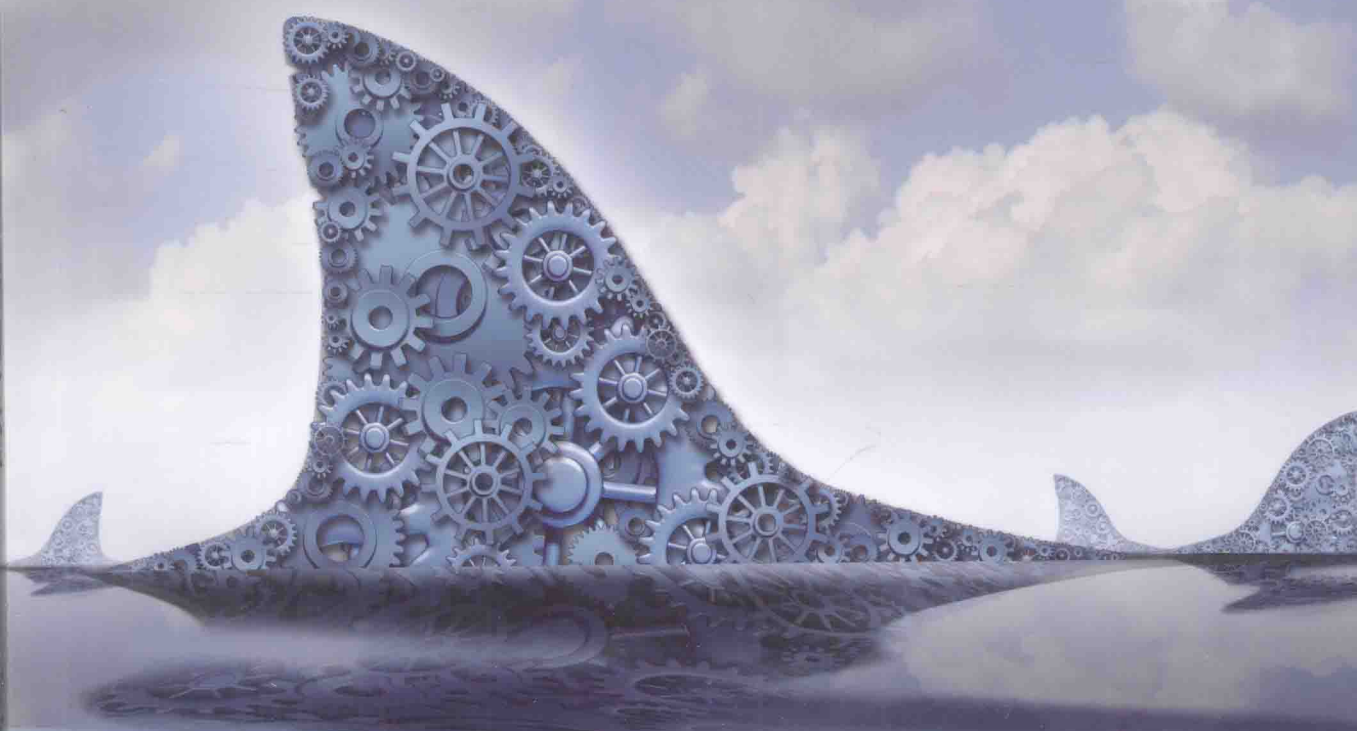
信息安全技术丛书

WIRESHARK

The Art of Network Analysis Using Wireshark



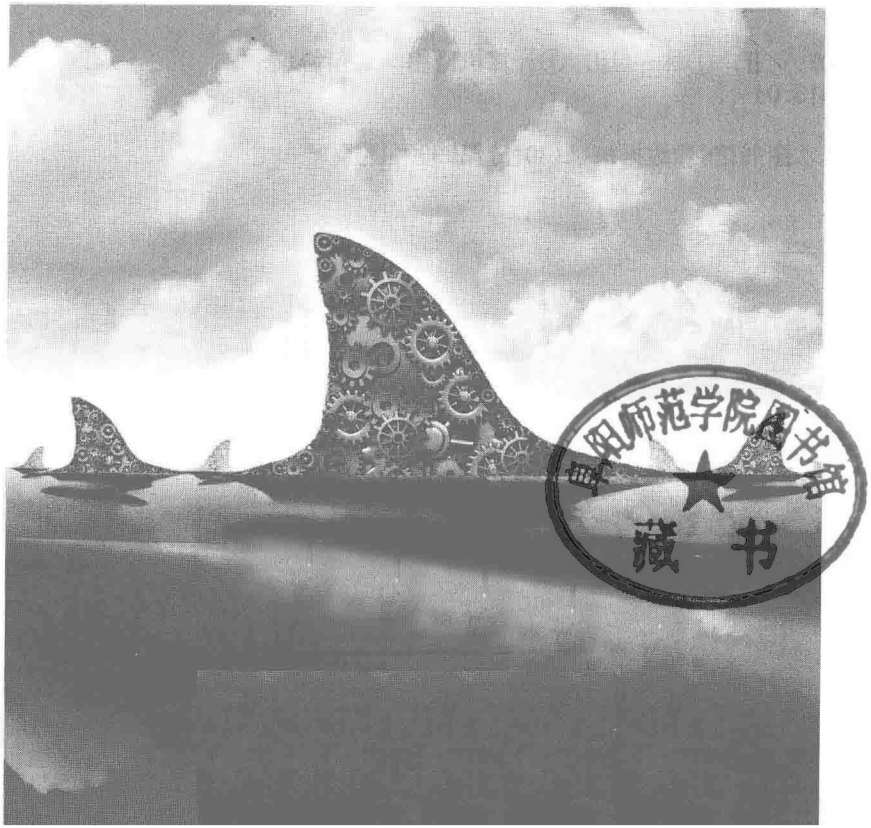
Wireshark 网络分析的艺术

林沛满 著

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

信息安全技术丛书



Wireshark 网络分析的艺术

林沛满 著

人民邮电出版社
北京

图书在版编目（CIP）数据

Wireshark网络分析的艺术 / 林沛满著. -- 北京 : 人民邮电出版社, 2016.2
ISBN 978-7-115-41021-4

Ⅰ. ①W… Ⅱ. ①林… Ⅲ. ①计算机网络－通信协议 Ⅳ. ①TN915.04

中国版本图书馆CIP数据核字(2015)第290041号

◆ 著　　林沛满
责任编辑　傅道坤
责任印制　张佳莹　焦志炜
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷
◆ 开本：800×1000　1/16
印张：13.5
字数：251 千字　　2016 年 2 月第 1 版
印数：1－4 000 册　　2016 年 2 月北京第 1 次印刷

定价：45.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

Wireshark 是当前最流行的网络包分析工具。它上手简单，无需培训就可入门。很多棘手的网络问题遇到 Wireshark 都能迎刃而解。

本书挑选的网络包来自真实场景，经典且接地气。讲解时采用了生活化的语言，力求通俗易懂，以使读者在轻松阅读的过程中，既可以学到实用的网络知识，又能形成解决问题的思路。

与大多网络图书的课堂式体验不同，阅读本书的感觉更像在听技术圈的朋友分享经验，除了知识，还有心情和想法。本书的覆盖范围从日常使用的手机 App，到企业级的数据中心；从对付运营商的网络劫持，到开发自己的分析工具，不一而足。无论你是系统管理员、实施工程师、技术支持、网管、培训教师，还是开发和测试人员，都适合阅读本书。

关于作者

林沛满，2005 年毕业于上海交通大学，现任 EMC 网络存储部门的主任工程师。多年来为多个产品团队提供过技术咨询，范围包括网络、操作系统、文件系统和域等，这就是本书所涵盖的协议如此五花八门的原因。每年临近加薪的日子，他也会组织一些技术培训来提醒上司，本书的部分内容就来自这些培训资料。

平时他也写一些技术博客，你或许还能在 IT168 或者 ChinaUnix 技术社区看到它们，本书也有少数内容来自这些博客。他也是《Wireshark 网络分析就这么简单》的作者。

当林先生不在工作时，大部分时间都花在了园艺花卉上，尤其是欧洲月季。

此为试读，需要完整PDF请访问：www.ertongbook.com

致　谢

我那些没有技术背景的亲友只能读懂这一部分，所以要尽量写得好一些。

分析网络包占用了很多本应该和家人在一起的时光，因此要特别感谢他们的理解和支持。我妻子在每天忙碌的工作之余，还要弥补我的那份亲子时间，让小满享受到完美的亲情。她也是第一个审核书稿的人，包括文字和技术两方面，“贤内助”一词已经不足以形容她的贡献了。我父母分担了很多家庭劳动，否则花园里早就杂草丛生。他们可能至今还以为我坐在电脑面前就是在赶稿子。

技术圈的很多朋友帮忙检阅了本书部分章节，为我严把技术关。请给我一次招待你们吃大餐的机会。

我的老板从没有提出过 KPI 上的要求，因此我才有这么多时间研究工作之外的技术问题。

此外还要感谢很多读者长期的鼓励，请恕我无法一一列举你们的名字。要不是你们隔段时间就催一下，以我的拖延症不知道何日才能写完。

前　言

Wireshark 已经用不着我来做广告了，它早已被多家权威机构评为最佳嗅探器，从事网络工作的工程师都知道它。即便我如实地列举它的种种好处，都涉嫌违反广告法。这也许就是我的上一本书《Wireshark 网络分析就这么简单》得以多次重印的原因，是神器总会流行的。读者的评价也超乎我的想象，随手复制两条书评过来满足一下我的虚荣心：

“这本书陪了我几个深夜。没有大部头的催眠和艰涩，每一节都精炼易读，和咖啡一样令人上瘾。我是网络小新人，但是不觉得特别难，很容易顺下来。里面很多干货，厚积薄发，都是实际环境中的情况。畅快淋漓读完大呼不过瘾，搜了一下作者就这一本书。遗憾！”

——亚马逊读者

“这本书是我 2014 年读过的 10 本好书之一，如果说我对这本书有什么不满的话，就只有一个：书写薄了，意犹未尽，读着完全不过瘾呀呀呀。或许这本书浅显易懂、幽默风趣的语言风格让你在无障碍阅读的同时，会让你有一种这书太浅、适合初学者的感觉，但是这本书实际上是越读越有味道，我就读了好几次。”

——豆瓣读者

既然有这么多人喜欢，我有什么理由不再写一本呢？于是就有了这本新书。虽然我在写稿这件事情上的拖延症不亚于洗碗，不过读者们的鼓励显然起了作用，最后收笔时间只比原计划晚了 6 个月。和老读者们期望的一样，它是上一本书的延续，尤其是在写作风格上。不同之处在于这一本不再着重分析基础协议，而更专注于解决现实问题。另外，考虑到现在手机上网日趋流行，本书也增加了一些手机 App 的内容，相信读者会喜欢。

就如我常在培训课上所讲的，学会 Wireshark 这个软件只需要几个小时，掌握一个网络协议也用不了几天，而养成解决问题的思路却需要经年累月的练习和思考。本书正提供了很多练习和思考的机会，本书 30 多篇文章，几乎都用了 Wireshark 来分析网络包。我希望每一篇都能让读者产生这样的感触："啊，原来 Wireshark 还可以这样用！""读完整本书，自然而然会形成看包的习惯和思维方式。

本书组织结构

就像时尚女郎每天都在看包包一样，我也每天都在看包。看到有趣又有价值的，就会记录下来，久而久之就形成了这本书。因此它有别于包罗万象的网络教材，而更像一个技术博客的合集。

全书根据素材来源可分为四个部分。

第一部分的选材来自老读者的咨询，相信很有代表性，说不定其他读者也会遇到。

- 《Linux 为什么卡住了》分析了登录 Linux 时卡顿 10 秒钟的现象。虽然我是 Linux 领域的菜鸟，但是仍然可以用 Wireshark 发现原因并解决它。
- 《像福尔摩斯一样思考》讲述的是如何根据网络包中的蛛丝马迹，找到被人为掩盖的线索。自己从网络包推理出来的东西，往往比对方提供的文档更可靠。
- 《一篇关于 VMware 的文章》介绍了一位读者在 VMware 知识库发现的文章。我们纯粹依靠协议分析，找到了这篇文章的真正内涵，最后再用 Wireshark 看包加以确认。
- 《来点有深度的》是在上一篇的基础上，通过发散思维，向读者"灌输"了一些相关的 TCP 知识。个人觉得 TCP 协议理解到这个深度就足够应付大多数性能问题了。
- 《三次握手的小知识》是应某论坛网友的要求而写的 TCP 握手科普，分享了一些用 Wireshark 来处理握手问题的小经验，顺便演示了"SYN flood"攻击的网络包。

- 《被误解的 TCP》澄清了被读者广泛误解的两个 TCP 概念，比较了 Linux、Windows 和安卓手机的不同 Ack 频率。

- 《最经典的网络问题》是我近年遇到过的最经典的案例了。虽然很多年前就听说过 Nagle 算法遇到延迟确认会出问题，但是在现实中还是第一次遇到，赶紧记录下来。

- 《为什么丢了单子？》讲述了一位销售朋友的遭遇，说明用 Wireshark 有助于发现产品的不足，并且找到改进之处。如果能用 Wireshark 分析自家产品与竞争对手产品的网络包，一定能找到不少差别，从而改进销售策略。

- 《受损的帧》分析了因为硬件等原因导致帧损坏，从而在 Wireshark 上体现出的奇怪症状。事情往往没有表面上看到的那么简单。

- 《虚惊一场》是因为一位眼尖的读者发现了我书中的一处“错误”（或者可以说是 TCP 的一个 bug），后来研究了很久才发现是虚惊一场，不过排查过程还是很值得分享的。这位读者还从“作者简介”的照片中，看到我手上的《TCP/IP 详解 卷 1:协议》是影印版，然后特意从美国帮我寄来了一本原版书。再次表示感谢！

- 《NTLM 协议分析》是这部分唯一的基础协议介绍，据说 NTLM 在中国用得还很多，所以才特意写了一篇。

- 《Wireshark 的提示》收集了读者感兴趣的很多 Wireshark 提示信息。文中不但介绍了每一个提示信息的意义，还分析了其产生的原因，希望让读者能够知其所以然。

第二部分是我自己在工作中遇到的网络问题。这部分讲得最细、最深，问题本身也最复杂。在阅读这一部分时，可能要多花点时间。

- 《书上错了吗？》解释了为什么对于同一个 TCP 连接，在两端抓到的网络包顺序是不同的。明白了这一点才能理解后面两篇的内容。

- 《计算“在途字节数”》介绍了如何从网络包中计算“已经发送但未被确认”的数据量。不用害怕数学，简单的加减法就够用了。
- 《估算网络拥塞点》在前两篇的基础上，提供了一个估算网络拥塞点的方法。掌握了这个技能，此后再优化 TCP 性能时就胸有成竹了。
- 《顺便说说 LSO》讲的是现在越来越普遍的 Large Segment Offload。在估算拥塞点的时候很可能会被 LSO 所干扰，因此我特意为它写了一篇。
- 《熟读 RFC》分析了一个颇为棘手的性能问题，即使擅长 Wireshark 也很难解决，向大家展示了熟悉 RFC 的重要性。
- 《一个你本该能解决的问题》用 Wireshark 分析了一个 UDP 导致的性能问题，从本质上分析 UDP 和 TCP 的差别。这一篇我在微博上发过，还引发了一场不小的讨论。
- 《几个关于分片的问题》其实是上一篇的后续。很多读者看到 UDP 包被分片之后出现了性能问题，所以对分片很感兴趣，问了不少问题。
- 《MTU 导致的悲剧》分享了几个 MTU 配置出问题而导致的事故。这类问题其实很多见的，尤其是对于实施和运维人员来说。
- 《迎刃而解》是来自一个运维部门的技术问题，相当隐蔽而且诡异，最终在 Wireshark 的辅助下迎刃而解。
- 《昙花一现的协议》回忆了一个我曾经支持过的协议。今天才学习它可能没有实际意义，但是其理念和创意还是值得借鉴的。当你对一个协议了解到一定程度时，肯定也会有改造它的想法。
- 《另一种流控》介绍的是 Pause Frame（暂停帧）流控。有别于 TCP 的“端到端”流控，它是“点到点”的，在有些场合很好用。
- 《过犹不及》分享了一个多线程传输的案例，说明不是增加连接数就一定能提高性能，有时候甚至有负面效果。

- 《治疗强迫症》演示了如何用 Wireshark 研究文本编辑软件的工作方式。也许这类软件不是你的兴趣所在，但是可以举一反三，用相同的方式研究其他软件。

- 《技术与工龄》算是半篇技术文章。除了介绍 Window Scale 这个技术点，还希望每个人都能正视工龄，善待新人。

- 《一个面试建议》只是分享面试经验，完全无关技术。文章写得很不严肃，目的是让读者休息一下，乐一乐。

- 《如何科学地推卸责任》不是想把你“教坏”，而是分享了如何在技术上划分责任。如果你是乙方工程师，肯定会需要的。

第三部分的选材是日常生活中的抓包，包括手机 App。在未来一两年，可能会有越来越多的人去抓手机上的包，因为用得多了，问题也会跟着增加。

- 《假宽带真相》本是央视某一期节目的名字，说测速软件“有明显的设计缺陷”。我用 Wireshark 进行了验证，结果如何呢？读了全文就知道了。

- 《手机抓包》讲解的是如何在家里搭建适合抓手机包的 WiFi 环境。如果你经常需要抓手机上的包来研究，相信我，是该改造一下家里的网络了。

- 《微博为什么会卡》分析了微博在 WiFi 环境下经常卡顿的问题，最后找出来的原因竟然是 DNS。本文对很多 App 的优化有借鉴作用。

- 《寻找 HttpDNS》讲述了一个“失败”的探索过程，因为到最后都没有找到想要的包。不过失败本身也有价值，因为我们知道了真相不过如此。

- 《谁动了我的网络》详细地讲解了被劫持的网络包有什么特征，以及如何在 Wireshark 中找到它们。下一次你怀疑自家网络被劫持时，就可以抓一个包自己分析了。

- 《一个协议的进化》介绍的是当前 HTTP 1.1 在性能上的落后之处，以及可能改进的空间。可惜现在 HTTP 2 的包还不容易抓到，否则我们还可以增加一些内容。

此为试读，需要完整PDF请访问：www.ertongbook.com

- 《假装产品经理》分析了在微博发图片的网络包，我们可以从中看到它的压缩比例、上传行为、CDN 服务商等。不用派卧底去新浪，就可以侦察到不少“机密”。
- 《自学的窍门》也无关技术，只是分享了本人的学习经验，希望对新人有些参考价值。

第四部分的内容很少，却花费了我不少时间，因为写的是两个项目/产品。

- 《打造自己的分析工具》介绍了我自己打造的一个性能分析网站，让大家体验一下量身定制的工具有多好用。本文也分享了开发过程的一些经验。
- 《一个创业点子》讲的是我曾经想做的一个网络加速器。里面知识点还是挺多的，也适合用 Wireshark 来研究。

你可能会问的一些问题

1. 阅读此书需要什么基础？

只需要具备网络常识，比如在学校里上过网络课或者考过 CCNA 就够了。如果读过《Wireshark 网络分析就这么简单》是最好的，会觉得衔接顺畅。对于缺乏网络基础的 Wireshark 用户，建议先阅读 Richard Stevens 的《TCP/IP 详解 卷 1：协议》。英文好的读者可以通过 http://www.tcpipguide.com/free/index.htm 页面免费阅读《The TCP/IP Guide》一书，里面的插图画得尤其好。由于读免费书籍很难坚持下去，你可以点击页面下方的 Donate 按钮给作者捐款，由此增加进一步学习的功力。

2. 本书的选材为何如此广泛？

我写这本书是为了让读者学有所获，因此选材也从读者的兴趣点出发。比如现在流行手机上网，因此我增加了这部分的内容；又比如技术圈正在热议 HttpDNS，所以我就去做了一系列实验……不同读者的关注点肯定会有所不同，如果某一篇的话题不是你感兴趣的，直接跳过也不影响后面的阅读。

3. 为什么我觉得有些内容太简单了？

人们读书时都会有这样的反应——读到自己不懂的内容时，就会觉得高大上；读到自己擅长的领域时，又会觉得太简单。这就是为什么有些作者喜欢把书写得很玄乎，然而我的风格恰恰相反，会尽可能地把复杂的问题简单化。我的技术培训也是坚持这样的风格，会假设所有听众都是刚毕业的文科妹子（嗯，这样也会使我的心情好一些）。

4. 为什么没有随书光盘？

我也希望能把这本书里的网络包都共享出来，但由于大多是在客户的生产环境中抓到的，所以不适合公开。毕竟从包里能暴露出来的安全隐患太多了，希望读者能理解这个苦衷。为了方便阅读，我已经尽量把 Wireshark 截图做清晰。建议大家在自己的环境中抓包分析，这会比看示例包更有价值。

5. 怎样联系作者？

如果对书中的内容有疑问，或者自己抓了包却不知道怎么分析，都可以联系作者，邮箱地址为 linpeiman@hotmail.com。你也可以在微博上@林沛满，但不建议关注，因为他是个整天晒园艺图片的话痨。

目　录

答读者问

1

在过去几年中，有不少读者、同事和网友向我咨询过网络问题，其中大部分都记录在案。我一直把这些案例视为珍贵的财富，因为既真实又有广泛的代表性，比我自己在实验室中“制造”出来的好多了。本书从中选择了最经典的部分，希望读者会感兴趣。如果你在工作或生活中遇到网络问题，也欢迎抓个包来找我分析。

此为试读,需要完整PDF请访问: www.ertongbook.com