A.2　数据包分析资源

从 Wireshark 的主页到教程、博客，有很多可用的数据包分析资源。我将在此列出我最喜欢的一些。

1．Wireshark 主页

与 Wireshark 有关的首要资源就是它的主页。主页包括软件文档、一个非常有用的包含了捕获文件样例的 wiki，以及 Wireshark 邮件列表的注册信息。

2．SANS 安全入侵检测深入课程

作为一名 SANS 导师，我可能会有点偏袒，但我真不认为这个星球上有比《SANS SEC 503：深度入侵检测》更好的数据包分析课程。这个课程集中于数据包分析的安全方面。即便你不集中于安全，该课程之前提供的对数据包分析和对 Tcpdump 的介绍也是我所见最好的。

该课程由我的两位数据包分析英雄 Mike Poor 和 Judy Novak 讲授。它每年提供好几次直播。若你的旅行经费有限，没关系，该课程也通过基于 Web 的按需格式在线讲授。

3．Chris Sanders 的博客

我没有太多时间写博客，但偶尔也会在我的博客上写一些有关数据包分析的文章。如果没有别的，我的博客就作为链接到我写的其他文章和书籍的门户，另外它也提供了我的联系方式。

4．Brad Duncan 的恶意软件流量分析网站

我最喜欢的安全相关数据包捕获资源是 Brad Duncan 的恶意软件流量分析（MTA）网站。Brad 每周多次发布包含感染链的数据包捕获资源，这些捕获资源包含相关的恶意软件二进制文件以及正在发生的事件的描述。如果你想获得解析恶意软件感染的经验并了解当前的恶意软件技术，请先下载其中一些捕获资源并尝试理解它们，你可以访问该网站，以便在发布更新时收到提醒。

5．IANA

互联网编号分配机构（Internet Assigned Numbers Authority，IANA）负责监督为北美分配 IP 地址和协议号码。它的网站提供了一些有价值的参考工具，比如查找端口号、查看有关顶级域名的信息，以及浏览合作以网站查阅 RFC 文档。

6．《TCP/IP 详解》（Addison-Wesley）

对生活在数据包层次的人而言，Richard Stevens 博士撰写的系列书籍是书架上的主要书目，已被多数人奉为 TCP/IP 圣经。这是我最喜欢的 TCP/IP 书籍，也是我写作本书时经常参考的文献。

7．《TCP/IP 指南》（No Starch 出版社）

在 TCP/IP 领域里，我最喜欢的另一本书是 Charles M. Kozierok 写的。这本巨著厚达 1000 多页，内容非常详细，并且为视觉型学习者准备了大量很优秀的图表。