Ingeniería Inversa del Software

- Parte III -

Modificación de textos en programas (Editores hexadecimales y de recursos)

Tradicionalmente, cuando se ha pretendido modificar un texto que se pueda ver en un programa compilado, se ha utilizado un editor hexadecimal. Últimamente, no obstante, se han puesto muy de moda los editores de recursos que hacen mucho más sencillo e intuitivo este acto. No obstante, los editores hexadecimales siguen siendo mucho más eficaces y no son tan complicados como pueda parecer a simple vista.

El editor hexadecimal es un tipo especial de editor que puede mostrar y modificar cualquier tipo de carácter, incluso los especiales. Esto lo consigue manejando los códigos hexadecimales en vez de los ASCII, aunque estos también son mostrados cuando no son especiales en otra ventana aparte que sirve de referencia. Gracias a esta característica se puede editar cualquier fichero, incluso ejecutables, sin perder ningún carácter.

El editor de recursos es otro tipo de editor que solo muestra las cadenas de texto estáticas que se han definido en tiempo de programación, ocultando de esta manera el resto de caracteres hexadecimales.

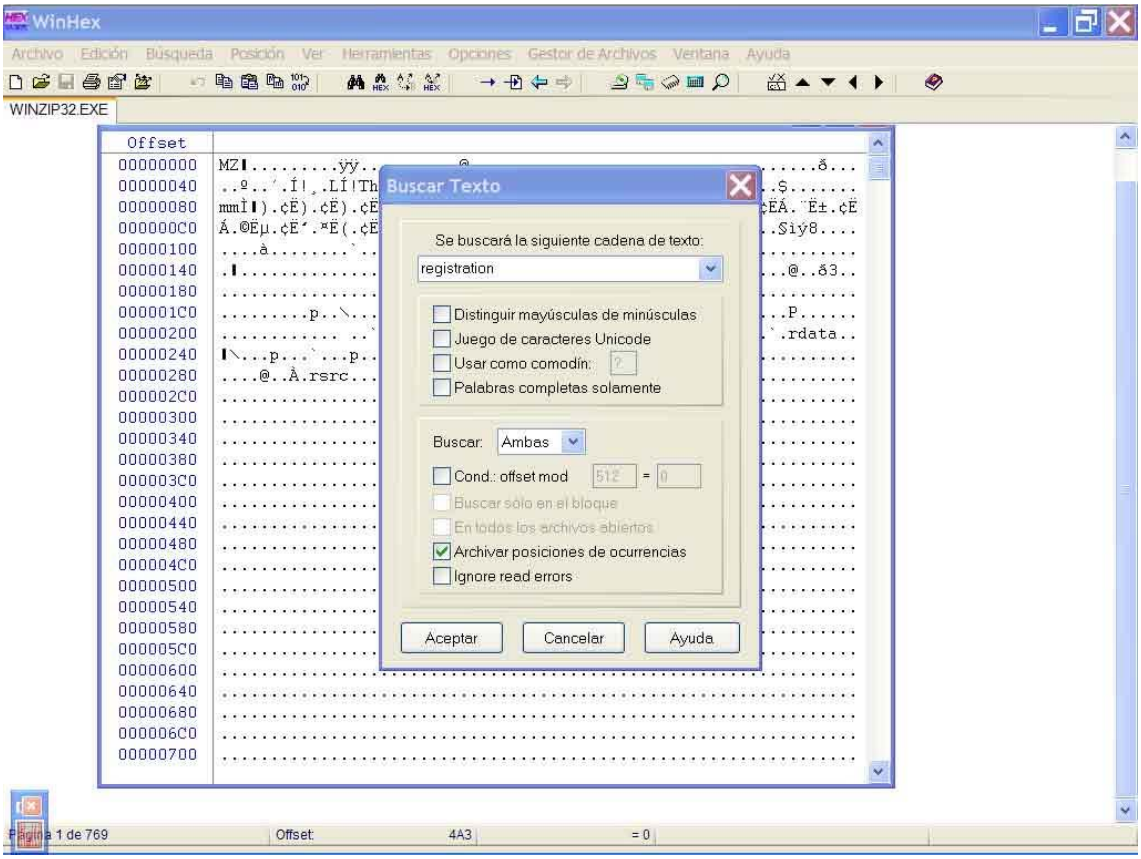
El problema de los editores de recursos es que muchas veces son incapaces de editar un programa que podría editarse hexadecimalmente. Esto es habitual cuando el programa contiene pantallas con caracteres en algún lenguaje que no está instalado en el ordenador, como por ejemplo el chino, japonés, árabe, etc.

La barrera que no puede saltarse ninguno de estos programas (de momento) es la encriptación. Por tanto, nosotros como programadores que sabemos esto, deberemos encriptar siempre la información importante contenida en nuestro software. Como vamos a ver a continuación, es muy fácil cambiar el nombre del creador del programa, su dirección de email o cualquier otro dato que se pueda proporcionar para cobrar por el uso del software completo.

Veamos como podría hacerse esto con un editor hexadecimal como el WinHex y con un editor de recursos como el Resource Hacker:

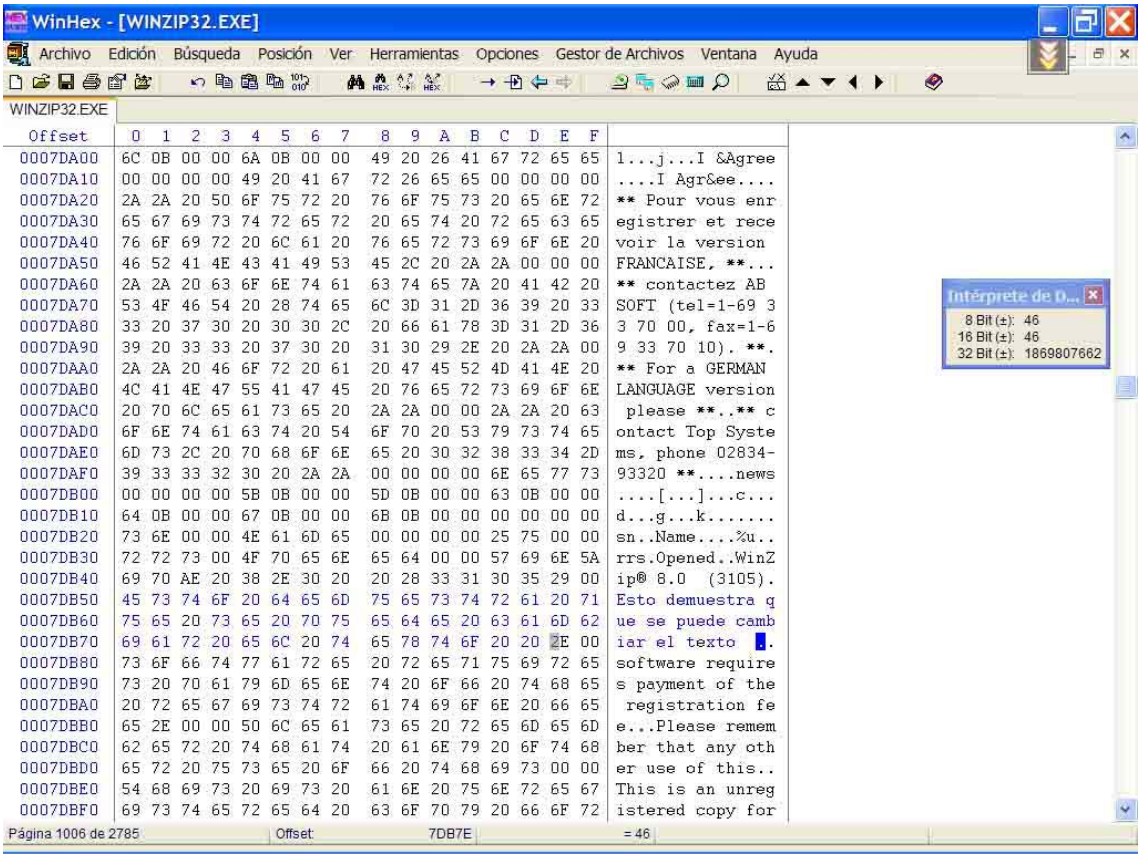
1. Se abre con el editor el programa (.exe) o la librería (.dll) correspondiente.

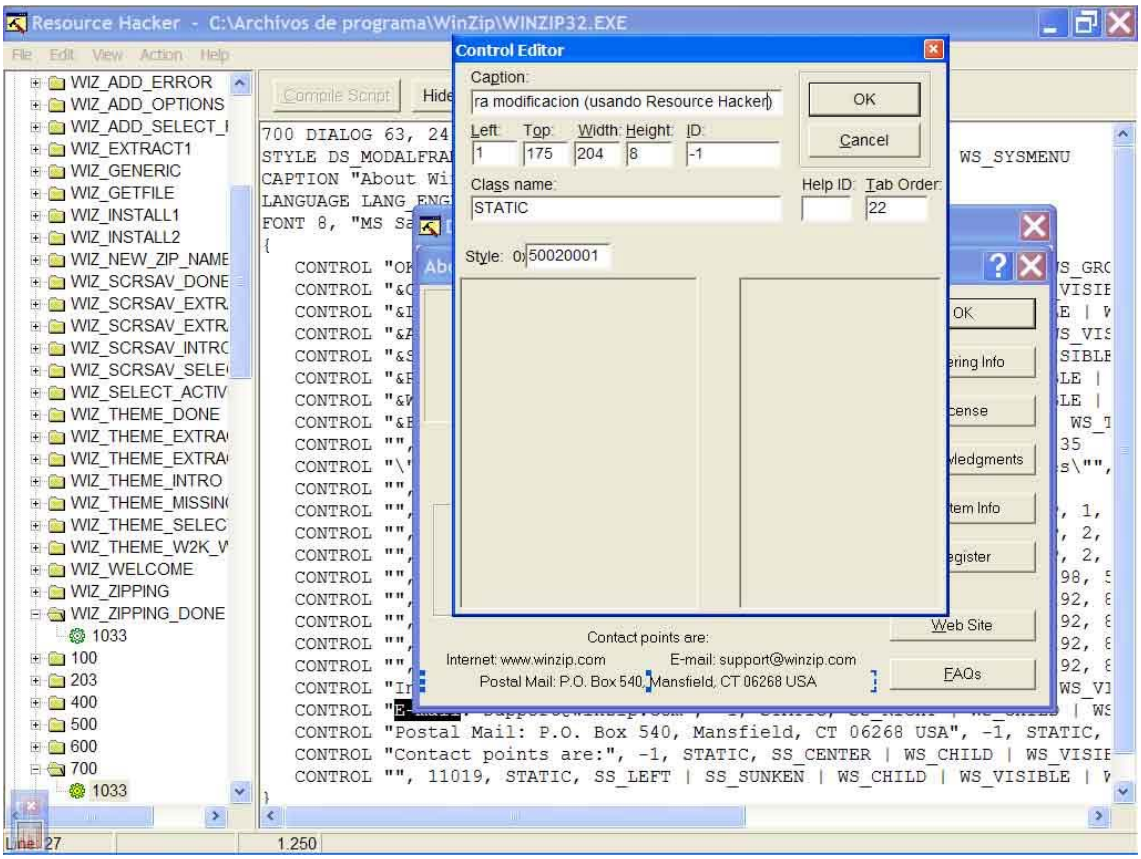
2. Se busca el texto que se quiera modificar.



3. Modificar el texto deseado, respetando siempre la longitud de la cadena de texto original si se hace con editor hexadecimal. Se puede escribir un texto más corto y rellenar con espacios, pero no se puede sobrepasar el texto original porque estaríamos sobrescribiendo el código del programa y dejaría de funcionar correctamente. Como los editores de recursos regeneran el

código para acomodar las nuevas cadenas, esta consideración no es necesaria si se usa uno de esos programas.





4. Salvar el archivo modificado.

Al ejecutar el programa se puede observar se puede observar el resultado:

A la vista está que no es nada complicado conseguir “retocar” el texto de un programa si éste no está oculto mediante encriptación, por lo que ésta debe de ser una de nuestras herramientas esenciales de programación. No cuesta nada encriptar los textos importantes de la aplicación y nos protege eficazmente contra cualquier ataque de este tipo.

Jöx€@n Nieto