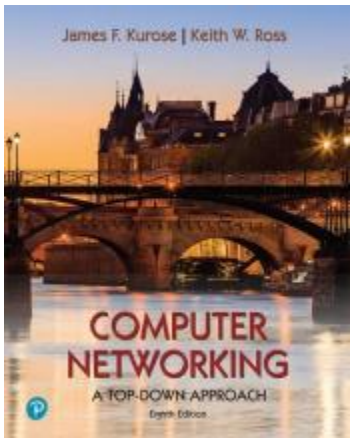
Wireshark实验室：入门指南v 8.1



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

“告诉我，我就会忘记。给我看，我就会记得。让我参与，我就会理解。”

一个人对网络协议的理解往往可以通过“看”而大大加深
“在行动中的协议”和“玩弄协议”——观察两个协议实体之间交换的消息序列，深入研究细节
协议操作，使协议执行某些操作，然后观察这些操作及其后果。这可以在模拟场景中或在
“真实”网络环境，如Internet。在本课程的Wireshark实验中，您将使用不同的场景运行各种网络应用程序
你自己的计算机。你会观察到你的计算机中的网络协议“在行动”，与互联网中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“活的”实验室的一个组成部分。
你会观察，也会通过实践来学习。

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。

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；它通常还会存储和/或显示这些捕获消息中各种协议字段的内容。数据包嗅探器本身是被动的。它观察运行在您计算机上的应用程序和协议发送和接收的消息，但自身从不发送数据包。同样，接收到的数据包也不会明确地发送给数据包嗅探器。相反，数据包嗅探器
接收应用程序和在您的计算机上运行的协议发送/接收的数据包的副本。

图1显示了数据包嗅探器的结构。图1右侧是通常在您的计算机上运行的协议（在这种情况下是Internet协议）和应用程序（如web浏览器或电子邮件客户端）。数据包嗅探器显示在虚线框内
图1中的矩形是计算机中通常软件的附加部分，由两部分组成。包捕获库接收从您的计算机通过给定接口发送或接收的每个链路层帧的副本（链路层，例如

以太网或WiFi)。回顾第1.5节中的讨论（图1.24 1　　），这是由HTTP等高层协议交换的消息　，FTP、TCP、UDP、DNS或IP最终都被封装在链路层帧中，通过链路层帧进行传输
物理介质，如以太网电缆或802.11 WiFi无线电。捕获所有链接-
因此，layer frame可以让您了解通过监控链路发送/接收的所有消息，这些消息来自/由计算机中执行的所有协议和应用程序发送/接收。

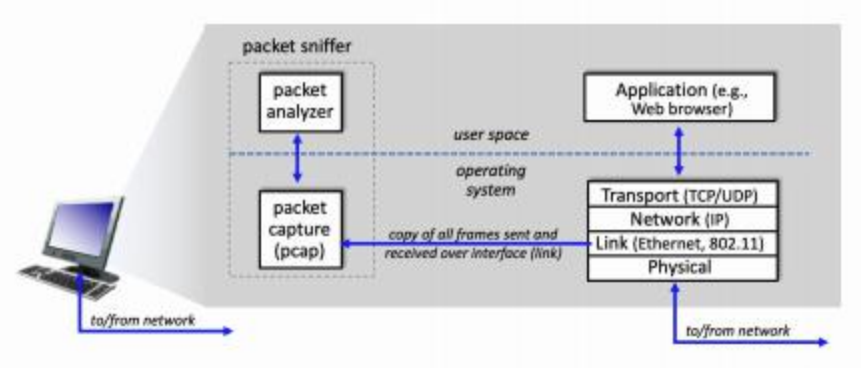


图1：数据包嗅探器结构

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。为此，包分析器
必须“理解”协议交换的所有消息的结构。例如，
假设我们对显示图1中通过HTTP协议交换的消息中的各种字段感兴趣。包分析器理解以太网的格式
框架，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，因此可以提取IP数据报中的TCP段。
最后，它理解TC P段结构，因此可以提取HTTP消息　　包含在TCP段中。最后，它理解HTTP协议，所以 为了
例如，知道HTTP消息的前几个字节将包含字符串　　如文本中的图2.8所示，可以使用GET、POST或HEAD。

我们将使用Wireshark包sniffer[http://www.wireshark.org/]为这些实验室提供服务，使我们能够显示在协议栈的不同级别上从/通过协议发送/接收的消息的内容。（从技术上讲，Wireshark是一个包
使用计算机中的包捕获库的分析器。另外，从技术上讲，如图1所示，Wireshark捕获链路层帧，但使用通用术语
“包”指的是链路层帧、网络层数据报、传输层段和应用层消息，所以我们将在这里使用不太精确的“包”一词
以及Wireshark惯例）。Wireshark是一个免费的网络协议分析器
它可以在Windows、Mac和Linux/Unix计算机上运行。它是我们的实验室的理想包分析器——它很稳定，拥有大量的用户基础，并且有很好的文档支持，包括一个用户-

1图和章节的引用均来自我们的教材《计算机网络：自上而下的方法》第8版，J.F. Kurose和K.W.Ross著，Addison- Wesley/ Pearson，2020。本书的作者网站是http://gaia.cs.umass.edu/kurose_ross　　你会在那里找到很多有趣的开放材料。

导航(http://www.wireshark.org/docs/wsug_html_chunked/)，人页
(http://www.wireshark.org/docs/man-pages/)，以及详细的常见问题解答
(http://www.wireshark.org/faq.html)，功能丰富，包括分析数百种协议的上限功能，以及精心设计的用户界面。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。

获取Wireshark

为了运行Wireshark，你需要有一台同时支持这两种功能的电脑
Wireshark和libpcap或WinPCap数据包捕获库。如果您的操作系统中没有安装
libpcap软件，当您安装Wireshark时，将为您安装libpcap软件。请参阅
http://www.wireshark.org/download.html 支持的列表
操作系统和下载站点。

下载并安装Wireshark软件：

- 。转到http:// www. wireshark. org/ download. html 下载并安装
  Wireshark二进制文件到您的计算机上。

Wireshark常见问题解答中有一些有用的提示和有趣的信息，特别是如果你在安装或运行Wireshark时遇到困难的话。

运行Wireshark

当你运行Wireshark程序时，你会看到一个启动屏幕，看起来有点像
如下面的屏幕所示。不同版本的Wireshark将具有不同的启动屏幕
-所以如果你的屏幕看起来不像下面的屏幕，不要惊慌！Wiresha rk
文档中写道：“由于Wireshark运行在许多不同的平台上
不同的窗口管理器，应用不同的样式，底层GUI工具包使用不同的版本，您的屏幕可能与提供的不同
屏幕截图。但是由于功能上没有真正的区别，这些屏幕截图应该仍然很容易理解。”说得好。

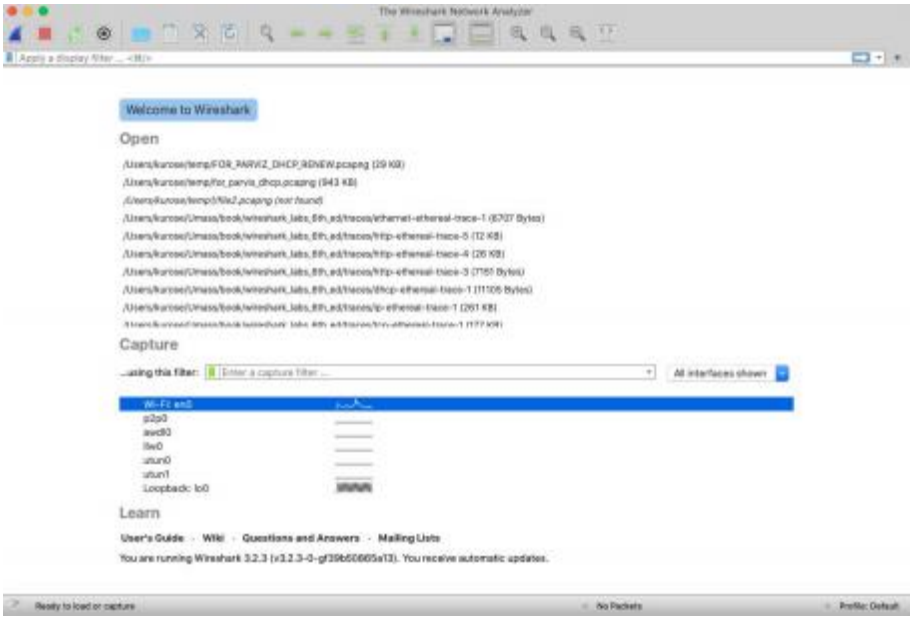


图2：初始Wireshark屏幕

这个屏幕上的内容没什么特别的。但是请注意，在“捕获”部分下面，有一个所谓的接口列表。我们正在使用的Mac电脑
屏幕截图显示只有一个接口——“Wi-Fi en0”（图2中用蓝色阴影表示），这是用于Wi-Fi访问的接口。所有进出这台计算机的数据包都会通过这个Wi-Fi接口，因此我们希望在这里捕获数据包。在Mac上，双击此接口（或在另一台计算机上，通过启动页面找到该接口）
您正在获得互联网连接，例如，很可能是WiFi或以太网
接口，并在Wireshark屏幕中选择该接口，您可以在该屏幕上指定包捕获接口）
。

让我们来试一试Wireshark！如果您单击其中一个接口以开始包捕获（即，让Wireshark开始捕获发送到/从该接口的所有包
接口），将显示一个类似于下面的屏幕，显示关于正在捕获的数据包的信息。一旦开始捕获数据包，您就可以使用以下方法停止它
捕获下拉菜单并选择停止（或点击图2中Wireshark旁边的红色方块按钮）。2

2如果您无法运行Wireshark，您仍然可以查看在作者之一（Jim）的计算机上捕获的数据包跟踪。您可以下载zip文件http://gaia. cs. umass. edu/ wireshark-
lab/wireshark-traces-8.1.zip并提取跟踪文件intro-wireshark-trace1.pcap.[如果您使用的是
学习管理系统（LMS）以回答本文档中的问题，您可能需要打开此入门跟踪文件的不同版本）。下载跟踪文件后，您可以将其加载到Wireshark中，并通过文件下拉菜单选择打开，然后依次选择intro-wireshark-trac e跟踪文件。显示结果应类似于图3和图5。（
在不同的操作系统和不同版本的Wireshark上，Wireshark用户界面的显示略有不同）。

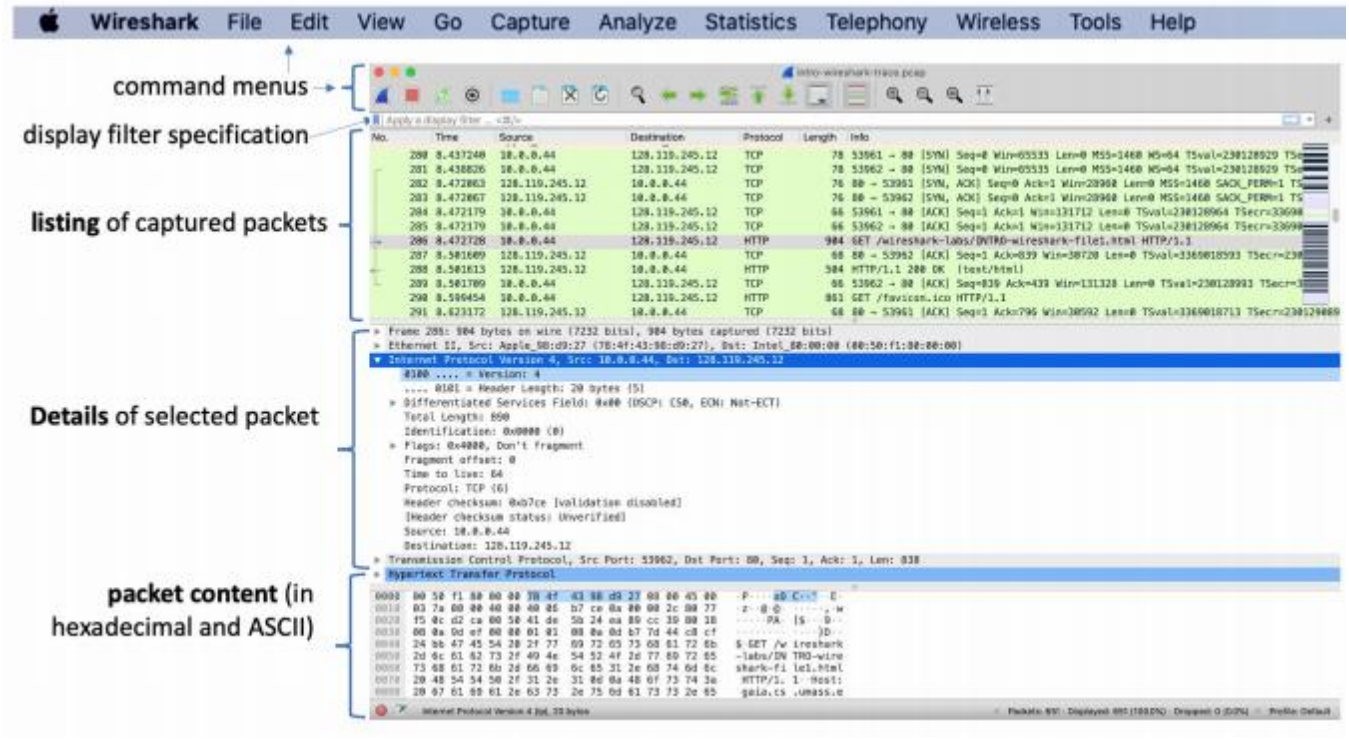


图3：Wireshark窗口，捕获期间和捕获后

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

Wireshark窗口（在Mac上位于屏幕顶部；图3中的截图来自Mac)。现在我们关注的是文件和捕获菜单。文件菜单允许您保存捕获的数据包或打开包含先前捕获的数据包的文件并退出Wireshark应用程序。捕获菜单允许您开始数据包捕获。

。数据包列表窗口显示每个捕获的数据包的一行摘要，包括数据包编号（由Wireshark分配；注意这不是任何协议的头部中包含的数据包编号）、数据包的时间
捕获，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于协议的信息。
通过单击某一列名称，可以按照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，即作为此数据包的源或最终接收方的协议。

。数据包头详细信息窗口提供了所选数据包的详细信息
（高亮显示）在数据包列表窗口中。（要在数据包列表窗口中选择一个数据包，将光标放在该数据包的一行摘要上
打开“包列表”窗口，然后用鼠标左键单击。）这些详细信息包括有关以太网帧的信息（假设该包是
通过以太网接口发送/接收）和包含该数据包的IP数据报。

可扩展或显示的以太网和IP层详细信息的数量
通过点击加减框或向右/向下指来最小化
在数据包详情窗口中，以太网帧或IP数据报行左侧的三角形。如果该数据包是通过TCP或UDP传输的，TCP或UDP的详细信息也会显示，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。

。包内容窗口显示捕获的帧的全部内容，以ASCII和十六进制格式显示。

在Wireshark图形用户界面顶部是数据包显示过滤器字段，可以在此输入协议名称或其他信息
命令过滤显示在包列表窗口（以及包头和包内容窗口）中的信息。在下面的示例中，我们将使用包显示过滤字段让Wireshark隐藏（不显示）包
与HTTP消息不对应.

对Wireshark进行测试运行

学习任何新的软件的最佳方法就是尝试它！我们假设您的计算机通过有线以太网接口或无线连接到互联网
802.11 WiFi接口。执行以下操作：

1.启动您喜欢的浏览器，它将显示您选择的主页。

2.启动Wireshark软件。您首先会看到一个类似于图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，请选择“捕获”下拉菜单并选择“接口”。这将导致显示“Wireshark：捕获接口”窗口（在PC上）或您可以在Mac上选择“选项”。您应该会看到一个接口列表，如图4a（Windows）和4b（M ac）所示。

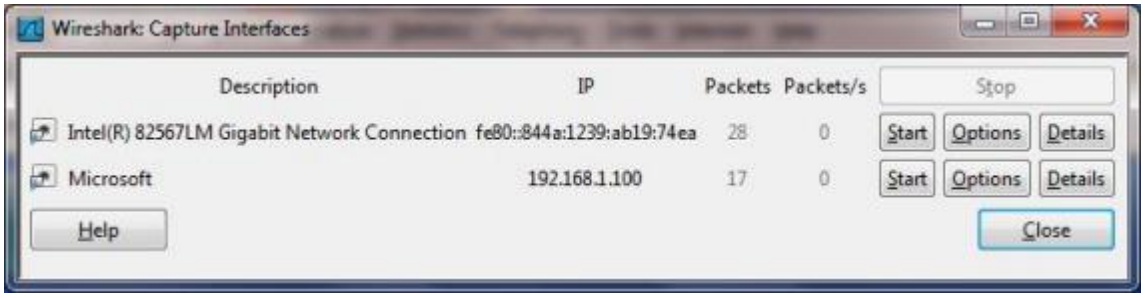


图4a：Windows计算机上的Wireshark捕获界面窗口

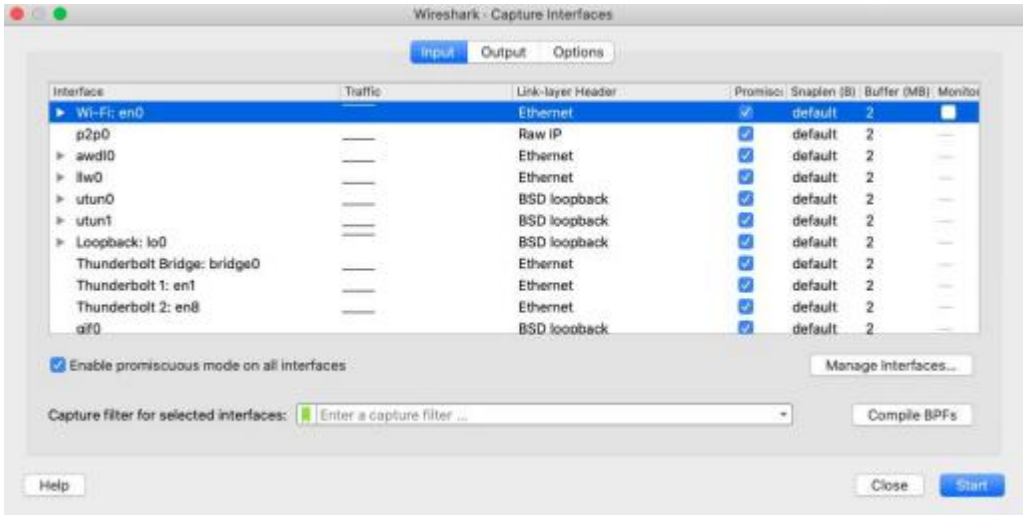


图4b：Mac电脑上的Wireshark捕获界面窗口

4.您将看到计算机上的接口列表以及接口数量

到目前为止，已在该界面上观察到了数据包。在Windows计算机上，单击“开始”以打开您要开始数据包捕获的界面（在图4a的情况下，是“千兆网络连接”）。在Windows计算机上，

选择接口，然后单击窗口底部的开始）。现在将开始包捕获- Wireshark现在正在捕获所有发送/接收的包

通过/从您的计算机！

5.一旦开始数据包捕获，将出现一个类似于图3所示的窗口。该窗口显示正在捕获的数据包。通过选择

捕获下拉菜单中选择停止，或者单击红色的停止方块，可以停止包捕获。但是先不要停止包捕获。让我们先捕获一些有趣的包。为此，我们需要生成一些网络

交通。让我们使用一个网络浏览器来实现这一点，它将使用HTTP协议 我们将在课堂上详细学习如何从网站下载内容。

6.当Wireshark正在运行时，输入URL：

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.h tml

并在浏览器中显示该页面。为了显示该页面，您需要

浏览器将联系gaia.cs.umass .edu的HTTP服务器并交换HTTP

与服务器通信以下载此页面，如第节所述

文本的2.2部分。包含这些HTTP消息的以太网或WiFi帧 （以及所有通过你的Ethern或WiFi适配器的其他帧）都将被

被Wireshark捕获。

7.在浏览器显示INTRO-wireshark-file1.html页面后（它是一个

简单的一行祝贺)，通过选择停止Wireshark数据包捕获

在Wireshark捕获窗口中停止。现在，主Wireshark窗口应该看起来类似于图3。您现在拥有包含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！

与gaia.cs.umass.edu web服务器的HTTP消息交换应显示

在捕获的数据包列表中的某个位置。但还有许多其他类型　显示为数据包看例如，图3中“协议”一栏显示的许多不同协议类型）。即使你唯一采取的行动是下载了一个网页，显然你的计算机上还有许多其他用户看不见的协议在运行。我们将了解更多关于这些协议的信息。

随着我们继续阅读本文，我们会发现其中的“协议”！目前，您应该知道，其中往往有比“表面所见”更多的事情发生！

8.键入“http“（不带引号，小写——所有协议名称在Wireshark中都是小写的，

并确保按enter/返回键）输入

在主Wireshark窗口顶部显示筛选器规格窗口。

然后选择应用（在输入“http的位置的右侧　　“)或直接点击返回。

这将导致仅在包列表窗口中显示HTTP消息下图5显示了应用http过滤器后的屏幕截图

图3中显示了前面的捕获窗口。请注意，在“已选”中

“数据包详细信息”窗口我们选择为超文本显示详细内容

在T CP段中找到的传输协议应用程序消息，

这是在以太网II（WiFi）帧中的IPv4数据报中。

在特定的消息、段、数据报和帧级别上关注内容使我们能够只关注我们想要查看的内容（在这种情况下是HTTP消息　　).

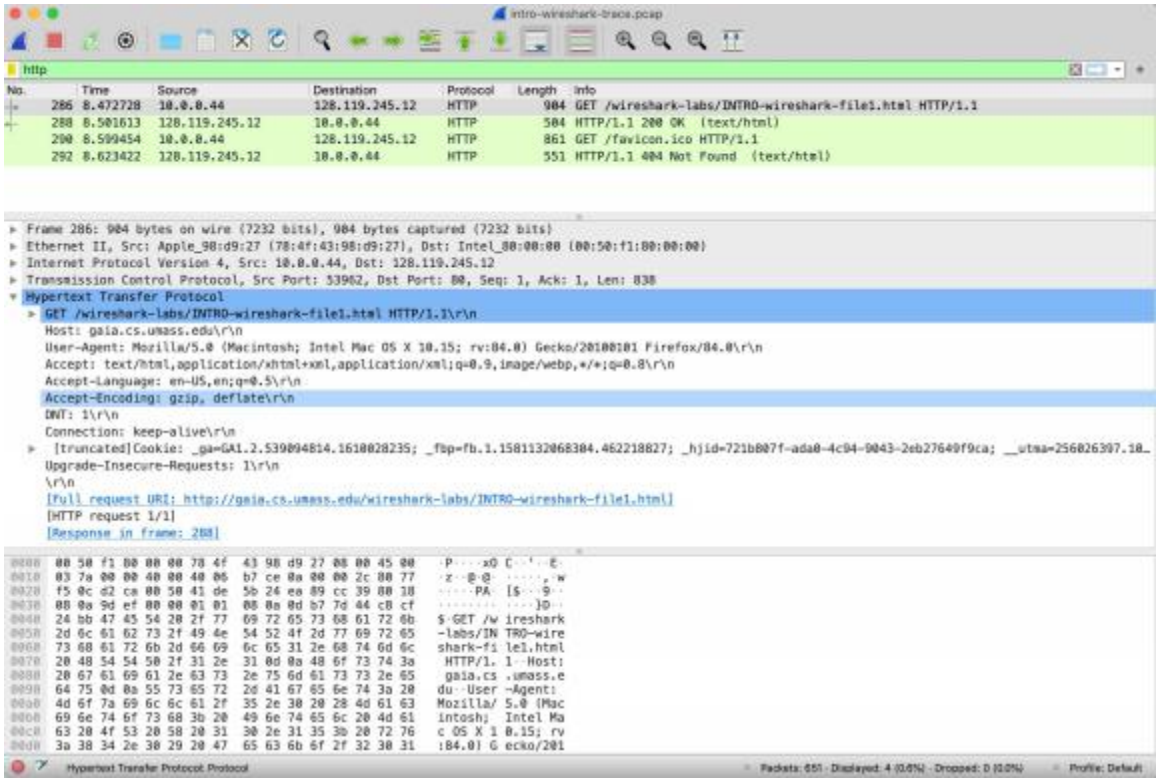


图5：查看包含GET的HTTP消息的详细信息

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1 .html

9.查找从您的计算机发送到的HTTP GET消息

gaia.cs.umass.edu HTTP服务器。(在中查找HTTP GET消息　Wireshark窗口中的“捕获的数据包列表”部分（请参见图3和图5）显示“GET”，然后是您输入的gaia.cs.umass.edu URL。当
您选择HTTP GET消息，以太网帧，IP数据报，TCP
分段，以及HTTP消息头信息将显示在数据包中-头窗口3 。通过单击“+”和“-”，以及数据包详细信息窗口左侧的向右和向下箭头，可减少帧、以太网、Internet协议和传输控制协议的量
显示的信息。最大化显示的关于
HTTP协议。现在，您的Wireshark显示应该大致如下所示
图5.（特别注意，最小化协议信息量
除HTTP以外的所有协议，以及在包头窗口中为HTTP最大化协议信息的数量).

10.退出Wireshark

恭喜！你已经完成了第一个实验！

现在回答下面的问题。如果你是作为课堂的一部分来做这个实验，你的老师将提供关于如何提交作业的详细信息，无论是书面的还是在学习管理系统（LMS）中。4　如果无法在实时网络上运行Wireshark
如果通过LMS进行连接或回答问题，您可以下载在按照上述步骤5执行时捕获的数据包跟踪文件　　.

1.下列协议中哪些显示为出现（即，列在
跟踪文件中的Wireshark“协议”列：TCP、QUIC和HTTP 、DNS、UDP、TLSv1.2？
2.从发送HTTP GET消息到HTTP完成需要多长时间　　是否收到回复？(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，以秒为单位。（如果要以时间格式显示“时间”字段，请选择“Wireshark视图”下拉菜单，然后选择“时间显示格式”，再选择“时间”。）

3回想一下，发送到gaia.cs.umass.edu web服务器的HTTP GET消息包含在以下内容中　　信息段，它包含（封装）在一个IP数据报中，而该数据报又封装在一个以太网帧中。如果这个封装过程还不太清楚，请参阅文本中的第1.5节

4对于作者的课堂和书面答案，学生打印出GET和响应消息
指出他们在消息中找到回答问题的信息的位置。他们通过以下方式做到这一点
用笔在纸质副本上做标记，或在彩色字体的文本上对电子副本进行注释。LMS模块允许教师让学生在线回答这些问题，并自动评分
这些Wireshark实验室在http://gaia.cs.umass.edu/kurose_ross/lms.htm

5您可以下载zip文件http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip 和
提取trace文件intro-wireshark-trace1。此trace文件可用于回答这些Wireshark实验室的问题
无需实际捕获数据包即可提出问题。每个跟踪记录都是使用作者的一台计算机上运行的Wireshark创建的，同时执行Wireshark实验室中指示的步骤。下载跟踪文件后，可以将其加载到Wireshark中，并通过文件下拉菜单选择打开，然后选择跟踪文件名来查看跟踪记录。

3.gaia.cs.umass.edu的互联网地址是什么(也称为www-net. cs. umass. edu)？您计算机的Internet地址是什么？或者（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：这是第286 6个数据包)。接下来的两个问题的目的是让您熟悉使用Wireshark的“选定数据包的详细信息
窗口”；参见图3。为此，请单击“包286”（屏幕应与图3类似）。然后回答下面的第一个问题，查看“选定包的详细信息”
为HTTP重新打开/关闭“数据包”窗口中的三角形（此时您的屏幕应该与图5类似）；对于下面的第二个问题，您需要扩展有关该数据包的传输控制协议（TCP）部分的信息。

4.在Wireshark中扩展HTTP消息中的信息“详细信息
选择“窗口”选项卡（参见上图3），这样您就可以看到字段了
HTTP GET请求消息。发出HTTP请求的Web浏览器是什么类型？ 答案显示在信息的右端，位于 “用户-
代理：在展开的H TTP消息显示中，“字段”.[此字段值在
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.扩展此数据包的传输控制协议信息
Wireshark“选定数据包的详细信息”窗口（见实验室中的图3 writeup)以便您可以看到携带HTTP消息的TCP段中的字段 。目标端口号是什么（“目标端口：”后面的数字
包含HTTP请求的TCP段)这是HTTP请求的接收方 送

最后...

6.打印两个HTTP消息上文问题2中提到的（GET和OK）。为此，请从
Wireshark文件“逗号”菜单中选择“打印”，然后选择
选择“仅选中数据包”和“按显示方式打印”放射状按钮，然后单击“确定”
。

6请记住，这个“数据包编号”是由Wireshark为列出目的而分配的；它并不是任何真实数据包头中的数据包编号。