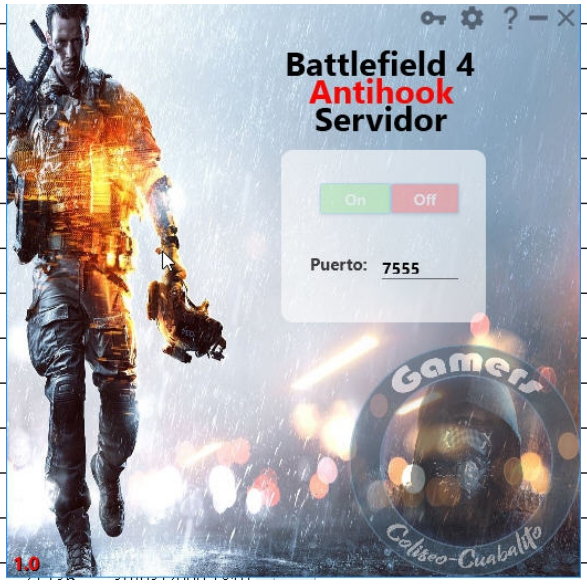
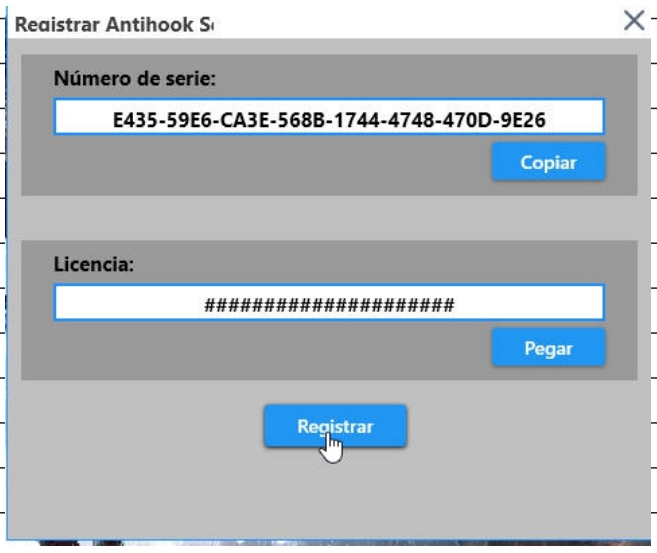
6 de Mayo de 2019

Programa:	Antihook Servidor Bf4
Descripción:	No tengo idea para que sirve
Protección:	Ninguna!
Objetivos:	Registrarme
Herramientas:	dnSpy 64
Dificultad:	Supongo que depende de cada uno, pero es muy fácil.
Cracker:	tincopasan

Primero aclaro que este escrito es para ayudar de forma simple a quien lo pidió, no es para mostrar todo lo que se puede hacer para romper este soft. Bueno, el objetivo ya se sabe, es registrarme.En este caso no hay dificultad. No tiene packer y es un .net
Por lo tanto lo cargo en el debugger lo ejecuto y a ver que hay.



Tiene desactivada la opción de on y no se que más se puede hacer ni me interesa, así que veo la opción de registro.El icono en forma de llave.



No voy a profundizar porque es una pérdida de tiempo, solo diré que mirando los métodos se encuentra el que se busca, hace referencia al largo = 32 , una llamada y el contenido del textbox licencia. si se cumplen las condiciones crea un archivo servidor.key con la licencia. Nada nuevo.

```
61          this.method_2();
62      }
63
64      // Token: 0x06000008 RID: 8 RVA: 0x00002788 File Offset: 0x00000988
65      private void method_2()
66      {
67          if (this.TextBoxLicencia.Text.Length == 32 && MainWindow.smethod_0(MainWindow.smethod_10(), this.TextBoxLicencia.Text))
68          {
69              using (campo) TextBox Activacion.TextBoxLicencia ervidor.key"))
70              {
71                  streamWriter.Write(this.TextBoxLicencia.Text);
72              }
73              MainWindow.smethod_13(this.TextBoxLicencia.Text);
74              this.IconNotReg.Visibility = Visibility.Hidden;
75              this.IconReg.Visibility = Visibility.Visible;
76              this.BtnPegar.IsEnabled = false;
77              this.TextBoxLicencia.IsEnabled = false;
78              this.BtnRegistrar.IsEnabled = false;
79              return;
80          }
81          this.IconReg.Visibility = Visibility.Hidden;
82          this.IconNotReg.Visibility = Visibility.Visible;
83      }
84
```

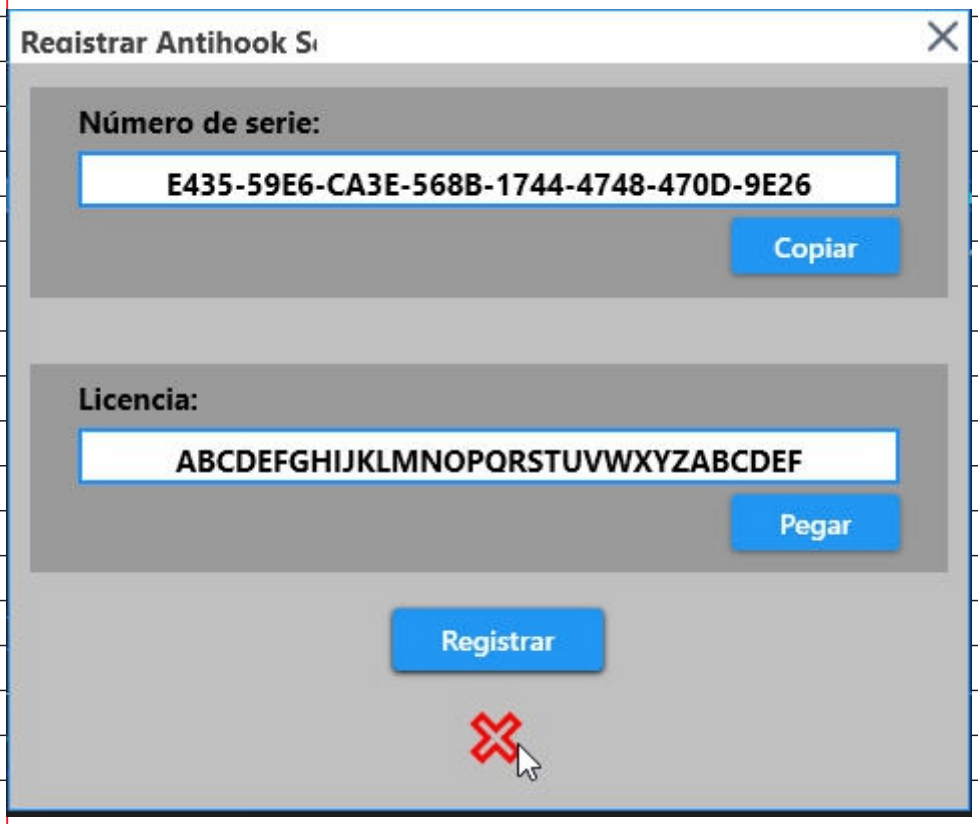
Como vi que hay una función recurrente puse un breakpoint al inicio, más que todo por curiosidad, supongo lo que hace pero estar seguro no está de más.

```
85
86      // Token: 0x06000011 RID: 17 RVA: 0x00002CE8 File Offset: 0x00000EE8
87      internal static bool smethod_0(string string_3, string string_4)
88      {
89          string[] array = string_3.Split(new char[]
90          {
91              '-'
92          });
93          array[0] = MainWindow.smethod_3(array[0]).Remove(5);
94          array[1] = MainWindow.smethod_3(array[1]).Remove(5);
95          array[2] = MainWindow.smethod_3(array[2]).Remove(5);
96          array[3] = MainWindow.smethod_3(array[3]).Remove(5);
97          array[4] = MainWindow.smethod_3(array[4]).Remove(5);
98          array[5] = MainWindow.smethod_3(array[5]).Remove(5);
99          array[6] = MainWindow.smethod_3(array[6]).Remove(5);
100         array[7] = MainWindow.smethod_3(array[7]).Remove(5).Remove(4);
101         return MainWindow.smethod_2(string.Concat(new string[]
102         {
103             array[0],
104             array[1],
105             array[2],
106             array[3],
107             array[4],
108             array[5],
109             array[6],
110             array[7]
111         })) == string_4;
112     }
113
114     // Token: 0x06000012 RID: 18 RVA: 0x00002DDC File Offset: 0x00000FDC
115     private static string smethod_1()
116     {
117         string text = "";
```

ales

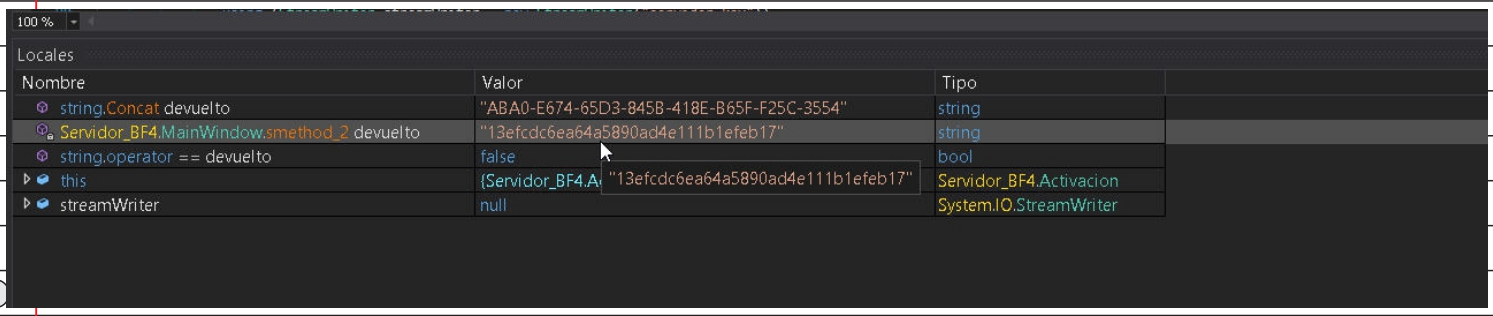
mbre	Valor	Tipo
string_3	"E435-59E6-CA3E-568B-1744-4748-470D-9E26"	string
string_4	"####################"	string
array	null	string[]

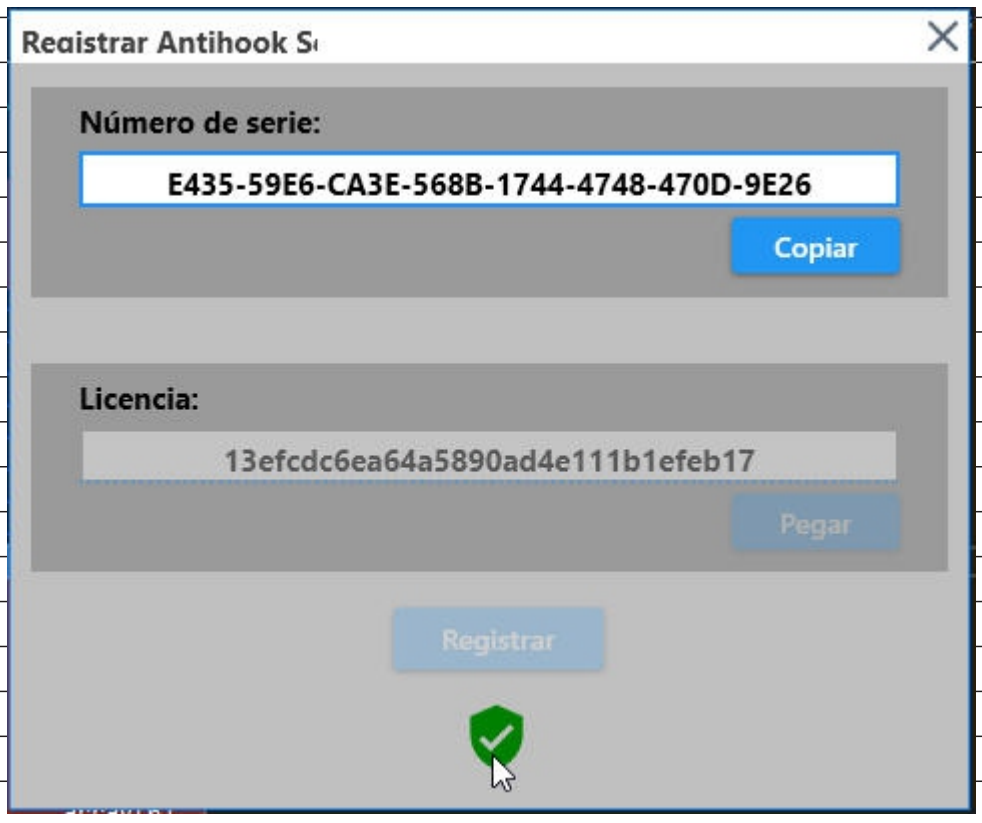
Se ve claramente que cadenas usa, y como las va manejando, en este caso cadena3= la suma de datos que obtiene por info del pc, que no pienso mostrar, el que quiera que los busque, están más que a la vista, más un hash. Obviamente este valor cambia en cada pc cadena 4 = es igual a la licencia que trae por defecto. Ok voy a cambiar la licencia por una que por lo menos tenga el largo adecuado y a repetir el proceso de registro.

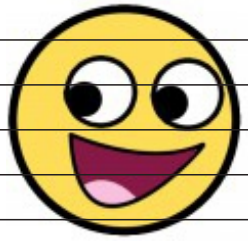


Le doy a Registrar y se ve que no le gustó el serial, no pone ningún mensaje escrito, muestra la imagen "X"

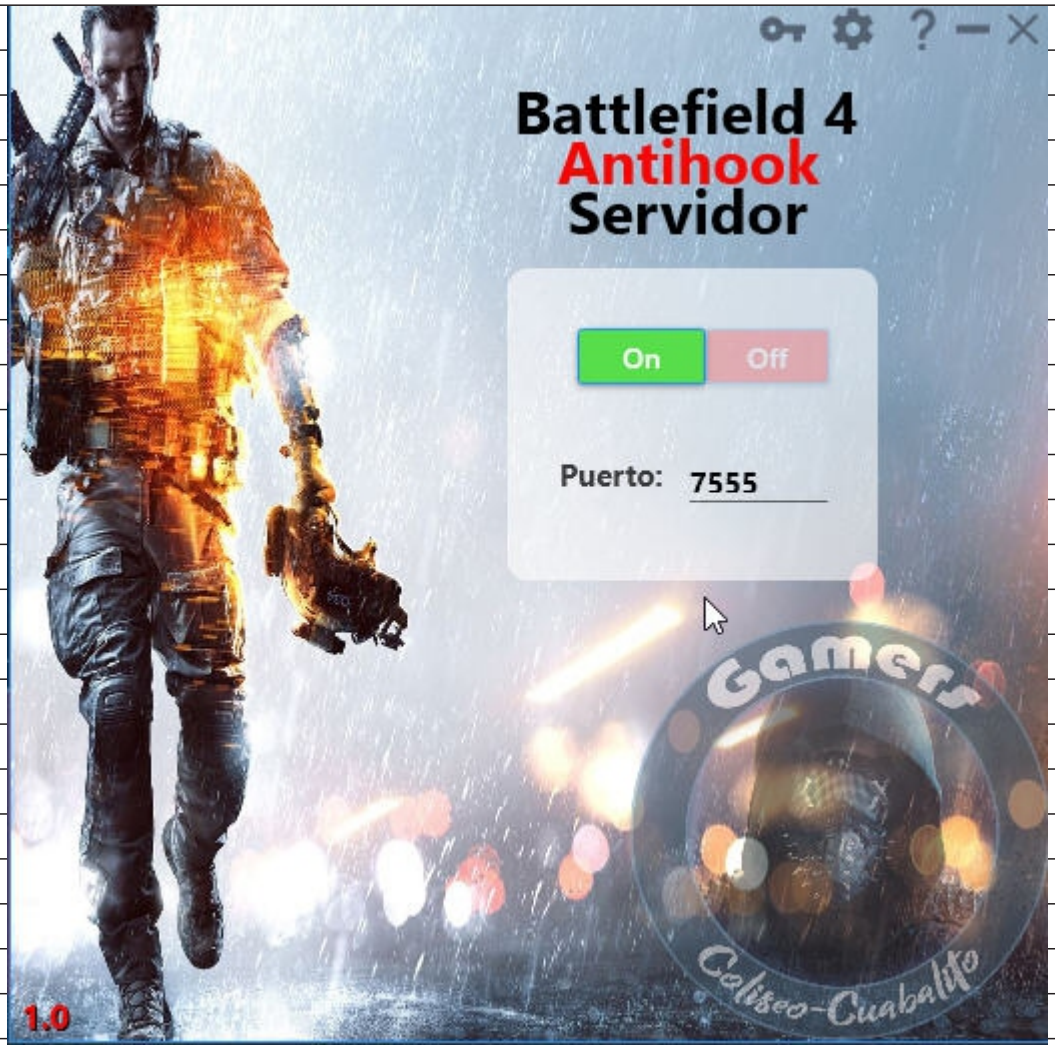
Ahora mirando el stack se ve claramente un valor devuelto que podría ser la licencia válida. ¿Qué se pierde con probar? Está demás decir que esta licencia solo me sirve a mí, ustedes busquen la suya, no es más de 1 minuto.







Listo! desactivó los botones, cambió el "X" por un visto y si miramos en el directorio de la aplicación creo el archivo antes mencionado. Supongo que esta huevada ya está registrada, no la puedo probar porque la verdad ni idea que carajo es. Además activo el "ON"



No me esfuerzo nada porque no le veo valor a hacerlo, no me sirve esta aplicación, si alguien quiere el keygen, pues que lo haga! Por lo menos ya ven como registrarse y como buscar los valores adecuados. Me perdí 1/2 hora en hacer este tute bastante inútil y un minuto en encontrar la licencia, pero bueno, escribir de vez en cuando no te mata.
Como siempre gracias a Ricardo Narvaja y a toda la lista de CracksLatinos que enseñan a perros como yo a destripar más de una tontería como esta. Saludos a quien pierda tiempo leyendo esto.