E-Crime and
Computer Forensics Training Course

信息犯罪与计算机取证实训教程

王永全　廖根为　涂　敏◎主编

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

E-Crime and
Computer Forensics Training Course

信息犯罪与计算机取证实训教程

王永全　廖根为　涂　敏◎主编

人民邮电出版社
北京

图书在版编目（CIP）数据

信息犯罪与计算机取证实训教程 / 王永全，廖根为，涂敏主编. -- 北京 : 人民邮电出版社，2019.3
ISBN 978-7-115-49603-4

Ⅰ. ①信… Ⅱ. ①王… ②廖… ③涂… Ⅲ. ①计算机犯罪－证据－数据收集－高等学校－教材 Ⅳ. ①D918

中国版本图书馆CIP数据核字(2018)第232876号

内 容 提 要

本书作为《信息犯罪与计算机取证》一书的配套实训教材，对其理论内容进一步拓展，实践性内容进一步充实。本书围绕信息犯罪与计算机取证这一主题，针对信息安全、信息犯罪、计算机取证、计算机司法鉴定、综合实训等问题进行了深入探讨，并分别设计了实践性内容引导读者锻炼或实验。内容主要包括：信息安全实验、信息犯罪讨论分析、计算机取证基础实验、计算机取证技术实验、电子数据证据的发现与收集实验、电子数据证据的固定与保全实验、数据恢复实验、电子数据证据分析与评估实验、计算机司法鉴定实验、案件综合实验等相关基础知识及实训内容，以进一步增强“信息犯罪与计算机取证”课程实践性环节的教学需要。

本书适用于计算机、信息安全、通信电子、网络安全与执法、法学、公安学等相关学科专业的本科高年级学生以及相关专业研究生、企事业单位及公检法司等部门工作人员作为教材或参考书使用。

◆ 主　　编　王永全　廖根为　涂　敏
责任编辑　邢建春
责任印制　彭志环

◆ 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
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：17　　2019 年 3 月第 1 版
字数：414 千字　　2019 年 3 月北京第 1 次印刷

定价：98.00 元

读者服务热线：(010) 81055488　印装质量热线：(010) 81055316
反盗版热线：(010) 81055315

本书编委会

主　编　王永全　廖根为　涂　敏

副主编　刘三满　唐　玲　王　弈

委　员（以撰写章节为序）

赵　帅　王永全　蒋　瑾　赵子玉

廖根为　田晶林　李　毅　明振亚

王　弈　赵　庸　徐志强　唐　玲

刘三满　涂　敏　段　莹

前　言

信息安全事关国家安全。对信息安全的保护包括事前、事中和事后保护。信息安全事件发生后，如何有效减少损失、及时追究责任人，需要运用计算机取证技术。在信息安全体系中，它是不可或缺的一个环节，发挥着不可取代的作用，是侦破信息犯罪的关键性技术。

作为一项应用实务型、交叉复合型学科领域，计算机取证的研究在我国尚未得到足够重视。总体来说，计算机取证基础理论匮乏、应用和实务操作不强。鉴此，我们根据理论、技术和实践的最新发展，重新编写了《信息犯罪与计算机取证》一书，并编写了本配套教材《信息犯罪与计算机取证实训教程》，力求理论性与实践性兼具，对主教材理论内容进一步拓展、实践内容进一步充实。

全书共 10 章，涵盖信息安全、信息犯罪、计算机取证、计算机司法鉴定、综合实训等方面实验，主要包括：信息安全实验、信息犯罪讨论分析、计算机取证基础实验、计算机取证技术实验、电子数据证据的发现与收集实验、电子数据证据的固定与保全实验、数据恢复实验、电子数据证据分析与评估实验、计算机司法鉴定实验、案件综合实验等相关基础知识及实训内容，与主教材《信息犯罪与计算机取证》的主要章节基本对应，以进一步增强《信息犯罪与计算机取证》课程实践性环节的教学需要。

本书第 1 章设计了若干信息安全实验，可作为信息安全系统性学习的引导；第 2 章精选了若干信息（网络）犯罪案例供学生讨论，要求能够准确对其进行法律认定；第 3 章为计算机取证基础实验，对常见的计算机取证工具进行了介绍，并设计了相关实验供学生锻炼；第 4 章为计算机取证技术实验，重点训练学生电子数据搜索、提取和远程取证的基本技能；第 5 章为电子数据证据的发现和收集实验，涵盖 Windows、Linux、Mac OS、Android、iOS 等操作系统的取证；第 6 章为电子数据证据的固定和保全实验，提供了 Hash 实验、硬盘复制机和软件镜像工具的实验；第 7 章为数据恢复实验，包括 FAT 文件系统和 NTFS 文件系统的分析，以及较为复杂的被删除文件的数据恢复的操作训练；第 8 章为电子数据证据的分析和评估实验，介绍事件过程分析、人员关联分析、证据保管链完整性评估这 3 种常见分析评估方法；第 9 章为计算机司法鉴定实验，提供了电子邮件真实性鉴定实验、恶意代码鉴定（功能分析）实验、软件相似性鉴定实验这 3 个实验；第 10 章为案件综合实验，以一个较完整的案例供读者锻炼和学习。

本书由主编王永全、廖根为拟定编写大纲并负责全书设计、统稿、校对和完善。

本书作者（以撰写章节为序）及其分工如下：赵帅第 1 章，第 6 章 6.1.2 节，第 10 章；王永全第 2 章 2.1 节、2.2 节，第 8 章；蒋瑾第 2 章 2.3 节、2.4 节，第 5 章 5.1.2 节；赵子玉第

3 章 3.1 节、3.5.2 节；廖根为第 3 章 3.2~3.4 节，第 4 章，第 5 章 5.2.2 节、5.3 节、5.4.2 节、5.5.2 节，第 6 章 6.2 节、6.3 节，第 7 章 7.1 节、7.2 节、7.3.1 节，第 9 章，第 10 章；田晶林第 3 章 3.5.1 节；李毅第 3 章 3.6.1 节、3.7.1 节，第 9 章 9.3.2 节；明振亚第 3 章 3.6.1 节、3.7.1 节；王弈第 3 章 3.6.2 节、3.7.2 节；赵庸第 5 章 5.1.1 节、5.2.1 节；徐志强第 5 章 5.1.1 节、5.2.1 节、5.4.1 节；唐玲第 5 章 5.2.1 节、5.4.1 节、5.5.1 节；刘三满第 5 章 5.4.1 节、5.5.1 节；涂敏第 7 章 7.1.2 节、7.2.2 节；段莹第 6 章 6.1.1 节，第 7 章 7.3.2 节。

本书在撰写过程中，作为“2018 年度上海高校市级精品课程”《信息犯罪与计算机取证》的配套实训教材以及上海市教育委员会 2013 年度市教委本科重点专业（特色）核心课程建设项目的成果之一，得到了华东政法大学以及各参编人员所在单位或部门领导的支持、关心、帮助和鼓励，在此表示衷心感谢！作者赵帅、田晶林、段莹和赵子玉除了完成各自撰写的内容外，还为本书的部分资料收集与实验验证做了相关工作，在此予以感谢！另外，本书的编辑出版得到了 2014 年国家社会科学基金重大项目（第二批）“涉信息网络违法犯罪行为法律规制研究”（No.14ZDB147）、江西省经济犯罪侦查与防控技术协同创新中心、山西省“1331 工程”重点学科建设计划（No.1331KSC）以及“山西警察学院创新团队”建设项目的支持，在此一并表示衷心感谢！

限于时间、经验和知识水平等因素，书中难免存在一些不足甚至错误，尚祈读者能够多提供宝贵意见，以资日后进一步完善。另外，如需要实验素材，可通过邮箱 forensics2019@sina.cn 获取。

编　者

2018 年 10 月

目 录

第1章 信息安全实验

随着互联网应用广度和深度不断延伸，越来越多的计算机连接到互联网上，这对信息系统的安全提出了更高要求，由单个节点扩展到局域网、广域网，直至整个互联网。网络不仅让世界互联互通，而且突破了人与人沟通上的技术阻隔，打破了传统方式交流的隔阂，在时空和逻辑关联上融合得更加紧密。但随之产生的网络安全、信息保障问题喷涌而出，如“斯诺登事件”暗示着国与国之间的网络信息战争，各种电商平台的用户信息泄露事件表明网络用户隐私数据保护的脆弱性问题，“永恒之蓝”病毒的肆意传播反映出网络用户对数据安全保护意识的缺失等问题，由此可见，信息安全与众多网络用户的合法权益和实际利益息息相关，在这样一个对抗性的领域中，有实施不法行为的破坏者，也就需要有技术能力的守护者。

应用是学习的目的，实验是应用的基础。要想做好信息网络的守护者，必须注重理论与实践相结合，针对这一要求，本书介绍涉及信息犯罪与计算机取证实训相关的理论基础和技术实验。本书给出相关实训内容，并列出实验目的、实验环境和工具、实验过程、实验现象与分析等，旨在加深对信息犯罪与计算机取证理论的理解，培养实践创新能力。

信息安全涉及的范围较广，不仅包括信息基础设施的安全、信息运行的安全，还包括信息内容的安全、信息价值的安全等。从信息系统安全体系角度看，它包括物理安全、节点安全、通信安全以及安全管理等内容。因而，信息安全外延远远超越了技术范畴。本章介绍信息安全实验，就网络安全检测、网络安全攻防和加密解密技术进行初步讨论和实训，希望通过本部分实验为深入系统地学习信息安全知识提供指引。

1.1 网络安全检测

在网络信息系统中，因意外或者恶意的某种外部或内部原因，威胁并实际破坏网络系统运行，甚至切断服务、窃取数据、影响网络生态安全的行为时有发生。因此，需要针对这些影响因素开展系统性的保护措施，包括事前的积极预防，事中的实时监测，事后的修复补漏。其中，网络安全检测是贯穿整个网络安全保护活动的重要手段和方式。

1.1.1 网络安全检测基础知识

1. 网络安全检测的基本概念

网络安全检测是通过收集和分析网络行为、安全日志、审计数据、其他网络上可获取信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。网络安全检测作为一种积极主动的安全防护技术，在网络系统受到危害之前拦截和响应入侵，提供防范内部攻击、外部攻击和误操作的实时保护。

网络安全检测技术可以分为静态安全技术（如防火墙技术）和动态安全技术（如网络入侵检测技术）。入侵检测作为防火墙防御的补充，实时应对网络入侵攻击，极大地扩展了网络系统管理人员的综合管理能力（包括监视、识别进攻、安全审计、应急响应），也提高了网络安全基础结构的完整性。以下对网络安全检测原理和分类的介绍侧重于后者的介绍。

2. 网络安全检测的技术原理

从动态安全技术角度看，存在两种不同的检测思路：异常检测和特征检测。

异常检测（Anomaly Detection）的假设是入侵者活动异常于正常主体的活动，是指使用者根据使用资源状况的正常程度判断入侵与否，根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。这种检测方式不针对某个特定行为，其难点在于如何建立“活动简档”以及如何设计统计算法，从而把不正常的操作作为“入侵”或忽略真正的“入侵”行为。异常检测方法首先定义一组系统处于“正常”情况时的数据，如 CPU 利用率、内存利用率、文件校验和等；然后进行分析确定是否出现异常。常见方法有概率统计法、神经网络法、计算机免疫技术等。

特征检测（Signature-Based Detection）又称误用检测（Misuse Detection），这一检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但对新的入侵方法无能为力，其难点在于如何设计模式既能够表达“入侵”现象又不会将正常的活动包含进来。具体方法是挖掘并提取网络传输中数据特征，对提取的数据特征进行信息识别、分类和学习，结合检测算法发现网络异常数据。

3. 网络安全检测的技术分类

（1）基于主机的安全检测（Host-based Security Detection）

基于主机的安全检测是侦测单个主机的各项表征数据源，如系统审计和日志记录，实时监控和记录系统异常操作，包括异常登录、越权访问、错误读取。这种类型的检测系统优势是不需要额外的硬件，定期扫描检查，监听主机端口活动，可以迅速做出响应，及时向管理员报警；劣势是依赖主机性能，占用主机自身资源，不能检测网络攻击，保护范围有局限性，分析检测成本可能随着主机数量而线性增长。

（2）基于网络的安全检测（Network-based Security Detection）

基于网络的安全检测通过监听网络传输的原始流量，提取数据包中有用的信息特征值，对比已知攻击特征或者匹配原型的正常特征值，侦测和识别攻击事件。与基于主机的安全检测区别是，它将关联各主机，通过探测器（专用主机，其网卡设为混杂模式）监视网段流量，然后通过管理站接收从探测器传来的警报，提示管理员及时采取防范措施。此类检测系统优势是不依赖单机的操作系统作为检测资源，可应用于不同的操作系统平台；配置简单，不需

要任何特殊的审计和登录机制；可检测协议攻击、特定环境的攻击等多种攻击。劣势是只能监视经过本网段的流量活动，无法得到主机系统的实时状态，精确度较差。

（3）分布式安全检测

随着网速的极速提升，分析匹配数据包中的特征值所消耗的时间和资源越来越高，此外，还存在攻击特征库更新不及时，不能与其他网络安全产品兼容，不能适应多元化攻击方式下的攻击等问题。显然传统的检测方式不能满足安全需求，而分布式安全检测能够及时、可适应、跨平台地应用于不同场景。分布式安全检测系统的一般性结构包括 3 个组成部分：位于监控主机上的传感器、局域网上的局域网管理器以及中央数据处理器。主机上的传感器和局域网管理器分别从主机和局域网上采集有用数据，然后将数据送至中央数据处理区做全局的入侵检测。在分布式安全检测的体系结构上，检测模型是研究的重点，如哥伦比亚大学和北卡罗来纳州立大学提出基于数据挖掘的模型建立方法。

网络范围内的入侵检测系统必须协同工作，但并非所有检测系统都出自同一厂商，为了实现不同厂商检测产品之间的通信融合，应当制定标准化规范、通信数据格式和相应的规程。具体来说，建立入侵检测系统之间，以及入侵检测系统和网络系统之间通信的功能需求介绍，制定统一的系统体系结构。例如，美国国防部 DARPA 所资助的一个研究组，提出了统一入侵检测框架。

1.1.2　网络安全检测实验

实验一　配置 Linux 开源防火墙

1. 实验背景

netfilter/iptables 组合是 Linux 系统中常见的防火墙技术解决方案，其中，netfilter 是 Linux 内核的防火墙功能模块，iptables 是防火墙管理工具。netfilter 组件实现静态包过滤和状态报文检查，iptables 则是工作在 Linux 用户空间中的防火墙配置工具，通过命令行方式运行允许用户为 netfilter 配置各种防火墙过滤和管理策略。

使用用户空间，可以自定制规则，这些规则存储在内核空间的数据包过滤表中。这些规则具有目标功能，在内核中对来自某些网络源、前往某些目的地或具有某些协议类型的数据包进行处理。例如，如果某个数据包与规则匹配，那么使用目标 ACCEPT 允许该数据包通过。还可以使用目标 DROP 或 REJECT 阻塞并抛弃数据包。

2. 实验目的

理解防火墙基本工作原理，配置 Linux 系统防火墙，并进行以下测试。

（1）过滤 ICMP 数据包，使主机收不到 ping 包。

（2）只允许特定 IP 地址访问主机的某一网络服务，而其他的 IP 地址无法访问。

3. 实验要求

（1）安装 netfileter/iptables 工具组件。

（2）查看并记录本地主机的网络配置，扫描本地局域网状态。

提示：使用 nmap 查看。

（3）过滤特定 IP 地址，进行测试并记录测试结果。

提示性操作如下。

（1）安装 netfilter/iptables 组件

netfilter/Iptables 的 netfilter 组件是与内核集成在一起的，所以只需要下载并安装

iptables 用户空间工具。如果是 Linux 版本 7.1 或更高版本，就不需要执行安装组件步骤。该 Linux 分发版（distribution）的标准安装中包含 iptables 用户空间工具（本实验及以下实验使用了 Kali Linux 环境，可以使用其他 Linux 环境和版本，但具体操作可能略有差异）。

（2）查看当前本机网络配置以及局域网连接状况

攻击端网络配置如下。

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.126  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::20c:29ff:feb2:6251  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b2:62:51  txqueuelen 1000  (Ethernet)
        RX packets 1644577  bytes 1929033551 (1.7 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161828  bytes 61599390 (58.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2605  bytes 350902 (342.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2605  bytes 350902 (342.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

局域网状态如下。

```
# nmap -n -sn 192.168.0.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-08 09:44 HKT
Nmap scan report for 192.168.0.1 Host is up (-0.17s latency).
MAC Address: B0:95:8E:10:B8:6A (Tp-link Technologies)
Nmap scan report for 192.168.0.104 Host is up (0.020s latency).
MAC Address: 60:F8:1D:A7:30:D6 (Apple)
Nmap scan report for 192.168.0.105 Host is up (0.018s latency).
MAC Address: F0:C8:50:E2:1A:27 (Huawei Technologies)
Nmap scan report for 192.168.0.106 Host is up (0.012s latency).
MAC Address: 64:BC:0C:4D:90:A9 (LG Electronics (Mobile Communications))
Nmap scan report for 192.168.0.107 Host is up (0.11s latency).
MAC Address: 8C:25:05:38:32:89 (Huawei Technologies)
Nmap scan report for 192.168.0.108 Host is up (0.013s latency).
MAC Address: B0:48:1A:23:D5:01 (Apple)
Nmap scan report for 192.168.0.110 Host is up (0.11s latency).
MAC Address: 88:53:95:B4:D0:63 (Apple)
Nmap scan report for 192.168.0.111 Host is up (0.0048s latency).
MAC Address: 44:37:E6:D7:71:AC (Hon Hai Precision Ind.)
Nmap scan report for 192.168.0.114 Host is up (0.11s latency).
MAC Address: E0:94:67:3D:3D:DA (Intel Corporate)
Nmap scan report for 192.168.0.115 Host is up (0.097s latency).
MAC Address: 00:21:27:B4:5E:9E (Tp-link Technologies)
Nmap scan report for 192.168.0.116 Host is up (0.044s latency).
```

```
MAC Address: A8:C8:3A:3C:7A:F3 (Huawei Technologies)
Nmap scan report for 192.168.0.117 Host is up (0.00044s latency).
MAC Address: 7C:67:A2:59:8E:31 (Intel Corporate)
Nmap scan report for 192.168.0.121 Host is up (0.023s latency).
MAC Address: 88:28:B3:C0:B5:91 (Huawei Technologies)
Nmap scan report for 192.168.0.127 Host is up (0.020s latency).
MAC Address: E0:94:67:3D:3D:E9 (Intel Corporate)
Nmap scan report for 192.168.0.126 Host is up.
Nmap done: 256 IP addresses (15 hosts up) scanned in 6.15 seconds
```

（3）显示当前默认规则链

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

（4）测试 ping

```
root@kali:~# ping 192.168.0.117
PING 192.168.0.117 (192.168.0.117) 56(84) bytes of data.
64 bytes from 192.168.0.117: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 192.168.0.117: icmp_seq=2 ttl=64 time=1.19 ms
64 bytes from 192.168.0.117: icmp_seq=3 ttl=64 time=1.29 ms
64 bytes from 192.168.0.117: icmp_seq=4 ttl=64 time=1.25 ms
^C
--- 192.168.0.117 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6013msrtt min/avg/max/mdev = 0.499/1.095/1.334/0.268 ms
```

测试结果显示，此时可以 ping 目标端。

（5）过滤 ICMP 数据包，使主机收不到 ping 包

iptables 为用户提供配置 netfilter 规则的命令行接口，其命令语法为

```
$ iptables[-t table] command [match] [target]
```

其中，-t 指定配置规则所在的表，缺失表包括 filter、nat、mangle、raw 等。command 是规则指令，如插入规则、删除规则等。

本实验配置如下。

```
root@kali:~# iptables -A INPUT -p icmp -j DROP
```

其中，-A 表示将一条规则附加到链的末尾；INPUT 为规则链；-p 为命令设置链的缺省目标操作；-icmp 代表数据包类型；-j DROP 代表数据包与具有 DROP 目标操作（过滤）的规则相匹配，会阻塞该数据包，并不对其做进一步处理。

测试结果显示如下。

```
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
```

```
target     prot opt source               destination

root@kali:~# ping 192.168.0.117
PING 192.168.0.117 (192.168.0.117) 56(84) bytes of data.
^C
--- 192.168.0.117 ping statistics ---
52 packets transmitted, 0 received, 100% packet loss, time 52218ms
```

ping 结果显示无法连接。

4. 实验器材和环境

（1）netfilter/iptables。

（2）Kali 操作系统。

5. 实验思考

防火墙过滤数据包的基本原理是什么？

实验二　在 Linux 系统中配置开源网络入侵检测系统 snort

1. 实验背景

snort 有 3 种工作模式：嗅探器、数据包记录器、网络入侵检测系统。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上，通过./snort-vde 输出包头信息和数据信息。数据包记录器模式把数据包记录到硬盘上，可以通过./snort-vde-l ./log 将嗅探到的数据包记入指定的目录下，加上-b 可以以 tcpdump 二进制日志文件格式记录。网络入侵检测系统分析网络数据流以发现其中包含的攻击行为。

2. 实验目的

理解 snort 网络入侵检测模式的基本工作原理。

3. 实验要求

（1）正确安装 snort。

提示：若存在 snort 依赖安装包和库的缺失问题，可对应下载并安装。

（2）入侵检测测试，并记录测试结果。

提示性操作如下。

（1）安装 snort

若 Linux 最新发行版本已安装，则不执行以下步骤。如需，则安装目录可以统一设置在/usr/local/文件夹中，方便管理。

Snort 支持 Linux 和 Windows 等多平台，在 Linux 平台上，如 Ubuntu 或 Debian 发行版本可以通过 apt-get 自动获取安装包，Redhat 或 Cent OS 等发行版本可通过 yum 在线安装和升级 snort。

通过./configure&&make&&make install 安装 snort 工具需要提前解决依赖的源码包问题，如 libpcap 和 libpcre 等。以下为简要说明，如仍存在问题可通过网络搜索 snort 源码安装的具体步骤和问题解决方法：

① 在 tcpdump 官方网站下载 libpcap-1.8.1.tar.gz 软件包，通过命令 tar -zxvf libpcap-1.8.1.tar.gz 解压文件，并将其放入自定义的安装目录；复制/usr/local/lib/libpcap.a 到/usr/lib。

② 通过“Fast lexical analyser generator”在 github 中搜索下载 flex-2.6.4.tar.gz 软件包，

通过 tar -zxvf flex-2.6.4.tar.gz 解压文件，并将其放入上述自定义的安装目录中。

注：如果没有编译安装此文件，在编译安装 libpcap 时，会出现“configure: error: Your operating system's lex is insufficient to compile libpcap.”的错误提示。

③下载 bison-3.0.tar.gz 软件包，通过 tar -zxvf bison-3.0.tar.gz 解压文件，并将其放入上述自定义的安装目录中。

注：如果没有编译安装此文件，在编译安装 libpcap 时，会出现“configure: WARNING: don't have both flex and bison; reverting to lex/yacc checking for capable lex... insufficient”的错误提示。

④下载 m4-1.4.18.tar.gz 软件包，通过 tar -zxvf m4-1.4.18. tar.gz 解压文件，并将其放入上述自定义的安装目录中。

注：如果没有编译安装此文件，在编译安装 bison-2.4.1 时，会出现“configure: error: GNU M4 1.4 is required”的错误提示。

而后依次进入目录 m4、bison、flex、libpcap 并执行以下命令。

```
(sudo) ./configure
(sudo) make
(sudo) make install
```

⑤ 安装最新的 lib 库，下载 pcre-8.38.tar.gz 软件包，通过 tar -zxvf pcre-8.38.tar.gz 解压文件，并将其放入上述自定义的安装目录中；下载 libdnet-1.11.tar.gz 软件包，通过 tar- zxvf libdnet-1.11.tar.gz 解压文件，并将其放入上述自定义的安装目录中；下载 daq-2.0.2.tar.gz 软件包并安装；下载 zlib 软件包并安装。

以上以最新版本为准。

⑥ 安装错误说明，configure 过程中发现缺失依赖库，按照提示操作即可。出现 snort: error while loading shared libraries: libdnet.1: cannot open shared object file: No such file or directory。

解决办法：创建一个符号链接 ln -s /usr/local/lib/libdnet.1 /usr/lib/libdnet.1。

⑦ 测试安装，如图 1-1 所示。

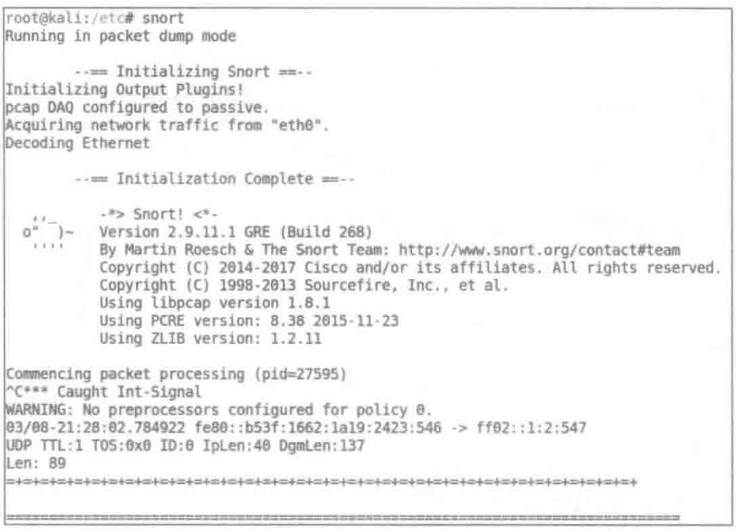

图 1-1　测试安装