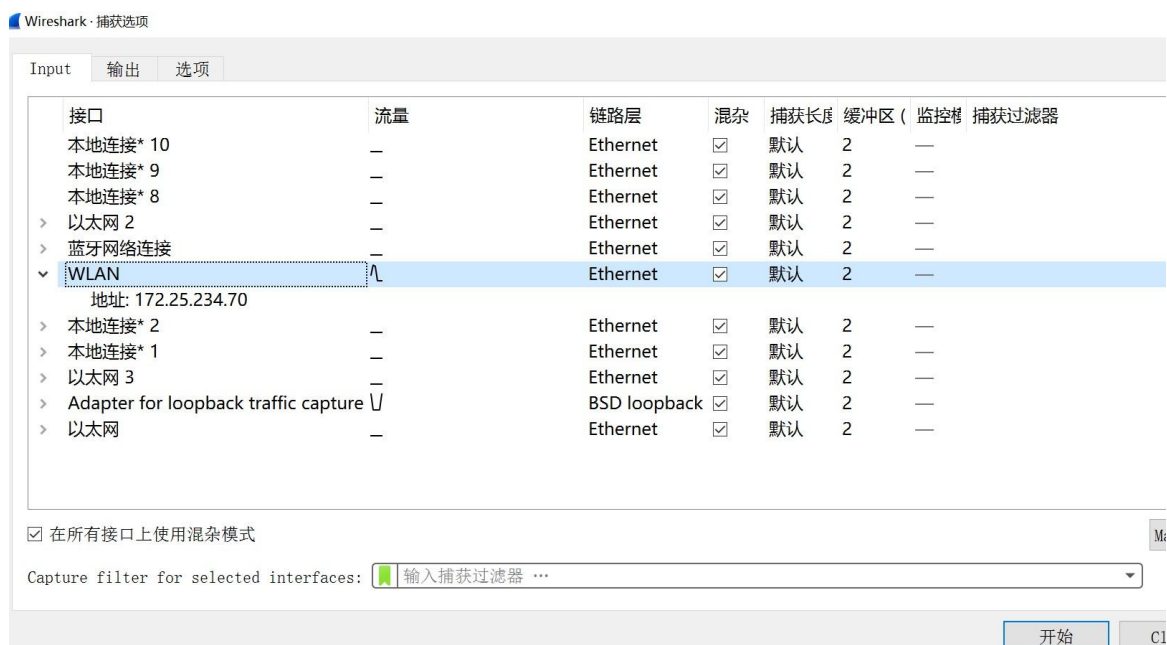


实验目的：掌握使用 wireshark 进行抓包

实验结果：

点击“开始”实现抓包



显示页面：



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

抓包结果：

111.pcapng

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
753	2023-03-03 16:58:18.327899	192.168.254.245	172.25.234.70	TCP	56	53 → 5
754	2023-03-03 16:58:18.327899	192.168.254.245	172.25.234.70	DNS	232	Standard
755	2023-03-03 16:58:18.328299	172.25.234.70	192.168.254.245	TCP	54	55938
756	2023-03-03 16:58:18.328566	172.25.234.70	20.212.96.199	TCP	66	55939
757	2023-03-03 16:58:18.329553	192.168.254.245	172.25.234.70	TCP	56	53 → 5
758	2023-03-03 16:58:18.329623	172.25.234.70	192.168.254.245	TCP	54	55937
759	2023-03-03 16:58:18.330653	192.168.254.245	172.25.234.70	TCP	56	53 → 5
760	2023-03-03 16:58:18.330708	172.25.234.70	192.168.254.245	TCP	54	55938
761	2023-03-03 16:58:18.330795	172.25.234.70	128.119.245.12	HTTP	652	GET /w

> Frame 761: 652 bytes on wire (5216 bits), 652 bytes captured on interface 0, 652 bytes from 172.25.234.70 to 128.119.245.12 on interface 0

> Ethernet II, Src: IntelCor\_06:43:e8 (18:26:49:06:43:e8), Dst: Realtek\_8c:85:4a (08:00:27:08:c5:4a), Protocol: 0x0800 (Ethernet II)

> Internet Protocol Version 4, Src: 172.25.234.70, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 55913, Dst Port: 80, Seq: 3042128128, Len: 652

> Hypertext Transfer Protocol

0000 28 a2 4b f6 12 a0 18 26 49 06 43  
0010 02 7e b8 6d 40 00 80 06 00 00 ac  
0020 f5 0c da 69 00 50 8b 86 6e 47 cf  
0030 02 01 0e 55 00 00 47 45 54 20 2f  
0040 68 61 72 6b 2d 6c 61 62 73 2f 49  
0050 77 69 72 65 73 68 61 72 6b 2d 66  
0060 68 74 6d 6c 20 48 54 54 50 2f 31  
0070 6f 73 74 3a 20 67 61 69 61 2e 63  
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e

1、列出步骤 7 中未过滤的包列表窗口中的协议列中的 3 个不同协议。

No.	Time	Source	Destination	Protocol
736	2023-03-03 16:58:18.315558	172.25.234.70	51.104.15.252	TCP
737	2023-03-03 16:58:18.315558	172.25.234.70	51.104.15.252	TLSv1.2
738	2023-03-03 16:58:18.321377	172.25.234.70	192.168.254.245	TCP
739	2023-03-03 16:58:18.321645	172.25.234.70	192.168.254.245	TCP
740	2023-03-03 16:58:18.323680	192.168.254.245	172.25.234.70	TCP
741	2023-03-03 16:58:18.323758	172.25.234.70	192.168.254.245	TCP
742	2023-03-03 16:58:18.323853	172.25.234.70	192.168.254.245	TCP
743	2023-03-03 16:58:18.323888	172.25.234.70	192.168.254.245	DNS

TCP DNS TLS

2、从发送 HTTP GET 消息到收到 HTTP OK 应答，它花了多长时间？

No.	Time	Source	Destination
761	2023-03-03 16:58:18.330795	172.25.234.70	128.119.245.12
822	2023-03-03 16:58:18.589989	128.119.245.12	172.25.234.70

大约 0.25s

3. gaia.cs.umass.edu 的互联网地址是什么？

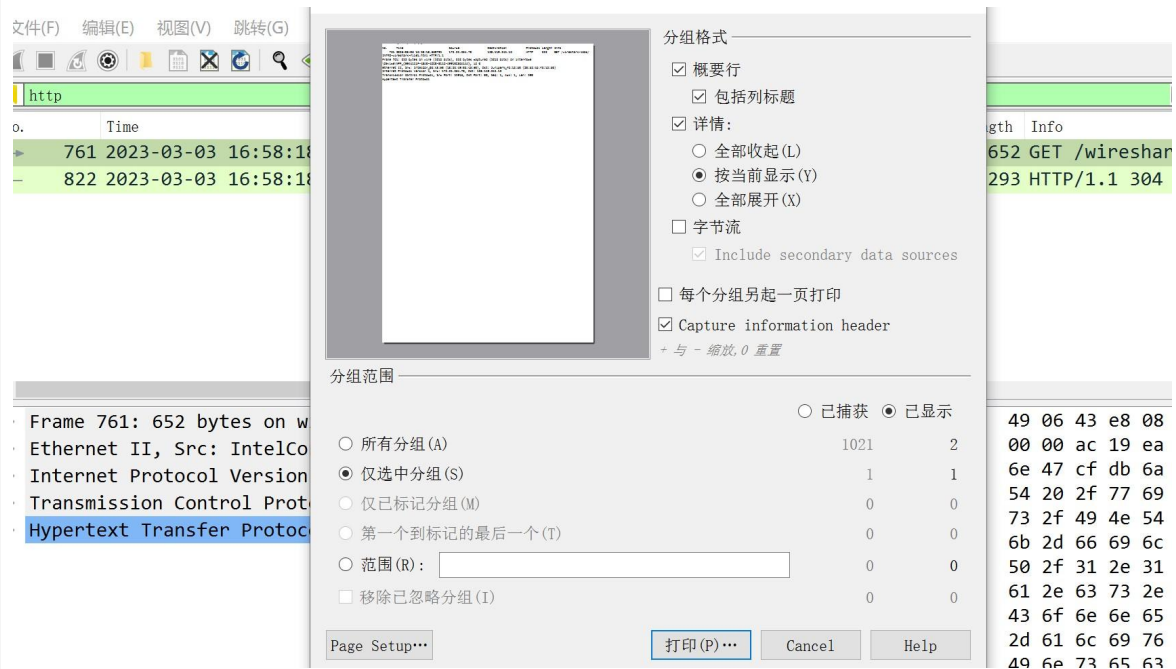
你的电脑的互联网地址是什么？

gaia. cs. umass. edu 的互联网地址：128. 119. 245. 12

我的电脑的互联网地址：172. 25. 234. 70

4. 打印上面问题 2 中提到的两条 HTTP 消息（GET 和 OK）

打印页面：



问题及收获：

学会使用 wireshark 进行抓包，掌握如何通过应用显示过滤器来筛选相关协议，掌握如何读懂协议内容。