网络与分布式计算

**实验课**

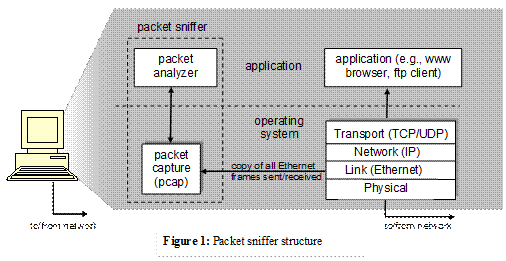
通过观察两个实体通过协议交换的消息序列，可以深入了解协议的细节，并熟练使用协议传递消息。通过反复观察这些过程，亦可大大加深对网络协议的理解。这个过程不仅可在模拟场景中完成，也可以在因特网的真实网络环境中进行。

在本实验课程中，主要通过Wireshark软件实验在不同的场景中运行各种网络应用程序并观察其所使用的网络协议，了解它们通过协议进行交互和交换信息的细节。通过这种实战动手，你不仅观察到细节，更能得到印象深刻的学习。

在第一次课的实验里，我们将熟悉Wireshark软件的操作，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包嗅探器。顾名思义，包嗅探器捕获（niffs）从计算机发送/接收/由计算机接收的消息；它还通常存储和/或显示这些捕获消息中各种协议字段的内容。包嗅探器本身是被动的。它观察计算机上运行的应用程序和协议发送和接收的消息，但从不发送数据包本身。类似地，接收到的数据包永远不会显式地发送到数据包嗅探器。相反，数据包嗅探器接收一份数据包的副本，这些数据包是由应用程序和在你的机器上执行的协议发送/接收的。

图1显示了包嗅探器的结构。图1右侧是通常在你的计算机上运行的协议（在本例中是Internet协议）和应用程序（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对你计算机中常用软件的补充，由两部分组成接收从你的计算机发送或接收的每个链路层帧的副本。回想课本（图1.24[1]）第1.5节中的讨论，高层协议（如HTTP、FTP、TCP、UDP、DNS）交换的消息，或者IP都最终封装在链路层帧中，链路层帧通过以太网电缆等物理介质传输。在图1中，假设物理介质是以太网，因此所有上层协议最终封装在以太网帧中。捕获所有链路层帧，从而为你提供发送/接收的所有消息从/通过计算机中执行的所有协议和应用程序。



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。为了这样做，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中由HTTP协议交换的消息中的各个字段感兴趣。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数据报的格式，以便提取IP数据报中的TCP段。最后，它了解TCP段的结构，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“ET”、“OST”或“EAD”，如文本中的图2.8所示。

我们将为这些实验室使用Wireshark数据包嗅探器[http://www.Wireshark.org/]，允许我们在协议栈的不同级别显示协议发送/接收/通过协议发送/接收的消息的内容。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。它是我们实验室理想的数据包分析器。它稳定，有大量的用户基础和文档支持，包括用户指南（http://www.wireshark.org/docs/wsug-html-chunked/）、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），丰富的功能包括功能分析数以百计的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无线局域网和许多其他链路层技术的计算机上运行（如果运行它的操作系统允许Wireshark这样做）。

获取Wireshark

为了运行Wireshark，你需要访问同时支持Wireshark和libpcap或WinPCap包捕获库的计算机。安装Wireshark时，如果你的操作系统中没有安装libpcap软件，则会为你安装该软件。有关支持的操作系统和下载站点的列表，请参阅http://www.Wireshark.org/download.html

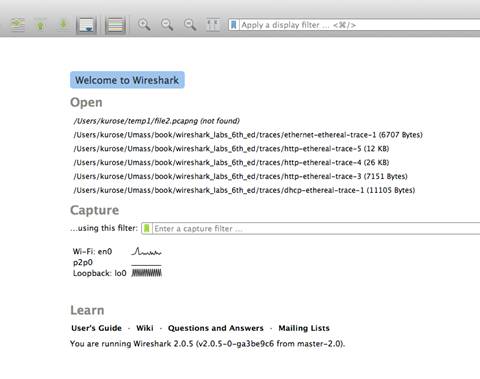
下载并安装Wireshark软件：

* 转到http://www.wireshark.org/download.html，下载并安装计算机的wireshark二进制文件。

Wireshark FAQ有很多有用的提示和有趣的信息，特别是在安装或运行Wireshark有困难时。

运行Wireshark

当你运行Wireshark程序时，你会得到一个类似下面屏幕的启动屏幕。不同版本的Wireshark会有不同的启动屏幕，所以如果你的屏幕与下面的屏幕不完全一样，就不要惊慌！Wireshark文档说明Wireshark运行在许多不同的平台上，有许多不同的窗口管理器，应用了不同的样式，使用了不同版本的底层图形用户界面工具包，你的屏幕可能与提供的屏幕截图不同。但由于这些截图在功能上没有真正的区别，所以还是可以很好地理解的。

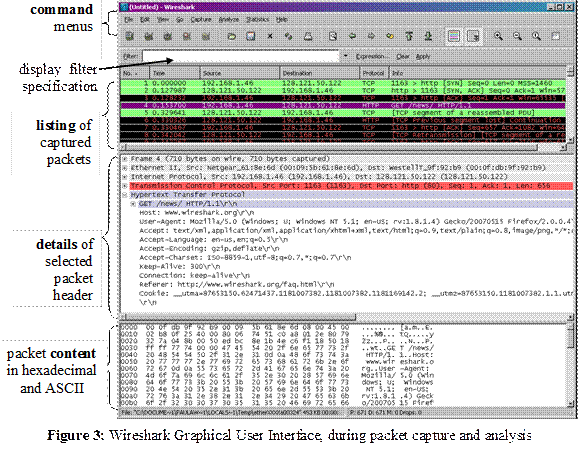


**图2：**初始Wireshark屏幕

这个屏幕上没有什么有趣的东西。但是请注意，在“捕获”部分下面，有一个所谓接口的列表。我们拍摄这些屏幕截图的计算机只有一个真正的接口，即Wi-Fi en0，它是Wi-Fi访问的接口。所有进出这台计算机的数据包都将通过Wi-Fi接口，在Mac电脑上，双击这个界面（或者在另一台电脑上，在启动页面上找到这个界面，你可以通过它获得互联网连接，例如，很可能是WiFi或以太网接口，然后选择那个界面。

让我们把线鲨带出去转一圈！如果你点击其中一个接口开始数据包捕获（即Wireshark开始捕获发送到/来自该接口的所有数据包），将显示一个类似于下面的屏幕，显示有关正在捕获的数据包的信息。——一旦你开始数据包捕获，你可以使用捕获下拉菜单并选择停止来停止它。

�



这看起来更有趣！Wireshark接口有五个主要组件：

* 命令菜单是位于窗口顶部的标准下拉菜单。我们席感兴趣的是文件和捕获菜单。文件菜单允许你保存捕获的分组数据或打开包含先前捕获的分组数据的文件，并退出WiReSARK应用程序。数据包捕获。
* 数据包列表窗口显示捕获的每个数据包的一行摘要，包括数据包编号（由Wireshark分配；这不是任何协议抯头中包含的数据包编号）、捕获数据包的时间、数据包抯源和目标地址、协议类型，以及包中包含的协议特定信息。数据包列表可以通过单击列名根据这些类别中的任何一个进行排序。–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”窗口中选定（突出显示）的数据包的详细信息，将光标放在“数据包列表”窗口中的“数据包一行摘要”上，并用鼠标左键单击。）。这些详细信息包括有关以太网帧（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数据报的信息。单击“数据包详细信息”窗口中“以太网帧”或“IP数据报”行左侧的加减框，可以扩展或最小化显示的以太网和IP层详细信息量。如果数据包已通过TCP或UDP传输，则还会显示TCP或UDP详细信息，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，是数据包显示过滤器字段，在该字段中可以输入协议名称或其他信息，以便过滤数据包列表窗口（以及数据包标题和数据包内容窗口）中显示的信息，我们使用packet display filter字段有Wireshark hide（not display）包，除了那些对应于HTTP消息的包。

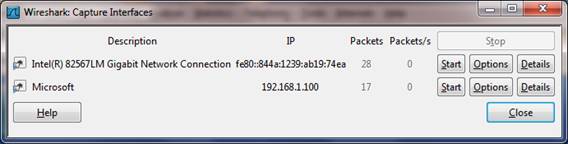
带Wireshark去试运行

学习任何新软件的最好方法就是试用它！我们假设你的计算机通过有线以太网接口连接到互联网。实际上，我建议你在一台有有线以太网连接的计算机上做第一个实验，而不仅仅是无线连接。执行以下操作

1. 启动你最喜欢的网页浏览器，它将显示你选择的主页。

1. 启动Wireshark软件。最初你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。

1. 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“ireshark:Capture接口”窗口，如图4所示。

**燜图4：**Wireshark捕获接口窗口

1. 你将看到计算机上接口的列表以及迄今为止在该接口上观察到的数据包的计数。——单击“开始”以获取要开始数据包捕获的接口（在这种情况下，是千兆网络连接）。燩acket捕获现在开始-Wireshark正在捕获从你的计算机发送/接收的所有数据包！

1. 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并选择停止，你可以停止数据包捕获。但是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，我们需要生成一些网络流量。让我们使用网络浏览器，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。

1. 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，你的浏览器将联系位于gaia.cs.umass.edu的HTTP服务器，并与服务器交换HTTP消息以下载此页，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。

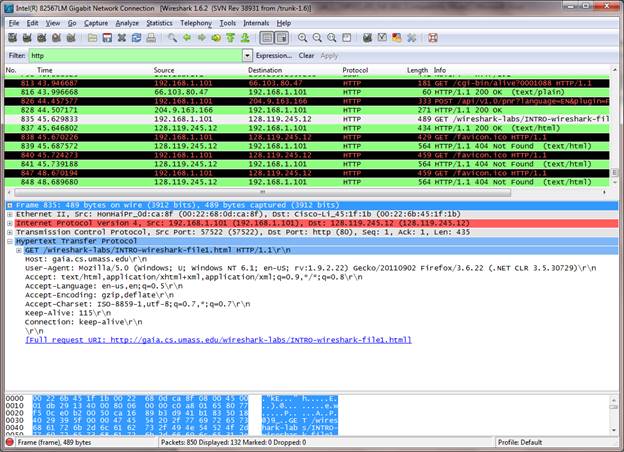
1. 在浏览器显示INTRO-wireshark-file1.html页面（这是一行简单的祝贺语）后，在wireshark捕获窗口中选择stop来停止wireshark数据包捕获。wireshark主窗口现在应该与图3类似。你现在有包含计算机和其他网络实体之间交换的所有协议消息的实时数据包数据！–与gaia.cs.umass.edu web服务器的HTTP消息交换应该出现在捕获的数据包列表中的某个位置。–但是也会显示许多其他类型的数据包（请参见，例如，图3的协议列中显示的许多不同的协议类型）。–即使你所采取的唯一操作是要下载网页，显然在你的电脑上有许多其他的协议是用户看不见的。——我们将学习更多关于这些协议，因为我们通过文本的进展！现在，你应该意识到，发生的事情往往比眼睛还多！

1. 在主Wireshark窗口顶部的“显示筛选器规范”窗口中键入“ttp”（不带引号，小写字母“所有协议名称在Wireshark中都是小写字母）然后选择“应用”（在你输入“ttp”的右侧）。这将导致在数据包列表窗口

1. 查找从计算机发送到gaia.cs.umass.edu HTTP服务器的HTTP GET消息。（在Wireshark窗口（参见图3）的“捕获包的存在”部分中查找一条HTTP GET消息，该部分显示“ET”，然后是你输入的gaia.cs.umass.edu URL。当你选择HTTP GET消息时，以太网帧、IP数据报、TCP段和HTTP消息头信息将是显示在数据包头窗口中[2]。通过单击“数据包详细信息”窗口左侧的右指和下指箭头，将显示的帧、以太网、Internet协议和传输控制协议信息量最小化。最大化HTTP协议席上显示的数量信息。你的WiReSARK显示现在应该大致上如图5所示。（特别注意，除了HTTP之外的所有协议的协议信息量最小化，以及在包头窗口中HTTP协议信息的最大量）。

1. 出口线缆

祝贺 你！你现在完成了第一个实验室。



**图5：**步骤9后的Wireshark窗口

交什么

第一个实验室的目标主要是向你介绍Wireshark。以下问题将证明你已经能够启动并运行Wireshark，并且已经探索了它的一些功能。根据你的Wireshark实验，回答以下问题：

1. 在上面的步骤7中，在未过滤包列表窗口的protocol列中列出3个不同的协议
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）。–若要以“每日时间”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“每日时间”。）
3. gaia.cs.umass.edu（也称为www.net.cs.umass.edu）的互联网地址是什么？你电脑的网址是什么？
4. 打印上面问题2中提到的两条HTTP消息（GET和OK）。要执行此操作，请从Wireshark文件命令菜单中选择“打印”，然后选择“仅选定数据包”和“打印为显示的径向”按钮，然后单击“确定”。

[[二]](" \l "_ftnref2" \o ")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，TCP段包含（封装）在IP数据报中，IP数据报封装在以太网帧中