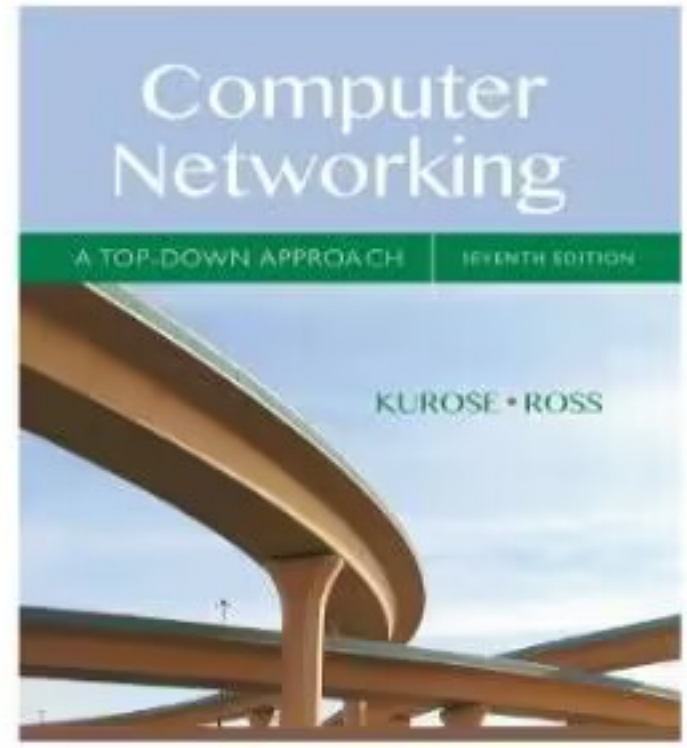
Wireshark 实验室:
入门 v7.0

《计算机网络补充:自上而下的方法》，7th ed。，
J.F.库罗斯和 K.W.罗斯

“告诉我，我忘了。告诉我，我就记得。让我参与，我就能理解。”
中国谚语



一个人对网络协议的理解，往往可以通过“看到协议在起作用”和“玩弄协议”——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，并使协议执行某些动作，然后观察这些动作及其后果。这可以在模拟场景或“真实”的网络环境(如互联网)中完成。在 Wireshark 实验室中，您将在本课程中进行操作，您将使用自己的计算机(或者您可以借用朋友:如果您没有可以安装/运行 Wireshark 的计算机，请告诉我)。你将在你的计算机中观察网络协议的“运行”，与在互联网其他地方执行的协议实体交互和交换消息。因此，你和你的计算机将成为这些“活动”实验室不可分割的一部分。你将通过实践进行观察和学习。

在第一个 Wireshark 实验中，您将熟悉 Wireshark，并进行一些简单的数据包捕获和观察。

用来观察正在执行的协议实体之间交换的消息的基本工具叫做**数据包嗅探器**。顾名思义，数据包嗅探器捕获(“嗅探”)正在从你的计算机发送/接收/接收的消息;它通常还会存储和/或显示这些捕获的消息中各种协议字段的内容。数据包嗅探器本身是被动的。它观察运行在你的计算机上的应用程序和协议发送和接收的消息，但从不自己发送数据包。同样，接收到的数据包也不会显式地指向数据包嗅探器。相反，数据包嗅探器接收的是在你的机器上执行的应用程序和协议发送/接收的数据包的*副本*。

图 1展示了一个包嗅探器的结构。图 1 的右边是通常在你的计算机上运行的协议(在本例中是互联网协议)和应用程序(例如 web 浏览器或 ftp 客户端)。图 1 中虚线矩形内所示的数据包嗅探器是计算机中常用软件的补充，由

由两部分组成。**数据包捕获库**接收计算机发送或接收的每个链路层帧的副本。回想一下本文第 1.5 节的讨论(图 1.24[1])，通过 HTTP、FTP、TCP、UDP、DNS 或 IP 等更高层协议交换的消息最终都封装在链路层帧中，这些帧通过物理介质(如以太网电缆)传输。在图 1 中，假定的物理介质是以太网，因此所有上层协议最终都封装在一个以太网帧中。因此，捕获所有链路层帧，就可以得到计算机中执行的所有协议和应用程序发送/接收的所有消息。

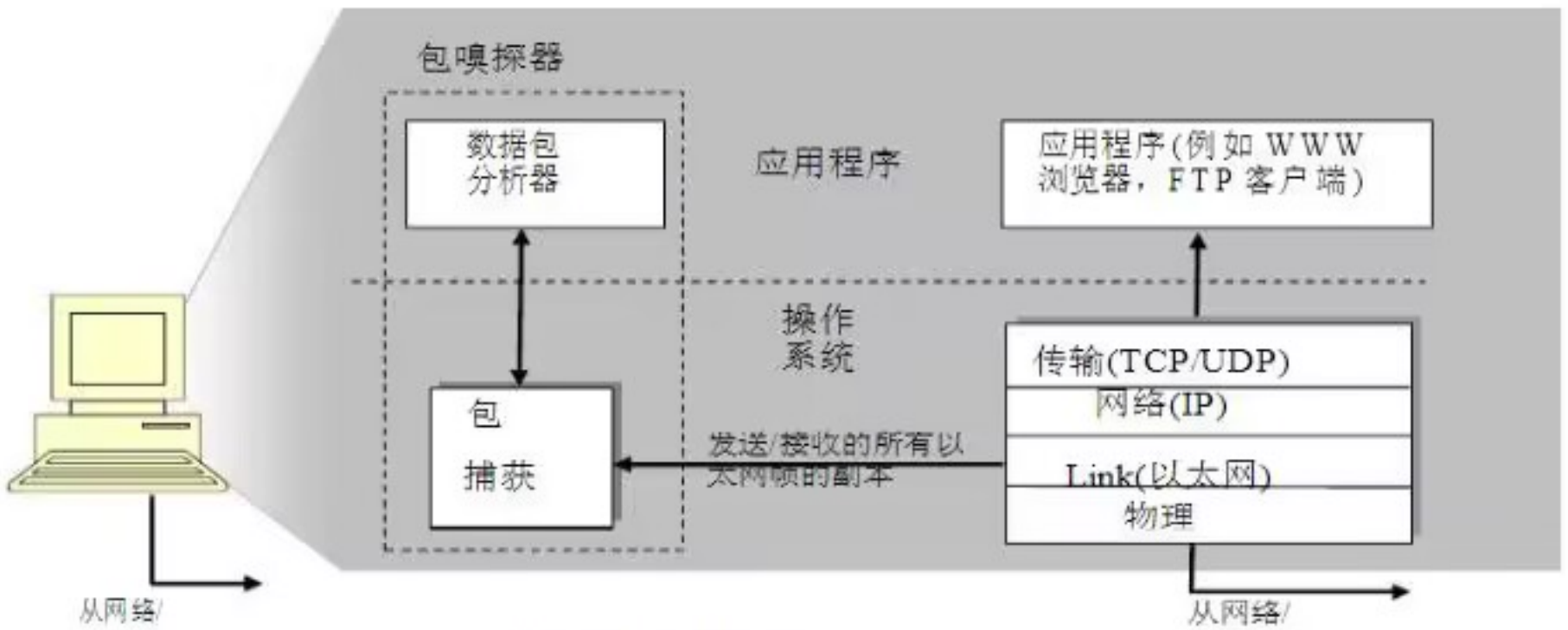


图 1:数据包嗅探器結构

包嗅探器的第二个组件是**包分析器**，它显示协议消息中所有字段的内容。为了做到这一点，包分析器必须“理解”协议交换的所有消息的结构。例如，假设我们想要显示图 1 中 HTTP 协议交换的消息中的各种字段。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 数据报格式，因此它可以提取 IP 数据报中的 TCP 段。最后，它理解 TCP 段结构，因此它可以提取包含在 TCP 段中的 HTTP 消息。最后，它理解 HTTP 协议，因此，例如，它知道 HTTP 消息的第一个字节将包含字符串“GET”、“POST”或“HEAD”，如图 2.8 中的文本所示。

我们将在这些实验中使用 Wireshark 数据包嗅探器[http://www.wireshark.org/]，使我们能够显示在协议栈的不同级别的协议发送/接收的消息的内容。(从技术上讲，Wireshark 是一个数据包分析器，它使用计算机中的数据包捕获库)。Wireshark 是一个免费的网络协议分析工具，可以运行在 Windows、Mac 和 Linux/Unix 计算机上。对于我们的实验室来说，这是一个理想的数据包分析器——它稳定，有大量的用户基础，并有良好的文档支持，包括用户指南(http://www.wireshark.org/docs/wsug_html_chunked/)，

[1] 参考图和章节是我们的 7th 版文本，*计算机网络，自上而下的方法，7th ed。， J.F. Kurose 和 K.W. Ross, Addison-Wesley/Pearson, 2016 年。*

手册页(http://www.wireshark.org/docs/man-pages/)，详细的FAQ(http://www.wireshark.org/faq.html)，丰富的功能，包括分析数百种协议的能力，以及设计良好的用户界面。它在使用以太网、串行(PPP 和 SLIP)、802.11 无线局域网和许多其他链路层技术的计算机中运行(如果它运行的操作系统允许 Wireshark 这样做)。

获取 Wireshark

为了运行 Wireshark，您需要访问一台既支持 Wireshark 又支持 *libpcap 或 WinPCap* 抓包库的计算机。如果您的操作系统中没有安装 *libpcap* 软件，则在安装 Wireshark 时将为您安装该软件。有关支持的操作系统和下载网站，请参阅
http://www.wireshark.org/download.html

下载并安装 Wireshark 软件:

- 到 http://www.wireshark.org/download.html 下载并安装 Wireshark 二进制文件。

Wireshark FAQ 有许多有用的提示和有趣的花絮信息，特别是如果您在安装或运行 Wireshark 时遇到问题。

运行 Wireshark

当你运行 Wireshark 程序时，你会得到一个启动屏幕，看起来像下面的屏幕。不同版本的 Wireshark 将有不同的启动屏幕-所以不要惊慌，如果你的不完全像下面的屏幕!Wireshark 文档指出“由于 Wireshark 运行在许多不同的平台上，有许多不同的窗口管理器，应用了不同的风格，并且使用了不同版本的底层 GUI 工具包，因此您的屏幕可能与提供的屏幕截图不同。”但由于功能上没有真正的差异，这些截图应该还是很容易理解的。”说得好。

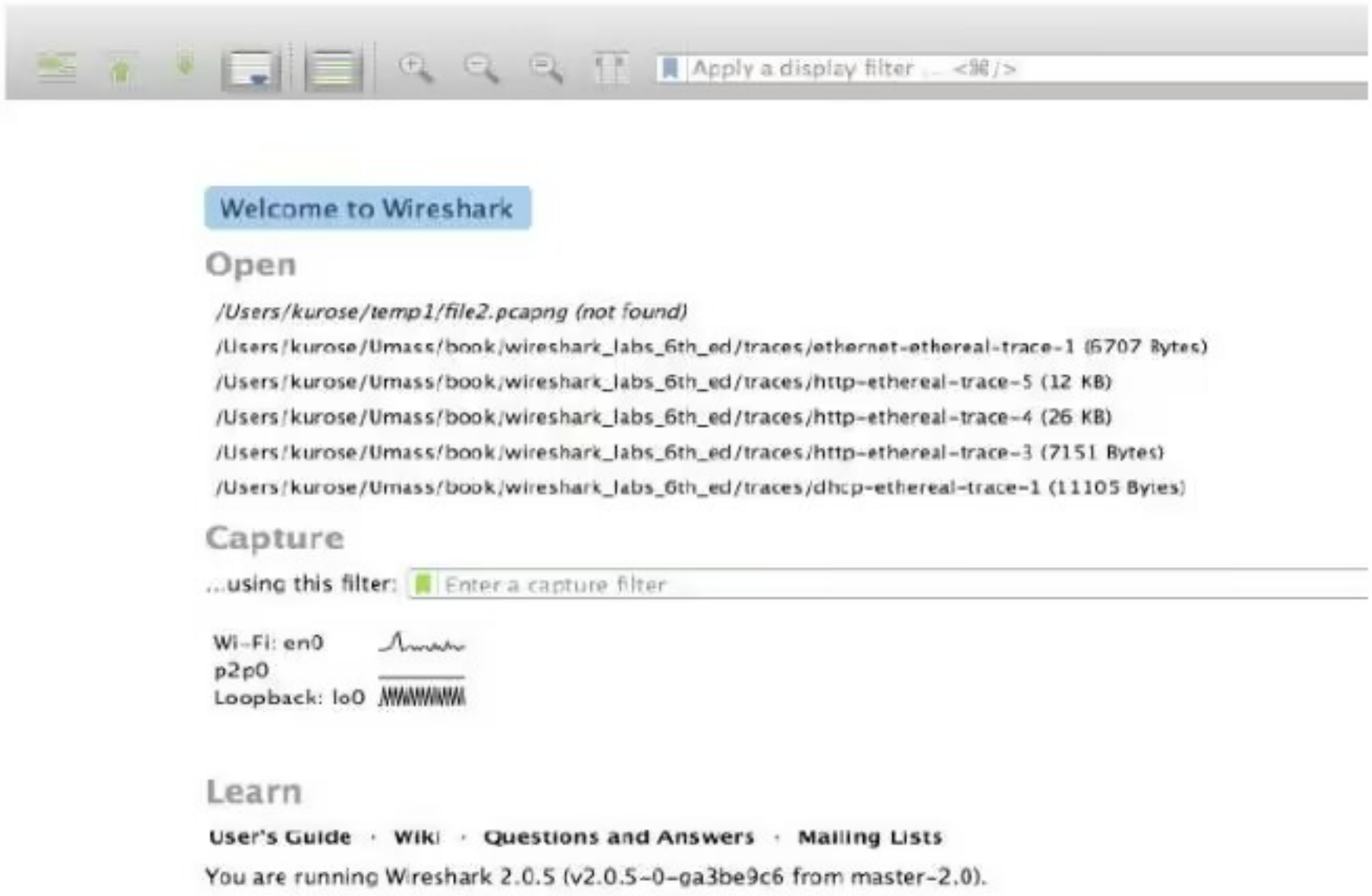


图 2:初始 Wireshark 屏幕

这个画面没什么有趣的。但请注意，在捕获部分下，有一个所谓接口的列表。我们拍摄这些屏幕截图的电脑只有一个真正的接口——“Wi-Fi en0”，这是 Wi-Fi 接入的接口。所有进出这台计算机的数据包都将通过 Wi-Fi 接口，所以我们要在这里捕获数据包。在 Mac 电脑上，双击这个界面(或在另一台电脑上找到启动页面上的接口，通过它你可以连接互联网，例如，最有可能是 WiFi 或以太网接口)，然后选择该接口。

让我们带 Wireshark 出去兜风吧!如果您单击其中一个接口开始抓包(即，Wireshark 开始抓包发送到/从该接口)，将显示如下所示的屏幕，显示被抓包的信息。一旦你开始抓包，你可以通过使用 capture 下拉菜单并选择 stop 来停止它。

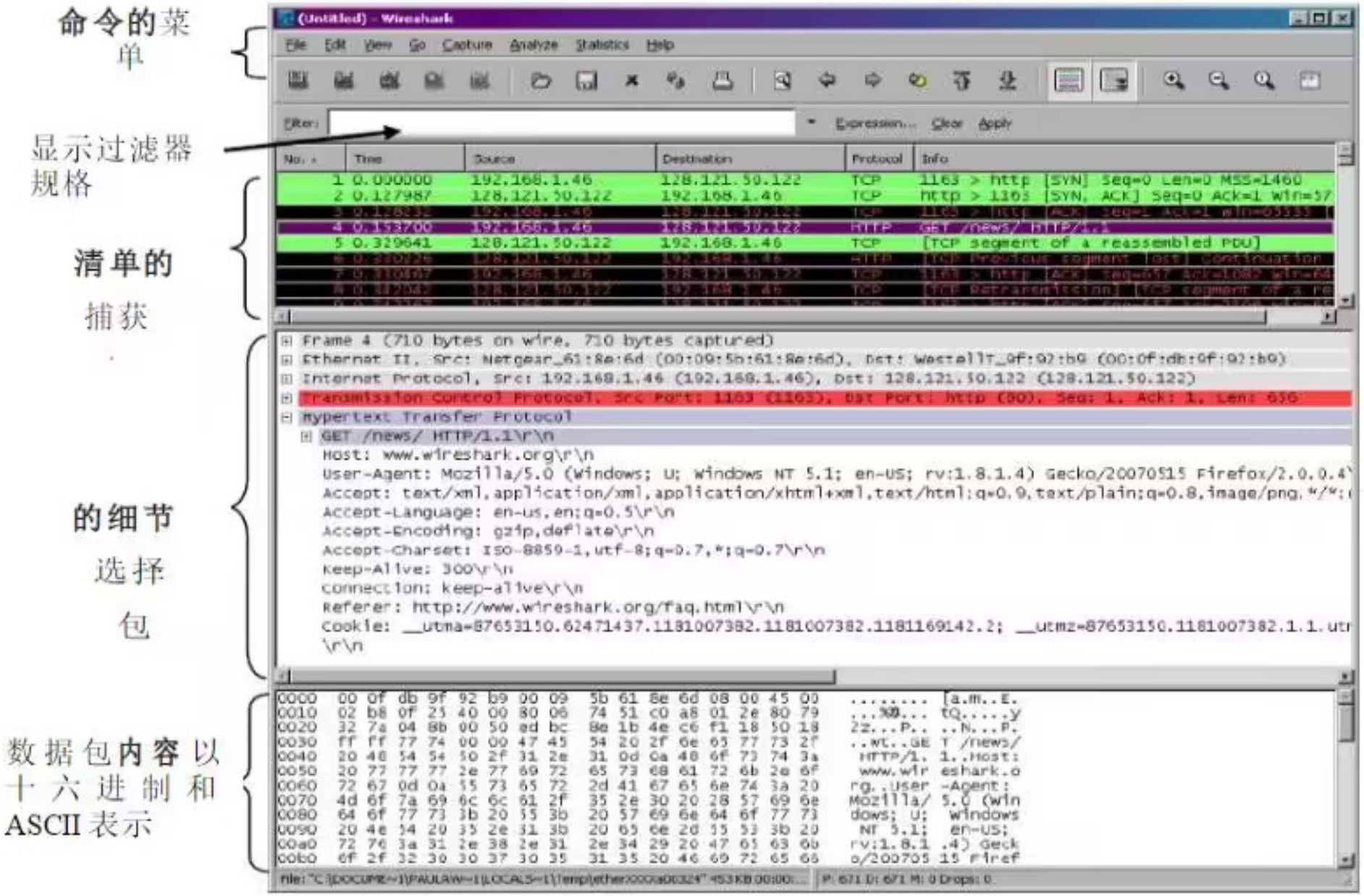


图 3: Wireshark 图形用户界面，在抓包和分析

这个看起来更有趣!Wireshark 界面主要由五个部分组成:

命令菜单是位于窗口顶部的标准下拉菜单。现在我们感兴趣的是文件和捕获菜单。在“文件”菜单中，您可以保存抓包数据或打开包含之前抓包数据的文件，并退出 Wireshark 应用程序。Capture 菜单允许你开始抓包。

- **包列表窗口**为每个捕获的包显示一行摘要，包括包号(由 Wireshark 分配;这*不是*包含在任何协议头中的包号)，包被捕获的时间，包的源地址和目的地址，协议类型，以及包中包含的特定协议信息。通过点击一个列名，可以根据这些类别中的任何一个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级别协议，即是此数据包的源或最终 sink 的协议。

- 数据包**报头详细信息窗口**提供了在数据包列表窗口中选择(高亮显示)的数据包的详细信息。(要在包列表窗口中选择一个包，将光标放在包列表窗口中包的一行摘要上，并用鼠标左键点击。)这些细节包括关于以太网帧的信息(假设数据包是通过以太网接口发送/接收的)和包含该数据包的 IP 数据报。通过单击数据包详细信息窗口中以太网帧或 IP 数据报行左侧的加减号框，可以扩展或最小化显示的以太网和 IP 层详细信息的数量。如果数据包已经通过 TCP 或 UDP 传输，则还将显示 TCP 或 UDP 的详细信息，这些详细信息可以类似地扩展或最小化。最后，还提供了发送或接收此数据包的最高级别协议的详细信息。

- **数据包内容窗口**显示捕获的帧的全部内容，包括 ASCII 和十六进制格式。

- Wireshark 图形用户界面的顶部是**包显示过滤字段**，可以在其中输入协议名称或其他信息，以便过滤在包列表窗口(以及包头和包内容窗口)中显示的信息。在下面的示例中，我们将使用包显示过滤器字段来让 Wireshark 隐藏(不显示)除了与 HTTP 消息相对应的数据包。

使用 Wireshark 进行测试

了解任何新软件的最好方法就是尝试!我们假设您的计算机通过有线以太网接口连接到互联网。实际上，我建议您在一台有有线以太网连接的计算机上做这个第一个实验，而不仅仅是无线连接。进行以下操作

1.启动你最喜欢的浏览器，它将显示你选择的主页。

2.启动 Wireshark 软件。最初你会看到一个类似于图 2 所示的窗口。Wireshark 还没有开始抓包。

3.要开始包捕获，请选择 capture 下拉菜单并选择*接口*。这将导致显示“Wireshark: Capture 接口”窗口，如图 4 所示。

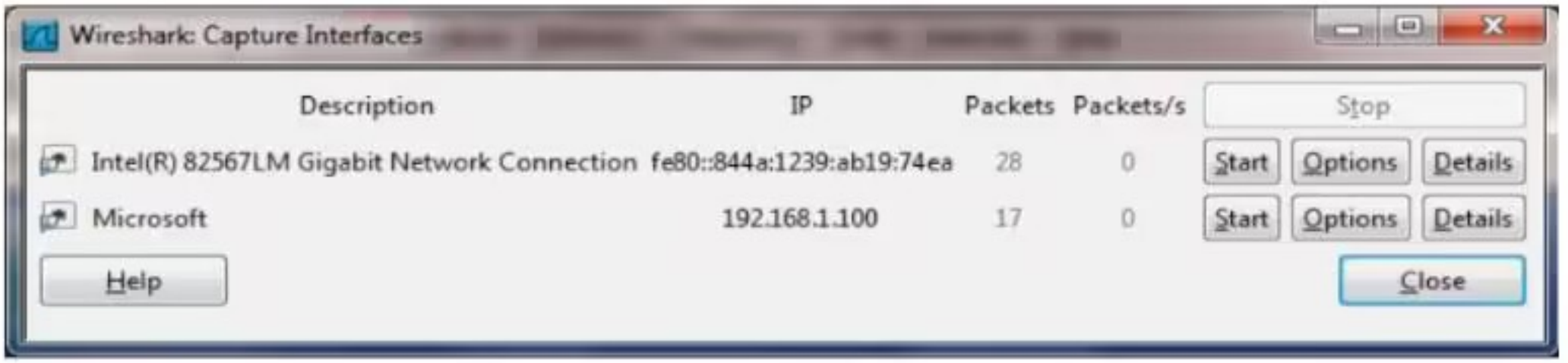


图 4: Wireshark 捕获界面窗口

4. 您将看到计算机上的接口列表，以及迄今为止在该接口上观察到的数据包数量。在你想要*开始*抓包的接口(在本例中是千兆网络连接)上单击 Start。数据包捕获现在将开始- Wireshark 现在捕获正在发送/接收来自/由您的计算机的所有数据包!

5. 开始抓包后，将出现一个类似于图 3 所示的窗口。这个窗口显示被捕获的数据包。通过选择 *Capture* 下拉菜单，*再选择 Stop*，就可以停止抓包。但先不要停止抓包。让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。让我们使用一个网络浏览器，它将使用我们将在课堂上详细学习的 HTTP 协议从网站下载内容。

6.当 Wireshark 运行时，输入 URL:

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html 并在浏览器中显示该页面。为了显示此页面，您的浏览器将与 gaia.cs.umass.edu 的 HTTP 服务器联系，并与服务器交换 HTTP 消息，以便下载此页面，如本文第 2.2 节所述。包含这些 HTTP 消息的以太网帧(以及通过以太网适配器的所有其他帧)将被 Wireshark 捕获。

7. 当浏览器显示“INTRO-wireshark-file1.html”页面(只是一行简单的祝贺)后，在 Wireshark 抓包窗口中选择“stop”，停止 Wireshark 抓包。主 Wireshark 窗口现在应该类似于图 3。你现在有了 live packet data，它包含了你的计算机和其他网络实体之间交换的所有协议消息!与 gaaia.cs.umass.edu web 服务器交换的 HTTP 消息应该出现在捕获的数据包列表中的某个位置。但是也会显示许多其他类型的数据包(参见，例如，在图 3 的协议列中显示的许多不同的*协议*类型)。即使您所采取的唯一操作是下载一个网页，显然还有许多其他协议在您的计算机上运行，用户是看不见的。随着本文的深入，我们将了解更多关于这些协议的内容!现在，你应该知道，除了“meet’s the eye”，还有很多事情要做!

8. 在 Wireshark 主窗口顶部的显示过滤器规格窗口中输入“http”(不带引号，并且用小写字母-在 Wireshark 中所有协议名称都是小写字母)。然后选择*应用*(在你输入“http”的位置右侧)。这将导致在包列表窗口中只显示 HTTP 消息。

9.查找从您的计算机发送到 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(参见图 3)中查找 HTTP GET 消息，该消息显示“GET”，后面跟着您输入的 gaia.cs.umass.edu URL。选择 HTTP GET 消息后，报头窗口[2]将显示以太网帧、IP 数据报、TCP 报文段和 HTTP 消息报头信息。通过点击信息包详细信息窗口左侧的“+”和“-”向右和向下箭头，*尽量减少*显示的帧、以太网、互联网协议和传输控制协议信息的数量。*最大限度地*显示 HTTP 协议的信息。您的 Wireshark 显示现在应该大致如图 5 所示。(特别要注意的是，除了 HTTP 之外，所有协议的协议信息量都是最小的，而在包头窗口中，HTTP 的协议信息量是最大的)。

10.退出 Wireshark

恭喜你!你现在已经完成了第一个实验室。

[2] 回想一下，发送到 gaaia.cs.umass.edu web 服务器的 HTTP GET 消息包含在 TCP 段中，该段包含(封装)在 IP 数据报中，该数据报封装在以太网帧中。如果这个封装的过程还不是很清楚，请回顾文本中的 1.5 节