Programa	Ultra iso 9.5.2.2836
Protección	Aspack v2.12
Objetivo	Más que desempacar descifrar el md5 para nuestro usuario y contraseña
Web/descarga	https://www.ezbsystems.com/ultraiso/
Dificultad	3 de 10
Plataforma	Windows 10
Lenguaje	Borland c++
Herramientas	Ollydbg, calculadora de Windows, ASPackDie_1.41
Cracker	Carlos Ismael
Fecha	23 de octubre del 2015
Contacto	Charly-091@hotmail.com

Bueno aquí estamos de nuevo como ya saben mi nombre es Carlos Ismael Tun Tun originario de Yucatan Mexico, pues este es mi siguiente tutorial, como siempre he dicho espero que no sea el último.

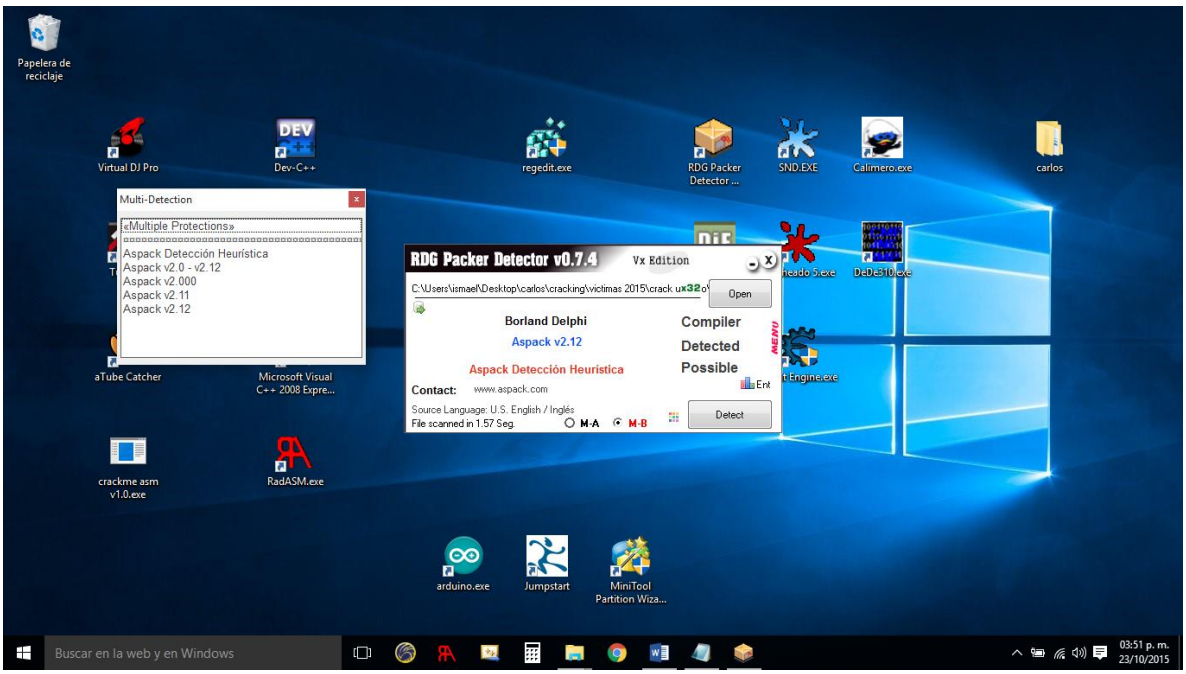
Es grato para mí escribir para difundir el conocimiento y más si se trata de este tipo de cosas, el cual es muy poco conocido en nuestro país.

Disclaimer

Este tutorial fue escrito con fines educativos y para difundir el conocimiento, el programa que se uso es solo para puro ejemplo.

Pues comencemos:

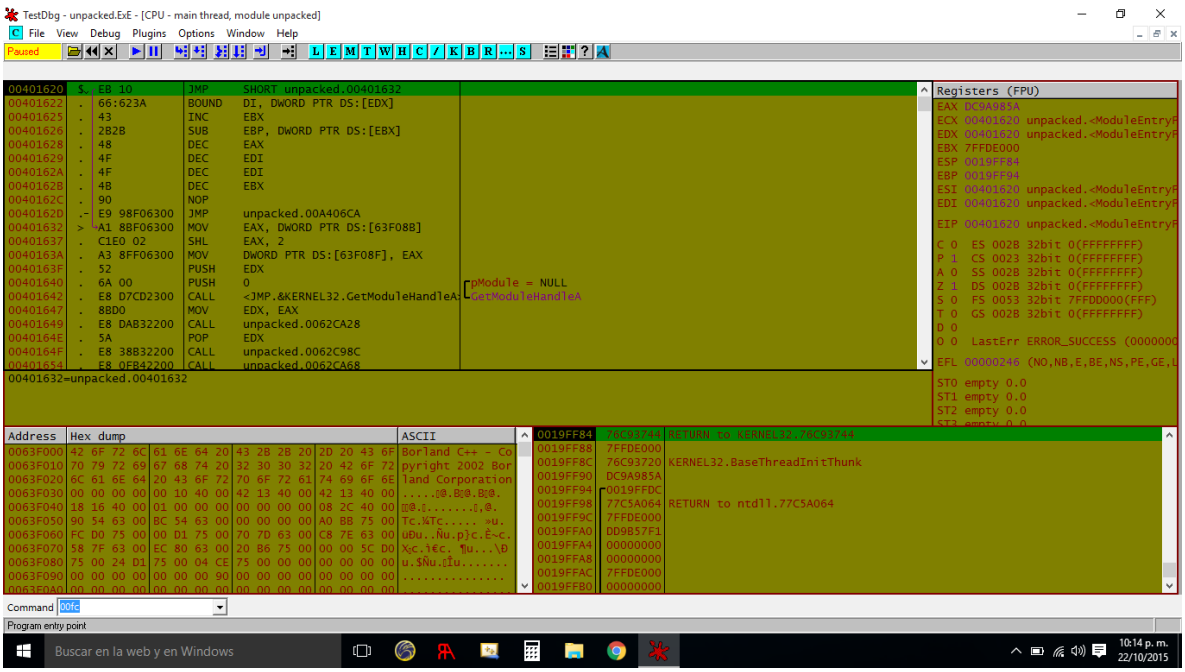
Lo primero es pasarle el detector de packers. Y esto es lo que nos muestra.



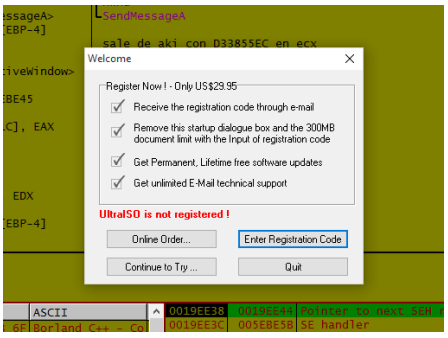
Vemos que está protegido con el aspack v2.12, me dio FIACA desempacarlo ya que sabemos cómo se hace, buscamos pushad breackpoint en esp dos veces F8 mas y ya, lo dumpeamos luego con el iRec lo preparamos y ya. Pero la verdad lo hice con el desempacador de akira (ASPackDie_1.41) que lo descargamos de la web de Ricardo en:

http://ricardonarvaja.info/WEB/OTROS/HERRAMIENTAS/A-B-C-D-E/ lo usamos con el programa y ya podemos seguir sale??

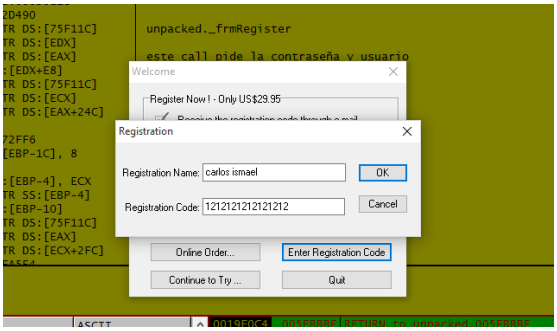
Entry point del programa….



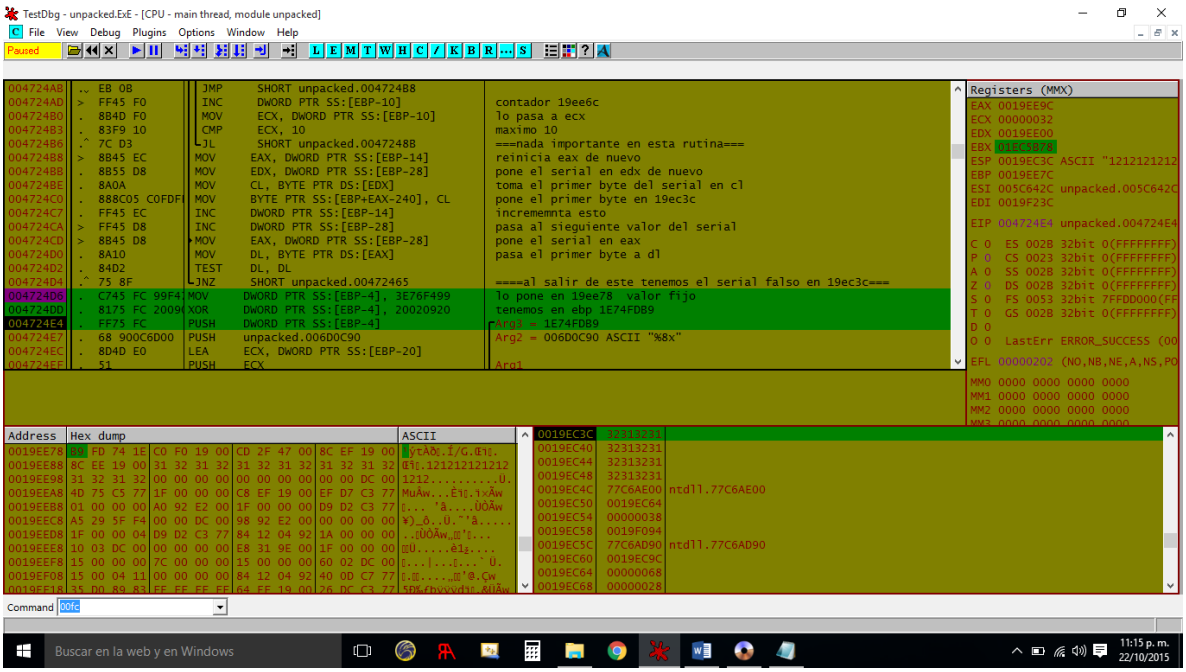
Iniciamos el programa



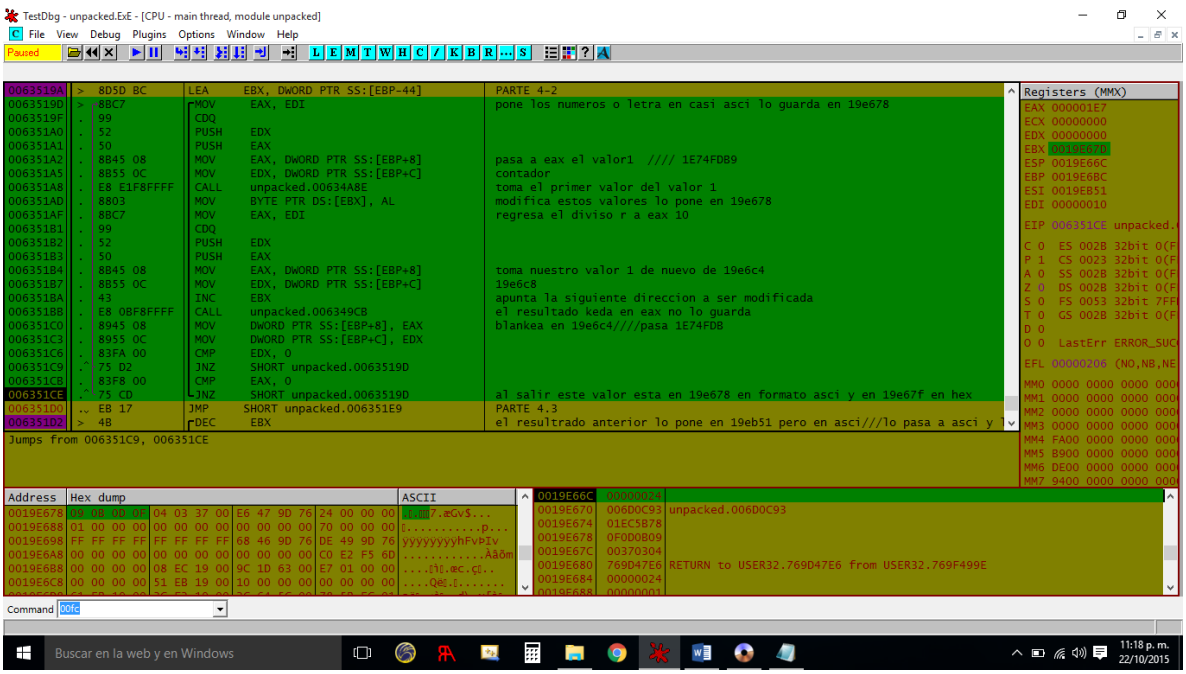
Metemos unos datos así jejejeje



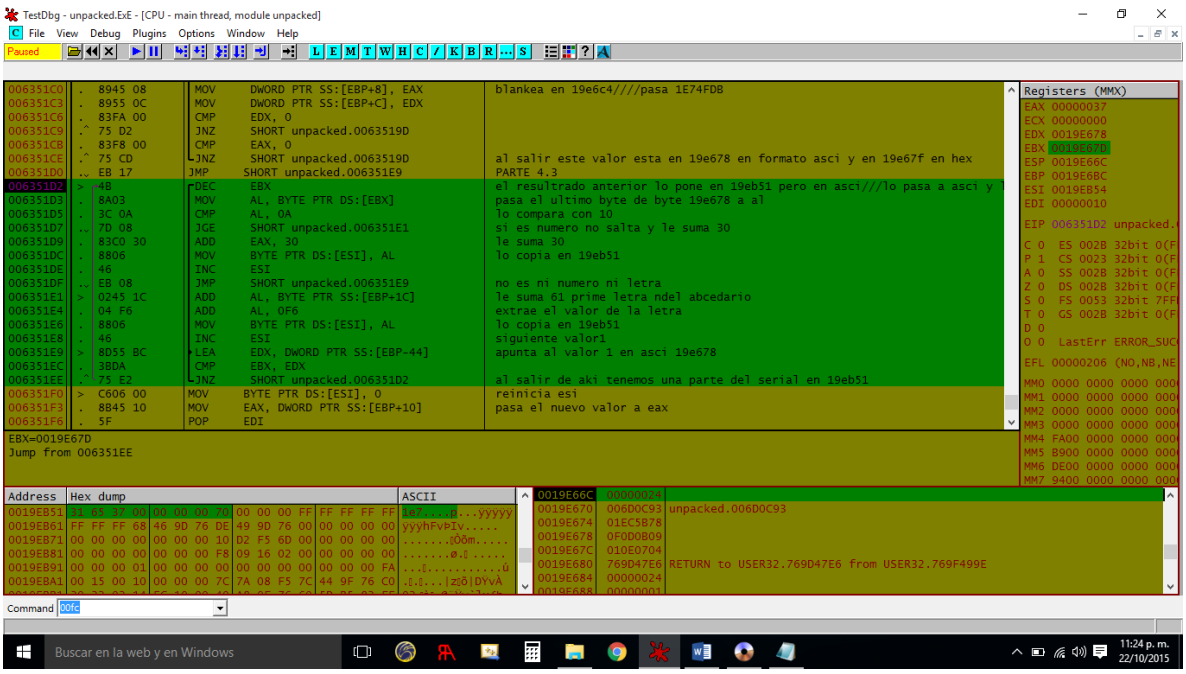
Aquí se genera un valor muy importante: 1e74fdb9, el cual es una constante, siempre va ser el mismo para todos los nombres que metamos.



En las dos siguientes imágenes lo transforma en ASCII con los siguientes procedimientos, (son muy fáciles de entender, de seguro lo usare en alguna aplicación más tarde jejejejejeje ;))

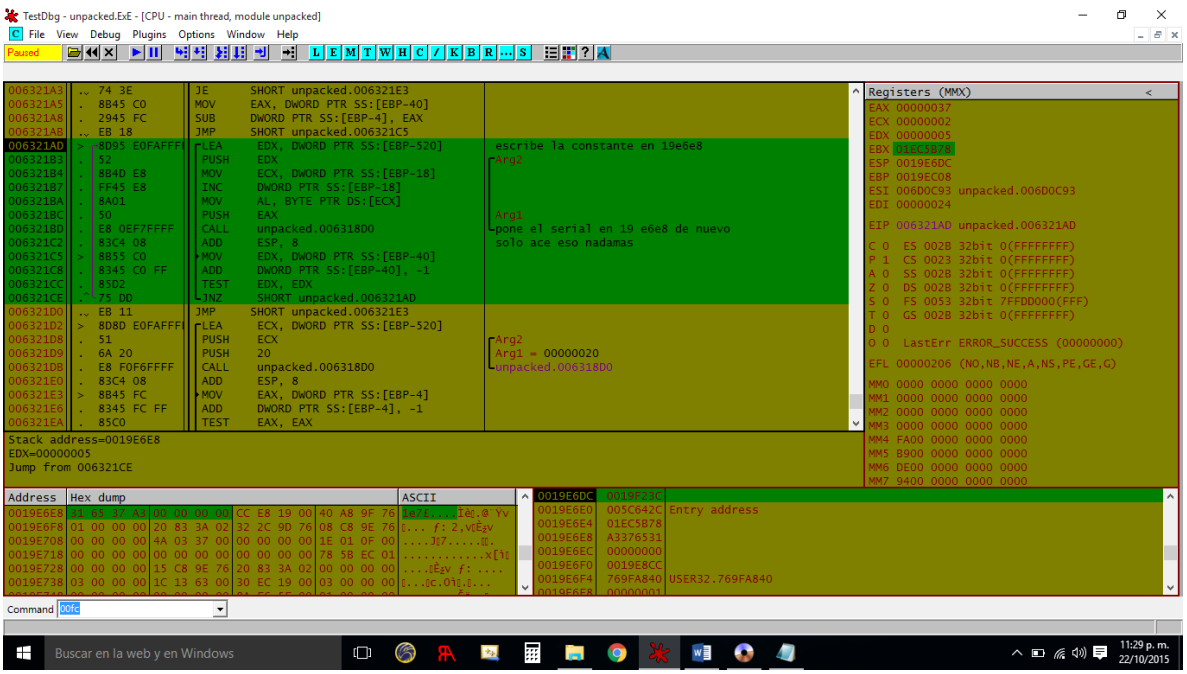


Tengo seleccionado donde lo va guardar y también sabemos que lo saca del procedimiento de la imagen anterior. Queda claro??

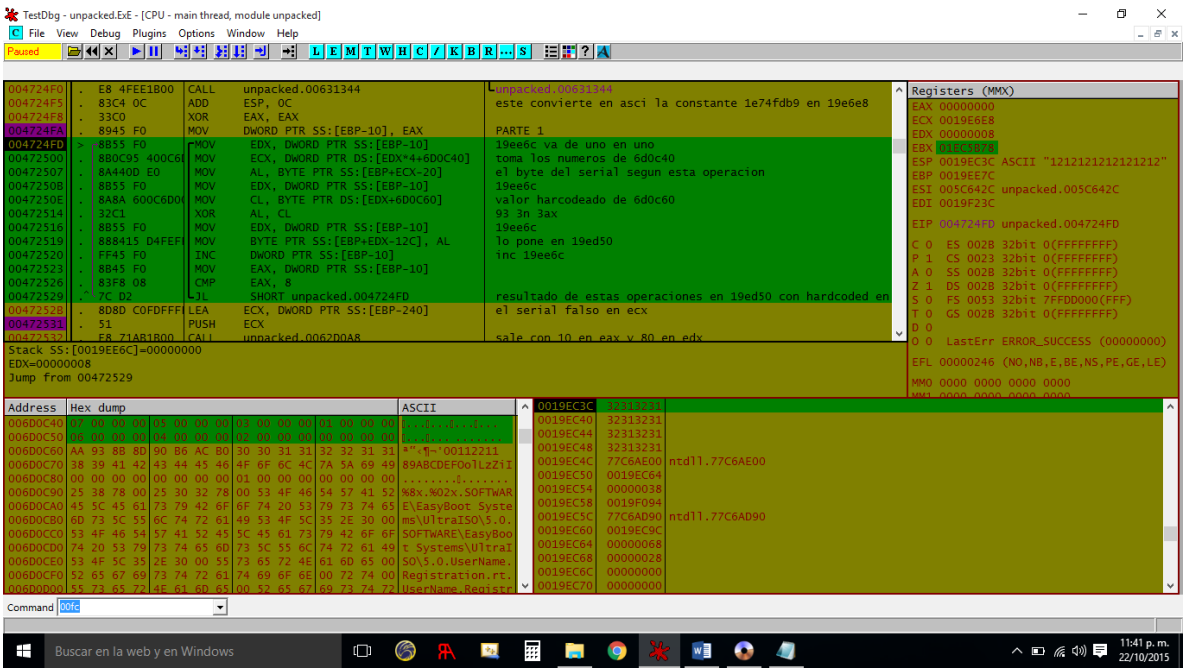


Pasa el valor contante a la dirección siguiente esto con el propósito de que no nos perdamos lo que hace el programa, les recuerdo que tiene mucho código que repite y repite las cosas o se la pasa copiando los valores en direcciones diferentes varias veces, lo digo de una vez por si acaso se quedan con “¿y de donde saco ese valor?” jejejejee ok?? Bueno sigamos..

Crackeando ultraiso by Carlos ismael



En la siguiente imagen seleccionamos la parte en la que trabaja con la constante



Estos números son los que tomara para calcular la posición siguiente el cual se traduce como

Posición = Contador*4 + dirección de memoria

0*4=0 posición 7

1*4=4 posición 5

2*4=8 posición 3

Fecha: 23 de octubre del 2015 Ultra Iso Carlos Ismael Tun Tun

3*4=12 posición 1

4*4=16 posición 6

5*4=20 posición 4

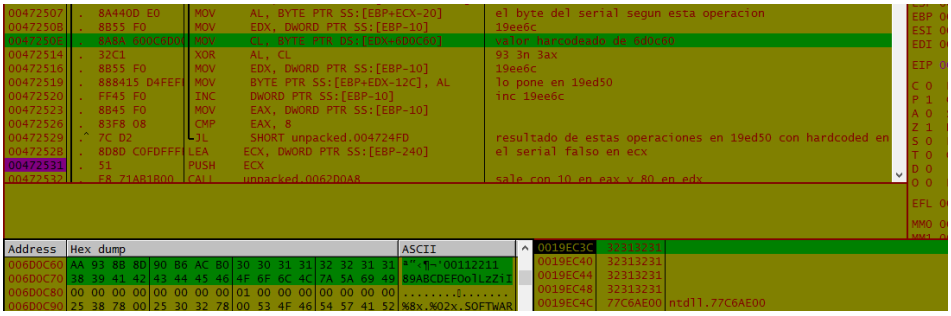
6*4=24 posición 2

7*4=28 posición 00

Estos son los números obtenidos en cada vuelta

Estos son las posiciones ya ordenados (yo lo ilustro así ya que el programa no trabaja de esta manera)

9d4ebf71= 39 64 34 65 62 66 37 31

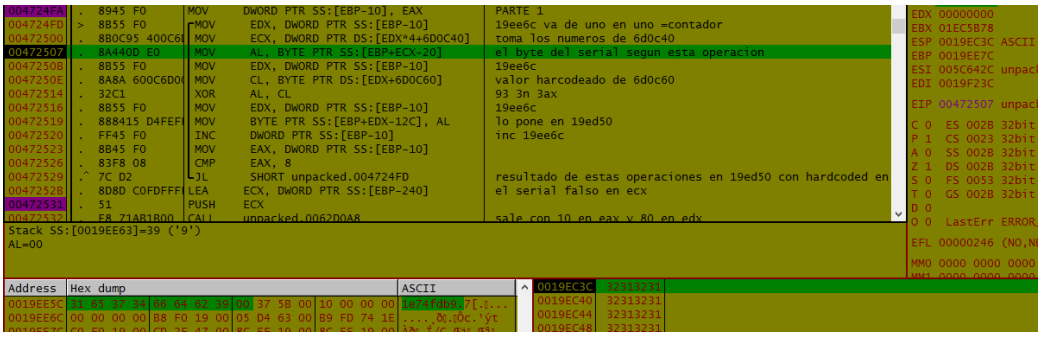


La operación siguiente lo toma como posición para el byte de la constante que vamos a tomar la cual la traducimos como:

Byte a tomar=dirección de memoria+posición

Estos son los valores que toma según la operación anterior

AA 93 8B 8D 90 B6 AC B0



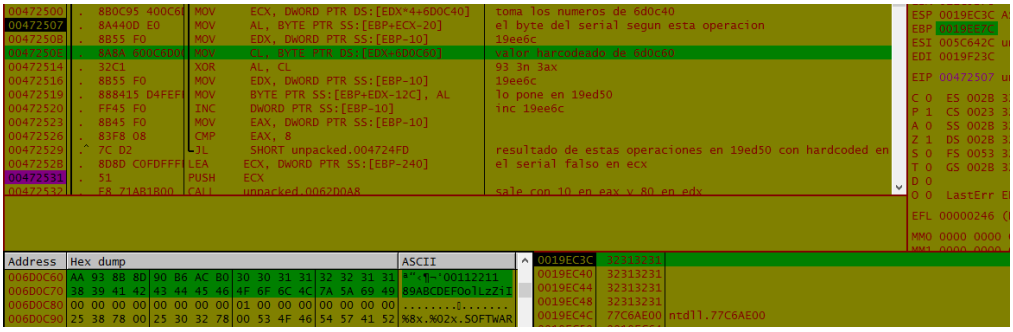
Toma valores de ahí según el contador

Después les hace xor

AA 93 8B 8D 90 B6 AC B0

xor

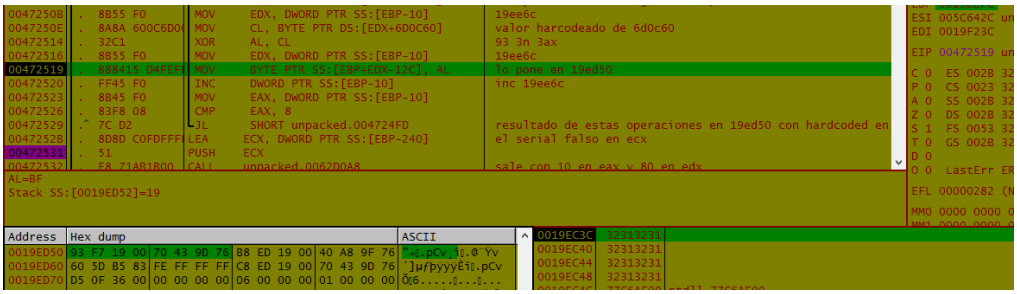
39 64 34 65 62 66 37 31



El resultado lo guarda ahí..

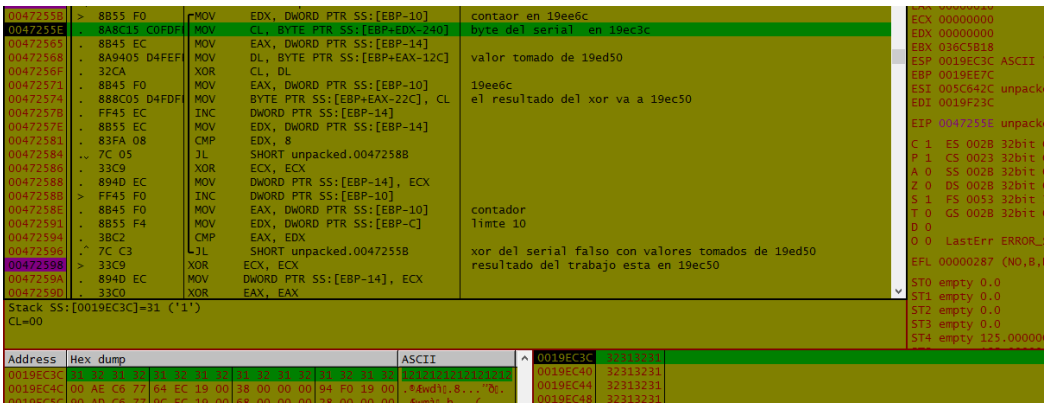
Resultado= 93 F7 BF E8 F2 D0 9B 81 la cual queda en 19ED50

A partir de aquí si queremos hacer nuestro keygen podemos tomar este valor como constante no es necesario hacer todo este marañero… jejejejejeje verdad???



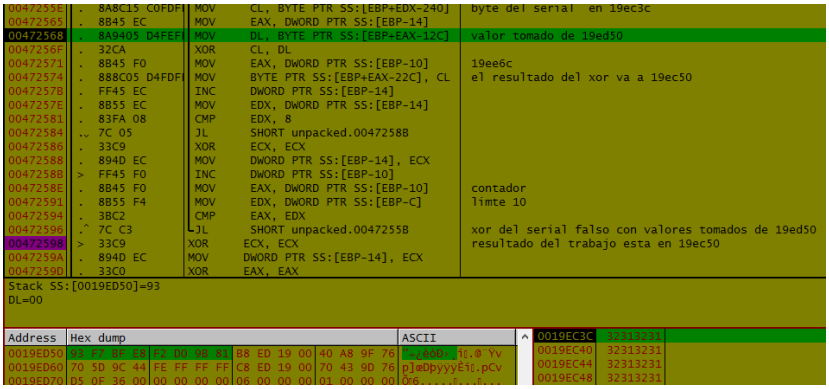
Parte 2 en la dirección 472559

Toma los bytes del serial que pusimos según el contador



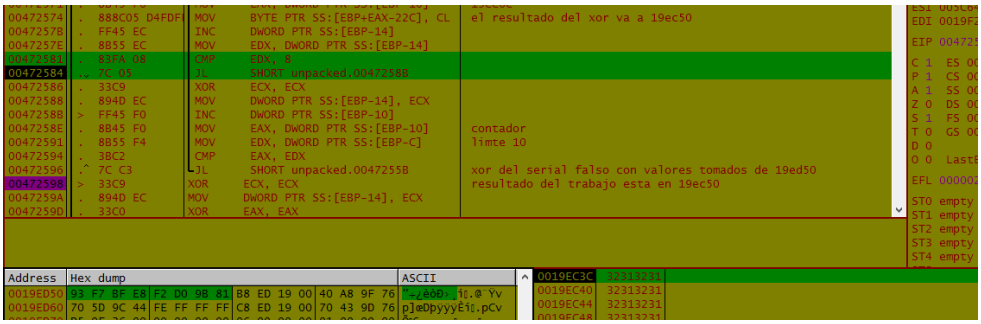
Ahí es donde toma los bytes de la operación anterior luego hace xor entre los dos valores y el resultado lo guarda en: 19ec50 como podemos ver en la imagen

Crackeando ultraiso by Carlos ismael



Para los que no se acuerden, en la primera operación, solo género 8 bytes, las cuales tomo de 1e74fdb9, ok??

Eso quiere decir que no alcanza para hacer xor a todos los valores del serial falso porque nos da un total de 16 bytes, entonces esa instrucción que hemos seleccionado en la imagen reinicia el contador y comienza a tomar los valores desde el principio pero no reinicia el contador que hace que tomemos byte por byte del serial falso, ok??? No se pierdan jejeje



Eso quiere decir que los valores a ser xoreados quedan de esta manera:

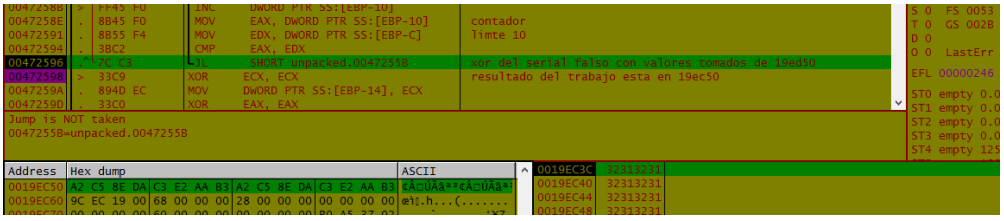
0019EC3C 31 32 31 32 31 32 31 32 31 32 31 32 31 32 31 32 1212121212121212

0019ED50 93 F7 BF E8 F2 D0 9B 81 93 F7 BF E8 F2 D0 9B 81 “÷¿èòÐ›

Para darnos como resultado:

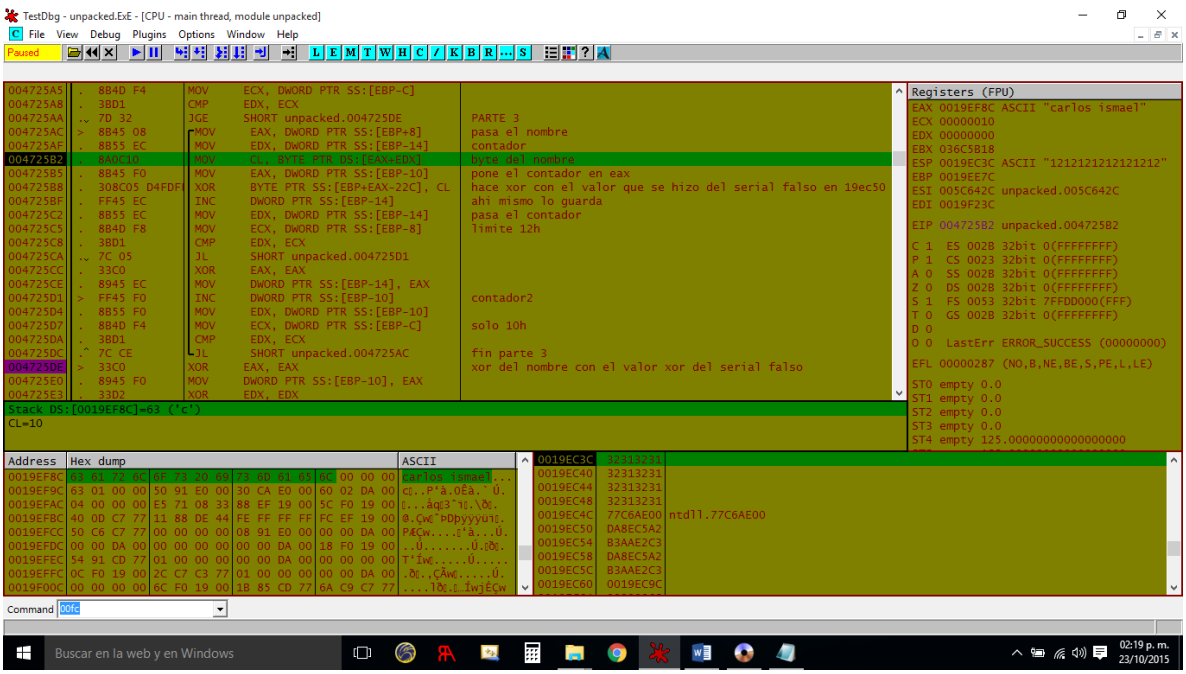
0019EC50 A2 C5 8E DA C3 E2 AA B3 A2 C5 8E DA C3 E2 AA B3 ¢ÅŽÚÃâª³¢ÅŽÚÃâª³

Bueno pues ahí está en la imagen de abajo



Ahora pasamos a la parte 3

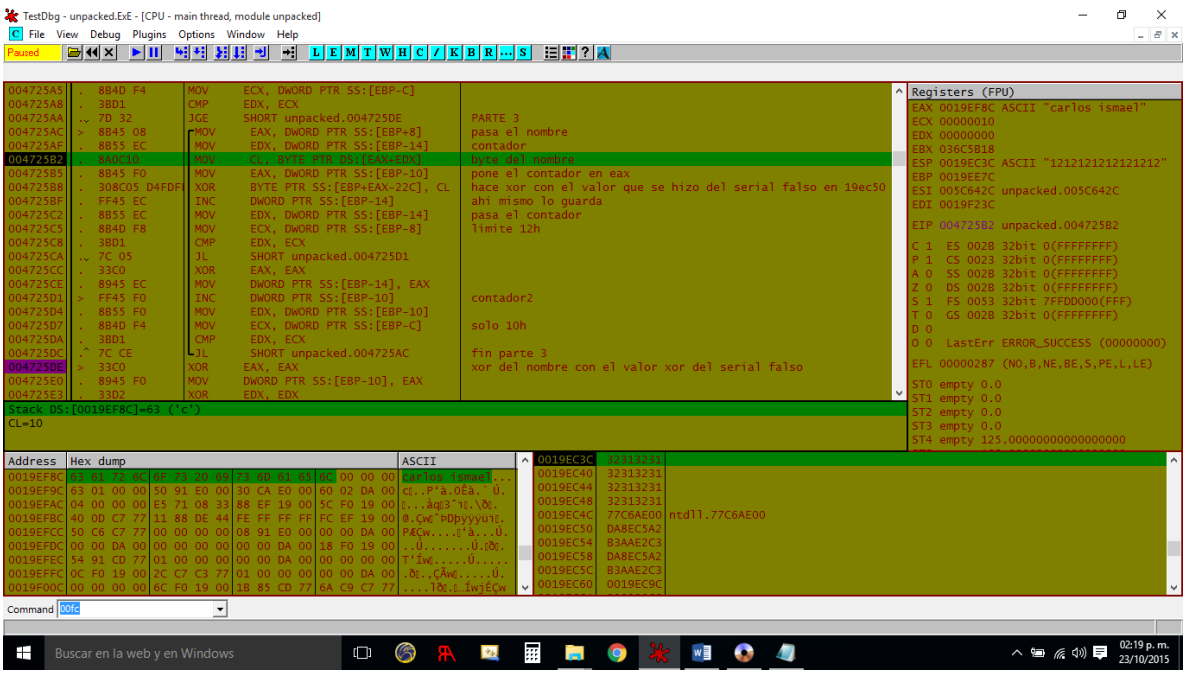
Crackeando ultraiso by Carlos ismael



En la imagen anterior vemos que toma el byte del nombre según el contador y lo pone en cl

Luego vemos que toma el byte de la operación anterior y hace xor byte a byte con el del nombre que introducimos, esta vez no lo cambia de lugar e deja ahí mismo, como podemos ver en la imagen de abajo:

Crackeando ultraiso by Carlos ismael



Esto lo podemos traducir en nuestro keygen como:

0019EF8C 63 61 72 6C 6F 73 20 69 73 6D 61 65 6C Carlos ismael

0019EC50 A2 C5 8E DA C3 E2 AA B3 A2 C5 8E DA C3 E2 AA B3 ¢ÅŽÚÃâª³¢ÅŽÚÃâª³

Como podemos ver nuestro nombre solo tiene 13 caracteres y el valor anterior 16, lo que el programa hace para remediarlo es, con la instrucción que seleccionamos en la imagen de bajo, reinicia el contador y así toma los caracteres desde el principio de nuevo para completar los 16 que necesita.

Esta operación se transforma en

0019EF8C 63 61 72 6C 6F 73 20 69 73 6D 61 65 6C 63 61 72 carlos ismaelcar

0019EC50 A2 C5 8E DA C3 E2 AA B3 A2 C5 8E DA C3 E2 AA B3 ¢ÅŽÚÃâª³¢ÅŽÚÃâª³

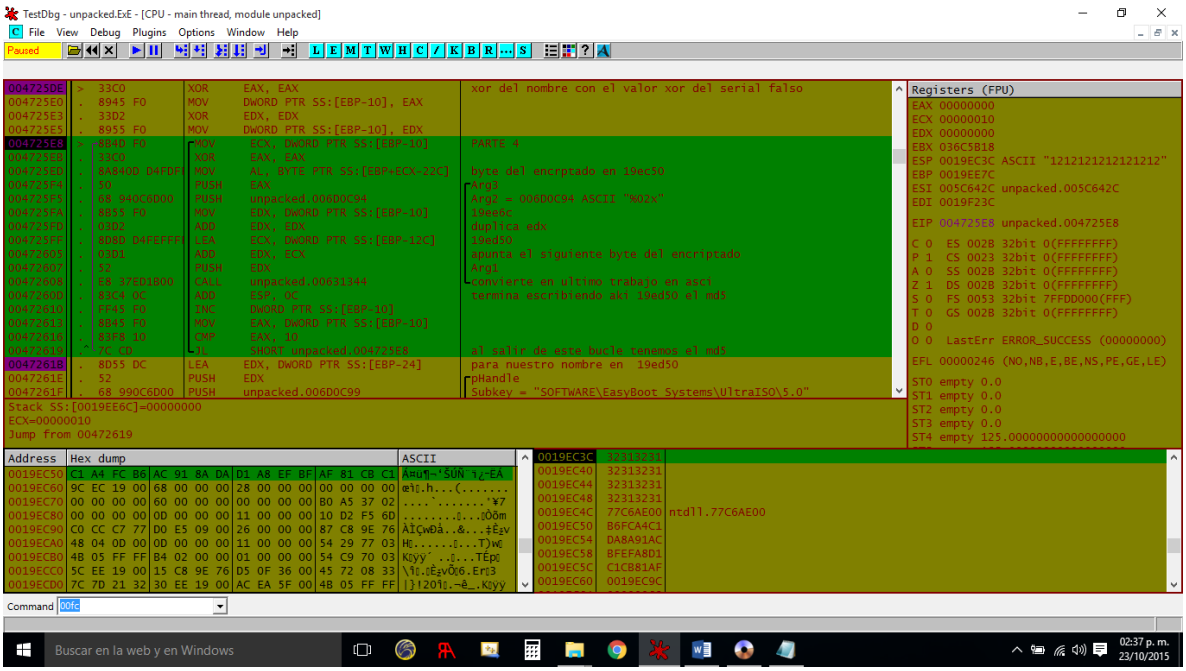
Dando como resultado:

0019EC50 C1 A4 FC B6 AC 91 8A DA D1 A8 EF BF AF 81 CB C1 Á¤ü¶¬'ŠÚÑ¨ï¿¯.Ëâª³

Fecha: 23 de octubre del 2015 Ultra Iso Carlos Ismael Tun Tun

A partir de aquí si se dan cuenta ya tenemos un valor md5 en los valores hexa que vemos son dos valores por cada posición dando un total de 32 valores o caracteres, ahora solo toca pasarlo a ASCII, vamos a ver como lo hace el programa:

Le aviso de una vez que tiene varios calls a lo mejor son para operaciones de comparación o cosas así no estoy seguro ya que me perdí en varios, solo vamos a ver la parte en la que convierte los valores sale? Bueno pues vamos a verlo. Es call de ahí es muy extenso…

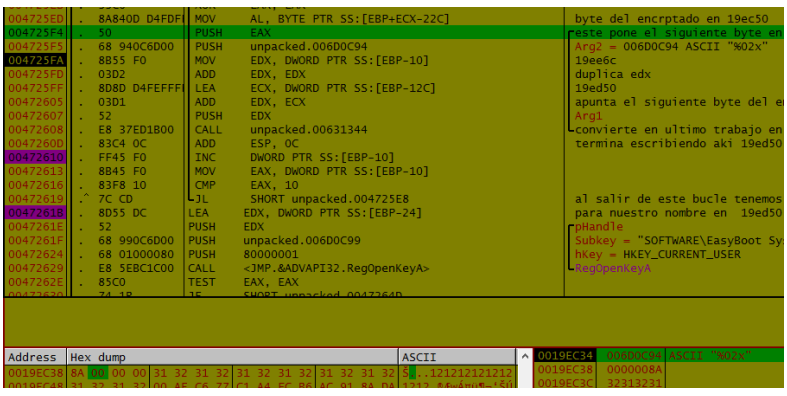


Dentro del call vemos uno mas

00631362 |. E8 D1050000 CALL unpacked.00631938 ; \unpacked.00631938

Vemos que al entrar ahí un montón de instrucciones que quien sabe que hacen pero damos a “step over” o F8 yo les diré donde parar sale???

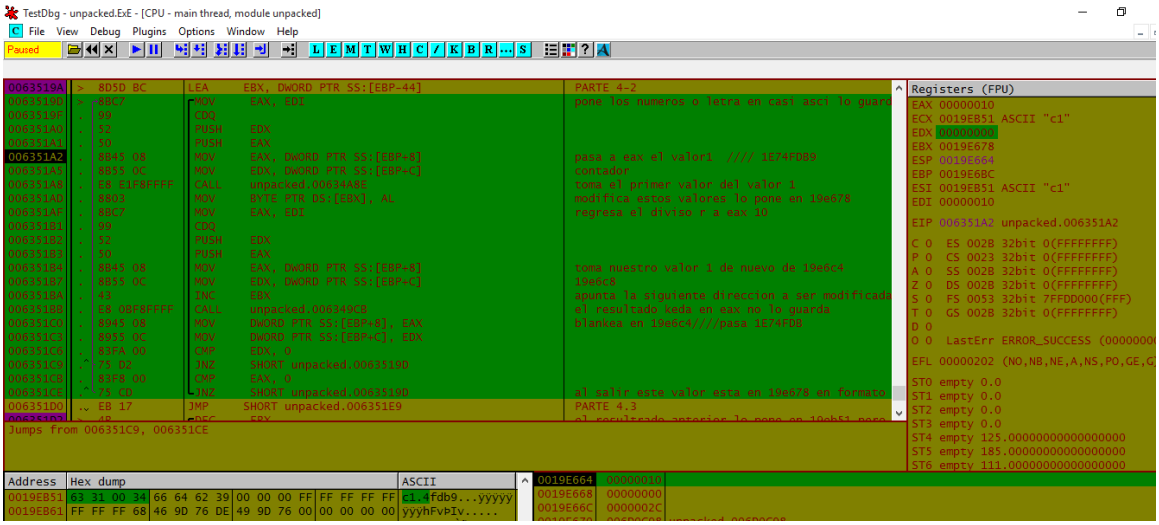
00631A23 |. /FF248D 2A1A63>||JMP DWORD PTR DS:[ECX*4+631A2A] ; a la tercera vuelta de este jmp ya podemos ver lo que hace con el valor, que ya sabes, por supuesto, pero ay que ver como lo hacen ellos.



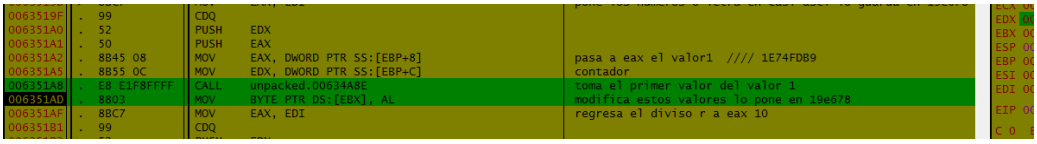
00631D3F |. 8B50 FC |MOV EDX, DWORD PTR DS:[EAX-4] ; toma un byte del serial que está en 19ec38

00631D42 |. 8955 D0 |MOV DWORD PTR SS:[EBP-30], EDX ; lo pasa a 19ebd8 == valor 1

Bueno en la siguiente imagen ya podemos deducir lo que va a hacer



En este call



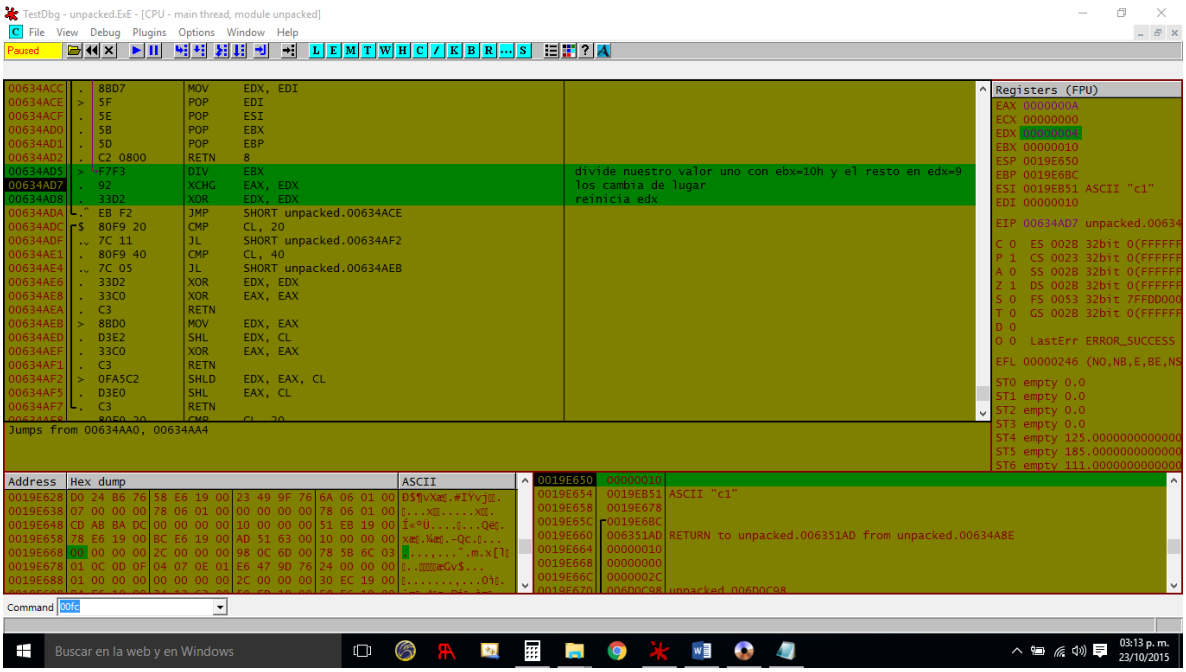
Los convierte a números o letras normales con esta operación

Ej: C1 / 10 ==C resultado 1

Luego en la segunda vuelta lo vuelve a hacer

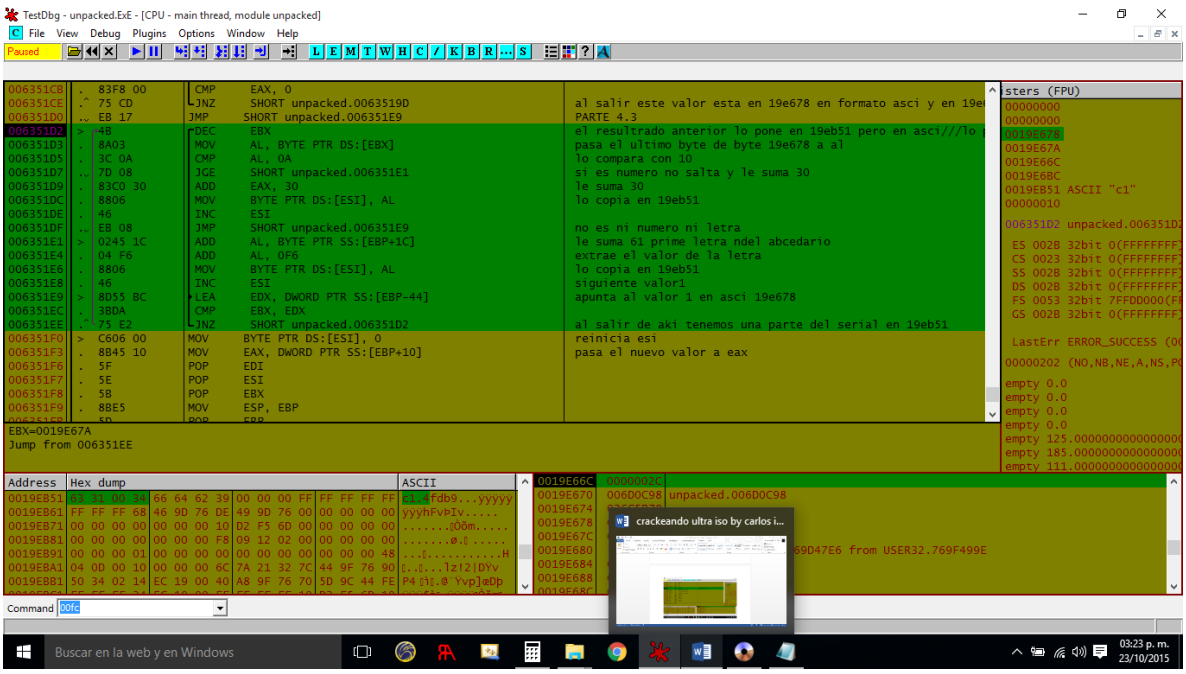
C / 10 = 0 resultado = C

Lo hace dos veces por cada byte y al salir guarda el resultado en:19e678 es un a manera de convertir a ASCII.

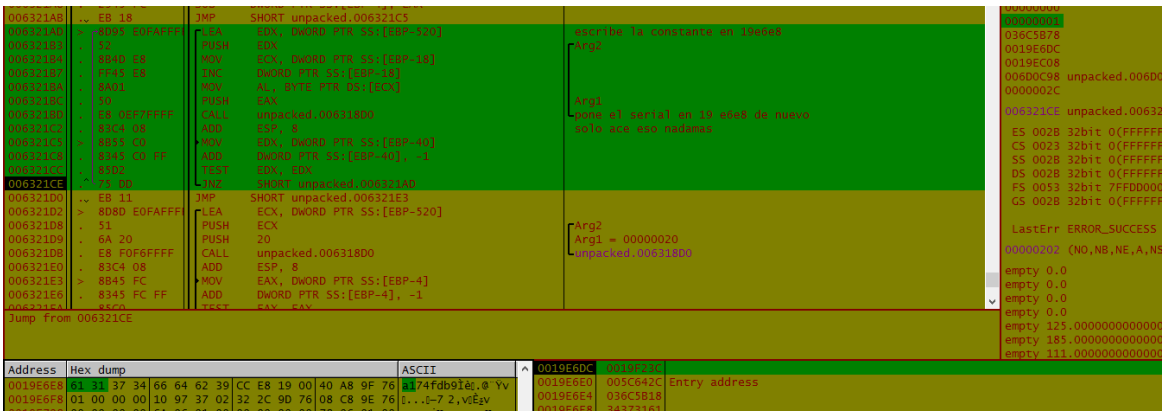


Después con estas instrucciones lo guarda en: 19eb51.

Al salir de aquí también lo deja en minúsculas.



Otro call que lo deja en 19e6e8

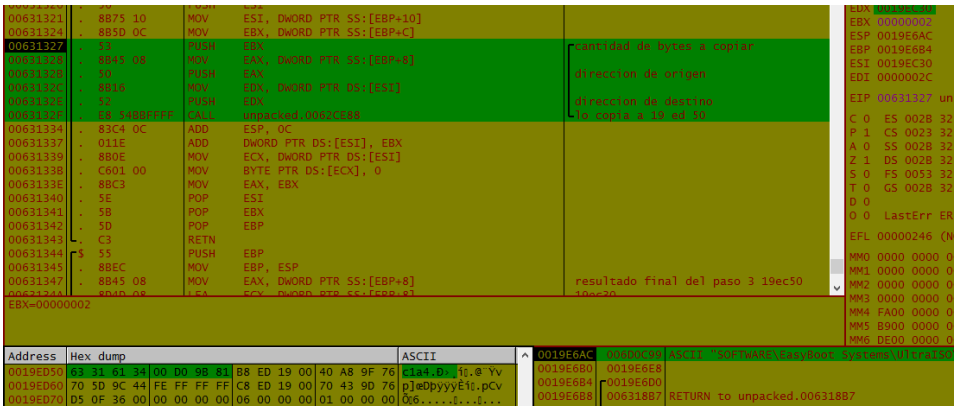


Dentro encontramos esto que es el encargado de copiarlo a esa dirección:

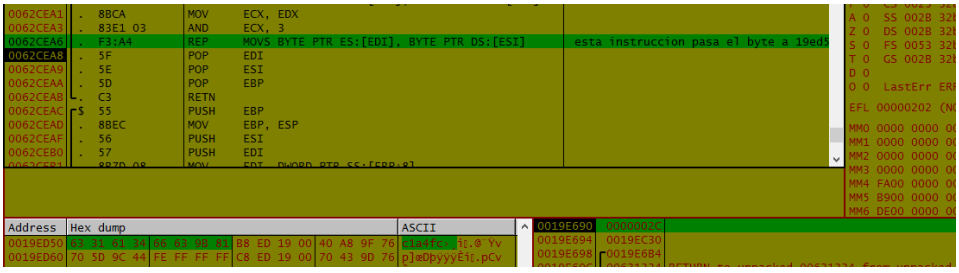
006318F8 |. 88040B MOV BYTE PTR DS:[EBX+ECX], AL

No le veo mucha ciencia.

00632265 |. E8 1EF6FFFF CALL unpacked.00631888 luego con este call lo copia a 19ed50 con la instrucción seleccionada en la imagen. Entremos para ver como lo hace.

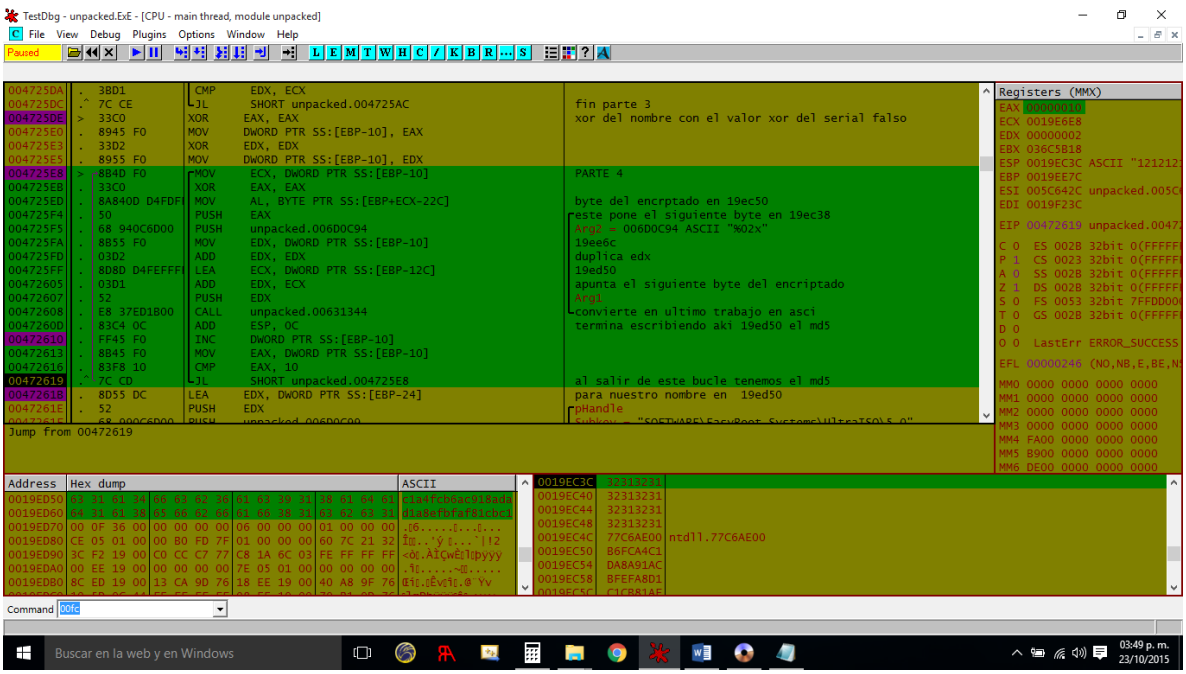


Al pasar ese rep podemos ver que se copió a esta dirección

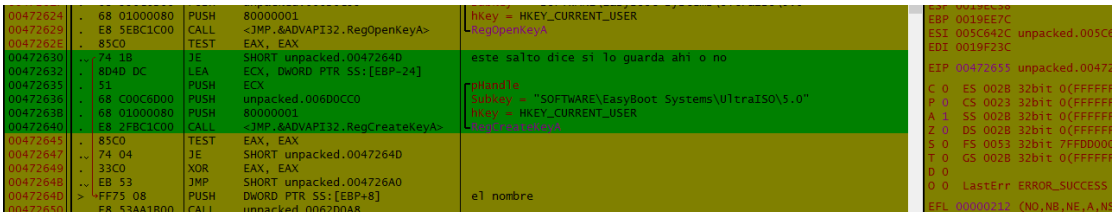


Al salir de ese bucle tenemos el md5 para nuestro nombre en 19ed50.

Crackeando ultraiso by Carlos ismael



Finalmente vemos como es el proceso de registro en este caso lo salto jejeje pero si estuviese todo correcto lo guarda ahí.



Y ya, al parecer es todo lo que este programa hace.

Podemos tomar este md5 y escribirlo en el registro a mano con los parámetros que más abajo podemos ver, uno para el nombre y otro para el registro.

Vamos a hacerlo con un pequeño código el cual es:

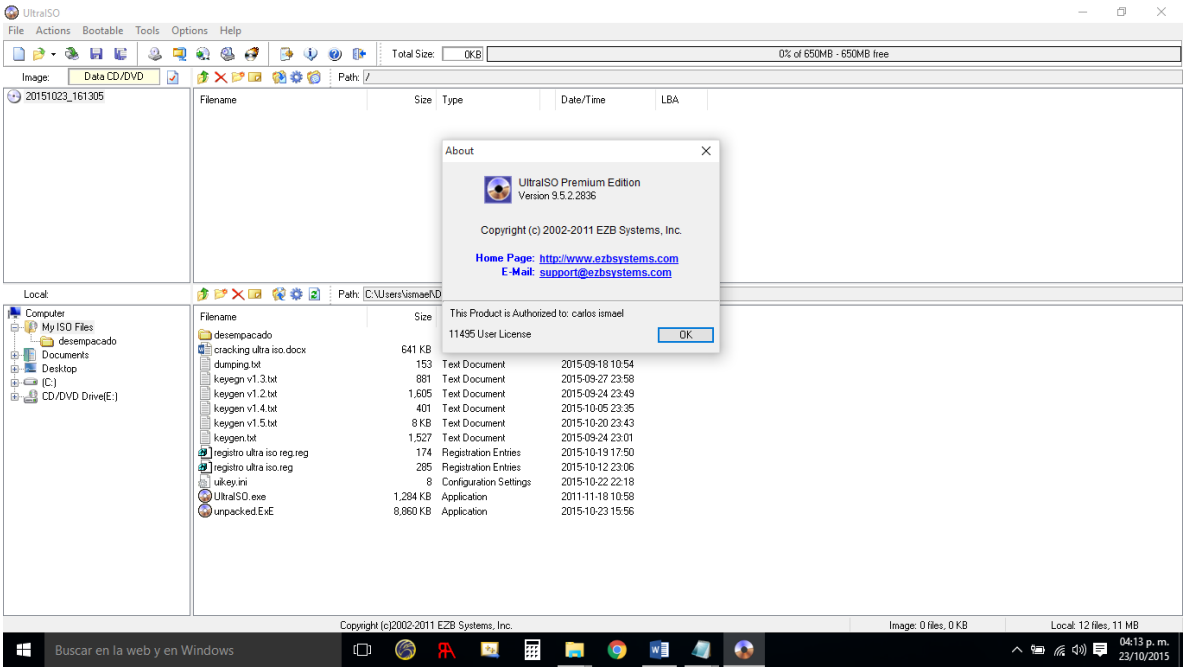
REGEDIT4

[HKEY_CURRENT_USER\SOFTWARE\EasyBoot Systems\UltraISO\5.0]

"UserName"="carlos ismael"

"Registration"="c1a4fcb6ac918adad1a8efbfaf81c8c2"

En el bloc de notas lo guardamos con la extensión .reg lo ejecutamos y ya



Listo es todo por ahora, lo del keygen lo dejo para más adelante ya que ando algo corto de tiempo pero tan pronto lo tenga lo subo a las web, sale???

Por lo pronto diré que es un programa muy bien hecho muchas rutinas como para perderse y nunca salir de nuevo, me imagino que ese es el plan de los programadores, de esto me agarro para decir que si hay algún error ya sea en la escritura o en los códigos de verdad mis disculpas, como humanos que somos tenemos derecho a cometer errores, me salte muchas partes pero así debe ser si no el tutorial no tendría fin, pues en fin cualquier queja comentario o sugerencia no lo duden, más abajo les dejo como contactar y gracias por leer.

Bueno pues por mi parte es todo, un saludo a toda la lista de crackslatinos que sin ellos no hubiera sido posible para mi llegar hasta aquí, gracias por leer el tutorial y practicarlo, y un saludo muy especial a los grandes maestros: Ricardo narvaja, invision, indulgeo, nox y muchos más que gracias a ellos soy capaz de hacer este tipo de cosas, aunque no los conozco en persona sé que están ahí y nos siguen apoyando como grandes personas que son.