6.9 TShark VS Tcpdump

本章介绍了两个基于命令行的数据包分析应用，它们都能很好地胜任分内的工作，而且无论其中哪一款都可以通过各种选项来完成你手头上的任何工作。这里列出两个工具的几点差别，可以让你根据需求选择最适合的那个。

操作系统：Tcpdump 只能在基于 UNIX 的系统下运行，而 TShark 既可以工作在 Windows 下，又可以工作在基于 UNIX 的系统下。

协议支持：两个工具都支持常见的第 3 层和第 4 层的协议，但 Tcpdump 对第 7 层的协议支持不足。TShark 提供了丰富的第 7 层协议支持，因为它在底层使用 Wireshark 的协议解析器。

分析功能：两个工具都必须依赖手工分析才能生成有价值的结果。但是 TShark 还提供了类似于 Wireshark 的强大统计分析功能，在 GUI 不可用时能够协助分析。

其实个人习惯和工具的可用性才是选择哪个应用的决定性因素。幸运的是，这些工具的使用方式都是类似的，学会其中一个就能很快上手另一个，正所谓技多不压身。