

2017

Revisando FastStone \*  
By  
Apuromafo & DavicoRm



Apuromafo & DavicoRm

CLS

10-7-2017

# Índice

## Contenido

Índice.....	1
Introducción .....	2
Herramientas usadas en el Escrito:.....	2
Explorando el Programa 1 .....	2
Explorando el Programa 2 .....	8
Explorando el Programa 3 .....	11
Explorando el Programa 4 .....	13
Palabras Finales: .....	15

Introducción

Programa	FastStone *
Descarga	http://www.faststone.org/ 1 http://www.faststone.org/FSCapturerDownload.htm 2 http://www.faststone.org/FSViewerDownload.htm 3 http://www.faststone.org/FSMaxViewDownload.htm 4 http://www.faststone.org/FSResizerDownload.htm
Dificultad	Depende de quien lo mire.
Información	http://www.faststone.org/
Herramientas usadas	X64dbg , PID ,IDR ,7zip
Fecha	10/07/2017
Cracker	Apuromafo & DavicoRm

"Las ideas no duran mucho. Hay que hacer algo con ellas"

Santiago Ramón y Cajal

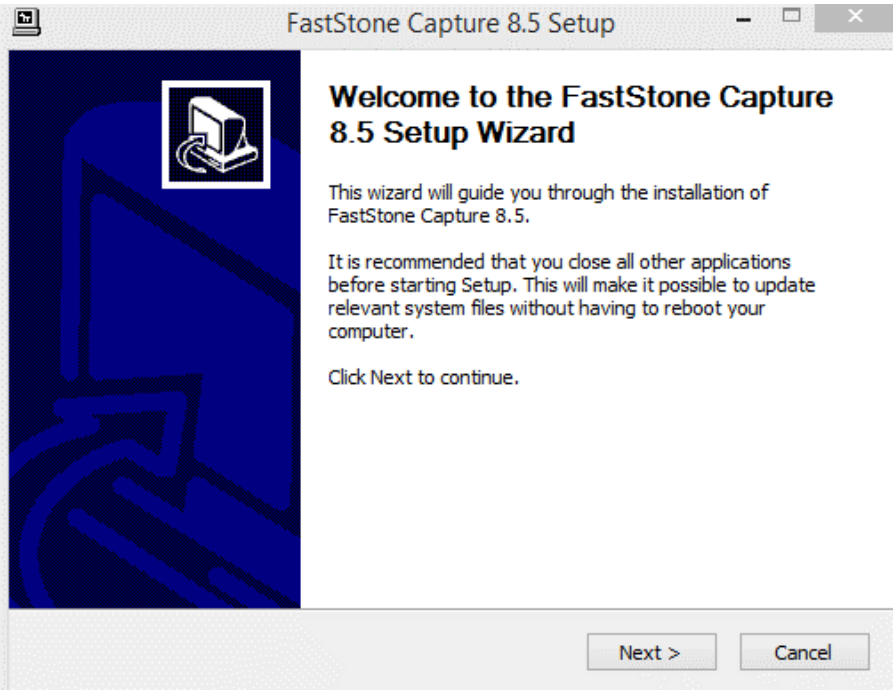
Herramientas usadas en el Escrito:

Herramienta	Descarga	Utilidad
Procesador de texto	(está incluido con el suite de office)	Para redactar el tutorial
Sharex	<a href="https://getsharex.com/">https://getsharex.com/</a>	Para capturar las imágenes
Everything	<a href="http://www.voidtools.com/">http://www.voidtools.com/</a>	Para buscar los archivos en el pc
X64dbg	<a href="http://x64dbg.com/">http://x64dbg.com/</a>	Depurador
7zip	<a href="http://www.7-zip.org/download.html">http://www.7-zip.org/download.html</a>	Descomprimir archivos
Uniextractor*	<a href="http://filehippo.com/es/download_universal_extractor/">http://filehippo.com/es/download_universal_extractor/</a>	Extractor de archivos
IDR	<a href="https://web.archive.org/web/20170501145746/http://kpnc.org/idr32/en/">https://web.archive.org/web/20170501145746/http://kpnc.org/idr32/en/</a> <a href="https://github.com/crypto2011/IDR">https://github.com/crypto2011/IDR</a>	Analizador de Delphi (interactive delphi ...)
Notepad ++	<a href="https://notepad-plus-plus.org/">https://notepad-plus-plus.org/</a>	Editar archivos (no hexadecimal)
Hex Workshop	<a href="http://www.hexworkshop.com/">http://www.hexworkshop.com/</a>	Comparar/Editar archivos (hexadecimal)
Free Hex Editor Neo*	<a href="https://www.hhdssoftware.com/free-hex-editor">https://www.hhdssoftware.com/free-hex-editor</a>	Comparar/Editar archivos (hexadecimal)
010 editor*	<a href="https://www.sweetscape.com/010editor/">https://www.sweetscape.com/010editor/</a>	Editor hexadecimal

\*herramienta opcional

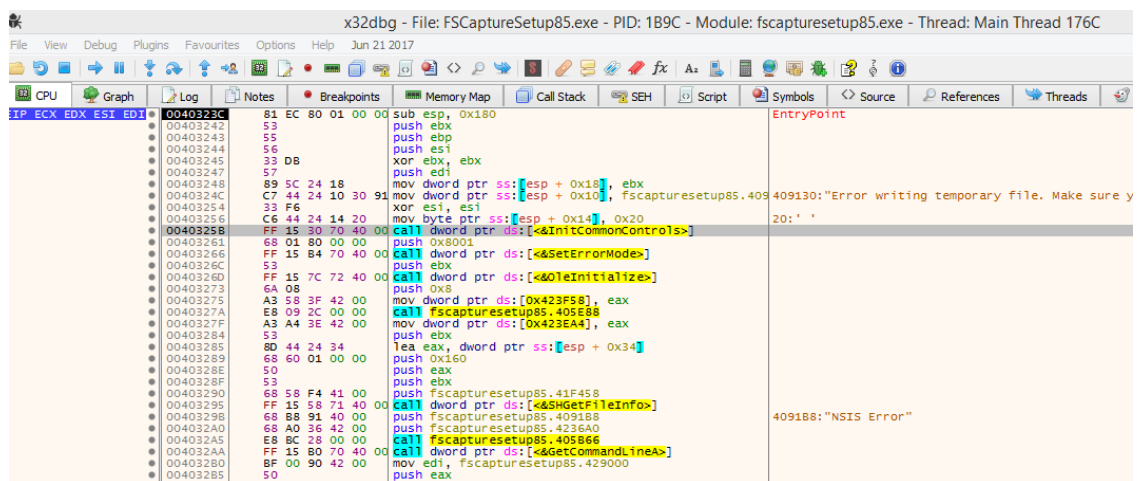
Explorando el Programa 1

Bienvenidos a esta pequeña lectura redactada esta vez por 2 buenos amigos, estamos a cada rato leyendo que este soft esta crackeado por muchos y también existe algún tutorial al respecto, dijimos que cada uno mira de forma distinta así que a unificar criterios y ver si llegamos a lo mismo

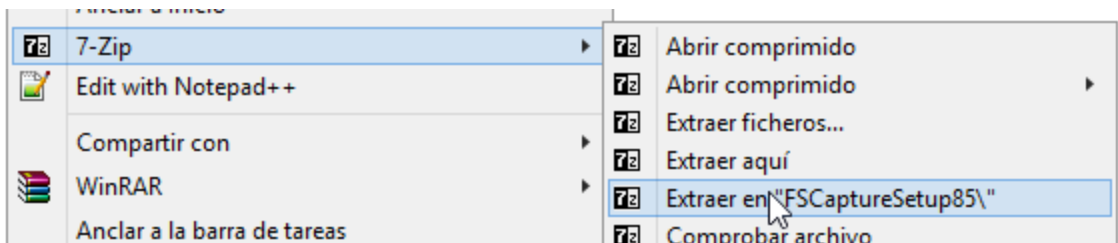











<img1 : Setup de Instalación>

Vemos un icono como nsis, veamos el setup en x64dbg



Confirmado esta en NSIS setup, la gran mayoría de las veces se puede descomprimir con 7z(7zip) o bien Universal Extractor (no usado, pero puede ser recomendado)



Nombre	Fecha de modifica...	Tipo	Tamaño
 \$PLUGINS\DIR	10/07/2017 08:27 ...	Carpeta de archivos	
 FSCapture.exe	08/05/2017 01:06 ...	Aplicación	5.057 KB
 FSCaptureHelp.chm	08/05/2017 01:18 ...	Archivo de Ayuda ...	128 KB
 FSCrossHair.exe	14/01/2016 03:09 ...	Aplicación	409 KB
 FSFocus.exe	14/01/2016 03:19 ...	Aplicación	392 KB
 FSLogo.png	13/12/2006 02:56 a...	Imagen PNG	17 KB
 FSRecorder.exe	08/05/2017 01:23 ...	Aplicación	4.480 KB
 LicenseAgreement.txt	02/05/2017 12:49 ...	Documento de tex...	1 KB
 <b>uninst.exe</b>	10/07/2017 08:21 ...	Aplicación	40 KB

Descripción del archivo: FastStone Capture 8.5 Setup  
 Organización: FastStone Soft  
 Versión del archivo: 8.5.0.0

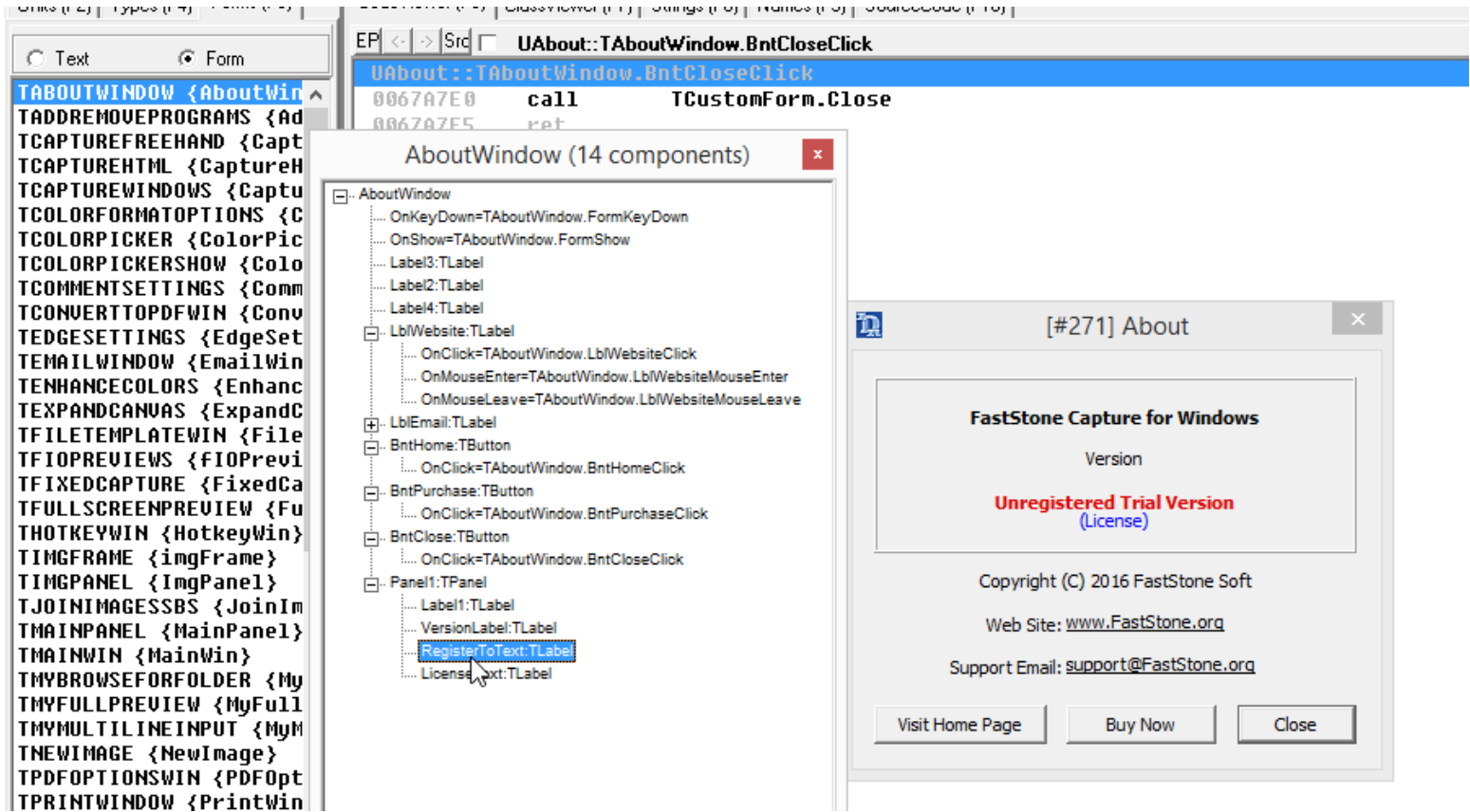
Así que ya tenemos el setup EN PID refiere el FSCapture.exe

```

[= [ ProtectionID v0.6.8.5 DECEMBER]=
(c) 2003-2017 CDKiLLER & TippeX
Build 24/12/16-13:09:21
Ready...
Scanning -> C:\Users\Pc\Downloads\Programs\FSCaptureSetup85\FSCapture.exe
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 5177856 (04F0200h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT)
[TimeStamp] 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT) | PE Header | - | Offset: 0x00000108 | VA: 0x00400108 | -
[File Heuristics] -> Flag #1 : 00000000000001001000000000100000 (0x00048020)
[Entrypoint Section Entropy] : 6.55 (section #0) "CODE " | Size : 0x390FA0 (3739552) byte(s)
[DllCharacteristics] -> Flag : (0x0000) -> NONE
[SectionCount] 8 (0x8) | ImageSize 0x4FD000 (5230592) byte(s)
[VersionInfo] Company Name : FastStone Soft
[VersionInfo] Product Name : FastStone Capture
[VersionInfo] Product Version : 8.5
[VersionInfo] File Description : FastStone Capture
[VersionInfo] File Version : 8.5.0.0
[VersionInfo] Legal Copyrights : Copyright (C) 2017 by FastStone Soft
[ModuleReport] [IAT] Modules -> kernel32.dll | user32.dll | advapi32.dll | oleaut32.dll | kernel32.dll | advapi32.dll | kernel32.dll | version.dll | gdi32.dll | msimg32.dll |
user32.dll | kernel32.dll | oleaut32.dll | ole32.dll | oleaut32.dll | comctl32.dll | imm32.dll | winspool.drv | shell32.dll | shell32.dll | comdlg32.dll | winmm.dll | avifil32.dll |
ole32.dll | MsVfw32.dll | kernel32.dll
[CdKeySerial] found "SerialNumber" @ VA: 0x00145E6C / Offset: 0x0014526C
[CdKeySerial] found "SerialNumber" @ VA: 0x00146CE6 / Offset: 0x001460E6
[CdKeySerial] found "Trial version" @ VA: 0x002A2478 / Offset: 0x002A1878
[CdKeySerial] found "Trial period" @ VA: 0x002A2490 / Offset: 0x002A1890
[CdKeySerial] found "Unregistered" @ VA: 0x0033FE00 / Offset: 0x0033F200
[CdKeySerial] found "Invalid code" @ VA: 0x003A3D96 / Offset: 0x003A3196
[CdKeySerial] found "Unregistered" @ VA: 0x0041EEB2 / Offset: 0x004126B2
[CdKeySerial] found "Trial version" @ VA: 0x0041EEBF / Offset: 0x004126BF
[CdKeySerial] found "Registration Code" @ VA: 0x0043C8DA / Offset: 0x004300DA
[CdKeySerial] found "Registration Code" @ VA: 0x00447B7B / Offset: 0x0043B37B
[CdKeySerial] found "Trial version" @ VA: 0x004C35D2 / Offset: 0x004B6DD2
[CdKeySerial] found "Trial period" @ VA: 0x004C3600 / Offset: 0x004B6E00
[CdKeySerial] found "Trial version" @ VA: 0x004C375F / Offset: 0x004B6F5F
[CdKeySerial] found "Registration Code" @ VA: 0x004C388B / Offset: 0x004B708B
[CdKeySerial] found "Registration Code" @ VA: 0x004FB2FF / Offset: 0x004EEAFF
[CdKeySerial] found "Registration Code" @ VA: 0x004FB345 / Offset: 0x004EEB45
[CdKeySerial] found "Registration Code" @ VA: 0x004FB720 / Offset: 0x004EEF20
[CompilerDetect] -> Borland Delphi 6
[!] File appears to have no protection or is using an unknown protection
- Scan Took : 1.610 Second(s) [00000056Eh (1390) tick(s)] [506 of 580 scan(s) done]

```

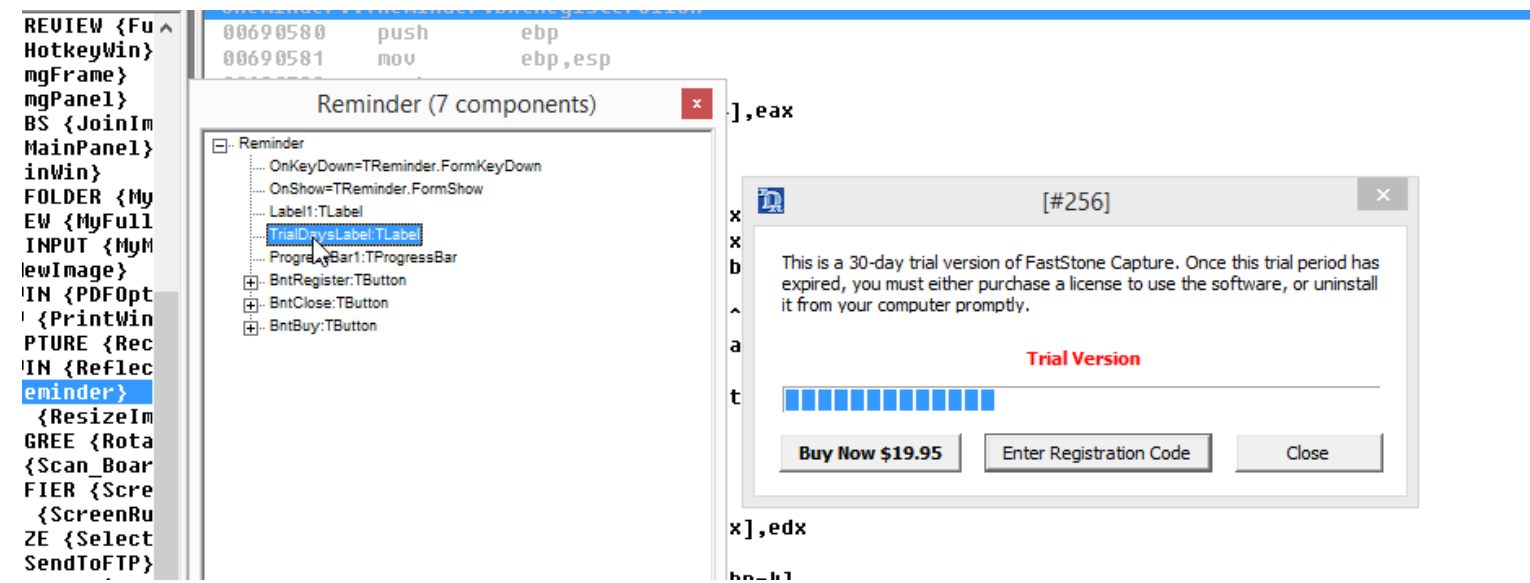
Para un archivo hecho en delphi, suele ser un buen comienzo conocer los form en IDR, además vemos que no trae packer (antiguamente leía que le colocaban upx)



<img5 IDR: About en FastStone Capture>

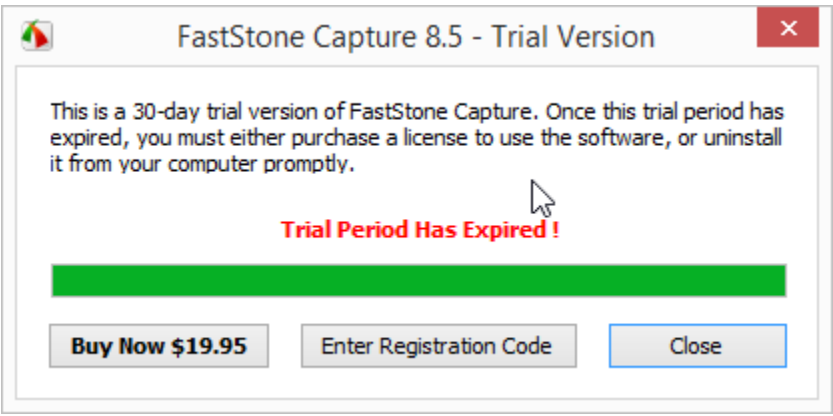
Desde el about tendremos nuestra version y licencia (license en inglés)

La segunda llamativa se llama Reminder.



<img6 IDR: Reminder-NAG- en FastStone Capture>

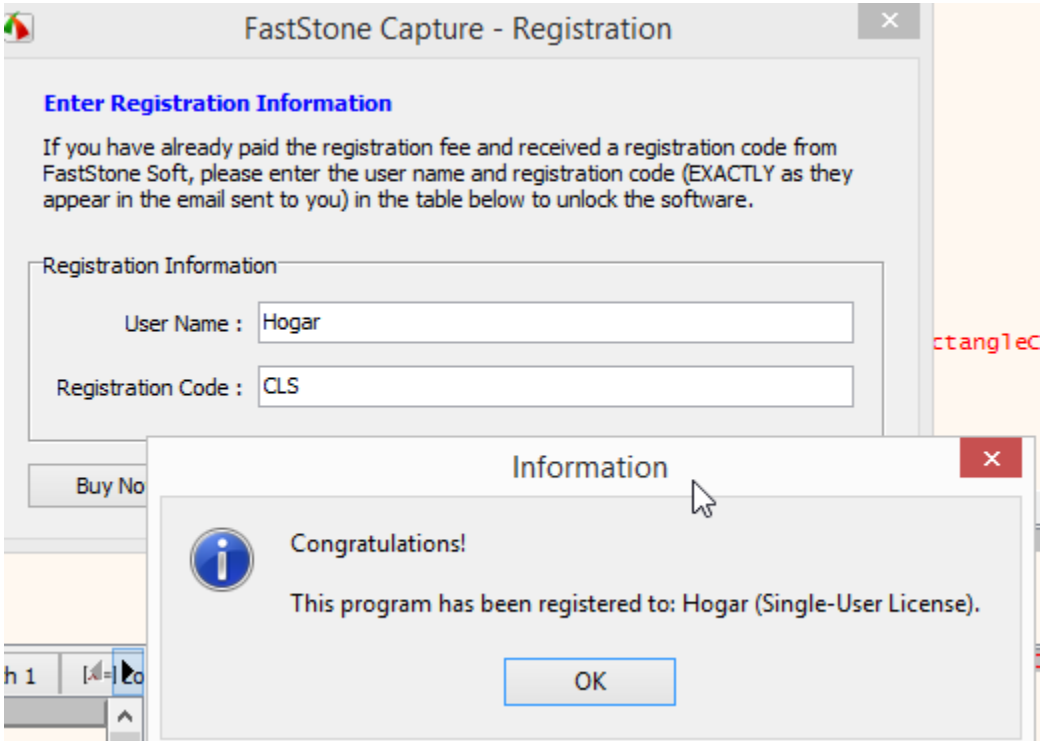
Comenzamos: Lo mas básico es comenzar expirado así me aseguro que debemos hacer mucho. (Desde idr, es ideal que conozcan los Form Show, desde ahí comenzar a depurar (no mostrado para que exploren IDR)



<img7 IDR: FastStone Capture Expired>

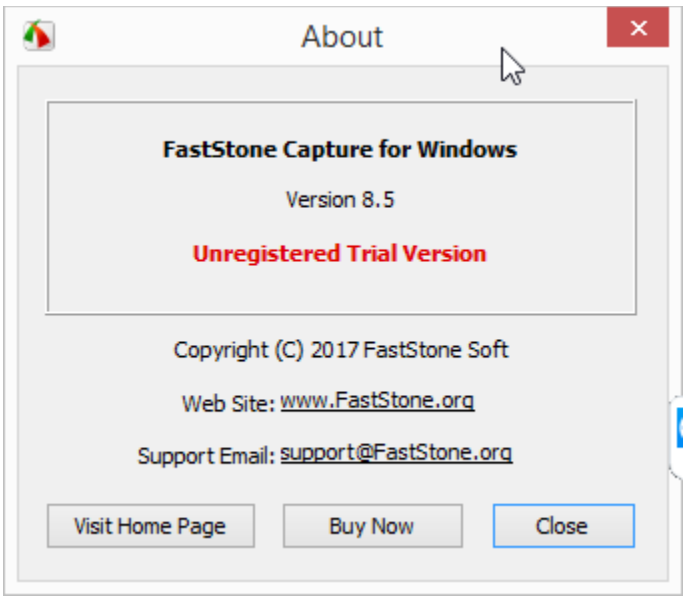
La idea es revivir el muerto ☺

Colocamos enter Registration code y con las direcciones desde el map, labels de idr, tenemos identificado 2 zonas importantes (ingresar la licencia y comparar la licencia) Identificamos un chico malo y mensajes de gracias por registrar, si evitamos que vaya a chico malo tenemos



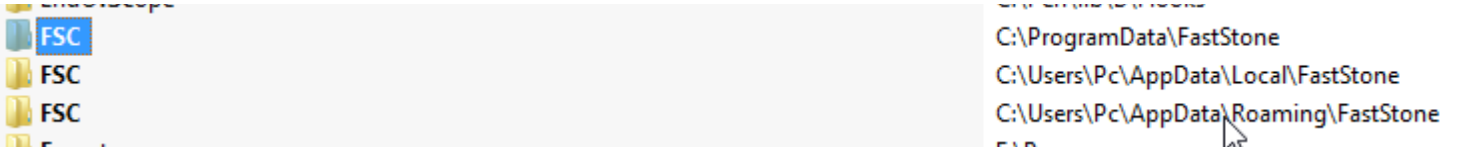
<img8 Programa: cuando el programa ha sido crackeado, permite cualquier valor de licencia>

Por lo que entra al programa pero about no ha validado el tipo de version.



<img9 Programa: pero de nuevo valida en about la licencia, así que estamos con doble validación>

El programa aunque acepto el programa ha creado en 3 rutas distintas una clave



<img10 Everything: al buscar faststone aparece una nueva carpeta llamada FSC ([F]ast [S]tone [C]apture)>

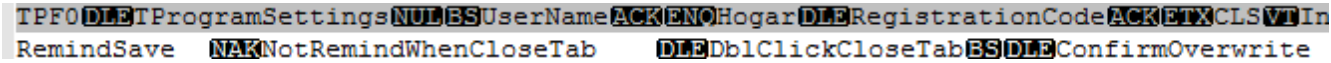
%USERPROFILE%\AppData\Local\FastStone\FSC

%USERPROFILE%\AppData\Roaming\FastStone\FSC

%PROGRAMDATA%\FastStone\FSC

Dentro de ello un archivo db llamado FSC.db

Que en su interior contiene la información ingresada hace no mucho (Hogar-CLS)

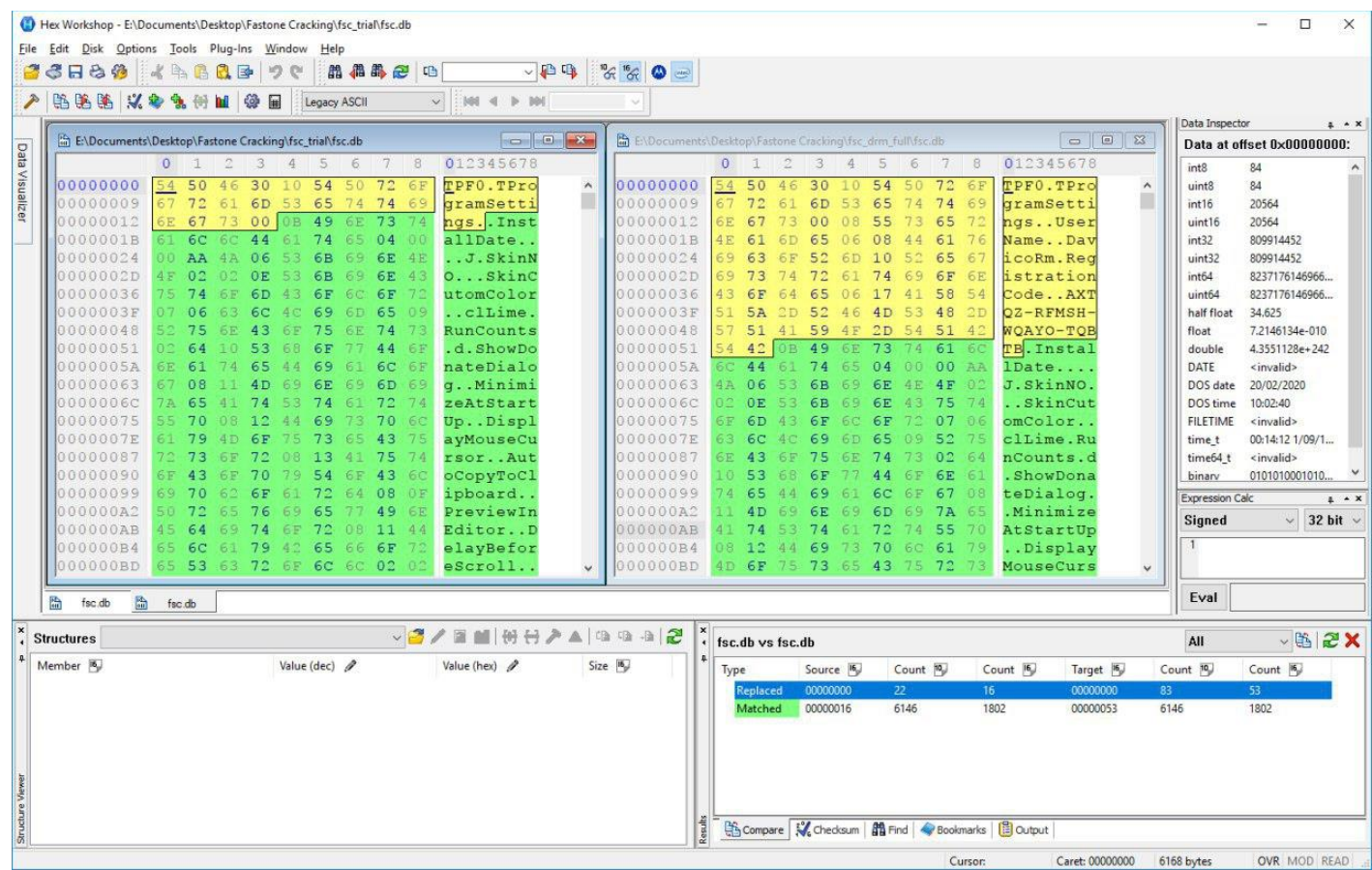


<img11 Notepad++: contenido del FSC.db>

Por lo que realmente no existe validación de tiempo una vez que se ha registrado aunque hubiese sido forzado, y esto corresponde a un stream (TPF0) <https://www.freepascal.org/docs-html/rtl/classes/filesignature.html> (Constant that is found at the start of a binary stream containing a streamed component.)



Si comparamos antes y después para que se vea mejor (herramienta hexadecimal) hex work shop vemos que es mas legible el cambio esta asociado solo al username y registration code., también se puede hacer uso de Free Hex Editor Neo.



<img12 hex workshop: comparando el archivo db>

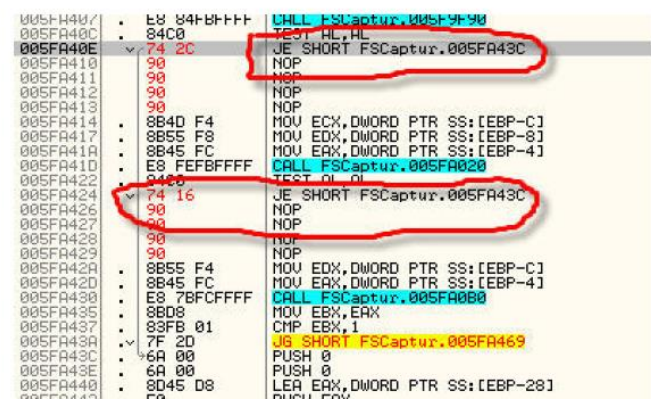
Lo demás es estético, puedes editar a gusto el Username y el registration code en este archivo, el descubrimiento de este archivo hace la diferencia (usarlo en trial, usarlo en Expired, usarlo licenciado) aun estando en expired permite abrirlo si aparecen las ramas de registrado.

Si estas licenciado y borras los 3 archivos, puedes volver a estar expired.

Y luego como ya tenemos con la licencia (3 archivos) solo falta lo estético, en general forzar saltos (JMP) o anular saltos (NOP), para guiarnos puede usarse algún escrito del pasado FastStone Capture v 6.1 por Kernel065, faststone por Softdat (video tutorial), FastStone por X.O (escrito), sea como sea llegamos a decir lo mismo, el programa no varia mucho con el tiempo.

Retomemos el escrito de teoría 1136, para ver que cosa podemos comentar:

saltos al chico malo, esto significa que si cambiamos el JE 5FA5D9 por JE 5FA43C estaremos registrados hagámoslo para ver que pasa.



Quedaría algo así luego le damos salvar pero con otro nombre por si no funciona, yo lo guarde con el nombre FSCapture\_Dump\_1.

<img13 tutorial teoría 1136: una sugerencia hacia lo visto del pasado>

Vemos que comenta que puede forzarse algunos saltos como je a jne pero aquí hay un error lógico, así que en consecuencia cuando crackeamos algo que alguien si ha comprado, no le quedará funcional, porque el salto je a jne solo hará la diferencia que si es no registrado va al registred, y si es registrado va al no registrado, ¿que pasa si yo tengo un serial valido? Entonces el salto lo que hará es pensar que está No registrado y expirará, por otro lado, lo demás del tutorial esta correcto el programa es fácilmente distinguir los chicos buenos y malos y es solo modificar los saltos tal cual como figura. Lo importante siempre es que tenga los valores básicos necesarios (ingresar usuario/serial)

Recreamos la hazaña en 2 pasos

- 1) Que vaya sin pasar a la validación errónea. ese jne a NOP o jmp un lugar (hay como 4 comparaciones con “al,al” , luego ebx)

0068B7F3	E8 F8 EF FF FF	call fscapture.68A7F0	
0068B7F8	84 C0	test al, al	
0068B7FA	0F 85 9C 02 00 00	jne <fscapture.chico_malo>	salto definitivo
0068B800	8B 55 FC	mov edx, dword ptr ss:[ebp - 0x4]	
0068B803	8B C6	mov eax, esi	
0068B805	E8 96 F0 FF FF	call fscapture.68A8A0	
0068B80A	84 C0	test al, al	
0068B80C	0F 85 8A 02 00 00	jne <fscapture.chico_malo>	
0068B812	8B 4D F8	mov ecx, dword ptr ss:[ebp - 0x8]	
0068B815	8B 55 FC	mov edx, dword ptr ss:[ebp - 0x4]	
0068B818	8B C6	mov eax, esi	
0068B81A	E8 61 FB FF FF	call fscapture.68B380	
0068B81F	84 C0	test al, al	
0068B821	0F 84 75 02 00 00	je <fscapture.chico_malo>	
0068B827	8B 4D F8	mov ecx, dword ptr ss:[ebp - 0x8]	
0068B82A	8B 55 FC	mov edx, dword ptr ss:[ebp - 0x4]	
0068B82D	8B C6	mov eax, esi	
0068B82F	E8 DC FB FF FF	call fscapture.68B410	
0068B834	84 C0	test al, al	
0068B836	0F 84 60 02 00 00	je <fscapture.chico_malo>	
0068B83C	8B 55 F8	mov edx, dword ptr ss:[ebp - 0x8]	
0068B83F	8B C6	mov eax, esi	
0068B841	E8 5A FC FF FF	call fscapture.68B4A0	
0068B846	48	dec eax	
0068B847	0F 8C 4F 02 00 00	j1 <fscapture.chico_malo>	
0068B84D	8B 55 F8	mov edx, dword ptr ss:[ebp - 0x8]	
0068B850	8B C6	mov eax, esi	
0068B852	E8 49 FC FF FF	call fscapture.68B4A0	
0068B857	8B D8	mov ebx, eax	
0068B859	83 FB 01	cmp ebx, 0x1	ebx indica cantidad de licencias
0068B85C	7F 40	jg fscapture.68B89E	
0068B85E	6A 00	push 0x0	
0068B860	8B C6	mov eax, esi	
0068B862	E8 75 A4 DC FF	call fscapture.455CDC	
0068B867	50	push eax	
0068B868	6A 00	push 0x0	

<img14 x32dbg: validación del serial desde el form de ingresar licencia>

- 2) Que acepte el serial como valido con los valores en ebx con el nivel de licencia que queramos. Según el valor de ebx , ahora bien hemos atacado a la enter serial

Respecto al about si valida el largo del nombre y serial (nombre no puede ser nulo) y serial debe ser de 0x17 hexadecimal o 23 decimal (hay como 4 comparaciones con “al,al”, luego esi para la cantidad de licencias)

0068C456	8B 46 34	mov eax, dword ptr ds:[esi + 0x34]	
0068C459	E8 1E 8A D7 FF	call <fscapture.System.@LStrCat>	
0068C45E	83 F8 17	cmp eax, 0x17	cmp eax,17
0068C461	0F 85 79 02 00 00	jne fscapture.68C6E0	
0068C467	33 C0	xor eax, eax	
0068C469	55	push ebp	
0068C46A	68 D9 C6 68 00	push <fscapture.sub_68C6D9>	

<img15 x32dbg: validación del serial desde about>

Solo necesitamos que llegue a algún valor de esi esperado

0068C583	E8 3C 2F DC FF	call fscapture.44F4C4	
0068C588	83 FE 01	cmp esi, 0x1	
0068C58B	75 15	jne fscapture.68C5A2	
0068C58D	8B 83 20 03 00 00	mov eax, dword ptr ds:[ebx + 0x320]	
0068C593	BA 48 C7 68 00	mov edx, fscapture.68C748	68C748:"(Single-User License)"
0068C598	E8 27 2F DC FF	call fscapture.44F4C4	
0068C59D	E9 CF 00 00 00	jmp fscapture.68C671	
0068C5A2	81 FE 57 04 00 00	cmp esi, 0x457	
0068C5A8	75 15	jne fscapture.68C5BF	
0068C5AA	8B 83 20 03 00 00	mov eax, dword ptr ds:[ebx + 0x320]	
0068C5B0	BA 68 C7 68 00	mov edx, fscapture.68C768	68C768:"(Family License that covers up to 5 compu
0068C5B5	E8 0A 2F DC FF	call fscapture.44F4C4	
0068C5BA	E9 B2 00 00 00	jmp fscapture.68C671	
0068C5BF	81 FE 85 13 00 00	cmp esi, 0x1385	
0068C5C5	75 15	jne fscapture.68C5DC	
0068C5C7	8B 83 20 03 00 00	mov eax, dword ptr ds:[ebx + 0x320]	
0068C5D0	BA A0 C7 68 00	mov edx, fscapture.68C7A0	68C7A0:"(Educational Site License)"
0068C5D2	E8 ED 2E DC FF	call fscapture.44F4C4	
0068C5D7	E9 95 00 00 00	jmp fscapture.68C671	
0068C5DC	81 FE 86 13 00 00	cmp esi, 0x1386	
0068C5E2	75 12	jne fscapture.68C5F6	
0068C5E4	8B 83 20 03 00 00	mov eax, dword ptr ds:[ebx + 0x320]	
0068C5EA	BA C4 C7 68 00	mov edx, fscapture.68C7C4	68C7C4:"(Educational Worldwide License)"
0068C5EF	E8 D0 2E DC FF	call fscapture.44F4C4	
0068C5F4	E9 7B 00 00 00	jmp fscapture.68C671	
0068C5F6	81 FE 87 13 00 00	cmp esi, 0x1387	
0068C5FC	75 12	jne fscapture.68C610	
0068C5FE	8B 83 20 03 00 00	mov eax, dword ptr ds:[ebx + 0x320]	
0068C604	BA EC C7 68 00	mov edx, fscapture.68C7EC	68C7EC:"(Corporate Site License)"
0068C609	E8 B6 2E DC FF	call fscapture.44F4C4	

<img16 x32dbg: validación del número de licencias desde about>

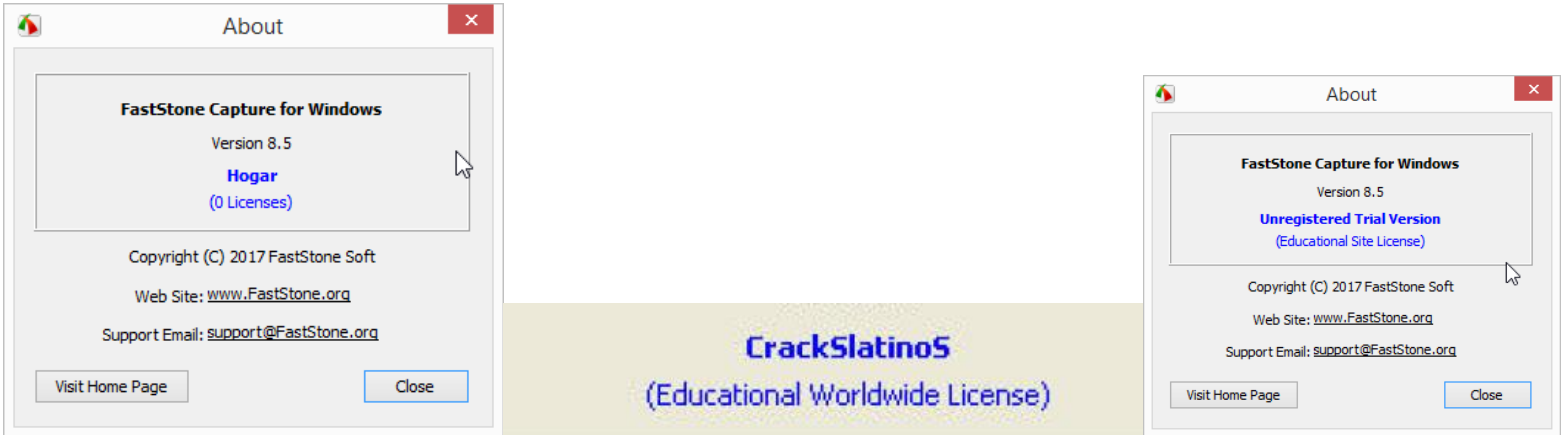
Para eso solo basta algunos valores de cl (en este caso esta en 1)

0068C4E1	A1 78 6E 7A 00	mov eax, dword ptr ds:[0x7A6E78]	
0068C4E6	8B 56 30	mov edx, dword ptr ds:[esi + 0x30]	
0068C4E9	8B 45 FC	mov eax, dword ptr ss:[ebp - 0x4]	
0068C4EC	E8 8F EE FF FF	call fscapture.68B380	
0068C4F1	84 C9	test cl, cl	
0068C4F3	0F 84 CA 01 00 00	je fscapture.68C6C3	
0068C4F9	A1 78 6E 7A 00	mov eax, dword ptr ds:[0x7A6E78]	
0068C4FE	8B 00	mov eax, dword ptr ds:[eax]	
0068C500	8B B8 CC 06 00 00	mov edi, dword ptr ds:[eax + 0x6CC]	
0068C506	8B 4F 34	mov ecx, dword ptr ds:[edi + 0x34]	
0068C509	A1 78 6E 7A 00	mov eax, dword ptr ds:[0x7A6E78]	
0068C50E	8B 57 30	mov edx, dword ptr ds:[edi + 0x30]	
0068C511	8B 45 FC	mov eax, dword ptr ss:[ebp - 0x4]	
0068C514	E8 F7 EE FF FF	call fscapture.68B410	
0068C519	84 C9	test cl, cl	

<img17 x32dbg: usando la sugerencia cambiar de “al,al” a “cl,cl” >

Y forzar los saltos o nop para ello (llegará a donde refiere el otro escrito





<img18-19-20 Programa: viendo los mensajes desde about>

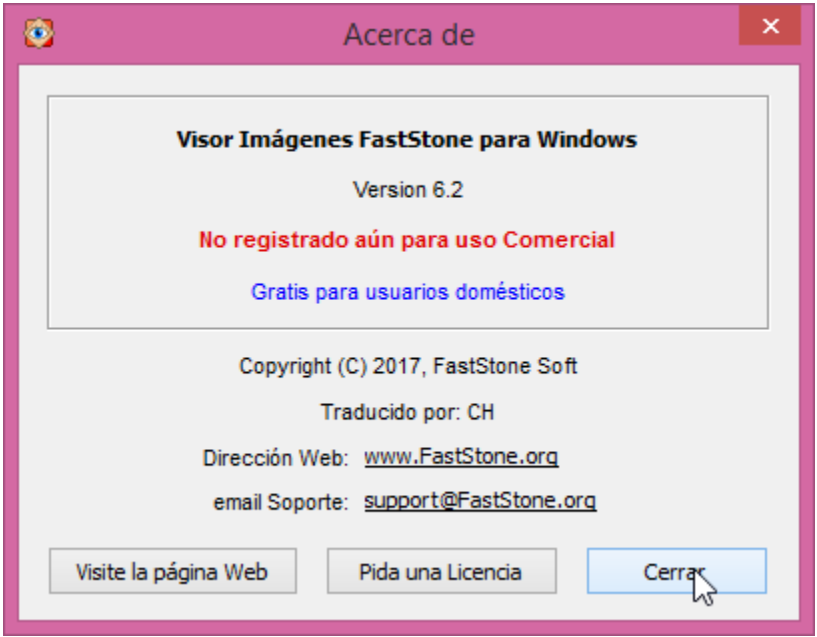
La primera imagen paso la validación, pero no tiene licencias, la segunda cambiamos el nombre, pero no altera el registro, esi es un valor alto, en cambio si no modificamos nada considerable, muestra registrado pasa al mov al,2 y muestra unregistred trial version, pero dado que ya valido que esta registrado muestra en otro color (azul) en conclusión, puede tener el nombre que queramos y licencia que queramos, solo dependerá hacia donde saltará.

## Explorando el Programa 2

Al revisar el programa 2 ya sabemos que encontraremos una realidad similar, pero veamos que tan diferente, pid refiere que también está en delphi 6

```
==[ ProtectionID v0.6.8.5 DECEMBER]==-
(c) 2003-2017 CDKiLLER & TippeX
Build 24/12/16-13:09:21
Ready...
Scanning -> C:\Users\Pc\Downloads\Programs\FSViewerSetup62\FSViewer.exe
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 6372352 (0613C00h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT)
[TimeStamp] 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT) | PE Header | - | Offset: 0x00000108 | VA: 0x00400108 | -
[File Heuristics] -> Flag #1 : 00000000000001001100000000100000 (0x0004C020)
[Entrypoint Section Entropy] : 6.54 (section #0) "CODE " | Size : 0x4E07C4 (5113796) byte(s)
[DllCharacteristics] -> Flag : (0x0000) -> NONE
[SectionCount] 8 (0x8) | ImageSize 0x628000 (6455296) byte(s)
[VersionInfo] Company Name : FastStone Soft
[VersionInfo] Product Name : FastStone Image Viewer
[VersionInfo] Product Version : 6.2
[VersionInfo] File Description : FastStone Image Viewer
[VersionInfo] File Version : 6.2.0.0
[VersionInfo] Legal Copyrights : Copyright (C) 2017 by FastStone Soft
[ModuleReport] [IAT] Modules -> kernel32.dll | user32.dll | advapi32.dll | oleaut32.dll | kernel32.dll | advapi32.dll | kernel32.dll | version.dll | gdi32.dll | msimg32.dll |
user32.dll | kernel32.dll | oleaut32.dll | ole32.dll | oleaut32.dll | comctl32.dll | imm32.dll | winspool.drv | shell32.dll | shell32.dll | comdlg32.dll | ole32.dll | kernel32.dll
| avifil32.dll | ole32.dll | MsVfW32.dll | winmm.dll | kernel32.dll | quartz.dll
[CdKeySerial] found "SerialNumber" @ VA: 0x001048FC / Offset: 0x00103CFC
[CdKeySerial] found "SerialNumber" @ VA: 0x00105776 / Offset: 0x00104B76
[CdKeySerial] found "Invalid code" @ VA: 0x004F2DE9 / Offset: 0x004F19E9
[CdKeySerial] found "Invalid code" @ VA: 0x004F2E06 / Offset: 0x004F1A06
[CdKeySerial] found "Invalid code" @ VA: 0x004FF4C2 / Offset: 0x004FE0C2
[CdKeySerial] found "Registration Code" @ VA: 0x005AEF8D / Offset: 0x0059AF8D
[CdKeySerial] found "Registration Code" @ VA: 0x005ECB67 / Offset: 0x005D8B67
[CdKeySerial] found "Registration Code" @ VA: 0x00623350 / Offset: 0x0060F350
[CdKeySerial] found "Registration Code" @ VA: 0x00623396 / Offset: 0x0060F396
[CdKeySerial] found "Registration Code" @ VA: 0x006237C5 / Offset: 0x0060F7C5
[CdKeySerial] found "Registration Code" @ VA: 0x00623CE6 / Offset: 0x0060FCE6
[CompilerDetect] -> Borland Delphi 6
[!] File appears to have no protection or is using an unknown protection
- Scan Took : 1.516 Second(s) [0000005CCh (1484) tick(s)] [506 of 580 scan(s) done]
```

El About refiere



<img21 programa2>

Veamos que tal nos va

006E3F92	33 C0	xor eax, eax	chicomalo
006E3F94	5A	pop edx	
006E3F95	59	pop ecx	
006E3F96	59	pop ecx	
006E3F97	64 89 10	mov dword ptr [eax], edx	
006E3F9A	E9 FD 01 00 00	jmp fsviewer.6E419C	
006E3F9F	8D 45 EC	lea eax, dword ptr ss:[ebp - 0x14]	
006E3FA2	50	push eax	
006E3FA3	B9 08 00 00 00	mov ecx, 0x8	
006E3FA8	BA 01 00 00 00	mov edx, 0x1	
006E3FAD	8B 45 D8	mov eax, dword ptr ss:[ebp - 0x28]	
006E3FB0	E8 E7 11 D2 FF	call <fsviewer.System.@LStrCopy>	
006E3FB5	8D 45 E8	lea eax, dword ptr ss:[ebp - 0x18]	
006E3FB8	E8 BF 0C D2 FF	call <fsviewer.System.@LStrClr>	
006E3FBD	BB 01 00 00 00	mov ebx, 0x1	
006E3FC2	BE 01 00 00 00	mov esi, 0x1	
006E3FC7	BF 01 00 00 00	mov edi, 0x1	
006E3FCC	E8 63	jmp fsviewer.6E4031	
006E3FCE	8B C7	mov eax, edi	
006E3FD0	25 01 00 00 80	and eax, 0x80000001	
006E3FD5	79 05	jns fsviewer.6E3FDC	
006E3FD7	48	dec eax	
006E3FD8	83 C8 FE	or eax, 0FFFFFFF	
006E3FDB	40	inc eax	
006E3FDC	85 C0	test eax, eax	

<img22 programa2 en x32dbg>

Comencemos a ver

006E3EC1	8B 45 F4	mov eax, dword ptr ss:[ebp - 0x4]	
006E3EC4	E8 E7 72 D2 FF	call <fsviewer.SysUtils.Trim>	
006E3EC9	8B 45 D4	mov eax, dword ptr ss:[ebp - 0x2C]	
006E3ECC	8D 55 D8	lea edx, dword ptr ss:[ebp - 0x28]	
006E3ECF	E8 84 6E D2 FF	call <fsviewer.SysUtils.UpperCase>	
006E3ED1	83 7D E4 00	cmp dword ptr ss:[ebp - 0x1C], 0x0	valida nombre
006E3ED8	75 0D	jne fsviewer.6E3EE7	
006E3EDA	33 C0	xor eax, eax	
006E3EDC	5A	pop edx	
006E3EDD	59	pop ecx	
006E3EDE	59	pop ecx	
006E3EDF	64 89 10	mov dword ptr [eax], edx	
006E3EE2	E9 B5 02 00 00	jmp fsviewer.6E419C	si no hay nombre chico malo
006E3EE7	83 7D D8 00	cmp dword ptr ss:[ebp - 0x28], 0x0	
006E3EEB	75 0D	jne fsviewer.6E3EFA	
006E3EED	33 C0	xor eax, eax	
006E3EEF	5A	pop edx	
006E3EF0	59	pop ecx	

<img23 programa2 en x32dbg>

Valida los 0x17 , (que tienen un formato AAAA-BBBB-CCCC-DDDD-EEEE) luego será validado de 0x14 (el mismo sin -) , luego de pasar los filtros el programa queda registrado.

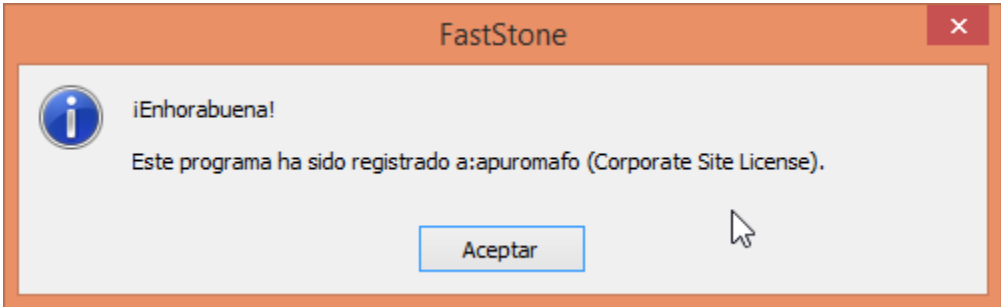
006E42DD	8D 55 D8	lea edx, dword ptr ss:[ebp - 0x28]	
006E42E0	E8 73 6A D2 FF	call <fsviewer.SysUtils.UpperCase>	
006E42E5	8B 45 D8	mov eax, dword ptr ss:[ebp - 0x28]	
006E42E8	E8 57 0C D2 FF	call <fsviewer.System.@LStrLen>	
006E42ED	83 F8 17	cmp eax, 0x17	
006E42F0	75 71	jne fsviewer.6E4363	
006E42F2	8D 45 D0	lea eax, dword ptr ss:[ebp - 0x30]	
006E42F5	50	push eax	
006E42F6	B9 05 00 00 00	mov ecx, 0x5	
006E42FB	BA 01 00 00 00	mov edx, 0x1	
006E4300	8B 45 D8	mov eax, dword ptr ss:[ebp - 0x28]	
006E4303	E8 94 0E D2 FF	call <fsviewer.System.@LStrCopy>	
006E4308	FF 75 D0	push dword ptr ss:[ebp - 0x30]	
006E430B	8D 45 CC	lea eax, dword ptr ss:[ebp - 0x34]	
006E430F	50	push eax	

<img24 programa2 en x32dbg>

En resumen lo que importa es al salir de toda la función y cuando este es comparado a los niveles de licencia:

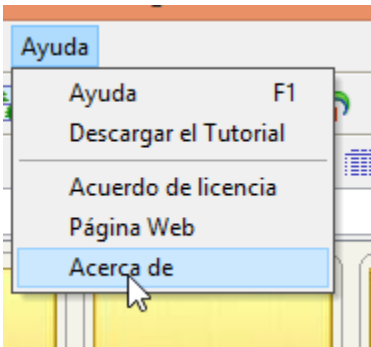
006E4A3A	E8 CD 00 FD FF	call <fsviewer.MyMessenger.sub_006B4B0C>	
006E4A3F	E9 57 01 00 00	jmp fsviewer.6E4B9B	
006E4A44	81 FB 87 13 00 00	cmp ebx, 0x1387	
006E4A4A	75 74	jne fsviewer.6E4AC0	
006E4A4C	66 A1 EC 4C 6E 00	mov ax, word ptr ds:[0x6E4CEC]	
006E4A52	50	push eax	
006E4A53	6A 00	push 0x0	
006E4A55	8B C6	mov eax, esi	
006E4A57	E8 08 9F D7 FF	call <fsviewer.Controls.TwinControl1.GetHandle>	
006E4A5C	50	push eax	
006E4A5D	6A 00	push 0x0	
006E4A5F	6A 00	push 0x0	
006E4A61	8D 45 C4	lea eax, dword ptr ss:[ebp - 0x3C]	
006E4A64	50	push eax	

<img25 programa2 en x32dbg>



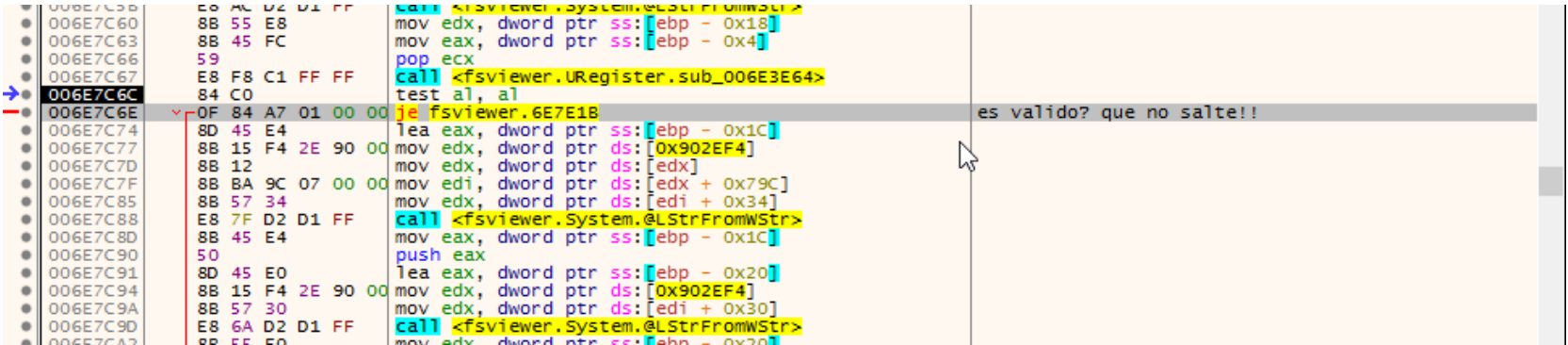
<img26 programa2 en x32dbg ha caído >

El about cambia

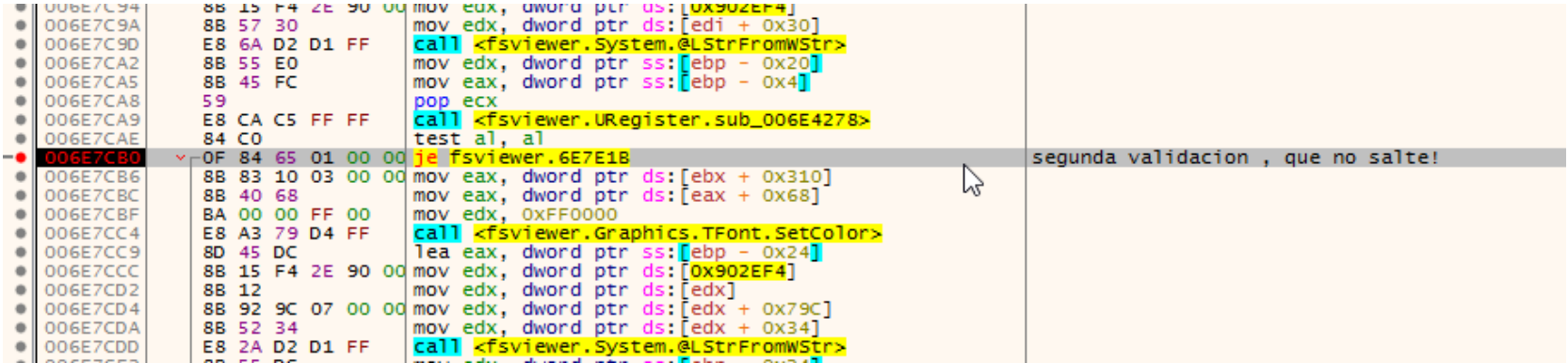


<img27 programa2 en ayuda ha cambiado su formato>

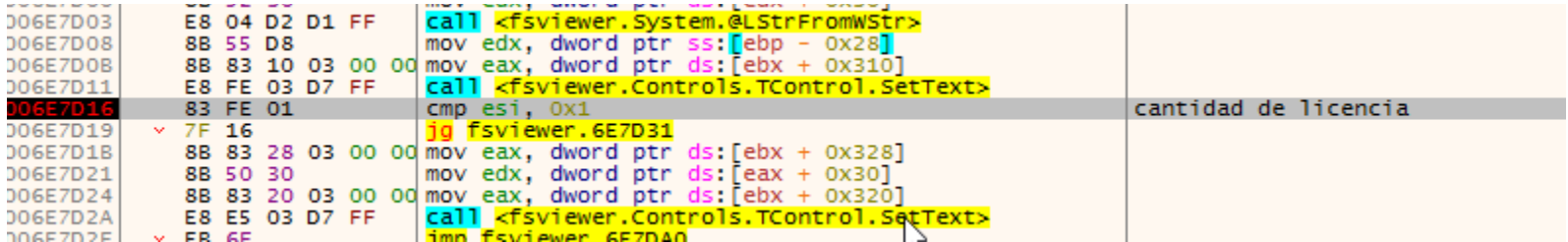
Resumimos los pasos



<img28 programa2 en x32dbg validación de los saltos validados en al,al>

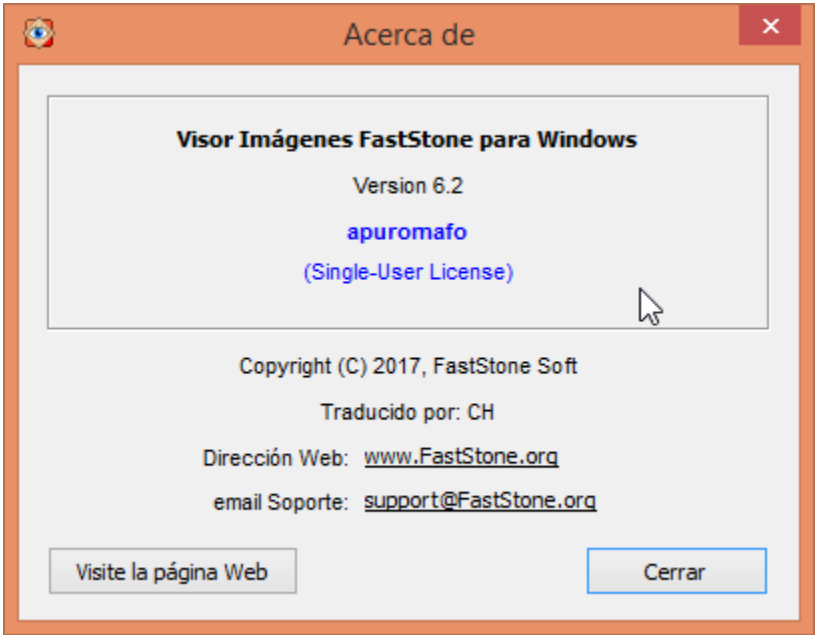


<img29 programa2 en x32dbg validación de los saltos validados en al,al>



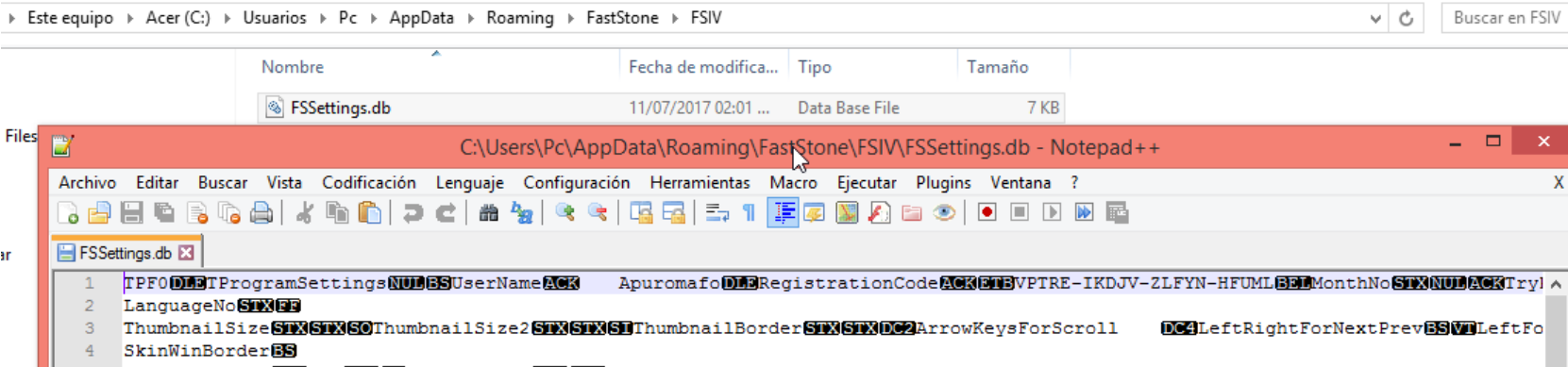
<img30 programa2 en x32dbg validación de licencias en esi>

Veamos que queda del experimento



<img31 programa2 about con los cambios hechos>

Para este programa 2 , solo ha guardado 1 lugar (roaming) en FSSettings.db



<img32 programa2 licencia guardada>

En ese lugar almacena la licencia y tiempo de uso.

### Explorando el Programa 3

Comenzamos con 7zip, luego en la ruta el exe mas importante con PID

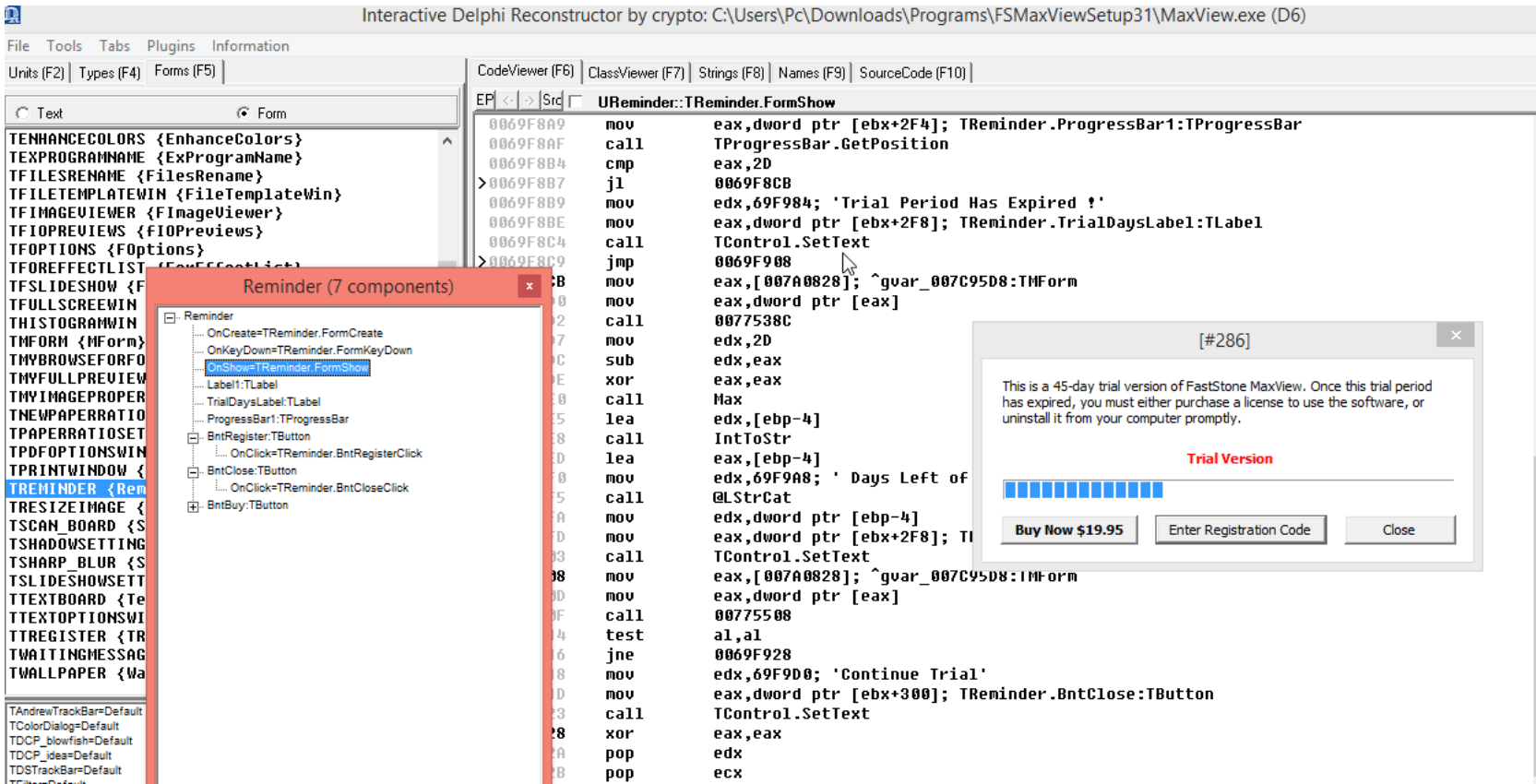
```

-=[ ProtectionID v0.6.8.5 DECEMBER]=-
(c) 2003-2017 CDKILLER & TippeX
Build 24/12/16-13:09:21
Ready...
Scanning -> C:\Users\PC\Downloads\Programs\FsMaxViewSetup31\MaxView.exe
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 4378624 (042D000h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT)
[TimeStamp] 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT) | PE Header | - | Offset: 0x00000108 | VA: 0x00400108 | -
[File Heuristics] -> Flag #1 : 00000000000001001100000000100000 (0x0004C020)
[Entrypoint Section Entropy] : 6.57 (section #0) "CODE " | Size : 0x37870C (3639052) byte(s)
[DllCharacteristics] -> Flag : (0x0000) -> NONE
[SectionCount] 8 (0x8) | ImageSize 0x45A000 (4562944) byte(s)
[VersionInfo] Company Name : FastStone Soft
[VersionInfo] Product Name : FastStone MaxView
[VersionInfo] Product Version : 3.1
[VersionInfo] File Description : FastStone MaxView
[VersionInfo] File Version : 3.1.0.0
[VersionInfo] Legal Copyrights : Copyright (C) 2017 by FastStone Soft
[ModuleReport] [IAT] Modules -> kernel32.dll | user32.dll | advapi32.dll | oleaut32.dll | kernel32.dll | advapi32.dll | kernel32.dll | version.dll | gdi32.dll | msimg32.dll |
user32.dll | kernel32.dll | oleaut32.dll | ole32.dll | oleaut32.dll | comctl32.dll | imm32.dll | winspool.driv | shell32.dll | shell32.dll | comdlg32.dll | winmm.dll | ole32.dll |
kernel32.dll | avifil32.dll | ole32.dll | MsVfw32.dll | kernel32.dll | quartz.dll
[CdKeySerial] found "SerialNumber" @ VA: 0x00136C5C / Offset: 0x0013605C
[CdKeySerial] found "SerialNumber" @ VA: 0x00137AD6 / Offset: 0x00136ED6
[CdKeySerial] found "Trial version" @ VA: 0x0029F96C / Offset: 0x0029ED6C
[CdKeySerial] found "Trial period" @ VA: 0x0029F984 / Offset: 0x0029ED84
[CdKeySerial] found "Invalid code" @ VA: 0x0038B235 / Offset: 0x00389E35
[CdKeySerial] found "Invalid code" @ VA: 0x0038B252 / Offset: 0x00389E52
[CdKeySerial] found "Invalid code" @ VA: 0x0039DEC2 / Offset: 0x0039CAC2
[CdKeySerial] found "Unregistered" @ VA: 0x0041C69C / Offset: 0x003EF69C
[CdKeySerial] found "Trial version" @ VA: 0x0041C6A9 / Offset: 0x003EF6A9
[CdKeySerial] found "Registration Code" @ VA: 0x0043BF00 / Offset: 0x0040EF00
[CdKeySerial] found "Trial version" @ VA: 0x00446E7F / Offset: 0x00419E7F
[CdKeySerial] found "Trial period" @ VA: 0x00446EAD / Offset: 0x00419EAD
[CdKeySerial] found "Trial version" @ VA: 0x0044700C / Offset: 0x0041A00C
[CdKeySerial] found "Registration Code" @ VA: 0x00447138 / Offset: 0x0041A138
[CdKeySerial] found "Registration Code" @ VA: 0x004580AE / Offset: 0x0042B0AE
[CdKeySerial] found "Registration Code" @ VA: 0x004580F4 / Offset: 0x0042B0F4
[CdKeySerial] found "Registration Code" @ VA: 0x00458358 / Offset: 0x0042B358
[CompilerDetect] -> Borland Delphi 6
[!] File appears to have no protection or is using an unknown protection
- Scan Took : 1.953 Second(s) [000000417h (1047) tick(s)] [506 of 580 scan(s) done]

```

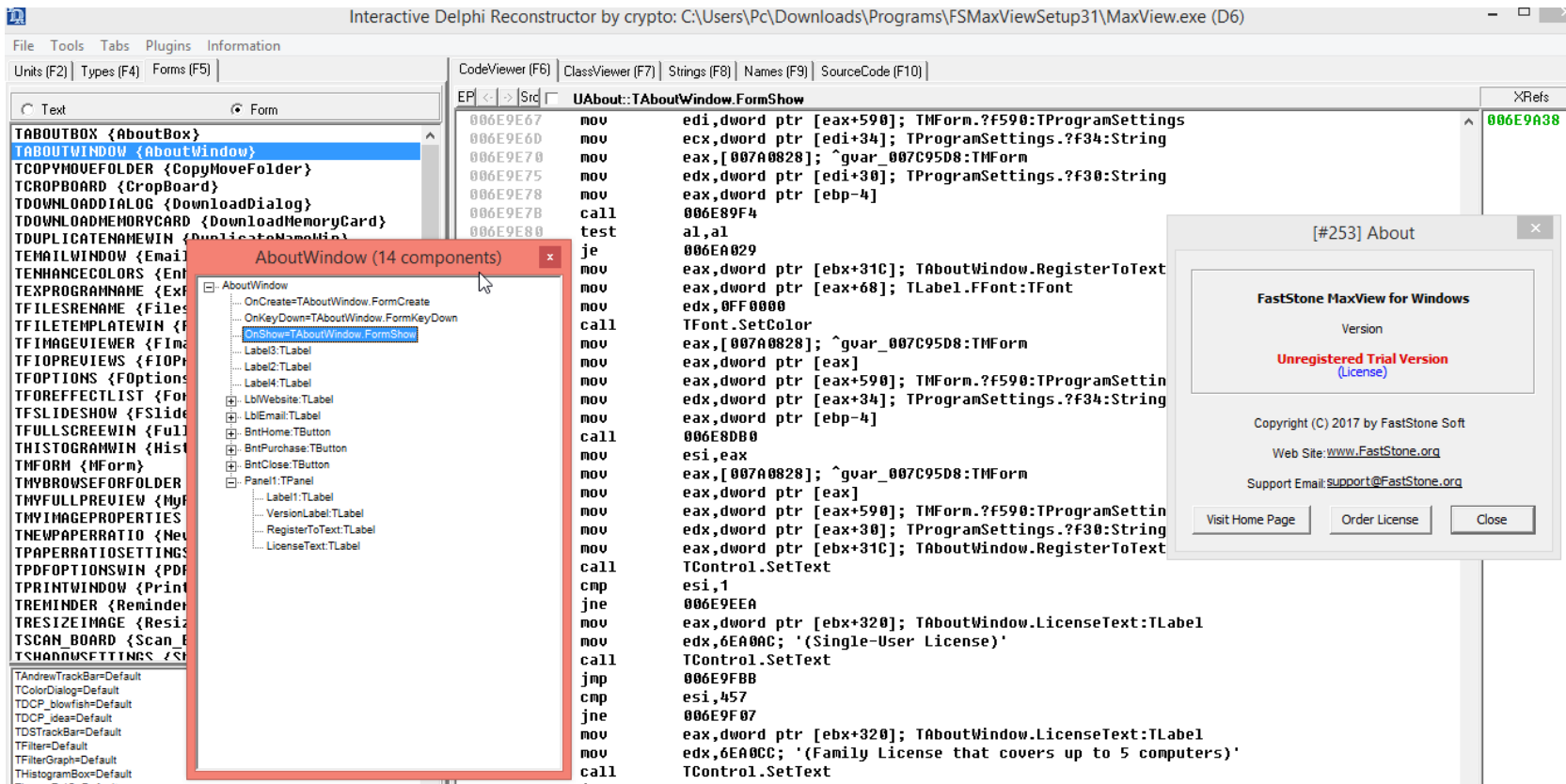
Luego seguimos a IDR (como verán al ver el form show, se tiene toda la realidad)



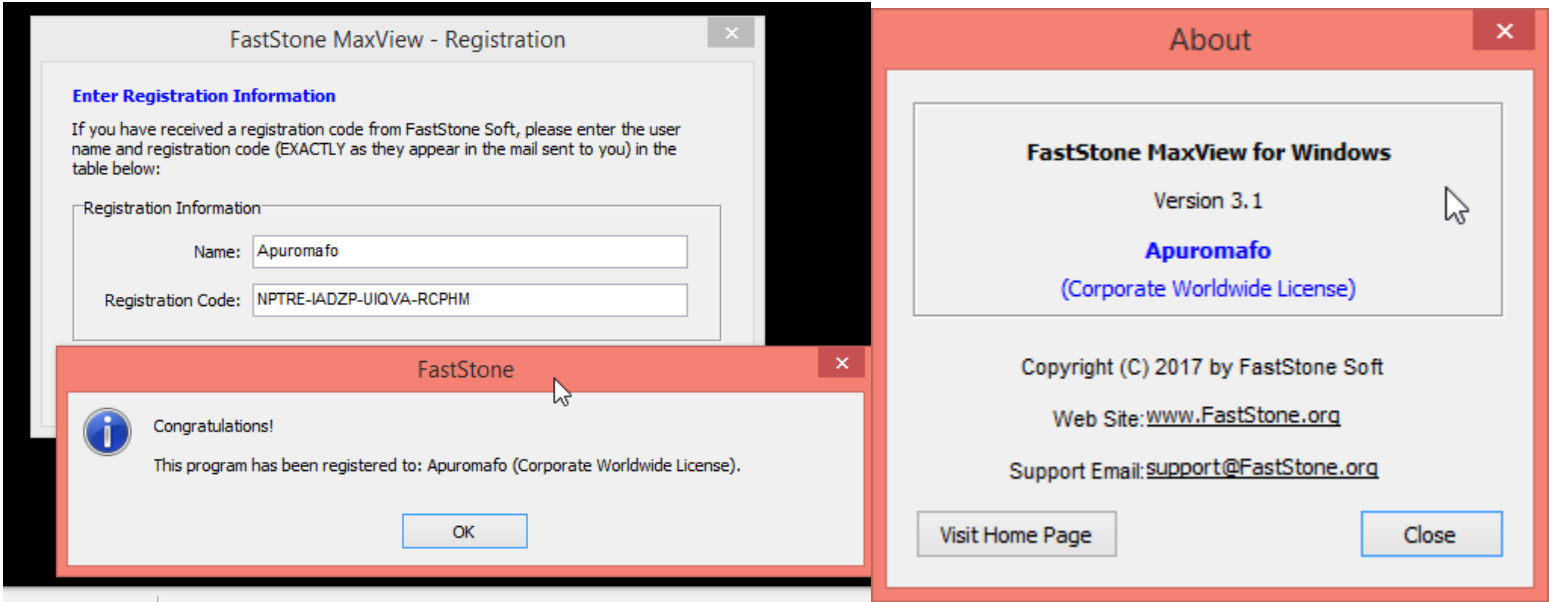


<img33 programa3 en IDR >

Aun sin depurarlo sabemos que ser similar al FastStone capture.



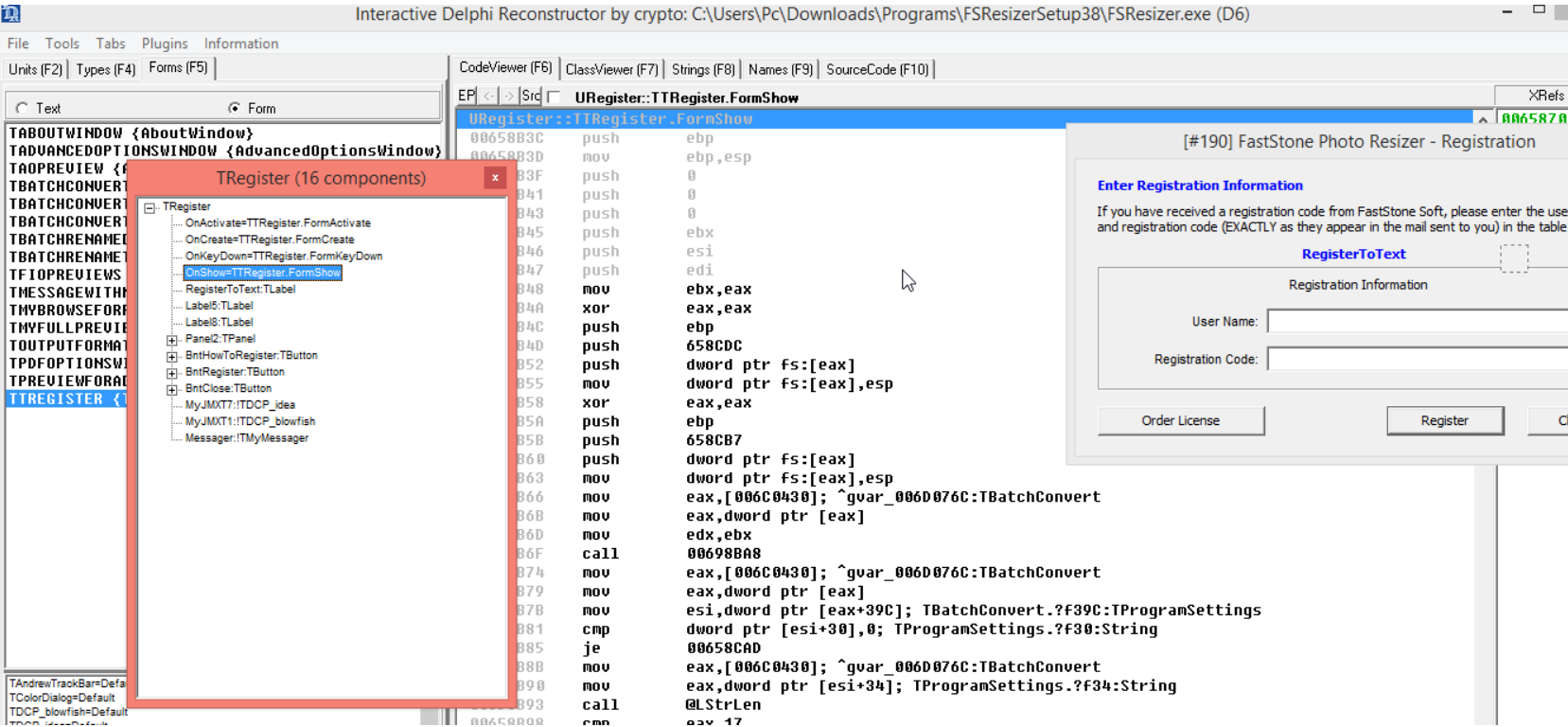
<img34 programa3 en IDR >



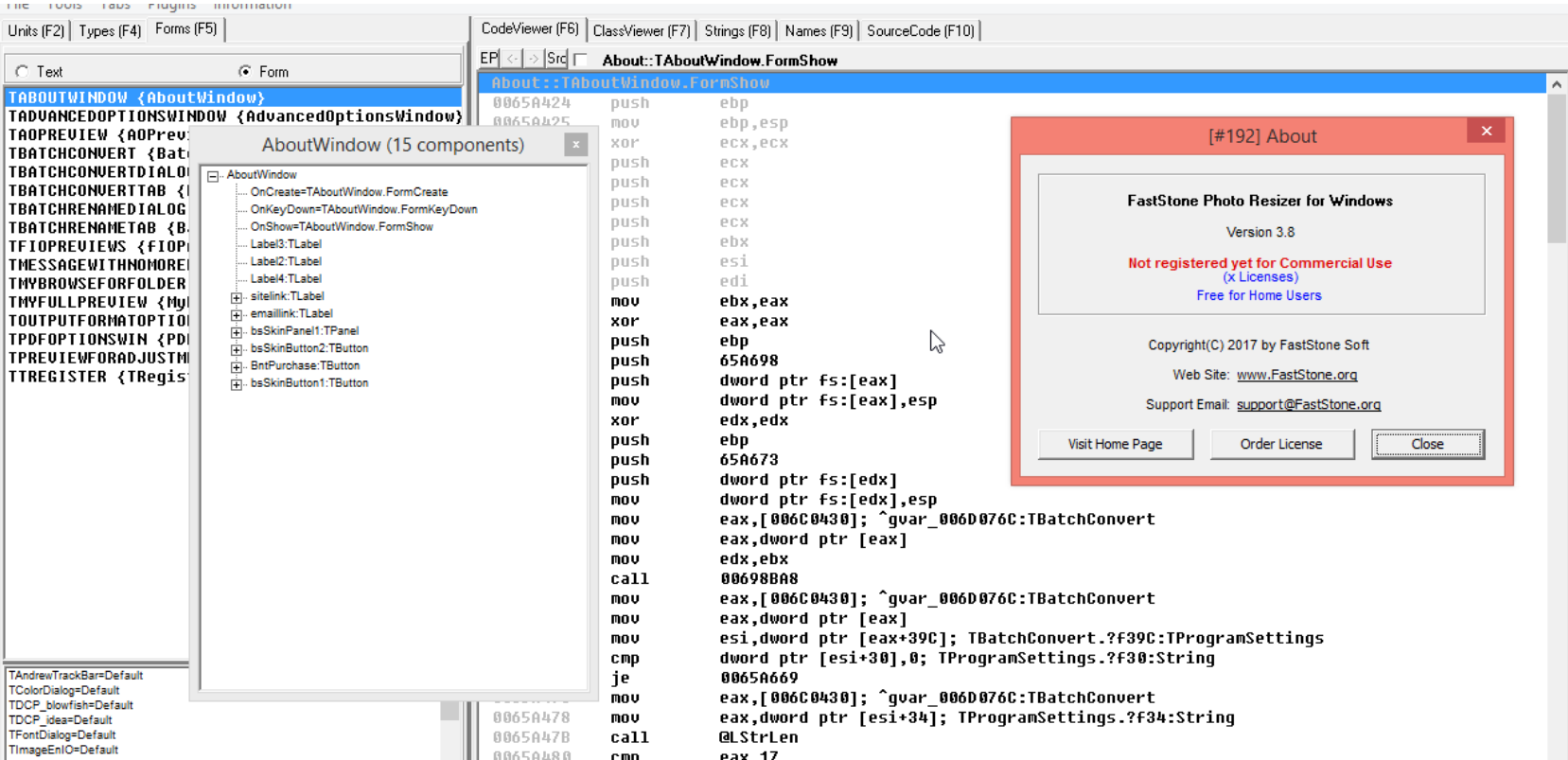
<img35 programa3 en x64dbg una vez parchado>



En Idr es claro que será como el segundo explorado



<img40 programa4 en IDR >

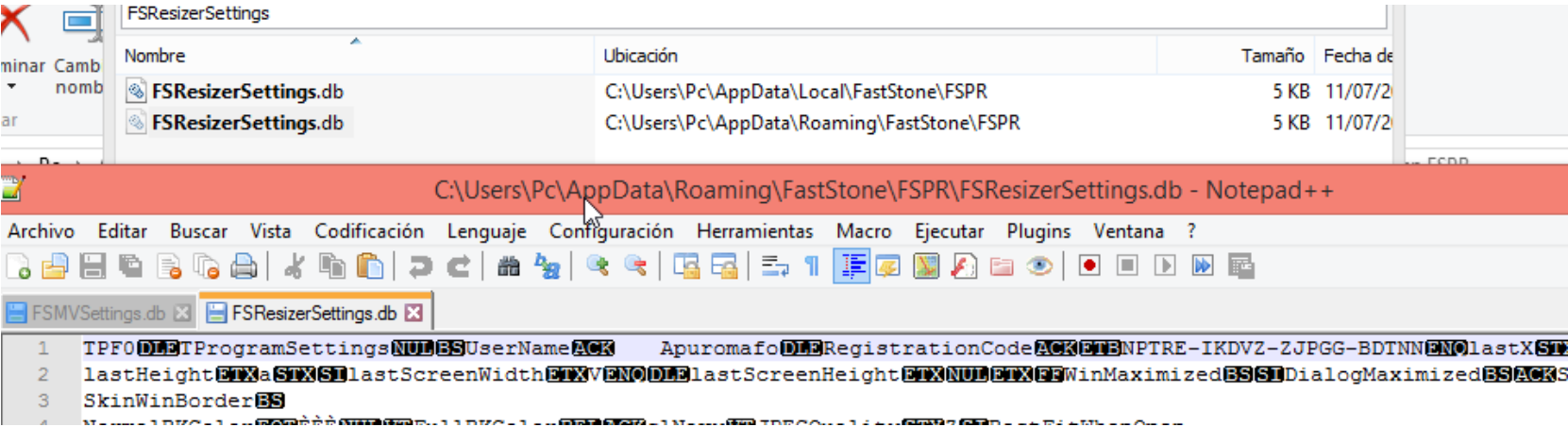


<img41 programa4 en IDR >



<img42 programa4 en x32dbg una vez parchado >

Y la licencia es almacenada en 2 lugares



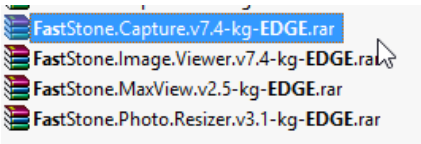
<img programa4 lugar de sus licencias >

Así que en resumen todos los soft han almacenado en roaming, con sus respectivos acrónimos

Usuarios > Pc > AppData > Roaming > FastStone >			
Nombre	Fecha de modifica...	Tipo	Tamaño
FSC	10/07/2017 09:34 ...	Carpeta de archivos	
FSIV	11/07/2017 02:01 ...	Carpeta de archivos	
FSMV	11/07/2017 02:18 ...	Carpeta de archivos	
FSPR	11/07/2017 02:26 ...	Carpeta de archivos	

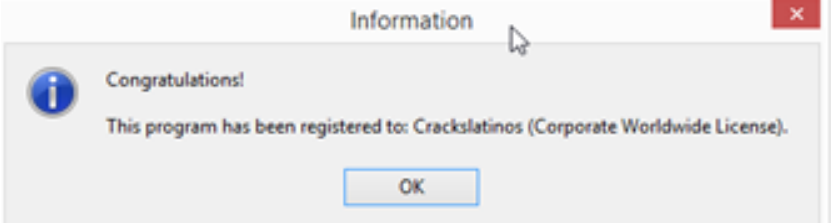
<img43 FastStone lugar de sus licencias en común >

Si hablamos de logro, sabemos que esta compañía ha sido keygeneada en el mundo underground, existen keygens para la compañía FastStone como el team edge el cual tiene keygens validos para todos los niveles de licencia.



<img44 Everything: keygens de edge para faststone>

Que como es de esperar registra el programa desde versiones antiguas hasta las más nuevas sin necesidad de parchar nada, en todos los soft



<img45 programa: usando el serial desde el keygens de edge para faststone>

Así que asumimos que el programa no ha cambiado con el tiempo en su algoritmo para cada soft personal.

Palabras Finales:

Tenemos un programa que ha sido revisado por un team y que su algoritmo no ha variado en el tiempo , existen 2 formatos de registración , puede entrarse por el lado de expired en el primer algoritmo , y en el entrar el registración puede ser el segundo, las validaciones anti nag, están bien (exploración de X.0), las validaciones de largo de serial también (por dos algoritmos uno para ingresar el serial y otro en el about), la verificación de expired se basa en la existencia de el archivo de licencia (solo en 1,2,3 lugares dependiendo de la version), sea como sea lo único novedoso del día de hoy es que su licencia es almacenado con los mismos nombres de variables, no hemos mostrado todos los parches para no comprometer mas el software que no se ve mal ,No se ha mostrado todos los parches del programa para dejar una idea amena que es posible solo explorando con IDR (herramienta indispensable del tute)

Tiempo en ser verificado	Tiempo en hacer el tutorial
Lapsos pequeños de a 5 -10 minutos, a lo más en 20 minutos ha caído	En lapsos pequeños de redacción, 3horas a lo más No me pidan corregir ortografía, es muy poco el tiempo que disponemos.

Saludos A la Lista de Crackslatinos, PeruCrackers y a TSRh.

Dedicado a los lectores que suelen practicar y/o aprender reversing o simplemente una lectura amena, está más que decir que si te ha gustado el software y si tienes la posibilidad de comprarlo no dejes de apoyar al soporte del programa.

Saludos Cordiales



Apuromafo TSRh

