Wireshark 入门

1 Wireshark 发展历史

1997 年底，Gerald Combs 需要一个能够追踪网络流量的工具软件作为其工作上的辅助，因此他开始撰写 Ethereal 软件，并在 1998 年 7 月发布其第一个版本 v0.2.0。自此之后，Combs 收到了来自全世界的补丁、错误回报与鼓励信件，Ethereal 的发展就此开始。

2006 年 5 月，Combs 因加入了一家新公司，不得不放弃原来的 Ethereal 商标，他随后创建了 Wireshark 网络协议分析器以继承 Ethereal。

2 数据包嗅探器简介

图 1 显示了数据包嗅探器的结构。在图中右边显示的是 Internet 协议和应用程序（如 Web 浏览器或 FTP 客户端）。在图中左边虚线方框中显示的是数据包嗅探器，它包含两个部分：数据包捕获函数库（packet capture library）和数据包分析器（packet analyzer）。前者接收你的电脑收发的每个链路层帧的一份拷贝，由于所有上层协议（包括 HTTP、FTP、TCP、UDP、DNS 或 IP 等）交换的信息最终都会封装进链路层的帧中，这就意味着只要捕获所有链路层的帧，你就能获得你的电脑中执行的应用程序以及所有协议收发的消息。

数据包分析器显示一个协议消息中所有字段的内容。为了做到这一点，数据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 HTTP 协议交换的消息中的字段内容感兴趣，数据包分析器首先需要理解以太网帧格式，这样它才能识别以太网帧中的 IP 报文；然后它还需要理解 IP 报文格式，这样它才能提取 IP 报文中的 TCP 段；最后它需要理解 HTTP 协议。

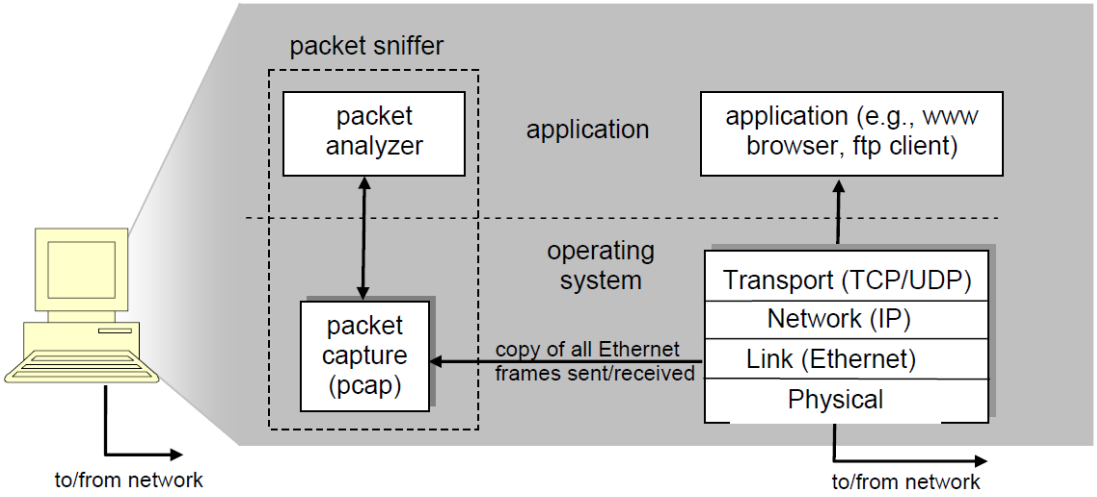


图 1 数据包嗅探器结构

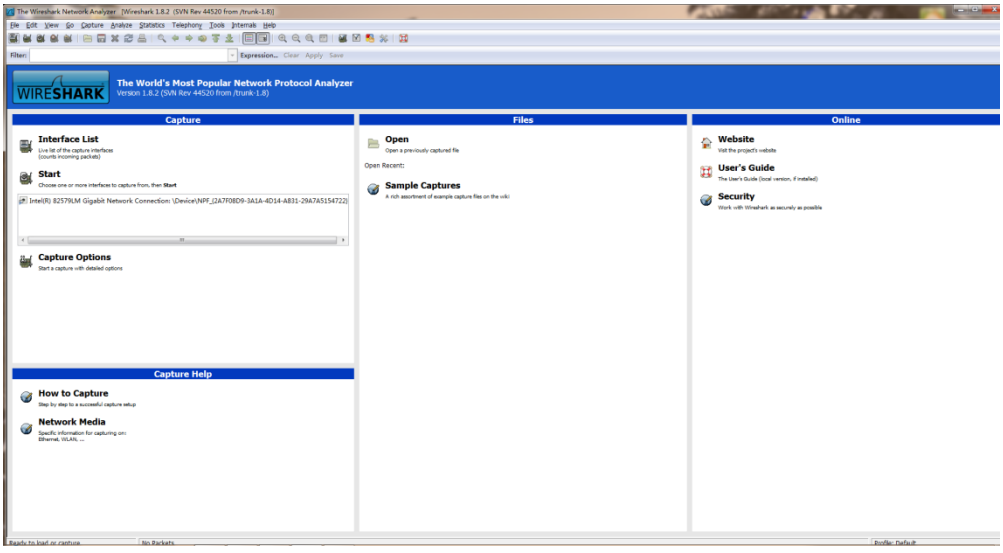
从技术上来说，Wireshark 就是一个调用了电脑中数据包捕获函数库的数据包分析器。

3 获取 Wireshark

通过网址 http://www.wireshark.org/download.html 下载并安装 Wireshark 软件，你也可以通过该网址下载 Wireshark 的用户手册。

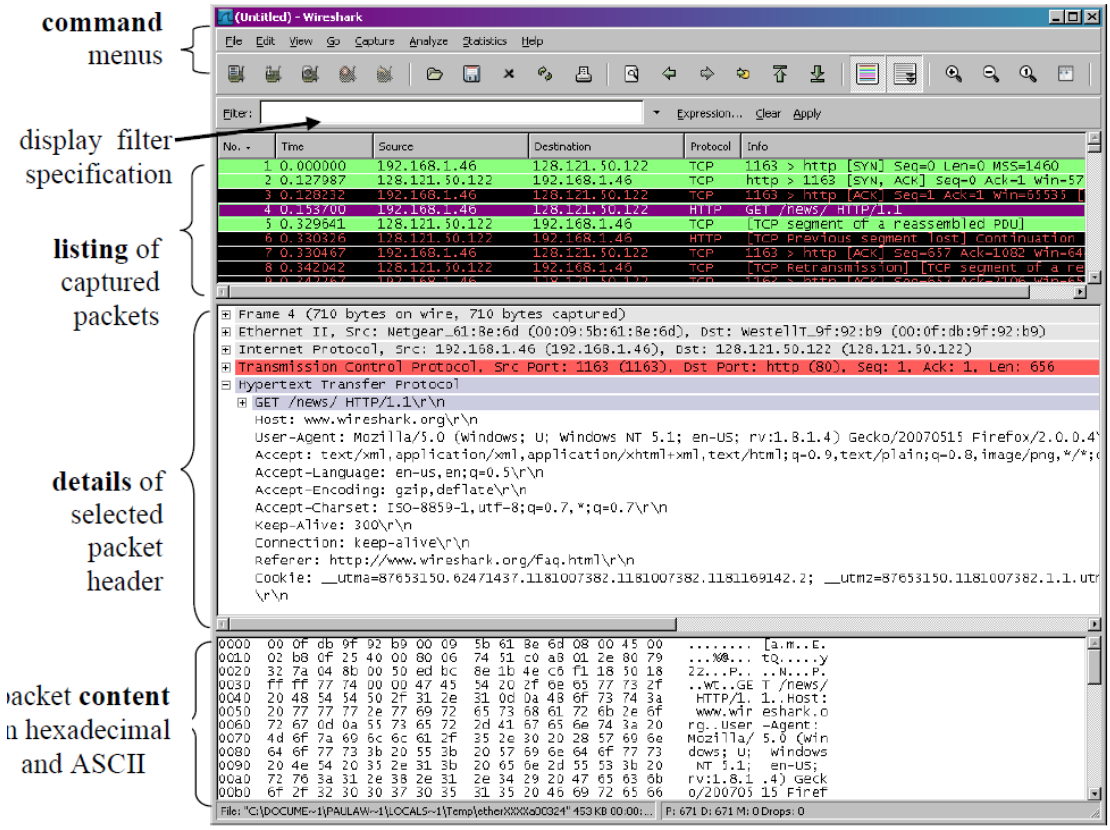
4 运行 Wireshark

运行 Wireshark，你首先会看到如图 2 所示的界面。



2 Wireshark 启动界面

选择好网络接口并点击“Capture”→“Start”开始捕获报文，你将看到如图 3 所示的界面。



3 Wireshark 捕获报文界面

图 3 的 Wireshark 界面由五个主要部分构成：

- **命令菜单（command menus）**：它是位于窗口最上面的标准下拉式菜单。我们常用的是 File 和 Capture 菜单。前者可以保存捕获的报文数据或打开以前捕获的报文数据文件，后者用于开始或停止报文捕获。
- **报文列表窗口（packet-listing window）**：显示捕获的每个报文的一行汇总信息，包括报文编号（由 Wireshark 分配，不是包含在任何协议头中的报文编号）、报文被捕获的时间、报文的源和目标地址、协议类型和报文中协议特定的信息。
- **报文首部详细信息窗口（packet-header details window）**：提供你在报文列表窗口中点击选择的报文的详细信息，包括以太网帧信息（假设报文通过一个以太网接口收发）和 IP 数据报信息。如果报文通过 TCP 或 UDP 携带，TCP 或 UDP 的详细信息也会被显示。同样的，收发该报文的最高层协议的详细信息也会被提供。
- **报文内容窗口（packet-contents window）**：同时以 ASCII 格式和十六进制格式显示被捕获数据帧的完整内容。
- **报文显示过滤框（packet display filter field）**：你可以输入协议名或其他信息以过滤可以在报文列表窗口中显示的信息。

5 一个示例

这里我们假设你的电脑是通过有线以太网接口联入 Internet，请执行如下操作：

1. 打开你的 Web 浏览器；
2. 启动 Wireshark 软件，点击菜单“capture”→“options”，你将看到如图 4 所示的界面。

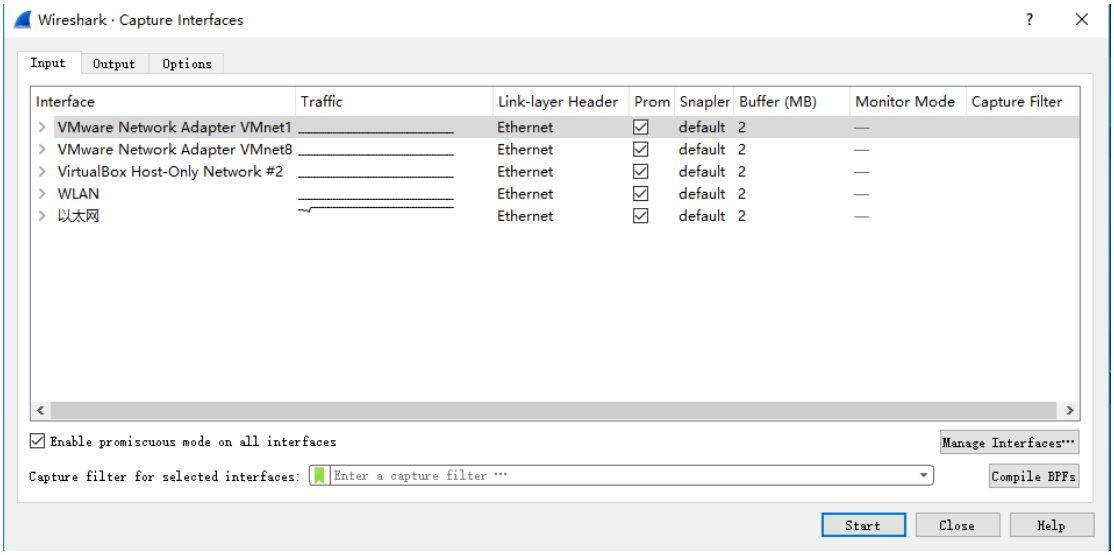


图 4 Wireshark 捕获选项窗口

如果你的电脑有多个激活的网络接口（例如一个无线接口和一个有线接口），你需要在窗口的上方框中选择一个用于收发报文的接口。然后，你就可以点击“Start”开始捕获报文了。

3. 保持 Wireshark 运行的同时，在浏览器中输入 http://www.nju.edu.cn 以访问南京大学网站首页。为了显示该页面，你的浏览器将联系 www.nju.edu.cn 的 HTTP 服务器，并与该服务器交换 HTTP 消息以下载首页内容。包含这些 HTTP 消息的以太网帧将被 Wireshark 捕获。
4. 在你的浏览器显示了首页内容之后，通过点击 Wireshark 主窗口上方快捷菜单中的“Stop capturing packets”以停止报文捕获。主窗口的内容现在应该如图 5 所示。

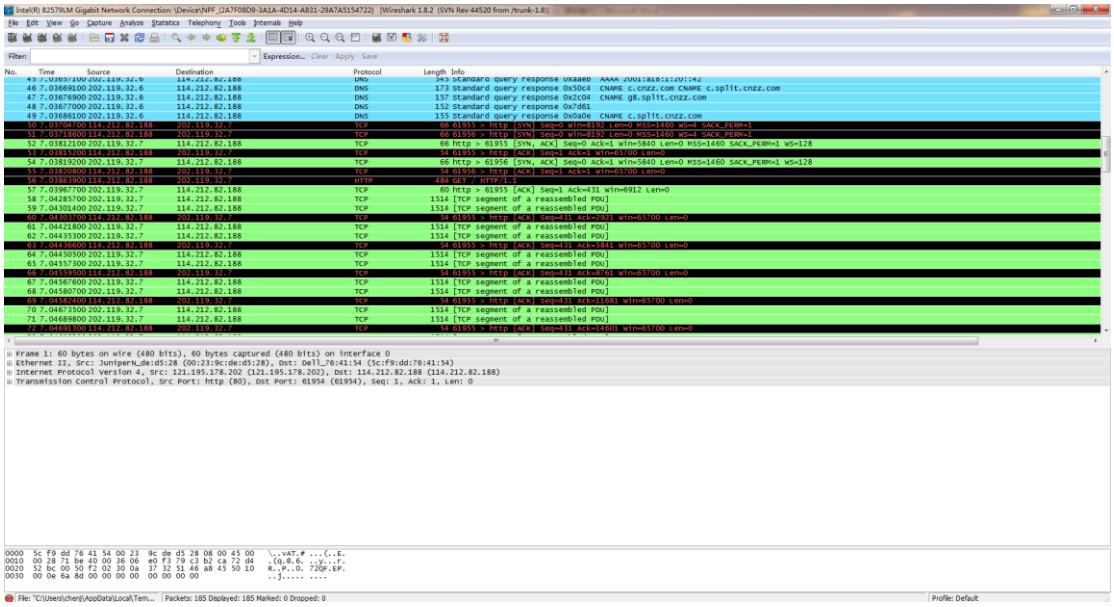


图 5 Wireshark 主窗口

你的电脑和 www.nju.edu.cn 之间交换的 HTTP 消息就显示在报文列表窗口的某处。报文列表窗口中同时也显示了很多其他类型的报文（我们可以在 Protocol 一列中看到许多不同的协议类型）。虽然你只做了访问网页这一件事情，但很明显你的电脑中还运行了许多你没有看到的协议。

5. 在“报文显示过滤框”中输入“http”（不要输入引号，并且全部用小写字母，因为 Wireshark 中的所有协议名都为小写），然后点击“Apply”，这将使得在报文列表窗口中只显示 HTTP 消息。
6. 选择报文列表窗口中的第一条 HTTP 消息，这是一条从你的电脑发往 HTTP 服务器 www.nju.edu.cn 的 HTTP GET 消息。它的以太网帧、IP 数据报、TCP 段和 HTTP 消息头信息将显示在报文头详细信息窗口中。