《你必须知道的.NET》读书笔记：从Hello World认识IL

2018-08-20 阅读 171

> 通用的语言基础是.NET运行的基础，当我们对程序运行的结果有异议的时候，如何透过本质看表面，需要我们从底层来入手探索，这时候，IL便是我们必须知道的基础。

一、IL基础概念

1.1 什么是IL?

IL是.NET框架中间语言（**Intermediate Language**）的缩写。使用.NET框架提供的编译器可以直接将源程序编译为.exe或.dll文件，但此时编译出来的程序代码并不是CPU能直接执行的机器代码，而是一种中间语言IL（Intermediate Language）的代码。

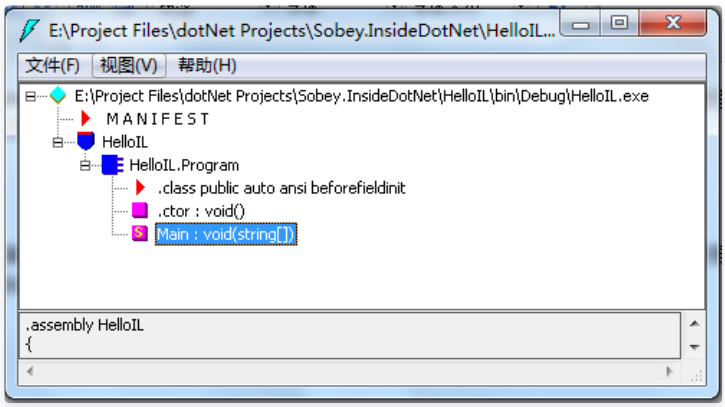
1.2 为何要了解IL?

元数据和IL是CLR的基础，了解必要的IL是深入认识CLR的捷径，我们没有理由放弃一条可以直接通达大门的便捷之路而盲目地以其他的方式追求深入。同时，大量的事例分析都是以IL来揭秘的，因此了解IL是读懂他人代码的必备基础，可以给自己更多的收获。

二、IL分析工具

2.1 ILASM.exe和ILDASM.exe

.NET Framework中自带了一套成熟的编译于反编译利器：ILASM.exe和ILDASM.exe，其中ILASM.exe工具用来执行IL代码并生成可执行程序，而ILDASM.exe则用来反编译可执行程序（反编译为IL代码进行查看）。



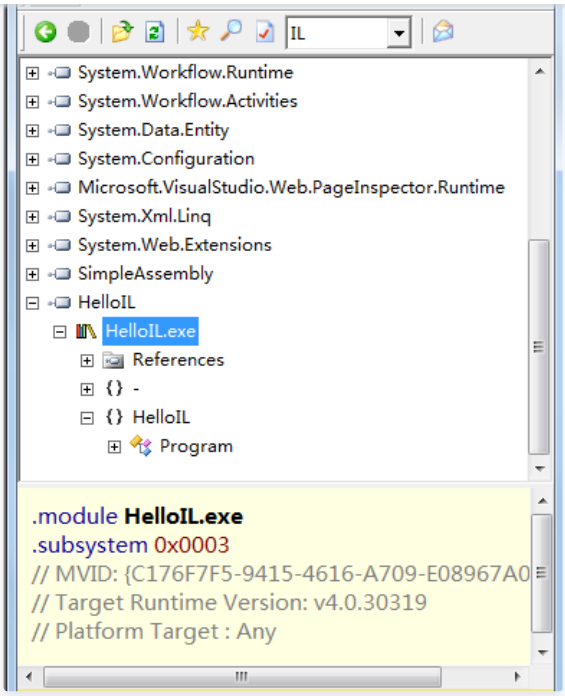
2.2 Reflector.exe

Reflector是由微软员工Lutz Roeder编写的免费程序。Reflector的出现使·NET程序员眼前豁然开朗，因为这个免费工具可以将·NET程序集中的IL反编译成C#或者Visual Basic代码。除了能将IL转换为C#或Visual Basic以外，Reflector还能够提供程序集中类及其成员的概要信息、提供查看程序集中IL的能力以及提供对第三方插件的支持。

目录

Edison Zhou
关注 专栏

文章 阅读量 获赞 作者排名
409 122.2K 1K 403



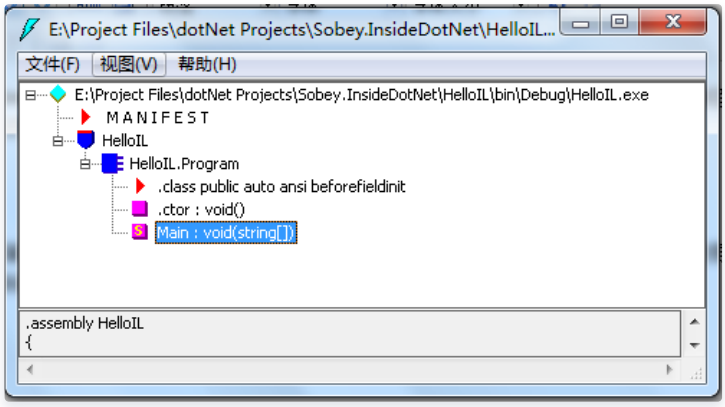
三、一个Hello World的IL之旅

3.1 准备一个Hello World程序

```
using System;
using System.Data;

namespace HelloIL
{
    public class Program
    {
        public static void Main(string[] args)
        {
            Console.WriteLine("Hello World!");
        }
    }
}
```

3.2 利用ILDASM体验IL

（1）对编译后的可执行文件HelloIL.exe，使用ILDasm.exe进行反编译，将会还原HelloIL为IL编码，结构如下：



分为两个部分：MANIFEST和HelloIL程序集。

（2）其中，MANIFEST是附加信息列表，主要包含了程序集的一些属性：程序集名称、版本号、哈希算法、程序集模块等，以及对外部引用程序集的引用项：

目录

```
{
  .publickeytoken = (B7 7A 5C 56 19 34 E0 89 )
  .ver 4:0:0:0
}
.assembly HelloIL
{
  .custom instance void [mscorlib]System.Runtime.CompilerServices.Cc
  .custom instance void [mscorlib]System.Runtime.CompilerServices.Ru

  .hash algorithm 0x00008004
  .ver 1:0:0:0
}
.module HelloIL.exe
// MVID: {C176F7F5-9415-4616-A709-E08967A0C6A0}
.imagebase 0x00400000
.file alignment 0x00000200
.stackreserve 0x00100000
.subsystem 0x0003       // WINDOWS_CUI
.corflags 0x00000001    //  ILONLY
// Image base: 0x00000000003C0000
```

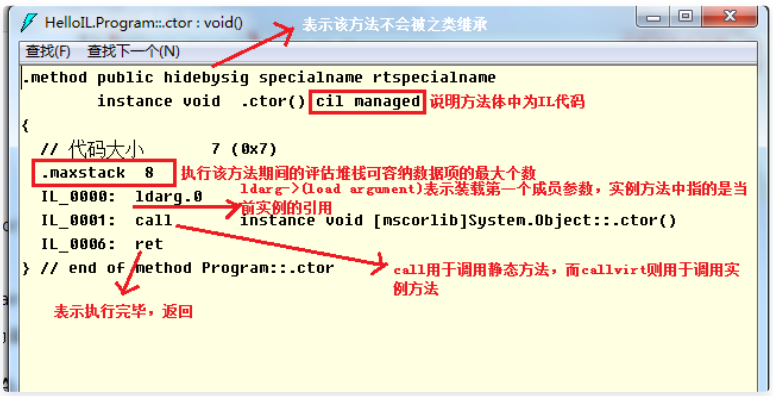
① **.assembly**指令用于定义编译目标或者加载外部库：这里只加载了mscorlib核心库，而System.Data被忽略，有效避免了过度加载引起的代码膨胀；

② **.ctor**指令表示构造函数，代码里没有任何显示构造函数，因此这里调用基类System.Object的构造函数（System.Object位于mscorlib程序集中）；

（3）其次，HelloIL程序集是我们要分析的重点：

① 首先是Program类

② 然后是ctor方法（构造方法）



③ 最后是Main方法

目录

```
{
  .entrypoint 表明CLR加载该程序时，首先从该方法开始执行，即将Main方法作为入口点。
  // 代码大小       13 (0xd)
  .maxstack  8
  IL_0000:  nop 即No Operation 没有任何操作，我们也不用管它
  IL_0001:  ldstr      "Hello World!" 将字符串压栈，此时"Hello World!"被移到栈顶
  IL_0006:  call       void [mscorlib]System.Console::WriteLine(string)
  IL_000b:  nop
  IL_000c:  ret
} // end of method Program::Main
```

（4）化繁为简，一览天下

这里将上面的IL代码简化一下，去粗取精来展现一下上面示例的IL代码，详细的分析以注释方式描述：

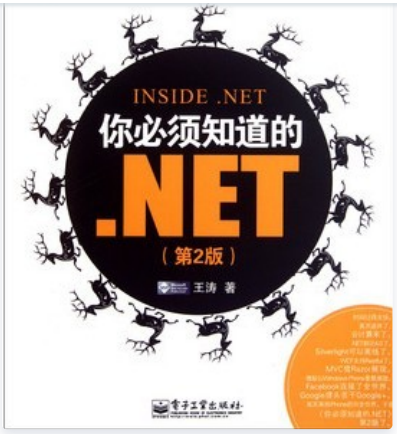
```
// 加载外部程序集
.assembly extern mscorlib
// 指定编译目标程序集
.assembly HelloIL

.class Program extends [mscorlib]System.Object
{
    .method public instanct void .ctor() cil managed
    {
        .maxstack 8
        // 调用基类构造函数
        ldarg.0
        call instance void [mscorlib]System.Object::.ctor()
        // 执行完毕，返回
        ret
    }

    .method static void Main() cil managed
    {
        // 表明程序入口点
        .entrypoint
        .maxstack 8
        // 装载string对象
        ldstr "Hello World!"
        // 调用静态方法WriteLine
        call void [mscorlib]System.Console::WriteLine(string)
        // 执行完毕，返回
        ret
    }
}
```

3.3 IL体验小结

通过一个Hello World示例，我们和IL进行了第一次的亲密接触。认识IL，是个循序渐进的过程，有了本次的小示例作为铺垫，我们可以轻松地认识简单的IL代码了。

参考资料

目录



（1）本文源自王涛(anytao)的《你必须知道的.NET（第二版）》，感谢金馆长熊猫表情。

（2）Zery，《读懂IL就这么简单（一）》

作者：周旭龙

出处：http://edisonchou.cnblogs.com

.NET 举报

点赞 2 分享

0 条评论 我来说两句

登录 后参与评论

相关文章

.NET面试题系列[2] - .NET框架基础知识(2)

面试出现频率：虽然很重要但不怎么出现，可能会考你定义，以及程序集包括什么，然后自然的话题就跑到反射上去了。

s055523

.NET高级特性-Emit

在这个大数据/云计算/人工智能研发普及的时代，Python的崛起以及Javascript的前后端的侵略，程序员与企业似乎越来越青睐动态语言所带来的便捷性与高效性...

目录

《你必须知道的.NET》读书笔记：方法表初窥

执行Main方法调用时，Three实例的创建与相应类型的加载也随之发生。然而，类型加载是在实例创建之前完成…

Edison Zhou

《你必须知道的.net》读书笔记 005——1.5 玩转接口

接口，理解这个东东用了好长的时间，从 2004年开始，写分页控件的时候需要实现一个接口，在网上找了一个例子，照猫画虎般的弄出来了，居然能用，但是完全没...

用户1174620

《你必须知道的.NET》读书笔记三：体验O…

此篇已收录至《你必须知道的.Net》读书笔记目录贴，点击访问该目录可以获取更多内容。

Edison Zhou

《你必须知道的.net》读书笔记 004 —— 1.4 多态的艺术

作者用了很大的篇幅讲解了一个程序，就是一个伪代码形式的，根据文件的扩展名打开文件的程序。比如要打开.doc的文件，那么就执行 OpenDocFile()函数。其...

用户1174620

《你必须知道的.net》读书笔记 001——1.1 对象的旅行

好久没看书了，上次看书的时候还是一年前了，一个偶然的机会，比较系统的看了一下OO的基础，封装、继承、多态等，当时真的是很不会，看了也是一知半解，迷迷...

用户1174620

《你必须知道的.net》读书笔记 002——1.2 什么是继承

1.2 什么是继承 “对于继承，就应该着手从这些容易误解与引起争论的话题来寻找关于全面认识和了解继承的答案。一点一滴摆出来，最后在对分析的要...

用户1174620

《你必须知道的.NET》读书笔记二：小OO…

此篇已收录至《你必须知道的.Net》读书笔记目录贴，点击访问该目录可以获取更多内容。

Edison Zhou

《你必须知道的.NET》读书笔记一：小OO…

此篇已收录至《你必须知道的.Net》读书笔记目录贴，点击访问该目录可以获取更多内容。

Edison Zhou

终于，我也要出一本C#的书了 - 我的写作历程与C#书单推荐

我于2012年3月开始工作，到现在马上就满六年了。这六年里，我从一个连Sql server

目录

《你必须知道的.net》读书笔记 007——2.3 开放封闭原则

开放封闭原则，核心思想：软件实体应该是可扩展，而不可修改的。也就是说，对扩展是开放的，而对修改是封闭的。 体现在两个方面： 1、对扩展开...

用户1174620

.NET面试题系列[1] - .NET框架基础知识(1)

面试出现频率：从来没人问过。事实上我都不知道怎么问，
考背书吗？倒是可以问问知不知道现在.NET最新版本是什…

s055523

厚积薄发，拥抱 .NET 2016

厚积薄发这个词是高三英语老师在高考前写在黑板上，高中
三年努力这么久，是时候迎面而上，冲刺向前。所以，一…

用户1161731

Go语言实战笔记（一）| Go包管理

这本是In Action系列的书籍，这个系列做研发的都知道，在研发届评价很多，很多新的技术、语言等都会有一本实战的书籍。既然是实战，那么这本书假设了他的读者有了...

飞雪无情

初识 C#

若尘_

写出好程序的11个技巧

有很多理由都能说明为什么我们应该写出清晰、可读性好的程序。最重要的一点，程序你只写一次，但以后会无数次的阅读。当你第二天回头来看你的代码时，你就要…

用户1289394

浅入 .NET Core 中的内存和GC知识

【1】https://docs.microsoft.com/zh-cn/dotnet/standard/managed-code

痴者工良

为什么 C# 的 string.Empty 是一个静态只读字段，而不是一个常…

使用 C# 语言编写字符串常量的时候，你可能会发现可以使用 "" 而不能使用 string.Empty。进一步可以发现 string.Empty 实...

walterlv

更多文章

目录

目录