

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]



Software	I Hate This Key Deluxe v5.0.0.98 (http://www.bytegems.com)
Descarga	http://www.bytegems.com/files/IHateThisKeyDeluxeSetup.exe I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)
Protección	Serial.
Herramientas	Windows 10 Version 1803 x64 Bits (SO donde trabajamos) OllyDBG OllyICE v1.10 (for.Win_v8.1_x64 nad_x32) Visual Studio 2015 (VB.NET)
SOLUCIÓN	SERIAL VÁLIDO + KEYGEN
AUTOR	LUISFECAB
RELEASE	Julio 2018

INTRODUCCIÓN

Todo lo que escribí lo perdí, más de cinco días haciendo este tuto, eran más de 34 páginas. Me sentía muy contento, de lo que había hecho; había explicado paso a paso y dejaba unas explicaciones de todo, que hasta parecían redundantes, y todo aquello dirigido al lector novato como yo. Las imágenes con explicaciones y resaltaba lo importante. ¡Ah! Dios mío todo se me perdió y es que para mí en hacer un tuto me conlleva un esfuerzo gigante, el esfuerzo físico que hago no es cualquier cosa, solo imagínense que solo puedo usar un solo dedo para hacer todo y literalmente es tecla por tecla.

Había abordado cómo cazar nuestro serial ingresado con la API_GetWindowTexA, luego utilizábamos un par de APIS para trabajar con el registro de Windows como son la API_RegOpenKeyExA y API_RegCreateKeyExA.

Hacíamos mucho traceo para explicar cómo funcionaba y qué hacía el programa, y ponía énfasis en lo que hacíamos porque sabía que podría servir para aprender un poco más, para crackear aplicaciones semejantes, dejaba mis consejos por así decirlo.

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

También había explicado, cómo se podía crackear cambiando código, invirtiendo saltos y valores de los registros (que era solo uno), que aceptara cualquier serial de 31 caracteres; mostrando que puede haber diferentes formas de lograr el cometido.

Todo, todo aquello se perdió completamente. Sentía que era un buen tuto. Solo me quedó lo de sacar el serial válido que era mi objetivo final, pero lo perdido era igual de importante porque la idea es siempre compartir lo aprendido para que otros también aprendan.

Ya mi tuto nos para un novato novato porque solo voy a dejarles lo salvado y es el serial válido.

Bueno, con escribir de nuevo la esta introducción muy diferente a la anterior, me desahogado un poco. Como siempre un saludo a Ricardo Narvaja y al resto de los miembros de CRACKSLATINOS y también a los chicos de PERUCRACKERS, que al final somos todos uno solo, aficionados al cracking que nos gusta compartir esta experiencia.

Para terminar, esto lo hice tuto a partir de una consulta en la lista.

AL ATAQUE

Como todo se perdió, entonces lo primero que deben hacer es llegar a la NAG e ingresar nuestro serial de 31 caracteres "S1E2R3I4A4LDEBETENERTREINTAYUNO", el cual es tomado como correcto y reiniciar la aplicación. Luego van a la dirección **0040A4C0** y le ponen un **BREAKPOINT (BP)**.

Esto será resumido, lo prometo y lo explicaré en contexto general, seguro ustedes lo entenderán, si pude yo solito, con mis observaciones no tardarán tanto como yo.

Address	Hex dump	Disassembly	Comment
0040A4C0	83EC 3C	JNZ SHORT IHateThi.0040A4F7	
0040A4C3	A1 082C	MOV EAX,DWORD PTR DS:[452C08]	
0040A4C8	33C4	XOR EAX,ESP	
0040A4CA	894424	MOV DWORD PTR SS:[ESP+38],EAX	
0040A4CE	55	PUSH EBP	
0040A4CF	56	PUSH ESI	
0040A4D0	8B7424	MOV ESI,DWORD PTR SS:[ESP+48]	IHateThi.00454000
0040A4D4	33ED	XOR EBP,EBP	
0040A4D6	3BF5	CMP ESI,EBP	
0040A4D8	894C24	MOV DWORD PTR SS:[ESP+14],ECX	
0040A4DC	897424	MOV DWORD PTR SS:[ESP+C],ESI	IHateThi.00454000
0040A4E0	75 15	JNZ SHORT IHateThi.0040A4F7	
0040A4E2	5E	POP ESI	IHateThi.004010E8
0040A4E3	32C0	XOR AL,AL	
0040A4E5	5D	POP EBP	IHateThi.004010E8
0040A4E6	8B4C24	MOV ECX,DWORD PTR SS:[ESP+38]	
0040A4EA	33CC	XOR ECX,ESP	
0040A4EC	E8 1FE8	CALL IHateThi.00428D10	
0040A4F1	83C4 3C	ADD ESP,3C	
0040A4F4	C2 0400	RETN 4	
0040A4F7	8BC6	MOV EAX,ESI	IHateThi.00454000
0040A4F9	C74424	MOV DWORD PTR SS:[ESP+18],4	Agrega estos valores constantes para
0040A501	C74424	MOV DWORD PTR SS:[ESP+1C],9	despues con estos tomar partes del
0040A509	C74424	MOV DWORD PTR SS:[ESP+20],0F	serial
0040A511	C74424	MOV DWORD PTR SS:[ESP+24],15	
0040A519	C74424	MOV DWORD PTR SS:[ESP+28],1A	que esta separado por -
0040A521	C74424	MOV DWORD PTR SS:[ESP+2C],1F	
0040A529	8D50 01	LEA EDX,DWORD PTR DS:[EAX+1]	
0040A52C	8D6424	LEA ESP,DWORD PTR SS:[ESP+1]	
0040A530	8A08	MOV CL,BYTE PTR DS:[EAX]	
0040A532	83C0 01	ADD EAX,1	
0040A535	84C9	TEST CL,CL	
0040A537	75 F7	JNZ SHORT IHateThi.0040A530	
0040A539	2BC2	SUB EAX,EDX	
0040A53B	83F8 1F	CMP EAX,1F	
0040A53E	75 A2	JNZ SHORT IHateThi.0040A4E2	
0040A540	33C0	XOR EAX,EAX	
0040A542	53	PUSH EBX	
0040A543	8B4C24	MOV BYTE PTR SS:[ESP+34],CL	
0040A547	894424	MOV DWORD PTR SS:[ESP+35],EAX	
0040A548	894424	MOV DWORD PTR SS:[ESP+39],EAX	
0040A54F	894424	MOV DWORD PTR SS:[ESP+3D],EAX	
0040A553	8B4424	MOV BYTE PTR SS:[ESP+41],AL	
0040A557	896C24	MOV DWORD PTR SS:[ESP+C],EBP	
0040A55B	57	PUSH EDI	IHateThi.00454000
0040A55C	8D6424	LEA ESP,DWORD PTR SS:[ESP]	
0040A560	8D48 01	LEA ECX,DWORD PTR DS:[EAX+1]	Se comporta como un contador
0040A563	83F9 06	CMP ECX,6	cuando sea 6 se termina. El serial tiene 6 partes.
0040A566	894C24	MOV DWORD PTR SS:[ESP+18],ECX	Guarda el aumento de nuestro contador
0040A56A	74 0E	JE SHORT IHateThi.0040A57A	
0040A56C	8B4C84	MOV ECX,DWORD PTR SS:[ESP+EAX*4]	
0040A570	803C0E	CMP BYTE PTR DS:[ESI+ECX],2D	Busca separacion del serial
0040A574	0F85 A9	JNZ IHateThi.0040A623	salta si diferente de cero. Z=0
0040A57A	8B7C84	MOV EDI,DWORD PTR SS:[ESP+EAX*4]	
0040A57E	33DB	XOR EBX,EBX	
0040A580	3BEF	CMP EBP,EDI	
0040A582	8BF5	MOV ESI,EBP	IHateThi.00454000
0040A584	7D 3A	JGE SHORT IHateThi.0040A5C0	
0040A586	8B5424	MOV EDX,DWORD PTR SS:[ESP+14]	
0040A58A	0FB043	MOVSX EAX,BYTE PTR DS:[EDX+ESI]	
0040A58E	50	PUSH EAX	

Recuerden estamos trabajando sobre el archivo original y hemos agregado nuestro serial de 31 caracteres, "S1E2R3I4A4LDEBETENERTREINTAYUNO". Ustedes deben analizarlo y llegar a entender el funcionamiento y pueden descubrir que algo que yo diga no es correcto y que lo he interpretado mal.

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

Empecemos por lo resaltado en rojo, ese **LOOP** es solo para comparar la longitud de nuestro serial que deber ser **0x1F**, y como esa es la longitud, pues no hay lio.

Esos valores constantes que se guardan en **[ESP+XX]** (resaltado azul) se utilizan con el serial en la zona amarilla. Con esto podemos hallar el formato de nuestro serial.

[ESP+18],04 es para comparar el quinto carácter de nuestro serial con **0x2D** (ASCII: -). En los archivos del tuto les adjunto la tabla que tiene los valores ASCII. Nuestro quinto carácter resaltado en rojo, "S1E2**R**3I4A4LDEBETENERTREINTAYUNO".

Como ven, debería ser - (**0x2D**). entonces sigamos esa lógica con los otros valores de **[ESP+XX]**.

[ESP+1C],9 "S1E2**R**3I4A4LDEBETENERTREINTAYUNO"

[ESP+20],0F "S1E2**R**3I4A4LDEBE**T**ENERTREINTAYUNO" : **0x0F** = 15

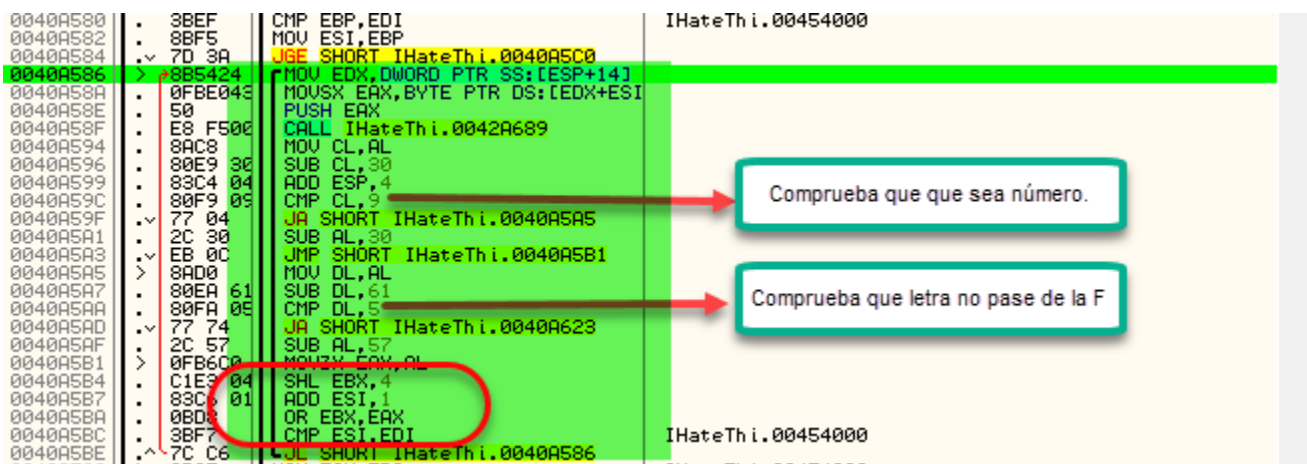
[ESP+24],15 "S1E2**R**3I4A4LDEBE**T**ENERT**R**EINTAYUNO" : **0x15** = 21

[ESP+28],1A "S1E2**R**3I4A4LDEBE**T**ENERT**R**EINT**A**YUNO" : **0x1A** = 26

Listo, debemos reemplazar nuestros caracteres resaltado en rojo por -, quedando nuestro serial "S1E2-3I4A-LDEBE-ENERT-EINT-YUNO".

Como podemos ver, el serial se compone de 6 partes y ahí entra en juego la zona resaltada en verde que es un **LOOP** que se repite por cada parte del serial.

Lleguemos a la NAG y metamos nuestro nuevo serial. Reiniciamos para ver qué pasa con nuestro nuevo serial en la "ZONA CALIENTE".



Lleguemos hasta **0040A586**. Ese **LOOP** resaltado en verde nos comprueba los caracteres permitidos en el serial. El serial solo puede tener números y hasta la letra F, y si miramos nuestro serial "S1E2-3I4A-LDEBE-ENERT-EINT-YUNO", nos podemos dar cuenta que tenemos letras que pasan de la F. Bueno cambiemos esos caracteres por unos que cumplan la condición de ese **LOOP**. Bueno, ahí lo cambié "F1E2-F3A4-48DEB-5589B-6435-4D23". En ese recuadro en rojo hay un procedimiento que se realiza con los valores que saca con cada carácter, ahí el valor importante va quedando en **EBX**. Cuando hagan este procedimiento con este serial ya

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

corregido notaran que en **EBX** queda la parte del serial que se está trabajando. Por ejemplo, la primera parte es "F1E2" entonces **EBX=0000F1E2**.

Listo, ya tenemos un nuevo serial que nos lleva más al fondo del camino correcto y no nos vota. Hagamos todo de nuevo, llegar a la NAG y meter este nuevo serial. Reinicias y llega de nuevo a la "ZONA CALIENTE".

Assembly code snippet:

```
0040A5FB : 03D0 ADD EDX, EAX
0040A5FD : 895424 MOV DWORD PTR SS:[ESP+10], EDX
0040A601 : 8B19 MOV BYTE PTR DS:[ECX], BL
0040A603 : C1FB 08 SAR EBX, 8
0040A606 : 83E9 01 SUB ECX, 1
0040A609 : 83E8 01 SUB EAX, 1
0040A60C : 75 F3 JNZ SHORT IHateThi.0040A601
0040A60E : 8B4424 MOV EAX, DWORD PTR SS:[ESP+18]
0040A612 : 83F8 06 CMP EAX, 6
0040A615 : 8D6F 01 LEA EBP, DWORD PTR DS:[EDI+1]
0040A618 : 7D 20 JGE SHORT IHateThi.0040A63A
0040A61A : 8B7424 MOV ESI, DWORD PTR SS:[ESP+14]
0040A61F : F9 8F8F JMP IHateThi.0040A65A
```

Hex dump snippet:

Address	Hex dump	Unicode
0019F7F4	F1 E2 F3 A4 04 8D EB 05 58 9B 64 35 4D 23 40 00@
0019F804	0E 12 A6 C5 E8 10 40 00 D8 04 60 02 D6 1D AC C5
0019F814	00 40 45 00 E8 20 44 00 07 00 00 00 69 00 6C 00il
0019F824	56 3A 39 77 5E C5 8A 96 88 54 74 00 00 00 73 00
0019F834	90 54 74 00 17 00 00 17 65 00 47 00 65 00 6D 00
0019F844	73 00 2E 00 02 00 00 02 6D 00 5C 00 26 03 00 25	s.8"m
0019F854	48 00 61 00 02 00 00 02 20 00 54 00 02 00 00 02	Ha"Te
0019F864	73 00 20 00 4B 00 65 00 79 00 20 00 44 00 65 00	s Key De
0019F874	6C 00 75 00 00 00 00 00 5C 00 49 00 15 00 00 00	lu..IS.
0019F884	F1 FC FF 00 00 00 00 69 00 73 00 4B 00 65 00	'...iske
0019F894	79 00 4C 00 4F 00 43 00 00 00 73 00 15 00 00 00	yLOC.sS.
0019F8A4	00 00 00 00 84 02 73 00 00 00 80 00 00 00 00	...s..t
0019F8B4	AA AA AA AA AA AA AA AA AA AA AA AA 88 54 74 AAt

Callout bubble text: Son los caracteres de nuestro serial unidos en parejas F1E2-F3A4-48DEB-5589B-6435-4D23

Recorre los **LOOP** hasta llegar a la dirección **0040A601**, fíjate lo que sucede ahí, hazlo hasta terminar todo. Esa imagen lo explica muy bien. Todo ese rollo de los dos **LOOP** es para llegar a esto. En el **DUMP** se guarda nuestro serial en la dirección **0019F7F4** en parejas originando valores hexadecimales y ese es el motivo de poder ingresar letras hasta la F. Esto se hace seis veces y ya saben el motivo, porque el serial se compone de seis partes.

Bueno, después de que salgan de esos procedimientos sigan traceando con **<F7>** hasta llegar a **0040A38D**.

Assembly code snippet:

```
0040A38C : 56 PUSH ESI
0040A38D : E8 DEC CALL IHateThi.0040A470
0040A392 : 6A 03 PUSH 3
0040A394 : 6A 07 PUSH 7
0040A396 : 6A 0E PUSH 0E
0040A398 : 56 PUSH ESI
0040A399 : 8BCF MOV ECX, EDI
0040A39B : 8BD8 MOV EBX, EAX
0040A39D : E8 CE0 CALL IHateThi.0040A470
0040A3A2 : 0FB656 MOVZX EAX, BYTE PTR DS:[ESI+1]
```

Registers (FPU) snippet:

Register	Value
EAX	00005589B
ECX	0000000A
EDX	0000000A
EBX	00048DEB
ESP	0019F7A4
EBP	00000020
ESI	0019F7F4
EDI	0019F818
EIP	0040A3A2

Comment: Sale EAX=048DEB valor trabajado datos de nuestro serial

Comment: F1E2-F3A4-48DEB-5589B-6435-4D23

Comment: Sale EAX a EBX=48DEB

Comment: Sale EAX=05589B valor trabajado datos de nuestro serial

Comment: Segundo byte serial

Y tenemos dos **CALL** y que hacen prácticamente lo mismo. El primer **CALL** pone la tercera parte del serial que inicialmente queda en **EAX**, pero termina finalmente en **EBX=00048DEB** cuando se llega al segundo **CALL**, y precisamente el segundo **CALL** pone la cuarta parte del serial en **EAX=0005589B**. Ahora en las siguientes imágenes se trabajará con la parte 1 y 2 del serial para hallar un valor y ser comparado con **EBX**; y también con la parte 5 y 6 para luego ser comparado con **EAX**.

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

0040A3A2	. 0FB656	MOVZX EDX,BYTE PTR DS:[ESI+1]	Segundo byte serial
0040A3A6	. 0FB64E	MOVZX ECX,BYTE PTR DS:[ESI+2]	Tercer byte serial
0040A3AA	. 0FB63E	MOVZX EDI,BYTE PTR DS:[ESI]	Primer byte serial
0040A3AD	. 0FAFCA	IMUL ECX,EDX	Multiplica tercer byte*segundo byte
0040A3B0	. 0FB656	MOVZX EDX,BYTE PTR DS:[ESI+3]	Mueve cuarto byte serial
0040A3B4	. 0FAFD7	IMUL EDX,EDI	Multiplica primer byte serial*cuarto byte serial
0040A3B7	. 03CA	ADD ECX,EDX	Suma las dos multiplicaciones
0040A3B9	. 8D0C49	LEA ECX,DWORD PTR DS:[ECX+ECX*2]	Trabaja con la suma
0040A3BC	. 8D5409	LEA EDX,DWORD PTR DS:[ECX+ECX+4B]	Sigue trabajando con la suma
0040A3C0	. 3BD3	CMP EDX,EBX	compara la suma con el valor hallado en 40A3B0
0040A3C2	. 75 2F	JNZ SHORT IHateThi.0040A3F3	
0040A3C4	. 0FB64E	MOVZX ECX,BYTE PTR DS:[ESI+C]	

EBX=00048DEB
EDX=0008A5C7

Aquí está la primera parte de la solución, todos estos cálculos se hacen con las partes 1 y 2 de nuestro serial y el resultado debería ser la tercera parte del serial, pero como vemos no son iguales. Nuestro resultado fue **EBX=00048DEB** y debería haber sido **EDX=0008A5C7**. Pues la solución es muy sencilla ya que la tercera parte del serial solo se utiliza para compararla con este resultado, pues ya sabemos que la tercera parte del serial debe ser **8A5C7**. El serial válido nos va quedando, "F1E2-F3A4-**8A5C7**-5589B-6435-4D23". Sigamos con el próximo cálculo que es lo mismo.

0040A3B7	. 03CA	ADD ECX,EDX	
0040A3B9	. 8D0C49	LEA ECX,DWORD PTR DS:[ECX+E	
0040A3BC	. 8D5409	LEA EDX,DWORD PTR DS:[ECX+E	
0040A3C0	. 3BD3	CMP EDX,EBX	
0040A3C2	. 75 2F	JNZ SHORT IHateThi.0040A3F3	
0040A3C4	. 0FB64E	MOVZX ECX,BYTE PTR DS:[ESI+4	
0040A3C8	. 0FB656	MOVZX EDX,BYTE PTR DS:[ESI+4	
0040A3CC	. 0FAFD1	IMUL EDX,ECX	
0040A3CF	. 0FB64E	MOVZX ECX,BYTE PTR DS:[ESI+4	
0040A3D3	. 0FB676	MOVZX ESI,BYTE PTR DS:[ESI+4	
0040A3D7	. 0FAFCE	IMUL ECX,ESI	
0040A3DA	. 8D0C49	LEA ECX,DWORD PTR DS:[ECX+E	
0040A3DD	. 8D9451	LEA EDX,DWORD PTR DS:[ECX+E	
0040A3E4	. 3BD0	CMP EDX,EAX	
0040A3E6	. 75 0B	JNZ SHORT IHateThi.0040A3F3	
0040A3E8	. 5E	POP ESI	
0040A3E9	. 5B	POP EBX	
0040A3EA	. B8 0100	MOV EAX,1	
0040A3EF	. 5F	POP EDI	
0040A3F0	. C2 0800	RETN 8	
0040A3F3	. 5E	POP ESI	
0040A3F4	. 5B	POP EBX	
0040A3F5	. 30C0	XOR EAX,EAX	
0040A3F7	. 5F	POP EDI	
0040A3F8	. C2 0800	RETN 8	
0040A3FB	. CC	INT3	
0040A3FC	. CC	INT3	
0040A3FD	. CC	INT3	
0040A3FE	. CC	INT3	

EAX=0005589B
EDX=00005B02

Primero, debemos pasar ese salto **JNZ** de **0040A3C2** porque como saben la comparación no nos dio, entonces nos bota fuera. Para eso nos posicionamos en la dirección **0040A3C4**, <Clic derecho -> **New origin here**>. Luego traceamos hasta la dirección próximo salto en **0040A3E4**.

0040A3D0	. 8D9451	LEA EDX,DWORD PTR DS:[ECX+EDX*2]	
0040A3E4	. 3BD0	CMP EDX,EAX	
0040A3E6	. 75 0B	JNZ SHORT IHateThi.0040A3F3	
0040A3E8	. 5E	POP ESI	
0040A3E9	. 5B	POP EBX	
0040A3EA	. B8 0100	MOV EAX,1	
0040A3EF	. 5F	POP EDI	
0040A3F0	. C2 0800	RETN 8	
0040A3F3	. 5E	POP ESI	
0040A3F4	. 5B	POP EBX	
0040A3F5	. 30C0	XOR EAX,EAX	
0040A3F7	. 5F	POP EDI	
0040A3F8	. C2 0800	RETN 8	
0040A3FB	. CC	INT3	
0040A3FC	. CC	INT3	
0040A3FD	. CC	INT3	
0040A3FE	. CC	INT3	

EAX=0005589B
EDX=00005B02

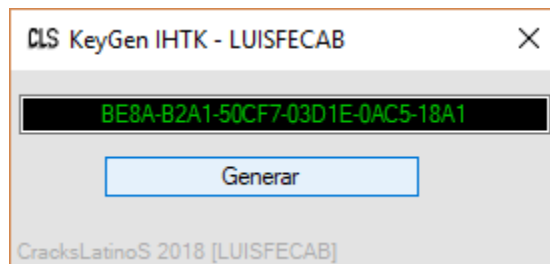
Lo mismo, pero el cálculo se realiza con las partes 5 y 6 del serial y el resultado obtenido en **EDX=00005B02**, se compara con la cuarta parte de nuestro serial que está en **EAX=0005589B** y como vemos no son iguales ni por las curvas. Entonces para tener nuestro serial válido la cuarta parte de nuestro serial es el resultado de ese procedimiento que viene siendo **05B02**.

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

Con todo lo que hemos hecho nuestro serial válido sería, "F1E2-F3A4-8A5C7-05B02-6435-4D23".

Ahí está les presento mi primer serial válido. Les diría que muy contento, pero no, con la perdida prácticamente de todo el tuto, me queda un sabor agridulce.

Ya para ir terminando, me le medí a hacer el Keygen y lo pude hacer. Lo hice de la mejor forma posible, al inicio ni idea por dónde empezar a hacerlo porque mi única experiencia programando es en Visual Basic y ahora con el VB.net programando las formulas de perforación, producción o yacimientos cuando estudié mi carrera y no trabajaba con valores HEXADECIMALES; por ahí consulté información y le busqué "la comba a palo" para hacerlo.



Me despido, un abrazo inmenso para todos y espero sea de utilidad para la comunidad este pequeño tuto, hecho con mucho esfuerzo, pero hecho con más cariño, aún.