《计算机网络》WireShark 实验

实验一 WireShark 安装运行

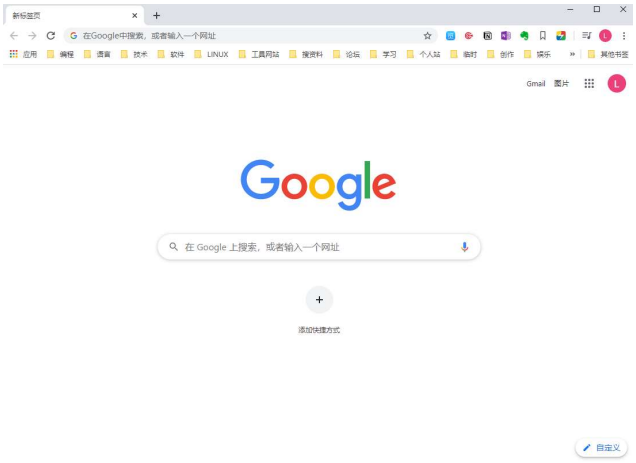
【实验目的】

1. WireShark 的安装及界面熟悉

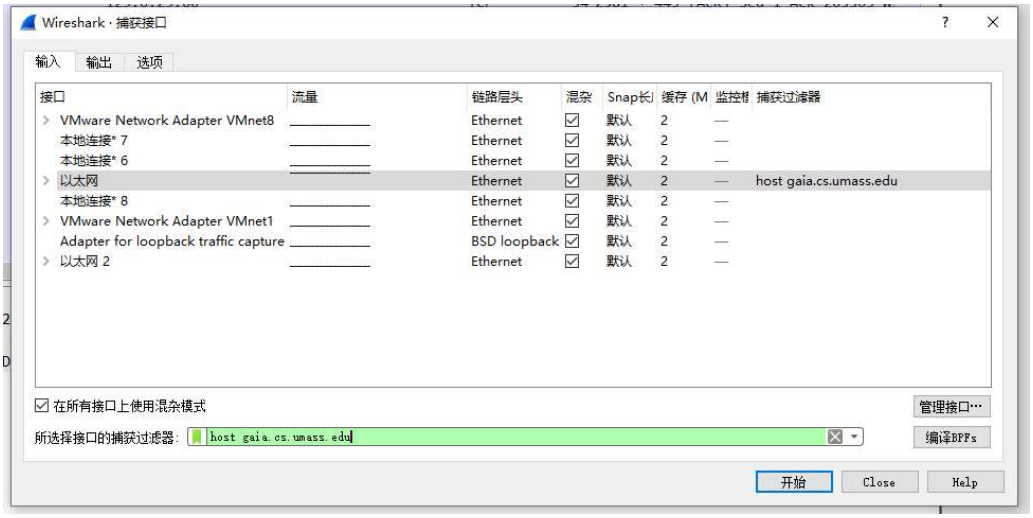
2. 简单 HTTP 的抓取和过滤，结果进行分析和导出

【实验步骤】

1. 打开浏览器



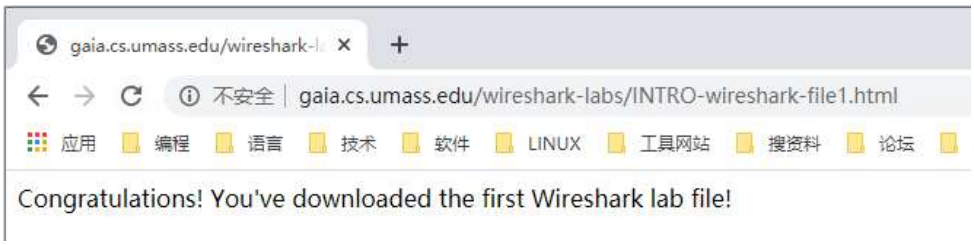
2. 打开 WireShark 在捕获选项选择合适网卡



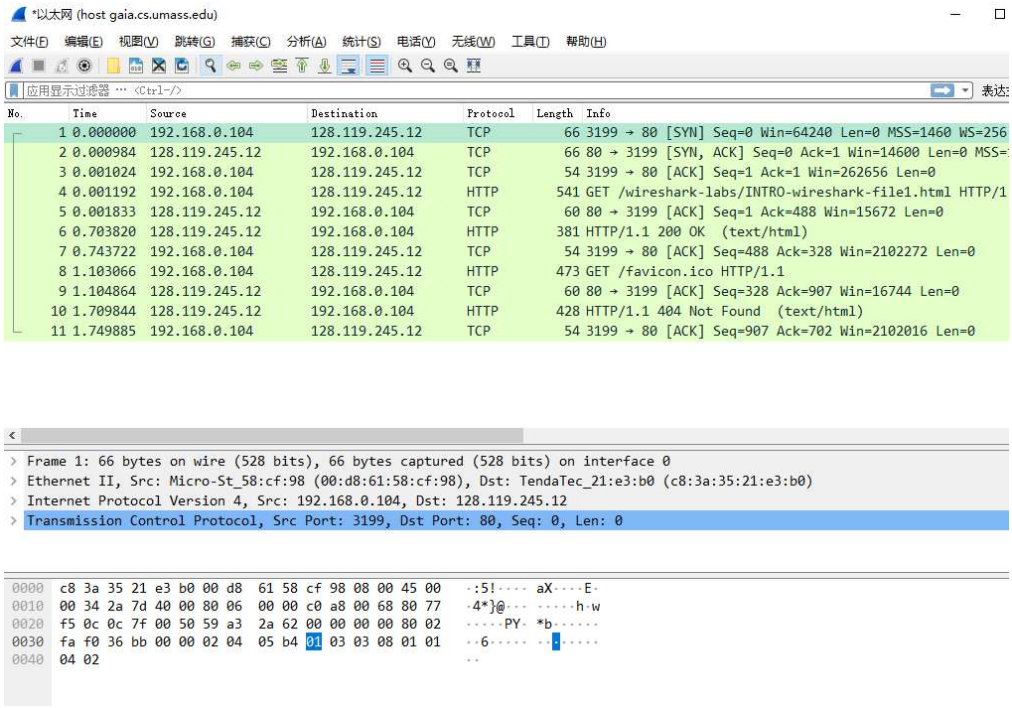
用 host 过滤指定的网站，去除无关干扰

3．进行抓包，在浏览器打开示例网页

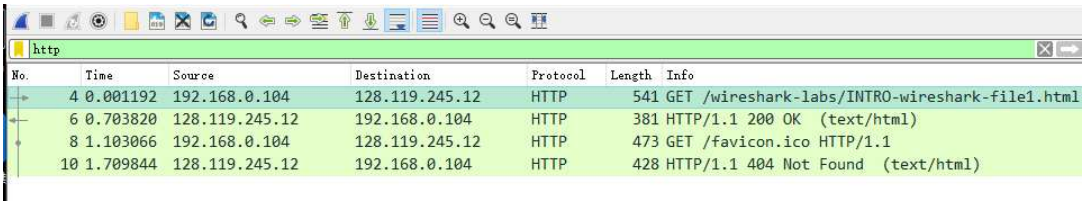
gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html



4．停止抓包并分析结果



5．选择 HTTP 过滤，查看结果

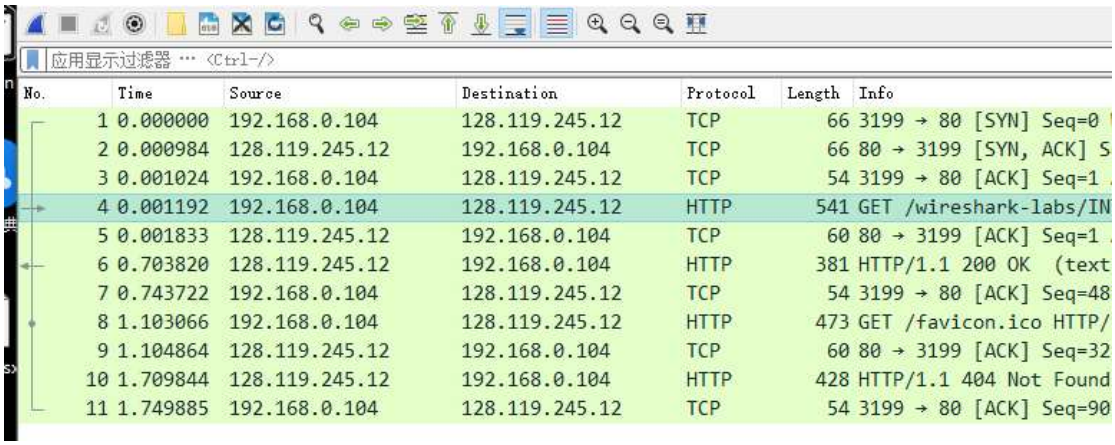


6．分析，详看解答

【问题和解答】

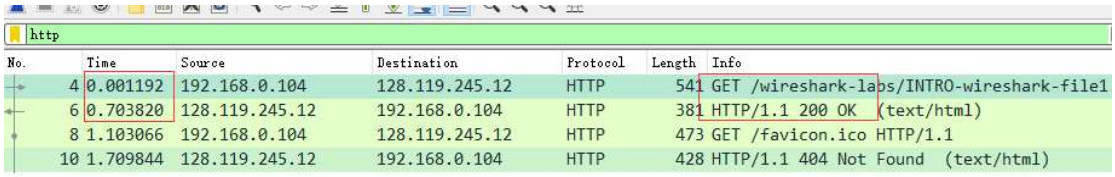
1．查看抓包结果中协议列出现多少不同协议？

答：TCP、HTTP



2. 从发送 HTTP GET 消息到受到 HTTP OK 回复用了多长时间？

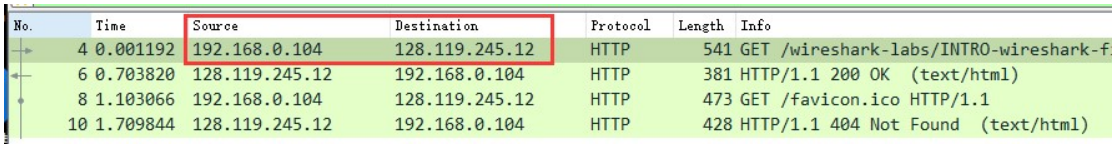
答：0.703820-0.001192 = 0.702628



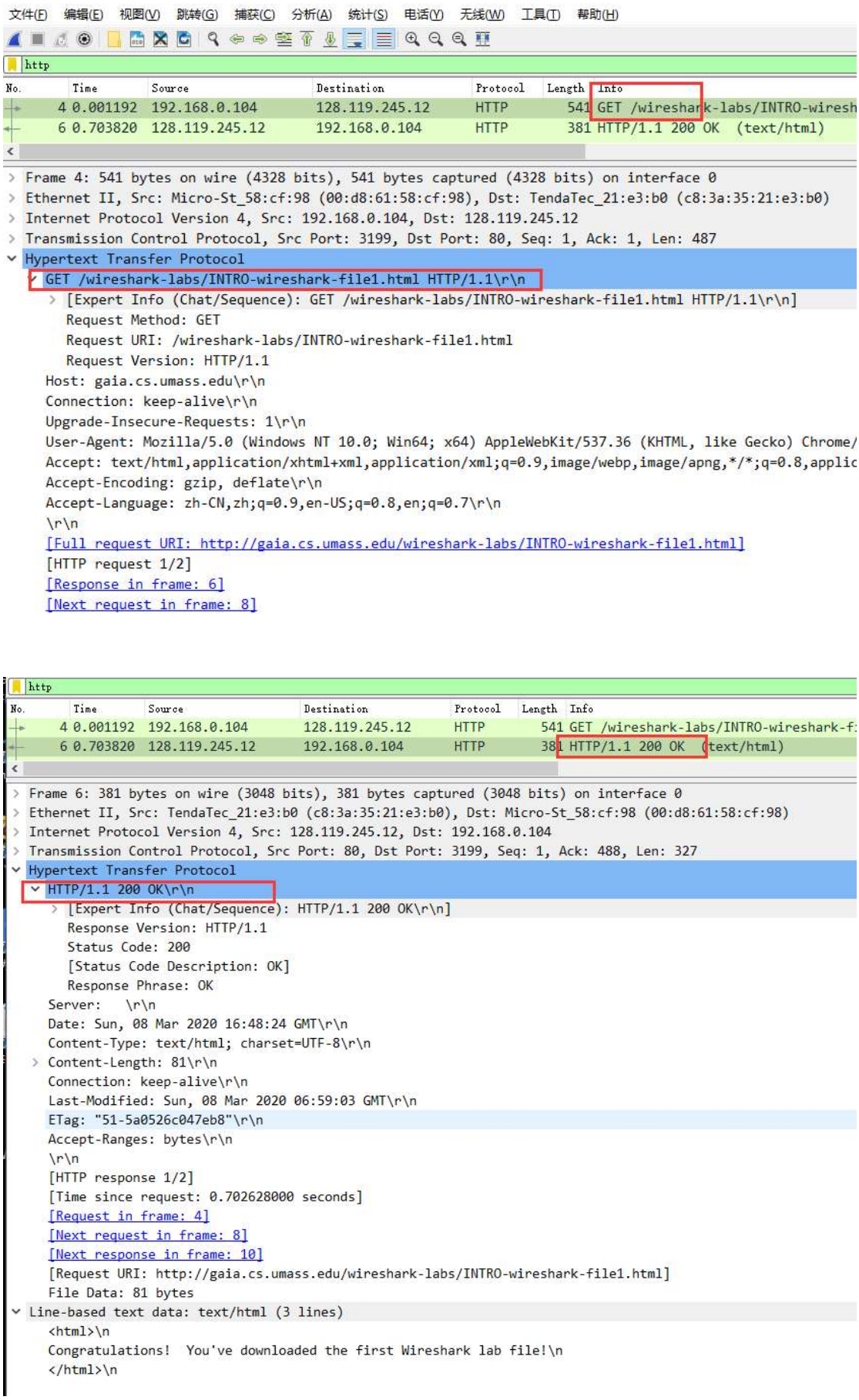
3. 你访问的网址 gaia.cs.umass.edu 的 IP 地址是什么，你的 IP 地址是什么？

答：gaia.cs.umass.edu 的 IP：128.119.245.12

我的 IP：192.168.0.104



4. 输出问题 2 中 HTTP 的 GET 和 OK 消息。


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
4 0.001192 192.168.0.104 128.119.245.12 HTTP 541 GET /wireshark-labs/INTRO-wiresh
6 0.703820 128.119.245.12 192.168.0.104 HTTP 381 HTTP/1.1 200 OK (text/html)
Frame 4: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface 0
Ethernet II, Src: Micro-St_58:cf:98 (00:d8:61:58:cf:98), Dst: TendaTec_21:e3:b0 (c8:3a:35:21:e3:b0)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 3199, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/INTRO-wireshark-file1.html
Request Version: HTTP/1.1
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/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7\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: 6]
[Next request in frame: 8]

http
No. Time Source Destination Protocol Length Info
4 0.001192 192.168.0.104 128.119.245.12 HTTP 541 GET /wireshark-labs/INTRO-wireshark-f
6 0.703820 128.119.245.12 192.168.0.104 HTTP 381 HTTP/1.1 200 OK (text/html)
Frame 6: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface 0
Ethernet II, Src: TendaTec_21:e3:b0 (c8:3a:35:21:e3:b0), Dst: Micro-St_58:cf:98 (00:d8:61:58:cf:98)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104
Transmission Control Protocol, Src Port: 80, Dst Port: 3199, Seq: 1, Ack: 488, Len: 327
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Server: \r\n
Date: Sun, 08 Mar 2020 16:48:24 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Content-Length: 81\r\n
Connection: keep-alive\r\n
Last-Modified: Sun, 08 Mar 2020 06:59:03 GMT\r\n
ETag: "51-5a0526c047eb8"\r\n
Accept-Ranges: bytes\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.702628000 seconds]
[Request in frame: 4]
[Next request in frame: 8]
[Next response in frame: 10]
[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)
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n