**计算机网络以太网和ARP实验报告**

**姓名：陈鹤影 学号：PB21061287 日期：2022.12.4**

1. **实验目的：**
2. **了解以太网协议及ARP协议。**
3. **学会分析ARP请求和响应报文。**
4. **学会分析链路层帧的结构。**
5. **了解MAC地址与IP地址各自的功能。**
6. **学会使用arp命令查看和修改ARP缓存。**
7. **实验流程及问题回答：**

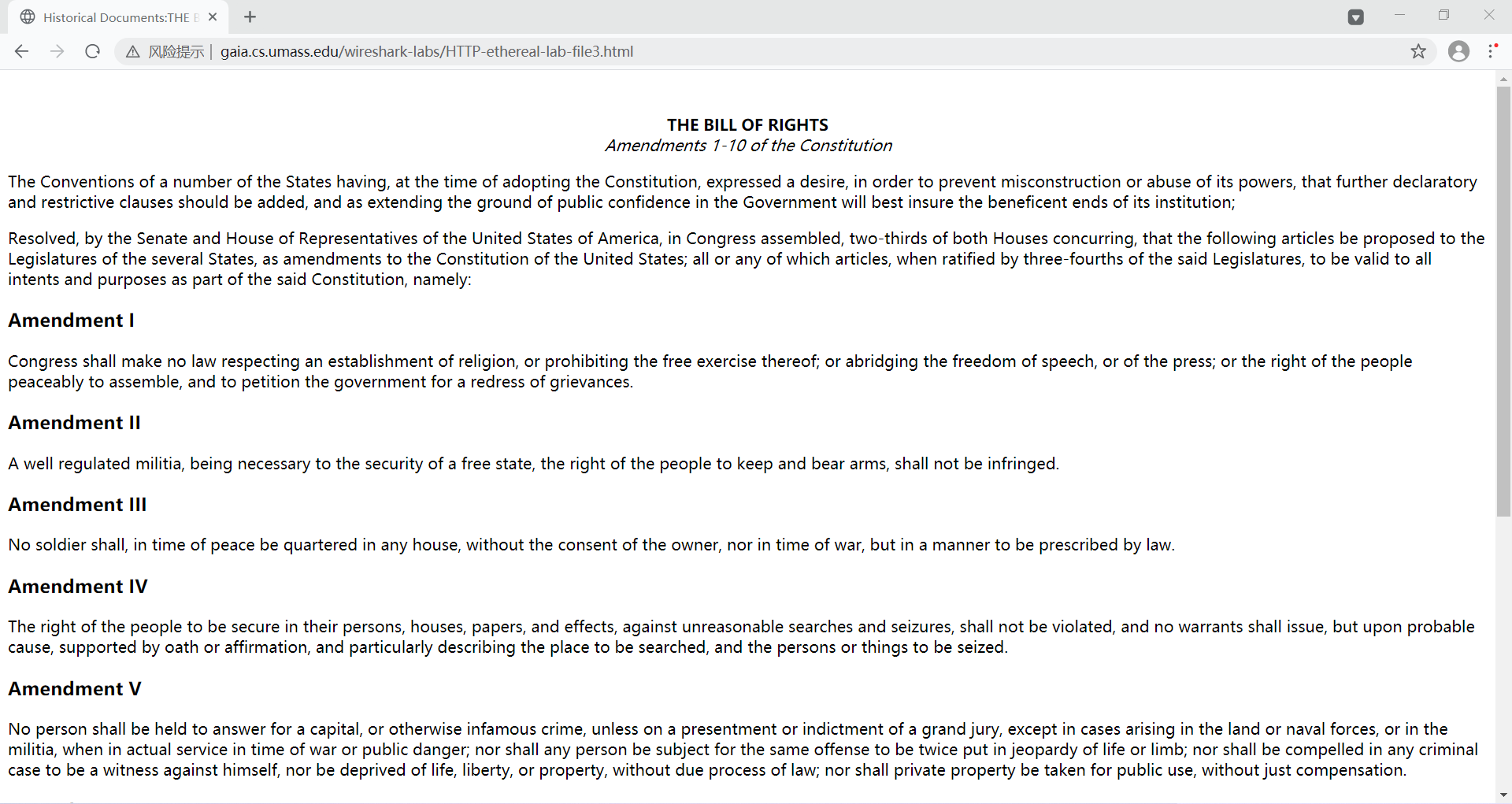
**Part 1：Capturing and analyzing Ethernet frames**

1. **实验流程：**

1）清除浏览器缓存，打开Wireshark抓包。

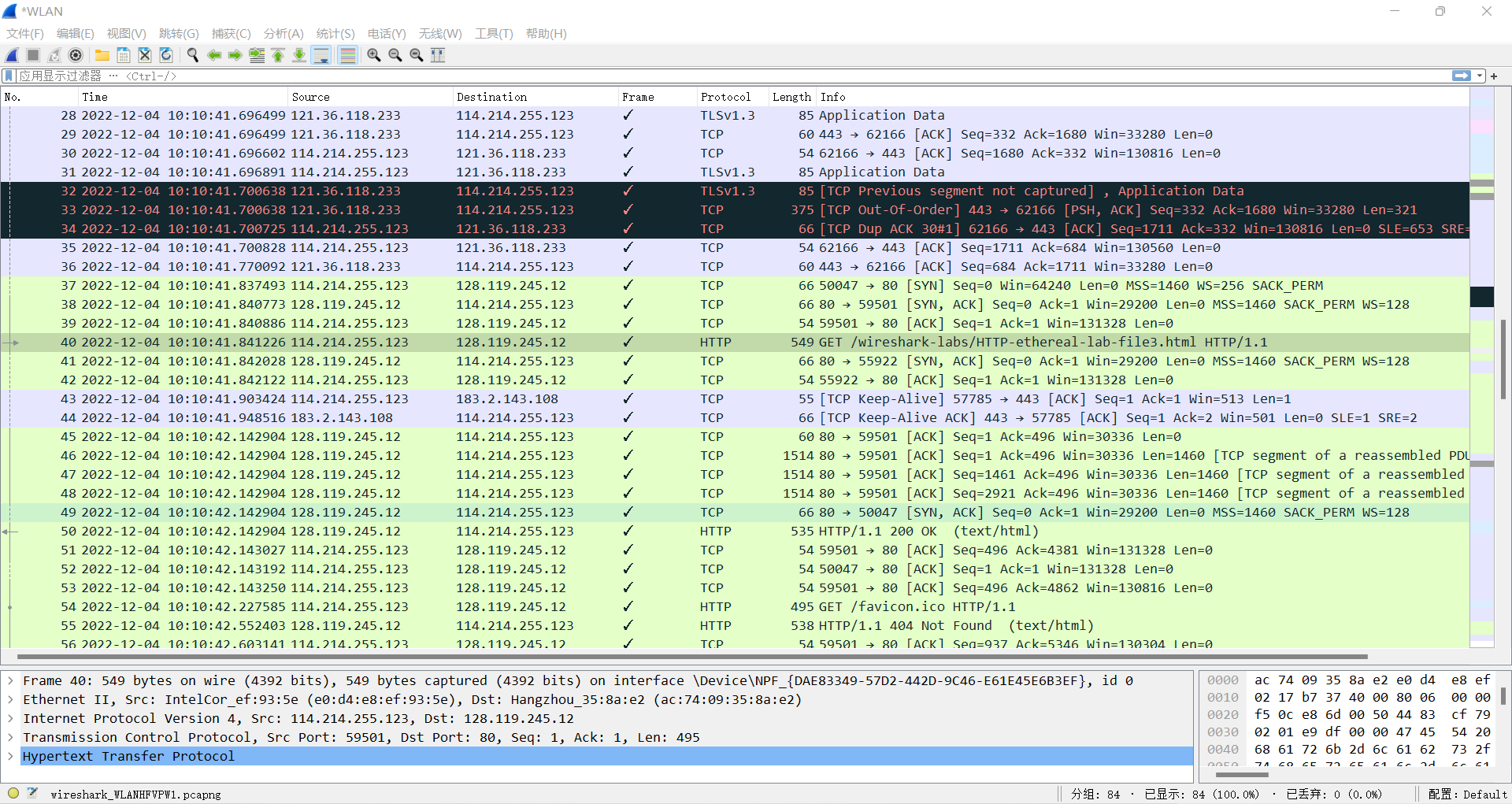
2）输入URL：<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>

显示界面如图：



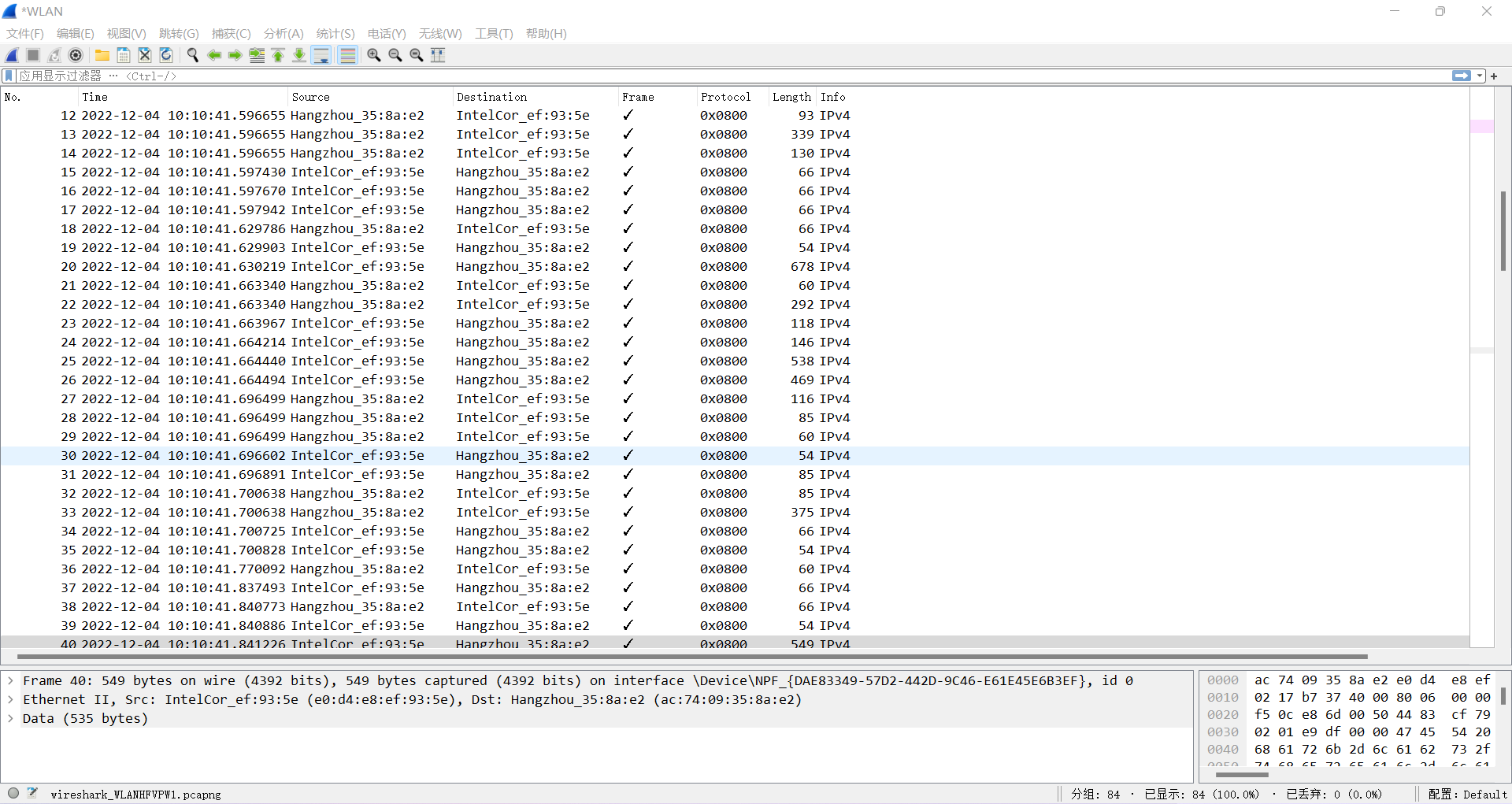
**（图1-1 输入网址显示界面）**

* + - 1. 停止抓包。找到HTTP GET（Num = 40）及响应（Num = 46）报文，显示如下：



**（图1-2 Wireshark抓包界面）**

* + - 1. 更改Wireshark的“捕获包列表”窗口，使其仅显示IP以下协议的信息。更改后显示界面如下：



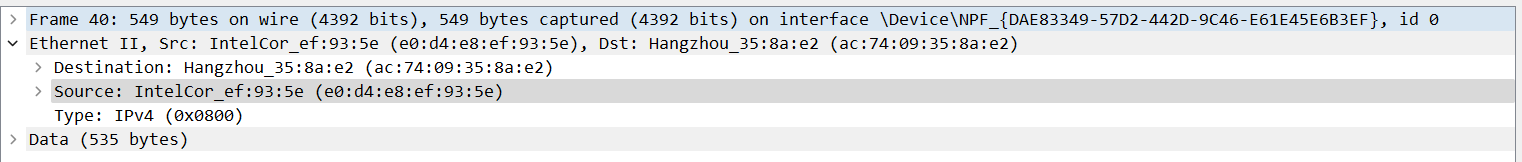
**（图1-3 更改显示界面）**

1. **问题回答：**

下面根据包含HTTP GET报文的以太网帧的内容，回答问题：

1. **What is the 48-bit Ethernet address of your computer?**

**Ans:** e0:d4:e8:ef:93:5e。（在前述步骤中已经找到HTTP GET 对应的Num = 40）。

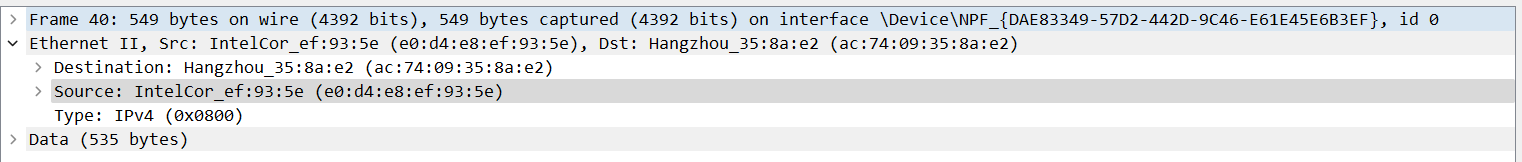


1. **What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]**

**Ans:** Destination address：ac:74:09:35:8a:e2；

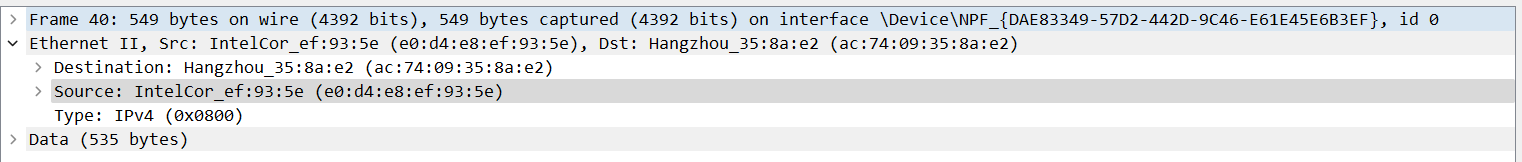
这不是gaia.cs.umass.edu的以太网地址。

这是主机所在子网的网关MAC地址。对应网关路由器拥有该地址。



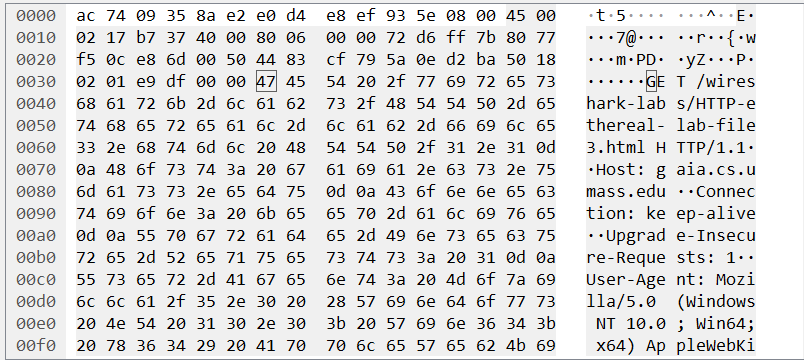
1. **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**

**Ans:** 0x0800，与之相对应的上层协议为IPv4。



1. **How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?**

**Ans:**出现在第55个字节。

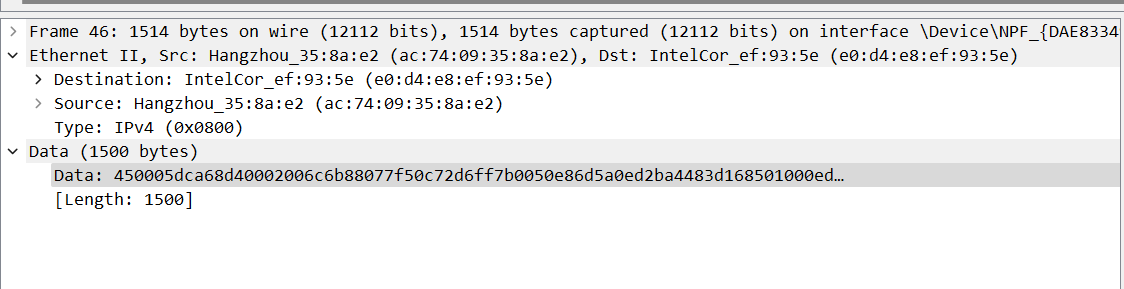


下面根据包含HTTP响应消息的第一个字节的以太网帧的内容，回答问题：

1. **What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?**

**Ans:**上述过程已记录首个HTTP response报文的Num = 46。则可知Ethernet source address为：ac:74:09:35:8a:e2；

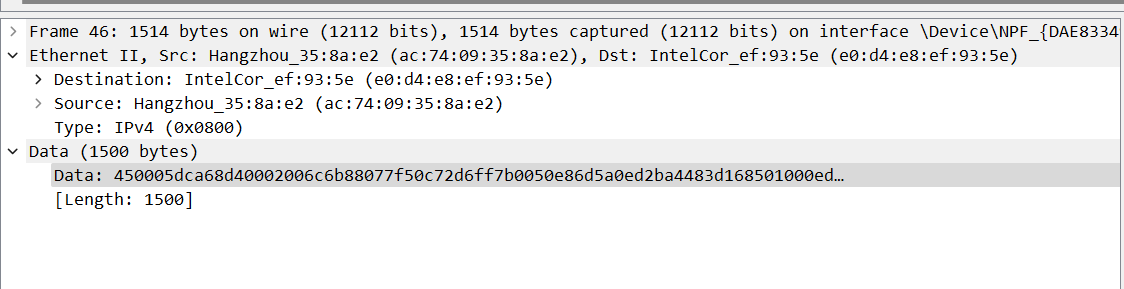
这既不是主机地址也不是gaia.cs.umass.edu的地址，这是主机所在子网的网关MAC地址。对应网关路由器拥有该地址。



1. **What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?**

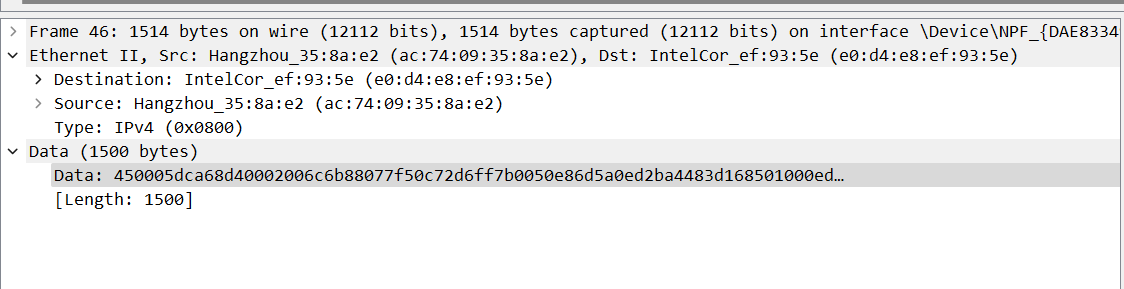
**Ans:** Destination address：e0:d4:e8:ef:93:5e；

这是我主机的以太网地址。



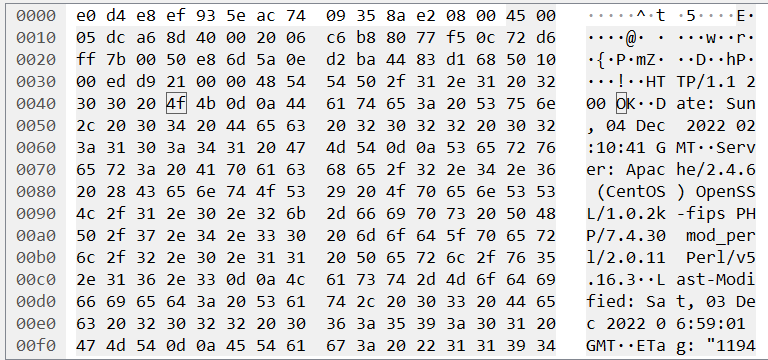
1. **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**

**Ans:** 0x0800，与之相对应的上层协议为IPv4。



1. **How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?**

**Ans:**出现在第68个字节。



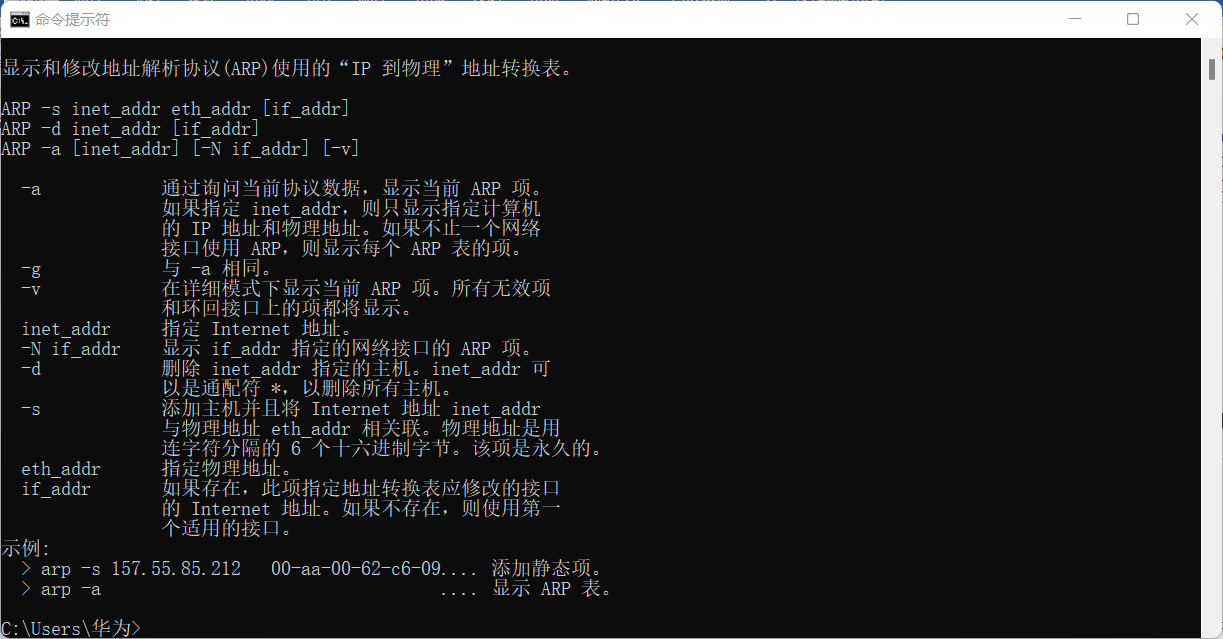
**Part 2：The Address Resolution Protocol**

1. **实验内容：**

研究ARP协议的运行。

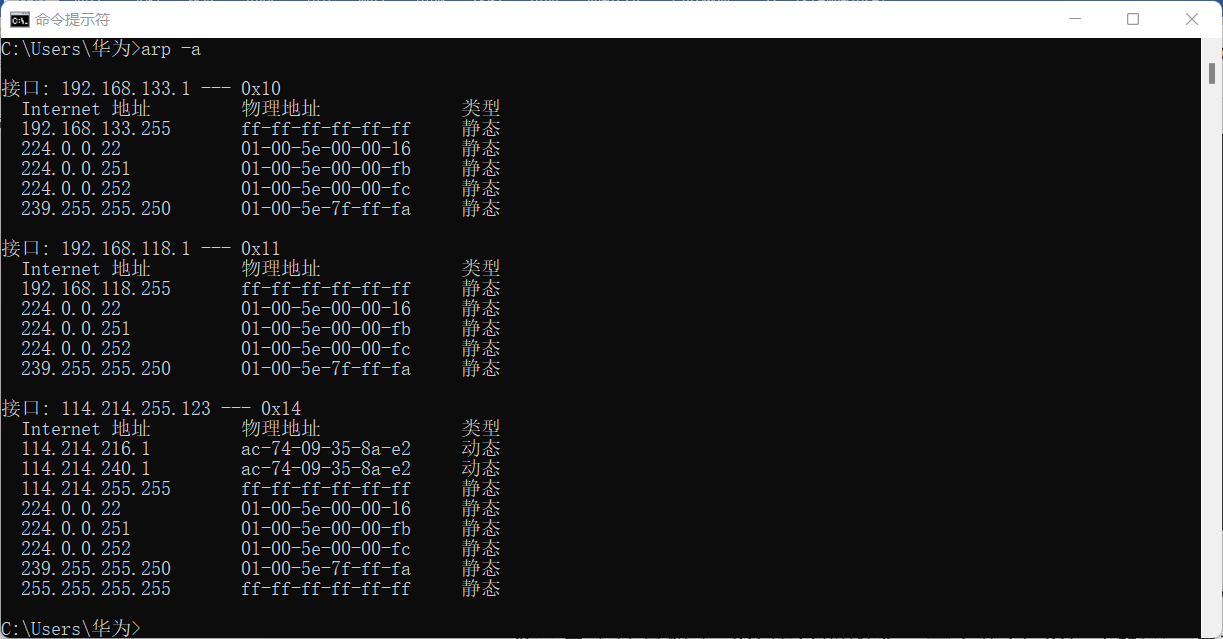
注意区分arp命令及ARP协议。arp命令用于显示和修改地址解析协议 (ARP)使用的“IP到物理”地址转换表。ARP 缓存中包含一个或多个表，它们用于存储IP地址及其经过解析的以太网或令牌环物理地址。

1. **实验流程及问题回答：**
2. 打开MS-DOS command line 输入“c:\windows\system32\arp” 。
3. 没有参数的Windows arp命令将显示计算机上arp缓存的内容。运行arp命令，显示如下：



**（图1-4 arp命令显示界面）**

1. 由于版本系统并不完全相同，在我的电脑上运行没有参数的Windows arp命令并不会显示计算机上arp缓存的内容。需要运行arp -a命令，显示如下：



**（图1-5 ARP缓存显示界面）**

1. **Write down the contents of your computer’s ARP cache. What is the meaning of each column value?**

**Ans:**

**接口: 192.168.133.1 --- 0x10**

**Internet 地址 物理地址 类型**

**192.168.133.255 ff-ff-ff-ff-ff-ff 静态**

**224.0.0.22 01-00-5e-00-00-16 静态**

**224.0.0.251 01-00-5e-00-00-fb 静态**

**224.0.0.252 01-00-5e-00-00-fc 静态**

**239.255.255.250 01-00-5e-7f-ff-fa 静态**

**接口: 192.168.118.1 --- 0x11**

**Internet 地址 物理地址 类型**

**192.168.118.255 ff-ff-ff-ff-ff-ff 静态**

**224.0.0.22 01-00-5e-00-00-16 静态**

**224.0.0.251 01-00-5e-00-00-fb 静态**

**224.0.0.252 01-00-5e-00-00-fc 静态**

**239.255.255.250 01-00-5e-7f-ff-fa 静态**

**接口: 114.214.255.123 --- 0x14**

**Internet 地址 物理地址 类型**

**114.214.216.1 ac-74-09-35-8a-e2 动态**

**114.214.240.1 ac-74-09-35-8a-e2 动态**

**114.214.255.255 ff-ff-ff-ff-ff-ff 静态**

**224.0.0.22 01-00-5e-00-00-16 静态**

**224.0.0.251 01-00-5e-00-00-fb 静态**

**224.0.0.252 01-00-5e-00-00-fc 静态**

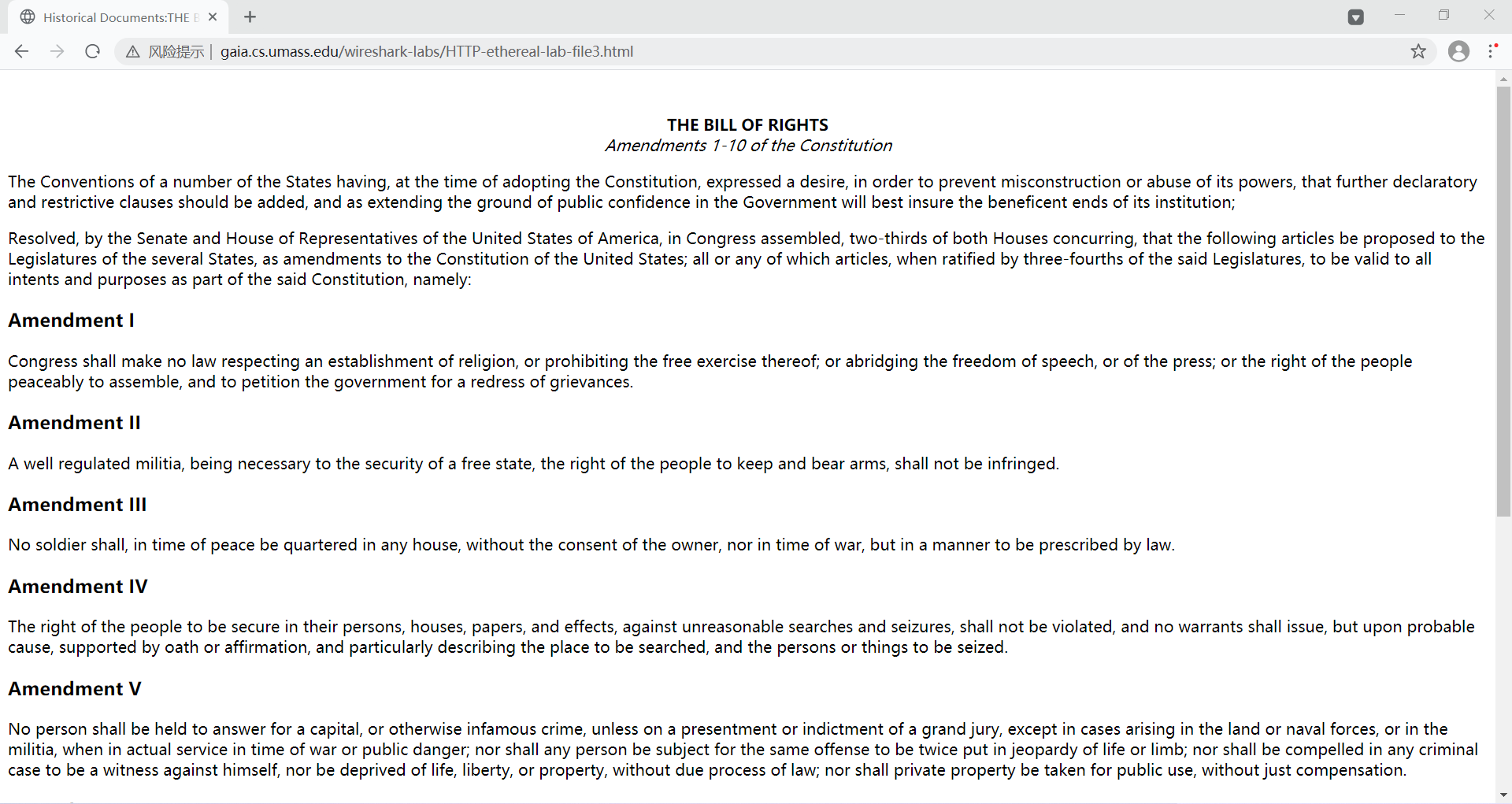
**239.255.255.250 01-00-5e-7f-ff-fa 静态**

**255.255.255.255 ff-ff-ff-ff-ff-ff 静态**

不同接口指示不同的网卡对应的IP地址；Internet 地址对应目的IP地址；物理地址表示IP地址对应的MAC地址；类型指示该条目的获取方式：类型列的“动态”表示使用ARP请求广播动态获取到的条目，“静态”表示是手工配置和维护的ARP表。

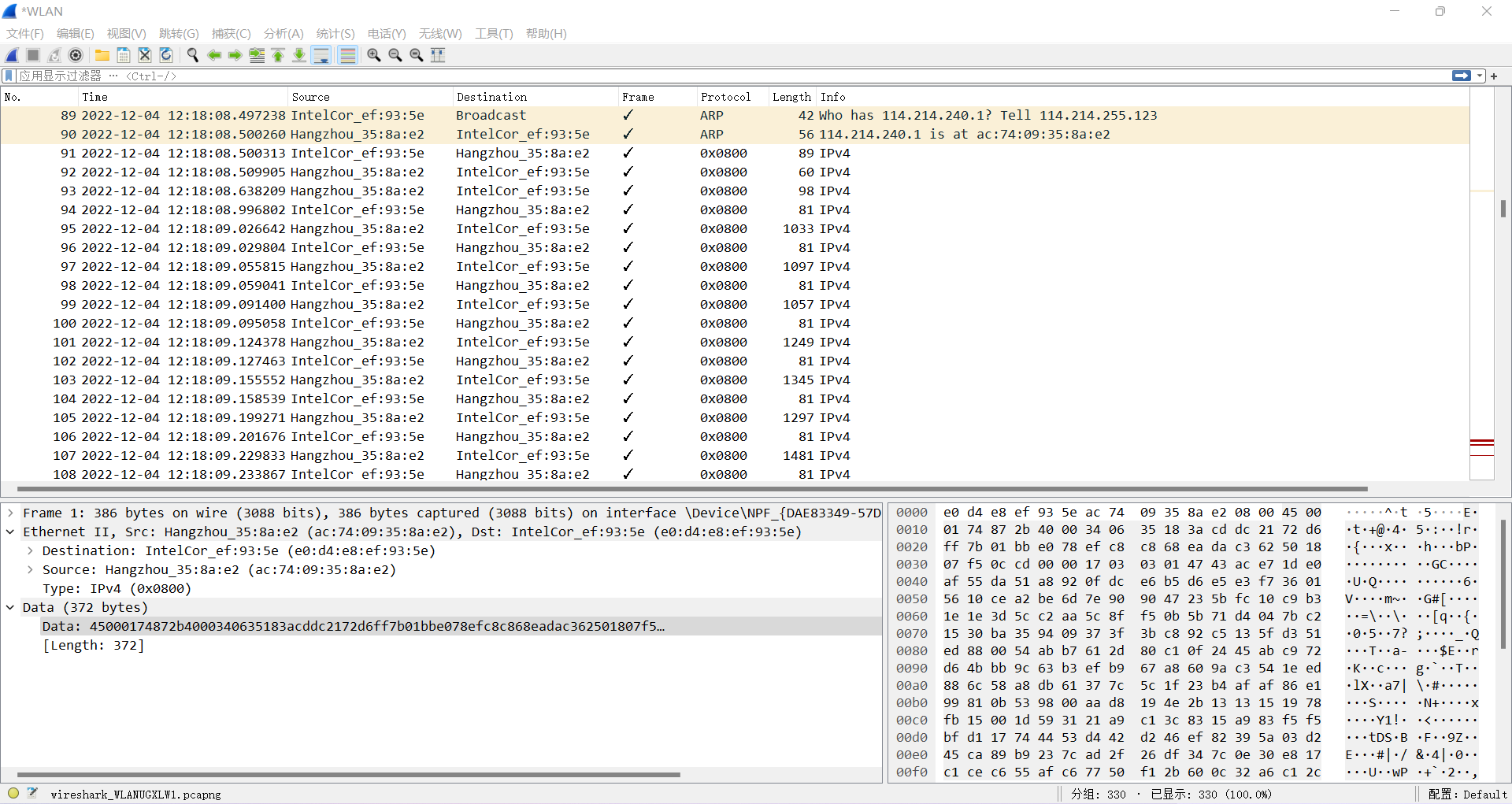
1. 运行arp -d命令清除arp缓存。
2. 清除浏览器缓存，开启Wireshark抓包。
3. 输入URL：<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>

显示界面如图：



**（图1-6 输入网址显示界面）**

1. 停止抓包。更改Wireshark的“捕获包列表”窗口，使其仅显示IP以下协议的信息。更改后显示界面如下：

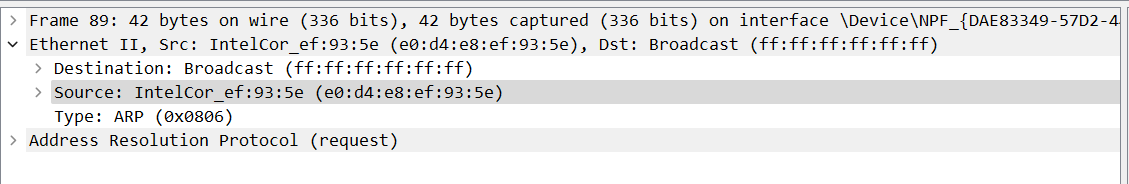


**（图1-7 Wireshark抓包界面）**

1. **10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?**

**Ans:** Source address：e0:d4:e8:ef:93:5e；

Destination address：ff:ff:ff:ff:ff:ff；

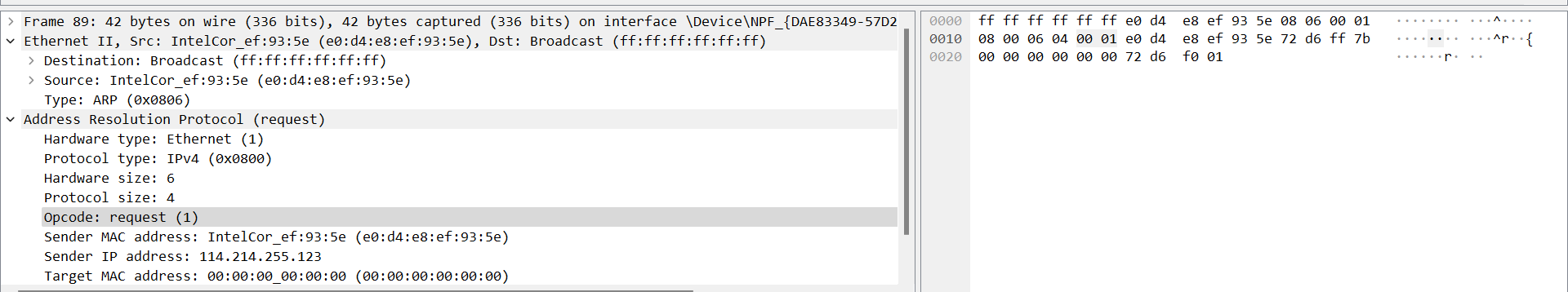


1. **Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?**

**Ans:**0x0806，对应的上层协议为ARP协议；

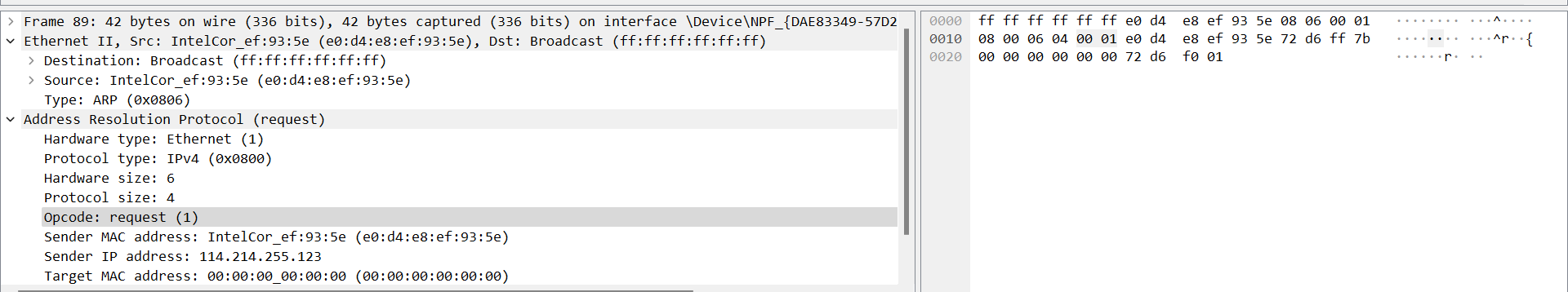
1. **Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.**
2. **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

**Ans:**ARP opcode域从第21字节开始；



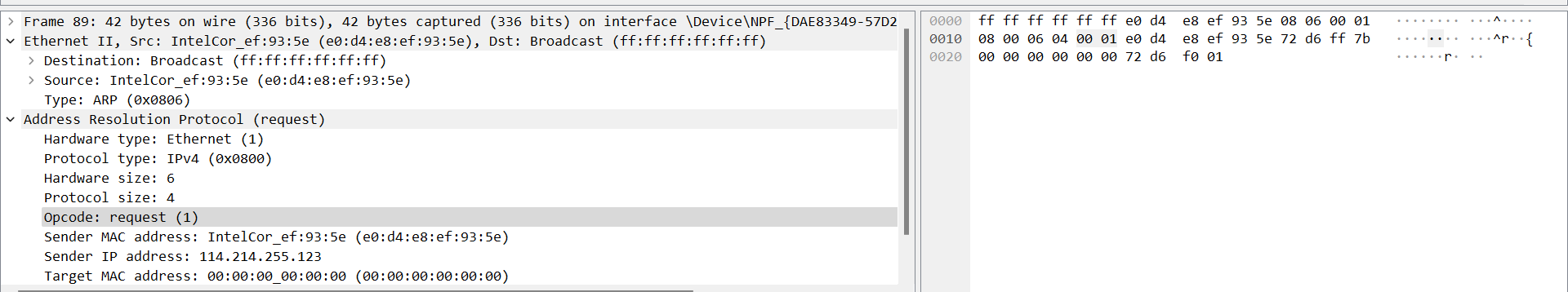
1. **What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?**

**Ans:** ARP请求中ARP opcode域的值为1；



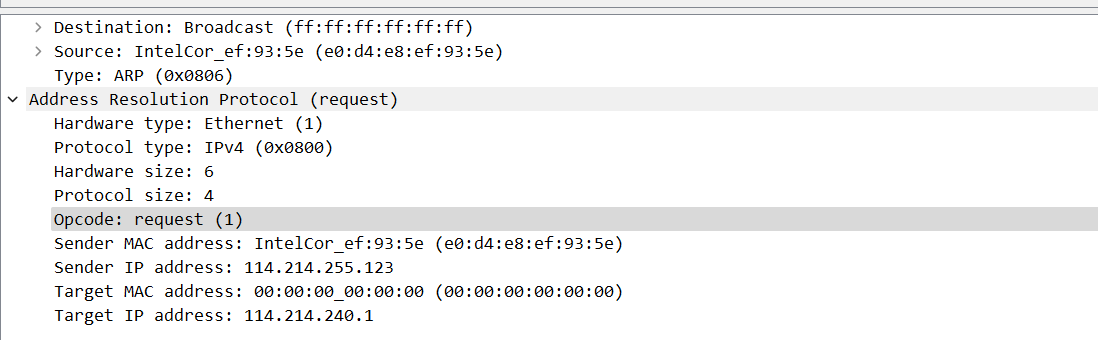
1. **Does the ARP message contain the IP address of the sender?**

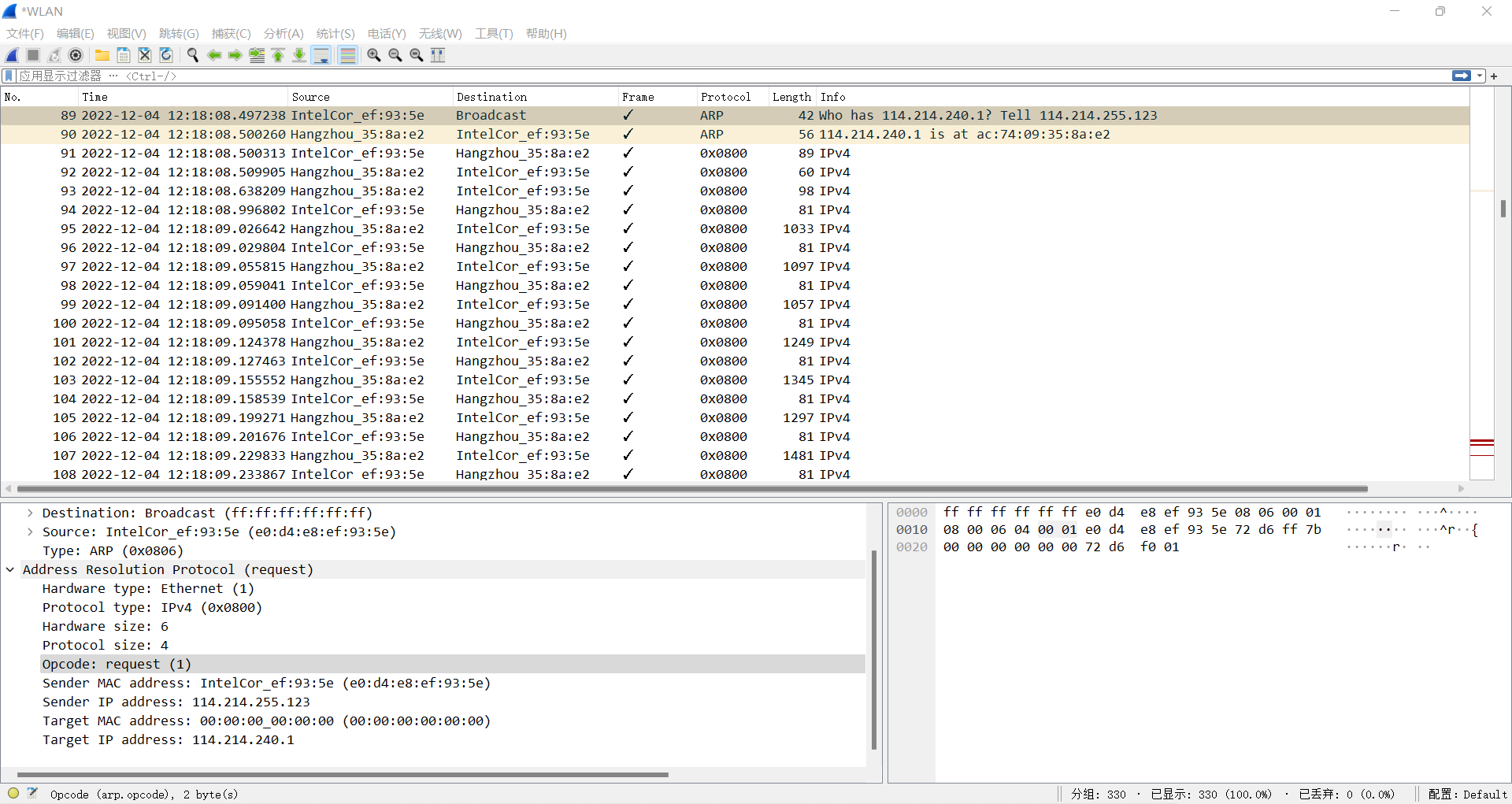
**Ans:** 包含，发送方IP地址为114.214.255.123；



1. **Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?**

**Ans:** Opcode的值为1，代表查询MAC地址，且Target MAC address为空。（也可以从info里看出）：





1. **Now find the ARP reply that was sent in response to the ARP request.**
2. **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

**Ans:**ARP opcode域从第21字节开始；



1. **What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?**

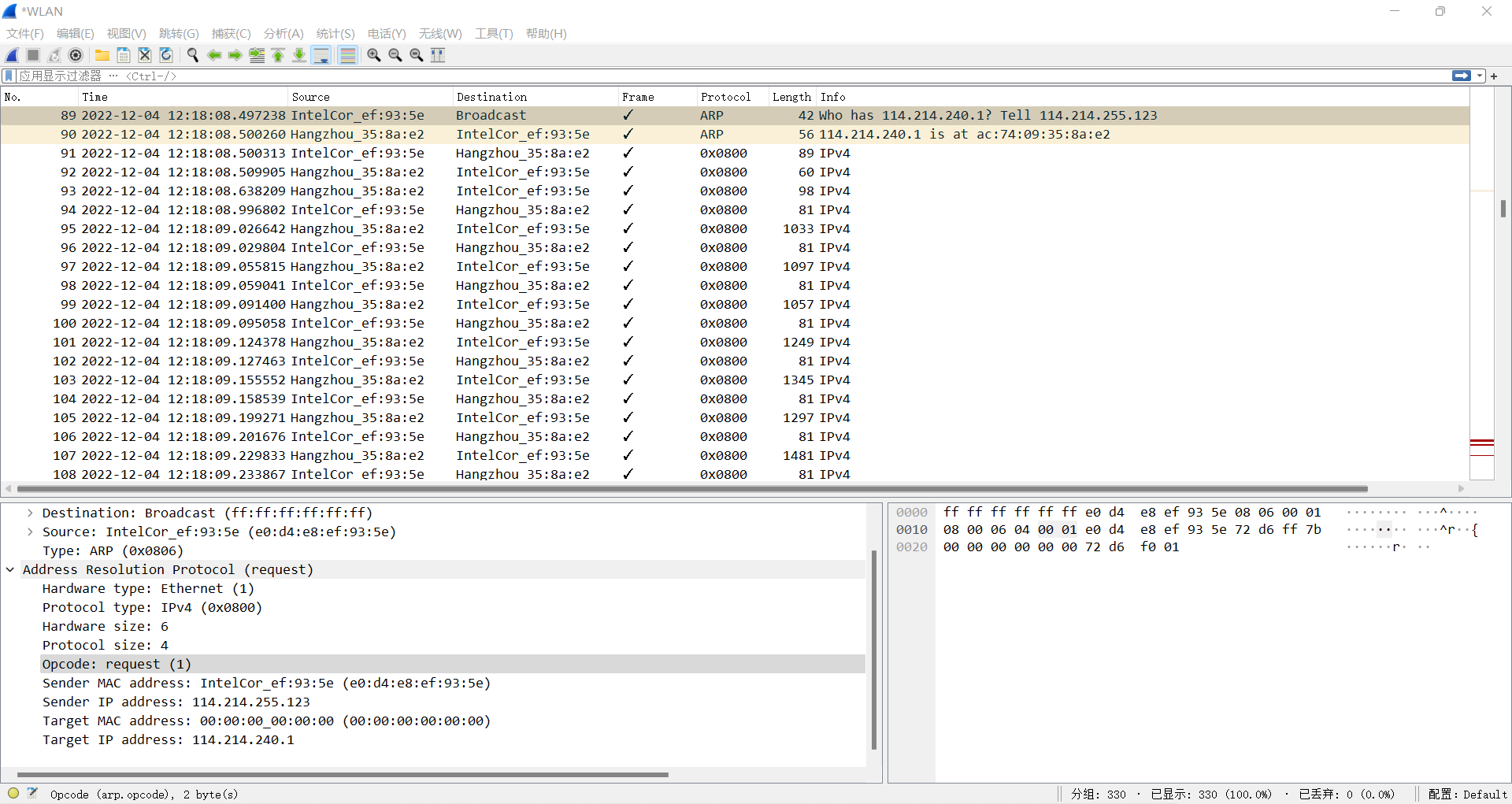
**Ans:** ARP请求中ARP opcode域的值为2；



1. **Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?**

**Ans:** 在Sender MAC address中。（也可以从info里看出）：

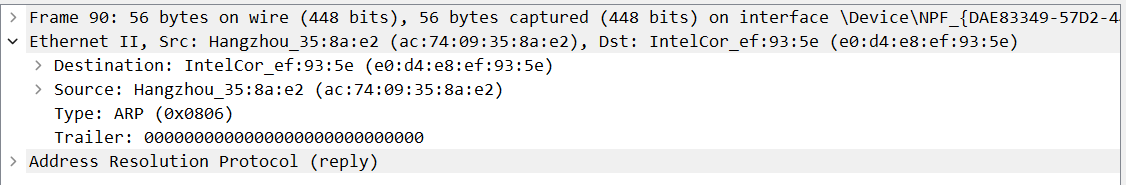




1. **What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?**

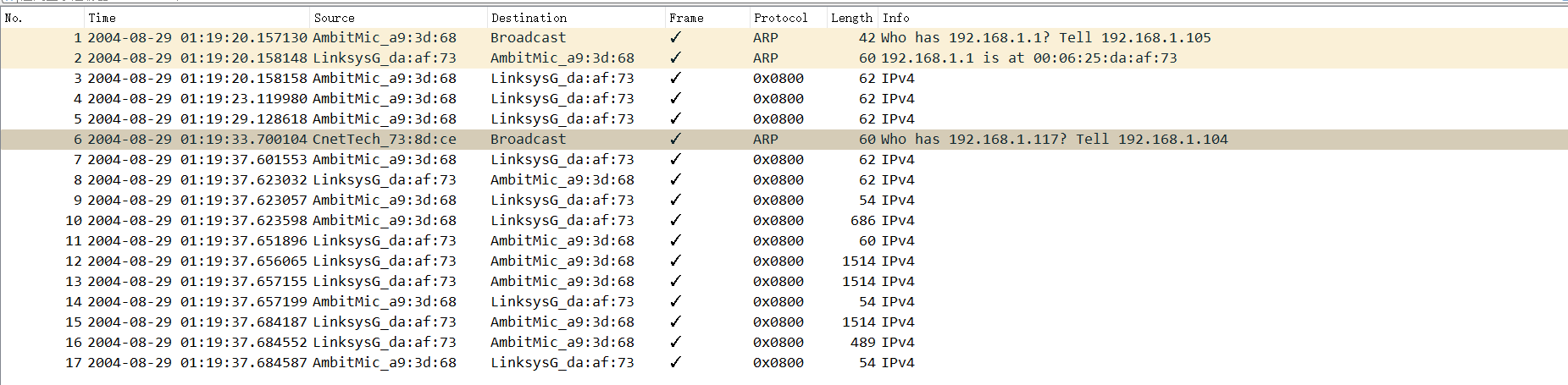
**Ans:** Source address：ac:74:09:35:8a:e2；

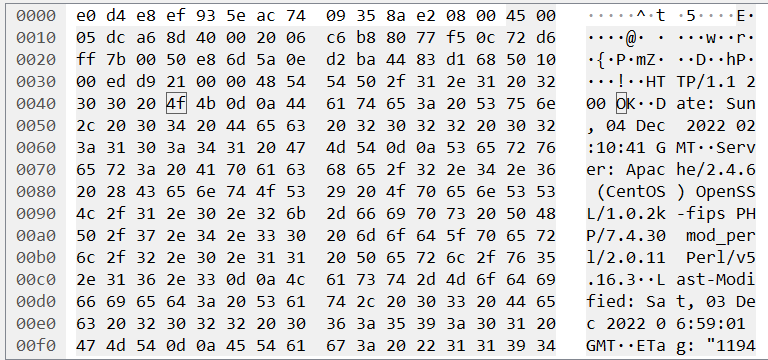
Destination address：e0:d4:e8:ef:93:5e；



1. **Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?**

**Ans:** 因为ARP请求是广播的，但是ARP响应是单播的，只有发送请求的主机可以接收到响应报文。第二次发送ARP请求的源不是对应主机，因此无法接收到ARP响应信息。





**Part 3：Extra Credit**

1. **问题回答：**
2. **The arp command: arp -s InetAddr EtherAddr allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?**

**Ans:** 此时主机将无法访问该IP地址对应的主机，但是它可以错误MAC地址对应的主机通信，直到TTL过期。

1. **What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.?**

**Ans:** 查阅华为的系统文档，发现缺省情况下，动态ARP表项的老化超时时间为1200秒，即20分钟。可以使用arp expire-time命令来设置动态ARP表项的老化超时时间以及undo arp expire-time命令来恢复动态ARP表项的老化超时时间为缺省值。（静态条目的生存周期见后文）。



**补充内容：**

**MAC表与ARP表：**

**MAC地址表**：

交换机在转发数据前需要知道它的每一个端口所连接的主机的MAC地址，构建出一个MAC地址表。当交换机从某个端口收到数据帧后，读取数据帧中封装的目的地MAC地址信息，然后查阅事先构建的MAC地址表，找出和目的地地址相对应的端口，从该端口把数据转发出去，其他端口则不受影响，这样避免了与其它端口上的数据发生碰撞。

**ARP表**：

主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址。收到返回消息后主机将该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，于是就形成了ARP表。

无论是主机还是交换机都会有一个用来缓存同一网段设备IP地址和MAC地址的ARP映射表用于数据帧的转发。设备通过ARP解析到目的MAC之后，将会在自己的ARP映射表中增加IP地址到MAC地址的映射表，以用于后续到同一目的地数据帧的转发。

**ARP静态条目的生命周期：**

上述问题中回答了动态条目的生存周期。而静态条目一直保留在ARP缓存中，意思是永久生效。但在不同的操作系统中，静态条目的保存方式是不同的。例如，在Windows XP系统中，重新启动计算机后该条目失效。而在Windows 7中，即使重新启动计算机后，该静态条目仍然保存。

**ARP欺骗攻击：**

ARP是建立在局域网中各个主机互相信任的基础上的，它的诞生使得网络能够更加高效的运行，但由于它没有安全认证机制，本身存在着很多漏洞和不足。

ARP转换映射表，是依赖于计算机中“高速缓冲存储器”动态更新的，而“高速缓冲存储器”的更新，是受到更新周期的限制的，只能保存最近使用的“地址映射的关系表项”，这使得攻击者有了可乘之机，可以在“高速缓冲存储器”更新表项之前，修改ARP转换映射表，以实现攻击。ARP请求是以广播的形式发送的，局域网上的所有主机，都可以自主地发送ARP应答消息，并且当其他主机收到应答消息时，不会检测该消息的真实性，就将其记录在本地的“ARP缓存表”中。这样攻击者就可以向目标主机发送伪造的“ARP请求包”（错误的IP地址和MAC地址的映射关系），从而篡改目标主机的本地“ARP缓存表”。

ARP欺骗可以导致目标主机与网关通信失败，更会导致通信重定向，可以使所有的数据均通过攻击者的主机，因此存在极大的安全隐患。

**成功！您的提交显示在此页面上。该提交的确认编号为 c31c2aaf-628f-4e43-a16c-314a9c0aa368。请复制并保存此编号以作为提交证明。**[**在“我的成绩”中查看您的所有提交确认。**](https://www.bb.ustc.edu.cn/webapps/bb-mygrades-BBLEARN/myGrades?course_id=_12565_1&stream_name=mygrades&is_stream=false)