# Wireshark实验：入门 v8.0

**《计算机网络：自顶向下方法》第8版补充材料，J.F. Kurose 和 K.W. Ross**

“告诉我，我会忘记；给我看，我会记住；让我参与，我会理解。” ——中国谚语

© 2005-2024, J.F. Kurose 和 K.W. Ross，保留所有权利

## 引言

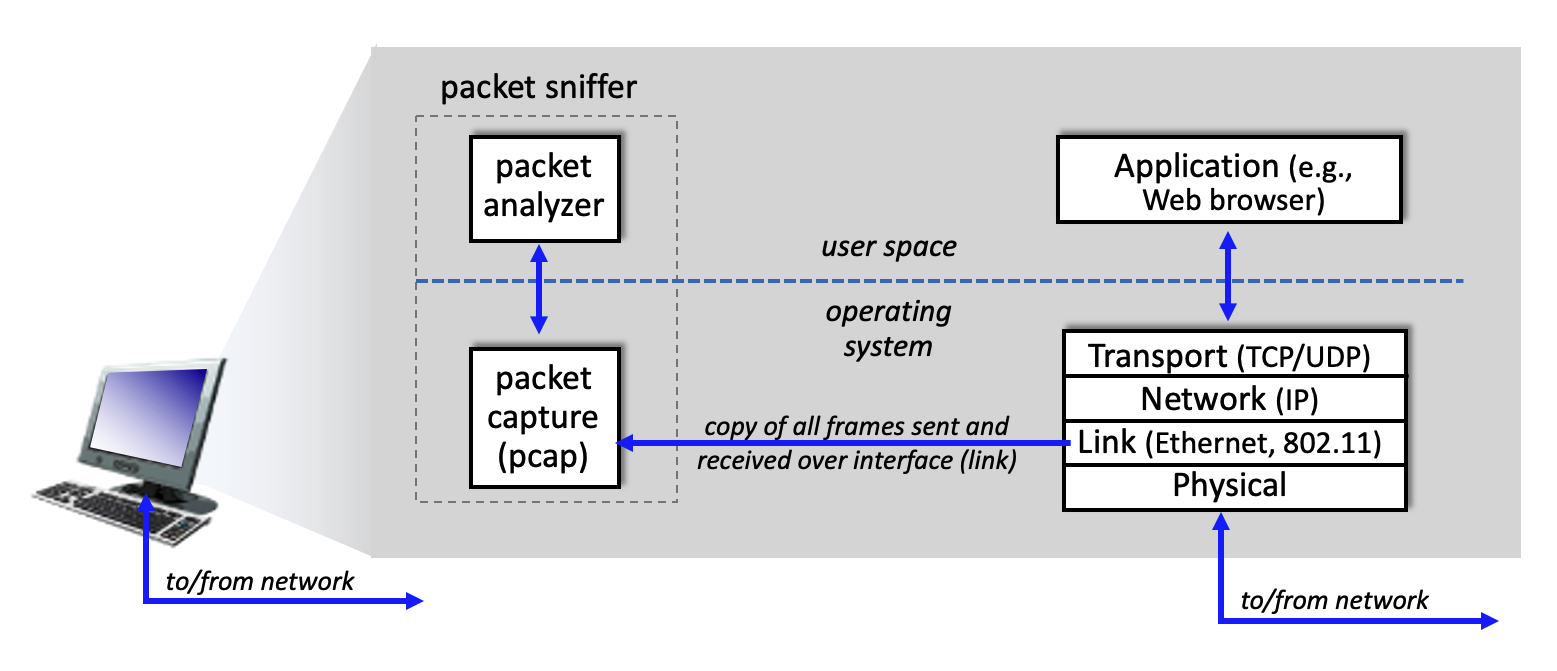
通过“观察协议的实际运行”和“与协议互动”——观察两个协议实体之间交换的消息序列，深入研究协议操作的细节，并触发协议执行特定动作，然后观察这些动作及其结果，可以极大地加深对网络协议的理解。这可以在模拟场景或真实的网络环境（如互联网）中进行。在本课程的Wireshark实验中，你将使用自己的计算机在不同场景下运行各种网络应用程序。你将观察计算机中的网络协议“实际运行”，与互联网中其他地方执行的协议实体进行交互并交换消息。因此，你和你的计算机将成为这些“现场”实验的组成部分。你将通过实践来观察和学习。

在本第一个Wireshark实验中，你将熟悉Wireshark，并进行一些简单的包捕获和观察。

观察协议实体之间交换消息的基本工具称为**数据包嗅探器**。顾名思义，数据包嗅探器捕获（“嗅探”）你的计算机发送/接收的消息；它通常还会存储和/或显示这些捕获消息中各个协议字段的内容。数据包嗅探器本身是被动的，它观察你的计算机上运行的应用程序和协议发送和接收的消息，但从不主动发送数据包。同样，接收到的数据包也不会明确地寻址到数据包嗅探器。相反，数据包嗅探器接收到的是你的计算机上运行的应用程序和协议发送/接收的数据包副本。

图1显示了数据包嗅探器的结构。图1右侧是通常在你的计算机上运行的协议（在本例中为互联网协议）和应用程序（如网络浏览器或电子邮件客户端）。数据包嗅探器（图1中虚线矩形内所示）是你计算机上常规软件的补充，包含两部分。**数据包捕获库**接收通过特定接口（链路层，如以太网或WiFi）发送或接收的每个链路层帧的副本。回顾教材第1.5节（图1.24[脚注1]）的讨论，较高层协议（如HTTP、FTP、TCP、UDP、DNS或IP）交换的消息最终都会被封装在链路层帧中，并通过物理介质（如以太网电缆或802.11 WiFi无线电）传输。因此，捕获所有链路层帧就能获取你的计算机上执行的所有协议和应用程序通过监控链路发送/接收的所有消息。

[脚注1：对图表和章节的引用均来自我们的教材《计算机网络：自顶向下方法》第8版，J.F. Kurose 和 K.W. Ross，Addison-Wesley/Pearson，2020年。]



**图1：数据包嗅探器结构**

数据包嗅探器的第二个组成部分是**数据包分析器**，它显示协议消息中所有字段的内容。为此，数据包分析器必须“理解”协议交换的所有消息的结构。例如，假设我们希望显示图1中HTTP协议交换消息的各个字段。数据包分析器理解以太网帧的格式，因此可以识别以太网帧中的IP数据报。它还理解IP数据报的格式，因此可以提取IP数据报中的TCP段。最后，它理解TCP段的结构，因此可以提取TCP段中包含的HTTP消息。此外，它理解HTTP协议，例如，知道HTTP消息的开头字节将包含“GET”、“POST”或“HEAD”等字符串，如教材中的图2.8所示。

我们将在这些实验中使用**Wireshark数据包嗅探器**（[http://www.wireshark.org/](http://www.wireshark.org/" \t "/Users/tiange/Documents\\x/_blank)），以显示不同协议栈层级中发送/接收的消息内容。（严格来说，Wireshark是一个数据包分析器，它使用你计算机中的数据包捕获库。此外，Wireshark捕获的是图1所示的链路层帧，但使用通用术语“数据包”来指代链路层帧、网络层数据报、传输层段和应用层消息，因此我们这里将遵循Wireshark的惯例，使用不够精确的“数据包”术语）。Wireshark是一个免费的网络协议分析器，运行在Windows、Mac和Linux/Unix计算机上。它是我们实验的理想数据包分析器——稳定、拥有庞大的用户基础和完善的文档支持，包括用户指南（[http://www.wireshark.org/docs/wsug\_html\_chunked/](http://www.wireshark.org/docs/wsug_html_chunked/" \t "/Users/tiange/Documents\\x/_blank)）、手册页（[http://www.wireshark.org/docs/man-pages/](http://www.wireshark.org/docs/man-pages/" \t "/Users/tiange/Documents\\x/_blank)）和详细的常见问题解答（[http://www.wireshark.org/faq.html](http://www.wireshark.org/faq.html" \t "/Users/tiange/Documents\\x/_blank)），功能丰富，能够分析数百种协议，并拥有设计良好的用户界面。它支持以太网、串行（PPP）、802.11（WiFi）无线局域网等多种链路层技术。

## 获取Wireshark

要运行Wireshark，你需要一台支持Wireshark和libpcap或WinPCap数据包捕获库的计算机。如果你的操作系统中未安装libpcap软件，它将在安装Wireshark时自动安装。请访问[http://www.wireshark.org/download.html](http://www.wireshark.org/download.html" \t "/Users/tiange/Documents\\x/_blank)查看支持的操作系统列表和下载站点。

**下载并安装Wireshark软件：**

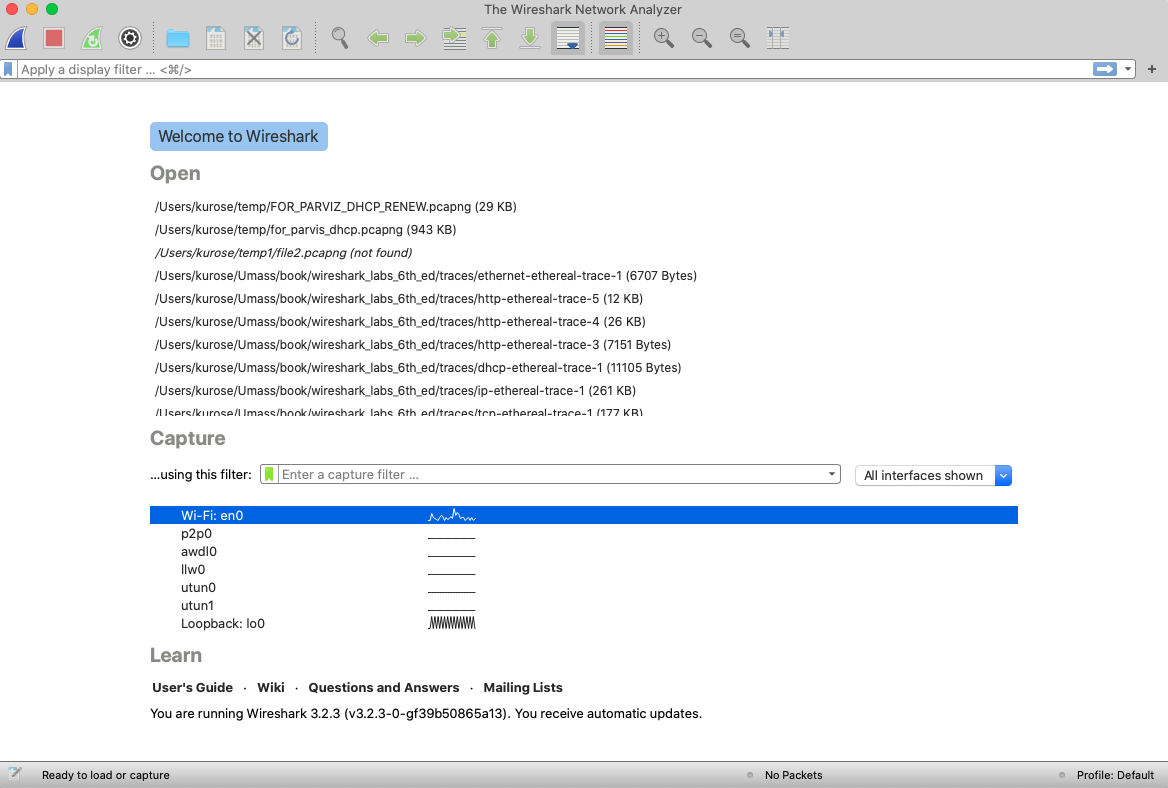
* 访问[http://www.wireshark.org/download.html](http://www.wireshark.org/download.html" \t "/Users/tiange/Documents\\x/_blank)，下载并安装适用于你的计算机的Wireshark二进制文件。 Wireshark常见问题解答页面包含许多有用的提示和有趣的信息，特别是在安装或运行Wireshark时遇到问题的情况下。

## 运行Wireshark

在运行Wireshark之前，请检查你的网络连接和浏览器配置的以下两点：

* 确保你未运行VPN（虚拟专用网络）服务。我们将在本课程后续学习VPN。目前，你只需知道，当运行VPN服务时，你的计算机发送的上层协议信息（HTTP、TCP）可能会被加密。这使得Wireshark无法查看这些协议内部的活动！
* 确保你的浏览器程序默认未使用HTTP/3协议或QUIC协议。我们将在第2章学习HTTP/3和QUIC。目前，你只需知道，当使用HTTP/3或QUIC时，你的计算机发送的上层协议信息（HTTP、TCP）将被加密。到2024年，大多数流行浏览器已默认采用HTTP/3和QUIC。有关如何禁用浏览器默认HTTP/3和QUIC的文档，请参见：[https://techysnoop.com/disable-quic-protocol-in-chrome-edge-firefox/](https://techysnoop.com/disable-quic-protocol-in-chrome-edge-firefox/" \t "/Users/tiange/Documents\\x/_blank)。

运行Wireshark程序时，你将看到一个启动界面，类似于下图所示。不同版本的Wireshark可能有不同的启动界面，因此如果你的界面与下图不完全相同，不必惊慌！Wireshark文档指出：“由于Wireshark运行在多种不同平台上，使用不同的窗口管理器、应用不同的样式，并且底层GUI工具包的版本不同，你的屏幕可能与提供的截图有所不同。但由于功能上没有实质差异，这些截图仍应易于理解。”说得很好。

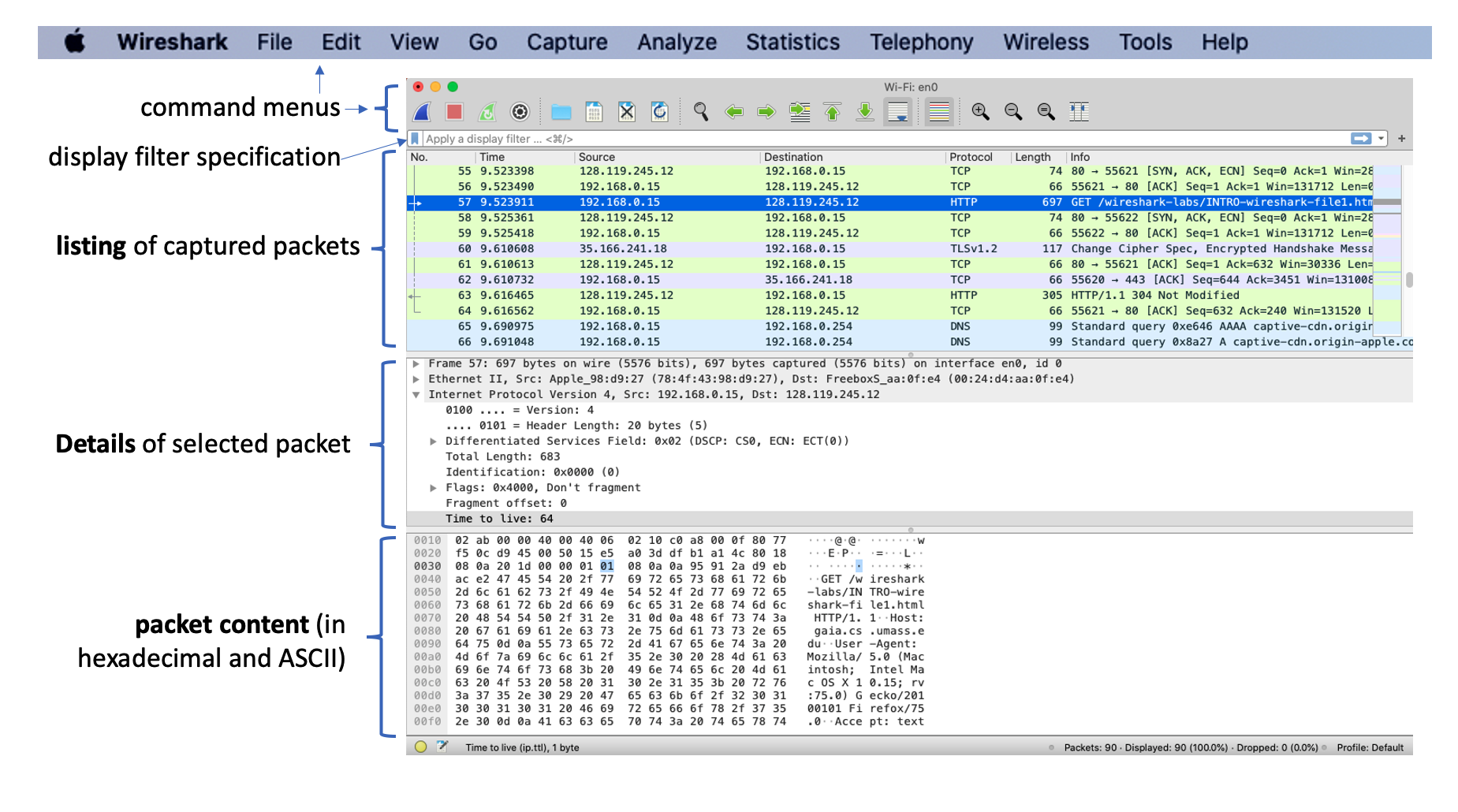


**图2：Wireshark初始界面**

这个界面上没有太多有趣的内容。但请注意，在“捕获”部分下，列出了所谓的接口。我们在Mac计算机上截图的界面显示只有一个接口——“Wi-Fi en0”（图2中以蓝色高亮显示），这是WiFi访问的接口。所有进出这台计算机的数据包都将通过WiFi接口，因此我们需要在这里捕获数据包。在Mac上，双击此接口（或在其他计算机上，在启动页面找到提供互联网连接的接口，例如WiFi或以太网接口，并选择该接口）。

让我们试着运行Wireshark！如果你点击一个接口开始数据包捕获（即让Wireshark开始捕获该接口发送/接收的所有数据包），将显示类似下图的界面，显示正在捕获的数据包信息。开始数据包捕获后，你可以通过“捕获”下拉菜单选择“停止”，或点击图2中Wireshark鳍旁边的红色方形按钮停止捕获。[脚注2]

[脚注2：如果你无法运行Wireshark，你仍然可以查看在作者（Jim）的计算机上捕获的数据包跟踪。下载zip文件[http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8E.zip](http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8E.zip" \t "/Users/tiange/Documents\\x/_blank)，并提取文件wireshark-intro-trace。这些跟踪文件是Wireshark在作者（Jim）的计算机上运行时，按照上述步骤收集的。下载跟踪文件后，你可以通过Wireshark的“文件”下拉菜单选择“打开”，然后选择wireshark-intro-trace跟踪文件加载它。显示结果应类似于图3和图5。（Wireshark的用户界面在不同操作系统和不同版本的Wireshark上显示略有不同）。]



**图3：Wireshark窗口，捕获期间和之后**

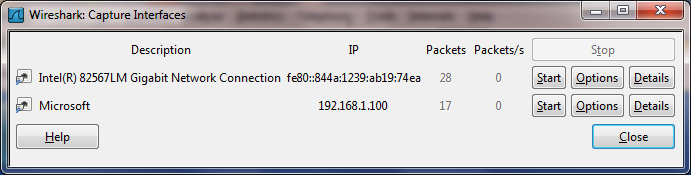
这个界面看起来更有趣！Wireshark界面有五个主要组成部分：

* **命令菜单**：位于Wireshark窗口顶部（在Mac上也位于屏幕顶部；图3的截图来自Mac）的标准下拉菜单。目前我们关注的是“文件”和“捕获”菜单。“文件”菜单允许你保存捕获的数据包数据、打开包含之前捕获数据包数据的文件，或退出Wireshark应用程序。“捕获”菜单允许你开始数据包捕获。
* **数据包列表窗口**：显示每个捕获数据包的单行摘要，包括数据包编号（由Wireshark分配；注意，这不是任何协议头中的数据包编号）、捕获数据包的时间、数据包的源和目标地址、协议类型以及数据包中包含的协议特定信息。可以通过点击列名按这些类别对数据包列表进行排序。协议类型字段列出发送或接收此数据包的最高层协议，即该数据包的源或最终接收协议。
* **数据包头部详细信息窗口**：提供在数据包列表窗口中选择（高亮显示）的数据包的详细信息。（要在数据包列表窗口中选择一个数据包，将光标放在数据包的单行摘要上，然后点击左键。）这些详细信息包括以太网帧（假设数据包通过以太网接口发送/接收）和包含此数据包的IP数据报的信息。可以通过点击数据包详细信息窗口中以太网帧或IP数据报行左侧的加号/减号框或右/下箭头，展开或最小化以太网和IP层细节的显示。如果数据包通过TCP或UDP传输，也会显示TCP或UDP的详细信息，同样可以展开或最小化。最后，还会提供发送或接收此数据包的最高层协议的详细信息。
* **数据包内容窗口**：以ASCII和十六进制格式显示捕获帧的全部内容。
* **数据包显示过滤器字段**：位于Wireshark图形用户界面顶部，可以输入协议名称或其他信息，以过滤数据包列表窗口（以及数据包头部和内容窗口）中显示的信息。在下面的示例中，我们将使用数据包显示过滤器字段，让Wireshark仅显示HTTP消息相关的包。

## Wireshark试运行

学习任何新软件的最佳方法是亲自尝试！我们假设你的计算机通过有线以太网接口或无线802.11 WiFi接口连接到互联网。请按照以下步骤操作：

1. 启动你喜欢的网络浏览器，显示你选择的首页。
2. 启动Wireshark软件。你将首先看到类似于图2所示的窗口。此时Wireshark尚未开始捕获数据包。
3. 要开始数据包捕获，选择“捕获”下拉菜单并选择“接口”。这将显示“Wireshark：捕获接口”窗口（在PC上）或在Mac上选择“选项”。你应该会看到接口列表，如图4a（Windows）和图4b（Mac）所示。



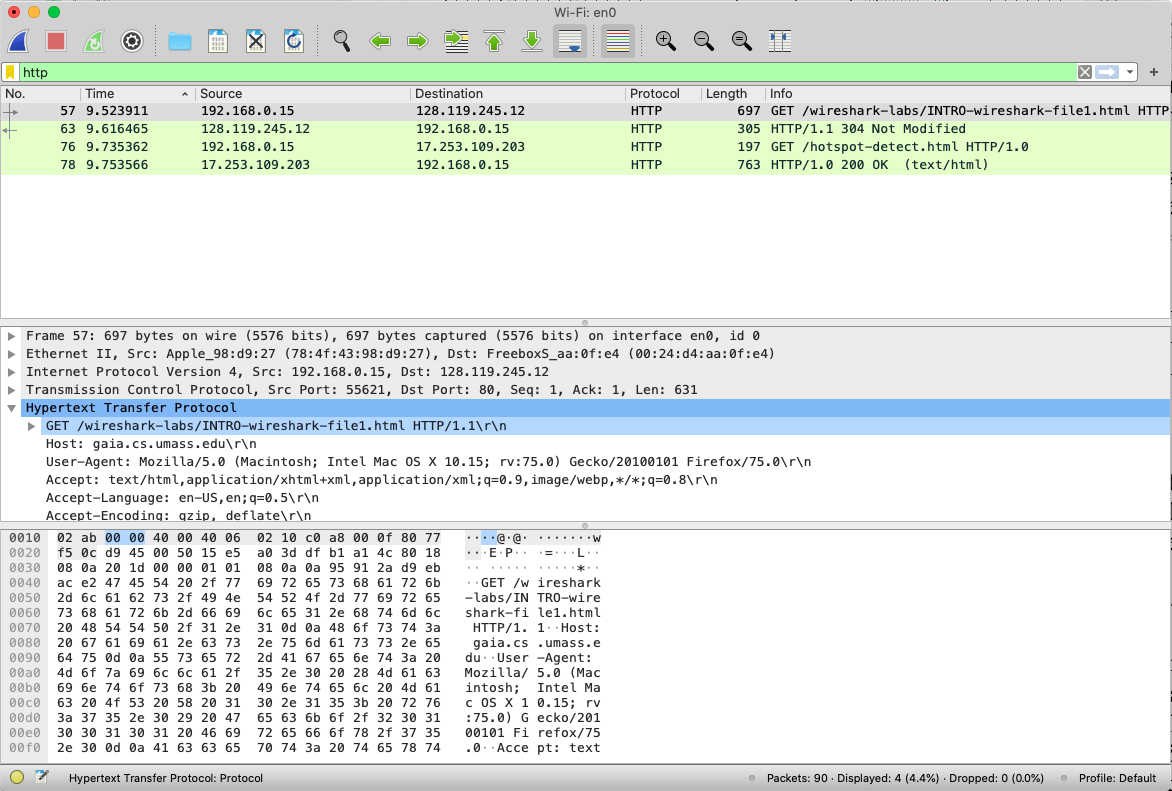
**图4a：Wireshark捕获接口窗口，在Windows计算机上**

A screenshot of a cell phone

Description automatically generated

**图4b：Wireshark捕获接口窗口，在Mac计算机上**

1. 你将看到计算机上的接口列表以及每个接口上至今观察到的数据包计数。在Windows计算机上，点击你希望开始捕获数据包的接口（在图4a的示例中为Gigabit网络连接）的“开始”按钮。在Mac上，选择接口并点击窗口底部的“开始”按钮。数据包捕获将开始——Wireshark现在正在捕获你的计算机发送/接收的所有数据包！
2. 开始数据包捕获后，将显示类似于图3的窗口，显示正在捕获的数据包。通过选择“捕获”下拉菜单并选择“停止”，或点击红色停止方块，可以停止数据包捕获。但现在不要停止捕获，我们先捕获一些有趣的数据包。为此，我们需要生成一些网络流量。让我们使用网络浏览器来生成流量，浏览器将使用我们在课堂上将详细学习的HTTP协议从网站下载内容。
3. 在Wireshark运行时，在浏览器中输入以下URL： [http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html](http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html" \t "/Users/tiange/Documents\\x/_blank) 并让浏览器显示该页面。为了显示此页面，你的浏览器将联系gaia.cs.umass.edu的HTTP服务器并与服务器交换HTTP消息以下载此页面，如教材第2.2节所述。包含这些HTTP消息的以太网或WiFi帧（以及通过你的以太网或WiFi适配器的所有其他帧）将被Wireshark捕获。
4. 在浏览器显示INTRO-wireshark-file1.html页面（这是一个简单的祝贺单行页面）后，通过选择Wireshark捕获窗口中的“停止”来停止Wireshark数据包捕获。现在主Wireshark窗口应类似于图3。你现在拥有包含你的计算机与其他网络实体之间交换的所有协议消息的实时数据包数据！与gaia.cs.umass.edu web服务器的HTTP消息交换应该出现在捕获的数据包列表中。但还会显示许多其他类型的数据包（例如，图3中的“协议”列显示了许多不同协议类型）。尽管你只下载了一个网页，但显然你的计算机上运行了许多用户看不到的其他协议。我们将在教材后续内容中进一步了解这些协议！现在，你只需知道网络中往往有许多“看不见”的活动！
5. 在Wireshark主窗口顶部的显示过滤器规范窗口中输入“http”（不带引号，且使用小写——Wireshark中所有协议名称均为小写）。然后点击右侧的“应用”按钮（或直接按回车键）。这将使数据包列表窗口仅显示HTTP消息。图5显示了在图3所示的捕获窗口应用http过滤器后的截图。请注意，在选定的数据包详细信息窗口中，我们选择了显示超文本传输协议（HTTP）应用消息的详细信息，该消息位于TCP段内，而TCP段位于IPv4数据报内，IPv4数据报位于以太网II（WiFi）帧内。专注于特定消息、段、数据报和帧级别的细节内容让我们能够专注于我们想查看的内容（在本例中为HTTP消息）。



**图5：查看包含**[http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html的GET请求的HTTP消息详情](http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html%E7%9A%84GET%E8%AF%B7%E6%B1%82%E7%9A%84HTTP%E6%B6%88%E6%81%AF%E8%AF%A6%E6%83%85" \t "/Users/tiange/Documents\\x/_blank)

1. 找到从你的计算机发送到gaia.cs.umass.edu HTTP服务器的HTTP GET消息。（在Wireshark窗口的“捕获数据包列表”部分（见图3和图5）中，查找显示“GET”后跟输入的gaia.cs.umass.edu URL的HTTP GET消息。选择HTTP GET消息后，数据包头部窗口将显示以太网帧、IP数据报、TCP段和HTTP消息头部信息[脚注3]。通过点击数据包详细信息窗口左侧的“+”和“-”以及右/下箭头，最小化Frame、以太网、互联网协议和传输控制协议信息的显示量。最大化HTTP协议信息的显示量。现在你的Wireshark显示应大致如图5所示。（特别注意，除了HTTP协议外，所有协议的协议信息显示量都被最小化，而HTTP协议信息的显示量被最大化）。）

[脚注3：回顾一下，发送到gaia.cs.umass.edu web服务器的HTTP GET消息包含在TCP段中，TCP段被封装在IP数据报中，IP数据报被封装在以太网帧中。如果对封装过程尚不清楚，请复习教材第1.5节。]

1. 退出Wireshark

恭喜！你已完成第一个实验！

## 提交内容

第一个实验的目标主要是让你熟悉Wireshark。以下问题将证明你已成功运行Wireshark并探索了其部分功能。根据你的Wireshark实验，回答以下问题：

1. 列出在第7步中未过滤的数据包列表窗口的“协议”列中出现的3种不同协议。
2. 从发送HTTP GET消息到接收HTTP OK回复之间花费了多长时间？（默认情况下，数据包列表窗口中的“时间”列值是以秒为单位，从Wireshark开始跟踪时算起。要以时间格式显示时间字段，选择Wireshark的“视图”下拉菜单，然后选择“时间显示格式”，再选择“时间-日期”。）
3. gaia.cs.umass.edu（也称为www-net.cs.umass.edu）的互联网地址是什么？你的计算机的互联网地址是什么？
4. 打印上述第2题中提到的两个HTTP消息（GET和OK）。为此，从Wireshark的“文件”命令菜单中选择“打印”，选择“仅选定数据包”和“按显示打印”单选按钮，然后点击“确定”。