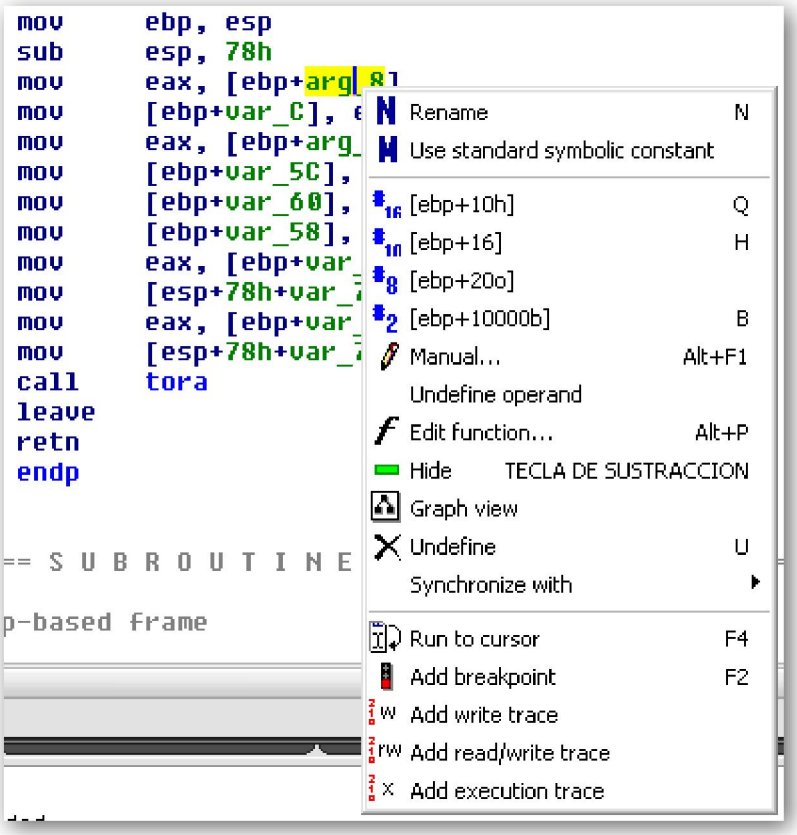
6.1.—Nombres y nombramiento

Si recordamos, hasta ahora hemos encontrado dos categorías de nombres en los desensamblados de IDA; los nombres asociados con direcciones virtuales, ubicaciones nombradas, y nombres asociados con las variables del stack frame. En la mayoría de los casos IDA generará automáticamente todos estos nombres siguiendo las directrices que anteriormente ya explicamos. A los nombres generados automáticamente IDA se refiere a ellos como **dummy names**.

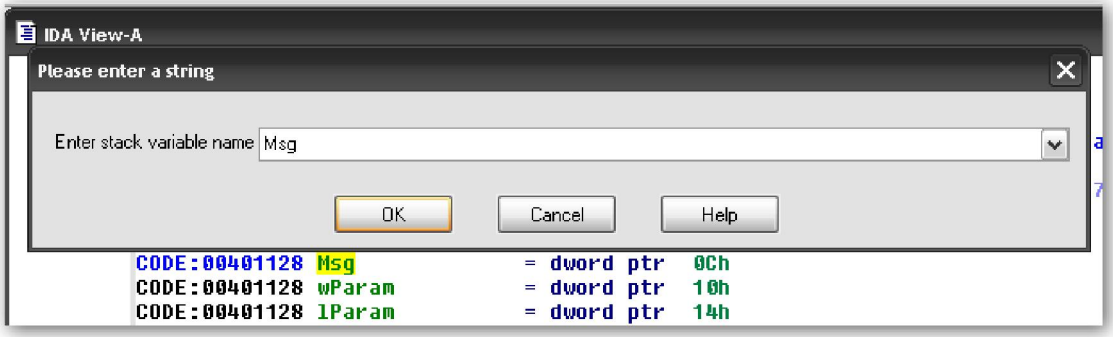
Por desgracia, estos nombres rara vez indican el propósito propuesto de una ubicación o variable y por consiguiente no nos aumenta la comprensión del comportamiento de un programa. Cuando empecemos a analizar un programa, lo primero y más normal a realizar, será manipular el listado de desensamblado cambiando los nombres implícitos por otros nombres más significativos. Por fortuna, IDA nos permite cambiar fácilmente cualquier nombre y se encarga de propagar dicho cambio de nombre a lo largo de todo el desensamblado. En la mayoría de los casos, cambiar un nombre es tan fácil como hacer click sobre el nombre que deseamos cambiar, este hecho realza el nombre, y utilizar el atajo **N**, estas acciones abrirán un diálogo para cambiar el nombre. Otra alternativa es hacer click derecho en el nombre a cambiar presentándonos un menú de contexto en el cual existe la opción **Rename**, figura abajo. El proceso para cambiar el nombre difiere entre hacerlo para variables de pila o nombrado de ubicaciones, dichas diferencias las detallaremos en los siguientes párrafos.



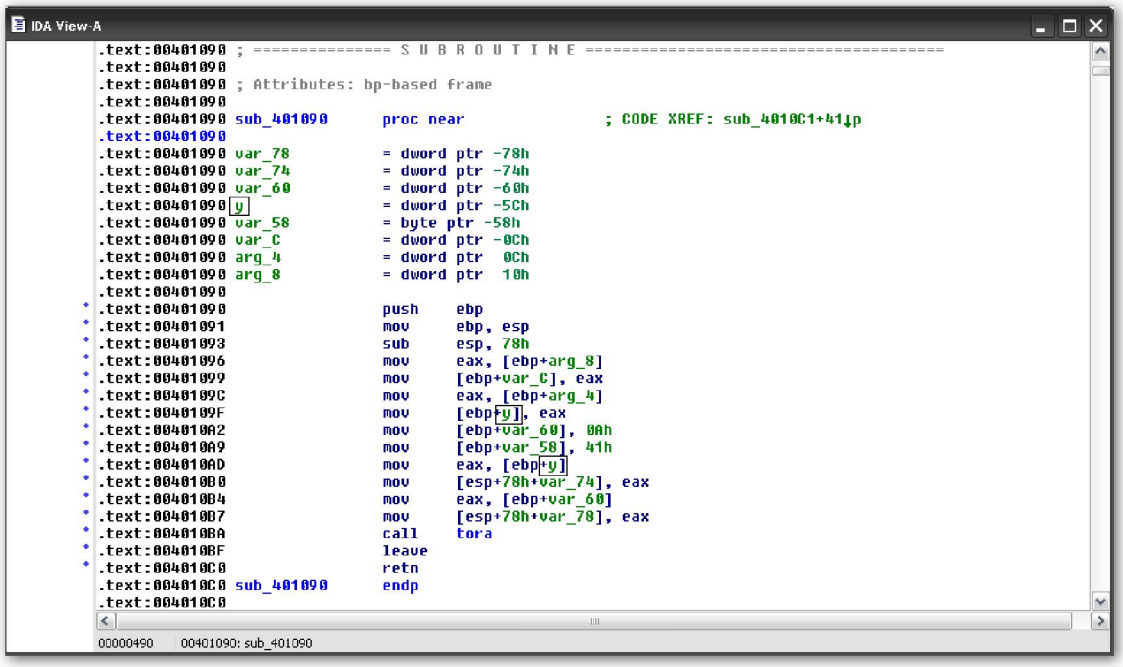
6.1.1.—Parámetros y locales variables

Los nombres asociados con variables de pila son las formas de nombres más simples del listado del desensamblado, principalmente porque no están asociados con ninguna dirección virtual específica y de esta forma nunca aparecerán en la ventana **Names**.

Como en la mayoría de lenguajes de programación, dichos nombres se consideran con un alcance limitado sólo dentro de la función por lo cual sólo pertenecen a un stack frame dado. Así, cada función de un programa podría tener su propia variable de pila nombrada como **arg_0**, pero ninguna función puede tener más de una variable llamada **arg_0**. El diálogo siguiente es utilizado para renombrar una variable de pila.



Una vez el nombre se ha cambiado, IDA cambia cualquier coincidencia del nombre antiguo dentro del contexto de la función actual. Vamos a realizar un cambio al ejemplo **demo_stackframe** cambiaremos el nombre de la variable **var_5C** por el nombre **y** veamos el resultado del nuevo listado con este cambio.

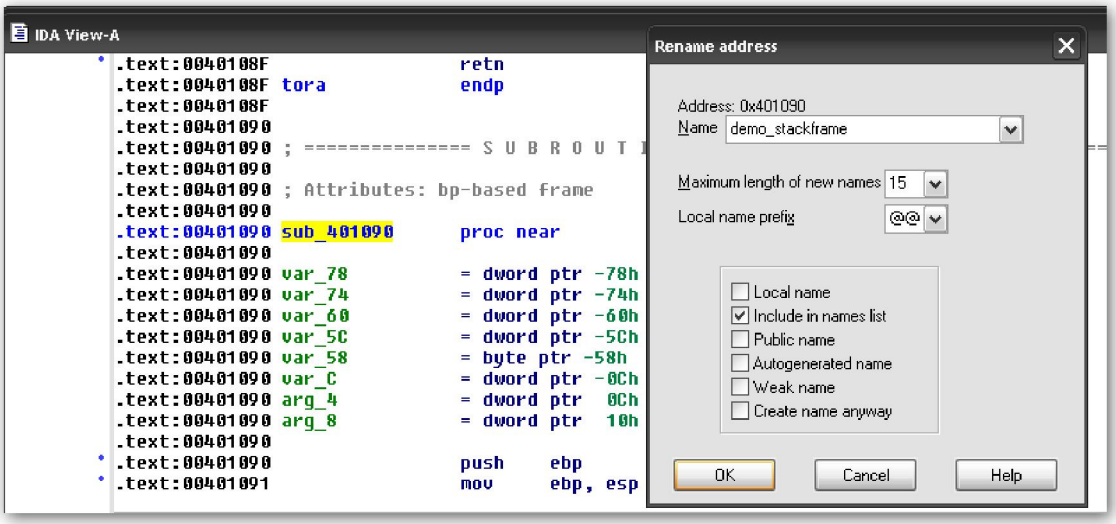


Fíjate en los rectángulos, figura arriba, se ha renombrado la variable en toda la función. Esta acción es reversible, si en alguna ocasión quisieras volver al nombre implícito de una variable, abre el diálogo de cambio de nombre de nuevo e introduce un nombre en blanco, al aceptar IDA regenerará el nombre implícito.

6.1.2.—Ubicaciones con nombre

Para renombrar una ubicación nombrada o añadir un nombre a una ubicación sin nombre es ligeramente distinto al cambio de nombre de una variable de pila. El proceso

para acceder al diálogo de cambio de nombre es idéntico, atajo **N**, pero la vista cambia, la figura abajo, muestra el diálogo asociado con el nombramiento de una ubicación.



Este diálogo nos informa exactamente qué dirección será nombrada juntamente con una lista de atributos que puedes asociar al nombre. La longitud máxima del nombre, ahora **15**, viene dado por un valor existente en el archivo de configuración de IDA, **Archivos de Programa\IDA\cfg\ida.cfg**. Puedes usar nombres más largos si cambias el valor del **ida.cfg**, si no es así se te informará que has superado la longitud establecida. Cualquier base de datos que abras siempre utilizará el valor establecido en **ida.cfg**.

Los siguientes atributos del diálogo pueden asociarse al nombrar una ubicación:

Local name
Si seleccionamos **local name** restringimos su vista sólo a la función actual, con lo cual se impone que sea único dentro de una función. Ya sabemos que como variables locales, dos funciones distintas pueden tener nombres locales idénticos, pero una única función no puede tener dos nombres locales idénticos. Las ubicaciones nombradas existentes fuera de los límites de la función, no pueden designarse como **local name**. Estas son los nombres que representan nombres de función y también las variables globales. La utilización de dicha opción, **Local name**, es proporcionar nombres simbólicos a los objetivos de los saltos dentro de una función, así como a las estructuras de desviación del control de flujo.

Include in names list
Seleccionar esta acción causa que el nombre sea añadido a la ventana **Names**, con lo cual nos será fácil encontrarlo cuando queramos retomarlo. Los nombres autogenerados (**dummy**) por defecto nunca se incluyen en la ventana **Names**.

Autogenerated name
Este atributo parece no tener ningún efecto en los desensamblados. Seleccionarlo causa que IDA no genere automáticamente dicho nombre.

Weak name
Un símbolo "**weak**" es un símbolo público especial que se utiliza cuando no se encuentra ningún nombre igual supeditado a él. Marcar un símbolo como weak tiene relevancia para el ensamblador pero casi ninguna para un ensamblado de IDA.

Create name anyway
Como ya hemos dicho previamente, no pueden existir dos ubicaciones con el mismo nombre en una función. Similarmente, dos ubicaciones fuera de cualquier función, con alcance global, no pueden tomar el mismo nombre. Esta opción puede confundir, ya que se comporta de formas distintas dependiendo del tipo de nombre que intentas crear.

Si estás editando un nombre de alcance global, como un nombre de función o una variable global, e intentaste asignarle un nombre que ya se usa en la base de datos, IDA nos muestra un diálogo de nombre contradictorio, figura abajo, ofreciéndonos generar de forma automática un sufijo numérico único para resolver dicho conflicto. Este diálogo se muestra aunque no hayas seleccionado la opción Create name anyway.

6.1.3.—Nombres de registro
Un tercer tipo de nombre, que a menudo se descuida, es el nombre de registro. Dentro de los límites de una función, IDA permite que los registros se renombren. Renombrar un registro puede ser útil cuando un compilador ha elegido colocar una variable en un registro antes que en la pila del programa, y que tú desees referirte a la variable con otro nombre que no sea EDX, por ejemplo. El renombrado de registros se realiza como el renombrado de ubicaciones. Utiliza el atajo **N**, o click derecho al nombre del registro y selecciona **Rename** para abrir el diálogo de renombrado. Cuando renombramos un registro, lo que hacemos es darle un alias al registro mientras que la función actual no finalice su tarea. IDA denota este alias con la sintaxis **alias = register** al inicio de la función, con lo cual tiene el cuidado de reemplazarlo en todos los casos del registro. No es posible renombrar un registro utilizado en el código que no pertenezca a una función.