**实验3 wireshark工具的基本使用方法**

**实验目的：**

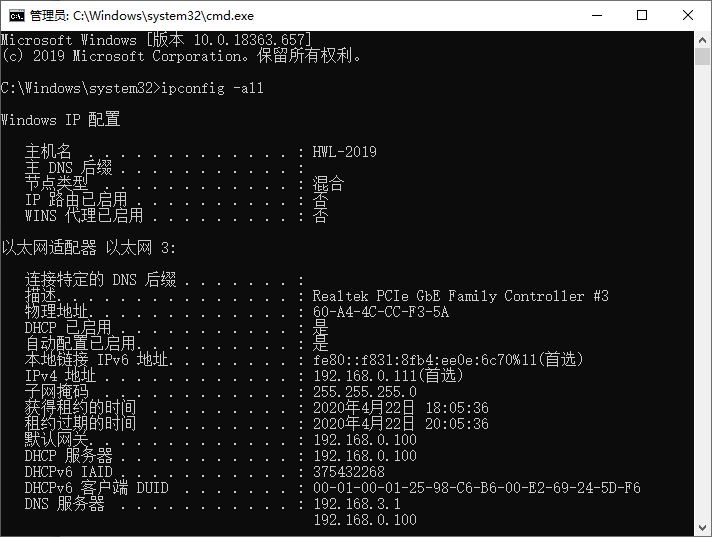
1、熟悉wireshark工具的主要用途。

2、掌握wireshark工具的基本使用方法。

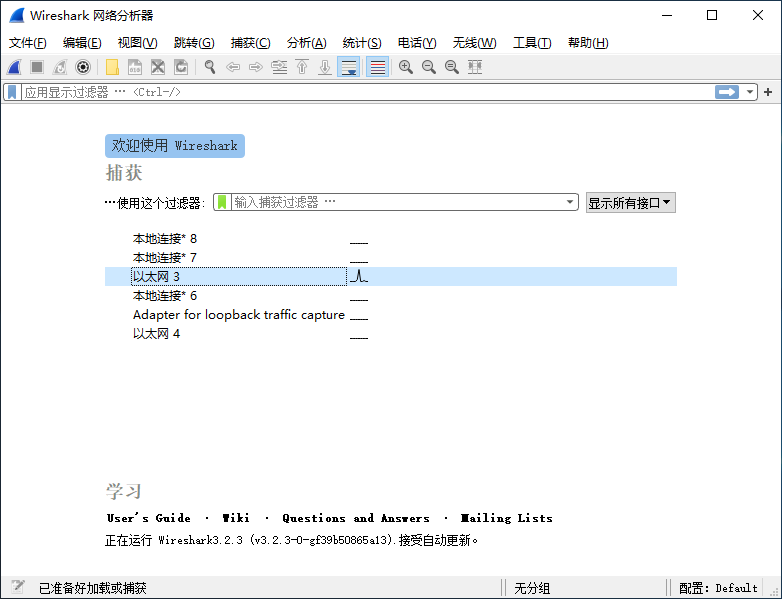
**实验步骤：**

1、下载wireshark抓包分析工具并安装。注意操作系统版本，特别是32位操作系统和64位操作系统的区别。建议用电脑安装，注意安装时的注意事项。苹果电脑请下载专用版本。

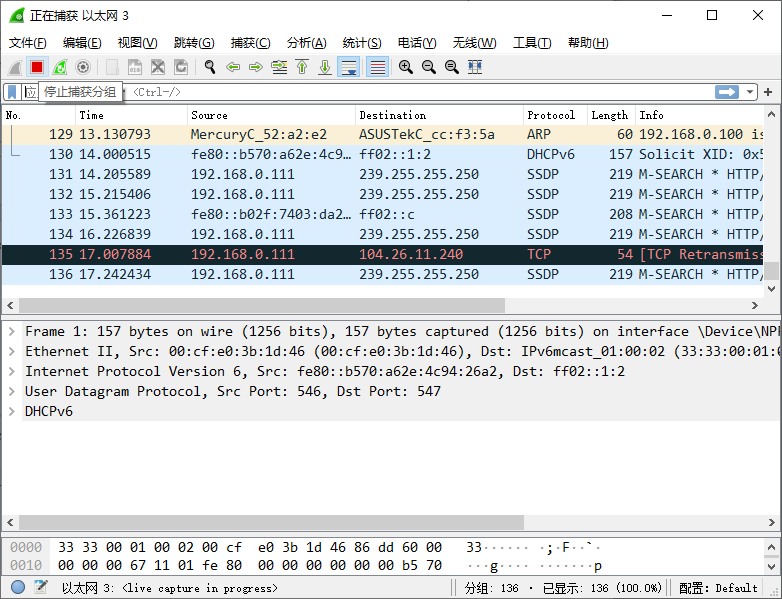
2、查看自己的IP地址和MAC地址。Windows系统用命令提示符查看，在运行中输入CMD，或在开始菜单“Windows附件”/“Windows系统”中打开命令提示符。在命令提示符中输入ipconfig -all，查看本机物理地址和IP地址。MAC系统在系统更偏好设置-网络-选择已连接网络查看本机物理地址和IP地址。



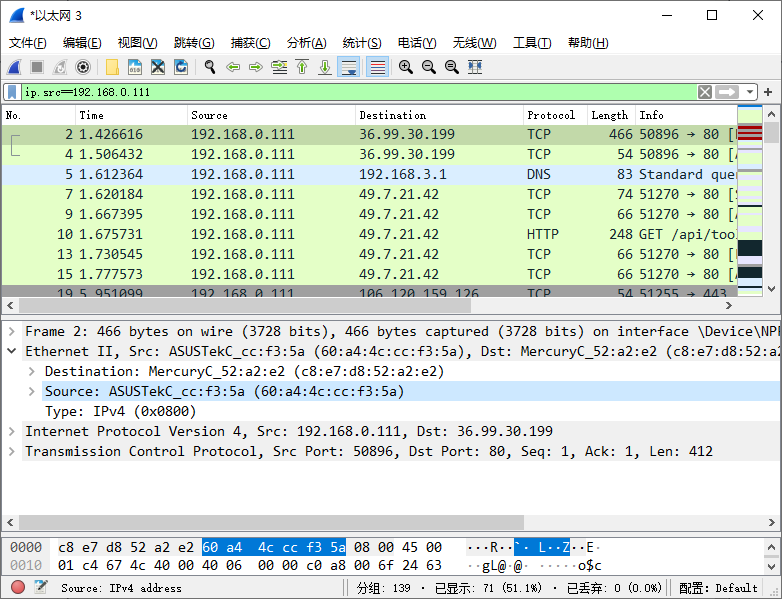
3、启动wireshark软件，选择准备捕获数据包的网卡接口。



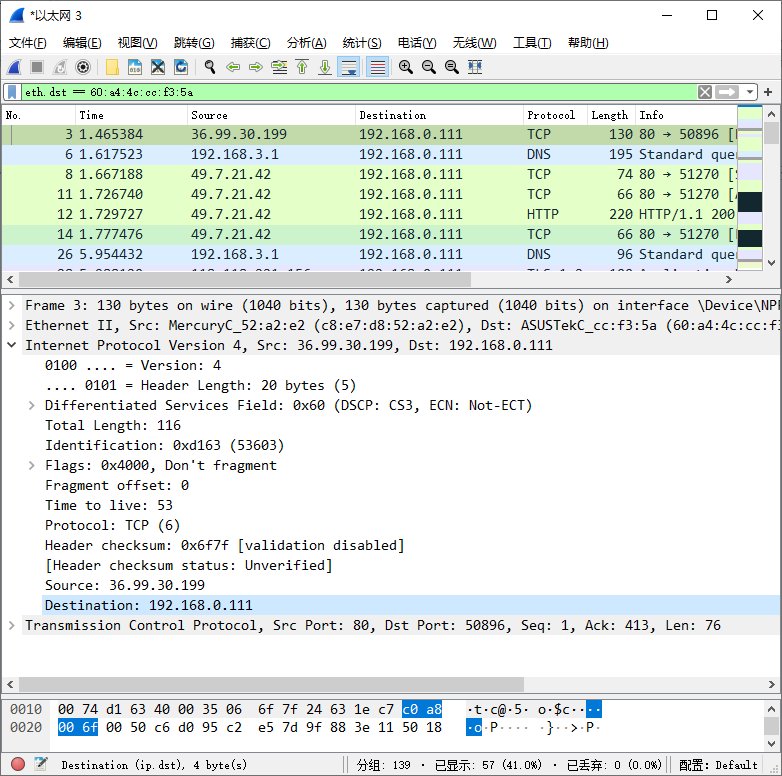
4、过几秒钟后停止捕获，观察捕获到的数据包。



5、在过滤条件中，选择查看自己IP地址发出的数据包，使用过滤条件“ip.src==步骤2中查看到的IP地址”，并在数据包详情窗口查看源MAC地址是否是步骤2中查看到的本机的物理地址。



6、重新设置过滤条件，选择查看由自己MAC地址接收的数据包，使用过滤条件“eth.dst == 步骤2中查看到的物理地址”（ 注意地址内16进制以冒号隔开），并在数据包详情窗口查看目的IP地址是否是自己的IP地址。



**思考题：**

1、每次自己发出或接收的数据包，自己的IP地址和MAC是否总是对应的？

2、尝试写一条规则，查找所有的HTTP协议的数据包。

3、尝试写一条规则，查找所有自己的IP地址发出的DNS数据包。

4、wireshark主要有哪些用途？