实验 4：ARP

班级_____　　学号　2021　　姓名_____

一、 实验内容

在这个实验中，我们将研究以太网协议和 ARP 协议。在开始这个实验之前，您可能需要复习文本 1 中的第 5.4.1 节（链路层寻址和 ARP）和第 5.4.2 节（以太网）。本实验的具体内容包括：

1. **捕获和分析以太网帧率**
2. **地址解析协议**

二、 实验操作步骤及结果

1、捕获和分析以太网帧

（1）实验步骤

① 首先，清空浏览器缓存。

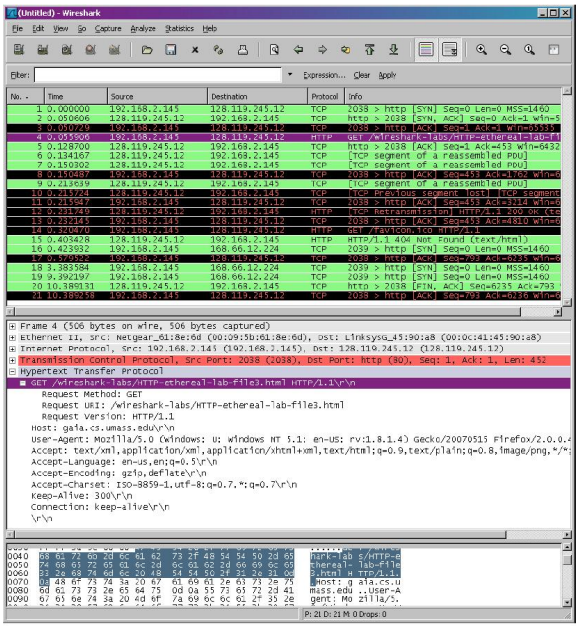
② 打开 Wireshark 数据包嗅探器。

③ 在浏览器中输入以下 URL：

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

浏览器应该显示美国权利法案。

④ 关闭 Wireshark 数据包捕获。Wireshark 中显示应如右侧图片所示：

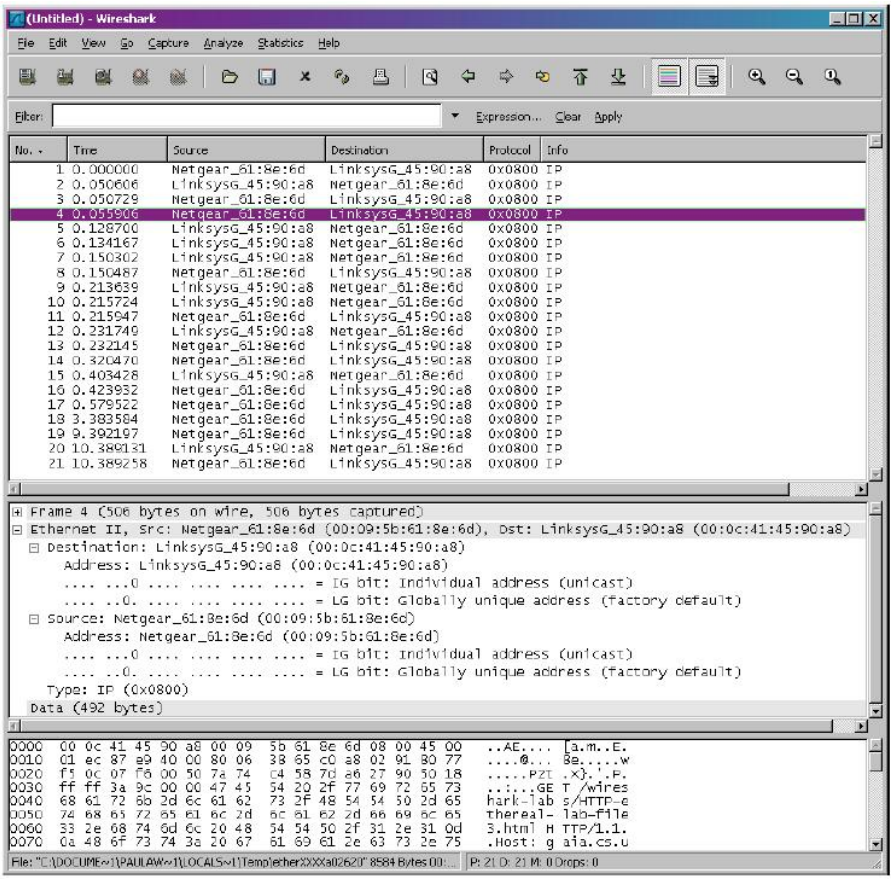


⑤ 找到从我的计算机发送到 gaia.cs.umass.edu 的 HTTP GET 消息的包号。以及由 gaia.cs.umass.edu 发送到您的计算机的 HTTP 响应消息的开头。

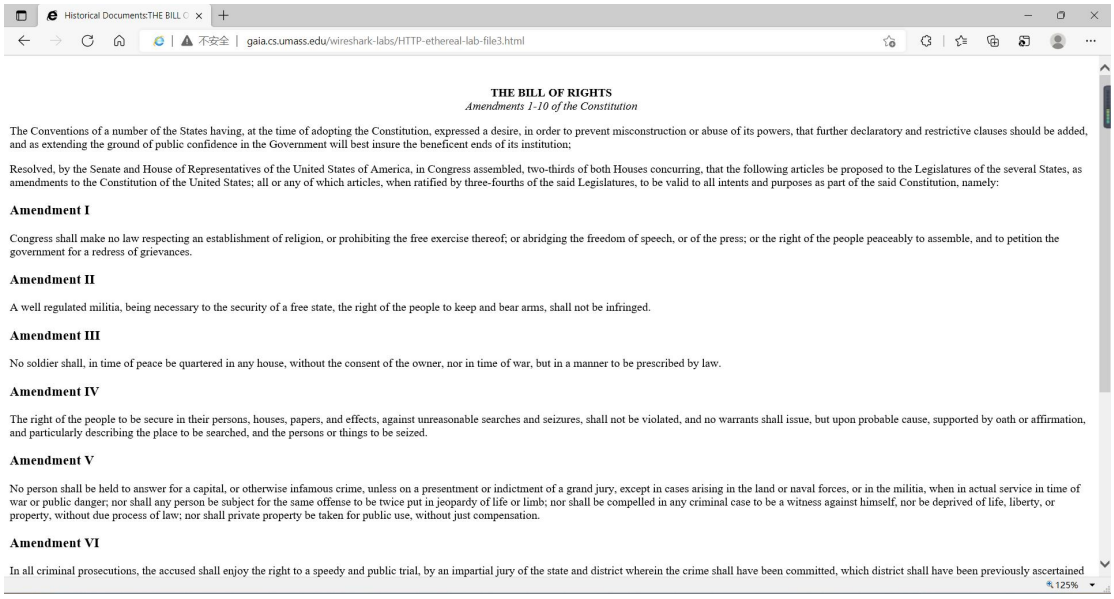
⑥ 更改 Wireshark 的“捕获数据包列表”窗口，只显示 IP 以下协议的

信息。在 Wireshark 中选择分析->启用的协议。然后取消选中 IP 框并选择 OK（确定）。

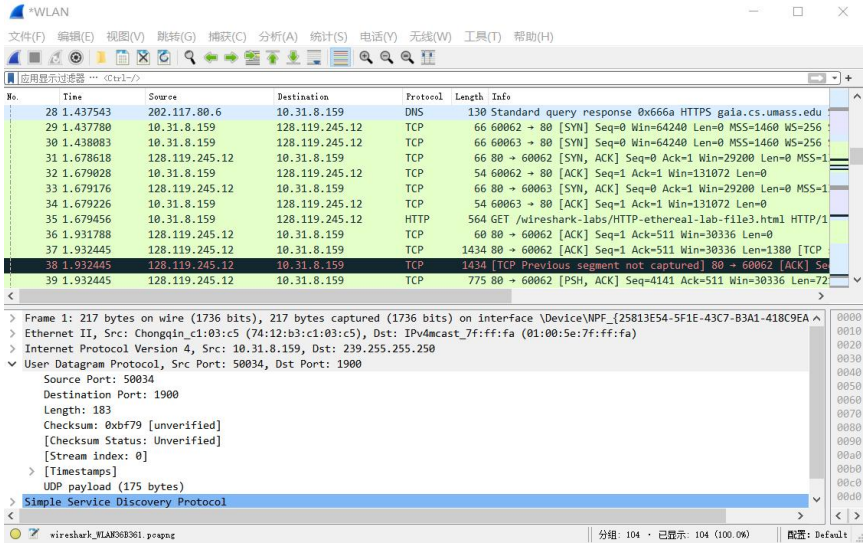
此时 Wireshark 中显示应如下面图片所示：

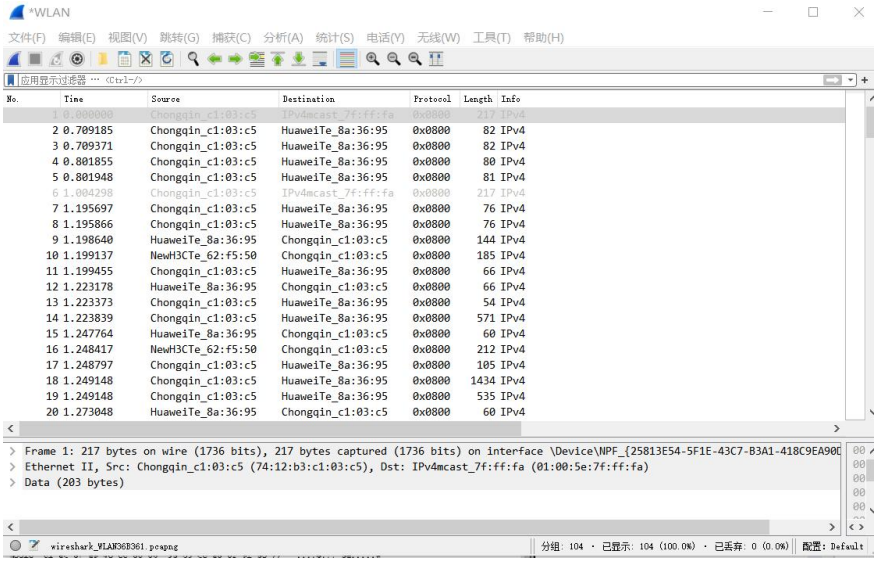


浏览器中：



我的 Wireshark 中的显示如下图：

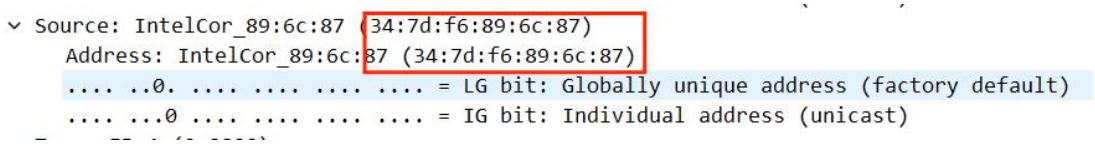




（2）回答问题

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

我电脑的以太网地址为 34:7d:f6:89:6c:87。如下图所示：



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.]

以太网帧中的 48 位目标地址是 a2:83:ad:3c:5a:0b，这不是 gaia.cs.umass 的以太网地址，而是我的主机的网关路由器的物理地址。如下图所示：

```
Destination: a2:83:ad:3c:5a:0b (a2:83:ad:3c:5a:0b)
    Address: a2:83:ad:3c:5a:0b (a2:83:ad:3c:5a:0b)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

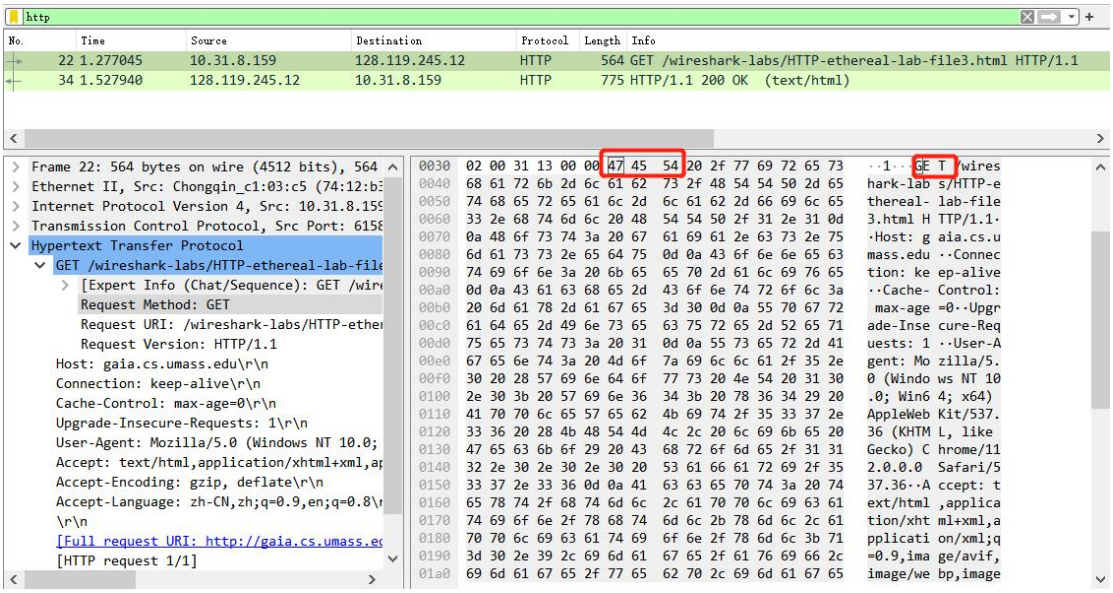
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Type：0x0800，表示网络层的 IPV4 协议。

```
        .... ..0. .... .... .... .... = LG bit: Globally unique
        .... ...0 .... .... .... .... = IG bit: Individual addr
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.31.8.159, Dst: 128.119.2
Transmission Control Protocol, Src Port: 61581, Dst Port: 80,
```

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

G 在第三行第 7 个，每行 16 字节，总共 3*16+7=55 字节。如下图所示：

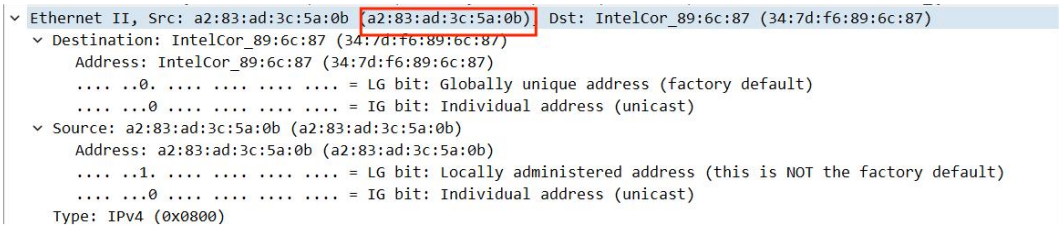


5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

源地址为：a2:83:ad:3c:5a:0b；

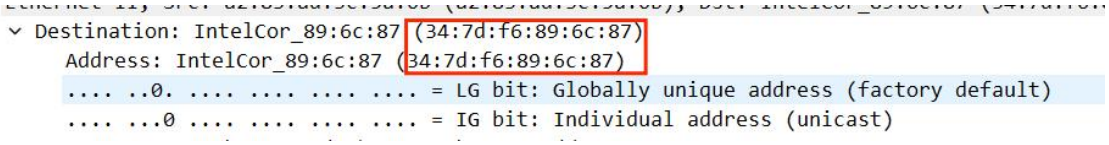
这个地址既不是我计算机的地址，也不是是 gaia.cs.umass.edu 的地址，这是我主机的网关路由器的物理地址；

离开子网的数据需要用到该地址。



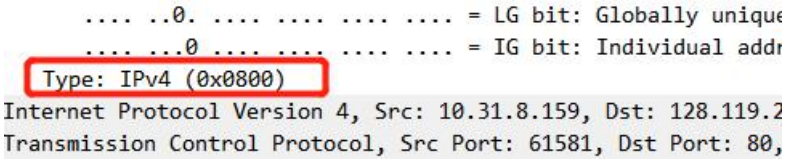
6.What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

目的地址 mac 为 34:7d:f6:89:6c:87，这是我电脑的物理地址。



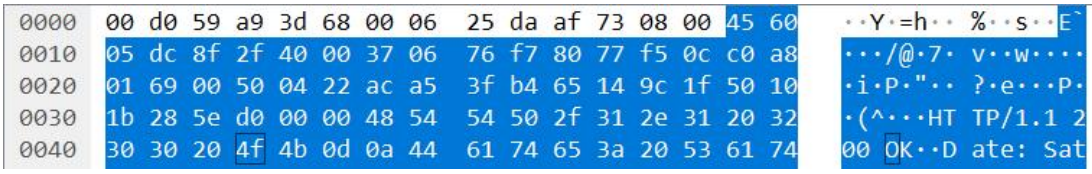
7.Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Type：0x0800，表示网络层的 IPV4 协议。



8. How many bytes from the very start of the Ethernet frame does the ASCII “0” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

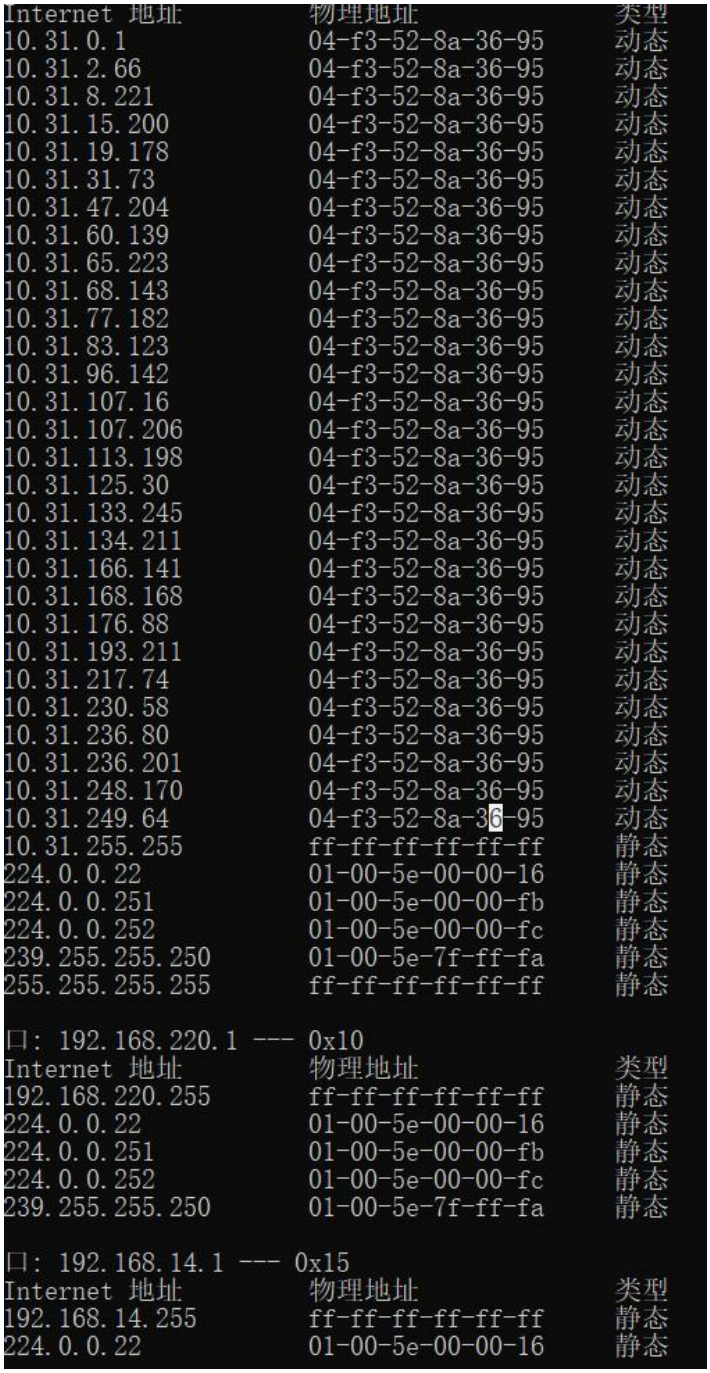
0 在第 5 行第 4 个，每行 16 字节，总共 4*16+4=68 字节。如下图所示：



2、地址解析协议

（1）实验步骤

① 在命令提示符中输入： arp -a，查看本机 ARP 表。



```
Internet 地址         物理地址              类型
10.31.0.1             04-f3-52-8a-36-95     动态
10.31.2.66            04-f3-52-8a-36-95     动态
10.31.8.221           04-f3-52-8a-36-95     动态
10.31.15.200          04-f3-52-8a-36-95     动态
10.31.19.178          04-f3-52-8a-36-95     动态
10.31.31.73           04-f3-52-8a-36-95     动态
10.31.47.204          04-f3-52-8a-36-95     动态
10.31.60.139          04-f3-52-8a-36-95     动态
10.31.65.223          04-f3-52-8a-36-95     动态
10.31.68.143          04-f3-52-8a-36-95     动态
10.31.77.182          04-f3-52-8a-36-95     动态
10.31.83.123          04-f3-52-8a-36-95     动态
10.31.96.142          04-f3-52-8a-36-95     动态
10.31.107.16          04-f3-52-8a-36-95     动态
10.31.107.206         04-f3-52-8a-36-95     动态
10.31.113.198         04-f3-52-8a-36-95     动态
10.31.125.30          04-f3-52-8a-36-95     动态
10.31.133.245         04-f3-52-8a-36-95     动态
10.31.134.211         04-f3-52-8a-36-95     动态
10.31.166.141         04-f3-52-8a-36-95     动态
10.31.168.168         04-f3-52-8a-36-95     动态
10.31.176.88          04-f3-52-8a-36-95     动态
10.31.193.211         04-f3-52-8a-36-95     动态
10.31.217.74          04-f3-52-8a-36-95     动态
10.31.230.58          04-f3-52-8a-36-95     动态
10.31.236.80          04-f3-52-8a-36-95     动态
10.31.236.201         04-f3-52-8a-36-95     动态
10.31.248.170         04-f3-52-8a-36-95     动态
10.31.249.64          04-f3-52-8a-36-95     动态
10.31.255.255         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

口: 192.168.220.1 --- 0x10
Internet 地址         物理地址              类型
192.168.220.255       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

口: 192.168.14.1 --- 0x15
Internet 地址         物理地址              类型
192.168.14.255        ff-ff-ff-ff-ff-ff     静态
224.0.0.22            01-00-5e-00-00-16     静态
```

② 清除 ARP 缓存。

```
C:\Users\钐二铭> netsh interface Ip delete arpcache
```

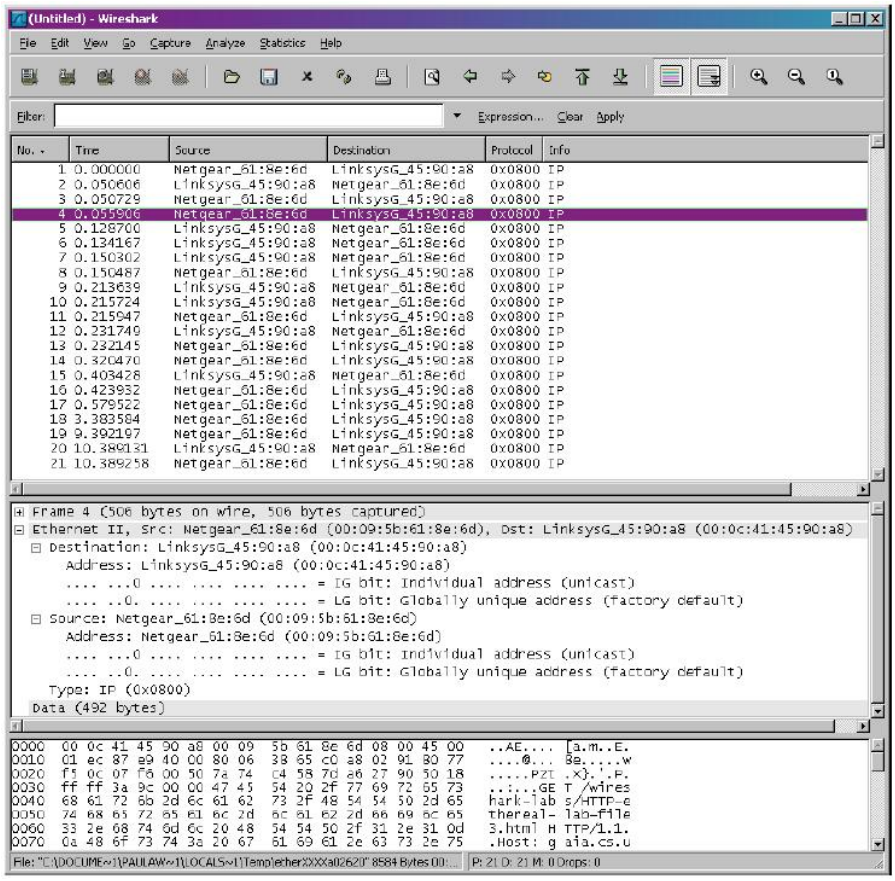
③ 清空浏览器缓存。启动 Wireshark 数据包嗅探器

④ 在浏览器中输入以下 URL：

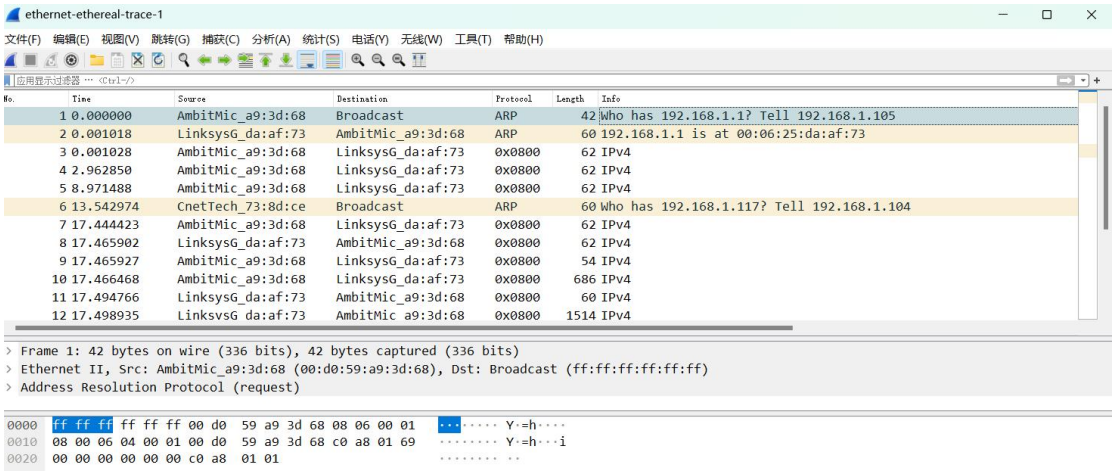
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html

你的浏览器会再次显示一份相当长的《美国权利法案》。

⑤ 在 Wireshark 中选择分析->启用协议。然后取消选中 IP 框并选择 OK。此时应该会看到一个 Wireshark 窗口，如下所示：



我抓取到的数据包里没有 arp 广播消息 Broadcast，因此下面使用题目提供 wireshark-traces.zip 中的数据包。如下图所示：



（2）回答问题

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

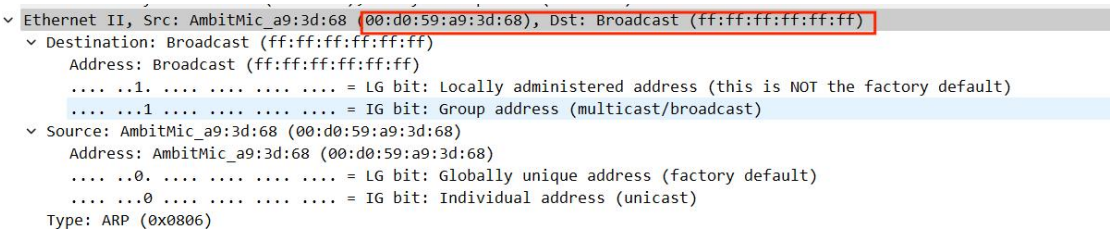
Internet 地址列表示 IP 地址；

物理地址列表示 MAC 地址，类型指示协议类型。

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

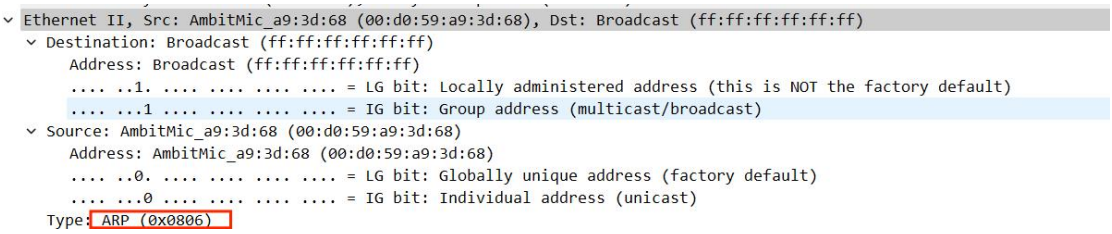
源地址为：00:d0:59:a9:3d:68；

目的地址为：ff:ff:ff:ff:ff:ff。如图所示：



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

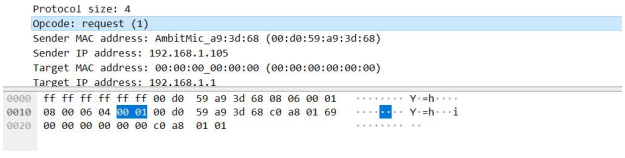
Type：ARP（0x0806），对应 ARP 协议。



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.

i.How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

从第二行第五个开始，16 + 5 = 21 Bytes。如下图所示：



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

操作码字段为 1。

```
Opcode: request (1)
```

iii. Does the ARP message contain the IP address of the sender?

包含 ARP 消息包含发送者的 IP 地址，为 192.168.1.105。

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

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

"目标 MAC 地址"字段设置为 00:00:00:00:00:00，请求为 broadcast，目标以太网全部为 0。

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

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?

从第二行第五个开始，16 + 5 = 21 Bytes。如下图所示：

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·=h·· ·i······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

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?

操作码字段为 2。

```
Opcode: reply (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?

对先前 ARP 请求的回复在“Sender address”字段中；

包含 IP 地址为 192.168.1.1 的发送方，以及目的以太网地址 00:d0:59:a9:3d:68。

```
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Target IP address: 192.168.1.105
```

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

源地址为：00:06:25:da:af:73；

目的地址为：00:d0:59:a9:3d:68。

```
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Target IP address: 192.168.1.105
```

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?
这是一个由于发送端发送的广播 arp 包。因此，同一子网中的每个主机都将收到该数据包。而 ARP 广播回复是单播的，只有请求的那台电脑才能收到，所以抓不到另一台电脑的 ARP 请求。

3、Extra Credit

EX-1. The arp command:
arp -s Inet
Addr 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?
当输入了正确的 IP 地址，但该远程接口的以太网地址不正确，则尝试连接输入的 IP 地址时，将得到错误的 MAC 地址。如果手动输入了不正确的以太网地址，接收 ARP 请求的远程主机将返回不正确的 ARP 响应,或者根本不会响应 ARP 请求，从而导致通信问题。

EX-2. 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.
默认情况下，ARP 缓存中的条目将存储 2 分钟。如果在这 2 分钟内使用条目，则截止时间将再延迟 2 分钟，直到超过 10 分钟。当条目存储 10 分钟时，必须将其删除。

三、实验中存在问题及分析

通过进行 ARP 实验，我对计算机网络的理解有了进一步的提升。首先是更加

熟悉了Wireshark软件的操作和功能，在解决问题时逐渐熟悉了wireshark软件，感到越发得心应手。在实验过程中我也遇到过一些小问题，这次实验遇到的问题和TCP实验中遇到的类似，都是自己抓到的数据包不能够很好得回答问题，需要使用题目提供的数据包。以后应该尽量在较好的网络环境下进行实验。

本次实验也加深了我对理论知识和一些生活里司空见惯的计算机网络现象的理解。现在，我终于明白了别人所说的不要随意连接陌生的免费WiFi的含义，原来计算机网络是如此神奇而复杂的。我希望在未来的学习和工作中，能够充分利用计算机网络的优势，让我们的生活变得更加安全和便捷。

这次充分的实践让我对计算机网络的学习更加深入和实际。我相信这种实践与理论相结合的学习方式，将有助于我更好地应对未来的挑战并在计算机网络领域取得更大的成就。