



Un saludo a todos en CrackSlatinoS. Bienvenidos a mi segundo tute. Realmente lo voy a llamar brute jejeje ya que le aplique la fuerza bruta, no muy elegante como dice el amigo Caos Reptante en su tutorial de assembler ya veremos porque, este tute lo hice en dos partes la primer él desempacado y la segunda en como registrarse. Quien quiera puede pasarse la primera y seguir con la según parte eso queda a su gusto. Bueno sin tanto hablar les presentare mi segunda victima.

Victima: FastStone Capture v6.1

Versión: 6.1

URL: <http://www.faststone.org/FSCaptureDetail.htm>

Proteccion: UPX v0.89.6- v1.02/v1.05-v1.25, serial, etc.

Herramientas: RDG Packer Detector, OllyDbg y plugins, ImportRec16f.

Compilador: Borland Delphi v6.0 – v7.0

Cracker: Kernel065

Datos de la victima:

FastStone Capture is a powerful, lightweight, yet full-featured screen capture tool that allows you to easily capture and annotate anything on the screen including windows, objects, menus, full screen, rectangular/freehand regions and even scrolling windows/web pages. You can choose to send captures to editor, file, clipboard, printer, email, Word/PowerPoint document or upload them to your website. Editing tools include annotating (texts, arrowed lines, highlights), resizing, cropping, sharpening, watermarking, applying edge effects and many more. It also allows you to record screen activities and sound into highly compressed video files. Other features include global hotkeys, automatic filename generation, support for external editors, a color picker, a screen magnifier and a screen ruler.

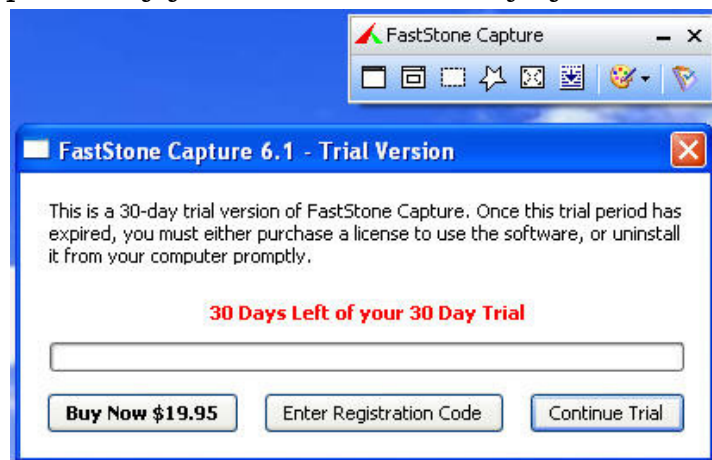
FastStone Capture saves files in BMP, GIF, JPEG, PCX, PNG, TGA, TIFF and PDF formats.



Primera parte

AL ATAQUE.

Bueno como que voy hacer una serie de tutoriales sobre los capturadores de pantalla jeje en fin al instalarlo y ejecutarlo nos muestra su bella presentación.

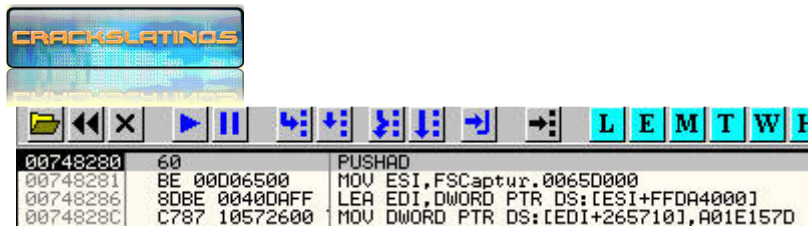


Bueno tenemos tres opciones para utilizar este programa comprándolo que lo dudo, metiendo un serial a ver si tenemos suerte ummm!!!! o utilizarlo como trial, bueno yo usare la cuarta opción buscar al chico bueno, jijijiji!!!!.

Sin más preámbulo vamos a analizarlo con RDG Packer Detector v0.6.6. 2k8 a ver que nos dice.



Bueno estamos en presencia de un upx v0.89.6-v1.02/v1.05-v1.25 etc, etc, etc, para este Packer existen muchas técnicas de cómo quitárnoslo del camino, yo opte por buscar el salto más largo para encontrar el OEP, analicémoslo con el Olly claro está que al arrancarlo nos dará unas advertencias nos saltamos y entramos.



Este es el EP que nos muestra el Olly en nuestro caso es el falso así bajamos más y buscamos nuestro salto largo.

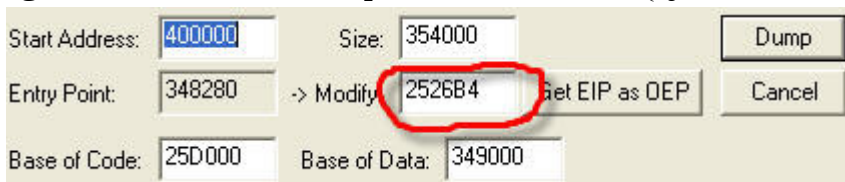
Aquí lo tenemos colocamos un break point con F2 y damos Run, después de



estar parados en la posición de memoria 00748433 lo corremos con F7, caemos en nuestro OEP,



ahí ya podemos utilizar uno de los plugins del Olly en este caso Ollydump, agamoslo a ver que nos da {ojo destildamos Rebuild Import}.



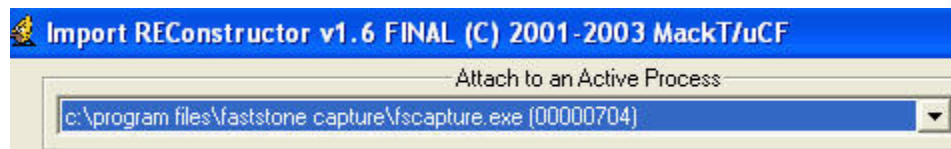
la información marcada con el círculo en rojo la guardamos para el ImportReconstructor, le damos click a Get EIP as OEP y luego a Dump, y nos crea un archivo el cual yo guarde con el nombre FSCapture_dump,



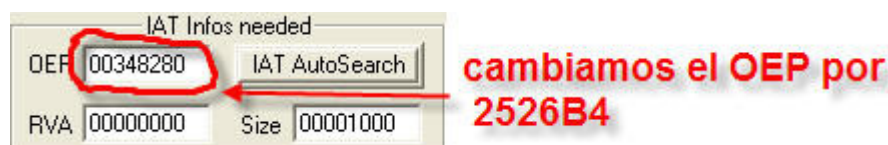
hay que recordar que este archivo al ejecutarlo nos dará error debido a que no hemos reparado la IAT como hacemos esto?. Bueno tenemos dos opciones buscamos el inicio y el final de la IAT el largo y el OEP yo lo hice pero no me funcionó jejeje no sé por qué, en fin o utilizando solo las herramientas a ver si tenemos suerte que es mi caso jejejeje.



Abrimos el ImportReconstructor y con el programa parado en el OEP con el olly hacemos click en el proceso como lo muestra la imagen.



Y luego hacemos click en IAT AutoSearch, pero antes de eso cambiamos el valor del OEP que nos muestra por el 2526B4, hagamos a ver que pasa.

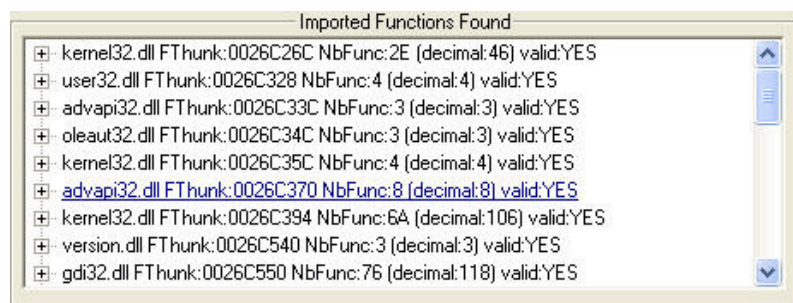



No arroja este cartelito hacemos click en ok, pero antes observamos algo



Original IAT RVA found at: 0026C368 in Section RVA: 0025D000 Size:000EC000

Que nos ha modificado los valores de la IAT, bueno lo dejamos así, hacemos click en Get Imports y...



Bien todo está de maravilla jejeje sin ningún problema vemos que todas las entradas a las Apis de la IAT están bien, hacemos click en Fix Dump  y en este momento nos solicita abrir el archivo dumpeado con el OllyDump en mis caso es FSCapture_Dump.exe.



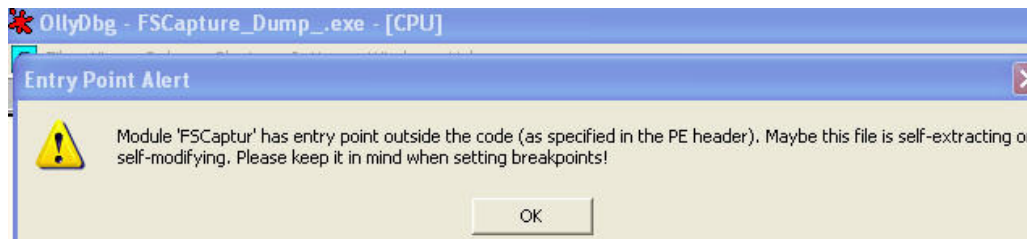
y lo guarda con el nombre FSCapture_Dump_.exe

```
Image Import Descriptor size: 258; Total length: 2558  
C:\Program Files\FastStone Capture\FSCapture_Dump_.exe saved successfully.
```

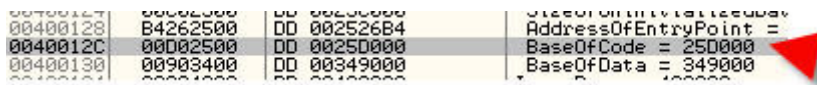
Lo abrimos y...



Arranca sin ningún problema jejeje bueno ya me ha restado 3 días, es lo que llevo haciendo el tute jejeje. Analicémoslo con el Olly a ver como le quedaron las entrañas después de lo que le hice jijiji.



Que Mierda es esta huy perdón por la mala palabra, nos muestra un cartel malo diciéndonos que nuestro entry point esta fuera de la sección de code. Bueno siguiendo siempre las teorías del Maestro RincNar nos vamos de forma inmediata PE-header en Olly y buscamos el puntero Base of code a ver que nos dice.



Allí esta nos apunta a 25D000, bueno eso es por hacerlo por el camino fácil jejeje fuel el ImporReconstructor que lo colocho cuando hizo los cálculos vamos a cambiarlo pero hacia donde jeje miremos con el Olly en VIEW-M y busquemos la sección code donde queremos mandarlo.

CRACKSLATINOS

003A0000	00002000	FSCaptur		PE header	Map	R	R
00400000	00001000	FSCaptur	UPX0	code	Imag	R	RWE
00401000	0025C000	FSCaptur	UPX1		Imag	R	RWE
0065D000	000EC000	FSCaptur	.rsrc	data,resource	Imag	R	RWE
00749000	0000B000	FSCaptur	.mact	imports	Imag	R	RWE
00754000	00003000	FSCaptur			Map	R E	R E
00760000	00004000				Map	R E	R E

Aquí esta es al 401000 a partir del 1000 así que lo cambiamos. Con modify integer en el Olly y...

003A0000	00002000	FSCaptur		PE header	Map	R	R
00400000	00001000	FSCaptur	UPX0	code	Imag	R	RWE
00401000	0025C000	FSCaptur	UPX1		Imag	R	RWE
0065D000	000EC000	FSCaptur	.rsrc	data,resource	Imag	R	RWE
00749000	0000B000	FSCaptur	.mact	imports	Imag	R	RWE
00754000	00003000	FSCaptur			Map	R E	R E
00760000	00004000				Map	R E	R E

Bueno hay lo tenemos jejeje lo corremos sin problemas asunto arreglado. Uffff!!! Esta es la primera parte del Brutorial, ya tenemos el programa desempacado ahora viene el poder registranos será para la segunda parte.

Breve descanso.

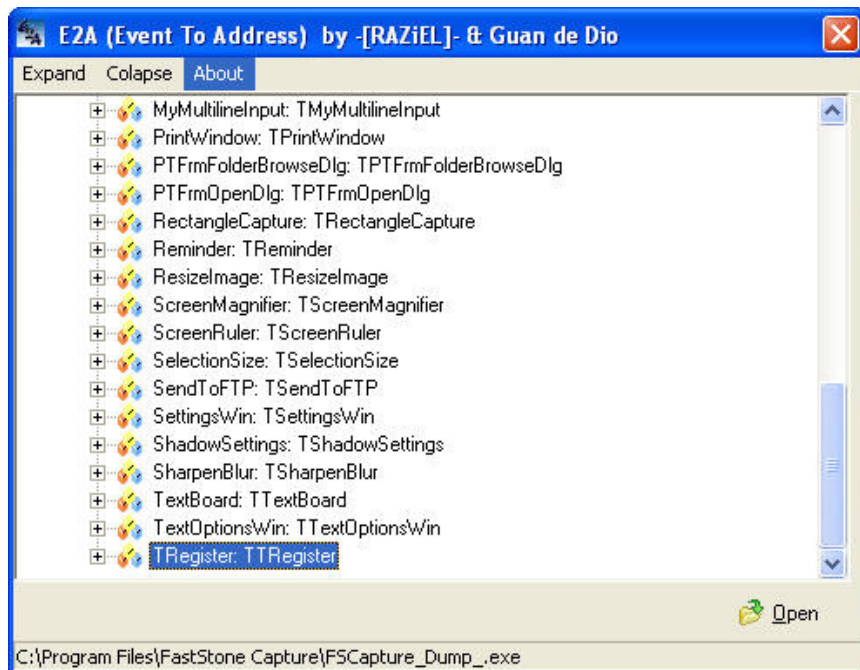




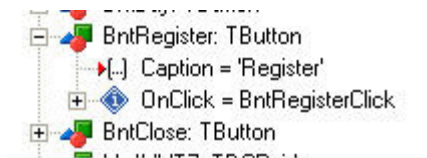
Segunda parte

Bueno espero no hayan quedado agotados ni decepcionados con la primera parte jejeje vámonos a la segunda a ver cómo nos va.

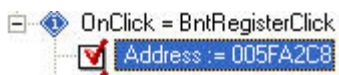
Ya el RDG Packer Detector v0.6.6. 2k8 nos dio una pista de cómo esta compilado el programa así que en este caso utilizaremos el E2A para probarlo a ver cómo nos va jejeje.



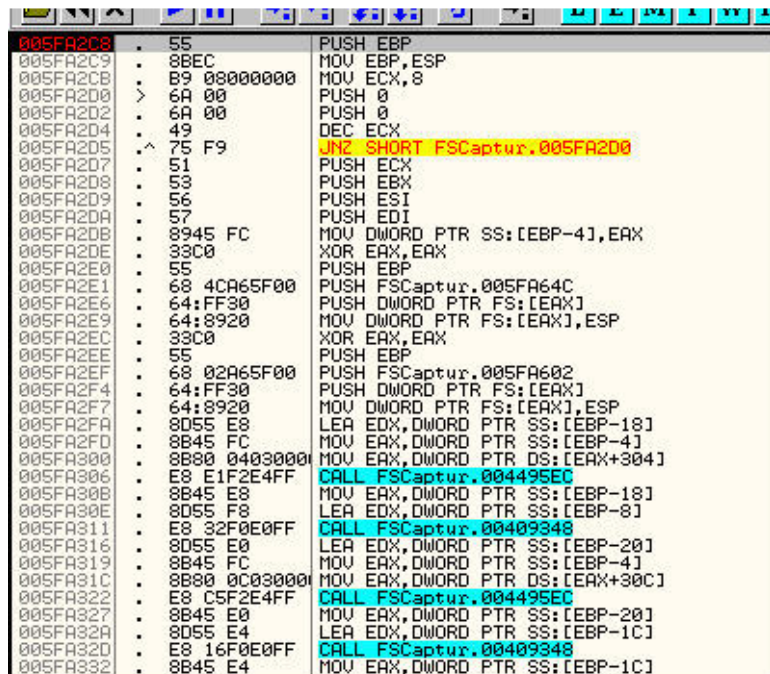
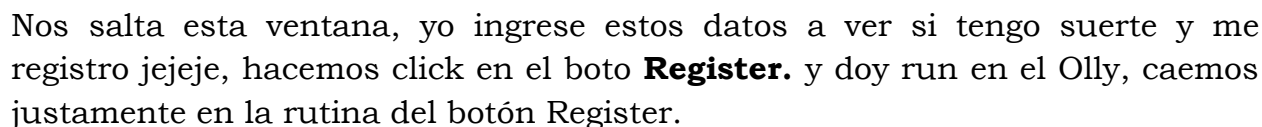
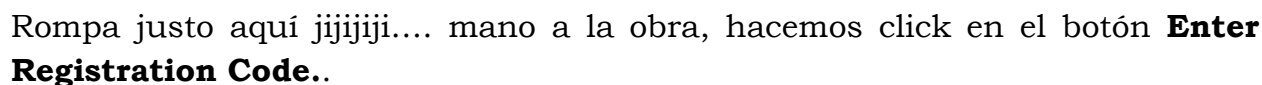
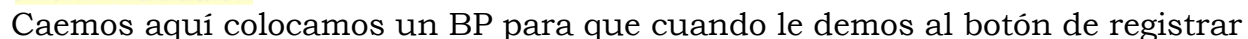
Bueno y buscando pistas encontramos algo como TRegister:TRegister que será entremos.



Ummm!!! aquí esta lo que buscábamos el control del boton para registrase jejeje. Le damos al evento OnClick.



Copiamos la dirección que allí no arroja en el Olly.





Recorramos esta rutina hacia abajo a ver a donde nos lleva.

005FA40E	0F84 C501000	JE FSCapture.005FA5D9
005FA414	8B55 F4	MOV ECX, DWORD PTR SS:[EBP-C]
005FA424	0F84 AF01000	JE FSCapture.005FA5D9
005FA42A	8B55 F4	MOV ECX, DWORD PTR SS:[EBP-C]

Aquí tenemos dos saltos, JE que nos lleva a la dirección 005FA5D9 el siguiente va la misma dirección.

```

005FA5D6 < E8 070E0FFF CALL FSCaptur.005FA5F8
005FA5D7 > EB 1F JMP SHORT FSCaptur.005FA5F8
005FA5D8 > 6A 00 PUSH 0
005FA5D9 > 66:8B0D 68A6 MOV CX,WORD PTR DS:[5FA668D]
005FA5E2 > B2 02 MOV DL,2
005FA5E4 > B8 3CA95F00 MOV EAX,FSCaptur.005FA93C
005FA5E9 > E8 A67BE4FF CALL FSCaptur.00442194
005FA5EE > 33C9 XOR EAX,EAX

```

Arg1 = 00000000

ASCII "Invalid User Name or Registration Code!"
FSCaptur.00442194

Al ir a dichas direcciones caemos en el chico malo. ya esto se guiso jejeje. Pero donde esta nuestro chico bueno.

```

005FA40E < 0F84 C5010001 JE FSCaptur.005FA509
005FA414 > 8B4D F4 MOV ECX,DWORD PTR SS:[EBP-C]
005FA417 > 8B55 F8 MOV EDX,DWORD PTR SS:[EBP-8]
005FA41A > 8B45 FC MOV EAX,DWORD PTR SS:[EBP-4]
005FA41D > E8 FEBFFFFF CALL FSCaptur.005FA020
005FA422 > 84C0 TEST AL,AL
005FA424 < 0F84 AF010001 JE FSCaptur.005FA509
005FA42A > 8B55 F4 MOV EDX,DWORD PTR SS:[EBP-C]
005FA42D > 8B45 FC MOV EAX,DWORD PTR SS:[EBP-4]
005FA430 > E8 7BFCFFFF CALL FSCaptur.005FA0B0
005FA435 > 8BDB MOV EBX,EAX
005FA437 > 83FB 01 CMP EBX,1
005FA43A < 7F 2D JB SHORT FSCaptur.005FA469
005FA43C > 6A 00 PUSH 0
005FA43E > 6A 00 PUSH 0
005FA440 > 5D45 D8 LEA EAX,DWORD PTR SS:[EBP-28]
005FA443 > 50 PUSH EAX
005FA444 > 33C9 XOR ECX,ECX
005FA446 > 8B55 F8 MOV EDX,DWORD PTR SS:[EBP-8]
005FA449 > B8 98A65F00 MOV EAX,FSCaptur.005FA698
005FA44E > E8 5D310500 CALL FSCaptur.006405B0
005FA453 > 8B45 D8 MOV EAX,DWORD PTR SS:[EBP-28]

```

ASCII "Congratulations! This program has been registered to: %1% (Single-User License)."

Que malos soy jejeje los hice sufrir un poco, bueno están justo debajo de los saltos al chico malo, esto significa que si cambiamos el JE 5FA5D9 por JE 5FA43C estaremos registrados hagámoslo para ver que pasa.

```

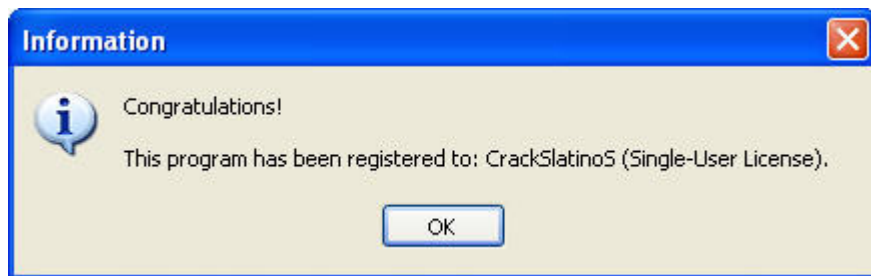
005FA490/ E8 74FBFFFF CALL FSCaptur.005FA990
005FA49C E8 84C0      TEST AL,AL
005FA40E 74 2C       JE SHORT FSCaptur.005FA43C
005FA410 90          NOP
005FA411 90          NOP
005FA412 90          NOP
005FA413 90          NOP
005FA414 90          NOP
005FA417 8B4D F4     MOV ECX,DWORD PTR SS:[EBP-C]
005FA418 8B55 F8     MOV EDX,DWORD PTR SS:[EBP-8]
005FA41A 8B45 FC     MOV EAX,DWORD PTR SS:[EBP-4]
005FA41D E8 FEFBFFFF CALL FSCaptur.005FA020
005FA422 90          TEST AL,AL
005FA424 74 16       JE SHORT FSCaptur.005FA43C
005FA426 90          NOP
005FA427 90          NOP
005FA428 90          NOP
005FA429 90          NOP
005FA42A 90          NOP
005FA42D 8B55 F4     MOV EDX,DWORD PTR SS:[EBP-C]
005FA42D 8B45 FC     MOV EAX,DWORD PTR SS:[EBP-4]
005FA430 E8 7BFCFFFF CALL FSCaptur.005FA000
005FA435 8BD8        MOV EBX,EBX
005FA437 83BF 01     CMP EBX,1
005FA43A 7F 2D       JG SHORT FSCaptur.005FA469
005FA43C 6A 00       PUSH 0
005FA43E 6A 00       PUSH 0
005FA440 8D45 D8     LEA EAX,DWORD PTR SS:[EBP-28]
005FA443 50          PUSH EAX
005FA444 33C9        XOR ECX,ECX
005FA446 8B55 F8     MOV EDX,DWORD PTR SS:[EBP-8]
005FA449 B8 98A65F00 MOV E8,FSCaptur.005FA698
005FA44E E8 5D310500 CALL FSCaptur.0064D500
005FA453 8B45 D8     MOV EAX,DWORD PTR SS:[EBP-28]
005FA456 66:8B0D 68A6 MOV CX,WORD PTR DS:[5FA668]
005FA45D B2 02       MOV DL,2
005FA45F E8 307DE4FF CALL FSCaptur.00442194

```

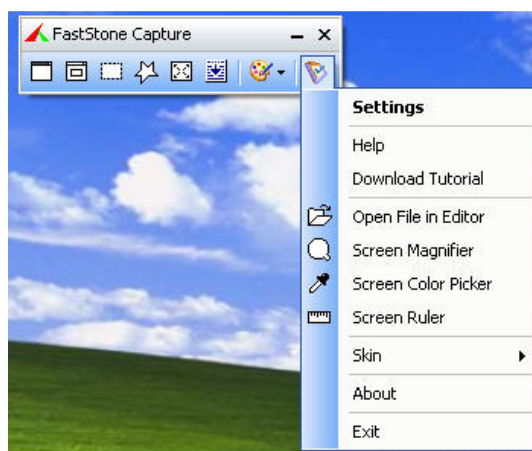
Quedaría algo así luego le damos salvar pero con otro nombre por si no funciona, yo lo guarde con el nombre `FSCapture_Dump_1`.



Ok lo corremos y le ingresamos lo mismos datos en **User Name:** CrackSlatinoS y en **Registration Code:** 98989898989898989898....., hacemos click en el botón Register y ta ta ta tan



Estamos registradooooos bravo bravo jejeje jejeje, sigamos miremos que otra cosa podemos quitar. Hacemos click en el botón **ok** y ya no nos sale esa fastidiosa nag solicitándonos registrar, hacemos click en **setting.** y luego no vamos a **About.**



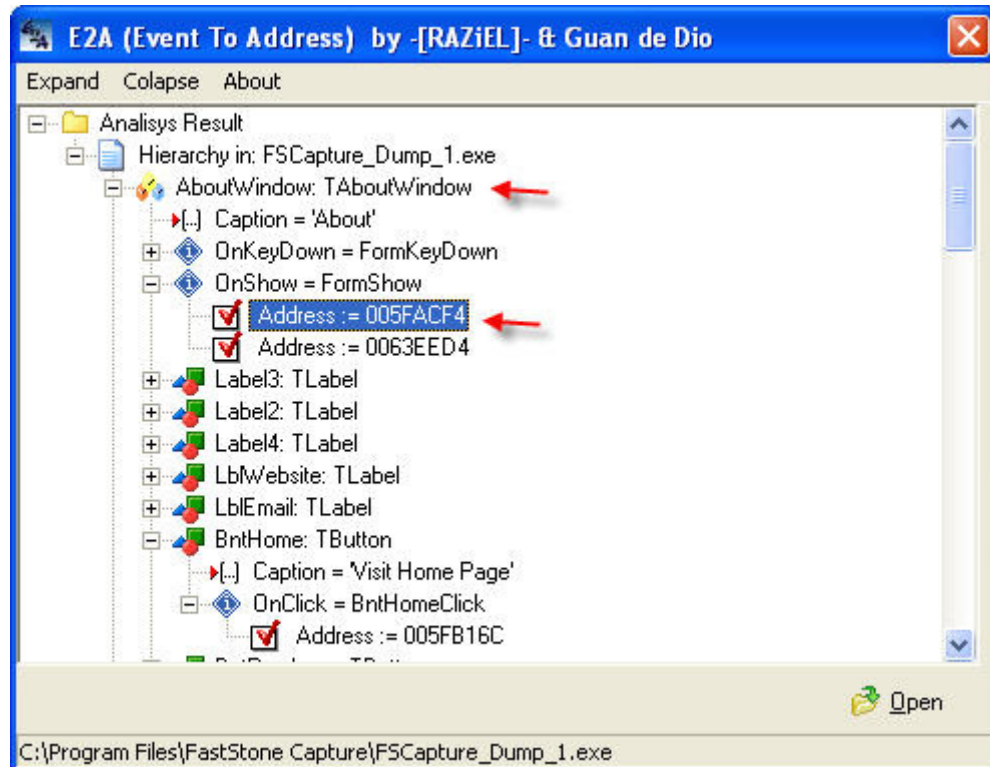
Para ver que información nos da.



Grrrrrr. No sale un cartelito Rojo recordándonos que es un versión trial y que no estamos registrados y aparte de eso que lo compremos.



Carguémoslo otra vez en el E2A y busquemos alguna pista con ese About.



Aquí tenemos algo en la Form **AboutWindow: TAboutWindow**. Abrimos el evento OnShow y copiamos la dirección **005FACF4** en el Olly y hacemos un BP para que pare cuando demos click en About. Hagámoslo!!!

005FACF0	00	008D4000	DB 00
005FACF4	55		DD FSCaptur.00408D00
005FACF5	8BEC		PUSH EBP
005FACF7	33C9		MOV EBP,ESP
005FACF9	51		XOR ECX,ECX
005FACFA	51		PUSH ECX
005FACFB	51		PUSH ECX
005FACFC	51		PUSH ECX

Efectivamente ahí nos para el programa y estamos dentro de la rutina del About, indaguemos un poco dentro de esta rutina.

005FADCC	83F8 17	CMP EAX,17
005FADCF	0F85 F9010000	JNZ FSCaptur.005FAFCE
005FADD5	33D2	XOR EDX,EDX
005FAE14	84C0	TEST AL,AL
005FAE16	0F84 95010000	JE FSCaptur.005FAFB1
005FAE1C	A1 E84E6600	MOV EAX,DWORD PTR DS:[664EE8]
005FAE21	8B40	MOV EAX,DWORD PTR DS:[EAX]
005FAE3C	84C0	TEST AL,AL
005FAE3E	0F84 6D010000	JE FSCaptur.005FAFB1
005FAE44	8B83 1C030000	MOV EAX,DWORD PTR DS:[EBX+31C]
005FAE4A	8B40 68	MOV EAX,DWORD PTR DS:[EAX+68]

Después de varios F7 y pruebas llegue a estos tres saltos que van hacia una misma dirección El CHICO MALO jeje, la dirección es 005FAFB1, tenemos dos opciones nopear los saltos o cambiar el CMP EAX,17 por CMP EAX,0 el TEST



AL,AL por TEST CL,CL cuando digo el cambiar el AL,AL por CL,CL es porque al recorrer el programa vamos a tener 01 en este registro, yo opte por hacer lo segundo cambiar el CMP EAX,17 para el salto JNZ y el TEST AL,AL para los dos salto JE y así evito los nop ya entendieron le que dije al principio del amigo Caos Reptante jejeje. Hagamoslo!!!.



Jejeje aparece el nombre con el cual lo registramos, y nos ale el botón de **Buy Now**. pero hay algo que no me gusta ese (0-User License) cambiémoslo. Nos vamos nuevamente al Olly y....



Dentro de la misma rutina del About encontramos este salto JNZ XXXXX para que no se ejecute y nos salga el texto que queremos cambiamos el CMP ESI,1386 por CMP ESI,0 así el JNZ no se ejecuta. Al correrlo nuevamente no queda asi.



Tenemos una licencia Educational Worldwide jejeje. Ok dejémonos de juegos jeje, se terminino



Espero les haya gustado este humilde tutorial (brutorial jeje), va dirigido en agradecimiento a un buen amigo Cracker que me ha tenido paciencia por tantas preguntas que le he hecho, así como también a todos los listeros de CrackSlatinoS un saludo especial.

Agradecimientos

Zelt@, Thunder, CIS | ShaDDy, +NCR/CRC! [ReVeRsEr], MCKSys Argentina, APOKLIPTIKO, Ratón, Guillermo, Joe Cracker, COCO, MAKKAKO, Lisa&Alquimista, Caos Reptante y mucho otros más que en estos momentos se me escapan de la mente, por supuesto no puede faltar el maestro Ricardo Narvaja. Muchas gracias por dar sus conocimientos Maestro. Nos estamos viendo en la próxima entrega.

