计算机网络第二次实验

网络层数据分组的捕获和解析

班级：2014211302

姓名： 周尧棋

学号：2014211168

**1、实验类别**

协议分析

**2****、实验内容和实验目的**

本次实验内容：

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。

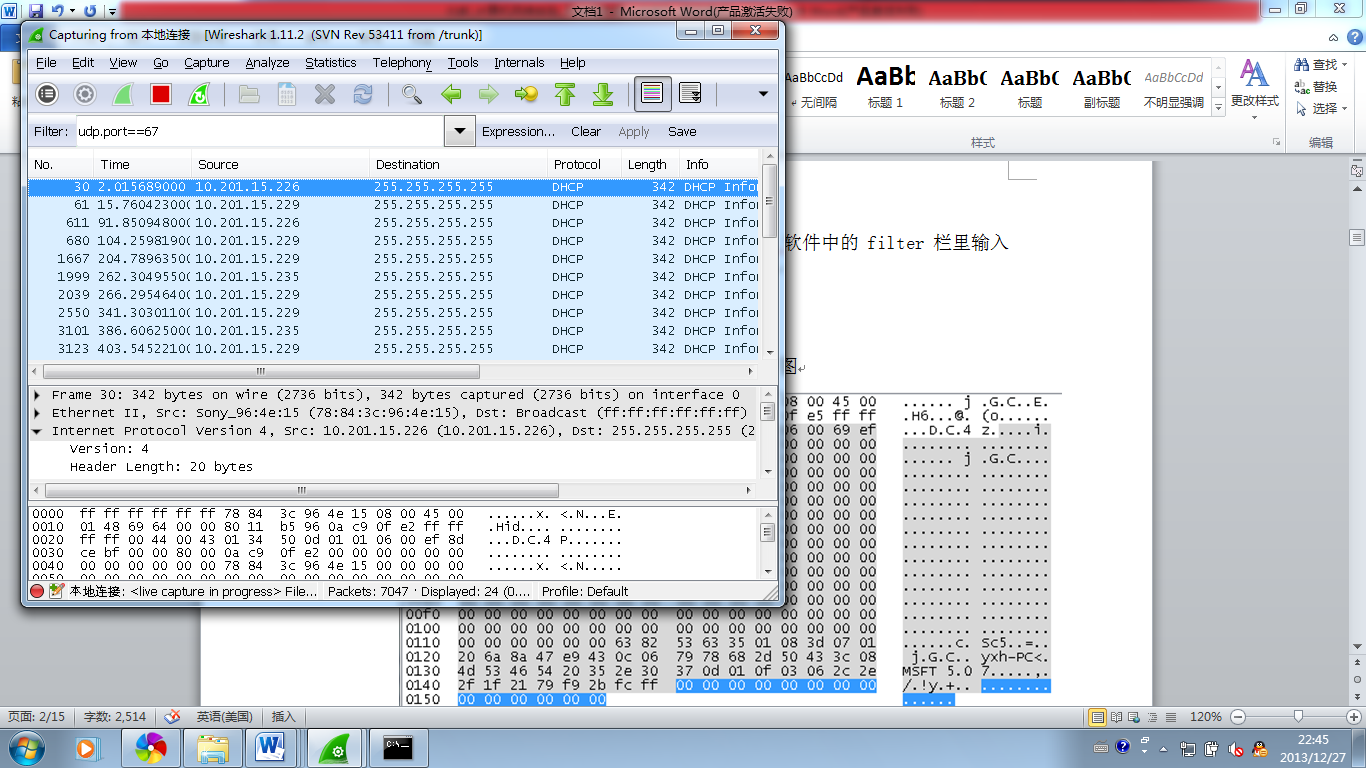
通过本次实验了解计算机上网的工作过程，学习各种网络层分组的格式及其作用，理解长度大于1500 字节IP 数据组分片传输的结构。

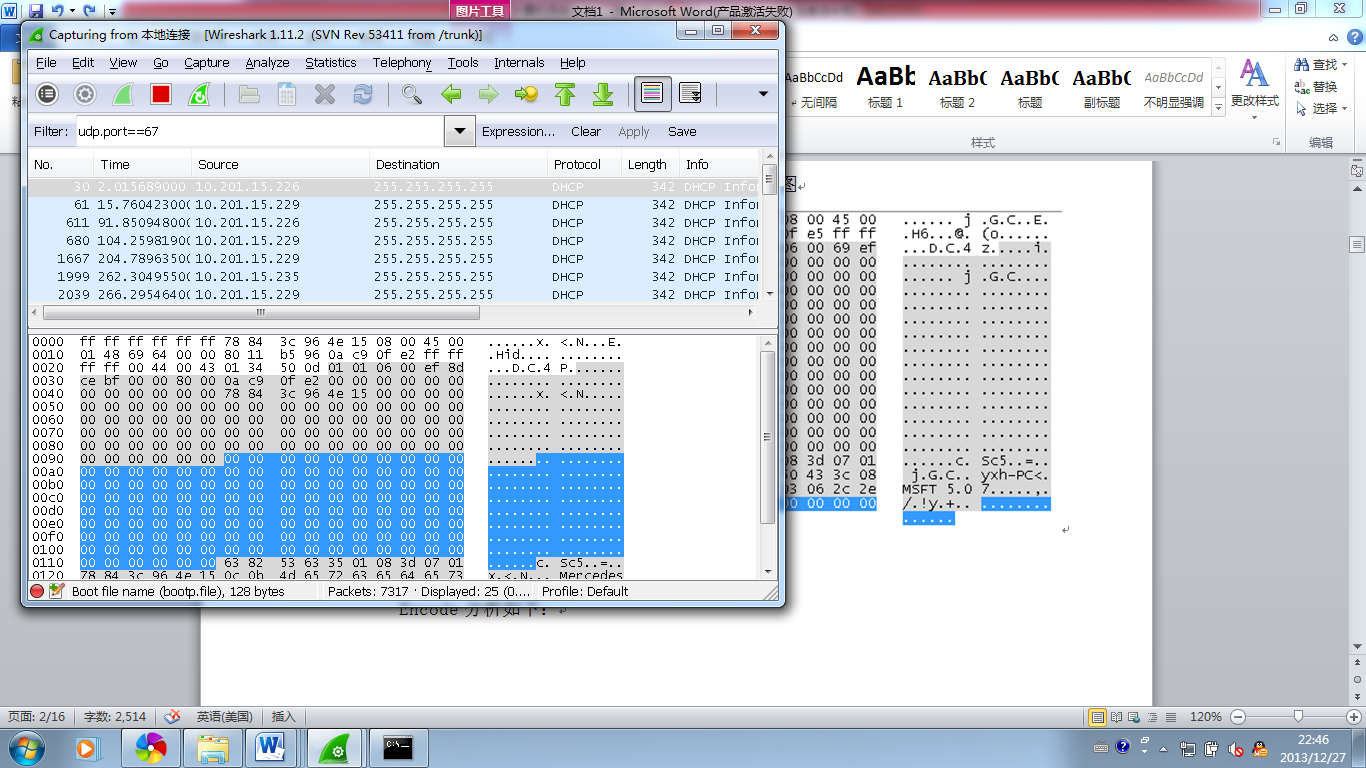
**3、实验设备环境**

1台装有Window7操作系统的pc机，要求能够连接到Internet，并安装Wireshark软件。

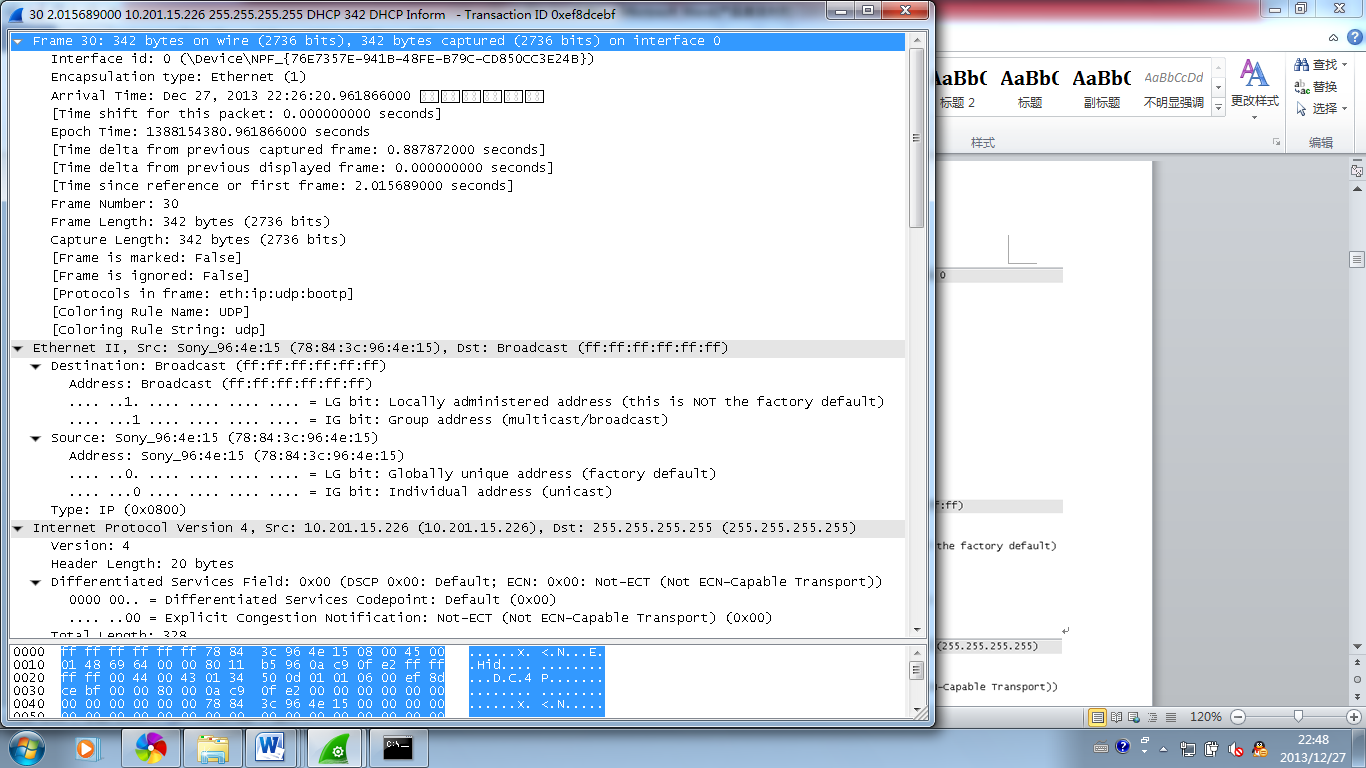
**4、分析网络层分组结构**

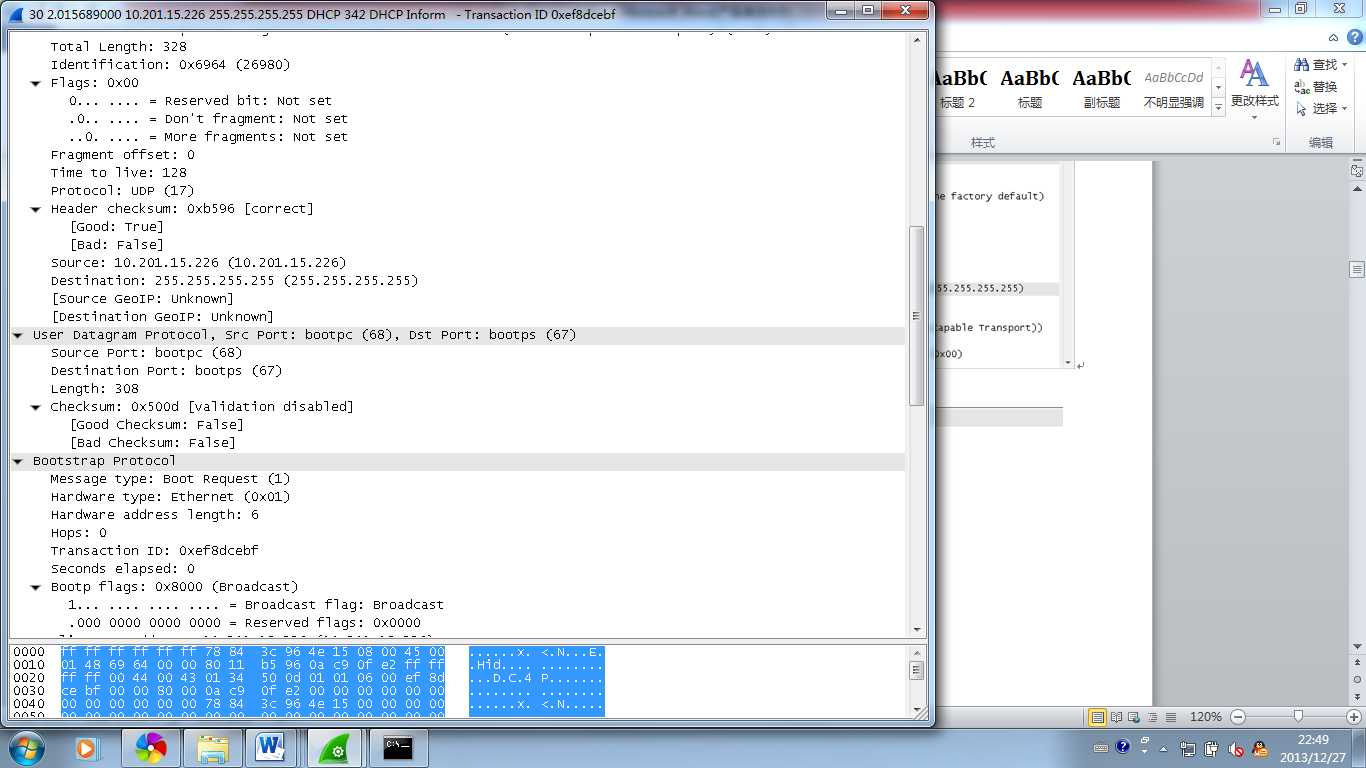
**1）捕获DHCP分组：**

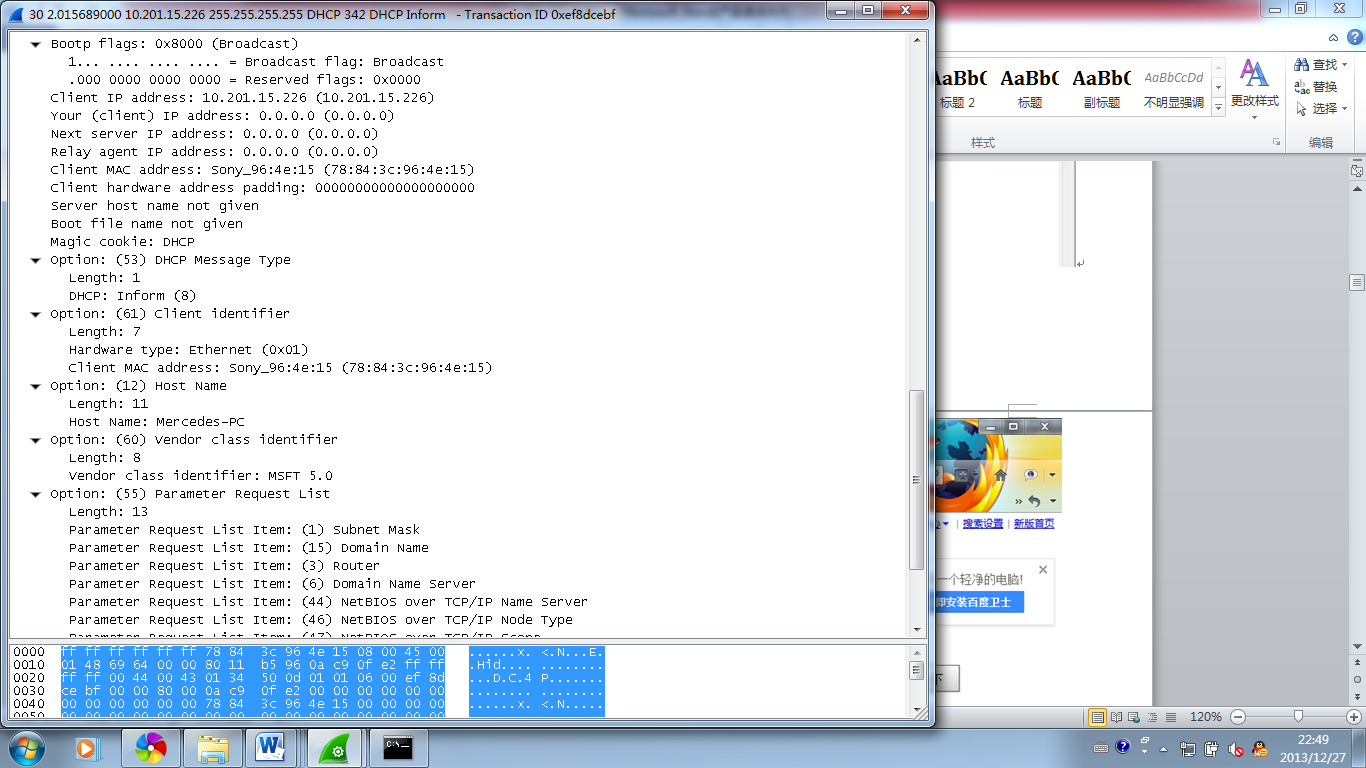


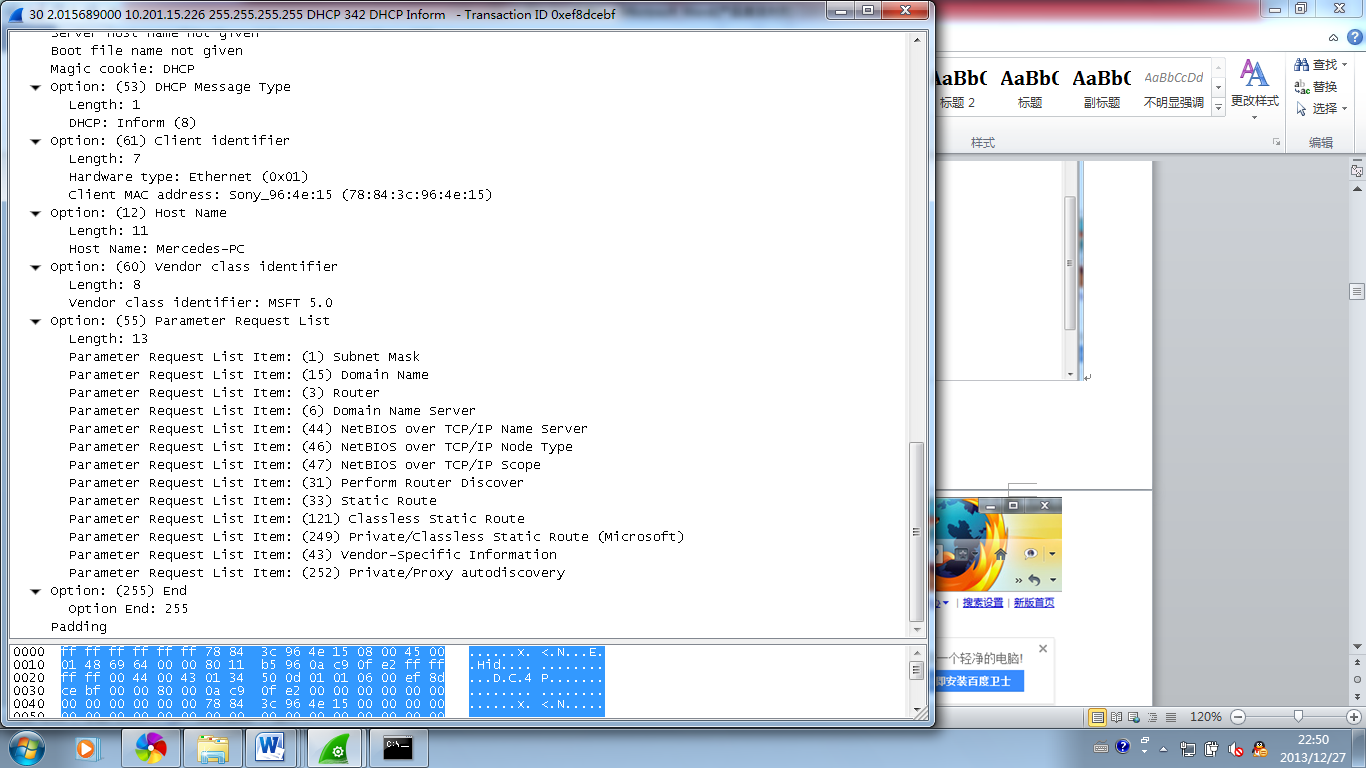


**Encode分析如下：**







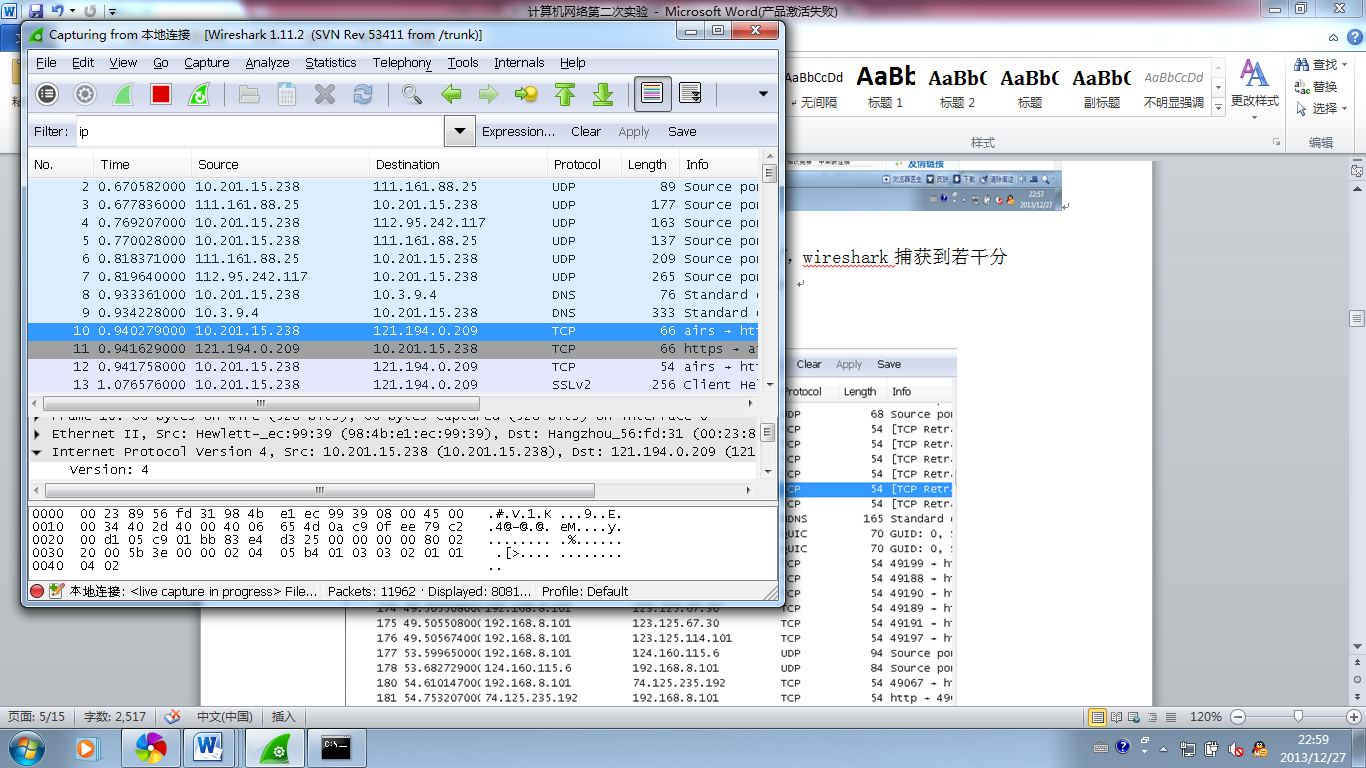


计算机以广播方式发送一个[DHCP](http://www.cnpaf.net/class/dhcp/)request请求信息，该信息中包含向它所选定的[DHCP](http://www.cnpaf.net/class/dhcp/)服务器请求IP地址10.201.15.226。

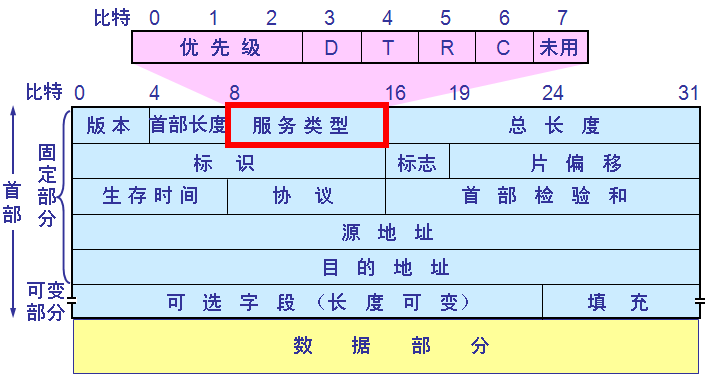
**（2）捕获IP数据分组：**

用浏览器登录北邮主页以产生网络流量

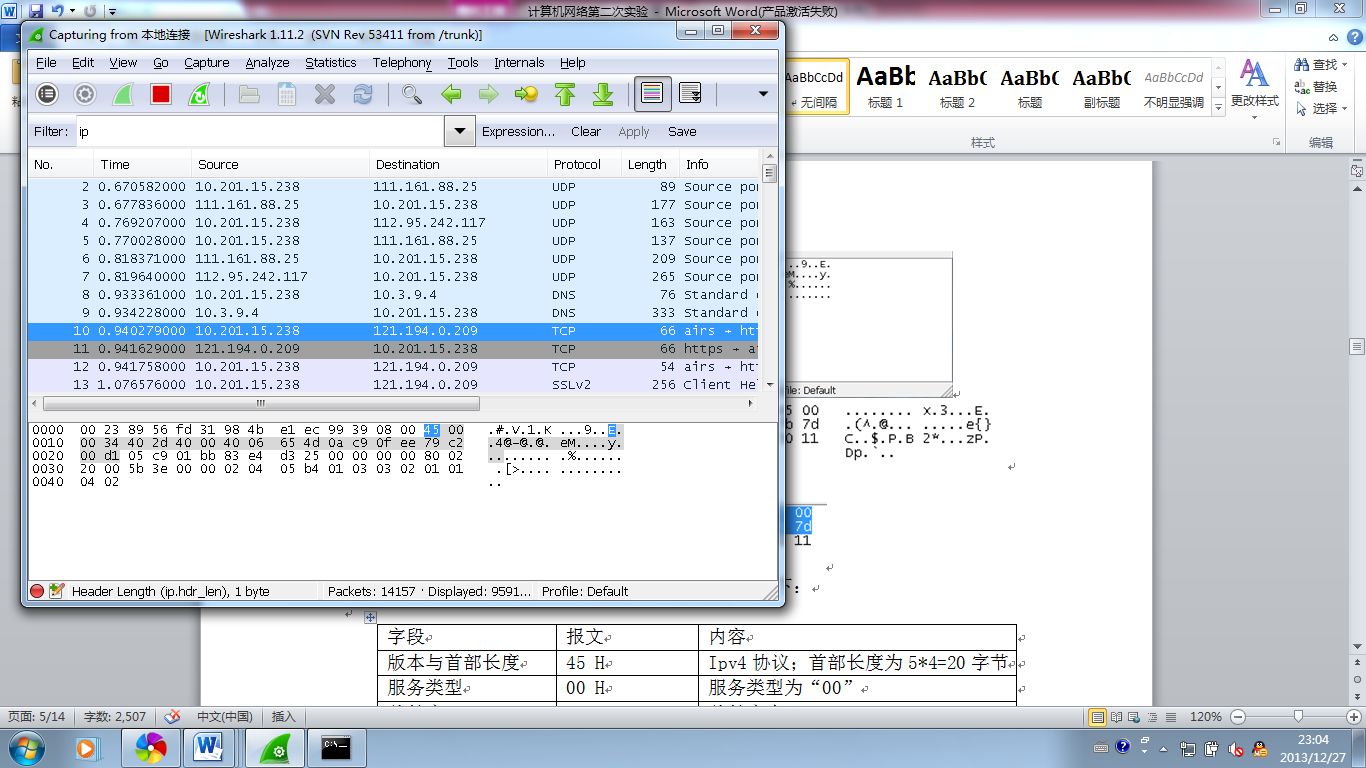
**捕获到ip协议数据包：**



**通常IP分组格式为:**

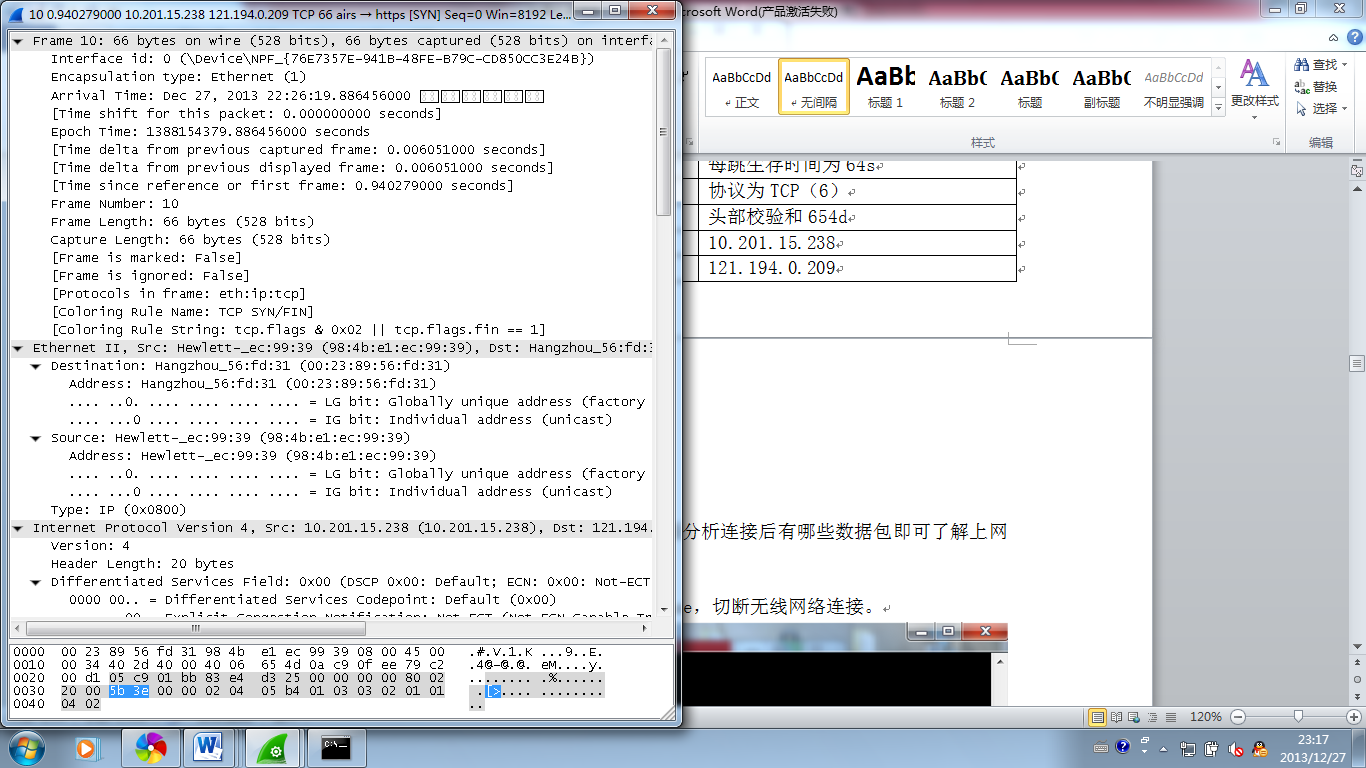


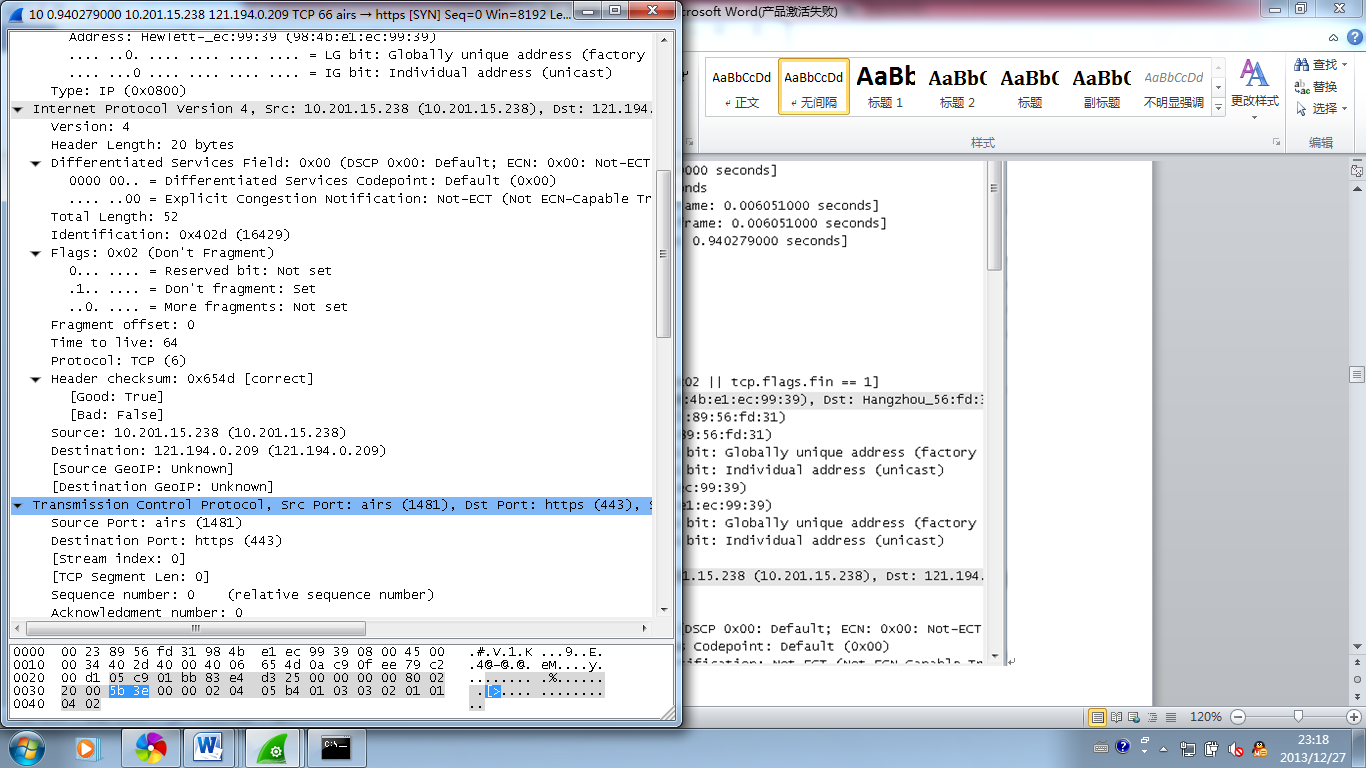
**分析IP数据分组：**

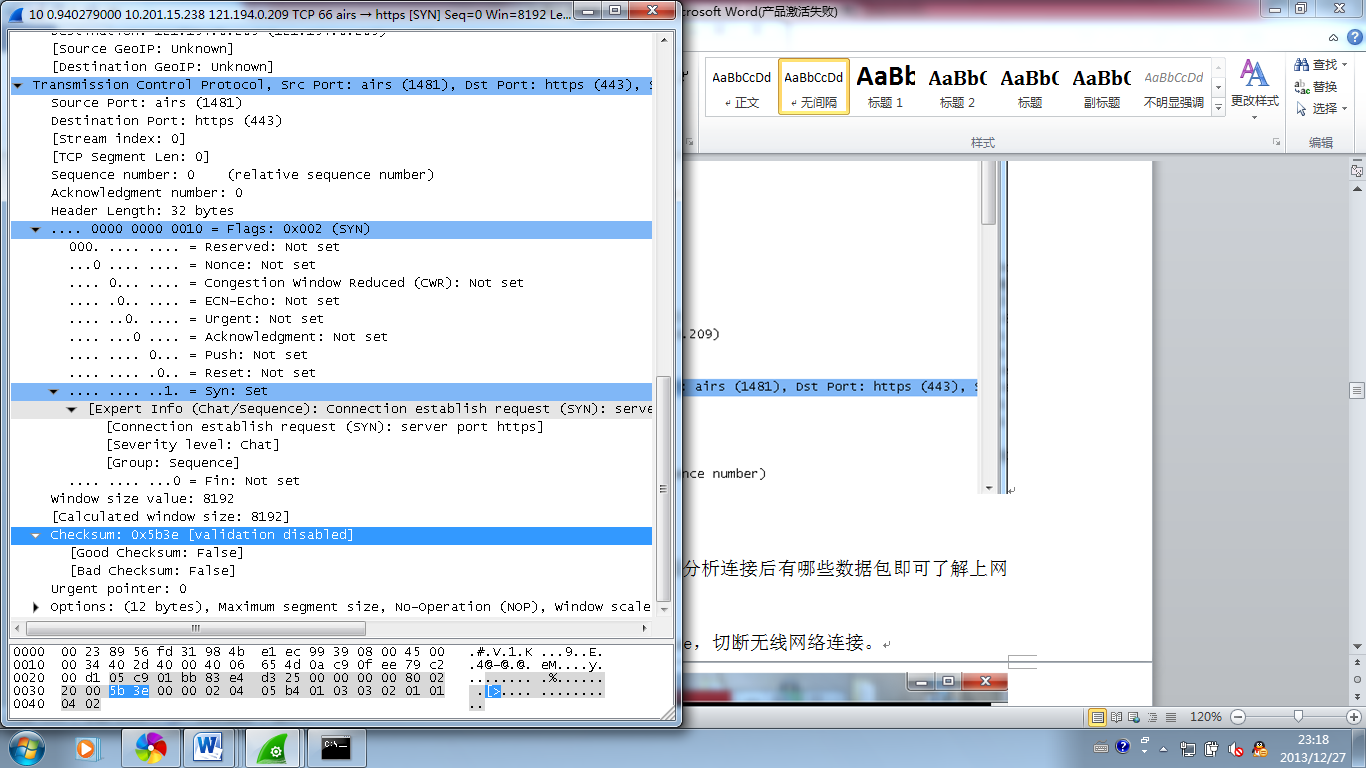


|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 H | 包头长20字节 |
| 服务类型 | 00 H | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 0034 H | 数据分组长度为52字节 |
| 标识 | 402d H | 标识为16429 |
| 标志 | 10 | DF=1，MF=0，表示不分片 |
| 片偏移 | 00H | 偏移量为0 |
| 生存周期 | 40H | 每跳生存时间为64s |
| 协议 | 06H | 协议为TCP（6） |
| 头部校验和 | 654dH | 头部校验和654d |
| 源地址 | 0ac90feeH | 10.201.15.238 |
| 目的地址 | 79c200d1H | 121.194.0.209 |

**以下为wireshark的分析：**







**(3)分析整个上网的工作过程，需要收发什么分组？每个分组的内容是什么？**

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：

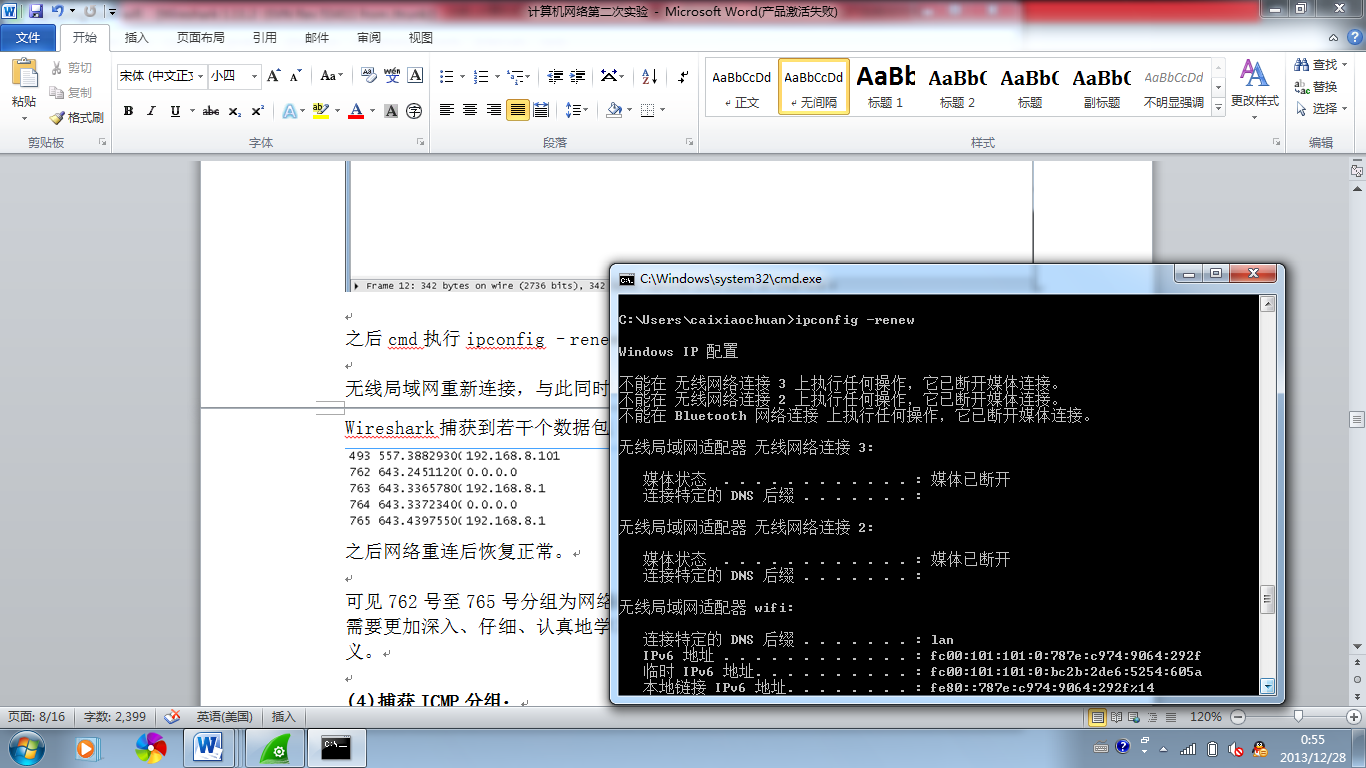
使用cmd切断无线网络连接。



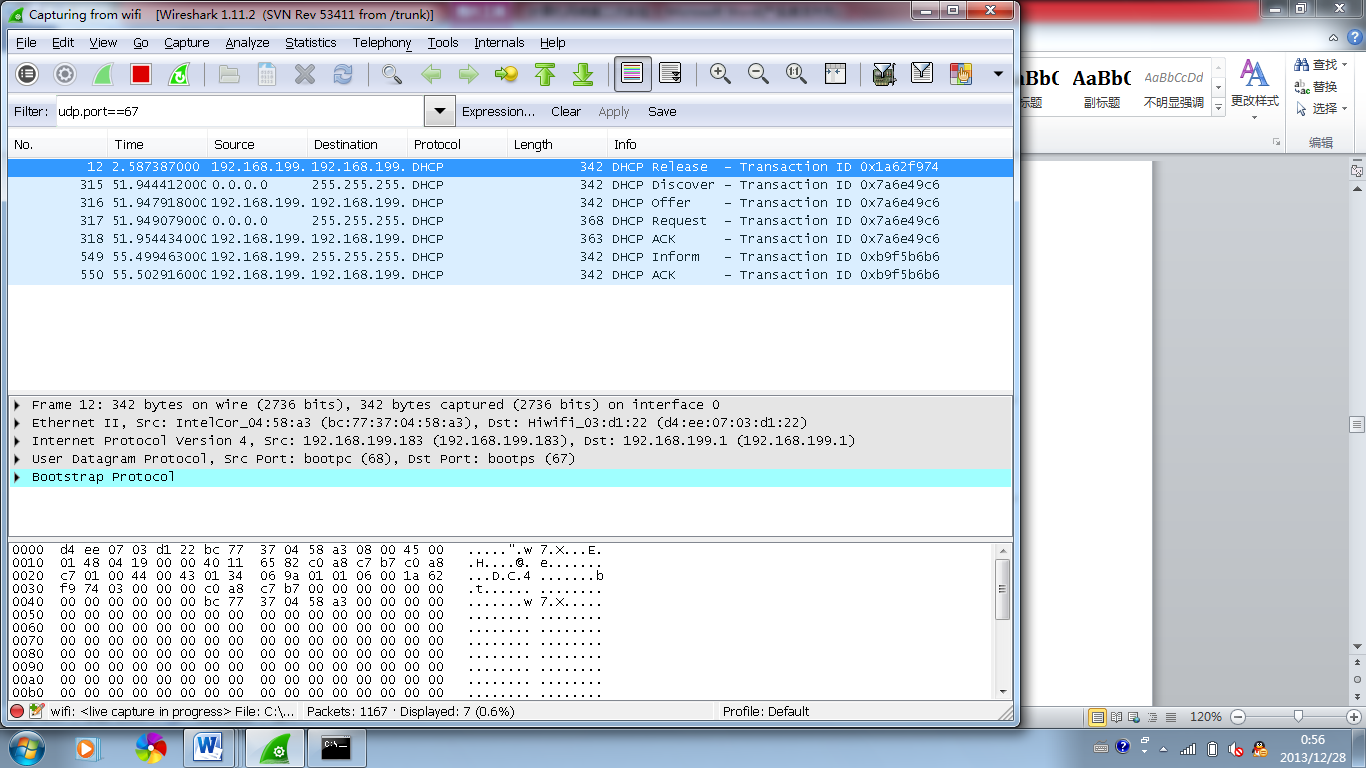
同时Wireshark捕获到DHCP Release用于断开网络：



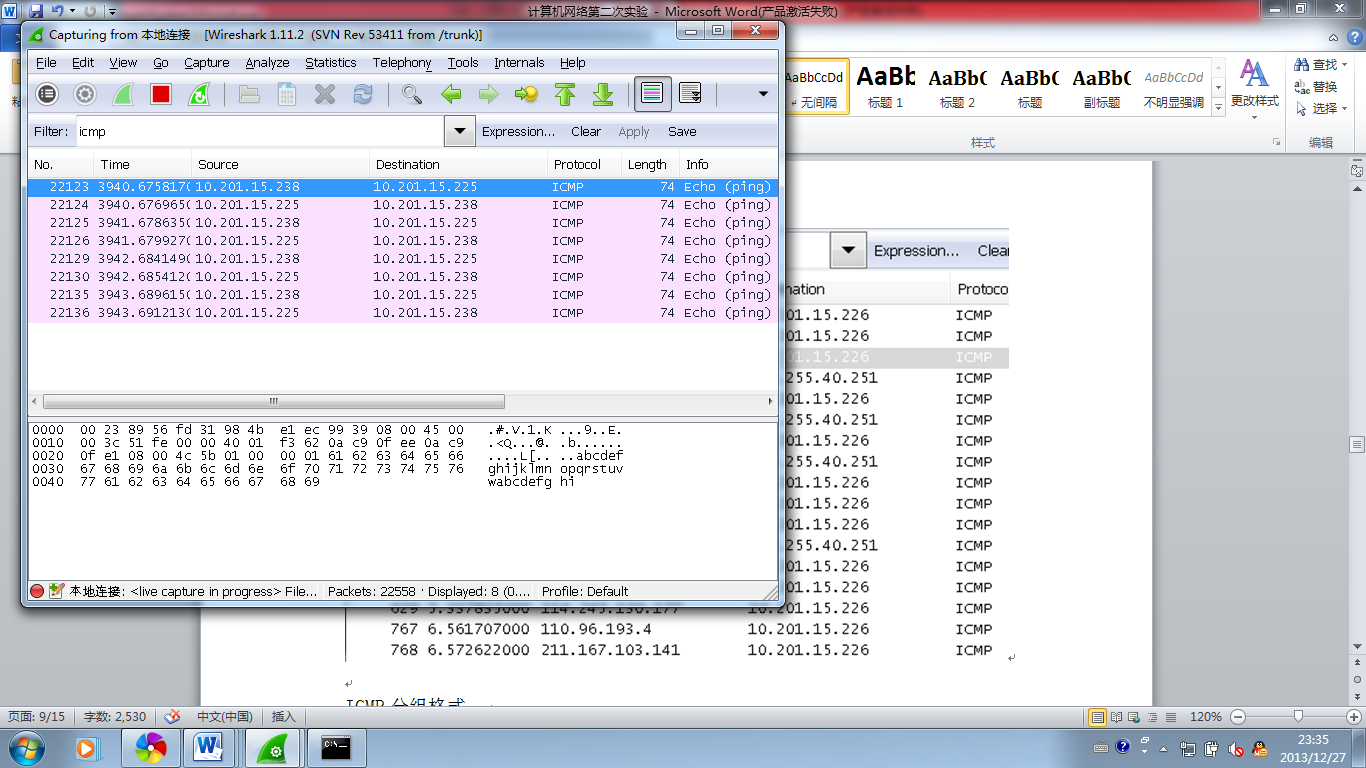
使用cmd重新连接网络



Wireshark捕获到DHCP ACK用于网络的重连：



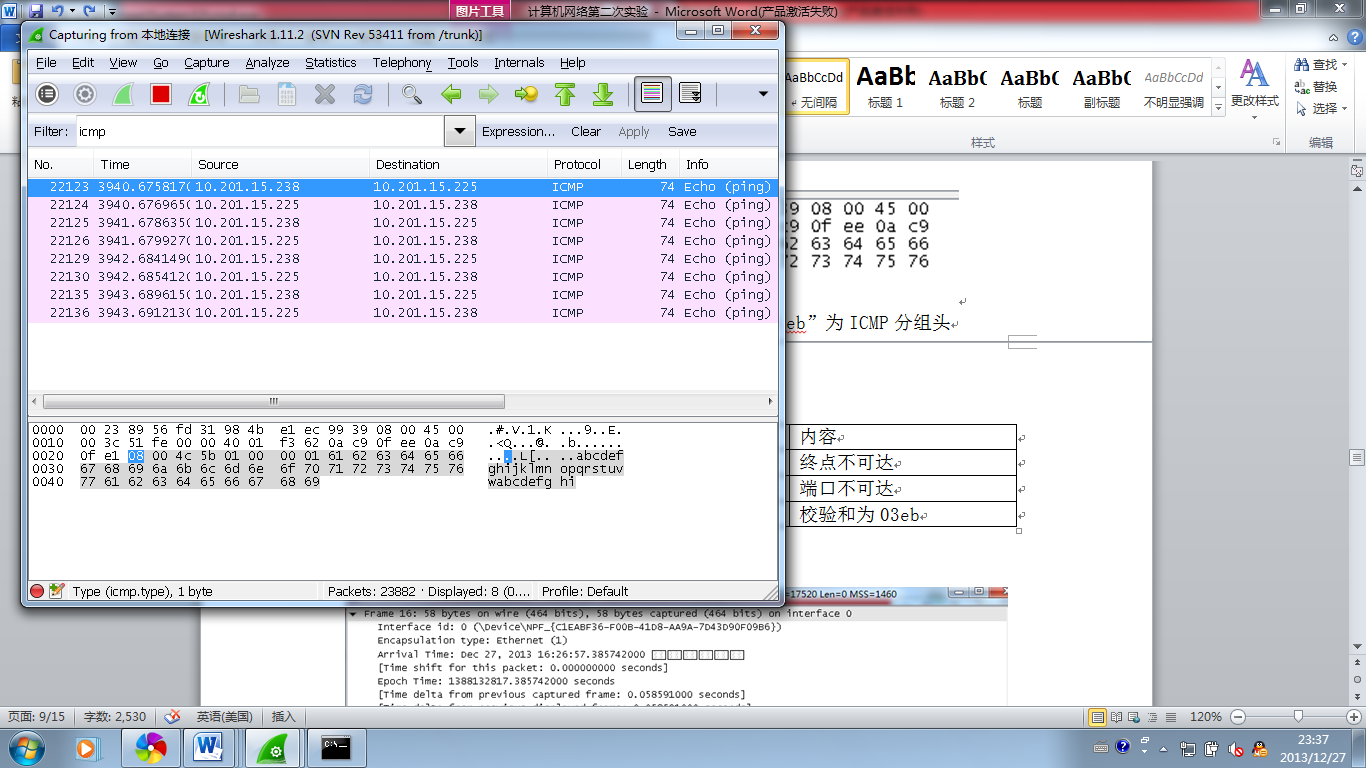
**(4)捕获ICMP分组：**



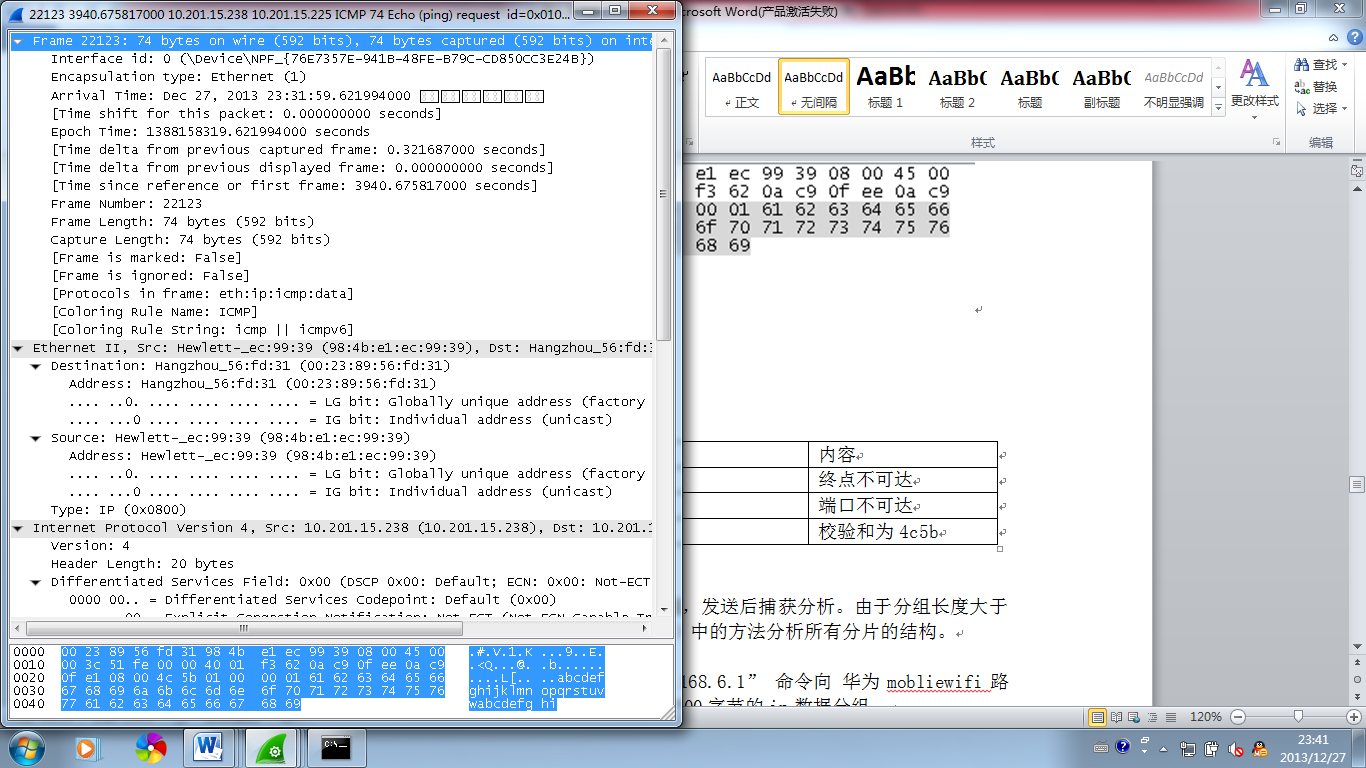
**ICMP分组格式：**

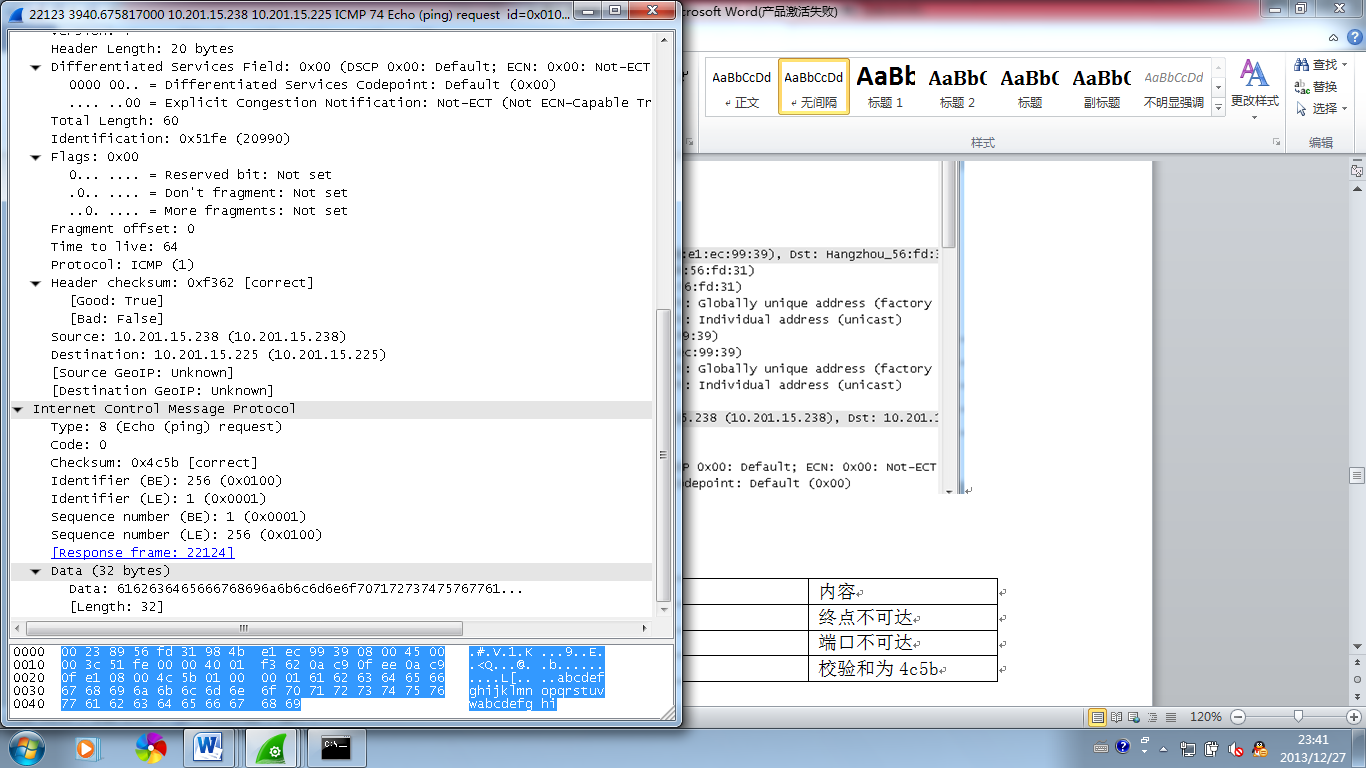


**分析ICMP分组：**



**Encode分析如下：**



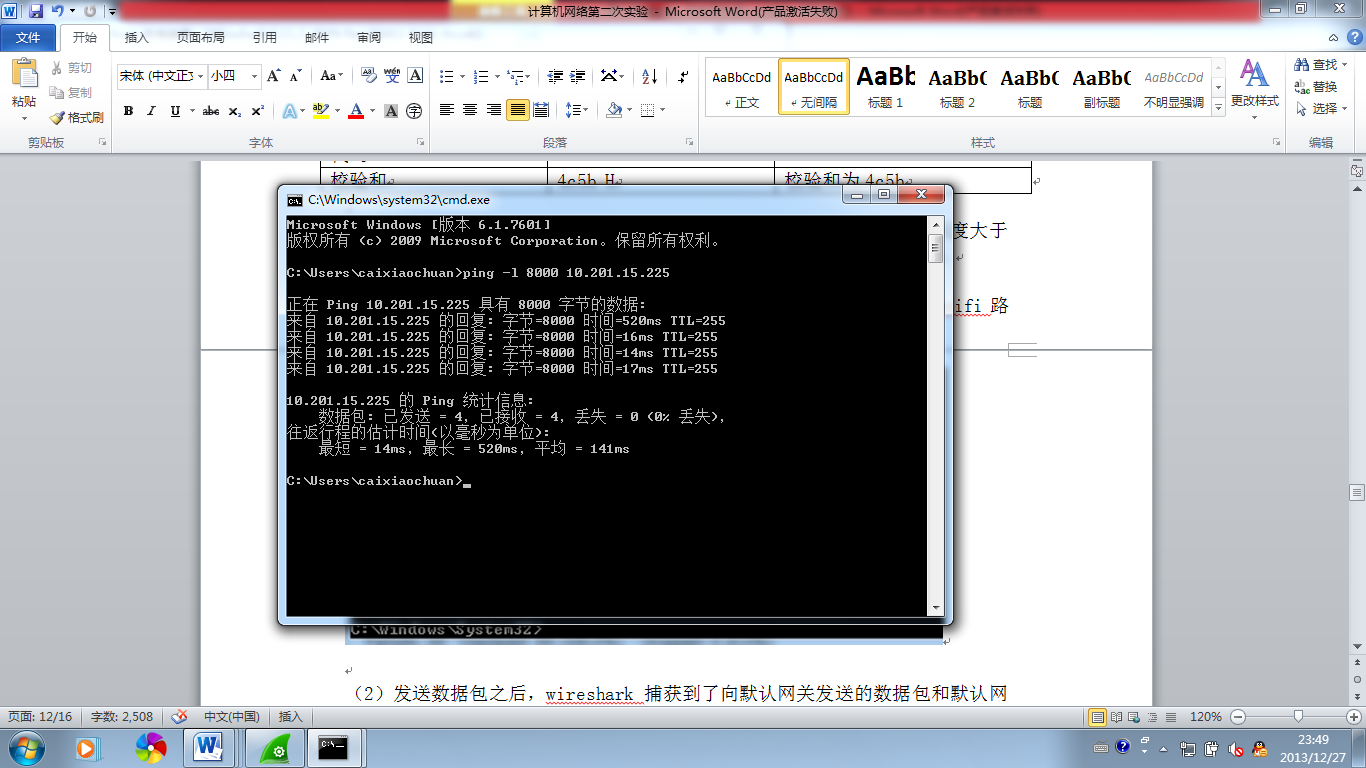


**分析ICMP分组：**

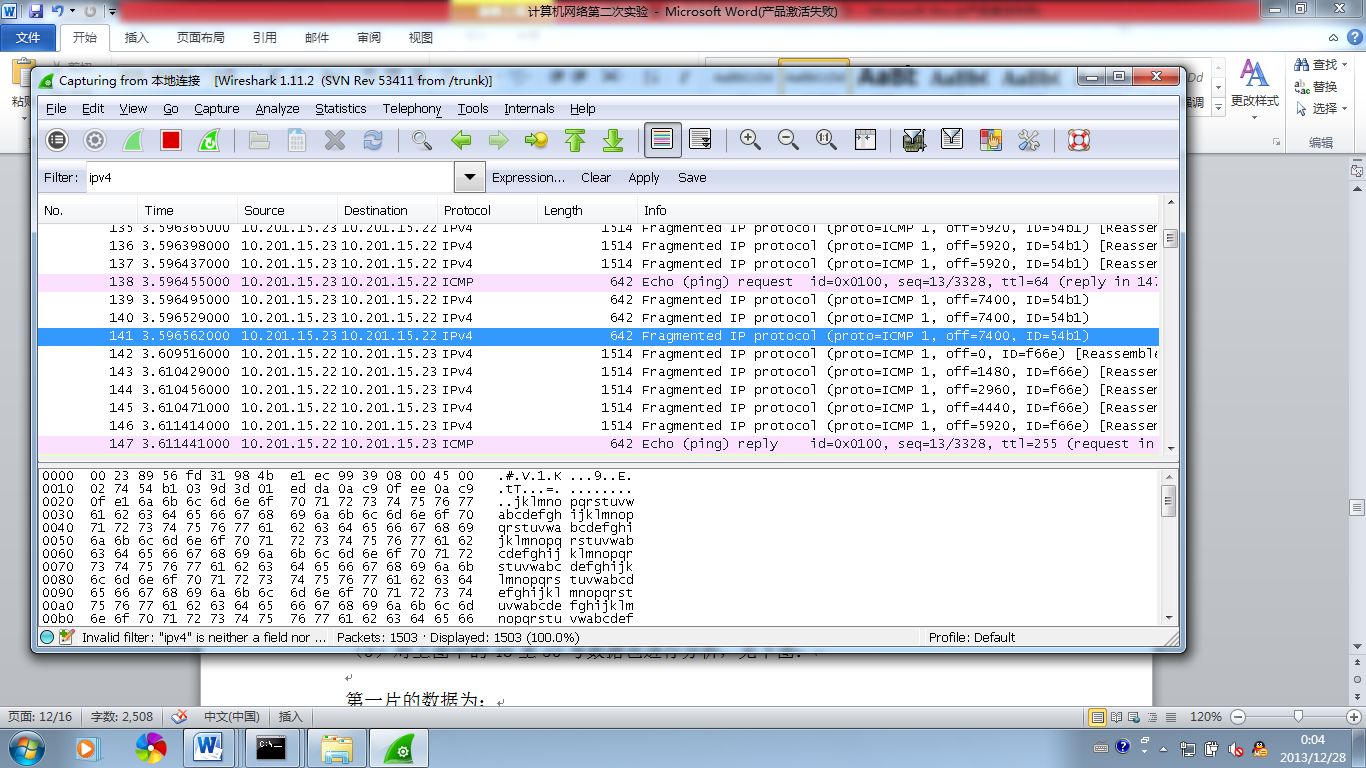
|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 类型 | 08 H | 问一台机器是否仍处于活动状态 |
| 代码 | 00 H |  |
| 校验和 | 4c5b H | 校验和为4c5b |

**（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。**

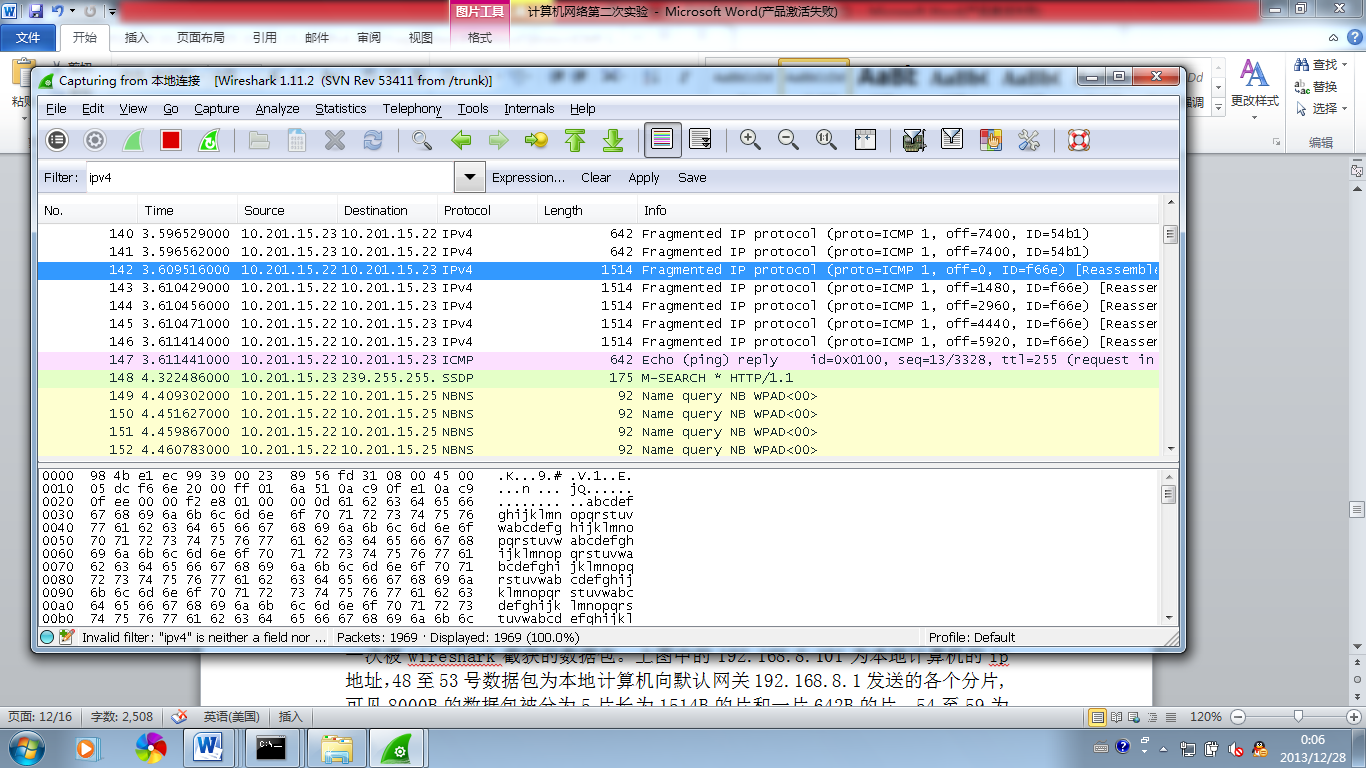
通过cmd向网关发送8000字节的数据。



发送数据包之后，捕获到了向默认网关发送的数据包和默认网关回复的数据包，如下图：



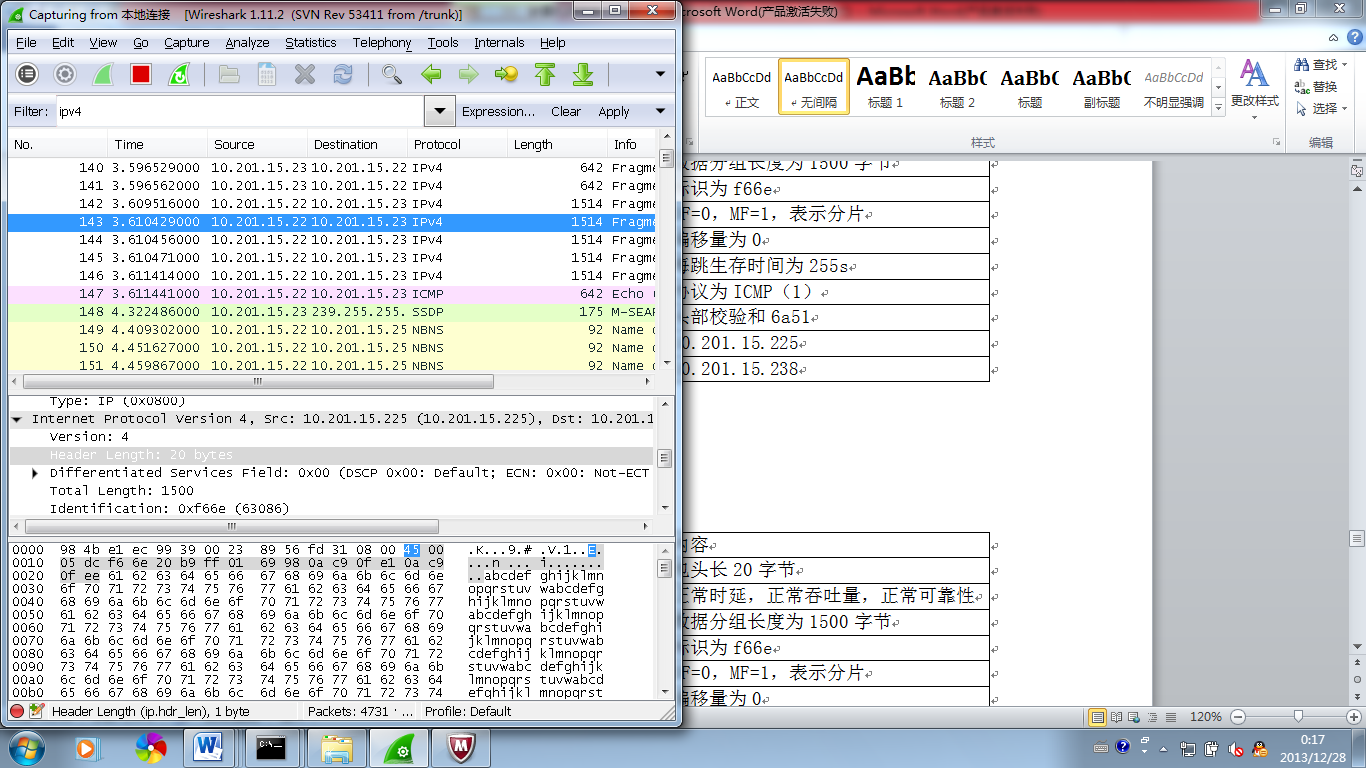
**第一片的数据为：**



**分析如下:**

|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 H | 包头长20字节 |
| 服务类型 | 00 H | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc H | 数据分组长度为1500字节 |
| 标识 | F66e H | 标识为f66e |
| 标志 | 01 | DF=0，MF=1，表示分片 |
| 片偏移 | 00H | 偏移量为0 |
| 生存周期 | ffH | 每跳生存时间为255s |
| 协议 | 01H | 协议为ICMP（1） |
| 头部校验和 | 6a51H | 头部校验和6a51 |
| 源地址 | 0ac90fe1H | 10.201.15.225 |
| 目的地址 | 0ac90feeH | 10.201.15.238 |

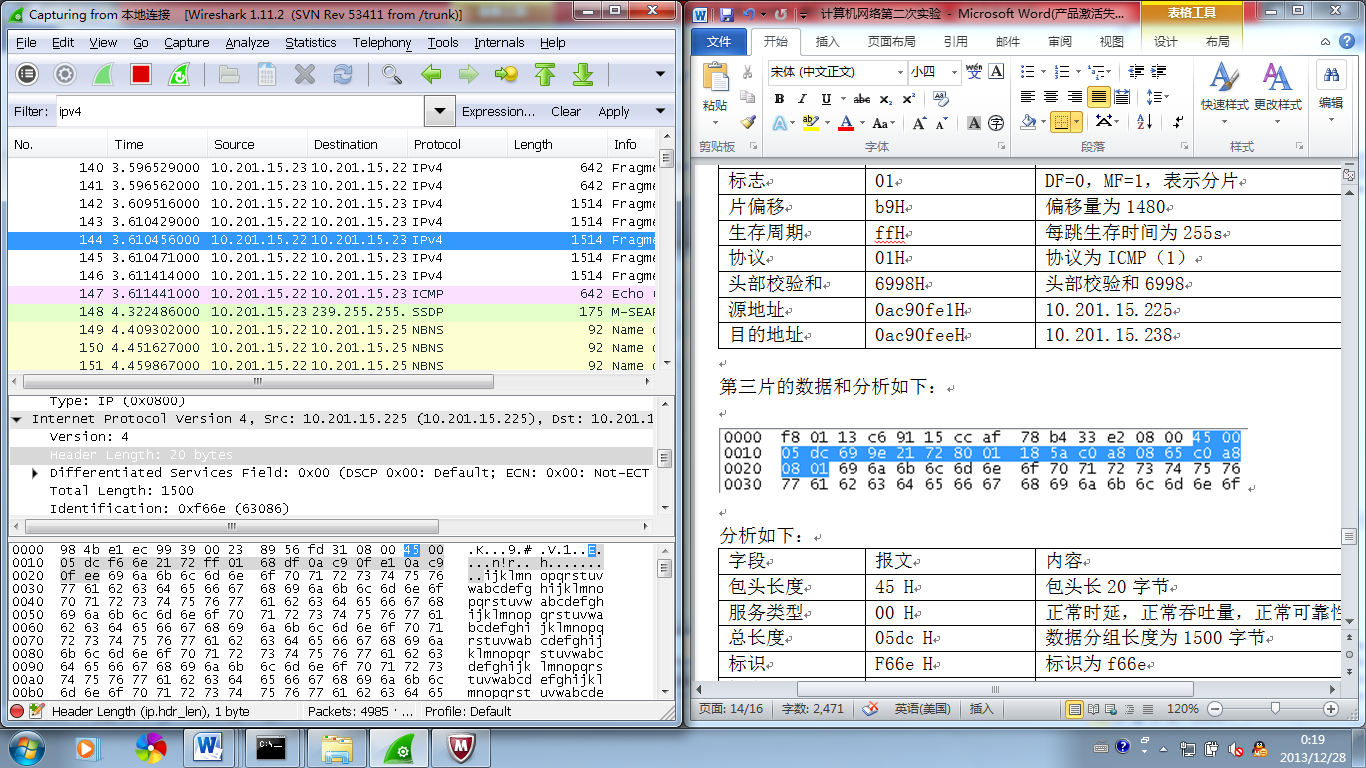
**第二片的数据为：**



**分析如下：**

|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 H | 包头长20字节 |
| 服务类型 | 00 H | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc H | 数据分组长度为1500字节 |
| 标识 | F66e H | 标识为f66e |
| 标志 | 01 | DF=0，MF=1，表示分片 |
| 片偏移 | b9H | 偏移量为1480 |
| 生存周期 | ffH | 每跳生存时间为255s |
| 协议 | 01H | 协议为ICMP（1） |
| 头部校验和 | 6998H | 头部校验和6998 |
| 源地址 | 0ac90fe1H | 10.201.15.225 |
| 目的地址 | 0ac90feeH | 10.201.15.238 |

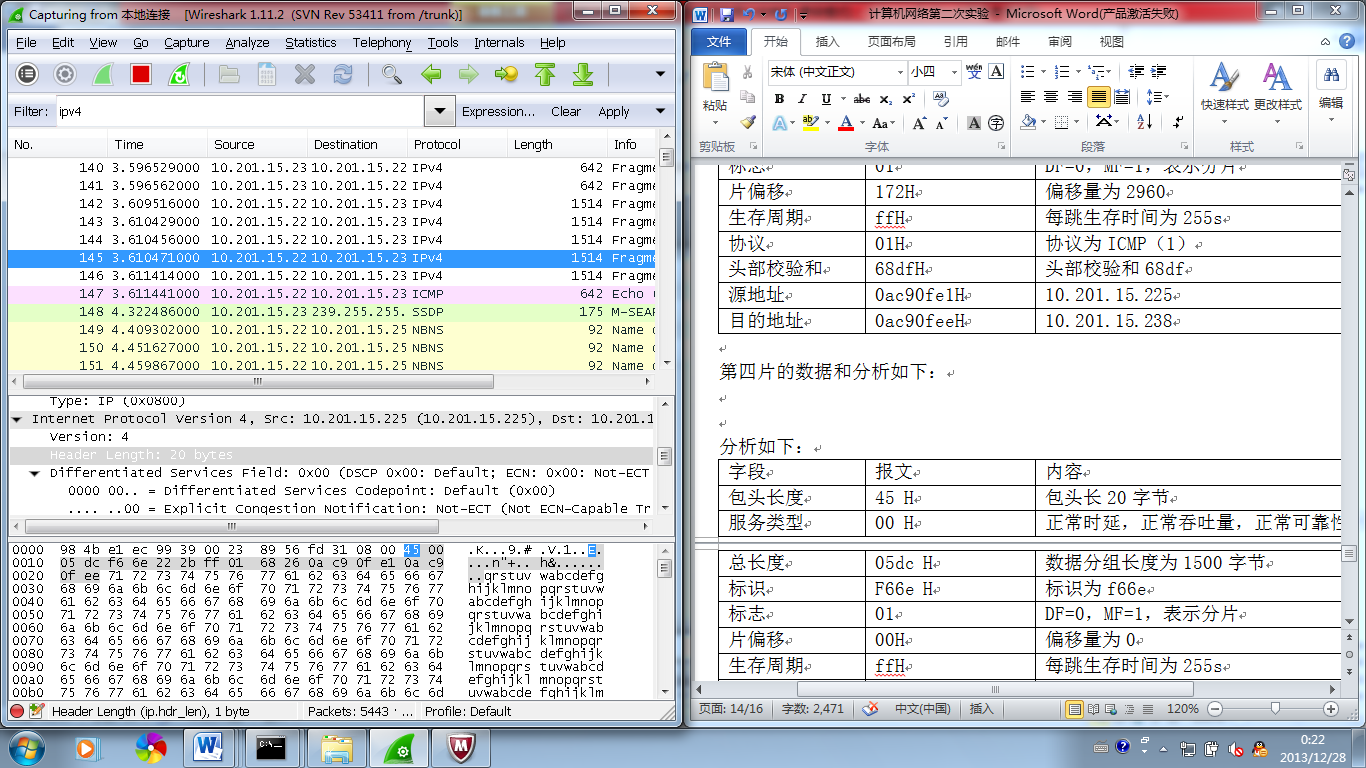
**第三片的数据和分析如下：**



**分析如下：**

|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 H | 包头长20字节 |
| 服务类型 | 00 H | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc H | 数据分组长度为1500字节 |
| 标识 | F66e H | 标识为f66e |
| 标志 | 01 | DF=0，MF=1，表示分片 |
| 片偏移 | 172H | 偏移量为2960 |
| 生存周期 | ffH | 每跳生存时间为255s |
| 协议 | 01H | 协议为ICMP（1） |
| 头部校验和 | 68dfH | 头部校验和68df |
| 源地址 | 0ac90fe1H | 10.201.15.225 |
| 目的地址 | 0ac90feeH | 10.201.15.238 |

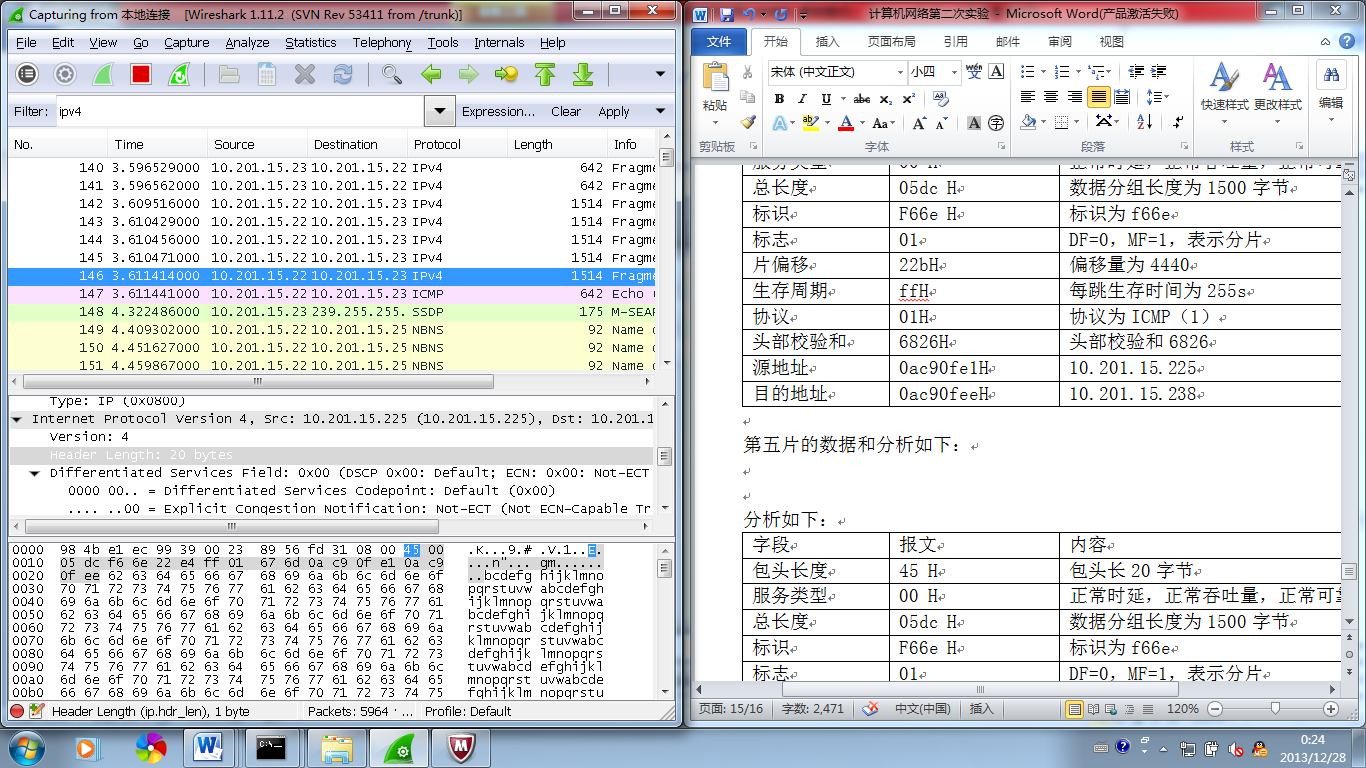
**第四片的数据和分析如下：**



**分析如下：**

|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 H | 包头长20字节 |
| 服务类型 | 00 H | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc H | 数据分组长度为1500字节 |
| 标识 | F66e H | 标识为f66e |
| 标志 | 01 | DF=0，MF=1，表示分片 |
| 片偏移 | 22bH | 偏移量为4440 |
| 生存周期 | ffH | 每跳生存时间为255s |
| 协议 | 01H | 协议为ICMP（1） |
| 头部校验和 | 6826H | 头部校验和6826 |
| 源地址 | 0ac90fe1H | 10.201.15.225 |
| 目的地址 | 0ac90feeH | 10.201.15.238 |

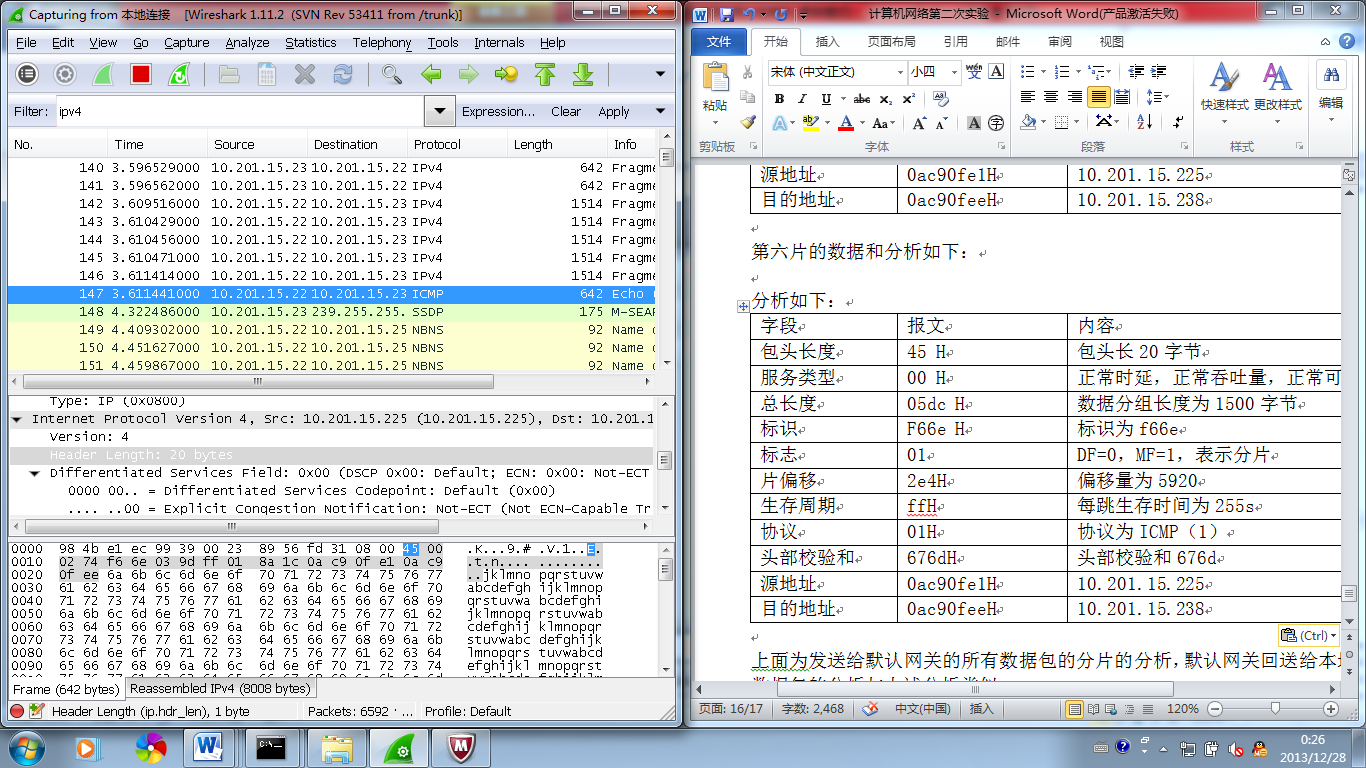
**第五片的数据和分析如下：**



**分析如下：**

|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 H | 包头长20字节 |
| 服务类型 | 00 H | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc H | 数据分组长度为1500字节 |
| 标识 | F66e H | 标识为f66e |
| 标志 | 01 | DF=0，MF=1，表示分片 |
| 片偏移 | 2e4H | 偏移量为5920 |
| 生存周期 | ffH | 每跳生存时间为255s |
| 协议 | 01H | 协议为ICMP（1） |
| 头部校验和 | 676dH | 头部校验和676d |
| 源地址 | 0ac90fe1H | 10.201.15.225 |
| 目的地址 | 0ac90feeH | 10.201.15.238 |

**第六片的数据和分析如下：**



**分析如下：**

|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 H | 包头长20字节 |
| 服务类型 | 00 H | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 0274 H | 数据分组长度为628字节 |
| 标识 | F66e H | 标识为f66e |
| 标志 | 00 | DF=0，MF=0，表示为最后一片 |
| 片偏移 | 39dH | 偏移量为7400 |
| 生存周期 | ffH | 每跳生存时间为255s |
| 协议 | 01H | 协议为ICMP（1） |
| 头部校验和 | 8a1cH | 头部校验和8a1c |
| 源地址 | 0ac90fe1H | 10.201.15.225 |
| 目的地址 | 0ac90feeH | 10.201.15.238 |

**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。

**5、实验结论和实验心得：**

做实验的时间有些略长，主要是分析耗费了很多时间，有点不熟练。虽说完成了实验，但是本次实验还是遇到了很多的问题。在做第一个DHCP分组时，因不知道可以查看具体某个协议，所以找了很久才找到快速寻找协议的办法。在第三个实验中，刚开始为想到通过cmd来解决，在请教同学后完成了第三个实验。第四个和第五个实验因类似前面的内容，所以完成的比较顺利。

通过这次实验，我加深了对网络层工作机制的理解，也通过实践加深了对课本上理论知识的理解，感觉自己对计算机网络整个的体系结构有个更深的认识。