**实验报告**

实验人： 戴秋艳 学号： B15070708 实验时间： 2018.03.09

院系： 物联网 专业： 网络工程

实验题目： 使用Wireshark简单分析ICMP、ARP报文

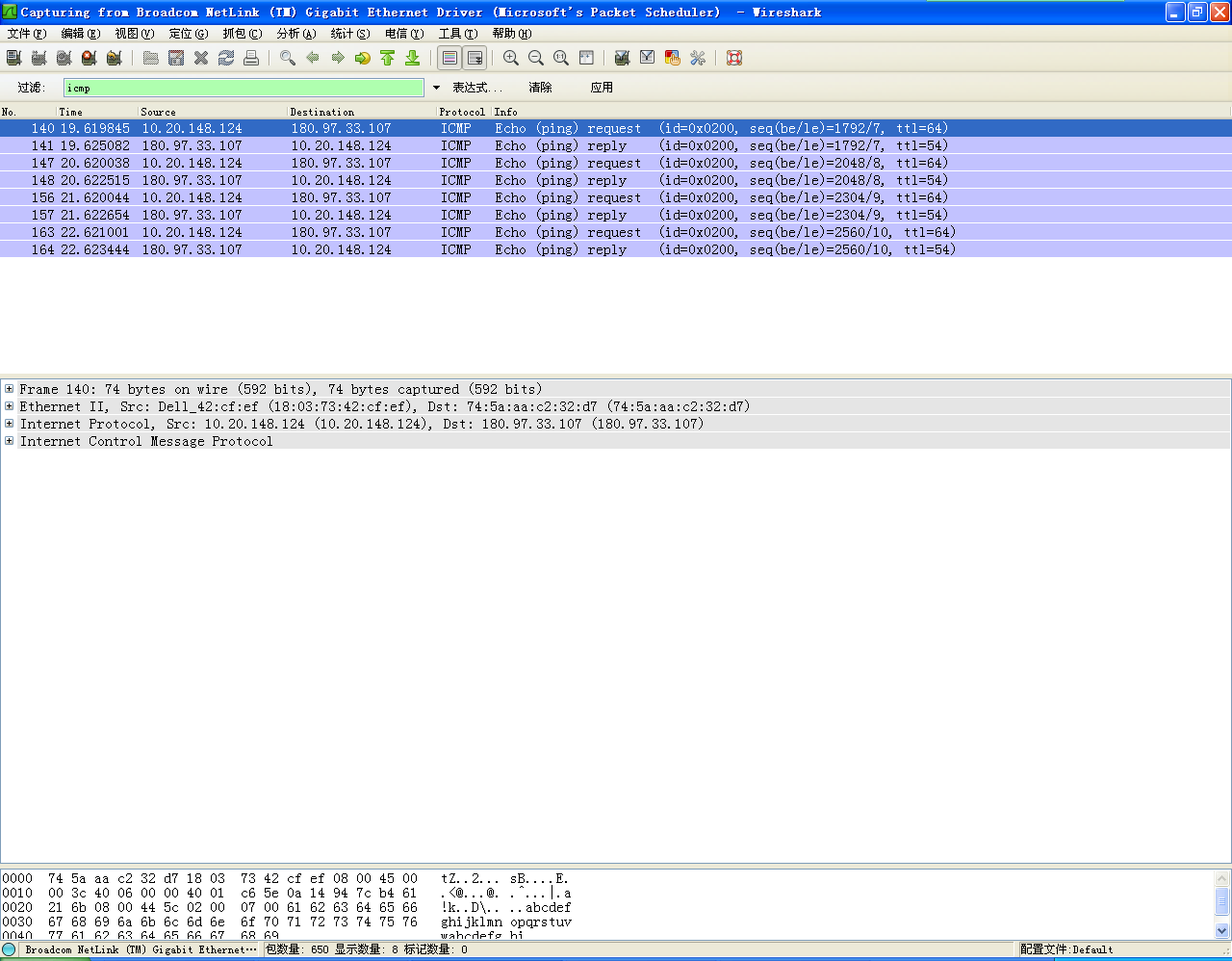
1. **实验目的：**
   1. 了解ICMP和ARP的原理
   2. 用Wireshark软件去分析ICMP和ARP报文
2. **实验内容：**
3. 实验器材：Wireshark软件
4. 实验原理：Wireshark:Wireshark 是网络包分析工具。网络包分析工具的主要作用是尝试获取网络包，并尝试显示包的尽可能详细的情况。网络包分析工具是一种用来测量有什么东西从网线上进出的测量工具，Wireshark 是最好的开源网络分析软件。

ICMP是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。ICMP报文作为IP层数据报的数据，加上数据报的首部，组成数据报发送出去。ICMP报文的种类有两种，即ICMP差错报告报文和ICMP询问报文。

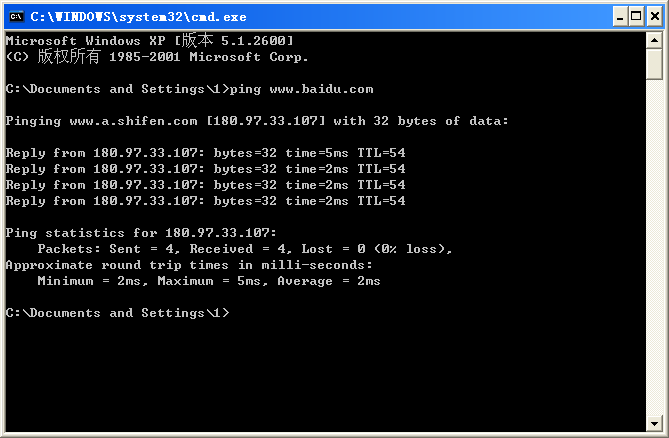
ARP根据IP地址获取物理地址的一个TCP/IP协议。ARP为IP地址到对应的硬件地址之间提供动态映射。主机发送信息时将包含目标IP地址的ARP请求广播到网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。地址解析协议是建立在网络中各个主机互相信任的基础上的，网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机ARP缓存。

1. **实验过程描述：**

首先打开Wireshark，设置过滤条件：icmp

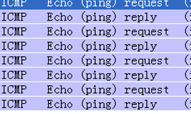


打开命令行窗口，执行命令：ping www.baidu.com



这时可以看到数据包抓取页面抓取到了8包，与命令行显示的已发送和已接受的包的数量是一致的：

在这个试验中，可以发现，icmp的报文就只有两种，请求和应答：



这两个报文的type不一样，8代表请求，0代表应答；code都为0，表示为回显应答；标示符和序列号都是一样的，表示这两个报文是配对的。

分析：ICMP是（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

各种ICMP报文的前32bits都是三个长度固定的字段：type类型字段(8位)、code代码字段(8位)、checksum校验和字段(16位) 8bits类型和8bits代码字段：一起决定了ICMP报文的类型。

常见的有：

类型0、代码0：回应应答。

类型3、代码0：网络不可达

类型3、代码1：主机不可达

类型5、代码1：为主机重定向数据包

类型8、代码0：回应

类型11、代码0：传输中超出TTL（常说的超时）

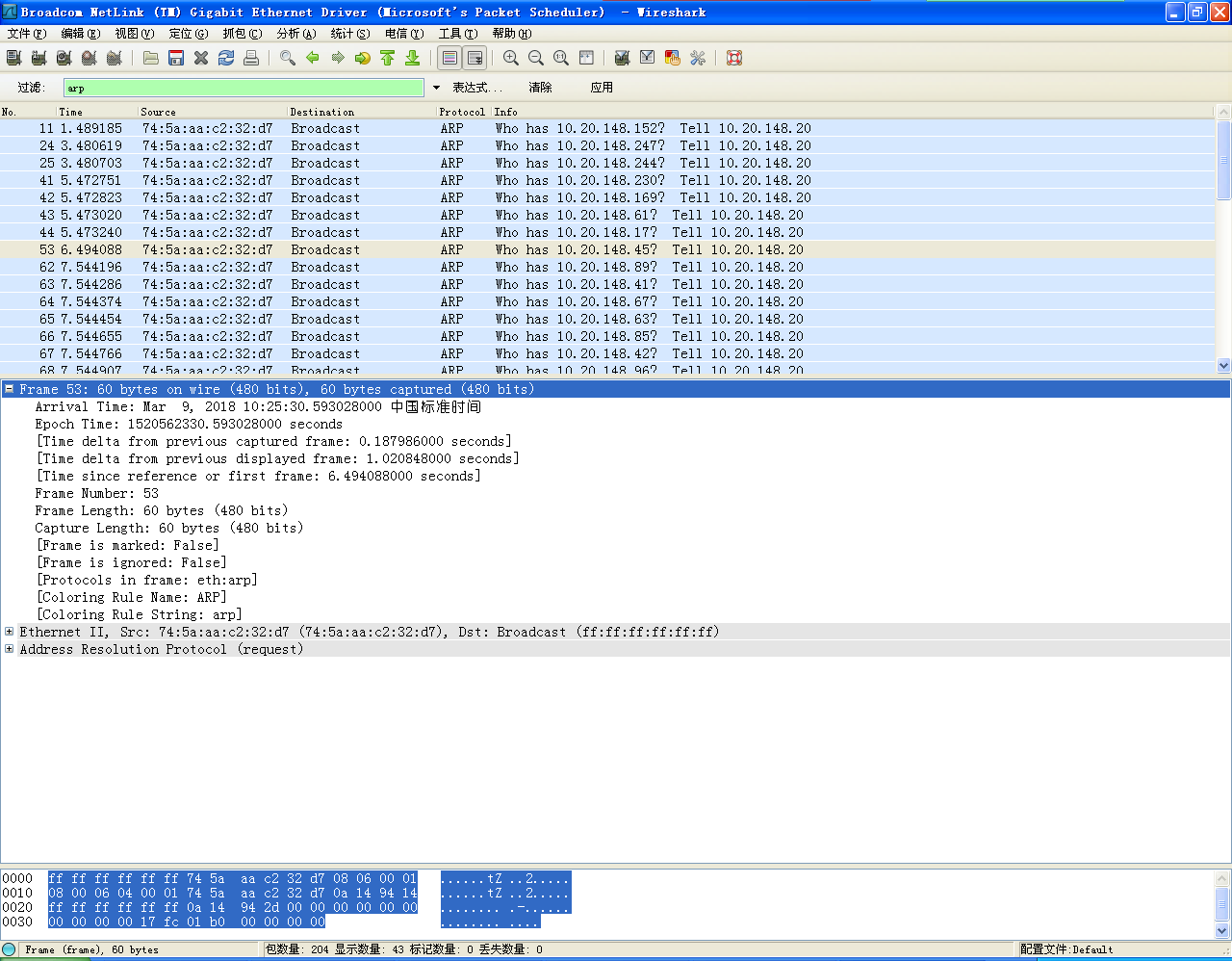
16bits校验和字段：包括数据在内的整个ICMP数据包的校验和，其计算方法和IP头部校验和的计算方法是一样的。

响应请求

我们日常使用最多的ping，就是响应请求（Type=8）和应答（Type=0），一台主机向一个节点发送一个Type=8的ICMP报文，如果途中没有异常（例如被路由器丢弃、目标不回应ICMP或传输失败），则目标返回Type=0的ICMP报文，说明这台主机存在，更详细的tracert通过计算ICMP报文通过的节点来确定主机与目标之间的网络距离

ARP协议

现在展开第一行：



帧在上图中我们看到这个帧的一些基本信息：

的编号：53（捕获时的编号）

帧的大小：60字节。

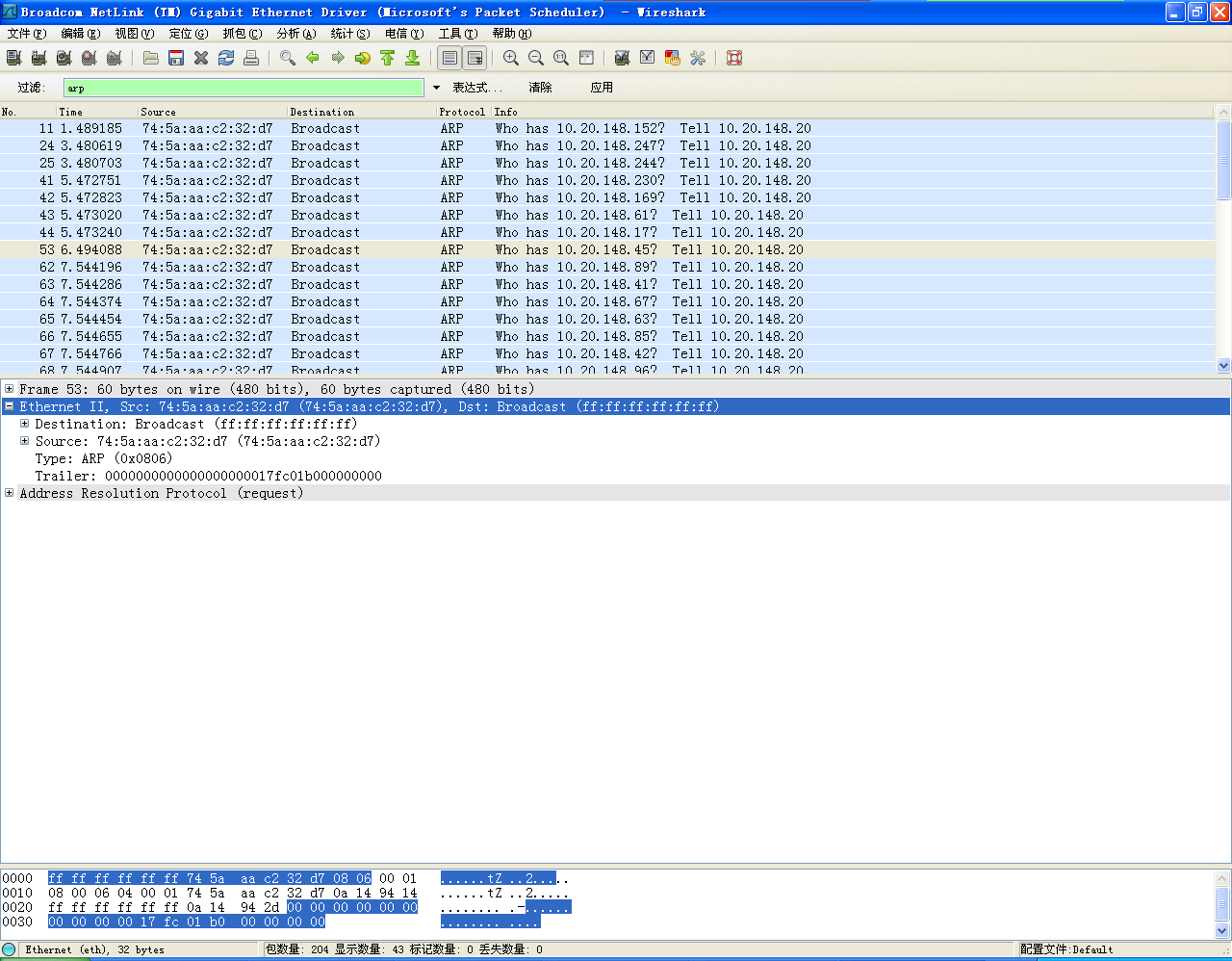
帧被捕获的日期和时间：Mar 9,2018……

帧距离前一个帧的捕获时间差：0.18……

帧距离第一个帧的显示时间差：1.02……

帧装载的协议：ARP

展开第二行

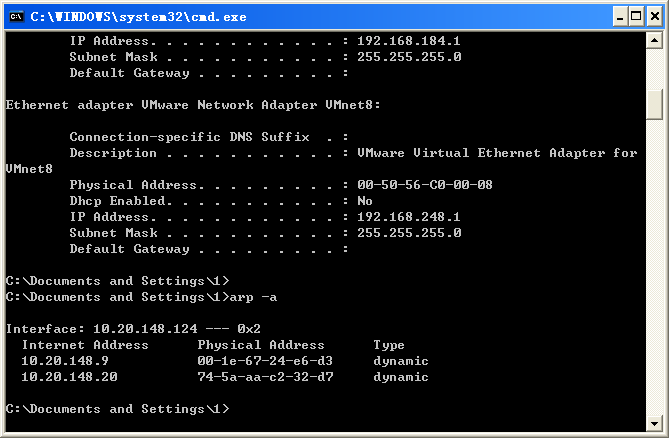
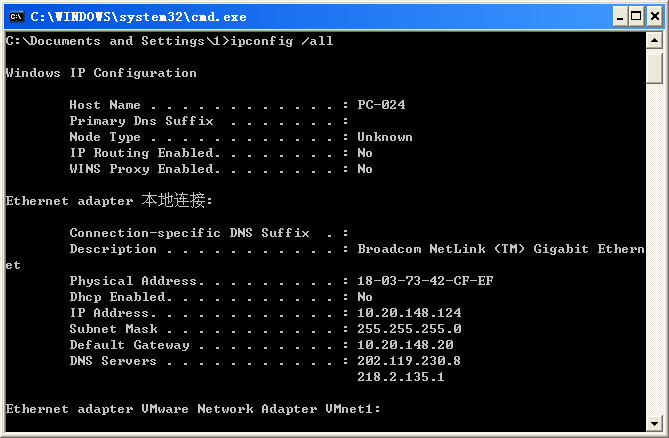


帧中封装的协议类型：0x0806，这个是ARP协议的类型编号。

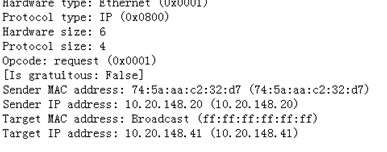
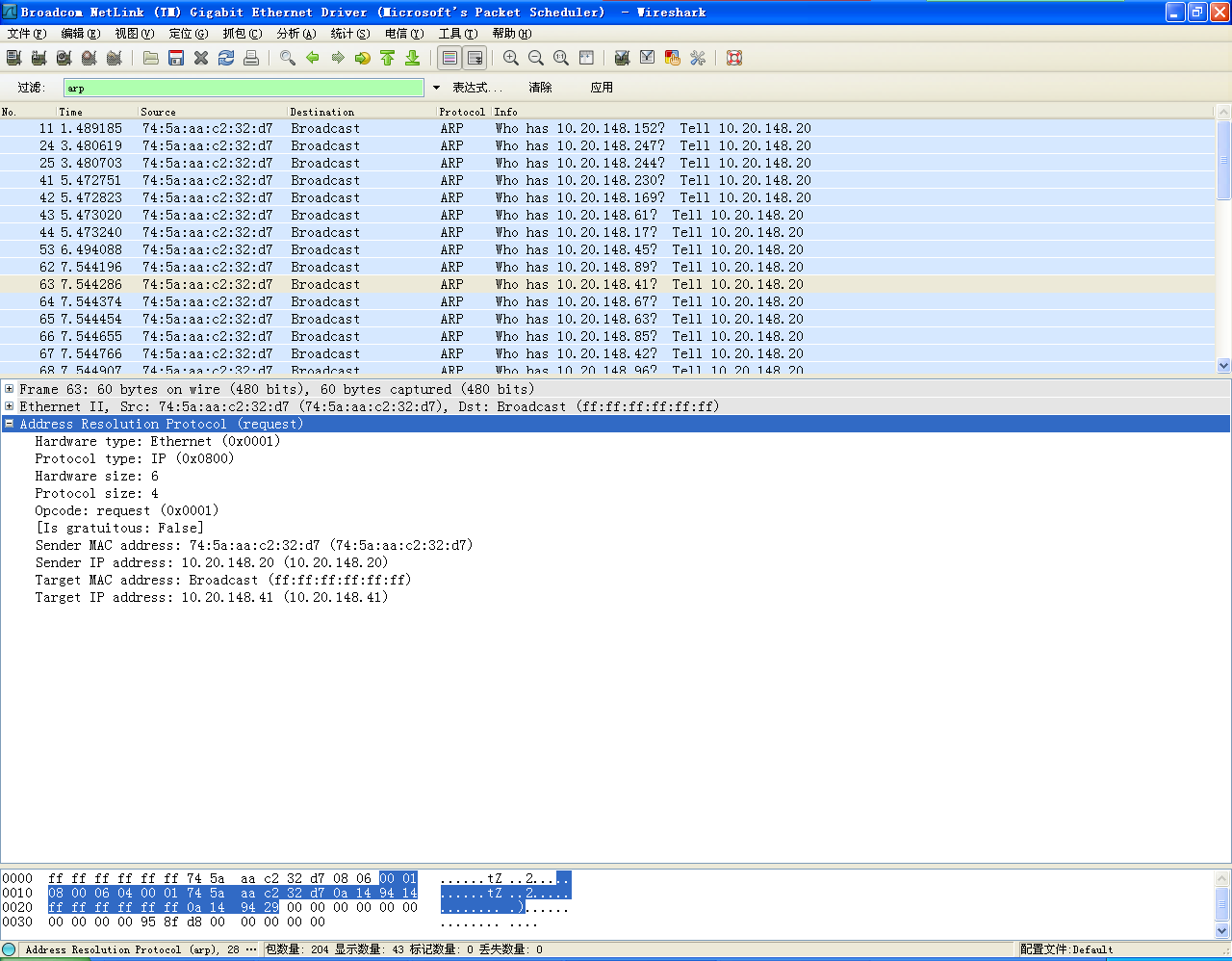
目的地址（Destination）：ff:ff:ff:ff:ff:ff（这是个MAC地址，这个MAC地址是一个广播地址，就是局域网中的所有计算机都会接收这个数据帧）

源地址（Source）：71:5a:aa:c2:32:d7 (74:5a:aa:c2:32:d7)

通过ipconfig/all，找到网关，然后arp –a（显示和本机通信了的一些机器的IP和MAC）



展开第三行

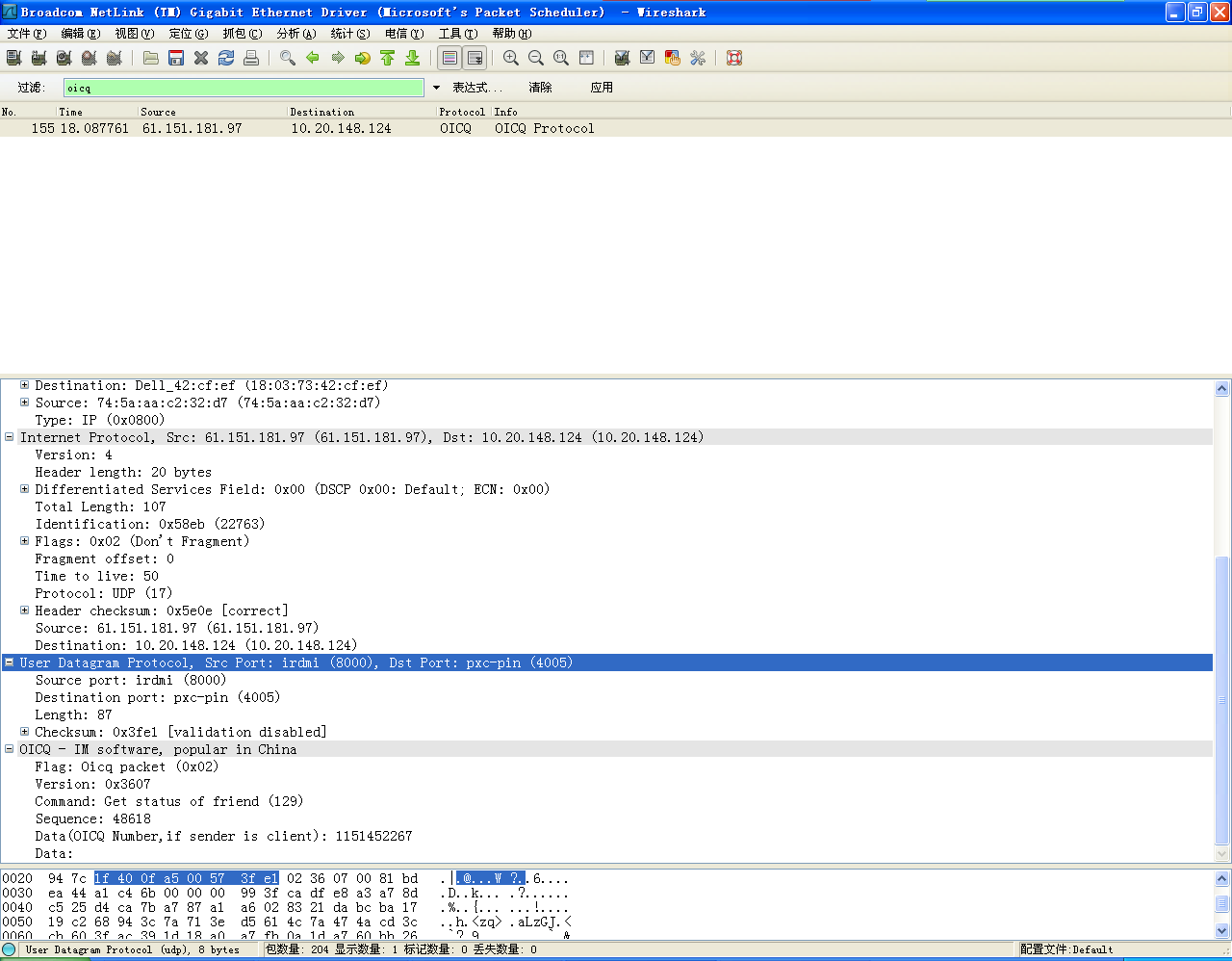


地址解析协议；硬件类型：以太网；协议类型：IP

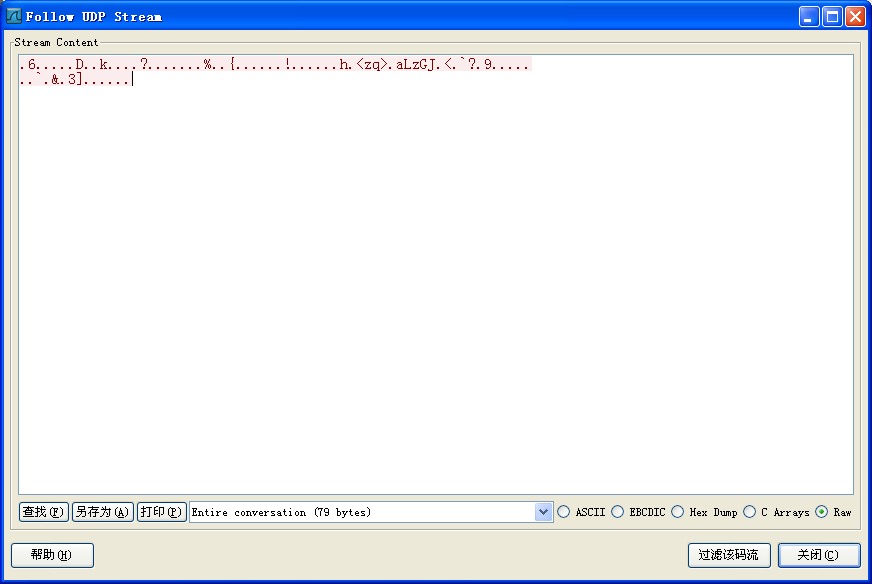
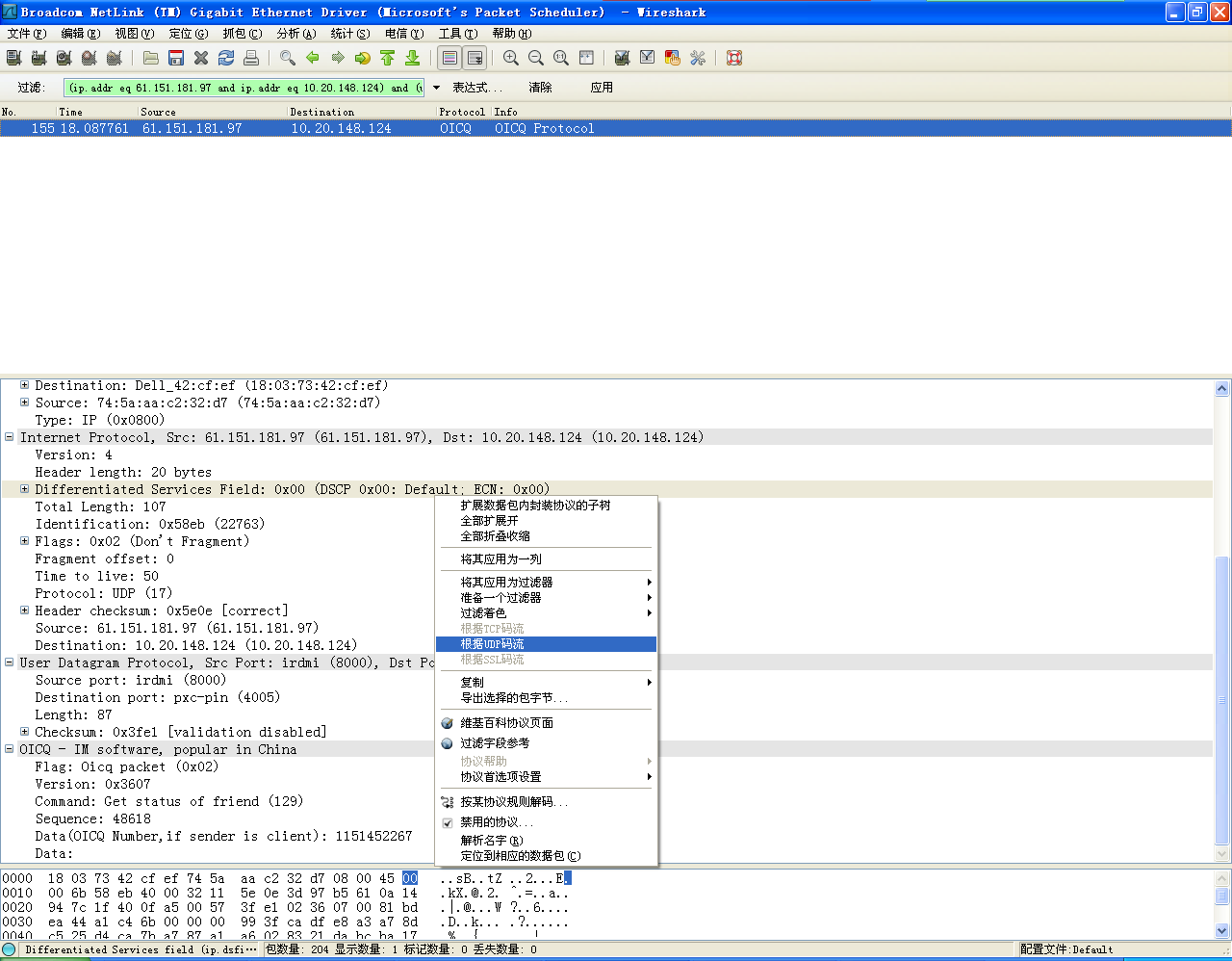
硬件大小：6；协议大小：4；发送方MAC地址

发送方IP地址；目的MAC地址；目的IP地址

看看qq每天做什么



查看传输数据 点鼠标右键，点“follow UDP stream（根据UDP码流）”可查看传输数据。



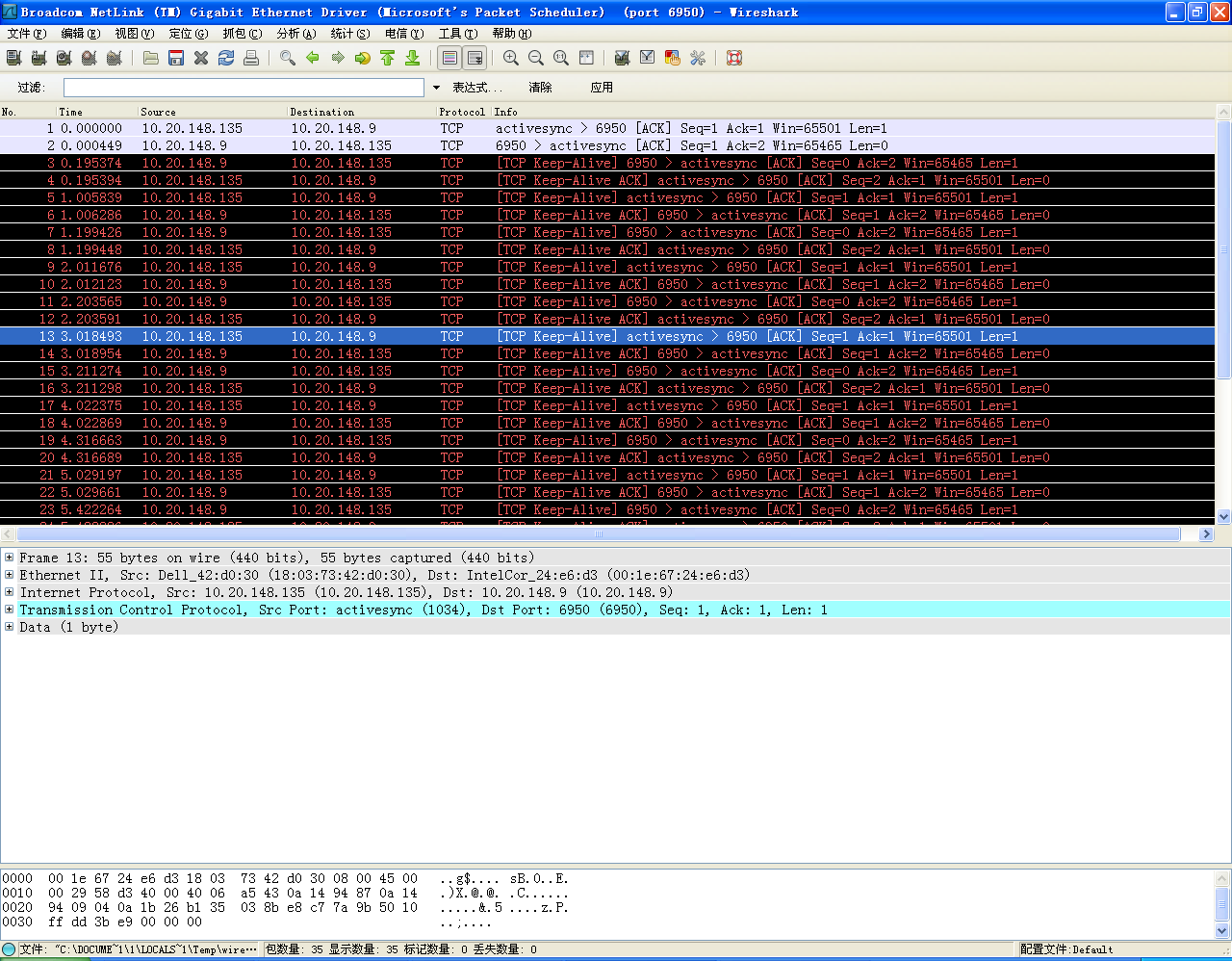
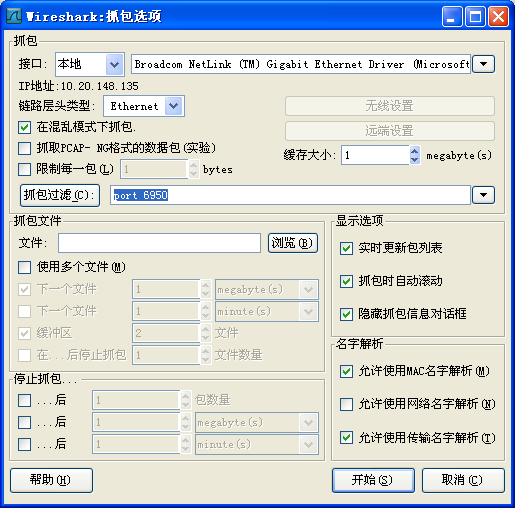
分析：QICQ是QQ的协议，此协议是基于UDP协议的。UDP是一种无连接的协议。从图中可以看到UDP包中源端口为irdmi（8000），这在国内主要是qq使用的端口号，目的端口为4001，长度为87，检验和显示验证禁止，不能验证。QICQ中可以看到自己的qq号码。通过查看“根据UDP码流”来查看数据传输，可以看出qq聊天内容是加密传送的，需要加密算法才能破解。

**四、实验小结**

本次抓包实验让我收获良多，尤其是让我意识到了书本上冷冰冰的网络协议和在网络上真实运行流动的各种各样的分层协作的协议是完全不一样的。通过本次实验，首先我熟悉了使用Wireshark的使用方法，学会了Wireshark软件捕获各协议报文包括协议序列和报文内容，并观察研究其工作原理，其中一些过滤统计的技巧也让实验变得更容易。然后，我透过对报文格式和各报文协同工作的分析，更加深入的ARP协议、ICMP协议的工作过程。最后，更是提高了多方面查找资料，结合自身所学理论，解决实际问题的能力。

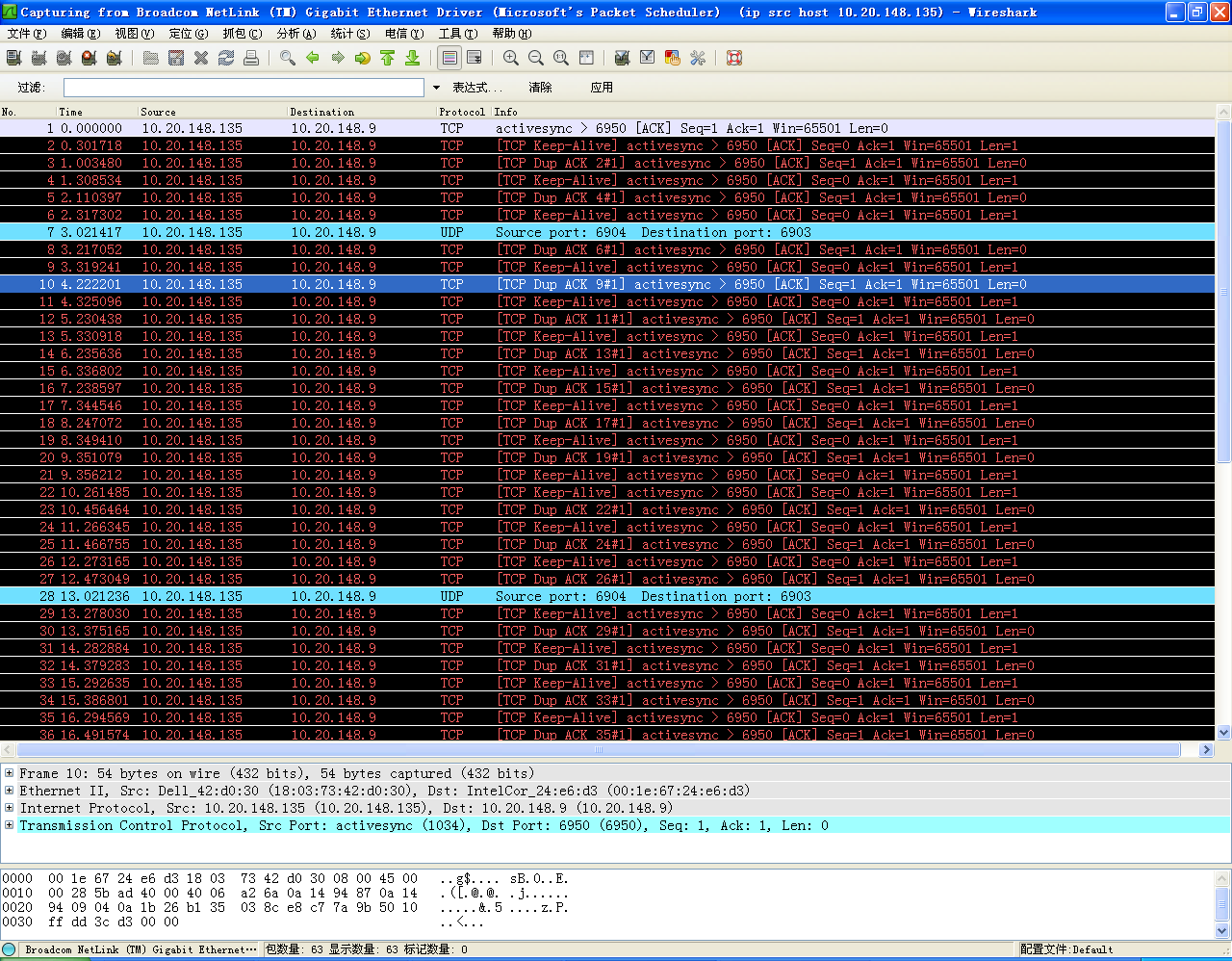
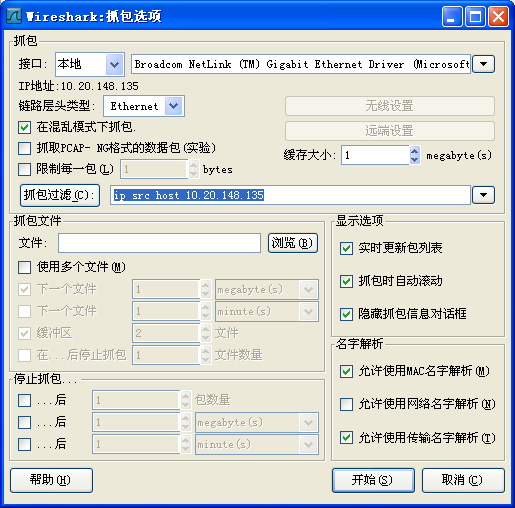
1、port 6950

显示目的TCP端口为6950的封包。



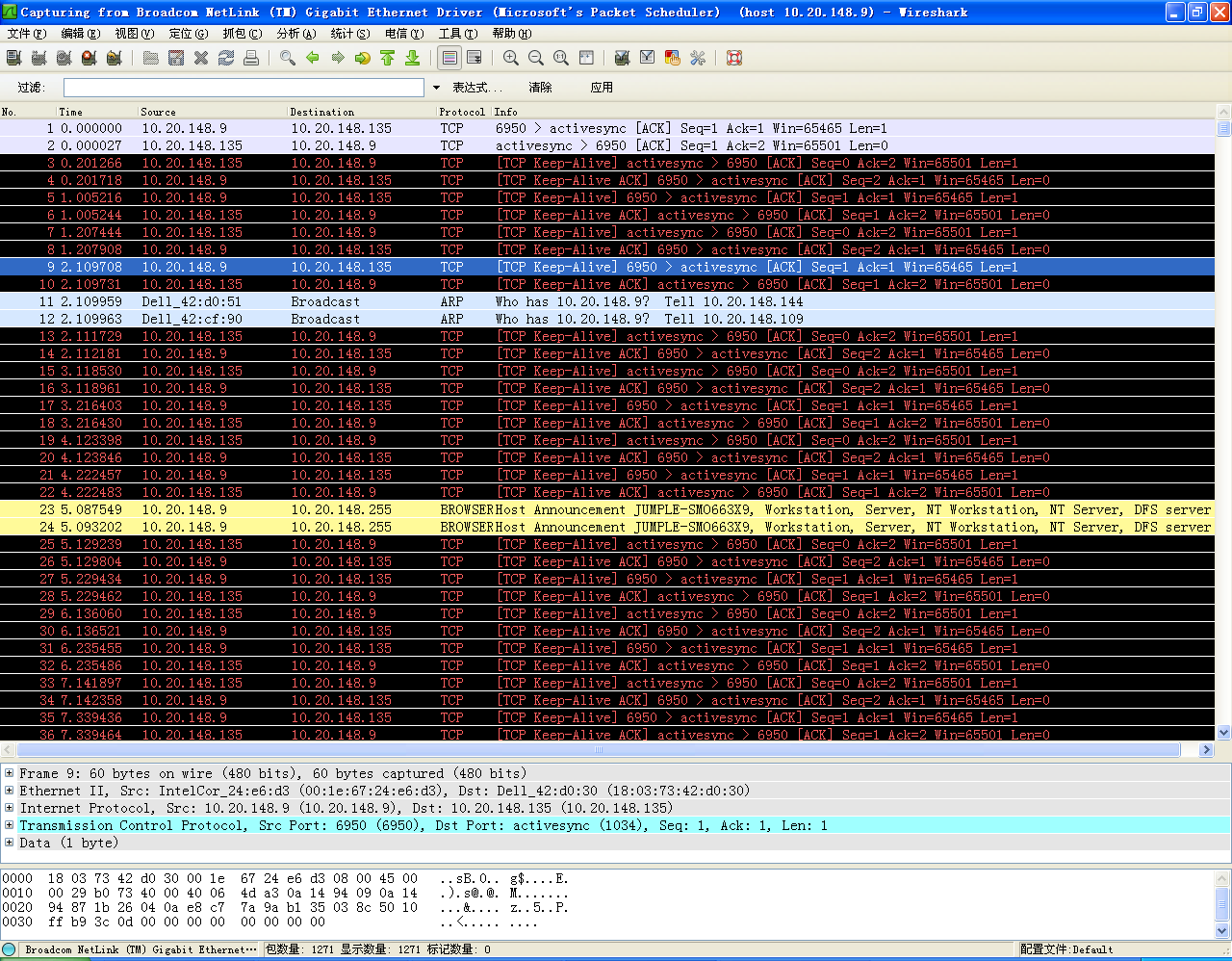
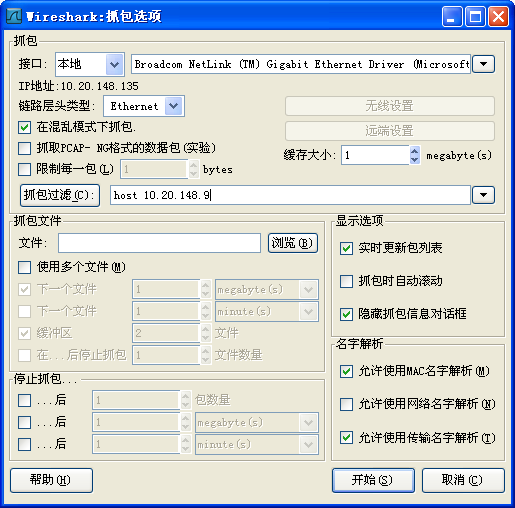
2、ip src host 10.20.148.135

显示来源IP地址为10.20.148.135的封包。



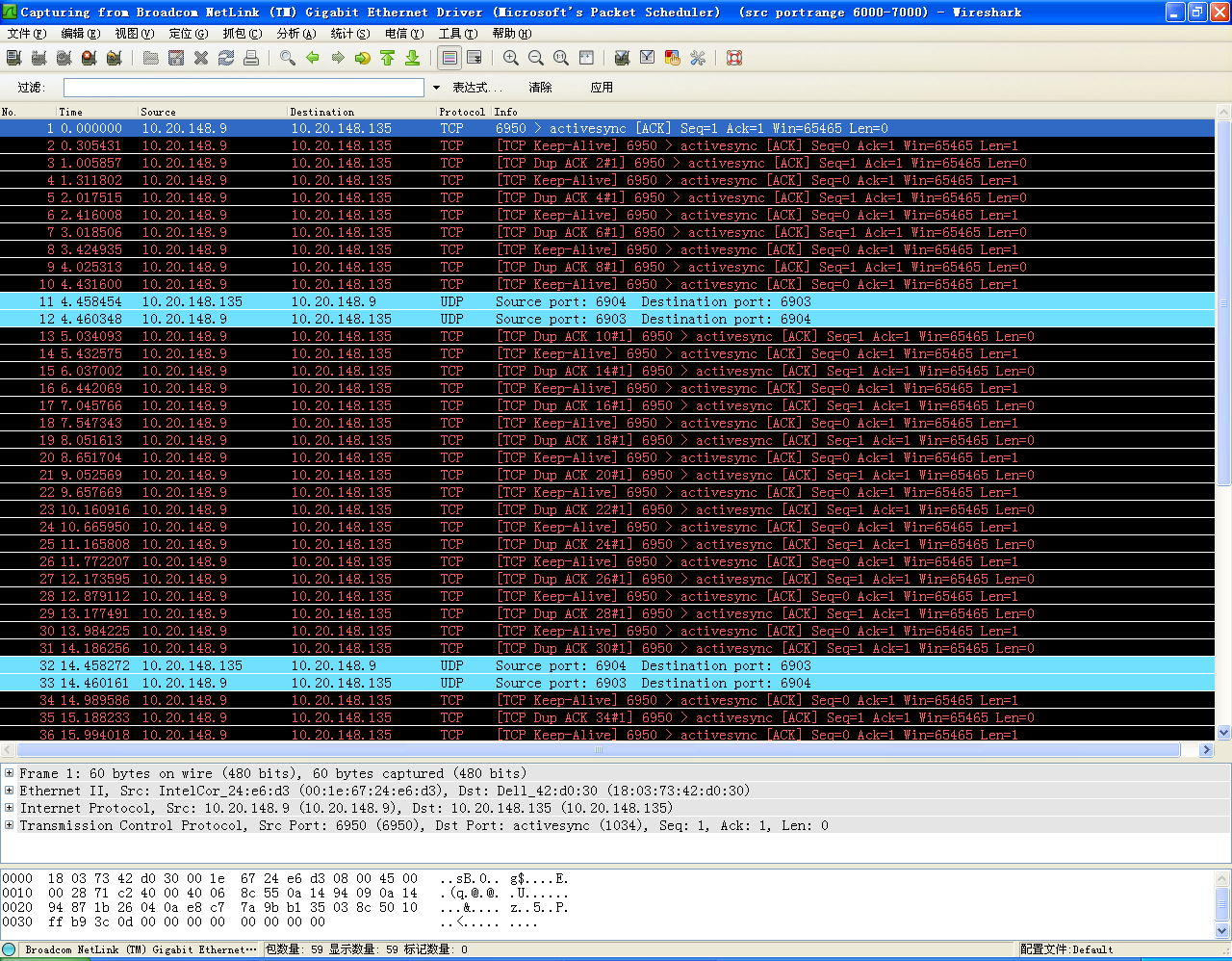
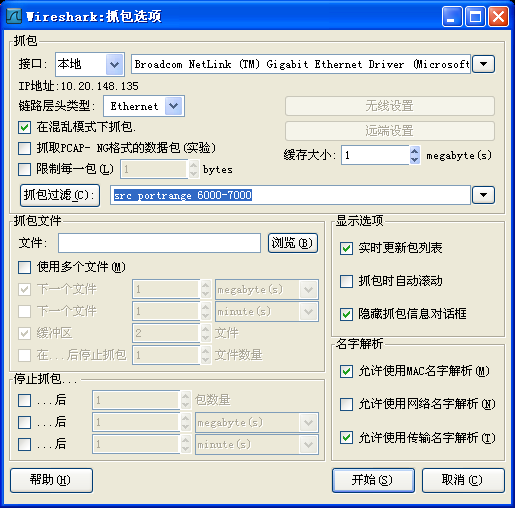
3、host 10.20.148.9

显示目的或来源IP地址为10.20.148.9的封包。

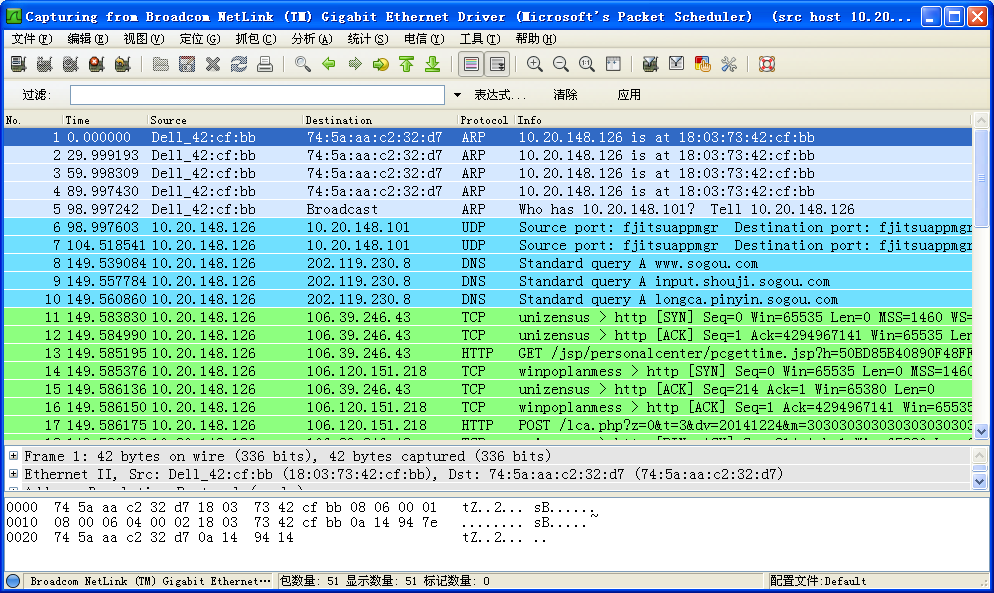
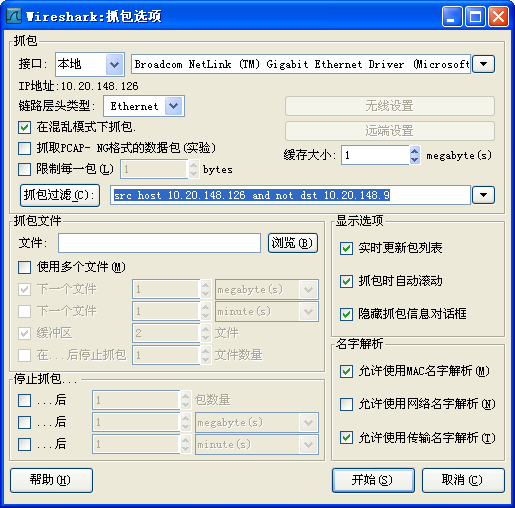


4、src portrange 6000-7000

显示来源为UDP或TCP，并且端口号在6000至7000范围内的封包。



5、src host 10.20.148.126 and not dst 10.20.148.9/16  
显示来源IP地址为10.20.148.126，但目的地不是10.20.148.9/16的封包。



6、src host10.20.148.124 and tcp dst portrange 200-10000

显示来源IP为10.20.148.124或者来源网络为10.6.0.0/16，目的地址TCP端口号在200至10000之间的所有封包。

