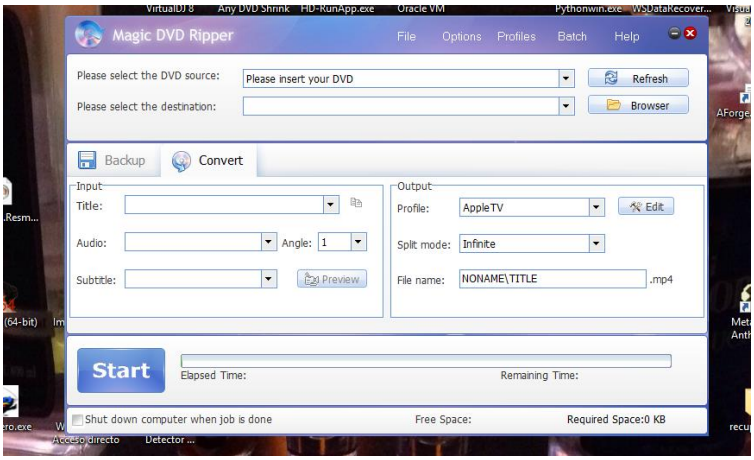
Crackeando Magic DVD Ripper.

Nombre	Magic DVD Ripper
Protección	No tiene.
Objetivo	Registrar con Keygen/ crear archivo que nos registre
Web	http://www.magicdvdripper.com/
Dificultad	Muy fácil
SO	Windows 10
Herramientas	1.- X64DBG 2.- Visual Studio 3.- RDG packer detector
Lenguaje	Borland C++
Cracker	Ismael Tun
Fecha	22 de noviembre del 2018
Tutorial N° 5	

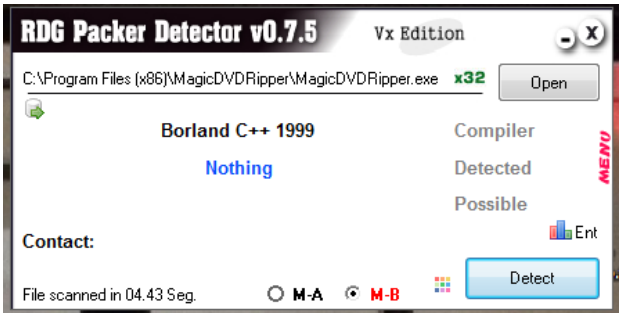
Bueno pues, ha pasado un tiempo desde mi último tutorial, y prometo no será el último, y la verdad es que el trabajo no ayuda mucho, pero aquí estoy de nuevo haciendo lo que más me gusta y sobre todo el poder compartirlo en este grupo que es como una familia muy grande; pues como dije y no voy a dejar de decir que en nuestro país no se le da tanta importancia a este tipo de conocimientos y en mi lugar de origen menos, y da un poco de lastima el desaprovechar toda la información que tenemos a nuestro alcance.

Quiero dejar claro que este tutorial y el programa usado es solamente como ejemplo, tiene un costo y al que le guste y lo necesite pues que lo pague, y no me hago responsable por el uso que se le dé a estos conocimientos.

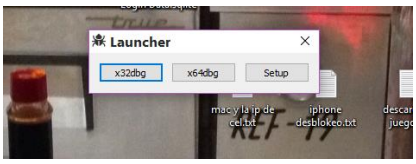
Sin más que mencionar vamos al meollo del asunto, abajo como pueden ver es la ventana del programa en modo trial.



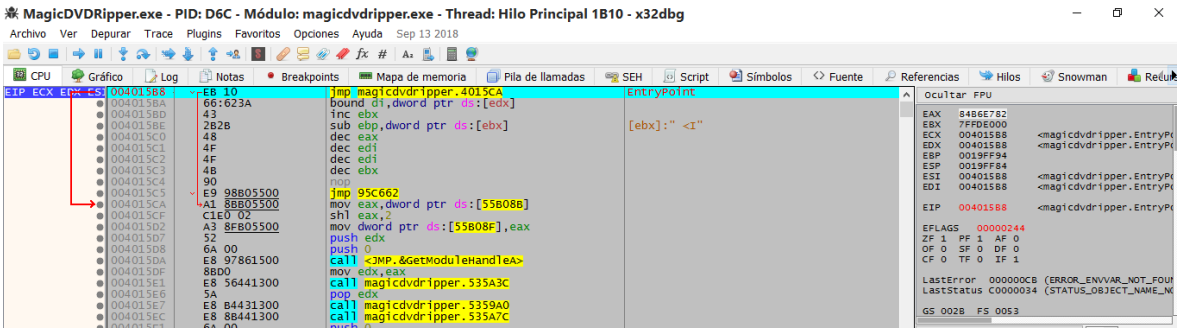
Para no perder la costumbre le pasamos el detector de protecciones, y como podemos ver, en modo M-A y en modo M-B nos muestra lo mismo.



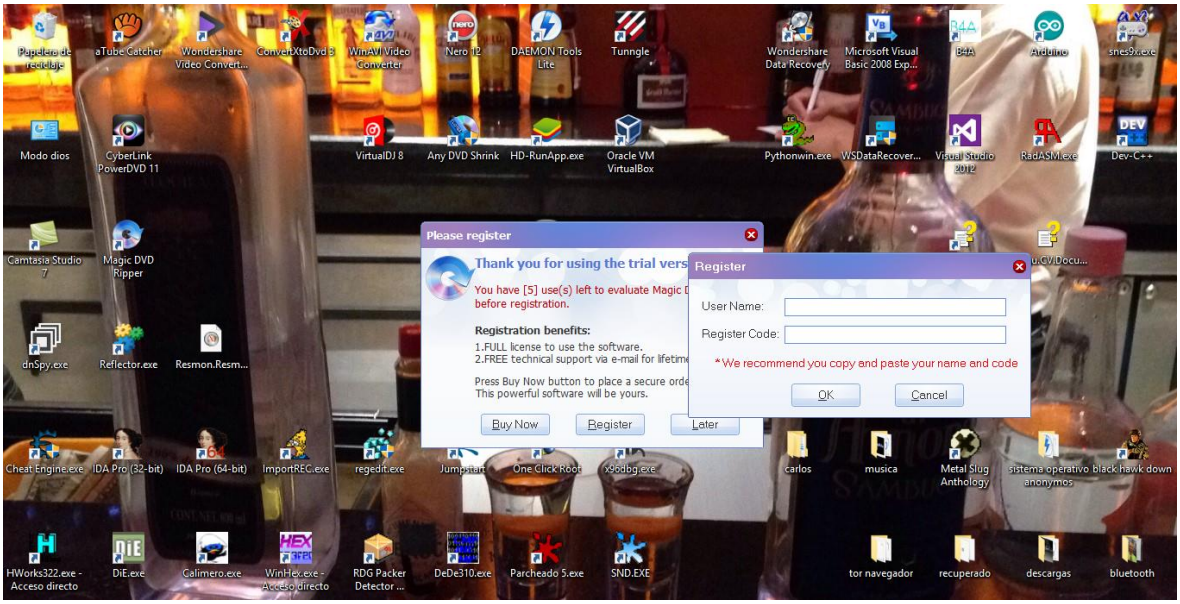
En este tutorial voy a usar el X64dbg pero para 32 bits, trae muchas funciones muy útiles y la verdad me adapte muy bien con este depurador.



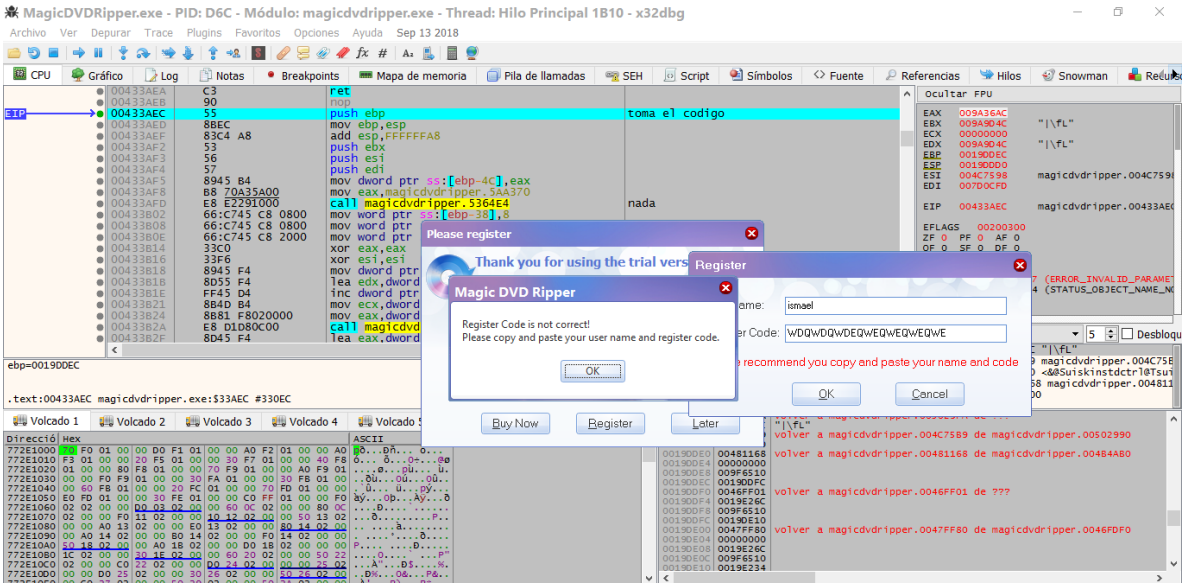
Ahí tenemos el programa detenido en su entry point. Presionamos la tecla ejecutar para iniciar la aplicación, ahí lo marco en la imagen, para los que aun estén despistados.



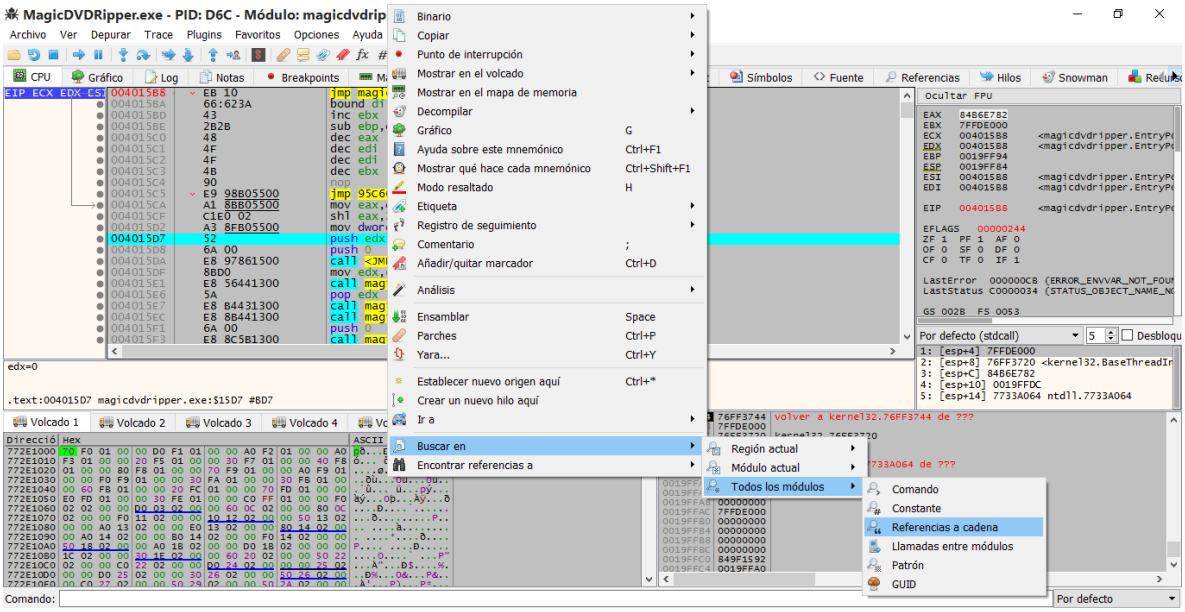
Ya una ves iniciada la aplicación le damos click al botón register y le metemos nuestro nombre y serial, obviamente falsos, para que nos presente al chico malo y asi comenzar a planear nuestro ataque, le damos al boton OK.



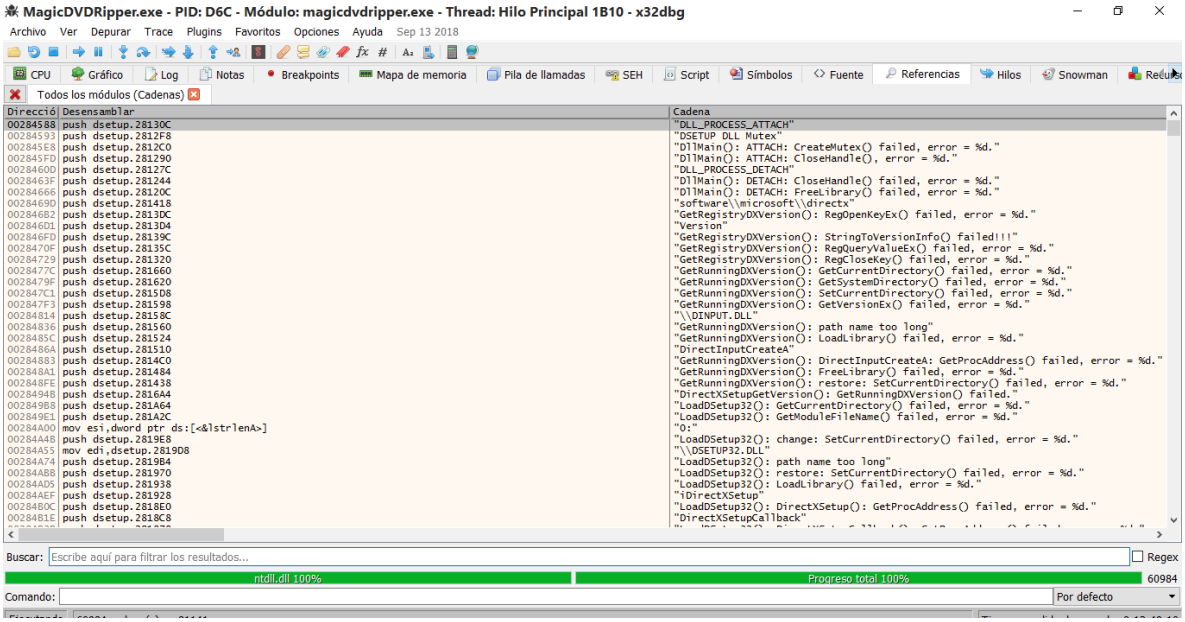
Una ves identificado nuestro chico malo, vamos a usar la técnica de buscar refrencias a cadena.



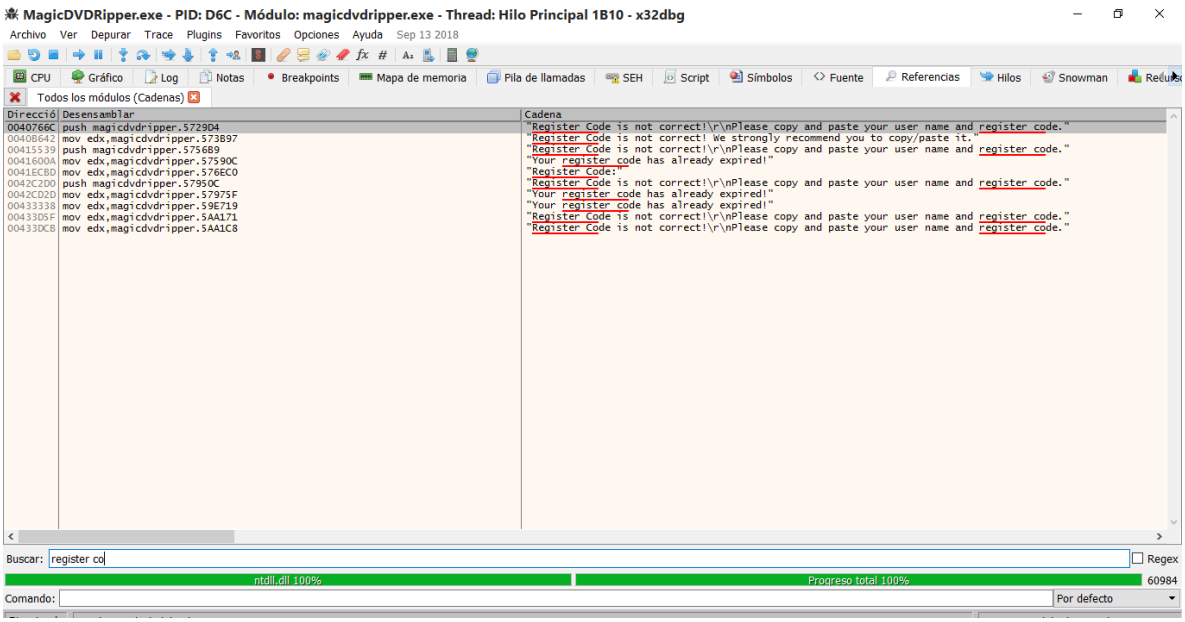
Ahí podemos ver como buscar cadenas.



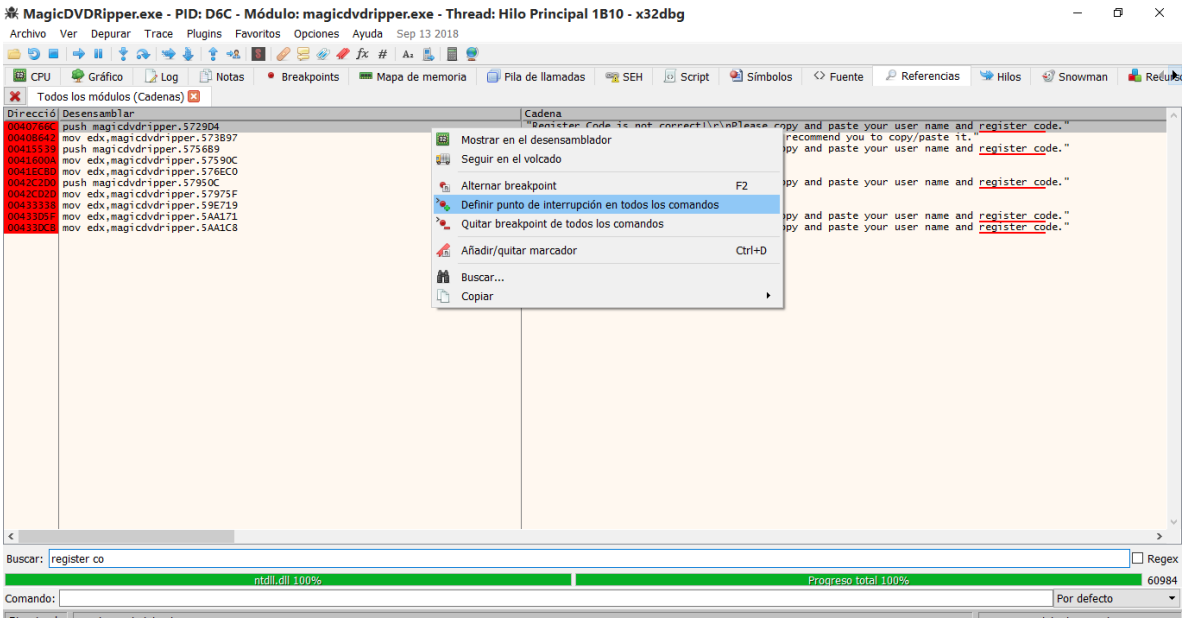
Dejamos termine de escanear todas las cadenas de texto.



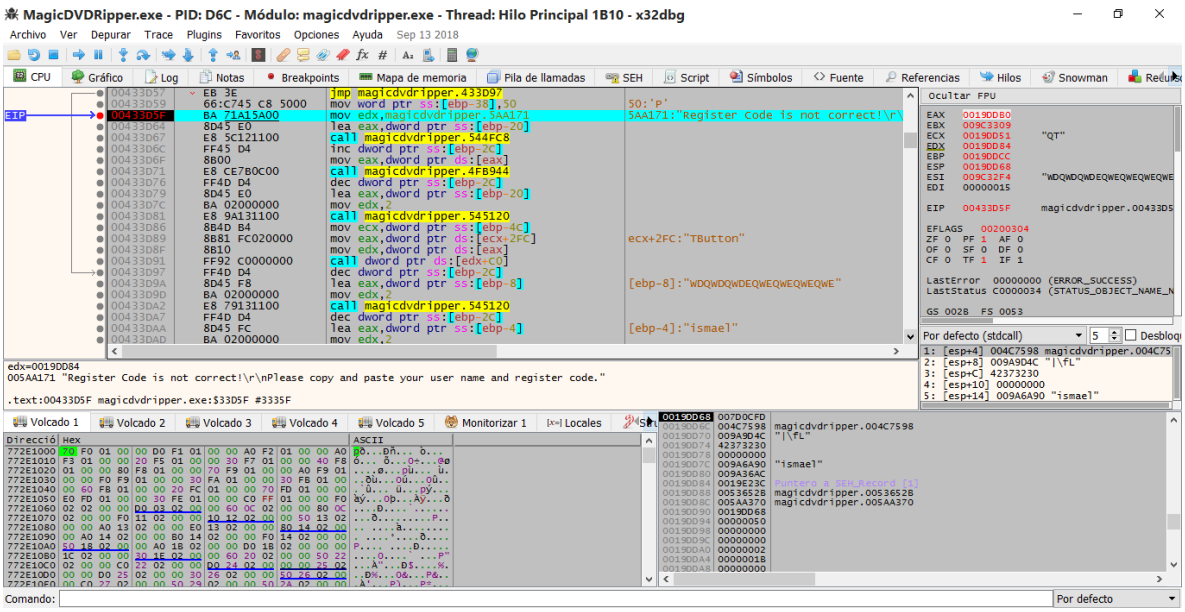
Ahí donde dice buscar escribimos: register code (es parte del chico malo), con eso es suficiente.



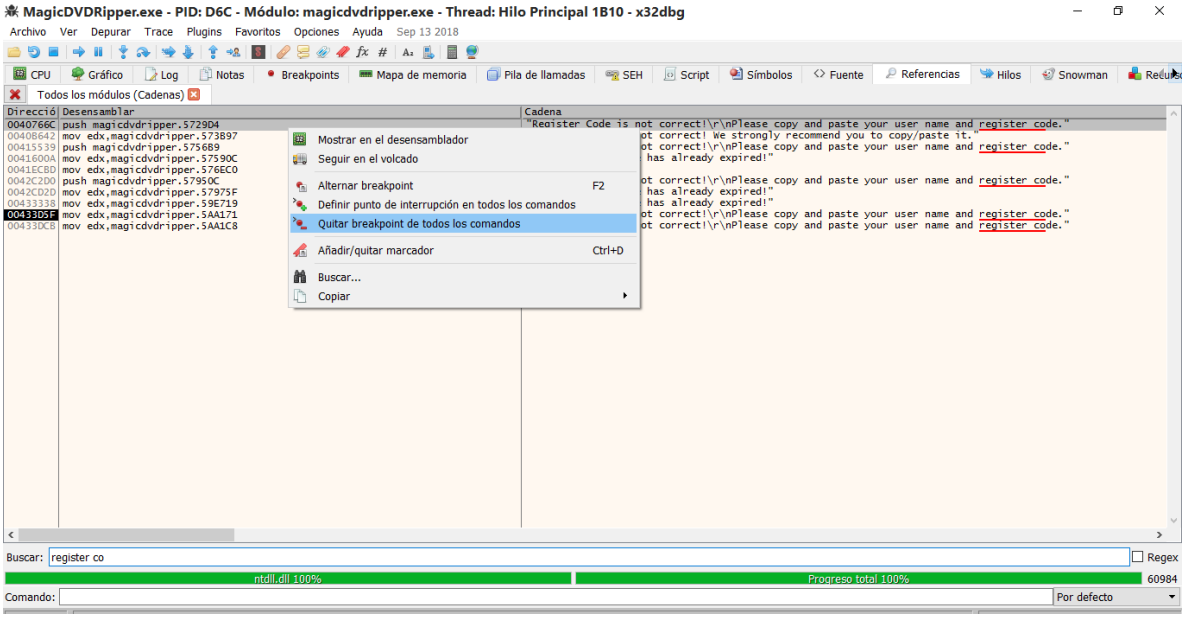
Cuando aparezcan las referencias le ponemos break point a todas, luego click en botón OK de nuevo.



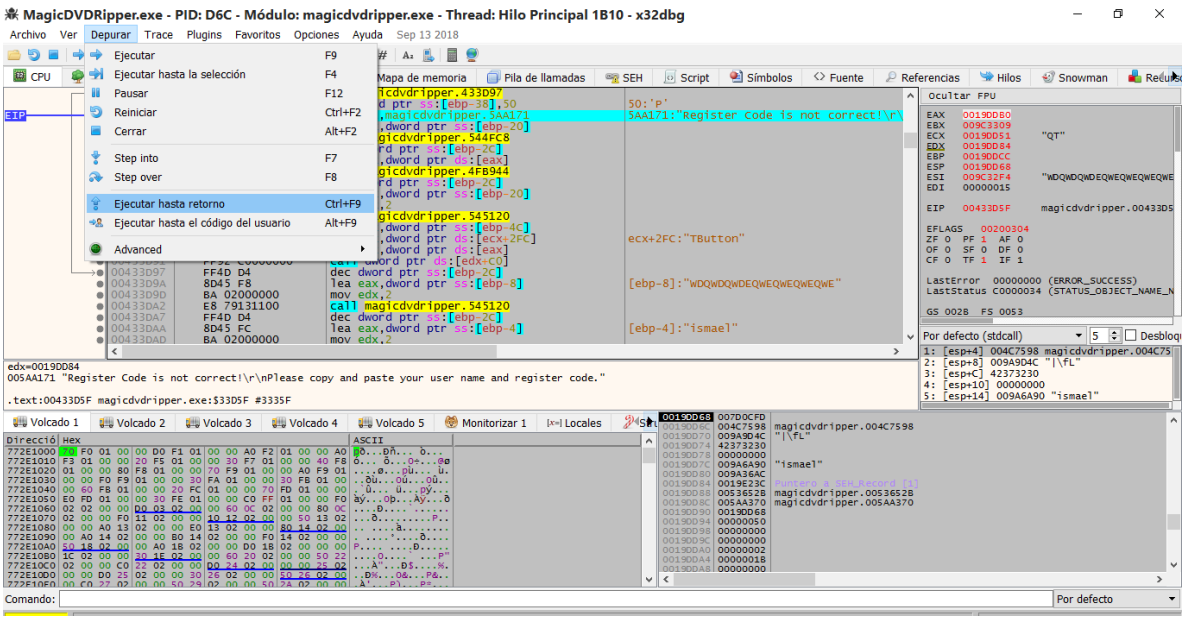
Y para ahí.



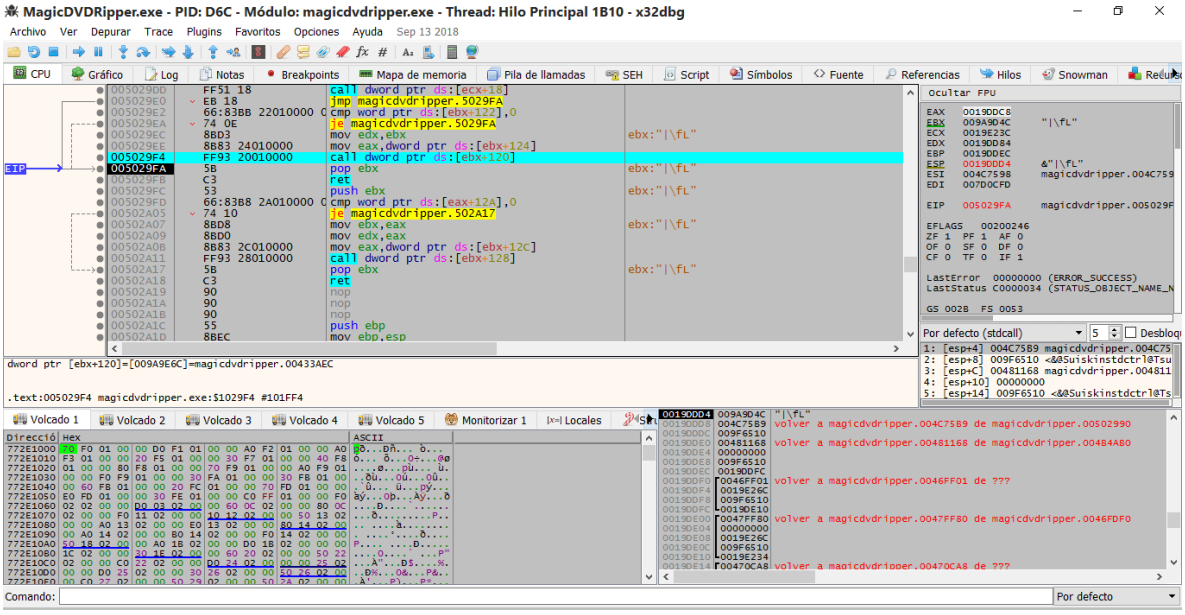
Quitamos de nuevo los break points.



Le damos a ejecutar hasta retorno, esto con el fin de llegar al final del call y de nuevo entrar en ella para saber donde inicia y de nuevo poner break point, pero esta ves al inicio de la rutina para calcular el serial.



Como podemos ver, este es call responsable de calcular nuestro serial.



El código de abajo es el inicio del call, poner break point en ella para que ahí pare la próxima ves que corramos el programa.

```
00433AEC 55 push ebp toma el codigo
```

Y termina en

```
00433E1E C3 ret
```

Ya adentro del call pasamos instrucción a instrucción y podemos reconocer la siguiente estructura que es una comprobación a una lista de 473h de nombres “fichados”, o sea que esos nombres, a pesar de tener código correcto, están bloqueados, y ese jmp nos lleva a chico malo.

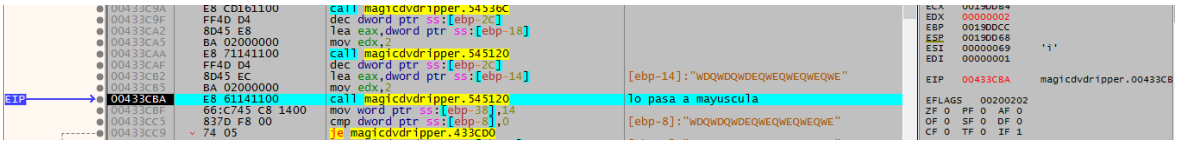
```
00433BFF E9 14020000   jmp magicdvdripper.433E18
00433C04 43            inc ebx                    ebx:"|\fL"
00433C05 81FB 73040000 cmp ebx,473                ebx:"|\fL"
00433C0B 0F8C 5EFFFFFF jl magicdvdripper.433B6F
```

Un poco mas abajo podemos ver la siguiente estructura, que es la encargada de calcular un código, básicamente suma el valor hexadecimal de cada carácter del nombre.

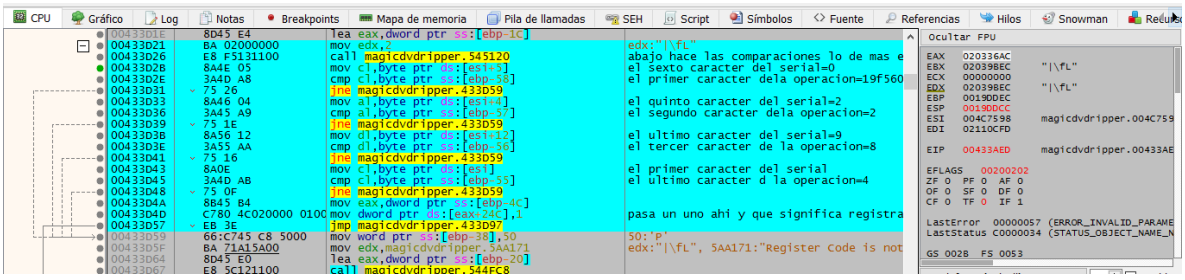
```
00433C22  8A03        mov al,byte ptr ds:[ebx]      ebx:"|\fL"
00433C24  03F0        add esi,eax
00433C26  47          inc edi
00433C27  43          inc ebx                       ebx:"|\fL"
00433C28  8B55 B0     mov edx,dword ptr ss:[ebp-50]
00433C2B  52          push edx
00433C2C  E8 6B241000 call magicdvdripper.53609C    longitud en eax ; edx=80800000
00433C31  59          pop ecx
00433C32  3BF8        cmp edi,eax
00433C34  72 EA       jb magicdvdripper.433C20
```

Y el call en 00433c2c le agrega ceros para completar cuatro bytes, eso en caso de que el usuario sea de un carácter, ya que en nuestro serial necesitaremos al menos 4 digitos.

El call siguiente solamente pasa a mayúsculas nuestro serial.



Llegando a esta estructura que esta hasta abajo, podemos notar que hace uso de unos datos, que no es nada mas y nada menos que comparar ciertos caracteres de nuestro serial con los caracteres de la suma de nuestro nombre, previamente convertidos a ascii.



Y para hacer nuestro keygen necesitamos saber lo siguiente:

1.- El sexto carácter del serial el igual al primer carácter de la suma

2.- El quinto carácter del serial debe ser igual al segundo carácter de la suma del nombre.

3.- El carácter 19 del serial debe ser igual al tercer carácter de la suma.

4.- El primer carácter del serial debe ser igual al último carácter de la suma.

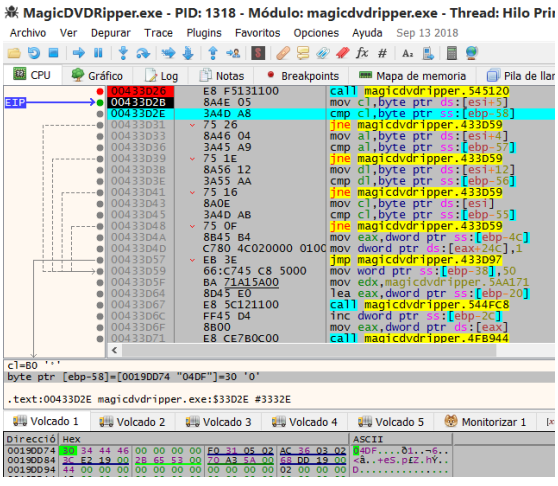
O sea que si mi nombre de usuario es: Carlos Ismael y sus valores hexadecimales son:

C—a---r-- -l---o—s-- --l----s---m—a—e--l

43-61-72-6c-6f-73-20-49-73-6d-61-65-6c

Vamos a usar la calculadora de Windows en modo programador configurado a valores hexadecimales y ahí vemos el resultado de dicha operación.

Y como vemos el volcado es el mismo valor



En caso de que la suma solo tenga 3 caracteres le agrega un cero, si tiene solo 2 caracteres le agrega 2 ceros, si tiene 4 no le agrega nada; (eso hace el call 00433C2C)

Ahora vamos a crear una pseudo clave, a ver si funciona, solo siguiendo la regla que el programa dicta. Usamos las primeras letras del abecedario.

abcdefghijklmnopqurs ← Vamos a usar esta. Y recordemos que la suma es: 4DF en hexadecimal, le agregamo un cero al principio lo que lo convierte en “04DF”

1.- El sexto carácter del serial es el primero de la suma “0” lo sustituimos donde corresponde.

Abcde0ghijklmnopqurs ← y tenemos esto

2.- El quinto carácter del serial debe ser igual al primer carácter de la suma del nombre.

Abcd40ghijklmnopqurs ← y tenemos esto

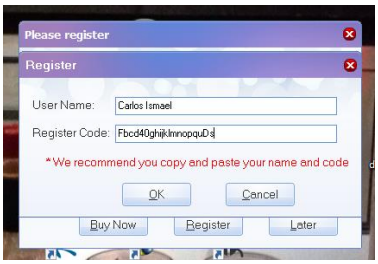
3.- El carácter 19 del serial debe ser igual al segundo carácter de la suma.

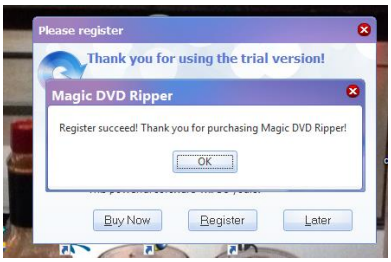
Abcd40ghijklmnopquDs ← y tenemos esto

4.- El primer carácter del serial debe ser igual al último carácter de la suma.

FbcdEOghijklmnopquDs ← y tenemos esto

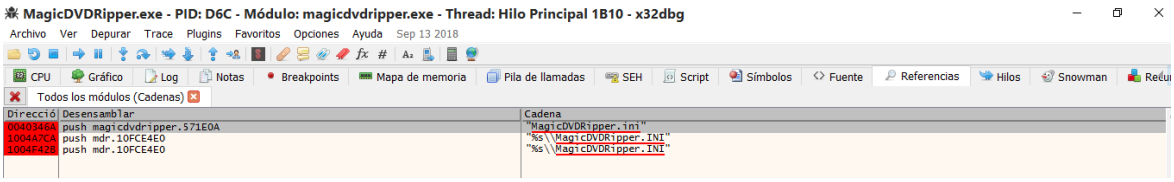
Probamos y…..



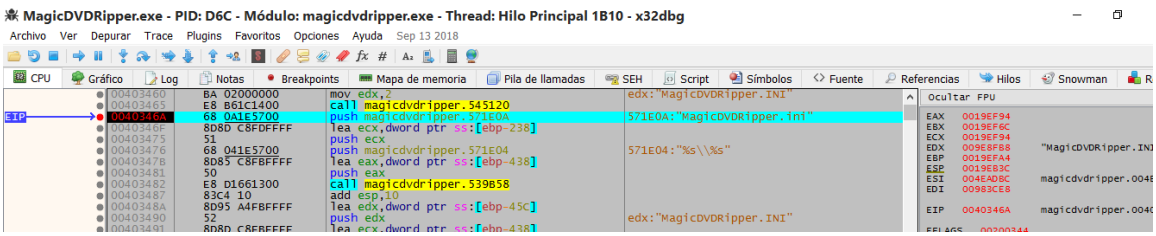


Como pueden ver si funcionó.

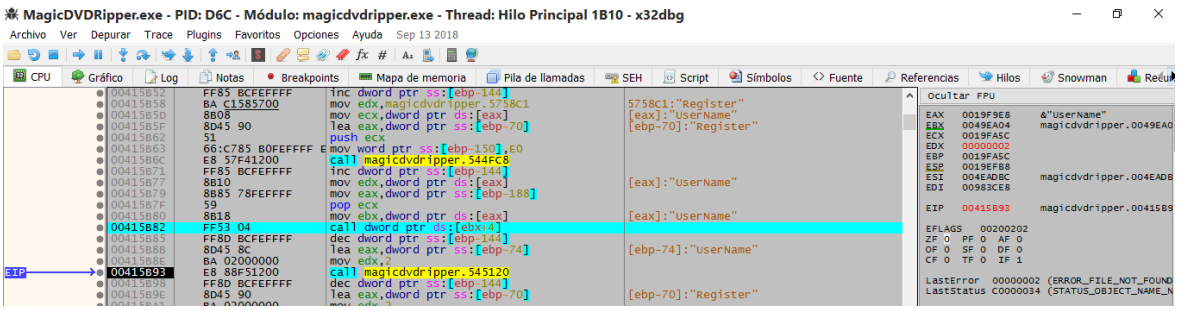
Para ver el archivo de licencia y donde se escribe seguimos los pasos a continuación.



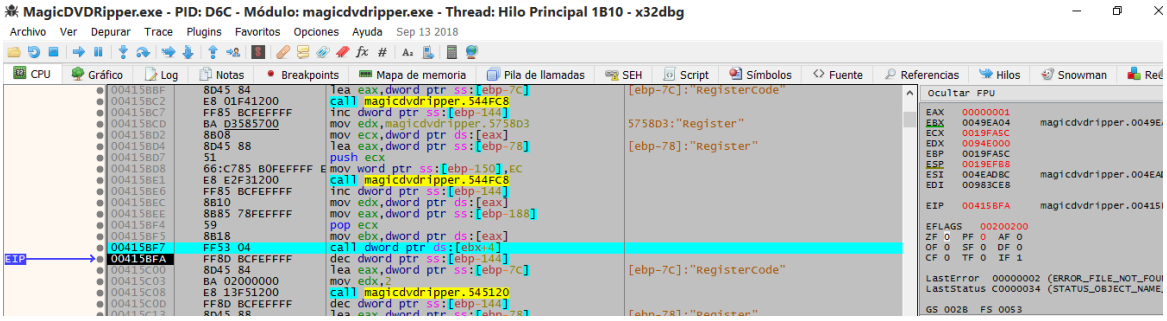
Caemos aquí



Este es el call que escribe el nombre en el archivo



Este escribe el serial en el archivo

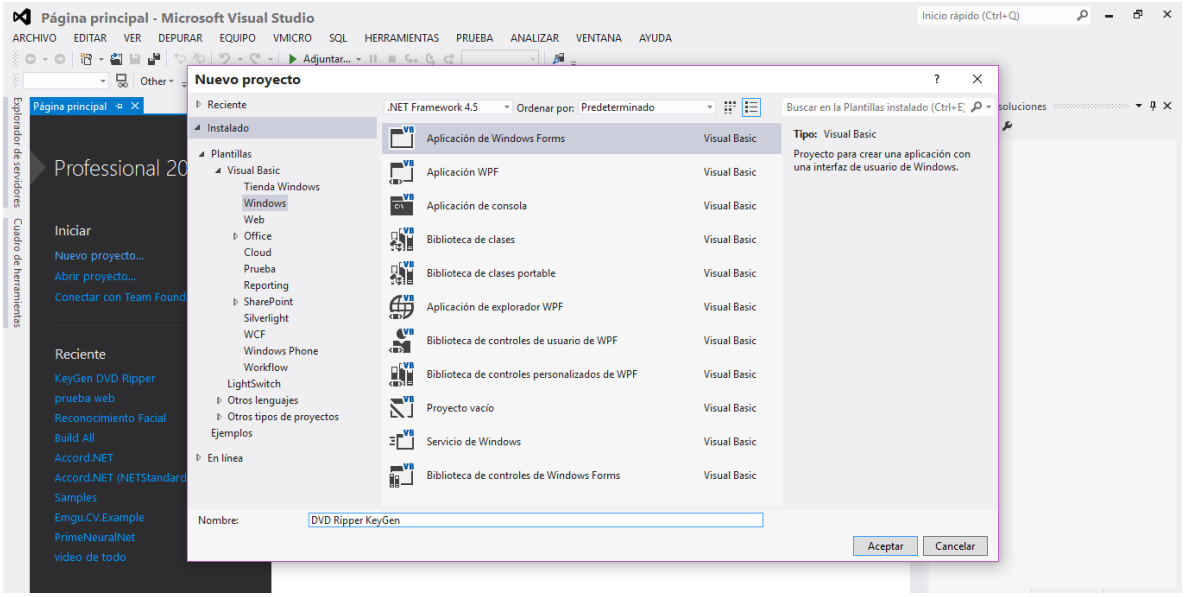


Y esta es la dirección obtenida.

C:\Users\ismael\AppData\Local\MagicSoftware\MagicDVDRipper

Hasta aquí el análisis del programa; ahora a crear el keygen.

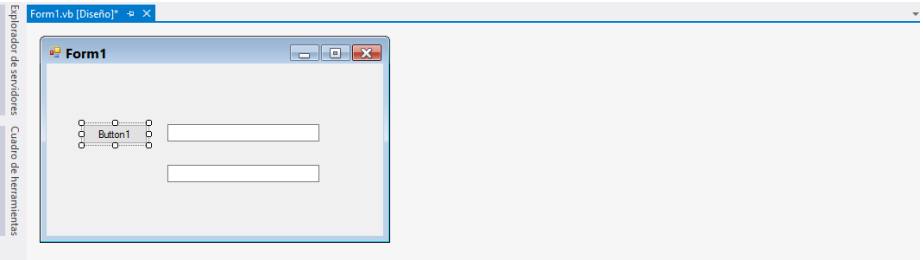
Iniciamos visual studio.



Click en nuevo proyecto > aplicación de Windows Form > le damos nombre al proyecto y le damos aceptar.

Agregamos al proyecto un botón, dos etxtbox y dos labels, con eso es suficiente para hacer el keygen. Dejo claro de una ves que no voy a entrar en detalle con la creación y diseño, solo pondré código y su explicación con el resultado final, además añadiré el exe ya compilado.

El diseño inicial será algo parecido al siguiente:



Todo será hecho con el botón y ahí es donde pondremos todo el código asi que le damos doble click para escribit código en el:

```
'este boton Registra con KeyGen
```

1.- paso 1: genera 19 caracteres aleatorios entre números y letras.

```
        If txtNombre.TextLength = 0 Then 'este if comprueba que al menos tenga un caracter.
            txtSerial.Text = "El serial debe tener al menos un caracter."
            Exit Sub
        End If

        Dim aleatorio As New Random         ‘creamos una variable random
        Dim num As Integer                  'numero generado
        Dim serial, letras As String        'serial y sus letras

        For i = 0 To 18 Step 1              'generamos uno de 19 caracteres
            num = aleatorio.Next(1, 3)      'numeros random sin incluir el 3 decide si letras
o números, esto con la idea de mezclar números y letras en nuestro seral.
            If num = 1 Then                         'si el numero generado es uno.
                num = aleatorio.Next(48, 58)      'genera numeros
            Else
                num = aleatorio.Next(65, 91)      'genera letras
            End If
            letras = Chr(num)
            serial = serial + letras
        Next                                'regresa a generar otro caracter
```

2.- paso 2: suma los valores hexadecimales de cada carácter de nuestro serial y lo convertimos a ascii.

```
        Dim nombre As String = txtNombre.Text
        Dim asci, suma As Integer           'variables para las letras y su suma
        For Each c As Char In nombre        'suma cada letra del nombre
            asci = Asc(c)
            suma = suma + asci
        Next
        Dim sumastr As String               'valor de la suma en hexadecimal
        sumastr = Hex(suma).ToString        'lo convertimos a ascii.
```

3.- paso 3: agregamos los ceros que hagan falta.

```
      If sumastr.Length < 3 Then        'este if es en caso de que un usuario terco quiera
registrar con un caracter,
            sumastr = "00" & sumastr
```

```
        End If
        If sumastr.Length < 4 Then
            sumastr = "0" & sumastr     'de hecho el programa, en sus entrañas, tiene esta
misma solucion .
        End If
```

4.- paso 4: colocamos los valores de la suma en el lugar que le corresponde según el algoritmo de la aplicación.

```
        Dim j As Integer
        For Each c As Char In sumastr   'lo coloca en las posiciones adecauadas
            Select Case j
                Case 0
                    serial = serial.Insert(3, c) '6° lugar
                Case 1
                    serial = serial.Insert(3, c) '5° lugar
                Case 2
                    serial = serial.Insert(17, c) '18° lugar
                Case 3
                    serial = serial.Insert(0, c) 'primera posición.
                Case Else
                    txtSerial.Text = "ERROR"
            End Select
            j = j + 1
        Next

        txtSerial.Text = serial
```

4.- paso 4: comprobamos que funcione:

Comprobramos generando caracteres para mi nombre:

Carlos Ismael

Claves generadas:

FMZ940719ZW6X6WBPRD36L9

F33M406805R2UG46JVD3D75

F7V140B2277PV0MM65D8B30 -----todas son válidas.

1.- Crear archivo de registro en cierta ubicación.

```
        If File.Exists(pathDVDRipper) Then
            MsgBox("Archivo encontrado, comieza proceso de registro")
        Else
            MsgBox("Archivo no existe aun, tienes que iniciar la aplicacion al menos una
ves")
            'inicia() 'inicia la aplicacion
            Exit Sub
        End If
        'estos son los datos del archivo de licencia
        My.Computer.FileSystem.WriteAllText(pathDVDRipper, "[Register]()" & vbCrLf, True)
        My.Computer.FileSystem.WriteAllText(pathDVDRipper, "UserName = Carlos Ismael" &
vbCrLf, True)
```

```
        My.Computer.FileSystem.WriteAllText(pathDVDRipper,
"RegisterCode=F6T140S0YLK851D376D4245" & vbCrLf, True)
      inicia() 'inicia la aplicación ya registrada
```

Con eso es suficiente para registrar pero a mi nombre y con cierto código.

Y si queremos estar de No registrados el siguiente código lo hace, el cual solo elimina el archivo anterior.

```
If File.Exists(pathDVDRipper) Then
      File.Delete(pathDVDRipper)
End If
```

Cabe mencionar que hay que crear ciertas variables globales las cuales son:

```
Public pathOriginal As String = My.Computer.FileSystem.SpecialDirectories.Temp
    Dim pathDVDRipper As String = pathOriginal.Remove(pathOriginal.LastIndexOf("\")) &
"\MagicSoftware\MagicDVDRipper\MagicDVDRipper.ini"
```

Ya con eso doy por terminado esta parte de programación.

TERMINANDO

Bueno no ha sido un programa muy complicado, solo unas horas de análisis y unos minutos para hacer un Keygen funcional y me tomo unos días redactar la presente, pero como siempre contento de haber terminado y que mas gusto da que tu mi amigo lector llegues hasta estas líneas; como pueden ver puse imágenes de los lugares exactos solo que tener en cuenta que las direcciones de memoria varian de maquina en maquina. Un saludo a todo cracklatinos en especial a Ricardo Narvaja, Ivinson, Nox, entre otros.

Les recuerdo que el X64dbg es nuevo pero es muy parecido al olly solo que con este ya podremos trabajar en Windows 10 incluso podemos trabajar con programas de 64 bits. Trae funciones similares y algo más.

Adjunto: este tutorial y el Keygen, ya que el exe lo pueden descargar de la página oficial del programa.

Contacto:

Charly-091@hotmail.com

Carlostun6@gmail.com

Saludos cordiales.

Carlos Ismael Tun Tun a 22 de noviembre del 2018