## 实验五.3 使用Wireshark分析以太网帧与ARP协议

**一、实验目的**

分析以太网帧，MAC地址和ARP协议

**二、实验环境**

与因特网连接的计算机网络系统；主机操作系统为windows；使用Wireshark、IE等软件。

**三、实验步骤：**

IP地址用于标识因特网上每台主机，而端口号则用于区别在同一台主机上运行的不同网络应用程序。在链路层，有介质访问控制（Media Access Control,MAC）地址。在局域网中，每个网络设备必须有唯一的MAC地址。设备监听共享通信介质以获取目标MAC地址与自己相匹配的分组。

Wireshark 能把MAC地址的组织标识转化为代表生产商的字符串，例如，00:06:5b:e3:4d:1a也能以Dell:e3:4d:1a显示，因为组织唯一标识符00:06:5b属于Dell。地址ff:ff:ff:ff:ff:ff是一个特殊的MAC地址，意味着数据应该广播到局域网的所有设备。

在因特网上，IP地址用于主机间通信，无论它们是否属于同一局域网。同一局域网间主机间数据传输前，发送方首先要把目的IP地址转换成对应的MAC地址。这通过地址解析协议ARP实现。每台主机以ARP高速缓存形式维护一张已知IP分组就放在链路层帧的数据部分，而帧的目的地址将被设置为ARP高速缓存中找到的MAC地址。如果没有发现IP地址的转换项，那么本机将广播一个报文，要求具有此IP地址的主机用它的MAC地址作出响应。具有该IP地址的主机直接应答请求方，并且把新的映射项填入ARP高速缓存。

发送分组到本地网外的主机，需要跨越一组独立的本地网，这些本地网通过称为网关或路由器的中间机器连接。网关有多个网络接口卡，用它们同时连接多个本地网。最初的发送者或源主机直接通过本地网发送数据到本地网关，网关转发数据报到其它网关，直到最后到达目的主机所在的本地网的网关。

1、俘获和分析以太网帧

（1）选择 工具->Internet 选项->删除文件

（2）启动Wireshark 分组嗅探器

（3）在浏览器地址栏中输入如下网址：

<http://gaia.cs.umass.edu/wireshark-labs> 会出现wireshark实验室主页。

（4）停止分组俘获。在俘获分组列表中（listing of captured packets）中找到HTTP GET 信息和响应信息，如图1所示。 。

HTTP GET信息被封装在TCP分组中，TCP分组又被封装在IP数据报中，IP数据报又被封装在以太网帧中）。在分组明细窗口中展开Ethernet II信息（packet details window）。

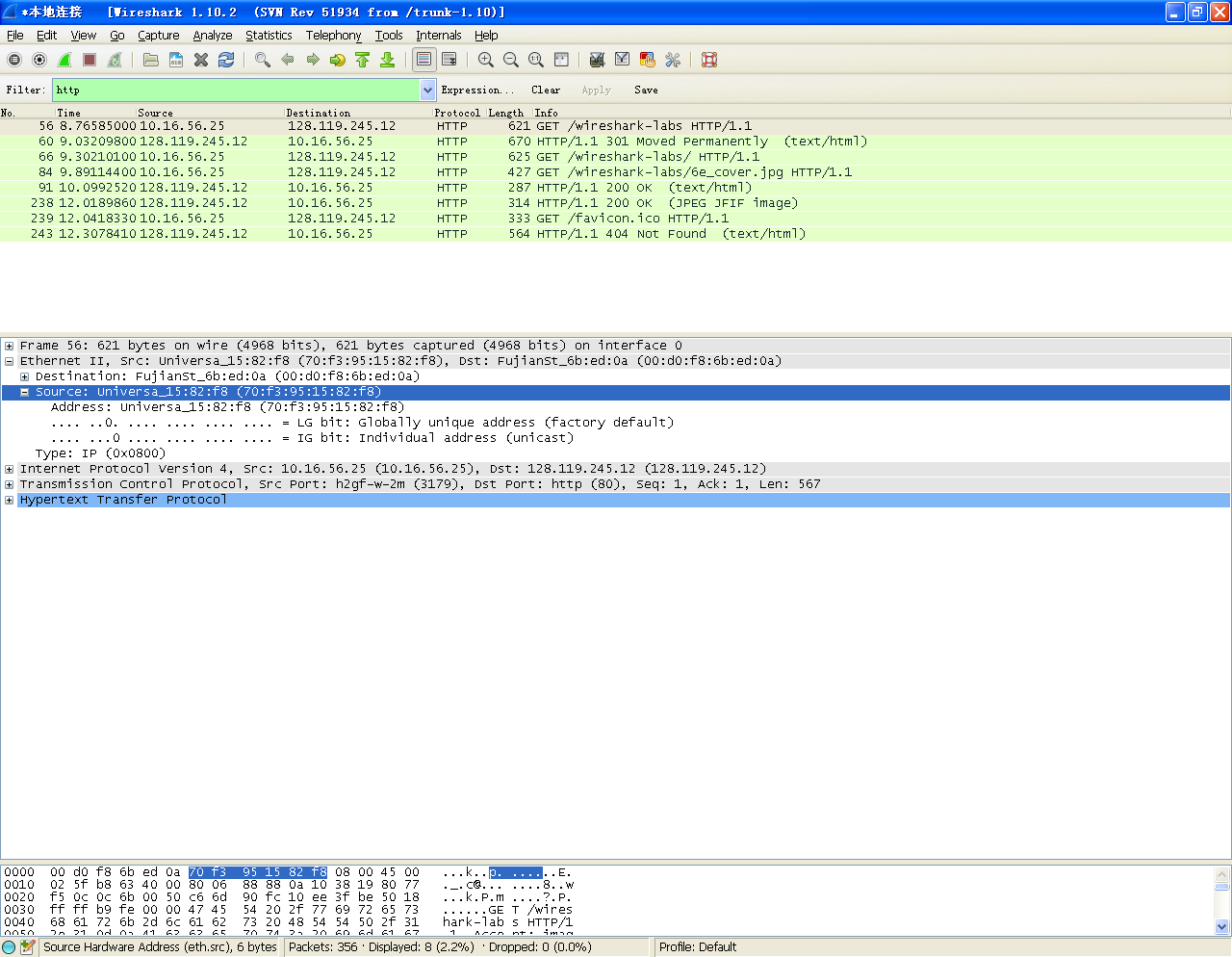


图2.1　HTTP GET信息和响应信息

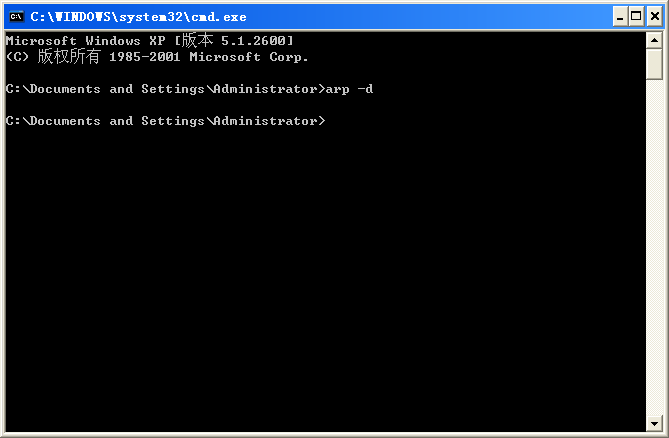
2、分析地址ARP协议

(1)ARP Caching

ARP协议用于将目的IP转换为对应的MAC地址。Arp命令用来观察和操作缓存中的内容。虽然arp命令和ARP有一样的名字，很容易混淆，但它们的作用是不同的。在命令提示符下输入arp可以看到在你所在电脑中ARP缓存中的内容。为了观察到你所在电脑发送和接收ARP信息，我们需要清除ARP缓存，否则你所在主机很容易找到已知IP和匹配的MAC地址。

步骤如下：

1. 清除ARP cache，具体做法：在MSDOS环境下，输入命令arp –d.



（2）选择 工具->Internet 选项->删除文件

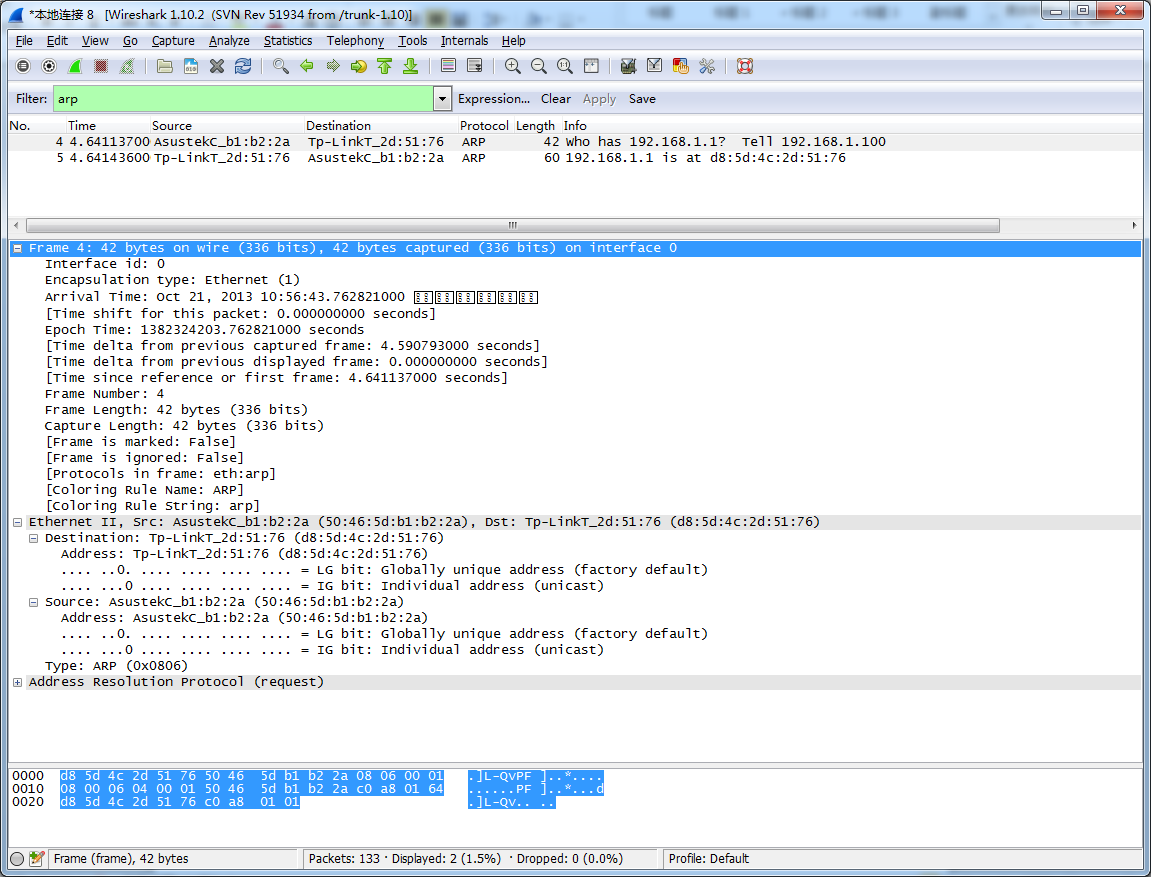
（3）启动Wireshark分组俘获器

（4）在浏览器地址栏中输入如下网址：

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html

（5）停止分组俘获。

（6）选择 Analyze->Enabled Protocols->取消IP选项->选择OK。如图3所示：



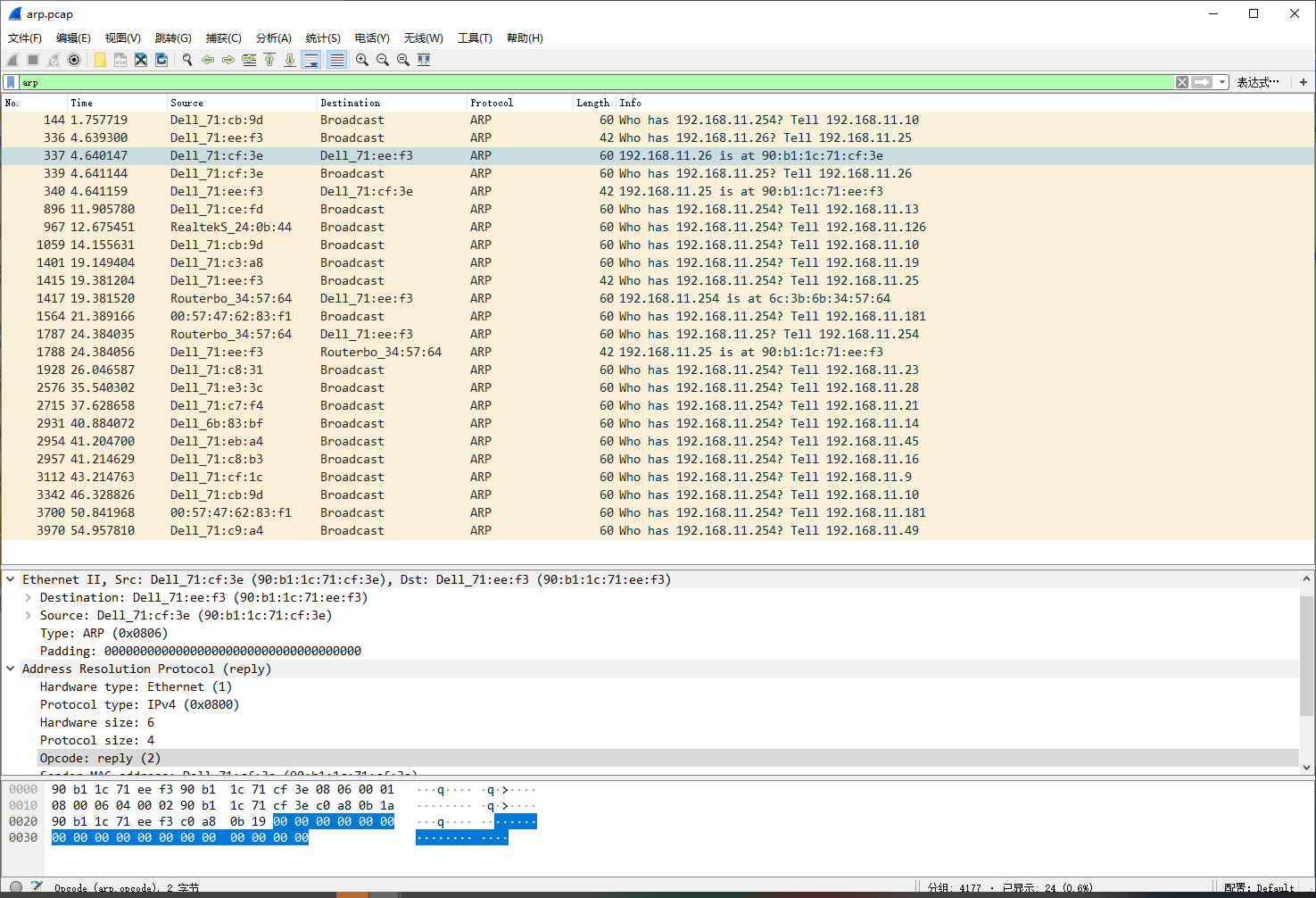
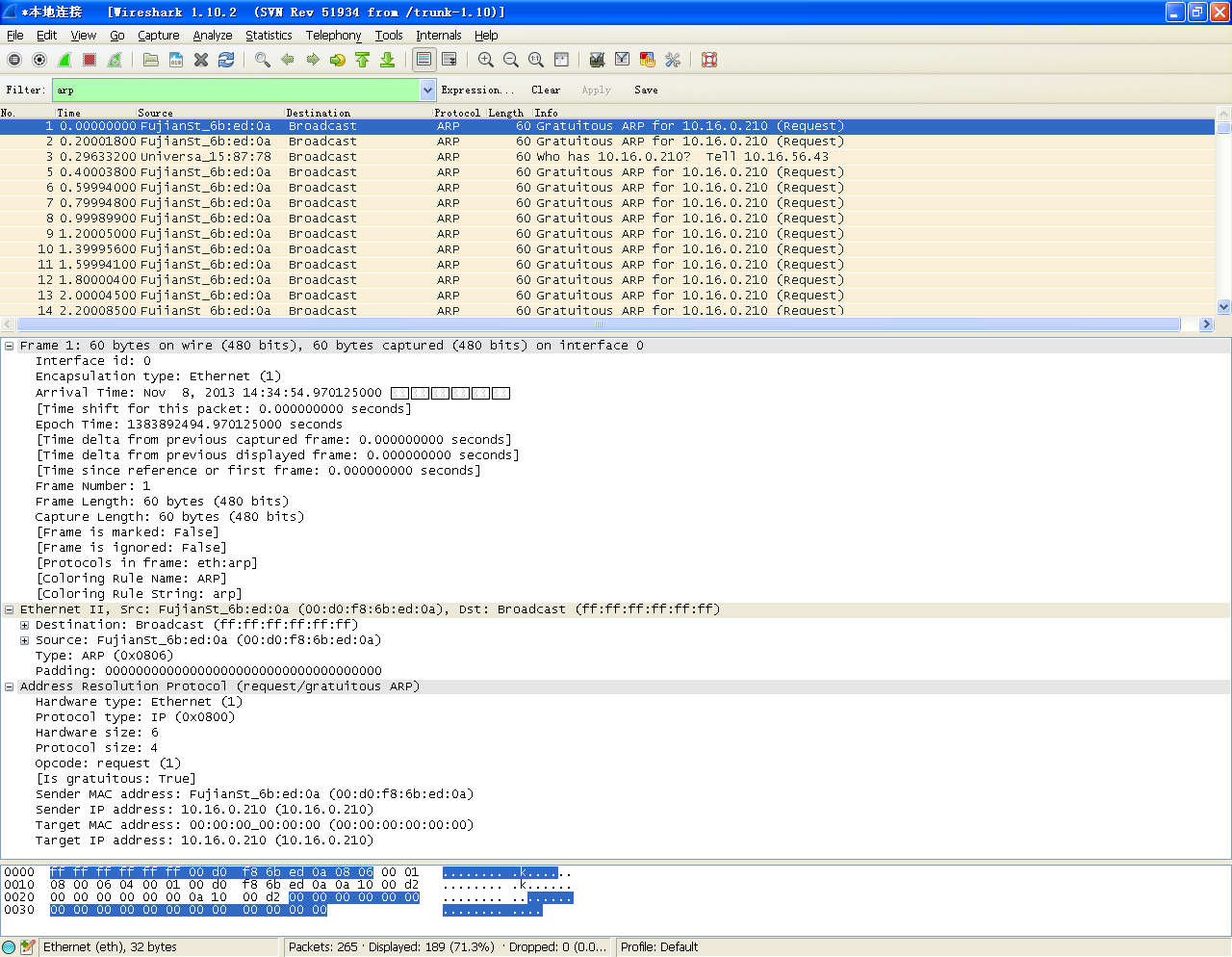


图2.2 利用Wireshark俘获的ARP分组

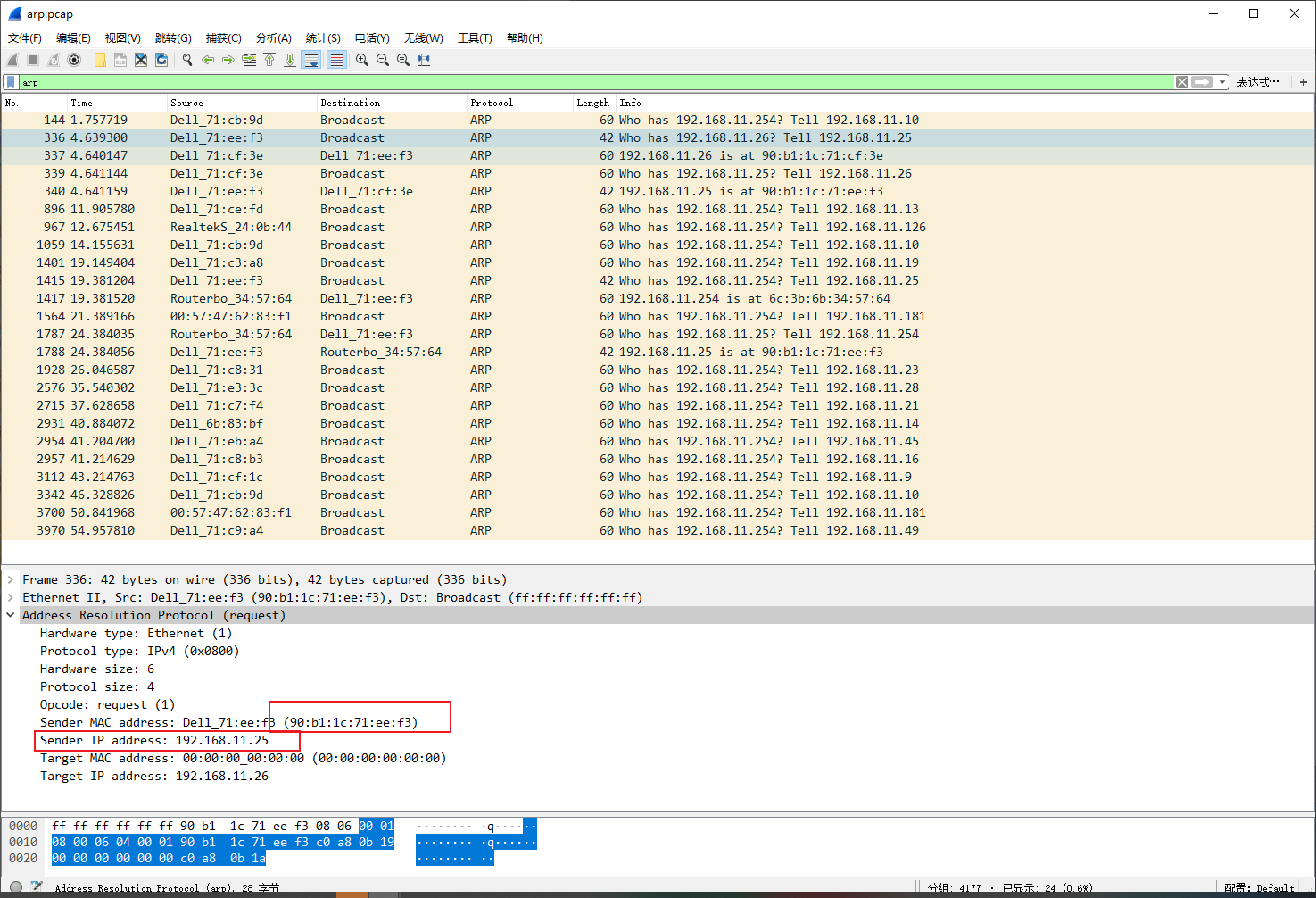


**四、实验报告**

根据实验，回答下面问题：

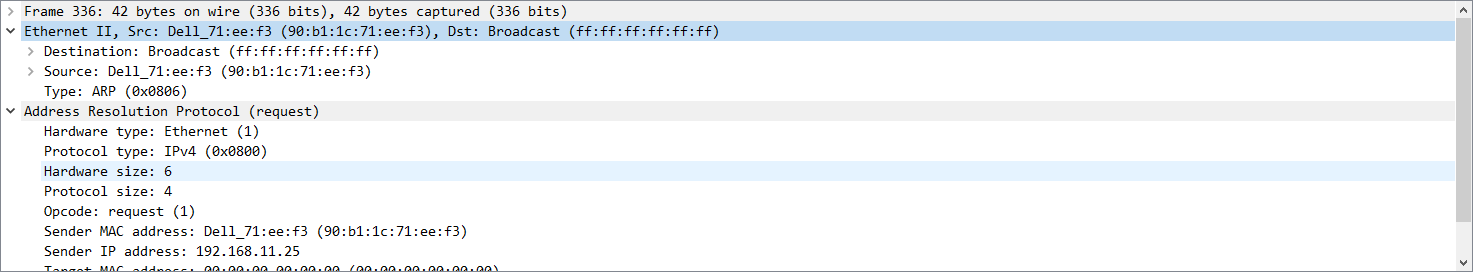
回答下面的问题：

1. 你所在的主机48-bit Ethernet 地址是多少？



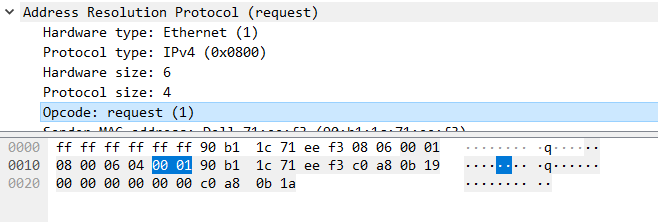
98:b1:1c:71:ee:f3

1. 包含ARP 请求消息的以太帧的十六进制目的地和源地址是什么？



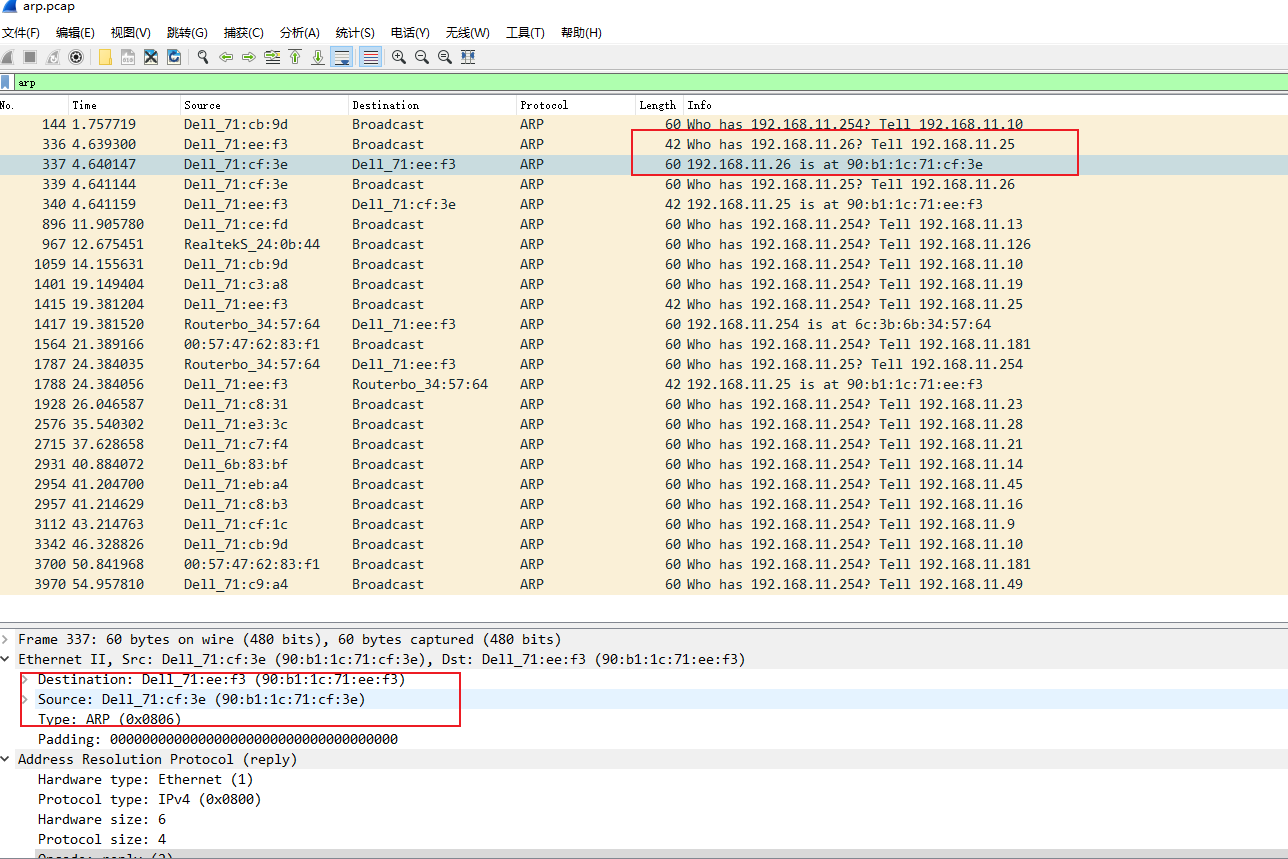
目的：ff:ff:ff:ff:ff:ff 源地址：90:b1:1c:71:ee:f3

1. ARP 操作码出现在以太帧从最前端开始的第几字节？（操作码：Opcode）



21

1. 包含ARP 响应消息的以太帧的十六进制目的地和源地址是什么？



Destination: Dell 71: ee: f3(90: b1: 1c: 71: ee: f3)

Source: Dell 71: cf: 3e(90: b1: 1c: 71: cf: 3e)