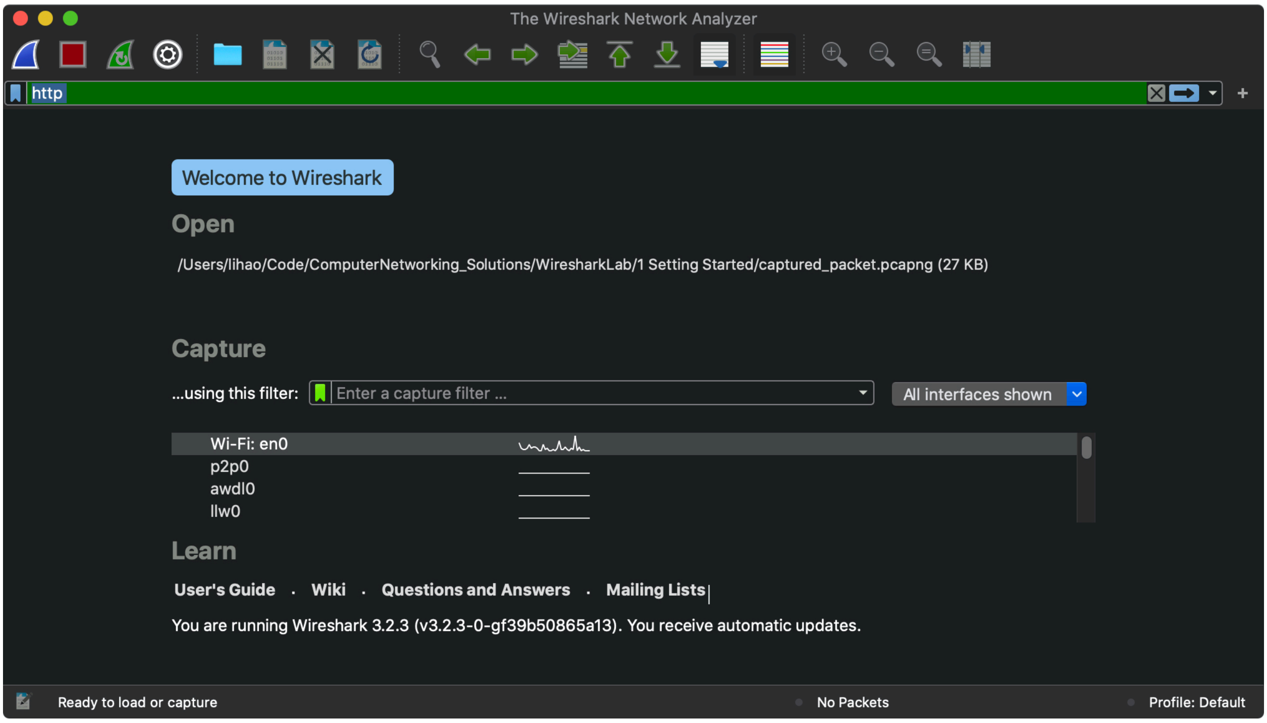
Getting Start 学习记录

首先下载 wireshark, 我是 MacOS 在官网下载安装包.

除了安装 Wireshark, 安装包内部还有一些依赖项和将 Wireshark 加入系统路径. 操作结束后即可打开运行 Wireshark

初始界面


The Wireshark Network Analyzer
http
Welcome to Wireshark
Open
Capture
Wi-Fi: en0
p2p0
awdl0
llw0
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

/Users/lihao/Code/ComputerNetworking_Solutions/WiresharkLab/1 Setting Started/captured_packet.pcapng (27 KB)

...using this filter: Enter a capture filter ... All interfaces shown

You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.

Ready to load or capture · No Packets · Profile: Default

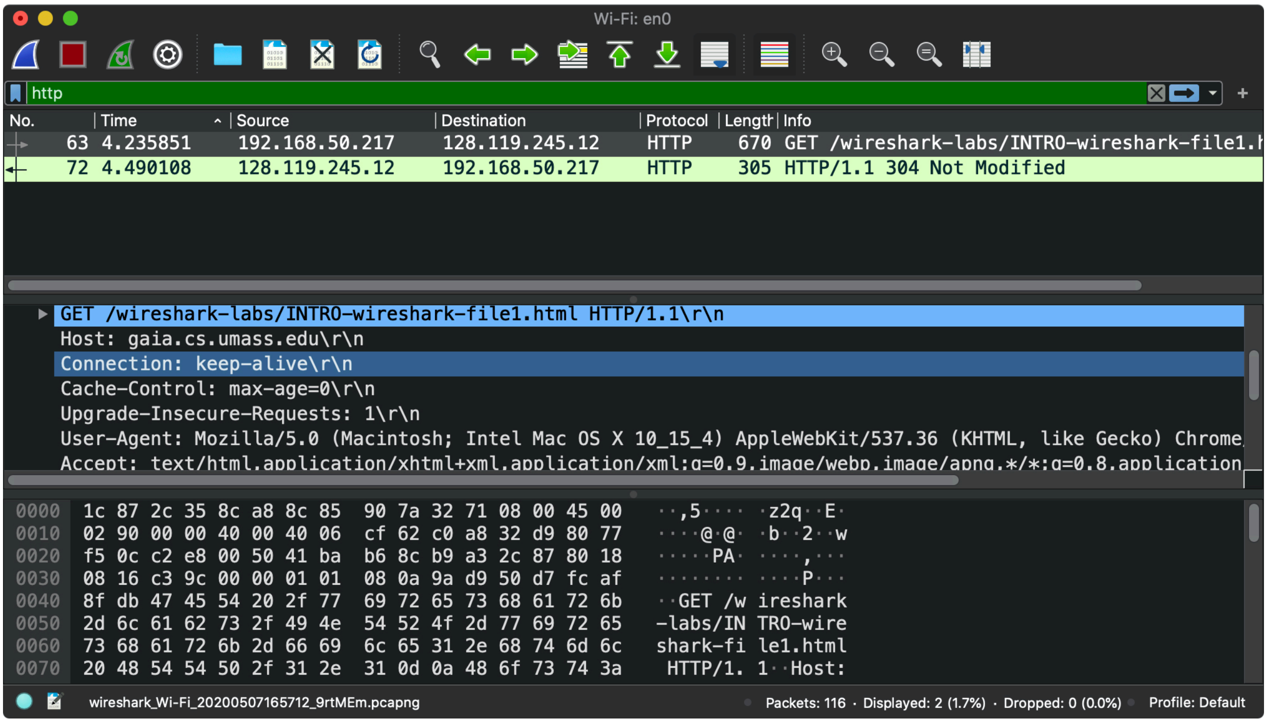
双击击`Wi-Fi: en0`开始监听, 进入监听界面

跟踪第一个 URL

在 Wireshark 开始抓包(packet capture)的时候, 在浏览器输入

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

然后通过 HTTP 标签过滤出对 HTTP协议包的计息结果, 结果如图



http

```
No.     Time        Source          Destination     Protocol Length Info
     63 4.235851    192.168.50.217  128.119.245.12  HTTP     670 GET /wireshark-labs/INTRO-wireshark-file1.h
     72 4.490108    128.119.245.12  192.168.50.217  HTTP     305 HTTP/1.1 304 Not Modified
```

```
▸ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application
```

```
0000  1c 87 2c 35 8c a8 8c 85  90 7a 32 71 08 00 45 00   ··,5···· ·z2q··E·
0010  02 90 00 00 40 00 40 06  cf 62 c0 a8 32 d9 80 77   ····@·@· ·b··2··w
0020  f5 0c c2 e8 00 50 41 ba  b6 8c b9 a3 2c 87 80 18   ·····PA· ····,···
0030  08 16 c3 9c 00 00 01 01  08 0a 9a d9 50 d7 fc af   ········ ····P···
0040  8f db 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
```

wireshark_Wi-Fi_20200507165712_9rtMEm.pcapng · Packets: 116 · Displayed: 2 (1.7%) · Dropped: 0 (0.0%) · Profile: Default

GET 对应的数据报如下

```
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh;q=0.8,zh-CN;q=0.7\r\n
    If-None-Match: "51-5a50893dfa37e"\r\n
    If-Modified-Since: Thu, 07 May 2020 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 72]

```

服务器返回的数据报如下

```
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Thu, 07 May 2020 08:57:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-5a50893dfa37e"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.254257000 seconds]
    [Request in frame: 63]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

```

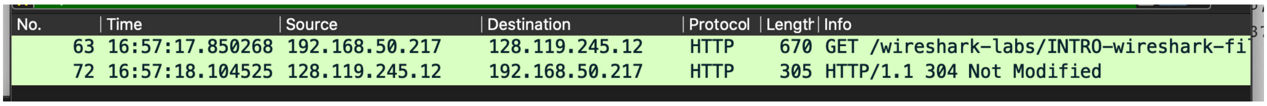
我将结果保存在了`captured_packet.pcapng`这里, 可以从 Wireshark 里面打开这个文佳回复当时的抓包.

其他作业题

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

MDNS, TCP, SSDP, ARP, STP, ICMP

> 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.)



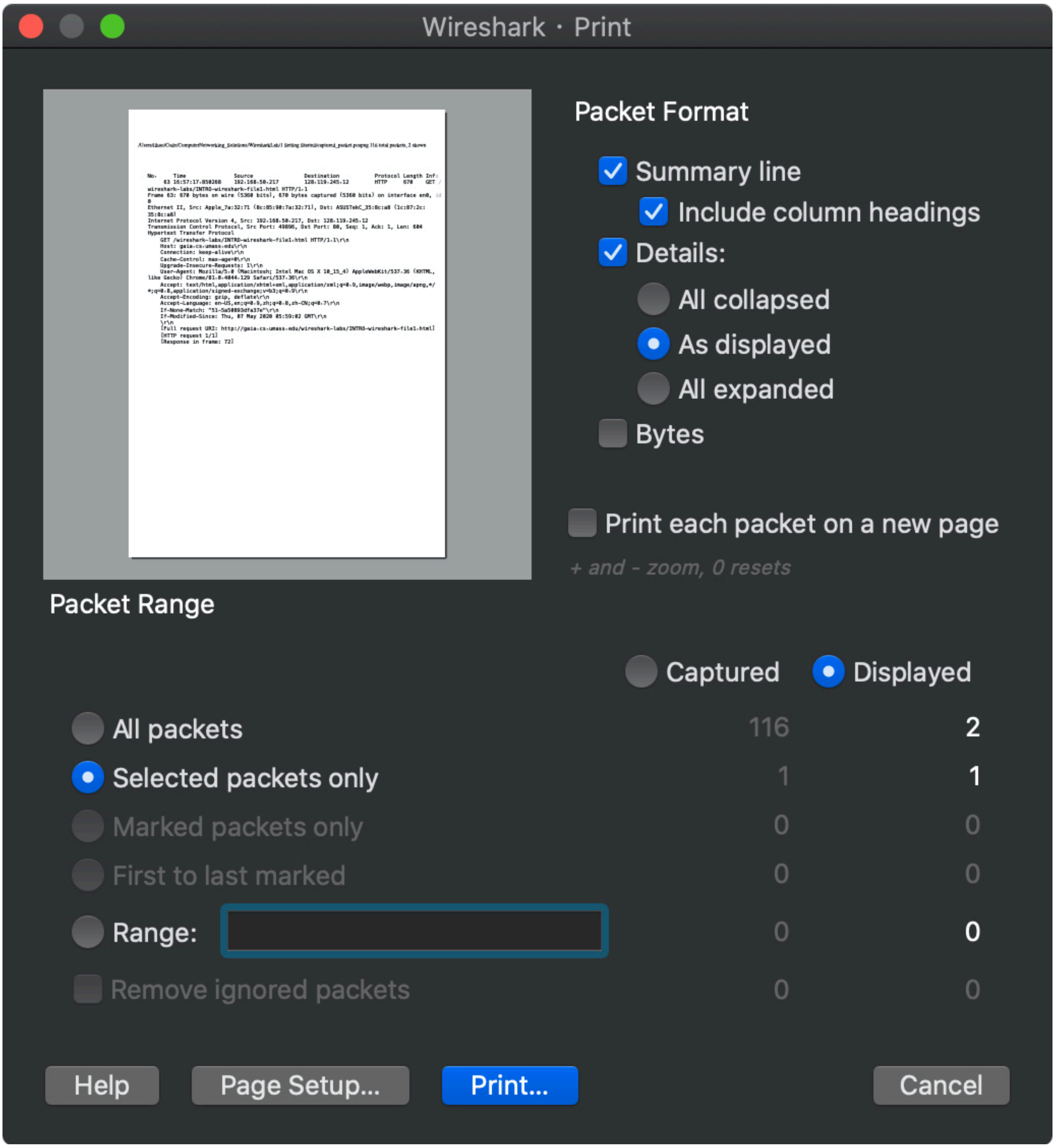
No.	Time	Source	Destination	Protocol	Length	Info
63	16:57:17.850268	192.168.50.217	128.119.245.12	HTTP	670	GET /wireshark-labs/INTRO-wireshark-fi
72	16:57:18.104525	128.119.245.12	192.168.50.217	HTTP	305	HTTP/1.1 304 Not Modified

> 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?

192.169.50.217

128.119.245.12

> 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.



```
/Users/lihao/Code/ComputerNetworking_Solutions/WiresharkLab/1 Getting Started/captured_packet.pcapng 116 total packets, 2 shown

No.     Time               Source                Destination           Protocol Length Info
     63 16:57:17.850268    192.168.50.217        128.119.245.12        HTTP     670    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 63: 670 bytes on wire (5360 bits), 670 bytes captured (5360 bits) on interface en0, id
0
Ethernet II, Src: Apple_7a:32:71 (8c:85:90:7a:32:71), Dst: ASUSTekC_35:8c:a8 (1c:87:2c:
35:8c:a8)
Internet Protocol Version 4, Src: 192.168.50.217, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49896, Dst Port: 80, Seq: 1, Ack: 1, Len: 604
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/81.0.4044.129 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh;q=0.8,zh-CN;q=0.7\r\n
    If-None-Match: "51-5a50893dfa37e"\r\n
    If-Modified-Since: Thu, 07 May 2020 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 72]
```

Packet Format

- ☑ Summary line
  - ☑ Include column headings
- ☑ Details:
  - ○ All collapsed
  - ● As displayed
  - ○ All expanded
- □ Bytes

□ Print each packet on a new page

+ and - zoom, 0 resets

Packet Range

	○ Captured	● Displayed
○ All packets	116	2
● Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove ignored packets	0	0