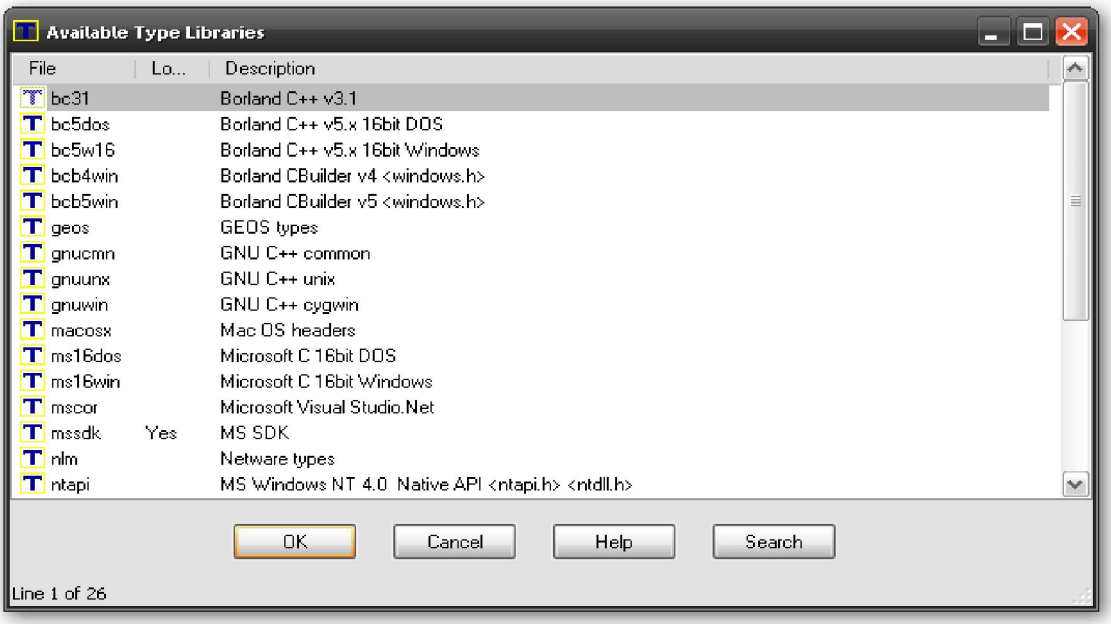
7.6.—Archivos de IDA con extensión TIL

Toda la información de IDA respecto a los tipos de dato y los prototipos de las funciones, se almacena en archivos TIL. IDA se suministra con la información de las librerías tipo de la mayoría de compiladores y API, guardada en el directorio **Archivos de programa\IDA\til**. A la ventana **Types**, se accede con la acción **View > Open Subview > Type Libraries**, en ella aparecerá el listado de los archivos **.til** cargados actualmente y además también se utiliza para cargar otros archivos **.til** que deseemos utilizar. Las librerías tipo se cargan automáticamente basándose en los atributos descubiertos del binario durante la fase de análisis. En circunstancias normales, los usuarios no necesitaremos trastear con los archivos **.til** directamente.

7.6.1.—Cargar nuevos archivos .til

En algunos casos, IDA puede fracasar al querer detectar el compilador que ha construido al binario, debido tal vez a que al binario se le ha aplicado algún tipo de ofuscación. Cuando esto sucede podemos cargar los archivos **.til** necesarios pulsando la tecla **INSERT** en la ventana **Types** y seleccionaremos los archivos **.til** que creamos oportunos. Cuando se ha cargado un nuevo **.til**, todas las definiciones de estructuras contenidas en el archivo son añadidas a la lista de estructuras estandarizadas y la información introducida es aplicada a cualquier función en el binario que coincida con los prototipos del nuevo archivo **.til** cargado. En otras palabras, cuando IDA recibe nuevas base de datos respecto a las funciones, automáticamente lo aplica a la nueva base de datos.



7.6.2.—Compartir archivos TIL

IDA también utiliza los archivos **.til** para guardar cualquier definición de estructura que hayamos creado manualmente en la ventana **Structures** o con el análisis de los encabezados C de los archivos. Tales estructuras son guardadas en un archivo **.til** dedicado y asociado con la base de datos en la cual ha sido creado. Dicho archivo comparte el nombre de la base de datos con la extensión **.til**. Por ejemplo para una base de datos llamada **CLS_archivo.idb**, la librería til asociada sería **CLS_archivo.til**. En circunstancias normales, nunca verás este archivo a no ser que tengas la base de datos abierta en IDA. Los archivos **.idb** son en realidad un archivo similar a un **.tar**, utilizados para albergar los componentes de una base de datos mientras esta no se utilice. Cuando abrimos una base de datos, los componentes del archivo, .til en este caso, son extraidos como archivos de trabajo por IDA.

Para poder compartir un archivo **.til** entre las bases de datos existentes, se pueden utilizar dos técnicas. La primera técnica, supone copiar el archivo **.til** de una base de datos abierta al directorio **IDA\til**, para ser abierta por otra base de datos por medio de la ventana **Types**. La segunda técnica para extraer información tipo a nuestro placer, de la base de datos, es realizando un **script IDC** el cual se utilizará para crear las estructuras que deseemos en cualquier otra base de datos. Dicho script se puede realizar utilizando la acción **File > Produce File > Dump Typeinfo to IDC File**. Sin embargo, la diferencia con la primera técnica, es que ésta realiza un volcado solamente de las estructuras listadas en la ventana **Structures**, con lo cual puede no incluir todas las estructuras C analizadas de los encabezados del archivo, mientras que con la primera técnica, copiar el archivo .til, si se realiza.

Performance Bigundill@