计算机网络入门实验实验报告

姓名：陈鹤影　　　　学号：PB21061287　　　　日期：2022.9.11

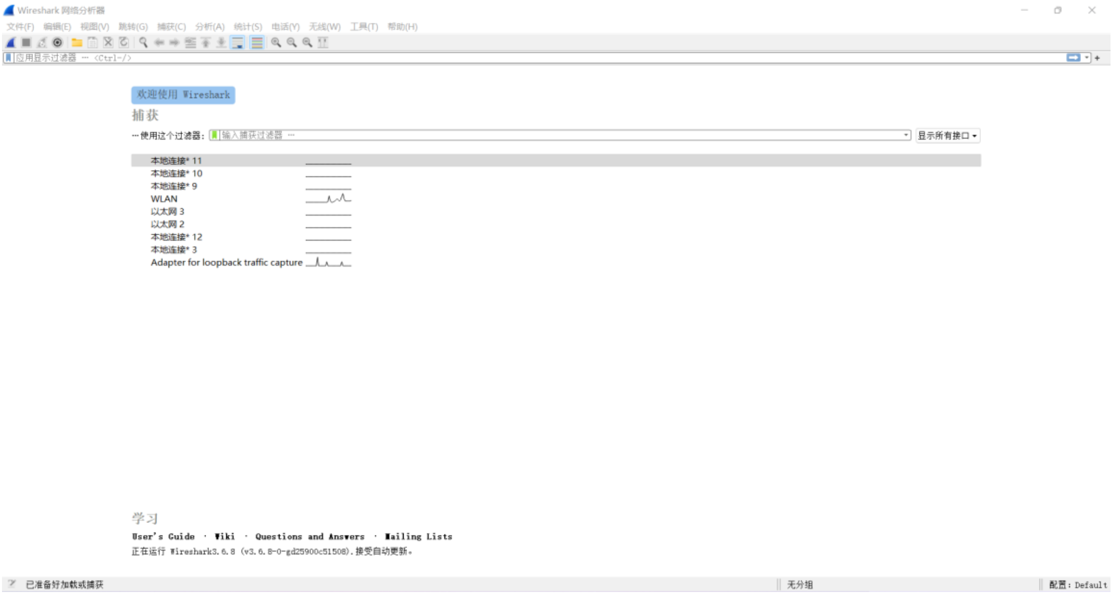
一、实验流程：

Step 1：Getting Wireshark

登入网页 http://www.wireshark.org/，根据计算机系统选择并下载 Windows-64 安装包。

Step 2：Running Wireshark

进入 Wireshark 界面，如下：


Wireshark 网络分析器
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
欢迎使用 Wireshark
捕获
显示所有接口
学习
User's Guide · Wiki · Questions and Answers · Mailing Lists

…使用这个过滤器：输入捕获过滤器 …

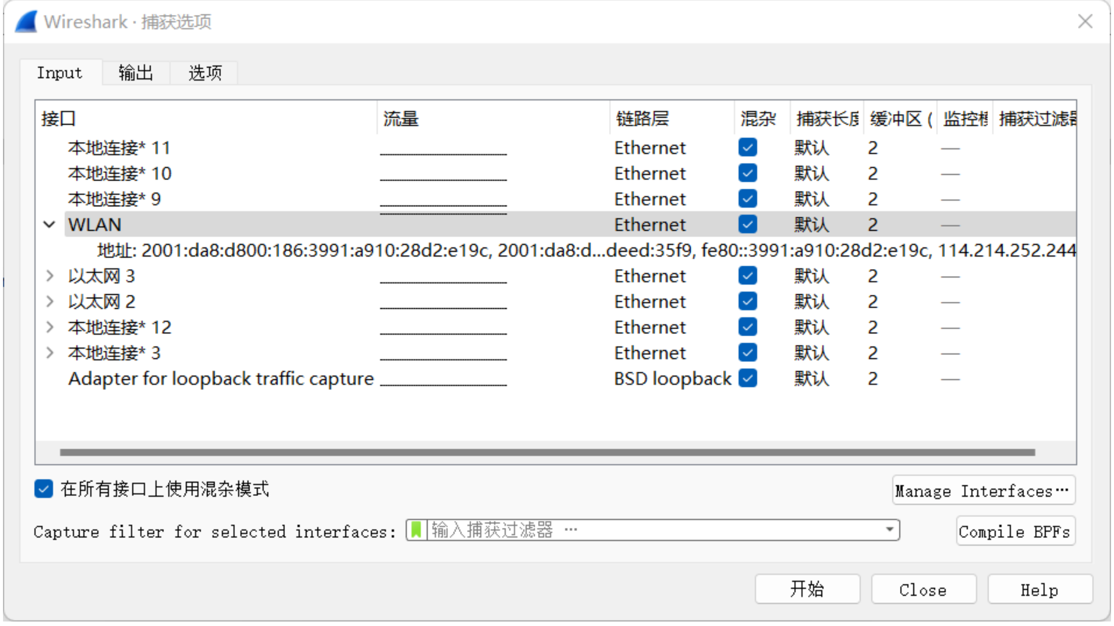
本地连接* 11
本地连接* 10
本地连接* 9
WLAN
以太网 3
以太网 2
本地连接* 12
本地连接* 3
Adapter for loopback traffic capture

正在运行 Wireshark3.6.8 (v3.6.8-0-gd25900c51508). 接受自动更新。

已准备好加载或捕获　　无分组　　配置：Default

（图 1-1 Wireshark 登入界面）

打开任意浏览器（实验中选择华为浏览器[Microsoft Edge 会显示 404 not found]）。点击 Capture 下拉菜单选择接口（实验中选择 WLAN）并开启 Wireshark。



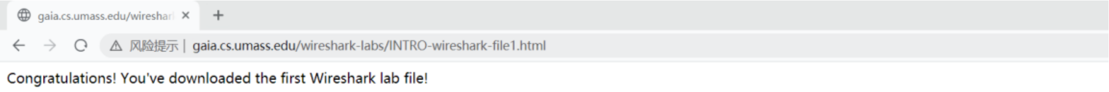
接口	流量	链路层	混杂	捕获长度	缓冲区（	监控模	捕获过滤器
本地连接* 11		Ethernet	☑	默认	2	—	
本地连接* 10		Ethernet	☑	默认	2	—	
本地连接* 9		Ethernet	☑	默认	2	—	
WLAN		Ethernet	☑	默认	2	—	
地址: 2001:da8:d800:186:3991:a910:28d2:e19c, 2001:da8:d...deed:35f9, fe80::3991:a910:28d2:e19c, 114.214.252.244							
以太网 3		Ethernet	☑	默认	2	—	
以太网 2		Ethernet	☑	默认	2	—	
本地连接* 12		Ethernet	☑	默认	2	—	
本地连接* 3		Ethernet	☑	默认	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	默认	2	—	

☑ 在所有接口上使用混杂模式

Capture filter for selected interfaces: 输入捕获过滤器 …

（图 1-2 Wireshark 接口选择界面）

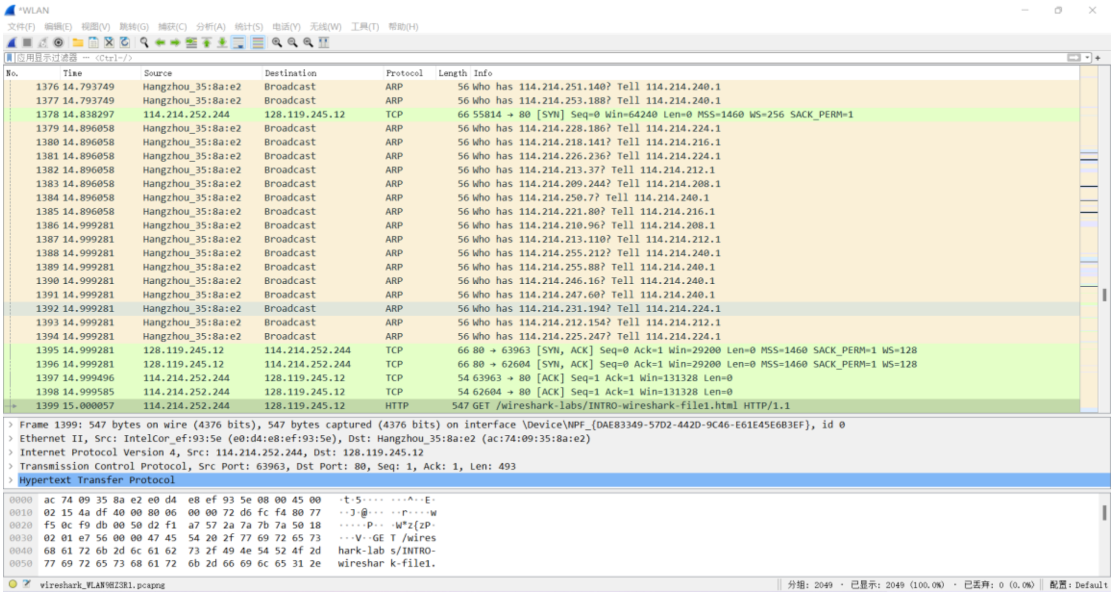
在运行 Wireshark 的情况下，打开 URL：http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html 。显示界面如下：


gaia.cs.umass.edu/wireshar
风险提示 | gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Congratulations! You've downloaded the first Wireshark lab file!

（图 1-3 URL 显示界面）

当浏览器成功显示上述信息后停止 Wireshark 抓包。Wireshark 显示界面如下：


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.       Time         Source              Destination         Protocol  Length Info
     1376 14.793749    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.251.140? Tell 114.214.240.1
     1377 14.793749    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.253.188? Tell 114.214.240.1
     1378 14.838297    114.214.252.244     128.119.245.12      TCP          66 55814 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
     1379 14.896058    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.228.186? Tell 114.214.224.1
     1380 14.896058    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.218.141? Tell 114.214.216.1
     1381 14.896058    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.226.236? Tell 114.214.224.1
     1382 14.896058    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.213.37? Tell 114.214.212.1
     1383 14.896058    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.209.244? Tell 114.214.208.1
     1384 14.896058    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.250.7? Tell 114.214.240.1
     1385 14.896058    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.221.80? Tell 114.214.216.1
     1386 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.210.96? Tell 114.214.208.1
     1387 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.213.110? Tell 114.214.212.1
     1388 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.255.212? Tell 114.214.240.1
     1389 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.255.88? Tell 114.214.240.1
     1390 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.246.16? Tell 114.214.240.1
     1391 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.247.60? Tell 114.214.240.1
     1392 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.231.194? Tell 114.214.224.1
     1393 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.212.154? Tell 114.214.212.1
     1394 14.999281    Hangzhou_35:8a:e2   Broadcast           ARP          56 Who has 114.214.225.247? Tell 114.214.224.1
     1395 14.999281    128.119.245.12      114.214.252.244     TCP          66 80 → 63963 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
     1396 14.999281    128.119.245.12      114.214.252.244     TCP          66 80 → 62604 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
     1397 14.999496    114.214.252.244     128.119.245.12      TCP          54 63963 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
     1398 14.999585    114.214.252.244     128.119.245.12      TCP          54 62604 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
     1399 15.000057    114.214.252.244     128.119.245.12      HTTP        547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

> Frame 1399: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
> Internet Protocol Version 4, Src: 114.214.252.244, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63963, Dst Port: 80, Seq: 1, Ack: 1, Len: 493
> Hypertext Transfer Protocol

0000  ac 74 09 35 8a e2 e0 d4  e8 ef 93 5e 08 00 45 00   ·t·5···· ···^··E·
0010  02 15 4a df 40 00 80 06  00 00 72 d6 fc f4 80 77   ··J·@··· ··r····w
0020  f5 0c f9 db 00 50 d2 f1  a7 57 2a 7a 7b 7a 50 18   ·····P·· ·W*z{zP·
0030  02 01 e7 56 00 00 47 45  54 20 2f 77 69 72 65 73   ···V··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.

wireshark_WLAN9HZ3R1.pcapng        分组: 2049 · 已显示: 2049 (100.0%) · 已丢弃: 0 (0.0%)   配置: Default
```

（图 1-4 Wireshark 抓包显示界面）

观察 IP 包结构，发现其包含：版本、头部长度、总长度、TTL、协议类型等字段。Packet Details Pane(数据包详细信息)，在数据包列表中选择指定数据包，在数据包详细信息中会显示数据包的所有详细信息内容。各行信息分别为：

（1）Frame：物理层的数据帧概况

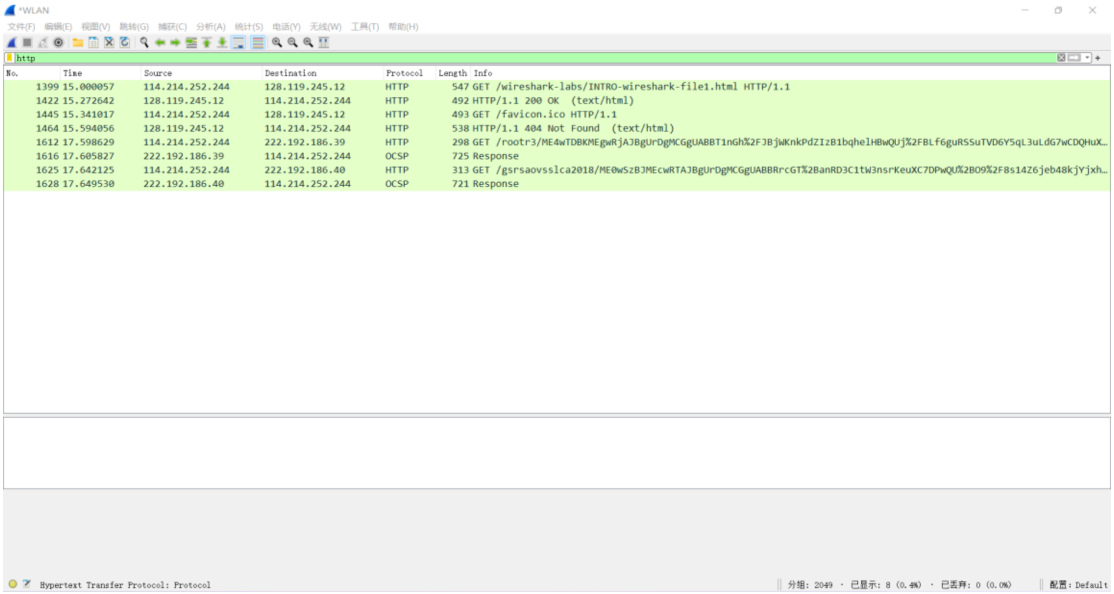
（2）Ethernet II：数据链路层以太网帧头部信息

（3）Internet Protocol Version 4：互联网层 IP 包头部信息

（4）Transmission Control Protocol：传输层 T 的数据段头部信息，此处是 TCP

（5）Hypertext Transfer Protocol：应用层的信息，此处是 HTTP 协议

在分组过滤器中选择 http（小写）协议，显示如下：

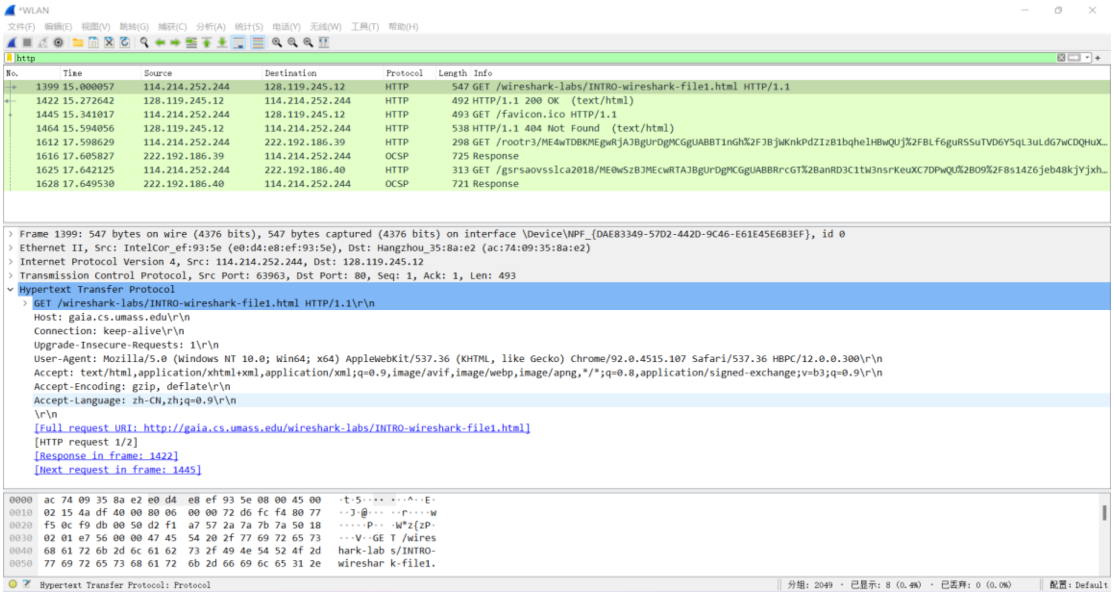

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http
No.     Time      Source           Destination      Protocol  Length Info
   1399 15.000057 114.214.252.244  128.119.245.12   HTTP      547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   1422 15.272642 128.119.245.12   114.214.252.244  HTTP      492 HTTP/1.1 200 OK  (text/html)
   1445 15.341017 114.214.252.244  128.119.245.12   HTTP      493 GET /favicon.ico HTTP/1.1
   1464 15.594056 128.119.245.12   114.214.252.244  HTTP      538 HTTP/1.1 404 Not Found  (text/html)
   1612 17.598629 114.214.252.244  222.192.186.39   HTTP      298 GET /rootr3/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBT1nGh%2FJBjWKnkPdZIzB1bqhelHBwQUj%2FBLf6guRSSuTVD6Y5qL3uLdG7wCDQHuX…
   1616 17.605827 222.192.186.39   114.214.252.244  OCSP      725 Response
   1625 17.642125 114.214.252.244  222.192.186.40   HTTP      313 GET /gsrsaovsslca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBRrcGT%2BanRD3C1tW3nsrKeuXC7DPwQU%2BO9%2F8s14Z6jeb48kjYjxh…
   1628 17.649530 222.192.186.40   114.214.252.244  OCSP      721 Response
```

```
Hypertext Transfer Protocol: Protocol          分组: 2049 · 已显示: 8 (0.4%) · 已丢弃: 0 (0.0%)    配置: Default
```

（图 1-5 Wireshark 抓包 http 协议显示界面）

找到 GET 包内容如下：


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http
No.     Time      Source           Destination      Protocol  Length Info
   1399 15.000057 114.214.252.244  128.119.245.12   HTTP      547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   1422 15.272642 128.119.245.12   114.214.252.244  HTTP      492 HTTP/1.1 200 OK  (text/html)
   1445 15.341017 114.214.252.244  128.119.245.12   HTTP      493 GET /favicon.ico HTTP/1.1
   1464 15.594056 128.119.245.12   114.214.252.244  HTTP      538 HTTP/1.1 404 Not Found  (text/html)
   1612 17.598629 114.214.252.244  222.192.186.39   HTTP      298 GET /rootr3/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBT1nGh%2FJBjWKnkPdZIzB1bqhelHBwQUj%2FBLf6guRSSuTVD6Y5qL3uLdG7wCDQHuX…
   1616 17.605827 222.192.186.39   114.214.252.244  OCSP      725 Response
   1625 17.642125 114.214.252.244  222.192.186.40   HTTP      313 GET /gsrsaovsslca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBRrcGT%2BanRD3C1tW3nsrKeuXC7DPwQU%2BO9%2F8s14Z6jeb48kjYjxh…
   1628 17.649530 222.192.186.40   114.214.252.244  OCSP      721 Response
```

```
> Frame 1399: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
> Internet Protocol Version 4, Src: 114.214.252.244, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63963, Dst Port: 80, Seq: 1, Ack: 1, Len: 493
v 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: zh-CN,zh;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 1422]
    [Next request in frame: 1445]
```

```
0000  ac 74 09 35 8a e2 e0 d4  e8 ef 93 5e 08 00 45 00   ·t·5···· ···^··E·
0010  02 15 4a df 40 00 80 06  00 00 72 d6 fc f4 80 77   ··J·@··· ··r····w
0020  f5 0c f9 db 00 50 d2 f1  a7 57 2a 7a 7b 7a 50 18   ·····P·· ·W*z{zP·
0030  02 01 e7 56 00 00 47 45  54 20 2f 77 69 72 65 73   ···V··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
```

```
Hypertext Transfer Protocol: Protocol          分组: 2049 · 已显示: 8 (0.4%) · 已丢弃: 0 (0.0%)    配置: Default
```

（图 1-6 GET 包内容显示）

退出 Wireshark。

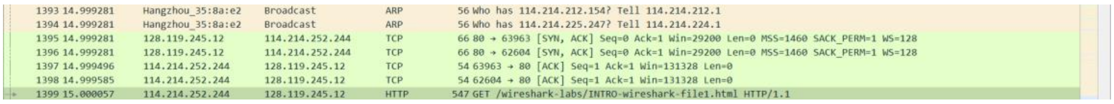
二、实验结果：

成功打开 gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html 网页，并获得 **Congratulations! You've downloaded the first Wireshark lab file!**的内容显示。Wireshark 成功捕相应的 GET 和 OK 报文。

三、Hand in：

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

   Ans：TCP、ARP、HTTP。



```
1393 14.999281   Hangzhou_35:8a:e2   Broadcast          ARP    56 Who has 114.214.212.154? Tell 114.214.212.1
1394 14.999281   Hangzhou_35:8a:e2   Broadcast          ARP    56 Who has 114.214.225.247? Tell 114.214.224.1
1395 14.999281   128.119.245.12      114.214.252.244    TCP    66 80 → 63963 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1396 14.999281   128.119.245.12      114.214.252.244    TCP    66 80 → 62604 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1397 14.999496   114.214.252.244     128.119.245.12     TCP    54 63963 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1398 14.999585   114.214.252.244     128.119.245.12     TCP    54 62604 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1399 15.000057   114.214.252.244     128.119.245.12     HTTP   547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
```

（图 2-1 Wireshark 抓包显示的几种不同协议）

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-isting 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.)**

   Ans：根据总时间显示：发送 GET 报文时间为自抓包启动后 15.000057s，接受到 OK 报文时间为自抓包启动后 15.272642s。上述过程一共用时 t = 15.272642s - 15.000057s = 0.272585s。将时间显示格式改用为时间和日期后 GET 报文和 OK 报文对应时间分别为 2022-09-11 20:56:49.404237 及 2022-09-11 20:56:49.676822。时间差为 0.272585s。

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?**

   Ans： Internet address of the gaia.cs.umass.edu：128.119.245.12。

   Internet address of your computer：114.214.252.244。

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.**

   Ans：报文导出内容如下：（附.pcapng 和.prn 文件）

```
No.     Time                           Source              Destination         Protocol Length Info
   1399 2022-09-11 20:56:49.404237     114.214.252.244     128.119.245.12      HTTP     547    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 

Frame 1399: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.252.244, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63963, Dst Port: 80, Seq: 1, Ack: 1, Len: 493
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: zh-CN,zh;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 1422]
    [Next request in frame: 1445]

No.     Time                           Source                Destination           Protocol Length Info
   1422 2022-09-11 20:56:49.676822    128.119.245.12        114.214.252.244       HTTP     492    HTTP/1.1 200 OK  (text/html)

Frame 1422: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.252.244
Transmission Control Protocol, Src Port: 80, Dst Port: 63963, Seq: 1, Ack: 494, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 11 Sep 2022 12:56:50 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 11 Sep 2022 05:59:01 GMT\r\n
    ETag: "51-5e86079cbdf11"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.272585000 seconds]
    [Request in frame: 1399]
    [Next request in frame: 1445]
    [Next response in frame: 1464]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

四、补充实验：

作为补充，我了解了 wireshark 内容过滤规则，将其中部分记录如下：

wireshark 过滤器表达式的规则

1、抓包过滤器语法

（1）协议过滤：直接在抓包过滤框中输入相应的协议名，如：tcp、http（应注意使用小写）。

（2）IP 过滤：使用 host+IP 地址的格式，若需要查询特定发送源或接收端对应分组，可在 host 前加上 src、dst 进行查询。

（3）端口过滤：使用 port+端口号的格式，若需要查询特定发送端口或接收端口对应分组，可在 port 前加上 src、dst 进行查询。

（4）过滤器语法支持逻辑运算符：与（&&）、或（||）、非（!）

2、显示过滤器语法和实例

（1）支持比较操作符：等于（==）、不等于（! =）、大于（>）、小于（<）、大于等于（>=）、小于等于（<=）。

（2）协议过滤：直接在 Filter 框中输入协议名。

（3）IP 过滤：使用 ip.src == IP 地址、ip.dst== IP 地址或 ip.addr == IP 地址的格式。

（4）端口过滤:使用 tcp.srcport == 端口号、tcp.dstport == 端口号或 tcp.port == 端口号的格式。

（5） Http 模式过滤：如 http.request.method"GET"（只显示 HTTP GET 方法的）。

（6）逻辑运算符为 and/or/not