

**IvinsonCLS**

**CracksLatinos Team**

## INTRODUCCIÓN

Como dicen que la práctica hace al maestro, quiero mantenerme activo en el cracking y ¿qué mejor forma que metiéndole mano a cualquier software que encuentre por ahí? Esta vez les traigo un mini-tutorial acerca de una aplicación para desbloquear PDF's. Se trata de SysTools PDF Unlocker v3.1 de la compañía **SYSTOOL SOFTWARE**.

## Contacto:

<b>SysTools PDF Unlocker</b>	<a href="http://www.pdf-unlocker.com">http://www.pdf-unlocker.com</a>
<b>Contact Support:</b>	<a href="mailto:support@systoolsgroup.com">mailto:support@systoolsgroup.com</a>
<b>SysTools Software Blog:</b>	<a href="http://systoolssoftware.wordpress.com/">http://systoolssoftware.wordpress.com/</a>
<b>SysTools Software FAQs:</b>	<a href="http://www.systoolsfaqs.com/">http://www.systoolsfaqs.com/</a>

## CONOCIENDO AL OBJETIVO

Para tener una mejor idea de cómo atacar un programa, necesitamos hacerle algunos chequeos como por ejemplo, ver si solo es un demo, si requiere serial, si está empacado, etc. Al instalar esta aplicación, la encontramos en:

C:\Archivos de programa\SysTools PDF Unlocker\PDFUnlocker.exe

Ejecutémoslo a ver:



En el título de la ventana, nos recuerda que es un demo y vemos el botón de comprar más abajo.

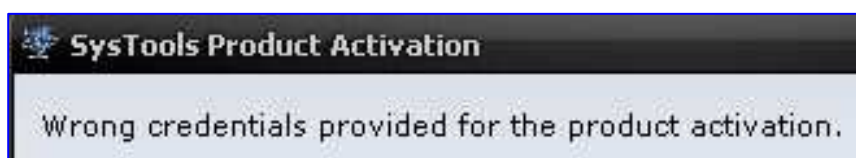
Vamos a Help/Activate:



Metamos nuestros datos falsos:

<b>Email Address:</b>	Ivinson@cracking.com
<b>Product Code:</b>	PDFUnlocker
<b>Product Key:</b>	12345

Al darle al botón activar nos muestra el mensaje de **Chico Malo**:



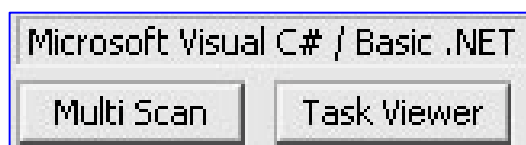
Hay muchas aplicaciones que no muestra este tipo de mensajes para dificultar un poco el trabajo "honesto" de los crackers que solo crackean por diversión y superación personal. Casi siempre, cuando tenemos un mensaje de clave incorrecta, lo primero que hacemos es buscar esa string en un depurador y ver donde está la comprobación y crear un keygen, auto-keygen, pescar un serial o simplemente hacer un parche. Hay algunos programadores que son un poco más "pilas" y empaican sus aplicaciones y que para dejarlas "incrackeables".

Voy a usar los clásicos detectores de packers a ver qué me dicen:

*RDG Packer Detector:*

<b>Visual C# / Basic .NET (Seems Obfuscated)</b>	<b>Compiler</b>
<b>Nada</b>	<b>Detected</b>

PEID:



Ambos detectores nos dicen que nuestra aplicación es un .NET, o sea, trabajaré con Reflector. ☺ También, dice RDG que parece estar ofuscado. “Veremos”.

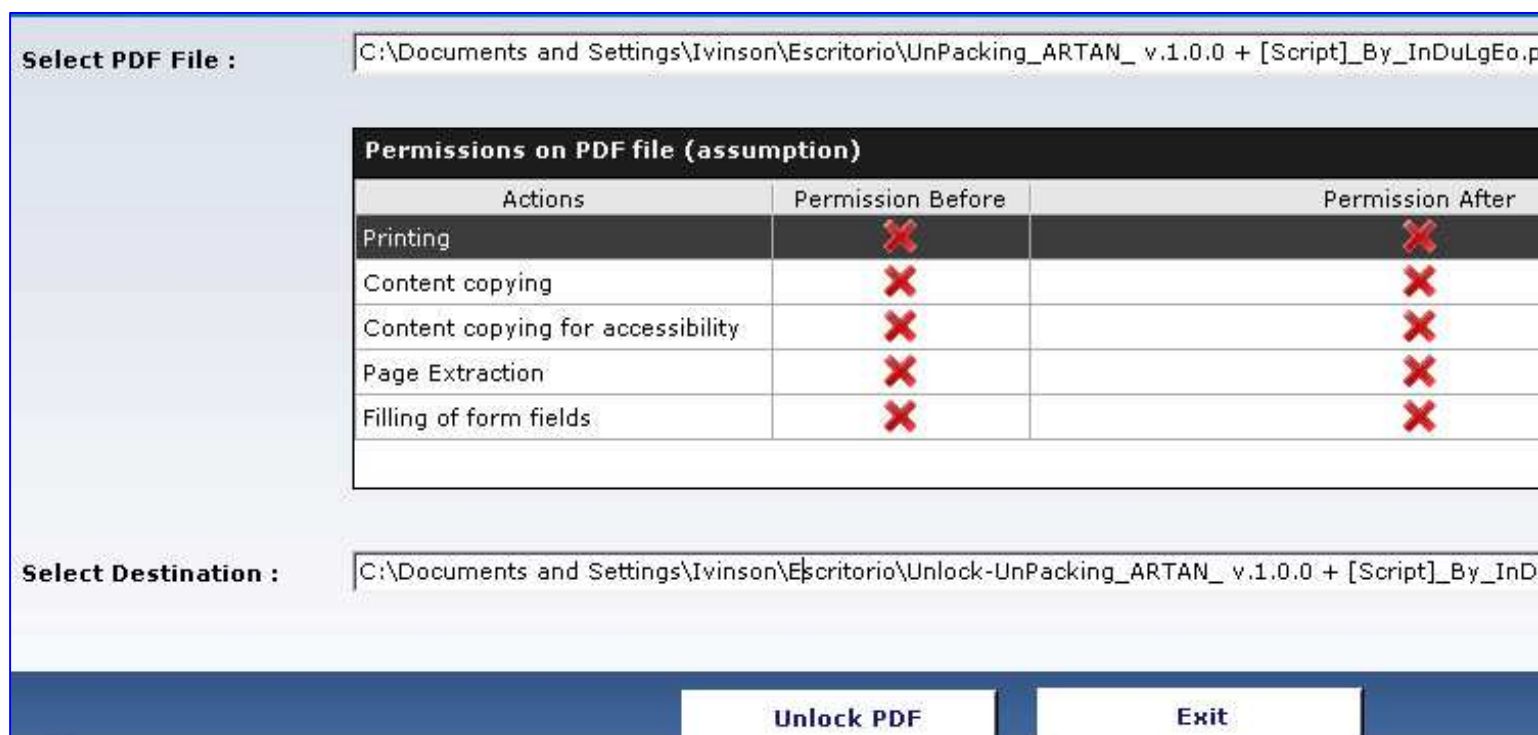
Voy a probar si este programa hace lo que promete. Tomaré como ejemplo el PDF de InDuLgEo que está protegido. Espero no se moleste. ☺ En el título de la ventana dice **PROTEGIDO** y seleccionamos el texto **INTRODUCCIÓN** y le damos clic derecho, no sale la opción Copiar, tampoco podemos imprimirlo:



Presionamos Unlock en Systools PDF Unlocker:



Cerremos el PDF y busquémoslo para desbloquearlo:



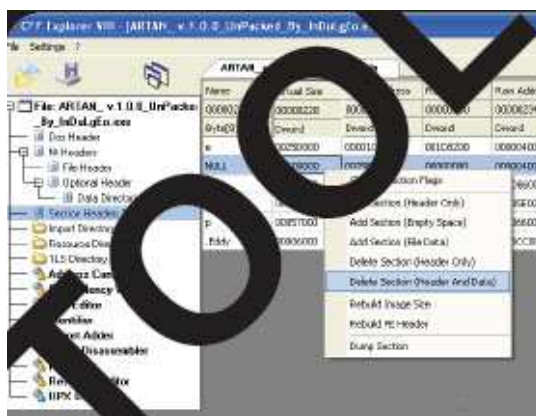
Elegimos el archivo PDF y la ubicación donde lo guardaremos. Vemos las **X** rojas indicando las restricciones del PDF: Imprimir, copiar, extracción de páginas, etc.

Le damos a Unlock PDF y nos avisa que fue desprotegido exitosamente:



El PDF original pesa 7.59 MB y el desprotegido con la versión demo, pesa 4.12 MB.

Le quitó todas las protecciones, pero como usé la versión demo, solo podemos leer una página sí y otra no. Intercaladas y con una marca de agua:



De forma intercalada, reemplaza el contenido poniendo el mensaje **Página en blanco intencionalmente insertada aquí:**

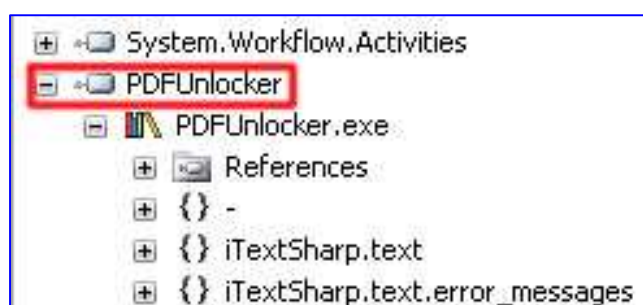
**Blank Page has been intentionally inserted  
here.**

<http://www.systoolsgroup.com/>

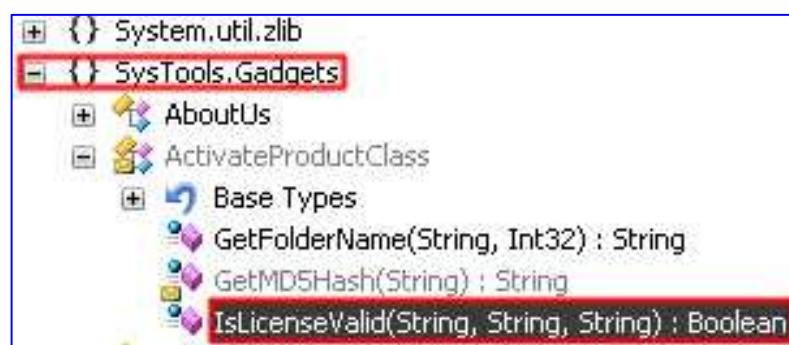


## Hora del cracking:

Carguemos el EXE en Reflector y mirémoslo:



Revisando un buen rato, encontré la parte caliente:



¿SysTools.Gadgets? Estaba difícil encontrarla. ☺



Si le damos clic a [IsLicenseValid](#), veremos a la derecha:

```
<MethodImpl(MethodImplOptions.NoInlining)> _  
Public Shared Function IsLicenseValid(ByVal productName As  
If (emailAddress = "PC-SYS408") Then  
    Return True  
End If  
Dim i As Integer  
For i = -3 To 3 - 1  
    Dim time As DateTime = DateTime.Today.AddDays(CDbl(i))  
    Dim str As String = ((time.Day.ToString & "-" & time.Month.T  
    If (ActivateProductClass.GetMD5Hash(String.Concat(New St  
        Return True  
    End If  
Next i  
Return False  
End Function
```

Ahí, vemos una condición. Si el **E-mail** es igual a **PC-SYS408**, retorna **TRUE** o verdadero. Luego, concatena la fecha, hora, etc.

Probaré ese “**E-mail**” y una clave cualquiera a ver:



SysTools Product Activation

Email Address: PC-SYS408

Product Code: PDFUnlocker

Product Key: 12345

Presiono el botón **Activate** y:



SysTools Product Activation

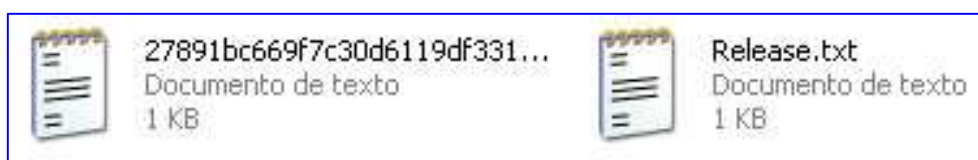
The product is successfully activated.

Reinicio el programa y ya lo tengo full:



☺ Resultó ser un **Hardcoded Serial**. Esto me recuerda los juegos que crackeó Daniel La Calavera. Los programadores cada vez están más flojos o no le están pagando bien.

Veamos los archivos que creó en la carpeta de instalación:



```
PDFUnlocker
=====
Email Address::PC-SYS408
Product Key::12345
ProductName::PDFUnlocker
Installed ON::viernes, 04 de octubre de 2013 12:04:45
Machine Name::X-xxxxxxxxxxxx
UID::d7d7d77d782gkg334434g34g4g4gg44h|
This license file is non-transferrable
```

Ese contenido lo tienen ambos archivos. En la última línea dice que esa licencia no es transferible. Pero el E:mail: **PC-SYS408** sí lo es. ☺

Esa parte la vemos en Reflector aquí:



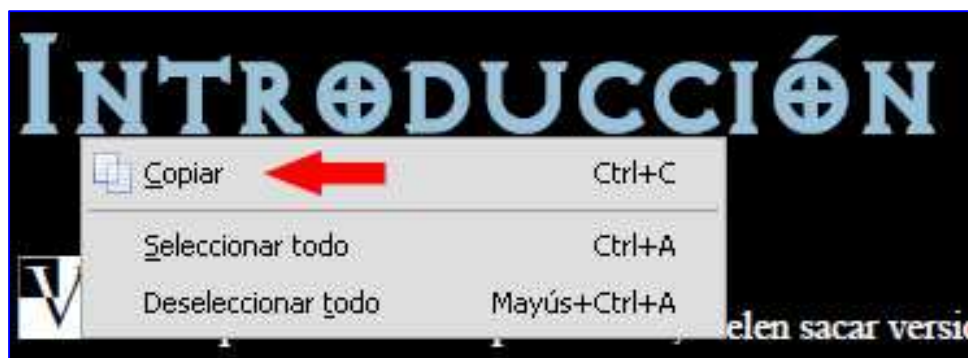
A la derecha nos lo muestra:

```
If ActivateProductClass.IsLicenseValid(Me.ProductName.Text, [text], productKey) Then
    Dim path As String = (Path.GetDirectoryName(Assembly.GetExecutingAssembly.Location) & "\Release.txt")
    Dim writer As New StreamWriter(path, False)
    writer.WriteLine(Me.ProductName.Text)
    writer.WriteLine("=====")
    writer.WriteLine("Email Address:" & [text])
    writer.WriteLine("Product Key:" & productKey)
    writer.WriteLine("ProductName:" & Me.ProductName.Text)
    writer.WriteLine("Installed ON:" & DateTime.Now.ToLongDateString & " " & DateTime.Now.ToLongTimeString))
    writer.WriteLine("Machine Name:" & Environment.MachineName)
    writer.WriteLine("UID:" & ActivateProductClass.GetMD5Hash((Environment.MachineName & Environment.OSVersion & Environment.I))
    writer.WriteLine("This license file is non-transferrable")
    writer.Close
    Dim input As String = File.ReadAllText(path)
    Dim str5 As String = ActivateProductClass.GetMD5Hash(input)
    writer = New StreamWriter((Path.GetDirectoryName(Assembly.GetExecutingAssembly.Location) & "\ " & str5 & ".txt"), False)
    writer.WriteLine(Me.ProductName)
    writer.WriteLine("=====")
    writer.WriteLine("Email Address:" & [text])
    writer.WriteLine("Product Key:" & productKey)
    writer.WriteLine("ProductName:" & Me.ProductName.Text)
    writer.WriteLine("Installed ON:" & DateTime.Now.ToLongDateString))
    writer.WriteLine("Machine Name:" & Environment.MachineName)
    writer.WriteLine("UID:" & ActivateProductClass.GetMD5Hash((Environment.MachineName & Environment.OSVersion & Environment.I))
    writer.WriteLine("This license file is non-transferrable")
    writer.Close
```

Y más abajo está el mensaje de Chico Bueno y Chico Malo. A buena hora lo vengo a encontrar. Después que registré el programa. ☺

```
Try
    Util.SendMailForActivation([text], input)
Catch obj1 As Object
End Try
Util.ShowAlert("PCVITA", "PCVITA Product Activation", "The product is successfully activated.", Choice.OK, Icon.Information)
Else
    Try
        Util.SendFailedActivation([text], productKey, Me.txtProductKey.Text)
    Catch obj2 As Object
    End Try
    Util.ShowAlert("PCVITA", "PCVITA Product Activation", "Wrong credentials provided for the product activation", Choice.OK, Icon.Information)
End If
MyBase.Close
End Sub
```

Probando la versión FULL:



Perfecto. Sin marca de agua ni páginas intercaladas. ☺

## Lo más chistoso:

No hace falta meterle el Product Key. ☺

E-mail address: **PC-SYS408**

Product Key:

Y puedo registrar creo que todos los programas de SysTools: ☺



Fin del tuto.



Comentarios | sugerencias:

E-mail: [ipadilla63@gmail.com](mailto:ipadilla63@gmail.com)

Twitter: @IvinsonCLS

Blog: [Crackingvenezolano.blogspot.com](http://Crackingvenezolano.blogspot.com)