Fadia道德黑客丛书

ANKIT FADIA 著
孟庆华 译

E-mail HACKING

E-mail 黑客攻防

电子科技大学出版社

E-mail 黑客攻防

法迪亚 著

孟庆华 译

电子科技大学出版社

图书在版编目（CIP）数据

E-mail 黑客攻防/（印）法迪亚著；孟庆华译. —成都：电子科技大学出版社，2007.10

ISBN 978-7-81114-653-0

Ⅰ.E… Ⅱ.①法…②孟 … Ⅲ.电子邮件—安全技术 Ⅳ.TP393.098

中国版本图书馆 CIP 数据核字（2007）第 153982 号

E-mail 黑客攻防

法迪亚 著

孟庆华 译

出　　版： 电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑： 郭　庆

责任编辑： 郭　庆　杜亚提　徐守铭

主　　页： www.uestcp.com.cn

电子邮箱： uestcp@uestcp.com.cn

发　　行： 新华书店经销

印　　刷： 成都市海翔印务有限责任公司

成品尺寸： 185mm×260mm　　**印张** 5.75　**字数** 159 千字

版　　次： 2007 年 10 月第一版

印　　次： 2007 年 10 月第一次印刷

书　　号： ISBN 978-7-81114-653-0

定　　价： 13.00 元

前 言

随着计算机与互联网的迅速普及，人类对计算机的依赖达到了前所未有的程度，计算机的安全直接关系到国家、企业、个人乃至人类社会的生存和发展。而对计算机与互联网构成最严重威胁的，正是防不胜防的网络黑客。纵观当今的互联网业界，病毒木马泛滥、黑客攻击猖獗，各种病毒变体花样百出，恶意攻击手段层出不穷。如何防黑、反黑、制黑，已成为所有互联网用户共同面对的巨大挑战。

上海兴韦教育集团及旗下的上海托普信息技术学院，利用自身的产业背景和专业优势，首度全面引进了国际互联网界资深反恐反黑精英、少年成名的网络安全大师 ANKIT FADIA 的系列专著——“法迪亚道德黑客丛书”。力图从黑客攻防两个角度，将国际最前沿的网络安全技术介绍给国内读者，帮助国内网络用户知黑、防黑、反黑，共同营造和维护健康、安全的互联网世界。

本书是“法迪亚道德黑客丛书”中，针对 E-Mail 系统安全的专著。本书从邮件攻击和邮件防护两个角度对邮件系统的各个层次作了深入细致的探讨。内容涉及 E-Mail 系统的各种安全威胁，包括匿名邮件攻击、邮件炸弹攻击、邮件伪造、邮件账户破解等，也系统阐述了邮件防护、邮件追踪、安全电子邮件等各种反黑手段，对邮件系统的安全原理也作了简要分析。此书内容深入浅出，技能明晰精深，是安全兴趣者和专业人士不可多得的一本 E-Mail 系统的安全专著。

本书主要由孟庆华博士主持翻译、统稿、审校。陆星家博士参与翻译了第一、二章，扬帆博士参与翻译了第三到第九章。由于译者水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

有关全套“法迪亚道德黑客丛书”的出版情况，敬请登录http://www.e-hacker.info.

译　　者

兴韦—法迪亚网络与信息安全中心（中国）

上海托普信息技术学院

2007 年 9 月

目　录

第一章 邮件攻击

- 你认为你接收到的邮件的发件人是不是他本人？
- 你的雇员是否会贪图享乐而对公司从事间谍工作，而通过电子邮件将公司的机密泄露给你的竞争对手？
- 你的孩子是否接收到充满色情内容的垃圾邮件？
- 你是否接收到邮件敲诈，问你要一大笔钱？
- 你的商业伙伴是否接收到诽谤邮件，而这些邮件是从你的邮箱发出的？

1.1 简介

电子邮件可能已经成为当今社会最常用和优先选择的交流方式。几乎所有的 Internet 用户至少有一个电子邮件账户，平均来说，每个用户有三个不同的邮箱账户。电子邮件可能是最具革命性的个人以及商业交流的工具。它能够使在不同地点的朋友和亲属经常保持联系，传输重要的商业文档，在瞬间共享喜怒哀乐。或者发送一些无聊的垃圾，搞笑的内容，甚至紧紧地将国与国之间的贸易紧密联系在一起。电子邮件的普及意味着我们使用传统的邮件进行通信的机会越来越少。许多公司实际上开始使用电子邮件和及时通信来代替传统的通信方式。不幸的是，越来越多的个人和组织依赖电子邮件处理重要的商业事务，邮箱的盗窃变得越来越受到人们的重视。邮件系统并不如我们想象的那么安全。电子邮件实际上有许多或暗或明的危险、威胁和漏洞，因此，每个人使用电子邮件都应该十分小心。

在 Internet 时代，大多数的企业如果没有电子邮件，可能无法生存。从短短几分钟的表演细节到紧急的工程报价，电子邮件被全世界的公司用来处理各种各样的事务。不幸的是，尽管电子邮件在商业的渗透力不断地加强，但是对于电子邮件的危险、威胁和脆弱性仍然没有引起足够的重视。大多数邮件用户在接收邮件时仍然面临巨大的风险。邮件被社会的广大群众所采用，随着商业邮件攻击的增长以及邮件渗透力的增加，意味着如何防范邮件攻击已经成为一件非常头疼的事。

不仅在企业用户中，而且包括个人用户也需要注意邮件的安全，现在，越来越多的人开始依赖电子邮件来保持人与人之间的沟通。长时间没联系的同学、工作过于繁忙的家人，孩时的朋友、两地分居的夫妻、家庭和亲戚——每一个使用电子邮件的人都可以利用电子邮件来保持沟通。电子邮件这样广泛的使用不仅表明电子邮件越来越普及，而且预示着攻击者可能利用电子邮件使用各种方式来破坏个人之间的关系。

1.2 邮件威胁

数以百万的全球的 Internet 用户使用电子邮件主要是商业和个人的目的，而没有过多地注意到其中巨大的威胁。一些与电子邮件相关的威胁如下：

1．在 Internet 上发送和接收的电子邮件有相当高比例是通过没有防护的公用系统进行传输的。换句话说，几乎所有在 Internet 上发送的邮件信息，从发送端到接收端总是要经过一些不信任的系统，这就造成邮件系统十分容易被拦截，被恶意的攻击者浏览。

2．近来的调查表明，超过 90%的电子邮件发送时，是使用明文进行发送的，只有极少数的用户使用一些安全措施或邮件加密来保障信件安全。因此，大多数的邮件对于恶意的攻击者来说，十分容易受到他们攻击。这些恶意的攻击者截获邮件信息，获得敏感的邮件信息内容。当一个邮件被从目标系统发送到源系统时，恶意攻击者有许多机会实施攻击。

3．邮件伪造已经成为 Internet 上非常广泛和严重的问题。大多数的邮件用户无法保证接收到的邮件的可靠性。近年来，犯罪案例显著的上升包括邮件伪造案例，邮件伪造主要是攻击者发送一个伪造的邮件，这个邮件从其他人的邮箱账户中发送出来的，而大多数的邮件攻击犯罪包含了性骚扰和精神折磨的内容。

4．使用电子邮件可以对大量的社会工程实施攻击。这样的攻击能够非常容易用来收集受害者敏感的信息（例如口令，信用卡信息，社会安全信息等）。

5．垃圾邮件邮件可能是所有邮件用户面临的非常普遍的问题。近年来研究表明，在 Internet 上，甚至超过 70%的的邮件流量是垃圾邮件消息。垃圾邮件不仅造成了使用者极大的不便，而且占用了电脑带宽和内存空间，使运行程序变慢。但不幸的是，至今仍然没有有效的方法来防范这种邮件。

6．许多人在 Internet 上使用电子邮件来传输敏感的数据或知识产权。而防止用户的邮件账户信息落入攻击者之手就显得十分重要。大多数的邮件账户对于攻击者来说，显得十分脆弱，口令攻击对于电脑罪犯来说，实施起来非常容易。

7．大多数的 Internet 用户继续使用邮件客户软件来发送和接收他们的邮件。使用这些工具的一个最大的问题是，他们需要用明文的方式来从客户端软件传输敏感的账户信息（例如用户名和口令）到邮件服务器。攻击者使用窃听软件记录受害者的账户信息记录非常容易，接着他们可以非法地获得邮箱中的内容。

8．邮件客户端：用户可以自己选择。

1.3 案例分析

案例 1 某国：教育部门

几年前，Internet 被广泛地引入到新加坡的所有中学和大学的教学中，给广大师生的学习带来了许多的方便。但是许多学生将 Internet 用在许多不好的方面。例如：一个在新加坡知名高校的学生准备在网上发布一些诽谤他人的消息，接着设法从一个伪造的邮件地址发

送这个通讯稿到国内主流的媒体。

利用这种方法，邮件可能来源于一个大学通讯部门的个人邮件地址。尽管大多数媒体在准备出版之前，都会给大学打去电话来证实这条消息。但是仍然有许多的通讯社由于时间安排较紧，而没有来得及证实消息的真伪。当这条消息错误地出现在当地的主流媒体时，学校非常地震惊，立即展开了调查。尽管犯罪嫌疑人很快被抓获，不幸的是，仍然给大学，官方，学生以及教师的形象造成了恶劣的影响。

案例2　个人

电子邮件渐渐的变成十分流行的媒介，无论是在办公还是在家里。通过电子邮件，我们可以保持友谊和商业关系，电子邮件普遍存在造成了在世界范围内许多于之相关的犯罪活动。在这一部分内，我们将列出与之相关的电子邮件的犯罪活动：

- 敲诈，恶作剧或感情折磨。
- 性骚扰。
- 通过一些与你相关的虚构故事进行商业诈骗。
- 给夫妻、商业合作伙伴发送伪造的电子邮件，造成夫妻、商业伙伴之间的矛盾。

案例3　某国，某地：个人

警察局长上大学的女儿，突然有天接受到一些含有骚扰内容的电子邮件，邮件中提到，除非一个特殊的罪犯（被她父亲关押的罪犯）被释放，才会停止发送骚扰邮件。很显然，警察是不可能同意他的要求。计算机安全专家开始检查受害者接收的骚扰邮件，通过邮件来追踪嫌疑犯。然而，调查显示，受害者接收到的邮件可能是伪造的。攻击者是在本地的一个咖啡馆，连接到远程的邮件服务器，发送伪造的骚扰邮件。发送伪造的邮件已经有几个月了，安全专家还是不能够发现犯罪分子。安全专家甚至与当地的 ISP 和本地 Internet 咖啡馆联系，然而，没有获得多少成果。攻击者非常聪明，从来没有在同一个咖啡馆上过两次网。然而，幸运的是，渐渐的，骚扰邮件的数量开始慢慢的减少，以致于消失。这个犯罪表明犯罪者多次使用的匿名骚扰邮件，借助邮件伪造和 Internet 咖啡馆作掩护，只是为了获得骚扰的乐趣，这种犯罪会造成许多严重的后果：

- 造成受害者个人和家庭成员的恐惧和心理上的恐吓。
- 受害者不得不常常改变电子邮件的地址。
- 造成工作极大的不便。

案例4　某国，某地：个人

一个在大的跨国公司工作的工程师，他有丰厚的经济收入。然而，他不能确定是否以后还是可以从事这种工作（what his job profile demanded）。一天，他接收到了一个邮件，另外一家跨国公司可以提供更高的工资和额外津贴，但这个项目可能更有挑战性，更加有趣。在与未来的项目主管进行了多次的邮件交换，他果断地辞掉了自己的工作，准备接受这份新的工作，当他打算要去公司时，发现所谓的老板根本不在这家公司。此事所造成的后果是：

- 失去自己的工作。

- 财政和感情上的损失。
- 受害公司失去了一名很有能力和潜力的员工。

案例 5 某国，某地：个人

2004 年，两名在重点中学的学生被牵扯到一个电子邮件犯罪中。一天，在放学后，有个家伙使用手机上的照相机记录下一段和他女朋友口交的片段。很快，这段视频被发送到许多的手机、文件共享网络、CD、色情产品市场、网站，还有邮箱内。在 Internet 上最重要的传播这段视频的手段是电子邮件，许多人通过电子邮件发送视频给他们的亲朋好友，包括电子邮件和多媒体信息成为了发布大众信息的主要手段。视频片断不仅可以通过网络传遍印度，而且可以传到中国、墨西哥、新加坡、加拿大和美国。该事件可以造成：

- 把学生和当局都拖下水。
- 财务和感情上的损失。
- 对色情视频中的主人公的感情造成了伤害。
- 非法的使用电子邮件来分发非法内容。

案例 6 某国，某地：零售业

日本的一个零售巨头发现在他们本年度的第一个季度收益有 17%的滑坡。而且，包括投资人和董事会都对零售业巨头的业绩的停滞感到十分的惊讶。突然，在一天早晨，所有的员工，客户，供应商和数以百万计的忠实客户从公司的 CEO 那里接收一封骚扰邮件。不仅如此，攻击者还发送伪造邮件到供应商和合作伙伴那里取消和改变订单。尽管，公司立即对可能的危险采取了应急保护工作，然而，情绪上，广大的用户还是受到了打击。由于许多相关的原因，零售商的利润出现大的滑坡：

- 公司和 CEO 的声誉受损。
- 财政损失。
- 竞争对手受益。
- 销售额下降。
- 损坏与合伙人联盟之间的关系等等。

1.4 不同类型的电子邮件威胁

电子邮件的安全现在已经变成一个很重要的大的领域，在全球计算机安全市场中，每一年公司和个人会花费大量金钱和资源保护他们的电子邮件资产。然而，电子邮件系统仍然很脆弱，会遭到不同的攻击：

- 在群体社会中，电子邮件常常被滥用，通过内部不满的员工有恶意的竞争对手实施的刺探活动、知识产权的盗窃；社会工程，商业情报的收集；辱骂性的攻击、敲诈；垃圾邮件、病毒感染、身份盗窃、社会性的污蔑和其他相关的攻击。
- 全世界的个人用户都可能体会到各种不同的电子邮件的威胁，包括敲诈，性骚扰，辱骂，扮演，社会工程，污蔑，病毒感染，垃圾邮件以及其他的方式。

尽管，有大量不同的电子邮件的威胁，但大多数的威胁主要包括以下几类：

- 侮辱邮件。
- 伪造邮件。
- 垃圾邮件。
- 病毒。
- 邮件账号攻击。

第二章 邮件追踪

- 你的孩子接收到过充满无聊的色情内容的垃圾邮件么？
- 有人利有邮件敲诈和威胁你，要你付一大笔钱么？
- 你的妻子从一些不满的朋友那里接收到辱骂性的邮件么？
- 你的公司雇员，伙伴或同盟是否接收到大量的垃圾邮件，妨碍了正常地商业活动？

2.1 简介

在今天，大多数的 Internet 用户使用标准的邮件客户软件（例如 outlook express Microsoft Outlook, Eudora Pro, Opera 等）来发送和接收消息。这样的邮件客户软件十分容易被使用，速度也很快，同时他们还能够为用户提供很多有用的功能。电子邮件客户软件使用户使用起来非常方便，而不需要注意里面的邮件工作的细节。然而，如果你打算解决电子邮件威胁，了解邮件系统工作的原理是非常重要的。

对于 Internet 用户来说，理解邮件如何在 Internet 上传输是十分重要的。除非你对邮件系统的工作非常熟悉，不会遇到相关的邮件威胁。在 Internet 上，一个邮件被发送和接收，一定要一些预定义的规则会自动的产生。所有的邮件通信主要依靠以下两个协议：

1．简单邮件传输协议（SMTP Port 25）；2．邮局协议（POP Port 110）。

Internet 上的邮件通信，从源端到目标端计算机的通信就像现实生活中的邮政邮件一样工作。每一次，邮件在 Internet 上发送，发送者会连接到本地邮件服务器（邮局）使用预定的 SMTP 命令来创建和发送邮件。这个本地邮件服务器接着使用 SMTP 协议传输邮件，通过其他中间邮件服务器，直到邮件最后到达目标邮件服务器（邮局）。邮件接收者接着连接到目标邮局服务器利用预定于的 POP 命令下载邮件。

SMTP 协议被用来发送邮件，当 POP 协议被用来接收电子邮件。因此，为了概括邮件发送传输的过程，每一个在 Internet 上的邮件在发送邮局服务器（借助 SMTP 命令），借助一些邮件服务器，最后到达接收邮局，接收者使用 POP 命令下载到本地系统：

Sender Outbox→Source Mail Server→Interim Mail Servers→Destination Mail Server→Destination Inbox

这个有组织的和可预测的邮件意味着，一个人能够辨别邮件发送的源头，只要简单地通过反向工程就能发现邮件的路径，每一次当一个邮件被发送到 Internet 上时，不仅可以携带信息体，而且还传输与路径相关的信息。这个关于传输路径的信息保留在邮件的标题。因此，每当人们接收到垃圾邮件，他只是简单地删除这个邮件，而没有认真地分析邮件的

标题，来追踪邮件的来源。

2.2 邮件标题

最有效和最容易的追踪垃圾邮件的方法是分析邮件的标题。他们包含了邮件来源的信息和路径的信息。大多数犯罪调查表明邮件标题保存有许多与犯罪相关的证据。邮件标题能够自动产生，并嵌入到邮件体内，在系统之间传输自动的组合。

他们不仅包含邮件的有价值的信息，而且还保持精确的路径信息。因此，通过分析一个邮件的邮件标题，能够通过逆向工程找到邮件的传输路径，以及最终到达的系统。例如，一个典型的邮件标题看起来像以下的形式：

Return-path: <abc@isp.com>

Received: from mx.ankit.com ([202.159.212.9]) by pop.ankit.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) for ankit@ankit.com; Thu, 06 May 2004 17:34:58 +0530 (IST)

Received: from web14525.mail.isp.com ([216.136.224.54]) by mx.ankit.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) for ankit@ankit.com (ORCPT ankit@ankit.com); Thu, 06 May 2004 17:34:57 +0530 (IST)

Received: from [61.247.235.152] by web14525.mail.isp.com via HTTP; Thu, 06 May 2004 04:54:12 -0700 (PDT)

X-Mailer: QUALCOMM Windows Eudora Version 5.2.1

Date: Thu, 06 May 2004 04:54:12 -0700 (PDT)

From: ABC <abc@isp.com>

Subject: Hi

To: ankit@ankit.com

Message-id: <20040506115412.59571.qmail@web14525.mail.isp.com>

MIME-version: 1.0

Content-type: text/plain; charset=us-ascii

Original-recipient: rfc822;ankit@ankit.com

有效分析邮件标题的诀窍是将标题信息分成不同的部分，检查每一部分，将每一部分作为一个整体来考虑，然后将每个部分联系在一起。另一个重要的事情是，当一个人在分析邮件标题时，是从底向上进行分析的，在本例中，邮件标题被分为以下的部分：

Date: Thu, 06 May 2004 04:54:12 -0700 (PDT)

From: Resh <abc@isp.com>

Subject: Hi

To: ankit@ankit.com

Message-id: <20040506115412.59571.qmail@web14525.mail.isp.com>
MIME-version: 1.0
Content-type: text/plain; charset=us-ascii
Original-recipient: rfc822;ankit@ankit.com

邮件标题信息告诉我们，这个邮件是由abc@isp.com发送到 ankit@ankit.com ，发送的时间是 2000 年 5 月 6 号的 04:54，邮件的主题是 Hi，他主要包括 MIME 类型，数据类型主要包括 MIME。

Message-id: <20040506115412.59571.qmail@web14525.mail.isp.com>

消息的 ID 行可能是邮件标题最重要的部分。在大多数的犯罪案例中，消息 ID 属性包含了有罪的证据，需要抓到犯人。它不仅能够提供有关可疑的邮件服务器有价值的信息，而且可以存储邮件的时间信息。邮件标题的消息 ID 部分可以使用以下方式破解：

1．20040506115412:表示邮件的时间，存储的格式是 yyyy-mm-dd-hh-mm-ss，它代表发送邮件的日期和时间，这些信息与发送邮件的原邮件服务器相关。例如，在本例中，邮件的发送时间是 2004 年，日期是(5^{th})，(6^{th})，时间是 11 小时，54 分钟，12 秒。

2．59571:这个号码代表相关邮件的参考号，每一个邮件从邮件发送器发送时，都带有一个唯一的消息 ID 参考号。邮件服务器的日志文件包含发送邮件的所有的信息。特殊邮件的参考号能够区分不同的邮件，邮件的取证主要通过获得不同的邮件参考号来实施调查。

每一时刻，如果打算跟踪一个特定的邮件，邮件标题的消息 ID 部分被证明是非常有用的。可与系统管理员保持联系，使用消息 ID 可以发现更多与犯罪相关的消息。我们下一步的分析过程是邮件头部的分析：

Return-path: <abc@isp.com>
X-Mailer: QUALCOMM Windows Eudora Version 5.2.1

以上的邮件标题揭示了这个邮件发送运行的操作系统是 Windows，使用的是 Eudora 5.2.1 作为邮件客户端软件。通过邮件的标题可以发现发送邮件的地址是abc@isp.com。

Received: from mx.ankit.com ([202.159.212.9]) by pop.ankit.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) for ankit@ankit.com; Thu, 06 May 2004 17:34:58 +0530 (IST)

Received: from web14525.mail.isp.com ([216.136.224.54]) by mx.ankit.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) for ankit@ankit.com (ORCPT ankit@ankit.com); Thu, 06 May 2004 17:34:57 +0530 (IST)

Received: from [61.247.235.152] by web14525.mail.isp.com via HTTP; Thu, 06 May 2004 04:54:12 -0700 (PDT)

以上的邮件标题摘录非常重要，它可以包含有关邮件传输路径的信息，从发送端到接收端的路由信息。这部分的邮件标题需要用反向工程来发现从原端到目的端。研究邮件标题最主要的方法是使用从底向上的方法。换句话，当分析邮件的部分头部，一个人必须分散最后接收行，再上移束缚：

Received: from [61.247.235.152] by web14525.mail.isp.com via HTTP; Thu, 06 May 2004 04:54:12 -0700 (PDT)

这是邮件标题的接收头部，我们可以检查这个例子。它揭示了某些人使用的 IP 地址 61.247.235.152 来发送特定的邮件，它告诉我们，这个邮件从原系统到目标系统（地址为 *web14525.mail.isp.com*）。大多数重要的内容，这一行被识别出原系统（61.247.235.152），这个邮件能够使用的技术在以后章节需要讨论的。

Received: from web14525.mail.isp.com ([216.136.224.54]) by mx.ankit.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) for ankit@ankit.com (ORCPT ankit@ankit.com); Thu, 06 May 2004 17:34:57 +0530 (IST)

以上的行代表发送邮件的服务器地址是（域名：*web14525.mail.isp.com* IP 地址：*216.136.224.54*），通过中间的邮件服务器（域名：*mx.ankit.com*）。而且，它揭示了邮件暂时的中转服务器是(*iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)*，同时还有发送邮件的时间戳，时间戳是在发送邮件时自动产生的。

Received: from mx.ankit.com ([202.159.212.9]) by pop.ankit.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) for ankit@ankit.com; Thu, 06 May 2004 17:34:58 +0530 (IST)

最后，我们可以看到三个接收行的第一个，这行有时作为最后一行，我们在邮件分析案例中详细说明。这一行代表邮件发送经过的中间服务器是（域名：*mx.ankit.com* IP Address: *202.159.212.9*））， 邮件服务器的目的地址（域名：*pop.ankit.com*），接收者连接到邮件服务器，下载邮件使用简单的 POP 命令。这是完整的传输信息，包含从发送端到目的端的信息。

当所有以上的信息都被收集，接着完整的邮件传输路径可以按照以下方式进行解释：

61.247.235.152 (ORIGIN) ⟶ web14525.mail.isp.com (SOURCE MAIL SERVER) ⟶ mx.ankit.com (INTERIM MAIL SERVER) ⟶ pop.ankit.com (DESTINATION MAIL SERVER) ⟶Target System (DESTINATION)

一个人能够清楚地看到阅读和分析邮局标题并不是十分的困难。而且，邮件标题揭示了许多有趣的和有价值的信息，不仅包括发送邮件的地址，还包括达到目的地址的整个路

由信息。研究邮件标题是警察局和调查机构通常采用的技术，这些结构利用这些技术来识别和追踪电脑犯罪。许多电脑犯罪与诽谤、在线约会、骚扰和敲诈相关，可以简单地通过邮件标题来分析。一个人员需要一些练习，才能更好地理解邮件标题。

2.3 高级的邮件标题

在前面的部分中，我们已经学习了如何追踪一个邮件到目的地，通过分析一些基本的邮件标题。不幸的是，在实际上，邮件标题看起来还是有点复杂，阅读起来很困难。一个非常好的例子，被发送到邮件列表的一个邮件具有很复杂的邮件标题。在以下的例子中，我们了解到如何分析一个邮件的标题，这个已经被发送到 Internet 上的讨论组或邮件列表：

Return-Path: <owner-movielees@lists.Stanford.EDU>

Received: from pobox4.Stanford.EDU ([unix socket]) by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Wed, 24 Nov 2004 01:47:08 -0800

X-Sieve: CMU Sieve 2.2

Received: from leland3.Stanford.EDU (leland3.Stanford.EDU [171.67.16.108])

by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAO9l6JI012568;

Wed, 24 Nov 2004 01:47:07 -0800 (PST)

Received: from lists.Stanford.EDU (lists.Stanford.EDU [171.64.14.236])

by leland3.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAO9gY9U026731;

Wed, 24 Nov 2004 01:46:34 -0800

Received: (from root@localhost) by lists.Stanford.EDU (8.12.10/8.12.10) id iAO9gXht000364 for movielees-out5741627; Wed, 24 Nov 2004 01:42:33 -0800 (PST)

Received: from smtp2.Stanford.EDU (smtp2.Stanford.EDU [171.67.16.125]) by lists.Stanford.EDU (8.12.10/8.12.10) with ESMTP id iAO9gVNK000358 for <movielees@lists.stanford.edu>; Wed, 24 Nov 2004 01:42:32 -0800 (PST)

Received: from CPQ20500143191.stanford.edu (whoopilaptop.Stanford.EDU [128.12.18.34]) by smtp2.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAO9gUX6004043 for <movielees@lists.stanford.edu>; Wed, 24 Nov 2004 01:42:31 -0800

Message-Id: <6.1.2.0.2.20041124013957.023ce3b0@isp.com >

X-Sender: vici@isp.com (Unverified)

X-Mailer: QUALCOMM Windows Eudora Version 6.1.2.0

Date: Wed, 24 Nov 2004 01:42:31 –0800

To: listname@lists.isp.com

From: Victoria Chungu <vici@isp.com>

Subject: Hi

Mime-Version: 1.0

Content-Type: text/plain; charset="us-ascii"; format=flowed