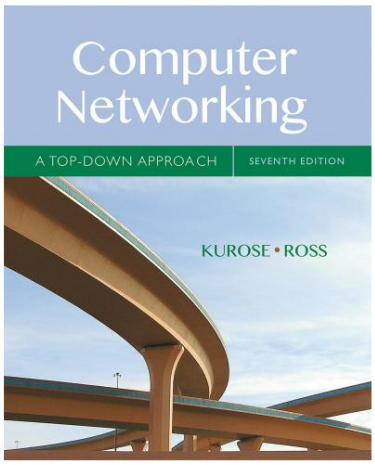
Wireshark 实验室:入门v7.0



计算机网络补充:自上而下的方法,第 7版， JF Kurose 和 KW Ross

“告诉我,我就忘了。给我看,我记得。让我参与进来,我理解。”中国谚语

一个人对网络协议的理解往往可以通过“看到协议在行动”和“玩弄协议”来大大加深 观察两个协议实体之间交换的消息顺序,深入研究协议操作的细节,并导致协议执行某些动作,然后观察这些动作及其后果。这可以在模拟场景中或在互联网等“真实”网络环境中完成。在本课程中您将进行的 Wireshark 实验室中,您将使用自己的计算机在不同的场景中运行各种网络应用程序（或者您可以借用朋友;如果您无法访问计算机,请告诉我您可以安装/运行 Wireshark）。您将观察计算机中的网络协议“运行中”,与在 Internet 其他地方执行的协议实体交互和交换消息。因此,您和您的计算机将成为这些“实时”实验室不可或缺的一部分。你会观察,你会边做边学。

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。

观察执行协议实体之间交换的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”)从您的计算机发送/接收的消息;它通常还会在这些捕获的消息中存储和/或显示各种协议字段的内容。数据包嗅探器本身是被动的。它会观察计算机上运行的应用程序和协议发送和接收的消息,但不会自行发送数据包。类似地,接收到的数据包永远不会明确寻址到数据包嗅探器。取而代之的是,数据包嗅探器会接收从您的计算机上执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 的右侧是通常在您的计算机上运行的协议（在本例中为 Internet 协议)和应用程序（例如 Web 浏览器或 ftp 客户端）。图 1 中虚线矩形内显示的数据包嗅探器是计算机中常用软件的补充,它包括

两部分。数据包捕获库接收从您的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 1.241 ），由更高层协议（如 HTTP、FTP、TCP、UDP、DNS 或 IP)交换的消息最终都封装在通过物理媒体传输的链路层帧中例如以太网电缆。在图 1 中，假设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，捕获所有链路层帧可为您提供从/由您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。

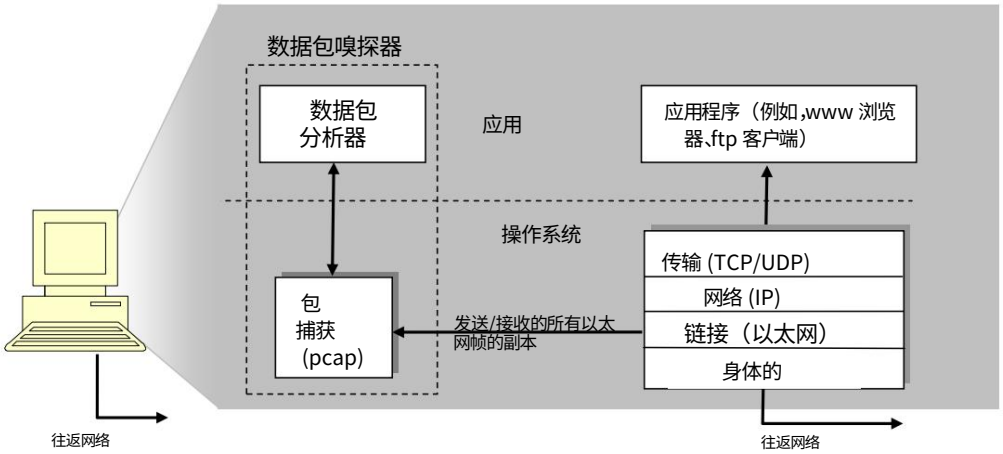


图 1:数据包嗅探器结构

数据包嗅探器的第二个组件是数据包分析器，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“了解”协议交换的所有消息的结构。例如，假设我们有兴趣在图 1 中显示由 HTTP 协议交换的消息中的各个字段。数据包分析器了解以太网帧的格式，因此可以识别以太网帧中的 IP 数据报。它还了解 IP 数据报格式，因此它可以提取 IP 数据报内的 TCP 段。

最后，它了解了 TCP 段结构，因此它可以提取 TCP 段中包含的 HTTP 消息。最后，它理解 HTTP 协议，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 所示。

我们将在这些实验中使用 Wireshark 数据包嗅探器[http://www.wireshark.org/] ，使我们能够显示协议栈不同级别的协议发送/接收的消息内容。 （从技术上讲，Wireshark 是一种数据包分析器，它在您的计算机中使用数据包捕获库）。 Wireshark 是一款免费的网络协议分析器，可在 Windows、Mac 和 Linux/Unix 计算机上运行。它是我们实验室的理想数据包分析器 它稳定、拥有庞大的用户群和有据可查的支持，其中包括用户指南(http://www.wireshark.org/docs/wsug_html_chunked/)，

[1] 对图表和章节的引用来自我们文本的第 7版，计算机网络，一种自上而下的方法，第 7版，JF Kurose 和 KW Ross，Addison-Wesley/Pearson，2016。

手册页(http://www.wireshark.org/docs/man-pages/)和详细的常见问题解答(http://www.wireshark.org/faq.html),丰富的功能包括分析数百协议和精心设计的用户界面。它在使用以太网、串行（PPP 和 SLIP）、802.11 无线 LAN 和许多其他链路层技术（如果运行它的操作系统允许 Wireshark 这样做)的计算机中运行。

获取 Wireshark

为了运行 Wireshark,您需要能够访问支持 Wireshark 和libpcap或WinPCap数据包捕获库的计算机。如果您的操作系统中未安装libpcap软件,则在安装 Wireshark 时将为您安装。有关支持的操作系统和下载站点的列表,请参见 http://www.wireshark.org/download.html

---

下载并安装 Wireshark 软件：

- 访问http://www.wireshark.org/download.html并为您的计算机下载并安装 Wireshark 二进制文件。

Wireshark 常见问题解答有许多有用的提示和有趣的信息花絮,特别是如果您在安装或运行 Wireshark 时遇到问题。

运行 Wireshark

当您运行 Wireshark 程序时,您将看到一个类似于以下屏幕的启动屏幕。不同版本的 Wireshark 会有不同的启动屏幕　所以如果您的屏幕看起来与下面的屏幕不完全一样,请不要惊慌！ Wireshark 文档指出：“由于 Wireshark 在许多不同的平台上运行,具有许多不同的窗口管理器、应用了不同的样式并且使用了不同版本的底层 GUI 工具包,因此您的屏幕可能看起来与提供的屏幕截图不同。但由于在功能上没有真正的区别,这些屏幕截图应该仍然可以很好理解。”说得好。

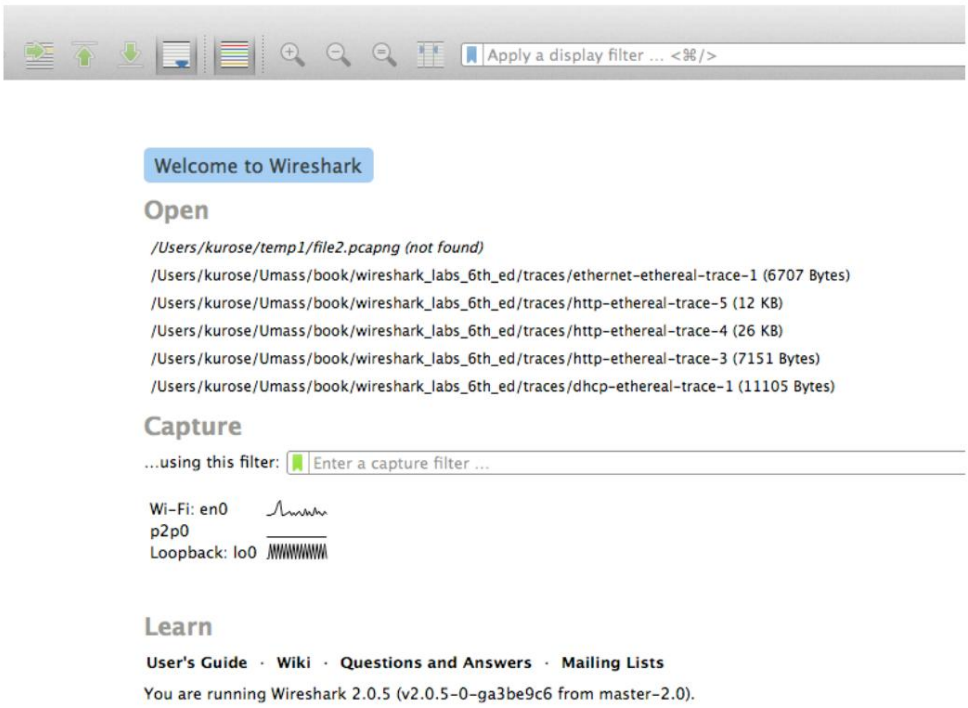


图 2:初始 Wireshark 屏幕

这个屏幕上没有太多有趣的东西。但请注意,在 Capture 部分下,有一个所谓的接口列表。我们从中截取这些屏幕截图的计算机只有一个真正的界面 “Wi-Fi en0”,它是用于 Wi-Fi 访问的界面。所有进出这台计算机的数据包都将通过 Wi-Fi 接口,因此我们要在此处捕获数据包。在 Mac 上,双击此接口(或在另一台计算机上,在启动页面上找到您正在通过其获得 Internet 连接的接口,例如,很可能是 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数据包捕获(即,Wireshark 开始捕获发送到/从该接口发送的所有数据包),将显示如下屏幕,显示有关正在捕获的数据包的信息。开始数据包捕获后,您可以使用捕获下拉菜单并选择停止来停止它。

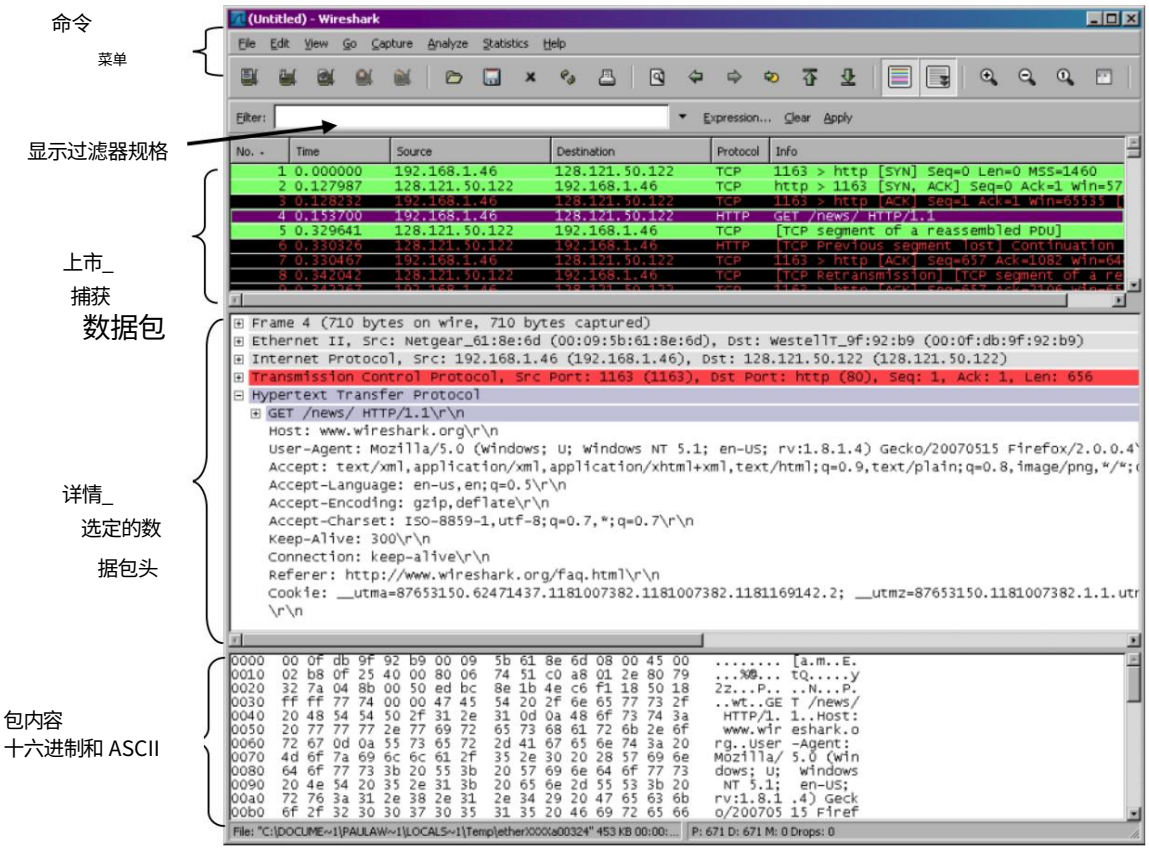


图 3： Wireshark 图形用户界面,在数据包捕获和分析期间

这看起来更有趣！ Wireshark 界面有五个主要组件：

·命令菜单是位于顶部的标准下拉菜单

窗户。我们现在感兴趣的是 File 和 Capture 菜单。 File 菜单允许您保存捕获的数据包数据或打开包含先前捕获的数据包数据的文件,并退出 Wireshark 应用程序。 Capture 菜单允许您开始数据包捕获。

·数据包列表窗口显示每个数据包的一行摘要
捕获,包括数据包编号（由 Wireshark 分配;这不是任何协议标头中包含的数据包编号）、捕获数据包的时间、数据包的源地址和目标地址、协议类型以及包含的协议特定信息在数据包中。通过单击列名,可以根据这些类别中的任何一个对数据包列表进行排序。协议类型字段列出了发送或接收此数据包的最高级别协议,即作为此数据包的源或最终接收器的协议。

·数据包头详细信息窗口提供有关在数据包列表窗口中选择（突出显示)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,请将光标放在数据包列表窗口中数据包的单行摘要上,然后单击鼠标左键。）。这些详细信息包括有关以太网帧的信息（假设数据包是通过以太网接口发送/接收的)和包含此数据包的 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。如果数据包已通过 TCP 或 UDP 传输,则还将显示 TCP 或 UDP 详细信息,可以类似地展开或最小化。最后,还提供了有关发送或接收此数据包的最高级别协议的详细信息。

· packet-contents 窗口以ASCII 和十六进制格式显示捕获帧的全部内容。

· 在 Wireshark 图形用户界面的顶部,是数据包显示过滤字段,可以在其中输入协议名称或其他信息,以过滤显示在数据包列表窗口中的信息（以及因此数据包头和数据包内容窗口）。在下面的示例中,我们将使用数据包显示过滤器字段让 Wireshark 隐藏（不显示)数据包,除了与 HTTP 消息对应的数据包。

使用 Wireshark 进行测试运行

了解任何新软件的最佳方式就是尝试一下!我们假设您的计算机通过有线以太网接口连接到 Internet。事实上,我建议您在具有有线以太网连接的计算机上进行第一个实验,而不仅仅是无线连接。请执行下列操作

1. 启动您喜欢的网络浏览器,它将显示您选择的主页。

2. 启动 Wireshark 软件。您最初将看到一个类似于图 2 所示的窗口。Wireshark 尚未开始捕获数据包。

3. 要开始数据包捕获,请选择 Capture 下拉菜单并选择Interfaces。
这将导致显示“Wireshark: Capture Interfaces”窗口,如图 4 所示。

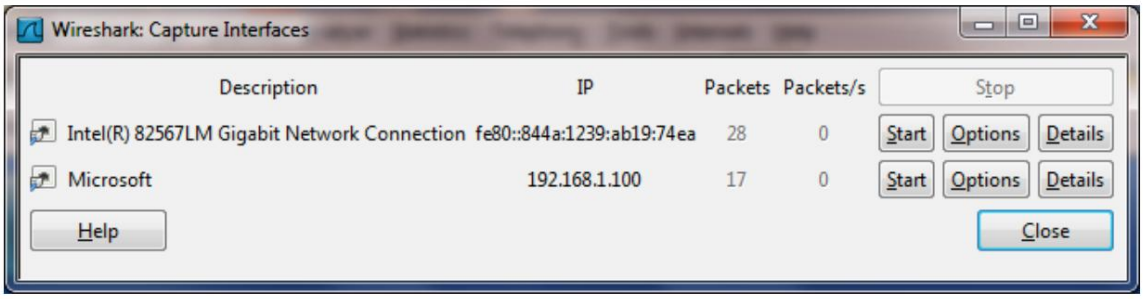


图 4： Wireshark 捕获界面窗口

4. 您将看到计算机上的接口列表以及数量
到目前为止在该接口上观察到的数据包。单击要开始数据包捕获的接口的开始（在这种情况下，千兆网络连接）。数据包捕获现在将开始 - Wireshark 现在正在捕获从您的计算机发送/接收的所有数据包！

5. 开始数据包捕获后，将出现类似于图 3 所示的窗口。此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，可以停止抓包。但不要停止数据包捕获。让我们先捕获一些有趣的数据包。为此，我们将
需要产生一些网络流量。让我们使用 Web 浏览器来执行此操作，该浏览器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. Wireshark 运行时，输入 URL：
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
并在您的浏览器中显示该页面。为了显示此页面，您的浏览器将联系 gaia.cs.umass.edu 上的 HTTP 服务器并与服务器交换 HTTP 消息以下载此页面，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. 在您的浏览器显示 INTRO-wireshark-file1.html 页面后（这是简单的一行祝贺），通过在 Wireshark 捕获窗口中选择停止来停止 Wireshark 数据包捕获。 Wireshark 主窗口现在应该类似于图 3。您现在拥有包含计算机和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。但是还会显示许多其他类型的数据包（例如，参见图 3 中协议列中显示的许多不同协议类型）。尽管您采取的唯一行动是下载网页，但显然您的计算机上运行着许多其他用户看不到的协议。随着文本的推进，我们将更多地了解这些协议！现在，您应该意识到，除了“见面”之外，还有很多事情要做！

8. 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,并且小写 - 所有协议名称在 Wireshark 中都是小写）。然后选择应用（在您输入“http”的右侧）。这将导致仅 HTTP 消息显示在数据包列表窗口中。

9. 找到从您的计算机发送到服务器的 HTTP GET 消息 gaia.cs.umass.edu HTTP 服务器。 （在 Wireshark 窗口（参见图 3)的“捕获的数据包列表”部分中查找 HTTP GET 消息,该消息显示“GET”,后跟您输入的 gaia.cs.umass.edu URL。当您选择 HTTP GET 报文、以太网帧、IP 数据报、TCP 段和 HTTP 报文头信息将显示在数据包头窗口 2中。单击“+”和“-”右箭头和下箭头

   在数据包详细信息窗口的左侧,最小化显示的帧、以太网、互联网协议和传输控制协议信息的数量。最大化显示有关 HTTP 协议的信息量。

   您的 Wireshark 显示现在应该大致如图 5 所示。（请特别注意,除了 HTTP 之外的所有协议的协议信息量最小化,而数据包头窗口中 HTTP 的协议信息量最大）。

10. 退出 Wireshark

恭喜!您现在已经完成了第一个实验。

[2] 回想一下,发送到 gaia.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 IP 数据报封装在以太网帧中。如果这个封装过程还不是很清楚,请查看文中的 1.5 节

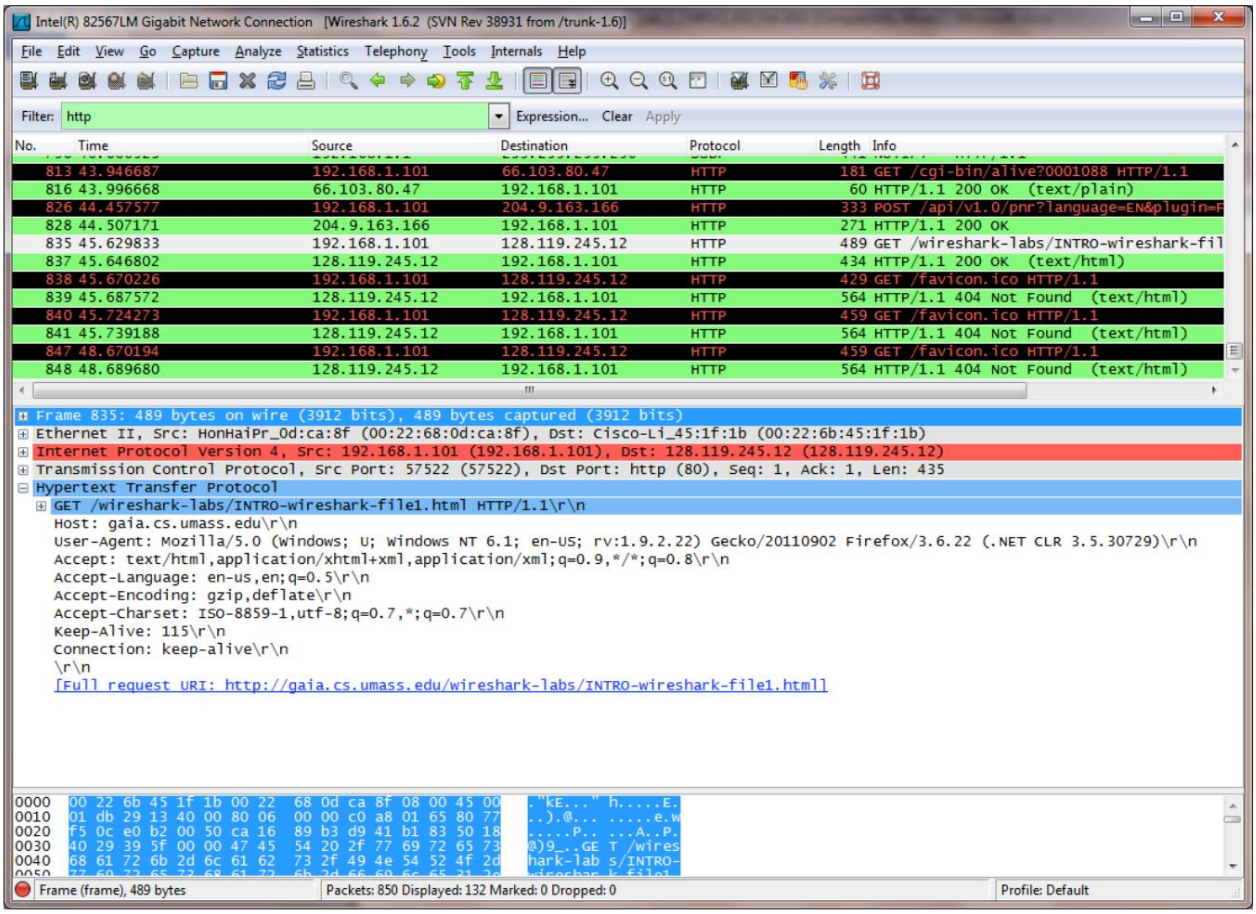


图 5:第 9 步之后的 Wireshark 窗口

交什么

第一个实验的目的主要是向您介绍 Wireshark。以下问题将证明您已经能够启动并运行 Wireshark,并探索了它的一些功能。根据您的 Wireshark 实验回答以下问题：

1.列出未过滤的协议栏中出现的3种不同的协议
上面步骤 7 中的数据包列表窗口。
2.从发送HTTP GET消息到收到HTTP OK回复需要多长时间？ （默认情况下,数据包列表窗口中时间列的值是自 Wireshark 跟踪开始以来的时间量,以秒为单位。

要以时间格式显示时间字段,请选择 Wireshark视图下拉菜单,然后选择时间显示格式,然后选择时间。）
3. gaia.cs.umass.edu（也称为www.cs.umass.edu)的网址是什么?您计算机的 Internet 地址是什么？
4. 打印上面问题 2 中提到的两条 HTTP 消息（GET 和 OK）。为此,请从 Wireshark文件命令菜单中选择打印,然后选择
“仅选择的数据包”和“按显示打印”单选按钮,然后单击确定。