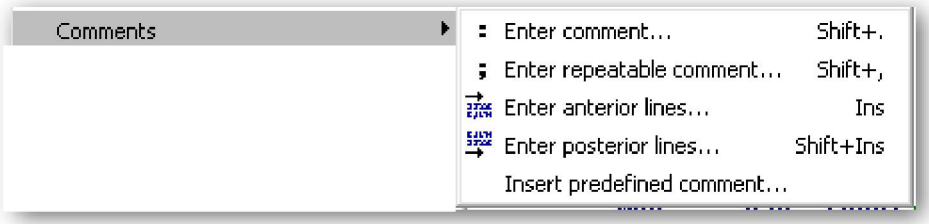
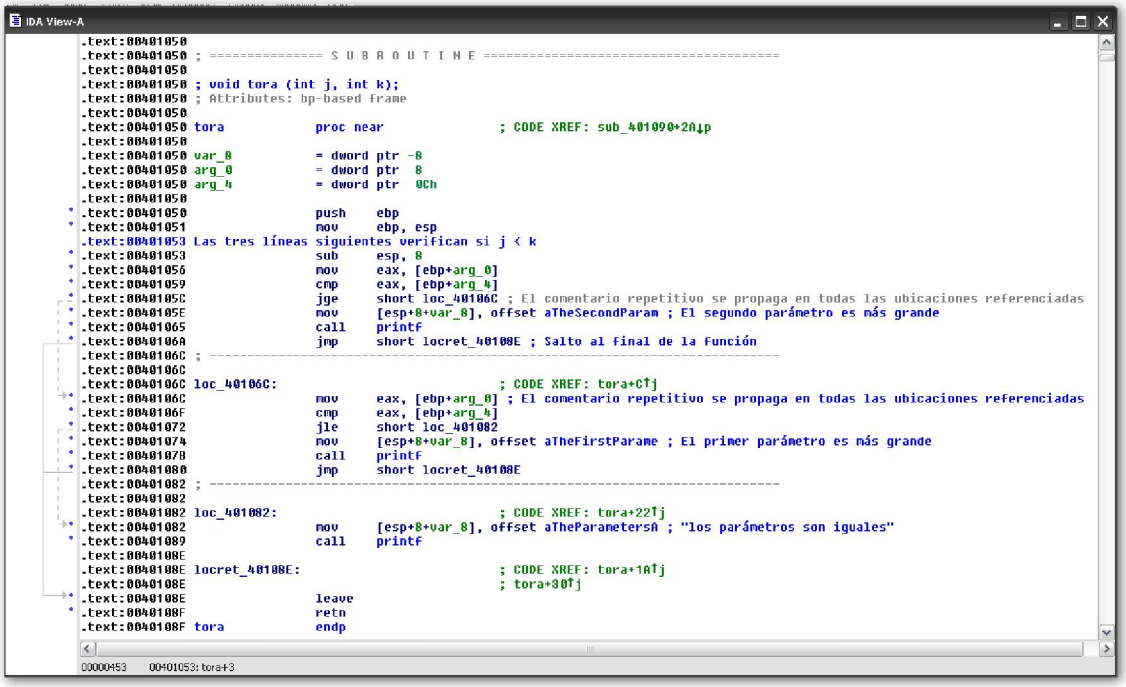
6.2.—Realizar comentarios en IDA

Otra característica de IDA es la habilidad de poder adjuntar comentarios nuestros en la base de datos. Estos comentarios son particularmente provechosos ya que podemos ir incluyendo apuntes o notas para ir viendo nuestro progreso en el análisis del programa. Particularmente son perfectos para describir secuencias de instrucciones en lenguaje ensamblador como si fuera un lenguaje de alto nivel. Por ejemplo, podemos optar por escribir comentarios como los que se usan en las declaraciones de lenguaje C para resumir el comportamiento particular de una función. En el análisis posterior de la función, dichos comentarios nos servirán para refrescarnos la memoria al reanalizar dichas declaraciones en lenguaje ensamblador.

IDA nos proporciona varios estilos distintos de comentarios, cada uno para propósitos distintos. Los comentarios pueden asociarse con cualquier línea del listado del desensamblado utilizando las opciones disponibles cuando realizamos la acción **Edit > Comments**. Figura abajo.



Los atajos y los menús contextuales nos ofrecen alternativas en las características de los comentarios de IDA. Para entender dichas características de los comentarios, realizaremos unas prácticas con el siguiente listado de desensamblado de la función **tora**:



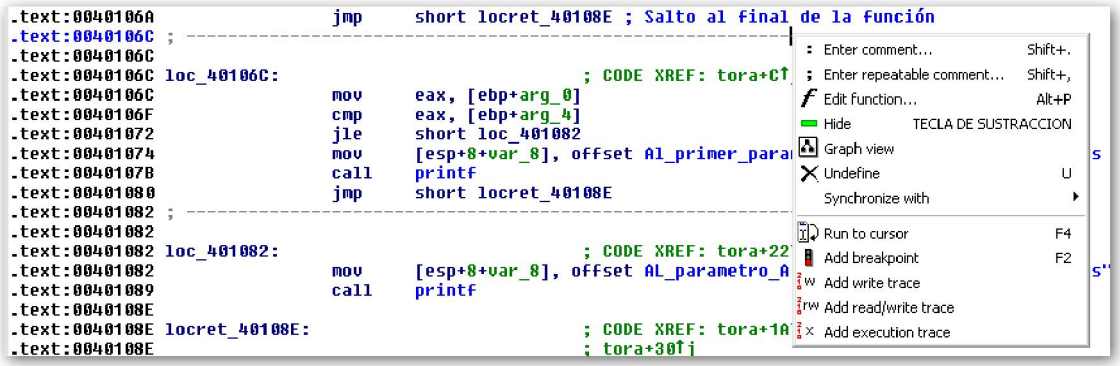
La mayoría de comentarios de IDA, contienen como prefijo un punto y coma con lo cual se indica que la línea se tiene que considerarse como un comentario. Como

podemos observar es similar a los estilos de comentario utilizados por algunos ensambladores o parecido al estilo de comentarios # en algunos lenguajes o el estilo // en C++.

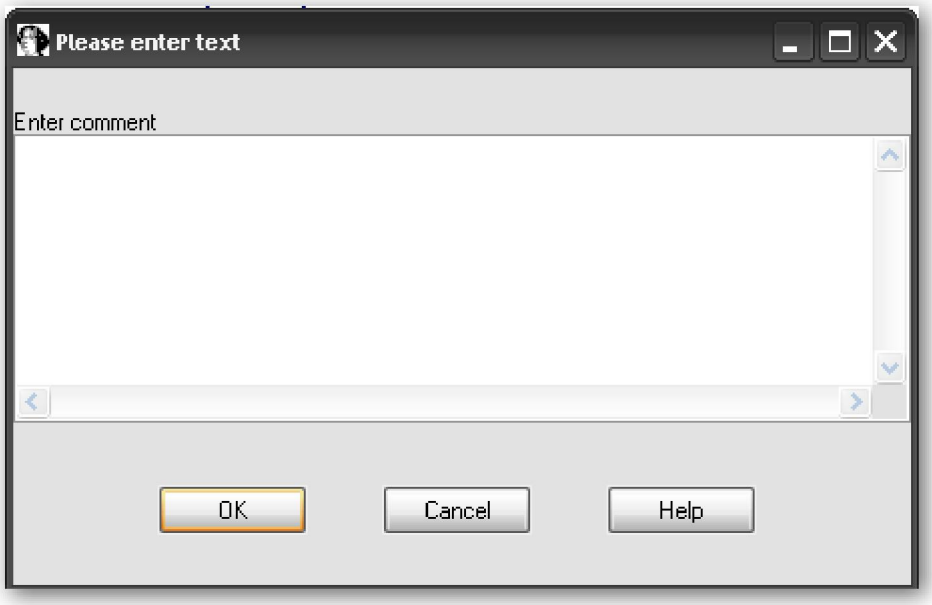
6.2.1.—Comentarios corrientes

El comentario más directo es el llamado **regular comment**. Dichos comentarios son colocados al final de la línea del desensamblado escogida, veamos la línea

Para realizarlo, click derecho en el margen derecho del desensamblado y aparecerá el siguiente diálogo para escoger



o utilizando el atajo (**:**), con lo cual activaremos el diálogo directamente para introducir el comentario que deseemos



Los comentarios corrientes pueden tener varias líneas, siempre y cuando lo realices en el momento de crear el comentario. Cada una de las líneas será sangrada para alinearlas a la derecha del desensamblado. Para editar o borrar un comentario, deberás reabrir el diálogo de comentarios y editar o borrar todo el texto del comentario apropiadamente. Por defecto los comentarios corrientes se muestran en texto azul.

El mismo IDA durante la fase de análisis inserta variados comentarios corrientes, para describir parámetros que serán pasados en las llamadas a funciones. Eso sí, sólo ocurre cuando IDA dispone del nombre del parámetro o del tipo de información de la función llamada. Esta información normalmente está contenida en las librerías tipo, de las cuales hablaremos más adelante.

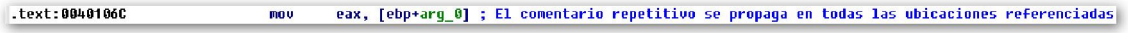
7.2.2.—Comentarios repetitivos

Un **repeatable comment** es aquel comentario que se introduce una vez pero aparece automáticamente en distintas ubicaciones a lo largo del desensamblado. La línea siguiente muestra un comentario repetitivo

Como podéis ver en el listado de desensamblado también se muestra en color azul, no pudiéndolo distinguir del comentario corriente. La diferencia está en su comportamiento, éste está unido al concepto de referencia cruzada. Cuando una ubicación de un programa referencia a una segunda ubicación, si contiene un comentario repetitivo el comentario se asocia a la segunda ubicación replicando a la primera ubicación. Por defecto el comentario replicado aparecerá en texto gris, de esa forma el comentario repetitivo se distinguirá de otros comentarios. El atajo para el comentario repetitivo es (**;**), lo cual es fácil confundirnos con el corriente y el repetitivo.

En el listado de la función **tora**, observa que el comentario de la línea

es idéntico al comentario de esta otra línea



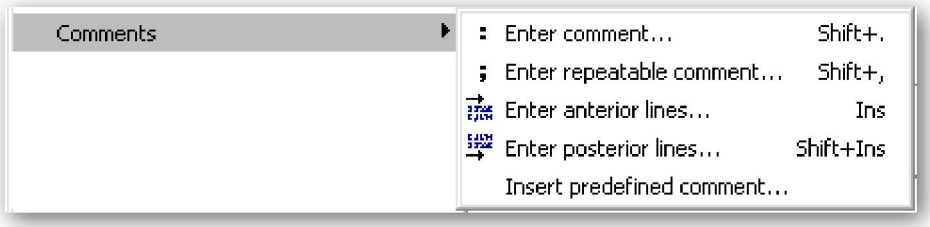
Esto es así, porque la instrucción, **jge short loc_40106C** referencia a la dirección **0040106cC.**

Si añadimos un comentario corriente en la ubicación donde se muestra el comentario repetitivo éste sobrescribe al repetitivo prevaleciendo solamente el corriente. Por lo tanto si borrásemos el comentario repetitivo de la línea **0040106C** el comentario repetitivo referenciado no se mostrará, pero si borrásemos otra vez el corriente el repetitivo se volvería a mostrar.

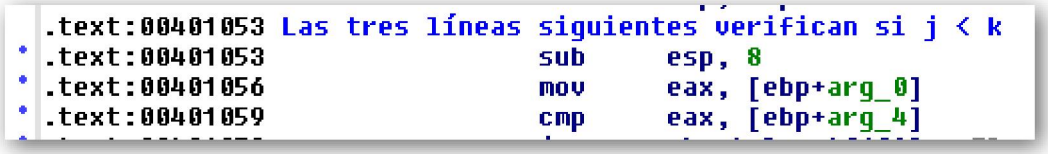
Una variante del comentario repetitivo está asociada con las **strings**. Cuando IDA crea automáticamente una variable **string**, se añade en la ubicación de la variable un comentario repetitivo virtual. Decimos virtual porque el comentario no se puede editar por el usuario. El contenido del comentario virtual se coloca donde esté la variable y se muestra a lo largo del listado como un comentario repetitivo. Como consecuencia, cualquier ubicación del programa que se refiera a la variable **string** mostrará el contenido de la variable como un comentario repetitivo. Los tres comentarios de las líneas siguientes muestran los comentarios referenciados a variables string.

6.2.3.—Comentario de línea anterior y posterior

Estos comentarios aparecen en la línea anterior o posterior de una línea de desensamblado en concreto. Estos comentarios no llevan el prefijo (**;**). Estos los podemos insertar haciendo la acción siguiente **Edit > Comments**, ver figura abajo.



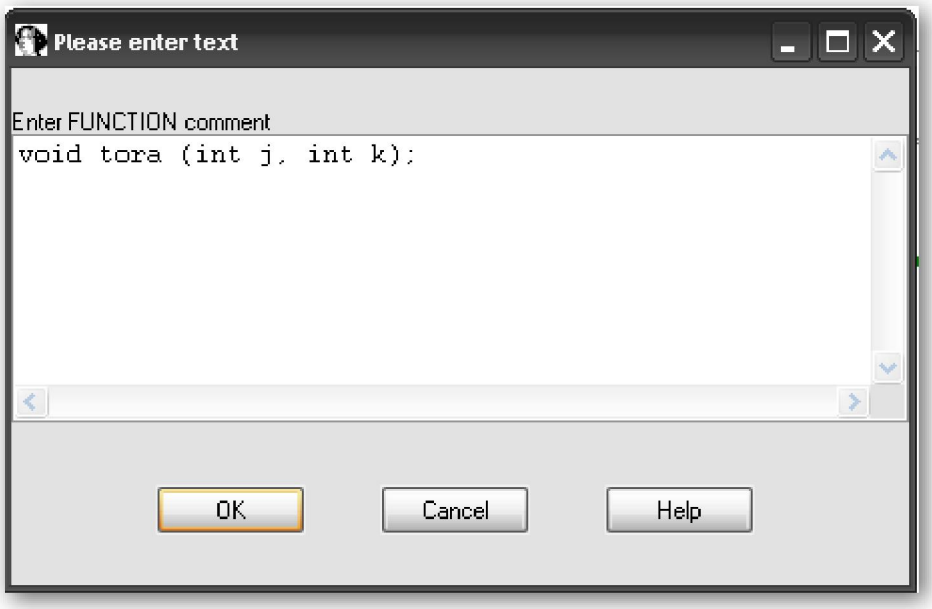
Y un ejemplo



6.2.4.—Comentarios de función

Los comentarios de función permiten agrupar comentarios que se muestran en el listado de desensamblado al inicio de una función. Un ejemplo es el siguiente, en el cual toda la función es redactada.

Para introducir los comentarios de función primero resaltas la función, al inicio de esta, en el listado de desensamblado y luego añades un comentario corriente o repetitivo. Si lo realizas repetitivo se mostrará en cualquier ubicación donde se llame a la función.



Performance Bigundill@