计算机网络第一次实验实验报告

舒文炫

2021 年 9 月 11 日

目录

Chapter 1

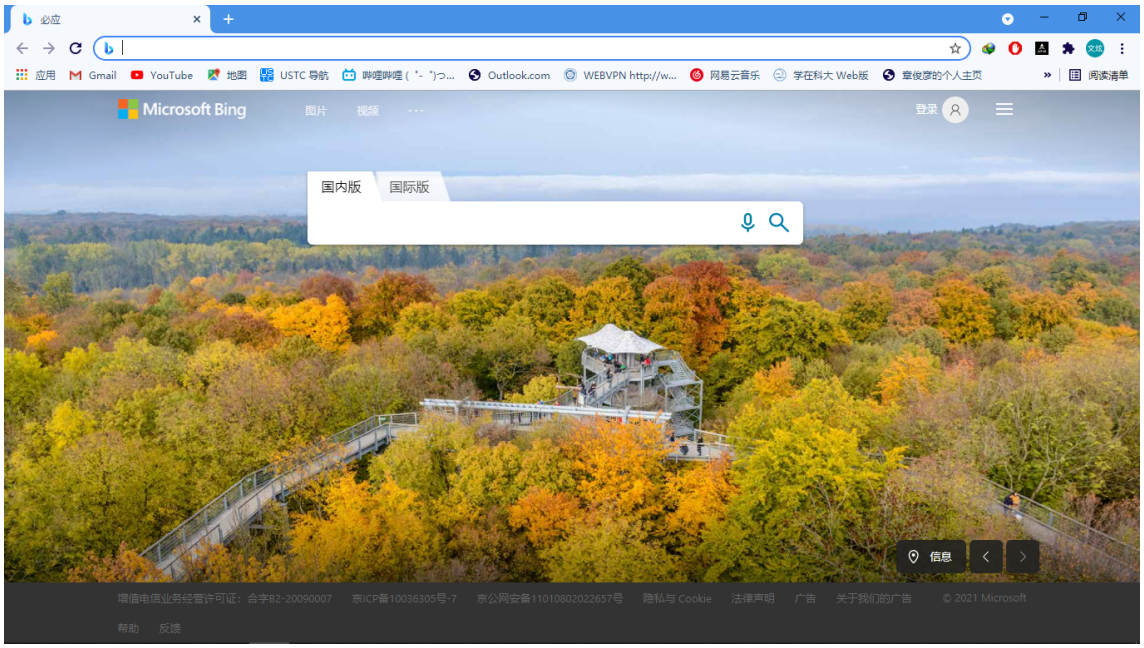
实验目的

本次实验是使用 wireshark 的入门实验，需要通过本次实验了解 wireshark 的基本操作。学会安装 wireshark，然后使用 wireshark 进行简单的抓包，并观察结果。

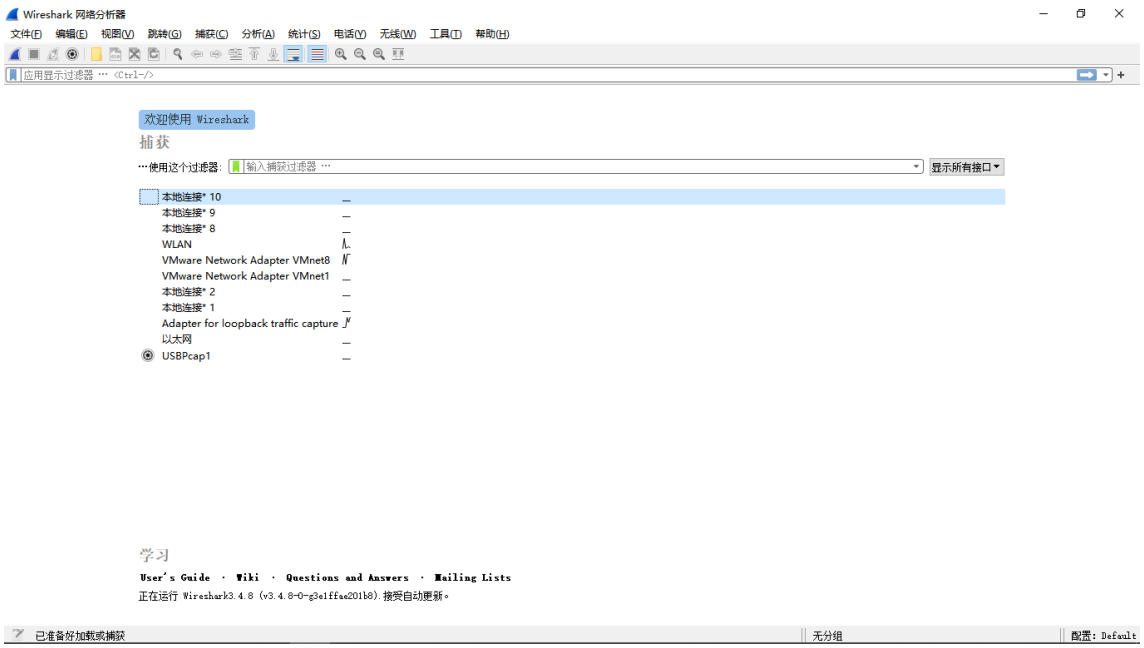
Chapter 2

实验过程

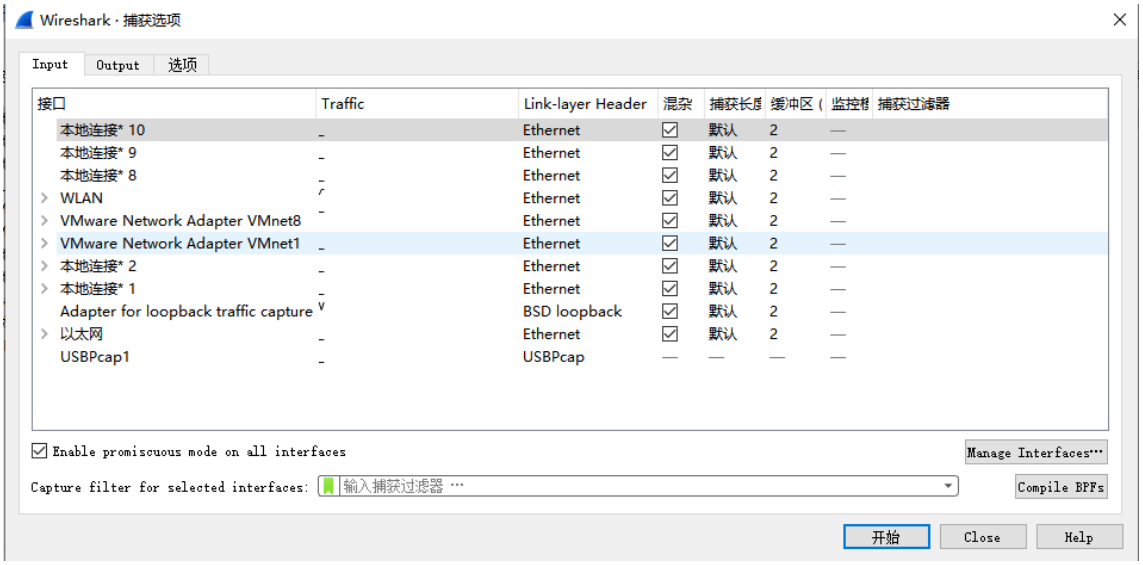
第一步，打开浏览器，我常用的是谷歌，主页 bing，如下图所示。



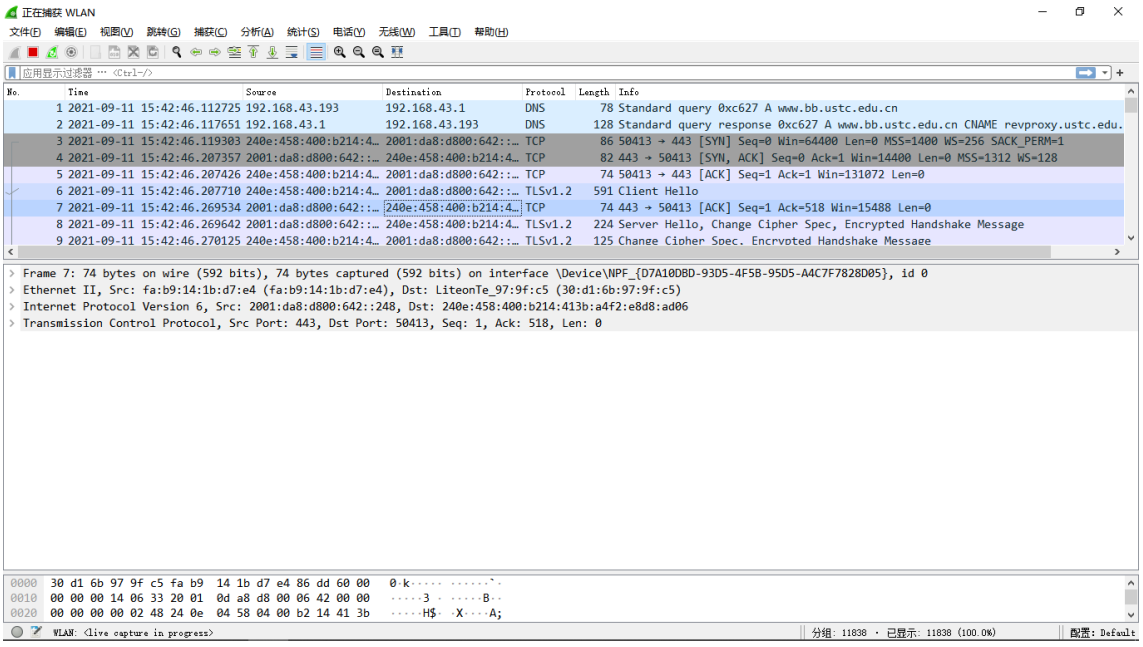
第二步，打开 wireshark，初始界面如下图所示，从上到下依次是：命令栏，此部分用来方便使用该软件一些基础功能，我们需要用到其中的文件和捕获两个菜单；过滤器，该部分用来过滤出所抓包的特定内容。再往下就是目前电脑连接网络的情况。



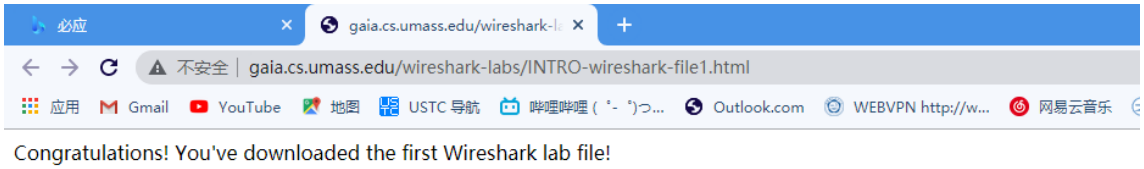
第三步，点击捕获菜单按钮，选择选项这一栏，弹出如下窗口，这个界面里面列出了各个接口，以及通过该接口的数据信息。



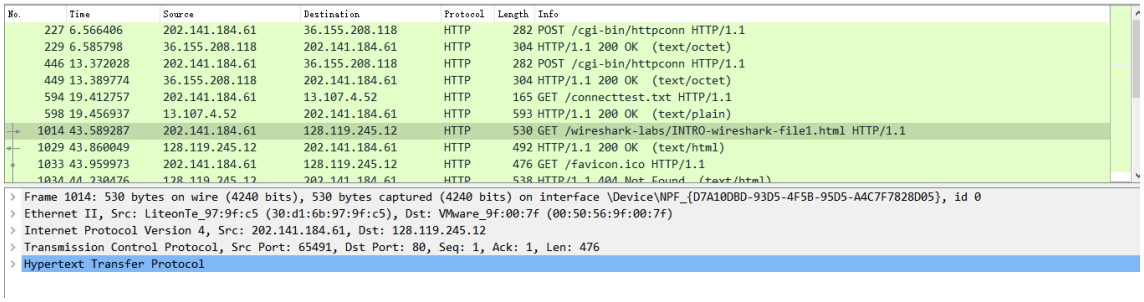
第四步，由于我们连接的是无线网，这里就选择 WLAN 这一项，然后开始捕获，然后就会进入如下界面。这里时间和我后面的图时间显示不一样，因为我一开始忘记了在这里截图，这是后来把时间显示的模式调整为了年月日这样的（实验问题的第二题提到），然后这个时候的 ip 地址也和后面不一样，这是我后来切换了连接的网络。这是后来截的图，就是做一个展示，没什么问题。菜单栏下面那个就是我们所捕获的包，如果不按停止键，个数会随着时间一直增加。



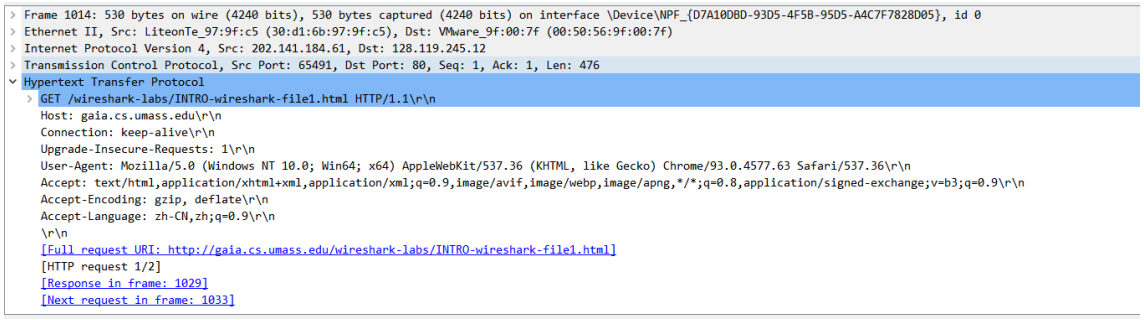
第五步，打开网址 http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html，显示的界面如下。



第六步，停止抓包，在过滤器上输入 http，这样可以过滤出所有 http 的信息，结果如下。



第七步，观察这个结果，我们可以找到 http get 的信息，后面的网址即我们刚刚打开的网址，打开这个网址即是先对该文件发出一个 get 请求，紧接在后面，有一个 ok，这个表示我们的请求被允许，可以访问，结果就是我们打开了这个网页。关于这个 get 项的详细信息如下, 此时实验完成。



Chapter 3

实验问题

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

- TCP 全称 Transmission Control Protocol, 是一种面向连接的、可靠的、基于字节流的传输层通信协议
- DNS 全称 Domain Name System, 是一个应用层协议，作用是将人类可读的域名转换为机器可读的 IP 地址
- ICMPv6，全称 Internet Control Message Protocol v6, 是 IPv6 协议族中的一个基础协议，它合并 rIPv4 中的 ICMP(控制报文协议),IGMP(组成员协议),ARP(地址解析协议),RARP(反向地址解析协议) 和 RA(路广播) 等多个协议的功能。

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.)

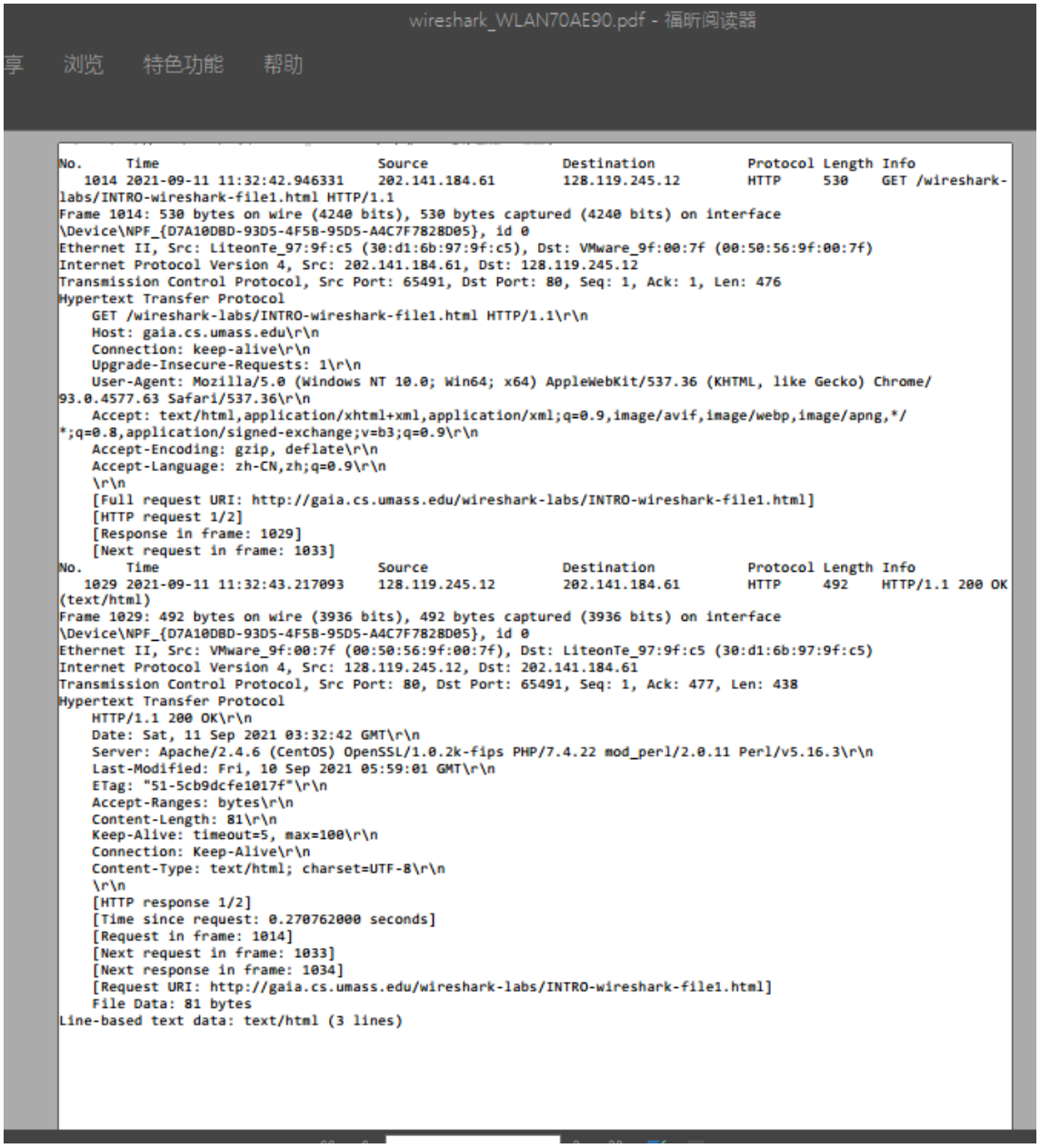
从我第六步的图可以看到，发送 get 请求是在 43.529287s，ok 是在 43.860049s，两者做差我们得出时间 0.270762s，这个就是我们所要求的时间。或者我们点击 ok 那一项，其中有一行写着 time since request：0.270762000seconds，这也可以得到结果。

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?

关于这个问题我们可以看 packets list 中的 Destination 一列，这里 get 请求的目的地就是所要网址的 ip 地址，即 202.141.184.61。ok 返回到我们的电脑，所有它的目的地就是我们电脑的 ip 地址，即 128.119.245.12

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.

关于这个问题，是一个打印操作，我按照要求，将需要的内容打印到了一个 pdf 里面，截图贴在下面




```
No.     Time                           Source                Destination           Protocol Length Info
   1014 2021-09-11 11:32:42.946331     202.141.184.61        128.119.245.12        HTTP     530    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 1014: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5), Dst: VMware_9f:00:7f (00:50:56:9f:00:7f)
Internet Protocol Version 4, Src: 202.141.184.61, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65491, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
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/
93.0.4577.63 Safari/537.36\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: 1029]
    [Next request in frame: 1033]
No.     Time                           Source                Destination           Protocol Length Info
   1029 2021-09-11 11:32:43.217093     128.119.245.12        202.141.184.61        HTTP     492    HTTP/1.1 200 OK
(text/html)
Frame 1029: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: VMware_9f:00:7f (00:50:56:9f:00:7f), Dst: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 202.141.184.61
Transmission Control Protocol, Src Port: 80, Dst Port: 65491, Seq: 1, Ack: 477, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 11 Sep 2021 03:32:42 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 1/2]
    [Time since request: 0.270762000 seconds]
    [Request in frame: 1014]
    [Next request in frame: 1033]
    [Next response in frame: 1034]
    [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)
```