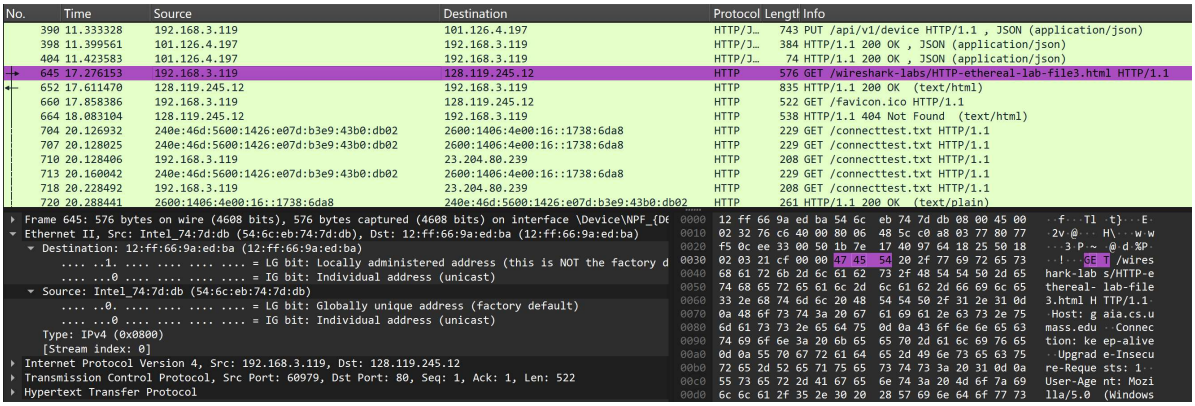
计算机网络 Lab8

一、实验任务一：Ethernet帧观察

捕获以太网帧

- step1：清空浏览器缓存
- step2：wireshark抓包
- step3：访问http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

选中包含HTTP GET消息的以太网帧，回答以下问题：



- **你的电脑的mac地址是多少?**

  我的电脑的mac地址是54:6c:eb:74:7d:db

- **以太网帧的目标mac地址是多少？这个地址是gaia.cs.umass.edu的mac地址吗?**

  目标mac地址是12:ff:66:9a:ed:ba。不是gaia.cs.umass.edu的mac地址

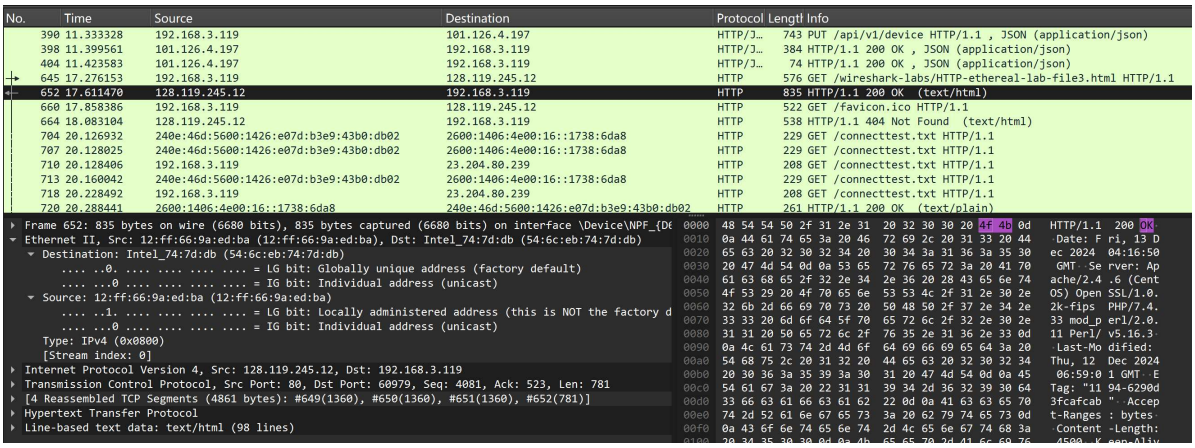
- **以太网帧EtherType字段值是多少，对应着什么协议?**

  以太网帧的EtherType字段值是`0x0800`，这对应着IPv4协议

- **从以太网帧的开始到"GET"中的'G'出现，有多少字节?**

根据wireshark抓包，前三行总共48个字节，第四行到`G`总共有7个字节，总共55个字节。

选中第一个包含HTTP响应消息的以太网帧，回答以下问题：



- **这个以太网帧中，源mac地址是多少？拥有这个以太网地址的设备是什么?**

  12:ff:66:9a:ed:ba拥有这个以太网地址的设备是我电脑连接热点的手机。

- **这个以太网帧中，目的mac地址是多少？拥有这个以太网地址的设备是什么?**

  54:6c:eb:74:7d:db拥有这个以太网地址的设备是我的电脑主机。

- **以太网帧EtherType字段值是多少，对应着什么协议?**

  以太网帧的EtherType字段值是 `0x0800`，这对应着IPv4协议

- **从以太网帧的开始到”OK”中的’O’出现，有多少字节?**

  根据wireshark抓包，到`o`总共有14个字节。

二、实验任务二：ARP

查看计算机上ARP缓存：　　MS-DOS: arp -a；
Linux/Unix/MacOS：arp

回答以下问题：

- 列出ARP缓存的内容(截图)，每列表示什么意思？

    1. **接口**：显示了ARP缓存对应的网络接口的IP地址。
    2. **Internet 地址**：这是与物理地址关联的IP地址。
    3. **物理地址**：这是与IP地址关联的MAC地址。
    4. **类型**：表示条目的类型，可以是“动态”或“静态”。动态条目是通过ARP请求和响应自动学习的，而静态条目是手动配置的。

```
C:\Users\IScream>arp -a

接口: 192.168.227.1 --- 0x3
  Internet 地址         物理地址              类型
  192.168.227.254       00-50-56-ff-77-cd     动态
  192.168.227.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     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
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.56.1 --- 0x4
  Internet 地址         物理地址              类型
  192.168.56.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     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: 192.168.229.1 --- 0x17
  Internet 地址         物理地址              类型
  192.168.229.254       00-50-56-eb-c1-56     动态
  192.168.229.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     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
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 10.223.122.88 --- 0x18
  Internet 地址         物理地址              类型
  10.223.0.1            10-c1-72-83-c8-1b     动态
  10.223.127.255        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
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

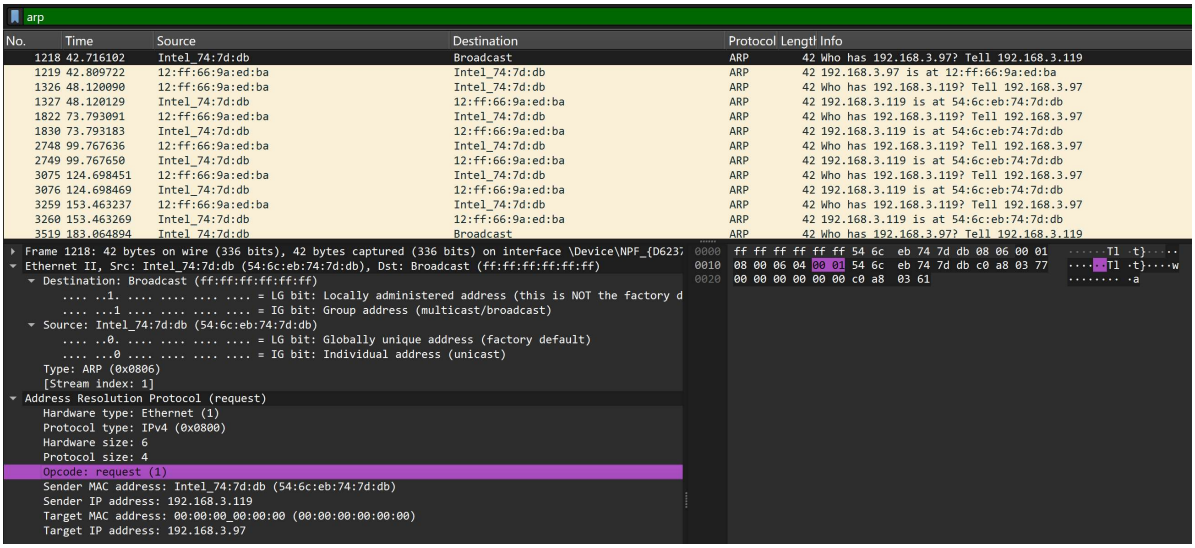
清除计算机上ARP缓存：　　MS-DOS: arp -d；
Linux/Unix/MacOS：arp -ad

抓取ARP包：

- step1 ： 清空ARP缓存

- step2：清空浏览器缓存
- step3：wireshark抓包
- step4：访问http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

抓取并观察ARP包，回答以下问题：



- **第一个包含ARP请求信息的以太网帧中，源和目的mac地址为?**

  源mac地址54:6c:eb:74:7d:db

  目的mac地址ff:ff:ff:ff:ff:ff

- **以太网帧EtherType字段值是多少，对应着什么协议?**

  0x0806，ARP协议

参考ARP规范，回答以下问题：

- **ARP操作字段在以太网帧的第几个字节?**

  第21个字节

- **进行ARP请求的以太网帧中，ARP负载部分操作字段值是多少?**

  0001

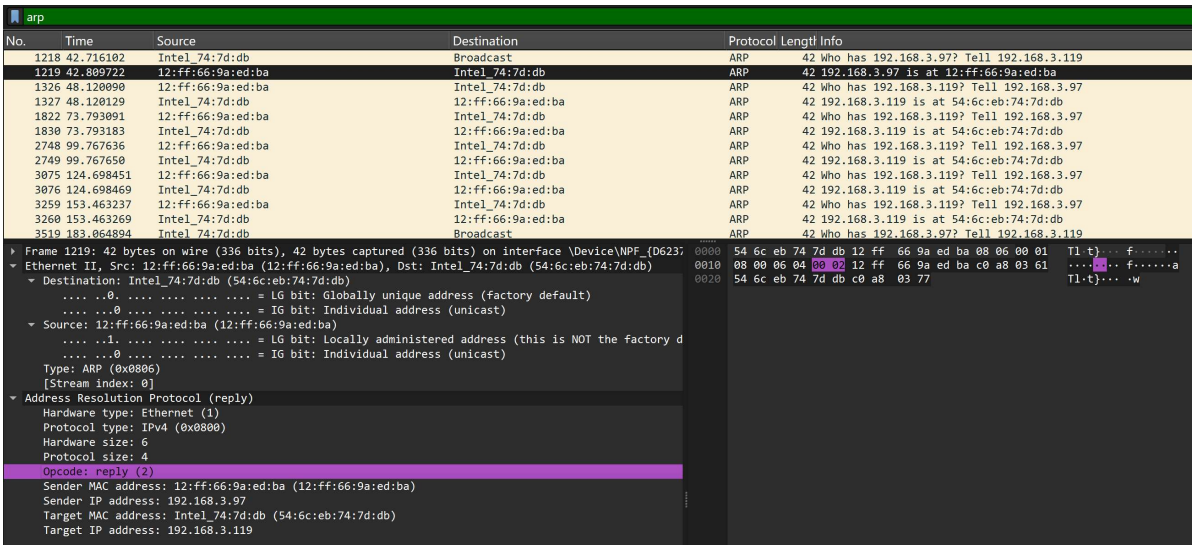
- **ARP消息是否包含发送方的IP地址?**

  包含。

- **在ARP请求中从哪里看出我们想查询相应IP的mac地址?**

  ARP请求的操作字段为01，表示是一个查询请求(request)。

找到ARP请求对应的回应包，回答以下问题:



- **ARP操作字段在以太网帧的第几个字节?**

  第21个字节

- **进行ARP响应的以太网帧中，ARP负载部分操作字段值是多少?**

  0002

- **ARP回应之前请求信息的内容?**

  192.168.3.97 is at 12:ff:66:9a:ed:ba

- **包含ARP回应信息的以太网帧中，源和目的mac地址为?**

  源mac地址:12:ff:66:9a:ed:ba

  目的mac地址:54:6c:eb:74:7d:db