高等学校法学实验教学系列教材

ECELS

Wangluo Fanzui Zhencha
Shiyan Jichu

网络犯罪侦查实验基础

许爱东 廖根为/编著

北京大学出版社
PEKING UNIVERSITY PRESS

Wangluo Fanzui Zhencha Shiyan Jichu

网络犯罪侦查实验基础

许爱东 廖根为/编著

北京大学出版社
PEKING UNIVERSITY PRESS

图书在版编目(CIP)数据

网络犯罪侦查实验基础/许爱东,廖根为编著. —北京:北京大学出版社,2011.8
(高等学校法学实验教学系列教材)
ISBN 978-7-301-19141-5

Ⅰ. ①网… Ⅱ. ①许… ②廖… Ⅲ. ①互联网络-计算机犯罪-刑事侦查-高等学校-教材 Ⅳ. ①D914

中国版本图书馆 CIP 数据核字(2011)第 122145 号

书　　名:网络犯罪侦查实验基础
著作责任者:许爱东　廖根为　编著
责 任 编 辑:杨丽明　王业龙
标 准 书 号:ISBN 978-7-301-19141-5/D·2877
出 版 发 行:北京大学出版社
地　　址:北京市海淀区成府路 205 号　100871
网　　址:http://www.pup.cn
电 子 邮 箱:law@pup.pku.edu.cn
电　　话:邮购部 62752015　发行部 62750672　编辑部 62752027
　　出版部 62754962
印 刷 者:河北滦县鑫华书刊印刷厂
经 销 者:新华书店
　　787 毫米×1092 毫米　16 开本　18.5 印张　426 千字
　　2011 年 8 月第 1 版　2011 年 8 月第 1 次印刷
定　　价:38.00 元

许爱东，男，1964年生，江苏江都人。副教授，高级工程师，硕士生导师。现任华东政法大学法学综合实验教学中心常务副主任。兼任上海市法学会公共卫生与生命法学研究会副会长，上海市司法鉴定专家委员会委员，上海市刑事科学协会文件检验常务理事，中国刑事科学协会文件检验专业委员会委员，中国刑事科学协会痕迹检验专业委员会委员，国家司法鉴定人，律师。

高等学校法学实验教学系列教材

网络犯罪侦查实验基础

上海市法学、政治学教育高地法学实验教学示范中心项目资助
上海市教育委员会重点学科建设项目资助（编号：司法鉴定J51102）

序　言

随着计算机网络技术的不断发展，互联网应用越来越丰富，范围越来越广泛。与此同时，网络犯罪呈现出逐年增长的趋势。近几年来，由于物联网等新技术的出现和飞快发展，网络犯罪手段和方式不断翻新，犯罪危害性也进一步加大，很多新问题有待进一步探索、发现和解决。因此，对网络犯罪有关问题进行专门研究十分重要和紧迫。其中，网络犯罪侦查技术是打击和控制网络犯罪的不可或缺的手段之一，具有较强的理论性和实践性，在控制网络犯罪中起着基础性作用。

华东政法大学是最早开展网络犯罪相关课程教学的高校之一。结合多年来的教学经验，我们深深感到，网络犯罪作为一门极具实践性的学科，完全采取讲授形式的传统教学模式难以达到理想的教学效果。网络犯罪所涉学科知识广，包括侦查学、犯罪学、法庭科学、计算机科学等，极具实践性。因此，有必要改变传统教学模式，逐步向讲授和实验相结合的教学模式转变。目前，我校正对相关实践性较强的学科积极探索新的教学模式，实验教学改革是其中重要的一项内容，它是改进传统教学模式的一种重要手段，是培养学生专业素质与提高工作实践能力的重要途径，是提高法学教学质量、培养学生创新能力和提高法律实务水平的重要措施。因此，编写一套适合于法学专业学生和具有法学特色的非法学专业学生使用的教材是非常必要的。

作为国家及上海市法学实验教学示范中心，我校教师结合历年来的教学经验，已经编撰了《司法鉴定实验教程》、《医患纠纷司法鉴定理论与疑案评析》等教材，我们非常欣慰地看到，《网络犯罪侦查实验基础》一书将付梓出版。该书涉及数字证据检索、收集、恢复、鉴定以及网络犯罪防控等内容，较系统地将网络侦查过程中涉及的技术和法律问题通过实验形式予以呈现。该书结构合理，内容通俗易懂，实验步骤详尽，便于引导学生学习。相信该书的出版将有助于提高司法鉴定学和侦查学专业学生实践操作的基本技能，为今后犯罪侦查和司法鉴定工作打下扎实、良好的基础。

许爱东

目　录

第一章
网络犯罪调查基础实验

内容提要 学习网络犯罪调查技术前，必须掌握计算机与网络基础知识，熟练使用相关调查软件。本章阐述了计算机局域网组装与维护实验、Win PE 制作使用实验、WinHex 使用实验、SysInternals 工具使用实验等内容。本章实验所涉工具是后续章节实验操作的基本工具，需要学生熟练掌握。

关键词 Win PE，WinHex，SysInternals，局域网

第一节 Autoruns 软件操作实验

Autoruns 是一款由 SysInternals 开发的系统软件，可以很方便地列举出 Windows 系统中所有自动运行的程序，并对它们进行编辑或删除等操作。在 Windows 系统中，很多木马程序和恶意软件会随着计算机启动而启动。Windows 启动过程十分复杂，每一启动步骤都有可能成为病毒或木马的利用对象。很多恶意软件在开机的多个阶段都可以进行启动并监视自己的运行，因此，需要有一个比较全面的监视系统自运行的软件。Autoruns 能够监视系统的所有启动程序和动态链接库，包括正常的 Windows 程序和恶意程序。

熟悉 Autoruns 软件等 SysInternals 工具集软件，是网络犯罪调查和取证的基础。Autoruns 提供的功能很多，熟练掌握它，对网络犯罪案件调查以及网络安全的进一步学习将会有很大帮助。

通过 Autoruns 可以查看注册表对应的影响计算机自动运行程序和代码的项目，包括系统启动自运行项目（登录情况）、系统资源管理器插件、IE 插件、计划任务项目、系统服务、Windows NT 用户登陆程序、Winsock 系统服务、打印功能、LSA 系统服务、系统驱动项目、启动执行、映像劫持、AppInit、KnowDlls 等项目。这些程序和代码一般在计算机启动过程中会自动执行，因此 Autoruns 对于自运行程序检查有非常重要的作用，其界面如图 1-1 所示：

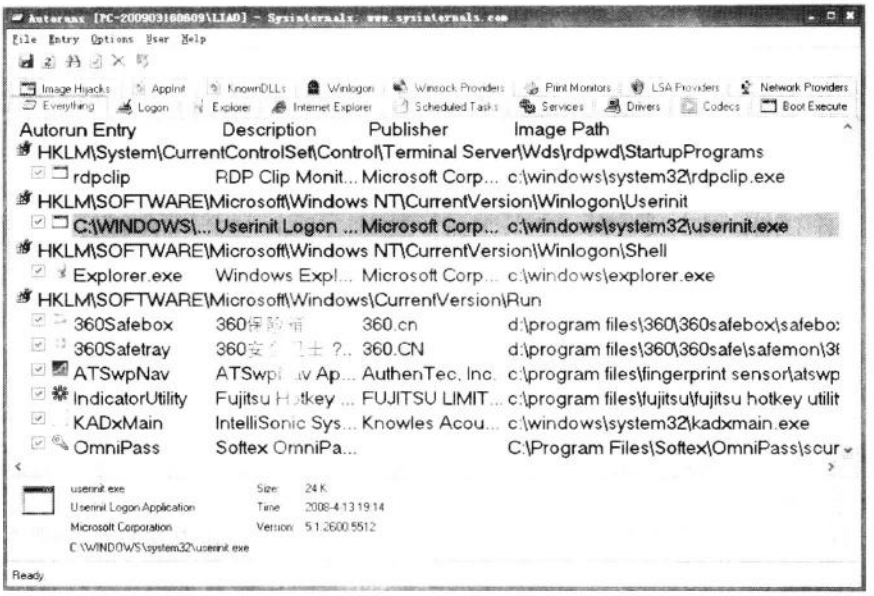

图 1-1　Autoruns 软件界面

Autoruns 除了查看注册表的对应项目外，还可以直接定位到注册表中的对应项目，只需要将鼠标定位在对应项目上，同时点击“jump to”按钮或菜单即可，也可以直接双击指定项目，如图 1-2、图 1-3 所示：

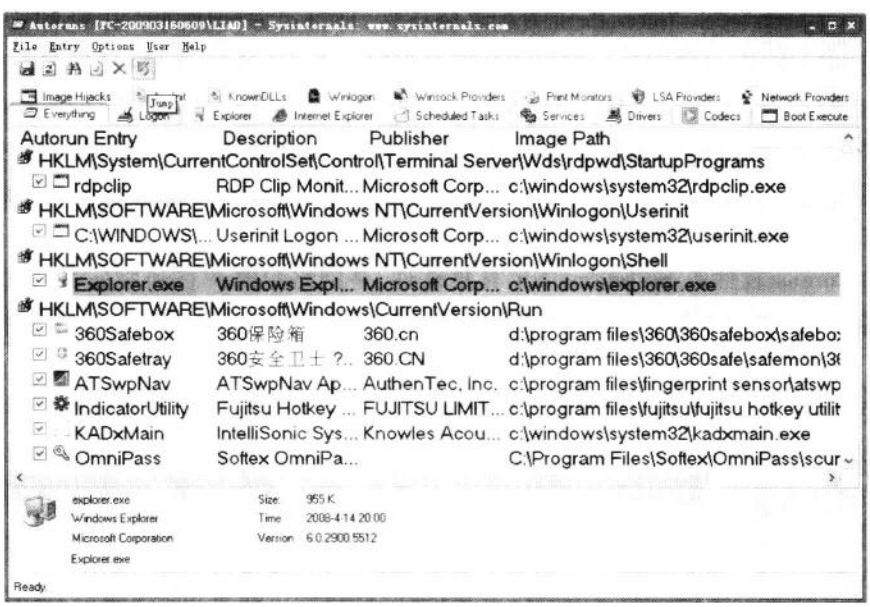

图 1-2　选择查看注册表的对应项目

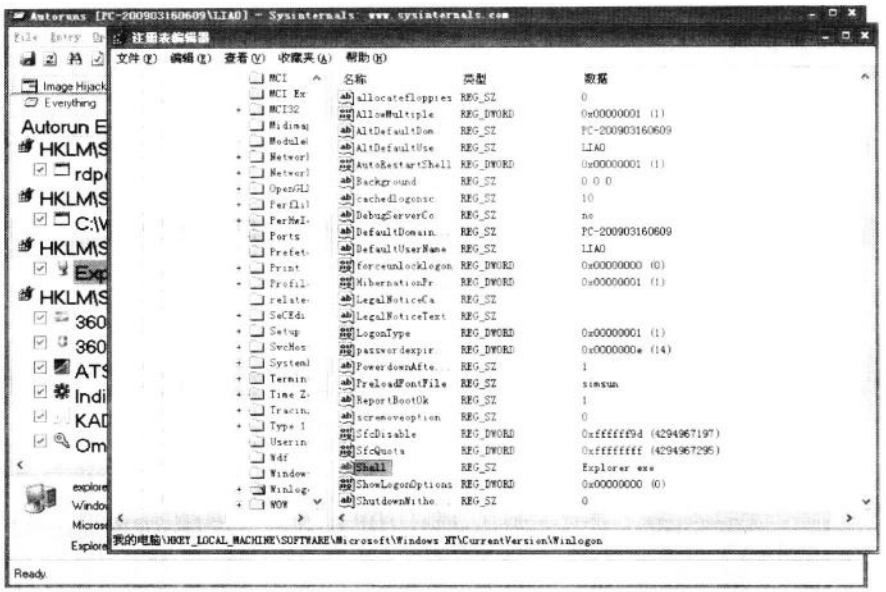

图 1-3　跳转至指定的注册表键

图 1-2 中，explorer. exe 程序对应的存储位置显示为“c:\windows\explorer. exe”，对应的项目在 Autoruns 中显示为“HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell”，其含义是在注册表中“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell”项目下 Shell 的值为 explorer. exe。通过“jump to”菜单或按钮可以直接定位到注册表中对应的项目。

一、实验目的

1. 熟悉 Autoruns 软件的使用方法；
2. 通过 Autoruns 软件操作，熟悉常见的自启动项；
3. 熟悉 SysInternals 其他软件的操作和使用方法。

二、实验要求

1. 每两人一组进行实验；
2. 能够运用 Autoruns 自行查看所有可能在系统启动过程中运行的程序；
3. 了解主要的计算机启动项目；
4. 在实验过程中，记录可疑的、异常的计算机启动项目。

三、实验器材和环境

1. Windows2000/XP/2003 操作系统；
2. Autoruns 软件。

四、实验主要步骤

1. 打开 Autoruns，了解初始界面，熟悉英文版 Autoruns 的菜单和主要功能。

2. 点击“查找”功能可以在所有自运行项目列表中检索能够匹配特定字符串的注册表项目（自启动项）和文件名，如图 1-4 所示：

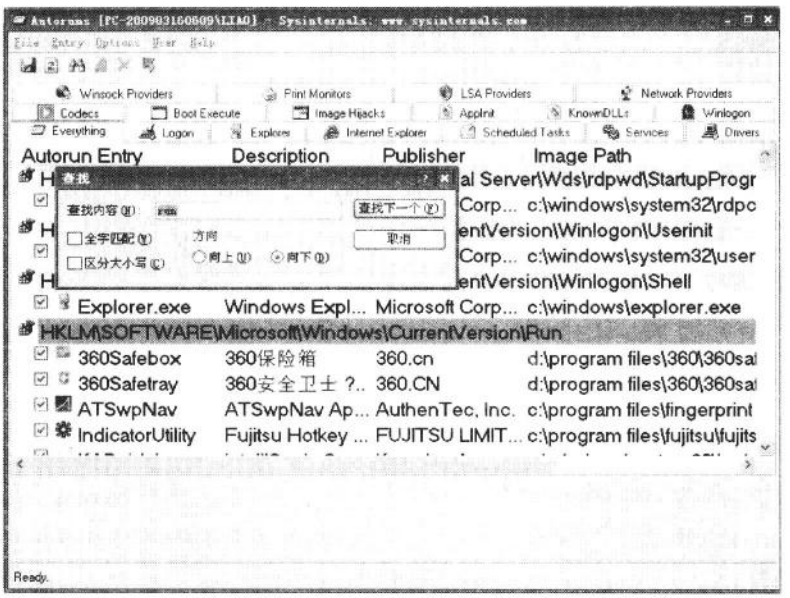

图 1-4　Autoruns 查找功能

3. 选中任意一个选项单击鼠标右键，可以看到所需要的菜单，如图 1-5 所示：

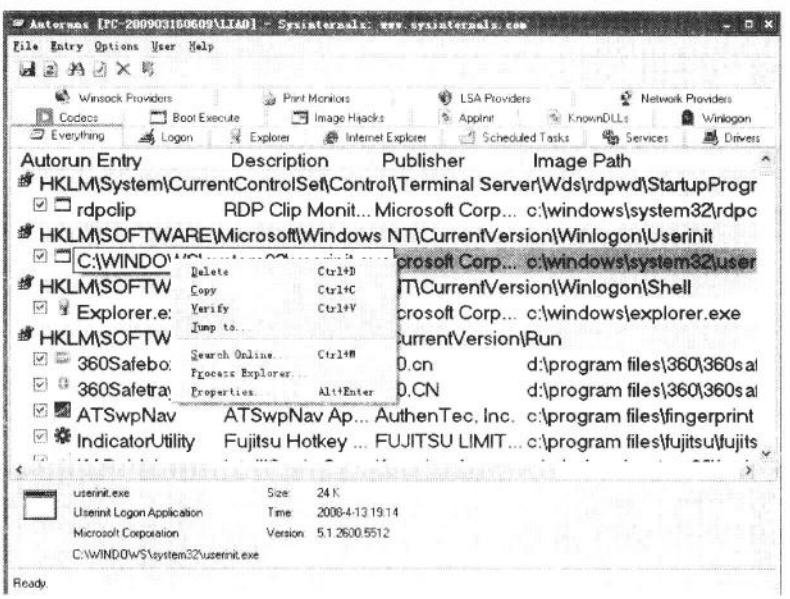

图 1-5　Autoruns 弹出菜单

上图中右键菜单主要有“Delete”、“Copy”、“Verify”、“Jump to”选项，其功能分别为删除一个选项、复制特定项目内容、验证确定程序是否可以通过验证、跳至注册表对应选项。

4. 双击任意一个 Autoruns 项目，可以跳转到该项目对应的注册表项，并查看该注册表项目或键值的内容，如图 1-6 所示：

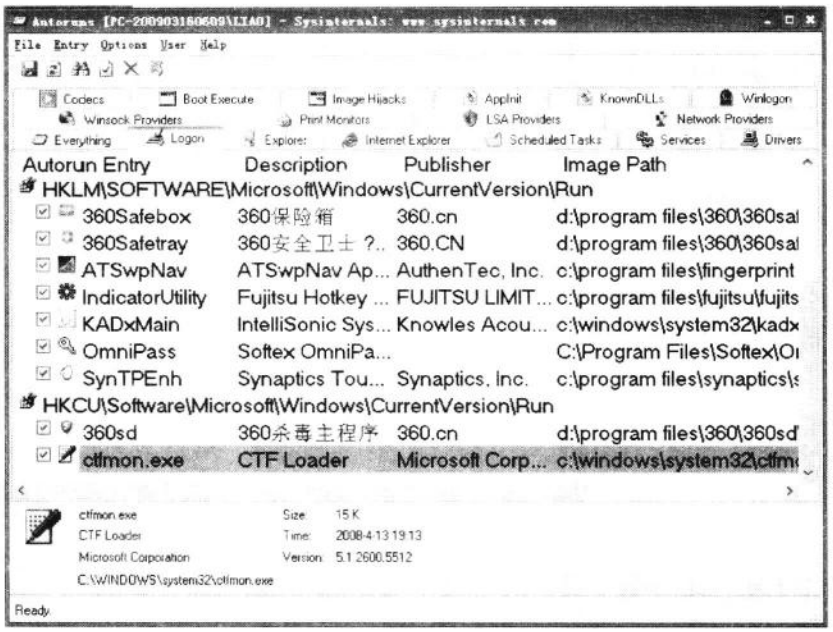

图 1-6　通过 Autoruns 跳转至注册表项

5. 查看“设备驱动程序”选项，确定哪些文件在系统启动过程中会自行启动，如图 1-7 所示：

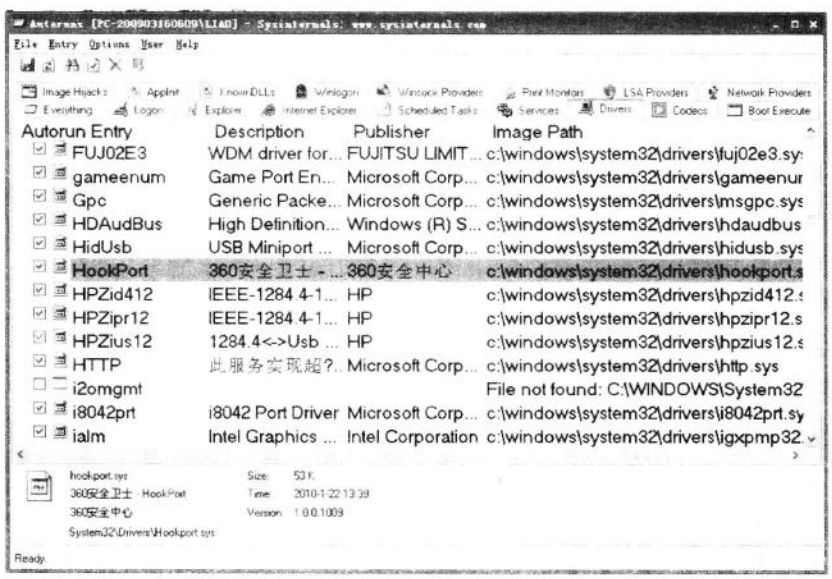

图 1-7　查看设备驱动程序选项

6. 查看“服务”选项。通过 Windows 的 sevices. msc 能够查看到的所有服务程序，使用 Autoruns 的“Sevices”选项也可以查看和编辑，如图 1-8 所示：

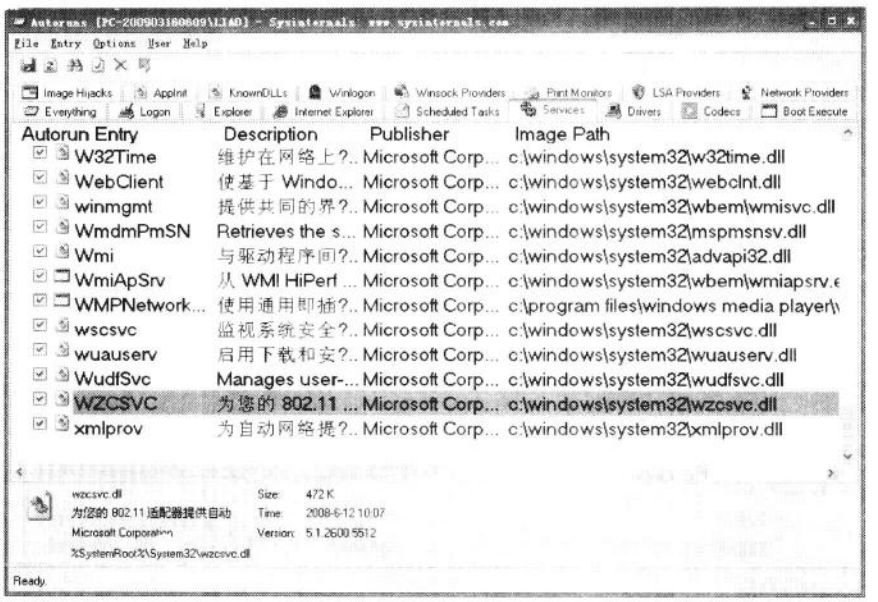

图 1-8 查看服务选项

7. 查看计算机中的“映像劫持”，看是否有异常情况，如图 1-9 所示：

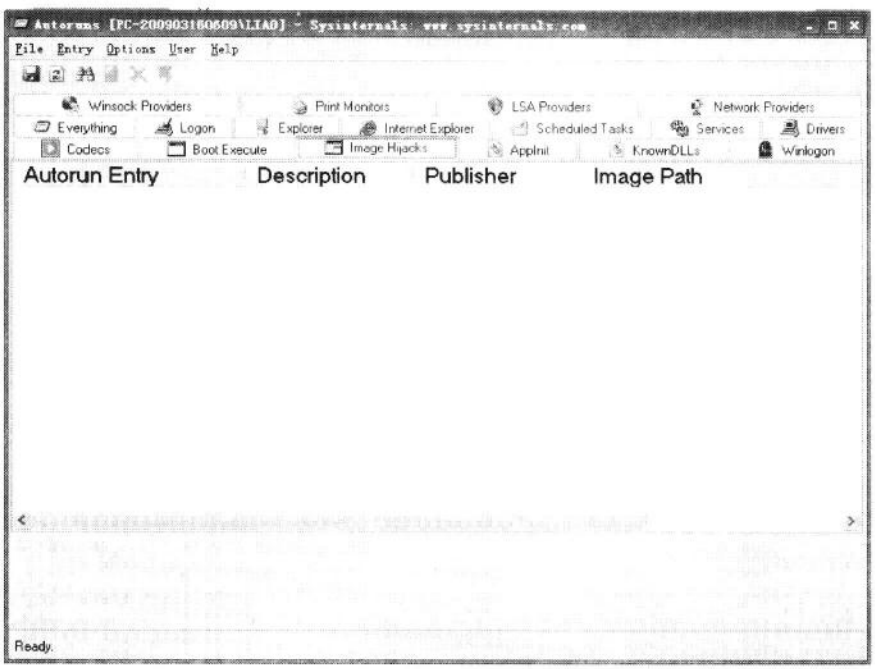

图 1-9 查看映像劫持选项

8. 查看 IE 插件情况。通过“Internet Explorer”选项可查看 IE 的插件情况，IE 插件是恶意软件经常利用的启动项，如图 1-10 所示：

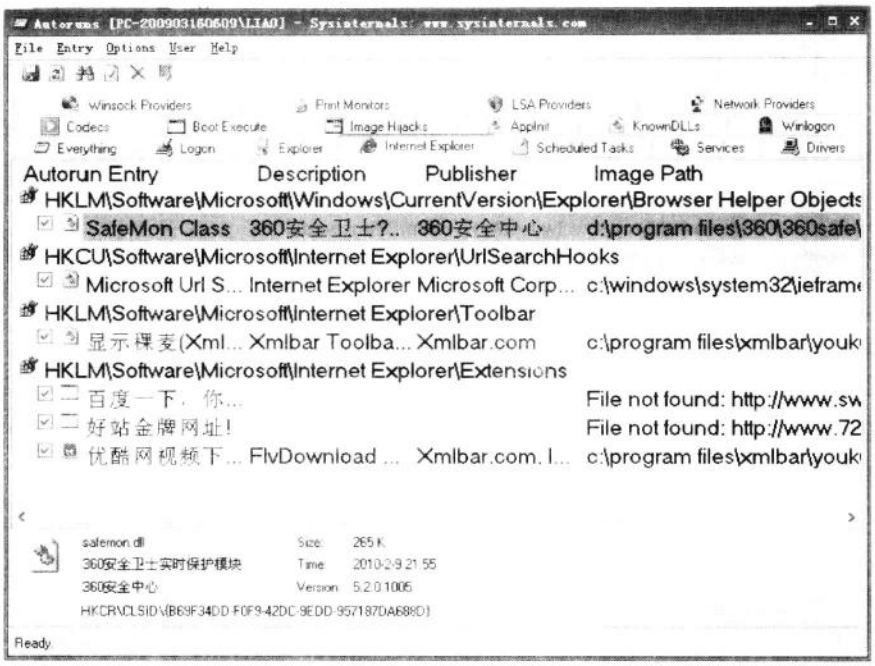

图 1-10　查看 IE 插件

9、查看“Explorer”插件情况，如图 1-11 所示：

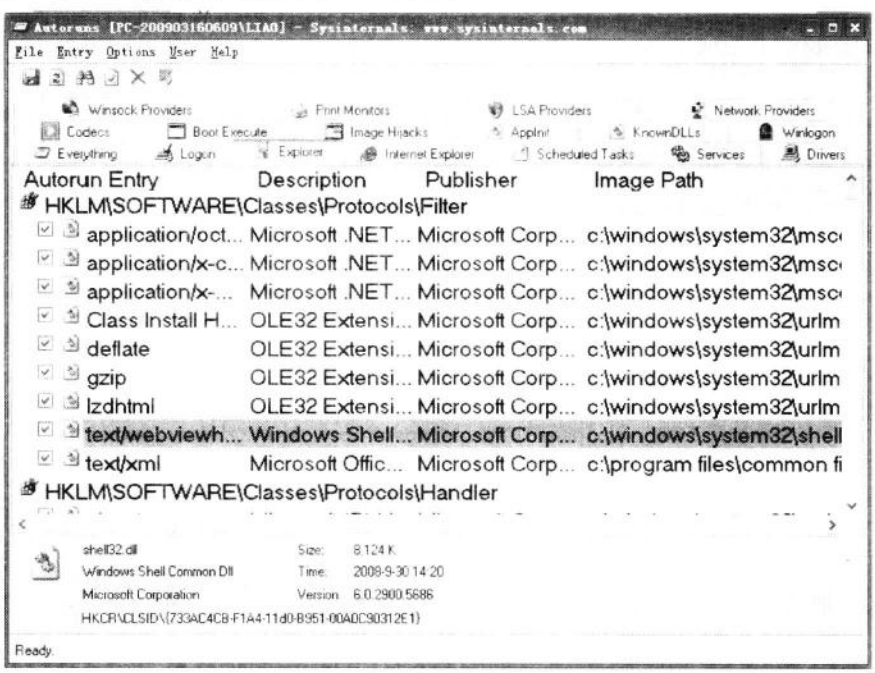

图 1-11　查看 Explorer 插件

10. 查看“Winsocket Provider”，查看 TCP/IP 协议处理是否安装异常过滤插件，标准的动态链接库是否已经被修改成其他选项，如图 1-12 所示：

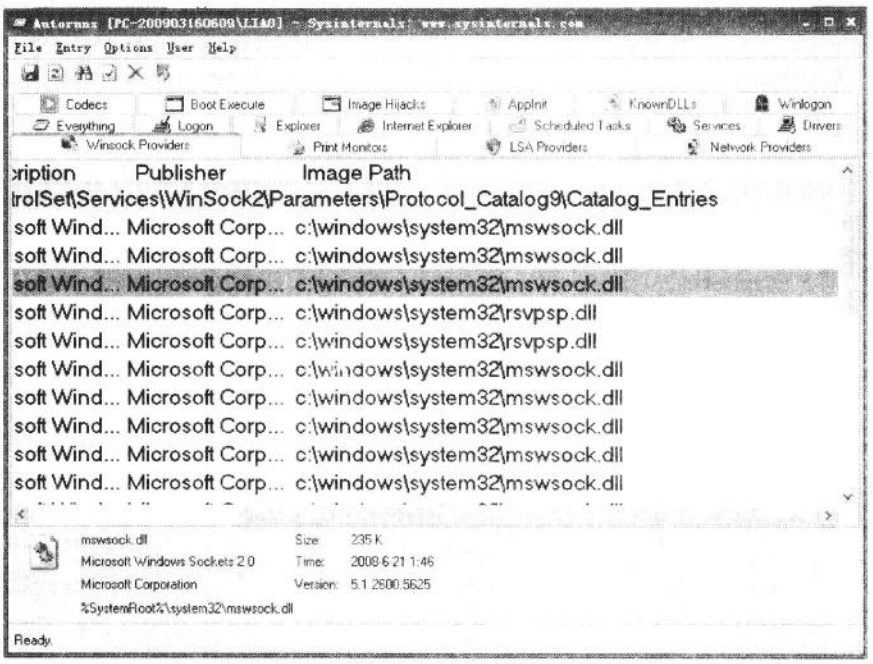

图 1-12　查看 Winsocket 提供者选项

11. 查看打印监视是否存在问题，如图 1-13 所示：

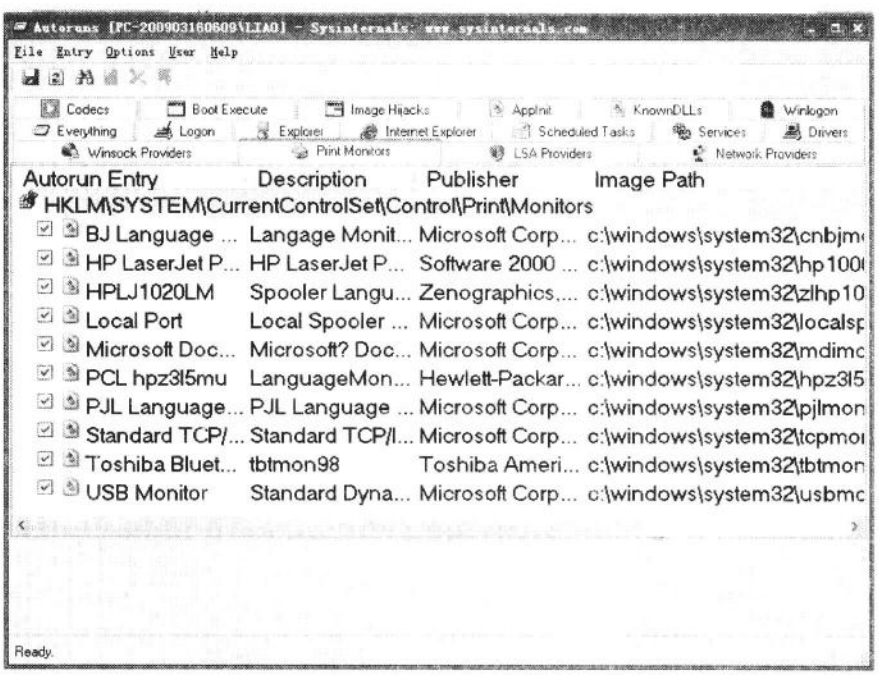

图 1-13　查看打印监视选项