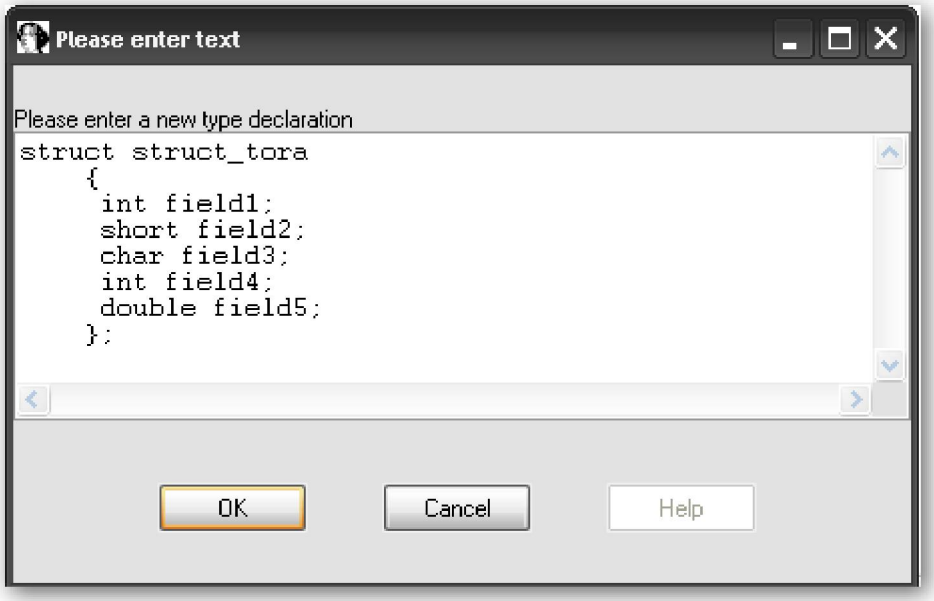
7.4.—Importar nuevas estructuras

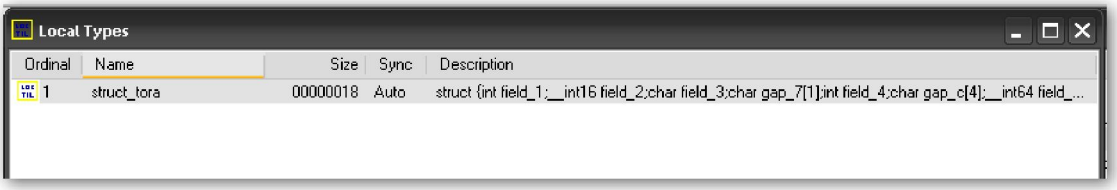
IDA nos ofrece ciertos atajos relacionados con estructuras nuevas, IDA es capaz de analizar individualmente declaraciones de datos en C, pero no en C++, así como los encabezados de archivos C, y automáticamente construir una estructura IDA la cual representará a cualquier estructura definida en esas declaraciones o a cualquier encabezado de un archivo. Si tenemos el código fuente, o al menos los headers del archivo binario al que queremos aplicarle ingeniería inversa, entonces podremos ahorrarle mucho tiempo a IDA si se extraen directamente del código fuente las estructuras.

7.4.1.—Analizar las declaraciones de estructuras C

En IDA tenemos una sub ventana llamada, **Local Types**, a la cual podemos acceder realizando la acción **View > OpenSubviews > Local Types**. Dicha ventana nos muestra una lista de todos los tipos que han sido analizados en la base de datos actual. En las bases de datos nuevas, la ventana **Local Types** inicialmente está vacía, no obstante la ventana ofrece la capacidad de analizar tipos nuevos con la tecla **INSERT** o con la opción **Insert** del menú contextual. El diálogo de entrada que se nos muestra es:



Los errores encontrados mientras se analiza el nuevo tipo se mostrarán en la ventana de mensaje de IDA. Si la declaración de tipo se analiza correctamente, el tipo y las declaraciones asociadas a él se listarán en la ventana **Local Types**, como se muestra:



Los tipos de dato añadidos a la ventana **Local Types** no están disponibles de inmediato en la ventana **Structures**. En vez, de añadirse cada tipo nuevo a la lista de estructuras

estándar; el nuevo tipo se debe de importar desde la ventana **Structures**, de la forma que veremos en la sección 7.5.

7.4.2.—Analizar encabezados de archivos C

Para analizar el encabezado de un archivo, utilizaremos la acción **File > Load File > Parse C Header File** para elegir el encabezado a analizar. Si la acción se efectúa sin ningún problema se te informará con este mensaje **Compilation successful**. Si el analizador encuentra cualquier problema, se nos notificará que existen errores. Cualquier mensaje de error se nos mostrará en la ventana de mensajes.

IDA añade todas las estructuras analizadas correctamente a su lista de estructuras estándares, al final de la lista para ser más exactos, disponibles en la base de datos actual. Cuando una nueva estructura tiene el mismo nombre que una estructura ya existente, la definición de la estructura existente es sobrescrita por el esquema de la nueva estructura. Como ya hemos apuntado, ninguna de las nuevas estructuras aparecerá en la ventana **Structures**, mientras no sea seleccionada y añadida explícitamente. Cómo añadir una estructura estándar a la ventana **Structures**, lo estudiaremos en la próxima parte.

Cuando analicemos el encabezado de un archivo C, nos será útil tener en cuenta los puntos siguientes:

** En la construcción de la estructura, el analizador no utiliza necesariamente la misma alineación de elementos que tú compilador, sin embargo sí acata la sentencia **pack**. Por defecto el analizador crea estructuras alineadas a 4-bytes.

** El analizador comprende la directiva de preprocesamiento C **include**. Para resolver las directivas include, el analizador busca el directorio donde está situado el archivo a analizar, así como cualquier directorio listado como **Include directories** en el dialogo de configuración que se muestra realizando la acción **Options > Compiler…**

** El analizador sólo comprende los datos de tipo estándares C. Sin embargo, el analizador también puede comprender la directiva de preprocesamiento **define** como una declaración C **typedef**. Así, tipos como **uint32_t** serán analizados correctamente si el analizador encuentra un **typedef** apropiado antes de su utilización.

** Cuando no tengamos ningún código fuente, podemos hallar de manera fácil y rápidamente una definición de un esquema de estructura con notación C utilizando el editor de texto y analizar el encabezado del archivo resultante, en vez de utilizar las herramientas de definición manual de estructuras de IDA.

** Las nuevas estructuras sólo están disponibles en la base de datos actual. En cada base de datos donde quieras utilizar las estructuras, tendrás que repetir los pasos de creación de ellas. Más adelante estudiaremos algunos pasos para simplificar este proceso, cuando estudiemos los archivos **TIL**.

Generalizando, para aumentar al máximo las posibilidades de analizar con buen resultado el encabezado de un archivo, tendrás que simplificar tus estructuras en definiciones que utilicen los **tipos de dato estándares C** y minimizar la utilización de archivos **include**. Recordemos, lo más importante respecto a la creación de estructuras en IDA es conseguir su esquema correcto. Al decir esquema correcto, éste dependerá más en conseguir el tamaño correcto de cada campo y la correcta alineación de la estructura, que no en conseguir el tipo exacto de cada campo. En otras palabras, si necesitamos reemplazar todas las ocurrencias de **unit32_t** con **int**, a fin de conseguir un archivo analizable correctamente, hazlo inmediatamente y sin dudar.

Performance Bigundill@