科爱传播
KE'AI COMMUNICATIONS

21世纪信息安全大系

Windows取证分析

（附DVD工具包）

Windows Forensic Analysis

【美】Harlan Carvey 著

王智慧 崔孝晨 陆道宏 译

科学出版社

Windows Forensic Analysis
Windows 取证分析

〔美〕 Harlan Carvey 著

王智慧 崔孝晨 陆道宏 译

科学出版社

北京

图字：01-2008-2323 号

ISBN 10：1-59749-156-X
ISBN 13：978-1-59749-156-3

图书在版编目(CIP)数据

Windows 取证分析/（美）Harlan Carvey 著；王智慧，崔孝晨，陆道宏译. —北京：科学出版社，2009
ISBN 978-7-03-023308-0

Ⅰ. W… Ⅱ. ①卡…②王…③崔…④陆… Ⅲ. 窗口软件，Windows-安全技术 Ⅳ. TP316.7

中国版本图书馆 CIP 数据核字（2008）第 169820 号

责任编辑：田慎鹏 霍志国/责任校对：张怡君
责任印制：钱玉芬/封面设计：耕者设计工作室

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销

*

2009 年 1 月第 一 版 开本：787×1092 1/16
2009 年 1 月第一次印刷 印张：15
印数：1—4 000 字数：320 000

定价：45.00元（含DVD光盘）
（如有印装质量问题，我社负责调换）

作者致谢

首先要感谢上帝赐给我生命中的一切，对于这一切我将永远感激。

感谢我生命中的爱和光——Terri，以及她美丽的女儿 Kylie。她们的耐心和理解是对我写作这第二本书的极大支持。我知道在我进入思考、字斟句酌的时候冷落了她们。和我这样的呆子生活在一起对这两个美丽的女人来说并不容易。

同时要感谢很多人对本书的贡献，无论大小，对本书的形成都是必不可少的。Jesse Kornblum 需要特别感谢，他不仅是本书的技术编辑，还是一个很好的朋友，并且他提供了很多建议，落实到书中。也要感谢 Jesse 在计算机取证领域的贡献，他的作品包括 FRED 磁盘工具、哈希工具等，还有很多计算机取证领域的论文。感谢 Cory Altheide，是他提供了跟踪 USB 设备在 Windows 系统中遗留的痕迹的想法。感谢 Andreas Schuster 在计算机取证领域当前和未来的贡献，包括 Windows 内存分析领域。其他为本书带来帮助的人包括 Aaron Walters，FATKit 工具的作者之一；通用动力（General Dynamics）高级信息系统的 Bill Harback；GSG Systems 公司的总裁 George M. Garner；密尔沃基警察局 Richard F. Mcquown 侦探；格温特郡警察局高科技犯罪调查科 Jon Evans 侦探；以及计算机取证分析专家 Don Lewis。

作者简介

Harlan Carvey（CISSP），同时也是《Windows 取证和事件恢复》（*Windows Forensics and Incident Recovery*）一书的作者。Harlan Carvey 是硅谷北部和大都会地区的计算机取证与应急响应顾问，现在他为全美所有地区的客户提供紧急事件响应和计算机取证服务。Harlan 的专业领域集中在 Windows 2000 及其后续平台的的应急响应、注册表和内存分析、以及事后的计算机取证分析。Harlan 曾作为专职的安全工程师提供漏洞评估和渗透测试服务。Harlan 也为联邦政府部门提供应急响应和计算机取证服务。

Harlan 曾获得弗吉利亚军事学院（Virginia Military Institute）电子工程学士学位和拉瓦尔研究生学院（Naval Postgraduate School）电子工程硕士学位

Harlan 在此对他的妻子——Terri，在本书写作过程中的支持、耐心和幽默表示感谢。

技术编辑

Jesse D. Kornblum 是 ManTech SMA 首席计算机取证工程师。现在为情报部门人员开发新的计算机取证工具和技术。Jesse 居住于华盛顿特区，是数个领域研究的开拓者，包括自动应急响应、模糊哈希和 Windows 内存分析。而且，他独立开发了几个广为使用的计算机取证工具，例如 md5deep 和 foremost。Jesse 现在是《数字调查》期刊的编委，并且为 ForensicsWiki 项目贡献了很多内容。Jesse 曾作为特别调查员为美国空军提供计算机犯罪调查服务。

Dave Kleiman（CAS，CCE，CIFI，CISM，CISSP，ISSAP，ISSMP，MCSE），从 1990 年开始就在信息安全领域工作。现在，他创建了 SecurityBreachResponse. com 网站，也是 Securit-e-Doc 公司的首席信息安全官。在此之前，他是 Intelliswitch 公司的技术运营副总裁，对国际通信和因特网进行监控。Dave 是一个安全专家，作为前佛罗里达州认证的司法官员，他擅长计算机取证调查、应急响应、入侵分析、安全审计和安全网络架构。Dave 为网络专家写过几本 Windows 方面的安全安装和配置指南，他开发的 Windows 操作系统防护工具——S-Lok（www. s-doc. com/products/slok. asp），比 NSA、NIST 和微软的通用安全指南更加好用。

Dave 参与了《微软 Log Parser 工具包》（*Microsoft Log Parser Toolkit*. Syngress Publishing，ISBN：1-932266-52-6）一书的写作。他经常参加国家安全会议的演讲，同时为很多安全相关的时事通讯、网站和网络论坛写稿。Dave 参加了数个安全相关的组织，包括国际反恐和安全专家协会（IACSP）、国际计算机取证分析员组织（ISFCE）、信息系统审计和控制协会（ISACA）、高科技犯罪调查协会（HTCIA）、网络和系统专家协会（NaSPA）、认证的欺诈检查人员协会（ACFE）、反恐委员会（ATAB）和 ASIS 国际。他也是 FBI InfraGard 高级会员、区域主席和国际信息系统取证协会（IIS-FA）的教育主管。

技术评审

Troy Larson是微软网络安全小组的高级取证工程师，他的工作就是分析微软最新的技术并保持取证实践技术的先进性。Troy是针对Windows和Office取证问题的讲师，当前专注于开发Vista和Office2007的取证技术。在加入微软取证小组之前，Troy工作于Ernst & Young国际取证实践和事务公司。Troy是华盛顿州Bar组织会员，毕业于加州大学伯克利分校并获得法律学士学位。

译者简介

王智慧 副研究员，1995年毕业于中国科技大学化学物理系，2006年毕业于清华大学电子工程系，获硕士学位。现就职于北京华夏物证鉴定中心，从事声像资料及电子物证鉴定，是中国合格评定国家认可委员会（CNAS）批准的授权签字人。

崔孝晨 2000年获华东政法学院法学学士学位，2006年毕业于复旦大学计算机科学与技术系（第二本科）。现就职于上海市公安局信安处，从事计算机取证和恶意软件分析工作。

陆道宏 1995年毕业于华东理工大学计算机与科学系，获硕士学位，长期从事信息安全与计算机取证研究工作。2004年合伙创建上海盘石数码信息技术有限公司，领导开发了盘石计算机取证系统（SafeImager）、盘石介质取证分析系统（SafeAnalyzer）、盘石手机取证分析系统（SafeMobile）等系列计算机取证专业工具。

序

自从1991年在美国召开的国际计算机专家会议上首次提出“计算机取证（Computer Forensic）”术语以来，随着互联网的普及和计算机犯罪案件的增多，计算机取证一直是信息安全领域中的热门话题，国际上几乎每年都要召开以计算机取证为主题的学术会议，用于计算机取证的技术工具逐渐发展成为信息安全产业的一个特殊种类，甚至很快也有了诸如“国际计算机证据组织（IOCE）”之类的“非政府”组织。自然，近年有关计算机取证的专业书籍也出版不少，其中涉及基础理论、取证技术和取证工具的专著先后被译介到国内，这些工作对国内计算机取证的研究和实践都起到了十分重要的推动作用。

因而，当王智慧先生将他与几位朋友的译著《Windows取证分析》的清样送来之后，我是怀着几分欣喜，利用两个周末的余暇认真奉读的。所以如此，一是因为智慧本人一直致力于，也乐于、长于计算机取证工作，在理论功底和实践经验上颇有见地并屡建奇功，能入他法眼的书籍自有不凡之处；二是因为对Windows的取证是现实生活中最常见，也最复杂的一项工作。据智慧介绍，原书作者Harlan Carvey曾在美国军方长期从事信息安全工作，有过十多年的取证工作经验，并且有过《Windows取证和事件恢复》一书面世，颇受业内人士推崇。有着这样的专业背景，加上今年岁末难得的晴天暖阳，我的两个周末是在愉快地阅读中度过的。

掩卷之时，正值满月初升。回味本书，觉得有三点特别的感受不得不说：一是知识内容上的创新。初看书名，很容易会先入为主地把它看作作者旧作《Windows取证和事件恢复》的翻版。其实不然，正如作者在前言中声明的，他不想将此书写成旧作的续集，细读本书中对开机取证、注册表分析的深入解析和在文件分析、内存分析、Rootkits分析方面的独到体会，你会相信作者说到做到了。二是技术工具上的创意。本书介绍了不少现实可用的取证工具，这些工具能帮助读者更好地理解和体会作者在书中提出和阐述的概念，而且这些工具并非对Encase之类的商业产品的简单罗列，而是精选了不少当下热门的“活的”网上新宠，尤其可喜的是，有的工具就是作者本人的杰作，用自己的看家本领说事，应该算是有创意。三是实践经验上的创见。由于作者在此领域有十多年的工作经验，本书中列举的实例很多是自身实践的积累，不少实例是在其他同类书籍中找不到的。例如结合英国布莱尔政府Word格式文档的信息泄露案例，作者介绍的与“对象链接嵌入技术（OLE）流”相关的信息痕迹与恢复经验，以及反复强调的可重复性和取证数据的自动化处理等体会，也都是其他著述鲜有涉猎的。

当然，如果要说本书不够过瘾的地方，可能要算第6章“可执行文件分析”部分，这本是当前恶意软件（间谍软件）作恶的重要环节。由于涉及逆向工程技术，作者的意见是可以就此另写一本书，因而分析不深。另外，从理论上讲，本书对分布式取证、自动化取证的后处理、数据挖掘和包括交换文件、休眠文件等在内的内存分析等热点问题尚可再深入一些。考虑到本书专为实践需要而写，面面俱到反倒有些苛求和不妥。

有过几次译书的经历，我知道翻译专业书籍的艰辛，尤其是信息安全这样的全新领域，技术发展快，概念创新多，要把一些特定的概念术语和技术细节译好，绝非易事。值得高兴的是，几位年轻朋友在本书的翻译中下了不少功夫，如将 live response 转意为“开机取证”，就没有拘泥于原文，但却传达了原意，用心良苦，可见一斑。

我把奉读清样后的感受写下来，算是对同行朋友们开拓视野、勇于冒险、敢于干译书这种“费力不讨好”的公益事业的一种支持和鼓励。一孔之见，权充为序。

吴世忠

二 OO 八年十二月十三日

于昆明湖畔

前　言

本书的写作目的来自实战需要。很多计算机取证专家在调查中过度依赖取证工具得出的结果，并不了解信息来自哪里或是怎样创建和推导出来的。“任天堂式取证”（加载获取的镜像，按一个键就能生成结果）的时代已经过去了。作为分析和检验人员，不能再希望取证调查是这种方式。网络犯罪手段和形式越来越复杂，调查人员需要理解系统中存在哪些证据要素，这些要素是怎样产生和修改的。只有掌握了这些知识，我们才能理解一些要素确实是证据所在，而且现在有很多关于反取证的演讲和论文资料，在一些主流的会议上都有关于针对取证分析专家培训和工具的反取证技术议题，一些技术正使得取证更加困难。本书旨在加深对取证信息的深入理解，不仅列举了调查人员从开机系统及获取的镜像中能够得到的信息，也提供了定位更多取证信息要素的方法。

本书的主要意图在于对取证社群的反馈，从这个社群中我得到了很多。我在信息安全领域从业超过 10 年（之前是在军方从事物理和通信安全方面的工作），期间遇到过很多厉害的人，也做过很多有趣的事，得到过很多人的帮助，这使我逐渐深入到安全和取证研究的领域。我的一些研究成果在不同的会议上发表，这又带来更多的问题和讨论，推动研究的进一步发展。知识的不断交流和讨论带动知识的发展，从而提高了整个研究领域的水平。

本书主要讨论 Windows 系统开机和关机的不同时刻对证据数据收集和分析的技术问题，但是不可能涉及每个方面，还有很多方面值得研究和深入。如果本书能够带动读者对 Windows 系统更加深入的调查和分析，就达到目的了。

目标读者

本书关注 Windows 取证分析这一技术领域，该领域相对来说比较狭窄，推荐正在从事 Windows 取证分析工作或者对这方面感兴趣的人阅读本书。本书可以作为一个有用的参考书，一些读者可能会觉得本书技术太过深奥、超过了个人的理解力，但我的感觉是取证需要逐步积累，可以将本书中的内容作为探寻和研究的起点。我开始写本书的时候，就没有想写成我的第一本书《Windows 取证和事件恢复》的续，而是要在 Windows 取证领域提供一些更加基础、更加全面的参考资源，不仅为了我自己，也为其他在计算机取证领域工作的人们。

本书写作的过程中，我的目标是为取证分析人员、调查人员和应急响应人员提供一个参考资源。取证人员就不说了，对于面临应急响应压力的系统管理员来说，就是要消除他们的疑问：“我应该怎么做?”。在这个前提下，本书逐步消除一些当前应急响应的误解，例如，擦除硬盘、重装系统等。有时给系统打补丁也不能解决问题，可能导致再次入侵，所以必须找到问题的根源。

本书可以为公司和政府的调查人员、司法官员和顾问提供参考和帮助，同时也可以

为在学校开发或参加计算机取证学位学习的研究人员提供帮助。

贯穿全书，调查人员、第一响应人员、分析员和管理员这几种称呼是可以交换使用的。因为在不同的场景下一个人可能变换不同的角色。一些情况下，调查人员会与公司的管理员一起工作，使用域管理员账户来收集数据。有时管理员陪同调查人员或应急响应人员使用管理员级别的用户账户来调查被入侵的系统。不要被这些名词混淆了，大部分情况下都是同样的意思。

通读本书时注意几件事请。首先，有很多 Perl 脚本编写的程序。选择 Perl 脚本并非一些神奇的原因：只是 Perl 脚本非常灵活而强大。我喜欢修改代码直接运行而不需要重新编译。说到编译，如果你从来没有用过 Perl 或是对 Perl 不熟悉，也不用担心。除了极少数例外，书中的大部分 Perl 脚本都同时提供了使用 Perl2Exe 程序编译的、可以在 Windows 系统中独立运行的可执行程序版本。这些执行程序可以在不安装 Perl 的情况下直接运行（书中使用的 Perl 版本可以从 ActiveState. com 或其他地方免费下载）。Perl 的另外一个特色是可以跨平台，随书附赠的光盘中提供的从二进制文件中提取数据的 Perl 脚本基本上都可以跨平台运行。光盘中编译好的独立执行程序只能在 Windows 平台运行，但是 Perl 脚本可以在 Windows，Linux，甚至 Mac OS X 平台运行。很多光盘中的脚本都在 Linux 的 Perl 环境中测试并成功运行。因而，分析人员并不局限于使用某一特定平台。一些脚本需要安装附加的模块，可以通过 Perl 包管理程序（PPM）来安装。PPM 是 ActiveState 发行的 Perl 程序的一部分，可以用于 Windows，Linux，Mac OS X 和一些其他平台。另一个使用 Perl 的实用效果是自动化。我发现，数据提取、二进制分析等很多工作会不断地重复，手工提取总是会犯一些错误。如果提取和分析任务可以使用 Perl 自动化处理，就可以写好代码，这样在做同样任务的时候就不会发生错误。如果流程已经就绪，对流程的调整还是很简单的——我发现只有在不知道该做什么的时候，调整才是特别困难的。

本书使用的取证分析程序是来自 Technology Pathways 的 ProDiscover 应急响应版。感谢 Chris Brown 的慷慨，我从版本 3.0 的时候就开始用 ProDsicover，而且极其简单易用。ProDiscover 分析 Windows 系统的镜像非常好，有很多易用而强大的功能。Chris 和 Alex Augustin 对问题的反馈和更新也很及时，与 Ted Augusting 在会议上交谈时，发现他在取证领域具有深厚的知识背景。ProDiscover 本身是个很好的分析平台，应急响应版本则在现场响应方面简单实用，可以方便地收集易失数据。同样，以我的观点来看，Chris 选择 Perl 作为 ProDiscover 的脚本非常明智。调查员可以使用 Perl 脚本（ProScripts）扩展对镜像的分析功能（例如，搜索、数据提取和细微的数据分析）。随书附赠的光盘中包含我写的几个常用的分析脚本（注意，ProScripts 是 Perl 脚本，而不是使用 Perl2Exe 编译的程序，在和 ProDiscover 一起使用的时候必须使用脚本的方式）。

本书内容组织

本书共分为 7 章。

第 1 章　开机取证：数据收集

本章解决从开机系统中收集易变数据的基本问题。由于网络犯罪的复杂化、存储容量的不断增长等原因，开机取证得到了更多的关注。开机取证不仅吸引了取证顾问（例

如，我）的注意，而且政府部门的专业人员也开始在调查过程中采用该技术从开机系统中收集易变数据。本章列举了收集易变数据的技术和工具，同时介绍了取证服务器项目（Forensic Server Project）。

第 2 章　开机取证：数据分析

将数据获取和数据分析分开是因为这是两个问题。很多情况下，需要获取的数据并不改变，例如，在特定时间得到系统活动的快照。这时候，数据的解释就对案件很重要了。同样，有时候我们到达现场，发现初始事件报告只是对系统活动特征的描述，而不触及问题根本所在。在开机取证过程中，怎样对收集的数据进行分析、如何找到想要的信息，常常依赖于案件性质，欺诈、入侵、恶意软件的案件各不相同。本章展现了一个对开机取证收集到的数据进行相关分析的框架，从而使得对系统行为的刻画和问题根本原因的识别变得更加简单易懂。

第 3 章　Windows 内存分析

自从 2005 年夏天 Windows 内存分析技术被正式介绍以来，对这一课题的研究已真正启动。过去，在开机系统中获取的物理内存数据只用来搜索字符串（例如，密码、IP 地址和电子邮件地址），然后数据就进入存档了。不幸的是，以这种方式发现的信息很少提供上下文环境。感谢 DFRWS 2005 内存分析挑战带来的研究成果，获取的内存可以使用更细的粒度被识别和调查，甚至可以提取执行文件的镜像。本章讨论获取和分析内存镜像的问题，同时也包括从开机系统中提取特定进程的内存数据。

第 4 章　注册表分析

Windows 注册表维护了大量（可以说过多的）关于系统状态的信息。很多情况下，注册表可以视为日志文件，因为注册表也以特定方式记录了时间戳。不过，由于数据记录存储方面的原因，使用 ASCII 或者 unicode 字符串搜索并不能得到很有价值的信息。本章将揭秘注册表结构，使读者能从二进制存储及删除空间中找到注册表数据单元。随后将用很大篇幅讨论注册表中不同的数据项（注册表中键/值），描述这些键值对调查的价值，同时讨论了用来从获取的镜像中提取信息的很多工具。

第 5 章　文件分析

很多调查人员忽略了 Windows 系统维护的一些列的日志文件，这些日志文件通常对记录的项目都有时间戳信息，而且一些文件中的时间戳信息可以作为对事件进行时间分析的一部分。很多时间戳是由应用程序维护，并不立即呈现。本章详细讨论各种不同的文件、文件格式和文件的元数据，并且包括提取信息的工具。

第 6 章　可执行文件分析

可执行文件是文件分析中一个特例。因为需要在不同版本的 Windows 系统中运行，可执行文件一般具有已知、一致的文档结构。不过，恶意软件的作者找到了混淆文件结构的方法，使得恶意软件更加难以（虽然不是不可能）分析。通过理解这些文件的格式及常规文件的结构，分析人员可以在调查中识别哪些文件是合法的、可疑文件对 Windows 系统的影响，以及恶意软件具有的因素。

第 7 章　Rootkits 及其检测

最后一章讨论系统级木马（Rootkits）的问题，希望对这一充满神秘色彩的恶意软件的讨论能给管理员、现场响应人员和分析人员（记住这可能是同一个人）提供定位和

识别 Rootkits 的有力武器。Rootkits 的使用在迅速增长，不仅网络犯罪分子在使用，一些“合法”的商业应用程序也在用。对 Rootkits 及其检测技术的理解是在 Windows 系统领域工作的最难点，本章详述对这一领域进行调查的各种技术。

光盘内容

本书附赠的光盘包括很多有价值的信息和工具。所有的工具都按照章节组织到不同的目录中，包括每章的代码和样例程序（第 7 章除外）。另外，有一个附加的目录包括一些不属于任何一章的几个工具，主要是我在实际工作中开发的，希望能有所帮助。

所有光盘上的工具都是 Perl 脚本。不过几乎所有的 Perl 脚本都已“编译”成简单易用的 Windows 独立执行程序。Perl 脚本自身是平台独立的，可以在 Windows，Linux，甚至 Mac OS X 操作系统运行。编译的 Windows 执行程序是为了方便未安装 Perl 的用户使用。有几章还包括 ProScripts，这是专为 Technology Pathways 公司（www. techpathways. com）的 ProDiscover 取证分析工具编写的 Perl 脚本。

另外，有几章目录中包括了样例文件，读者可以通过这些文件熟悉工具的用途。尤其是第 5 章提供了不少文件。使用工具解释其用途是一回事，但是真要使用它来提取信息就是另外一回事了。通过样例文件，读者可以在任何地方（例如，飞机上）通过笔记本使用这些工具，而不需要自己获取文件。

最后，光盘中还包括了几个视频文件。这些视频文件（. wmv）对书中谈到的工具进行演示，涉及的工具也在光盘上。过去，我通过写附录来解释取证服务器项目的安装和使用，但是发现听录音、看视频比看书更加有效。

光盘中提供的所有工具仅供“参考”，作者对其使用不做任何担保。除了 bonus 目录中的工具之外，所有工具在书中都有描述。因而，读者通过本书可以了解工具的用途。所有的 Perl 脚本编译的 exe 工具都提供了源代码脚本，全部基于命令行，双击运行不会产生有效的输出。大部分工具需要文件名（包括全路径）作为命令行参数。如果使用中有问题，可以看 Perl 脚本的源码，或者通过“-h”参数来显示帮助信息。如果还有问题，可以发送电子邮件到 keydet89@yahoo. com，附加简洁、完整的问题描述，我会看问题出在哪里。

由于授权的问题，其他人所写的第三方工具没有包括在光盘中，但在书中提供了工具的链接。

非常感谢！希望你能觉得本书有用并喜欢它。有任何问题，请和我联系。

——Harlan Carvey

目　录