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，可以深入理解协议的细节，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，并进行一些简单的分组捕获和观察。

观察执行协议的网络实体之间交换消息的基本工具称为包嗅探器。顾名思义，包嗅探器捕获（sniff）从计算机发送/接收的消息；且通常还存储和/或显示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，但并不发送分组。类似，接收到的分组也不会显式地发到包嗅探器，而是由包嗅探器获取一份分组的副本，原始的分组是由应用程序和在主机上执行的协议发送/接收的。

图1显示了包嗅探器的结构。其右侧是在主机上通常运行的协议（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是分组嗅探器，其由两部分组成。包嗅探器是主机中常用软件之外的一个软件，接收从主机发送或接收的每个链路层的帧的副本。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的帧中，链路层的帧通过以太网网线等物理介质传输。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。通过捕获链路层中所有的帧，提供主机上执行的所有协议和应用程序发送/接收的消息。

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。分组分析器理解以太网帧的格式，从而可以识别以太网帧中的IP数据报。进而因为包分析器还理解IP数据报的格式，其能够提取IP数据报中的TCP段。其后还因它理解TCP段的结构，从而可以提取包含在TCP段中的HTTP消息。最后因其理解HTTP协议，因此知道HTTP消息的第一个字节将包含字符串“GET”、“POST”或“HEAD”，如课本中的图2.8所示。

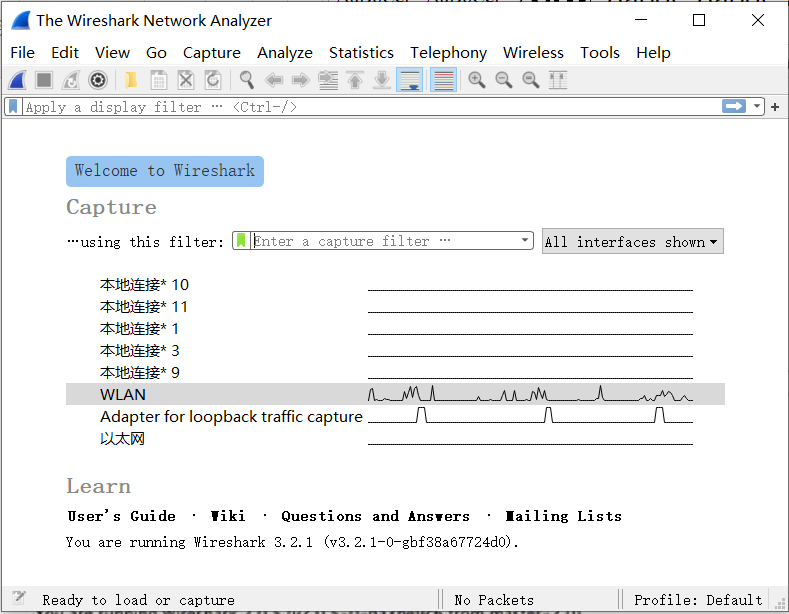
这些实验我们使用Wireshark包嗅探器[http://www.Wireshark.org/]，在协议栈的不同级别显示协议发送/接收的消息的内容。Wireshark是一个开源的网络协议分析器，具有跨平台的能力，可以运行在Windows、Mac和Linux/Unix等不通过平台的计算机上。网上有大量的社区文档支持，包括用户指南（http://www.wireshark.org/docs/wsug-html-chunked/）、手册页（http://www.wireshark.org/docs/man-pages/）和详细的常见问题解答（http://www.wireshark.org/FAQ.html），丰富的功能包括可以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）。

**安装Wireshark**

运行Wireshark需要下载支持Wireshark的libpcap或WinPCap包捕获库。安装Wireshark时，如果你的操作系统中没有安装libpcap软件，则会自动安装该软件。其支持的操作系统参阅http://www.Wireshark.org/download.html，请在该站点下载并安装wireshark二进制执行文件。也可从github上下载其源代码自己编译生成，详细参见https://github.com/network-distributed/wireshark。

**运行Wireshark**

当你运行Wireshark程序后，你会看到一个类似下面屏幕的启动屏幕。



**图2：**Wireshark启动屏幕

请注意，在“捕获”部分下面，有一个所谓接口的列表。上面这个屏幕截图的计算机只有一个真正的接口，即WLAN，它是Wi-Fi访问的接口。所有进出这台计算机的分组都将通过WLAN接口，在电脑上，双击这个界面可以获得互联网连接，例如，很可能是WiFi或以太网接口，然后选择那个界面。

下面我们把wireShark拉出来溜溜！如果你点击其中一个接口开始分组捕获（即Wireshark开始捕获发送到/来自该接口的所有分组），将显示一个类似于下面的屏幕，显示有关正在捕获的分组的信息。——一旦你开始分组捕获，你可以使用捕获下拉菜单并选择停止来停止它。



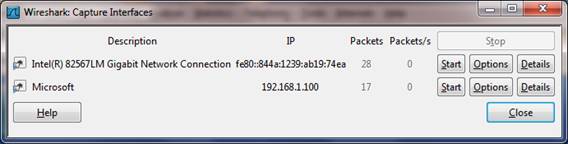
Wireshark接口有五个主要组件：

* 命令菜单是位于窗口顶部的标准下拉菜单。用的最多的是文件和捕获菜单。文件菜单允许你启动分组捕获，保存捕获的分组数据或打开先前捕获的分组数据文件，也可以退出wireShark应用程序。
* 分组列表窗口显示捕获的每个分组的一行摘要，包括分组编号（由Wireshark分配；这不是任何协议抯头中包含的分组编号）、捕获分组的时间、分组抯源和目标地址、协议类型，以及包中包含的协议特定信息。分组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分组的最高级别协议，即，作为此分组的源或最终接收器的协议。
* “分组头详细信息”窗口提供有关在“分组列表”窗口中选定（突出显示）的分组的详细信息，将光标放在“分组列表”窗口中的“分组一行摘要”上，并用鼠标左键单击。）。这些详细信息包括有关以太网帧（假设分组是通过以太网接口发送/接收的）和包含此分组的IP数据报的信息。单击“分组详细信息”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。如果分组已通过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分组的最高级别协议的详细信息。
* “分组内容”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，是分组显示过滤器字段，在该字段中可以输入协议名称或其他信息，以便过滤分组列表窗口（以及分组标题和分组内容窗口）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。

**试运行Wireshark**

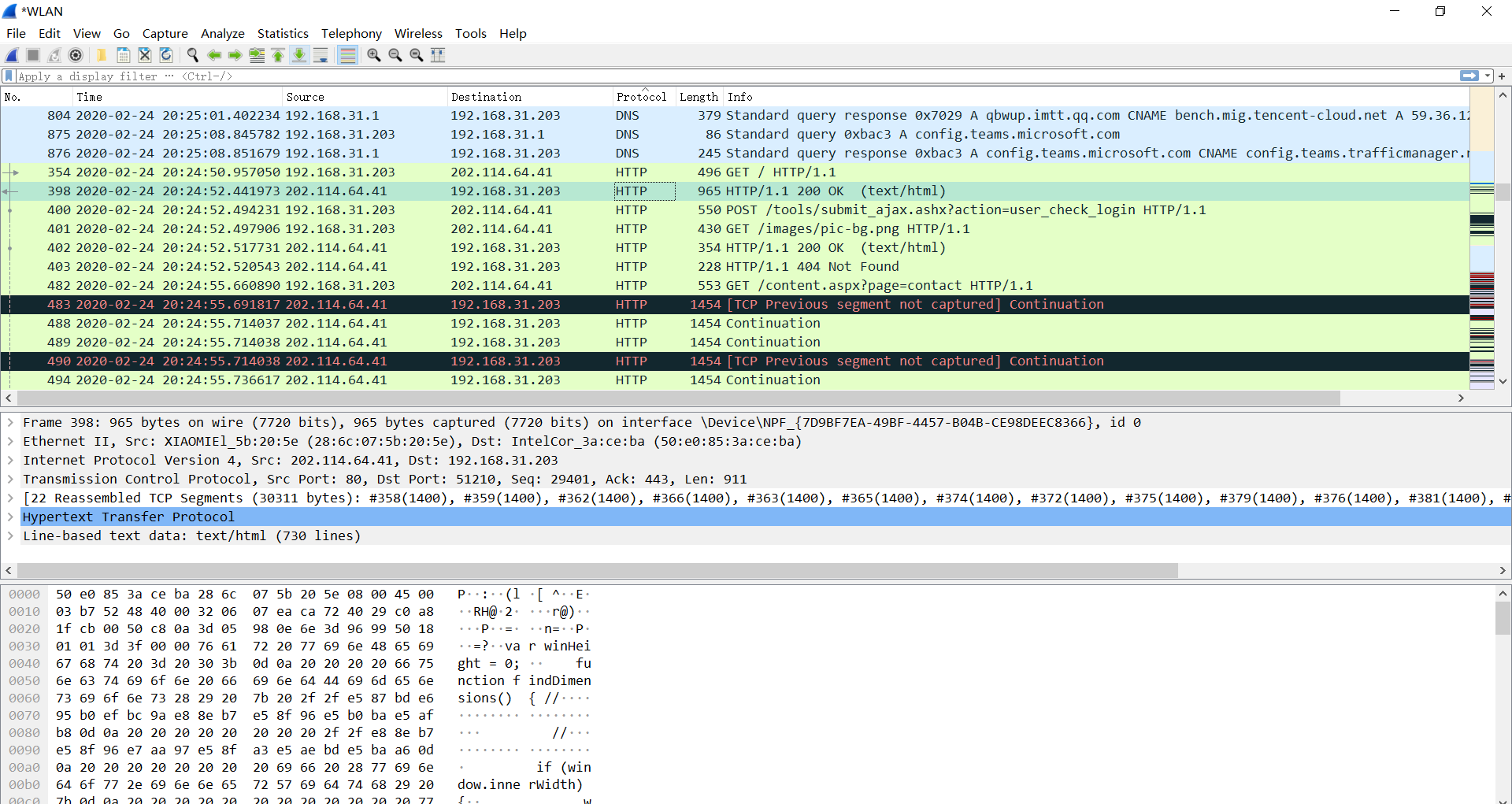
学习任何新软件的最好方法就是试用它！我们假设主机通过有线以太网接口连接到互联网。执行以下操作

1. 启动你网页浏览器，输入你欲访问的主页地址。
2. 启动Wireshark软件。最初你将看到一个类似于图2所示的窗口。Wireshark尚未开始捕获分组。
3. 要开始分组捕获，请选择捕获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捕获接口窗口

1. 你将看到计算机网络接口的列表以及迄今为止在该接口上观察到的分组的计数。——单击“开始”以获取要开始分组捕获的接口，并开始捕获从主机发送/接收的所有分组！
2. 一旦开始分组捕获，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分组。通过选择捕获下拉菜单并选择停止，你可以停止分组捕获。但是不要停止分组捕获。让我们先捕获一些有趣的分组。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。
3. Wireshark运行后，在浏览器地址栏中输入http://cs.whu.edu.cn/显示该页面。为了显示此页浏览器连接了位于cs.whu.edu.cn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。
4. 在浏览器显示http://cs.whu.edu.cn/index.aspx页面后，在wireshark捕获窗口中选择stop来停止wireshark分组捕获。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分组数据！–与cs.whu.edu.cn web服务器的HTTP消息交换应该出现在捕获的分组列表中的某个位置。–但是也会显示许多其他类型的分组（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。随着理论课教学的进展，后续教学将学习更多关于这些协议。现在，你应该意识到，发生的事情往往比眼睛看到的多得多！
5. 在Wireshark主窗口顶部的“显示筛选规则”窗口中键入“http”（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“http”的右侧）。这将导致分组列表窗口中只显示http消息。
6. 查找从主机发送到cs.whu.edu.cn 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“GET”，然后是你输入的cs.whu.edu.cn 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分组头窗口中[2]。通过单击“分组详细信息”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。现在WireShark显示应该大致上如图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）。
7. 退出wireShark

至此，完成了第一个实验。



**图5：**步骤9后的Wireshark窗口

**实验报告提交内容**

第一次实验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. 观察上面第7个步骤，在未过滤包窗口的protocol列中标出3个不同协议
2. 从发送HTTP GET消息到收到HTTP OK回复需要多长时间？（默认时“分组列表”窗口中“时间”列的值是自Wireshark跟踪开始以来的时间量是以秒为单位。若要以“每日时间”格式显示“时间”字段，请在下拉菜单的view中将“时间显示格式”设置为“每日时间”。）
3. cs.whu.edu.cn的互联网ip地址是什么？你电脑的ip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“仅选定分组”打印到pdf文件，然后单击“确定”。

回想一下，发送到cs.whu.edu.cn 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