Broadview
www.broadview.com.cn

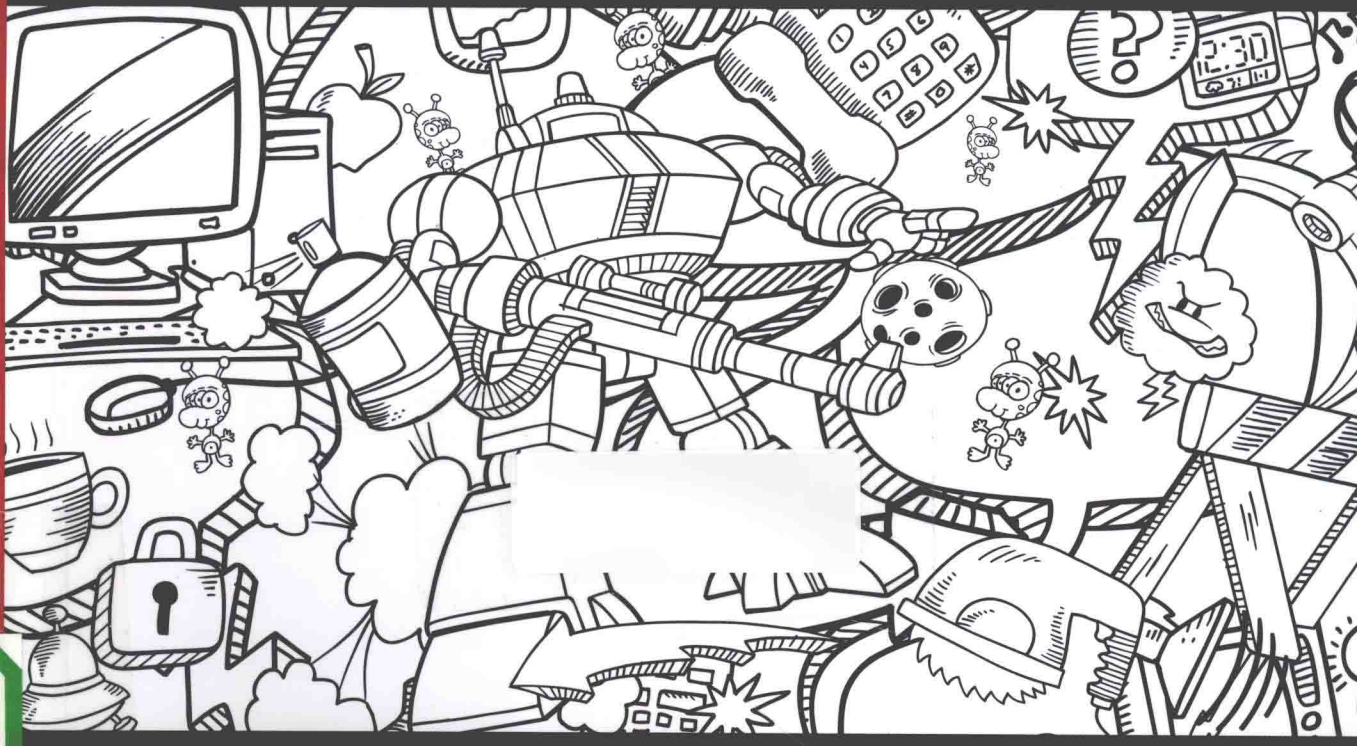
安全技术大系

PEARSON

一本书掌握基于大数据的智能化海量情报分析方法和技能！

黑客大追踪

网络取证核心原理与实践



Network Forensics

TRACKING HACKERS THROUGH CYBERSPACE

[美] Sherri Davidoff Jonathan Ham 著
崔孝晨 陆道宏 等译

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

黑客大追踪

网络取证核心原理与实践

Network Forensics

TRACKING HACKERS THROUGH CYBERSPACE

[美] Sherri Davidoff Jonathan Ham 著
崔孝晨 陆道宏 等译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

网络取证是计算机取证技术的一个新的发展方向，是计算机网络技术与法学的交叉学科。本书是网络取证方面的第一本专著，一经出版便好评如潮，在 Amazon 网站上的评分达 4.5 星。

本书根据网络取证调查人员的实际需要，概述了网络取证的各个方面，不论是对各种网络协议的分析和对各种网络设备的处理方式，还是取证流程的设计都有独到之处。

本书共分四大部分十二章，第 1 章“实用调查策略”，第 2 章“技术基础”和第 3 章“证据获取”属于第一部分，其中给出了一个取证的方法框架，并介绍了相关的基础知识；第 4 章“数据包分析”，第 5 章“流统计分析”、第 6 章“无线：无须网线的取证”和第 7 章“网络入侵的侦测及分析”属于第二部分，介绍了对网络流量进行分析的各种技术；第 8 章“事件日志的聚合、关联和分析”、第 9 章“交换器、路由器、防火墙”和第 10 章“Web 代理”属于第三部分，详述了在各种网络设备和服务器中获取和分析证据的方法。第 11 章“网络隧道”和第 12 章“恶意软件取证”属于第四部分，针对网络隧道和恶意软件分析这两个网络取证中的难点和热点问题展开讨论。

本书在学术理论上具有交叉性、前沿性和创新性，在实践应用中注重可操作性和实用性。可作为网络安全/计算机取证专业的教材，对于司法工作者、律师、司法鉴定人和 IT 从业人员，也具有良好的参考价值。

版权贸易合同登记号图字：01-2014-1277

图书在版编目（CIP）数据

黑客大追踪：网络取证核心原理与实践 /（美）大卫杜夫（Davidoff,S.），（美）汉姆（Ham,J.）著；崔孝晨等译.
北京：电子工业出版社，2015.1
（安全技术大系）
书名原文：Network Forensics: Tracking Hackers through Cyberspace
ISBN 978-7-121-24554-1

Ⅰ. ①黑… Ⅱ. ①大… ②汉… ③崔… Ⅲ. ①计算机网络－安全技术－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 243622 号

策划编辑：刘 皎
责任编辑：徐津平
特约编辑：顾慧芳
印 刷：北京京科印刷有限公司
装 订：三河市皇庄路通装订厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
开 本：787×980 1/16 印张：31 字数：752 千字
版 次：2015 年 1 月第 1 版
印 次：2015 年 1 月第 1 次印刷
定 价：119.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

推荐序

当安全圈前辈 cnhawk 找到我，希望我为这本由崔孝晨老师及公安系统一线专家团队翻译的亚马逊 5 星畅销书写份推荐的时候，小生何其惶恐。网络犯罪取证和黑客追踪溯源，不但是“猫捉老鼠”般的斗智斗力，更需要侦查人员广博深厚的知识技术水平和长时间的经验积累。

在这个领域，小生沉醉多年，从最开始摸索如何利用 Network general 的 sniffer portable 便携式设备抵近目标局域网，到利用网关设备旁路分光/镜像采集、分析重要内网网络流量和协议，再到利用机器学习方法挖掘处理海量日志和社工证据，更亲身实践过先进木马和僵尸网络的攻防对抗……10 多年一路走来，深感网络取证追踪领域的浩瀚复杂、相关技术资料搜集整理的艰辛，更为**“如何构建完备的网络取证知识技能体系？如何将长期以来在各个层次实施取证/对抗的经验教训进行系统化的梳理？”**这个巨大的课题而长期的困惑着……**直到我读完这本书。**

从本地取证到网络追踪，远不仅仅是从磁盘数据恢复+内存 dump 到网络数据包截获分析的“升级”，而是实现了从**“单点证据采集”**到**“全域、多层次海量数据证据链信息的挖掘推理”**的跃变。取证的装备和技术在发展，侦查人员的思维和眼界更要改变。

书中把“证据”定义为：任何可观察且可记录的事件或者是事件的因素，即能用来正确理解一个已被观察到的事件发生原因和本质的，任何可以被观察到并被记录下来的活动或产生活动的人为因素。从我的理解看，本书围绕网络取证和黑客追踪这个主题，通过深入浅出的技术总结和实战案例分析，囊括了**“观察”“记录”和“理解”**三个核心要素：

1．如何成为一名精通无线/有线网络通信和协议分析的侦查员？

针对广域网、园区有线网、无线网等不同网络目标，了解网络中各类系统的配置、接口和功能，从不同类型的接入点（如：无线 AP、交换机）或中间媒介（如光纤、以太网线）切入网络，主动/被动地截获各级各类网络流量，从各种标准网络协议如 802.11b/g/n, ARP, DHCP, IPv4, IPv6, TCP, UDP, ICMP, TLS/SSL, SMTP, IMAP, DNS, HTTP, SMB, FTP, RTP 等或目标内部通信协议入手，分析黑客的通信要素和信息内容，追踪黑客在网络中的行动轨迹。

2．如何成为一名深刻理解网络运维和安全防护的侦查员？

大型重要网络的运维和一体化安全防护，不再是过去网管员“重装系统、配置 DHCP、升级杀毒软件病毒库”的简单重复劳动。各类自动化运维系统和安全防御工具，定期对应用服务器、路由器、防火墙、网络设备、照相机和各种其他设备产生的事件日志中进行采集，获取特定时间、

特定系统/环境下的设备状态，并进行可视化的统计和格式化标准化处理。各类监控摄像探头的录像、登记记录、网络访问日志、无线接入点的日志、动态主机配置协议保留的地址分配日志、活动目录、域控制器、VPN 控制器等提供的日志、活动目录事件日志、Web 代理服务器日志以及目标电脑中可能会安装的位置追踪软件日志等，都是我们进行综合关联与分析的重要素材。多源日志信息的融合与关联分析将成为侦查员们的利器，我们将能够快速准确地定位黑客电脑的物理位置——移动设备联入建筑物里的哪个无线接入点？还可以通过跟踪移动设备联入各个 WAP 的情况，勾画出黑客设备移动的轨迹图；准确的时间和位置要素，能让我们从海量的监控摄像数据中迅速找到黑客的面部特征。

3．如何成为一名熟练运用系统架构思想和数据科学方法的侦查员？

互联网如此复杂，以至于我们已无法彻底分析和理解其工作模式。自其诞生以来，匿名性就是互联网的特质之一，甚至即便设备位于你掌握的组织内部时，准确定位到它也需要分析海量的网络文档和日志。当前的各种自动化运维（slunk）或安防设备（如 IDS）已经具有一定的统计处理和关联分析能力，但对于“黑客行为模式识别、攻击者分类、未来攻击动作预测、黑客总体实力评估”等更高等级的侦查工作仍然力不从心。我们仍然需要更加深刻地理解网络信息系统的架构，对海量的样本数据中主动的学习特征、建立模型，在机器学习、人工智能等科学方法的帮助下，在重重迷雾中抽丝剥茧，理清繁荣复杂的海量证据间关系。

相信读完本书，无论是大专院校计算机和网络安全相关专业的学生，还是公安网络安全保卫部门的一线侦查员，亦或国家网络安全应急响应单位的技术人员，都会大有裨益。末了，小生不才，也附送一句忠告：黑客和 APT 攻击者正变得越来越强大，侦查员们一刻都不能停歇，请尽快的进一步学习掌握基于大数据的智能化海量情报分析方法和技能，让犯罪者在我国的网络空间中无所遁迹。

张宇翔（ID：潜伏鹰）

2014.11.1.北京.

译者序

这是一本视角独特的电子取证书籍，令人耳目一新！

我自从 2002 年起从事电子取证工作至今已有十余年了，应该说这一行里几乎一直不停地涌现出新的技术、思路，你看嘛：

十几年前，几乎所有的取证书籍讨论的都只有一件事——数据恢复/文件系统分析。好像凭着一手数据恢复技术就能包打天下了。2005 年出版的 *File System Forensic Analysis* 是个巅峰，至此文件系统分析技术已经非常成熟了，并出现了各种傻瓜式的工具。毫不夸张地说，现在用一样的工具，一个初出茅庐的新手做数据恢复，得到的结果已经和老鸟们差不多了——到停滞期了？才不是呢！

接下来的几年时间里，各种奇招、怪招、损招层出不穷。拿注册表里的各种信息（比如通过注册表里缓存的驱动信息，倒推计算机上曾插过几个什么样的 USB 设备），分析内存中的数据（找被 rootkit 隐藏的进程/数据），分析应用程序存储下来的信息（比如拿各种 IM 工具的聊天记录），对应用程序/病毒木马本身进行分析从中获取信息（比如上海 2009.7.18 私车额度拍卖网站遭 DDOS 攻击案，就是我通过分析攻击用的木马破获的），等等不一而足。我本人也分别在 2008 年和 2012 年在安全焦点峰会上提出过利用信息熵分析重构 raid 5 阵列和针对单个文件（而非文件系统）做数据恢复的两个思路，也曾和一些朋友合作翻译出版了《Windows 取证分析》一书，综述了当年 Windows 平台下的取证技巧。

不过，这条路貌似又有点……，单机平台上能挖的地方基本上都已经过了一遍了，再要找点新鲜的实在是难啊……

上面的历史经验告诉我们，每到这样的关头就会有全新的思路出现。问题是这个全新的思路是什么呢？是 Android/iOS 平台？当然这是非常有可能的，不过不要忘了还有另一个重要方向——网络取证，也就是本书的主题。

任何技术要发展都离不开天时、地利、人和。天时者，时代大背景也。目前移动网络、物联网等网络技术的发展普及是所谓“天时”，正如第 1 章中的那个案例那样，现在丢个手机都能通过单位内部的 Wi-Fi 热点日志寻踪，这在以前是不可想象的。离开这个背景去谈网络取证都是扯；地利者，所需的各类设备上取证技术的成熟。网络设备种类繁多，但随着近年来网络设备的普及，这些设备的操作方法也不再是少数人的专利了，越来越多的人能玩转这些设备是基础；人和者，

人的观念。自从内存取证的概念被提出来之后，证据的易灭失等级就开始受到了大家的重视。[①]传统的计算机取证的眼光囿于计算机单机设备，我们的思路总是从某一台具体的设备入手进行分析的。尽管我们也强调电子现场的还原，但那也仅仅是囿于某台设备内部状态的保护和分析。有人说，具体办案时不是一样会把各台设备中获得的信息串到一起分析吗？这不就是网络取证吗？还真不一样！因为网络取证是把网络整体看作一个现场的高度。这个高度的上升立马导致你分析问题的思路发生了变化。现在你会考虑各个设备上证据的易灭失等级，容易灭失的先取，不容易灭失的后取。而不像以前看到一台设备，不分析网络就拉起袖子开始干活了，结果导致因为没有及时勘查载有易灭失证据的设备而造成证据的永久性丢失。在这方面，本书作者提出的 OSCAR 方法绝对是个亮点。

也正是由于这些原因，这本 *Network Forensics: Tracking Hackers through Cyberspace* 自从 2012 年 6 月出版后，在 Amazon 上一直深受好评排名居高不下。我有幸读到这本书，并将其推荐到国内，深感压力。

本书的翻译团队是个非常强大的团队，有经验丰富的鉴定师（拥有公安部和司法部认证的电子数据鉴定资质的鉴定人各一名），也有来自一线的技术支持人员和网络安全保卫实战单位的办案民警，还有教学经验丰富的外语专业教师。这也是一次公安专业院校与地方网络安全/电子取证专业团队合作的尝试。全书十二章内容翻译的分工安排如下：

第 1 章由武晓音同志翻译，第 2 章由龚济悦同志翻译，第 3 章由殷方同志翻译，第 4、5、6、7、8、9 章由上海弘连网络科技有限公司的陆道宏同志及数字犯罪调查小组（DCI）的沈永安、罗鸣和蹇星亮同志翻译，第 10 章由王宏同志翻译，第 11、12 章及剩余其他部分由我翻译。全书由我和陆道宏同志统一审校。除陆道宏、沈永安、罗鸣和蹇星亮同志之外的其他译者均为上海公安高等专科学校信息化、涉外警务等教研室的教师教官。本书中文版的面世首先要感谢各位译者付出的辛勤劳动。

其次，我要感谢博文视点的各位编辑老师，特别是顾慧芳、刘皎老师，感谢你们对我的一贯支持和耐心的指导，使我从中获益良多！同时也感谢你们为本书的出版所花费的大量时间！

当前，习近平总书记提出了“把我国从网络大国建设成为网络强国”的战略构想，2013 版的《中华人民共和国刑事诉讼法》中也首次将电子数据作为一种正式的法定证据类型。可以预见，网络安全-电子取证工作在我国将会有一个较大的发展。本书既可供广大从事电子取证教学和实际工作的人员阅读，也计划作为我校侦查专业第二本科电子取证类课程的参考资料使用。

崔孝晨

2014 年 5 月

---

① 所谓的易灭失等级是指证据的稳定性。就像传统的物证也会有灭失的现象，如尸体会腐烂、指纹会被擦除一样，有些电子证据在系统重启后会丢失（比如路由表），有些电子证据在断电之后会消失（比如内存中的信息），而有些电子物证只有当有数据写入时才会丢失（比如硬盘未分配空间里的数据）。

序

我的曾祖父是个木匠。我现在就趴在他做的桌子上，坐着他做的椅子写这篇序。他的世界是一门手艺，“熟能生巧”[①]。他生命后期的作品，即使表面上看是个与某个早期作品一样的东西，但旁人仍能看出他技艺的精湛。

网络安全的特点是其革新速度——不光是迅速增长的进步，还有那些时不时冒出来的“惊喜”。用数学术语说，网络安全的“功系数”是不断被技术进步打断的阶梯函数的积分。我的祖先在提高他的技艺时，可不会受困于胡桃木、钢铁或亚麻籽等原材料性状的改变，但在现如今提升网络安全水平时可没有这么好运。

乍一看，取证好像只是为解释已经发生的事而做的简单活计，因此还显得有些矫情。但事实并非如此，究其原因在于它的复杂性。这个复杂性是逐渐积累起来的。而且，就像作者在一开始说过的那样，如果积累足够多的话，即便只是一个最简单的网络，想知道其中发生的所有事也会变得不可能。因此，取证的目的就在于揭示那些发生在网络及其基础设施上的，有意义的，先前不为人知的重要因素。只有在知道了这些因素之后，将来才真正有改进的机会。

取证是一门艺术，勤能补拙。取证的发现过程就在于排除正在调查的事件的可能成因。就像雕刻时，我们的目的就是去掉所有使它看上去不像一头大象的多余石料一样，取证也是要去掉所有经观察并不成立的假说，并最终得出结论。套用 EF 舒马赫的观点，取证是个收敛的问题；但网络安全却是个发散的问题。换而言之，在取证中付出的努力越多，解的集合就越趋向于某一个答案，但这一结论在一般的网络安全问题上却不成立。

或许我们应该说：取证不是一门关于安全的学科，而是一门关于“不安全”的学科。安全是关于所有潜在的事件的，正如 Peter Bernstein 的定义：“风险就是诸多难以预见的情况”。取证不必从越来越复杂的事实中归纳出各种可能性，只须推导出其“何以至此”的原因即可。然而，一般来说，在网络安全中，犯罪分子总是有一种先天的优势，而在取证中，是防御者拥有这一优势。

取证是门艺术，“真的假不了，假的真不了”是它天生具有的战略优势。对你（现在或将来的取证人员）来说，你的任务就是在你拥有战略优势的地方提高你的技艺——不光是理论上的，还要有实际操作技能。这就是你需要这本书的原因。

---

① “WordNet Search—3.1,” Princeton University, 2011. http://wordnetweb.princeton.edu/perl/webwn.

技精于学生是老师的义务，而“青出于蓝而胜于蓝”同样也是学生的责任。但是在变成顶尖高手之前，你还是需要老师的教导，超越他们并非易事。说到底，技艺非凡的大师能让你知道当前的工具箱中哪些东西是一直能用的，哪些是随着时代的进步可能被淘汰掉的。他同样也能清楚地知道，你缺些什么。从这个角度来讲，这本书的篇幅安排绝对是大师所选。

基本上，由于每起案件案情的不同，各个案件的取证调查过程中，各自所需的工具集也都不尽相同，所以最好的办法就是拥有所有会用到的专业工具，当然其中的一些工具的使用频率会高于其他工具。将工具集的作用发挥到极致的前提是：你深入了解其中的每个功能，当然，这并不是说你需要而无须经常使用其中的每一个工具。Nicholas Taleb 是这样描述 Unberto Eco 的逆图书收藏主义的：“……应该在你的经济状况、按揭利率以及不动产资产允许的情况下，尽可能多地收集你所不了解的资料。”[①]

你，亲爱的读者，能拿到这样一本与众不同的取证书籍，且读且珍惜！

Daniel E. Geer, Jr., Sc.D.

① 这一段的理解应该参考这篇文章 http://ruchir75.blogspot.com/2008/01/umberto-ecos-anti-library.html。大意是说，一般的图书收藏是收藏已经看过的书（把看过的书放在一起，因为看过的书实在太多了，就变成图书馆了），而 Eco 是收藏那些他没有看过的书或不了解的相关研究领域的书籍的。所以把 anti-library 译为“逆图书收藏主义”。——译者注

前　言

每天，互联网上流经的比特数比世界上全部沙滩上的所有沙子还多。根据思科 Visual Networking Index，截止到 2011 年，全球的 IP 流量预计会达到每天约 8.4×10^{18} 比特。而据夏威夷大学的数学家们估算，世界上全部沙滩上的所有沙子都加起来也不过只有约 7.5×10^{18} 颗。按思科的估计，全球 IP 流量的年增长率是 32%，所以当你读到这一段时，每天流经互联网的比特数可能已经远远超过世界上全部沙滩上的所有沙子数了。①②③

当然这些估算都是非常粗略的。因为这两个例子中所涉及的系统之大，之复杂，已经远远超过了人类的工具所能量化分析的范围。互联网早已过了我们可以完全分析和理解其工作模式的时代了。我们可以深入剖析它的某一部分，也可以做一个宽泛的概括，但事实是：我们人类已经创造出了一个能力和复杂度远远超过我们的理解能力的庞然大物。

在这一环境下，出现了一个新兴的，目前还看不到其发展尽头的研究领域——网络取证。一般来说，取证就是“把科学知识应用在法律问题上，特别是对（比如来自某个犯罪现场的）物理证据进行科学分析”。因此，网络取证就是指：通常应用在司法问题上的，对基于网络的证据进行的科学研究。当然，网络取证并不是一个脱离具体案情的研究领域，而且许多专为司法调查而做的学科前沿进展、工具和技术同样可以用于社会学研究、历史分析以及网络环境的科学探索。在本书中，我们力图提供一个不光对肩负完成司法调查任务的专业网络取证分析师有用，也对学生、独立研究员以及其他所有对此感兴趣的人士具有实用价值的技术基础。

0.1　不断变化着的土壤

互联网是变化无常的。每当硬件或软件上开发出了一种新的特性时，就会有反映这些变化的新协议出现，而老的协议也会被修订或更新，以适应最新的技术。在过去的这个世纪里，在我们见证下，涌现出来的新协议有：分布式点对点视频聊天系统、在数千英里之外为患者远程动手术

---

① Cisco estimates the total global IP traffic for 2011 at 28,023 petabytes per month. Dividing this by 30 days in one month, we get approximately 8.4 * 1018 bits each day.

② “Networking Solutions,” Cisco, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ ns705/ns827/white paper c11-481360 ns827 Networking Solutions White Paper.html.

③ Howard McAllister, “Grains of Sand on the World’s Beaches,” 21st Century Problem Solving, http://www.hawaii.edu/suremath/jsand.html.

的协议，以及能绕过半个地球操纵机器人的协议。

对于熟悉传统的文件系统取证技术的调查人员来说，网络取证看上去是那么令人望而却步。相对于动辄成百上千种的网络协议，被广泛使用的文件系统格式也就那么寥寥几种。在 Windows 系统中一般就是 FAT32 或 NTFS 文件系统，在 UNIX/Linux 系统中，常见的也就是 ext2, 3, 4, ZFS, 或是 HFS+文件系统。相反，如果随意指定一个网络，你可以在上面发现以太网，802.11b/g/n, ARP, DHCP, IPv4, IPv6, TCP, UDP, ICMP, TLS/SSL, SMTP, IMAP, DNS, HTTP, SMB, FTP, RTP 等许多许多的协议。

在互联网上，也没什么能保证你遇到的协议一定会符合文档规定，或者能马上找得到文档。此外，协议实现的细节也会经常变化。厂商们不会纠结于任何标准，为了能最佳适配他们的产品，在实现协议时他们会在软件或硬件上随心所欲地进行修正。

有时，协议的开发过早，或在协议发展成熟到能支持协议中所有特性之前，就需要编写出应用程序。在这一过渡阶段，相关协议或者特定的字段可能会被闲置，或者被销售商、标准委员会或黑客挪作他用。而当环境发生变化，旧的协议不再能正常工作时，协议也会被替换掉。这方面的一个完美例子就是 IPv4。这个协议在最初相对较小的环境中工作良好。IPv4 设计时使用 32 位的一个字段来存放源和目的地址，它能容纳 2^{32} 或者说大约 43 亿个不重复的地址。而在互联网发展的早期，这一地址方案中的大网段是分配给用户相对较少的不同的组织的。现在，有超过十亿人连在互联网上，对于这一需求，32 位的地址空间就显得相当窘迫。因而，就开发出了拥有大得多的 128 位地址空间（2^{128}，或者 3.4×10^{38} 个不重复的地址）的 IPv6。随之涌现出来的还有许多其他协议，比如 Teredo（这个协议是用来在只支持 IPv4 的网络中隧道连接 IPv6 流量的）。

当协议发生变化时，取证工具也会随之改变或修正。一个 2010 年编写的工具可能无法正确解析 2002 年抓下来的某个数据包，反之亦然。有时这些错误可能会非常微妙，甚至可能无法被察觉。所以对于调查人员来说，理解取证工具的工作原理，并能深入到最底层验证所发现的结果是非常重要的。网络取证专家必须是技能高超、积极性高并有丰富经验的人员，因为别人编写的工具并不总能帮助你正确地解释结果，甚至无法在法庭上完成结果的验证。

把这些问题综合起来的是各种不同的海量的网络设备，其中有路由器、交换机、应用服务器等，任何一个给定网络中的每一个系统都可能会有唯一的配置、接口和功能。对于调查人员来说，是不可能熟悉所有的网络设备的——甚至只是其中百分之几都不现实——包括现在和过去生产定型的设备。相反，网络调查人员必须准备好，要在较短的时间内学会和掌握相关设备的使用方法。同时还要自信满满地管理调查和项目的进展。这简直就是在走钢丝。

在第一时间里追踪到需要检查的设备会是非常困难，甚至是不可能的。自其诞生以来，匿名性就是互联网的特质之一。有时，一个 IP 地址很可能会落到一个外地 ISP 那里，这时从第三方那里拿到更进一步的位置信息基本就是不可能的了——特别是当这个 IP 地址落到了一个安全立法宽松的其他国家时尤为如此。甚至即便设备位于你能掌控的组织内部时，准确定位到它的物理位置，也需要分析海量的网络文档和日志——这些东西可不保证能完全满足取证所需。随着移动

网络的兴起，追踪设备的位置常常就像是捉迷藏游戏，而在这场游戏中，占得先机的总是（甚至可能是在无意间）移动设备的用户。

问题的关键是要把互联网的这些功能看作生态系统。它不受任何中央势力的控制，也不会像我们设计一辆汽车那样被“设计”出来。当你检查网络流量时，没有人能告诉你可能会遇到什么，或者你的工具是不是能正确地解析你的抓包文件中，某个特定版本的协议。当你需要从网络设备中收集证据或重新配置它们时，你可能不得不研究特定型号的设备，才能正确理解接口和证据来源。当你需要定位某些系统时，你或许不得不满世界地做布朗运动，去追踪一台移动设备，或者给许多不同国家里的 ISP 联系人和执法官员打电话，才能准确定位源头。

没有规定大家都一定要使用哪家厂商生产的设备，也没有全球所有用户都必须遵守的规则，更没有哪本手册能准确地告诉你该怎样开展调查工作。

0.2 组织结构

本书力图能最大限度地囊括网络取证中的所有最重要的主题。全书共分为 4 个部分：《基础篇》、《数据流分析》、《网络设备和服务器》和《高级议题》。

0.2.1 第一部分 基础篇

第一部分《基础篇》中涵盖的是证据处理、网络和设备获取的基本概念，为本书之后将要讨论的更高一级的主题打好基础。除了这几章里的相关主题之外，我们强烈建议所有的读者能很好地理解 TCP/IP 网络。W. Richard Stevens 编写的《TCP/IP 详解》一书是一本极好的书籍，我们强烈推荐你把它作为参考资料。

第一部分中包含以下章节：

- 第 1 章《实用调查策略》，展示了网络取证调查人员将会面临的大量挑战。介绍了电子取证中的重要概念，并给出了一个如何着手开展基于网络的调查的方法清单。
- 第 2 章《技术基础》，这一章里给出了通用网络组件的技术概览，以及它们在取证调查中的价值。同时也会依网络取证调查的背景给出协议和 OSI 模型的概念。
- 第 3 章《证据获取》，研究各种被动式和主动式的证据获取方法，其中包括使用软件或硬件嗅探网络流量，以及从网络设备中主动收集证据的策略。

0.2.2 第二部分 数据流分析

第二部分《数据流分析》中讨论各种可供调查人员分析网络流量的方法。我们从数据包分析开始讲起，从检查协议头部，到提取数据包的载荷，再到重构传输的数据。由于保留记录下来的数据流已经是一种司空见惯的事了，所以我们特意用了一整章的篇幅讨论对流记录的统计分析。再接下来会深入探究无线网络和 802.11 协议族。最后，我们将讨论设计用来实时分析流量、生成

报警以及在某些情况下能即时抓包的网络入侵检测和防范系统。

第二部分中包含以下章节：

- 第 4 章《数据包分析》，综合研究了各种协议、数据包及数据流，以及分析它们的各种方法。
- 第 5 章《流统计分析》，展示了一个日益重要的领域——静态流记录的收集、合并和分析方法
- 第 6 章《无线：无须网线的取证》，讨论无线网络，特别是在 IEEE 802.11 协议族中的证据收集和分析技术。
- 第 7 章《网络入侵的侦测及分析》，这一章回顾了专门用于生成安全报警，并支持证据固定的网络入侵防护系统和入侵检测系统。

0.2.3 第三部分 网络设备和服务器

第三部分《网络设备和服务器》中讨论了从各类网络设备中获取和分析证据的方法。一开始我们先讨论事件日志的收集和检查方法，还讨论了各种日志架构的优缺点。接下来，我们专门讨论对交换机、路由器以及防火墙——这些构成了我们网络骨干部分的设备的取证调查技巧。由于 Web 代理日趋流行，而且其中常常含有许多富有价值的证据，因此我们将详细讨论 Web 代理中证据的收集和分析方法。

第三部分中包含以下章节：

- 第 8 章《事件日志的聚合、关联和分析》，讨论从不同的源，包括从服务器或工作站的操作系统（比如 Windows、Linux 和 UNIX）、应用程序、网络设备和物理设备中，收集和分析日志的方法。
- 第 9 章《交换机、路由器、防火墙》，研究如何从不同的网络设备中收集证据，以及根据不同的接口和证据的易灭失级别，收集证据的策略。
- 第 10 章《Web 代理》，回顾了 Web 代理日益流行的趋势，以及调查人员如何利用这些设备收集上网冲浪的历史记录，甚至是缓存下来的 Web 对象的副本。

0.2.4 第四部分 高级议题

第四部分《高级议题》讨论了网络取证中最令人着迷的两个议题：网络隧道和恶意软件。我们将回顾网络隧道的合法性和隐蔽性，并讨论处理不同类型隧道时的调查策略。为了使叙述内容完备，我们还将回顾恶意软件的发展历史及其对取证分析产生的影响，其中包括命令和控制信道的进化史、僵尸网络、规避 IDS/IPS 的检测以及高级持续性威胁（Advanced Persistent Threat，APT）

第四部分包括以下章节：

- 第 11 章《网络隧道》，讨论了网络隧道的合法性和隐蔽性，识别隧道的方法以及重构经隧

道传输的流量中的证据的策略。

- 第 12 章《恶意软件取证》，在这一章里将概述恶意软件开发的简史，包括命令和控制信道的进化、僵尸网络、规避 IDS/IPS 的检测以及高级持续性威胁（APT）。在这一过程中，我们还将穿插讨论恶意软件对取证调查的影响，以及取证调查是如何改变恶意软件的。

0.3 工具

本书内容的编排面向最广大的读者，教你网络取证的基本原则和技术。尽管有许多商用的、点点鼠标就能帮助你找到同样答案的工具，而且我们在书中也会泛泛地介绍其中的一些。但是我们还是着重介绍那些可以免费获得，同时也能用来演示基本技术的工具。通过这一方式，我们希望能让你理解取证工具的底层工作原理，拥有验证自动化工具得出的结论，以及在调查过程中选用正确工具的能力。

0.4 案例

第二、三、四部分的每一章中都会安排一个详细的案例，用以展示这一章中讨论的工具和技术。你可以把证据文件下载到你自己的取证工作站中，并亲自动手分析它们。

这些案例中的证据文件位于：

http://lmgsecurity.com/nf/

你可以免费使用它们，但仅限于个人使用。

0.5 勘误表

任何一本这么厚、信息量这么大的书中，都不可避免地会有一些错误，我们把勘误表放在下面这个网址中：

http://lmgsecurity.com/nf/errata

如果你找到了一个错误，我们将很高兴能知道它，请给我们发送电子邮件：errata@lmgsecurity.com。不过在写信之前，请先对照一下勘误表，不要重复发送勘误表上已有的内容。

0.6 最后一点说明

本书是爱的结晶。每一章都花掉了无数研究、讨论、质疑和写作的时间。在编写案例及相关抓包文件时，我们专门构建了一个相当于一个小型商务网络的实验室。在每一次练习、编写每一

个场景时，我们都反复配置/重新配置这个网络，然后一遍又一遍地运行相关场景，直到得到的所有结果都完全正确为止。

无数个白天黑夜，无数次反复开关的断路开关，无数块挂掉的硬盘，无数罐放温了的啤酒和无数块放凉了的比萨——最终成就了本书。尽管这本书已经有几百页厚了，但我们仍旧觉得我们只是泛泛地介绍了博大精深的网络取证工作中一些肤浅的内容。我们从付出的艰苦劳动中学到了很多东西，希望你也是。

致　谢

如果没有两位广受尊敬的安全专家：Rob Lee 和 Ed Skoudis 的支持，这本书不可能问世。三年前，Rob Lee 拉我们去为 SANS 协会开设一门网络取证课程。这是我们第一次把共同的才智交汇在这个主题上，并正式给这一工作的主体起了个名字。打那以后，Rob 就成了我的良师益友，不断推动我们改进工作，吸取反馈意见以及拓展我们知识的极限。Rob，感谢你的高标准、开诚布公的意见，以及最重要的——对我们的信任。没有你，我们不可能完成这本书。

还有 Ed，是你鼓励我们写出了这本书，并花时间把我们介绍给你们的编辑。在这一过程中，你的建议被证明是无价的。感谢你的帮助和支持，Ed，我们会永远感激你。

感谢为出版这本书花了大量的时间和精力的 Pearson 出版社的全体工作人员，特别是本书的编辑老师 Chris Guzikowski，同时还有 Jessica Goldstein, Raina Chrobak, Julie Nahil, Olivia Basegio, Chris Zahn, Karen Gettman, Chuti Prasertsith, John Fuller 和 Elizabeth Ryan 老师，在此一并感谢。同时也特别感谢 Laserwords 团队为本书的出版付出的努力，特别感谢 Patty Donovan 的耐心指导。

非常感谢 Jonah Elgart 为本书创作的精美封面。我们也非常欣赏本书序言的作者 Dan Geer 博士的工作。另外，我们也非常感谢为本书进行技术审校的朋友和同仁们，他们是：Michael Ford, Erik Hjelmvik, Randy Marchany, Craig Wright 和 Joshua Wright。他们的意见和对细节的关注为本书增辉无限。

我们也想把欢呼送给我们 LMG Security 团队的优秀的组员们，特别是 Eric Fulton, Jody Miller, Randi Price, Scott Fretheim, David Harrison 和 Diane Byrne，你们在帮助我们进行网络取证技术研究和课程开发上花了大量的时间。Eric Fulton 是 ForensicsContest.com 网站上多个谜题的编写者，本书中的一些案例，特别是“HackMe”和“Ann 的极光行动”，就是从这些谜题那里发展而来的。Jody Miller，在你冲进来，摆平了骷髅王的邪恶魔力之后，你就成了我们的硬汉——呃，我是说，你统一了本书所有注释的格式（将近 500 行！）。

感谢我们的朋友、同事以及教导了我们多年的导师：Shane Vannatta, Marsha&Bill Dahlgren, Pohl Longsine, Gary Longsine, John Strand, Michael P. Kenny, Gary & Pue Williams，（美国）中西部的好乡亲们，Mike Poor, Kevin Johnson, Alan Ptak, Michael Grinberg, Sarah & Kerry Metlen, Anissa Schroeder, Bradley Coleman, Blake Brasher, Stephanie Henry, Nadia Madden 和 Jon McElroy, Clay Ward，麻省理工学院学生信息处理板（Student Information Processing Board，SIPB），Wally Deschene, Steven & Linda Abate, Karl Reinhard, Brad Cool, Nick Lewis, Richard Souza, Paul Asadoorian, Larry

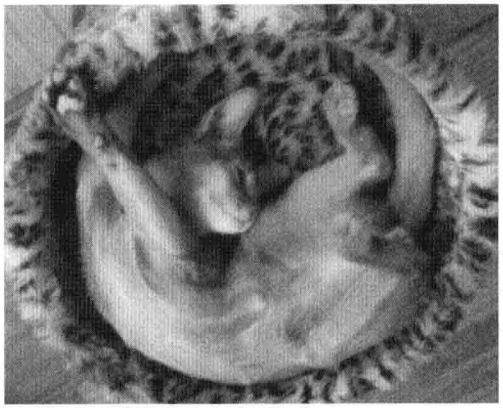
Pesce, George Bakos, Johannes Ullrich, Paul A. Henry, Rick Smith, Guy Bruneau, Lenny Zeltser, Eric Cole, Judy Novak, Alan Tu, Fabienne van Cappel, Robert C de Baca, Mark Galassi 和 Dan Starr。

特别感谢 SANS 协会的教职员工，尤其是：Steven & Kathy Northcutt，Deb Jorgensen，Katherine Webb Calhoon，Lana Emery，Kate Marshall，Velda Lempka，Norris Campbell 和 Lynn Lewis。

我们也要感谢每一位在 ForensicsContest.com 上做出过贡献的人——不论您是原创了工具/文章，回帖，还是只是为了好玩才来的。我们都从你们身上学到了很多！

感谢在本书编写过程中一直鼓励和支持我们的家人，特别是：Sheila Temkin Davidoff, E. Martin Davidoff, Philip & Lynda Ham, Barbara & Larry Oltmanns, Laura Davidoff, Michele Kirk, 和 Naomi Robertson, Latisha Mike, Makenna, Braelyn Monnier, Chad, Amy, Brady Rempel, Sheryl & Tommy Davidoff, Jonathan & Stefanie Davidoff, Jill & Jake Dinov, Jamie & Adam Levine, Annabelle Temkin, Norman & Eileen Shoenfeld, Brian & Marie Shoenfeld，以及 Debbie Shoenfeld。

感谢我们的小猫——Shark，在我们写作的这上百个小时里，你一直依偎在我们身边。



最重要的——感谢我们的两个女儿：Charlie 和 Violet，这本书是写给你们的。