**实验二 利用wireshark抓包工具抓包**

### 实验名称

使用网络协议分析仪 Wireshark

### 二、实验目的

### 1. 掌握安装和配置网络协议分析仪Wireshark的方法；

### 2. 熟悉使用Wireshark工具分析网络协议的基本方法，加深对协议格式、协议层次和协议交互过程的理解。

### 三、实验内容和要求

1. 安装和配置Wireshark的网络协议分析仪，下载Wireshark软件。

2. 使用并熟悉Wireshark分析协议的部分功能。

**四、实验环境**

1．Windows7 操作系统PC机器。

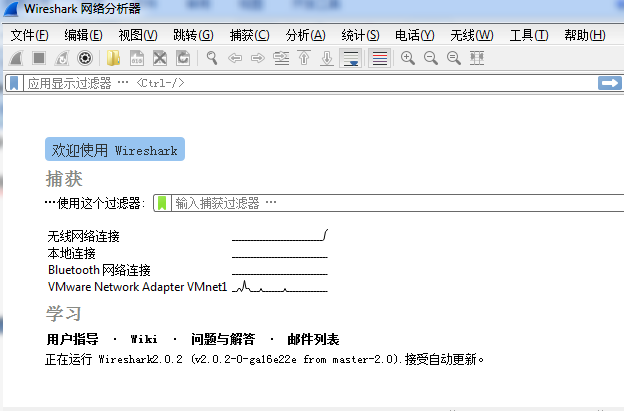
2.PC机器具有以太网卡一块，通过双绞线与局域网连接。

**五、操作方法与实验步骤**

1：安装网络协议分析仪，从官网下载exe软件双击安装Wireshark-win64-2.0.2。

2：启用Wireshark进行试验。

2.1：启动初始如下显示：



2.2：分组捕获数据，并将捕获的数据保存为文件抓包实验数据.pcapng，当再次需要捕获时，可以打开文件在进行实验抓包。

2.3：对数据进行协议分析。

在**上部**“俘获分组的列表”窗口中，有编号(No)、时间(Time)、源地址(Source)、目的地址(Destination)、协议(Protocol)、长度(Length)和信息(Info)等列(栏目)，各列下方依次排列着俘获的分组。**中部**“所选分组首部的细节信息”窗口给出选中帧的首部详细内容。**下部**“分组内容”窗口中是对应所选分组以十六进制数和 ASCII 形式的内容。

2.4无线网连接抓包实验数据如下图1

2.5本地连接网页抓包实验数据如下图2

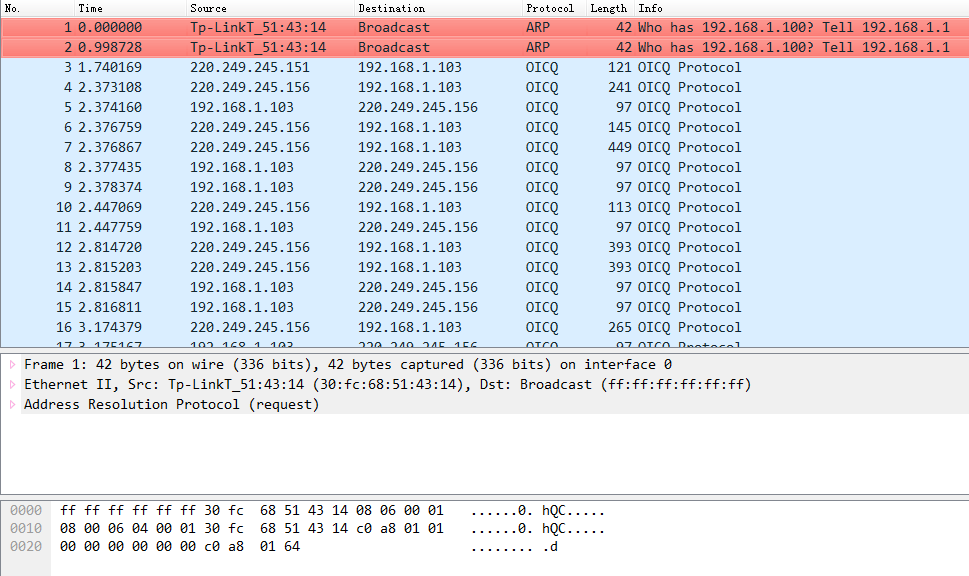


图 1

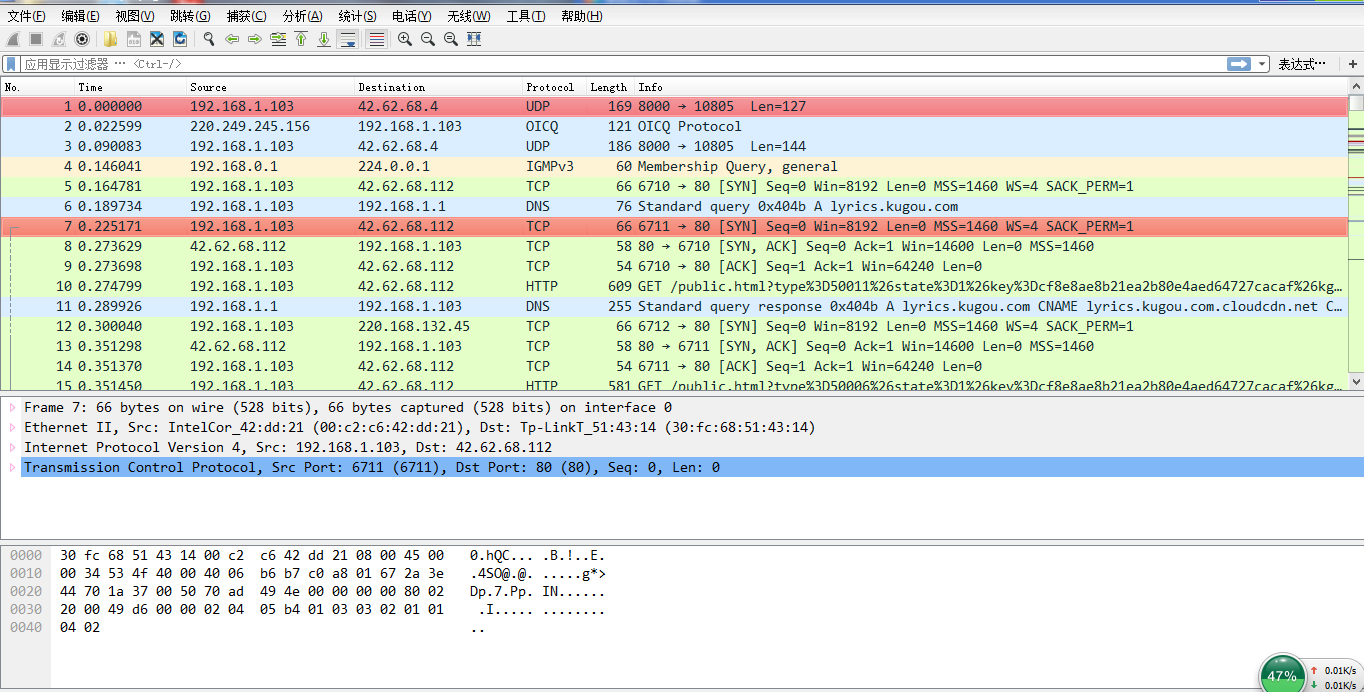


图 2

### 六、实验数据记录和结果分析

1：网络抓包实验获取的数据如下图3

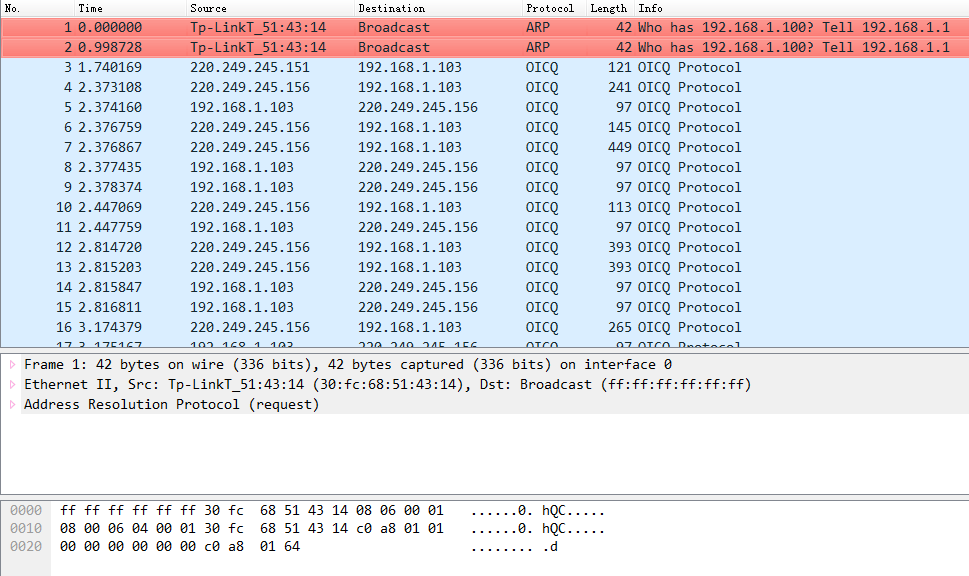


图 3

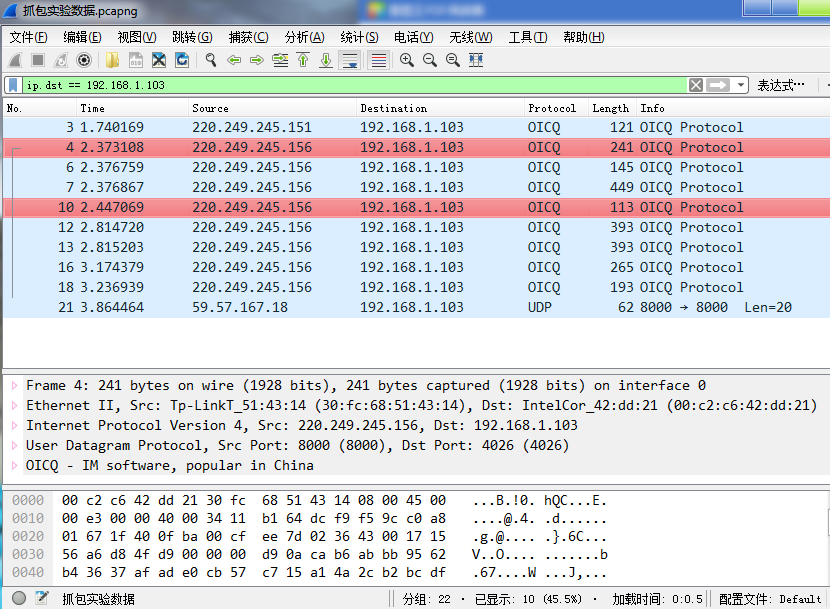
2：使用过滤器过滤数据 比如以下图4中的Time=4 2.373108作为过滤条件，可以将图2过滤为图3，如果你需要符合某些条件的数据，这种方案可以分组，减少数据量，因此可以提高效率。

图 4

3：使用过滤器过滤数据 比如以下图5中的Source=192.168.1.163与Destination=220.168.132.45作为过滤条件，可以将图4过滤为图5，如果你需要符合某些条件的数据，这种方案可以分组，减少数据量，因此可以提高效率。

**4：熟悉以上操作后自行进行练习，练习内容包括：①对捕获的数据包（任选一个）进行简单分析；②设置不同的过滤条件，对捕获的数据包进行过滤。请将练习步骤用文字和插图进行描述**。

### 七、实验体会、质疑和建议