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

一、 实验目的：

1. 了解以太网协议及 ARP 协议。
2. 学会分析 ARP 请求和响应报文。
3. 学会分析链路层帧的结构。
4. 了解 MAC 地址与 IP 地址各自的功能。
5. 学会使用 arp 命令查看和修改 ARP 缓存。

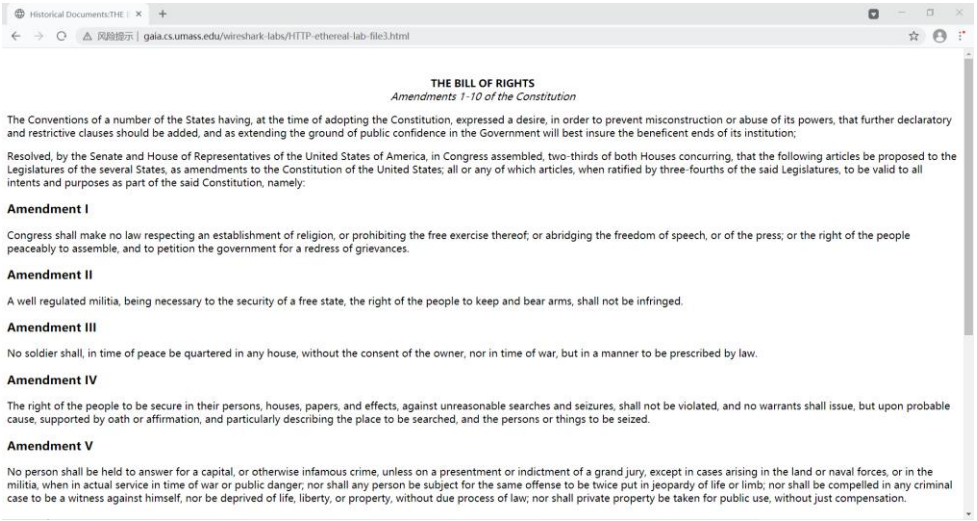
二、 实验流程及问题回答：

Part 1：Capturing and analyzing Ethernet frames

1. 实验流程：

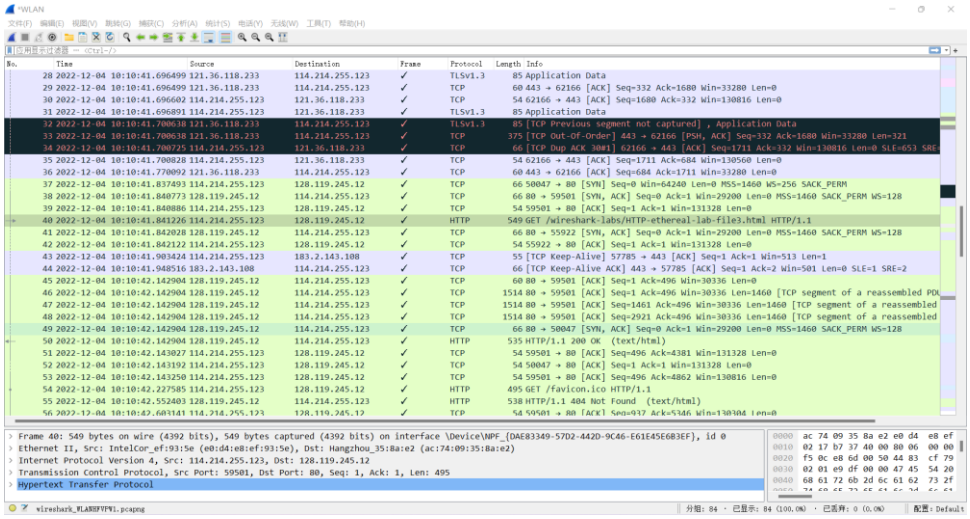
1）清除浏览器缓存，打开 Wireshark 抓包。

2）输入 URL：http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html 显示界面如图：



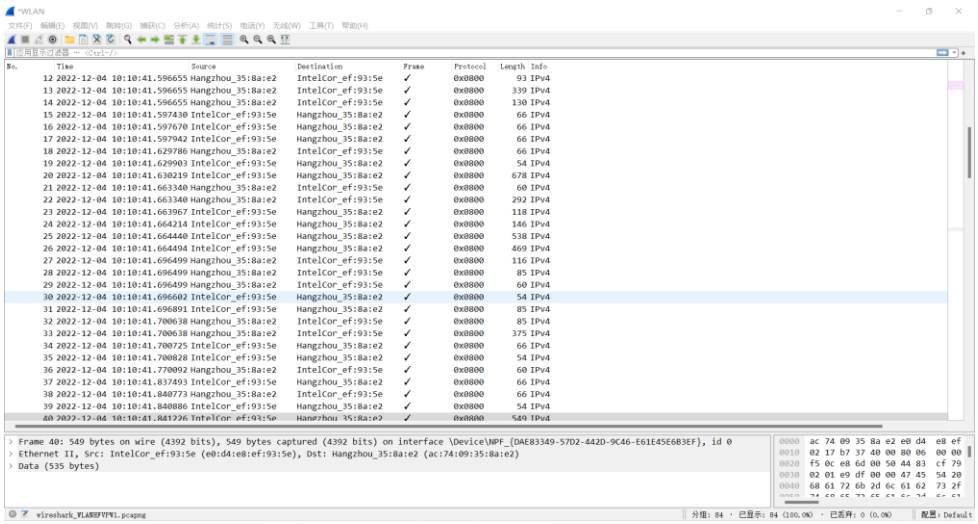
（图 1-1 输入网址显示界面）

3）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）

4） 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：



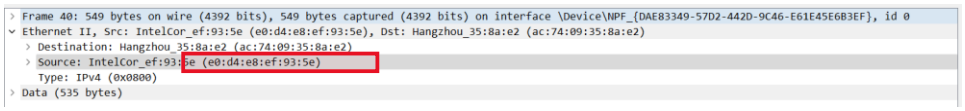
（图 1-3 更改显示界面）

2. 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）。

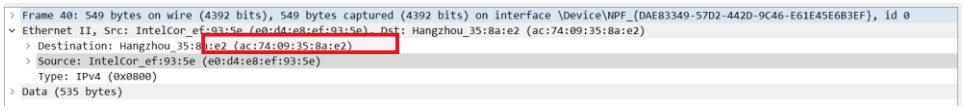


2. **What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text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

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

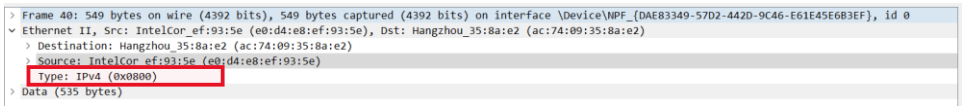
   这不是 gaia.cs.umass.edu 的以太网地址。

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。



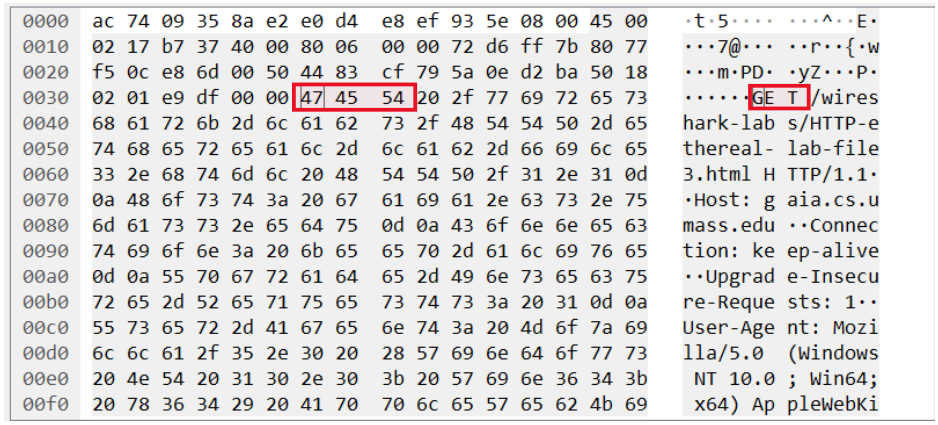
3. **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**

   Ans: 0x0800，与之相对应的上层协议为 IPv4。



4. **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。

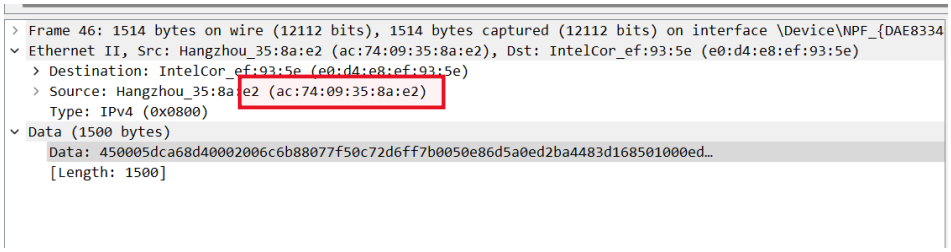


下面根据包含 HTTP 响应消息的第一个字节的以太网帧的内容，回答问题：

5. **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；

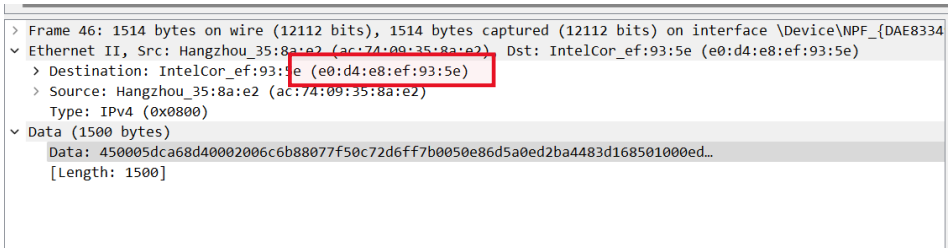
   这既不是主机地址也不是 gaia.cs.umass.edu 的地址，这是主机所在子网的网关 MAC 地址。对应网关路由器拥有该地址。



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

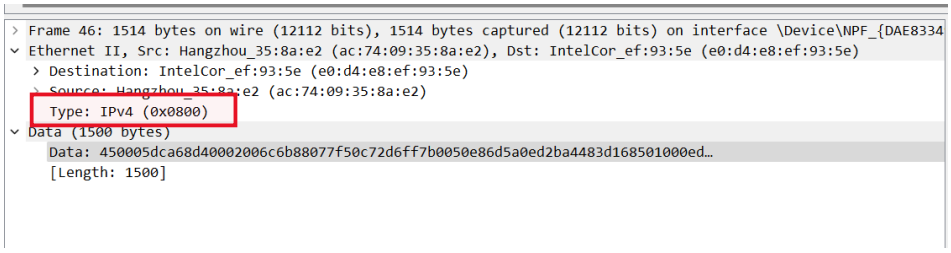
   Ans: Destination address：e0:d4:e8:ef:93:5e；

   这是我主机的以太网地址。



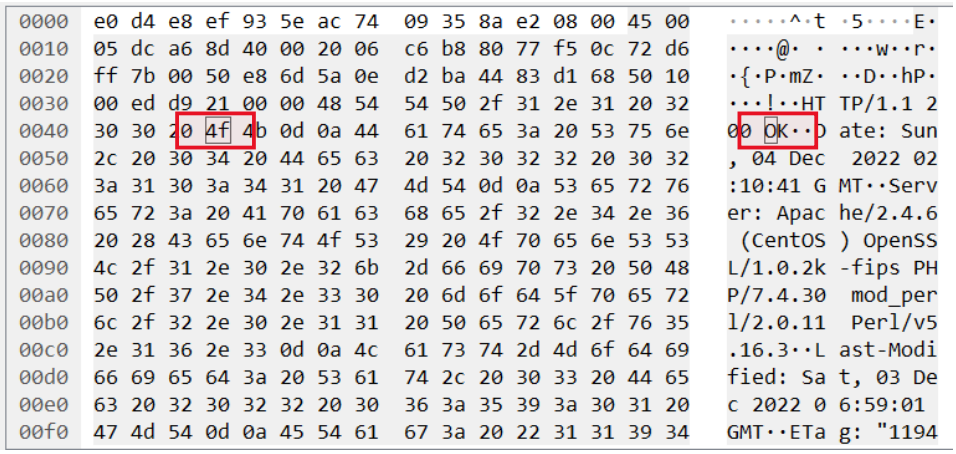
7. **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**

   Ans: 0x0800，与之相对应的上层协议为 IPv4。



8. **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

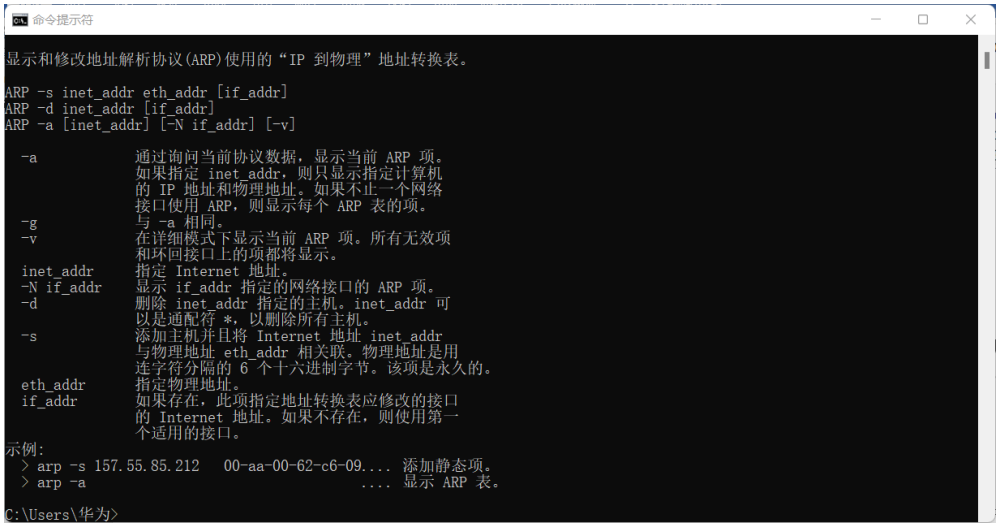
1. **实验内容：**

   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。

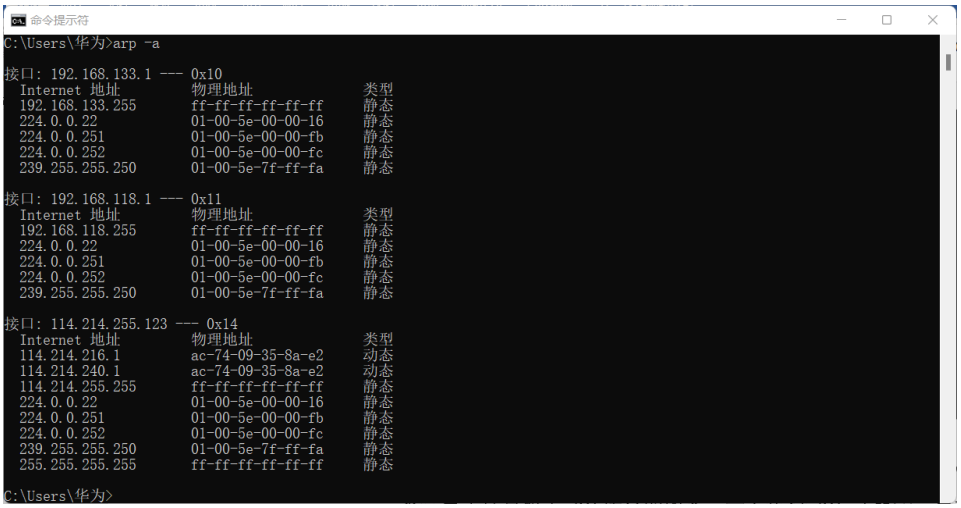
2. **实验流程及问题回答：**

   1) 打开 MS-DOS command line 输入"c:\windows\system32\arp" 。
   2) 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）

3） 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）

9. 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

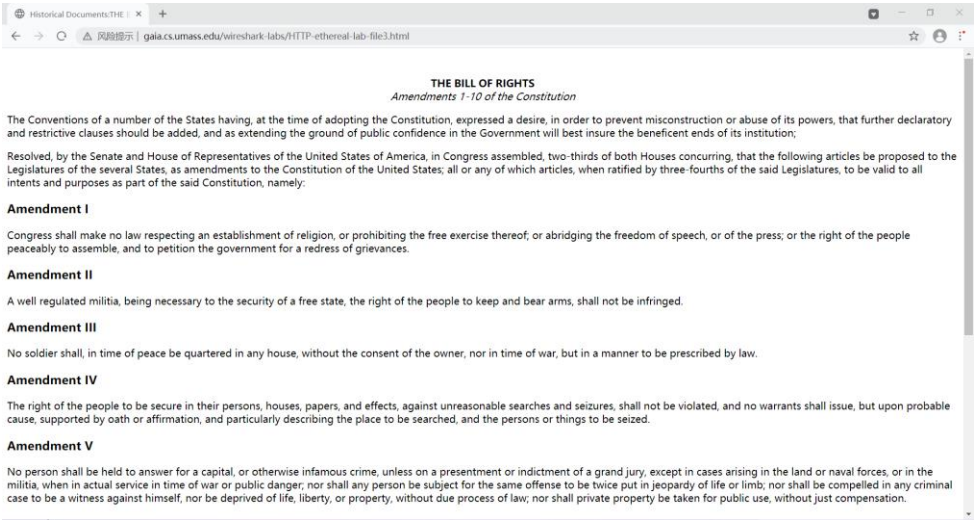
Internet 地址	物理地址	类型
114.214.216.1	ac-74-09-35-8a-e2	动态
114.214.240.1	ac-74-09-35-8a-e2	动态
114.214.255.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.251	01-00-5e-00-00-fb	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态

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。

4） 运行 arp -d 命令清除 arp 缓存。

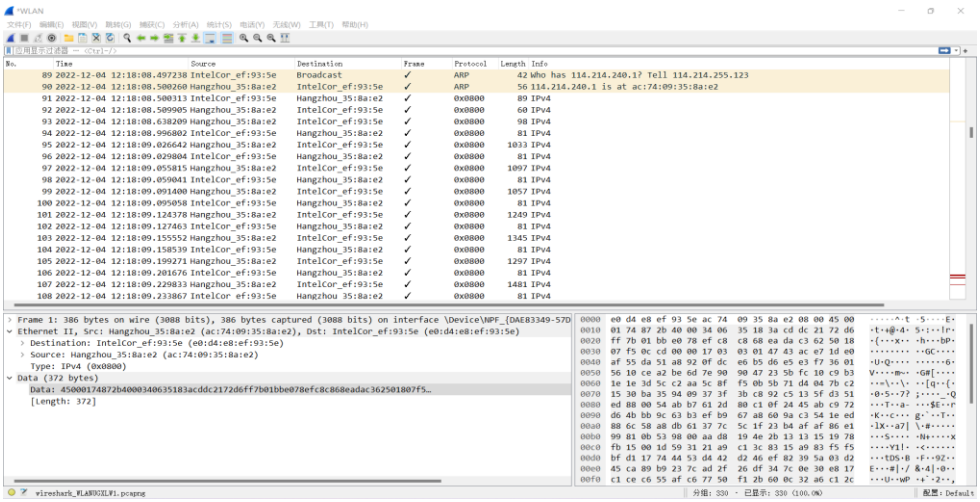
5） 清除浏览器缓存，开启 Wireshark 抓包。

6） 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）

7） 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：

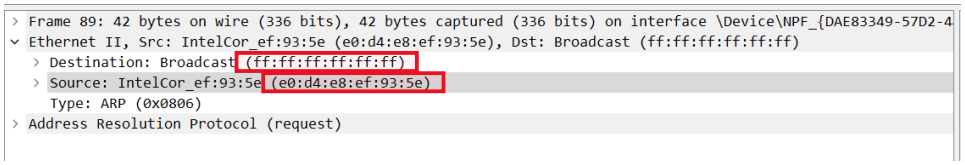


（图 1-7 Wireshark 抓包界面）

10. **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；



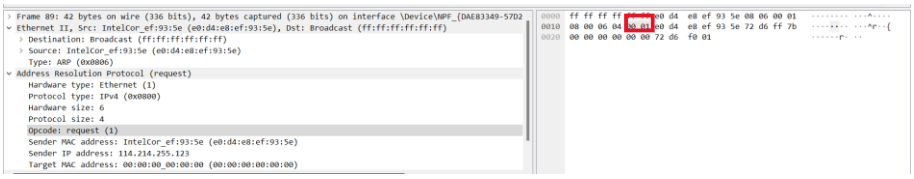
11. **Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?**

    Ans:0x0806，对应的上层协议为 ARP 协议；

12. **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.**

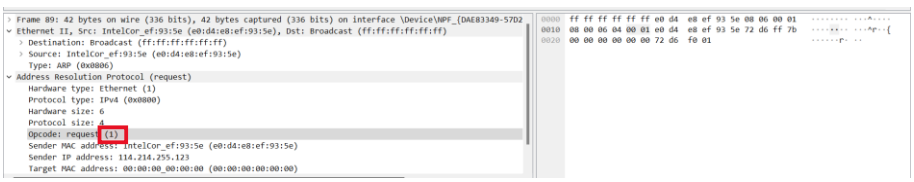
    a) **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

    Ans:ARP opcode 域从第 21 字节开始；



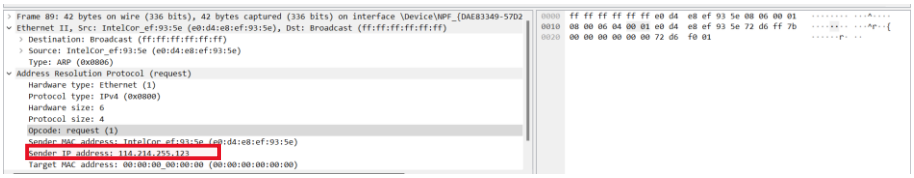
    b) **What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?**

    Ans: ARP 请求中 ARP opcode 域的值为 1；



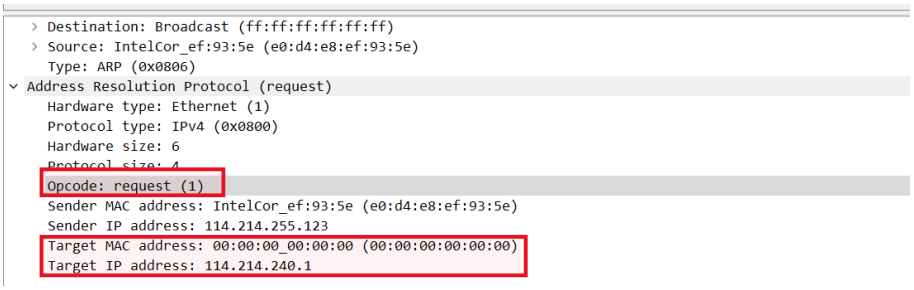
    c) **Does the ARP message contain the IP address of the sender?**

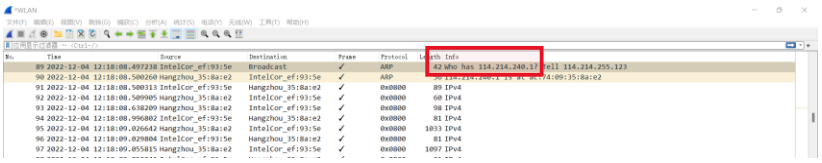
Ans: 包含，发送方 IP 地址为 114.214.255.123；



d) **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）：





13. **Now find the ARP reply that was sent in response to the ARP request.**

a) **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

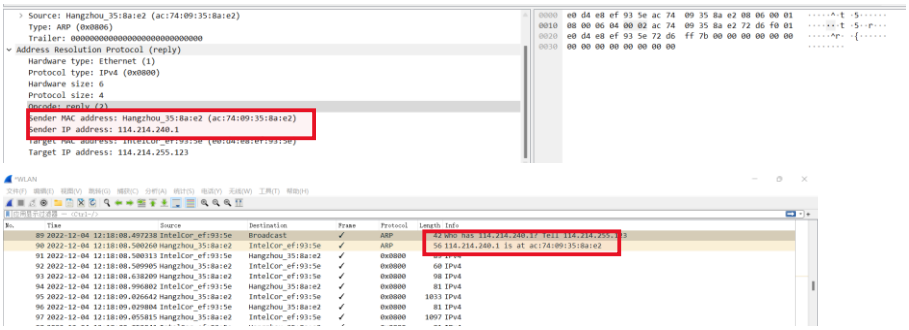
Ans:ARP opcode 域从第 21 字节开始；

b) **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；

c) **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?**

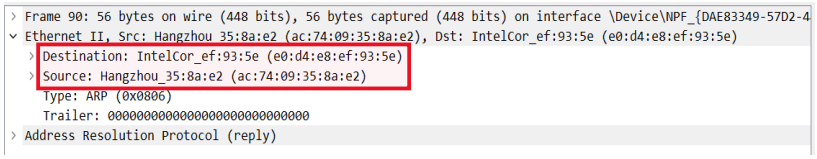
Ans: 在 Sender MAC address 中。（也可以从 info 里看出）：



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

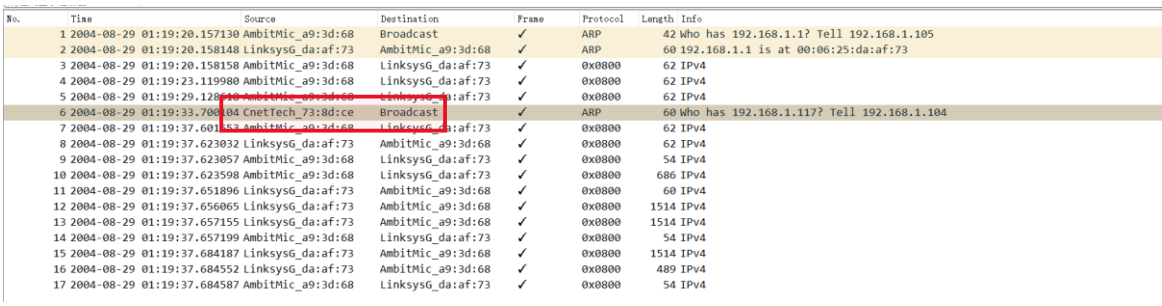
Ans: Source address：ac:74:09:35:8a:e2;

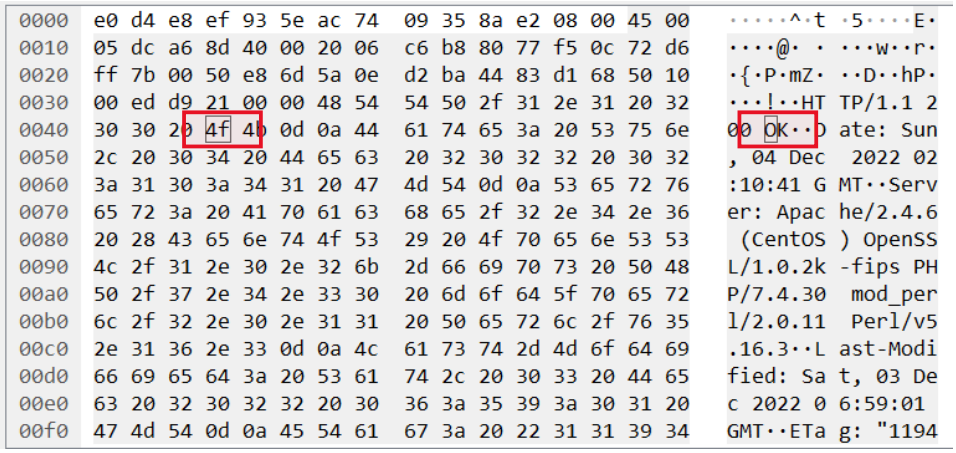
Destination address：e0:d4:e8:ef:93:5e;



15. **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：**

16. **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。

17. **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)。

命令功能

arp expire-time命令用来设置动态ARP表项的老化超时时间。

undo arp expire-time命令用来恢复动态ARP表项的老化超时时间为缺省值。

缺省情况下，动态ARP表项的老化超时时间为1200秒，即20分钟。

命令格式

arp expire-time *expire-time*

undo arp expire-time

参数说明

参数	参数说明	取值
expire-time	指定ARP表项的老化超时时间。	整数形式，取值范围是30～62640，单位是秒。缺省值是1200秒，即20分钟。

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。