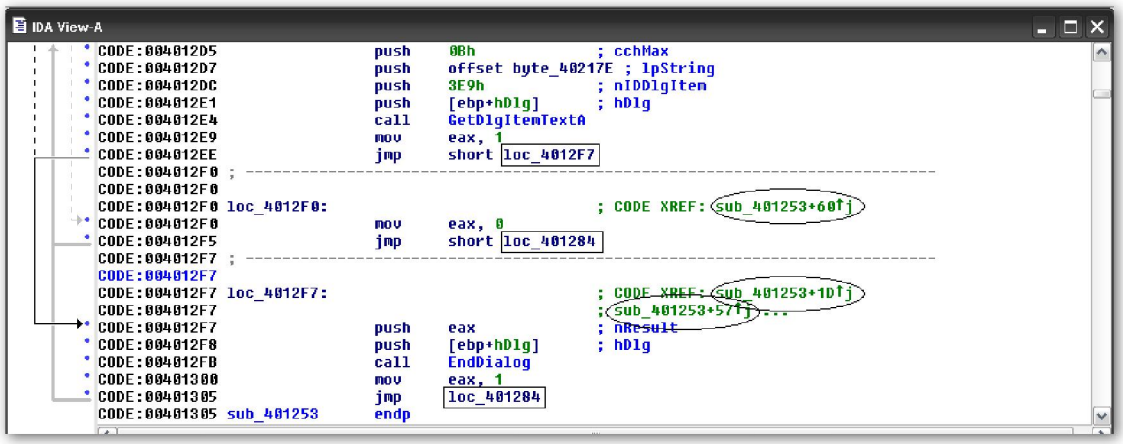
5.1.—Navegación básica de IDA

Vamos a iniciar nuestra experiencia con IDA, para empezar utilizaremos las características que nos ofrece para navegar. Además de proporcionarnos unas características de búsqueda como las que se utilizan en los editores de texto o procesadores de texto, IDA desarrolla una vista de listado de referencias cruzadas fácilmente comprensibles parecidas a los hipervínculos de una página web. El resultado de ambas características, en la mayoría de los casos, es poder posicionarte en las ubicaciones que nos interesen con no más de un doble click.

5.1.1.—Navegación con doble click.

Cuando un programa se ha desensamblado, cualquier ubicación del programa tiene asignada una dirección virtual. Esto da como resultado, el poder navegar a cualquier lugar del programa proporcionando la dirección virtual de la ubicación que nos interesa visitar. Desgraciadamente para nosotros, retener un catálogo de direcciones en nuestra cabeza no es una tarea fácil. Este hecho motivó a los primeros programadores asignar nombres simbólicos a las ubicaciones del programa las cuales se pueden referenciar, para hacernos las cosas más fáciles. La asignación de nombres simbólicos a las direcciones del programa no es distinta que la asignación de nombres de instrucciones **mnemonic** a los **opcode** del programa; con eso los programas se volvían fáciles de leer y escribir haciéndolos fáciles de recordar.

Como ya apuntamos anteriormente, durante la fase de análisis, IDA genera nombres simbólicos examinando la tabla de símbolos o automáticamente basando el nombre en como está referenciada una ubicación en el binario. Además del propósito simbólico, cualquier nombre mostrado en la ventana de desensamblado es un potencial objetivo de navegación al igual que un hiperenlace en una página web. La única diferencia entre estos nombres y los hiperenlaces es que no están resaltados indicándonos que nos trasladará a ellos y que es necesario realizar un doble click para trasladarnos. Hemos visto también la utilización de nombres en distintas ventanas como **Names**, **Imports**, **Exports** y **Functions**. Rellamar a cualquier elemento en dichas ventanas haciendo doble click, nos trasladaba a la vista de desensamblado en la ubicación referenciada. En la figura abajo, cada símbolo enmarcado con un rectángulo representa un objetivo de navegación nombrado, haciendo doble click en cualquiera de ellos nos proporciona la recolocación de la vista de desensamblado en la ubicación seleccionada.



Además para propósitos de navegación, IDA utiliza dos entidades visuales más como objetivo de navegación. La primera son las **referencias cruzadas (XREF)**, en la figura arriba encerradas en elipses, se tratan como objetivos de navegación. Las referencias cruzadas normalmente están formadas por un nombre y un Offset hexadecimal. La referencia cruzada **sub_401253+60**, figura arriba, se refiere a la ubicación anterior, **60 en hexa o 96 en decimal**, bytes anteriores a la ubicación **00401253**. Por lo tanto en este caso si hiciéramos doble click en ella seríamos trasladados a la ubicación referenciada por **004012B3**, ya que **401253 + 60 = 4012B3**. Como ya hemos dicho anteriormente las referencias cruzada las trataremos más adelante.

El segundo tipo de entidad visual tiene un trato especial en cuanto que utiliza valores hexadecimales. Si se nos muestra un valor hexadecimal, el cual represente a una dirección virtual válida del binario, ejemplo **4037B0h**, cuando hagamos doble click en él la vista del desensamblado se reposicionará en dicho valor. Si por el contrario son valores hexa tipo **0Ah, 4, etc** no realizarán ninguna acción de navegación.

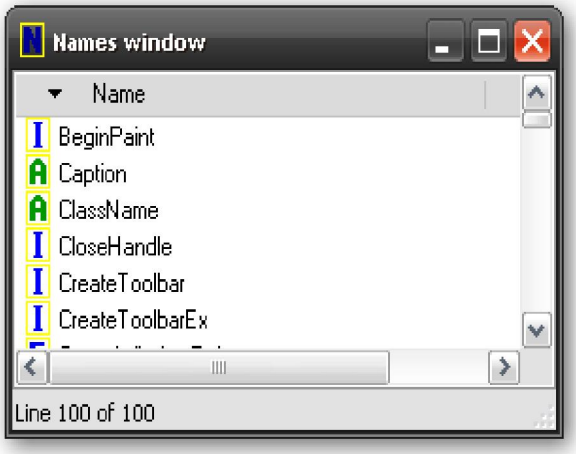
Para finalizar lo concerniente a la navegación con doble click diremos que en la ventana mensajes, cuando aparezca un objetivo de navegación como los descritos previamente y que aparezca como primer elemento del mensaje, si hacemos doble click en él, nos trasladaremos a la ubicación que el mensaje tenga como objetivo.

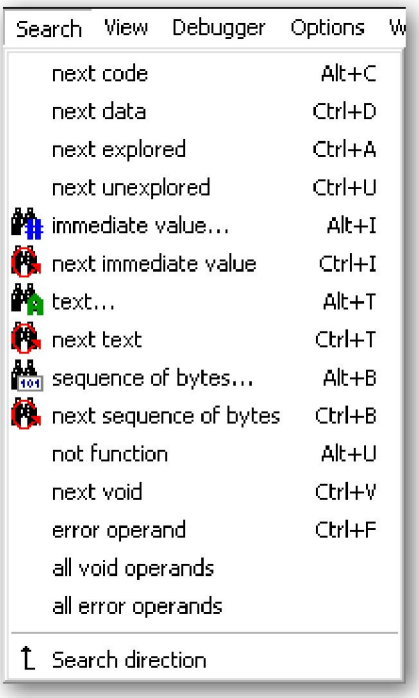
```
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
40134e is an interesting location
Testing: 40134e
loc_4013B7
Testing: loc_4013B7
```

En el ejemplo anterior tenemos dos mensajes, para navegar tendríamos que utilizar el inicio de cada mensaje. Uno nos trasladaría a la ubicación **0040134E** y el otro a **004013B7**, todas las demás líneas del mensaje no nos darían ninguna acción.

5.1.2.—Saltar a una dirección

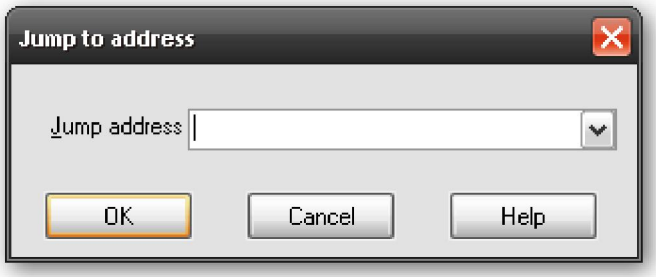
En ocasiones, sabrás exactamente a qué dirección quieres desplazarte, sin embargo no tendrás ningún nombre para hacer doble click y trasladarte a dicha dirección, en la ventana de desensamblado. Llegado este caso tenemos varias opciones. La primera y la más sencilla es desplazarte por la pantalla de desensamblado hasta llegar a la dirección deseada. Esto es factible cuando la dirección conocida es, linealmente posible, acceder a ella. Si lo único que sabemos es una ubicación nombrada, por ejemplo una subrutina llamada "**torabar**", esta primera opción es de pitonisa. Llegado a este punto lo que podríamos hacer es abrir la ventana **Names** y clasificarla por órden alfabético buscando el nombre en cuestión, y hacer doble click en el nombre. Si haces click en la barra que pone **Name**, de la ventana **Names**, los nombres se clasificarán alfabéticamente. Figura abajo izquierda.





La tercera opción es utilizar una característica de búsqueda que tiene IDA, realizando la acción en menú **Search**, donde podrás especificar ciertos criterios de búsqueda antes de ejecutarla. Figura arriba. En el caso de buscar una ubicación conocida, dichos criterios te los puedes ahorrar.

Finalmente, la forma más fácil para llegar a una ubicación del desensamblado conocida, es utilizar el diálogo de salto a una dirección, ver figura abajo. A este diálogo se accede



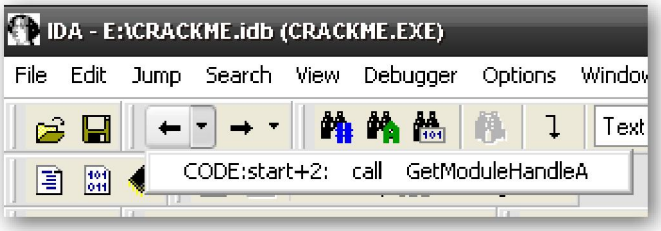
Realizando la acción **Jump > Jump to Adress** o utilizando el atajo **G** cuando la ventana del desensamblado está activa. Desplazarse a cualquier ubicación del binario es tan simple como especificar la **dirección, nombre** o **valor hexa** deseado y hacer click en **OK**, inmediatamente se te mostrará la ubicación deseada. Los valores introducidos en el diálogo serán recordados con lo cual podrás escogerlo de la lista. Esta lista historial te hará más fácil volver a las peticiones anteriores.

5.1.3.—Historial de navegación

Podemos comparar la navegación con IDA por las funciones, con la navegación de un web browser, podemos decir que los nombres y las direcciones son similares a los hiperenlaces, con cada uno podemos, con cierta facilidad, ver una nueva ubicación. Otra característica compartida con los navegadores es el concepto de desplazamiento hacia

atrás o hacia delante, basado en el orden por el cual se desplaza en el desensamblador. Cada vez que te desplazas a una ubicación nueva en el desensamblado la ubicación actual se añade a la lista. Existen dos formas a través de menú para acceder a dicha lista. La primera es **Jump > Jump to Previous Position**, esta reposiciona el desensamblado en la ubicación inmediatamente anterior de la ubicación actual. Esto es idéntico al botón página anterior del navegador. El atajo asociado es **ESC**, uno de los atajos más utilizados memorízalo. Sin embargo acuérdate que la tecla **ESC** en cualquier otra ventana que no sea la de desensamblado y si está activa, se cerrará. Aunque acuérdate que si realizamos la acción **View > Open Subviews** podremos abrir la ventana cerrada accidentalmente. El desplazamiento hacia atrás es extremadamente práctico cuando has estado siguiendo el rastro de una función del programa dentro de distintos niveles de llamadas, y decides desplazarte a la posición original en el desensamblado.

La segunda forma es **Jump > Jump to Next Position** es la operación contraria a la anterior, es moverse hacia delante de la misma manera que el botón página posterior del web browser. El atajo asociado a esta operación es **CTRL-ENTER**, el cual se utiliza menos que ESC, atajo para ir hacia atrás. Para finalizar existen dos botones en la barra de herramientas, figura abajo, que son muy útiles para desplazarse, y nos proporciona la familiaridad del **web browser**.



Tengo que indicarte que si no te has desplazado adelante o atrás en alguna función, las flechas indicadoras no estarán resaltadas. Si te posicionas en una de las flechitas, figura arriba, te mostrará una lista de los pasos realizados en el desplazamiento, de esta forma podrás ir directamente al lugar deseado sin tener que tracear todo el camino de nuevo.

Performance Bigundill@