计算机网络实验二

网络层数据分组的捕获和解析

班级：2011211319 姓名：蒋雪枫 学号 ：2017211319

1、实验类别

协议分析型

2、实验内容和实验目的

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。

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，理解长度大于 1500 字节 IP 数据组分片传输的结构。

3、实验设备环境

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

4、实验过程：

1. 捕获 DHCP 报文：

首先在 CMD 中使用 ipconfig /release 断开链接，这时再使用 ipconfig /renew 重新建立链接等待获取一个 ip 地址，这时候在 WireShark 里面采用 udp.port==68 进行过滤，发现能够收到一系列 DHCP 包，我们对其中一个进行分析。

注：如果不这么做，很有可能看不见 DHCP，而只能看见 DHCPv6

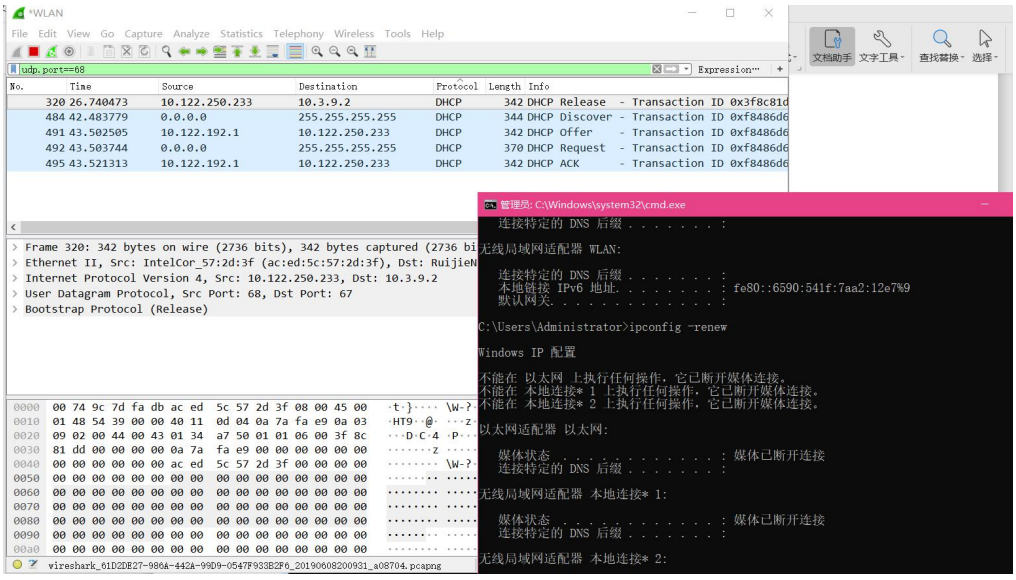

图 1 DHCP 捕获

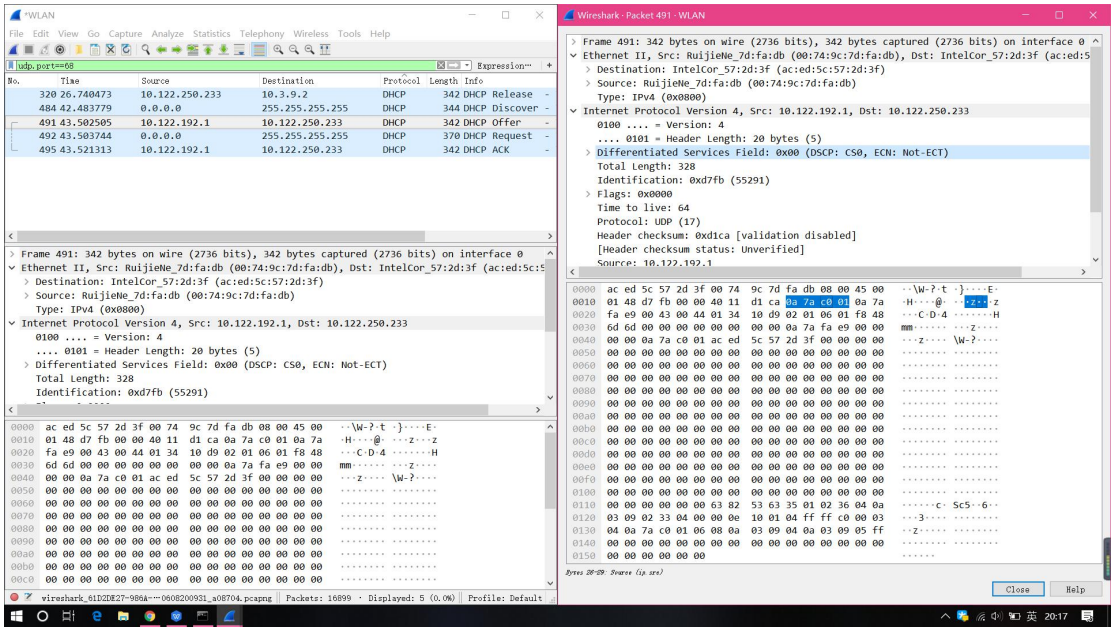

图 2 DHCP 分析 1

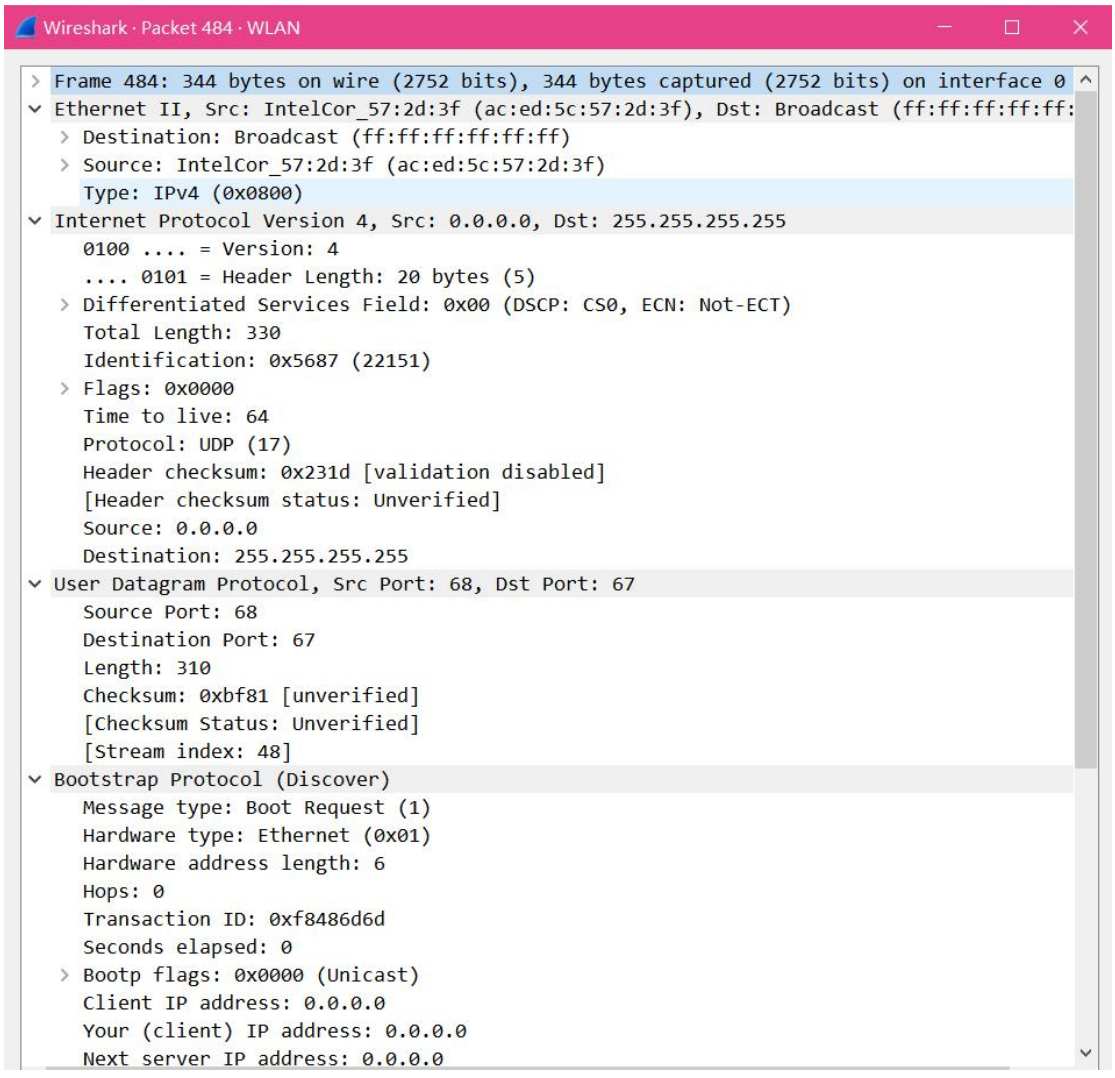

图 3 DHCP 字段

2、捕获 IP 数据包，进行分析

图 4 上知乎网

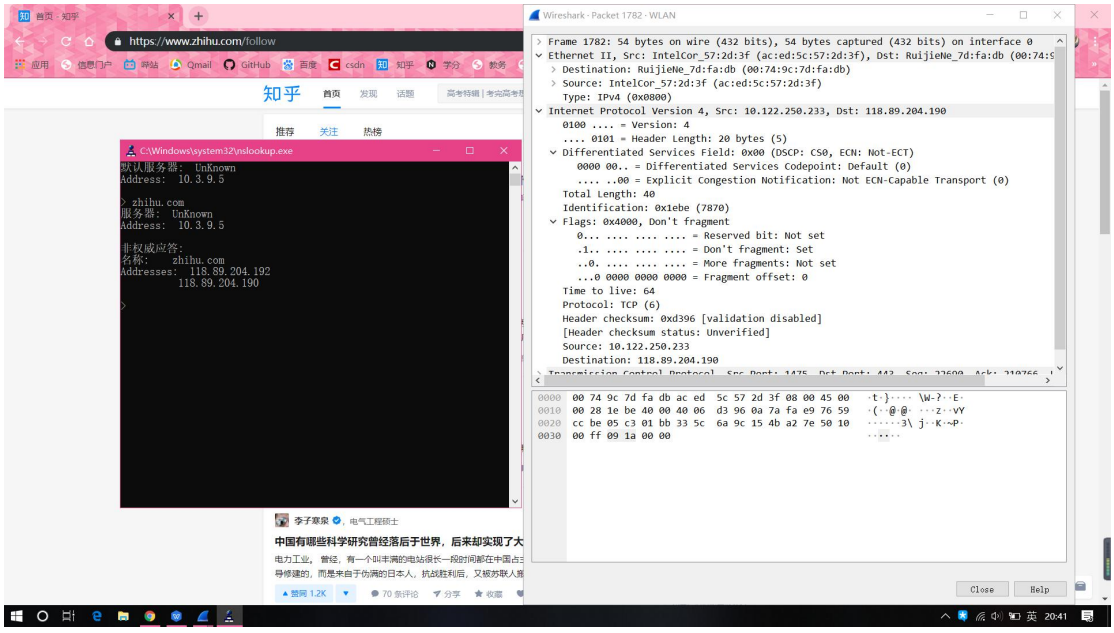

图 5 获取知乎网相关的数据报，进行字段分析

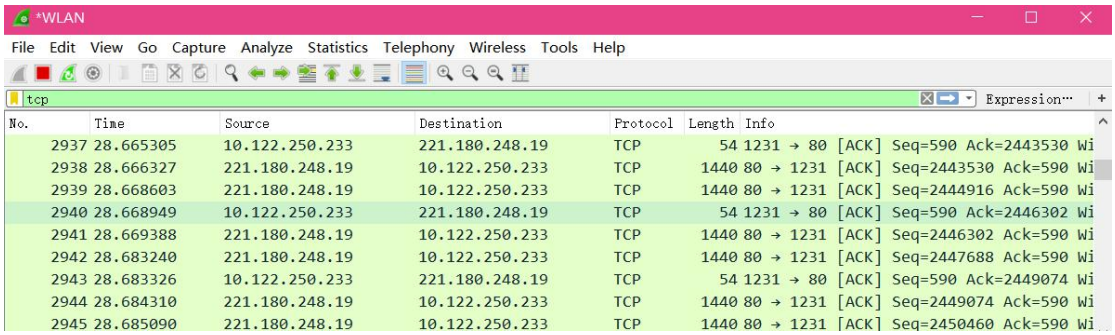

图 6 一系列 IP 数据报

图 7 一般的 IPV4 数据报字段模式

对于知乎网相关报文，首部分析如下：

字段	报文	内容
包头长度	45 H	包头长 20 字节（5*4，版本号 ipv4）
服务类型	00 H	正常时延，正常吞吐量，正常可靠性
总长度	0028 H	数据分组长度为 2*16+8=40 字节
标识	1ebe H	标识为 1ebe(H)
标志	010(3bit)	DF=1，MF=0，表示不分片
片偏移	0H(13bit)	偏移量为 0
生存周期	40H	每跳生存时间为 64s,TTL,time to live
协议	06 H	协议为 TCP（6）
头部校验和	d396 H	头部校验和 d396 (H)
源地址	0a7afae9 H	10.122.250.233(本地 ip)
目的地址	7659ccbe H	118.89.204.190(远程 ip)

3.分析上网流程：

通过连接网络的过程，之后分析连接后有哪些数据包即可了解上网的过程。可以发现在断开网络的时候，可以捕获到 DHCP Release 分组用于断开网络，局域网重新连接，与此同时，捕获到 DHCP ACK 分组用于网络的重连。

具体步骤：

1.使用 cmd 切断无线网络连接。

2.同时 Wireshark 捕获到 DHCP Release 用于断开网络。

3.使用 cmd 重新连接网络

4.Wireshark 捕获到 DHCP ACK 用于网络的重连：

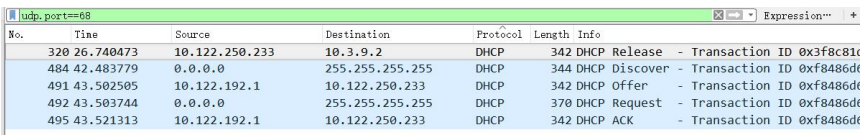

图 8 DHCP 相关包

4.ICMP 报文解析:

图 9 ICMP 内容字段模式

分析 ICMP 分组:

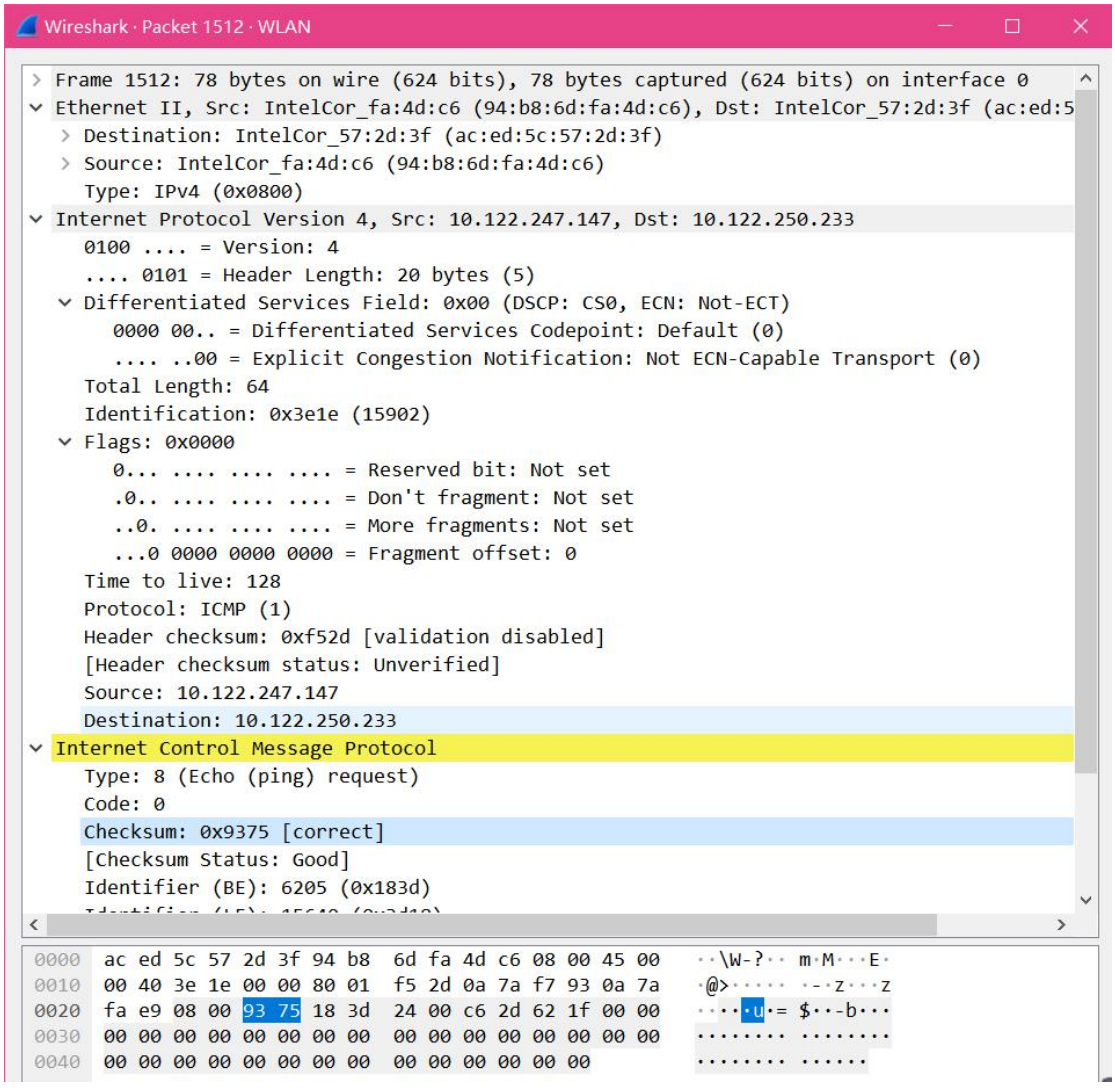

图 10 ICMP 字段捕获

字段	报文	内容
类型	08 H	问一台机器是否仍处于活动状态
代码	00 H	
校验和	9375 H	校验和为 9375 H

（5）制作一个 8000 字节的 IP 数据分组，发送后捕获分析。由于分组长度大于 1500 字节，因此需要分片传输。按照 2）中的方法分析所有分片的结构。

通过 cmd 向网关发送 8000 字节的数据。

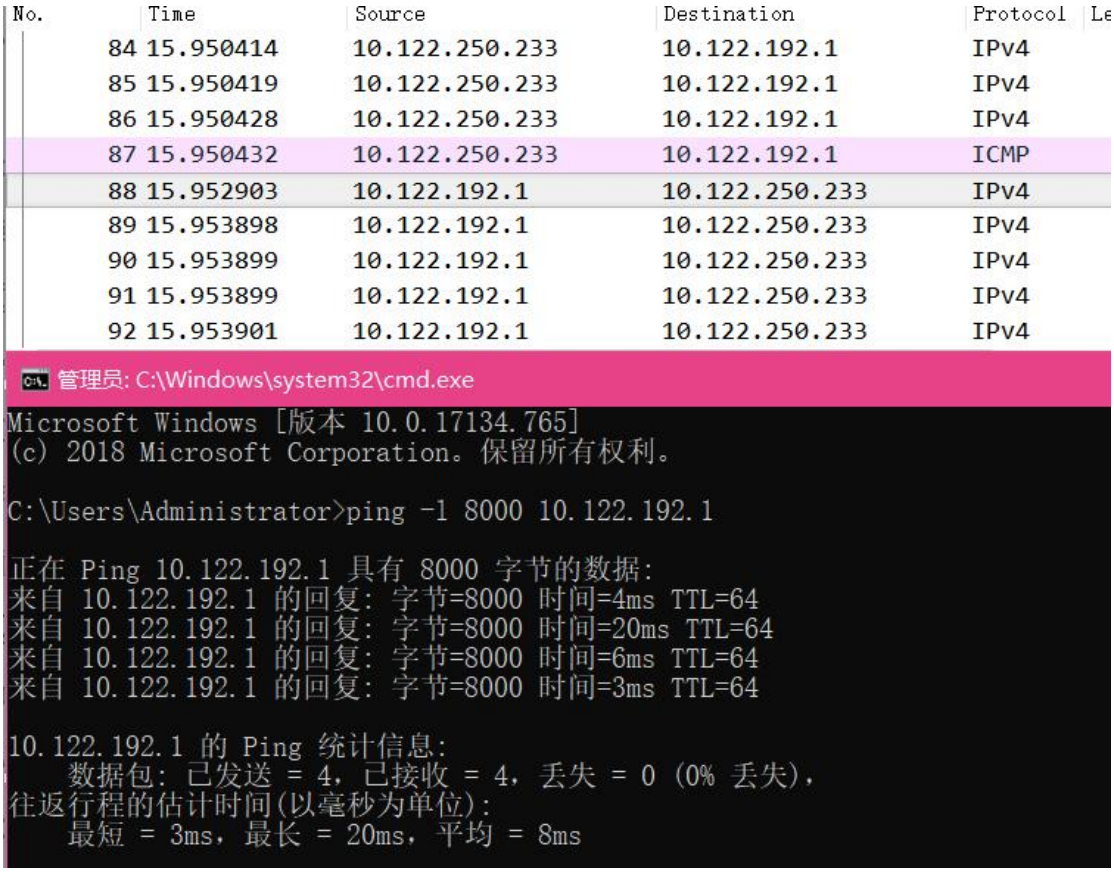

图 11 给默认网关发送 8000 字节数据

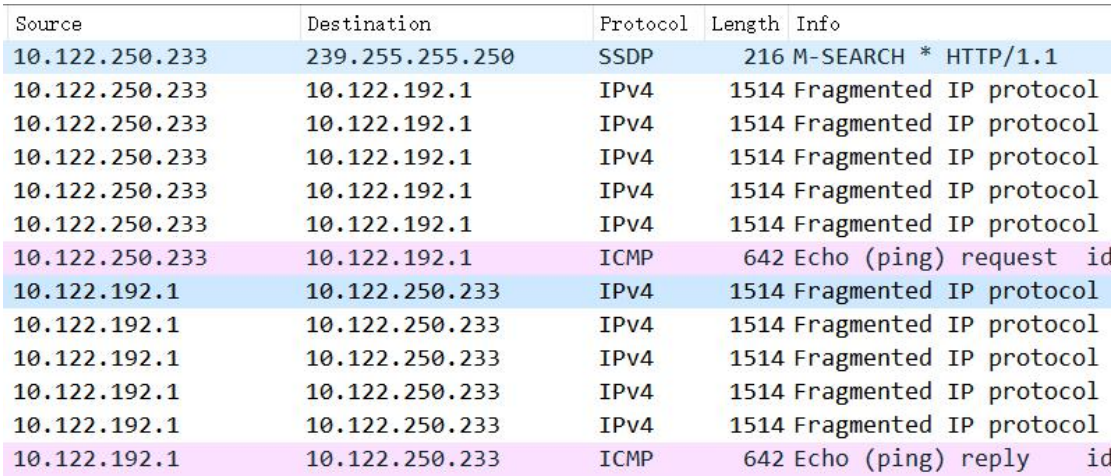

图 12 分析这 8000 字节信息走向

结论分析：

上面为发送给默认网关的所有数据包的分片的分析，5 个长度为 1500 字节的 IP 分组，每个分组的净荷域=1500-20=1480，最后一个分组为 628，要减去头部 20 字节和 icmp 的 8 字节，故前五个分组组装起来为 1480*5=7400。加上最后一个分片，其总长度为 7400+600=8000，结果正确。

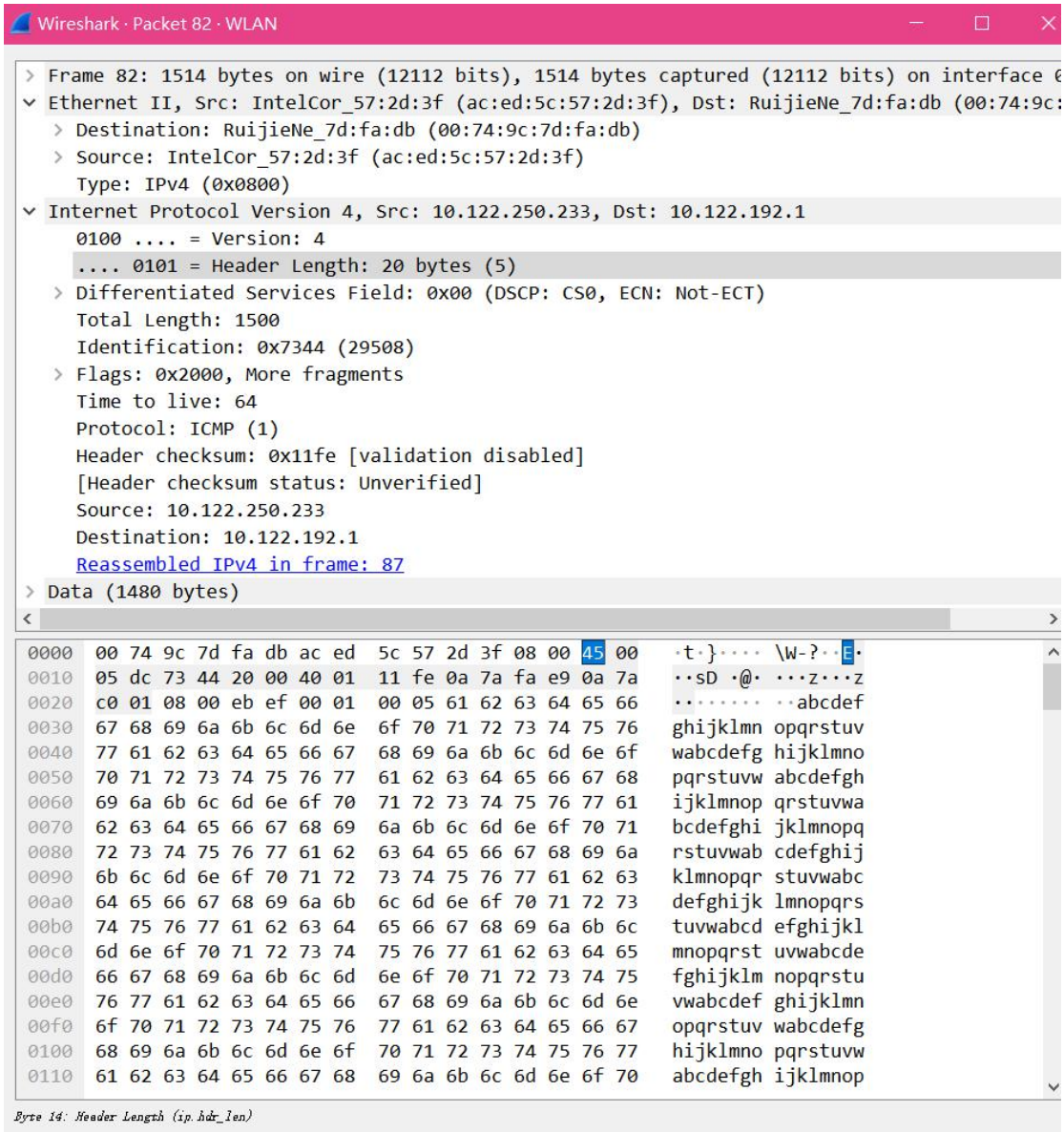

图 13 第一个 Fraction 的字段，具体内容在实验 2 已完成，不予赘述

5、实验结论和实验心得：

做实验的时间基本为预期中的 2 个小时内，完成了实验要求的内容。在写完了计网大作业--DNS 中继服务器之后，其实对 Wireshark 的使用可以说掌握得很不错了。在做第一个捕捉 DHCP 分组时，由于最开始想要偷懒就没有禁用网卡，但发现这样无法捕获 DHCP 报只能出现 DHCPv6 报。同时我也更会使用 Wireshark 的 filter 工具了。之后的第二个实验在寻找 ip 分组的过程，通过结合 Nslookup 和浏览特定网站的办法寻找了一个合适的 ip 分组。在第三个实验需要结合第一个实验的思路，完整地理解你是如何被分配到一个 ip，之后又是如何上网的(在断开网络的时候，可以捕获到 DHCP Release 分组用于断开网络，局域网重新连接，与此同时，捕获到 DHCP ACK 分组用于网络的重连)。第四个和第五个实验与前面的思路相似，只是依葫芦画瓢，完成比较顺利。

总之，最有收获的还是一步步对报文进行分析，完成相关参数表的填写。

通过这次实验，我对网络层的概念有了更深层次的理解，同时也对计算机连接校园网的机制更加清晰，也更加熟练得使用 WireShark 工具。之前只是停留于课本，而未实践过，所以比较概念化，没有真正的理解网络的内涵，虽通过本次实验也只是了解有限，但是我还是对网络层有了更加深刻的认识，希望以后能更好的运用所学的内容完成其他工作。