TURING 图灵程序设计丛书

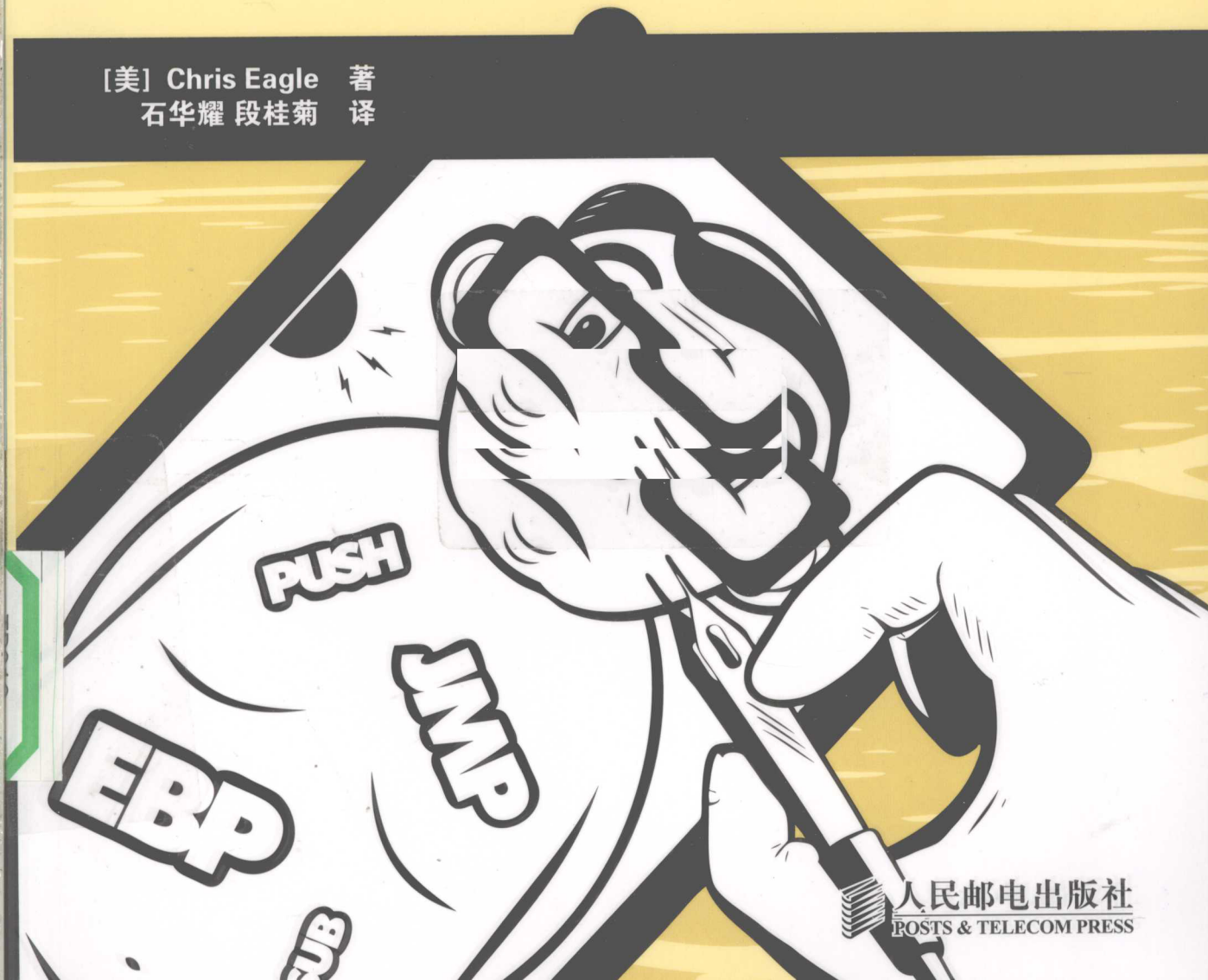
no starch press

The IDA Pro Book

The Unofficial Guide to the World's Most Popular Disassembler

IDA Pro权威指南

[美] Chris Eagle 著
石华耀 段桂菊 译



人民邮电出版社
POSTS & TELECOM PRESS

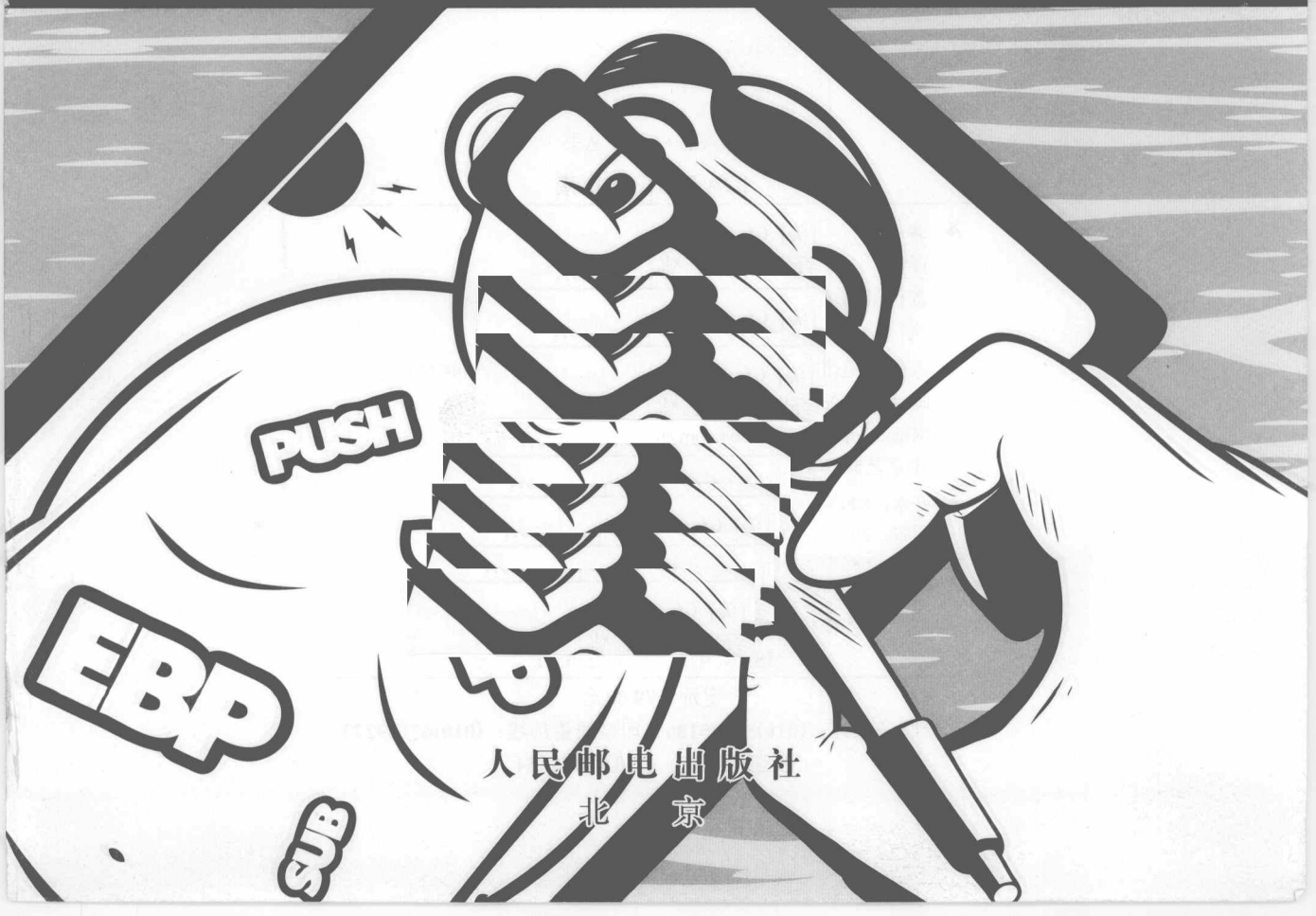
TURING 图灵程序设计丛书

The IDA Pro Book

The Unofficial Guide to the World's Most Popular Disassembler

IDA Pro权威指南

[美] Chris Eagle 著
石华耀 段桂菊 译



人民邮电出版社
北京

图书在版编目（CIP）数据

IDA Pro 权威指南 /（美）伊格尔（Eagle, C.）著；
石华耀，段桂菊译．—北京：人民邮电出版社，2010.3
（图灵程序设计丛书）
ISBN 978-7-115-22263-3

Ⅰ.①I… Ⅱ.①伊…②石…③段… Ⅲ.①反汇编
程序 Ⅳ.① TP313

中国版本图书馆CIP数据核字（2010）第017240号

内 容 提 要

本书一共分为六个部分，以反汇编与逆向工程的基本信息和 IDA Pro 的背景知识开篇，为读者奠定基础，紧接着循序渐进地讲解 IDA Pro 的基本使用、高级使用、扩展功能和它在安全领域的实际应用，最后介绍 IDA 调试器，一方面让用户对 IDA Pro 有全面深入的了解，另一方面让读者掌握 IDA Pro 在现实中的应用。

本书适合 IT 领域的所有安全工作者阅读。

图灵程序设计丛书

IDA Pro权威指南

◆ 著 [美] Chris Eagle
译 石华耀 段桂菊
责任编辑 傅志红
执行编辑 谢灵芝

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：29
字数：685千字 2010年3月第1版
印数：1－3 000册 2010年3月北京第1次印刷

著作权合同登记号 图字：01-2008-5833号

ISBN 978-7-115-22263-3

定价：79.00元

读者服务热线：(010)51095186 印装质量热线：(010)67129223
反盗版热线：(010)67171154

版权声明

译 者 序

说到IDA Pro，相信有过逆向工程经验的读者一定不会陌生。事实上，IDA Pro是目前应用最广的静态反汇编工具，它已经成为分析恶意代码、研究漏洞攻击的主要工具。这款软件具有交互式、可编程、可扩展等特点，支持各种处理器和平台，功能非常强大。也因为如此，一些用户可能觉得IDA Pro过于复杂，对其望而生畏。

本书是一本专门介绍IDA Pro的著作，它由浅入深，由基本的界面到复杂的功能，全面而翔实地介绍了IDA Pro的用法，并提供了大量应用实例。相信通过本书，喜爱IDA Pro的用户一定能够迅速掌握IDA Pro的用法，这也是我们翻译和出版本书的初衷。

如本书作者在前言中所述，本书主要以IDA 5.2为介绍对象。当然，和其他软件一样，从诞生的那一天起，IDA Pro这款商业软件就在不断地发展更新。到本书出版时为止，IDA 5.5已经发布，而本书的内容是IDA所有版本的使用者都必须掌握的，有关新版本的新增功能，感兴趣的读者可以通过访问Hex-Rays网站（http://www.hex-rays.com/idapro/55/index.htm）查阅。读完本书你会发现，它是目前为止最全面的IDA Pro译作，其内容不仅适用于初学者，也适用于IDA的高级用户。

由于IDA功能极其强大，涉及诸多方面的专业知识，加之时间仓促，译文难免存在疏漏，还请读者指正。

石华耀

2009年12月

序

上个世纪90年代中期，当IDA Pro的开发者Ilfak Guilfanov和我决定离开共享软件领域，转向专业市场时，我并没有预见到，10多年后，IDA会在IT安全领域扮演如此重要的角色。但是，当IDA赢得市场份额后，我们多次听到用户的抱怨：它的文档资料不够，且不说质量是否够高，至少在表述上还不够好。要知道，grep要求很严格，文档不能出错。

这些年有几本有关IDA的书面市。虽然其中一些书有了重大的突破，我们也始终感谢这些作者推广我们的劳动成果，但我们一直没有看到理想的IDA图书——那种既告诉我们如何使用IDA，又教会我们如何扩展它以解决新问题的书。

确实，撰写有关IDA图书需要有很大的勇气。一本描述如此复杂的工具的书不可能只是蜻蜓点水，薄薄的小册子是绝对交待不过去的。这是一个大型项目，需要作者投入大量时间，并且必须仔细规划。作者必须对数量惊人的信息进行整理并归入各个章节中。这才仅仅是开始，你不能将大量的信息硬塞给一个无助的读者，还希望得到最佳效果。所以，作者还必须是一名经验丰富的教师。

当然，拿到书后，它的实际益处需要根据读者能够利用它做什么来评估。最基本的是你想要从中学会什么，而不是信息本身。当然，名师出高徒，学生学得怎么样，还要看老师教得好不好。

最后同样重要的是，IDA图书的目标读者也许是技术最为熟练的IT专业人士。乐观主义者认为他们明辨是非，而悲观主义者则认为他们吹毛求疵。你需要一套既权威又令人信服的理论来使这群人满意。由于有这么多苛刻的要求，许多年来，撰写一本优秀的IDA图书似乎一直是件不可能的事。

Chris Eagle出现了。我第一次注意到Chris是在他发布他的模拟器插件时。那时，我还在直接参与恶意代码分析，并且知道模拟是解决所有问题的正确方法，只是这需要做大量工作。一个发布模拟器源代码的人，与一群发布攻击教程的所谓的黑客，他们之间有着明显的区别。

让人印象更深刻的是，Chris愿与他人分享自己的劳动成果。我清楚地知道，有另外几个IDA用户已经开发出了非常优秀的处理器模块和附加件，但他们一直保密，这些知识从未得到共享。令人遗憾的是，这有悖于IDA的开放式体系架构。Chris是第一个打破这种藩篱的优秀的IDA用户。很快，Ilfak和我在心底里默默企望，Chirs，或者某个像Chris一样的人，能够撰写一本有关IDA Pro的图书。不久，我们的希望变成了实现。当我翻开Chris诚心诚意送来给我审阅的PDF文件时，我心里的喜悦之情溢于言表。

信息量有多大？自己看！Chris做了大量工作，收集并整理了尽可能多的信息，最终撰写出这

本言简意赅的书。本书结构紧凑，与现在的许多IT图书截然不同。在这本书里，你看不到花里胡哨的样式、毫无价值的截图、含糊其辞的概述和浪费页面的表格。

教学方法是什么？自己看！本书设置了各种情景，并以此为基础，由使用IDA的基础功能顺理成章地扩展到利用其最强大的功能（脚本和可扩展性）来处理实际的复杂问题。本书证明，Chris拥有很高的教学天赋。

你能够学到什么知识？自己看！Chris很好地把握了问题的核心，他首先描述一个问题，然后有条不紊地设计解决方案。他从不满足于只能临时应急的解决办法。虽然他提供的方法需要读者付出更大的努力才能完成，但我们知道，他提供的是正确的方法。

有哪些权威的观点？自己看！Chris的模拟器是公开发布的IDA插件中最有用的插件之一。他已经撰写了一些有关IDA的重要论文，并多次宣讲和演示。多年来，他一直是一位受人尊敬的IDA公告牌撰写人。从他作品的字里行间，我们可以体会他精益求精的态度。

恰当的材料，充足的时间，于是诞生了这本书。它是迄今为止最全面、最准确、最好的IDA Pro图书。希望你和我们一样喜欢这本书。

Pierre Vandevenne，1996年至2007年的IDA Pro研发者

2008年7月于比利时列日市

前　言

这些年来，人们曾无数次地问我一个问题：究竟应该如何开始逆向工程？当然，回答这个问题并不容易，因为每个人的具体情况都不一样。一些人希望阅读一本有关这个主题的好书，另一些人宁愿参加培训，还有人却愿意坐下来自学必要的技能。我应该属于最后一类，在逆向工程方面，我主要靠自学，尽管我在计算机工程和计算机科学方面接受了良好的正规教育。接受正规教育通常是达到某种目的（如取得学位）的途径，不过更多的是为我研究某个我更感兴趣的、非专业的领域而服务。

如果想进入逆向工程领域，需要特别强调的是，你必须培养熟练的编程技能。你最好是爱上代码，甚至是吃饭、睡觉、呼吸都离不开代码。如果你害怕编程，那么逆向工程可能不适合你。就我而言，编程和逆向工程就像做《纽约时报》上的填字游戏一样——解决特别困难的问题总是会有所回报。

我撰写本书的目的，是帮助其他人学习使用IDA和培养对逆向工程的兴趣。我想通过本书为读者提供一些更加具体的内容，而不是让大家花几个小时听我漫谈IDA和各种逆向工程问题。

阅读本书的方式多种多样。对逆向工程知之甚少的用户可以从第1章和第2章开始，了解有关逆向工程和反汇编器的一些信息；对IDA了解不多、希望深入学习的用户可以从第3章开始，这一章主要介绍IDA的基本布局；第4章则描述如何启动IDA并加载二进制文件；第5章到第7章介绍IDA的主要界面窗口和基本功能。

对IDA有一定了解的读者可以从第8章开始阅读，这一章讨论如何使用IDA处理复杂的数据结构，包括C++类；而第9章则介绍IDA交叉引用，它是IDA基于图形的显示（也在第9章介绍）的基础；第10章说明如何在非Windows平台上（Linux或OS X）运行IDA。

更加高级的IDA用户可能会发现，第11章到第14章是不错的起点，主要介绍IDA的高级用法及其自带的一些工具。第11章简要说明IDA的一些配置选项；第12章描述IDA的FLIRT/FLAIR技术和相关工具，我们利用它们开发签名，并利用这些签名将库代码与应用程序代码区分开来；第13章讨论IDA类型库及如何扩展类型库；而第14章则回答一些常见的问题，说明IDA是否可用于修补二进制文件。

IDA是一款即装即用的强大工具，可扩展是它的一个最大的优点，这些年来，用户利用这一优点让IDA完成了一些非常有趣的任务。IDA的可扩展性在第15章到第19章讨论。第15章介绍IDA的脚本功能，并系统讨论IDA的SDK（软件开发工具包）提供的编程API；第16章全面介绍SDK；而第17章到第19章则讨论插件、文件加载器和处理器模块。

介绍完IDA的全部功能后，第20章至第23章转而讨论IDA在逆向工程方面更加实际的用法，分析各种编译器的区别（第20章），介绍如何使用IDA分析恶意软件中常见的模糊代码（第21章），以及如何利用IDA发现和分析漏洞（第22章）。第23章则介绍这些年来发布的一些有用的IDA扩展（插件），以此结束这一部分的讨论。

最后，第24章至第26章介绍IDA的内置调试器。第24章首先介绍调试器的基本功能；第25章讨论使用调试器分析模糊代码遇到的一些挑战，以及调试器与反汇编器的集成；第26章则讨论IDA的远程调试功能。

本书在很大程度上以IDA 5.2为介绍对象，这主要是因为5.2版与5.1版和5.0版有许多相似之处。Hex-Rays公司非常慷慨，为用户提供了一个免费版本。IDA免费版是IDA 4.9的一个删减了部分功能的版本。本书讨论的大部分IDA功能也适用于免费版本，附录A简要介绍了用户在使用免费版本时可能遇到的一些不同之处。

首先学习IDA脚本功能，然后逐步学习如何创建编译插件，这似乎是一个自然的发展过程。因此，我们在附录B中全面介绍了每一个IDC函数及其对应的SDK操作。有时候，你可以在IDC函数与SDK函数之间建立起一一对应的关系（尽管这些函数的名称并不相同）；其他情况下，单独一个IDC函数可能等同于几个SDK函数调用。附录B回答了这个问题："我知道如何用IDC完成某个任务，但是，如何使用插件完成这个任务呢？"附录B中的信息通过逆向工程IDA内核获得，根据IDA的非传统许可协议，这样做完全合法。

在整本书中，我都尽量使用较短的代码说明问题。绝大多数的示例代码，以及许多用于生成示例的二进制文件，都可以在本书的官方网站上找到，其地址为http://www.idabook.com/。在那里，你还可以找到本书并未包含的一些示例，以及本书所使用的所有参考文献（如脚注中引用的URL的最新链接）。

致　谢

首先，最重要的是感谢我的家人，感谢他们在我撰写本书时对我的容忍。没有他们的耐心和宽容，我将一事无成。感谢Ole，我期待再次与他共进晚餐，以便我们可以讨论逆向工程。

我还要感谢本书的技术编辑Tim Vidas，感谢他在整个过程中所付出的一切劳动。对于我所有异乎寻常的想法，无论是否与本书有关，他都提出他的看法，并为我提供了大量建议。感谢Sk3wl过去和现在的所有成员，感谢他们让我的工作充满乐趣。希望他们也和我一样，从我们的合作中获益良多。

值得一提的是，如果不是Halvar多年前向我介绍IDA，可能永远也不会有这本书。退一步说，就算不提Halvar的功劳，如果没有IDA开发者Ilfak的鼓励，我也绝不会动手写这本书，对于Ilfak，我充满感激。这些年来，Ilfak始终慷慨地帮助我，我衷心地希望，这本书符合他对IDA质量设定的高标准。

最后，我想感谢No Starch出版社的所有工作人员，感谢他们为本书顺利出版所付出的辛苦劳动（他们考虑得非常周到）。Bill Pollock非常善解人意，因为就在我正要决定写一本有关IDA的书时，就接到了他的电话。感谢Adam Wright为出版本书投入的热情，许多时候，都是他的鼓励促使我前进。最后，感谢Megan Dunchak迅速完成文稿的编辑工作，其速度快到我几乎没有察觉到。大家的帮助使我的写作变得如此轻松，这对我来说意义重大，要知道，我喜欢编写代码，但不擅长写东西。

目 录

第一部分 IDA 简介

第二部分 IDA 基本用法

Part 1 第一部分

IDA 简介

本部分内容

第1章 反汇编简介

拿到一本专门介绍IDA Pro的书，你很可能急切地想知道书里会讲些什么。很明显，本书以IDA为中心，但我并不希望读者将其作为IDA Pro用户手册。相反，本书旨在将IDA作为推动逆向工程技术讨论的工具。你会发现，在分析各种软件（包括易受攻击的应用程序和恶意软件）时，这些技术非常有用。在适当的时候，我将提供在使用IDA时需要遵循的详细步骤，好让你执行与你手头的任务有关的特殊操作。因此，我将简略地介绍IDA的功能，包括最初分析文件时需要执行的基本任务，最后讨论IDA的高级用法和定制功能（用来解决更具挑战性的逆向工程问题）。我不会介绍IDA的所有功能。但是，你将发现，在应对逆向工程挑战时，本书介绍的功能极其有用，这也使得IDA成为你工具箱中最强大的武器。

在详细介绍IDA之前，了解反汇编过程的一些基础知识，以及其他一些对编译代码进行逆向工程的可用工具，会有一定好处。虽然这些工具的功能都不如IDA全面，但它们具备IDA的一部分功能，有助于我们了解IDA的某些功能。本章的剩余部分主要介绍反汇编过程。

1.1 反汇编理论

任何学过编程语言的人都知道，编程语言分为好几代，下面为那些上课不认真的读者简要总结一下。

- **第一代语言**。这些语言是最低级的语言，一般由0和1或某些简写编码（如十六进制码）组成。只有像Skape[①]这样的超人才能读懂它们。由于数据和指令看起来都差不多，人们往往很难将它们区分开来。因此，这种语言很容易造成混淆。第一代语言也称为*机器语言*，有时也叫做*字节码*，而机器语言程序常被称为二进制文件。
- **第二代语言**。第二代语言也叫*汇编语言*，它只是一种脱离了机器语言的查找方式。通常，汇编语言会将具体的位模式或操作码，与短小且易于记忆的字符序列（即助记符）对应起来。有时候，这些助记符确实有助于程序员记住与它们有关的指令。汇编器是程序员用来将汇编语言程序转换成能够执行的机器语言的工具。
- **第三代语言**。这些语言引入了关键字和结构（它们是程序的构建块），因而其表达能力更

① Skape是Metasploit团队的核心成员，并且是一位全面的二进制分析师。