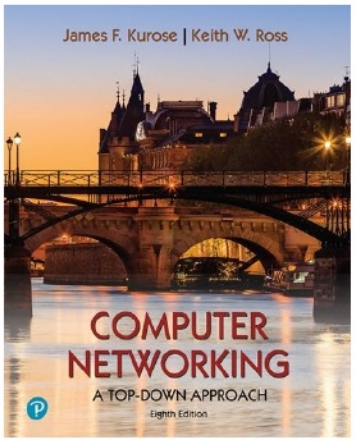
Wireshark 实验室:入门v8.1

《计算机网络:自上而下的方法》,第8版,J.F. Kurose, K.W. Ross



*"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。在本课程的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。你将在你的计算机中观察网络协议的“行动”，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浏览器或电子邮件客户端)。图1中虚线矩形内所示的数据包嗅探器是对计算机中常见软件的补充，由两部分组成。**数据包捕获库**接收你的计算机通过给定接口(链路层，如

以太网或WiFi)。回顾本文第1.5节的讨论(图1.241)，通过HTTP、FTP、TCP、UDP、DNS或IP等更高层协议交换的消息最终都被封装在链路层帧中，这些帧通过以太网电缆或802.11 WiFi无线电等物理介质传输。因此，捕获所有链路层帧就可以让您获得在计算机中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。

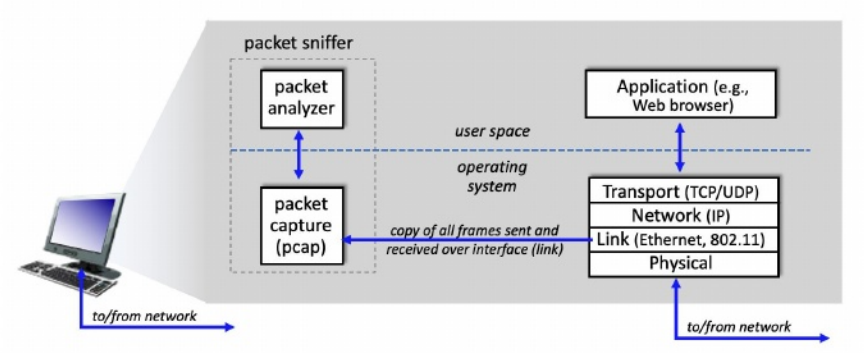


图1:数据包嗅探器结构

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/]，允许我们显示在协议栈的不同级别上的协议发送/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。此外，从技术上讲，Wireshark捕获如图1所示的链路层帧，但使用通用术语“包”来指代链路层帧、网络层数据报、传输层段和应用层消息，因此我们在这里使用不太精确的“包”术语，以符合Wireshark的惯例。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，它是一个理想的数据包分析器——它是稳定的，有大量的用户基础和良好的文档支持，包括一个用户

[1] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.* Our authors' website for this book is http://gaia.cs.umass.edu/kurose_ross You'll find lots of interesting open material there.

指南(http://www.wireshark.org/docs/wsug_html_chunked/)，手册页(http://www.wireshark.org/docs/man-pages/)，以及详细的FAQ(http://www.wireshark.org/faq.html)，丰富的功能，包括分析数百个协议的能力，以及设计良好的用户界面。它在使用以太网、串行(PPP)、802.11 (WiFi)无线局域网和许多其他链路层技术的计算机中运行。

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*包捕获库的计算机。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:

进入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，如果你的看起来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。

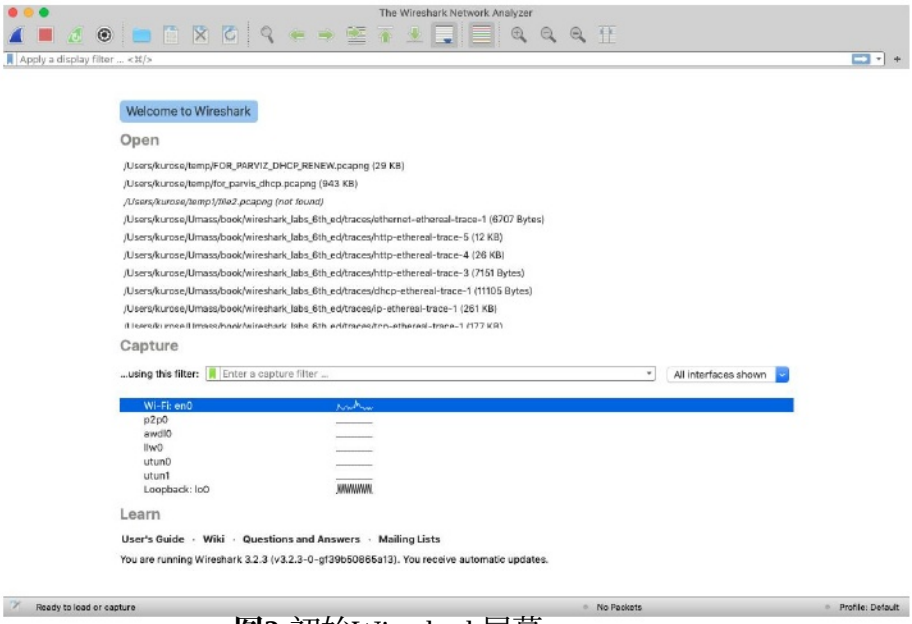


图2:初始Wireshark屏幕

这个屏幕上并没有太多有趣的东西。但请注意，在捕获部分下，有一个所谓接口的列表。我们截取这些截图的Mac电脑只有一个接口——“Wi-Fi en0”(图2中蓝色阴影部分)，这是Wi-Fi接入接口。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，双击该接口(或在另一台计算机上找到启动页面上的接口，通过该接口您可以获得互联网连接，例如，很可能是WiFi或以太网接口，并在Wireshark屏幕中选择该接口，其中指定了数据包捕获接口)。

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。一旦开始抓包，您可以使用capture下拉菜单并选择stop(或单击图2中Wireshark鳍旁边的红色方形按钮)来停止抓包

---

2 If you are unable to run Wireshark, you can still look at packet traces that were captured on one of the author’s (Jim’s) computer. You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file intro-wireshark-trace1.pcap. [If you are using an Learning Management System (LMS) to answer questions in this document, you may be instructed to open a different version of this introductory trace file). Once you’ve downloaded a trace file, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then and then selecting the *intro-wireshark-trace* trace file. The resulting display should look similar to Figures 3 and 5. (The Wireshark user interface displays just a bit differently on different operating systems, and in different versions of Wireshark).

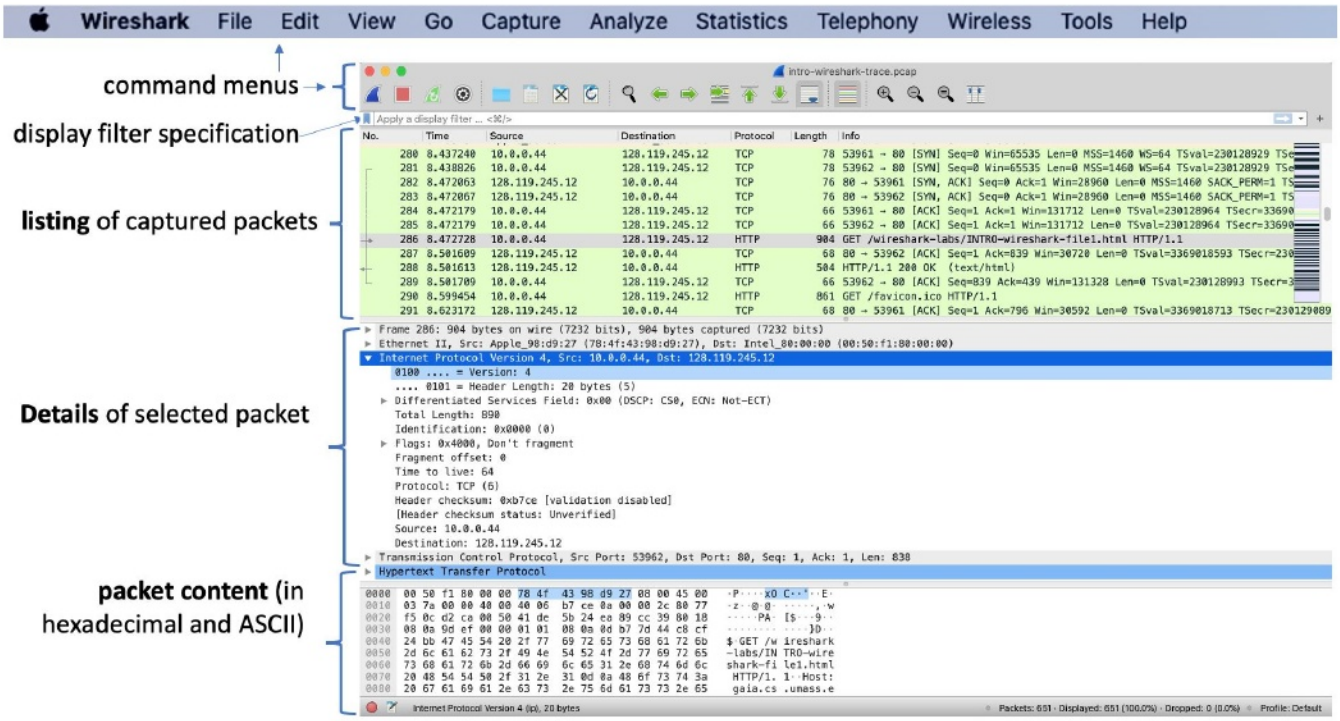


图3:捕获期间和捕获后的Wireshark窗口

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Wireshark窗口顶部的标准下拉菜单(在Mac上也位于屏幕顶部);图3中的截图来自一台Mac电脑)。我们现在感兴趣的是文件和捕获菜单。通过“文件”菜单，您可以保存抓包数据或打开包含以前抓包数据的文件，并退出Wireshark应用程序。Capture菜单允许你开始抓包。

· **包列表窗口**为捕获的每个包显示一行摘要，包括包号(由Wireshark分配;注意，这不是包含在任何协议首部中的数据包编号)，数据包被捕获的时间，数据包的源和目的IP地址，上层协议类型，以及数据包中包含的特定协议信息。通过点击某一列的名称，可以根据这些类别中的任何一类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。

☒**包头详细信息窗口**提供了在包列表窗口中选中(突出显示)的包的详细信息。(要在包列表窗口中选择数据包，将光标放在包列表窗口中数据包的一行摘要上，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数据报行左侧的正负方框或右/向下指向的三角形，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。在下面的例子中，我们将使用包显示过滤器字段来让Wireshark隐藏(而不是显示)与HTTP消息不对应的数据包。

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或无线802.11 WiFi接口连接到互联网。执行以下操作:

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*。这将显示“Wireshark: Capture接口”窗口(在PC上)，或者您可以在Mac上选择“选项”，您将看到一个接口列表，如图4a (Windows)和4b (Mac)所示。

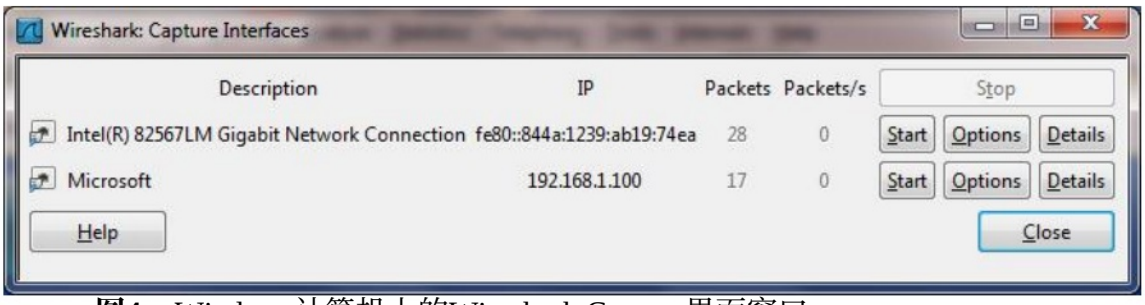


图4a: Windows计算机上的Wireshark Capture界面窗口

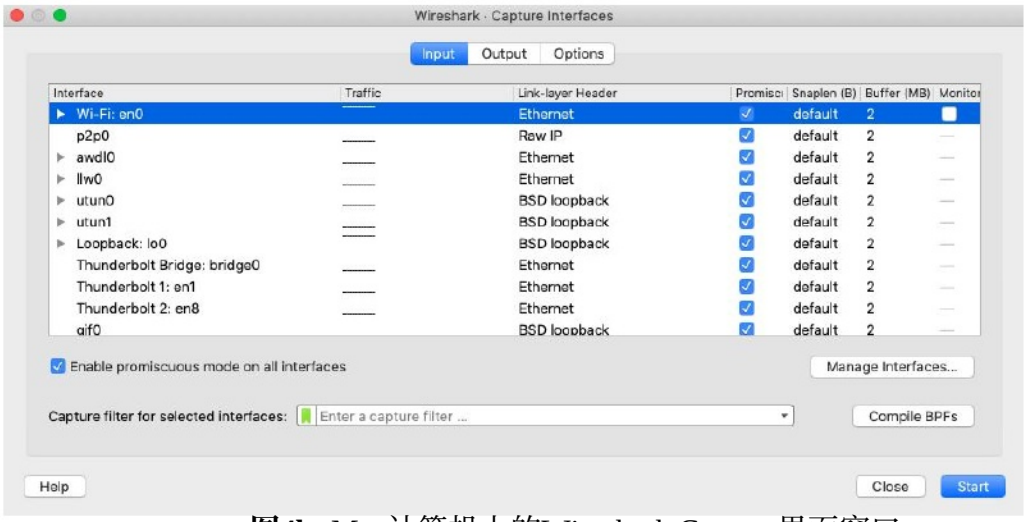


图4b: Mac计算机上的Wireshark Capture界面窗口

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。在一台Windows机器上，单击*Start*，找到您想要开始数据包捕获的接口(在图4a的情况下，是千兆网络连接)。在Windows机器上，选择界面并单击窗口底部的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*下拉菜单并选择*Stop*，或者点击红色Stop方块，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. 在Wireshark运行过程中，输入URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
并将该页面显示在浏览器中。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消息的以太网或WiFi帧(以及通过以太网或WiFi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!的

与gaaia.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，并使用小写字母- Wireshark中所有协议名称都是小写字母，并确保按下enter/return键)。然后选择*应用*(在你输入“http”的位置右侧)或者直接按回车键。这将导致在包列表窗口中只显示HTTP消息。下面的图5显示了将http过滤器应用于前面图3中所示的数据包捕获窗口后的屏幕截图。还要注意，在选定的数据包详细信息窗口中，我们选择显示在TCP段内发现的超文本传输协议应用程序消息的详细内容，这是在Ethernet II (WiFi)帧内的IPv4数据报中。关注特定消息、段、数据报和帧级别的内容可以让我们只关注我们想要查看的内容(在本例中是HTTP消息)。

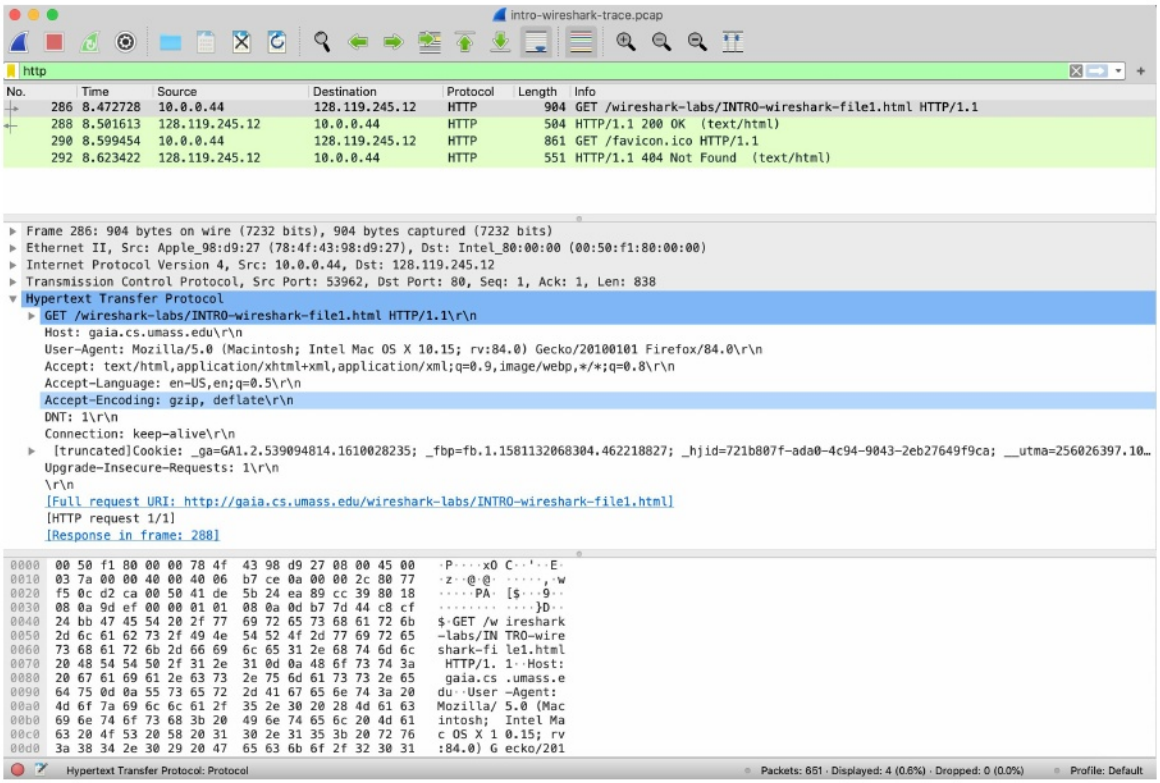


Figure 5: looking at the details of the HTTP message that contained a GET of http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

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和图5)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。当选择HTTP GET消息时，在报头窗口窗口3中将显示以太网帧、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“-”以及向右和向下指向的箭头，*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!

现在回答下面的问题。如果你把这个实验作为课堂的一部分，你的老师会详细说明如何上交作业，无论是书面的还是在学习管理系统(LMS)中如果您无法在实时网络连接上运行Wireshark或通过LMS回答问题，您可以下载在执行上述步骤时捕获的数据包跟踪文件5。

1. 在您的跟踪文件中显示以下哪一种协议(即在Wireshark“协议”列中列出):TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?
2. 从发送HTTP GET消息到收到HTTP OK应答需要多长时间?(默认情况下，数据包列表窗口中Time列的值是自Wireshark跟踪开始以来的时间(以秒为单位)。(如果您希望将“时间”字段以日显示，请选择“Wireshark*视图*”下拉菜单，然后选择“时间*显示格式*”，然后选择“*日显示时间*”。)

---

3 Recall that the HTTP GET message that is sent to the gaia.cs.umass.edu web server is contained within a TCP segment, which is contained (encapsulated) in an IP datagram, which is encapsulated in an Ethernet frame. If this process of encapsulation isn’t quite clear yet, review section 1.5 in the text

4 For the author’s class and written answers, students print out the GET and response messages and indicate where in the message they’ve found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are LMS modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

5 You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file intro-wireshark-trace1. This trace file can be used to answer these Wireshark lab questions without actually capturing packets on your own. Each trace was made using Wireshark running on one of the author’s computers, while performing the steps indicated in the Wireshark lab. Once you’ve downloaded a trace file, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the trace file name.

3. gaia.cs.umass.edu(又称www-net.cs.umass.edu)的互联网地址是什么?您的计算机或(如果您使用跟踪文件)发送HTTP GET消息的计算机的Internet地址是什么?

要回答以下两个问题，您需要选择包含HTTP GET请求的TCP数据包(提示:这是数据包号286-6)。下面这两个问题的目的是让您熟悉使用Wireshark的“选定包窗口的详细信息”;见图3。为此，单击Packet 286(您的屏幕应类似于图3)。要回答下面的第一个问题，然后查看“所选数据包的详细信息”窗口，将三角形切换为HTTP(然后您的屏幕应类似于图5);对于下面的第二个问题，您需要展开关于此数据包的传输控制协议(TCP)部分的信息。

4. 在Wireshark“所选包的详细信息”窗口(参见上面的图3)中展开有关HTTP消息的信息，以便您可以看到HTTP GET请求消息中的字段。发出HTTP请求的Web浏览器类型是什么?在扩展的HTTP消息显示中，答案显示在“User-Agent:”字段后面信息的右端。[这个字段值在HTTP消息是web服务器了解您使用的浏览器类型的方式。☒Firefox, Safari, Microsoft Internet Edge，其他
5. 在Wireshark“所选包的详细信息”窗口中展开关于该数据包的传输控制协议的信息(参见实验报告中的图3)，这样您就可以看到携带HTTP消息的TCP段中的字段。发送HTTP请求的目的端口号是什么(对于包含HTTP请求的TCP段，“Dest port:”后面的数字)?

最后…

6. 打印上面问题2中提到的两个HTTP消息(GET和OK)。在“Wireshark *文件*”命令菜单中选择“*打印*”，然后选择“打印”
“*仅选择包*”和“*按显示打印*”径向按钮，然后单击OK。

[6] Remember that this “packet number” is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header.