[**操作步骤：用ildasm/ilasm修改IL代码**](http://www.cnblogs.com/dudu/archive/2011/05/17/ildasm_ilasm_il.html)

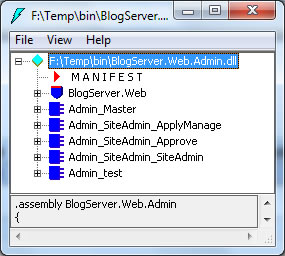
在开发中遇到这样一个场景，需要修改一个dll文件(.NET程序集)中某些地方的类型名称，但没有源代码，只能修改IL代码。

操作步骤如下：

1. 运行ildasm

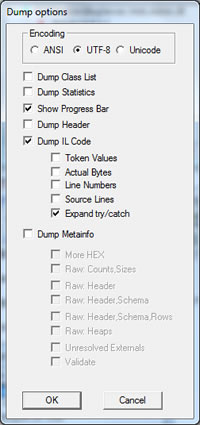
ildasm是由微软提供的.NET程序反编译工具，位于“C:\Program Files\Microsoft SDKs\Windows\v7.0A\bin\”。

2. 用ildasm打开要修改的程序集，如下图：

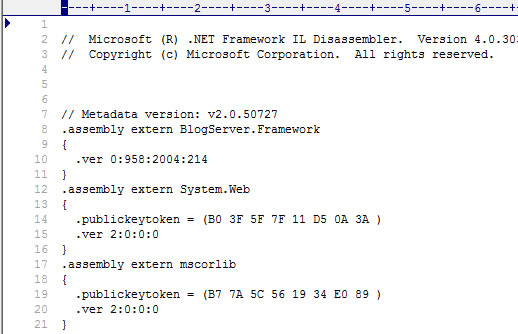


3. 通过ildasm保存为IL文件

选择菜单File>Dump，选择UTF-8编码，如下图：



4. 用文本编辑器打开第3步中得到的.il文件，如下图：



5. 修改.il文件中的代码并保存

6. 用ilasm（MSIL汇编程序）将.il文件编译为.dll文件

ilasm位于相应的.NET Framework目录中，比如：C:\Windows\Microsoft.NET\Framework\v2.0.50727\ilasm.exe

在命令行中执行下面的命令：

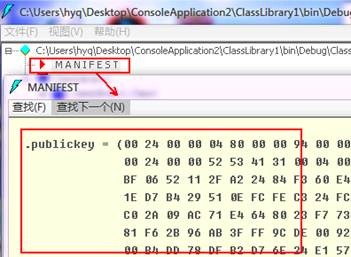
ilasm 源文件.il /output=目标文件.dll /dll

附：修改时如果有强命名的情况怎么处理

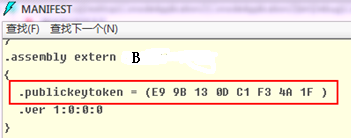
强名称程序集是否安全？

知道强名称签名验证后，我们来看看强名称程序集到底附加了什么信息，比如：强名称程序集A 引用强名称程序集B

-------强名称程序集B本身多出 .publickey 标识

[](http://images.cnblogs.com/cnblogs_com/heyuquan/201203/201203311919311374.jpg)

-------强名称程序集A对B的引用处多出 .publickeytoken 标识

[](http://images.cnblogs.com/cnblogs_com/heyuquan/201203/201203311919401562.png)

    通过Microsoft SDK 工具：ildasm.exe（IL反汇编工具），我们已经知道可以对程序集内容进行篡改，并且篡改的内容会因为强名称验证而报错。但是：

a)         如果把如上强名称程序集A的 .publickey 内容删除，那么A   
就不再是强名称程序集了，即在加载程序集A时不会进行强名称程序集A的篡改检查。那么这时候可以对A进行任意更改。

b)         A引用B时因为有.publickeytoken强名称标识所以要求B是强名称且生成和A中记录的相同公钥标识。如果仅仅删除A的.publickeytoken那么会报如下错误：

[1111](http://images.cnblogs.com/cnblogs_com/heyuquan/201204/201204020117098114.jpg)

因为找不到指定的强名称标识程序集（ [《(5)CLR 运行时探测程序集引用的步骤》](http://www.cnblogs.com/heyuquan/archive/2012/03/31/2427557.html) ），所以我们必须将B的.publickey内容一并删除。这样可以实现被引用的程序集任意更改。

来源： <<http://www.cnblogs.com/heyuquan/archive/2012/03/31/2427531.html>>

来源： <<http://www.cnblogs.com/dudu/archive/2011/05/17/ildasm_ilasm_il.html>>