6.1 安装 TShark

TShark 是基于终端的 Wireshark，它是能够提供大量和 Wireshark 功能相同的数据包分析应用，但仅限于没有 GUI 的命令行界面。如果你安装了 Wireshark，那么你应该也安装了 TShark，除非你在 Wireshark 安装过程中明确反选了安装 TShark。你可以按照以下步骤确认 TShark 是否安装。

（1）在 Windows 系统中打开一个**命令提示窗口**。单击开始菜单，输入 cmd，然后单击命令行提示符。

（2）打开 Wireshark 的安装目录。如果选择默认安装，那么你可以在命令提示符里输入 cd C:\Program Files\Wireshark。

（3）输入 tshark -v 来运行 TShark 并且打印出版本信息。如果没安装 TShark，那么你会收到一个错误消息，提示你这个工具没有安装；如果 TShark 装好了，你会收到类似下面的版本信息：

```
   C:\Program Files\Wireshark>tshark –v
TShark (Wireshark) 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0
--snip--
```

如果没安装 TShark 但你现在又想使用它，那么你可以直接回到 Wireshark 的安装向导重新安装，并确保默认的 TShark 安装选项被勾选。

如果想立马开始学习 TShark 的功能，那么你可以在命令后面加上-h 参数。我们在本章之后的小节还会介绍这样的命令。

```
   C:\Program Files\Wireshark>tshark -h
```

TShark 就像 Wireshark 那样可以在多种操作系统上运行。但是因为它不依赖于操作系统的图形库，所以不同操作系统的用户体验会更趋于一致。正因为如此，TShark 在 Windows、Linux 和 OS X 上的操作基本相同。然而 Tshark 在不同平台上的操作有时候也有不同。在本书中，我们把重点放在 Windows 平台上的 TShark，因为 TShark 主要被设计在 Windows 上工作。