

# 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.

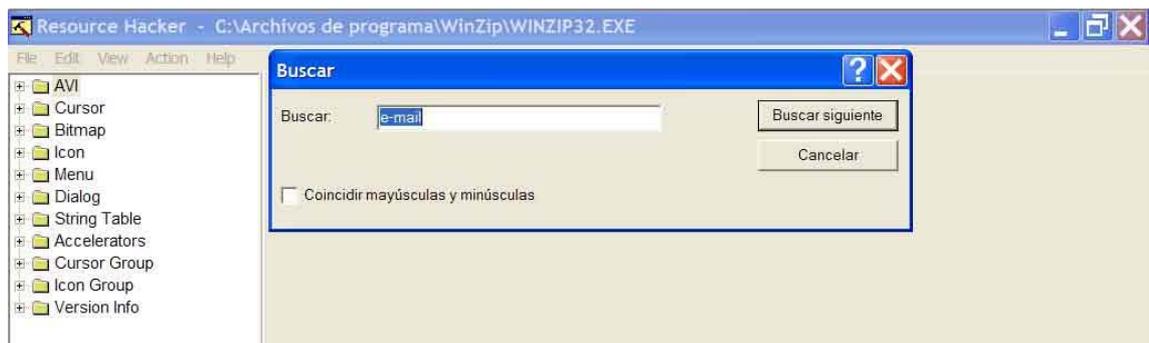
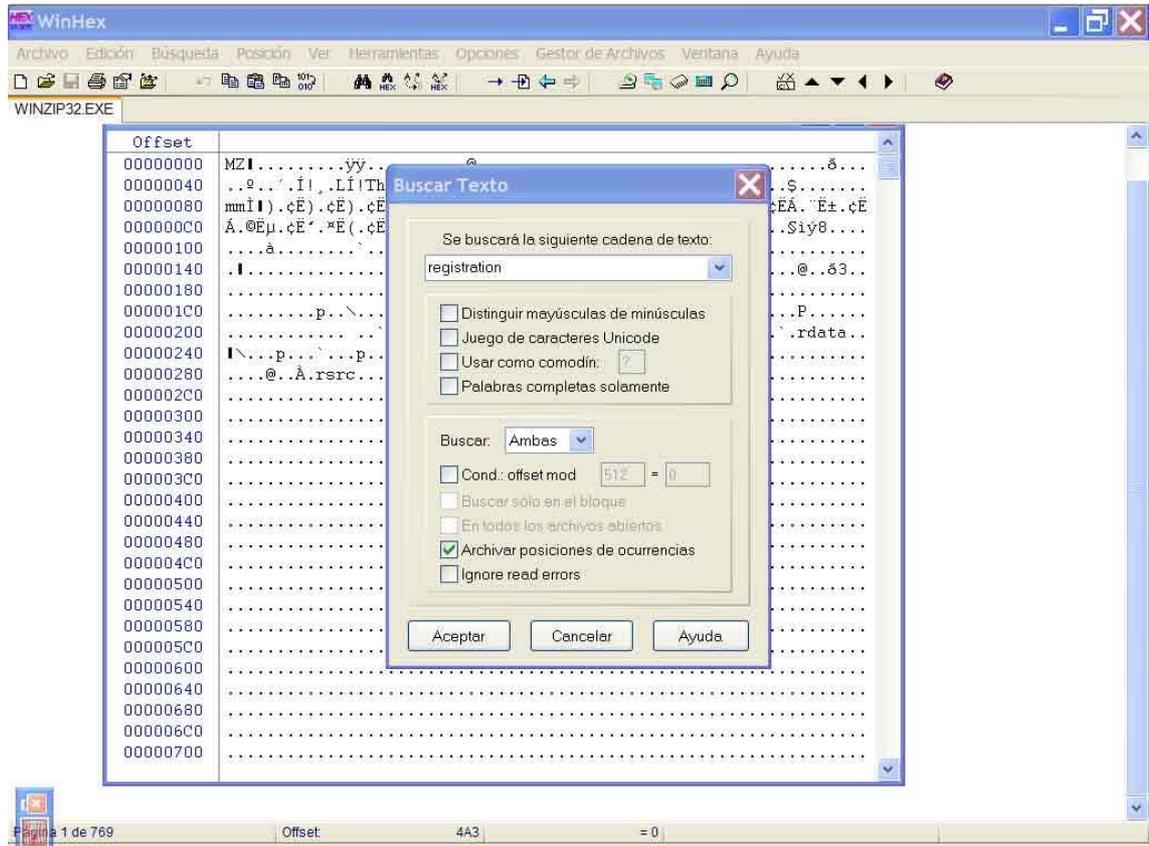
El editor de recursos es otro tipo de editor que solo muestra las cadenas de texto estáticas que se han definido en tiempo de programación, ocultando de esta manera el resto de caracteres hexadecimales.

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.

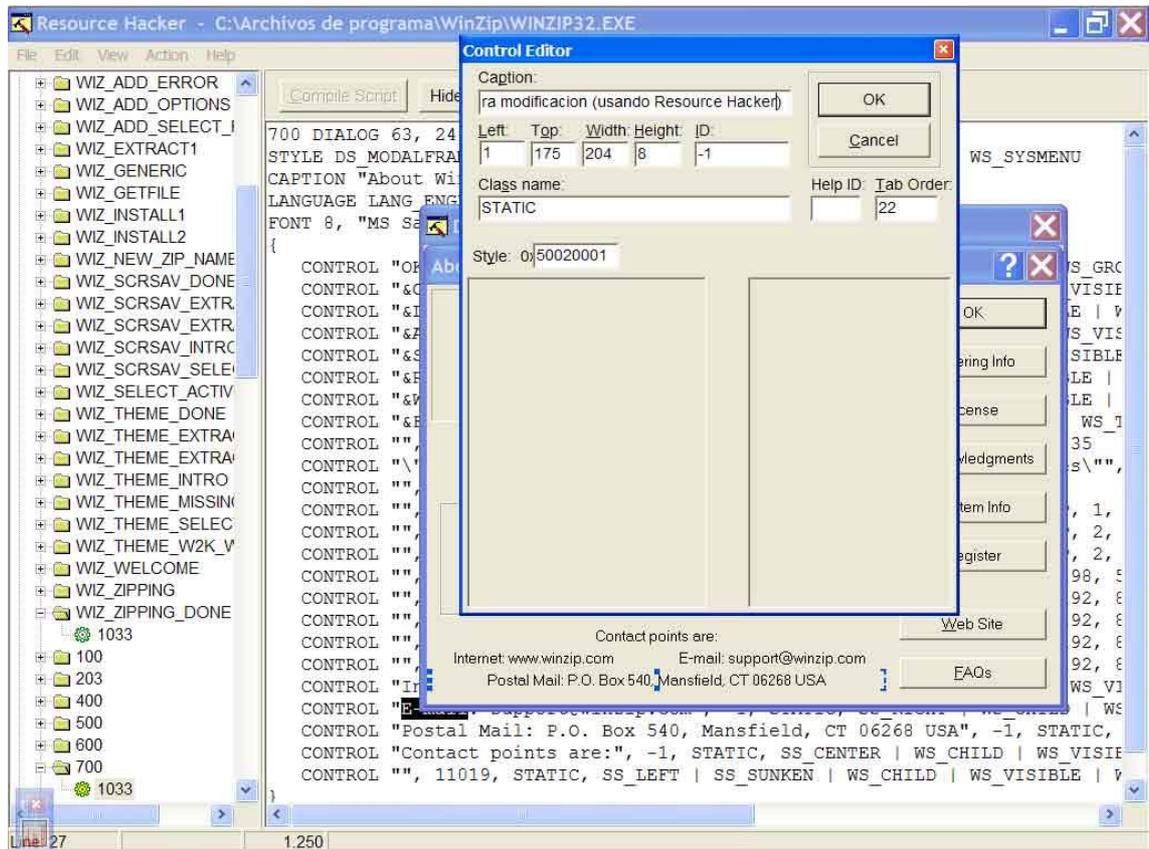


3. Modificar el texto deseado, respetando siempre la longitud de la cadena de texto original si se hace con editor hexadecimal. Se puede escribir un texto más corto y rellenar con espacios, pero no se puede sobrepasar el texto original porque estaríamos sobrescribiendo el código del programa y dejaría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

The screenshot shows the WinHex application window titled "WinHex - [WINZIP32.EXE]". The interface includes a menu bar (Archivo, Edición, Búsqueda, Posición, Ver, Herramientas, Opciones, Gestor de Archivos, Ventana, Ayuda) and a toolbar. The main area displays a hex dump of the file WINZIP32.EXE, with columns for Offset (0-15) and hex values. To the right of the hex dump is an ASCII view of the data. A small dialog box titled "Intérprete de D..." is open on the right side of the window, showing bit sizes: 8 Bit (±): 46, 16 Bit (±): 46, and 32 Bit (±): 1869807662. The status bar at the bottom indicates "Página 1006 de 2785", "Offset: 7DB7E", and "= 46".

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
0007DA00	6C	0B	00	00	6A	0B	00	00	49	20	26	41	67	72	65	65	l...j...I &Agree
0007DA10	00	00	00	00	49	20	41	67	72	26	65	65	00	00	00	00	....I Agr&ee....
0007DA20	2A	2A	20	50	6F	75	72	20	76	6F	75	73	20	65	6E	72	** Pour vous enr
0007DA30	65	67	69	73	74	72	65	72	20	65	74	20	72	65	63	65	egistrer et rece
0007DA40	76	6F	69	72	20	6C	61	20	76	65	72	73	69	6F	6E	20	voir la version
0007DA50	46	52	41	4E	43	41	49	53	45	2C	20	2A	2A	00	00	00	FRANCAISE, **...
0007DA60	2A	2A	20	63	6F	6E	74	61	63	74	65	7A	20	41	42	20	** contactez AB
0007DA70	53	4F	46	54	20	28	74	65	6C	3D	31	2D	36	39	20	33	SOFT (tel=1-69 3
0007DA80	33	20	37	30	20	30	30	2C	20	66	61	78	3D	31	2D	36	3 70 00, fax=1-6
0007DA90	39	20	33	33	20	37	30	20	31	30	29	2E	20	2A	2A	00	9 33 70 10). **.
0007DAA0	2A	2A	20	46	6F	72	20	61	20	47	45	52	4D	41	4E	20	** For a GERMAN
0007DAB0	4C	41	4E	47	55	41	47	45	20	76	65	72	73	69	6F	6E	LANGUAGE version
0007DAC0	20	70	6C	65	61	73	65	20	2A	2A	00	00	2A	2A	20	63	please **.* ** c
0007DAD0	6F	6E	74	61	63	74	20	54	6F	70	20	53	79	73	74	65	ontact Top Syste
0007DAE0	6D	73	2C	20	70	68	6F	6E	65	20	30	32	38	33	34	2D	ms, phone 02834-
0007DAF0	39	33	33	32	30	20	2A	2A	00	00	00	00	6E	65	77	73	93320 **....news
0007DB00	00	00	00	00	5B	0B	00	00	5D	0B	00	00	63	0B	00	00	....[...].c....
0007DB10	64	0B	00	00	67	0B	00	00	6B	0B	00	00	00	00	00	00	d...g...k.....
0007DB20	73	6E	00	00	4E	61	6D	65	00	00	00	00	25	75	00	00	sn..Name....%u..
0007DB30	72	72	73	00	4F	70	65	6E	65	64	00	00	57	69	6E	5A	rrs.Opened..WinZ
0007DB40	69	70	AE	20	38	2E	30	20	20	28	33	31	30	35	29	00	ip@ 8.0 (3105).
0007DB50	45	73	74	6F	20	64	65	6D	75	65	73	74	72	61	20	71	Esto demuestra q
0007DB60	75	65	20	73	65	20	70	75	65	64	65	20	63	61	6D	62	ue se puede camb
0007DB70	69	61	72	20	65	6C	20	74	65	78	74	6F	20	20	2E	00	iar el texto .
0007DB80	73	6F	66	74	77	61	72	65	20	72	65	71	75	69	72	65	software require
0007DB90	73	20	70	61	79	6D	65	6E	74	20	6F	66	20	74	68	65	s payment of the
0007DBA0	20	72	65	67	69	73	74	72	61	74	69	6F	6E	20	66	65	registration fe
0007DBB0	65	2E	00	00	50	6C	65	61	73	65	20	72	65	6D	65	6D	e...Please remem
0007DBC0	62	65	72	20	74	68	61	74	20	61	6E	79	20	6F	74	68	ber that any oth
0007DBD0	65	72	20	75	73	65	20	6F	66	20	74	68	69	73	00	00	er use of this..
0007DBE0	54	68	69	73	20	69	73	20	61	6E	20	75	6E	72	65	67	This is an unreg
0007DBF0	69	73	74	65	72	65	64	20	63	6F	70	79	20	66	6F	72	istered copy for



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