一、实验目的：

通过 wireshark 分析 IP 协议并了解 IP 数据报的组成及各部分的含义.

IP 是英文 Internet Protocol（网络之间互连的协议）的缩写，中文简称为“网协”，也就是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。

二、实验准备：

下载并安装本实验使用的软件：wget（http://www.gnu.org/software/wget/）、wireshark（www.wireshark.org）

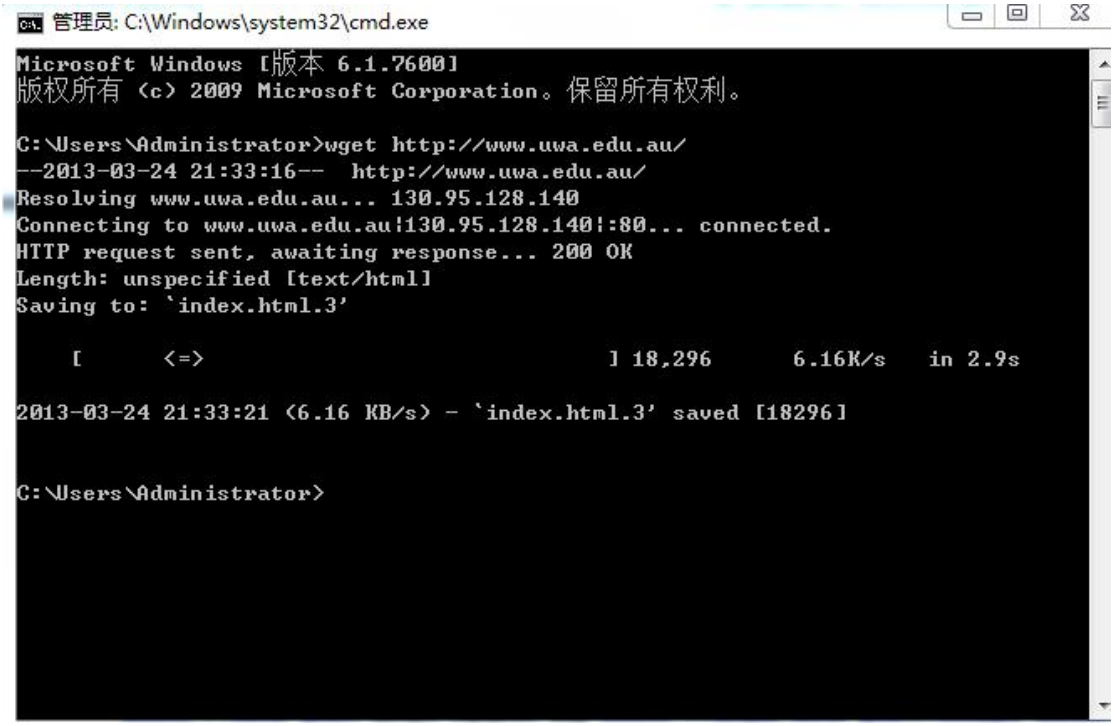
windows 下相关命令:tracert、wget

三、实验步骤：

1、捕获数据

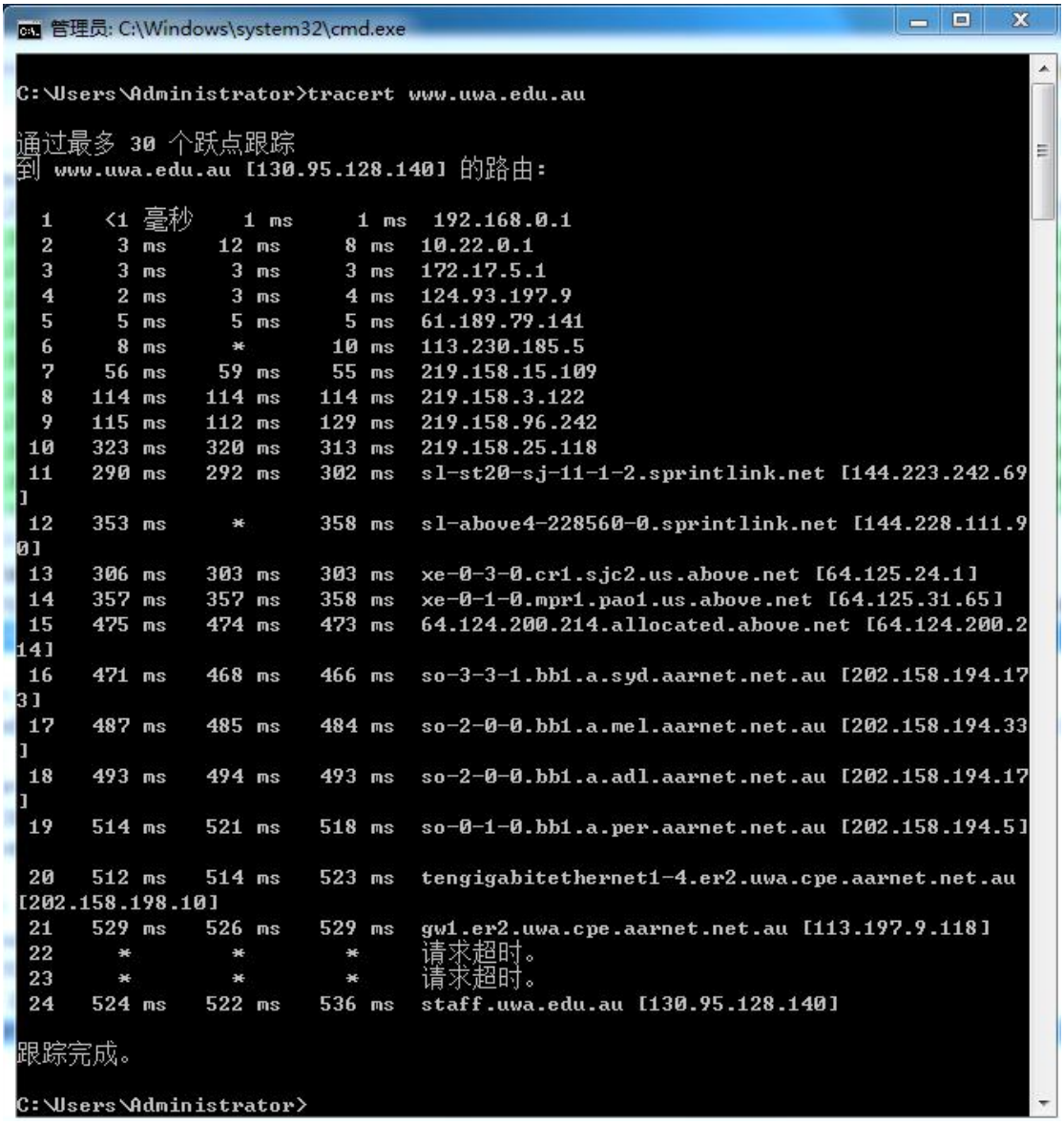
在 DOS 命令行下使用 wget 命令得到如下数据:

```
wget http://www.uwa.edu.au/
```

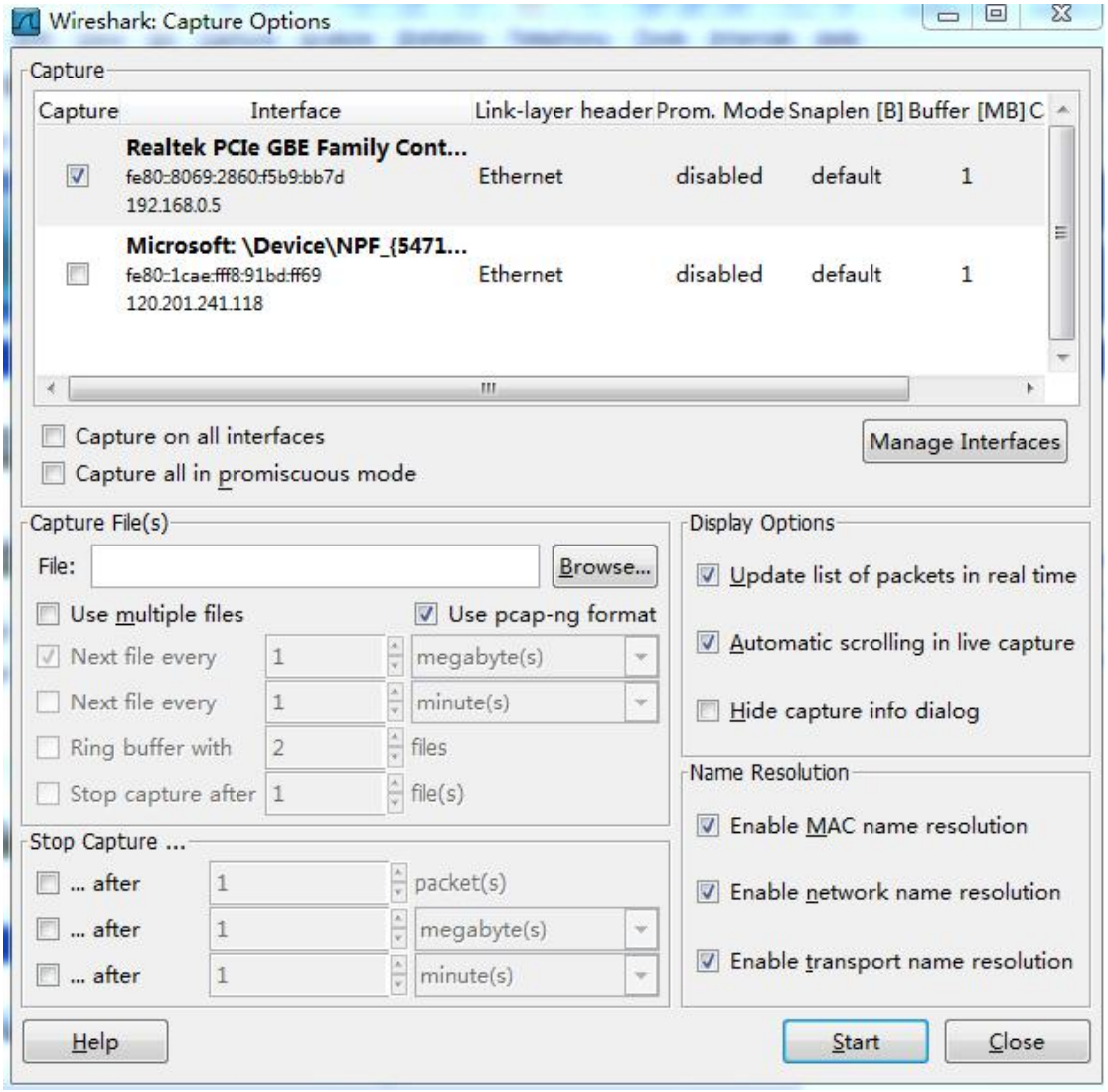


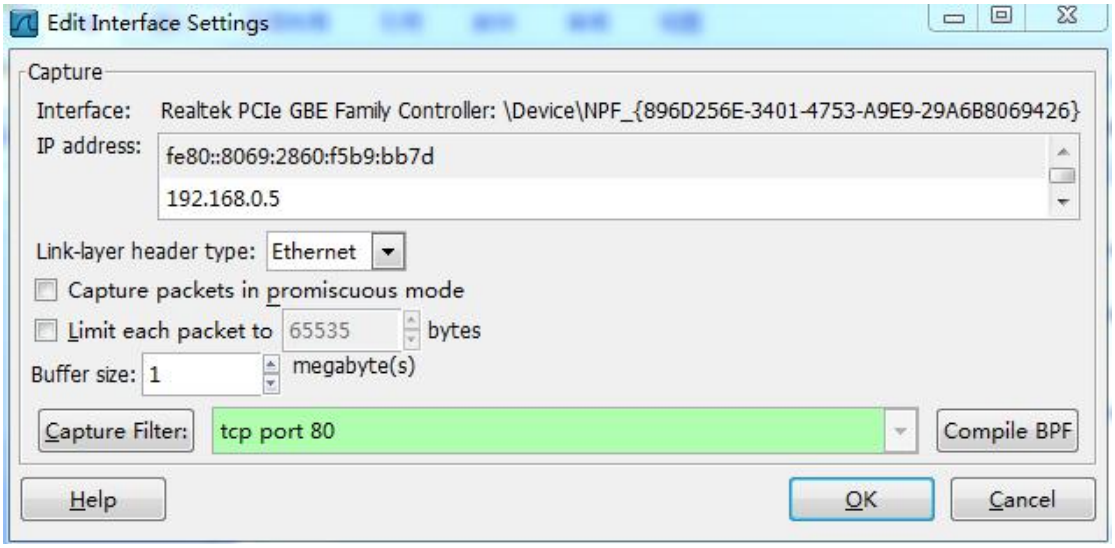
在 DOS 命令行下使用 tracert 命令得到如下数据:

```
tracert www.uwa.edu.au
```

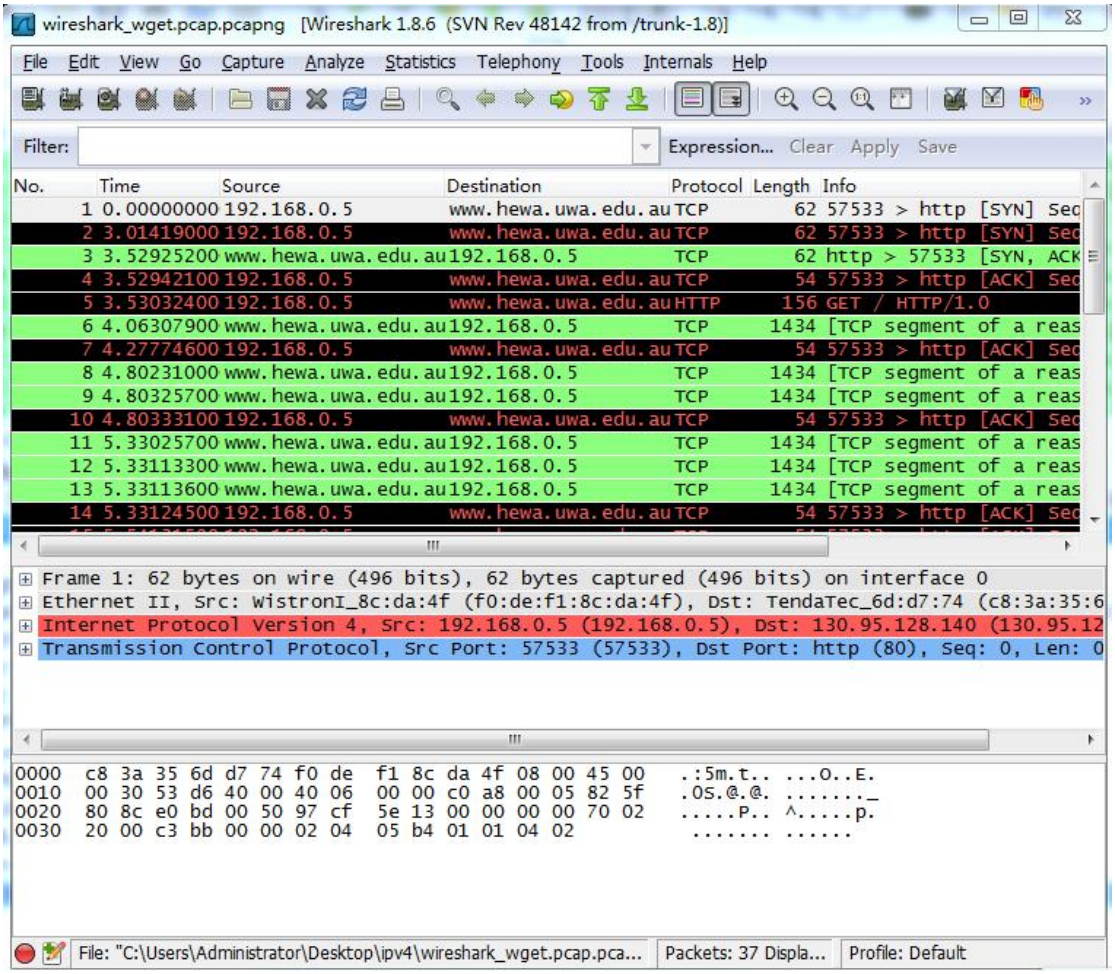


wireshark 中的设置项如下图所示，过滤掉其它类型的数据包只捕获 ip 数据包：

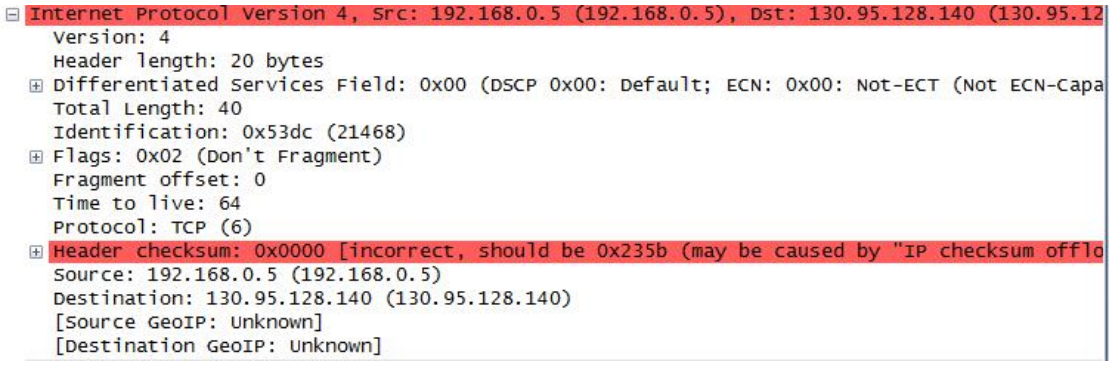




wireshark 设置完成后开始捕获数据，捕获到的数据如下:



2、数据分析：



上图所示即为 IP 数据报的格式：

Version：“4“说明此数据报通过 ipv4 发送/接收

Header length:IP 数据包头部的长度

Differentiated Services ： 区分服务

Total Length:数据包的总长度

Identification ： 标示

Flags:标志

Fragment offset ： 片偏移量
Time to live/TTL :生存周期
Protocol ： 协议
Header checksum ： 首部检验和
Source/ Destination :源/目的地址