计算机网络-实验2:0ucer勇闯链路层

姓名：翟一航 学号：23020011046

一、实验目的

To explore the details of Ethernet frames. Ethernet is a popular link layer protocol. Modern computers connect to Ethernet switches rather than use classic Ethernet.

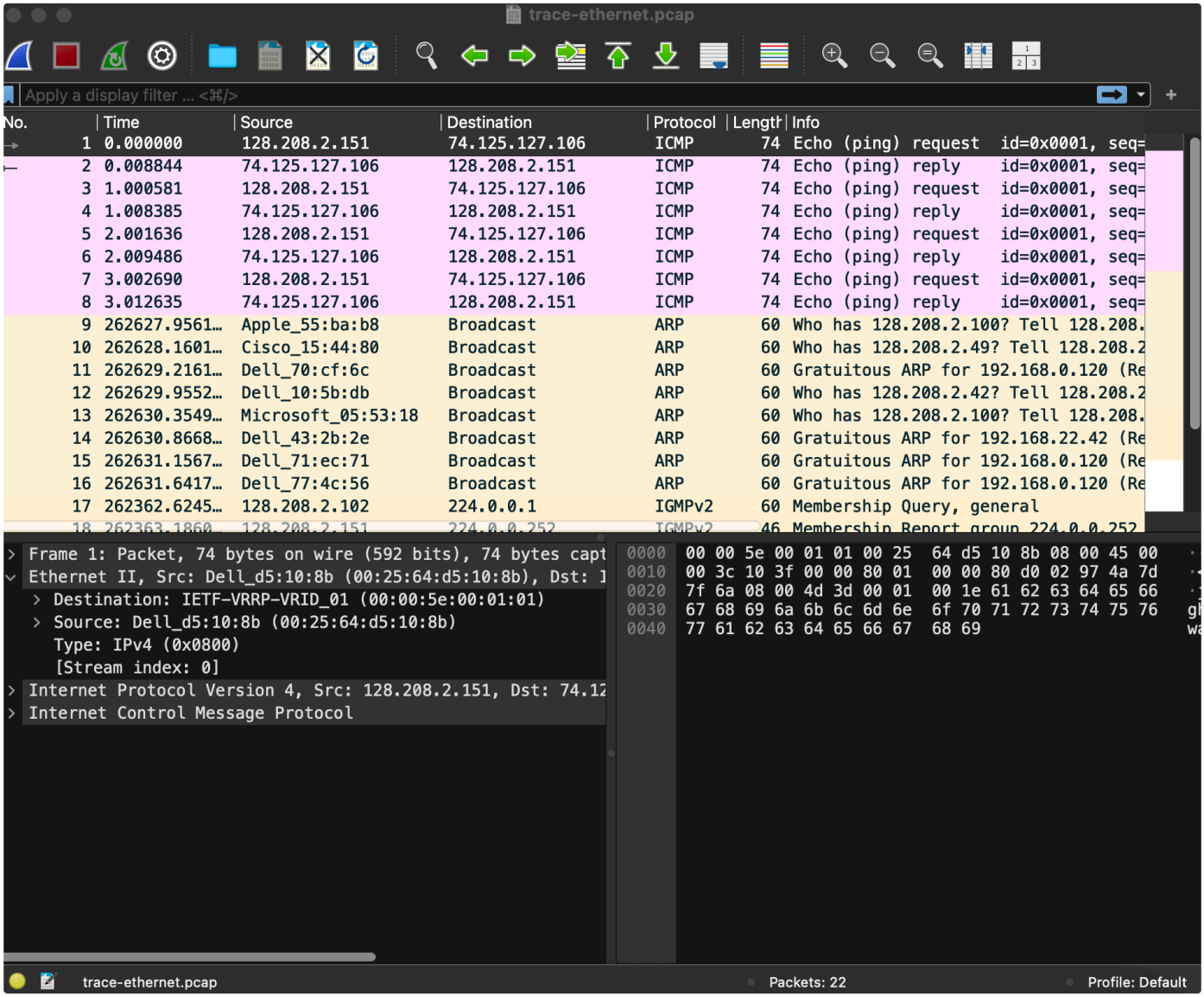
二、实验环境

环境	说明
操作系统	MacOS
抓包工具	Wireshark
网络接口	Wi-Fi:en0
数据包过滤器	ether multicast

三、实验内容

Step 1:Load the Lab Trace

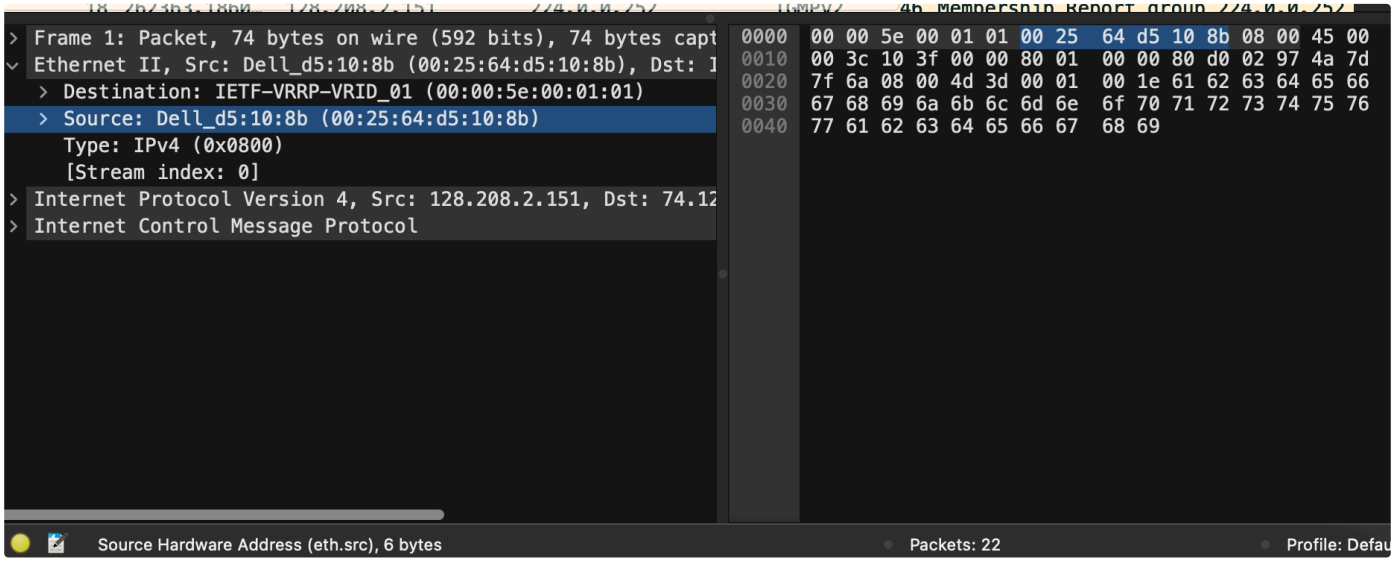
下载实验室的跟踪文件，并打开，得到如下界面：



Step 2:Inspect the Trace

> Q1. What is the MAC address of the source of # 1 from IP address 128.208.2.151?

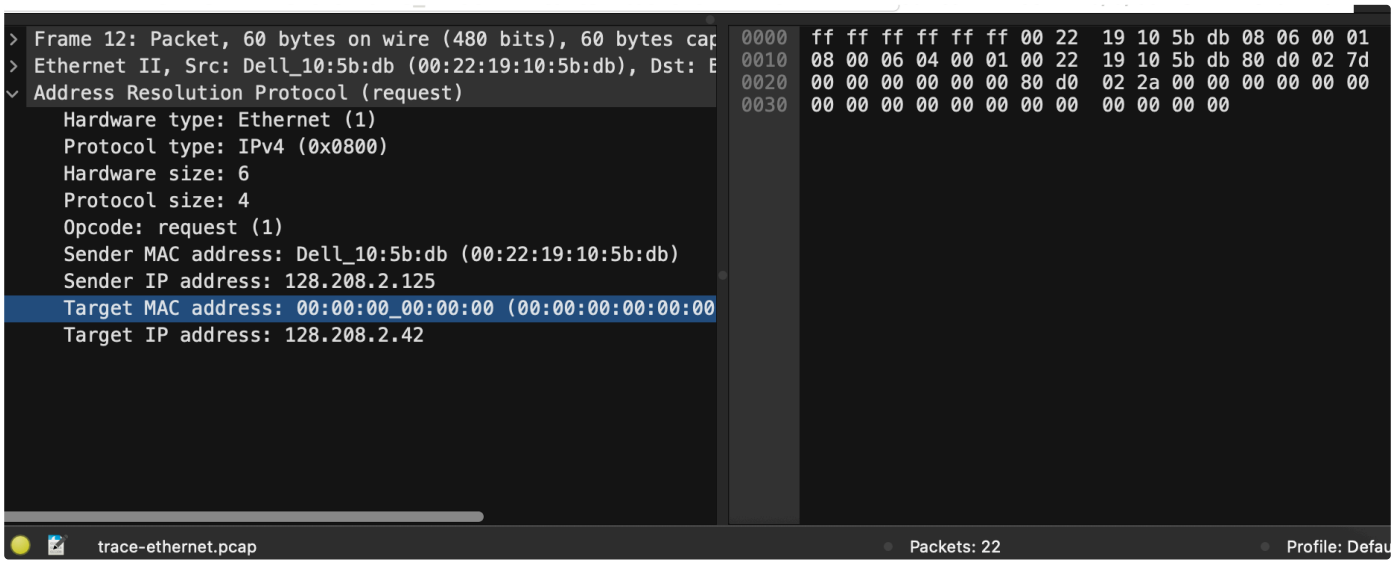
点击1号数据包，在下边的详细信息窗口查看数据包的具体内容。在以太网链路层可以看见源MAC地址（Source），长度为6字节，为 `00:25:64:d5:10:8b` 。



> Q2. Click on # 12 and expand the Address Resolution Protocol section in middle pane. What does Target MAC address: 00:00:00:00:00:00 mean?

点击12号数据包并展开“Address Resolution Protocol”部分后，可以看到“Target MAC address: 00:00:00:00:00:00”，这说明发送这个ARP请求的设备还不知道目标 IP 地址对应的 MAC 地址是什么，它正在询问和等待这个信息，所以发送者使用一串全0作为占位符，来填充目标 MAC 地址字段。

之后，当拥有目标 IP 地址对应的 MAC 地址的设备收取到这个广播请求之后，它才会单独回复一个ARP应答，这个包中包含发送者缺少的那部分 MAC 地址。



> Q3. Click again on # 12 and expand the Address Resolution Protocol section in middle pane.Why is the protocol type listed as IP when it is not an IP packet?

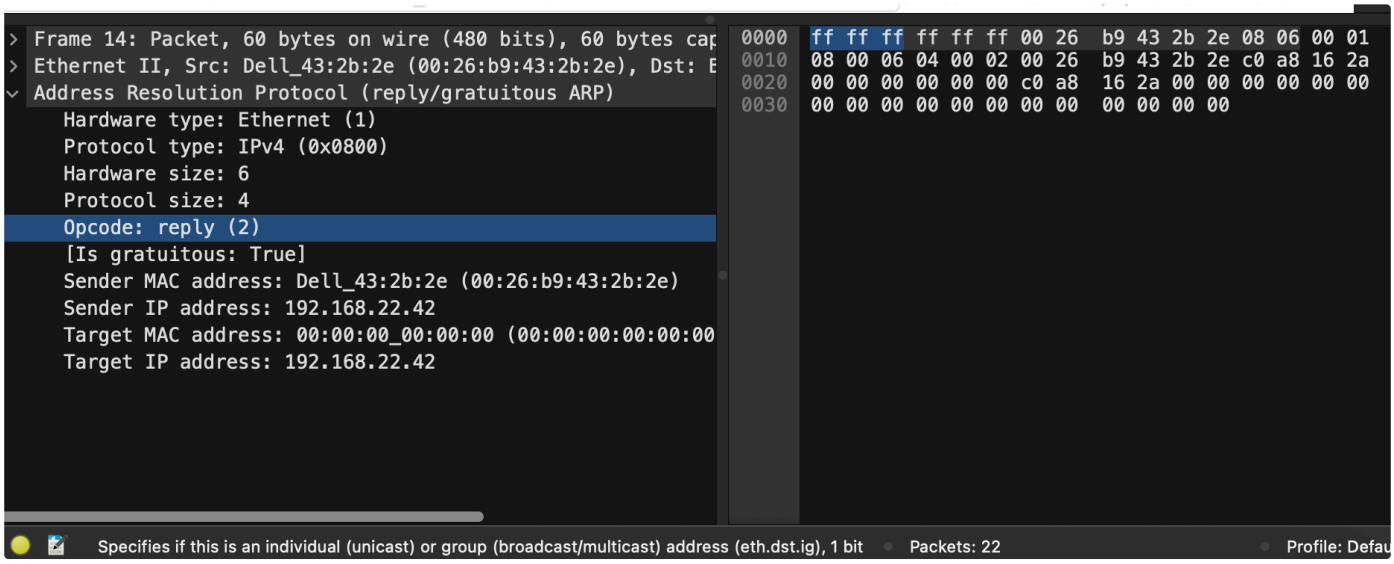
如上图所示，“Protocol type: IPv4 (0x0800)”。这是因为 ARP 协议的工作就是为 IP 协议服务的，它询问的内容是关于一个 IP 地址的信息，它定义了 ARP 请求和应答中携带的网络层地址类型。

Step 3:Ethern Frame Structure

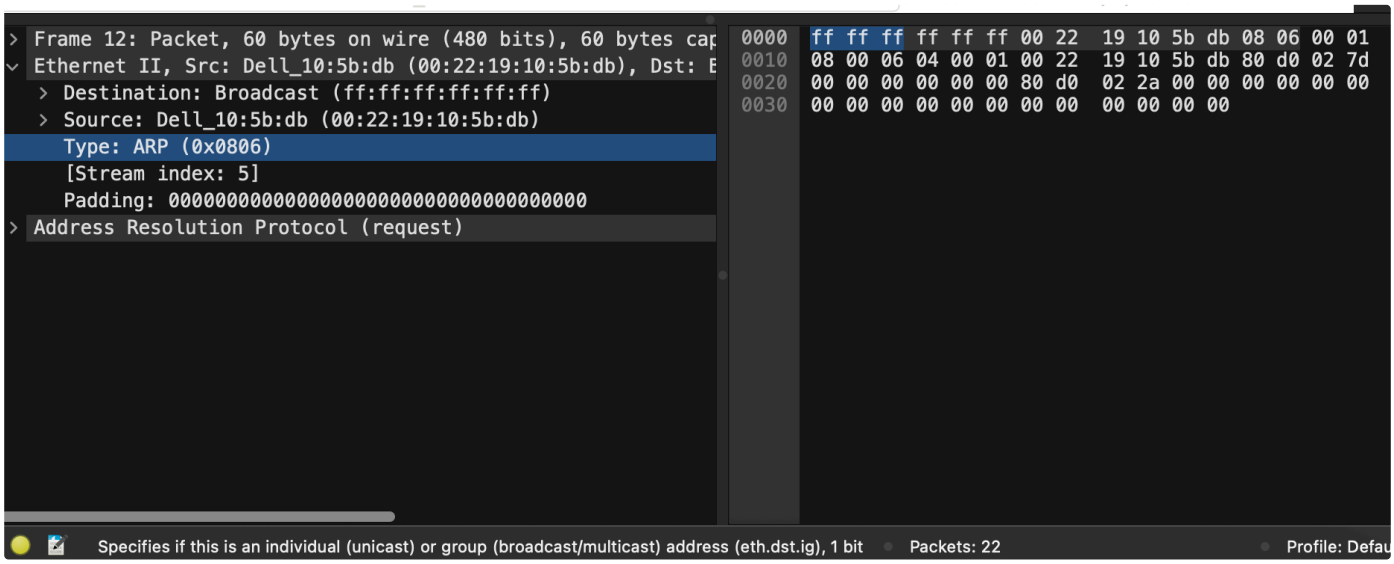
> Q1. Click on # 12 and expand the Address Resolution Protocol section in middle panel through the down arrow [v]. What does opcode (1) signify? What does opcode (2) signify?

仍然如上图所示，12号数据包的操作码为“request (1)”，这说明在此次抓包中，12号数据包是一个 ARP 请求，它的操作码是1。它是一台设备在局域网内发出的广播，目的是询问目标 IP 地址的 MAC 地址。

如下图所示，14号数据包的操作码为“reply (2)”，这说明在此次抓包中，14号数据包是一个 ARP 回复，它的操作码是2。它是对于 ARP 请求的回复，即拥有目标 IP 地址和对应 MAC 地址的设备对该请求进行回复，由于该设备也不知道具体是哪个设备发出的请求，所以也以广播的形式进行回复，Target MAC address 也为 00:00:00:00:00:00。



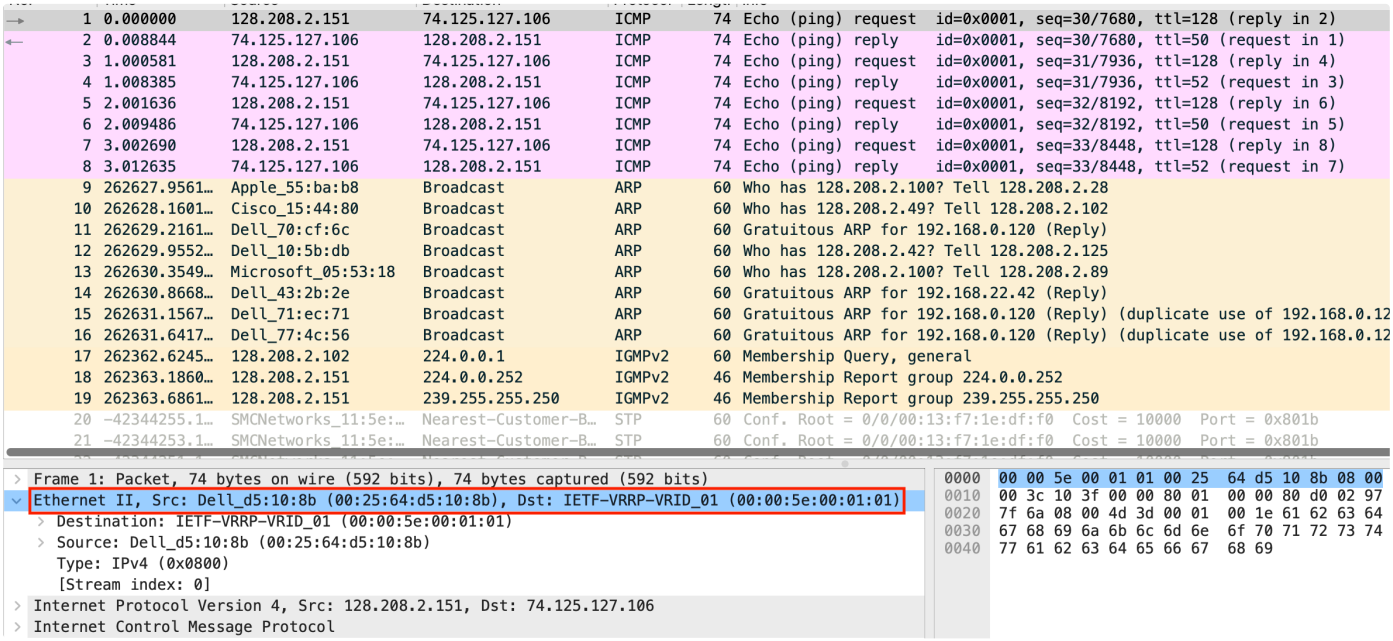
> Q2. Click on # 12 and expand using the [v] arrow and give the hexadecimal value for the two-byte Ethernet Frame type field?



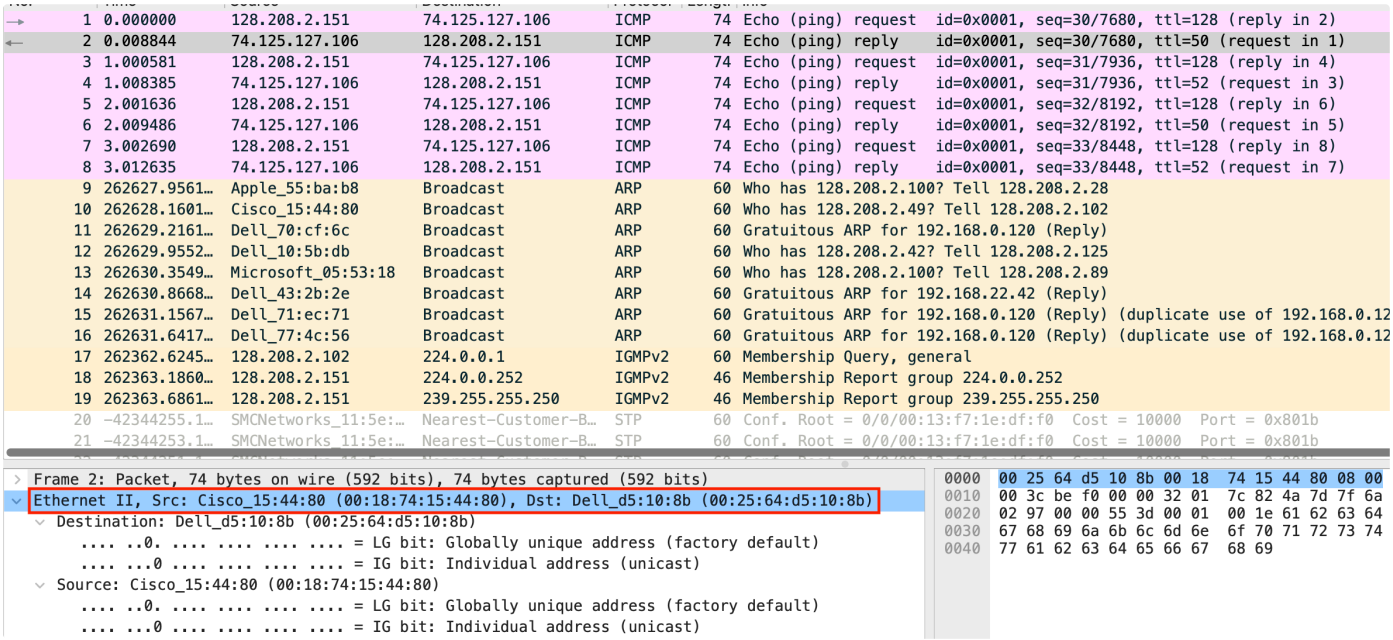
如上图所示，查看12号数据包的具体内容，点击展开“Ethernet II”层内容，可以看到“Type: ARP (0x0806)”，因而两字节以太网帧类型字段的16进制值为 `0x0806` ，这是对于 ARP 协议的固定值。

Step 4:Scope of Ethernet Addresses

1号数据包的内容：



2号数据包的内容：

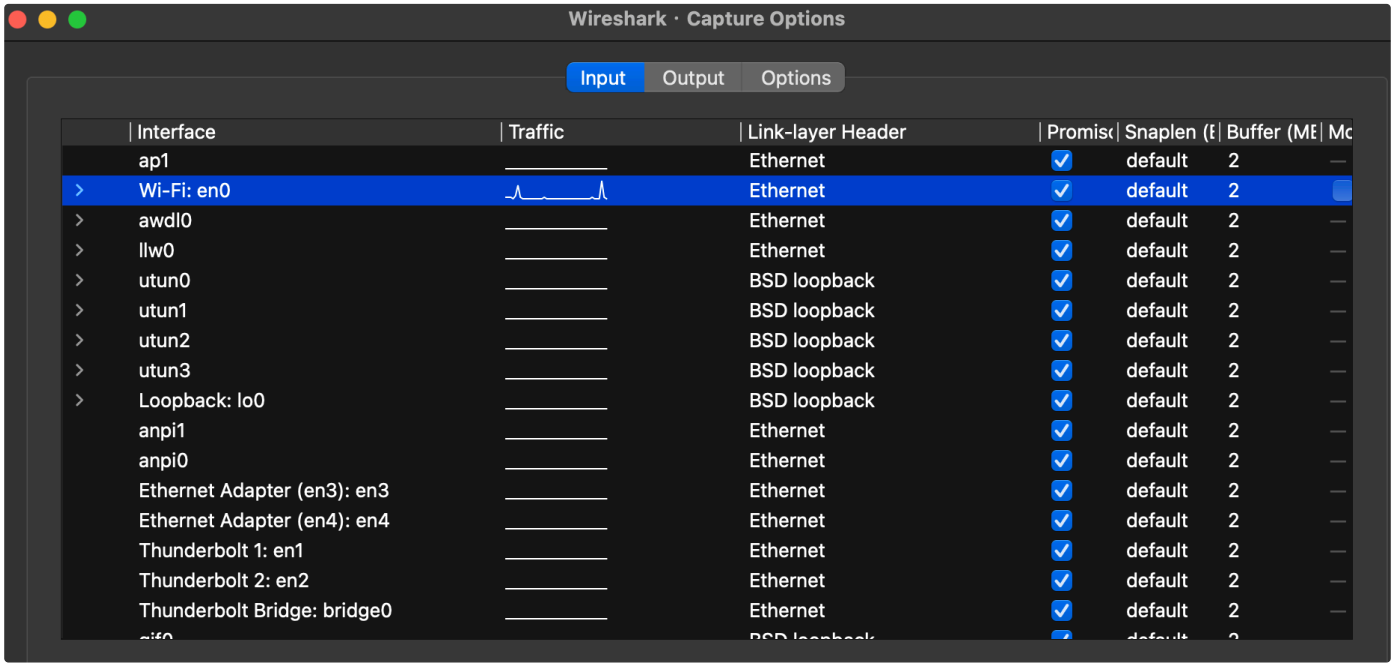


> 网关 MAC 地址

现在本地设备要向远端服务器发送消息，但是不知道目标的 MAC 地址，因而将数据包发送给网关，正如1号数据包中的内容，本地设备的 MAC 地址为 `00:25:64:d5:10:8b` ，网关的 MAC 地址为 `00:00:5e:00:01:01` 。网关将信息转发给目标远端服务器，信息中还包含本地设备的 MAC 地址，因而远端服务器（MAC 地址为 `00:18:74:15:44:80` ）可以直接回复本地设备，无需经过网关进行通信。（正如1号数据包中的注释“reply in 2”，和2号数据包中与之对应的“request in 1”）

Step 5:Broadcast Frames

在终端中输入命令 `wireshark &` 打开一个新的 Wireshark 窗口，并选择要监听的以太网端口。可以发现有 en0 - en4 共5个端口，但是我们选择监听 en0 端口。



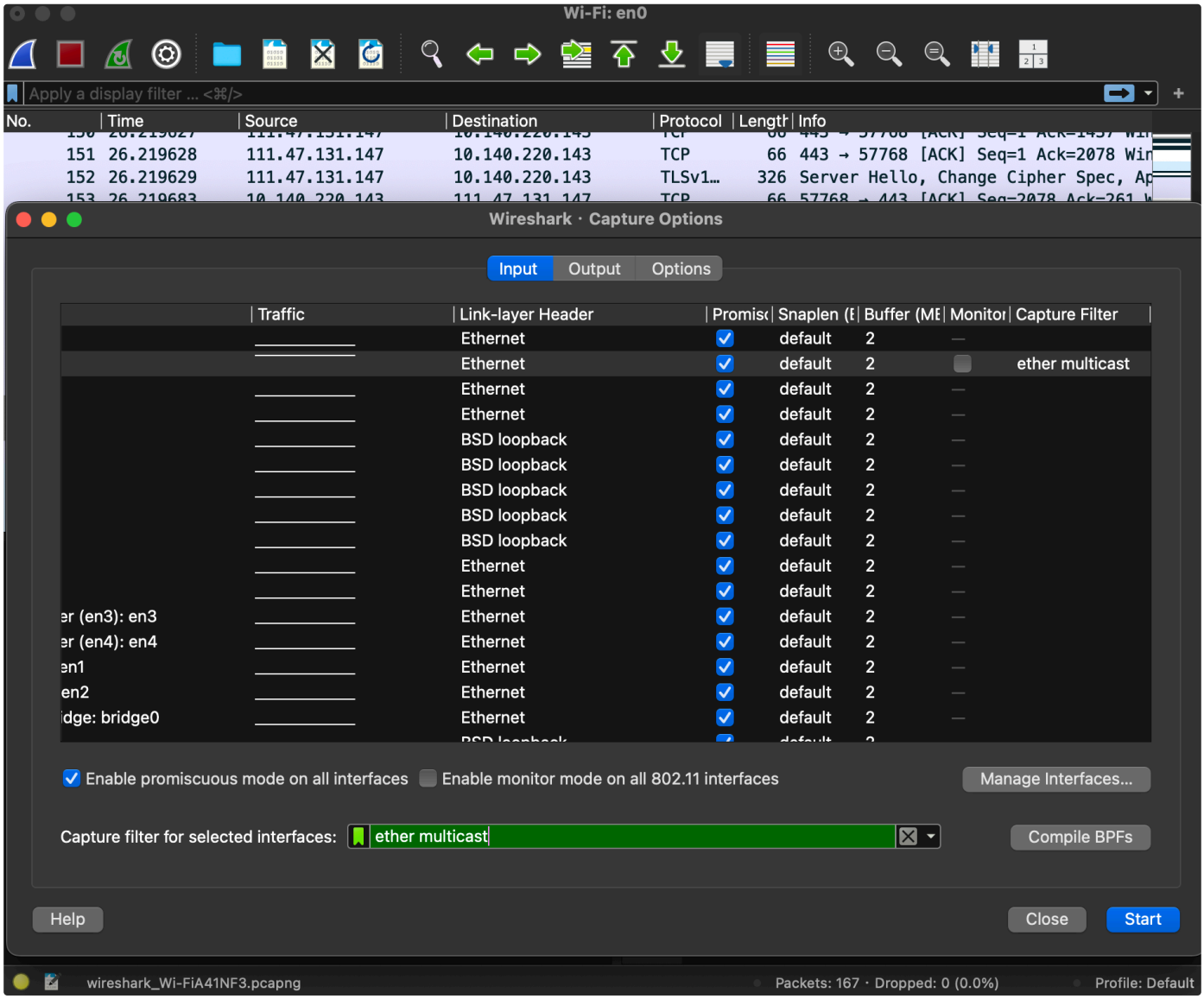
这是因为我的电脑使用校园网进行上网，使用的是 en0 端口，观察图形化界面也可以看到只有该端口后有流量曲线，在终端中输入命令 `ifconfig` 查看也可以进行验证，如下图所示：

```
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 1a:48:ad:74:84:82
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 1a:48:ad:74:84:83
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:65:e5:b2:fa:80
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:65:e5:b2:fa:84
        media: autoselect <full-duplex>
        status: inactive
```

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 66:43:46:09:d4:bc
        inet6 fe80::185b:c74d:9b63:63df%en0 prefixlen 64 secured scopeid 0xb
        inet 10.140.220.143 netmask 0xfffffc00 broadcast 10.140.223.255
        inet6 240c:ca02:2140:dbc:4:2047:726b:cc47 prefixlen 64 autoconf secured
        inet6 240c:ca02:2140:dbc:e87c:81b4:31d:db37 prefixlen 64 autoconf temporary
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

可以发现只有 en0 端口的 status 为 active，其余都为 inactive。

接下来需要选择 `filter`，要注意的是只有先停止捕获数据包才能够更改，如下图所示：



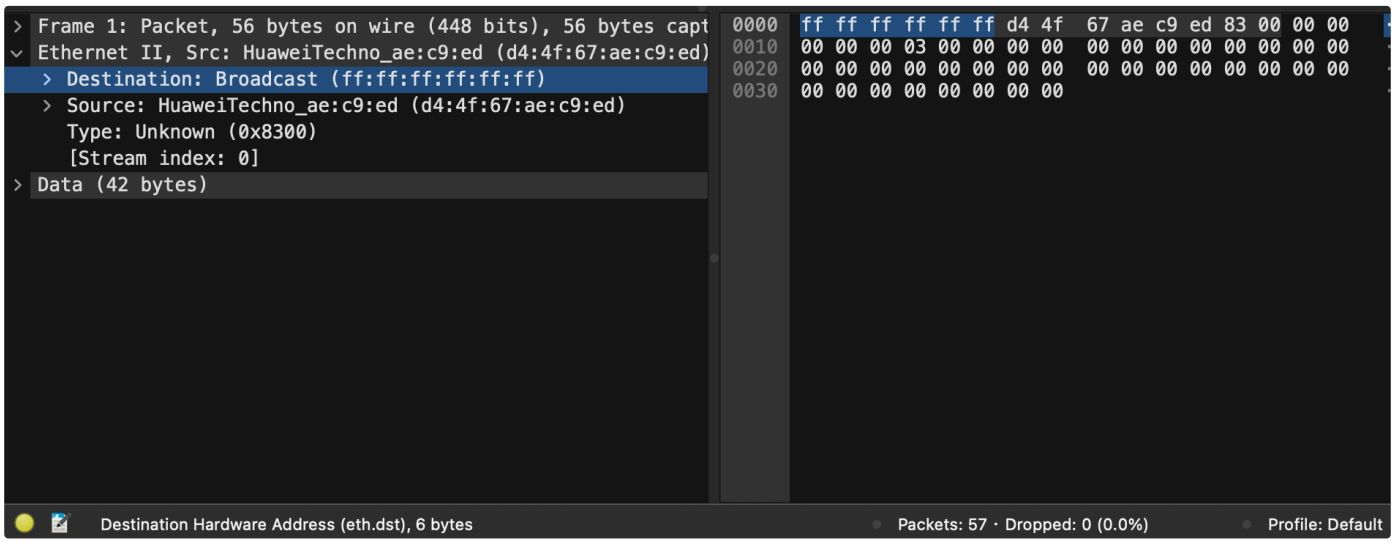
Examining Live Ethernet Multicast Traffic

过滤器 `ether multicast` 的作用是只捕获和显示目标 MAC 地址为广播或者多播类型的以太网帧

> a. What is the broadcast Ethernet address, written in standard form as Wireshark displays it?

广播以太网地址的标准形式为 `ff:ff:ff:ff:ff:ff` ，这个目标地址会使得该数据包能够被所有设备进行捕获。

可以点击一个广播以太网数据包进行查看，如图：



> b. Which bit of the Ethernet address is used to determine whether it is unicast or multicast/broadcast?

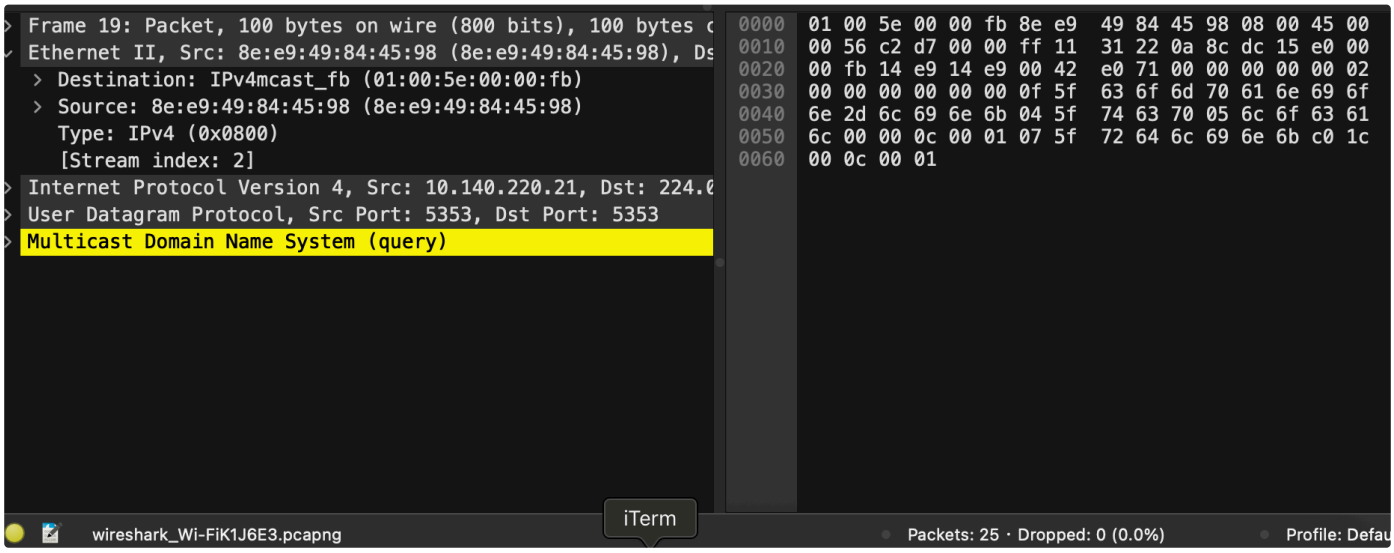
数据包的第一个字节的最低有效位

如果这一位为1，则说明这是一个广播或者多播的地址，指向一组接收者；

如果这一位为0，则说明这是一个单播地址，指向网络中的某一个具体的设备。

补充：

广播和多播的数据包的第一个字节的最低有效位尽管都为1，但是他们的 Destination 还是有着显著的差别，以下为一个多播数据包的具体内容：



可以发现 Destination 并非全为 ff，只是仍然保证了第一个字节的最低有效位为1。

四、总结建议

通过此次实验，我对于计算机网络的链路层、以太网帧的结构和工作原理都有了更深刻的理解。

通过分析捕获的数据包，我更直观地认识了以太网帧的各个字段，包括源/目的 MAC地址、类型字段等，更直观地认识到了他们在网络通信中的作用。

通过观察ARP请求和应答数据包，我理解了 ARP 协议如何完成从 IP 地址到 MAC 地址的解析过程。特别是理解了操作码1和2分别代表请求和应答，以及目标MAC地址全零的含义。

除此之外，我还学会了通过 MAC 地址的第一个字节的最低位来区分单播、多播/广播地址，这是识别网络流量类型的重要技能，还认识了广播和多播在局域网中的作用，它们是链路层局域网正常通信的基础。