第 6 章　用命令行分析数据包

虽然使用 GUI 就能解决大部分问题，但是在有些时候需要使用命令行工具——TShark 或 Tcpdump。以下列举了可能需要使用命令行工具而不是 Wireshark 的一些情况。

- Wireshark 一次性提供了太多的信息。使用命令行工具可以限制打印出的信息，最后只显示相关数据，比如用单独一行来显示 IP 地址。
- 命令行工具适用于过滤数据包捕获文件，并提供结果给另一个支持 UNIX 管道的工具。
- 当处理大量的捕获文件时，Wireshark 可能会挂掉，因为整个文件都要载入内存当中。先使用流来处理大型捕获文件，可以让你快速地过滤出相关数据包，来给文件瘦身。
- 如果你在没有图形化界面的服务器上操作，则这时候你可能不得不依靠命令行工具了。

本章我会展示数据包分析领域常用的两个命令行工具——TShark 和 Tcpdump。在我看来最好两个工具你都能掌握，但我发现自己在 Windows 系统上通常使用 TShark，而在 UNIX 系统中则使用 Tcpdump。如果你只用 Windows 系统，那么你也许可以跳过 Tcpdump 的部分。