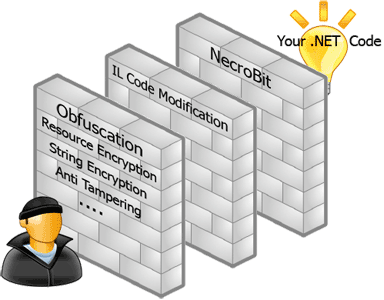
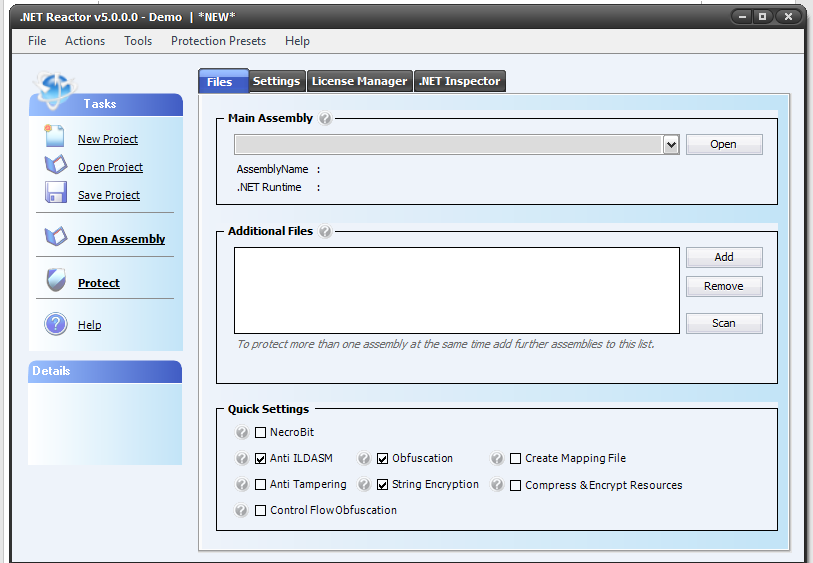
.Net Reactor 簡易功能說明





Step3 Click to protect your file

Step2 Quick Setting

Step1 Select your file

# Quick Setting

## NecroBit

防止程序被反編譯（比如.net reflector)，但不支持.net Compact Framework

## Anti ILDASM

防止被使用 ILDASM 來反編譯 IL code

## Anti Tampering

防止黑客利用工具修改程式，運行前會進行二進製完整性檢查

勾選A,B,C可以阻止反編譯程式進行反編譯，原先實作的方法會變成空

[MethodImpl(MethodImplOptions.NoInlining)]

private void InitializeComponent()

{

}

[MethodImpl(MethodImplOptions.NoInlining)]

public ACLCodeReferenceFunctionsForm(string code, bool isReadOnly = false)

{

}

## Native EXE file

轉換成不受管理的程式

勾選此選項加密出來的exe檔會無法執行，不建議勾選

## Pre-JIT method

把受管理的方法轉換成不受管理

勾選此選項加密出來的exe檔會無法執行，不建議勾選

## String Encryption :

字串加密，僅對字串進行加密。EX:”INSERT INTO …..”

範例如下:

cmd = "DELETE FROM [RoleACL] WHERE Code='{0}' AND RoleID='{1}'";

dt.Rows[i]["Role"]

上面程式碼在勾選String Encryption 之後會被轉變為

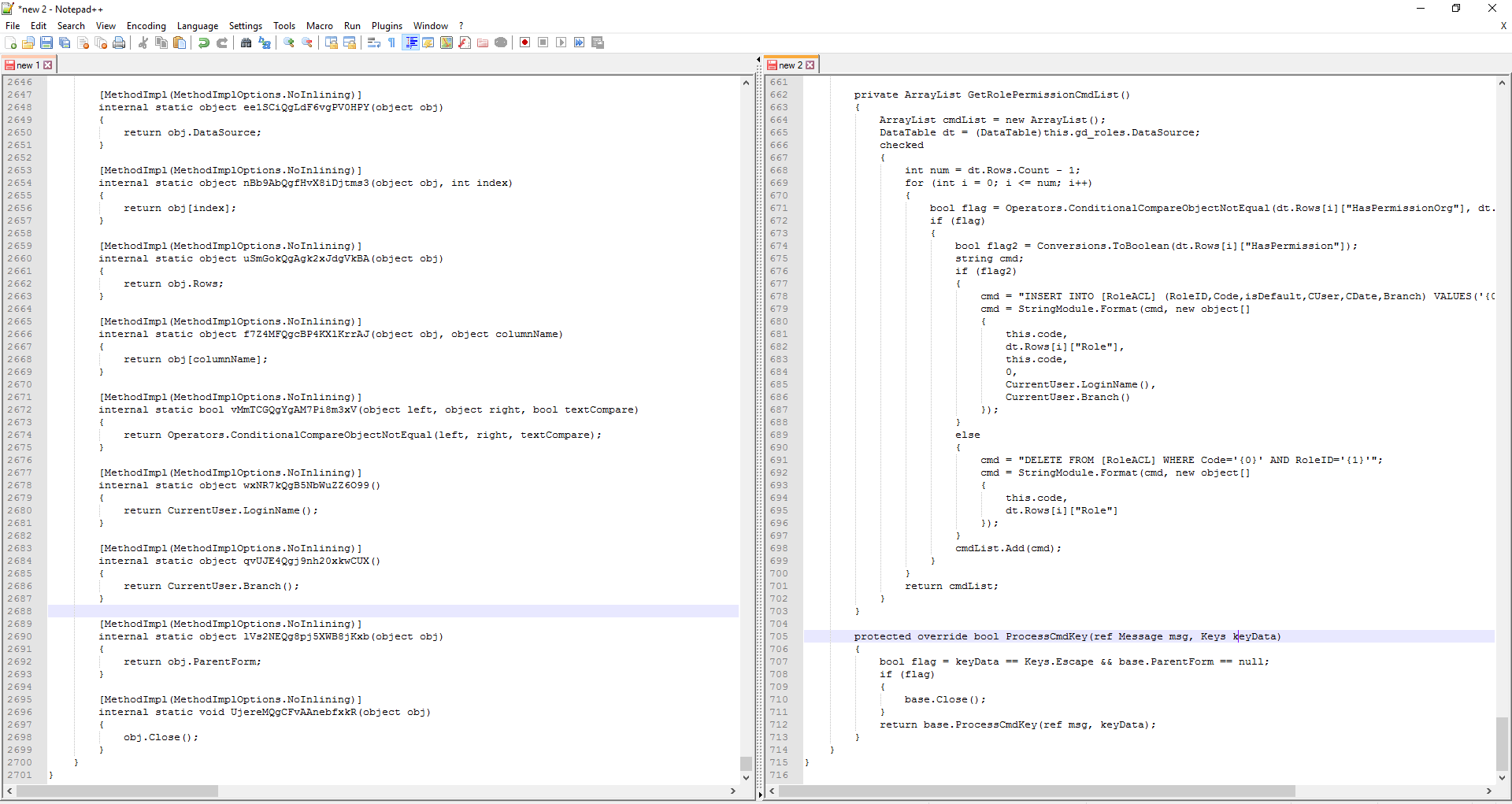
text = kgbOBx7BanbFa22Hp9.ol99ukmDA(1524832);

dataTable.Rows[i][kgbOBx7BanbFa22Hp9.ol99ukmDA(1522772)]

## Control Flow Obfuscation

把代碼轉換成 麵條式代碼（Spaghetti code），程式碼會變得混亂無法直接辨識出程式邏輯。(level 9 為最高安全層級)

範例如下: (程式會失去原版的架構)



[MethodImpl(MethodImplOptions.NoInlining)]

internal static object wxNR7kQgB5NbWuZZ6O99()

{

return CurrentUser.LoginName();

}

[MethodImpl(MethodImplOptions.NoInlining)]

internal static object qvUJE4Qgj9nh20xkwCUX()

{

return CurrentUser.Branch();

}

[MethodImpl(MethodImplOptions.NoInlining)]

internal static object lVs2NEQg8pj5XWB8jKxb(object obj)

{

return obj.ParentForm;

}

[MethodImpl(MethodImplOptions.NoInlining)]

internal static void UjereMQgCFvAAnebfxkR(object obj)

{

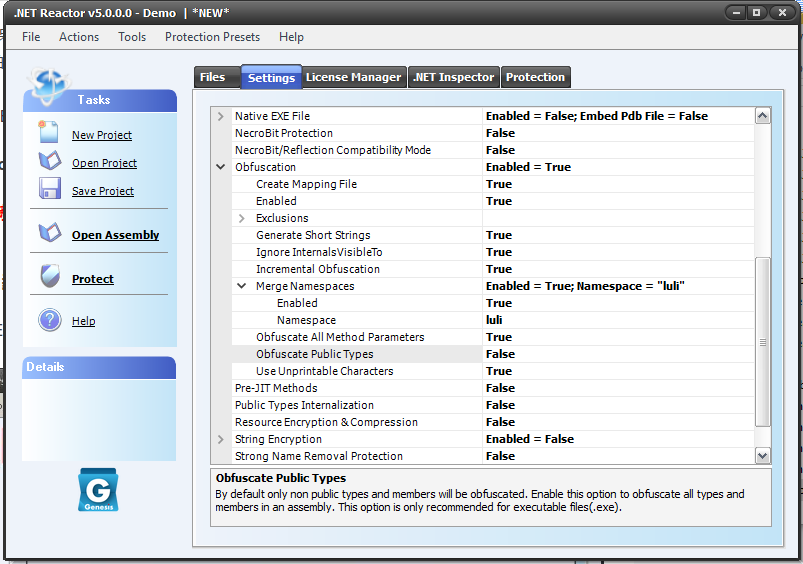
obj.Close();

}

## Compress & Encrypt Resources

壓縮和加密託管資源，運行時會自動解壓和解密資源。

# Obfuscation Setting 混淆程式碼設定



## Create Mapping File

允許創建混淆過字段與未混淆字段的映射文件(不建議開啟)

範例如下:

set\_Culture



get\_\_String



## Enabled

啟用混淆非public類別和成員的名稱

## Generate Short Strings

使用短字符串，可以减小程序集大小

## Ignore InternalVisibleTo

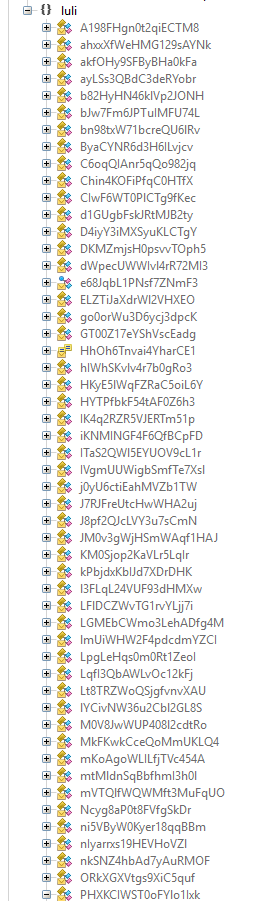
Enable this option to ignore the Internals Visible To assembly attribute.

## Merge NameSpace

會將所有混淆的type類型放置在一個name space中

this way you can prevent multiple obfuscates namespaces foe DLLS used in development environments like Visual Studio.

範例如下:



## Obfuscate Public Types

混淆所有類型和成員的名稱

若啟用此選項加密完的專案會無法執行，不建議勾選

## Incremental Obfuscation

有規律的規定混淆後的名稱

## Exclusions

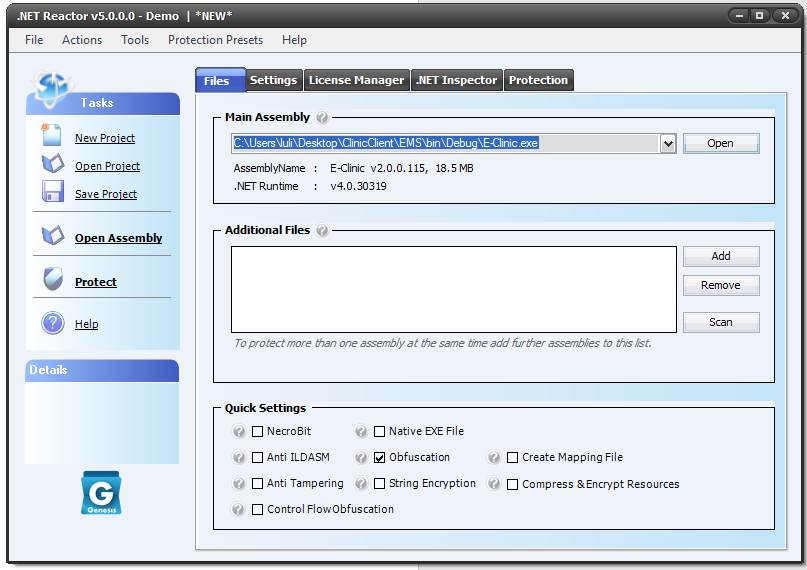
排除某個類型，不進行混淆

## Use Unprintable Characters

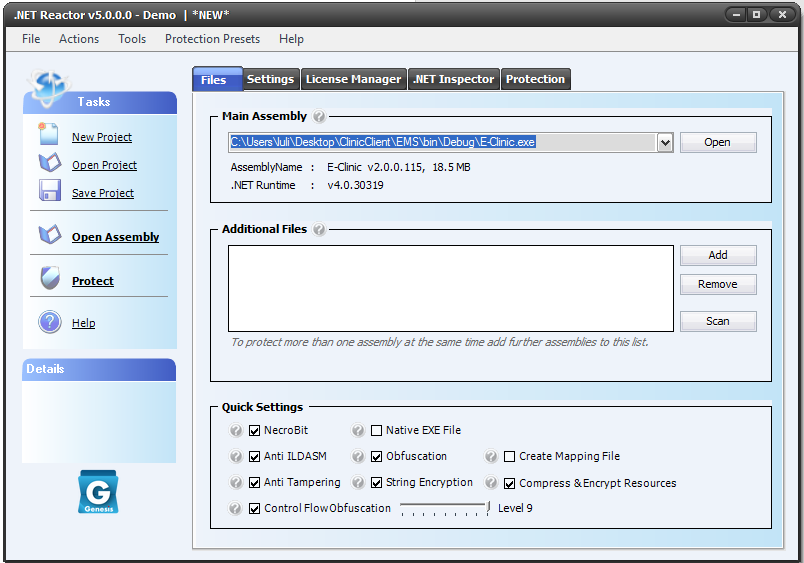
使用亂碼進行混淆

# Step

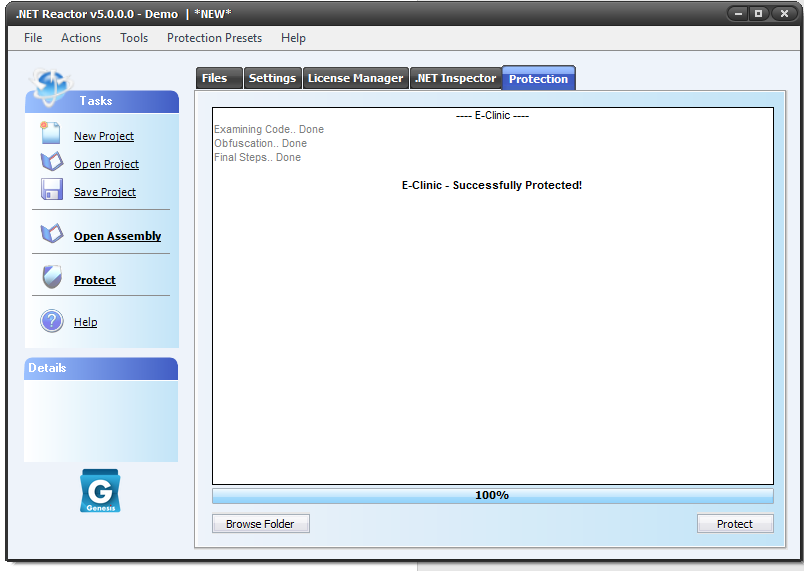
Step 1. Choose your file.



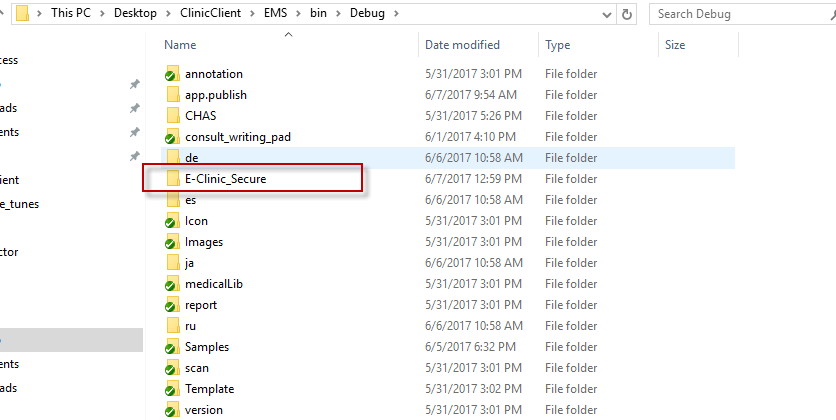
Step2. Setting



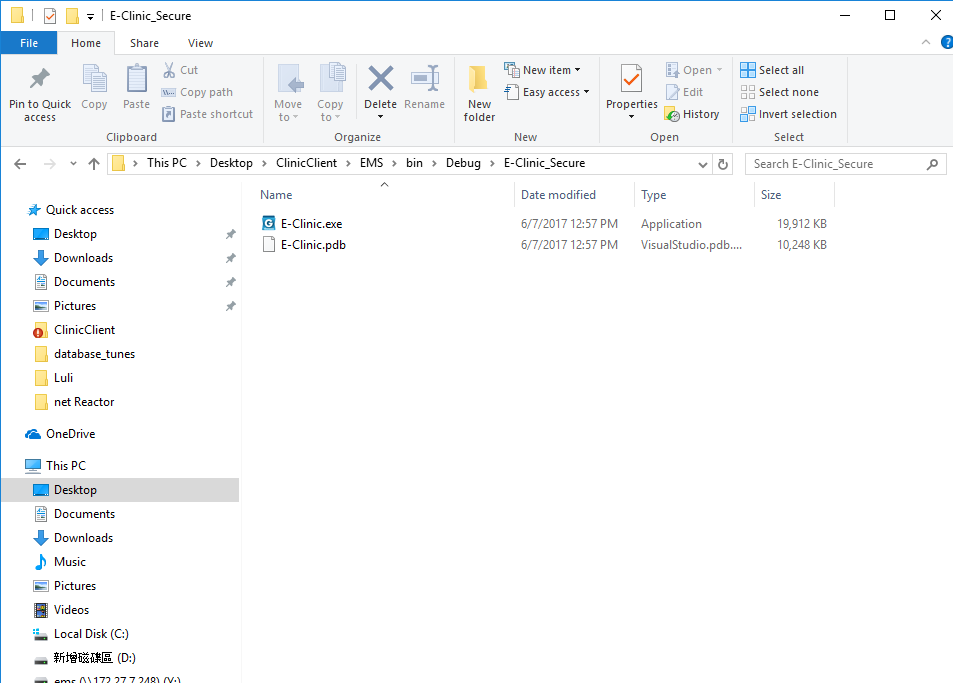
Step3. Click Prodect button to start protect



Step4.結束保護生成的檔案資料夾會建立在原來的目錄底下(EX:filename\_Secure)



Step5. 把檔案與其他必要檔案放置同一資料夾即可開啟



※執行前會通知該程式有受到保護

