Packt>

异步图书
www.epubit.com

Wireshark 网络分析实战

（第2版）

Network Analysis Using Wireshark 2 Cookbook

(2nd Edition)

[印　度] 甘德拉·库马尔·纳纳（Nagendra Kumar Nainar）
[印　度] 尧戈什·拉姆多斯（Yogesh Ramdoss）
[以色列] 约拉姆·奥扎赫（Yoram Orzach）

孙余强　王涛　译

中国工信出版集团　人民邮电出版社 POSTS & TELECOM PRESS

Packt>

异步图书
www.epubit.com

（第2版）

Network Analysis Using Wireshark 2 Cookbook

(2nd Edition)

[印　度] 甘德拉·库马尔·纳纳（Nagendra Kumar Nainar）
[印　度] 尧戈什·拉姆多斯（Yogesh Ramdoss）
[以色列] [illegible]ach）

人民邮电出版社
北　京

图书在版编目（CIP）数据

Wireshark网络分析实战 : 第2版 / (印) 甘德拉·库马尔·纳纳, (印) 尧戈什·拉姆多斯 (Yogesh Ramdoss) , (以) 约拉姆·奥扎赫 (Yoram Orzach) 著 ; 孙余强, 王涛译. -- 北京 : 人民邮电出版社, 2019.1
ISBN 978-7-115-50002-1

Ⅰ. ①W… Ⅱ. ①甘… ②尧… ③约… ④孙… ⑤王… 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(2018)第247604号

版权声明

◆ 著 [印度]甘德拉·库马尔·纳纳（Nagendra Kumar Nainar）
[印度]尧戈什·拉姆多斯（Yogesh Ramdoss）
[以色列]约拉姆·奥扎赫（Yoram Orzach）
译 孙余强 王 涛
责任编辑 傅道坤
责任印制 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
三河市君旺印务有限公司印刷

◆ 开本：800×1000 1/16
印张：31.5
字数：686 千字 2019 年 1 月第 1 版
印数：1－3 000 册 2019 年 1 月河北第 1 次印刷
著作权合同登记号 图字：01-2017-8620 号

定价：118.00 元

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内容提要

本书是畅销书《Wireshark 网络分析实战》的全新升级版，按部就班地讲解了 Wireshark 的用法以及如何使用该工具解决实际的网络问题。

本书共分为 19 章，其内容涵盖了 Wireshark 版本 2 简介，熟练使用 Wireshark 排除网络故障，抓包过滤器的用法，显示过滤器的用法，基本信息统计工具的用法，高级信息统计工具的用法，Expert Information 工具的用法，Ethernet 和 LAN 交换，无线 LAN，网络层协议及其运作方式，传输层协议分析，FTP、HTTP/1 和 HTTP/2，DNS 协议分析，E-mail 协议分析，NetBIOS 和 SMB 协议分析，企业网应用程序行为分析，排除 SIP、多媒体及 IP 电话故障，排除由低带宽或高延迟所引发的故障，网络安全和网络取证等知识。

本书适合对 Wireshark 感兴趣的网络从业人员阅读，高校网络相关专业的师生也能从本书中获益。

献辞

谨将本书献给我的挚友 Suresh Kumar 及其亡妻 Dharshana Suresh。

——Nagendra Kumar Nainar

谨将本书奉献给我的父母 Ramdoss 和 Bhavani，他们为我的成功倾注了自己的生命。

——Yogesh Ramdoss

关于作者

Nagendra Kumar Nainar（CCIE #20987），Cisco 公司 RP 升级（escalation）团队的高级技术领导。他是 80 多项专利申请的共同发明人，以及 6 份 Internet RFC、多份 Internet 草案和 IEEE 论文的共同作者。他还是北卡罗来纳州立大学的客座讲师，在各种网络论坛上发表过演讲。

我要感谢我那亲爱的妻子 Lavanya 和可爱的女儿 Ananyaa，感谢你们的理解和支持；感谢我的父母 Nainar 和 Amirtham；还要感谢我的兄弟 Natesh 以及家人的支持。

要特别感谢我的导师 Carlos Pignataro 和领导 Mike Stallings。要感谢 Arun 和 Abayom 提出的意见。还要感谢我的朋友 Satish、Poornima、Praveen、Rethna、Vinodh、Mani、Parthi 和出版社。

Yogesh Ramdoss（CCIE #16183），Cisco 公司技术服务机构的高级技术领导。他是 Cisco Live 大会的杰出演讲者，在会上向客户分享并传授与企业/数据中心技术和平台、故障排除和抓包工具，以及与开放性网络编程有关的技术。他还是机器/行为学习（machine/behavior learning）方面某些专利的共同发明人。

我要感谢我的妻子 Vaishnavi，孩子 Janani 和 Karthik，感谢你们的耐心和支持。

要特别提及并感谢马杜赖（印度南部城市）蒂加拉杰工程学院的校长 V. Abhaikumar 博士。万分感谢本书的合著者 Nagendra Kumar Nainar、我的领导 Michael Stallings、我的导师 Carlos Pignataro，以及我所有的朋友和家人。

Yoram Orzach，毕业于以色列海法理工学院，拥有该校颁发的科学学士学位。他最初以系统工程师的身份就职于 Bezeq 公司，从事传输及接入网相关工作。在担任过 Netplus 公司的技术管理者一职之后，现任 NDI 通信公司的 CTO。Yoram 对大型企业网络、服务提供商网络及 Internet 服务提供商网络极有心得，Comverse、Motorola、Intel、Ceragon Networks、Marvel 以及 HP 等公司都接受过他提供的服务。他在网络设计、实施及排障方面浸淫多年，具有研发、工程及 IT 团队培训工作的丰富经验。

关于技术审稿人

Abayomi Adefila，Cisco 公司服务机构的技术领导。他握有科学学士学位（B.Tech）和理科硕士学位（M.Sc），获得的证书包括 CCNA、CCDA、CCNP、CCIP、CCDP、CCIE（R&S），精通 MPLS L3 VPN、VRF、ISIS、IPv6、BGP4、MP-BGP、OSPFv2&3、RIPng、EIGRPv6、DS1、DS3、城域以太网、EEM、OER 等诸多技术，熟练掌握 Cisco 网络设备的高级路由和交换、GRE、IPSec 的配置以及 Cisco VPN 集中器和 Juniper 设备的配置。在 Verizon 公司效力期间，他获得过 MCI 的杰出表现奖，在 Cisco 公司也因表现出色而获得过多个 CAP 奖。

Jason Morris，系统和研究工程师，在系统架构、研究工程和大数据分析方面拥有 18 年以上的经验。

他是设计大型体系结构、云上最佳安全实践、基于深度学习的贴近实时图像检测分析，以及针对 ETL 的无服务器体系结构的演讲者和顾问。他近期的工作角色包括 Amazon Web 服务的解决方案架构师、大数据工程师、大数据专家和导师。他是 Next Rev Technologies 公司现任的首席技术官。

我要感谢 Packt 出版社的整个编辑和制作团队，感谢你们为出品精良图书所付出的努力，同时也要感谢本书的读者。愿本书能帮助读者探索伟大之事。

前言

Wireshark 早已成为网络分析领域里的标配工具，随着 Internet 和 TCP/IP 网络的极速发展，该工具受到了网络分析专家及排障工程师的热捧，同时获得了（网络协议或应用程序）研发工程师们的青睐，因为后一类人需要知道协议在网络中的实际运作方式以及在运行时所碰到的问题。

本书包含排除数据通信网络故障的实战秘诀。本书第 2 版围绕 Wireshark 2 展开，该软件因其所提供的增强功能，从而获得了很强的吸引力。本书第 2 版对第 1 版探讨的某些主题做了进一步的扩充，这些主题包括 TCP 性能、网络安全、无线 LAN 以及如何用 Wireshark 监控云和虚拟系统。读者将学会如何借助于 Wireshark 分析端到端 IPv4 和 IPv6 单、多播流量的连通性故障。本书还会展示 Wireshark 抓包文件的内容，好让读者将所学理论知识与实战相结合。读者将会认识 E-mail 协议的常规运作方式，学会如何用 Wireshark 进行基本分析和故障排除。使用 Wireshark，读者将能够排除企业网内常用的应用程序（比如 NetBIOS 和 SMB）的故障。最后，读者还将学会如何借助 Wireshark 测量网络（性能）参数，检查并有效解决由网络性能导致的网络故障。在本书的末尾，读者会掌握如何分析流量，如何发现各种违规流量模式，以及如何加固网络使其不受违规流量的影响。

本书的书名既然叫《Wireshark 网络分析实战》，那么其内容一定是由一系列利用 Wireshark 对网络故障进行有效性、针对性分析的实用诀窍构成。书中包含的每个诀窍都与某一具体的网络故障相关联，在介绍如何使用 Wireshark 解决相关故障时，作者会指出应关注 Wireshark 工具的哪些地方、哪些（抓包）内容以及正在处理的故障的起因。为求表述圆满，每个诀窍都会包含相应主题的理论基础知识，好让尚未掌握基础概念的读者先行武装自己。

书中包含了许多示例，所有示例均来源于真实案例。作者在处理这些案例时，所花费的时间虽长短不一（有些只花了几分钟时间，有些则要花几小时甚至几天），但所遵循的原则只有一条，那就是：按部就班，选择正确的工具，当应用程序开发者肚里的“蛔虫”，外加像某些人说的那样，从网络的角度思考问题。只要按此原则行事，兼之能活学活用 Wireshark，定能将故障查个水落石出。本书的目的也正在于此，享受这一切吧。

本书读者对象

本书的读者对象包括使用 Wireshark 进行网络分析及排障的安全专业人员、网管人员、研发人员、工程和技术支持人员以及通信管理人员。阅读本书的读者需掌握网络的基本概念，但

不要求读者对具体的协议及厂商实现有深入的了解。

本书内容

- **第 1 章，Wireshark 版本 2 简介**，介绍 Wireshark 所能行使的基本任务。
- **第 2 章，熟练使用 Wireshark 排除网络故障**，向读者传授如何更加娴熟地将 Wireshark 作为网络排障工具来使用。
- **第 3 章，抓包过滤器的用法**，讨论抓包过滤器的使用方法。
- **第 4 章，显示过滤器的用法**，讨论显示过滤器的使用方法。
- **第 5 章，基本信息统计工具的用法**，介绍 Wireshark 自带的信息统计工具的基本用法。
- **第 6 章，高级信息统计工具的用法**，介绍 Wireshark 自带的信息统计工具的高级用法，包括如何用 Statistics 菜单下的有关菜单项，生成 IO 图（IO graph）、TCP 流图（TCP stream graph）以及 UDP 多播流图（UDP multicast stream）。
- **第 7 章，Expert Information 工具的用法**，向读者传授如何使用 Wireshark 内置的专家系统（Expert System）工具，该工具可对网络中发生的各种现象（包括各种网络事件和网络故障）洞察秋毫。
- **第 8 章，Ethernet 和 LAN 交换**，主要介绍如何发现并解决基于第 2 层的网络故障，重点关注基于 Ethernet 的网络故障（比如，广播/多播事件和错误）以及如何发现故障的源头。
- **第 9 章，无线 LAN**，介绍无线 LAN 流量的分析方法，以及如何诊断由用户申告的无线网络连通性故障及性能问题。
- **第 10 章，网络层协议及其运作方式**，重点关注 OSI 参考模型的第 3 层，向读者传授如何对各种第 3 层协议（IPv4/IPv6）的运作方式加以分析。本章还将介绍单、多播流量的分析方法。
- **第 11 章，传输层协议分析**，重点关注 OSI 参考模型的传输层，向读者传授如何对各种第 4 层协议（TCP/UDP/SCTP）的运作方式加以分析。
- **第 12 章，FTP、HTTP/1 和 HTTP/2**，介绍这几种协议、它们的运作方式，以及如何借助 Wireshark 发现网络中与这几种协议有关的常见错误和问题。
- **第 13 章，DNS 协议分析**，涵盖 DNS 协议的基本原理、功能、常见问题以及如何用 Wireshark 分析并解决与该协议有关的问题。
- **第 14 章，E-mail 协议分析**，介绍各种 E-mail 协议的常规运作方式，以及如何用

Wireshark 针对这些协议进行基本的分析和排障。

- **第 15 章，NetBIOS 和 SMB 协议分析**，向读者传授如何用 Wireshark 解决并排除企业网络内常用的应用程序（涉及 NetBIOS 和 SMB 协议的应用程序）的故障。
- **第 16 章，企业网应用程序行为分析**，介绍如何用 Wireshark 解决并排除企业网络内常用的应用程序的故障。
- **第 17 章，排除 SIP、多媒体及 IP 电话故障**，介绍各种多媒体协议以及如何用 Wireshark 分析语音和视频流。
- **第 18 章，排除由低带宽或高延迟所引发的故障**，向读者传授如何测量带宽和延迟这两项网络参数，如何检查由两者所引发的网络故障，以及如何尽可能地解决此类网络故障。
- **第 19 章，网络安全和网络取证**，首先讲解如何区分正常和异常的网络流量，然后介绍各类网络攻击，说明攻击自哪儿发起，外加如何隔离并消除攻击。

阅读准备

阅读本书之前，请先到 Wireshark 官方站点下载并安装 Wireshark 软件。

资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

配套资源

本书提供如下资源：

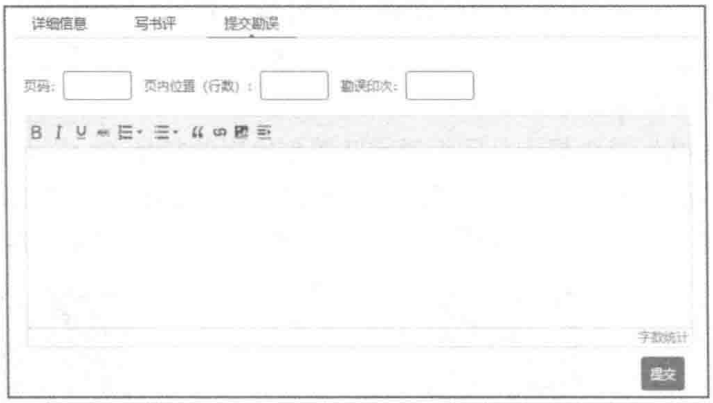
- 书中彩图文件。

要获得以上配套资源，请在异步社区本书页面中单击 配套资源，跳转到下载界面，按提示进行操作即可。注意：为保证购书读者的权益，该操作会给出相关提示，要求输入提取码进行验证。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，单击“提交勘误”，输入勘误信息，单击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。



扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“**异步社区**”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“**异步图书**”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目录