**实验4: 分析IP报文结构**

### 一、实验名称

分析IP数据包的格式

### 二、实验目的

1：深入理解IP报文结构和工作原理。

2：掌握抓包工具分析捕获的跟踪文件的基本技能。

### 三、实验内容和要求

1) 运行Windows 7 操作系统的 PC 一台。

2) PC 具有以太网卡一块，通过双绞线与校园网相连；或者具有适合的踪迹文件。

3) 每台 PC 运行程序协议分析仪 Wireshark。

### 四、实验环境

1：运行Windows 7 操作系统PC机。

2：PC 具有以太网卡一块，通过双绞线与网络相连；或者具有适合的踪迹文件。

3：机房，可以访问Internet。

**五、操作方法与实验步骤概念**

1、启动wireshark捕获功能，访问河南大学官网和其他网站，使用nslookup指令解析河南大学官网的IP地址，记为**河大IP**。

2、分析俘获的分组。

打开踪迹文件，用鼠标点选感兴趣的帧，按右键出现如图1菜单。该菜单提供了许多非常有用的功能，当选中目的地址为**河大IP的**分组，用鼠标指向其源地址，打开如图 2 所示菜单，点击“Selected”，就会出现如图2所示的界面。可见，系统已经自动用其源地址作为过滤条件，从众多分组中过滤出与 本地主机 有关分组了。

如果过滤掉较高层协议的细节，比如选择去掉IP，则会屏蔽IP相关信息。结果如图3。

3、分析IP报文。

为了进一步分析 IP 数据报结构，点击首部细节信息栏中的“Internet Protocol”行，有关信息展开如图5首部信息窗口所示。

3：回答下列问题：

1. 你使用的计算机的 IP 地址是什么？

10.12.50.200

1. 在 IP 数据报首部，较高层协议字段中的值是什么？

1

1. IP 首部有多少字节？载荷字段有多少字节？

IP 首部有20个字节，载荷字段有40字节

1. 该 IP 数据报分段了没有？如何判断该 IP 数据报有没有分段？

该 IP 数据报没有分段，fragment offset：0，即片偏移为零

1. 关于高层协议有哪些有用信息？

对方服务器mac地址00:00:5e:00:01:0a

**六、实验数据记录和结果分析**

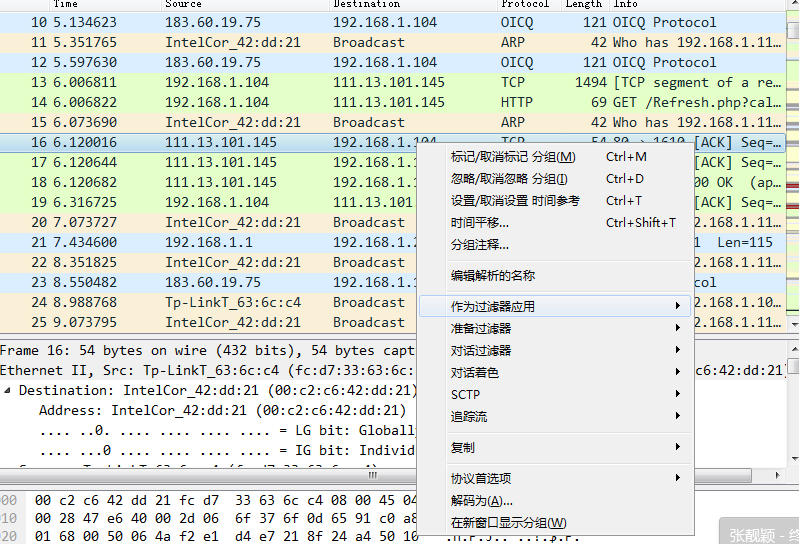


图1

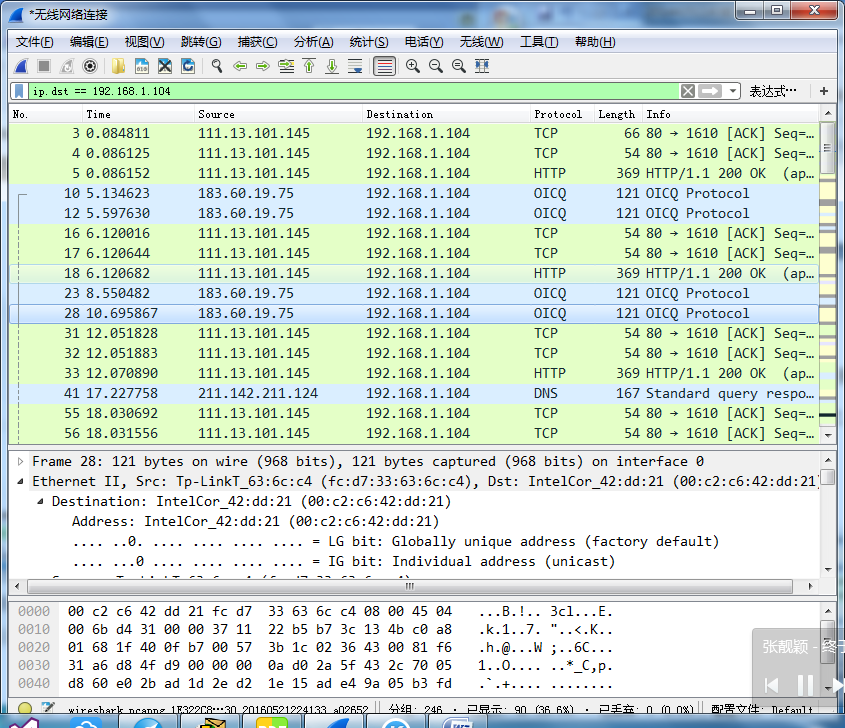


图2

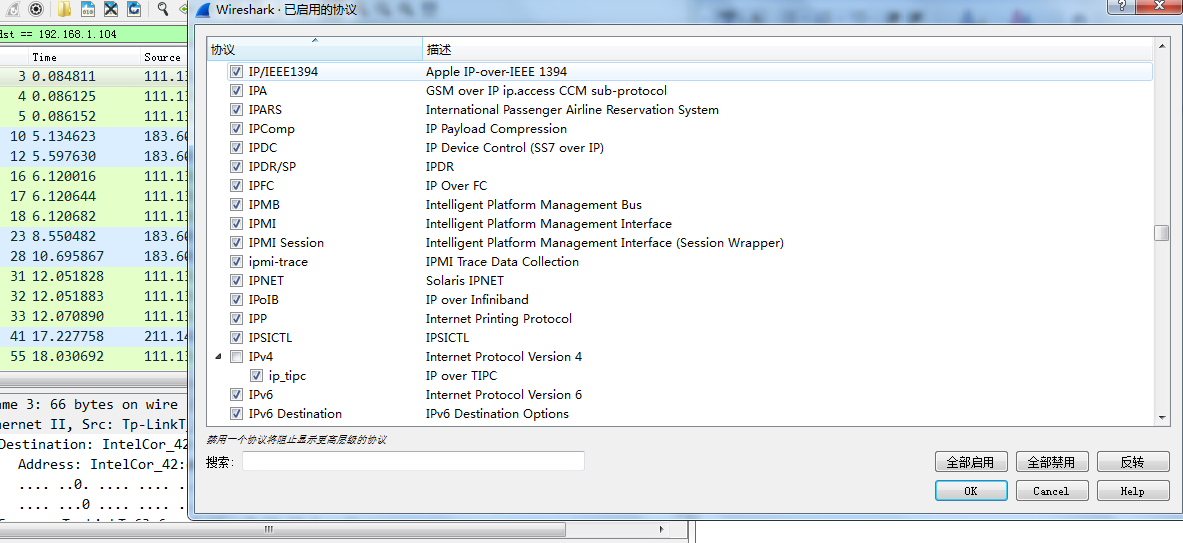


图3

图3中的IPv4勾选后，点击ok，就会出现图4的结果。

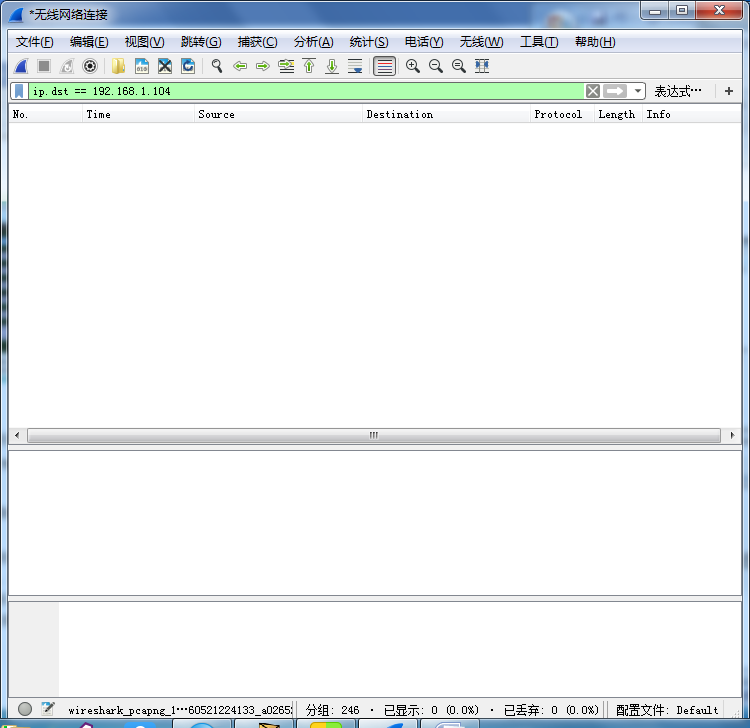


图4

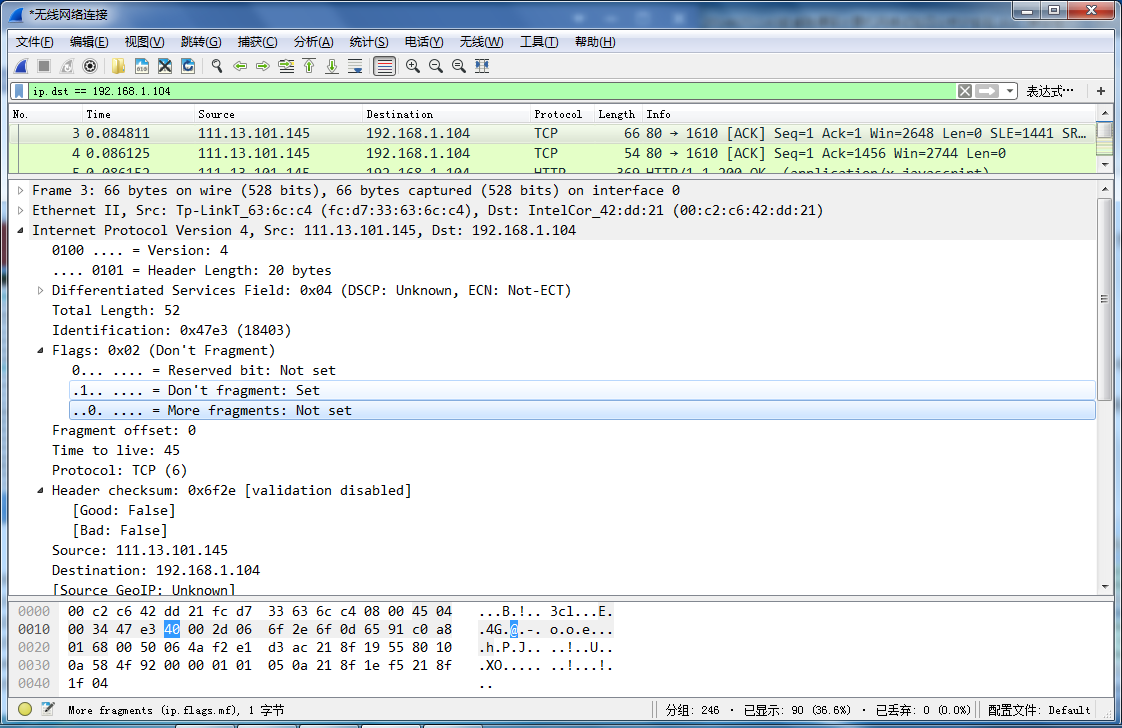


图5

1：IP地址： 10.12.50.200

2：值： 1

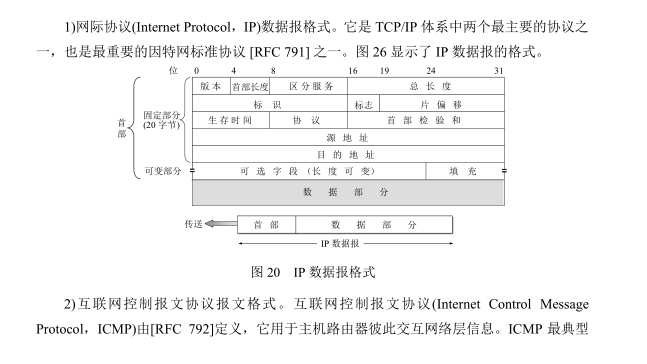
3：该IP数据报分段了吗？

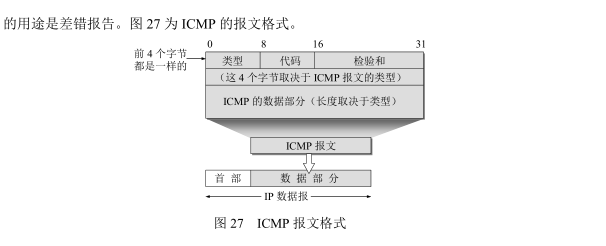
没有，Fragment offset为0。

4：通过高层协议，我们可以看到我们正在做什么，是请求还是回应，还是传递信息。

### 七、实验体会、质疑和建议

知识回顾：





进一步了解IP的构成，IP数据部分与首部信息，进一步了解IP报文的格式，ICMP报文的格式。