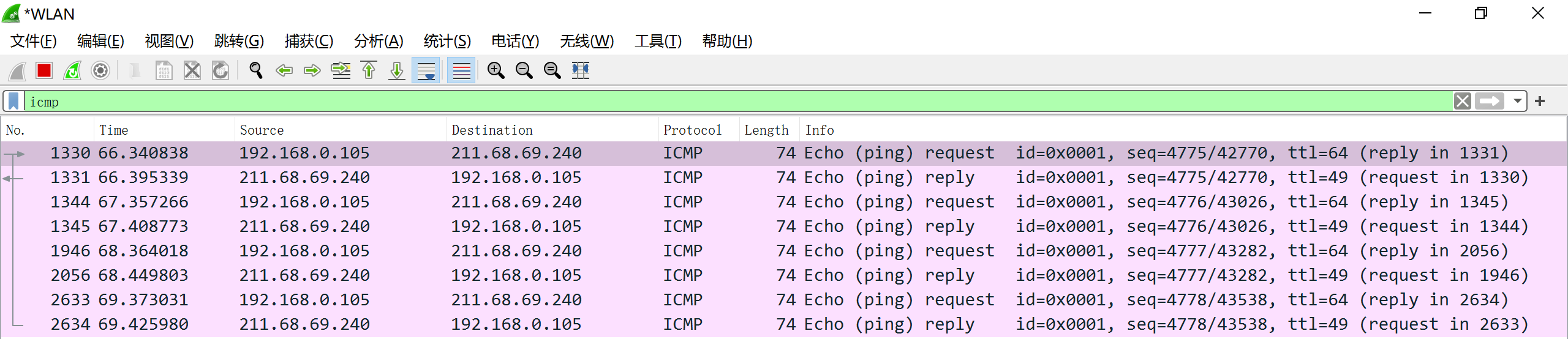
（1）在应用显示过滤器中输入icmp，过滤出ICMP报文



1. 打开cmd，输入ping www.bupt.edu.cn，回车执行

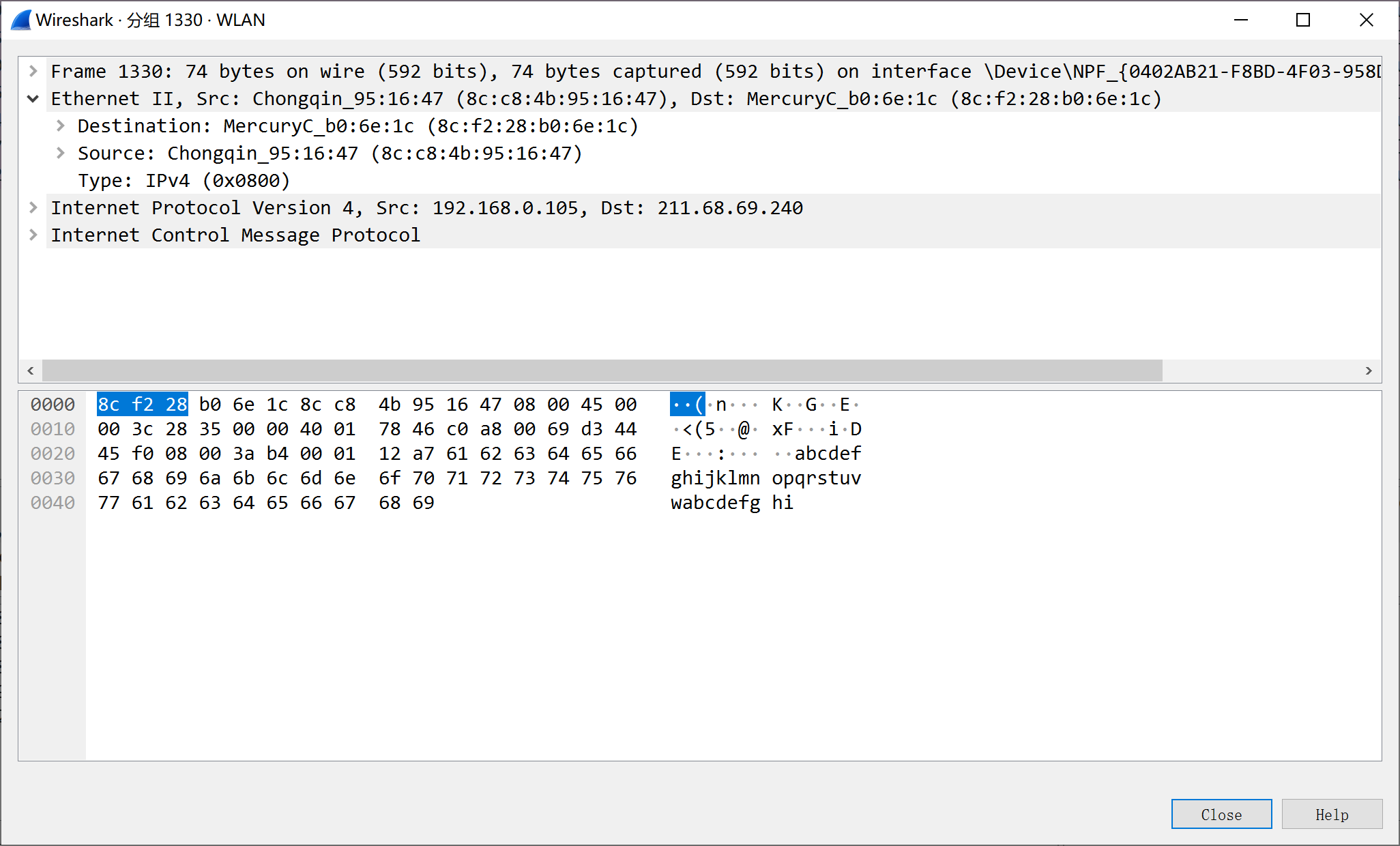


观察 Wireshark 捕获的数据报，系统默认 ping 四次，得到 8 个报文，4个为 request，4个为 reply：



解析ICMP报文（分析 request）

下图为其中一次的报文：



IP 数据报格式如下：

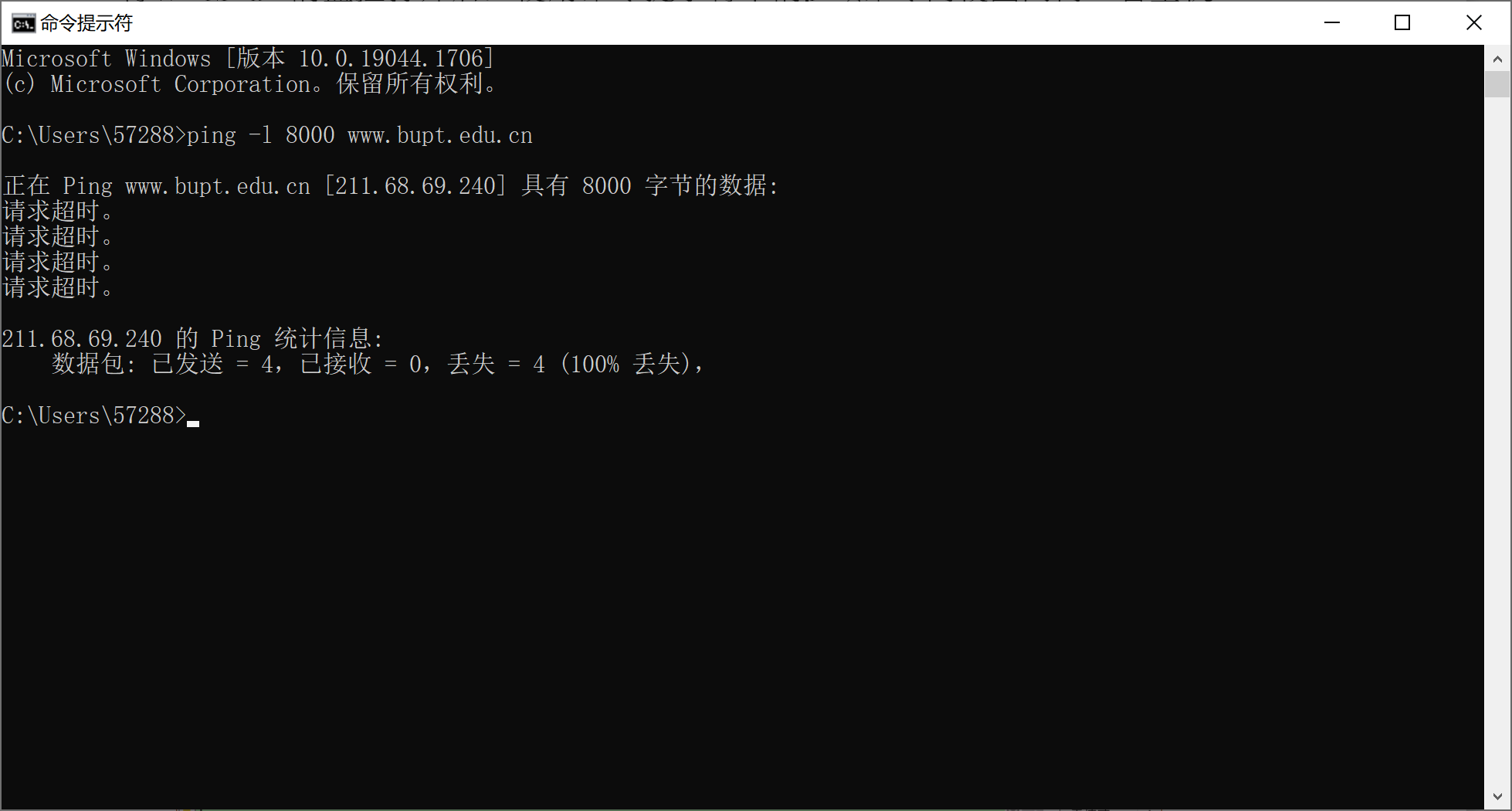


IP 报头

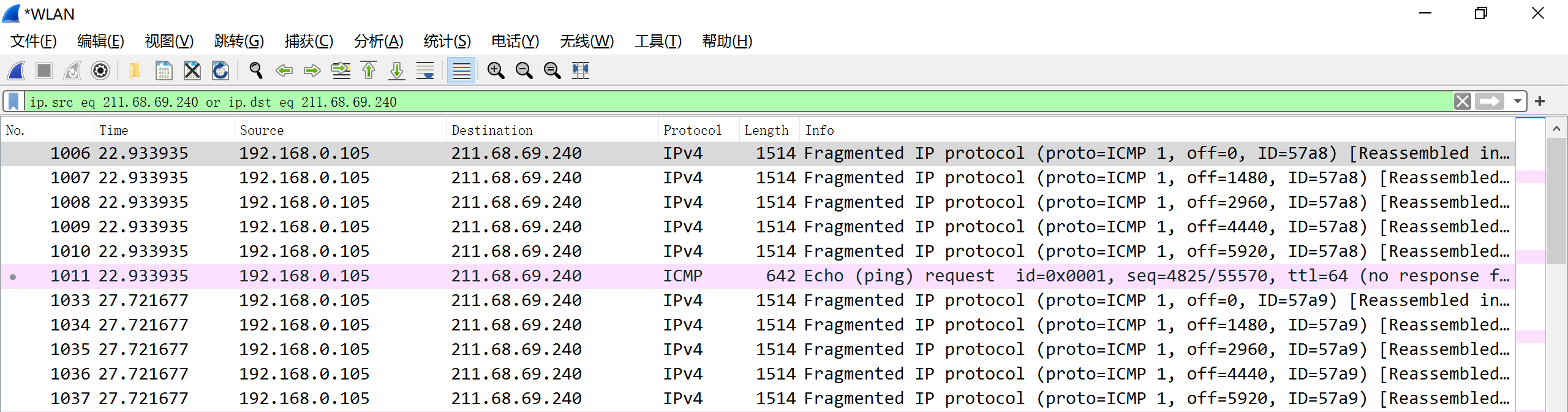
|  |  |  |
| --- | --- | --- |
| 单元的字节数 | **报文（16进制）** | 说明分析 |
| 14 | 略 | 以太网报头 |
| 1 | 45 | IP报头的开始  版本：0100，表示IPv4  首部长度：0101，表示首部共20字节（单位4 Byte） |
| 1 | 00 | 服务类型：未被使用 |
| 2 | 00 3c | 总长度，单位为字节,这里为 60 字节 |
| 2 | 28 35 | 标识，是一个计数器，用来产生数据报的标识 |
| 2 | 00 00 | 标志：前2比特有意义，这里为000；  低字段MF=0表示最后一片；中间段DF=0允许分片  片偏移：分片后在原分组中相对位置，8 Byte为单位，等于0无偏移 |
| 1 | 40 | 生存时间(TTL) |
| 1 | 01 | 数据报使用的UDP协议 |
| 2 | 78 46 | 首部检验和 |
| 4 | c0 a8 00 69 | 源地址：192.168.0.105 |
| 4 | d3 44 45 f0 | 目的地址：211.68.69.240 |

**3.IP 包的分段功能的分析**

将WireShark的监控打开后，使用命令提示符中的ping命令向www.bupt.edu.cn发送大小为8000字节的分组，如下图：

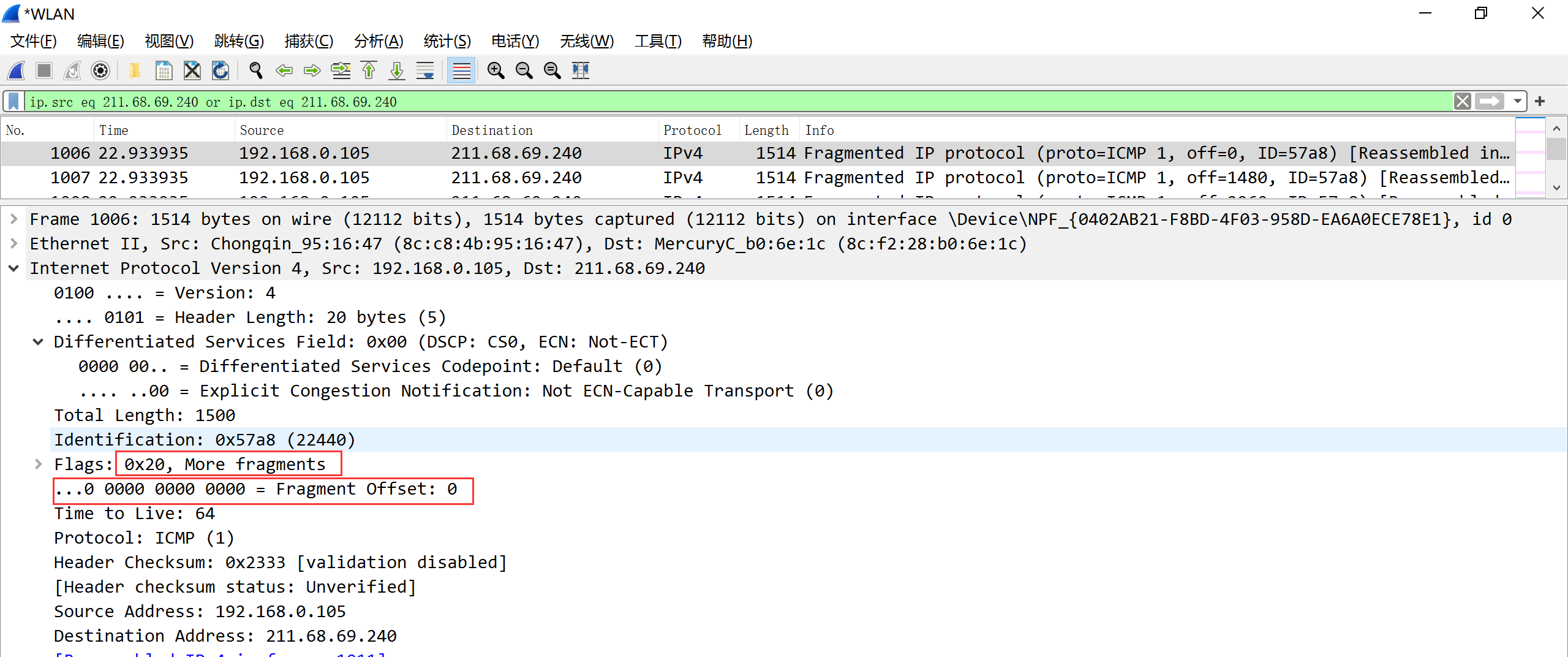


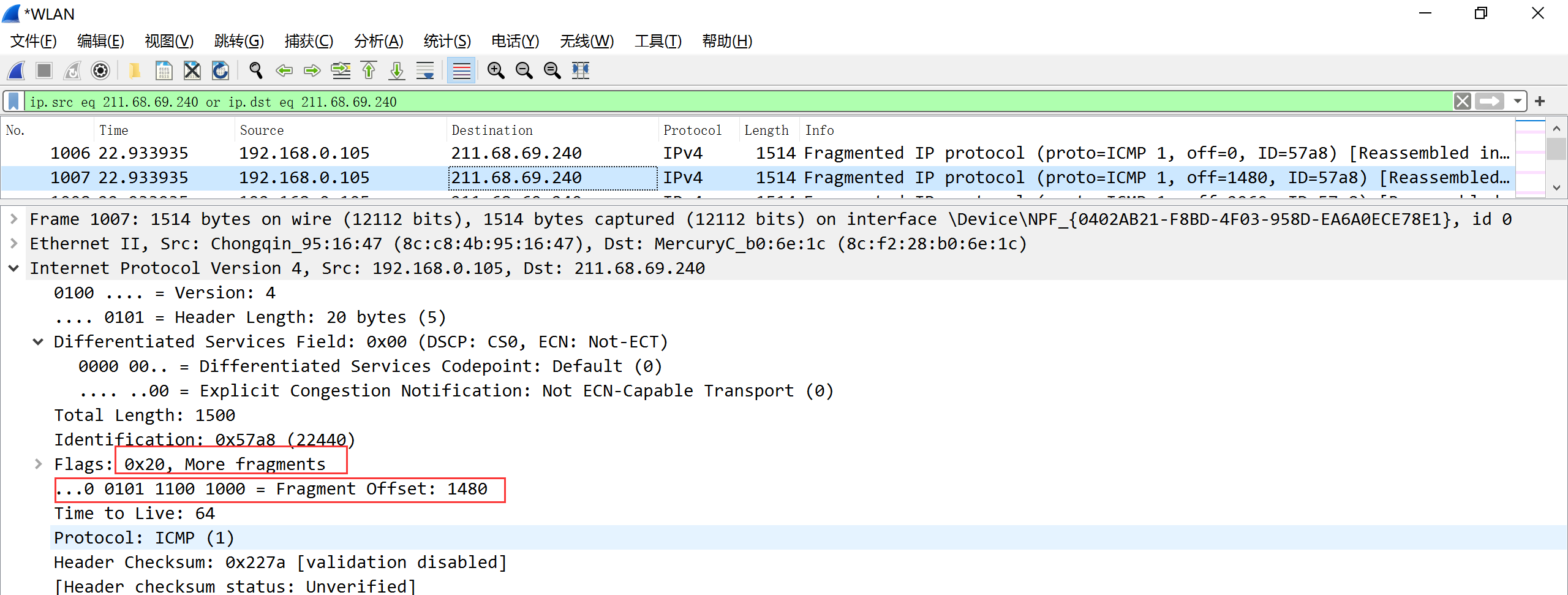
打开Wireshark，开启抓包，在过滤器一栏输入 ip.src eq 211.68.69.240 or ip.dst eq 211.68.69.240，用来过滤IP。

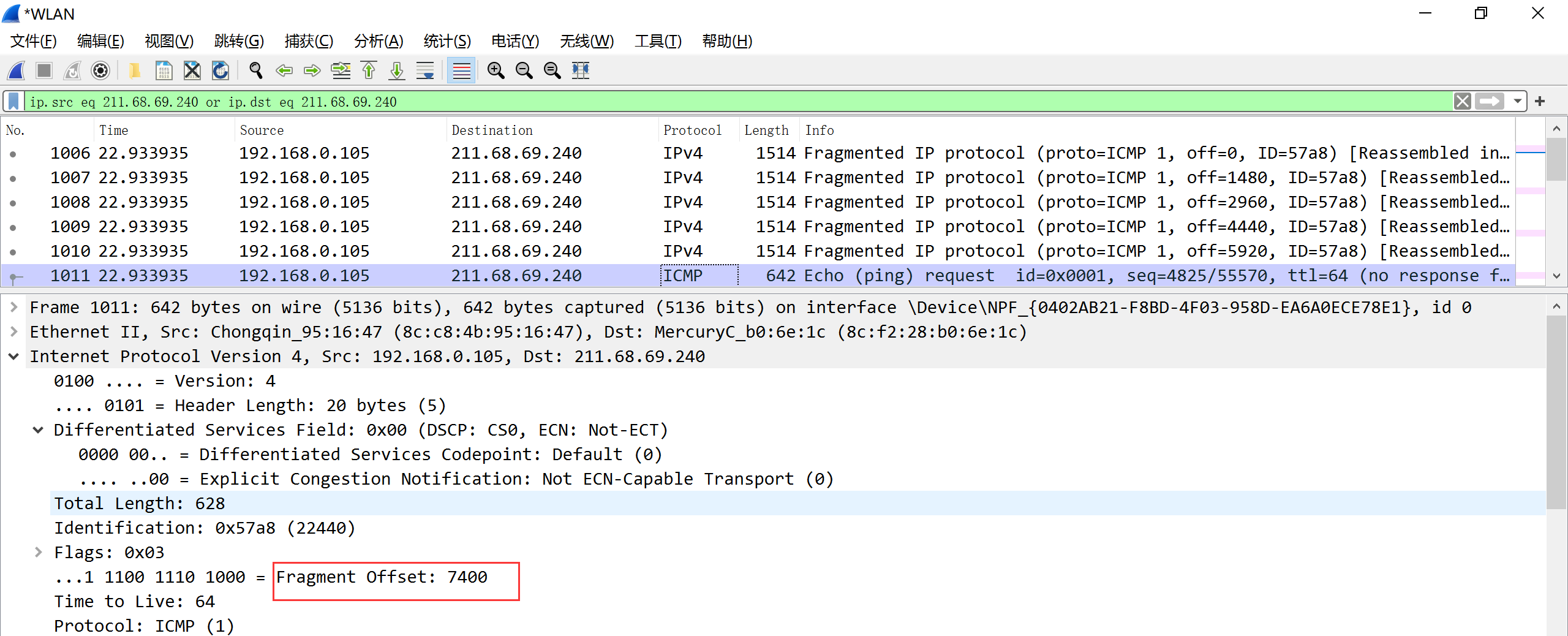


分片传输的分组结构分析如下：

仅展示前2个报文和ICMP报文：







分析如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 分片编号 （按时间戳从早到晚） | 协议类型 | DF标志位 | MF标志位 | 分片偏移(Fragment Offset) |
| 1 | IP | 0 | 1 | 0 |
| 2 | IP | 0 | 1 | 1480 |
| 3 | IP | 0 | 1 | 2960 |
| 4 | IP | 0 | 1 | 4440 |
| 5 | IP | 0 | 1 | 5920 |
| 6 | ICMP | 0 | 0 | 7400 |

（1）因为最后一个分片携带了ICMP报文，所以其被Wireshark识别为ICMP协议，对照其他几个分片，验证了 ICMP 协议属于 IP 协议

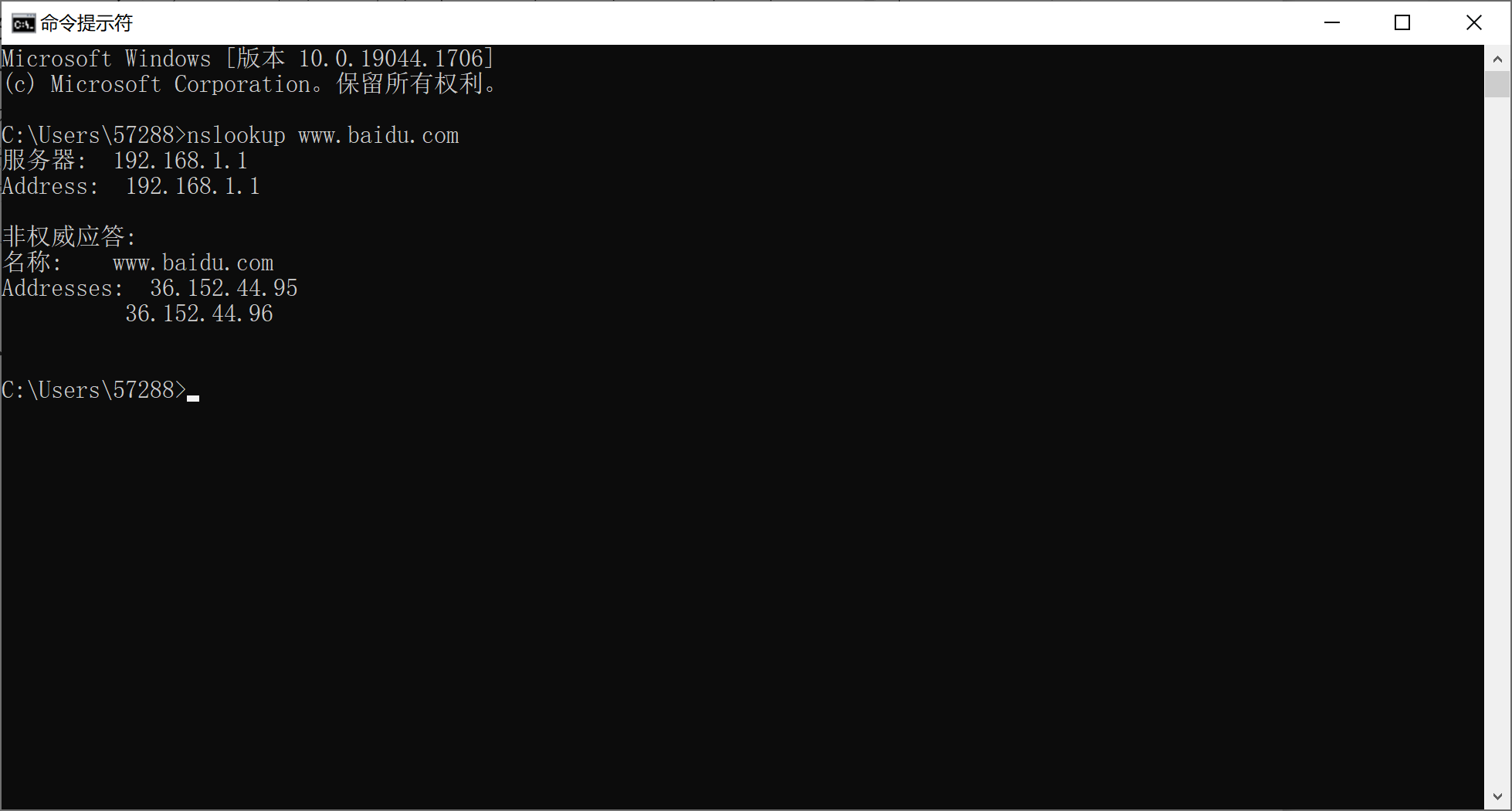
（2）DF(Don’t Fragment)字段=1时不允许分片，等于0时允许。一般设置为0；MF(More Fragment)字段=1，表示后面“还有分片”；等于0 表示最后一个分片。路由器或主机收到分片时检查该字段，若收齐了全部分片就还原IP分组。前5个数据包中的MF位均为1，而第6个数据包的MF位为0，这代表前5个数据包的后面均还存在同一组的数据包，而第六个数据包则为最后一个数据包；

（3）以太网的最大数据部分长度为1500字节，因此发送总长度为8000字节的数据报是必须要经过分片的。上述的1480字节加上对应IP数据包长达20字节的首部恰好为1500字节，符合预期。

（4）IP数据报头的分片偏移字段为该分片的首字节在原IP数据报中的偏移量

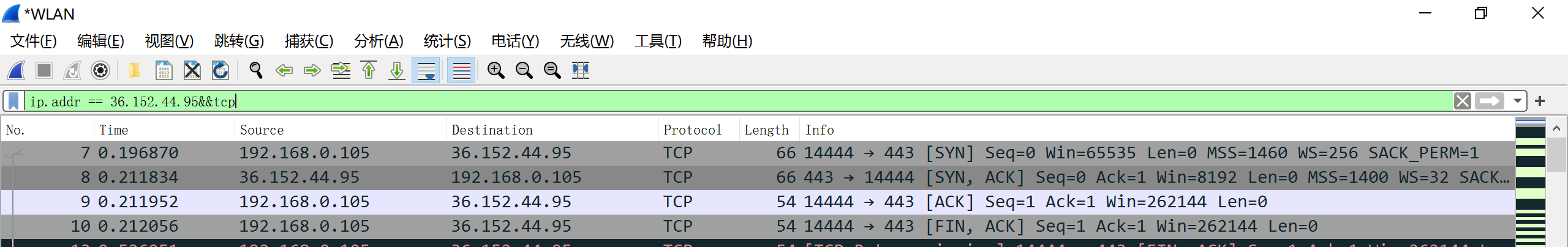
**4.TCP 建立连接和释放连接的分析**

在cmd窗口输入ookup www.baidu.com，可以查看到其IP地址：36.152.44.96：

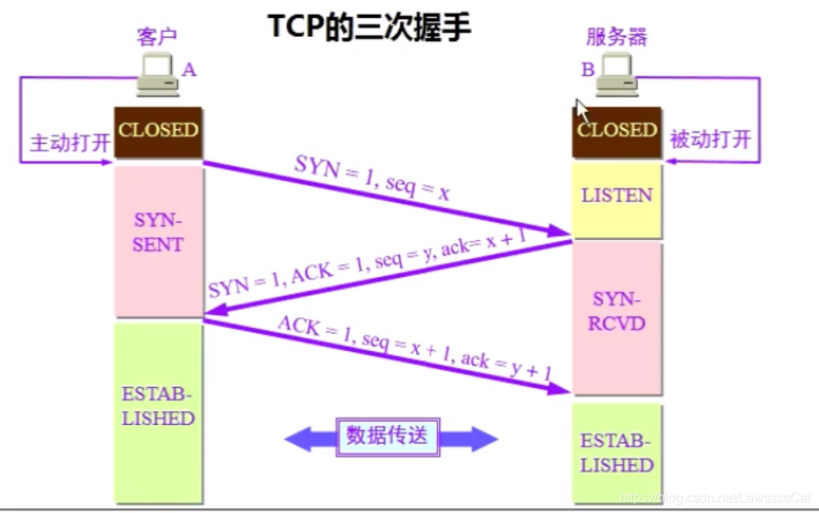


开启 wireshark 监控，打开www.baidu.com，停止监控。

在显示过滤器输入ip.addr==36.152.44.96&&tcp，如下图：

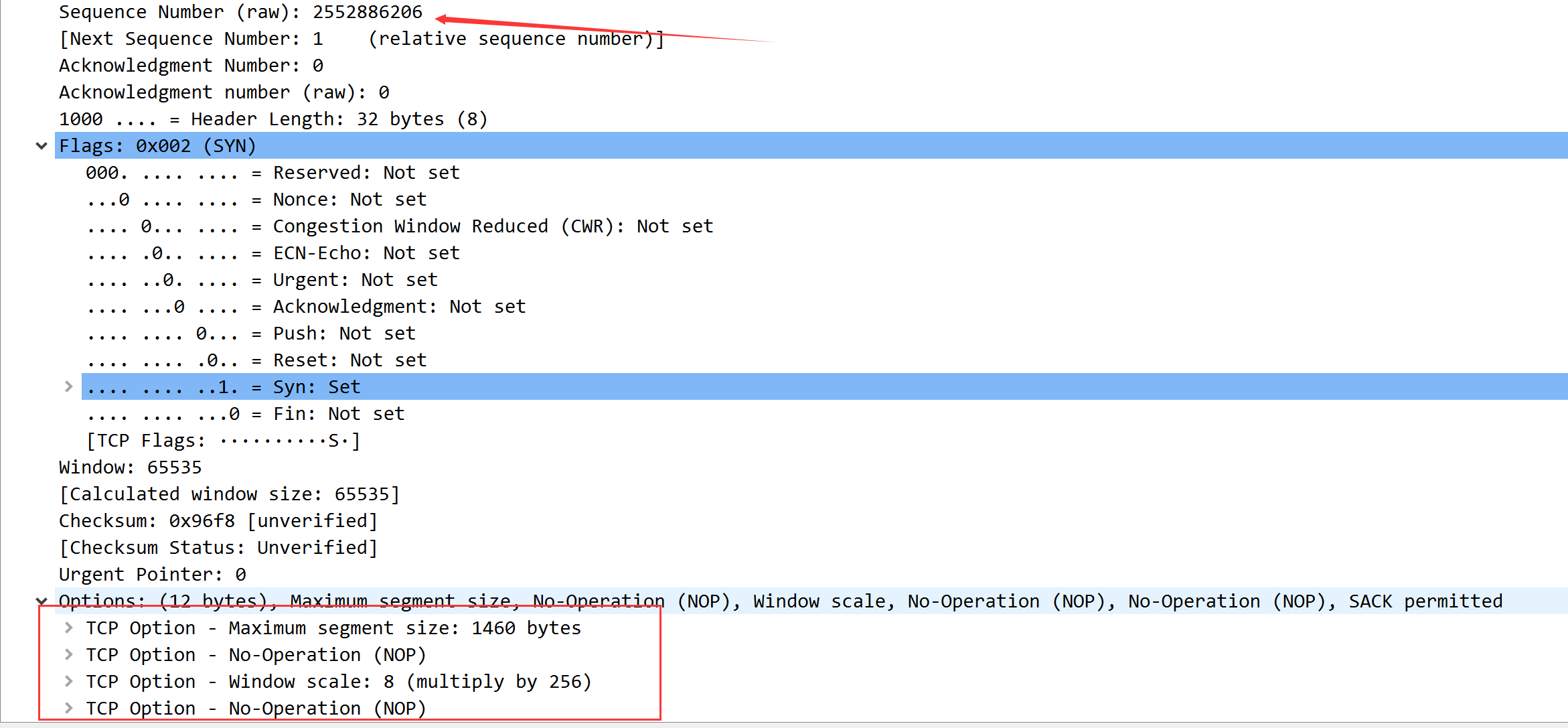


分析TCP三次握手：



第一次握手 [SYN]：

客户端：“请求连接”（syn）

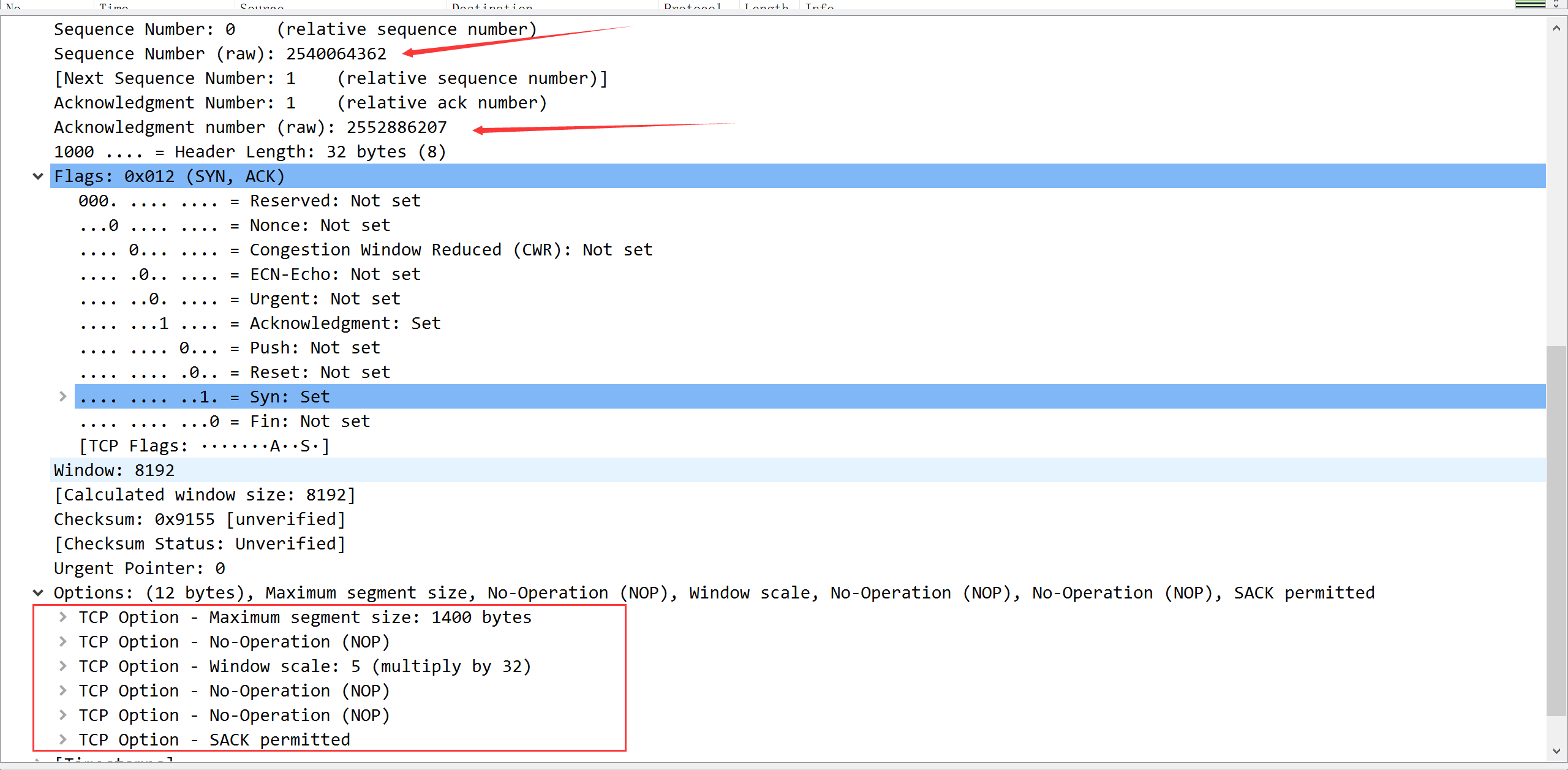


第二次握手 [SYN, ACK]：

服务端：收到（ack）

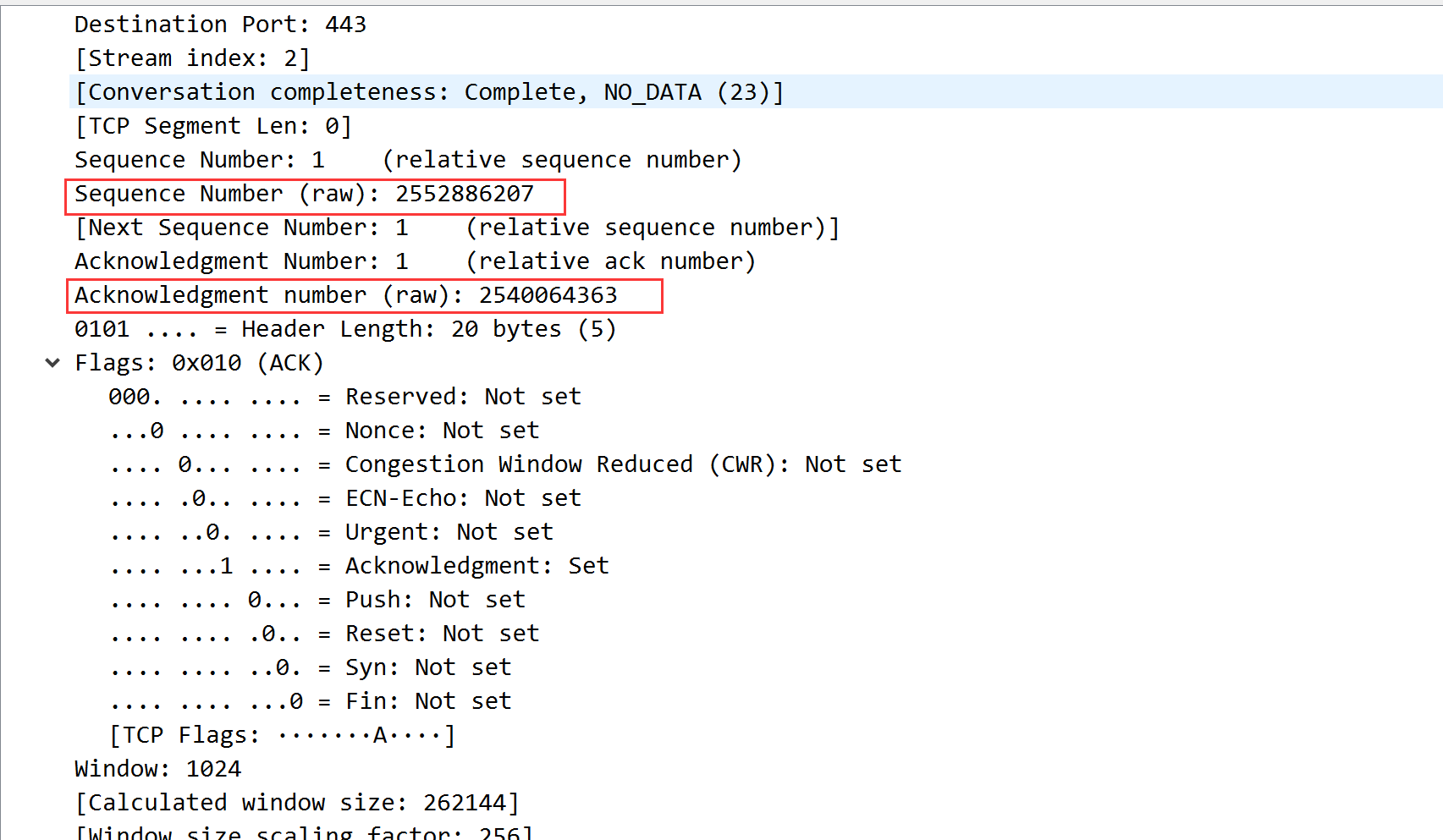
服务端：同意建立连接（syn）

和第一次握手对比。服务端发起的报文中，有自己新生成的 seq num，且ack num 为第一次报文的seq num 加一。



第三次握手 [ACK]

客户端：“收到，已开启连接”（ack）



**五．实验总结**

本次实验的进展不是十分顺利，我从实验开始至实验报告大致完成共花费了7个小时，但本次实验的收获也是较为丰富的。经过本次实验，对诸多协议有了更加深刻的理解，对TCP的三次握手及可靠传输机制也有了更深的认识。