

[Tuto005 - CrackME_@1 by QwErTy CLS (.NET)(.NET Reflector)(SERIAL)]



Crackme	CrackME_@1 by QwErTy CLS
Protección	Serial. (Hardcoded)
Herramientas	Windows 7 SP1 x64 Bits (WMWare Workstation 12 Pro) .NET Reflector v8.5.0.179 Detect It Easy v1.01
SOLUCIÓN	Hallar USER y SERIAL
AUTOR	LUISFECAB
RELEASE	Julio 27 2018
DESCARGA CRACKME	https://drive.google.com/drive/folders/1TKaBQLj4dazwvpJzAjX_Y96y45EjlfK-?usp=sharing

INTRODUCCIÓN

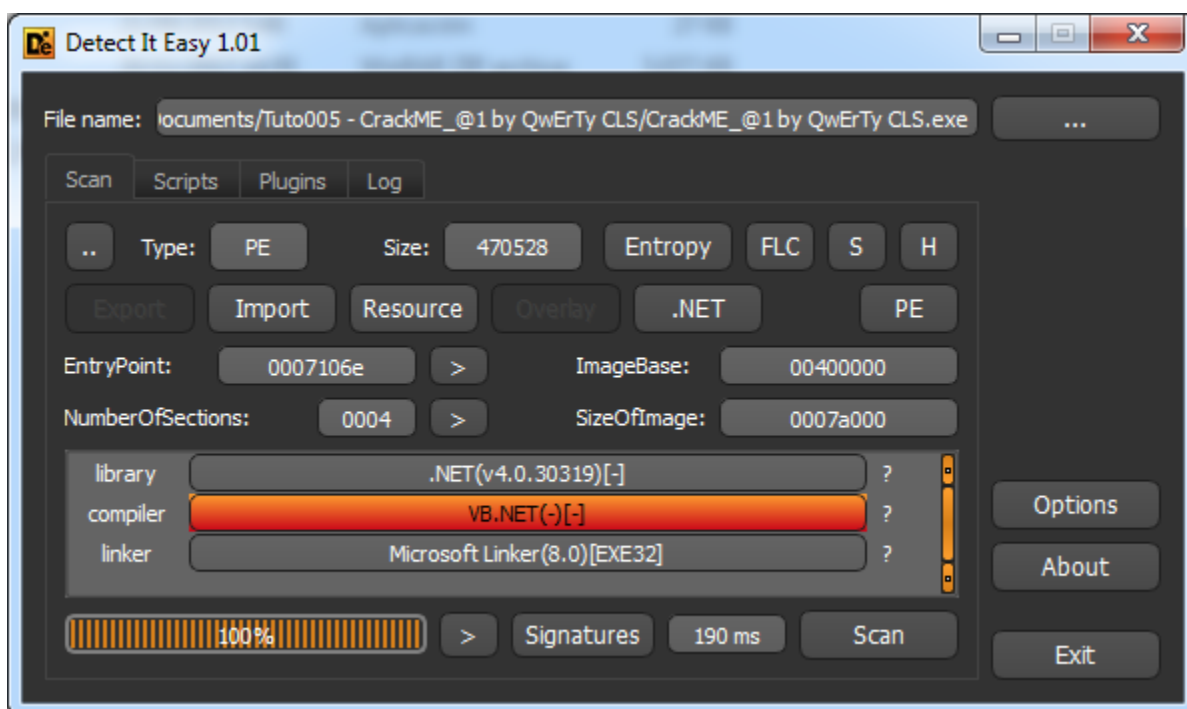
Escribiendo este tuto para compartirlo con la comunidad de CracksLatinoS y dedicarlo a **QwErTy** que nos compartió su crackme.

Sea esta la oportunidad para aproximarme al **.NET Reflector** y aprender a utilizarlo, ya sea por encimita porque según leí en su web es tremenda herramienta para trabajar con .NET. Mi aproximación con los .NET lo hice con el **dnSpy v3.0.2**, el cual me pareció muy buena herramienta; que sin tener ningún conocimiento previo con el **dnSpy** lo pude utilizar lo más de bien; creo que lo que más me ayudó fue saber programar algo de VB.NET porque sabía por dónde iba el código. El fruto de todo eso fueron dos tutoriales que el maestro **Ricardo** los subió a la web, que a propósito unas saludes especiales para él. Los tutoriales son [\[1643\]](#), [\[1644\]](#) que si desean pueden leerlos y si están buscando información de cómo utilizar el **dnSpy** les será de ayuda.

Listo, no más carreta. Espero compartir con todos ustedes lo poquito que voy aprendiendo y algún día todo lo escrito hoy sea de ayuda, como para mí ha sido todo lo compartido por todos ustedes.

ANALISIS INICAL

Empecemos averiguando en que está hecho y si está protegido. Para esto utilizamos la tool **Detect It Easy v1.01**.



[Tuto005 - CrackME_@1 by QwErTy CLS (.NET)(.NET Reflector)(SERIAL)]

Ya lo había dicho en la **INTRUCCIÓN** que era un .NET, pero mostramos esto porque debemos seguir el análisis ordenadamente. Junto al crackme viene nuestro archivo "Leeme.txt" y esto nos dice:

Encuentra el User y Password correctos, Si lo consigues, puedes mandarme la solución con un pequeño tutorial a

qwerty63.cls@gmail.com

Salu2

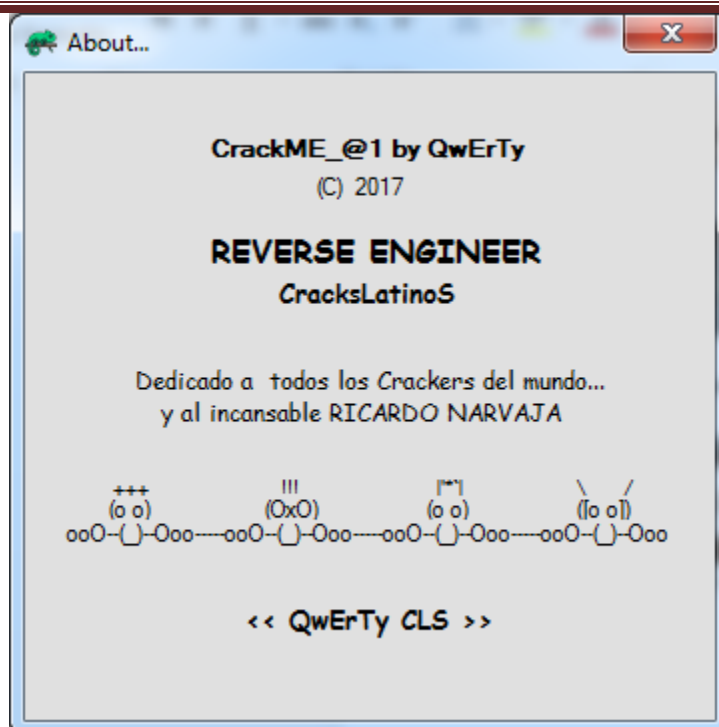
Nos pide hallar el serial, lo cual es lo más lógico y se entiende que estamos hablando de un serial **Hardcoded** porque si se pudiera registrar con diferentes **Pass** seguro que nos pediría hacer un KeyGen. Otra cosa que podemos notar es que pide también hallar el **User**, entonces no podremos colocar cualquiera.

Bueno, ejecutemos el crackme para ver qué nos sale y qué podemos observar.



Listo, ahí podemos ver el **User**, **Password** y el botón **Check** para registrarlo, pero antes miremos el "About..." para ver que nos muestra.

[Tuto005 - CrackME_@1 by QwErTy CLS (.NET)(.NET Reflector)(SERIAL)]



Buena dedicatoria y un saludo para ti querido **QwErTy** y totalmente de acuerdo contigo a **Ricardo** le debemos mucho por todo lo que ha hecho.

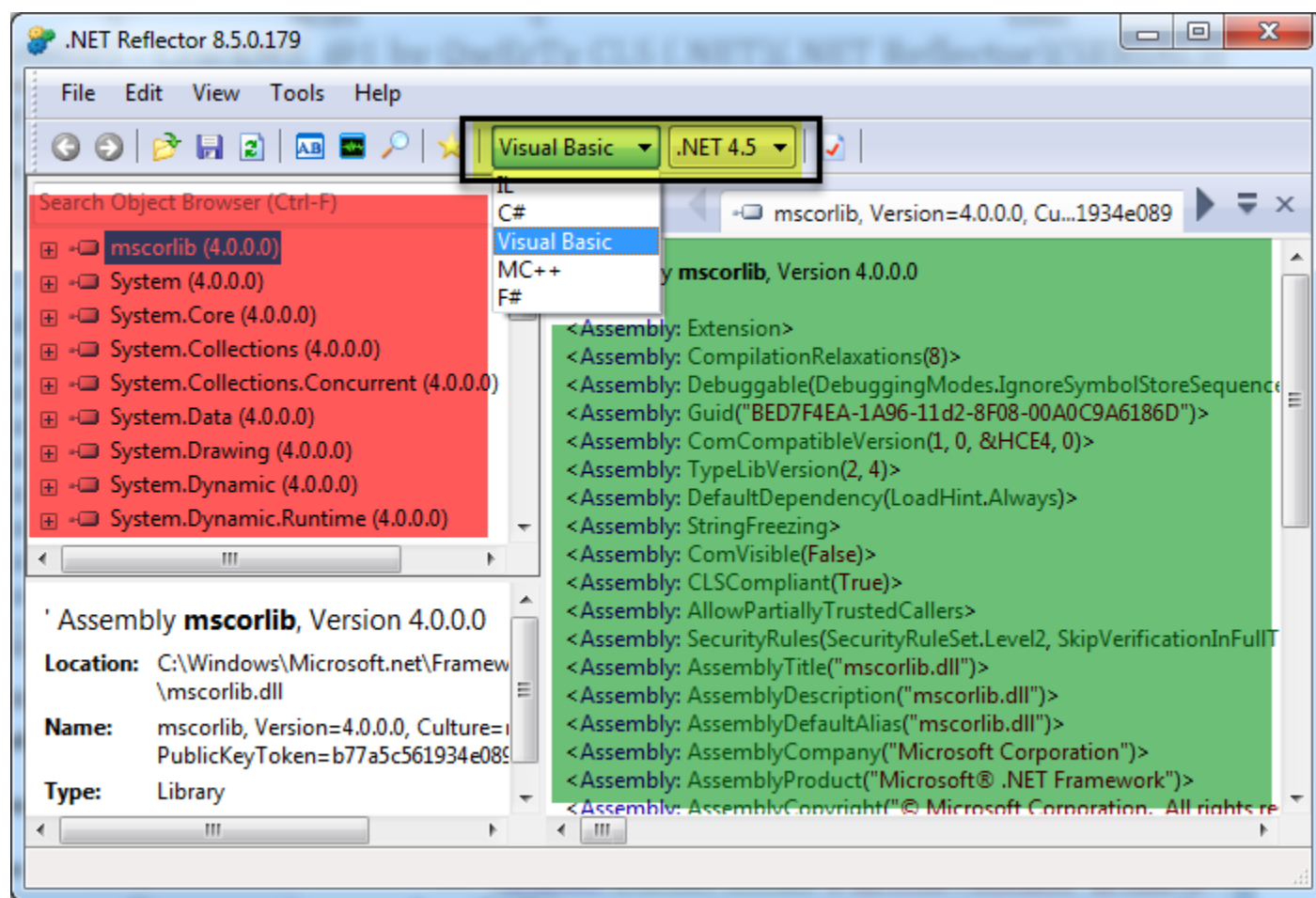
Metamos unos datos y veremos al <CHICO MALO> porque no creo que haya puesto los míos.



Hola <CHICO MALO>, ya veremos cómo volverte bueno. Listo, ahora al ataque con **.NET Reflector**.

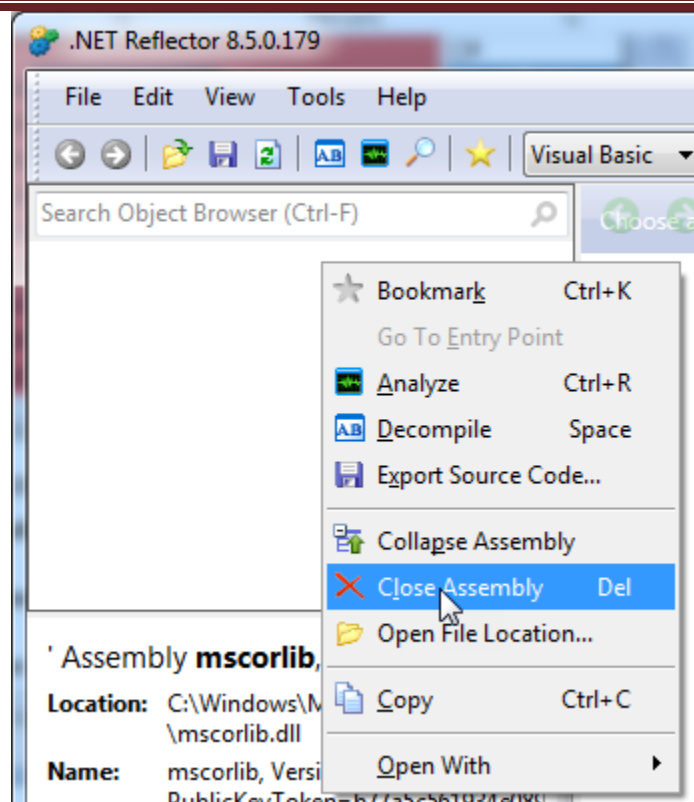
AL ATAQUE

Abrimos el **.NET Reflector**, pero antes comentarles que el **.NET Reflector** así instalado solito, solo permite ver todo el código descompilado, pero no puedes editar o cambiar código para crear nuestros **Cracks** o **Patches**; para poder hacer esto debemos instalar el **Plug-In Reflexil**, pero por fortuna con este Crackme solo debemos buscar nuestro **User** y **Pass** ocultos dentro del código, lo cual es perfecto para hacer nuestra primera aproximación con el **.NET Reflector**.



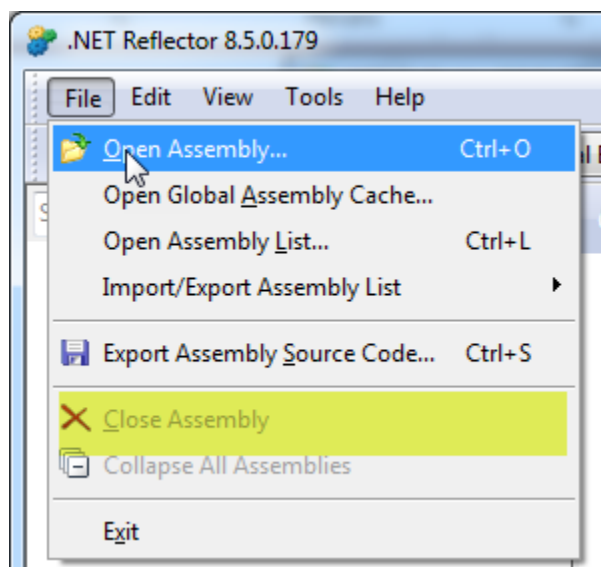
Listo, tiene las ventanas de trabajo muy similares por no decir iguales que el **dnSpy**. Resaltado en **ROJO** tenemos la ventana donde se carga el programa y todos sus componentes (ventana **OBJETOS**), se comporta como un explorador. En la parte **VERDE** se mostrará el código (ventana **DESAMBLADO**) de lo que seleccionamos en el explorador, ventana **OBJETOS** (Resaltado en **ROJO**) y arriba resaltado en **AMARILLO** escogemos el tipo de código que se mostrará en el **DESAMBLADO** (Resaltado en **VERDE**), yo lo dejaré en **Visual Basic** que es lo que entiendo un poquito.

[Tuto005 - CrackME_@1 by QwErTy CLS (.NET)(.NET Reflector)(SERIAL)]



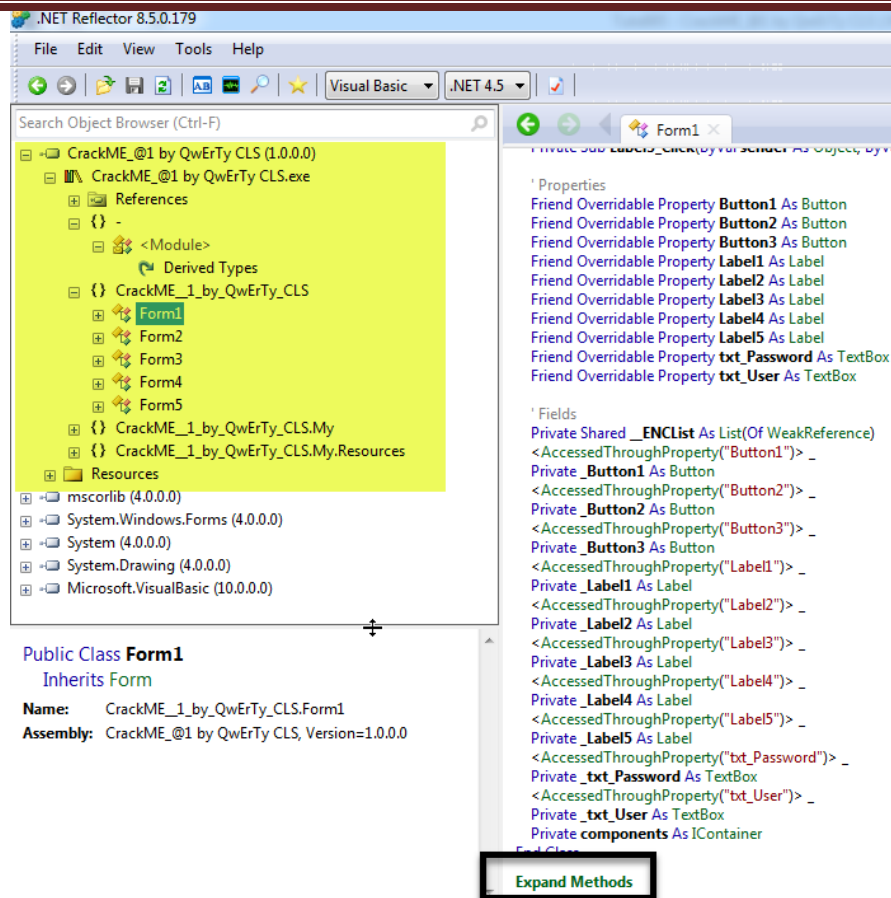
Como ven en la ventana de **OBJETOS** no hay nada ahora, a mí me gusta dejar esa parte limpia y que solo quede lo que estoy analizando, que en este caso será el crackme. Como ves en la imagen de arriba, seleccionas lo que quieres quitar <**Clic derecho- Close Assembly**> o con la tecla <**DEL**> que vendría siendo <**SUPR**> pero que raramente no me sirvió.

Carguemos nuestro crackme en el **.NET Reflector** <**File->Open Assembly...**>, también puedes ver resaltado en **AMARILLO** la opción para quitar los objetos que no queramos tener en esa ventana.

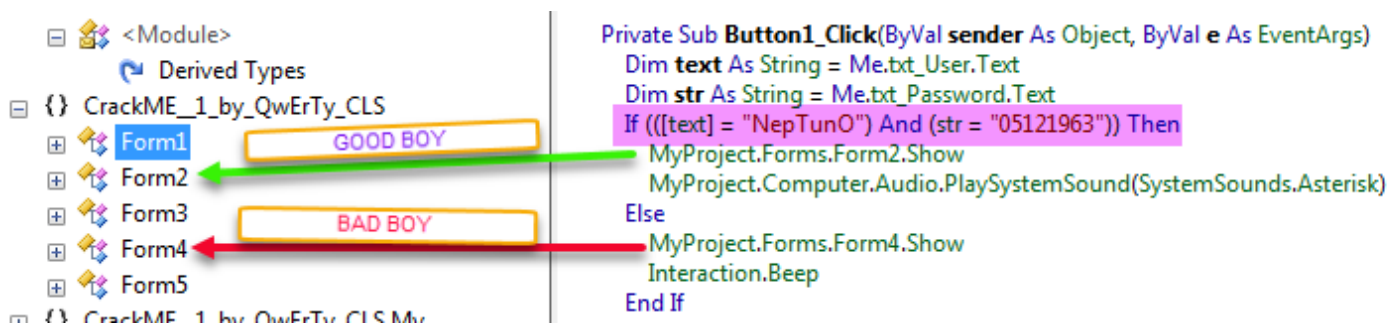


Ahí está cargado en nuestra ventana **OBJETOS**. Ahora ya solo nos queda ir desplegando todos los objetos que tiene el crackme.

[Tuto005 - CrackME_@1 by QwErTy CLS (.NET)(.NET Reflector)(SERIAL)]



Solo nos queda es ir mirando lo que nos muestra **.NET Reflector** y si es la primera vez que estás analizando un .NET debes desmenuzar la ventana **OBJETOS** para que vayas reconociendo las zonas de interés. Por ejemplo, podemos ver que estoy parado en el **Form1** y ahí pienso revisar primero; para hacer eso desplegamos todos los métodos en **EXPAND METHODS** y ahí veremos todos los procedimientos y si le pegamos al lugar indicado puede que encontremos ahí nuestro **User** y **Pass**.



Perfecto, ahí están. Podemos ver la declaración de las variables, variable **text** que contiene nuestro **User** y la variable **str** contiene nuestro **Pass**. Vemos que la compara con **User=NepTunO** y **Pass=05121963**. Así que solo nos queda meter esos datos y seguro todo funcionará.

[Tuto005 - CrackME_@1 by QwErTy CLS (.NET)(.NET Reflector)(SERIAL)]



Perfecto, esos eran los datos correctos. Utilizando el **.NET Reflector** los pudimos encontrar. Solo deben darle a botón "Entry" para ver a **RANGO**. Eso se los dejo a ustedes.

PARA TERMINAR

Agradecer a **QwErTy** por compartir su crackme.

No sé, pero creo que con estas herramientas como el **.NET Reflector** es más sencillo analizar los .NET, claro mientras los tengamos así sin ofuscaciones, bien limpiecitos y buenitos, lo cual fue una buena forma de empezar con el **.NET Reflector**.

No recuerdo dónde lo leí, pero alguien comentaba que este **.NET Reflector** mostraba la información mejor que el **dnSpy**, que se deja confundir cuando analiza en parte el código para mostrar en el **DESAMBLADO** (para mí no es relevante para el cracking). Yo creo que este **.NET Reflector** les sirve más a aquellos que ya tienen las cosas más claras con el lenguaje .NET porque si no me equivoco no te permite debugear como el **dnSpy**; cuando tú quieres ver cómo te quedan los cambios que hagas con el **.NET Reflector** primero los debes guardar en un ejecutable y luego probarlos, cosa que con el **dnSpy** lo puedes hacer dentro del mismo programa.

Listo, termino este tuto más contento, no tuve mayores problemas al escribirlo y por fortuna no se perdió nada. Saludos para toda la comunidad.