



CRACKING

WOW Sinastry

Escrito por: tHOBAS

DESCARGO LEGAL

**DOCUMENTO ESCRITO PARA FINES DE
EDUCACION/INVESTIGACION**

[Proyección]

Aprender un poco mas de la generación de seriales

[E/I a realizar]

Encontrar el numero de serie para registrarnos

[WOW Sinastry]

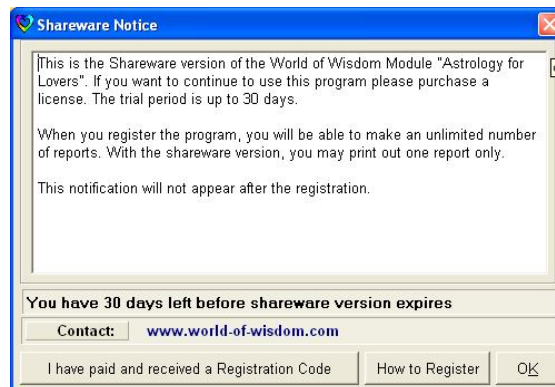
The WOW synastry program lets you see how a relationship functions, the energy between the two people involved, the areas which may be problematic and the areas where each partner is able to help and support the other.

[Url de Descarga]

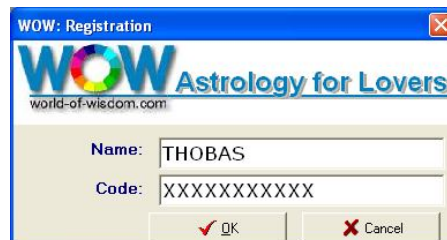
<http://world-of-wisdom.com>

[Manos a la Obra]

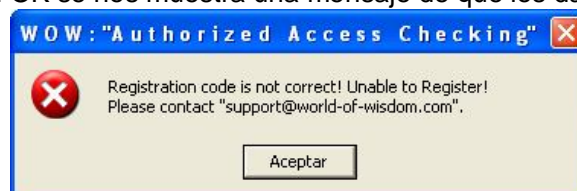
Cuando ejecutamos el programa nos muestra una ventana que nos pide registrarnos



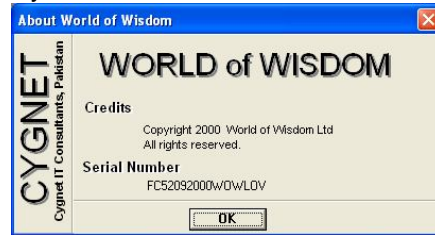
Intentaremos registrarnos dándole Click en el Boton : I have paid and received a Registration code. Se nos muestra una ventana donde nos pide que ingresemos nuestros datos



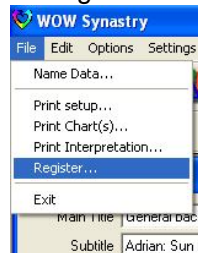
Al darle en el botón OK se nos muestra una mensaje de que los datos son incorrectos



Si ingresamos al programa y vemos en el About nos muestra que:



Y en el menú archivo esta el botón de Registrar



Solo nos faltaría saber si el programa esta empaquetado o no y saber en que lenguaje fue hecho para empezar. Para eso lo analizaremos con el RDG. El cual nos muestra la siguiente información



Bueno el programa esta hecho en Delphi y para suerte nuestra no esta empaquetado.

Como no me va bien aun con Delphi, haremos uso del DeDe para averiguar la dirección exacta del botón de OK.

El DeDe nos da la siguiente información.

Classes Info		Units Info	Forms	Procedures	Project	Exports
Unit Name	Class Name	TFrmRegDlg				
Aboutbox	TAboutForm					
aspects	TVinAspects					
Compgrap	TCompGraph					
CompText	TfrmIntersp					
Cusposos	TVinCPos					
DBISAMPw	TDBISAMPPasswordDialog					
DBLogDlg	TLoginDialog					
DBPwDlg	TPasswordDialog					
DGRDIALS	TDegreeDial					
GraphView	TVheelView					
NameDlg2	TNameDlg					
Prev	TPreview					
Printk	TPrintout					
RegDlg	TFrmRegDlg					
Splash	TSplashForm					
Swmsg	TFrmSwMsg					

Event	RVA	Hint
FormCreate	00578710	0011
GenSynCode	00578734	0011
Btnm1Click	00578CF0	0013
Btnm2Click	00578D3C	0013
Edt1Change	00578D54	0012
Timer1Timer	00578DF4	0012
Edt2Change	00578E3C	0012
Edt2KeyDown	00578EC0	0013
_PROC_005788EC	005788EC	FFFF
_PROC_00578C48	00578C48	FFFF
_PROC_00578F18	00578F18	FFFF
_PROC_00578F48	00578F48	FFFF

Ahí esta la dirección de nuestro botón OK, en la dirección 00578CF0. Ahora bien como sabemos que es el botón de Ok?

Bueno el DeDe nos lo aclara bien

Class Name	Offset	
TAboutForm	001FE884	AutoSize = False
TAtlasDlg	001FFD18	Caption = 'Version:'
TCompGraph	002048A0	Font.Charset = ANSI_CHARSET
TDBISAMPasswordDi...	00205598	Font.Color = clNavy
TDegreeDlg	00205968	Font.Height = -13
TEMGraph	002063A4	Font.Name = 'MS Sans Serif'
TExtDlg	00206E00	Font.Style = [fsBold]
TFormTips	00207424	ParentFont = False
TfrmInterp	002087E8	Visible = False
TfrmMessage	002089FC	end
TfrmRegDlg	00208D60	object BitBtn1: TBitBtn
TfrmSwMsg	0020DD28	Tag = 506
TInterpWin	0020E680	Left = 117
TLoginDialog	002158F4	Top = 149
TMainForm	00215D68	Width = 120
TNameDlg	002EC77C	Height = 26
TObjsDlg	002EFD5C	Caption = 'OK'
TPageDlg	002F0590	Enabled = False
TPasswordDialog	002F2044	Font.Charset = ANSI_CHARSET
TPlanetsWin	002F4C78	Font.Color = clWindowText
TPreview	002F51F0	Font.Height = -11
TPrintout	002F5FD4	Font.Name = 'MS Sans Serif'
TPrintProgress	002F9698	Font.Style = []
TPrintProgressLight	002F9960	ParentFont = False
		TabOrder = 0
		OnClick = BitBtn1Click

Bueno despejada nuestras dudas. Abrimos nuestro OllyDbg, cargamos el ejecutable y CTRL+G y colocamos la dirección 00578cf0 y llegamos hasta aquí

```

[CPU - main thread, module WOW32]
File View Debug Plugins Options Window Help
Paused
00578C40 dd 00000000
00578C44 dd 0000000A
00578C48 dd 00000000
00578C4C dd 00000000
00578C50 dd 00000000
00578C54 dd 00000000
00578C58 dd 00000000
00578C5C dd 00000000
00578C60 dd 00000000
00578C64 dd 00000000
00578C68 dd 00000000
00578C6C dd 00000000
00578C70 dd 00000000
00578C74 dd 00000000
00578C78 dd 00000000
00578C7C dd 00000000
00578C80 dd 00000000
00578C84 dd 00000000
00578C88 dd 00000000
00578C8C dd 00000000
00578C90 dd 00000000
00578C94 dd 00000000
00578C98 dd 00000000
00578CA0 dd 00000000
00578CA4 dd 00000000
00578CA8 dd 00000000
00578CAC dd 00000000
00578CB0 dd 00000000
00578CB4 dd 00000000
00578CB8 dd 00000000
00578CC0 dd 00000000
00578CC4 dd 00000000
00578CC8 dd 00000000
00578CCC dd 00000000
00578CD0 dd 00000000
00578CD4 dd 00000000
00578CD8 dd 00000000
00578CE0 dd 00000000
00578CE4 dd 00000000
00578CE8 dd 00000000
00578CF0 dd 00000000
00578CF4 dd 00000000
00578CFF dd 00000000
00578D00 dd 00000000
00578D04 dd 00000000
00578D08 dd 00000000
00578D0C dd 00000000
00578D10 dd 00000000
00578D14 dd 00000000
00578D18 dd 00000000
00578D1C dd 00000000
00578D20 dd 00000000
00578D24 dd 00000000
00578D28 dd 00000000
00578D2C dd 00000000
00578D30 dd 00000000
00578D34 dd 00000000
00578D38 dd 00000000
00578D3C dd 00000000
00578D40 dd 00000000
00578D44 dd 00000000
00578D48 dd 00000000
00578D4C dd 00000000
00578D50 dd 00000000
00578D54 dd 00000000
00578D58 dd 00000000
00578D5C dd 00000000
00578D60 dd 00000000
00578D64 dd 00000000
00578D68 dd 00000000
00578D6C dd 00000000
00578D70 dd 00000000
00578D74 dd 00000000
00578D78 dd 00000000
00578D7C dd 00000000
00578D80 dd 00000000
00578D84 dd 00000000
00578D88 dd 00000000
00578D8C dd 00000000
00578D90 dd 00000000
00578D94 dd 00000000
00578D98 dd 00000000
00578D9C dd 00000000
00578DA0 dd 00000000
00578DA4 dd 00000000
00578DA8 dd 00000000
00578DAC dd 00000000
00578DB0 dd 00000000
00578DB4 dd 00000000
00578DB8 dd 00000000
00578DBC dd 00000000
00578DC0 dd 00000000
00578DC4 dd 00000000
00578DC8 dd 00000000
00578DCC dd 00000000
00578DD0 dd 00000000
00578DD4 dd 00000000
00578DD8 dd 00000000
00578DDC dd 00000000
00578DE0 dd 00000000
00578DE4 dd 00000000
00578DE8 dd 00000000
00578DEC dd 00000000
00578DED dd 00000000
00578DEE dd 00000000
00578DEF dd 00000000
00578DF0 dd 00000000
00578DF4 dd 00000000
00578DF8 dd 00000000
00578DFC dd 00000000
00578E00 dd 00000000
00578E04 dd 00000000
00578E08 dd 00000000
00578E0C dd 00000000
00578E10 dd 00000000
00578E14 dd 00000000
00578E18 dd 00000000
00578E1C dd 00000000
00578E20 dd 00000000
00578E24 dd 00000000
00578E28 dd 00000000
00578E2C dd 00000000
00578E30 dd 00000000
00578E34 dd 00000000
00578E38 dd 00000000
00578E3C dd 00000000
00578E40 dd 00000000
00578E44 dd 00000000
00578E48 dd 00000000
00578E4C dd 00000000
00578E50 dd 00000000
00578E54 dd 00000000
00578E58 dd 00000000
00578E5C dd 00000000
00578E60 dd 00000000
00578E64 dd 00000000
00578E68 dd 00000000
00578E6C dd 00000000
00578E70 dd 00000000
00578E74 dd 00000000
00578E78 dd 00000000
00578E7C dd 00000000
00578E80 dd 00000000
00578E84 dd 00000000
00578E88 dd 00000000
00578E8C dd 00000000
00578E90 dd 00000000
00578E94 dd 00000000
00578E98 dd 00000000
00578E9C dd 00000000
00578EA0 dd 00000000
00578EA4 dd 00000000
00578EA8 dd 00000000
00578EAC dd 00000000
00578EB0 dd 00000000
00578EB4 dd 00000000
00578EB8 dd 00000000
00578EBC dd 00000000
00578EBE dd 00000000
00578EBF dd 00000000
00578EC0 dd 00000000
00578EC4 dd 00000000
00578EC8 dd 00000000
00578ECE dd 00000000
00578ED0 dd 00000000
00578ED4 dd 00000000
00578ED8 dd 00000000
00578EDC dd 00000000
00578EE0 dd 00000000
00578EE4 dd 00000000
00578EE8 dd 00000000
00578EEC dd 00000000
00578EEF dd 00000000
00578EF0 dd 00000000
00578EF4 dd 00000000
00578EF8 dd 00000000
00578EFC dd 00000000
00578F00 dd 00000000
00578F04 dd 00000000
00578F08 dd 00000000
00578F0C dd 00000000
00578F10 dd 00000000
00578F14 dd 00000000
00578F18 dd 00000000
00578F1C dd 00000000
00578F20 dd 00000000
00578F24 dd 00000000
00578F28 dd 00000000
00578F2C dd 00000000
00578F30 dd 00000000
00578F34 dd 00000000
00578F38 dd 00000000
00578F3C dd 00000000
00578F40 dd 00000000
00578F44 dd 00000000
00578F48 dd 00000000
00578F4C dd 00000000
00578F50 dd 00000000
00578F54 dd 00000000
00578F58 dd 00000000
00578F5C dd 00000000
00578F60 dd 00000000
00578F64 dd 00000000
00578F68 dd 00000000
00578F6C dd 00000000
00578F70 dd 00000000
00578F74 dd 00000000
00578F78 dd 00000000
00578F7C dd 00000000
00578F80 dd 00000000
00578F84 dd 00000000
00578F88 dd 00000000
00578F8C dd 00000000
00578F90 dd 00000000
00578F94 dd 00000000
00578F98 dd 00000000
00578F9C dd 00000000
00578FA0 dd 00000000
00578FA4 dd 00000000
00578FA8 dd 00000000
00578FAC dd 00000000
00578FB0 dd 00000000
00578FB4 dd 00000000
00578FB8 dd 00000000
00578FBC dd 00000000
00578FBF dd 00000000
00578FC0 dd 00000000
00578FC4 dd 00000000
00578FC8 dd 00000000
00578FCC dd 00000000
00578FD0 dd 00000000
00578FD4 dd 00000000
00578FD8 dd 00000000
00578FDC dd 00000000
00578FE0 dd 00000000
00578FE4 dd 00000000
00578FE8 dd 00000000
00578FEC dd 00000000
00578FEF dd 00000000
00578FF0 dd 00000000
00578FF4 dd 00000000
00578FF8 dd 00000000
00578FFC dd 00000000
00579000 dd 00000000
00579004 dd 00000000
00579008 dd 00000000
0057900C dd 00000000
00579010 dd 00000000
00579014 dd 00000000
00579018 dd 00000000
0057901C dd 00000000
00579020 dd 00000000
00579024 dd 00000000
00579028 dd 00000000
0057902C dd 00000000
00579030 dd 00000000
00579034 dd 00000000
00579038 dd 00000000
0057903C dd 00000000
00579040 dd 00000000
00579044 dd 00000000
00579048 dd 00000000
0057904C dd 00000000
00579050 dd 00000000
00579054 dd 00000000
00579058 dd 00000000
0057905C dd 00000000
00579060 dd 00000000
00579064 dd 00000000
00579068 dd 00000000
0057906C dd 00000000
00579070 dd 00000000
00579074 dd 00000000
00579078 dd 00000000
0057907C dd 00000000
00579080 dd 00000000
00579084 dd 00000000
00579088 dd 00000000
0057908C dd 00000000
00579090 dd 00000000
00579094 dd 00000000
00579098 dd 00000000
0057909C dd 00000000
005790A0 dd 00000000
005790A4 dd 00000000
005790A8 dd 00000000
005790AC dd 00000000
005790B0 dd 00000000
005790B4 dd 00000000
005790B8 dd 00000000
005790BC dd 00000000
005790BF dd 00000000
005790C0 dd 00000000
005790C4 dd 00000000
005790C8 dd 00000000
005790CC dd 00000000
005790D0 dd 00000000
005790D4 dd 00000000
005790D8 dd 00000000
005790DC dd 00000000
005790E0 dd 00000000
005790E4 dd 00000000
005790E8 dd 00000000
005790EC dd 00000000
005790EF dd 00000000
005790F0 dd 00000000
005790F4 dd 00000000
005790F8 dd 00000000
005790FC dd 00000000
00579100 dd 00000000
00579104 dd 00000000
00579108 dd 00000000
0057910C dd 00000000
00579110 dd 00000000
00579114 dd 00000000
00579118 dd 00000000
0057911C dd 00000000
00579120 dd 00000000
00579124 dd 00000000
00579128 dd 00000000
0057912C dd 00000000
00579130 dd 00000000
00579134 dd 00000000
00579138 dd 00000000
0057913C dd 00000000
00579140 dd 00000000
00579144 dd 00000000
00579148 dd 00000000
0057914C dd 00000000
00579150 dd 00000000
00579154 dd 00000000
00579158 dd 00000000
0057915C dd 00000000
00579160 dd 00000000
00579164 dd 00000000
00579168 dd 00000000
0057916C dd 00000000
00579170 dd 00000000
00579174 dd 00000000
00579178 dd 00000000
0057917C dd 00000000
00579180 dd 00000000
00579184 dd 00000000
00579188 dd 00000000
0057918C dd 00000000
00579190 dd 00000000
00579194 dd 00000000
00579198 dd 00000000
0057919C dd 00000000
005791A0 dd 00000000
005791A4 dd 00000000
005791A8 dd 00000000
005791AC dd 00000000
005791B0 dd 00000000
005791B4 dd 00000000
005791B8 dd 00000000
005791BC dd 00000000
005791BF dd 00000000
005791C0 dd 00000000
005791C4 dd 00000000
005791C8 dd 00000000
005791CC dd 00000000
005791D0 dd 00000000
005791D4 dd 00000000
005791D8 dd 00000000
005791DC dd 00000000
005791E0 dd 00000000
005791E4 dd 00000000
005791E8 dd 00000000
005791EC dd 00000000
005791EF dd 00000000
005791F0 dd 00000000
005791F4 dd 00000000
005791F8 dd 00000000
005791FC dd 00000000
00579200 dd 00000000
00579204 dd 00000000
00579208 dd 00000000
0057920C dd 00000000
00579210 dd 00000000
00579214 dd 00000000
00579218 dd 00000000
0057921C dd 00000000
00579220 dd 00000000
00579224 dd 00000000
00579228 dd 00000000
0057922C dd 00000000
00579230 dd 00000000
00579234 dd 00000000
00579238 dd 00000000
0057923C dd 00000000
00579240 dd 00000000
00579244 dd 00000000
00579248 dd 00000000
0057924C dd 00000000
00579250 dd 00000000
00579254 dd 00000000
00579258 dd 00000000
0057925C dd 00000000
00579260 dd 00000000
00579264 dd 00000000
00579268 dd 00000000
0057926C dd 00000000
00579270 dd 00000000
00579274 dd 00000000
00579278 dd 00000000
0057927C dd 00000000
00579280 dd 00000000
00579284 dd 00000000
00579288 dd 00000000
0057928C dd 00000000
00579290 dd 00000000
00579294 dd 00000000
00579298 dd 00000000
0057929C dd 00000000
005792A0 dd 00000000
005792A4 dd 00000000
005792A8 dd 00000000
005792AC dd 00000000
005792B0 dd 00000000
005792B4 dd 00000000
005792B8 dd 00000000
005792BC dd 00000000
005792BF dd 00000000
005792C0 dd 00000000
005792C4 dd 00000000
005792C8 dd 00000000
005792CC dd 00000000
005792D0 dd 00000000
005792D4 dd 00000000
005792D8 dd 00000000
005792DC dd 00000000
005792E0 dd 00000000
005792E4 dd 00000000
005792E8 dd 00000000
005792EC dd 00000000
005792EF dd 00000000
005792F0 dd 00000000
005792F4 dd 00000000
005792F8 dd 00000000
005792FC dd 00000000
00579300 dd 00000000
00579304 dd 00000000
00579308 dd 00000000
0057930C dd 00000000
00579310 dd 00000000
00579314 dd 00000000
00579318 dd 00000000
0057931C dd 00000000
00579320 dd 00000000
00579324 dd 00000000
00579328 dd 00000000
0057932C dd 00000000
00579330 dd 00000000
00579334 dd 00000000
00579338 dd 00000000
0057933C dd 00000000
00579340 dd 00000000
00579344 dd 00000000
00579348 dd 00000000
0057934C dd 00000000
00579350 dd 00000000
00579354 dd 00000000
00579358 dd 00000000
0057935C dd 00000000
00579360 dd 00000000
00579364 dd 00000000
00579368 dd 00000000
0057936C dd 00000000
00579370 dd 00000000
00579374 dd 00000000
00579378 dd 00000000
0057937C dd 00000000
00579380 dd 00000000
00579384 dd 00000000
00579388 dd 00000000
0057938C dd 00000000
00579390 dd 00000000
00579394 dd 00000000
00579398 dd 00000000
0057939C dd 00000000
005793A0 dd 00000000
005793A4 dd 00000000
005793A8 dd 00000000
005793AC dd 00000000
005793B0 dd 00000000
005793B4 dd 00000000
005793B8 dd 00000000
005793BC dd 00000000
005793BF dd 00000000
005793C0 dd 00000000
005793C4 dd 00000000
005793C8 dd 00000000
005793CC dd 00000000
005793D0 dd 00000000
005793D4 dd 00000000
005793D8 dd 00000000
005793DC dd 00000000
005793E0 dd 00000000
005793E4 dd 00000000
005793E8 dd 00000000
005793EC dd 00000000
005793EF dd 00000000
005793F0 dd 00000000
005793F4 dd 00000000
005793F8 dd 00000000
005793FC dd 00000000
00579400 dd 00000000
00579404 dd 00000000
00579408 dd 00000000
0057940C dd 00000000
00579410 dd 00000000
00579414 dd 00000000
00579418 dd 00000000
0057941C dd 00000000
00579420 dd 00000000
00579424 dd 00000000
00579428 dd 00000000
0057942C dd 00000000
00579430 dd 00000000
00579434 dd 00000000
00579438 dd 00000000
0057943C dd 00000000
00579440 dd 00000000
00579444 dd 00000000
00579448 dd 00000000
0057944C dd 00000000
00579450 dd 00000000
00579454 dd 00000000
00579458 dd 00000000
0057945C dd 00000000
00579460 dd 00000000
00579464 dd 00000000
00579468 dd 00000000
0057946C dd 00000000
00579470 dd 00000000
00579474 dd 00000000
00579478 dd 00000000
0057947C dd 00000000
00579480 dd 00000000
00579484 dd 00000000
00579488 dd 00000000
0057948C dd 00000000
00579490 dd 00000000
00579494 dd 00000000
00579498 dd 00000000
0057949C dd 00000000
005794A0 dd 00000000
005794A4 dd 00000000
005794A8 dd 00000000
005794AC dd 00000000
005794B0 dd 00000000
005794B4 dd 00000000
005794B8 dd 00000000
005794BC dd 00000000
005794BF dd 00000000
005794C0 dd 00000000
005794C4 dd 00000000
005794C8 dd 00000000
005794CC dd 00000000
005794D0 dd 00000000
005794D4 dd 00000000
005794D8 dd 00000000
005794DC dd 00000000
005794E0 dd 00000000
005794E4 dd 00000000
005794E8 dd 00000000
005794EC dd 00000000
005794EF dd 00000000
005794F0 dd 00000000
005794F4 dd 00000000
005794F8 dd 00000000
005794FC dd 00000000
00579500 dd 00000000
00579504 dd 00000000
00579508 dd 00000000
0057950C dd 00000000
00579510 dd 00000000
00579514 dd 00000000
00579518 dd 00000000
0057951C dd 00000000
00579520 dd 00000000
00579524 dd 00000000
00579528 dd 00000000
0057952C dd 00000000
00579530 dd 00000000
00579534 dd 00000000
00579538 dd 00000000
0057953C dd 00000000
00579540 dd 00000000
00579544 dd 00000000
00579548 dd 00000000
0057954C dd 00000000
00579550 dd 00000000
0
```

```

005788EC /$ 55      push ebp
005788ED |. 8BEC      mov     ebp, esp
005788EF |. B9 58000000 mov     ecx, 58
005788F4 > 6A 00      push     0
005788F6 |. 6A 00      push     0
005788F8 |. 49         dec     ecx
005788F9 |.^ 75 F9      jnz     short 005788F4
005788FB |. 53         push    ebx
005788FC |. 8B45 FC     mov     dword ptr [ebp+4], eax
005788FE |. 33C0        xor     eax, eax
00578900 |. 55         push    ebp
00578901 |. 68 D78B5700 push    dword ptr [ebp+0]
00578903 |. 64 FF30     mov     dword ptr [eax], esp
00578905 |. 8D95 80FDFFF lea     edx, dword ptr [ebp-28]
00578907 |. A1 D8055D00 mov     eax, dword ptr [5D05D8]
00578909 |. 8B00        mov     eax, dword ptr [eax]
0057890B |. E8 498FEDFF call    00451868
0057890D |. 8B85 80FDFFF mov     eax, dword ptr [ebp-28]
0057890F |. 8D55 EC     lea     edx, dword ptr [ebp-14]
00578911 |. E8 3317E9FF call    0040A060
00578913 |. C645 FB 01  mov     byte ptr [ebp+5], 1
00578915 |. C745 F4 9CFF mov     dword ptr [ebp+3], -64
00578917 |. 8D95 78FDFFF lea     edx, dword ptr [ebp-28]
00578919 |. 8B45 FC     mov     eax, dword ptr [ebp+4]
0057891B |. 8B80 6402000 mov     eax, dword ptr [eax+2E4]
0057891D |. E8 CC45EBFF call    00432F18
0057891F |. 8B85 78FDFFF mov     eax, dword ptr [ebp-28]
00578921 |. 8D80 7C0DFFF lea     edx, dword ptr [ebp-28]
00578923 |. 8B55 FC     mov     eax, dword ptr [ebp+4]
00578925 |. 8B92 F002000 mov     edx, dword ptr [edx+2F0]
00578927 |. 8B92 1C02000 mov     edx, dword ptr [edx+21C]
00578929 |. 42         inc     edx
0057892B |. E8 E722E9FF call    0045AC54
0057892D |. 8B85 7C0DFFF mov     eax, dword ptr [ebp-28]
0057892F |. 50         push    eax
00578931 |. 8D95 74FDFFF lea     edx, dword ptr [ebp-28]
00578933 |. 8B45 FC     mov     eax, dword ptr [ebp+4]
00578935 |. 8B80 EC02000 mov     eax, dword ptr [eax+2EC]
00578937 |. E8 90A5EBFF call    00432F18
00578939 |. 8B95 74FDFFF mov     edx, dword ptr [ebp-28]
0057893B |. 58         pop     eax
0057893D |. E8 CCB8E9FF call    00404260
0057893F |. 6A 10       push    short 005789CF
00578941 |. 6A 10       push    10
00578943 |. E8 A3F9E9FF call    <mp.>user32.MessageBeep
00578945 |. 6A 10       push    10
00578947 |. B9 E88B5700 mov     ecx, 00578B88
00578949 |. 6A 38       push    short 00578B88
0057894B |. A1 D8055D00 mov     eax, dword ptr [5D05D8]

```

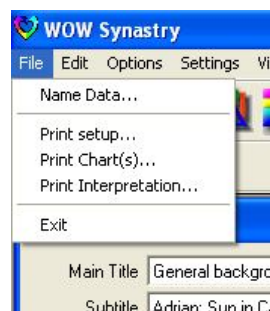
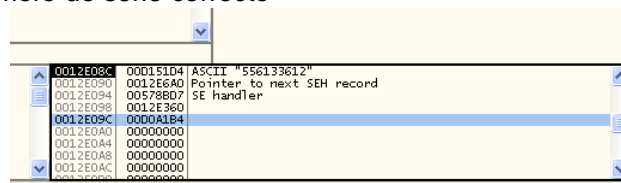
En la parte de abajo esta la cadena de Texto que nos dice que el código para registrar no es correcto. Traceamos otra vez con F8 pero si nos fijamos en esta parte :

```

005788EC /$ 55      push ebp
005788ED |. 8BEC      mov     ebp, esp
005788EF |. B9 58000000 mov     ecx, 58
005788F4 > 6A 00      /push 0
005788F6 |. 6A 00      |push 0
005788F8 |. 49         |dec  ecx
005788F9 |.^ 75 F9      \jnz  short 005788F4
005788FB |. 53         push    ebx

```

Existe un bucle que se va a repetir 58h veces (88 veces en decimal) hasta que ecx sea 0. Como no nos pasaremos un buen rato traceando hasta que ECX valga 0. Entonces colocare un BP en la dirección 005788FB y apretamos F9 para que se detenga en el BP. Traceamos hasta el CALL de la dirección 00578983 y vemos en la ventana del Stack nuestro numero de serie correcto



Para los que quieren ver como se genera el serial, esta se realiza en el CALL de la dirección 00578968. Lo que realiza el programa es que juega con nuestro nombre ingresado hasta lograr un resultado de 8 digitos, por ejemplo en mi caso seria : 87307322 de ahí coge el resultado y realiza operación cogiendo el ultimo digito primero y terminando con el primer digito del resultado, hasta lograr nuestro numero de serie correcto que en este caso seria : 55613612

Y como para tener un poco mas de ayuda el serial correcto siempre será de 9 digitos, sea cual fuese el nombre ingresado

[Aclaracion]

Perdonen, se que lo hice extenso pero es la forma como lo hice yo

[pF del autor]

Saludos a todo rVLCN; CracksLatinoS, Arc; y a ti por tomarte tu tiempo para leer este tutorial

[El autor puede ser contactado]

eMail: tHOBAS@gmail.com

www: <http://RVLCN.com>
<http://RVLCNsecurity.com>
<http://rvlcn.iespana.es>
<http://beam.to/RVLCN> - Lista
<http://RVLCNsecurity.com/foro> - Foro

Noviembre-2008

-----/ REVOLUCION /-----