工具：

1、.NET Reflector 8.3-反编译

2、reflexil IL-修改

3、ScanId-查壳

4、de4dot -脱壳

知识点：

1、.NET Reflector的简单使用

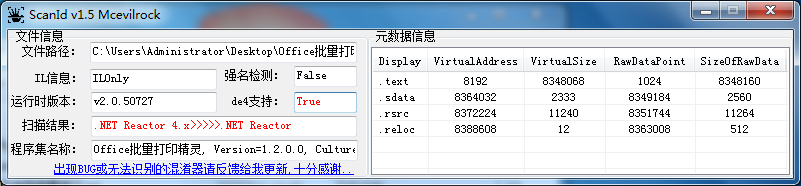
2、IL语法的简单使用

软件来源：

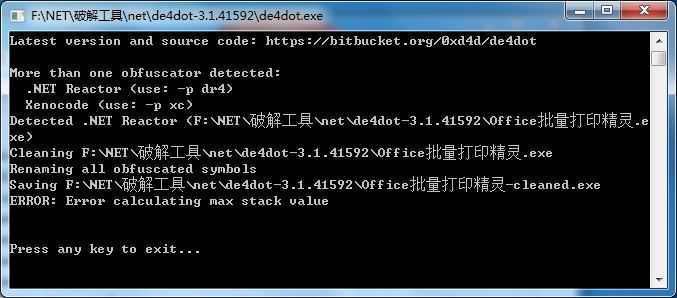
受@ damgda文章：<http://www.52pojie.cn/thread-339252-1-1.html> 启发，在学习练手的过程中决定一锅踹了这一系列软件。软件官网大家自己百度。

正文：

以下所提到的待破解程序都使用ScanId-查壳后，de4dot去混淆。

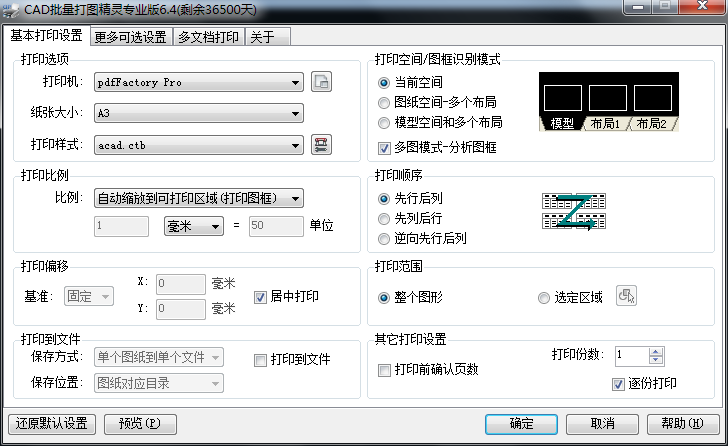
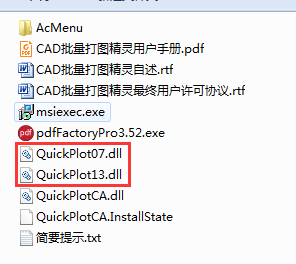


将待破解文件直接拖到de4dot的exe程序上就可以脱壳，不用敲命令行。

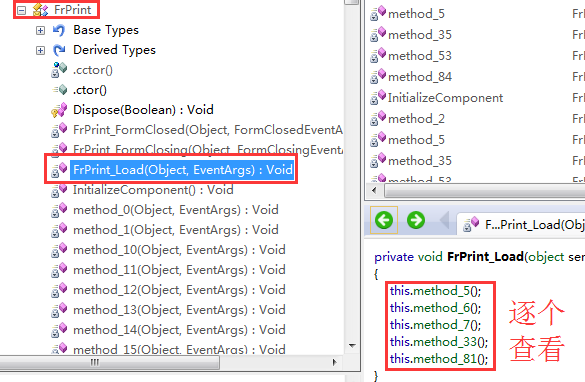


一、CAD批量打图精灵[QuickPloat]

需要CAD环境才可以测试，正好折腾装修的图纸，所以装了CAD2010，嘿嘿，真是天时地利啊，软件安装以后，找到了2个核心的dll，脱壳。



直接.NET Reflector打开，寻找主窗口，一般以frm，fr等打头（编程习惯），从frm\_load事件开始，我们看能找到些什么。



果然，第一个函数就是彩头，从这个窗体载入事件的逻辑我们可以看到，，再怎么折腾注册也会是个未注册版，除非替换这个文件。从作者的演示视频中我们也可以看到，确实注册以后作者会发给你2个dll文件替换。

private [void](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.Void" \o ) [method\_5](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_5())()

{

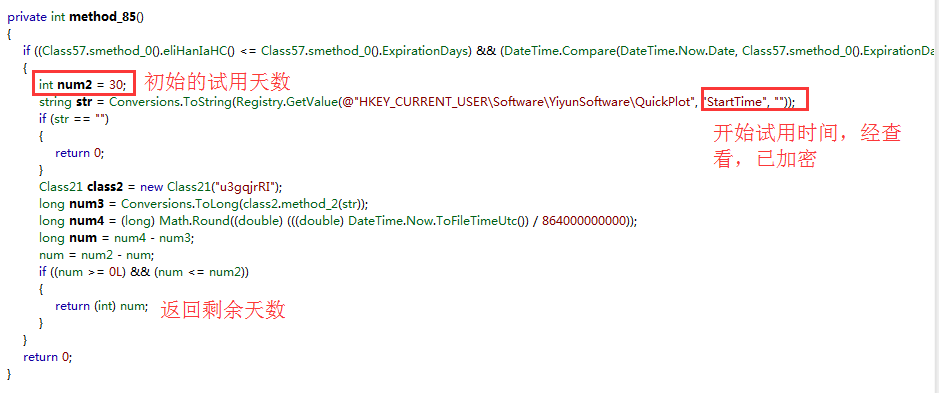
[int](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.Int32" \o ) num = this.[method\_85](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_85():Int32" \o )(); //获取剩余天数

this.[Text](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:4.0.0.0:b77a5c561934e089/System.Windows.Forms.Form/property:Text:String" \o ) = this.[Text](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:4.0.0.0:b77a5c561934e089/System.Windows.Forms.Form/property:Text:String" \o ) + "(剩余" + [Conversions](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.Conversions" \o ).[ToString](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.Conversions/ToString(Int32):String" \o )(num) + "天)";

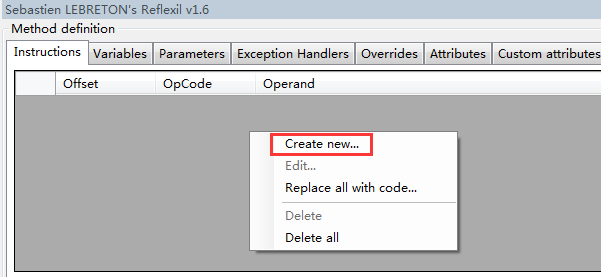
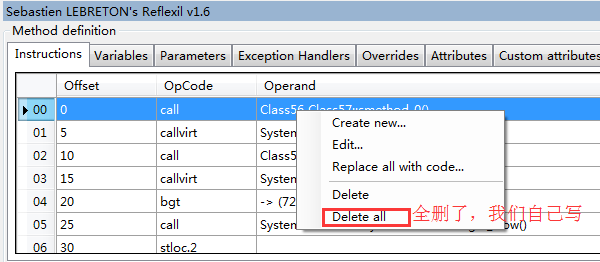
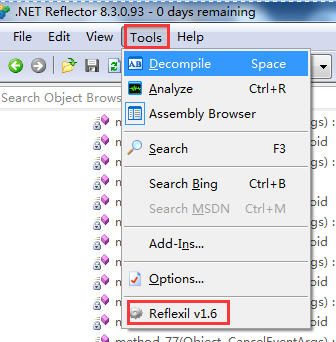
this.[vmethod\_68](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/vmethod_68():System.Windows.Forms.Label" \o )().[Text](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:4.0.0.0:b77a5c561934e089/System.Windows.Forms.Label/property:Text:String" \o ) = "未注册";

}

跟踪到：this.[method\_85](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_85():Int32" \o )()

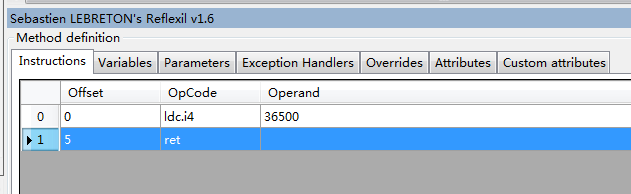


//直接修改返回天数,改个够用的数，因为后面还有很多地方都会调用这个函数，所以不能直接XX掉。具体方法：(后面修改同这，不再赘述)。

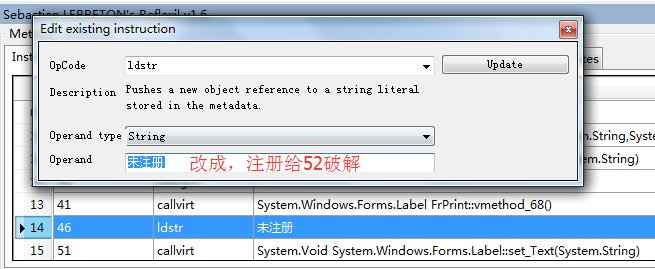


这里需要大家了解下IL，有汇编经验的应该学得很快，我也是边用边学，我菜鸟中的战斗公鸡，嘿嘿。（学习地址：http://www.cnblogs.com/flyingbirds123/archive/2011/01/29/1947626.html）

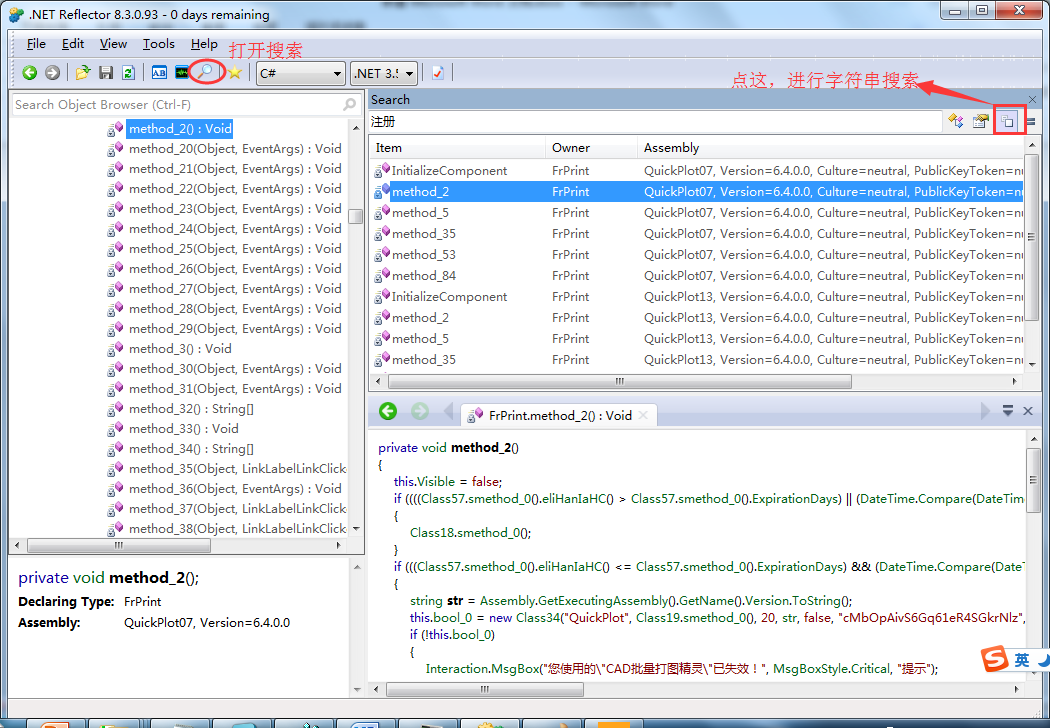
使用Ldc.I4指令，将所提供的 int32 类型的值作为 int32 推送到计算堆栈上。给100年，哈哈，够用。记得ret返回，任何程序片段的结束都要返回哦。



this.[vmethod\_68](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/vmethod_68():System.Windows.Forms.Label" \o )().[Text](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:4.0.0.0:b77a5c561934e089/System.Windows.Forms.Label/property:Text:String" \o ) = "未注册"; //改成已注册，给我们伟大的52破解论坛。



接下来搜索字符串“注册”，看看还有什么。



终于，找到了主要的注册判断函数。从这个函数的逻辑上来看，只要调用这个函数就会有提示框弹出，但是试用的时候没有弹出，可能哪个地方有优化吧，暂时没找到。下面对这个函数进行简单的分析。有源码就是简单易懂，呵呵。比ASM强多了。

|  |
| --- |
| private [void](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.Void" \o ) [method\_2](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_2())()  {  this.[Visible](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:4.0.0.0:b77a5c561934e089/System.Windows.Forms.Control/property:Visible:Boolean" \o ) = false;//自己不可见，可能是什么界面吧，没仔细看。  if (((([Class57](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57/smethod_0():Class56" \o )().[eliHanIaHC](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class56/eliHanIaHC():Int32" \o "int Class56.eliHanIaHC();  CTRL+Click to open in new tab.)() > [Class57](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57/smethod_0():Class56" \o )().[ExpirationDays](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class56/property:ExpirationDays:Int32" \o "int Class56.ExpirationDays { ... }  CTRL+Click to open in new tab.)) || ([DateTime](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.DateTime" \o "System.DateTime  CTRL+Click to open in new tab.).[Compare](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.DateTime/Compare(System.DateTime,System.DateTime):Int32" \o )([DateTime](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.DateTime" \o "System.DateTime  CTRL+Click to open in new tab.).[Now](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/System.DateTime/property:Now:System.DateTime" \o ).[Date](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/System.DateTime/property:Date:System.DateTime" \o ), [Class57](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57/smethod_0():Class56" \o )().[ExpirationDate](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class56/property:ExpirationDate:System.DateTime" \o "DateTime Class56.ExpirationDate { ... }  CTRL+Click to open in new tab.)) > 0)) || (this.[method\_85](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_85():Int32" \o )() == 0)) && ([Interaction](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.Interaction" \o "Microsoft.VisualBasic.Interaction  CTRL+Click to open in new tab.).[MsgBox](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.Interaction/MsgBox(Object,Microsoft.VisualBasic.MsgBoxStyle,Object):Microsoft.VisualBasic.MsgBoxResult" \o )("您使用的\"CAD批量打图精灵\"已超过试用期限，点\"确认\"查看注册流程。", [MsgBoxStyle](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.MsgBoxStyle" \o ).[OkCancel](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.MsgBoxStyle/OkCancel" \o ), "注册提示") == [MsgBoxResult](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.MsgBoxResult" \o ).[Ok](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.MsgBoxResult/Ok" \o )))  {  [Class18](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class18" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class18/smethod_0()" \o )();//跟踪了下，会转到作者主页，修改时上面全部干掉，防止弹框  }  if ((([Class57](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57/smethod_0():Class56" \o )().[eliHanIaHC](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class56/eliHanIaHC():Int32" \o "int Class56.eliHanIaHC();  CTRL+Click to open in new tab.)() <= [Class57](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57/smethod_0():Class56" \o )().[ExpirationDays](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class56/property:ExpirationDays:Int32" \o "int Class56.ExpirationDays { ... }  CTRL+Click to open in new tab.)) && ([DateTime](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.DateTime" \o "System.DateTime  CTRL+Click to open in new tab.).[Compare](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.DateTime/Compare(System.DateTime,System.DateTime):Int32" \o )([DateTime](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.DateTime" \o "System.DateTime  CTRL+Click to open in new tab.).[Now](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/System.DateTime/property:Now:System.DateTime" \o ).[Date](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/System.DateTime/property:Date:System.DateTime" \o ), [Class57](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class57/smethod_0():Class56" \o )().[ExpirationDate](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class56/property:ExpirationDate:System.DateTime" \o "DateTime Class56.ExpirationDate { ... }  CTRL+Click to open in new tab.)) <= 0)) && (this.[method\_85](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_85():Int32" \o )() != 0))  {  [string](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.String" \o ) str = [Assembly](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Reflection.Assembly" \o ).[GetExecutingAssembly](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Reflection.Assembly/GetExecutingAssembly():System.Reflection.Assembly" \o )().[GetName](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Reflection.Assembly/GetName():System.Reflection.AssemblyName" \o )().[Version](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/System.Reflection.AssemblyName/property:Version:System.Version" \o ).[ToString](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Version/ToString():String" \o )();  this.[bool\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/bool_0:Boolean" \o ) = new [Class34](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/.ctor(String,String,Int32,String,Boolean,String,String)" \o )("QuickPlot", [Class19](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class19" \o ).[smethod\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class19/smethod_0():String" \o )(), 20, str, false**/\*重点，打开的版本，FALSE=试用，TRUE注册\*/,** "cMbOpAivS6Gq61eR4SGkrNlz", "TQbLakcydsU0DknBkKCHnLn0XalLyrCl").[method\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/method_0():Boolean" \o )();//[method\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/method_0():Boolean" \o )**()关键方法，返回真，有戏，假，就直接OVER**  if (!this.[bool\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/bool_0:Boolean" \o ))  {  [Interaction](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.Interaction" \o ).[MsgBox](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.Interaction/MsgBox(Object,Microsoft.VisualBasic.MsgBoxStyle,Object):Microsoft.VisualBasic.MsgBoxResult" \o )("您使用的\"CAD批量打图精灵\"已失效！", [MsgBoxStyle](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.MsgBoxStyle" \o ).[Critical](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.MsgBoxStyle/Critical" \o ), "提示");  }  if (this.[bool\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/bool_0:Boolean" \o ))  {  [int](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.Int32" \o ) num = 0;  num = [Conversions](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.Conversions" \o ).[ToInteger](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.Conversions/ToInteger(Object):Int32" \o )([Application](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://acmgd:17.0.51.0/Autodesk.AutoCAD.ApplicationServices.Application" \o ).[GetSystemVariable](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://acmgd:17.0.51.0/Autodesk.AutoCAD.ApplicationServices.Application/GetSystemVariable(String):Object" \o )("BACKGROUNDPLOT"));  [Application](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://acmgd:17.0.51.0/Autodesk.AutoCAD.ApplicationServices.Application" \o ).[SetSystemVariable](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://acmgd:17.0.51.0/Autodesk.AutoCAD.ApplicationServices.Application/SetSystemVariable(String,Object)" \o )("BACKGROUNDPLOT", 0);  try  {  this.[method\_4](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_4()" \o )();  this.[method\_3](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_3()" \o )();  this.[method\_82](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/FrPrint/method_82()" \o )();  }  catch ([Exception](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Exception" \o ) exception1)  {  [ProjectData](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.ProjectData" \o ).[SetProjectError](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.ProjectData/SetProjectError(System.Exception)" \o )(exception1);  [ProjectData](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.ProjectData" \o ).[ClearProjectError](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://Microsoft.VisualBasic:8.0.0.0:b03f5f7f11d50a3a/Microsoft.VisualBasic.CompilerServices.ProjectData/ClearProjectError()" \o )();  }  finally  {  [Application](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://acmgd:17.0.51.0/Autodesk.AutoCAD.ApplicationServices.Application" \o ).[SetSystemVariable](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://acmgd:17.0.51.0/Autodesk.AutoCAD.ApplicationServices.Application/SetSystemVariable(String,Object)" \o )("BACKGROUNDPLOT", num);  [Class5](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class5" \o ).[frProgress\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class5/frProgress_0:FrProgress" \o ).[Close](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:2.0.0.0:b77a5c561934e089/System.Windows.Forms.Form/Close()" \o )();  }  }  }  if ([Class5](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class5" \o ).[bool\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class5/bool_0:Boolean" \o ))  {  this.[Visible](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:4.0.0.0:b77a5c561934e089/System.Windows.Forms.Control/property:Visible:Boolean" \o ) = true;  }  else  {  this.[Close](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://System.Windows.Forms:2.0.0.0:b77a5c561934e089/System.Windows.Forms.Form/Close()" \o )();  }  } |

|  |
| --- |
| 查看下这个.[method\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/method_0():Boolean" \o )()方法。  internal [bool](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.Boolean" \o ) [method\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/method_0():Boolean)()  {  [string](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.String" \o ) str;  [bool](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.Boolean" \o )[?](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Nullable%3cBoolean%3e" \o ) nullable = null;  [Random](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Random" \o ) random = new [Random](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Random/.ctor()" \o )();  if (random.[Next](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Random/Next(Int32):Int32" \o )(this.[int\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/int_0:Int32" \o )) == 0)  {  nullable = this.[method\_1](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/method_1():System.Nullable%3cBoolean%3e" \o )();//好像是从xml取注册数据，从上下文看的，图省事，这里直接改成True即可，我们往下跟踪了下他的实现  }  if (this.[bool\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/bool_0:Boolean" \o )) // 版本区分，注册和试用版  {  str = "tlic";  }  else  {  str = "rlic";  }  if (nullable == true)  {  [Registry](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/Microsoft.Win32.Registry" \o ).[SetValue](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/Microsoft.Win32.Registry/SetValue(String,String,Object,Microsoft.Win32.RegistryValueKind)" \o )(@"HKEY\_CURRENT\_USER\Software\YiyunSoftware\" + this.[string\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/string_0:String" \o ), str, "true", [RegistryValueKind](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/Microsoft.Win32.RegistryValueKind" \o ).[String](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/Microsoft.Win32.RegistryValueKind/String" \o ));  return true;  }  if (nullable == false)  {  [Registry](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/Microsoft.Win32.Registry" \o ).[SetValue](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/Microsoft.Win32.Registry/SetValue(String,String,Object,Microsoft.Win32.RegistryValueKind)" \o )(@"HKEY\_CURRENT\_USER\Software\YiyunSoftware\" + this.[string\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/string_0:String" \o ), str, "false", [RegistryValueKind](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/Microsoft.Win32.RegistryValueKind" \o ).[String](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:4.0.0.0:b77a5c561934e089/Microsoft.Win32.RegistryValueKind/String" \o ));  return false;  }  [object](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:65535.65535.65535.65535:b77a5c561934e089/System.Object" \o ) obj2 = [Registry](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/Microsoft.Win32.Registry" \o ).[GetValue](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/Microsoft.Win32.Registry/GetValue(String,String,Object):Object" \o )(@"HKEY\_CURRENT\_USER\Software\YiyunSoftware\" + this.[string\_0](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/string_0:String" \o ), str, true);  return ((obj2 != null) && [Convert](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Convert" \o ).[ToBoolean](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://mscorlib:2.0.0.0:b77a5c561934e089/System.Convert/ToBoolean(Object):Boolean" \o )(obj2));  }  往下看到一个线程的委托函数，是nullable的返回值，既然需要nullable返回true，那我们干脆将每个分支都改成true，修改2处  前面提到的new [Class34](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://QuickPlot07:6.4.0.0/Class34/.ctor(String,String,Int32,String,Boolean,String,String)" \o )（）构造函数中一个参数需要改成true，注册判断的时候这个True决定了版本  关于这些指令的修改位置是怎么找到的，需要大家对IL指令、程序流程的熟悉。我也是蒙的，嘿嘿。  注册失效时，打开软件主页，以防万一，使用BR指令修改（无条件地将控制转移到目标指令）。  前面提到了这个程序有点demo的性质，在后面发现了一处demo的特征，找了很久没找到限制打印的代码在哪里，不管了，先干掉意淫下。后面也测试了，没有发现只打印3页的问题，可能是注册了的缘故，有问题大家跟帖。  用软件查看，lb在，但是隐藏了，不可见。  经过以上的修改，其实这里完全可以把标题写专业版了。从作则网站的注册流程看到，注册以后会发个重新打包的版本给你，这个demo也就这样了，起码里面的核心功能没有缺失。  二、Office批量打印精灵  软件打开：  去混淆程序用.NET Reflector 8.3打开，按F3，搜索字符串 “注册”，经过分析发现注册授权检测类ObpgLicChecker，其中的成员函数BaseCheck(),程序会多次调用进行注册检测，我们需要直接从源头解决。  主要是移除一个if判断，并且在对类的私有成员赋值按成以后就返回，后面的垃圾代码就不用执行了。  打开reflexil，查看IL，直接删除掉不需要的判断，并在适当位置加入ret返回。修改好以后如上图。  下面顺便分析下哪些地方用到了这个类，选中这个类，Ctrl+R，打开分析窗口，直接展开到Used By，作者还是蛮狠心的，基本上主要的功能处都有是否注册的判断，但是我们不怕，因为我们堵住了源头，一切高枕无忧。  已改以上一处以后，保存，不处意外，已经注册成功。  接下来我们做些美化，并查看一些其他代码，是否有值得关注的地方。  注册按钮，判断method\_0()是否返回1，返回1，注册成功。  修改method\_0()的返回值，直接给1.  网络KEY注册的按钮  IL修改：  改完的效果  最后：加个破解的LOGO。  字符串搜索：“如果您有”  修改location主要是让标签创建的时候移动下位置，好看点，因为我们改了label中的内容，就不对中了。  选中，右键，Edit  修改标签单击事件，打开52破解论坛  修改结果：  至此，这个软件就完全破解完成。  三、MagicTable  这个软件给做机械制图的朋友，那真是牛逼哄哄啊。（因为我以前就是做大型机械结构件设计的，提取材料清单真的好方便）  老规矩，载入，查找“注册”字符串。  查看了下，发现会反复调用这个函数检测是否注册，跟第二个程序如出一辙。  改掉第一个判断。前面几个赋值完成就返回。  本来想加个LOGO给52，找了半天字符串都在资源里，就没改了，不知道怎么改，有人会的回帖哦，谢谢。(用HEX改就没试了) |
| CAD相关的2个软件需要在CAD中用命令行打开哦。破解文件直接覆盖就可以了。请对准以下版本覆盖。  2015年3月17日14:00:55  无痕 |
|  |

