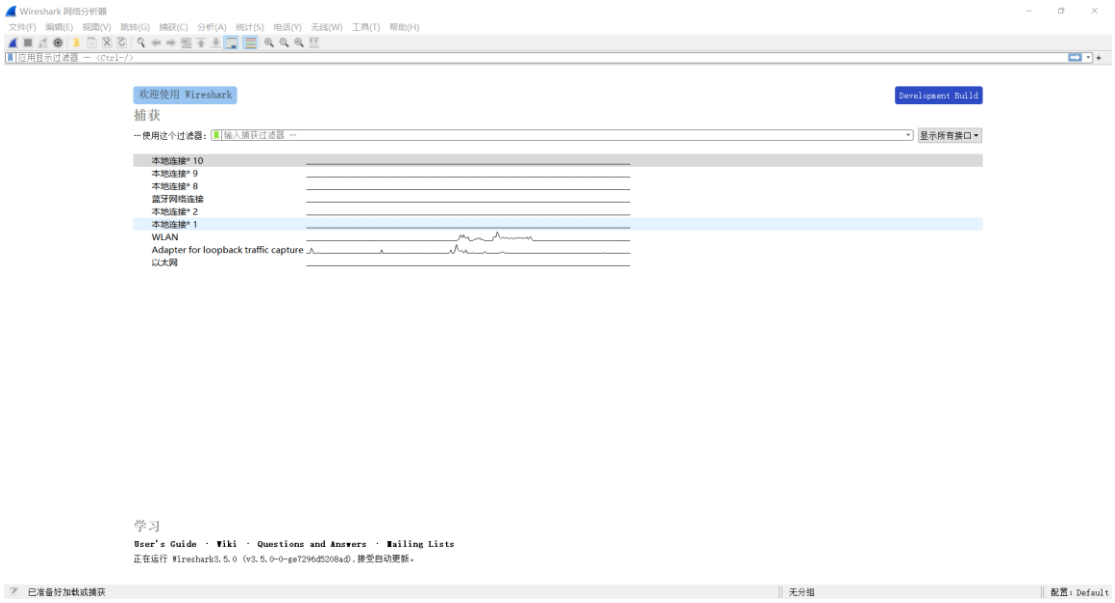
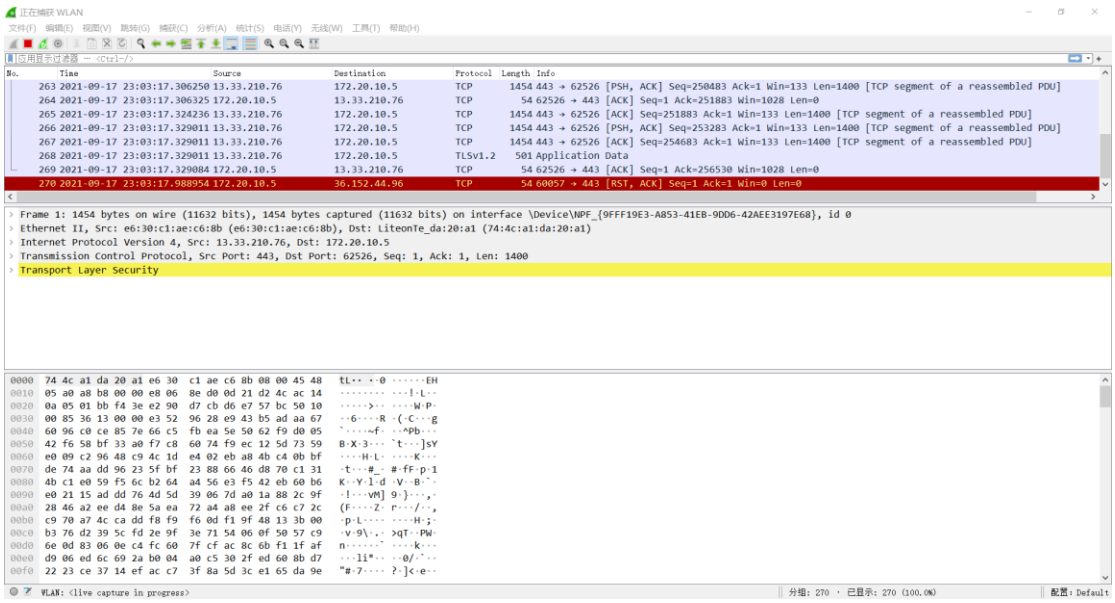
下载了 Wireshark 后下载网络数据包抓包工具 npcap，打开 Wireshark 出现如下界面

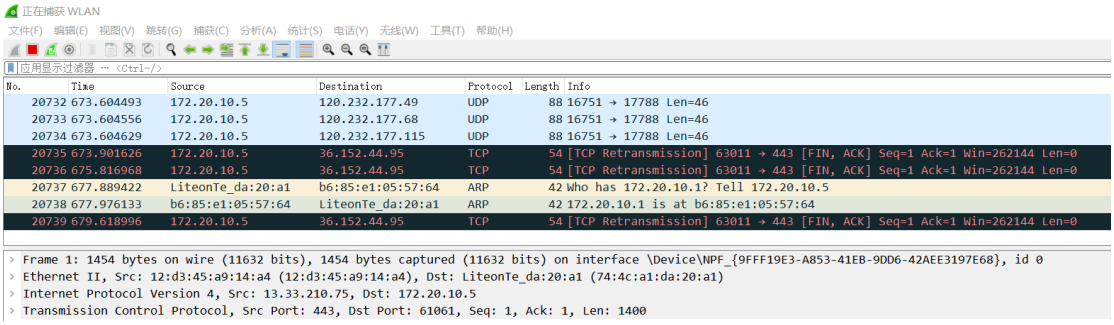


点击 WIAN,Wireshark 开始进行数据抓包，工作界面如下



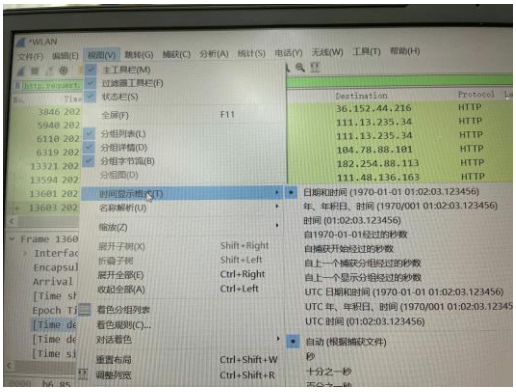
1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

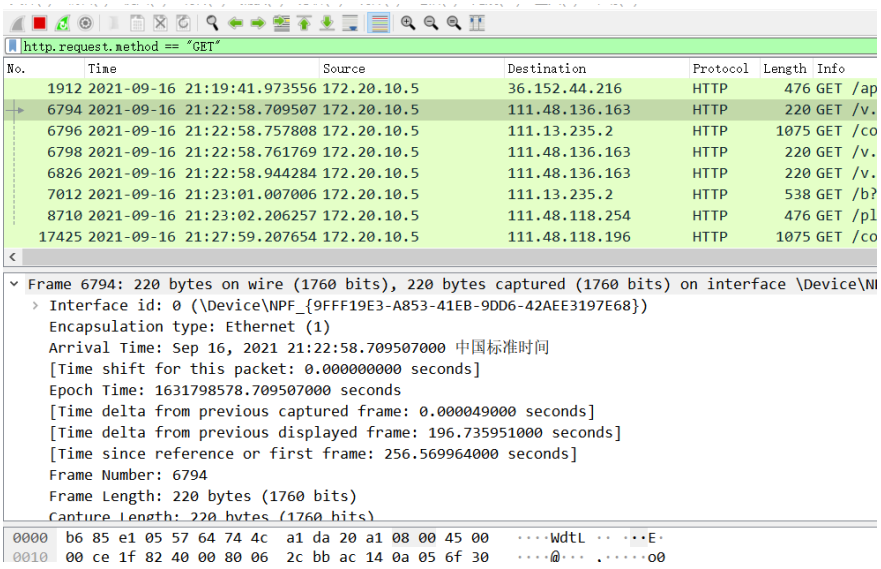
   UDP、TCP、ARP



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.)

修改时间显示格式：视图——时间显示格式——日期和时间

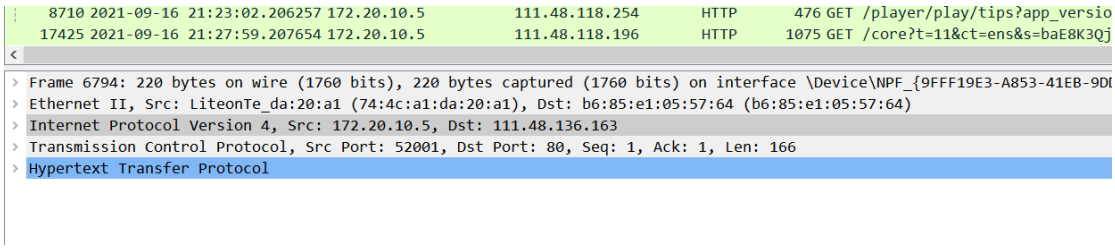




在应用显示过滤器栏中输入：http.request.method=="GET"，数据详细区中 Frame 6794 下面则会出现对应的时间，得到 Time shift:0.000000000 seconds

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?

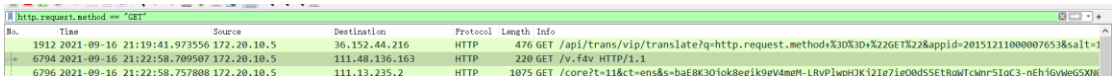
   在 wireshark 运行时，进入网站 http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html，在数据详细区的 Internet Protocol Versioin 4 中显示了 Src 和 Dst，即对应的网站地址与电脑地址。



   address of the gaia.cs.umass.edu(Src): 172.20.10.5
   Internet address of my computer(Dst): 111.48.136.163

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.

在问题 2 中，点击数据详细区的 Hypertext Transfer Protocol 中的最底部的 Response in frame，得到如下图的两个数据。



其详细信息分别为：

1912 2021-09-16 21:19:41.973556 172.20.10.5 36.152.44.216 HTTP 476 GET /api/trans/vip/translate?q=http.request.method+%3D%3D+%22GET%22&appid=20151211000007653&salt=1631798381858&from=auto&to=zh&sign=7fe0b5bf3c9a28112fc7cbf91a8615c7 HTTP/1.1

6794 2021-09-16 21:22:58.709507 172.20.10.5 111.48.136.163 HTTP 220 GET /v.f4v HTTP/1.1