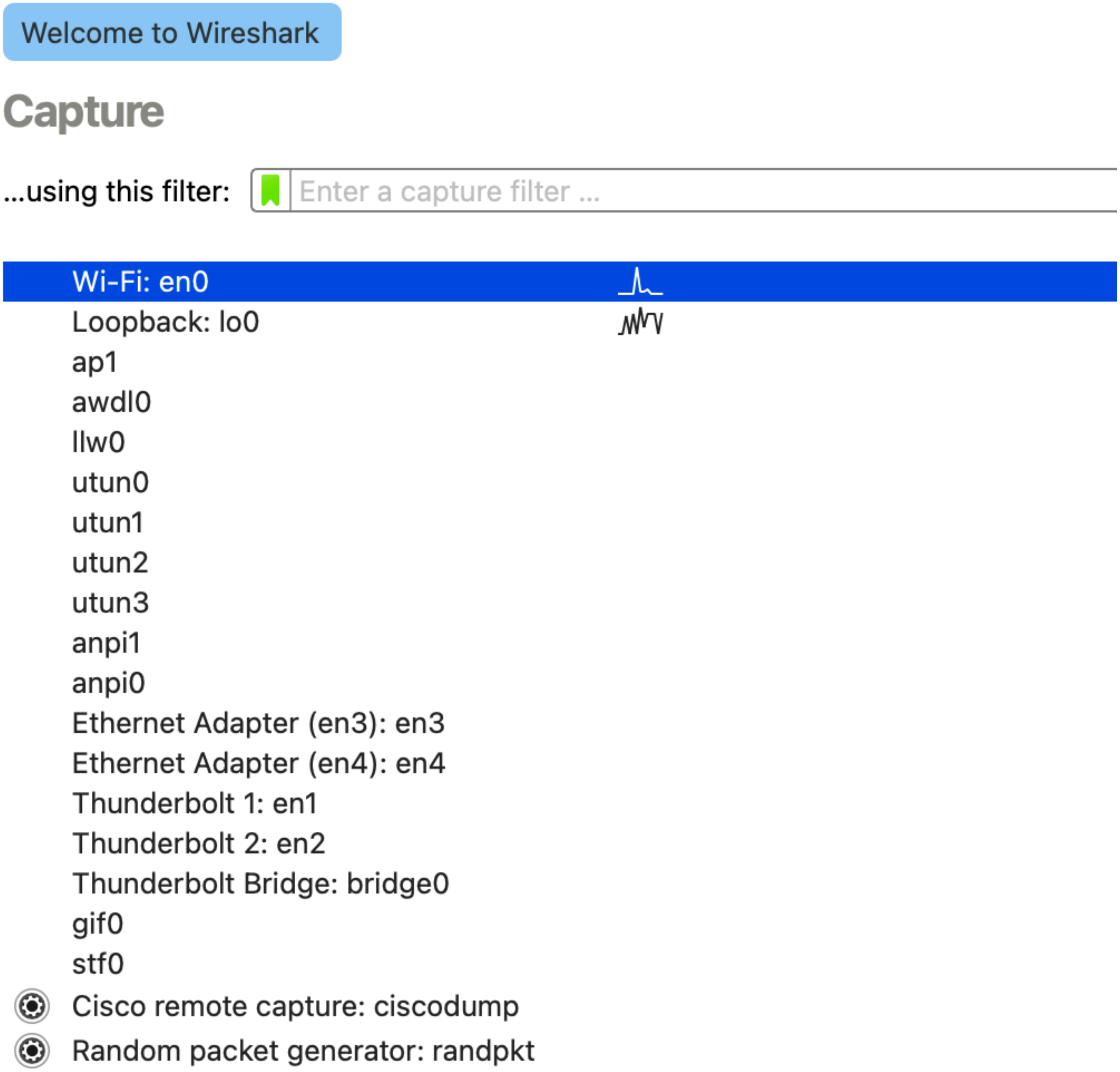
第一次实验

打开 Wireshark 后，在 MacOS 操作系统下，会直接显示 Interfaces 面板，双击 Wi-Fi:en0 选项，开启抓包页面。



Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

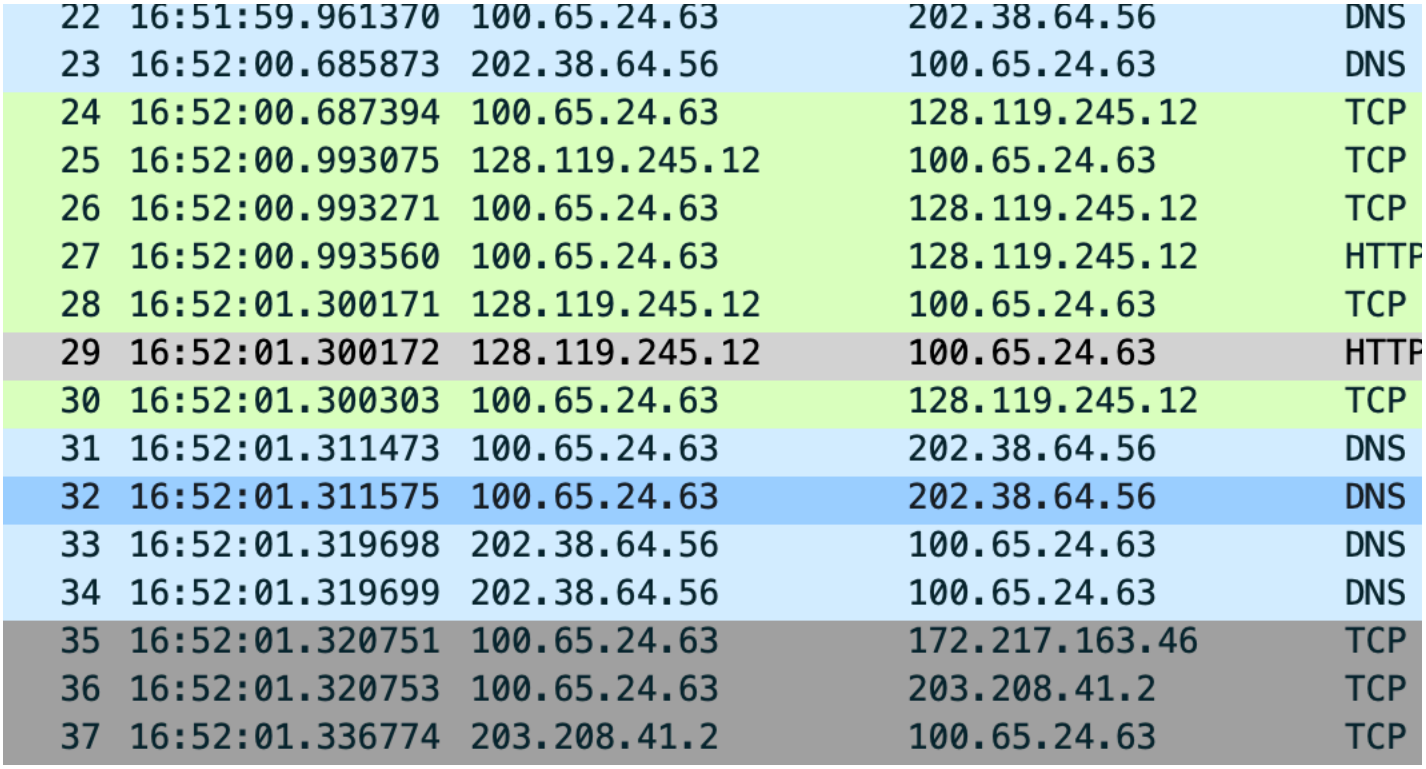
Wi-Fi: en0
Loopback: lo0
ap1
awdl0
llw0
utun0
utun1
utun2
utun3
anpi1
anpi0
Ethernet Adapter (en3): en3
Ethernet Adapter (en4): en4
Thunderbolt 1: en1
Thunderbolt 2: en2
Thunderbolt Bridge: bridge0
gif0
stf0
Cisco remote capture: ciscodump
Random packet generator: randpkt

用浏览器访问实验文档中给的示例网址 http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html 后，停止抓包。在 filter 搜索框中输入 http 得到包含对该网址的 GET 请求 及 OK 响应。找到后点击进入观察 packet list.

问题

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

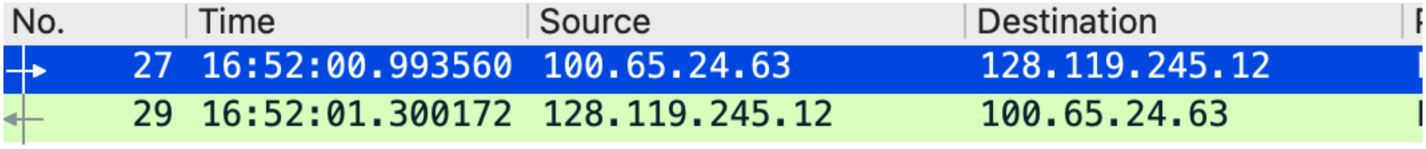
   如下图: TCP, HTTP, DNS



22	16:51:59.961370	100.65.24.63	202.38.64.56	DNS
23	16:52:00.685873	202.38.64.56	100.65.24.63	DNS
24	16:52:00.687394	100.65.24.63	128.119.245.12	TCP
25	16:52:00.993075	128.119.245.12	100.65.24.63	TCP
26	16:52:00.993271	100.65.24.63	128.119.245.12	TCP
27	16:52:00.993560	100.65.24.63	128.119.245.12	HTTP
28	16:52:01.300171	128.119.245.12	100.65.24.63	TCP
29	16:52:01.300172	128.119.245.12	100.65.24.63	HTTP
30	16:52:01.300303	100.65.24.63	128.119.245.12	TCP
31	16:52:01.311473	100.65.24.63	202.38.64.56	DNS
32	16:52:01.311575	100.65.24.63	202.38.64.56	DNS
33	16:52:01.319698	202.38.64.56	100.65.24.63	DNS
34	16:52:01.319699	202.38.64.56	100.65.24.63	DNS
35	16:52:01.320751	100.65.24.63	172.217.163.46	TCP
36	16:52:01.320753	100.65.24.63	203.208.41.2	TCP
37	16:52:01.336774	203.208.41.2	100.65.24.63	TCP

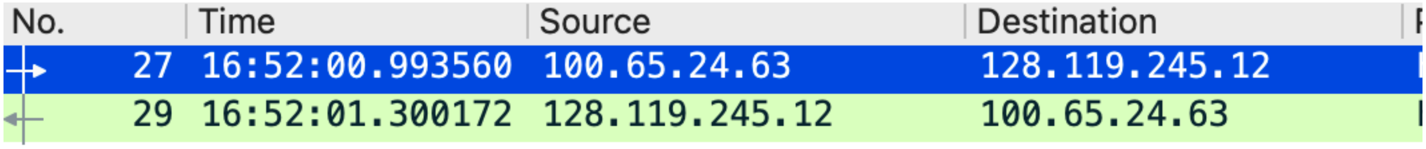
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark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

   找到 HTTP Get 和 HTTP OK 两行，选择 Time Display Format 为 Time-of-day, 比较这两行的time 的值，相减得: 1.300172 - 0.993560 = 0.306612(s)



No.	Time	Source	Destination
27	16:52:00.993560	100.65.24.63	128.119.245.12
29	16:52:01.300172	128.119.245.12	100.65.24.63

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



No.	Time	Source	Destination
27	16:52:00.993560	100.65.24.63	128.119.245.12
29	16:52:01.300172	128.119.245.12	100.65.24.63

   Internet address of gaia.cs.umass.edu: 128.119.245.12
   我的 IP: 100.65.24.63

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.

   见打印结果 PDF 文件: wireshark_HTTP_GET.pdf 和 wireshark_HTTP_OK.pdf。