计算机网络以太网实验报告

PB19071535徐昊天

一.实验目的

- 了解与学习以太网协议。
- 了解与学习ARP协议。
- 深入理解计算机链路层。

二.实验环境与工具

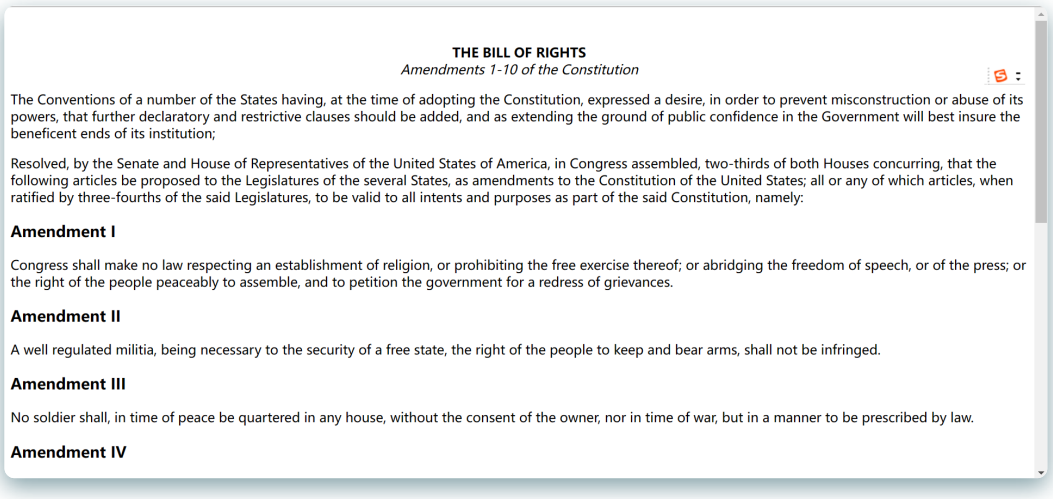
- windows操作系统。
- wireshark数据包嗅探器。
- Microsoft Edge浏览器。

三.实验步骤

1.捕获和分析以太网帧

1. 清空Microsoft Edge浏览器缓存。
2. 开启wireshark抓包并在浏览器中打开http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html。

   得到浏览器界面如下图所示：



THE BILL OF RIGHTS

Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

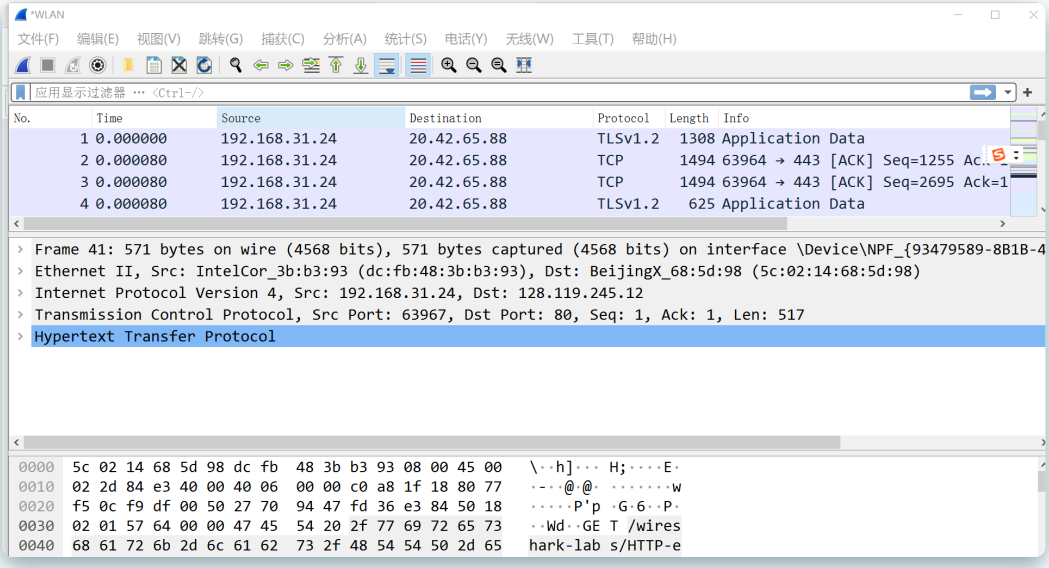
A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

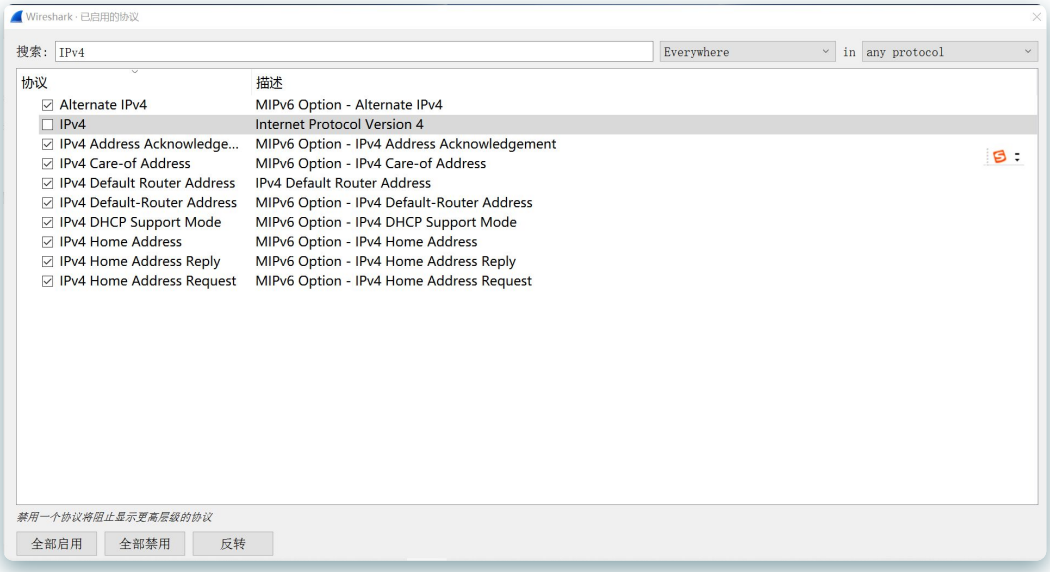
No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

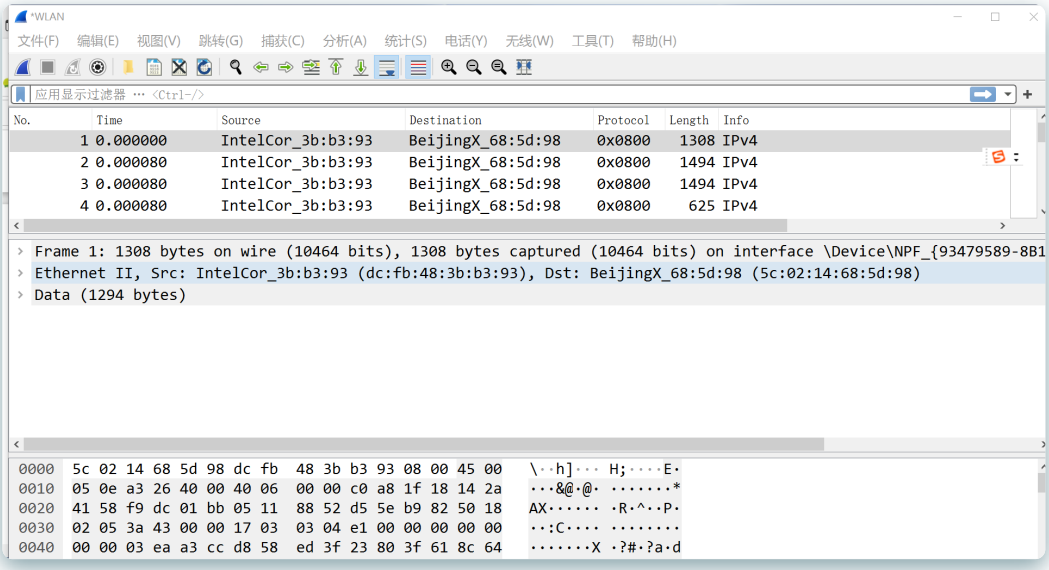
wireshark界面如下图所示：



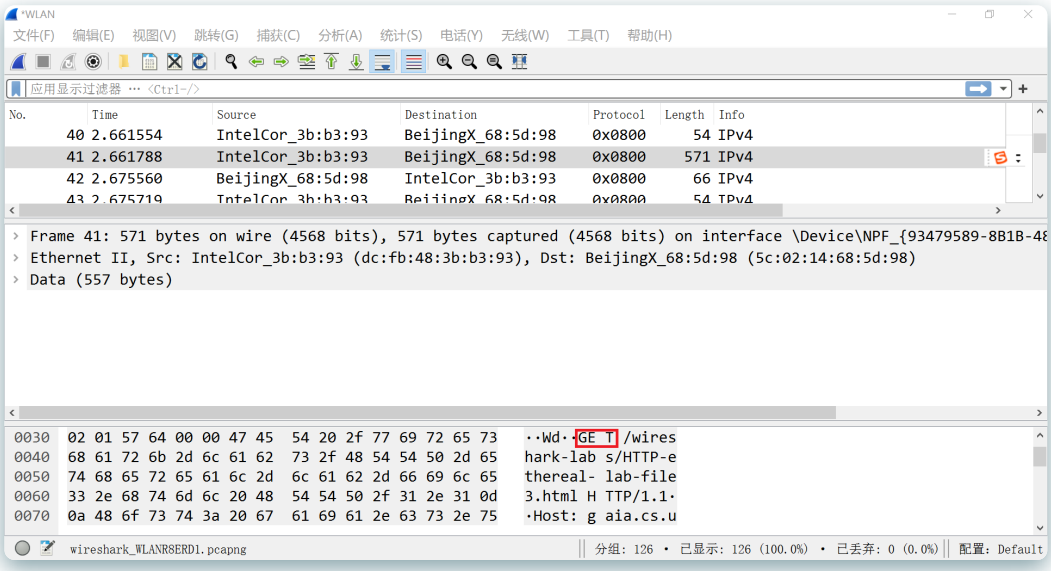
3. 更改wireshark抓获数据包的列表窗口，使其只显示有关IP协议以下的信息，在 Analyze ->Enabled Protocols 中对 IPV4 选项取消勾选，如下图所示：



得到wireshark界面如下图所示：



4. 选择包含HTTP GET消息的以太网帧，如下图所示：

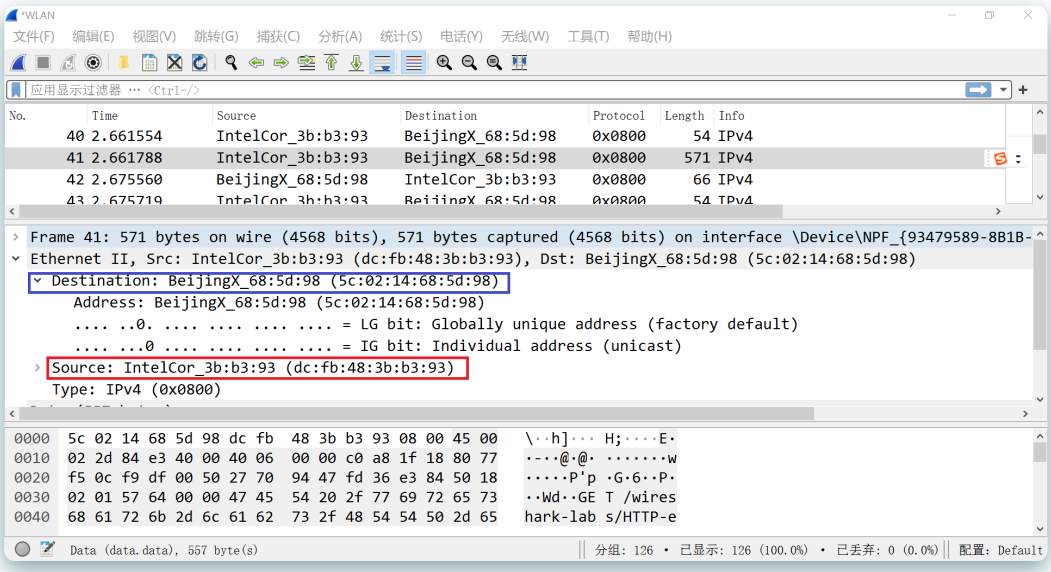


图中红色框中内容即表明为 HTTP GET 消息。

回答如下问题：

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

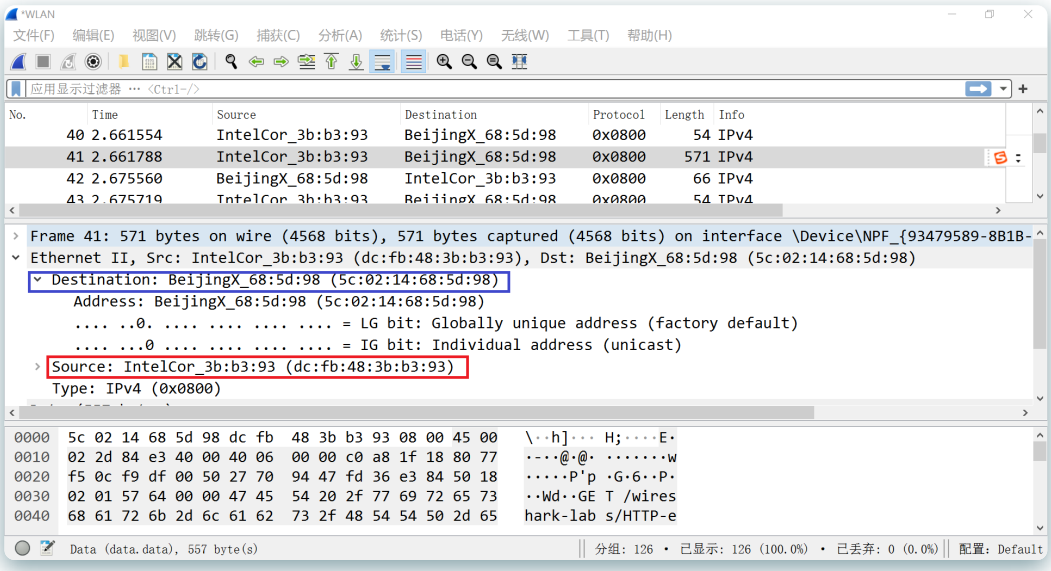
答：HTTP GET消息具体内容如下图所示：



根据红色框中内容可知我的计算机的48位以太网地址为 dc:fb:48:3b:b3:93 。

> 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.]

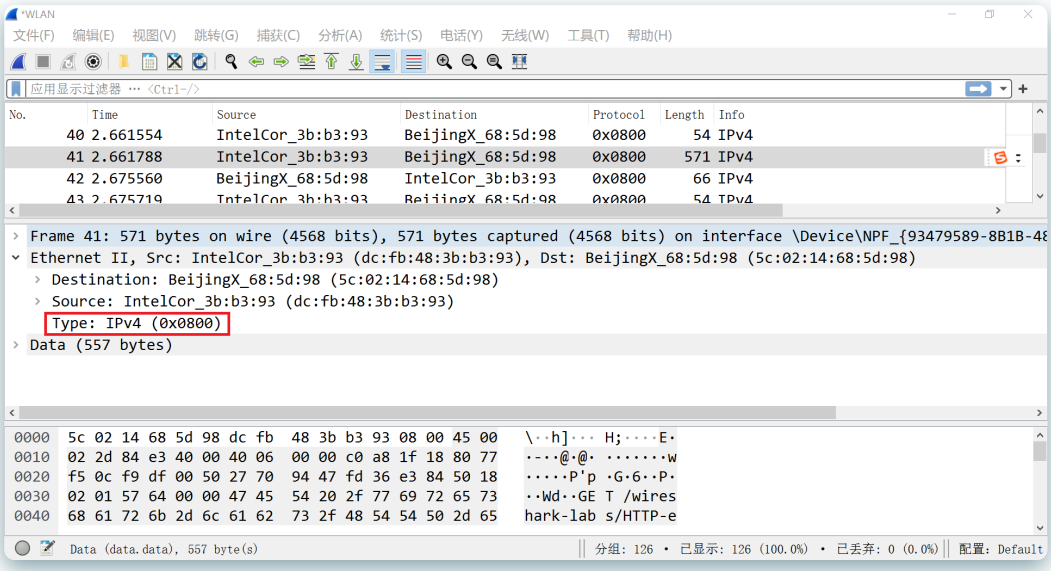
答：HTTP GET消息具体内容如下图所示：



根据蓝色框中内容可知以太网帧中的48位目标地址为 5c:02:14:68:5d:98 ；这不是 gaia.cs.umass.edu 的以太网地址，而是离开子网的路由器地址。

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

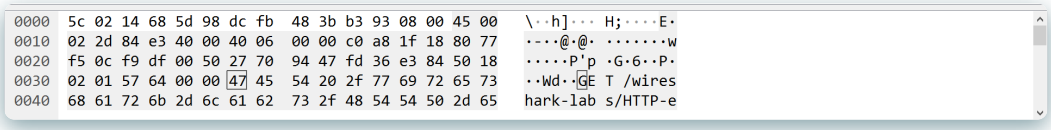
答：HTTP GET消息具体内容如下图所示：



根据红色框中内容，以太网帧上层协议的16进制值为 0x8000 ，对应的上层协议为 IPv4 。

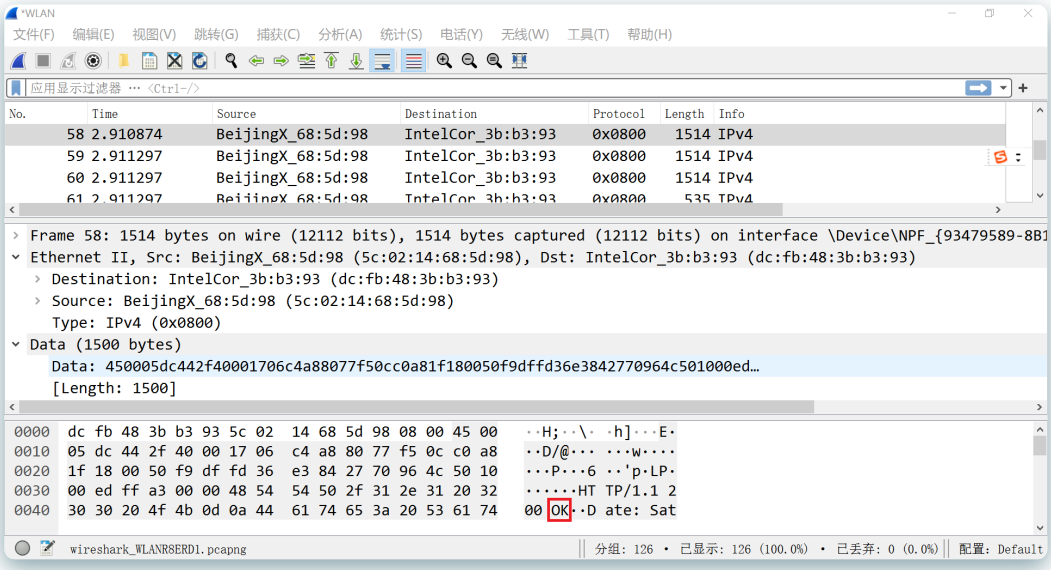
> 4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

答：以太网帧信息如下图所示：



根据"G"在以太网帧中的位置，从开始到"G"出现一共有3*16+7=55个字节。

5. 选择包含HTTP响应消息的以太网帧，如下图所示：

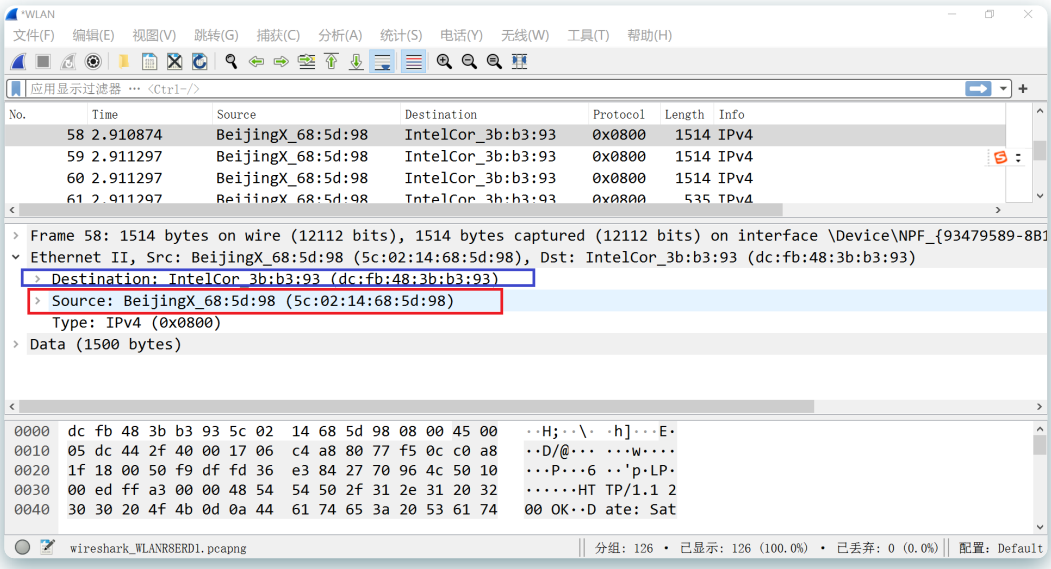


图中红色框中内容表明为响应消息。

回答以下问题：

> 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?

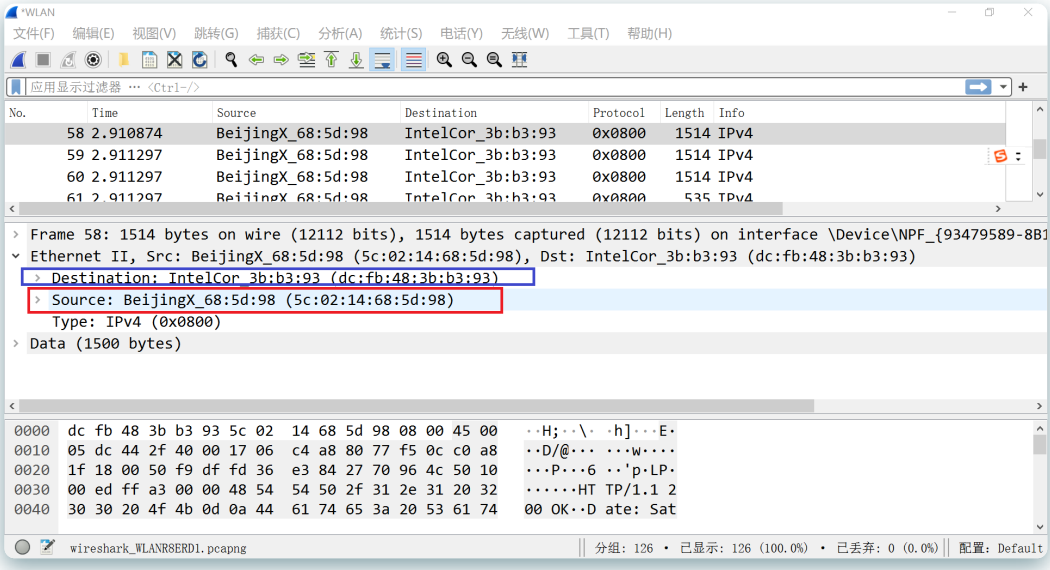
答：HTTP响应消息具体内容如下图所示：



根据图中红色框中内容，以太网源地址为 `5c:02:14:68:5d:98` ；这不是我的计算机的以太网地址或 `gaia.cs.umass.edu` 的以太网地址，而是离开子网的路由器地址。

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

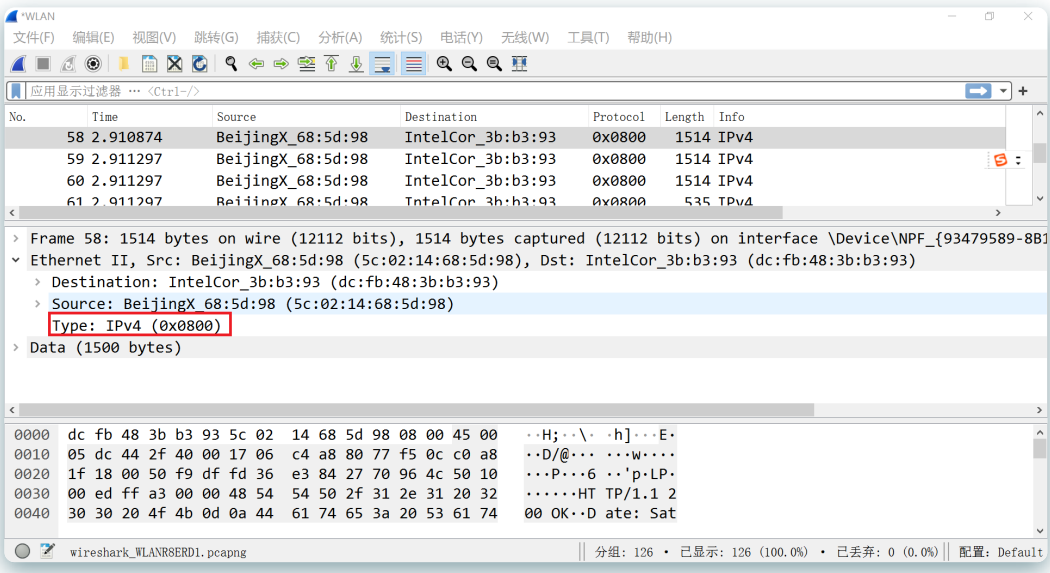
答：HTTP响应消息具体内容如下图所示：



根据图中蓝色框中内容，以太网帧目的地址为 `dc:fb:48:3b:b3:93` ，这是我的计算机的以太网地址。

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

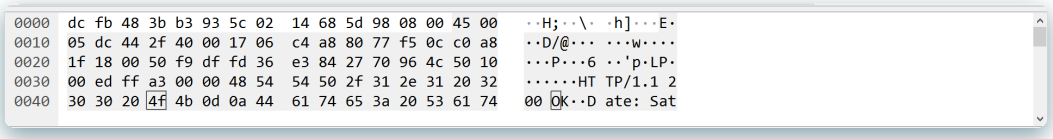
答：HTTP响应消息具体内容如下图所示：



根据红色框中内容，以太网帧上层协议的16进制值为 `0x8000` ，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?

答：以太网帧信息如下图所示：

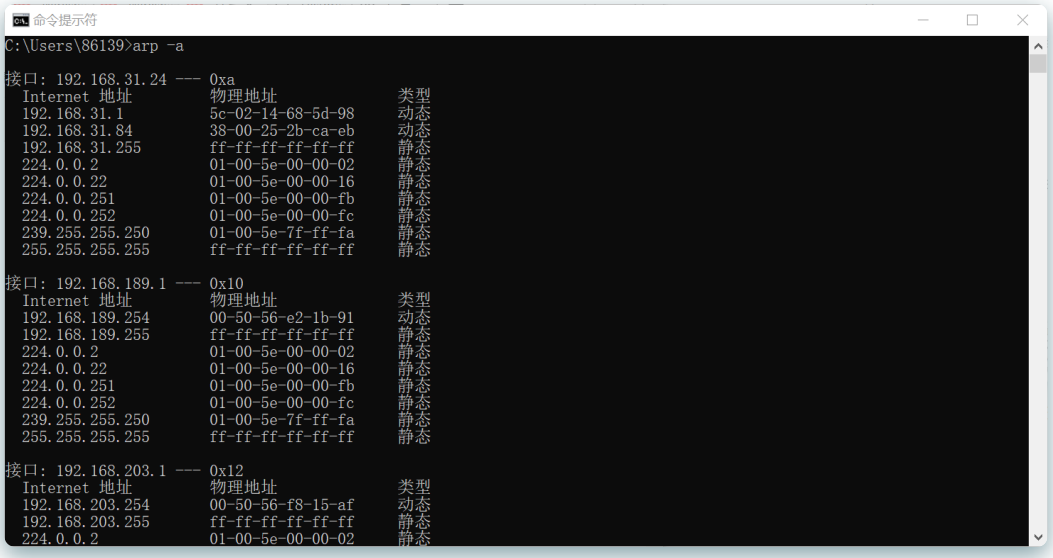


根据"O"在以太网帧中的位置，从开始到"O"出现一共有4*16+4=68个字节。

2.地址解析协议

1. 查看计算机上ARP缓存的内容。

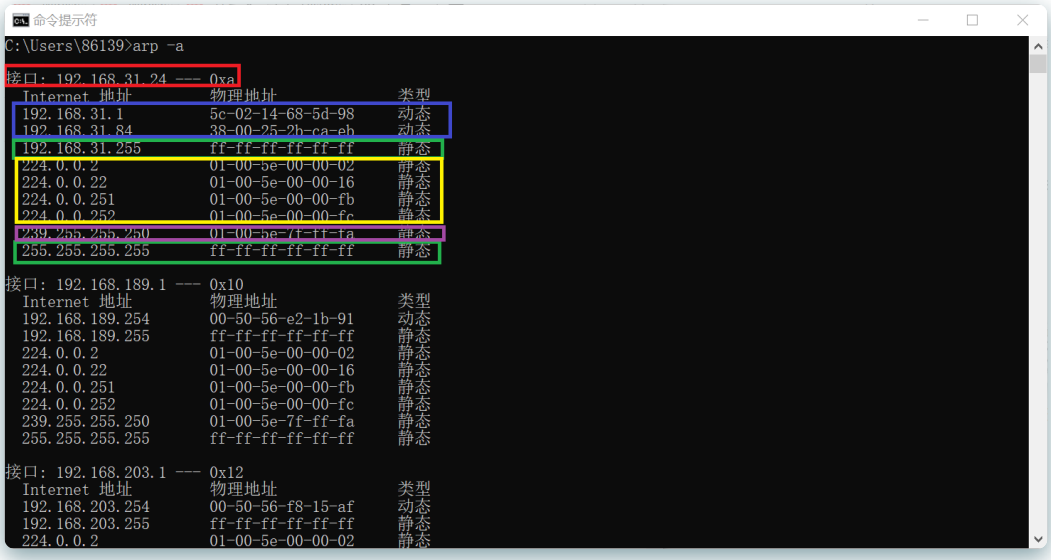
   在命令行中输入命令 `arp -a` ，得到arp缓存内容如下图所示：



   回答下列问题：

> 9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

答：计算机ARP缓存的内容如下图所示：

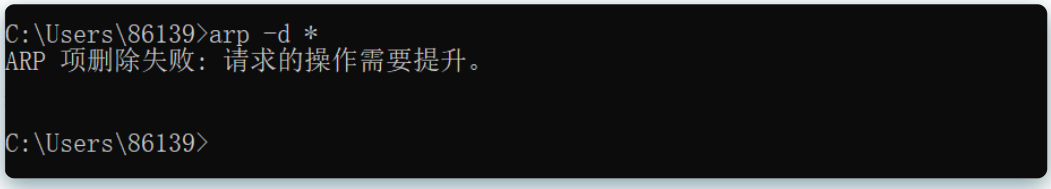


以第一个接口为例：

红色框中列值表示网卡；蓝色框中列值表示路由地址和路由MAC；绿色框中列值表示广播地址；黄色框中列值表示使用类组播地址；紫色框中列值表示管理类组播地址。

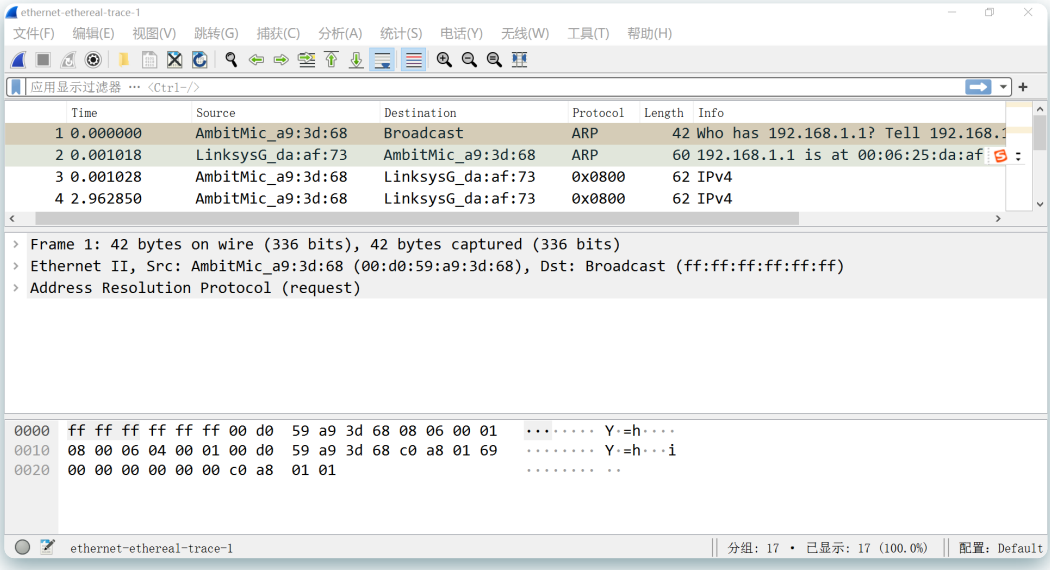
2. 清除ARP缓存。

在命令行中输入命令 arp -d *，得到下图结果：



删除缓存失败，故这一部分使用作者的抓包结果。

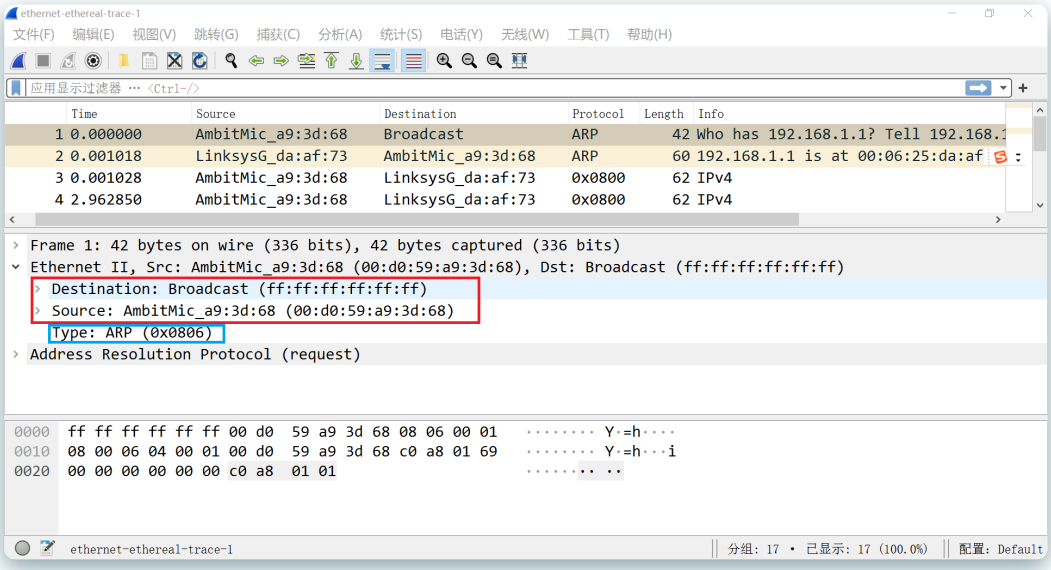
3. 对作者的数据包，更改wireshark抓获数据包的列表窗口，使其只显示有关IP协议以下的信息，在 Analyze->Enabled Protocols 中对 IPV4 选项取消勾选，如下图所示：



回答下列问题：

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

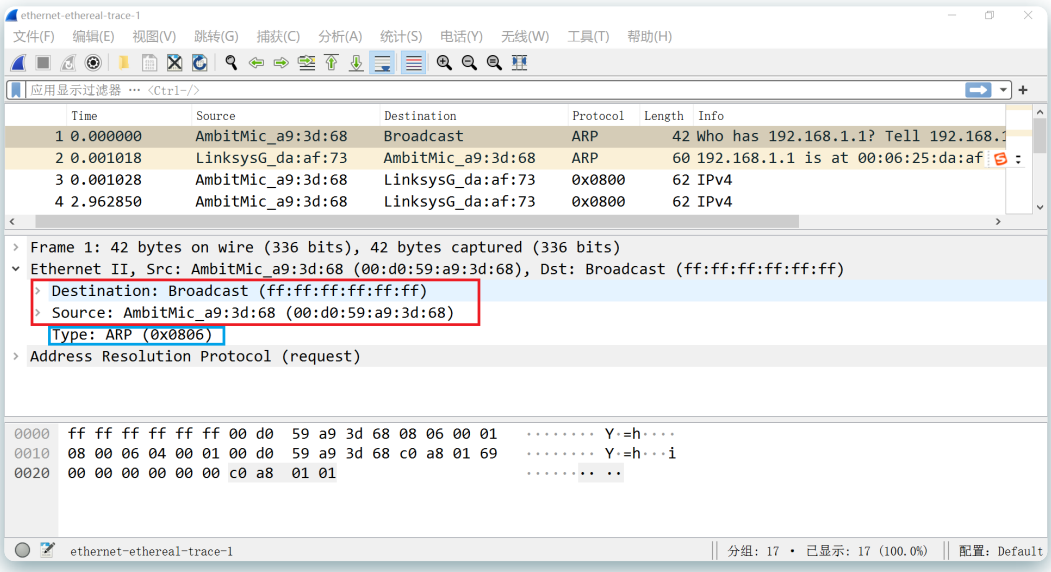
答：包含ARP请求消息的以太网帧具体内容如下图所示：



根据图中红色框中内容可知，以太网帧中源地址为 `00:d0:59:a9:3d:68` ，目标地址为 `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?

答：包含ARP请求消息的以太网帧具体内容如下图所示：



根据图中蓝色框中内容，以太网帧上层协议16进制值为 `0x0806` 。

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?

    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?

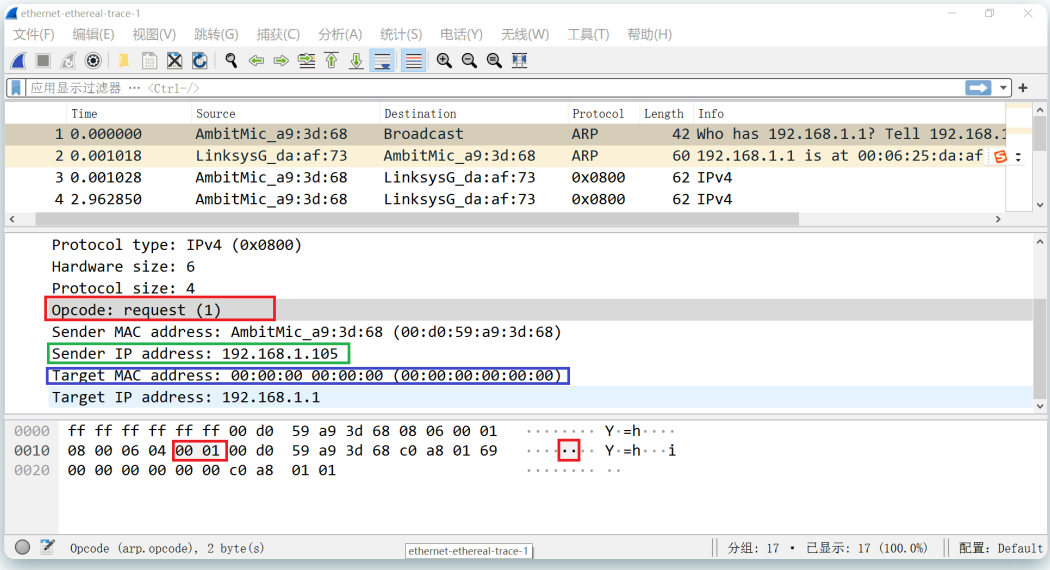
    c) Does the ARP message contain the IP address of the sender?

    d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

答:

(a)

如下图所示:



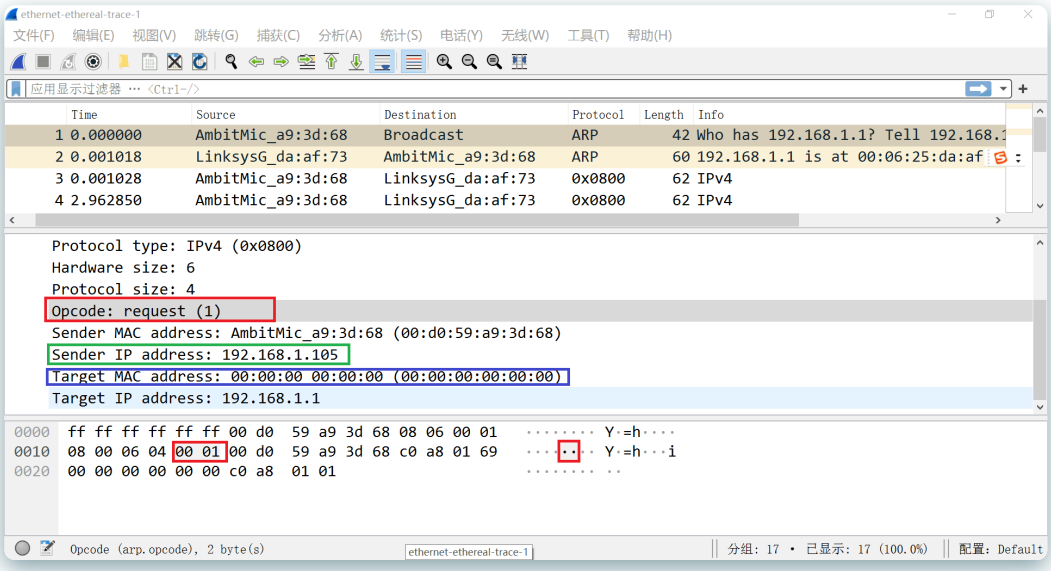
根据图中红色框中内容，从以太网帧开始到 opcode 字段有16+5=21个字节。

(b)

根据(a)中截图红色框中内容，操作码字段值为 1 。

(c)

ARP消息如下图所示：



根据绿色框中内容，可知ARP消息包含发送方IP地址，为 192.168.1.105 。

(d)

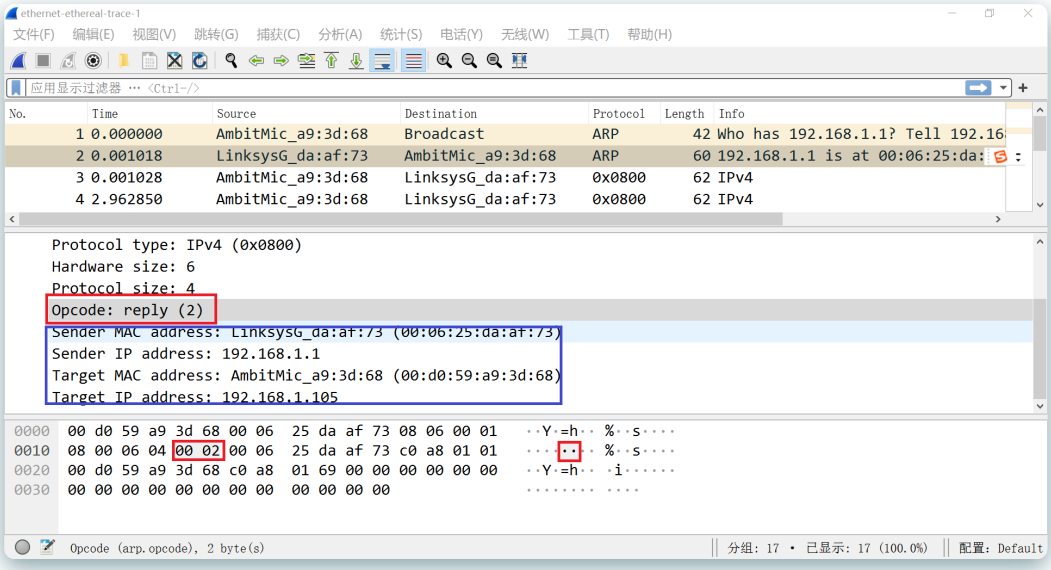
根据(c)中截图蓝色框中内容，要查询的以太网地址为 00:00:00:00:00:00 。

> 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?
>
> 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?
>
> 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?

答：

(a)

ARP回复消息如下图所示：



根据图中红色框中内容，从以太网帧开始到 opcode 字段有16+5=21个字节。

(b)

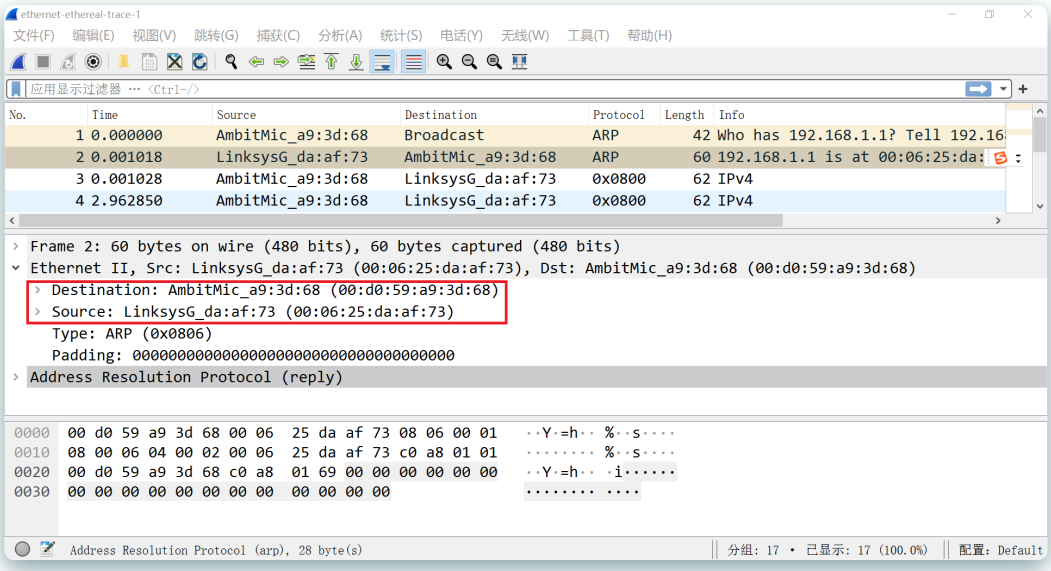
根据(a)中截图红色框中内容，操作码字段值为 2 。

(c)

根据(a)中截图蓝色框中内容，发送方IP地址为 192.168.1.1 ，MAC地址为 00:06:25:da:af:73 ，即为早期ARP请求的答案。

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

答：ARP响应消息具体内容如下图所示：



根据图中红色框中内容可知，以太网帧中源地址为 00:06:25:da:af:73 ，目标地址为 00:d0:59:a9:3d:68 。

> 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?

答：因为ARP发送的请求是广播的，所有在该网段内的电脑均可收到；ARP响应是单播的，只直接发送回发送方的以太网地址。

四.实验收获与感想

1. 深入理解了ARP和以太网协议。
2. 学习了arp有关的指令，可直接观察有关arp缓存的信息。
3. 加强了对wireshark的了解和运用，了解了更多数据的抓取位置。
4. 深入了解了计算机的链路层。