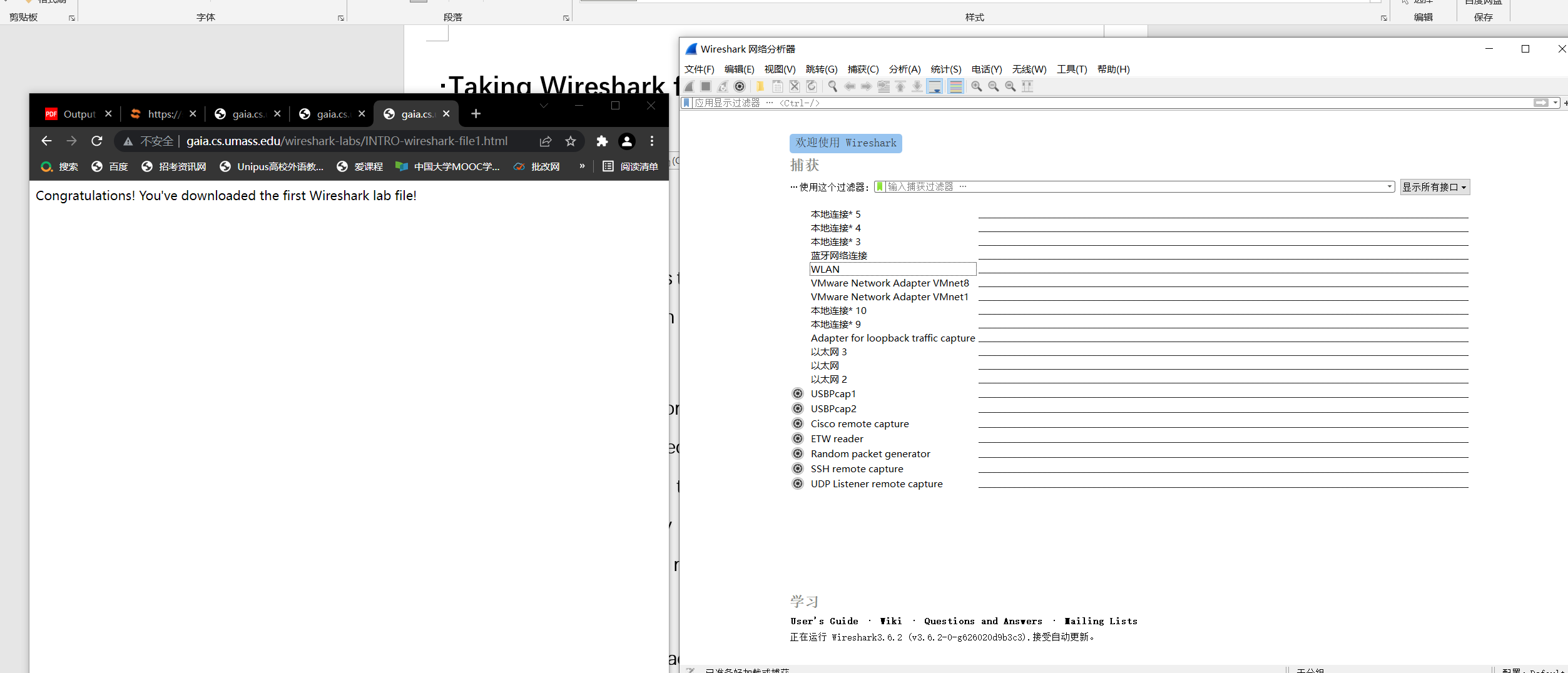
Taking Wireshark for a Test Run

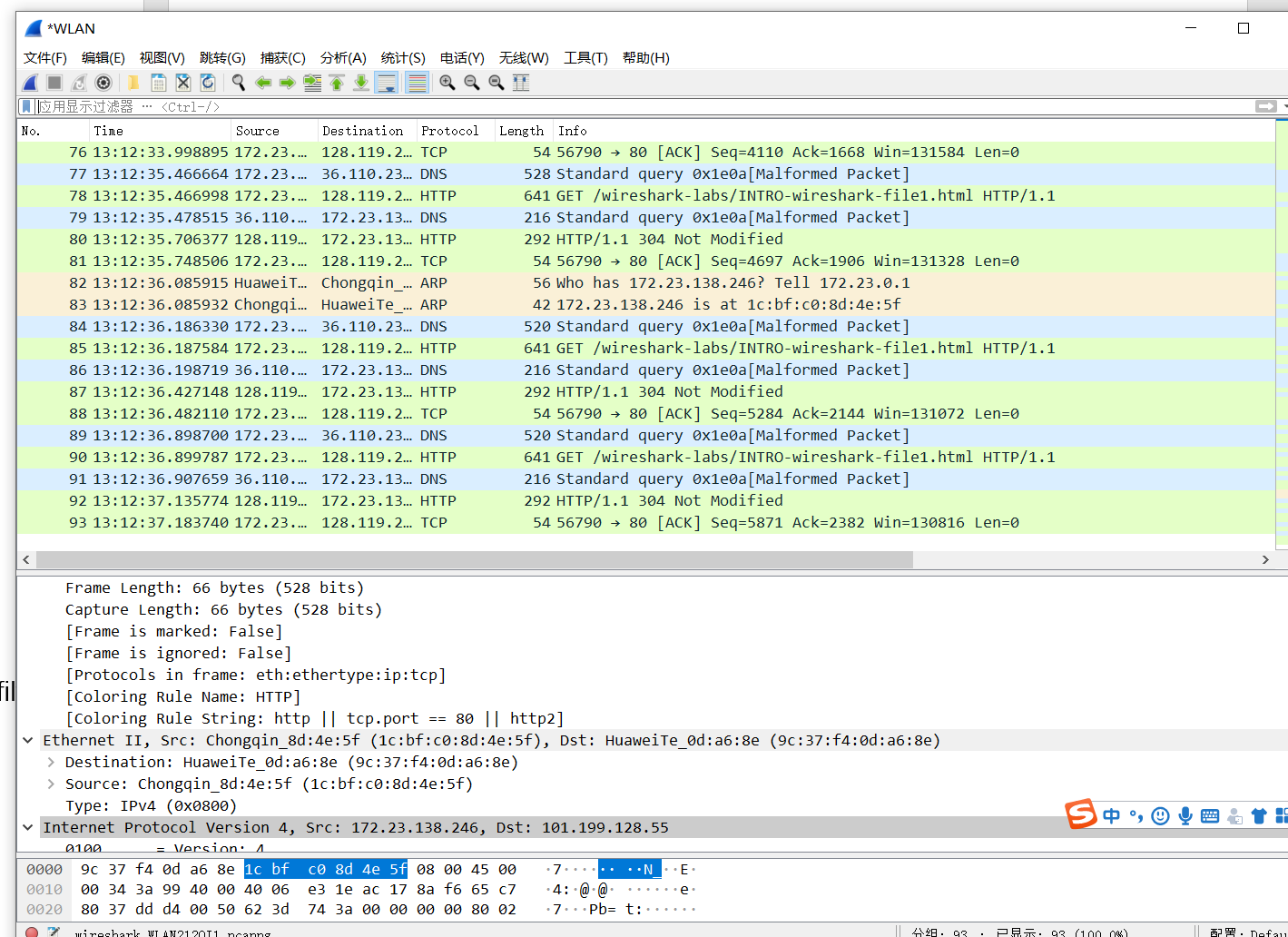
1.先安装wireshark,之前我就下载过。



2.准备好这两个界面，首先根据在浏览器中打开实验文档中的网址，为后面的捕获准备。

当前通过WLAN连接网络选择WLAN接口，然后就可以开始捕获数据包了

在开始以后多次刷新左侧浏览器界面，会出现多次的httpGET请求方便我们定位到我们需要的数据包

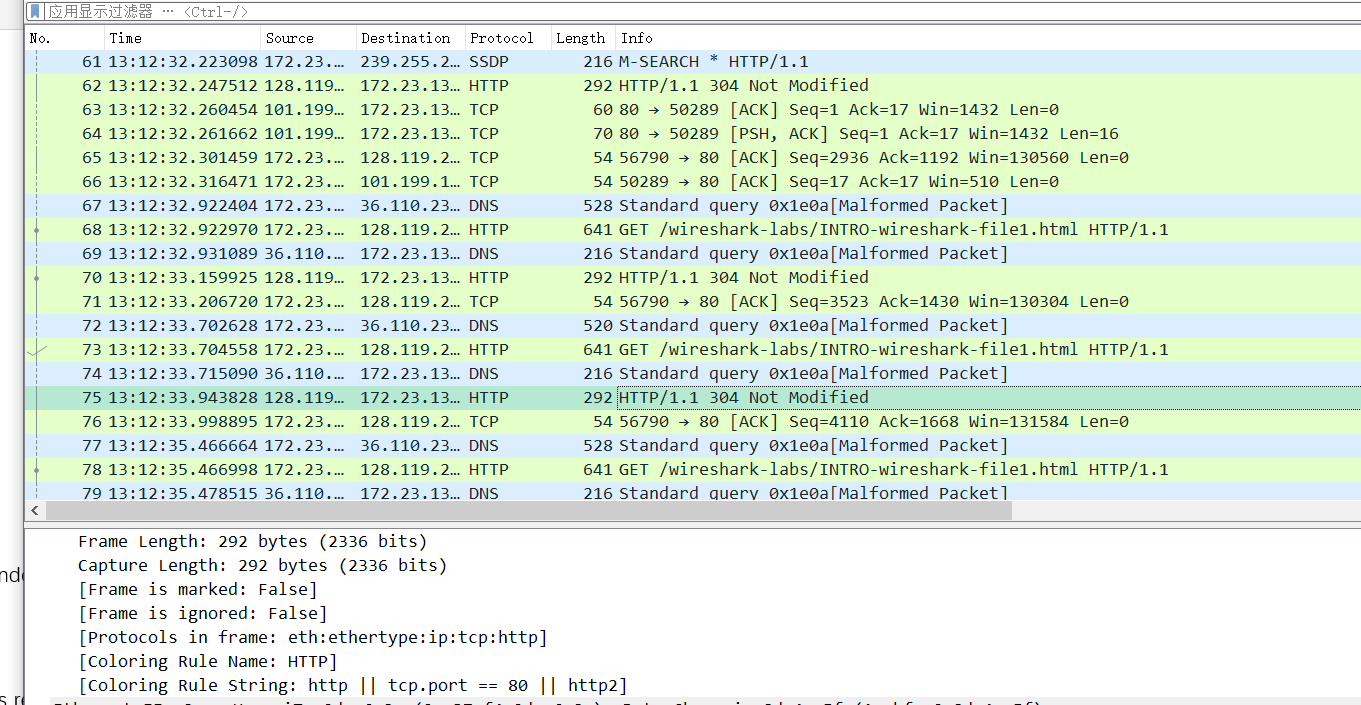


3.接下来就可以开始what to hand in 任务了

What to hand in

1.List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

列出上面步骤7中未过滤数据包列表窗口中协议列中出现的3个不同协议。

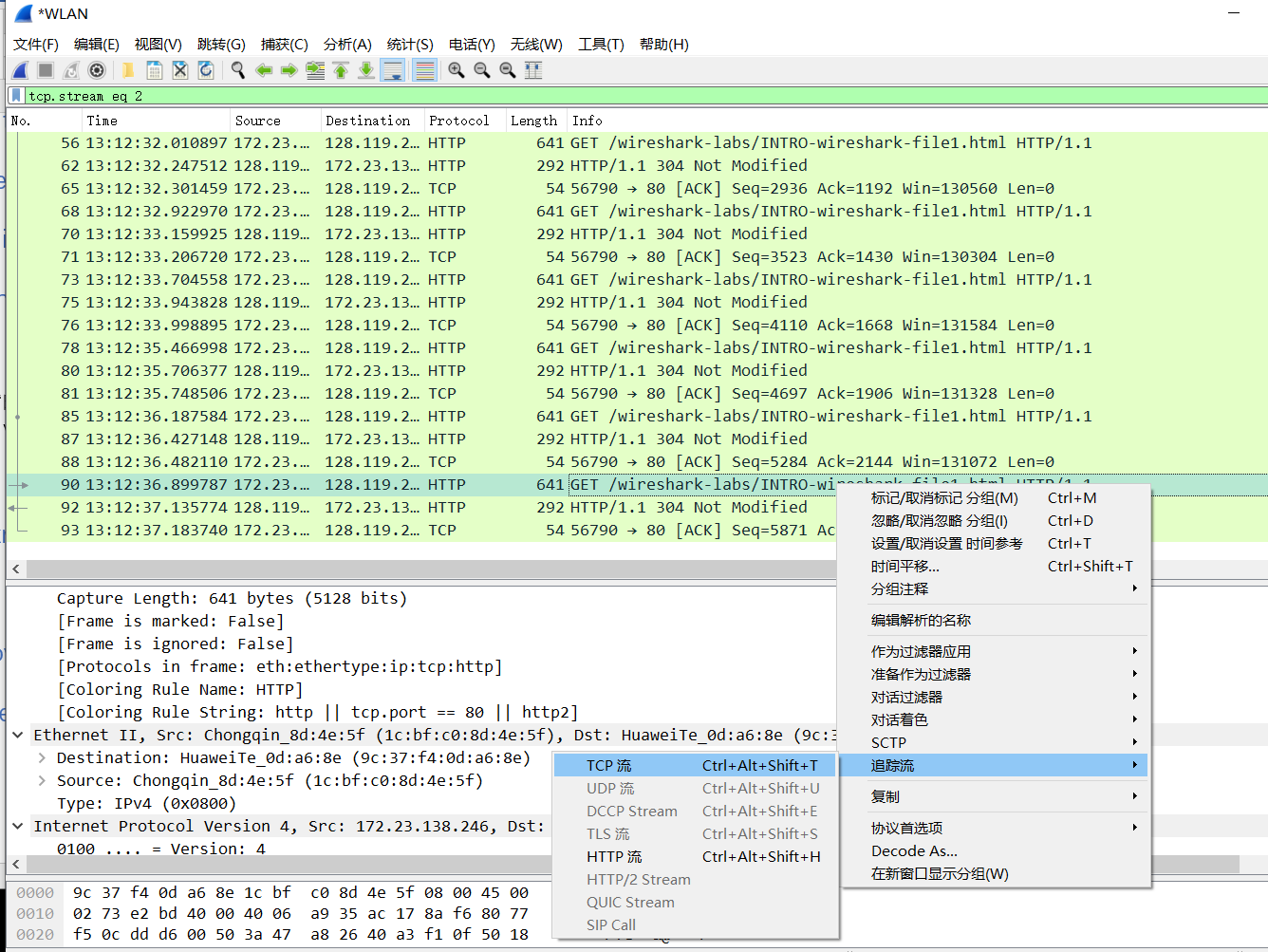


我们可以看到这张图片和上一张图片中protocol协议共有TCP，DNS，HTTP，ARP，SSDP

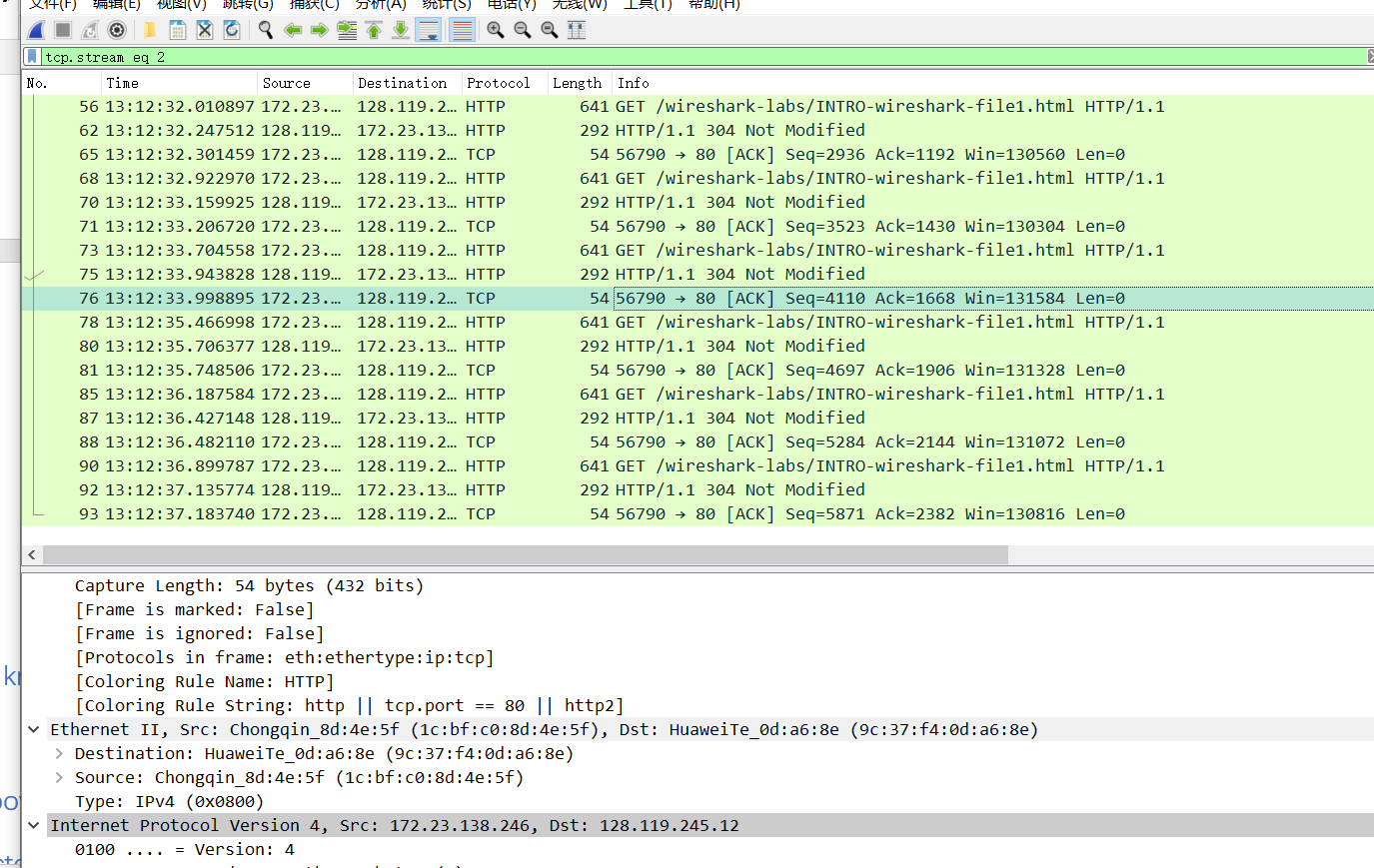
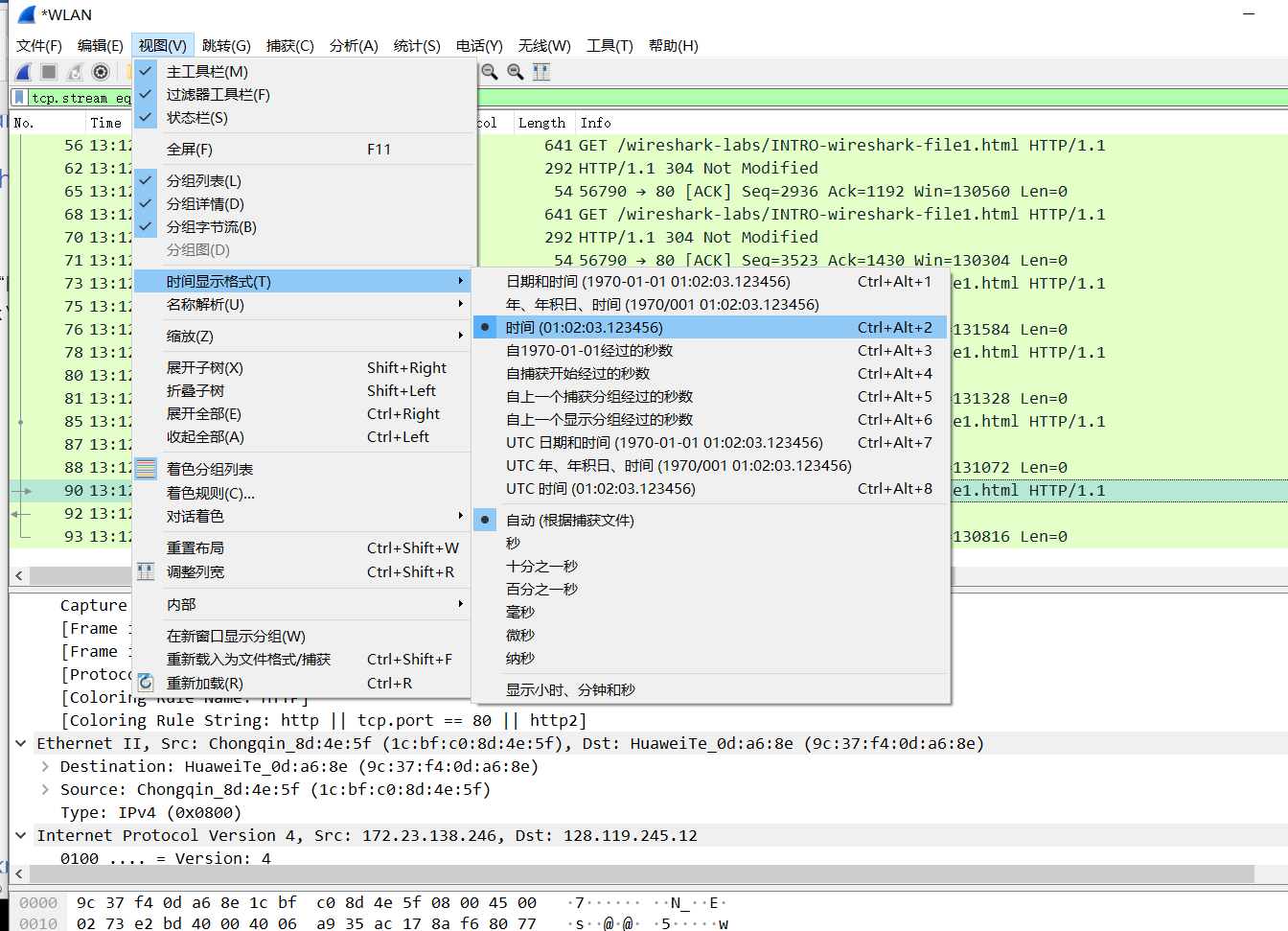
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

从发送HTTP GET消息到收到HTTP OK回复需要多长时间？（默认情况下，“数据包列表”窗口中“时间”列的值是自Wireshark跟踪开始以来的时间量（以秒为单位）。要以时间格式显示时间字段，请选择Wireshark View下拉菜单，然后选择Time display format，再选择Time of day。）

首先我们筛选出我们刚才的HTTPget请求，右键点击我们要查看的项目追从TCP流或HTTP流

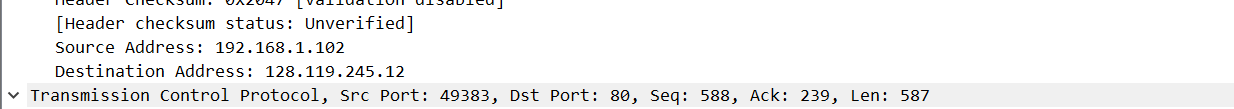


最后根据提示完成任务



3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

Gaia.cs.umass.edu的网络地址是什么？你的计算机网络地址呢？



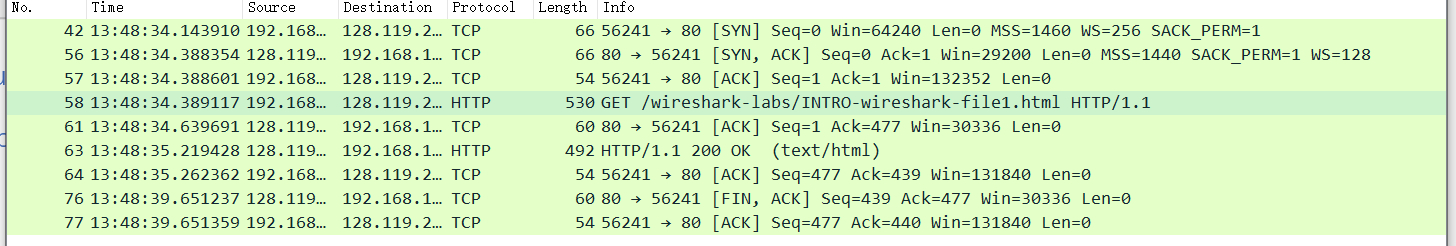
本地的网络地址是192.168.1.102这个ip是本地路由给我分配的地址，是私有地址

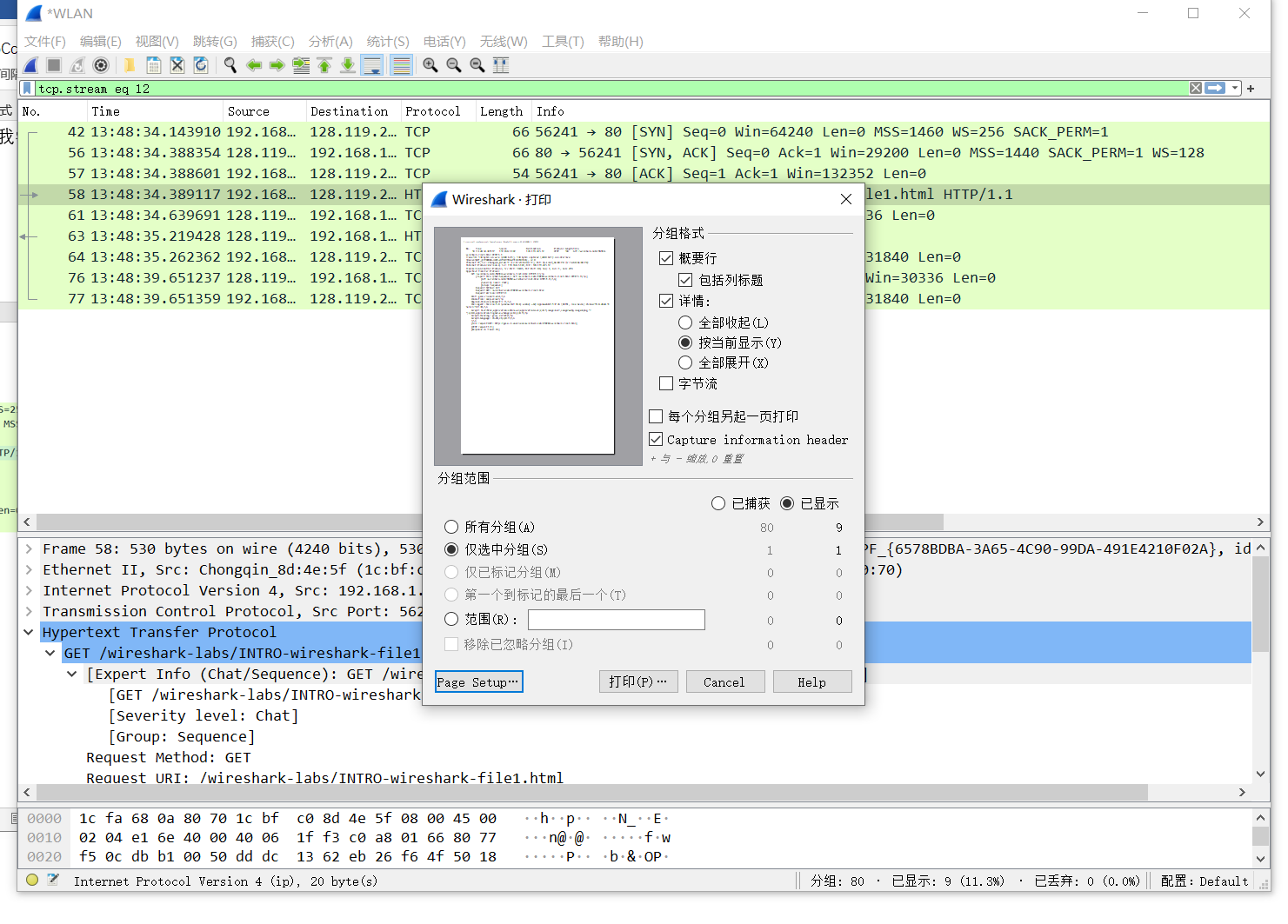
128.119.245.12 来自 美国 马萨诸塞州 阿默斯特 Five Colleges Network这个ip可以查到定位

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK

在做这个题时我发现了一个问题，如果一直刷新一个已经打开的界面http不会返回200而是304 not modified。

于是我重新输入地址再点击跳转还是不行。我考虑是不是浏览器缓存的原因，于是我尝试清理缓存，结果成功返回200OK。





按照提示打印即可

