新世纪高等学校规划教材 · 信息安全系列

网络犯罪侦查实验教程

武鸿浩◎主编

WANGLUO FANZUI ZHENCHA SHIYAN JIAOCHE

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

新世纪高等学校规划教材 · 信息安全系列

网络犯罪侦查实验教程

武鸿浩◎主编

WANGLUO FANZUI ZHENCHA SHIYAN JIAOCHENG

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

图书在版编目（CIP）数据

网络犯罪侦查实验教程/武鸿浩主编. —北京：北京师范大学出版社，2017.6

新世纪高等学校规划教材 · 信息安全系列

ISBN 978-7-303-22376-3

Ⅰ. ①网… Ⅱ. ①武… Ⅲ. ①互联网络－计算机犯罪－刑事侦查－高等学校－教材 Ⅳ. ①D918

中国版本图书馆 CIP 数据核字（2017）第 114365 号

营 销 中 心 电 话 010-62978190 62979006
北师大出版社科技与经管分社网 www. jswsbook.com
电 子 信 箱 jswsbook@163.com

出版发行：北京师范大学出版社 www.bnup.com
北京市海淀区新街口外大街 19 号
邮政编码：100875

印 刷：北京京师印务有限公司
经 销：全国新华书店
开 本：184 mm×260 mm 1/16
印 张：8
字 数：162 千字
版 次：2017 年 6 月第 1 版
印 次：2017 年 6 月第 1 次印刷
定 价：18.80 元

策划编辑：赵洛育 责任编辑：赵洛育
美术编辑：刘 超 装帧设计：刘 超
责任校对：赵非非 责任印制：赵非非

前言

随着互联网的普及，网络给人们的工作和生活带来了极大的方便，但同时网络犯罪也在近年出现了快速增长的态势，几乎所有传统犯罪都已触网。为了更好地遏制网络犯罪，需要一支具有专业素养的网络犯罪侦查技术队伍。

网络犯罪侦查工作既需要传统的刑事侦查技术，也需要极强的利用电子数据发现和扩展犯罪线索的能力。随着网络犯罪侦查工作实践和教学工作的开展，有关网络犯罪侦查的技术得到了快速的发展，本教材从网络犯罪侦查工作实践出发，归纳和梳理了网络犯罪侦查的主要技术。

本教材主要包括网络犯罪案件现场勘查、本地主机数据文件线索查找实验、数据恢复、隐藏文件线索查找、网络设备线索查找、侦查实验、日志查找与分析以及互联网线索查找等内容，覆盖了网络犯罪侦查技术的主要方面。本教材从培养读者实践操作能力为出发点，强调动手操作能力的养成，图文并茂，并对主流的软件作了介绍。

本教材的撰写工作得到了佟晖教授和齐莹素老师的帮助。

由于时间仓促，不妥和错误之处在所难免，殷切希望使用本教材的老师、同学和其他读者提出宝贵的意见和建议。

编　者

2016 年 11 月

目录

第1章

网络犯罪案件现场勘查

网络犯罪案件的现场勘查往往是侦查工作的开端，和传统的刑事案件相同，犯罪现场是包含犯罪线索最丰富的地方。犯罪现场勘查工作开展得是否得当很大程度上影响了后期侦查工作是否能够顺利进行。

同时，网络犯罪现场也包含许多自身的特点，其中最主要的一条就是，网络犯罪现场的勘查目标主要是电子设备，电子数据具有易失性，因此在进行网络犯罪现场勘查时要特别注意勘查流程。

1.1 网络犯罪现场勘查基础

1.1.1 网络犯罪现场勘查的概念

网络犯罪现场（如图 1-1 所示）是指犯罪嫌疑人实施网络犯罪活动的物理空间地点，操纵的计算机系统与相关附属设备、有计算机数据信息保留的网络传输节点，以及留有其他犯罪痕迹物证的有关场所。

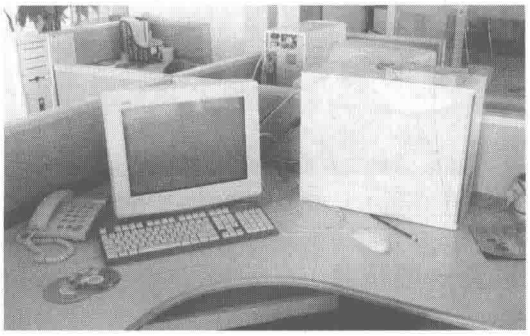

图 1-1 网络犯罪现场

任何一起网络犯罪案件，都有一个或一个以上明显的作案现场，即使犯罪分子为了逃避打击，采取各种手段企图改变或销毁犯罪现场，也只能是掩盖或改变作案现场的某些现象，已经存在的犯罪事实是掩盖不了的，作案现场更是销毁不了的，即犯罪现场是客观存

在的。实施现场勘查对于侦查机关了解案情、确定侦查方向、制订侦查计划直至最终的破案都有重要的意义，常常被作为案件的第一突破口。

如果对网络犯罪现场分类，可以有多种分类方法，其中根据网络犯罪现场勘查的任务分工和取证内容可以分为物理现场和数字现场。物理现场一般是指犯罪行为发生所依赖的计算机、网络设备等硬件实物以及这些硬件实物所在的场所，是具体存在的可被人们所感知的事物。比如犯罪行为人实施犯罪行为所使用的计算机、移动存储设备、数码产品、通信工具等，以及这些实物所位于的犯罪行为人的办公室、工作室、网吧等场所。数字现场又称信息现场，由物理现场硬件支撑，表现为电子数据形式的各类计算机信息。无论是以计算机信息系统为犯罪对象，还是以计算机信息系统为犯罪工具的各类犯罪活动，在数字现场中，网络犯罪行为都具体表现为各种各样的计算机操作，网络犯罪行为的危害常常直接体现为计算机信息系统的运行状态及数据内容的改变。

网络犯罪现场勘验是指在犯罪现场实施勘验，以提取固定现场留存的与犯罪有关的电子数据、电子设备、传统物证和其他信息。网络犯罪现场勘查（如图 1-2 所示）的任务是：发现、固定、提取与犯罪相关的电子数据、电子设备、传统物证和其他信息；进行现场调查访问，制作和存储现场信息资料；判断案件性质；确定侦查方向和范围；为侦查破案提供线索和证据。

图 1-2　网络犯罪现场勘查

1.1.2　网络犯罪现场勘查一般程序

在进行现场勘查前需要完成对犯罪现场的保护、准备勘查工具等工作。

现场保护的目的在于网络犯罪行为人大多都具有高超的计算机技术，只要事先得到消息就有足够的时间篡改或销毁证据，所以对于网络犯罪案件的现场一经确定，必须迅速加以保护。另外，要注意防止现场被侦查人员有意或无意污染，防止因为计算机信息系统的

操作不当而破坏现场。

现场保护主要内容包括：

（1）封锁所有可疑的犯罪现场，包括计算机工作室和进出路线，在门口、窗口设岗看守，不许无关人员进入室内。进一步封锁整个计算机区域，包括通信线路、电磁辐射区。找到网络连接设备和变电箱（如图 1-3 所示），并派专人值守，对犯罪现场不明显，且难以确定的，应适当扩大现场保护范围，划出警戒线，安排人员监视。

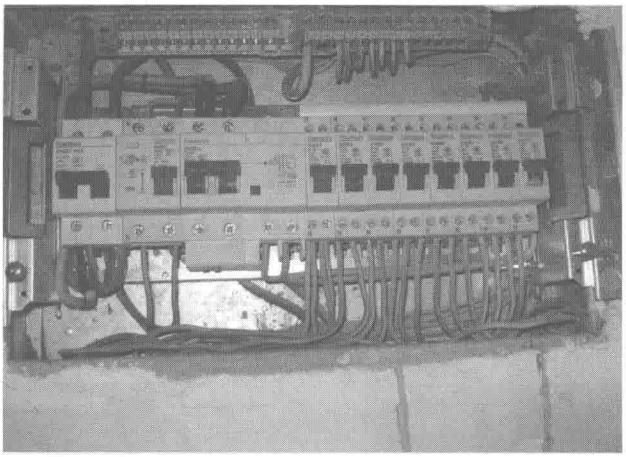

图 1-3　网络犯罪现场变电箱

（2）对于关乎重大利益无法暂停或者停止的系统使用拍照、摄像的方式进行监视，记录有关的犯罪活动。

（3）切断远程连接，对于已经结束犯罪行为的现场勘查，在获取网络状态后一般要切断远程连接，并进行详细记录，防止嫌疑人远程销毁证据。如图 1-4 所示即为网络犯罪现场的联网设备。

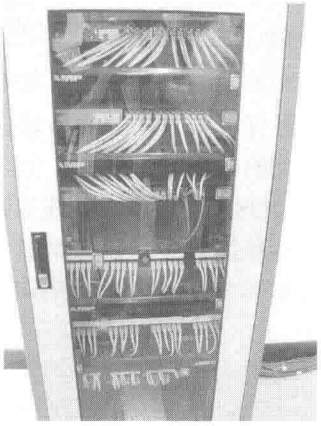

图 1-4　网络犯罪现场联网设备

（4）在网络犯罪现场勘查时，应当看管好所有涉案人员，禁止涉案人员接触计算机等电子设备。如果确需涉案人员提供密码或其他操作的，应当询问涉案人员相应的信息，并由侦查人员完成操作，不得由涉案人员操作计算机。

（5）防止调查人员无意中破坏证据。如果电子设备（包括计算机、PDA、移动电话、打印机、传真设备等）已经打开，不要立即关闭该电子设备。如果电子设备已经关闭，不要打开该电子设备。对于黑屏状态的计算机，在勘查时要先确认该计算机处于开启或者关闭状态后再实施操作。如果计算机上应用程序正在运行，一般不要立刻关闭，但禁止重新运行计算机上原有的任何应用程序。如果打印机正在执行打印任务，不要停止该打印任务，让打印机将打印任务执行完毕。如果嫌疑人正在编辑电子文档，不要直接保存该电子文档，必须将该电子文档另存到勘查人员自带的存储媒介。对于发现勘查人员无法识别的设备，要与相关的专家联系以获得技术帮助，否则应直接关闭电源，切忌尝试

对该设备的任何操作。

（6）防止正在运行的系统破坏证据。如果操作系统正在进行整理硬盘、格式化硬盘、批量复制信息、下载信息、杀毒等可能大量访问存储媒介的操作，要立刻终止。如果数码摄像机正在摄像，要停止该数码摄像机，因为当前拍摄的内容会覆盖以前存留的信息。如果数码录音设备正在录音，要停止该录音设备，因为当前录音内容会覆盖以前存留的信息。

由于网络犯罪现场勘查工作属于技术性较强的工作，因此在进入网络犯罪现场之前需要准备好进行勘查所需的硬件和软件设备。

在硬件方面，为了防止对现场电子设备的破坏，除特殊情况，一般勘查工作都需要在自带的计算机中完成，因此需要携带笔记本电脑或移动 PC 对现场发现的嫌疑计算机进行证据采集和分析。

移动硬盘或 U 盘：用于存取网络犯罪现场勘查中发现的嫌疑计算机中有价值的信息，还可用于存储对嫌疑计算机进行勘查时所需要的软件工具。如图 1-5 所示即为用于存储数据的空白盘。

高速硬盘复制机（如图 1-6 所示）：用于对在网络犯罪勘查现场发现的嫌疑计算机的硬盘进行复制，以便进行下一步的证据分析。

图 1-5　用于存储数据的空白盘

图 1-6　硬盘复制机

单向硬盘只读锁（如图 1-7 所示）：用于在网络犯罪现场勘查过程中读取嫌疑存储介质时保证数据的单向传输，避免了侦查人员对于电子证据的污染，保证所提取的证据在法律上的效力。

USB 连接线、网线以及其他必要的通信传输线：网络犯罪现场的复杂性体现之一就是设备种类繁多，如何做好多种设备之间的连接以读取所需数据是保证现场勘查顺利进行的重要环节。如图 1-8 所示即为适用于各种接口的数据线。

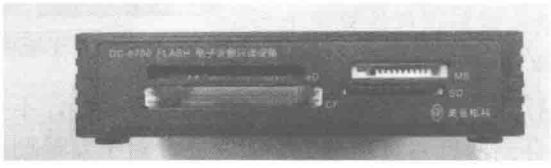

图 1-7　单向硬盘只读锁

图 1-8　适应各种接口的数据线

适应多种计算机接口转换的转接卡：和传输线一样，转接卡也是为了在网络犯罪现场勘查过程中对于多种设备和接口进行转接，使多种设备顺利进行数据传输和交换，保证现场勘查顺利完成。如图 1-9 所示即为常见的存储卡转接口，如图 1-10 所示即为三合一硬盘转换器。

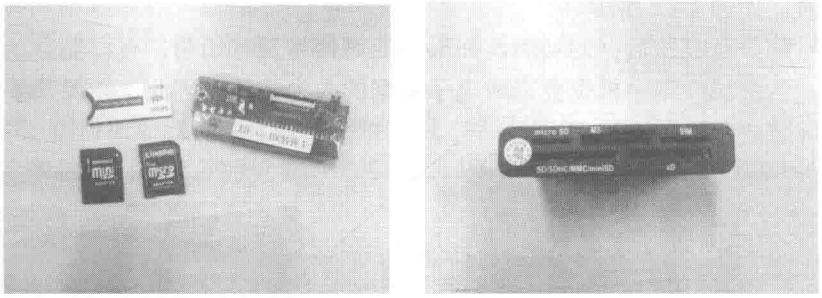

图 1-9　常见存储卡转接口

图 1-10　三合一硬盘转换器

螺丝刀等拆卸工具：在网络犯罪现场勘查过程中，为了获取侦查时所需要的信息，常需要对各种设备进行拆装，诸如螺丝刀等拆卸工具在现场勘查过程中也是必不可少的硬件工具，如图 1-11 所示。

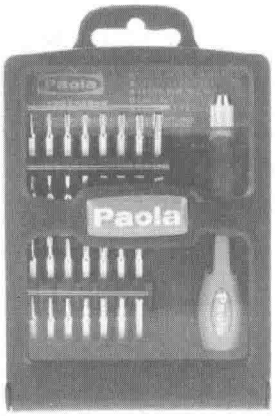

图 1-11　多规格螺丝刀套装

计算机配件的电源线、插座：网络犯罪现场瞬息万变，设备种类繁多并且随时可能发生意想不到的突发情况，配齐常用设备的电源线和插座能够保证现场设备的正常运行，才能保证现场勘查的实施。

由于静电会对电子设备造成破坏，因此在提取电子设备，尤其是电子元器件时需要带上防静电手套，如图 1-12 所示。

智能手机都具有收发数据的功能，如果不能对信号及时切断，有可能会造成电子数据的人为破坏，但贸然操作手机也会造成电子数据的人为破坏。因此，在保存手机时需要使用手机信号屏蔽盒，如图 1-13 所示。

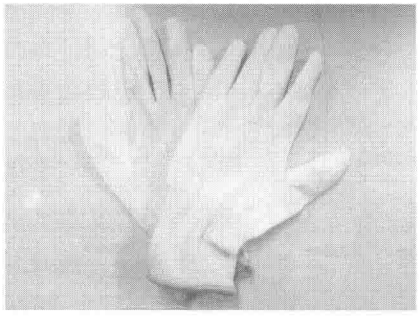

图 1-12　防静电手套

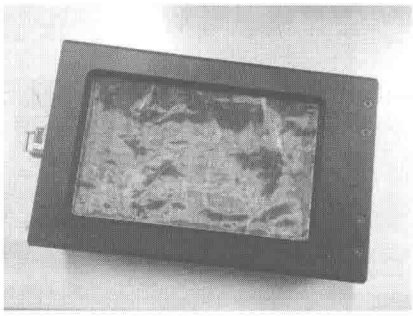

图 1-13　手机信号屏蔽盒

在进行现场勘查时需要携带的软件主要包括：

工具资料软盘。在进行现场勘查的过程中，侦查人员一般都要携带自行制作的工具资料软盘，里面包含常用的系统命令，通过这些系统命令可以获取诸如系统时间、网络连接状态、端口状态、用户账户状态等信息，这将有助于侦查工作的进一步开展。

密码破译工具。在进行网络犯罪现场勘查取证过程中，侦查人员所获取的文件信息有可能已经被犯罪分子进行了加密处理，这时如果犯罪嫌疑人不愿意主动提供加密文件的密码，可以采用相应的密码破译工具进行解密以得到相关的证据。好的密码破译工具将会大大缩短现场勘查的时间。

数据恢复工具。网络犯罪作为高科技领域的犯罪，犯罪行为人大都具有高超的计算机技术，为了逃避侦查，他们会在作案完毕之后清除犯罪的痕迹，例如删除一些记录他们作案行为的日志信息等，而这些被删除的文件信息正是侦查人员进行现场勘查所要获取的犯罪证据，此时借助数据恢复工具可以更好地完成现场勘查工作。数据恢复工具有很多，现场勘查中较为实用的有 EasyRecovery 和 FinalData。

日志分析软件。日志作为记录计算机状态的文档，在现场勘查过程中对于日志文件的读取和分析也是重要的工作之一，更好地对日志文件进行分析将会使侦查人员掌握更多的犯罪行为人活动的信息。

文件浏览工具。这类工具是在现场勘查中专门用来查看数据文件的阅读工具，只用于查看而没有编辑和修改的功能，可以防止对于证据的破坏。比较好的文件浏览软件是 Quick View Plus，它能在不嵌入其他应用软件的情况下很方便地开启和浏览各种文件。

网络监控工具。NetMonitor 网络信息监控与取证系统是针对因特网开发的网络内容监

控系统，能够记录网络上的全部底层报文，监控流经网络的全部信息流，是侦查人员在现场勘查中进行网络信息流监测的重要工具。

证据分析软件。一般情况下，证据分析工作不在现场勘查阶段开展，但是在特殊的情况下也需要侦查人员在现场勘查的过程中直接应用证据分析软件对现场搜集的证据进行分析以获取所需要的信息。

在现场勘查时需要严格按照操作流程进行，防止误操作毁灭证据或线索。

现场拍照：在对现场进行勘查时应全程录像，并对重点设备和现场全景拍照，如设备的位置、连接状态、显示屏幕信息等。

现场拍照的内容主要是勘查前的状态：建筑物外景，门牌号信息，房间全景，具体设备的状态，连线情况（如图 1-14 所示）。

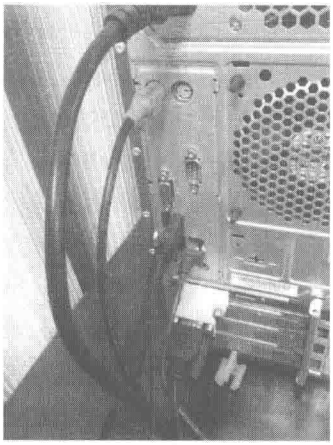

图 1-14　涉案主机线缆连接情况

在拍照之后需要对整个犯罪现场进行全面具体的搜查，主要搜查目标包括以下几种。

（1）纸质文件：便签、打印材料、笔记本等。

（2）移动存储介质：U 盘、移动硬盘、存储卡、光盘等，特别需要注意异形 U 盘的搜集。

（3）计算机、移动终端及其外部设备，如电池、充电器、扩展卡等。

（4）网络设备：路由器、交换机等。

对于犯罪现场中的电子设备要进行重点勘查。

在对计算机设备进行勘查时的原则是不要改变开机状态，不要将处于关机状态的计算机开机，因为一些计算机安装了还原卡，或具有自动清除一些数据的功能，这些工作往往在开机时完成。如果一台计算机处于开机状态，则尽量保持其活跃状态，不要关机，也不要让其进入锁屏状态，应当时常按 Ctrl 键或者晃动鼠标保持其活跃状态，并关闭计算机的自动锁屏功能，如图 1-15 所示。

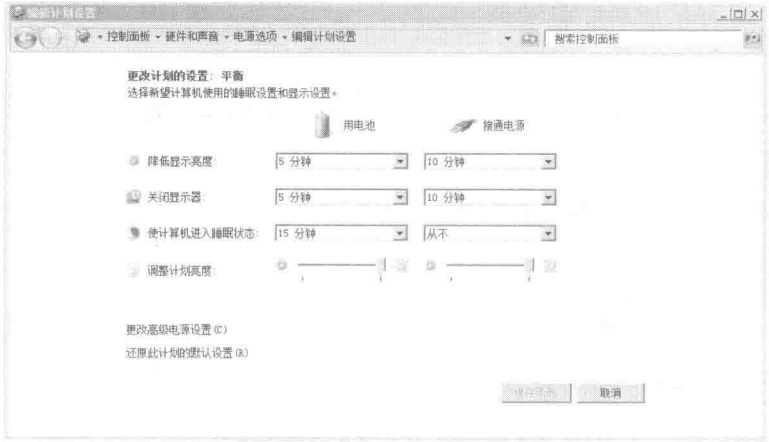

图 1-15　关闭计算机的自动锁屏功能

遇到黑屏的计算机，有可能并不是关机而是进入屏保或休眠状态，需要确定其是否为开机状态。首先观察计算机指示灯，如图 1-16 所示。或者晃动鼠标或按方向键（禁止按 Enter 或者 Esc 键，防止误操作），以及短按开机键。在一些情况下需要查看屏幕是否处于开机状态。

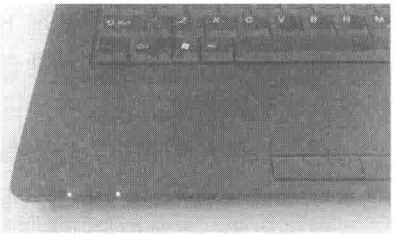

图 1-16　电源指示灯

如果现场计算机处于开机状态，需要将其中的易失证据和线索及时固定，具体内容见 1.3 节。在提取易失证据之后将计算机关机，需要注意的是在关机时要直接拔掉电源，对于笔记本电脑，还要卸下电池，防止由于关机程序造成的数据消失。

为了不破坏原始证据，在进行现场勘查和后期分析时不能对原始数据磁盘进行检验，应当对磁盘进行复制，详细过程见 1.4 节。

对于需要带回实验室进一步分析的计算机要扣押封存。封存原则：保证封条位置正确，不破坏封条则无法使用封存设备。可移动介质标上标签，装入防静电袋，封口处贴封条。

对于手机、平板电脑等能发射、接收无线信号的设备，为了防止嫌疑人远程销毁证据，需要放到手机信号屏蔽袋中，如图 1-17 所示。

每个封条具有唯一标识，并让证据的所有者在封条上签字确认；物证需贴标签，注明提取时间、人员姓名以及设备的名称、型号等信息。如图 1-18 所示为线缆标签。

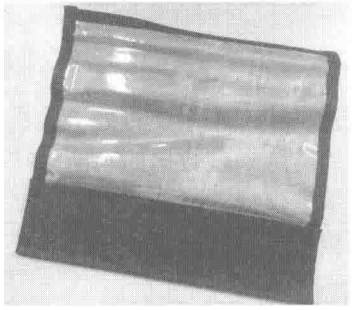

图 1-17　手机信号屏蔽袋

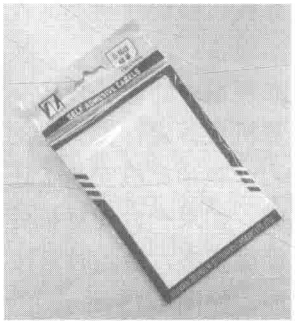

图 1-18　线缆标签

1.2　对主机运行程序的调查

计算机的运行依赖于操作系统和各种应用程序，计算机所运行的每一项任务都需要开辟一个进程，因此对正在运行的计算机进程和操作系统的服务进行调查，可以发现犯罪线索，这项工作在恶意代码类网络犯罪的勘查工作中显得尤为重要。

Autoruns 是一款强大的工具，可以查看系统的进程信息，并可以将进程与内存信息进行关联，以及将注册表与应用程序信息联系在一起。具体使用功能如下：

对于面向 Windows 系统的 Autoruns 工具，可以直接在微软的官方网站上下载，Autoruns 工具具有较高的权限，建议通过正规途径下载，防止其中含有恶意代码。当打开 Autoruns

时呈现如图 1-19 所示的界面。

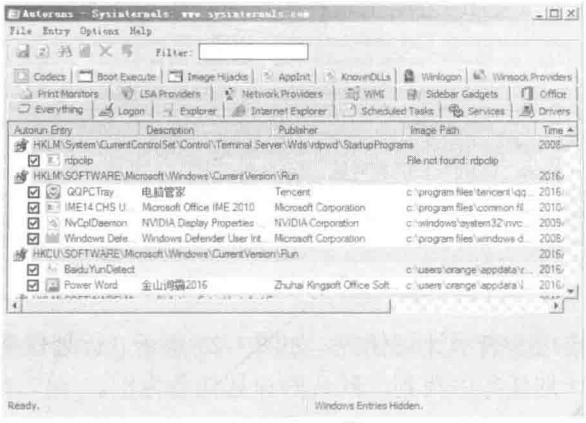

图 1-19　Autoruns 界面

在 Autoruns 的主窗口显示的是系统自启动的程序，在默认情况下，展示的是 Everything 选项卡，该选项卡将所有的自启动项都罗列在其中，并且展现了每个程序的入口、名称、发布者、磁盘路径以及时间戳等信息。

1. 主要选项卡的介绍

除了 Everything 选项卡，还可打开 Logon 选项卡，如图 1-20 所示，可以看到系统启动时的程序，这里面第一项和最后一项为 Windows 自带的程序，中间七项为用户安装的自启动程序。

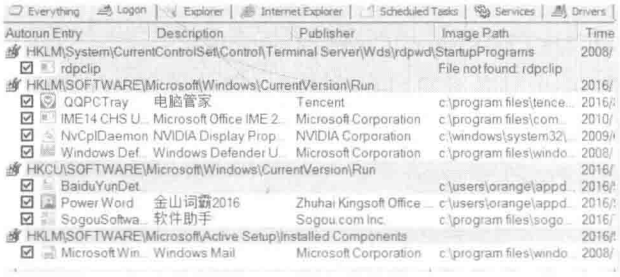

图 1-20　Autoruns 的 Logon 选项卡

Explorer 选项卡列举了注册表中资源管理器的键值，如图 1-21 所示。

图 1-21　Autoruns 的 Explorer 选项卡

Internet Explorer 选项卡对应的是 IE 所有浏览器帮助对象（BHO）、网络 URL 地址搜索钩子、各类 IE 工具条以及 IE 常用工具栏按钮所对应的注册表子项和注册表值项值，如图 1-22 所示。

图 1-22　Autoruns 的 Internet Explorer 选项卡

Scheduled Tasks 选项卡表示计划任务，如图 1-23 所示。计划任务同样可以在操作系统的“开始”菜单中的计划任务中找到，默认的计划任务为空。

图 1-23　Autoruns 的 Scheduled Tasks 选项卡

Services 选项卡即 HKLM\System\CurrentControlSet\Services 对应的开机自启动服务的项目，如图 1-24 所示。由于具备开机自启动功能，而且依靠 ROOTKIT 技术可以隐蔽运行，因此许多恶意软件寄存于开机自启动服务中。

图 1-24　Autoruns 的 Services 项卡

Drivers 选项卡即 HKLM\System\CurrentControlSet\Services，该项对应开机自启动驱动程序的项目，如图 1-25 所示。和上面的开机自启动服务一样，开机自启动驱动程序同样是恶意代码经常寄存的场所。

图 1-25　Autoruns 的 Drivers 选项卡

Image Hijacks 选项卡中的内容能够在开机后夺取系统的控制权，使系统不能正常运行，这是恶意代码经常驻留的地方，如图 1-26 所示。

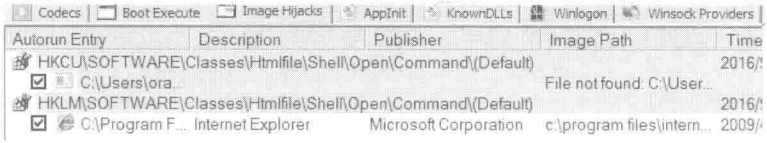

图 1-26　Autoruns 的 Image Hijacks 选项卡

AppInit 选项卡用于初始化动态链接库，其内容是开机时系统加载的必要的初始化动态链接库文件。除了卡巴斯基等少数软件需要通过添加 DLL 文件到此处实现从开机就接管系统底层的目的外，一般此项目应为空。

KnownDLLs 选项卡显示系统中已知的 DLL 文件。

Winlogon 选项卡显示 Winlogon 登录项对应的自启动注册表子项及值项。

Winsock Providers 选项卡显示已注册的 Winsock 协议，包括 Winsock 服务商。由于目前只有很少的工具能够移除该项目下的内容，恶意软件经常伪装成 Winsock 服务商实现自我安装。Autoruns 可以卸载此项目下的内容，但不能禁用它们。

Print Monitos 选项卡显示在 Print Spooler 服务中被加载的 DLL 文件。一些恶意软件可能利用此服务项目实现开机自启动。

LSA Providers 选项卡，其中，LSA 的全称为 Local Security Authority，即本地安全授权，是 Windows 系统中一个相当重要的服务，所有安全认证相关的处理都要通过这个服务。它从 Winlogon.exe 中获取用户的账号和密码，然后经过密钥机制处理，并和存储在账号数据库中的密钥进行对比，如果对比的结果匹配，LSA 就认为用户的身份有效，允许用户登录计算机。如果对比的结果不匹配，LSA 就认为用户的身份无效，这时用户就无法登录计算机。

2. 主要功能菜单的介绍

在菜单栏有一个望远镜标志，可以用来查找和定位包含输入字段的所有自启动子项和值项，是比较实用的功能，如图 1-27 所示。

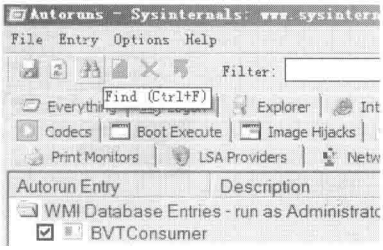

图 1-27　Autoruns 的 Find 功能