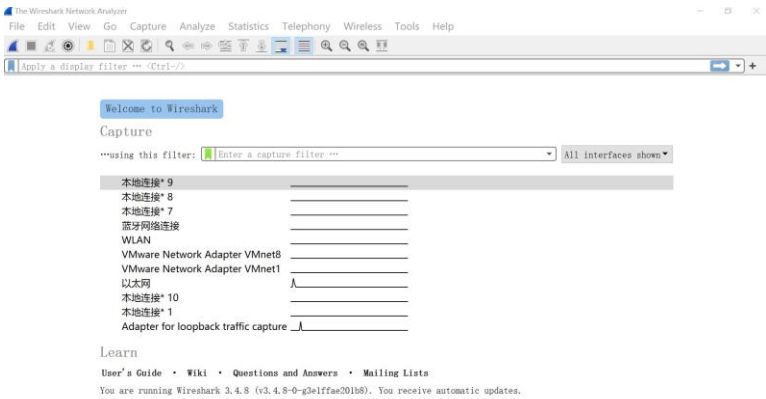


# 实验一

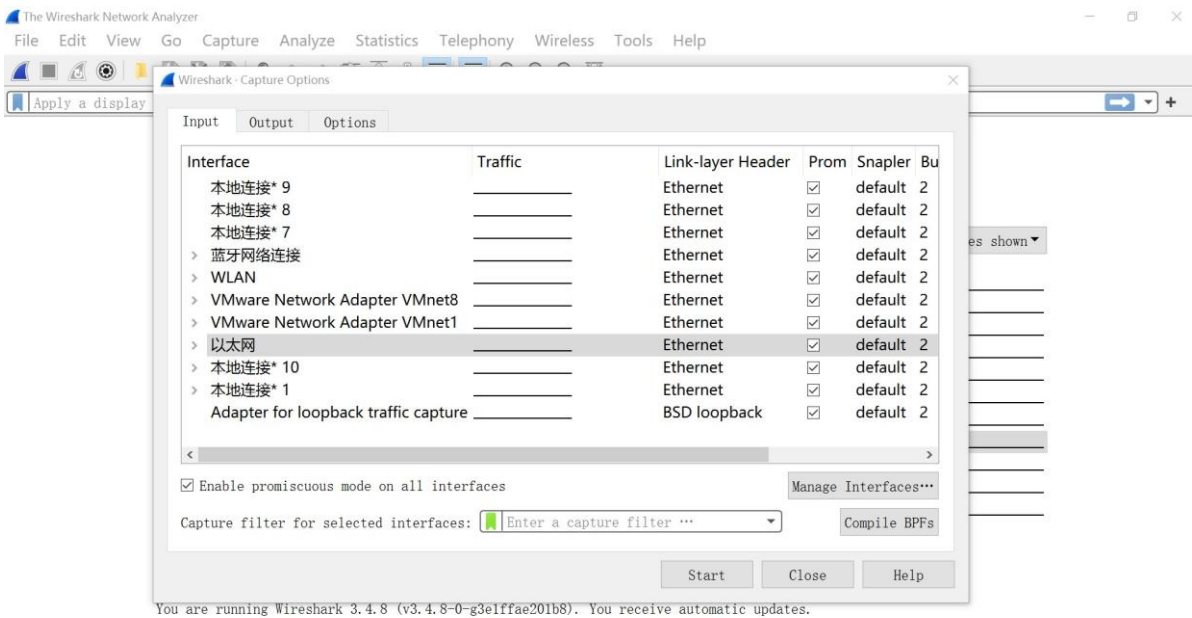
## Wireshark Lab: Getting Started

阅读实验文档，按照操作下载安装 wireshark，版本 v3.4.8，打开后界面如图示：



根据实验文档的指导按步骤进行实验。

1.打开浏览器，再打开 Wireshark，选择以太网开始捕捉。如图：



2.在浏览器打开网站 <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>, 然后在

Wireshark 暂停捕捉, 在上方输入 http 筛选。找到对应网站的数据:

Wireshark packet capture showing HTTP traffic. The packet list shows a GET request for /wireshark-labs/INTRO-wireshark-file1.html. The packet details show the HTTP request structure. The packet bytes show the raw data, including the User-Agent string.

No.	Time	Source	Destination	Protocol	Length	Info
1073	21.884650	114.214.185.163	128.119.245.12	HTTP	576	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1204	22.182760	128.119.245.12	114.214.185.163	HTTP	492	HTTP/1.1 200 OK (text/html)
1218	22.228667	114.214.185.163	128.119.245.12	HTTP	522	GET /favicon.ico HTTP/1.1
1246	22.523999	128.119.245.12	114.214.185.163	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 1073: 576 bytes on wire (4608 bits), 576 bytes captured (4608 bits) on interface \Device\NPF\_{53AA7A70-F030-49F4-8A7D-63797E2E9CD3}, id 0

Ethernet II, Src: Dell\_00:9b:5d (e4:54:e8:00:9b:5d), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)

Internet Protocol Version 4, Src: 114.214.185.163, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 9035, Dst Port: 80, Seq: 1, Ack: 1, Len: 522

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

DNT: 1\r\n

00a0 44 4e 54 3a 20 31 0d 0a 55 70 67 72 61 64 65 2d DNT: 1\r\n Upgrade-

49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 Insecure-Request

73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 s: 1\r\n User-Agent

3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 : Mozilla/5.0 (W

69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 indows NT 10.0;

57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c win64; x 64) Appl

65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 eWebKit/537.36 (

4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b KHTML, like Gecko

6f 29 20 43 68 72 6f 6d 65 2f 39 33 2e 30 2e 34 o) Chrome/93.0.4

3.观察筛选到的数据并分析, 实验完成。

## Questions

1、 观察到的协议有: TCP TLSv1.2 SSDP STP;

Wireshark packet capture showing HTTP traffic. The packet list shows a GET request for /wireshark-labs/INTRO-wireshark-file1.html. The packet details show the HTTP request structure. The packet bytes show the raw data, including the User-Agent string.

No.	Time	Source	Destination	Protocol	Length	Info
1385	10:36:18.974824	114.214.175.233	128.119.245.12	HTTP	661	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1437	10:36:19.233539	128.119.245.12	114.214.175.233	HTTP	492	HTTP/1.1 200 OK (text/html)
1445	10:36:19.280119	114.214.175.233	128.119.245.12	HTTP	522	GET /favicon.ico HTTP/1.1
1453	10:36:19.529627	128.119.245.12	114.214.175.233	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1520	10:36:20.694291	114.214.175.233	128.119.245.12	HTTP	687	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1539	10:36:20.987836	128.119.245.12	114.214.175.233	HTTP	292	HTTP/1.1 304 Not Modified

Transmission Control Protocol, Src Port: 4656, Dst Port: 80, Seq: 1, Ack: 1, Len: 607

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

DNT: 1\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/93.0.4577.63 Safari/537.36 Edg/93.0.961.38\r\n

2、 由上图可知, 从发送到回复 OK 的时间差是  $19.233539 - 18.974824 = 0.258715$ ;

3、 gaia: 128.119.245.12 my address: 114.214.175.233

4、 按照操作输出为 pdf, 如下:

```
No.      Time                Source                Destination            Protocol Length Info
1385 10:36:18.974824    114.214.175.233      128.119.245.12        HTTP      661    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 1385: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F936F7CD}, id 0
Ethernet II, Src: ASIXElec_4b:e9:b8 (f8:e4:3b:4b:e9:b8), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
Internet Protocol Version 4, Src: 114.214.175.233, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4656, Dst Port: 80, Seq: 1, Ack: 1, Len: 607
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
  DNT: 1\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/93.0.4577.63 Safari/537.36 Edg/93.0.961.38\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: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  If-None-Match: "51-5cb7594387f39"\r\n
  If-Modified-Since: Wed, 08 Sep 2021 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/4]
[Response in frame: 1437]
[Next request in frame: 1445]
No.      Time                Source                Destination            Protocol Length Info
1437 10:36:19.233539    128.119.245.12      114.214.175.233      HTTP      492    HTTP/1.1 200 OK (text/html)
Frame 1437: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F936F7CD}, id 0
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: ASIXElec_4b:e9:b8 (f8:e4:3b:4b:e9:b8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.175.233
Transmission Control Protocol, Src Port: 80, Dst Port: 4656, Seq: 1, Ack: 608, Len: 438
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sat, 11 Sep 2021 02:36:18 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Fri, 10 Sep 2021 05:59:01 GMT\r\n
  ETag: "51-5cb9dcfe1017f"\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 1/4]
[Time since request: 0.258715000 seconds]
[Request in frame: 1385]
[Next request in frame: 1445]
[Next response in frame: 1453]
[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)
```